Lab 4.4.7 Configure Cisco IOS IPSec using Pre-Shared Keys

Objective

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

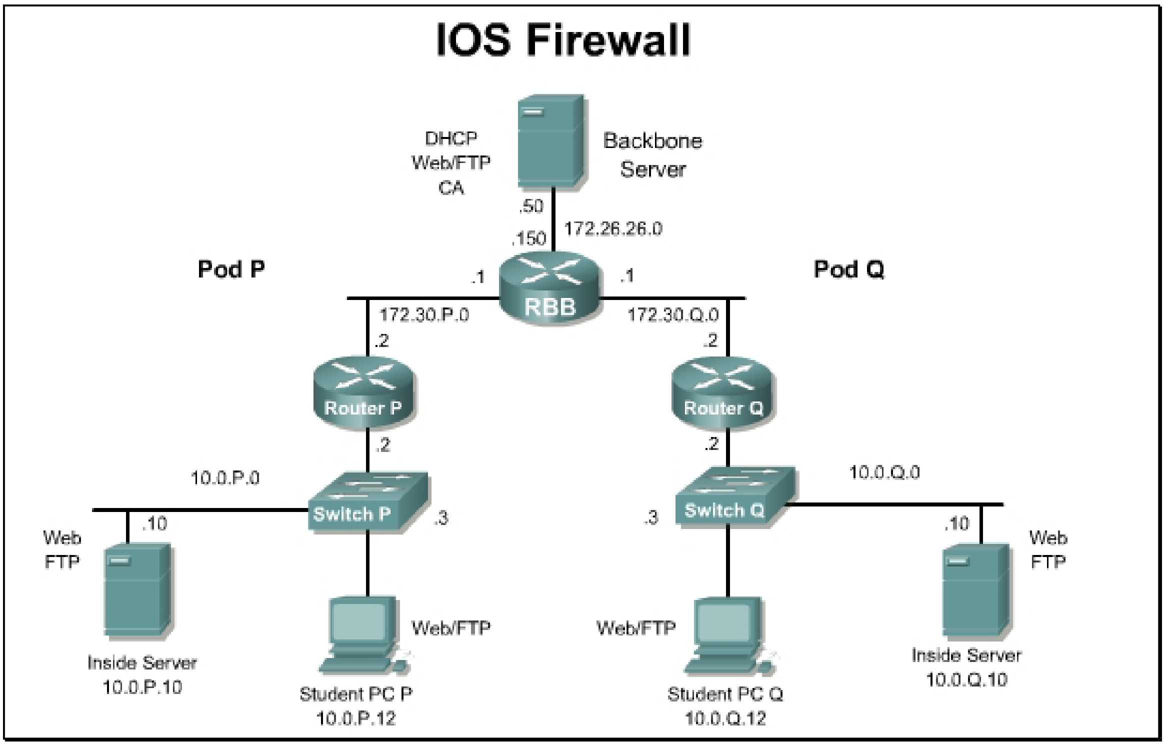
- Prepare to configure Virtual Private Network (VPN) Support
- Configure Internet Key Exchange (IKE) phase one
- Configure IKE parameters and verify IKE and IP Security (IPSec) configuration
- Configure IPSec parameters
- Verify and test IPSec configuration

Scenario

The XYZ Company has Cisco routers at two branch locations. The company wants to create a secure VPN over the Internet between the two sites. The company wants to configure a secure VPN gateway using IPSec between the two Cisco routers to use pre-shared keys for authentication. The security policy has been updated accordingly.

Topology

This figure illustrates the lab network environment.



Preparation

Begin with the standard lab topology and verify the starting configuration on the pod routers. Test the connectivity between the pod routers. Access the perimeter router console port using the terminal

Copyright © 2005, Cisco Systems, Inc.

emulator on the Windows 2000 server. If desired, save the router configuration to a text file for later analysis. Refer back to the *Student Lab Orientation* if more help is needed.

Tools and resources or equipment

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

- Standard IOS Firewall lab topology
- Console cable
- HyperTerminal

Additional materials

Further information about the objectives covered in this lab can be found at the following website:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ddebe.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
authentication {rsa-sig |rsa-encr | pre-share}	Specify the authentication method within an IKE policy.
crypto ipsec transform-set *transform-set-name transform1* **[** *transform2***[** *transform3***]]**	Define a transform set, which is an acceptable combination of security protocols and algorithms, and enters crypto transform configuration mode.
crypto isakmp enable	Enables IKE/ISAKMP on the router.
crypto isakmp key *key* **address** *peer -address*	Sets up the pre-shared key and peer address.
crypto isakmp policy *priority*	Define an IKE policy, and enters ISAKMP policy configuration mode.
crypto map *map-name*	Apply a previously defined crypto map set to an interface.
crypto map *map-name seq-num* **[ipsec-isakmp]**	Create or modifies a dynamic crypto map entry, and enters the crypto map configuration mode.
hash {sha | md5}	Specify the hash algorithm within an IKE policy.
match address [*access-list-id* **|** *name***]**	Specify an extended access list for a crypto map entry.
mode [tunnel | transport]	Specify the mode for the transform set.

Copyright © 2005, Cisco Systems, Inc.

Step 1 Prepare to Configure VPN Support

Perform the following steps to prepare for the IPSec configuration:

a. Determine the IKE and IPSec policy. In this exercise, use the default values except when directed to enter a specific value. The following are the overall policies used in the lab exercise:

- IKE policy is to use pre-shared keys.
- IPSec policy is to use Encapsulating Security Payload (ESP) mode with Data Encryption Standard (DES) encryption.
- IPSec policy is to encrypt all traffic between perimeter routers.

b. Verify that connectivity has been established to the peer router. Answer the following question:

```
RouterP>enable
password:cisco
RouterP#ping 172.30.Q.2
```

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

1. In a production environment, what other steps would need to be completed at this point?

____

Answer: Share the key.

Step 2 Configure IKE Parameters

Work with the members of the pod group to complete this lab. Perform the following steps to configure IKE on the Cisco router:

Be aware when the command line prompt changes while entering commands. This helps distinguish what configuration mode is active.

a. Ensure configuration mode is enabled.

```
RouterP#configure terminal
```

b. Enable IKE/ISAKMP on the router.

```
RouterP(config)#crypto isakmp enable
```

c. Create an IKE policy to use pre-shared keys by completing the following substeps:

i. Set the policy priority and enter config-isakmp mode.

```
RouterP(config)#crypto isakmp policy 110
```

ii. Set authentication to use pre-shared keys.

```
RouterP(config-isakmp)#authentication pre-share
```

iii. Set IKE encryption.

```
RouterP(config-isakmp)#encryption des
```

iv. Set the Diffie-Hellman group.

```
RouterP(config-isakmp)#group 1
```

v. Set the hash algorithm.

```
RouterP(config-isakmp)#hash md5
```

vi. Set the IKE security association (SA) lifetime.

```
RouterP(config-isakmp)#lifetime 86400
```

vii. Exit the config-isakmp mode.

```
RouterP(config-isakmp)#exit
```

Copyright © 2005, Cisco Systems, Inc.

viii. Set up the pre-shared key and peer address.

```
RouterP(config)#crypto isakmp key cisco1234 address 172.30.Q.2
```

ix. Exit config mode.

```
RouterP(config)#exit
```

x. Examine the crypto policy suite.

```
RouterP#show crypto isakmp policy
Protection suite of priority 110
        encryption algorithm:   DES - Data Encryption Standard (56 bit
        keys).
        hash algorithm:         Message Digest 5
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #1 (768 bit)
        lifetime:               86400 seconds, no volume limit
         Default protection suite
       encryption algorithm:   DES - Data Encryption Standard (56 bit
       keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #1 (768 bit)
        lifetime:               86400 seconds, no volume limit
```

Step 3 Configure IPSec Parameters

Perform the following steps to configure IPSec on the Cisco router.

a. Configure transform sets and security association Parameters

b. Ensure that configuration mode is enabled.

```
RouterP#configure terminal
```

c. View the available crypto IPSec command options. Answer the following question:

```
RouterP(config)#crypto ipsec ?
```

1. What options can be set at this level?

____

Answer: client, df-bit, fragmentation, nat-transparency, optional, profile, security-association, and transform-set

d. Check the transform set options. Answer the following question:

```
RouterP(config)#crypto ipsec transform-set ?
```

1. Is it possible to configure a transform set without naming it first?

____

Answer: No

e. Define a transform set. Use the following parameters:

- Transform name: **MINE**
- ESP protocols: **des**
- Mode: **tunnel**

```
RouterP(config)#crypto ipsec transform-set MINE esp-des
```

1. Has the command prompt changed? What can now be set? Hint: type **?** to see the options.

   ____

   ____

   Answer: Yes. Transport or tunnel mode can be set at this prompt.

f. Set the mode to tunnel.

```
RouterP(cfg-crypto-trans)#mode tunnel
```

g. Exit the configuration mode.

```
RouterP(cfg-crypto-trans)#^Z
```

h. Check the configuration.

```
RouterP#show crypto ipsec transform-set MINE
Transform set MINE: { esp-des  }
      will negotiate = { Tunnel,  },
```

i. Configure crypto access lists

Perform the following steps to configure the crypto access lists. Create an access control list (ACL) to select traffic to protect. The ACL should encrypt traffic between perimeter routers. Use the following parameters:

- Traffic permitted: **all**
- Peer address: **peer router external interface**
- ACL number: **102**
- Protocol: **any Internet protocol**

j. Ensure configuration mode is enabled.

```
RouterP(config)#config terminal
```

k. Configure the ACL.

```
RouterP(config)#access-list 102 permit ip host 172.30.P.2 host
172.30.Q.2
```

(where P = pod number, Q = peer's pod number)

l. Configure crypto maps

Perform the following steps to configure a crypto map. Use the following parameters:

- Name of map: **MYMAP**
- Number of map: **10**
- Key exchange type: **isakmp**
- Peer: **172.30.Q.2**
- Transform set: **MINE**
- Match address: **102**

m. Set the name of the map, the map number, and the type of key exchange to be used.

```
RouterP(config)#crypto map MYMAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
     and a valid access list have been configured.
```

n. Specify the extended ACL to use with this map.

```
RouterP(config-crypto-map)#match address 102
```

o. Specify the transform set defined earlier.

```
RouterP(config-crypto-map)#set transform-set MINE
```

p. Assign the VPN peer using the host name or IP address of the peer. Answer the following question:

```
RouterP(config-crypto-map)#set peer 172.30.Q.2
```

1. What other parameters can be set at this level? Hint: type **set ?**

____

Answer:

```
RouterP(config-crypto-map)#set ?
  identity                Identity restriction.
  ip                      Interface Internet Protocol config commands
  isakmp-profile          Specify isakmp Profile
  peer                    Allowed Encryption/Decryption peer.
  pfs                     Specify pfs settings
  security-association    Security association parameters
  transform-set           Specify list of transform sets in priority
                          order
```

q. Exit the crypto map configuration mode.

```
RouterP(config-crypto-map)#exit
```

r. Apply the crypto map to an interface

Perform the following steps to assign the crypto map to the appropriate router interface. Use the following parameters:

- Interface to configure: **FastEthernet 0/1 (outside interface)**
- Crypto map to use: **MYMAP**

s. Access the interface configuration mode.

```
RouterP(config)#interface FastEthernet 0/1
```

t. Assign the crypto map to the interface.

```
RouterP(config-if)#crypto map MYMAP
```

u. Exit configuration crypto mode.

```
RouterP(config-if)#^Z
```

Step 4 Verify and Test IPSec Configuration

Perform the following steps to verify and test the IPSec configuration. Coordinate the test with the peer router pod group.

a. Display the configured IKE policies.

```
RouterP#show crypto isakmp policy

Protection suite of priority 110

     encryption algorithm:   DES - Data Encryption Standard (56 bit
     keys)

     hash algorithm:         Message Digest 5

     authentication method:  Pre-Shared Key

     Diffie-Hellman group:   #1 (768 bit)

     lifetime:               86400 seconds, no volume limit

     Default protection suite

     encryption algorithm:   DES - Data Encryption Standard (56 bit
     keys)

     hash algorithm:         Secure Hash Standard

     authentication method:  Rivest-Shamir-Adleman Signature

     Diffie-Hellman group:   #1 (768 bit)

     lifetime:               86400 seconds, no volume limit
```

b. Display the configured transform sets.

```
RouterP#show crypto ipsec transform-set

Transform set MINE: { esp-des  }

   will negotiate = { Tunnel,  },
```

c. Display the configured crypto maps.

```
RouterP#show crypto map

Crypto Map "MYMAP" 10 ipsec-isakmp

        Peer = 172.30.Q.2

        Extended IP access list 102

access-list 102 permit ip host 172.30.P.2 host 172.30.Q.2

        Current peer: 172.30.Q.2

Security association lifetime: 4608000 kilobytes/3600 seconds

        PFS (Y/N): N

        Transform sets={ MINE, }
```

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

d. Display the current state of the IPSec SAs. The IPSec SAs may have been previously established by routing traffic. The following example shows initialized IPSec SAs before encryption traffic:

```
RouterP#show crypto ipsec sa

interface: FastEthernet0/1

    Crypto map tag: MYMAP, local addr. 172.30.P.2
    local  ident (addr/mask/prot/port):
(172.30.P.2/255.255.255.255/0/0)

    remote ident (addr/mask/prot/port):
(172.30.Q.2/255.255.255.255/0/0)

    current_peer: 172.30.Q.2

     PERMIT, flags={origin_is_acl,}

    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0

    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0

    #send errors 0, #recv errors 0


local crypto endpt.: 172.30.P.2, remote crypto endpt.: 172.30.Q.2

     path mtu 1500, media mtu 1500

     current outbound spi: 0


     inbound esp sas:

     inbound ah sas:


     outbound esp sas:

     outbound ah sas:
```

e. Clear any existing SAs.

```
RouterP#clear crypto sa
```

f. Enable debug output for IPSec events.

```
RouterP#debug crypto ipsec
```

g. Enable debug output for ISAKMP events.

```
RouterP#debug crypto isakmp
```

h. Turn on console logging to see the debug output.

```
RouterP(config)#logging console
```

i. Initiate a ping to the peer pod perimeter router. Observe the IKE and IPSec debug output.

```
RouterP#ping 172.30.Q.2
```

j. Verify the IKE and IPSec SAs. Note the number of packets encrypted and decrypted when viewing the IPSec SAs.

```
RouterP#show crypto isakmp sa

dst             src             state         conn-id   slot

172.30.P.2      172.30.Q.2      QM_IDLE            16      0

RouterP#show crypto ipsec sa

interface: FastEthernet0/1

    Crypto map tag: MYMAP, local addr. 172.30.P.2

   local  ident (addr/mask/prot/port):
(172.30.P.2/255.255.255.255/0/0)

   remote ident (addr/mask/prot/port):
(172.30.Q.2/255.255.255.255/0/0)
```

```
   current_peer: 172.30.Q.2
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 6, #pkts encrypt: 6, #pkts digest 0
    #pkts decaps: 6, #pkts decrypt: 6, #pkts verify 0
    #send errors 4, #recv errors 0

     local crypto endpt.: 172.30.P.2, remote crypto endpt.:
172.30.Q.2
     path mtu 1500, media mtu 1500
     current outbound spi: DB5049D

     inbound esp sas:
      spi: 0x26530A0D(642976269)
        transform: esp-des ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2, crypto map: MYMAP
        sa timing: remaining key lifetime (k/sec): (4607999/3542)
        IV size: 8 bytes
        replay detection support: N

     inbound ah sas:

     outbound esp sas:
      spi: 0xDB5049D(229967005)
        transform: esp-des ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 3, crypto map: MYMAP
        sa timing: remaining key lifetime (k/sec): (4607999/3542)
        IV size: 8 bytes
        replay detection support: N
     outbound ah sas:
```

k. Ensure that the encryption is working between routers by generating additional traffic. Then observe that the packets encrypted and decrypted counter has incremented.

```
RouterP#ping 172.30.Q.2
RouterP#show crypto ipsec sa
interface: FastEthernet0/1
    Crypto map tag: MYMAP, local addr. 172.30.P.2
   local  ident (addr/mask/prot/port):
(172.30.P.2/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port):
(172.30.Q.2/255.255.255.255/0/0)
```

```
   current_peer: 172.30.Q.2
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 11, #pkts encrypt: 11, #pkts digest 0
    #pkts decaps: 11, #pkts decrypt: 11, #pkts verify 0
    #send errors 4, #recv errors 0

     local crypto endpt.: 172.30.P.2, remote crypto endpt.:
172.30.Q.2
     path mtu 1500, media mtu 1500
     current outbound spi: DB5049D

     inbound esp sas:
      spi: 0x26530A0D(642976269)
        transform: esp-des ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2, crypto map: MYMAP
        sa timing: remaining key lifetime (k/sec): (4607998/3506)
        IV size: 8 bytes
        replay detection support: N

     inbound ah sas:

     outbound esp sas:
      spi: 0xDB5049D(229967005)
        transform: esp-des ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 3, crypto map: MYMAP
        sa timing: remaining key lifetime (k/sec): (4607998/3506)
        IV size: 8 bytes
        replay detection support: N

     outbound ah sas:
```

Step 5 (Optional) Fine Tune the Crypto ACL

Fine tune the crypto ACL that is used to determine interesting traffic so that only the traffic between the internal LANs. Remember to work with the peer pod group to make the ACLs symmetrical between the perimeter routers. Ensure that desired traffic is encrypted between peers.

a. Ensure that configuration mode is enabled.

```
RouterP#config terminal
```

b. Remove the previously configured ACL.

```
RouterP(config)#no access-list 102
```

Copyright © 2005, Cisco Systems, Inc.

c. Configure a new ACL for the servers.

```
RouterP(config)#access-list 102 permit ip 10.0.P.0 0.0.0.255
10.0.Q.0 0.0.0.255
```

d. Verify the configuration by connecting to the peer web server at 10.0.Q.12, where Q = peer pod number, using the browser on the server.