



Lab 4.5.5a Configure a PIX Security Appliance Site-to-Site IPSec VPN Tunnel Using CLI

Objective

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

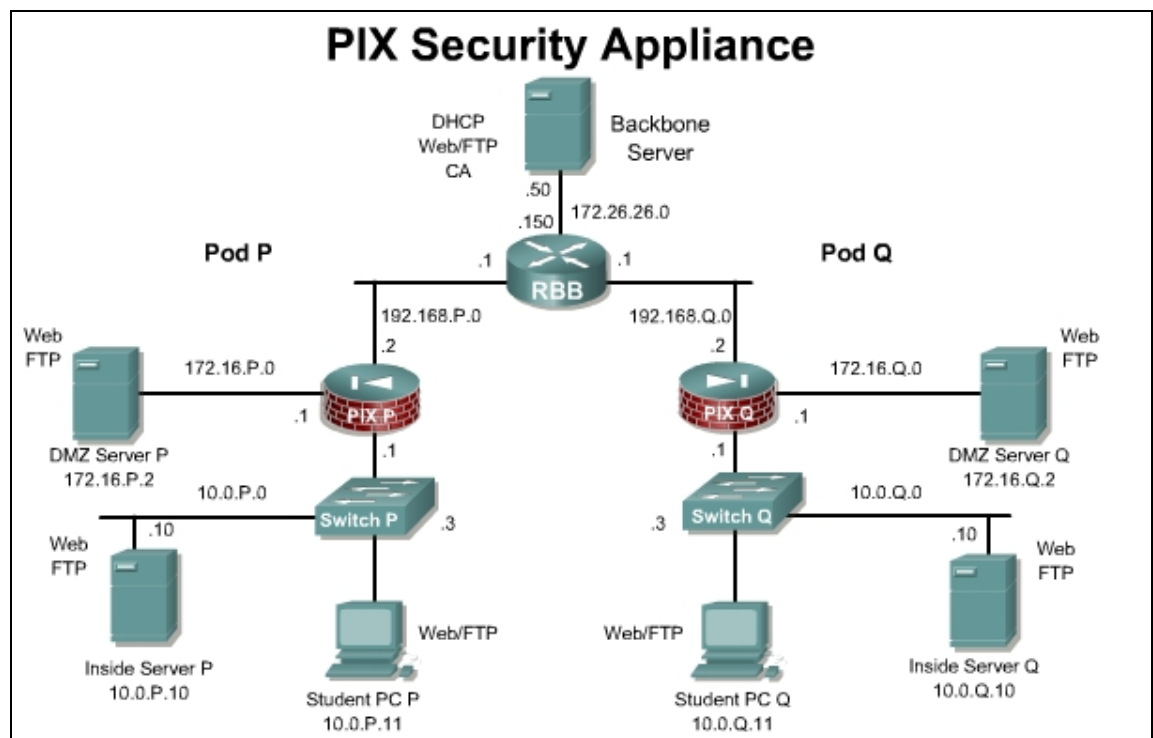
- Prepare to configure VPN support.
- Configure IKE and IPSec parameters.
- Test and verify IPSec configuration.

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 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.

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/en/US/products/hw/vpndevc/ps2030/prod_configuration_examples_list.html

http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_configuration_guide_chapter09186a00804231dc.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
<code>clear configure access-list [id]</code>	To clear an access list from the running configuration, use the <code>clear configure access list</code> command in global configuration mode.
<code>clear configure crypto map</code>	Removes the crypto map configuration.
<code>clear configure ipsec</code>	Removes the ipsec configuration.
<code>clear configure isakmp</code>	Removes the isakmp configuration.
<code>clear configure sysopt</code>	Removes all <code>sysopt</code> commands from the configuration.
<code>clear configure tunnel-group</code>	Removes all tunnel groups from the configuration.
<code>crypto ipsec map-name seq-num transform-set transform-set-name transform1 [transform2]</code>	To define a transform set, use the <code>crypto ipsec transform-set</code> command in global configuration mode. This command is used to identify the IPSec encryption and hash algorithms to be used by the transform set.
<code>crypto map map-name seq-num match address acl_name</code>	To assign an access list to a crypto map entry, use the <code>crypto map match address</code> command in global configuration mode.
<code>crypto map map-name seq-num set peer {ip_address hostname}{...ip_address hostname10}</code>	To specify an IPSec peer in a crypto map entry, use the <code>crypto map set peer</code> command in global configuration mode.

Command	Description
crypto map <i>map-name seq-num set transform-set transform-set-name1 [... transform-set-name9]</i>	To specify the transform sets to use with the crypto map entry, use the crypto map set transform-set command in global configuration mode.
crypto map <i>map-name interface 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.
isakmp identity { address hostname key-id <i>key-id-string</i> auto }	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 authentication</i> { pre-share dsa-sig rsa-sig }	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.
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.
show running-config isakmp	To display the complete ISAKMP configuration, use the show running-config isakmp command in global configuration or privileged EXEC mode.
show running-config static	To display all static commands in the configuration, use the show running-config static command in privileged EXEC mode.
sysopt connection permit-ipsec	To let IPsec packets bypass interface access lists, use the sysopt connection permit-ipsec command in global configuration mode. Group policy and per-user authorization access lists still apply to the traffic.
tunnel-group <i>name type type</i>	To create and manage the database of connection-specific records for IPsec, use the tunnel-group command in global configuration mode.
tunnel-group <i>name ipsec-attributes</i>	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 Prepare for the IKE and IPSec Configuration

Reload the PIX Security Appliance and begin with the starting configuration. Complete the following steps to prepare for the IKE and IPSec configuration. For this task, use default values except when directed to enter a specific value. Use pre-shared keys for the IKE policy and ESP mode with DES encryption for the IPSec policy.

- a. Verify that a static translation is configured from a global IP address on the outside interface to the internal host:

```
PixP(config)# show static
static (dmz,outside) 192.168.P.11 bastionhost netmask 255.255.255.255
static (inside,outside) 192.168.P.10 insidehost netmask 255.255.255.255
(where P = pod number)
```

- b. Verify that an ACL permitting Web access to the inside host has been configured:

```
PixP(config)# show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
      alert-interval 300
access-list ACLDMZ; 1 elements
access-list ACLDMZ line 1 extended permit icmp any any (hitcnt=0)
access-list OUTSIDE_ACCESS_IN; 4 elements
access-list OUTSIDE_ACCESS_IN line 1 extended permit tcp any host
192.168.P.11 eq www (hitcnt=0)
access-list OUTSIDE_ACCESS_IN line 2 extended permit tcp any host
192.168.P.11 eq ftp (hitcnt=0)
access-list OUTSIDE_ACCESS_IN line 3 extended permit icmp any any
(hitcnt=0)
access-list OUTSIDE_ACCESS_IN line 4 extended permit tcp any host
192.168.P.10 eq www (hitcnt=0) (hitcnt=0)
(where P = pod number)
```

- c. Ensure that a web connection can be established between the peer inside hosts from the student PCs using the static and ACL. Also, ping the DMZ server at 192.168.Q.11 from the student PCs.
- d. Enable the PIX Security Appliance to implicitly permit any packet from an IPSec tunnel, and bypass checking with an associated **access-group** command for IPSec connections:

```
PixP(config)# sysopt connection permit-ipsec
```

Step 2 Configure and Verify IKE on the PIX Security Appliance

Complete the following steps to configure IKE on the PIX Security Appliance:

- a. Ensure IKE is enabled on the outside interface:

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

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

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

- c. Set the IKE identity:

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

- d. Configure the tunnel group type:

```
PixP(config)# tunnel-group 192.168.Q.2 type IPSec_L2L  
(where Q = peer pod number)
```

- e. Enter the tunnel-group ipsec-attributes submode:

```
PixP(config)# tunnel-group 192.168.Q.2 ipsec-attributes
```

- f. Enter the per-shared key:

```
PixP(config-ipsec)# pre-shared-key cisco123  
PixP(config-ipsec)# exit
```

- g. Verify the IKE policy. Note the default values.

```
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  
isakmp policy 65535 authentication pre-share  
isakmp policy 65535 encryption 3des  
isakmp policy 65535 hash sha  
isakmp policy 65535 group 2  
isakmp policy 65535 lifetime 86400
```

Step 3 Configure and Verify IPSec Configuration

Complete the following steps to configure IPSec (IKE phase two) parameters:

- a. Create an ACL to select traffic to protect. The ACL should protect IP traffic between the student PCs:

```
PixP(config)# access-list CRYPTO_ACL permit ip host 192.168.P.10  
host 192.168.Q.10
```

(where P = pod number, and Q = peer pod number)

- b. Verify the Crypto ACL:

```
PixP(config)# show access-list  
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)  
alert-interval 300  
access-list ACLDMZ; 1 elements  
access-list ACLDMZ line 1 extended permit icmp any any (hitcnt=0)  
access-list OUTSIDE_ACCESS_IN; 4 elements  
access-list OUTSIDE_ACCESS_IN line 1 extended permit tcp any host  
192.168.P.11 eq www (hitcnt=0)  
access-list OUTSIDE_ACCESS_IN line 2 extended permit tcp any host  
192.168.P.11 eq ftp (hitcnt=0)
```

```

access-list OUTSIDE_ACCESS_IN line 3 extended permit icmp any any
(hitcnt=54)

access-list OUTSIDE_ACCESS_IN line 4 extended permit tcp any host
192.168.P.10 eq www (hitcnt=0)

access-list CRYPTO_ACL; 1 elements

access-list CRYPTO_ACL line 1 extended permit ip host 192.168.P.10 host
192.168.Q.10 (hitcnt=0)

```

(where P = pod number, and Q = peer pod number)

- b. Configure an IPSec transform set to use ESP and DES. The transform set is made up of the IKE phase two parameters. Use a **transform-set-name** of **ESP-DES-MD5**.

```

PixP(config)# crypto ipsec transform-set ESP-DES-MD5 esp-des esp-
md5-hmac

```

(where Q = peer pod number)

1. What are some other IPSec security protocol combinations that can be used?
-

- c. Create a crypto map by completing the following sub-steps:

- i. Create a crypto map entry. Use a map-name of peer Q and assign the ACL to the crypto map.

```

PixP(config)# crypto map peerQ 10 match address CRYPTO_ACL

```

(where Q = peer pod number)

- ii. Define the peer. The peer IP address should be set to the outside interface IP address of the peer pod PIX Security Appliance:

```

PixP(config)# crypto map peerQ 10 set peer 192.168.Q.2

```

(where Q = peer pod number)

- iii. Specify the transform set used to reach the peer. Use the transform set name configured in sub-step b.

```

PixP(config)# crypto map peerQ 10 set transform-set ESP-DES-MD5

```

(where Q = peer pod number)

- iv. Apply the crypto map set to the outside interface:

```

PixP(config)# crypto map peerQ interface outside

```

(where Q = peer pod number)

- d. View the available **show running-config crypto** commands

```

PixP(config)# show running-config crypto ?

```

exec mode commands/options:

```

  accelerator  Show accelerator operational data
  ca           Show certification authority policy
  ipsec        Show IPsec operational data
  isakmp       Show ISAKMP operational data
  key          Show long term public keys
  protocol     Show protocol statistics

```

- e. Verify that the crypto map configuration is correct:

```
PixP(config)# show running-config crypto map  
crypto map peer2 10 match address CRYPTO_ACL  
crypto map peer2 10 set peer 192.168.Q.2  
crypto map peer2 10 set transform-set ESP-DES-MD5  
crypto map peer2 interface outside  
Crypto Map: "peer2" interfaces: { outside }  
(where Q = peer pod number)
```

Step 4 Test the VPN Connection

Complete the following steps to test the VPN connection:

- a. Turn on debugging for IPsec and ISAKMP:

```
PixP(config)# debug crypto ipsec  
PixP(config)# debug crypto isakmp
```

- b. Clear the IPsec SA by using the following command:

```
PixP(config)# clear crypto ipsec sa
```

- c. Enable logging to the console:

```
PixP(config)# logging enable  
PixP(config)# logging console debug
```

- d. From the Student PC, ping the peer pod Student PC

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

- e. Initiate a web session from the student PC to the peer pod's student PC. Observe the debug output and verify that the web session was established. The debug output should state the following status indicating that IPsec was successful:

```
return status is IKMP_NO_ERROR
```

- f. Examine the ISAKMP SA. Note the IKE peer and tunnel type as well as the state:

```
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: 192.168.2.2  
   Type      : L2L                      Role      : initiator  
   Rekey     : no                       State     : MM_ACTIVE
```

- g. Disable logging to the console:

```
PixP(config)# no logging console debug
```

- h. Examine the IPsec SAs. Note the number of packets encrypted and decrypted.

```
PixP(config)# show crypto ipsec sa  
  
interface: outside  
  
Crypto map tag: peer2, local addr: 192.168.P.2
```

```

    local ident (addr/mask/prot/port):
(192.168.P.10/255.255.255.255/0/0)
    remote ident (addr/mask/prot/port):
(192.168.Q.10/255.255.255.255/0/0)
    current_peer: 192.168.Q.2

    #pkts encaps: 20, #pkts encrypt: 20, #pkts digest: 20
    #pkts decaps: 16, #pkts decrypt: 16, #pkts verify: 16
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 20, #pkts comp failed: 0, #pkts decomp
failed: 0
    #send errors: 0, #recv errors: 0

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

    path mtu 1500, ipsec overhead 60, media mtu 1500
    current outbound spi: 413A007D

inbound esp sas:
    spi: 0x44B13645 (1152464453)
        transform: esp-des esp-md5-hmac
        in use settings ={L2L, Tunnel, }
        slot: 0, conn_id: 1, crypto-map: peer2
        sa timing: remaining key lifetime (kB/sec): (3824998/28308)
        IV size: 8 bytes
        replay detection support: Y
outbound esp sas:
    spi: 0x413A007D (1094320253)
        transform: esp-des esp-md5-hmac
        in use settings ={L2L, Tunnel, }
        slot: 0, conn_id: 1, crypto-map: peer2
        sa timing: remaining key lifetime (kB/sec): (3824997/28301)
        IV size: 8 bytes
        replay detection support: Y

```

(where P = pod number, and Q = peer pod number)

- i. Generate additional traffic by clicking the **Reload** button of the web browser.
- j. Examine the IPSec SAs again. Note that the packet counters have increased incrementally.
- k. If desired, compare the running configuration of the PIX Security Appliance against the ending configuration before proceeding with the rest of the lab.

Step 5 Clear IPsec and IKE

Complete the following steps to remove the IPsec and IKE configurations.

- a. Clear the IPsec SAs:

```
PixP(config)# clear crypto ipsec sa
```

- b. Remove all **isakmp** command statements:

```
PixP(config)# clear configure isakmp
```

- c. Remove the previously configured transform set:

```
PixP(config)# clear configure ipsec
```

- d. Remove all **tunnel-group** command statements:

```
PixP(config)# clear configure tunnel-group
```

- e. Remove all parameters entered through the **crypto map** command:

```
PixP(config)# clear configure crypto map
```

- f. Remove the **sysopt** command statements:

```
PixP(config)# clear configure sysopt
```

- g. Remove the **CRYPTO_ACL** ACL:

```
PixP(config)# clear configure CRYPTO_ACL
```

- h. Save the configuration:

```
PixP(config)# write memory
```