



Lab 6.5.9a Configure a Secure VPN Using IPsec between a PIX and a VPN Client using ASDM

Objective

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

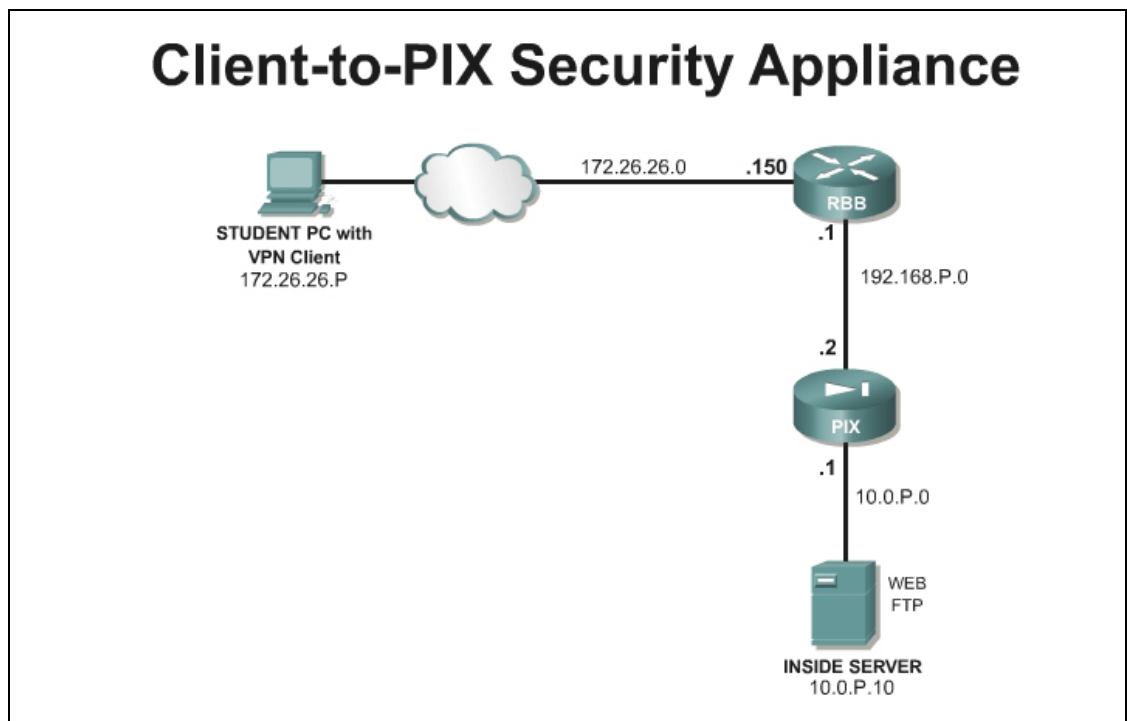
- Configure the PIX Easy VPN Server feature using ASDM.
- Install and configure the Cisco VPN Client on the Student PC.
- Verify and Test the Cisco VPN Client remote access connection

Scenario

A network administrator needs secure management access to the PIX Security Appliance and other critical devices on the internal network. In a small company, the budget may not allow for a dedicated VPN Concentrator. Fortunately, the PIX can be configured as an Easy VPN Remote server, allowing a Cisco VPN software client to connect. Once connected, the remote user can access internal IP based resources. The Easy VPN Server feature can be configured using ASDM.

Topology

This figure illustrates the lab network environment:



Preparation

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

The Cisco VPN 4.6 or later client software is required for this lab. This software can be obtained through the instructor or can be downloaded at <http://www.cisco.com/kobayashi/sw-center/vpn/client/>. A CCO login is required to access this site.

Tools and Resources

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

- Standard Client-to-PIX Security Appliance lab topology
- Console cable
- HyperTerminal
- Cisco VPN Client v4.6 or later

Additional Materials

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

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

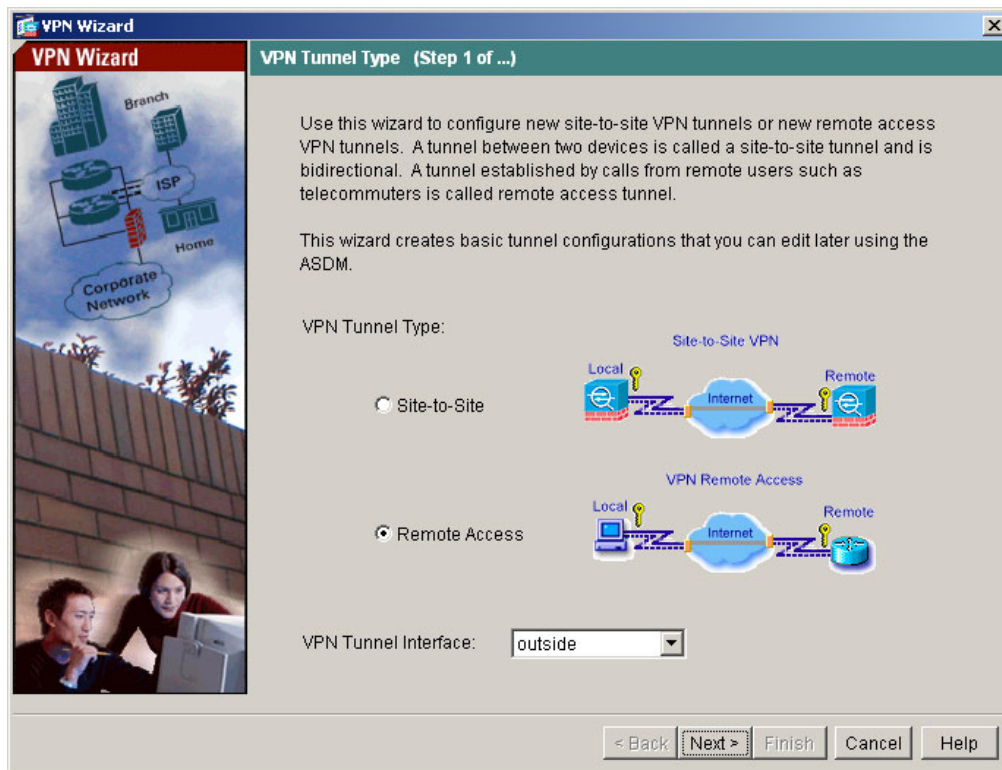
<http://www.cisco.com/en/US/products/sw/secursw/ps2308/index.html>

http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_configuration_guide_chapter09186a0080450bed.html

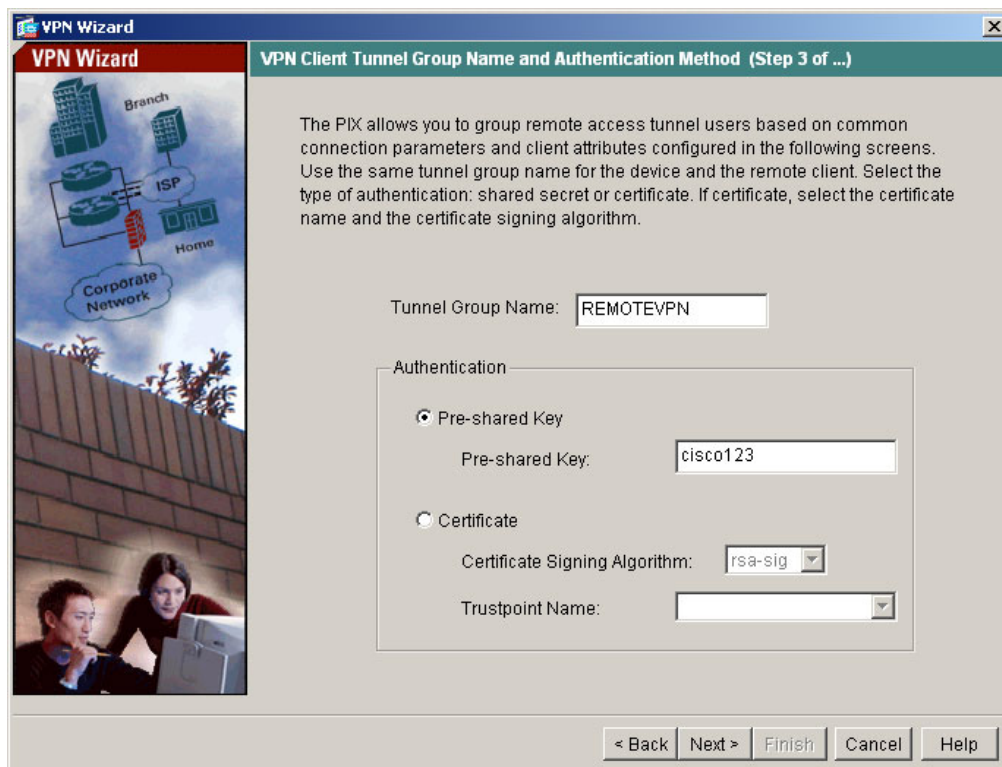
Step 1 Configure the PIX Security Appliance

Complete the following steps to use ASDM to configure the Easy VPN Server feature on the PIX Security Appliance:

- a. Initiate an ASDM session with the PIX Security Appliance.
- b. Choose **Wizards>VPN Wizard**. The VPN Wizard window will launch.
- c. Check the **Remote Access** radio button.
- d. Select the **outside** interface in the drop down list.



- e. Click the **Next** button to continue. The Remote Access Client Window appears.
- f. Verify that the **Cisco VPN Client, Release 3.x or higher, or other VPN Remote product** radio button is chosen. Click **Next**. The VPN Client Tunnel Group Name and Authentication Method window opens.
- g. Enter a Group Name of **REMOTEVPN** with a password of **cisco123**.



- h. Click the **Next** button to continue. The Client Authentication Window appears.

- i. Verify that the **Authenticate using the local user database** radio button is selected.

VPN Wizard
Client Authentication (Step 4 of ...)

To authenticate remote users using local device user database, select the first option below. You can create user accounts in the next screen.

To use external AAA servers instead, select the second option. You can select an existing AAA server group or create a new one using the New button below.

To manage all other AAA settings, use Configuration > Features > Properties > AAA Setup category in the main ASDM window.

☒ Authenticate using the local user database

☐ Authenticate using an AAA server group

AAA Server Group

< Back Next > Finish Cancel Help

- j. Click the **Next** button to continue. The User Accounts window appears.
- k. Add a user **remoteuser** and the password **cisco123**.

VPN Wizard
User Accounts (Step 5 of 11)

Enter a new username/password into the user authentication database. To edit existing entries in the database or to remove them from the database, go to Configuration > Device Administration > Administration > User Accounts in the main ASDM window.

User to Be Added

Username:

Password (optional):

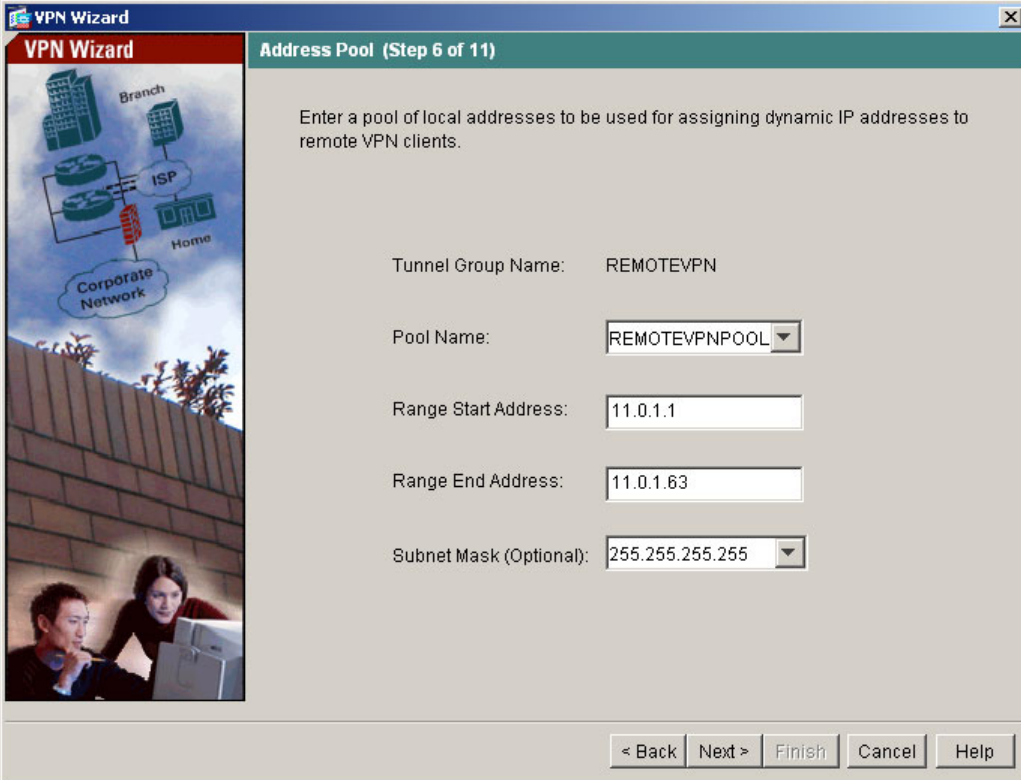
Confirm Password (optional):

Username

< Back Next > Finish Cancel Help

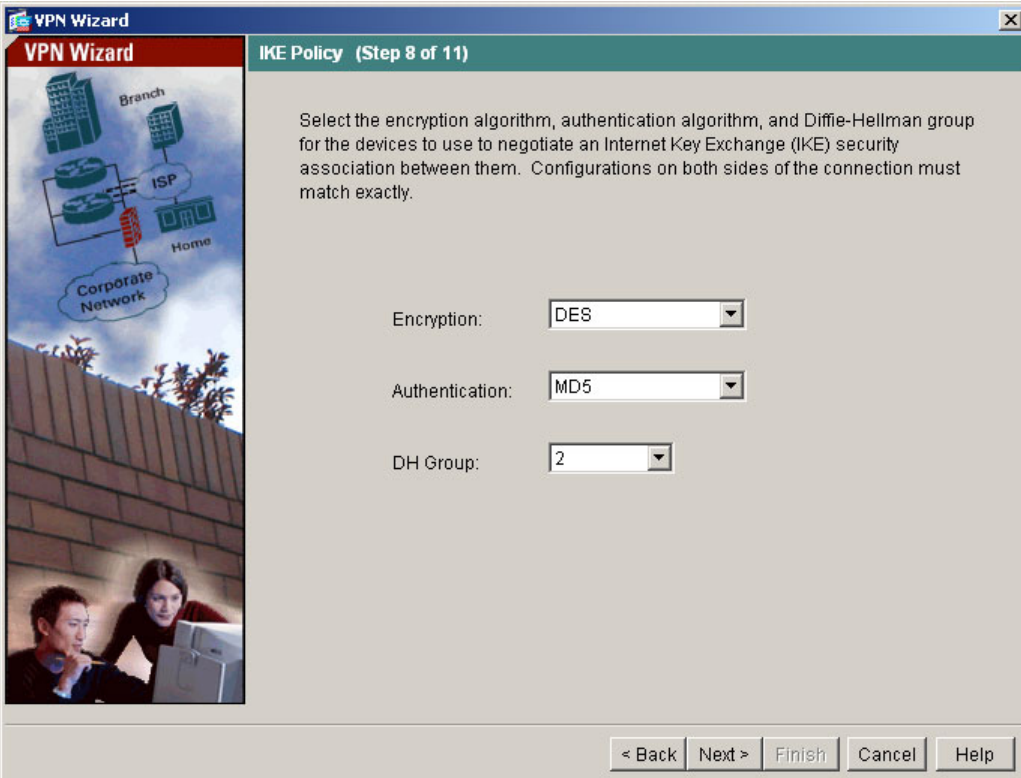
- l. Click the **Next** button to continue. The Address Pool window opens.

- m. Create a pool called **REMOTEVPNPOOL** with a range of **11.0.P.1 – 11.0.P.63**



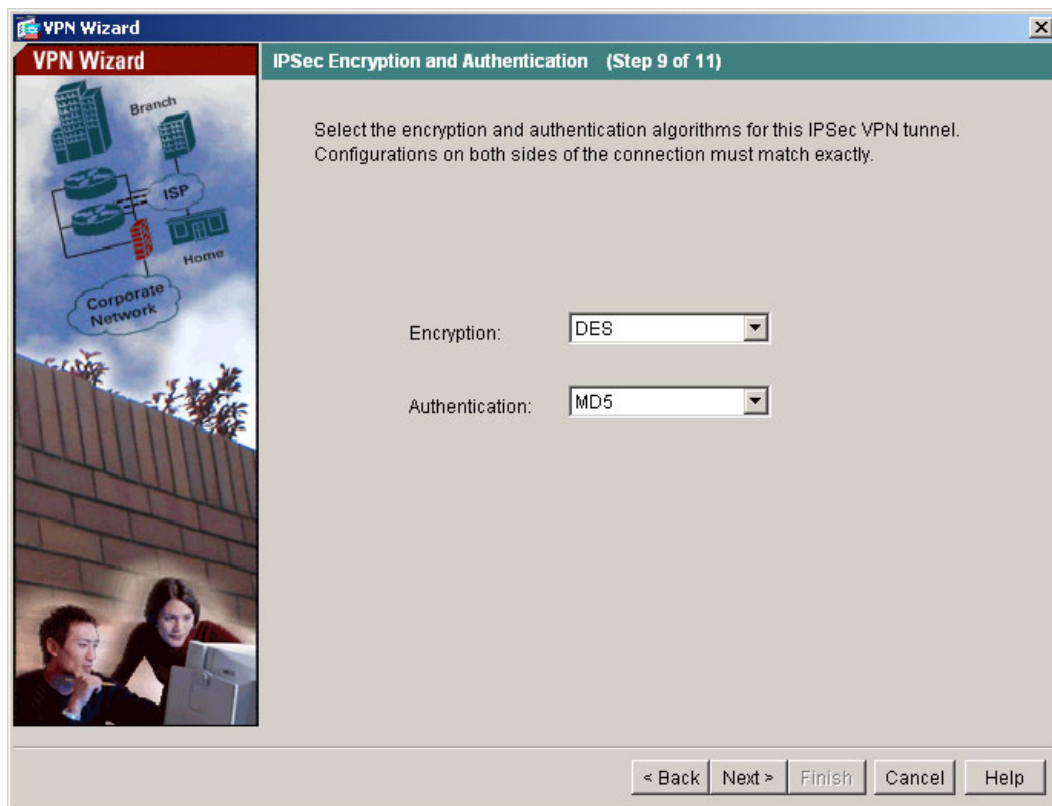
The screenshot shows the 'VPN Wizard' window at 'Address Pool (Step 6 of 11)'. The left sidebar contains a network diagram with 'Branch', 'ISP', 'Home', and 'Corporate Network' components, and an image of two people at a computer. The main area has the instruction: 'Enter a pool of local addresses to be used for assigning dynamic IP addresses to remote VPN clients.' The configuration fields are: Tunnel Group Name: REMOTEVPN; Pool Name: REMOTEVPNPOOL (dropdown); Range Start Address: 11.0.1.1; Range End Address: 11.0.1.63; Subnet Mask (Optional): 255.255.255.255 (dropdown). Navigation buttons at the bottom are '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

- n. Click the **Next** button. The Attributes Pushed to Client window appears.
- o. Click the **Next** button. The IKE Policy window appears.
- p. Configure DES, MD5, and DH Group 2.

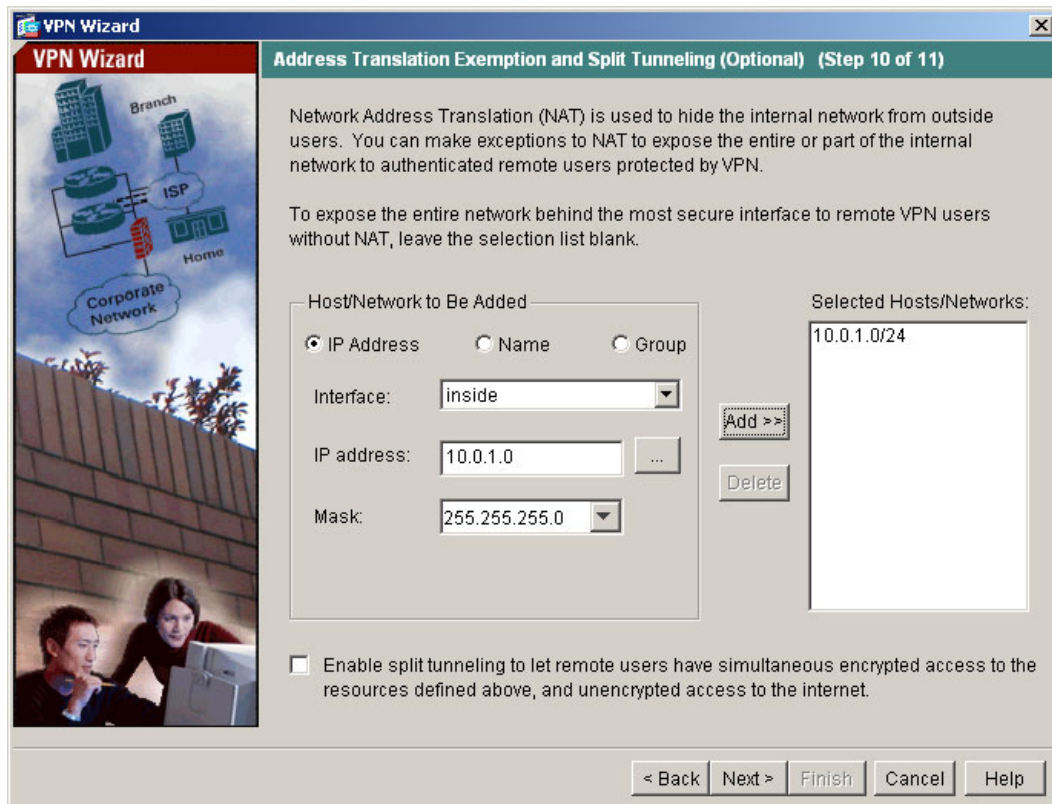


The screenshot shows the 'VPN Wizard' window at 'IKE Policy (Step 8 of 11)'. The left sidebar is identical to the previous window. The main area has the instruction: 'Select the encryption algorithm, authentication algorithm, and Diffie-Hellman group for the devices to use to negotiate an Internet Key Exchange (IKE) security association between them. Configurations on both sides of the connection must match exactly.' The configuration fields are: Encryption: DES (dropdown); Authentication: MD5 (dropdown); DH Group: 2 (dropdown). Navigation buttons at the bottom are '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

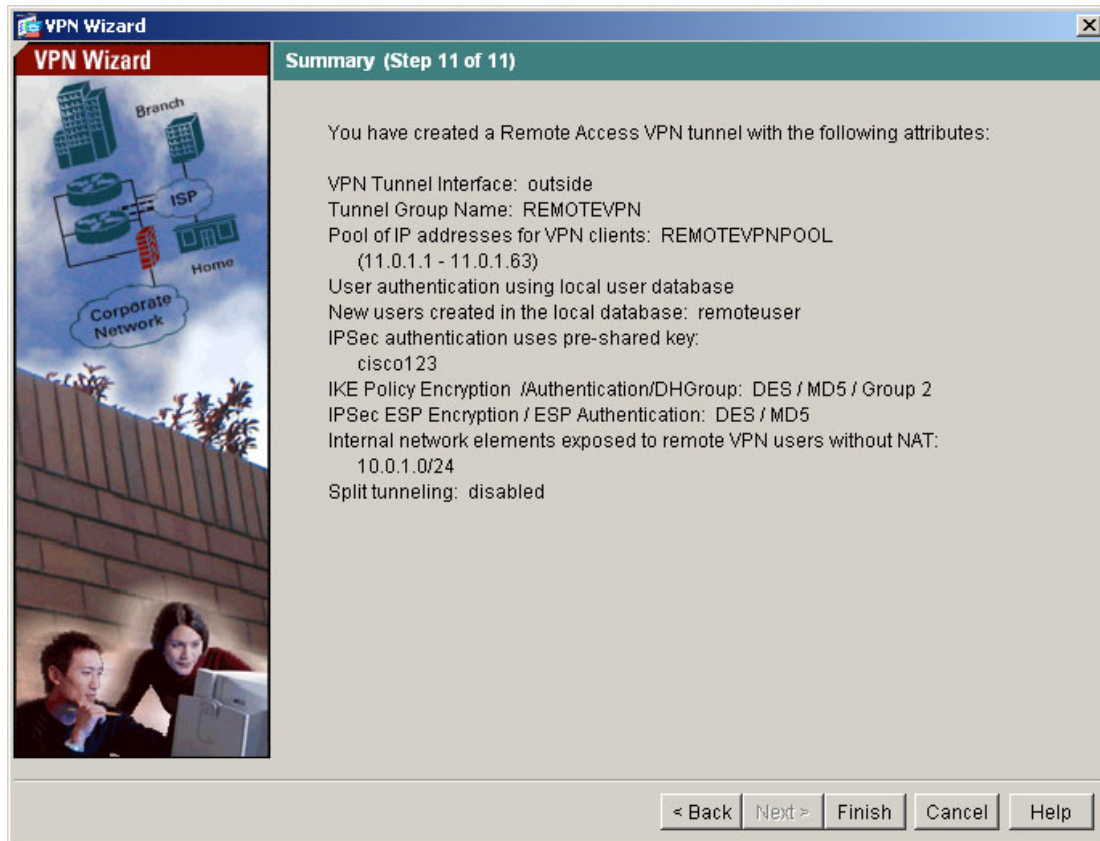
- q. Click the **Next** button. The IPsec Encryption and Authorization window appears.
- r. Choose DES and MD5.



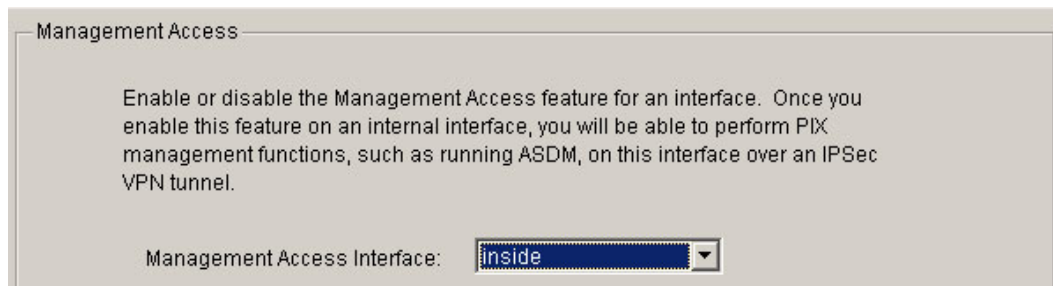
- s. Click the **Next** button. The Address Translation Exemption and Split Tunneling window appears
- t. Click on the ... button and choose the **10.0.P.0** network. Add this to the Selected list.



- u. Click the **Next** button to continue. The Summary window appears.



- v. Click the **Finish** button.
- w. If the Preview CLI commands window appears, click the **Send** button to continue.
- x. Navigate to the **Configuration>Features>Device Administration>Administration>Management Access**.
- y. Choose the **inside** interface in the drop down menu. Click **Apply**. Click **Send** if prompted.



- z. Disconnect the ASDM session.

Step 2 Configure the Student PC Networking Parameters

Certain networking parameters must be configured before the student PC will operate in the lab environment. Complete the following steps to configure the student PC networking parameters.

- a. Move the Student PC connection to the outside network on VLAN 1
- b. Change the IP address and default gateway of the student PC. Obtain a DHCP address from RBB or use the following configuration parameters:

IP address - **172.26.26.P**

(where P = pod number)

Subnet mask - **255.255.255.0**

Default gateway - **172.26.26.150**

- b. Ping the backbone router's IP address. The ping should be successful.

```
C:\> ping 172.26.26.150
```

```
Pinging 172.26.26.150 with 32 bytes of data:
```

```
Reply from 172.26.26.150: bytes=32 time<10ms TTL=128
```

```
Reply from 172.26.26.150: bytes=32 time<10ms TTL=128
```

Step 3 Configure the Networking Parameters of the VPN Client

Use the following procedure to configure the networking parameters of the VPN Client. This procedure assumes Windows 2000 is already running.

- a. Choose **Start>Programs>Cisco Systems VPN Client>VPN Client**. The Cisco Systems VPN Client window opens.
- b. Click **New**. The New Connection Entry wizard opens.
- c. Enter **PixP** as the name in the Connection Entry field. Enter the PIX Security Appliance's public interface IP address, **192.168.P.2**, as the IP address of the remote host.
- b. Enter the following group information in the **Authentication** tab.
 - Enter a group name: **REMOTEVPN**
 - Enter and Confirm a group password: **cisco123**

VPN Client | Properties for "Pix1"

Connection Entry:

Description:

Host:

Authentication | Transport | Backup Servers | Dial-Up

☒ Group Authentication ☐ Mutual Group Authentication

Name:

Password:

Confirm Password:

☐ Certificate Authentication

Name:

☐ Send CA Certificate Chain

Erase User Password | Save | Cancel

- c. In the **Transport** tab, select the **Enable Transparent Tunneling** checkbox.

VPN Client | Properties for "Pix1"

Connection Entry:

Description:

Host:

Authentication | Transport | Backup Servers | Dial-Up

☒ Enable Transparent Tunneling

☒ IPsec over UDP (NAT / PAT)

☐ IPsec over ICP TCP Port:

☐ Allow Local LAN Access

Peer response timeout (seconds):

Erase User Password | Save | Cancel

- d. Click the **Save** button to complete the VPN Client configuration.

Step 4 Launch the VPN Client on the Student PC

Complete the following steps to launch the VPN Client on the student PC:

- a. Choose **Start>Programs>Cisco Systems VPN Client>VPN Client**.
- b. Verify that the Connection Entry is **PixP**.
- c. Verify that the IP address of the remote server is set to the PIX Security Appliance's public interface IP address, **192.168.P.2**.
- d. Click the **Connect** button. Complete the following sub-steps to complete the VPN tunnel connection:
 - i. When prompted for a username, enter **remoteuser**.
 - ii. When prompted to enter a password, enter **cisco123**.



- e. The window closes and a VPN (lock) icon appears in the system tray. This indicates the VPN tunnel has been successfully created.

Step 5 Verify the VPN Connection

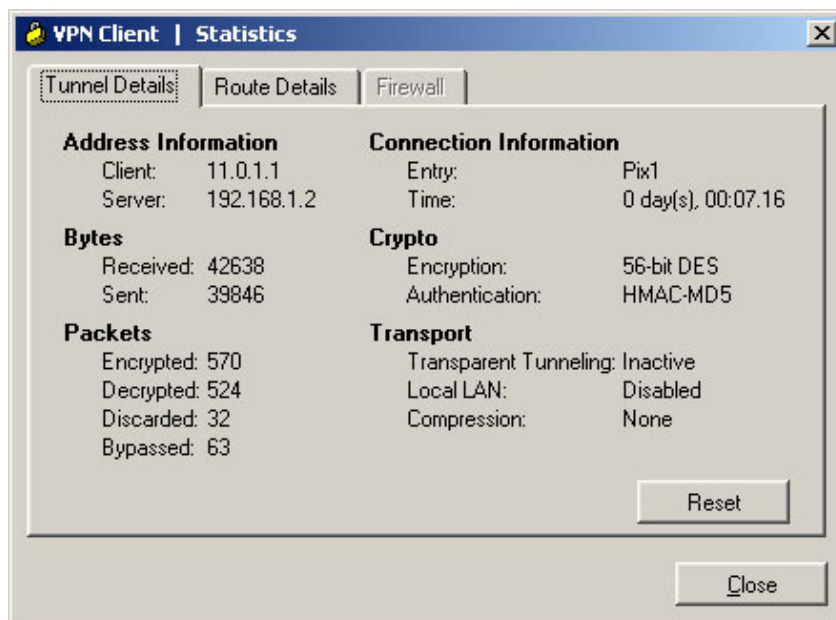
Complete the following steps to verify the IPSec connection:

- a. Open a web browser on the VPN Client PC.
- b. Use the web browser to access the inside web server by entering **http://10.0.P.10**
- c. The web server's home page should display.
- d. On the Student PC, use the browser to attempt to establish an ASDM session.

https://10.0.P.1

This connection to ASDM should fail.

- e. Right-click the VPN Dialer icon in the system tray, then left click on **Statistics** and observe the IP address that was assigned to the student PC. Keep this window open. Note the number of encrypted packets shown on the window.



- f. Console to the PIX Security Appliance. Add the Client IP Address pool to the list of permitted http locations.

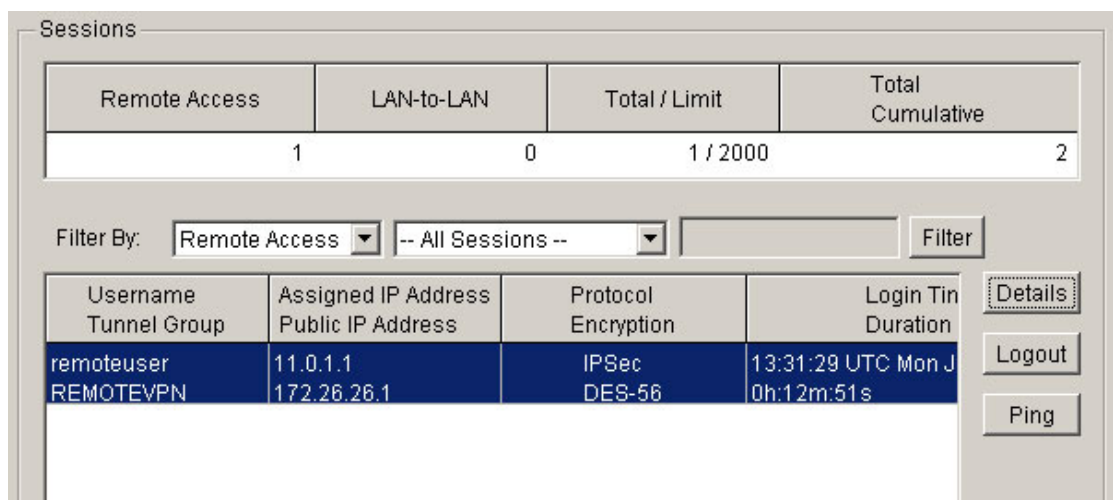
```
Pix1(config)# http 11.0.P.0 255.255.255.192 inside
```

- g. On the Student PC, use the browser to initiate an ASDM session.

https://10.0.P.1

This connection to ASDM should be successful.

- h. Return the **VPN Client Statistics** window tab and view the information provided. Notice the number of packets encrypted and decrypted have increased. Return to ASDM and click on the **Refresh** button. Observe the packet counts increase.
- i. Navigate to **Monitoring>Features>VPN>VPN Statistics>Sessions** to view information about the existing VPN connections.



- j. Click on the **Details** button to view more detailed information about the connection.
- k. Click the **Close** button.
- l. Left click on the VPN lock in the system tray of the student PC and right click on **Disconnect**.
- m. Verify the running configuration with the end configuration for this lab.