


# 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, page 6-1
- Licensing Requirements for Remote Access IPsec VPNs, page 6-2
- Guidelines and Limitations, page 6-5
- Configuring Remote Access IPsec VPNs, page 6-6
- Configuration Examples for Remote Access IPsec VPNs, page 6-13
- Feature History for Remote Access VPNs, page 6-14


# 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 ACL 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 the Creating an IKEv1 Transform Set, page 10-6 in Chapter 10, "LAN-to-LAN IPsec VPNs" of this guide.

You can configure the ASA to assign an IPv4 address, an IPv6 address, or both an IPv4 and an IPv6 address to an AnyConnect client by creating internal pools of addresses on the ASA or by assigning a dedicated address to a local user on the ASA.

The endpoint must have the dual-stack protocol implemented in its operating system to be assigned both types of addresses. In both scenarios, when no IPv6 address pools are left but IPv4 addresses are available or when no IPv4 address pools are left but IPv6 addresses are available, connection still occurs. The client is not notified; however, so the administrator must look through the ASA logs for the details.

Assigning an IPv6 address to the client is supported for the SSL protocol. This feature is not supported for the IKEv2/IPsec protocol.

# Licensing Requirements for Remote Access IPsec VPNs

The following table shows the licensing requirements for this feature:

**Note** This feature is not available on No Payload Encryption models.w

| Model | License Requirement[1] |
|---|---|
| ASA 5505 | • IPsec remote access VPN using IKEv2 (use one of the following):<br>– AnyConnect Premium license:<br>Base license and Security Plus license: 2 sessions.<br>*Optional permanent or time-based licenses: 10 or 25 sessions.*<br>*Shared licenses are not supported.*[2]<br>– AnyConnect Essentials license[3]: 25 sessions.<br>• IPsec remote access VPN using IKEv1 and IPsec site-to-site VPN using IKEv1 or IKEv2:<br>– Base license: 10 sessions.<br>– Security Plus license: 25 sessions. |
| ASA 5512-X | • IPsec remote access VPN using IKEv2 (use one of the following):<br>– AnyConnect Premium license:<br>Base license and Security Plus license: 2 sessions.<br>*Optional permanent or time-based licenses: 10, 25, 50, 100, or 250 sessions.*<br>*Optional Shared licenses*[2]*: Participant or Server. For the Server license, 500-50,000 in increments of 500 and 50,000-545,000 in increments of 1000.*<br>– AnyConnect Essentials license[3]: 250 sessions.<br>• IPsec remote access VPN using IKEv1 and IPsec site-to-site VPN using IKEv1 or IKEv2:<br>Base license and Security Plus license: 250 sessions. |

| Model | License Requirement[1] |
|---|---|
| ASA 5515-X | • IPsec remote access VPN using IKEv2 (use one of the following):<br>– AnyConnect Premium license:<br>Base license: 2 sessions.<br>*Optional permanent or time-based licenses: 10, 25, 50, 100, or 250 sessions.*<br>*Optional Shared licenses[2]: Participant or Server. For the Server license, 500-50,000 in increments of 500 and 50,000-545,000 in increments of 1000.*<br>– AnyConnect Essentials license[3]: 250 sessions.<br>• IPsec remote access VPN using IKEv1 and IPsec site-to-site VPN using IKEv1 or IKEv2:<br>Base license: 250 sessions. |
| ASA 5525-X | • IPsec remote access VPN using IKEv2 (use one of the following):<br>– AnyConnect Premium license:<br>Base license: 2 sessions.<br>*Optional permanent or time-based licenses: 10, 25, 50, 100, 250, 500, or 750 sessions.*<br>*Optional Shared licenses[2]: Participant or Server. For the Server license, 500-50,000 in increments of 500 and 50,000-545,000 in increments of 1000.*<br>– AnyConnect Essentials license[3]: 750 sessions.<br>• IPsec remote access VPN using IKEv1 and IPsec site-to-site VPN using IKEv1 or IKEv2:<br>Base license: 750 sessions. |
| ASA 5545-X | • IPsec remote access VPN using IKEv2 (use one of the following):<br>– AnyConnect Premium license:<br>Base license: 2 sessions.<br>*Optional permanent or time-based licenses: 10, 25, 50, 100, 250, 500, 750, 1000, or 2500 sessions.*<br>*Optional Shared licenses[2]: Participant or Server. For the Server license, 500-50,000 in increments of 500 and 50,000-545,000 in increments of 1000.*<br>– AnyConnect Essentials license[3]: 2500 sessions.<br>• IPsec remote access VPN using IKEv1 and IPsec site-to-site VPN using IKEv1 or IKEv2:<br>Base license: 2500 sessions. |
| ASA 5555-X | • IPsec remote access VPN using IKEv2 (use one of the following):<br>– AnyConnect Premium license:<br>Base license: 2 sessions.<br>*Optional permanent or time-based licenses: 10, 25, 50, 100, 250, 500, 750, 1000, 2500, or 5000 sessions.*<br>*Optional Shared licenses[2]: Participant or Server. For the Server license, 500-50,000 in increments of 500 and 50,000-545,000 in increments of 1000.*<br>– AnyConnect Essentials license[3]: 5000 sessions.<br>• IPsec remote access VPN using IKEv1 and IPsec site-to-site VPN using IKEv1 or IKEv2:<br>Base license: 5000 sessions. |

| Model | License Requirement[1] |
|---|---|
| ASA 5585-X with SSP-10 | • IPsec remote access VPN using IKEv2 (use one of the following):<br>– AnyConnect Premium license:<br>Base license: 2 sessions.<br>*Optional permanent or time-based licenses: 10, 25, 50, 100, 250, 500, 750, 1000, 2500, or 5000 sessions.*<br>*Optional Shared licenses[2]: Participant or Server. For the Server license, 500-50,000 in increments of 500 and 50,000-545,000 in increments of 1000.*<br>– AnyConnect Essentials license[3]: 5000 sessions.<br>• IPsec remote access VPN using IKEv1 and IPsec site-to-site VPN using IKEv1 or IKEv2:<br>Base license: 5000 sessions. |
| ASA 5585-X with SSP-20, -40, and -60 | • IPsec remote access VPN using IKEv2 (use one of the following):<br>– AnyConnect Premium license:<br>Base license: 2 sessions.<br>*Optional permanent or time-based licenses: 10, 25, 50, 100, 250, 500, 750, 1000, 2500, 5000, or 10000 sessions.*<br>*Optional Shared licenses[2]: Participant or Server. For the Server license, 500-50,000 in increments of 500 and 50,000-545,000 in increments of 1000.*<br>– AnyConnect Essentials license[3]: 10000 sessions.<br>• IPsec remote access VPN using IKEv1 and IPsec site-to-site VPN using IKEv1 or IKEv2:<br>Base license: 10000 sessions. |
| ASASM | • IPsec remote access VPN using IKEv2 (use one of the following):<br>– AnyConnect Premium license:<br>Base license: 2 sessions.<br>*Optional permanent or time-based licenses: 10, 25, 50, 100, 250, 500, 750, 1000, 2500, 5000, or 10000 sessions.*<br>*Optional Shared licenses[2]: Participant or Server. For the Server license, 500-50,000 in increments of 500 and 50,000-545,000 in increments of 1000.*<br>– AnyConnect Essentials license[3]: 10000 sessions.<br>• IPsec remote access VPN using IKEv1 and IPsec site-to-site VPN using IKEv1 or IKEv2:<br>Base license: 10000 sessions. |

| Model | License Requirement[1] |
|---|---|
| ASAv with 1 Virtual CPU | • IPsec remote access VPN using IKEv2:<br>– Standard license: 2 sessions.<br>– Premium license: 250 sessions.<br>• IPsec remote access VPN using IKEv1 and IPsec site-to-site VPN using IKEv1 or IKEv2:<br>Standard and Premium licenses: 250 sessions. |
| ASAv with 4 Virtual CPUs | • IPsec remote access VPN using IKEv2:<br>– Standard license: 2 sessions.<br>– Premium license: 750 sessions.<br>• IPsec remote access VPN using IKEv1 and IPsec site-to-site VPN using IKEv1 or IKEv2:<br>Standard and Premium licenses: 750 sessions. |

1. The maximum combined VPN sessions of *all* types cannot exceed the maximum sessions shown in this table. For the ASA 5505, the maximum combined sessions is 10 for the Base license, and 25 for the Security Plus license.
2. A shared license lets the ASA act as a shared license server for multiple client ASAs. The shared license pool is large, but the maximum number of sessions used by each individual ASA cannot exceed the maximum number listed for permanent licenses.
3. The AnyConnect Essentials license enables AnyConnect VPN client access to the ASA. This license does not support browser-based SSL VPN access or Cisco Secure Desktop. For these features, activate an AnyConnect Premium license instead of the AnyConnect Essentials license.

   **Note**: With the AnyConnect Essentials license, VPN users can use a Web browser to log in, and download and start (WebLaunch) the AnyConnect client.

   The AnyConnect client software offers the same set of client features, whether it is enabled by this license or an AnyConnect Premium SSL VPN Edition license.

   The AnyConnect Essentials license cannot be active at the same time as the following licenses on a given ASA: AnyConnect Premium license (all types) or the Advanced Endpoint Assessment license. You can, however, run AnyConnect Essentials and AnyConnect Premium licenses on different ASAs in the same network.

   By default, the ASA uses the AnyConnect Essentials license, but you can disable it to use other licenses by using the **webvpn**, and then the **no anyconnect-essentials** command.

   For a detailed list of the features supported by the AnyConnect Essentials license and AnyConnect Premium license, see *AnyConnect Secure Mobility Client Features, Licenses, and OSs*:

   http://www.cisco.com/en/US/products/ps10884/products_feature_guides_list.html

# Guidelines and Limitations

This section includes the guidelines and limitations for this feature.

### Context Mode Guidelines

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

### Firewall Mode Guidelines

Supported only in routed firewall mode. Transparent mode is not supported.

### Failover Guidelines

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

# Configuring Remote Access IPsec VPNs

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


- Configuring Interfaces, page 6-6
- Configuring ISAKMP Policy and Enabling ISAKMP on the Outside Interface, page 6-7
- Configuring an Address Pool, page 6-8
- Adding a User, page 6-8
- Creating an IKEv1 Transform Set or IKEv2 Proposal, page 6-9
- Defining a Tunnel Group, page 6-10
- Creating a Dynamic Crypto Map, page 6-11
- Creating a Crypto Map Entry to Use the Dynamic Crypto Map, page 6-12
- Saving the Security Appliance Configuration, page 6-13


## 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*}<br><br>**Example:**<br>hostname(config)# interface ethernet0<br>hostname(config-if)# | Enters interface configuration mode from global configuration mode. |
| **Step 1** | **ip address** *ip_address* [*mask*] [**standby** *ip_address*]<br><br>**Example:**<br>hostname(config)# interface ethernet0<br>hostname(config-if)#<br>hostname(config-if)# ip address<br>10.10.4.200 255.255.0.0 | Sets the IP address and subnet mask for the interface. |

| | Command | Purpose |
|---|---|---|
| **Step 2** | **nameif** *name*<br><br>**Example:**<br>hostname(config-if)# nameif outside<br>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<br><br>**Example:**<br>hostname(config-if)# no shutdown<br>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 commands:

| | Command | Purpose |
|---|---|---|
| **Step 1** | crypto ikev1 policy *priority*<br>authentication {crack \| pre-share \|<br>rsa-sig}<br><br>**Example:**<br>hostname(config)# **crypto ikev1 policy 1**<br>**authentication pre-share**<br>hostname(config)# | Specifies the authentication method and the set of parameters to use during IKEv1 negotiation.<br><br>*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.<br><br>In this example and the steps that follow, we set the priority to 1. |
| **Step 2** | **crypto ikev1** policy *priority* encryption<br>{aes \| aes-192 \| aes-256 \| des \| 3des}<br><br>**Example:**<br>hostname(config)# **crypto ikev1 policy 1**<br>**encryption 3des**<br>hostname(config)# | Specifies the encryption method to use within an IKE policy. |
| **Step 3** | **crypto ikev1** policy *priority* hash {md5 \|<br>sha}<br><br>**Example:**<br>hostname(config)# **crypto ikev1 policy 1**<br>**hash sha**<br>hostname(config)# | Specifies the hash algorithm for an IKE policy (also called the HMAC variant). |
| **Step 4** | **crypto ikev1** policy *priority* group<br>{1 \| 2 \| 5}<br><br>**Example:**<br>hostname(config)# **crypto ikev1 policy 1**<br>**group 2**<br>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. |

| | Command | Purpose |
|---|---|---|
| **Step 5** | **crypto ikev1** policy *priority* lifetime {*seconds*}<br><br>**Example:**<br>hostname(config)# **crypto ikev1 policy 1 lifetime 43200**<br>hostname(config)# | Specifies the encryption key lifetime—the number of seconds each security association should exist before expiring.<br><br>The range for a finite lifetime is 120 to 2147483647 seconds. Use 0 seconds for an infinite lifetime. |
| **Step 6** | **crypto ikev1** enable *interface-name*<br><br>**Example:**<br>hostname(config)# **crypto ikev1** enable outside<br>hostname(config)# | Enables ISAKMP on the interface named *outside*. |
| **Step 7** | write memory<br><br>**Example:**<br>hostname(config-if)# write memory<br>Building configuration...<br>Cryptochecksum: 0f80bf71 1623a231 63f27ccf 8700ca6d<br><br>11679 bytes copied in 3.390 secs (3893 bytes/sec)<br>[OK]<br>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*]<br><br>**Example:**<br>hostname(config)# **ip local pool testpool 192.168.0.10-192.168.0.15**<br>hostname(config)# | Creates an address pool with a range of IP addresses, from which the ASA assigns addresses to the clients.<br><br>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*]<br><br>**Example:**<br>hostname(config)# **username testuser password 12345678**<br>hostname(config)# | Creates a user, password, and privilege level. |

# Creating an IKEv1 Transform Set or IKEv2 Proposal

This section shows how to configure a transform set (IKEv1) or proposal (IKEv2), which combines an encryption method and an authentication method.

Perform the following task:

| Command | Purpose |
|---|---|
| To configure an IKEv1 transform set:<br>`crypto ipsec ikev1 transform-set` *transform-set-name encryption-method* [*authentication*]<br><br>**Example:**<br>`hostname(config)# crypto ipsec transform set FirstSet esp-3des esp-md5-hmac`<br>`hostname(config)#` | Configures an IKEv1 transform set that specifies the IPsec IKEv1 encryption and hash algorithms to be used to ensure data integrity.<br>Use one of the following values for *encryption*:<br>• **esp-aes** to use AES with a 128-bit key.<br>• **esp-aes-192** to use AES with a 192-bit key.<br>• **esp-aes-256** to use AES with a 256-bit key.<br>• **esp-des** to use 56-bit DES-CBC.<br>• **esp-3des** to use triple DES algorithm.<br>• **esp-null** to not use encryption.<br>Use one of the following values for *authentication*:<br>• **esp-md5-hmac** to use the MD5/HMAC-128 as the hash algorithm.<br>• **esp-sha-hmac** to use the SHA/HMAC-160 as the hash algorithm.<br>• **esp-none** to not use HMAC authentication. |
| To configure an IKEv2 proposal:<br>**crypto ipsec ikev2 ipsec-proposal** *proposal_name*<br><br>Then:<br>**protocol** {**esp**} {**encryption** {**des** \| **3des** \| **aes** \| **aes-192** \| **aes-256** \| **null**} \| **integrity** {**md5** \| **sha-1**}<br><br>**Example:**<br>`hostname(config)# crypto ipsec ikev2 ipsec-proposal secure_proposal`<br>`hostname(config-ipsec-proposal)# protocol esp encryption des integrity md5` | Configures an IKEv2 proposal set that specifies the IPsec IKEv2 protocol, encryption, and integrity algorithms to be used.<br>**esp** specifies the Encapsulating Security Payload (ESP) IPsec protocol (currently the only supported protocol for IPsec).<br>Use one of the following values for *encryption*:<br>• **des** to use 56-bit DES-CBC encryption for ESP.<br>• **3des** (default) to use the triple DES encryption algorithm for ESP.<br>• **aes** to use AES with a 128-bit key encryption for ESP.<br>• **aes-192** to use AES with a 192-bit key encryption for ESP.<br>• **aes-256** to use AES with a 256-bit key encryption for ESP.<br>• **null** to not use encryption for ESP.<br>Use one of the following values for *integrity*:<br>• **md5** specifies the md5 algorithm for the ESP integrity protection.<br>• **sha-1** (default) specifies the Secure Hash Algorithm (SHA) SHA-1, defined in the U.S. Federal Information Processing Standard (FIPS), for ESP integrity protection. |

# 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 remote-access tunnel group, and DefaultL2Lgroup, which is the default 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.

Perform the following task:

**Detailed Steps**

| | Command | Purpose |
|---|---|---|
| **Step 1** | `tunnel-group` *name* `type` *type*<br><br>**Example:**<br>`hostname(config)#` **`tunnel-group testgroup type ipsec-ra`**<br>`hostname(config)#` | Creates an IPsec remote access tunnel-group (also called connection profile). |
| **Step 2** | **`tunnel-group`** *name* **`general-attributes`**<br><br>**Example:**<br>`hostname(config)# tunnel-group testgroup general-attributes`<br>`hostname(config-tunnel-general)#` | Enters tunnel group general attributes mode where you can enter an authentication method. |
| **Step 3** | **`address-pool`** `[(`*interface name*`)]`<br>**`address_pool1`** `[...address_pool6]`<br><br>**Example:**<br>`hostname(config-general)# address-pool testpool` | Specifies an address pool to use for the tunnel group. |
| **Step 4** | **`tunnel-group`** *name* **`ipsec-attributes`**<br><br>**Example:**<br>`hostname(config)# tunnel-group testgroup ipsec-attributes`<br>`hostname(config-tunnel-ipsec)#` | Enters tunnel group ipsec attributes mode where you can enter IPsec-specific attributes for IKEv1 connections. |
| **Step 5** | **`ikev1 pre-shared-key`** *key*<br><br>**Example:**<br>`hostname(config-tunnel-ipsec)#`<br>`pre-shared-key 44kkaol59636jnfx` | (Optional) Configures a pre-shared key (IKEv1 only). The key can be an alphanumeric string from 1-128 characters.<br>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.<br>**Note** Configure AAA authentication for IKEv2 using certificates in the tunnel group webvpn-attributes. |

# 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.

Perform the following task:

### Detailed Steps

| | Command | Purpose |
|---|---|---|
| **Step 1** | For IKEv1, use this command:<br>`crypto dynamic-map` *`dynamic-map-name seq-num`* `set ikev1 transform-set` *`transform-set-name`*<br><br>**Example:**<br>`hostname(config)# crypto dynamic-map dyn1 1 set ikev1 transform-set FirstSet`<br>`hostname(config)#`<br><br>For IKEv2, use this command:<br>`crypto dynamic-map` *`dynamic-map-name seq-num`* `set ikev2 ipsec-proposal` *`proposal-name`*<br><br>**Example:**<br>`hostname(config)# crypto dynamic-map dyn1 1 set ikev2 ipsec-proposal FirstSet`<br>`hostname(config)#` | Creates a dynamic crypto map and specifies an IKEv1 transform set or IKEv2 proposal for the map. |
| **Step 2** | **`crypto dynamic-map`** ***`dynamic-map-name dynamic-seq-num`*** **`set reverse-route`**<br><br>**Example:**<br>`hostname(config)# crypto dynamic-map dyn1 1 set reverse route`<br>`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."

Perform the following task:

**Detailed Steps**

| | Command | Purpose |
|---|---|---|
| **Step 1** | `crypto map map-name seq-num ipsec-isakmp dynamic dynamic-map-name`<br><br>**Example:**<br>`hostname(config)# crypto map mymap 1 ipsec-isakmp dynamic dyn1`<br>`hostname(config)#` | Creates a crypto map entry that uses a dynamic crypto map. |
| **Step 2** | **crypto map** *map-name* **interface** *interface-name*<br><br>**Example:**<br>`hostname(config)# crypto map mymap interface outside`<br>`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`<br><br>**Example:**<br>`hostname(config-if)# write memory`<br>`Building configuration...`<br>`Cryptochecksum: 0f80bf71 1623a231 63f27ccf 8700ca6d`<br><br>`11679 bytes copied in 3.390 secs (3893 bytes/sec)`<br>`[OK]`<br>`hostname(config-if)#` | Saves the changes to the configuration. |

# Configuration Examples for Remote Access IPsec VPNs

The following example shows how to configure a remote access IPsec/IKEv1 VPN:

```
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)# crypto ikev1 policy 1
hostname(config-ikev1-policy)# authentication pre-share
hostname(config-ikev1-policy)# encryption 3des
hostname(config-ikev1-policy)# hash sha
hostname(config-ikev1-policy)# group 2
hostname(config-ikev1-policy)# lifetime 43200
hostname(config)# crypto ikev1 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 ikev1 transform set FirstSet esp-3des esp-md5-hmac
hostname(config)# tunnel-group testgroup type remote-access
hostname(config)# tunnel-group testgroup general-attributes
hostname(config-general)# address-pool testpool
hostname(config)# tunnel-group testgroup ipsec-attributes
hostname(config-ipsec)# ikev1 pre-shared-key 44kkaol59636jnfx
hostname(config)# crypto dynamic-map dyn1 1 set ikev1 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
```

The following example shows how to configure a remote access IPsec/IKEv2 VPN:

```
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)# crypto ikev2 policy 1
hostname(config-ikev2-policy)# group 2
hostname(config-ikev2-policy)# integrity sha
hostname(config-ikev2-policy)# lifetime 43200
hostname(config-ikev2-policy)# prf sha
hostname(config)# crypto ikev2 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 ikev2 ipsec-proposal FirstSet
hostname(config-ipsec-proposal)# protocol esp encryption 3des aes
hostname(config)# tunnel-group testgroup type remote-access
hostname(config)# tunnel-group testgroup general-attributes
hostname(config-general)# address-pool testpool
hostname(config)# tunnel-group testgroup webvpn-attributes
hostname(config-webvpn)# authentication aaa certificate
hostname(config)# crypto dynamic-map dyn1 1 set ikev2 ipsec-proposal 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 VPNs

Table 6-1 lists the release history for this feature.

***Table 6-1 Feature History for Feature-1***

| Feature Name | Releases | Feature Information |
|---|---|---|
| Remote access VPNs for IPsec IKEv1 and SSL. | 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. |
| Remote access VPNs for IPsec IKEv2 | 8.4(1) | Added IPsec IKEv2 support for the AnyConnect Secure Mobility Client. |