



Site-to-Site VPN Configuration Examples

A site-to-site VPN protects the network resources on your protected networks from unauthorized use by users on an unprotected network, such as the public Internet. The basic configuration for this type of implementation has been covered in [Chapter 6, “Configuring IPSec and Certification Authorities.”](#) This chapter provides examples of the following site-to-site VPN configurations:

- [Using Pre-Shared Keys](#)
- [Using PIX Firewall with a VeriSign CA](#)
- [Using PIX Firewall with an In-House CA](#)
- [Using an Encrypted Tunnel to Obtain Certificates](#)
- [Manual Configuration with NAT](#)



Note

Throughout the examples in this chapter, the local PIX Firewall unit is identified as PIX Firewall 1 while the remote unit is identified as PIX Firewall 2. This designation makes it easier to clarify the configuration required for each.

Using Pre-Shared Keys

This section describes an example configuration for using pre-shared keys. It contains the following topics:

- [Scenario Description](#)
- [Configuring PIX Firewall 1 with VPN Tunneling](#)
- [Configuring PIX Firewall 2 for VPN Tunneling](#)

Scenario Description

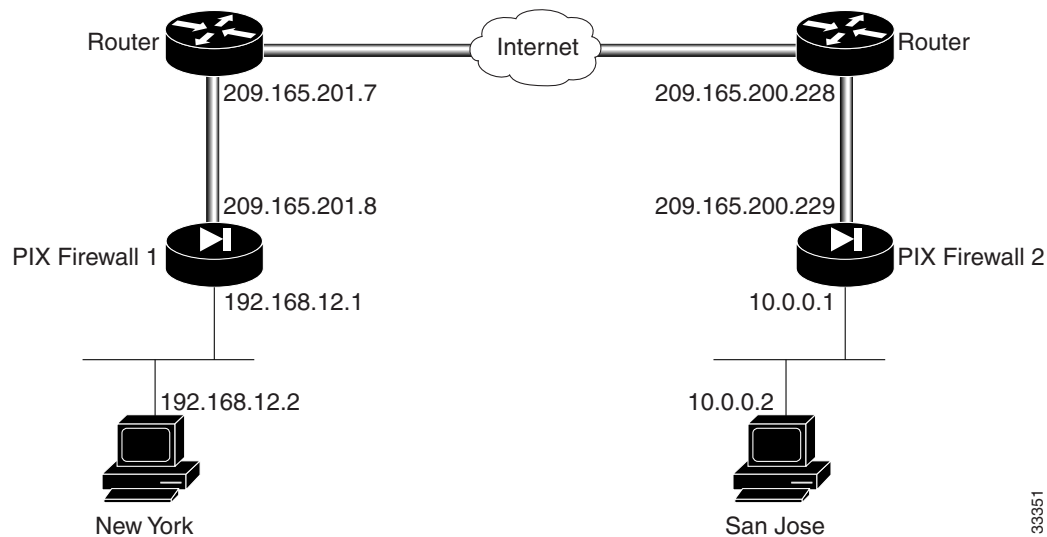
In the example illustrated in [Figure 7-1](#), the intranets use unregistered addresses and are connected over the public Internet by a site-to-site VPN. In this scenario, NAT is required for connections to the public Internet. However, NAT is not required for traffic between the two intranets, which can be transmitted using a VPN tunnel over the public Internet.

**Note**

If you do not need to do VPN tunneling for intranet traffic, you can use this example without the **access-list** or the **nat 0 access-list** commands. These commands disable NAT for traffic that matches the access list criteria.

If you have a limited number of registered IP addresses and you cannot use PAT, you can configure PIX Firewall to use NAT for connections to the public Internet, but avoid NAT for traffic between the two intranets. This configuration might also be useful if you were replacing a direct, leased-line connection between two intranets.

Figure 7-1 VPN Tunnel Network



The configuration shown for this example uses an access list to exclude traffic between the two intranets from NAT. The configuration assigns a global pool of registered IP addresses for use by NAT for all other traffic. By excluding intranet traffic from NAT, you need fewer registered IP addresses.

Configuring PIX Firewall 1 with VPN Tunneling

Follow these steps to configure PIX Firewall 1:

-
- Step 1** Define a host name:
- ```
hostname NewYork
```
- Step 2** Configure an ISAKMP policy:
- ```
isakmp enable outside
isakmp policy 9 authentication pre-share
isakmp policy 9 encrypt des
```
- Step 3** Configure a pre-shared key and associate with the peer:
- ```
crypto isakmp key cisco1234 address 209.165.200.229
```

**Step 4** Configure the supported IPsec transforms:

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

**Step 5** Create an access list:

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

This access list defines traffic from network 192.168.12.0 to 10.0.0.0. Both of these networks use unregistered addresses.




---

**Note** Steps 5 and 6 are not required if you want to enable NAT for all traffic.

---

**Step 6** Exclude traffic between the intranets from NAT:

```
nat 0 access-list 90
```

This excludes traffic matching access list 90 from NAT. The **nat 0** command is always processed before any other **nat** commands.

**Step 7** Enable NAT for all other traffic:

```
nat (inside) 1 0 0
```

**Step 8** Assign a pool of global addresses for NAT and PAT:

```
global (outside) 1 209.165.202.129-209.165.202.159
global (outside) 1 209.165.202.160
```

The pool of registered addresses are only used for connections to the public Internet.

**Step 9** 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 10** Apply the crypto map to the outside interface:

```
crypto map toSanJose interface outside
```

**Step 11** Specify that IPsec traffic be implicitly trusted (permitted):

```
sysopt connection permit-ipsec
```

---

[Example 7-1](#) lists the configuration for PIX Firewall 1.

### **Example 7-1 PIX Firewall 1 VPN Tunnel Configuration**

```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
interface ethernet0 auto
interface ethernet1 auto
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname NewYork
domain-name example.com
fixup protocol ftp 21
fixup protocol http 80
fixup protocol smtp 25
```

```

fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol sqlnet 1521
names
pager lines 24
no logging on
mtu outside 1500
mtu inside 1500
ip address outside 209.165.201.8 255.255.255.224
ip address inside 192.168.12.1 255.255.255.0
no failover
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
arp timeout 14400
nat 0 access-list 90
access-list 90 permit ip 192.168.12.0 255.255.255.0 10.0.0.0 255.0.0.0
nat (inside) 1 0 0
global (outside) 1 209.165.202.129-209.165.202.159
global (outside) 1 209.165.202.160
no rip outside passive
no rip outside default
rip inside passive
no rip inside default
route outside 0.0.0.0 0.0.0.0 209.165.201.7 1
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
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
sysopt connection permit-ipsec
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
isakmp enable outside
isakmp key cisco1234 address 209.165.200.229 netmask 255.255.255.255
isakmp policy 9 authentication pre-share
isakmp policy 9 encryption 3des
telnet timeout 5
terminal width 80

```

**Note**

In this example, the following statements are not used when enabling NAT for all traffic:

```

nat 0 access-list 90
access-list 90 permit ip 192.168.12.0 255.255.255.0 10.0.0.0 255.0.0.0

```

## Configuring PIX Firewall 2 for VPN Tunneling

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** Create a net static:

```
static (inside,outside) 10.0.0.0 10.0.0.0 netmask 255.0.0.0
```

**Step 4** Configure the ISAKMP policy:

```
isakmp enable outside
isakmp policy 8 authentication pre-share
isakmp policy 8 encryption 3des
```

**Step 5** Configure a pre-shared key and associate it with the peer:

```
crypto isakmp key cisco1234 address 209.165.201.8
```

**Step 6** Configure IPsec supported transforms:

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

**Step 7** Create an access list:

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

This access list defines traffic from network 10.0.0.0 to 192.168.12.0. Both of these networks use unregistered addresses.



**Note** Step 7 and Step 8 are not required if you want to enable NAT for all traffic.

**Step 8** Exclude traffic between the intranets from NAT:

```
nat 0 access-list 80
```

This excludes traffic matching access list 80 from NAT. The **nat 0** command is always processed before any other **nat** commands.

**Step 9** Enable NAT for all other traffic:

```
nat (inside) 1 0 0
```

**Step 10** Assign a pool of global addresses for NAT and PAT:

```
global (outside) 1 209.165.202.160-209.165.202.89
global (outside) 1 209.165.202.190
```

The pool of registered addresses are only used for connections to the public Internet.

**Step 11** 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 12** Apply the crypto map to an interface:

```
crypto map newyork interface outside
```

**Step 13** Specify that IPSec traffic be implicitly trusted (permitted):

```
sysopt connection permit-ipsec
```

---

[Example 7-2](#) lists the configuration for PIX Firewall 2.

### **Example 7-2 PIX Firewall 2 VPN Tunnel Configuration**

```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 dmz security50
nameif ethernet3 perimeter security40
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname SanJose
domain-name example.com
fixup protocol ftp 21
fixup protocol http 80
fixup protocol smtp 25
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol sqlnet 1521
names
pager lines 24
no logging on
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto
interface ethernet3 auto
mtu outside 1500
mtu inside 1500
mtu dmz 1500
mtu perimeter 1500
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
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
arp timeout 14400
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
nat (inside) 1 0 0
global (outside) 1 209.165.202.160-209.165.202.89
global (outside) 1 209.165.202.190
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
route outside 0.0.0.0 0.0.0.0 209.165.200.228 1
```

```

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
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
sysopt connection permit-ipsec
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
isakmp enable outside
isakmp key cisco1234 address 209.165.201.8 netmask 255.255.255.255
isakmp policy 8 authentication pre-share
isakmp policy 8 encryption 3des
telnet timeout 5
terminal width 80

```

**Note**

In [Example 7-2](#), the following statements are not used when enabling NAT for all traffic:

```

nat 0 access-list 80
access-list 80 permit ip 10.0.0.0 255.0.0.0 192.168.12.0 255.255.255.00

```

## Using PIX Firewall with a VeriSign CA

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. This section includes the following topics:

- [Scenario Description](#)
- [Configuring PIX Firewall 1 with a VeriSign CA](#)
- [Configuring PIX Firewall 2 with a VeriSign CA](#)

### Scenario Description

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. VeriSign is a public CA that issues its CA-signed certificates over the Internet. 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.

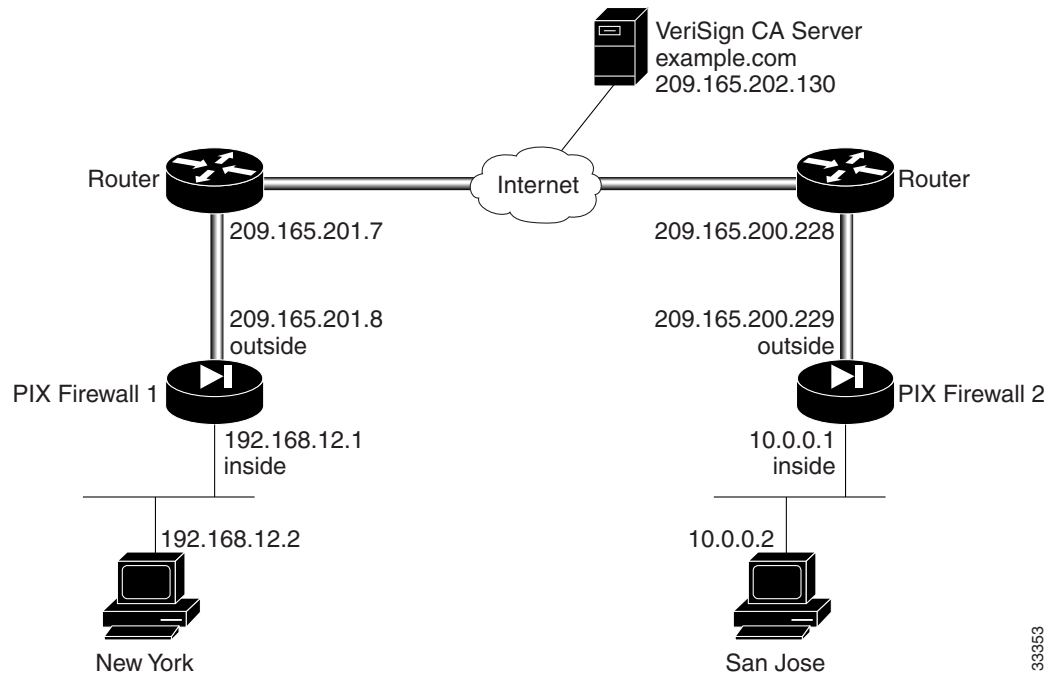
**Note**

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

For the general procedures to configure the PIX Firewall for a CA, see “Using Certification Authorities” in Chapter 6, “Configuring IPSec and Certification Authorities.”

This section provides an example configuration for the specific network illustrated in Figure 7-2.

Figure 7-2 VPN Tunnel Network



33353

## Configuring PIX Firewall 1 with a VeriSign CA

Perform the following steps to configure PIX Firewall 1 to use a public CA:

**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 20 crloptional
```

These commands are stored in the configuration. “2” 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 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
```

---

[Example 7-3](#) lists the configuration for PIX Firewall 1. PIX Firewall default configuration values and certain CA commands are not displayed in configuration listings.

**Example 7-3 PIX Firewall 1 with Public CA**

```

nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname NewYork
domain-name example.com
fixup protocol ftp 21
fixup protocol http 80
fixup protocol smtp 25
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol sqlnet 1521
names
pager lines 24
no logging on
interface ethernet0 auto
interface ethernet1 auto
mtu outside 1500
mtu inside 1500
ip address outside 209.165.201.8 255.255.255.224
ip address inside 192.168.12.1 255.255.255.0
no failover
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
arp timeout 14400
nat (inside) 0 0.0.0.0 0.0.0.0 0 0
nat 0 access-list 90
access-list 90 permit ip 192.168.12.0 255.255.255.0 10.0.0.0 255.0.0.0
no rip outside passive
no rip outside default
rip inside passive
no rip inside default
route outside 0.0.0.0 0.0.0.0 209.165.200.227 1
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
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
sysopt connection permit-ipsec
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
isakmp policy 8 authentication rsa-sig
isakmp policy 8 encryption des
isakmp policy 8 hash sha
isakmp policy 8 group 1
isakmp policy 8 lifetime 86400
ca identity example.com 209.165.202.130:cgi-bin/pkclient.exe
ca configure example.com ca 1 100 crloptional
telnet timeout 5
terminal width 80

```

## Configuring PIX Firewall 2 with a VeriSign CA



### Note

The following steps are nearly the same as those in the previous section “[Configuring PIX Firewall 1 with a VeriSign CA](#)” for configuring PIX Firewall 2. The differences are in Steps 1 and 2, and Steps 11 to 13, which are specific for the PIX Firewall 2 in this example.

Perform the following steps to configure PIX Firewall 2 for using a VeriSign CA:

**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 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 20 crloptional
```

These commands are stored in the configuration. “2” 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 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:

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

Before entering this command, contact your CA administrator because they will have to authenticate your PIX Firewall manually before granting its certificate.

“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 following 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
```

---

[Example 7-4](#) lists the configuration for PIX Firewall 2. PIX Firewall default configuration values and certain CA commands are not displayed in a configuration listing.

#### **Example 7-4** PIX Firewall 2 CA Configuration

```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 dmz security50
nameif ethernet3 perimeter security40
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname SanJose
domain-name example.com
fixup protocol ftp 21
fixup protocol http 80
fixup protocol smtp 25
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol sqlnet 1521
names
pager lines 24
no logging on
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto
interface ethernet3 auto
mtu outside 1500
mtu inside 1500
mtu dmz 1500
mtu perimeter 1500
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
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
arp timeout 14400
nat (inside) 0 10.0.0.0 255.0.0.0 0 0
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
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
route outside 0.0.0.0 0.0.0.0 209.165.200.227 1
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
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
sysopt connection permit-ipsec
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
isakmp policy 8 authentication rsa-sig
isakmp policy 8 encryption des
isakmp policy 8 hash sha
isakmp policy 8 group 1
isakmp policy 8 lifetime 86400
ca identity example.com 209.165.202.130:cgi-bin/pkiclient.exe
ca configure example.com ca 2 20 crloptional
telnet timeout 5
terminal width 80

```

## Using PIX Firewall with an In-House CA

For the general procedures to configure the PIX Firewall for a CA, see “[Using Certification Authorities](#)” in [Chapter 6, “Configuring IPsec and Certification Authorities.”](#) This section provides a specific example for the network illustrated in [Figure 7-3](#) and includes the following topics:

- [Scenario Description](#)
- [Configuring PIX Firewall 1 for an In-House CA](#)
- [Configuring PIX Firewall 2 for an In-House CA](#)

## Scenario Description

PIX Firewall supports the use of the following certification authorities (CAs):

- VeriSign support is provided through the VeriSign Private Certificate Services (PCS) and the OnSite service, which lets you establish an in-house CA system for issuing digital certificates.
- Entrust, Entrust VPN Connector, version 4.1 (build 4.1.0.337) or higher. The Entrust CA server is an in-house CA server solution.
- Baltimore Technologies, UniCERT Certificate Management System, version 3.1.2 or higher. 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 higher. The Windows 2000 CA server is an in-house CA server solution.

These are all in-house CA servers, except for VeriSign, which provides both a public CA and a private CA solution.



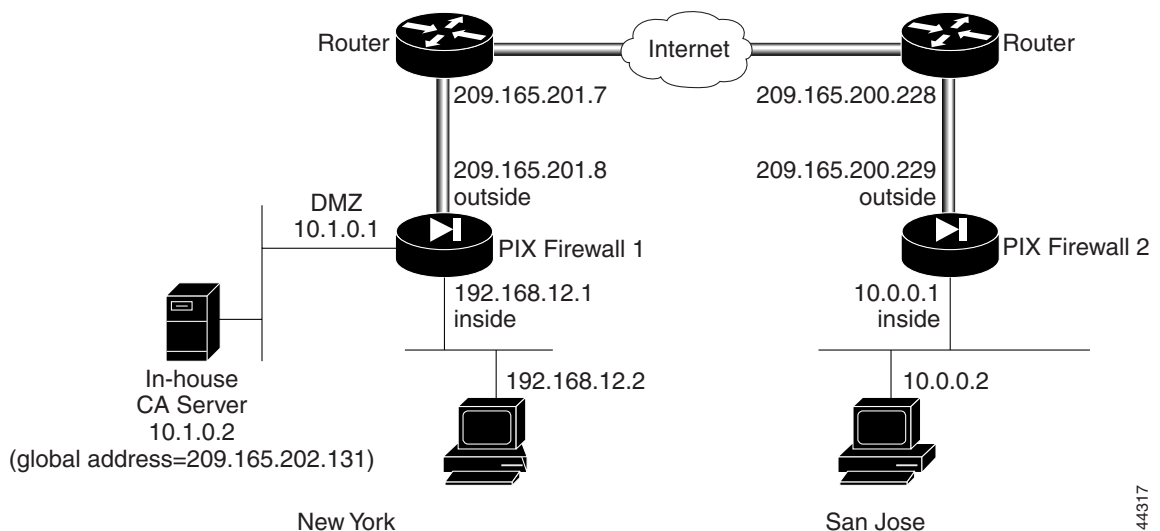
### Note

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

The in-house CA server in the following example is placed within the DMZ network of one PIX Firewall network (PIX Firewall 1). The VPN peer, PIX Firewall 2, should 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.

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.

**Figure 7-3 VPN Tunnel Network**



44317

## Configuring PIX Firewall 1 for an In-House CA

Follow these steps to configure PIX Firewall 1 for use with an in-house CA. These steps are similar to the procedure shown in “Using PIX Firewall with a VeriSign CA.”

**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 CA-related enrollment commands:

```
ca identity abcd 209.165.202.131 209.165.202.131
ca configure abcd ra 2 20 crloptional
```

These commands are stored in the configuration. **2** is the retry period, **20** is the retry count, and the **crloptional** option disables CRL checking.



**Note** For a Microsoft CA server, specify the internal network address followed by a colon and the pathname to the server executable, such as 10.1.0.2:/CERTSRV/mscep/mscep.dll.

**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:

```
ca enroll abcd cisco
```

Before entering this command, contact your CA administrator because they will have to authenticate your PIX Firewall manually before granting its certificate.

“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
```
-

[Example 7-5](#) lists the configuration for PIX Firewall 1.

Example 7-5 PIX Firewall 1 VPN Tunnel Configuration

```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname NewYork
domain-name example.com
fixup protocol ftp 21
fixup protocol http 80
fixup protocol smtp 25
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol sqlnet 1521
names
pager lines 24
no logging on
interface ethernet0 auto
interface ethernet1 auto
mtu outside 1500
```

```

mtu inside 1500
ip address outside 209.165.201.8 255.255.255.224
ip address inside 192.168.12.1 255.255.255.0
no failover
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
arp timeout 14400
static (dmz, outside) 209.165.202.131 10.1.0.2 netmask 255.255.255.255
conduit permit tcp host 209.165.202.131 eq 389 209.165.200.229 255.255.255.255
conduit permit tcp host 209.165.202.131 eq http 209.165.200.229 255.255.255.255
nat 0 access-list 90
access-list 90 permit ip 192.168.12.0 255.255.255.0 10.0.0.0 255.0.0.0
no rip outside passive
no rip outside default
rip inside passive
no rip inside default
route outside 10.0.0.0 255.0.0.0 209.165.200.229 1
route outside 0.0.0.0 0.0.0.0 209.165.200.227 1
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
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
sysopt connection permit-ipsec
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
isakmp policy 8 authentication rsa-sig
isakmp policy 8 encryption des
isakmp policy 8 hash sha
isakmp policy 8 group 1
isakmp policy 8 lifetime 86400
ca identity abcd 209.165.202.131 209.165.202.131
ca configure abcd ra 1 100 crloptional
telnet timeout 5
terminal width 80

```

Configuring PIX Firewall 2 for an In-House CA

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 CA-related enrollment commands:

```
ca identity abcd 209.165.202.131 209.165.202.131
ca configure abcd ra 2 20 crloptional
```

These commands are stored in the configuration. **2** is the retry period, **20** is the retry count, and the **crloptional** option disables CRL checking.




---

**Note** For a Microsoft CA server, specify the external (global) network address followed by a colon and the pathname to the server executable, such as 209.165.202.131:/certserv/mscep/mscep.dll.

---

**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
```

---

Example 7-6 lists the configuration for PIX Firewall 2.

**Example 7-6 PIX Firewall 2 VPN Tunnel Configuration**

```

nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 dmz security50
nameif ethernet3 perimeter security40
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname SanJose
domain-name example.com
fixup protocol ftp 21
fixup protocol http 80
fixup protocol smtp 25
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol sqlnet 1521
names
pager lines 24
no logging on
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto
interface ethernet3 auto
mtu outside 1500
mtu inside 1500
mtu dmz 1500
mtu perimeter 1500
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
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
arp timeout 14400
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
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
route outside 0.0.0.0 0.0.0.0 209.165.200.227 1
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
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
sysopt connection permit-ipsec
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
isakmp policy 8 authentication rsa-sig
isakmp policy 8 encryption des
isakmp policy 8 hash sha
isakmp policy 8 group 1
isakmp policy 8 lifetime 86400
ca identity abcd 209.165.202.131 209.165.202.131
ca configure abcd ra 1 100 crloptional
telnet timeout 5
terminal width 80

```

## Using an Encrypted Tunnel to Obtain Certificates

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 example, both PIX Firewall units enroll and request certificates from a CA server protected by PIX Firewall 1. PIX Firewall 2 enrolls and requests its certificate using an encrypted tunnel.

To accomplish this, you first establish a tunnel between the PIX Firewalls using a pre-shared key. You then use this tunnel to enroll and request the certificate for PIX Firewall 2. After obtaining a certificate, clear the IKE and IPSec SAs on both units and then configure them to use digital certificates.



### Note

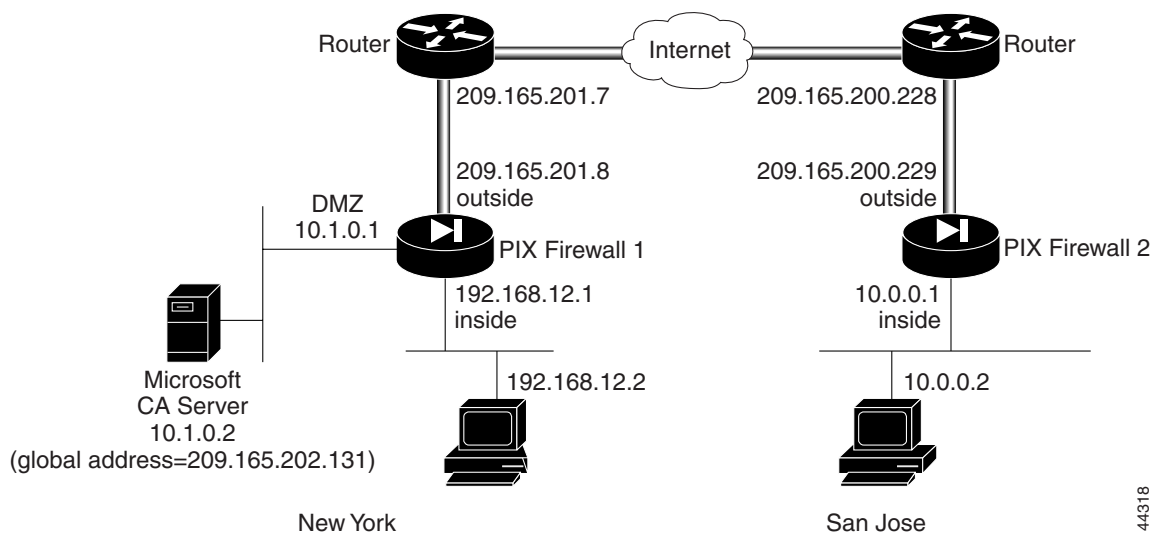
The example CA server address is to be used for example purposes only.

This section includes the following topics:

- [Establishing a Tunnel Using a Pre-Shared Key](#)
- [Establishing a Tunnel with a Certificate](#)

This example uses the network diagram shown in [Figure 7-4](#).

**Figure 7-4** VPN Tunnel Network



44318

## Establishing a Tunnel Using a Pre-Shared Key

This section describes how to establish a tunnel using a pre-shared key. It includes the following topics:

- [PIX Firewall 1 Configuration](#)
- [PIX Firewall 2 Configuration](#)

### PIX Firewall 1 Configuration

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.



Note The **ca identity** command shown is specific to the Microsoft CA. The **ca identity** you use depends 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.

PIX Firewall 2 Configuration

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.



Note The **ca identity** command shown is specific to the Microsoft CA. The **ca identity** you use depends 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.

Establishing a Tunnel with a Certificate

This section describes how to clear the SAs on each PIX Firewall and to establish a tunnel using a certificate. It includes the following topics:

- [PIX Firewall 1 Configuration](#)
- [PIX Firewall 2 Configuration](#)

PIX Firewall 1 Configuration

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
```
- 

### PIX Firewall 2 Configuration

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
```
-

# Manual Configuration with NAT

In this example, two PIX Firewall units are used to create a Virtual Private Network (VPN) between the networks on each PIX Firewall unit's inside interface. This section includes the following topics:

- [PIX Firewall 1 Configuration](#)
- [PIX Firewall 2 Configuration](#)

This network is part of an intranet. In this example, the VPN is created without the use of IKE or a CA and pre-shared keys are used.

## PIX Firewall 1 Configuration

Follow these steps to program the PIX Firewall 1 unit for IPSec:

- 
- Step 1** Create a **crypto map** command statement.
- Step 2** Create the **access-list** command entries to select traffic for this policy.



**Note** For manual keying, only one **access-list permit** command statement is permitted in the configuration.

---

- Step 3** Create the transform set for the **crypto** command statement entry.
- Step 4** Define cryptographic state informations. These include SPI, and the necessary keys for manual keying and policy negotiation for ISAKMP.
- Step 5** Repeat Steps 1-4 for each group of policies.
- Step 6** Associate the **crypto map** command statement with an interface.
- 

[Example 7-7](#) lists the configuration for PIX Firewall 1.

### **Example 7-7 Two Interfaces with IPSec—PIX Firewall 1 Configuration**

```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
interface ethernet0 auto
interface ethernet1 auto
ip address outside 192.168.1.1 255.255.255.0
ip address inside 10.1.1.1 255.255.255.0
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pixfirewall
fixup protocol ftp 21
fixup protocol http 80
fixup protocol smtp 25
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol sqlnet 1521
access-list 10 permit ip host 192.168.128.3 host 209.165.200.225
no failover
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
```

```

names
pager lines 24
no logging timestamp
logging console debugging
logging monitor errors
logging buffered errors
no logging trap
logging facility 20
mtu outside 1500
mtu inside 1500
arp timeout 14400
nat (inside) 1 0 0
global (outside) 1 192.168.1.100-192.168.1.150
static (inside,outside) 192.168.128.3 10.1.1.3 netmask 255.255.255.255 0 0
no rip outside passive
no rip outside default
no rip inside passive
no rip inside default
route outside 0.0.0.0 0.0.0.0 192.168.1.49 1
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
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
sysopt connection tcpmss 1380
sysopt connection permit-ipsec
crypto ipsec transform-set myset ah-md5-hmac esp-des
crypto map mymap 10 ipsec-manual
crypto map mymap 10 match address 10
crypto map mymap 10 set peer 192.168.1.100
crypto map mymap 10 set transform-set myset
crypto map mymap 10 set session-key inbound ah 400 123456789A123456789A123456789A12
crypto map mymap 10 set session-key outbound ah 300 123456789A123456789A123456789A12
crypto map mymap 10 set session-key inbound esp 400 cipher abcd1234abcd1234
crypto map mymap 10 set session-key outbound esp 300 cipher abcd1234abcd1234
telnet timeout 5
terminal width 80
crypto map mymap interface outside

```

## PIX Firewall 2 Configuration

Follow these steps to program the PIX Firewall 2 unit for IPsec:

- 
- Step 1** Create a **crypto map** command statement.
  - Step 2** Create the **access-list** command entries to select traffic for this policy.




---

**Note** For manual keying, only one **access-list permit** command statement is permitted in the configuration.

---

- Step 3** Create the transform set for the **crypto** command statement entry.
- Step 4** Define cryptographic state informations. These include SPI, and the necessary keys for manual keying and policy negotiation for ISAKMP.
- Step 5** Repeat Steps 1-4 for each group of policies.

**Step 6** Associate the **crypto map** command statement with an interface.

**Example 7-8** lists the configuration for PIX Firewall 2.

**Example 7-8 Two Interfaces with IPSec—PIX Firewall 2 Configuration**

```

nameif ethernet0 outside security0
nameif ethernet1 inside security100
interface ethernet0 auto
interface ethernet1 auto
ip address outside 209.165.201.3 255.255.255.224
ip address inside 10.0.0.3 255.255.255.0
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pixfirewall
fixup protocol ftp 21
fixup protocol http 80
fixup protocol smtp 25
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol sqlnet 1521
access-list 10 permit ip host 209.165.200.225 host 192.168.128.3
no failover
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
names
pager lines 24
no logging timestamp
logging console debugging
logging monitor errors
logging buffered errors
no logging trap
logging facility 20
mtu outside 1500
mtu inside 1500
arp timeout 14400
nat (inside) 1 0 0
static (inside,outside) 209.165.200.225 10.0.0.3 netmask 255.255.255.255 0 0
route outside 0.0.0.0 0.0.0.0 192.168.1.49 1
route inside 10.0.0.0 255.255.255.0 10.0.0.3 1
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
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
no rip outside passive
no rip outside default
no rip inside passive
no rip inside default
sysopt connection tcpmss 1380
crypto ipsec transform-set myset ah-md5-hmac esp-des
crypto map mymap 10 ipsec-manual
crypto map mymap 10 match address 10
crypto map mymap 10 set peer 192.168.1.1
crypto map mymap 10 set transform-set myset
crypto map mymap 10 set session-key inbound ah 300 123456789A123456789A123456789A12
crypto map mymap 10 set session-key outbound ah 400 123456789A123456789A123456789A12
crypto map mymap 10 set session-key inbound esp 300 cipher abcd1234abcd1234
crypto map mymap 10 set session-key outbound esp 400 cipher abcd1234abcd1234
telnet timeout 5
terminal width 80

```

