



Lab 3.6.3 Configuring the PIX Security Appliance with ASDM

Objective

In this lab exercise, the students will complete the following tasks:

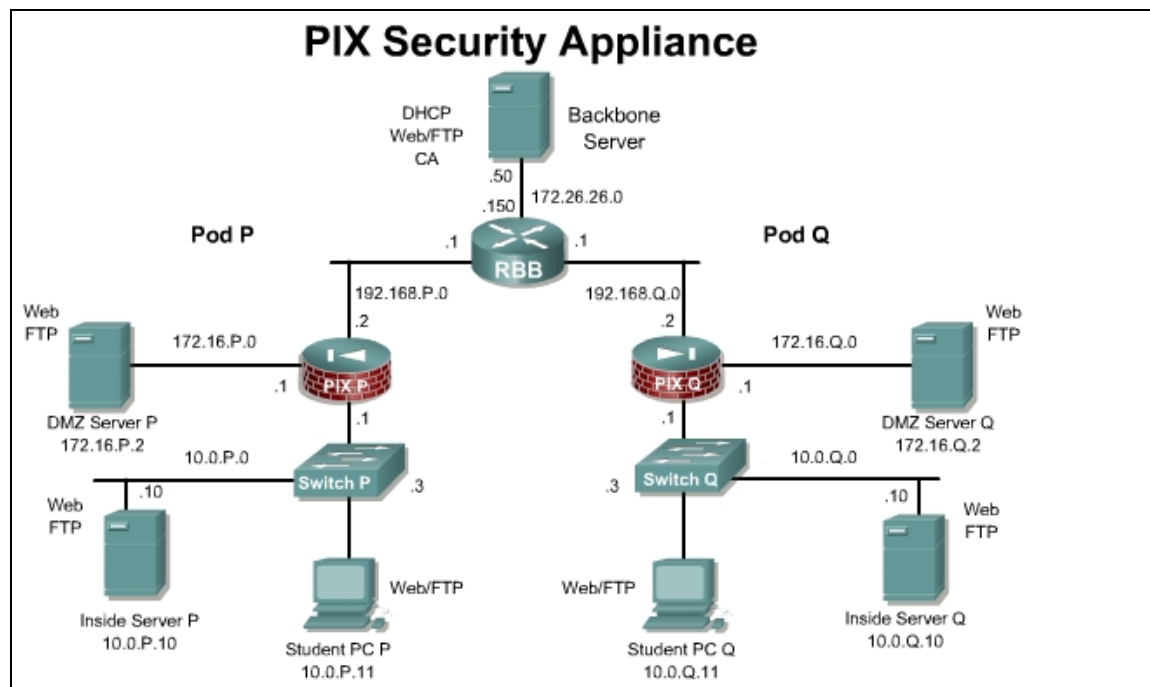
- Configure basic settings using ASDM
- Configure outbound access with NAT.
- Test connectivity through the PIX Security Appliance.
- Configure Banners
- Configure Telnet and SSH for remote access

Scenario

The Cisco Adaptive Security Device Manager is a browser-based configuration tool that enables administrators to set up, configure, and monitor the PIX Security Appliance graphically, without requiring an extensive knowledge of the PIX Security Appliance command-line interface (CLI).

Topology

This figure illustrates the lab network environment:



Preparation

Begin with the standard lab topology. Access the PIX Security Appliance console port using the terminal emulator on the Student PC. If desired, save the PIX Security Appliance configuration to a text file for later analysis.

Tools and Resources

In order to complete the lab, the following is required:

- Standard PIX Security Appliance lab topology
- Console cable
- HyperTerminal

Additional Materials

Student can use the following link for more information on ASDM:

<http://www.cisco.com/go/asdm>

If needed, a TFTP server can be found at <http://www.weird-solutions.com/>

If needed, a SSH client can be found at <http://www.chiark.greenend.org.uk/~sgtatham/putty/>

Command List

In this lab exercise, the following commands will be used. Refer to this list if assistance or help is needed during the lab exercise.

Command	Description
<code>reload</code>	Reload the PIX Security Appliance
<code>write erase</code>	Erase the startup configuration.

Step 1 Erase the Current PIX Security Appliance Configuration

Complete the following steps to erase the current PIX Security Appliance configuration and allow access the PIX using ASDM:

- In the Terminal window, erase the current PIX Security Appliance configuration. When prompted to confirm, press **Enter**.

```
PixP# write erase
```

```
Erase PIX configuration in flash memory? [confirm] <Enter>
```

- In the Terminal window, reload the PIX Security Appliance. When prompted to confirm, press **Enter**.

```
PixP# reload
```

```
Proceed with reload? [confirm] <Enter>
```

- When prompted to pre-configure the PIX Security Appliance through interactive prompts, press **Enter**.
- Accept the default Firewall mode, routed, by pressing **Enter**

```
Firewall Mode [Routed]: <Enter>
```

- Agree to use the current password by pressing **Enter**:

```
Enable password [<use current password>]: <Enter>
```

- f. Allow password recovery by pressing **Enter**.
Allow password recovery [yes]? **<Enter>**
- g. Accept the default year by pressing **Enter**:
Clock (UTC):
Year [2002]: **<Enter>**
- h. Accept the default month by pressing **Enter**:
Month [Nov]: **<Enter>**
- i. Accept the default day by pressing **Enter**:
Day [14]: **<Enter>**
- j. Accept the default time stored in the host computer by pressing **Enter**:
Time [11:21:25]: **<Enter>**
- k. Enter the inside interface IP address of the PIX Security Appliance:
Inside IP address: **10.0.P.1**
(where P = pod number)
- l. Enter the network mask that applies to inside IP address:
Inside network mask: **255.255.255.0**
- m. Enter the hostname:
Host name: **PixP**
(where P = pod number)
- n. Enter the DNS domain name of the network on which the PIX Security Appliance runs:
Domain name: **cisco.com**
- o. Enter the IP address of the host running ASDM:
IP address of host running Device Manager: **10.0.P.11**
(where P = pod number)
- p. Enter **y** at the prompt to save the information to the Flash memory of the PIX Security Appliance.

Step 2 Verify the Student PC Configuration

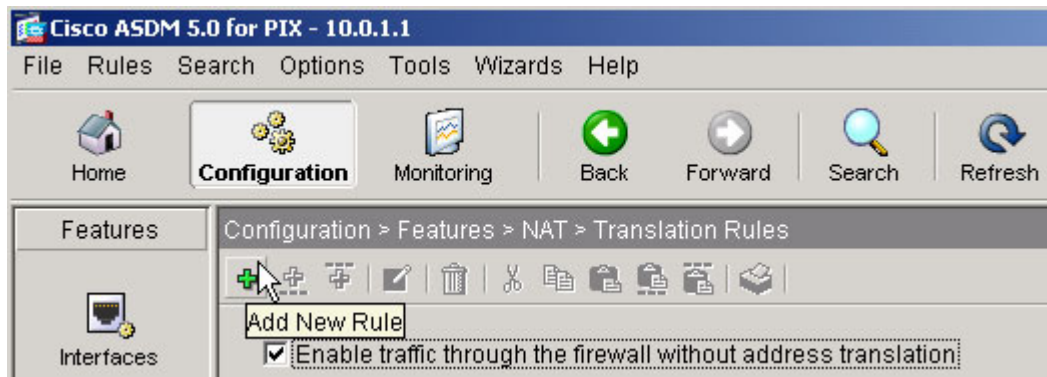
- a. Open the network control panel.
- b. Verify that the Student PC address is 10.0.P.11 /24 with a Gateway address of 10.0.P.1.
(where P = pod number)
- c. Access the ASDM console by completing the following sub-steps:
- d. Open a web browser and enter **https://10.0.P.1.** to access ASDM.
- e. In the Security Alert window, click **Yes**.
- f. The initial Cisco ASDM 5.0 window opens. Click **Run ASDM as a Java Applet**.
- g. In the Warning – Security window, click **Yes**.
Note: Multiple security alert windows may appear when launching ASDM. If a security alert window appears, review the message contained in the window, and click **Yes** to continue
- h. When prompted for a username and password, do not enter a username or password. Click **OK** to launch ASDM.

Step 3 Configure the Inside and Outside Interfaces of the PIX Security Appliance

Complete the following steps to configure the inside and outside interfaces of the PIX Security Appliance, establish a default route, enable NAT for the internal network, and create a global pool of addresses for address translation:




- a. Click the **Configuration** button to navigation to the Configuration screen..
- b. Select **Interfaces** from the Features panel.
- c. Configure the inside interface by completing the following sub-steps:
 - i. Double-click in the row for **ethernet1** in the Interfaces table. Click the **OK** button when a warning about loss of connectivity appears. The Edit Interface window opens.
 - ii. Verify that the Enable Interface check box is selected.
 - iii. Verify that inside appears in the Interface Name field.
 - iv. Verify that 10.0.P.1 appears in the IP Address field.
(where P = pod number)
 - v. Verify that 255.255.255.0 appears in the Subnet Mask drop-down menu.
 - vii. Verify that 100 appears in the Security Level field.
 - viii. Click **OK** to close the Edit Interface window.
- d. Configure the outside interface by completing the following sub-steps:
 - i. Double-click in the row for **ethernet0** in the Interfaces table. Click the **OK** button when a warning about loss of connectivity appears. The Edit Interface window opens.
 - ii. Select the **Enable Interface** check box.
 - iii. Enter the interface name **outside** in the Interface Name field.
 - iv. Select the **Use Static IP** radio button within the IP Address group box.
 - v. Enter **192.168.P.2** in the IP Address field.
(where P = pod number)
 - vi. Choose **255.255.255.0** from the Subnet Mask drop-down menu.
 - viii. Enter **0** in the Security Level field.
 - ix. Click **OK**. Click the **OK** button in the Security Level Change window.
 - x. Click the **Apply** button.
 - xi. If the Preview CLI Commands window appears, click the **Send** button to continue.
- e. To establish a default route, complete the following sub-steps:
 - i. Select **Routing** from the Features panel.
 - ii. Expand the **Routing** branch in the Categories tree.
 - iii. Choose **Static Route** from the Routing list.
 - iv. Select **Add** from the Static Route group box. The Add Static Route window opens.
 - v. Choose **outside** from the Interface Name drop-down menu.
 - vi. Enter **0.0.0.0** in the IP Address field.
 - vii. Enter **0.0.0.0** in the Mask drop-down menu.
 - vii. Enter **192.168.P.1** in the Gateway IP field.
(where P = pod number)
 - viii. Verify that 1 appears in the Metric field.

- ix. Click **OK**. The static route appears in the Static Route table.
- x. Click the **Apply** button.
- xi. If the Preview CLI Commands window appears, click the **Send** button to continue.
- f. Configure a global pool of addresses to be used for address translation by completing the following sub-steps:
 - i. Select **NAT** from the Features panel.
 - ii. Click the **Manage Pools** button. The **Manage Global Address Pools** window opens.
 - iii. Click **Add**. The **Add Global Pool** Item window opens.
 - iv. Choose **outside** from the Interface drop-down menu.
 - v. Enter **1** in the Pool ID field.
 - vi. Verify that the Range radio button is selected.
 - vii. Enter 192.168.P.32 in the first IP address field.
(where P = pod number)
 - viii. Enter 192.168.P.254 in the second IP address field.
(where P = pod number)
 - ix. Enter 255.255.255.0 in the Network Mask field.
 - x. Click **OK** to return to the **Manage Global Address Pools** window.
 - xi. Click **OK** to close the **Manage Global Address Pools** window.
 - xii. Click the **Apply** button. If the Preview CLI Commands window appears, click the **Send** button to continue.
- g. Configure NAT by completing the following sub-steps:
 - i. Verify that the **Translation Rules** panel is still active.
 - ii. Verify that the **Translation Rules** radio button is selected.



- iii. Choose **Rules>Add** from the main menu or click on the **Add New Rule** icon. The **Add Address Translation Rule** window opens.
- iv. Verify that the inside interface is chosen in the **Interface** drop-down menu.
- v. Click **Browse**. The **Select host/network** window opens.
- vi. Verify that the inside interface is chosen in the drop-down menu.
- vii. Select the inside network by doing the following:
- viii. Click **10.0.P.0** in the directory structure list.
(where P = pod number)

- ix. Click **OK**. This will return to the Add **Address Translation Rule** window.
- x. Verify that **outside** is chosen in the **Translate address on Interface** drop-down menu.
- xi. Verify that **Dynamic** is selected in the **Translate Address To** group box.
- xii. Choose **1** from the **Address Pool** drop-down menu.
- xiii. Verify that the global pool configured earlier, 192.168.P.32–192.168.P.254, appears under **Address**.
(where P = pod number)
- xiv. Click **OK** in the **Add Address Translation Rule** window. The new rule appears in the rules table.

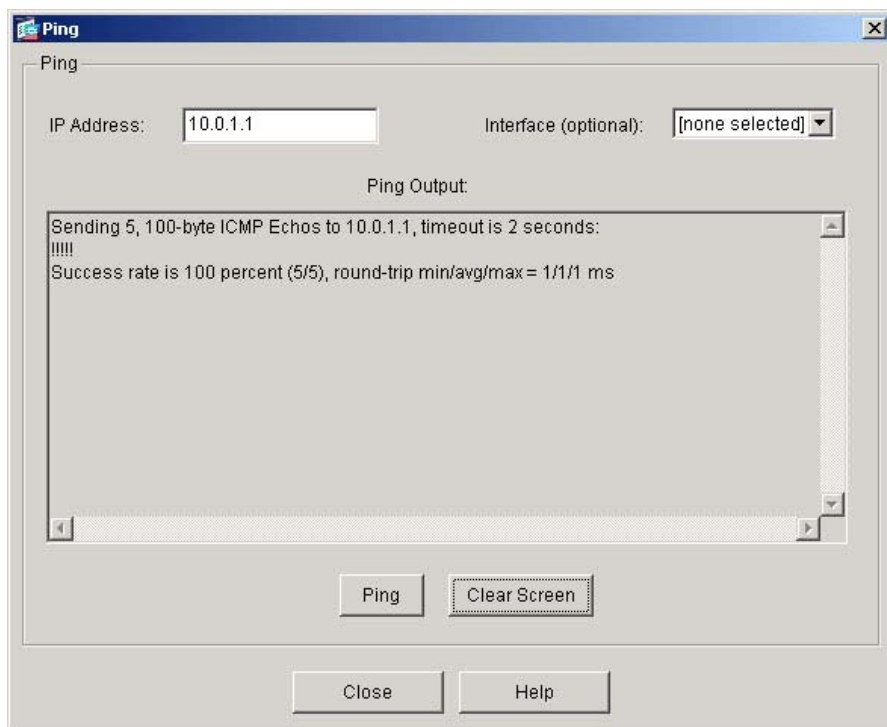
Rule	Original			Translated	
Type	Interface	Source Network	Destination Network	Interface	Address
	inside	 10.0.1.0/24	 any	outside	192.168.1.32-192.168.1.254

- xv. Click **Apply**. If the Preview CLI Commands window appears, click the **Send** button to continue.

Step 4 Test Interface Connectivity and NAT

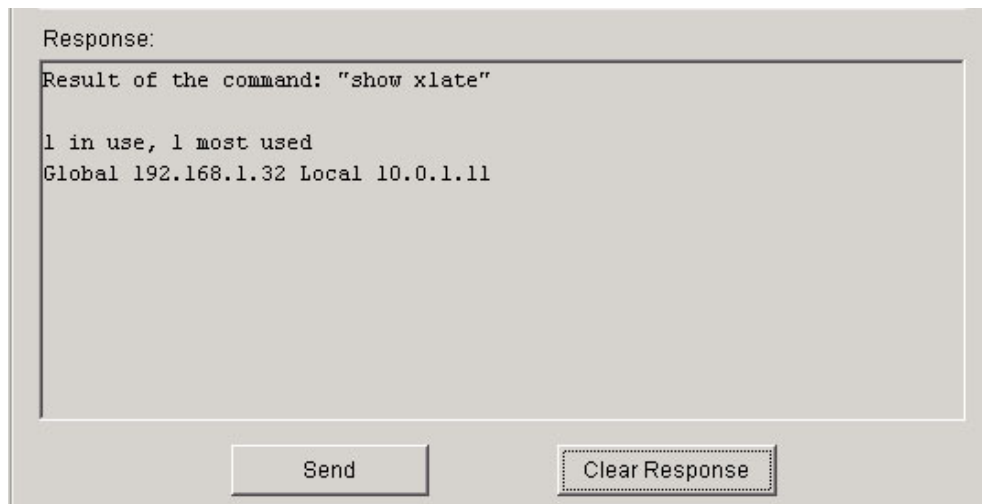
Complete the following steps to test interface connectivity and NAT:

- a. Test interface connectivity by completing the following sub-steps:
 - i. Choose **Tools> Ping**.
 - ii. In the IP Address field, enter **10.0.P.1**.
(where P = pod number)
 - iii. Click **Ping**.
 - iv. Observe the following output in the Ping Output window. The output should appear similar to the following:



- v. Click Clear Screen.
 - b. Repeat the ping for the following IP addresses. A response for all pings should be received:
 - The inside host:
10.0.P.11
(where P = pod number)
 - The outside interface:
192.168.P.2
(where P = pod number)
 - The backbone router:
192.168.P.1
(where P = pod number)
 - c. Exit the Ping window by clicking **Close**.
 - d. Test the operation of the global and NAT configured by originating connections through the PIX Security Appliance. To do this, complete the following sub-steps:
 - i. Open a web browser on the student PC.
 - ii. Use the web browser to access the SuperServer web page at IP address 172.26.26.50 by entering **http://172.26.26.50**.
-
- Note** An HTTP connection is used as a test here because ICMP pings are not allowed through the PIX by default.
-
- e. Observe the translation table by completing the following sub-steps:
 - i. Choose **Tools> Command Line Interface**. The Command Line Interface window opens.
 - ii. In the Command field, enter **show xlate**.

- iii. Click **Send**.
- iv. Observe the output in the Response field. It should appear similar to the following:



Note that a global address chosen from the low end of the global range has been mapped to the student PC.

- f. Exit the Command Line Interface window by clicking **Close**.

Step 5 Configure remote access to the PIX Security Appliance

Complete the following steps to configure remote access to the PIX for remote configuration.

- a. Select **Device Administration** from the Features panel.
- b. Select **Administration>Telnet** from the tree menu.
- c. Click the **Add** button in the Telnet window.
- d. Configure the following values:
 - 1. Interface Name: inside
 - 2. IP Address: 10.0.P.11
 - 3. Mask: 255.255.255.255
- e. Click the **OK** button.
- f. Set the timeout to 10 minutes.
- g. Click the **Apply** button.
- h. If the Preview CLI Commands window appears, click the **Send** button to continue.
- i. From the Student PC, telnet to the PIX
`C:\>telnet 10.0.P.1`
- j. Login with the default password **cisco**.
- k. Exit the telnet session.
- l. Navigate to **Administration>Password** in the tree menu.
- m. Change the Telnet password to **cisco123**.
- n. Click the **Apply** button.
- o. If the Preview CLI Commands window appears, click the **Send** button to continue.
- p. From the Student PC, telnet to the PIX.
`C:\>telnet 10.0.P.1`

- q. Login with the password **cisco123**.
- r. Exit the telnet session.

Note	Telnet is not recommended for remote access since the username and password are sent in clear text. SSH or SSL is recommended.
-------------	--

Step 6 Configure Banners

Complete the following steps to configure the PIX banners.

- a. Navigate to **Administration>Banner** in the tree menu.
- b. Configure the following banners.
 - 1. Session: Session Banner - Authorized users only
 - 2. Login: Login Warning - Authorized users only
 - 3. Message of the Day: MOTD - Authorized users only
- c. Click the **Apply** button.
- d. If the Preview CLI Commands window appears, click the **Send** button to continue.
- e. From the Student PC, telnet to the PIX

```
C:\>telnet 10.0.P.1
```
- f. Login with the password **cisco123**. Note the appearance of the session banner.
- g. Return to the ASDM interface and click on the **Monitoring** button on the main menu bar.
- h. Click on **Administration** in the Features panel and **Telnet Sessions** in the tree menu. Note the **Currently Connected Telnet Sessions**.
- i. On the Student PC, exit the Telnet session.
- j. Return the Telnet monitoring window and click the **Refresh** button. The session entry should disappear.

Step 7 Configure Secure remote access to the PIX Security Appliance

Complete the following steps to configure secure remote access to the PIX for remote configuration.

- a. Click on the **Configuration** button.
- b. Click on **Device Administration** in the Features panel.
- c. Click on **Key Pair** in the tree menu.
- d. Click the **Add** button. The **Add Key Pair** window appears.
- e. Verify that **Use default RSA key** is selected, and that the modulus size is 1024. Click **Generate Now** to create a new RSA key pair to be used when establishing an SSH connection to the PIX.
- f. To configure the hosts that are permitted to make SSH connections to the PIX Security Appliance, click on **Secure Shell** in the tree menu.
- g. Click the **Add** button and then configure the following values:
 - a. Interface Name: inside
 - b. IP Address: 10.0.P.11
 - c. Mask: 255.255.255.255
- h. Click the **OK** button.
- i. Set the timeout to 10 minutes
- j. Click the **Apply** button.

- k. If the Preview CLI Commands window appears, click the **Send** button to continue.
- l. From the student PC, open a SSH client (PuTTY or equivalent) and login into the PIX at 10.0.P.1.
- m. Login with credentials
 - a. Username: pix
 - b. Password: cisco123
- n. Note the banners configured previously.
- o. Return to the ASDM interface and click on the **Monitoring** button on the main menu bar.
- p. Click on **Secure Shell Sessions** in the tree menu. Note the **Currently Connected Secure Shell Sessions**.

Secure Shell Sessions

Currently Connected Secure Shell Sessions.

Client	User	State	Version	Encryption (In)	Encryption (Out)	Host
10.0.1.11	pix	SessionStarted	2.0	aes256-cbc	aes256-cbc	sh...

- q. On the Student PC, exit the SSH session.
- r. Return the Secure Shell monitoring window and click the **Refresh** button. The Session entry should disappear.
- s. Click on **ASDM/HTTPS Sessions** in the tree menu. Note the **Currently Connected ASDM/HTTPS Sessions**.

ASDM/HTTPS Sessions

Currently Connected ASDM/HTTPS Sessions.

Session ID	IP Address
0	10.0.1.11

- t. The current ASDM session will be displayed. Note that this session can be disconnected by selecting the session in the window and then clicking the **Disconnect** button.
- u. Exit PDM. When prompted to save the configuration, click the **Don't Save** button.