NETSCREEN-500
Installer's Guide

Version 2.6.x and 3.0.x P/N 093-0199-000 Rev. A

Copyright Notice

Copyright © 1998-2001 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 and software provided to you with the NetScreen product, and includes any accompanying documentation, any updates and enhancements of the Firmware and software 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 and software in accordance with the terms set forth in this License Agreement. The Firmware and software are "in use" on the product when they are 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 software or accompanying documentation in any form to any person; or (c) remove any proprietary notice, labels, or marks on the Firmware, software, documentation, and containers.

3.Transfer. You may transfer (not rent or lease) the Firmware or software 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, software, documentation, and any copy made by you remain with NetScreen. You acknowledge that no title to the intellectual property in the Firmware and software 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 and software. 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.

6. 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.

10. Tax Liability. You agree to be responsible for the payment of any sales or use taxes imposed at any time whatsoever on this transaction.

11. General. If any provisions of this Agreement are held invalid, the remainder shall continue in full force and effect. The laws of the State of California, excluding the application of its conflicts of law rules shall govern this License Agreement. This Agreement will not be governed by the United Nations Convention on the Contracts for the International Sale of Goods. This Agreement is the entire agreement between the parties as to the subject matter hereof and supersedes any other Technologies, advertisements, or understandings with respect to the Firmware and documentation. This Agreement may not be modified or altered, except by written amendment, which expressly refers to this Agreement and which, is duly executed by both parties.

You acknowledge that you have read this Agreement, understand, it, and agree to be bound by its terms and conditions.

Hardware, including technical data, is subject to U.S. export laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. Customer agrees to comply strictly with all such regulations and acknowledges that it has the responsibility to obtain licensed to export, re-export, or import hardware.

NetScreen is a trademark belonging to NetScreen Technologies, Inc. All other product names mentioned in this manual are trademarks or registered trademarks of their respective manufacturers.

Contents

Manual Organization x

Related Publications xi

Conventions xii
- WebUI Conventions xii
- CLI Conventions xiii
  - Keyboard Shortcuts xiv
- Menu System Conventions xv

Chapter 1 Hardware Description 1-1

Front Panel 1-1
- LCD and Control Pad 1-2
- LED Dashboard 1-3
- Interface Modules 1-6
  - Position Determines Function 7
- PCMCIA 1-8
- Management Interfaces 1-8
- High Availability Interfaces 1-9

Rear Panel 1-9

Chapter 2 Hardware Installation and Replacement 2-1

Installing the Interface Modules 2-2
- Labeling the Interface Modules 2-2
- Inserting Interface Modules 2-3
- Removing Interface Modules 2-6

Mounting the NetScreen-500 2-8
- Front Mount 2-9
- Mid Mount 2-10
- Rear and Front Mount 2-11

Replacing the Fan Assembly 2-13

Power Supplies 2-15
- Wiring the DC Power Supplies 2-16
- Replacing an AC Power Supply 2-18
- Replacing a DC Power Supply 2-20

Chapter 3 Connecting to the Network 3-1

Connecting the NetScreen-500 as a Singe Security Appliance 3-2

Connecting the NetScreen-500 for High Availability 3-4

Chapter 4 Initial Configuration 4-1

Configuring via the WebUI 4-3
Logging On and Setting the System IP Address 4-3
Setting Interface Addresses 4-5
Allowing Outbound Traffic 4-7
Changing Your Login Name and Password 4-8
Testing the Configuration 4-8

Configuring via the CLI 4-9
Logging On and Setting the System IP Address 4-10
Setting Interface Addresses 4-10
Allowing Outbound Traffic 4-11
Changing Your Login Name and Password 4-11
Testing the Configuration 4-11

Configuring via the Menu System 4-12
Setting the System IP Address 4-12
Setting Interface Addresses 4-13

High Availability 4-15
Configuring HA via the WebUI 4-16
Configuring HA via the CLI 4-18

Resetting the Device to the Factory Default Settings 4-19

Appendix A Menu System A-1

1. Setting A-2
11. Admin A-2
12. Interface A-6
13. Time/Date A-9
14. Audible Alarm A-11
15. Temp Threshold A-12
16. LCD Display A-14

2. Status A-15
21. Utilization A-15
22. Temperature A-17
23. Version A-18

3. Alarm A-19
31. View A-19
32. Clear All A-19

4. PCMCIA A-20
41. Save A-20

5. Reset A-21
51. Save & Reset A-21
52. Unsave & Reset A-21
6. Exit A-22

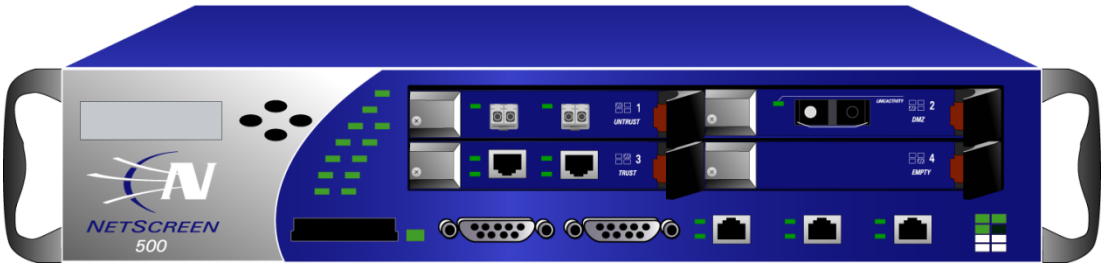
Appendix B Safety Recommendations and Warnings B-1

Safety Recommendations and Warnings B-1
General Guidelines B-1
Important Warnings B-1
Before Supplying Power B-2
No User-Serviceable Parts Warning B-2
Product Disposal Warning B-2
Power Disconnection Warning B-2
Circuit Breaker (15A) Warning B-2
SELV Circuit Warning B-3
Lightning Warning B-3
General Site Requirements B-3
Site Environment B-3
Configuring Equipment Racks B-4
Power Supply Considerations B-4
Environmental Requirements in an Office Environment B-5
BSMI Labeling Requirement B-5

Index IX-1

Preface

The NetScreen-500 is a network security device that protects your Ethernet local area network (LAN) when connecting to the Internet. Using a NetScreen-500 firewall and VPN allows you to control inbound and outbound access to and from your protected LAN.



This manual provides NetScreen-500 users with a guide to perform the following tasks:

- Installing and replacing hardware components
- Rack mounting the device
- Cabling the device to the network and, optionally, to another NetScreen-500 device in a high availability configuration
- Creating a basic configuration that defines the following parameters:
  - Operational mode: Transparent, Network Address Translation (NAT), or Route
  - Interface and management IP addresses
  - Admin login names and passwords
  - A basic outgoing access policy
  - High availability settings

In addition, this manual describes all of the NetScreen-500 hardware features, thoroughly examines the menu system—accessible through the LCD and control pad on the front panel—and lists safety recommendations, warnings, and site requirements.

FIPS Certification Note: *For information on NetScreen compliance with Federal Information Processing Standards (FIPS) and for instructions on setting a FIPS-compliant NetScreen-500 device in FIPS mode, see the* NetScreen-500 Cryptographic Module Security Policy *on the documentation CD-ROM.*

MANUAL ORGANIZATION

This section outlines the chapters and summarizes their content.

Chapter 1,"Hardware Description", details the physical structure of the NetScreen-500 device. It identifies and explains the elements on the front and rear panels of the device and the interface modules.

Chapter 2,"Hardware Installation and Replacement" explains how to install the traffic module cards, rack mount the NetScreen-500, and replace the fan assembly and power supplies.

Chapter 3,"Connecting to the Network", includes diagrams that show the typical placement of the NetScreen device between your network and the Internet, and a summary of the tools and information necessary to connect the device.

Chapter 4,"Initial Configuration", explains how to configure the basic functions of the NetScreen-500 and provides the default user name and password. The chapter also explains how to set up a basic Access Policy, and details a method to ensure that your device is working correctly on the network.

Appendix A, "Menu System", presents an overview of the entire menu system available through the LCD.

Appendix B, "Safety Recommendations and Warnings", provides safety warnings concerning installation environment, power, and cabling. It also includes general cautions when using the NetScreen-500 device.

RELATED PUBLICATIONS

The following publications are included on the documentation CD included with the NetScreen-500:

- **NetScreen Concepts & Examples ScreenOS Reference Guide**: A guide to the ScreenOS™ used to manage the NetScreen-5, -10, -100, -500, and -1000. This guide presents the concepts behind NetScreen product features, and provides examples to illustrate those concepts in practice.
- **NetScreen WebUI Reference Guide**: A thorough examination of the NetScreen Web user interface (WebUI). This guide provides descriptions of all the features on the WebUI for the NetScreen-5, -10, -100, -500, and -1000.
- **NetScreen CLI Reference Guide**: A compendium of all the command line interface (CLI) commands. For each command, the complete syntax is presented, its arguments explained, and examples provided.
- **NetScreen-500 Release Notes**: A set of notes containing an overview of new features, lists of addressed issues and known issues, and suggested bug fixes and work-arounds.
- **NetScreen-500 Cryptographic Module Security Policy**: A description of NetScreen-500 conformity to FIPS regulations and the functions affected by operation in FIPS mode.

If you plan to administer NetScreen-500 unit(s) remotely, and have purchased the NetScreen-Global Manager™ version 2.6.0, refer to the following:

- **NetScreen-Global Manager User's Guide**: A manual for installing and using the NetScreen-Global Manager software. NetScreen-Global Manager is software enabling centralized management of NetScreen devices.

If you use NetScreen-Remote clients to allow users to connect to the corporate network via IPSec VPN tunnels, read the following:

- **NetScreen-Remote Administrator's Guide**: A manual for installing and using the NetScreen-Remote software. NetScreen-Remote allows a remote user to connect to a NetScreen security appliance via a virtual private network (VPN) tunnel.

CONVENTIONS

This book presents three management methods for configuring a NetScreen device: the Web user interface (WebUI), the command line interface (CLI), and the menu system. The conventions used for these methods are introduced below.

WebUI Conventions

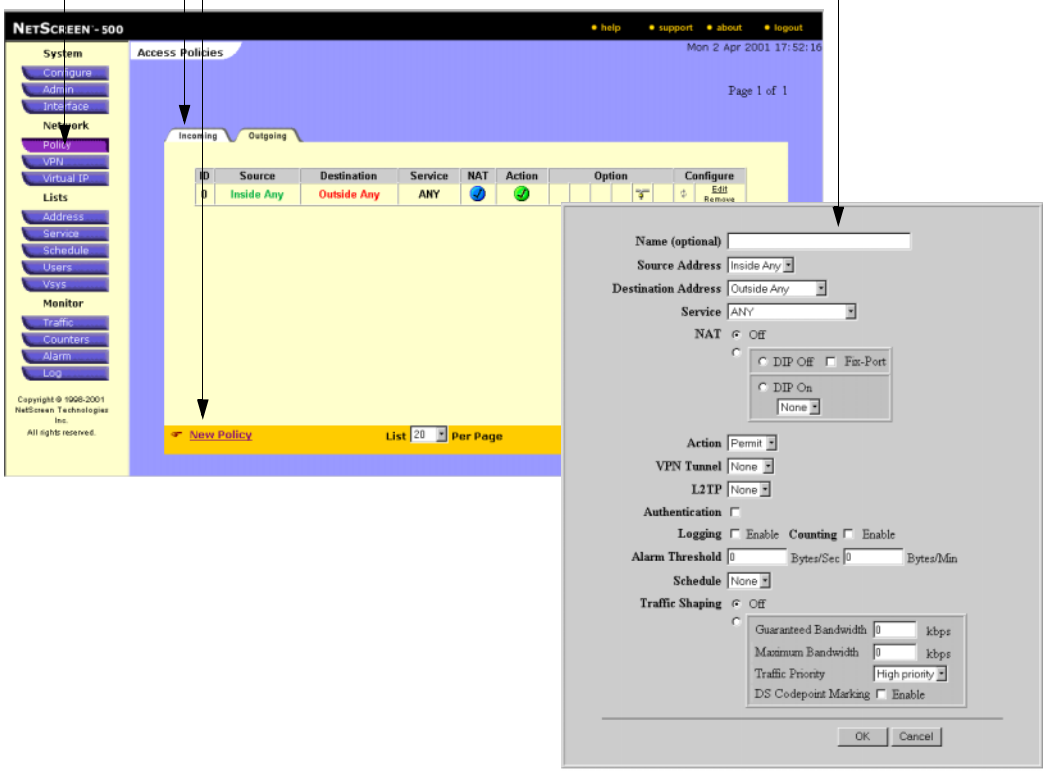
Throughout this book, a double chevron (>>) is used to indicate navigation through the WebUI by clicking buttons, tabs, and links. For example:

Policy >> Incoming >> New Policy

To access the Policy Configuration dialog box to create an incoming access policy, do the following:

1. Click the **Policy** button in the menu column.
2. Click the **Incoming** tab.
3. Click the **New Policy** link.

   The Policy Configuration dialog box appears.



CLI Conventions

The CLI conventions are as follows:

- 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, **interface { trust | untrust | dmz }** means "choose the trusted, untrusted, or DMZ interface."
- IP addresses are represented by <a.b.c.d> and <e.f.g.h>.

A subnet mask is represented by <A.B.C.D>.

For example, when entering a route to the route table for the IP address 2.2.2.2/32 via the untrusted interface, use the following syntax:

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

to produce this command:

> set route 2.2.2.2 255.255.255.255 interface untrust

Because the gateway IP address and the metric[1] are optional—these arguments are presented within brackets [ ]—you can omit them from the command. In this example, the gateway IP address would be that of a router on the untrusted side through which you want to route traffic bound for 2.2.2.2/32. By not specifying a router, the default router for the untrusted interface is used.

> ***Note:*** *When typing a key word, you only have to type enough letters to identify the word uniquely. For example, typing* ***set interf t n*** *is enough to enter the command* ***set interface trust nat****.*

If you want to see the options following part of a command, press the SPACE key and then type ? (question mark). For example, typing **set interface ?** displays the following options: trust, untrust, dmz, mgt, ha1, ha2, tunnel—which are the available options that you can enter after typing **set interface**.

1. The **metric <number>** argument specifies the number of hops between the NetScreen-500 and the specified gateway. In this example, you do not specify a gateway; consequently, you do not specify a metric for it. However, even if you do specify a gateway, specifying a metric is optional.

Keyboard Shortcuts

You can use the following keyboard shortcuts when connected to the NetScreen-500 via a console, SCS, or Telnet session.

- To remove a single character, press BACKSPACE or CTRL+H.
- To remove an entire line, press CTRL+U.
- To interrupt and stop displaying the output from a get command, press CTL+C.
- To traverse up to 16 lines backward in the command history buffer, press CTRL+B or the UP ARROW key.
- To traverse up to 16 lines forward in the command history buffer, press CTRL+F or the DOWN ARROW key.

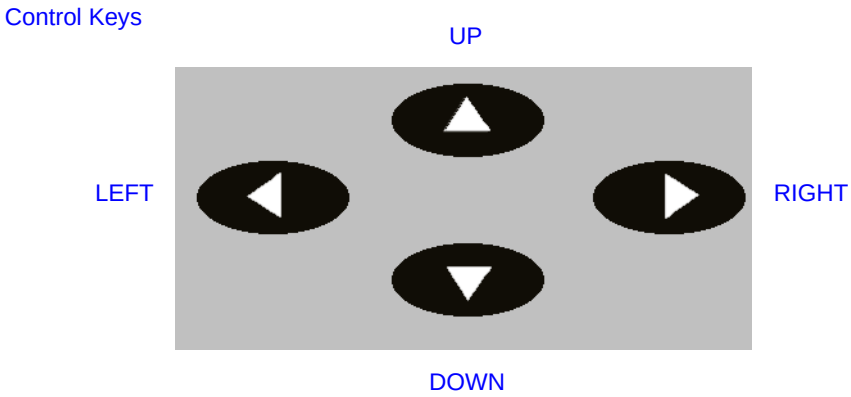
Note: *To use the arrow keys for navigating among commands in a Telnet session on Windows 95, 98, NT, or 2000: On the Terminal menu, click* ***Preferences****, select the* ***VT100 Arrows*** *check box, and click the* ***OK*** *button.*

- To see the options following part of a command and a brief description of usage, press the SPACE key and then type ? (question mark). For example, typing **set interface ?** displays the following options: trust, untrust, dmz, mgt, ha1, ha2, tunnel—which are the available options that you can enter after typing **set interface**.
- By default, the console times out and the connection is broken if no keyboard activity is detected for 10 minutes. To change the default, use the following CLI command: **set console timeout <number>**, where <number> represents the length of idle time in minutes. A value of 0 indicates that the session never times out.

For further explanation of NetScreen commands and their syntax, refer to the *NetScreen CLI Reference Guide*, which is included on the product CD.

Menu System Conventions

Similar to the navigational conventions for the WebUI, a double chevron (>>) indicates navigation through the menu system by pressing the UP, DOWN, LEFT, and RIGHT control keys to select options.



For example, **1. Setting >> 11. Admin >> 111. System Address >> 1111. System IP** means to do the following:

1. Press the RIGHT control key to select **1. Setting** on the LCD.

   The 1. Setting options appear: 11. Admin, 12. Interface, 13. Time/Date, 14. Audible Alarm, 15. Temp Threshold, 16. LCD Display.

2. Press the RIGHT control key to select **11. Admin**.

   The 11. Admin options appear: 111. System Address, 112. Admin Address, 113. Global.

3. Press the RIGHT control key again to select **111. System Address**.

   The 111. System Address options appear: 1111. System IP, 1112. Config Port.

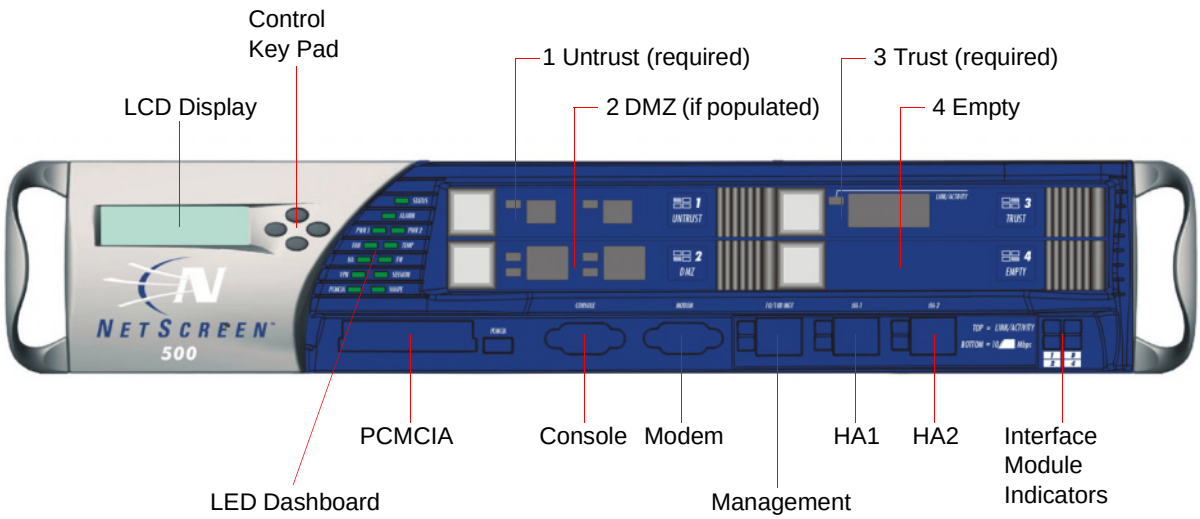
4. Press the RIGHT control key to select 1111. **System IP**.

Hardware Description 1

This chapter provides detailed illustrations and descriptions of the NetScreen-500 chassis.

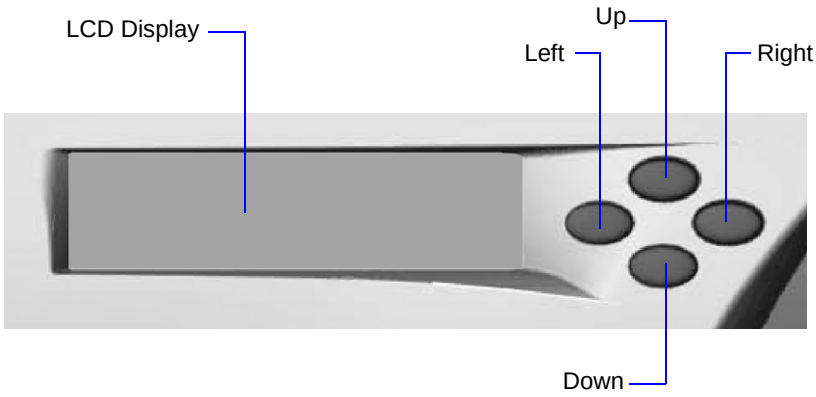
FRONT PANEL

Located at the front of the NetScreen-500 device are bays for four interface modules, various ports for management and line access, an LCD display and associated lockable key pad, and various LEDs that show the status of components, software, and traffic.



LCD and Control Pad

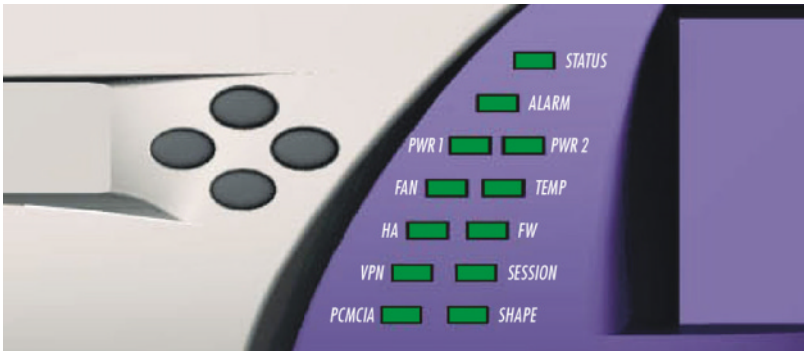
You can perform basic configurations and view status reports through the LCD and control pad. The LCD displays two lines, each line capable of displaying up to 16 characters. The control pad has four keys—up, down, left, and right—that you can use for navigating through the menu system, a hierarchically structured menu composed of configuration and data retrieval options.



Note: *For instructions on basic navigational techniques, see "Menu System Conventions" on page xv. For a complete description of the menu system, see Appendix A, "Menu System".*

LED Dashboard

The LED dashboard provides information about various critical functions.



Unless specified otherwise in the following table, all LED states are for solid, non-blinking illumination.

LED	Purpose	Color	Meaning
STATUS	System Status	**blinking amber**	Booting up normally
		blinking green	Normal operation
ALARM	System Alarm	**red**	Critical alarm—failure of hardware component or software module (such as a cryptographic algorithm)
		amber	Major alarm: • Low memory (<10% remaining) • High CPU utilization (>90%) • Log memory full • Sessions full • Maximum number of VPN tunnels reached • Firewall attacks detected • HA status changed or redundant group member not found
		green	No alarm condition present.
		dark	No alarms

LED	Purpose	Color	Meaning
PWR 1	Power Supply #1	**green**	Power supply #1 is functioning correctly.
		red	Power supply #1 failure or power bay #1 is empty.
PWR 2	Power Supply #2	**green**	Power supply #2 is functioning correctly.
		red	Power supply #2 failure or power bay #2 is empty.
FAN	Fan Status	**green**	All fans functioning properly
		red	One or more fans failed.
TEMP	Temperature	**green**	Temperature is within safety range.
		red	Temperature is outside safety range.
HA	High Availability Status	**green**	Unit is master.
		blinking green	Redundant group member cannot be found.
		amber	Unit is slave.
		dark	HA not configured
FW	Firewall Alarm	**green**	No firewall attacks
		red	Firewall event/alarm has occurred*.
VPN	VPN Activity	**blinking green**	VPN activity—encrypting/decrypting traffic
		blinking amber	VPN drops or denies traffic
		red	VPN tunnels have reached 90% of the maximum number of simultaneously active IPSec SAs.
		dark	No VPN defined or no tunnels active
SESSION	Session Utilization	**green**	Sessions are <70% utilization.
		amber	Sessions are between 70% and 90% utilization.
		red	Sessions are >90% utilization.
PCMCIA	PC Card Status	**green**	PC card is installed in PCMCIA slot.
		blinking green	PC card is active.

LED	Purpose	Color	Meaning
		red	PC card is >90% full or read/write activity has failed.
		dark	PCMCIA slot is empty.
SHAPE	Traffic Shaping	**green**	Traffic shaping in operation
		blinking green	Traffic shaping transmits packets
		blinking amber	Traffic shaping drops packets
		red	Configured guaranteed bandwidth > available interface bandwidth†
		dark	No traffic shaping configured

* To change the Alarm LED or Firewall LED from red to green but keep the alarm message(s) in the menu system, use the CLI command **clear led {alarm | firewall}**. To change the LCD to green and remove the alarm or firewall message(s), use the control keys to select **3. Alarm >> 32. Clear All >> Yes**.

† The LED changes to green when you correct the configuration.

When the NetScreen-500 is powered up, the Status LED changes from dark to blinking amber to blinking green. Start-up takes up to one minute to complete. If an error is detected, the LED glows red. The LED changes to amber when the device writes to the internal flash card.

Note: *If you want to turn the NetScreen-500 off and on again, wait a few seconds between shutting it down and powering it back up.*

Interface Modules

On the front of the NetScreen-500 are four bays for interface modules. Each interface module can have one or two ports, and each port has a pair of LEDs. There are three types of modules available:

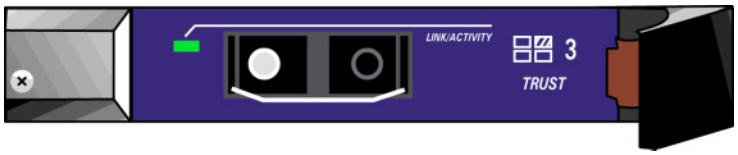
- The 10/100 Mbps module, which is appropriate for a 10BaseT or 100BaseT LAN. Connect using a twisted pair cable with RJ45 connectors. See Chapter 3, "Connecting to the Network" for cabling guidelines.
- The gigabit interface connector (GBIC) module and the mini-GBIC interface connector module, which provide connectivity to fiber-based, gigabit ethernet LANs. Connect using an optical cable with SX or LX connectors.

10/100 BaseT Dual Interface Module

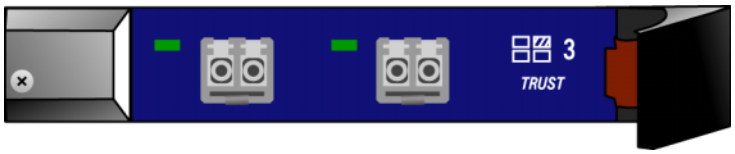
Top Status LED:
Green: Link is up, no activity
Blinking Green: Link is up and active

Bottom Status LED:
Dark: 10 Mbps line rate
Orange: 100 Mbps line rate

GBIC Single Interface Module



Mini-GBIC Dual Interface Module



Status LED:
Green: Link is up, no activity
Blinking Green: Link is up and active

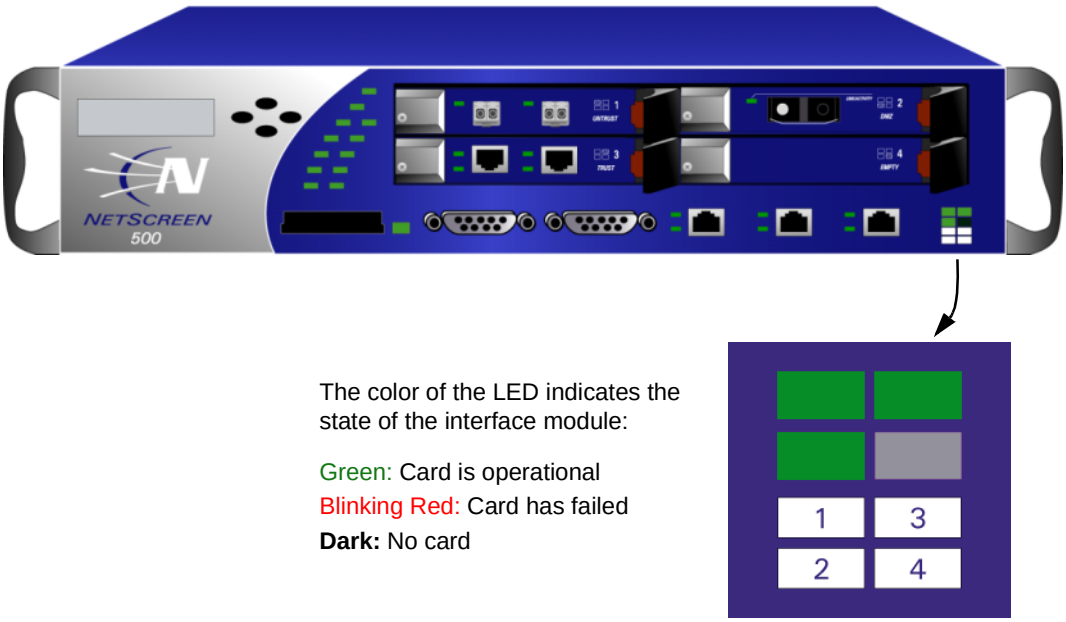
Position Determines Function

The three interface module bays determine the interface for whatever card you insert.

Bay	Interface	Type of Card
1	Untrusted	10/100 Base-T or GBIC (fiber)
2	DMZ	10/100 Base-T or GBIC (fiber)
3	Trusted	10/100 Base-T or GBIC (fiber)
4	None	Blank

You can use both 10/100 BaseT and GBIC cards simultaneously for the same NetScreen-500; there are no combination restrictions. However, the cards are not hot-swappable.

The interface module indicators, located at the lower right corner on the front of the device, are LEDs that correspond positionally to the interface modules.



The color of the LED indicates the state of the interface module:

Green: Card is operational

Blinking Red: Card has failed

Dark: No card

PCMCIA

You can insert a type I, II, or III SanDisk® ATA PC card in the PCMCIA slot to download or upload either the system software or a configuration. Use the following CLI command:

save { software | config } from { slot1 | flash } <file_name> to { flash | slot1} <file_name>

where slot1 refers to the PCMCIA slot and flash refers to the internal flash memory.

Note: *For more information on the* ***save*** *command, see the* NetScreen CLI Reference Guide.

Management Interfaces

The NetScreen-500 offers three management interfaces:

Port	Description
Console	DB-9 serial port for local configuration and administration via the CLI. This cables to the serial port of the administrator's workstation using a DB-9 female to DB-9 male straight-through serial cable.
Modem	DB-9 serial port for connecting to a modem, allowing the user to control the device remotely*.
10/100 MGT	This management port has a fixed 10/100 Base-T interface and provides a dedicated connection for management traffic. It has a separate IP address and netmask, configurable via the CLI or WebUI. ***Important:*** *Do not connect user's data traffic to this interface.*

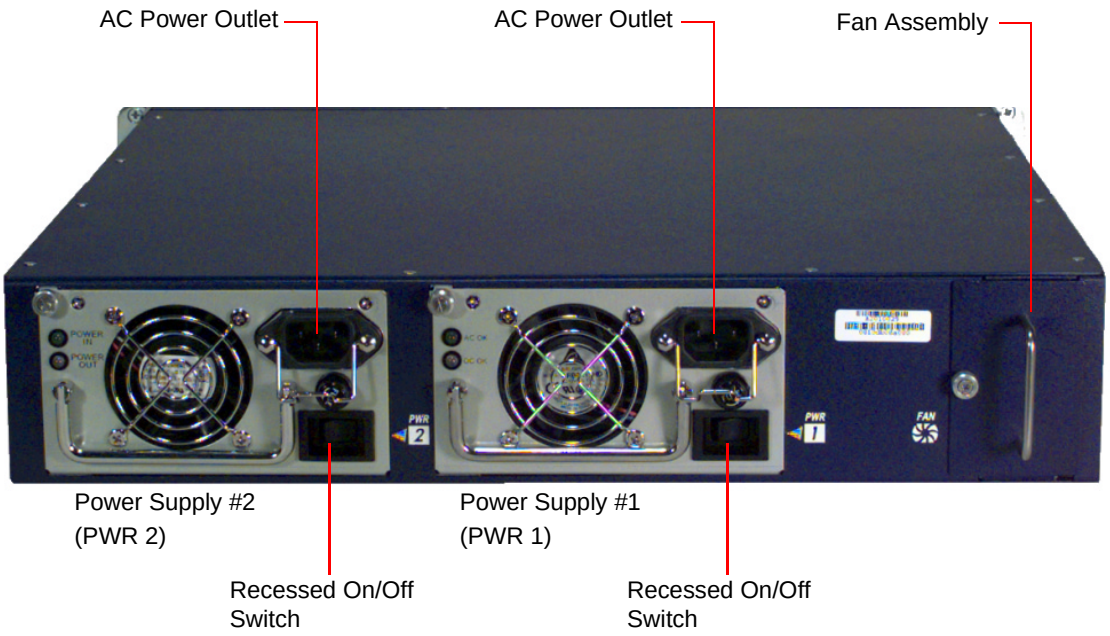
* For security reasons, NetScreen recommends using a modem for troubleshooting or a one-time configuration only, not for regular remote administration.

High Availability Interfaces

The NetScreen-500 has two 10/100 BaseT physical ports dedicated for high availability (HA) traffic: HA-1 and HA-2. You can link two NetScreen-500 devices together in a redundant group, with one device acting as the master unit and the other as the slave unit. The two HA links provide redundancy. In the event that the main link (HA-1) fails, the second link (HA-2) takes over HA communications. For information on cabling for HA, see "Connecting the NetScreen-500 for High Availability" on page 3-4.

REAR PANEL

The back panel of the NetScreen-500 is where the access to the power supplies, on/off switch, and fan assembly is located.



Power Supplies: The NetScreen-500 supports dual, redundant, fault-tolerant, auto-switching power supplies which may be replaced one at a time without interrupting the unit's operation (are "hot-swappable"). For information on replacing a power supply, see "Power Supplies" on page 2-15.

The power supplies are monitored by management software and can generate system alarms and set SNMP traps.

AC Power Input: There is one AC outlet for each power supply. Use the outlets to connect power to the NetScreen-500 with the supplied power cables.

Note: *You can order a NetScreen-500 device that runs on DC power. On DC-powered units, there are two screws for terminating power cables for each power supply.*

On/Off Switch: This switch turns the power to the NetScreen-500 on and off.

Fan Assembly: The fan assembly is a single unit comprised of four fans. The fan assembly must be replaced only in the event of failure, indicated when the FAN LED on the LED dashboard glows red and an event alarm and SNMP trap are triggered. Although the device can operate with only two of the four fans running, there is a serious risk of overheating, again indicated when the TEMP LED glows red.

Note: *If the power supplies become too hot, the system shuts down automatically. For a description of replacing the fan assembly, see* *"Replacing the Fan Assembly" on page 2-13*.

2 Hardware Installation and Replacement

Follow the instructions in this chapter to install the interface modules and rack-mount the NetScreen-500 hardware.

- "Installing the Interface Modules" on page 2-2
  - "Labeling the Interface Modules" on page 2-2
  - "Inserting Interface Modules" on page 2-3
  - "Removing Interface Modules" on page 2-6
- "Mounting the NetScreen-500" on page 2-8
  - "Front Mount" on page 2-9
  - "Mid Mount" on page 2-10
  - "Rear and Front Mount" on page 2-11

This chapter also explains the following procedures:

- "Replacing the Fan Assembly" on page 2-13
- "Wiring the DC Power Supplies" on page 2-16
- "Replacing an AC Power Supply" on page 2-18
- "Replacing a DC Power Supply" on page 2-20

INSTALLING THE INTERFACE MODULES

The NetScreen-500 ships with the interface modules packaged separately from the chassis. This allows you to install the 10/100 BaseT cards and GigaBit Interface Connector (GBIC) cards in the combination and arrangement to suit your network needs.

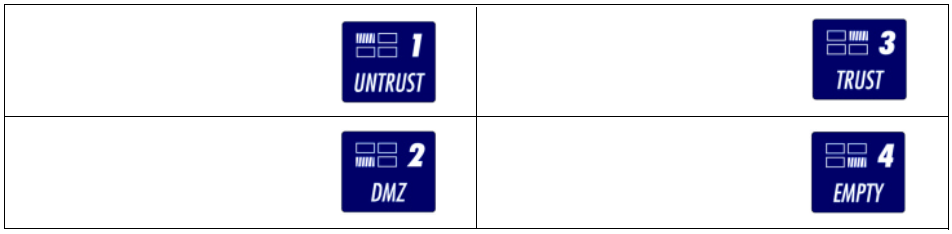
Labeling the Interface Modules

Before inserting the interface modules in the bays, determine the types of card (10/100BaseT or GBIC) that you want to use for the untrusted interface and the trusted and/or DMZ interfaces. Use the enclosed labels to designate into which bay you are going to insert each card.

1. Remove the interface modules from the antistatic bags in which they ship.
2. Affix the enclosed labels on the cards.

Note: *On the front right corner of each interface module, you can see two white L-shaped marks. You can use these marks as a guide for placing the labels.*

The striped rectangle and the number indicate which bay you plan to insert each card, as shown below.



For ScreenOS 2.6.x and 3.0.x, the interface modules must go in the following bays:

- Bay 1: Untrusted interface module (required)
- Bay 2: DMZ interface module (optional)
- Bay 3: Trusted interface module (required)
- Bay 4: Blank card

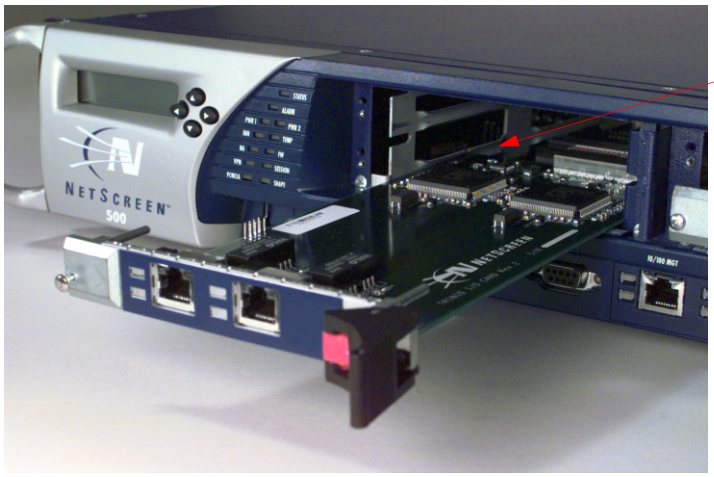
Note: *Because the fourth bay is not functional in ScreenOS 2.6.x and 3.0.x releases, the NetScreen-500 ships with a blank card loaded in bay 4. If you order cards for only two interfaces, you must install them in bays 1 and 3 and install a second blank card, which is included, in bay 2.*

Inserting Interface Modules

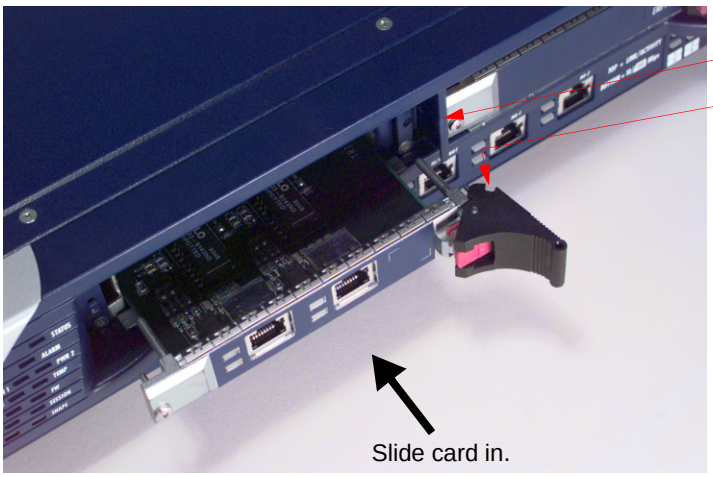
You can insert interface modules in the bays in any order. Use the following procedure for inserting each card.

Caution *When inserting or removing interface modules, be sure that the power is off.*

1. Align the side edges of the card with the grooves in the side walls of the bay.



2. Slide the card in until the groove in the black latch contacts the ridge at the outermost edge of the right bay wall.



Caution *When inserting and removing a card in bay 2 (that is, the lower left bay), take care that the electromagnetic interference (EMI) fingers spread along the top edge of the front wall of the interface module do not catch on the lower edge of a card above it in bay 1 (the upper left bay).*

3. With your left thumb, push on the front left corner while, with your right thumb, you push the latch away from yourself and slightly toward your left until the red locking tab clicks into place. (If you push the latch before it contacts the ridge on the bay wall, the locking tab clicks into place prematurely and you will not be able to seat the interface module properly.)

4. Using a Phillips screwdriver, screw in the captive screw on the front left corner.

Removing Interface Modules

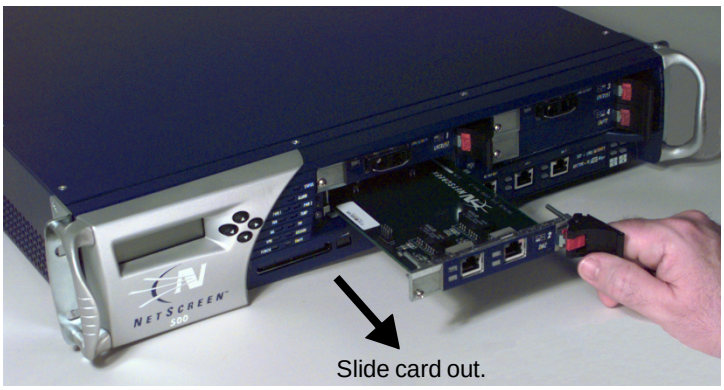
To remove a interface module from a bay, do the following.

Caution *When inserting or removing interface modules, be sure that the power is off.*

1. Using a Phillips screwdriver, unscrew the captive screw on the front left corner of the interface module.
2. Push the red locking tab to the right, releasing the black latch.

3. Lever the latch to the right, popping the card free.

4. Gripping the latch, slide the card straight out.



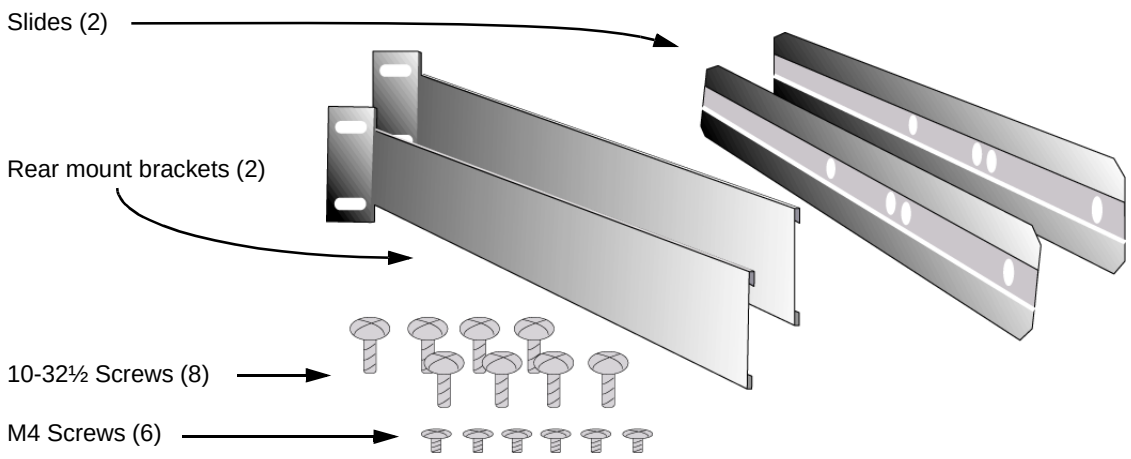
Caution *When inserting and removing a card in bay 2, take care that the electromagnetic interference (EMI) fingers spread along the top edge of the front wall of the interface module do not catch on the lower edge of a card above it in bay 1.*

MOUNTING THE NETSCREEN-500

You can place the chassis on a table top or mount it in a standard 19-inch equipment rack. Table-top installation requires no tools. Rack mounting requires the following:

- 1 Phillips-head screwdriver
- 4 screws to match the rack (if the thread size of the screws provided in the NetScreen-500 product package do not fit the thread size of the rack)
- The included rear slide mount kit (for the rear-and-front-mount method)

Rear Slide Mount Kit



There are three ways to rack-mount the NetScreen-500:

- Front mount
- Mid mount
- Rear and front mount

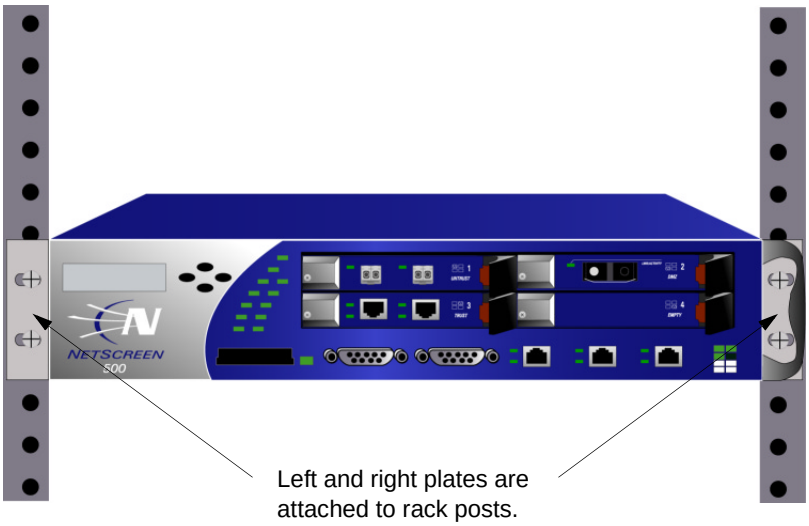
Each method for mounting the NetScreen-500 is presented below.

Front Mount

To front-mount the NetScreen-500, you need 4 screws to match the rack thread size and a screwdriver.

1. Slide the NetScreen-500 in the rack.
2. Screw the left and right plates to the rack.

Note: *If the side handles interfere with the screwdriver, you might need to remove them.*



Note: The left handle is removed to show the left plate more clearly.

Mid Mount

To mid-mount the NetScreen-500, you need 4 screws to match the rack thread size and a Phillips-head screwdriver.

1. Using the Phillips-head screwdriver remove the left and right side handles.
2. Unscrew the left and right plates, and then screw them to the middle of each side of the NetScreen-500 chassis.
3. Screw the left and right plates to the rack.

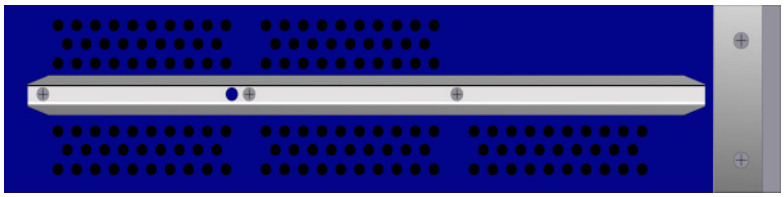
Rear and Front Mount

To mount the NetScreen-500 with support from the rear and front, use the rear slide mount kit. You also need a Phillips-head screwdriver.

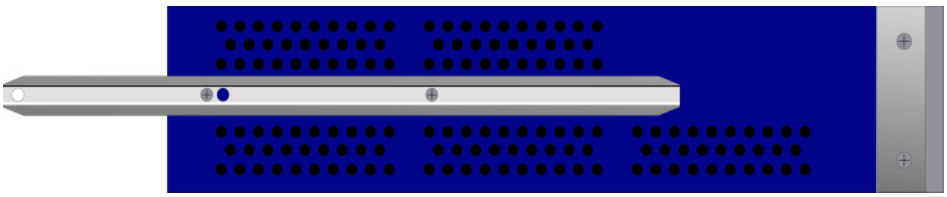
1. Screw the rear mount bracket to the rear rack posts.
2. With the indented groove that runs the length of each slide facing outward, screw the slides to the middle of each side of the NetScreen-500 chassis.

Note: *Depending on the depth of the rack, screw the slides in place either running the length of the sides or extending over the rear of the chassis.*

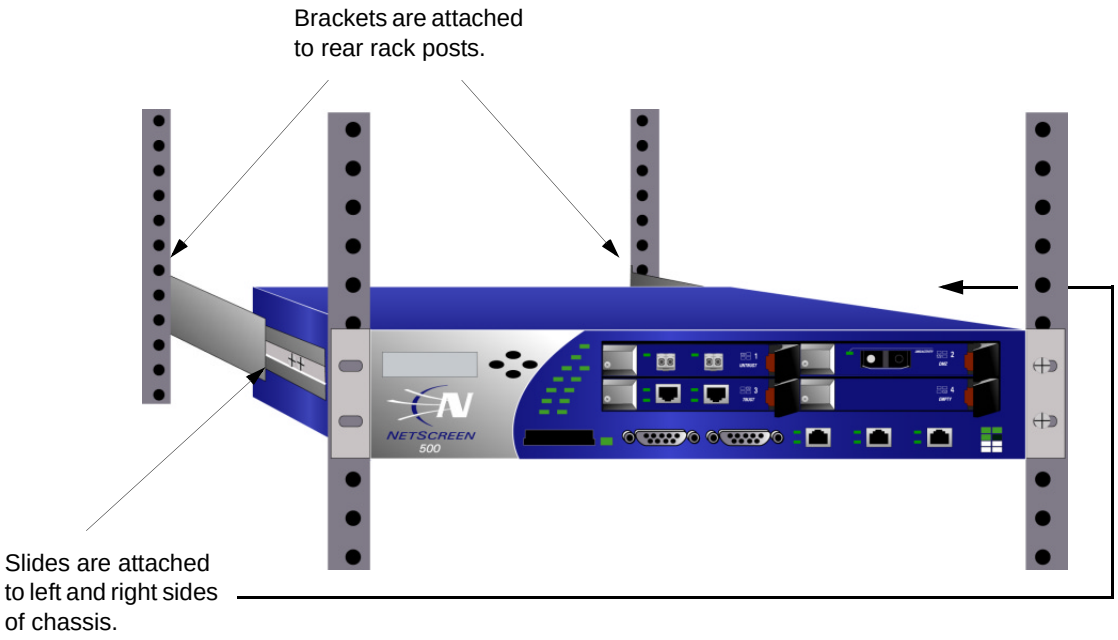
For normal rack depth, screw the slides along the length of each side.



For a deeper rack, screw the slides so that they extend beyond the rear of the chassis.



3. Slip the slides into the rear mount brackets, and push the NetScreen-500 forward until the left and right plates contact the front rack posts.
4. Screw the left and right plates to the rack.

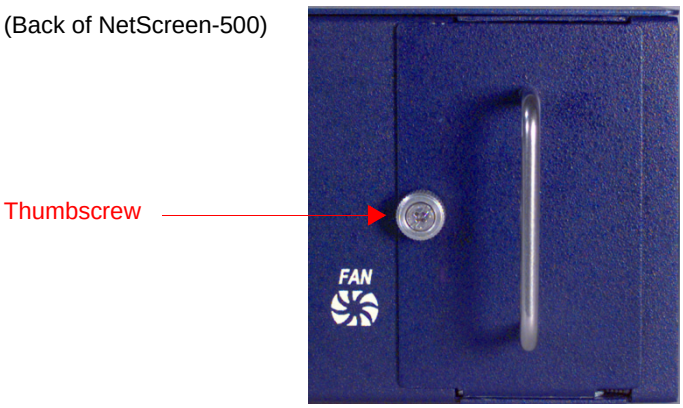


REPLACING THE FAN ASSEMBLY

You only need to replace the fan assembly in the event of failure, indicated when the FAN LED glows red (see "LED Dashboard" on page 1-3), and an event alarm and SNMP trap is triggered. Although the unit can operate with three of the four fans, there is a serious risk of overheating.

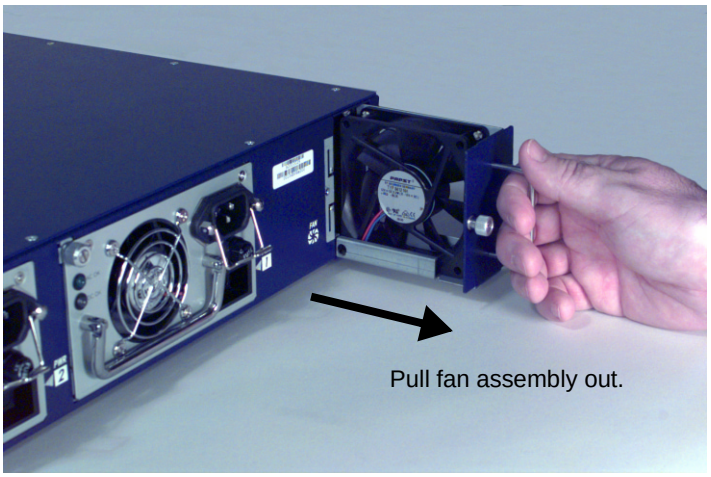
To obtain a replacement fan assembly while it is still protected under the one-year warranty, call NetScreen support. After that, contact the NetScreen sales department.

1. To remove the fan assembly, turn the captive thumbscrew counterclockwise.



2. Grip the handle and slide the assembly straight out.

Caution *Do not remove the fan assembly while the fans are still spinning.*



3. Insert the new fan assembly in the fan bay, and push it straight in.

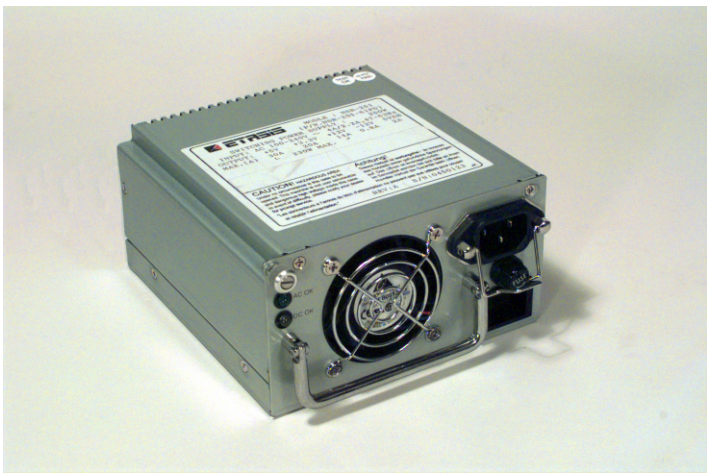
4. Secure it in place by tightening the thumbscrew clockwise.

POWER SUPPLIES

The NetScreen-500 ships with one or two AC or DC power supplies. You can specify the following voltage options:

- AC: 90-264 VAC (47 to 63 Hz)
- DC: 36-72 Volts

The NetScreen-500 power supplies share the power load equally. If one power supply fails, the other one automatically assumes the full load, and the NetScreen-500 sends a system alarm and the PWR LED for the failed power supply glows red.

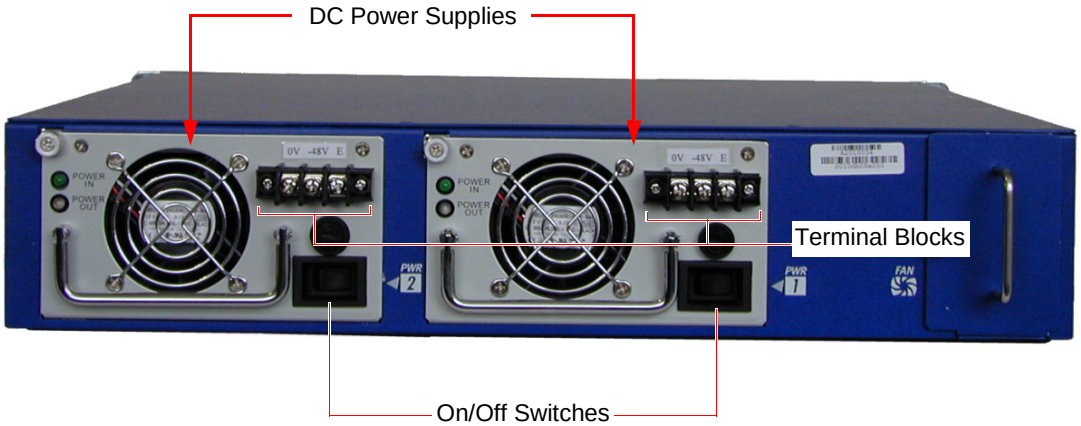


AC Power Supply

The redundant power supplies are hot-swappable. In other words, you can remove one of them and replace it without affecting operations.

Wiring the DC Power Supplies

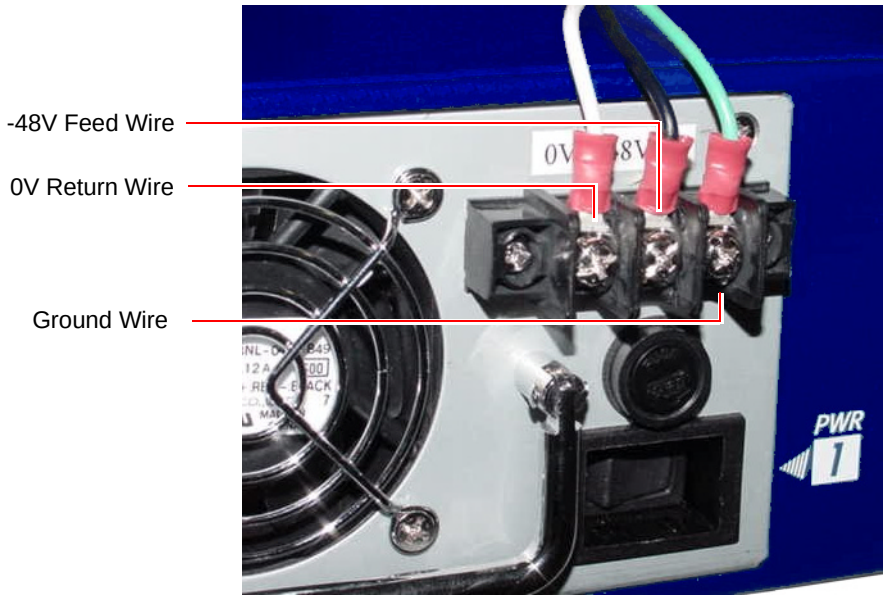
The DC power supplies, on/off switches, and terminal blocks, are located in the back of the chassis.



Warning *You must shut off current to the DC feed wires before connecting the wires to the power supplies. Also, make sure that the on/off switches on the NetScreen-500 power supplies are in the off position; that is, the right side of the on/off switch is pressed in.*

To connect DC power feeds to the terminal blocks, do the following:

1. Loosen the three retaining screws on each terminal block.
2. Insert the 0V DC return wire into the left power connector, the -48V DC power feed wire into the middle power connector, and the ground wire into the ground (E) on the right.

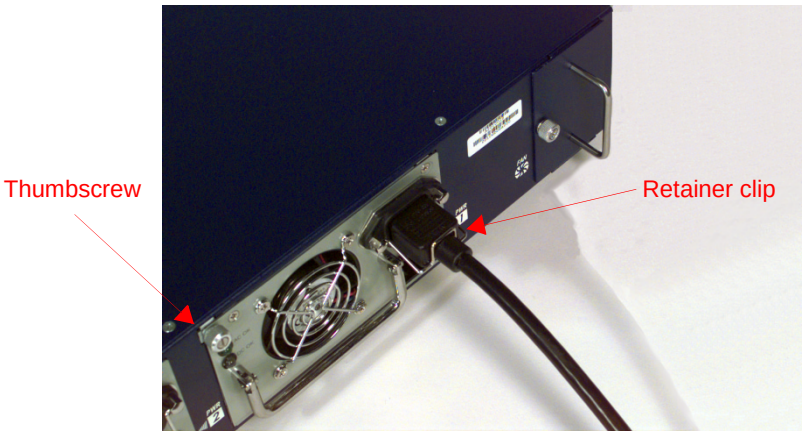


3. Fasten the screws over the connectors and ground.

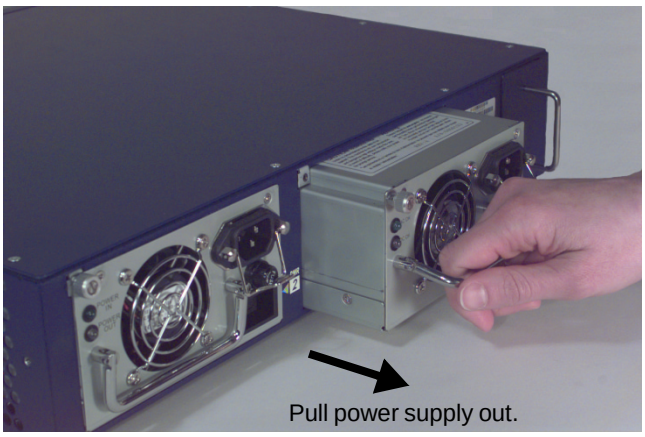
Replacing an AC Power Supply

To replace one of the AC power supplies, do the following:

1. Turn off the power supply.
2. Lift the AC power cord retainer clip.

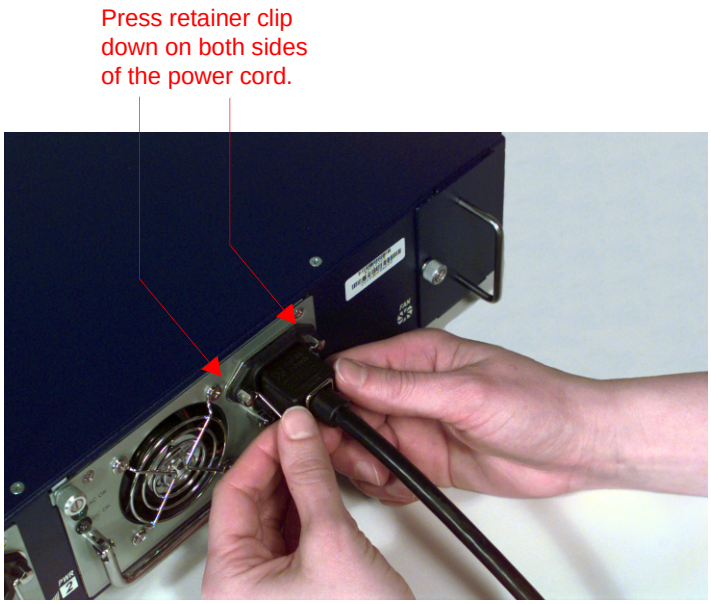


3. Unplug the cord from the power supply.
4. Turn the thumbscrew counterclockwise to release the power supply.
5. Lift the handle and, gripping the handle, pull the power supply straight out.



6. Insert the new power supply into the bay.

7. Secure it in place by tightening the thumbscrew clockwise.
8. Lift the retainer clip, and plug the power cord into the power supply.
9. Press the retainer clip over the cord, securing it in place.



Replacing a DC Power Supply

Warning *You must shut off current to the DC feed wires leading to the power supply that you want to replace. Also, make sure that the on/off switch on the power supply is in the off position; that is, the right side of the on/off switch is pressed in.*

To replace one of the DC power supplies, do the following:

1. Loosen the three retaining screws on the terminal block.
2. Remove the feed wires.
3. Turn the thumbscrew counterclockwise to release the power supply.
4. Lift the handle and, gripping the handle, pull the power supply straight out.
5. Insert the new power supply into the bay.
6. Secure it in place by tightening the thumbscrew clockwise.
7. Reconnect the wires as explained in "Wiring the DC Power Supplies" on page 2-16.

Connecting to the Network 3

After installing the interface modules as described in "Installing the Interface Modules" on page 2-2, follow the instructions in this chapter to connect the NetScreen-500 to the network as either a single security appliance or as a member in a redundant group of several NetScreen-500 devices cabled for high availability (HA).

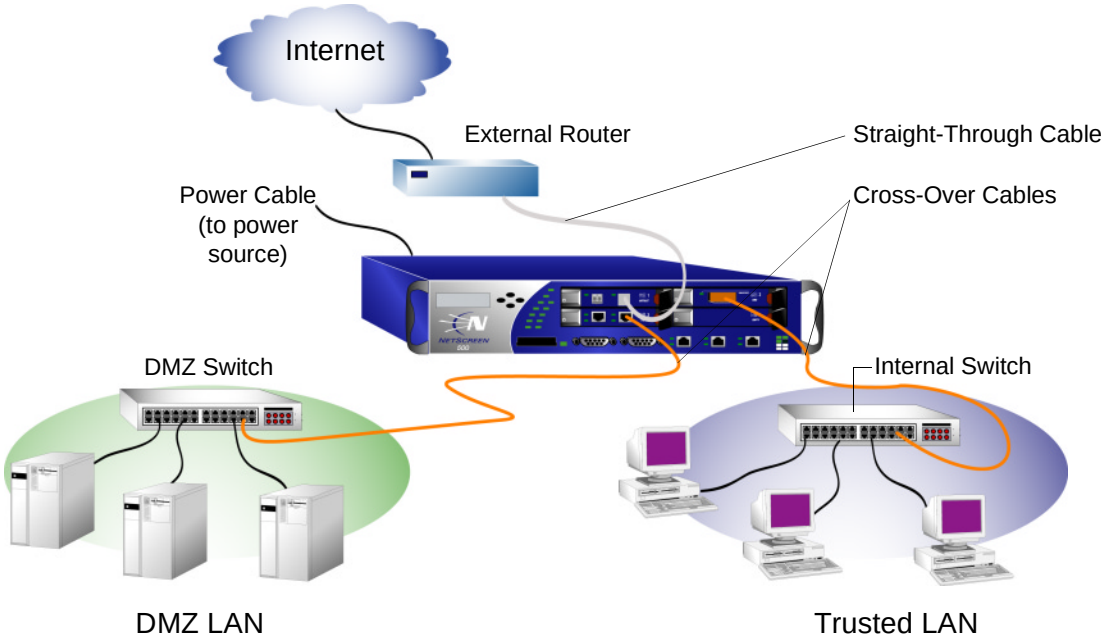
Important: *Before connecting the NetScreen-500 to a network, read "Safety Recommendations and Warnings" on page B-1.*

When you connect the NetScreen-500 to your network, the type of network determines whether you use a 10/100 BaseT interface or a gigabit interface connector (GBIC) interface. In the two cabling procedures described in this chapter, the cables to use for both network types—10/100 BaseT and fiber optic—are described.

Because of the wide variety of available routers, hubs, and switches, the cabling configuration presented here might not satisfy your network connection requirements. If the cabling suggested here does not work, try other cable configurations until a link light indicates an active link.

CONNECTING THE NETSCREEN-500 AS A SINGE SECURITY APPLIANCE

Note: *This illustration shows cables used for 10/100 BaseT networks. For fiber optic networks, use optical cables for all network connections.*



To add a single NetScreen-500 to your network, do the following:

1. Install the NetScreen-500 in a rack (optional—see "Mounting the NetScreen-500" on page 2-8) or on a level surface.
2. Make sure that the NetScreen-500 on/off switch is turned off.
3. Connect the power cable, included in the product package, to the NetScreen-500 power supply and to a power source[1].

1. If you want to use both power supplies, connect the second power supply to a different power source, if possible. In the event that one power source fails, the second source might still be operative.

4. For 10/100 BaseT, connect a cross-over cable from the right[2] trusted interface to the internal switch, router, or hub[3].

   For fiber optic, connect an optical cable from the trusted interface to the internal switch, router, or hub.

5. For 10/100 BaseT, connect a straight-through cable from the right untrusted interface to the external router.

   For fiber optic, connect an optical cable from the untrusted interface to the external router.

6. For 10/100 BaseT, connect a cross-over cable from the right DMZ interface to the DMZ switch, router, or hub.

   For fiber optic, connect an optical cable from the DMZ interface to the DMZ switch, router, or hub.

7. Flip the on/off switch to the ON position.
8. After the NetScreen-500 boots up, check the following LEDs:
   - The PWR 1 LED (and PWR 2 LED, if power supply #2 is also cabled to a power source) glows green.
   - The STATUS LED blinks green.
   - The top Link Status LEDs for each interface glows or blinks green. (For more details about interpreting the Link Status LEDs, see "Interface Modules" on page 1-6.)

2. For ScreenOS 2.6.x and 3.0.x, use only the right ports on the dual-port interface modules.

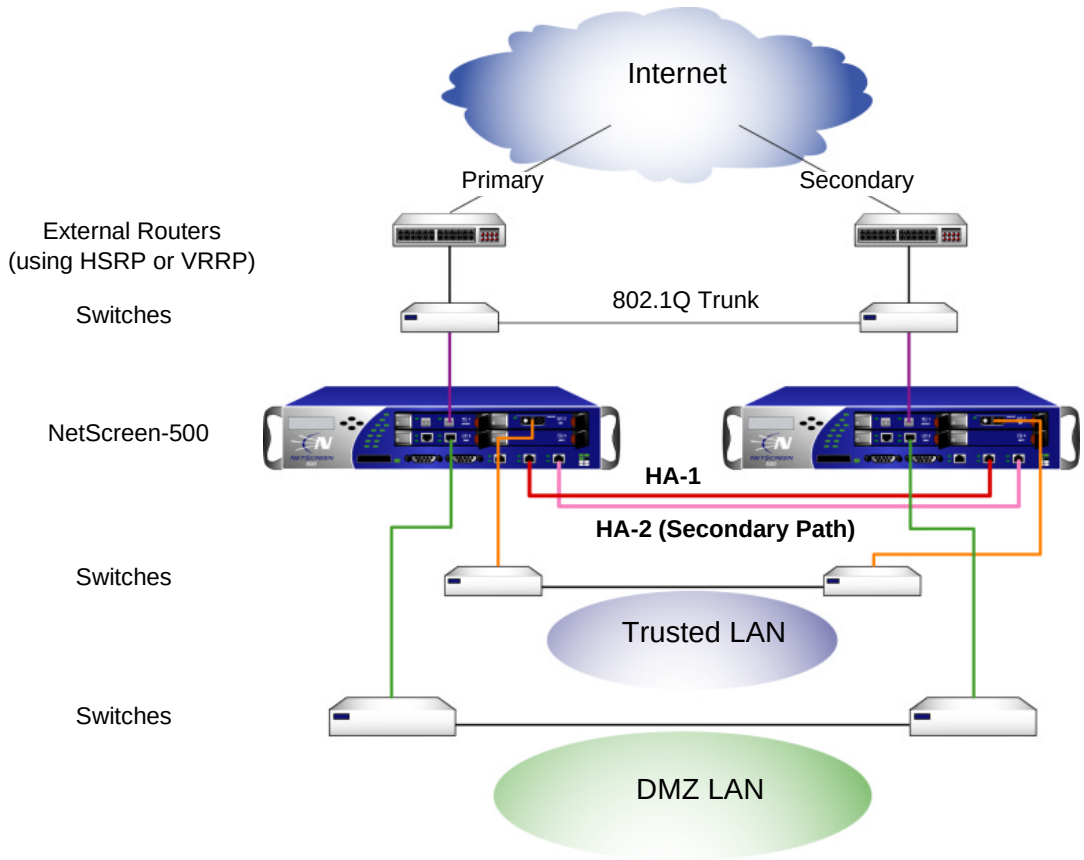
3. Check your router, hub, or computer documentation to determine if the device must be reconfigured, or if the power supply must be switched off when connecting new equipment to the LAN.

Connecting the NetScreen-500 for High Availability

By cabling together two or more NetScreen-500 devices to form a redundant group, you can configure the units for high availability (HA). In each redundant group of NetScreen-500 devices, one device acts as the master and the others as the slaves. If the master fails, a slave is elected as the new master and assumes all the functions of the previous master without causing any interruption to services.

This section explains how to cable two NetScreen-500 devices together in a redundant group for HA and connect them to network switches. After you have cabled the devices together, you must then configure them to be in the same redundant group and assign each unit a priority number to define its status as master or slave. For information on configuring the NetScreen-500 for HA, see "High Availability" on page 4-15.

Note: *For more information about HA, see Chapter 10, "High Availability" in the* NetScreen Concepts & Examples ScreenOS Reference Guide.



To cable two NetScreen-500 devices together for HA and connect them to the network, do the following:

1. Install the NetScreen-500 devices in a rack (optional—see "Mounting the NetScreen-500" on page 2-8) or on a level surface.
2. Make sure that the NetScreen-500 on/off switch is turned off on both devices.
3. On both devices, connect the power cable, included in the product package, to the NetScreen-500 power supply and to a power source[4].
4. Connect a 10/100 BaseT cross-over cable from the HA-1 port on one device to the HA-1 port on the second device.
5. Connect a 10/100 BaseT cross-over cable from the HA-2 port on one device to the HA-2 port on the second device[5].

Master Unit

6. For 10/100 BaseT, connect a cross-over cable from the trusted interface to a switch.

   For fiber optic, connect an optical cable from the trusted interface to the a switch.
7. For 10/100 BaseT, connect a cross-over cable from the DMZ interface to a second switch.

   For fiber optic, connect an optical cable from the DMZ interface to a second switch.
8. For 10/100 BaseT, connect a straight-through cable from the untrusted interface to a third switch.

   For fiber optic, connect an optical cable from the untrusted interface to a third switch.

4. If you want to use both power supplies, connect the second power supply to a different power source, if possible. In the event that one power source fails, the second source might still be operative.

5. The connection between the HA-2 ports provides a secondary path for HA communication in the event that the primary path between the HA-1 ports fails.

Slave Unit

9. For 10/100 BaseT, connect a cross-over cable from the trusted interface to the same switch to which the trusted interface on the master unit is cabled.

   For fiber optic, connect an optical cable from the trusted interface to the same switch to which the trusted interface on the master unit is cabled.

10. For 10/100 BaseT, connect a cross-over cable from the DMZ interface to the same switch to which the DMZ interface on the master unit is cabled.

    For fiber optic, connect an optical cable from the DMZ interface to the same switch to which the DMZ interface on the master unit is cabled.

11. For 10/100 BaseT, connect a straight-through cable from the untrusted interface to the same switch to which the untrusted interface on the master unit is cabled.

    For fiber optic, connect an optical cable from the untrusted interface to the same switch to which the untrusted interface on the master unit is cabled.

Switches

12. Cable the switches on the trusted side together.
13. Cable the switches on the DMZ side together.
14. Cable the switches on the untrusted side together
15. Connect the switches on the untrusted side to routers.

Note: *The switch ports must be defined as 802.1Q trunk ports, and the external routers must be able to use either Hot Standby Router Protocol (HSRP) or Virtual Router Redundancy Protocol (VRRP). See the switch and router vendor's documentation for the best configuration method to use.*

16. Turn on both NetScreen-500 devices.

Initial Configuration 4

This chapter describes how to perform an initial configuration using each of the following three tools:

- "Configuring via the WebUI" on page 4-3
- "Configuring via the CLI" on page 4-9
- "Configuring via the Menu System" on page 4-12[1]

The initial configuration consists of the following tasks:

- Logging on
- Setting the system IP address
- Setting interface IP addresses
- Configuring an access policy
- Changing the administrator's login name and password
- Testing the initial configuration

The requirements for using each kind of configuration method are listed below:

Table 4-1 Administration Requirements

Configuration Method	Requirements
WebUI	Web browser: Netscape® Communicator® v4.5 or greater, or Microsoft® Internet Explorer v5 or greater. TCP/IP network connection to the NetScreen-500
CLI	Via the console port: a VT100 terminal emulator, such as Hilgraeve® Hyperterminal®, and an RS-232 male-to-female serial cable Via Telnet: TCP/IP network connection to the NetScreen-500
Menu system	Physical access to the NetScreen-500 device

1. The initial configuration presented here cannot be performed entirely through the menu system, which does not allow you to create an access policy, change the admin login name and password, or test the initial configuration.

The chapter also contains a section on setting up two NetScreen-500 devices in a redundant group for high availability (HA). (See "High Availability" on page 4-15.)

Finally, the chapter concludes with a section on returning the device to its factory default settings, which is quite useful should you lose a password. (See "Resetting the Device to the Factory Default Settings" on page 4-19.)

The NetScreen-500 device supports three operational modes: Transparent mode, NAT (Network Address Translation) mode, and Route mode.

Transparent Mode

In Transparent mode, the NetScreen device filters packets traversing the firewall without modifying any of the source or destination information in the IP packet header. Because it does not translate addresses, the IP addresses on the protected network must be valid, routable addresses on the untrusted network[2], which might be the Internet. In Transparent mode, the IP addresses for the trusted, untrusted, and DMZ interfaces are set at 0.0.0.0, making the presence of the NetScreen device invisible, or "transparent," to users.

Network Address Translation (NAT) Mode

When in NAT mode, the NetScreen device translates two components in the header of an outgoing IP packet traversing the firewall from the trusted side: its source IP address and source port number. The NetScreen device replaces the source IP address of the host that sent the packet with the IP address of the untrusted port[3] of the NetScreen device. Also, it replaces the source port number with another random port number generated by the NetScreen device.

Route Mode

In Route mode, the NetScreen device routes traffic between different interfaces without performing NAT; that is, the source address and port number in the IP packet header remain unchanged as it traverses the NetScreen device. Unlike NAT, the hosts on the trusted side must have public IP addresses, and you do not need to establish Mapped and Virtual IP addresses to allow sessions initiated on the untrusted side to reach hosts on the trusted side. Unlike Transparent mode, the trusted and untrusted interfaces are on different subnets.

---

2. If the router on the untrusted side performs NAT, then the addresses on the trusted side can be private IP addresses.

3. If the outbound traffic is destined for the DMZ, then the source IP address is translated to that of the DMZ port.

CONFIGURING VIA THE WEBUI

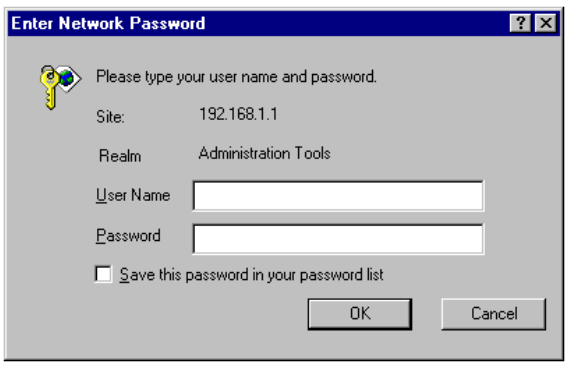
The following sections provide instructions for performing an initial configuration via the WebUI. Before starting, make sure that the NetScreen-500 is connected to the network as described in "Connecting to the Network" on page 3-1. Also make sure that your workstation has a Web browser (see "Administration Requirements" on page 4-1) and is on the same subnet as the NetScreen-500 device. For an explanation of the WebUI conventions used in this book, see "WebUI Conventions" on page xii.

Logging On and Setting the System IP Address

To perform an initial configuration through the WebUI, you must first change the IP address of the management workstation to the same subnet as that of the NetScreen-500 default system IP address, which is 192.168.1.1. You can then access the system IP address via a Web browser, log on, and change the system IP address to one that is appropriate for your network.

1. Record the IP address and netmask of your workstation. (You must reenter them later.)
2. Change the IP address of your workstation to 192.169.1.2 and the netmask to 255.255.255.0. (You might have to restart your workstation for the changes to take effect.)
3. Start your Web browser, and enter **http://192.168.1.1** in the URL field.

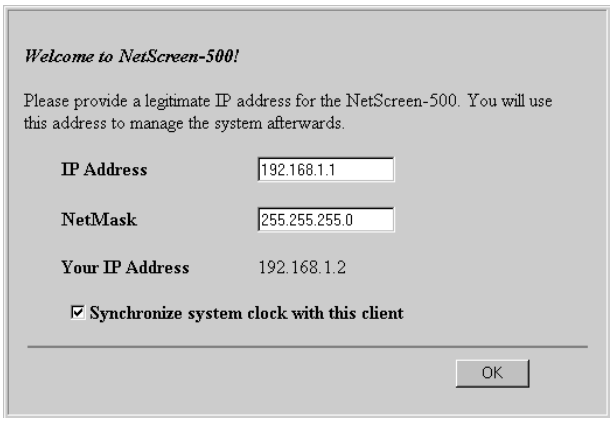
   The Enter Network Password dialog box appears.



4. Type **netscreen** for both the user name and password, and then click **OK**.

Note: *The user name and password are case sensitive.*

For the initial configuration, you are directed to a special setup page.



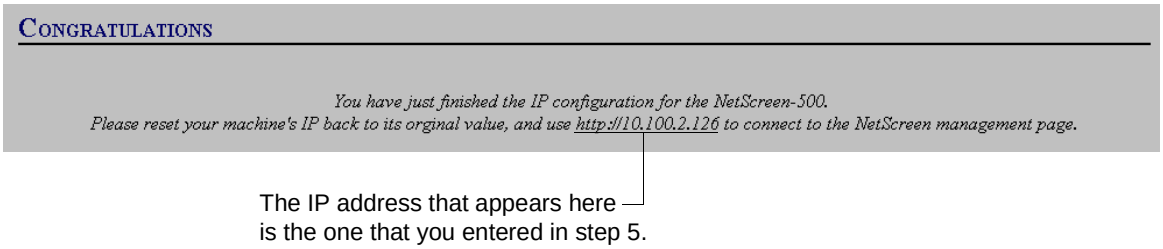
5. Enter the IP address and netmask for administration of the NetScreen-500, and then click **OK**.

   The IP address must be reachable from the management workstation; that is, if the management workstation is on the trusted side, then the System IP address must also be on the trusted side. If the management workstation is on the untrusted[4] or DMZ side, then the system IP address must be on the untrusted or DMZ side respectively.

Note: *To synchronize the NetScreen-500 clock with the clock in your workstation, select the* ***Synchronize system clock with this client*** *check box.*

4. To enable management using the WebUI via the untrusted or DMZ interface, you must first change the default settings that block management from those interfaces. You can do that by connecting to the console port (see "Connecting to the Console Port" on page 4-9) and using the following CLI command: **set interface { untrust | dmz } manage web**.

6. When the following message appears, close your Web browser, and reset the IP address and netmask of your workstation to the values you recorded in Step 1. (You might have to restart your workstation again.)



After changing the system IP address, you must again log on.

7. Start your Web browser, and type the new system IP address in the URL field.

   The Enter Network Password dialog box reappears.

8. Type **netscreen** for both the user name and password, and then click **OK**.

   The Access Policies pages appear, with the Outgoing page displayed.

Setting Interface Addresses

The NetScreen-500 ships with all its interface addresses and netmasks set as 0.0.0.0. If you want to operate the NetScreen-500 in Transparent mode, leave the trusted, untrusted, and DMZ interface addresses as they are; the MGT interface is the only one that you can assign an address. Indeed, it is highly recommended that you set the MGT interface address and use it exclusively for all administrative traffic.

To operate the NetScreen-500 in NAT mode or Route mode, you must also configure the trusted, untrusted, and DMZ interface addresses.

1. Interface >> MGT >> Edit: Enter the following, and then click **Save**:

   IP Address: Type an IP address for the MGT interface.

   Netmask: Type an appropriate netmask.

   Default Gateway: Type the IP address of the router—if there is one—between the MGT network and the NetScreen-500.

2. Interface >> Trusted >> Edit: Enter the following, and then click **Save**:

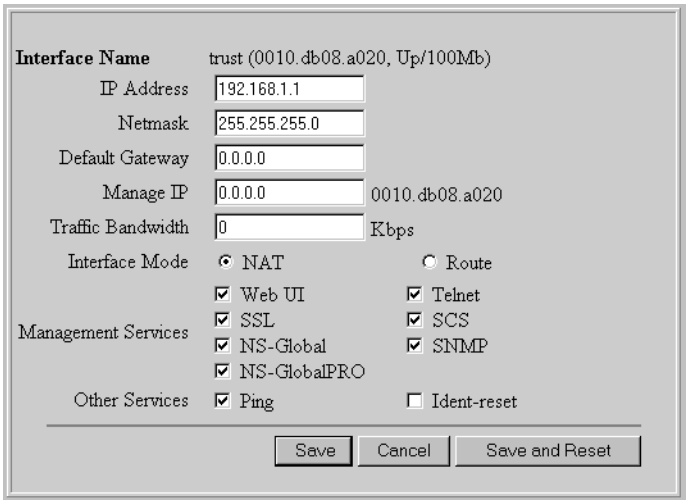
   IP Address: Type an IP address for the trusted interface.

   Netmask: Type an appropriate netmask.

   Default Gateway: Type the IP address of the router—if there is one—between the trusted network and the NetScreen-500.

   Interface Mode: Select either **NAT** or **Route**.

NAT or Route mode option.



3. Interface >> Untrusted >> Edit: Enter the following, and then click **Save**:

   IP Address: Type an IP address for the untrusted interface.

   Netmask: Type an appropriate netmask.

   Default Gateway: Type the IP address of the external router.

4. Interface >> DMZ >> Edit: Enter the following, and then click **Save and Reset**:

   IP Address: Type an IP address for the DMZ interface.

   Netmask: Type an appropriate netmask.

   Default Gateway: Type the IP address of the router—if there is one—between the DMZ network and the NetScreen-500.

Allowing Outbound Traffic

By default, the NetScreen-500 does not allow inbound or outbound traffic, nor does it allow traffic to or from the DMZ. You need to create access policies to permit specified kinds of traffic in the direction(s) you want. (You can also create access policies to deny and tunnel traffic.)

The following access policy permits all kinds of outbound traffic from any point on the trusted network to any point on the untrusted network. Of course, your network might require a more restrictive policy. The following is offered to illustrate how an access policy is created; it is not presented as a requirement for an initial configuration.

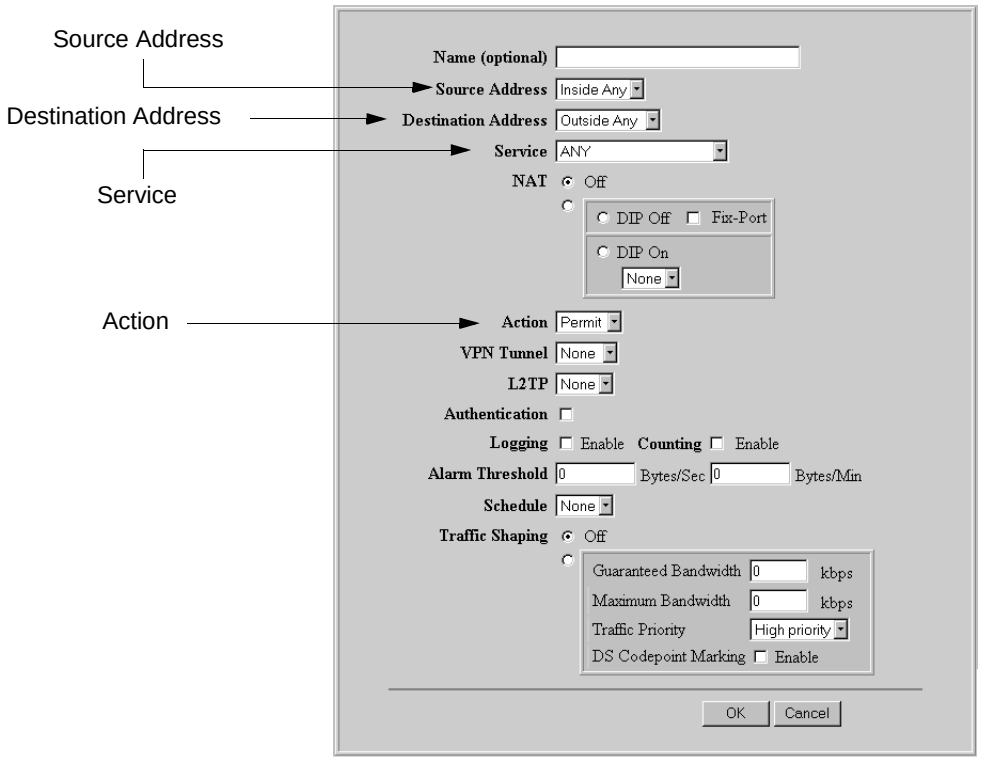
Policy >> Outgoing >> New Policy: Enter the following, and then click **OK**:

Source Address: Inside Any

Destination Address: Outside Any

Service: Any

Action: Permit



Changing Your Login Name and Password

Because all NetScreen products use the same login name and password (netscreen), it is highly recommended that you change your login name and password immediately.

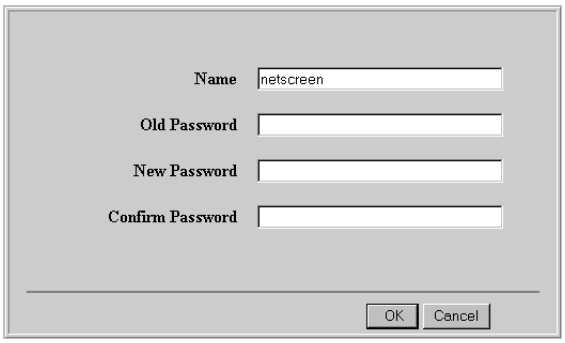
Admin >> Admin >> Edit: Enter the following, and then click **Apply**:

Name: Type your new login name.

Old Password: netscreen

New Password: Type your new password.

Confirm Password: Type your new password again.



Note: *For information on creating different levels of administrators, see Chapter 4, "Administration," in the* NetScreen Concepts & Examples ScreenOS Reference Guide.

If you forget your password, see *"Resetting the Device to the Factory Default Settings" on page 4-19*.

Testing the Configuration

From a point on the trusted network, use a Web browser to access an external Web site, such as www.netscreen.com. If everything has been configured correctly, you will be able to locate the site and access its Web pages.

If you cannot access the Web site, check the following:

- Link lights on the NetScreen-500, the workstation, and all intervening hubs and routers are lit.
- The workstation IP address and netmask have the correct settings.
- The workstation gateway points to the router on its subnet.
- The workstation is configured properly for DNS.

CONFIGURING VIA THE CLI

The following sections provide instructions for performing an initial configuration via the CLI. For CLI conventions, see "CLI Conventions" on page xiii.

You can access the NetScreen-500 directly, using Hyperterminal and connecting a console cable from your workstation to the console port. You can also access the NetScreen-500 remotely, using Telnet over a network connection. Connection instructions for both approaches are offered below:

Connecting to the Console Port

You need direct access to the NetScreen device and the items listed in "Administration Requirements" on page 4-1. Follow these steps:

1. Connect the serial cable from your workstation to the console port on the NetScreen-500.
2. Start the terminal emulator on your workstation.
3. To create a new connection, type a name, select an icon, and then click **OK**.

   The Direct To dialog box appears.
4. Select the serial port to which the serial cable is connected to the workstation (usually COM1 or COM2), and then click **OK**.

   The COM1 (or COM2) Properties dialog box appears.
5. Configure the port settings as follows, and then click **OK**:
   - Bits per second: 9600
   - Data bits: 8
   - Parity: None
   - Stop bits: 1
   - Flow control: None
6. Press the ENTER key to see the login prompt.

Note: *By default the console times out after 10 minutes of idle time. To change the timeout value, use the following command:* ***set console timeout <number>****, where the* ***<number>*** *variable indicates the length of idle time in minutes before a session is terminated. Use a value of 0 if you do not want a session to time out.*

Connecting via Telnet

You need network access to the NetScreen device and the items listed in "Administration Requirements" on page 4-1. Then do the following:

Open a Telnet session to 192.168.1.1. (In Windows, click **Start >> Run**, type **telnet 192.168.1.1**, and then click **OK**.)

Note: *The terminal type must be vt100. Click* ***Connect****, and then select* ***Remote System****. In the dialog box that appears, select* ***vt100*** *from the Term Type menu.*

Logging On and Setting the System IP Address

To manage the NetScreen device over a network connection, you must change the system IP address from its default (192.168.1.1) to one that is appropriate for your network. To log on and change the system IP address, enter the following commands, where <a.b.c.d> is the new system IP address:

1. At the login prompt, type **netscreen**.
2. At the password prompt, type **netscreen**.
3. set admin sys-ip <a.b.c.d>
4. save

Setting Interface Addresses

The NetScreen-500 ships with all its interface addresses and netmasks set as 0.0.0.0. If you want to operate the NetScreen-500 in Transparent mode, leave the trusted, untrusted, and DMZ interface addresses as they are; the MGT interface is the only one that you can assign an address. Indeed, it is highly recommended that you set the MGT interface address and use it exclusively for all administrative traffic.

To operate the NetScreen-500 in NAT mode or Route mode, you must also configure the trusted, untrusted, and DMZ interface addresses, using addresses and netmasks appropriate for your network environment.

To set the interface addresses, enter the following commands, where <a.b.c.d> are the interface IP addresses and <A.B.C.D> is the netmask:

1. set interface mgt ip <a.b.c.d> <A.B.C.D> [gateway <a.b.c.d>]
2. set interface trust ip <a.b.c.d> <A.B.C.D> [gateway <a.b.c.d>]
3. set interface untrust ip <a.b.c.d> <A.B.C.D> [gateway <a.b.c.d>]
4. set interface dmz ip <a.b.c.d> <A.B.C.D> [gateway <a.b.c.d>]
5. save

Allowing Outbound Traffic

By default, the NetScreen-500 does not allow inbound or outbound traffic, nor does it allow traffic to or from the DMZ. You need to create access policies to permit specified kinds of traffic in the direction(s) you want. (You can also create access policies to deny and tunnel traffic.)

The following access policy permits all kinds of outbound traffic from any point on the trusted network to any point on the untrusted network. Of course, your network might require a more restrictive policy. The following is offered to illustrate how an access policy is created; it is not presented as a requirement for an initial configuration:

1. set policy outgoing “inside any” “outside any” any permit
2. save

Changing Your Login Name and Password

Because all NetScreen products use the same login name and password (netscreen), it is highly recommended that you change your login name and password immediately. Enter the following commands:

1. set admin name <name>
2. set admin password <password>
3. save

Note: *For information on creating different levels of administrators, see Chapter 4, “Administration,” in the* NetScreen Concepts & Examples ScreenOS Reference Guide.

If you forget your password, see *“Resetting the Device to the Factory Default Settings” on page 4-19*.

Testing the Configuration

From a point on the trusted network, use a Web browser to access an external Web site, such as www.netscreen.com. If everything has been configured correctly, you will be able to locate the site and access its Web pages.

If you cannot access the Web site, check the following:

- Link lights on the NetScreen-500, the workstation, and all intervening hubs and routers are lit.
- The workstation IP address and netmask have the correct settings.
- The workstation gateway points to the router on its subnet.
- The workstation is configured properly for DNS.

CONFIGURING VIA THE MENU SYSTEM

Through the menu system, you can configure the system and interface IP addresses. However, you cannot create an access policy, change the administrator's login name and password, or test the configuration. To perform these configurations, you must use either the WebUI or CLI. Still, the menu system offers a convenient tool for performing part of an initial configuration on site. For menu system conventions, see "Menu System Conventions" on page xv. For a complete description of the menu system, see Appendix A, "Menu System".

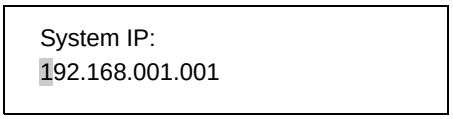
Note: *If you are concerned about unauthorized physical access to the device, you can disable the LCD and control keys. See "16. LCD Display" on page A-14.*

Setting the System IP Address

To manage the NetScreen device over a network connection, you must change the system IP address from its default (192.168.1.1) to one that is appropriate for your network. To change the system IP address, enter the following commands, where <a.b.c.d> is the new system IP address:

1. 1. Setting >> 11. Admin >> 111. System Address >> 1111. System IP: Press the RIGHT control key.

   The default system IP address appears, with the cursor flashing over the far left digit.

2. Use the UP and DOWN control keys to scroll through digits 0-2[5].
3. When you reach the digit you want, press the RIGHT control key.

   The first digit is selected, and the cursor moves to the second digit from the left.

4. Use the UP and DOWN control keys to scroll through digits 0-9 until you reach the digit you want, and then press the RIGHT control key to select that.

5. You can scroll cyclically through the digits.

5. Continue until you have selected all the digits for the system IP address.
6. Position the cursor on the far right digit, and then press the RIGHT control key.

   The newly created IP address appears (shown as XXX.XXX.XXX.XXX below), and you are prompted to confirm or cancel it.

```
XXX.XXX.XXX.XXX
No (<-),  Yes (->) ?
```

7. Press the RIGHT control key to confirm the new address.

Setting Interface Addresses

The NetScreen-500 ships with all its interface addresses and netmasks set as 0.0.0.0. If you want to operate the NetScreen-500 in Transparent mode, leave the trusted, untrusted, and DMZ interface addresses as they are; the MGT interface is the only one that you can assign an address. Indeed, it is highly recommended that you set the MGT interface address and use it exclusively for all administrative traffic.

To operate the NetScreen-500 in NAT mode or Route mode, you must also configure the trusted, untrusted, and DMZ interface addresses.

Setting the MGT Interface IP Address, Netmask, and Gateway

1. 1. Setting >> 12. interface >> 124. MGT >> 1241. IF IP: Press the RIGHT control key.

   The default MGT interface IP address appears, with the cursor flashing over the far left digit.

```
IF IP:
000.000.000.000
```

2. Use the UP and DOWN control keys to scroll through digits 0-2.
3. When you reach the digit you want, press the RIGHT control key.

   The first digit is selected, and the cursor moves to the second digit from the left.

4. Use the UP and DOWN control keys to scroll through digits 0-9 until you reach the digit you want, and then press the RIGHT control key to select that.
5. Continue until you have selected all the digits for the MGT interface IP address.
6. Position the cursor on the far right digit, and then press the RIGHT control key.
7. When prompted to confirm the new MGT IP address, press the RIGHT control key.
8. 1. Setting >> 12. interface >> 124. MGT >> 1242. IF Netmask: Press the RIGHT control key, and select the digits for the MGT interface netmask as you did for the IP address.
9. 1. Setting >> 12. interface >> 124. MGT >> 1243. Gateway IP: Press the RIGHT control key, and select the digits for the MGT interface gateway IP address.

Setting the Trusted Interface IP Address, Netmask, and Gateway

1. 1. Setting >> 12. interface >> 121. Trust >> 1211. IF IP: Press the RIGHT control key, and select the digits for the trusted interface IP address.
2. 1. Setting >> 12. interface >> 121. Trust >> 1212. IF Netmask: Press the RIGHT control key, and select the digits for the trusted interface netmask.
3. 1. Setting >> 12. interface >> 121. Trust >> 1213. Gateway IP: Press the RIGHT control key, and select the digits for the trusted interface gateway IP address.

Setting the Untrusted Interface IP Address, Netmask, and Gateway

1. 1. Setting >> 12. interface >>122. Untrust >> 1221. IF IP: Press the RIGHT control key, and select the digits for the untrusted interface IP address.
2. 1. Setting >> 12. interface >> 122. Untrust >> 1222. IF Netmask: Press the RIGHT control key, and select the digits for the untrusted interface netmask.
3. 1. Setting >> 12. interface >> 122. Untrust >> 1223. Gateway IP: Press the RIGHT control key, and select the digits for the untrusted interface gateway IP address.

Setting the DMZ Interface IP Address, Netmask, and Gateway

1. 1. Setting >> 12. interface >>123. DMZ >> 1231. IF IP: Press the RIGHT control key, and select the digits for the DMZ interface IP address.
2. 1. Setting >> 12. interface >> 123. DMZ >> 1232. IF Netmask: Press the RIGHT control key, and select the digits for the DMZ interface netmask.
3. 1. Setting >> 12. interface >> 123. DMZ >> 1233. Gateway IP: Press the RIGHT control key, and select the digits for the DMZ interface gateway IP address.

HIGH AVAILABILITY

Before you can configure two NetScreen-500 devices in a redundant group for high availability (HA), you must cable them together as shown in "Connecting the NetScreen-500 for High Availability" on page 3-4. Then you must assign one device as the master unit and one as the slave. The master performs all the firewall, VPN, and traffic management functions, while the slave waits to take over should the master unit fail. The master sends configuration and session state information to the slave over the HA link, so that the slave can instantly assume master status during a failover without interrupting service. The NetScreen-500 also has a second HA link to provide a backup should the primary HA link fail.

Configuring HA via the WebUI

To activate HA communications between two NetScreen-500 devices that are already cabled for HA, you must assign both to the same redundant group and assign each device a priority number, used to define the master and slave status. Also, if you are managing the devices through any interface other than the MGT interface, it is important that you set the manage IP address on that interface so that you can manage the slave unit if necessary[6].

Master Unit

1. Interface >> Trusted | Untrusted | DMZ >> Edit: Enter the following, and then click **Save**:

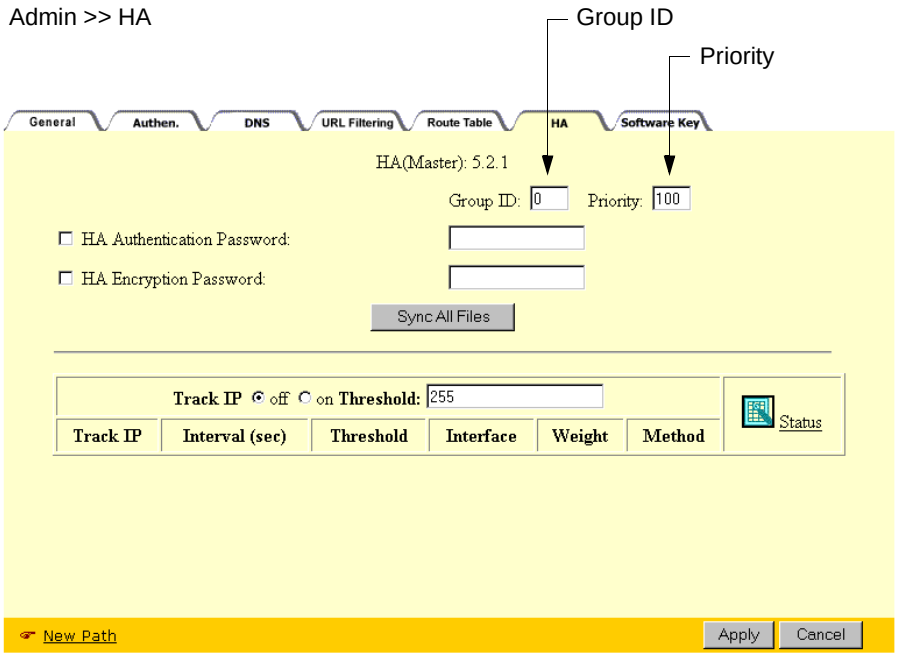
   Manage IP: Enter an IP address in the same subnet as that of the physical interface.

2. Admin >> HA: Enter the following, and then click **Apply**:

   Group ID: Enter a number to identify this device as a member of a specific redundant group.

   Priority: Enter a number between 1 and 65,535. The device with the number closest to 1 is the master. (A value of 0 disables HA and shuts down the HA ports.)

6. Some HA features are configurable only through the CLI. To set the link-up state of the slave unit and save the configuration from the master unit to the slave, refer to the CLI section.



Slave Unit

1. Interface >> Trusted | Untrusted | DMZ >> Edit: Enter the following, and then click **Save**:

   Manage IP: Enter an IP address in the same subnet as that of the physical interface.

2. Admin >> HA: Enter the following, and then click **Apply**:

   Group ID: Enter the same number you used for the master unit.

   Priority: Enter a lower number than the one you gave the master unit.

Note: *To verify that both devices are properly configured, check the HA LED on each unit. The HA LED on the master unit glows green. The HA LED on the slave unit glows amber. For more information on the meanings of the LEDs, see* *"LED Dashboard" on page 1-3.*

Configuring HA via the CLI

To activate HA communications between two NetScreen-500 devices that are already cabled for HA, you must assign both to the same redundant group and assign each device a priority number, used to define the master and slave status. Also, if you are managing the devices through any interface other than the MGT interface, it is important that you set the manage IP address on that interface so that you can manage the slave unit if necessary.

Master Unit

1. set interface { trust | untrust | dmz } manage-ip <a.b.c.d>
2. set ha group <number>
3. set ha priority <number>
4. set ha link-up-on-slave

Slave Unit

1. set interface { trust | untrust | dmz } manage-ip <a.b.c.d>
2. set ha group <same_number_as_master>
3. set ha priority <larger_number_than_master>
4. save config ha-master
5. reset

   Configuration modified, save? [y]/n (Type **n**.)

   System reset, are you sure? y/[n] (Type **y**.)

Note: *To verify that both devices are properly configured, check the HA LED on each unit. The HA LED on the master unit glows green. The HA LED on the slave unit glows amber. For more information on the meanings of the LEDs, see* *"LED Dashboard" on page 1-3.*

RESETTING THE DEVICE TO THE FACTORY DEFAULT SETTINGS

If the admin password is lost, you can use the following procedure to reset the NetScreen device to its default settings. The configurations will be lost, but you will restore access to the device. To perform this operation, you need to make a console connection, which is described in "Connecting to the Console Port" on page 4-9.

> ***Note:*** *By default the device recovery feature is enabled. You can disable it by entering the following CLI command:* ***unset admin device-reset****.*

1. At the login prompt, type the serial number of the device.
2. At the password prompt, type the serial number again.

   The following message appears:

   !!! Lost Password Reset !!! You have initiated a command to reset the device to factory defaults, clearing all current configuration, keys and settings. Would you like to continue? y/[n]

3. Press the **y** key.

   The following message appears:

   !! Reconfirm Lost Password Reset !! If you continue, the entire configuration of the device will be erased. In addition, a permanent counter will be incremented to signify that this device has been reset. This is your last chance to cancel this command. If you proceed, the device will return to factory default configuration, which is: System IP: 192.168.1.1; username: netscreen; password: netscreen. Would you like to continue? y/[n]

4. Press the **y** key to rest the device.

   You can now login in using *netscreen* as the default username and password.

Menu System

A

Using the control pad and the LCD, you can navigate through the NetScreen-500 menu system to perform some administrative and network-related configurations. You can view system status, configuration settings, and alarms, and you can save the software or configuration to a PC card.

The menu system is organized hierarchically. The organization of the level 1 and 2 branches of the system are shown below. Following this, each level 1 branch and all its sublevels are examined in turn.

Level 1	Level 2
1. Setting	
	11. Admin
	12. Interface
	13. Time/Date
	14. Audible Alarm
	15. Temp Threshold
	16. LCD Display
2. Status	
	21. Utilization
	22. Temperature
	23. Version
3. Alarm	
	31. View
	32. Clear All
4. PCMCIA	
	41. Save
5. Reset	
	51. Save & Reset
	52. Unsave & Reset
6. Exit	

1. SETTING

The Setting branch of the menu system is where you can create and modify settings that define the following system parameters:

11. Admin (administrative settings and restrictions)

12. Interface (trusted, untrusted, DMZ, and MGT interface addresses and options)

13. Time/Date (settings for the time and date for the NetScreen-500 device)

14. Audible Alarm (audible alarm functionality)

15. Temp Threshold (temperature control adjustments)

16. LCD Display (LCD and control pad access)

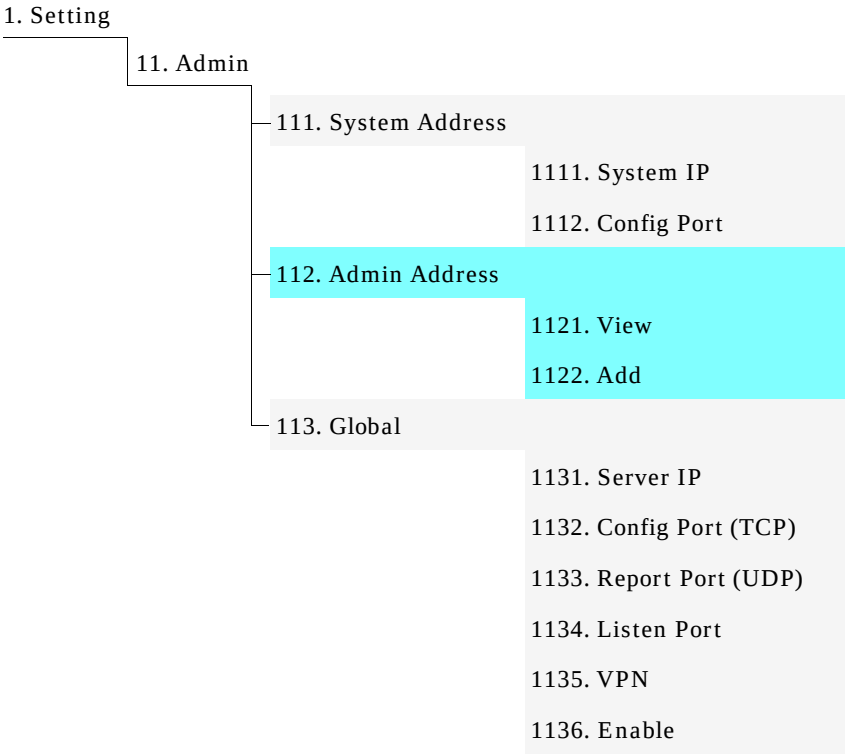
11. Admin

The Admin branch is where you can configure and view the following settings:

111. System Address: The system IP address and port number for administrative traffic via the Web

112. Admin Address: A remote administrator's IP address and netmask

113. Global: The remote IP address and port numbers required for communicating with a NetScreen-Global Manager client, and whether VPN encryption is enabled when transmitting Global Manager messages


1. Setting
11. Admin
111. System Address
1111. System IP
1112. Config Port
112. Admin Address
1121. View
1122. Add
113. Global
1131. Server IP
1132. Config Port (TCP)
1133. Report Port (UDP)
1134. Listen Port
1135. VPN
1136. Enable

111. System Address

1111. System IP

The system IP address is the address that you can use for managing the NetScreen-500 via an Ethernet connection. To set it, do the following:

1. Press the RIGHT control key.

   You can see the current system IP address:

   ```
   System IP:
   192.168.001.001
   ```

2. Press the RIGHT and LEFT control keys to move the cursor to a specific digit.
3. Press the UP and DOWN control keys to scroll through digits to change the selected digit to a different one.
4. When the cursor is at the digit you want, press the RIGHT or LEFT control key to select it.
5. Repeat steps 3 and 4 for all the digits you want to change.
6. When done, move the cursor to the far right position, and press the RIGHT control key. (When the cursor is at the far left digit and you press the LEFT control key, you return to **1111. System IP**.)

   The following display appears, in which <a.b.c.d> is the IP address you just set:

   ```
   a.b.c.d
   ▶ No (<-), Yes (->) ?
   ```

7. Press the LEFT control key to select **Yes** or the RIGHT control key to select **No**.

1112. Config Port

The port number for administrative traffic to the system IP address. The default is 80. You can scroll from 1 to 65,535.

112. Admin Address		
	1121. View	The IP address for the administrator. The default is 0.0.0.0, which allows administrative access from any IP address. Restricting access to a single host or subnet increases security.
	1122. Add	Set the admin IP address as you did the system IP address. Add: 000.000.000.000 Then press the RIGHT control key to display the admin netmask. Admin netmask: 000.000.000.000 Use the control keys to set the netmask.
113. Global		
	1131. Server IP	The IP address of the server running NetScreen-Global Manager.
	1132. Config Port	The port number on which the NetScreen-500 sends (TCP) configuration messages to NetScreen-Global Manager.The default is 15397. The scrolling range is from 1 to 65535.
	1133. Report Port	The port number on which the NetScreen-500 sends (UDP) log messages to NetScreen-Global Manager. The default is 15397. The scrolling range is from 1 to 65535.
	1134. Listen Port	The port number on which the NetScreen-500 receives messages from NetScreen-Global Manager. The default is 15397. The scrolling range is from 1 to 65535.
	1135. VPN	Enables or disables VPN encryption in Global.
	1136. Enable	Enables manageability from NetScreen-Global Manager.

12. Interface

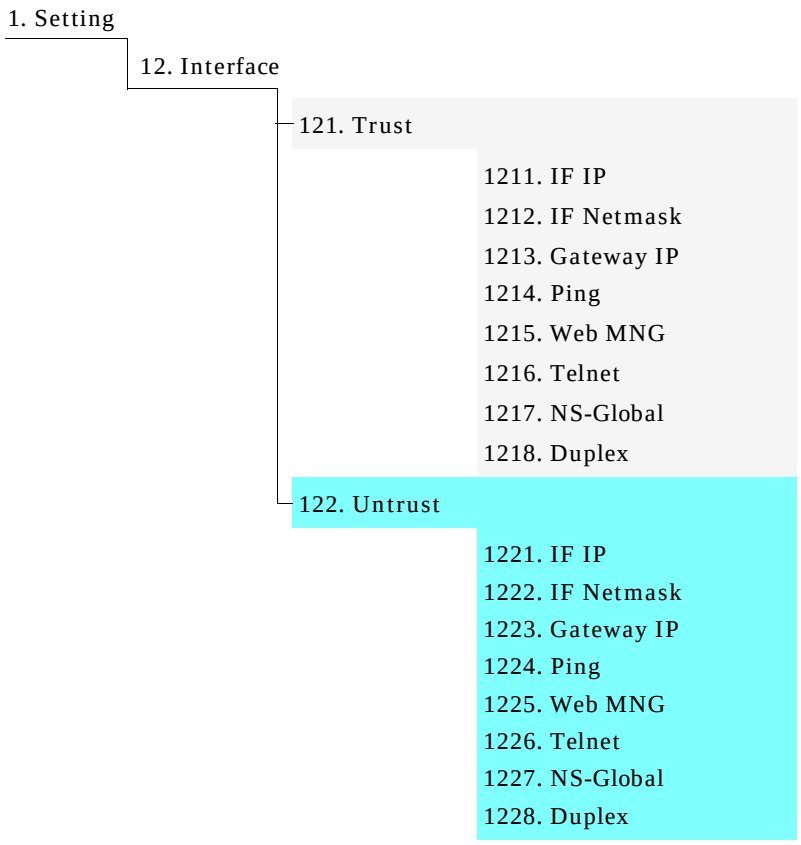
The Interface branch is where you can configure and view the following settings:

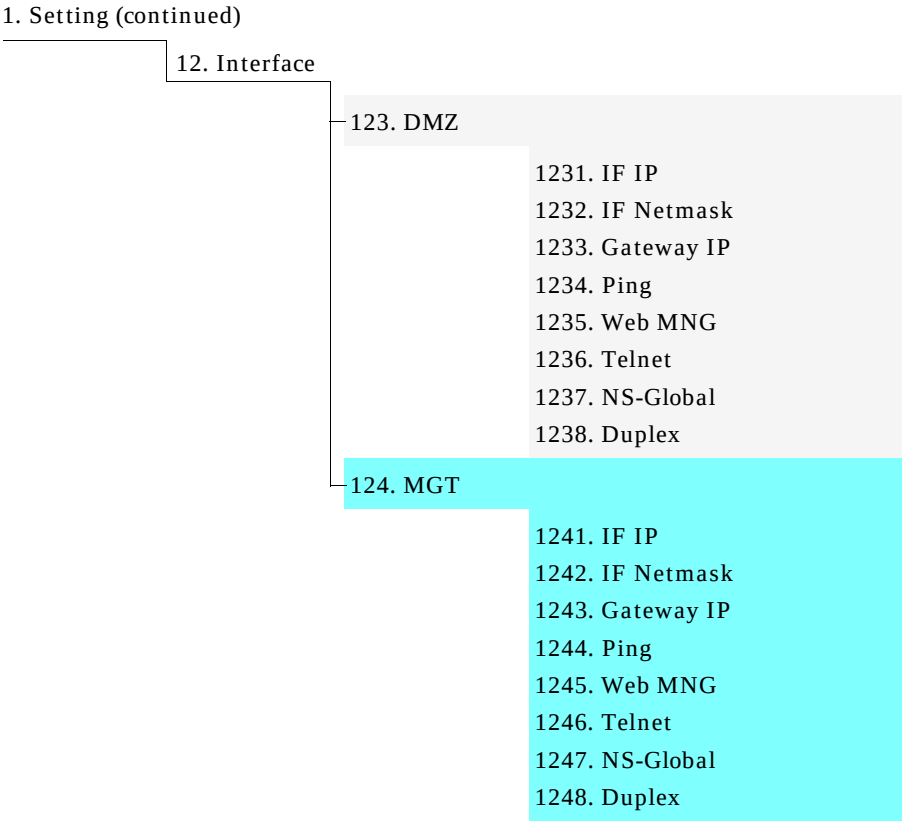
121. Trust: The IP address, netmask, default gateway, manageability options, and duplex processing preference for the trusted interface

122. Untrust: The IP address, netmask, default gateway, manageability options, and duplex processing preference for the untrusted interface

123. DMZ: The IP address, netmask, default gateway, manageability options, and duplex processing preference for the DMZ interface

124. MGT: The IP address, netmask, default gateway, manageability options, and duplex processing preference for the management (MGT) interface





Note: *Because the untrusted, DMZ, and MGT interface options are identical to those for the trusted interface, the following descriptions of the trusted interface options apply equally well to those for the other interfaces.*

121. Trust

1211. IF IP

The IP address of the trusted interface. To set it, do the following:

1. Press the RIGHT control key.

   You can see the current trusted interface IP address:

   ```
   IF IP:
   000.000.000.000
   ```

2. Press the RIGHT and LEFT control keys to move the cursor to a specific digit.
3. Press the UP and DOWN control keys to scroll through digits to change the selected digit to a different one.
4. When the cursor is at the digit you want, press the RIGHT or LEFT control key to select it.
5. Repeat steps 3 and 4 for all the digits you want to change.
6. When done, move the cursor to the far right position, and press the RIGHT control key. (When the cursor is at the far left digit and you press the LEFT control key, you return to **1211. IF IP**.)

   The following display appears, in which <a.b.c.d> is the IP address you just set:

   ```
   a.b.c.d
   ▶ No (<-), Yes (->)  ?
   ```

7. Press the LEFT control key to select **Yes** or the RIGHT control key to select **No**.

1212. IF Netmask

The netmask for the trusted interface. Use the control keys as you did to configure the address for the trusted interface to configure its netmask.

1213. Gateway IP

The IP address for the internal default gateway (if there is one) connecting the subnet for the trusted interface with a different subnet.

1214. Ping

Enables the trusted interface to respond to ICMP echo requests (PINGs).

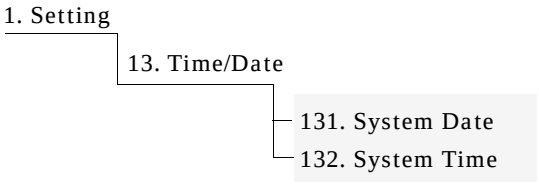
1215. Web MNG	Enables the trusted interface to permit administrative traffic via the Web.
1216. Telnet	Enables the trusted interface to permit administrative traffic via Telnet.
1217. NS-Global	Enables the trusted interface to permit administrative traffic originating from a NetScreen-Global Manager client.
1218. Duplex	The mode of data transmission on the trusted interface. The options are as follows: • half-duplex: data can only be transmitted in one direction at a time (either incoming or outgoing). • full duplex: Data can be transmitted in both directions concurrently. • auto duplex: Data is transmitted in either half-duplex or full-duplex mode, depending on the capability, or preference, of the other communicating party.

13. Time/Date

The Time/Date branch is where you can configure and view the following settings:

131. System Date: The date for the NetScreen-500 device

132. System Time: The time for the NetScreen-500 device



131. System Date

To set the date for the NetScreen-500 device, do the following:

1. Press the RIGHT control key.

   You can see the current date (yyyy/mm/dd):

   ```
   System Date:
   0000/00/00
   ```

2. Press the RIGHT and LEFT control keys to move the cursor to a specific digit.
3. Press the UP and DOWN control keys to scroll through digits to change the selected digit to a different one.
4. When the cursor is at the digit you want, press the RIGHT or LEFT control key to select it.
5. Repeat steps 3 and 4 for all the digits you want to change.
6. When done, move the cursor to the far right position, and press the RIGHT control key. (When the cursor is at the far left digit and you press the LEFT control key, you return to **131. System Date**.)

   The following display appears, in which <yyyy/mm/dd> is the date you just set:

   ```
   yyyy/mm/dd
   ▶ No (<-), Yes (->)  ?
   ```

7. Press the LEFT control key to select **Yes** or the RIGHT control key to select **No**.

132. System Time

To set the time for the NetScreen-500 device, use the control keys to select digits (see “131. System Date”).

```
System Time:
09:30:00
```

Note that when the cursor is on the first hour digit, pressing the UP and DOWN control keys changes both hour digits. For example, if the hour digits are **09** and the cursor is on **0**, pressing the UP key changes both digits to **10**. For minutes and seconds, you can change both pairs of digits individually.

14. Audible Alarm

The Audible Alarm branch is where you can enable and disable the audible alarm, which sounds to signal alarms for both firewall attacks and physical conditions such as a high temperature.

1. After you navigate to 1. Setting >> 14. Audible Alarm, press the RIGHT control key.

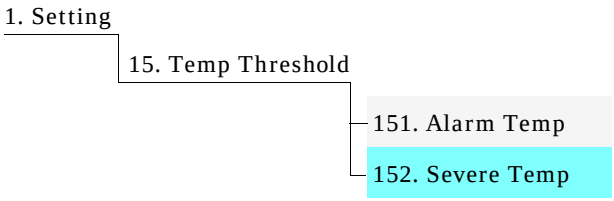
   The following display appears:

```
Setting Audible:
disabled
```

2. Press the UP or DOWN control key to toggle between enable and disable.
3. Select enable or disable by pressing the RIGHT control key.

15. Temp Threshold

The Temperature Threshold branch is where you can define the thresholds for triggering a temperature alarm and a severe temperature alarm[1].



151. Alarm Temp

The alarm temperature is a threshold setting, that when passed triggers an alert in the alarm event log and causes the Alarm LED to glow orange. To set it, do the following:

1. Press the RIGHT control key.

   You can see the current temperature alarm threshold:

   ```
   Alarm Temp (‘F):
   122
   ```

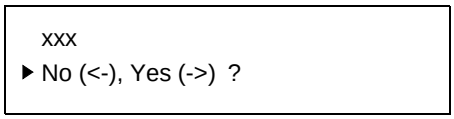
2. Press the RIGHT and LEFT control keys to move the cursor to a specific digit.
3. Press the UP and DOWN control keys to scroll through digits to change the selected digit to a different one.
4. When the cursor is at the digit you want, press the RIGHT or LEFT control key to select it.
5. Repeat steps 3 and 4 for all the digits you want to change.

---

1. The default temperature thresholds are 122° Fahrenheit for an alarm (also indicated by an orange Alarm LED) and 140° Fahrenheit for a severe temperature alarm (also indicated by a red Alarm LED).

6. When done, move the cursor to the far right position, and press the RIGHT control key. (When the cursor is at the far left digit and you press the LEFT control key, you return to **151. Alarm Temp**.)

   The following display appears, in which <xxx> is the temperature you just set:



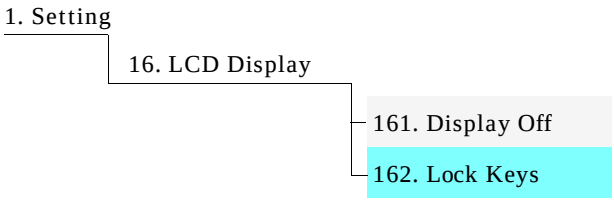
7. Press the LEFT control key to select **Yes** or the RIGHT control key to select **No**.

152. Severe Temp

The severe temperature is a threshold setting, that when passed triggers an alert in the alarm event log and causes the Alarm LED to glow red. To set it, follow the same procedure as described above (151. Alarm Temp).

16. LCD Display

The LCD Display branch is where you can turn off the LCD display and disable the control pad. Note that if you disable either of these features, you can only reactivate them by using the CLI commands provided below.



161. Display Off

To turn off the LCD display, do the following:

1. Press the RIGHT control key.

   The following display appears.

```
161. Display Off
No (<-) , Yes (->) ?
```

2. Press the RIGHT control key.

To reactivate the LCD display, use the following CLI command: **set lcd display**.

162. Lock Keys

To disable the control keys, do the following:

1. Press the RIGHT control key.

   The following display appears.

```
162. Lock Keys
No (<-) , Yes (->) ?
```

2. Press the RIGHT control key.

To reactivate the key pad, use the following CLI command: **set lcd key**.

2. STATUS

The Status branch of the menu system is where you can view data on the following:

21. Utilization (the utilization status of the CPU, memory, sessions, tunnels, and bandwidth)

22. Temperature (the temperature of the device)

23. Version (the serial number, hardware and software version numbers, and the image file name)

21. Utilization

The Utilization branch is where you can view the current utilization status of the following:

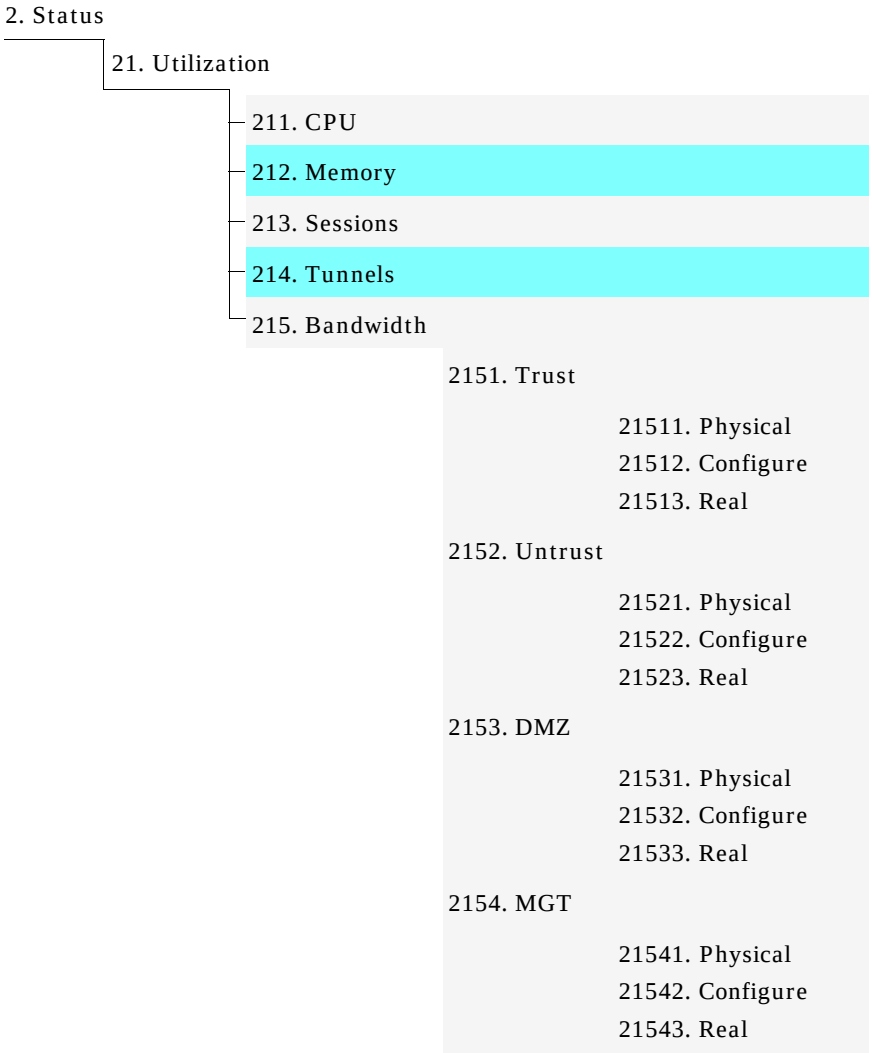
211. CPU (the percentage of the CPU currently in use)

212. Memory (the amounts of currently allocated and available—or free—memory)

213. Sessions (the total number of currently active user sessions)

214. Tunnels (the total number of currently active VPN tunnels)

215. Bandwidth (physical bandwidth, configured bandwidth, and real bandwidth—that is, the bandwidth currently in use)



Note: *Because the untrusted, DMZ, and MGT bandwidth options are identical to those for the trusted interface, the following descriptions of the trusted bandwidth options apply equally well to those for the other interfaces.*

211. CPU	Displays the percentage of the CPU currently engaged.
212. Memory	Displays two figures: the first is amount, in kilobytes, of allocated memory; the second is the amount of available memory remaining.(To see the second figure, scroll to the right.) To determine the total amount of memory, add these two figures together.
213. Sessions	Displays the number of currently active sessions.
214. Tunnels	Displays the number of currently active VPN tunnels.
215. Bandwidth	
2151. Trust	
21511. Physical	Displays the amount of bandwidth that the trusted interface is physically capable.
21512. Configure	Displays the amount of bandwidth that has been configured for the trusted interface.
21513. Free	Displays the amount of bandwidth currently in use.

22. Temperature

The Temperature branch is where you can view the current temperature of the NetScreen device.

1. Navigate to 2. Status >> 22. Temperature.
2. Press the RIGHT control key.

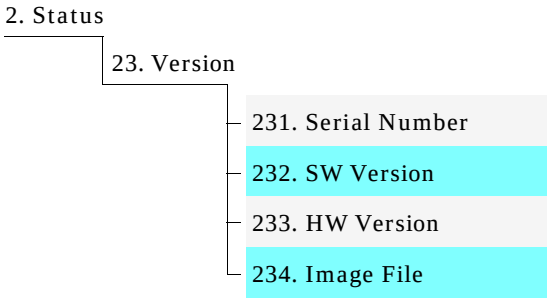
   The following display appears, where <xxx> is the temperature in Fahrenheit:

```
Temperature (‘F):
xxx
```

23. Version

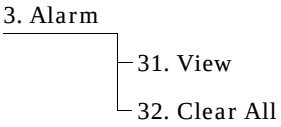
The Version branch is where you can view the following information:

- 231. Serial Number (the serial number of the device)
- 232. SW Version (the software version number and the checksum used to verify software authenticity)
- 233. HW Version (the hardware version number)
- 234. Image File (the image file name)



3. ALARM

The Alarm branch is where you can view alarm entries and clear entries from the event alarm log.



31. View

31. View

Displays the alarm entries in chronological order. Each entry consists of two lines of data:

- The first line of the entry states the date and time of the alarm in the format <mm/dd/yyyy mm:ss>
- The second line states the type of alarm (attack, system, HA), and provides a description of what occurred. Note that you can scroll to the right to read the entire description. You can press the UP or DOWN control key to return to the beginning of the entry.

32. Clear All

32. Clear All

To clear all entries from the event alarm log, do the following:

1. Press the RIGHT control key.

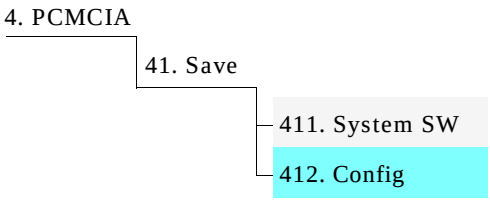
   The following display appears.

   ```
   32. Clear All
   No (<-) , Yes (->) ?
   ```

2. Press the RIGHT control key.

4. PCMCIA

The PCMCIA branch is where you can save the ScreenOS software or the current configuration to a PC card.



41. Save

411. System SW

To save the ScreenOS software to a PC card loaded in the PCMCIA slot, do the following:

1. Press the RIGHT control key.

   The following display appears.

```
411. System SW
No (<-) , Yes (->) ?
```

2. Press the RIGHT control key.

412. Config

To save the current configuration to a PC card loaded in the PCMCIA slot, do the following:

1. Press the RIGHT control key.

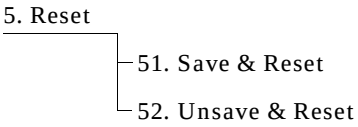
   The following display appears.

```
412. Config
No (<-) , Yes (->) ?
```

2. Press the RIGHT control key.

5. RESET

The Reset branch is where you can either save the configuration and reset the device, or reset the device without saving any recent changes to the configuration.



51. Save & Reset

51. Save & Reset

To save the current configuration and reset the device, do the following:

1. Press the RIGHT control key.

   The following display appears.

   ```
   51. Save & Reset
   No (<-) , Yes (->) ?
   ```

2. Press the RIGHT control key.

52. Unsave & Reset

52. Unsave & Reset

To reset the device without saving the current configuration, do the following:

1. Press the RIGHT control key.

   The following display appears.

   ```
   52. Unsave & Reset
   No (<-) , Yes (->) ?
   ```

2. Press the RIGHT control key.

6. EXIT

Use the Exit branch to exit the menu system and return to the default display.

1. Navigate to 6. Exit.
2. Press the RIGHT control key.

   The default display appears, as shown below where <X> is the number of sessions and <Y> is the number of tunnels.

Safety Recommendations and Warnings

B

SAFETY RECOMMENDATIONS AND WARNINGS

This section describes the safety guidelines to follow when operating the NetScreen-500.

GENERAL GUIDELINES

Keep these important guidelines in mind when installing or operating the NetScreen-500.

- Make sure that the work area is dry and is not excessively humid.
- Keep the chassis area clear and dust-free during and after installation.
- Disconnect all power supply connections before:
  - changing the Ethernet or serial port connection
  - removing a chassis
  - changing a fuse
- *Always* ensure that power is disconnected from a circuit.
- Use all the mounting hardware included in the NetScreen-500 product package.
- Do not work alone if potentially hazardous conditions exist.
- Examine the area for possible hazards, such as moist floors, ungrounded power extension cables, frayed power cords, and missing safety grounds

IMPORTANT WARNINGS

Ensure that strict attention is paid to these warnings during installation and maintenance.

⚠ Warning *Do not perform any action that creates a potential hazard to people or renders the equipment unsafe. Do not stack or balance the equipment on other devices to avoid tripping over cords and cables, and to allow air circulation. Confirm that the installation is secure.*

Before Supplying Power

Read the installation instructions carefully before connecting the NetScreen-500 to its power source.

Examine the work area for possible hazards, such as moist floors, ungrounded power extension cables, and missing safety grounds.

Locate the emergency power-off switch for the room.

⚠ Warning *Carefully read the installation instructions before connecting the NetScreen-500 to its power source.*

No User-Serviceable Parts Warning

⚠ Warning *The NetScreen-500 has no user-serviceable parts and is housed in a tamper-proof enclosure. Opening the chassis for any reason voids the NetScreen-500's warranty.*

Product Disposal Warning

⚠ Warning *Handle ultimate disposal of the NetScreen-500 according to all national and local laws and regulations.*

Power Disconnection Warning

⚠ Warning *Before working on a system that has an On/Off switch, turn the power off and unplug the power cord.*

Circuit Breaker (15A) Warning

⚠ Warning *The NetScreen-500 relies on the building's installation for short-circuit (over-current) protection. Use a fuse or circuit breaker no larger than 120 VAC, 15A U.S. (240 VAC, 10A international) on the phase conductor (all current-carrying conductors).*

SELV Circuit Warning

⚠ Warning *The Ethernet 10BaseT, 100BaseT, serial, console, and auxiliary ports have safety extra-low voltage (SELV) circuits. Do not connect to a telephone line or any Telco line (e.g., T-1, T-3, RJ-48 lines).*

Lightning Warning

⚠ Warning *Do not manipulate cables on the NetScreen-500 during lightning storms.*

GENERAL SITE REQUIREMENTS

The site must meet these requirements to allow safe installation and operation of the NetScreen-500. Verify that the site meets these requirements before beginning the hardware installation.

Site Environment

The NetScreen-500 may be placed on a desktop or mounted in a rack. The location of the chassis and the layout of the equipment rack or wiring room are extremely important for proper device operation. Equipment placed too closely results in inadequate ventilation.In addition, the NetScreen-500 cannot be accessed easily for maintenance when malfunctions and shutdowns occur.

To avoid equipment failures and reduce the possibility of shutdowns resulting from environmental conditions.

Important: *The NetScreen-500 requires adequate air circulation. Natural air temperature might not be sufficient to cool equipment sufficiently; add an additional circulation system if necessary.*

Configuring Equipment Racks

Keep this information in mind when planning an acceptable equipment rack configuration.

- Enclosed racks must have adequate ventilation. Ensure that the rack is not overcrowded, because each unit generates heat. An enclosed rack should have louvered sides and a fan to provide cooling.
- When mounting a chassis in an open rack, make sure that the rack frame does not block the intake or exhaust ports on the NetScreen-500. If the chassis is installed on slides, check the position of the chassis to be certain it is seated all the way into the rack.
- In an enclosed rack with a ventilation fan in the top, excessive heat generated by equipment near the bottom of the rack can be drawn upward and into the intake ports of the equipment above it in the rack. Ensure that there is adequate ventilation for equipment at the bottom of the rack.
- Baffles can help isolate exhaust air from intake air, which helps draw cooling air through the chassis. Try different arrangements to determine the best placement of the baffles considering the airflow patterns in the rack.

Power Supply Considerations

Check the power at the site to ensure that it is “clean” (free of spikes and noise). Install a power conditioner if necessary.

Environmental Requirements in an Office Environment

The NetScreen-500 may be operated in a standard office environment. For environments in which more extreme conditions exist, verify that the temperature, humidity, and power conditions meet the specifications indicated below.

Item	Operating Specification
Temperature	32-122°F, 0- 40°C
Relative humidity	5-90%, non-condensing: for storage 10-90%, non-condensing: for operation
Voltage AC	85-263 VAC
Voltage DC	36-72 VDC (isolated)
Input frequency	36-63 Hz
AC input current	1A (120VAC), 0.5A (240VAC)
Altitude	0-12,000 feet, 0-3,660 meters
Maximum power consumption	100 Watts per system (If one power supply is active, it uses 100 watts. If two power supplies are active, they divide the 100 watts between them.)

BSMI Labeling Requirement

The Bureau of Standards Metrology and Inspection (BSMI) is an agency of the government of China (Taiwan), which requires the following label on technological equipment:

Index

A

administration
- admin IP (LCD) A-5
- NetScreen-Global Manager A-5

alarms
- clearing (LCD) A-19
- viewing (LCD) A-19

asset recovery 4-19
Audible Alarm, enabling/disabling A-11

B

bandwidth A-17
BSMI labeling requirement B-5

C

cabling
- network interfaces 3-3
- power supply 3-2, 3-5

CLI, conventions xiii
configuration
- saving (LCD) A-21
- saving to PC card (CLI) 1-8
- saving to PC card (LCD) A-20

console
- changing timeout 4-9
- initiating a session 4-9

console port 1-8
- connecting to 4-9

control pad 1-2
- locking keys A-14

conventions
- CLI xiii
- menu system xv
- WebUI xii

CPU A-17

E

environmental requirements, office B-5
equipment racks, configuring B-4
exiting menu system A-22

F

fan assembly 1-10, 2-13– 2-14
FIPS ix, xi

H

HA 3-4– 3-6
- cabling 3-4
- ports 1-9
- secondary path 3-5
- verifying configuration 4-17, 4-18

I

image file name, viewing (LCD) A-18
interface
- configuring (CLI) 4-10
- configuring (LCD) A-6– A-8
- configuring (WebUI) 4-5

interface modules 2-2– 2-7
- indicator LEDs 1-7
- inserting 2-3
- removing 2-6

L

LCD
- menu system A-1– A-22
- turning off display A-14

LEDs
- ALARM 1-3
- FAN 1-4, 2-13
- FW 1-4
- HA 1-4

Link Status 1-6
PCMCIA 1-4
PWR 1 1-4
PWR 2 1-4
SESSION 1-4
SHAPE 1-5
STATUS 1-3
TEMP 1-4
VPN 1-4
login name
changing (CLI) 4-11
changing (WebUI) 4-8

M

memory utilization A-17
menu system 1-2, A-1– A-22
alarm A-1, A-19
conventions xv
exit A-1, A-22
PCMCIA A-1, A-20
reset A-1, A-21
setting A-1
status A-1, A-15
MGT port 1-8
modem port 1-8

N

NAT mode 4-2
NetScreen-Global Manager A-5

O

On/Off switch 1-10

P

password
changing (CLI) 4-11
changing (WebUI) 4-8
forgetting 4-19
PC card 1-8
port number, setting (LCD) A-4
ports
console 1-8
HA 1-9
MGT 1-8
modem 1-8
power supplies 1-10, 2-15
AC 1-10, 2-15
AC, replacing 2-18– 2-19
considerations B-4
DC 1-10, 2-15
DC ground posts 2-17
DC terminal blocks 2-17
DC, replacing 2-20
DC, wiring 2-16

R

rack mounting
front-mount 2-9
mid-mount 2-10
rear and front mount 2-11
rear slide mount kit 2-8
reset 4-19
resetting device (LCD) A-21
Route mode 4-2

S

serial number A-18
sessions A-17
site requirements, environment B-3
software
saving to PC card (CLI) 1-8
saving to PC card (LCD) A-20
Status LEDs 1-6
system IP
setting (CLI) 4-10
setting (LCD) A-4
setting (WebUI) 4-3

T

temperature
- setting thresholds A-12
- viewing (LCD) A-17

time/date, setting (LCD) A-9– A-11
Transparent mode 4-2

U

utilization
- allocated memory A-17
- available memory A-17
- bandwidth A-17
- CPU A-17
- sessions A-17
- VPN tunnels A-17

V

version numbers
- hardware A-18
- software A-18

VPN tunnels A-17

W

warnings B-1
- circuit breakers (15A) B-2
- lightning activity B-3
- no user-serviceable parts B-2
- power disconnection B-2
- product disposal B-2
- SELV circuit B-3
- supplying power B-2

WebUI, conventions xii