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, page 69-1
- Licensing Requirements for Remote Access IPsec VPNs, page 69-2
- Guidelines and Limitations, page 69-6
- Configuring Remote Access IPsec VPNs, page 69-7
- Configuration Examples for Remote Access IPsec VPNs, page 69-14
- Feature History for Remote Access VPNs, page 69-15

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 the “Creating an IKEv1 Transform Set” section on page 73-5 in Chapter 73, “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:

### Note

This feature is not available on No Payload Encryption models.

<table>
<thead>
<tr>
<th>Model</th>
<th>License Requirement¹</th>
</tr>
</thead>
</table>
| ASA 5505 | - IPSec remote access VPN using IKEv2 (use one of the following):  
  - AnyConnect Premium license:  
    - Base license and Security Plus license: 2 sessions.  
    - *Optional permanent or time-based licenses: 10 or 25 sessions.*  
    - *Shared licenses are not supported.*²  
    - AnyConnect Essentials license³: 25 sessions.  
  - IPSec remote access VPN using IKEv1 and IPSec site-to-site VPN using IKEv1 or IKEv2:  
    - Base license: 10 sessions.  
    - Security Plus license: 25 sessions. |
| ASA 5510 | - IPSec remote access VPN using IKEv2 (use one of the following):  
  - AnyConnect Premium license:  
    - Base and Security Plus license: 2 sessions.  
    - *Optional permanent or time-based licenses: 10, 25, 50, 100, or 250 sessions.*  
    - *Optional Shared licenses²: Participant or Server. For the Server license, 500-50,000 in increments of 500 and 50,000-545,000 in increments of 1000.*  
    - AnyConnect Essentials license³: 250 sessions.  
  - IPSec remote access VPN using IKEv1 and IPSec site-to-site VPN using IKEv1 or IKEv2:  
    - Base license and Security Plus license: 250 sessions. |
### Licensing Requirements for Remote Access IPsec VPNs

<table>
<thead>
<tr>
<th>Model</th>
<th>License Requirement</th>
</tr>
</thead>
</table>
| ASA 5520 | • IPsec remote access VPN using IKEv2 (use one of the following):  
|         |   – AnyConnect Premium license:  
|         |     Base license: 2 sessions.  
|         |     *Optional permanent or time-based licenses: 10, 25, 50, 100, 250, 500, or 750 sessions.*  
|         |     *Optional Shared licenses*:  
|         |     Participant or Server. For the Server license, 500-50,000 in increments of 500 and 50,000-545,000 in increments of 1000.  
|         |   – AnyConnect Essentials license: 750 sessions.  
|         | • IPsec remote access VPN using IKEv1 and IPsec site-to-site VPN using IKEv1 or IKEv2:  
|         |     Base license: 750 sessions.  
| ASA 5540 | • IPsec remote access VPN using IKEv2 (use one of the following):  
|         |   – AnyConnect Premium license:  
|         |     Base license: 2 sessions.  
|         |     *Optional permanent or time-based licenses: 10, 25, 50, 100, 250, 500, 750, 1000, or 2500 sessions.*  
|         |     *Optional Shared licenses*:  
|         |     Participant or Server. For the Server license, 500-50,000 in increments of 500 and 50,000-545,000 in increments of 1000.  
|         |   – AnyConnect Essentials license: 2500 sessions.  
|         | • IPsec remote access VPN using IKEv1 and IPsec site-to-site VPN using IKEv1 or IKEv2:  
|         |     Base license: 2500 sessions.  
| ASA 5550 | • IPsec remote access VPN using IKEv2 (use one of the following):  
|         |   – AnyConnect Premium license:  
|         |     Base license: 2 sessions.  
|         |     *Optional permanent or time-based licenses: 10, 25, 50, 100, 250, 500, 750, 1000, 2500, or 5000 sessions.*  
|         |     *Optional Shared licenses*:  
|         |     Participant or Server. For the Server license, 500-50,000 in increments of 500 and 50,000-545,000 in increments of 1000.  
|         |   – AnyConnect Essentials license: 5000 sessions.  
|         | • IPsec remote access VPN using IKEv1 and IPsec site-to-site VPN using IKEv1 or IKEv2:  
|         |     Base license: 5000 sessions.  

---

### Licensing Requirements for Remote Access IPsec VPNs

<table>
<thead>
<tr>
<th>Model</th>
<th>License Requirement¹</th>
</tr>
</thead>
</table>
| ASA 5580  | • IPsec remote access VPN using IKEv2 (use one of the following):  
|           |   – AnyConnect Premium license:  
|           |     Base license: 2 sessions.  
|           |     *Optional permanent or time-based licenses: 10, 25, 50, 100, 250, 500, 750, 1000, 2500, 5000, or 10000 sessions.*  
|           |     *Optional Shared licenses²: Participant or Server. For the Server license, 500-50,000 in increments of 500 and 50,000-545,000 in increments of 1000.*  
|           |   – AnyConnect Essentials license³: 10000 sessions.
|           | • IPsec remote access VPN using IKEv1 and IPsec site-to-site VPN using IKEv1 or IKEv2:  
|           |     Base license: 10000 sessions. |
| ASA 5512-X| • IPsec remote access VPN using IKEv2 (use one of the following):  
|           |   – AnyConnect Premium license:  
|           |     Base license: 2 sessions.  
|           |     *Optional permanent or time-based licenses: 10, 25, 50, 100, or 250 sessions.*  
|           |     *Optional Shared licenses²: Participant or Server. For the Server license, 500-50,000 in increments of 500 and 50,000-545,000 in increments of 1000.*  
|           |   – AnyConnect Essentials license³: 250 sessions.
|           | • IPsec remote access VPN using IKEv1 and IPsec site-to-site VPN using IKEv1 or IKEv2:  
|           |     Base license: 250 sessions. |
| ASA 5515-X| • IPsec remote access VPN using IKEv2 (use one of the following):  
|           |   – AnyConnect Premium license:  
|           |     Base license: 2 sessions.  
|           |     *Optional permanent or time-based licenses: 10, 25, 50, 100, or 250 sessions.*  
|           |     *Optional Shared licenses²: Participant or Server. For the Server license, 500-50,000 in increments of 500 and 50,000-545,000 in increments of 1000.*  
|           |   – AnyConnect Essentials license³: 250 sessions.
|           | • IPsec remote access VPN using IKEv1 and IPsec site-to-site VPN using IKEv1 or IKEv2:  
|           |     Base license: 250 sessions. |
| ASA 5525-X| • IPsec remote access VPN using IKEv2 (use one of the following):  
|           |   – AnyConnect Premium license:  
|           |     Base license: 2 sessions.  
|           |     *Optional permanent or time-based licenses: 10, 25, 50, 100, 250, 500, or 750 sessions.*  
|           |     *Optional Shared licenses²: Participant or Server. For the Server license, 500-50,000 in increments of 500 and 50,000-545,000 in increments of 1000.*  
|           |   – AnyConnect Essentials license³: 750 sessions.
|           | • IPsec remote access VPN using IKEv1 and IPsec site-to-site VPN using IKEv1 or IKEv2:  
<p>|           |     Base license: 750 sessions. |</p>
<table>
<thead>
<tr>
<th>Model</th>
<th>License Requirement¹</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASA 5545-X</td>
<td>• IPsec remote access VPN using IKEv2 (use one of the following):</td>
</tr>
<tr>
<td></td>
<td>– AnyConnect Premium license:</td>
</tr>
<tr>
<td></td>
<td>Base license: 2 sessions.</td>
</tr>
<tr>
<td></td>
<td>Optional permanent or time-based licenses: 10, 25, 50, 100, 250, 500, 750, 1000, or 2500 sessions.</td>
</tr>
<tr>
<td></td>
<td>Optional Shared licenses²: Participant or Server. For the Server license, 500-50,000 in increments of 500 and 50,000-545,000 in increments of 1000.</td>
</tr>
<tr>
<td></td>
<td>– AnyConnect Essentials license³: 2500 sessions.</td>
</tr>
<tr>
<td></td>
<td>• IPsec remote access VPN using IKEv1 and IPsec site-to-site VPN using IKEv1 or IKEv2:</td>
</tr>
<tr>
<td></td>
<td>Base license: 2500 sessions.</td>
</tr>
<tr>
<td>ASA 5555-X</td>
<td>• IPsec remote access VPN using IKEv2 (use one of the following):</td>
</tr>
<tr>
<td></td>
<td>– AnyConnect Premium license:</td>
</tr>
<tr>
<td></td>
<td>Base license: 2 sessions.</td>
</tr>
<tr>
<td></td>
<td>Optional permanent or time-based licenses: 10, 25, 50, 100, 250, 500, 750, 1000, 2500, or 5000 sessions.</td>
</tr>
<tr>
<td></td>
<td>Optional Shared licenses²: Participant or Server. For the Server license, 500-50,000 in increments of 500 and 50,000-545,000 in increments of 1000.</td>
</tr>
<tr>
<td></td>
<td>– AnyConnect Essentials license³: 5000 sessions.</td>
</tr>
<tr>
<td>ASA 5585-X with SSP-10</td>
<td>• IPsec remote access VPN using IKEv2 (use one of the following):</td>
</tr>
<tr>
<td></td>
<td>– AnyConnect Premium license:</td>
</tr>
<tr>
<td></td>
<td>Base license: 2 sessions.</td>
</tr>
<tr>
<td></td>
<td>Optional permanent or time-based licenses: 10, 25, 50, 100, 250, 500, 750, 1000, 2500, or 5000 sessions.</td>
</tr>
<tr>
<td></td>
<td>Optional Shared licenses²: Participant or Server. For the Server license, 500-50,000 in increments of 500 and 50,000-545,000 in increments of 1000.</td>
</tr>
<tr>
<td></td>
<td>– AnyConnect Essentials license³: 5000 sessions.</td>
</tr>
<tr>
<td></td>
<td>• IPsec remote access VPN using IKEv1 and IPsec site-to-site VPN using IKEv1 or IKEv2:</td>
</tr>
<tr>
<td></td>
<td>Base license: 5000 sessions.</td>
</tr>
</tbody>
</table>
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.
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 69-7
- Configuring ISAKMP Policy and Enabling ISAKMP on the Outside Interface, page 69-8
- Configuring an Address Pool, page 69-9
- Adding a User, page 69-9
- Creating an IKEv1 Transform Set or IKEv2 Proposal, page 69-10
- Defining a Tunnel Group, page 69-11
- Creating a Dynamic Crypto Map, page 69-12
- Creating a Crypto Map Entry to Use the Dynamic Crypto Map, page 69-13
- Saving the Security Appliance Configuration, page 69-14

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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> interface {interface}</td>
<td>Enters interface configuration mode from global configuration mode.</td>
</tr>
<tr>
<td>Example: hostname(config)# interface ethernet0 hostname(config-if)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 1</strong> ip address ip_address [mask] [standby ip_address]</td>
<td>Sets the IP address and subnet mask for the interface.</td>
</tr>
<tr>
<td>Example: hostname(config)# interface ethernet0 hostname(config-if)# hostname(config-if)# ip address 10.10.4.200 255.255.0.0</td>
<td></td>
</tr>
</tbody>
</table>
## 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.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong></td>
<td><code>nameif name</code></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>hostname(config-if)# nameif outside</code></td>
</tr>
<tr>
<td>Specifies a name for the interface (maximum of 48 characters). You cannot change this name after you set it.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>shutdown</code></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>hostname(config-if)# no shutdown</code></td>
</tr>
<tr>
<td>Enables the interface. By default, interfaces are disabled.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>`crypto ikev1 policy priority authentication {crack</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>hostname(config)# crypto ikev1 policy 1 authentication pre-share</code></td>
</tr>
<tr>
<td>Specifies the authentication method and the set of parameters to use during IKEv1 negotiation. <strong>Priority</strong> 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.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>`crypto ikev1 policy priority encryption {aes</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>hostname(config)# crypto ikev1 policy 1 encryption 3des</code></td>
</tr>
<tr>
<td>Specifies the encryption method to use within an IKE policy.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>`crypto ikev1 policy priority hash {md5</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>hostname(config)# crypto ikev1 policy 1 hash sha</code></td>
</tr>
<tr>
<td>Specifies the hash algorithm for an IKE policy (also called the HMAC variant).</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>`crypto ikev1 policy priority group {1</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>hostname(config)# crypto ikev1 policy 1 group 2</code></td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>
Configuring Remote Access IPsec VPNs

Chapter 69      Configuring Remote Access IPsec VPNs

Configuring Remote Access IPsec VPNs

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.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip local pool poolname first-address-last-address [mask mask]</td>
<td>Creates an address pool with a range of IP addresses, from which the ASA assigns addresses to the clients.</td>
</tr>
<tr>
<td>Example: hostname(config)# ip local pool testpool 192.168.0.10-192.168.0.15 hostname(config)#</td>
<td></td>
</tr>
</tbody>
</table>

Adding a User

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

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>username name {nopassword</td>
<td>password password [mschap</td>
</tr>
</tbody>
</table>

Example:
hostname(config)# username testuser password 12345678
hostname(config)#
### Command Purpose

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| To configure an IKEv1 transform set:  
crypto ipsec ikev1 transform-set  
transform-set-name encryption-method  
[authentication] | Configures an IKEv1 transform set that specifies the IPsec IKEv1 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. |
| Example:  
hostname(config)# crypto ipsec transform set  
FirstSet esp-3des esp-md5-hmac  
hostname(config)# | |

| To configure an IKEv2 proposal:  
crypto ipsec ikev2 ipsec-proposal  
proposal_name | Configures an IKEv2 proposal set that specifies the IPsec IKEv2 protocol, encryption, and integrity algorithms to be used.  
esp specifies the Encapsulating Security Payload (ESP) IPsec protocol (currently the only supported protocol for IPsec).  
Use one of the following values for encryption:  
- des to use 56-bit DES-CBC encryption for ESP.  
- 3des (default) to use the triple DES encryption algorithm for ESP.  
- aes to use AES with a 128-bit key encryption for ESP.  
- aes-192 to use AES with a 192-bit key encryption for ESP.  
- aes-256 to use AES with a 256-bit key encryption for ESP.  
- null to not use encryption for ESP.  
Use one of the following values for integrity:  
- md5 specifies the md5 algorithm for the ESP integrity protection.  
- 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.  
Example:  
hostname(config)# crypto ipsec ikev2  
ipsec-proposal secure_proposal  
hostname(config-ipsec-proposal)# protocol  
esp encryption des integrity md5 | |

---

### 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.
Chapter 69      Configuring Remote Access IPsec VPNs

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.

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

Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>tunnel-group name type type</strong>&lt;br&gt;Example: hostname(config)# tunnel-group testgroup type ipsec-ra hostname(config)#</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>tunnel-group name general-attributes</strong>&lt;br&gt;Example: hostname(config)# tunnel-group testgroup general-attributes hostname(config-tunnel-general)#</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>address-pool ([interface name]) address_pool1 [...address_pool6]</strong>&lt;br&gt;Example: hostname(config-general)# address-pool testpool</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>tunnel-group name ipsec-attributes</strong>&lt;br&gt;Example: hostname(config)# tunnel-group testgroup ipsec-attributes hostname(config-tunnel-ipsec)#</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>ikev1 pre-shared-key key</strong>&lt;br&gt;Example: hostname(config-tunnel-ipsec)# pre-shared-key 44kkaol59636jnf</td>
</tr>
</tbody>
</table>

**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.

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

Detailed Steps

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Creates a dynamic crypto map and specifies an IKEv1 transform set or IKEv2 proposal for the map.</td>
</tr>
</tbody>
</table>
| crypto dynamic-map dynamic-map-name seq-num set ikev1 transform-set transform-set-name | For IKEv1, use this command:  
Example:  
hostname(config)# crypto dynamic-map dyn1 1 set ikev1 transform-set FirstSet  
hostname(config)# |
| crypto dynamic-map dynamic-map-name seq-num set ikev2 ipsec-proposal proposal-name | For IKEv2, use this command:  
Example:  
hostname(config)# crypto dynamic-map dyn1 1 set ikev2 ipsec-proposal FirstSet  
hostname(config)# |
| **Step 2** | (Optional) Enables Reverse Route Injection for any connection based on this crypto map entry. |
| 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)# |

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>crypto map map-name seq-num ipsec-isakmp dynamic dynamic-map-name</td>
<td>Creates a crypto map entry that uses a dynamic crypto map.</td>
</tr>
<tr>
<td></td>
<td>Example: hostname(config)# crypto map mymap 1 ipsec-isakmp dynamic dyn1 hostname(config)#</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>crypto map map-name interface interface-name</td>
<td>Applies the crypto map to the outside interface.</td>
</tr>
<tr>
<td></td>
<td>Example: hostname(config)# crypto map mymap interface outside hostname(config)#</td>
<td></td>
</tr>
</tbody>
</table>

### Saving the Security Appliance Configuration

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>write memory</td>
<td>Saves the changes to the configuration.</td>
</tr>
</tbody>
</table>

**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)#
```

### 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 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 ikev1 transform-set FirstSet esp-3des esp-md5-hmac
hostname(config)# tunnel-group testgroup type remote-access
tunnel-group testgroup general-attributes
hostname(config)# crypto ipsec attributes
hostname(config)# ikev1 pre-shared-key 44kkaol596jnfx
tunnel-group testgroup type remote-access
tunnel-group testgroup ipsec-attributes
hostname(config)# crypto dynamic-map dyn1 1 set ikev1 transform-set FirstSet
hostname(config)# crypto dynamic-map dyn1 1 set reverse-route
tunnel-group testgroup ipsec-attributes
hostname(config)# crypto map mymap 1 ipsec-isakmp dynamic dyn1
tunnel-group testgroup general-attributes
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
tunnel-group testgroup general-attributes
hostname(config)# crypto ipsec attributes
hostname(config)# ikev2 policy 1
tunnel-group testgroup general-attributes
hostname(config)# crypto ikev2 policy 1
tunnel-group testgroup general-attributes
hostname(config)# crypto ikev2 policy 1
hostname(config)# crypto ikev2 outside
hostname(config)# crypto ipsec ikev2 ipsec-proposal FirstSet
tunnel-group testgroup general-attributes
hostname(config)# crypto ipsec ikev2 ipsec-proposal FirstSet
tunnel-group testgroup webvpn-attributes
hostname(config)# tunnel-group testgroup type remote-access
tunnel-group testgroup general-attributes
hostname(config)# crypto dynamic-map dyn1 1 set ikev2 ipsec-proposal FirstSet
tunnel-group testgroup webvpn-attributes
hostname(config)# crypto dynamic-map dyn1 1 set reverse-route
tunnel-group testgroup webvpn-attributes
hostname(config)# crypto map mymap 1 ipsec-isakmp dynamic dyn1
tunnel-group testgroup general-attributes
hostname(config)# crypto map mymap interface outside
hostname(config)# write memory

Feature History for Remote Access VPNs

Table 69-1 lists the release history for this feature.

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote access VPNs for IPsec IKEv1 and SSL.</td>
<td>7.0</td>
<td>Remote access VPNs allow users to connect to a central site through a secure connection over a TCP/IP network such as the Internet.</td>
</tr>
<tr>
<td>Remote access VPNs for IPsec IKEv2</td>
<td>8.4(1)</td>
<td>Added IPsec IKEv2 support for the AnyConnect Secure Mobility Client.</td>
</tr>
</tbody>
</table>