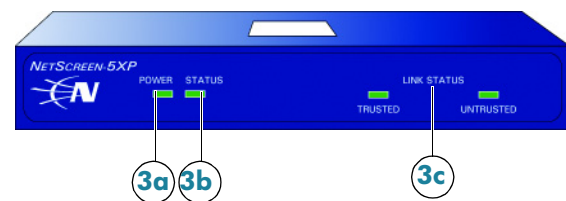
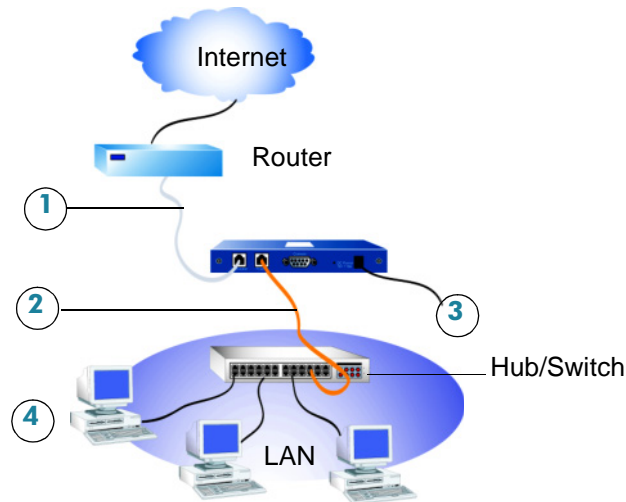


NetScreen-5XP

Getting Started

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



The numbers on the diagram are paired with the steps below



CONNECTING THE DEVICE

Using the instructions below, connect the NetScreen-5XP 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 an Ethernet cable from the Untrust port of the NetScreen-5XP to the external router, cable modem, or DSL modem.

Step 2

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

Step 3

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

- Ensure that the Power LED glows green. This indicates the device is receiving power.
- After the NetScreen-5XP starts (should take about 30 seconds), ensure that the Status LED blinks green. This indicates the device is operating normally.

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

Step 4

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

- Ensure that your workstation is properly connected to your LAN (use the diagram above).
- Change the TCP/IP settings of your workstation to obtain its IP address automatically from the NetScreen-5XP 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.

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



CONFIGURING THE DEVICE

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

Operational Mode. You can deploy the NetScreen-5XP 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-5XP replaces the source IP address of the sending host with the IP address of the Untrusted port of the NetScreen-5XP. 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-5XP.

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 the Trust Zone (Enabling DHCP Server). You can choose to have the NetScreen-5XP assign IP addresses, via DHCP, to hosts in your network. If you have the NetScreen-5XP 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 subnet 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 Wizard appears.

Step 2

If your network uses NetScreen-Security Manager 2004, you can use a Rapid Deployment (RD) configlet to automatically configure the NetScreen-5XP. Obtain a configlet from your Security Manager administrator, select the Yes option, click in the **Load Configlet from:** field, browse to the file location, then click **Next**. The configlet sets up the NetScreen-5XP for you. If you use a configlet, you can skip the remaining instructions in this guide.

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

If you are not using a configlet to configure the NetScreen-5XP and you want to use the configuration wizard, select the first option, then

click **Next**. The Initial Configuration Wizard welcome screen appears.

Click **Next**.

Step 3

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



Step 4

Initial Configuration Wizard

Enter the administrator's login name and password:

Administrator Login Name:

Password:

Confirm Password:

Note: You cannot retrieve the login name and password if you lose it. Please make sure you have a copy of this information in a secure location.

<< Previous Next >> Cancel

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

Step 5

Initial Configuration Wizard

How does the Netscreen device connect to the untrust zone (Internet)?

Dynamic IP via DHCP

Dynamic IP via PPPoE

 Username:

 Password:

Static IP

 Untrust Zone Interface IP:

 Netmask:

 Gateway:

<< Previous Next >> Cancel

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-5XP to receive an IP address for the Untrust zone interface from an ISP.
- Select **Dynamic IP via PPPoE** to enable the NetScreen-5XP 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, Netmask, and Gateway address (the gateway address is the IP address of the router port connected to the NetScreen-5XP).

Click **Next**.

Step 6

Initial Configuration Wizard

Enter the IP address and subnet mask for the interface connected to you local hosts (in the Trust zone).

Trust Zone Interface IP Address:

Netmask:

A zone sections part of a network into a defined segment or area. In effect, a zone protects one area from other areas. You can apply various security options to a zone, according to the specific needs of your organization. The Trust zone is the area where your local (protected) hosts reside. Specify the IP address and subnet mask that encompasses the portion of your network that contains your hosts.

<< Previous Next >> Cancel

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 zone

interface of the NetScreen-5XP might be in different subnetworks. To manage the NetScreen-5XP with the WebUI, ensure that your workstation and the NetScreen-5XP are in the same subnetwork. Click **Next**.

Step 7

Initial Configuration Wizard

Do you want the NetScreen device to dynamically assign IP addresses to your local hosts using DHCP? If so, select Yes and enter an IP address range from which to assign the addresses.

Yes

 IP Address Range Start:

 End:

 DNS Server 1 (optional):

 DNS Server 2 (optional):

No

<< Previous Next >> Cancel

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

- Select **Yes** if the NetScreen-5XP 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-5XP using the WebUI, ensure that your workstation and the NetScreen-5XP are in the same subnetwork.
- Select **No** if you do not want the NetScreen-5XP to assign IP addresses to hosts in the Trust zone interface.

Click **Next**.

Step 8

Initial Configuration Wizard

Before proceeding further, review the following settings.

Trust interface in NAT mode	
Trust Interface IP	192.168.1.1
Trust Interface Netmask	255.255.255.0
Untrust Interface	DHCP

```
set admin password "netscreen"
set interface trust manage
set interface trust ip 192.168.1.1 255.255.255.0
set interface untrust dhcp-client enable
set interface trust nat
unset dhcp server ip all
```

Click **Next** to enter the configuration.

<< Previous Next >> Cancel

A confirmation screen like the above appears:

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

Your system reboots after clicking Next.



Step 9

At the final review configuration window, click **Finish**. Launch a Web browser. In the URL address field, enter the Trust zone interface or Work zone interface IP address. (Your workstation and the NetScreen-5XP 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, like 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-5XP permits workstations in your network to start sessions with outside workstations, while outside workstations cannot start sessions with your workstations. You can set up access policies that tell the NetScreen-5XP what kinds of sessions to restrict or permit.

To set up an access 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.

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.netscreen.com.