NETSCREEN-5XP

User's Guide

Version 5.0 P/N 093-0969-000 Rev. B

Copyright Notice

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 device 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

Table of Contents

Preface

The NetScreen-5XP device provides IPSec VPN and firewall services for a broadband telecommuter, a branch office, or a retail outlet. While at the entry level of the NetScreen appliance product line, the NetScreen-5XP device uses the same firewall, VPN, and traffic management technology as Juniper's high-end central site products.

Juniper offers two versions of the NetScreen-5XP device:

- The 10-user version supports up to 10 users
- The Elite version supports an unrestricted number of users

GUIDE ORGANIZATION

This manual has three chapters and two appendices.

Chapter 1, "Overview" provides an overview of the NetScreen-5XP device, ports, and power requirements.

Chapter 2, "Installing the Device" details how to install the NetScreen-5XP device on a desktop, connect the power, and connect the device to your network.

Chapter 3, "Configuring the Device" details how to establish a Console session, set an IP address for managing the NetScreen-5XP device, and access the device using the WebUI.

Appendix A, "Specifications" provides a list of physical specifications about the NetScreen-5XP device.

COMMAND LINE INTERFACE (CLI) CONVENTIONS

The following conventions are used when presenting the syntax of a command line interface (CLI) command:

- Anything inside square brackets [ ] is optional.
- Anything inside braces { } is required.
- If there is more than one choice, each choice is separated by a pipe (|). For example,

  ```
  set interface { ethernet1 | ethernet2 | ethernet3 }
  manage
  ```

  means "set the management options for the ethernet1, ethernet2, or ethernet3 interface".

- Variables appear in *italic*. For example:

  set admin user *name1* **password** *xyz*

When a CLI command appears within the context of a sentence, it is in **bold** (except for variables, which are always in *italic*). For example: "Use the **get system** command to display the serial number of a NetScreen device."

Note: *When typing a keyword, you only have to type enough letters to identify the word uniquely. For example, typing* ***set adm u joe j12fmt54*** *is enough to enter the command* ***set admin user joe j12fmt54****. Although you can use this shortcut when entering commands, all the commands documented here are presented in their entirety.*

JUNIPER PUBLICATIONS

To obtain technical documentation for any Juniper Networks NetScreen product, visit www.juniper.net/techpubs/.

For technical support, open a support case using the Case Manager link at http://www.juniper.net/support/ or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (outside the United States).

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

techpubs-comments@juniper.net

1

Overview

This chapter provides detailed descriptions of the NetScreen-5XP chassis.

Topics explained 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.*

Port and Power Connectors

The rear panel of the NetScreen-5XP device contains port and power connectors.

The NetScreen-5XP device includes the following ports:

- A Console port, for connecting to serial terminal emulation programs such as HyperTerminal.
- A Trusted interface, for connecting the device to an internal switch or hub or directly to your computer.
- An Untrusted interface, for connecting the device to your external router, DSL modem, or cable modem.

The following table describes the ports on the device:

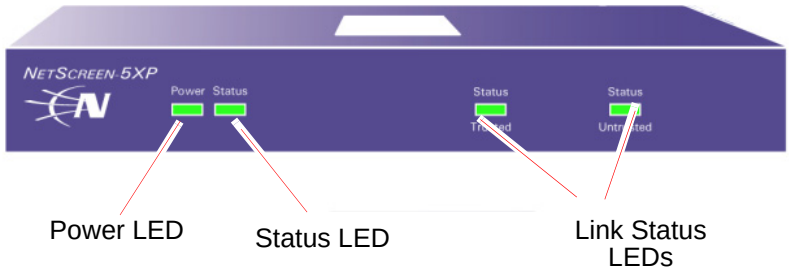
Port	Description	Connector Type	Speed/Protocol
Console	Enables a serial connection to establish terminal sessions with the system. Used for launching Command Line Interface (CLI) sessions.	DB-9	9600 bps RS-232
Trusted	Enables a direct connection to your workstation or a LAN connection through a switch or hub. This connection also allows you to manage the device through a Telnet session or the WebUI management application.	RJ-45	10 Mbps Ethernet
Untrusted	Enables an Internet connection through an external router, DSL modem, or cable modem.	RJ-45	10 Mbps/ Ethernet

The NetScreen-5XP device runs at 5V DC and maximum power consumption is 5 watts. When properly connected to an AC power source, the power LED on the front panel glows solid green. When power fails, the power LED turns off.

Important: *We recommend using a surge protector for the power connection.*

STATUS LEDS

The front panel of the NetScreen-5XP device has power and status LEDs for the device, and link status LEDs for the Trusted and Untrusted interfaces.



Interpreting Status LEDs for the Device

The device status LEDs indicate whether the device is operating properly. The following table describes the status possibilities for each.

LED	LED Color	Meaning of the LED
POWER	**green**	Indicates the system is receiving power.
	off	Indicates the system is not receiving power.
STATUS	**amber**	Indicates the module is starting up.
	blinking green	Indicates the module is functioning.
	blinking red	Indicates a diagnostics or system initialization error.
	Off	Indicates the module is not operational.

Interpreting Link Status LEDs

The link status LEDs indicate whether the ports on the modules are operating properly. The following table describes the status possibilities for the Trusted and Untrusted ports.

LED	LED Color	Meaning of the LED
Trusted or Untrusted	**blinking green**	Indicates the device detects Ethernet traffic for the port.
	off	Indicates the port has not established a link with another device.
	green	Indicates the port has established a link with another device.

2

Installing the Device

This chapter describes how to install a NetScreen-5XP device on a desktop, connect the power, and connect the device to your network.

Topics explained in this chapter include:

DESKTOP INSTALLATION GUIDELINES

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

- Never assume that the power cord 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 device in a secure environment.*

CONNECTING THE POWER

To connect the power to the NetScreen-5XP device:

1. Plug the DC connector end of the power cable into the DC power receptacle on the back of the system.
2. Plug the AC adapter end of the power cable into an AC power source.

Important: *We recommend using a surge protector for the power connection.*

CONNECTING THE NETSCREEN-5XP DEVICE TO YOUR NETWORK

The following sections describe how to connect your NetScreen-5XP system to your network.

Connecting the Device to an External Router or Modem

You can establish a high-speed connection to an external router, DSL modem, or cable modem, and provide firewall and general security for your network. Connect the white, straight-through cable from the Untrusted interface on the NetScreen-5XP device to the external router or modem.

Connecting the Device to Your Internal Network, Workstation, or Devices

You can connect the NetScreen-5XP device to a LAN (via an internal switch or hub) or directly to your workstation. There are two ways to create this connection:

- If you have a LAN, connect the colored cross-over cable from the Trusted interface on the NetScreen-5XP device to the internal switch or hub.
- If you are connecting to a single workstation, get another straight-through cable and connect it from the Trusted interface on the NetScreen-5XP device directly to the Ethernet port on the workstation.

3

Configuring the Device

This chapter describes how to configure a NetScreen-5XP device after you have installed it on a desktop, connected it to a power source, and plugged in the necessary cables. Topics explained in this chapter are:

Note: *You must register your product at www.juniper.net/support/ so that certain ScreenOS services, such as the Deep Inspection Signature Service, can be activated on the device. After registering your product, use the WebUI or CLI to obtain the subscription for the service. For more information about registering your product and obtaining subscriptions for specific services, see the "System Parameters" chapter in Volume 2 of the* NetScreen Concepts & Examples ScreenOS Reference Guide.

Note: *If you access the device for the first time using the ScreenOS WebUI graphical interface, the Initial Configuration Wizard appears when you log in to the WebUI. This Wizard guides you through the configuration described in this chapter. For more information about starting the Initial Configuration Wizard, refer to the* Getting Started Guide *for the NetScreen-5XP.*

OPERATIONAL MODES

The NetScreen-5XP device supports two operational modes, Transparent mode and Route mode. The default mode is Route.

Transparent Mode

In Transparent mode, the NetScreen-5XP 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 address for the Layer-2 security zone is 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-5XP 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 & 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 & Examples ScreenOS Reference Guide.

THE NETSCREEN-5XP INTERFACES

Each NetScreen-5XP device provides Ethernet interfaces for access and connectivity. In addition, there are logical (non-physical) interfaces that perform special Layer-2 or management functions.

The configurable interfaces available on a NetScreen-5XP device are as follows:

Interface Type	Description
Ethernet interfaces	These interfaces are denoted by a physical port on the module although each interface is bound to a security zone by default.
	• **Trusted** Bound to the **Trust** zone by default. Connect this interface using a twisted pair cable with RJ-45 connectors.
	• **Untrusted** Bound to the **Untrust** zone by default. Connect this interface using a twisted pair cable with RJ-45 connectors.
Layer-2 interfaces	**vlan1** specifies a logical interface used for management and for VPN traffic termination while the NetScreen device is in Transparent mode.
Tunnel interfaces	**untrust-tun** specifies a logical tunnel interface. This interface is for VPN traffic.

Establishing a Console Session

The NetScreen-5XP device has a serial port (called the *Console port*) that enables you to establish a console session with ScreenOS, the device operating system.

Important: *For the console connection, you will need to obtain a serial cable with a male DB-9 connector on one end and female DB-9 connector on the other end.*

To establish a console session:

1. Plug the female DB-9 end of the serial cable into the serial port of your computer. (Be sure that the DB-9 clip is seated properly in the port.)
2. Plug the male DB-9 end of the serial cable into the Console port of the NetScreen-5XP device. (Be sure that the DB-9 is seated properly in the port.)
3. Launch a serial terminal program. (A commonly-used terminal program is Hilgraeve HyperTerminal.) Typical settings to launch a console session with your NetScreen-5XP device are as follows:
   - Baud Rate to **9600**
   - Parity to **No**
   - Data Bits to **8**
   - Stop Bit to **1**
   - Flow Control to **none**
4. At the login prompt, type **netscreen**.
5. At the password prompt, type **netscreen**.

Note: *Both login and password are case-sensitive.*

Changing Your Admin Name and Password

Because all NetScreen products use the same admin name and password (**netscreen**), it is highly advisable to change your admin 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 & Examples ScreenOS Reference Guide.*

Setting an IP Address for Managing the Device

The default IP address of the Trusted interface on the NetScreen-5XP device is 192.168.1.1. This is the IP address that you use to manage the device through a Telnet session or with the WebUI management application. If you do not wish to use this default IP address, you need to assign a new one.

To set the IP address of the NetScreen-5XP Trusted interface:

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

   `set interface trust ip` *`ip_addr/mask`*

   For example, to set the IP address and subnet mask of the NetScreen-5XP device to 10.100.2.183 and 16, respectively:

   `set interface trust ip 10.100.2.183/16`

3. To confirm the new setting, execute the following command:

   `get interface`

   You should see that the IP address for the Trusted interface is the IP address you set.

Accessing the Device Using the WebUI

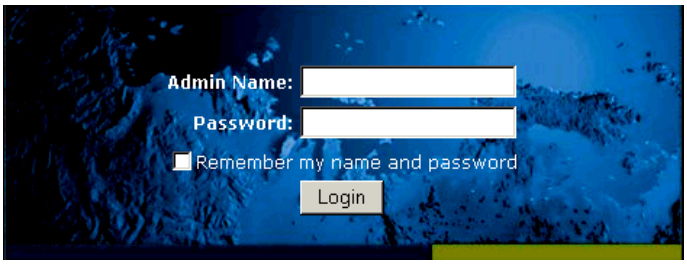
To access the NetScreen-5XP device with the WebUI management application:

1. Connect your computer (or your LAN hub) to the Trusted interface, as described in "Connecting the Device to Your Internal Network, Workstation, or Devices" on page 7.
2. Launch your browser, enter the IP address for the Trusted interface in the URL field, and then press Enter.

   For example, if you assigned the Trusted interface of the device the IP address of 10.100.2.183/16, enter the following:

   `10.100.2.183`

   The NetScreen WebUI software displays the login prompt.



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

   The NetScreen WebUI application window appears.

   Note: *NetScreen-Security Manager 2004 and NetScreen Rapid Deployment: If you are using NSM, you can optionally configure Juniper appliances with Rapid Deployment. Refer to the* Rapid Deployment Getting Started Guide *for more information.*

USING THE WEBUI WIZARDS TO CONFIGURE THE DEVICE

The WebUI contains wizards you can run to configure the NetScreen-5XP:

- The **Initial Configuration** wizard allows you to set the operational mode, and depending upon which mode you select, configure basic configuration and management options. When you use the WebUI to access the device for the first time, the Initial Configuration wizard appears.
- The **Outgoing Policy** wizard allows you to configure rules that tell your NetScreen device what kind of services users on your network (the **Trust** zone) are allowed to access on outside computers (the **Untrust** zone).
- The **Incoming Policy** wizard allows you to configure rules that tell your NetScreen device the services and computers that users on outside computers (the **Untrust** zone) are allowed to access on your network (the **Trust** zone).
- The **VPN** wizard allows you to create and configure a Virtual Private Network.

In the WebUI, select the appropriate option under **Wizards**.

ASSET RECOVERY

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 Console Session" on page 12.

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 and settings. Would you like to continue? y/[n]
3. Press the **y** key.

   The following message appears:

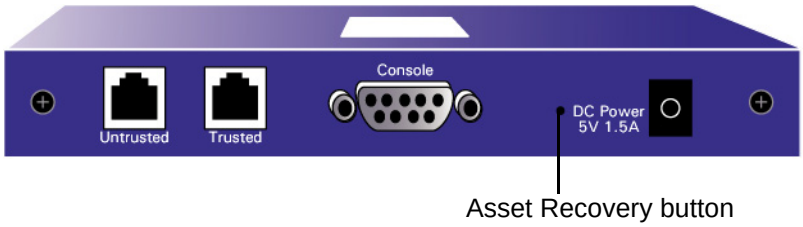
   !! Reconfirm Lost Password Reset !! If you continue, the entire configuration of the device will be erased. In addition, a permanent counter will be incremented to signify that this device has been reset. This is your last chance to cancel this command. If you proceed, the device will return to factory 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 reset the device.

   You can now login in using *netscreen* as the default admin name 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 button. To perform this operation, you need to make a console connection, as described in "Establishing a Console Session" on page 12.

1. Locate the asset recovery pinhole on the front panel. Using a thin, firm wire (such as a paper clip), push the button located behind the asset recovery pinhole for four to six seconds.



   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.

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

2. Release the button for one second.
3. Push the button again for four to six seconds. A serial console message states "Second push has been confirmed."

   The Status LED lights amber for one-half second, then returns to the blinking green state. Continue to press the button until the message "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.*

4. Release the button.
5. The device now erases the configuration and restarts.

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

A

This appendix provides general system specifications for the NetScreen-5XP device.

NetScreen-5XP Attributes

Height: 1.25 inches (3.18 cm)

Depth: 5 inches (13 cm)

Width: 6 inches (15 cm)

Weight: 1 pound (.5 kg)

Electrical Specification

AC voltage: 100-240 VAC +/- 10% 50/60 Hz

DC Watts: 7.5 Watts

DC voltage: 5 Volts

Environmental

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

The maximum normal altitude is 12,000 ft. (0-3,660 m)

Safety Certifications

UL, CUL, CSA, ICE 60950, Austel

EMI Certifications

FCC Part 15 class B, VCCI, C-Tick, BSMI, CE

Connectors

The RJ-45 twisted-pair ports are compatible with the IEEE 802.3 Type 10 Base-TX standard. The following table media type and distance for these connectors.

Standard	Media Type	Mhz/Km Rating	Maximum Distance
10Base-TX	Category 5 and higher Unshielded Twisted Pair (UTP) Cable		100 m

Index