



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

### Objectives

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

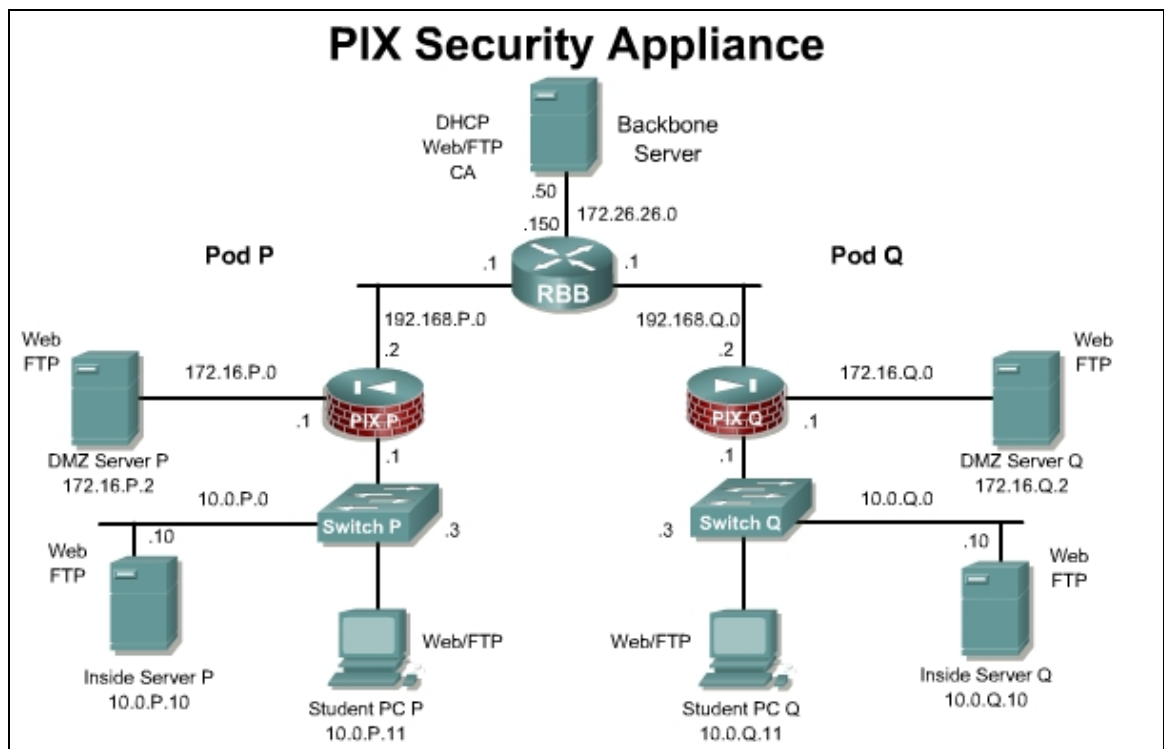
- Prepare for Configuring CA Support
- Configure CA Support
- Configure and Verify IKE and IPsec Parameters
- Verify the VPN connection
- Verify the VPN status and configuration using ASDM

### 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/sw/secursw/ps2120/products_configuration_guide_book09186a00803d8a02.html)

[http://www.cisco.com/en/US/products/ps6120/products\\_configuration\\_guide\\_chapter09186a008045247b.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
<b>crypto ipsec</b> <i>map-name seq-num transform-set transform-set-name transform1 [transform2]</i>	To define a transform set, use the <b>crypto ipsec transform-set</b> command in global configuration mode. This command is used to identify the IPsec encryption and hash algorithms to be used by the transform set.
<b>crypto map</b> <i>map-name seq-num match address acl_name</i>	To assign an access list to a crypto map entry, use the <b>crypto map match address</b> command in global configuration mode.
<b>crypto map</b> <i>map-name seq-num set peer {ip_address   hostname}{...ip_address   hostname10}</i>	To specify an IPsec peer in a crypto map entry, use the <b>crypto map set peer</b> command in global configuration mode.
<b>crypto map</b> <i>map-name seq-num set transform-set transform-set-name1 [... transform-set-name9]</i>	To specify the transform sets to use with the crypto map entry, use the <b>crypto map set transform-set</b> command in global configuration mode.
<b>crypto map</b> <i>map-name interface interface-name</i>	Use the <b>crypto map interface</b> command in global configuration mode to apply a previously defined crypto map set to an interface.

Command	Description
<b>isakmp enable</b> <i>interface-name</i>	To enable ISAKMP negotiation on the interface on which the IPsec peer communicates with the PIX security appliance, use the <b>isakmp enable</b> command in global configuration mode.
<b>isakmp policy</b> <i>priority</i> <b>authentication</b> { <i>pre-share</i>   <i>dsa-sig</i>   <i>rsa-sig</i> }	To specify an authentication method within an IKE policy, use the <b>isakmp policy authentication</b> command in global configuration mode. IKE policies define a set of parameters for IKE negotiation.
<b>show running-config isakmp</b>	To display the complete ISAKMP configuration, use the <b>show running-config isakmp</b> command in global configuration or privileged EXEC mode.
<b>show running-config static</b>	To display all static commands in the configuration, use the <b>show running-config static</b> command in privileged EXEC mode.
<b>sysopt connection permit-ipsec</b>	To let IPsec packets bypass interface access lists, use the <b>sysopt connection permit-ipsec</b> command in global configuration mode. Group policy and per-user authorization access lists still apply to the traffic.
<b>tunnel-group</b> <i>name</i> <b>type</b> <i>type</i>	To create and manage the database of connection-specific records for IPsec, use the <b>tunnel-group</b> command in global configuration mode.
<b>tunnel-group</b> <i>name</i> <b>ipsec-attributes</b>	To enter the ipsec-attribute configuration mode, use the <b>tunnel-group ipsec-attributes</b> 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 7bachfab 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
```

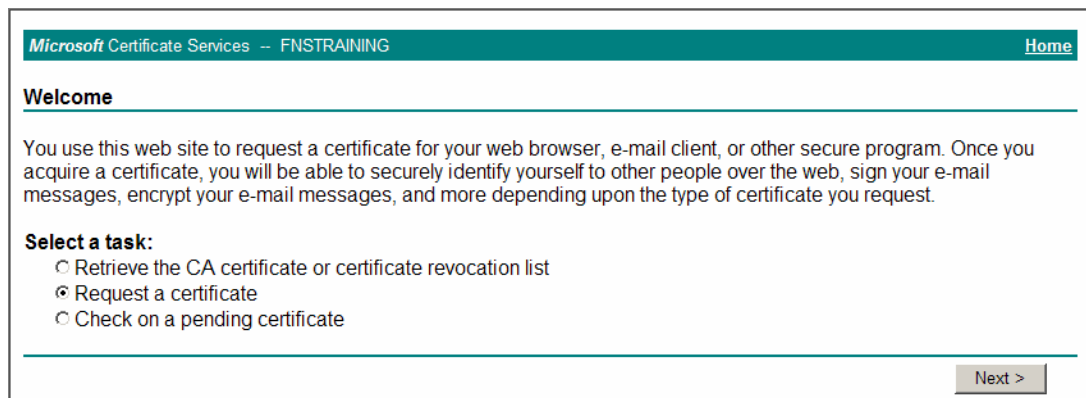
(where Q = peer pod number)

- 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?

---

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
7fad8b95 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.
```

- I. 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:
Pixl.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
Pixl(config)#

CRYPTO_PKI: Cert record not found, returning E_NOT_FOUND
Current Certificate list contents:
Certificate 1:
```

```

SERIAL: 0aa3f49400000000000002
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: 0aa3f4f200000000000003
ISSUER: cn=FNSTRaining,ou=CNAP,o=Cisco,l=Phoenix,st=AZ,c=US
Certificate 2:
SERIAL: 0aa3f49400000000000002
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=US
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: 4848f1710000000000013
ISSUER: cn=FNSTRaining,ou=CNAP,o=Cisco,l=Phoenix,st=AZ,c=US
Certificate 2:
SERIAL: 0aa3f4f20000000000003
ISSUER: cn=FNSTRaining,ou=CNAP,o=Cisco,l=Phoenix,st=AZ,c=US
Certificate 3:
SERIAL: 0aa3f4940000000000002
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: 4848f1710000000000013
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=FNSTRRAINING  
ou=CNAP  
o=Cisco  
l=Phoenix  
st=AZ  
c=US  
Subject Name:  
cn=FNSTRRAINING  
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?

\_\_\_\_\_

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

\_\_\_\_\_

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?

\_\_\_\_\_

## 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	<b>QM_IDLE</b>	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
```

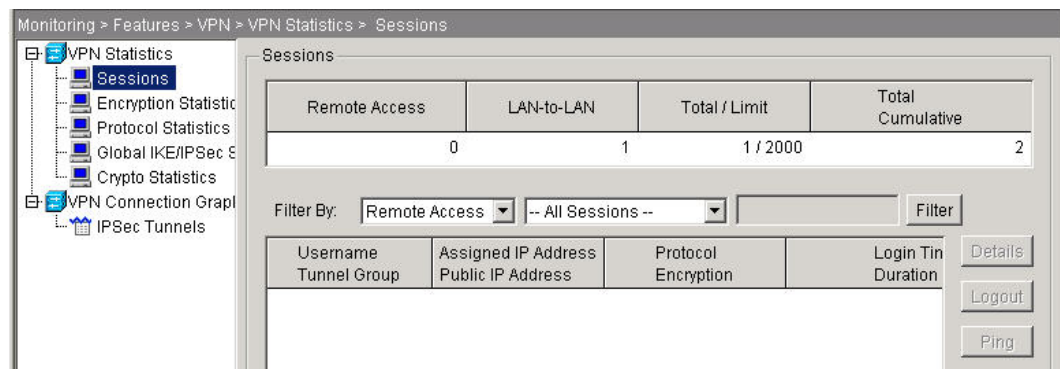
```
#pkts encaps: 6, #pkts encrypt: 6, #pkts digest: 6
#pkts decaps: 6, #pkts decrypt: 6, #pkts verify: 6
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 6, #pkts comp failed: 0, #pkts decomp failed: 0
#send errors: 0, #recv errors: 0
```

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

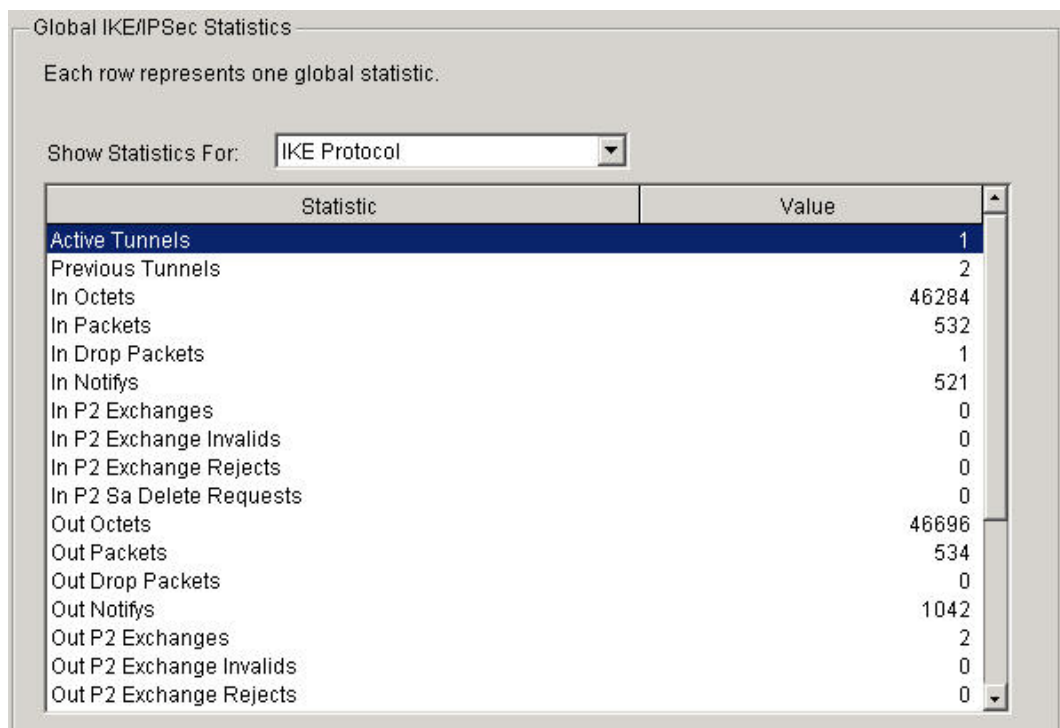
## Task 6 Verify the VPN Status and Configuration using ASDM

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

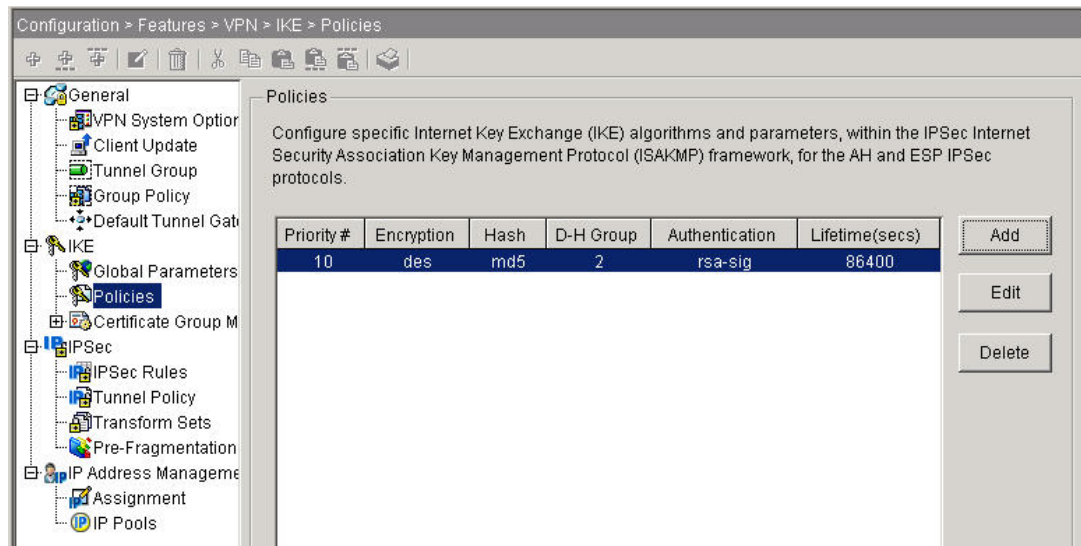
- a. Initiate an ASDM session with the PIX Security Appliance.
- b. Navigate to **Monitoring>Tasks>VPN>VPN Statistics>Sessions**. One LAN-to-LAN connection should be displayed.



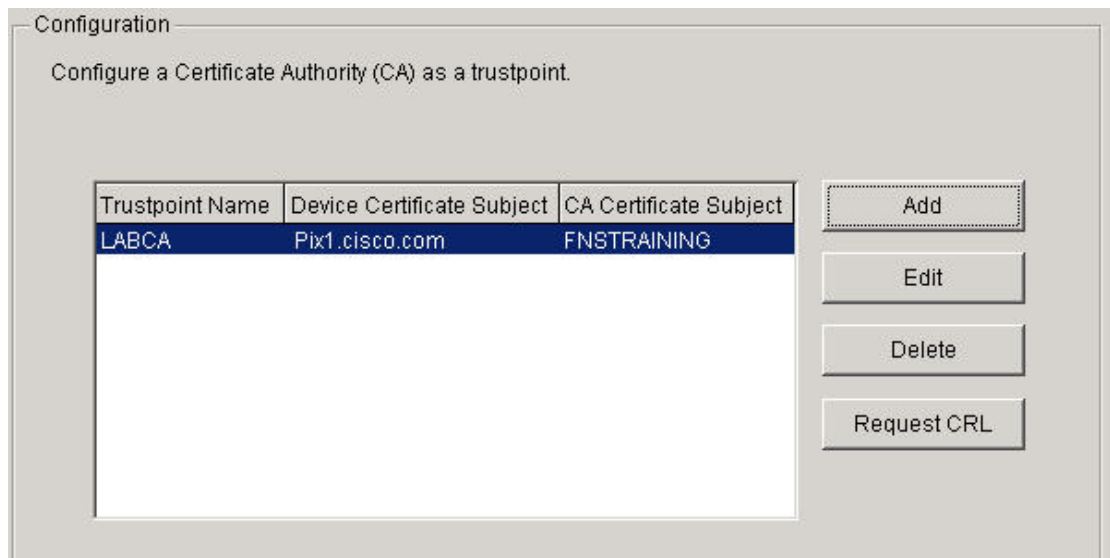
- c. Navigate to the **Monitoring>Features>VPN>VPN Statistics>Global IKE/IPSec Statistics** to view the IKE and IPSec statistics.



- 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.

Trustpoint Name: LABCA

☐ Generate a self-signed certificate on enrollment

If this option is enabled, only Key Pair and Certificate Parameters can be specified.

Enrollment Settings | CRL Retrieval Policy | CRL Retrieval Method | Advanced

Key Pair: <Default-RSA-K...> Show Details New Key Pair...

Challenge Password: Confirm Challenge Password:

Enrollment Mode can only be specified if there are no certificates associated with this trustpoint.

Enrollment Mode

Automatic enrollment can only be specified if the selected key pair is of type RSA.

☐ Use manual enrollment

☒ Use automatic enrollment

Enrollment URL: http:// 172.26.26.50:80/certsrv/msce

Retry Period: 1 minutes

Retry Count: 20 (Use 0 to indicate unlimited retries)

Certificate Parameters...

OK Cancel Help

- g. Exit ASDM.