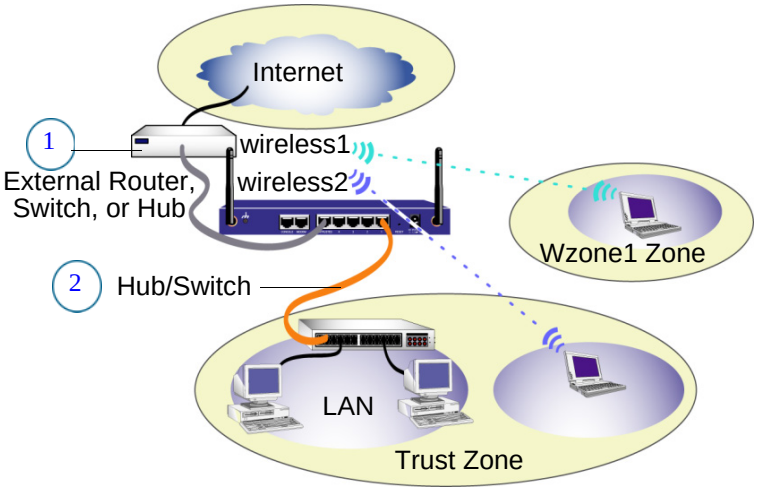
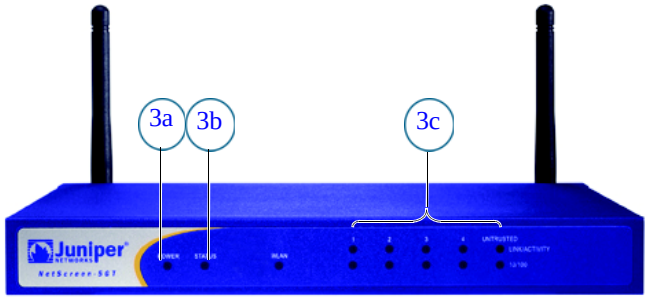
Juniper Networks NetScreen-5GT Wireless

Getting Started

Use the instructions in this guide to help you connect and configure your NetScreen-5GT Wireless device. For additional configuration information, see the *NetScreen-5GT Wireless User's Guide* and the *NetScreen Wireless Reference Guide*.





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

CONNECTING THE DEVICE

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

Step 1

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

Step 2

Note: *You can access the Initial Configuration Wizard (ICW) from the Trust Ethernet interface.*

- 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 computer, connect an Ethernet cable from the Trusted port directly to the Ethernet port on the workstation. We recommend this connection method.

Step 3

Connect the power cable between the NetScreen device and a power source. We recommend using a surge protector.

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

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

c. Ensure that the Link Activity LEDs glow green for the connected interfaces. This indicates that 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 (see diagram).

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

Network Address Translation (NAT). You can deploy the NetScreen device in Route mode with NAT enabled on the Trust and wireless2 interfaces (Trust zone interfaces) 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 interfaces 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 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 Trust zone 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 device.

Port Mode. A port mode binds interfaces to zones. The default port mode, Trust-Untrust, binds the Trust Ethernet and wireless2 interfaces to the Trust zone and binds the wireless1 interface to the Wzone1 zone.

Wireless Interfaces. By default, the wireless2 interface is bound to the Trust zone. The default IP address and netmask for the wireless2 interface is 192.168.2.1/24. You can change this address to match the IP addresses on your network. The wireless1 interface is bound to the Wzone1 zone and does not have an assigned IP address.

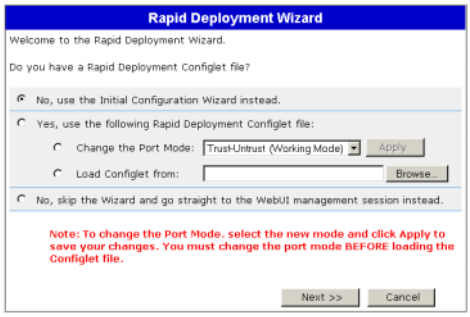
Trust Ethernet Interface IP Address. The default IP address and netmask for the Trust interface is 192.168.1.1/24, which is located in the Trust zone. You can change this address to match existing IP addresses on your network.

Assigning IP Addresses to Hosts in the Trust Zone (Enable DHCP Server). You can choose to have the NetScreen device assign IP addresses via DHCP to wired or wireless hosts in your network. If you have the device assign IP addresses, 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 Ethernet interface or the wireless2 interface IP address.

Step 1

Launch a web browser. In the URL address field, enter **http://192.168.1.1**. The Rapid Deployment Wizard window appears.

Note: *You can access the Initial Configuration Wizard (ICW) from the Trust Ethernet interface.*



Step 2

If your network uses Juniper Networks NetScreen-Security Manager, you can use a Rapid Deployment 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, and 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, and click **Apply** before loading the configlet.

Note: *Skip the ICW if you want to configure the Extended or Combined port mode on the NetScreen-5GT Wireless device. You must use the WebUI or CLI to configure the Extended or Combined port mode.*

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

If you are not using a configlet to configure the NetScreen device and want to use the ICW, select the first option and click **Next**. The Initial Configuration Wizard welcome screen appears. Click **Next**.

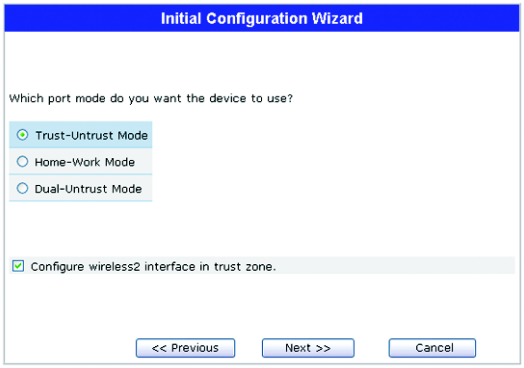
Step 3

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

Step 4

Check the **Enable NAT** checkbox 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.

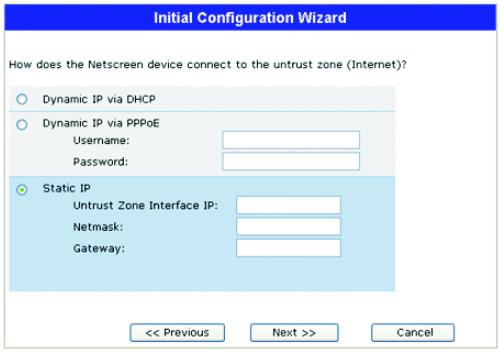
- **Trust-Untrust** mode, the default, binds the Trusted Ethernet and wireless2 interfaces to the Trust zone.
- **Home-Work** mode binds interfaces to the Untrust, Home, and Work zones.
- **Dual-Untrust** mode binds the Trusted 4 interface and Untrust interface to the Untrust Zone.

If you want to configure the default wireless2 interface for the Trust zone, check the box. Click **Next**.

Note: *Extended and Combined are the other port mode options. You must use the WebUI or CLI to configure these port modes.*

Note: *The remaining steps in this guide show the screens for the default Trust-Untrust port mode with the Trust and wireless2 interfaces bound to the Trust zone and the Untrust interface bound to the Untrust zone.*

Step 6



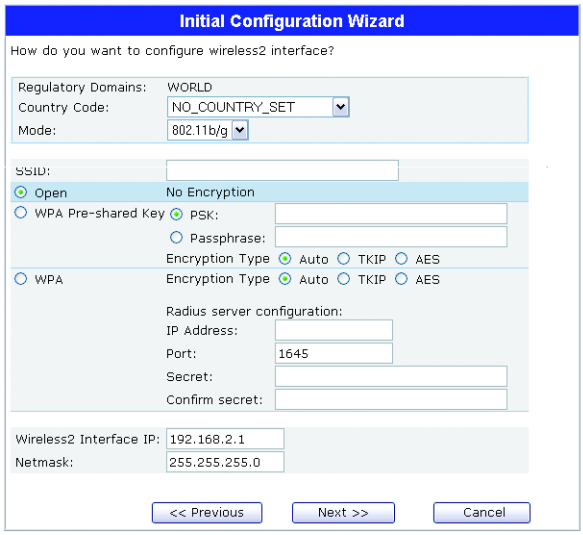
Note: *If you selected* ***Dual-Untrust Mode*** *in Step 5, this screen appears for each Untrust zone interface.*

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

- Select **Dynamic IP via DHCP** to enable the NetScreen device to receive an IP address for the Untrust zone interface from a DHCP server.
- 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 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



Note: *If you are configuring a NetScreen device that has the Regulatory Domain WORLD setting, you must set the country code. If you are configuring a NetScreen device that has the Regulatory Domain FCC or TELEC setting, the country code is preset and cannot be changed.*

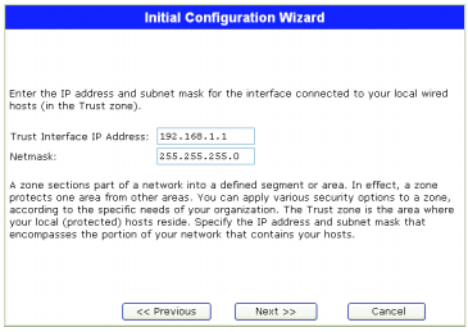
You must set a Service Set Identifier (SSID) before the wireless2 interface can be activated.

- **Open** authentication, the default, allows anyone to access the device. There is no encryption for this authentication option.
- **WPA Pre-Shared Key** authentication sets the Pre-Shared Key (PSK) or passphrase that must be entered when accessing wireless connectivity. You can choose to enter a HEX or an ASCII value for the PSK. A HEX PSK must be a 256-bit (64 text character) HEX value. An ASCII passphrase must be 8 to 63 text characters. You must select Temporal Key Integrity Protocol (TKIP) or Advanced Encryption Standard (AES) encryption type for this option, or select **Auto** to allow either option.
- **WPA** permits authentication with an external RADIUS server. Enter the RADIUS server IP address, the port number to which the NetScreen device sends authentication requests, and the shared secret (password) between the NetScreen device and the RADIUS server. You must select TKIP or AES encryption type for this option, or select **Auto** to allow either option.

The options presented are the most common ways to secure a wireless network. For information about all the security options, see the *NetScreen Wireless Reference Guide*. To use a security method that is not listed here, complete the ICW and then use the WebUI or CLI to configure it.

To change the IP address of the wireless2 interface, enter a new IP address and netmask. The default is 192.168.2.1/24.

Step 8



To change the IP address of the Trusted Ethernet interface, enter a new IP address and netmask. If you change the IP address and netmask of the Trust interface, your workstation and the Trust interface of the NetScreen device might be on different subnetworks. 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 Trusted Ethernet interface. You also have the option of choosing to receive an address via DHCP.*

Step 9

You can choose to have the NetScreen device assign IP addresses to wired or wireless 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). To manage the NetScreen device with the WebUI, ensure that your workstation and the NetScreen interface are in the same IP network.
- Select **No** if you do not want the NetScreen device to assign IP addresses to hosts in the Trust zone.

Click **Next**.

Step 10

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

The NetScreen device reboots after you click **Next**.

Step 11

Click **Finish** in the final window and close the web browser. Relaunch the web browser and enter one of the Trust or Work zone interface IP addresses in the URL address field. (Your workstation and the NetScreen interface must be in the same subnetwork.)

BASIC SECURITY AND POLICY ADMINISTRATION

You must register your product at www.juniper.net/support/ 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 the 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 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 click **Apply**. You must configure these features 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 093-1482-000 Rev. A