

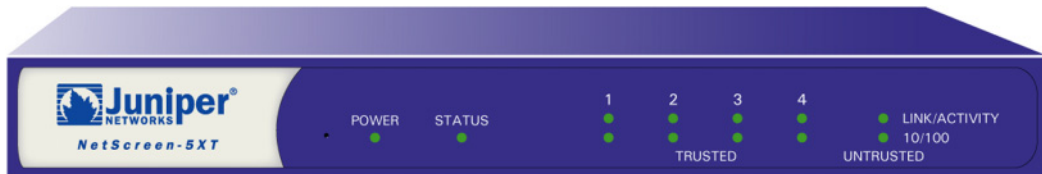
NETSCREEN-5XT

User's Guide

Version 5.0

093-1323-000

Rev. B



Copyright Notice

Copyright © 2005 Juniper Networks, Inc. All rights reserved.

Juniper Networks, the Juniper Networks logo, NetScreen, NetScreen Technologies, GigaScreen, and the NetScreen logo are registered trademarks of Juniper Networks, Inc. NetScreen-5GT, NetScreen-5XP, NetScreen-5XT, NetScreen-25, NetScreen-50, NetScreen-100, NetScreen-204, NetScreen-208, NetScreen-500, NetScreen-5200, NetScreen-5400, NetScreen-Global PRO, NetScreen-Global PRO Express, NetScreen-Remote Security Client, NetScreen-Remote VPN Client, NetScreen-IDP 10, NetScreen-IDP 100, NetScreen-IDP 500, GigaScreen ASIC, GigaScreen-II ASIC, and NetScreen ScreenOS are trademarks of Juniper Networks, 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:

Juniper Networks, Inc.
ATTN: General Counsel
1194 N. Mathilda Ave.
Sunnyvale, CA 94089-1206

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

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 JUNIPER NETWORKS REPRESENTATIVE FOR A COPY.

Contents

Preface	v
Guide Organization	v
Command Line Interface (CLI) Conventions	v
Juniper Networks NetScreen Publications	vi
Chapter 1 Overview	1
Port and Power Connectors	2
Status LEDs	3
Interpreting Status LEDs for the Device	3
Interpreting Port Status LEDs	3
Chapter 2 Installing the Device	5
Desktop Installation Guidelines	6
Connecting the Power	6
Connecting the NetScreen-5XT To Your Network	7
Connecting the Device to an External Router or Modem	7
Connecting the Device to Your Internal Network, Workstations, or Other Devices	7
Chapter 3 Configuring the Device	9
Operational Modes	10
Transparent Mode	10
Route Mode	10
The NetScreen-5XT Interfaces	11
Establishing a Console Session	12
Changing Your Admin Name and Password	12
Setting an IP Address for Managing NetScreen-5XT	13
Accessing the NetScreen-5XT Using the WebUI	13
Using the WebUI Wizards to Configure the Device	14
Asset Recovery	14
Using CLI Commands to Reset the NetScreen-5XT	15
Using the Asset Recovery Pinhole to Reset the Device	15
Appendix A Specifications	A-I
NetScreen-5XT Attributes	A-II
Electrical Specification	A-II
Environmental	A-II
Safety Certifications	A-II
EMI Certifications	A-II

Contents

Connectors	A-II
Index.....	IX-I

Preface

The Juniper Networks NetScreen-5XT 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-5XT uses the same firewall, VPN, and traffic management technology as NetScreen's high-end central site products.

Juniper Networks offers two versions of the NetScreen-5XT:

- 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 one appendix.

Chapter 1, "[Overview](#)" provides an overview of the NetScreen-5XT, ports, and power requirements.

Chapter 2, "[Installing the Device](#)" details how to install the NetScreen-5XT 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-5XT, and access it using the WebUI.

Appendix A, "[Specifications](#)" provides a list of physical specifications about the NetScreen-5XT.

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 NETWORKS NETSCREEN 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

Overview

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

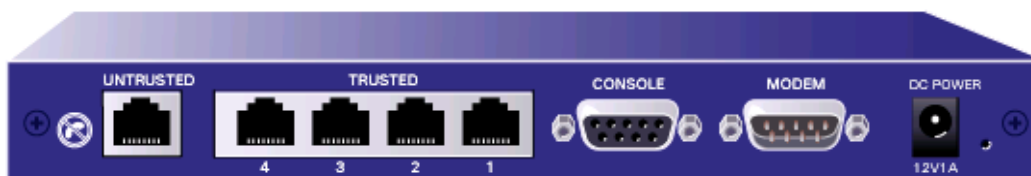
Topics explained in this chapter include:

- [“Port and Power Connectors” on page 2](#)
- [“Status LEDs” on page 3](#)

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-5XT contains port and power connectors.



The NetScreen-5XT includes the following ports:

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

The following table describes the ports on the device:

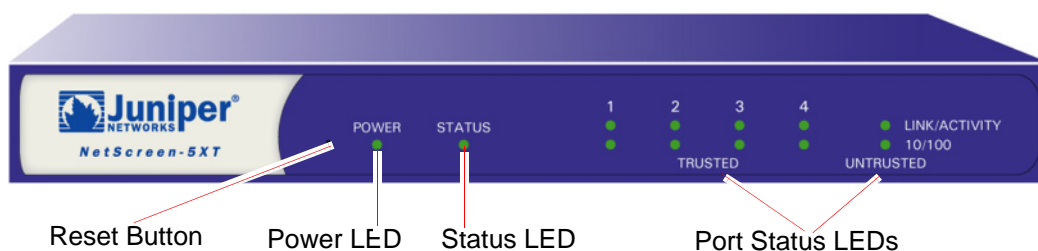
Port	Description	ConnectorType	Speed/Protocol
Console	Enables a serial connection to establish terminal sessions with the system. Used for launching Command Line Interface (CLI) sessions.	DB-9 (DTE)	9600 bps/ RS-232C
Modem	Attaches an asynchronous modem or ISDN terminal adapter for dial disaster recovery.	DB-9 (DTE)	9600 bps-115 Kbps/ RS-232C
Trusted Ports 1-4	Enables direct connections to workstations 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	10/100 Mbps/ Ethernet
Untrusted	Enables an Internet connection through an external router, DSL modem, or cable modem.	RJ-45	10/100 Mbps/ Ethernet

The NetScreen-5XT runs at 100-240 VAC +/- 10% (AC volts) and 12 watts. When properly connected to an AC power source, the power LED on the faceplate glows solid green. When power fails, the power LED turns off.

Important: Juniper Networks recommends using a surge protector for the power connection.

STATUS LEDs

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



Interpreting Status LEDs for the Device

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

LED Name	Purpose	Status	Meaning
Power	Power Status	green	Power is functioning correctly.
		off	The device is not receiving power.
Status	System Status	amber	The module is starting up.
		blinking green	Normal operation.
		blinking red	There is a diagnostics or system initialization error.
		off	The module is not operational.

Interpreting Port Status LEDs

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

LED Name	Purpose	Status	Meaning
Link/Activity	Link Status	blinking green	The device detects Ethernet traffic for the port.
		off	The port has not established a link with another device.
		green	The port has established a link with another device.
10/100	Device Connection	green	The port is connected to a 100 Base-T device.
		off	The port is connected to a 10 Base-T device.

Installing the Device

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

Topics explained in this chapter include:

- [“Desktop Installation Guidelines” on page 6](#)
- [“Connecting the Power” on page 6](#)
- [“Connecting the NetScreen-5XT To Your Network” on page 7](#)

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 NetScreen-5XT 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-5XT in a secure environment.*

CONNECTING THE POWER

To connect the power to the NetScreen-5XT:

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

Important: *Juniper Networks recommends using a surge protector for the power connection.*

CONNECTING THE NETSCREEN-5XT TO YOUR NETWORK

The following sections describe how to connect your NetScreen-5XT 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 provided Ethernet cable from the Untrusted interface on the NetScreen-5XT to the external router or modem.

Connecting the Device to Your Internal Network, Workstations, or Other Devices

The Trusted interface on the NetScreen-5XT consists of four RJ-45 connector ports. You can use one of these ports to connect the device to a LAN via an internal switch or hub. You can also connect one or all of the ports in the Trusted interface directly to workstations, eliminating the need for a hub or switch.

You can use either cross-over or straight-through cables to connect NetScreen-5XT ports to other devices. Obtain a cable for each device you are connecting to the NetScreen-5XT Trusted interface ports.

Configuring the Device

This chapter describes how to configure a NetScreen-5XT 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 include:

- “Operational Modes” on page 10
- “The NetScreen-5XT Interfaces” on page 11
- “Establishing a Console Session” on page 12
- “Changing Your Admin Name and Password” on page 12
- “Setting an IP Address for Managing NetScreen-5XT” on page 13
- “Accessing the NetScreen-5XT Using the WebUI” on page 13
- “Using the WebUI Wizards to Configure the Device” on page 14
- “Asset Recovery” on page 14

Note: You must register your product at www.juniper.net/support/ so that certain NetScreen 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 NetScreen-5XT for the first time using the NetScreen 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 Juniper Networks NetScreen-5XT Getting Started Guide.

OPERATIONAL MODES

The NetScreen-5XT supports two operational modes: Transparent mode and Route mode. The default mode is Route.

Transparent Mode

In Transparent mode, the NetScreen-5XT operates as a Layer-2 bridge. Because the NetScreen-5XT cannot translate packet IP addresses, it cannot perform Network Address Translation (NAT). Consequently, for the NetScreen-5XT 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 of the zone interfaces are 0.0.0.0, thus making the NetScreen-5XT invisible to the network. However, it can still perform firewall, VPN, and traffic management according to configured security policies.

Route Mode

In Route mode, the NetScreen-5XT 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 NetScreen-5XT 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 NetScreen-5XT in Route mode. To configure it in Transparent mode, see the *NetScreen Concepts & Examples ScreenOS Reference Guide*.

THE NETSCREEN-5XT INTERFACES

Each NetScreen-5XT 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-5XT 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.
	Trusted1 - Trusted4 Bound to the Trust security zone by default. Connect this interface using a twisted pair cable with RJ-45 connectors.
	Untrusted Bound to the Untrust security 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-5XT is in Transparent mode.
Loopback interfaces	loopback emulates a physical interface on the NetScreen-5XT. A loopback interface is always in the up state as long as the device on which it resides is up.
Tunnel interfaces	untrust-tun specifies a logical tunnel interface. This interface is for VPN traffic.

ESTABLISHING A CONSOLE SESSION

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

Note: 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 wired straight-through cable.

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-5XT. (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-5XT 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 Juniper Networks 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 NETSCREEN-5XT

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

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

1. Choose an unused IP address within the current address range of your Local Area Network.
2. Set the it's IP address 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-5XT to 10.100.2.183 and 16, respectively:

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

3. To confirm the new settings, 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 NETSCREEN-5XT USING THE WEBUI

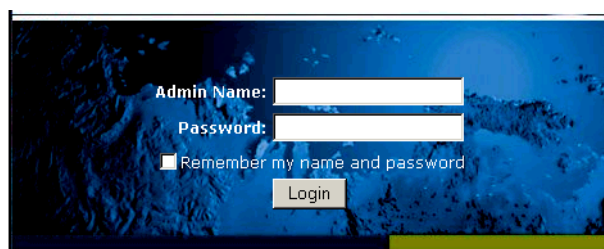
To access the NetScreen-5XT with the WebUI management application:

1. Connect your computer (or your LAN hub) to the Trusted interface, as described in [“Connecting the Device to Your Internal Network, Workstations, or Other 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 an IP address of 10.100.2.183/16, enter the following:

```
10.100.2.183
```

The Juniper Networks NetScreen WebUI software displays the login prompt.



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

The Juniper Networks NetScreen WebUI application window appears.

***Note:** NetScreen-Security Manager 2004 (NSM) and NetScreen Rapid Deployment (RD): If you are using NSM, you can optionally configure NetScreen appliances with RD. 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-5XT:

- 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-5XT 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-5XT 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-5XT to its default settings.

***Note:** After you successfully reset and reconfigure the NetScreen-5XT, you should back up the new configuration setting. As a precaution against lost passwords, you should back up a new configuration that contains the Juniper Networks NetScreen default password. This backup 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 NetScreen-5XT

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 NetScreen-5XT 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 NetScreen-5XT.
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]

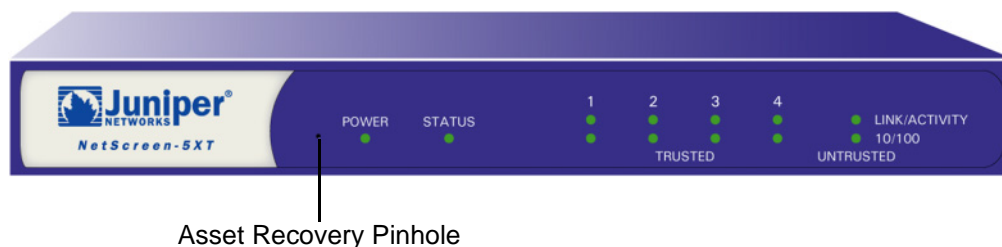
4. Press the **y** key to reset it.

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 NetScreen-5XT and restore the factory default configuration 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 reset 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 before the reset reaches the receiver.*

4. Release the button.
5. The NetScreen-5XT 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

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

- [“NetScreen-5XT Attributes” on page A-II](#)
- [“Electrical Specification” on page A-II](#)
- [“Environmental” on page A-II](#)
- [“Safety Certifications” on page A-II](#)
- [“EMI Certifications” on page A-II](#)
- [“Connectors” on page A-II](#)

NETSCREEN-5XT ATTRIBUTES

Height: 1.35 inches (3.43 cm)

Depth: 5 inches (13 cm)

Width: 8 inches (20 cm)

Weight: 1.5 pounds (6.8 hectograms)

ELECTRICAL SPECIFICATION

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

AC Watts: 12 Watts

DC voltage: 12 Volts, 1 Ampere

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, CE, CB, 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 10/100 Base-T standard. The following table media type and distance for these connectors.

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

Index

A

accessing 13
asset recovery 14

C

cables, twisted pair 11
changing login and password 12
connecting, system to a router or modem 7
connecting, system to LAN or workstation 7
connecting, system to other devices 7

G

guide organization v

I

IP address, system 13

L

LED 3
link status LED 3
login, changing 12

N

NetScreen publications vi
NetScreen-5XT

connecting to a LAN or workstation 7
connecting to a router or modem 7
connecting to other devices 7
port status LEDs 3
system status LEDs 3

P

password
 changing 12
 resetting 14
port status LEDs 3
power LED 2

R

reset 14

S

status 3
status LED 3
system IP address 13
system status LEDs 3

T

transparent mode 10

