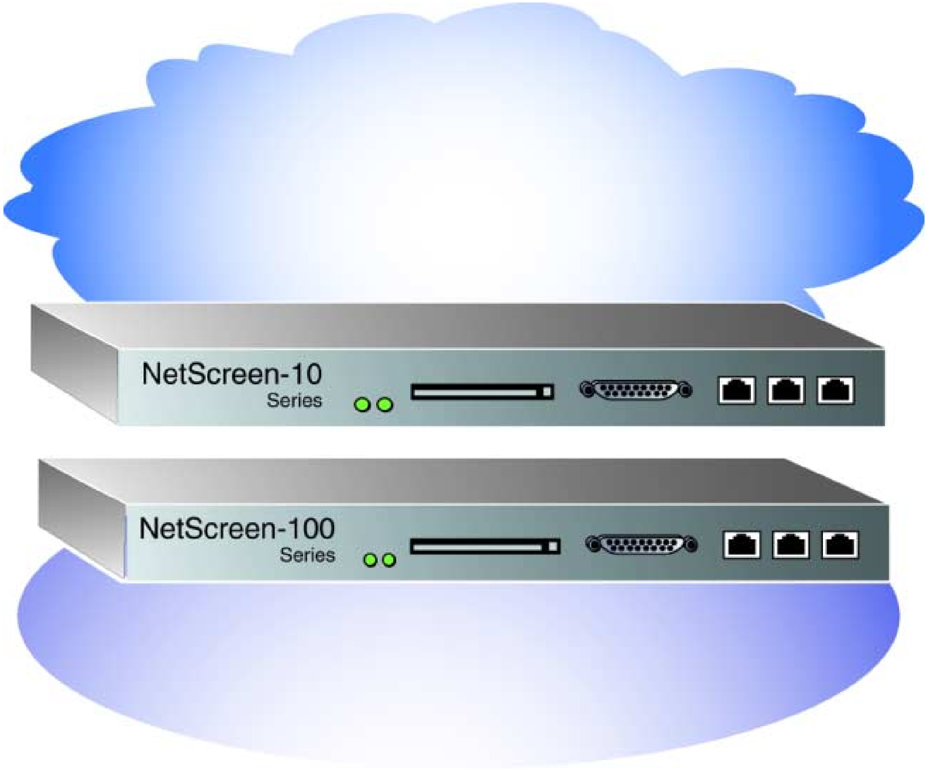
NETSCREEN-10/100

Installer's Guide

Note to Reader: This is a preliminary version of this document.

An updated version will be made available in the very near future.

Version 2.6.0 P/N 093-0042-000 Rev. B



Copyright Notice

NetScreen, the NetScreen logo, NetScreen-5, NetScreen-10, and NetScreen-100 are registered trademarks or trademarks of NetScreen Technologies, Inc.

Netscape Communicator is a registered trademark of Netscape in the United States and/or other countries. Microsoft, Windows and Windows NT are registered trademarks of Microsoft Corporation in the U.S.A. and/or other countries. Hyperterminal is a registered trademarks of Hilgaeve Corporation. All other brands and their products mentioned in this document are trademarks or registered trademarks of their respective owners.

The specifications regarding the products in this manual are subject to change without notice. All statements, information, and recommendations in this manual are believed to be accurate but are presented without warranty of any kind, express or implied. Users must take full responsibility for their application of any products. This document may only be used or copied in accordance with the terms of such license.

NetScreen Technologies, Inc.
350 Oakmead Parkway, Suite 500
Sunnyvale, CA 94085 U.S.A.
www.netscreen.com

FCC Statement

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 in a light commercial installation. This equipment generates, uses and can radiate radio frequency energy, and, if not installed and used in accordance with the instruction, may cause harmful interference to radio communications. 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.

Product License Agreement

PLEASE READ THIS LICENSE AGREEMENT (“AGREEMENTS”) CAREFULLY BEFORE USING THIS PRODUCT. BY INSTALLING AND OPERATING, YOU INDICATE YOUR ACCEPTANCE OF THE TERMS OF THIS LEGAL AND BINDING AGREEMENT AND ARE CONSENTING TO BE BOUND BY AND ARE BECOMING A PART TO THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, DO NOT START THE INSTALLATION PROCESS.

1. License Grant. This is a license, not a sales agreement, between you, the end user, and NetScreen Technologies, Inc. (“NetScreen”). The term “Firmware” includes all NetScreen and third party Firmware and software provided to you with the NetScreen product, and includes any accompanying documentation, any updates and enhancements of the Firmware and software provided to you by NetScreen, at its option. NetScreen grants to you a non-transferable (except as provided in section 3 (“Transfer”) below, non-exclusive license to use the Firmware and software in accordance with the terms set forth in this License Agreement. The Firmware and software are “in use” on the product when they are loaded into temporary memory (i.e. RAM).

2. Limitation on Use. You may not attempt and if you are a corporation, you will use best efforts to prevent your employees and contractors from attempting to, (a) modify, translate, reverse engineer decompile, disassemble, create, derivative works based on, sublicense, or distribute the Firmware or the accompanying documentation; (b) rent or lease any rights in the Firmware or software or accompanying documentation in any form to any person; or (c) remove any proprietary notice, labels, or marks on the Firmware, software, documentation, and containers.

3. Transfer. You may transfer (not rent or lease) the Firmware or software to the end user on a permanent basis, provided that: (i) the end user receives a copy of this Agreement and agrees in writing to be bound by its terms and conditions, and (ii) you at all times comply with all applicable United States export control laws and regulations.

4. Proprietary Rights. All rights, title, interest, and all copyrights to the Firmware, software, documentation, and any copy made by you remain with NetScreen. You acknowledge that no title to the intellectual property in the Firmware and software is transferred to you and you will not acquire any rights to the Firmware except for the license as expressly set forth herein.

5. Term and Termination. The term of the license is for the duration of NetScreen's copyright in the Firmware and software. NetScreen may terminate this Agreement immediately without notice if you breach or fail to comply with any of the terms and conditions of this Agreement. You agree that, upon such termination, you will either destroy all copies of the documentation or return all materials to NetScreen. The provisions of this Agreement, other than the license granted in Section 1 (“License Grant”) shall survive termination.

6. Limited Warranty. For a period of one (1) year after delivery to Customer, NetScreen will repair or replace any defective product shipped to Customer, provided it is returned to Netscreen at Customer's expense within that period. For a period of ninety (90) days after the initial delivery of a particular product, NetScreen warrants to Customer that such product will substantially conform with NetScreen's published specifications for that product if properly used in accordance with the procedures described in documentation supplied by NetScreen. NetScreen's exclusive obligation with respect to non-conforming product shall be, at NetScreen's option, to replace the product or use diligent efforts to provide Customer with a correction of the defect, or to refund to customer the purchase price paid for the unit. Defects in the product will be reported to NetScreen in a form and with supporting information reasonably requested by NetScreen to enable it to verify, diagnose, and correct the defect. For returned product, the customer shall notify NetScreen of any nonconforming product during the warranty period, obtain a return authorization for the nonconforming product, from NetScreen, and return the nonconforming product to NetScreen's factory of origin with a statement describing the nonconformance.

NOTWITHSTANDING ANYTHING HEREIN TO THE CONTRARY, THE FOREGOING IS CUSTOMER'S SOLE AND EXCLUSIVE REMEDY FOR BREACH OF WARRANTY BY NETSCREEN WITH RESPECT TO THE PRODUCT.

The warranties set forth above shall not apply to any Product or Hardware which has been modified, repaired or altered, except by NetScreen, or which has not been maintained in accordance with any handling or operating instructions supplied by NetScreen, or which has been subjected to unusual physical or electrical stress, misuse, abuse, negligence or accidents.

THE FOREGOING WARRANTIES ARE THE SOLE AND EXCLUSIVE WARRANTIES EXPRESS OR IMPLIED GIVEN BY NETSCREEN IN CONNECTION WITH THE PRODUCT AND HARDWARE, AND NETSCREEN DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. NETSCREEN DOES NOT PROMISE THAT THE PRODUCT IS ERROR-FREE OR WILL OPERATE WITHOUT INTERRUPTION.

7. Limitation of Liability. IN NO EVENT SHALL NETSCREEN OR ITS LICENSORS BE LIABLE UNDER ANY THEORY FOR ANY INDIRECT, INCIDENTAL, COLLATERAL, EXEMPLARY, CONSEQUENTIAL OR SPECIAL DAMAGES OR LOSSES SUFFERED BY YOU OR ANY THIRD PARTY, INCLUDING WITHOUT LIMITATION LOSS OF USE, PROFITS, GOODWILL, SAVINGS, LOSS OF DATA, DATA FILES OR PROGRAMS THAT MAY HAVE BEEN STORED BY ANY USER OF THE FIRMWARE. IN NO EVENT WILL NETSCREEN'S OR ITS LICENSORS' AGGREGATE LIABILITY CLAIM BY YOU, OR ANYONE CLAIMING THROUGH OR ON BEHALF OF YOU, EXCEED THE ACTUAL AMOUNT PAID BY YOU TO NETSCREEN FOR FIRMWARE.

Some jurisdictions do not allow the exclusions and limitations of incidental, consequential or special damages, so the above exclusions and limitations may not apply to you.

8. Export Law Assurance. You understand that the Firmware is subject to export control laws and regulations.

YOU MAY NOT DOWNLOAD OR OTHERWISE EXPORT OR RE-EXPORT THE FIRMWARE OR ANY UNDERLYING INFORMATION OR TECHNOLOGY EXCEPT IN FULL COMPLIANCE WITH ALL UNITED STATES AND OTHER APPLICABLE LAWS AND REGULATIONS.

9. U.S. Government Restricted Rights. If this Product is being acquired by the U.S. Government, the Product and related documentation is commercial computer Product and documentation developed exclusively at private expense, and (a) if acquired by or on behalf of civilian agency, shall be subject to the terms of this computer Firmware, and (b) if acquired by or on behalf of units of the Department of Defense ("DoD") shall be subject to terms of this commercial computer Firmware license Supplement and its successors.

10. Tax Liability. You agree to be responsible for the payment of any sales or use taxes imposed at any time whatsoever on this transaction.

11. General. If any provisions of this Agreement are held invalid, the remainder shall continue in full force and effect. The laws of the State of California, excluding the application of its conflicts of law rules shall govern this License Agreement. This Agreement will not be governed by the United Nations Convention on the Contracts for the International Sale of Goods. This Agreement is the entire agreement between the parties as to the subject matter hereof and supersedes any other Technologies, advertisements, or understandings with respect to the Firmware and documentation. This Agreement may not be modified or altered, except by written amendment, which expressly refers to this Agreement and which, is duly executed by both parties.

You acknowledge that you have read this Agreement, understand it, and agree to be bound by its terms and conditions.

Hardware, including technical data, is subject to U.S. export laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. Customer agrees to comply strictly with all such regulations and acknowledges that it has the responsibility to obtain licensed to export, re-export, or import hardware.

Table of Contents

Preface

Note to Reader: *This is a preliminary version of this document. An updated version will be made available in the very near future.*

The NetScreen-10™ and NetScreen-100™ are network security devices that protect your Ethernet local area network (LAN) when connecting to the Internet. Using a NetScreen-10/100 as a firewall, you can configure access policies that control inbound and outbound network and VPN traffic.

Manual Organization

This manual has 3 chapters and 2 appendices.

Chapter 1, Hardware Description, describes the NetScreen® device. It explains the functions of the status LEDs, identifies the device interface ports, and details the front and back panels of the device.

Chapter 2, Connecting the NetScreen-10/100 to the Network, explains how to connect the NetScreen-10/100 to the network as a standalone unit or, with two or more NetScreen-100 devices, for High Availability (HA).

Chapter 3, Initial Configuration, explains how to configure the NetScreen-10/100 with a network using both the command line interface (CLI) and the web user interface (WebUI).

Appendix A, "Safety Recommendations and Warnings" provides general site requirements as well as safety warnings and general cautions when using the NetScreen-10/100 device.

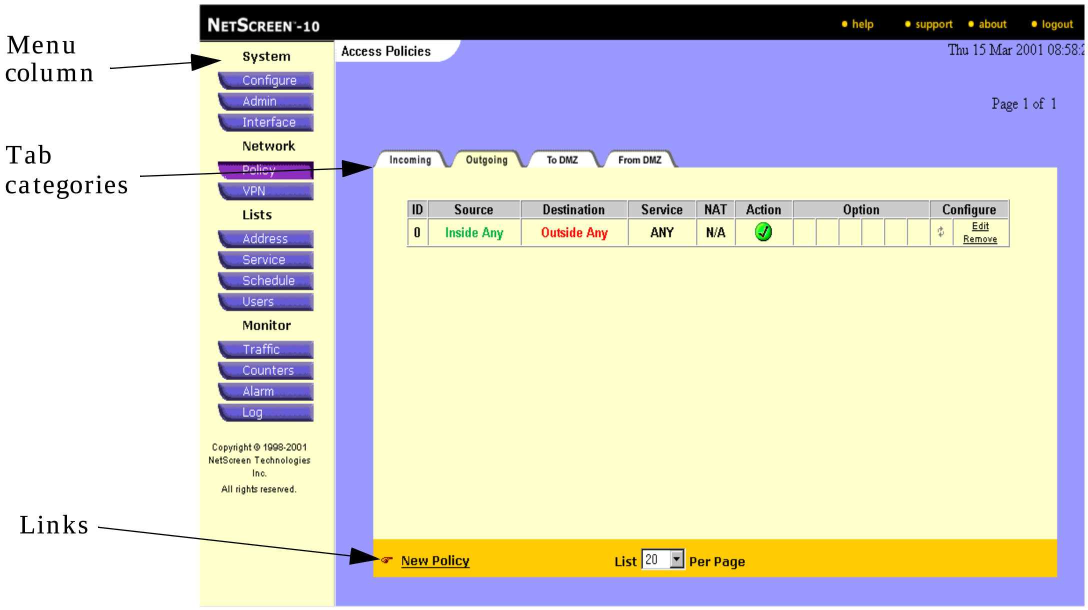
Appendix B, "DC Power Supply" provides technical specifications and electrical requirements for the DC power supply unit of the NetScreen-10/100.

General Layout of the NetScreen-10/100 Web UI

The web user interface (WebUI) consists of two main logical sections: the menu column and the central display area.

- The menu column consists of four main functional categories: System, Network, Lists, and Monitor, each of which contain further sub-functions, represented by tabs in the central display area. During the configuration process, you first must select a main functional category before choosing the various utilities offered within each sub-category.

- The central display area lists the information for each of the categories in the menu column, in either a tabular or graphical format. These pages generally contain links to dialog boxes through links such as **New Policy**, **New Manual Key User**, **New Entry**, **Edit** and so forth.



ID	Source	Destination	Service	NAT	Action	Option	Configure
0	Inside Any	Outside Any	ANY	N/A	✓		Edit Remove

The NetScreen-10/100 Central Display Area

Command Line Interface (CLI) Syntax

These conventions apply to all NetScreen commands:

- To remove a single character, press BACKSPACE or CTRL+H.
- To remove an entire line, press CTRL+U.
- To traverse up to 16 lines forward in the command history buffer, press CTRL+F or the DOWN ARROW key.

Note: *To use the arrow keys for navigating among commands in a Telnet session on Windows 95, 98, NT, or 2000: On the Terminal menu, click* ***Preferences...****, select the* ***VT100 Arrows*** *check box, and click the* ***OK*** *button.*

- To traverse up to 16 lines backward in the command history buffer, press CTRL+B or the UP ARROW key.
- To see the next available keyword or input, and a brief description of usage, type a question mark (?).
- A parameter inside [ ] (square brackets) is optional.
- A parameter inside { } (braces) is required.
- Anything inside < > is a variable.
- If there is more than one choice for a parameter inside [ ] and { }, they are separated by *a pipe* (|). For example, [auth {md5 | sha-1}] means “choose either MD5 or SHA-1 as your authentication method.”
- IP addresses are represented by <a.b.c.d> and <w.x.y.z>.
- A subnet mask is represented by <A.B.C.D>.
- The console times out and the connection is broken if no keyboard activity is detected for 10 minutes.

Items you enter are into the system are in **bold** text.

Related Publications

The following technical publication ships with the NetScreen-100 device.

NetScreen-100 Getting Started Guide
(P/N 093-0019-000, Rev. B)

The following publication ships with the NetScreen-10 device:

NetScreen-10 Getting Started Guide
(P/N 093-0018-000, Rev. B)

The following publications are included on the product CD for both devices:

NetScreen CLI Reference Guide
(P/N 093-0011-000, Rev. C)

NetScreen WebUI Reference Guide
(P/N 093-0040-000, Rev. B)

NetScreen Concepts & Examples ScreenOS Reference Guide
(P/N 093-0039-000, Rev. B)

Hardware Description 1

This chapter provides illustrations and descriptions of the NetScreen-10/100 front and back panels.

Before you install your NetScreen device, you should unpack it onsite and verify the contents against the packing slip.

A front view of the NetScreen-10/100 is shown below. The label on the left side indicates the model name: NetScreen-10 or NetScreen-100.

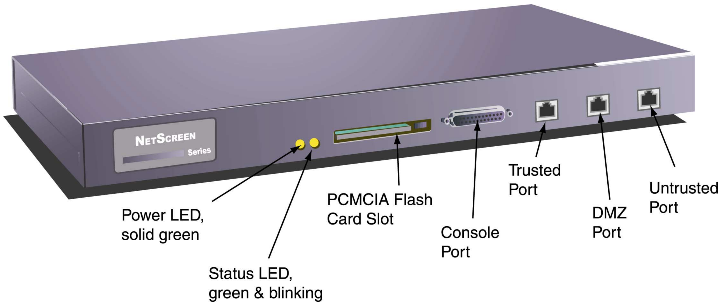


Figure 1-1 Front Panel of the NetScreen-10/100

- **Power LED**: glows solid green when power is supplied to the NetScreen-10/100.
- **Status LED**: glows solid green when the NetScreen-10/100 is first powered up and the unit first performs diagnostics. Then the unit goes into a startup phase, which takes up to one minute to complete. During startup, the LED blinks orange, after which the LED blinks green. If an error is detected, then the LED glows red. The LED changes to yellow whenever the unit writes to the internal flash card.
- **PCMCIA Flash Card Slot**: The NetScreen-10/100 supports a PCMCIA ATA-compatible flash card. Supported cards include the SanDisk 96-MB and 20-MB CompactFlash. The NetScreen device automatically detects the presence of a flash card and records the event log to it.

- **Console Port**: DB25 serial port connector for local configuration and administration.
- **Trusted Port**: Connect the NetScreen-10/100 using a twisted pair cable with RJ45 connectors. The trusted port is a data circuit-terminating equipment (DCE) port.
- **DMZ Port**: Connect the NetScreen-10/100 using a twisted pair cable with RJ45 connectors. The DMZ port is also a DCE port.
- **Untrusted Port**: Connect the NetScreen-10/100 using a twisted pair cable with RJ45 connectors. The untrusted port is a data terminal equipment (DTE) port.

Note: *For cabling guidelines and instructions, see "Connecting the NetScreen-10/100 as a Single Security Appliance" on page 2-1.*

- **Trusted, DMZ, and Untrusted Ethernet LEDs**: Each Ethernet port has two link lights, or LEDs. The left LED indicates network traffic activity and the right LED indicates if the link is up (connected to an active device). These LEDs differ for the NetScreen-10 and NetScreen-100. See Figure 1-2.

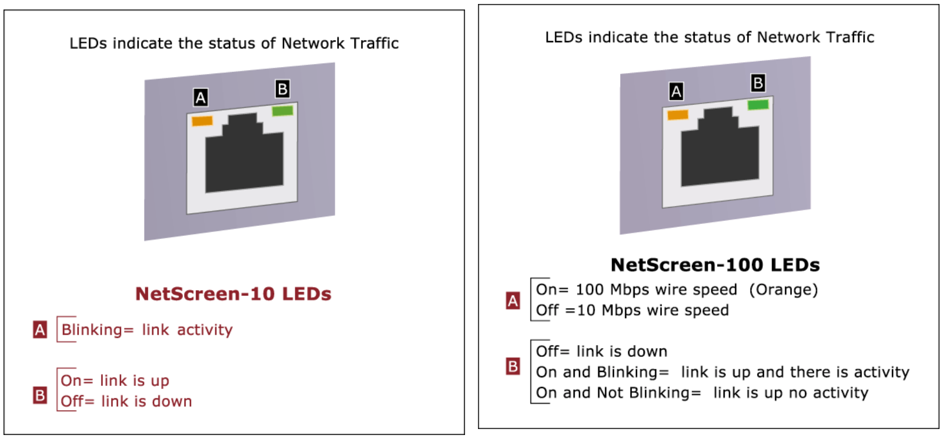

LEDs indicate the status of Network Traffic
A
B
NetScreen-10 LEDs
A Blinking= link activity
B On= link is up
Off= link is down
LEDs indicate the status of Network Traffic
A
B
NetScreen-100 LEDs
A On= 100 Mbps wire speed (Orange)
Off =10 Mbps wire speed
B Off= link is down
On and Blinking= link is up and there is activity
On and Not Blinking= link is up no activity

Figure 1-2 Ethernet LEDs

The back panel of the NetScreen-10/100 is shown in Figure 1-3.

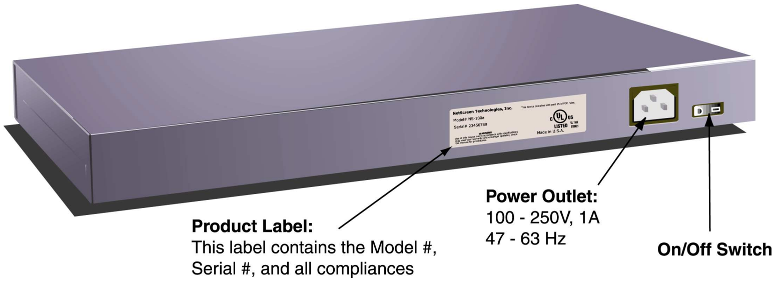


Figure 1-3 Back Panel of the NetScreen-10/100

- **Product Label**: The model number is either NS-10x or NS-100x, where x=a, e, or f.

Table 1-1 NetScreen-10/100 Model Numbers

Model Type	Functionality
a	Firewall & VPN (3DES & DES)
e	Firewall & VPN (DES)
f	Firewall

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

- **Power Outlet**: Use the outlet to connect power to the NetScreen-10/100 with the supplied power cable.

Note: *Figure 1-3 does not show a NetScreen-10/100 equipped with a DC power supply. See "Appendix B: DC Power Supply" for more information.*

- **On/Off Switch**: Turns the power to the NetScreen-10/100 on or off.

⚠ **Caution** *Make sure you have read the Appendix, "Safety Recommendations and Warnings", before you begin installation.*

Connecting the NetScreen-10/100 to the Network

2

Follow the instructions in this chapter to connect the NetScreen-10/100 device to the network and to configure the software for the first time. For further configuration options, see the *NetScreen Concepts & Examples ScreenOS Reference Guide*, on the product CD.

⚠ **Caution** *Make sure you have read Appendix A, "Safety Recommendations and Warnings" , before you begin this chapter.*

This chapter contains the following sections:

- "Gathering the Necessary Tools" on page 2-1
- "Connecting the NetScreen-10/100 as a Single Security Appliance" on page 2-1
- "Connecting the NetScreen-100 for High Availability" on page 2-4

Gathering the Necessary Tools

The chassis can be placed on a table top or mounted in a standard 19-inch equipment rack. Table top installation requires no tools. Rack mounting requires a Phillips-head screwdriver, the rack mount bracket kit, and four screws to match the rack. Screws for attaching the mounting brackets to the chassis are provided in the NetScreen-10/100 product package. Users will have to supply screws to match rack thread size.

Connecting the NetScreen-10/100 as a Single Security Appliance

Note that if you are configuring multiple NetScreen-10/100 devices, you should install and configure them one at a time. Otherwise, because they all share the same default IP address (192.168.1.1), you might run into IP address conflicts.

To set up the NetScreen-10/100 network connections, follow these steps:

1. Install the NetScreen-10/100 in a rack (optional) or on a level surface.
2. Make sure that the power connection to the NetScreen-10/100 is turned off; that is, that “0” is pressed.
3. Connect the power cable provided in the product package, from the NetScreen-10/100 power outlet to the power supply.
4. Connect the NetScreen-10/100 to the network as shown in one of the examples beginning on page 2-3[1].
5. Turn on the NetScreen-10/100 and any other network devices that you had turned off.
6. If all cables are connected correctly, the link light for each connection glows.

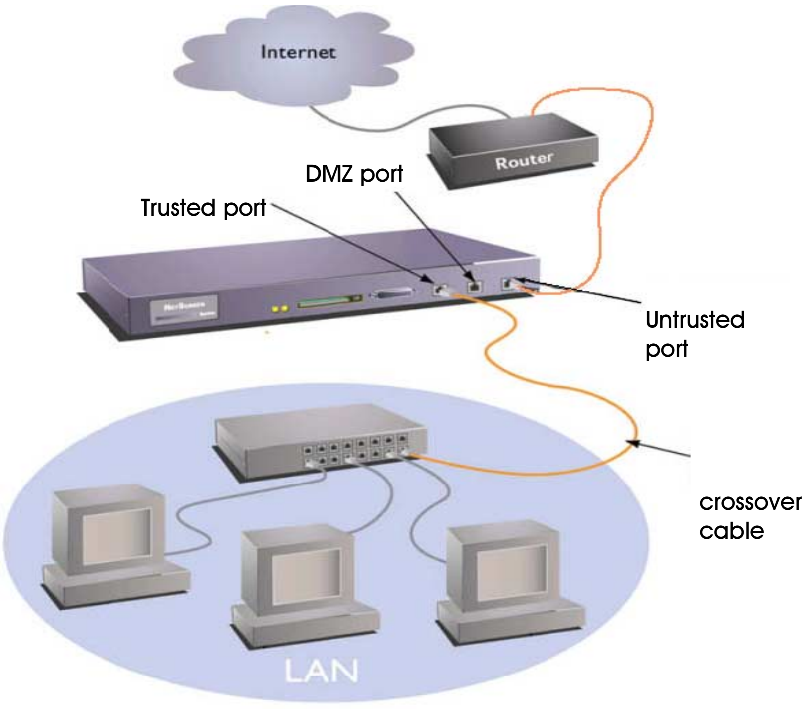


Figure 2-1 Sample Configuration with a Router Connected to the Untrusted Port, Local Area Network (LAN) Connected to the Trusted Port

[1] *Check your router, hub, or computer documentation to determine if you must reconfigure the device or if you must switch off the power supply when connecting new equipment to the LAN.*

To use the DMZ, connect a crossover cable from the DMZ port on the NetScreen-10/100 to the switch linking the machines in the DMZ to the DMZ interface. See Figure 2-2 for an example of this configuration.

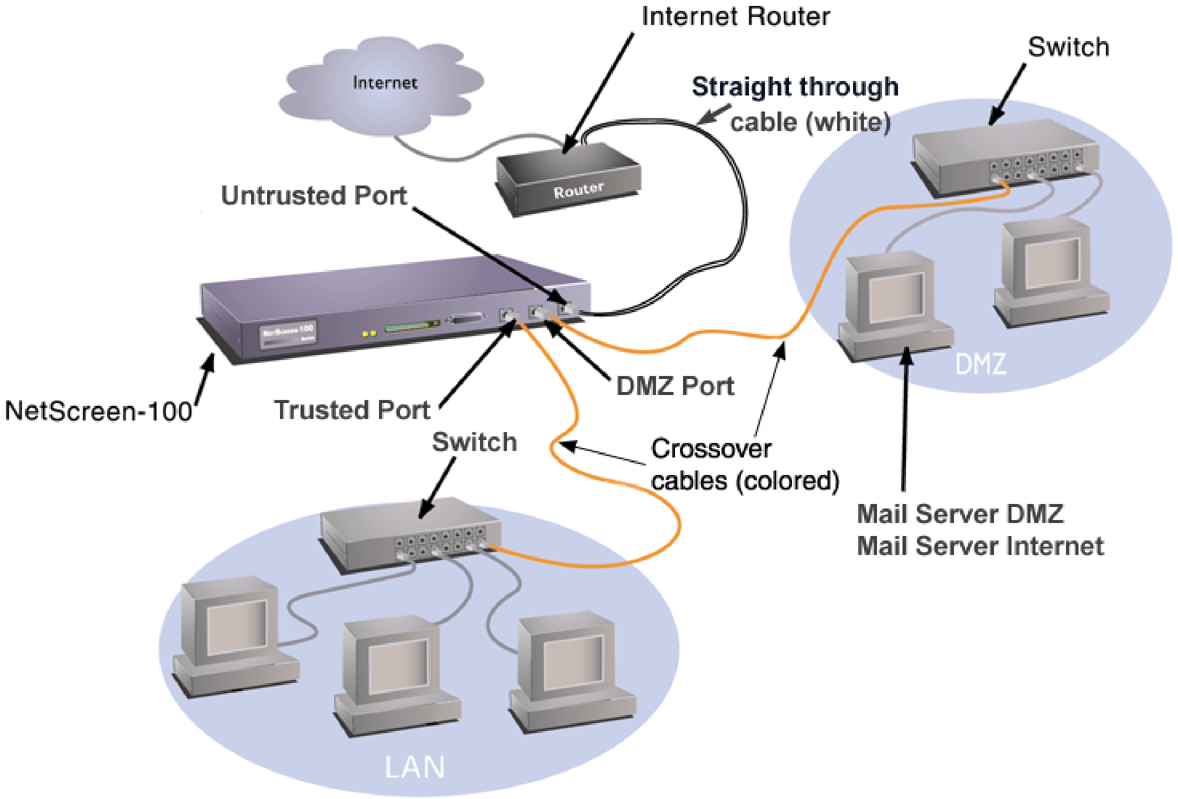


Figure 2-2 Sample Configuration Using DMZ Port

CONNECTING THE NETSCREEN-100 FOR HIGH AVAILABILITY

High Availability (HA) is an option for NetScreen-100 devices that provides protection against device failures in networks with two or more devices. If one unit fails, the second unit can assume its functions with no service or traffic interruption. See “High Availability” in NetScreen *Concepts and Examples Screen OS Reference Guide* for more information.

To implement HA configuration, you need to perform the following steps:

1. Cable the NetScreen-100 units together.
2. Create redundant groups.
3. Specify device priority. (This task is optional).
4. Enter the password(s), if you want to encrypt or authenticate HA communications between members of a redundant group.
5. Set up IP addresses with which the units can perform path monitoring tests. (This task is optional.)
6. Synchronize configurations.

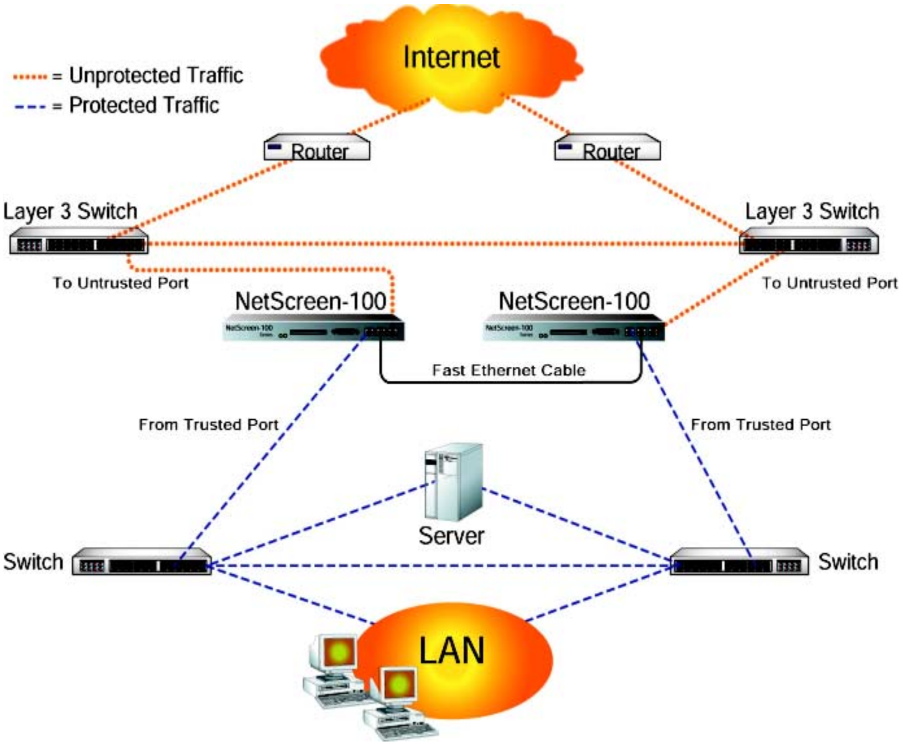


Figure 2-3 Sample HA Configuration (NetScreen-100)

Note: *You may have to supply additional cables, depending on your particular configuration. A DTE (Data Terminal Equipment) device requires a crossover cable to connect to a DTE port. A DCE (Data Communications Equipment) device requires a crossover cable to connect to a DCE port.*

Table 2-1 Typical NetScreen-10/100 Cable Connections.

For a Device Connected to:	Untrusted Port (DTE)*	Trusted Port (DCE)
Workstation (DTE)	crossover	straight-through
Switch/Hub (DCE)	straight-through	crossover
Router§ (DTE)	crossover	straight-through

*An Untrusted Ethernet port is not technically a DTE but for cabling purposes, should be treated as such.

§ Routers with uplink ports may behave in reverse.

If all cables are connected correctly, the link light for each connection glows.

Initial Configuration 3

The NetScreen-10/100 device supports three operational modes: Transparent mode, NAT (Network Address Translation) mode, and Route mode.

Transparent Mode

In Transparent mode, the NetScreen device inspects packets traversing the firewall without modifying any of the source or destination information in the IP packet header. Because it does not translate addresses, the IP addresses on the protected network must be valid, routable addresses on the Untrusted network[1], which might be the Internet. In Transparent mode, the IP addresses for the Trusted and Untrusted interfaces are set at 0.0.0.0, making the presence of the NetScreen device invisible, or “transparent,” to users. The NetScreen device acts as a Layer 2 bridge.

Network Address Translation (NAT) Mode

When in NAT mode, the NetScreen device translates two components in the header of an outgoing IP packet traversing the firewall from the Trusted side: its source IP address and source port number. The NetScreen device replaces the source IP address of the host that sent the packet with the IP address of the Untrusted port[2] of the NetScreen device. Also, it replaces the source port number with another random port number generated by the NetScreen device.

Route Mode

In Route mode, the NetScreen device routes traffic between different interfaces without performing NAT; that is, the source address and port number in the IP packet header remain unchanged as it traverses the NetScreen device. Unlike NAT, the hosts on the Trusted side must have public IP addresses, and you do not need to establish Mapped and Virtual IP addresses to allow sessions initiated on the Untrusted side to reach hosts on the Trusted side. Unlike Transparent mode, the Trusted and Untrusted interfaces are on different subnets.

[1] If the router on the Untrusted side performs NAT, then the addresses on the Trusted side can be private IP addresses.

[2] If the outbound traffic is destined for the DMZ, then the source IP address is translated to that of the DMZ port.

This section shows you how to configure your NetScreen-10/100 in Transparent mode and allow internal users to access the Internet while denying internal access from the Internet. You do this by setting the System IP address and creating an Access Policy that permits outgoing traffic. Incoming traffic is denied by default; therefore, you do not need to set an incoming Access Policy expressly to deny it.

> ***Note:*** *For instructions on configuring the NS-10/100 for NAT or Route mode, see the NetScreen Concepts and Examples ScreenOS Reference Guide.*

There are two methods for configuring the NetScreen-10/100 for the first time: via the Web user interface (WebUI) and via the command line interface (CLI). Table 3-1 “Administration Requirements” lists the workstation requirements for each method.

Table 3-1 Administration Requirements

Configuration Method	**Requirements**
WebUI	Netscape® Communicator® V4.5 or greater, or Microsoft® Internet Explorer V5 Web browser. TCP/IP network connection to the NetScreen-10/100. SSL requires that a certificate be loaded into the NetScreen-10/100. See the *NetScreen Concepts and Examples ScreenOS Reference Guide* for further information.
CLI	Via the console port, using Hilgraeve® Hyperterminal® or a VT100 terminal emulator on the administrator's workstation and an RS-232 Console cable Via Telnet, using TCP/IP network connection to the NetScreen device. SSH requires that a key be generated in the NetScreen-10/100. See the *NetScreen Concepts and Examples ScreenOS Reference Guide* for further information.

The installation procedure using a Web browser is explained first, followed by the CLI procedures using the console port and Telnet.

CONFIGURING VIA THE WEBUI

To perform the initial configuration through the WebUI, you need to change the IP address of the management workstation to the same subnet as the NetScreen-10/100 default system IP address, which is 192.168.1.1. You can then log on through a Web browser and reset the system IP address. The following sections detail the procedures for administration of the NetScreen-10/100 device from the administrator’s workstation.

> ***Note:*** *The NetScreen-10/100 ships from the factory with the IP address set to 192.168.1.1.*

Refer to Table 3-1 for administration requirements.

Making a Connection

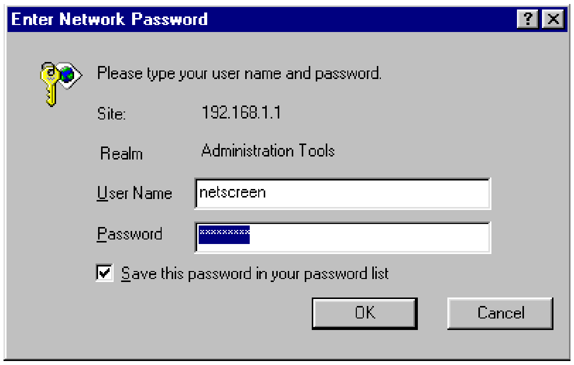
Before you begin, be sure you connected the NetScreen-10/100 hardware to the network as outlined in“Connecting the NetScreen-10/100 to Networks and Devices” on page 2-2.

Logging On and Setting the System IP Address

For remote administration of the NetScreen device over a network connection, you must reconfigure the system IP to be in a reachable subnet. The NetScreen-10/100 ships from the factory with a default IP address of 192.168.1.1. To change this to an address on the same subnet as the other network devices to which the NetScreen-10/100 is connected, perform the following procedure:

1. Record the IP address and subnet mask of your workstation; you must re-enter them later in this process.
2. Change the IP address of the workstation to 192.168.1.2 and the netmask to 255.255.255.0. (You might have to restart the workstation to enable the changes to take effect.) The workstation is now part of the same subnet as the default IP address of the NetScreen-10/100.
3. Start your Web browser.
4. In the URL field of the browser, enter the IP address of the NetScreen-10/100: http://192.168.1.1.

   The Enter Network Password dialog box appears, as shown in Figure 3-1.



Please type your user name and password.

Site: 192.168.1.1

Realm Administration Tools

User Name netscreen

Password *********

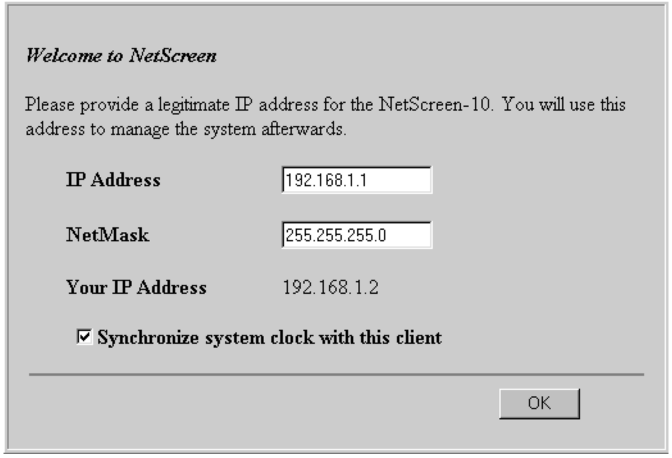
☑ Save this password in your password list

Figure 3-1 Enter Network Password Dialog Box

5. In the dialog box, type **netscreen** for both the user name and password, and then click **OK**.

Note: *The user name and password are case-sensitive. After configuring the NetScreen device for the first time, you should change the default user name and password as described in "Changing the Administrator Login Name and Password" on page 3-18.*

For a first-time configuration, you are directed to a special setup page as shown in Figure 3-2.



Welcome to NetScreen

Please provide a legitimate IP address for the NetScreen-10. You will use this address to manage the system afterwards.

IP Address 192.168.1.1

NetMask 255.255.255.0

Your IP Address 192.168.1.2

☑ **Synchronize system clock with this client**

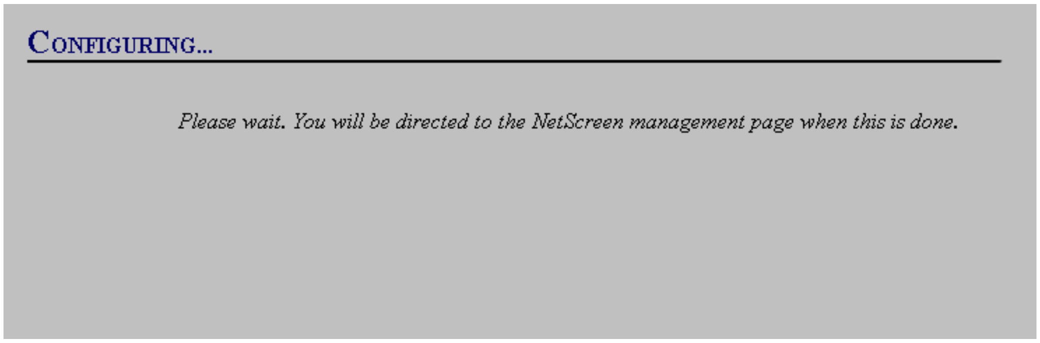
Figure 3-2 Initial IP Address Configuration

6. Enter the IP address and netmask for administration of the NetScreen-10/100, and then click **OK**.

Note: *Select the* ***Synchronize system clock with this client*** *checkbox to synchronize the NetScreen-10/100 clock with the clock in the administrator's workstation.*

The IP address must be a valid and available IP address on your local network and the subnet mask must be an appropriate value for your local network.

The Configuring in Progress screen appears, as shown in Figure 3-3 "Configuring in Progress Screen" on page 3-5.



CONFIGURING...

Please wait. You will be directed to the NetScreen management page when this is done.

Figure 3-3 Configuring in Progress Screen

7. Reconfigure your administration workstation IP address and netmask back to the values you recorded in step 1. Depending on the operating system, you might have to restart your workstation.

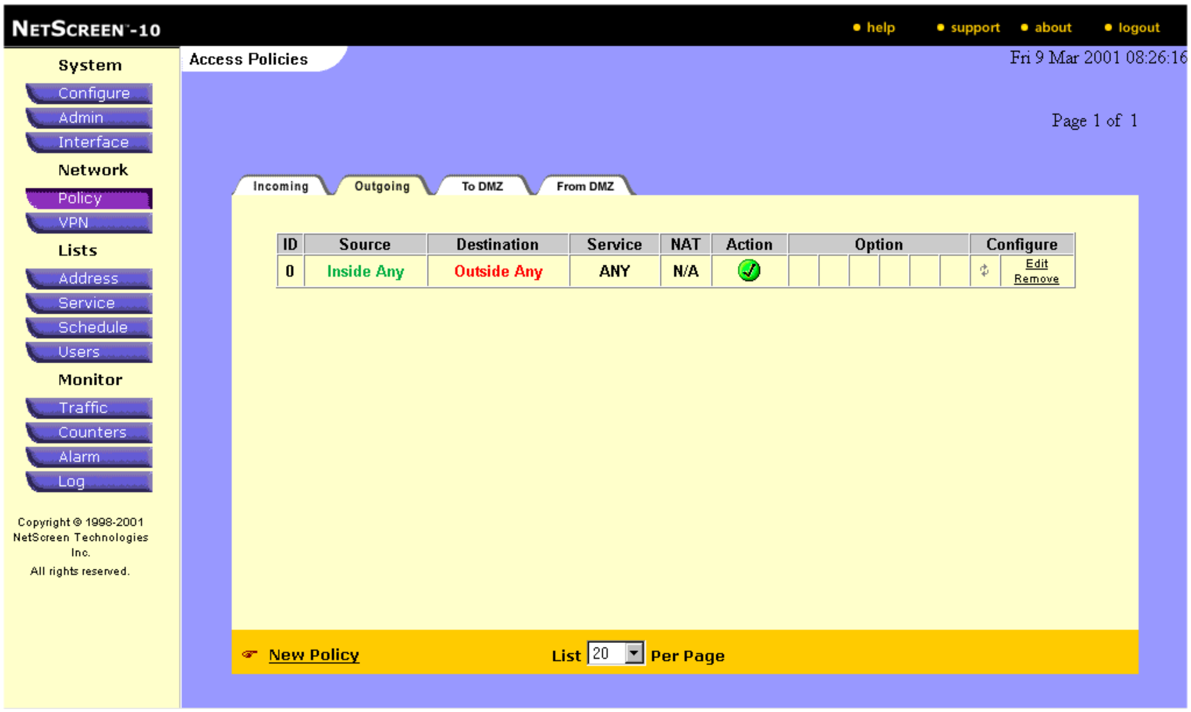
   After the IP configuration is complete, you must again log on.

8. In the URL field of the browser, enter the new IP address for the NetScreen device.

   The Enter Network Password dialog box re-appears.

9. In the dialog box, type **netscreen** for both the user name and password, and then click **OK**. (Remember that the user name and password are case-sensitive.)

   The Access Policies pages appear, with the Outgoing Access Policies page displayed, as shown in Figure 3-4 "Access Policies Page" on page 3-6. You are now logged on to the NetScreen-10/100.



Access Policies

Fri 9 Mar 2001 08:26:16

Page 1 of 1

ID	Source	Destination	Service	NAT	Action	Option	Configure
0	Inside Any	Outside Any	ANY	N/A	✓		Edit Remove

Figure 3-4 Access Policies Page

Setting Interface Addresses

The NetScreen-10/100 has a Trusted interface, an Untrusted interface and a DMZ interface. These are physical interfaces used for channeling network user traffic.

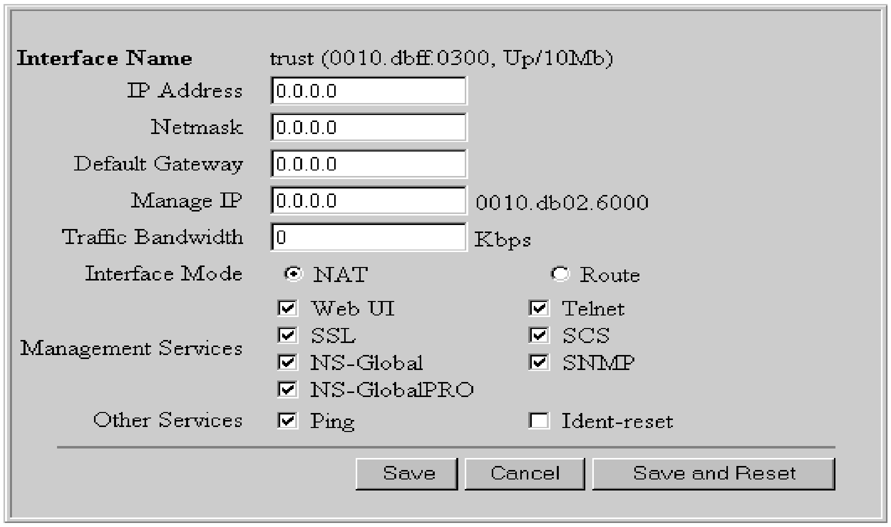
The Trusted interface leads to the network (usually the intranet or corporate network) protected by the NetScreen device. The Untrusted interface leads to the network (usually the Internet) against which the NetScreen device defends. The DMZ interface leads to a protected network to which access from the Untrusted side is typically granted.

Trusted Interface Configuration

1. Click the **Interface** button in the menu column.

   The Interface pages appear, with the Trusted Interface page displayed.

2. Click **Edit** to open the Trusted Interface Configuration dialog box.



Interface Name trust (0010.dbff.0300, Up/10Mb)

IP Address 0.0.0.0

Netmask 0.0.0.0

Default Gateway 0.0.0.0

Manage IP 0.0.0.0 0010.db02.6000

Traffic Bandwidth 0 Kbps

Interface Mode ● NAT ○ Route

Management Services ☑ Web UI ☑ Telnet ☑ SSL ☑ SCS ☑ NS-Global ☑ SNMP ☑ NS-GlobalPRO

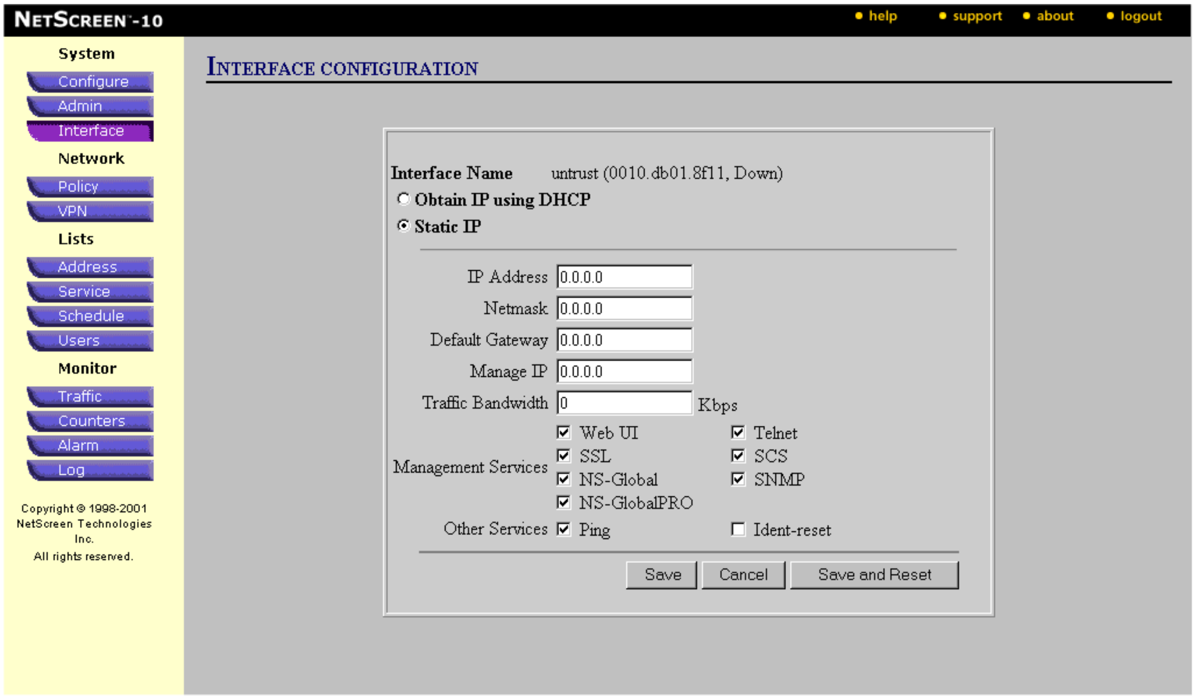
Other Services ☑ Ping □ Ident-reset

Figure 3-5 Trusted Interface Configuration

3. Enter the following, and then click **Save**:
   - IP Address: Type an IP address for the Trusted interface.
   - Netmask: Type an appropriate netmask.
   - Default Gateway: Type the IP address of the router—if there is one—that exists between the Trusted network and the NetScreen-10/100.
4. Select either **NAT Mode** or **Route Mode**, and then click **Save**.

Untrusted Interface Configuration

1. Click the Untrusted tab, and then Edit to open the Untrusted Interface Configuration dialog box.



Interface Name untrust (0010.db01.8f11, Down)

○ Obtain IP using DHCP

● Static IP

IP Address	0.0.0.0		
Netmask	0.0.0.0		
Default Gateway	0.0.0.0		
Manage IP	0.0.0.0		
Traffic Bandwidth	0 Kbps		
Management Services	☑ Web UI	☑ Telnet	
	☑ SSL	☑ SCS	
	☑ NS-Global	☑ SNMP	
	☑ NS-GlobalPRO		
Other Services	☑ Ping	□ Ident-reset	

Figure 3-6 Untrusted Interface Configuration

2. For the Untrusted Interface Configuration, select one of the following and click **Save and Reset**:

Note: *The NetScreen-100 does not provide DHCP, and uses Static IP as its default.*

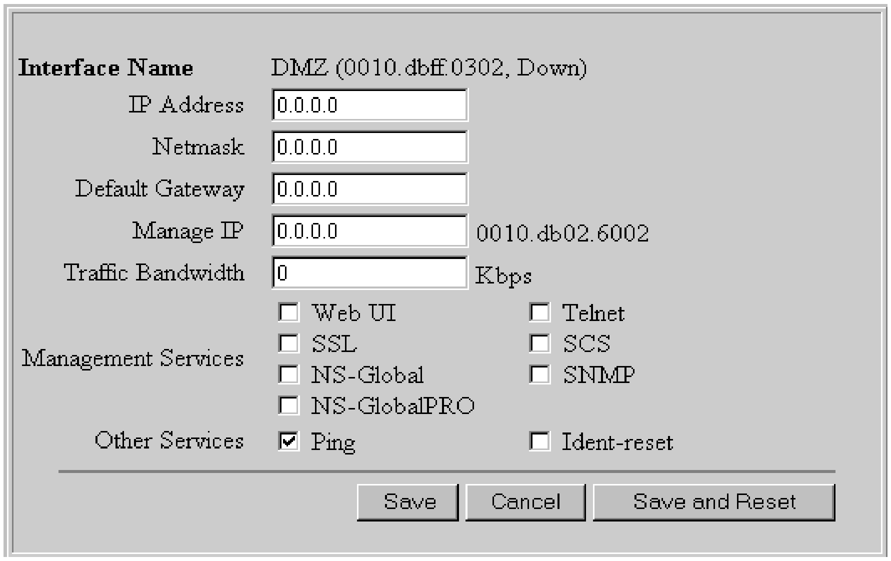
Obtain IP using DHCP (Dynamic Host Control Protocol) (NetScreen-10 only)

Static IP, and enter the following (NetScreen-10 only):

- IP Address: Enter the Untrusted IP address.
- Netmask: Enter the netmask IP address.
- Default Gateway: Enter the IP address of the external router.

DMZ Interface Configuration

1. If you plan to use the DMZ interface to add another security domain, click the DMZ tab, and then Edit to open the DMZ Interface Configuration dialog box.



Interface Name DMZ (0010.dbff.0302, Down)

IP Address 0.0.0.0

Netmask 0.0.0.0

Default Gateway 0.0.0.0

Manage IP 0.0.0.0 0010.db02.6002

Traffic Bandwidth 0 Kbps

Management Services □ Web UI □ Telnet □ SSL □ SCS □ NS-Global □ SNMP □ NS-GlobalPRO

Other Services ☑ Ping □ Ident-reset

Figure 3-7 DMZ Interface Configuration

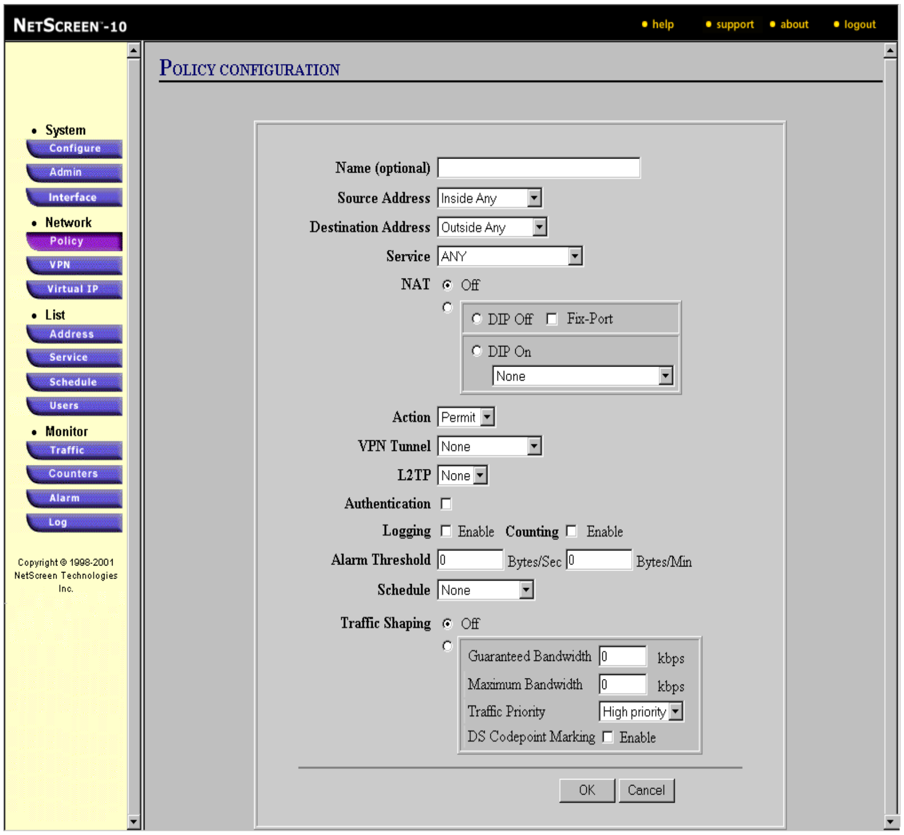
2. Enter the following, and then click **Save and Reset**:
   - IP Address: Type an IP address within the same subnet as the DMZ network.
   - Netmask: Type an appropriate netmask.
   - Default Gateway: Type the IP address of the router—if there is one—that exists between the DMZ network and the NetScreen-100.

Allowing Outbound Traffic

By default, the NetScreen-10/100 does not allow inbound or outbound traffic. You need to create an outgoing Access Policy to permit outbound traffic to traverse the firewall.

1. On the Outgoing Access Policies page, click the **New Policy** link in the lower left corner of the page.

The Policy Configuration dialog box appears, as shown in Figure 3-8.



POLICY CONFIGURATION

Name (optional)

Source Address: Inside Any

Destination Address: Outside Any

Service: ANY

NAT ● Off
○
○ DIP Off □ Fix-Port
○ DIP On
None

Action: Permit

VPN Tunnel: None

L2TP: None

Authentication □

Logging □ Enable Counting □ Enable

Alarm Threshold 0 Bytes/Sec 0 Bytes/Min

Schedule: None

Traffic Shaping ● Off
○
Guaranteed Bandwidth 0 kbps
Maximum Bandwidth 0 kbps
Traffic Priority: High priority
DS Codepoint Marking □ Enable

Figure 3-8 Policy Configuration Dialog Box

2. Set an Access Policy that allows all inside hosts to access the Internet. Set the options as follows:
   - **Source Address:** Inside Any (Inside Any is a predefined address for all hosts on the Trusted network.)
   - **Destination Address:** Outside Any (Outside Any is a predefined address for all locations on the Untrusted network, usually the Internet.)
   - **Service:** Any (Any is a predefined value for any IP service.)
   - **Action:** Permit (Allows the traffic defined by the Access Policy to traverse the firewall.)
   - Leave the rest of the options at their default values, and click the **OK** button.

The Outgoing Access Policies page now has one Access Policy that permits any inside traffic to pass through the firewall and access the Internet.

If you want to configure the NetScreen device for Transparent mode, you do not have to define IP addresses for the Trusted, Untrusted and DMZ interfaces. Initial configuration is complete.

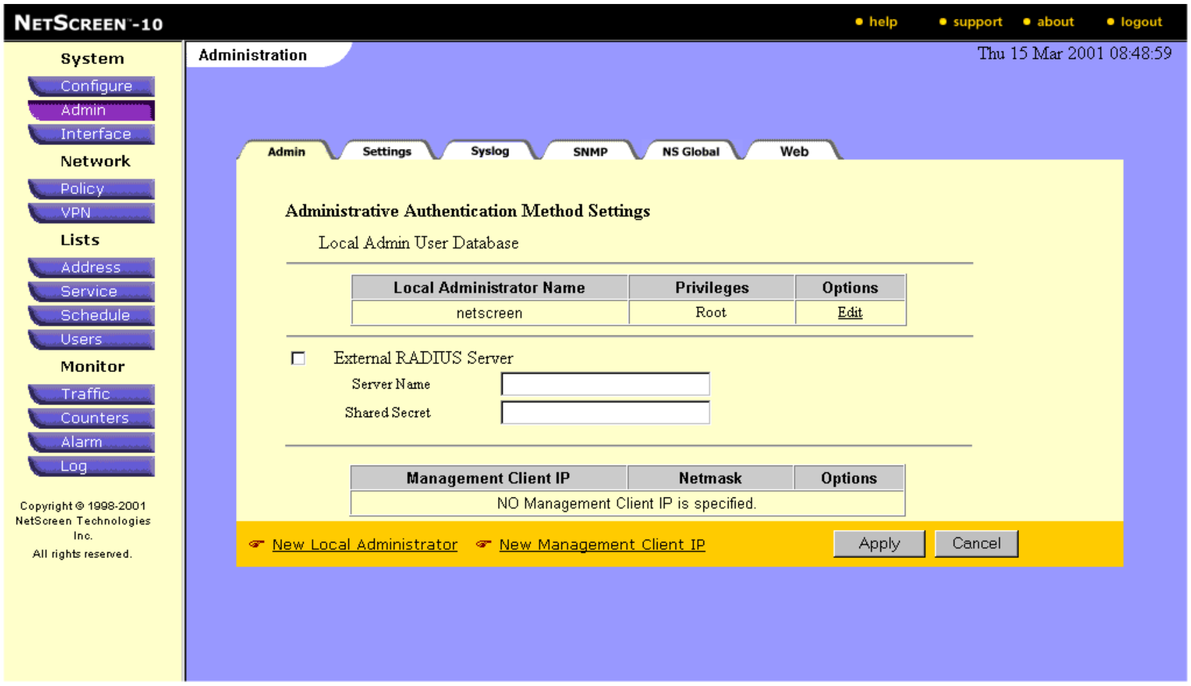
To configure the NetScreen-10/100 device for Network Address Translation (NAT) mode or Route mode, you must configure the Trusted, Untrusted and DMZ (if used) interfaces.

> ***Note:*** *For further information and examples on other configuration options, please refer to the* NetScreen Concepts & Examples ScreenOS Reference Guide.

Changing the Administrator Login Name and Password

To change the default administrator login and password via the WebUI:

1. Select the **Admin** button in the menu column to view the **Admin** page, as shown in Figure 3-9.



Administration

Thu 15 Mar 2001 08:48:59

Administrative Authentication Method Settings

Local Admin User Database

Local Administrator Name	Privileges	Options
netscreen	Root	Edit

☐ External RADIUS Server

Server Name

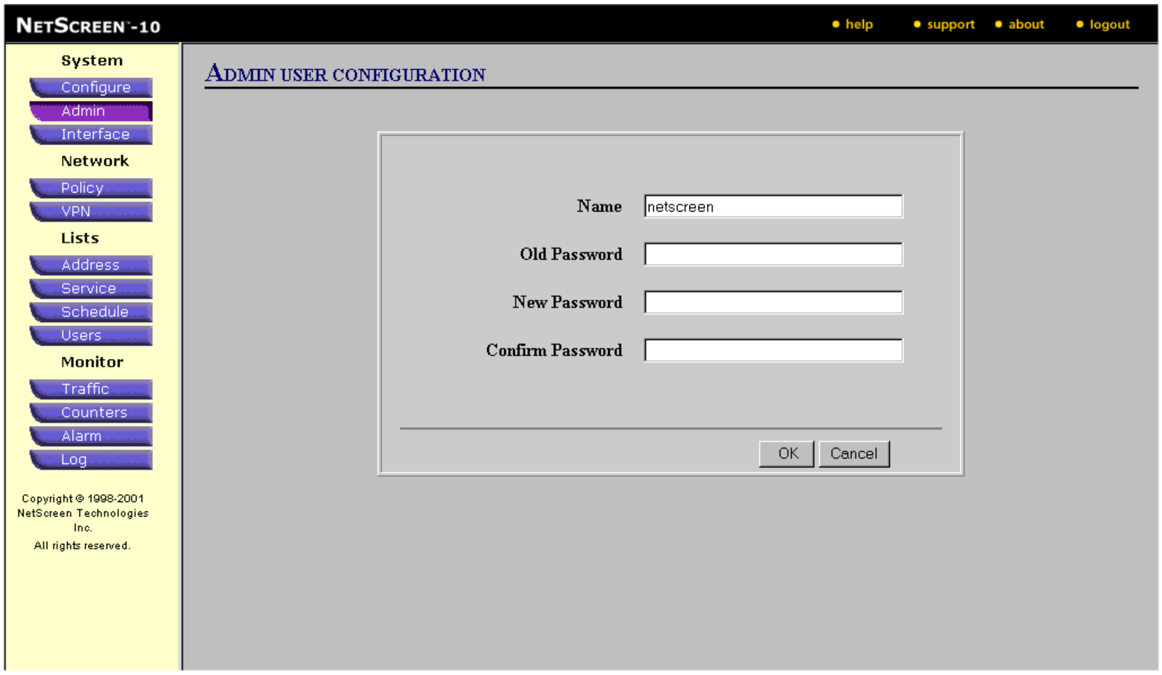
Shared Secret

Management Client IP	Netmask	Options
NO Management Client IP is specified.		

Figure 3-9 The Administration Settings Page

2. On the Local Administrator Name Click **Edit** under **Options**.

   The Admin User Configuration Menu appears, as in Figure 3-10.



Name: netscreen

Old Password:

New Password:

Confirm Password:

Figure 3-10 Admin User Configuration Menu

3. Type a new Admin Login Name.

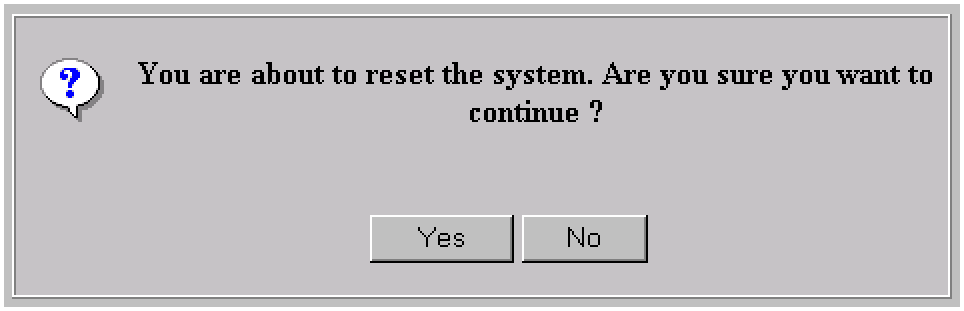
Note: *The login name and password must be alphanumeric. The login username and password are case-sensitive.*

4. Type the old password (initially *netscreen*) in the Old Password field. You must enter the old password to change to the new password.
5. Type the new password in the New Password field and the Confirm New Password field.
6. Record the new Administrator Login Name and Password in a secure manner.

Warning *Make sure that you remember your password! If you forget it, you will have to return the unit to the factory for initialization. This feature has been implemented in this manner as an extra security measure.*

7. Leave the other fields at their default entries, and select the **Apply** button.

   The changes require the NetScreen-10/100 to reset, which it automatically does at this point. Figure 3-11 shows the system message that appears.



You are about to reset the system. Are you sure you want to continue ?

Figure 3-11 System Message Display

8. Click the **Yes** button to confirm your command to reset the system.

   The next time you log in, use the new login name and password.

Note: *To receive important news on product updates, please visit our web site at www.netscreen.com and register your product.*

Testing the Configuration

Use a Web browser to access an external Web site (for example, www.netscreen.com). You should be able to locate the site and access the available Web pages.

If you cannot access the Web site, check the following:

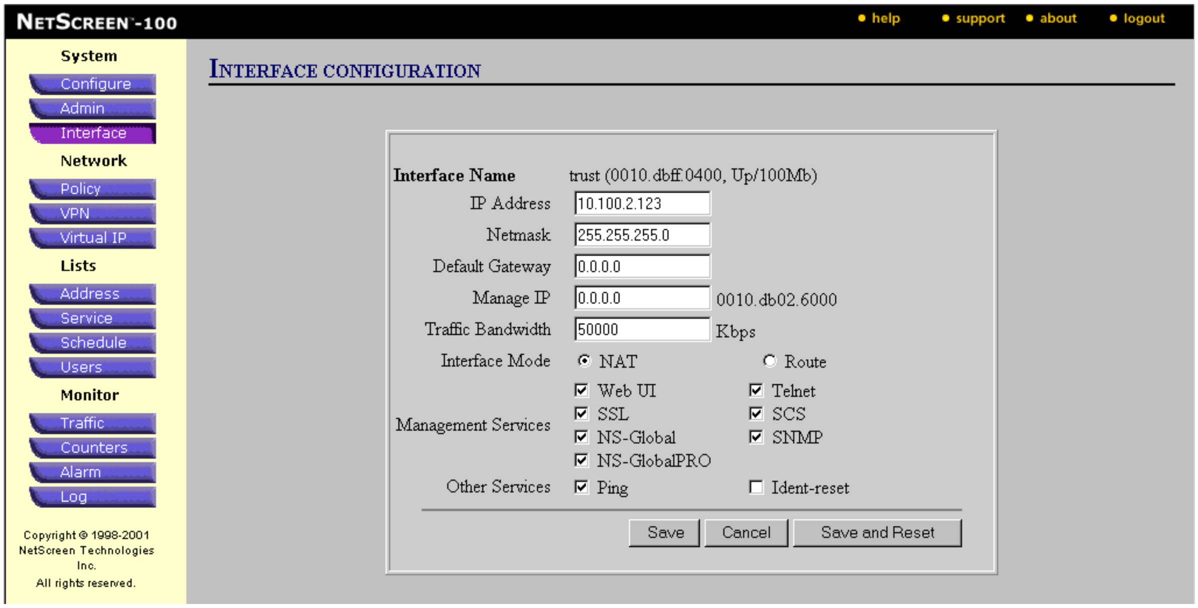
- Link lights on the NetScreen-10/100, workstations, hubs, and the router are glowing.
- The workstation IP and Netmask have the correct settings.
- The workstation gateway points to the router.
- The workstation has a valid DNS entry.

Configuring High Availability via the WebUI

Before you can configure two NetScreen-100 devices in a redundant group for high availability (HA), you must cable them together. Then you must assign one device as the master unit and one as the slave. The master performs all the firewall, VPN, and traffic management functions, while the slave waits to take over should the master unit fail. The master sends configuration and session state information to the slave over the HA link, so that the slave can instantly assume master status during a failover without interrupting service. The NetScreen-100 also has a second HA link to provide a backup should the primary HA link fail.

To activate HA communications between two NetScreen-100 devices that are already cabled for HA, you must assign both to the same redundant group and assign each device a priority number, used to define the master and slave status. Also, if you are managing the devices through any interface other than the MGT interface, it is important that you set the manage IP address on that interface so that you can manage the slave unit if necessary[1].

1. To configure the Master Unit, in the Interface menu, select Trusted, Untrusted, or Mgt and then Edit. The menu appears, as in Figure 3-12 on page 14:



INTERFACE CONFIGURATION

Interface Name	trust (0010.dbff.0400, Up/100Mb)	
IP Address	10.100.2.123	
Netmask	255.255.255.0	
Default Gateway	0.0.0.0	
Manage IP	0.0.0.0	0010.db02.6000
Traffic Bandwidth	50000	Kbps
Interface Mode	● NAT	○ Route
Management Services	☑ Web UI	☑ Telnet
	☑ SSL	☑ SCS
	☑ NS-Global	☑ SNMP
	☑ NS-GlobalPRO	
Other Services	☑ Ping	□ Ident-reset

Figure 3-12 Master Unit Interface Configuration

2. In the Manage IP field, enter an IP address in the same subnet as that of the physical interface, and then click **Save.**

[1] Some HA features are configurable only through the CLI. To set the link-up state of the slave unit and save the configuration from the master unit to the slave, refer to the CLI section.

3. To configure the Slave Unit, in the Admin Menu, select HA.
4. Enter the following, and then click **Apply**:

   Group ID: Enter a number to identify this device as a member of a specific redundant group.

   Priority: Enter a number between 1 and 65,535. The device with the number closest to 1 is the master. (A value of 0 disables HA and shuts down the HA ports.)

Configuring Via the CLI

The following section provides information on how to configure the device using the command line interface (CLI). For more information regarding command syntax, see “Command Line Interface (CLI) Syntax” on page -ix.

Making a Connection

You can access the NetScreen-10/100 either by connecting directly via a console (or serial) cable to the NetScreen-10/100 console port, or you can make a network connection via Telnet. Connection instructions are offered for both methods.

Connecting via the Console Port

You need direct access to the NetScreen device you want to configure and the following items before you start:

- An RS-232 male-to-female serial cable
- Hilgreave Hyperterminal software on the management workstation (or, if you are using a different operating system, a VT100 terminal emulator)

Follow these steps to connect the NetScreen device to the workstation:

1. Connect the serial cable from the management workstation to the console port on the NetScreen-10/100.
2. Start the terminal emulator on the workstation.
3. To create a new connection, type a name, select an icon, and then click **OK**.

   The Connect To dialog box appears.

4. Select the serial port to which the serial cable is connected to the workstation (usually COM1 or COM2), and click **OK**.

   The COM1 (or COM2) Properties dialog box appears.

5. Configure the port settings as follows, and then click **OK**:
   - Serial communications 9600 bps
   - 8 bit
   - no parity
   - 1 stop bit
   - no flow control
6. Press the **ENTER** key to see the login prompt.

Connecting via Telnet

Telnet operates over TCP/IP networks. It allows you to configure the device remotely using the CLI.

Using Telnet to manage NetScreen devices requires the following:

- Telnet software on the administrative workstation
- An Ethernet connection to the NetScreen device

Before you begin, be sure you connected the NetScreen device hardware to the network as outlined in "Connecting the NetScreen-10/100 as a Single Security Appliance" on page 2-1.

1. Establish a Telnet connection to the NetScreen device.
2. For Host name, type: 192.168.1.1, the NetScreen-100 default IP address.

> ***Note:*** *The Terminal type for Telnet sessions must be vt100. Click on* ***Connect****, and on the drop-down menu select* ***Remote System****. In the dialog box, select* ***vt100*** *from the Term Type menu.*

For more specific information, see the *NetScreen CLI Manual* and the *NetScreen Concepts and Examples Manual*.

Logging On and Setting the System IP Address

To log on, enter the default administrator login name and password.

1. At the login prompt, enter **`netscreen.`**
2. At the password prompt, enter **`netscreen.`**

> ***Note:*** *The user name and password are case-sensitive.*

To administer the NetScreen device over a network connection, you must change the system IP address. The NetScreen-10/100 ships from the factory with a default IP address of 192.168.1.1. To change this to an address on the same subnet as the other network devices to which the NetScreen-10/100 is connected, enter the following command, substituting your system IP address for the letters:

```
ns-> set admin sys-ip <a.b.c.d>
```

Setting Interface Addresses

The NetScreen-10/100 ships with all its interface addresses and netmasks set as 0.0.0.0. If you want to operate the NetScreen-10/100 in Transparent mode, leave the trusted and untrusted interface addresses as they are.

To set the interface addresses, enter the following commands, where <a.b.c.d> are the interface IP addresses and <A.B.C.D> is the netmask:

```
1. set interface trust ip <a.b.c.d> <A.B.C.D>
2. set interface untrust ip <a.b.c.d> <A.B.C.D>
3. save
```

Allowing Outbound Traffic

By default, the NetScreen-10/100 does not allow inbound or outbound traffic. You need to create an outgoing Access Policy to permit outbound traffic to traverse the firewall. Enter the following command:

```
ns-> set policy outgoing “inside any” “outside any” any permit
```

Changing the Administrator Login Name and Password

Because all NetScreen units come with the same default name and password, it is highly recommended that you change the default Admin Login name and Password.

> ***Note:*** *The information in this guide has been widely published, and failure to change the defaults can expose your system to attack.*

1. Enter the following commands:

   ```
   ns-> set admin name <name>
   ns-> set admin password <password>
   ns-> save
   ```

2. Record the new Administration name and Password in a secure manner.

⚠ **Warning** *Make sure that you remember your password! If you forget it, you will have to return the unit to the factory for initialization. This feature has been implemented in this manner as an extra security measure.*

If you want to configure the NetScreen device for Transparent mode, you do not have to define IP addresses for the Trusted, Untrusted and DMZ interfaces. Initial configuration is complete.

To configure the NetScreen-10/100 device for Network Address Translation (NAT) mode or Route mode, see the *NetScreen Concepts & Examples ScreenOS Reference Guide*.

Testing the Configuration

From a workstation on the Trusted side of the NetScreen-10/100, use a Web browser to access an external Web site (for example, www.netscreen.com). You should be able to locate the site and access the available Web pages.

If you cannot access the Web site, check the following:

- The power, status, and link lights on NetScreen-10/100 are illuminated.
- The LEDs on the host, hubs, and router(s) are illuminated.
- The administrator’s workstation IP address and netmask are correct.
- The workstation gateway points to the external router.
- The workstation has a valid Domain Name Service (DNS) entry.

Configuring High Availability via the CLI

To activate HA communications between two NetScreen100 devices that are already cabled for HA, you must assign both to the same redundant group and assign each device a priority number, used to define the master and slave status. Also, it is important that you set the manage IP address on that interface so that you can manage the slave unit if necessary.

Master Unit

1. set interface { trust | untrust | dmz } manage-ip <a.b.c.d>
2. set ha group <number>
3. set ha priority <number>
4. set ha link-up-on-slave

Slave Unit

1. set interface {trust | untrust | dmz} manage-ip <a.b.c.d>
2. set ha group <same_number_as_master>
3. set ha priority <larger_number_than_master>
4. save config ha-master
5. reset

   Configuration modified, save? y/]/[n] (Type **n**.)

   System reset, are you sure? y/[n] (Type **y**.)

Safety Recommendations and Warnings

A

Before supplying power to the NetScreen-10/100, follow these safety guidelines:

- Look carefully for possible hazards in the work area, such as moist floors, ungrounded power extension cables, and missing safety grounds.
- Locate the emergency power-off switch for the area where you are working.

Do not perform any action that creates a potential hazard to people or makes the equipment unsafe. To allow adequate air circulation and to avoid the devices tipping over, do not stack or balance the equipment on other devices. Make sure the installation is securely in place.

SAFETY WARNINGS

Make sure that you adhere to the following set of safety warnings.

Installation Warning

⚠ **Caution** *Read the cabling instructions before connecting the NetScreen-10/100 to its power source.*

Power Disconnection Warning

⚠ **Warning** *Before working on a device that has an On/Off switch, turn OFF the power and unplug the power cord.*

No User-Serviceable Parts Warning

⚠ **Warning** *The NetScreen-10/100 contains no user-serviceable parts and is housed in a tamper-proof enclosure. Therefore, the chassis should never be opened under any circumstances. Doing so will also void the warranty.*

Circuit Breaker (15A) Warning

⚠ **Caution** *The NetScreen-10/100 relies on the building's installation for short-circuit (over-current) protection. Ensure that a fuse or circuit breaker no larger than 120 VAC, 15A U.S. (240 VAC, 10A international) is used on the phase conductor (all current-carrying conductors).*

SELV Circuit Warning

⚠ **Warning** *The Ethernet 10BaseT, 100BaseT, serial, console, and auxiliary ports contain safety extra-low voltage (SELV) circuits. Do not connect the NetScreen-10/100 to a telephone line or any Telco line (e.g., T-1, T-3, RJ-48 lines).*

Lightning Activity Warning

⚠ **Danger** *Do not work on the device, specifically, connecting or disconnecting cables during periods of lightning activity, as the unit can function as a conduit.*

Lithium Battery Warning

⚠ **Warning** *There is a danger of explosion if the battery is incorrectly replaced. The chassis should never be opened under any circumstances. Doing so will also void the warranty. Return the device to the manufacturer for battery replacement.*

Product Disposal Warning

⚠ **Warning** *Ultimate disposal of this product should be handled according to all national laws and regulations.*

GENERAL SITE REQUIREMENTS

For the safe installation and operation of your NetScreen device, ensure that your site is properly prepared before beginning the hardware installation.

- Check the power at your site to ensure that you are receiving “clean” power (free of spikes and noise). Install a power conditioner if necessary.
- The NetScreen device is intended for use in a normal office environment. For more extreme conditions, verify that temperature, humidity, and power conditions meet the specifications indicated below.

Item	**Operating Specification**
Temperature	32-122°F, 0- 50°C: for storage 50-104°F, 10-40°C: for operation
Relative Humidity	5-90%, non-condensing: for storage 10-90%, non-condensing: for operation
Nominal Voltage Voltage Range	120 +/-15%, 220 +/-15% 102-253 Auto Sensing
Input frequency	47-63 Hz
AC input current	1A (120VAC), 0.5A (220VAC)
Altitude	0-12,000 feet, 0-3,660 meters

Onsite Precautions

You can place the NetScreen-10/100 on a desktop or mounted in a rack. The location of the chassis and the layout of your equipment rack or wiring room are extremely important for proper system operation. Equipment placed too close together will cause inadequate ventilation, besides rendering areas of the device inaccessible for system maintenance during any system malfunctions and shutdowns.

When planning your site layout and equipment locations, follow the precautions described below to help avoid equipment failures and reduce the possibility of environmentally caused shutdowns. If you are experiencing shutdowns or unusually high errors with your existing equipment, these precautions may help you isolate the cause of the failures and prevent future problems.

- Electrical equipment generates heat. Natural air temperature might not be sufficient to cool equipment to acceptable operating temperatures without an additional circulation system. Ensure that the room in which you operate your system has adequate air circulation.
- Do not work alone if potentially hazardous conditions exist.
- Never assume that the power supply has been disconnected from a circuit. Always check.

Look carefully for possible hazards in your work area, such as moist floors, ungrounded power extension cables, frayed power cords, and missing safety grounds.

Equipment Rack Mounting Guidelines

The following information will help you plan an acceptable equipment rack configuration.

- Enclosed racks must have adequate ventilation. Ensure that the rack is not overly congested because each unit generates heat. An enclosed rack should have louvered sides and a fan to provide cooling air.
- When mounting a chassis in an open rack, ensure that the rack frame does not block the intake or the exhaust ports. If the chassis is installed on slides, check the position of the chassis when it is seated all the way into the rack.
- In an enclosed rack with a ventilation fan in the top, excessive heat generated by equipment near the bottom of the rack can be drawn upward and into the intake ports of the equipment above it in the rack. Ensure that you provide adequate ventilation for equipment at the bottom of the rack.
- Baffles can help to isolate exhaust air from intake air, which also helps to draw cooling air through the chassis. The best placement of the baffles depends on the airflow patterns in the rack, which can be found by experimenting with different arrangements.

COMPLIANCE SPECIFICATIONS

Parameter	**Specification**
Safety Certification	UL, CUL
EMI/RFI	FCC Part 15, Class A
Standards Compliance	IEEE 802.3, Ethernet IPSec Compliance: RFC 2401 (Security Architecture for the Internet Protocol) RFC 2402 (IP Authentication Header) RFC 2403 (The Use of HMAC-MD5-96 within ESP and AH) RFC 2404 (The Use of HMAC-SHA-1-96 within ESP and AH) RFC 2405 (The ESP DES-CBC Cipher Algorithm With Explicit IV) RFC 2406 (IP Encapsulating Payload) RFC 2409 (The Internet Key Exchange, IKE) RFC 2410 (The NULL Encryption Algorithm and Its Use With IPSec) RFC 1851 (The ESP–Triple DES Transform)

DC Power Supply

B

The NetScreen-10/100 can come equipped with a -48V DC power supply which can operate on one or two DC feeds ranging from -36V to -72V. If two feeds are used, they share the load. If one feed fails, the other automatically assumes the full load.

The figure below shows the DC terminal block, with two -48V DC feeds connected. The NetScreen-10/100 can operate on either one feed alone or with two feeds in use. The block is located on the back of the chassis.

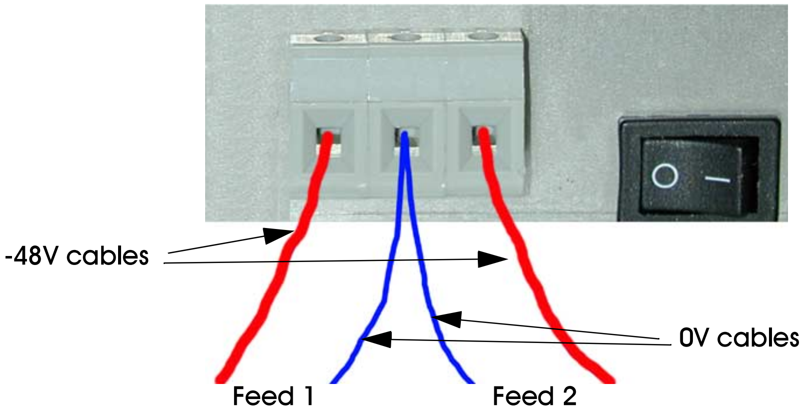


Figure: DC Power Supply Cabling

Connecting to DC Power Supply Cables

⚠ **Warning** *You must shut off all current to the DC feed wires before connecting the power supply.*

To connect two feeds to the DC power supply, do the following:

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

Index