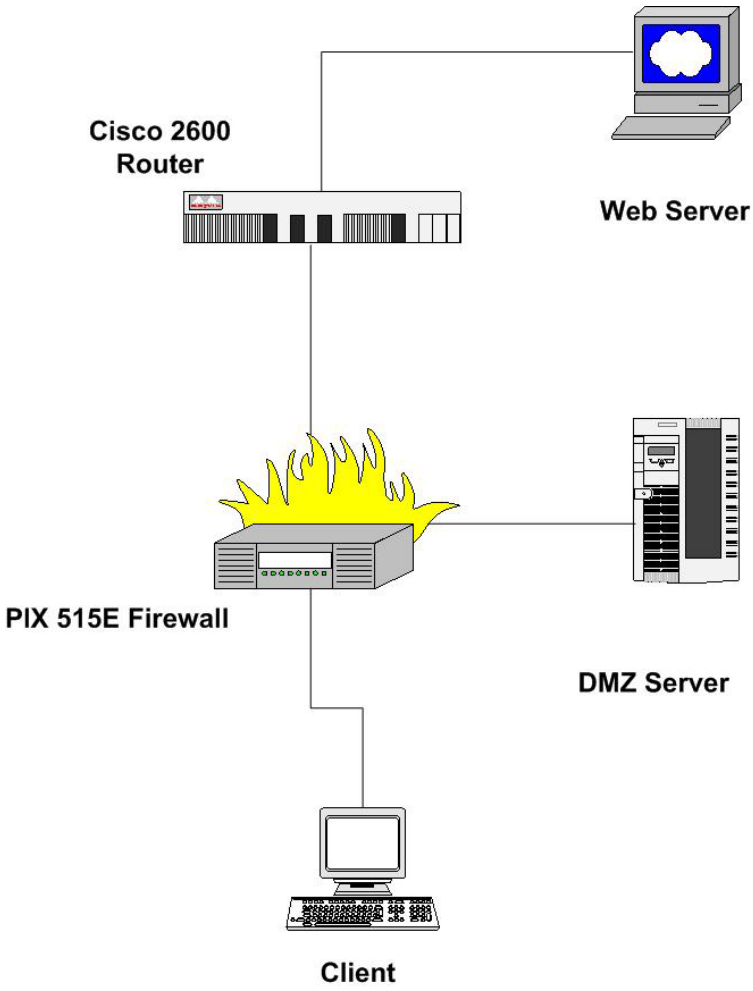
Configuring the PIX Firewall with PDM

Objectives

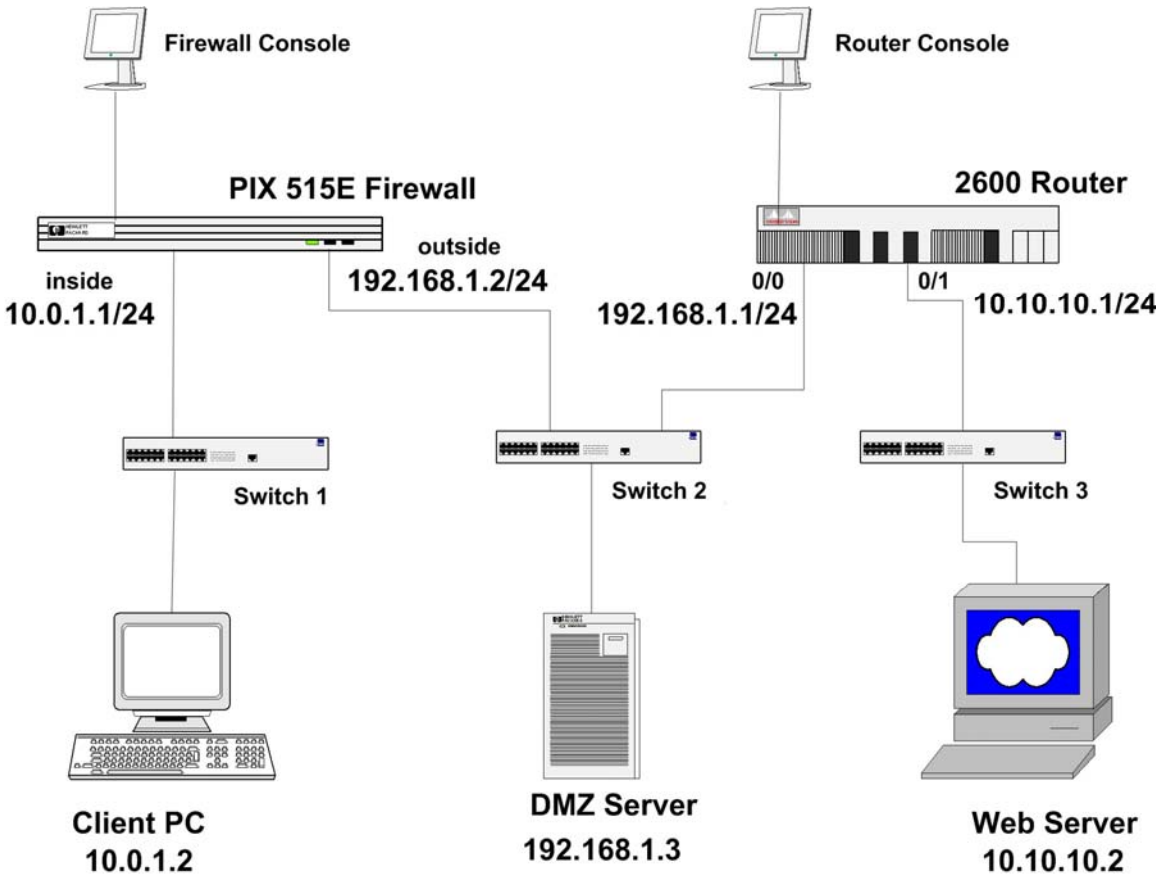
In this lab exercise you will complete the following tasks:

- Install PDM
- Configure inside to outside access through your PIX Firewall using PDM
- Configure outside to inside access through your PIX Firewall using PDM
- Allow ICMP traffic
- Configure PIX IDS
- Configure Site to Site IPSec VPN's
- Test and verify PDM operation

Visual Objective



Lab Setup Diagram



Passwords

PIX Password: Either no password (just press **Enter** key) or **cisco**
Router Password: **cisco**

Note

Lab I Configuration of PIX Firewall and Router is needed in order to perform Lab II.

Task 1 – Clear the PIX Firewall's Configuration and Access the PIX Startup Wizard

Complete the following steps to erase your current PIX Firewall configuration and access the PDM startup wizard.

Step 1 Erase your current PIX Firewall configuration :

```
pix1(config)# write erase
Erase PIX configuration in flash memory? [confirm]
```

Step 2 After the flash has been cleared, reload the PIX Firewall :

```
pix1(config)# reload
Procees with reload ? [confirm]
```

Step 3 When prompted to "**Pre-configure the PIX Firewall through interactive prompts [yes] ?**" press **Enter** to respond:

Step 4 Answer the questions from the interactive prompts:

```
Enable password [<use current password>]: (press Enter)
  Clock (UTC):
  Year [2004]: (Type current year and then press Enter)
  Month [Aug]: (Type current month and then press Enter)
  Day [25]: (Type current day and then press Enter)
  Time [14:31:46]: (Type current time and then press Enter)
Inside IP address: (Type 10.0.1.1 and then press Enter)
Inside network mask: (Type 255.255.255.0 and then press Enter)
Host name: (Type pix1 and then press Enter)
Domain name: (Type hackinglab.com and then press Enter)
IP address of host running PIX Device Manager: (Type 10.0.1.2
and then press Enter)
Use this configuration and write to flash? (Type y and then
press Enter)
Building configuration...
Cryptochecksum: f34c98c9 680835eb 85729885 a4fdde0d
[OK]
```

Step 5 Access the PDM by doing the following :

1. Open a browser on the inside client and enter (https://10.10.1.1)
2. You may be presented with a "Security Alert" window ("You are about to view pages over a secure connection……."), click **OK.**
3. You may be presented with a "Security Alert" window ("**Information you exchange with this site cannot be viewed or changed…….**"), you are asked **"Do you want to proceed ?**" Click on Yes.
4. The "Enter Network Password" window is presented. **Do not** enter a username or password. Click **OK** to continue.

Note The password that is used by PDM is the Enable password. Since we did not enter an enable password during setup, the password is not set.

5. After a few seconds, another "Security Warning" window opens. This window asks "**Do you want to install and run "Cisco PIX Device Manager" signed on**….". Click on **Yes**.
6. After a few more seconds, the "Update Config" window opens. This window asks **"This may be the first time the PDM has been used…."** . Click on Proceed.

Note The Startup Wizard should automatically start. You have completed this Task.

Task 2 – Use the PDM startup Wizard to Perform basic Configuration tasks.

The first time you use PDM, the Startup Wizard will start automatically. You can also launch the Startup Wizard at any time by clicking on **Wizards>Startup Wizard**. Complete the following steps to configure the PIX Firewall's outside and interfaces, and enable NAT :

Step 1 You can use the PIX Device Manager Startup Wizard to setup a basic configuration for your PIX. Click **Next**.

Step 2 In the "Basic Configuration" window, verify your hostname and domain name, then click **Next**.

Step 3 In the "Outside Interface Configuration" window, your outside interface speed in **auto**, and "Static IP Address" is selected. In the "IP Address" field, enter 192.168.1.2. In the dropdown menu next to "Subnet Mask" choose **255.255.255.0**. Enter 192.168.1.1 for the "Default Gateway" and then click **Next.**

Step 4 In the "Auto Update Configuration" window, leave the "Auto Update" checkbox blank, and click **Next**:

Step 5 **In the "Other Interfaces Configuration" window,** click Next**.**

Step 6 **Click** Next**. The "NAT and PAT Configuration" window opens.**

Step 7 Configure a global pool of addresses to be used for address translation by doing the following :

1. Select "Use Network Address Translation".

2. Enter **192.168.1.20** in the "Starting Global Address Pool" field.
3. Enter **192.168.1.253** in the "Ending Global Address Pool" field.
4. Select **255.255.255.0** from drop-down menu.

Step 8 Click **Finish**.

Note You may get an "Error in sending command" when the PDM send the commands to the PIX Firewall. The error message should only have to do with interface that are not used in this lab, and is not fatal. Click **OK**.

Note PDM has an option that will allow you to see what commands are being sent to the PIX. You can toggle this option by going to **Options>Preferences.** Check the box next to "Preview commands before sending to the firewall" to turn this option on or uncheck it to turn it off.

Task 3 – Verify the Configuration Created by the PDM Startup Wizard and Configure Security Level, Passwords, and Statics.

Complete the following steps to configure the PIX Firewall's outside and interfaces, the global address pool, routing and NAT :

Step 1 The previous Task should have left you at the PDM Home Screen. Notice all of
the statistics that is available on the Home Screen.

Step 2 Click the **Configuration** icon near the top left of menu bar.

Step 3 You are presented with Configuration window. You should see tabs labeled **Access Rules**, **Translation Rules**, **VPN**, **Hosts/Networks**, and **System Properties**.

Step 4 Click the **System Properties.** Correct any errors by clicking on **Edit.**

1. Verify that ethernet0, ethernet1 are enabled.
2. Verify that ethernet0, ethernet1 are correctly enabled.
3. Verify that ethernet0 has a security level 0, ethernet1 has security level 100.
4. Verify the IP address and subnet masks of ethernet0, ethernet1.

Step 5 Verify the NAT configuration and global address pool you entered earlier by doing the following :

1. Click the **Translation Rules** tab.
2. You should see the one translation that has been configured to this point.

Step 5 Verify the default route configuration by doing the following :

1. Click the **System Properties** tab.
2. Under Categories on the left side of the screen, click on **Routing** to expand the category.
3. Click on **Static Route**.
4. Verify that the outside gateway under "Gateway IP" is 192.168.1.1

Step 7 Configure privileged mode and Telnet passwords by doing the following:

1. Click on Administration from the Categories tree on the left side of the panel. Password appears under Administration.
2. Click on Password. The Password group box appears on the right side of the panel.
3. Enter **cisco** in the "New Password" text box in the "Enable Password" group box.
4. Enter **cisco** in the "Confirm New Password" text box in the Enable password group box.
5. Click **Apply** in the "Enable Password" group box.
6. The "Enter Network Password" window will open. Type **cisco** in the Password field and click **OK**.
7. Enter **cisco** in the "Old password" textbox (**cisco** is the default) in the Telnet Password group box.
8. Enter **cisco** in the "New password" textbox (**cisco** is the default) in the Telnet Password group box.
9. Enter **cisco** in the "Confirm New password" textbox (**cisco** is the default) in the Telnet Password group box.
10. Click Apply in the "Telnet Password" group box. (All the password fields should be blank after apply.)

Step 8 Define a Static Translation for the inside client by doing the following :

1. From the **Translation Rules** tab, Select **Rules>Add**.
2. Select inside as the "Original Host/Network Interface" from the drop down menu at the top of the "Add address Translation Rule" screen
3. In the "IP Address" field of the Original Host/Network Interface, enter 10.0.1.2.
4. From the drop-down menu next to Mask, select 255.255.255.255.
5. Make sure that "Translate address on interface :" is **outside.** If not, use the drop-down menu to change it.
6. In the "Translate Address to" area select **Static**.
7. In the "IP address" field enter **192.168.1.10**.
8. Click **OK**.
9. You should be back at the **Translation Rules** tab of the Configuration window. Click **Apply**.

Task 4 – Test the Inside and Outside Interface Connectivity

Perform the following steps to test NAT and interface connectivity:

Step 1 Test the operation of the global and NAT you configured by originating connections through the PIX Firewall.

1. Open another web browser on the inside client.

Use the web browser to access the outside server at IP address 10.10.10.2 by entering http://192.168.1.2

2. The outside server web page should display.

Step 2 Observe the translation table by doing the following in PDM.

1. Choose **Tools-> Command Line Interface……**The "Command Line Interface" window opens.
2. In the Command field, enter **show xlate**.
3. Click **Send**.
4. Observe the output in the Response text box. It should appear similar to the following :

```
Result of firewall command: "show xlate"

1 in use, 1 most used
Global 192.168.1.10 Local 10.0.1.2
```

Note that the static "outside" address assigned to the inside client has been used. Any other hosts on the inside network could be assigned an address in the 192.168.1.20-253 range from the global pool that you configured earlier.

Step 3 Exit the "Command Line Interface" window by clicking **Close.**

Step 4 Test interface connectivity by doing the following in PDM :

1. Choose **Tools > Ping**.
2. In the "IP Address" field, enter 10.0.1.1
3. Click **Ping**.
4. Observe the following output in the "Ping Output" window. The output must appear similar to the following :

```
10.0.1.1 response received -- 0ms
10.0.1.1 response received -- 0ms
10.0.1.1 response received -- 0ms
```

5. Click **Clear Screen** to remove the output.

Step 5 Repeat Step4 for the following IP addresses. You have successfully completed this task if responses are received for all of the pings.

1. Inside host 10.0.1.2

2. Outside Interface 192.168.1.2
3. Outside Web server 10.10.10.2

Step 6 Exit the Ping window by clicking **Close**.

Task 5 – Use PDM to Configure NAT

Perform the following steps to test NAT for inside interface :

Step 1 Remove the NAT that we configured using the Startup Wizard by doing the following :

1. Click the **Translation Rules** tab.
2. Highlight the inside rule you configured earlier in the lab exercise (the one with the pool **192.168.1.20-192.168.1.253**).
3. Choose **Rules>Delete** from the menu bar (note that you aren't asked if you really want to delete it !)

Step 2 Configure NAT for the internal network's range of IP addresses by doing the following:

1. Click the Rules menu.
2. Click **Add…**The "Add Address Translation Rule" window opens.
3. Verify that the **inside** interface is selected in the Interface drop-down menu.
4. Click **Browse….**The "Select host/network" window opens.
5. Verify that the **inside** interface is selected in the Interface drop-down menu.
6. Click on 10.0.1.0
7. Click **OK**.
8. Verify that the **outside** interface is selected in the "Translate address on interface" drop-down menu.
9. Verify that **Dynamic** is selected in the "Translate Address to**"** group box.
10. Select 10 in the "Address pool" drop-down menu.
11. Verify that the global pool you configured earlier **(192.168.1.20-192.168.1.253)** appears under Address.
12. Click **OK** in the "Add Translation Rule" window. Your new rule appears on the **Translation Rules** tab.
13. Click **Apply**.

Step 3 Write the current configuration to flash memory by doing the following **:**

1. Click on the "floppy disk" icon (labeled **Save**) at the top of the screen.
2. The "Save Running Configuration to Flash" window opens. Click **Apply**
3. The "Save Successful!" window opens. Click **OK**

Task 6 – Test Globals and NAT Configuration

To test the globals and NAT configuration, complete the following:

Step 1 Test the operation of the global and NAT you configured by originating connections through the PIX Firewall :

1. Open a web browser on the inside client.
2. Use the web browser to access the outside server at IP address 10.10.10.2 by entering http://10.10.10.2
3. The home page of the outside server should open in your web browser.

Note If you think you have configured everything correctly but cannot reach the outside webpage, save the PIX configuration and reload the PIX

Step 2 Observe the translation table with **show xlate** command by doing the following:

1. Choose **Tools-> Command Line Interface……**The "Command Line Interface" window opens.
2. In the Command field, enter **show xlate**.
3. Click **Send**.
4. Verify the output in the Response window is similar to the following :

```
Result of firewall command: "show xlate"

1 in use, 1 most used
Global 192.168.1.10 Local 10.0.1.2
```

5. Exit the "Command Line Interface" window by clicking **Close.**

Step 3 Observe the transaction by doing the following:

1. Choose **Tools-> Command Line Interface……**The "Command Line Interface" window opens.
2. In the Command field, enter **show arp**.
3. Click **Send**.
4. Verify the output in the Response window is similar to the following :

```
outside 192.168.1.3 0006.5b1b.470b
outside 192.168.1.1 000f.34df.5800
inside 10.0.1.2 0006.5b1b.3733
```

5. Click **Clear Response**.
6. In the Command field, enter **show conn**.
7. Click **Send**.
8. Verify the output in the Response window is similar to the following :

```
Result of firewall command: "show xlate"

1 in use, 1 most used
Global 192.168.1.10 Local 10.0.1.2
```

9. Click **Clear Response**.
10. Click **Close**.

Note If you have successfully reached the webpage but did not see any connection information, you probably need to turn off the caching on your web browser. For Internet Explorer : Tools> Internet Options…….->Click on General Tab ->Click on Settings in the Temporary Internet Files area -> Under Check for new versions of stored pages: select the Every visit to the page option-> Click Ok->Click Ok.

Task 7 – Use PDM to Configure Access from Lower to Higher Security Levels

Complete the following steps to configure the PIX Firewall to permit outside access to hosts on the Inside interface :

Step 1 Ping the outside server from your internal client. The ping should fail because the access policy does not yet allow it.

```
C:\>ping 10.10.10.2

Pinging 10.10.10.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
```

Step 2 Configure an ACL to allow pinging through your PIX Firewall by doing the following in PDM :

1. Click the **Access Rules** tab.
2. Select **Rules > Add….** The “Add Rules” window opens.
3. Verify that **permit** is selected in “Select an action” drop-down menu.
4. Select **outside** in the Interface drop-down menu in the “Source Host/Network” group box.
5. Select **inside** in the Interface drop-down menu in the “Destination Host/Network” group box.
6. Select ICMP in the “Protocol and Service” group box.
7. Verify that **any** is selected in the ICMP type box.
8. Click **OK**. Your new rule appears on the **Access Rules** tab.
9. Click **Apply**.

Step 3 Ping the outside server from your internal client. The ping should fail because the access policy does not yet allow it.

```
C:\>ping 10.10.10.2

Pinging 10.10.10.2 with 32 bytes of data:

Reply from 10.10.10.2: bytes=32 time<10ms TTL=127
Reply from 10.10.10.2: bytes=32 time<10ms TTL=127
Reply from 10.10.10.2: bytes=32 time<10ms TTL=127
Reply from 10.10.10.2: bytes=32 time<10ms TTL=127
```

Step 4 Configure an ACL to allow Telnet access to the inside host from the outside by doing the following:

1. Click the **Access Rules** tab.
2. Select **Rules > Add….** The "Add Rules" window opens.
3. Verify that **permit** is selected in "Select an action" drop-down menu.
4. Choose **outside** in the Interface drop-down menu in the "Source Host/Network" group box.
5. Select **inside** in the Interface drop-down menu in the "Destination Host/Network" group box.
6. Click **Browse…** in the "Destination Host/Network" group box. The "Select host/network" window opens.
7. Verify that **inside** is selected in the Interface drop-down menu.
8. Select 10.0.1.2
9. Click **OK**. You should be back to the **"Add Rule"** window.
10. Select TCP in the "Protocol and Service" group box.
11. Verify that **Service=** is selected in the drop-down menu under "Source Port".
12. Verify that **any** is selected in the "Source Port" text box.
13. Click the …button under "Destination Port". The Service window opens.
14. Select **Telnet.** Click **OK.**
15. Verify that **Service=** is selected in the drop-down menu under "Destination Port".
16. Click **OK**. You should be back to the **"Add Rule"** window.
17. Click **Apply**.

Step 5 Clear current translations by doing the following:

1. Choose **Tools-> Command Line Interface……**The "Command Line Interface" window opens.
2. In the Command field, enter **clear xlate**.
3. Click **Send**.
4. Verify the output in the Response window is similar to the following :

```
Result of firewall command: "clear xlate"
The command has been sent to the firewall.
```

Step 6 View current translations by doing the following:

1. Click **Clear Response** in the "Command Line Interface" window.
2. In the Command field, enter **show xlate**.
3. Click **Send**.
4. Verify the output in the Response window is similar to the following :

```
Result of firewall command: "show xlate"
0 in use, 2 most used
```

5. Click **Close** in the "Command Line Interface" window.

Step 7 Test Telnet Access to the inside hosts by completing the following:

1. On the outside server, test Telnet to the inside host by choosing

```
Start->Run
C:\>telnet 10.10.1.2 Username: user Password : cisco
```

You should be able to access the inside host via Telnet.

Step 8 Observe the transactions by doing the following in PDM :

1. Choose **Tools-> Command Line Interface……**The "Command Line Interface" window opens.
2. In the Command field, enter **show arp**.
3. Click **Send**.
4. Verify the output in the Response window is similar to the following :

```
outside 192.168.1.3 0006.5b1b.470b
outside 192.168.1.1 000f.34df.5800
inside 10.0.1.2 0006.5b1b.3733
```

5. Click **Clear Response** in the "Command Line Interface" window.
6. In the Command field, enter **show conn**.
7. Click **Send**.
8. Verify the output in the Response window is similar to the following :

```
Result of firewall command: "show conn"

0 in use, 2 most used
```

9. Click **Clear Response** in the "Command Line Interface" window.
10. In the Command field, enter **show xlate**.
11. Click **Send**.
12. Verify the output in the Response window is similar to the following :

```
Result of firewall command: "show xlate"

1 in use, 1 most used
Global 192.168.1.10 Local 10.0.1.2
```

13. Click **Close** in the "Command Line Interface" window.

Task 8 – Use PDM to Configure the PIX Firewall to Permit ICMP Packets

Complete the following steps to test current access through the PIX Firewall, and then configure the PIX Firewall to allow ICMP packets between the inside and outside interfaces:

Step 1 Ping the outside server from your internal client. The ping should fail because the access policy does not yet allow it.

```
C:\>ping 10.10.10.2

Pinging 10.10.10.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
```

Step 2 Configure NAT for the internal network's range of IP addresses by doing the following:

1. Click the **Access Rules** menu.
2. Choose the **Rules>Add…**The "Add Rule" window opens.
3. Verify that **permit** is selected in "Select an action" drop-down menu
4. Choose **outside** from the Interface drop-down menu under "Source Host/Network".
5. Choose **inside** from the Interface drop-down menu under "Destination Host/Network".
6. Select **icmp** in the Protocol an Service group box.
7. Click **OK**. You are returned to the Access Rules tab.
8. Click **Apply**.

Step 3 From your inside host, ping your bastion host:

```
C:\>ping 10.10.10.2

Pinging 10.10.10.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
```

Task 9 – Configure a Site-to-Site VPN

To create a secure site-to-site VPN between your PIX Firewall and your peer pod's PIX Firewall, complete the following steps:

Step 1 Choose **Wizards>VPN Wizard…**from the PDM main menu. The "VPN Wizard" window opens.
Step 2 Verify that "Site to Site VPN" is selected.
Step 3 Verify that the **outside** interface is chosen from drop-down box.
Step 4 Click **Next**. The "Remote Site Peer" window opens.
Step 5 Enter 192.168.2.1 in the "Peer IP Address" field
Step 6 Verify that "Pre-shared Key" is selected from the Authentication group box.
Step 7 Enter cisco123 in the "Pre-shared Key" field.
Step 8 Enter cisco123 in the "Reenter" Key field.
Step 9 Click Next. The IKE Policy window opens.
Step 10 Choose **DES** from the Encryption drop-down menu.
Step 11 Choose SHA from the Authentication drop-down menu.
Step 12 Choose Group 1 (768-bit) from the "DH Group" drop-down menu.
Step 13 Click **Next**. The "Transform Set" window opens
Step 14 Choose **DES** from the Encryption drop-down menu.
Step 15 Choose SHA from the Authentication drop-down menu.
Step 16 Click **Next**. The "IPSec Traffic Selector" window opens
Step 17 Verify that "IP Address" is selected within the Host/Network group.
Step 18 Verify that **outside** is chosen from the Interface drop-down menu.
Step 19 Enter 10.0.1.2 in the "IP Address field".
Step 20 Choose 255.255.255.255 from the Mask drop-down menu.
Step 21 Click the arrow to move the host address to the Selected list. The "Add host/network" window opens.
Step 22 Click OK. Create host/network window opens. The IP address and netmask for your inside host appear in the Basic Information group box.
Step 23 Verify that "inside" appears in the Interface drop-down menu.
Step 24 Click Next. The "Static route" screen appears
Step 25 Click Next. The "NAT (Network Address Translation)" screen appears
Step 26 Click Finish. You are returned to the IPSec Traffic selector window.
Step 27 Click the arrow button >> to move the IP address 10.0.1.2 to the Selected List.
Step 28 Click Next. The "IPSec Traffic selector (Continue)" window opens.
Step 29 Verify that "IP Address" is selected within the " On Remote Site" Host/Network group box.
Step 30 Verify that **outside** is chosen from the Interface drop-down menu.

Step 31 Enter the statically mapped IP address of your peer's inside host 192.168.2.2 in the IP Address field.
Step 32 Choose 255.255.255.255 from the Mask drop-down menu.

Step 33 Click **the arrow** to move the IP address 192.168.2.2 to the Selected list. The "Add host/network ?" window opens.

Step 34 Click OK. The "Create host/network" window opens. The IP address and netmask for your peer's inside host appears in the Basic Information group box.
Step 35 Verify that **outside** appears in the Interface drop-down menu.
Step 36 Click **Next**. A reminder appears in the Create host/network window.

Step 37 Click Next. The "IPSec Traffic selector (Continue)" window opens.
Step 38 Click the arrow button to move the IP address of your peer's inside host to the selected list.
Step 39 Click Finish.
Step 40 Save the PIX Firewall configuration by clicking the Save icon in the PDM toolbar. The "Save Running Configuration to Flash" window opens.
Step 41 Click Apply.
Step 42 From the PDM Configuration screen, click on the VPN tab.
Step 43 Click on the Show Detail button. Verify that the VPN is configured properly.

Task 10 – Test and Verify Your VPN

To test your site-to-site VPN, complete the following steps :

Note Task 11 must be finished in Peer Pod. Otherwise this will not work correctly.

Step 1 Test the access to your peer's inside host from your inside host by completing the following sub-steps :
Step 2 Open a DOS window on your inside client.
Use ping to access your peer's inside host by entering
Step 3 In PDM, select the **Monitoring** icon.
Step 4 Expand the VPN Connection Graphs in the tree.
Step 5 Click on **IPSec Tunnels**.
Step 6 Highlight **IPSec Active Tunnels and IKE Active Tunnels** and click **Add**.
Step 7 Click Graph It !
Step 8 The graph shows one IKE tunnel, and 2 IPSec tunnels (one in each direction).