



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

Objective

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

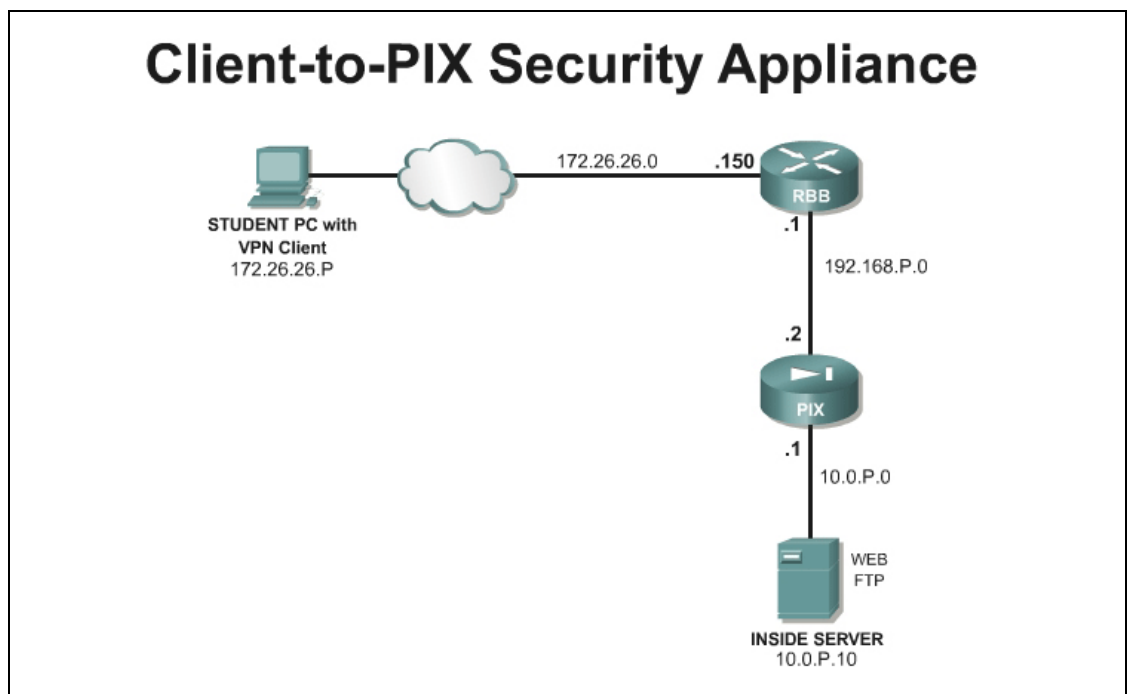
- Configure and Verify the PIX Easy VPN Server feature using CLI
- Install and configure the Cisco VPN Client on a Microsoft Windows end-user PC.
- Verify and Test the Cisco VPN Client remote access connection

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.

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. Also, change the cable of the Student PC to the VLAN1 port.

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 higher

Additional Materials

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

<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

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
address-pool [(<i>interface name</i>)] <i>address_pool1</i> [... <i>address_pool6</i>]	To specify a list of address pools for allocating addresses to remote clients, use the address-pool command in tunnel-group general-attributes configuration mode.
crypto dynamic-map <i>dynamic-map-name</i> <i>dynamic-seq-num</i> set peer <i>ip_address</i> <i>hostname</i>	To specify an IPSec peer in a crypto map entry, use the crypto map set peer command in global configuration mode. The dynamic-map keyword is used to specify a dynamic crypto map set.
crypto ipsec transform-set	To define a transform set, use the crypto ipsec transform-set command in global configuration mode. This command is used to identify the IPSec encryption and hash algorithms to be used by the transform set.
crypto map <i>map-name</i> interface <i>interface-name</i>	Use the crypto map interface command in global configuration mode to apply a previously defined crypto map set to an interface.
isakmp enable <i>interface-name</i>	To enable ISAKMP negotiation on the interface on which the IPSec peer communicates with the PIX Security Appliance, use the isakmp enable command in global configuration mode.

Command	Description
isakmp identity { <i>address</i> <i>hostname</i> <i>key-id</i> <i>key-id-string</i> <i>auto</i> }	To set the Phase 2 ID to be sent to the peer, use the isakmp identity command in global configuration mode.
isakmp policy <i>priority</i> authentication { <i>pre-share</i> <i>dsa-sig</i> <i>rsa-sig</i> }	To specify an authentication method within an IKE policy, use the isakmp policy authentication command in global configuration mode. IKE policies define a set of parameters for IKE negotiation.
nat (<i>real_interface</i>) <i>nat_id</i> <i>real_ip</i> [<i>mask</i> [<i>dns</i>] [<i>outside</i>] [[<i>tcp</i>] <i>tcp_max_conns</i> [<i>emb_limit</i>] [<i>norandomseq</i>]]] [<i>udp</i> <i>udp_max_conns</i>]	To define an address on one interface that is translated to a global address on another interface, use the nat command in global configuration mode. A <i>nat_id</i> of 0 indicates that no address translation takes place for <i>real_ip</i> .
pre-shared-key <i>key</i>	To specify a preshared key to support IKE connections based on preshared keys, use the pre-shared-key command in tunnel-group ipsec-attributes configuration mode.
tunnel-group <i>name</i> general-attributes	To enter the general-attribute configuration mode, use the tunnel-group general-attributes command in global configuration mode. This mode is used to configure settings that are common to all supported tunneling protocols.
tunnel-group <i>name</i> ipsec-attributes	To enter the ipsec-attribute configuration mode, use the tunnel-group ipsec-attributes command in global configuration mode. This mode is used to configure settings that are specific to the IPSec tunneling protocol.

Step 1 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.

- Move the Student PC connection to the outside network on VLAN 1
- 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**

- Ping the IP address of the backbone router. 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 2 Configure the PIX Security Appliance

The instructor will provide the procedures for access to the PIX Security Appliance console port. After accessing the PIX Security Appliance console port, enter configuration mode, and complete the following steps to configure the PIX Security Appliance:

- a. Create two local user accounts for remote clients

```
PixP(config)# username sales password sales123 privilege 3
PixP(config)# username admin password admin123 privilege 15
```

- b. Enable IKE on the outside interface:

```
PixP(config)# isakmp enable outside
```

- c. Set the IKE identity:

```
PixP(config)# isakmp identity address
```

- d. Configure the ISAKMP policy by completing the following substeps:

- i. Configure a basic IKE policy using pre-shared keys for authentication:

```
PixP(config)# isakmp policy 10 authentication pre-share
```

- ii. Verify the isakmp configuration:

```
PixP(config)# show running-config isakmp
isakmp enable outside
isakmp identity address
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption 3des
isakmp policy 10 hash sha
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400
```

- e. Set up a pool of IP addresses that will dynamically be assigned to the Cisco VPN.

Clients via IKE mode configuration:

```
PixP(config)# ip local pool MYPOOL 11.0.P.1-11.0.P.254
(where P = pod number)
```

- f. Insert an access-list to allow remote clients access to the untranslated inside host:

```
PixP(config)# access-list ACLIN line 2 extended permit tcp 11.0.P.0
255.255.255.0 host 10.0.P.10 eq www
(where P = pod number)
```

- g. Set the tunnel-group training name to training and the type to remote access:

```
PixP(config)# tunnel-group training type IPSec_RA
```

- h. Enter the tunnel-group training general-attributes submode:

```
PixP(config)# tunnel-group training general-attributes
```

- i. Set the address pool to MYPOOL:

```
PixP(config-general)# address-pool MYPOOL
```

- j. Enter the tunnel-group training ipsec-attributes submode:

```
PixP(config)# tunnel-group training ipsec-attributes
```

- k. Set the pre-shared key to training:

```
PixP(config-ipsec)# pre-shared-key training
```

- l. Create an access list that permits traffic from the inside network to hosts using addresses from mode-config pool:

```
PixP(config-ipsec)# access-list 101 permit ip 10.0.P.0 255.255.255.0 11.0.P.0 255.255.255.0
```

```
PixP(config-ipsec)# exit
```

(where P = pod number)

- m. Configure the PIX Security Appliance to bypass NAT for VPN traffic:

```
PixP(config)# nat (inside) 0 access-list 101
```

- n. Set up a transform set that will be used for the Cisco VPN Clients:

```
PixP(config)# crypto ipsec transform-set RAVPN esp-3des esp-sha-hmac
```

- o. Set up a dynamic crypto map to enable the Cisco VPN Clients to connect to the PIX Security Appliance:

```
PixP(config)# crypto dynamic-map DYNOMAP 10 set transform-set RAVPN
```

- p. Create a crypto map, and assign the dynamic crypto map to it:

```
PixP(config)# crypto map VPNPEER 20 ipsec-isakmp dynamic DYNOMAP
```

- q. Apply the crypto map to the PIX Security Appliance interface:

```
PixP(config)# crypto map VPNPEER interface outside
```

(where P = pod number)

Step 3 Verify the PIX Security Appliance Configuration

Complete the following steps to verify the PIX Security Appliance configuration:

- a. Verify the IP local pool:

```
PixP(config)# show running-config ip local pool
```

```
ip local pool MYPOOL 11.0.1.1-11.0.1.254
```

- b. Verify the Network Address Translation (NAT) configuration:

```
PixP(config)# show running-config nat
```

```
nat (inside) 0 access-list 101
```

```
nat (inside) 1 10.0.P.0 255.255.255.0
```

(where P = pod number)

- c. Verify the crypto map:

```
PixP(config)# show running-config crypto map
```

```
crypto map VPNPEER 20 ipsec-isakmp dynamic DYNOMAP
```

```
crypto map VPNPEER interface outside
```

- d. Verify the transform set:

```
PixP(config)# show running-config crypto ipsec
```

```
crypto ipsec transform-set RAVPN esp-3des esp-sha-hmac
```

- e. Verify the IKE policy:

```
PixP(config)# show running-config isakmp
```

```
isakmp identity address
```

```
isakmp enable outside
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption 3des
isakmp policy 10 hash sha
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400
```

- f. Verify the tunnel-group configuration:

```
PixP(config)# show running-config tunnel-group
tunnel-group training type IPSec_RA
tunnel-group training general-attributes
address-pool MYPOOL
tunnel-group training ipsec-attributes
pre-shared-key *
```

Step 4 Configure the Cisco VPN Client

If needed, complete the following steps to configure the Cisco VPN Client.

- Choose **Start>Programs>Cisco Systems VPN Client>VPN Client**. The Cisco Systems VPN Client window opens.
- Click **New**. The New Connection Entry window opens.
- Enter **PixP** as the name in the Connection Entry field. Enter the IP address of the PIX Security Appliance public interface, **192.168.P.2**, as the IP address of the Host.
- In the **Authentication** tab, verify that the Group Authentication radio button is selected and enter the following group information.

Enter a group name: **training**

Enter and Confirm a group password: **training**

- In the **Transport** tab, verify that Enable Transparent Tunneling is checked.
- Click the **Save** button to save the connection entry.

Step 5 Launch the VPN Client on the Student PC

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

- Choose **Start>Programs>Cisco Systems VPN Client>VPN Client**.
- Verify that the Connection Entry is **PixP**.
- Verify that the IP address of the remote server is set to the public interface IP address of the PIX Security Appliance, **192.168.P.2**.
- Click **Connect**. Several messages flash by quickly. Complete the following sub-steps to establish the VPN tunnel:
 - When prompted for a username, enter **admin**.
 - When prompted to enter a password, enter **admin123**.

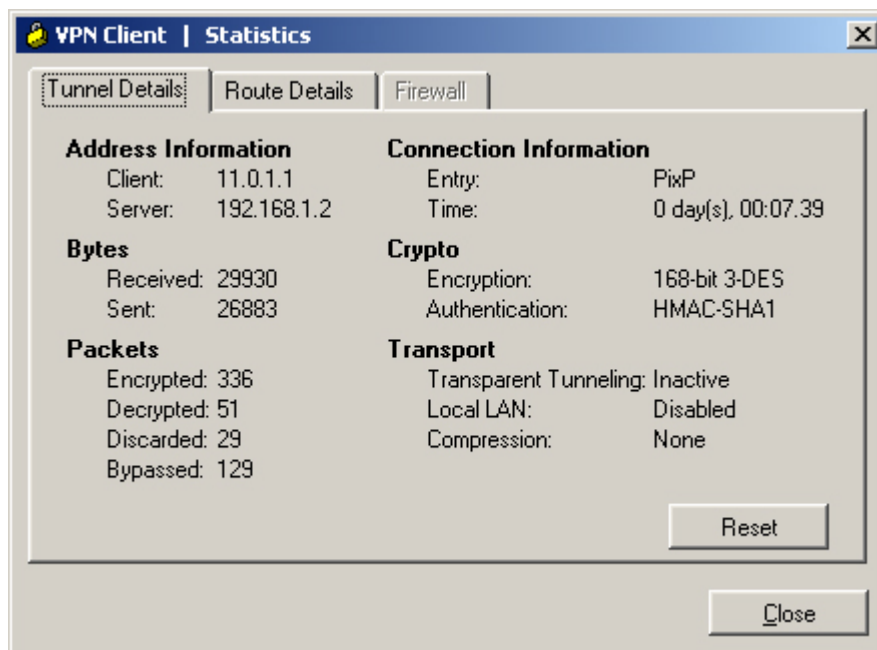


- e. The window closes and a VPN (lock) icon appears in the system tray. This indicates the VPN tunnel has been successfully created.

Step 6 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 home page of the inside server should display.
- d. 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.



- e. On the PIX Security Appliance console, view the IKE SAs.

```
PixP(config)# show crypto isakmp sa
Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1  IKE Peer: 172.26.26.P
```

```
Type      : user          Role      : responder
Rekey     : no            State     : AM_ACTIVE
```

f. View the IPSec SAs.

```
PixP(config)# show crypto ipsec sa
interface: outside
Crypto map tag: DYNOMAP, local addr: 192.168.P.2

local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port):
(11.0.P.1/255.255.255.255/0/0)
current_peer: 172.26.26.1
dynamic allocated peer ip: 11.0.P.1

#pkts encaps: 51, #pkts encrypt: 51, #pkts digest: 51
#pkts decaps: 416, #pkts decrypt: 416, #pkts verify: 416
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 51, #pkts comp failed: 0, #pkts decomp
failed: 0
#send errors: 0, #recv errors: 0

local crypto endpt.: 192.168.P.2, remote crypto endpt.:
172.26.26.P

path mtu 1500, ipsec overhead 60, media mtu 1500
current outbound spi: CDDEC9BF

inbound esp sas:
spi: 0xABAA2D4D3 (2879575251)
transform: esp-3des esp-sha-hmac
in use settings ={RA, Tunnel, }
slot: 0, conn_id: 2, crypto-map: DYNOMAP
sa timing: remaining key lifetime (sec): 28109
IV size: 8 bytes
replay detection support: Y
outbound esp sas:
spi: 0xCDDEC9BF (3453929919)
transform: esp-3des esp-sha-hmac
in use settings ={RA, Tunnel, }
slot: 0, conn_id: 2, crypto-map: DYNOMAP
```



```
sa timing: remaining key lifetime (sec): 28107
IV size: 8 bytes
replay detection support: Y
```

- g. Verify the running configuration with the ending configuration.
- h. On the Student PC, **Disconnect** the remote VPN session.

Step 7 Modify the Transform Sets (OPTIONAL)

If time permits, increase the level of security by using a stronger encryption and authentication transform set and IKE proposal. Re-connect with the VPN Client to verify operation.

Step 8 Configure a TACACS+ Server for Authentication (OPTIONAL)

If time permits, change the authentication from LOCAL to TACACS+. Configure the AAA server location and secretkey on the PIX. Use Cisco Secure ACS as the authentication server. Re-connect with the VPN Client to verify operation