



Configuring IPSec

This chapter provides the steps to configure IPSec where IPSec security associations will be established via IKE or pre-shared keys (without IKE).

For IPSec background information, see Chapter 2, “About IPSec.”

For a complete description of the IPSec-related commands used in this chapter, refer to Chapter 12, “Command Reference.” For a complete description of the non-IPSec commands used in this chapter, refer to the “Command Reference” chapter within the *Configuration Guide for the Cisco Secure PIX Firewall Version 5.3*.

The following sections are included in this chapter:

- Configuring IPSec with IKE
- Configuring Manual IPSec
- What to Do Next

Configuring IPSec with IKE

The following steps cover minimal IPSec configuration where the IPSec security associations will be established via IKE:

Step 1 Create an access list to define the traffic to protect:

```
access-list access-list-name {deny | permit} ip source source-netmask destination
destination-netmask
```

For example:

```
access-list 101 permit ip 10.0.0.0 255.255.255.0 10.1.1.0 255.255.255.0
```

In this example, the **permit** keyword causes all traffic that matches the specified conditions to be protected by crypto.

Step 2 Configure a transform set that defines how the traffic will be protected. You can configure multiple transform sets, and then specify one or more of these transform sets in a crypto map entry (Step 4d).

```
crypto ipsec transform-set transform-set-name transform1 [transform2, transform3]
```

For example:

```
crypto ipsec transform-set myset1 esp-des esp-sha-hmac
crypto ipsec transform-set myset2 ah-sha-hmac esp-3des esp-sha-hmac
```

In this example, “myset1” and “myset2” are the names of the transform sets. “myset1” has two transforms defined, while “myset2” has three transforms defined.

Step 3 Create a crypto map entry by performing the following steps:

- a. Create a crypto map entry in IPSec ISAKMP mode:

```
crypto map map-name seq-num ipsec-isakmp
```

For example:

```
crypto map mymap 10 ipsec-isakmp
```

In this example, “mymap” is the name of the crypto map set. The map set’s sequence number is 10, which is used to rank multiple entries within one crypto map set. The lower the sequence number, the higher the priority.

- b. Assign an access list to a crypto map entry:

```
crypto map map-name seq-num match address access-list-name
```

For example:

```
crypto map mymap 10 match address 101
```

In this example, access-list 101 is assigned to crypto map “mymap.”

- c. Specify the peer to which the IPSec protected traffic can be forwarded:

```
crypto map map-name seq-num set peer ip-address
```

For example:

```
crypto map mymap 10 set peer 192.168.1.100
```

The security association will be set up with the peer having an IP address of 192.168.1.100. Specify multiple peers by repeating this command.

- d. Specify which transform sets are allowed for this crypto map entry. List multiple transform sets in order of priority (highest priority first). You can specify up to six transform sets.

```
crypto map map-name seq-num set transform-set transform-set-name1  
[transform-set-name2, ...transform-set-name6]
```

For example:

```
crypto map mymap 10 set transform-set myset1 myset2
```

In this example, when traffic matches access list 101, the security association can use either “myset1” (first priority) or “myset2” (second priority) depending on which transform set matches the peer’s transform set.

- e. (Optional) Specify security association lifetime for the crypto map entry, if you want the security associations for this entry to be negotiated using different IPSec security association lifetimes other than the global lifetimes.

```
crypto map map-name seq-num set security-association lifetime {seconds seconds |  
kilobytes kilobytes}
```

For example:

```
crypto map mymap 10 set security-association lifetime seconds 2700
```

This example shortens the timed lifetime for the crypto map “mymap 10” to 2,700 seconds (45 minutes). The traffic volume lifetime is not change.

- f. (Optional) Specify that IPsec should ask for perfect forward secrecy (PFS) when requesting new security associations for this crypto map entry, or should require PFS in requests received from the peer:

```
crypto map map-name seq-num set pfs [group1 | group2]
```

For example:

```
crypto map mymap 10 set pfs group2
```

This example specifies that PFS should be used whenever a new security association is negotiated for the crypto map “mymap 10.” The 1024-bit Diffie-Hellman prime modulus group will be used when a new security association is negotiated using the Diffie-Hellman exchange.

Step 4 (Optional) Create a crypto dynamic map entry by performing the following steps:

- a. (Optional) Assign an access list to a dynamic crypto map entry, which determines which traffic should be protected and not protected:

```
crypto dynamic-map dynamic-map-name dynamic-seq-num match address access-list-name
```

For example:

```
crypto dynamic-map dyn1 10 match address 101
```

In this example, access list 101 is assigned to dynamic crypto map “dyn1.” The map’s sequence number is 10.

- b. (Optional) Specify the peer to which the IPsec-protected traffic can be forwarded. This is *rarely* configured in dynamic crypto map entries because dynamic crypto map entries are often used for unknown peers.

```
crypto dynamic-map dynamic-map-name dynamic-seq-num set peer ip-address
```

For example:

```
crypto dynamic-map dyn1 10 set peer 192.168.1.102
```

In this example, the security association will be set up with the peer having an IP address of 192.168.1.102. Specify multiple peers by repeating this command.

- c. Specify which transform sets are allowed for this dynamic crypto map entry. List multiple transform sets in order of priority (highest priority first).

```
crypto dynamic-map dynamic-map-name dynamic-seq-num set transform-set  
transform-set-name1, [transform-set-name2, ...transform-set-name9]
```

For example:

```
crypto dynamic-map dyn 10 set transform-set myset1 myset2
```

In this example, when traffic matches access list 101, the security association can use either “myset1” (first priority) or “myset2” (second priority) depending on which transform set matches the peer’s transform sets.

- d. (Optional) Specify security association lifetime for the crypto dynamic map entry, if you want the security associations for this entry to be negotiated using different IPsec security association lifetimes other than the global lifetimes:

```
crypto dynamic-map dynamic-map-name dynamic-seq-num set security-association lifetime  
{seconds seconds | kilobytes kilobytes}
```

For example:

```
crypto dynamic-map dyn1 10 set security-association lifetime 2700
```

This example shortens the timed lifetime for dynamic crypto map “dyn1 10” to 2,700 seconds (45 minutes). The time volume lifetime is not changed.

- e. (Optional) Specify that IPSec should ask for PFS when requesting new security associations for this dynamic crypto map entry, or should demand PFS in requests received from the peer:

```
crypto dynamic-map dynamic-map-name dynamic-seq-num set pfs [group1 | group2]
```

For example:

```
crypto dynamic-map dyn1 10 set pfs group1
```

- f. Add the dynamic crypto map set into a static crypto map set.

Be sure to set the crypto map entries referencing dynamic maps to be the lowest priority entries (highest sequence numbers) in a crypto map set.

```
crypto map map-name seq-num ipsec-isakmp dynamic dynamic-map-name
```

For example:

```
crypto map mymap 200 ipsec-isakmp dynamic dyn1
```

- Step 5** Apply a crypto map set to an interface on which the IPSec traffic will be evaluated:

```
crypto map map-name interface interface-name
```

For example:

```
crypto map mymap interface outside
```

In this example, the PIX Firewall will evaluate the traffic going through the outside interface against the crypto map “mymap” to determine whether it needs to be protected.

- Step 6** Specify that IPSec traffic be implicitly trusted (permitted):

```
sysopt connection permit-ipsec
```

Configuring Manual IPSec

The following steps cover minimal IPSec configuration where the security associations will be established via pre-shared keys:

- Step 1** Create an access list to define the traffic to protect:

```
access-list access-list-name {deny | permit} ip source source-netmask destination destination-netmask
```

For example:

```
access-list 101 permit ip 10.0.0.0 255.255.255.0 10.1.1.0 255.255.255.0
```

In this example, the keyword **permit** causes all traffic that matches the specified conditions to be protected by crypto.

- Step 2** Configure a transform set that defines how the traffic will be protected.
- You can configure only one transform set for manually established security associations. The peer must also have the same transform set specified.
- ```
crypto ipsec transform-set transform-set-name transform
```
- For example:
- ```
crypto ipsec transform-set myset3 ah-sha-hmac esp-des esp-sha-hmac
```
- In this example, “myset3” is the name of the transform set and three transforms have been defined.
- Step 3** Create a crypto map entry in IPsec manual mode:
- ```
crypto map map-name seq-num ipsec-manual
```
- For example:
- ```
crypto map mymaptwo 30 ipsec-manual
```
- Step 4** Name an IPsec access list. The access list can specify only one permit entry when you are establishing manual security associations.
- ```
crypto map map-name seq-num match address access-list-name
```
- For example:
- ```
crypto map mymaptwo 30 match address 101
```
- Step 5** Specify the peer to which the IPsec protected traffic can be forwarded. Only one peer can be specified when you are establishing manual security associations.
- ```
crypto map map-name seq-num set peer ip-address
```
- For example:
- ```
crypto map mymaptwo 30 set peer 192.186.1.103
```
- Step 6** Specify which transform set should be used. This must be the same transform set that is specified in the peer's corresponding crypto map entry.
- ```
crypto map map-name seq-num set transform-set transform-set-name
```
- For example:
- ```
crypto map mymaptwo 30 set transform-set myset3
```
- Step 7** If the specified transform set includes the AH protocol (authentication via MD5-HMAC or SHA-HMAC), set the AH Security Parameter Index (SPI) and key to apply to inbound protected traffic. If the specified transform set includes only the ESP protocol, skip to Step 9.
- ```
crypto map map-name seq-num set session-key inbound ah spi hex-key-data
```
- For example:
- ```
crypto map mymaptwo 30 set session-key inbound ah 300
123456789A123456789A123456789A123456789A
```
- In this example, the IPsec session key for AH protocol is specified within crypto map “mymaptwo” to be used with the inbound protected traffic.
- Step 8** Set the AH SPIs and keys to apply to outbound protected traffic:
- ```
crypto map map-name seq-num set session-key outbound ah spi hex-key-data
```

For example:

```
crypto map mymaptwo 30 set session-key outbound ah 400
123456789A123456789A123456789A123456789A
```

- Step 9** If the specified transform set includes the ESP protocol, set the ESP SPIs and keys to apply to inbound protected traffic. If the transform set includes an ESP cipher algorithm, specify the cipher keys. If the transform set includes an ESP authenticator algorithm, specify the authenticator keys.

```
crypto map map-name seq-num set session-key inbound esp spi cipher hex-key-data
[authenticator hex-key-data]
```

For example:

```
crypto map mymaptwo 30 set session-key inbound esp 300 cipher 1234567890123456
authenticator 0000111122223333444455556666777788889999
```

- Step 10** Set the ESP SPIs and keys to apply to outbound protected traffic. If the transform set includes an ESP cipher algorithm, specify the cipher keys. If the transform set includes an ESP authenticator algorithm, specify the authenticator keys.

```
crypto map map-name seq-num set session-key outbound esp spi cipher hex-key-data
[authenticator hex-key-data]
```

For example:

```
crypto map mymaptwo 30 set session-key outbound esp 300 cipher abcdefghijklmnop
authenticator 9999888877776666555544443333222211110000
```

- Step 11** Apply a crypto map set to an interface on which the IPsec traffic will be evaluated:

```
crypto map map-name interface interface-name
```

For example:

```
crypto map mymaptwo interface outside
```

In this example, the PIX Firewall will evaluate the traffic going through the outside interface against the “mymaptwo” crypto map to determine whether it needs to be protected.

- Step 12** Specify that IPsec traffic be implicitly trusted (permitted):

```
sysopt connection permit-ipsec
```

---

## What to Do Next

If the PIX Firewall will interoperate with remote VPN Clients, and you will use TACACS+ or RADIUS as your user authentication method, configure IKE Extended Authentication (Xauth). See “Configuring Extended Authentication” within Chapter 8, “Advanced Configurations.”

If the PIX Firewall will interoperate with remote VPN Clients, configure IKE Mode Configuration (Config), which allows for dynamic IP address assignment for the VPN Clients. See “Configuring Extended Authentication” within Chapter 8, “Advanced Configurations.”

If you will configure both Xauth and IKE Mode Config, configure Xauth first.

If you will not configure either Xauth or IKE Mode Config, you have completed the required IPsec configurations.