CHAPTER 66

Configuring Remote Access IPsec VPNs

This chapter describes how to configure Remote Access IPsec VPNs and includes the following sections:

Information About Remote Access IPsec VPNs

Remote access VPNs allow users to connect to a central site through a secure connection over a TCP/IP network such as the Internet. The Internet Security Association and Key Management Protocol, also called IKE, is the negotiation protocol that lets the IPsec client on the remote PC and the ASA agree on how to build an IPsec Security Association. Each ISAKMP negotiation is divided into two sections called Phase1 and Phase2.

Phase 1 creates the first tunnel to protect later ISAKMP negotiation messages. Phase 2 creates the tunnel that protects data travelling across the secure connection.

To set the terms of the ISAKMP negotiations, you create an ISAKMP policy. It includes the following:

- An authentication method, to ensure the identity of the peers.
- An encryption method, to protect the data and ensure privacy.
- A Hashed Message Authentication Codes (HMAC) method to ensure the identity of the sender and to ensure that the message has not been modified in transit.
- A Diffie-Hellman group to set the size of the encryption key.
- A time limit for how long the ASA uses an encryption key before replacing it.

A transform set combines an encryption method and an authentication method. During the IPsec security association negotiation with ISAKMP, the peers agree to use a particular transform set to protect a particular data flow. The transform set must be the same for both peers.

A transform set protects the data flows for the access list specified in the associated crypto map entry. You can create transform sets in the ASA configuration, and then specify a maximum of 11 of them in a crypto map or dynamic crypto map entry. For more overview information, including a table that lists valid encryption and authentication methods, see Creating a Transform Set in Chapter 70, "Configuring LAN-to-LAN IPsec VPNs" of this guide.

Licensing Requirements for Remote Access IPsec VPNs

The following table shows the licensing requirements for this feature:

Model	License Requirement
ASA 5505	Base License: 10 sessions (25 combined IPSec and SSL VPN[1]). Security Plus License: 25 sessions (25 combined IPSec and SSL VPN[1]).
ASA 5510	Base and Security Plus License: 250 sessions (250 combined IPSec and SSL VPN[1]).
ASA 5520	Base and Security Plus License: 750 sessions (750 combined IPSec and SSL VPN[1]).
ASA 5540	Base and Security Plus License: 5000 sessions (5000 combined IPSec and SSL VPN[1]).
ASA 5550 and 5580	Base and Security Plus License: 5000 sessions (5000 combined IPSec and SSL VPN[1]).

[1] Although the maximum IPSec and SSL VPN sessions add up to more than the maximum VPN sessions, the combined sessions should not exceed the VPN session limit. If you exceed the maximum VPN sessions, you can overload the ASA, so be sure to size your network appropriately.

Guidelines and Limitations

This section includes the guidelines and limitations for this feature.

Context Mode Guidelines

Supported in single context mode only. Does not support multiple context mode.

Firewall Mode Guidelines

Not supported in routed or transparent firewall mode.

Failover Guidelines

IPsec VPN sessions are replicated in Active/Standby failover configurations only. Active/Active failover configurations are not supported.

IPv6 Guidelines

Does not support IPv6.

Configuring Remote Access IPsec VPNs

This section describes how to configure remote access VPNs and includes the following topics:

- Configuring Interfaces, page 66-3

- Configuring ISAKMP Policy and Enabling ISAKMP on the Outside Interface, page 66-4
- Configuring an Address Pool, page 66-5
- Adding a User, page 66-5
- Creating a Transform Set, page 66-6
- Defining a Tunnel Group, page 66-6
- Creating a Dynamic Crypto Map, page 66-7
- Creating a Crypto Map Entry to Use the Dynamic Crypto Map, page 66-8
- Saving the Security Appliance Configuration, page 66-9

Configuring Interfaces

An ASA has at least two interfaces, referred to here as outside and inside. Typically, the outside interface is connected to the public Internet, while the inside interface is connected to a private network and is protected from public access.

To begin, configure and enable two interfaces on the ASA. Then assign a name, IP address and subnet mask. Optionally, configure its security level, speed and duplex operation on the security appliance.

To configure interfaces, perform the following steps, using the command syntax in the examples:

Detailed Steps

	Command	Purpose
Step 1	**interface** {*interface*} **Example:** hostname(config)# interface ethernet0 hostname(config-if)#	Enters interface configuration mode from global configuration mode.
Step 1	**ip address** *ip_address* [*mask*] [**standby** *ip_address*] **Example:** hostname(config)# interface ethernet0 hostname(config-if)# hostname(config-if)# ip address 10.10.4.200 255.255.0.0	Sets the IP address and subnet mask for the interface.
Step 2	**nameif** *name* **Example:** hostname(config-if)# nameif outside hostname(config-if)#	Specifies a name for the interface (maximum of 48 characters). You cannot change this name after you set it.
Step 3	**shutdown** **Example:** hostname(config-if)# no shutdown hostname(config-if)#	Enables the interface. By default, interfaces are disabled.

Configuring ISAKMP Policy and Enabling ISAKMP on the Outside Interface

This section describes the procedure to configure an ISAKMP policy on the outside interface and how to enable the policy.

Detailed Steps

Perform the following steps and use the command syntax in the following examples as a guide.

	Command	Purpose

Step 1	**isakmp policy** *priority* **authentication** {**crack** | **pre-share** | **rsa-sig**}
	Example:
	`hostname(config)# isakmp policy 1 authentication pre-share`
	`hostname(config)#`
		Specifies the authentication method and the set of parameters to use during IKE negotiation.
		Priority uniquely identifies the Internet Key Exchange (IKE) policy and assigns a priority to the policy. Use an integer from 1 to 65,534, with 1 being the highest priority and 65,534 the lowest.
		In this example and the steps that follow, we set the priority to 1.

Step 2	**isakmp policy** *priority* **encryption** {**aes** | **aes-192** | **aes-256** | **des** | **3des**}
	Example:
	`hostname(config)# isakmp policy 1 encryption 3des`
	`hostname(config)#`
		Specifies the encryption method to use within an IKE policy.

Step 3	**isakmp policy** *priority* **hash** {**md5** | **sha**}
	Example:
	`hostname(config)# isakmp policy 1 hash sha`
	`hostname(config)#`
		Specifies the hash algorithm for an IKE policy (also called the HMAC variant).

Step 4	**isakmp policy** *priority* **group** {**1** | **2** | **5**}
	Example:
	`hostname(config)# isakmp policy 1 group 2`
	`hostname(config)#`
		Specifies the Diffie-Hellman group for the IKE policy—the crypto protocol that allows the IPsec client and the ASA to establish a shared secret key.

Step 5	**isakmp policy** *priority* **lifetime** {*seconds*}
	Example:
	`hostname(config)# isakmp policy 1 lifetime 43200`
	`hostname(config)#`
		Specifies the encryption key lifetime—the number of seconds each security association should exist before expiring.
		The range for a finite lifetime is 120 to 2147483647 seconds. Use 0 seconds for an infinite lifetime.

	Command	Purpose
Step 6	**isakmp enable** *interface-name* **Example:** hostname(config)# isakmp enable outside hostname(config)#	Enables ISAKMP on the interface named *outside*.
Step 7	**write memory** **Example:** hostname(config-if)# write memory Building configuration... Cryptochecksum: 0f80bf71 1623a231 63f27ccf 8700ca6d 11679 bytes copied in 3.390 secs (3893 bytes/sec) [OK] hostname(config-if)#	Saves the changes to the configuration.

Configuring an Address Pool

The ASA requires a method for assigning IP addresses to users. This section uses address pools as an example. Use the command syntax in the following examples as a guide.

Command	Purpose
ip local pool *poolname* *first-address***—***last-address* [**mask** *mask*] **Example:** hostname(config)# ip local pool testpool 192.168.0.10-192.168.0.15 hostname(config)#	Creates an address pool with a range of IP addresses, from which the ASA assigns addresses to the clients. The address mask is optional. However, You must supply the mask value when the IP addresses assigned to VPN clients belong to a non-standard network and the data could be routed incorrectly if you use the default mask. A typical example is when the IP local pool contains 10.10.10.0/255.255.255.0 addresses, since this is a Class A network by default. This could cause routing issues when the VPN client needs to access different subnets within the 10 network over different interfaces.

Adding a User

This section shows how to configure usernames and passwords. Use the command syntax in the following examples as a guide.

Command	Purpose
username *name* {**nopassword** | **password** *password* [**mschap** | **encrypted** | **nt-encrypted**]} [**privilege** *priv_level*] **Example:** hostname(config)# username testuser password 12345678 hostname(config)#	Creates a user, password, and privilege level.

Creating a Transform Set

This section shows how to configure a transform set, which combines an encryption method and an authentication method.

Use the command syntax in the following examples as a guide.

Command	Purpose

crypto ipsec transform-set *transform-set-name encryption-method* [*authentication*]
Example:
`hostname(config)# crypto ipsec transform set FirstSet esp-3des esp-md5-hmac`
`hostname(config)#`
	Configures a transform set that specifies the IPsec encryption and hash algorithms to be used to ensure data integrity.
	Use one of the following values for *encryption*:
	• **esp-aes** to use AES with a 128-bit key.
	• **esp-aes-192** to use AES with a 192-bit key.
	• **esp-aes-256** to use AES with a 256-bit key.
	• **esp-des** to use 56-bit DES-CBC.
	• **esp-3des** to use triple DES algorithm.
	• **esp-null** to not use encryption.
	Use one of the following values for *authentication*:
	• **esp-md5-hmac** to use the MD5/HMAC-128 as the hash algorithm.
	• **esp-sha-hmac** to use the SHA/HMAC-160 as the hash algorithm.
	• **esp-none** to not use HMAC authentication.

Defining a Tunnel Group

This section describes how to configure a tunnel group, which is a set of records that contain tunnel connection policies. You configure a tunnel group to identify AAA servers, specify connection parameters, and define a default group policy. The ASA stores tunnel groups internally.

There are two default tunnel groups in the ASA system: DefaultRAGroup, which is the default IPsec remote-access tunnel group, and DefaultL2Lgroup, which is the default IPsec LAN-to-LAN tunnel group. You can change them but not delete them. The ASA uses these groups to configure default tunnel parameters for remote access and LAN-to-LAN tunnel groups when there is no specific tunnel group identified during tunnel negotiation.

Use the command syntax in the following examples as a guide.

Detailed Steps

	Command	Purpose
Step 1	**tunnel-group** *name* **type** *type* **Example:** hostname(config)# tunnel-group testgroup type ipsec-ra hostname(config)#	Creates an IPsec remote access tunnel-group (also called connection profile).
Step 2	**tunnel-group** *name* **general-attributes** **Example:** hostname(config)# tunnel-group testgroup general-attributes hostname(config-tunnel-general)#	Enters tunnel group general attributes mode where you can enter an authentication method.
Step 3	**address-pool** [(*interface name*)] **address_pool1** [...address_pool6] **Example:** hostname(config-general)# address-pool testpool	Specifies an address pool to use for the tunnel group.
Step 4	**tunnel-group** *name* **ipsec-attributes** **Example:** hostname(config)# tunnel-group testgroup ipsec-attributes hostname(config-tunnel-ipsec)#	Enters tunnel group ipsec attributes mode where you can enter ipsec-specific attributes.
Step 5	**pre-shared-key** *key* **Example:** hostname(config-tunnel-ipsec)# pre-shared-key 44kkaol59636jnfx	(Optional) Configures a pre-shared key. The key can be an alphanumeric string from 1-128 characters. The keys for the adaptive security appliance and the client must be identical. If a Cisco VPN Client with a different preshared key size tries to connect, the client logs an error message indicating it failed to authenticate the peer.

Creating a Dynamic Crypto Map

This section describes how to configure dynamic crypto maps, which define a policy template where all the parameters do not have to be configured. These dynamic crypto maps let the ASA receive connections from peers that have unknown IP addresses. Remote access clients fall in this category.

Dynamic crypto map entries identify the transform set for the connection. You also enable reverse routing, which lets the ASA learn routing information for connected clients, and advertise it via RIP or OSPF.

Use the command syntax in the following examples as a guide.

Detailed Steps

	Command	Purpose

Step 1	**crypto dynamic-map** *dynamic-map-name* *seq-num* **set transform-set** *transform-set-name*
	Example:
	`hostname(config)# crypto dynamic-map dyn1 1 set transform-set FirstSet`
	`hostname(config)#`
		Creates a dynamic crypto map and specifies a transform set for the map.

Step 2	**crypto dynamic-map** *dynamic-map-name* *dynamic-seq-num* **set reverse-route**
	Example:
	`hostname(config)# crypto dynamic-map dyn1 1 set reverse route`
	`hostname(config)#`
		(Optional) Enables Reverse Route Injection for any connection based on this crypto map entry.

Creating a Crypto Map Entry to Use the Dynamic Crypto Map

This section describes how to create a crypto map entry that lets the ASA use the dynamic crypto map to set the parameters of IPsec security associations.

In the following examples for this command, the name of the crypto map is *mymap*, the sequence number is 1, and the name of the dynamic crypto map is *dyn1*, which you created in the previous section, "Creating a Dynamic Crypto Map."

Use the command syntax in the following examples as a guide.

Detailed Steps

	Command	Purpose

Step 1	**crypto map** *map-name* *seq-num* **ipsec-isakmp dynamic** *dynamic-map-name*
	Example:
	`hostname(config)# crypto map mymap 1 ipsec-isakmp dynamic dyn1`
	`hostname(config)#`
		Creates a crypto map entry that uses a dynamic crypto map.

Step 2	**crypto map** *map-name* **interface** *interface-name*
	Example:
	`hostname(config)# crypto map mymap interface outside`
	`hostname(config)#`
		Applies the crypto map to the outside interface.

Saving the Security Appliance Configuration

After performing the preceding configuration tasks, be sure to save your configuration changes as shown in this example:

Command	Purpose
write memory **Example:** hostname(config-if)# write memory Building configuration... Cryptochecksum: 0f80bf71 1623a231 63f27ccf 8700ca6d 11679 bytes copied in 3.390 secs (3893 bytes/sec) [OK] hostname(config-if)#	Saves the changes to the configuration.

Configuration Examples for Remote Access IPsec VPNs

The following example shows how to configure Remote Access IPsec VPNs:

```
hostname(config)# interface ethernet0
hostname(config-if)# ip address 10.10.4.200 255.255.0.0
hostname(config-if)# nameif outside
hostname(config-if)# no shutdown
hostname(config)# isakmp policy 1 authentication pre-share
hostname(config)# isakmp policy 1 encryption 3des
hostname(config)# isakmp policy 1 hash sha
hostname(config)# isakmp policy 1 group 2
hostname(config)# isakmp policy 1 lifetime 43200
hostname(config)# isakmp enable outside
hostname(config)# ip local pool testpool 192.168.0.10-192.168.0.15
hostname(config)# username testuser password 12345678
hostname(config)# crypto ipsec transform set FirstSet esp-3des esp-md5-hmac
hostname(config)# tunnel-group testgroup type ipsec-ra
hostname(config)# tunnel-group testgroup general-attributes
hostname(config-general)# address-pool testpool
hostname(config)# tunnel-group testgroup ipsec-attributes
hostname(config-ipsec)# pre-shared-key 44kkaol59636jnfx
hostname(config)# crypto dynamic-map dyn1 1 set transform-set FirstSet
hostname(config)# crypto dynamic-map dyn1 1 set reverse-route
hostname(config)# crypto map mymap 1 ipsec-isakmp dynamic dyn1
hostname(config)# crypto map mymap interface outside
hostname(config)# write memory
```

Feature History for Remote Access IPsec VPNs

Table 66-1 lists the release history for this feature.

Table 66-1 Feature History for Feature-1

Feature Name	Releases	Feature Information
Remote access VPNs	7.0	Remote access VPNs allow users to connect to a central site through a secure connection over a TCP/IP network such as the Internet.