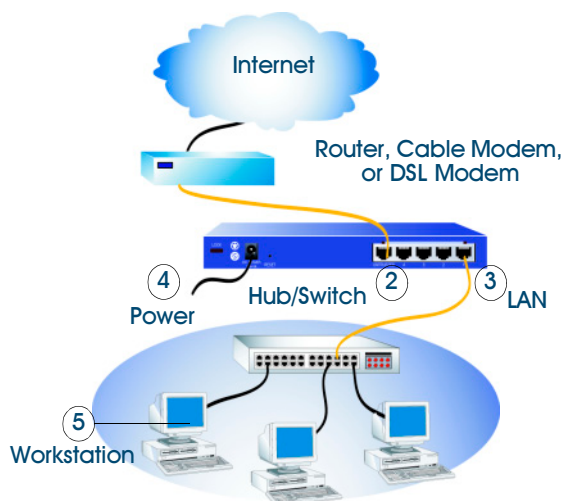


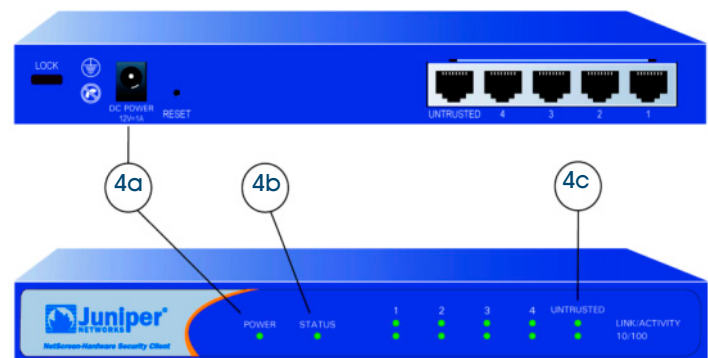
Juniper Networks Rapid Development

Getting Started

This guide helps you connect and configure your NetScreen FW/VPN device using Rapid Deployment (RD). RD automatically configures your device for management by Juniper Networks NetScreen-Security Manager 2004, the integrated management system for all NetScreen FW/VPN devices.



Device shown is a NetScreen-HSC; for network diagrams of your device, see the Getting Started Guide that shipped with your device.



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



CONNECTING THE DEVICE

Using the instructions below, connect the NetScreen FW/VPN device and prepare to configure it to protect your network. Use the LEDs on the front panel of the device to help you determine device status.

Step 1

On a workstation, save the configlet. If you do not have a configlet, contact your Security Manager administrator.

Step 2

Connect an Ethernet cable from the Untrust port of the device to the external router, cable modem, or DSL modem.

Step 3

- If the workstation is in a LAN, connect an Ethernet cable from a Trust port to the internal switch or hub.
- If the workstation is a single workstation, connect an Ethernet cable from a Trust port to the Ethernet port on the workstation.

Step 4

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

- Ensure the Power LED glows green. This indicates the device is receiving power.
- After the device starts (about 30 seconds), ensure the Status LED blinks green. This indicates the device is operating normally.
- Ensure the Link LEDs glow for the connected interfaces. This indicates the device has network connectivity.



Step 5

Configure the workstation to access the NetScreen FW/VPN device via a Web browser:

- Ensure that your workstation is properly connected to your LAN, and that your internal network does not already use a DHCP server.
- Configure your workstation to automatically receive an IP address from the NetScreen FW/VPN device. For help, see your operating system documentation.
- If necessary, restart your workstation. Some operating systems must restart before new settings take effect.



CONFIGURING THE DEVICE

Using the instructions below, follow the Rapid Deployment (RD) Wizard to configure the device for management. The Wizard helps you install the configlet and enables the NetScreen-Security Manager administrator to begin managing the device remotely.

For details on other configuration methods and local management features, see the *User's Guide* that shipped with your NetScreen FW/VPN device.

Step 1

Launch a Web browser. In the Web browser URL address field, enter <http://192.168.1.1>. The RD Wizard appears.

Step 2

Select **Load Configlet from** and browse to the location of the saved configlet (.cfg) file. Click **Next** to continue.

The RD Wizard opens the configlet, verifies the integrity of the configlet, and then decrypts the configlet information. Using this information, the Wizard prepares the device for management.

During this preparation process, the Wizard prompts you for any required information. Some or all of the required information might have already been entered by the NetScreen-Security Manager administrator.

Because the Wizard prompts you only for missing information, you might not need to complete all of the following steps.

Step 3

If prompted, enter the configlet password provided by your NetScreen-Security Manager administrator.

Step 4

If prompted for PPPoE information, enter the username and password for your PPPoE account.

Step 5

If prompted for PPPoA information, enter the VPI/VCI pair, multiplexing and operating mode, and the username, password for your PPPoA account.



Step 6

If prompted for static IP information, enter:

- The IP address and netmask of the interface connected to the external router, cable modem, or DSL modem.
- The gateway address (the IP address of the router port connected to the device).

Rapid Deployment Wizard

Please provide network connectivity information.

Interface: untrust

Using ISP-supplied settings (Static IP)

IP Address/Netmask: 0 / 0

Gateway: 0

Step 7

If the NetScreen-Security Manager administrator did not specify any ISP information, you must select the ISP environment in which you deployed your device:

Rapid Deployment Wizard

Please provide network connectivity information.

Interface: untrust

Using cable modem (Dynamic IP via DHCP)

Using DSL modem (Dynamic IP via PPPoE)

Username: []

Password: []

Using ISP-supplied settings (Static IP)

IP Address/Netmask: 0.0.0.0 / []

Gateway: []

When using a configlet with a NetScreen-5GTADSL device, the following screen appears instead:

Rapid Deployment Wizard

Please provide network connectivity information.

Interface: adsl1

VPI/VCI: 0 / 35

Multiplexing Method: VC

Operating Mode: Auto ANSI DMT ITU DMT G.Lite

Using Dynamic IP via PPPoA

Username: []

Password: []

Using Dynamic IP via PPPoE

Username: []

Password: []

Using ISP-supplied settings (Static IP)

IP Address/Netmask: 0.0.0.0 / []

Gateway: []

- If your device uses DHCP to obtain an IP address, select **Using cable modem** (Dynamic IP via DHCP).
- If your device uses a PPPoE connection to the Internet, select **Using DSL modem (Dynamic IP via PPPoE)**. This option enables your device to act as a PPPoE client that receives an IP address for the Untrust interface from an ISP. Enter the following:
 - The username for your PPPoE account.
 - The password for your PPPoE account.
- If your device uses a PPPoA connection to the Internet, select **Using Dynamic IP via PPPoA**. This option enables your device to act as a PPPoA client that receives an IP address for the Untrust interface from an ISP. Enter:
 - The VPI/VCI pair.
 - The multiplexing and operating mode.
 - The username for your PPPoA account.
 - The password for your PPPoA account.
- If your device uses a static IP address, select **Using ISP-supplied settings** (Static IP). This option enables your device to use a unique and fixed IP address for the Untrust interface. Enter the following:
 - The IP address and netmask of the interface connected to the external router, cable modem, or DSL modem.
 - The gateway address (the IP address of the router port connected to the device).

Step 8

The device processes the information; when completed, the device contacts the management system and establishes a secure connection. The following message appears:

Rapid Deployment Wizard

Acquiring IP address from DHCP/PPPoE server for interface 'adsl1' ...

If the device needs to acquire a dynamic IP address from your ISP, the following message also appears:

Rapid Deployment Wizard

Completed processing startup file. Start connecting to management server.

When the device connects, a confirmation screen appears indicating that you have successfully installed the configlet on the device.

Click **Finish** to exit the Wizard and close the Web browser.



MANAGING THE DEVICE

Now that your device is connected to Juniper Networks NetScreen-Security Manager, the NetScreen-Security Manager administrator can complete the device configuration and create a Security Policy to protect your network.

For details on using Juniper Networks NetScreen-Security Manager to configure policies, VPNs, attack protection, or other features, see the *NetScreen-Security Manager 2004 Administrator's Guide*.

You can also manage the device locally using the WebUI or the Command Line Interface (CLI):

- Using the WebUI, you can manage basic device features and view device configuration. For details, see the *NetScreen Concepts & Examples ScreenOS Reference Guide*.
- Using CLI, you can manage all features of your device from the NetScreen ScreenOS command line. For details, see the *NetScreen CLI Reference Guide*.



TROUBLESHOOTING

During the configlet installation process, errors can occur if the NetScreen FW/VPN device is not properly connected to the network, or if the device is not running a factory default configuration.

The following sections provide details on resolving configlet installation issues.

Untrust Interface Failure Warning



This warning appears when the DHCP service, PPPoE service, or PPPoA service cannot assign an IP address to the device Untrust interface. The device cannot connect to NetScreen-Security Manager without an untrust IP address. To resolve the issue, check the following:

- Ensure that the untrust interface of the device is connected to the external network.
- If you are using DHCP to assign an address to the untrust interface, ensure that the DHCP server is functioning properly.
- If you are using PPPoE or PPPoA to assign an address to the untrust interface, ensure that PPPoE or PPPoA is supported on your network.

Factory Default Warning



This error appears when the device is not running a factory default configuration. RD is designed to configure non-deployed devices and enable them to connect to NetScreen-Security Manager. If your device already contains a device configuration, you must reset the device before you can use a RD configlet. For details on resetting the device, see the *User's Guide* that shipped with your device.

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 the 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.