NETSCREEN-100

Installer's Guide

Version 4.0 P/N 093-0577-000 Rev.B

Copyright Notice

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-100 is a versatile, purpose-built, high-performance security device that provides IPSec VPN and firewall services for medium and large enterprise offices and service-provider environments.

This manual describes the NetScreen-100 device. It also explains how to perform physical installation, establish connectivity through terminal emulator programs, and perform initial configuration tasks. It also shows how to establish Telnet and WebUI sessions with the device.

GUIDE ORGANIZATION

This manual has three chapters and one appendix.

Chapter 1, "Overview" provides a detailed overview of the NetScreen-100 device, including its front-panel and back-panel features.

Chapter 2, "Installing the Device" describes how to rack-mount the NetScreen-100 device, and connect the device on a network.

Chapter 3, "Configuring the Device" details how to connect the device to the network and perform initial configuration.

Appendix A, "Specifications" provides a list of physical specifications about the NetScreen-100 device.

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-100 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 Variables

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

date_str	A date value.
dom_name	A domain name, such as “acme” in **www.acme.com**.
filename	The name of a file.
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.
loc_str	A location of a file or other resource.
mac_addr	A MAC address.
mask	A subnet mask, such as **255.255.255.0** 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.
string	A character string, such as a comment.
time_str	A time value.
url_str	A URL, such as **www.acme.com**.
vrouter	A local virtual router, such as trust-vr or untrust-vr.
zone	The name of a security zone.

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

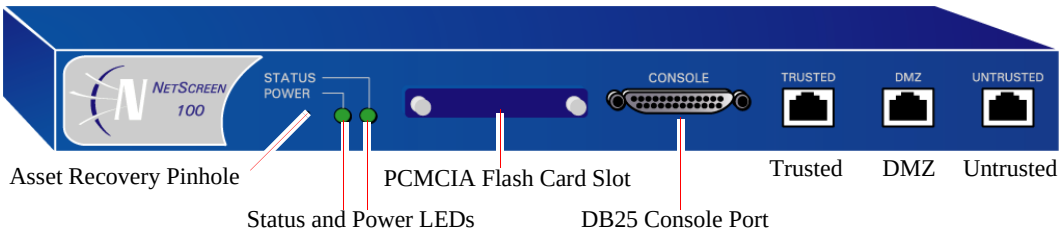
This chapter provides detailed descriptions of the NetScreen-100 system devices, interfaces, power supplies, and fan assemblies.

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 NETSCREEN-100 MODEL

The NetScreen-100 is a chassis-based, rack-mountable network security device with three ethernet 10/100 BaseT interface ports (Trusted, DMZ, and Untrusted). The figure below shows a NetScreen-100 device.



THE FRONT PANEL

The front panel of the NetScreen-100 device includes:

- An Asset Recovery Pinhole
- A Status LED
- A Power LED
- A PCMCIA Flash Card slot
- A DB25 Console port
- Three Ethernet interfaces (Trusted, DMZ, and Untrusted)

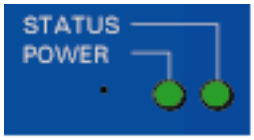
Asset Recovery Pinhole

The Asset Recovery Pinhole is a switch that resets the device to its original default settings. To use this switch, insert a stiff wire (such as a straightened paper clip) into the pinhole.

Warning! *Because resetting the device restores it to the original factory default configuration, any new configuration settings are lost, and the firewall and all VPN service become inoperative.*

Status and Power LEDs

The front panel of each NetScreen-100 device has a Status LED and a Power LED.



LED Name	Purpose	Color	Meaning
Status	System Status	solid amber	At initial power up.
		solid green	At startup and while performing diagnostics.
		blinking green	Normal operation.
		blinking red	Error detected.
Power	Power Supply	green	Power supply is functioning correctly.
		dark	Power supply failure.

PCMCIA Flash Card Slot

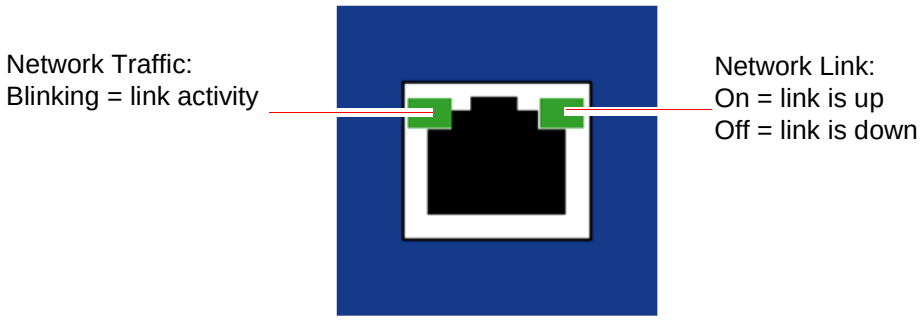
The NetScreen-100 device supports a PCMCIA ATA-compatible flash card. Supported cards include the SanDisk 96-MB and 20-MB CompactFlash. The device automatically detects the presence of a flash card and records the event log to it.

DB25 Console Port

The Console port is a DB-25 serial console port connector. This port is for performing local configuration and administration using a vt100 terminal emulator program.

Ethernet Interfaces

Each Ethernet port is a 10/100 auto-sensing Interface with two link LEDs. The left LED indicates network traffic, and the right LED indicates an active network link.



The Rear Panel

The figure below shows the back panel of a NetScreen-100 device (with an AC power supply.)

Note: *Certain export restrictions may apply to international customers. Check with your sales representative.*

Power Supplies

A NetScreen-100 device can have an AC power supply or a DC power supply.

The DC power supply can operate on one or two DC feeds ranging from -36V to -72V. When you use two feeds, they share the load. If one feed fails, the other automatically assumes the full load.

The internal fuse for the DC power supply is a 3.15A/250V, fast-acting fuse. This is not replaceable.

Installing the Device 2

This chapter describes how to install a device on an equipment rack or desktop, and how to configure the device on a network.

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.

Warning! *To prevent abuse and intrusion by unauthorized personnel, it is extremely important to install the NetScreen system in a locked-room environment.*

PERFORMING EQUIPMENT-RACK INSTALLATION

Although you can install a NetScreen-100 device on a desktop, it is advisable to install the device in an equipment rack if possible.

Equipment Rack Installation Guidelines

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

Use the following guidelines while configuring your equipment rack.

- Enclosed racks must have adequate ventilation. 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 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.

You can mount the device in a standard 19-inch equipment rack. Rack mounting requires the following tools:

- 1 Phillips-head screwdriver
- Rack-compatible screws
- The supplied front-mount brackets

You can only front-mount a NetScreen-100 device.

Rack-Mounting the Device

To mount the NetScreen-100 device on your equipment rack:

1. Screw the front mount bracket to the side of the chassis.
2. Screw the front mount bracket to the rack, as shown below.

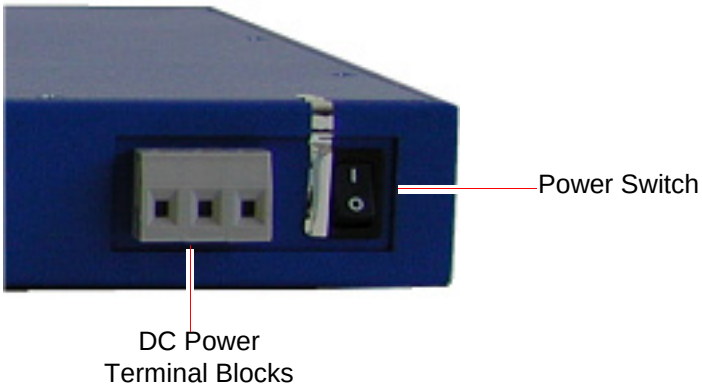
Connecting the Power

To connect the power supply to the NetScreen-100 device:

1. Plug the female end of a power cable into the male power receptacles on the back of the system.
2. Turn the Power switch ON.

WIRING A DC POWER SUPPLY

The DC power supply, ON/OFF switch, and terminal blocks, are located in the back of the chassis of the power supply unit.



Warning: *You must shut off current to the DC feed wires before connecting the wires to the power supplies. Also, make sure that the ON/OFF switches are in the OFF position (right side pressed in).*

NetScreen-100 devices can operate on one feed alone or two feeds. To connect DC power feeds to the terminal blocks, do the following:

1. Strip the ends of the power cables.
2. Loosen the three screws in the top of the block. (These are captive screws, which you cannot completely remove.)
3. Insert the -48V DC power feed wires into the two outside receptacles of the terminal block
4. Insert the 0V DC feed wires into the center receptacle.
5. Tighten the screws over the receptacles.

CONNECTING THE NETSCREEN-100 DEVICE TO OTHER DEVICES

To connect the device, use the ethernet interfaces (**Trusted**, **DMZ**, and **Untrusted**). The purpose of each interface depends upon the security zone to which it is bound.

By default, the zone and interface bindings are as follows:

- **Trusted** is bound to the **Trust** security zone by default.

  Connect this interface using a twisted pair cable with RJ-45 connectors.
- **DMZ** is bound to the **DMZ** security zone by default.

  Connect this interface using a twisted pair cable with RJ-45 connectors.

- **Untrusted** is bound to the **Untrust** security zone by default.

  Connect this interface using a twisted pair cable with RJ-45 connectors.

The default IP address of each ethernet interface is 0.0.0.0.

For information on interfaces and security zones, see "The NetScreen-100 Interfaces" on page 13.

Configuring the Device 3

This chapter describes how to perform initial configuration on a NetScreen-100 device once you have mounted it in a rack or desktop, plugged in the necessary cables, and turned the power on.

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-100 device supports two device modes, Transparent mode and Route mode. The default mode is Transparent.

Transparent Mode

In Transparent mode, the NetScreen-100 device operates as a Layer-2 bridge. Because the device cannot translate packet IP addresses, it cannot perform Network Address Translation (NAT). Consequently, for the device to access the Internet, any IP address in your trusted (local) networks must be routable and accessible from untrusted (external) networks.

In Transparent mode, the IP addresses for the Layer-2 security zones V1-Trust, V1-DMZ, and V1-Untrust 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-100 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.
- When the interface does *not* perform NAT services, the source IP address and port number in each packet header remain unchanged. Therefore, to reach the Internet your local hosts must have routable IP addresses.

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-100 INTERFACES

Each NetScreen-100 device provides ethernet interfaces for access and connectivity. In addition, there are logical (non-physical) interfaces that perform special Layer-2 or management functions.

Status and Power LEDS Console Port Ethernet Interfaces **Trusted**, **DMZ**, **Untrusted**

The configurable interfaces available on a NetScreen-100 device are as follows:

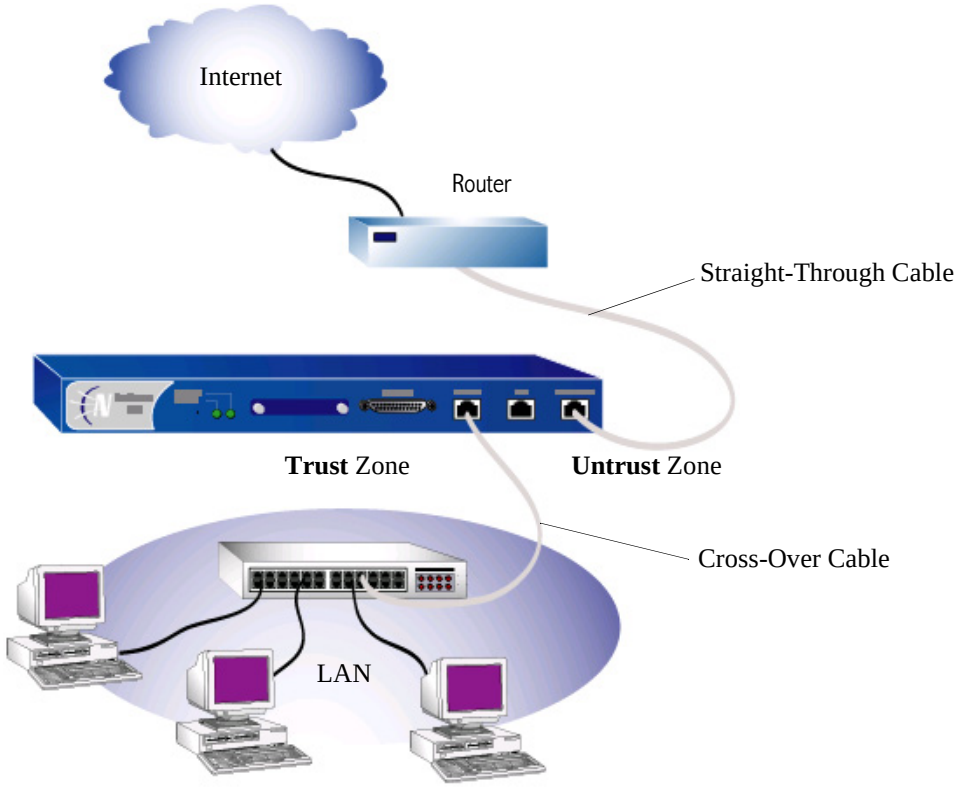
Interface Type	Description
Ethernet interfaces	• **Trusted** Bound to the **V1-Trust** security zone by default. Connect this interface using a twisted pair cable with RJ-45 connectors.
	• **DMZ** Bound to the **V1-DMZ** security zone by default. Connect this interface using a twisted pair cable with RJ-45 connectors.
	• **Untrusted** Bound to the **V1-Untrust** security zone by default. Connect this interface using a twisted pair cable with RJ-45 connectors.
Layer-2 interfaces	**vlan1** specifies logical interface used for management and for VPN traffic termination while the NetScreen device is in Transparent mode.
	v1-trust specifies a logical Layer-2 interface bound to the V1-Trust zone.
	v1-untrust specifies a logical Layer-2 interface bound to the V1-Untrust zone.
	v1-dmz specifies a logical Layer-2 interface bound to the V1-DMZ zone.
Tunnel interfaces	**tunnel.***n* specifies a logical tunnel interface. This interface is for VPN traffic.

CONNECTING THE DEVICE AS A SINGLE SECURITY GATEWAY

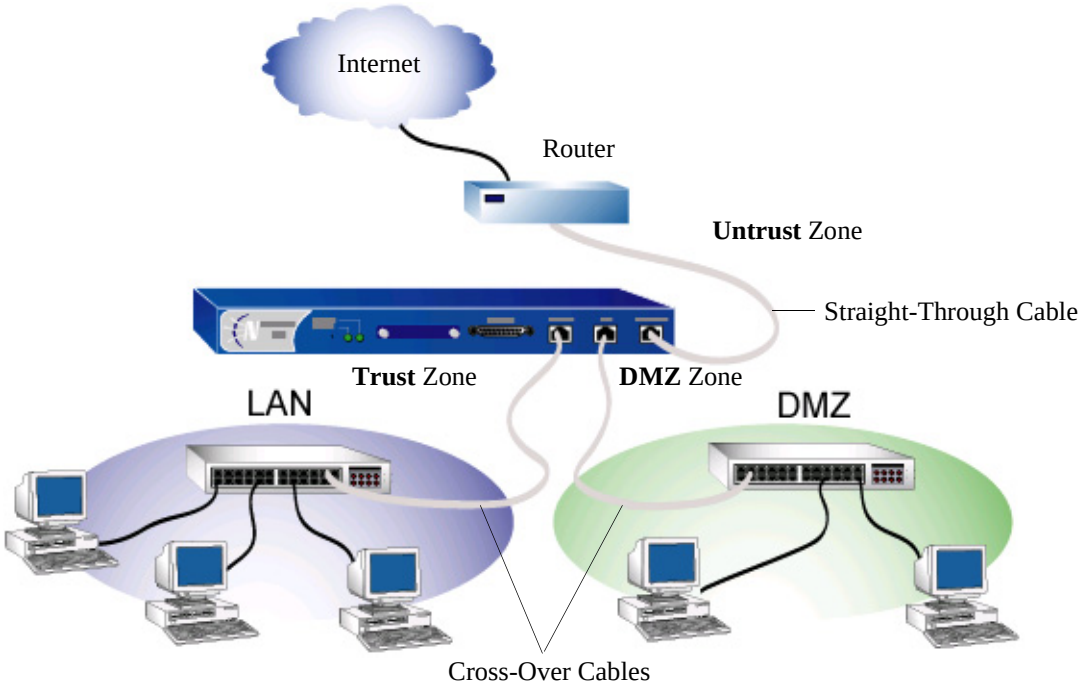
There are many ways to connect a NetScreen-100 device to your network system. In most cases, the device serves as a single security gateway that protects a LAN (usually connected to the device from a switch or a hub).

Connectivity Examples

In the following example, a NetScreen-100 device connects to the protected LAN through the **Trusted** interface (bound to the Trust security zone). The device connects externally to a router through the **Untrusted** interface (bound to the Untrust security zone).



In the following example, a NetScreen-100 device connects to a protected LAN through the **Trusted** ethernet interface (bound to the Trust security zone) and to a protected DMZ through the **DMZ** ethernet interface (bound to the DMZ security zone). The device connects externally to a router through the **Untrusted** ethernet interface (bound to the Untrust security zone).



Performing Device Connection

Note: *If you have multiple NetScreen-100 devices, install and configure them one at a time. Because they all share the same default* ***vlan1*** *IP address and subnet mask (192.168.1.1/24), you might encounter IP address conflicts.*

To set up the NetScreen-100 network connections:

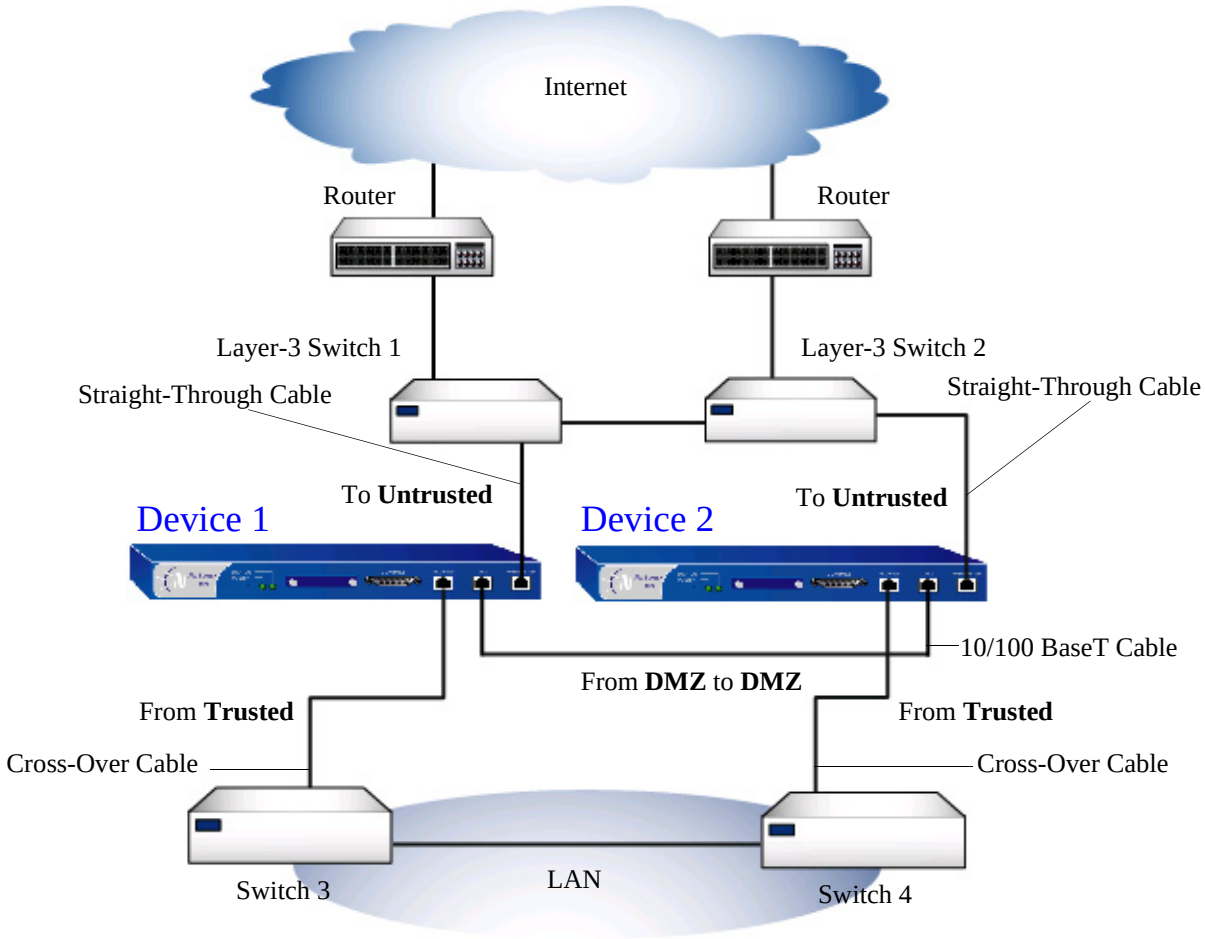
1. Place the NetScreen-100 device in a rack (see "Rack-Mounting the Device" on page 11) or on a desktop.
2. Confirm that the power connection to the device is turned OFF ("**0**" pressed in).
3. Connect the provided power cable from the power outlet to the power supply.
4. Connect the device to the network (see examples above).
5. Turn the NetScreen-100 device power switch ON, then turn the other network device power switches ON. (If all cables are connected correctly, the link light for each connection glows.)

ESTABLISHING AN HA CONNECTION BETWEEN DEVICES

To assure continuous traffic flow in the event of system failure, you can cable and configure two NetScreen devices in a redundant cluster. The devices propagate all network, configuration and session information to each other. Should one device fail, the other takes over the traffic processing.

Note: *For the NetScreen-100, the HA interface is usually* ***DMZ****.*

The following diagram shows a typical HA setup for NetScreen-100 devices.



To cable two NetScreen-100 devices together for HA and connect them to the network:

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.*

1. (Optional) Install the NetScreen-100 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-100 power supply and connect them to a power source.

   Note: *Whenever you deploy two NetScreen-100 devices in an HA cluster, connect each 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 cable from the **DMZ** port on Device 1 to the **DMZ** port on Device 2.

Device 1

5. On Device 1, connect a crossover cable from the **Trusted** port to the switch labeled "Switch 3."
6. On Device 1, connect a straight-through cable from the **Untrusted** port to the switch labeled "Layer 3 switch 1."

Device 2

7. On Device 2, connect a crossover cable from the **Trusted** port to the switch labeled "Switch 4."
8. On Device 2, connect a straight-through cable from the **Untrusted** port to the switch labeled "Layer 3 switch 2."

Switches

9. Cable together the switches labeled "Switch 3" and "Switch 4."
10. Cable together the switches labeled "Layer 3 switch 1" and "Layer 3 switch 2."
11. Cable the switches labeled "Layer 3 switch 1" and "Layer 3 switch 2" to routers.

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

12. Turn the power switches for all devices ON.

For more advanced HA configurations, see the *NetScreen Concepts and Examples ScreenOS Reference Guide*.

PERFORMING INITIAL CONNECTION AND CONFIGURATION

To establish the first console session with the NetScreen-100 device, use a vt100 terminal emulation program through the provided DB9/DB25 serial cable.

Establishing a Terminal Emulator Connection

To establish an initial console session:

1. Plug the DB9 end of the supplied DB9/DB25 serial cable into the serial port of your PC. (Be sure that the DB9 is seated properly and secured with thumbscrews.)
2. Plug the DB25 end of the cable into the Console port of the NetScreen-100 device. (Be sure that the DB25 is seated properly and secured with thumbscrews.)
3. Launch a Command Line Interface (CLI) session between your PC and the NetScreen-100 device using a standard serial terminal emulation program such as Hilgreave 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.

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

To make an interface work as the management interface, you must set the IP address and subnet mask to the same address range as your PC (or LAN).

To configure the **Trusted** interface to serve as a management interface:

1. Determine the IP address and subnet mask for your PC (or LAN).
2. Assign the IP address and subnet mask to the **Trusted** interface by executing the following command:

   ```
   set interface trust 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 **Trusted** ethernet interface to 10.100.2.183/16:

   ```
   set interface trust ip 10.100.2.183/16
   ```

3. Enable management on the **ethernet1** interface by executing the following command:

   ```
   set interface trust manage
   ```

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

   ```
   get interface trust
   ```

Setting the IP Address for the Untrust Zone Interface

The NetScreen-100 device usually communicates with external devices through an interface bound to the Untrust zone (such as the **Untrusted** interface). To allow an interface to communicate with external devices, you must assign it a public IP address.

To set the IP address and subnet mask for the **Untrusted** interface:

1. Choose an unused public IP address and subnet mask.
2. Set the **Untrusted** interface to this IP address and subnet mask by executing the following command:

   set interface untrust 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 **Untrusted** interface to 172.16.16.183:

   set interface untrust ip 172.16.2.183/16

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

   get interface untrust

Allowing Outbound Traffic

By default, the NetScreen-100 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.

You can also use the Outgoing Policy Wizard in the WebUI management application to create access policies for outbound traffic. See "Establishing a GUI Management Session" on page 22 for information on accessing the WebUI application.

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* *"Resetting the Device to Factory Default Settings" on page 23*.

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-100 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-100 device:

1. Connect an RJ-45 cable from the **Trusted** interface to the internal switch, router, or hub in your LAN (see "Connecting the Device as a Single Security Gateway" on page 13).
2. Open a Telnet session, specifying the current IP address for the **Trusted** interface. For example, in Windows, click **Start >> Run**, enter **telnet** *ip_addr* (where *ip_addr* is the address of the **Trusted** interface), and then click **OK.**

   For example, if the current IP address of the **Trusted** interface is 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.

Establishing a GUI Management Session

To access the NetScreen-100 device with the WebUI management application:

1. To use the Trusted interface as the management interface, you must set the IP address and subnet mask to the same address range as your PC (or LAN). See "Setting Port and Interface IP Addresses" on page 19.
2. Launch your browser, enter the IP address of the Trusted interface in the URL field, and then press Enter.

   For example, if you assigned the Trusted interface 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.

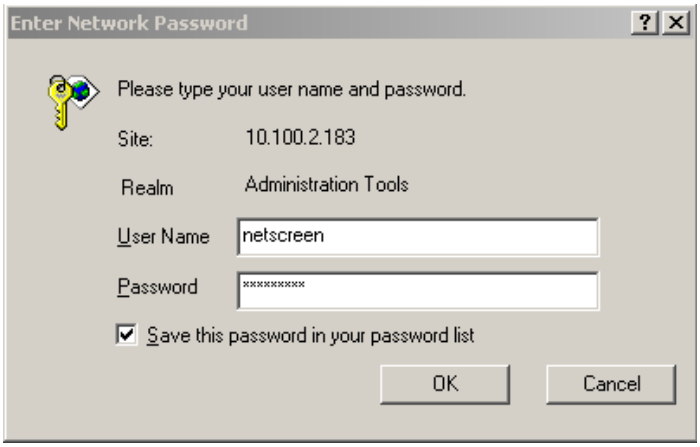


Figure 3-1 Enter Network Password Dialog Box

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.

RESETTING THE DEVICE TO FACTORY DEFAULT SETTINGS

If you lose the admin password, you can use one of the following procedures to reset the NetScreen device to its default settings. This destroys any existing configurations, but restores access to the device.

Warning! *Resetting the device will delete all existing configuration settings, and the firewall and VPN service will be rendered inoperative.*

Note: *After you successfully reset and reconfigure the NetScreen device, you should back up the new configuration setting. As a precaution against lost passwords, you should back up a new configuration that contains the NetScreen default password. This will ensure a quick recovery of a lost configuration. You should change the password on the system as soon as possible.*

Using CLI Commands to Reset the Device

To perform this operation, you need to make a console connection, as described in "Establishing a Terminal Emulator Connection" on page 18.

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.

Using the Asset Recovery Pinhole to Reset the Device

You can also reset the device and restore the factory default settings by pressing the asset recovery pinhole. To perform this operation, you need to make a console connection, as described in "Establishing a Terminal Emulator Connection" on page 18.

1. Locate the asset recovery pinhole on the front panel (see "The Front Panel" on page 2). Using a thin, firm wire (such as a paper clip), push the pinhole for four to six seconds and then release.

   A serial console message states that the "Configuration Erasure Process has been initiated" and the system sends an SNMP/SYSLOG alert. The Status LED blinks amber once every second.

2. Wait for one-half to two seconds.

   After the first reset is accepted, the power LED blinks green; the device is now waiting for the second push. The serial console message now reads, "Waiting for 2nd confirmation."

3. Push the reset pinhole again for four to six seconds.

   The Status LED lights amber for one-half second, and then returns to the blinking green state.

4. The device resets to its original factory settings.

   When the device resets, the Status LED will turn amber for one-half second and then return to the blinking green state. The serial console message states "Configuration Erase sequence accepted, unit reset." The system generates SNMP and SYSLOG alerts to configured SYSLOG or SNMP trap hosts.

   Note: *During a reset, there is no guarantee that the final SNMP alert sent to the receiver before the reset will be received.*

5. The device now reboots.

If you do not follow the complete sequence, the reset process cancels without any configuration change and the serial console message states, "Configuration Erasure Process aborted." The status LED returns to blinking green. If the unit did not reset, an SNMP alert is sent to confirm the failure.

Specifications

This appendix provides general system specifications for the NetScreen-100 device.

NetScreen-100 Attributes

Height: 1.75 inches

Depth: 10.8 inches

Width: 17.5 inches

Weight: 8 pounds

Electrical Specification

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

DC voltage: -36 to -72 VDC

AC Watts: 45 Watts

DC Watts: 50 Watts

Environmental

Temperature	Operating
Normal altitude	32 - 105° F, 0 - 40° C
Relative humidity	10-90%
Non-condensing	10-90%

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

FIPS Certification

FIPS 140-1 Level 1

Safety Certifications

UL, CUL, CSA

EMI Certifications

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

Index

R

V