

# *NetScreen CLI Reference Guide*

*Note to Reader: This is a preliminary version of this document. An updated version will be made available in the very near future.*

P/N 093-0011-000 Rev D  
Version 2.6.0

## *Copyright Notice*

Copyright © 2000-2001 NetScreen Technologies, Inc.  
All rights reserved. Printed in USA.

## *Licenses, Copyrights, and Trademarks*

THE SPECIFICATIONS REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS. NO PART OF THIS DOCUMENT MAY BE REPRODUCED OR TRANSMITTED IN ANY FORM OR BY ANY MEANS, ELECTRONIC OR MECHANICAL, FOR ANY PURPOSE, WITHOUT RECEIVING WRITTEN PERMISSION FROM NETSCREEN TECHNOLOGIES INC.

## *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.

# Contents

Who Should Read This Manual? .....	v
Organization .....	v
Related Publications .....	vi
<b>Chapter 1 Getting Started .....</b>	<b>1-1</b>
Before You Begin .....	1-1
Connect the NetScreen Device to the PC .....	1-2
Starting the Terminal Emulator .....	1-2
Conventions .....	1-2
Command Summary .....	1-4
Set and Unset Commands.....	1-4
Get Commands.....	1-6
Clear Commands.....	1-8
Miscellaneous Commands.....	1-9
<b>Chapter 2 Set and Unset Commands .....</b>	<b>2-1</b>
address.....	2-3
admin .....	2-5
alarm.....	2-11
arp.....	2-12
auth .....	2-14
clock .....	2-18
console.....	2-20
dhcp.....	2-23
dhcp client (see “dhcp” on page 2-23).....	2-27
dhcp server (see “dhcp” on page 2-23) .....	2-29
dialup-group .....	2-32
dns.....	2-34
domain .....	2-35
envar .....	2-36
ffilter .....	2-37
firewall .....	2-39
ftp .....	2-44
gc-reg .....	2-45
global .....	2-46
global-pro .....	2-49
group.....	2-51
ha .....	2-54
ha track ip .....	2-57
hostname .....	2-60

ike.....	2-61
interface .....	2-66
ippool .....	2-75
l2tp .....	2-76
mac .....	2-78
mip .....	2-79
ntp .....	2-81
pki .....	2-83
policy .....	2-85
pppoe .....	2-88
route.....	2-90
scheduler .....	2-92
scs .....	2-93
service .....	2-94
snmp .....	2-96
ssl.....	2-98
syslog.....	2-99
timer .....	2-101
traffic-shaping .....	2-102
url .....	2-103
user .....	2-106
vip .....	2-108
vpn .....	2-110
vpnmonitor .....	2-112
vsys.....	2-113
vsys-traffic.....	2-114
webtrends.....	2-115
Chapter 3 Get Commands.....	3-1
address.....	3-4
admin .....	3-5
alarm.....	3-8
arp.....	3-13
auth .....	3-14
chassis.....	3-17
clock .....	3-18
config.....	3-19
console.....	3-21
counter .....	3-22
dhcp.....	3-27
dialup-group .....	3-28
dip.....	3-29
dns.....	3-30
domain .....	3-31
envvar .....	3-32
file.....	3-33
firewall .....	3-35

---

gate.....	3-36
global.....	3-37
global-pro .....	3-38
glog.....	3-39
group.....	3-40
ha.....	3-42
hostname .....	3-43
ike.....	3-44
interface .....	3-47
ippool .....	3-50
l2tp .....	3-51
lance.....	3-52
log .....	3-53
mac-count .....	3-58
mac-learn .....	3-59
master .....	3-60
memory .....	3-61
mpsess.....	3-62
mip .....	3-63
nsp-tunnel.....	3-64
ntp .....	3-65
os.....	3-66
pki .....	3-67
policy .....	3-69
pport.....	3-71
route.....	3-72
sa.....	3-74
scheduler .....	3-77
scs .....	3-78
service .....	3-79
session .....	3-81
snmp .....	3-83
socket.....	3-85
software-key .....	3-86
ssl.....	3-87
syslog.....	3-88
system.....	3-90
tech-support .....	3-91
timer .....	3-92
traffic-shaping interface .....	3-93
url .....	3-94
user .....	3-95
vip .....	3-97
vpn .....	3-98
vpnmonitor .....	3-100
vsys.....	3-101
webtrends.....	3-102



Chapter 4 Clear Commands.....	4-1
admin .....	4-2
alarm.....	4-3
arp.....	4-5
auth .....	4-6
counter.....	4-7
crypto.....	4-8
dbuf.....	4-9
dhcp.....	4-10
dns.....	4-12
file.....	4-13
ike-cookie.....	4-14
l2tp .....	4-15
log .....	4-16
mac-count .....	4-18
mac-learn .....	4-19
node_secret .....	4-20
pppoe .....	4-21
sa.....	4-22
sa-statistics.....	4-23
session .....	4-24
Chapter 5 Miscellaneous Commands.....	5-1
enter vsys.....	5-2
exec dhcp.....	5-3
exec dns.....	5-4
exec ha .....	5-5
exec ntp .....	5-6
exec ping (see “ping” on page 5-14) .....	5-7
exec pki.....	5-8
exec pppoe .....	5-9
exec save (see “save” on page 5-16).....	5-10
exec software-key .....	5-11
exec trace-route .....	5-12
exit.....	5-13
ping .....	5-14
reset.....	5-15
save .....	5-16
snoop .....	5-19
trace-route .....	5-21
Index .....	IX-1

# Preface

*Note to Reader:* This is a preliminary version of this document. An updated version will be made available in the very near future.

The *NetScreen CLI Reference Guide* describes the commands used to configure and manage a NetScreen device from a console interface. The *Command Line Interface Guide* is an ongoing publication, published with each NetScreen OS release.

## WHO SHOULD READ THIS MANUAL?

This document is used by system and network administrators who 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,” 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,” describes each command available for configuring the NetScreen device.

Chapter 3, “Get Commands,” 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.



### Note

*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 are into the system are 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 2-3	All models
admin on page 2-5	All models
arp on page 2-12	All models
auth on page 2-14	All models
clock on page 2-18	All models
console on page 2-20	All models
dhcp client (see “dhcp” on page 2-23) on page 2-27	NetScreen-5 at version 1.65 or later
dhcp server (see “dhcp” on page 2-23) on page 2-29	NetScreen-5 at version 1.65 or later
dialup-group on page 2-32	All models
domain on page 2-35	All models
dns on page 2-34	All models
envar on page 2-36	All models except the NetScreen-5
ffilter on page 2-37	All models
firewall on page 2-39	All models
ftp on page 2-44	All models at version 1.66 or later
global on page 2-46	All models (future release for the NetScreen-1000)
global-pro on page 2-49	All models

**Table 1.1** Summary of Set and Unset Commands (continued)

<b>Command and Page</b>	<b>Supported on These NetScreen Device Models</b>
group on page 2-51	All models at version 2.0 or later
hostname on page 2-60	All models
ha on page 2-54	NetScreen-100 and NetScreen-1000
ike on page 2-61	All models
interface on page 2-66	All models
ippool on page 2-75	All models
mip on page 2-79	All models
ntp on page 2-81	NetScreen-5 at version 1.65 or later
pki on page 2-83	All models at version 2.0 or later
policy on page 2-85	All models
pppoe on page 2-88	NetScreen-5
route on page 2-90	All models
scheduler on page 2-92	All models
scs on page 2-93	NetScreen-100 and NetScreen-1000 (future release)
service on page 2-94	All models
snmp on page 2-96	All models
ssl on page 2-98	All models
syslog on page 2-99	All models
timer on page 2-101	NetScreen-5, NetScreen-10, and NetScreen-100 only
traffic-shaping on page 2-102	All models
url on page 2-103	All models
user on page 2-106	All models
vip on page 2-108	All models; load balancing on the NetScreen-100 and NetScreen-1000 only
vsys on page 2-113	NetScreen-1000
vpn on page 2-110	All models with some exceptions



## Get Commands

Use **Get** commands to display system configuration parameters and data.

**Table 1.2** Summary of Get Commands

<b>Command and Page</b>	<b>Supported on These NetScreen Device Models</b>
address on page 3-4	All models
admin on page 3-5	All models
alarm on page 3-8	All models except the NetScreen-1000
arp on page 3-13	All models
auth on page 3-14	All models
chassis on page 3-17	NetScreen-1000
clock on page 3-18	All models
config on page 3-19	All models
console on page 3-21	All models
counter on page 3-22	All models
dialup-group on page 3-28	All models
dip on page 3-29	All models
domain on page 3-31	All models
envar on page 3-32	All models except the NetScreen-5
file on page 3-33	All models
firewall on page 3-35	All models
global on page 3-37	All models (future release for the NetScreen-1000)
group on page 3-40	All models at version 2.0 or later
hostname on page 3-43	All models
ha on page 3-42	NetScreen-100 and NetScreen-1000
ike on page 3-44	All models
interface on page 3-47	All models
log on page 3-53	All models except the NetScreen-1000
mac-count on page 3-58	NetScreen-1000

**Table 1.2** Summary of Get Commands (continued)

<b>Command and Page</b>	<b>Supported on These NetScreen Device Models</b>
mac-learn on page 3-59	All models
memory on page 3-61	NetScreen-1000
mip on page 3-63	All models
mpsess on page 3-62	NetScreen-1000
ntp on page 3-65	NetScreen-5
pki on page 3-67	All models
policy on page 3-69	All models
route on page 3-72	All models
sa on page 3-74	All models
scheduler on page 3-77	All models
service on page 3-79	All models
session on page 3-81	All models
snmp on page 3-83	All models
scs on page 3-78	Future release for the NetScreen-100 and NetScreen-1000
syslog on page 3-88	All models
system on page 3-90	All models
tech-support on page 3-91	All models
timer on page 3-92	NetScreen-5, NetScreen-10, and NetScreen-100 only
traffic-shaping interface on page 3-93	NetScreen-5, NetScreen-10, and NetScreen-100 only.
url on page 3-94	All models
user on page 3-95	All models
vip on page 3-97	All models
vsys on page 3-101	NetScreen-1000
vpn on page 3-98	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

<b>Command and Page</b>	<b>Supported on These NetScreen Device Models</b>
admin on page 4-2	All models
alarm on page 4-3	All models except the NetScreen-1000
arp on page 4-5	All models
auth on page 4-6	All models
counter on page 4-7	All models
dbuf on page 4-9	All models
dhcp on page 4-10	NetScreen-5 at version 1.65 or later
dns on page 4-12	All models
file on page 4-13	All models
ike-cookie on page 4-14	All models
log on page 4-16	All models except the NetScreen-1000
mac-count on page 4-18	NetScreen-1000
mac-learn on page 4-19	All models
node_secret on page 4-20	All models
sa on page 4-22	All models
sa-statistics on page 4-23	All models
session on page 4-24	All models

## Miscellaneous Commands

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

**Table 1.4** Summary of Miscellaneous Commands

<b>Command and Page</b>	<b>Supported on These NetScreen Device Models</b>
enter vsys on page 5-2	NetScreen-1000
exec dhcp on page 5-3	NetScreen-5
exec dns on page 5-4	All models
exec ha on page 5-5	NetScreen-100 at version 2.0 or later, and the NetScreen-1000
exec ntp on page 5-6	NetScreen-5
exec pki on page 5-8	All models except the NetScreen-1000
exit on page 5-13	All models
ping on page 5-14	All models
reset on page 5-15	All models
save on page 5-16	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.

The **Set / Unset** commands include the following:

- **address** (page 2-3)
- **admin** (page 2-5)
- **alarm** (page 2-11)
- **arp** (page 2-12)
- **auth** (page 2-14)
- **clock** (page 2-18)
- **console** (page 2-20)
- **dhcp** (page 2-23)
- **dhcp client** (see “**dhcp**” on page 2-23) (page 2-27)
- **dhcp server** (see “**dhcp**” on page 2-23) (page 2-29)
- **dialup-group** (page 2-32)
- **dns** (page 2-34)
- **domain** (page 2-35)
- **envar** (page 2-36)
- **ffilter** (page 2-37)
- **firewall** (page 2-39)
- **ftp** (page 2-44)
- **gc-reg** (page 2-45)
- **global** (page 2-46)
- **global-pro** (page 2-49)
- **group** (page 2-51)
- **ha** (page 2-54)
- **ha track ip** (page 2-57)
- **hostname** (page 2-60)
- **ike** (page 2-61)

- 
- **interface** (page 2-66)
  - **ippool** (page 2-75)
  - **l2tp** (page 2-76)
  - **mac** (page 2-78)
  - **mip** (page 2-79)
  - **ntp** (page 2-81)
  - **pki** (page 2-83)
  - **policy** (page 2-85)
  - **pppoe** (page 2-88)
  - **route** (page 2-90)
  - **scheduler** (page 2-92)
  - **scs** (page 2-93)
  - **service** (page 2-94)
  - **snmp** (page 2-96)
  - **ssl** (page 2-98)
  - **syslog** (page 2-99)
  - **timer** (page 2-101)
  - **traffic-shaping** (page 2-102)
  - **url** (page 2-103)
  - **user** (page 2-106)
  - **vip** (page 2-108)
  - **vpn** (page 2-110)
  - **vpnmonitor** (page 2-112)
  - **vsys** (page 2-113)
  - **vsys-traffic** (page 2-114)
  - **webtrends** (page 2-115)

---

# address

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

## Syntax

**set address trust <string>**

**set address untrust <string>**

**set address DMZ <string>**

## Arguments

<b>trust &lt;string&gt;</b>	Specifies the trusted interface.
<b>untrust &lt;string&gt;</b>	Specifies the untrusted interface.
<b>dmz &lt;string&gt;</b>	For NS-10 and -100. Specifies the DMZ interface.

## Availability

This feature is supported on all NetScreen device models.

## Defaults

There are four system-defined address book entries:

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

## Examples

To define a PM2 address for a web server named **webserver** with an IP address and netmask 184.2.50.9/24 and a netmask:

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



---

To define a trusted address for a desktop machine named **mparker** with an IP address and netmask 172.16.10.1/32 and a netmask with the comment **Mary's desktop**:

```
ns-> set address trust mparker 172.16.10.1 255.255.255.255 Mary's
desktop
```

To delete an untrusted address for a partner site named **my-partner**:

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

See Also

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

---

## admin

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

Syntax

**set admin auth** { radius-port <number> | secret <string> | server-name <string> | timeout <number> | type { Local | Radius } }

**set admin format** { dos | unix }

**set admin mail** { alert | mail-addr1 <string> | mail-addr2 <string> | server-name <string> | traffic-log }

**set admin manager-ip** <a.b.c.d>

**set admin name** <string>

**set admin password** <string>

**set admin port** <number>

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

**set admin user** <string>

---

## Arguments

### **auth**

#### **radius-port <number>**

Server port for a RADIUS server.

#### **secret**

Shared secret for a RADIUS server.

#### **server-name**

The IP address or the server name (DNS is configured and enabled) of the RADIUS server.

#### **timeout**

Specifies the length of idle time in minutes before automatically closing the administrative session. The value can be up 999 minutes. Using 0 indicates that an inactive administrative session never times out.

#### **type { local | radius }**

Specifies either the internal database or an external RADIUS server.

### **format {dos | unix}**

Applies to all NetScreen devices. Use to select the format the device uses to generate a configuration file, which can be downloaded to a TFTP server or PCMCIA card (NS-10, -100, and -1000) via the CL1 and to a local directory via the WebUI.

---

**mail**

Enables e-mail for sending alerts and traffic logs.

**alert**

Collects system alarms from the device for sending to an e-mail address.

**mail-addr1 <email-address>**

Sets the first e-mail address for sending alert and traffic logs.

**mail-addr2 <email-address>**

Sets a second e-mail address for sending alert and traffic logs.

**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).

**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.

**manager-ip <a.b.c.d>**

Restrict management to an IP address for remote host or subnet. The <a.b.c.d> represents the IP address. The default IP address is 0.0.0.0, which allows management from any workstation. All NetScreen devices allow you to specify up to six hosts or subnets, one at a time.

When using the **unset admin manager-ip** command, specifies one or all of the six possible management IP addresses.

**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.

NS-1000. The root administrator of a virtual system issues the **set admin name** command to assign the login name for a virtual system administrator.

---

<b>password</b>	<p>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.</p> <p>Also, the root administrator of a virtual system issues the <b>set admin password name</b> command to assign the login name for a virtual system administrator.</p>
<b>port &lt;number&gt;</b>	<p>Sets the port number for listening for configuration changes when using the web. Use any number between 1024 and 32,767, or use the default port number—80.</p> <p>Changing the admin port number on the NetScreen-5 and -10 requires resetting the device. See the <b>reset</b> command on page 5-12.</p>
<b>sys-ip</b>	<p>Use this IP address to manage the NetScreen device. If the NetScreen device is in NAT or Route mode, the system IP address must be in the subnet as the physical interface through which you plan to access the system IP address.</p>
<b>user</b>	<p>The login name of non-root administrators (super administrators and sub administrators) for the NetScreen device. The maximum length of the user name is 31 characters, including all symbols except ?. The user name is case-sensitive.</p>

### Availability

This feature is supported on all NetScreen device models.

### Defaults

This is a list of 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 NetScreen device assigns this default.
- The sys-ip is 192.168.1.1 (it is 209.125.148.254 before firmware 1.61).
- The default privilege for a super administrator is all.
- 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 39yJoJ15:

```
ns-> set admin password 39yJoJ15
```

To assign a super administrator named joe with the password rc1404AL:

```
ns-> set admin user joe password rc1404AL
```

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** commands.

---

# alarm

**Description:** Use the **set alarm** command to set alarm parameters.

Syntax

**alarm threshold { CPU <number> | memory <number> }**

Arguments

**threshold**

**CPU <number>**

Percentage of CPU used (1 to 100%).

**memory <number>**

Percentage of threshold memory used (1 to 100%).

Availability

This feature is supported on all NetScreen device models.

Defaults

—

Examples

To set alarm parameters :

```
ns-> set alarm
```

See Also

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



---

## arp

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

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

### Syntax

**set arp <a.b.c.d>**

**set arp age <number>**

**set arp always-on-dest**

**set arp no-cache**

### Arguments

<b>&lt;a.b.c.d&gt;</b>	Defines the IP address for the machine.
<b>age &lt;number&gt;</b>	Sets the age-out value (in seconds) for ARP entries.
<b>always-on-dest</b>	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.
<b>no-cache</b>	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 **get arp** and **clear arp** commands.

---

## 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).

When the NetScreen device is using SecurID to authenticate users and is not communicating properly with the ACE server, check the **clear node\_secret** command to clear the current SecurID shared secret so that you can reset.

Syntax

**set auth ldap { server-name <string> }**

**set auth radius-port <number>**

**set auth secret <string>**

**set auth securid { auth-port <number> | duress <number> | encr <number> | master <string> | retries <number> | slave <string> | timeout <number> | server-name <string> | timeout <number> }**

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

---

## Arguments

<b>ldap server-name &lt;string&gt;</b>	Specifies the name for the LDAP server.
<b>radius-port &lt;number&gt;</b>	Specifies the Radius Server port.
<b>secret &lt;string&gt;</b>	Defines the password shared between the NetScreen device and the RADIUS server. It is used to authenticate all transactions between the two devices.
<b>server-name &lt;string&gt;</b>	Defines the RADIUS server for user authentication and specifies either the server IP address or domain name (if you have already configured the DNS settings).

---

  
**securid****auth-port <number>**

Specifies the port number to use for communications with the SecurID server.

**duress { 0 | 1 }**

The number 1 specifies that the SecurID server is licensed to use duress mode, a SecurID feature that allows you to log in using a password that secretly alerts the SecurID server to suspend your login privileges until you have contacted the SecurID admin. The 0 specifies that the duress mode option is not enabled.

**encr <number>**

Specifies the encryption algorithm for SecurID network traffic:

- 0 specifies (SDI)
- 1 specifies Data Encryption Standard (DES)

The default type DES is recommended.

**master <string>**

Specifies either the IP address or domain name for the primary SecurID server.

**retries <number>**

Specifies the number of retries allowed for attempting authentication with the SecurID server.

**slave <string>**

Specifies either the IP address or the domain name for the secondary SecurID server.

**timeout <number>**

Specifies the length of idle time in minutes before terminating authentication status. Valid range is from 0-255 minutes.

---

**type { 0 | 1 | 2 | 3 }**

Specifies the type of authentication method to use:

- 0 for the built-in NetScreen database
- 1 for a RADIUS server
- 2 for a SecurID server
- 3 for a LDAP server

### 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 **2CKpt5ab**:

```
ns-> set auth secret 2CKpt5ab
```

To specify the SecurID server primary IP address as 209.134.22.1 with authentication port 5005, and using the DES encryption:

```
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
```

### See Also

See the **get auth**, **clear 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>

**set clock dst-off**

**set clock ntp**

**set clock zone** <number>

## Arguments

<mm/dd/yyyy>	Specifies the month, day, and year. Specifies the hour and minutes in the 24-hour time format.
<b>dst-off</b>	Turns off the automatic time adjustment for daylight saving time.
<b>ntp</b>	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.
<b>zone</b> <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.

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.

Syntax

**set console dbuf**

**set console disable**

**set console page <number>**

**set console timeout <number>**

Arguments

<b>dbuf</b>	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.
<b>disable</b>	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.
<b>page &lt;number&gt;</b>	Specifies how many lines are displayed per page on the console, where <number> is an integer.
<b>timeout &lt;number&gt;</b>	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.

---

# dhcp

**Description:** Use the **set dhcp** command to configure the DHCP.

Syntax

For NetScreen-5, -10 only:

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

For NetScreen-5, -10, -100 device models:

```
set dhcp relay { server-name <string> | service | vpn }
```

```
set dhcp server { ip <a.b.c.d> | option { dns1 <a.b.c.d> | dns2 <a.b.c.d> |  
dns3 <a.b.c.d> | domainname <string> | gateway <a.b.c.d> | lease  
<number> | netmask <a.b.c.d> | news <a.b.c.d> | nis1 { nis1 } | nis2  
<a.b.c.d> | nistag <string> | pop3 <a.b.c.d> | smtp <a.b.c.d> | wins1  
<a.b.c.d> | wins2 <a.b.c.d> } | service }
```

---

## Arguments

---

<b>client (NS-5, NS-10 only)</b>	<b>autoconfig</b>
	<b>lease &lt;number&gt;</b>
	<b>server &lt;a.b.c.d&gt;</b>
	<b>vendor &lt;string&gt;</b>
<b>relay</b>	<b>server-name &lt;string&gt;</b>
	<b>service</b>
	<b>vpn</b>

---

**server**

**ip <a.b.c.d>**

**option**

- **dns1 <a.b.c.d>**  
Sets the DNS.
- **dns2 <a.b.c.d>**  
Sets the DNS.
- **dns3 <a.b.c.d>**  
Sets the DNS.
- **domainname <string>**  
Sets the domain name.
- **gateway <a.b.c.d>**  
Sets the client gateway IP.
- **lease <number>**  
Sets the lease
- **netmask <a.b.c.d>**  
Sets the netmask IP.
- **news <a.b.c.d>**  
Sets the news.
- **nis1 { nis1 }**  
Sets the net info server.
- **nis2 <a.b.c.d>**  
Sets the net info server.
- **nistag <string>**  
Sets the net info tag.
- **pop3 <a.b.c.d>**  
Sets the POP3.
- **smtp <a.b.c.d>**  
Sets the SMTP.
- **wins1 <a.b.c.d>**  
Sets the wins.
- **wins2 <a.b.c.d>**  
Sets the wins.

**service**

---

### Availability

This feature is supported on the NetScreen-5, 10, -100. This feature is not supported on the NetScreen-1000.

### Defaults

—

### Examples

To \_ :

```
ns-> set dhcp
```

### See Also

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

---

## dhcp client (see “dhcp” on page 2-23)

**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.

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.

### Syntax

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

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

### Arguments

<b>server &lt;a.b.c.d&gt;</b>	Defines the IP address (a.b.c.d) of the DHCP server from which the NetScreen device obtains its IP address.
<b>vendor</b>	Identifies the manufacturer of the device requesting the IP address.
<b>lease</b>	Defines how long, in minutes, the lease for the IP address lasts. There is no maximum lease time.
<b>autoconfig</b>	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 devices at version 1.65 or later and NetScreen-10 devices at version 2.0 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:

```
set dhcp client server 10.0.0.1
```

## See Also

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

---

## dhcp server (see “dhcp” on page 2-23)

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

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.



### Note

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

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

<b>server service</b>	Enables the DHCP server.
<b>server ip &lt;a.b.c.d&gt; to &lt;e.f.g.h&gt;</b>	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.
<b>server ip &lt;a.b.c.d&gt; mac &lt;mac&gt;</b>	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>.
<b>server option lease &lt;minutes&gt;</b>	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>.
<b>server option gateway &lt;a.b.c.d&gt;</b>	Specifies the IP address of the default trusted gateway used by the clients.
<b>server option netmask &lt;A.B.C.D&gt;</b>	Specifies the trusted netmask of the default gateway.
<b>server option dns1 &lt;a.b.c.d&gt;</b>	Specifies the IP address of the first Domain Name Server.
<b>server option dns2 &lt;a.b.c.d&gt;</b>	Specifies the IP address of the second Domain Name Server.
<b>server option dns3 &lt;a.b.c.d&gt;</b>	Specifies the IP address of the third Domain Name Server.
<b>server option domainname &lt;domain&gt;</b>	Specifies the registered domain name of the networks.
<b>smtp &lt;a.b.c.d&gt;</b>	Specifies the IP address of the SMTP mail server.
<b>pop3 &lt;a.b.c.d&gt;</b>	Specifies the IP address of the POP3 mail server.
<b>news &lt;a.b.c.d&gt;</b>	Specifies the IP address of the News server.
<b>wins1 &lt;a.b.c.d&gt;</b> <b>wins2 &lt;a.b.c.d&gt;</b>	Specifies the IP address of the WINS 1 or WINS 2 server.

## Availability

This feature is supported on the NetScreen-5 model at version 1.65 or later and the NetScreen-10 at version 2.0 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 **get dhcp**, **clear dhcp**, and **exec dhcp** commands.

---

# dialup-group

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

Different platforms can have different number of users in a dialup group.

An access policy for a dialup-group applies to all the members in the group; consequently, all the group members must be the same kind—either IKE/2TP users, or Manual Key users.

## Syntax

**set dialup-group** <string>

## Arguments

<string> Assigns a name to the dialup group.

## 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 remove 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.

---

## dns

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

Syntax

**set dns forward**

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

Arguments

**forward**

Sets up forward DNS requests.

**host { dns1 <a.b.c.d> | dns2 <a.b.c.d> | schedule }**

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 <string>**

## Arguments

**<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** command.



---

## envar

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

### Syntax

**set envar** <string>

### Arguments

<string> 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

On 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:

```
ns1000-> 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.

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 later specify the port numbers for the packets.

However, 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 you 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.

## Syntax

**set ffilter dst-ip <a.b.c.d>**

**set ffilter dst-port <number>**

**set ffilter ip-proto <number>**

**set ffilter src-ip <a.b.c.d>**

**set ffilter src-port <number>**

## Arguments

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

## 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.

---

# firewall

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

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

## Syntax

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

**set firewall applet**

**set firewall bypass-non-ip**

**set firewall bypass-others-ipsec**

**set firewall default-deny**

**set firewall icmp-flood [ threshold <number> ]**

**set firewall ip-spoofing**

**set firewall ip-sweep [ threshold <number> ]**

**set firewall land**

**set firewall log-self**

**set firewall ping-of-death**

**set firewall port-scan [ threshold <number> ]**

**set firewall src-route**

**set firewall syn-flood [ alarm-threshold <number> | attack-threshold <number> | queue-size <number> ]**

**set firewall tear-drop**

**set firewall udp-flood [ threshold <number> ]**

**set firewall winnuke**

---

## Arguments

<b>applet</b>	Blocks all embedded Java and ActiveX applets, DOS .exe files, .dll files, and compressed files of types .zip, .gzip, and .tar.
<b>bypass-non-ip</b>	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.)
<b>bypass-others-ipsec</b>	Openly passes all IPSec traffic through a NetScreen device in Transparent mode. The NetScreen device does not act as a VPN tunnel gateway but passes the IPSec packets onward to other gateways.
<b>default-deny</b>	Denies all traffic not specifically allowed by an Access Policy.
<b>icmp-flood [threshold &lt;number&gt;]</b>	<p>Detects Internet Control Message Protocol (ICMP) floods. 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.</p> <p>The threshold defines the number of ICMP packets per second allowed to ping the same destination address before the NetScreen device rejects further ICMP packets. The range is 1 to 1,000,000.</p>
<b>ip-spoofing</b>	Spoofing attacks occur when unauthorized agents attempt to bypass firewall security by imitating valid client IP addresses. Invalidates these false source IP address connections.
<b>ip-sweep [threshold &lt;microseconds&gt;]</b>	Detects and prevents an IP Sweep attack. This kind of attack occurs when ICMP echo requests (pings) are sent to different destination addresses in hopes that one of them will reply, thus uncovering an address to target. You can set the IP Sweep threshold in microseconds between 1 and 1,000,000. When the threshold is reached, the NetScreen device drops further echo requests from the remote source address.

---

<b>land</b>	Prevents Land attacks by combining elements of the SYN flood defense mechanism and IP spoofing protection. Land attacks occur when an attacker sends spoofed IP packets containing the IP address of the target as both the source and destination IP address in its header. These packets are sent with the SYN flag set to a system with any port that is listening. The victim creates empty sessions to itself by filling its session table and overwhelms its resources.
<b>log-self</b>	Enables the feature that logs dropped packets and pings destined for the NetScreen device.
<b>ping-of-death</b>	<p>Detects and rejects oversized and irregular ICMP packet sizes.</p> <p>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.</p>
<b>port-scan [threshold &lt;microseconds&gt;]</b>	<p>Prevents port scan attacks based upon the defined port-scan threshold value in microseconds. When the threshold is reached, the NetScreen device rejects further packets from the remote source. Valid range is 1 to 1,000,000.</p> <p>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.</p>
<b>src-route</b>	<p>Blocks all IP traffic that uses the IP Source Route Option.</p> <p>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.</p>
<b>syn-flood</b>	SYN flood attacks occur when the connecting host continuously sends TCP SYN requests without replying to the corresponding ACK responses. Detects SYN Flood attacks.

---

<b>syn-flood [alarm-threshold &lt;number&gt;]</b>	Defines the number of proxied, half-complete connections per second at which an alarm is entered in the Event Alarm log.
<b>syn-flood [attack_threshold &lt;number&gt; ]</b>	Defines the number of SYN packets per second required to trigger the SYN proxying mechanism.
<b>syn-flood [queue-size &lt;number&gt;]</b>	Defines the number of proxied connection requests held in the proxied connection queue before the system starts rejecting new connection requests.
<b>tear-drop</b>	Tear Drop attacks occur when fragmented IP packets overlap and cause the host attempting to reassemble the packets to crash. If the NetScreen device discovers such a discrepancy in a fragmented packet, it drops it.
<b>udp-flood [threshold &lt;number&gt;]</b>	<p>UDP flooding occurs when UDP packets are sent with the purpose of slowing down the system to the point that it can no longer process valid connection requests.</p> <p>The number of packets allowed per second to the same destination IP address/port pair. When this number is exceeded, an alarm is generated and subsequent packets are dropped. The valid range is from 1 to 1,000,000.</p>
<b>winnuke</b>	Detects attacks on Windows NetBios communications, modifies the packet as necessary, and passes it on. A WinNuke attack triggers an attack log entry in the event alarm log.

## Availability

This feature is supported on all NetScreen device models.

## Defaults

If all the firewall defense mechanisms are enabled by default, performance might be affected. The following firewall features are enabled by default:

- src-route
- syn-flood
- tear-drop
- ping-of-death
- ip-spoofing
- land
- applets

---

Default firewall option values for all NetScreen device models:

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



---

## ftp

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

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 is still metered by the stateful inspection monitor.

### Syntax

**set ftp data-port { any }**

### Arguments

**data-port { any }** Specifies any FTP data port.

### 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
```

---

## gc-reg

**Description:** Use the **set gc-reg** command to set GC registers.

Syntax

**set gc-reg <number>**

Arguments

**gc-reg <number>** Specifies the port number (0 to 2).

Availability

This feature is supported on only the NetScreen-1000.

Defaults

—

Examples

To \_ :

```
ns-> set gc-reg
```

See Also

See the **get gc-reg** command.

---

# global

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

The NetScreen device uses configuration port and the reporting port to send information to the management station (the workstation running the NetScreen-Global Manager software). The NetScreen device uses the local listening port 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 argument.



## Note

*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.*

## Syntax

**set global config-port <number>**

**set global enable**

**set global keep-alive <number>**

**set global listen <number>**

**set global report-port <number>**

**set global send [ log [ network { resource [ summary ] | summary } ] | [ network | resource [ summary ] | summary ] | network [ resource [ summary ] | summary ] | summary ] | resource [ summary ] | summary ]**

**set global server-name <string>**

**set global vpn**

---

## Arguments

<b>config-port</b> <number>	Designates the port number for sending configuration information to the management station.
<b>enable</b>	Enables the NetScreen device for remote management with NetScreen-Global Manager software.
<b>keep-alive</b> <number>	Specifies how often (in seconds) the NetScreen device sends <b>keep-alive</b> UDP packets to affirm its existence to the management station. The range is 5–60 seconds.
<b>listen</b> <number>	Designates the port number on the NetScreen device for receiving (listening) for configuration information from the management station.
<b>report-port</b> <number>	Designates the port number for sending out <b>keep-alive</b> UDP packets to the management station.
<b>send</b> [ <b>log</b>   <b>network</b>   <b>resource</b>   <b>summary</b> ]	Specifies the kind of information that the NetScreen device sends to the management station: <b>log</b> Specifies event logs, self-deny logs, and traffic logs. <b>network</b> Specifies network activities on the trusted, untrusted, and DMZ interfaces. <b>resource</b> Specifies CPU, flash card, and memory utilization. <b>summary</b> Specifies Traffic summary reports showing the total number of sessions and bytes for the following areas: outbound traffic, inbound traffic, services, access policies, and VPNs.
<b>server-name</b> <string>	Designates the IP address or the server name of the management station.
<b>vpn</b>	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.

---

# global-pro

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

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

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

Syntax

```
set global-pro config { primary <string> | secondary <string> | timeout <number> }
```

```
set global-pro enable
```

```
set global-pro report { alarm-attack { enable } | alarm-other { enable } | alarm-traffic { enable } | attack-stat { enable } | ethernet-stat { enable } | flow-stat { enable } | log-config { enable } | log-info { enable } | log-self { enable } | log-traffic { enable } | policy-stat { enable } | proto-dist { enable | <string> } }
```

**Arguments**

**config { primary <a.b.c.d> | secondary <a.b.c.d> | timeout <number> }** 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.

**timeout <number>**

Specifies the timeout on the SME.

**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).

---

<b>alarm-traffic</b>	Reports all traffic alarms.
<b>attack-stat</b>	Reports all attack statistics.
<b>ethernet-stat</b>	Reports ethernet statistics.
<b>flow-stat</b>	Reports flow statistics.
<b>log-config</b>	Produces the configuration logs.
<b>log-info</b>	Produces information logs.
<b>log-self</b>	Produces self-logs.
<b>log-traffic</b>	Produces traffic logs.
<b>policy-stats</b>	Reports policy statistics.
<b>proto-dist</b>	Reports the distribution of different protocols types.

### 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
```

### 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 can then be referenced by its name in an access policy.

### Syntax

```
set group address { trust <string> | untrust <string> | DMZ <string> }
```

```
set group service <string>
```

### Arguments

**address { trust <string> | untrust <string> | DMZ <string> }** Defines the group as an address group, and specifies the interface for the address group.

**service <string>** Defines the name of the address 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 add the service AOL 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

You cannot include addresses for trusted, untrusted, and DMZ interfaces within the same group.

Each address group and service group you create must have a unique name. In other words, you cannot create a trusted group named **outside-sales** and an untrusted group named **outside-sales**. Similarly, you cannot use the same address group name as a service 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 device	Number of Address Groups	Number of Members per Group
NetScreen-100	64	64
NetScreen-1000	256	64

NetScreen device	Number of Service Groups	Number of Members per Group
NetScreen-5	8	16
NetScreen-10	8	32
NetScreen-100	16	64
NetScreen-1000	32	64

See Also

See the **get group** command.

---

## 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.

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 (NetScreen-100) indicates whether a NetScreen device is operating as a master or a slave. Green indicates the device is running in master mode, and yellow indicates the slave mode.

### Syntax

**set ha arp <number>**

**set ha auth { password <string> }**

**set ha encrypt { password <string> }**

**set ha fast-mode <string>**

**set ha group <number> <string>**

**set ha interface { dmz | trust | untrust }**

**set ha link-up-on-slave <string>**

**set ha monitor { dmz [ trust | untrust ] | trust [ untrust ] | untrust }**

**set ha priority <number>**

**set ha second-path { dmz | trust | untrust }**

**set ha session { off }**

### Arguments

<b>arp &lt;number&gt;</b>	Sets the number of requests the HA master sends out. The default is 2.
---------------------------	--

---

<b>auth { password &lt;string&gt; }</b>	Specifies that HA perform authentication and enforce the specified password. Valid passwords contain from 1 to 16 characters.
<b>encrypt { password &lt;password&gt; }</b>	Specifies that HA encrypt all sessions and configuration packets, and enforce the specified password. Valid passwords contain from 1 to 16 characters.
<b>fast-mode &lt;string&gt;</b>	Specifies the fast mode.
<b>group &lt;number&gt; &lt;string&gt;</b>	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.
<b>interface &lt;trust   untrust   DMZ&gt;</b>	This is only for the NetScreen-100 model. Specifies the interface on which the NetScreen-100 devices are grouped for HA.
<b>link-up-on-slave</b>	Sets the slave unit to the link-up state so that it does not have to go through the spanning tree operation before it can become the master immediately when failover occurs.
<b>monitor</b>	Sets failover from the master HA to the slave. The default is set to monitor the trusted, untrusted, and DMZ interfaces.
<b>priority &lt;number&gt;</b>	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.
<b>second-path</b>	Specifies the second ha link.
<b>session { off }</b>	Stops the master HA from propagating the session's services. Using this command may improve performance.

---

## Availability

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

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

## 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
```

## See Also

See the **get ha** and **exec ha** 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.

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.

The interface name (main or subinterface) must be configured before monitoring can be set.

## 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

 **Note** 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
```

See Also

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



---

# 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>**

## Arguments

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

## Availability

This feature is supported on all NetScreen device models.

## Defaults

For NetScreen-5, it is **ns5**.

For NetScreen-10, it is **ns10**.

For NetScreen-100, it is **ns100**.

For NetScreen-1000, it is **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:

```
acme-> unset hostname
```

## See Also

See the **get hostname** 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 tunnel configuration, and to specify other IKE parameters. For the complete sequence of commands needed to create a VPN tunnel, see **Notes** on page 2-68.

### Syntax

**set ike accept-all-proposal**

**set ike gateway** <string>

**set ike id-mode** { ike ip | subnet }

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

**set ike initiator-set-commit**

**set ike p1-proposal** <string>

**set ike p2-proposal** <string>

**set ike policy-checking**

**set ike respond-bad-spi** <number>

**set ike responder-set-commit**

**set ike single-ike-tunnel** <string>

**set ike soft-lifetime-buffer** <number>

### Arguments

<b>accept-all-proposal</b>	Accepts all incoming proposals. The default is to accept only those proposals matching predefined or user-defined proposals.
<b>gateway</b> <string>	Specifies the gateway name.
<b>id-mode</b> { ip   subnet }	Defines the IKE ID mode in the Phase exchange as either an IP address or a subnet. (Use IP when setting up a VPN tunnel between a NetScreen device and a CheckPoint 4.0 device. Otherwise, use the subnet option.)

---

<b>initial-contact { all-peers   single-gateway &lt;string&gt;   single-user &lt;string&gt; }</b>	<p>By specifying all-peers, the NetScreen device deletes all SAs, and sends an INITIAL_CONTACT notification to each IKE peer during the first IKE single-user &lt;string&gt;   session with that peer after a system reset.</p> <p>By specifying single-gateway &lt;string&gt; or single-user &lt;string&gt;, the NetScreen device deletes all SAs associated with the specified IKE gateway or IKE user, then sends an INITIAL_CONTACT notification during the next IKE session after a system reboot.</p> <p>The default is unset.</p>
<b>initiator-set-commit</b>	<p>Requests the responder to 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.</p>
<b>p1-proposal &lt;name&gt;</b>	<p>Adds or modifies the IKE Phase 1 proposal, which defines the parameters for creating and exchanging session key and security association for securing data to be sent through the IPSec tunnel. You can specify up to four Phase 1 proposals.</p>
<b>p2-proposal &lt;name&gt;</b>	<p>Adds or modifies the IKE Phase 2 proposal, which defines the parameters for creating and exchanging session key and security association for securing data to be sent through the IPSec tunnel. You can specify up to four Phase 2 proposals.</p>
<b>policy-checking</b>	<p>Checks if the access policies of the two VPN participants match before establishing a connection.</p> <p>With release ScreenOS 2.5 or higher, use policy checking 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.</p> <p>For backwards compatibility with ScreenOS 2.0 and earlier, you can disable policy checking when only one policy is configured between two peers.</p>
<b>respond-bad-spi</b>	<p>Respond to bad SP1 after a reboot.</p>
<b>single-ike-tunnel &lt;string&gt;</b>	<p>Single Phase 2 SA for several policies to the peer.</p>
<b>soft-lifetime-buffer &lt;number&gt;</b>	<p>Sends (L59) time to initiate IKE before lifetime (seconds).</p>

---

## Availability

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

## Defaults

Main mode is the default method for Phase 1 negotiations.

3DES and SHA-1 are the default algorithms for encryption and authentication.

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 only necessary if the data traffic is between two security gateways, one of which is a CheckPoint 4.0 device.)

The default for initiator- and responder-set-commit commands is **Unset**. The default soft-lifetime-buffer size is 10 seconds.

## Examples

To define a Phase 1 proposal named `pre-g1-3des-md5` with the following attributes:

- Preshared key and a group 1 Diffie-Hellman exchange
- Encapsulating Security Payload (ESP) protocol using the 3DES and MD5 algorithms
- Lifetime of 3 minutes:

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

By default, the `single-ike-tunnel` flag is not set.

By default, the commit bit is not set when initiating or responding to a Phase 2 proposal.

To define a Phase 2 proposal named `g2-esp-3des-null` with the following attributes:

- Group 2 Diffie-Hellman exchange
- ESP using 3DES without authentication
- Lifetime of 15 minutes:

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

---

To define a remote gateway named “san\_fran” with the following attributes:

- Main mode
- Preshared Key with the value bi273T1L
- Reference to the Phase 1 proposal pre-gl-3des-md5

```
ns-> set ike gateway san_fran main preshare bi273T1L proposal pre-gl-3des-md5
```

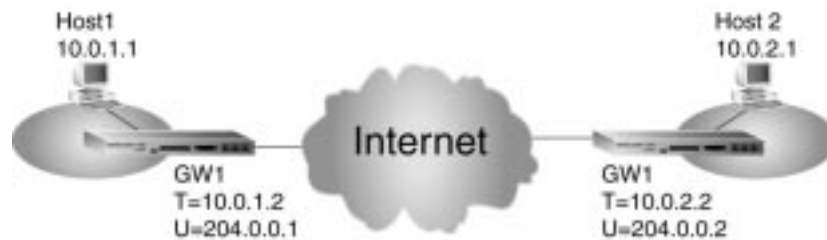
For an example of the complete procedure for setting up a VPN tunnel, see the Notes section below.

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 constitutes up to five steps. To set up one end of a VPN tunnel gateway 1 (GW1) in the illustration for bidirectional traffic, follow the steps below.



T = Trusted Port  
U = Untrusted Port

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 an outgoing incoming access policy:

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

```
ns-> set policy incoming host2 host1 any tunnel vpn vpn1
```

The procedure for setting up a VPN tunnel for a dialup user with IKE constitutes up to four steps.

1. Define the user as a IKE user. See the **set user** command on page 2-122.
2. Define the IKE Phase 1 proposal, Phase 2 proposal, and remote gateway. (Note: If you use the default proposals, you do not need to define a Phase 1 or Phase 2 proposal.)
3. Define the VPN tunnel as AutoKey IKE. See the **set vpn** command on page 2-131.
4. Define an incoming access policy, with **Dial-Up VPN** as the source address and the VPN tunnel you configured in step 3 specified. See the **set policy** command on page 2-92.

See Also

See the **get ike** and **clear ike-cookie** commands.

---

# interface

**Description:** Use the **set interface** command to define the interface settings for network and VPN traffic.

The syntax is divided into two sections to distinguish between settings for a physical interface (trust, untrust, dmz, tunnel) and a logical interface (trust/<number>, tunnel/<number>).

## Syntax

For NS-5 only:

```
set interface trust { bandwidth <number> | dip <number> | gateway  
<a.b.c.d> | ident-reset | ip <a.b.c.d> | manage { global | global-pro | ping  
| scs | snmp | ssl | telnet | web } | manage-ip <a.b.c.d> | mip <a.b.c.d> |  
phy { full | half } | route }
```

For NS-10 only:

```
set interface trust { bandwidth <number> | dip <number> | gateway  
<a.b.c.d> | ident-reset | ip <a.b.c.d> | manage { global | global-pro | ping  
| scs | snmp | ssl | telnet | web } | manage-ip <a.b.c.d> | mip <a.b.c.d> |  
phy { full | half } | vlan { trunk } }
```

For NS-100 only:

```
set interface trust { bandwidth <number> | dip <number> | gateway  
<a.b.c.d> | ident-reset | ip <a.b.c.d> | manage { global | global-pro | ping  
| scs | snmp | ssl | telnet | web } | manage-ip <a.b.c.d> | mip <a.b.c.d> |  
phy { auto { 100Mbps | 10Mbps } | full { 100Mbps | 10Mbps } | half {  
100Mbps | 10Mbps } } | route }
```

For NS-1000 only:

```
set interface trust { bandwidth <number> | dip <number> | gateway  
<a.b.c.d> | ident-reset | ip <a.b.c.d> | manage { global | global-pro | ping  
| scs | snmp | ssl | telnet | web } | manage-ip <a.b.c.d> | mip <a.b.c.d> |  
phy { auto { 100Mbps | 10Mbps } | full { 100Mbps | 10Mbps } | half {  
100Mbps | 10Mbps } | manual } | route }
```

---

For NS-5 only:

```
set interface untrust { bandwidth <number> | dip <number> | gateway  
<a.b.c.d> | ident-reset | ip <a.b.c.d> | manage { global | global-pro | ping  
| scs | snmp | ssl | telnet | web } | manage-ip <a.b.c.d> | mip <a.b.c.d> |  
phy { full | half } }
```

For NS-10 only:

```
set interface untrust { bandwidth <number> | dip <number> | gateway  
<a.b.c.d> | ident-reset | ip <a.b.c.d> | manage { global | global-pro | ping  
| scs | snmp | ssl | telnet | web } | manage-ip <a.b.c.d> | mip <a.b.c.d> |  
phy { full | half } | vlan { trunk } }
```

For NS-100 only:

```
set interface untrust { bandwidth <number> | dip <number> | gateway  
<a.b.c.d> | ident-reset | ip <a.b.c.d> | manage { global | global-pro | ping  
| scs | snmp | ssl | telnet | web } | manage-ip <a.b.c.d> | mip <a.b.c.d> |  
phy { auto { 100Mbps | 10Mbps } | full { 100Mbps | 10Mbps } | half {  
100Mbps | 10Mbps } } | route }
```

For NS-1000 only:

```
set interface untrust { bandwidth <number> | dip <number> | gateway  
<a.b.c.d> | ident-reset | ip <a.b.c.d> | manage { global | global-pro | ping  
| scs | snmp | ssl | telnet | web } | manage-ip <a.b.c.d> | mip <a.b.c.d> |  
phy { auto { 100Mbps | 10Mbps } | full { 100Mbps | 10Mbps } | half {  
100Mbps | 10Mbps } | manual } }
```

For NS-1000 only:

```
set interface mgt { gateway <a.b.c.d> | ip <a.b.c.d> | manage { global {  
global | global-pro | ping | scs | snmp | ssl | telnet | web } } | phy { auto  
{ 100mbps | 10mbps } | full { 100mbps | 10mbps } | half { 100mbps |  
10mbps } }
```

For NS-1000 only:

```
set interface ha { phy { auto { 100mbps | 10mbps } | full { 100mbps |  
10mbps } | half { 100mbps | 10mbps } }
```

For NS-10 only:

```
set interface DMZ { bandwidth <number> | dip <number> | gateway  
<a.b.c.d> | ident-reset | ip <a.b.c.d> | manage { global | global-pro | ping  
| scs | snmp | ssl | telnet | web } | manage-ip <a.b.c.d> | mip <a.b.c.d> |  
phy { full | half } }
```



---

For NS-100 only:

```
set interface DMZ { bandwidth <number> | dip <number> | gateway  
<a.b.c.d> | ident-reset | ip <a.b.c.d> | manage { global | global-pro | ping  
| scs | snmp | ssl | telnet | web } | manage-ip <a.b.c.d> | mip <a.b.c.d> |  
phy { auto { 100Mbps | 10Mbps } | full { 100Mbps | 10Mbps } | half {  
100Mbps | 10Mbps } }
```

For NS-100 only:

```
set interface tunnel/<number> { dip <number> | ip <a.b.c.d> | mip  
<a.b.c.d>}
```

For NS-5, -10, 1000 only:

```
set interface tunnel/<number> { ip <a.b.c.d> }
```

## Arguments

<b>trust</b>	The trusted interface.
<b>bandwidth &lt;number&gt;</b>	
	The guaranteed maximum bandwidth in kbps for all traffic crossing the interface.
<b>dip</b>	
	Creates a DIP set ( 4 to 255) from the IP pool.
<b>gateway &lt;a.b.c.d&gt;</b>	
	IP address for the router leading to addresses beyond the immediate subnet of the interface. A value of 0.0.0.0 indicates that only systems on the same subnet as the NetScreen device can manage it.
<b>ident-reset</b>	
	When enabled, the NetScreen device sends a TCP Reset announcement in response to an IDENT request to port 113.
<b>ip &lt;a.b.c.d&gt;</b>	
	The IP address <a.b.c.d> and subnet mask <A.B.C.D> for the interface.

---

**manage**

The interface manageability.

**global**

Enables the interface to allow NetScreen Global-Manager manageability.

**global-pro**

Enables the interface to allow NetScreen Global-Pro manageability.

**ping**

Enables the ability to ping the IP address of the NetScreen device through the specified interface.

**scs**

Enables the interface to allow the secure command shell (SCS) manageability.

**snmp**

NetScreen-5, -10, and -100. Enables the interface to allow Simple Network Management Protocol (SNMP) manageability.

**telnet**

Enables the interface to allow Telnet manageability.

**web**

Enables the interface to allow Web manageability.

**manage-ip <a.b.c.d>**

The IP address specified is used to manage the NetScreen device on a per interface basis.

**mip <a.b.c.d>**

Sets the public IP address to be mapped to an internal private IP address.

**nat**

The private address. **nat** is a keyword indicating that Network Address Translation (NAT) is performed on outgoing traffic from the trusted network.

---

	<b>route</b>	A keyword indicating that source address in the IP header packet is translated.
<b>untrust</b>		The untrusted interface.
<b>mgt</b>		The out-of-band Management interface (for the NetScreen-1000 only).
<b>ha</b>		The ha interface (for the NetScreen-1000 only).
<b>tunnel</b>		Creates a logical interface with an identifying number for a VPN or L2TP tunnel.
	<b>dip</b>	Specifies the dynamic IP configuration.
	<b>ip</b>	Specifies the interface IP address.
	<b>mip</b>	Specifies mapped IP configuration.
<b>DMZ</b>		The DMZ interface (where applicable).
	<b>phy</b>	Specifies the interface physical feature.
	<b>phy auto</b>	Enables the data flow autosensing feature. The NetScreen system automatically selects the duplex mode as <b>full</b> or <b>half</b> based on the connected device.
	<b>phy full</b>	Disables the network autosensing feature. Specifies the duplex as <b>full</b> .
	<b>phy half</b>	Disables the network autosensing feature. Specifies the duplex as <b>half</b> .
	<b>100mb   10mb</b>	For the NetScreen-100 only. Selects a speed for transmission—100mb or 10mb.

- 
- The slash number (/) in the **set interface tunnel** command is used to provide different names for multiple tunnel interfaces. The **unset interface tunnel ip** command not only deletes the particular tunnel interface, but also removes all MIP and DIP configurations on it.

### Availability

This feature is supported on all NetScreen device models.

### Defaults

You can ping both the trusted Mgt and DMZ interfaces.

Interface IP addresses, manage-IP addresses, netmasks, and gateways are 0.0.0.0.

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

Ident reset is disabled.

A trusted interface or subinterface is configured for NAT mode.

### Examples

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 manage web
```

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

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

To configure the untrusted interface to 100Mb/sec with full duplex:

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

To enable the ability to reset the ident requests on the trusted interface:

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

To create a sub-interface (SIF) and associate it with a particular VLAN, issue the **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> tag <number>
```

**Note**

*For more information on virtual systems, see set virtual system on 2-113.*

To create or modify a tunnel interface named **tunnel/1** with the IP address 172.10.10.5/24:

```
ns1000-> set interface tunnel/1 ip 172.10.10.5 255.255.255.0
```

To define a DIP pool of five port-translatable addresses (4.4.4.1 - 4.4.4.5) for a tunnel interface named tunnel/2:

```
ns1000-> set interface tunnel/2 4.4.4.1 4.4.4.5
```

To set up a DIP set of 10 DIPs with no port translation on a tunnel interface named tunnel/8:

```
ns-> set interface tunnel/2 dip <dip number> 4.4.4.1 4.4.4.5
```

---

To set an IP address for the Management (Mgt) port through which to manage a NetScreen-1000 device:

```
ns1000-> set interface mgt 172.16.40.1 255.255.255.0
```

To unset the tunnel interface named **tunnel/1**:

```
ns-> unset interface tunnel/1
```

See Also

See the **get interface** and **set vsys** 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.)

When the NetScreen-5 is acting as a DHCP client and you want to change the address of the untrusted interface to a static IP address, first issue the **unset interface DHCP** command. If you do not issue the **unset interface dhcp** command first, the DHCP-assigned IP address cannot be changed to a static IP address. The specific sequence required is:

1. `unset interface untrust dhcp`
2. `set interface untrust ip <a.b.c.d> <A.B.C.D>`

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

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

Both the Manage IP and interface IP address will respond to ICMP messages (ping) to allow network administrators to debug the network by pinging each as needed.

**Important:** Remember to remove all routing entries that use the deleted interface from the routing table.

---

**Important:** A valid DIP pool must not include the IP address of the interface for which the DIP pool is associated. It must also not include any MIPs set for that interface.

```
set interface { trust | untrust | DMZ | tunnel/1
```

#### Physical Interface

```
set interface { trust | untrust |DMZ } { bandwidth <number> | dip
<id_number> <a.b.c.d> [ fix_port | <e.f.g.h> [ fix_port ]] | gateway
<a.b.c.d> | ident_request | ip <a.b.c.d> <A.B.C.D> | manage [ global |
global-pro | ping | scs | snmp | ssl | telnet | web ] | manage-ip
<a.b.c.d> | mip <a.b.c.d> host <e.f.g.h > [ netmask <A.B.C.D> [modify
<a.b.c.d> netmask <A.B.C.D> ]] | phy { auto | full | half > 100mb |
10mb }
```

```
set interface trust { nat | route }
```

```
set interface untrust dhcp
```

#### Logical Interface

```
set interface tunnel/<number> { dip <id_number> <a.b.c.d> [fix_port |
<e.f.g.h> [ fix_port ]] | ip <a.b.c.d> <A.B.C.D> | mip <a.b.c.d> host
<e.f.g.h> [ netmask <A.B.C.D> [modify <a.b.c.d> netmask <A.B.C.D> ]] }
```

#### See Also

See the **get interface** command.

---

# ippool

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

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

## Syntax

**set ippool <string>**

## Arguments

**<string>** Specifies the name of the IP pool.

## Availability

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

## Defaults

None.

## Examples

To configure the 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 **get ippool** command.



---

# l2tp

**Description:** Use the **set l2tp** command to set the L2TP configuration.

Syntax

**set l2tp** <string>

**set l2tp default** { **auth** { **local** | **radius** } | **dns1** <a.b.c.d> | **dns2** <a.b.c.d> | **ippool** <string> | **ppp-auth** { **any chap** [ **pap** ] | **pap** } | **radius-port** <number> | **radius-secret** <string> | **server-name** <string> | **wins1** <a.b.c.d> | **wins2** <a.b.c.d> }

Arguments

<b>&lt;string&gt;</b>	Specifies the tunnel name.
<b>default auth</b> { <b>local</b>   <b>radius</b> }	Specifies the auth database location.
<b>default dns1</b> <a.b.c.d>	Specifies the DNS primary server IP.
<b>default dns2</b> <a.b.c.d>	Specifies DNS secondary server IP.
<b>default ippool</b> <string>	Specifies the IP pool.
<b>default ppp-auth</b> { <b>any</b>   <b>chap</b>   <b>pap</b> }	Specifies the PPP auth type.
<b>default radius-secret</b> <string>	Specifies the Radius Server port.
<b>default server-name</b> <string>	Specifies Radius secret server.
<b>default wins1</b> <a.b.c.d>	Specifies the WINS primary server IP.
<b>default wins2</b> <a.b.c.d>	Specifies the WINS secondary server IP.

Availability

This feature is supported on the NetScreen-5, -10, -100. This feature is not supported on the NetScreen-1000.

Defaults

-

Examples

To \_ :

```
ns-> set l2tp
```

---

See Also

See the **get l2tp** and **clear l2tp** commands.

---

## mac

**Description:** Use the **set mac** command to configure static MAC entry.

### Syntax

**set mac** <xxxxyyyyzzzz>

### Arguments

<xxxxyyyyzzzz>                      Specifies the MAC address.

### Availability

This feature is supported on all NetScreen device models.

### Defaults

—

### Examples

To \_ :

```
ns-> set mac
```

### See Also

See the **get mac**, **clear mac**, and **get mac-count** commands.

---

# mip

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

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.

**Important:** *The MIP must be on the same subnet as its associated interface IP address. When creating a new MIP, check for overlapping with other MIPs or DIPs. Check Virtual IPs (VIP) as well.*

## Syntax

**set mip <a.b.c.d>**

## Arguments

<b>&lt;a.b.c.d&gt;</b>	Maps the untrusted IP address <a.b.c.d> to the actual IP address <e.f.g.h> of the device to receive the mapped traffic.
------------------------	---

## 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 define a subnet-to-subnet Mapped IP configuration for a subnet with IP address starting from 209.125.15.1 to an actual subnet with IP addresses starting from 10.1.1.1 using a netmask of 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.

---

## 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.

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

### Syntax

**set ntp interval <number>**

**set ntp server <a.b.c.d>**

### Arguments

<b>interval &lt;number&gt;</b>	Defines in minutes how often the NetScreen device updates its clock time by synchronizing with the NTP server.
<b>server &lt;a.b.c.d&gt;</b>	Defines the NTP server with which the NetScreen device synchronizes time. Replace a.b.c.d with the IP address of the NTP server.

### 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

This is a list of system 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 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.

---

# 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 { crl-url <string> }
```

## Arguments

<b>crl-url &lt;string&gt;</b>	Sets the default LDAP URL for the CA certificate revocation list (CRL) to be used for X.509 CRL retrieval purposes.
-------------------------------	---

## 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 server-name 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 outgoing** <string>

**set policy incoming** <string>

**set policy fromdmz** <string>

**set policy todmz** <string>

**set policy before** <number>

**set policy default-permit-all**

**set policy id** <number>

**set policy move** <number>

**set policy name** <string>

---

## Arguments

<b>outgoing</b>	Defines the traffic going out through the trusted port.
<b>incoming</b>	Defines the traffic coming in through the untrusted port.
<b>fromdmz</b>	Defines the traffic going out through the DMZ port.
<b>todmz</b>	Defines the traffic coming in through the DMZ port.
<b>before &lt;number&gt;</b>	Inserts a policy.
<b>default-permit-all</b>	Allows access if there are no policy matches.
<b>id &lt;number&gt;</b>	Specifies the specify policy ID.
<b>move &lt;number&gt;</b>	Repositions an access policy before or after a specified access policy in the list.
<b>policy name &lt;string&gt;</b>	Up to six possible policy sets may be generated. These sets are combinations of the four available policy directions ( <b>outgoing</b> , <b>incoming</b> , <b>fromdmz</b> , or <b>todmz</b> ), and the address books for the trusted, untrusted, and DMZ interfaces. Choose the number of the policy set you wish to use.

## Availability

The **set policy** 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
```

To define the DIP without a fixed port for NAT on the trusted interface:

```
ns-> set policy outgoing 10.1.1.9 10.150.42.41 any nat dip-id 7
```

To define the DIP with a fixed port on the trusted interface:

```
ns-> set policy outgoing 10.1.1.9 10.150.42.41 any nat dip-id 7 fix
```

---

See Also

See the **get policy** command.

---

## pppoe

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

### Syntax

```
set pppoe ac <string>  
set pppoe authentication { CHAP | PAP | any }  
set pppoe idle-interval <number>  
set pppoe interface [ <string> ]  
set pppoe service <string>  
set pppoe static-ip  
set pppoe username <string>
```

### Arguments

<b>ac</b> <string>	Allows the interface to connect only to the specified AC.
<b>authentication</b> { CHAP   PAP   any }	Sets the authentication methods to CHAP, or PAP, or both.
<b>idle-interval</b> [ <string> ]	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 with never been taken down for lack of activity.
<b>interface</b> <string>	Specifies the interface for PPPoE encapsulation.
<b>service</b> <string>	Allows the interface to connect only to the specified service.
<b>static-ip</b>	Specifies that your connection uses the IP addresses assigned by the AC.
<b>username</b> <string>	Sets the user name and password.

### 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**, **clear pppoe**, and **exec 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.

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.

**Important:** *Make sure the default gateway is established for a tunnel interface before setting its route.*

If there are multiple route entries for the same target address in the route table, the NetScreen device uses the one with the lowest metric value. Note that the N-5 device does not fail over automatically to the other route table entries, if the route with the lowest metric value does not work.

## Syntax

**set route <a.b.c.d>**

## Arguments

**<a.b.c.d>** The IP address of the router that forwards all traffic to the specified target address.

## 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 172.16.15.0/24 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 define a route for a tunnel interface named tunnel/1 to the target IP address 172.10.10.1/24:

```
ns-> set route 172.10.10.1 255.255.255.0 interface tunnel/1
```

To delete a static route entry for network 244.1.2.0/24:

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

See Also

See the **get route** command.



---

# 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>

## Arguments

<string> Defines a name for the schedule.

## 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 configure a NetScreen device from a remote system.

### Syntax

**set scs enable**

**set scs key\_gen\_time <number>**

### Arguments

<b>enable</b>	Enables the secure shell feature.
<b>key_gen_time &lt;number&gt;</b>	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.

The maximum timeout value for TCP connections is 40 minutes.

The maximum timeout value for UDP connections is 40 minutes.

## Syntax

**set service** <string>

## Arguments

<string> Defines a name for the service.

## 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 0-65535 dst 10115-10115
```

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

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

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

To unset a service named **test**:

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

See Also

See the **get service** command.

---

## snmp

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



**Note**

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

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

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

Syntax

**set snmp auth-trap { enable }**

**set snmp community <string>**

**set snmp contact <string>**

**set snmp host <string>**

**set snmp location <string>**

**set snmp name <string>**

**set snmp vpn**

---

## Arguments

<b>auth-trap { enable }</b>	Enables Simple Network Management Protocol (SNMP) authentication traps.
<b>community &lt;string&gt;</b>	Defines the name for the SNMP community.
<b>contact &lt;string&gt;</b>	Defines the system contact.
<b>host &lt;string&gt;</b>	Defines the IP address of the SNMP host.
<b>location &lt;string&gt;</b>	Defines the location of the system.
<b>name &lt;string&gt;</b>	Defines the name of the system.
<b>vpn</b>	

## 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 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 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
```

## See Also

See the **get snmp** command.

---

## ssl

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

### Syntax

**set ssl cert <number>**

**set ssl enable**

**set ssl encrypt { 3des | sha-1 | des | sha-1 | rc4 | md5 | rc4-40 | md5 }**

**set ssl port <number>**

### Arguments

<b>cert &lt;name&gt;</b>	Specifies that the named certificate is required.
<b>enable</b>	Turns on SSL.
<b>encrypt</b>	Enables encryption over the SSL connection.
<b>port</b>	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 VPN**  
**set syslog config <string>**  
**set syslog enable**  
**set syslog port <number>**  
**set syslog traffic**

## Arguments

<b>VPN</b>	Enables syslog VPN encryption.
<b>config &lt;string&gt;</b>	Defines the configuration settings for the Syslog.
<b>enable</b>	Enables the NetScreen device to send messages to the Syslog host.
<b>port &lt;number&gt;</b>	Defines the port number on the Syslog host that receives the User Datagram Protocol (UDP) packets from the NetScreen device.
<b>traffic</b>	Enables the NetScreen device to send traffic logs to the Syslog host.

## 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
```



**Note**

*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
```



**Note**

*You must configure the Websense host IP address before you enable the Websense feature.*

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 functionality at a specified time.

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

### Syntax

**set timer** <mm/dd/yyyy>

### Arguments

<mm/dd/yyyy> Specifies the date when the NetScreen device executes the defined action.

### 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
```

---

# traffic-shaping

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

## Syntax

**traffic-shaping ip\_precedence <number>**

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

## Arguments

- |                                     |  |
|-------------------------------------|--|
| <b>ip_precedence &lt;number&gt;</b> | Specifies the priority for IP precedence (TOS) mapping.  |
| <b>mode { auto   off   on }</b>     | 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 auto mode 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 up to automatic mode.

## Examples

To turn on the traffic shaping function:

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

## See Also

See the **get traffic-shaping** command.

---

# url

**Description:** Use the **set url** command to enable URL filtering. URL filtering is provided by a Websense server.

## Syntax

```
set url config { disable | enable }  
set url fail-mode { block | permit }  
set url message <string>  
set url msg-type <number>  
set url server <string>
```

## Arguments

<b>config { disable   enable }</b>	Enables or disables URL filtering by the Websense server.
<b>fail-mode { block   permit }</b>	If connection to the Websense server is lost, this either blocks or permits all HTTP requests.
<b>message &lt;string&gt;</b>	Defines a custom message (up to 220 characters in length) to send to the client who is blocked from reaching a URL.
<b>msg-type &lt;number&gt;</b>	A 0 uses the message sent by the Websense server. A 1 uses the user-defined message from the NetScreen device.
<b>server &lt;string&gt;</b>	Defines communication with a Websense server with a domain name (www.abc.com) or IP address <a.b.c.d>, using port number <port_number> with a timeout value <timeout_value> in seconds. The timeout value specifies how long the NetScreen device waits for a response from the Websense filter before it either blocks or permits traffic to the URL.

## Availability

This feature is supported on all NetScreen device models except the NS-1000 which does not support URL filtering.

---

## Defaults

The default port number for a Websense server is 15868. The default fail-mode behavior is to block all HTTP requests. The Websense server is the default source of a message indicating that user access to a URL is blocked.

---

## 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 NetScreen device:

```
ns-> set url msg-type 1
```

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** and **get url-filter** commands.

---

## user

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

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.

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

### Syntax

**set user <string>**

### Arguments

<b>&lt;string&gt;</b>	Adds a user name <user_name> and password <password> to the database.
-----------------------	---

### 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 **ipsecmmaryj**, and with a local-spi defined as 3456 and 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 **jane**:

```
ns-> unset user jane
```

## See Also

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



---

## vip

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

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

	<b>VIPs</b>	<b>Services/VIP</b>	<b>Servers/VIP</b>
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

### Syntax

**set vip** <a.b.c.d>

**set vip untrust-ip** [ <number> | + [ <number> ] ]

### Arguments

<a.b.c.d>	Specifies the IP Address.
<b>untrust-ip</b> [ <number>   + [ <number> ] ]	Specifies the untrusted interface IP.
<number>	Specifies the port number for the service.
+	
<number>	Appends the service to virtual IP.

### 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 of 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.

---

## vpn

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

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 <name> trust gateway** command, the error message **AutoKey VPN is not supported on trust interface** appears.

### Syntax

**set vpn <string>**

### Arguments

**<string>** Defines a name for the VPN.

### Availability

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

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

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

A VPN tunnel terminates at the untrusted interface (NAT and Route mode) and the system IP address (Transparent mode). To create a Manual Key tunnel to an NetScreen device from the trusted side, use the **trust** argument.

### Defaults

The key lifetime is set to 3600 seconds.

The ESP authentication algorithm is NULL when not specified otherwise.

---

## 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, and 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 **funafuti**, 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**, **set vpnmonitor**, and **set ike** commands. The **set ike** command section contains the complete steps for setting up a VPN tunnel.

---

# vpnmonitor

**Description:** Use the **set vpnmonitor** command to set the monitor frequency.

## Syntax

**set vpnmonitor frequency <number>**

## Arguments

**frequency <number>** Specifies the monitor frequency in intervals (10 seconds).

## Availability

This feature is supported on the NetScreen-5, -10, -100. This feature is not supported on the NetScreen-1000.

## Defaults

-

## Examples

To \_ :

```
ns-> set vpnmonitor
```

## See Also

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

---

## VSYS

**Description:** Use the **set vsys** command to create virtual systems from the root level of 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 settings and management.

To access an existing virtual system, issue the **enter vsys** command. Use the **unset vsys** command to remove a specific virtual system and all its associated settings.

 **Note**

*Note: The number of virtual systems depends on the quantity obtained via the virtual system software\_key feature:*

*example: 25 virtual system user software\_key only allows you to configure up to 25 virtual systems.*

 **Note**

*Note: The default has 0 virtual system user*

### Syntax

**set vsys <string>**

### Arguments

**<string>**

Defines the name of a virtual system and automatically places the root level admin within the virtual system so that subsequent commands configure the newly created virtual system.

### Availability

This feature is available only on NetScreen-1000 devices.

### Examples

To create a virtual system named **3**:

```
ns1000-> set vsys organization3
```

### See Also

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

---

# vsys-traffic

**Description:** Use the **set vsys-traffic** command to set the virtual system traffic properties.

## Syntax

**set vsys-traffic { loop { all } }**

## Arguments

<b>loop</b>	Specifies the loop-back traffic.
<b>all</b>	Specifies the loop-back traffic for all virtual systems.

## Availability

This feature is supported on only the NetScreen-1000.

## Defaults

—

## Examples

To \_ :

```
ns-> set vsys-traffic
```

## See Also

See the **get vsys-traffic** command.

---

# webtrends

**Description:** Use the **set vsys-traffic** command to configure WebTrends.

Syntax

**set webtrends VPN**

**set webtrends enable**

**set webtrends host-name <string>**

**set webtrends port <number>**

Arguments

<b>VPN</b>	Enables WebTrends VPN encryption.
<b>enable</b>	Enables WebTrends.
<b>host-name &lt;string&gt;</b>	Specifies the WebTrends host name.
<b>port &lt;number&gt;</b>	Specifies the WebTrends host port.

Availability

This feature is supported on the NetScreen-5, -10, -100. This feature is not supported on the NetScreen-1000.

Defaults

—

Examples

To \_ :

```
ns-> set vsys-traffic
```

See Also

See the **get vsys-traffic** command.



---

# Get Commands

# 3

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

The **Clear** commands include the following:

- **address** (page 3-4)
- **admin** (page 3-5)
- **alarm** (page 3-8)
- **arp** (page 3-13)
- **auth** (page 3-14)
- **chassis** (page 3-17)
- **clock** (page 3-18)
- **config** (page 3-19)
- **console** (page 3-21)
- **counter** (page 3-22)
- **dhcp** (page 3-27)
- **dialup-group** (page 3-28)
- **dip** (page 3-29)
- **dns** (page 3-30)
- **domain** (page 3-31)
- **envar** (page 3-32)
- **file** (page 3-33)
- **firewall** (page 3-35)
- **gate** (page 3-36)
- **global** (page 3-37)
- **global-pro** (page 3-38)
- **glog** (page 3-39)
- **group** (page 3-40)
- **ha** (page 3-42)
- **hostname** (page 3-43)
- **ike** (page 3-44)
- **interface** (page 3-47)

- 
- **ippool** (page 3-50)
  - **l2tp** (page 3-51)
  - **lance** (page 3-52)
  - **log** (page 3-53)
  - **mac-count** (page 3-58)
  - **mac-learn** (page 3-59)
  - **master** (page 3-60)
  - **memory** (page 3-61)
  - **mpsess** (page 3-62)
  - **mip** (page 3-63)
  - **nsp-tunnel** (page 3-64)
  - **ntp** (page 3-65)
  - **os** (page 3-66)
  - **pki** (page 3-67)
  - **policy** (page 3-69)
  - **pport** (page 3-71)
  - **route** (page 3-72)
  - **sa** (page 3-74)
  - **scheduler** (page 3-77)
  - **scs** (page 3-78)
  - **service** (page 3-79)
  - **session** (page 3-81)
  - **snmp** (page 3-83)
  - **socket** (page 3-85)
  - **software-key** (page 3-86)
  - **ssl** (page 3-87)
  - **syslog** (page 3-88)
  - **system** (page 3-90)
  - **tech-support** (page 3-91)
  - **timer** (page 3-92)
  - **traffic-shaping interface** (page 3-93)
  - **url** (page 3-94)
  - **user** (page 3-95)

- 
- **vip** (page 3-97)
  - **vpn** (page 3-98)
  - **vpnmonitor** (page 3-100)
  - **vsys** (page 3-101)
  - **webtrends** (page 3-102)

If you wish 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**

---

# address

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

## Syntax

```
get address [ trust [ group [ <string> ] ] | untrust [ group [ <string> ] ] | DMZ [ group [ <string> ] ] ]
```

## Arguments

<b>trust   untrust   DMZ</b>	Displays the addresses for the trusted, untrusted, or DMZ (NS-10 and -100) interface. If you do not specify an interface, all individual addresses and address groups are displayed.
<b>group [ &lt;string&gt; ]</b>	Displays the address groups for each respective interface.

## Availability

This feature is supported on all NetScreen device models.

## Examples

To display all address book entries:

```
ns-> get address
```

To display only address book entries for the DMZ interface:

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

To display a list of the trusted address groups:

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

## See Also

See the **set address** command.

---

# admin

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

The display for each address book entry shows the name, IP address, and netmask, or domain name, flag, and comments for the entry.

## Syntax

```
get admin [ auth [ > { tftp <a.b.c.d> } | settings [ > { tftp <a.b.c.d> } ] ] ] |  
current-user [ > { tftp <a.b.c.d> } ] | manager-ip [ > { tftp <a.b.c.d> } ] |  
user [ > { tftp <a.b.c.d> } | cache [ > { tftp <a.b.c.d> } ] | login [ > { tftp  
<a.b.c.d> } ] ] ]
```

For the NetScreen-1000 only:

```
get admin [ auth [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } |  
settings [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ] ] ] |  
current-user [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ] |  
manager-ip [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ] |  
user [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } | cache [ # {  
slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ] | login [ # { slot  
<number> | vsys <string> } | > { tftp <a.b.c.d> } ] ] ]
```

---

## Arguments

<b>auth [ settings ]</b>	Displays the authentication settings for administrators (compare this command with the <b>get auth</b> command which displays the authentication settings for users. You can use the internal database or a RADIUS server for admin authentication. For users, you can use the internal database, a RADIUS server or an LDAP server).
<b>current-user</b>	Lists only the name of the current user of the device; that is, the one entering the command.
<b>manager-ip</b>	Displays the IP address and netmask of the management workstation.
<b>user</b>	Lists the names of the different administrators of the device.

## 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:

- The system IP address and port number for Web management
- The e-mail alert status
- The e-mail server IP address or domain name
- The remote e-mail address or addresses for the recipients of e-mail alerts

- 
- The status for including the traffic logs with system sent logs when sending through e-mail notification
  - The configuration format—DOS or UNIX



---

# alarm

**Description:** Use the **get alarm** command to display alarm entries.

## Syntax

```
get alarm { event [ > { tftp <a.b.c.d> } | begin <string> | end-time <string> | exclude <string> | include <string> | start-time <string> ] | threshold [ > { tftp <a.b.c.d> } ] | traffic [ > { tftp <a.b.c.d> } | detail [ > { tftp <a.b.c.d> } | end-time <string> | minute { > { tftp <a.b.c.d> } | rate { <number low-high> | <number> } | threshold { <number low-high> | <number> } } | second { > { tftp <a.b.c.d> } | rate { <number low-high> | <number> } } | threshold { <number low-high> | <number> } } | start-time <string> ] | dst-address <string> | policy { <number low-high> | <number> } | service <string> | src-address <string> ] ]
```

For the NetScreen-1000 only:

```
get alarm { event [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } | begin <string> | end-time <string> | exclude <string> | include <string> | start-time <string> ] | threshold [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ] | traffic [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } | detail [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } | end-time <string> | minute { # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } | rate { <number low-high> | <number> } | threshold { <number low-high> | <number> } } | second { # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } | rate { <number low-high> | <number> } | threshold { <number low-high> | <number> } } | start-time <string> ] | dst-address <string> | policy { <number low-high> | <number> } | service <string> | src-address <string> ] ]
```

## Arguments

**event** Specifies event alarm entries.

---

<b>start-time</b> <dd/mm[/yy   yyyy] [hh[:mm[:ss]]]>	<p>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 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:</p> <ul style="list-style-type: none"> <li>• <b>12/31/2001 23:59:00</b></li> <li>• <b>12/31/2001-23:59:00</b></li> <li>• <b>12/31/2001_23:59:00</b></li> </ul>
<b>end-time</b> <dd/mm[/yy   yyyy] [hh[:mm[:ss]]]>	Displays event alarm entries that occurred at and before the time specified.
<b>include</b> <include_string>	Displays event alarm entries that include the detail specified.
<b>exclude</b> <exclude_string>	Displays event alarm entries that exclude the detail specified.
<b>begin</b> <begin_string>	Displays event alarm entries that follow a specified alarm event.
<b>traffic</b>	Specifies traffic alarm entries.
<b>policy</b> <policy_id>   <policy_id_range>	<p>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:</p> <p>&lt;policy_id&gt;-&lt;policy_id&gt;</p>
<b>service</b> <service_name>	<p>Displays traffic alarm entries for a specified service, such as TCP, ICMP, or FTP. (Type <b>Any</b> to display all services.) The name does not have to be complete; for example, both <b>TC</b> and <b>CP</b> are recognized as <b>TCP</b>. Although you cannot specify a service group, note that because <b>TP</b> is recognized as <b>FTP</b>, <b>HTTP</b>, and <b>TFTP</b>, entering <b>TP</b> displays traffic alarm entries for all three of these Services.</p>

---

<b>src</b> <address_string>	Displays traffic alarm entries originating from a specified IP address or from a specified direction, such as <b>Inside_Any</b> or <b>Outside_Any</b> .
<b>dst</b> <address_string>	Displays traffic alarm entries destined for a specified IP address or for a specified direction, such as <b>inside_any</b> or <b>outside_any</b> .
<b>detail</b>	Displays detailed information for each access policy, including all the traffic alarm entries that occurred under it. If this 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.
<b>start time</b> <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.
<b>end-time</b> <dd/mm[/yy   yyyy] [hh[:mm[:ss]]]>	Displays traffic alarm entries that occurred at and before the time specified—day/month-hour:minute.
<b>second</b>   <b>minute</b>	Displays traffic alarm entries for access policies with threshold settings at bytes/second or bytes/minute.
<b>threshold</b> <value>   <range>	Displays traffic alarm entries for access policies with threshold settings at a specified value or within a specified range.
<b>rate</b> <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 the following 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
```

## Note

*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 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.

The **get arp** command displays all the ARP entries in the 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 contains a maximum of 256 entries.

## 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.

---

# auth

**Description:** Use the **get auth** command to display the user authentication configuration settings.

## Syntax

```
get auth [ > { tftp <a.b.c.d> } | history [ > { tftp <a.b.c.d> } ] | queue [ > { tftp <a.b.c.d> } ] | settings [ > { tftp <a.b.c.d> } ] | table [ > { tftp <a.b.c.d> } ] ]
```

For the NetScreen-1000 only:

```
get auth [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ] | > | history [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ] | queue [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ] | settings [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ] | table [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ] ]
```

## 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 used:

NetScreen internal database:

RADIUS server: the timeout value for the authenticated entry, the IP address for the RADIUS server, and the shared secret.

SecurID server: these values:

- The authentication type (SecurID)
- The authentication port number
- The SecurID Master server IP address or domain name, and that of the SecurID Slave, if used
- If duress can be used
- The type of encryption (DES or SPI)
- The maximum number of user authentication retries
- The authentication attempt timeout value
- The length of idle time before a user session times out and is closed.

**table**

Displays a table of the source IP addresses of authentication requests the authentication user's name how much time each entry has before being deleted, and whether an authentication attempt has been 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. When the entry reaches the 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 for authentication are rejected and must be retried.

---

# chassis

**Description:** Use the **get chassis** command to display the status of Processing board slot occupation and activity, power supply, fan, and temperature (in Celsius and Fahrenheit).

## Syntax

**get chassis [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ]**

## Arguments

None.

## Availability

This feature is only supported 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.

If you have a NetScreen-1000, use this command to copy the configuration settings from the root system or 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 only:

```
get config [ saved ] [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ] | [ slot1 <file_name> | # {slot <slot_number> | vsys <virtual-system_name>} | > tftp <a.b.c.d> <file_name> ] | [ slot2 <file_name> | #{slot <slot_number> | vsys <virtual-system_name>} | >tftp <a.b.c.d> <file_name>]
```

## Arguments

<b>saved</b>	Displays the configuration file saved in flash memory.
<b># slot &lt;slot_number&gt;   vsys &lt;virtual-system_name&gt;</b>	For the NetScreen-1000. Selects output from the PCMCIA card in slot 1 or 2, or from the virtual system <virtual-system_name>.
<b>&gt; tftp &lt;a.b.c.d&gt; &lt;file_name&gt;</b>	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>.
<b>slot1 &lt;file_name&gt;</b>	For the NetScreen-1000. Specifies the configuration file <file_name> in slot 1.
<b>slot2 &lt;file_name&gt;</b>	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 that has been saved in the flash memory:

```
ns-> get config saved
```

To download a configuration file named `new_cfg` 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_cfg # slot 1
```

To download a configuration file named `ns_cfg` from a TFTP server at 156.24.54.9 to a virtual system named `cyborg`:

```
ns1000-> get config tftp 156.24.54.9 ns_cfg # vsys cyborg
```

To copy a configuration file named `cfg5` from the PCMCIA card in slot 1 to a file named `ns_cfg5` in a TFTP server at 125.34.156.9:

```
ns1000-> get config slot1 cfg5 >tftp 125.34.156.9 ns_cfg5
```

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 the 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 [ interface { trust | untrust | DMZ } ] } | { hw [ interface { trust | untrust | DMZ } ] } | { policy <number> } | { statistics [ interface { trust | untrust | DMZ } ] }
```

For the NetScreen-1000 only:

```
get counter  
{ flow [ interface { trust | untrust | DMZ } | # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ] } | { hw [ interface { trust | untrust | } | # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ] } | { policy <number> } | { statistics [ interface { trust | untrust | } | # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ] }
```

---

## Arguments

<b>flow</b>	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.
<b>hw</b>	For the NetScreen-1000 only. Specifies the slot number of a Processing board.
<b>interface</b>	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.
<b>policy &lt;number&gt;</b>	Identifies the physical or sub interface. Identifies a particular access policy, allowing the administrator to monitor the amount of traffic it permits.
<b>statistics</b>	
<b>day   minute   month   second</b>	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 only possible on the NetScreen-1000

## Notes

This command is used only for technical support.

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 because of 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 because of 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 of unavailable Dynamic IP (DIP) addresses
  - no map – the number of packets dropped because there was no map to the trusted side
  - url block – the number of HTTP requests that were blocked
  - tcp proxy – the number of packets dropped from 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 because of 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 with 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

**Description:** Use the **get dhcp** command to .

## Syntax

```
get dhcp { relay | server { > { tftp <a.b.c.d> } | ip { > { tftp <a.b.c.d> } |  
allocate | idle } | option [ > { tftp <a.b.c.d> } ] }
```

## Arguments

None.

## Availability

This feature is available on the NetScreen-5 at version 1.65 or later, and on the NetScreen-10 at version 2.0 or later. This feature is not supported on the NetScreen-1000.

## 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.

---

# dialup-group

**Description:** Use the **get dialup-group** command to display dialup group configuration parameters.

## Syntax

```
get dialup-group { all [ > { tftp <a.b.c.d> } ] | id <number> }
```

For the NetScreen-1000 only:

```
get dialup-group { all [ # { slot <number> | vsys <string> } ] | > { tftp <a.b.c.d> } ] | id <number> }
```

## Arguments

- |                    |   |
|--------------------|---|
| <b>all</b>         | Displays the dialup group ID, name, and the total number of members for all the configured dialup groups.   |
| <b>id</b> <number> | Displays detailed information for a specific dialup group with ID <number>. The information includes the names of the members in the group, their status (enabled or disabled), and their SPI values for Manual Key dialup users, or the IKE. ID-type and for the IKE dialup users. |

## Availability

This feature is available on all NetScreen models that support VPNs.

## Examples

To display all the dialup-group configurations:

```
ns-> get dialup-group all
```

To display the configuration settings for the dialup-group with ID number 4:

```
ns-> get dialup-group id 4
```

## See Also

See the **set dialup-group** and **set user** commands.

---

# dip

**Description:** Use the **get dip** command to display the dynamic IP (DIP) configuration for the NetScreen device.

## Syntax

**get dip [ > { tftp <a.b.c.d> } ]**

For the NetScreen-1000 only:

**get dip [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ]**

## Arguments

<b>id &lt;number&gt;</b>	Displays the dynamic IP (DIP) settings for the DIP with the specified ID number <number>. If you do not specify an ID number, the <b>get dip</b> command displays all the DIP settings.
--------------------------	---

## Availability

This feature is supported on all NetScreen device models.

## Examples

To display all DIP configurations:

```
ns-> get dip
```

## See Also

See the **set dip** command.

---

# dns

**Description:** Use the **get dns** command to .

## Syntax

```
get dns { forward [ > { tftp <a.b.c.d> } ] | host { cache [ > { tftp <a.b.c.d> } ] | report [ > { tftp <a.b.c.d> } ] | settings [ > { tftp <a.b.c.d> } ] } | name <string> }
```

For the NetScreen-1000 only:

```
get dns { forward [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ] | host { cache [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ] | report [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ] | settings [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ] } | name <string> }
```

## Arguments

None.

## Availability

This feature is available on all NetScreen device models.

## Example

To get the dns of the NetScreen-1000:

```
ns1000-> get dns
```

## See Also

See the **set dns** command.

---

## domain

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

### Syntax

**get domain [ > { tftp <a.b.c.d> } ]**

For the NetScreen-1000 only:

**get domain [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ]**

### 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** [ > { **tftp** <a.b.c.d> } ]

For the NetScreen-1000 only:

**get envar** [ # { **slot** <number> | **vsys** <string> } | > { **tftp** <a.b.c.d> } ]

### 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 [ > { tftp <a.b.c.d> } | <string> | info [ > { tftp <a.b.c.d> } ]
```

For the NetScreen-1000 only:

```
get file [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ]
```

## Arguments

<b>file name</b>	Defines the file name stored in the flash card memory.
<b>device</b>	Defines the PCMCIA slot number in the NetScreen-1000: <b>slot1</b> for the card in slot 1 or <b>slot2</b> 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 note which settings are enabled or not.

## Syntax

**get firewall [ > { tftp <a.b.c.d> } ]**

For the NetScreen-1000 only:

**get firewall [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ]**

## 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 output from the **get firewall** command lists the elements comprising the set firewall command and notes if each one is enabled.

---

# gate

**Description:** Use the **get gate** command to .

Syntax

**get gate [ > { tftp <a.b.c.d> } ]**

For the NetScreen-1000 only:

**get gate [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ]**

Availability

This feature is supported on all NetScreen device models.

Examples

To display the firewall protection settings:

```
ns-> get gate
```

See Also

See the **set gate** command.

---

# global

**Description:** Use the `get global` command to display the NetScreen-Global Manager settings.

Syntax

**get global** [ > { **tftp** <a.b.c.d> } ]

For the NetScreen-1000 only:

**get global** [ # { **slot** <number> | **vsys** <string> } | > { **tftp** <a.b.c.d> } ]

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:

- Whether the NetScreen-Global Manager feature is enabled or not
- 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
- Whether the VPN encryption feature is enabled or not
- The type of reports that the NetScreen-Global Manager station requests

---

# global-pro

**Description:** Use the **get global-pro** command to .

## Syntax

```
get global-pro { config [ > { tftp <a.b.c.d> } ] | proto-dist { table { bytes [ > { tftp <a.b.c.d> } ] | packets { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } } | user-service } }
```

For the NetScreen-1000 only:

```
get global-pro { config [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ] | proto-dist { table { bytes [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ] | packets { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } } | user-service } }
```

## Availability

This feature is supported on all NetScreen device models.

## Examples

To display the firewall protection settings:

```
ns-> get global-pro
```

## See Also

See the **set global-pro** command.

---

# glog

**Description:** Use the **get glog** command to .

Syntax

**get glog [ > { tftp <a.b.c.d> } ]**

For the NetScreen-1000 only:

**get glog [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ]**

Availability

This feature is supported on all NetScreen device models.

Examples

To display the firewall protection settings:

```
ns-> get glog
```

See Also

See the **set glog** command.



---

# 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 [ > { tftp <a.b.c.d> } | <string> ] | untrust [ > { tftp <a.b.c.d> } | <string> ] | DMZ [ > { tftp <a.b.c.d> } | <string> ] } | service [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } | <string> ] }
```

For the NetScreen-1000 only:

```
get group { address { trust [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } | <string> ] | untrust [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } | <string> ] | service [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } | <string> ] }
```

## Arguments

<b>address</b> { <b>trust</b>   <b>untrust</b>   <b>dmz</b> }	Defines the group as a trusted, untrusted, or DMZ (NS-10 and -100) address group.
<address_group_name>	Specifies the name of an address group if you do not include an address group name, the <b>get group address</b> { <b>trust</b>   <b>untrust</b>   <b>dmz</b> } command displays all the address groups for the specified interface. To see all addresses and address groups for all interfaces, use the <b>get address</b> command.
<b>service</b> <service_group_name>	Defines the group as a service group, and specifies its name if you do not include a service group name, all service groups are displayed.

## Availability

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

## Examples

To display a trusted address group named engineering:

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

---

To display a service group named `inside-sales`:

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

To display all untrusted address groups:

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

To display all service groups:

```
ns-> get group service
```

See Also

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

---

## ha

**Description:** Use the **get ha** command to display the configuration settings for high availability.

### Syntax

```
get ha [ > { tftp <a.b.c.d> } | counter [ > { tftp <a.b.c.d> } ] | track { ip [ > { tftp <a.b.c.d> } ] } ]
```

For the NetScreen-1000 only:

```
get ha [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } | counter [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ] | track { ip [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ] } ]
```

### 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

---

# hostname

**Description:** Use the **get hostname** command to display the hostname of the NetScreen device.

## Syntax

**get hostname [ > { tftp <a.b.c.d> } ]**

For the NetScreen-1000 only:

**get hostname [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ]**

## 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.

---

## ike

**Description:** Use the **get ike** command to display various settings for Internet Key Exchange (IKE).

### Syntax

```
get ike { accept-all-proposal | ca-and-type | cert | conn-entry | cookies |  
gateway [ <string> ] | id-mode | initial-contact { all-peers | single--  
gateway <string> | single-user <string> } | initiator-set-commit | p1-  
proposal [ <string> ] | p2-proposal [ <string> ] | policy-checking |  
respond-bad-spi | responder-set-commit | single-ike-tunnel <string> |  
soft-lifetime-buffer }
```

---

## Arguments

<b>accept-all-proposal</b>	Notes if all incoming proposals are accepted or not.
<b>ca-and-type</b>	Displays the types of certs the NS device supports.
<b>cert</b>	Displays all local certs loaded in the NS device.
<b>conn-entry</b>	Displays the current IKE connections.
<b>cookies</b>	Displays all IKE cookies.
<b>gateway [string]</b>	Shows the following details for all remote gateways: gateway ID number, gateway name, IP address if it uses Main or aggressive mode, its preshared key (if used), and all its Phase 1 proposals if you specify a gateway name, more details are displayed.
<b>id-mode</b>	Shows if the IKE ID mode is the IP address only or is includes the subnet.
<b>initial-contact</b>	
<b>initiator-set-commit</b>	Notes if the commit bit is set when initiating a Phase 2 proposal.
<b>p1-proposal [string]</b>	Shows the following details of all the Phase 1 proposals, or just for the proposal specified.  Proposal 1 ID number, proposal name, authentication method (preshared key, RSA signature, or DSA signature) Diffie-Hellman Group (1, 2 or 5) ESP encryption algorithm (DES or 3DES), ESP authentication algorithm (MD5 or SHA-1), and the key lifetime.

---

<b>p2-proposal [string]</b>	Shows the following details of all the Phase 2 proposals, or just for the proposal specified.  Proposal ID number, proposal name, Diffie-Hellman Group number (1, 2, or 5; 0 indicates no Pfs, and so there is no DM exchange), AH or ESP protocol, encryption algorithm (DES, 3DES), authentication algorithm (MD5, SHA-1), key lifetime (in seconds), and key lifesize (in kilobytes).
<b>policy-checking</b>	Notes if the access policies for both VPN participants must match before a VPN connection is established.
<b>respond-bad-spi</b>	
<b>responder-set-commit</b>	Notes if the commit bit is set when responding to a Phase 2 proposal.
<b>single-ike-tunnel</b>	Notes if the single-ike-tunnel flag has been set for the VPN connections with the specified remote gateway.
<b>soft-lifetime-buffer</b>	Displays the soft-lifetime buffer size (in seconds).

### Availability

This feature is available on NetScreen devices that include VPN support.

### Examples

To display all the details of the Phase 1 proposal **sf1**:

```
ns-> get ike pl-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 physical and logical interface settings for the NetScreen device.

## Syntax

For the NetScreen-5 only:

```
get ippool [ > { tftp <a.b.c.d> } trust [ > { tftp <a.b.c.d> } ] | untrust [ > { tftp <a.b.c.d> } ] | mgt [ > { tftp <a.b.c.d> } ] | all [ > { tftp <a.b.c.d> } ] ]
```

For the NetScreen-10 only:

```
get ippool [ > { tftp <a.b.c.d> } trust [ > { tftp <a.b.c.d> } ] | untrust [ > { tftp <a.b.c.d> } ] | DMZ [ > { tftp <a.b.c.d> } ] | mgt [ > { tftp <a.b.c.d> } ] | all [ > { tftp <a.b.c.d> } ] ]
```

For the NetScreen-100 only:

```
get ippool [ > { tftp <a.b.c.d> } trust [ > { tftp <a.b.c.d> } | dip [ <number> | detail [ > { tftp <a.b.c.d> } ] ] ] | untrust [ > { tftp <a.b.c.d> } | dip [ <number> | detail [ > { tftp <a.b.c.d> } ] ] ] | mip [ > { tftp <a.b.c.d> } | detail [ > { tftp <a.b.c.d> } ] ] ] | DMZ [ > { tftp <a.b.c.d> } ] | mgt [ > { tftp <a.b.c.d> } ] | all [ > { tftp <a.b.c.d> } ] ]
```

For the NetScreen-1000 only:

```
get ippool [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } trust [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ] | untrust [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } | mip [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } | detail [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ] ] ] | mgt [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ] | ha [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ] | all [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ] ]
```



---

## Arguments

<b>trust</b>	<return> dip
<b>untrust</b>	<return> dip mip
<b>DMZ</b>	<return>
<b>all</b>	<return>

## Availability

This feature is supported on all NetScreen device models.

## Examples

To display general information for all physical and logical interfaces:

```
ns-> get interface
```

To display detailed information for the Trusted interface:

```
ns-> get interface trust
```

To display all tunnel interfaces:

```
ns-> get interface tunnel
```

To display detailed information on a tunnel interface:

```
ns-> get interface tunnel | <tunnel number>
```

To display all the DIPs associated with a tunnel interface:

```
ns-> get interface <interface name> tunnel dip
```

To display all MIPs associated with the trust/4 interface:

```
ns-> get interface trust/4 mip
```

---

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 HTTP/HTTPS (via the Web) or Telnet or SCS (via the CLI).
- 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 used by the administrator to log on to the NetScreen device for system administration, either through the Web management interface or the Telnet protocol.
- Each interface is shown with its MAC address, IP address, and netmask.
- The status of the interface is shown, including the data transmission speed obtained through auto-sensing.
- The ability to respond to the **ping** command for each interface.
- The Manage IP address is the IP address used for performing Web management from a specific interface.
- The IP addresses and netmasks for the gateways used by the trusted and untrusted interfaces.
- On a NetScreen-1000, the **get interface all** command displays all virtual interfaces configured on the device.
- The **unset interface** command not only deletes the particular tunnel interface, but also removes all MIP and DIP configurations on it.

***Important:*** Ensure that all routing entries that use the deleted interface are removed from the routing table.

---

# ippool

**Description:** Use the **get ippool** command to display information about all of the IP pools.

Syntax

**get ippool [ > { tftp <a.b.c.d> } ]**

For the NetScreen-1000 only:

**get ippool [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ]**

Arguments:

<b>ippoolname</b>	Returns information about a particular IP pool.
<b>start ip</b>	Beginning IP address range for the pool.
<b>end ip</b>	End of IP address range for the pool.
<b>pool type</b>	

Availability:

This feature is available on all NetScreen devices models.

Examples:

To display the ippool values for IP pools 1 and 2:

```
ns1000-> get ippool
```

<b>ippoolname</b>	<b>start ip</b>	<b>end ip</b>	<b>pool type</b>
pool1	10.1.1.1	10.1.1.10	l2tp
pool 2	10.1.1.11	10.1.1.20	l2tp

See Also

See the **set ippool** command.

---

# l2tp

**Description:** Use the **get l2tp** command to .

## Syntax

```
get l2tp { <string> | all [ > { tftp <a.b.c.d> } | active [ > { tftp <a.b.c.d> } ] ] |  
default [ > { tftp <a.b.c.d> } ] }
```

## Availability

This feature is not supported on the NetScreen-1000.

## Examples

To display the firewall protection settings:

```
ns-> get l2tp
```

## See Also

See the **set l2tp** command.

---

# lance

**Description:** Use the **get lance** command to .

## Syntax

```
get lance [ > { tftp <a.b.c.d> } | info { tftp <a.b.c.d> } } ]
```

For the NetScreen-1000 only:

```
get lance [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } | info > { tftp <a.b.c.d> } } ]
```

## Availability

This feature is supported on all NetScreen device models.

## Examples

To display the firewall protection settings:

```
ns-> get lance
```

## See Also

See the **set lance** command.

---

# log

**Description:** Use the **get log** command to display all the entries in the log table.

## Syntax

```
get log { event [ > { tftp <a.b.c.d> } | begin <string> | end-time <string> |  
exclude <string> | include <string> | start-time <string> ] | self [ > { tftp  
<a.b.c.d> } | dst-ip <a.b.c.d> | end-time <string> | max-duration <string>  
| min-duration <string> | no-rule-displayed [ > { tftp <a.b.c.d> } ] |  
service <string> | src-ip <a.b.c.d> | src-port <number> | start-time  
<string> ] | traffic [ > { tftp <a.b.c.d> } | dst-ip <a.b.c.d> | end-time  
<string> | max-duration <string> | min-duration <string> | no-rule-  
displayed [ tftp <a.b.c.d> ] | policy { <number low-high> | < number> } |  
service <string> | src-ip { <a.b.c.d> | <a.b.c.d> } src-port { <number low-  
high> | <number> } | start-time <string> ] }
```

For the NetScreen-1000 only:

```
get log { event [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } |  
begin <string> | end-time <string> | exclude <string> | include <string>  
| start-time <string> ] | self [ # { slot <number> | vsys <string> } | > { tftp  
<a.b.c.d> } | dst-ip <a.b.c.d> | end-time <string> | max-duration <string>  
| min-duration <string> | no-rule-displayed [ # { slot <number> | vsys  
<string> } | > { tftp <a.b.c.d> } ] | service <string> | src-ip <a.b.c.d> | src-  
port <number> | start-time <string> ] | traffic [ # { slot <number> | vsys  
<string> } | > { tftp <a.b.c.d> } | dst-ip <a.b.c.d> | end-time <string> | max-  
duration <string> | min-duration <string> | no-rule-displayed [ # { slot  
<number> | vsys <string> } | > { tftp <a.b.c.d> } ] | policy { <number low-  
high> | < number> } | service <string> | src-ip { <a.b.c.d> | <a.b.c.d> } src-  
port { <number low-high> | <number> } | start-time <string> ] }
```

## Arguments

<b>event</b>	Specifies event log entries.
<b>get log self</b>	Packet denied by interfaces.

---

<b>start time</b> <dd/mm[/yy   yyyy] [hh[:mm[:ss]]]>	<p>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 can be omitted. Separate the date from the time with a space, a dash, or an underscore:</p> <ul style="list-style-type: none"> <li>• 12/31/2001 23:59:00</li> <li>• 12/31/2001-23:59:00</li> <li>• 12/31/2001_23:59:00</li> </ul>
<b>end-time</b> <dd/mm[/yy   yyyy] [hh[:mm[:ss]]]>	Displays event log entries that occurred at and before the time specified.
<b>include</b> <include_string>	Displays event log entries that include the detail specified.
<b>exclude</b> <exclude_string>	Displays event log entries that exclude the detail specified.
<b>begin</b> <begin_string>	Displays event log entries that follow a specified event.
<b>traffic</b>	Specifies traffic log entries.
<b>policy</b> <policy_id>   <policy_id_range>	<p>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:</p> <p>&lt;policy_id&gt;-&lt;policy_id&gt;</p>
<b>min-duration</b> <hh[:mm[:ss]]>	Displays traffic log entries for traffic whose duration was longer than or equal to the minimum duration specified.
<b>max-duration</b> <hh[:mm[:ss]]>	Displays traffic log entries for traffic whose duration was shorter than or equal to the maximum duration specified.

---

<b>service</b> <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. Although you cannot specify a service group, note that because TP is recognized as FTP, HTTP, and TFTP, entering TP displays log entries for all three Services.
<b>src-ip</b> {<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.
<b>src-port</b> {<port_number>   <port_range>}	Displays traffic log entries for a specified port number or range of source port numbers.
<b>dst-ip</b> {<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.
<b>no-rule-displayed</b>	Displays only traffic log entries, but does not display access policy information.

### Availability

The get log command is completely supported on the NetScreen-1000. All 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 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** [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> }

### 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 counter of the packets received and transmitted through the Switching board, including 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 [ trust [ > { tftp <a.b.c.d> } ] | untrust [ > { tftp <a.b.c.d> } ] ]**

## Arguments

None.

## Availability

This feature is available on only the NetScreen-10.

## 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.

Use this command only when the NetScreen device is in Transparent mode.

---

# master

**Description:** Use the **get master** command to.

## Syntax

```
get master [ > { tftp <a.b.c.d> } | config [ > { tftp <a.b.c.d> } ] ]
```

For the NetScreen-1000 only:

```
get master [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } |  
config [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ] ]
```

## Availability

This feature is supported on all NetScreen device models.

## Examples

To display the firewall protection settings:

```
ns-> get master
```

## See Also

See the **set master** command.

---

# memory

**Description:** Use the **get memory** command to display the memory allocation status.

## Syntax

```
get memory [ > { tftp <a.b.c.d> } | <number> | all [ > { tftp <a.b.c.d> } ] | error [ > { tftp <a.b.c.d> } ] | free [ > { tftp <a.b.c.d> } ] | used [ > { tftp <a.b.c.d> } ] ]
```

For the NetScreen-1000 only:

```
get memory [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } | <number> | all [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ] | error [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ] | free [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ] | used [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ] ]
```

## Arguments

## 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 mpssess** command to display the session allocation status on the NetScreen-1000 main processing board.

### Syntax

```
get mpssess [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } |  
session <number> | stats [ # { slot <number> | vsys <string> } | > { tftp  
<a.b.c.d> } ] ]
```

### Arguments

### 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 mpssess
```

### Notes

The **get mpssess** 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 [ > { tftp <a.b.c.d> } | all [ > { tftp <a.b.c.d> } ] ]
```

For the NetScreen-1000 only:

```
get mip [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } | all [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ] ]
```

## Arguments

## 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.



---

# nsp-tunnel

**Description:** Use the **get nsp-tunnel** command to .

## Syntax

**get nsp-tunnel** [ > { **tftp** <a.b.c.d> } | **info** { **tftp** <a.b.c.d> } } ]

For the NetScreen-1000 only:

**get nsp-tunnel** [ # { **slot** <number> | **vsys** <string> } | > { **tftp** <a.b.c.d> } | **info** { **tftp** <a.b.c.d> } } ]

## Arguments

## Availability

This feature is supported on all NetScreen device models.

## Examples

To display the firewall protection settings:

```
ns-> get nsp-tunnel
```

## See Also

See the **set nsp-tunnel** command.

---

# ntp

**Description:** Use the **get ntp** command to display the settings for the Network Time Protocol (NTP).

## Syntax

**get ntp [ > { tftp <a.b.c.d> } ]**

For the NetScreen-1000 only:

**get ntp [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ]**

## Arguments

## 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, and NetScreen-1000 at version 2.6 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.

**Description:** Use the **get os** command to .

Syntax

**get os [ > { tftp <a.b.c.d> } ]**

For the NetScreen-1000 only:

**get os [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ]**

Availability

This feature is supported on all NetScreen device models.

Examples

To display the firewall protection settings:

```
ns-> get os
```

See Also

See the **set os** command.

---

# 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 [ > { tftp <a.b.c.d> } | ldap [ > { tftp <a.b.c.d> } ] | x509 { cert-path [ > { tftp <a.b.c.d> } ] | crl-refresh [ > { tftp <a.b.c.d> } ] | dn [ > { tftp <a.b.c.d> } ] | list { ca-cert [ > { tftp <a.b.c.d> } ] | cert [ > { tftp <a.b.c.d> } ] | local-cert [ > { tftp <a.b.c.d> } ] } | ns-cert [ > { tftp <a.b.c.d> } ] | pkcs10 [ > { tftp <a.b.c.d> } ] ]
```

For the NetScreen-1000 only:

```
get pki [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } | ldap [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ] | x509 { cert-path [ > { tftp <a.b.c.d> } # { slot <number> | vsys <string> } | ] | crl-refresh [ > { tftp <a.b.c.d> } # { slot <number> | vsys <string> } | ] | dn [ > { tftp <a.b.c.d> } # { slot <number> | vsys <string> } | ] | list { ca-cert [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ] | cert [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ] | local-cert [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ] | ns-cert [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ] | pkcs10 [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ] ]
```

```
get os [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ]
```

## Arguments

<b>ldap</b>	Shows the default certificate authority server's address and the default LDAP URL for the certificate revocation list (CRL) retrieval.
<b>rsa</b>	Displays the current RSA key length in bits.
<b>x509</b>	Specifies an International Telecommunications Union (ITU-T) X.509/PKCS digital certificate. (PKCS: Public Key Cryptography Standard)
<b>crl-refresh</b>	Displays the X.509 CRL refresh frequency rate.

---

<b>dn</b>	Displays the distinguished name on the NetScreen X.509 digital certificate.
<b>list</b>	Displays the X.509 object list loaded in the NetScreen device.
<b>ca-cert</b>	Shows the certificate authority (CA) X.509 certificates currently loaded in the NetScreen device.
<b>cert</b>	Displays the X.509 certificates currently loaded in the NetScreen device.
<b>local-cert</b>	Displays the non-CA (that is, local) X.509 certificates currently loaded in the NetScreen device.
<b>pkcs10</b>	Shows the destination of the PKCS10 file and generates the file in that location.

### Availability

This feature will be 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 [ > { tftp <a.b.c.d> } | id <number> | traffic-shaping [ > { tftp <a.b.c.d> } ] | outgoing [ > { tftp <a.b.c.d> } | asic [ > { tftp <a.b.c.d> } ] ] | traffic-shaping [ > { tftp <a.b.c.d> } ] ] | incoming [ > { tftp <a.b.c.d> } | asic [ > { tftp <a.b.c.d> } ] ] | traffic-shaping [ > { tftp <a.b.c.d> } ] ] | fromdmz [ > { tftp <a.b.c.d> } | asic [ > { tftp <a.b.c.d> } ] ] | traffic-shaping [ > { tftp <a.b.c.d> } ] ] | todmz [ > { tftp <a.b.c.d> } | asic [ > { tftp <a.b.c.d> } ] ] | traffic-shaping [ > { tftp <a.b.c.d> } ] ] ]
```

For the NetScreen-1000 only:

```
get policy [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } | id <number> | outgoing [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } | asic [ > { tftp <a.b.c.d> } ] ] | incoming [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } | asic [ > { tftp <a.b.c.d> } ] ] ] ]
```

## Arguments

<b>all</b>	Displays a summary of access policies for all the interfaces.
<b>incoming</b>	Displays a summary of Incoming access policies.
<b>outgoing</b>	Displays a summary of Outgoing access policies.
<b>todmz</b>	Displays a summary of access policies to the DMZ interface (if applicable).
<b>fromdmz</b>	Displays a summary of access policies from the DMZ interface (if applicable).
<b>number</b>	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.

---

# pport

**Description:** Use the **get pport** command to .

Syntax

```
get pport [ > { tftp <a.b.c.d> } | count [ > { tftp <a.b.c.d> } ] | dst <a.b.c.d> ]
```

For the NetScreen-1000 only:

```
get pport [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } | count  
[ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ] | dst <a.b.c.d> ]
```

Availability

This feature is supported on all NetScreen device models.

Examples

To display the firewall protection settings:

```
ns-> get pport
```

See Also

See the **set pport** command.



---

# route

**Description:** Use the **get route** command to display entries in the static route table.

## Syntax

**get route** [ > { **tftp** <a.b.c.d> } | **ip** <a.b.c.d> ]

For the NetScreen-1000 only:

**get route** [ # { **slot** <number> | **vsys** <string> } ] > { **tftp** <a.b.c.d> } | **ip** <a.b.c.d> ]

## Arguments

**ip** <a.b.c.d>                      Displays a specific static route for the target 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 target IP address is specified.

## Examples

To display all the entries in the static route table:

```
ns-> get route
```

To display the static route information to 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, and flag
- The Flag value is **8000** for a well-known route generated from the interface IP address and interface gateway
- The Flag value is **0000** if the entry uses the gateway from the interface listed of a specified IP address
- When you specify an IP address in the get route command, the output appears in this format:

`<ip-addr> => <interface>/<gateway>, <metric>`

- Use the **get route** command to find out if a packet with particular IP address gets routed by the NetScreen device to the correct interface

---

## sa

**Description:** Use the **get sa** command to display the IPSec security associations (SA) only when you define VPN policies for a manual VPN.

### Syntax

```
get sa [ > { tftp <a.b.c.d> } | active [ > { tftp <a.b.c.d> } | stat [ > { tftp <a.b.c.d> } ] | id <number> } | inactive [ > { tftp <a.b.c.d> } | stat [ > { tftp <a.b.c.d> } | stat [ > { tftp <a.b.c.d> } ] ] ] ]
```

For the NetScreen-1000 only:

```
get sa [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } | active [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } | stat [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ] | id <number> } | inactive [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } | stat [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } | stat [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ] ] ]
```

```
get sa [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } | once [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ] | recurrent [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ] ] ]
```

---

## Arguments

<b>id &lt;number&gt;</b>	Displays a specific IPSec security association (SA) entry with the ID number <number>.
<b>stat</b>	<p>Displays the following statistics for all incoming/outgoing SA pairs:</p> <ul style="list-style-type: none"><li>• <b>Fragment:</b> The total number of fragmented incoming and outgoing packets.</li><li>• <b>Auth-Fail:</b> The total number of packets for which authentication has failed.</li><li>• <b>Other:</b> The total number of miscellaneous internal error conditions other than those listed in the auth-fail category.</li><li>• <b>Total Bytes:</b> The amount of active incoming and outgoing traffic</li><li>• <b>ID:</b> The SA ID number</li><li>• <b>Gateway:</b> The remote GW IP address</li><li>• <b>Algorithm:</b> The AH and ESP algorithms</li><li>• <b>SPI:</b> The security parameter index numbers</li><li>• <b>Life (sec):</b> The key lifetimes in seconds</li><li>• <b>Life (Kb):</b> The key lifetimes in kilobytes</li><li>• <b>Status:</b> The</li><li>• <b>PID:</b> The</li><li>• <b>Link:</b> The notes if it is currently active or inactive</li></ul>

## Availability

This feature is available on all NetScreen device models that support VPNs.

---

## Examples

To display all the 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**, **set ike**, and **clear sa-statistics** commands.

---

# scheduler

**Description:** Use the **get scheduler** command to display the schedules configured for the NetScreen device.

## Syntax

```
get scheduler [ > { tftp <a.b.c.d> } | name <string> | once [ > { tftp <a.b.c.d> } ] | recurrent [ > { tftp <a.b.c.d> } ] ]
```

For the NetScreen-1000 only:

```
get scheduler [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } | name <string> | once [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ] | recurrent [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ] ]
```

## Arguments

**all** Displays all the schedules configured on the NetScreen device.

## Availability

This feature is available on all NetScreen device models.

## Examples

To display all the schedule definitions:

```
ns-> get scheduler all
```

## 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 to a NetScreen device from a remote system.

### Syntax

**get scs [ > { tftp <a.b.c.d> } ]**

For the NetScreen-1000 only:

**get scs [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ]**

### Arguments

<b>scs</b>	Displays all users and keys. Because each key is identified by a number, when you use the <b>unset scs &lt;key_id&gt;</b> command you can enter only the key identification number, not the entire key.
------------	---

### Availability

This feature is available on the NetScreen-100 and NetScreen-1000 at version 2.0 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 list.

## Syntax

```
get service [ > { tftp <a.b.c.d> } | group [ > { tftp <a.b.c.d> } | <string> ] |  
pre-defined [ > { tftp <a.b.c.d> } ] | user [ > { tftp <a.b.c.d> } ] ]
```

For the NetScreen-1000 only:

```
get service [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } |  
group [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } | <string> ]  
| pre-defined [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ] |  
user [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ] ]
```

## Arguments

<b>&lt;string&gt;</b>	Displays a specific service named <string>.
<b>user</b>	Displays all user-defined services.
<b>group</b>	Displays all service groups.
<b>pre-defined</b>	Displays all the pre-defined services.

## Availability

This feature is available on all NetScreen device models.

## Defaults

Using the **get service** command without any arguments displays all entries pre-defined, user-defined, and service groups in the service list.

## Examples

To display all entries in the service list:

```
ns-> get service
```

To display all user-defined entries in the service list:

```
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 [ > { tftp <a.b.c.d> } | id <number> | ip <a.b.c.d> | port <number> | protocol <number> | tunnel [ > { tftp <a.b.c.d> } ] ]
```

For the NetScreen-1000 only:

```
get session [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } | id <number> | ip <a.b.c.d> | port <number> | protocol <number> | tunnel [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ] ]
```

## Arguments

<b>ip</b> <a.b.c.d>	Displays the entries in the session table for the IP address a.b.c.d.
<b>protocol</b> <number>	Displays the entries in the session table for a specific protocol number.
<b>port</b> <number>	Displays the entries in the session table for a specific port number.
<b>id</b> <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 by default.

## Examples

To display all the entries in the session table:

```
ns-> get session
```

To display all the entries in the session table for a specific IP address:

```
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 [ > { tftp <a.b.c.d> } ] | auth-trap [ > { tftp <a.b.c.d> } ] | community <string> | settings [ > { tftp <a.b.c.d> } ] | vpn [ > { tftp <a.b.c.d> } ] }
```

For the NetScreen-1000 only:

```
get snmp { all [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ] | auth-trap [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ] | community <string> | settings [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ] | vpn [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ] }
```

### Arguments

<b>all</b>	Displays all communities and their hosts.
<b>auth-trap</b>	Displays the status of SNMP authentication traps.
<b>community</b> <name>	Displays the permissions assigned to the named SNMP community.
<b>settings</b>	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 the 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.

---

## socket

**Description:** Use the **get socket** command to .

Syntax

**get socket** [ > { **tftp** <a.b.c.d> } | **id** <number> ]

For the NetScreen-1000 only:

**get socket** [ # { **slot** <number> | **vsys** <string> } | > { **tftp** <a.b.c.d> } | **id** <number> ]

Availability

This feature is supported on all NetScreen device models.

Examples

To display the firewall protection settings:

```
ns-> get socket
```

See Also

See the **set socket** command.

---

## software-key

**Description:** Use the **get software-key** command to .

Syntax

**get software-key [ > { tftp <a.b.c.d> } ]**

For the NetScreen-1000 only:

**get software-key [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ]**

Availability

This feature is supported on all NetScreen device models.

Examples

To display the firewall protection settings:

```
ns-> get software-key
```

See Also

See the **set software-key** command.

---

# ssl

**Description:** Use the **get ssl** command to .

Syntax

```
get ssl [ > { tftp <a.b.c.d> } | cert-list { tftp <a.b.c.d> } ]
```

For the NetScreen-1000 only:

```
get ssl [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } | cert-list [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ]
```

Availability

This feature is supported on all NetScreen device models.

Examples

To display the firewall protection settings:

```
ns-> get ssl
```

See Also

See the **set ssl** command.



---

# syslog

**Description:** Use the **get syslog** command to display the syslog configuration.

## Syntax

```
get syslog [ > { tftp <a.b.c.d> } | VPN > { tftp <a.b.c.d> } | config > { tftp <a.b.c.d> } | enable > { tftp <a.b.c.d> } | port > { tftp <a.b.c.d> } | traffic > { tftp <a.b.c.d> } ]
```

For the NetScreen-1000 only:

```
get syslog [ [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ] | VPN [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ] | config [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ] | enable [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ] | port [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ] | traffic [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ] ]
```

## Arguments

<b>config</b>	Shows whether the syslog mechanism is configured or not.
<b>enable</b>	Shows whether syslog is enabled or not.
<b>port</b>	Displays the port used to communicate with the syslog server.
<b>traffic</b>	Indicates whether the traffic log is sent to syslog.
<b>websense</b>	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 communicate 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 Webtrends server is enabled or not:

```
ns-> get syslog webtrends
```

See Also

See the **set syslog** command.

---

# system

**Description:** Use the **get system** command to display general system information.

## Syntax

**get system [ > { tftp <a.b.c.d> } ]**

For the NetScreen-1000 only:

**get system [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ]**

## Arguments

None.

## Availability

This feature is available on all NetScreen device models.

## 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 [ > { tftp <a.b.c.d> } ]**

For the NetScreen-1000 only:

**get tech-support [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ]**

## 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** [ > { **tftp** <a.b.c.d> } ]

For the NetScreen-1000 only:

**get timer** [ # { **slot** <number> | **vsys** <string> } | > { **tftp** <a.b.c.d> } ]

## 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 the named interface. If no name is specified, the information for all interfaces is displayed.

## Syntax

```
get traffic-shaping { interface [ <string> ] | ip_precedence [ > { tftp  
<a.b.c.d> } ] | mode [ > { tftp <a.b.c.d> } ]
```

## Arguments

**<name>** Defines the name of the interface.

## Availability

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

## Defaults

{

## Examples

To display traffic management information for all interfaces:

```
ns-> get traffic-shaping interface
```

---

# url

**Description:** Use the **get url** command to display the URL blocking configuration settings.

## Syntax

**get url [ > { tftp <a.b.c.d> } ]**

For the NetScreen-1000 only:

**get url [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ]**

## Arguments

None.

## Availability

This feature is available on all NetScreen device models.

## Examples

To display information about the URL blocking settings:

```
ns-> get url
```

## See Also

See the **set url** command.

## Notes

NetScreen monitors the status of the WebSense server once a minute. When the WebSense server does not respond, this is reported in the Web User Interface (Web UI). 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 have a maximum of 256 requests.

---

## user

**Description:** Use the **get user** command to display the user authentication database.

### Syntax

```
get user { <string> | all [ > { tftp <a.b.c.d> } ] | id <number> }
```

For the NetScreen-1000 only:

```
get user { <string> | all [ # { slot <number> | vsys <string> } | > { tftp  
<a.b.c.d> } ] | id <number> }
```

### Arguments

<b>all</b>	Displays a the following information for all the entries in the User database: <ul style="list-style-type: none"><li>• User ID number</li><li>• User name</li></ul>
<b>id</b> <number>	Displays the information elicited from the set user all command plus any user-specified remote L2TP settings. a specific user with ID <number>.
<string>	Displays the following information with the name <user_name>: <ul style="list-style-type: none"><li>• Status (enabled or not)</li><li>• Use type_auth, ike 12tp, auth/ike, auth/12tp, auth/ike/12tp, ike/12tps</li><li>• IKE ID types - email address, IP address, domain name</li><li>• IKE identities</li></ul>

### 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 { > { tftp <a.b.c.d> } | server [ > { tftp <a.b.c.d> } ] | session [ > { tftp <a.b.c.d> } ] }
```

For the NetScreen-1000 only:

```
get vip { # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } | server [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ] | session [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ] }
```

## Arguments

<b>server</b>	Displays the load balance status of servers receiving traffic to VIPs.
<b>session</b>	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.

---

## vpn

**Description:** Use the **get vpn** command to display all Virtual Private Network (VPN) configurations.

### Syntax

```
get vpn { > { tftp <a.b.c.d> } | auto [ > { tftp <a.b.c.d> } ] | manual [ > { tftp <a.b.c.d> } ] }
```

For the NetScreen-1000 only:

```
get vpn { # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } | auto [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ] | manual [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ] }
```

### Arguments

**<string>** Displays the following information for a specific VPN with the name <string>. Name: <vpn\_name>, Trunk VPN local and remote SP1 numbers remote-gu IP address

SA: 0

Fag: 0010

AH or ESP protocol and the algorithms try employ algorithm passwords and keys if VPN monitoring is on or off.

**manual** Displays all Manual key VPNs.

**auto** Displays all Autokey IKE VPNs.

### Availability

This feature is available on NetScreen devices that support VPNs.

### 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.

---

# vpnmonitor

**Description:** Use the **get vpnmonitor** command to .

Syntax

**get vpnmonitor [ > { tftp <a.b.c.d> } ]**

Availability

This feature is supported on all NetScreen device models.

Examples

To display the firewall protection settings:

```
ns-> get vpnmonitor
```

See Also

See the **set vpnmonitor** 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 [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ]
```

### 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 netmask for a virtual system named **organization3**:

```
ns-> get vsys organization3
```

### See Also

See the **set interface**, **set vsys**, **enter vsys**, and **exit** commands.

### 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 0xFF.

---

# webtrends

**Description:** Use the **get webtrends** command to .

## Syntax

**get webtrends [ > { tftp <a.b.c.d> } ]**

For the NetScreen-1000 only:

**get webtrends [ # { slot <number> | vsys <string> } | > { tftp <a.b.c.d> } ]**

## Availability

This feature is supported on all NetScreen device models.

## Examples

To display the firewall protection settings:

```
ns-> get webtrends
```

## See Also

See the **set webtrends** 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.

The **Clear** commands include the following:

- **admin** (page 4-2)
- **alarm** (page 4-3)
- **arp** (page 4-5)
- **auth** (page 4-6)
- **counter** (page 4-7)
- **crypto** (page 4-8)
- **dbuf** (page 4-9)
- **dhcp** (page 4-10)
- **dns** (page 4-12)
- **file** (page 4-13)
- **ike-cookie** (page 4-14)
- **l2tp** (page 4-15)
- **log** (page 4-16)
- **mac-count** (page 4-18)
- **mac-learn** (page 4-19)
- **node\_secret** (page 4-20)
- **pppoe** (page 4-21)
- **sa** (page 4-22)
- **sa-statistics** (page 4-23)
- **session** (page 4-24)



---

# admin

**Description:** Use the **clear admin** command to remove remote administrator profiles.

## Syntax

```
clear admin user { cache | login }
```

## Arguments

<b>user</b>	Specifies the admin user.
<b>cache</b>	Specifies the profiles of remote administrators stored in flash memory.
<b>login</b>	Specifies administrators that are currently logged in.

## Availability

This feature is supported on all Product Name device models.

## Examples

To clear the profiles for all remote administrators:

```
ns-> clear admin user cache
```

## See Also

See the **set admin**, **unset admin**, **get admin** command.

---

# alarm

**Description:** Use the **clear alarm** command to clear the entries in the alarm table.

## Syntax

**clear alarm event** [ **end-time** <mm/dd/yy-hh:mm:ss> ]

**clear alarm traffic** [ **end-time** <mm/dd/yy-hh:mm:ss> | **policy** { <number low-high> | <number> } ]

## Arguments

<b>event</b>	Specifies entries in the event alarm table.
<b>traffic</b>	Specifies entries in the traffic alarm table.
<b>end-time</b> <mm/dd/yy-hh:mm:ss>	<p>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:</p> <ul style="list-style-type: none"><li>• <b>12/31/01 23:59:00</b></li><li>• <b>12/31/01-23:59:00</b></li><li>• <b>12/31/01_23:59:00</b></li></ul>
<b>policy</b> { <number low-high>   <number> }	<p>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: &lt;number low-high&gt;-&lt;number&gt;</p>

## Availability

This feature is supported on all Product Name device 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 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 **set alarm**, **unset alarm**, **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 Product Name device models.

## Examples

To clear the entries in the ARP table:

```
ns-> clear arp
```

## See Also

See the **set arp**, **unset arp**, **get arp** command.



---

# counter

**Description:** Use the **clear counter** command to clear interface and flow counters.

## Syntax

**clear counter flow**

**clear counter ha**

**clear counter interface**

## Arguments

<b>flow</b>	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.
<b>ha</b>	Specifies counters for packets transmitted across a high-availability (HA) link between two Product Name devices. An HA-level inspection keeps count of the number of packets and packet errors.
<b>interface</b>	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 Product Name device models.

## Examples

To clear interface counters:

```
ns-> clear counter interface
```

To clear flow counters:

```
ns-> clear counter flow
```

## See Also

See the **get counter** command.

---

# crypto

**Description:** Use the **clear crypto** command to clear.

## Syntax

**clear crypto auth-key**

**clear crypto file**

## Arguments

**auth-key** Deletes image authentication key.

**file** Deletes all crypto files.

## Availability

This feature is supported on all Product Name device models.

## Examples

To clear:

```
ns-> clear crypto
```

## See Also

See the **ping crypto** and **trace-route crypto** commands.

---

# 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 Product Name device models.

## Examples

To clear the contents of the debug buffer:

```
ns-> clear dbuf
```



---

# dhcp

**Description:** Use the **clear dhcp** command to release the IP address the Product Name 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**

**clear dhcp server { ip { <a.b.c.d> | all } }**

## Arguments

<b>client</b>	Clears the DHCP client.
<b>server</b>	Clears the DHCP server.
<b>ip</b>	(Client) Releases the IP address assigned to the Product Name device.  (Server) Resets the server IP address.
<b>&lt;a.b.c.d&gt;</b>	(Server only) Returns the IP address <b>&lt;a.b.c.d&gt;</b> to the DHCP server pool.
<b>all</b>	(Server only) Returns all IP addresses to the DHCP server pool.

## Availability

This feature is supported on the Product Name-5 at version 1.63 or later, the Product Name-10 at version 2.0 or later (server only), and the Product Name-100. This feature is not supported for the Product Name-1000.

## Examples

To release the IP address that the Product Name 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 **set dhcp**, **unset dhcp**, **get dhcp**, and **exec dhcp client** 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 Product Name device models.

## Examples

To clear the dns cache:

```
ns-> clear dns
```

## See Also

See the **set dns**, **unset dns**, **get 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 Product Name 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>**

**clear ike-cookie all**

## Arguments

<b>&lt;a.b.c.d&gt;</b>	Clear the entries for IP address <b>&lt;a.b.c.d&gt;</b> in the IKE cookie table.
<b>all</b>	Clears all entries in the IKE cookie table.

## Availability

This feature is supported on all Product Name 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 **set ike**, **unset ike** and **get ike** commands.

---

# I2tp

**Description:** Use the **clear l2tp** command to clear.

## Syntax

```
clear l2tp all  
clear l2tp ip <a.b.c.d>
```

## Arguments

<b>all</b>	Clears all active l2tp tunnels.
<b>ip &lt;a.b.c.d&gt;</b>	Specifies the peer IP address.

## Availability

This feature is supported only on the Product Name-5, -10, and -100. This feature is not supported on the Product Name-1000.

## Examples

To clear:

```
ns-> clear l2tp
```

## See Also

See the **set l2tp**, **unset l2tp**, **get l2tp**, **unset l2tp**, **ping l2tp** and **trace-route l2tp** commands.

---

# log

**Description:** Use the **clear log** command to clear the entries in the log table.

## Syntax

```
clear log event [ end-time <mm/dd/yy-hh:mm:ss> ]
```

```
clear log self [ end-time <mm/dd/yy-hh:mm:ss> ]
```

```
clear log traffic [ end-time <mm/dd/yy-hh:mm:ss> | policy { <number low-high> | <number> } ]
```

## Arguments

<b>event</b>	Clears event entries from the log.
<b>self</b>	Clears self-log entries from the log.
<b>traffic</b>	Clears traffic entries from the log.
<b>end-time &lt;mm/dd/yy-hh:mm:ss&gt;</b>	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: <ul style="list-style-type: none"><li>• <b>12/31/01 23:59:00</b></li><li>• <b>12/31/01-23:59:00</b></li><li>• <b>12/31/01_23:59:00</b></li></ul>
<b>policy { &lt;number low-high&gt;   &lt;number&gt; }</b>	Clears the traffic entries in the log table for the access policy with ID number <number low-high> or <number > or for access policies within the range of specified ID numbers.

## Availability

This feature is supported on all Product Name device models.

## 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 Product Name-1000 Switching board.

### Syntax

**clear mac-count**

### Arguments

None.

### Availability

This feature is supported only on the Product Name-1000.

### Example

To clear the packet counters:

```
ns1000-> clear mac-count
```

### See Also

See the **get mac-count** command.



---

# node\_secret

**Description:** Use the **clear node\_secret** command when the Product Name device is using SecurID to authenticate users and is not communicating properly with the ACE Server. If the system IP or interface IP address changes, the node secret must be cleared and reset on both NS device and the ACE Server.

## Syntax

**clear node\_secret**

## Arguments

None.

## Availability

This feature is supported on all Product Name device models.

## Defaults

None.

## Examples

To clear and prompt the Product Name device to request the node secret from the ACE server:

```
ns-> clear node_secret
```

## Notes

If you remove, move, or reconfigure a Product Name device, it might 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 Product Name device in flash nonvolatile memory.

### **Caution**

*Because it is not stored in the configuration, it is not cleared by an **unset all** command. Whenever the Product Name changes its IP address, or the ACE server administrator decides to delete and recreate the client, this secret will need to be reset.*

---

# pppoe

**Description:** Use the **clear pppoe** command to reset PPPoE statistical registers.

## Syntax

**clear pppoe**

## Arguments

None.

## Availability

This feature is supported only on Product Name-5 device models.

## Examples

To reset the statistics for your PPPoE connection:

```
ns5-> clear pppoe
```

## See Also

See **set pppoe**, **unset pppoe**, **get pppoe**, and **exec pppoe** commands.

---

## sa

**Description:** Use the **clear sa** command to clear the IKE value for the specified Security Association (SA).

### Syntax

**clear sa** <number>

### Arguments

<number> Specifies the SA index number.

### Availability

This feature is supported on all Product Name device models.

### Examples

To clear the IKE value for SA 2:

```
ns-> clear sa 2
```

### See Also

See the **clear sa-statistics** 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 Product Name 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.

The miscellaneous commands include the following:

- **enter vsys** (page 5-2)
- **exec dhcp** (page 5-3)
- **exec dns** (page 5-4)
- **exec ha** (page 5-5)
- **exec ntp** (page 5-6)
- **exec ping (see “ping” on page 5-14)** (page 5-7)
- **exec pki** (page 5-8)
- **exec pppoe** (page 5-9)
- **exec save (see “save” on page 5-16)** (page 5-10)
- **exec software-key** (page 5-11)
- **exec trace-route** (page 5-12)
- **exit** (page 5-13)
- **ping** (page 5-14)
- **reset** (page 5-15)
- **save** (page 5-16)
- **snoop** (page 5-19)
- **trace-route** (page 5-21)



---

## enter vsys

**Description:** Use the **enter vsys** command to enter a virtual system on the Product Name device.

### Syntax

```
enter vsys <string>
```

### Arguments

<string> Specifies an existing virtual system to be entered.

### Availability

This feature is supported on all Product Name device models.

### Examples

To enter the virtual system named **cloister**:

```
ns1000-> enter vsys cloister
```

### See Also

See the **set vsys**, **unset vsys**, **set vsys-traffic**, and **unset vsys-traffic** commands.

---

# exec dhcp

**Description:** Use the **exec dhcp** command to renew the lease for an IP address from a DHCP server.

## Syntax

**exec dhcp client { renew }**

**exec dhcp server { sync }**

## Arguments

<b>client</b>	Executes the DHCP client.
<b>renew</b>	Renews DHCP client lease.
<b>server</b>	Executes the DHCP server.
<b>sync</b>	Syncs DHCP server IP allocation.

## Availability

This feature is available on the Product Name-5 at version 1.65 or later, the Product Name-10 at version 2.0 or later, and the Product Name-100. This feature is unavailable on the NetScreen-1000.

## 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**, **get dhcp**, and **clear dhcp** commands.

## Notes

The **exec dhcp** 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 Product Name device once the DHCP server reboots. The Product Name device may or may not obtain the same IP address it was using.

---

## exec dns

**Description:** Use the **exec dns** command to refresh all DNS entries.

### Syntax

```
exec dns { refresh }
```

### Arguments

<b>refresh</b>	Refreshes all DNS entries.
----------------	----------------------------

### Availability

This feature is supported on all Product Name device models.

### Examples

To refresh DNS entries:

```
ns-> exec dns refresh
```

### See Also

See the **set dns**, **unset dns**, **get dns**, and **clear dns** commands.

---

# exec ha

**Description:** Use the **exec ha** command to copy files from a master unit to a slave unit. Execute this command in the master unit.

## Syntax

**exec ha file-sync [ <string> ]**

## Arguments

**file-sync <string>** 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 Product Name-100 at version 2.0 or later and the Product Name-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**, **unset ha**, **get ha** commands.

---

## **exec ntp**

**Description:** Use the **exec ntp** command to immediately update the Product Name device clock using Network Time Protocol (NTP).

### Syntax

**exec ntp { update }**

### Arguments

**update** Updates time from NTP server.

### Availability

This feature is available on Product Name-5 devices at version 1.65 or later, Product Name-10, -100, -100p, and -1000 devices at version 2.0 or later.

### Examples

To update the Product Name device time by synchronizing it with the NTP server:

```
ns-> exec ntp update
```

### See Also

See the **set ntp**, **unset ntp**, and **get ntp** commands.

---

## **exec ping (see “ping” on page 5-14)**

See Also

See the **ping ping** and **trace-route ping** commands.

---

# exec pki

**Description:** Use the **exec pki** commands to manage RSA and PSA key pair generation and X.509 certificate requests and removals for public-key infrastructure (PKI).

## Syntax

```
exec pki dsa { new-key <number> }
```

```
exec pki rsa { new-key <number> }
```

```
exec pki x509 { delete <number> | pkcs10 | tftp <a.b.c.d> }
```

## Arguments

<b>dsa new-key &lt;number&gt;</b>	Generates a new DSA key pair with a specified bit length (512, 768, 1024, 2048).
<b>rsa new-key &lt;number&gt;</b>	Generates a new RSA key pair with a specified bit length (512, 768, 1024, 2048).
<b>x509 delete &lt;number&gt;</b>	Removes a specified X.509 certificate from a Product Name device.
<b>x509 pkcs10</b>	Generates a PKCS10 file for a X.509 certificate request for the Product Name device.
<b>x509 tftp &lt;a.b.c.d&gt;</b>	Upload the specified certificate or CRL file for the specified TFTP server.

## Availability

This feature is supported on all Product Name 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 Product Name device:

```
ns-> exec pki x509 delete 3
```

## See Also

See also the **set pki**, **unset 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**

**exec pppoe disconnect**

### Arguments

<b>connect</b>	Starts PPPoE connection.
<b>disconnect</b>	Takes down a PPPoE connection.

### Availability

This feature is available only on Product Name-5 device models.

### Examples

To setup your PPPoE connection:

```
ns1000-> exec pppoe connect
```

### See Also

See **set pppoe**, **unset pppoe**, **get pppoe**, and **clear pppoe** commands.



---

## **exec save (see “save” on page 5-16)**

### See Also

See the **save config**, **reset save-config**, and **save software** commands.

---

# exec software-key

**Description:** Use the **exec software-key** command to.

## Syntax

```
exec software-key { vpn <string> }
```

## Arguments

**vpn <string>**

## Availability

This feature is supported on all Product Name device models.

## Examples

```
ns-> exec software-key
```

## See Also

See the **get software-key** and **save software** commands.

---

## exec trace-route

**Description:** Use the **exec trace-route** command to.

### Syntax

**exec trace-route** <string>

### Arguments

<string>

### Availability

This feature is supported on all Product Name device models.

### Examples

ns-> **exec software-key**

---

# exit

**Description:** (1) Use the **exit** command to exit from the console and command-line interface; (2) For a Product Name-1000 device, use the **exit** command to exit from a virtual system console.

## Syntax

**exit**

## Arguments

None.

## Availability

This feature is supported on all Product Name device models. However, virtual systems are only supported on the Product Name-1000.

## Examples

To log off the console:

```
ns-> exit
```

To log off the virtual system console on the Product Name-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 Product Name device.

### *Product Name-1000*

After using the **exit** command, you must log back in to the virtual system console to configure a Product Name-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** <string>

## Arguments

<a.b.c.d>                      Pings the host with IP address <a.b.c.d>

## Availability

This feature is supported on all Product Name 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 Product Name device.

## Syntax

**reset no-prompt**

**reset save-config { no [ no-prompt ] | yes [ no-prompt ] }**

## Arguments

**no-prompt**

Indicates no confirmation.

**save-config { no | yes }**

Saves the configurations:

- **no** Does not save configuration
- **yes** Saves the configurations

## Availability

This feature is supported on all Product Name device models.

## Examples

To reboot a Product Name device:

```
ns-> reset
```

---

## save

**Description:** Use the **save** command to save the Product Name 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 Product Name device. The TFTP server option is available only with firmware version 1.6 or above. The Product Name-5 device saves to the TFTP server. The Product Name-10, -100, and -1000 save to either the flash memory card or to a TFTP server.

**Product Name-100 and Product Name-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.

**Product Name-1000 only:** Use the **save vsys** command to save a single virtual system setting, or all the virtual system settings on the Product Name device to a file or to the TFTP server.

### Syntax

```
save
config [ all-virtual-system | from { flash [ append | to { flash [ append ] | slot1 <string> |
tftp <a.b.c.d> } ] | slot1 <string> | tftp <a.b.c.d> } | ha-master | to { flash [ append ] | slot1
<string> | tftp <a.b.c.d> } ]
save software { from { flash { to { flash | slot1 <string> | tftp <a.b.c.d> } } | slot1 <string> |
tftp <a.b.c.d> }
```

### Arguments

<b>config to tftp &lt;a.b.c.d&gt; &lt;filename&gt;</b>	Saves the configuration settings to a TFTP server with the IP address <a.b.c.d> and names the file <filename>.
<b>config from tftp &lt;a.b.c.d&gt; &lt;file_name&gt;</b>	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 Product Name device.
<b>config from tftp &lt;a.b.c.d&gt; &lt;file_name&gt; append</b>	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 Product Name device.
<b>software from tftp &lt;a.b.c.d&gt; &lt;file_name&gt;</b>	Downloads the software file with the name <file_name> from the TFTP server with the IP address <a.b.c.d> to the Product Name device.

---

<b>config ha-master</b>	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.
<b>config ha-slave</b>	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.
<b>save vsys</b> <b>&lt;virtual_system_name&gt; tftp</b> <b>&lt;a.b.c.d&gt; &lt;filename&gt;</b>	Applies only to Product Name-1000. This command saves the configuration settings for virtual system <b>&lt;virtual_system_name&gt;</b> to the TFTP server with an IP address <b>&lt;a.b.c.d&gt;</b> and names the configuration file <b>&lt;filename&gt;</b> .
<b>save vsys</b> <b>&lt;virtual_system_name&gt;</b> <b>&lt;filename&gt;</b>	Applies only to Product Name-1000. This command saves the configuration settings for virtual system <b>&lt;virtual_system_name&gt;</b> to a file <b>&lt;filename&gt;</b> .
<b>save all tftp &lt;a.b.c.d&gt;</b> <b>&lt;filename&gt;</b>	Applies only to Product Name-1000. This command saves the configuration settings for all virtual systems on the device to the TFTP server with an IP address <b>&lt;a.b.c.d&gt;</b> and names the configuration file <b>&lt;filename&gt;</b> .
<b>{slot1   slot2}</b>	Applies only to Product Name-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.
<b>&lt;file_name_new&gt;</b>	Applies only to Product Name-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 Product Name device models.

The **save vsys** command applies only to Product Name-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 Product Name 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 Product Name 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 Product Name-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 **save software** command.

---

# snoop

**Description:** Use the **snoop** command to display the current filter settings and review specified traffic flows.

## Syntax

```
snoop direction { both | incoming | outgoing } | ethernet { arp | vlan | <number> } | info | interface { all | trust | untrust } } | ip { dst-ip <a.b.c.d> | dst-port <number> | proto <number> | src-ip <a.b.c.d> | src-port <number> } | off ]
```

## Arguments

<b>direction { both   incoming   outgoing }</b>	Specifies the packet flow to which snoop is applied: both incoming and outgoing traffic, incoming traffic only, or outgoing traffic only.
<b>ethernet { arp   vlan   &lt;number&gt; }</b>	Specifies the 2-byte value in the ethernet header. (For an IP packet, it is 0x800.  For an ARP packet, it is 0x806.) This 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.
<b>info</b>	Displays the current filter settings.
<b>interface { all   trust   untrust   DMZ   mgt   ha }</b>	Specifies the interface traffic to which snoop is applied: <ul style="list-style-type: none"><li>• <b>all</b> Specifies all interfaces</li><li>• <b>trust</b> Specifies the trusted interface</li><li>• <b>untrust</b> Specifies the untrusted interface</li><li>• <b>DMZ</b> Specifies the DMZ interface (available on the Product Name-10, -100).</li><li>• <b>mgt</b> Specifies the mgt interface (available on the Product Name-1000).</li><li>• <b>ha</b> Specifies the ha interface (available on the Product Name-1000).</li></ul>

---

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

- **dst-ip** <a.b.c.d> Specifies the destination IP address of the packets to be snooped.
- **dst-port** <number> Specifies the destination IP port number of the packets to be snooped.
- **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.)
- **src-ip** <a.b.c.d> Specifies the source IP address of the packets to be snooped.
- **src-port** <number> Specifies the source IP port number of the packets to be snooped.

**off**

Turns off snoop by pressing the ESC key.

## Availability

This feature is available on the Product Name-5, -10, and -100 at version 2.0, and the Product Name-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
```

---

# trace-route

**Description:** Use the **trace-route** command to.

## Syntax

**trace-route**

## Arguments

None

## Availability

This feature is supported on all Product Name device models.

## Examples

```
ns-> trace-route
```



# Index

## A

- access policies
  - defining 2-85
  - displaying 3-69
- access policy 3-69
  - Incoming 3-69
  - Outgoing 3-69
- ACE Server 4-20
- ACE Server log 4-20
- address book
  - adding entries 2-3
  - entries, default 2-3
- address book entry 3-5
  - domain name 3-5
  - flag 3-5
  - IP address 3-5
  - name 3-5
  - netmask 3-5
- Address Resolution Protocol (ARP) 3-13, 3-24, 5-19
- addresses
  - entering 2-3
  - grouping 2-51, 3-40
- admin
  - get admin 4-1, 4-2
  - set admin 4-1, 4-2
  - unset admin 4-1, 4-2
- admin authentication 3-6
- administration parameters 2-5
- aggressive mode 3-45
- alarm event 3-11
  - exclude untrust 3-11
  - include trust 3-11
- alarms, clearing 4-3
- alarms, displaying 3-8
- all 3-79
- append 5-18
- arp

- set arp 4-3
- ARP (Address Resolution Protocol) table 3-13
- ARP table, clearing 4-5
- auth
  - get auth 4-6
  - set auth 4-6
  - unset auth 4-6
- authentication algorithm 3-46
- authentication table 3-14
- authentication, users 2-14
- auto-sensing 3-49

## B

- back store 3-25
- bit stream 3-25
- buffer, clearing 4-9

## C

- CA (certificate authority) 3-67
- Canonical Format Indicators (CFI) 3-101
- CheckPoint 2-61
- clear 4-1, 4-5, 4-6, 4-7
  - Address Resolution Protocol (ARP) table 4-5
  - flow counters 4-7
  - interface counters 4-7
  - user authentication information 4-6
- Clear Commands 4-1
- Clear commands 3-1
- clear commands
  - active-user 4-2
  - alarm 4-3
  - arp 4-5
  - auth 4-6
  - counter 4-7, 4-8, 4-15
  - dbuf 4-9
  - dhcp client ip 4-10, 4-12
  - file 4-13

---

ike cookie 4-14  
log 4-16  
mac-count 4-18  
mac-learn 4-19  
session 4-24  
summary 1-8

clearing alarms 4-3

command

- clear active-user 4-2
- clear alarm 4-3
- clear arp 4-5
- clear auth 4-6
- clear counter 4-7, 4-8, 4-15
- clear dbuf 4-9
- clear dhcp client ip 4-10, 4-12
- clear file 4-13
- clear ike cookie 4-14
- clear log 4-16
- clear mac-count 4-18
- clear mac-learn 4-19
- clear node\_secret 4-20
- clear session 4-24
- conventions 1-2
- enter vsys 5-2
- exec dhcp client renew 5-3, 5-4, 5-11, 5-12
- exec ha file-sync 5-5
- exec ntp 5-6
- exec pki 5-8
- exit 5-13
- get alarm 3-8
- get arp 3-13
- get auth 3-14
- get chassis 3-17
- get clock 3-18
- get config 3-19
- get console 3-21
- get counter 3-22
- get dhcp client 3-27
- get dialup-group 3-28
- get dip 3-29
- get file 3-33
- get firewall 3-35, 3-36, 3-38, 3-39, 3-51, 3-52, 3-60, 3-64, 3-66, 3-71, 3-85, 3-86, 3-87, 3-100, 3-102
- get global 3-37
- get globp 3-40
- get group 3-40
- get ha 3-42
- get hostname 3-43
- get ike 3-44
- get interface 3-47
- get log 3-53
- get mac-count 3-58
- get mac-learn 3-59
- get mip 3-63, 3-67
- get mpssess 3-62
- get ntp 3-65
- get pki 3-67
- get policy 3-69
- get route 3-72
- get sa 3-74
- get scheduler 3-77
- get service 3-79
- get session 3-81
- get snmp 3-83
- get ssh 3-78
- get syslog 3-88
- get system 3-90
- get tech-support 3-91
- get timer 3-92
- get traffic-shaping interface 3-93
- get url 3-94
- get user 3-95
- get vip 3-97
- get vpn 3-98
- get vsys 3-101
- ping 5-14
- reset 5-15
- save 5-16
- set address 2-3
- set admin 2-5
- set arp 2-12
- set auth 2-14

- 
- set clock 2-18
  - set console 2-20
  - set dhcp client 2-27
  - set dhcp server 2-29
  - set dialup-group 2-32
  - set domain 2-35
  - set envar 2-36
  - set ffilter 2-37
  - set firewall 2-39
  - set ftp data-port any 2-44
  - set global 2-46, 2-49
  - set group 2-51
  - set ha 2-54
  - set hostname 2-60
  - set ike 2-61
  - set interface 2-66
  - set mip 2-79, 2-83
  - set ntp 2-81
  - set pki 2-83
  - set policy 2-85
  - set proto-dist 2-88
  - set route 2-90
  - set scheduler 2-92
  - set service 2-94
  - set snmp 2-96
  - set ssh 2-93
  - set syn-threshold 2-98
  - set syslog 2-99
  - set timer 2-101
  - set traffic-shaping mode 2-102
  - set url 2-103
  - set user 2-106
  - set vip 2-108
  - set vpn 2-110
  - set vsys 2-113
- Commands
- Clear 4-1
  - commands 4-1, 5-2
  - communication requirements, console 1-1
  - configuration settings, saving 3-19
  - console
    - displaying configuration 3-21
    - exiting 5-13
    - log back 5-13
    - parameters, defining 2-20
  - console and command-line interface 5-13
    - exit 5-13
  - console communication requirements 1-1
  - console configuration information 3-21
    - debug messages 3-21
    - IP address 3-21
    - number of active connections 3-21
    - number of lines to display 3-21
    - timeout value 3-21
  - console parameters 3-21
  - control messages 5-16
  - conventions 1-2
  - cookie table 4-14
  - copying environment variable records 5-5
  - copying files 5-5
  - counter 4-7
    - flow 4-7
    - interface 4-7
  - counters 4-18
  - CRL file 5-8
  - current filter settings display 5-19
    - display 5-19
- D**
- debug buffer 4-9
  - default address book entries 2-3
  - Defaults 4-3
  - defining
    - a schedule 2-92
    - a static route 2-90
    - access policies 2-85
    - console parameters 2-20
    - services 2-94
    - users for authentication 2-106
- DHCP**
- client IP address, clearing 4-10, 4-12
  - client, renewing an IP address 5-3, 5-4, 5-11, 5-12



- protocol 2-29
- DHCP client 3-27, 5-3
- DHCP client lease 5-3
- DHCP server 5-3
- DHCP server IP allocation 5-3
- DHCP server pool 4-10
- DHCP server reboot 5-3
- dialup group
  - configuration parameters 3-28
  - defining 2-32
- display 3-4
- displaying
  - access policies 3-69
  - alarms 3-8
  - console configuration 3-21
  - dynamic IP settings 3-29
  - entries in the log table 3-53
  - entries in the MAC table 3-59
  - files in flash card memory 3-33
  - firewall settings 3-35, 3-36, 3-38, 3-39, 3-51, 3-52, 3-60, 3-64, 3-66, 3-71, 3-85, 3-86, 3-87, 3-100, 3-102
  - general system information 3-90
  - high availability settings 3-42
  - IKE information 3-44
  - interface settings 3-47
  - mapped IPs 3-63, 3-67
  - NetScreen-Global Manager settings 3-37
  - PKI settings 3-67
  - schedules 3-77
  - security associations 3-74
  - service entries 3-79
  - syslog configuration 3-88
  - system time 3-18
  - the hostname of the NetScreen device 3-43
  - the sessions table 3-81
  - the static route table 3-72
  - the user authentication table 3-14
  - traffic information 3-22
  - URL blocking 3-94
  - user database 3-95

- VIP settings 3-97
- VPN information 3-98
- DMZ interface 3-69
- DNS cache 4-12
- DNS entries 5-4
  - refresh 5-4
- Dynamic Host Configuration Protocol (DHCP) 4-10
- dynamic IP 3-29
- Dynamic IP (DIP) 3-24
- dynamic IP (DIP) configuration 3-29

## E

- encryption (DES or SPI) 3-15
- encryption algorithm 3-46
- encryption secret 4-20
- enter vsys command 5-2
- entries in the alarm table 4-3
- environment variable 3-32
- event alarm entries 3-8
  - at and after the time specified 3-9
  - at and before the time specified 3-9
  - detail specified 3-9
  - exclude the detail specified 3-9
  - specified alarm event 3-9
- event alarm table 4-1, 4-3
  - table 4-1
- event entries 4-16
- example 4-3
- exec dhcp client renew command 5-3, 5-4, 5-11, 5-12
- exec ha file-sync command 5-5
- exec ntp command 5-6
- exec pki command 5-8
- exit command 5-13
- Extended ping 5-14

## F

- fan 3-17
- filter source route 3-23
- filtering traffic 2-37
- firewall protection 3-35

- firewall settings, displaying 3-35, 3-36, 3-38, 3-39, 3-51, 3-52, 3-60, 3-64, 3-66, 3-71, 3-85, 3-86, 3-87, 3-100, 3-102
  - flash
    - card 4-1
  - flash card 4-1
    - clearing files 4-13
    - memory 3-33
  - flash card memory 3-33, 4-13, 5-16
  - flash memory 3-19
  - flow counters 4-7
  - flow level 3-23
  - flow-level counters 3-23
  - flow-level counters, system information 3-23
  - flow-level inspection 4-7
- G**
- general information, displaying 3-90
  - get 3-4, 3-5
  - get admin 4-1
  - get admin command 3-5
    - display system administration parameters 3-5
  - get alarm command 3-8
    - display alarm entries 3-8
  - get arp 4-3
  - get auth 4-6
  - Get commands 3-1
    - display data on the console 3-1
    - display system configuration parameters 3-1
    - redirect the output of a Get command 3-3
  - get commands
    - alarm 3-8
    - arp 3-13
    - auth 3-14
    - chassis 3-17
    - clock 3-18
    - config 3-19
    - console 3-21
    - counter 3-22
    - dhcp client 3-27
    - dialup-group 3-28
    - dip 3-29
    - file 3-33
    - firewall 3-35, 3-36, 3-38, 3-39, 3-51, 3-52, 3-60, 3-64, 3-66, 3-71, 3-85, 3-86, 3-87, 3-100, 3-102
    - global 3-37
    - group 3-40
    - ha 3-42
    - hostname 3-43
    - ike 3-44
    - interface 3-47
    - log 3-53
    - mac-count 3-58
    - mac-learn 3-59
    - mip 3-63, 3-67
    - mpsess 3-62
    - ntp 3-65
    - pki 3-67
    - policy 3-69
    - route 3-72
    - sa 3-74
    - scheduler 3-77
    - service 3-79
    - session 3-81
    - snmp 3-83
    - ssh 3-78
    - summary 1-6
    - syslog 3-88
    - system 3-90
    - tech-support 3-91
    - timer 3-92
    - traffic-shaping interface 3-93
    - url 3-94
    - user 3-95
    - vip 3-97
    - vpn 3-98
    - vsys 3-101
  - grouping
    - addresses 2-51, 3-40
    - remote users 2-32
    - services 2-51, 3-40

---

## H

### high availability

- defining a group 2-54

- displaying 3-42

### high-availability (HA) 4-7

### hostname 2-60

## I

### id-mode 2-61

### IKE (Internet Key Exchange) 2-61

### IKE cookie table 4-14

### IKE cookie table, clearing 4-14

### IKE information, displaying 3-44

### inactive SA 3-25

### include trust 3-11

### incoming/outgoing SA pairs statistics 3-75

- Algorithm 3-75

- Auth-Fail 3-75

- Fragment 3-75

- Gateway 3-75

- ID 3-75

- Life (Kb) 3-75

- Life (sec) 3-75

- Link 3-75

- Other 3-75

- PID 3-75

- SPI 3-75

- Status 3-75

- Total Bytes 3-75

### in-short error 3-25

### interface 3-4

- DMZ 3-4

- trusted 3-4

- untrusted 3-4

### interface counter 4-7

### interface settings, displaying 3-47

### interface traffic 5-19

- all 5-19

- DMZ 5-19

- ha 5-19

- mgt 5-19

- trust 5-19

- untrust 5-19

### interface-level counters 3-25

### interface-level counters, traffic information 3-25

### internal database 3-6

### Internet Control Message Protocol (ICMP) 3-23

### Internet Key Exchange (IKE) 3-44, 4-14

### IP pools 3-50

### IPSec security associations (SA) 3-74

## K

### key lifesize 3-46

### key lifetime 3-46

## L

### LDAP server 3-68

### log entries 4-16

### log table 4-1

- table 4-1

### log table, displaying 3-53

### logical interface 3-48

### logs, clearing 4-16

## M

### MAC address 3-13

### MAC learning table 4-19

### MAC table

- clearing 4-19

- displaying 3-59

### main mode 3-45

### manual VPN 3-74

### Mapped IP (MIP) 3-63

### mapped IPs

- creating 2-79

- displaying 3-63, 3-67

### Master unit 5-17

### Media Access Control (MAC) 3-24, 4-19

### memory allocation status 3-61

### memory usage status 3-61

MIPs 5-14  
 miscellaneous commands 5-1  
 miscellaneous commands, summary 1-9

**N**

NAT vector error 3-24  
 netmask 3-49  
 NetScreen device  
   displaying hostname 3-43  
   setting the hostname 2-60  
 NetScreen-1000 Switching board 4-18  
 NetScreen-Global Manager 3-37  
   displaying settings 3-37  
   enabling 2-46, 2-49  
 Network Address Translation (NAT) 3-24  
 network connection check 5-14  
   ping 5-14  
 Network Time Protocol (NTP) 3-65, 5-6  
 network traffic 3-13  
 node secret 4-20  
 nonvolatile memory 4-20  
 NTP 5-6

**O**

overwrite 5-18

**P**

packet counters 4-18  
 packet errors 3-23  
 packets 3-23  
   Address Resolution Protocol (ARP) 3-24  
   address spoofing attack 3-23  
   collision 3-25  
   Control Message Protocol (ICMP) 3-23  
   denied 3-24  
   dropped 3-23, 3-24  
   fragmented 3-23  
   illegal 3-25  
   incoming 3-25  
   Internet Control Message Protocol (ICMP) 3-25

IPSec 3-25  
 land attack 3-24  
 Network Address Translation (NAT) 3-24  
 ping-of-death attack 3-23  
 Point to Point Tunneling Protocol (PPTP) 3-24  
   received 3-25  
   transmitted underrun 3-25  
   UNKNOWN 3-26  
   unreceivable 3-25  
   unroutable 3-24  
 parent connection 3-24  
 PCMCIA card 3-19, 5-18  
 PCMCIA cards 3-33  
 physical interface 3-23, 3-48  
 ping command 5-14  
 PKI 2-83, 3-67  
 Point to Point Tunneling Protocol (PPTP) 3-24  
   policy 4-3  
   pool of IP addresses 4-10  
   power supply 3-17  
 PPPoE connection 5-9  
   set up 5-9  
   take down 5-9  
 PPPoE statistical registers 4-21  
 preshared key 3-45  
 Processing 3-17  
   board slot activity 3-17  
   board slot occupation 3-17  
   fan 3-17  
   power supply 3-17  
   temperature 3-17

Protocol  
   Address Resolution protocol 4-3  
   TCP/IP 4-3

Protocols 4-1  
 PSA key pair generation 5-8  
 pseudo port allocation 3-62  
 public-key infrastructure (PKI) 5-8

**R**

RADIUS server 3-6

- reboot NetScreen device 5-15
    - reset 5-15
  - remote administrators
    - administrator 4-1
  - remote gateway 3-45
  - remove 4-2, 4-3
    - all entries from the event alarm table 4-3
    - all entries from traffic alarm table 4-3
    - data stored in log tables 4-1
    - information stored in memory 4-1
    - information stored on the flash card 4-1
    - remote administrator profile 4-2
  - renewing the lease 5-3
  - reset command 5-15
  - resetting a device 5-15
  - root system 3-19
  - RSA key length 3-67
  - RSA key pair generation 5-8
- S**
- SA policy 3-25
  - save command 5-16
  - saving a configuration file 5-16
  - schedule
    - creating or modifying 2-92
    - displaying 3-77
  - secure command shell 3-78
  - secure shell 2-93, 3-78
  - SecurID server 3-14
  - SecurID, resetting communication 4-20
  - Security Association (SA) 4-22
  - Security Associations (SA) 3-25
  - security associations, displaying 3-74
  - self-log entries 4-16
  - server 3-6
    - LDAP 3-6
    - RADIUS 3-6
    - SecurID 3-14
  - server configuration port 3-37
  - server reporting port 3-37
  - service 3-79
    - groups 3-79
    - pre-defined 3-79
    - specific 3-79
    - user-defined 3-79
  - service entries, displaying 3-79
  - Services
    - grouping 2-51, 3-40
  - services
    - creating custom 2-94
  - session allocation status 3-62
  - Session table
    - clearing 4-24
    - displaying 3-81
  - session table, entries 3-81
  - session-related slot 3-62
  - set commands
    - address 2-3
    - admin 2-5
    - arp 2-12
    - auth 2-14
    - clock 2-18
    - console 2-20
    - dhcp client 2-27
    - dhcp server 2-29
    - dialup-group 2-32
    - domain 2-35
    - envar 2-36
    - ffilter 2-37
    - firewall 2-39
    - ftp data-port any 2-44
    - global 2-46, 2-49
    - group 2-51
    - ha 2-54
    - hostname 2-60
    - ike 2-61
    - interface 2-66
    - mip 2-79, 2-83
    - ntp 2-81
    - pki 2-83
    - policy 2-85
    - proto-dist 2-88

- route 2-90
  - scheduler 2-92
  - service 2-94
  - snmp 2-96
  - ssh 2-93
  - summary 1-4
  - syn-threshold 2-98
  - syslog 2-99
  - timer 2-101
  - traffic-shaping mode 2-102
  - url 2-103
  - user 2-106
  - vip 2-108
  - vpn 2-110
  - vsys 2-113
  - set interface tunnel/<number> 2-68
  - set interface untrust dhcp 2-27
  - setting system time 2-18
  - shared secret 3-15
  - Simple Network Management Protocol (SNMP) 3-83
  - single virtual system 5-16
  - Slave unit 5-16
  - Slave unit console 5-17
  - SNMP
    - displaying configuration 3-83
    - enabling 2-96
  - snoop 5-20
    - all outgoing packets 5-20
    - all packets 5-20
    - ARP packets 5-20
    - TCP traffic 5-20
  - SNTP 2-81
  - source route 3-23
  - starting the terminal emulator 1-2
  - static route table 3-72
  - static route table, displaying 3-72
  - static route, defining 2-90
  - sub interface 3-23
  - subnet 3-45
  - subnet mask 3-63
  - summary
    - Clear commands 1-8
    - Get commands 1-6
    - miscellaneous commands 1-9
    - Set and Unset commands 1-4
  - switching board 3-58
  - syn flood protection 3-24
  - synchronizing 5-6
  - Syslog 2-99
    - syslog configuration 3-88
    - syslog configuration, displaying 3-88
    - syslog mechanism 3-88
    - syslog server 3-88
  - system administration configuration parameters 3-6
    - addresses for the recipients of e-mail alerts 3-6
    - configuration format 3-7
    - domain name 3-6
    - e-mail alert status 3-6
    - e-mail server IP address 3-6
    - port number for Web management 3-6
    - remote e-mail address 3-6
    - status for including the traffic logs 3-7
    - system IP address 3-6
  - system time
    - displaying 3-18
    - setting 2-18
- T**
- table
    - session table 4-1
  - TCP proxy 3-24
  - TCP/IP protocol 5-19
  - TCP/IP
    - Protocols 4-1
  - Telnet connection 3-21
  - Telnet protocol 3-49
  - temperature 3-17
  - terminal emulator, starting 1-2
  - TFTP server 3-19, 5-8
  - tftp server 3-3
  - timer settings 3-92
  - traffic 4-3

---

traffic alarm entries 3-9

- access policies 3-10
- at and after the time specified 3-10
- at and before the time specified 3-10
- direction specified 3-10
- IP address specified 3-10
- policy specified 3-9
- service specified 3-9

traffic alarm table 4-1, 4-3

- table 4-1

traffic entries 4-16

traffic flows 5-19

traffic information 3-22

traffic information, displaying 3-22

traffic management information 3-93

traffic, filtering 2-37

traffic-shaping interface 3-93

Transparent mode 3-59, 4-19

Trivial File Transfer Protocol (TFTP) 3-19, 5-16

troubleshooting 3-91

trusted interface 3-48

tunnel interface 3-48, 3-49

## U

unset admin 4-1

unset arp 4-3

unset auth 4-6

unset interface 3-49

untrusted interface 4-10

updating NetScreen device clock 5-6

URL blocking

- displaying 3-94
- enabling 2-103

URL blocking configuration 3-94

user authentication

- clearing 4-6
- creating entries 2-14

- displaying table 3-14
- user authentication configuration settings 3-14
- user authentication information 4-6
- user database, displaying 3-95
- users, creating 2-106

## V

VIP (virtual IP) 2-108

VIP settings, displaying 3-97

virtual interface 3-49

Virtual IP (VIP) 3-97

Virtual Private Network (VPN) 3-98

virtual system 3-12, 5-2

- creating 2-113
- displaying 3-101
- entering 5-2
- exiting 5-13

virtual system command

- command 5-2
- enter vsys 5-2

virtual system console 5-13

- exit 5-13
- log off 5-13

VPN (Virtual Private Network) 2-110

VPN encryption 3-37

VPN information, displaying 3-98

VPN policies 3-74

## W

Web management interface 3-49

WebSense server 3-88

WebTrends 2-103

WebTrends server 3-89

## X

X.509 certificate requests 5-8