



## Lab 4.5.5b Configure a PIX Security Appliance Site-to-Site IPsec VPN Tunnel Using ASDM

### Objective

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

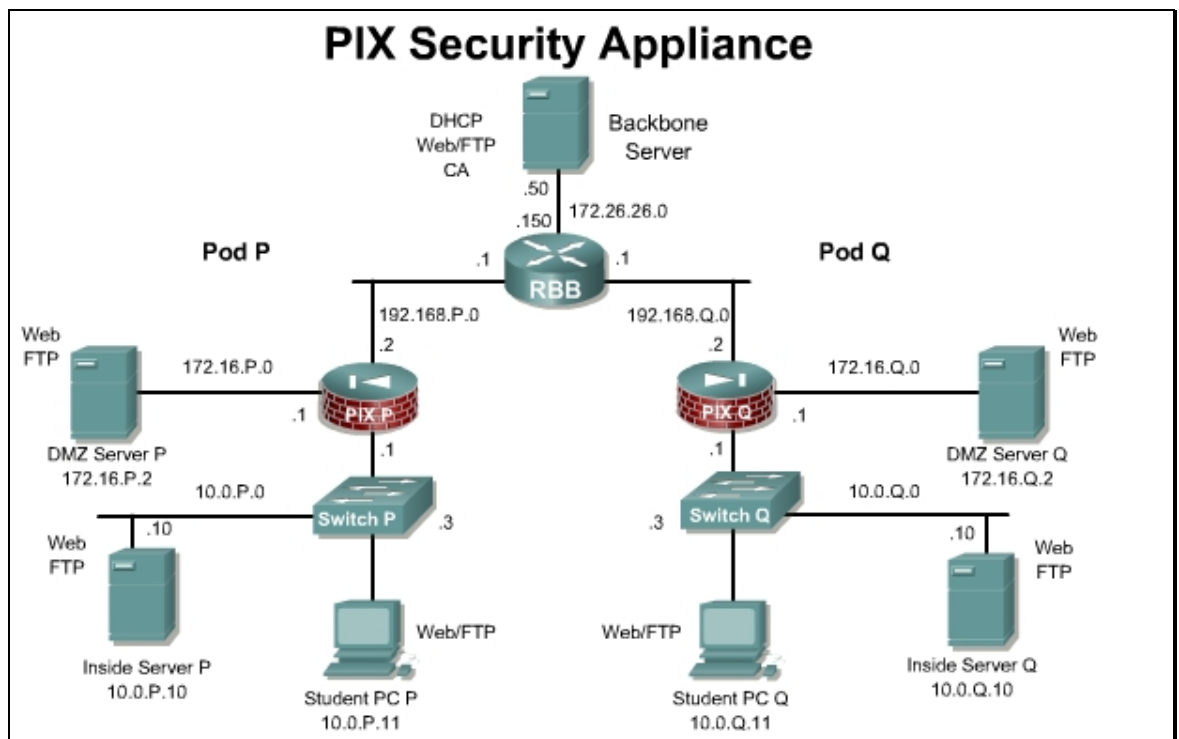
- Configure IKE and IPsec parameters using the ASDM VPN Wizard
- Test and verify IPsec configuration.

### Scenario

A company has just opened a new remote office. The office is currently connected to the Internet through a cable Internet service. The remote office needs to securely access files on the internal network at the main site. In this case, a Site-to-Site VPN should be configured between the Main site (PodP) and remote site (PodQ) PIX Security Appliances.

### Topology

This figure illustrates the lab network environment:



## Preparation

Begin with the standard lab topology and verify the starting configuration on 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

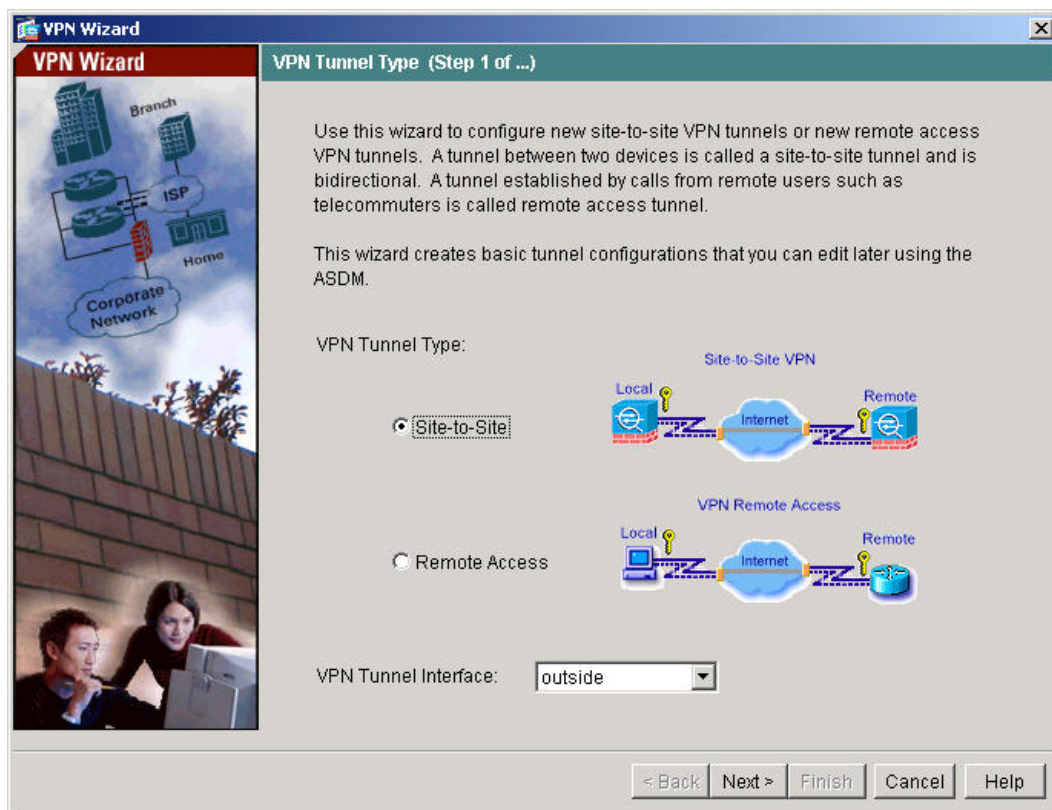
Student can use the following link for more information on the objectives covered in this lab:

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

### Step 1 Create a Secure Site-to-Site VPN using the VPN Wizard

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

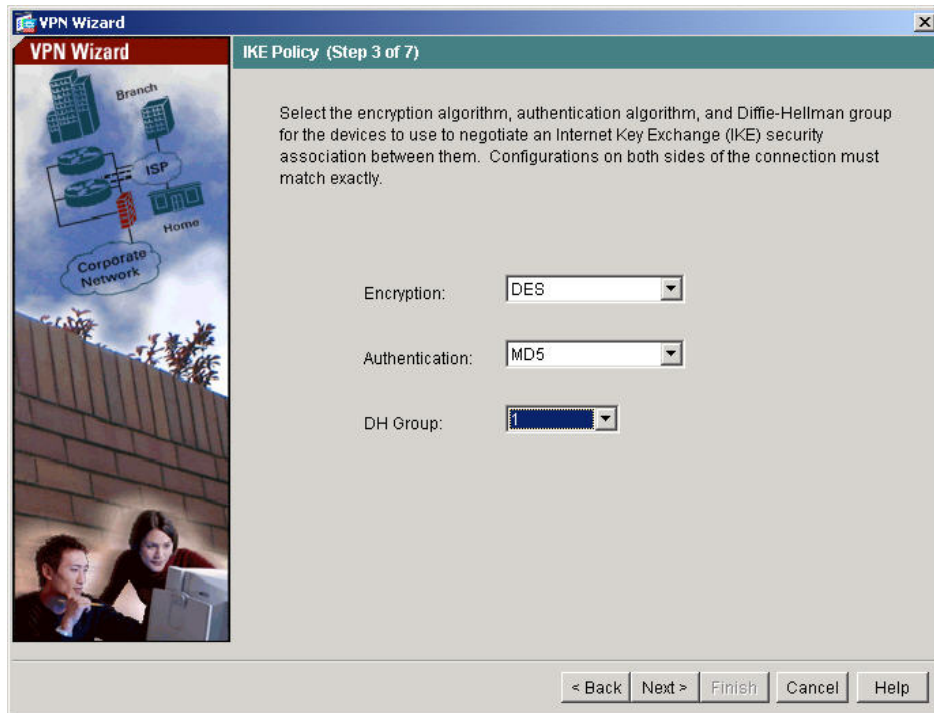
- Initiate an ASDM session with the PIX Security Appliance.
- Choose **Wizards>VPN Wizard** from the main menu. The VPN Wizard window opens.



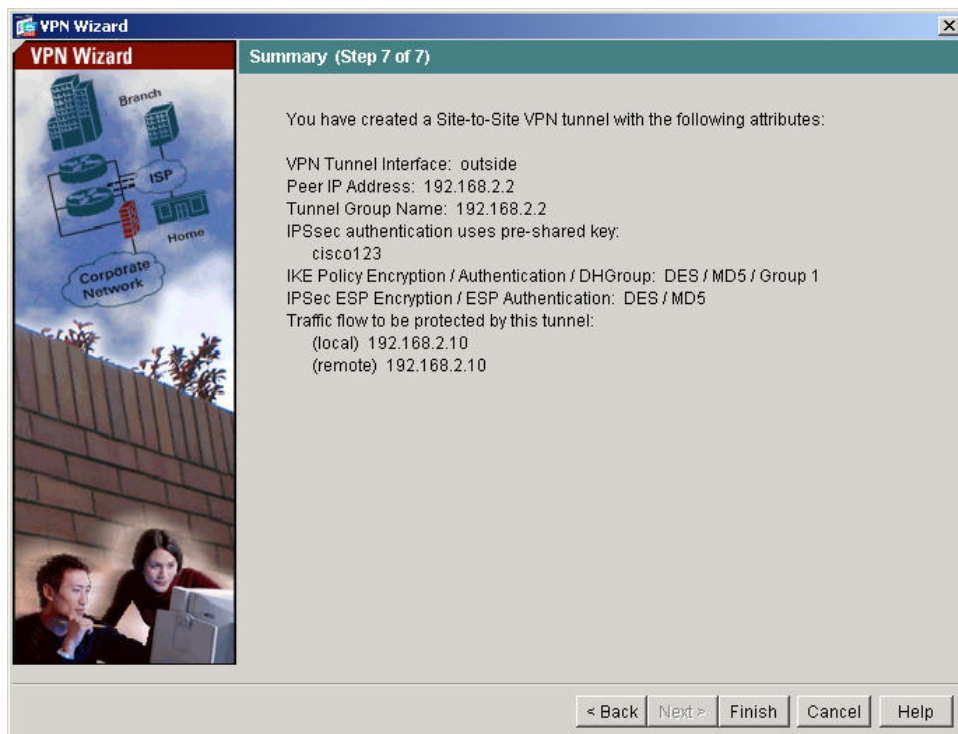
- Verify that the **Site-to-Site VPN** radio button is selected. Verify that the **outside** interface is chosen from the drop-down box.
- Click the **Next** button. The Remote Site Peer window opens. Enter the IP address of the peer pod PIX Security Appliance outside interface, **192.168.Q.2**, in the Peer IP Address field. If the

Tunnel Group Name text box does not auto complete, enter **192.168.Q.2**.  
(where Q = peer pod number)

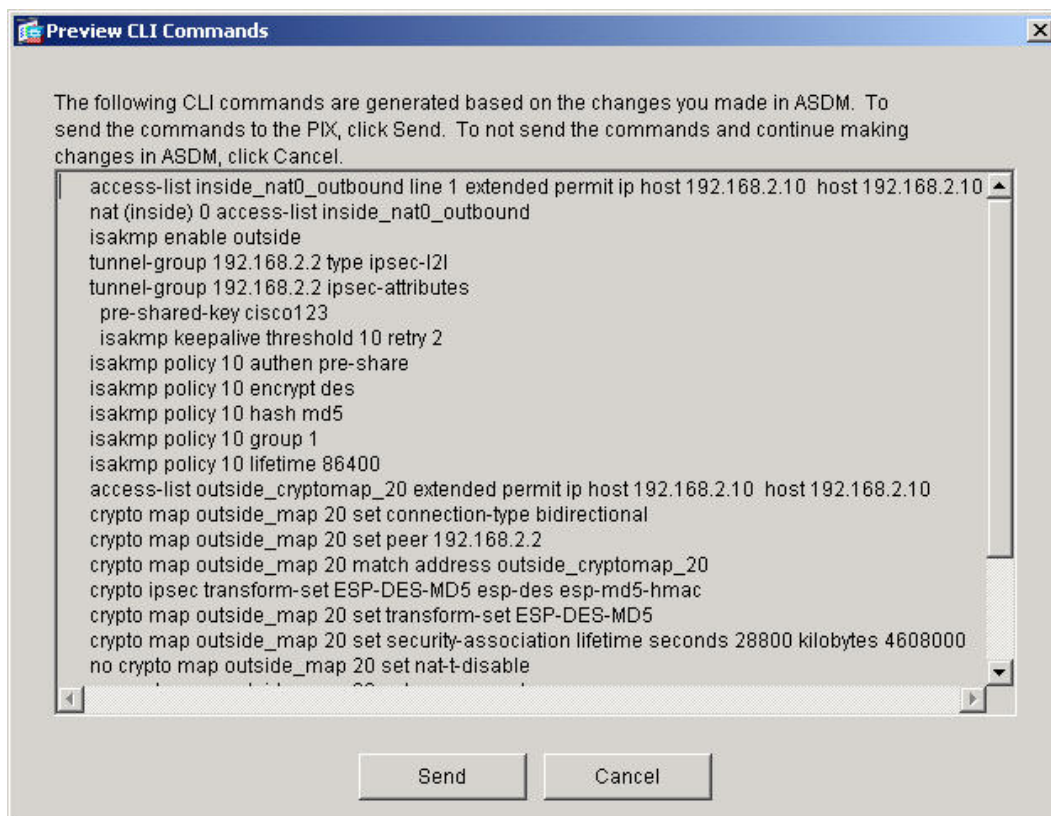
- e. Verify that the Pre-shared Key radio button is selected from the Authentication group box.
- f. Enter **cisco123** in the Pre-shared Key field.
- g. Click the **Next** button. The IKE Policy window opens.



- h. Choose **DES** from the Encryption drop-down menu. Choose **MD5** from the Authentication drop-down menu. Choose **Group 1 (768-bit)** from the DH Group drop-down menu.
- i. Click the **Next** button. The IPSec Encryption and Authentication window opens.



- j. Choose **DES** from the Encryption drop-down menu. Choose **MD5** from the Authentication drop-down menu.
- k. Click **Next**. The Local Hosts and Networks window opens.
- l. Verify that the IP Address radio button is selected within the Host/Network to be added group box. Verify that inside is chosen from the Interface drop-down menu. Enter **192.168.P.10** in the IP Address field.
- m. (where P = pod number)
- n. Choose **255.255.255.255** from the Mask drop-down menu.
- o. Click the **Add >>** button to move the address to the Selected Hosts/Networks list.
- p. Click the **Next** button. The Remote Hosts and Networks window opens. Click **OK**. The Create host/network window opens.
- m. Verify that the IP Address radio button is selected within the Host/Network group box.
- n. Verify that **outside** is chosen in the Interface drop-down menu. Enter the statically mapped IP address of the peer's inside host, **192.168.Q.10**, in the IP Address field. Choose **255.255.255.255** from the Mask drop-down menu. Click the **Add >>** button to move the address to the Selected Hosts/Networks list.
- q. Click the **Next** button. The Summary Window appears.  
Figure Summary Window (3)
- r. Review the VPN parameters and then click the **Finish** button.
- s. The Preview CLI Commands window opens.

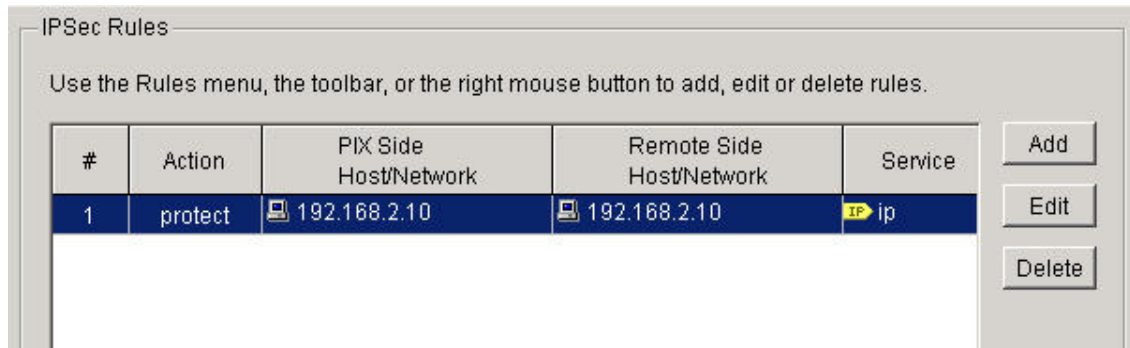


- t. Click **Send**. After the commands are sent the interface returns to the ASDM main window.

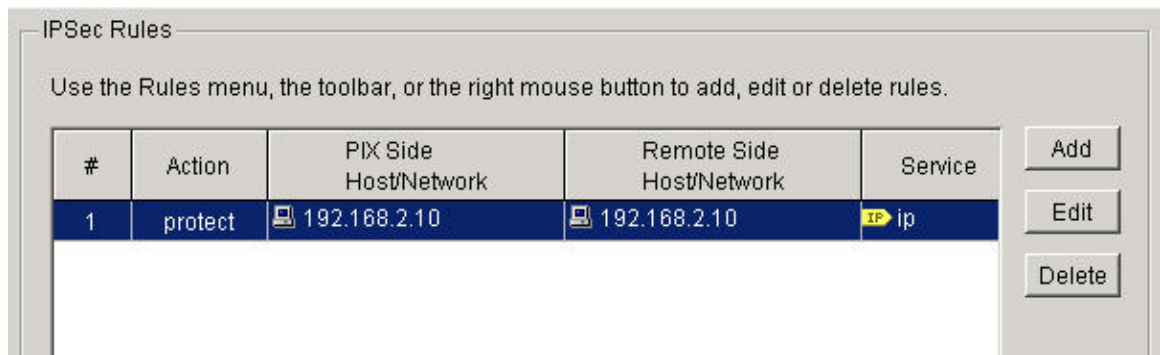
## Step 2 Verify the VPN Configuration

To verify the VPN configuration, complete the following steps:

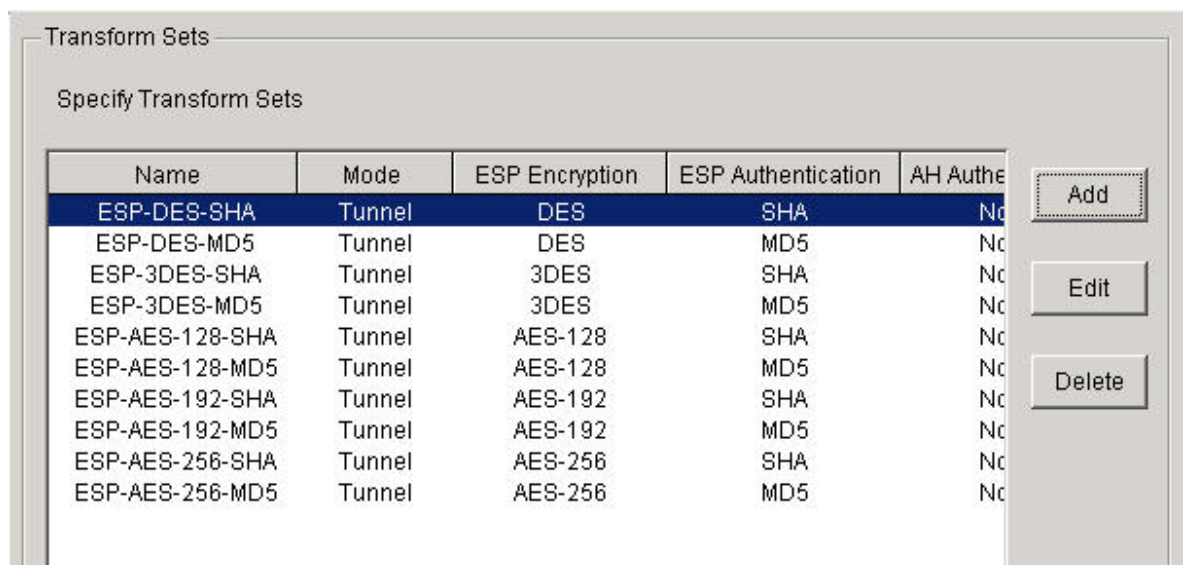
- Click on the **Configuration** button at the top of the ASDM interface.
- Click on the **VPN** in the **Features** panel.
- Click on **IPsec>IPSec Rules** in the tree menu to view the IPSec Rule configuration.



- Click on **IPsec>Tunnel Policy** in the tree menu to view the Tunnel Policy configuration.



- Click on **IPsec>Transform Sets** in the tree menu to view the available transform sets.





- f. Click on **IKE>Policies** in the tree menu to view the IKE Policies.

Policies

Configure specific Internet Key Exchange (IKE) algorithms and parameters, within the IPsec Internet Security Association Key Management Protocol (ISAKMP) framework, for the AH and ESP IPsec protocols.

Priority #	Encryption	Hash	D-H Group	Authentication	Lifetime(secs)
10	des	md5	1	pre-share	86400

Add

Edit

Delete

### Step 3 Test the Site-to-Site VPN

Test the web access to the peer's inside host from the Windows NT server by completing the following sub-steps:

- Open a web browser on the student PC.
- From the Student PC, ping the Peer's inside host

```
C:\> ping 192.168.Q.10
```

Pinging 192.168.2.10 with 32 bytes of data:

```
Reply from 192.168.2.10: bytes=32 time=1ms TTL=128
```

```
Reply from 192.168.2.10: bytes=32 time=1ms TTL=128
```

```
Reply from 192.168.2.10: bytes=32 time=1ms TTL=128
```

```
Reply from 192.168.2.10: bytes=32 time=1ms TTL=128
```

(where Q = peer pod number)

- Use the web browser to access the peer's inside host by entering

**http://192.168.Q.10**

The home page of the peer's inside host should open in the web browser.

- Click on the **Monitoring** button at the top of the ASDM interface.
- Navigate to **VPN Statistics>Sessions** in the tree menu.

Sessions

Remote Access	LAN-to-LAN	Total / Limit	Total Cumulative
0	1	1 / 2000	1

- f. Navigate to **VPN Statistics>Global IKE/IPSec Statistics** in the tree menu. Verify that IKE Protocol is shown in the Show Statistics For drop down menu:

Global IKE/IPSec Statistics

Each row represents one global statistic.

Show Statistics For: IKE Protocol

Statistic	Value
Active Tunnels	1
Previous Tunnels	1
In Octets	2596
In Packets	28
In Drop Packets	0
In Notifys	24
In P2 Exchanges	0
In P2 Exchange Invalids	0
In P2 Exchange Rejects	0
In P2 Sa Delete Requests	0
Out Octets	2728
Out Packets	29
Out Drop Packets	0
Out Notifys	48
Out P2 Exchanges	1
Out P2 Exchange Invalids	0
Out P2 Exchange Rejects	0

- g. Select IPsec Protocol is shown in the Show Statistics For drop down menu:

Global IKE/IPSec Statistics

Each row represents one global statistic.

Show Statistics For: IPSec Protocol

Statistic	Value
Active tunnels	1
Previous tunnels	1
Inbound	
Bytes	621
Decompressed bytes	621
Packets	7
Dropped packets	0
Replay failures	0
Authentications	7
Authentication failures	0
Decryptions	7
Decryption failures	0
Outbound	
Bytes	763
Uncompressed bytes	763
Packets	8
Dropped packets	0

#### Step 4 Configure Stronger Encryption and Authentication (OPTIONAL)

Work with the Peer pod to reconfigure a stronger tunnel policy using 3DES or AES for encryption and SHA for authentication. Change the IKE policy to use AES, SHA, and DH Group 5.

Clear the exiting tunnel by issuing a `clear crypto sa` command. Repeat Step 3.