ARTISAN®
TECHNOLOGY GROUP

Your **definitive** source for quality pre-owned equipment.

Artisan Technology Group
(217) 352-9330 | sales@artisantg.com | artisantg.com

Full-service, independent repair center
with experienced engineers and technicians on staff.

We buy your excess, underutilized, and idle equipment
along with credit for buybacks and trade-ins.

Custom engineering
so your equipment works exactly as you specify.

- Critical and expedited services
- In stock / Ready-to-ship
- Leasing / Rentals / Demos
- ITAR-certified secure asset solutions

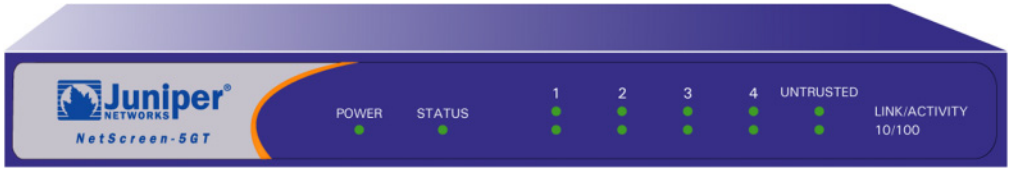
Expert team | Trust guarantee | 100% satisfaction

All trademarks, brand names, and brands appearing herein are the property of their respective owners.

Find the *Juniper Networks NS-5GT-001* at our website: *Click HERE*

NETSCREEN-5GT
USER'S GUIDE

Version 5.0.0 P/N 093-1239-000 Rev. B



Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

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.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Contents

Preface v

Organization v

CLI Conventions v

Juniper Networks NetScreen Publications vi

Chapter 1 Connecting the Device 1

Connecting the NetScreen Device to the Network 1

Connecting the Power 1

Rack Mounting (Optional) 1

Chapter 2 Chapter 3 Configuring the Device 3

Default Settings 4

Accessing the Device 7

Configuring the Untrust Interface 9

Changing Your Admin Name and Password 9

Verifying External Connectivity 10

Resetting the Device to Factory Defaults 10

Chapter 4 Hardware Descriptions 13

Port and Power Connectors 13

Status LEDs 14

Appendix A Specifications A-1

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Preface

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

Juniper Networks offers three versions of NetScreen-5GT:

- The 10-user version supports up to 10 users.
- The Plus version supports an unrestricted number of users.
- The Extended version provides the same capabilities as the Plus version with additional features: High Availability (NSRP Lite), the DMZ security zone, and additional sessions and tunnel capacity.

ORGANIZATION

This manual has three chapters and one appendix.

Chapter 1, "Connecting the Device" describes how to install the NetScreen-5GT device in a rack, connect the device to your network, and connect the power.

Chapter 3, "Configuring the Device" describes the default settings and operation of the NetScreen-5GT and the configuration required to use the device with its default settings.

Chapter 4, "Hardware Descriptions" provides an overview of the NetScreen-5GT ports, LEDs, and power requirements.

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

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".

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

- Variables appear in *italic*. For example:

```
set admin user name password
```

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

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

1

Connecting the Device

This chapter describes how to connect a NetScreen-5GT device to the network and connect the power. If you are using the optional NetScreen-5GT rack mount kit, rack mounting instructions are included at the end of this chapter.

Note: *For safety warnings and instructions, 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.*

Connecting the NetScreen Device to the Network

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 port on the NetScreen-5GT to the external router or modem.

The NetScreen-5GT contains four trusted ports. You can use one of these ports to connect it to a LAN via an internal switch or hub. You can also connect one or all of the ports directly to workstations, eliminating the need for a hub or switch. You can use either cross-over or straight-through cables to connect NetScreen-5GT ports to other devices.

Connecting the Power

To connect the power to the NetScreen-5GT :

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.

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

Rack Mounting (Optional)

With a NetScreen-5GT rack-mount kit, you can mount one or two NetScreen-5GTs in a standard 19-inch equipment rack. The NetScreen-5GT rack-mount kit includes these instructions and a rack-mounting tray. The dimensions of the tray are as follows:

- Width: 19 inches
- Height: 1 5/8 inches; that is, 1 RU (rack unit)
- Depth: 10 3/4 inches

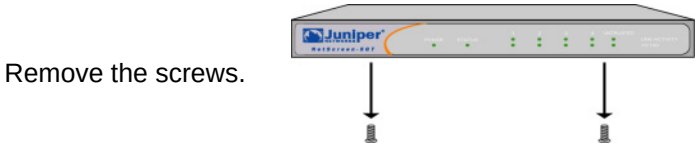
Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

In addition to a NetScreen-5GT, rack-mount kit, and equipment rack, you also need the following:

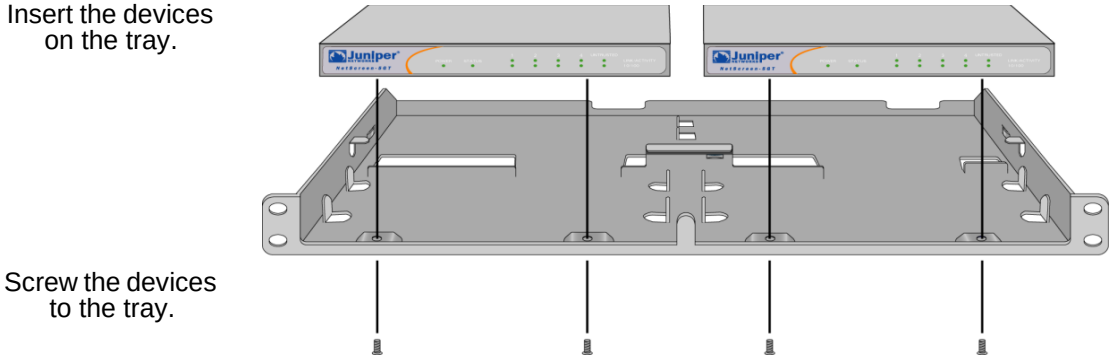
- Phillips-head screwdriver
- Four screws that match the thread size of the equipment rack

To mount the device in a rack:

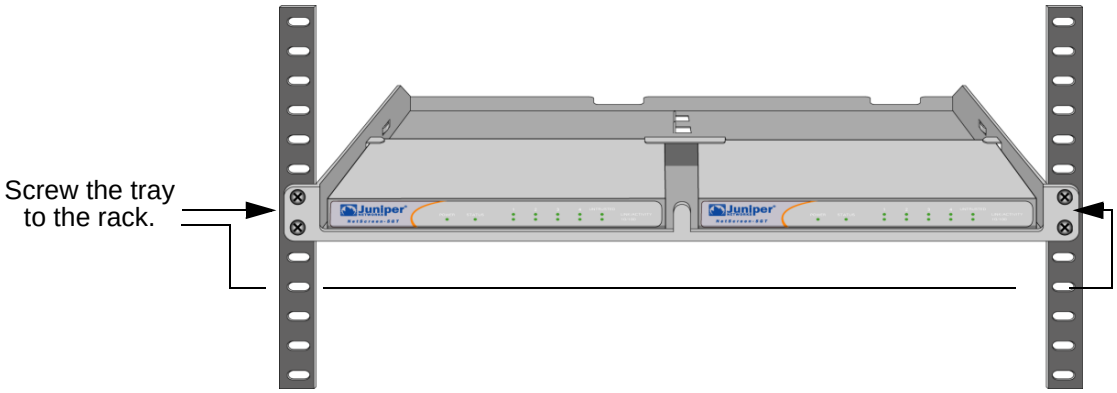
1. Use the Phillips-head screwdriver to remove the two screws from the underside of each NetScreen-5GT that you intend to mount. The screws are located on the underside of the NetScreen-5GT near the front panel. (Keep the screws for use in the next step.)



2. Insert the NetScreen-5GT devices on the rack-mount tray and screw them to the tray with the screws that you removed in step 1.



3. Screw the left and right tray plates to the equipment rack.



You can run power cords and ethernet cables through the openings in the floor of the tray or out the depressions in the back wall. You can also use the space behind the devices to hold power supplies. The switching power supplies, which you can order separately, fit easily in a 1-RU height space.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

2

Configuring the Device

This chapter describes how to configure a NetScreen-5GT after you have installed and connected it to your network and to a power source. After completing the necessary configurations, users in your network will be able to access the Internet through the NetScreen-5GT while resources in your network are protected from outside computers.

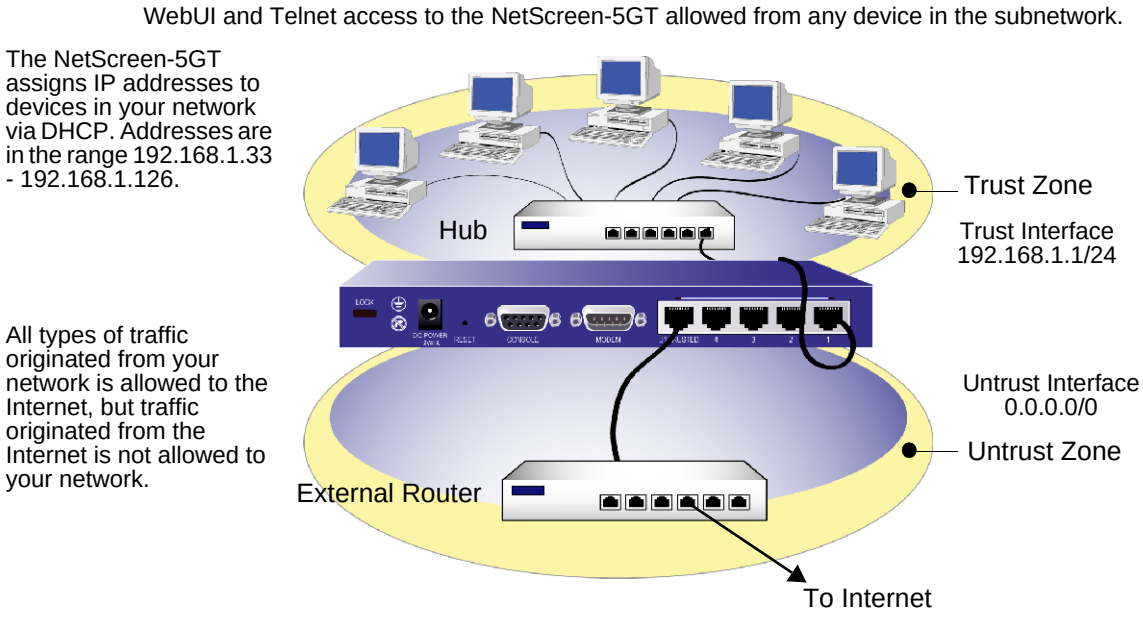
Note: *You must register your product at www.juniper.net/support/ so that certain NetScreen ScreenOS services, such as internal antivirus or Deep Inspection Signature Service, can be activated on the device. After registering your product, use the WebUI or CLI to obtain the subscription for the service. 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 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-5GT Getting Started Guide.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

DEFAULT SETTINGS

This section describes the default settings and operation of the NetScreen-5GT as it is shipped from the factory. These default settings are such that, in most cases, there are only a few items that you must configure. The figure below shows the default configuration for the NetScreen-5GT.



The Untrust interface is bound to the Untrust zone and is configured with the IP address 0.0.0.0/0. To allow the NetScreen-5GT (and the devices on your network) to connect to the Internet, you must configure the Untrust interface according to information obtained from your Internet Service Provider (ISP). Refer to "Untrust Interface Address" on page 5.

Any user in the subnetwork can manage the NetScreen-5GT if they know the login and password. To change the default login and password, refer to "Admin Name and Password" on page 5. To restrict management of the NetScreen-5GT to specific workstations, refer to "Restricting Management" on page 6.

The Trust interface is bound to the Trust zone and is configured with the subnetwork address 192.168.1.1/24. This means that all devices in your network that you connect to the Trust interface must be in the same subnetwork and have IP addresses in that subnetwork. The NetScreen-5GT is also configured to assign IP addresses for the 192.168.1.1/24 subnetwork to your devices. For more information, refer to "Trust Interface Address" on page 6.

The NetScreen-5GT allows any type of traffic to the Internet that originates from devices in your network, but does not allow any traffic that originates in the Internet to reach your network. You can configure additional restrictions; refer to "Additional Policies" on page 7.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Required Configuration

This section describes the configurations that you must complete to use the NetScreen-5GT with its default settings.

Note: *If you have any problems completing a configuration and you need to restore the device to its default settings, see* *"Resetting the Device to Factory Defaults" on page 10*.

Untrust Interface Address

You must configure an IP address for the Untrust interface to enable the NetScreen-5GT to connect to the Internet. This IP address represents your network to the outside world and is obtained from your Internet Service Provider (ISP) in one of the following ways:

- Your ISP gives you a specific, fixed IP address and netmask for your network.
- Your network receives an IP address from a server via Dynamic Host Configuration Protocol (DHCP).
- Your network receives an IP address from a server via Point-to-Point Protocol over Ethernet (PPPoE).

See "Configuring the Untrust Interface" on page 9.

Admin Name and Password

Juniper Networks highly recommends that you change your admin name and password to the NetScreen-5GT, as all Juniper Networks NetScreen products use the same default admin name and password. See "Changing Your Admin Name and Password" on page 9.

Optional Configuration

The following optional configurations are not described in detail in this manual. Refer to the appropriate sections in the *NetScreen Concepts & Examples ScreenOS Reference Guide* for more information.

Port Mode

The *port mode* is the binding of physical ports, logical interfaces, and zones. The default port mode, Trust-Untrust, binds the Trust interface to the Trust zone and the Untrust interface to the Untrust zone. Changing the port mode changes these bindings. This manual only covers configuring the NetScreen-5GT in the Trust-Untrust port mode. For more information about port modes and how to change them, refer to the "Zones" chapter in Volume 2 of the *NetScreen Concepts & Examples ScreenOS Reference Guide*.

Warning: *Changing the port mode removes any existing configurations on the NetScreen-5GT. Therefore, change the port mode before configuring it.*

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Restricting Management

By default, anyone in your network can manage the NetScreen-5GT if they know the login and password. You can configure the NetScreen-5GT to be managed only from a specific host on your network. (And you can choose which services — for example, WebUI, Telnet, ping — you want enabled on the NetScreen-5GT.) Refer to the "Administration" chapter in Volume 3 of the *NetScreen Concepts & Examples ScreenOS Reference Guide.*

Operational Mode

The *operational mode* is the way an interface on a NetScreen-5GT processes traffic between zones. By default, the NetScreen-5GT operates in Route mode with network address translation (NAT) enabled on the Trust interface. This means that when devices in the Trust zone send traffic to the Internet, the NetScreen-5GT replaces the original source IP addresses with the IP address of the Untrust interface. While the NetScreen-5GT assigns "private" IP addresses to the devices in your network, these addresses remain hidden to computers outside your network.

If all devices in your network have public IP addresses, you can configure the NetScreen-5GT for Transparent mode or Route mode without NAT enabled. In Transparent mode, the NetScreen-5GT forwards traffic without checking IP addresses. In Route mode without NAT enabled, the NetScreen-5GT routes traffic by checking IP addresses. For more information about configuring the device for Transparent mode or Route mode without NAT enabled, refer to the "Interface Modes" chapter in Volume 2 of the *NetScreen Concepts & Examples ScreenOS Reference Guide.*

Trust Interface Address

You can change the IP address and netmask of the Trust interface if necessary. (Remember that the IP addresses of devices in your network are never seen by computers outside your network; outside computers see only the IP address of the Untrust interface.) For example, you might need to change the Trust interface to match the IP addresses that already exist on your network. If you change the IP address and netmask of the Trust interface, you also need to change either the range of addresses that the NetScreen device assigns via DHCP to devices in the network, or disable the DHCP server on the Trust interface.

To assign a different IP address and netmask to the Trust interface, refer to the "Interfaces" chapter in Volume 2 of the *NetScreen Concepts & Examples ScreenOS Reference Guide.*

To change the DHCP settings for the NetScreen-5GT, refer to the "System Parameters" chapter in Volume 2 of the *NetScreen Concepts & Examples ScreenOS Reference Guide.*

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Additional Policies

The NetScreen-5GT is configured with a default policy that permits workstations in your network to access any kind of service with outside computers, while outside computers are not allowed to access or start sessions with your workstations. You can configure policies that direct the NetScreen-5GT to permit outside computers to start specific kinds of sessions with your computers. To create or modify policies, refer to the "Policies" chapter in Volume 2 of the *NetScreen Concepts & Examples ScreenOS Reference Guide.*

ACCESSING THE DEVICE

You can configure and manage the NetScreen-5GT in several ways:

- WebUI: The NetScreen ScreenOS WebUI is a graphical interface that is available through a Web browser. To use the WebUI, you must be on the same subnetwork as the NetScreen-5GT. See "Using the WebUI" on page 7.
- Telnet: Telnet is an application that allows you to access devices through an IP network. To access and configure the NetScreen-5GT, enter the NetScreen ScreenOS Command Line Interface (CLI) commands in a Telnet session from your workstation. See "Using Telnet" on page 8.

  Note: *You can also access remote NetScreen-5GT using Secure Shell (SSH) applications. Refer to the "Administration" chapter in Volume 3 of the* NetScreen Concepts & Examples ScreenOS Reference Guide *for more information.*

- 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.
- Console connection: The Console port on the NetScreen-5GT allows you to access it through a serial cable connected to your workstation or terminal. To access and configure the NetScreen-5GT, enter the NetScreen ScreenOS CLI commands on your terminal or in a terminal emulation program on your workstation. See "Using a Console Connection" on page 8.

Using the WebUI

To use the WebUI, you must be on the same subnetwork as the NetScreen-5GT. To access it with the WebUI management application:

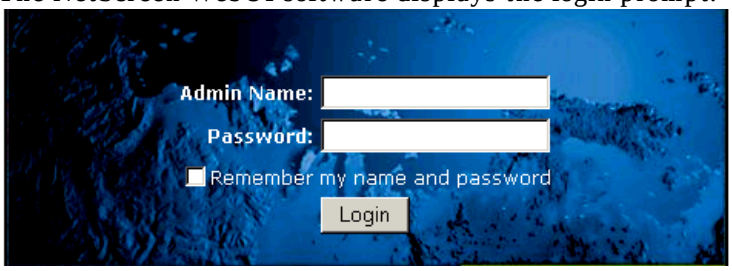
1. Connect your workstation (or your LAN hub) to the Trusted port, as described in "Connecting the NetScreen Device to the Network" on page 1.
2. Launch your browser, enter the IP address for the Trust interface in the URL field, and then press Enter.

   For example, if the IP address of the Trust interface on the NetScreen-5GT is 192.168.1.1/24, enter the following:

   `192.168.1.1`

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

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. (If you access the NetScreen-5GT for the first time using the WebUI, the Initial Configuration Wizard appears; refer to the *Juniper Networks NetScreen-5GT Getting Started Guide*.)

Using Telnet

1. Connect your workstation (or your LAN hub) to the Trusted port, as described in "Connecting the NetScreen Device to the Network" on page 1.
2. Start a Telnet client application to the IP address for the Trust interface.

   For example, if the IP address of the Trust interface on the NetScreen-5GT is 192.168.1.1/24, enter the following:

   `192.168.1.1`
3. Enter **netscreen** in both the **login** and **password** prompts. (Use lowercase letters only. The login and password fields are both case sensitive.)

Using a Console Connection

Note: *For the console connection, you require 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 connection:

1. Plug the female DB-9 end of the serial cable into the serial port of your computer. (Be sure that the DB-9 connector is seated properly in the port.)
2. Plug the male DB-9 end of the serial cable into the Console port of the NetScreen-5GT (Be sure that the DB-9 connector is seated properly in the port.)
3. Launch a serial terminal emulation program. (A commonly-used terminal program is Hilgreave HyperTerminal.) The required settings to launch a console session with your NetScreen-5GT are as follows:
   - Baud Rate: 9600
   - Parity: No

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

- Data Bits: 8
- Stop Bit: 1
- Flow Control: None

4. Enter **netscreen** in both the **login** and **password** prompts. (Use lowercase letters only. The login and password fields are both case sensitive.)

Configuring the Untrust Interface

Your network uses the Untrust interface on the NetScreen-5GT to connect to the Internet. If you are setting up your Internet connection for the first time, contact your ISP for information on your network IP address assignment.

Note: *If you access the device for the first time using the NetScreen ScreenOS WebUI graphical interface, the Initial Configuration Wizard appears when you log in to the WebUI to guide you through the configuration described in this chapter. Therefore, only the CLI commands are shown in this chapter.*

- If your ISP gave you a specific, fixed IP address and netmask for your network, configure the IP address and netmask for the network and the IP address of the router port connected to the NetScreen device. Enter the following CLI commands in a Telnet or Console session:

```
set interface untrust ip ip_addr/mask
set interface untrust gateway ip_addr
save
```

- If your network receives an IP address from a server via DHCP, enter the following CLI commands in a Telnet or Console session:

```
set interface untrust dhcp client enable
save
```

- If your network receives an IP address from a server via PPPoE, configure the user name and password assigned by your ISP. Enter the following CLI commands in a Telnet or Console session:

```
set pppoe interface untrust
set pppoe username name_str password pswd_str
save
```

Changing Your Admin Name and Password

Because all Juniper Networks NetScreen products use the same default admin name and password (**netscreen**), it is highly advisable to change your admin name and password immediately. In a Telnet or Console session, enter the following CLI commands:

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


Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

For information on creating different levels of administrators, see the “Administration” chapter in Volume 3 of the *NetScreen Concepts & Examples ScreenOS Reference Guide*.

Verifying External Connectivity

To verify that workstations in your network can access resources on the Internet, start a Web browser from any workstation in the network and enter the following URL: www.juniper.net.

Resetting the Device to Factory Defaults

If you lose the admin password, you can reset the NetScreen-5GT to its default settings. This destroys any existing configurations, but restores access to it.

Warning: *Resetting the device deletes all existing configuration settings and renders existing firewall and VPN service inoperative.*

You can restore the NetScreen-5GT to its default settings in one of the following ways:

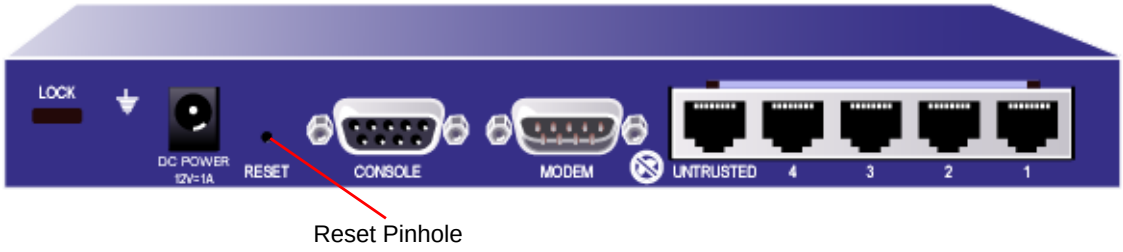
- Using a Console connection. For further information, see the “Administration” chapter in Volume 3 of the *NetScreen Concepts & Examples ScreenOS Reference Guide*.
- Using the reset pinhole on the rear panel of the device, as described in the next section.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Using the Reset Pinhole

You can reset the NetScreen-5GT and restore the factory default settings by pressing the reset pinhole. To perform this operation, you need to either view the status LEDs on the front panel or have a Console session as described in "Using a Console Connection" on page 8.

1. Locate the reset pinhole on the rear panel. Using a thin, firm wire (such as a paper clip), push the pinhole for four to six seconds and then release.



   The Status LED blinks amber. A message on the Console states that erasure of the configuration has started and the system sends an SNMP/SYSLOG alert.

2. Wait for one to two seconds.

   After the first reset, the power LED blinks green; the NetScreen-5GT is now waiting for the second push. The Console message now states that it is waiting for a second 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 NetScreen-5GT resets to its original factory settings.

   When it resets, the Status LED turns amber for one-half second and then returns to the blinking green state. The Console message states that the configuration is erased and the unit is reset. The system generates SNMP and SYSLOG alerts to configured SYSLOG or SNMP trap hosts.

5. The NetScreen-5GT restarts.

If you do not follow the complete sequence, the reset process cancels without any configuration change and the console message states that the erasure of the configuration is aborted. The Status LED returns to blinking green. If the device did not reset, an SNMP alert is sent to confirm the failure.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

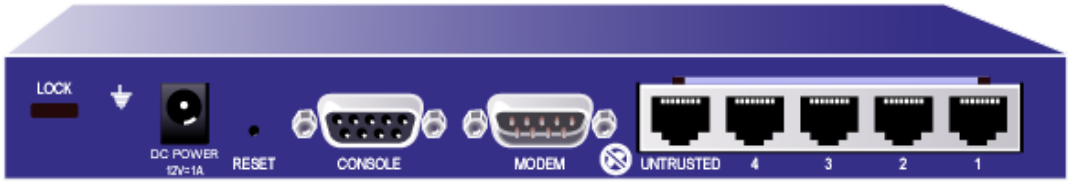
4

Hardware Descriptions

This chapter provides descriptions of the NetScreen-5GT chassis.

Port and Power Connectors

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



The DC power receptacle is for connecting power to the NetScreen-5GT.

The Reset pinhole allows you to reset the device and restore its factory default settings.

The NetScreen-5GT includes the following ports:

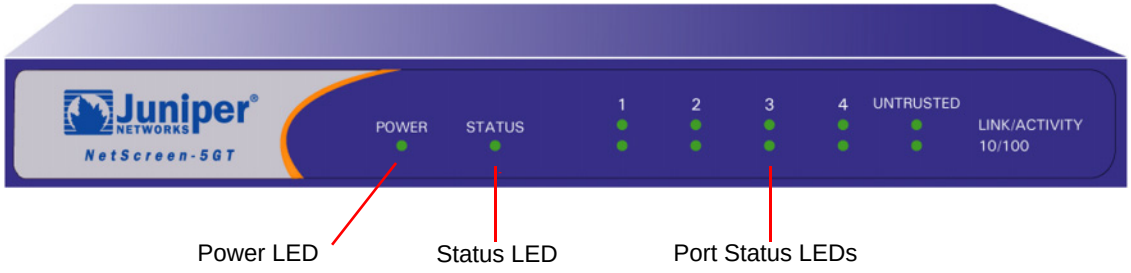
Port	Description	Connector	Speed/Protocol
Console	Enables a serial connection with the system. Used for launching Command Line Interface (CLI) sessions.	DB-9	9600 bps/ RS-232
Modem	High-speed modem port.	DB-9	9600 bps-115 Kbps/ RS-232
Untrusted	Enables an Internet connection through an external router, DSL modem, or cable modem.	RJ-45	10/100 Mbps/ Ethernet
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

Warning: *Do not connect a TNV circuit (phone line or ISDN line) directly to the modem port on the NetScreen-5GT. You must first connect the device to a modem, using an RS-232 port, then connect the modem to the TNV circuit.*

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

STATUS LEDS

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



Interpreting Status LEDs for NetScreen-5GT

The device status LEDs indicate whether it 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 system is starting up.
	Green	Blinking On indicates the system is functioning.
	Red	Blinking On indicates a diagnostics or system initialization error.
	Off	Off indicates the system is not operational.

Interpreting Port Status LEDs

The port status LEDs indicate whether the ports on the NetScreen-5GT are operating properly. The following table describes the possible status for the 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.
	Amber	Solid On indicates the port is connected to a 10 Base-T device.

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

A

Specifications

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

Attributes		
Height	1.125 inches	
Depth	5 inches	
Width	8.25 inches	
Weight	1.3 pounds	
Electrical	Switching Regulator	Linear Regulator
	AC voltage: 100-240 VAC +/- 10% 50/60 Hz AC Watts: 12 Watts DC voltage: 12 Volts	AC voltage: 120 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)	
Certifications	Safety	EMI
	UL CUL CSA CE CB Austel	FCC Part 15 class B VCCI CTIC BSMI
Connectors	The RJ-45 twisted-pair ports are compatible with the IEEE 802.3 Type 10/100 Base-T standard	
Standard	100Base-TX	
Media Type	Category 5 and higher Unshielded Twisted Pair (UTP) Cable	
Maximum Distance	100 meters	

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Artisan Technology Group - Quality Instrumentation ... Guaranteed | (888) 88-SOURCE | www.artisantg.com

Artisan Technology Group is an independent supplier of quality pre-owned equipment

Gold-standard solutions

Extend the life of your critical industrial, commercial, and military systems with our superior service and support.

We buy equipment

Planning to upgrade your current equipment? Have surplus equipment taking up shelf space? We'll give it a new home.

Learn more!

Visit us at **artisantg.com** for more info on price quotes, drivers, technical specifications, manuals, and documentation.

Artisan Scientific Corporation dba Artisan Technology Group is not an affiliate, representative, or authorized distributor for any manufacturer listed herein.

We're here to make your life easier. How can we help you today?

(217) 352-9330 | sales@artisantg.com | artisantg.com

ARTISAN® TECHNOLOGY GROUP