

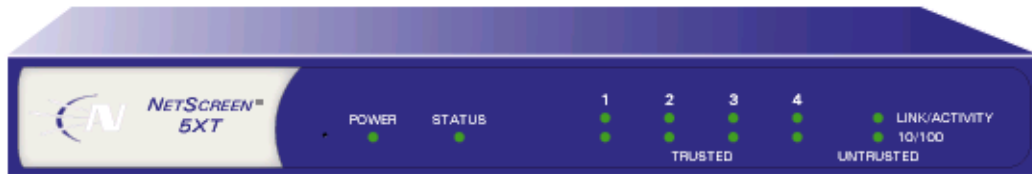
NETSCREEN-5XT

Installer's Guide

Version 4.0

P/N 093-0581-000

Rev. E



Copyright Notice

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

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without receiving written permission from

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

FCC Statement

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. The equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and

may radiate radio-frequency energy. If it is not installed in accordance with NetScreen's installation instructions, it may cause interference with Radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital devices in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Consult the dealer or an experienced radio/TV technician for help.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

Caution: Changes or modifications to this product could void the user's warranty and authority to operate this device.

Disclaimer

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

Table of Contents

Preface.....	v
Guide Organization	v
Command Line Interface (CLI) Conventions	v
CLI Command Variables	v
Variable Notation	v
Common CLI Variables	vi
CLI Command Syntax.....	vii
Dependency Delimiters	vii
Nested Dependencies	vii
Availability of CLI Commands and Features	viii
NetScreen Publications	viii
How To Get More Information	viii
Overview	1
Port and Power Connectors	2
Status LEDs	3
Interpreting Status LEDs for the Device	3
Interpreting Port Status LEDs	4
Installing the Device	5
Desktop Installation Guidelines	6
Connecting the Power	6
Connecting the NetScreen-5XT Device to Your Network	7
Connecting the Device to an External Router	7
Connecting the Device to Your Internal Network or Workstations.....	7
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 Login Name and Password	12
Setting an IP Address for Managing the Device	13

Table of Contents

Accessing the System Using the WebUI	13
Using the WebUI Wizards to Configure the Device	14
Resetting the Device to Factory Default Settings	15
Using CLI Commands to Reset the Device	15
Using the Asset Recovery Pinhole to Reset the Device	16
Specifications	A-1
NetScreen-5XT Attributes	2
Electrical Specification	2
Environmental	2
Safety Certifications	2
EMI Certifications	2
Connectors	3
Configuration for Common Criteria, EAL2	B-1
Properly Identifying the NetScreen Device for Common Criteria EAL2 Compliance	1
Proper Steps to Secure a NetScreen Device for Common Criteria EAL2 Compliance	2
Index	1-1

Preface

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

NetScreen offers two versions of the NetScreen-5XT 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-5XT device, ports, and power requirements.

Chapter 2, "[Installing the Device](#)" details how to install the NetScreen-5XT 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-5XT device.

Appendix B, "[Configuration for Common Criteria, EAL2](#)" provides information about configuring NetScreen devices for Common Criteria, EAL2 compliance.

COMMAND LINE INTERFACE (CLI) CONVENTIONS

Some of the instructions and examples provided in this manual contain CLI commands, most of which perform initial configuration of the NetScreen-5XT 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 documentation represents these parameters as variables. Such variables may include names, identification numbers, IP addresses, subnet masks, numbers, dates, and other values.

Variable Notation

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

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

where

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

Thus, the command might take the following form:

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

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

Common CLI Variable Names

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

<i>comm_name</i>	The community name of a host or other device.
<i>date_str</i>	A date value.
<i>dev_name</i>	A device name, as with flash card memory.
<i>dom_name</i>	A domain name, such as “acme” in www.acme.com .
<i>dst_addr</i>	A destination address, as with a policy definition that defines a source and destination IP address.
<i>filename</i>	The name of a file.
<i>grp_name</i>	The name of a group, such as an address group or service group.
<i>interface</i>	A physical or logical interface.
<i>id_num</i>	An identification number.
<i>ip_addr</i>	An IP address.
<i>key_str</i>	A key, such as a session key, a private key, or a public key.
<i>key_hex</i>	A key expressed as a hexadecimal number.
<i>loc_str</i>	A location of a file or other resource.
<i>mac_addr</i>	A MAC address.

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

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

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

CLI Command Syntax

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

Dependency Delimiters

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

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

Nested Dependencies

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

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

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

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

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

The { and } brackets indicate that specifying 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



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

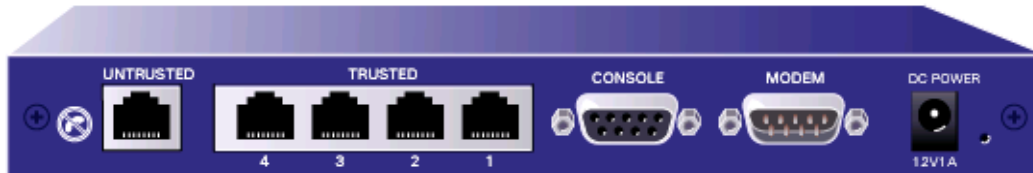
Topics explained in this chapter include:

- [“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-5XP device contains port and power connectors.



The NetScreen-5XT device 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, for connecting the device to your external router, DSL modem, or cable modem.

The following table describes the ports on the device:

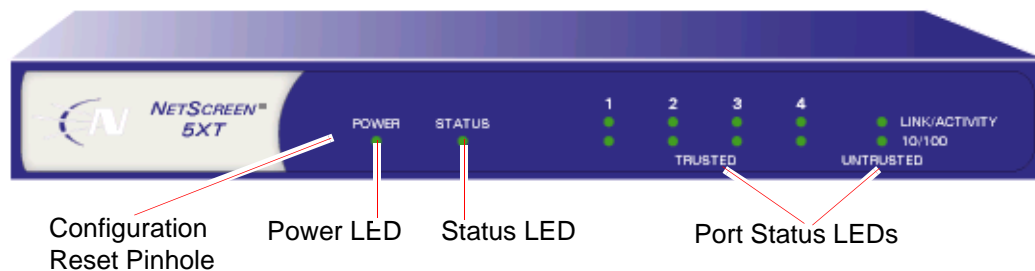
Port	Description	Connector Type	Speed/Protocol
Console	Enables a serial connection, to establish terminal sessions with the system. Used for launching Command Line Interface (CLI) sessions.	DB-9	9600 bps/ RS-232
Modem	Reserved for future use.	DB-9	9600 bps-115 Kbps/ RS-232
Trusted Ports 1-4	Enables direct 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 device 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! NetScreen recommends using a surge protector for the power connection.

STATUS LEDs

The front panel of the NetScreen-5XT device 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 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	Solid On indicates the system is receiving power
	Off	Off indicates the system is not receiving power.
STATUS	Amber	Solid On indicates the module is starting up.
	Green	Blinking On indicates the module is functioning.
	Red	Blinking On indicates a diagnostics or system initialization error.
	Off	Off indicates 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	LED Color	Meaning of the LED
Link/ Activity	Green	Blinking On indicates the device detects Ethernet traffic for the port.
		Off indicates the port has not established a link with another device.
		Solid On indicates the port has established a link with another device.
10/100	Green	Solid On indicates the port is connected to a 100 Base-T device. Off indicates the port is connected to a 10 Base-T device.

Installing the Device

2

This chapter describes how to install a NetScreen-5XT device on a desktop, connect the power, and connect the device 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 Device 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 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 secure environment.*

CONNECTING THE POWER

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

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! *NetScreen recommends using a surge protector for the power connection.*

CONNECTING THE NETSCREEN-5XT DEVICE TO YOUR NETWORK

The following sections describe how to connect your NetScreen-5XT device to your network.

- [“Connecting the Device to an External Router” on page 7](#)
- [“Connecting the Device to Your Internal Network or Workstations” on page 7](#)

Connecting the Device to an External Router

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 device to the external router or modem.

Connecting the Device to Your Internal Network or Workstations

The Trusted interface on the NetScreen-5XT device 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

3

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

- [“Operational Modes” on page 10](#)
- [“The NetScreen-5XT Interfaces” on page 11](#)
- [“Establishing a Console Session” on page 12](#)
- [“Changing Your Login Name and Password” on page 12](#)
- [“Setting an IP Address for Managing the Device” on page 13](#)
- [“Accessing the System Using the WebUI” on page 13](#)
- [“Using the WebUI Wizards to Configure the Device” on page 14](#)
- [“Resetting the Device to Factory Default Settings” on page 15](#)

OPERATIONAL MODES

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

Transparent Mode

In Transparent mode, the NetScreen-5XT 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 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-5XT 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-5XT INTERFACES

Each NetScreen-5XT 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-5XT 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, you can bind it to another zone as required.
	<ul style="list-style-type: none"> • Trusted1 - Trusted4 Bound to the Trust security zone by default. Connect this interface using a twisted pair cable with RJ-45 connectors.
	<ul style="list-style-type: none"> • 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 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.
Tunnel interfaces	untrust-tun specifies a logical tunnel interface. This interface is for VPN traffic.

ESTABLISHING A CONSOLE SESSION

The NetScreen-5XT 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 PC. (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 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 Hilgreave HyperTerminal.) Typical settings to launch a console session with your NetScreen-5XT 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 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 AN IP ADDRESS FOR MANAGING THE DEVICE

The default IP address of the Trusted interface on the NetScreen-5XT 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-5XT Trusted interface:

1. Choose an unused IP address within the current address range of your Local Area Network.
2. Set the device'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 device to 10.100.2.183 and 255.255.0.0, 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 SYSTEM USING THE WEBUI

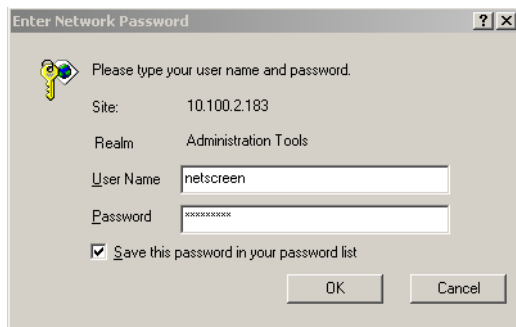
To access the NetScreen-5XT device with the WebUI management application:

1. Connect your PC (or your LAN hub) to the Trusted interface, as described in [“Connecting the Device to Your Internal Network or Workstations” 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 NetScreen WebUI software displays the Enter Network Password prompt.



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.

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 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**.

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 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, 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]

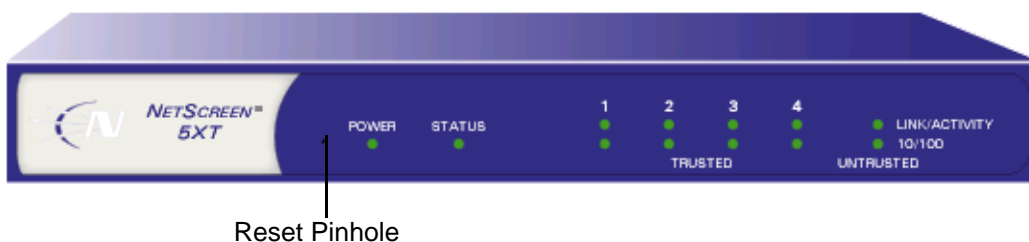
4. Press the **y** key to reset the device.

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 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 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

A

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

- [“NetScreen-5XT Attributes” on page 2](#)
- [“Electrical Specification” on page 2](#)
- [“Environmental” on page 2](#)
- [“Safety Certifications” on page 2](#)
- [“EMI Certifications” on page 2](#)
- [“Connectors” on page 3](#)

NETSCREEN-5XT ATTRIBUTES

Height: 1.35 inches

Depth: 5 inches

Width: 8 inches

Weight: 1.5 pounds

ELECTRICAL SPECIFICATION

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

AC Watts: 12 Watts

DC voltage: 12 Volts

ENVIRONMENTAL

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

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

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 meters

Configuration for Common Criteria, EAL2

B

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

PROPERLY IDENTIFYING THE NETSCREEN DEVICE FOR COMMON CRITERIA EAL2 COMPLIANCE

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

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

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

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

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

```
get system
```

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

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

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

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

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

```
set syslog config ip_address security_facility
local_facility
```

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

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

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

```
emergency
alert
critical
error
warning
notification
information
```

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

```
set log audit-loss-mitigation
```

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

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

```
unset policy id 0
```

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

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

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

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

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

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

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

```
set zone name screen all
```

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

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

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

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

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

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

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

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

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

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

```
unset interface interface manage
```

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

```
NetScreen-5XP: unset interface trust manage
NetScreen-5XT: unset interface trust manage
NetScreen-25: unset interface ethernet1 manage
NetScreen-50: unset interface ethernet1 manage
NetScreen-100: unset interface trust manage
NetScreen-204: unset interface ethernet1 manage
NetScreen-208: unset interface ethernet1 manage
NetScreen-500: unset interface ethernet3/2 manage
NetScreen-5200: unset interface ethernet2/2 manage
```

- There are two important steps to take every time a policy is being created. First, all security policies that are created must have counting and logging enabled to ensure that all audit log information is maintained for traffic passing through the device. Second, policies must be as specific as possible to ensure that the traffic being permitted is done intentionally, and not as part of a generic policy.

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

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

The following is an example of a valid policy:

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

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

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

STARTING, STOPPING, AND REVIEWING AUDIT LOGS

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

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

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

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

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

The event log shows the following events:

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

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

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

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

where *name* is the person making the change.

Index

A

Accessing 13
asset recovery 15

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 status 3
link status LED 3
login, changing 12

N

NetScreen Publications viii
NetScreen-5XT, connecting to a LAN or workstation 7
NetScreen-5XT, connecting to a router or modem 7
NetScreen-5XT, connecting to other devices 7
NetScreen-5XT, port status LEDs 4
NetScreen-5XT, system status LEDs 3

P

password
 forgetting 15
password, changing 12
port status LEDs 4
power LED 2

R

reset 15

S

status LED 3
system IP address 13
system status LEDs 3

T

Transparent mode 10

