

Lab 9.1.7a Configure Access Through the PIX Security Appliance using ASDM

Objective

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

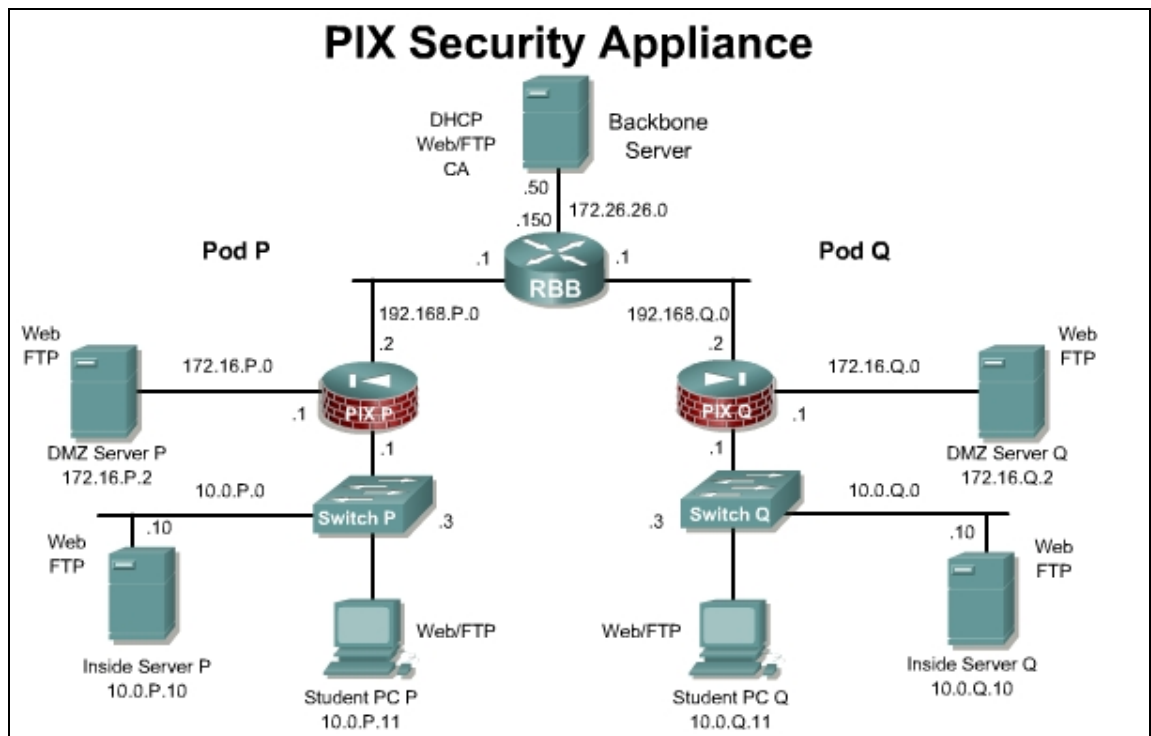
- Use ASDM to verify the starting configuration.
- Configure the PIX Security Appliance to allow inbound traffic to the bastion host using ASDM
- Configure the PIX Security Appliance to allow inbound traffic to the inside host using ASDM
- Test and verify correct PIX Security Appliance operation using ASDM

Scenario

In this exercise, the task is to configure the PIX Security Appliance using ASDM to protect Company XYZ internal network and public web services from intruders.

Topology

This figure illustrates the lab network environment.



Preparation

Begin with the standard lab topology and verify the starting configuration on the pod PIX Security Appliances. 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

Further information about the objectives covered in this lab can be found at, http://www.cisco.com/application/pdf/en/us/guest/products/ps6121/c1225/ccmigration_09186a008045786c.pdf

Step 1 Verify the starting configuration.

The starting configuration should be loaded for this lab. Verify the configuration.

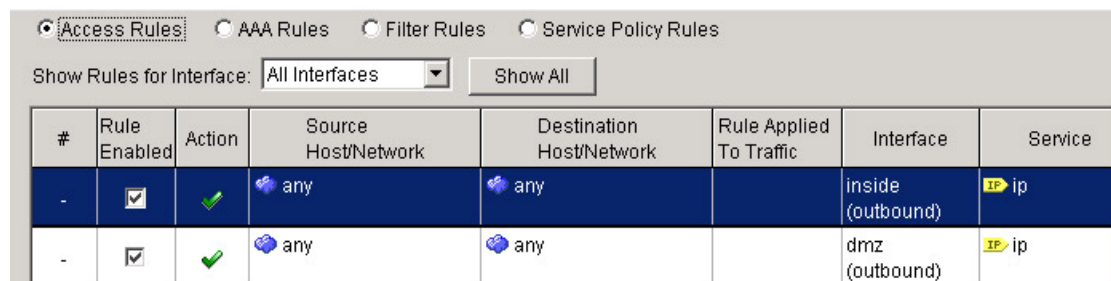
- a. From the student PC web browser, log into ASDM

https://10.0.P.1

(Where P= pod number)

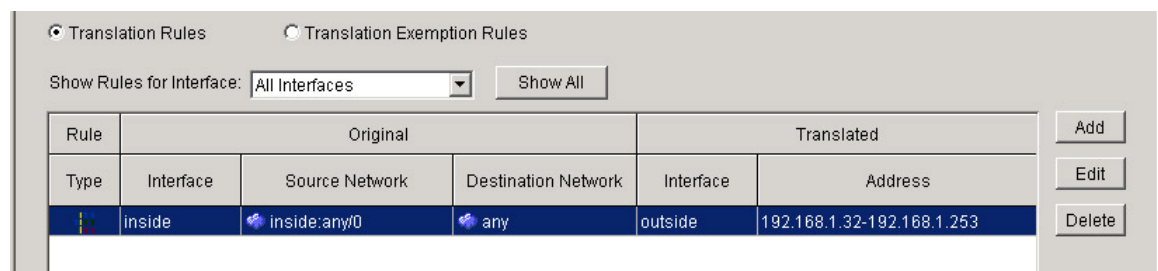
- b. Click on the **Configuration** button.

- c. Click on **Security Policy** in the **Features** tab, and verify that there are rules to allow traffic from inside (outbound) and dmz (outbound).



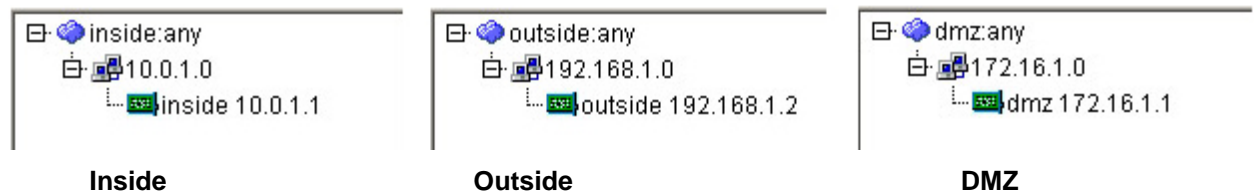
#	Rule Enabled	Action	Source Host/Network	Destination Host/Network	Rule Applied To Traffic	Interface	Service
-	<input checked="" type="checkbox"/>		any	any		inside (outbound)	IP ip
-	<input checked="" type="checkbox"/>		any	any		dmz (outbound)	IP ip

- d. Click on the **NAT** in the **Features** panel, and verify the NAT configuration.



Rule	Original			Translated		
Type	Interface	Source Network	Destination Network	Interface	Address	
	inside	inside: any/0	any	outside	192.168.1.32-192.168.1.253	<div>Add Edit Delete</div>

- e. Click on the **Building Blocks** in the **Features** panel, and then select **Hosts/Networks** from the tree menu. Verify the inside, outside, and DMZ address configuration. A sample from Pix1 is shown below.



- f. Click on the **Interfaces** in the **Features** panel.
- g. Verify the inside, outside, and DMZ address configuration. A sample from Pix1 is shown below.

Interface	Name	Enabled	Security Level	IP Address	Subnet Mask	Management Only	MTU
Ethernet1	inside	Yes	100	10.0.1.1	255.255.255.0	No	1500
Ethernet2	dmz	Yes	50	172.16.1.1	255.255.255.0	No	1500
Ethernet0	outside	Yes	0	192.168.1.2	255.255.255.0	No	1500

- h. Click on **Routing** in the **Features** panel, and select **Static Route** from the tree menu. Verify the default outbound route.

The screenshot shows the 'Static Route' configuration window. It has a title bar 'Static Route' and a subtitle 'Specify static routes.' Below this is a table with the following data:

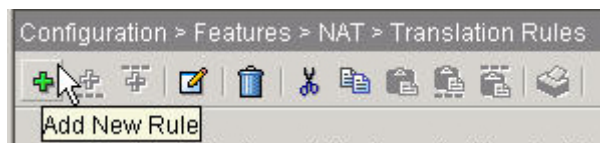
Interface	IP Address	Netmask	Gateway IP	Metric	Tunneled
outside	0.0.0.0	0.0.0.0	192.168.1.1	1	No

- i. Navigate to **Tools>Ping...** and ping the following addresses.
- RBB: 192.168.P.1 and 172.26.26.150
 - SuperServer 172.26.26.50
 - DMZ: 172.16.1.2
- j. Using a web browser, test connectivity from the Student PC to the RBB web interface:
http://172.26.26.150
- k. Using a web browser, test connectivity from the Student PC to the SuperServer web interface:
http://172.26.26.50

Step 2 Configure the PIX Security Appliance to Allow Users on the Inside Interface to Access the Bastion Host

In this step, access will be configured to allow traffic from the inside network to access the DMZ network.

- Click on the **NAT** in the Features panel.
- Click on the **Add New Rule** icon or click on **Rules>Add** from the menu.



- c. The **Add Address Translation Rule** window appears

Use NAT ☒ Use Policy NAT ☐

Source Host/Network

Interface:

IP Address:

Mask:

Browse ...

NAT Options...

Translate Address on Interface:

Translate Address To

☐ Static ☒ Dynamic

Static IP Address:

☐ Redirect port

☒ TCP ☐ UDP

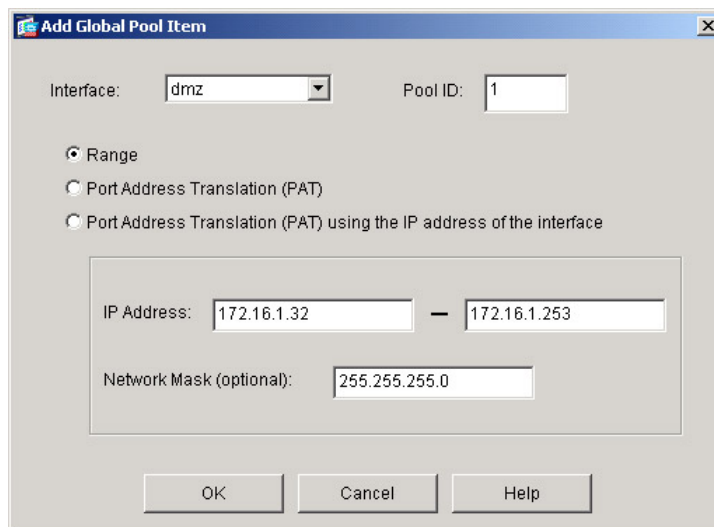
Original port: Translated port:

Dynamic Address Pool: Manage Pools...

Pool ID	Address
N/A	No address pool defined

OK Cancel Help

- d. Click on the **Browse** button and select the **inside:any/0** network
- e. In the **Translate address on interface** drop down menu, verify that **dmz** is selected.
- f. Click on the **Manage Pools** Button. The **Manage Global Address Pools** window appears.
- g. Click on the **Add** button. The **Add Global Pool Item** window appears.
- h. Choose **dmz** for the interface and enter a Pool ID: of **1**. Enter a Range of **172.16.P.32 – 172.16.P.253** with a mask of **255.255.255.0**



Add Global Pool Item

Interface: Pool ID:

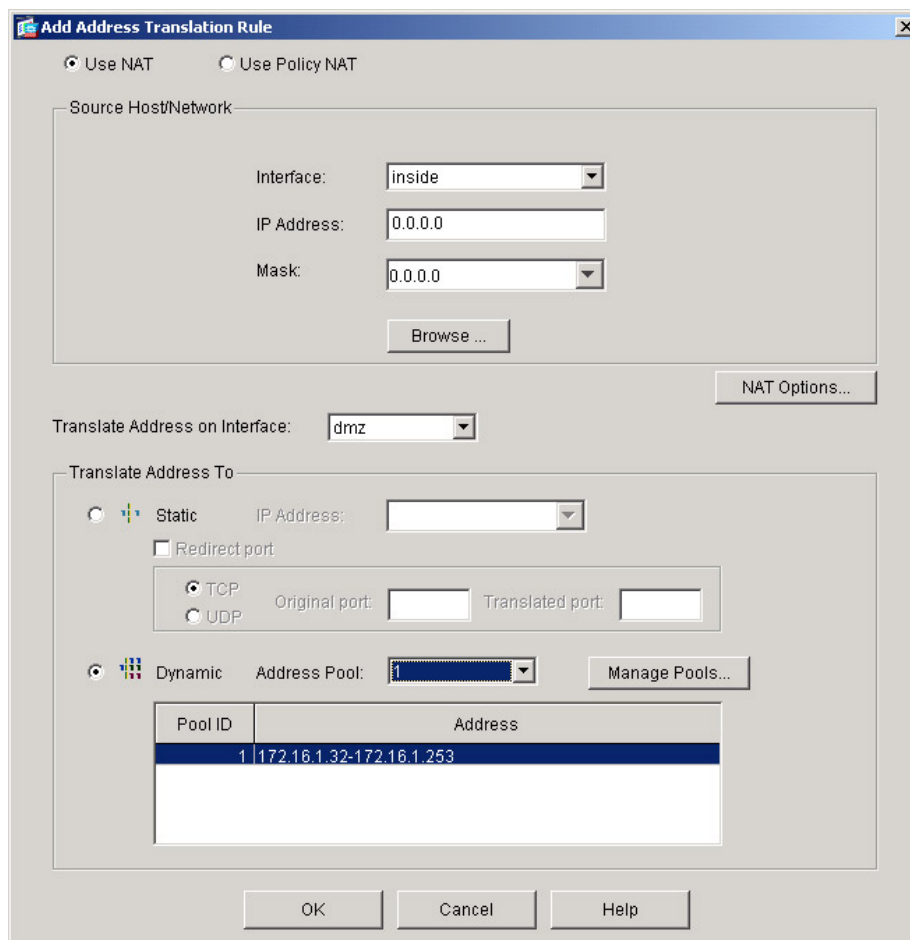
☒ Range
☐ Port Address Translation (PAT)
☐ Port Address Translation (PAT) using the IP address of the interface

IP Address: —

Network Mask (optional):

OK Cancel Help

- i. Click the **OK** button to return to the **Manage Global Address Pools** window.
- j. Click **OK** to return to the **Add Address Translation Rule** window.
- k. In the Dynamic Address pool drop down menu, Select 1



Add Address Translation Rule

☒ Use NAT ☐ Use Policy NAT

Source Host/Network

Interface:

IP Address:

Mask:

Browse ...

NAT Options...

Translate Address on Interface:

Translate Address To

☐ Static IP Address:

☐ Redirect port







☒ TCP Original port: Translated port:
☐ UDP

☒ Dynamic Address Pool: Manage Pools...

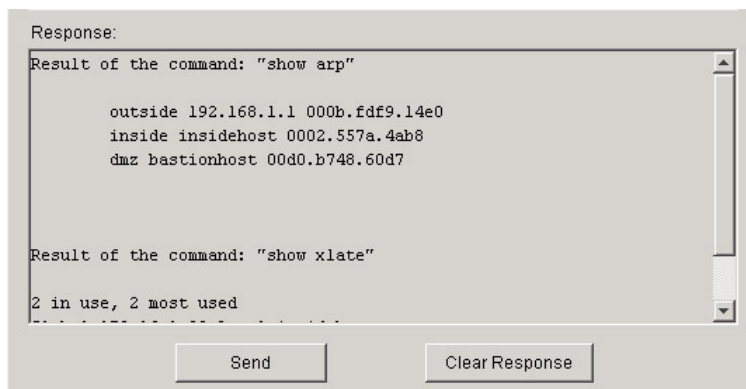
Pool ID	Address
1	172.16.1.32-172.16.1.253

OK Cancel Help

- l. Click **OK** to return to the main **Translation Rules** window.
- m. Click on the **Apply** button. If the **Preview CLI Commands** window appears, click the **Send** button to continue.

Rule	Original			Translated	
Type	Interface	Source Network	Destination Network	Interface	Address
	inside	 inside:any/0	 any	dmz	172.16.1.32-172.16.1.253
	inside	 inside:any/0	 any	outside	192.168.1.32-192.168.1.25

- n. Go to **Tools>Command Line Interface...** and issue a `clear xlate` command.
- o. Close the **Command Line Interface** window. If a **Confirm Configuration Refresh** dialog box appears, click the **Yes** button to continue.
- p. Test web access to the pod bastion host from the pod PC using the web browser to access the pod bastion host by entering **http://172.16.P.2**. The home page of the bastion host should appear on the web browser.
- q. Return to **Tools>Command Line Interface...** Use the `show arp`, `show conn`, and `show xlate` commands to observe the transaction:



- r. Click on the **Close** button.
- s. Test the FTP access to the bastion host from the PC. Verify that there is an FTP server running on the DMZ server.
- t. Establish an FTP session using a command prompt, web browser, or ftp client. If a web browser or ftp client is used, the Passive FTP option must be available and enabled in the FTP client application.
- u. For a command prompt, choose **Start > Run > ftp 172.16.P.2**. If the following message appears, this indicates the bastion host has been reached:

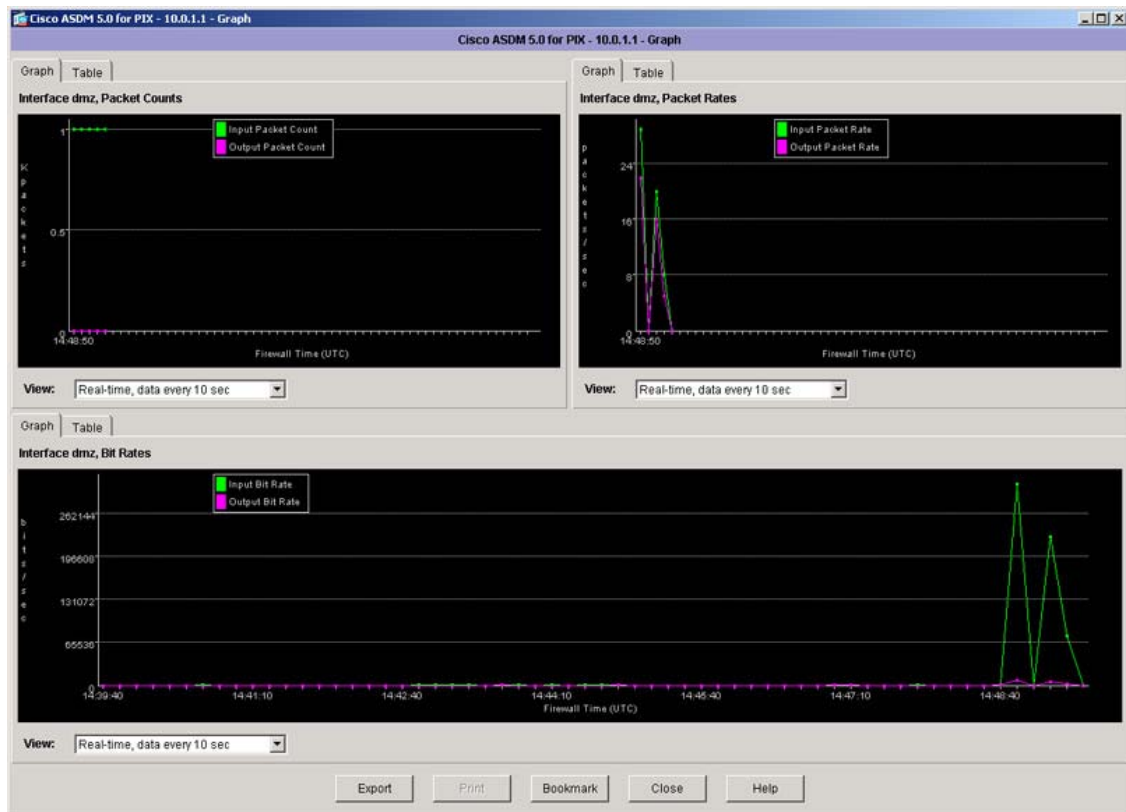

```
"Connected to 172.16.P.2."
```

 (where P = pod number)
- v. Log into the FTP session:


```
User (172.16.P.2(none)): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password: cisco
```

 (where P = pod number)
- w. In ASDM, click on the **Monitoring** button.
- x. Click on **the Interface Graphs>DMZ** in the tree menu.
- y. Add the following to the graph list and Click the **Graph It!** button.
 - a. Packet Counts

- b. Packet Rates
- c. Bit Rates
- z. Download a large file to the Student PC.
- aa. Observe the traffic graph in real time.



- bb. Log out of the FTP session and close the traffic graph window.

Step 3 Configure Access from the Outside to the Bastion Host

Configure a static translation so that traffic originating from the bastion host always has the same source address on the outside interface of the PIX Security Appliance. Then configure an ACL to allow users on the outside interface to access the bastion host.

- a. On the Configuration page, click on the **NAT** in the **Features** panel.
- b. Click on the **Add New Rule** icon or click on **Rules>Add** from the menu. The **Add Address Translation Rule** window appears.
- c. Create a static translation for the pod bastion host. Use the IP address 172.16.P.2 /32 for the bastion host. Translate this address to the static outside address 192.168.P.11. A sample screenshot of Pix1 is shown below.

- d. Click the **OK** button to return to the main translation tab window.
- e. Click the **Apply** button. Notice the new static translation is added to the existing list of 2 dynamic translation entries.

Rule	Original			Translated	
	Type	Interface	Source Network	Destination Network	Address
		dmz	bastionhost 172.16.1.2	any	outside 192.168.1.11
		inside	inside:any/0	any	dmz 172.16.1.32-172.16.1.253
		inside	inside:any/0	any	outside 192.168.1.32-192.168.1.25

- f. After the static entry is complete, the next step is to define an ACL to permit web and ftp traffic associated with the static entry.
- g. Click on **Security Policy** in the **Features** panel.
- h. Click on the **Add New Rule** icon. The **Add Access Rule** window appears.
- i. Configure the ACL as follows
 1. Action: Permit
 2. Source: Outside (0.0.0.0/0.0.0.0)
 3. Destination: dmz –bastionhost 172.16.1.2
- j. Verify that **TCP** is selected in the Protocol and Service group box.
- k. Verify that = is chosen in the Service drop-down menu within the Source Port group box.

- l. Verify that **any** appears in the Service field within the Source Port group box.
- m. Verify that = is chosen in the Service drop-down menu within the Destination Port group box.
- n. Click the ... button within the Destination Port group box. The Service window opens.
- o. Choose **http** from the Service list.
- p. Click **OK**. This will return to open the **Add Access Rule** window.
- q. Click **OK** to return to the main **Access Rules** window.
- r. Repeat the same steps to Add an Access Rule for ftp.
- s. Click the **OK** button
- t. Click the **Apply** button.
- u. Click **Send** if the preview CLI Commands window appears. The following Access rules should be displayed in the main Access Rules window.

#	Rule Enabled	Action	Source Host/Network	Destination Host/Network	Rule Applied To Traffic	Interface	Service
-	<input checked="" type="checkbox"/>		any	any		inside (outbound)	ip
-	<input checked="" type="checkbox"/>		any	any		dmz (outbound)	ip
1	<input checked="" type="checkbox"/>		any	bastionhost/ 172.16.1.2	incoming	outside	http/tcp
2	<input checked="" type="checkbox"/>		any	bastionhost/ 172.16.1.2	incoming	outside	ftp/tcp

- v. From a console session on the PIX, clear the translations and turn on packet debugging for the DMZ interface.

```
PixP# clear xlate
PixP# debug packet dmz
```

- w. Test web access to the bastion host. Observe the debug output while the connections occur.

Option 1: Peer pod groups complete the testing.

- i. Open a web browser on the Student PC.
- ii. Use the web browser to access the bastion host of the peer pod group:
http://192.168.Q.11 (where Q = peer pod number)
- iii. Use the web browser or ftp client to access the bastion host of the peer pod group:
ftp://192.168.Q.11 (where Q = peer pod number)
- iv. Have a peer pod group test the configuration in the same way.

Option 2: Independent testing – From an Internet PC located on the outside (172.26.26.0/24) network, test access to the DMZ server. The internet PC can be configured to receive IP settings from the DHCP server function of RBB.

- i. Open a web browser on the Internet PC.
- ii. Use the web browser to access the bastion host:
http://192.168.P.11 (where P = pod number)
- iii. Use the web browser or ftp client to access the bastion host:
ftp://192.168.P.11 (where P = pod number)
- iv. Have a peer pod group test the configuration in the same way.

- v. If you are using a Windows 2K Superserver, you may need to enter a static route statement using a command prompt on the Superserver:

```
C:\> route add 172.26.26.220 mask 255.255.255.255 172.16.P.1
```

(where 172.26.26.220 is the Internet PC address)

- x. From a console session on the PIX, disable the debugging.

```
PixP# no debug packet dmz
```

```
PACKET trace off
```

- y. In ASDM, navigate to **File>Show Running Configuration in New Window**. Note the configuration statements that have been added from this Step.

```
access-list outside_access_in permit tcp any host 192.168.1.11 eq  
www
```

```
access-list outside_access_in permit tcp any host 192.168.1.11 eq  
ftp
```

```
static (dmz,outside) 192.168.1.11 bastionhost netmask  
255.255.255.255
```

```
access-group outside_access_in in interface outside
```

Step 4 Configure Inbound Access to the Student PC

Complete the following steps to configure the PIX Security Appliance to permit inbound access to the Student PC on the inside interface:

- a. Create a static translation for the inside host by completing the following sub-steps:
 - i. Select **NAT** from the **Features** panel.
 - ii. Select the **Add New Rule** icon in the toolbar. The **Add Address Translation Rule** window opens.
 - iii. Verify that the **inside** interface is chosen in the Interface drop-down menu for the **Source/Host Network** group box.
 - iv. Enter the IP address **10.0.P.11** and subnet mask **255.255.255.255** for the inside host.
(where P = pod number)
 - v. Verify that **outside** is chosen in the **Translate Address on Interface** drop-down menu.
 - vi. Select **Static** in the **Translate address To** group box.
 - vii. Enter **192.168.P.10** in the IP Address field.
(where P = pod number)

- viii. Click **OK**. The new rule appears on the Translation Rules tab.
 - ix. Click **Apply**. The Preview CLI Commands window opens.
 - x. Click **Send**.
- b. Configure an ACL to allow ping through the PIX Security Appliance by completing the following sub-steps:
- i. Select **Security Policy** from the **Features** panel.
 - ii. Click on the **Add New Rule** icon. The **Add Access Rule** window appears.
 - iii. Verify that **permit** is chosen in the **Select an action** drop-down menu.
 - iv. Choose **outside** from the **Interface** drop-down menu in the **Source Host/Network** group box.
 - v. Choose **inside** from the **Interface** drop-down menu in the **Destination Host/Network** group box.
 - vi. Select **ICMP** in the **Protocol and Service** group box.
 - vii. Verify that **any** is selected in the **ICMP type** group box.

Add Access Rule

Action
 Select an action: **permit**
 Apply to Traffic: **incoming to src interface**

Source Host/Network
☒ IP Address ☐ Name ☐ Group
 Interface: **outside**
 IP address: **0.0.0.0**
 Mask: **0.0.0.0**

Destination Host/Network
☒ IP Address ☐ Name ☐ Group
 Interface: **inside**
 IP address: **0.0.0.0**
 Mask: **0.0.0.0**

Time Range
 Time Range: **-- Not Applied --** **New...**

Syslog
 Default Syslog **More Options...**

Rule Flow Diagram
 Rule applied to traffic incoming to source interface
 any — outside —> [Firewall] —> inside —> any
 Allow traffic

Protocol and Service
☐ TCP ☐ UDP ☒ **ICMP** ☐ IP **Manage Service Groups...**
 ICMP Type
 ICMP type: **any**

Please enter the description below (optional):

OK **Cancel** **Help**

- viii. Click **OK**. The new rule appears in the **Access Rules** window.
 - ix. Click **Apply**. The Preview CLI Commands window opens.
 - x. Observe the ACLs to be sent to the PIX Security Appliance.
 - xi. Click **Send**.
- c. Ping the inside host of the peer pod from the internal host. Be sure to coordinate with the peer pod:
- ```
C:\> ping 192.168.Q.10
```
- Pinging 192.168.Q.10 with 32 bytes of data:
- ```
Reply from 192.168.Q.10: bytes=32 time<10ms TTL=125>
Reply from 192.168.Q.10: bytes=32 time<10ms TTL=125>
Reply from 192.168.Q.10: bytes=32 time<10ms TTL=125>
Reply from 192.168.Q.10: bytes=32 time<10ms TTL=125>
```
- (where Q = peer pod number)
- d. Configure an ACL to allow Web access to the inside host from the outside by completing the following sub-steps:
- i. Select **Security Policy** from the **Features** panel.
 - ii. Click on the **Add New Rule** icon. The **Add Access Rule** window appears..

- iii. Verify that **permit** is chosen in the **Select an action** drop-down menu.
- iv. Choose **outside** from the **Interface** drop-down menu within the **Source Host/Network** group box.
- v. Choose **inside** from the **Interface** drop-down menu within the **Destination Host/Network** group box.
- vi. Click the ... button in the **Destination Host/Network** group box. The **Select host/network** window opens.
- vii. Verify that **inside** is chosen in the interface drop-down menu.
- viii. Select the IP address of the inside host:
`10.0.P.11`
 (where P = pod number)
- ix. Click **OK**. The **Add Access Rule** window becomes active.
- x. Select **TCP** in the **Protocol and Service** group box.
- xi. Verify that **=** is chosen in the **Service** drop-down menu within the **Source Port** group box.
- xii. Verify that **any** appears in the **Service** field within the **Source Port** group box.
- xiii. Verify that **=** is chosen in the **Service** drop-down menu within the **Destination Port** group box.
- xiv. Click the ... button within the **Destination Port** group box. The Service window opens.
- xv. Choose **http** from the **Service** list.
- xvi. Click **OK** to return to the **Add Access Rule** window.
- xvii. Click **OK**.
- xviii. Click **Apply**. The **Preview CLI Commands** window opens.
- xix. Note the ACLs to be sent to the PIX Security Appliance.
- xx. Click **Send**.
- e. Clear current translations by completing the following sub-steps:
 - i. Choose **Tools>Command Line Interface**. The **Command Line Interface** window opens.
 - ii. Enter **clear xlate** in the **Command** field.
 - iii. Click **Send**.
 - iv. Verify that the output in the Response field is similar to the following:

```
Result of the command: "clear xlate"
The command has been sent to the device
```
- f. View current translations by completing the following sub-steps:
 - i. Click **Clear Response** in the **Command Line Interface** window.
 - ii. Enter **show xlate** in the **Command** field.
 - iii. Click **Send**.
 - iv. Verify that the output in the Response field is similar to the following:

```
Result of the command: "show xlate"
2 in use, 4 most used
Global 192.168.1.11 Local bastionhost
Global 192.168.1.10 Local insidehost
```

- v. Click **Close** in the **Command Line Interface** window.
- g. Test web access to the Student PC.

Option 1: Peer pod groups complete the testing.

- i. Open a web browser on the Student PC.
- ii. Use the web browser to access the Student PC of the peer pod group:
http://192.168.Q.10 (where Q = peer pod number)
- iii. Have a peer pod group test the configuration in the same way.

Option 2: Independent testing – From an Internet PC located on the outside (172.26.26.0/24) network, test access to the Student PC.

- i. Open a web browser on the Internet PC.
- ii. Use the web browser to access the Student PC:
http://192.168.P.10 (where P = pod number)
- iii. If you are using a Windows 2K Superserver, you may need to enter a static route statement using a command prompt on the Superserver:

```
C:\> route add 172.26.26.220 mask 255.255.255.255 172.16.P.1
```

(where 172.26.26.220 is the Internet PC address)