CISCO SYSTEMS

CISCO NETWORKING ACADEMY PROGRAM

Network Security 2 v2.0

Instructor Lab Manual

Lab 2.1.6 Configure a Router with the IOS Intrusion Prevention System

Objective

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

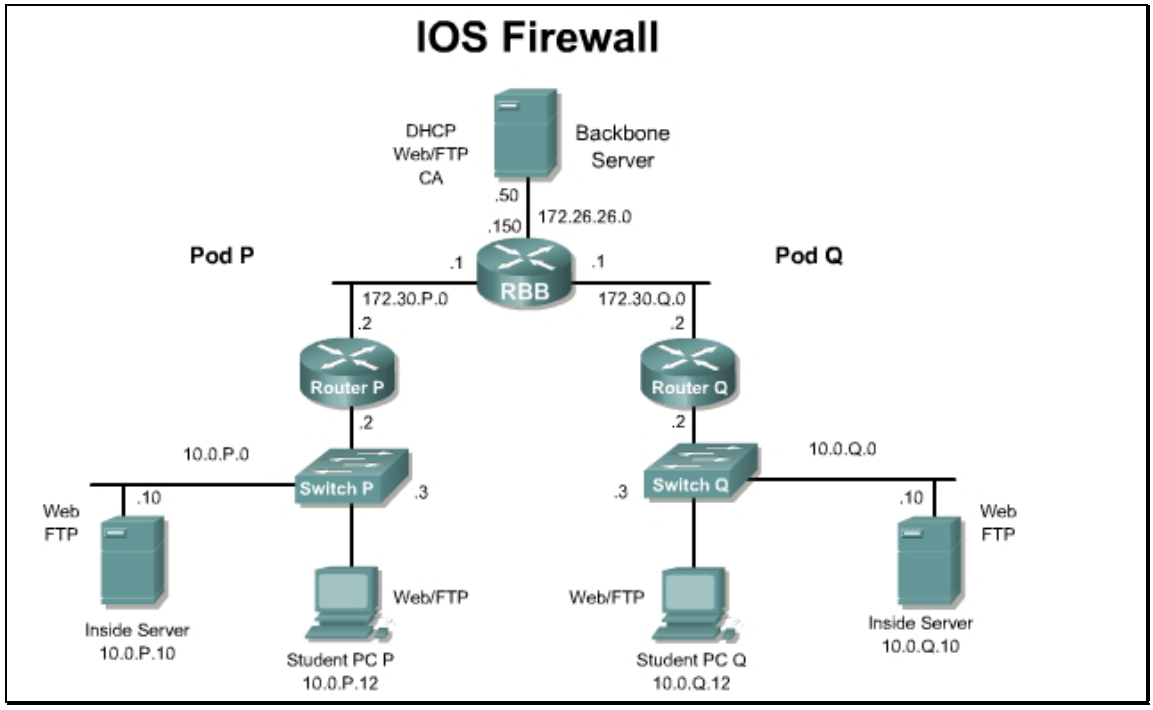
- Initialize the Intrusion Protection System (IPS) on the router.
- Disable signatures.
- Merge signature definition files.
- Verify the IPS configuration.
- Generate a test message.

Scenario

A company wants additional network protection beyond stateful inspection at the perimeter. The security policy has been updated to require basic intrusion prevention at the perimeter of the network. This will allow the perimeter router to take appropriate action on packets and flows that violate the security policy or represent malicious network activity.

Topology

This figure illustrates the lab network environment.



Preparation

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

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

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

- Standard IOS Firewall lab topology
- Console cable
- HyperTerminal
- The signature definition file, attack-drop.sdf

Additional materials

The latest attack-drop.sdf file can be downloaded from the following URL. A valid CCO login is required to access the site.

http://www.cisco.com/cgi-bin/tablebuild.pl/ios-sigup

Command List

In this lab exercise, the following switch commands will be used. Refer to this list if assistance or help is needed during the lab exercise.

Router Commands

Command	Description
ip ips *ips-name* **{in | out} [list** *acl***]**	To apply an IPS rule to an interface, use the **ip ips** command in interface configuration mode.
ip ips fail closed	To instruct the router to drop all packets until the signature engine is built and ready to scan traffic, use the **ip ips fail closed** command in global configuration mode.
ip ips name *ips-name*	To specify an IPS rule, use **the ip ips name** command in global configuration mode.
ip ips signature *signature-id***[:***sub-signature-id***] {delete | disable | list** *acl-list***}**	To attach a policy to a signature, use the **ip ips signature** command in global configuration mode.
ip ips sdf location *url*	To specify the location in which the router will load the signature definition file (SDF), use the **ip ips sdf** location command in global configuration mode.
show ip ips {[all] [configuration] [interfaces] [name *name***] [statistics [reset]] [sessions [details]] [signatures [details]]}**	To display IPS information such as configured sessions and signatures, use the **show ip ips** command in privileged EXEC mode.

Step 1 Initialize the IPS on the Router

Complete the following steps to initialize IPS on the router:

a. From the student PC, access the router console.

b. Switch to privileged-EXEC mode:

```
RouterP> enable
```

(Where P = pod number)

```
Password: cisco
```

c. Switch to global configuration mode:

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

d. Configure the router to use the built in signature definition file (SDF).

```
RouterP(config)# ip ips sdf builtin
```

e. Create an IPS rule named **SECURIPS**.

```
RouterP(config)# ip ips name SECURIPS
```

f. Enter interface configuration mode for Fa 0/1.

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

g. Apply the IPS rule at an interface. This command automatically loads the signatures and builds the signature engines.


```
RouterP(config-if)# ip ips SECURIPS in
```

Note	The router prompt is suspended while the signature engines are being built. The router prompt will be available again after the engines are built.

h. If the NetBIOS name service is running on the student PC, it may trigger an IPS signature in the router. The debug message for the signature will be similar to the following example:

```
*May 19 22:56:40.884: %IPS-4-SIGNATURE: Sig:4050 Subsig:0 Sev:3 UDP
Bomb [10.0.P.12:137 -> 10.0.P.255:137]
```

Disable this signature with the **ip ips signature 4050 disable** command in global configuration mode.

i. Exit to global configuration mode.

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

j. Configure logging to the student PC.

```
RouterP(config)# logging 10.0.P.12
```

k. Configure a trap level to log messages at the level of 4 or lower.

```
RouterP(config)# logging trap warnings
```

l. Turn on logging.

```
RouterP(config)# logging on
```

m. Exit to privileged mode using **Ctrl+Z** or the **end** command.

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

n. Display the IPS configuration.

```
RouterP# show ip ips configuration
Configured SDF Locations: none
Builtin signatures are enabled and loaded
Last successful SDF load time: 22:30:12 UTC May 19 2005
IPS fail closed is disabled
Fastpath ips is enabled
Quick run mode is enabled
Event notification through syslog is enabled
Event notification through SDEE is disabled
Total Active Signatures: 132
Total Inactive Signatures: 0
Signature 4050:0 disable
Signature 1107:0 disable
IPS Rule Configuration
 IPS name SECURIPS
Interface Configuration
 Interface FastEthernet0/1
  Inbound IPS rule is SECURIPS
  Outgoing IPS rule is not set
```


1. How many active signatures are configured?

   _____

   Answer: 132

2. What IPS signatures are disabled?

   _____

   Answer: Signature 1107, RFC 1918 addresses, is disabled. If signature 4050 has been disabled because NetBIOS name service is running on the student PC, it should be included in the answer as well.

Step 2 Load Signatures

Complete the following steps to replace the existing signatures in the router with the latest IPS signature file, attack-drop.sdf.

a. Verify that the attack-drop.sdf file is present in the flash memory of the pod router. If the file is present, proceed to sub-step c.

```
RouterP# show flash
System flash directory:
File  Length   Name/status
  1   16077820  c2600-advsecurityk9-mz.123-14.T1.bin
  2   1038     home.shtml
  3   1654     sdmconfig-26xx.cfg
  4   113152   home.tar
  5   820224   common.tar
  6   3085312  sdm.tar
  7   93095    attack-drop.sdf
[20192748 bytes used, 12837392 available, 33030140 total]
32768K bytes of processor board System flash (Read/Write)
```

b. If necessary, load the SDF file into the flash memory of the router.

```
RouterP# copy tftp://10.0.P.12/attack-drop.sdf flash:attack-drop.sdf
Destination filename [attack-drop.sdf]?<Enter>
Accessing tftp://10.0.P.12/attack-drop.sdf...
Erase flash: before copying? [confirm]n
Loading attack-drop.sdf from 10.0.P.12 (via FastEthernet0/0):
!!!!!!!!!!!!!!!!!!
[OK - 93095 bytes]
```

c. Enter global configuration mode and create an IPS rule

```
RouterP# configure terminal
RouterP(config)# ip ips name SECURIPS
```

d. Specify the location where the router will load the SDF. If this command is not issued, the router will load the default SDF.

```
RouterP(config)# ip ips sdf location flash:attack-drop.sdf
```


e. View the IPS configuration and answer the following questions.

```
RouterP# show ip ips configuration
```

1. What are the configured SDF locations?

_____

Answer: `flash:attack-drop.sdf`

2. What information is provided about the built in signatures?

_____

Answer: `Builtin signatures are enabled and loaded`

f. Configure the router to drop all packets until the signature engine is built and ready to scan traffic with the **ip ips fail closed** comamnd. If this command is issued, one of the following scenarios will occur:

- If IPS fails to load the SDF, all packets will be dropped unless the user specifies an ACL for packets to send to IPS.
- If IPS successfully loads the SDF but fails to build a signature engine, all packets that are destined for that engine will be dropped.

If this command is not issued, all packets will be passed without scanning if the signature engine fails to build.

```
RouterP(config)# ip ips fail closed
```

g. Enter interface configuration mode for Fa 0/1.

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

h. Remove the existing IPS rule at the interface.

```
RouterP(config-if)# no ip ips SECURIPS in
```

i. Apply an IPS rule at an interface. This command automatically loads the signatures and builds the signature engines.

```
RouterP(config-if)# ip ips SECURIPS in
```

Note	Whenever signatures are replaced or merged, the router prompt is suspended while the signature engines for the newly added or merged signatures are being built. The router prompt will be available again after the engines are built.

j. Exit configuration mode.

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

k. View the IPS configuration and answer the following questions.

```
RouterP# show ip ips configuration
Configured SDF Locations:
 flash:attack-drop.sdf
Builtin signatures are enabled but not loaded
Last successful SDF load time: 00:20:07 UTC May 20 2005
IPS fail closed is enabled
Fastpath ips is enabled
Quick run mode is enabled
Event notification through syslog is enabled
```



```
Event notification through SDEE is disabled
Total Active Signatures: 82
Total Inactive Signatures: 0
IPS Rule Configuration
 IPS name SECURIPS
Interface Configuration
 Interface FastEthernet0/1
  Inbound IPS rule is SECURIPS
  Outgoing IPS rule is not set
```

1. What are the configured SDF locations?

   _____

   Answer: `flash:attack-drop.sdf`

2. What information is provided about the built in signatures?

   _____

   Answer: `Builtin signatures are enabled but not loaded`

3. What is the total number of active signatures?

   _____

   Answer: 82

l. Review the IPS signature engine configuration.

```
RouterP# show ip ips signatures
```

Step 3 Merge the attack-drop.sdf File with the Default, Built-in Signatures

It may be necessary to merge the built-in signatures with the attack-drop.sdf file if the built-in signatures are not providing the network with adequate protection from security threats. Complete the following steps to add the SDF and to change default parameters for a specific signature within the SDF or signature engine.

a. Reload the built-in signatures.

```
RouterP(config)# no ip ips sdf location flash:attack-drop.sdf
RouterP(config)# int fastEthernet 0/1
RouterP(config-if)# no ip ips SECURIPS in
RouterP(config-if)# ip ips SECURIPS in
```

b. From privileged EXEC mode, merge the flash-based SDF file, attack-drop.sdf, with the built-in signatures.

```
RouterP(config-if)# end
RouterP# copy flash:attack-drop.sdf ips-sdf
```

This command is used to merge the SDF with the signatures that are already loaded in the router, unless the **/erase** keyword is issued.

c. Save the newly merged signatures in a new file.

```
RouterP# copy ips-sdf flash:my-signatures.sdf
```


d. Configure the router to use new file.

```
RouterP(config)# ip ips sdf location flash:my-signatures.sdf
```

e. Reinitialize the IPS by removing the IPS rule set and reapplying the rule set.

```
RouterP(config)# interface fastEthernet 0/1
RouterP(config-if)# no ip ips SECURIPS in
```

f. Reapply the rule set to interface.

```
RouterP(config-if)# ip ips SECURIPS in
```

g. Leave interface configuration mode:

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

h. Leave global configuration mode:

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

i. View the IPS configuration and answer the following questions.

```
RouterP# show ip ips configuration
Configured SDF Locations:
 flash:my-signatures.sdf
Builtin signatures are enabled but not loaded
Last successful SDF load time: 00:31:50 UTC May 20 2005
IPS fail closed is enabled
Fastpath ips is enabled
Quick run mode is enabled
Event notification through syslog is enabled
Event notification through SDEE is disabled
Total Active Signatures: 183
Total Inactive Signatures: 0
Signature 4050:0 disable
Signature 1107:0 disable
IPS Rule Configuration
 IPS name SECURIPS
Interface Configuration
 Interface FastEthernet0/1
  Inbound IPS rule is SECURIPS
  Outgoing IPS rule is not set
```

1. What are the configured SDF locations?

_____

Answer: `flash:my-signatures.sdf`

2. What information is provided about the built in signatures?

_____

Answer: `Builtin signatures are enabled but not loaded`

3. What is the total number of active signatures?

Answer: 183

Step 4 Verify the Configuration

Complete the following steps to verify the configuration.

a. Display the IPS configuration:

```
RouterP# show ip ips configuration
```

The parameters that were just configured along with several default settings are displayed.

b. Display the IPS interface configuration:

```
RouterP# show ip ips interface
Interface Configuration
 Interface FastEthernet0/1
  Inbound IPS rule is SECURIPS
  Outgoing IPS rule is not set
```

Step 5 Generate a Test Message

Complete the following steps to generate a test message.

a. Start the Syslog server on the Student PC.

b. Send multiple fragmented packets to the perimeter router of the peer pod using the following special technique:

```
RouterP# ping
Protocol [IP] <Enter>
Target IP address: 172.30.Q.2
Repeat count [5]: 20
Datagram size [100]: 2000
Timeout in seconds [2]: <Enter>
Extended commands [n]: <Enter>
Sweep range of sizes [n]: <Enter>
```

(Where Q = peer pod number)

The router will now send multiple fragmented packets to the peer router. This will cause the audit rules to generate events to the Syslog server.

c. Analyze the Syslog messages on the Syslog server. The following messages should also appear on the router console session:

1. What signatures are shown in the Syslog server messages?

Answer: 2151– Large ICMP, 2150 – Fragmented ICMP, and 2004 – ICMP Echo Request

Lab 2.3.3 Configure Intrusion Prevention on the PIX Security Appliance

Objective

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

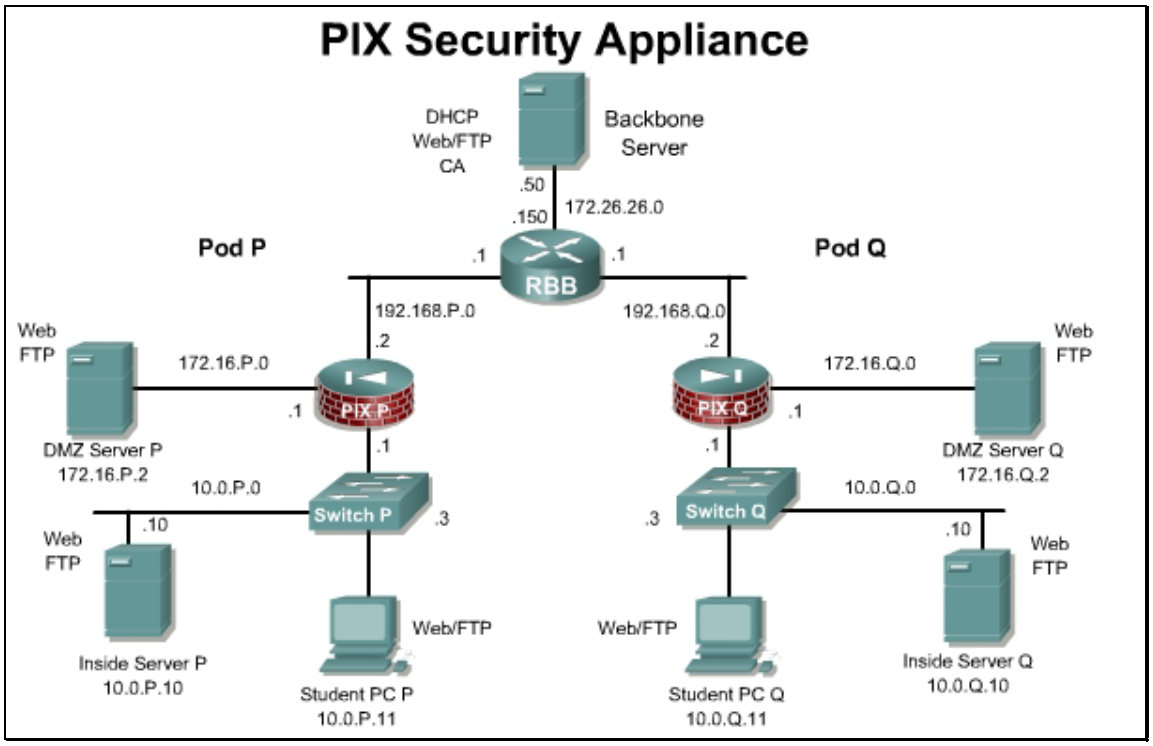
- Configure the use of Cisco Intrusion Prevention System (IPS) information signatures and send Cisco IPS Syslog output to a Syslog server.
- Configure the use of IPS attack signatures and send Cisco IPS Syslog output to a Syslog server.

Scenario

A small company is wants to increase security by adding intrusion prevention on the current PIX Security Appliance. Any output produced by the IPS will be logged to a Syslog server and monitored.

Topology

This figure illustrates the lab network environment.



Preparation

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

Download NMapWin from http://sourceforge.net/projects/nmapwin and install on the Student PC.

Tools and Resources

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

- Standard PIX Security Appliance lab topology
- Console cable
- HyperTerminal
- NMapWin

Additional materials:

Refer to *Cisco PIX Security Appliance System Log Messages* for a list of the supported IPS signature messages. The documentation can be viewed online at the following website:

http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_system_message_guides_list.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
ip audit interface *interface_name policy_name*	To assign an audit policy to an interface, use the **ip audit interface** command in global configuration mode.
ip audit name *name* **{info | attack} [action [alarm] [drop] [reset]]**	To create a named audit policy that identifies the actions to take when a packet matches a predefined attack signature or informational signature, use **the ip audit name** command in global configuration mode.
show ip audit count [global | interface *interface_name***]**	To show the number of signature matches when you apply an audit policy to an interface, use the **show ip audit count** command in privileged EXEC mode.
show running-config ip audit attack	To show the ip audit attack configuration in the running configuration, use the **show running-config ip audit attack** command in privileged EXEC mode.
show running-config ip audit interface	To show the ip audit interface configuration in the running configuration, use the **show running-config ip audit interface** command in privileged EXEC mode.
show running-config ip audit name [*name* **[info | attack]]**	To show the ip audit name configuration in the running configuration, use the **show running-config ip audit name** command in privileged EXEC mode.

Step 1 Configure the Configure the Use of IPS Information Signatures and Send Cisco IPS Syslog Output to a Syslog Server

Reboot the PIX and load the starting configuration.

Complete the following steps to configure the use of Cisco IPS information signatures and to send Cisco IPS Syslog output to a Syslog server:

a. Turn on logging and send messages to the syslog server:

```
PixP(config)# logging enable
PixP(config)# logging host inside insidehost
PixP(config)# logging trap debugging
```

b. Verify connectivity by pinging RBB from the Windows command prompt:

```
C:\>ping 192.168.P.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
```

c. Specify the information signature policy on the PIX Security Appliance:

```
PixP(config)# ip audit name INFOPOLICY info action alarm reset
```

d. Apply the information signature policy to the inside interface:

```
PixP(config)# ip audit interface inside INFOPOLICY
```

e. Disable the chargen signature, which is number 4052

```
PixP(config)# ip audit signature 4052 disable
```

f. Verify the information signature policy on the PIX Security Appliance:

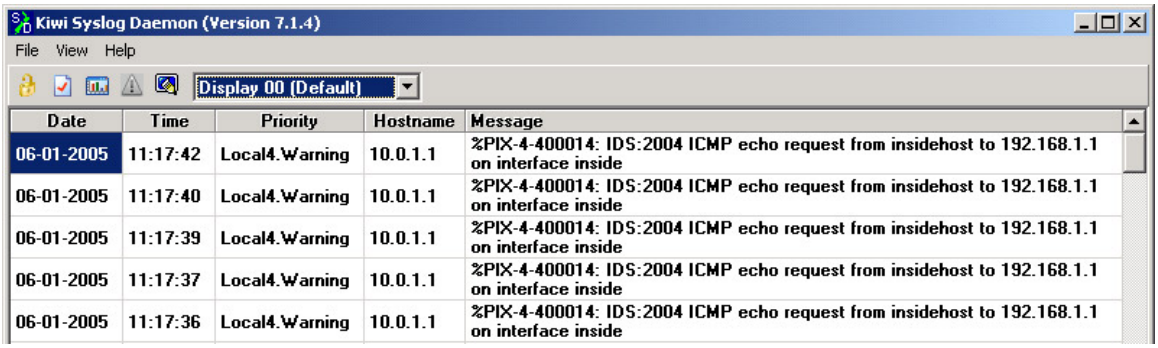
```
PixP(config)# show running-config ip audit interface
ip audit interface inside INFOPOLICY
PixP(config)# show running-config ip audit name
ip audit name INFOPOLICY info action alarm reset
PixP(config)# show running-config ip audit signature
ip audit signature 4052 disable
```

g. Open and the Kiwi Syslog Daemon on the desktop. Clear any existing log entries.

h. Return to the Windows command line and attempt to ping RBB. The ping should fail.

```
C:\>ping 192.168.P.1
```

i. Observe the messages that appear on the Kiwi Syslog Daemon display. The log should be similar to the following:



j. View the IP audit counts

```
PixP# show ip audit count
```

1. Which info signatures were incremented?

_____

Answer: 2004 I ICMP Echo Request.

k. Remove the information signature policy from the inside interface:

```
PixP(config)# no ip audit interface inside INFOPOLICY
```

l. Remove the audit policy audit_name:

```
PixP(config)# no ip audit name INFOPOLICY
```

m. Verify that the information signature policy has been removed from the inside interface, the default informational actions have been restored, and the ip audit name has been removed:

```
PixP(config)# show running-config ip audit interface
PixP(config)# show running-config ip audit name
```

Step 2 Configure the Use of IDS Attack Signatures and Send IDS Syslog Output to a Syslog Server

Complete the following steps to configure the use of IDS attack signatures and send IDS Syslog output to a Syslog server:

a. Ping the bastion host with an Internet Control Message Protocol (ICMP) packet size of 10000 from the command line of the student PC:

```
C:\>ping /l 10000 192.168.P.1
Pinging 192.168.P.1 with 10000 bytes of data:
Reply from 192.168.P.1: bytes=10000 time=23ms TTL=255
Reply from 192.168.P.1: bytes=10000 time=17ms TTL=255
Reply from 192.168.P.1: bytes=10000 time=18ms TTL=255
Reply from 192.168.P.1: bytes=10000 time=18ms TTL=255
```

c. Specify an attack policy:

```
PixP(config)# ip audit name ATTACKPOLICY attack action alarm reset
```

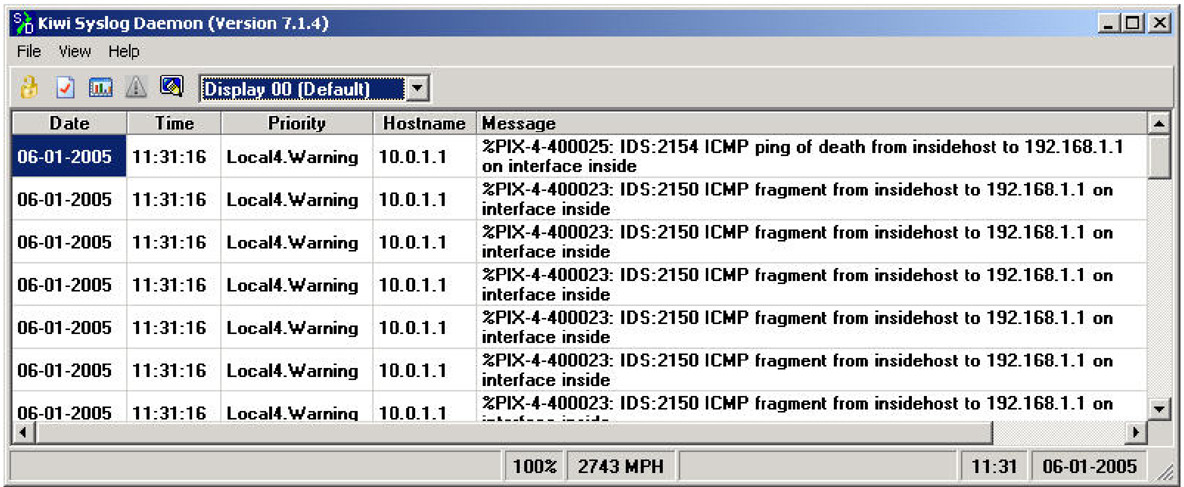
d. Apply the attack policy to the inside interface:

```
PixP(config)# ip audit interface inside ATTACKPOLICY
```

e. Ping the bastion host with an ICMP packet size of 10000 from the Windows 2000 command line:

```
C:\>ping /l 10000 192.168.P.1
Pinging 192.168.P.1 with 10000 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

f. Observe the messages that appear on the Kiwi Syslog Daemon display. The log should be similar to the following:



1. Why is the syslog server showing the ICMP fragment in the log?

   Answer: Ethernet MTU size is 1500 bytes. Ping packets of 10,000 bytes will be fragmented as they are sent to the destination.

n. View the IP audit counts

```
PixP# show ip audit count
```

1. Which info signatures were incremented?

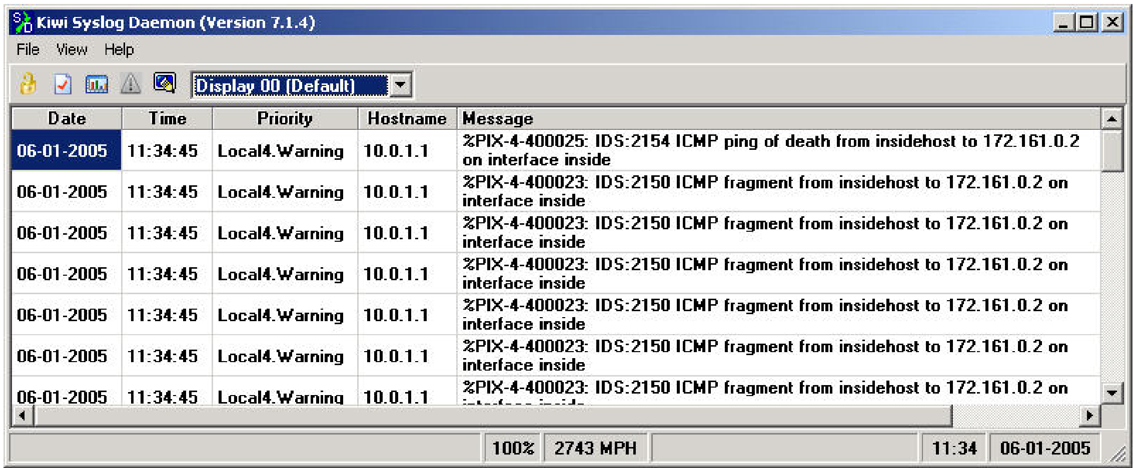
   Answer: 2150 A Fragmented ICMP and 2154 A Ping of Death.

g. Ping the bastion host with an increased ICMP packet size from the command line of the student PC:

```
C:\>ping /l 65000 172.16.P.2

Pinging 172.16.P.2 with 65000 bytes of data:

Request timed out.

Request timed out.

Request timed out.

Request timed out.
```

(where P = pod number)

g. Observe the messages that appear on the Kiwi Syslog Daemon display. The log should be similar to the following:

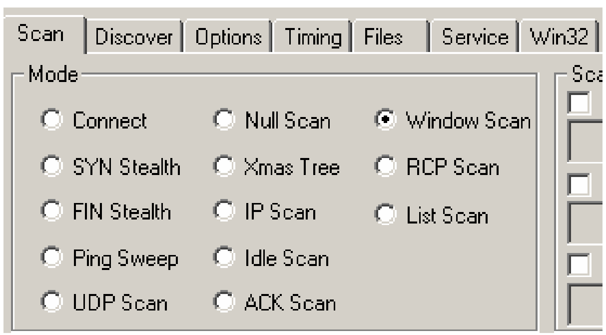


Step 3 Launch an NMapWin scan

Complete the following steps to launch a NMAP scan against RBB:

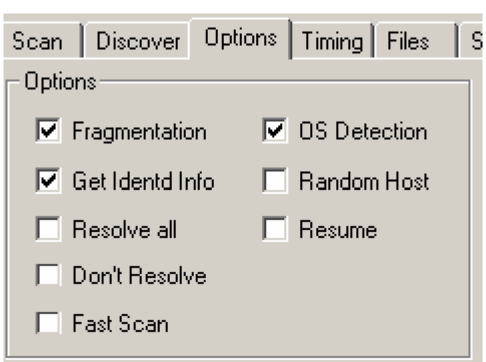
a. Open NMapWin.

b. In the Scan tab, choose Window Scan.



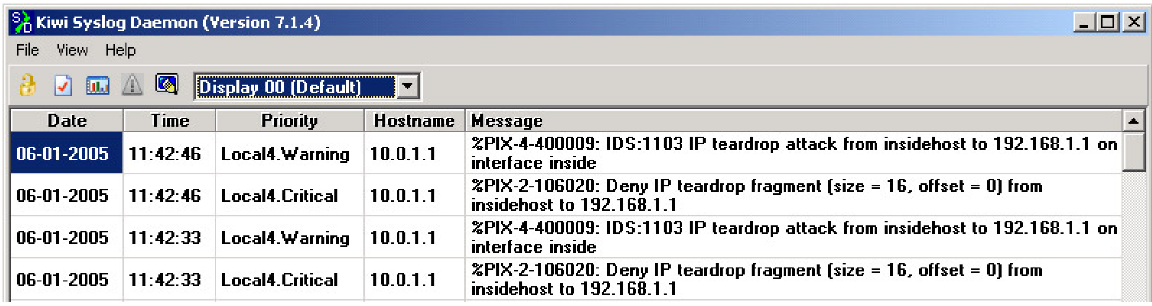
c. In the Discover tab choose TCP+ICMP.

d. In the Options tab, choose the following:

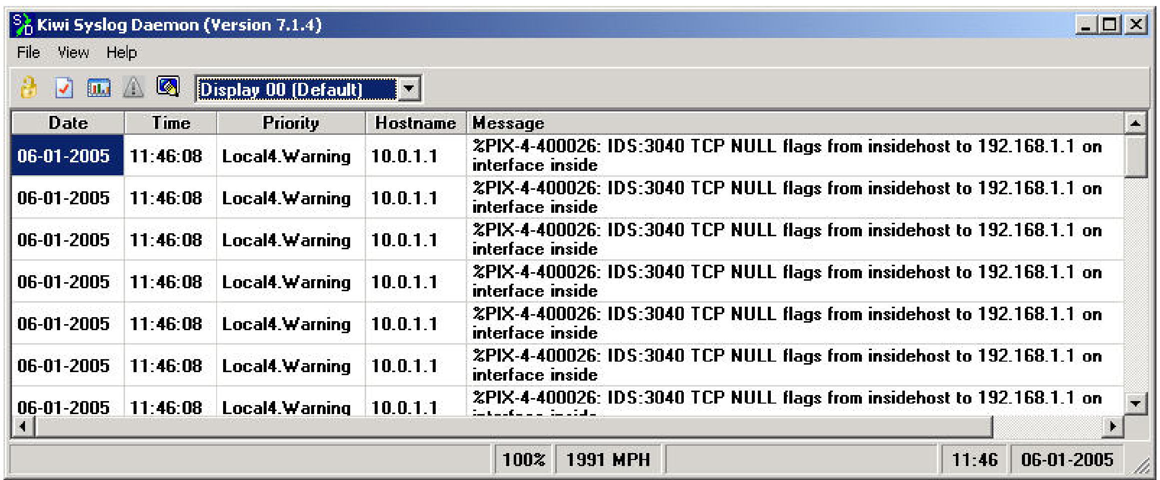


e. In the Host field, enter 192.168.P.1 and click the Scan button.

f. Return to the Kiwi Syslog Daemon display.



g. Stop the previous scan and perform a Null Scan. View the Kiwi output



h. Stop the Nmap Scan.

i. Compare the current configuration to the ending configuration for this lab if desired.

j. Remove the attack policy.

```
PixP(config)# no ip audit name ATTACKPOLICY
```

k. Verify that the attack policy has been removed from the inside interface, the default attack actions have been restored, and the ip audit name has been removed:

```
PixP(config)# show running-config ip audit interface
PixP(config)# show running-config ip audit attack
PixP(config)# show running-config ip audit name
```


Lab 4.4.7 Configure Cisco IOS IPSec using Pre-Shared Keys

Objective

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

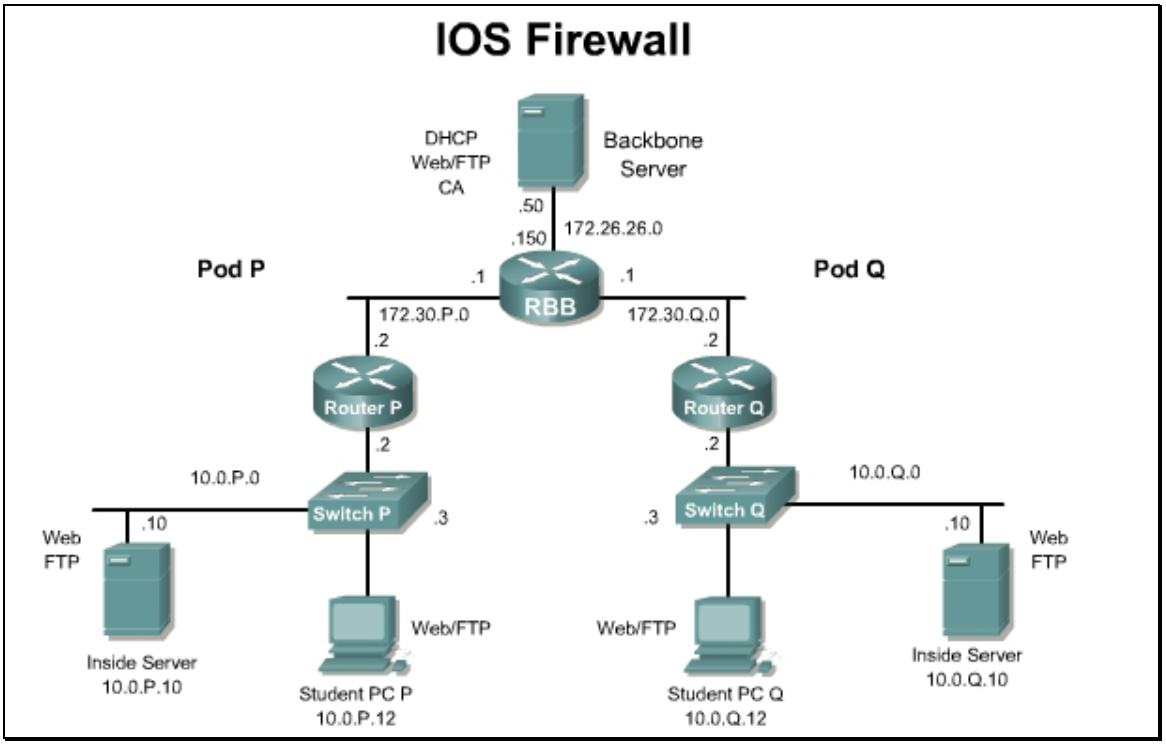
- Prepare to configure Virtual Private Network (VPN) Support
- Configure Internet Key Exchange (IKE) phase one
- Configure IKE parameters and verify IKE and IP Security (IPSec) configuration
- Configure IPSec parameters
- Verify and test IPSec configuration

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

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.

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
```


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
```


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.

Lab 4.4.8a Configure a Cisco GRE over IPSec Tunnel using SDM

Objective

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

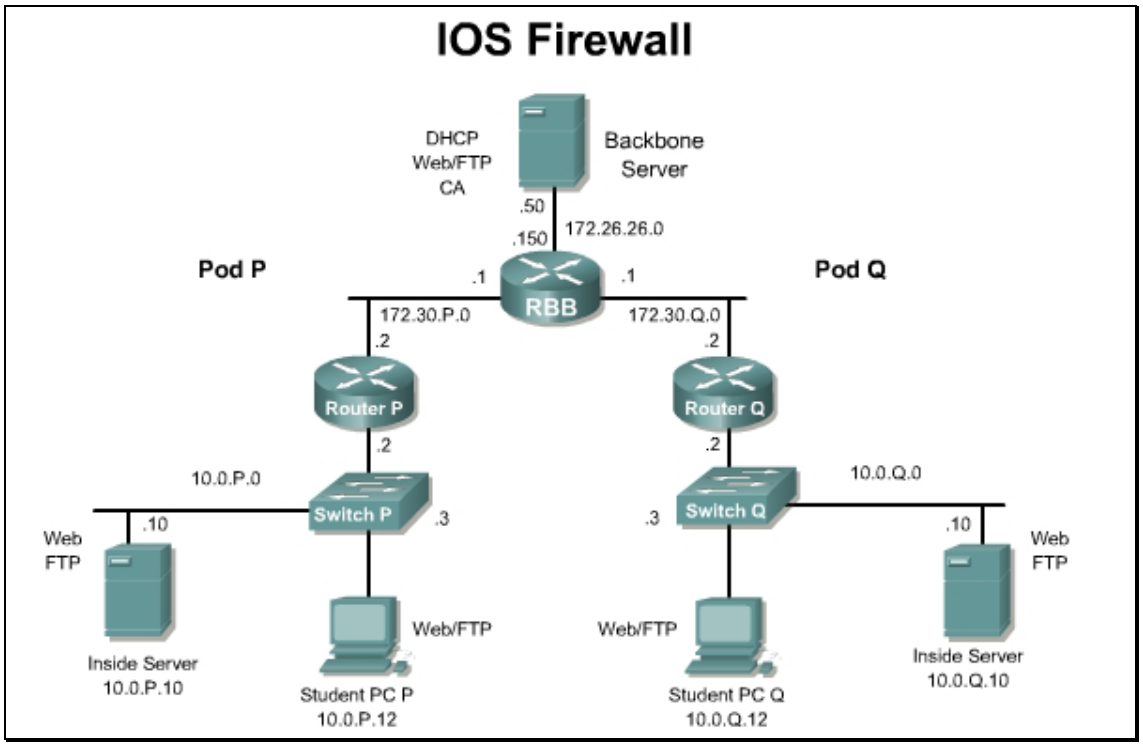
- Prepare to configure Virtual Private Network (VPN) Support
- Configure GRE over IPSec tunnel using SDM VPN Wizard
- Modify GRE over IPSec configuration
- Verify and test GRE over IPSec configuration

Scenario

The XYZ Company has Cisco routers at two branch offices, with SDM installed, and wants to create a secure VPN over the Internet between the two sites. The company needs to support IP, IPX, and Appletalk traffic across the WAN. Therefore a GRE over IPSec tunnel must be configured.

Topology

This figure illustrates the lab network environment.



Preparation

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

http://www.cisco.com/en/US/products/sw/secursw/ps5318/products_user_guide_chapter09186a008040443e.html

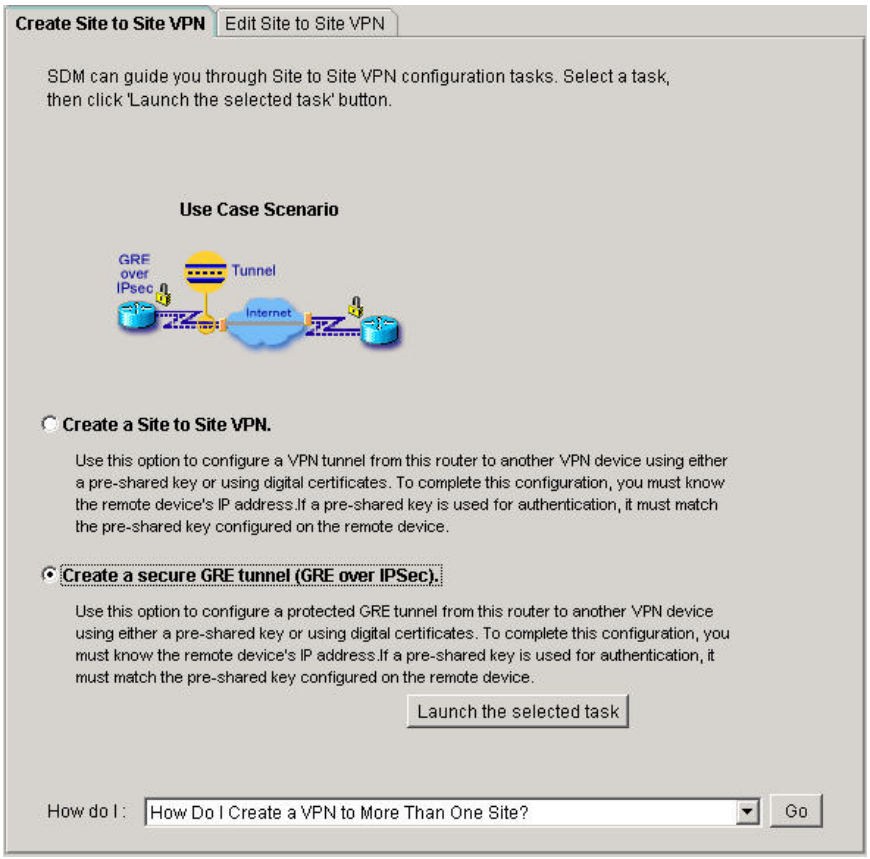
Step 1 Configure GRE over IPSec VPN Parameters

Work with the members of the pod group to complete the VPN configuration.

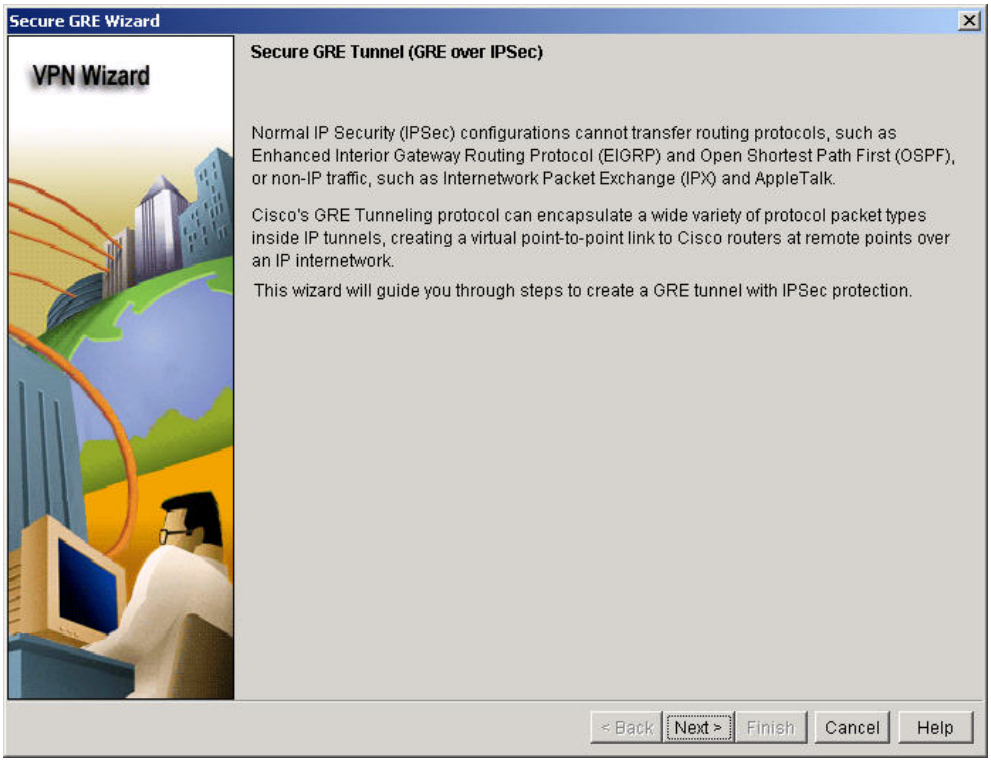
a. Establish an SDM session with the pod router. When prompted for a username and password, use **sdm**/**sdm**.

b. In SDM, select **VPN** from the Tasks panel of the **Configuration** page.

c. Select the **Create a secure GRE tunnel (GRE over IPSec).** Option from the **Site to Site VPN** tab.

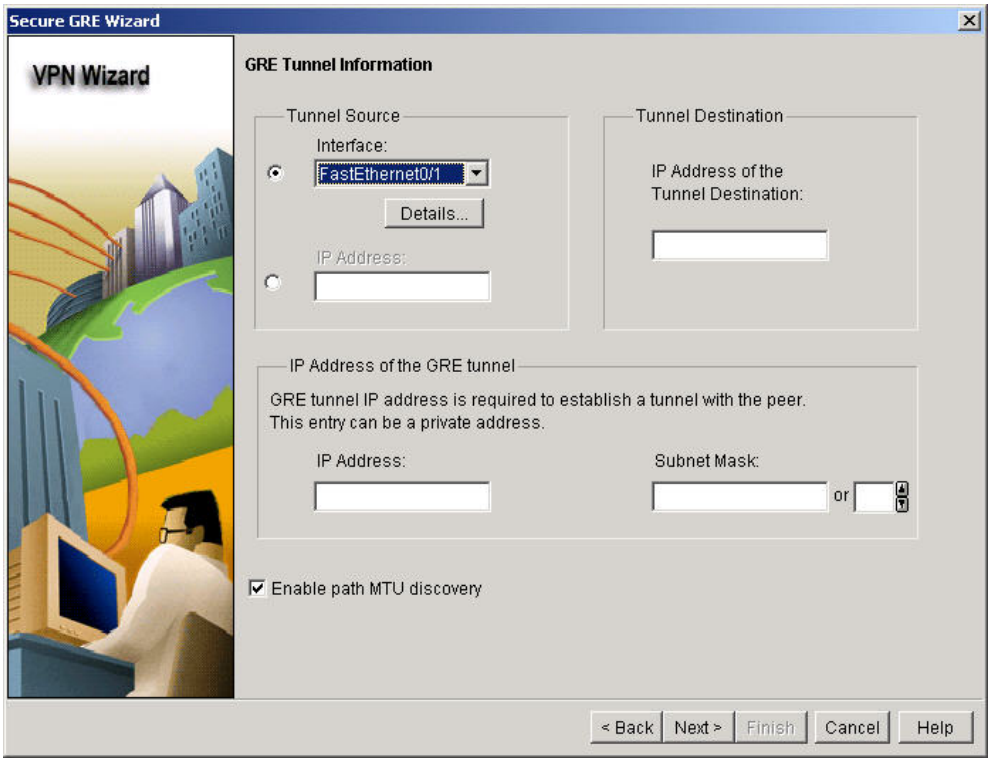


d. Click **Launch the selected task** button.



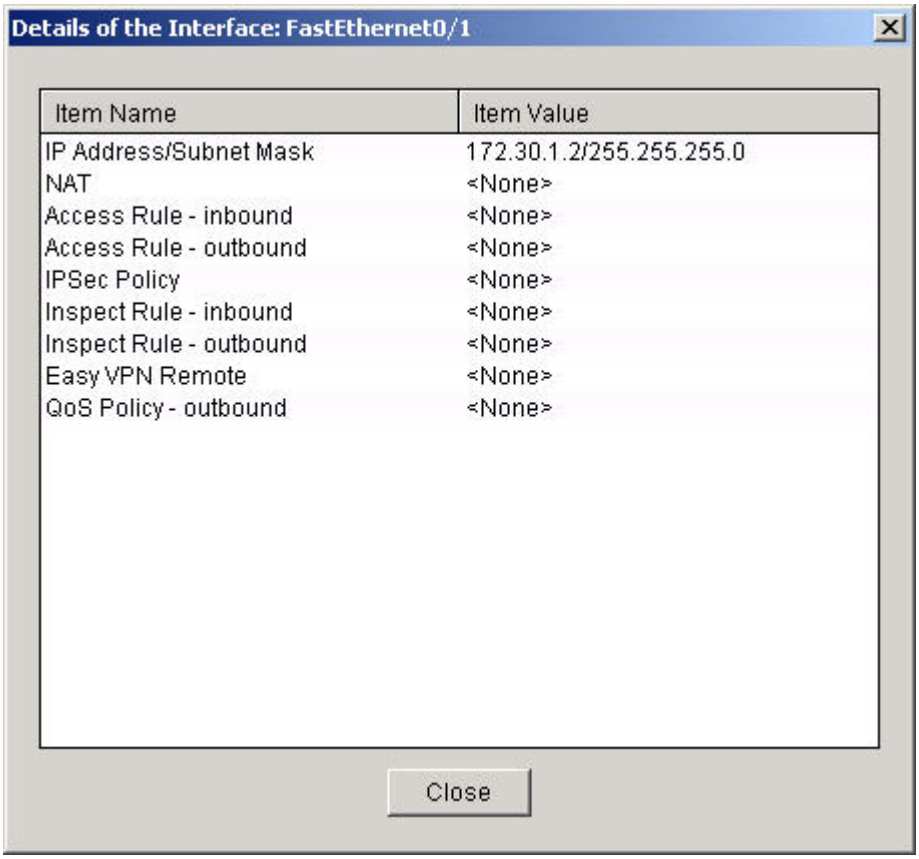
e. Click the **Next** button.

f. Select the outside interface (Fa0/1) for the Tunnel Source Interface.



g. Click on the Details button to verify the proper external address.

172.30.P.2 / 255.255.255.0



h. Set the Tunnel Destination as **172.30.Q.2** (where Q = peer pod number).

i. Enter the IP address and subnet mask of the GRE Tunnel.

172.16.1.P

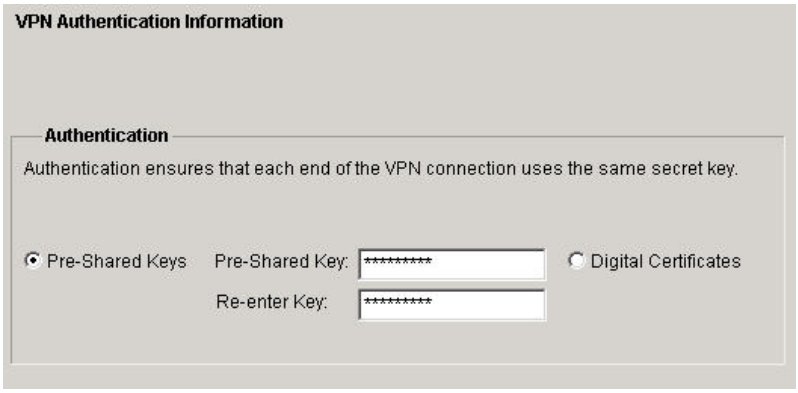
255.255.255.0 or 24

j. Click the **Next** button.

k. Skip the Backup GRE Tunnel Window and click the **Next** button. A backup will not be configured.

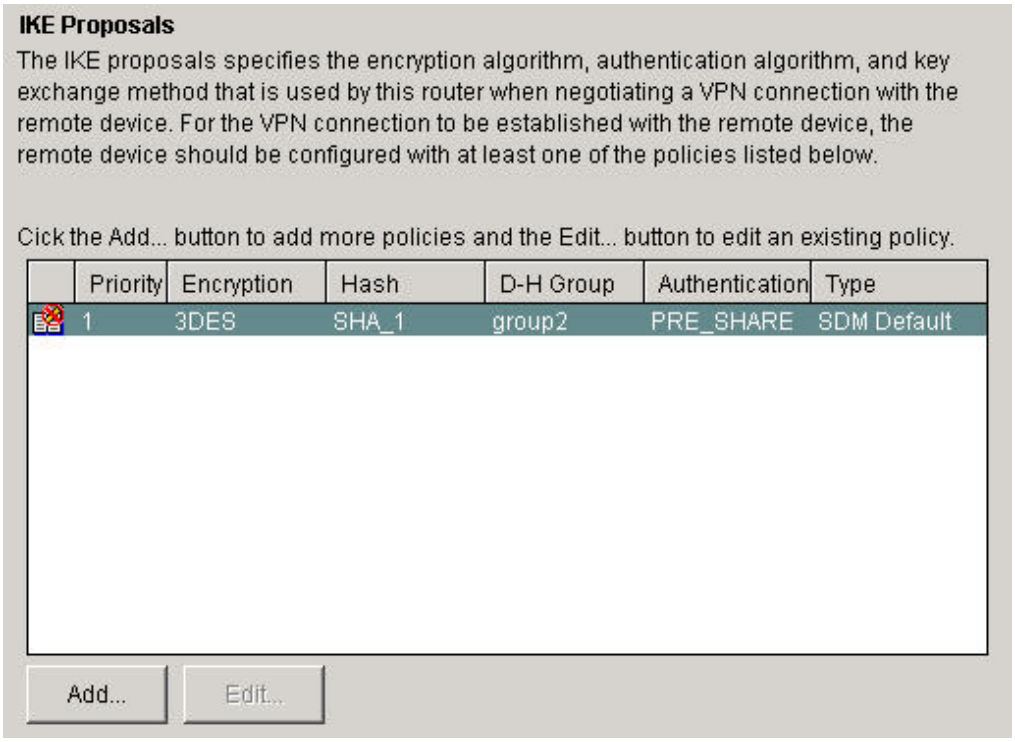
l. In the VPN Authentication window, enter and re-enter to confirm a pre-shared key to be used for authentication. (make sure the CAPS lock is not on)

cisco1234



m. Click the **Next** button.

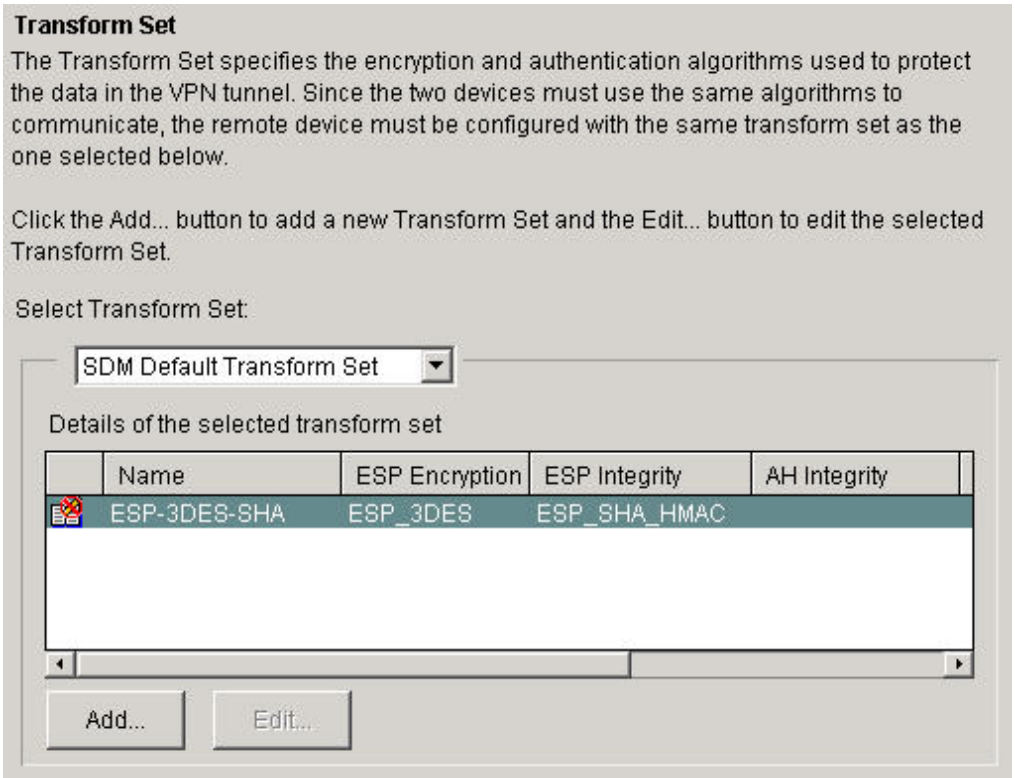
n. In the **IKE Proposal** window, notice the default policy.



o. Click the **Next** button

p. An information window will appear about IKE.

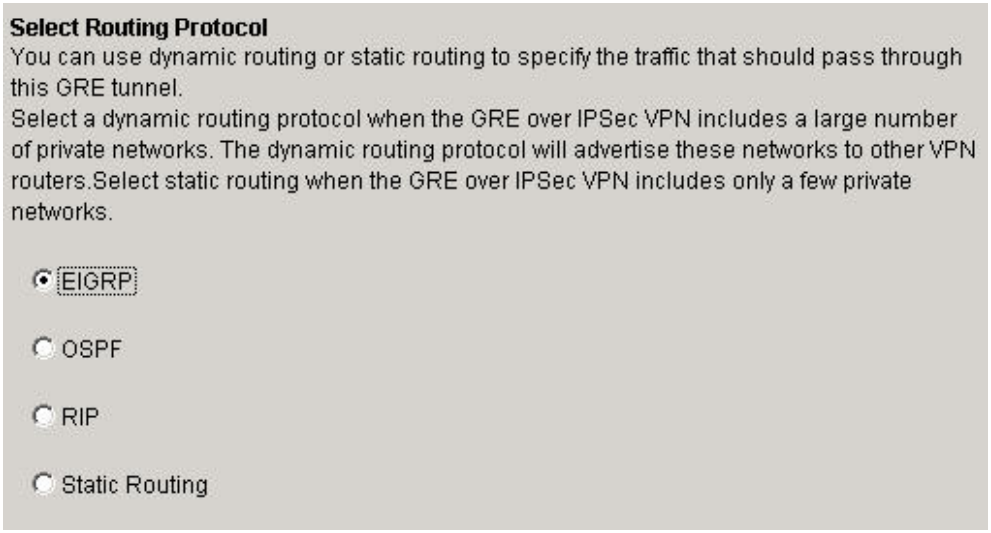
q. The **Transform Set** window will appear.



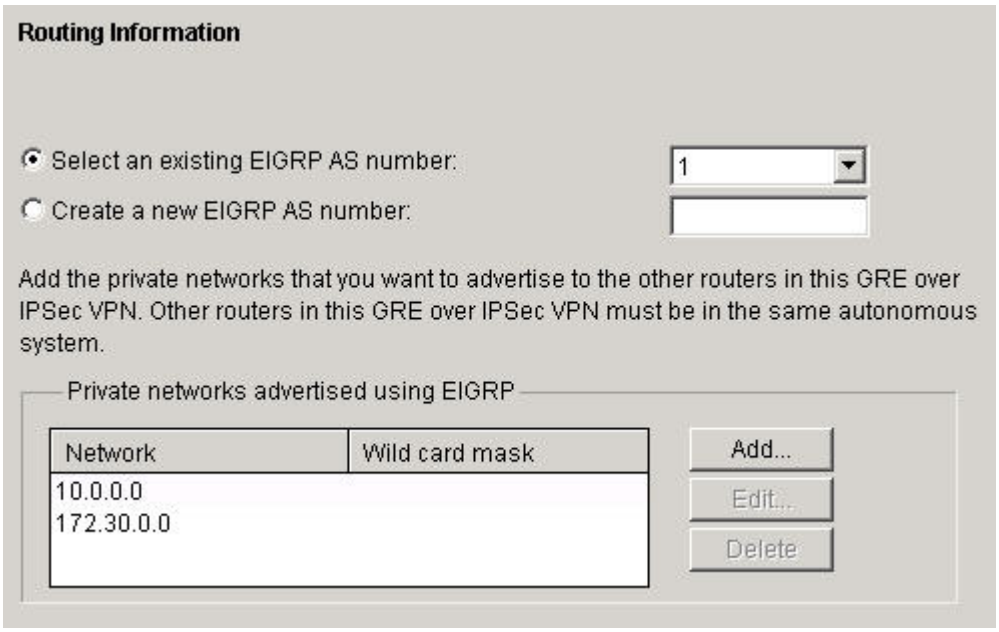
r. Click the **Next** button

s. The **Select Routing Protocol** window will appear.

t. Select **EIGRP** and click the **Next** button

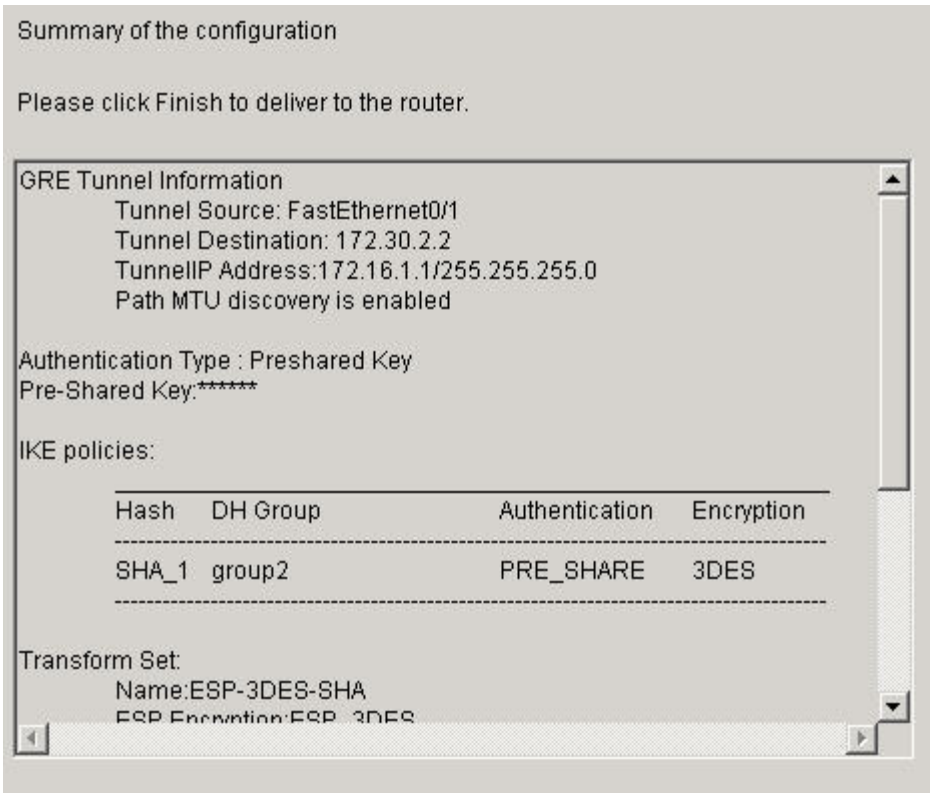


u. The **Routing Information** window will appear for EIGRP.



v. Click the **Next** button.

w. The **Configuration Summary** window will appear.



x. Verify the configuration.

y. Click the **Finish** button

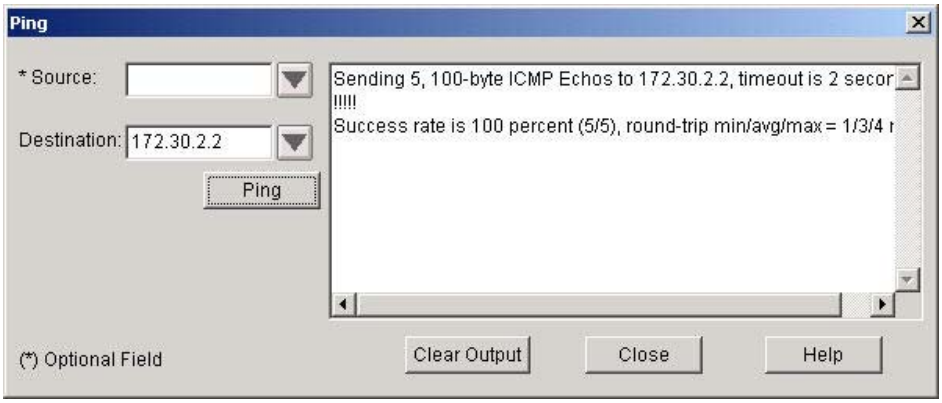
z. Click the **OK** button on the **Command Deliver Status** window to complete the configuration delivery.

Step 2 Verify and Monitor the VPN Tunnel

Work with the members of the pod group to verify the VPN Tunnel.

a. Navigate to the **Tools>Ping**.

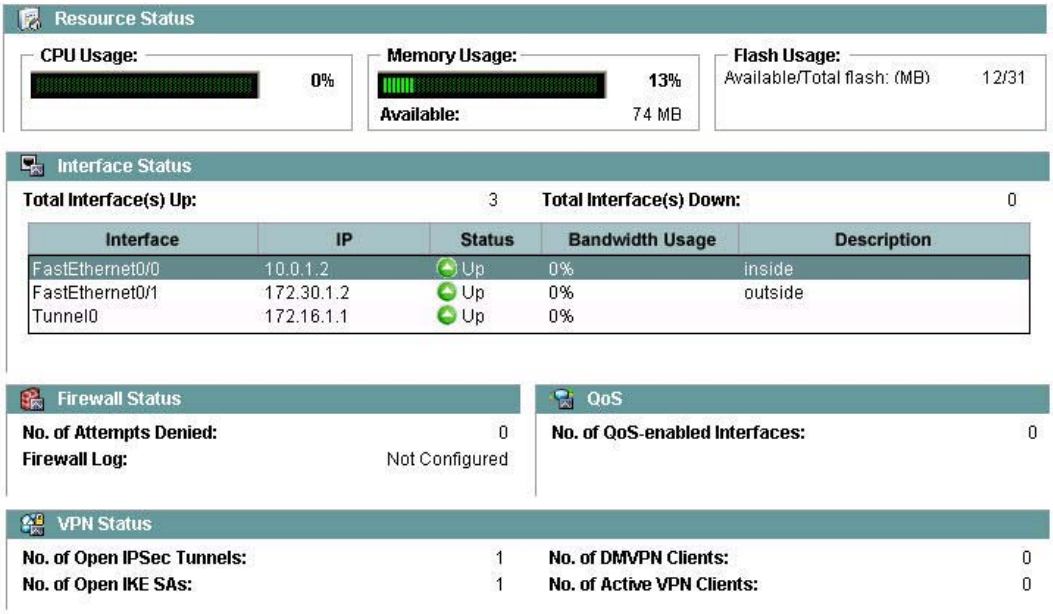
b. Ping the peer's router outside address at 172.30.Q.2.



c. The ping should be successful. Most likely, the tunnel is already established due to the EIGRP routing update traffic.

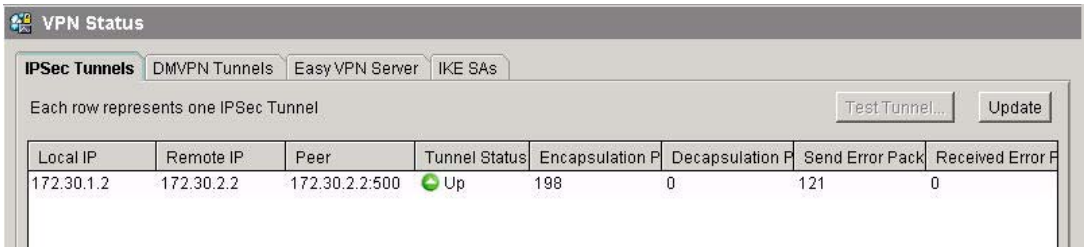
d. Click on the **Close** button.

e. Now click on the **Monitor** button on the top navigation bar.

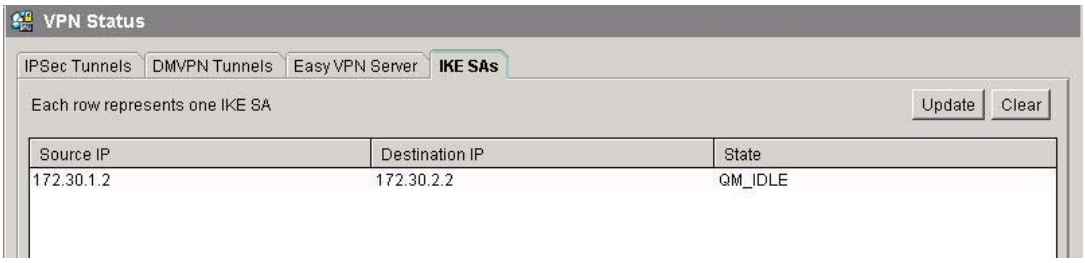


f. Notice the VPN Status box where one open IKE SA and one open IPSec tunnel are now shown.

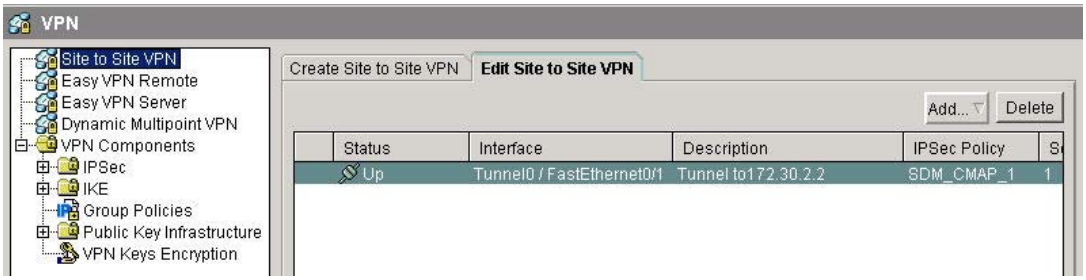
g. Click on **VPN Status** in the **Tasks** panel to view detailed information about the established VPN tunnel. The VPN tunnel status should display as Up by the green icon.



h. Select the **IKE SAs** tab to view the active IKE SAs.

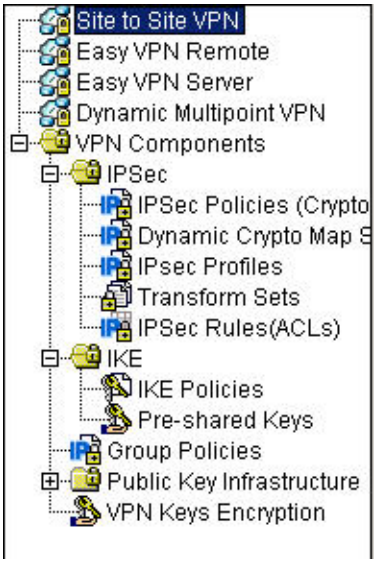


i. Select **VPN** from the Tasks panel of the **Configuration** page.



j. This will provide the tunnel status as well as additional information about the VPN tunnel configuration.

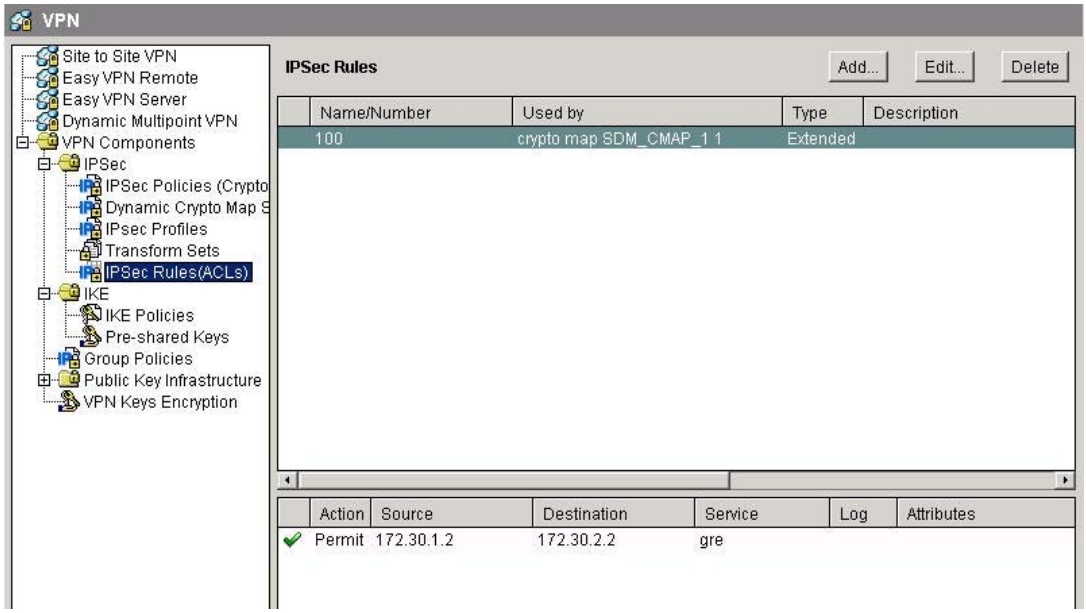
k. Click through the **VPN Components** tree to view the detailed configuration.



Step 3 Modify the GRE over IPSec configuration

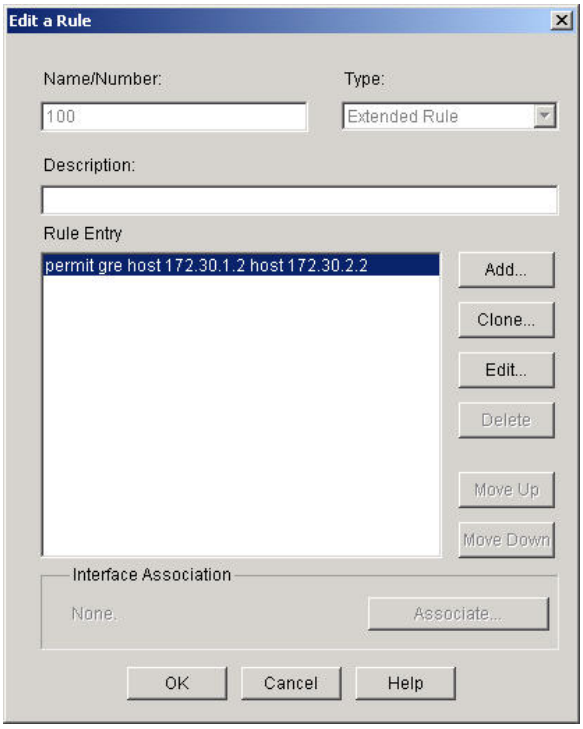
Work with the members of the pod group to modify the VPN encryption settings

a. Click on **IPSec Rules(ACLs)** in the VPN Components tree.



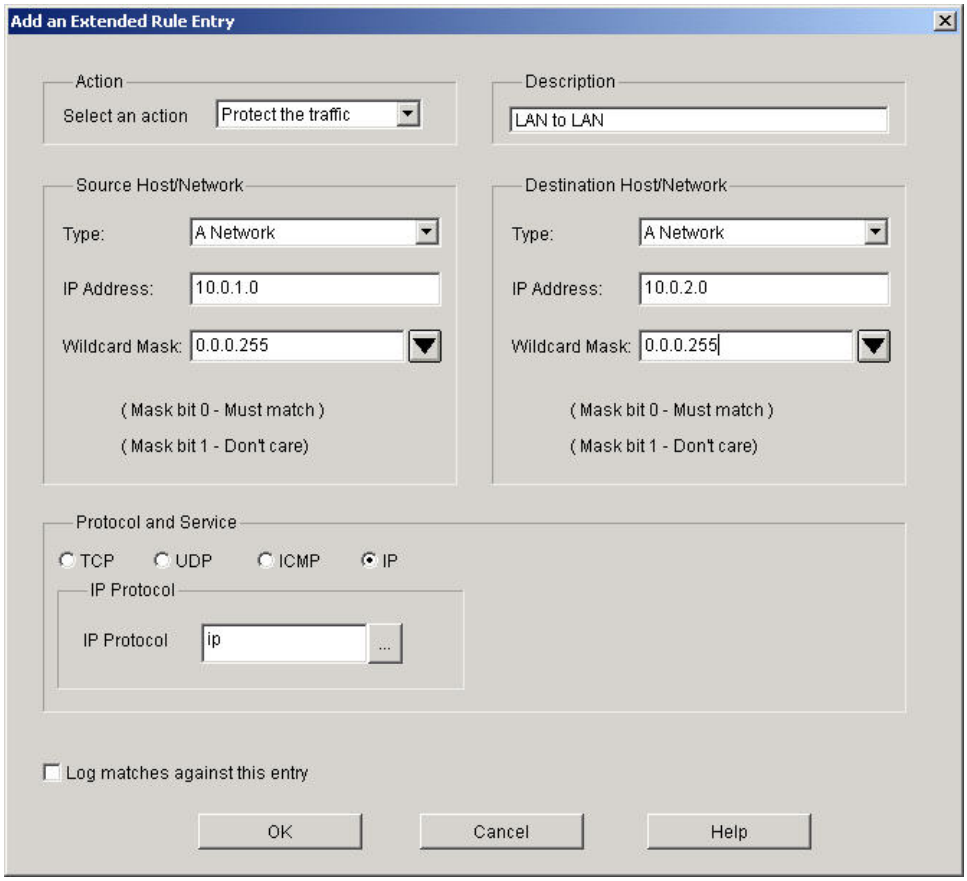
b. Click on the IPSec Rules Number **100**.

c. Click the **Edit** button.



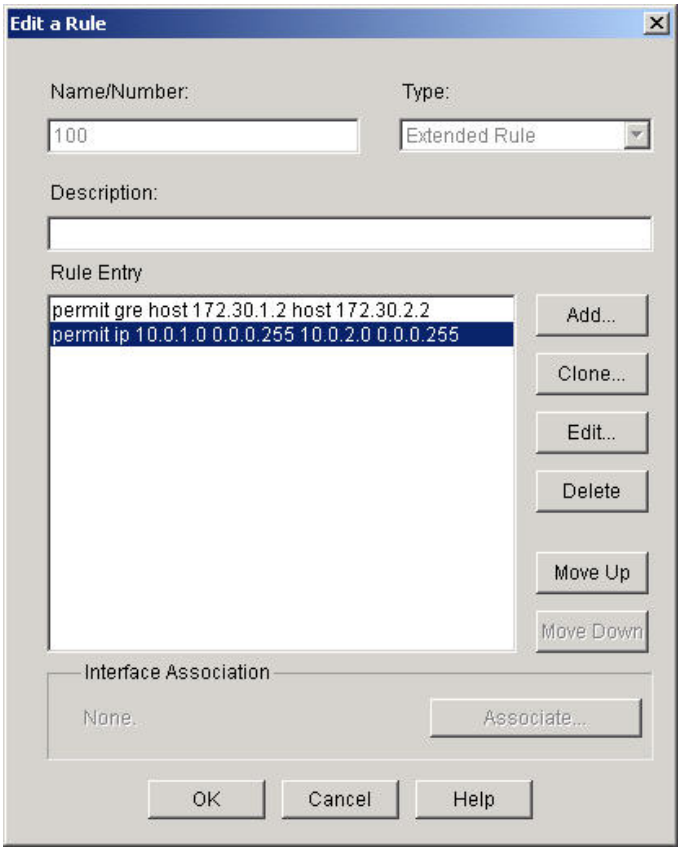
Notice that the only traffic which is in the GRE over IPSec tunnel is from outside interface of the router to the outside interface of the peer router.

d. Click the **Add** button to add an ACL to protect LAN to LAN traffic.



This sample shows the ACL added on Router1. Router 2 will have Source/Destination Networks reversed.

e. Click the **OK** button. The **Edit a Rule** window will appear now with the added ACL entry.



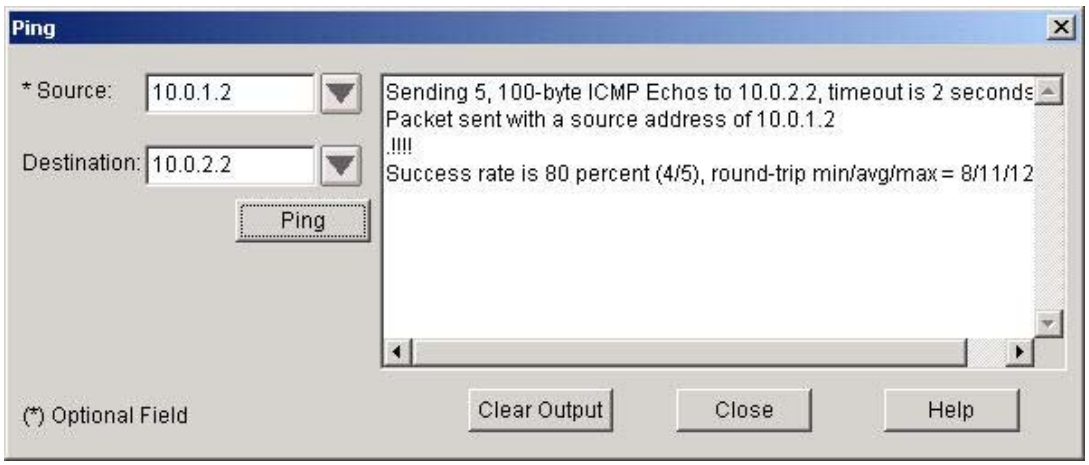
f. If the **Command Delivery Status** window appears, click the **OK** button to continue.

g. Verify that there are now two ACL entries.

	Action	Source	Destination	Service	Log	Attributes
✔	Permit	172.30.1.2	172.30.2.2	gre		
✔	Permit	10.0.1.0/0.0.0.255	10.0.2.0/0.0.0.255	ip		

l. Navigate to the **Tools>Ping**.

h. Ping the inside address of the peer router at 10.0.Q.2 from a source address of 10.0.P.2. 20% may be lost while the tunnel is negotiated for the first time for this traffic.



Lab 4.4.8b Configure Cisco IOS IPSec with Pre-Shared Keys using SDM

Objective

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

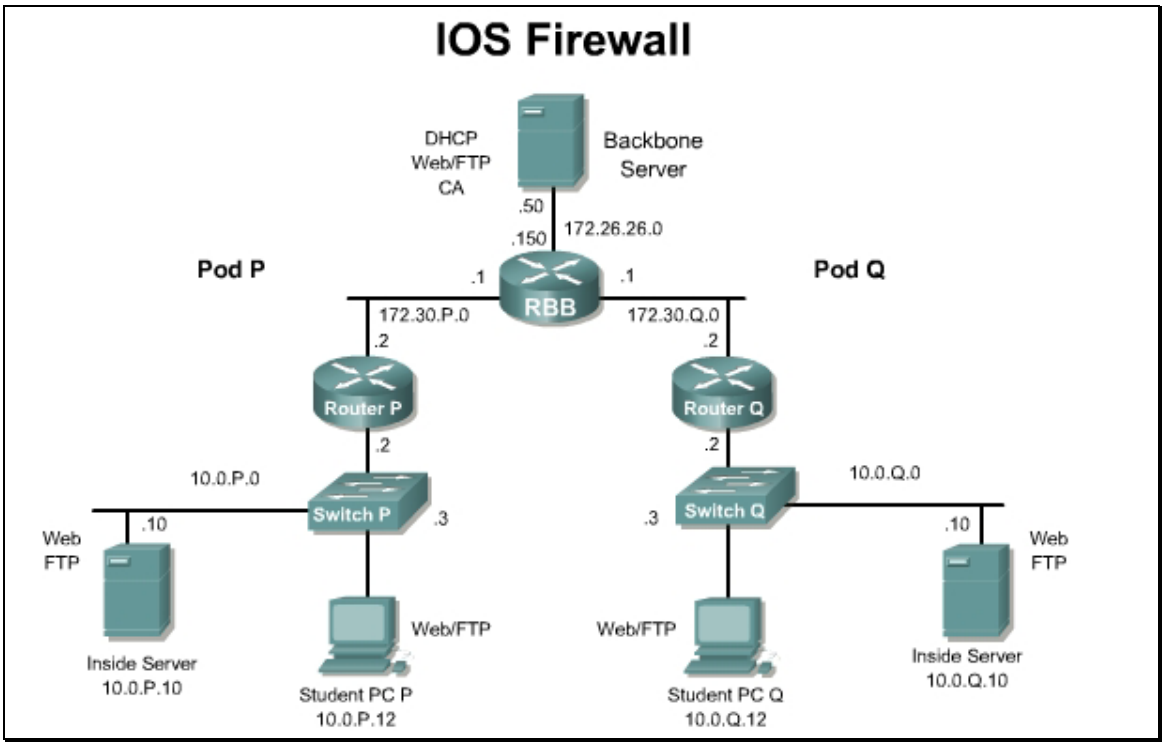
- Prepare to configure Virtual Private Network (VPN) Support
- Configure VPN tunnel using SDM VPN Wizard
- Modify IKE and IP Security (IPSec) configuration
- Verify and test IPSec configuration

Scenario

The XYZ Company has Cisco routers at two branch offices, with SDM installed, and wants to create a secure VPN over the Internet between the two sites. The security policy specifies using IPSec with pre-shared keys for authentication.

Topology

This figure illustrates the lab network environment.



Preparation

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

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 Advanced Encryption Standard (AES) 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:

```
ping 172.30.Q.2
```

(where Q = peer pod number)

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

_____

Answer: The key would need to be shared.

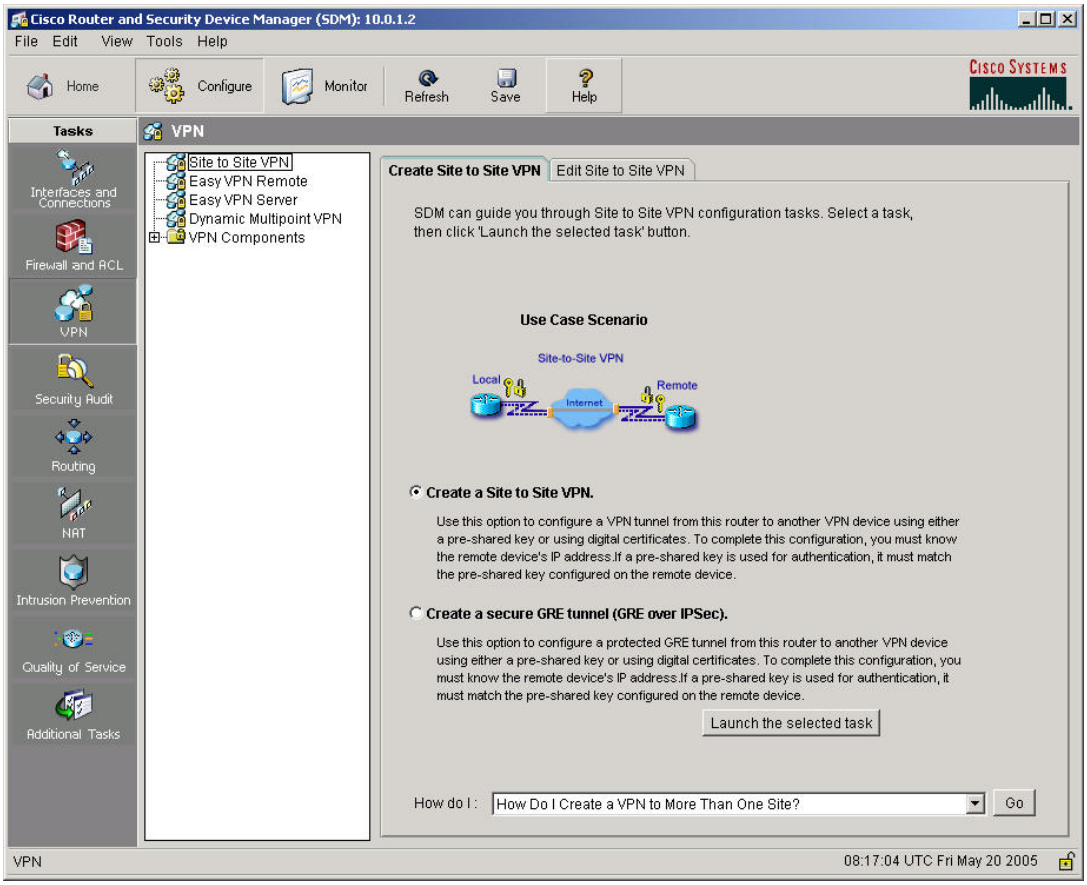
Step 2 Configure VPN Parameters

Work with the members of the pod group to complete the VPN configuration.

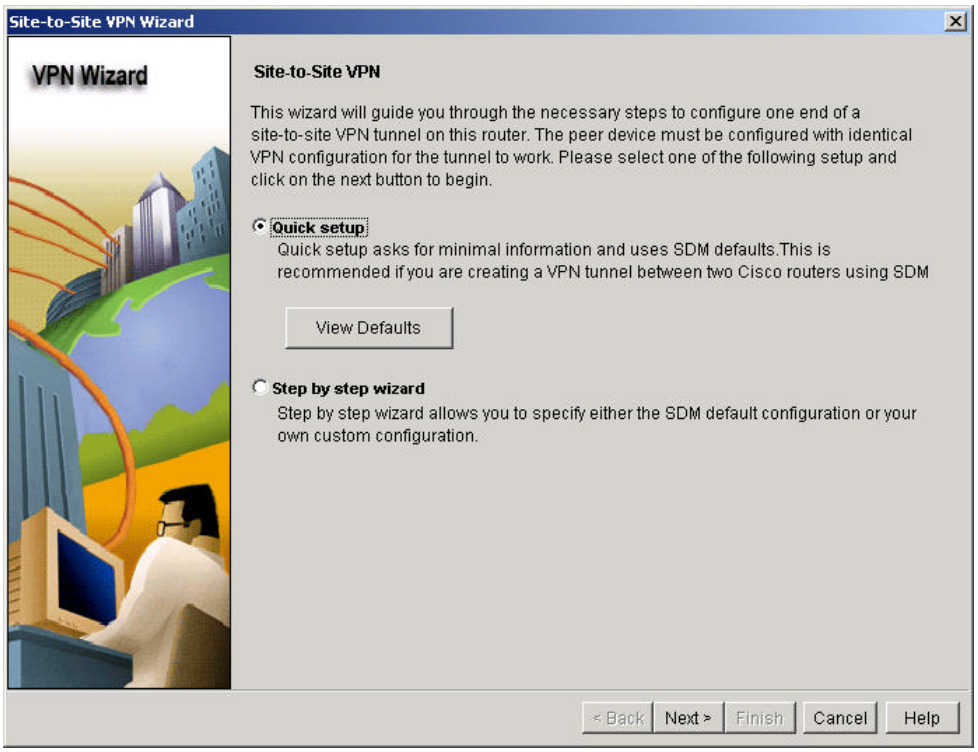
a. Establish an SDM session with the pod router. When prompted for a username and password, use **sdm**/**sdm**.

b. In SDM, select **VPN** from the Tasks panel of the **Configuration** page.

c. Select the **Create a Site to Site VPN.** option from the **Create Site to Site VPN** tab.

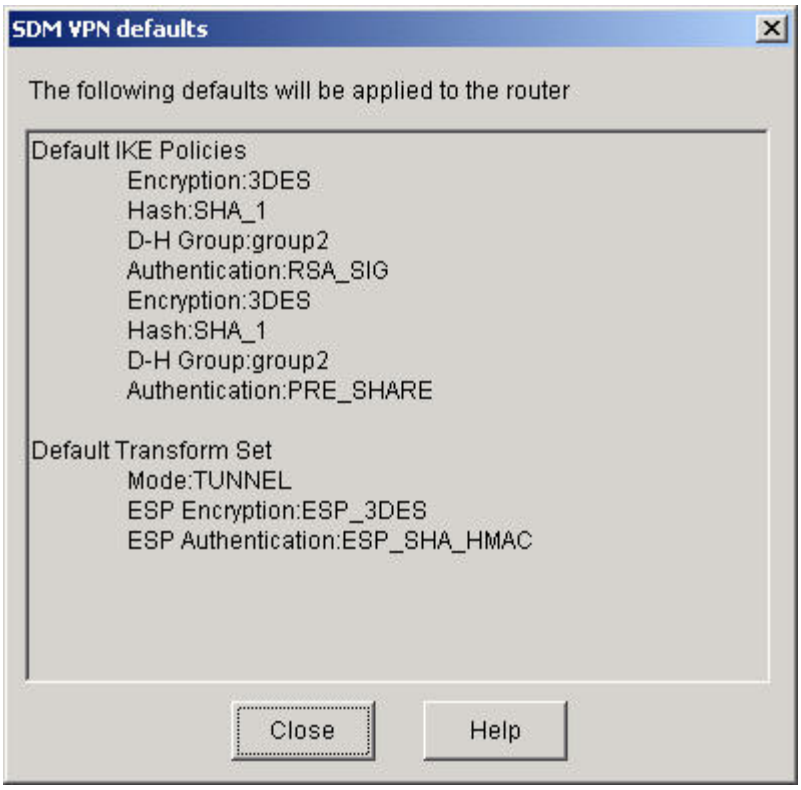


d. Click **Launch the selected task** button.



At this point, a choice between one of two options is available. The Quick setup mode or the Step by step wizard can be used. For this lab exercise, use the Quick setup mode.

e. Click **View Defaults** button to see how the quick setup will configure the VPN.

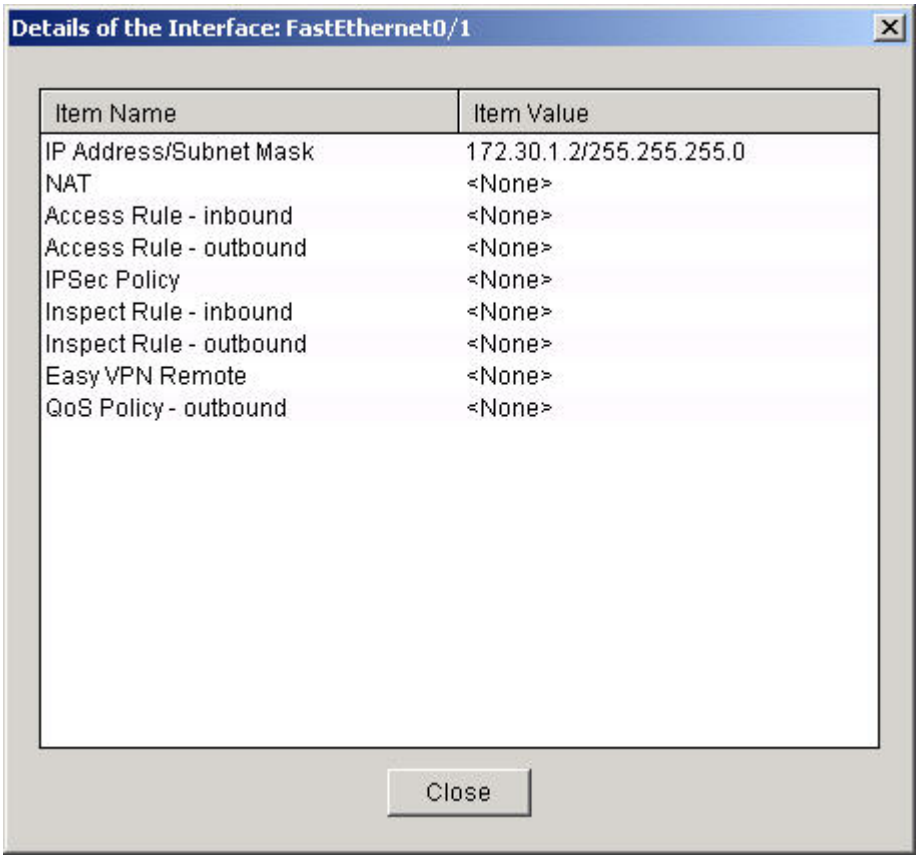


f. Select **Quick Setup** and click the **Next** button.

g. Click the **Close** button to return to the Site to Site VPN Wizard.

h. Select the outside interface (Fa0/1) for the VPN connection.

i. Click on the **Details** button to verify the proper external address.



The IP address should be ***172.30.P.2*** (where P = pod number)

j. Click the **Close** button to return to the Site to Site VPN Wizard.

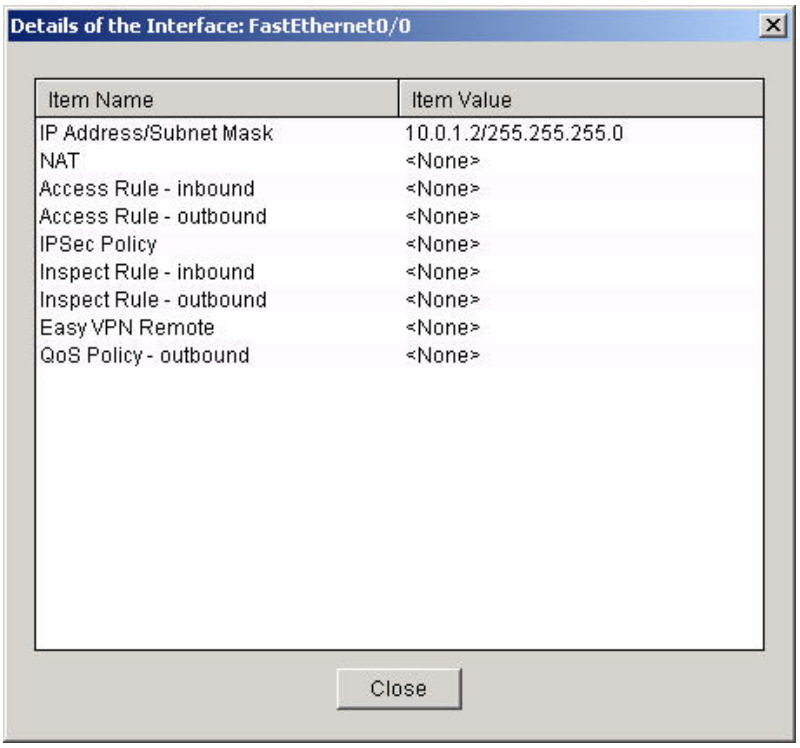
k. Set the Peer Identity as **172.30.Q.2** (where Q = peer pod number).

l. Enter and confirm a pre-shared to be used for authentication. (make sure the CAPS lock is not on)

cisco1234

m. Select the inside interface (Fa0/0) where the traffic to be encrypted originates to protect the source traffic.

n. Click on the **Details** button to verify the address is 10.0.P.2/255.255.255.0 (where P = pod number).



o. Click the **Close** button to return to the Site to Site VPN Wizard.

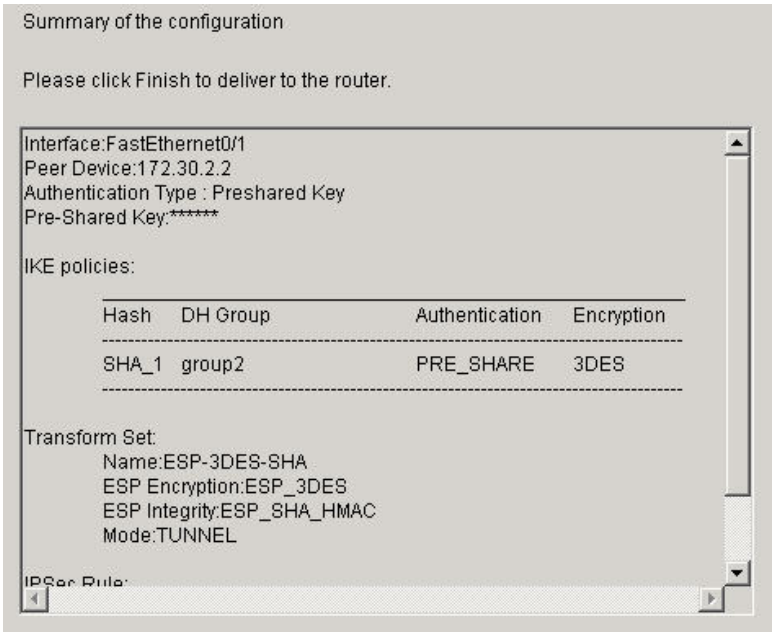
p. Make the appropriate selection for the destination where encrypted traffic terminates to protect all destination traffic.

IP Address: **10.0.Q.0**/ (where Q = peer pod number)

Subnet Mask: **255.255.255.0** or **24**

q. Click the **Next** button. When a message appears stating that IKE is disabled on the router, click the **OK** button.

r. Verify the configuration summary.



Note which IKE policy and Transform set will be deployed. If there are any mistakes, go back and fix them before proceeding.

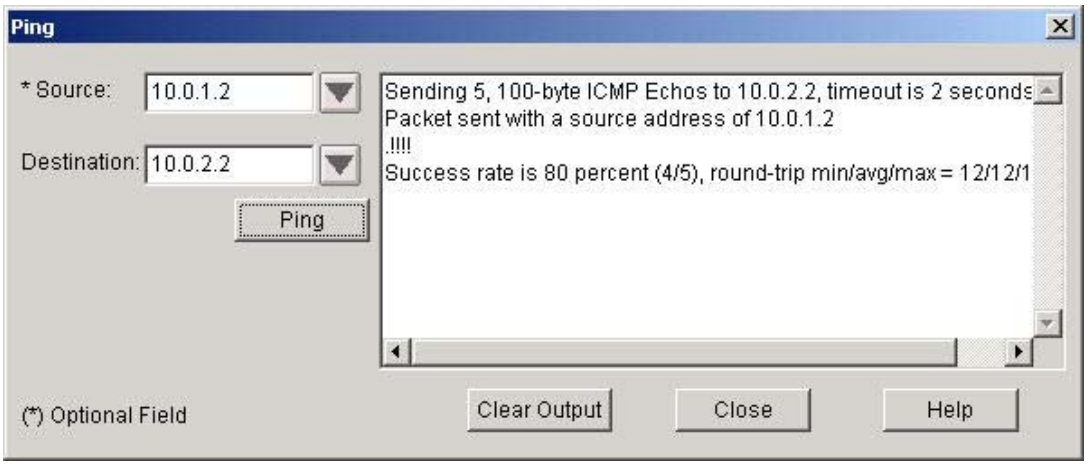
s. Click the **Finish** button to apply this change to the router configuration. Click the **OK** button on the **Command Deliver Status** window to complete the configuration delivery.

Step 3 Verify and Monitor the VPN Tunnel

Work with the members of the pod group to verify the VPN Tunnel.

a. Navigate to the **Tools>Ping**..

b. Ping the peer's inside router interface address at 10.0.Q.2. Make sure the source address is the inside address of the router.10.0.P.2. In the example below, the ping is initiated from Pod 1.



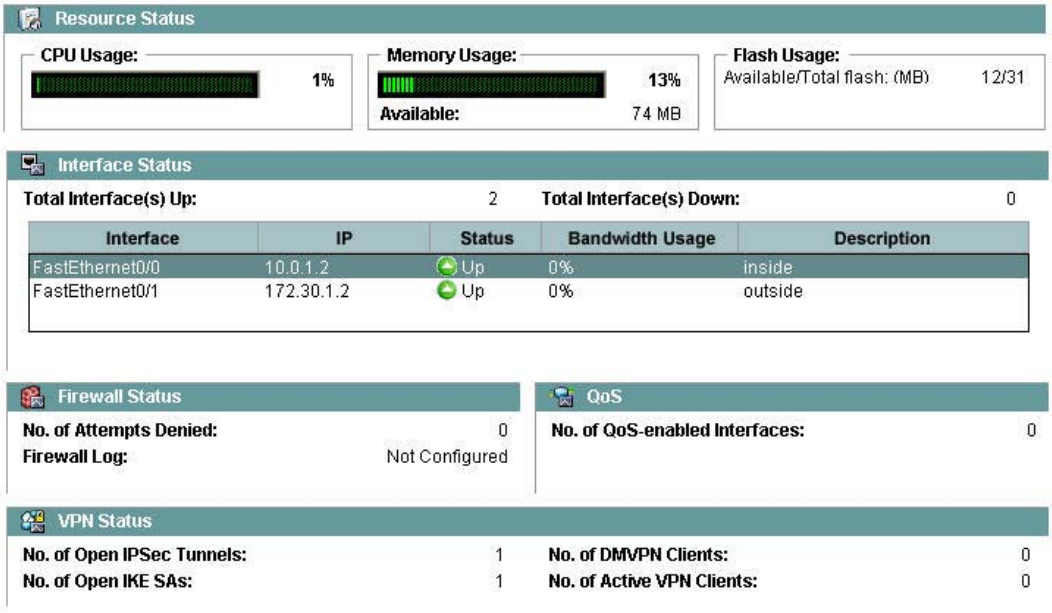
c. If the ping is less than 100% successful the first time, this is due to the tunnel establishment phase.

d. Click on the **Clear Output** button and repeat the ping.

e. The ping should be at 100%.

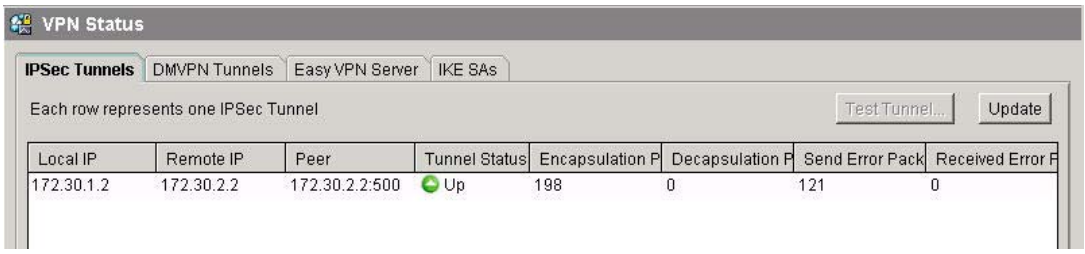
f. Click on the **Close** button.

g. Now click on the **Monitor** button on the top navigation bar.



h. Notice the VPN Status box where one open IKE SA and one open IPSec tunnel are now shown.

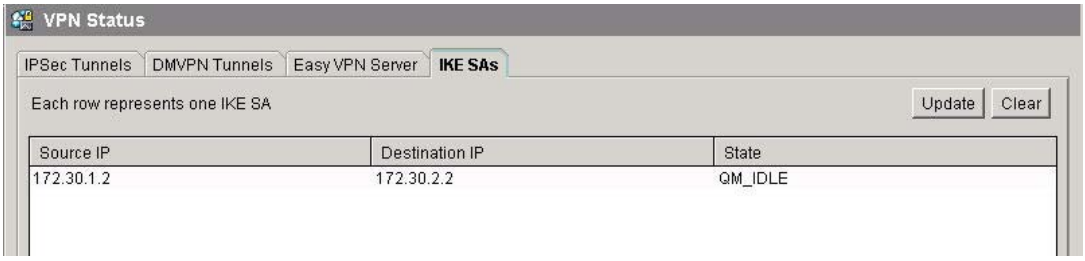
i. Click on **VPN Status** in the **Tasks** panel to view detailed information about the established VPN tunnel. The VPN tunnel status should display as Up by the green icon.



1. What other types of connections can be viewed on this page?

Answer: The tabs at the top of the window are IPSec Tunnels, DMVPN Tunnels, Easy VPN Server, and IKE SAs

j. Select the **IKE SAs** tab to view the active IKE SAs.

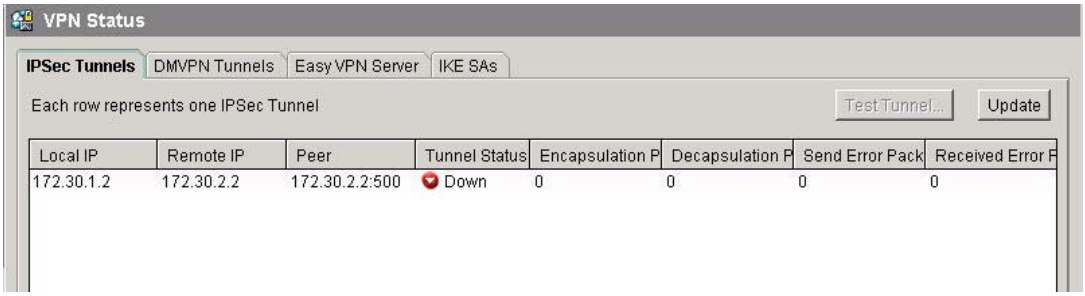


k. Click on the **Clear** button. This will delete the IKE SA.

l. On the router, through the command line, clear the VPN session

```
RouterP#clear crypto session
```

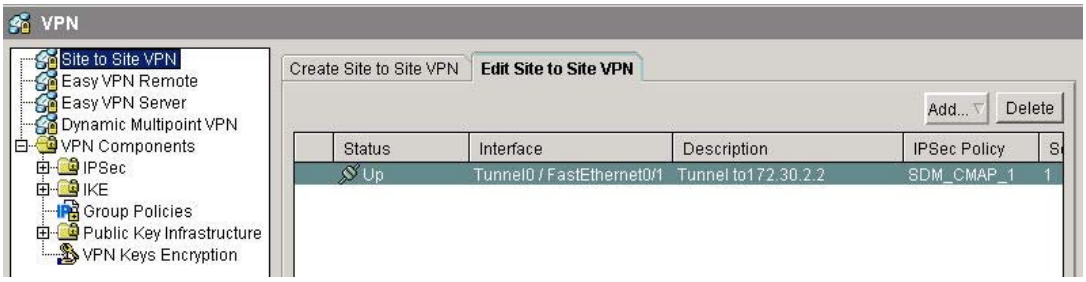
m. Return back to the **IPSec Tunnels** tab in SDM. Click the **Update** button to update the **IPSec Tunnels** status.



n. The VPN tunnel will show a down state indicated by the red icon.

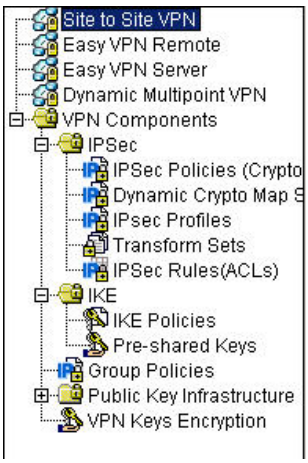
o. Repeat the ping as directed, beginning in Step3a to reestablish the tunnel.

p. Select **VPN** from the Tasks panel of the **Configuration** page.



q. This will provide the tunnel status as well as additional information about the VPN tunnel configuration.

r. Click through the **VPN Components** tree to view the detailed configuration.

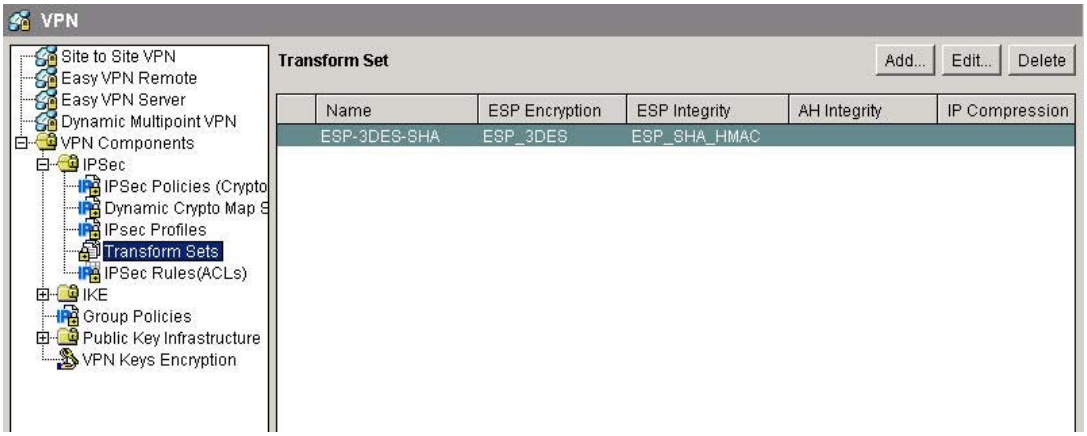


Step 4 Modify the VPN configuration

Work with the members of the pod group to modify the VPN encryption settings

a. Navigate to the **Configure>VPN**.

b. Click on **VPN Components>IPSec>Transform Sets** in the tree menu.



c. Click on the **Edit** button

d. Change the Encryption Algorithm: to **ESP_AES_256**

e. Click **OK**.

f. If the **Command Delivery Status** window appears, click the **OK** button to continue.

1. On the router, through the command line, clear the VPN sessions.

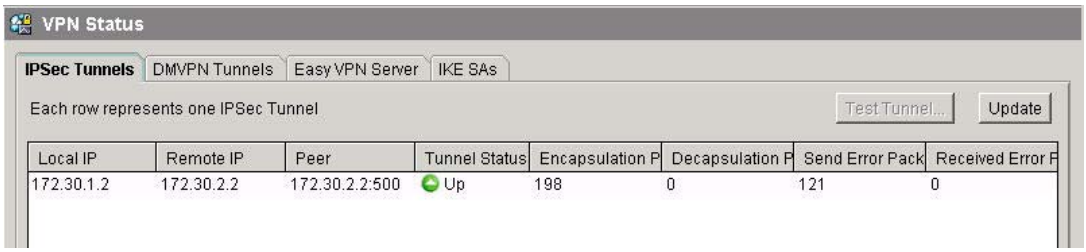
```
RouterP#clear crypto session
```

2. Make sure the peer router has changed to ESP_AES256.

g. Ping the peer as directed, beginning in Step3a. The ping step may have to be repeated a second time.

h. Navigate to **Monitor>VPN Status>IPSec Tunnels**.

i. Click the **Update** button. The tunnel should now be up.

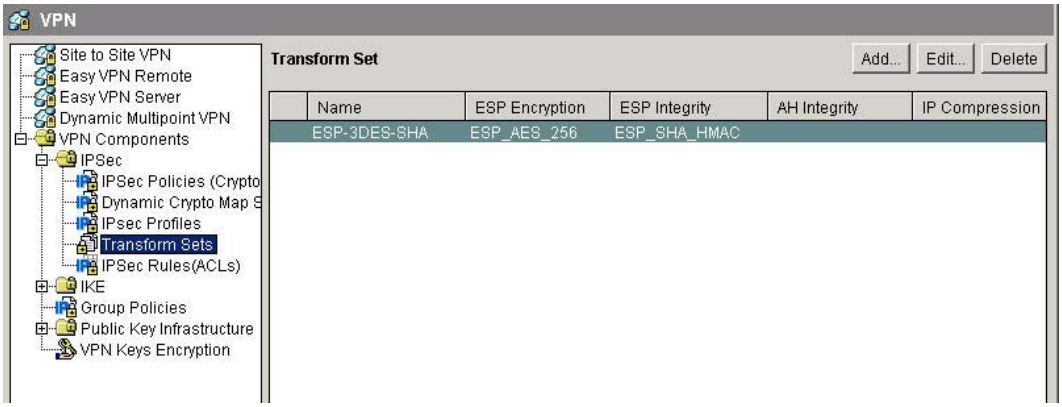


j. Click the **Configure** button at the top of the SDM window.

k. Select **VPN** from the **Tasks** panel.

l. In the tree menu, select **VPN Components>IPSec>Transform Sets**

m. The transform set ESP_AES_256 should be shown.



n. If desired, change the IKE Policy to AES_256

o. If desired, change the DH group to Group 5.

p. If desired, change the Pre-shared Keys.

q. If desired, change the lifetimes of the IKE and IPSec Policies. Change these to a low value around 2 or 3 minutes. Debug the IPSec output to observer the Tunnel rekey before the time expiration. Also, configure a different lifetime value on the Peer router and observer the Tunnel characteristics at the expiration time.

r. Enable debug output for IPSec events.

```
RouterP#debug crypto ipsec
```

s. Enable debug output for ISAKMP events.

```
RouterP#debug crypto isakmp
```


Step 5 Configure VPN Parameters using Step by Step Wizard.(Optional)

Work with the members of the pod group to complete the VPN configuration using the Step by step wizard.

a. Delete the current VPN.

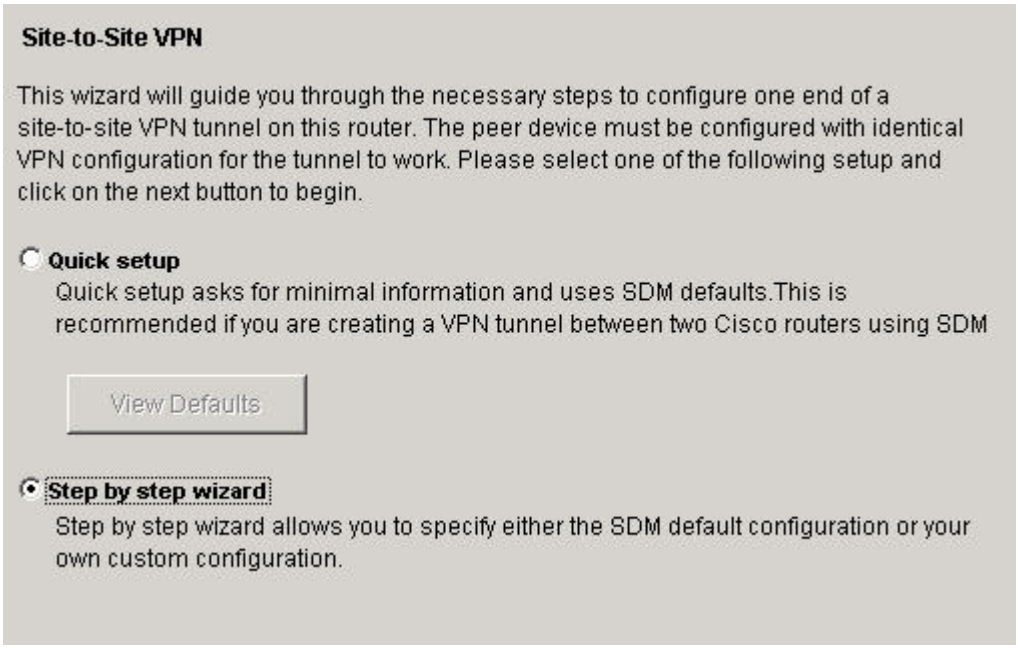
b. Select the **VPN** wizard from the category bar.

Figure1

c. Select the **Create a Site to Site VPN with Pre-Shared Key** option.

d. Click **Launch the selected task** button.

e. Choose the **Step by step wizard**.



f. Continue through the Step by step wizard using the same values that were used in the previous steps.

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:

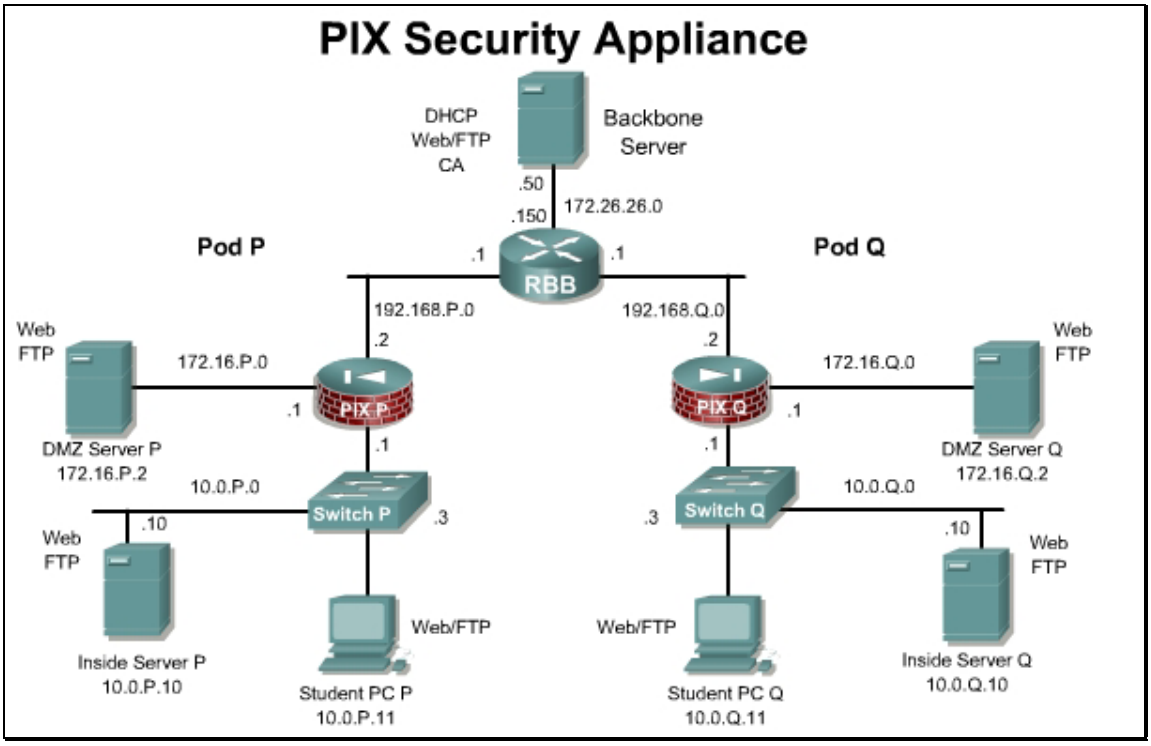
- Prepare to configure VPN support.
- Configure IKE and IPSec parameters.
- Test and verify IPSec configuration.

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
clear configure access-list [*id*]	To clear an access list from the running configuration, use the **clear configure access list** command in global configuration mode.
clear configure crypto map	Removes the crypto map configuration.
clear configure ipsec	Removes the ipsec configuration.
clear configure isakmp	Removes the isakmp configuration.
clear configure sysopt	Removes all **sysopt** commands from the configuration.
clear configure tunnel-group	Removes all tunnel groups from the configuration.
crypto ipsec *map-name seq-num* **transform-set** *transform-set-name transform1* [*transform2*]	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 *map-name seq-num* **match address** *acl_name*	To assign an access list to a crypto map entry, use the **crypto map match address** command in global configuration mode.
crypto map *map-name seq-num* **set peer** {*ip_address* | *hostname*}{...*ip_address* | *hostname10*}	To specify an IPSec peer in a crypto map entry, use the **crypto map set peer** command in global configuration mode.
crypto map *map-name seq-num set* **transform-set** *transform-set-name1* [… *transform-set-name9*]	To specify the transform sets to use with the crypto map entry, use the **crypto map set transform-set** command in global configuration mode.

Command	Description
crypto map *map-name* **interface** *interface-name*	Use the **crypto map interface** command in global configuration mode to apply a previously defined crypto map set to an interface.
isakmp enable *interface-name*	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 *key-id-string* **| auto}**	To set the Phase 2 ID to be sent to the peer, use the **isakmp identity** command in global configuration mode.
isakmp policy *priority* **authentication {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 *key*	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 *name* **type** *type*	To create and manage the database of connection-specific records for IPSec, use the **tunnel-group** command in global configuration mode.
tunnel-group *name* **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 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?

_____

Answer: esp-3des, esp-aes, esp-aes-192, esp-aes-256, esp-none, esp-null, esp-sha-hmac

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 crytpo 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
```


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:

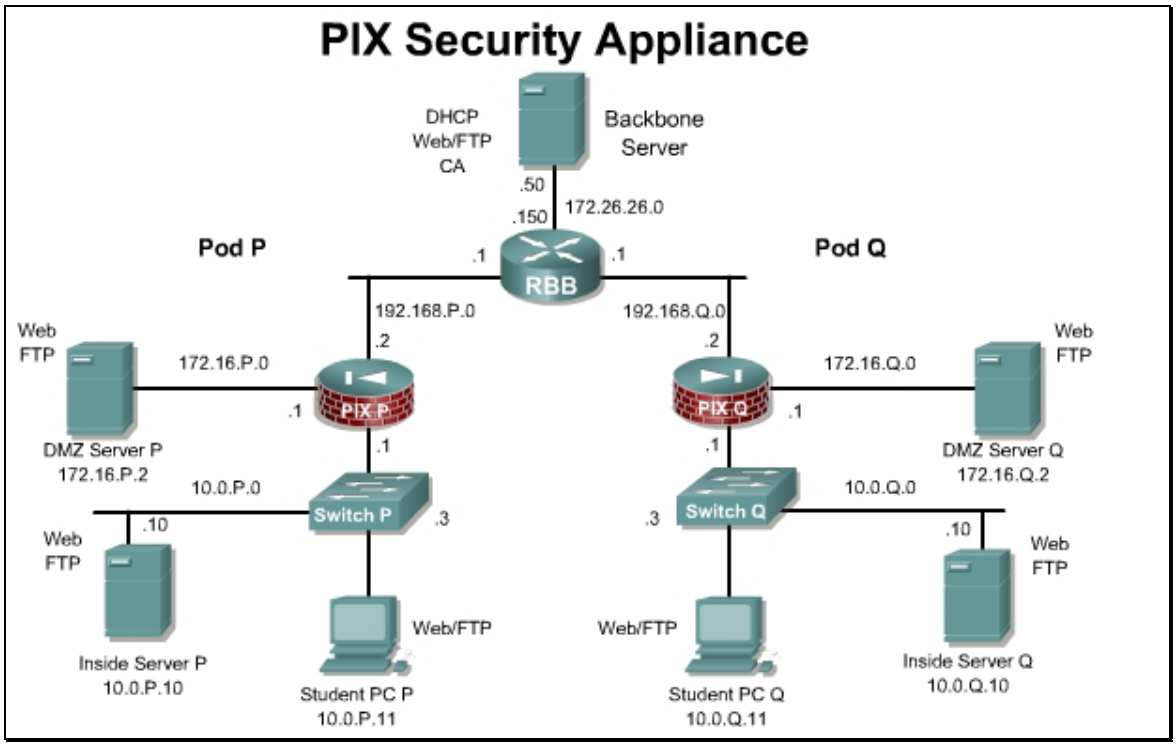
- Configure IKE and IPSec parameters using the ASDM VPN Wizard
- Test and verify IPSec configuration.

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:

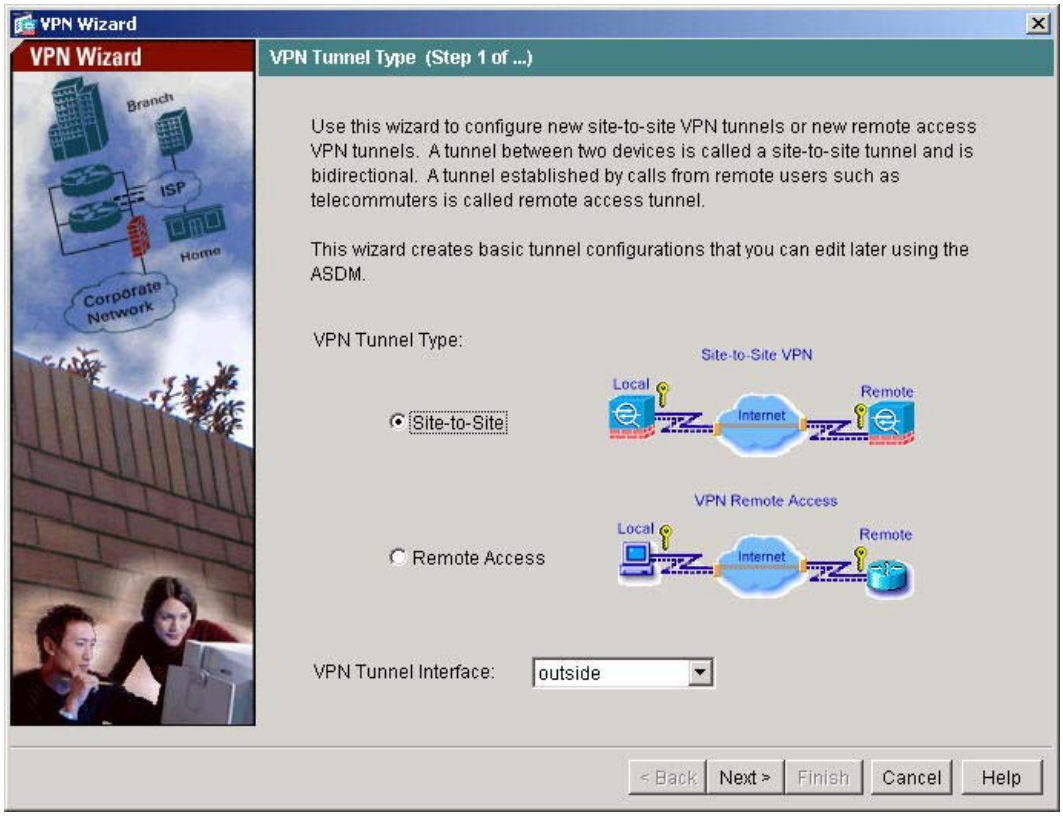
http://www.cisco.com/go/ASDM

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:

a. Initiate an ASDM session with the PIX Security Appliance.

b. Choose **Wizards>VPN Wizard** from the main menu. The VPN Wizard window opens.



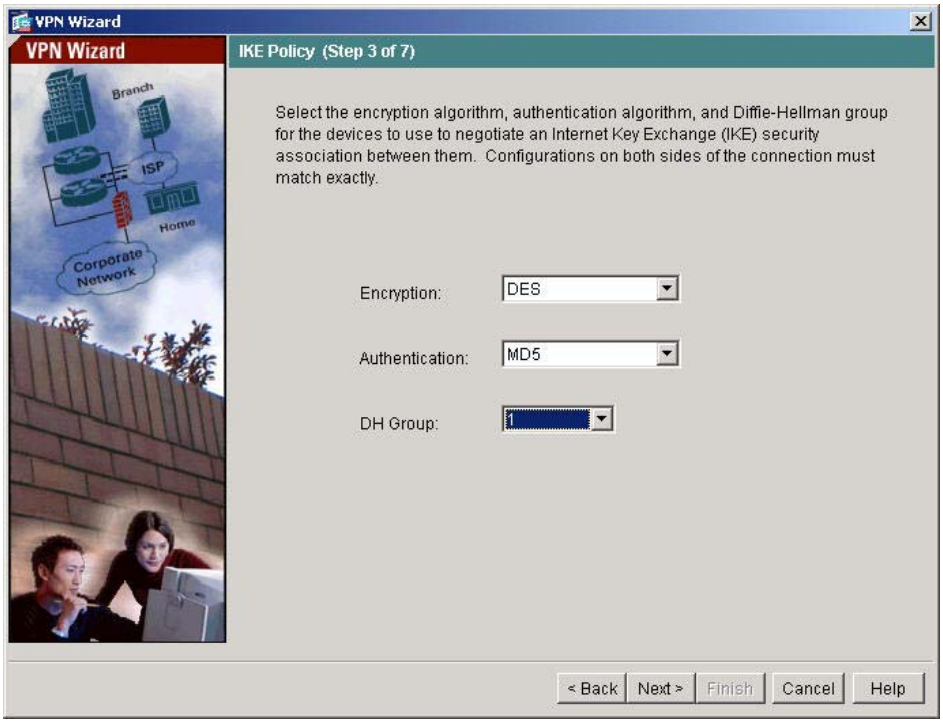
c. Verify that the **Site-to-Site VPN** radio button is selected. Verify that the **outside** interface is chosen from the drop-down box.

d. 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.

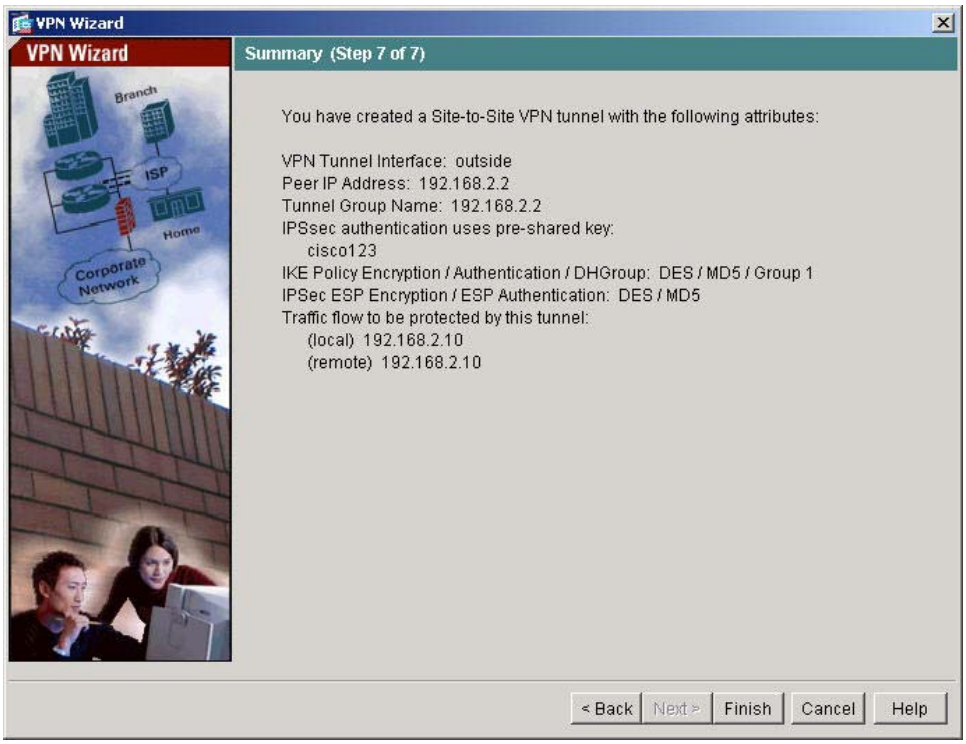
f. Enter **cisco123** in the Pre-shared Key field.

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 widow 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.

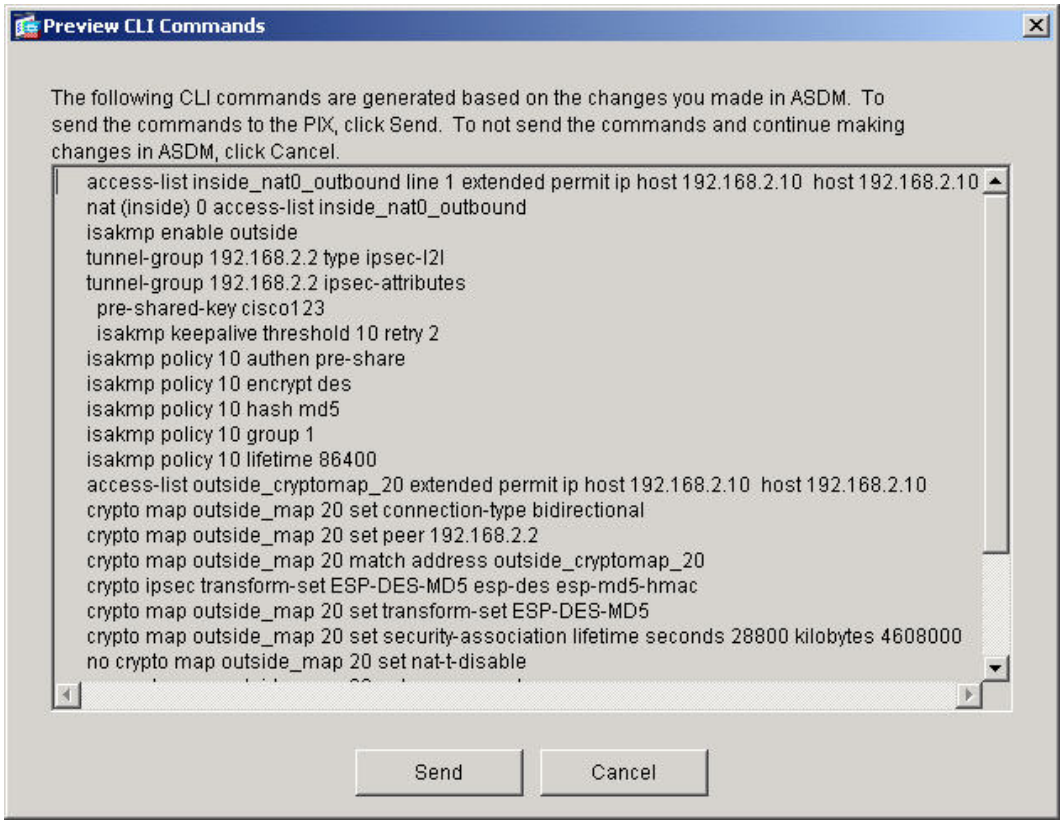
n. Verify that **outside** is chosen in the Interface drop-down menu. Enter the statically mapped IP address of the peer's inside host, **192.168.Q.10,** in the IP Address field. Choose **255.255.255.255** from the Mask drop-down menu. Click the **Add >>** button to move the address to the Selected Hosts/Networks 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.

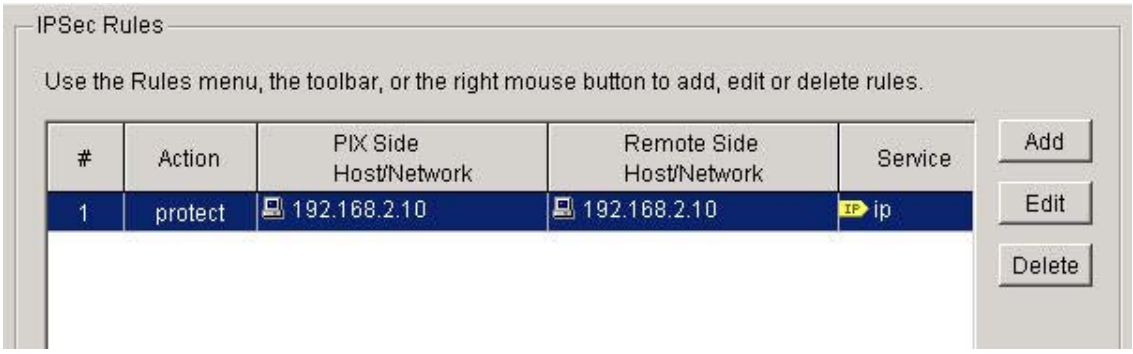
Step 2 Verify the VPN Configuration

To verify the VPN configuration, complete the following steps:

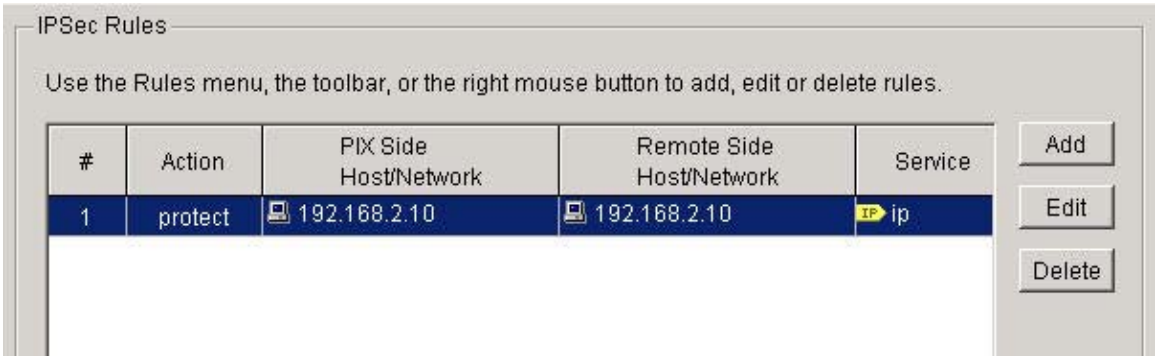
a. Click on the **Configuration** button at the top of the ASDM interface.

b. Click on the **VPN** in the **Features** panel.

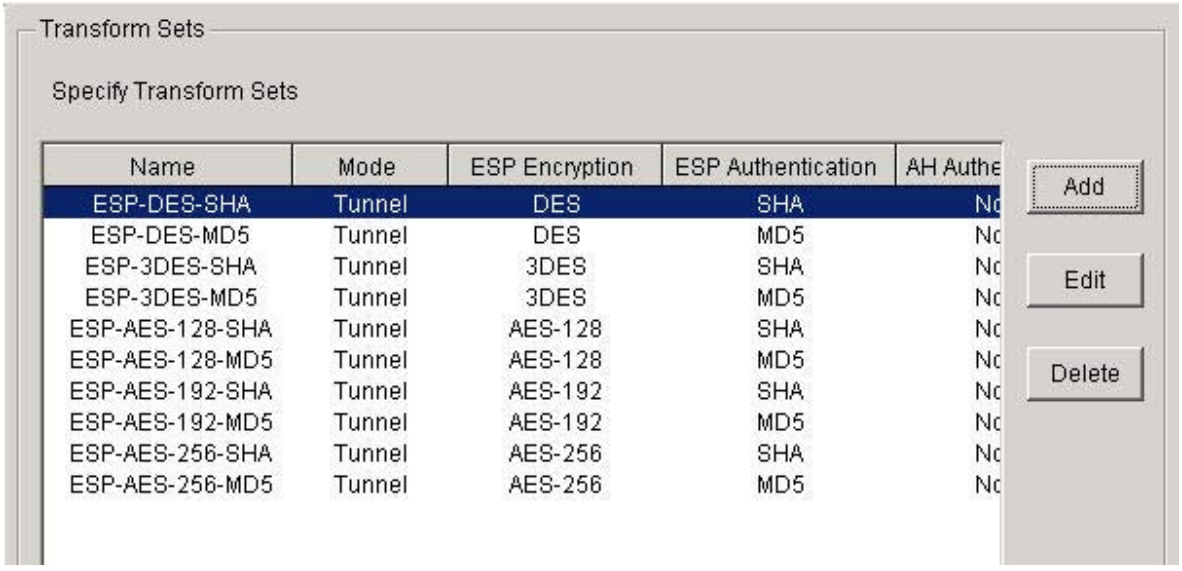
c. Click on **IPsec>IPSec Rules** in the tree menu to view the IPSec Rule configuration.



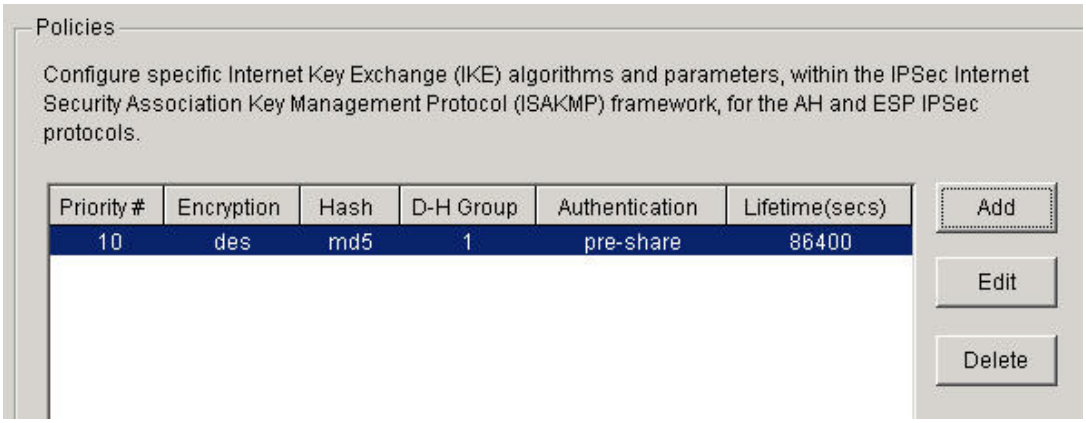
d. Click on **IPsec>Tunnel Policy** in the tree menu to view the Tunnel Policy configuration.



e. 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.



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:

a. Open a web browser on the student PC.

b. 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)

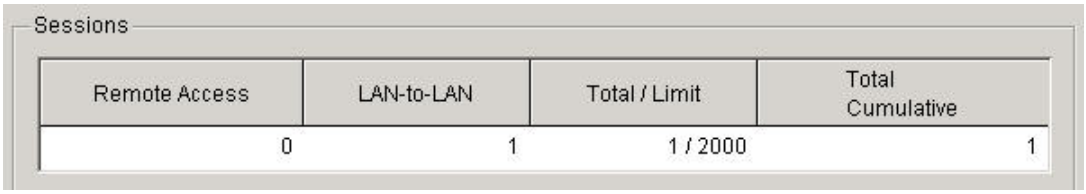
c. Use the web browser to access the peer's inside host by entering

http://192.168.Q.10

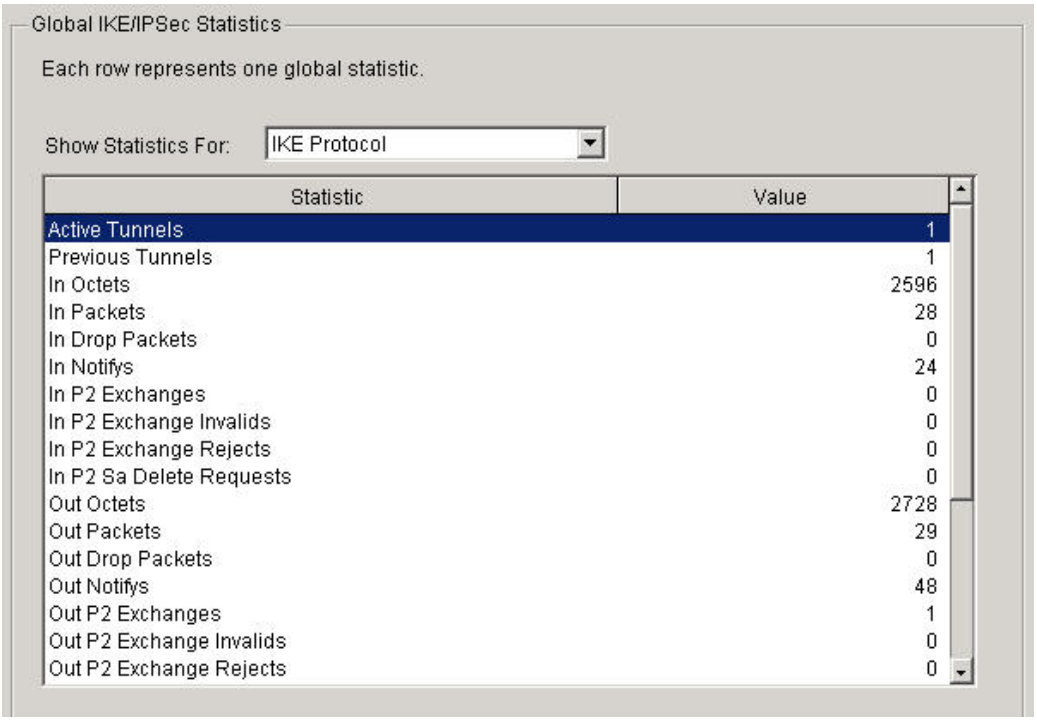
The home page of the peer's inside host should open in the web browser.

d. Click on the **Monitoring** button at the top of the ASDM interface.

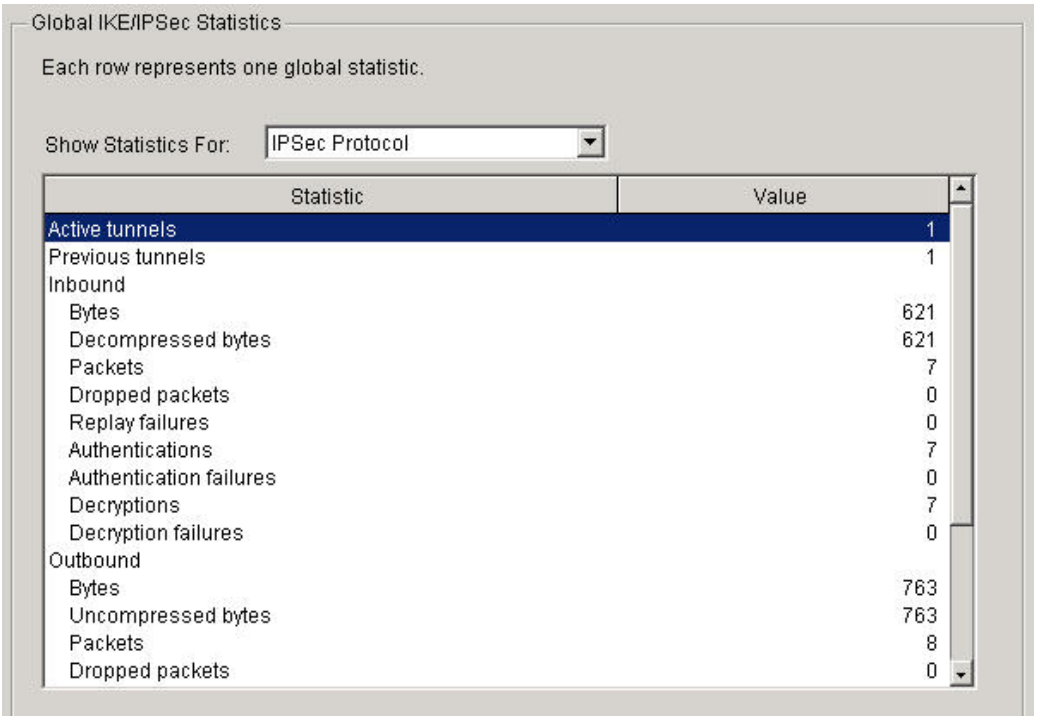
e. Navigate to **VPN Statistics>Sessions** in the tree menu.



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:



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



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.

Lab 5.2.6 Configure a Cisco Router for IPSec using Digital Certificates

Objective

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

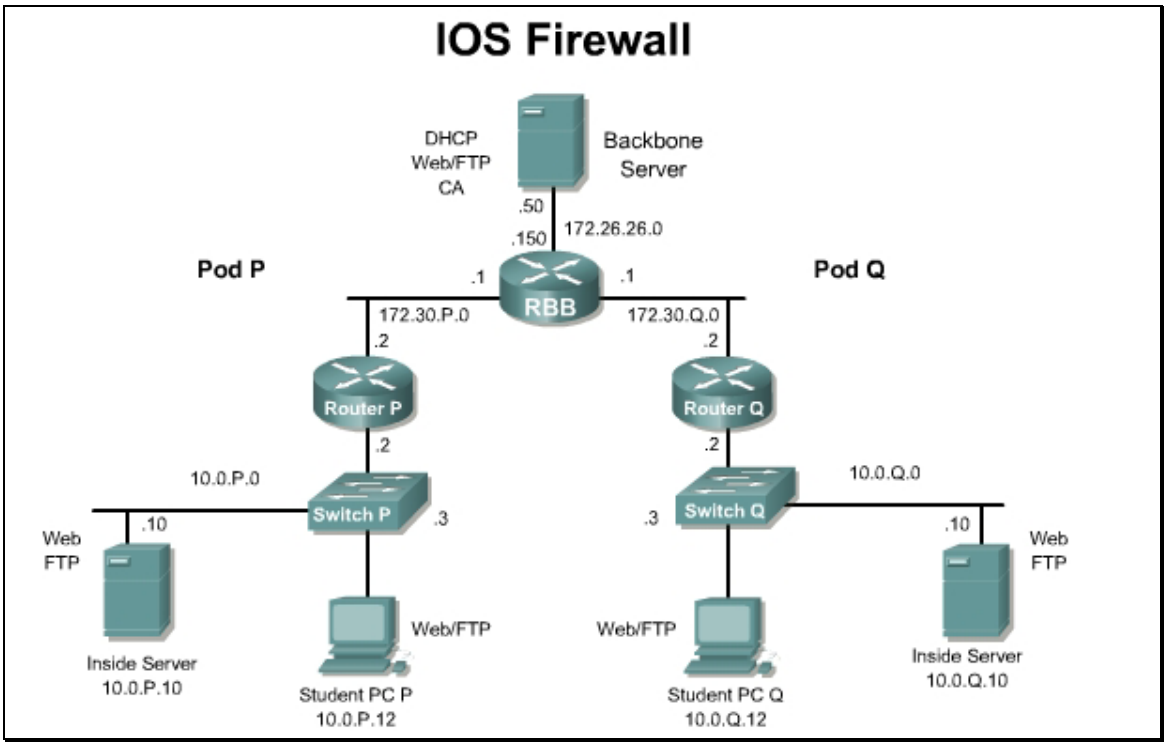
- Prepare for Internet Key Exchange (IKE) and IPSec configure certificate support
- Configure certificate support
- Configure IKE and IPSec
- Test and verify IPSec

Scenario

The XYZ Company has purchased Cisco routers and wants to create a secure Virtual Private Network (VPN) over the Internet between two sites. The company wants to configure a secure VPN gateway using IPSec between two Cisco routers using a certificate authority (CA) server.

Topology

This figure illustrates the lab network environment.



Preparation

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

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

- Standard IOS Firewall lab topology
- Console cable
- HyperTerminal
- Certificate Authority Server on the Backbone Server

Additional materials

Further information about the objectives covered in this lab can be found at:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca7b2.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`	Sets IKE authentication method.
`crl optional`	Specifies that the router can still accept other peers certificates if the CRL is not accessible.
`crypto ca authenticate labca`	Authenticates the CA server. Verifies the fingerprint of the CA server with the CA administrator.
`crypto ca enroll labca`	Enrolls to the CA server.
`crypto ca trustpoint`	Creates a name for the CA.
`crypto isakmp ?`	Displays crypto ISAKMP options.
`crypto isakmp enable`	Enables IKE on the router.
`crypto isakmp policy`	Used to create IKE policy.
`crypto isakmp trustpoint address`	Sets isakmp trustpoint to address.
`crypto key generate rsa usage-keys`	Generates RSA usage-keys.
`encryption`	Sets IKE encryption method.
`enrollment url http://vpnca`	Specifies the URL of the CA.

Command	Description
group	Sets Diffie-Hellman group number.
hash	Sets hash algorithm.
ip domain-name cisco.com	Defines the router domain name.
ip host	Defines the CA server's static hostname-to-IP address mapping.
lifetime	Sets lifetime in seconds and KB.
show crypto ca certificate	Shows the CA certificates.

Step 1 Prepare for IKE and IPSec

Complete the following steps to prepare for 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 IKE policy is to use Rivest, Shamir, and Adleman (RSA) signature keys.
- The IPSec policy is to use Encapsulating Security Payload (ESP) mode with Data Encryption Standard (DES) encryption.
- The IPSec policy is to encrypt all traffic between perimeter routers.

b. Set the router time zone, calendar, and time. Make sure to coordinate the time with the instructor who will set the time on the CA server. A time mismatch between the router and CA server will create invalid certificates and IPSec negotiation will fail during the main mode exchange of isakmp.

Note The easiest way to ensure proper time is to set all devices to (GMT 0) time zone. Make sure the certificates on the Backbone server are valid and display as OK. This is accessible in the Certificate Authority administration application.

```
RouterP(config)#clock timezone zone hours [minutes]
RouterP#clock set hh:mm:ss day month year
```

c. Verify connectivity with the peer router:

```
RouterP>ping 172.30.Q.2
```

(where Q = peer pod number)

d. Ensure connectivity to the CA server from the pod router:

```
RouterP#ping 172.26.26.50
```

e. Establish an HTTP session to the CA server. Test this capability from the student PC by opening a web browser and entering the following URL:

http://172.26.26.50/certsrv

f. Turn on console logging to see the debug output:

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


Logging messages should appear on the console by default, but if they do not appear this feature can be turned on with the **terminal monitor** command.

```
RouterP#terminal monitor
```

Step 2 Configure CA Support

Complete the following steps to configure CA support on the Cisco router. Make sure to work with the CA server administrator to complete this portion of the lab exercise.

a. Define the router domain name:

```
RouterP(config)#ip domain-name cisco.com
```

b. Define the CA server static hostname-to-IP address mapping:

```
RouterP(config)#ip host vpnca 172.26.26.50
```

c. Generate RSA usage-keys:

```
RouterP(config)#crypto key generate rsa usage-keys
```

Note Follow the router prompts to complete the task. Use 512 for the number of bits for the modulus.

d. Perform the following substeps to configure the CA server trustpoint:

i. Create a name for the CA and enter ca-trustpoint mode:

```
RouterP(config)#crypto ca trustpoint vpnca
```

ii. Choose the registration authority mode:

```
RouterP(ca-trustpoint)#enrollment mode ra
```

iii. Specify the URL of the CA:

- For a Microsoft CA:

```
RouterP(ca-trustpoint)#enrollment url
http://vpnca/certsrv/mscep/mscep.dll
```

Note Make sure this is spelled exactly.

iv. Specify that the router can still accept other peers certificates if the certificate revocation list (CRL) is not accessible:

```
RouterP(ca-trustpoint)#crl optional
```

v. Exit CA configuration mode by pressing Control+Z and save the configuration:

```
RouterP(ca-trustpoint)#^Z
RouterP#copy running-config startup-config
```

vi. Turn on PKI debugging to observe debug messages for the CA process:

```
RouterP#debug crypto pki messages
RouterP#debug crypto pki transactions
```

vii. Authenticate the CA server. Verify the fingerprint of the CA server with the CA administrator:

```
RouterP#configure terminal
RouterP(config)#crypto ca authenticate vpnca
Certificate has the following attributes:
Fingerprint: 527D8DCA 4D52A047 C8DA1DAD D5368629
```



```
% Do you accept this certificate? [yes/no]: y
```

Note Because debug is on, several full screen messages flash by, which may require the student to press **Enter** to see this question.

viii. Enroll to the CA server. Ensure that the CA administrator accepts the enrollment request. Answer the prompts as shown in the example.

WARNING *Stop and ensure the instructor is ready to accept the enrollment request before continuing to the next step.*

```
RouterP(config)#crypto ca enroll vpnca
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide
this
   password to the CA Administrator in order to revoke your
certificate.
   For security reasons your password will not be saved in the
configuration.
   Please make a note of it.
Password: cisco
Re-enter password: cisco

% The subject name in the certificate will be: r1.cisco.com
% Include the router serial number in the subject name? [yes/no]: n
% Include an IP address in the subject name? [yes/no]: n
Request certificate from CA? [yes/no]: y
% Certificate request sent to Certificate Authority
% The certificate request fingerprint will be displayed.
% The 'show crypto ca certificate' command will also show the
fingerprint.
```

ix. Verify the CA certificates:

```
RouterP(config)#exit
RouterP#copy running-config startup-config
RouterP#show crypto ca certificate
```

Step 3 Configure IKE

Complete the following steps to configure IKE on the Cisco router. Make sure to work with the members of the peer pod to complete this section of the lab.

Note While entering commands, notice when the command line prompt changes. This helps distinguish what configuration mode is active.

a. Enable IKE/ISAKMP on the router:

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

b. Create an IKE policy to use RSA signatures by completing the following substeps:

i. Set the policy priority:

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

ii. Set authentication to use RSA signatures:

```
RouterP(config-isakmp)#authentication rsa-sig
```

iii. Set the IKE encryption:

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

1. What other encryption choice can be used?

_____

Answer: 3DES

iv. Set the Diffie-Hellman group:

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

2. What would be the benefit of using Diffie-Hellman Group 2?

_____

Answer: Stronger key since it uses 1024 bits

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 config-isakmp mode:

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

Step 4 Configure IPSec

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

a. Configure transform sets and security association parameters

Complete the following steps to configure transform sets and security association (SA) parameters:

b. View the available crypto IPSec command options:

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

c. Check the transform set options:

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

d. 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
```

e. Set the mode to tunnel:

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


f. Exit configuration mode by pressing Control+Z:

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

g. Check the configuration:

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

h. Configure crypto access lists

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

- Traffic permitted = **all**
- Peer address = **Peer router outside interface**
- Access list number = **102**
- Protocol = **IP**

i. Ensure that configuration mode is enabled:

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

j. Configure the access list:

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

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

k. Configure crypto maps

Complete 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**

l. 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
```

m. Specify the extended access list to use with this map:

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

n. Specify the transform set defined earlier:

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

o. Assign the VPN peer using the hostname or IP address of the peer:

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

p. Exit crypto-map configuration mode:

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

q. Apply the crypto map to an interface

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

- Interface to configure = **FastEthernet0/1**
- Crypto map to use = **mymap**

r. Access the interface configuration mode:

```
RouterP(config)#interface FastEthernet0/1
```

s. Assign the crypto map to the interface:

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

t. Exit configuration crypto mode by pressing Contol+Z:

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

Step 5 Test and Verify IPSec

Complete the following steps to verify and test the IPSec configuration. Coordinate 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:  Rivest-Shamir-Adelman Signature
        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-Adelman 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, }
            Interfaces using crypto map mymap:
                  FastEthernet0/1
```

d. Display the current state of the IPSec SAs. The IPSec SAs may have already been established by routing traffic.

```
RouterP#show crypto ipsec sa
interface: FastEthernet0/1
    Crypto map tag: mymap, local addr. 172.30.1.2


   local  ident (addr/mask/prot/port):
(172.30.1.2/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port):
(172.30.2.2/255.255.255.255/0/0)
   current_peer: 172.30.2.2
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 21, #pkts encrypt: 21, #pkts digest 0
    #pkts decaps: 21, #pkts decrypt: 21, #pkts verify 0
    #send errors 0, #recv errors 0


local crypto endpt.: 172.30.1.2, remote crypto endpt.: 172.30.2.2
     path mtu 1500, media mtu 1500
     current outbound spi: 8AE1C9C


     inbound esp sas:
      spi: 0x1B781456(460854358)
        transform: esp-des ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 17, crypto map: mymap
        sa timing: remaining key lifetime (k/sec): (4607997/3107)
        IV size: 8 bytes
        replay detection support: N


     inbound ah sas:


     outbound esp sas:
      spi: 0x8AE1C9C(145628316)
        transform: esp-des ,
        in use settings ={Tunnel, }
```



```
        slot: 0, conn id: 18, crypto map: mymap
        sa timing: remaining key lifetime (k/sec): (4607997/3107)
        IV size: 8 bytes
        replay detection support: N

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

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

i. Verify 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
172.30.1.2     172.30.2.2     QM_IDLE           1      0
```

The sample output below will indicate if there is a misconfiguration with isakmp. This could also indicate a problem with certificate validity on either router. The MM Exchange indicates the router cannot go beyond the main mode exchange of isakmp. This problem will also be indicated by a continuous looping of debug output of isakmp exchange messages.

```
dst           src          state          conn-id   slot
172.30.1.2    172.30.2.2   MM Exchange        1      0
RouterP#show crypto ipsec sa
interface: FastEthernet0/1
    Crypto map tag: mymap, local addr. 172.30.1.2


   local  ident (addr/mask/prot/port):
(172.30.1.2/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port):
(172.30.2.2/255.255.255.255/0/0)
   current_peer: 172.30.2.2
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 26, #pkts encrypt: 26, #pkts digest 0
    #pkts decaps: 26, #pkts decrypt: 26, #pkts verify 0
    #send errors 0, #recv errors 0


local crypto endpt.: 172.30.1.2, remote crypto endpt.: 172.30.2.2
     path mtu 1500, media mtu 1500
```



```
    current outbound spi: 8AE1C9C

    inbound esp sas:
     spi: 0x1B781456(460854358)
       transform: esp-des ,
       in use settings ={Tunnel, }
       slot: 0, conn id: 17, crypto map: mymap
       sa timing: remaining key lifetime (k/sec): (4607996/2963)
       IV size: 8 bytes
       replay detection support: N

     inbound ah sas:

    outbound esp sas:
     spi: 0x8AE1C9C(145628316)
       transform: esp-des ,
       in use settings ={Tunnel, }
       slot: 0, conn id: 18, crypto map: mymap
       sa timing: remaining key lifetime (k/sec): (4607996/2963)
       IV size: 8 bytes
       replay detection support: N

    outbound ah sas:
```

j. Ensure that encryption is working between the routers by first generating additional traffic, and then by observing 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. 172.30.1.2


   local  ident (addr/mask/prot/port):
(172.30.1.2/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port):
(172.30.2.2/255.255.255.255/0/0)
   current_peer: 172.30.2.2:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 31, #pkts encrypt: 31, #pkts digest 0
    #pkts decaps: 31, #pkts decrypt: 31, #pkts verify 0
    #send errors 0, #recv errors 0
```



```
     local crypto endpt.: 172.30.1.2, remote crypto endpt.:
172.30.2.2
     path mtu 1500, media mtu 1500
     current outbound spi: 8AE1C9C

     inbound esp sas:
      spi: 0x1B781456(460854358)
        transform: esp-des ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 17, crypto map: mymap
        sa timing: remaining key lifetime (k/sec): (4607995/2954)
        IV size: 8 bytes
        replay detection support: N

     inbound ah sas:

     outbound esp sas:
      spi: 0x8AE1C9C(145628316)
        transform: esp-des ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 18, crypto map: mymap
        sa timing: remaining key lifetime (k/sec): (4607996/2954)
        IV size: 8 bytes
        replay detection support: N

     outbound ah sas:
```

Step 6 Fine Tuning the ACL

Fine-tune the crypto access lists used to determine interesting traffic to encrypt traffic only between the internal student PCs. Remember to work with the peer pod group to make the access lists symmetrical between the perimeter routers. Ensure that desired traffic is encrypted between the peers.

a. Remove the previously configured access list:

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

b. Configure a new access list for the Windows 2000 servers:

```
RouterP(config)#access-list 102 permit ip host 10.0.P.12 host
10.0.Q.12
```

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

c. Verify the configuration by connecting to the web server at 10.0.Q.12 using the browser on the Student PC.

(where Q = peer pod number)

Lab 5.3.2 Configure a PIX Security Appliance Site-to-Site IPSec VPN Tunnel with CA support

Objectives

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

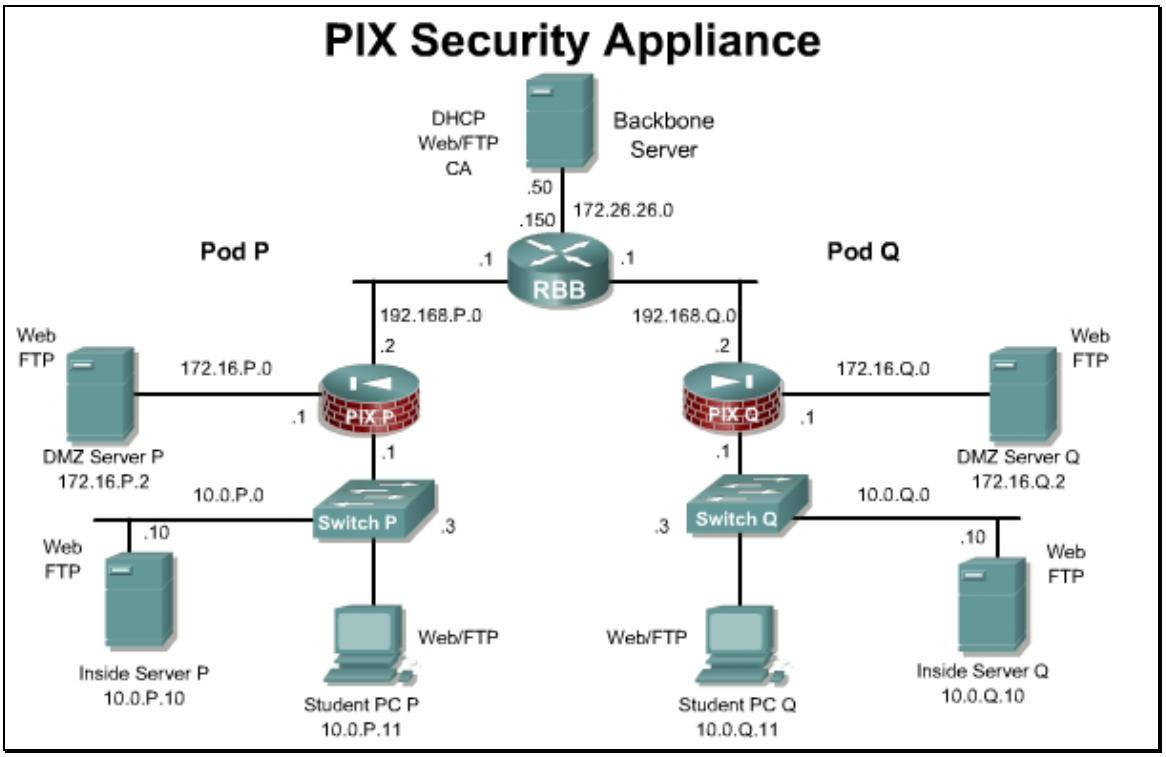
- Prepare for Configuring CA Support
- Configure CA Support
- Configure and Verify IKE and IPSec Parameters
- Verify the VPN connection
- Verify the VPN status and configuration using ASDM

Scenario

A savings and loan bank needs to setup a remote site, but there are concerns about security. It is decided that a site-to-site VPN using digital certificates will provide additional security beyond pre-shared keys.

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
- CA server installed at the backbone Web Server

Additional Materials

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

http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_configuration_guide_book09186a00803d8a02.html

http://www.cisco.com/en/US/products/ps6120/products_configuration_guide_chapter09186a008045247b.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
crypto ipsec *map-name seq-num* **transform-set** *transform-set-name transform1* **[***transform2***]**	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 *map-name seq-num* **match address** *acl_name*	To assign an access list to a crypto map entry, use the **crypto map match address** command in global configuration mode.
crypto map *map-name seq-num* **set peer {***ip_address* **|** *hostname***}{...***ip_address* **|** *hostname10***}**	To specify an IPSec peer in a crypto map entry, use the **crypto map set peer** command in global configuration mode.
crypto map *map-name seq-num set* **transform-set** *transform-set-name1* **[…** *transform-set-name9***]**	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 *map-name* **interface** *interface-name*	Use the **crypto map interface** command in global configuration mode to apply a previously defined crypto map set to an interface.
isakmp enable *interface-name*	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 policy *priority* **authentication {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.
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

Command	Description
	the traffic.
tunnel-group *name* **type** *type*	To create and manage the database of connection-specific records for IPSec, use the **tunnel-group** command in global configuration mode.
tunnel-group *name* **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 Prepare for Configuring CA Support

Perform the following steps to prepare for the IPSec configuration:

a. See if any certificates or keys exist in memory.

```
PixP(config)# show crypto ca certificates

      Certificate
        Status: Available
        Certificate Serial Number: 4848f171000000000013
        Certificate Usage: General Purpose
        Public Key Type: RSA (1024 bits)
PixP(config)# show crypto key mypubkey rsa

Key pair was generated at: 10:12:30 UTC Jun 1 2005

Key name: <Default-RSA-Key>

 Usage: General Purpose Key

 Modulus Size (bits): 1024

 Key Data:

  30819f30 0d06092a 864886f7 0d010101 05000381 8d003081 89028181 0097f601

  899a756d b4361019 71588eeb ccec6af7 9c69e9d8 96115cab f207c1e7 4974bfc7

  c848ba18 0d96b0f5 ef73d5dc a8ec8ec4 8abd2172 cdd63695 d684e4de f29ccde2

  6c3e4f8e 7bacbfab 30b012cb 7ae9a987 6b6bfbfe e69f6e40 c013a137 9e74f36f

  13dd0af9 9e578af3 3a5c2643 4f8cb1cf 08f47903 c6419ca7 a6c82ed3 35020301 0001
```

b. Delete any existing RSA keys and certificates.

```
PixP(config)# crypto key zeroize rsa
WARNING: All device certs issued using these keys will also be
removed.
Do you really want to remove these keys? [yes/no]:yes
PixP(config)# clear configure crypto ca trustpoint
WARNING: Removing an enrolled trustpoint will destroy all
certificates received from the related Certificate Authority.
Are you sure you want to do this? [yes/no]:yes
```



```
INFO: Be sure to ask the CA administrator to revoke your
certificates.
```

c. Reboot the PIX Security Appliance.

```
PixP(config)# reload
```

d. Verify the certificate is deleted

```
PixP(config)# show crypto ca certificates
PixP(config)# show crypto key mypubkey rsa
```

e. Verify that a static translation is configured from a global IP address on the outside interface to the internal Windows NT server.

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

f. Verify that an ACL permitting web access to the Student PC 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)
```

g. Ensure a web connection can be established between Student PC pods.

h. Verify connectivity to the peer PIX Security Appliance.

```
PixP(config)# ping 192.168.Q.2
```

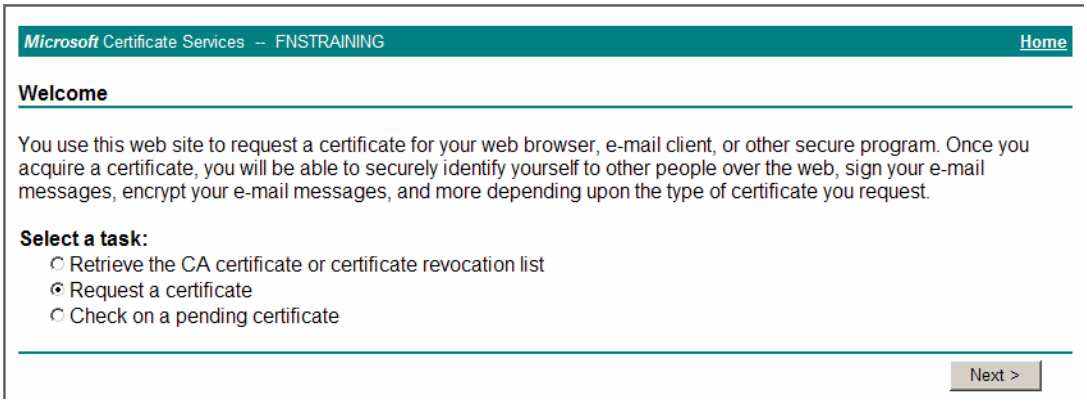
(where Q = peer pod number)

i. Ensure connectivity to the CA server from the PIX Security Appliance.

```
PixP(config)# ping 172.26.26.50
```

j. Ensure that an HTTP session can be established to the CA server. Test this capability from the Student PC by opening a web browser and entering following the location:

http://172.26.26.50/certsrv



k. Enable the PIX Security Appliance to implicitly permit any packet that came from an IPSec tunnel and bypass the checking with an associated **access-group** command for IPSec connections.

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

Step 2 Configure CA Support

Perform the following steps to configure CA support on the PIX Security Appliance. Work with the CA server administrator to complete this portion of the lab:

a. If needed, configure the PIX Security Appliance's host name

```
PixP(config)# hostname PixP
```

(where P = pod number)

b. Set the time and date.

```
PixP(config)# clock set <set to current GMT time and date>
```

Check with the instructor for time and date settings.

c. If needed, define the domain name of the PIX Security Appliance.

```
PixP(config)# domain-name cisco.com
```

d. Generate a general purpose RSA key pair with the 512 bit modulus.

```
PixP(config)# crypto key generate rsa modulus 512
INFO: The name for the keys will be: <Default-RSA-Key>
Keypair generation process begin. Please wait...
PixP(config)#
```

1. What other type of RSA key pair can be generated for CA support?

_____

Answer: DSA key pair

e. View the generated RSA key.

```
PixP(config)# show crypto key mypubkey rsa
Key pair was generated at: 15:25:21 UTC Jun 3 2005
Key name: <Default-RSA-Key>
 Usage: General Purpose Key
 Modulus Size (bits): 512
 Key Data:
```



```
305c300d 06092a86 4886f70d 01010105 00034b00 30480241 00d5b285
bb9f0231 96ba8deb 9e1b607e d89e36fb 62c6836b 8b79592d cc1fc7c9
7fadb895 0e6be092 23e37037 1d8e7bcb b5f39259 b4868c9e 6941f2d2
f36bf8e5 f1020301 0001
```

f. Enter the Crypto ca trustpoint configuration mode.

```
PixP(config)# crypto ca trustpoint LABCA
PixP(config-ca-trustpoint)#
```

g. Configure the CA enrollment URL. For a Microsoft CA use the following command:

```
PixP(config-ca-trustpoint)# enrollment url
http://172.26.26.50:/certsrv/mscep/mscep.dll
```

h. Configure the communication parameters between the PIX Security Appliance and the CA to use a retry period of one minute, a retry count of 20, and indicate that a CRL check is optional.

```
PixP(config-ca-trustpoint)# enrollment retry period 1
PixP(config-ca-trustpoint)# enrollment retry count 20
PixP(config-ca-trustpoint)# crl optional
```

i. Exit Crypto ca trustpoint configuration mode.

```
PixP(config-ca-trustpoint)# exit
```

j. Turn on PKI debugging and observe debug messages for the CA process.

```
PixP(config)# debug crypto ca
```

k. Authenticate the CA by obtaining its public key and its certificate. When prompted to accept the certificate, enter **y**.

```
PixP(config)# crypto ca authenticate LABCA
Crypto CA thread wakes up!


CRYPTO_PKI: Sending CA Certificate Request:
GET
/certsrv/mscep/mscep.dll/pkiclient.exe?operation=GetCACert&message=L
ABCA HTTP/1.0
CRYPTO_PKI: http connection opened
Crypto CA thread sleeps!
INFO: Certificate has the following attributes:
Fingerprint:     38f2bfed 0d596232 45902b3e 236e4060
Do you accept this certificate? [yes/no]: y
Trustpoint CA ce
CRYPTO_PKI: Cert record not found, returning E_NOT_FOUND
Current Certificate list contents:
Certificate 1:
  SERIAL: 2926da616d2cf9a54fa27d84dc40be78
  ISSUER: cn=FNSTRAINING,ou=CNAP,o=Cisco,l=Phoenix,st=AZ,c=US
CRYPTO_PKI: crypto_process_ra_certs(trust_point=LABCA)rtificate
accepted.
```


l. Request signed certificates from the CA Server for the PIX Security Appliance's RSA key pair. Before entering this command, contact the CA Server administrator (instructor) to authenticate the PIX Security Appliance manually and grant its certificate.

```
PixP(config)# crypto ca enroll LABCA
```

Use the responses shown in the example below when prompted during the enrollment process.

Note The password **passwordcisco** in the example is a password, which is not saved with the configuration. The password is required in a production environment in the event the certificate needs to be revoked, so it is crucial that the password is recorded.

```
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide
this password to the CA Administrator in order to revoke your
certificate.
For security reasons your password will not be saved in the
configuration.
   Please make a note of it.
Password: passwordcisco
Re-enter password: passwordcisco
% The fully-qualified domain name in the certificate will be:
Pix1.cisco.com
% Include the device serial number in the subject name? [yes/no]: n
Request certificate from CA? [yes/no]: y
                                        Crypto CA thread wakes up!
CRYPTO_PKI: Sending CA Certificate Request:
GET
/certsrv/mscep/mscep.dll/pkiclient.exe?operation=GetCACert&message=L
ABCA HTTP/1.0
CRYPTO_PKI: http connection opened
% Certificate request sent to Certificate Authority
Pix1(config)#
CRYPTO_PKI: Cert record not found, returning E_NOT_FOUND
Current Certificate list contents:
Certificate 1:
  SERIAL: 0aa3f494000000000002
  ISSUER: cn=FNSTRAINING,ou=CNAP,o=Cisco,l=Phoenix,st=AZ,c=US
Certificate 2:
  SERIAL: 2926da616d2cf9a54fa27d84dc40be78
  ISSUER: cn=FNSTRAINING,ou=CNAP,o=Cisco,l=Phoenix,st=AZ,c=US
CRYPTO_PKI: Cert record not found, returning E_NOT_FOUND
Current Certificate list contents:
Certificate 1:
```



```
  SERIAL: 0aa3f4f2000000000003
  ISSUER: cn=FNSTRAINING,ou=CNAP,o=Cisco,l=Phoenix,st=AZ,c=US
Certificate 2:
  SERIAL: 0aa3f494000000000002
  ISSUER: cn=FNSTRAINING,ou=CNAP,o=Cisco,l=Phoenix,st=AZ,c=US
Certificate 3:
  SERIAL: 2926da616d2cf9a54fa27d84dc40be78
  ISSUER: cn=FNSTRAINING,ou=CNAP,o=Cisco,l=Phoenix,st=AZ,c=USCrypto
CA thread sl
eeps!
CRYPTO_PKI: Received enroll message for vcid:  0
CRYPTO_PKI: http connection opened
CRYPTO_PKI:  received msg of 642 bytes
CRYPTO_PKI: status = 102: certificate request pending
CRYPTO_PKI: http connection opened
CRYPTO_PKI:  received msg of 642 bytes
CRYPTO_PKI: status = 102: certificate request pending
```

Note Notify the CA administrator to accept the pending certificate. On the CA Server, the certificate must manually be issued in the Certification Authority if it is not set to automatically issue the certificate.

```
Crypto CA thread wakes up!
Crypto CA thread sleeps!
CRYPTO_PKI: Received enroll message for vcid:  0
CRYPTO_PKI: resend GetCertInitial for session: 0
CRYPTO_PKI: http connection opened
The certificate has been granted by CA!
CRYPTO_PKI:  received msg of 1976 bytes
CRYPTO_PKI: status = 100: certificate is granted
CRYPTO_PKI: Cert record not found, returning E_NOT_FOUND
Current Certificate list contents:
Certificate 1:
  SERIAL: 4848f171000000000013
  ISSUER: cn=FNSTRAINING,ou=CNAP,o=Cisco,l=Phoenix,st=AZ,c=US
Certificate 2:
  SERIAL: 0aa3f4f2000000000003
  ISSUER: cn=FNSTRAINING,ou=CNAP,o=Cisco,l=Phoenix,st=AZ,c=US
Certificate 3:
  SERIAL: 0aa3f494000000000002
  ISSUER: cn=FNSTRAINING,ou=CNAP,o=Cisco,l=Phoenix,st=AZ,c=US
```



```
Certificate 4:

  SERIAL: 2926da616d2cf9a54fa27d84dc40be78

  ISSUER:
cn=FNSTRAINING,ou=CNAP,o=Cisco,l=Phoenix,st=AZ,c=USCRYPTO_PKI: All
enrollment requests completed.

CRYPTO_PKI: All enrollment requests completed.

CRYPTO_PKI: All enrollment requests completed.


CRYPTO_PKI:remove_superceded_certs(LABCA)CRYPTO_PKI: All enrollment
requests completed.

CRYPTO_PKI: status = 100: certificate is granted

CRYPTO_PKI: All enrollment requests completed.

CRYPTO_PKI: All enrollment requests completed.
```

If the PIX Security Appliance reboots after the **crypto ca enroll** command is issued, but before the certificates is received, the **crypto ca enroll** command must be reissued.

m. Verify that the enrollment process was successful. A sample certificate is shown below

```
PixP(config)# show crypto ca certificates

Certificate

  Status: Available

  Certificate Serial Number: 4848f171000000000013

  Certificate Usage: General Purpose

  Public Key Type: RSA (1024 bits)

  Issuer Name:

    cn=FNSTRAINING

    ou=CNAP

    o=Cisco

    l=Phoenix

    st=AZ

    c=US

  Subject Name:

    Name: PixP.cisco.com

    hostname=PixP.cisco.com

  CRL Distribution Points:

    [1]  http://cisco-nik4uglii/CertEnroll/FNSTRAINING.crl

    [2]  file://\\cisco-nik4uglii\CertEnroll\FNSTRAINING.crl

  Validity Date:

    start date: 09:03:15 UTC Jun 3 2005
```



```
    end   date: 09:13:15 UTC Jun 3 2006
    renew date: 00:00:00 UTC Jan 1 1970
  Associated Trustpoints: LABCA


CA Certificate
  Status: Available
  Certificate Serial Number: 2926da616d2cf9a54fa27d84dc40be78
  Certificate Usage: Signature
  Public Key Type: RSA (512 bits)
  Issuer Name:
    cn=FNSTRAINING
    ou=CNAP
    o=Cisco
    l=Phoenix
    st=AZ
    c=US
  Subject Name:
    cn=FNSTRAINING
    ou=CNAP
    o=Cisco
    l=Phoenix
    st=AZ
    c=US
  CRL Distribution Points:
    [1]  http://cisco-nik4uglii/CertEnroll/FNSTRAINING.crl
    [2]  file://\\cisco-nik4uglii\CertEnroll\FNSTRAINING.crl
  Validity Date:
    start date: 12:56:59 UTC Aug 27 2004
    end   date: 13:05:32 UTC Aug 27 2006
  Associated Trustpoints: LABCA
```

n. Save the configuration.

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


Step 3 Configure and Verify IKE Parameters

Perform the following steps to configure IKE to use RSA signatures 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 RSA signatures for authentication:

```
PixP(config)# isakmp policy 10 authentication rsa-sig
```

c. Set the encryption to DES:

```
PixP(config)# isakmp policy 10 encryption des
```

d. Set the hash algorithm to MD5:

```
PixP(config)# isakmp policy 10 encryption des
```

e. Configure the tunnel group type:

```
PixP(config)# tunnel-group 192.168.Q.2 type ipsec-l2l
```

(where Q = peer pod number)

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

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

g. Configure the trustpoint:

```
PixP(config-ipsec)# trust-point LABCA
PixP(config-ipsec)# exit
```

h. View the IKE policy and answer the following questions:

```
PixP(config)# show running-config isakmp
isakmp policy 10 authentication rsa-sig
isakmp policy 10 encryption des
isakmp policy 10 hash md5
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400
```

1. What five policy items are configured in an IKE policy?

   _____

   Answer: There are five parameters which must be defined in each IKE policy. They are encryption algorithm, hash algorithm, authentication method, key exchange, and IKE SA lifetime.

2. Which IKE policy parameter must be modified when digital certificates are used?

   _____

   Answer: The authentication method.

3. How will the PIX Security Appliance know to use the IKE policy suite using RSA signatures instead of the default policy that uses a pre-shared key for authentication?

   _____

Answer: The matching policy with the highest priority is used. Since the peer PIX Security Appliance has a policy matching this one, it will be used instead of the default.

Step 4 Configure and Verify IPSec Parameters

Perform the following steps to configure IPSec on the PIX Security Appliance:

a. Create an access list to select traffic to protect. The access list should protect IP traffic between the student PCs of peer PIX Security Appliances.

```
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. Configure an IPSec transform set, the IKE phase two parameters, to use the **esp-des** and **esp-md5-hmac** transforms. Use a transform-set-name of **ESP-DES-MD5**.

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

c. Create a crypto map entry and assign the access list to the crypto map.

```
PixP(config)# crypto map peerQ 20 match address CRYPTO_ACL
```

(where Q = peer pod number)

d. Define the peer. The peer IP address should be set to the peer's outside interface IP address.

```
PixP(config)# crypto map peerQ 20 set peer 192.168.Q.2
```

(where Q = peer pod number)

e. Specify the transform set used to reach the peer.

```
PixP(config)# crypto map peerQ 20 set transform-set ESP-DES-MD5
```

(where Q = peer pod number)

f. Specify the trustpoint use dto authenticate the peer device.

```
PixP(config)# crypto map peerQ 20 set trustpoint LABCA
```

(where Q = peer pod number)

g. Apply the crypto map set to the outside interface.

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

(where Q = peer pod number)

h. Verify the crypto access list.

```
Pix1(config)# show access-list CRYPTO_ACL
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)
```

i. Verify the correct IPSec parameters for IKE phase two.

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

crypto ipsec transform-set ESP-DES-MD5 esp-des esp-md5-hmac
```

j. Verify the correct crypto map configuration.

```
PixP(config)# show running-config crypto map
crypto map peerQ 20 match address CRYPTO_ACL
crypto map peerQ 20 set peer 192.168.Q.2
crypto map peerQ 20 set transform-set ESP-DES-MD5
```



```
crypto map peerQ 20 set trustpoint LABCA
crypto map peerQ interface outside
```

Step 5 Test the VPN connection

a. Make sure that the peer group has finished Step 4.

b. Turn on debugging for IPSec and ISAKMP.

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

c. Clear any security associations that may have been set up.

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

d. From the Student PC command prompt, ping the peer Student PC. Observe the PIX debug output during the ping and verify the ping is successful in the command prompt.

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

e. Initiate a web session from the Student PC to the peer Student PC. Ensure that traffic between peers is being encrypted by performing the following sub-steps:

i. Examine the IKE SAs Check for the **QM_IDLE** status. This ensures the rsa-sig authentication was successful.

```
pix1(config)# show crypto isakmp sa
Total     : 1
Embryonic : 0
      dst               src        state     pending     created
   192.168.2.2      192.168.1.2    QM_IDLE         0           1
```

ii. Examine the IPSec SAs. Note the number of packets encrypted and decrypted:

```
pix1(config)# show crypto ipsec sa

    Crypto map tag: peerQ, 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: 3, #pkts encrypt: 3, #pkts digest: 3
      #pkts decaps: 3, #pkts decrypt: 3, #pkts verify: 3
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 3, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0
```

iii. Generate additional traffic by clicking on the Reload button of the web browser.

iv. Examine the IPSec SAs again. Note that the packet counters have incremented:

```
pix2(config)# show cry ipsec sa
Crypto map tag: peerQ, 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: 6, #pkts encrypt: 6, #pkts digest: 6
#pkts decaps: 6, #pkts decrypt: 6, #pkts verify: 6
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 6, #pkts comp failed: 0, #pkts decomp failed: 0
#send errors: 0, #recv errors: 0
```

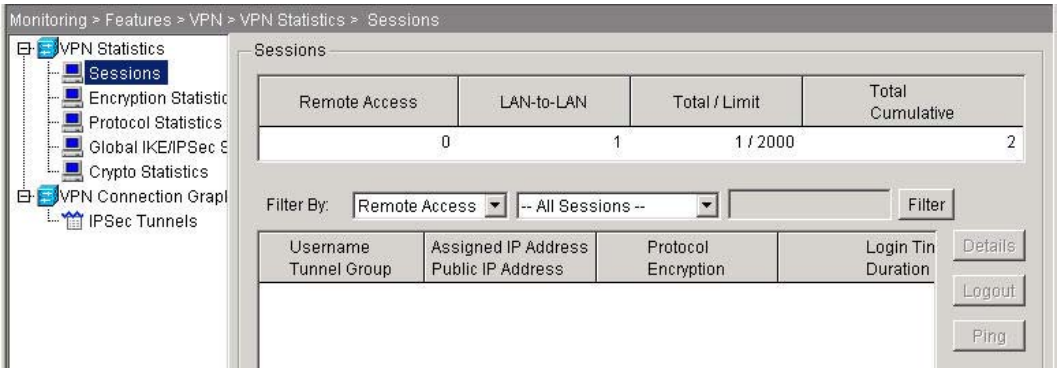
f. Compare the running configuration to the ending configuration for this lab.

Task 6 Verify the VPN Status and Configuration using ASDM

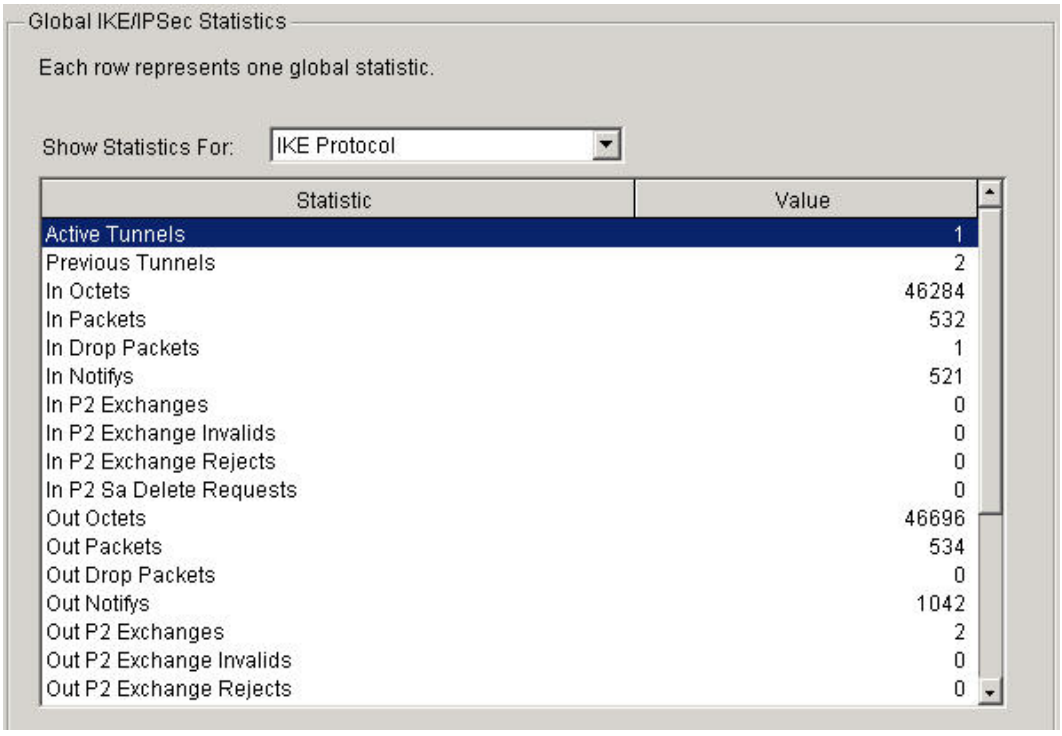
Use ASDM to verify the site-to-site VPN using CA certificates configuration

a. Initiate an ASDM session with the PIX Security Appliance.

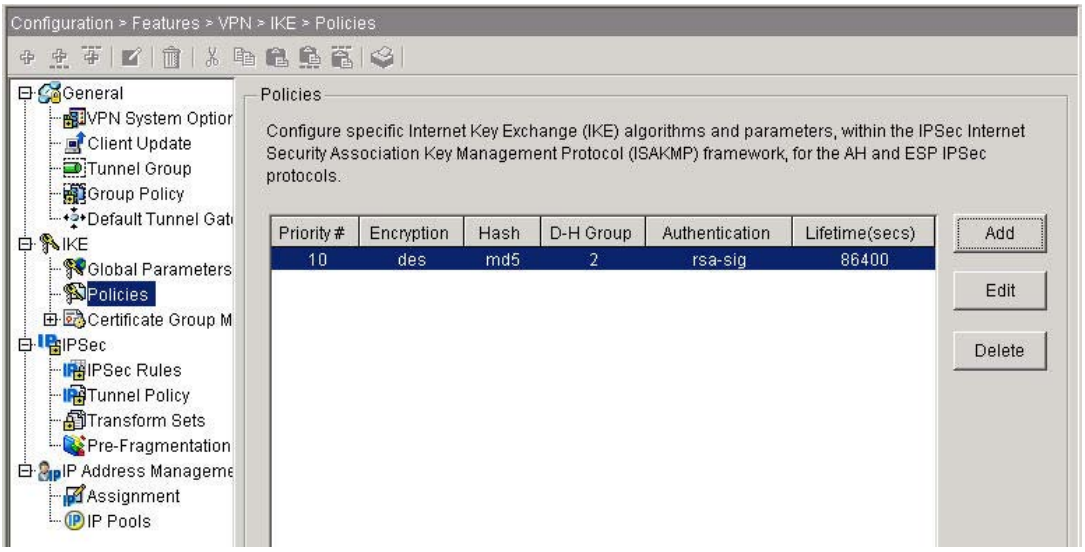
b. Navigate to **Monitoring>Tasks>VPN>VPN Statistics>Sessions**. One LAN-to-LAN connection should be displayed.



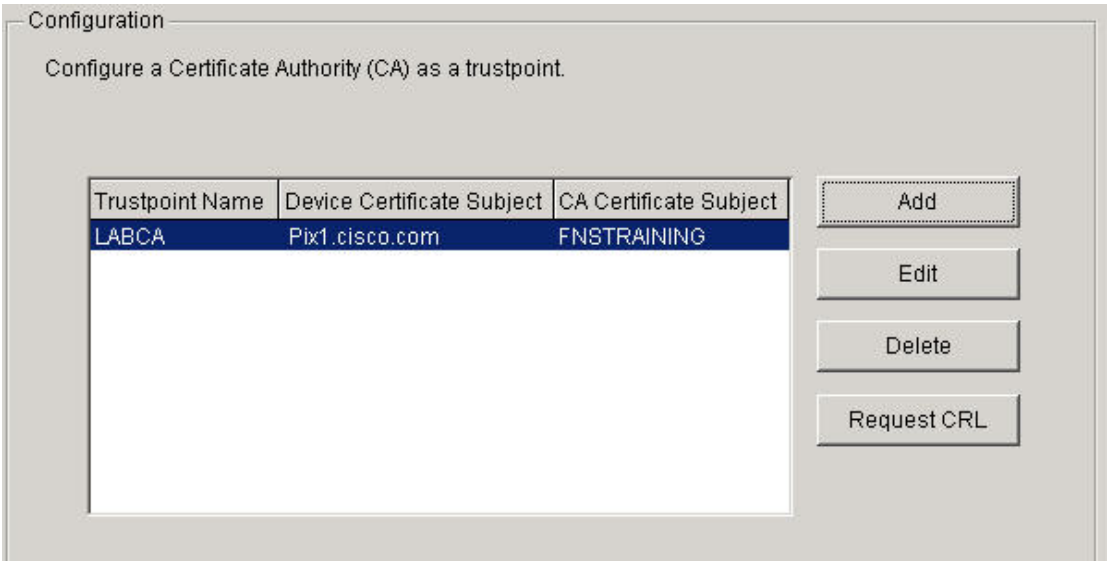
c. Navigate to the **Monitoring>Features>VPN>VPN Statistics>Global IKE/IPSec Statistics** to view the IKE and IPSec statistics.



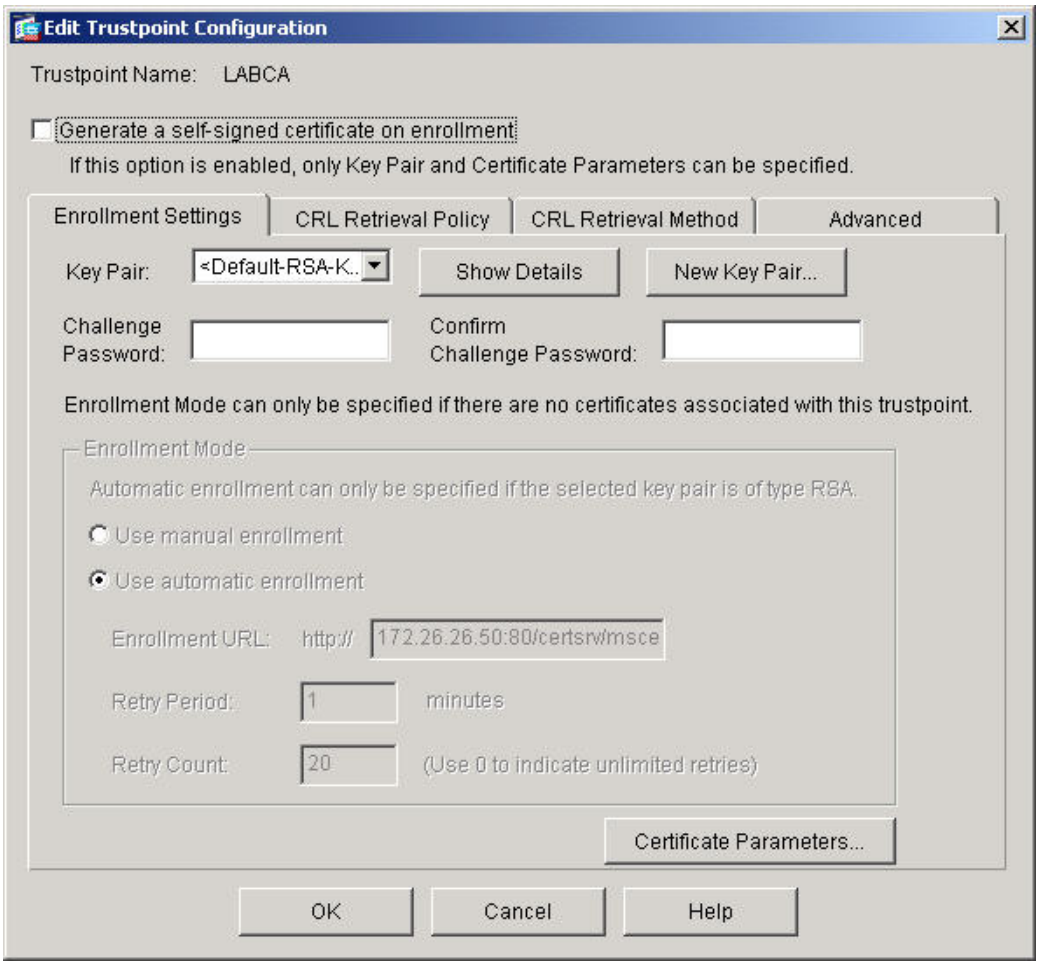
d. Navigate to the **Configuration>VPN>Features>IKE>Policies** to view the IKE policy using rsa-sig, hostname identity.



e. Navigate to the **Configuration>Features>Device Administration>Certificate>Trustpoint>Configuration** to view the CA parameters. Double click on the **LABCA** entry to see additional details the trustpoint. Click the **OK** button when finished.



f. Navigate to the **Configuration>Features>Device Administration>Certificate>Enrollment**. Click the **Edit** button to view the CA enrollment parameters. Click the **OK** button when finished.



g. Exit ASDM.

Lab 6.2.12a Configure Remote Access Using Cisco Easy VPN

Objective

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

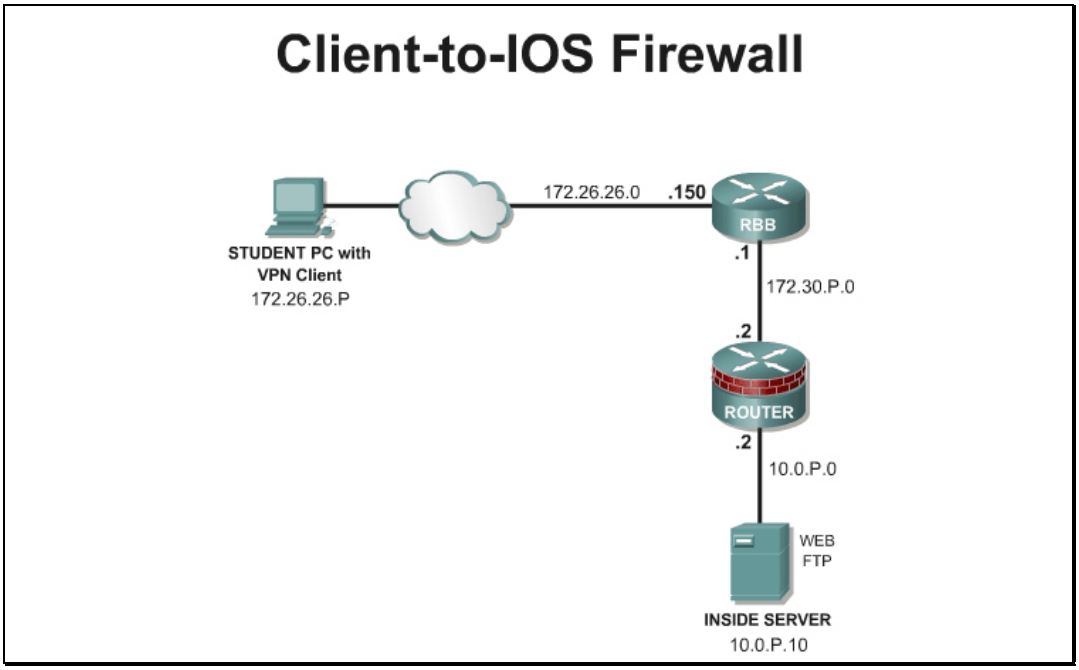
- Enable policy lookup via authentication, authorization, and accounting (AAA)
- Define group policy information for mode configuration push
- Configure and Verify the IPSec Transforms and Crypto Maps
- Install and configure the Cisco VPN Client 4.0 or later
- Connect to the corporate Intranet using the Cisco VPN Client

Scenario

A network administrator needs secure management access to the perimeter router and other critical devices on the internal network. In a small company, the budget may not allow for a dedicated VPN Concentrator. Fortunately, the IOS Firewall router 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 topology above and verify the starting configuration on the pod routers. Access the perimeter router console port using the terminal emulator on the Student PC. 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.

Before beginning this lab exercise, it is imperative to change the static IP address of the Student PC to **172.26.26.P 255.255.255.0** (where P =pod number) with a default gateway of 172.26.26.150. Also, the Student PC must be physically connected to a switch port on VLAN 1.

Tools and resources

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

- Standard Client-to-IOS Firewall lab topology
- Console cable
- HyperTerminal
- Cisco VPN Client 4.6 or later

Additional materials

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

http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a0080087d1e.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
aaa authentication	Set parameters that restrict a user's network access
aaa new-model	Enables AAA.
crypto isakmp client configuration group {group-name **| default}**	Specifies which group's policy profile will be defined and enters Internet Security Association Key Management Protocol (ISAKMP) group configuration mode. If no specific group matches and a default group is defined, users will automatically be given the default group's policy.
crypto map *map-name* **client authentication list** *list-name*	Enforces Xauth. The *list-name* argument is used to determine the appropriate username and password storage location (local or RADIUS) as defined in the **aaa authentication login** command.

Command	Description
crypto map *map-name* **client configuration address** ***[initiate | respond]***	Configures the router to initiate or reply to Mode Configuration requests. Note that the Cisco clients require the **respond** keyword to be used. However, if the Cisco Secure VPN Client 1.x is used, the **initiate** keyword must be used. The **initiate** and **respond** keywords may be used simultaneously.
crypto map *map-name* **isakmp authorization list** *list-name*	Enables IKE querying for group policy when requested by the client. The *list-name* argument is used by AAA to determine which storage source is used to find the policy (local or RADIUS) as defined in the **aaa authorization network** command.
ip local pool {default | *pool-name low-ip-address* **[***high-ip-address***]}**	Configures a group of local IP address pools
username ***name*** **password** *encryption-type encrypted-password*	Defines local users for Xauth if RADIUS or TACACS+ is not used. Use this command only if no external validation repository will be used.

Step 1 Enable Policy Lookup using Local AAA

To enable policy lookup using local AAA, complete the following commands for the perimeter router beginning in global configuration mode:

a. Enable AAA:

```
RouterP(config)#aaa new-model
```

b. Set AAA authentication at login. Note that this command must be enabled to enforce Xauth.

```
RouterP(config)#aaa authentication login VPNAUTHEN local
```

c. Set AAA authorization at login.

```
RouterP(config)# aaa authorization network VPNAUTHOR local
```

d. Define local users:

```
RouterP(config)#username vpnstudent password cisco
```

Step 2 Define Group Policy Information for Mode Configuration Push

Define the policy attributes that are pushed to the VPN Client via mode configuration. Use the following commands beginning in global configuration mode:

a. Configure a local pool of IP addresses to be used when a remote peer connects to a point-to-point interface.

```
RouterP(config)#ip local pool IPPOOL 11.0.P.20 11.0.P.30
```

(where P = pod number)

b. Create the ISAKMP policy:

```
RouterP(config)#  crypto isakmp policy 3
RouterP(config-isakmp)# encryption des
```



```
RouterP(config-isakmp)# hash md5
RouterP(config-isakmp)# authentication pre-share
RouterP(config-isakmp)# group 2
RouterP(config-isakmp)# exit
RouterP(config)#
```

c. Specify which group policy profile will be defined and enter ISAKMP group configuration mode. If no specific group matches and a default group is defined, users will automatically be given the default group policy. For this exercise, use a group name of “SALES”.

```
RouterP(config)#crypto isakmp client configuration group SALES
```

d. Specify the IKE pre-shared key for group policy attribute definition. Note that this command must be enabled if the VPN Client identifies itself with a pre-shared key. For this exercise, use a key of “cisco123”.

```
RouterP(isakmp-group)#key cisco123
```

e. Select a local IP address pool. Note that this command must refer to a valid local IP local address pool or the VPN Client connection will fail. Use the “IPPOOL” pool name.

```
RouterP(isakmp-group)#pool IPPOOL
```

f. Define a domain name:

```
RouterP(isakmp-group)#domain cisco.com
RouterP(isakmp-group)#exit
```

g. Examine the crypto policy suite.

```
RouterP# show crypto isakmp policy
```

Step 3 Configure and Verify the IPSec Transforms and Crypto Maps

a. Create the transform set to be used with the dynamic crypto map. Name the transform set **MYSET**. Specify triple-DES for encryptions in the ESP and MD5 HMAC authentication in the ESP.

```
RouterP(config)# crypto ipsec transform-set MYSET esp-des esp-md5-
hmac
RouterP(cfg-crypto-trans)# exit
```

b. Create the dynamic crypto map:

```
RouterP(config)# crypto dynamic-map DYNMAP 10
RouterP(config-crypto-map)# set transform-set MYSET
RouterP(config-crypto-map)# reverse-route
RouterP(config-crypto-map)# exit
```

c. Configure the router to initiate or reply to mode configuration requests. Note that VPN Clients require the **respond** keyword to be used.

```
RouterP(config)#crypto map CLIENTMAP client configuration address
respond
```

d. Enable IKE querying for group policy when requested by the VPN Client. The list-name argument is used by AAA to determine which storage is used to find the policy, local or RADIUS, as defined in the **aaa authorization network** command.

```
RouterP(config)#crypto map CLIENTMAP isakmp authorization list
VPNAUTHOR
```


e. Enforce Xauth. The list-name argument is used to determine the appropriate username and password storage location, local or RADIUS, as defined in the **aaa authentication login** command.

```
RouterP(config)#crypto map CLIENTMAP client authentication list
VPNAUTHEN
```

f. Assign the dynamic crypto map to CLIENTMAP:

```
RouterP(config)# crypto map CLIENTMAP 10 ipsec-isakmp dynamic DYNMAP
```

g. Assign the crypto map to the outside interface:

```
RouterP(config)# interface fastEthernet 0/1
RouterP(config-if)# crypto map CLIENTMAP
RouterP(config-if)# exit
```

h. To verify the configurations for this feature, use the following command in EXEC mode to view the crypto map configuration:

```
RouterP#show crypto map {interface interface | tag map-name}
```

i. To verify the configurations for this feature, use the following command in EXEC mode to view the transform set:

```
RouterP# show crypto ipsec transform-set
```

Step 4 Install the Cisco VPN Client 4.0

Complete the following steps to install the Cisco VPN Client version 4.0 or later on the Student PC:

a. Open the VPN Client desktop folder.

b. Locate and run the Cisco VPN Client setup.exe executable. If this is the first time the VPN Client is installed, a window opens and displays the following message: **Do you want the installer to disable the IPSec Policy Agent?**

c. Click **Yes** to disable the IPSec policy agent. The Welcome window opens.

d. Read the Welcome window and click **Next**. The License Agreement window opens.

e. Read the license agreement and click **Yes**. The Choose Destination Location window opens.

f. Click **Next**. The Select Program Folder window opens.

g. Accept the defaults by clicking **Next**. The Start Copying Files window opens.

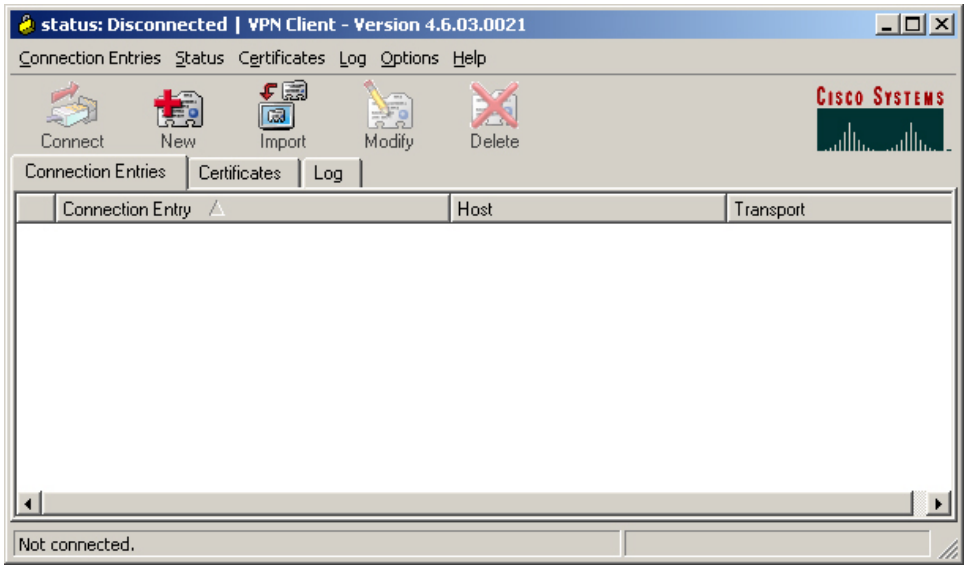
The files are copied to the hard disk drive of the PC and the InstallShield Wizard Complete window opens.

h. Select **Yes, I want to restart my computer now** and click **Finish**. The PC restarts. This completes the installation of the Cisco VPN Client (Software Client).

Step 5 Create a New Connection Entry

Complete the following steps to create a new VPN connection entry:

a. Choose **Start** > **Programs** > **Cisco Systems VPN Client** > **VPN Client**. The Cisco Systems VPN Client window opens.



b. Click the **New** button. The Create New VPN Connection Entry window opens.

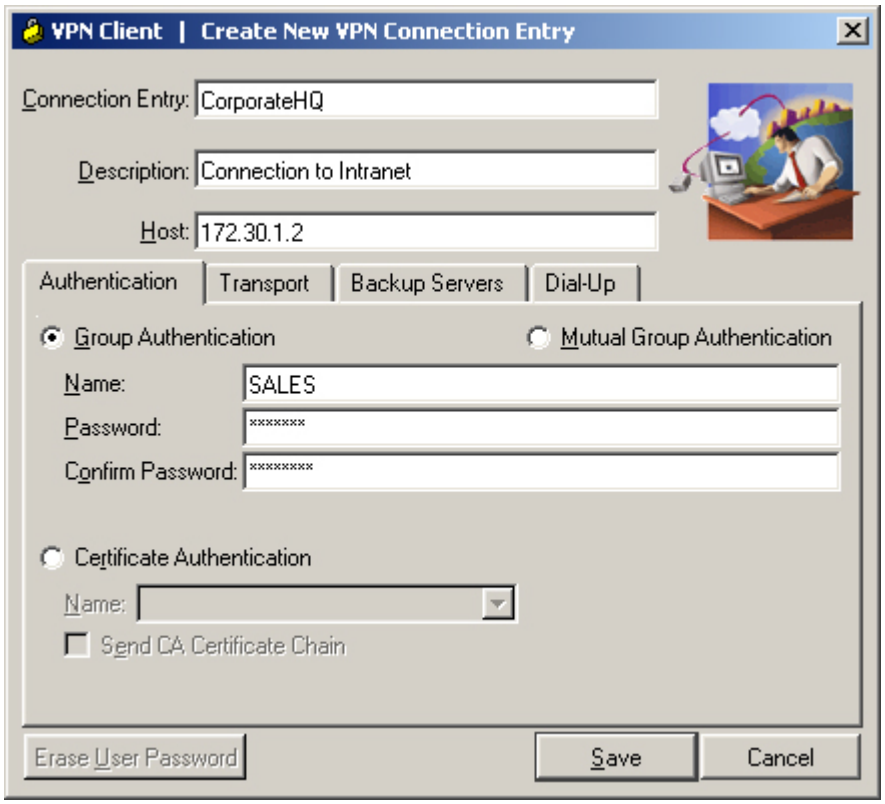
c. Enter **CorporateHQ** in the **Connection Entry** field.

d. Enter a public interface IP address of **172.30.P.2** in the **Host** field.

(where P = pod number)

e. Click on the **Group Authentication** radio button and complete the following substeps. The following entries are always case sensitive.

- Enter a group name, **SALES**.
- Enter the group password, **cisco123**.
- Confirm the password, **cisco123**.



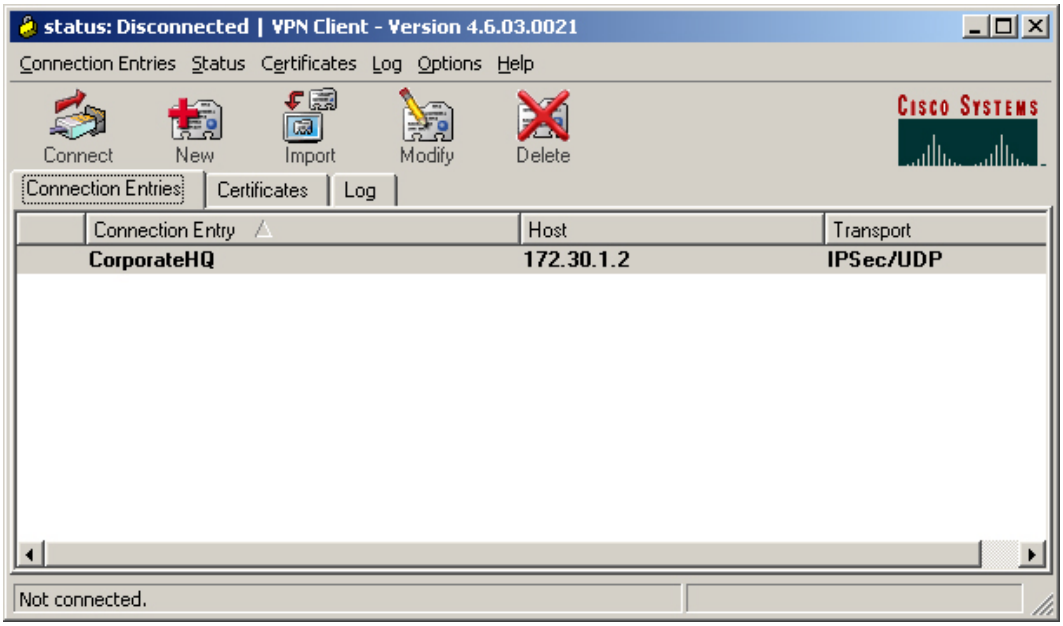
f. Click the **Save** button and leave the Cisco Systems VPN Client window open.

The network parameters for the VPN Client have been configured and a new VPN private networking connection entry has been created successfully.

Step 6 Launch the Cisco VPN Client

Complete the following steps to launch the Cisco VPN client on the PC:

a. Verify that the connection entry is **CorporateHQ**.



b. Verify that the IP address of remote server is set to the perimeter router public interface IP address of 172.30.P.2.

(where P = pod number)

c. Click **Connect**. The User Authentication window opens and several messages flash by quickly. Complete the following substeps:

i. When prompted for a username, enter **vpnstudent**.

ii. When prompted to enter a password, enter **cisco**.

iii. Click **OK**.

The Authentication window disappears and a VPN lock icon appears in the system tray. The VPN Client has been successfully launched.

d. On the router console, the following message should appear.

```
Router1#

03:12:00: %CRYPTO-5-SESSION_STATUS: Crypto tunnel is UP   .  Peer
172.26.26.1:500       Id: SALES
```

Step 7 Monitor the Cisco VPN Client

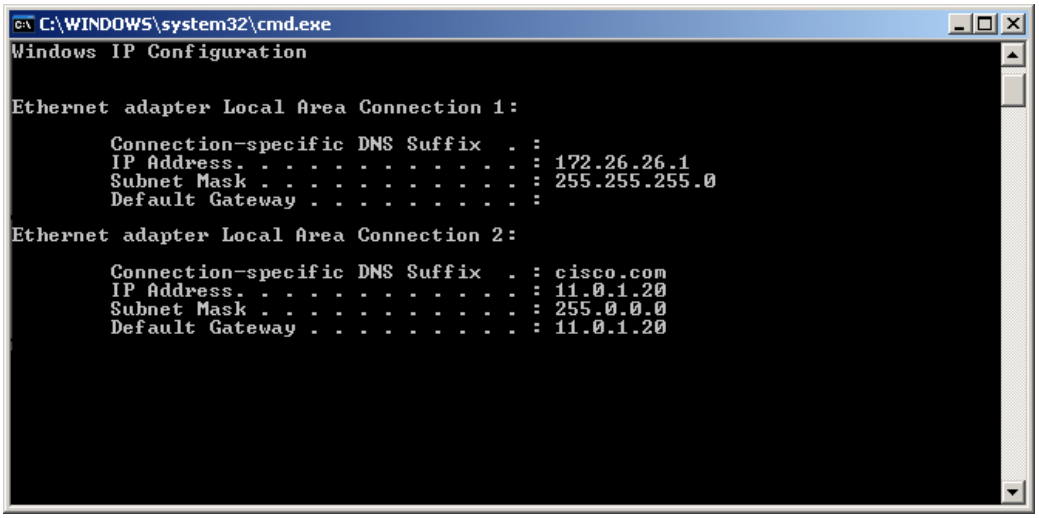
Complete the following steps to monitor the Cisco VPN client connection on the PC:

a. Go to **Start**>**Run** on a Win2k or XP computer.

b. Type in **cmd**

c. A command prompt will appear. Check the interface configuration using the command.

```
C:\> ipconfig
```

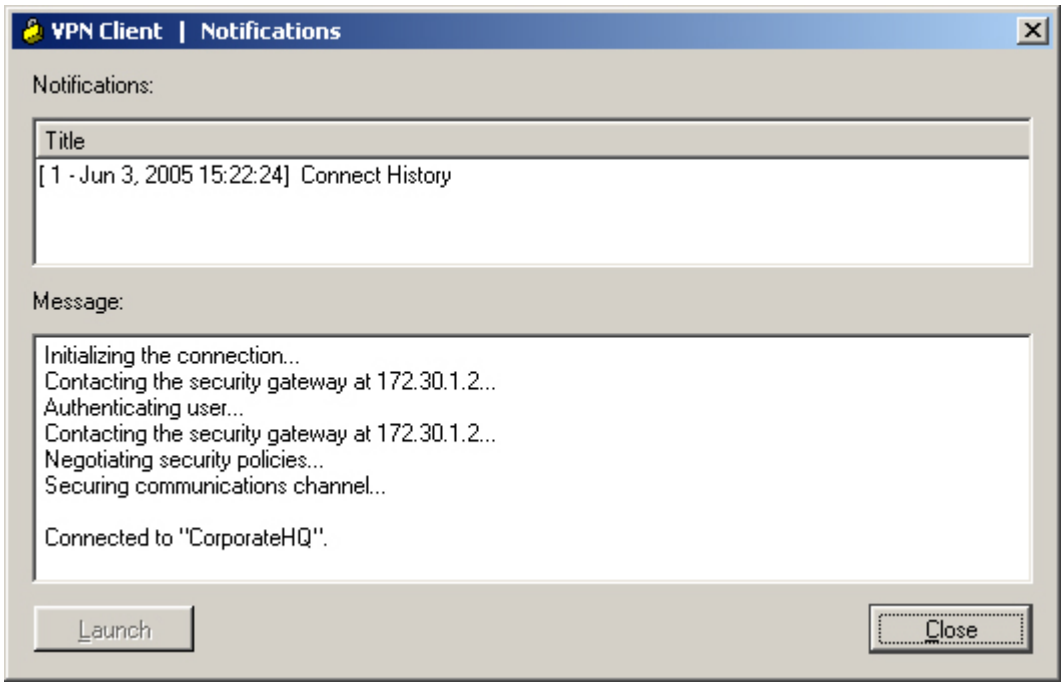



Notice the two Local Area Connection addresses. One is the physical interface, the other is the virtual interface created by the Cisco VPN client. The virtual interface allows for greater application support.

Note This figure shows the results with VPN client version 4.6. The virtual interface is not available previous to 4.0.

---

d. Right click on the lock icon located in the system tray and left click on **Notifications**.



e. This will provide the connection history. Click on the **Close** button when finished.

f. Next, right click on the lock icon located in the system tray and left click on **Statistics**

g. In the Tunnel Details tab, verify the Address Information. The IP address should be in the range of 11.0.P.20 – 30. The Server address should be 172.30.P.2

h. Verify the encryption and authentication protocols.

i. To get a clear picture of the traffic, click on the Reset button to reset the counters to zero.

j. On the Student PC, open a web browser and connect to the inside interface of the router

http://10.0.P.2

k. On the Student PC, open a web browser and connect to the Inside server

http://10.0.P.10

l. When finished, right click on the lock and left click Disconnect.

m. On the router console, the following message should appear.

```
03:20:36: %CRYPTO-5-SESSION_STATUS: Crypto tunnel is DOWN.  Peer
172.26.26.223:500       Id: SALES
```

n. 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 isakmp sa
RouterP# show crypto ipsec sa
```

Step 8 Modify the IPSec Transforms

Company XYZ has decided to strengthen the VPN encryption.

a. Create the transform set to be used with the dynamic crypto map. Name the transform set "MYSET". Specify AES 256 for encryptions and SHA HMAC authentication.

```
RouterP(config)# no crypto ipsec transform-set MYSET esp-des esp-
md5-hmac
RouterP(config)# crypto ipsec transform-set MYSET esp-aes 256 esp-
sha-hmac
RouterP(cfg-crypto-trans)# exit
```

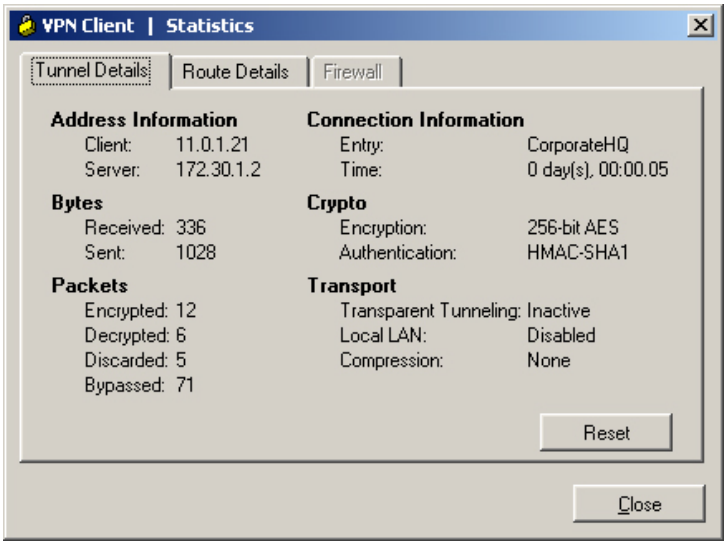
b. Open the VPN client and click **Connect**. The User Authentication window opens and several messages flash by quickly. Complete the following substeps:

i. When prompted for a username, enter **vpnstudent**.

ii. When prompted to enter a password, enter **cisco**.

iii. Click **OK**.

c. Open the Statistics and verify the new encryption and authentication.



Lab 6.2.12b Configure Cisco Easy VPN Server with NAT

Objective

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

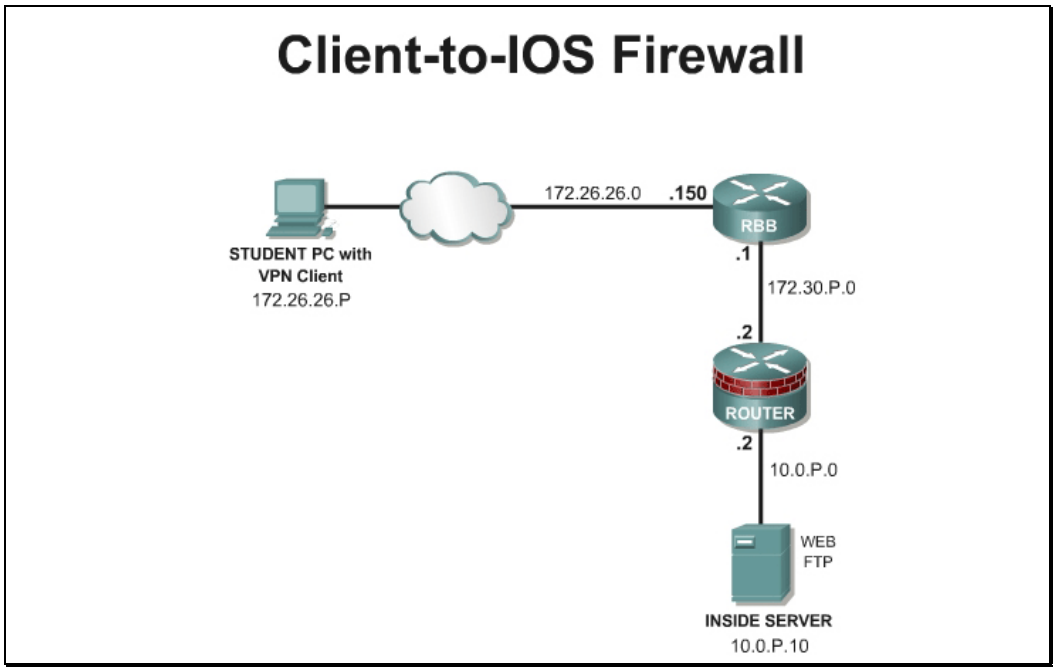
- Verify Easy VPN Server configuration
- Configure and Modify PAT using CLI
- Configure and Modify PAT using SDM
- Test remote connectivity

Scenario

The Cinko Company opened a new office in China and wants to allow Account Mangers to connect to the internal web and email servers. A DSL line with one static IP address has recently been installed. The Remote access VPN must be configured to work with PAT. The local IT manager has already configured the router with a VPN configuration used at the Headquarters. The VPN client will connect to the router, but connectivity to the inside devices on the network is not possible at this time.

Topology

This figure illustrates the lab network environment.



Preparation

Begin with the topology above and verify the starting configuration on the pod router. Access the perimeter router console port using the terminal emulator on the Student PC. 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.

Before beginning this lab exercise, it is imperative to change the static IP address of the student PC to **172.26.26.P 255.255.255.0** (where P =pod number) with a default gateway of 172.26.26.150 or obtain an IP address from a DHCP pool configured on RBB. Also, the Student PC must be physically connected to a switch port on VLAN 1.

Tools and resources

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

- Standard Client-to-IOS Firewall lab topology
- Console cable
- HyperTerminal
- Cisco VPN Client 4.6 or later

Additional materials

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

http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a0080087d1e.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
access-list	Define an access list permitting those addresses that are to be translated.
ip nat {inside | outside} | log {translations syslog}	Mark the interface as connected to the inside or outside.
ip nat inside source static *local-ip global-ip*	Establish static translation between an inside local address and an inside global address.

Step 1 Verify the Easy VPN Server Configuration

a. Load the starting configuration for the lab. This configuration contains the Easy VPN Server configuration that was completed in the previous lab.

b. Open the VPN client and click **Connect**. The User Authentication window opens and several messages flash by quickly. Complete the following substeps:

   i. When prompted for a username, enter **vpnstudent** if the username does not already appear in the text box.

   ii. When prompted to enter a password, enter **cisco**.

   iii. Click **OK**.

c. The closed lock should now appear in the System tray.

d. On the router, the following message should appear.

```
18:13:54: %CRYPTO-5-SESSION_STATUS: Crypto tunnel is UP  .  Peer
172.26.26.1:5
00       Id: SALES
```

e. Disconnect the VPN session. The open lock should appear in the System tray.

f. On the router, the following message should appear.

```
18:20:29: %CRYPTO-5-SESSION_STATUS: Crypto tunnel is DOWN.  Peer
172.26.26.1:5
00       Id: SALES
```

Step 2 Configure PAT

a. Define addresses to be translated by creating an extended access list.

```
RouterP(config)# access-list 150 permit ip 10.0.P.0 0.0.0.255 any
```

1. What is the purpose of this access list?

_____

Answer: This access list defines the range of IP addresses that will be translated when PAT, or overloaded NAT, is configured.

b. Verify the access list created.

```
RouterP# show access-list
```

c. Now connect the access list to a NAT statement.

```
RouterP(config)#ip nat inside source list 150 interface
fastEthernet0/1 overload
```

d. Configure the router interface which is connected to the inside network and which interface is connected to the outside.

```
RouterP(config)#interface fastEthernet0/0
RouterP(config-if)#ip nat inside

RouterP(config)#interface fastEthernet0/1
RouterP(config-if)#ip nat outside
```

Step 3 Test the Connectivity

a. From the Student PC on the outside, open a command prompt and ping the inside interface address on the router at 10.0.P.2

```
C:\>ping 10.0.P.2
```

Was it successful?

_____

Answer: No

b. From the Student PC, try to telnet to 10.0.P.2

```
C:\>telnet 10.0.P.2
```

Was it successful?

_____

Answer: No

c. From the Student PC, try to make an http connection to 10.0.P.2

```
http://10.0.P.2
```

Was it successful?

_____

Answer: No

d. Open the VPN client and click **Connect**. The User Authentication window opens and several messages flash by quickly. Complete the following substeps:

i. When prompted for a username, enter **vpnstudent** if the username does not already appear in the text box.

ii. When prompted to enter a password, enter **cisco**.

iii. Click **OK**.

e. The closed lock should now appear in the System tray.

f. From the Student PC on the outside, open a command prompt and ping the inside interface address on the router at 10.0.P.2

```
C:\>ping 10.0.P.2
```

Was it successful?

_____

Answer: No

g. From the Student PC, try to telnet to 10.0.P.2

```
C:\>telnet 10.0.P.2
```

Was it successful?

_____

Answer: No

h. From the Student PC, try to connect using SDM to 10.0.P.2

```
http://10.0.P.2
```

Was it successful?

_____

Answer: No

i. Test inside to outside translation. From a workstation or server on the inside network, ping RBB at 172.26.26.150

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

Was it successful?

_____

Answer: No

j. Now verify the routers address translation.

```
RouterP#show ip nat translations
RouterP#show ip nat translations verbose
RouterP#show ip nat statistics
```


k. At this point, it should be clear that the PAT is working correctly for traffic originating from the the inside network, but the remote access connection is not functioning correctly. This is caused by the return VPN traffic being translated. The translation invalidated the return VPN packet. In the next step, this problem is easily fixed.

Step 4 Modify the PAT ACL

a. Define the inside addresses to be translated while excluding the VPN traffic from translation. First, clear the access list.

```
RouterP(config)# no access-list 150
RouterP(config)# access-list 150 deny ip 10.0.P.0 0.0.0.255 11.0.P.0
0.0.0.255 log
```

Note Notice that the local 10.0.P.0 network is define as the source and the 11.0.P.0 remote address pool is the destination.

```
RouterP(config)# access-list 150 permit ip 10.0.P.0 0.0.0.255 any
```

b. Right click on the closed lock icon in the system try and select **Disconnect** from the menu.

c. Reopen the VPN client and click **Connect**. The User Authentication window opens and several messages flash by quickly. Complete the following substeps:

   i. When prompted for a username, enter **vpnstudent** if the username does not already appear in the text box.

   ii. When prompted to enter a password, enter **cisco**.

   iii. Click **OK**.

d. The closed lock should now appear in the System tray.

e. From the Student PC on the outside, open a command prompt and ping the inside interface address on the router at 10.0.P.2

```
C:\>ping 10.0.P.2
```

Was it successful?

_____

Answer: Yes

f. From the Student PC, try to telnet to 10.0.P.2. Log into the router using **sdm**/**sdm**

```
C:\>telnet 10.0.P.2
```

Was it successful?

_____

Answer: Yes

g. From the Student PC, try to connect using SDM to 10.0.P.2. Log into the router using sdm/sdm

```
http://10.0.P.2
```

Was it successful?

_____

Answer: Yes

Step 5 Modify the PAT ACL using SDM

In this step, define the inside addresses to be translated while excluding the VPN traffic from translation

a. Remove the NAT configuration or load the startup configuration.

b. From the Student PC on the outside, connect to the router using SDM.

`http://10.0.P.2`

Note	When the SDM session is initiated at the inside interface of the router, the session is protected by the VPN tunnel.

c. Click on the **Configure** button at the top of the SDM interface.

d. Click the **NAT** button in the **Tasks** panel.

e. Click on the **Designate NAT Interfaces** button.

f. Verify that the appropriate inside and outside interfaces are checked and click **OK**.

g. Click on the **Add** button in the **Network Address Translation Rule** area.

h. The **Add Address Translation Rul**e window appears. Choose the **Dynamic** radio button.

i. Define an ACL rule using the **…** button. Click on **Create a new rule (ACL) and select** option.

j. Name the extended ACL as **NAT_ACL** with a description of **ACL for NAT**

k. Click on the **Add** button to define the first ACL statement which will deny traffic from the remote VPN network, **11.0.P.0/24**, to the local LAN network, **10.0.P.0/24**. Log this traffic.

l. Add a second ACL to translate all inside **10.0.P.0** traffic.

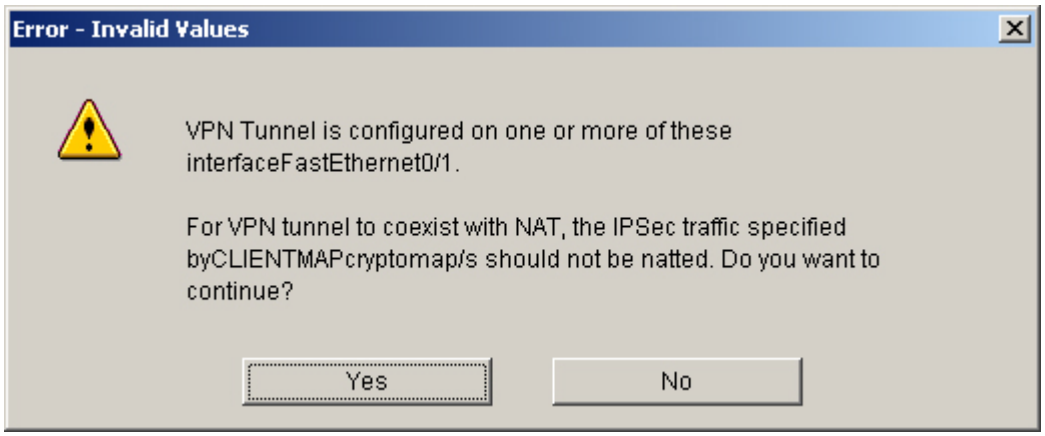
m. Click the **OK** button to complete the Rule and return to the **Add Address Translation Rule** window.

n. Choose the outside interface to translate to.

   a. Type: Interface

   b. Interface: Fa0/1

o. Click **OK.** An **Error-Invalid Values** window will appear.



p. Click the **Yes** button.

q. Click on the **Deliver** button.

r. The Command Delivery Status window will appear, click the **OK** button to continue. The configuration from Router1 is shown below.

```
ip access-list extended NAT_ACL
 remark ACL for NAT
 remark SDM_ACL Category=2
 remark Except remote access VPN traffic from translation
```



```
 deny ip 10.0.1.0 0.0.0.255 11.0.1.0 0.0.0.255 log
 remark Translate all Inside traffic
 permit ip 10.0.1.0 0.0.0.255 any
 exit
interface FastEthernet0/1
 ip nat outside
 exit
interface FastEthernet0/0
 ip nat inside
 exit
route-map SDM_RMAP_1 permit 1
 match ip address NAT_ACL
 exit
ip nat inside source route-map SDM_RMAP_1 interface FastEthernet0/1
overload
```

s. Notice that SDM uses a route map in the NAT configuration. This accomplished the same translation process as configured in previous steps.

t. Exit SDM.

Step 6 Test the SDM Configuration

a. Right click on the closed lock icon in the system try and select **Disconnect** from the menu.

b. Reopen the VPN client and click **Connect**. The User Authentication window opens and several messages flash by quickly. Complete the following substeps:

   i. When prompted for a username, enter **vpnstudent** if the username does not already appear in the text box.

   ii. When prompted to enter a password, enter **cisco**.

   iii. Click **OK**.

c. The closed lock should now appear in the System tray.

d. On the router, the following message should appear.

```
18:13:54: %CRYPTO-5-SESSION_STATUS: Crypto tunnel is UP  .  Peer
172.26.26.1:5
00       Id: SALES
```

e. From the Student PC on the outside, open a command prompt and ping the inside interface address on the router at 10.0.P.2

```
C:\>ping 10.0.P.2
```

Was it successful?

_____

Answer: Yes

f. From the Student PC, try to telnet to 10.0.P.2. Log into the router using sdm/sdm

```
C:\>telnet 10.0.P.2
```

Was it successful?

_____

Answer: Yes

g. From the Student PC, try to connect to the pod router web inside interface located at 10.0.P.2. Log into the router using sdm/sdm

```
http://10.0.P.2
```

Was it successful?

_____

Answer: Yes

h. Now verify the address translation. If traffic has not originated from the LAN, then no translations should appear.

```
RouterP#show ip nat translations
RouterP#show ip nat translations verbose
RouterP#show ip nat statistics
```


Lab 6.5.11a 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:

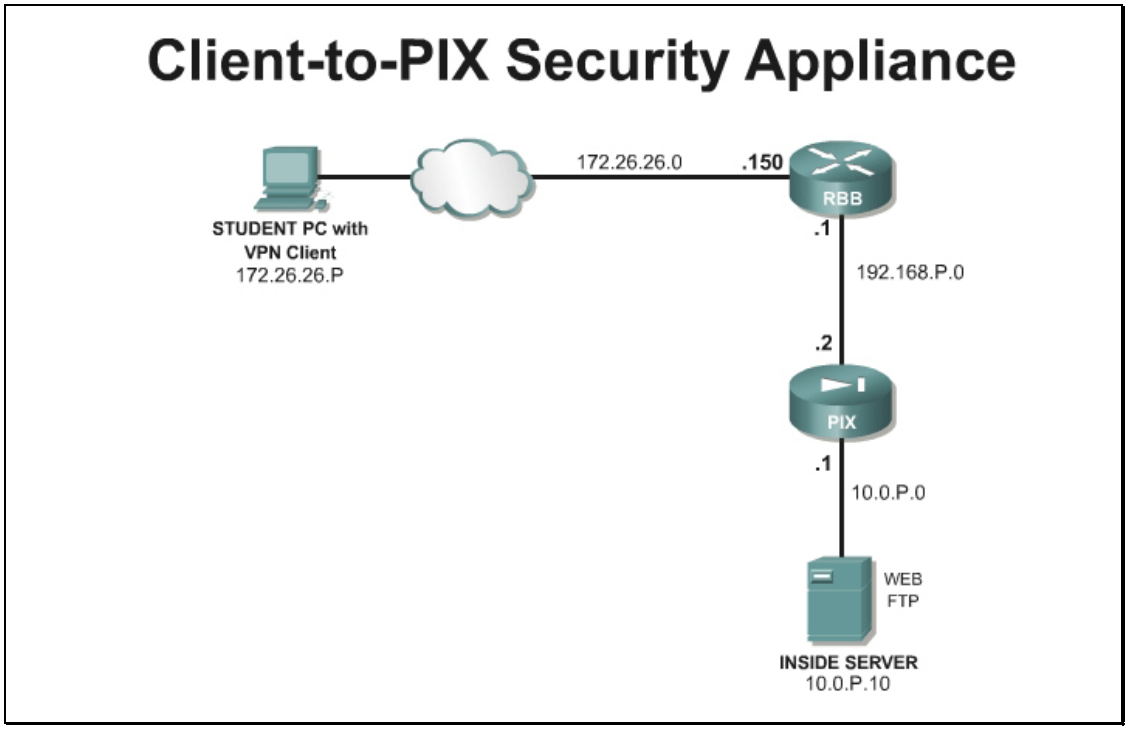
- Configure the PIX Easy VPN Server feature using ASDM.
- Install and configure the Cisco VPN Client on the Student PC.
- Verify and Test the Cisco VPN Client remote access connection

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

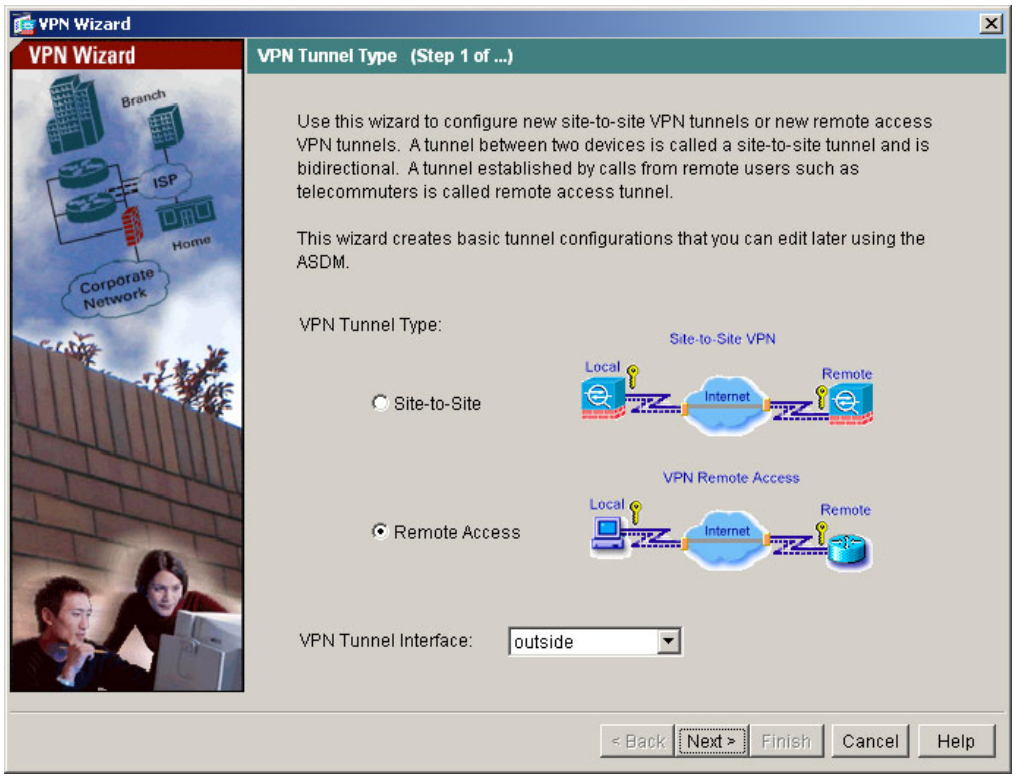
Complete the following steps to use ASDM to configure the Easy VPN Server feature on the PIX Security Appliance:

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.

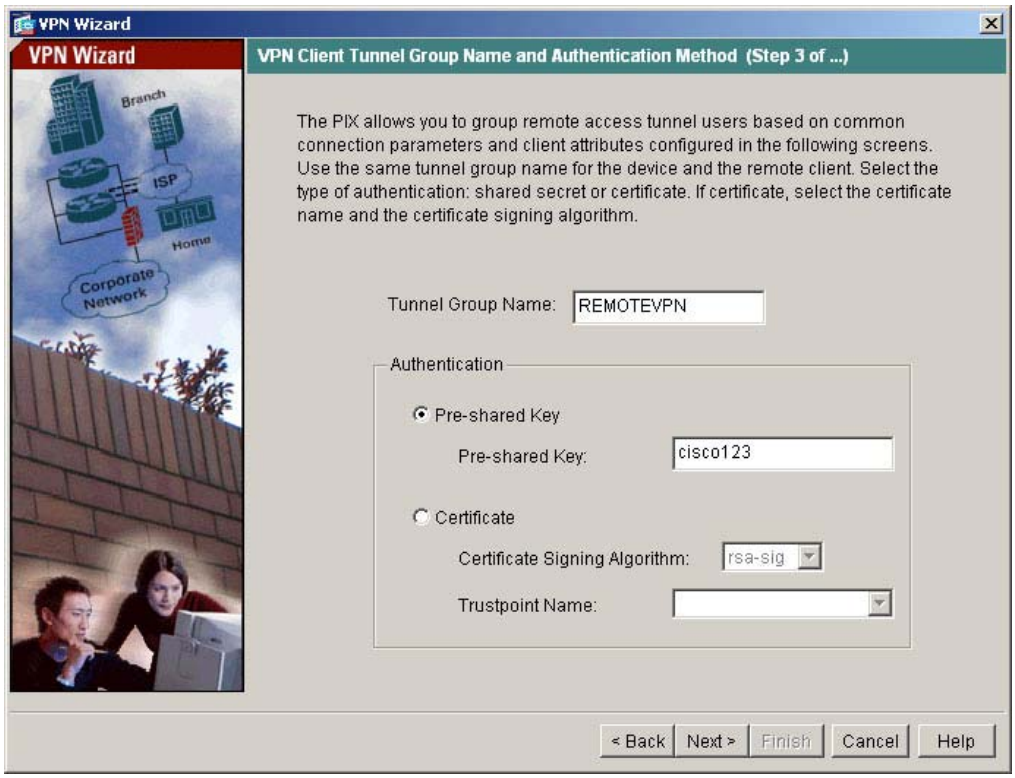
d. Select the **outside** interface in the drop down list.



e. Click the **Next** button to continue. The Remote Access Client Window appears.

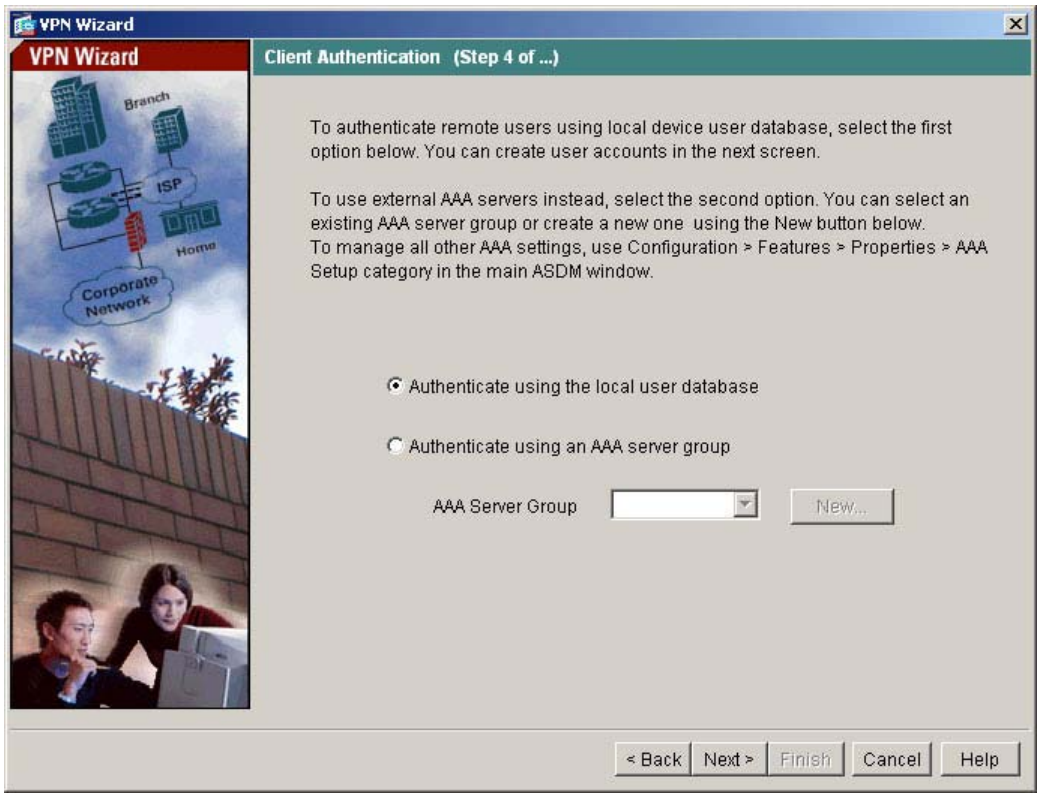
f. Verify that the **Cisco VPN Client, Release 3.x or higher, or other VPN Remote product** radio button is chosen. Click **Next**. The VPN Client Tunnel Group Name and Authentication Method window opens.

g. Enter a Group Name of **REMOTEVPN** with a password of **cisco123**.



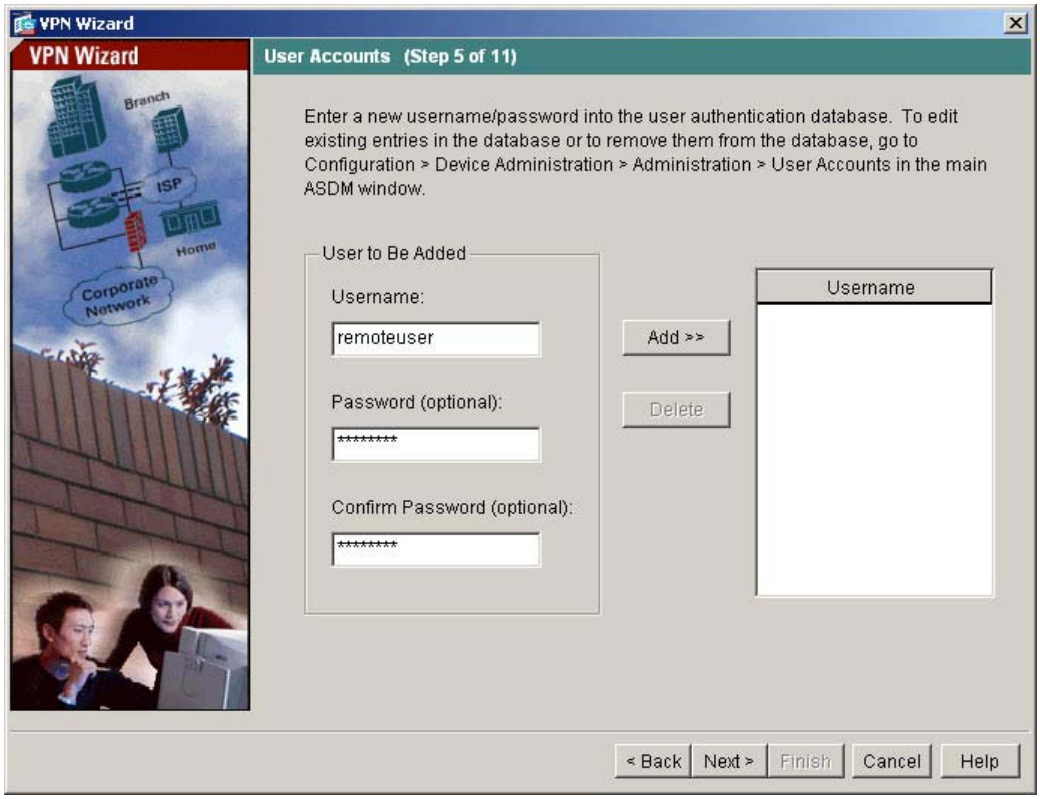
h. Click the **Next** button to continue The Client Authentication Window appears.

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



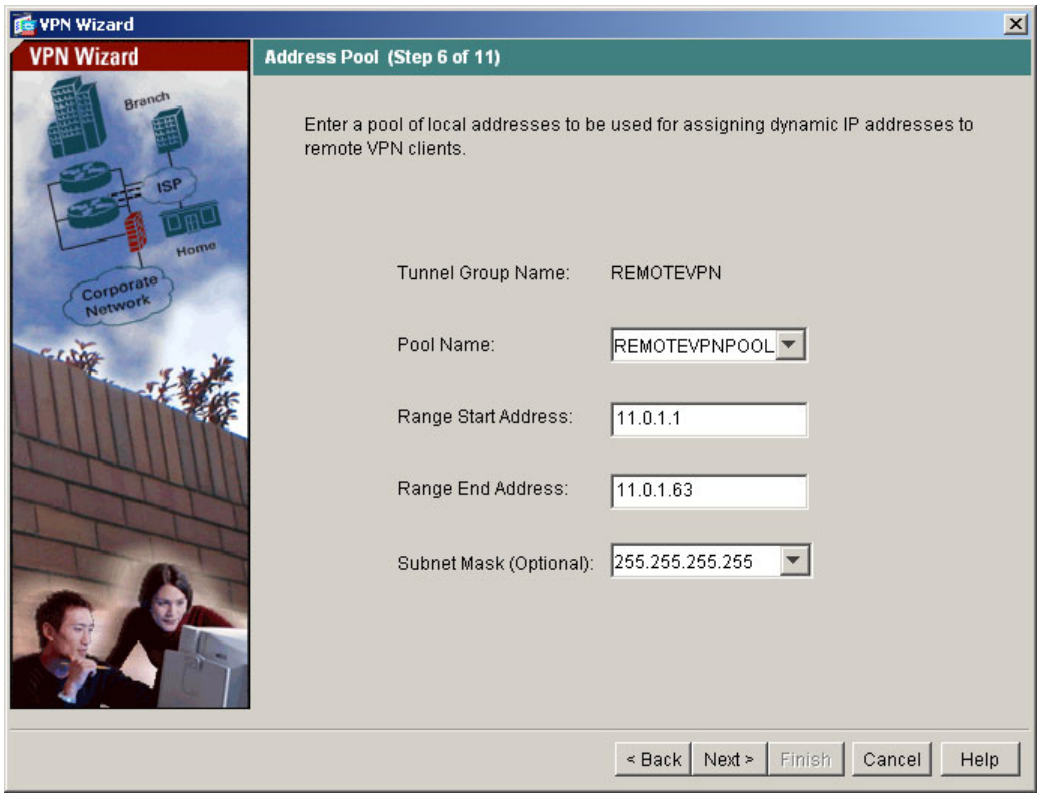
j. Click the **Next** button to continue. The User Accounts window appears.

k. Add a user **remoteuser** and the password **cisco123**.



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

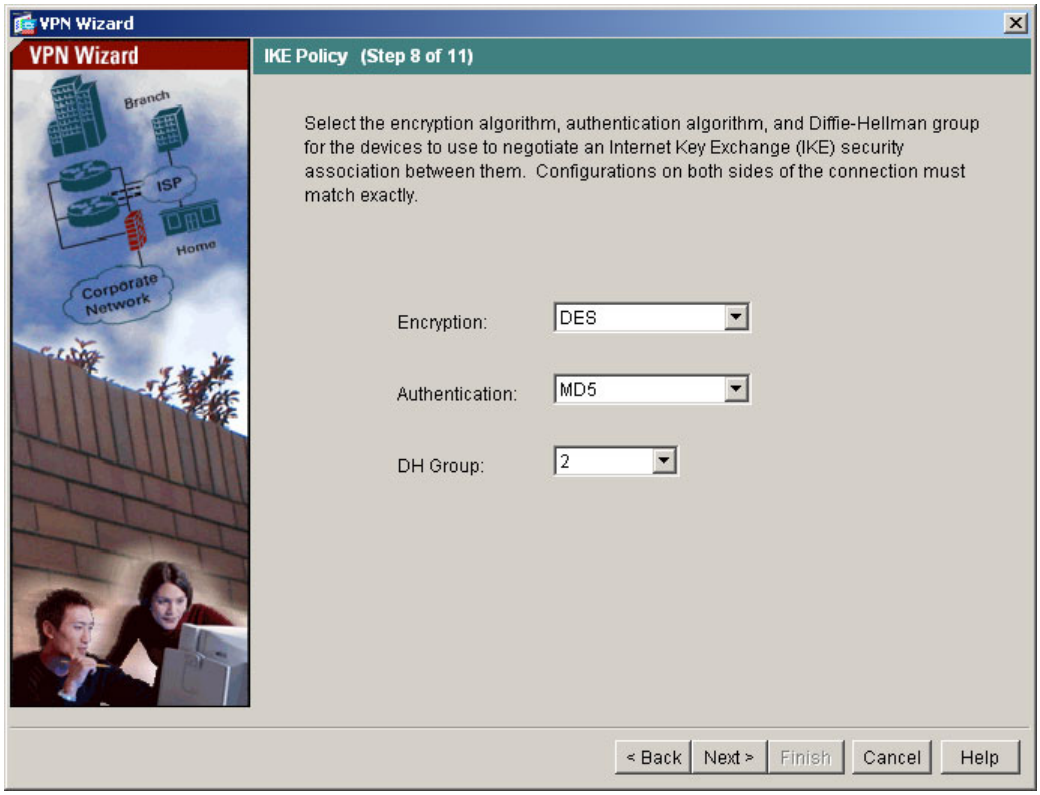
m. Create a pool called **REMOTEVPNPOOL** with a range of **11.0.P.1** – **11.0.P.63**



n. Click the **Next** button. The Attributes Pushed to Client window appears.

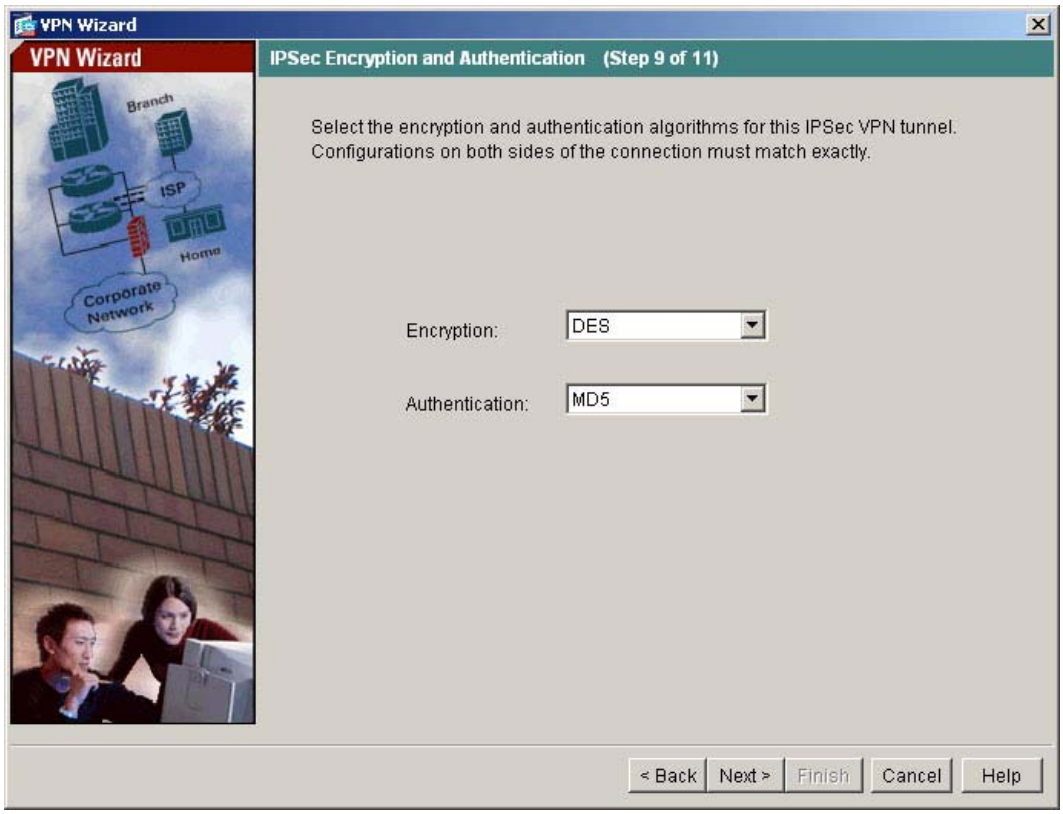
o. Click the **Next** button. The IKE Policy window appears.

p. Configure DES, MD5, and DH Group 2.



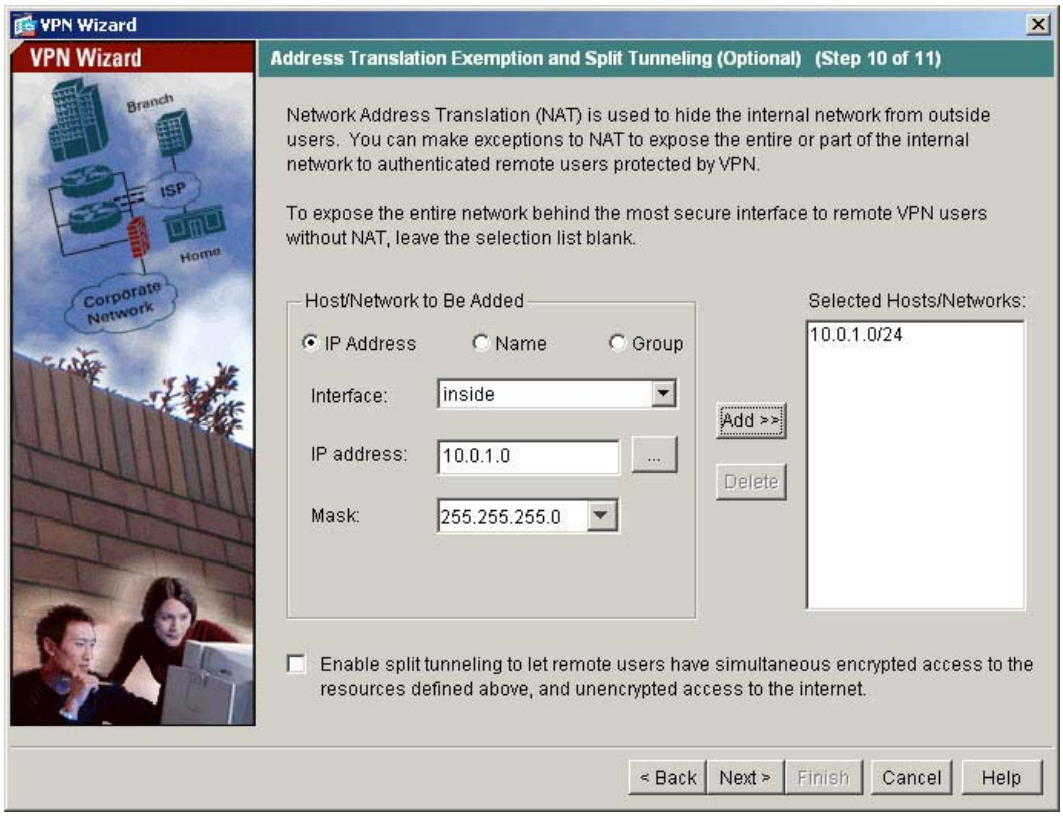
q. Click the **Next** button. The IPSec Encryption and Authorization window appears.

r. Choose DES and MD5.

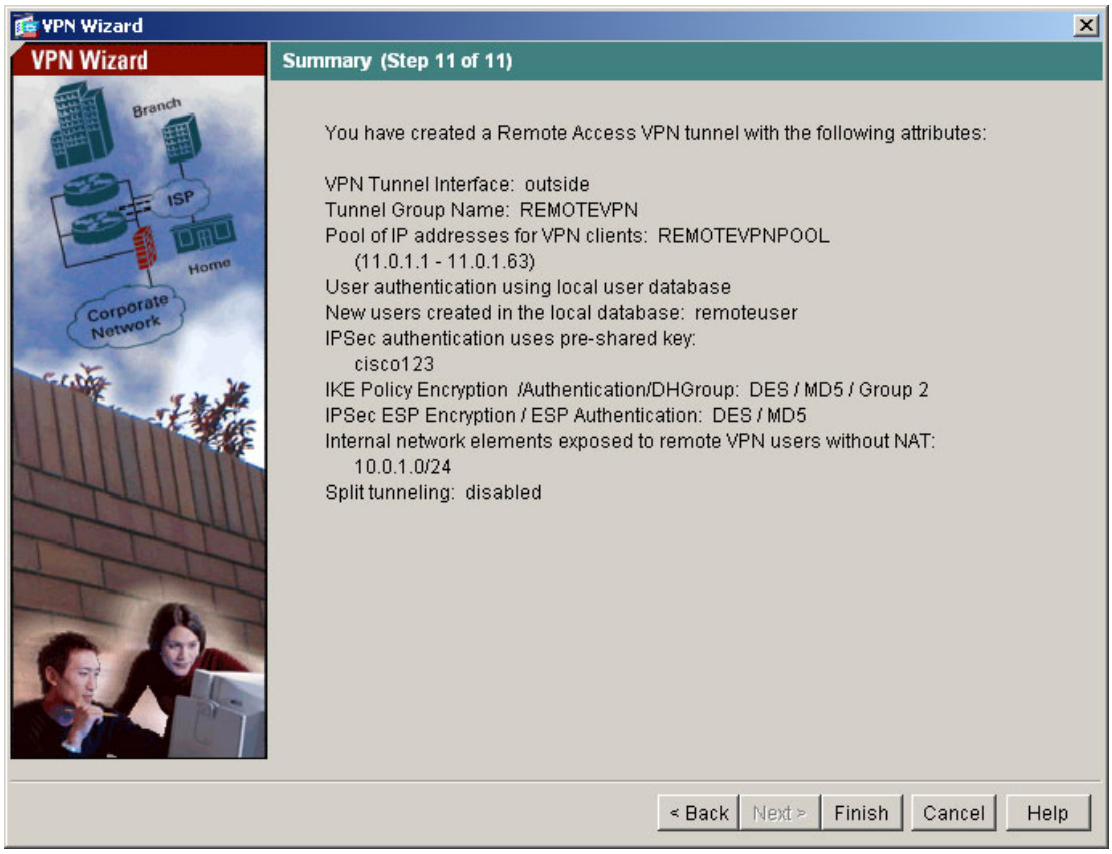


s. Click the **Next** button. The Address Translation Exemption and Split Tunneling window appears

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.

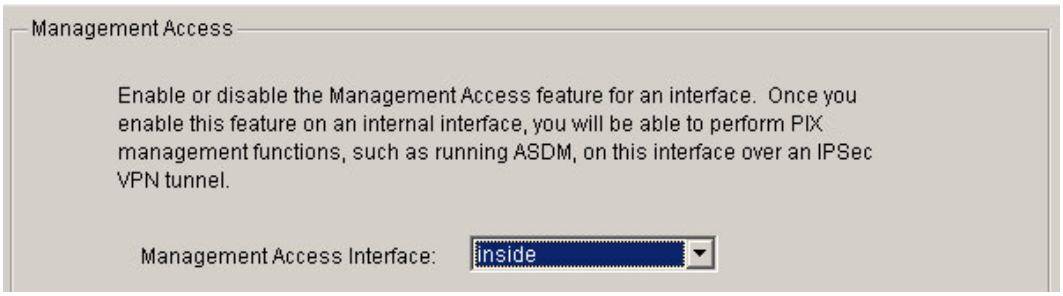


v. Click the **Finish** button.

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.

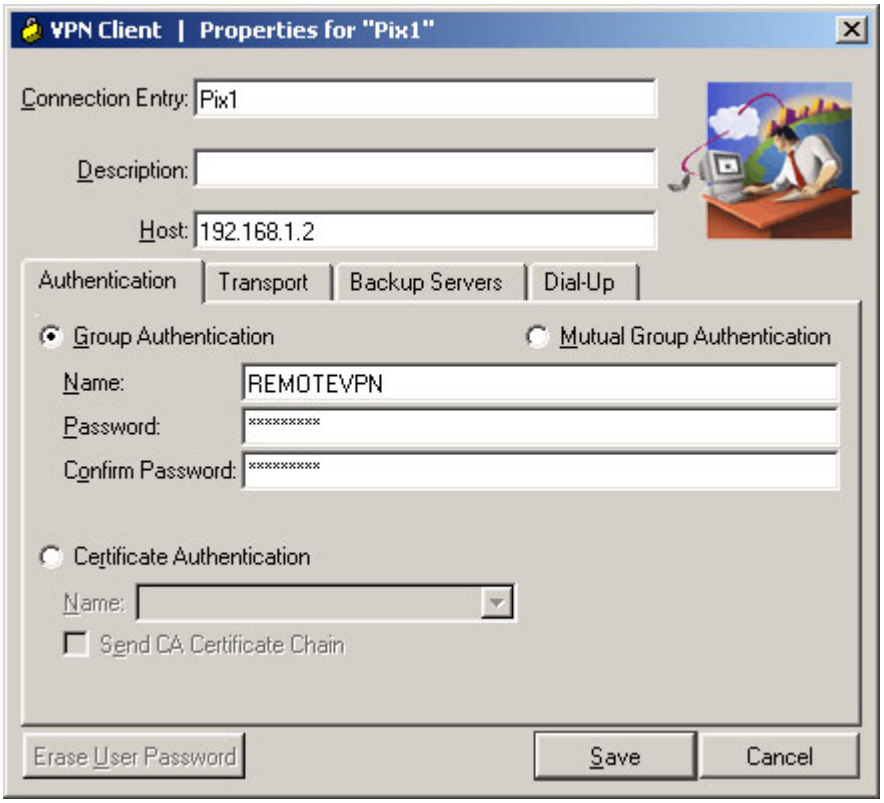
a. Choose **Start>Programs>Cisco Systems VPN Client>VPN Client**. The Cisco Systems VPN Client window opens.

b. Click **New**. The New Connection Entry wizard opens.

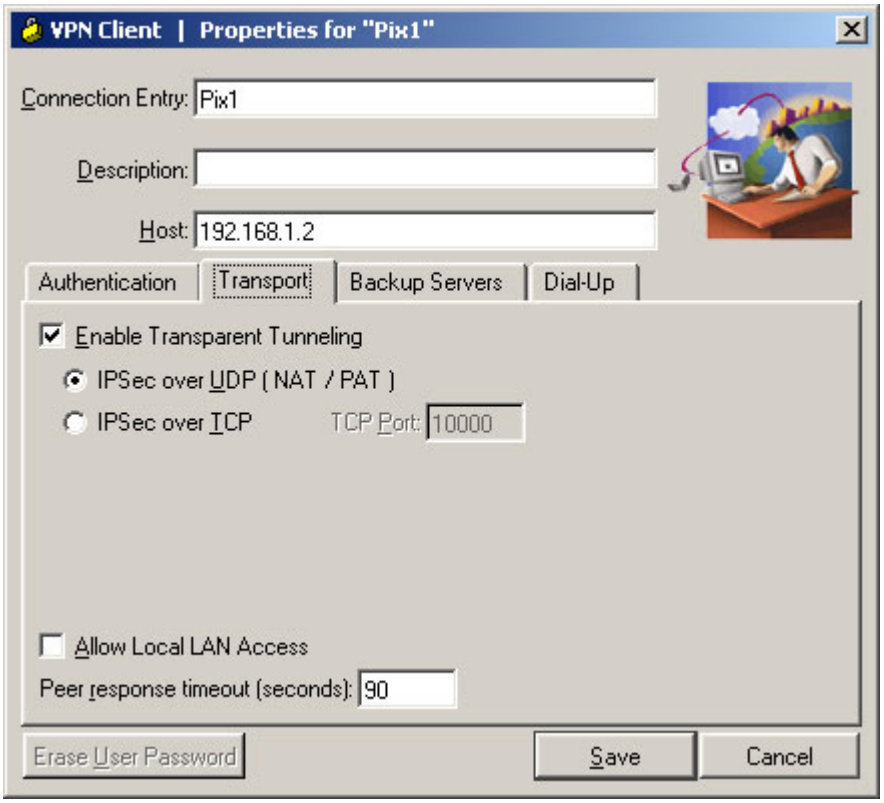
c. Enter **PixP** as the name in the Connection Entry field. Enter the PIX Security Appliance's public interface IP address, **192.168.P.2**, as the IP address of the remote host.

b. Enter the following group information in the **Authentication** tab.

- Enter a group name: **REMOTEVPN**
- Enter and Confirm a group password: **cisco123**



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



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**

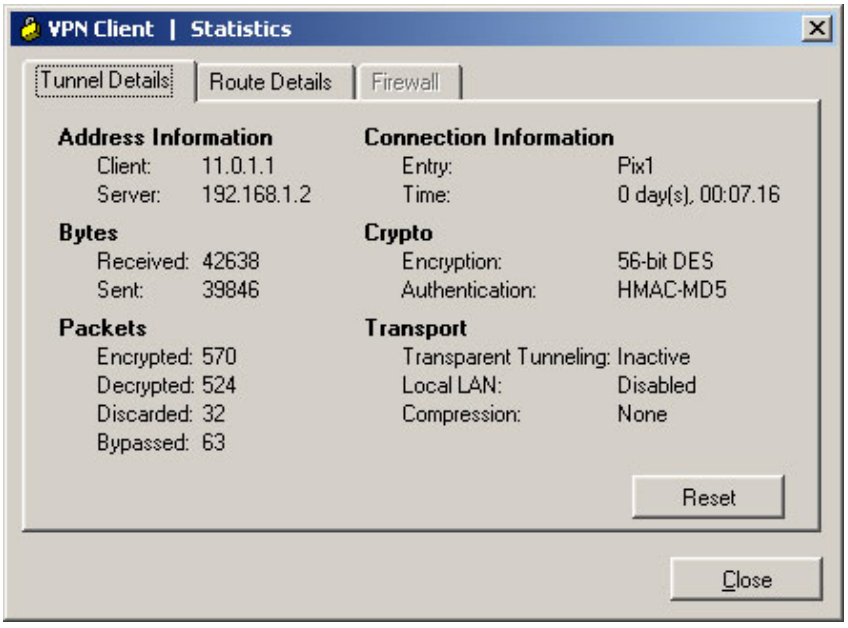
c. The web server's home page should display.

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
```

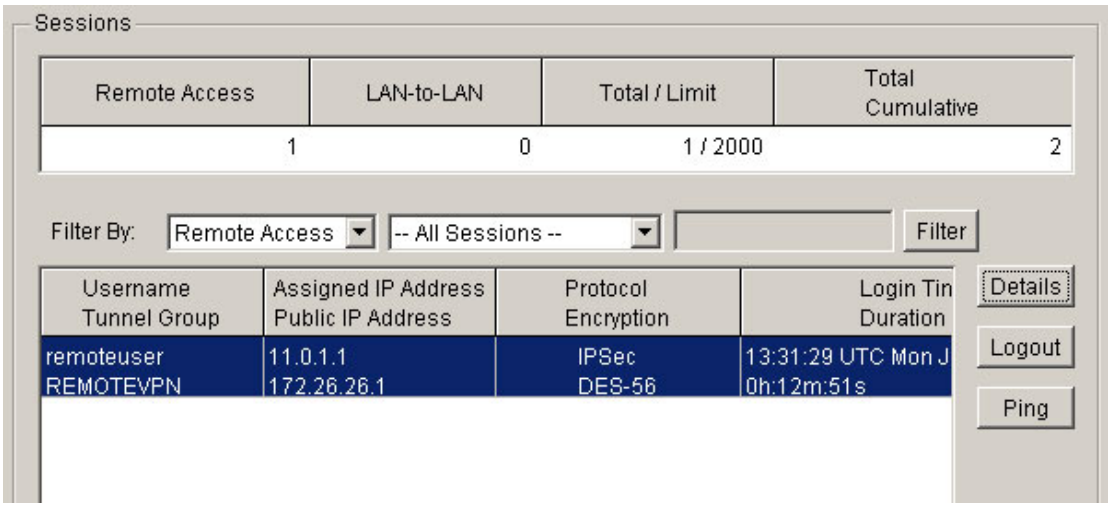
g. On the Student PC, use the browser to initiate an ASDM session.

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.

Lab 6.5.11b 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:

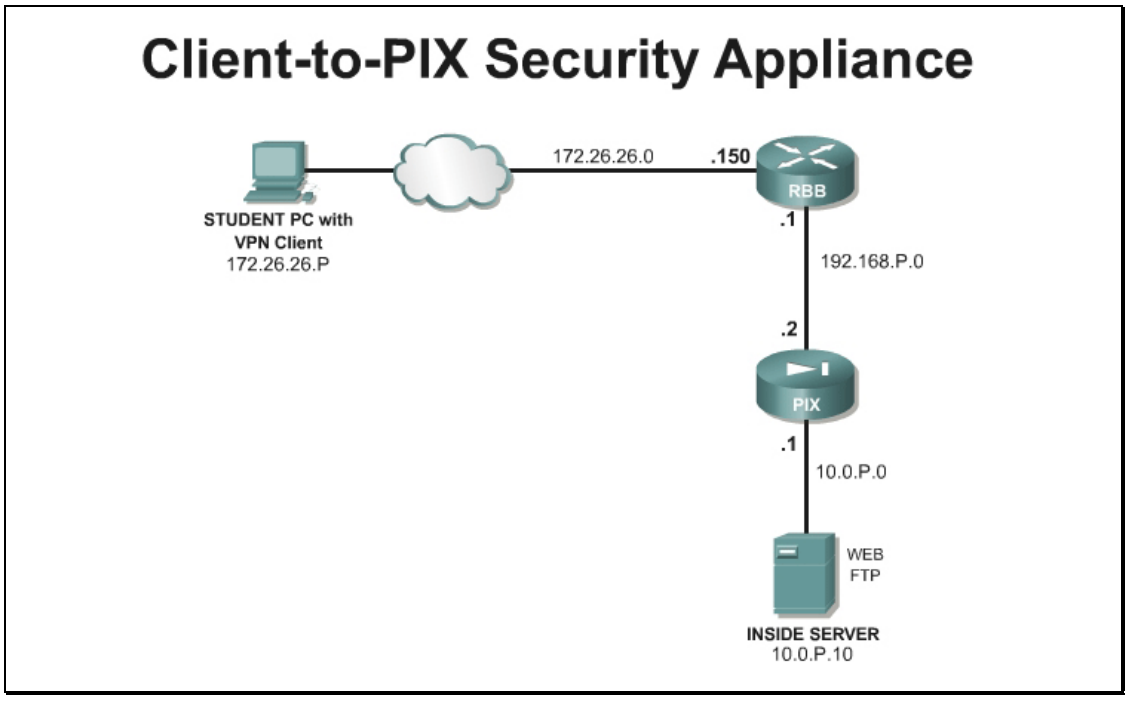
- Configure and Verify the PIX Easy VPN Server feature using CLI
- Install and configure the Cisco VPN Client on a Microsoft Windows end-user PC.
- Verify and Test the Cisco VPN Client remote access connection

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 [(*interface name***)]** *address_pool1* **[...***address_pool6***]**	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 *dynamic-map-name dynamic-seq-num* **set peer** *ip_address* **|** *hostname*	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 *map-name* **interface** *interface-name*	Use the **crypto map interface** command in global configuration mode to apply a previously defined crypto map set to an interface.
isakmp enable *interface-name*	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 {address | hostname | key-id *key-id-string* **| auto}**	To set the Phase 2 ID to be sent to the peer, use the **isakmp identity** command in global configuration mode.
isakmp policy *priority* **authentication {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.
nat (*real_interface***)** *nat_id real_ip* **[mask [dns] [outside] [[tcp]** *tcp_max_conns* **[***emb_limit***] [norandomseq]]] [udp** *udp_max_conns***]**	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 *nat_id* of 0 indicates that no address translation takes place for *real_ip*.
pre-shared-key *key*	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 *name* **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 *name* **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.

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 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:

```
Pix(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.

a. Choose **Start>Programs>Cisco Systems VPN Client>VPN Client**. The Cisco Systems VPN Client window opens.

b. Click **New**. The New Connection Entry window opens.

c. 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.

d. 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**

e. In the **Transport** tab, verify that Enable Transparent Tunneling is checked.

f. 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:

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 public interface IP address of the PIX Security Appliance, **192.168.P.2**.

d. Click **Connect**. Several messages flash by quickly. Complete the following sub-steps to establish the VPN tunnel:

i. When prompted for a username, enter admin.

ii. 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

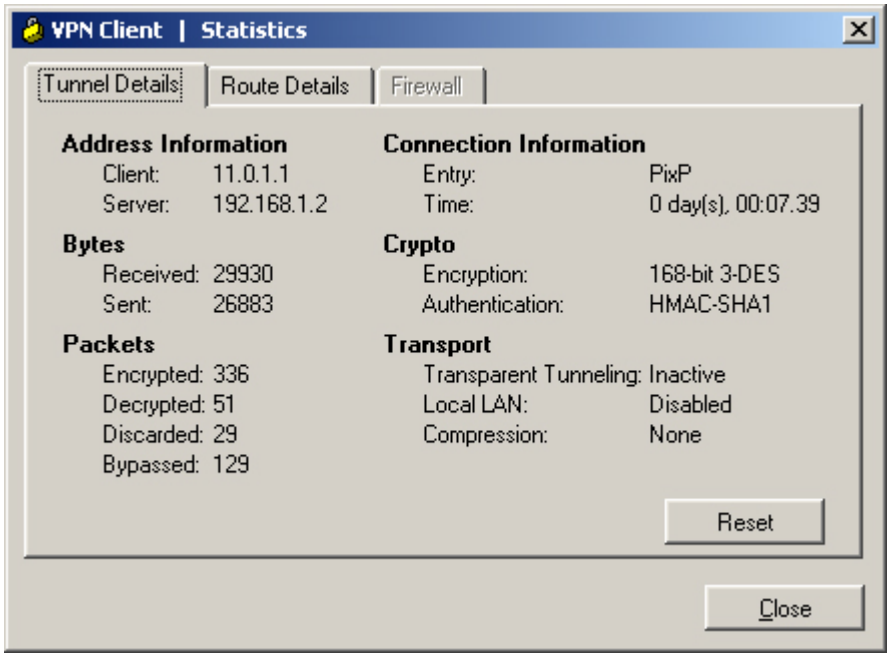
Complete the following steps to verify the IPSec connection:

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: 0xABA2D4D3 (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

Lab 7.4.5 Configure SNMP Messages on a Cisco Router

Objective

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

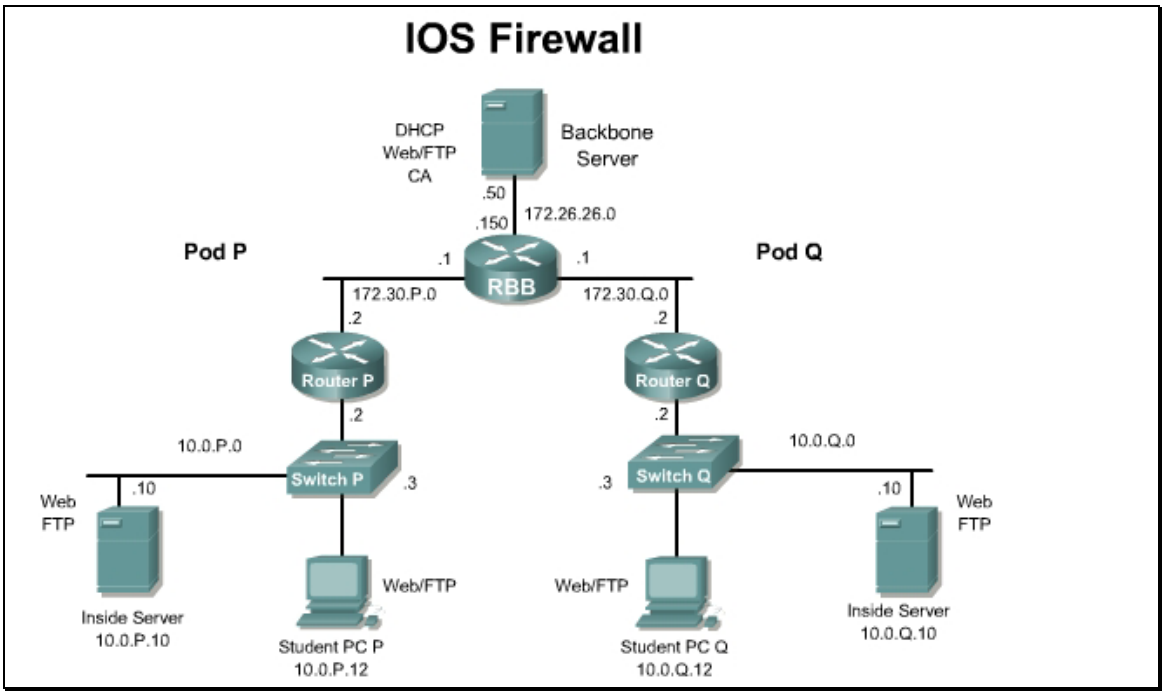
- Enable SNMP community string
- Establishing the Contact and location of the SNMP Agent
- Testing the configuration
- Limit SNMP to inside server
- Disable SNMP traps, SNMP service and associated access list

Scenario

A small company has recently expanded. The IT department is having problems maintaining logs, configuration changes, and so on. The security policy has been updated allowing SNMP management of key devices. SNMP access must be limited to key management stations.

Topology

This figure illustrates the lab network environment.



Preparation

Begin with the standard lab topology and verify the starting configuration on the pod router. Test the connectivity between the pod routers. Access the perimeter router console port using the terminal emulator on the Student PC. 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
- Kiwi Syslog Server

Additional materials

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

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a008030c762.html

http://www.kiwisyslog.com

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
no snmp-server	Disable SNMP.
show snmp	Monitors SNMP status.
snmp-server community	Defines the community access string.
snmp-server contact	Sets the system contact string.
snmp-server enable traps snmp	Enables the sending of traps and specifies the type of notification to be sent.
snmp-server host	Configures the recipient of an SNMP trap operation.
snmp-server location	Sets the system location string.

Step 1 Open Kiwi Syslog

Kiwi Syslog server can be used to receive syslog and SNMP messages from network equipment, including routers, switches, and workstations. Traps are sent when errors or specific events occur on the network.

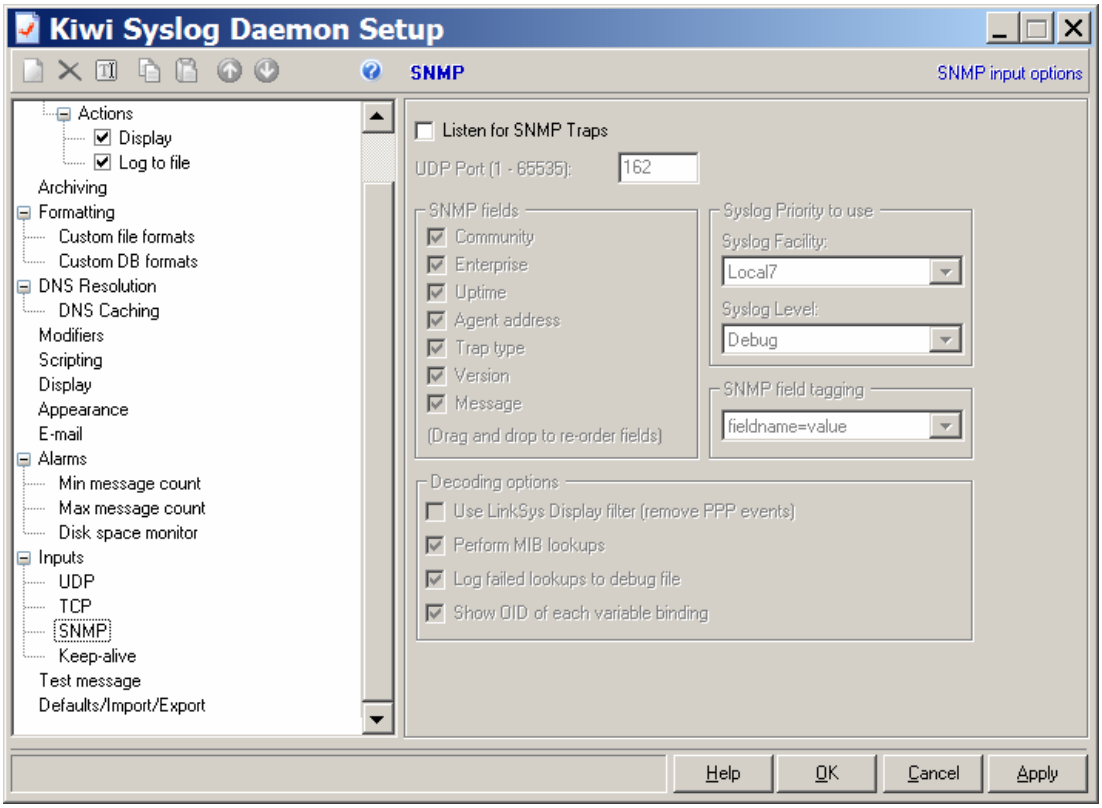
a. Go to the following website to download the free copy of Kiwi if needed,

   http://www.kiwisyslog.com

b. After opening the Kiwi application navigate to File>Setup or click on the Setup Icon  in the menu bar.

c. Go to **Inputs>SNMP**.

d. Check the **Listen for SNMP Traps**.



e. Notice that the Syslog server can be configured to send alerts automatically via email. Also, note the port number that SNMP uses for listening for traps, this will be used later.

f. Click the **OK** button.

Step 2 Enable SNMP Community String

a. Use an SNMP community string to define the relationship between the SNMP manager and the agent. The community string acts like a password to permit access to the agent on the router. The default values for these strings are “public” for read-only and “private” for read-write. These should always be changed to some other string values. Configure the community string by using the **`snmp-server community`** command. Let writemib be the read-write permission and readmib be the read-only permission.

```
RouterP(config)#snmp-server community writemib rw
RouterP(config)#snmp-server community readmib ro
```

Step 3 Establishing the Contact and Location of the SNMP Agent

a. Set the system contact and location of the SNMP agent. To do so, use the following commands in global configuration mode.

```
RouterP(config)#snmp-server contact Dial System Operator at beeper # 27345
RouterP(config)#snmp-server location Floor 4 Room 20
```

1. What command displays this information on a router?

_____

Answer: `show running-config, show startup config, show snmp`

Step 4 Configure the Router to Send Traps to a Host

a. To enable all the SNMP trap types at once, use the **snmp-server enable traps snmp** command.

```
RouterP(config)#snmp-server enable traps snmp
```

b. Specify to the router what host the trap notifications will be sent to by using the **snmp-server host** ***host community_string*** **udp-port** ***port_number*** command.

```
RouterP(config)#snmp-server host 10.0.P.12 writemib udp-port 162
```

c. Look at the applications main window to see the UDP-port that it is listening on.

1. If the default for an SNMP response is on port 162, what port is the request sent on?

_____

Answer: 161

2. Why is it important to know the SNMP port?

_____

Answer: The port information is important when configuring the router and the SNMP host to use the same port numbers.

Step 5 Testing the Configuration

a. Exit out of the router and log back in using the wrong password. After the failed attempts, log back into the router and issue the following commands:

```
RouterP(config)#interface fastEthernet 0/1
RouterP(config-if)#shutdown
RouterP(config-if)#no shutdown
```

b. Now check the Kiwi Syslog software

There will now be entries of traps sent from the router to the manager.

1. Where would information be found on the contact, location, and SNMP logging information for SNMP on the router besides startup-config and running-config?

_____

_____

Answer: The output of the **show snmp** command

Step 6 Limit SNMP to Inside Server

a. Limit the SNMP access to the inside server located at 10.0.P.12 by creating a restrictive access list along with a read-only community string.

```
RouterP(config)#no snmp-server community writemib rw
RouterP(config)#no snmp-server community readmib ro
RouterP(config)#access-list 70 permit 10.0.P.12
RouterP(config)#access-list 70 deny any
RouterP(config)#snmp-server community readmib ro 70
```

1. What command would be used to secure the SNMP **rw** access?

_____

Answer: RouterP(config)**#snmp-server community public rw 70**

b. Issue the following commands to generate SNMP traps:

```
RouterP(config)#int fa 0/1
RouterP(config-if)#shutdown
RouterP(config-if)#no shutdown
```

c. View the SNMP trap application.

1. Were the new traps displayed?

_____

Answer: Yes

d. If desired, compare the running configuration with the ending configuration provided for this lab.

Step 7 Disable SNMP Traps

a. Disable the SNMP traps on the router by using the following commands:

```
RouterP(config)#no snmp-server enable traps
RouterP(config)#no snmp-server system-shutdown
RouterP(config)#no snmp-server trap-auth
```

By disabling SNMP trap notifications, network performance will increase by freeing up bandwidth and eliminate unnecessary SNMP processing tasks.

Step 8 Disable SNMP and Associated Access List

a. Disable the SNMP and the associated access list by using the following commands:

```
RouterP(config)#no snmp-server
RouterP(config)#no access-list 70
```

1. When should the SNMP be disabled?

_____

_____

Answer: When the service is not being used.

Lab 7.4.6 Configure SNMP Monitoring of the PIX Security Appliance Using ASDM

Objective

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

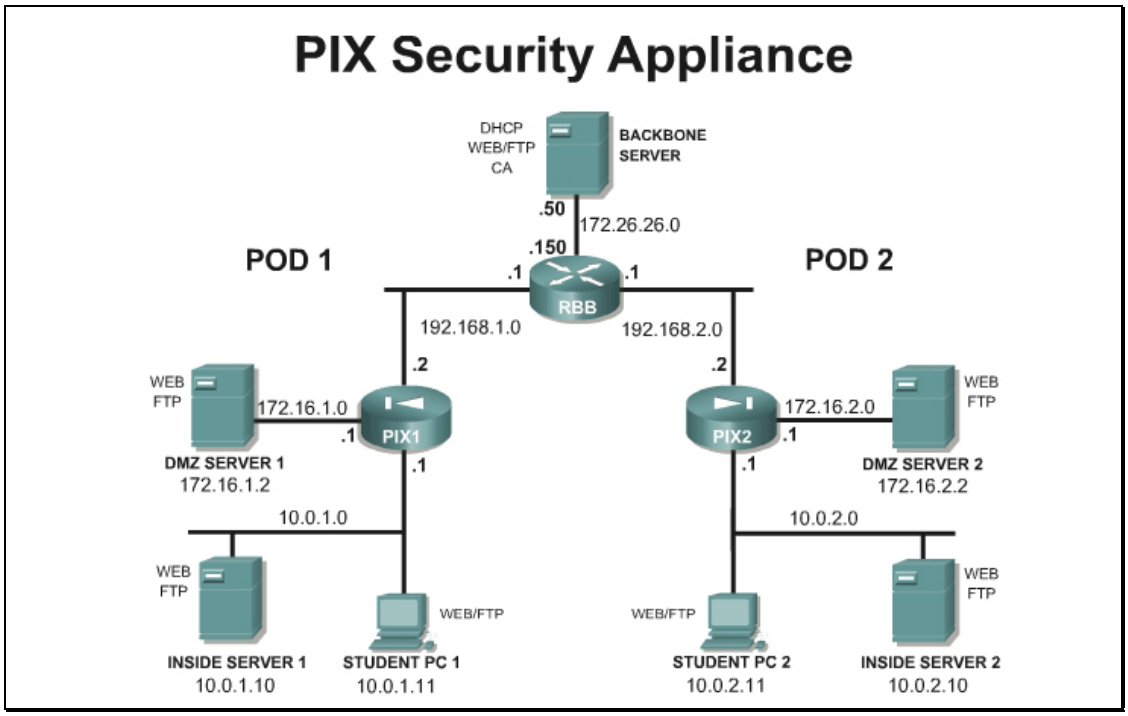
- Enable SNMP community string
- Establishing the Contact and location of the SNMP Agent
- Limit SNMP to inside server
- Testing the configuration

Scenario

A small company wants to monitor the PIX Security Appliance using SNMP.

Topology

This figure illustrates the lab network environment.



Preparation

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

Download SNMPwalk for Windows from http://www.bradford-sw.com/board/board.cgi?id=BSI_Tools&action=view&gul=13&page=1&go_cnt=0

Tools and Resources

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

- Standard PIX Security Appliance lab topology
- Console cable
- HyperTerminal
- SNMPwalk

Additional Materials

For more information on PIX SNMP go to:

http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_configuration_guide_chapter09186a0080450bf7.html#wp1042028

Step 1 Verify SNMP Operation

Complete the following steps to verify that SNMPWalk is operational

a. Download and install SNMPWalk in a folder with the name **SNMP** on C:\

b. On the Student PC, open a command prompt.

c. Get to a root C:\> by entering **cd **

d. Go to the snmp directory and verify the files

```
C:\> cd snmp
C:\SNMP>dir
Volume in drive C has no label.
 Volume Serial Number is A49B-A399

 Directory of C:\SNMP

06/25/2004  03:05 PM    <DIR>          .
06/25/2004  03:05 PM    <DIR>          ..
04/03/1999  08:57 AM            99,840 libsnmp.dll
04/03/1999  08:58 AM            11,776 snmpget.exe
04/03/1999  08:59 AM            11,776 snmpwalk.exe
               3 File(s)        123,392 bytes
               2 Dir(s)  17,925,615,616 bytes free
C:\SNMP>
```


e. Perform SNMP reconnaissance using SNMPWalk. Some output has been omitted.

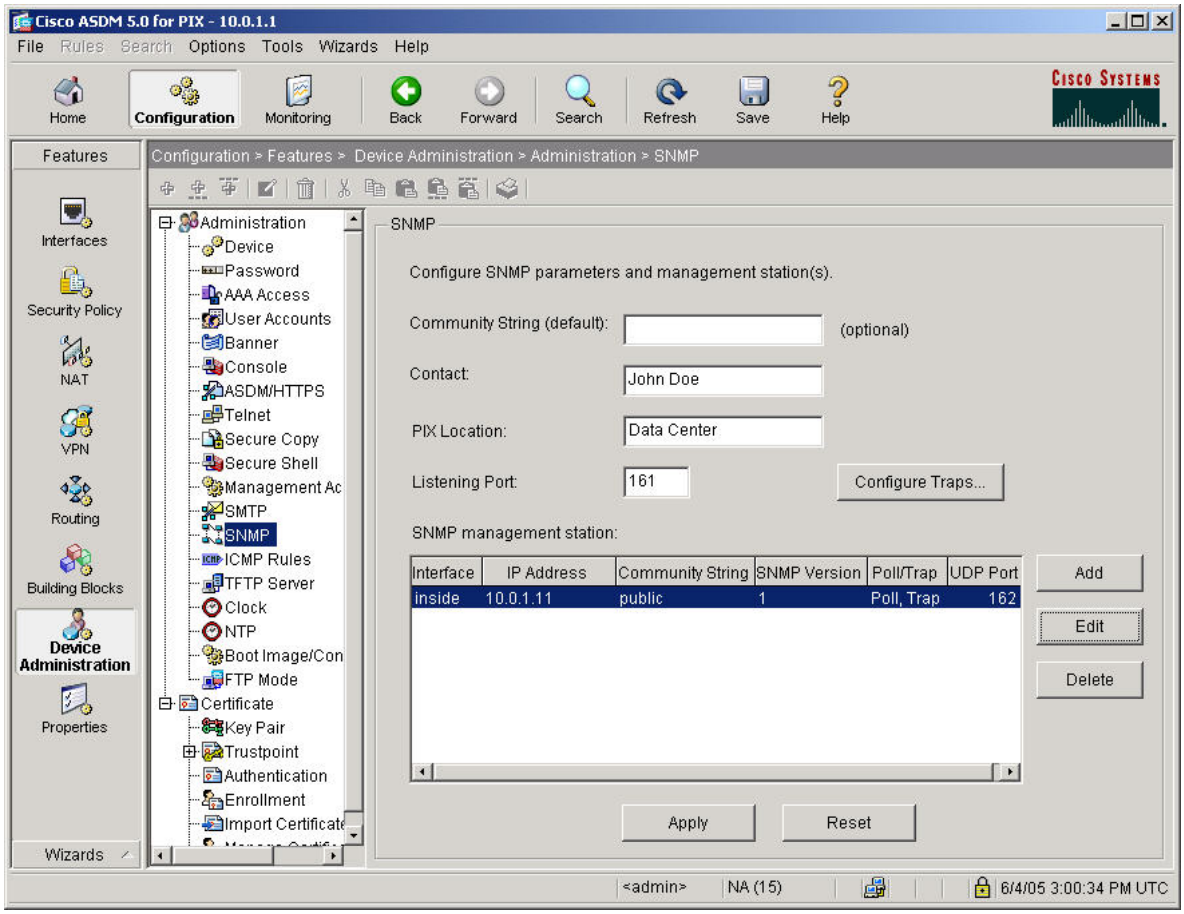
```
C:\SNMP> snmpwalk -v 1 10.0.P.1 public
Timeout: No Response from 10.0.1.1
C:\SNMP>
```

Step 2 Configure the PIX Security Appliance to Send SNMP Messages

Complete the following steps to configure the PIX Security Appliance to send SNMP messages to a SNMP server:

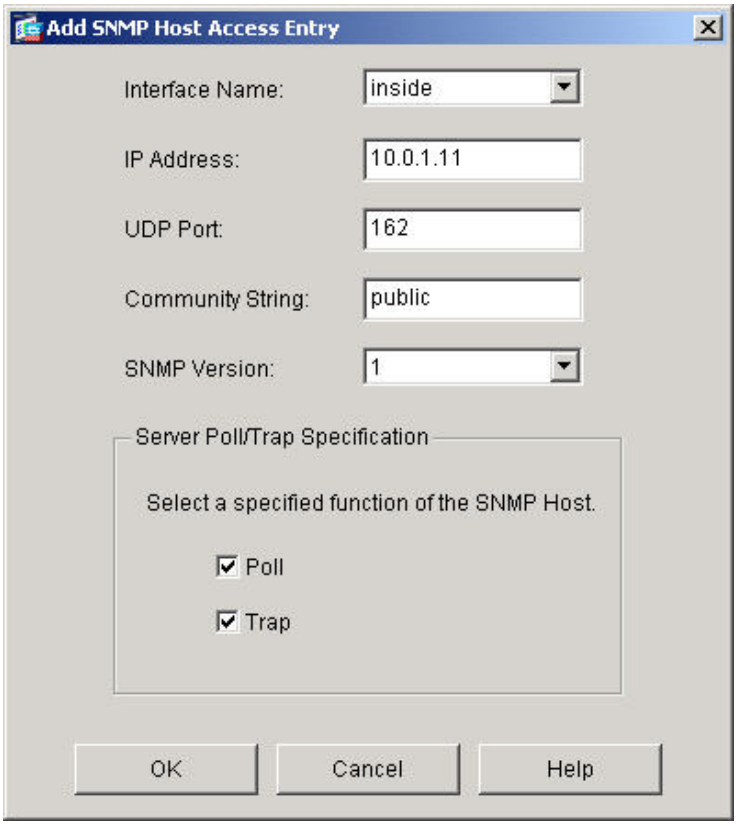
a. Initiate an ASDM session with the PIX Security Appliance.

b. Navigate to **Configuration>Features>Device Administration>Administration>SNMP**.



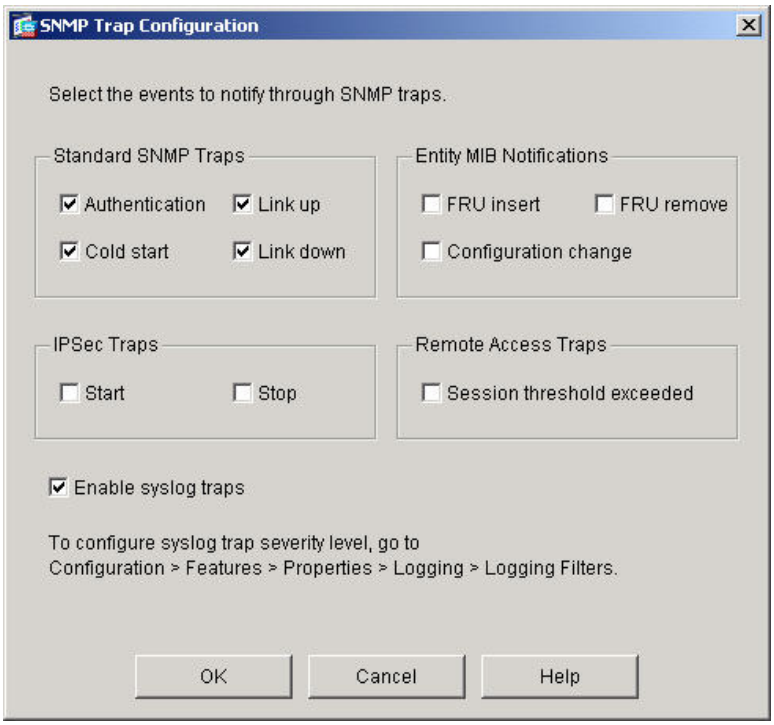
c. Configure a System administrator name and location.

d. Click the **Add** button to configure the Student PC address as the SNMP management station. Select **inside** for the interface and verify that both **Poll** and **Trap** functions are checked.



e. Click the **OK** button to return to the SNMP window.

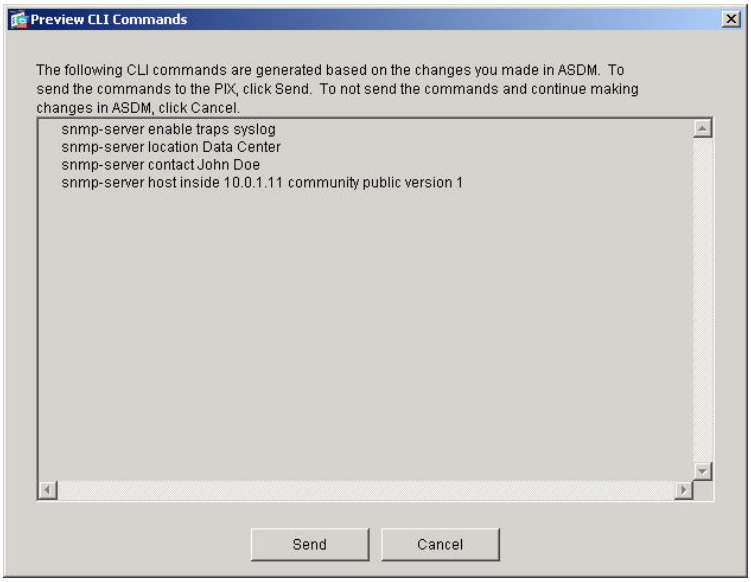
f. Click the **Configure Traps** button to configure the SNMP trap properties. Check the **Enable syslog traps** button. Click the **OK** button A warning appears with a notification regarding the logging trap level.



g. Click the **OK** button to return to the SNMP window.

h. Click the **Apply** button.

i. If the **Preview CLI Commands** window appears, click the **Send** button to continue.

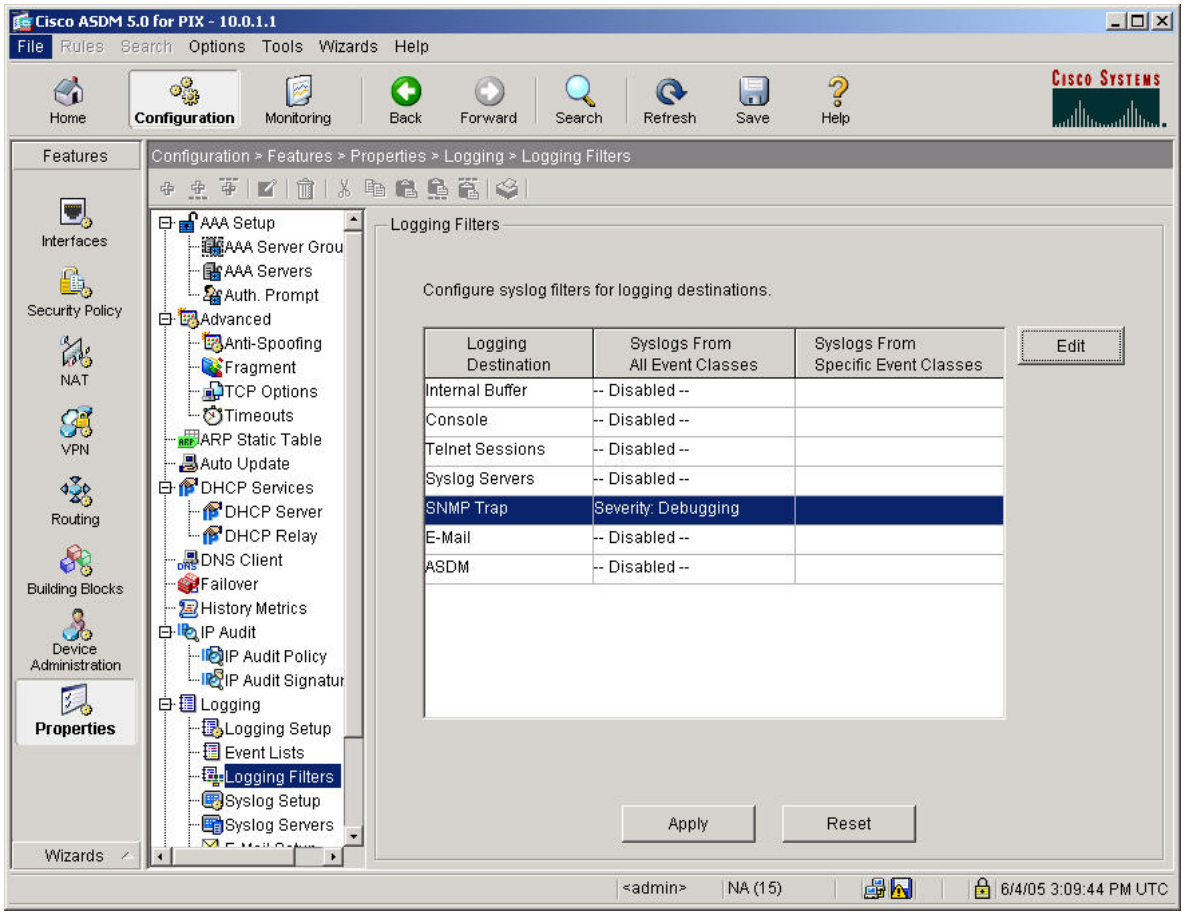


j. Navigate to **Configuration>Features>Properties>Logging>Logging Filters**.

k. Select **SNMP Trap** from the **Logging Filters** group. Click the **Edit** button to bring up the **Edit Logging Filters** window.

l. Select the **Filter on severity** radio button and then select **Debugging** from the drop down menu.

m. Click the **OK** button to return to the **Logging Filters** window.



n. Click the **Apply** button.

o. If the **Preview CLI Commands** window appears, click the **Send** button to continue.

Step 3 Verify SNMP Operation

Complete the following steps to verify SNMP is operational

a. Download and install SNMPWalk in a SNMP folder on `C:\`

b. On the Student PC, open a command prompt.

c. Get to a root C:\> by entering **`cd \`**

d. Go to the snmp directory.

```
C:\> cd snmp

C:\SNMP>
```

e. Perform SNMP reconnaissance using snmpwalk.exe. Some output has been omitted.

```
C:\SNMP>snmpwalk -v 1 10.0.1.1 public

.iso.3.6.1.2.1.1.1.0 = "Cisco PIX Firewall Version 7.0(1)."

.iso.3.6.1.2.1.1.2.0 = OID: .iso.3.6.1.4.1.9.1.451

.iso.3.6.1.2.1.1.3.0 = Timeticks: (128200) 0:21:22.00

.iso.3.6.1.2.1.1.4.0 = "John Doe"

.iso.3.6.1.2.1.1.5.0 = "Pix1.cisco.com"

.iso.3.6.1.2.1.1.6.0 = "Data center"

.iso.3.6.1.2.1.2.2.1.2.1 = "Cisco PIX Security Appliance 'outside'
interface"

.iso.3.6.1.2.1.2.2.1.2.2 = " Cisco PIX Security Appliance 'inside'
interface"

.iso.3.6.1.2.1.2.2.1.2.3 = " Cisco PIX Security Appliance 'dmz'
interface"

.iso.3.6.1.2.1.2.2.1.4.1 = 1500

.iso.3.6.1.2.1.2.2.1.4.2 = 1500

.iso.3.6.1.2.1.2.2.1.4.3 = 1500

.iso.3.6.1.2.1.2.2.1.5.1 = Gauge: 100000000

.iso.3.6.1.2.1.2.2.1.5.2 = Gauge: 100000000

.iso.3.6.1.2.1.2.2.1.5.3 = Gauge: 100000000

.iso.3.6.1.2.1.2.2.1.6.1 =  Hex: 00 0B FD 81 EB 83

.iso.3.6.1.2.1.2.2.1.6.2 =  Hex: 00 0B FD 81 EB 84

.iso.3.6.1.2.1.2.2.1.6.3 =  Hex: 00 02 B3 BB D0 D0

.iso.3.6.1.2.1.2.2.1.9.1 = Timeticks: (3531000000) 408 days,
16:20:00.00

.iso.3.6.1.2.1.2.2.1.9.2 = Timeticks: (3545000000) 410 days,
7:13:20.00

.iso.3.6.1.2.1.2.2.1.9.3 = Timeticks: (3557000000) 411 days,
16:33:20.00

.iso.3.6.1.2.1.4.20.1.1.10.0.1.1 = IpAddress: 10.0.1.1

.iso.3.6.1.2.1.4.20.1.1.172.16.1.1 = IpAddress: 172.16.1.1
```



```
.iso.3.6.1.2.1.4.20.1.1.192.168.1.2 = IpAddress: 192.168.1.2
.iso.3.6.1.2.1.4.20.1.3.10.0.1.1 = IpAddress: 255.255.255.0
.iso.3.6.1.2.1.4.20.1.3.172.16.1.1 = IpAddress: 255.255.255.0
.iso.3.6.1.2.1.4.20.1.3.192.168.1.2 = IpAddress: 255.255.255.0
```


Lab 8.2.4 Configure LAN-Based Failover Between Two PIX Security Appliances (OPTIONAL)

Objectives:

This is a two part lab. In the first part, students will configure and test active/standby failover. In the second part of this lab, students will configure and test active/active failover.

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

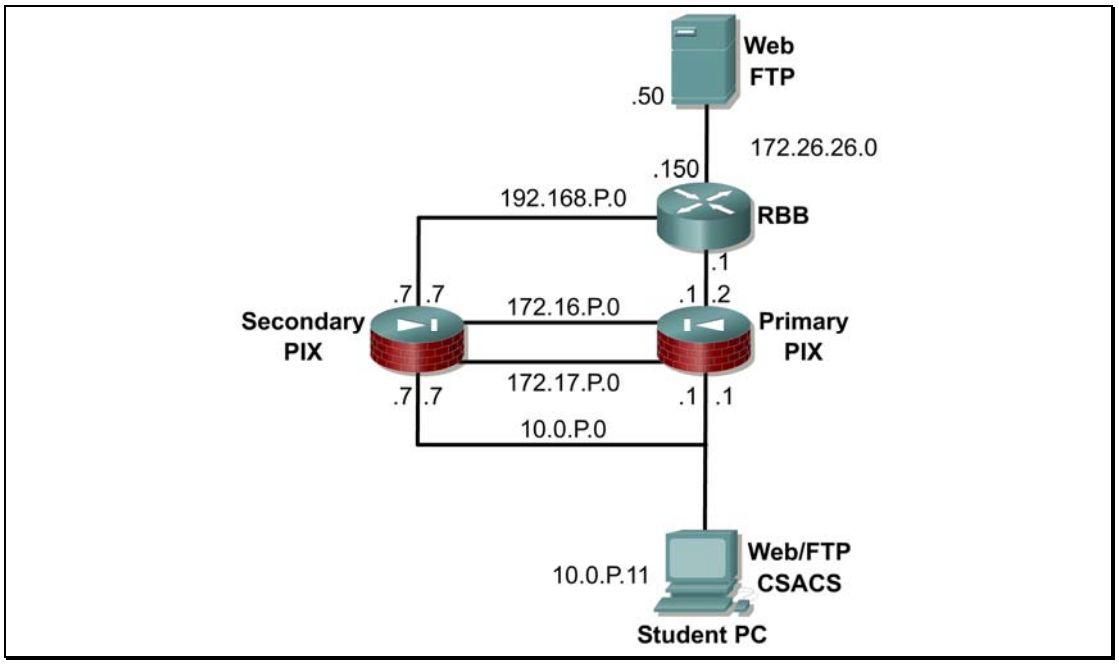
- Configure the primary PIX Security Appliance for LAN-based active/standby failover.
- Configure the secondary PIX Security Appliance for LAN-based active/standby failover.
- Test LAN-based active/standby failover.
- Configure the primary PIX Security Appliance for LAN-based active/active failover.
- Configure the secondary PIX Security Appliance for LAN-based active/active failover.
- Test LAN-based active/active failover.

Scenario

In an enterprise network, network outages are not an option. Many businesses and service providers must maintain continuous service, otherwise the monetary loss can be high. In addition to redundant routers, the PIX supports failover capabilities.

Topology

This figure illustrates the lab network environment used for the active/standby failover portion of this lab exercise:



Preparation

Begin with the failover 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:

- One primary unrestricted(UR) PIX Security Appliance
- One secondary PIX Security Appliance (with a Failover Only (FO), Failover Only Active-Active (FO_AA), or Unrestricted (UR) license.)
- Console cable
- HyperTerminal
- One student PC
- One Backbone Server

Note A least one of the PIX Security Appliance units must have an unrestricted (UR) license. The other unit can have a Failover Only (FO) license, a Failover Only Active-Active (FO_AA) license, or another UR license. Units with a Restricted license cannot be used for failover, and two units with FO or FO_AA licenses cannot be used together as a failover pair.

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/ps2120/products_configuration_guide_chapter09186a008045247e.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
changeto {system | context *name***}**	To change between security contexts and the system, use the **changeto** command in privileged EXEC mode.
clear configure failover	To remove **failover** commands from the configuration and restore the defaults, use the **clear configure failover** command in global configuration mode.
clear configure interface [*physical_interface***[.***subinterface***] |** *mapped_name* **|** *interface_name***]**	To clear the interface configuration, use the **clear configure interface** command in global configuration mode.
failover	To enable failover, use the **failover** command in global configuration mode.
failover active	To switch a standby security appliance or failover group to the active state, use the **failover active** command in privileged EXEC mode.
failover group [group *group_id***]**	To configure an Active/Active failover group, use the **failover group** command in global configuration mode.
failover interface ip *if_name ip_address mask* **standby** *ip_address*	To specify the IP address and mask for the failover interface and the Stateful Failover interface, use the **failover interface ip** command in global configuration mode.
failover lan enable	To enable lan-based failover, use the **failover lan enable** command in global configuration mode.
failover lan interface *if_name phy_if*	To specify the interface used for failover communication, use the **failover lan interface** command in global configuration mode.
failover key *secret*	To specify the failover shared secret for encrypted and authenticated communication between failover pairs, use the **failover key** command in global configuration mode.
failover lan unit {primary | secondary}	To configure the PIX Security Appliance as either the primary or secondary unit in a LAN failover configuration, use the **failover lan unit** command in global configuration mode.
failover link *if_name* **[***phy_if***]**	To specify the Stateful Failover interface, use the **failover link** command in global configuration mode.

mode {single | multiple} [noconfirm]	To set the security context mode to single or multiple, use the **mode** command in global configuration mode.
show context [*name* **| detail | count]**	To show context information including allocated interfaces and the configuration file URL, the number of contexts configured, or from the system execution space, a list of all contexts, use the **show context** command in privileged EXEC mode.
show failover	To display information about the failover status of the unit, use the **show failover** command in privileged EXEC mode.
show mode	To show the security context mode for the running software image and for any image in Flash memory, use the **show mode** command in privileged EXEC mode.

Part I: Configure Active/Standby Failover

Step 1 Configure the Primary PIX Security Appliance for LAN-Based Stateful Failover to the Secondary PIX Security Appliance

Complete the following steps to configure the primary PIX Security Appliance for failover to the secondary PIX Security Appliance:

a. Save the current configuration

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

b. Step 2 IMPORTANT: Copy the current configuration to Flash: The same configuration will be reloaded at the end of this lab.

```
PixP(config)# copy running-config flash:/pre_fo_lab.cfg
```

c. Step 3 Clear the existing configuration for the DMZ interface, interface ethernet2. In this lab, interface e2 will be used for the failover link.

```
PixP(config)# clear configure interface ethernet2
```

d. Step 4 Enable the interface used for the failover link:

```
PixP(config)# interface ethernet2
PixP(config-if)# no shutdown
PixP(config-if)# exit
```

e. Step 5 Assign a standby IP address for each interface:

```
PixP(config)# interface ethernet0
PixP(config-if)# ip address 192.168.P.2 255.255.255.0 standby
192.168.P.7
PixP(config-if)# exit
PixP(config)# interface ethernet1
PixP(config-if)# ip address 10.0.P.1 255.255.255.0 standby 10.0.P.7
PixP(config-if)# exit
```

(where P = pod number)

f. Step 6 Use the **failover lan interface** command to specify the name of the dedicated failover interface:

```
PixP(config)# failover lan interface MYFAILOVER ethernet2
INFO: Non-failover interface config is cleared on Ethernet2 and is
sub-interfaces
```

(where P = pod number)

g. Step 7 Specify the failover link IP addressing:

```
PixP(config)# failover interface ip MYFAILOVER 172.16.P.1
255.255.255.0 standby 172.16.P.7
```

(where P = pod number)

h. Enable encryption and authentication of LAN-based failover messages between PIX Security Appliances:

```
PixP(config)# failover lan key 1234567
```

(where P = pod number)

i. Specify the primary PIX security Appliance to use for LAN-based failover:

```
PixP(config)# failover lan unit primary
```

(where P = pod number)

j. Enable LAN-based failover:

```
PixP(config)# failover lan enable
```

(where P = pod number)

k. Enable failover:

```
PixP(config)# failover
```

l. Save all changes to Flash memory:

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

m. Wait for the failover initialization process to complete. The following message will be displayed on the PIX Security Appliance console:

```
No Response from Mate
```

n. Make sure that the primary PIX Security Appliance is enabled for failover by using the **show failover** command:

```
PixP(config)# show failover
Failover On
Cable status: N/A - LAN-based failover enabled
Failover unit Primary
Failover LAN Interface: myfailover Ethernet2 (up)
Unit Poll frequency 15 seconds, holdtime 45 seconds
Interface Poll frequency 15 seconds
Interface Policy 1
Monitored Interfaces 0 of 250 maximum
Last Failover at: 18:03:38 UTC Nov 12 2004
This host: Primary - Active
Active time: 30 (sec)
```



```
Interface outside (192.168.1.2): Normal (Waiting)
Interface inside (10.0.1.1): Normal (Waiting)
Other host: Primary - Failed
Active time: 0 (sec)
Interface outside (192.168.1.7): Unknown (Waiting)
Interface inside (10.0.1.7): Unknown (Waiting)
Stateful Failover Logical Update Statistics
Link : Unconfigured.
```

o. Verify that the SuperServer can be pinged:

```
C:\> ping 172.26.26.50
```

p. Verify that the backbone router is available by Telnet:

```
C:\> telnet 192.168.P.1
```

(where P = pod number)

Step 2 Configure the Secondary PIX Security Appliance for LAN-Based Failover

Complete the following steps to prepare the secondary PIX Security Appliance for failover. The instructor will provide the instructions for accessing the secondary PIX.

a. Ask the instructor to power up the secondary PIX Security Appliance.

b. Complete the following substeps on the secondary PIX Security Appliance:

   i. When prompted to configure the secondary PIX Security Appliance through interactive prompts, press **<Control Z>** to escape.

   ii. Enter configuration mode.

c. Enable the interface used for the failover link:

```
PixP(config)# interface ethernet2
PixP(config-if)# no shutdown
PixP(config-if)# exit
```

d. Use the failover lan interface command to specify the name of the dedicated failover interface:

```
PixP(config)# failover lan interface MYFAILOVER ethernet2
```

Note: Non-failover interface config is cleared on Ethernet2 and its sub-interfaces

(where P = pod number)

e. Specify the failover link IP addressing:

```
PixP(config)# failover interface ip MYFAILOVER 172.16.P.1
255.255.255.0 standby 172.16.P.7
```

(where P = pod number)

f. Enable encryption and authentication of LAN-based failover messages between PIX security Appliances:

```
PixP(config)# failover lan key 1234567
```

(where P = pod number)

g. Specify the secondary PIX security Appliance to use for LAN-based failover:

```
PixP(config)# failover lan unit secondary
```

(where P = pod number)

h. Enable LAN-based failover:

```
PixP(config)# failover lan enable
```

(where P = pod number)

i. Enable failover:

```
PixP(config)# failover
```

j. Wait for the failover initialization process to complete. The following messages will be displayed on the secondary PIX Security Appliance console:

```
Detected an Active mate
Beginning configuration replication from mate.
End configuration replication from mate.
```

Step 3 Test LAN-Based Stateful Failover

Complete the following steps to test LAN-based stateful failover:

a. Switch to the primary PIX console. After the message “End Configuration Replication to mate” is displayed on the primary PIX Security Appliance console, verify that failover is running and the secondary failover device is recognized:

```
PixP(config)# show failover
Failover On
Cable status: N/A - LAN-based failover enabled
Failover unit Primary
Failover LAN Interface: myfailover Ethernet2 (up)
Unit Poll frequency 15 seconds, holdtime 45 seconds
Interface Poll frequency 15 seconds
Interface Policy 1
Monitored Interfaces 0 of 250 maximum
Last Failover at: 18:03:38 UTC Nov 12 2004
This host: Primary - Active
Active time: 645 (sec)
Interface outside (192.168.1.2): Normal
Interface inside (10.0.1.1): Normal
Other host: Secondary – Standby Ready
Active time: 0 (sec)
Interface outside (192.168.1.7): Normal
Interface inside (10.0.1.7): Normal
Stateful Failover Logical Update Statistics
Link : Unconfigured.
```

b. Start a continuous ping to 172.26.26.50:

```
C:\ ping 172.26.26.50 –t
```

c. From the student PC open a telnet session to the backbone router

```
C:\>telnet 192.168.P.1
User Access Verification
```



```
Password: cisco
RBB> enable
Password: <cr>
Password: <cr>
Password: <cr>
% Bad passwords
RBB>
```

d. Reload the primary PIX security Appliance:

```
PixP(config)# reload
```

(where P = pod number)

e. When asked to confirm the reload, press **Enter**.

f. Notice the ping request times out and eventually resume after a configurable delay. After the successful pings return, try to access `rbb>enable`. The connection to `rbb>` should be lost. Stateful Failover is not enabled. Stop the pings cntrl-C

g. After the primary PIX has completely rebooted, enter the show failover command on the primary Security Appliance and observe the new role and the new addresses displayed on the primary PIX:

```
PixP(config)# show failover
Failover On
Cable status: N/A - LAN-based failover enabled
Failover unit Primary
Failover LAN Interface: myfailover Ethernet2 (up)
Unit Poll frequency 15 seconds, holdtime 45 seconds
Interface Poll frequency 15 seconds
Interface Policy 1
Monitored Interfaces 0 of 250 maximum
Last Failover at: 18:03:38 UTC Nov 12 2004
This host: Primary – Standby Ready
Active time: 645 (sec)
Interface outside (192.168.P.7): Normal (waiting)
Interface inside (10.0.P.7): Normal (waiting)
Other host: Secondary – Active
Active time: 0 (sec)
Interface outside (192.168.P.2): Normal
Interface inside (10.0.P.1): Normal
Stateful Failover Logical Update Statistics
Link : Unconfigured.
```

h. Make the primary PIX Security Appliance the active PIX Security Appliance by using the **`failover active`** command. Make sure to connect to the console port of the primary PIX Security Appliance.

```
PixP(config)# failover active
```



```
Switching to Active.
```

(where P = pod number)

i. Step 9 Enable Stateful failover on the primary PIX.

```
PixP(config)# failover link myfailover
```

(where P = pod number)

i. Save the configuration on the primary.

ii. Verify that the stateful failover is enabled by using the **show failover** command. The stateful failover statistics should be present.

```
PixP(config)# show failover
Failover On
Cable status: N/A - LAN-based failover enabled
Failover unit Primary
Failover LAN Interface: myfailover Ethernet3 (up)
Unit Poll frequency 15 seconds, holdtime 45 seconds
Interface Poll frequency 15 seconds
Interface Policy 1
Monitored Interfaces 0 of 250 maximum
Last Failover at: 18:03:38 UTC Nov 12 2004
This host: Primary – Active
Active time: 140 (sec)
Interface outside (192.168.P.2): Normal
Interface inside (10.0.P.1): Normal
Other host: Secondary – Standby Ready
Active time: 3105 (sec)
Interface outside (192.168.P.7): Normal
Interface inside (10.0.P.7): Normal
Stateful Failover Logical Update Statistics
Link : myfailover Ethernet3 (up)
Stateful Obj xmit xerr rcv rerr
General 0 0 0 0
sys cmd 4 0 4 0
up time 0 0 0 0
RPC services 0 0 0 0
TCP conn 0 0 0 0
UDP conn 0 0 0 0
ARP tbl 0 0 8 0
Xlate_Timeout 0 0 0 0
Logical Update Queue Information
Cur Max Total
```



```
Recv Q: 0 1 4
Xmit Q: 0 2 38
```

(where P = pod number)

j. Start a continuous ping to 172.26.26.50:

```
C:\ ping 172.26.26.50 -t
```

k. From the student PC, open a telnet session to the backbone router

```
C:\>telnet 192.168.P.1
User Access Verification
Password: cisco
RBB> enable
Password: <cr>
Password: <cr>
Password: <cr>
% Bad passwords
RBB>
```

l. Reload the primary PIX Security Appliance:

```
PixP(config)# reload
```

(where P = pod number)

m. When asked to confirm the reload, press **Enter**.

n. Notice that the ping request times out and eventually resume after a delay.

o. After the pings resume, try to access `rbb>enable` through the telnet session. The connection to `rbb>` should still be present. Stateful Failover is enabled.

```
RBB> enable
Password: <cr>
Password: <cr>
Password: <cr>
% Bad passwords
RBB>
```

p. Stop the pings with **Ctrl-C**. Close the telnet session.

Step 4 Make the Primary PIX Security Appliance Active

Complete the following steps to make the primary PIX Security Appliance the active PIX Security Appliance:

a. Make the primary PIX Security Appliance the active PIX Security Appliance by using the failover active command. Make sure to connect to the console port of the primary PIX Security Appliance.

```
PixP(config)# failover active
```

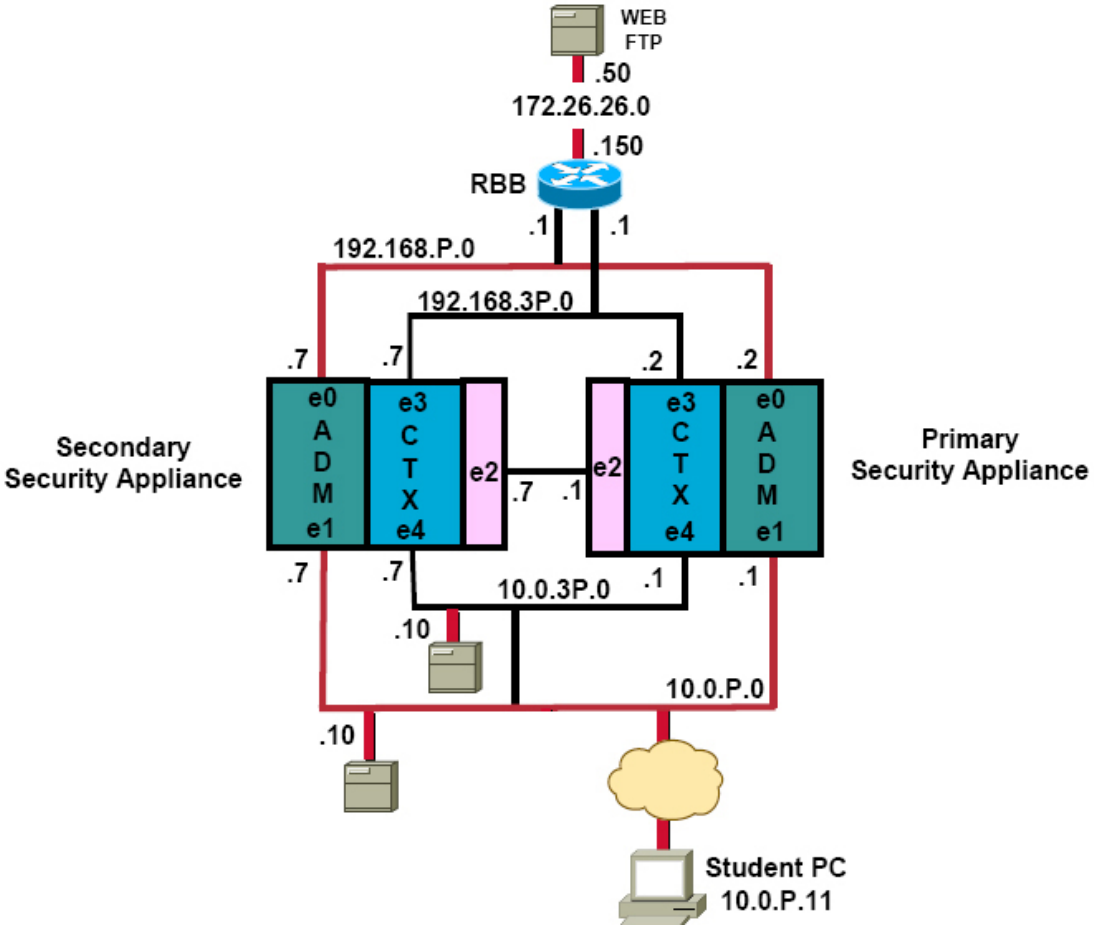
(where P = pod number)

b. Verify that the failover active command worked by using the **show failover** command. The primary PIX Security Appliance should show that it is in active mode and the secondary PIX Security Appliance should show that it is in the standby mode.


```
PixP(config)# show failover
Failover On
Cable status: N/A - LAN-based failover enabled
Failover unit Primary
Failover LAN Interface: myfailover Ethernet3 (up)
Unit Poll frequency 15 seconds, holdtime 45 seconds
Interface Poll frequency 15 seconds
Interface Policy 1
Monitored Interfaces 0 of 250 maximum
Last Failover at: 18:03:38 UTC Nov 12 2004
This host: Primary – Active
Active time: 140 (sec)
Interface outside (192.168.P.2): Normal
Interface inside (10.0.P.1): Normal
Other host: Secondary – Standby Ready
Active time: 3105 (sec)
Interface outside (192.168.P.7): Normal
Interface inside (10.0.P.7): Normal
stateful Failover Logical Update Statistics
Link : myfailover Ethernet3 (up)
Stateful Obj xmit xerr rcv rerr
General 0 0 0 0
sys cmd 224 0 224 0
up time 0 0 0 0
RPC services 0 0 0 0
```


Part II: Configure Active/Active Failover

The following figure displays the configuration that will be completed in the active/active failover portion of this lab exercise. There is a primary and secondary Security Appliance. Each Security Appliance is composed of two contexts, **admin** and **ctx1** contexts. In active/active failover, only one of the **admin** and one of the **ctx1** contexts will be active at any one time.



Step 1 Enable Multiple Context Mode

By default, a PIX Security Appliance operates in single mode. Active/active failover requires the PIX Security Appliance to operate with multiple mode with virtual security contexts. Complete the following steps to enable multiple context mode.

a. On the primary PIX Security Appliance, verify security context is a licensed feature of this PIX Security Appliance.

```
PixP(config)# show version

…….

License Feature of this Platform:

……..

Security Contexts :5
```

b. Check the current mode of the PIX Security Appliance:

```
PixP(config)# show mode
```



```
Security appliance mode: single
```

c. Enable Multiple Context mode:

```
PixP(config)# mode multiple
WARNING: This command will change the behavior of the device
WARNING: This command will initiate a Reboot
Proceed with change mode? [confirm] <Enter>
Convert the system configuration? [confirm] <Enter>
The old running configuration file will be written to flash
The admin context configuration will be written to flash
The new running configuration file was written to flash
```

Step 2 Confirm Multiple Context Mode

When a PIX Security Appliance changes to a multiple mode configuration, the default multiple mode configuration is two security contexts, system and admin contexts. The PIX Security Appliance boots into the system context. In the system context, the administrator can view and create contexts. They can also allocate system resources and configure failover links. Complete the following steps to examine the default multiple mode environment:

a. After the primary PIX Security Appliance re-boots, confirm the PIX Security Appliance is in multiple context mode:

```
PixP# show mode
Security context mode: multiple
```

b. Confirm the PIX Security Appliance saved the original configuration as `old_running.cfg`:

```
PixP# show flash
Directory of flash:/
3 -rw- 5031936 08:30:41 Aug 12 2004 pix_7_82.bin
8 -rw- 2028 08:30:41 Aug 12 2004 old_running.cfg
9 -rw- 1682 08:30:41 Aug 12 2004 admin.cfg
```

c. Examine the current security contexts.

```
PixP# show context
Context Name Interfaces URL
*admin Ethernet0, Ethernet1 flash:/admin.cfg
Total active Security Contexts: 1
PixP# show context detail
Context "system", is a system resource
Config URL: startup-config
Real Interfaces:
Mapped Interfaces: Ethernet0, Ethernet1, Ethernet2, Ethernet3,
Ethernet4, Ethernet5
Flags: 0x00000019, ID: 0
Context "admin", has been created, but initial ACL rules not
complete
Config URL: flash:/admin.cfg
```



```
Real Interfaces: Ethernet0, Ethernet1
Mapped Interfaces: Ethernet0, Ethernet1
Flags: 0x00000013, ID: 1
Context "null", is a system resource
Config URL: ... null ...
Real Interfaces:
Mapped Interfaces:
Flags: 0x00000009, ID: 257
```

Step 3 Configure the Failover Link

A failover link can only be configured in system context. In this task, remove the previous active/standby failover configuration on interface Ethernet 2. Re-configure it as an active/active failover link. Complete the following steps to configure the failover link in the system context:

a. Clear the existing failover configuration

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

b. Enable the interface used for the failover link:

```
PixP(config)# interface ethernet2
PixP(config-if)# no shutdown
PixP(config-if)# exit
```

c. Use the failover lan interface command to specify the name of the dedicated failover interface:

```
PixP(config)# failover lan interface MYFAILOVER ethernet2
INFO: Non-failover interface config is cleared on Ethernet3 and its
sub-interfaces
```

(where P = pod number)

d. Enable LAN-based failover:

```
PixP(config)# failover lan enable
```

(where P = pod number)

e. Specify the failover link IP addressing:

```
PixP(config)# failover interface ip MYFAILOVER 172.16.P.1
255.255.255.0 standby 172.16.P.7
```

(where P = pod number)

f. Enable stateful failover:

```
PixP(config)# failover link MYFAILOVER ethernet2
```

(where P = pod number)

g. Enable encryption and authentication of LAN-based failover messages between PIX Security Appliances:

```
PixP(config)# failover lan key 1234567
```

(where P = pod number)

h. Configure this device as the primary failover unit:

```
PixP(config)# failover lan unit primary
```

(where P = pod number)

i. Configure failover group 1 to be active on the primary:

```
PixP(config)# failover group 1
PixP(config-fover-group)# exit
```

(where P = pod number)

j. Configure failover group 2 to be active on the secondary:

```
PixP(config)# failover group 2
PixP(config-fover-group)# exit
```

k. Save all changes to Flash memory:

l. Show the failover status

```
PixP# show failover
Failover Off
Cable status: N/A - LAN-based failover enabled
Failover unit Primary
Failover LAN Interface: myfailover Ethernet2 (up)
Unit Poll frequency 15 seconds, holdtime 45 seconds
Interface Poll frequency 15 seconds
Interface Policy 1
Monitored Interfaces 2 of 250 maximum
```

Step 4 Allocate Interfaces and Failover Groups by Context

The system context has no physical connections of its own other than the failover link. The system context is used to create other contexts and allocate resources to each context. In this task, create a ctx1 context and allocate resources to both the admin and ctx1 contexts. Complete the following steps to allocate interfaces and a failover group to each context:

a. Access the admin context configuration commands:

```
PixP(config)# context admin
```

b. Allocate interfaces to the admin context:

```
PixP(config-ctx)# allocate-interface ethernet0
PixP(config-ctx)# allocate-interface ethernet1
```

c. Configure a URL for admin context configuration:

```
PixP(config-ctx)# config-url flash:/admin.cfg
```

d. Allocate a failover group to the admin context:

```
PixP(config-ctx)# failover group 1
PixP(config-if)# exit
```

e. Create the ‘ctx1’ context:

```
PixP(config)# context ctx1
Creating context ‘ctx1’ . . Done.
```

f. Allocate interfaces to the ctx1 context:

```
PixP(config-ctx)# allocate-interface ethernet3
PixP(config-ctx)# allocate-interface ethernet4
```


g. Configure a new URL for ctx1 context configuration:

```
PixP(config-ctx)# config-url flash:/ctx1.cfg
WARNING: Could not fetch the URL flash:/ctx1.cfg
INFO: Creating context with default config
```

h. Allocate a failover group to the ctx1 context:

```
PixP(config-ctx)# failover group 2
PixP(config-fover-group)# exit
```

i. Enable interfaces Ethernet3 and Ethernet4

```
PixP(config)# interface ethernet3
PixP(config-if)# no shutdown
PixP(config-if)# exit
PixP(config)# interface ethenet4
PixP(config-if)# no shut
PixP(config-if)# exit
```

j. Verify the context allocation configuration:

```
PixP# show context
Context Name Interfaces URL
*admin Ethernet0, Ethernet1 flash:/admin.cfg
ctx1 Ethernet3, Ethernet4 flash:/ctx1.cfg
Total active Security Contexts: 2
```

Step 5 Configure the admin and ctx1 Context

In this task, configure a virtual security context. Use the “changeto” command to navigate between each context. Complete the following steps to configure the ctx1 context:

a. From the primary PIX Security Appliance console, access the admin context configuration commands:

```
PixP(config)# changeto context admin
PixP/admin(config)#
```

Notice the prompt has changed. Admin was added to the hostname. You are now administratively located in the admin context.

b. Notice the configuration from the interfaces still exists.

```
PixP/admin(config)# show running-config interface
```

c. Notice that if the commands **show running-config failover** or **configure failover** parameters are used while in the admin context, an error message is displayed.

```
PixP/admin(config)# show running-config failover
ERROR: % Invalid input detected at marker
Failover is configured in the system context only.
```

d. Access the ctx1 context configuration commands:

```
PixP(config)# changeto context ctx1
PixP/ctx1(config)#
```


Notice the prompt has changed. Ctx1 was added to the hostname. You are now administratively located in the ctx1 context.

e. View the interface configuration. The context ctx1interfaces are available but not configured.

```
PixP/ctx1(config)# show interface
Interface Ethernet2 " " is up, line protocol is up
Available but not configured via nameif
Interface Ethernet3 " " is up, line protocol is up
Available but not configured via nameif
```

f. Step 6 Configure context ctx1 interfaces:

```
PixP/ctx1(config)# interface ethernet3
PixP/ctx1(config-if)# nameif ctxout
Info: Security level for "ctxout" set to 0 by default.
PixP/ctx1(config-if)# ip address 192.168.30+P.2 255.255.255.0
standby 192.168.30+P.7
PixP/ctx1(config-if)# no shutdown
PixP/ctx1(config-if)# exit
PixP/ctx1 config)# interface e4
PixP/ctx1(config-if)# nameif ctxin
Info: Security level for "ctxin" set to 0 by default.
PixP/ctx1(config-if)# ip address 10.0.30+P.1 255.255.255.0 standby
10.0.30+P.7
PixP/ctx1(config-if)# security-level 100
PixP/ctx1(config-if)# no shutdown
PixP/ctx1(config-if)# exit
```

g. Add a default route.

```
PixP/ctx1(config)# route ctxout 0 0 192.168.31.1
```

h. Add a static route from super server to outside network

```
PixP/ctx1(config)# static (ctxin,ctxout) 192.168.31.10 10.0.31.10
```

i. Add an access-list for allow outside access to super server.

```
PixP/ctx1(config)# access-list ctxin permit tcp any host
192.168.31.10
```

j. Add an access-list to allow ICMP.

```
PixP/ctx1(config)# access-list ctxin permit icmp any any
```

k. Bind the access-list to the outside interface

```
PixP/ctx1(config)# access-group ctxin in interface outside
```

l. Save the changes.

```
PixP/ctx1(config)# write memory
```

m. From the student PC, try to ping the backbone router:

```
C:\ ping 172.26.26.50
```

n. From the student PC, try to ping the context ctx1 outside interface:


```
C:\ ping 192.168.31.2
```

o. From the student PC, try to ping the context ctx1 inside host:

```
C:\ ping 192.168.31.10
```
(translated address for the inside host)

Connectivity should be present from the student PC through context admin to the backbone, 172.26.26.50, and back through context ctx1, 192.168.31.2 to the inside host, 192.168.31.10.

Step 6 Enable Failover on the Primary Failover Device

Once connectivity with failover disabled has been established, enable failover on the primary failover device.

a. Change to the system context

```
PixP/ctx1(config)# changeto system
```

b. Show the failover status of the primary failover device

```
PixP(config)# show failover
Failover Off
Cable status: N/A - LAN-based failover enabled
Failover unit Primary
Failover LAN Interface: myfailover Ethernet2 (up)
Unit Poll frequency 15 seconds, holdtime 45 seconds
Interface Poll frequency 15 seconds
Interface Policy 1
Monitored Interfaces 4 of 250 maximum
```

c. Enable failover

```
PixP(config)# failover
```

After a pause, the following message should be displayed on the console:

```
No response from Mate
Group 1 No response from Mate, Switch to Active
Group 2 No response from Mate, Switch to Active
```

d. Show the new failover status of the primary failover device

```
PixP# show failover
Failover On
Cable status: N/A - LAN-based failover enabled
Failover unit Primary
Failover LAN Interface: myfailover Ethernet2 (up)
Unit Poll frequency 15 seconds, holdtime 45 seconds
Interface Poll frequency 15 seconds
Interface Policy 1
Monitored Interfaces 4 of 250 maximum
Group 1 last failover at: 15:54:49 UTC Dec 14 2004
Group 2 last failover at: 15:55:00 UTC Dec 14 2004
This host: Primary
```



```
Group 1 State: Active
Active time: 6135 (sec)
Group 2 State: Active
Active time: 0 (sec)
admin Interface outside (192.168.P.2): Normal (Waiting)
admin Interface inside (10.0.P.1): Normal (Waiting)
cx1 Interface outside (192.168.3P.2): Normal (Waiting)
cx1 Interface inside (10.0.3P.1): Normal (Waiting)
Other host: Primary
Group 1 State: Failed
Active time: 0 (sec)
Group 2 State: Failed
Active time: 0 (sec)
admin Interface outside (192.168.P.7): Unknown (Waiting)
admin Interface inside (10.0.P.7): Unknown (Waiting)
cx1 Interface outside (192.168.31.7): Unknown (Waiting)
cx1 Interface inside (10.0.31.7): Unknown (Waiting)
Configure the Secondary Failover Security Device
```

Step 7 Enable Multiple Context Mode

Once the primary PIX Security Appliance is configured, the next task is to prepare the secondary PIX Security Appliance for active/active failover. Complete the following steps to enable multiple mode on the secondary PIX Security Appliance.

a. Ask the instructor how to access the console port of the secondary failover device.

b. Once the console of the secondary PIX Security Appliance is accessed, verify that this PIX Security Appliance is licensed to support security contexts.

```
PixP(config)# show version
```

c. Check the current mode of the secondary PIX Security Appliance:

```
PixP(config)# show mode
Security appliance mode: single
The flash mode is the SAME as the running mode.
```

d. Enable Multiple Context mode:

```
PixP(config)# mode multiple
WARNING: This command will change the behavior of the device
WARNING: This command will initiate a Reboot
Proceed with change mode? [confirm] <Enter>
Convert the system configuration? [confirm] <Enter>
The old running configuration file will be written to flash
The admin context configuration will be written to flash
The new running configuration file was written to flash
```


e. After the secondary Security Appliance re-boots, confirm the PIX Security Appliance is in multiple context mode:

```
PixP# show mode
Security context mode: multiple
```

f. Confirm the PIX Security Appliance saved the original configuration as `old_running.cfg`:

```
PixP# show flash
Directory of flash:/
3 -rw- 4810752 08:30:41 Aug 12 2004 pix_7_82.bin
8 -rw- 2028 08:30:41 Aug 12 2004 old_running.cfg
9 -rw- 1682 08:30:41 Aug 12 2004 admin.cfg
```

g. Examine the current security contexts.

```
PixP# show context
Context Name Interfaces URL
*admin Ethernet0,Ethernet1 flash:/admin.cfg
Total active Security Contexts: 1
PixP# show context detail
Context "system", is a system resource
Config URL: startup-config
Real Interfaces:
Mapped Interfaces: Ethernet0, Ethernet1, Ethernet2,
Ethernet3, Ethernet4, Ethernet5
Flags: 0x00000019, ID: 0
Context "admin", has been created, but initial ACL rules not
complete
Config URL: flash:/admin.cfg
Real Interfaces: Ethernet0, Ethernet1
Mapped Interfaces: Ethernet0, Ethernet1
Flags: 0x00000013, ID: 1
Context "null", is a system resource
Config URL: ... null ...
Real Interfaces:
Mapped Interfaces:
Flags: 0x00000009, ID: 257
```

Step 8 Configure the Failover Link

Complete the following steps to add a failover link to the system context:

a. Enable the interface used for the failover link:

```
PixP(config)# interface ethernet2
PixP(config-if)# no shutdown
PixP(config-if)# exit
```


b. Use the **failover lan interface** command to specify the name of the dedicated failover interface:

```
PixP(config)# failover lan interface MYFAILOVER ethernet2
INFO: Non-failover interface config is cleared on Ethernet3 and its
sub-interfaces
```

(where P = pod number)

c. Enable LAN-based failover:

```
PixP(config)# failover lan enable
```

(where P = pod number)

d. Specify the failover link IP addressing:

```
PixP(config)# failover interface ip MYFAILOVER 172.16.P.1
255.255.255.0 standby 172.16.P.7
```

(where P = pod number)

e. Enable stateful failover:

```
PixP(config)# failover link MYFAILOVER ethernet2
```

(where P = pod number)

f. Enable encryption and authentication of LAN-based failover messages between PIX Security Appliances:

```
PixP(config)# failover lan key 1234567
```

(where P = pod number)

g. Configure this device as the secondary failover device:

```
PixP(config)# failover lan unit secondary
```

h. Enable failover on the secondary failover device:

```
PixP(config)# failover
```

After a pause, from the secondary device console the following messages should be displayed:

```
Detected an active mate
Beginning configuration replication from mate
Creating context 'admin'. . . Done
Creating context 'ctx1'. . . Done
End configuration replication
Group 1 detected active mate
Group 2 detected active mate
End configuration replication from mate.
```

i. Return to the console of the primary failover device.

Task 9 Exercise Active/Active Failover

Complete the following steps to exercise active/active failover:

a. From the primary device console, verify that you are in the system context.

b. View the failover statistics. Notice the primary group 1 and group 2 are both active.

Notice the secondary group 1 and group 2 are in standby ready state. Also notice the host addresses of each interface. The standby interface addresses end in .7


```
PixP(config)# show failover
Failover On
Cable status: N/A - LAN-based failover enabled
Failover unit Primary
Failover LAN Interface: myfailover Ethernet2 (up)
Unit Poll frequency 15 seconds, holdtime 45 seconds
Interface Poll frequency 15 seconds
Interface Policy 1
Monitored Interfaces 4 of 250 maximum
Group 1 last failover at: 15:54:49 UTC Dec 14 2004
Group 2 last failover at: 15:55:00 UTC Dec 14 2004
This host: Primary
Group 1 State: Active
Active time: 765 (sec)
Group 2 State: Active
Active time: 765 (sec)
admin Interface outside (192.168.1.2): Normal
admin Interface inside (10.0.1.1): Normal
ctx1 Interface outside (192.168.31.2): Normal
ctx1 Interface inside (10.0.31.1): Normal
Other host: Secondary
Group 1 State: Standby Ready
Active time: 0 (sec)
Group 2 State: Standby Ready
Active time: 0 (sec)
admin Interface outside (192.168.1.7): Normal
admin Interface inside (10.0.1.7): Normal
ctx1 Interface outside (192.168.31.7): Normal
ctx1 Interface inside (10.0.31.7): Normal
```

c. From the student PC, perform a continuous ping to host 172.26.26.50

```
C:\>ping 172.26.26.50 -t
```

d. From the student PC open a telnet session to the backbone router

```
C:\>telnet 192.168.P.1
User Access Verification
Password: Cisco
RBB> enable
Password: <cr>
Password: <cr>
Password: <cr>
```



```
% Bad passwords
RBB>
```

e. Force the peer PIX Security Appliance to become active.

```
PixP(config)# no failover active
```

f. After the failover, verify the ping is still active and the telnet session is still open.

From the telnet session type the following:

```
RBB> enable
Password: <cr>
Password: <cr>
Password: <cr>
% Bad passwords
RBB>
```

g. Close the telnet session and stop the pings.

h. From the primary failover device console, view failover statistics:

```
PixP(config)# show failover
Failover On
Cable status: N/A - LAN-based failover enabled
Failover unit Primary
Failover LAN Interface: myfailover Ethernet2 (up)
Unit Poll frequency 15 seconds, holdtime 45 seconds
Interface Poll frequency 15 seconds
Interface Policy 1
Monitored Interfaces 4 of 250 maximum
Group 1 last failover at: 15:54:49 UTC Dec 14 2004
Group 2 last failover at: 15:55:00 UTC Dec 14 2004
This host: Primary
Group 1 State: Standby Ready
Active time: 765 (sec)
Group 2 State: Standby Ready
Active time: 765 (sec)
admin Interface outside (192.168.1.7): Normal
admin Interface inside (10.0.1.7): Normal
ctx1 Interface outside (192.168.31.7): Normal
ctx1 Interface inside (10.0.31.7): Normal
Other host: Secondary
Group 1 State: Active
Active time: 240 (sec)
Group 2 State: Active
Active time: 240 (sec)
```



```
admin Interface outside (192.168.1.2): Normal
admin Interface inside (10.0.1.1): Normal
ctx1 Interface outside (192.168.31.2): Normal
ctx1 Interface inside (10.0.31.1): Normal
```

Notice after the failover, the host address of the primary interfaces end in .7 while the standby secondary interfaces end in .2. The interface addresses switched between primary and secondary units due to the failover.

Step 10 Return the Failover Devices to Single Mode

Complete the following steps to return the failover devices to single mode:

a. From the primary failover device console, disable failover:

```
PixP(config)# no failover
```

b. Return the failover device to single mode

```
PixP(config)# mode single
WARNING: This command will change the behavior of the device
WARNING: This command will initiate a Reboot
Proceed with change mode? [confirm] <Enter>
```

c. After the primary device reboots, erase the configuration.

```
PixP # write erase
Erase configuration in flash memory? [confirm] <Enter>
PixP # reload
Proceed with reload? [confirm] <Enter>
```

d. After the primary Security Appliance reloads, copy the configuration that was saved at the beginning of this lab to the running-config.

```
pixfirewall(config)# copy flash:/pre_fo_lab.cfg running-config
```

e. Save the configuration.

f. From the secondary failover device console:

```
PixP(config)# no failover
```

g. Return the failover device to single mode

```
PixP(config)# mode single
WARNING: This command will change the behavior of the device
WARNING: This command will initiate a Reboot
Proceed with change mode? [confirm] <Enter>
```

h. After the secondary device reboots, erase the configuration.

```
PixP # write erase
Erase configuration in flash memory? [confirm] <Enter>
PixP # reload
```


Lab 8.3.3 Configure a PIX Security Appliance as a Transparent Firewall

Objective

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

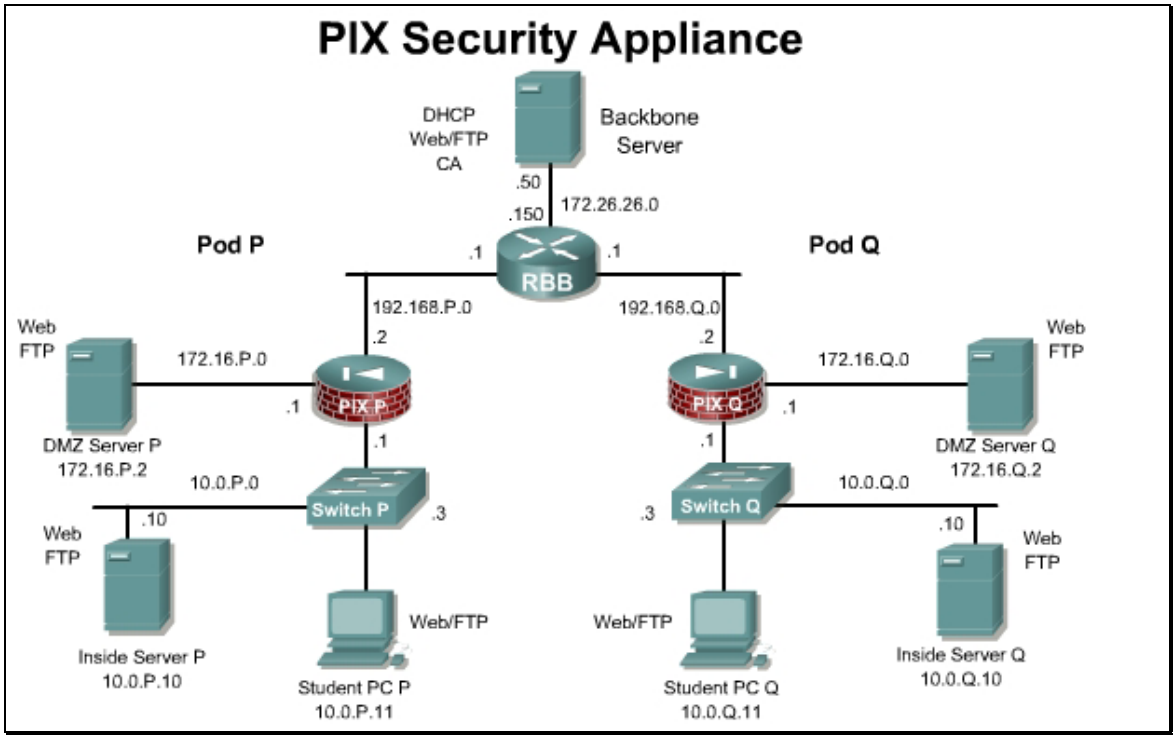
- Enable transparent firewall mode.
- Configure the PIX Security Appliance interfaces and a management IP address.
- Test the inside and outside connectivity.
- Allow ICMP traffic through the transparent firewall
- Disable transparent firewall mode.

Scenario

The XYX Company has decided to change the operational mode of an existing PIX Firewall from router to transparent. The PIX must be reconfigured to operate in transparent mode. The PIX will also need to be configured to allow layer 3 traffic, such as ICMP, to pass through the transparent firewall as allowed by the company security policy.

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.

When the PIX Security Appliance is in transparent firewall mode, both of the interfaces are on the same IP network. The student PC must be reassigned to the same IP network as the outside host for this lab activity. Use the IP address 172.16.P.11/24 and a default gateway of 172.16.P.1 for the student PC. (Where P = pod number)

Tools and Resources

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

- Standard PIX Security Appliance lab topology
- Console cable
- HyperTerminal

Additional Materials

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

http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_configuration_guide_chapter09186a0080450b68.html

Step 1 Enable Transparent Firewall Mode

To enable the PIX Security Appliance to operate in transparent firewall mode, complete the following steps:

a. Save the configuration to flash:

```
PixP# copy running-config flash:saved.cfg
Source filename [running-config]? <Enter>
Destination filename [saved.cfg]? <Enter>
Cryptochecksum: bdeb536f 156358e5 a7d99020 7f1ed561
2420 bytes copied in 0.940 secs
```

b. Change to configuration mode:

```
PixP# configure terminal
PixP(config)#
```

c. Set the firewall mode to transparent:

```
PixP(config)# firewall transparent
Switched to transparent mode
Pixfirewall(config)#
```

d. Confirm that the PIX Security Appliance is now operating in transparent firewall mode.

```
Pixfirewall(config)# show firewall
```

Examine the running configuration:

```
Pixfirewall(config)# write terminal
: Saved
:
PIX Version 7.0(1)
```



```
firewall transparent
names
!
interface Ethernet0
 shutdown
 no nameif
 no security-level
!
interface Ethernet1
 shutdown
 no nameif
 no security-level
!
interface Ethernet2
 shutdown
 no nameif
 no security-level
!
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pixfirewall
ftp mode passive
pager lines 24
no ip address
no failover
no asdm history enable
arp timeout 14400
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp
telnet timeout 5
ssh timeout 5
console timeout 0
!
```



```
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map global_policy
 class inspection_default
  inspect dns maximum-length 512
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
!
service-policy global_policy global
Cryptochecksum:bdeb536f156358e5a7d990207f1ed561
: end
```

Step 2 Configure the PIX Security Appliance Interfaces and Management Address

Complete the following steps to configure PIX Security Appliance Ethernet interfaces and management address:

a. Configure the Ethernet 1 interface.

Note By default the interfaces are disabled. Any interface that will be used must be enabled.

```
pixfirewall(config)# interface ethernet1
pixfirewall(config-if)# nameif inside
pixfirewall(config-if)# no shutdown
```

b. Configure the Ethernet 2 interface.

```
pixfirewall(config-if)# interface ethernet2
pixfirewall(config-if)# nameif outside
pixfirewall(config-if)# no shutdown
```

c. Exit interface configuration mode.

```
pixfirewall(config-if)# exit
```


d. Configure the management IP address.

```
pixfirewall(config)# ip address 172.16.P.30 255.255.255.0
```

(where P = pod number)

e. Verify the management IP address configuration.

```
pixfirewall(config)# show ip address
Management System IP Address:
         ip address 172.16.P.30 255.255.255.0
Management Current IP Address:
         ip address 172.16.P.30 255.255.255.0
```

(where P = pod number)

f. Write the configuration to memory.

```
pixfirewall(config)# write memory
```

Step 3 Test Inside and Outside Connectivity

Complete the following steps to test and troubleshoot interface connectivity using the PIX Security Appliance **ping** command:

a. Ping the inside host:

```
pixfirewall(config)# ping 172.16.P.11
Sending 5, 100-byte ICMP Echos to 172.16.P.11, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

(where P = pod number)

b. Ping the outside host:

```
pixfirewall(config)# ping 172.16.P.2
Sending 5, 100-byte ICMP Echos to 172.16.P.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

(where P = pod number)

c. Examine the MAC address table:

```
pixfirewall(config)# show mac-address-table
interface         mac address             type     Age(min)
-------------------------------------------------------------------
outside                 0002.fd1c.3c43          dynamic     4
inside                  00d0.b7b9.62af          dynamic     4
```

d. Test the inside host connectivity, by pinging the outside host from the student PC:

```
C:\>ping 172.16.P.2
Pinging 172.16.P.2 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
```



```
Request timed out.
```

Step 4 Allow ICMP Through the Transparent Firewall

Complete the following steps to allow ICMP traffic through the PIX Security Appliance transparent firewall:

a. Create an ACL the allows ICMP traffic from the inside to the outside network:

```
pixfirewall(config)# access-list ACLIN permit icmp 172.16.P.0
255.255.255.0 172.16.P.0 255.255.255.0
```

(where P = pod number)

b. Apply the ACL to the inside and outside interfaces:

```
pixfirewall(config)# access-group ACLIN in interface inside
pixfirewall(config)# access-group ACLIN in interface outside
```

c. Test the inside host connectivity, by pinging the outside host from the student PC:

```
C:\>ping 172.16.P.2
Pinging 172.16.P.2 with 32 bytes of data:
Reply from 172.16.P.2: bytes=32 time<10ms TTL=126
Reply from 172.16.P.2: bytes=32 time<10ms TTL=126
Reply from 172.16.P.2: bytes=32 time<10ms TTL=126
Reply from 172.16.P.2: bytes=32 time<10ms TTL=126
```

d. Verify the access list and note the hit counts:

```
pixfirewall(config)# show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max
4096)
            alert-interval 300
access-list ACLIN; 1 elements
access-list ACLIN line 1 extended permit icmp 172.16.P.0
255.255.255.0 172.16.P.0 255.255.255.0 (hitcnt=2)
```

e. If desired, compare the running configuration with the ending configuration provided for this lab.

Step 5 Disable Transparent Firewall Mode

Complete the following steps to disable Transparent Firewall mode:

a. Set the firewall mode to router:

```
pixfirewall(config)# no firewall transparent
Switched to router mode
```

b. Restore the original configuration and reboot:

```
pixfirewall# copy flash:saved.cfg startup-config
Source filename [saved.cfg]? <Enter>
Copy in progress...C
2420 bytes copied in 0.70 secs
pixfirewall(config)# reload
```


Lab 8.4.3a Configure User Authentication and Command Authorization using ASDM

Objective

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

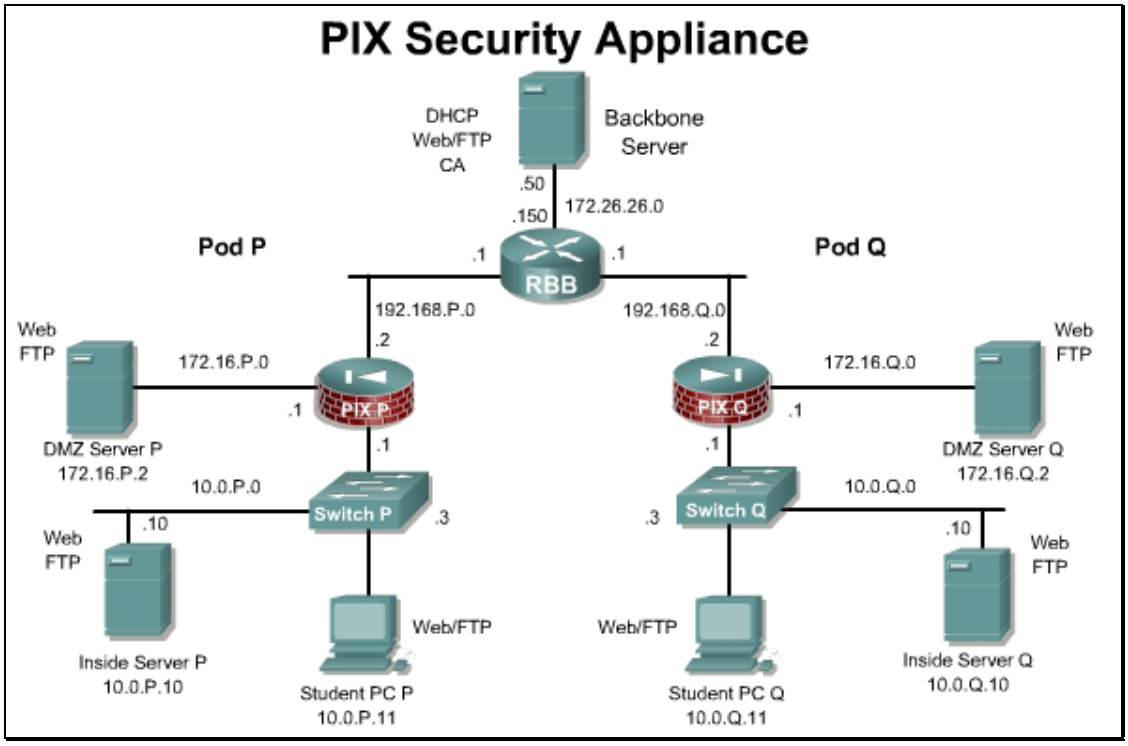
- Configure command authorization.
- Configure Local User Authentication.
- Configure SSH

Scenario

A company has just expanded and now has 5 remote offices with PIX Security Appliances. Currently there are no VPN tunnels between the remote offices and the main office. To increase security of the remote management session, it is necessary to use SSH to protect the administrator username and password. SSH should also be used when managing devices over the LAN. It is also necessary to setup limited access accounts on the PIX for junior administrators and various IT staff.

Topology

This figure illustrates the lab network environment.



Preparation

Begin with the standard lab topology and verify the starting configurations on the 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.

A SSH client is required for this lab. http://www.chiark.greenend.org.uk/~sgtatham/putty/

Tools and resources

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

- Standard PIX Security Appliance lab topology
- Console cable
- HyperTerminal
- SSH client

Additional materials

Students can use the following links for more information on the objectives covered in this lab:

http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_configuration_guide_chapter09186a0080450d39.html

Step 1 Configure Administrative Passwords and Monitor Sessions.

To configure these passwords, complete the following steps:

a. Initiate an ASDM connection to the PIX Security Appliance.

b. Navigate to **Configuration>Features>Device Administration>Administration>Password**.

c. Check the **Change the privileged mode password** checkbox.

d. Change the enable password to **cisco123**. Click the **Apply** button. Click **Send** if prompted.

e. Change the telnet password from the default of **cisco** to **telnet123**. Click the **Apply** button.

f. ASDM will prompt for authentication. Log in using **cisco123**.

g. On the Student PC, open a command prompt and telnet to the PIX. Notice the failed attempt.

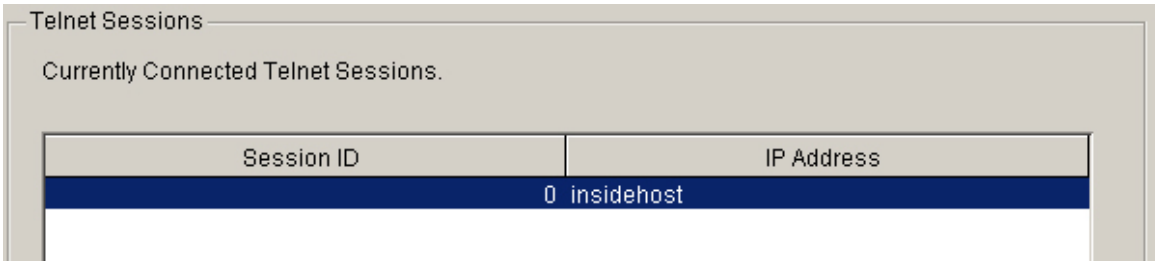
h. Navigate to **Configuration>Features>Device Administration>Administration>Telnet**.

i. Click the **Add** button. Allow the Student PC address to access the PIX Security Appliance inside interface using Telnet. Apply the changes.

j. On the Student PC, open a command prompt and telnet to the PIX.

k. Log in using the new **telnet123** password. Enter into privileged mode with the new password **cisco123**.

l. Navigate to **Monitoring>Features>Administration>Telnet Sessions.** The following should be displayed:



m. Close the session, but leave the command prompt window open.

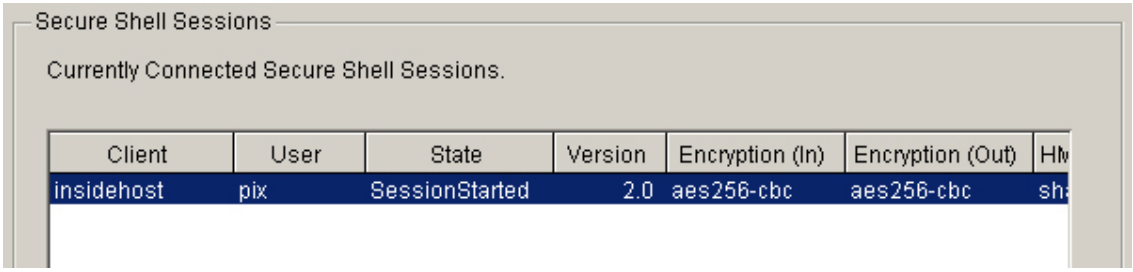
n. Navigate to **Configuration>Features>Device Administration>Administration>Secure Shell**.

o. Click the **Add** button. Permit the Student PC address to access the PIX Security Appliance inside interface using Secure Shell. Apply the changes.

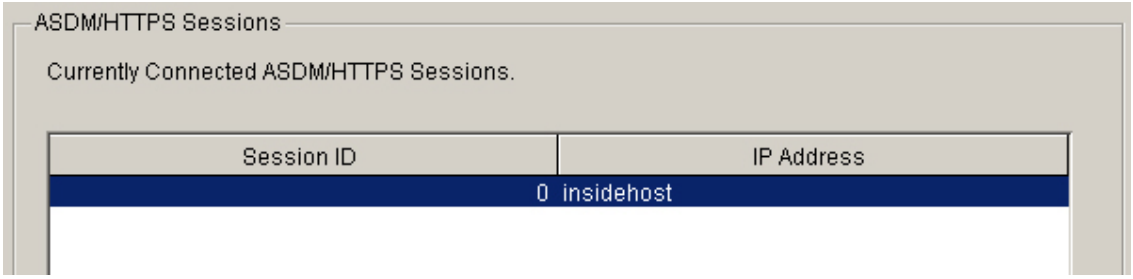
p. On the Student PC, open a PuTTy session and SSH to the PIX

q. Log in using the default username **pix** the **telnet123** password. Enter into privileged mode with the new password **cisco123**.

r. Navigate to **Monitoring>Features>Administration>Secure Shell Sessions**. The following should be displayed.



s. Navigate to **Monitoring>ASDM/HTTPS Sessions.** The following should be displayed.



t. Disconnect the SSH session.

Step 2 Enable Command Authorization with Privileged Mode Passwords

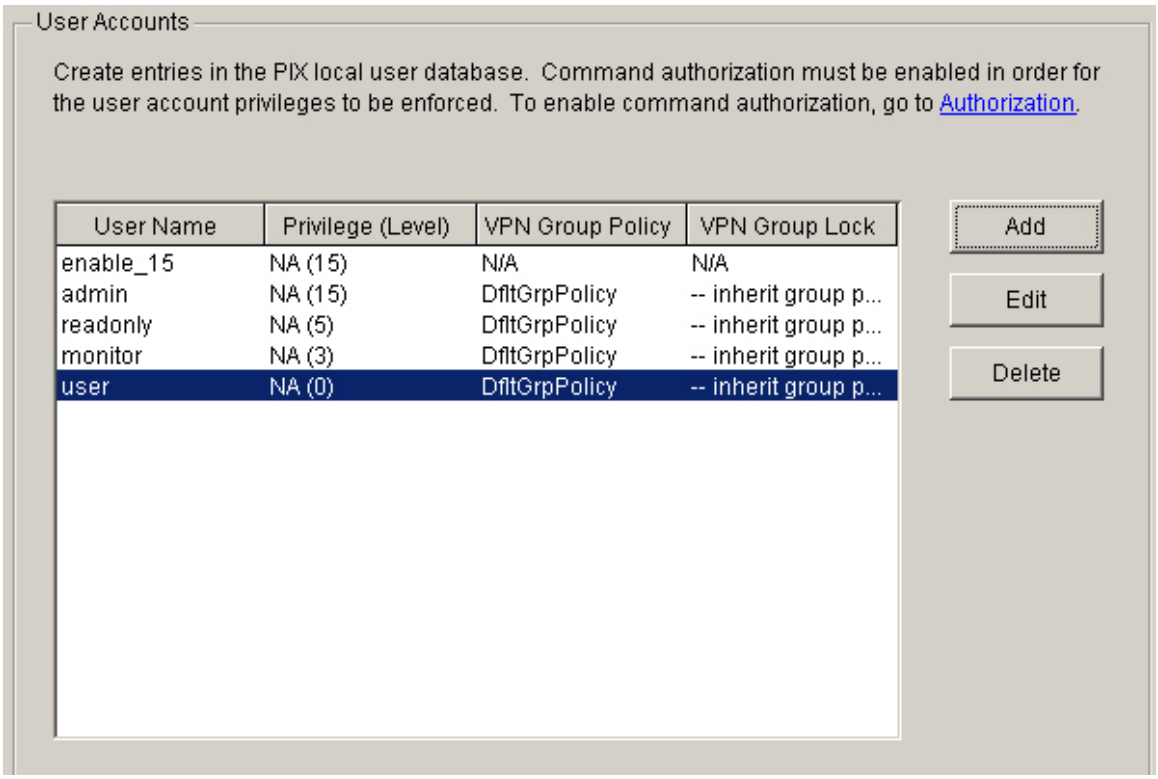
Perform the following tasks to enable command authorization with privileged mode passwords.

a. Navigate to **Configuration>Features>Device Administration>Administration>User Accounts.**

b. Add the following users and apply the changes.

User	**Password**	**Privilege level**
admin	admin	15
readonly	readonly	5
monitor	monitor	3
user	user	0

c. The following users should now appear in the User Accounts window.

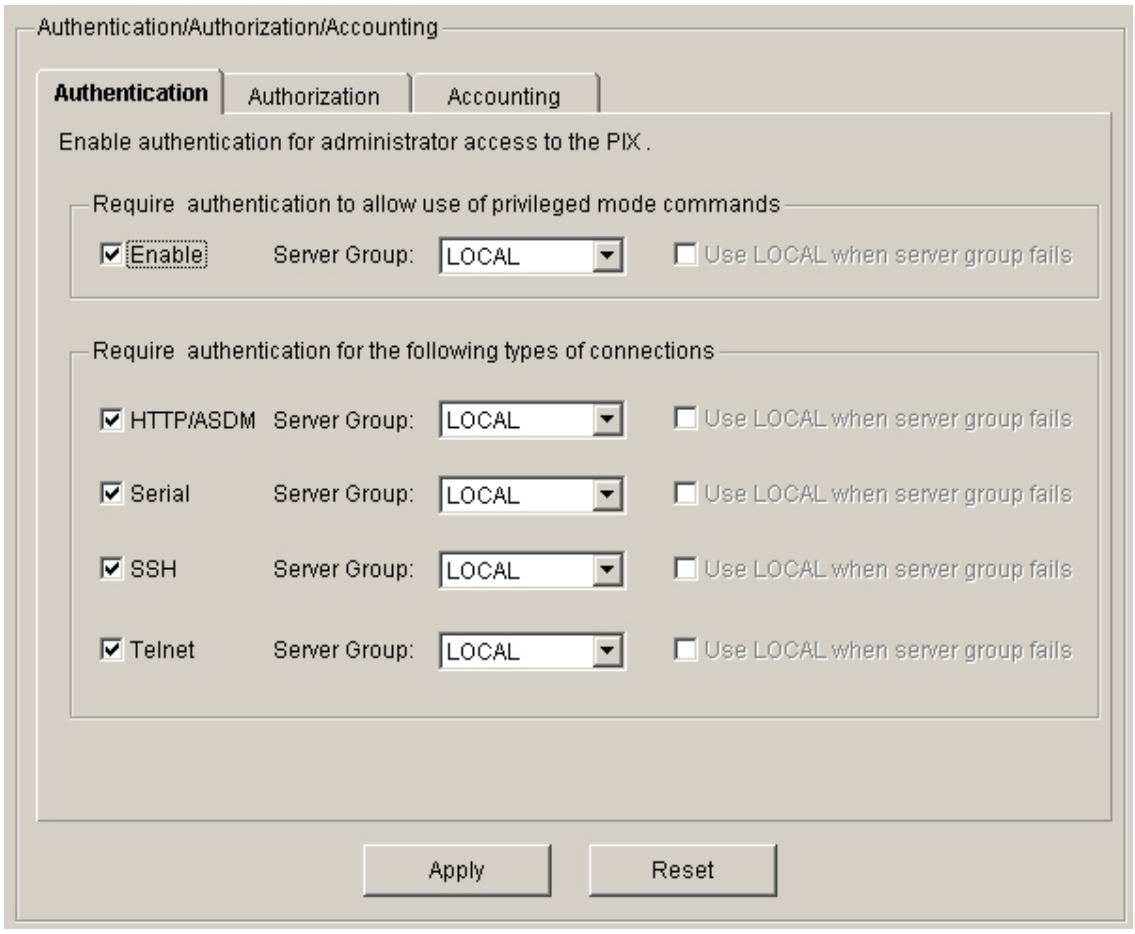


d. Click the **Apply** button.

e. Click the **Authorization** hyperlink to go to **Configuration>Features>Device Administration>Administration>AAA Access>Authorization**.

f. Click the **Authentication** tab. Enable AAA Authentication for HTTP/ADSM, Serial, SSH, and Telnet using the LOCAL database. Do not apply the changes yet.

g. Check the **Enable** checkbox to enable AAA authentication to use privileged mode commands. Do not apply the changes yet.



h. Verify the configuration, using the sample above.

i. Return to the Authorization tab. Click on the **Advanced** button to view the current privilege levels of all the commands.

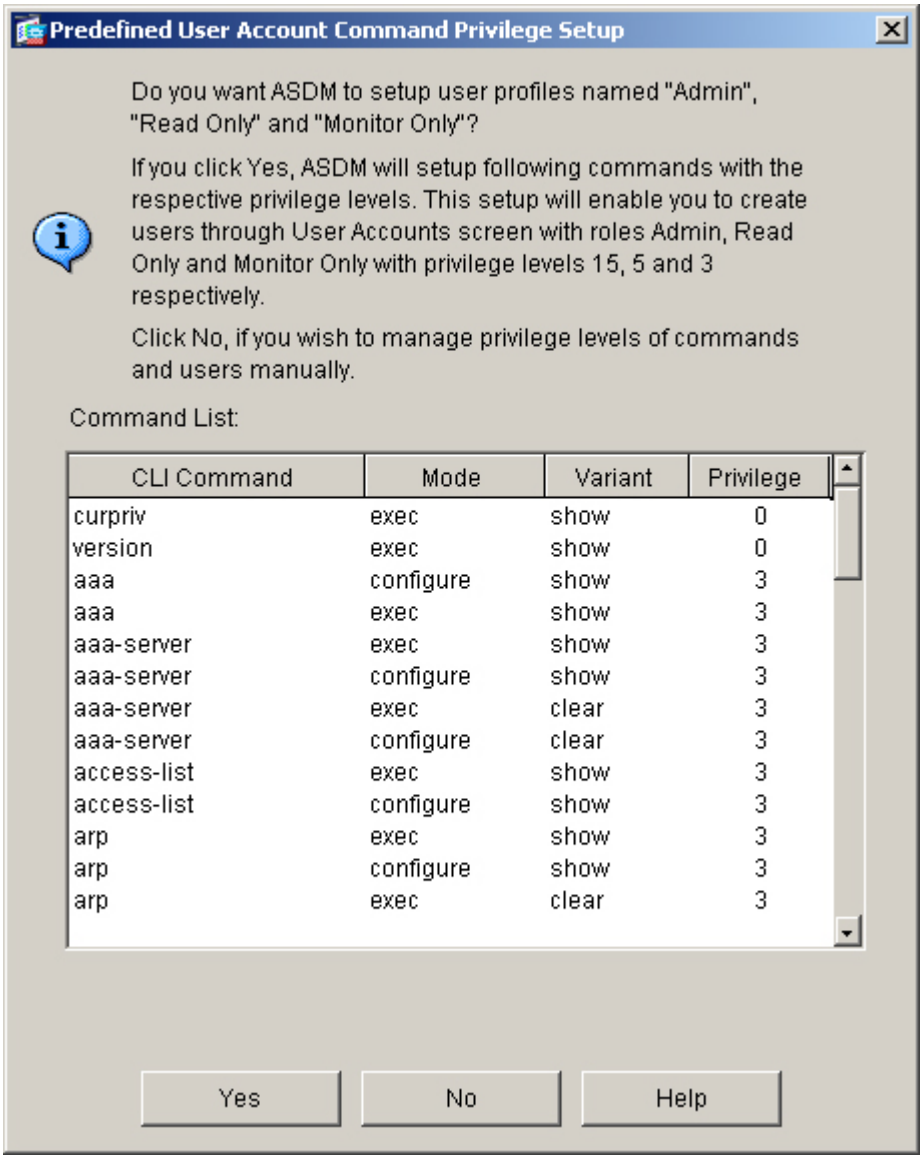
j. Select the checkbox next to **Enable Authorization for PIX command access** to enable command authorization using the LOCAL database.

Note Enabling AAA authentication and authorization for enable commands will cause the user to be required to use the **`login`** command in user mode to gain access to the enable mode.

---

k. Click the **Apply** button to implement the changes.

l. A message about Predefined User Account Privileges will appear. Note the CLI commands and privilege levels.



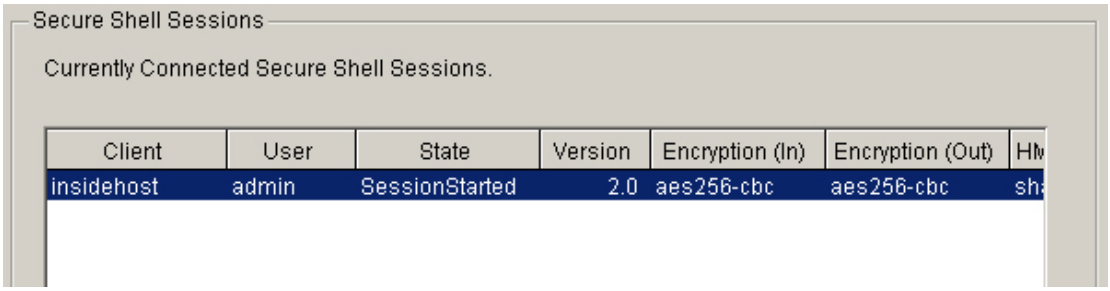
m. Click the **Yes** button to continue.

n. Click on the **Advanced** button again, noting the new command privilege levels. After reviewing the privilege levels, click the **OK** button to close the window.

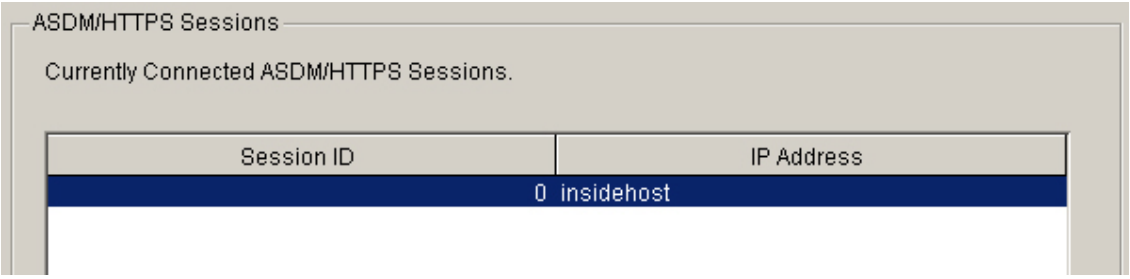
u. On the Student PC, open PuTTy and initiate an SSH connection to the PIX

v. Log in using the **admin** password. Enter into privileged mode with the new password **admin**.

w. Navigate to **Monitoring>Features>Administration>Secure Shell Sessions.** The following should be displayed.



x. Navigate to **Monitoring>Features>Administration>ASDM/HTTPS Sessions.** The following should be displayed.



Step 3 Test Command Authorization

a. Exit out of the console connection. Log back in using **user**/**user**. Type the **?** to see which commands are available. Try to enter into privileged mode. Access should be denied.

b. Telnet and SSH to the PIX, using the various accounts. Type the **?** to see which commands are available. Try to enter into privileged mode. Exit the sessions when finished.

c. Navigate to **Configuration>Features>Device Administration>Administration>AAA Access>Authorization**.

d. Click on the **Advanced** button. Allow the readonly user to view the tech support.

e. Click on the **tech-support** line, click **Edit** and change to **5**. Click the **OK** button to continue. Click **Apply**.

f. Using the console, login with the readonly account. Verify the command is accessible. Logout using the **`logout`** command.

```
PixP# logout
Logoff
Username:
```

g. Change the tech-support command back to level 15.

h. Login with the readonly account.

```
PixP> login
```

i. Verify the show tech-support command is not accessible.

```
PixP# show tech-support
Command authorization failed
```

d. View the user account that is currently logged in:

```
PixP# show curpriv
Username : readonly
Current privilege level : 5
Current Mode/s : P_PRIV
```

1. Why would different levels and passwords be assigned?

_____

_____

Answer: Different privilege levels and passwords can be given to individuals or groups of individuals to restrict access to only the privilege level that is appropriate and necessary for those users.

Lab 8.4.3b Configure SSH, Command Authorization, and Local User Authentication using CLI

Objective

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

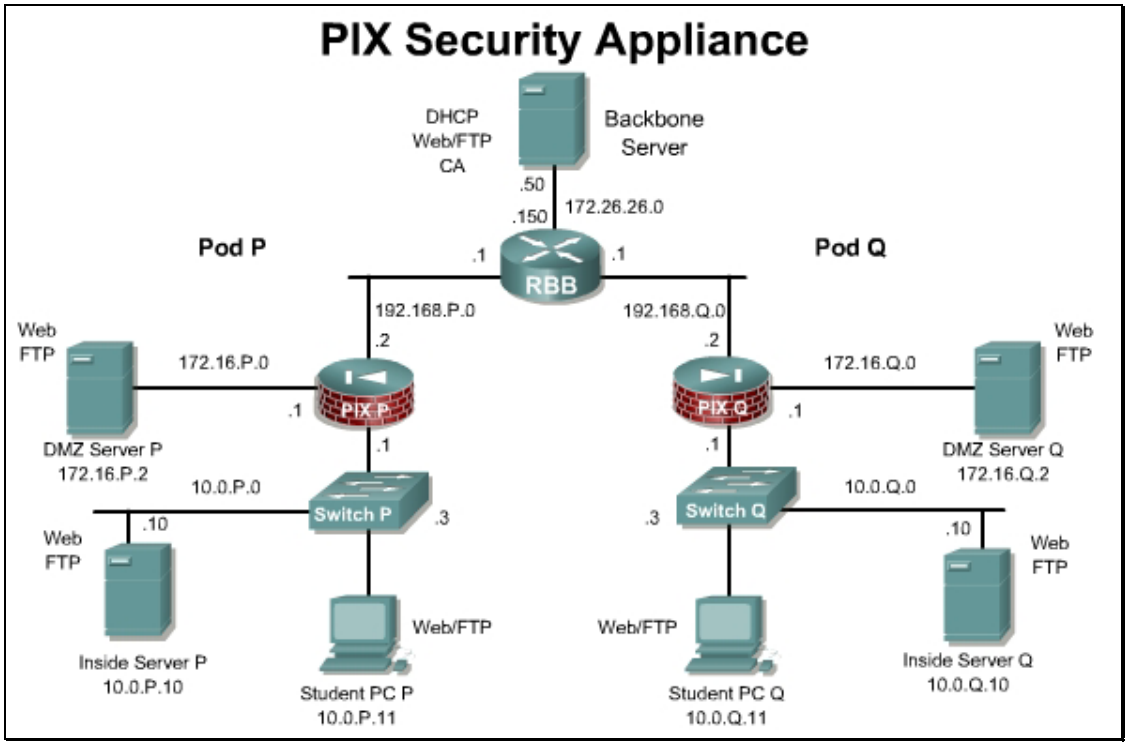
- Configure and verify SSH operation
- Configure command authorization.
- Configure Local User Authentication.

Scenario

A company has just expanded and now has 5 remote offices with PIX Security Appliances. Currently there are no VPN tunnels between the remote offices and the main office. To increase security of the remote management session, it is necessary to use SSH to protect the administrator username and password. SSH should also be used when managing devices over the LAN. It is also necessary to setup limited access accounts on the PIX for junior administrators and IT staff.

Topology

This figure illustrates the lab network environment.



Preparation

Begin with the standard lab topology and verify the starting configurations on the pod PIX Security Appliances. Access the PIX Security Appliance console port using the HyperTerminal on the student PC. If desired, save the PIX Security Appliance configuration to a text file for later analysis.

An SSH client is required for this lab. http://www.chiark.greenend.org.uk/~sgtatham/putty/

Tools and resources

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

- Standard PIX Security Appliance lab topology
- Console cable
- HyperTerminal
- SSH client

Additional materials

Students can use the following links for more information on the objectives covered in this lab:

http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_configuration_guide_chapter09186a0080450d39.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
aaa authorization command {LOCAL | *tacacs_server_tag*}	Enable or disable LOCAL or TACACS+ user authorization services. Configuration mode.
enable password *password*	Configures the enable password
ca generate rsa key *modulus*	The **ca generate rsa** command generates Rivest, Shamir, and Adleman (RSA) key pairs for the PIX Security Appliance. RSA keys are generated in pairs of one public RSA key and one private RSA key. Configuration Mode.
clear aaa	Removes **aaa** command statements from the configuration.
debug ssh	Debug information and error messages associated with the **ssh** command.
privilege [show | clear | configure] level *level* **[mode** *enable* **|** *configure*] **command** *command*	Configures or displays command privilege levels. Configuration mode.
show ca	Displays information about CEP (Certificate Enrollment Protocol).

Command	Description
show ssh [sessions [*ip_address*]]	Displays active, all or host-specific SSH sessions on the PIX Security Appliance.
ssh timeout *mm*	Specify a host for PIX Security Appliance console access through Secure Shell (SSH). Configuration mode.
static [(*internal_if_name*, *external_if_name***)] {tcp | udp}{***global_ip* **| interface}** *global_port local_ip local_port* **[netmask** *mask***][***max_conns* **[***emb_limit* **[norandomseq]]]**	Configure a persistent one-to-one address translation rule by mapping a local IP address to a global IP address. This is also known as Static Port Address Translation (Static PAT). Configuration mode.
username *username* **{[{nopassword | password** *password***} [encrypted]] [privilege** *level***]}**	Sets the username for the specified privilege level. Configuration mode.

Step 1 Enable Command Authorization with Privileged Mode Passwords

To enable command authorization with privileged mode passwords, complete the following steps:

a. Set privilege level 10 for the enable mode **configure** command:

```
PixP(config)# privilege configure level 10 mode enable command
configure
```

b. Set privilege level 10 for the **nameif** command:

```
PixP(config)# privilege level 10 command nameif
```

c. Set privilege level 12 for the **interface** command:

```
PixP(config)# privilege level 12 command interface
```

d. Assign an enable password for privileged level 15:

```
PixP(config)# enable password prmode15
```

e. Assign an enable password for privileged level 5:

```
PixP(config)# enable password prmode5 level 5
```

f. Assign an enable password to privileged level 10:

```
PixP(config)# enable password prmode10 level 10
```

g. Assign an enable password to privileged level 12:

```
PixP(config)# enable password prmode12 level 12
```

1. Why would different levels and passwords be assigned?

_____

_____

Answer: Different privilege levels and passwords can be given to individuals or groups of individuals to restrict access to only the privilege level that is appropriate and necessary for those users.

h. Enable command authorization by entering the following command:

```
PixP(config)# aaa authorization command LOCAL
```

1. What other command authorization services can be used? Why can't RADIUS be used?

_____

_____

Answer: TACACS+ can also be used. RADIUS cannot be used because authorization is not supported in the protocol.

i. Exit configuration mode:

```
PixP(config)# exit
PixP#
```

j. Exit privileged mode:

```
PixP# exit
Logoff
Type help or '?' for a list of available commands.
PixP>
```

Step 2 Test the Command Authorization

To test the command authorization configured in Step 1, complete the following steps:

a. Enter privileged mode level 12. When prompted for a password, enter **prmode12**.

```
PixP> enable 12
Password:
PixP#
```

b. Enter configuration mode:

```
PixP# configure terminal
```

c. Verify that the **interface** command is useable:

```
PixP(config)# interface ethernet2
```

d. Verify that the **nameif** command is useable:

```
PixP(config-if)# nameif PRIVTEST
```

e. View the configuration:

```
PixP(config-if)# show nameif
Interface                Name                    Security
Ethernet0                outside                   0
Ethernet1                inside                  100
Ethernet2                PRIVTEST                 50
```

f. Exit configuration mode:

```
PixP(config)# end
PixP#
```

g. Exit privileged mode:

```
PixP# exit
Logoff
```



```
Type help or '?' for a list of available commands.
PixP>
```

h. Enter privileged mode level 10. When prompted for a password, enter **prmode10**:

```
PixP> enable 10
Password:
PixP#
```

i. Enter configuration mode:

```
PixP# configure terminal
PixP(config)#
```

j. Try to use the **interface** command:

```
PixP(config)# interface ethernet2
Command authorization failed.
```

k. Exit configuration mode:

```
PixP(config)# exit
PixP#
```

l. Exit privileged mode:

```
PixP# exit
Logoff
Type help or '?' for a list of available commands.
PixP>
```

m. Enter privileged mode level 5. When prompted for a password, enter **prmode5**.

```
PixP> enable 5
Password:
PixP#
```

n. Try to enter configuration mode:

```
PixP# configure terminal
Command authorization failed.
```

o. Exit privileged mode:

```
PixP# exit
Logoff
Type help or '?' for a list of available commands.
PixP>
```

p. Enter privileged mode. When prompted for a password, enter **prmode15**.

```
PixP> enable
Password:
PixP#
```

q. Enter configuration mode:

```
PixP# configure terminal
PixP(config)#
```


Step 3 Generate an RSA Key Pair

To generate an RSA key pair to encrypt the SSH terminal session, complete the following steps:

a. Delete any previously created RSA keys:

```
PixP(config)# crypto key zeroize rsa
```

b. Save the configuration to complete the erasure of the old RSA key pair:

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

c. Configure the domain name:

```
PixP(config)# domain-name cisco.com
```

d. Generate an RSA key pair to use to encrypt SSH sessions:

```
PixP(config)# crypto key generate rsa modulus 1024
INFO: The name for the keys will be: <Default-RSA-Key>
Keypair generation process begin. Please wait...
PixP(config)#
```

1. What are the modulus sizes that can be used?

   _____

   Answer: 512, 768, 1024, 2048

e. Save the keys to Flash memory:

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

f. View the public key:

```
PixP(config)# show crypto key mypubkey rsa
Key pair was generated at: 16:05:11 UTC Jun 4 2005
Key name: <Default-RSA-Key>
 Usage: General Purpose Key
 Modulus Size (bits): 1024
30819f30 0d06092a 864886f7 0d010101 05000381 8d003081 89028181
00bc43bf
33d9c65d e508b6df ecf71e37 5574a21d 56185faf cbb9fe14 5a345222
42cd2927
604fd719 a58d4f82 dc382fc4 ae037d15 f4f11ca8 06020c8d 5cd350d1
9bf19457
a6dc1a86 f1e101ae 842b0281 f42f38c5 c8e5c095 711ac751 f28d693f
ffdcb40f
2892169e 90be60dd 15c2fdc9 b8bda690 e55b29bf 670ed794 30e9c012
5f020301 0001
```

(where P = pod number)

Step 4 Connect to the PIX Security Appliance using SSH

To securely connect to the PIX Security Appliance using SSH, complete the following steps:

a. Enable SSH debugging:

```
PixP(config)# debug ssh
SSH debugging on
```


b. Grant SSH access to the inside subnet:

- For a local lab:

```
PixP(config)# ssh 10.0.P.0 255.255.255.0 inside
```

(where P = pod number)

c. Set the SSH inactivity timeout to 30 minutes:

```
PixP(config)# ssh timeout 30
```

d. Minimize, but do not close, the HyperTerminal session window. Double-click the **PuTTY** icon on the desktop. The shortcut will vary depending on the SSH client used.

e. Enter the IP Address of the pod PIX.

```
10.0.P.1
```

f. Select the **SSH** radio button.

g. Click **Yes** to the Security Warning window. The SSH Authentication window opens.

h. The following will be displayed in the PIX console:

```
SSH: Device opened successfully.

SSH0: SSH client: IP = 'insidehost'  interface # = 2

SSH: host key initialised

SSH: license supports 3DES: 2

SSH: license supports DES: 2

SSH0: starting SSH control process

SSH0: Exchanging versions - SSH-1.99-Cisco-1.25

SSH0: send SSH message: outdata is NULL

server version string:SSH-1.99-Cisco-1.25SSH0: receive SSH message:
   83 (83)

SSH0: client version is - SSH-2.0-PuTTY-Release-0.56

client version string:SSH-2.0-PuTTY-Release-0.56SSH0: begin server
   key generation

SSH0: complete server key generation, elapsed time = 1980 ms

SSH2 0: SSH2_MSG_KEXINIT sent

SSH2 0: SSH2_MSG_KEXINIT received

SSH2: kex: client->server aes256-cbc hmac-sha1 none

SSH2: kex: server->client aes256-cbc hmac-sha1 none

SSH2 0: expecting SSH2_MSG_KEXDH_INIT

SSH2 0: SSH2_MSG_KEXDH_INIT received

SSH2 0: signature length 143

SSH2: kex_derive_keys complete

SSH2 0: newkeys: mode 1

SSH2 0: SSH2_MSG_NEWKEYS sent

SSH2 0: waiting for SSH2_MSG_NEWKEYS

SSH2 0: newkeys: mode 0

SSH2 0: SSH2_MSG_NEWKEYS received
```


i. Enter **pix** as the username and **cisco** as the pass phrase.

```
SH(pix): user authen method is 'no AAA', aaa server group ID = 0
SSH2 0: authentication successful for pix
SSH2 0: channel open request
SSH2 0: pty-req request
SSH2 0: requested tty: xterm, height 24, width 80
SSH2 0: shell request
SSH2 0: shell message received
SSH2 0: channel window adjust message received 52
SSH2 0: channel window adjust message received 7
```

j. In the SSH window, enter the privileged mode. When prompted for a password, enter **prmode15**.

```
PixP>enable
Password:
PixP#
```

k. Enter configuration mode:

```
PixP# configure terminal
PixP(config)#
```

l. To view the status the SSH session, enter the following command:

```
PixP(config)# show ssh sessions

SID Client IP  Version        Mode Encryption Hmac   State          Username
0   insidehost      2.0       IN   aes256-cbc sha1   SessionStarted   pix
                              OUT  aes256-cbc sha1   SessionStarted   pix
```

m. Disconnect the SSH session:

```
PixP(config)# ssh disconnect 0
```

n. Return to the HyperTerminal session window, and change the PIX Security Appliance's Telnet password from **cisco** to **sshpass**:

```
PixP(config)# passwd sshpass
```

o. Exit configuration mode:

```
PixP(config)# exit
PixP#
```

p. Exit privileged mode:

```
PixP# exit
Logoff
Type help or '?' for a list of available commands.
PixP>
```

q. Minimize the HyperTerminal window. Do not close it.

r. Leave this HyperTerminal session open throughout the rest of this lab exercise.

s. Establish another SSH session to the PIX Security Appliance. When prompted to authenticate, enter **pix** as the username and **sshpass** as the pass phrase.

Step 5 Configure Local User Authentication using a Secure SSH Session

To configure local user authentication using a secure SSH session, complete the following steps:

a. Enter privileged mode. When prompted for a password, enter **prmode15**.

```
PixP>enable
Password:
PixP#
```

b. Enter configuration mode:

```
PixP# configure terminal
PixP(config)#
```

c. Create three user accounts in the local database:

```
PixP(config)# username user10 password user10pass privilege 10
PixP(config)# username user12 password user12pass privilege 12
PixP(config)# username admin password adminpass privilege 15
```

1. Why is setting user's privilege level different recommended?

_____

_____

Answer: The concept of least privilege access required should be assigned to the users. The users should have access to only the privilege level that is appropriate and necessary to perform their needed tasks.

d. Enable authentication using the LOCAL database:

```
PixP(config)# aaa authentication enable console LOCAL
```

e. Disconnect the SSH session.

Step 6 Test Command Authorization with Local User Authentication

To test command authorization with local user authentication, complete the following steps:

a. Return to the HyperTerminal session.

b. Enter privileged mode. When prompted for a username, enter **user12**. When prompted for a password, enter **user12pass**.

```
PixP> enable
Username:
Password:
PixP#
```

c. Enter configuration mode:

```
PixP# configure terminal
PixP(config)#
```

d. View the user account that is currently logged in:

```
PixP(config)# show curpriv
Username : user12
```



```
Current privilege level : 12
Current Mode/s : P_PRIV P_CONF
```

e. Verify that the **interface** command is useable:

```
PixP(config)# interface ethernet2
```

Verify that the **nameif** command is useable by attempting to change the Ethernet 2 name back to **dmz**:

```
PixP(config-if)# nameif dmz
```

f. View the configuration:

```
PixP(config)# show nameif
Interface               Name                    Security
Ethernet0               outside                   0
Ethernet1               inside                  100
Ethernet2               dmz                      50
```

g. Try to create a static mapping for a demilitarized zone (DMZ) host 172.16.P.4:

```
PixP(config)# static (dmz,outside) 192.168.P.18 172.16.P.4 netmask
255.255.255.255
Command authorization failed
```

(where P = pod number)

h. Log out of the user12 account:

```
PixP(config)# logout
Logoff
Type help or '?' for a list of available commands.
PixP>
```

i. Log in to the user 10 account. When prompted for a username, enter **user10**. When prompted for a password, enter **user10pass**.

```
PixP>login
Username:
Password:
PixP#
```

j. Enter configuration mode:

```
PixP# config t
PixP(config)#
```

k. Try to use the **interface** command to configure the Ethernet 2 interface:

```
PixP(config)# interface ethernet2
Command authorization failed
```

n. Log out of the user10 account:

```
PixP(config)# logout
Logoff
Type help or '?' for a list of available commands.
PixP>
```


o. Log in to the user admin account. When prompted for a username, enter **admin**. When prompted for a password, enter **adminpass**.

```
PixP>login
Username:
Password:
PixP#
```

p. Enter configuration mode:

```
PixP# configure terminal
PixP(config)#
```

q. Clear the AAA configuration:

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


Lab 8.4.4 Perform Password Recovery on the PIX Security Appliance

Objective

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

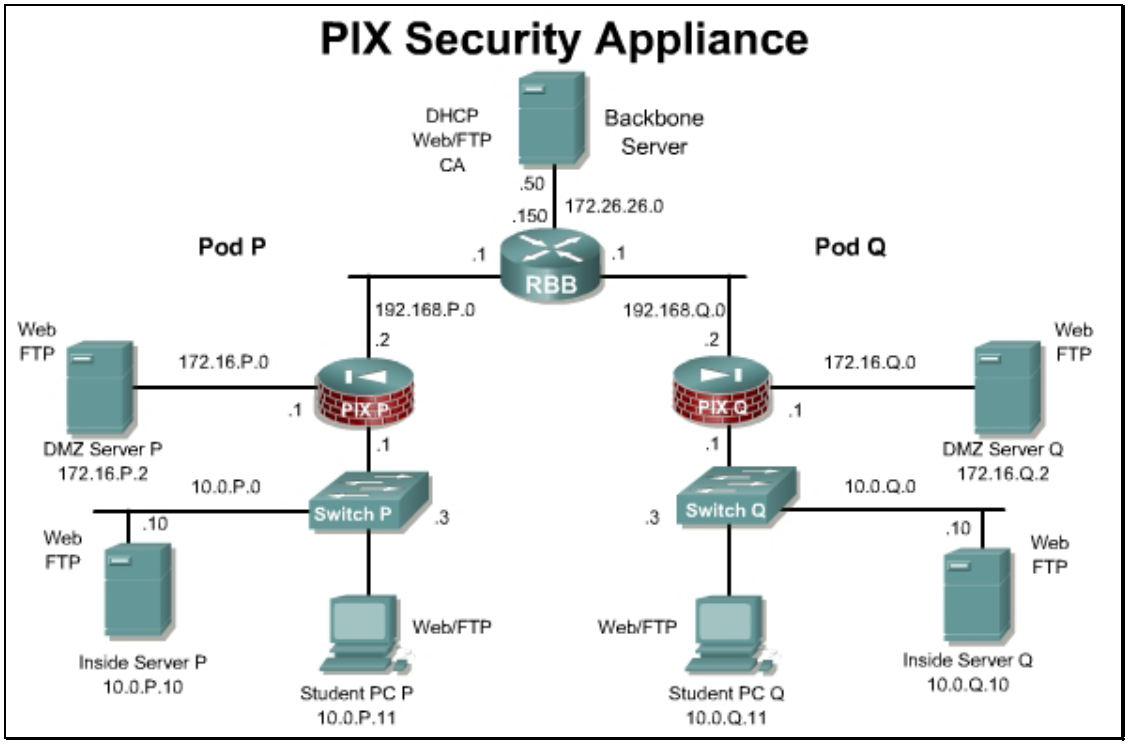
- Upgrade the PIX Security Appliance image.
- Perform password recovery procedures.

Scenario

One of the major job duties of a network administer is planning. Network administrators plan for new network design projects, future performance requirements, image upgrades, and contingency plans. Upgrading and performing password recovery are core skills needed by all network administrators. There may be situations when network administrators are locked-out of their PIX Security Appliance. Password lockouts can occur from incorrectly configured enable passwords, incorrectly configured AAA parameters, and improperly documenting passwords. In this lab, students will perform the steps involved in performing password recovery and upgrading the image of a PIX Security Appliance.

Topology

This figure illustrates the lab network environment.



Preparation

Begin with the standard lab topology and verify the starting configuration on the 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, download the proper password recovery file and copy to the TFTP root folder. Some TFTP programs may not work properly with the PIX.

Tools and Resources

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

- Standard PIX Security Appliance lab topology
- Console cable
- HyperTerminal
- TFTP server
- PIX password recovery file (np70.bin)

Additional materials

Students can use the following links for more information on the objectives covered in this lab:

http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_password_recovery09186a008009478b.shtml

http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_configuration_guide_chapter09186a0080450b92.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
clear xlate	Clears the contents of the translation slots.
copy tftp[:[[//*location*] [/*tftp_pathname*]]] **flash**[:[*path*]]	Downloads Flash memory software images via TFTP without using monitor mode.
reload	Reloads the PIX Security Appliance.

Step 1 Perform a Password Recovery for the PIX Security Appliance Model 515E

To perform a password recovery for the PIX Security Appliance model 515E, complete the following steps:

a. Open and minimize the TFTP server on the desktop.

b. Clear the translation table on the PIX Security Appliance:

```
PixP(config)# clear xlate
```

c. Create an enable password for entering into privileged mode:

```
PixP(config)# enable password badpassword
```


d. Save the configuration:

```
PixP(config)# write memory
Building configuration...
Cryptochecksum: e18c684e d86c9171 9f63acf0 f64a8b43
[OK]
```

e. Log out of the admin account:

```
PixP(config)# logout
Logoff
Type help or '?' for a list of available commands.
PixP>
```

f. Attempt to enter privileged mode with the old password, **prmode15**:

```
PixP> enable
Password:
Invalid password:
```

g. Enter privileged mode with the new password, **badpassword**:

```
Password:
PixP#
```

h. Reboot the PIX Security Appliance.

```
PixP# reload
```

Note If the enable password is lost and the **reload** command cannot be used, the PIX can be powered off and then powered back on using the power switch on the back of the appliance.

i. When the PIX Security Appliance reboots, interrupt the boot process to enter monitor mode. To do this, press the Escape key or send a break character.

j. Specify the PIX Security Appliance interface to use for TFTP:

```
monitor> interface 1
```

k. Specify the PIX Security Appliance interface IP address:

```
monitor> address 10.0.P.1
```

(where P = pod number)

l. Verify connectivity to the TFTP server:

```
monitor> ping 10.0.P.11
```

(where P = pod number)

m. Name the server:

```
monitor> server 10.0.P.11
```

(where P = pod number)

m. Name the image filename:

```
monitor> file np70.bin
```

o. Start the TFTP process:

```
monitor> tftp
```



```
tftp
np70.bin@10.0.P.11.....................................................
.....................................................................
.....................
Received 73728 bytes
Cisco Secure PIX Firewall password tool (3.0) #0: Wed Mar 27
11:02:16 PST 2002
Flash=i28F640J5 @ 0x300
BIOS Flash=AT29C257 @ 0xd8000
```

(where P = pod number)

p. When prompted, press **Y** to erase the password:

```
Do you wish to erase the passwords? [yn] y
The following lines will be removed from the configuration:
enable password GlFe5rCOwv2JUi5H level 5 encrypted
enable password .7P6WvOReYzHKnus level 10 encrypted
enable password tgGMO76/Nf26X5Lv encrypted
passwd w.UT.4mPsVA418Ij encrypted
Do you want to remove the commands listed above from the
configuration? [yn]
Please enter a y or n.
```

q. When prompted, press **Y** to erase the passwords:

```
Do you want to remove the commands listed above from the
configuration? [yn] y
Passwords and aaa commands have been erased.
```

The system automatically erases the passwords and starts rebooting.

> **Note** If AAA is running, it will prompt for a username and password (user: pix, password: <enter>).

r. Verify that the password **badpassword** has been erased by entering privileged mode on the PIX Security Appliance:

```
Pix> enable
password: <Enter>
PixP#
```

Step 2 Load the PIX Security Appliance 515E Image Using TFTP

To load the PIX Security Appliance 515E image using TFTP, complete the following steps:

a. Ask the instructor for the PIX security appliance image file name. Use the **copy tftp flash** command to load the image file:

```
PixP# copy tftp: flash:
Address or name of remote host[]? 10.0.1.10
Source filename []? pix-701.bin
Destination filename [pix-701.bin]? <Enter>
```


(where P = pod number)

b. Use the **show bootvar** command to ensure that the boot image file is correctly defined. If it is not, be sure to use the **boot system flash** command to set the boot image:

```
PixP# show bootvar
BOOT variable = flash:/pix701.bin
Current BOOT variable = flash:/pix701.bin
CONFIG_FILE variable =
Current CONFIG_FILE variable =
```

c. After the PIX Security Appliance has received the image from the TFTP server and it has been verified that the boot variable is pointing to the correct image, reload the PIX Security Appliance. When prompted to confirm, press **Enter**.

```
PixP# reload
Proceed with reload? [confirm] <Enter>
```

(where P = pod number)

d. After the PIX finishes reloading, enter the **show version** command to verify that the correct version PIX Security appliance has been loaded.

```
PixP> show version
Cisco PIX Security Appliance Software Version 7.0(1)
Device Manager Version 5.0(1)
Compiled on Thu 31-Mar-05 14:37 by builders
System image file is "flash:/pix701.bin"
Config file at boot was "startup-config"
Pix1 up 7 mins 48 secs
Hardware:   PIX-515E, 64 MB RAM, CPU Pentium II 433 MHz
Flash E28F128J3 @ 0xfff00000, 16MB
BIOS Flash AM29F400B @ 0xfffd8000, 32KB
 0: Ext: Ethernet0           : media index  0: irq 10
 1: Ext: Ethernet1           : media index  1: irq 11
 2: Ext: Ethernet2           : media index  2: irq 11
Licensed features for this platform:
Maximum Physical Interfaces : 6
Maximum VLANs               : 25
Inside Hosts                : Unlimited
Failover                    : Active/Active
VPN-DES                     : Enabled
VPN-3DES-AES                : Enabled
Cut-through Proxy           : Enabled
Guards                      : Enabled
URL Filtering               : Enabled
Security Contexts           : 5
```



```
GTP/GPRS                    : Disabled
VPN Peers                   : Unlimited
This platform has an Unrestricted (UR) license.
Serial Number: 807043526
Running Activation Key: 0xc335d572 0xa882e04f 0x24f21c7c 0xbbe45090
0x420cf18a
Configuration has not been modified since last system restart.
```

(where P = pod number)

