



CA Configuration Examples

This chapter provides configuration examples showing how to configure interoperability between two PIX Firewall units (PIX Firewall 1 and 2) for site-to-site VPN using CAs for device enrollment and certificate requests. Because each peer will be using digital certificates for the device authentication method, each peer must be configured to enroll with a given CA and to request to obtain its CA-signed certificates from the CA. The examples shown in this chapter illustrate how to set up the peers to obtain certificates from a CA that is either within a private network (referred to as an in-house CA server) or outside of a private network.

Most of the CA servers in the examples are in-house CA servers and are placed within the DMZ network of one PIX Firewall network (PIX Firewall 1) with the exception of the VeriSign CA server. The VPN peer, PIX Firewall 2, must enroll and obtain its CA-signed certificates from the CA server residing within the network of PIX Firewall 1. PIX Firewall 2's enrollment and certificate request process is accomplished through the Internet. For a more secure way of performing CA enrollment and certificate requests, one example is provided that shows how to perform the CA enrollment and certificate requests within an encrypted tunnel. The example first shows how to establish a VPN tunnel using the authentication method of a pre-shared key for IKE authentication. After the tunnel is established, PIX Firewall 2 is shown to be configured to perform the CA enrollment and certificate request via the tunnel.

Currently, the PIX Firewall supports the following CA servers:

- VeriSign, support is provided through the VeriSign Private Certificate Services (PCS) and the OnSite service, which lets you establish a CA system for issuing digital certificates. The VeriSign CA server in the given example is a server that resides outside of the private network within the Internet.
- Entrust, Entrust VPN Connector, version 4.1 (build 4.1.0.337) or later. The Entrust CA server is an in-house CA server solution.
- Baltimore Technologies, UniCERT Certificate Management System, version 3.1.2 or later. The Baltimore CA server is an in-house CA server solution.
- Microsoft Windows 2000, specifically the Windows 2000 Advanced Server, version 5.00.2195 or later. The Windows 2000 CA server is an in-house CA server solution.

The following sections are included in this chapter:

- IPSec/VPN Tunnel Using VeriSign Digital Certificates
- IPSec/VPN Tunnel Using Entrust Digital Certificates
- IPSec/VPN Tunnel Using Baltimore Digital Certificates
- IPSec/VPN Tunnel Using Microsoft Digital Certificates
- Digital Certificate Issued via an Encrypted Tunnel

**Note**

The first four examples shown are essentially the same, differing only within the CA server configuration steps.

For CA background information, see Chapter 4, “About CA.” For more information about CA configurations, see Chapter 7, “Configuring CA.”

IPSec/VPN Tunnel Using VeriSign Digital Certificates

This section provides configuration examples showing how to configure interoperability between two PIX Firewall units (PIX Firewall 1 and 2) for site-to-site VPN using the VeriSign CA server for device enrollment, certificate requests, and digital certificates for the IKE authentication. VeriSign issues its CA-signed certificates over the Internet.

The two VPN peers in the configuration examples are shown to be configured to enroll with VeriSign at the IP address of 209.165.202.130 and to obtain their CA certificates from this CA server. Once each peer obtains its CA-signed certificate, tunnels can be established between the two VPN peers using digital certificates as the authentication method used during IKE authentication. The peers dynamically authenticate each other using the digital certificates.

**Note**

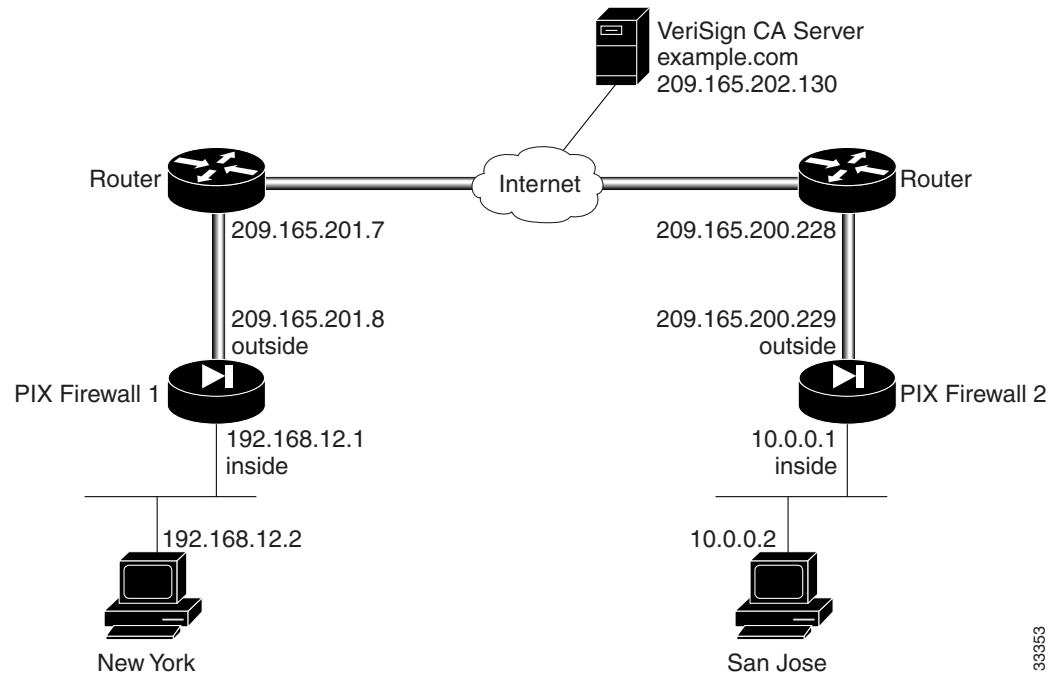
VeriSign’s actual CA server address differs. The example CA server address is to be used for example purposes only.

This section includes the following topics:

- Configuring PIX Firewall 1 for a VeriSign Certificate
- Configuring PIX Firewall 2 for a VeriSign Certificate

This example uses the network diagram shown in Figure 11-1.

Figure 11-1 VPN Tunnel Network



33353

Configuring PIX Firewall 1 for a VeriSign Certificate

Follow these steps to configure PIX Firewall 1:

Step 1 Define a host name:

```
hostname NewYork
```

Step 2 Define the domain name:

```
domain-name example.com
```

Step 3 Generate the PIX Firewall RSA key pair:

```
ca generate rsa key 512
```

This command is not stored in the configuration.

Step 4 Define VeriSign-related enrollment commands:

```
ca identity example.com 209.165.202.130
ca configure example.com ca 2 100 crloptional
```

These commands are stored in the configuration. “2” is the retry period, “100” is the retry count, and the **crloptional** option disables CRL checking.

Step 5 Authenticate the CA by obtaining its public key and its certificate:

```
ca authenticate example.com
```

This command is not stored in the configuration.

- Step 6** Request signed certificates from your CA for your PIX Firewall's RSA key pair. Before entering this command, contact your CA administrator because they will have to authenticate your PIX Firewall manually before granting its certificate:

```
ca enroll example.com abcdef
```

“abcdef” is a challenge password. This can be anything. This command is not stored in the configuration.

- Step 7** Verify that the enrollment process was successful using the **show ca certificate** command:

```
show ca certificate
```

- Step 8** Save keys and certificates, and the CA commands (except those indicated) in Flash memory:

```
ca save all
write memory
```



Note Use the **ca save all** command any time you add, change, or delete **ca** commands in the configuration. This command is not stored in the configuration.

- Step 9** Create a net static:

```
static (inside,outside) 192.168.12.0 192.168.12.0
```

- Step 10** Configure an IKE policy:

```
isakmp enable outside
isakmp policy 8 auth rsa-sig
```

- Step 11** Create a partial access list:

```
access-list 90 permit ip 192.168.12.0 255.255.255.0 10.0.0.0 255.0.0.0
```

- Step 12** Configure a transform set that defines how the traffic will be protected:

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

- Step 13** Define a crypto map:

```
crypto map toSanJose 20 ipsec-isakmp
crypto map toSanJose 20 match address 90
crypto map toSanJose 20 set transform-set strong
crypto map toSanJose 20 set peer 209.165.200.229
```

- Step 14** Apply the crypto map to the outside interface:

```
crypto map toSanJose interface outside
```

- Step 15** Tell the PIX Firewall to implicitly permit IPSec traffic:

```
sysopt connection permit-ipsec
```

Table 11-1 lists the configuration for PIX Firewall 1.

Table 11-1 PIX Firewall 1 VPN Tunnel Configuration

Configuration	Description
<code>nameif ethernet0 outside security0</code> <code>nameif ethernet1 inside security100</code>	PIX Firewall provides nameif command statements for the interfaces in the configuration.
<code>enable password 8Ry2YjIyt7RRXU24 encrypted</code> <code>passwd 2KFQnbNIdI.2KYOU encrypted</code>	Default values for the privileged mode password and the Telnet password.
<code>hostname NewYork</code>	Define a host name for the PIX Firewall.
<code>domain-name example.com</code>	Set the domain name.
<code>fixup protocol ftp 21</code> <code>fixup protocol http 80</code> <code>fixup protocol smtp 25</code> <code>fixup protocol h323 1720</code> <code>fixup protocol rsh 514</code> <code>fixup protocol sqlnet 1521</code>	Default fixup protocol values that define port usage.
<code>names</code> <code>pager lines 24</code> <code>no logging on</code>	Default values that let you use names instead of IP addresses, display 24 lines of text before you are prompted to continue, and disable syslog output.
<code>interface ethernet0 auto</code> <code>interface ethernet1 auto</code>	Default interface definitions indicating that each Ethernet interface has automatic sensing capabilities to determine line speed and duplex.
<code>mtu outside 1500</code> <code>mtu inside 1500</code>	Set the maximum transmission unit values for the Ethernet interfaces.
<code>ip address outside 209.165.201.8 255.255.255.224</code> <code>ip address inside 192.168.12.1 255.255.255.0</code>	The IP addresses for each PIX Firewall interface.
<code>no failover</code> <code>failover ip address outside 0.0.0.0</code> <code>failover ip address inside 0.0.0.0</code>	Default values to disable failover.
<code>arp timeout 14400</code>	Default value specifying that the ARP cache be reinitialized every four hours.
<code>nat (inside) 0 0.0.0.0 0.0.0.0 0 0</code>	Disable NAT for the inside interface.
<code>nat 0 access-list 90</code> <code>access-list 90 permit ip 192.168.12.0 255.255.255.0</code> <code>10.0.0.0 255.0.0.0</code>	The nat 0 access-list command statement lets you exempt traffic that is matched by the access-list command statement from the NAT services. Adaptive Security remains in effect with the nat 0 access-list command. The access-list command statement permits IP traffic on all hosts on the inside network to be accessed by the hosts on PIX Firewall 2.
<code>no rip outside passive</code> <code>no rip outside default</code> <code>rip inside passive</code> <code>no rip inside default</code>	Default values to disable RIP listening or broadcasting. However, the inside interface does listen for RIP broadcasts.
<code>route outside 0.0.0.0 0.0.0.0 209.165.200.227 1</code>	Specify the router on the outside interface for default routes.
<code>timeout xlate 3:00:00 conn 1:00:00 half-closed</code> <code>0:10:00 udp 0:02:00</code> <code>timeout rpc 0:10:00 h323 0:05:00</code> <code>timeout uauth 0:05:00 absolute</code>	Default timer values.

Table 11-1 PIX Firewall 1 VPN Tunnel Configuration (continued)

Configuration	Description
<pre>aaa-server TACACS+ protocol tacacs+ aaa-server RADIUS protocol radius</pre>	Default values that permit access to the TACACS+ or RADIUS protocols; however, AAA is not used in this configuration.
<pre>no snmp-server location no snmp-server contact snmp-server community public no snmp-server enable traps</pre>	Default values to disable SNMP access.
<pre>crypto ipsec transform-set strong esp-3des esp-sha-hmac crypto map toSanJose 20 ipsec-isakmp crypto map toSanJose 20 match address 90 crypto map toSanJose 20 set peer 209.165.200.229 crypto map toSanJose 20 set transform-set strong crypto map toSanJose interface outside</pre>	Define the crypto map transforms, specify ISAKMP access, match the map to the access list (both use ID 90 to be associated), set the tunnel peer to be the outside interface IP address of PIX Firewall 2 (209.165.200.229), and apply the crypto map to the outside interface.
<pre>isakmp enable outside isakmp policy 9 encryption 3des</pre>	Configure the IKE policy.
<pre>ca identity example.com 209.165.202.130:cgi-bin/pkiclient.exe ca configure example.com ca 1 100 crloptional</pre>	Define VeriSign-related enrollment commands.
<pre>sysopt connection permit-ipsec</pre>	Tell the PIX Firewall to implicitly permit IPsec traffic.
<pre>telnet timeout 5 terminal width 80</pre>	Default values for how long a Telnet console session can be idle and that a console session should display up to 80 characters wide on the console computer.

Configuring PIX Firewall 2 for a VeriSign Certificate

Follow these steps to configure PIX Firewall 2:

Step 1 Define a host name:

```
hostname SanJose
```

Step 2 Define the domain name:

```
domain-name example.com
```

Step 3 Generate the PIX Firewall RSA key pair:

```
ca generate rsa key 1024
```

This command is not stored in the configuration.

Step 4 Define VeriSign-related enrollment commands:

```
ca identity example.com 209.165.202.130
ca configure example.com ca 1 20 crloptional
```

These commands are stored in the configuration. “2” is the retry period, “100” is the retry count, and the **crloptional** option disables CRL checking.

Step 5 Authenticate the CA by obtaining its public key and its certificate:

```
ca authenticate example.com
```

This command is not stored in the configuration.

Step 6 Request signed certificates from your CA for your PIX Firewall's RSA key pair. Before entering this command, contact your CA administrator because they will have to authenticate your PIX Firewall manually before granting its certificate:

```
ca enroll example.com abcdef
```

"abcdef" is a challenge password. This can be anything. This command is not stored in the configuration.

Step 7 Verify that the enrollment process was successful using the **show ca certificate** command:

```
show ca certificate
```

Step 8 Save keys and certificates, and the CA commands (except those indicated) in Flash memory:

```
ca save all
write memory
```



Note Use the **ca save all** command any time you add, change, or delete **ca** commands in the configuration. This command is not stored in the configuration.

Step 9 Create a net static:

```
static (inside,outside) 10.0.0.0 10.0.0.0
```

Step 10 Configure an IKE policy:

```
isakmp enable outside
isakmp policy 8 auth rsa-sig
```

Step 11 Create a partial access list:

```
access-list 80 permit ip 10.0.0.0 255.0.0.0 192.168.12.0 255.255.255.0
```

Step 12 Configure a transform set that defines how the traffic will be protected:

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

Step 13 Define a crypto map:

```
crypto map newyork 10 ipsec-isakmp
crypto map newyork 10 match address 80
crypto map newyork 10 set transform-set strong
crypto map newyork 10 set peer 209.165.201.8
```

Step 14 Apply the crypto map to the outside interface:

```
crypto map toSanJose interface outside
```

Step 15 Tell the PIX Firewall to implicitly permit IPSec traffic:

```
sysopt connection permit-ipsec
```

Table 11-2 lists the configuration for PIX Firewall 2.

Table 11-2 PIX Firewall 2 VPN Tunnel Configuration

Configuration	Description
<pre>nameif ethernet0 outside security0 nameif ethernet1 inside security100 nameif ethernet2 dmz security50 nameif ethernet3 perimeter security40</pre>	PIX Firewall provides nameif command statements interfaces in the default configuration, but in this case, the configuration required different names and security levels for the perimeter interfaces.
<pre>enable password 8Ry2YjIyt7RRXU24 encrypted passwd 2KFQnbNIdI.2KYOU encrypted</pre>	Default values for the privileged mode password and the Telnet password.
<pre>hostname SanJose</pre>	Define a host name for the PIX Firewall.
<pre>domain-name example.com</pre>	Set the domain name.
<pre>fixup protocol ftp 21 fixup protocol http 80 fixup protocol smtp 25 fixup protocol h323 1720 fixup protocol rsh 514 fixup protocol sqlnet 1521</pre>	Default fixup protocol values that define port usage.
<pre>names pager lines 24 no logging on</pre>	Default values that let you use names instead of IP addresses, display 24 lines of text before you are prompted to continue, and disable syslog output.
<pre>interface ethernet0 auto interface ethernet1 auto interface ethernet2 auto interface ethernet3 auto</pre>	Default interface definitions indicating that each Ethernet interface has automatic sensing capabilities to determine line speed and duplex.
<pre>mtu outside 1500 mtu inside 1500 mtu dmz 1500 mtu perimeter 1500</pre>	Set the maximum transmission unit values for the Ethernet interfaces.
<pre>ip address outside 209.165.200.229 255.255.255.224 ip address inside 10.0.0.1 255.0.0.0 ip address dmz 192.168.101.1 255.255.255.0 ip address perimeter 192.168.102.1 255.255.255.0</pre>	The IP addresses for each PIX Firewall interface.
<pre>no failover failover ip address outside 0.0.0.0 failover ip address inside 0.0.0.0 failover ip address dmz 0.0.0.0 failover ip address perimeter 0.0.0.0</pre>	Default values to disable failover.
<pre>arp timeout 14400</pre>	Default value specifying that the ARP cache be reinitialized every four hours.
<pre>nat (inside) 0 10.0.0.0 255.0.0.0 0 0</pre>	Disable NAT for the inside interface.
<pre>nat 0 access-list 80 access-list 80 permit ip 10.0.0.0 255.0.0.0 192.168.12.0 255.255.255.0</pre>	<p>The nat 0 access-list command statement lets you exempt traffic that is matched by the access-list command statement from the NAT services. Adaptive Security remains in effect with the nat 0 access-list command.</p> <p>The access-list command statement permits IP traffic on all hosts on the inside network to be accessed by the hosts on PIX Firewall 1.</p>

Table 11-2 PIX Firewall 2 VPN Tunnel Configuration (continued)

Configuration	Description
<pre>no rip outside passive no rip outside default no rip inside passive no rip inside default no rip dmz passive no rip dmz default no rip perimeter passive no rip perimeter default</pre>	Default values to disable RIP listening or broadcasting.
<pre>route outside 0.0.0.0 0.0.0.0 209.165.200.227 1</pre>	Specify the router on the outside interface for default routes.
<pre>timeout xlate 3:00:00 conn 1:00:00 half-closed 0:10:00 udp 0:02:00 timeout rpc 0:10:00 h323 0:05:00 timeout uauth 0:05:00 absolute</pre>	Default timer values.
<pre>aaa-server TACACS+ protocol tacacs+ aaa-server RADIUS protocol radius</pre>	Default values that permit access to the TACACS+ or RADIUS protocols; however, AAA is not used in this configuration.
<pre>no snmp-server location no snmp-server contact snmp-server community public no snmp-server enable traps</pre>	Default values to disable SNMP access.
<pre>crypto ipsec transform-set strong esp-3des esp-sha-hmac crypto map newyork 10 ipsec-isakmp crypto map newyork 10 match address 80 crypto map newyork 10 set peer 209.165.201.8 crypto map newyork 10 set transform-set strong crypto map newyork interface outside</pre>	Define the crypto map transforms, specify ISAKMP access, match the map to the access list (both use ID 80 to be associated), set the tunnel peer to be the outside interface IP address of PIX Firewall 1 (209.165.201.8), and apply the crypto map to the outside interface.
<pre>isakmp enable outside isakmp key cisco1234 address 209.165.201.8 netmask 255.255.255.255 isakmp policy 8 encryption 3des</pre>	Configure the IKE policy.
<pre>ca identity example.com 209.165.202.130:cgi-bin/pkiclient.exe ca configure example.com ca 1 20 crloptional</pre>	Define VeriSign-related enrollment commands.
<pre>sysopt connection permit-ipsec</pre>	Tell the PIX Firewall to implicitly permit IPSec traffic.
<pre>telnet timeout 5 terminal width 80</pre>	Default values for how long a Telnet console session can be idle and that a console session should display up to 80 characters wide on the console computer.

IPSec/VPN Tunnel Using Entrust Digital Certificates

This section provides configuration examples showing how to configure interoperability between two PIX Firewall units (PIX Firewall 1 and 2) for site-to-site VPN using the Entrust CA server for device enrollment and certificate requests, and digital certificates for the IKE authentication.

The two VPN peers in the configuration examples are shown to be configured to enroll with and obtain their CA-signed certificates from the Entrust CA server. PIX Firewall 1 will obtain its certificate from the CA's local IP address of 10.1.0.2. PIX Firewall 2 will obtain its certificate from the CA's global IP address of 209.165.202.131. After each peer obtains its CA-signed certificate, tunnels can be established between the two VPN peers. The peers dynamically authenticate each other using the digital certificates.



Note

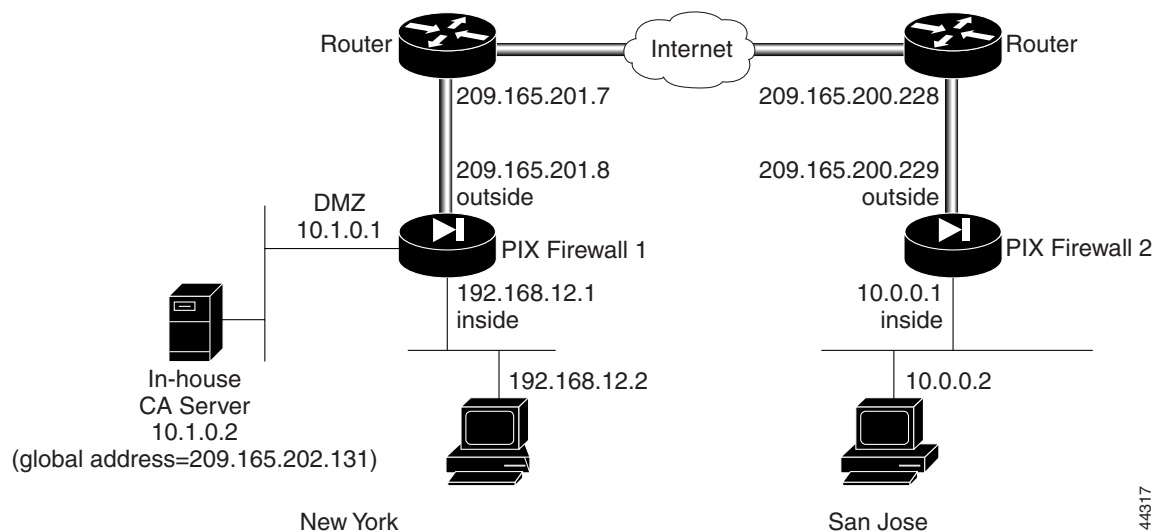
The example CA server address is to be used for example purposes only.

This section includes the following topics:

- Configuring PIX Firewall 1 for an Entrust Certificate
- Configuring PIX Firewall 2 for an Entrust Certificate

This example uses the network diagram shown in Figure 11-2.

Figure 11-2 VPN Tunnel Network



44317

Configuring PIX Firewall 1 for an Entrust Certificate

Follow these steps to configure PIX Firewall 1:

Step 1 Define a host name:

```
hostname NewYork
```

Step 2 Define the domain name:

```
domain-name example.com
```

Step 3 Generate the PIX Firewall RSA key pair:

```
ca generate rsa key 512
```

This command is entered at the command line and does not get stored in the configuration.

Step 4 Define Entrust-related enrollment commands:

```
ca identity abcd 209.165.202.131 209.165.202.131
ca configure abcd ra 1 20 crloptional
```

These commands are stored in the configuration. **1** is the retry period, **20** is the retry count, and the **crloptional** option disables CRL checking.

Step 5 Authenticate the CA by obtaining its public key and its certificate:

```
ca authenticate abcd
```

This command is entered at the command line and does not get stored in the configuration.

Step 6 Request signed certificates from your CA for your PIX Firewall's RSA key pair. Before entering this command, contact your CA administrator because they will have to authenticate your PIX Firewall manually before granting its certificate:

```
ca enroll abcd cisco
```

"cisco" is a challenge password. This can be anything. This command is entered at the command line and does not get stored in the configuration.

Step 7 Verify that the enrollment process was successful using the **show ca certificate** command:

```
show ca certificate
```

Step 8 Save keys and certificates, and the CA commands (except those indicated) in Flash memory:

```
ca save all
write memory
```



Note Use the **ca save all** command any time you add, change, or delete **ca** commands in the configuration. This command is not stored in the configuration.

Step 9 Map a local IP address to a global IP address:

```
static (dmz, outside) 209.165.202.131 10.1.0.2 netmask 255.255.255.255
```

Step 10 Permit the host (PIX Firewall 2) to access the global host via LDAP, port 389:

```
conduit permit tcp host 209.165.202.131 eq 389 209.165.200.229 255.255.255.255
```

Step 11 Permit the host (PIX Firewall 2) to access the global host via HTTP:

```
conduit permit tcp host 209.165.202.131 eq http 209.165.200.229 255.255.255.255
```

Step 12 Configure an IKE policy:

```
isakmp enable outside
isakmp policy 8 auth rsa-sig
isakmp identity hostname
```

- Step 13** Configure a transform set that defines how the traffic will be protected:
- ```
crypto ipsec transform-set strong esp-3des esp-sha-hmac
```
- Step 14** Create a partial access list:
- ```
access-list 90 permit ip 192.168.12.0 255.255.255.0 10.0.0.0 255.0.0.0
```
- Step 15** Define a crypto map:
- ```
crypto map toSanJose 20 ipsec-isakmp
crypto map toSanJose 20 match address 90
crypto map toSanJose 20 set transform-set strong
crypto map toSanJose 20 set peer 209.165.200.229
```
- Step 16** Apply the crypto map to the outside interface:
- ```
crypto map toSanJose interface outside
```
- Step 17** Tell the PIX Firewall to implicitly permit IPSec traffic:
- ```
sysopt connection permit-ipsec
```

Table 11-3 lists the configuration for PIX Firewall 1.

**Table 11-3 PIX Firewall 1 VPN Tunnel Configuration**

| Configuration                                                                                                                                             | Description                                                                                                                                             |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>nameif ethernet0 outside security0 nameif ethernet1 inside security100</pre>                                                                         | PIX Firewall provides <b>nameif</b> command statements for the inside and outside interfaces in the default configuration.                              |
| <pre>enable password 8Ry2YjIyt7RRXU24 encrypted passwd 2KFQnbNIdI.2KYOU encrypted</pre>                                                                   | Default values for the privileged mode password and the Telnet password.                                                                                |
| <pre>hostname NewYork</pre>                                                                                                                               | Define a host name for the PIX Firewall.                                                                                                                |
| <pre>domain-name example.com</pre>                                                                                                                        | Set the domain name.                                                                                                                                    |
| <pre>fixup protocol ftp 21 fixup protocol http 80 fixup protocol smtp 25 fixup protocol h323 1720 fixup protocol rsh 514 fixup protocol sqlnet 1521</pre> | Default <b>fixup protocol</b> values that define port usage.                                                                                            |
| <pre>names pager lines 24 no logging on</pre>                                                                                                             | Default values that let you use names instead of IP addresses, display 24 lines of text before you are prompted to continue, and disable syslog output. |
| <pre>interface ethernet0 auto interface ethernet1 auto</pre>                                                                                              | Default interface definitions indicating that each Ethernet interface has automatic sensing capabilities to determine line speed and duplex.            |
| <pre>mtu outside 1500 mtu inside 1500</pre>                                                                                                               | Set the maximum transmission unit values for the Ethernet interfaces.                                                                                   |
| <pre>ip address outside 209.165.201.8 255.255.255.224 ip address inside 192.168.12.1 255.255.255.0</pre>                                                  | The IP addresses for each PIX Firewall interface.                                                                                                       |
| <pre>no failover failover ip address outside 0.0.0.0 failover ip address inside 0.0.0.0</pre>                                                             | Default values to disable failover.                                                                                                                     |

Table 11-3 PIX Firewall 1 VPN Tunnel Configuration (continued)

| Configuration                                                                                                                                                                                                                                                                                                            | Description                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>arp timeout 14400</code>                                                                                                                                                                                                                                                                                           | Default value specifying that the ARP cache be reinitialized every four hours.                                                                                                                                                                                                                                                                                                                |
| <code>static (dmz, outside) 209.165.202.131 10.1.0.2<br/>netmask 255.255.255.255<br/>conduit permit tcp host 209.165.202.131 eq 389<br/>209.165.200.229 255.255.255.255<br/>conduit permit tcp host 209.165.202.131 eq http<br/>209.165.200.229 255.255.255.255</code>                                                   | Map a local IP address to a global IP address.<br><br>Permit the host (PIX Firewall 2) to access the global host via LDAP, port 389.<br><br>Permit the host (PIX Firewall 2) to access the global host via HTTP.                                                                                                                                                                              |
| <code>nat 0 access-list 90<br/>access-list 90 permit ip 192.168.12.0 255.255.255.0<br/>10.0.0.0 255.0.0.0</code>                                                                                                                                                                                                         | The <b>nat 0 access-list</b> command statement lets you exempt traffic that is matched by the <b>access-list</b> command statement from the NAT services. Adaptive Security remains in effect with the <b>nat 0 access-list</b> command.<br><br>The <b>access-list</b> command statement permits IP traffic on all hosts on the inside network to be accessed by the hosts on PIX Firewall 2. |
| <code>no rip outside passive<br/>no rip outside default<br/>rip inside passive<br/>no rip inside default</code>                                                                                                                                                                                                          | Default values to disable RIP listening or broadcasting. However, the inside interface does listen for RIP broadcasts.                                                                                                                                                                                                                                                                        |
| <code>route outside 10.0.0.0 255.0.0.0 209.165.200.229 1<br/><br/>route outside 0.0.0.0 0.0.0.0 209.165.200.227 1</code>                                                                                                                                                                                                 | Specify a static route to access the inside network of PIX Firewall 2.<br><br>Specify the router on the outside interface for default routes.                                                                                                                                                                                                                                                 |
| <code>timeout xlate 3:00:00 conn 1:00:00 half-closed<br/>0:10:00 udp 0:02:00<br/>timeout rpc 0:10:00 h323 0:05:00<br/>timeout uauth 0:05:00 absolute</code>                                                                                                                                                              | Default timer values.                                                                                                                                                                                                                                                                                                                                                                         |
| <code>aaa-server TACACS+ protocol tacacs+<br/>aaa-server RADIUS protocol radius</code>                                                                                                                                                                                                                                   | Default values that permit access to the TACACS+ or RADIUS protocols; however, AAA is not used in this configuration.                                                                                                                                                                                                                                                                         |
| <code>no snmp-server location<br/>no snmp-server contact<br/>snmp-server community public<br/>no snmp-server enable traps</code>                                                                                                                                                                                         | Default values to disable SNMP access.                                                                                                                                                                                                                                                                                                                                                        |
| <code>crypto ipsec transform-set strong esp-3des<br/>esp-sha-hmac<br/><br/>crypto map toSanJose 20 ipsec-isakmp<br/>crypto map toSanJose 20 match address 90<br/>crypto map toSanJose 20 set peer 209.165.200.229<br/>crypto map toSanJose 20 set transform-set strong<br/>crypto map toSanJose interface outside</code> | Define the crypto map transforms, specify ISAKMP access, match the map to the access list (both use ID 90 to be associated), set the tunnel peer to be the outside interface IP address of PIX Firewall 2 (209.165.200.229), and apply the crypto map to the outside interface.                                                                                                               |
| <code>isakmp enable outside<br/>isakmp policy 9 encryption 3des</code>                                                                                                                                                                                                                                                   | Configure the IKE policy.                                                                                                                                                                                                                                                                                                                                                                     |
| <code>ca identity abcd 209.165.202.131 209.165.202.131<br/>ca configure abcd ra 1 100 crloptional</code>                                                                                                                                                                                                                 | Define Entrust-related enrollment commands.                                                                                                                                                                                                                                                                                                                                                   |

Table 11-3 PIX Firewall 1 VPN Tunnel Configuration (continued)

| Configuration                                                   | Description                                                                                                                                                  |
|-----------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>sysopt connection permit-ipsec</code>                     | Tell the PIX Firewall to implicitly permit IPSec traffic.                                                                                                    |
| <code>telnet timeout 5</code><br><code>terminal width 80</code> | Default values for how long a Telnet console session can be idle and that a console session should display up to 80 characters wide on the console computer. |

## Configuring PIX Firewall 2 for an Entrust Certificate

Follow these steps to configure PIX Firewall 2:

**Step 1** Define a host name:

```
hostname SanJose
```

**Step 2** Define the domain name:

```
domain-name example.com
```

**Step 3** Configure an IKE policy:

```
isakmp enable outside
isakmp policy 8 auth rsa-sig
```

**Step 4** Define Entrust-related enrollment commands:

```
ca identity abcd 209.165.202.131 209.165.202.131
ca configure abcd ra 1 20 crloptional
```

These commands are stored in the configuration. **1** is the retry period, **20** is the retry count, and the **crloptional** option disables CRL checking.

**Step 5** Generate the PIX Firewall RSA key pair:

```
ca generate rsa key 512
```

This command is entered at the command line and does not get stored in the configuration.

**Step 6** Get the public key and the certificate of the CA server:

```
ca authenticate abcd
```

This command is entered at the command line and does not get stored in the configuration.

**Step 7** Contact your CA administrator and send your certificate request:

```
ca enroll abcd cisco
```

“cisco” is a challenge password. This can be anything. This command is entered at the command line and does not get stored in the configuration.

**Step 8** Configure supported IPSec transforms:

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

**Step 9** Save keys and certificates, and the CA commands (except those indicated) in Flash memory:

```
ca save all
write memory
```



**Note** Use the **ca save all** command any time you add, change, or delete **ca** commands in the configuration. This command is not stored in the configuration.

**Step 10** Create a partial access list:

```
access-list 80 permit ip 10.0.0.0 255.0.0.0 192.168.12.0 255.255.255.0
```

**Step 11** Define a crypto map:

```
crypto map newyork 20 ipsec-isakmp
crypto map newyork 20 match address 80
crypto map newyork 20 set transform-set strong
crypto map newyork 20 set peer 209.165.201.8
```

**Step 12** Apply the crypto map to the outside interface:

```
crypto map newyork interface outside
```

**Step 13** Tell the PIX Firewall to implicitly permit IPSec traffic:

```
sysopt connection permit-ipsec
```

Table 11-4 lists the configuration for PIX Firewall 2.

**Table 11-4** PIX Firewall 2 VPN Tunnel Configuration

| Configuration                                                                                                                                             | Description                                                                                                                                                                                                                                                                                                                           |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>nameif ethernet0 outside security0 nameif ethernet1 inside security100 nameif ethernet2 dmz security50 nameif ethernet3 perimeter security40</pre>   | PIX Firewall provides <b>nameif</b> command statements for the inside and outside interfaces in the default configuration. In addition, the default configuration provides default names for the perimeter interfaces, but in this case, the configuration required different names and security levels for the perimeter interfaces. |
| <pre>enable password 8Ry2YjIyt7RRXU24 encrypted passwd 2KFQnbNIdI.2KYOU encrypted</pre>                                                                   | Default values for the privileged mode password and the Telnet password.                                                                                                                                                                                                                                                              |
| <pre>hostname SanJose</pre>                                                                                                                               | Define a host name for the PIX Firewall.                                                                                                                                                                                                                                                                                              |
| <pre>domain-name example.com</pre>                                                                                                                        | Set the domain name.                                                                                                                                                                                                                                                                                                                  |
| <pre>fixup protocol ftp 21 fixup protocol http 80 fixup protocol smtp 25 fixup protocol h323 1720 fixup protocol rsh 514 fixup protocol sqlnet 1521</pre> | Default <b>fixup protocol</b> values that define port usage.                                                                                                                                                                                                                                                                          |
| <pre>names pager lines 24 no logging on</pre>                                                                                                             | Default values that let you use names instead of IP addresses, display 24 lines of text before you are prompted to continue, and disable syslog output.                                                                                                                                                                               |
| <pre>interface ethernet0 auto interface ethernet1 auto interface ethernet2 auto interface ethernet3 auto</pre>                                            | Default interface definitions indicating that each Ethernet interface has automatic sensing capabilities to determine line speed and duplex.                                                                                                                                                                                          |

Table 11-4 PIX Firewall 2 VPN Tunnel Configuration (continued)

| Configuration                                                                                                                                                                                                                                                                  | Description                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>mtu outside 1500 mtu inside 1500 mtu dmz 1500 mtu perimeter 1500</pre>                                                                                                                                                                                                    | Set the maximum transmission unit values for the Ethernet interfaces.                                                                                                                                                                                                                                                                                                                                |
| <pre>ip address outside 209.165.200.229 255.255.255.224 ip address inside 10.0.0.1 255.0.0.0 ip address dmz 192.168.101.1 255.255.255.0 ip address perimeter 192.168.102.1 255.255.255.0</pre>                                                                                 | The IP addresses for each PIX Firewall interface.                                                                                                                                                                                                                                                                                                                                                    |
| <pre>no failover failover ip address outside 0.0.0.0 failover ip address inside 0.0.0.0 failover ip address dmz 0.0.0.0 failover ip address perimeter 0.0.0.0</pre>                                                                                                            | Default values to disable failover.                                                                                                                                                                                                                                                                                                                                                                  |
| <pre>arp timeout 14400</pre>                                                                                                                                                                                                                                                   | Default value specifying that the ARP cache be reinitialized every four hours.                                                                                                                                                                                                                                                                                                                       |
| <pre>nat 0 access-list 80 access-list 80 permit ip 10.0.0.0 255.0.0.0 192.168.12.0 255.255.255.0</pre>                                                                                                                                                                         | <p>The <b>nat 0 access-list</b> command statement lets you exempt traffic that is matched by the <b>access-list</b> command statement from the NAT services. Adaptive Security remains in effect with the <b>nat 0 access-list</b> command.</p> <p>The <b>access-list</b> command statement permits IP traffic on all hosts on the inside network to be accessed by the hosts on PIX Firewall 1.</p> |
| <pre>no rip outside passive no rip outside default no rip inside passive no rip inside default no rip dmz passive no rip dmz default no rip perimeter passive no rip perimeter default</pre>                                                                                   | Default values to disable RIP listening or broadcasting.                                                                                                                                                                                                                                                                                                                                             |
| <pre>route outside 0.0.0.0 0.0.0.0 209.165.200.227 1</pre>                                                                                                                                                                                                                     | Specify the router on the outside interface for default routes.                                                                                                                                                                                                                                                                                                                                      |
| <pre>timeout xlate 3:00:00 conn 1:00:00 half-closed 0:10:00 udp 0:02:00 timeout rpc 0:10:00 h323 0:05:00 timeout uauth 0:05:00 absolute</pre>                                                                                                                                  | Default timer values.                                                                                                                                                                                                                                                                                                                                                                                |
| <pre>aaa-server TACACS+ protocol tacacs+ aaa-server RADIUS protocol radius</pre>                                                                                                                                                                                               | Default values that permit access to the TACACS+ or RADIUS protocols; however, AAA is not used in this configuration.                                                                                                                                                                                                                                                                                |
| <pre>no snmp-server location no snmp-server contact snmp-server community public no snmp-server enable traps</pre>                                                                                                                                                             | Default values to disable SNMP access.                                                                                                                                                                                                                                                                                                                                                               |
| <pre>crypto ipsec transform-set strong esp-3des esp-sha-hmac  crypto map newyork 10 ipsec-isakmp crypto map newyork 10 match address 80 crypto map newyork 10 set peer 209.165.201.8 crypto map newyork 10 set transform-set strong crypto map newyork interface outside</pre> | Define the crypto map transforms, specify ISAKMP access, match the map to the access list (both use ID 80 to be associated), set the tunnel peer to be the outside interface IP address of PIX Firewall 1 (209.165.201.8), and apply the crypto map to the outside interface.                                                                                                                        |

Table 11-4 PIX Firewall 2 VPN Tunnel Configuration (continued)

| Configuration                                                                                             | Description                                                                                                                                                  |
|-----------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>isakmp enable outside isakmp policy 8 authentication pre-share isakmp policy 8 encryption 3des</pre> | Configure the IKE policy.                                                                                                                                    |
| <pre>ca identity abcd 209.165.202.131 209.165.202.131 ca configure abcd ra 1 100 crloptional</pre>        | Define Entrust-related enrollment commands.                                                                                                                  |
| <pre>sysopt connection permit-ipsec</pre>                                                                 | Tell the PIX Firewall to implicitly permit IPSec traffic.                                                                                                    |
| <pre>telnet timeout 5 terminal width 80</pre>                                                             | Default values for how long a Telnet console session can be idle and that a console session should display up to 80 characters wide on the console computer. |

## IPSec/VPN Tunnel Using Baltimore Digital Certificates

This section provides configuration examples showing how to configure interoperability between two PIX Firewall units (PIX Firewall 1 and 2) for site-to-site VPN using the Baltimore CA server for device enrollment and certificate requests, and digital certificates for the IKE authentication.

The two VPN peers in the configuration examples are shown to be configured to enroll with and obtain their CA-signed certificates from the Baltimore CA server. PIX Firewall 1 will obtain its certificate from the CA's local IP address of 10.1.0.2. PIX Firewall 2 will obtain its certificate from the CA's global IP address of 209.165.202.131. After each peer obtains its CA-signed certificate, tunnels can be established between the two VPN peers. The peers dynamically authenticate each other using the digital certificates.



### Note

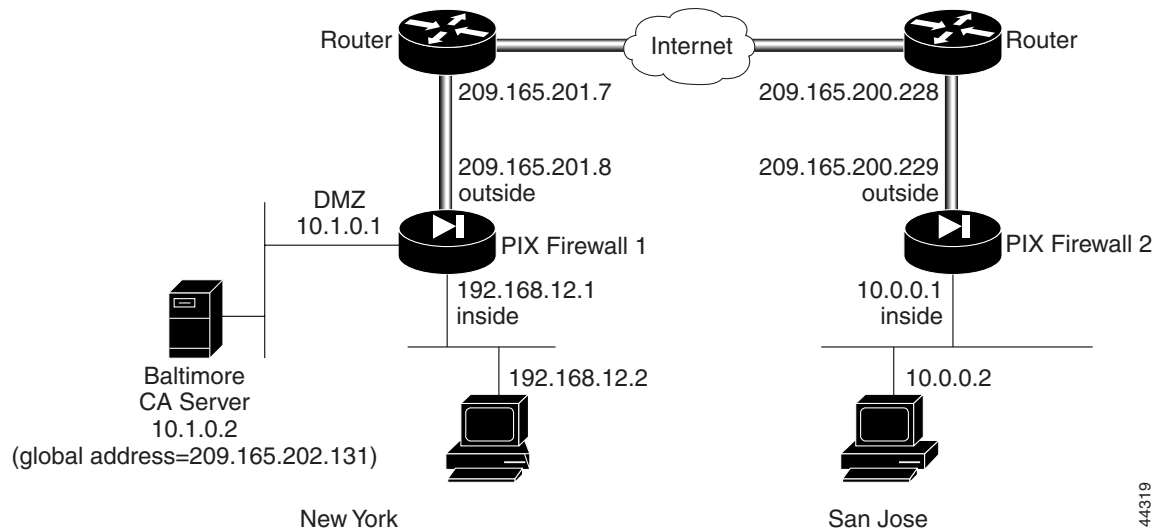
The example CA server address is to be used for example purposes only.

This section includes the following topics:

- Configuring PIX Firewall 1 for a Baltimore Certificate
- Configuring PIX Firewall 2 for a Baltimore Certificate

This example uses the network diagram shown in Figure 11-3.

**Figure 11-3 VPN Tunnel Network**



44819

## Configuring PIX Firewall 1 for a Baltimore Certificate

Follow these steps to configure PIX Firewall 1:

**Step 1** Define a host name:

```
hostname NewYork
```

**Step 2** Define the domain name:

```
domain-name example.com
```

**Step 3** Generate the PIX Firewall RSA key pair:

```
ca generate rsa key 512
```

This command is entered at the command line and does not get stored in the configuration.

**Step 4** Define Baltimore-related enrollment commands:

```
ca identity abcd 209.165.202.131 209.165.202.131
ca configure abcd ra 1 20 crloptional
```

These commands are stored in the configuration. **1** is the retry period, **20** is the retry count, and the **crloptional** option disables CRL checking.

**Step 5** Authenticate the CA by obtaining its public key and its certificate:

```
ca authenticate abcd
```

This command is entered at the command line and does not get stored in the configuration.

- Step 6** Request signed certificates from your CA for your PIX Firewall's RSA key pair. Before entering this command, contact your CA administrator because they will have to authenticate your PIX Firewall manually before granting its certificate:

```
ca enroll abcd cisco
```

"cisco" is a challenge password. This can be anything. This command is entered at the command line and does not get stored in the configuration.

- Step 7** Save keys and certificates, and the CA commands (except those indicated) in Flash memory:

```
ca save all
write memory
```



**Note** Use the **ca save all** command any time you add, change, or delete **ca** commands in the configuration. This command is not stored in the configuration.

- Step 8** Map a local IP address to a global IP address:

```
static (dmz, outside) 209.165.202.131 10.1.0.2 netmask 255.255.255.255
```

- Step 9** Permit the host (PIX Firewall 2) to access the global host via LDAP, port 389:

```
conduit permit tcp host 209.165.202.131 eq 389 209.165.200.229 255.255.255.255
```

- Step 10** Permit the host (PIX Firewall 2) to access the global host via HTTP:

```
conduit permit tcp host 209.165.202.131 eq http 209.165.200.229 255.255.255.255
```

- Step 11** Configure an IKE policy:

```
isakmp enable outside
isakmp policy 8 auth rsa-sig
```

- Step 12** Create a partial access list:

```
access-list 90 permit ip 192.168.12.0 255.255.255.0 10.0.0.0 255.0.0.0
```

- Step 13** Configure a transform set that defines how the traffic will be protected:

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

- Step 14** Define a crypto map:

```
crypto map toSanJose 20 ipsec-isakmp
crypto map toSanJose 20 match address 90
crypto map toSanJose 20 set transform-set strong
crypto map toSanJose 20 set peer 209.165.200.229
```

- Step 15** Apply the crypto map to the outside interface:

```
crypto map toSanJose interface outside
```

- Step 16** Tell the PIX Firewall to implicitly permit IPSec traffic:

```
sysopt connection permit-ipsec
```

---

For a complete configuration example of PIX Firewall 1, see Table 11-3.

## Configuring PIX Firewall 2 for a Baltimore Certificate

Follow these steps to configure PIX Firewall 2:

**Step 1** Define a host name:

```
hostname SanJose
```

**Step 2** Define the domain name:

```
domain-name example.com
```

**Step 3** Generate the PIX Firewall RSA key pair:

```
ca generate rsa key 512
```

This command is entered at the command line and does not get stored in the configuration.

**Step 4** Define Baltimore-related enrollment commands:

```
ca identity abcd 209.165.202.131 209.165.202.131
ca configure abcd ra 1 20 crloptional
```

These commands are stored in the configuration. **1** is the retry period, **20** is the retry count, and the **crloptional** option disables CRL checking.

**Step 5** Authenticate the CA by obtaining its public key and its certificate:

```
ca authenticate abcd
```

This command is entered at the command line and does not get stored in the configuration.

**Step 6** Request signed certificates from your CA for your PIX Firewall's RSA key pair. Before entering this command, contact your CA administrator because they will have to authenticate your PIX Firewall manually before granting its certificate:

```
ca enroll abcd cisco
```

“cisco” is a challenge password. This can be anything. This command is entered at the command line and does not get stored in the configuration.

**Step 7** Save keys and certificates, and the CA commands (except those indicated) in Flash memory:

```
ca save all
write memory
```



**Note** Use the **ca save all** command any time you add, change, or delete **ca** commands in the configuration. This command is not stored in the configuration.

**Step 8** Configure an IKE policy:

```
isakmp enable outside
isakmp policy 8 auth rsa-sig
```

**Step 9** Create a partial access list:

```
access-list 80 permit ip 10.0.0.0 255.0.0.0 192.168.12.0 255.255.255.0
```

**Step 10** Configure a transform set that defines how the traffic will be protected:

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

**Step 11** Define a crypto map:

```
crypto map newyork 20 ipsec-isakmp
crypto map newyork 20 match address 80
crypto map newyork 20 set transform-set strong
crypto map newyork 20 set peer 209.165.201.8
```

**Step 12** Apply the crypto map to the outside interface:

```
crypto map newyork interface outside
```

**Step 13** Tell the PIX Firewall to implicitly permit IPSec traffic:

```
sysopt connection permit-ipsec
```

---

For a complete configuration example of PIX Firewall 2, see Table 11-4.

## IPSec/VPN Tunnel Using Microsoft Digital Certificates

This section provides configuration examples showing how to configure interoperability between two PIX Firewall units (PIX Firewall 1 and 2) for site-to-site VPN using the Microsoft CA server for device enrollment and certificate requests, and digital certificates for the IKE authentication.

The two VPN peers in the configuration examples are shown to be configured to enroll with and obtain their CA-signed certificates from the Microsoft CA server. PIX Firewall 1 will obtain its certificate from the CA's local IP address of 10.1.0.2. PIX Firewall 2 will obtain its certificate from the CA's global IP address of 209.165.202.131. After each peer obtains its CA-signed certificate, tunnels can be established between the two VPN peers. The peers dynamically authenticate each other using the digital certificates.



---

**Note** The example CA server address is to be used for example purposes only.

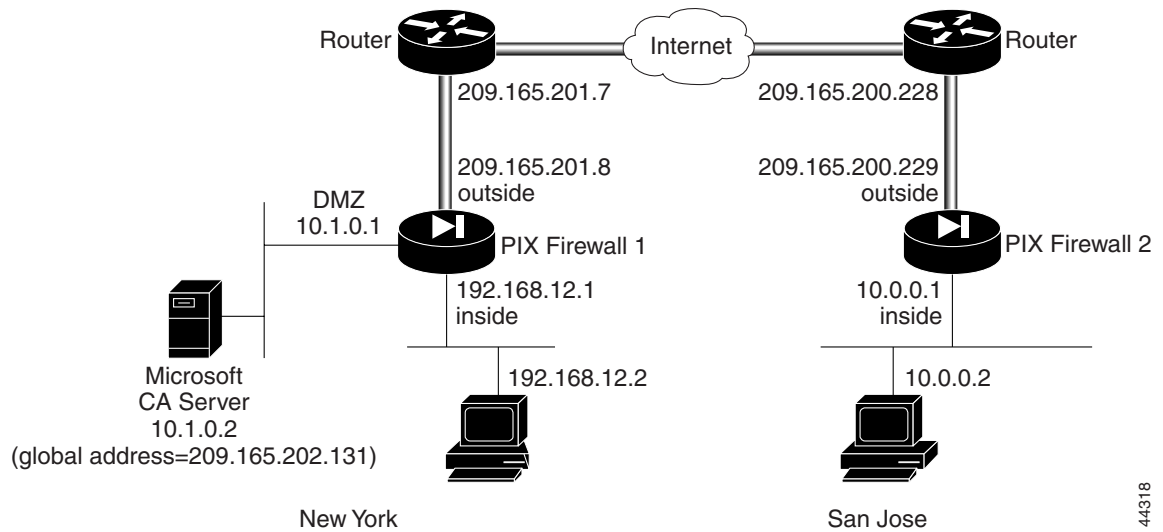
---

This section includes the following topics:

- Configuring PIX Firewall 1 for a Microsoft Certificate
- Configuring PIX Firewall 2 for a Microsoft Certificate

This example uses the network diagram shown in Figure 11-4.

**Figure 11-4 VPN Tunnel Network**



44318

## Configuring PIX Firewall 1 for a Microsoft Certificate

Follow these steps to configure PIX Firewall 1:

**Step 1** Define a host name:

```
hostname NewYork
```

**Step 2** Define the domain name:

```
domain-name example.com
```

**Step 3** Generate the PIX Firewall RSA key pair:

```
ca generate rsa key 512
```

This command is entered at the command line and does not get stored in the configuration.

**Step 4** Define Microsoft-related enrollment commands:

```
ca identity abcd 10.1.0.2:/certsrv/mscep/mscep.dll
ca configure abcd ra 1 20 crloptional
```

These commands are stored in the configuration. **1** is the retry period, **20** is the retry count, and the **crloptional** option disables CRL checking.

**Step 5** Authenticate the CA by obtaining its public key and its certificate:

```
ca authenticate abcd
```

This command is entered at the command line and does not get stored in the configuration.

- Step 6** Request signed certificates from your CA for your PIX Firewall's RSA key pair. If you are set up with the Microsoft CA server be granted the PIX Firewall unit's certificate manually, contact your CA administrator before entering this command.

```
ca enroll abcd cisco
```

"cisco" is a challenge password. This can be anything. This command is entered at the command line and does not get stored in the configuration.

- Step 7** Save keys and certificates, and the CA commands (except those indicated) in Flash memory:

```
ca save all
write memory
```



---

**Note** Use the **ca save all** command any time you add, change, or delete **ca** commands in the configuration. This command is not stored in the configuration.

---

- Step 8** Map a local IP address to a global IP address:

```
static (dmz, outside) 209.165.202.131 10.1.0.2 netmask 255.255.255.255
```

- Step 9** Permit the host (PIX Firewall 2) to access the global host via HTTP:

```
conduit permit tcp host 209.165.202.131 eq http 209.165.200.229 255.255.255.255
```

- Step 10** Configure an IKE policy:

```
isakmp enable outside
isakmp policy 8 auth rsa-sig
```

- Step 11** Create a partial access list:

```
access-list 90 permit ip 192.168.12.0 255.255.255.0 10.0.0.0 255.0.0.0
```

- Step 12** Configure a transform set that defines how the traffic will be protected:

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

- Step 13** Define a crypto map:

```
crypto map toSanJose 20 ipsec-isakmp
crypto map toSanJose 20 match address 90
crypto map toSanJose 20 set transform-set strong
crypto map toSanJose 20 set peer 209.165.200.229
```

- Step 14** Apply the crypto map to the outside interface:

```
crypto map toSanJose interface outside
```

- Step 15** Tell the PIX Firewall to implicitly permit IPSec traffic:

```
sysopt connection permit-ipsec
```

---

For a complete configuration example of PIX Firewall 1, see Table 11-3. Table 11-3 does not reflect the Microsoft-related commands. To reflect the Microsoft-related commands, enter the Microsoft-related commands in place of the CA-related commands in the Table 11-3.

## Configuring PIX Firewall 2 for a Microsoft Certificate

Follow these steps to configure PIX Firewall 2:

**Step 1** Define a host name:

```
hostname SanJose
```

**Step 2** Define the domain name:

```
domain-name example.com
```

**Step 3** Generate the PIX Firewall RSA key pair:

```
ca generate rsa key 512
```

This command is entered at the command line and does not get stored in the configuration.

**Step 4** Define Microsoft-related enrollment commands:

```
ca identity my_nickname 209.165.202.131:/certsrv/mscep/mscep.dll
ca configure my_nickname ra 1 20 crloptional
```

These commands are stored in the configuration. **1** is the retry period, **20** is the retry count, and the **crloptional** option disables CRL checking.

**Step 5** Authenticate the CA by obtaining its public key and its certificate:

```
ca authenticate abcd
```

This command is entered at the command line and does not get stored in the configuration.

**Step 6** Request signed certificates from your CA for your PIX Firewall's RSA key pair. If you are set up with the Microsoft CA server be granted the PIX Firewall unit's certificate manually, contact your CA administrator before entering this command.

```
ca enroll abcd cisco
```

“cisco” is a challenge password. This can be anything. This command is entered at the command line and does not get stored in the configuration.

**Step 7** Save keys and certificates, and the CA commands (except those indicated) in Flash memory:

```
ca save all
write memory
```



**Note** Use the **ca save all** command any time you add, change, or delete **ca** commands in the configuration. This command is not stored in the configuration.

**Step 8** Configure an IKE policy:

```
isakmp enable outside
isakmp policy 8 auth rsa-sig
```

**Step 9** Create a partial access list:

```
access-list 80 permit ip 10.0.0.0 255.0.0.0 192.168.12.0 255.255.255.0
```

**Step 10** Configure a transform set that defines how the traffic will be protected:

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

**Step 11** Define a crypto map:

```
crypto map newyork 20 ipsec-isakmp
crypto map newyork 20 match address 80
crypto map newyork 20 set transform-set strong
crypto map newyork 20 set peer 209.165.201.8
```

**Step 12** Apply the crypto map to the outside interface:

```
crypto map newyork interface outside
```

**Step 13** Tell the PIX Firewall to implicitly permit IPSec traffic:

```
sysopt connection permit-ipsec
```

---

For a complete configuration example of PIX Firewall 2, see Table 11-4. Table 11-4 does not reflect the Microsoft-related commands. To reflect the Microsoft-related commands, enter the Microsoft-related commands in place of the CA-related commands in the Table 11-4.

## Digital Certificate Issued via an Encrypted Tunnel

This section shows an example of how to perform CA enrollment and certificate requests via a site-to-site VPN tunnel between two PIX Firewall units (PIX Firewall 1 and 2). In the illustrated example, the CA server with which both PIX Firewall units will enroll and from which both units request their certificates reside within the DMZ network of one PIX Firewall (PIX Firewall 1). PIX Firewall 2 is shown to perform its CA enrollment and certificate request via an encrypted tunnel. To accomplish this, a tunnel between the two VPN peers must first be established using a pre-shared key as the device authentication method. Once a tunnel is established, PIX Firewall 2 can perform its CA enrollment and certificate request via the tunnel.

The example configuration steps are shown to be performed on PIX Firewall 1 and 2 in two phases—Phase 1 and Phase 2. Phase 1 involves the following:

- configuring the PIX Firewall units to establish a tunnel using a pre-shared key
- enrolling and requesting the CA-signed certificates

The goal of the Phase 1 configurations is to successfully enroll the PIX Firewall with the CA server and obtain the CA-signed certificate. The order of your configurations for Phase 1 is important. Configure PIX Firewall 1 before PIX Firewall 2. After Phase 1 is completed, proceed to Phase 2 configurations, which involves the following:

- clearing the IKE and IPsec SAs on both units
- configuring the PIX Firewall units to establish a tunnel using digital certificates

The order of configurations during Phase 2 is not important. You can perform Phase 2 configurations on PIX Firewall 2 before performing the Phase 2 configurations on PIX Firewall 1.

**Note**

---

The example CA server address is to be used for example purposes only.

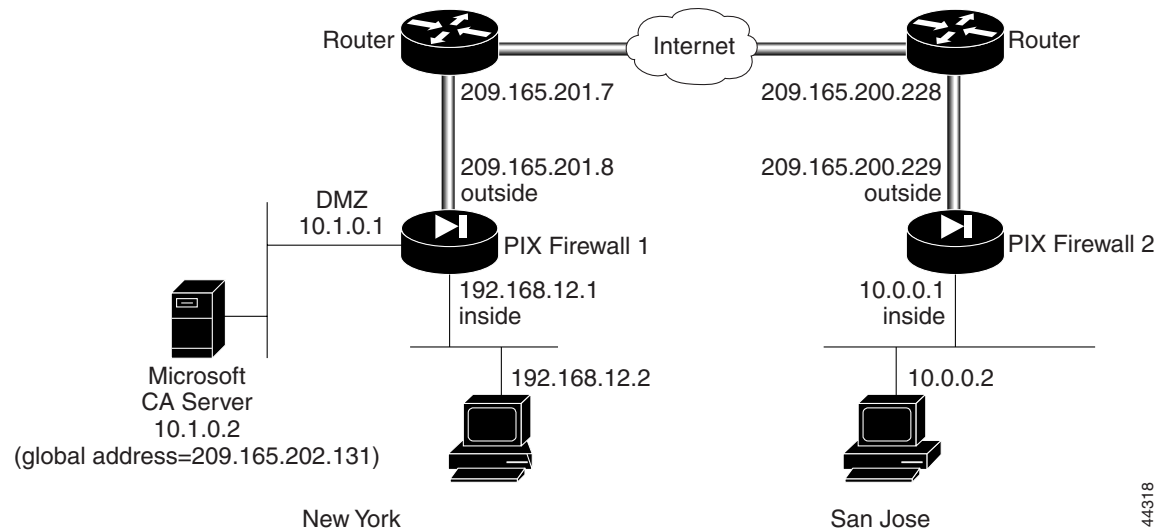
---

This section includes the following topics:

- Configuring PIX Firewall 1 to Obtain Certificate via Encrypted Tunnel
- Configuring PIX Firewall 2 to Obtain Certificate via Encrypted Tunnel

This example uses the network diagram shown in Figure 11-5.

**Figure 11-5 VPN Tunnel Network**



44318

## Configuring PIX Firewall 1 to Obtain Certificate via Encrypted Tunnel

### Phase 1



**Note** The order of your configurations for Phase 1 is important. Configure PIX Firewall1 before PIX Firewall 2.

Follow these steps to configure PIX Firewall 1:

- 
- Step 1** Define a host name:
- ```
hostname NewYork
```
- Step 2** Define the domain name:
- ```
domain-name example.com
```
- Step 3** Configure an IKE policy:
- ```
isakmp enable outside
isakmp policy 8 auth pre-share
isakmp key cisco address 209.165.200.229 netmask 255.255.255.255
```
- Step 4** Create a partial access list:
- ```
access-list 90 permit ip host 10.1.0.2 host 209.165.200.229
```

**Step 5** Configure NAT 0:

```
nat (dmz) 0 access-list 90
```

**Step 6** Configure a transform set that defines how the traffic will be protected:

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

**Step 7** Define a crypto map:

```
crypto map toSanJose 20 ipsec-isakmp
crypto map toSanJose 20 match address 90
crypto map toSanJose 20 set transform-set strong
crypto map toSanJose 20 set peer 209.165.200.229
```

**Step 8** Apply the crypto map to the outside interface:

```
crypto map toSanJose interface outside
```

**Step 9** Tell the PIX Firewall to implicitly permit IPsec traffic:

```
sysopt connection permit-ipsec
```

**Step 10** Generate the PIX Firewall RSA key pair:

```
ca generate rsa key 512
```

This command is entered at the command line and does not get stored in the configuration.

**Step 11** Define CA-related enrollment commands:

```
ca identity abcd 10.1.0.2:/certsrv/mscep/mscep.dll
ca configure abcd ra 1 20 crloptional
```

These commands are stored in the configuration. The CA-related commands shown are specific to the Microsoft CA. The actual CA-related commands you configure depend on the CA you are using.

**Step 12** Get the public key and the certificate of the CA server:

```
ca authenticate abcd
```

This command is entered at the command line and does not get stored in the configuration.

**Step 13** Contact your CA administrator and send your certificate request:

```
ca enroll abcd cisco
```

“cisco” is a challenge password. This can be anything. This command is entered at the command line and does not get stored in the configuration.

**Step 14** Save keys and certificates, and the CA commands (except those indicated) in Flash memory:

```
ca save all
write memory
```



**Note** Use the **ca save all** command any time you add, change, or delete **ca** commands in the configuration. This command is not stored in the configuration.

## Phase 2

Follow these steps to configure PIX Firewall 1:

- 
- Step 1** Clear the IPsec SAs:  
`clear ipsec sa`
- Step 2** Clear the ISAKMP SAs:  
`clear isakmp sa`
- Step 3** Create a partial access list:  
`access-list 90 permit ip 192.168.12.0 255.255.255.0 10.0.0.0 255.0.0.0`
- Step 4** Configure NAT 0:  
`nat (inside) 0 access-list 90`
- Step 5** Specify the authentication method of rsa-signatures for the IKE policy:  
`isakmp policy 8 auth rsa-sig`
- 

## Configuring PIX Firewall 2 to Obtain Certificate via Encrypted Tunnel

### Phase 1

**Note**

---

The order of your configurations for Phase 1 is important. Before configuring PIX Firewall 2 for Phase 1, configure PIX Firewall1 for Phase 1.

---

Follow these steps to configure PIX Firewall 2:

- 
- Step 1** Define a host name:  
`hostname SanJose`
- Step 2** Define the domain name:  
`domain-name example.com`
- Step 3** Configure an IKE policy:  
`isakmp enable outside`  
`isakmp policy 8 auth pre-share`  
`isakmp key cisco address 209.165.201.8 netmask 255.255.255.255`
- Step 4** Create a partial access list:  
`access-list 80 permit ip host 209.165.200.229 host 10.1.0.2`
- Step 5** Configure NAT 0:  
`nat (inside) 0 access-list 80`

**Step 6** Configure a transform set that defines how the traffic will be protected:

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

**Step 7** Define a crypto map:

```
crypto map newyork 20 ipsec-isakmp
crypto map newyork 20 match address 80
crypto map newyork 20 set transform-set strong
crypto map newyork 20 set peer 209.165.201.8
```

**Step 8** Apply the crypto map to the outside interface:

```
crypto map newyork interface outside
```

**Step 9** Tell the PIX Firewall to implicitly permit IPSec traffic:

```
sysopt connection permit-ipsec
```

**Step 10** Generate the PIX Firewall RSA key pair:

```
ca generate rsa key 512
```

This command is entered at the command line and does not get stored in the configuration.

**Step 11** Define CA-related enrollment commands:

```
ca identity abcd 10.1.0.2:/certsrv/mscep/mscep.dll
ca configure abcd ra 1 20 crloptional
```

These commands are stored in the configuration. The CA-related commands shown are specific to the Microsoft CA. The actual CA-related commands you configure depend on the CA you are using.

**Step 12** Authenticate the CA by obtaining its public key and its certificate:

```
ca authenticate abcd
```

This command is entered at the command line and does not get stored in the configuration.

**Step 13** Request signed certificates from your CA for your PIX Firewall's RSA key pair. Before entering this command, contact your CA administrator because they will have to authenticate your PIX Firewall manually before granting its certificate:

```
ca enroll abcd cisco
```

“cisco” is a challenge password. This can be anything. This command is entered at the command line and does not get stored in the configuration.

**Step 14** Save keys and certificates, and the CA commands (except those indicated) in Flash memory:

```
ca save all
write memory
```



**Note** Use the **ca save all** command any time you add, change, or delete **ca** commands in the configuration. This command is not stored in the configuration.

## Phase 2

Follow these steps to configure PIX Firewall 2:

---

**Step 1** Clear the IPsec SAs:

```
clear ipsec sa
```

**Step 2** Clear the ISAKMP SAs:

```
clear isakmp sa
```

**Step 3** Create a partial access list:

```
access-list 80 permit ip 10.0.0.0 255.0.0.0 192.168.12.0 255.255.255.0
```

**Step 4** Specify the authentication method of rsa-signatures for the IKE policy:

```
isakmp policy 8 auth rsa-sig
```

---

