NETSCREEN-500

Installer's Guide

Version 4.0 P/N 093-0575-000 Rev.E

Copyright Notice

NetScreen, NetScreen Technologies, GigaScreen, and the NetScreen logo are registered trademarks of NetScreen Technologies, Inc. NetScreen-5XP, NetScreen-5XT, NetScreen-25, NetScreen-50, NetScreen-100, NetScreen-204, NetScreen-208, NetScreen-500, NetScreen-1000, NetScreen-5200, NetScreen-5400, NetScreen-Global PRO, NetScreen-Global PRO Express, NetScreen-Remote Security Client, NetScreen-Remote VPN Client, NetScreen-IDP 100, NetScreen-IDP 500, GigaScreen ASIC, GigaScreen-II ASIC, and NetScreen ScreenOS are trademarks of NetScreen Technologies, Inc. All other trademarks and registered trademarks are the property of their respective companies.Information in this document is subject to change without notice.

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.
350 Oakmead Parkway
Sunnyvale, CA 94085 U.S.A.
www.netscreen.com

FCC Statement

The following information is for FCC compliance of Class A devices: 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 when the equipment is operated in a commercial environment. The equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with NetScreen's installation instructions, it may cause interference with Radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital devices in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. 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.

Disclaimer

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR NETSCREEN REPRESENTATIVE FOR A COPY.

Table of Contents

Preface

The NetScreen-500 is a purpose-built, high-performance security system designed to provide a flexible solution to medium and large enterprise central sites and service providers. The NetScreen-500 security system integrates firewall, VPN, and traffic management functionality in a low-profile, modular chassis.

The NetScreen-500 is built around NetScreen's custom, second-generation purpose-built GigaScreen ASIC, which provides accelerated encryption algorithms and policy look ups. In addition, there are two high speed busses to off-load management traffic from application traffic processing. This prevents High Availability and other management traffic from impacting throughput performance.

This manual introduces the NetScreen-500 device, describes how to install and service the device, and shows how to perform initial configuration. It also lists device requirements and performance specifications.

Guide Organization

This manual has four chapters and two appendices.

Chapter 1, "Overview" provides a detailed overview of the system and its modules, Fast Ethernet (FE) and mini-GBIC connectors, power supplies and fan tray.

Chapter 2, "Installing the Device" details how to rack-mount the NetScreen-500 device, connect the power supplies, and connect the modules to the network in addition to providing desktop site requirements and guidelines for rack mounting.

Chapter 3, "Configuring the Device" details how to obtain an IP address for an interface on one of the modules and how to aggregate ports on one of the modules.

Chapter 4, "Servicing the Device" provides procedures on how to replace your modules and power supplies.

Appendix A, "Specifications" provides a list of physical specifications about the NetScreen-500 Series, the modules, and power supplies.

Appendix B, "Configuration for Common Criteria, EAL2" provides information about configuring NetScreen devices for Common Criteria, EAL2 compliance.

Command Line Interface (CLI) Conventions

Some of the instructions and examples provided in this manual contain CLI commands, most of which perform initial configuration of the NetScreen-500 device. The command examples use conventions for variables and syntax.

CLI Command Variables

Most NetScreen CLI commands have changeable parameters that affect the outcome of command execution. NetScreen documention represents these parameters as variables. Such variables may include names, identification numbers, IP addresses, subnet masks, numbers, dates, and other values.

Variable Notation

The variable notation used in this manual consists of italicized parameter identifiers. For example, the **set arp** command uses four identifiers, as shown here:

```
set arp
    {
    ip_addr mac_addr interface
    age number |
    always-on-dest |
    no-cache
    }
```

where

- *ip_addr* represents an IP address.
- *mac_addr* represents a MAC address.
- *interface* represents a physical or logical interface.
- *number* represents a numerical value.

Thus, the command might take the following form:

```
ns-> set arp 172.16.10.11 00e02c000080 ethernet2
```

where **172.16.10.11** is an IP address, **00e02c000080** is a MAC address, and **ethernet2** is a physical interface.

Common CLI Variable Names

The following list shows the CLI variable names used in NetScreen documents.

comm_name	The community name of a host or other device.
date_str	A date value.
dev_name	A device name, as with flash card memory.
dom_name	A domain name, such as “acme” in **www.acme.com**.
dst_addr	A destination address, as with a policy definition that defines a source and destination IP address.
filename	The name of a file.
grp_name	The name of a group, such as an address group or service group.
interface	A physical or logical interface.
id_num	An identification number.

ip_addr	An IP address.
key_str	A key, such as a session key, a private key, or a public key.
key_hex	A key expressed as a hexadecimal number.
loc_str	A location of a file or other resource.
mac_addr	A MAC address.
mbr_name	The name of a member in a group, such as an address group or a service group.
mask	A subnet mask, such as **255.255.255.224** or ***/24***.
name_str	The name of an item, such as an address book entry.
number	A numeric value, usually an integer, such as a threshold or a maximum.
pol_num	A policy number.
port_num	A number identifying a logical port.
pswd_str	A password.
ptcl_num	A number uniquely identifying a protocol, such as TCP, IP, or UDP.
serv_name	The name of a server.
shar_secret	A shared secret value.
spi_num	A Security Parameters Index (SPI) number.
src_addr	A source address, as with a policy definition that defines a source and destination IP address.
string	A character string, such as a comment.
svc_name	The name of a service, such at HTTP or MAIL.
time_str	A time value.
tunn_str	The name of a tunnel, such as an L2TP tunnel.
url_str	A URL, such as **www.acme.com**.
usr_str	A user, usually an external entity such as a dialup user.
vrouter	A local virtual router, such as trust-vr or untrust-vr.
zone	The name of a security zone.

Some commands contain multiple variables of the same type. The names of such variables may be numbered to identify each individually. For example, the **set dip** command contains two *id_num* variables, each numbered for easy identification:

set dip group *id_num1* [**member** *id_num2*]

CLI Command Syntax

Each CLI command description in this manual reveals some aspect of command syntax. This syntax may include options, switches, parameters, and other features. To illustrate syntax rules, some command descriptions use *dependency delimiters*. Such delimiters indicate which command features are mandatory, and in which contexts.

Dependency Delimiters

Each syntax description shows the dependencies between command features by using special characters.

- The { and } symbols denote a mandatory feature. Features enclosed by these symbols are essential for execution of the command.
- The [and] symbols denote an optional feature. Features enclosed by these symbols are not essential for execution of the command, although omitting such features might adversely affect the outcome.
- The | symbol denotes an "or" relationship between two features. When this symbol appears between two features on the same line, you can use either feature (but not both). When this symbol appears at the end of a line, you can use the feature on that line, or the one below it.

Nested Dependencies

Many CLI commands have *nested* dependencies, which make features optional in some contexts, and mandatory in others. The three hypothetical features shown below demonstrate this principle.

```
[ feature_1 { feature_2 | feature_3 } ]
```

In this example, the delimiters [and] surround the entire clause. Consequently, you can omit **feature_1**, **feature_2**, and **feature_3**, and still execute the command successfully. However, because the { and } delimiters surround **feature_2** and **feature_3**, you must include either **feature_2** or **feature_3** if you include **feature_1**. Otherwise, you cannot successfully execute the command.

The following example shows some of the **set interface** command's feature dependencies.

```
set interface vlan1 broadcast { flood | arp [ trace-route ] }
```

The { and } brackets indicate that specifyng either **flood** or **arp** is mandatory. By contrast, the [and] brackets indicate that the **arp** option's **trace-route** switch is not mandatory. Thus, the command might take any of the following forms:

```
ns-> set interface vlan1 broadcast flood
ns-> set interface vlan1 broadcast arp
ns-> set interface vlan1 broadcast arp trace-route
```

Availability of CLI Commands and Features

As you execute CLI commands using the syntax descriptions in this manual, you may find that certain commands and command features are unavailable for your NetScreen device model.

Because NetScreen devices treat unavailable command features as improper syntax, attempting to use such a feature usually generates the **unknown keyword** error message. When this message appears, confirm the feature's availability using the **?** switch. For example, the following commands list available options for the **set vpn** command:

```
ns-> set vpn ?
ns-> set vpn vpn_name ?
ns-> set vpn gateway gate_name ?
```

NETSCREEN PUBLICATIONS

To obtain technical documentation for any NetScreen product, visit www.netscreen.com/support/manuals.html. To access the latest NetScreen documentation, see the **Current Manuals** section. To access archived documentation from previous releases, see the **Archived Manuals** section.

To obtain the latest technical information on a NetScreen product release, see the release notes document for that release. To obtain release notes, visit www.netscreen.com/support and select **Software Download**. Select the product and version, then click **Go**. (To perform this download, you must be a registered user.)

If you find any errors or omissions in the following content, please contact us at the e-mail address below:

techpubs@netscreen.com

HOW TO GET MORE INFORMATION

To receive important news on product updates, please visit our Web site at www.netscreen.com.

Overview

1

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

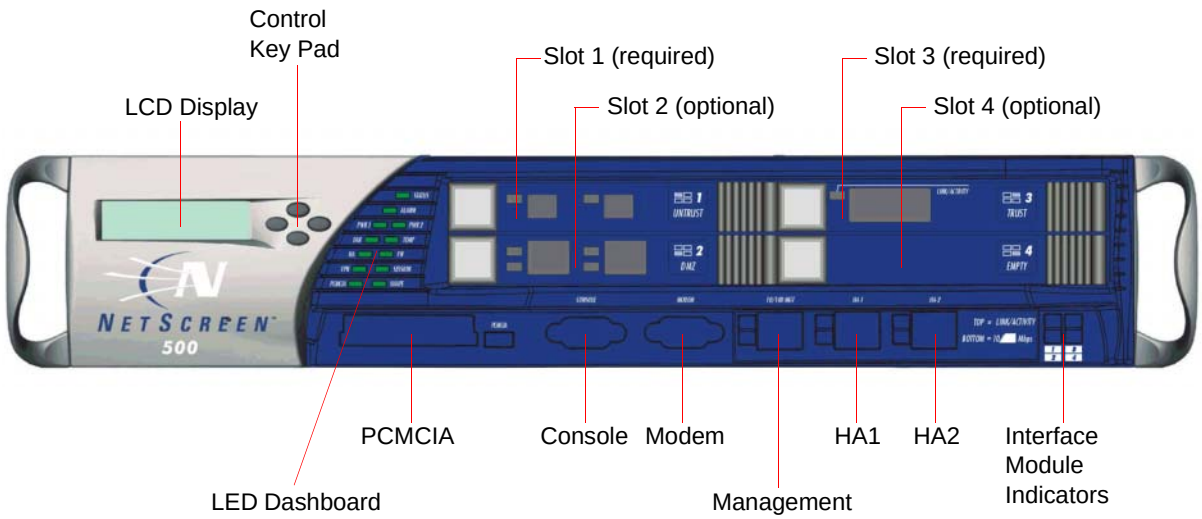
Topics in this chapter include:

Note: *For safety warnings and instructions, please refer to the* NetScreen Safety Guide. *The instructions in this guide warn you about situations that could cause bodily injury. Before working on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents.*

THE FRONT PANEL

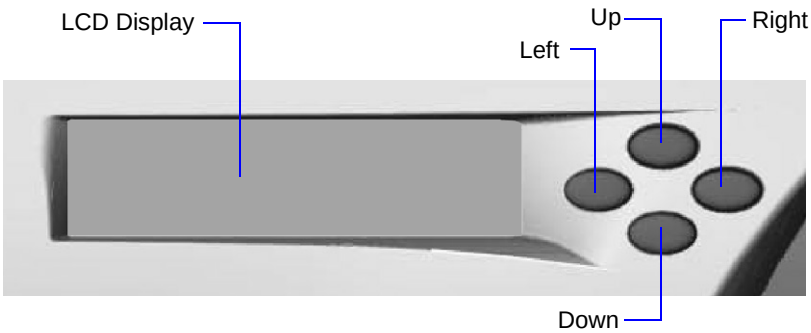
The front panel of the NetScreen-500 device has the following:

- A LCD and control pad menu interface
- A LED dashboard
- Four removable, replaceable interface modules
- A PCMCIA memory card slot
- Managment, Console, and Modem ports
- High-availability (HA) ports



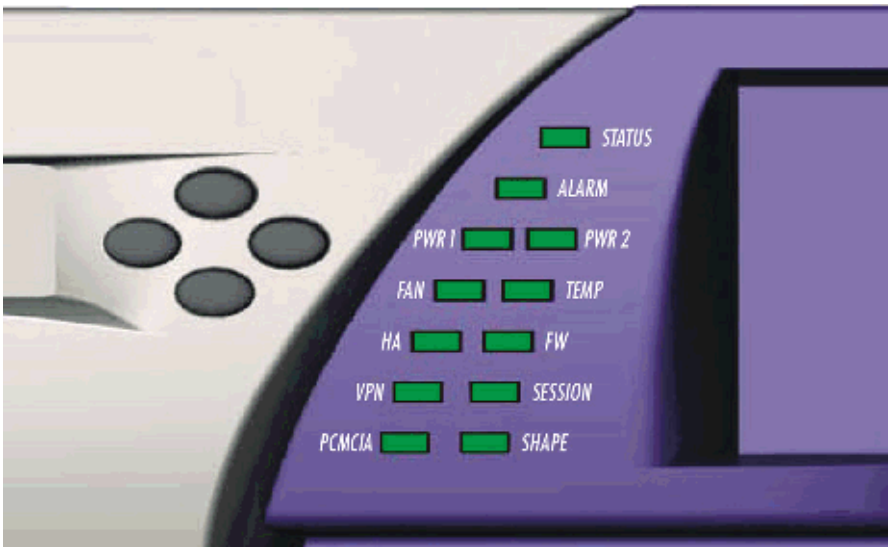
LCD and Control Pad Menu Interface

The LCD and control pad menu interface allows you to perform basic configurations and view status reports. The LCD can display two lines, each containing up to 16 characters. The control pad has four menu navigation keys (up, down, left, and right).



LED Dashboard

The LED dashboard displays up-to-date information about critical NetScreen-500 functions.



The LEDs in the dashboard are as follows:

LED	Purpose	Color	Meaning
STATUS	System Status	**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.
		off	No alarms
PWR 1	Power Supply #1	**green**	Power supply #1 is functioning correctly.
		red	Power supply #1 failure or power bay #1 is empty.

LED	Purpose	Color	Meaning
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.
		orange	Temperature is outside normal alarm range.
		red	Temperature is outside severe alarm range.
HA	High Availability Status	**green**	Unit is master.
		blinking green	Redundant group member cannot be found.
		amber	Unit is backup.
		off	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.
		off	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	Read-write activity is detected.
		off	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 (changes to green when you correct the configuration)
		off	No traffic shaping configured

Note: *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 messages, use the control pad menu keys to select* **3. Alarm >> 32. Clear All >> Yes**.

When you apply power to the NetScreen-500 device, the Status LED changes from off to blinking green. Startup takes up to one minute to complete.

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

The front of the NetScreen-500 device has four interface module bays. Each interface module has either one or two ports, and each port has a pair of LEDs.

Note: *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 10/100 Mbps Interface Module

The 10/100 Mbps interface module is appropriate for a 10BaseT or 100BaseT LAN. Connect the ports using a twisted pair cable with RJ-45 connectors. (See "Operational Modes" on page 18 for cabling guidelines.)

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

The Gigabit Interface Connector (GBIC) Module

The GBIC interface module provides connectivity to fiber-based, gigabit ethernet LANs. Connect the ports using an optical cable with SX or LX connectors.

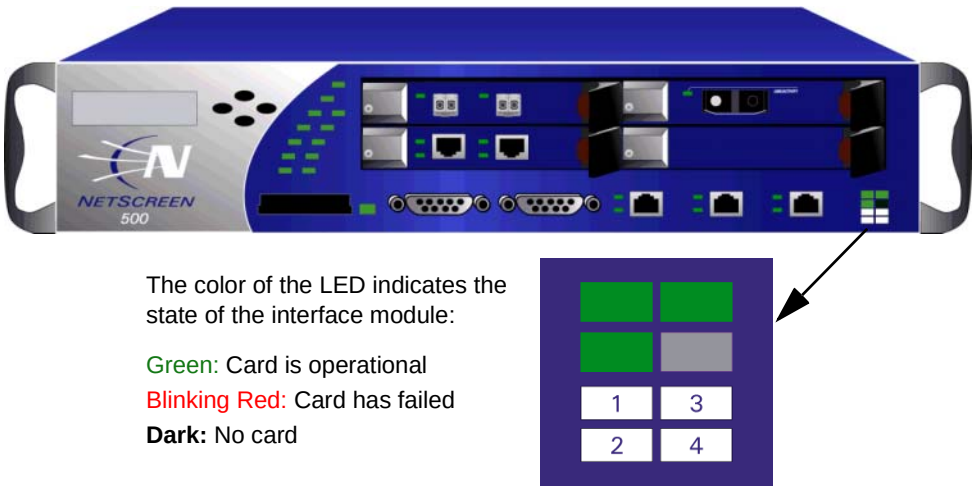
Status LED:
- Green: Link is up, no activity
- Blinking Green: Link is up and active

The Mini-GBIC Interface Connector Module

The mini-GBIC interface module provides connectivity to fiber-based, gigabit ethernet LANs. Connect using an optical cable with SX or LX connectors.

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

The interface module LEDs are in the lower-right corner of the front panel. The relative position of each LED corresponds to the position of the represented module.



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

The PCMCIA slot is for downloading or uploading system software or configuration files and saving log files. This slot can accept a type I, II, or III SanDisk® ATA PC card.

To perform download or upload, execute the CLI command **save**:

```
save
    { software | config }
        from { flash | slot1 filename } to
            { flash | slot1 filename }
```

where **slot1** refers to the PCMCIA slot, **flash** refers to internal flash memory, and *filename* is the name of the software or configuration file on the card.

For example, the following command downloads the current device configuration to a file named **ns500_config** on a card in the PCMCIA slot:

```
save config from flash to slot1 ns500_config
```

Management Interfaces

The NetScreen-500 device offers three management interfaces:

Port	Description
Console	This DB-9 port is for local configuration and administration using the CLI. Connect the Console port to your workstation using a DB-9 female to DB-9 male straight-through serial cable.
Modem	This DB-9 serial port is for connecting to a modem, allowing the user to control the device remotely. (For security reasons, it is advisable to use a modem only for troubleshooting or a one-time configuration, not for regular remote administration.)
10/100 MGT	This management port has a fixed 10/100 BaseT interface and provides a dedicated, out-of-band connection for management traffic. It has a separate IP address and netmask, configurable with the CLI or WebUI. (For security reasons, do not pass session traffic through this interface.)

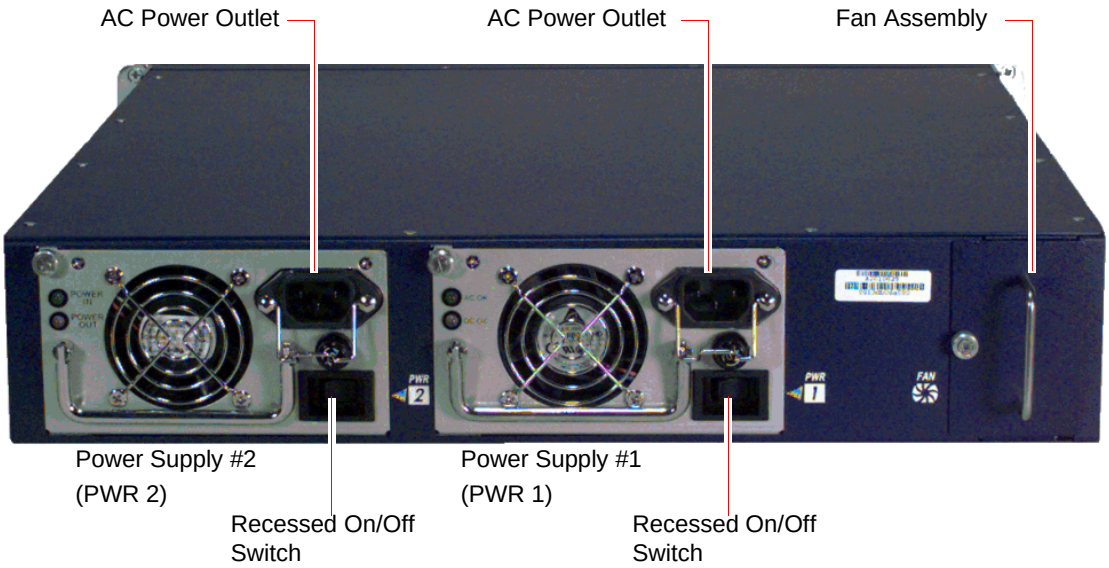
High Availability Interfaces

The NetScreen-500 device has two 10/100 BaseT physical ports (HA1 and HA2) dedicated for high availability (HA) traffic. Using these ports, 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 backup unit. If the master unit fails, the backup unit takes over.

For information on cabling for HA, see "Connecting the NetScreen-500 for High Availability" on page 22.

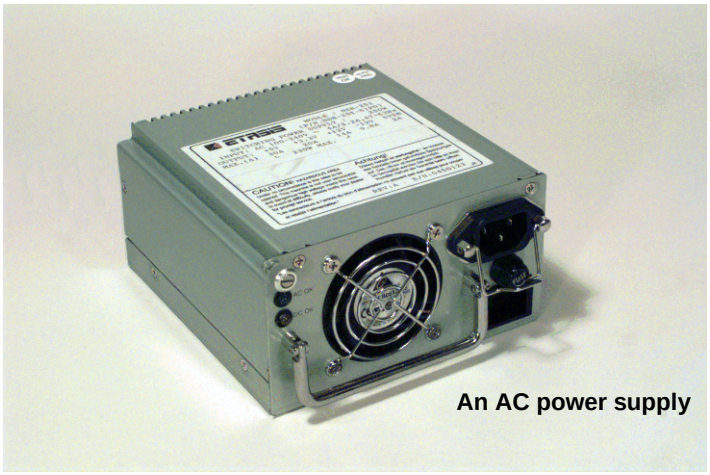
THE REAR PANEL

The rear panel of the NetScreen-500 device contains the power supplies and the fan module.



Power Supplies

The NetScreen-500 device supports two redundant, fault-tolerant and auto-switching power supplies. The power supplies are hot-swappable, so you can remove or replace one power supply without interrupting device operation.



An AC power supply

You can order the NetScreen-500 device with one or two power supplies. These power supplies have the following characteristics:

- The AC power supply weighs about three pounds. The faceplate contains power LEDs, a power switch, a cooling fan vent, and a male power outlet.
- The DC power supply weighs about three pounds. The faceplate contains power LEDs, a power switch, a cooling fan vent, and a terminal block with three connectors for DC power feeds.

Although the NetScreen-500 device can run with one power supply, it is advisable to install both. This practice minimizes the likelihood of system failure due to individual power supply failure.

When the NetScreen-500 device contains two power supplies, they share the power load equally. If one power supply fails, the other assumes the full load automatically and the device sends a system alarm. The PWR 1 or PWR 2 LEDs light up as follows:

LEDs	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.

The Fan Module

The NetScreen-500 has a four-fan module, which you can access on the left rear side of the chassis.

Fan Handle

Fan Module

Warning! *If a fan stops operating due to failure or removal, the system continues to run. However, be sure to replace the fan within ten minutes. Otherwise, heat failure or permanent damage may occur.*

Installing the Device 2

This chapter describes how to install a NetScreen-500 device in an equipment rack.

Topics in this chapter include:

Note: *For safety warnings and instructions, please refer to the* NetScreen Safety Guide. *The instructions in this guide warn you about situations that could cause bodily injury. Before working on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents.*

General Installation Guidelines

Observing the following precautions can prevent injuries, equipment failures and shutdowns.

- Never assume that the power supply is disconnected from a power source. *Always* check first.
- Room temperature might not be sufficient to keep equipment at acceptable temperatures without an additional circulation system. Ensure that the room in which you operate the device has adequate air circulation.
- Do not work alone if potentially hazardous conditions exist.
- Look carefully for possible hazards in your work area, such as moist floors, ungrounded power extension cables, frayed power cords, and missing safety grounds.

Important! *Although you can place the device on a desktop for operation, it is not advisable to deploy a NetScreen-500 Series system in this manner. The best deployment technique is equipment rack mounting, described below.*

Warning! *To prevent abuse and intrusion by unauthorized personnel, install the NetScreen-500 device in a locked-room environment.*

Equipment Rack Mounting

The NetScreen-500 device comes with accessories for mounting the device in a standard 19-inch equipment rack.

Equipment Rack Installation Guidelines

The location of the chassis, the layout of the equipment rack, and the security of your wiring room are crucial for proper system operation.

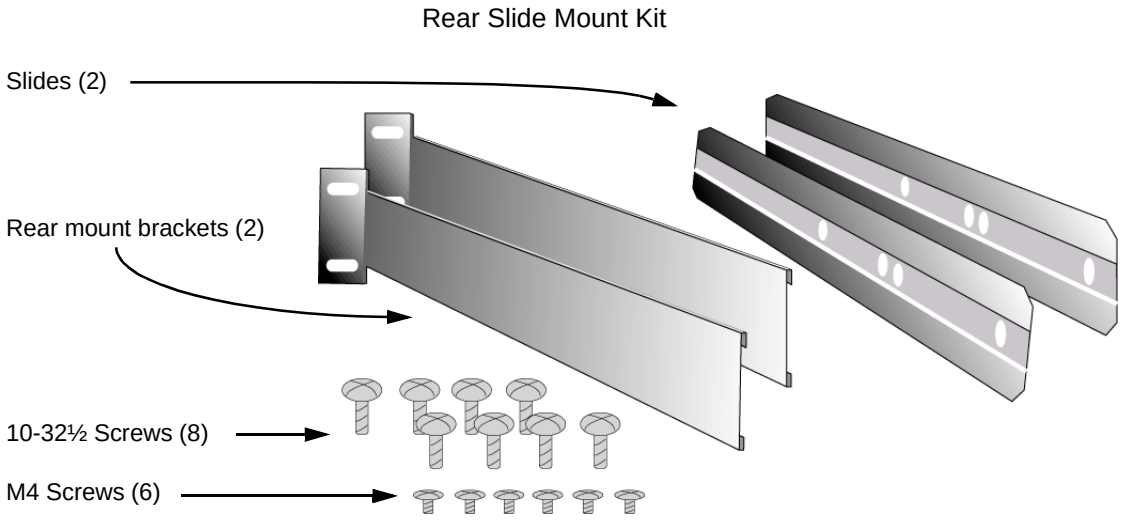
Use the following guidelines while configuring your equipment rack.

- Enclosed racks must have adequate ventilation. Such ventilation requires louvered sides and a fan to provide cooling air.
- When mounting a chassis in an open rack, be sure that the rack frame does not block the intake or exhaust ports. If you install the chassis 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, equipment higher in the rack can draw heat from the lower devices. Always provide adequate ventilation for equipment at the bottom of the rack.
- Baffles can isolate exhaust air from intake air. The best placement of the baffles depends on the airflow patterns in the rack.

Equipment Rack Accessories and Required Tools

Rack mounting requires the following accessories and tools:

- 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)



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

- Front mount
- Mid mount
- Rear-and-front mount.

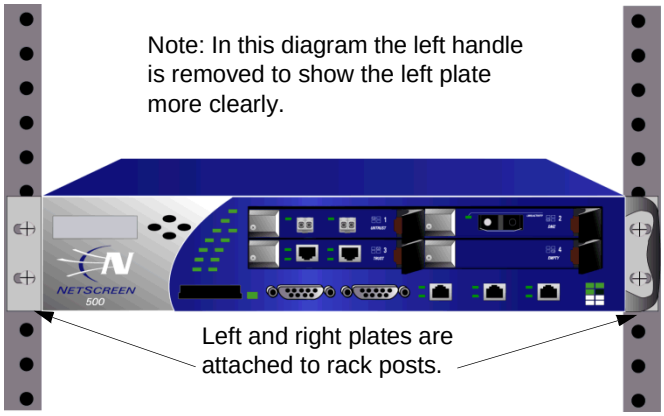
Note: *NetScreen strongly recommends the rear-and-front rack mount configuration.*

Front Mount

To front-mount the NetScreen-500 device:

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.*



Mid Mount

To mid-mount the NetScreen-500 device:

1. 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.

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.

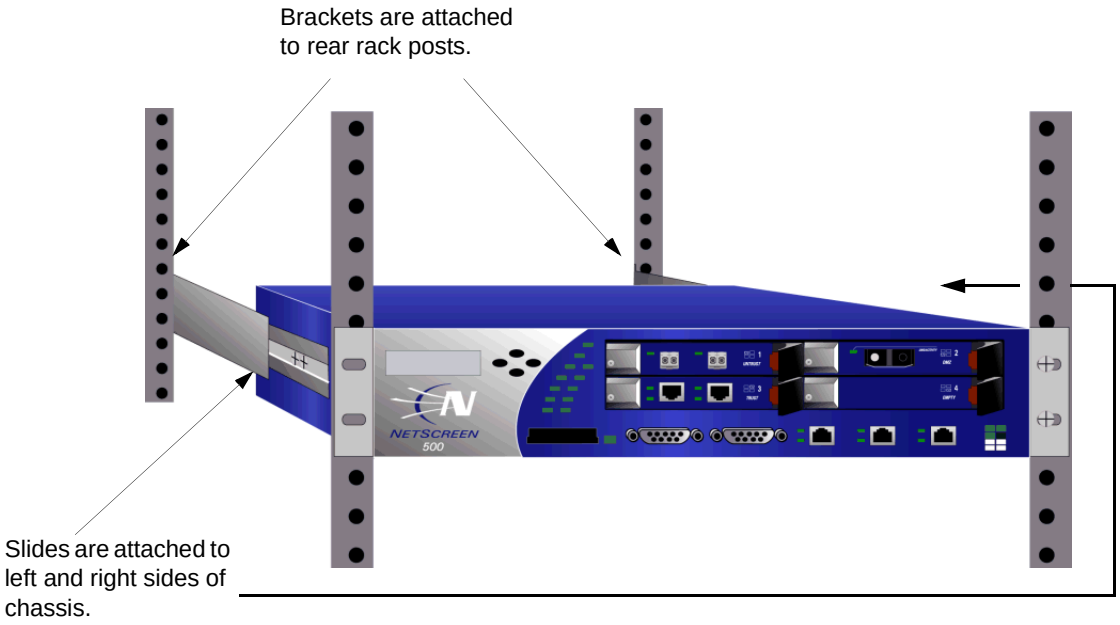
Note: *Depending on the depth of your equipment rack, you can attach the slides along the length of the sides or extending over the rear of the chassis.*

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.
4. Push the NetScreen-500 forward until the left and right plates contact the front rack posts.

5. Screw the left and right plates to the rack.



Configuring the Device 3

This chapter describes how to connect a NetScreen-500 system to your network and perform initial configuration on the device.

Topics in this chapter include:

Note: *For safety warnings and instructions, please refer to the* NetScreen Safety Guide. *The instructions in this guide warn you about situations that could cause bodily injury. Before working on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents.*

OPERATIONAL MODES

The NetScreen-500 Series supports two device modes, Transparent mode and Route mode. The default mode is Transparent.

Note: *Because you enable NAT capability by configuring interfaces and creating security policies, NAT is not considered a device mode. To configure your device for NAT, the device must be in Route mode.*

Transparent Mode

In Transparent mode, the NetScreen-500 device operates as a Layer-2 bridge. Because the device cannot translate packet IP addresses, it cannot perform Network Address Translation (NAT). Consequently, any IP address in your trusted (local) networks must be public, routable, and accessible from untrusted (external) networks.

In Transparent mode, the IP addresses for the Trust security zone and Untrust security zone are 0.0.0.0, thus making the NetScreen device invisible to the network. However, the device can still perform firewall, VPN, and traffic management according to configured security policies.

Route Mode

In Route mode, the NetScreen-500 device operates at Layer 3. Because you can configure each interface using an IP address and subnet mask, you can configure individual interfaces to perform NAT.

- When the interface performs NAT services, the device translates the source IP address of each outgoing packet into the IP address of the untrusted port. It also replaces the source port number with a randomly-generated value. It performs translations using either Mapped IP (MIP) or Virtual IP (VIP).
- When the interface does *not* perform NAT services, the source IP address and port number in each packet header remain unchanged. Therefore, your local hosts must have public IP addresses, and you cannot assign the packet source IP addresses using MIP or VIP.

For more information on NAT, see the *NetScreen Concepts and Examples ScreenOS Reference Guide*.

Important! *Performing the setup instructions below configures your device in Route mode. To configure your device in Transparent mode, see the* NetScreen Concepts and Examples ScreenOS Reference Guide.

THE NETSCREEN-500 INTERFACES

The NetScreen-500 device provides physical ports, each of which can serve as a physical interface. In addition, you can configure ethernet ports to serve as virtual (*logical*) interfaces.

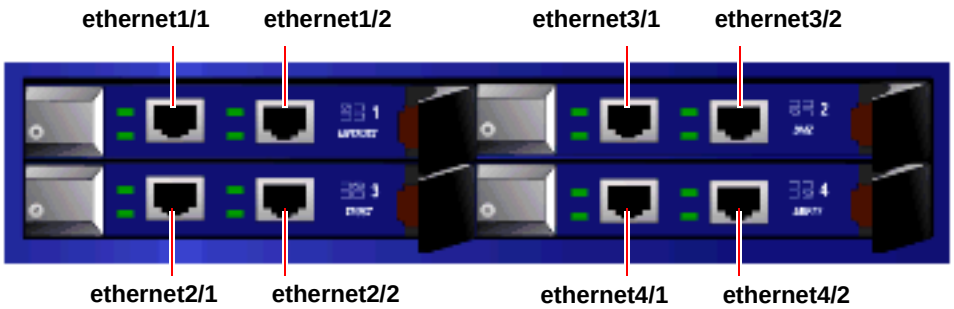
Configurable Interfaces

The interfaces available on the NetScreen-500 are as follows.:

Interface Type	Description
Ethernet interfaces	**ethernet***n1*/*n2* specifies a physical ethernet interface, denoted by an interface module in a slot (*n1*) and a physical port (*n2*) on the module.
	ethernet*n1*/*n2*.*n3* specifies a logical interface, denoted by an interface module in a slot (*n1*), a physical port (*n2*) on the module, and a logical interface number (**.***n3*). You create logical interfaces using the **set interface** command.
Layer-2 interfaces	**vlan1** specifies the interface used for VPNs while the NetScreen device is in Transparent mode.
	v1-trust specifies a Layer-2 interface bound to the V1-Trust zone. Use this interface when the device is in Transparent mode.
	v1-untrust specifies a Layer-2 interface bound to the V1-Untrust zone. Use this interface when the device is in Transparent mode.
	v1-dmz specifies a Layer-2 interface bound to the V1-DMZ zone. Use this interface when the device is in Transparent mode.
Tunnel interfaces	**tunnel.***n* specifies a tunnel interface. Use this interface for VPN traffic.
Function interfaces	**mgt** specifies an interface bound to the MGT zone.
	ha1 and **ha2** specify the names of the dedicated HA ports.

The Ethernet Interfaces

The ethernet interfaces are located on the interface modules (see "Interface Modules" on page 5). The interface names are as follows:



Interfaces to Change During Initial Configuration

The default IP address and subnet mask settings for NetScreen-500 interfaces are 0.0.0.0 and 0.0.0.0, respectively. The exception is **vlan1**, a special interface used only in Transparent mode. The default IP address and subnet mask settings for **vlan1** are 192.168.1.1 and 255.255.255.0, respectively.

- For all operational modes, it is advisable to change the IP address and subnet mask for the **MGT** interface, and to use it exclusively for out of band management.
- To access the **vlan1** interface in Transparent mode, you must change the IP address and subnet mask of **vlan1** to match your current network.
- In Transparent mode, *only* the **MGT** and **vlan1** interfaces may have a new IP address and subnet mask. All others must keep their default IP address and subnet mask settings (0.0.0.0 and 0.0.0.0, respectively).
- In Route mode (with or without NAT), at least 2 ethernet interfaces must have new IP addresses and subnet masks.

Connecting the Device to a Network

The NetScreen-500 chassis has four interface module bays, which can contain the following types of modules:

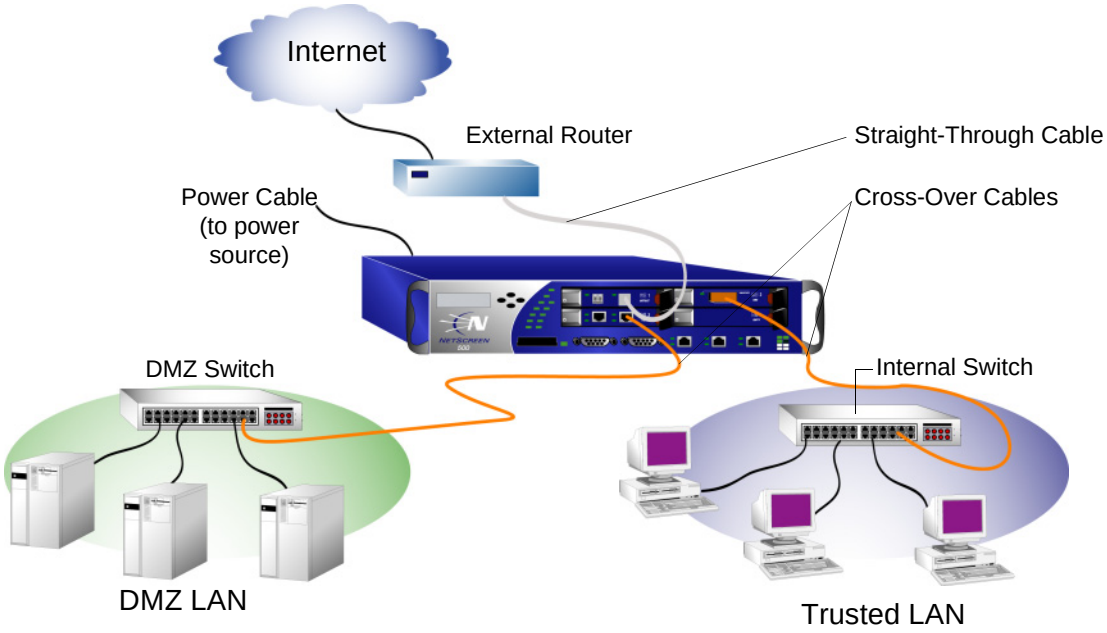
- 10/100 Mbps interface module, for 10/100 BaseT connections
- GBIC interface module, for fiber-optic connections
- Mini-GBIC interface module, for fiber-optic connections

The type of network used by your organization determines the kind of interface needed to connect the NetScreen-500 device. (For more information on interface modules, see "Interface Modules" on page 5.)

Note: *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 in this chapter do not work, try other cable configurations until a link light indicates an active link.*

Connecting the NetScreen-500 as a Single Security Appliance

The following illustration shows typical cabling for 10/100 BaseT networks. (For fiber optic networks, use optical cables for all network connections.)



To add a NetScreen-500 device to your network:

1. (Optional) Install the NetScreen-500 device in an equipment rack (see "Equipment Rack Mounting" on page 12).
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.

> ***Note:*** *Whenever you deploy both power supplies in a NetScreen-500 device, connect each power supply to a different power source, if possible. If one power source fails, the other source might still be operative.*

4. If your network is 10/100 BaseT, connect a RJ-45 cross-over cable from the right interface of Module 2 (**ethernet2/2**) to the internal switch, router, or hub.

   or

   If your network is fiber optic, connect an optical cable from the right interface of Module 2 (**ethernet2/2**) to the internal switch, router, or hub.

   Note: *Check your router, hub, switch, or PC documentation to see if these devices require any further configuration. In addition, see if it is necessary to switch OFF the power to any new device you add to the LAN.*

5. If your network is 10/100 BaseT, connect a RJ-45 straight-through cable from the right interface of Module 1 (**ethernet1/2**) to the external router.

   or

   If your network is fiber optic, connect an optical cable from the right interface of Module 1 (**ethernet1/2**) to the external router.

6. If your network is 10/100 BaseT, connect a RJ-45 cross-over cable from the right interface of Module 3 (**ethernet3/2**) to the DMZ switch, router, or hub.

   or

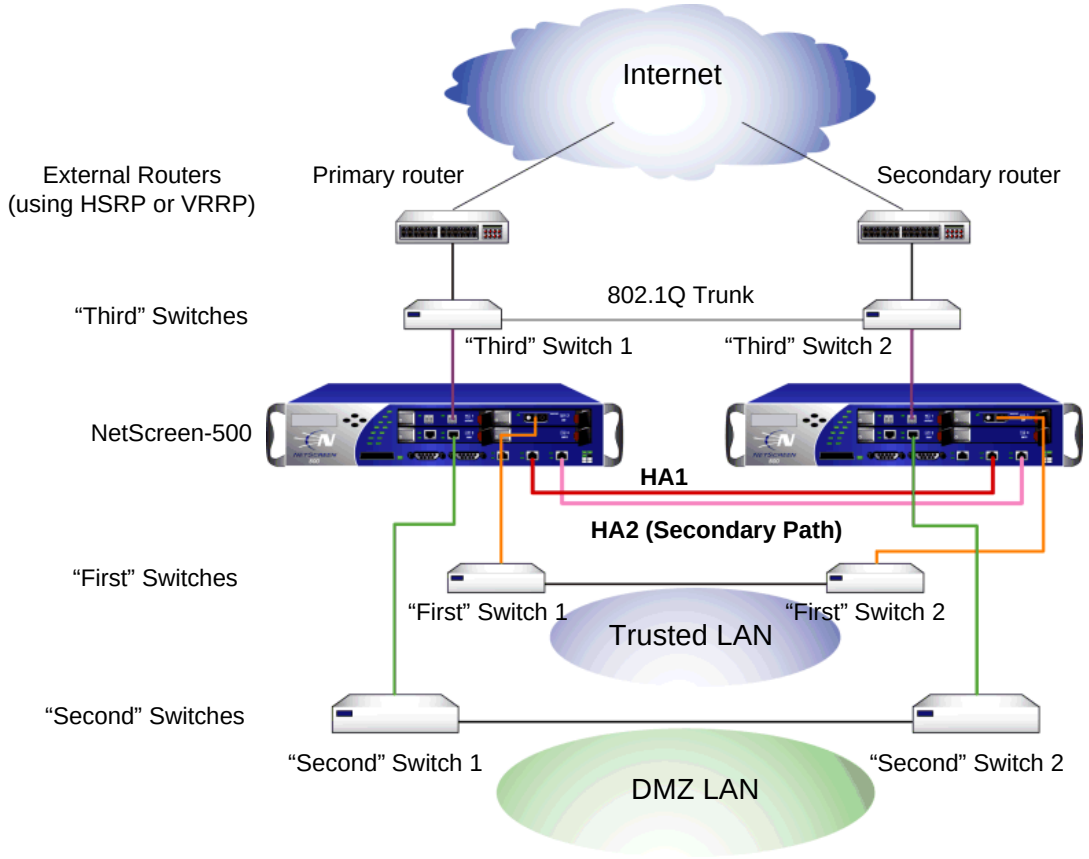
   If your network is fiber optic, connect an optical cable from the DMZ interface to the right interface of Module 3 (**ethernet3/2**) to the DMZ switch, router, or hub.

7. Flip the ON/OFF switch to the ON position.
8. After the NetScreen-500 boots up, the power, status, and link LEDs should light up as follows:
   - The PWR LED for each deployed power supply 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 5.)

Connecting the NetScreen-500 for High Availability

The NetScreen-500 chassis has two high-availability ports, HA1 and HA2. You can use these ports to cable two or more devices together, then configure the devices to work as a *redundant group*. A redundant group consists of a master device and at least one backup device. If the master device fails, a backup device takes over as the new master, thus avoiding interruption of services.

Note: *For more information on HA configuration, see the* NetScreen Concepts & Examples ScreenOS Reference Guide.



Note: *The cabling instructions given below reproduce the configuration shown here. However, this is not the only possible HA configuration. In addition, the instructions assume that all physical ports and interfaces are still set at their default settings. If you have changed the port and interface configurations, the instructions below might not work properly.*

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

1. (Optional) Install the NetScreen-500 devices in an equipment rack (see "Equipment Rack Mounting" on page 12).
2. Make sure that all ON/OFF power supply switches are OFF.
3. Connect the power cables to each NetScreen-500 power supply and connect them to a power source.

   Note: *Whenever you deploy both power supplies in a NetScreen-500 device, connect each power supply to a different power source, if possible. If one power source fails, the other source might still be operative.*

4. Connect a 10/100 BaseT cross-over cable from the HA1 port on one device to the HA1 port on the second device.
5. Connect a 10/100 BaseT cross-over cable from the HA2 port on one device to the HA2 port on the second device.

Master Unit

6. If your network is 10/100 BaseT, connect a cross-over cable from **ethernet2/2** to the switch labeled “First Switch 1” in the diagram above.

   or

   If your network is fiber optic, connect an optical cable from **ethernet2/2** to the switch labeled “First Switch 1” in the diagram above.
7. If your network is 10/100 BaseT, connect a cross-over cable from **ethernet3/2** to the switch labeled “Second Switch 1” in the diagram above.

   or

   If your network is fiber optic, connect an optical cable from **ethernet3/2** to the switch labeled “Second Switch 1” in the diagram above.
8. If your network is 10/100 BaseT, connect a straight-through cable from **ethernet1/2** to the switch labeled “Third Switch 1” in the diagram above.

   or

   If your network is fiber optic, connect an optical cable from **ethernet1/2** to the switch labeled “Third Switch 1” in the diagram above.

Backup Unit

9. If your network is 10/100 BaseT, connect a cross-over cable from **ethernet2/2** to the switch labeled “First Switch 2” in the diagram above.

   or

   If your network is fiber optic, connect an optical cable from **ethernet2/2** to the switch labeled “First Switch 2” in the diagram above.
10. If your network is 10/100 BaseT, connect a cross-over cable from **ethernet3/2** to the switch labeled “Second Switch 2” in the diagram above.

    or

    If your network is fiber optic, connect an optical cable from **ethernet3/2** to the the switch labeled “Second Switch 2” in the diagram above.
11. If your network is 10/100 BaseT, connect a straight-through cable from **ethernet1/2** to the switch labeled “Third Switch 2” in the diagram above.

    or

    If your network is fiber optic, connect an optical cable from **ethernet1/2** to the switch labeled “Third Switch 2” in the diagram above.

Switches

12. Cable together the “First” switches (which are connected to the **ethernet2/2** ports).
13. Cable together the “Second” switches (which are connected to the **ethernet3/2** ports).
14. Cable together the “Third” switches (which are connected to the **ethernet1/2** ports).
15. Cable to routers the “Third” switches (which are connected to the **ethernet1/2** ports).

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). For the best configuration method, see the documentation for your switch or router.*

16. Turn ON both NetScreen-500 devices.

Performing Initial Connection and Configuration

To establish the first console session with the NetScreen-500 device, use a vt100 terminal emulator program through the provided DB9 serial port connector.

Establishing a Terminal Emulator Connection

To establish an initial console session:

1. Plug the female end of the supplied DB-9 serial cable into the serial port of your PC. (Be sure that the DB-9 clip is seated properly and secured with the thumbscrews.)
2. Plug the male end of the DB-9 serial cable into the Console port of the NetScreen-500 device. (Be sure that the DB-9 clip is seated properly and secured with the thumbscrews.)
3. Launch a Command Line Interface (CLI) session between your PC and the NetScreen-500 device using a standard serial terminal emulation program such as Hilgraeve Hyperterminal (provided with your Windows PC). The settings should be as follows:

   - Baud Rate to 9600
   - Parity to No
   - Data Bits to 8
   - Stop Bit to 1
   - Flow Control to none

4. Press the ENTER key to see the login prompt.
5. At the login prompt, type **netscreen**.
6. At the password prompt, type **netscreen**.

   Note: *Use lowercase letters only. Both login and password are case-sensitive.*

7. (Optional) By default, the console times out and terminates automatically after 10 minutes of idle time. To change this timeout interval, execute the following command:

   set console timeout *number*

   where *number* is the length of idle time in minutes before session termination. To prevent any automatic termination, specify a value of 0.

Changing Your Login Name and Password

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

```
set admin name name_str
set admin password pswd_str
save
```

For information on creating different levels of administrators, see "Administration" in the *NetScreen Concepts and Examples ScreenOS Reference Guide*.

Setting Port and Interface IP Addresses

Through the CLI, you can execute commands that set IP address and subnet mask values for most of the physical interfaces. Use the CLI **save** command to save your configuration.

Viewing Current Interface Settings

To begin the configuration process, it is advisable to view existing port settings by executing the following command:

```
get interface
```

This command displays current port names, IP addresses, MAC addresses, and other useful information.

Setting the IP Address of the Management Interface

The default IP address of the management port (MGT) is 192.168.1.1. If you do not wish to use this default IP address, you need to assign the port a new one.

To set the IP address of the MGT port:

1. Choose an unused IP address within the current address range of your Local Area Network.
2. Set the MGT port to this unused IP address by executing the following command:

   set interface mgt ip *ip_addr/mask*

   For example, to set the IP address and subnet mask of the MGT port to 10.100.2.183 and 255.255.0.0, respectively:

   set interface mgt ip 10.100.2.183/16

3. To confirm the new port settings, execute the following command:

   get interface mgt

Setting the IP Address for the Trust Zone Interface

The NetScreen-500 device usually communicates with your protected network through an interface bound to the Trust zone. To allow an interface to communicate with internal devices, you must assign it the IP address and subnet mask for your protected network.

To set up the **ethernet2/2** interface to communicate with your trusted network:

1. Determine the IP address and subnet mask of your trusted network.
2. Set the **ethernet2/2** interface to the Trust zone by executing the following command:

   set interface ethernet2/2 zone trust

3. Set the IP address and subnet mask by executing the following command:

   set interface ethernet2/2 ip *ip_addr/mask*

   where *ip_addr* is the IP address and *mask* is the subnet *mask*. For example, to set the IP address and subnet mask of the **ethernet3** interface to 10.250.2.1/16:

   set interface ethernet2/2 ip 10.250.2.1/16

4. (Optional) To confirm the new port settings, execute the following command:

   get interface ethernet2/2

Setting the IP Address for the Untrust Zone Interface

The NetScreen-500 device usually communicates with external (untrusted) devices through an interface bound to the Untrust zone. To allow an interface to communicate with external devices, you must assign it a public IP address.

To set up the **ethernet2/1** interface to communicate with external devices:

1. Choose an unused public IP address and subnet mask.
2. Set the **ethernet2/1** interface to the Untrust zone by executing the following command:

   set interface ethernet2/1 zone untrust

3. Set the IP address and subnet mask by executing the following command:

   set interface ethernet2/1 ip *ip_addr/mask*

   where *ip_addr* is the IP address and *mask* is the subnet *mask*. For example, to set the IP address and subnet mask of the **ethernet2/3** interface to 172.16.20.1/16:

   set interface ethernet2/1 ip 172.16.20.1/16

4. (Optional) To confirm the new interface settings, execute the following command:

   get interface ethernet2/1

Allowing Outbound Traffic

By default, the NetScreen-500 device does not allow inbound or outbound traffic, nor does it allow traffic to or from the DMZ. To permit (or deny) traffic, you must create access policies.

The following CLI command creates an access policy that permits all kinds of outbound traffic, from any host in your trusted LAN to any device on the untrusted network.

```
set policy from trust to untrust any any any permit
save
```

Important! *Your network might require a more restrictive policy than the one created in the example above. The example is NOT a requirement for initial configuration. For detailed information about access policies, see the* NetScreen Concepts and Examples ScreenOS Reference Guide.

Changing Your Login Name and Password

Because all NetScreen products use the same default login name and password (**netscreen**), it is highly advisable to change them immediately.

To change the login name and password:

```
set admin name name_str
set admin password pswd_str
save
```

Note: *If you forget your password, see* *"Configuring the Chassis Alarm" on page 30*.

Configuring the Device for Telnet and WebUI Sessions

In addition to terminal emulator programs, you can use Telnet (or dialup) to establish console sessions with the NetScreen-500 device. In addition, you can start management sessions using the NetScreen WebUI, a web-based GUI management application.

Starting a Console Session Using Telnet

To establish a Telnet session with the NetScreen-500 device:

1. Connect a RJ-45 cable from the MGT interface the internal switch, router, or hub in your LAN (see "Setting the IP Address for the Trust Zone Interface" on page 27).
2. Open a Telnet session, specifying the current MGT interface IP address. For example, in Windows, click **Start >> Run**, enter **telnet** *ip_addr (*where *ip_addr* is the IP address of the MGT interface), and then click **OK.**

   For example, if the MGT interface has an IP address of 10.100.2.183, enter:

   telnet `10.100.2.183`
3. At the Username prompt, type your user name (default is **netscreen**).
4. At the Password prompt, type your password (default is **netscreen**).

   Note: *Use lowercase letters only. Both Username and Password are case-sensitive.*
5. (Optional) By default, the console times out and terminates automatically after 10 minutes of idle time. To change this timeout interval, execute the following command:

   set console timeout *number*

   where *number* is the length of idle time in minutes before session termination. To prevent any automatic termination, specify a value of 0.

Starting a Console Session Using Dialup

Each NetScreen-500 device provides a modem port that allows you to establish a remote console session using a dialup connection through a 9600 bps modem. Dialing into the modem establishes a dialup console connection.

Note: *The Terminal type for dialup sessions must be vt100. For example, in Hilgraeve HyperTerminal (a commonly-used terminal application), click* ***Connect****, select* ***Remote System*** *from the dropdown menu, then select* ***vt100*** *from the Term Type menu.*

Establishing a GUI Management Session

To access the NetScreen-500 device with the WebUI management application:

1. Connect your PC (or your LAN hub) to the MGT port using a Category-5 Ethernet cable.
2. Launch your browser, enter the IP address of the MGT port in the URL field, and then press Enter.

For example, if you assigned the MGT port an IP address of 10.100.2.183/16, enter the following:

```
10.100.2.183
```

The NetScreen WebUI software displays the Enter Network Password prompt.

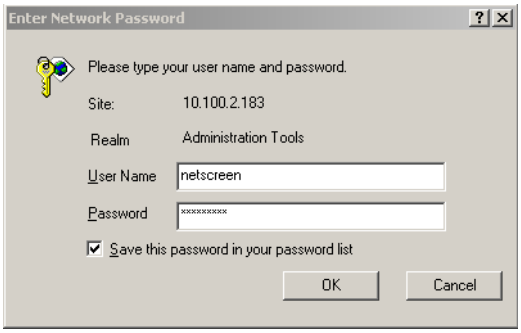


Figure 3-1 Enter Network Password Dialog Box

3. Enter **netscreen** in both the **User Name** and **Password** fields, then click **OK**. (Use lowercase letters only. The User Name and Password fields are both case sensitive.)

   The NetScreen WebUI application window appears.

Configuring the Chassis Alarm

The NetScreen-500 allows you to configure the chassis alarm, an audible warning that sounds when a system failure or hazardous event occurs.

To specify which failures and events trigger the chassis alarm:

1. Configure the audible alarms by executing the following command:

   `set audible-alarm` *`string`*

   where *string* can be any of the following keywords:

   - **all** Enables all chassis alarms.
   - **fan-failed** Sets the chassis alarm to sound when a fan fails.
   - **module-failed** Sets the chassis alarm to sound when an interface module fails.
   - **power-failed** Sets the chassis alarm to sound when a power supply fails.
   - **temperature** Sets the chassis alarm to sound when the temperature goes outside of the acceptable range.

2. (Optional) Confirm the new alarm settings by executing the following command:

   ```
   get chassis
   ```

PERFORMING INITIAL CONFIGURATION USING THE MENU SYSTEM

Through the control pad menu interface, you can configure many device settings, including system and interface IP addresses.

Note: *You cannot use the control pad menu system to create an access policy, change the administrator's login name and password, or test the configuration. To perform these tasks you must use either the WebUI or CLI. Even so, the control pad menu system is a convenient tool for configuring interfaces and performing other initial configurations on site.*

For more information on the control pad menu system, see "LCD and Control Pad Menu Interface" on page 2.

Setting Interface IP Addresses

The most important initial configuration task you can perform using the control pad menu interface is setting MGT, vlan1, and ethernet interface IP addresses and subnet masks.

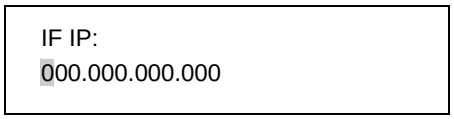
Setting the MGT Interface IP Address and Netmask

1. Navigate to the following menu location:

   1. Setting >> 12. Interface >> 128. MGT >> 1281. IF IP:

2. Press the RIGHT control key.

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

3. Use the UP and DOWN control keys to scroll through digits 0-2. When you reach the digit you want, move to the next digit by pressing the RIGHT control key.
4. Repeat Step 3 until you have specified all digits for the MGT interface IP address.
5. With the cursor positioned on the far right digit, press the RIGHT control key. When prompted to confirm the new MGT IP address, press the RIGHT control key again.
6. Navigate to the following menu location:

   1. Setting >> 12. Interface >> 128. MGT >> 1282. IF Netmask:

7. Press the RIGHT control key, and select the digits for the MGT interface netmask as you did for the IP address.

Setting the vlan1 IP Address for Transparent Mode

To manage the NetScreen device over a network connection, you must change the vlan1 IP address from its default (192.168.1.1) to one that is appropriate for your network.

To change the system IP address:

1. Setting >> 12. Interface >> 129. vlan1 >> 1291. IF Netmask:
2. Press the RIGHT control key.

   The current vlan1 interface IP address appears, with the cursor flashing over the far left digit.

   ```
   IF IP:
   192.168.001.001
   ```

3. Use the UP and DOWN control keys to scroll through digits 0-2. When you reach the digit you want, move to the next digit by pressing the RIGHT control key.
4. Repeat Step 3 until you have specified all digits for the vlan1 interface IP address.
5. With the cursor positioned on the far right digit, press the RIGHT control key. When prompted to confirm the new vlan1 IP address, press the RIGHT control key again.

Setting Ethernet Interface IP Address and Netmask

1. 1. Setting >> 12. Interface >> 12*n*. ethernet*n1*/*n2* >> 12*n*1. IF IP:

   where *n* uniquely identifies the interface, *n1* identifies the interface module slot, and *n2* represents a physical interface on the module.
2. Press the RIGHT control key.

   The current ethernet interface IP address appears, with the cursor flashing over the far left digit.

   ```
   IF IP:
   000.000.000.000
   ```

3. Use the UP and DOWN control keys to scroll through digits 0-2. When you reach the digit you want, move to the next digit by pressing the RIGHT control key.
4. Repeat Step 3 until you have specified all digits for the ethernet interface IP address.
5. With the cursor positioned on the far right digit, press the RIGHT control key. When prompted to confirm the new ethernet IP address, press the RIGHT control key again.

6. Navigate to the following menu location:

   1. Setting >> 12. Interface >> 12*n*. ethernet*n1*/*n2* >> 12*n*2. IF Netmask:

   where *n* uniquely identifies the interface, *n1* identifies the interface module slot, and *n2* represents a physical interface on the module.

7. Press the RIGHT control key, and select the digits for the ethernet interface netmask as you did for the IP address.

RESETTING THE DEVICE TO FACTORY DEFAULT SETTINGS

If you lose the admin password, you can use the following procedure to reset the NetScreen device to its default settings. This destroys any existing configurations, but restores access to the device. To perform this operation, you need to make a console connection, as described in "Establishing a Terminal Emulator Connection" on page 25.

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.

Servicing the Device 4

This chapter describes service and maintenance procedures for your NetScreen-500 system.

Topics in this chapter include:

Note: *For safety warnings and instructions, please refer to the* NetScreen Safety Guide. *The instructions in this guide warn you about situations that could cause bodily injury. Before working on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents.*

Removing and Inserting Interface Modules

The NetScreen-500 has four interface module bays. The supplied modules are pre-installed, although they are removable and replaceable.

There are three types of interface modules:

- 10/100 BaseT module
- GigaBit Interface Connector (GBIC) module
- Mini-GBIC Interface Connector module

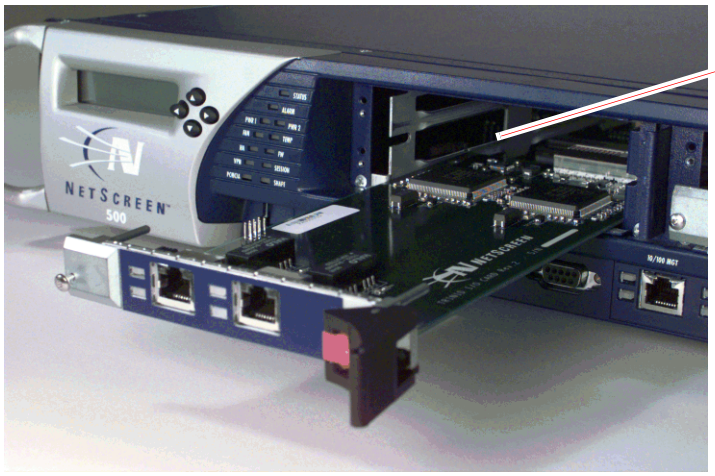
You can use these interface modules in whatever combination and arrangement suits the special needs of your network infrastructure.

Inserting Interface Modules

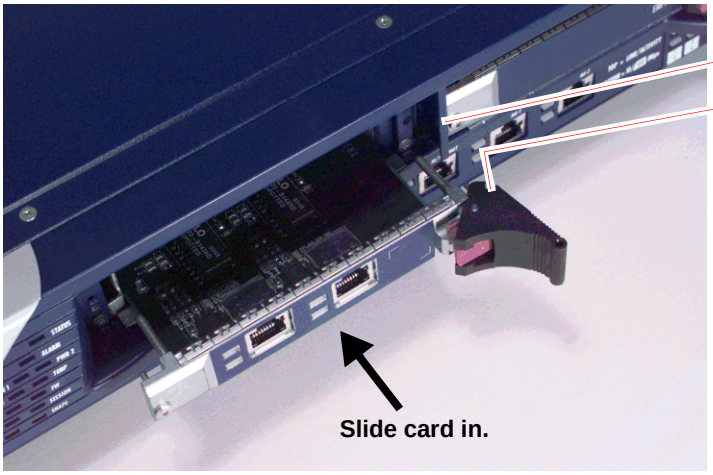
To insert an interface modue into a module bay:

Warning! *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.



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

3. Simultaneously push in the front left corner of the module (with your left thumb) and push the latch in and slightly toward your left (with your right thumb) until the red locking tab clicks into place.

Important! *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

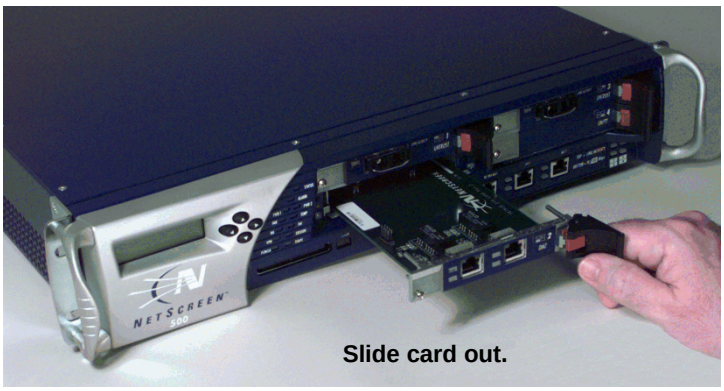
To remove an interface module from a bay:

Warning! *While 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. Pull the latch to the right, popping the card free.

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



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

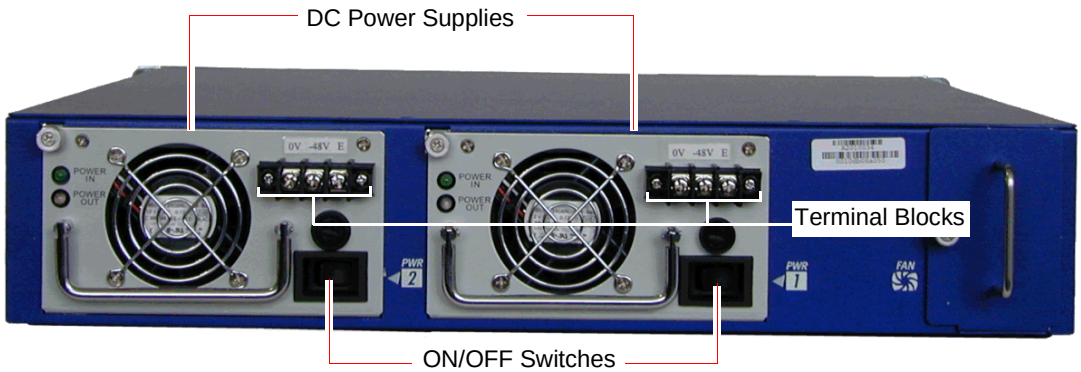
INSTALLING POWER SUPPLIES

Although the NetScreen-500 device can run with one power supply, it is advisable to install both to minimize the likelihood of system failure due to individual power supply failure.

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 power supply switches are in the OFF position (right side pressed in).*

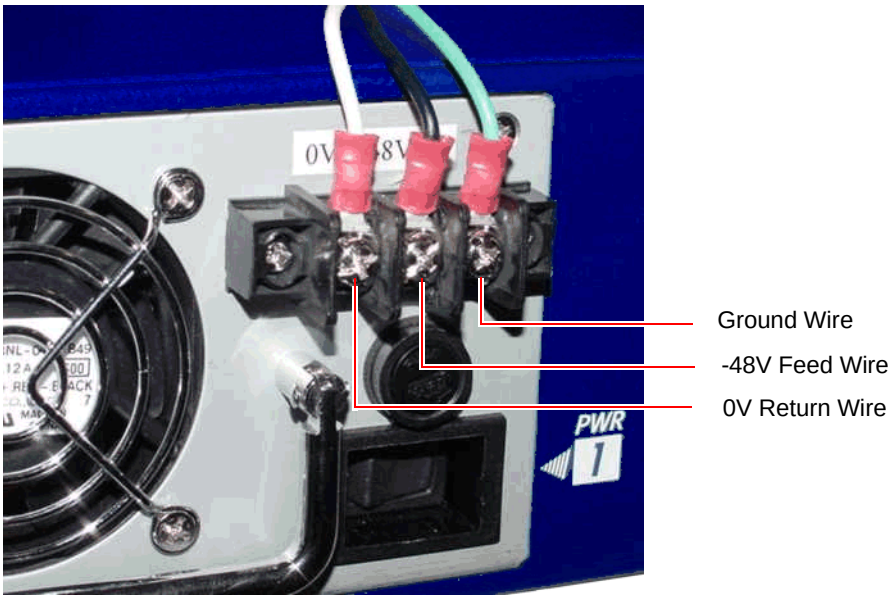
Wiring the DC Power Supplies

The DC power supplies are located in the back of the chassis.



To connect DC power feeds to the terminal blocks:

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



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 (right side pressed in).*

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

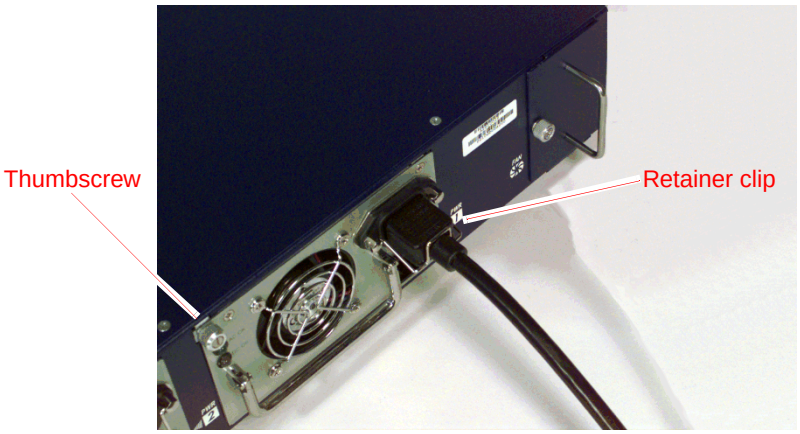
1. Loosen the three retaining screws on the terminal block.
2. Remove the feed wires.
3. Turn the thumbscrew counterclockwise to release the power supply.
4. Lift the handle and, gripping the handle, pull the power supply straight out.
5. Insert the new power supply into the bay.
6. Secure the power supply in place by tightening the thumbscrew clockwise.

Reconnect the wires as explained in "Wiring the DC Power Supplies" on page 40.

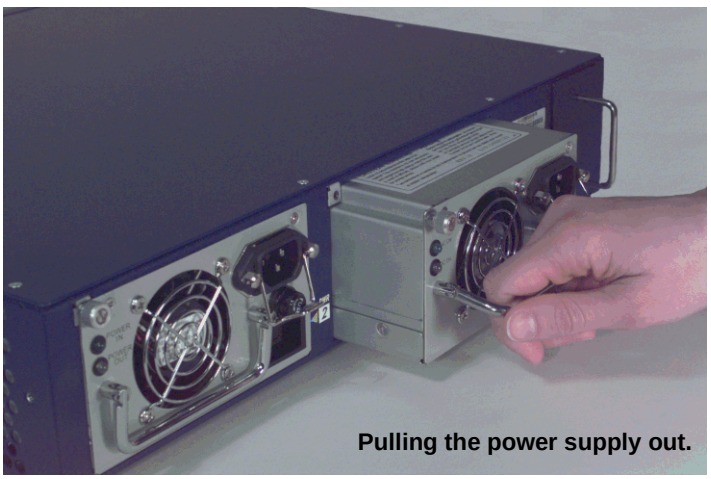
Replacing an AC Power Supply

To replace an AC power supply:

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

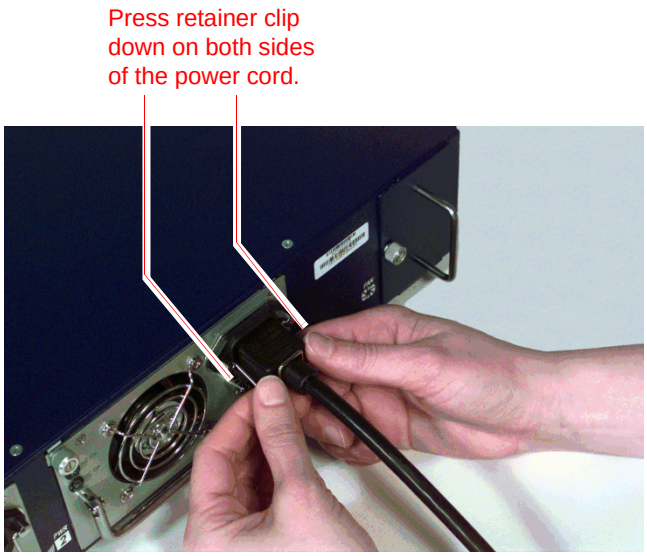


3. Unplug the cord from the power supply.
4. Turn the thumbscrew counterclockwise to release the power supply.
5. Lift the handle and, gripping the handle, gently pull the power supply straight out.



Pulling the power supply 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 THE FAN MODULE

Note: *During the one-year warranty period, you can obtain a replacement fan module by contacting NetScreen Technical support. After the warranty period, contact the NetScreen Sales department.*

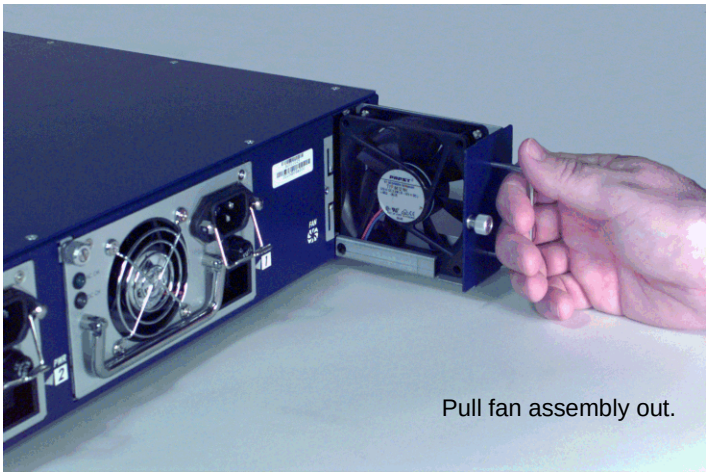
You only need to replace the fan module when a failure occurs. When this happens, the FAN LED glows red, and the device generates an event alarm and a SNMP trap.

To remove the fan module:

1. Turn the captive thumbscrew counterclockwise.

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

Warning! *Do not remove the fan module while the fans are still spinning.*



3. Insert the new fan module in the fan bay, and push it straight in.
4. Secure the fan module in place by tightening the thumbscrew clockwise.

Connecting and Disconnecting Gigabit Ethernet Cables

To connect a Gigabit Ethernet cable to a mini-GBIC connector transceiver port:

1. Hold the cable clip firmly but gently between your thumb and forefinger, with your thumb on top of the clip and your finger under the clip. (Do not depress the clip ejector on top of the clip.)
2. Slide the clip into the transceiver port until it clicks into place.

   Because the fit is close, you may have to apply some force to seat the clip. To avoid clip breakage, apply force evenly and gently.

To remove the cable from the transceiver port:

1. Make sure the black transceiver ejector under the port is not pressed in. Otherwise, when you attempt to remove the cable, the transceiver might come out with the cable still attached.
2. Hold the cable clip firmly but gently between your thumb and forefinger, with your thumb on top of the clip and your finger under the clip.
3. Using your thumb, gently press the clip ejector on top of the clip, down and forward. This action loosens the clip from the transceiver port.
4. Gently but firmly, pull the clip from the transceiver port.

Removing and Installing a mini-GBIC Transceiver

To remove a mini-GBIC-transceiver from a module:

1. Push in the black ejector (located on the underside of the transceiver) until it locks into place, disengaging the transceiver.
2. Grasp the transceiver at both sides and, firmly but gently, pull the transceiver toward you to remove it from the module.

To install a mini-GBIC transceiver into a module:

1. Grasp the transceiver with the label facing up, and insert it into the transceiver slot until seated.
2. Check to see if the black transceiver ejector extends fully out to the front of the ejector slot, flush with the port portion of the transceiver.

Removing and Installing a GBIC Transceiver

There are two types of GBIC transceivers: one has a locking handle to secure the GBIC in the module, the other has clips on either side of the GBIC. To remove a GBIC transceiver from a module:

- If the GBIC has a locking handle, lift the handle up first before sliding the GBIC out of the slot.

- If the GBIC has clips on either side, squeeze the clips and slide the GBIC out of the slot.

To install a GBIC transceiver:

- If the GBIC has a locking handle, slide the GBIC into the slot and then lower the handle on the GBIC.
- If the GBIC has clips on either side, squeeze the clips and slide the GBIC into the slot.

Specifications

This appendix provides general system specifications for the NetScreen-500 system.

NetScreen-500 Attributes

Height: 3.5 inches

Depth: 17 inches

Width: 17.5 inches

Weight: 27 pounds

Electrical Specification

AC voltage: 100 - 240 VAC +/- 10%

DC voltage: -36 to -60 VDC

AC Watts: 100 Watts

DC Watts: 100 Watts

Input frequency: 47 - 63 Hz

Fuse Rating: 5A / 250V

Environmental

Temperature	Operating
Normal altitude	0°- 50° C, 32-122°F
Relative humidity	10-90%
Non-condensing	10-90%

The maximum normal altitude is 12,000 feet (0-3,660 meters)

FIPS Certification

FIPS 140-1 Level 1

Safety Certifications

CSA

EMI Certifications

FCC class A, BSMI, CE class A, C-Tick, VCCI class A

CONNECTORS

The RJ-45 twisted-pair ports are compatible with the IEEE 802.3 Type 10/100 Base-T standard.

The mini-Gigabit transceivers used in NetScreen-500 modules are Shortwave or SX type, so they are good for up to 550 meters. (This varies by manufacturer.) The limit is 850 for the optic LC-type connector. The mini-Gigabit transceivers are compatible with the IEEE 802.3z Gigabit Ethernet standard.

The following table lists media types and distances for the different types of connectors used in the NetScreen-500 Series.

Standard	Media Type	Mhz/Km Rating	Maximum Distance
1000Base-SX	50/125µm Multimode Fiber	400	500 Meters
	50/125µm Multimode Fiber	500	550 meters
	62.5/125µm Multimode Fiber	160	220 meters
	62.5/125µm Multimode Fiber	200	275 meters
1000Base-LX	50/125µm Multimode Fiber	400	550 meters
	62.5/125µm Multimode Fiber	500	550 meters
	9/125µ Single-mode Fiber		10,000 meters
100Base-TX	Category 5 and higher Unshielded Twisted Pair (UTP) Cable		100 meters

SESSIONS

Maximum concurrent sessions: 250,000

Maximum new sessions/second: 17,000

Configuration for Common Criteria, EAL2

B

All NetScreen devices are designed to meet the Common Criteria requirements, and are currently under evaluation for Common Criteria, EAL2. However, there are certain configuration actions that are required for a security administrator to properly secure the device to be in compliance with the Common Criteria EAL2 security target. While these requirements are for anyone needing Common Criteria assurance, they can also be used as general guidelines for administrators wishing to better secure the deployment of a NetScreen device.

Properly Identifying the NetScreen Device for Common Criteria EAL2 Compliance

Before carrying out any step to secure a NetScreen device, you must make sure that the received product has not been tampered with, and ensure that the product received matches the version that is certified as Common Criteria EAL2 compliant.

To ensure that the product has not been tampered with, verify two items:

- The outside packaging cannot show damage, or evidence that it has been opened. If the cardboard shows damage that would allow the device to be removed or exchanged, this may be evidence of tampering.
- The internal packaging cannot show damage or evidence of tampering. The plastic bag should not have a large hole and the label that seals the plastic bag should not be detached or missing. If the bag or the seal are damaged in any way, this may be evidence of tampering.

Both of these tamper evidence criteria must be met to ensure that the product has not been tampered with during shipment.

To verify that the product received is the correct version of hardware and software, run the following command from the Command Line Interface (CLI):

```
get system
```

The output of this command includes two key items, hardware version and software version. The Common Criteria evaluated versions are listed in NetScreen's S*ecurity Target for Common Criteria EAL2*, section 1.1. The hardware and software versions must match the Security Target to be in full compliance with the Common Criteria evaluation.

PROPER STEPS TO SECURE A NETSCREEN DEVICE FOR COMMON CRITERIA EAL2 COMPLIANCE

To configure a NetScreen device to operate securely, and in conformance with the requirements outlined in NetScreen's *Security Target for Common Criteria EAL2*, the following actions must be taken:

- You must configure a Syslog server as a backup for security audit information, and for long-term audit log information storage. This will help prevent a loss in security audit information. See Chapter 2, "Monitoring NetScreen Devices," in Volume 3 of the *NetScreen Concepts & Examples* manual for more information on how to set up and configure a Syslog server to work with NetScreen devices.

  The specific commands required to set up a Syslog server are listed below:

  set syslog config *ip_address security_facility local_facility*

  Note: *The* **set syslog config** *command requires that you define the security facility and local facility. See the* **syslog** *command in the* NetScreen CLI Reference Guide *for a complete list of options for security_facility and local_facility.*

  set syslog enable
  set syslog traffic
  set log module system level *level* **destination syslog**

  Note: *You must enter the* **set log** *command once for each message level. The options for* **level** *are listed below:*

  emergency
  alert
  critical
  error
  warning
  notification
  information

- There are cases where more auditable events can occur than the NetScreen device is able to write to a syslog server. To be compliant with Common Criteria requirements, the NetScreen device must stop further auditable events from occurring until the audit trail is able to handle more traffic. An authorized administrator must enable the following command:

  set log audit-loss-mitigation

- The NetScreen-5XP and NetScreen-5XT have a default policy that allows traffic to traverse the device from the interface in the Trust zone to the interface in the Untrust zone. You must delete this default policy to avoid inadvertently allowing information to traverse the device. See the **policy** commands in the *NetScreen CLI Reference Guide* for more information on how to set and unset policies.

To disable this default policy on the NetScreen-5XP and -5XT, enter the following CLI command:

```
unset policy id 0
```

- NetScreen devices must be configured to prevent all types of Denial of Service (DoS) and attack signatures on every security zone to prevent these types of attacks from occurring on the LAN. See Chapter 2, "Zones," in Volume 2 in the *NetScreen Concepts & Examples* manual for more information on configuring the Screen functions and for descriptions of the attacks that the Screen functions are designed to prevent.

  You must turn on IP spoofing and enable dropping of traffic where there is no source route by using the following command:

  set zone *zone* **screen ip-spoofing drop-no-rpf-route**

  where *zone* is the name of the zone (for example, trust or untrust). See the **zone** commands in the *NetScreen CLI Reference Guide* for more information.

  The screening options that are enabled by default for interfaces in the Untrust security zone in ScreenOS 4.0 are listed below:

Tear-drop Attack Protection	on
SYN Flood Protection (200)	on
Alarm Threshold:	512
Queue Size:	1024
Timeout Value:	20
Source Threshold:	4000
Destination Threshold:	4000
Drop unknown MAC (transparent mode only):	no
Ping-of-Death Protection	on
Source Route IP Option Filter	on
Land Attack Protection	on

  All other security zones have no screens enabled by default. The CLI command below enables all screens, on a per-zone basis (and are applied to all interfaces within that zone):

  set zone *name* **screen all**

  The command **set zone** *name* **screen all** enables all screen functions on all interfaces that are configured within the zone. For the purposes of Common Criteria, you must run the following two commands to protect the internal and external interfaces:

  ```
  set zone untrust screen all
  set zone trust screen all
  ```

  You must run the same command for each additional security zone that is configured and used.

- NetScreen device administrators must choose logins and passwords that are not only long (at least 8 characters), but that also employ as many types of characters as possible. Passwords are case sensitive, so mixing lower case and upper case is required to ensure proper protection. In addition, user names and

passwords should not be easily guessed, such as a mother's maiden name, a birth date, or names of relatives. NetScreen devices ship with a default user name and password of "netscreen". You must change this as soon as possible to prevent unauthorized access. See Chapter 1, "Administration," in Volume 3 in the *NetScreen Concepts & Examples* manual for more information on administrative passwords. The recommended time between password changes is no longer than 30 days to mitigate the effects of a compromised administrator identity.

The following CLI commands, in order, are required to set a new administrator name and password:

```
set admin name name
set admin password password
```

- It is expected and assumed that authorized administrators are not hostile.
- The NetScreen device must be placed in a physically secure location to prevent physical tampering, or device startup or shutdown. All persons who have physical access to this location, including access to the console, must have the same level of trustworthiness as an administrator.
- To place a NetScreen device into a mode consistent with that specified in NetScreen's *Security Target for Common Criteria*, management access must be limited to the locally connected console port. NetScreen devices do not ship this way by default. To limit management access to the console port, the interface that is by default in the V1-Trust or Trust security zone needs to have management access turned off. See the **interface** commands in the *NetScreen CLI Reference Guide* for more information.

  All other interfaces have management access turned off by default, so no action is necessary to turn management off.

  To disable management to the interface in the V1-Trust or Trust security zone, issue the following CLI command:

  ```
  unset interface interface manage
  ```

  For each NetScreen device, you must enter the following commands:

  NetScreen-5XP: **unset interface trust manage**
  NetScreen-5XT: **unset interface trust manage**
  NetScreen-25: **unset interface ethernet1 manage**
  NetScreen-50: **unset interface ethernet1 manage**
  NetScreen-100: **unset interface trust manage**
  NetScreen-204: **unset interface ethernet1 manage**
  NetScreen-208: **unset interface ethernet1 manage**
  NetScreen-500: **unset interface ethernet3/2 manage**
  NetScreen-5200: **unset interface ethernet2/2 manage**
- There are two important steps to take every time a policy is being created. First, all security policies that are created must have counting and logging enabled to ensure that all audit log information is maintained for traffic passing through the device. Second, policies must be as specific as possible to ensure that the traffic being permitted is done intentionally, and not as part of a generic policy.

When creating a policy, always make sure that counting and logging are enabled. This ensures that all traffic matching the policy is logged appropriately.

When creating a policy, always use specific source IP, destination IP, source zone, destination zone, protocol, and service when feasible. One example where it may not make sense to be specific is for traffic destined for an external network for general web access.

The following is an example of a valid policy:

```
set policy id 1 from trust to untrust 192.168.1.2
1.1.1.1 ftp permit count log
```

The above policy allows traffic from 192.168.1.2 to 1.1.1.1 for FTP traffic only, with the Trust zone as the source and the Untrust zone as the destination, and enables logging and counting.

- All traffic from an internal network to an external network must flow through the NetScreen device. Setting up network connections that do not cross the NetScreen device is not a secure setup and leaves the network susceptible to intrusion attacks.
- The CLI is the only administration interface available in the evaluated configuration of the NetScreen devices for Common Criteria EAL2.
- Currently, NetScreen devices are in evaluation for Common Criteria EAL2. This certification is for NetScreen devices to be deployed in environments where the threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.

Starting, Stopping, and Reviewing Audit Logs

The NetScreen device automatically logs the starting and stopping of audit logs. Each time the device boots up, message logging automatically begins (see the Traffic Log messages section in the Messages Log). Upon initial bootup, the message **system is operational** indicates that all message logging has started. The command **get log setting** shows the current state of the logging settings.

To enable or disable any of the eight message logging states, the administrator must issue one of the following commands:

```
set log module system level level-name dest syslog
unset log module system level level-name dest syslog
```

where *level-name* is one of the following:

- emergency
- alert
- critical
- error
- warning
- notification
- information
- debugging

The event log shows the following events:

```
Log setting is modified to {enable|disable} level-name
level by admin name
```

where *level-name* is the same as the *level-name* in the issued command and *name* is the person making the change.

The NetScreen device logs an event each time an audit log is reviewed. The event log will show the following events:

```
Alarm log was reviewed by admin name
Traffic log was reviewed by admin name
Asset recovery log was reviewed by admin name
Self log was reviewed by admin name
Event log was reviewed by admin name
```

where *name* is the person making the change.

Index

N

P

R

S

T

V