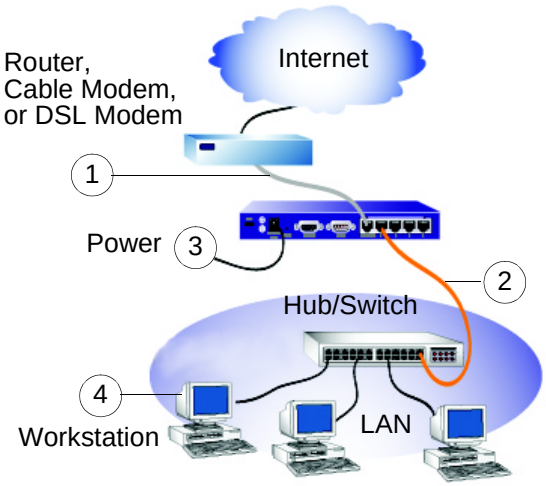
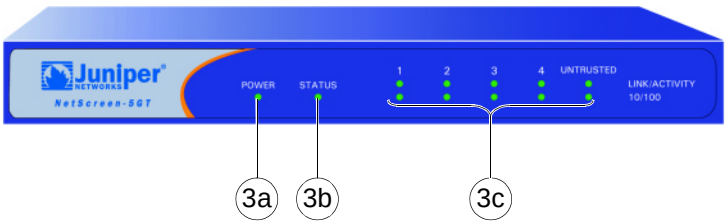
Juniper Networks NetScreen-5GT

Getting Started

Use the instructions in this guide to help you connect and configure your NetScreen-5GT. For more configuration examples and details, see the *NetScreen-5GT User's Guide* and the *NetScreen Concepts & Examples ScreenOS Reference Guide*.



The numbers in the diagram are paired with the steps below.



CONNECTING THE DEVICE

Using the instructions below, connect the NetScreen-5GT and prepare to configure it to protect your network. Use the LEDs on the front panel of the device to help you determine its status.

Step 1

Connect an Ethernet cable from the Untrusted port of the NetScreen-5GT to the external router, cable modem, or DSL modem.

Step 2

- If the workstation is in a LAN (see diagram), connect an Ethernet cable from the Trusted port to the internal switch or hub.
- If the workstation is a single workstation, connect an Ethernet cable from the Trusted port directly to the Ethernet port on the workstation.

Step 3

Connect the power cable between the NetScreen-5GT and a power source. Juniper Networks recommends using a surge protector.

a. Ensure that the Power LED glows green. This indicates the device is receiving power.

b. After the device starts (about 30 seconds), ensure that the Status LED blinks green. This indicates the device is operating normally.

c. Ensure that the Link Activity LEDs glow green for the connected interfaces. This indicates the device has network connectivity.

Step 4

Configure the workstation to access the NetScreen-5GT via a Web browser:

a. Ensure that your workstation is properly connected to your LAN (see diagram).

b. Change the TCP/IP settings of your workstation to obtain its IP address automatically from the NetScreen-5GT via DHCP. For help, see the operating system documentation for your workstation.

Note: *Ensure that your internal network does not already have a DHCP server.*

c. If necessary, restart your workstation to enable the changes to take effect.

CONFIGURING THE DEVICE

Use the Initial Configuration Wizard to configure the NetScreen-5GT. Before starting the Wizard, decide how you want to deploy your device. (For additional information, see the *NetScreen-5GT User's Guide*.)

Operational Mode. You can deploy the NetScreen-5GT in Route mode with NAT enabled on the Trust zone interface or in Route mode without NAT. When using Route mode with NAT enabled, the NetScreen-5GT replaces the source IP address of the sending host with the IP address of the Untrusted port of the NetScreen-5GT. Route mode with NAT is the most common way to configure the Trust zone interface on the NetScreen-5GT. Your network uses the Untrust zone interface to connect to the Internet. This interface can have a static IP address or a dynamic IP address assigned via DHCP or PPPoE. When using Route mode without NAT, an interface routes traffic without changing the source address and port number in the IP packet header. You must assign public IP addresses to hosts connected to non-NAT interfaces. Your network uses the Untrust zone interface to connect to the Internet. To configure this interface, you need the IP address of the interface that is connected to the external router, cable modem, or DSL modem and the IP address of the router port connected to the NetScreen-5GT.

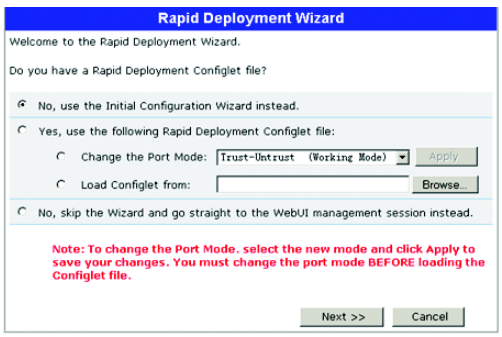
Port Mode. Port modes allow the interfaces to be reconfigured and binds them to zones. The default port mode, Trust-Untrust, binds the Trust interface to the Trust zone and the Untrust interface to the Untrust zone.

Trust Zone Interface IP Address. The default IP address and netmask for the Trust zone interface is 192.168.1.1/24. You can change this address to match IP addresses that exist on your network.

Assigning IP Addresses to Hosts in Trust Zone (Enabling DHCP Server). You can choose to have the NetScreen-5GT assign IP addresses, via DHCP, to hosts in your network. If you have the NetScreen-5GT assign IP addresses, then you can define the range of addresses to be assigned. You need to ensure that the range of addresses is in the same subnetwork as the Trust zone interface IP address.

Step 1

Launch a Web browser. In the URL address field, enter **http://192.168.1.1** or **http://ns.setup**. The Rapid Deployment (RD) Wizard appears.



Step 2

If your network uses Juniper Networks NetScreen-Security Manager 2004, you can use an RD configlet to automatically configure the NetScreen-5GT. Obtain a configlet from your Security Manager administrator, select the **Yes** option, select the **Load Configlet from** option, browse to the file location, and then click **Next**. The configlet sets up the NetScreen-5GT for you. If you use a configlet, you can skip the remaining instructions in this guide.

Note: *Skip the Inital Configuration Wizard if you want to configure the Combined or Extended Port Mode on the NetScreen-5GT. You must use the CLI to configure these ports.*

If you need to change the port mode on the device, select the **Change the Port Mode** option, select the port mode from the drop-down menu, and then click **Apply** before loading the configlet.

If you want to bypass the configuration wizard and go directly to the WebUI, select the last option, and then click **Next**. (See the *NetScreen-5GT User's Guide* for configuration instructions.)

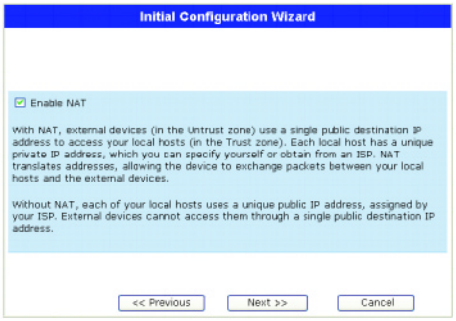
If you are not using a configlet to configure the NetScreen-5GT and want to use the configuration wizard, select the first option, and then click **Next**. The Initial Configuration Wizard screen appears.

Click **Next**.

Step 3

Enter a new administrator login name and password. Click **Next**.

Step 4



Select the **Enable NAT** check box if you want the NetScreen-5GT to be in Route mode with NAT enabled. Click **Next**.

Step 5

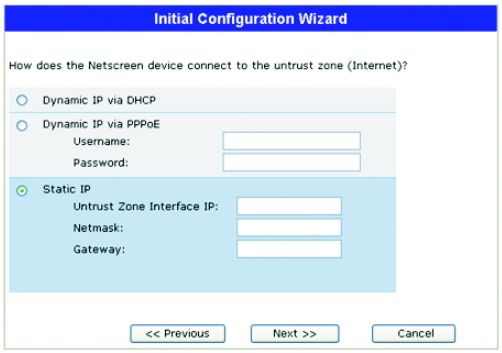
Port modes allow you to bind physical ports, logical interfaces, and zones. Select one of the following port modes:

- **Trust-Untrust Mode** - **(**Default) binds the Trust zone interface to the Trust zone and the Untrust interface to the Untrust zone.
- **Home-Work Mode** - binds interfaces to the Untrust zone and to new Home and Work zones. The Home and Work zones enable you to segregate users and resources in each zone.
- **Dual-Untrust Mode** - binds two interfaces, a primary and a backup, to the Untrust zone. The backup interface is used only when there is a failure on the primary interface.

Click **Next**.

Note: *The remaining steps in this guide show the screens for the default Trust-Untrust Mode. If you select a different port mode, you might see slightly different screens.*

Step 6



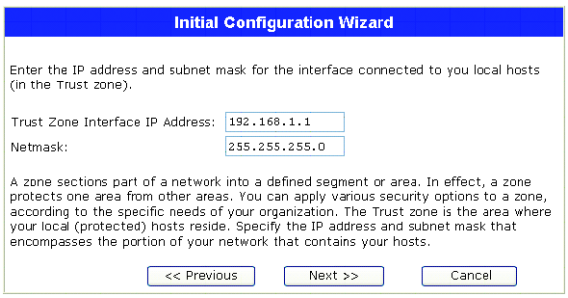
Note: *If you selected* ***Dual-Untrust Mode*** *in Step 5, the preceding screen appears for each Untrust zone interface.*

The Untrust zone interface can have a static IP address or a dynamic IP address assigned via DHCP or PPPoE.

- Select **Dynamic IP via DHCP** to enable the NetScreen-5GT to receive an IP address for the Untrust zone interface from an ISP.
- Select **Dynamic IP via PPPoE** to enable the NetScreen-5GT to act as a PPPoE client, receiving an IP address for the Untrust zone interface from an ISP. Enter the Username and Password assigned by the ISP.
- Select **Static IP** to assign a unique and fixed IP address to the Untrust zone interface. Enter the Untrust Zone Interface IP address, Netmask, and Gateway (the gateway address is the IP address of the router port connected to the NetScreen-5GT).

Click **Next**.

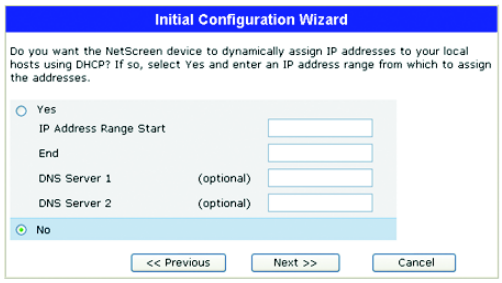
Step 7



To change the IP address of the Trust zone interface, enter a new IP address and netmask. If you change the IP address and netmask of the Trust zone interface, then your workstation and the Trust interface of the NetScreen-5GT might be on different subnetworks. To manage the NetScreen-5GT with the WebUI, ensure that your workstation and the NetScreen-5GT are in the same IP network and use the same netmask. Click **Next**.

Note: *If you selected the* ***Home-Work Mode*** *in Step 5, you are prompted to provide the IP addresses and netmasks for the Home and Work zone interfaces instead of the Trust zone interface. You also have the option of choosing to receive an address via DHCP.*

Step 8

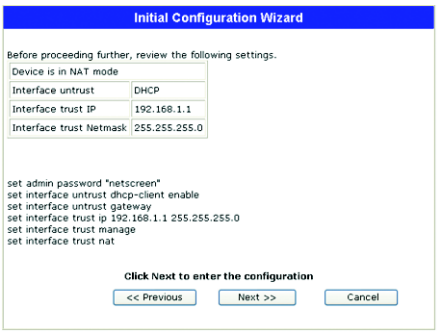


You can choose to have the NetScreen-5GT assign IP addresses to hosts in your network.

- Select **Yes** if the NetScreen-5GT is to act as a DHCP server and assign dynamic IP addresses to hosts in the Trust zone interface. Enter a range for the assigned IP addresses or enter the address(es) of the DNS server(s). If you specify an IP address range that is in a different subnetwork than the Trust subnetwork, then your workstation and the Trust zone interface of the NetScreen-5GT might be in different subnetworks. To manage the NetScreen-5GT using the WebUI, ensure that your workstation and the NetScreen-5GT are in the same subnetwork.
- Select **No** if you do not want the NetScreen-5GT to assign IP addresses to hosts in the Trust zone interface.

Click **Next**.

Step 9



A confirmation screen like the above appears:

- Click **Previous** to modify configuration information.
- Click **Next** to enter the configuration.

The NetScreen-5GT reboots after clicking **Next**.

Step 10

Click **Finish** in the final window and close the web browser. Relaunch the Web browser and in the URL address field, enter the Trust zone interface or Work zone interface IP address. (Your workstation and the NetScreen-5GT must be in the same subnetwork.) Your NetScreen device configuration is now complete.

BASIC SECURITY AND POLICY ADMINISTRATION

You must register your product at www.netscreen.com/cso to activate certain NetScreen ScreenOS services, such as the Deep Inspection Signature Service. After registering, use the WebUI or CLI to obtain the subscription for the service.

Step 1

Using Policy Wizards. By default, the NetScreen-5GT device permits workstations in your network to start sessions with outside workstations, while outside workstations cannot start sessions with your workstations. You can set policies that tell the device what kinds of sessions to restrict or permit.

To set a policy to either restrict the kinds of traffic that can be initiated from inside your network to go out to the Internet, or to permit certain kinds of traffic that can be initiated from outside workstations to your network, use the WebUI Policy Wizard. In the WebUI menu column, click **Wizards > Policy**. Follow the directions in the Wizard to configure a policy.

You can use the Wizards only when the device is in the default Trust-Untrust Port Mode. For details on setting up policies, see the *NetScreen Concepts & Examples ScreenOS Reference Guide*.

Step 2

Using Protection Options. The firewall attack protection (SCREEN) menu enables you to tailor detection and threshold levels for a range of potential attacks.

a. In the WebUI menu column, click **Screening > Screen**.

b. Select the zone for which you want to configure firewall attack protection.

c. Select the appropriate protection options, and then click **Apply**. Remember these features must be configured on each zone where they are required.

Step 3

Verifying Access. 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 URL: www.juniper.net.

Copyright © 2004 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, NetScreen, NetScreen Technologies, GigaScreen, NetScreen-Global PRO, NetScreen-Remote, NetScreen ScreenOS and the NetScreen logo are trademarks and registered trademarks of Juniper Networks, Inc. in the United States and other countries. 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.

P/N 093-1240-000 Rev. A