Juniper Networks Integrated Firewall and IPSec VPN Evaluators Guide

How to configure and test firewall, VPN and Deep Inspection functionality
# Table of Contents

Introduction .....................................................................................................................................................................3
What You Will Need ..........................................................................................................................................................4
Recommendations and Assumptions .............................................................................................................................4
Juniper Networks Terminology ....................................................................................................................................5
Key Features ....................................................................................................................................................................6
Setting Up a Basic Firewall .........................................................................................................................................6
  Set up the initial connectivity on the Juniper Networks NetScreen-5XT .................................................................7
  Log in to the Juniper Networks device .....................................................................................................................8
  Make decisions about the type of connectivity .........................................................................................................9
  Define your IP addresses and DHCP configuration ...............................................................................................10
  Review your configuration and save it ....................................................................................................................11
  Review your progress ..............................................................................................................................................12
The WebUI, Juniper Networks Graphical User Interface ............................................................................................12
  The WebUI Menus – Powerfully Simple ..................................................................................................................13
Configuring a Layer 3 Firewall with the WebUI ...........................................................................................................13
Testing Your Juniper Networks Firewall ..................................................................................................................15
  Testing with a traffic generator ..................................................................................................................................15
  Testing between personal computers ....................................................................................................................15
  Modify the firewall rule and test it ..........................................................................................................................16
Configuring the Deep Inspection Firewall ................................................................................................................17
  Loading the Deep Inspection License Key and Attack Database .........................................................................18
  Enabling Deep Inspection in the Default Policy .....................................................................................................20
  Testing the Deep Inspection Firewall ....................................................................................................................21
  Testing the Deep Inspection Firewall with Action to Close ..................................................................................23
  Review your work ....................................................................................................................................................25
Setting Up a Layer 3 Firewall on the Second Juniper Networks Device .................................................................25
  Log in to the Juniper Networks Device ..................................................................................................................26
  Bind interfaces to zones ..........................................................................................................................................27
  Configure the interface IP address and netmask ......................................................................................................28
  Define your DHCP configuration ...........................................................................................................................28
  Review your configuration and save it ....................................................................................................................29
Configuring the Layer 3 Firewall on the Second Juniper Networks Device with the WebUI ..................................29
  Set up your routing ..................................................................................................................................................30
  Set your access policy .............................................................................................................................................31
Setting Up a VPN between Two Juniper Networks firewalls ..................................................................................32
  Setting up a VPN on the First Firewall Using the VPN Wizard ..............................................................................32
  Setting up a VPN on the Second Firewall Using the VPN Wizard ..........................................................................36
  Testing Your VPN Tunnel ........................................................................................................................................41
Setting Up a Juniper Networks Transparent Mode Firewall ....................................................................................41
  Place Interfaces into the predefined Layer 2 Zones ..................................................................................................43
  Create firewall policies between Zones ..................................................................................................................44
  Testing the Transparent Mode Deployment ..........................................................................................................45
  Review your work ....................................................................................................................................................45
Summary ....................................................................................................................................................................45
Introduction

The purpose of this document is to help you evaluate some of the many capabilities of the Juniper Networks firewall/VPN devices while pointing out the benefits to the user, through a means of simple, easy-to-follow instructions and guidelines. You will configure your Juniper Networks security devices to support simple firewall deployments, first through the use of the built-in Initial Configuration Wizard, and then through the easy-to-traverse WebUI. You will then configure and test the Deep Inspection firewall feature of the Juniper Networks device. By taking advantage of the VPN Wizard, you will build a secure IPSec tunnel between two Juniper Networks security devices.

You can have a Juniper Networks firewall/VPN device up and running in less then 10 minutes, a task that may take much longer with a competitive product. We will expose a unique ability to deploy the Juniper Networks NetScreen-5XT in a variety of custom configurations tailored to fit into common small office and home office environments. We will also show you how, though the simple click of the mouse, you can select deployment options to support different Internet access offerings, be it cable modem, DSL access using PPPoE or an access offering with a statically assigned IP address.

As a final exercise, we will guide you through a Transparent Mode firewall deployment, which uncovers a unique deployment option offered by Juniper Networks. When configured as a Transparent Mode firewall, a Juniper Networks firewall/VPN device can be installed into an existing network infrastructure as a Layer 2 device, not assigning IP addresses to its interfaces. Transparent Mode enforces security policies in your IP traffic without requiring you to change your existing IP addresses.

This Guide provides:

- An explanation of some of the key terminology used by Juniper Networks
- An exploration of the WebUI, Juniper Networks built-in graphical user interface
- An exercise in setting up a Juniper Networks firewall
- An exercise in configuring the Deep Inspection firewall
- An exercise in setting up a secure IPSec tunnel between two Juniper Networks security devices
- An exercise in setting up a Juniper Networks firewall in Transparent Mode
What You Will Need

To complete your Juniper Networks firewall/VPN evaluation, you will need the following equipment, at a minimum:

- A Juniper Networks NetScreen-5XT firewall/VPN device\(^1\)
- A second Juniper Networks firewall/VPN device. In this Guide, we use a Juniper Networks NetScreen-50 firewall/VPN device, but a second Juniper Networks NetScreen-5XT\(^1\) could be used as well.
- One Microsoft Windows based personal computer with an Ethernet network adapter and an Internet browser, such Internet Explorer. We will refer to this as PC-1.
- A second Microsoft Windows based personal computer with an Ethernet network adapter and an Internet browser, such Internet Explorer. The second PC should also have Web and FTP server software installed. We will refer to this as PC-2.
- 4 RJ-45 Ethernet cables to interconnect all devices
- The Juniper Networks documentation CD
- Optionally, a traffic generation tool, such as Spirent SmartBits or IXIA

Recommendations and Assumptions

- The Juniper Networks NetScreen-5XT supports a DHCP server on the Trusted interfaces. This eases the burden of pre-configuring IP addresses for devices connected to the Juniper Networks security device. Should you already have a DHCP server on your network, the NetScreen-5XT DHCP server will recognize its existence and turn itself off automatically.

To take advantage of the DHCP server for this evaluation, configure PC-1 to receive an IP address using DHCP by performing the following steps:

- Navigate your PC through the Windows Start>Settings>Control Panel folder
- Open the Network and Dial-up Connections folder
- Double click the Local Area Connection Icon
- Click on the Properties button
- Double click the Internet Protocol (TCP/IP) option
- Select Obtain an IP address automatically and press OK
- Press OK at the Local Area Connection window

- Keep network addressing in test environments simple.
  - Use 192.168.1.0/24 for the NetScreen-5XT Trust network. This is the address range that the DHCP Server on the NetScreen-5XT uses by default.
  - Use 172.16.10.0/24 for the Untrusted network(s)
  - Use 10.0.0.0/24 for the Trust network on your second Juniper Networks device

It is assumed that the reader possesses a fundamental knowledge of overall networking topologies, IP networking and protocols as well as a basic understanding of firewall and VPN concepts.

\(^1\) You can use a Juniper Networks NetScreen-5GT for this evaluation instead.
Juniper Networks Terminology

The following is list of some of the terms we will use throughout this Guide, some of which are specific to Juniper Networks.

- **Interface** – Any Ethernet port on a Juniper Networks security device. On the Juniper Networks NetScreen-5XT, the interfaces are labeled **Trusted 1, 2, 3 and 4**, and **Untrusted**. On the Juniper Networks NetScreen-50, the interfaces are labeled **E1, E2, E3** and **E4**.

- **Security Zone** – A collection or group of interfaces in a Juniper Networks device. Juniper Networks uses Security Zones to logically group network entities. For example, all the members of your Sales Department reside in a collective area of your building. Their workstations are interconnected through a series of Ethernet switches, which could be connected to one or more interfaces on the Juniper Networks device. Through a simple means of placing these interfaces into a single Security Zone, you have logically grouped the Sales Department, and you can define security policies for the entire Sales Department.

- **Trust Zone** – A default Security Zone on the Juniper Networks device, containing interfaces that interconnect internal devices, such as the ones in the corporate network. The Trust Zone can be used to house the entire internal network to either facilitate the migration from legacy firewall products or when individual departments of your organization do not require unique access control policies.

- **Untrust Zone** – A default Security Zone on the Juniper Networks device, containing the interfaces that interconnect external devices. The Untrust Zone generally represents the Internet.

- **DMZ Zone** – A default Security Zone on the Juniper Networks device, containing the interfaces that interconnect devices that do not require the same security as internal devices in the Trust Zone and that typically need to be accessed by devices in the Untrust Zone. The DMZ (demilitarized zone) is generally used to place publicly accessible Web and mail servers.

- **Policies** – Rules that govern what can and cannot pass between the Security Zones on the Juniper Networks device. Policies are used to allow or disallow selected services from individual systems, groups of systems or any address between your Security Zones. Policies can allow an entire realm of services or a single service. Yet policies are easy to understand and simple to deploy via Juniper Networks comprehensive, built-in WebUI utility.

- **Deep Inspection** – Mechanism for filtering network traffic at the application layer by the Juniper Networks firewall. Configured per policy, Deep Inspection examines application content and protocol characteristics in an effort to detect and prevent attacks or anomalous behavior that might be present in application messages.

- **Dynamic Routing Protocols** – Juniper Networks firewall/VPN devices support the most common dynamic routing protocols, including RIPv2, BGP and OSPF. Though description of this feature is beyond the scope of this document.

- **Network Address Translation (NAT)** – The ability to translate an IP address or range of addresses to another. NAT is typically used to allow non-routable internal IP addresses to traverse the Internet.

- **Transparent Mode** – Juniper Networks term referring to the configuration in which a Juniper Networks device can be deployed without IP addresses assigned to its interfaces and still provide firewall and VPN functionality. This compelling advantage allows you to quickly install a Juniper Networks device into an existing infrastructure.
**Key Features**

Juniper Networks firewall/VPN solutions provide some unique features that we will call out as you go through this evaluation. Look for the following key features:

- **Customizable security zones** – Juniper Networks uses Security Zones to logically group network entities that share similar characteristics and/or security needs, for example, all the members of a specific department in your organization. You can create Security Zones to group your internal devices and enforce security policies between these Security Zones.

- **Dynamic Routing** – Protocols like OSPF, BGP and RIPv2 are supported on Juniper Networks firewall/VPN devices. Juniper Networks implementation allows for seamless integration into your existing network infrastructure.

- **Consistent built-in user interfaces** – Throughout its product line, Juniper Networks provides a consistent user interface in both the WebUI and the Command Line Interface (CLI). There is no need to install a management station with special software and complex configurations. Simply use an Internet browser, and you are ready to configure, modify, and monitor the device via the built-in user interface.

- **Fully Featured Command Line Interface (CLI)** – Juniper Networks firewall/VPN devices offer fully featured CLI for configuration and management, accessible through ssh, telnet and a serial port. The CLI can easily adapt to the use of custom scripts for configuring and managing your devices.

**Setting Up a Basic Firewall**

Before you begin any setup, it is important to gather pertinent information that will speed the configuration process. We list this information to help provide an understanding of what you will experience during this installation:

We will configure our first firewall installation to accomplish the following connectivity:

- **Network One (Trusted)** – We will define our first network as 192.168.1.0/24. We will use this to represent the internal network.
  - IP address of the trusted interface on the firewall is 192.168.1.2/24
  - IP address of PC-1 connected to the trusted interface will be 192.168.1.33/24 (assigned by DHCP Server on the NetScreen-5XT)

- **Network Two (Untrusted)** – We will define our second network as 172.16.10.0/24. We will use this to represent the external network.
  - IP address of the untrusted interface on the firewall is 172.16.10.2/24. In a typical deployment, your Internet service provider assigns the configuration information for the untrusted interface. Depending on the type of access service you have, this information can be a static IP address (as in our example), a DHCP assigned IP address (used by most cable providers), or a PPPoE assigned IP address (used by most DSL providers).
  - IP address of PC-2 connected to the untrusted interface will be 172.16.10.1/24

- **Desired end result**—Connect the two networks in such a way that:
  - The Trusted network (192.168.1.0/24) has full access to the Untrusted network.
  - The Untrusted network (172.16.10.0/24) has no access to the Trusted network.
Our first firewall configuration will use the Initial Configuration Wizard. This is a self-guided and easy to use configuration tool. By referring to the information we listed above, we can step through this process and have our NetScreen-5XT connected and working as a firewall in less than 10 minutes.

To skip the Initial Configuration Wizard and launch the WebUI directly, you will need to access the device via a telnet connection, modify the Trust Interface IP address and issue a Save Command from the CLI.

**To skip the Initial Configuration Wizard:**

- Start on PC-1 a Telnet session to 192.168.1.1
- At the Remote Management Console, enter netscreen for the login name and password
- Enter the CLI command: `set interface trust ip 192.168.1.2/24`
  - We set the new IP address to 192.168.1.2 because we want this NetScreen-5XT Trusted interface to be different from the default IP address.
- Enter the CLI command: `save`
- Exit and close your Telnet session

For an overview of the WebUI, skip to Section 0, “The WebUI, Juniper Networks Graphical User Interface,” on page 12. Otherwise, continue using the configuration wizard and your Internet browser to set up your Juniper Networks firewall with the steps below.

**Set up the initial connectivity on the Juniper Networks NetScreen-5XT**

The basic physical connectivity for this is quite simple:

- Connect an RJ-45 Ethernet cable from the Ethernet port on PC-1 to the Trusted 1 port on the NetScreen-5XT.
- Connect an RJ-45 Ethernet cable from the Ethernet port on PC-2 or a port on the traffic generator, mentioned in the “
What You Will Need” section on page 4) to the **Untrusted** port on the NetScreen-5XT.

- Connect the NetScreen-5XT to a power source.
- Change the TCP/IP settings of your PC-1 so that it obtains its TCP/IP settings automatically through DHCP. (Consult the documentation for your operating system if necessary.)
- Verify your new IP configuration. For Windows-based systems, open a command window and run `ipconfig`. The IP address of the Trusted computer should be **192.168.1.33**, assigned by the Juniper Networks device.
- Close the command window.
- Next, open your Internet browser. All further description is done showing the browser Interface. In this Guide, we use Microsoft Internet Explorer version 6.0.

**Log in to the Juniper Networks device**

Open your browser to the default address of the Juniper Networks device: **http://192.168.1.1**. The Juniper Networks NetScreen Rapid Deployment (NSRD) Configuration Wizard appears and asks if you have a “start-up” file.

NSRD is a Juniper Networks process designed to ease the installation of large numbers of remote devices. The Juniper Networks devices automatically interact with the Juniper Networks NetScreen-Security Manager, our centralized management system. When using NSRD, the system administrator provides a user with a startup file that contains a minimum configuration. The user uploads this file to the Juniper Networks remote device. The remote device connects over the network to NetScreen-Security Manager and retrieves a complete configuration file. In this way, NSRD greatly simplifies the deployment of a large number of remote devices and eliminates the need to have IT experts on site for the installation of remote devices.

For the purposes of this evaluation, we will bypass this screen, and continue with the Initial Configuration Wizard. Click **Next>>** to continue.

The Initial Configuration Wizard starts and prompts you for an administrator’s login name and password. You can enter any name and password here, however, for the purposes of this evaluation, enter the default of **netscreen** for both the login name and password. These can be easily changed once the Initial Configuration is complete.
After you have typed your login name and password, click **Next>>**.

**Make decisions about the type of connectivity**

The Juniper Networks Initial Configuration Wizard then asks you to decide the connectivity mode that you want, either Network Address Translation (NAT) Mode or Route Mode. In NAT Mode, the Juniper Networks firewall performs address translation to all traffic going from the Trust Zone to the Untrust Zone, as it assumes that the devices connected to the Trust Zone are using private IP addresses, which cannot be routed on the Internet. In Route Mode, the Juniper Networks firewall does not do address translation by default.

Since NetScreen-5XT’s are commonly deployed in small offices or home office environments, where the Internet Service Provider (ISP) assigns a single IP address, we will use the default NAT Mode deployment option, which best illustrates this environment. Choose **NAT Mode** and click **Next>>**.
Once you have chosen your deployment mode, you are presented with a list of Operational Mode offerings: Trust-Untrust Mode, Home-Work Mode, and Dual-Untrust Mode. These offerings represent the variety of Security Zone options available from the NetScreen-5XT device. You can simply choose the Operational Mode that best fits your environment.

In Trust-Untrust Mode, you are offered four Trusted Ethernet ports to host PC’s or other devices in a “Trusted Zone” and a single Untrusted Ethernet connection in the “Untrust Zone” to face the Internet.

In Home-Work Mode, Ethernet Ports 1 and 2 are assigned to the “Work” Security Zone, while Ethernet Ports 3 and 4 are assigned to the “Home” Security Zone. The benefit here is the built-in isolation feature of Juniper Networks Security Zones. The Work Zone is completely isolated from the Home Zone, thus enhancing the security of the devices in each zone.

In Dual-Untrust Mode, Ethernet Port 4 is moved to the “Untrust” Zone, while Ethernet Ports 1, 2, and 3 remain in the “Trust” Zone. This provides the added benefit of being able to support a second high speed Internet connection for resiliency.

For our testing, choose the default Trust-Untrust Mode and click Next>.

Define your IP addresses and DHCP configuration
Next you are asked to define how the NetScreen-5XT device connects to the Internet. Choose **Static IP**, and then enter the IP address, netmask and gateway for the Untrust interface. Since we decided to use **172.16.10.2** for the Untrust interface, enter the appropriate values here:

In this case, we have defined our Untrust interface IP with an address of **172.16.10.2**, a 24-bit Netmask (**255.255.255.0**) and a Gateway of **172.16.10.1**. The Gateway address is actually the IP address of the routing device that will interconnect the Juniper Networks and the Internet. In this first example however, this will be the IP address of PC-2 or the traffic generator port connected to the Untrust Interface.

Now we configure the Trusted Zone IP address. We set the new IP address to **192.168.1.2**.

Click **Next>>** to confirm and move to the next screen. Next you are asked if you want to enable a DHCP server and configure the address range that you want it to assign. We will select **Yes** and define a range of addresses between **192.168.1.33** (the IP address your workstation is currently using) to **192.168.1.126**, as these are the factory defaults, and click **Next>>** to move to the review screens.
Review your configuration and save it

The NetScreen-5XT device next shows you a summary screen with all of the configuration choices you have made on it. Review each item to ensure it meets your installation requirements. At this time you can scroll back to any of the previous screen and make any modifications necessary by simply using the <<Previous button. Also note that the CLI commands appear on this screen, describing how you could have used the CLI to achieve the same results. With Juniper Networks firewall/VPN devices, you can easily switch from the WebUI to the CLI. When you have finished your review, click >>Next and the configuration will be saved to the Juniper Networks device.

Click Finish on the next page and close your browser.

Review your progress

Look at the previous illustration, and consider this: you have successfully configured a firewall in only minutes. The Juniper Networks device makes a formerly complex process a straightforward and easy process.

The WebUI, Juniper Networks Graphical User Interface

You have arrived to this step by either configuring your NetScreen-5XT through the Initial Configuration Wizard, or by taking the steps outlined to bypass the Wizard. Since you will use the WebUI for future interaction with the NetScreen-5XT, this section presents you with a brief overview of how to navigate the WebUI.

From PC-1 open an Internet browser window and open http://192.168.1.2, which is the address that you use for the Trusted interface of the NetScreen-5XT. Log in with the login name and password of netscreen.
The left panel provides a list of the menu commands available to you. Commands with a plus (+) sign next to them indicate that further commands appear beneath. Click on the command or the plus sign to open that menu. In the exercises that appear in this Guide, we refer to these commands in bold font. If several menus are to be opened, you see those commands separated by the “>” symbol. For example, **Objects> Addresses>List** means to open the **Objects** menu, click on the **Addresses** menu choice, and then click **List**. You can choose to see these command choices with graphical icons by clicking **Toggle Menu**. In our examples, we use the version shown above.

Depending upon the task you have chosen on the left panel, the center panel shows the relevant information. In the Home menu choice, you see an overview of your Juniper Networks device and the environment in which it is operating. This includes System Status, Interface Link Status, a list of the most recent Alarms, and a log of recent Events.

**The WebUI Menus – Powerfully Simple**

The WebUI menus and the command line interface *both* give you full access of the Juniper Networks functionality. We summarize the WebUI menus below. Remember that every action taken at the WebUI can also be completed with the CLI. The menus are:

- **Configuration** – Use these options to configure date/time, administration, upload configuration files and ScreenOS firmware, authentication and report settings.
- **Network** – Use these options to assign DNS settings, create zones, add IP addresses, configure DHCP and PPPoE as well as to set up routing and redundancy parameters.
- **Screening** – Use these options to enable predefined attack protections, malicious URL protection, antivirus configuration and URL filtering.
- **Policies** – Use this to create, modify or delete security policies.
- **VPNs** – Use these options to create Manual or AutoKey IKE VPN links to other devices.
- **Objects** – Use these options to view and configure device specific objects such as IP address book entries, predefined and custom services, user information, IP pools and certificates.
- **Reports** – Use these options to view system and policy logs, interface hardware and flow counters as well as screening counters.
- **Wizards** – Use these to quickly configure policies or VPNs.
Configuring a Layer 3 Firewall with the WebUI

You may skip this section and proceed to Section 0, “Testing Your Juniper Networks Firewall,” on p. 15, only if you have successfully run through the Initial Configuration Wizard.

Our next step in setting up our firewall will be to assign IP addresses to our Interfaces. To do this, open your web browser to your Juniper Networks device, at 192.168.1.2. Then open the Networking>Interface Menu choice.

Notice the trust interface already has the IP address we assigned earlier. We simply need to add an IP address to the untrust interface at this point. To do so, click Edit for the untrust interface.

Enter the IP address of 172.16.10.2 and 24 for the Netmask. Ensure that the Interface Mode is Route and then click Apply. Your screen should look like the one above.

You must configure a default route that directs non-local traffic to the appropriate network. To do this, open Routing>Route Table and then click New.
Since we want to send all non-local traffic out the untrust interface, the Network Address should be 0.0.0.0 and the Netmask is also 0 (default route). Select Gateway option, choose untrust for the Interface and type in 172.16.10.1 as the IP address of the Gateway. This is the IP address to either the traffic generator or to PC-2, which is connected to the Untrusted Interface.

The IP addresses and the default route are configured in the NetScreen-5XT. There is already a default policy on the device that allows all outbound traffic, so we ready to test our newly configured firewall.

CLI Interface commands.

```
set admin password "netscreen"
set interface untrust ip 172.16.10.2 255.255.255.0
set interface untrust gateway 172.16.10.1
set interface trust ip 192.168.1.2 255.255.255.0
set interface trust manage
unset dhcp server ip all
set interface trust dhcp server ip 192.168.1.33 to 192.168.1.126
```

Testing Your Juniper Networks Firewall

It is now time to test your new firewall. If you have a traffic generator, connect it to the NetScreen-5XT, as described below. If you do not have a traffic generator, skip to the section on Testing between personal computers on page 15.

Testing with a traffic generator

To test with a traffic generator, we will connect one port on the traffic generator to the Trusted 1 interface on the NetScreen-5XT, and a second port on the traffic generator to the Untrusted interface, as shown in the following illustration (using an IXIA Traffic Generator):
• Configure your traffic generator Application. Consult your local reference guide for specific details.

• Configure the address on the IXIA port connected to the **Trusted 1** interface with address 192.168.1.33 and gateway 192.168.1.2.

• Configure the address on the IXIA port connected to the **Untrusted** interface with address 172.16.10.1 and gateway 172.16.10.2.

• Set your traffic flow direction, in this case from the **Trusted 1** interface to the **Untrusted** interface.

• Choose your traffic pattern and file size. In our first test, almost any IP traffic type can be used, but we recommend you start with UDP, ICMP, or HTTP. A file size of 1400 bytes is a good starting point.

• Start the traffic flow and observe the results within the traffic generator application.

**Testing between personal computers**

To test the NetScreen-5XT with two personal computers, your network looks like the diagram below, with PC-1 plugged into the **Trusted 1** interface and PC-2 plugged into the **Untrusted** interface:

![Diagram of a network setup with PC-1 and PC-2 connected to the trusted and untrusted interfaces of a NetScreen-5XT firewall.]()  

Connect your PC-2 to the Untrusted interface and set its IP configuration to:

- **IP Address:** 172.16.10.1  
- **Netmask:** 255.255.255.0  
- **Gateway:** 172.16.10.2

Consult the Windows operation system documentation for guidelines on how to change the IP addresses. At this point, you have the connectivity you want:

- The **Trusted network** (192.168.1.0/24) has full access to the **Untrusted network**.
- The **Untrusted network** (172.16.10.0/24) has no access at all to the **Trusted network**.

Attempt to ping the IP address of PC-2. Issue the command `ping 172.16.10.1` from PC-1.

PC-2 should be running a web server, as detailed in the “What You Will Need” section. From PC-1, start an Internet browser and open [http://172.16.10.1](http://172.16.10.1). All succeed, as they should.

Trust to Untrust is allowed by the NetScreen-5XT firewall. Now, let’s try to send traffic in the opposite direction. Try to ping PC-1 from PC-2 by issuing the command `ping 192.168.1.33` on PC-2.
This ping command should fail. The NetScreen-5XT does not permit traffic to pass unless you explicitly allow it in the security policy.

Next, we go to the WebUI and modify the service type on the default policy and observe the effect on our outbound traffic.

**Modify the firewall rule and test it**

- Open **Policies**, and select **Edit** on the existing policy.

- Click on the **Service** list box to see your choices for this policy.

In this case, we are allowing the PING service only. Choose PING from the Service list, optionally give your policy a name (optional), and click **OK**. A review of your policies shows the new setting:

Test that the PING packets still traverse your network from the Trusted Zone to the Untrusted Zone. Do this either by changing the protocol type on your traffic generator to ICMP or by running `ping 172.16.10.1` from PC-1. Test HTTP traffic by either setting the protocol type to HTTP on your traffic generator, or by opening an Internet browser window on PC-1 to `http://172.16.10.1`. What happens?
When you are finished testing, return the default policy service to the default of **ANY**. This simple test demonstrated how easy it is to modify policies on the Juniper Networks device to control outbound access. With a few clicks of the mouse inside the WebUI, you can create as strict or as open an access policy as you want.

## Configuring the Deep Inspection Firewall

Juniper Networks Deep Inspection firewall integrates intrusion prevention technology into the firewall to provide application-level attack protection at the network perimeter. The Deep Inspection firewall can efficiently perform network security functions as well as analysis on the application message to determine whether to accept or deny traffic.

Juniper Networks Deep Inspection technology applies a deeper level of application understanding to the traffic to make access control decisions based on the intent of that traffic. The Inspection firewall focuses on preventing application-level attacks aimed at Internet-facing applications, such as Web, e-mail, FTP and DNS. It eliminates application-level ambiguities, performing de-fragmentation, reassembly, scrubbing and normalization, to convert network packets to application-level messages. It then looks for protocol conformance and attacks patterns. The Deep Inspection then decides to accept or deny the traffic based on high impact protocol anomalies or any given attack pattern. The Deep Inspection firewall can block application-level attacks at the Internet gateway so they never reach their destination.

To enable the Deep Inspection firewall, you need to register your NetScreen-5XT with Juniper Networks and obtain a Deep Inspection license key. Please note that you are entitled to obtain a Deep Inspection license key with the product at no additional cost. However, you will need to subscribe to the Deep Inspection Signature Service to obtain regular updates of the Deep Inspection attack database.

To test the Deep Inspection firewall, we’ll use the same network setup as the one created in the Section **Setting Up a Basic Firewall**. The diagram below shows the setup for the NetScreen-5XT, PC-1 and PC-2 and their respective IP addresses.

![Network Diagram](image)

### Loading the Deep Inspection License Key and Attack Database

Once you have registered your NetScreen-5XT and have submitted your request for a Deep Inspection license key, CSO automatically emails you a license key. You will use this license key to enable the Deep Inspection engine in the NetScreen-5XT.

To load the license key, open an Internet browser window in PC-1 to 192.168.1.2.
- Open **Configuration>Update>ScreenOS/Keys**, and select **License Key Update (Features)** on the top options.

- Click the **Browse...** button and load the license key file that you received via e-mail from Juniper Networks.

Once you load the license key, you need to upload the initial Deep Inspection attack database from Juniper Networks update servers.

Open **Configuration>Update>Attack Signature** screen.
• In the Database Server field, type 
  https://services.netscreen.com/restricted/sigupdates
• Click the Update Now button to download the latest Deep Inspection attack database from 
  Juniper Networks update servers.
• Verify that a new Deep Inspection attack database has been loaded into your NetScreen-5XT by 
  making sure that the Current Version of the Deep Inspection Signature Update is greater than 0 
  (at the top of the Attack Signature screen).

Note that you can configure your NetScreen-5XT to automatically download the latest Deep Inspection 
attack database on regular intervals (i.e., once a day). With constant updates, your network will be 
protected from the latest security threats, without you having to manually configure each security device 
to stop a new worm that is rapidly spreading across the Internet.
Enabling Deep Inspection in the Default Policy

Now that you have loaded Deep Inspection license key and the latest Deep Inspection attack database, it is time to enable Deep Inspection in a policy.

To set up Deep Inspection in your NetScreen-5XT’s default policy, open an Internet browser window in PC-1 to 192.168.1.2.

- Open Policies, and select Edit on the existing policy.

- Click on the Deep Inspection button to see the configuration options for Deep Inspection in this policy.

- Add all the Attack Groups to this policy by selecting all the Attack Groups on the left list and clicking the << button. To select all the entries, click the first Attack Group, hold the Shift key pressed, scroll down the list, and click on the last Attack Group.

- Select None for the Action, mark the Alert checkbox, and click OK to close the window.

You have now configured the NetScreen-5XT to perform Deep Inspection on the default outgoing policy. Since the Action is set to None, the NetScreen-5XT will inspect the traffic to detect application level attacks, but will not drop the traffic or close the connection when it sees an attack. You have added all Attack Group objects, thus instructing the NetScreen-5XT to detect the most common application-level attacks at the Internet gateway.
Testing the Deep Inspection Firewall

To test the Deep Inspection firewall in the NetScreen-5XT, you’ll launch simple attacks at the web server running on PC-2. The attacks selected for this Guide can be easily carried out using an Internet browser. In the first example, we will attempt to exploit a directory traversal vulnerability. Using this attack, a remote attacker could send a specially-crafted URL request containing "dot dot" sequences (/../) to traverse directories and view/run arbitrary files on a Web server, including viewing files with IDs and passwords. To find out the list of web servers vulnerable to this type of attack, search the CVE database for “directory traversal” at www.cve.mitre.org.

- To run a directory traversal attack, open an Internet browser window on PC-1 and type in the URL field: http://172.16.10.1/../

The NetScreen-5XT detects the directory traversal attempt and logs the attack. To view the log entries, open your Internet browser on PC-1 to 192.168.1.2.

- In the NetScreen-5XT Home page, under The most recent alarms title, click on the More... link to view recent attacks detected by the Deep Inspection firewall.

While reviewing the log entries, note that the NetScreen-5XT was able to detect the directory traversal attempt that we just launched.

The second attack that we will test is the Unicode Encoded Directory Traversal attack, which attempts to hide the “../” string by using a Unicode equivalent string. For instance, the Unicode equivalent of “/” is “%c0%af”. Unpatched Microsoft IIS 4.0 and IIS 5.0 servers may be vulnerable to this attack².

---
² CVE-2000-0884: Microsoft IIS 4.0 and 5.0 vulnerability via malformed URLs that contain UNICODE encoded characters
To run the Unicode Encoded Directory Traversal attack, open an Internet browser window on PC-1 and type in the URL field: \texttt{http://172.16.10.1/..%c0%af}

The NetScreen-5XT detects the directory traversal attempt and logs the attack. To view the log entries, open your Internet browser on PC-1 to 192.168.1.2.

- In the NetScreen-5XT Home page, under \textbf{The most recent alarms} title, click on the \textit{More}... link to view recent attacks detected by the Deep Inspection firewall.

For the Unicode Encoded Directory Traversal attack, two alarms are generated in the NetScreen-5XT: a protocol anomaly alarm due to exceedingly long UTF8 codes in the HTTP request and a protocol anomaly alarm for a HTTP directory traversal attempt.

In the third attack, we attempt to exploit the vulnerability in filename processing of the CGI program in Microsoft IIS 4.0 and 5.0\textsuperscript{3}. The CGI program incorrectly decodes the filename string twice. Exploitation of this vulnerability may allow remote attackers to run an arbitrary system command. By using malformed CGI filenames, attacker can get around filename check-ups, like the "../" or "./" check-up, thus directory traversal attacks may be executed. The 3-character Unicode for "\%" is "\%25" and for "\" is "\%5c". Since the CGI filename is decoded twice, the string "\%255c" is actually interpreted as "\".

- To run the Double Encoding attack, open an Internet browser window on PC-1 and type in the URL field:

\texttt{http://172.16.10.1/scripts/..%255c..%255cwinnt/system32/cmd.exe?/c+dir+c}

This maliciously crafted URL attempts to execute a directory listing of the root directory in a Windows server. The NetScreen-5XT detects the double encoding and the directory traversal attempts and logs the attacks. To view the log entries, open your Internet browser on PC-1 to 192.168.1.2.

\textsuperscript{3} CVE-2001-0333: Microsoft IIS 5.0 and earlier vulnerability via encoding characters twice
In the NetScreen-5XT Home page, under The most recent alarms title, click on the More... link to view recent attacks detected by the Deep Inspection firewall.

The NetScreen-5XT displays two alarms for this event: a protocol anomaly alarm due to double encoding in the HTTP request and a protocol anomaly alarm for a HTTP directory traversal attempt.

**Testing the Deep Inspection Firewall with Action to Close**

In our fourth test of the Juniper Networks Deep Inspection firewall, we'll change the Action in the Deep Inspection policy to Close the session. With this action, the Deep Inspection firewall will stop attacks before they reach their victims by dropping the malicious packets and immediately closing the session.

We recommend that you deploy the Deep Inspection firewall with Action to None for a few weeks and review and research the alarms generated by it. You’ll want to make sure that the Attacks triggered represent a real threat to your network. Consider that some Attack Objects may generate false alarms, as certain traffic in your network may not precisely comply with standard protocol specifications. You should investigate the triggered Attack Objects and remove all Attack Groups that generate false alarms before you attempt to enable any Action different from None.

In this test, we’re going to create a policy for FTP traffic with a Deep Inspection action of Close. To create the policy, open your Internet browser on PC-1 to 192.168.1.2.

- Choose Policies. Use the list box to set the policy to go from Trust to Untrust and click the New button.
- Select FTP in the Service field and click the Position at the Top checkbox.
• Click on the **Deep Inspection** button to select the Attack Groups for this policy

![Deep Inspection Configuration](image)

• Add the 5 Attack Groups associated with the FTP service into the Selected Members list on the left by selecting the appropriate Attack Groups on the Available Members list on the right and clicking the << button.

• Select **Close** Action, mark the **Alert** checkbox, and click the **OK** button.

• Click **OK** on the policy screen to save the policy configuration

You should have two policies in your NetScreen-5XT: the top policy that allows FTP traffic with a Deep Inspection action of **Close** and the bottom policy that allows ANY traffic with Deep Inspection action of **None**. Since security policies are evaluated in strict order, FTP traffic will only match the top policy.

We'll attempt to login to the FTP server running on PC-2 with an invalid login name or password, which triggers the FTP:REQERR:LOGIN-FAILED Alert Object. This alarm is used to identify a remote attacker attempting to login using brute force.

• To login to an FTP server using a invalid login name or password, open a command prompt window on PC-1 and type in `ftp 172.16.10.1`

![Command Prompt](image)

• Login as **root** and password **xyz**

Note that NetScreen-5XT’s Deep Inspection firewall immediately closed the FTP connection after it detected the failed login. To view the log entries, open your Internet browser on PC-1 to 192.168.1.2.
In the NetScreen-5XT Home page, under **The most recent alarms** title, click on the More… link to view recent attacks detected by the Deep Inspection firewall.

When you are finished testing, delete the FTP policy. From the menu on the left, choose **Policies**, and click the **Remove** link in the policy for the FTP service, which should be at the top of the list.

**Review your work**

We have shown how you can use Juniper Networks Deep Inspection firewall feature to protect your network against the most common application-level attacks at the Internet gateway. You were able to configure the Deep Inspection firewall to detect and/or stop application-level attacks. Juniper Networks Deep Inspection provides granular control regarding what Attack Objects to look for and what actions to take in each policy.

We mainly used the WebUI to set up the Deep Inspection firewall in the NetScreen-5XT. Note that you can also configure the Juniper Networks Deep Inspection firewall using CLI commands and obtain the same results.

**Setting Up a Layer 3 Firewall on the Second Juniper Networks Device**

Setting up the second NetScreen firewall/VPN device is almost the same as setting up the first one. In this example, we are using the NetScreen-50 to represent our Corporate Office. We will configure the NetScreen-50 to accomplish the following connectivity:

- **Network Two (Untrusted)** – We will define our second network in the **172.16.10.0/24** space. We will use this to represent the Internet, or other untrusted addresses.
- **Network Three (Trusted)** – We will define our third network in the **10.0.0.0/24** space. We will use this to represent the Corporate network.
- **Desired end result** – Connect these two networks to our existing NetScreen-5XT network in such a way that:
  - The Trusted network (**10.0.0.0/24**) has full access to the Untrusted network.
  - The Untrusted network (**172.16.10.0/24**) has no access to the Trusted network.
We will accomplish this configuration by following these steps:

- Set up the initial connectivity
- Log in to the Juniper Networks device with PC-1
- Configure basic options using the built-in “Initial Configuration Wizard”
- Rewire our network to mirror the diagram above
- Configure other options using the WebUI

Unlike the Initial Configuration Wizard on the NetScreen-5XT, the NetScreen-50’s Initial Configuration Wizard will only walk you through basic IP address configuration for the default Security Zones, and DHCP Server settings, should you wish to utilize the Juniper Networks device as your DHCP server. You will need to configure the firewall functionality, as detailed in the section following the Initial Configuration Wizard section.

We will start by connecting the port E1 of the NetScreen-50 to one of the unused Trusted Ethernet ports on the NetScreen-5XT. Remember that we changed the default NetScreen-5XT’s Trusted IP address to 192.168.1.2. This will allow us to connect our next Juniper Networks device to that trusted network and access it via its default IP address of 192.168.1.1 without having duplicate addresses in the NetScreen-5XT’s Trusted Zone.

To skip the Initial Configuration Wizard and launch the WebUI directly, you will need to access the device via a telnet connection and issue a Save Command from the CLI.

**To skip the Initial Configuration Wizard:**

- Start a Telnet session to 192.168.1.1
- At the Remote Management Console, enter netscreen for the login name and password
- Enter the CLI command: set interface ethernet1 ip 10.0.0.2/24
- Enter the CLI command: save
- Exit and close your Telnet session

You should now proceed to Section 0, “Configuring the Layer 3 Firewall on the Second Juniper Networks Device with the WebUI”, on page 29.

**Log in to the Juniper Networks Device**

From PC-1, open your browser to the default address of the Juniper Networks device: http://192.168.1.1. Since we changed the IP address of the NetScreen-5XT to 192.168.1.2, so we go straight to the NetScreen-50. The Juniper Networks NetScreen Rapid Deployment (NSRD) Configuration Wizard appears and asks if you have a “start-up” file.
Skip the NSRD by clicking **Next>>**. The Initial Configuration Wizard starts and presents a Welcome screen. Click **Next>>** to start the Initial Configuration Wizard. You will be prompted for an administrator's login name and password. You can enter any name and password here, however, for the purposes of this evaluation, enter the default of `netscreen` for both the login name and password. These can be easily changed once the Initial configuration is complete.

After you have typed your login name and password, click **Next>>**.

**Bind interfaces to zones**

The NetScreen-50 next asks you to bind interfaces to security zones. You have the option of binding a single interface or multiple interfaces to each security zone. The flexibility of this architecture is easily realized. Implementing a network topology change is a simple task. For example, to add a new network segment, just bind an interface to an existing security zone and then connect the new network segment to that interface. Polices for this security zone are already in place, and the new network segment will automatically inherit these policies.
We will only be using ethernet1 and ethernet3 in our configuration. You should place ethernet2 into the Null zone using the list box. When you complete these choices, click Next>>.

Juniper Networks also recommends to leave the ethernet4 interface unused and to assign it to the High Availability (HA) Zone when needed. Interfaces in the HA zone can be used to link a pair of identical Juniper Networks devices to enable device redundancy. Should anything unforeseen happen to your primary device or any of its interfaces, the second device connected via the HA link takes over seamlessly. Since configurations, session state, and VPN tunnel state are synchronized over the two HA devices, there is basically no downtime in the event of a device or link failure.

Configure the interface IP address and netmask

Next the Juniper Networks Initial Configuration Wizard asks you to input the IP address and Netmask for the two interfaces that you are configuring:

<table>
<thead>
<tr>
<th>Interface</th>
<th>Zone</th>
<th>IP / Netmask</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet1</td>
<td>Trust</td>
<td>10.0.0.2/24</td>
</tr>
<tr>
<td>ethernet3</td>
<td>Untrust</td>
<td>176.16.10.1/24</td>
</tr>
</tbody>
</table>

Enter 10.0.0.2/24 for ethernet1, your Trust zone, and 176.16.10.1/24 for Ethernet 3, your Untrust zone. When you complete filling out this dialog box, click Next>>.

Define your DHCP configuration

Next you are asked if you want to enable the DHCP server. Since many corporate networks usually have a DHCP server deployed in the environment, we will select No, and click Next>> to move to the review screens.
Review your configuration and save it

The Juniper Networks device next shows you a summary screen with all of the configuration choices you have made on it. Note that the CLI commands also appear on this screen, describing how you could have used the CLI to achieve the same results. With Juniper Networks firewall/VPN devices, you can easily switch from the WebUI to the CLI.

Click **Next>>** to apply your new configuration and click **Finish** at the last screen Close your browser.

Configuring the Layer 3 Firewall on the Second Juniper Networks Device with the WebUI

Next we will set up the basic firewall configuration on the NetScreen-50 device. Connect PC-2 to E1 (ethernet1) of the NetScreen-50. Connect E3 (ethernet3) of the NetScreen-50 to Untrust on the NetScreen-5XT. Your network should now mirror the following diagram:

Set the IP address on PC-2 in order to access the NetScreen-50’s WebUI. The IP configuration on PC-2 connected to port E1 should be:

- **IP Address:** 10.0.0.33
- **Netmask:** 255.255.255.0
- **Gateway:** 10.0.0.2

Consult the Windows operation system documentation for guidelines on how to change the IP address.
Begin by opening an Internet browser window on PC-2 to http://10.0.0.2, the IP address you configured earlier for this device. When prompted, login using your netscreen for user name and password. The NetScreen-50 WebUI shows you the home screen.

**Set up your routing**

Start by setting up the routing. From the menu on the left, choose **Network>Routing>Routing Table**. You will see the route entries that currently are on your system.

You must configure a default route that directs non-local traffic to the appropriate network. To do this, click **New**.

Since we want to send all non-local traffic out the untrust interface, our Network Address should be 0.0.0.0 and the Netmask is 0 (default route). Select **Gateway** option, choose **ethernet3** (our interface in the Untrusted Zone) for the Interface and type in 172.16.10.2 as the IP addresses of the Gateway. Note that this is the IP address of our NetScreen-5XT’s Untrust interface.
Set your access policy

The final step is to apply a policy to allow traffic from our Trusted zone to the Untrusted zone. From the menu on the left, choose Policies. Use the list box to set our policy to go from Trust to Untrust and select New to be presented with the policy screen below.

The default selections will allow all traffic from the Trust Zone to the Untrust Zone, so select OK.

The IP addresses, the default route and the default firewall policy are all configured in the NetScreen-50. In the next section we set up a VPN tunnel between our two Juniper Networks devices using the VPN Wizard.

**CLI Commands:**

```bash
set admin password "netscreen"
set interface ethernet1 zone Trust
set interface ethernet1 ip 10.0.0.2 255.255.255.0
set interface ethernet1 manage
set interface ethernet2 zone Null
set interface ethernet3 zone Untrust
set interface ethernet3 ip 172.16.10.1 255.255.255.0
unset interface ethernet3 manage
set interface ethernet4 zone Null
set interface vlan1 manage
set policy from "Trust" to "Untrust" "Any" "Any" "Any" permit
set route 0.0.0.0/0 interface ethernet3 gateway 172.16.10.2
save
```
Setting Up a VPN between Two Juniper Networks firewalls

We will now set up a VPN tunnel between two Juniper Networks devices, using the built-in VPN wizards. When finished, the new network will look like this:

The network diagram looks very similar to our previous example. However, notice that in this diagram there is a “tunnel” between the two devices, across the Untrust Zone. This tunnel represents a secure path, over which encrypted data traverses non-secure networks, such as the Internet, to arrive at the destination gateway.

Setting up a VPN on the First Firewall Using the VPN Wizard

To set up a VPN tunnel, start the VPN Wizard on the NetScreen-5XT device first. Using PC-1 directly connected to the NetScreen-5XT, start an Internet browser window and open http://192.168.1.2. Login using the default user name and password and from the left menu click Wizards>Routing-based VPN. The VPN Wizard displays the first screen, prompting you for the type of VPN that you want to create:

Choose Trust for your Local site and Untrust for your remote site, the default choice, and then click Next>>. The Juniper Networks device prompts you for the binding that you want for this VPN:
Choose **New tunnel interface**, and bind it to the untrust (trust-vr) interface. Then click **Next>>**. The Juniper Networks device asks you for the type of VPN that you want:

LAN-to-LAN VPN tunnels are used to interconnect with another VPN hardware device, typically providing secure connectivity to various systems in either side of the tunnel. Dialup-to-LAN VPN tunnels are used to connect with a remote dialup client. Juniper Networks firewall/VPN devices support in the same system both LAN-to-LAN and Dialup-to-LAN tunnels.

We are setting up an LAN-to-LAN tunnel, so click **LAN-to-LAN** and click **Next>>**. Now the Juniper Networks device asks you to be more specific about the IP address types:
As you can see, broad flexibility has been incorporated into the Juniper Networks VPN features. We can support Static IP to Static IP, Static IP to Dynamic IP or Dynamic IP to Static IP configurations. In this case, we are connecting devices with statically assigned IP addresses on their Untrust interfaces, so click **Local Static IP <-> Remote Static IP** and click **Next>>**. Now the Juniper Networks VPN Wizard asks us for the IP address of the remote system:

![VPN Wizard](image)

The device we want to set up the VPN tunnel with is NetScreen-50, with the IP address of **172.16.10.1** on its untrusted interface. Enter that address and click **Next>>**. You are now prompted for the security level for your VPN tunnel.

![VPN Wizard](image)

By default, the Juniper Networks device offers you two encryption choices: a **Compatible** choice, which will work with many third-party IPSec VPN devices, or a **Standard** choice, which uses only long encryption keys (128-bit encryption keys for AES or 168-bit encryption keys for 3DES). In either configuration, the NetScreen-5XT accelerates encryption algorithms in hardware to maintain high performance. Choose **Standard** for a higher security level for this VPN tunnel, and enter your shared secret. We will use **netscreen** for our shared secret.

Click **Next>>**. Now you are prompted for the source and remote addresses of the networks that you want to interconnect. Fill in the dialog box with addresses of **192.168.1.0/24** for your local address and **10.0.0.0/24** for the remote address:
Click **Next>>**. You will be prompted for the type of service:

Choose **ANY** and **Both direction**, and then click **Next>>**. You will be prompted to decide on logging, counting, and alarms:

Choose **Logging**, and click **Next>>**. You will be prompted for a schedule. We don’t want to set a schedule at this time, so simply click **Next>>**.

Now you are prompted with a confirmation screen, showing the choices you have made in this VPN Wizard. Review them and click **Next>>** to continue. Now the VPN Wizard
presents a summary of all of your choices, along with the CLI commands that you could have used to accomplish the same task:

```plaintext
You can click Create another VPN or you can Finish. We're done with the VPN tunnel configuration on the NetScreen-5XT at this point, so click Finish. Your Juniper Networks VPN Wizard concludes and closes your session.

CLI Commands:

set interface tunnel.1 zone Untrust
set interface tunnel.1 unnumbered interface untrust
set ike gateway "Gateway for 10.0.0.0/24" ip 172.16.10.1 outgoing-interface
untrust preshare "netscreen" sec-level standard
set vpn "VPN for 10.0.0.0/24" gateway "Gateway for 10.0.0.0/24" replay
sec-level standard
set vpn "VPN for 10.0.0.0/24" bind interface tunnel.1
set address Trust 192.168.1.0/24 192.168.1.0/24
set address Untrust 10.0.0.0/24 10.0.0.0/24
set policy top from "Trust" to "Untrust" "192.168.1.0/24" "10.0.0.0/24"
"ANY" Permit log
set policy top from "Untrust" to "Trust" "10.0.0.0/24" "192.168.1.0/24"
"ANY" Permit log
set route 10.0.0.0/24 interface tunnel.1
save
```

**Setting up a VPN on the Second Firewall Using the VPN Wizard**

Start the VPN Wizard on the NetScreen-50 device. Using PC-2 that is directly connected to the NetScreen-50, start an Internet browser window and open http://10.0.0.2. Login using the default user name and password and from the left menu click Wizards>Routing-based VPN. The VPN Wizard screens are almost the same as the ones for the NetScreen-5XT.
The VPN Wizard displays the first screen, prompting you for the location of the local and remote site of VPN tunnel that you want to create:

![VPN Wizard](image)

Choose Trust for your Local site and Untrust for your remote site, the default choice, and then click Next>>. The Juniper Networks device prompts you for the binding that you want for this VPN:

![VPN Wizard](image)

Choose New tunnel interface, and bind it to the ethernet3 (trust-vr) interface. Then click Next>>. The Juniper Networks device asks you for the type of VPN that you want:

![VPN Wizard](image)
We are setting up an LAN-based interface, so click **LAN-to-LAN** and click **Next>>**. Now the Juniper Networks device asks you whether you are using dynamically assigned IP addresses in either side of the VPN tunnel:

![VPN Wizard](image1)

In this case, we are connecting devices with statically assigned IP addresses on their untrust interfaces, so click **Local Static IP <-> Remote Static IP** and click **Next>>**. Now the Juniper Networks device asks us for the IP address of the remote system:

![VPN Wizard](image2)

The device we want to set up the VPN tunnel with is the NetScreen-5XT, with the IP address of 172.16.10.2 in its untrusted interface. Enter that address and click **Next>>**. You are now prompted for the security level for your tunnel. Choose **Standard** for a higher security level for this VPN tunnel, and enter your shared secret. We will use **netscreen** for our shared secret.
Click **Next>>**. Now you are prompted for the source and remote addresses of the networks that you want to interconnect. Fill in the dialog box with addresses of **10.0.0.0/24** for your local address and **192.168.1.0/24** for the remote address:

Click **Next>>**. You will be prompted for the type of service:
Choose ANY and Both direction, and then click Next>>. You will be prompted to decide on logging, counting, and alarms:

Choose Logging, and click Next>>. You will be prompted for a schedule. We don’t want to set a schedule at this time, so simply click Next>>.

Now you are prompted with a confirmation screen, showing the choices you have made in this VPN Wizard. Review them and click Next>> to continue. Now the VPN Wizard presents a summary of all of your choices, along with the CLI that you could have used to accomplish the same tasks:

You can set up Create another VPN or you can Finish. We’re done creating the VPN tunnel between the NetScreen-5XT and the NetScreen-50 at this point, so click Finish. Your Juniper Networks Wizard concludes and closes your session.
CLI Commands:

set interface tunnel.1 zone Untrust
set interface tunnel.1 ip unnumbered interface ethernet3
set ike gateway "Gateway for 192.168.1.0/24" ip 172.16.10.2 outgoing-interface ethernet3 preshare "netscreen" sec-level standard
set vpn "VPN for 192.168.1.0/24" gateway "Gateway for 192.168.1.0/24" replay sec-level standard
set vpn "VPN for 192.168.1.0/24" bind interface tunnel.1
set address Trust "10.0.0.0/24" 10.0.0.0/24
set address Untrust "192.168.1.0/24" 192.168.1.0/24
set policy top from "Trust" to "Untrust" "10.0.0.0/24" "192.168.1.0/24" "ANY" Permit log
set policy top from "Untrust" to "Trust" "192.168.1.0/24" "10.0.0.0/24" "ANY" Permit log
set route 192.168.1.0/24 interface tunnel.1
save

Testing Your VPN Tunnel

Once again, you have completed a difficult task, and this time, the VPN Wizard helped you to accomplish it. The Juniper Networks devices also provide the CLI commands so that you can review, edit, and rerun this configuration on other Juniper Networks devices.

Now that you have created a VPN tunnel, you can test it to make sure that it works. You should be able to ping from one system to the other. We will ping PC-1 from PC-2 using the command ping 192.168.1.33 on PC-2. The results should be:

Success. We have set up a VPN tunnel, and all with just a couple of mouse clicks with the Juniper Networks VPN Wizard. This is a very complex network configuration that you created in minutes. Juniper Networks easy-to-use WebUI, combined with its CLI, made it all work, while you made the choices.

Setting Up a Juniper Networks Transparent Mode Firewall

We have seen how to set up the Juniper Networks device using wizards and the corresponding CLI commands, including setting up a firewall and setting up a VPN. Now, we look at one of Juniper Networks unique deployment option: Transparent Mode.

In Transparent Mode, the Juniper Networks device will protect any number of layer 3 devices and/or subnets with full firewall functionality, with the added security benefit of being virtually invisible to the rest of the network infrastructure. The Juniper Networks firewall/VPN device can be easy deployed, requiring very little effort on the administrator’s part. Because the device does not have an IP address associated with any of its physical network interfaces, there is no need to change the IP addresses of the existing network. Simply place the device between the devices or networks that you want to isolate from each other.

All Juniper Networks firewall/VPN products inherently support transparent mode deployment. There are unique zones, predefined for support of Layer 2 functionality, V1-Trust, V1-Untrust and V1-DMZ (V1-DMZ
is not available on Juniper Networks NetScreen-5 product line). In most cases, devices in the internal network reside in the V1-Trust Zone, while the devices in the external network reside in the V1-Untrust Zone. The following illustration provides an overview of this example:

To demonstrate how easy a Transparent Mode firewall deployment can be, we will walk through configuring the example above. In our example we will use the NetScreen-50 as our Transparent Mode firewall. PC-1 will reside in V1-Trust and PC-2 will reside in V1-Untrust.

We must also unset the configuration on the NetScreen-50. The fastest way to accomplish this task is via the CLI.

To erase the configuration:

- Start a Telnet session from PC-2 to 10.0.0.2
- At the Remote Management Console, enter netscreen for the login name and password
- Enter the CLI command: unset all
  - At the Erase all system config, are you sure y/[n] ? prompt, enter y
- Enter the CLI command reset and press return
  - At the Configuration modified, save? [y]/n prompt, enter n
  - At the System reset, are you sure? y/[n] prompt, enter y and the device will reset.
- Close your Telnet session

We need to configure static IP addresses to PC-1 and PC-2. Consult the Windows operation system documentation for guidelines on how to change the IP address. The IP configuration on PC-1 connected to port E1 should be:

- IP Address: 192.168.1.33
- Netmask: 255.255.255.0
- Gateway: 192.168.1.1
The IP configuration on PC-2 connected to E3 should be:

- **IP Address:** 192.168.1.129
- **Netmask:** 255.255.255.0
- **Gateway:** 192.168.1.1

Connect PC-1 to E1 (ethernet1) of the NetScreen-50 and connect PC-2 to E3 (ethernet3) of the NetScreen-50 to represent the diagram above. Please note that both PC-1 and PC-2 are in the same IP subnet, 192.168.1.0/24. The Juniper Networks firewall will enforce security policies in all IP traffic between these two devices, even when they are directly connected to the same IP subnet.

Next we must configure the device to skip the Initial Configuration Wizard.

**To skip the Initial Configuration Wizard:**

- Start a Telnet session from PC-1 to 192.168.1.1
- At the Remote Management Console, enter `netscreen` for the login name and password
- Enter the CLI command: `save`
- Exit and close your Telnet session

You are now ready to configure the Transparent Mode firewall.

**Place Interfaces into the predefined Layer 2 Zones**

Begin by opening an Internet browser window on PC-1 to `http://192.168.1.1`. Login with the default username and password of `netscreen` and you will be presented with the WebUI main menu.

Open the Network>Interface page and click on the edit option for the ethernet1 interface. Use the list box to place this interface into the V1-Trust zone and click OK.
Repeat this, placing ethernet2 into the Null zone and ethernet3 into the V1-Untrust zone.

**Create firewall policies between Zones**

In our example, for simplicity we want to allow V1-Trust Zone full access to V1-Untrust Zone, and V1-Untrust no access to V1-Trust.

Open Policies and use the list boxes to select From V1-Trust and To V1-Untrust and click New.

The default values of Any for Source Address, Destination Address and Service will allow all traffic to traverse from V1-Trust to V1-Untrust. Click OK to apply this policy. You are finished.

**CLI Commands:**

```
set interface ethernet1 zone v1-trust
unset interface Ethernet2 zone
set interface ethernet3 zone v1-untrust
set policy from v1-trust to v1-untrust any any any permit
save
```


**Testing the Transparent Mode Deployment**

Now that you have created a policy, you can test it to make sure that it works. You should be able to ping PC-2 from PC-1. We will ping from PC-1 using the command `ping 192.168.1.129`. The results should be:

```
C:\>ping 192.168.1.129
Pinging 192.168.1.129 with 32 bytes of data:
Reply from 192.168.1.129: bytes=32 time<10ms TTL=128
Reply from 192.168.1.129: bytes=32 time<10ms TTL=128
Reply from 192.168.1.129: bytes=32 time<10ms TTL=128
Reply from 192.168.1.129: bytes=32 time<10ms TTL=128
Ping statistics for 192.168.1.129:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
          Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

In this example, V1-Untrust to V1-Trust traffic is not allowed by the Juniper Networks firewall. Try to ping from PC-2 by issuing the command `ping 192.168.1.33`.

```
C:\>ping 192.168.1.33
Pinging 192.168.1.33 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.1.33:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
    Approximate round trip times in milli-seconds:
          Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

**Review your work**

Once again, you have completed a difficult task. This time, the WebUI helped you set up your Juniper Networks firewall in Transparent Mode, allowing you to enforce security policies in devices within the same IP subnet. The example also provided you with the CLI commands so that you can review, edit, and rerun this configuration on other Juniper Networks devices.

**Summary**

In this Guide, we have shown how you can configure and deploy Juniper Networks firewall/VPN devices in various network environments. We used Juniper Networks built-in wizards and WebUI to configure two Juniper Networks devices, the NetScreen-5XT and the NetScreen-50. We also used the VPN Wizard to easily create a VPN tunnel between the two Juniper Networks devices. Throughout the various scenarios and configuration tasks, we showed you how you could accomplish the same results by using Juniper Networks fully featured command line interface (CLI).