NETSCREEN-1000

Installer's Guide

Version 2.6.0 P/N 093-0044-000 Rev. D

Copyright Notice

NetScreen Technologies, Inc.
350 Oakmead Parkway, Suite 500
Sunnyvale, CA 94085 U.S.A.
www.netscreen.com

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.

Licenses, Copyrights, and Trademarks

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 “Software” includes all NetScreen and third party Software provided to you with the NetScreen product, and includes any accompanying documentation, any updates and enhancements of the 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 Software in accordance with the terms set forth in this License Agreement. The Software is “in use” on the product when it is loaded into temporary memory (i.e. RAM).

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

3. Transfer. You may transfer (not rent or lease) the 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 and title and interest in and to, and all intellectual property rights, including copyrights, to the software, and documentation, remain with NetScreen. You acknowledge that no title to the intellectual property in the Software is transferred to you and you will not acquire any rights to the Software except for the license as specifically set forth herein.

5. Term and Termination. The term of the license is for the duration of NetScreen's copyright in the 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 ninety (90) days after delivery to Customer, NetScreen will repair or replace any defective software product shipped to Customer, provided it is returned to NetScreen at Customer's expense within that period. 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 commercially reasonable 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 HEREIN 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 SOFTWARE. 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 SOFTWARE. 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 Software is subject to export control laws and regulations. YOU MAY NOT DOWNLOAD OR OTHERWISE EXPORT OR RE-EXPORT THE SOFTWARE 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 Software, and (b) if acquired by or on behalf of units of the Department of Defense ("DoD") shall be subject to terms of this commercial computer Software 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 Software 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.

Table of Contents

Preface

This manual provides NetScreen-1000 users with a guide to installing and maintaining the NetScreen-1000 network security system.

The NetScreen-1000 is an extremely fast, high volume, high availability network security system that provides a firewall and VPN solution running at gigabit speeds. Using a NetScreen-1000 you can implement up to 100 virtual systems (with a software key). Each virtual system appears to be its own system, with independent addresses, VPNs, access policies, and administrators.

The NetScreen-1000 is supplied with the following components:

- Dual gigabit trusted, untrusted, and HA ports
- An eight-slot modular chassis
- Dual hot-swappable, load-sharing power supplies
- Redundant fans in a fan assembly with failure alarms
- Flash memory and two PCMCIA card slots to store images, configurations, and event, traffic, and self logs

The NetScreen-1000 also has 10/100-Mbps “out-of-band” management capability that allows a system administrator to log in and manage the device from anywhere on an internal local area network (LAN) without interfering with the traffic on the trusted and untrusted interfaces.

You can configure and manage the NetScreen-1000 from a local console or a remote console (through a modem connection), or via a network connection using Secure Command Shell (SCS), a VPN tunnel, Secure Sockets Layer (SSL), Telnet, or HTTP.

Cabling two NetScreen-1000 devices together, you can configure them for high availability (HA). One device acts as the master and the other as its backup. The master processes all the traffic. The backup maintains the master's configuration settings and mirrors all the run-time objects. Should the master fail, the backup can take over all the master's firewall and VPN functions while maintaining uninterrupted service.

MANUAL ORGANIZATION

This manual has four chapters and one appendix.

Chapter 1, "Hardware Description," identifies and explains the various hardware components on the NetScreen-1000 device—auxiliary board, switch module, processor modules, LEDs, network and management ports, power supplies, and fan assembly.

Chapter 2, "Hardware Setup and Maintenance," explains how to install, replace, and maintain the modules, cables, power supplies, and fans in the NetScreen-1000 chassis. It also provides instructions for mounting the cover and two methods for rack-mounting the device.

Chapter 3, "Connecting to the Network," details how to connect the NetScreen-1000 to a network as a single unit, or—with another NetScreen-1000 device—for high availability (HA).

Chapter 4, "Initial Configuration," explains how to perform a basic configuration of the NetScreen-1000, defining its operational mode and interface settings, changing the default login name and password, creating a basic outgoing access policy, and checking that it is configured properly. The configuration for a single NetScreen-1000 device is followed by that for a pair of devices in an HA grouping.

Appendix A, "Safety Recommendations and Warnings," provides general site requirements as well as safety warnings and general cautions when installing and using the NetScreen-1000 device.

RELATED PUBLICATIONS

The following publications are available on the documentation CD included with the NetScreen-1000:

- **NetScreen Concepts & Examples ScreenOS Reference Guide**: A guide to the ScreenOS™ used to manage the NetScreen-5, -5XP, -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 WebUI features for the NetScreen-5, -5XP, -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-1000 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.

If you plan to administer NetScreen-1000 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 two management methods for configuring a NetScreen device: the Web user interface (WebUI) and the command line interface (CLI). The writing conventions used for these methods are introduced below.

WebUI Conventions

The WebUI consists of two main logical sections: the menu column and the central display area.

- The menu column consists of four main functional categories:
  - System
  - Network
  - Lists
  - Monitor

  Each functional category contains sub-functions, represented by tabs in the central display area. During configuration, you first select a main functional category, then choose one of the utilities offered within its sub-categories.

- The central display area lists the information for each of the categories in the menu column. The pages display configuration settings and provide options and links to dialog boxes where you can configure system, firewall, VPN, and traffic-shaping elements.

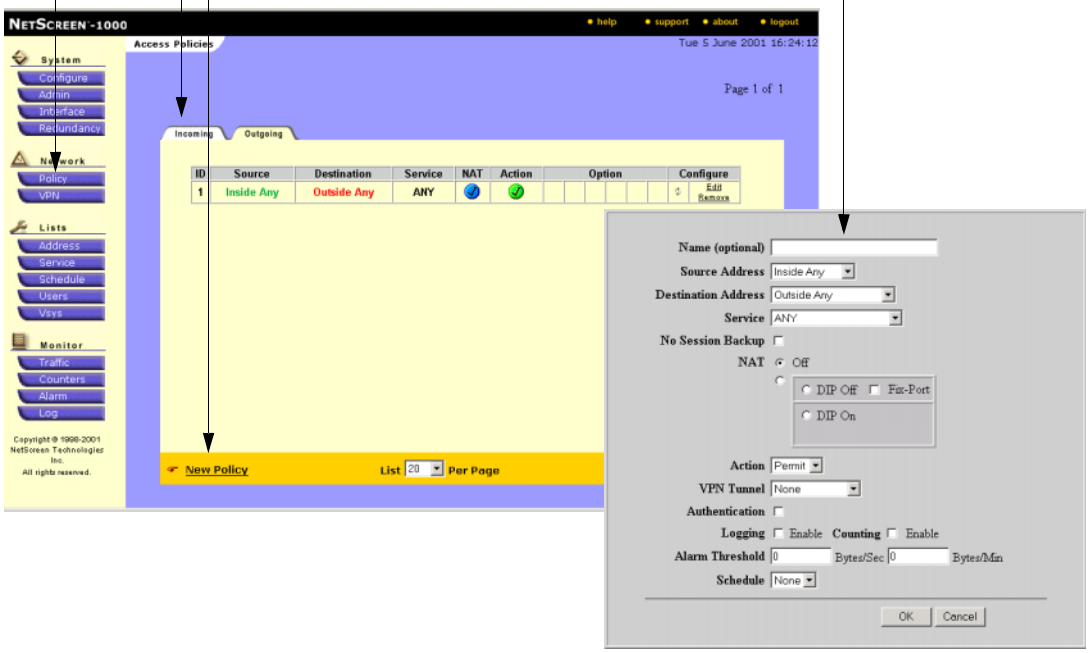
Throughout this book, a double chevron (>>) is used to indicate navigation through the WebUI by clicking buttons, tabs, and links. For example:

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 }** means "choose the trusted or untrusted 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 | 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 an address, the default gateway 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****.*

1. The **metric <number>** argument specifies the number of hops between the NetScreen-1000 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-1000 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, 2000, or NT: 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, 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 documentation CD.

Hardware Description 1

The NetScreen-1000 is a 50-pound rack-mountable unit containing the following hardware components:

- A circuit board cage housing three kinds of circuit boards
  - 1 switch II module
  - 1 auxiliary module
  - 2–6 processor modules
- Dual AC or DC power supplies
- A fan assembly unit equipped with three fans

This chapter contains detailed illustrations and descriptions of each of these components in the following sections:

MAIN CHASSIS

The main chassis of the NetScreen-1000 is a standard compact peripheral component interconnect (PCI) unit with room for eight circuit boards, or modules, as shown in Figure 1-1. The backplane inside the cage supplies power and system communication links to the modules. The ports are available on the front of each module for convenient cabling access.

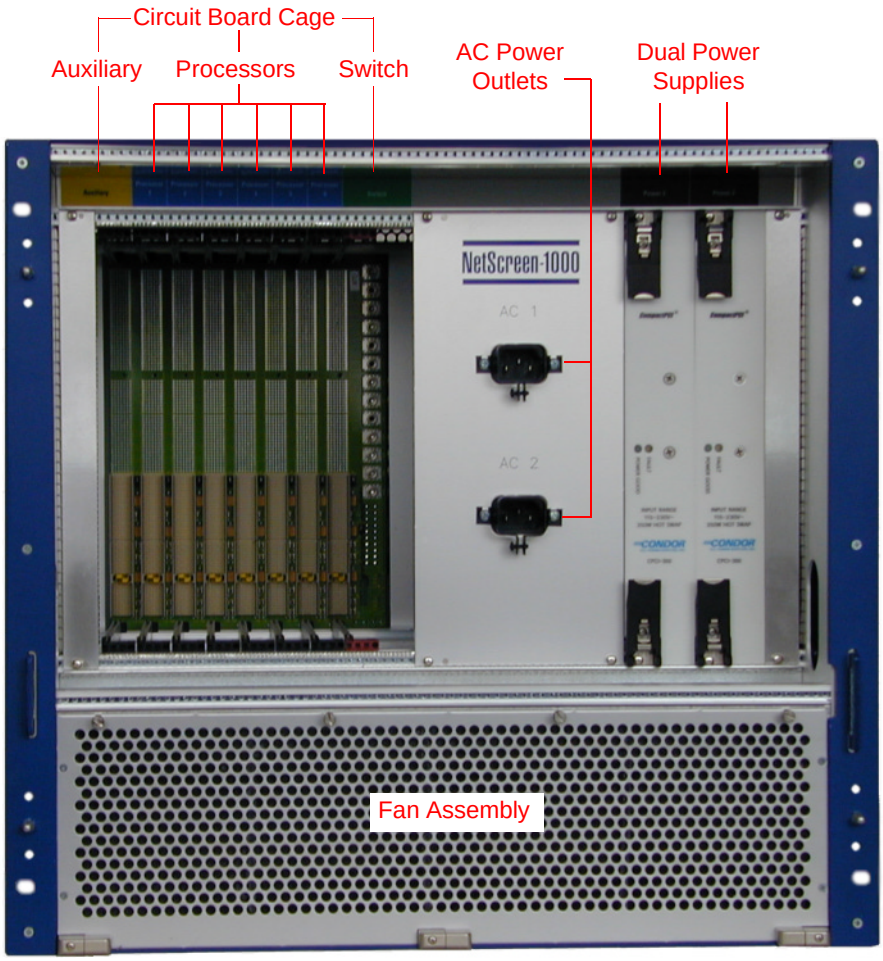


Figure 1-1 The NetScreen-1000 with Backplane Exposed

CIRCUIT BOARD CAGE

The NetScreen-1000 circuit board cage contains 8 labeled and color-coded circuit board slots.

- The auxiliary module is inserted in the yellow slot on the far left.
- Processor modules can be inserted in the blue slots, 1 through 6[1].
- The switch II module is inserted in the green slot on the far right.

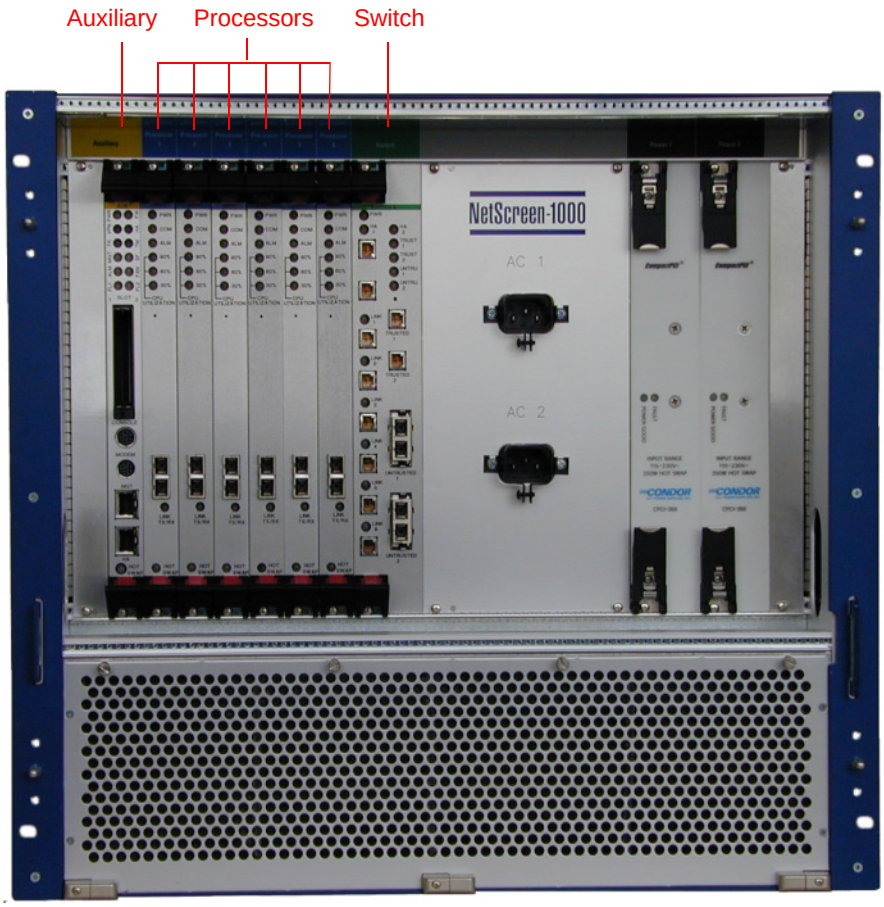


Figure 1-2 The NetScreen-1000 with Circuit Boards Loaded

1. You can cover unoccupied slots with filler panels to promote air flow and enhance air filtering.

Auxiliary Module

The auxiliary module provides the NetScreen-1000 with management interfaces; PCMCIA slots for uploading software images, for uploading and downloading configurations, and for saving log information; and an HA interface for high availability functions.

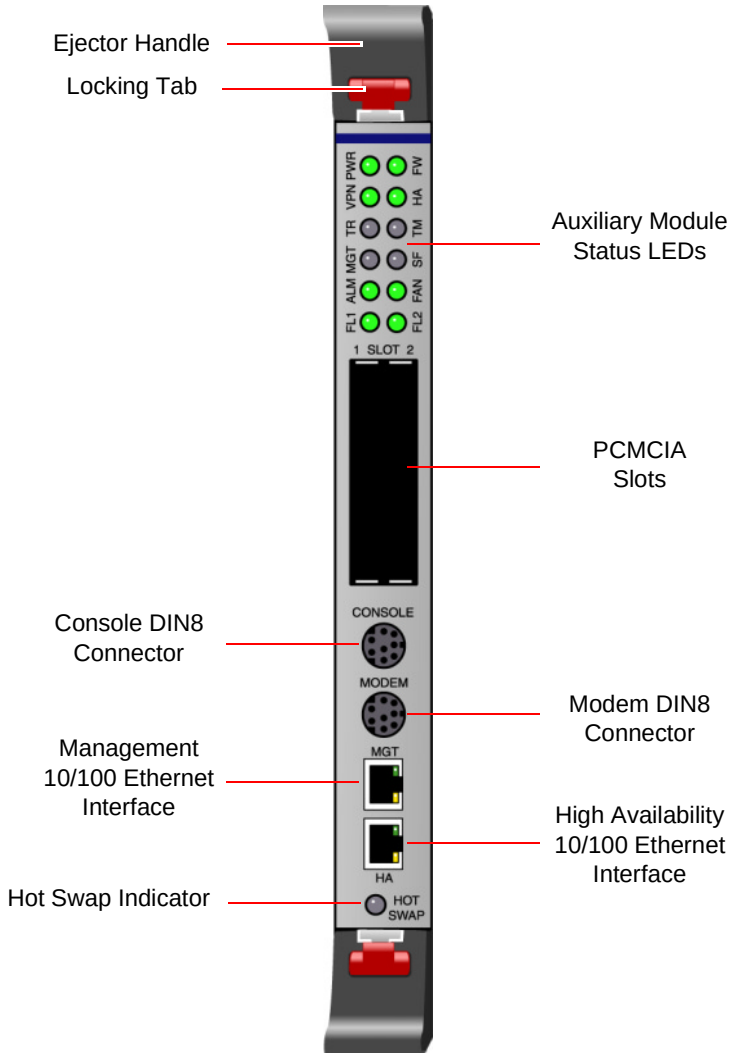


Figure 1-3 The Auxiliary Module Interface and Connections

Auxiliary Module Status LEDs

The auxiliary module status LEDs provide information about various critical functions. The meanings of the auxiliary module LEDs are as follows:

LED	Purpose	Color	Meaning
PWR	Power	**Green**	Board has power.
FW	Firewall Alarm	**Red**	Firewall event has occurred.
VPN	VPN	**Blinking Green**	VPN activity present.
		Yellow	VPN has been dropped or denied.
HA	High Availability	**Green**	Unit is master.
		Yellow	Unit is backup.
TR	Traffic Alarm	**Yellow**	Traffic exceeds threshold.
TM	Traffic Monitor	**Yellow**	Packets have been dropped.
MGT	Management	**Green**	A management session is in progress.
SF	Session Failure	**Blinking Yellow**	Policy enforcement or routing has failed, or the session table is full. Stays yellow for the duration of the session-full condition.
ALM	System Alarm	**Red**	Critical Alarm—Crash or system component failure.
		Yellow	Major Alarm—Low memory.
FAN	Fan	**Red**	Fan failure.
FL1	Flash Card 1	**Green**	PC card is installed in slot 1.
		Blinking Red	PC card is full or has an error.
FL2	Flash Card 2	**Green**	PC card is installed in slot 2.
		Blinking Red	PC card is full or has an error.

PCMCIA Slots

The auxiliary module houses two 96-MB PCMCIA slots—slot 1 and slot 2, as shown in Figure 1-3 on page 1-4. The card in slots 1 or 2 can store the system image and configuration settings. You can upload the system image or configuration settings from a PC card in either slot to flash memory and download a configuration from flash to a PC card in either slot. The card in slot 1 can also store logs.

You can determine the location of the image from which the NetScreen-1000 boots up as either slot 1 or slot 2 by using the **set envar** command: **set envar boot=slot1:image** or **set envar boot=slot2:image**. When booting up, the system first checks for a system image on a PC card in the specified PCMCIA slot. If the NetScreen-1000 is unable to boot from the PC card in that slot, it then boots from the image stored in its internal flash memory.

Note: *You can download either the system image or configuration from a Trivial File Transfer Protocol (TFTP) server to either flash memory or to a PC card.*

Management Interfaces

You can manage and configure the NetScreen-1000 through either or both of the DIN-8 serial ports—console or modem—located on the auxiliary module, as shown in Figure 1-3 on page 1-4. The console port functions identically to the modem port except that you can download a system image to a TFTP server only via the console port.

For local configuration and management, cable the console port to the serial port on the administrator's workstation. For remote configuration and management, cable the modem port to a modem[2].

The Management (MGT) port provides a dedicated connection for management traffic. To manage the device through the MGT port, you need a network connection. The management port has a 10/100 Base-T interface and provides a dedicated connection for management traffic. It has a separate address and netmask, configurable via the CLI and WebUI.

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

HA Interface

The high availability (HA) port on the auxiliary module provides a 10/100 Base-T interface for passing HA communications between the local device and one or more other NetScreen-1000 devices in a redundant cluster. In the cluster, one device acts as master, processing all the firewall and VPN traffic. The other members in the cluster are in hot standby mode, ready to take over the processing if the master fails.

To provide uninterrupted service in the event of a failover, the HA feature consists of the following three main functions:

- Mirroring configuration settings among all members in the redundant cluster
- Maintaining all currently active network and VPN session tables on both the master and standby systems
- Monitoring the status of all members in the cluster and applying a failover algorithm to select the next master when necessary

Note: *For more information about using HA, see* *"Connecting the NetScreen-1000 for High Availability" on page 3-3*, *"HA Configuration" on page 4-13*, *and the HA chapter in the* NetScreen Concepts & Examples ScreenOS Reference Guide.

Processor Modules

The processor modules (see Figure 1-4) perform most of the NetScreen-1000 system functions. You can use from two to six processor modules. One module acts as the master processor, and the remaining processor modules handle the packet processing. The more processors there are, the better the performance.

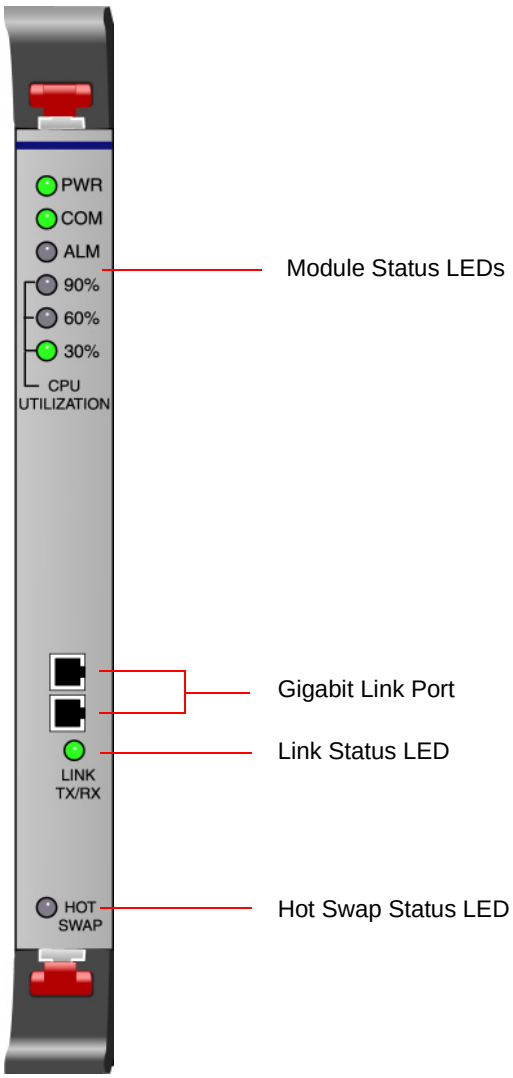


Figure 1-4 The Processor Module Interface LEDs and Connectors

The processor module with the lowest numerical value functions as the master; that is, if one module is in slot 1 and another is in slot 2, the module in slot 1 becomes the master. When the switch II module receives the first packet in a session, it sends it to the master processor for packet classification and policy lookup. The master processor inspects the packet and checks the access control list to determine which action, or actions, to take—permit, deny, encrypt, decrypt, authenticate. It then assigns the session to one of the other processor modules based on the processing required and the processing load that that module currently has. The master processor then notifies the switch II module to forward all subsequent packets in the session to that processor.

If the master processor fails, the processor module in the next numerically higher slot assumes the master function after the device restarts.

Processor Module Status LEDs

Each processor module has a series of six LEDs. The meanings of the processor module LEDs are as follows:

LED	Purpose	Color	Meaning
PWR	Power	**Green**	Module has power.
COM	Communication with master	**Blinking Green**	Module is communicating with the master processor module.
		Yellow	Module is unable to communicate with the master processor.
		Steady Green	Module is acting as the master processor.
ALM	Alarm	**Red**	Critical Alarm—Crash or major component failure.
		Yellow	Major Alarm—Low memory.
90%	Utilization	**Steady Yellow**	CPU utilization is greater than 90%.
60%	Utilization	**Steady Green**	CPU utilization is greater than 60%.
30%	Utilization	**Steady Green**	CPU utilization is greater than 30%.

Processor Module Gigabit Link Port

The processor module shown in Figure 1-4 on page 1-8 contains a gigabit link port that must be connected to one of the six processor module ports on the switch II module with a fiber optic cable.

Processor Module Link Status LED

The link status LED indicates activity on the gigabit link ports. If the link is receiving optical carrier but no traffic, the link status LED glows a steady green. If the link is receiving network traffic, it blinks green.

Processor Module Hot Swap LED

The hot swap LED on the bottom of the processor module shown in Figure 1-4 on page 1-8 is located directly above the lower ejector handle. The meanings of the Hot Swap LED states are as follows:

LED	Purpose	Color	Meaning
Hot Swap	State indicator	Dark	Normal operation
		Red	Module ejector handle has been released.
		Dark	OK to remove card

If more than two processors are in the chassis, you can change, or “hot swap”, any processor module other than the master without interruption to service. When you remove a processor module, all the sessions on that module, including VPN sessions, are redistributed to the remaining processors.

Note: *Plugging a new processor module into a slot from which you have removed a defective one and cabling it to the corresponding processor module port on the switch does not cause sessions that were on the failed module to be assigned to the new one.*

Switch II Module

The switch II module receives network and VPN traffic from the trusted and untrusted ports and directs it to the master processor module.

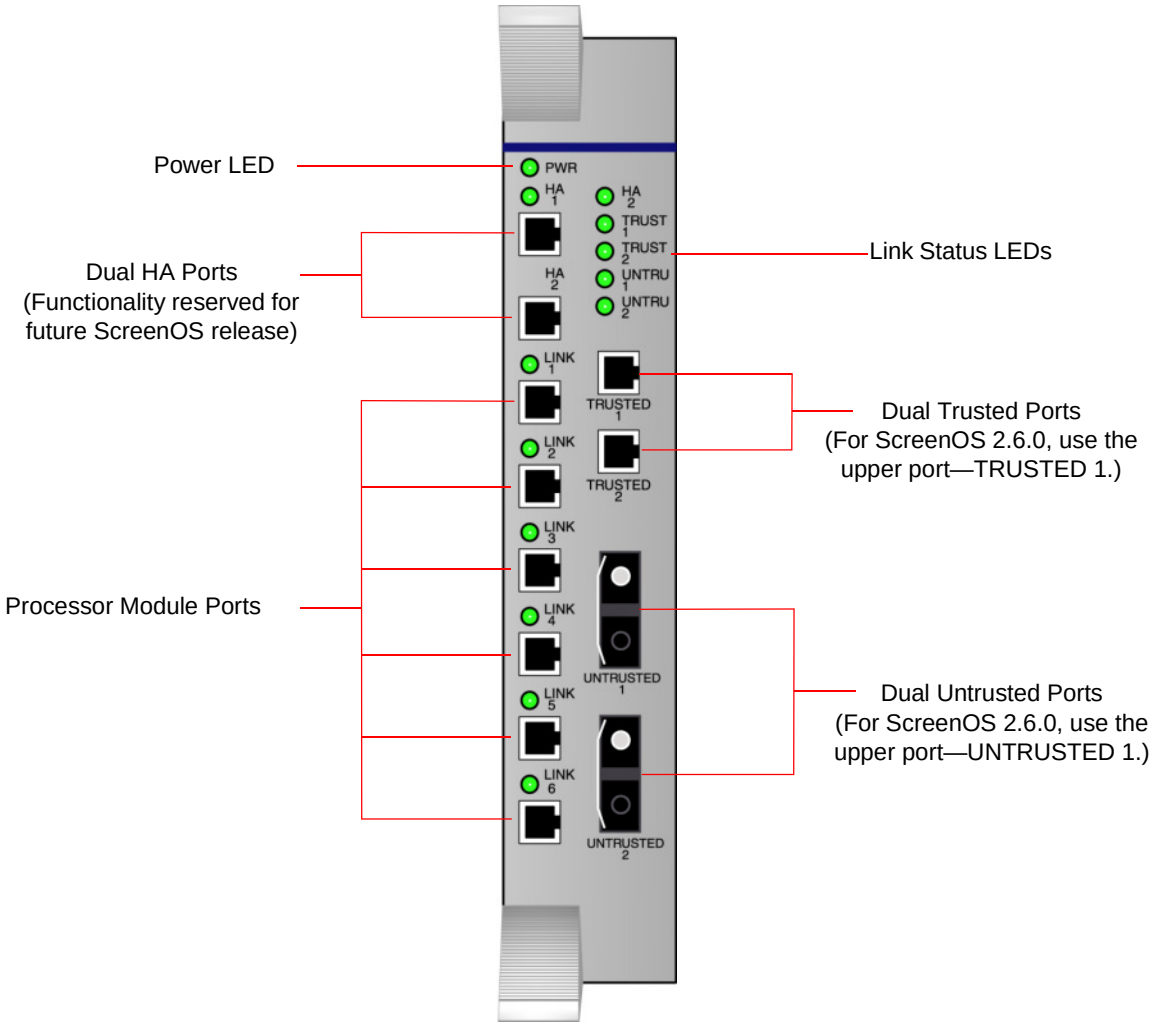


Figure 1-5 The Switch II Module Ports and LEDs

Switch II Module Status LEDs

The LEDs on the switch II module indicate the status of the gigabit links.

LED	Purpose	Color	Meaning
Power	Power reception	**Steady green**	Board receiving power
Link TX/RX	Traffic status	**Steady Green**	Link receiving optical carrier but no traffic
		Blinking green	Link receiving network traffic

Dual Trusted and Untrusted Ports

In a future release, NetScreen ScreenOS will provide support for redundant trusted and untrusted ports. For ScreenOS 2.6.0, use only the upper trusted port—TRUSTED 1—and the upper untrusted port—UNTRUSTED 1. The trusted ports host MT-RJ connectors. The untrusted ports host SC connectors. Both trusted and untrusted ports have SX transceivers.

Note: *The untrusted ports have removable GBIC transceivers. Although the default transceiver type is SX, optional LX transceivers are available for ordering.*

Dual HA Ports

The dual HA ports on the switch II module are reserved for a future ScreenOS release. For ScreenOS 2.6.0, use the HA port on the auxiliary module for HA communications. The HA ports host MT-RJ connectors with SX transceivers.

Note: *For HA cabling and software configuration, see "Connecting the NetScreen-1000 for High Availability" on page 3-3, and "HA Configuration" on page 4-13.*

Processor Module Ports

The processor module ports on the switch host connections between the processor modules and the switch. These connections require SC-to-MTRJ gigabit optical cables. Although system communications pass to the processor modules via the backplane, all traffic flows through the cabling. You must cable the processor modules to the ports corresponding to their slot positions on the switch II module.

POWER SUPPLIES

The NetScreen-1000 is equipped with two hot-swappable, load-sharing AC or DC power supplies. The power supplies are monitored by management software. If one of the installed power supplies fails, the other one automatically assumes the full load, and the NetScreen-1000 sends a system alarm and sets an SNMP trap.

You can specify the following voltage options:

- AC: 95–240 variable (47 to 63 Hz)
- DC: -48 Volts

Note: *For instructions on removing, installing, and cabling both AC and DC power supplies, see* *"Replacing Power Supplies" on page 2-16*.

AC Power Supplies

Figure 1-6 shows the NetScreen-1000 with dual AC power supplies installed.

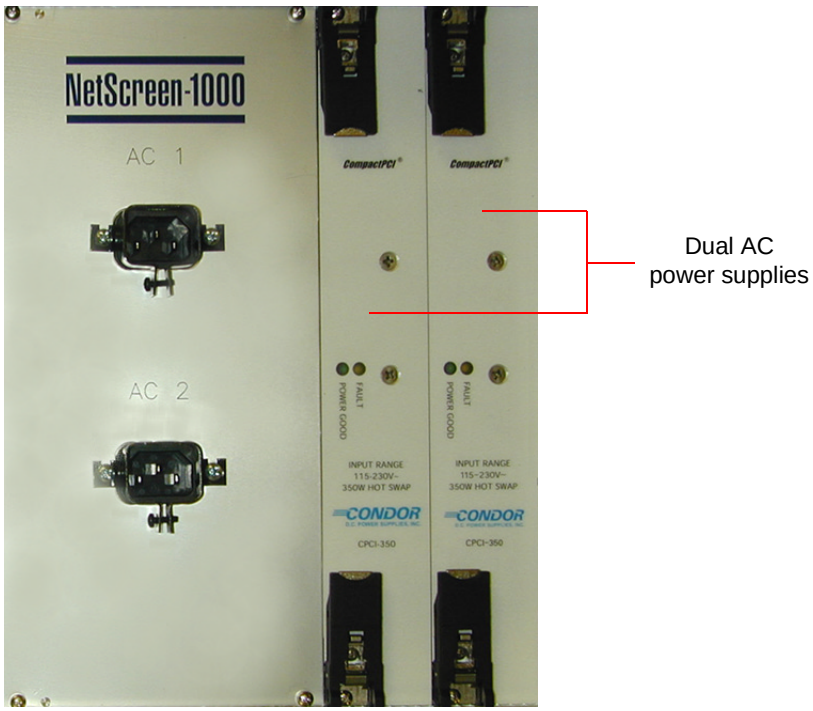


Figure 1-6 Dual AC Power Supplies

DC Power Supplies

The NetScreen-1000 can also be equipped with dual DC power supplies, which can operate on one or two DC feeds ranging from -36V to -72V. For DC power, you must connect wires from the DC power source to one or both of the terminal blocks located at the rear of the chassis. If you use two feeds, the dual power supplies share the load. If one feed fails, the other automatically assumes the full load.

The figure below shows the rear of the NetScreen-1000 chassis, with an on/off power switch, dual terminal blocks for two -48V DC feeds, and dual ground posts.

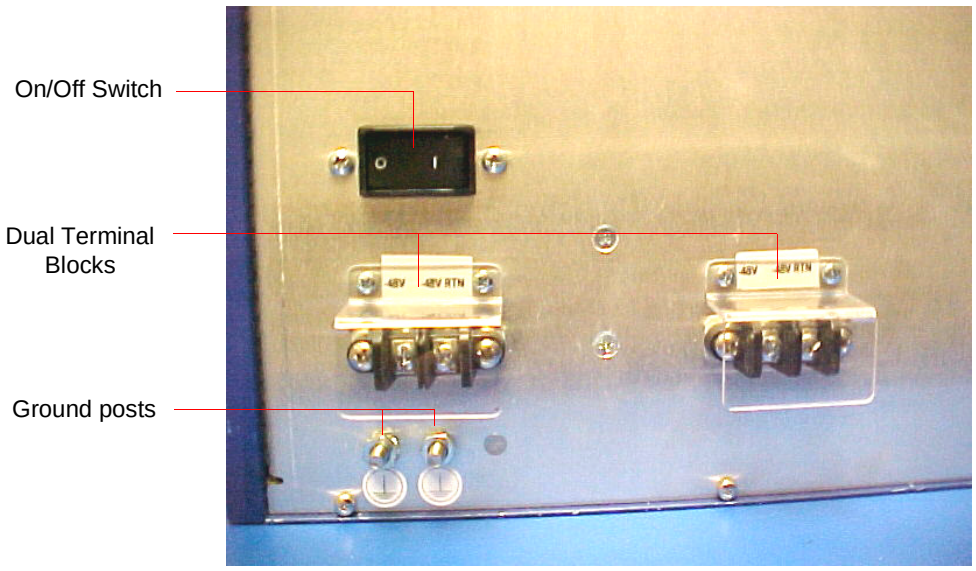


Figure 1-7 Figure: DC Power Terminal Blocks at Rear of Chassis

FANS

The NetScreen-1000 fan assembly, shown in Figure 1-8, contains three user-replaceable fans. Failure of any one of these fans generates an event alarm and sets an SNMP trap.

Figure 1-8 The NetScreen-1000 Fan Assembly Cage

Hardware Setup and Maintenance

2

Follow the procedures in this chapter to set up the NetScreen-1000 for operation. The first part of the chapter explains how to cable the processor modules to the switch II module, connect and secure the power cord, and mount and lock the cover.

In addition, this chapter also explains the following procedures:

BASIC OPERATIONAL REQUIREMENTS

For basic operation without the high availability (HA) option, the NetScreen-1000 needs the following modules and cables:

- 1 switch II module
- 1 auxiliary module
- 2 processor modules (minimum)
- MT-RJ to SC duplex optical cables—1 per processor module—to connect each processor to the switch II module
- 1 MT-RJ to SC optical cable[1] to connect the trusted port to the network
- 1 SC duplex to SC duplex to connect the untrusted port to the network

Note: *The untrusted ports have removable GBIC transceivers. The default transceiver type is SX. Optional LX transceivers are available for ordering.*

For operation of multiple NetScreen-1000 devices in an HA configuration, you also need a 10/100 BaseT cross-over cat5 cable for the HA link on the auxiliary module.

The on-site electrical requirements for AC and DC power supplies are as follows:

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

1. The network devices to which you connect the trusted and untrusted ports determine the cable connector types you require. The NetScreen-1000 trusted port requires an MT-RJ connector and the untrusted port requires an SC duplex connector. The ports on your network switches or routers might require you to use different cables than those provided.

GETTING STARTED

The unit ships with a lockable cover, on which the key is taped. To remove the cover, unlock it, grip the indented sections along the left and right sides, and pull toward yourself. The cover comes free from the ball studs on the left and right flanges.

Note: *For instructions on replacing the cover, see* *"Mounting and Locking the Cover" on page 2-7.*

The device ships with the modules already installed. For example, if you ordered a unit with six processor modules and AC power supplies, when you opened the cover, you would see the following:

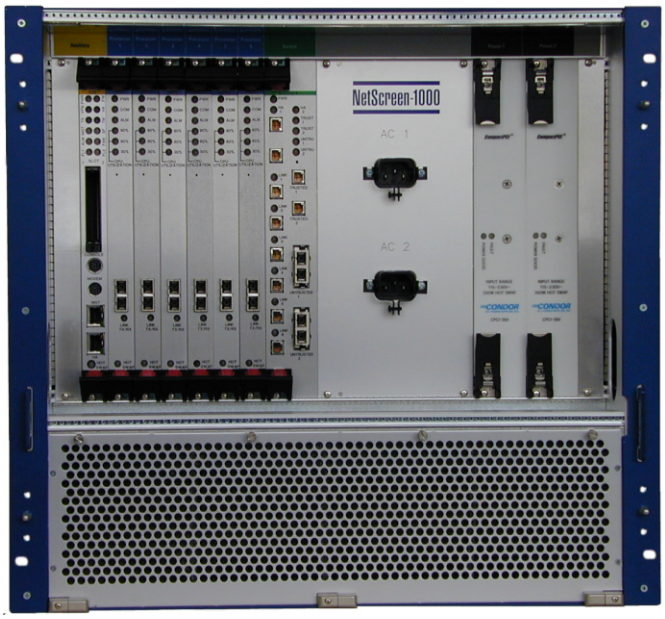


Figure 2-1 NetScreen-1000 (AC Version) with Cover Removed

CABLING THE PROCESSOR MODULES TO THE SWITCH II MODULE

There are six numbered ports on the switch II module, each corresponding to a numbered processor module slot. The cables must connect each processor module to the matching port on the switch II module.

Note: *Each port on the processor modules has two segments: a receive segment and a transmit segment. The SC duplex connector is keyed so that it can only be plugged in with the correct orientation.*

1. Connect processor module 1 to port 1 on the switch II module, as shown in Figure 2-2.

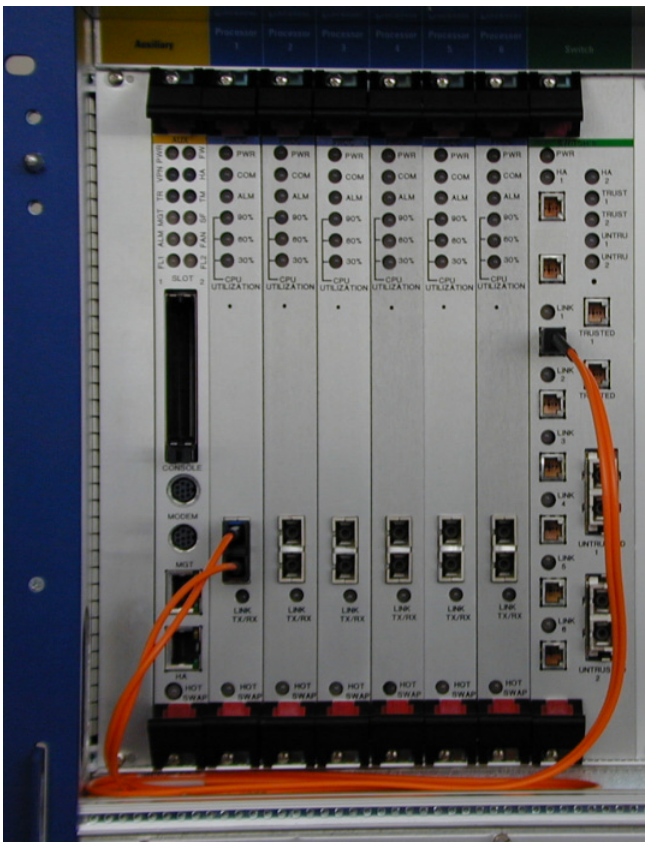


Figure 2-2 Cabling between Processor Module 1 and Port 1 on the Switch II Module

2. Connect processor module 2 to port 2.
3. Continue until all the modules are connected.
4. After the cabling is complete, lay the cables on the cable channel inside the chassis.

Note: *For cabling directions to connect the NetScreen-1000 device to the network as either a single security device or in a redundant series of devices for high availability (HA), see* *Chapter 3, "Connecting to the Network".*

SECURING THE AC POWER CORDS

When using AC power, the device powers up when you plug a power cord connected to a working power source into one of the AC sockets on the device. When you unplug both power cords from the device, it powers down. To prevent the cords from accidentally becoming unplugged, you can secure them by tightening the power cord retention brackets around the plugs.

⚠ Warning *Before installing any power cords, check to be sure that the voltage on the building's power source matches the voltage for which the NetScreen-1000 has been preconfigured: 95 to 240 Volts (AC) and -36 to -72 Volts (DC).*

1. Feed the two power cords that ship with the unit through the right cable access opening.
2. Plug them into the AC 1 and AC 2 sockets.
3. With a cross-head screwdriver, tighten the screw on the power cord retention brackets until the brackets close securely around the plugs.

Note: *If processor cables are connected to the switch II module, you might need to use a short-necked screwdriver or temporarily disconnect the cables to access the screws.*

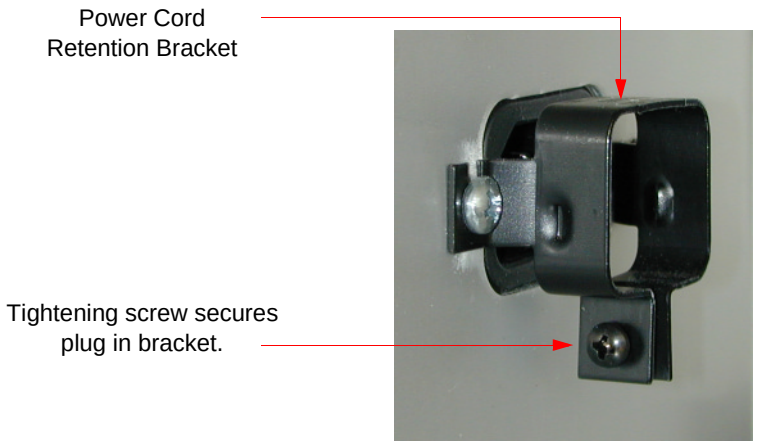


Figure 2-3 Power Cord Retention Bracket (Cord Removed for Clarity)

MOUNTING AND LOCKING THE COVER

No matter the quality of a firewall nor the careful design of its access control policies, if the device or devices protecting your network are not secure from physical attacks, your network security is incomplete. Physical access to the location where the NetScreen-1000 is kept should only be allowed by key network security personnel. To tighten physical security even further, you can mount and lock a cover on the front of the NetScreen-1000 device.

1. Align the four retaining clips on the inside of the cover with the four ball studs on the left and right flanges.

Closeup of a Retaining Clip from the Inside Cover

Ball Studs Located in Left and Right Flanges

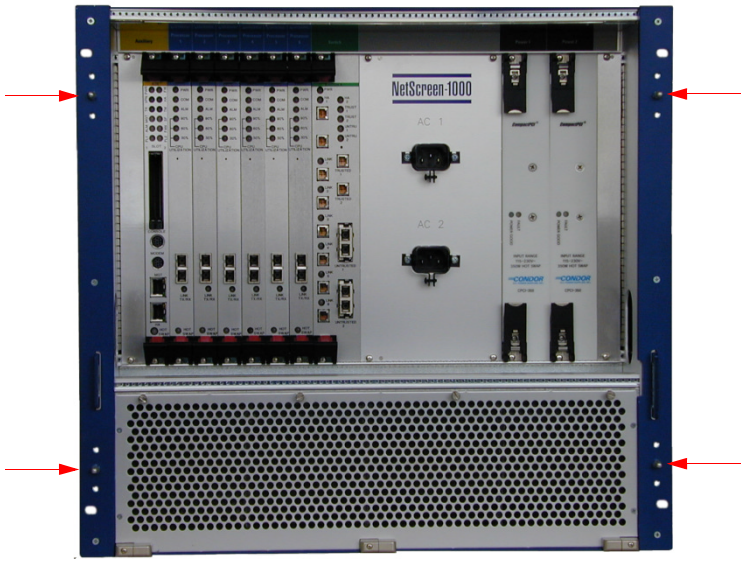


Figure 2-4 Cover Retaining Clips and Ball Studs on Chassis

2. Press firmly until the cover snaps in place.

3. Lock the cover with the key.

   When the cover is in place, the status LEDs are piped out through slots to remain visible.

Note that status LEDs are visible through slots in the cover.

Figure 2-5 NetScreen-1000 without and with Cover

REPLACING THE AUXILIARY MODULE

The auxiliary module is not hot-swappable. Before replacing the auxiliary module, make sure that the power is off. The replacement procedure is divided into two sections: the removal and the installation.

Removing the Auxiliary Module

1. With a cross-head screwdriver, loosen the screw above the upper ejector (shown in Figure 2-6) and the screw below the lower ejector on the auxiliary module.

   The screws are captive screws; that is, you can loosen them to remove the module without having to remove the screws completely.

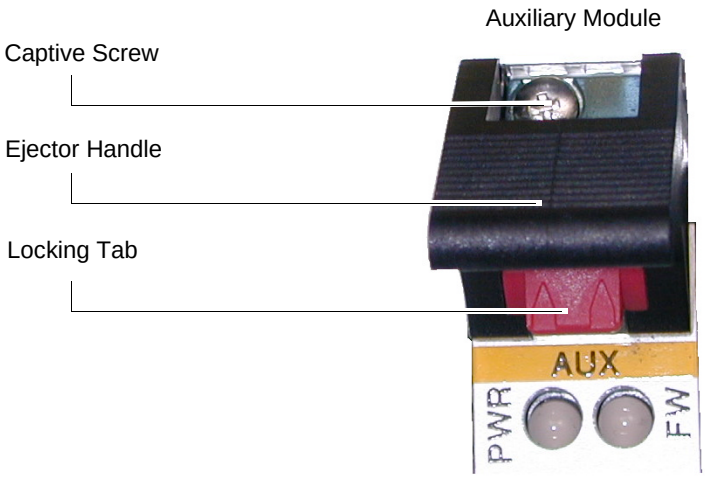
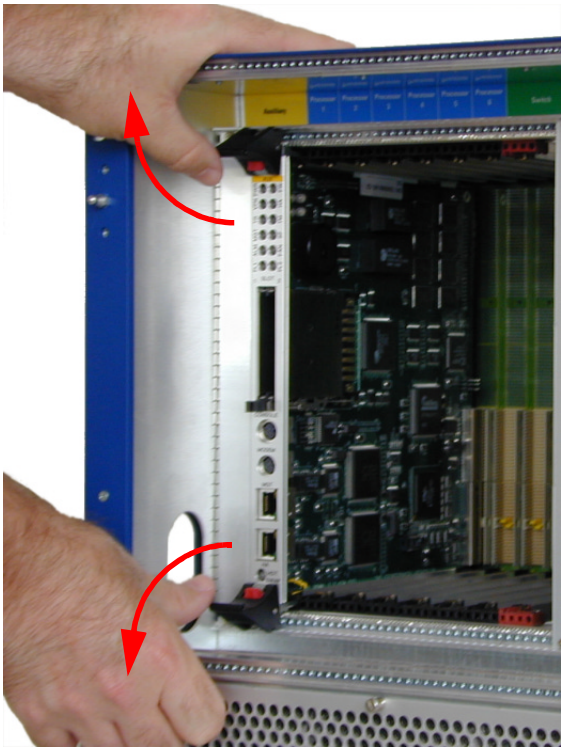


Figure 2-6 Auxiliary Module Upper Ejector

2. Open the ejector handles by pushing the red locking tabs into the handles.

3. Push the handles away from each other, causing them to pivot against the mounting rail and disconnecting the module from the backplane, as shown in Figure 2-7.

Lever the ejector handles away from each other to release the module from the backplane.



Note: For clarity, only the auxiliary module is shown.

Figure 2-7 Releasing the Auxiliary Module

4. Slide the module straight out.

Installing the Auxiliary Module

1. With the ejector handles open, align the upper and lower edges of the module with the upper and lower tracks at the far left of the circuit board cage.
2. Push the module gently into the Auxiliary slot until the ejectors contact the mounting rail at the edge of the circuit board cage.

   You can see a closeup of the lower ejector contacting the mounting rail in Figure 2-8 on page 2-11.

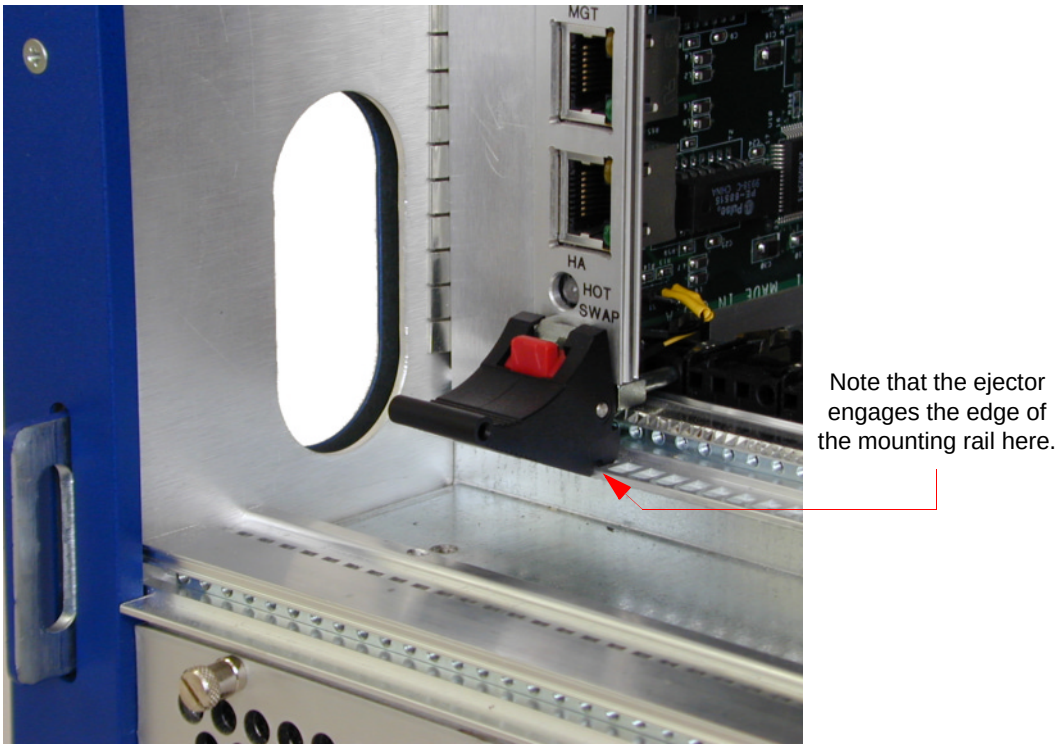


Figure 2-8 Inserting the Auxiliary Module

3. Pull the handles towards each other until the locking tabs snap into place, securing the auxiliary module in the slot.
4. Secure the auxiliary module in place by tightening the screws.

REPLACING PROCESSOR MODULES

The NetScreen-1000 device can house from two (minimum) to six (maximum) processor modules in the blue-labeled Processing slots. Each NetScreen-1000 device must have at least two processor modules—a master processor to manage packet assignments and another to do the processing.

Note: *The master processor is always the first processor on the left. If you have processors in all six slots, the processor in slot 1 is the master. If you have only two processors in slots 2 and 4, the processor in slot 2 is the master.*

Because the processor modules are hot-swappable, you can replace any processor other than the master during normal operations without disrupting service. Hot swapping processors requires at least three processors—a master and two others, one of which handles all the processing while the other is being replaced.

Removing a Processor Module

1. Disconnect the cable from the gigabit link port on the processor module that you want to remove.
2. With a cross-head screwdriver, loosen the screw above the upper ejector (shown in Figure 2-9) and the screw below the lower ejector of the processor module you are replacing.

   The screws are captive screws; that is, you can loosen them to remove the module without having to remove the screws completely.

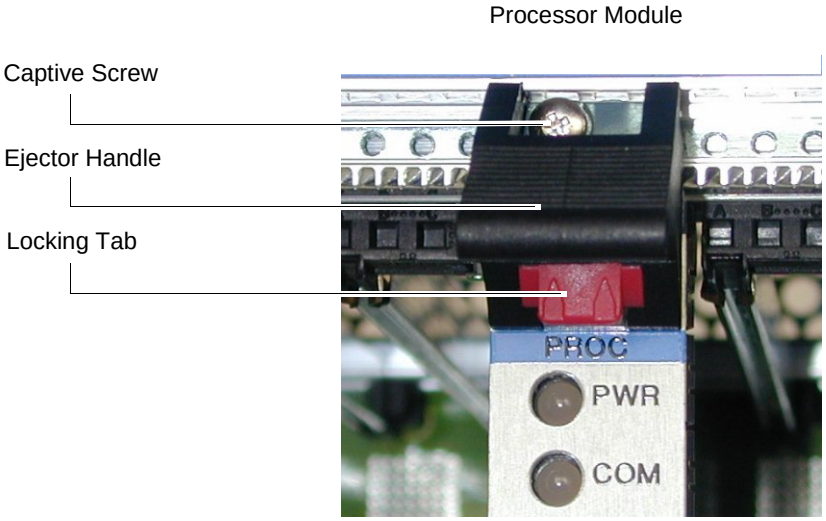


Figure 2-9 Processor Module Upper Ejector

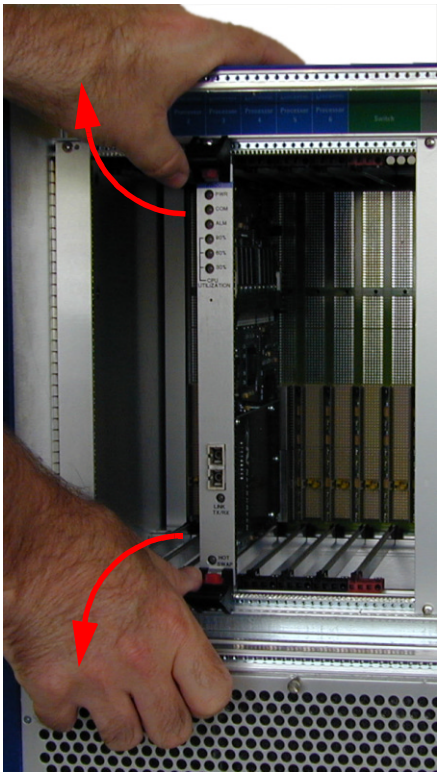
3. Open the ejector handles by pushing the red locking tabs into the handles.

   The Hot Swap LED changes from dark to red.

4. Push the handles away from each other, causing them to pivot against the mounting rail, disconnecting the module from the backplane, as shown in Figure 2-10.

   The Hot Swap LED changes from red to dark.

Lever the ejector handles away from each other to release the module from the backplane.



Note: For clarity, only a single processor module without cabling is shown in the circuit board cage.

Figure 2-10 Releasing the Processor Module

5. Slide the module straight out.

Installing a Processor Module

1. With the ejector handles open, align the upper and lower edges of the board with the upper and lower tracks at the far left of the circuit board cage.
2. Slide the module in, as shown in Figure 2-11, until the ejectors contact the mounting rail at the edge of the circuit board cage.

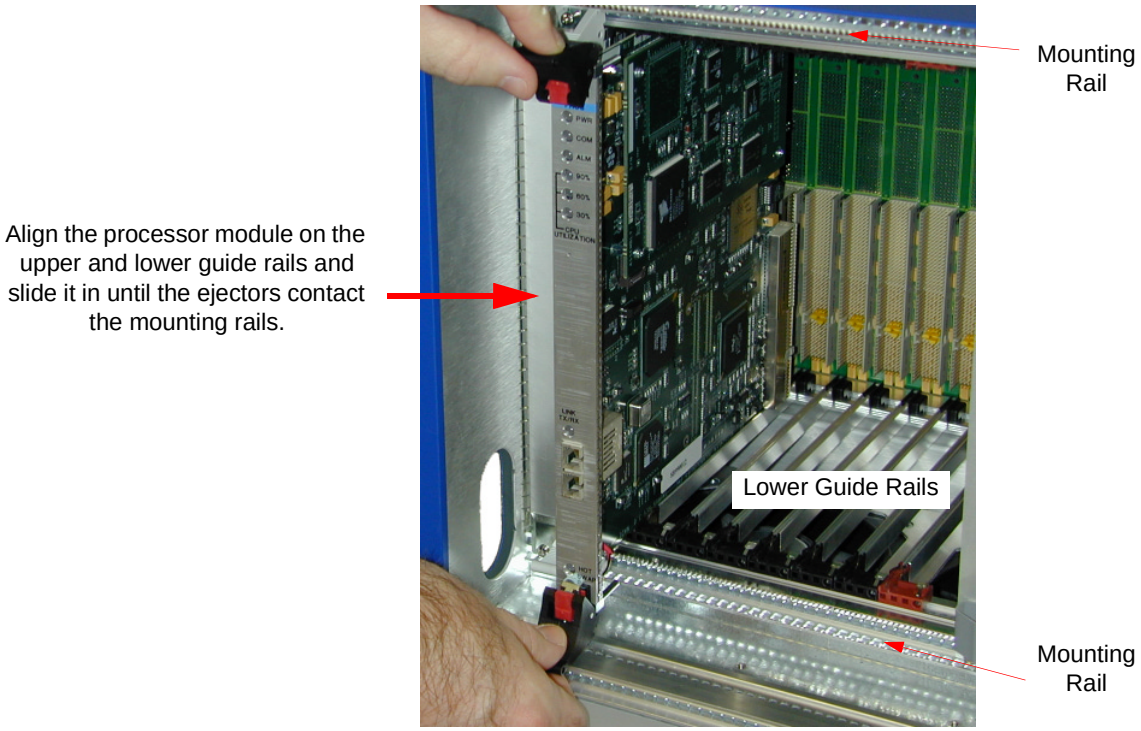


Figure 2-11 Installing a Processor Module

3. Press in firmly, then pull the ejectors toward each other until the locking tabs snap into place, securing the processor module in the slot.
4. Secure the processor module in place by tightening the screws above the upper ejector and below the lower ejector.
5. Reconnect the cable between the processor module and the switch II module.

REPLACING THE SWITCH II MODULE

The switch II module is not hot swappable. When replacing the switch II module, the NetScreen-1000 should not be actively connected to the network.

Removing the Switch II Module

1. Disconnect any processor cables running from the switch II module.
2. With a cross-head screwdriver, loosen the retaining screws in the upper and lower ejectors.
3. Pull the ejector handles away from each other, pivoting the upper and lower handles against the mounting rails to disconnect the switch from the backplane.
4. Gripping both ejector handles, pull the switch II module straight out.

Installing the Switch II Module

1. Align the upper and lower edges of the switch II module with the guide tracks.
2. Slide the module in until the ejectors contact the upper and lower mounting rails.
3. Press the ejectors toward each other, levering them against the mounting rails and completely seating the module against the backplane.
4. Secure the switch II module in place by tightening the retaining screws.
5. Reconnect the processor cables to their respective ports on the switch II module.

REPLACING POWER SUPPLIES

Because the power supplies are hot swappable, if both are plugged in to a power source, you can replace either one while the remaining supply carries the full load. The replacement procedure is the same whether you replace an AC or DC power supply.

Removing Power Supplies

1. Loosen but do not completely remove the captive screws in the upper and lower ejectors.

Note: *There are two screws in each ejector. Remove the screw closest to the outer edge of the power supply, as shown in Figure 2-12.*

Figure 2-12 Removing a Power Supply

2. Press the silver locking tab into each ejector handle.
3. Pull the handles away from each other, pivoting them against the upper and lower mounting rails to disconnect the power supply from the backplane.

   An audible alarm sounds and the POWER GOOD LED goes dark, indicating that the power supply has been disconnected from the backplane.
4. Gripping both ejector handles, slide the power supply straight out.

Installing Power Supplies

1. Align the upper and lower edges of the power supply with the guide tracks.
2. Slide the power supply in until the ejectors contact the upper and lower mounting rails.
3. Press the ejectors toward each other, levering them against the mounting rails and completely seating the power supply against the backplane.
4. Secure the power supply in place by tightening the retaining screws.

Connecting DC Power Supply Wires

The DC power on/off switch, dual terminal blocks, and dual grounding posts are located in the back of the chassis.

⚠ Warning *You must shut off current to the DC feed wires before connecting to the power supply. Also, make sure that the on/off switch on the NetScreen-1000 chassis is in the off position; that is, the side with the circle is pressed in.*

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

1. Strip the ends of the power cables for insertion into the power connector terminal blocks.
2. Loosen the inner two screws of each terminal block.
3. Insert the -48V DC power feed wire into the left power connector and the 0V DC return wire into the right power connector.
4. Fasten the screws over the connectors.
5. Secure the plastic cover over the terminal blocks.
6. Connect the ground wire to the ground posts.

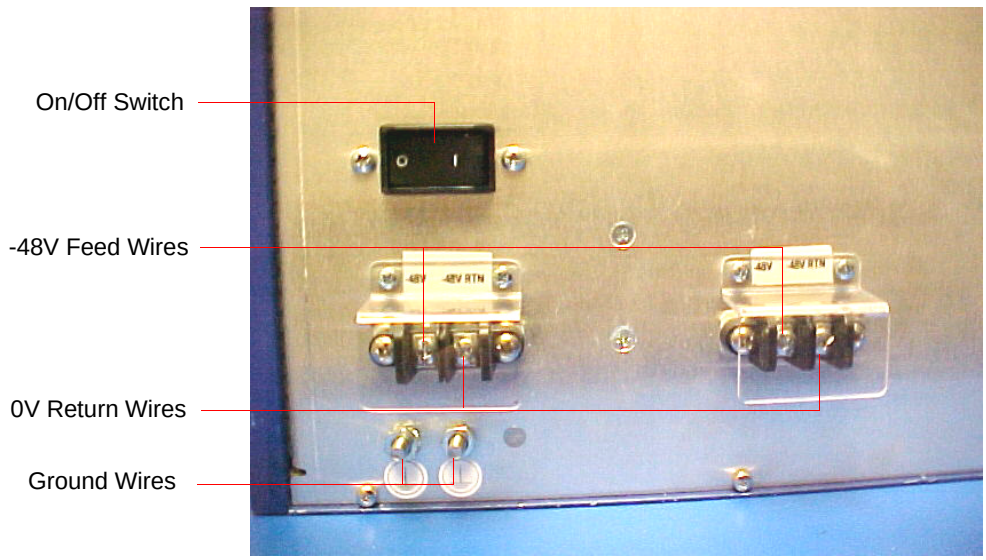


Figure: NetScreen-1000 DC Power Terminal Block

REPLACING THE FAN ASSEMBLY

You only need to replace the fan assembly in the event of failure, indicated when the FAN LED on the auxiliary module glows red (see "Auxiliary Module Status LEDs" on page 1-5), and an event alarm and SNMP trap is triggered. Although the unit can operate with two of the three fans, there is a serious risk of overheating. Especially critical is the far right fan, located directly beneath the dual power supplies. Should the power supplies become too hot, the system automatically shuts down.

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. Open the fan access port by loosening the 4 captive screws and pulling the upper edge of the door forward, as shown in Figure 2-13.

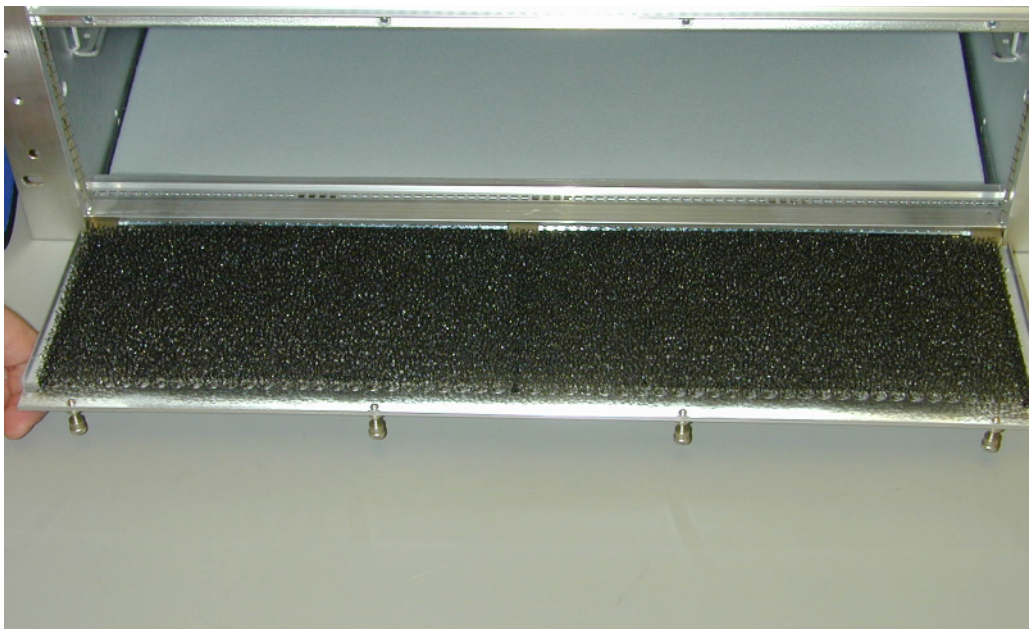


Figure 2-13 Opening the Fan Access Port

2. Press the fan assembly release tabs, located at the far left and right sides, toward the center, as shown in Figure 2-14.

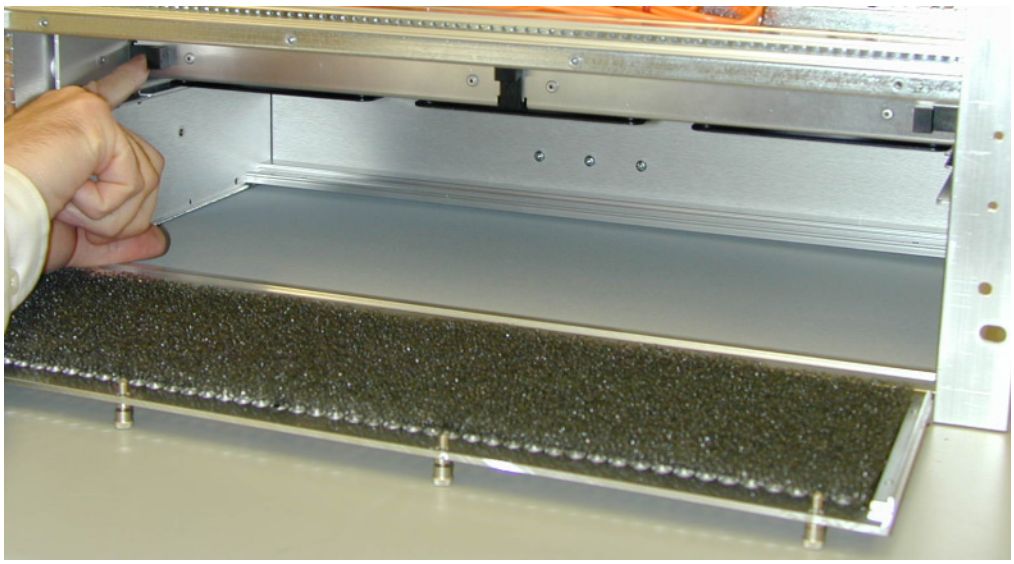


Figure 2-14 Releasing the Fan Assembly

⚠ Danger *The fans spin at high speed and can cause physical injury. Exercise extreme caution when removing the fan assembly, and handle it only by the sides. Do not reach into any of the 3 air ducts. Figure 2-15 on page 2-21 illustrates the correct method of removing the fan assembly.*

3. With both hands, reach underneath the fan tray, and slide out the unit toward yourself, as shown in Figure 2-15.

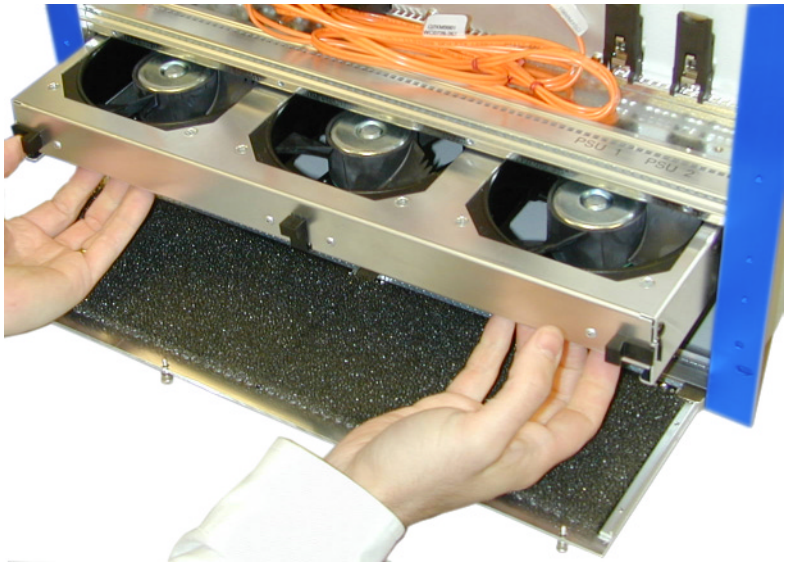


Figure 2-15 Safely Removing the Fan Assembly

Note: *Note the orientation of the plug (see Figure 2-16) when you remove the fan tray. Attempting to install the fan assembly upside down will break the plug and can result in serious damage to the NetScreen-1000.*

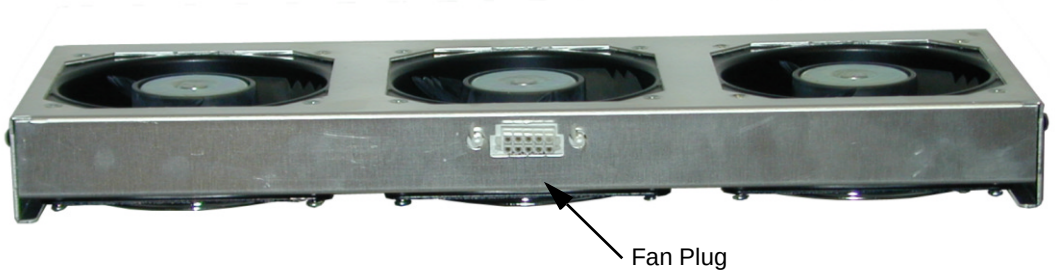


Figure 2-16 Fan Plug on the Back of the Fan Assembly

Cleaning the Air Filter

You do not need to replace the air filter, but it is recommended that you periodically clean it. Depending on the amount of dust it collects, you might want to clean it once or twice a year.

1. Open the fan access port, as shown in Figure 2-13 on page 2-19.

   The air filter is affixed inside the front grill of the access port.

2. Remove the air filter, as shown in Figure 2-17, and take it some distance from the NetScreen-1000 device.

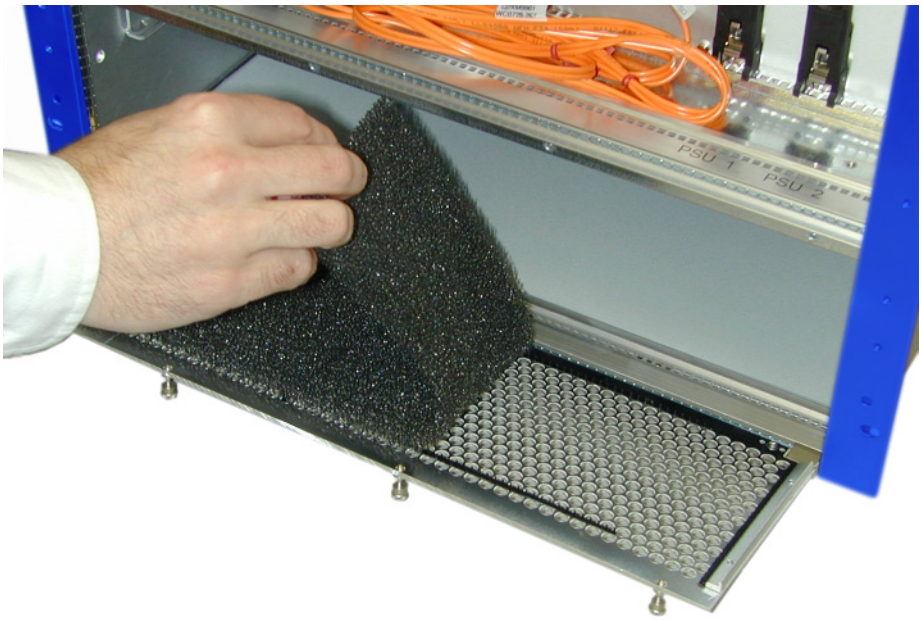


Figure 2-17 Removing the Air Filter

3. Vigorously shake the air filter to dislodge accumulated dust.
4. Replace the filter and close the access port.

RACK-MOUNTING THE NETSCREEN-1000

There are two ways to rack-mount the NetScreen-1000 chassis: front mounting and extended front mounting. To front mount the chassis, you simply bolt the chassis to the rack through the left and right flanges. To front mount the chassis so that it extends forward beyond the front of the rack, you must use the rack-mounting kit that ships with the unit.

Caution *Because the NetScreen-1000 weighs 50 pounds (23 kilograms), do not attempt to rack mount it by yourself. Two or three people should work together to mount it. Before continuing, read "Configuring Equipment Racks" on page A-4.*

Front Mounting

This method of mounting the NetScreen-1000 chassis leaves it flush with the front of the rack.

1. If necessary, remove the cover to expose the left and right flanges of the chassis.
2. With the help of one or two others, lift the chassis to the desired position in the rack and bolt it in place.

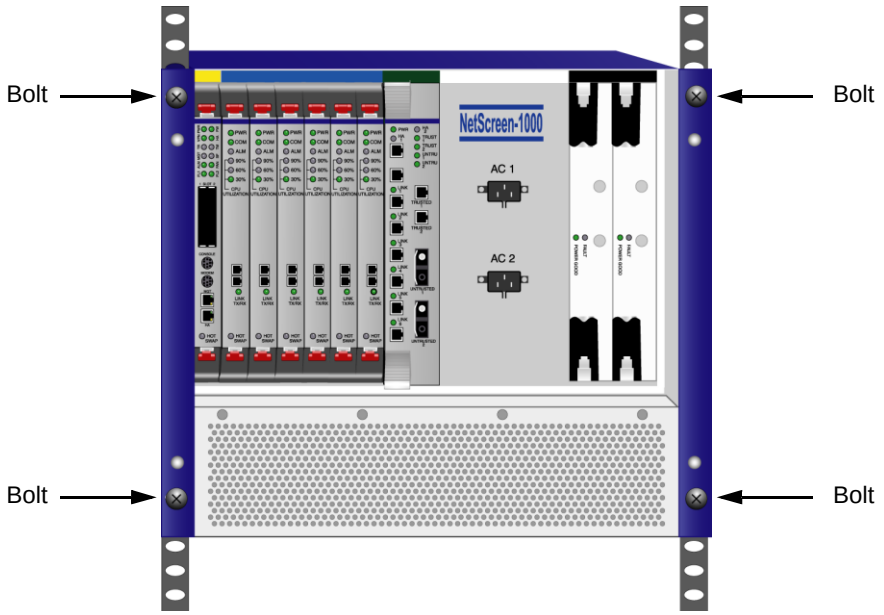


Figure 2-18 Front Mount

Extended Front Mounting

This method of mounting the NetScreen-1000 chassis leaves it extended beyond the front of the rack.

1. With a cross-head screwdriver, unscrew the six screws on the left side panel and the six screws on the right side panel.
2. Remove the left and right side panels.
3. With a hex wrench, screw two rack-mounting brackets to each side of the chassis, as shown in Figure 2-19.

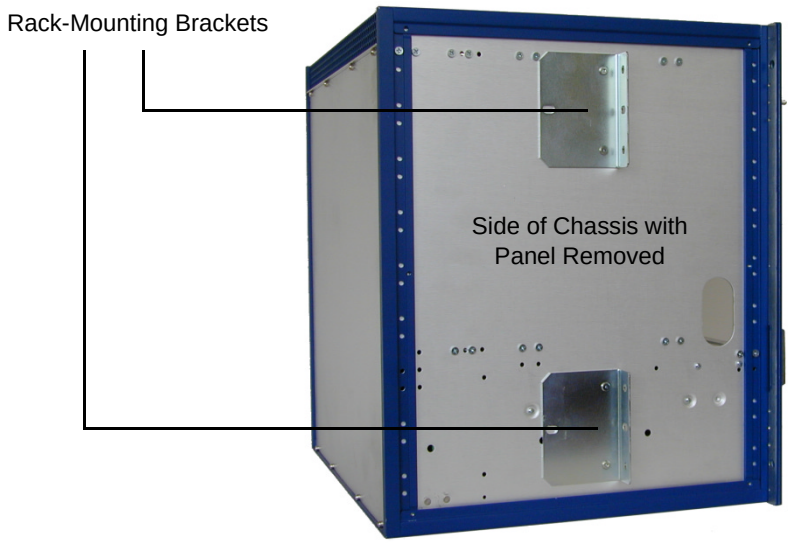


Figure 2-19 Rack-Mounting Brackets

4. Replace the side panels over the brackets and screw them back in place.
5. With the help of one or two others, lift the chassis to the desired position in the rack and bolt it in place, as shown Figure 2-20 on page 2-25.

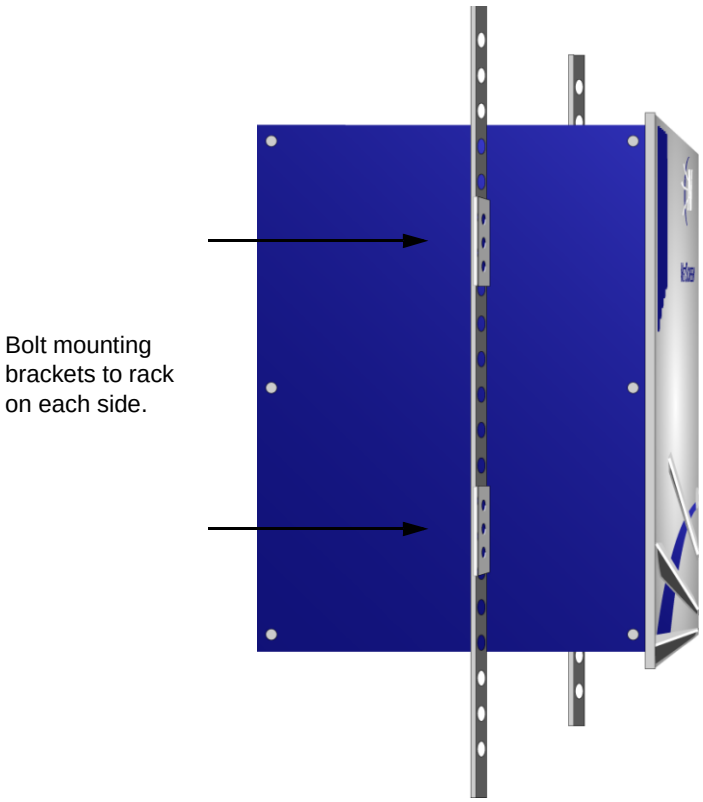


Figure 2-20 Extended Front Mount

Connecting to the Network 3

This chapter explains how to connect the NetScreen-1000 device to the network as a single security system and in a redundant cluster for high availability in the following sections:

Caution *Make sure you have read Appendix A,"Safety Recommendations and Warnings", before you begin this chapter.*

The NetScreen-1000 uses gigabit optical cables with MT-RJ and SC connectors, and Category-5 (cat5) cables with 10/100 RJ45 connectors. The cables to use for each port on the switch II module[1] are as follows:

- Untrusted port: SC to SC optical cable[2]
- Trusted port: MT-RJ to SC optical cable

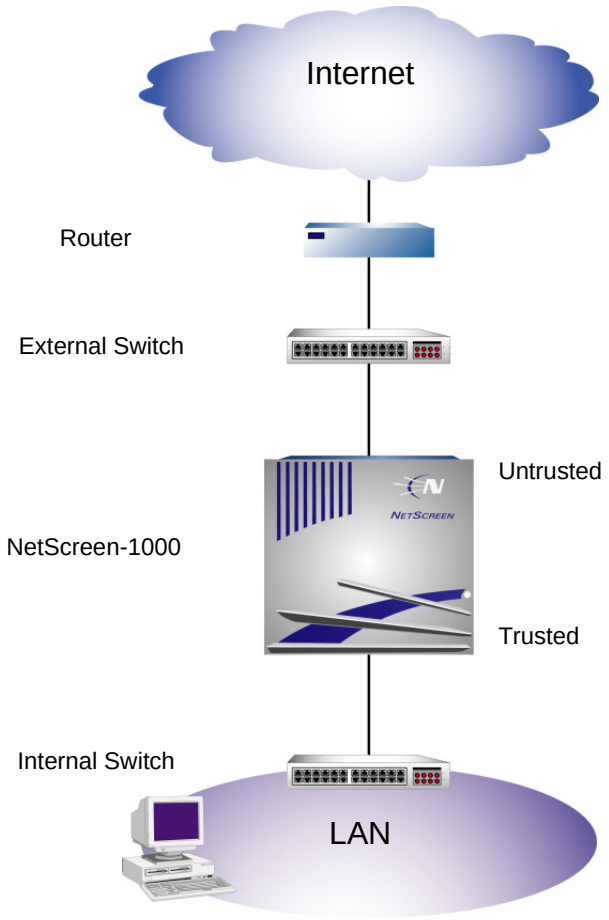
The cable to use for the HA port on the auxiliary module is an RJ45 10/100 cat5 cross-over cable.

1. Earlier versions of the NetScreen-1000 contain a switch I module. Refer to the documentation received with the unit for cabling options.

2. The network devices to which you connect the trusted and untrusted ports determine the cable connector types you require. The NetScreen-1000 trusted port requires an MT-RJ connector and the untrusted port requires an SC connector. The ports on your network switches or routers might require you to use different cables than those provided.

Connecting the NetScreen-1000 as a Single Security Appliance

When setting up a NetScreen-1000 device as a single security appliance, cable it to the trusted and untrusted networks as shown below.



Cable the NetScreen-1000 device as a single security appliance to the trusted and untrusted network as follows:

1. Cable the trusted port to the internal switch.
2. Cable the untrusted port to the external switch.
3. Cable the external switch to the router.

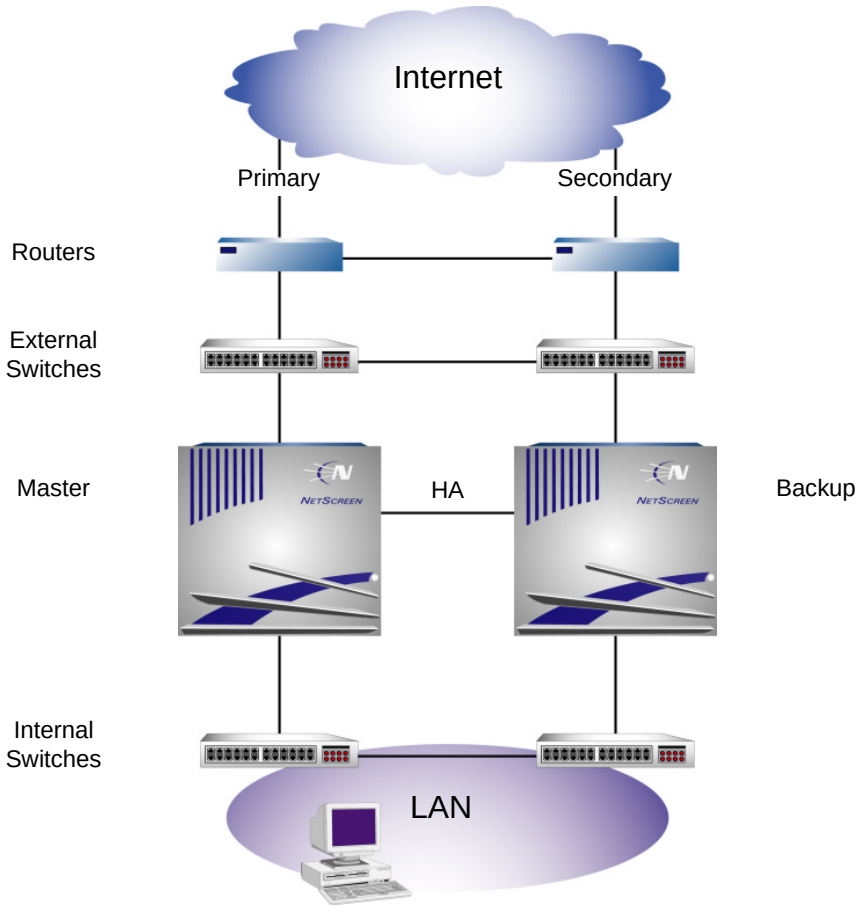
Note: *For configuring the ScreenOS, see Chapter 4, "Initial Configuration".*

CONNECTING THE NETSCREEN-1000 FOR HIGH AVAILABILITY

The following diagram illustrates the cabling of two NetScreen-1000 devices to each other and to redundant pairs of internal switches and external switches. The external switches are then cabled to a pair of redundant routers.

Note: *Depending on the topology in which you are deploying the NetScreen devices and the kinds of switches and routers you use, the cabling presented in the following diagram might differ from what your network requires.*

The trusted ports host gigabit optical connections using MTRJ connectors. The untrusted ports host gigabit optical connections using SC connectors. The HA port on the auxiliary module uses a 10/100 cat5 cross-over cable with RJ45 connectors.



Cable two NetScreen-1000 devices for HA in a full-mesh configuration as follows:

1. Cable together the 10/100 HA ports on the auxiliary module of each NetScreen-1000 device.
2. Cable the untrusted ports to different external switches, and then cable the external switches together.
3. Cable the external switches to the routers, and then cable the routers together.
4. Cable the trusted ports to different internal switches, and then cable the internal switches together.

Note: *For directions on configuring the device for high availability, see* *"HA Configuration" on page 4-13.*

Initial Configuration 4

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

- "Configuring via the WebUI" on page 4-3
- "Configuring via the CLI" on page 4-9

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-1000
CLI	Via the console port: a VT100 terminal emulator, such as Hilgraeve® Hyperterminal®, and a male 9-pin mini DIN to female 9-pin RS-232 serial port cable Via Telnet: TCP/IP network connection to the NetScreen-1000

The chapter concludes with a section on setting up two NetScreen-1000 devices in a redundant group for high availability (HA) using the NetScreen Redundancy Protocol (NSRP). For more information, see "HA Configuration" on page 4-13.

The NetScreen-10000 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[1], which might be the Internet. In Transparent mode, the IP addresses for the trusted and untrusted 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 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.

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

CONFIGURING VIA THE WEBUI

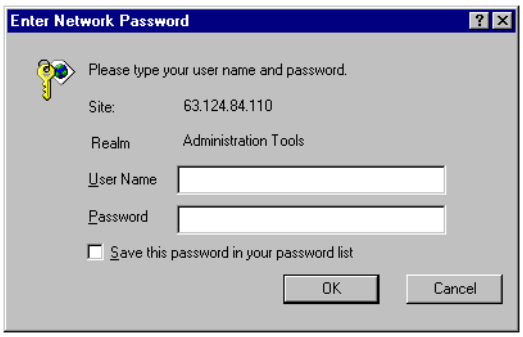
The following sections provide instructions for performing an initial configuration via the WebUI. Before starting, make sure that the NetScreen-1000 is connected to the network as described in "Connecting to the Network" on page 3-1. Also make sure that your workstation has a Web browser (see "Administration Requirements" on page 4-1) and is on the same subnet as the NetScreen-1000 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-1000 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.

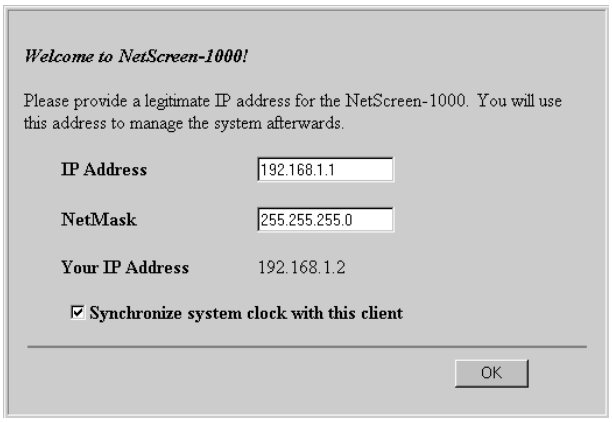
   The Enter Network Password dialog box appears.



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.



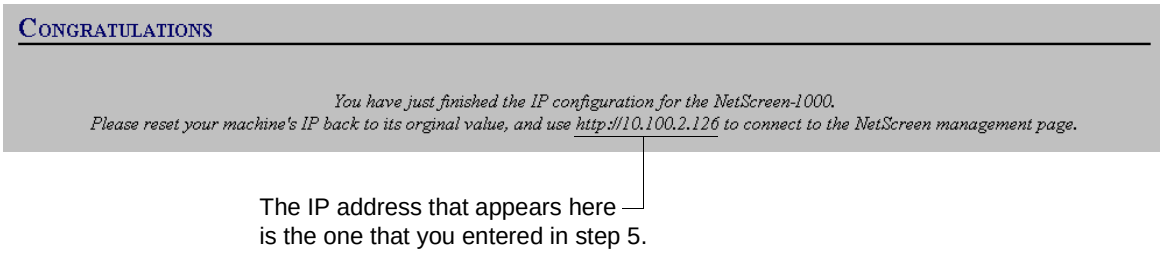
5. Enter the IP address and netmask for administration of the NetScreen-1000, and then click **OK**.

   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 in the same subnet as the trusted interface. If the management workstation is on the untrusted[2] side, then the system IP address must be in the same subnet as the untrusted interface.

Note: *To synchronize the NetScreen-1000 clock with the clock in your workstation, select the* ***Synchronize system clock with this client*** *check box.*

2. To enable management using the WebUI via the untrusted 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 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-1000 ships with all its interface addresses and netmasks set as 0.0.0.0. If you want to operate the NetScreen-1000 in Transparent mode, leave the trusted and untrusted 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-1000 in NAT mode or Route mode, you must also configure the trusted and untrusted 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-1000.

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

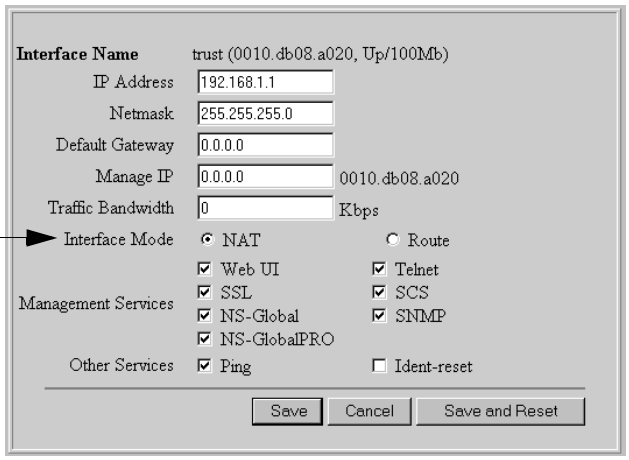
   IP Address: Type an IP address for the trusted interface.

   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-1000.

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

NAT or Route mode option.



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

   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.

Allowing Outbound Traffic

By default, the NetScreen-1000 does not allow inbound or outbound traffic. You must 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.

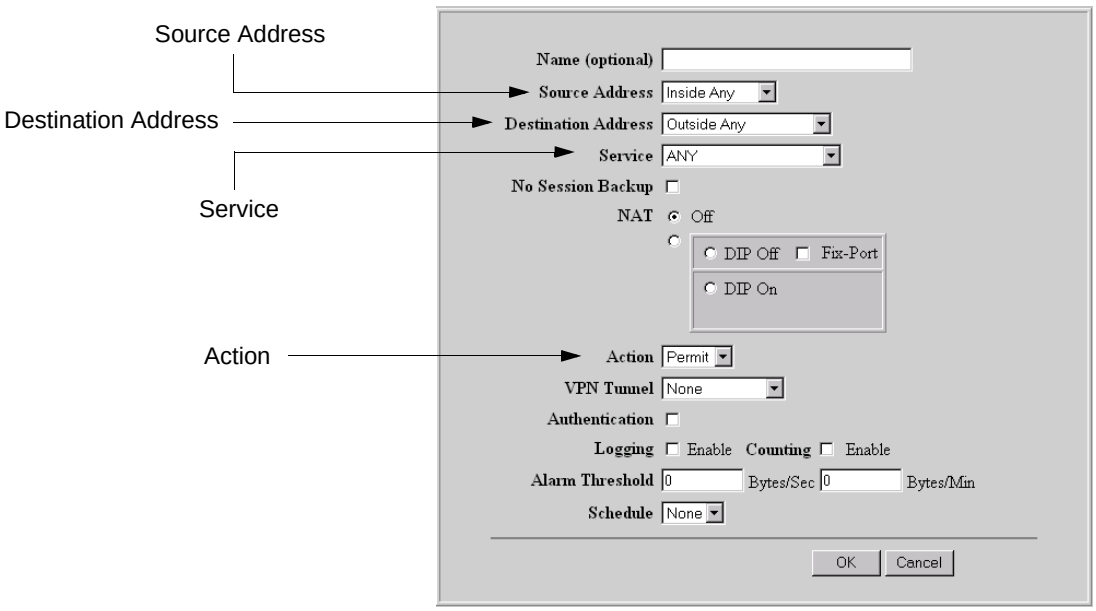
Policy >> Outgoing >> New Policy: Enter the following, and then click **OK**:

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 default login name and password (netscreen), it is highly recommended that you change your login name and password immediately.

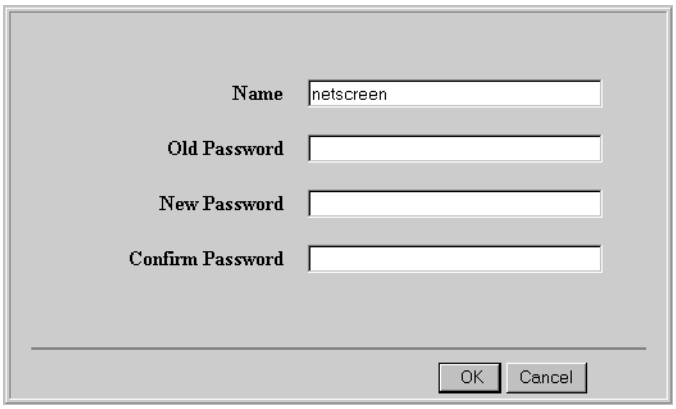
Admin >> Admin >> Edit: Enter the following, and then click **Apply**:

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.

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-1000, 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-1000 directly, using Hyperterminal and connecting a console cable from your workstation to the console port. You can also access the NetScreen-1000 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-1000.
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.

Change the IP address of the management workstation to the same subnet as that of the NetScreen-1000 default system IP address, which is 192.168.1.1. In Windows, you can access the system IP address via Telnet as follows:

1. Click **Start >> Run**.
2. Type **telnet 192.168.1.1**
3. 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

Note: *If you are connected to the NetScreen-1000 via Telnet, you lose the connection after you save the new system IP address. Establish a new connection by entering the new system IP address when launching Telnet again.*

Setting Interface Addresses

The NetScreen-1000 ships with all its interface addresses and netmasks set as 0.0.0.0. If you want to operate the NetScreen-1000 in Transparent mode, leave the trusted and untrusted 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-1000 in NAT mode or Route mode, you must also configure the trusted and untrusted 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. save

Allowing Outbound Traffic

By default, the NetScreen-1000 does not allow inbound or outbound traffic. You must 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.

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-1000, 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.

HA CONFIGURATION

After cabling the NetScreen-1000 devices together and to the surrounding network devices (see "Connecting the NetScreen-1000 for High Availability" on page 3-3), you must configure them for HA. A complete configuration involves the following steps:

1. Defining the Manage IP addresses for the trusted and untrusted interfaces
2. Defining a redundant group
3. Assigning each group member a priority number[3]

Note: *Although you can configure HA through both the WebUI and the CLI, the CLI provides more options, which can improve performance during a failover.*

WebUI (Master)

1. Interface >> Trusted >> Edit (for "trust"): 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-1000.

   Manage IP: Type an address on the same subnet as the IP address for the physical trusted interface. (Through this address, you can manage the device when it is acting as a backup.)

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

3. You only need to assign a priority number between 1 and 99 for the master. By default, the priority for a device is 100, which is the priority for the backup if you do not assign it another value.

2. Interface >> Untrusted >> Edit (for “untrust”): 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.

   Manage IP: Type an address on the same subnet as the IP address for the physical untrusted interface. (Through this address, you can manage the device when it is acting as a backup.)

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

   Group ID: Enter any number between 1 and 255.

   Priority: Enter any number between 1 and 99. (The device with the number closest to 1 is the master unit. A value of 0 disables high availability and shuts down the HA port.)

   HA Authentication Password: Select and type a password for use in creating an authentication key.

   HA Encryption Password: Select and type a password for use in creating an encryption key.

   Secondary Path: Trusted[4]

4. If the HA link is lost, HA communications pass via the trusted interface. Although you can select the untrusted interface, due to the sensitive nature of HA traffic, NetScreen recommends that you use the trusted interface.

WebUI (Backup)

1. Interface >> Trusted >> Edit (for “trust”): Enter the following, and then click **Save**:

   Manage IP: Type a unique address on the same subnet as the IP address for the physical trusted interface. (Through this address, you can manage the device when it is acting as a backup.)

2. Interface >> Untrusted >> Edit (for “untrust”): Enter the following, and then click **Save**:

   Manage IP: Type a unique address on the same subnet as the IP address for the physical untrusted interface. (Through this address, you can manage the device when it is acting as a backup.)

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

   Group ID: Type the same group ID number that you typed for the master.

   HA Authentication Password: Select and type a password for use in creating an authentication key.

   HA Encryption Password: Select and type a password for use in creating an encryption key.

CLI (Master)

1. set interface trust ip <a.b.c.d> <A.B.C.D>
2. set interface trust gateway <a.b.c.d>
3. set interface trust manage-ip <a.b.c.d>
4. set interface trust { nat | route }
5. set ha group <id_number>
6. set ha priority <number>
7. set ha encrypt password <string>
8. set ha auth password <string>
9. set ha second-path trust
10. set ha link-up-on-slave
11. set ha fast-mode[5]
12. save

CLI (Backup)

1. set interface trust manage-ip <a.b.c.d>
2. set ha group <id_number>
3. set ha encrypt password <string>
4. set ha auth password <string>
5. save config ha-master
6. reset

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

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

5. When there are only two devices in a redundant group, using the fast-mode option accelerates the failover procedure by eliminating the election process for the next master.

Safety Recommendations and Warnings

A

SAFETY RECOMMENDATIONS AND WARNINGS

When using the NetScreen-1000, follow these safety guidelines:

- Make sure that the work area is dry and without excess humidity.
- Keep the chassis area clear and dust-free during and after installation.
- Never assume that power is disconnected from a circuit. Always check.

Before supplying power:

- Look carefully for possible hazards in the work area, such as moist floors, ungrounded power extension cables, and missing safety grounds.
- Locate the emergency power-off switch for the room where you are working.

Do not perform any action that creates a potential hazard to people or makes the equipment unsafe. Do not stack or balance the equipment on other devices to avoid tipping over and to allow air circulation. Make sure that the installation is securely in place.

⚠ Warning *The NetScreen-1000 device weighs 50 pounds (23 kilograms). The unit requires two people to move or rack-mount it.*

Product Disposal Warning

Warning *Ultimate disposal of this product should be handled according to all national laws and regulations.*

Power Disconnection Warning

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

Installation Warning

Warning *Before you connect the system to its power source, read Chapter 2, "Hardware Description".*

Grounding Warning

Warning *When inserting and removing components, wear anti-static wrist straps. Also, either stand on an anti-static mat or set the NetScreen-1000 on one. Not taking such precautions might negatively affect the circuitry.*

Circuit Breaker (15A) Warning

Warning *This product relies on the building's installation for short-circuit (over-current) protection. Ensure that a fuse or circuit breaker no larger than 120 VAC, 15A U.S. (240 VAC, 10A international) is used on the phase conductor (all current-carrying conductors).*

SELV Circuit Warning

Warning *The Ethernet 10BaseT, 100BaseT, serial, console, and auxiliary ports contain safety extra-low voltage (SELV) circuits. Do not connect to a telephone line.*

Lightning Activity Warning

Danger *Do not work on the system, connect or disconnect cables during periods of lightning activity*

GENERAL SITE REQUIREMENTS

This section describes the requirements your site must meet for the safe installation and operation of your system. Ensure that your site is properly prepared before beginning the hardware installation.

Warning *This unit is intended for installation in restricted access areas. A restricted access area is where access can only be gained by service personnel through the use of a special tool, lock and key, or other means of security, and is controlled by the authority responsible for the location.*

Site Environment

The NetScreen-1000 can be placed on a desktop or mounted in a rack. The location of the chassis and the layout of your equipment rack or wiring room are extremely important for proper system operation. Equipment placed too close together will cause inadequate ventilation, besides rendering areas of the device inaccessible for system maintenance during any system malfunctions and shutdowns.

When planning your site layout and equipment locations, follow the precautions described in the next section to help avoid equipment failures and reduce the possibility of environmentally caused shutdowns. If you are experiencing shutdowns or unusually high errors with your existing equipment, these precautions may help you isolate the cause of the failures and prevent future problems.

Preventive Site Configuration

The following precautions will help you plan an acceptable operating environment for your NetScreen-1000 and will help you avoid environmentally caused equipment failures:

- Operate the device in a controlled environment with a temperature between 68 and 72° Fahrenheit (20–22° Celsius). Although the device can operate within a wider temperature range (see "Environmental Requirements" on page A-4), the temperatures provided here optimize performance.
- Electrical equipment generates heat. Natural air temperature might not be sufficient to cool equipment to acceptable operating temperatures without an

additional circulation system. Ensure that the room in which you operate your system has adequate air circulation.

- Do not work alone if potentially hazardous conditions exist.
- Look carefully for possible hazards in your work area, such as wet floors, ungrounded power extension cables, frayed power cords, and missing safety grounds.

Configuring Equipment Racks

The following information will help you plan an acceptable equipment rack configuration.

- Enclosed racks must have adequate ventilation. Ensure that the rack is not overly congested because each unit generates heat. An enclosed rack should have louvered sides and a fan to provide cooling air.
- When mounting a chassis in an open rack, ensure that the rack frame does not block the intake or the exhaust ports. If the chassis is installed on slides, check the position of the chassis when 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 you provide adequate ventilation for equipment at the bottom of the rack.
- Baffles can help to isolate exhaust air from intake air, which also helps to draw cooling air through the chassis. The best placement of the baffles depends on the airflow patterns in the rack, which can be found by experimenting with different arrangements.

Power Supply Considerations

The following power supply considerations can affect the performance and reliance of the NetScreen-1000.

- Check the power at your site to ensure that you are receiving “clean” power (free of spikes and noise). Install a power conditioner if necessary.
- Plug the dual power supplies into two outlets running on different circuits. If one circuit should fail, the other might continue providing power to the unit.

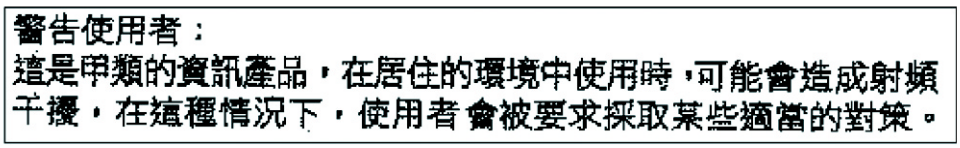
Environmental Requirements

The NetScreen-1000 is intended for use in a normal office environment. For more extreme conditions, verify that temperature, humidity, and power conditions meet the specifications indicated in Table A-1.

Table A-1 Environmental Requirements

Item	Operating Specification
Temperature	Operating: 32–104°F, 0–40°C Storage: 14–158°F, -10–70°C
Relative humidity	5–90%, non-condensing: for storage 10–90% non-condensing: for operation
AC Voltage	90–264 VAC (47–63 Hz)
DC Voltage	36–72 Volts
Power consumption	300 watts
Weight Dimensions	50 lbs., 19-inch rack-mountable Width: 17.5 inches Height: 22 inches Depth: 20 inches
Altitude	0–12,000 feet, 0–3,660 meters

BSMI Labeling Requirements



Index

I

L

M

N

O

P

R

S

T

V

W