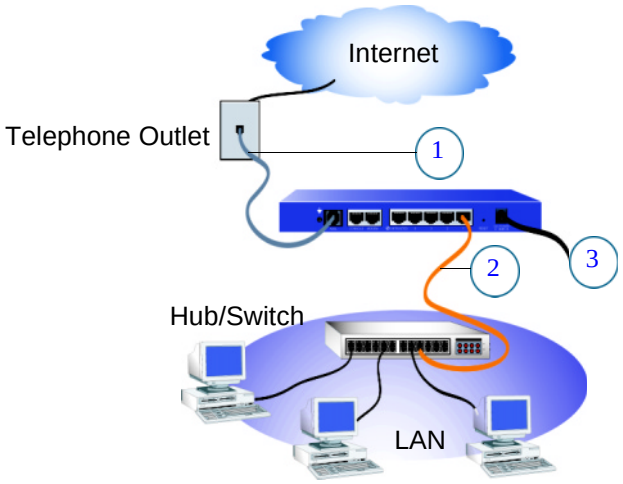
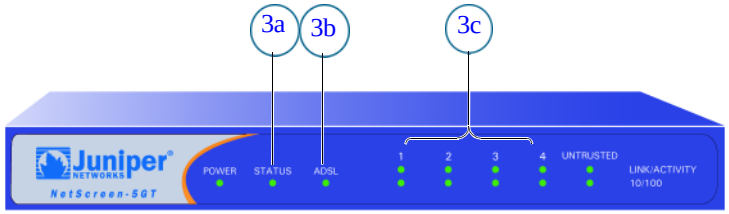
Juniper Networks NetScreen-5GT ADSL

Getting Started

Use the instructions in this guide to help you connect and configure your NetScreen-5GT ADSL device. For additional configuration information, see the *NetScreen-5GT ADSL User's Guide* and the *ADSL Reference Guide*. For information on ADSL line compatibility, see http://www.juniper.net/products/integrated/5GT-ADSL/.





The numbers on the diagram are paired with the steps below

CONNECTING THE DEVICE

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

Step 1

Connect the provided ADSL cable from the ADSL port of the NetScreen device to the telephone outlet.

Note: *You can obtain and install a signal splitter on the ADSL line. The splitter divides the ADSL signal into low-frequency voice signals for voice calls and high-frequency data signals for data traffic. You can also install microfilters on telephones that share the ADSL line.*

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 device 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 glows 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 device via a Web browser:

a. Ensure that your workstation is properly connected to your LAN (use the diagram above).

b. Change the TCP/IP settings of your workstation to obtain its IP address automatically from the NetScreen device 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 ADSL device. Before starting the Wizard, decide how you want to deploy your device. (For additional information, see the *NetScreen-5GT ADSL User's Guide*.)

Network Address Translation (NAT). You can deploy the NetScreen device 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 device replaces the source IP address of the sending host with the IP address of the Untrust zone interface. Route mode with NAT is the most common way to configure the Trust zone interface on the NetScreen device. 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 PPPoA 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 the Trust zone interfaces. To configure the Untrust zone interface, you need to configure the IP address of the interface that is connected to the service provider's DSLAM.

Port Mode. A port mode binds interfaces to zones. The default port mode, Trust-Untrust, binds the Trust interface to the Trust zone and the ADSL interface to the Untrust zone.

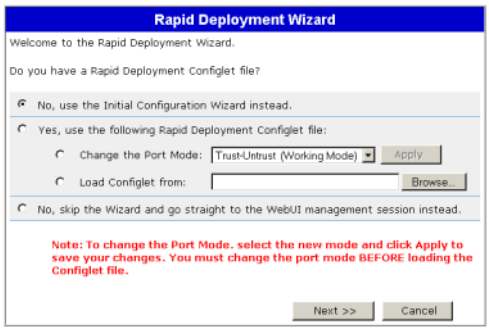
ADSL Interface. By default, the ADSL interface is bound to the Untrust zone and is the primary interface for traffic to the outside network.

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 (Enable DHCP Server). You can choose to have the NetScreen device assign IP addresses via DHCP to hosts in your network. If you have the device 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

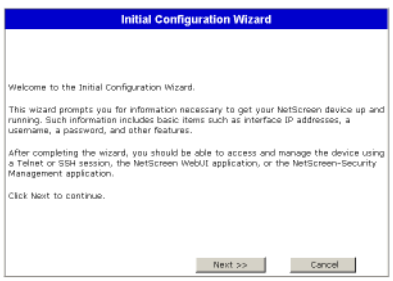
If your network uses Juniper Networks NetScreen-Security Manager 2004, you can use an (RD) configlet to automatically configure the NetScreen device. Obtain a configlet from your Security Manager administrator, select the **Yes** option, select the **Load Configlet from:** option, browse to the file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

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, then click **Apply** before loading the configlet.

Note: *Skip the Initial Configuration Wizard if you want to configure the Trust/Untrust/DMZ port mode on the NetScreen-5GT ADSL device. You must use the WebUI or CLI to configure the Trust/Untrust/DMZ port mode.*

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

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

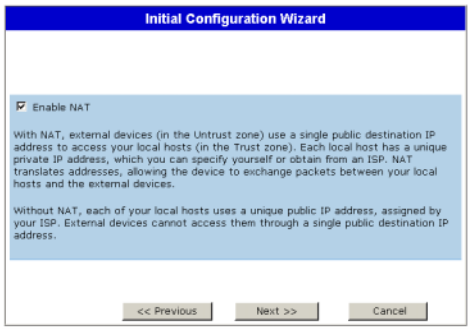


Click **Next**.

Step 3

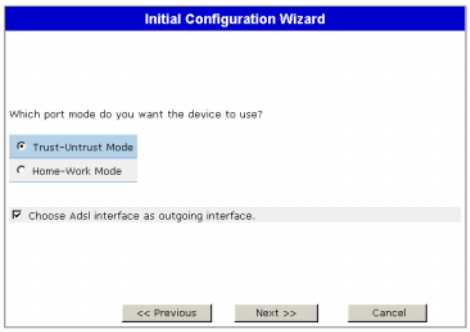
Enter a new administrator login name and password, then click **Next**.

Step 4



Check the **Enable NAT** check box if you want the NetScreen device to be in Route mode with NAT enabled. Click **Next**.

Step 5



Port modes bind physical ports, logical interfaces, and zones.

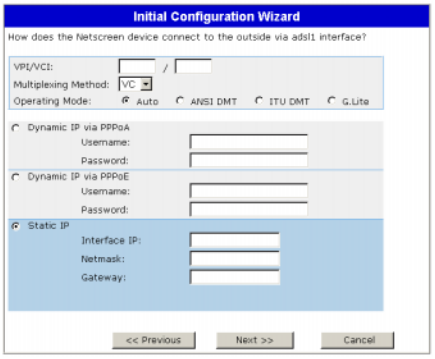
- **Trust-Untrust** mode, the default, binds the Trusted interface to the Trust zone and the ADSL interface to the Untrust zone.
- **Home-Work** mode binds interfaces to the Untrust, Home and Work zones.

Note: *There is a third port mode option, Trust/Untrust/DMZ mode, which is only available with the Extended version of the NetScreen-5GT ADSL device. You must use the WebUI or CLI to configure the Trust/Untrust/DMZ port mode.*

The ADSL interface is the default interface to the Untrust zone. If you do not want to use the ADSL interface, uncheck the box. Click **Next**.

Note: *The remaining steps in this guide show the screens for the default Trust-Untrust port mode with the ADSL interface as the default Untrust zone interface. If you selected different options, you may see different screens.*

Step 6



Enter the following information from your service provider:

- VPI/VCI values to identify the permanent virtual circuit.*
- ATM multiplexing method (LLC is the default).
- Operating mode for the physical line (auto is the default).

(Annex B model only) Select **Deutsche Telekom** to connect to a Deutsch Telecom ADL line; otherwise select **non-Deutsche Telekom**.

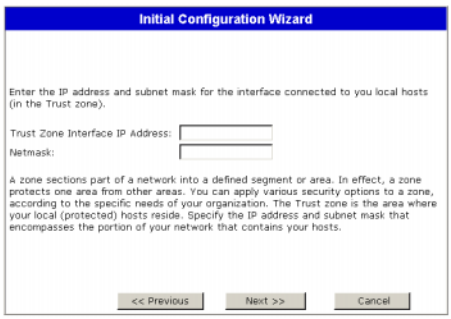
Select **Dynamic IP via PPPoA** to enable the NetScreen device to act as a PPPoA client. Enter the Username and Password assigned by the service provider.

Select **Dynamic IP via PPPoE** to enable the NetScreen device to act as a PPPoE client. Enter the Username and Password assigned by the service provider.

(Optional) Select **Static IP** to assign a unique and fixed IP address to the ADSL interface. Enter the interface IP address, Netmask, and Gateway (the gateway address is the IP address of the router port connected to the NetScreen device).

Click **Next**.

Step 7

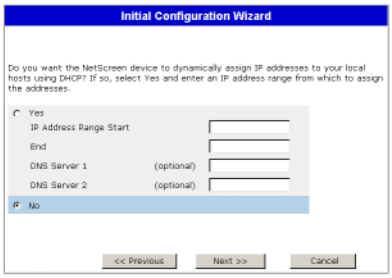


To change the IP address of the Trust zone interface, enter a new IP address and netmask. If you change the IP address and netmask of the Trust zone interface, then your workstation and the Trust interface of the NetScreen device might be on different subnetworks. To manage the NetScreen device with the WebUI, ensure that your workstation and the NetScreen device 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.*

*See http://www.juniper.net/products/integrated/5GT-ADSL/

Step 8

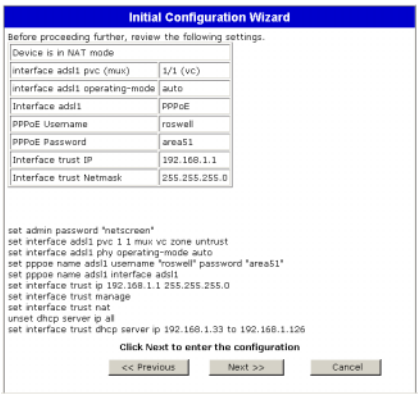


You can choose to have the NetScreen device assign IP addresses to hosts in your network.

- Select **Yes** if the NetScreen device is to act as a DHCP server and assign dynamic IP addresses to hosts in the Trust zone. 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 device might be in different subnetworks. To manage the NetScreen device using the WebUI, ensure that your workstation and the NetScreen device are in the same subnetwork.
- Select **No** if you do not want the NetScreen device to assign IP addresses to hosts in the Trust zone.

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 device 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 ADSL device must be in the same subnetwork.)

Your NetScreen configuration is complete.

BASIC SECURITY AND POLICY ADMINISTRATION

You must register your product at www.netscreen.com/cso to activate certain 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 device permits workstations in your network to start sessions with outside workstations, while outside workstations cannot start sessions with your workstations. You can set up policies that tell the device what kinds of sessions to restrict or permit.

To set up 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, 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.

P/N 093-1197-000 Rev. A