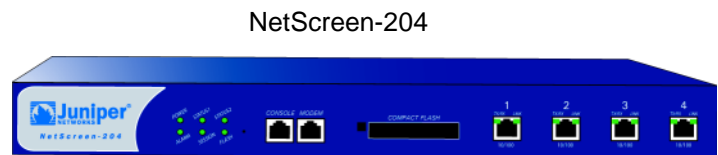
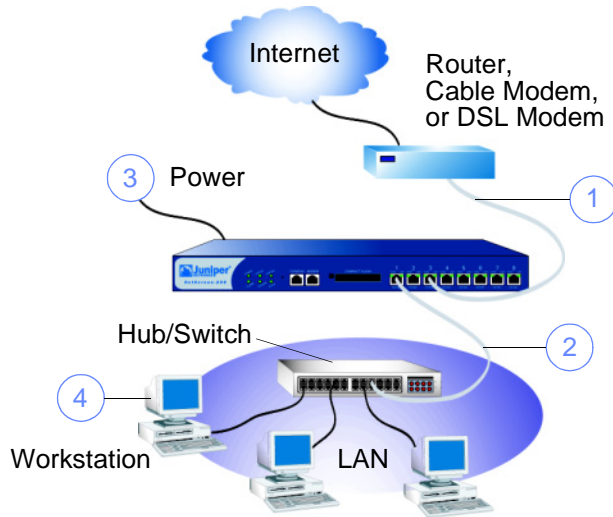




Juniper Networks NetScreen-200 Series

Getting Started

Use the instructions in this guide to help you connect and configure your NetScreen-200 Series device. For more configuration examples and details, see the *NetScreen-200 Series 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-200 Series device 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 ethernet3 port of the NetScreen device to the external router, cable modem, or DSL modem.

Step 2

Connect an Ethernet cable from the ethernet1 port to the internal switch or hub.

Step 3

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

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

- Ensure that the Link 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:

- Ensure that your workstation is properly connected to your LAN (see diagram).
- Record the IP address and netmask of your workstation. You need to re-enter them later in this process.
- Change the IP address and netmask of your workstation to 192.168.1.2 and 255.255.255.0, respectively. For help, see the operating system documentation for your workstation.
- If necessary, restart the workstation to enable the changes to take effect. The workstation is now part of the same subnetwork as the NetScreen device default IP address, which is 192.168.1.1.



CONFIGURING THE DEVICE

Use the Initial Configuration Wizard to configure the NetScreen-200 Series device. Before starting the Wizard, decide how you want to deploy your device. (For additional information, see the *NetScreen-200 Series User's Guide*.)

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 device assign IP addresses, via DHCP, to hosts in your network. If you have the

NetScreen 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 a RD configlet to automatically configure the NetScreen device. Obtain a configlet from your Security Manager administrator, select the **Yes** option, click in the **Load Configlet from** field, browse to the file location, and then click **Next**.

If you want to bypass the configuration wizard and go directly to the WebUI, select the last option, and then click **Next**.

If you are not using an RD configlet to configure the NetScreen device and you 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

Interface	Zone
ethernet1	Trust
ethernet2	DMZ
ethernet3	Untrust
ethernet4	Null
ethernet5	Null
ethernet6	Null
ethernet7	Null
ethernet8	Null

Bind interface to NULL zone if you are not planning to configure it at this time

Select the zones to which each interface is bound. Click **Next**.



Step 5

Initial Configuration Wizard

Configure the IP address and subnet mask for the interfaces.

If you do not know the IP address and subnet mask for these interfaces at this time, you can leave the fields blank and configure them after you complete the Initial Configuration Wizard.

Note: You can only configure DHCP and PPPoE using the CLI or the WebUI after you complete the Initial Configuration Wizard.

Interface	Zone	IP / Netmask
ethernet1	Trust	192.168.1.1 / 255.255.255.0
ethernet2	DMZ	
ethernet3	Untrust	

<< 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 device might be in different subnetworks. To manage the NetScreen device with the WebUI, ensure that your workstation and the NetScreen device are in the same subnetwork. Click **Next**.

Note: To change the IP address of the Untrust or DMZ zone interfaces, enter a new IP address and netmask. If you are using DHCP or PPPoE to assign an IP address for these interfaces, then leave the fields blank. You need to configure the addresses after you have completed the Initial Configuration Wizard. Please refer to Step 9 to assign IP addresses.

Step 6

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 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 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 in a different subnetwork than the Trust subnetwork, then your workstation and the Trust zone interface of the NetScreen device might then 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 interface.

Click **Next**.

Step 7

Initial Configuration Wizard

Before proceeding further, review the following settings.

Interface	Zone	IP	Netmask
ethernet1	Trust	192.168.1.1	255.255.255.0
ethernet2	DMZ		
ethernet3	Untrust		
ethernet4	Null		
ethernet5	Null		
ethernet6	Null		
ethernet7	Null		
ethernet8	Null		

```
set admin password "netscreen"
set interface ethernet1 zone Trust
set interface ethernet1 ip 192.168.1.1 255.255.255.0
set interface ethernet1 manage
set interface ethernet2 zone DMZ
set interface ethernet3 zone Untrust
```

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.

Clicking **Next** reboots your NetScreen device.

Step 8

At the final review configuration window, click **Finish**.

Note: If you left blanks in Step 5, then you need to configure the Untrust interface. Proceed to Step 9 to configure the Untrust interface.

Step 9

To configure the NetScreen device to receive an IP address via DHCP or PPPoE:

- Launch a Web browser and, in the URL address field, enter **http://192.168.1.1** or the new IP address you entered in Step 5. The login dialog box appears.

Admin Name:

Password:

Remember my name and password

Login

- Both the admin name and password are case-sensitive. In the dialog box, enter the admin name and password you specified in Step 3.
- Click **Login**.



Step 10

To configure the **ethernet3** interface:

a. Select **Network > Interfaces > Edit** for the **ethernet3** interface.

Interface Name ethernet3 (mac 0010.dbff.2060)
As member of loopback group none
As member of group none
Zone Name Untrust

Obtain IP using DHCP Automatic update DHCP server parameters
 Obtain IP using PPPoE None [Create new pppoe setting](#)
 Status:

Static IP
IP Address / Netmask / Manageable
Manage IP * (mac 0010.db18.2396)

b. If your ISP is using PPPoE, select **Create new PPPoE settings**. Enter a name for the PPPoE instance, then enter the admin name and password provided by your ISP. Click **OK**. Select **Obtain IP using PPPoE**, and then select the PPPoE instance you configured. Click **OK**.

or

c. If your ISP is using DHCP, select **Obtain IP using DHCP**, scroll down, and then click **OK**.

Your NetScreen device configuration is complete.



BASIC SECURITY AND POLICY ADMINISTRATION

You must register your product at www.netscreen.com/cso to activate certain NetScreen 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 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.

For details on setting 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.

- In the WebUI menu column, click **Screening > Screen**.
- Select the zone for which you want to configure firewall attack protection.
- 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.