CHAPTER 9

Mobile IP Security

All registration messages between a mobile node and home agent are required to contain the Mobile-Home Authentication Extension (MHAE).

The integrity of the registration messages is protected by a shared 128-bit key between a mobile node and home agent. The keyed message digest algorithm 5 (MD5) in “prefix+suffix” mode is used to compute the authenticator value in the appended MHAE. Mobile IP also supports the hash-based message authentication code (HMAC-MD5). The receiver compares the authenticator value it computes over the message with the value in the extension to verify the authenticity.

Optionally, the Mobile-Foreign Authentication Extension and Foreign-Home Authentication Extension are appended to protect message exchanges between a mobile node and foreign agent and between a foreign agent and home agent, respectively.

Replay protection uses the identification field in the registration messages as a time stamp and sequence number. The home agent returns its time stamp to synchronize the mobile node for registration.

The Cisco IOS software allows the mobility keys to be stored on an authentication, authorization, and accounting (AAA) server that can be accessed using Terminal Access Controller Access Control System Plus (TACACS+) or Remote Authentication Dial-In User Service (RADIUS) protocols. You can restrict who is allowed to register by using registration filters.

For more information on security in a Mobile IP environment, refer to the “Configuring Mobile IP” chapter of the Cisco IOS IP Configuration Guide, Release 12.2.

AAA in the Mobile IP Environment

To configure AAA in the Mobile IP environment, use the following commands in global configuration mode:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Router(config)# aaa new-model</td>
<td>Enables the AAA access control model.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Router(config)# aaa authorization ipmobile (tacacs+</td>
<td>Authorizes Mobile IP to retrieve security associations from the AAA server using TACACS+ or RADIUS.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>radius)</td>
</tr>
</tbody>
</table>
Configuring RADIUS in the Mobile IP Environment

RADIUS is a method for defining the exchange of AAA information in the network. In the Cisco implementation, RADIUS clients run on Cisco routers and send authentication requests to a RADIUS server that contains all user authentication and network server access information. For detailed information about RADIUS configuration options, refer to the “Configuring RADIUS” chapter in the Cisco IOS Security Configuration Guide.

To configure RADIUS in the Mobile IP environment, use the following commands in global configuration mode:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1: <code>radius-server host</code></td>
<td>Specifies a RADIUS server host.</td>
</tr>
<tr>
<td>Step 2: <code>radius-server key</code></td>
<td>Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.</td>
</tr>
</tbody>
</table>

Configuring TACACS+ in the Mobile IP Environment

Terminal Access Controller Access Control System Plus (TACACS+) is an authentication protocol that provides remote access authentication and related services, such as event logging. For detailed information about TACACS+ configuration options, refer to the “Configuring TACACS+” chapter in the Cisco IOS Security Configuration Guide.

To configure TACACS+ in the Mobile IP environment, use the following commands in global configuration mode:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1: <code>tacacs-server host</code></td>
<td>Specifies a TACACS+ server host.</td>
</tr>
<tr>
<td>Step 2: <code>tacacs-server key</code></td>
<td>Sets the authentication encryption key used for all TACACS+ communications between the access server and the TACACS+ daemon.</td>
</tr>
</tbody>
</table>

Example of a AAA Server Configuration

In the following AAA server configuration, the home agent can use an AAA server for storing security associations. Mobile IP has been authorized using TACACS+ server to retrieve the security association information, which is used by the home agent to authenticate registrations. The user is the mobile node IP address. The syntax for the security association is `spi#num = string`, where `string` is the rest of the IP address. This format can be imported into a CiscoSecure server.

```bash
user = 20.0.0.1 {
    service = mobileip {
        set spi#0 = "spi 100 key hex 12345678123456781234567812345678"
    }
}
```
The following example shows how the home agent is configured to use the AAA server:

```plaintext
aaa new-model
aaa authorization ipmobile tacacs+
!
ip mobile home-agent
ip mobile network 20.0.0.0 255.0.0.0
ip mobile host 20.0.0.1 20.0.0.3 virtual-network 20.0.0.0 255.0.0.0 aaa
!
tacacs-server host 1.2.3.4
tacacs-server key cisco
```

**IPSec in the Mobile IP Environment**

Security associations establish trust between two devices in a peer-to-peer relationship. There are two types of security association. The first is Internet Key Exchange (IKE), which provides negotiation, peer authentication, key management, and key exchange. IKE provides a secure communication channel between two devices that is used to negotiate an encryption algorithm, a hash algorithm, an authentication method, and any relevant group information.

The second type of security association is called IPsec security association (IPsec SA). IPsec SA is unidirectional, thus requiring that separate IPsec SAs be established in each direction to provide non-repudiation, data integrity, and payload confidentiality. Non-repudiation is often necessary to verify that a transaction has taken place, such as a financial exchange between parties. Data integrity verifies that packets are not altered in transit by a third party. Payload confidentiality is provided by encryption.

It might be necessary to protect certain traffic on the mobile network. This is accomplished by enabling IPSec between the mobile access router and an IPSec gateway located behind the home agent. Since an IPSec tunnel is established within the Mobile IP tunnel, IKE renegotiation is unnecessary as the mobile access router moves about. The result is secure, scalable mobile networks based on standards.

The IPSec encryption algorithm that runs between the mobile access router and the IPSec gateway can either be Triple Data Encryption Standard (DES) or Advanced Encryption Standard (AES). Note that AES provides greater security than DES and is more efficient than 3DES.

**IPSec Interoperability**

IPSec sets up its peering between the egress interface of the encrypting router and any interface on the decrypting router. This relationship is hampered because the egress interface of a mobile access router changes based on available network connectivity. In addition, the egress interfaces might have non-routable IP addresses associated with them, which makes setting up an IPSec session impossible using the standard model.
To overcome the problems, all traffic must exit the same interface that will always be up and will always have a routable IP address. The method applied in this example is anchoring the IPsec session to the loopback interface on the mobile access router. The home address of the mobile access router should be configured on a loopback interface because loopback interfaces are software and are always up.

It is possible to forward traffic into a loopback interface. If the traffic is not destined for the IP address of the loopback, the traffic exits the interface and is looped back into the router. At this point, normal routing processes take delivery of the packet.

The only way to forward traffic out a loopback is with the `set interface` target of a `route map` command. All traffic from the mobile network that needs to be encrypted is sent by a route map out the loopback and back in to the router for normal delivery.

In summary, the loopback interface is always up and not affected by the movement of the mobile access router (in which the interface or point of attachment changes dynamically). This provides the invariant endpoint of the IPSec connection. Thus, the IPSec connection is always alive in conjunction with mobility.

**IPSec Gateway**

The IPSec gateway might be any Cisco router with IPSec software and an IPSec-capable image that corresponds to the mobile access router. The IPSec gateway is not required to have the Mobile IP feature set, because it is not providing mobility service. Since this router is acting as an IPSec traffic aggregator, it is recommended that you install hardware accelerator modules in the connected device for better performance. Ideally, the IPSec gateway router is a Cisco 7200 Series router with an ISA/VPN Acceleration Module (VAM) card, or a Catalyst 6500 switch with an American Contractors Exchange (ACE) card.

**Figure 9-1  IPSec Gateway Network Topology**

Figure 9-1 shows three types of nodes in the network topology: nodes on a mobile network, nodes on a secured network, and nodes on a public network. The mobile access router establishes an IPSec tunnel between it and the IPSec gateway to protect traffic to nodes on the secured network. Communications with nodes on the public network is not encrypted. The home agent and IPSec gateway must be deployed in the Demilitarized Zone (DMZ).

**Figure 9-2** shows how a mobile access router sets up an IPSec tunnel with the IPSec gateway by exchanging IKE messages, which traverse the Mobile IP tunnel. The IPSec tunnel is established when traffic flows between a node on the secured network and a node on a mobile network.
Data traffic can be categorized into either secure or public. Communications that must be protected are encrypted and wrapped in IPSec. Otherwise, packets are sent in the clear.

**IPSec Configuration**

This section contains configurations for the mobile access router, IPSec gateway, home agent, foreign agent, and mobile nodes in a specified network topology. Traffic is secured between the mobile access router network and networks in the home domain. The IPSec endpoints are the mobile access router and the IPSec Gateway located behind the home agent on the home network. The networks in the home domain in which protection is desired are placed behind the IPSec gateway.
Example of IPSec Mobile Network Configuration

The mobile access router has one Ethernet interface on the mobile network and two interfaces, serial and Ethernet, connected to a foreign agent. The foreign agent is providing Mobile IP service only on the Ethernet interface, not on the serial interface.

The serial interface is a roaming interface with static collocated care-of-address. The roaming Ethernet interface is used to detect foreign agents. The other Ethernet interface is for the LAN on the mobile access router. All nodes on the mobile network use the mobile access router as the default gateway.

Note

If the mobile access router has only one network interface, the mobile network and the roaming interface functions should be combined. If the mobile access router has multiple interfaces or VLANs, it should have a dedicated roaming interface and a mobile network interface.

The IPSec configuration must meet the following criteria:

- The mobile access router home address must be configured as a loopback address.
- On the inbound interface where the mobile access router networks are configured, a routemap must be applied to select the traffic to be encrypted (named SecureNetPolicy in the example configuration).
- The access control list must list the networks for which traffic must be encrypted. In the configuration example, the access control list is:

  access-list 155 permit ip 80.80.80.0 0.0.0.255 60.60.60.0 0.0.0.255

Since the source is 80.80.80.0/24, it corresponds to the mobile access router network connected on the Ethernet interface. The destination network is 60.60.60.0/24, which implies that all traffic towards 60.60.60.0/24 will be encrypted. Since communication with the network 60.60.60.0/24 is IPSec protected, this network is referred to as a protected network. All protected networks must be listed in the access control list. The last implicit entry in the access control list is deny ip any any. If the traffic does not match any of the previous entries and was not marked for encryption, the traffic is sent in clear.

Unprotected access is provided to all other (public) networks (those not listed the access control list with the permit clause). For example:

```plaintext
crypto isakmp policy 1
  hash md5
  authentication pre-share
  group 2
  crypto isakmp key 1234567890 address 200.200.200.1
  crypto isakmp peer address 200.200.200.1
  crypto IPsec transform-set testtrans esp-des
  !
crypto map ToSecureNet 10 IPsec-isakmp
  set peer 200.200.200.1
  set transform-set testtrans
  match address 155
  !
interface Loopback1
  ip address 65.1.1.1 255.255.255.255
  crypto map ToSecureNet
  !
interface Ethernet3/2
  ip address 10.10.10.1 255.255.255.0
  ip mobile router-service roam
```
interface Ethernet3/3
  ip address 80.80.80.4 255.255.255.0
  ip policy route-map SecureNetPolicy
!
interface Serial4/1
  ip address 50.50.50.1 255.255.255.0
  ip mobile router-service roam
  ip mobile router-service collocated gateway 50.50.50.2
!
router mobile
!
ip local policy route-map SecureNetPolicy
!
ip mobile secure home-agent 100.100.100.3 spi 100 key hex 112233445566778811234455667788
  algorithm md5 mode prefix-suffix
  ip mobile router
    address 65.1.1.1 255.0.0.0
    home-agent 100.100.100.3
    reverse-tunnel
!
access-list 155 permit ip 80.80.80.0 0.0.0.255 60.60.60.0 0.0.0.255
!
route-map SecureNetPolicy permit 10
  match ip address 155
  set interface Loopback1

Foreign Agent Example

To support mobile access router home domain network IPSec, no special configuration of the foreign agent is required. For example:

interface Serial1/2
  ip address 50.50.50.2 255.255.255.0
!
interface Ethernet3/1
  ip address 100.100.100.1 255.255.255.0
!
interface Ethernet3/3
  ip address 70.70.70.1 255.255.255.0
  ip irdp
  ip irdp maxadvertinterval 5
  ip irdp minadvertinterval 2
  ip irdp holdtime 15
  ip mobile foreign-service reverse-tunnel
!
router mobile
!
router rip
  redistribute mobile
    network 50.0.0.0
    network 70.0.0.0
    network 100.0.0.0
!
ip mobile foreign-agent care-of Ethernet3/1
Home Agent Example

Because the home agent does not participate in providing traffic protection, no special IPSec configuration is required at the home agent. The Mobile IP configurations are shown below:

```plaintext
interface Ethernet3/1
  ip address 100.100.100.3 255.255.255.0
!
interface Ethernet3/2
  ip address 200.200.200.2 255.255.255.0
!
interface Ethernet3/3
  ip address 150.150.150.2 255.255.255.0
!
routing mobile
!
routing rip
  redistribute mobile metric 1
  network 100.0.0.0
  network 150.150.150.0
  network 200.200.200.0
!
routing mobile home-agent
ip mobile virtual-network 65.0.0.0 255.0.0.0
ip mobile host 65.1.1.1 virtual-network 65.0.0.0 255.0.0.0
ip mobile mobile-networks 65.1.1.1
  description SecureTransport
  network 80.80.80.0 255.255.255.0
ip mobile secure host 65.1.1.1 spi 100 key hex 1123345678901234567890 algorithm
d5 mode prefix-suffix
  no ip mobile tunnel path-mtu-discovery
```

Node on Mobile Network Example

```plaintext
interface Ethernet3/3
  ip address 80.80.80.1 255.255.255.0
!
ip route 60.60.60.0 255.255.255.0 80.80.80.4
```

Node in Public Network Example

```plaintext
interface Ethernet1/1
  ip address 150.150.150.1 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 150.150.150.2
```

Node in Secure Network Example

```plaintext
interface Ethernet1/1
  ip address 60.60.60.1 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 60.60.60.60
```
Mobile Network Security Testing

From a node on the mobile network, you can ping a node in the protected network. You can ping from the protected network node to the mobile network node with same results. The first few packets might be dropped (due to ARP, IKE, or IPSec secure area setup). After the initial packet loss, ping should be successful.

IKE and IPSec security associations are established at mobile access router and IPSec Gateway. To see the IKE security association (SA) state, use the `show crypto` command. For example:

```
MobileRouter# show crypto isakmp sa
f_vrf/i_vrf   dst            src             state       conn-id slot
/           200.200.200.1   65.1.1.1      QM_IDLE 3 0
```

After the security area has been established, the state is typically QM_IDLE.

To see the IPSec secure area, use the `show crypto ipsec sa` command:

```
MobileRouter#show crypto ipsec sa
interface: Loopback1
    Crypto map tag: ToSecureNet, local addr. 65.1.1.1
protected vrf:
    local ident (addr/mask/prot/port): (80.80.80.0/255.255.255.0/0/0)
    remote ident (addr/mask/prot/port): (60.60.60.0/255.255.255.0/0/0)
    current_peer: 200.200.200.1:500
    PERMIT, flags={origin_is_acl,}
    #pkts encaps: 397876, #pkts encrypt: 397876, #pkts digest 0
    #pkts decaps: 397559, #pkts decrypt: 397559, #pkts verify 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 1, #recv errors 0
    local crypto endpt.: 65.1.1.1, remote crypto endpt.: 200.200.200.1
    path mtu 1514, media mtu 1514
    current outbound spi: 21E53ABF

    inbound esp sas:
    <snip>
```

Notice the `#pkts encaps` and `#pkts decaps` counters. To clear the counters, use the `clear crypto sa counters` command.

Ping from a mobile access router node to a node on the secured network (or vice versa), and look at the value of counters again. The counters should match the number of ping packets you sent.

Other methods for detecting the encryption activity:

- Use the `debug ip packet detail dump` command, and observe that the contents do not appear to be logical.
- Attach a sniffer (or Pagent device) between the mobile access router and the IPSec Gateway, and watch the packets on the wire.
- Measure the size of packets as seen by egress interfaces on the mobile access router, home agent and IPSec gateway.

To clear the IKE security associations, use the `clear crypto isakmp` command:

```
MobileRouter#clear crypto isakmp <0-32766>
```

where `<0-32766>` is the connection ID of the secure area.
To clear the IPSec security associations, use the `clear crypto sa` command:

```
MobileRouter# clear crypto sa [counters | map | peer | spi | vrf]
```

where:
- `counters` resets the secure area counters
- `map` clears all secure areas for a given crypto map
- `peer` clears all secure areas for a given crypto peer
- `spi` clears secure areas by SPI
- `vrf` clears VRF (Routing/Forwarding) instance

This command can also clear the packet counters, and it can be used for debugging.

**IPSec Commands**

**encryption Command**

Use the `encryption` command, a isakmp policy command, to establish IKE policy.

```
encryption {aes | aes 192 | aes 256}
```

Where:
- `aes` specifies 128-bit AES
- `aes 192` specifies 192-bit AES
- `aes 256` specifies 256-bit AES

View information about the configuration by using the `show crypto isakmp policy` EXEC command.

**crypto ipsec transform-set Command**

Use the `crypto ipsec transform-set` command to define IPSec security protocols and algorithms.

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

The accepted transform values are expanded. Under the category of Encapsulating Security Payload (ESP) Encryption Transform, one of the following can be chosen:

- `esp-aes` ESP with the 128-bit AES encryption algorithm
- `esp-aes192` ESP with the 192-bit AES encryption algorithm
- `esp-aes256` ESP with the 256-bit AES encryption algorithm
- `esp-des` ESP with the 56-bit Data Encryption Standard (DES) encryption algorithm
- `esp-3des` ESP with the 168-bit 3DES encryption algorithm
- `esp-null` null encryption algorithm

View information about the configuration by using the `show crypto ipsec transform-set` and `show crypto isakmp policy` EXEC commands.
Manual Certificate Enrollment

The TFTP and cut-and-paste (Manual Certificate Enrollment) generates a certificate request and accept certification authority (CA) certificates as well as the router certificates. These tasks are accomplished by using a TFTP server or manual cut-and-paste operations. Use TFTP or manual cut-and-paste enrollment in the following situations:

- The CA does not support Simple Certificate Enrollment Protocol (SCEP), the most commonly used method for sending and receiving requests and certificates.
- A network connection between the router and the CA is not possible.

Brief descriptions of some of the commands are provided in this section. A detailed explanation of the commands needed to configure Manual Certificate Enrollment can be found in the “Command Reference” section of Manual Certificate Enrollment (TFTP and Cut-and-Paste), and can be found at http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftmancrt.htm.

Manual Certificate Enrollment (TFTP and Cut-and-Paste) Prerequisites

TFTP and cut-and-paste enrollment has been added to the public key infrastructure (PKI) subsystem. The PKI subsystem requires the crypto subsystem.


You can switch between TFTP and cut-and-paste; for example, you can paste the CA certificate by using the enrollment terminal command, and then enter the no enrollment terminal and enrollment url tftp://certserver/file_specification commands to TFTP the requests and router certificates. However, Cisco does not recommend switching URLs if SCEP is used; that is, if the enrollment URL is “http://,” do not change the enrollment URL between fetching the CA certificate and enrolling the certificate.

Manual Certificate Enrollment Concepts

This section describes the TFTP Certificate Enrollment and Cut-and-Paste Certificate Enrollment concepts.

TFTP Certificate Enrollment

A user might enable TFTP certificate enrollment if his or her CA does not support SCEP, which is the most commonly used method for sending and receiving requests and certificates. This feature takes the existing enrollment ca-trustpoint configuration subcommand and enhances the url url option to support TFTP certificate enrollment—enrollment url tftp://certserver/file_specification.

This subcommand specifies that TFTP should be used to send the enrollment requests and to retrieve the certificate of the CA and the certificate of the router. The file_specification is optional. However, if the file_specification is included in the URL, the router appends an extension to the file specification.

When the crypto ca authenticate command is entered, the router retrieves the certificate of the CA from the specified TFTP server. As appropriate, the router appends the extension “.ca” to the filename or the fully qualified domain name (FQDN). (If the url url option does not include a file specification, the router FQDN is used.) For example, if a user enters enrollment url
Manual Certificate Enrollment

Chapter 9 Mobile IP Security

Cut-and-Paste Certificate Enrollment

A user might want to manually cut-and-paste certificate enrollment requests and certificates when he or she does not have a network connection between the router and CA. Cut-and-paste enrollment introduces a new ca-trustpoint configuration subcommand—enrollment. This command should be used when configuring the trustpoint CA. After entering the crypto ca enroll command, you are asked the same questions about the IP address and serial number as a TFTP enrollment. The base 64 encoded certificate request is displayed on the terminal.

Similar to the TFTP process, the user enters the crypto ca import command to enter the granted certificate. With cut-and-paste, the base 64 encoded certificate is accepted from the console terminal. Certificate input ends after the user enters “quit” on a line by itself.

How to Configure Manual Certificate Enrollment

To enable manual certificate enrollment via TFTP or cut-and-paste, you must configure a trustpoint CA and the relevant enrollment tasks. This section contains the following procedures:

- Configuring Certificate Enrollment by Using TFTP
- Configuring Certificate Enrollment by Using Cut-and-Paste
- Verifying Manual Certificate Enrollment

Configuring Certificate Enrollment by Using TFTP

To declare the trustpoint CA that your router should use and to configure that trustpoint CA for manual enrollment by using TFTP, use the commands described in this section.

- You must know the correct URL to use if you are configuring certificate enrollment by using TFTP.
- The router must be able to write a file to the TFTP server for the crypto ca enroll command. Some TFTP servers require that the file exist on the server before it can be written. Most TFTP servers require that the file be writeable by the world. This requirement might pose a risk because any router or other device can write or overwrite the certificate request; in such a case, the router would not be able to use the certificate after it is granted by the CA because the request has been modified.
### Command or Action | Purpose
---|---
**Step 1** | enable
Enables higher privilege levels, such as privileged EXEC mode. Enter your password if prompted.

**Step 2** | configure (terminal | memory | network)
Enters global configuration mode.

**Step 3** | crypto ca trustpoint name
Declares the CA that your router should use and enters ca-trustpoint configuration mode.

**Step 4** | enrollment [mode] [retry minutes] [retry number] [url url]
Specifies the enrollment parameters of your CA.
- *mode*—Specifies registration authority (RA) mode if your CA system provides a RA.
- *retry minutes*—Specifies the wait period between certificate request retries. The default is 1 minute between retries.
- *retry number*—Specifies the number of times that a router will resend a certificate request when it does not receive a response from the previous request. (Specify from 1 to 100 retries.)
- *url url*—Specifies the URL of the CA to which your router should send certificate requests.

  If you are using SCEP for enrollment, *url* must be in the form http://CA_name, where CA_name is the CA’s host Domain Name System (DNS) name or IP address.

  If you are using TFTP for enrollment, *url* must be in the form tftp://certserver/file_specification.

**Step 5** | crypto ca authenticate name
Takes the name of the CA as the argument.

**Step 6** | exit
Exits ca-trustpoint configuration mode and returns to global configuration.

**Step 7** | crypto ca enroll name
Obtains your router’s certificate(s) from the CA.

**Step 8** | crypto ca import name certificate
Imports a certificate by using TFTP or manual cut-and-paste at the terminal.

### Configuring Certificate Enrollment by Using Cut-and-Paste

To declare the trustpoint CA that your router should use and to configure that trustpoint CA for manual enrollment via cut-and-paste, use the commands described in this section.

### Command or Action | Purpose
---|---
**Step 1** | enable
Enables higher privilege levels, such as privileged EXEC mode. Enter your password if prompted.

**Step 2** | configure (terminal | memory | network)
Enters global configuration mode.

**Step 3** | crypto ca trustpoint name
Declares the CA that your router should use and enters ca-trustpoint configuration mode.

**Step 4** | enrollment terminal
Specifies manual cut-and-paste certificate enrollment.

**Step 5** | crypto ca authenticate name
Takes the name of the CA as the argument.
Manual Certificate Enrollment

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 6**
| `exit` | Exits ca-trustpoint configuration mode and returns to global configuration mode. |
| **Step 7**
| `crypto ca enroll name` | Obtains your router’s certificate(s) from the CA. |
| **Step 8**
| `crypto ca import name certificate` | Imports a certificate via TFTP or manually at the terminal. You must enter the `crypto ca import` command twice if usage keys (signature and encryption keys) are used. The first time the command is entered, one of the certificates is pasted into the router; the second time the command is entered, the other certificate is pasted into the router. (It does not matter which certificate is pasted first.) |

Certificate Enrollment Command Descriptions

crypto ca import Command
To import a certificate manually by using TFTP or cut-and-paste at the terminal, use the `crypto ca import` command in global configuration mode:

```plaintext
crypto ca import name certificate
```

where `name certificate` specifies the name of the CA. This name is the same name used when the certification authority (CA) was declared with the `crypto ca trustpoint` command (declares the CA that your router should use).

You must enter the `crypto ca import` command twice if usage keys (signature and encryption keys) are used. The first time the command is entered, one of the certificates is pasted into the router; the second time the command is entered, the other certificate is pasted into the router. (It does not matter which certificate is pasted first.)

enrollment terminal Command
To specify manual cut-and-paste certificate enrollment, use the enrollment terminal command in ca-trustpoint configuration mode.

```plaintext
enrollment terminal
```

To delete a current enrollment request, use the `no` form of this command.

enrollment Command
To specify the enrollment parameters of your certification authority (CA), use the `enrollment` command in ca-trustpoint configuration mode:

```plaintext
enrollment [mode] [retry minutes] [retry number] URL url
```

Where `url` specifies the URL of the CA where your router should send certificate requests. If you are using TFTP for enrollment, the URL must be in the form `tftp://certserver/file_specification`. The `file_specification` is optional. If the `file_specification` is included in the URL, the router appends an extension to the file specification.

To remove any of the configured parameters, use the `no` form of this command.
Example of Manual Certificate Enrollment Configuration

The following example shows how to specify a manual cut-and-paste certificate enrollment by using the `enrollment terminal` subcommand of the `crypto ca trustpoint` command. In this example, the name of the trustpoint CA is “MS,” and the `crypto ca import` command is entered twice because usage keys (signature and encryption keys) are used.

```
Router(config)# crypto ca trustpoint MS
Router(ca-trustpoint)# enrollment terminal
Router(ca-trustpoint)# crypto ca authenticate MS

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIICNDCCAdwAwIBAgIQCmNtcmFjcm9vbCdwYgIBAgYIKoZIhvcNAQkFMB0GA1Ud
-----END CERTIFICATE-----

Certificate has the following attributes:
Fingerprint:D6C12961 CD78808A 4E02193C 0790082A
% Do you accept this certificate? [yes/no]:y
Trustpoint CA certificate accepted.
% Certificate successfully imported

Router(config)#
Router(config)#crypto ca enroll MS

% Start certificate enrollment...

% The subject name in the certificate will be:Router.cisco.com
% Include the router serial number in the subject name? [yes/no]:n
% Include an IP address in the subject name? [no]:n
Display Certificate Request to terminal? [yes/no]:y
Signature key certificate request -
Certificate Request follows:

-----BEGIN CERTIFICATE-----
MIICnTCCB7wAwIBAgIgQpZnZjcm9vbCdwYgIBAgYIKoZIhvcNAQkFMB0GA1Ud
-----END CERTIFICATE-----

Certificate has the following attributes:
Fingerprint:D6C12961 CD78808A 4E02193C 0790082A
% Do you accept this certificate? [yes/no]:y
Trustpoint CA certificate accepted.
% Certificate successfully imported

Router(config)#
Router(config)#crypto ca enroll MS

% Start certificate enrollment...

% The subject name in the certificate will be:Router.cisco.com
% Include the router serial number in the subject name? [yes/no]:n
% Include an IP address in the subject name? [no]:n
Display Certificate Request to terminal? [yes/no]:y
Signature key certificate request -
Certificate Request follows:

-----BEGIN CERTIFICATE-----
MIIBhTCB7wIBAgIgQpZnZjcm9vbCdwYgIBAgYIKoZIhvcNAQkFMB0GA1Ud
-----END CERTIFICATE-----

Certificate has the following attributes:
Fingerprint:D6C12961 CD78808A 4E02193C 0790082A
% Do you accept this certificate? [yes/no]:y
Trustpoint CA certificate accepted.
% Certificate successfully imported

Router(config)#
Router(config)#crypto ca enroll MS

% Start certificate enrollment...

% The subject name in the certificate will be:Router.cisco.com
% Include the router serial number in the subject name? [yes/no]:n
% Include an IP address in the subject name? [no]:n
Display Certificate Request to terminal? [yes/no]:y
Signature key certificate request -
Certificate Request follows:

-----BEGIN CERTIFICATE-----
MIICnTCCB7wAwIBAgIgQpZnZjcm9vbCdwYgIBAgYIKoZIhvcNAQkFMB0GA1Ud
-----END CERTIFICATE-----

Certificate has the following attributes:
Fingerprint:D6C12961 CD78808A 4E02193C 0790082A
% Do you accept this certificate? [yes/no]:y
Trustpoint CA certificate accepted.
% Certificate successfully imported

--- End - This line not part of the certificate request---

Redisplay enrollment request? [yes/no]:
Encryption key certificate request -
Certificate Request follows:

MIIDbTC89IwIABDA7MSwWfQYJKoZIhvcNAQcKFCfRTIwN5Qm5FmZ2VyLyMpc2NvLmV
bTCBnzZNBkgkik1gS90gBAQFAQF8A0BijQwYkCgYAW0QjojDBz8Kyj88YFi0c
THDKP7XV1L7XAJ90jgSic8m0CdCtXhV1BWtp/09iYFKxL1h+MBCRI9L3t8
01XyA0931PFev7Q6PzesAi886aFrq7W7IwLObxgQ1jLcL4cbVU0rjLY0yu5A2+Z
kXmpC7c+pN9YFDlE91CAWEDAAAnHMB8CGsS1b3DQ6EjD3ESMAAW3gYDVR0PAQH/
BQAqDGaMA0CSgISb3DQ6BBAUA4GBACF7FeUrJ/F3Mo/pBIR67a9Br11My+2F
H9LYN/C12s2n4MhTWHkLoT8Wu6f2aN9A7x+y1nFD/05355wLfiq62n2bSCTW4aem
8jlJMMAeFxw5v/ceQRucmcNCluVx+fBy9rhKn88j60XE25tnp1U08r6om/pBQAUB
enNFPhozaq/2

--- End - This line not part of the certificate request---

Redisplay enrollment request? [yes/no]:
n
Router(config)#crypto ca import MS certificate

Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself

MIIDaXCAxSgwAIWAgfIKF7N76QAAAAMARzANBgkqhkiG9w0BAQFDA5MQwCQYD
VQQGSw7V0NzEMWBBQAIAEUAHEMQ2Iy28gU3lzDGTc=ESMBAGAIUEAUXjBmXNjY3SY
b29ONBH4XDTADyMxODAxMTHOnVQoDXA2MDxODAxMjY1MlOMoTJzMCBCGSqS1b3
DQ6XJAhMMU2fZEuZg22ldc15jaXNjby5jz20Q28G8DD+YKQjRZhsuN9BQBBtQrY0A
MIGJoaGBAMVXzX4ljoj45BGFCt20z8mA2bZv6oB7exV41ae52mb6XQ4eTmNSaA6S
MIHGA1U1dWnPmREaAFKtacis6DkAnN9VuYnSLQy8bZ1e20A5neVhyPQyQOGQ
Bxu7V0ZEMWBBQAIAU8hQ1I2y28gU3lzDGTc=ESMBAGAIUEAUXjBmXNjY3SY1by29Q
gh6aKZeX1ofch00gViGPrbuzTCGIALdU6ERQ/B0YcI4GeHntcmYmRwK8BoX12z1
Y8u2Y9Mc2GAgAIU68k5gMQuaJtwz6AtoC0u9XWcdHA6ly9tc2NLXIVb30Q2Vove
0msB6Ch42XNLXjVb30q3y3X3hGG6h3h6h3tmaXmek10418XV3xtc2hNLXIVb30cV
2yEvu3Ucb00kxtc2hNLXIVb30q3y3j3MsMIgUGhrBgbFbQbEgABQShhCheBDA/Bl
ggbEG/BQCaW0yAhrO06Cv2L1y2ZTcm9vCDXJ20RgR5b2x2L1y2zRtcm9vD9tc2hN
LXXIVb3ly3J3HEGECBeGAVFqBeA0ChjVmaWolc10418XV3xtc2hNLXIVb30cV
2yEvu3Ucb00kxtc2hNLXIVb30cV3y3j4Y1y290lMymDDANBgqkhkiG9w0BAQFAQF
AANBj02/2e6P4enm21NvRZ

% Router Certificate successfully imported

Router(config)#crypto ca import MS certificate

Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself

MIIDaXCAxSgwAIWAgfIKF7N76QAAAAMARzANBgkqhkiG9w0BAQFDA5MQwCQYD
VQQGSw7V0NzEMWBBQAIAEUAHEMQ2Iy28gU3lzDGTc=ESMBAGAIUEAUXjBmXNjY3SY
b29ONBH4XDTADyMxODAxMTHOnVQoDXA2MDxODAxMjY1MlOMoTJzMCBCGSqS1b3
DQ6XJAhMMU2fZEuZg22ldc15jaXNjby5jz20Q28G8DD+YKQjRZhsuN9BQBBtQrY0A
MIGJoaGBAMVXzX4ljoj45BGFCt20z8mA2bZv6oB7exV41ae52mb6XQ4eTmNSaA6S
MIHGA1U1dWnPmREaAFKtacis6DkAnN9VuYnSLQy8bZ1e20A5neVhyPQyQOGQ
Bxu7V0ZEMWBBQAIAU8hQ1I2y28gU3lzDGTc=ESMBAGAIUEAUXjBmXNjY3SY1by29Q
gh6aKZeX1ofch00gViGPrbuzTCGIALdU6ERQ/B0YcI4GeHntcmYmRwK8BoX12z1
Y8u2Y9Mc2GAgAIU68k5gMQuaJtwz6AtoC0u9XWcdHA6ly9tc2NLXIVb30Q2Vove
Verifying Manual Certificate Enrollment

To verify that the Manual Certificate Enrollment feature is working, perform the following optional steps:

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables higher privilege levels, such as privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> show crypto ca certificates</td>
<td>(Optional) Verifies information about your certificate, the certificate of the CA, and RA certificates.</td>
</tr>
<tr>
<td><strong>Step 3</strong> show crypto ca trustpoints</td>
<td>(Optional) Displays the trustpoints that are configured in the router.</td>
</tr>
</tbody>
</table>

The following sample output is displayed after manual certificate enrollment has been successfully configured by using the `enrollment terminal` command (cut-and-paste):

Router# show crypto ca certificates

Certificate
Status:Available
Certificate Serial Number:14DCE050000000000C48
Certificate Usage:Encryption
Issuer:
  CN = msca-root
  O = Cisco Systems
  C = US
Subject:
  Name:Router.cisco.com
  OID.1.2.840.113549.1.9.2 = Router.cisco.com
CRL Distribution Point:
  http://msca-root/CertEnroll/msca-root.crl
Validity Date:
  start date:18:16:45 PDT Jun 7 2002
  end date:18:26:45 PDT Jun 7 2003
  renew date:16:00:00 PST Dec 31 1969
Associated Trustpoints:MS

Certificate
Status:Available
Certificate Serial Number:14DEC2E90000000000C47
Certificate Usage:Signature
Issuer:
  CN = msca-root
  O = Cisco Systems
  C = US
Subject:
  Name:Router.cisco.com
  OID.1.2.840.113549.1.9.2 = Router.cisco.com
CRL Distribution Point:
  http://msca-root/CertEnroll/msca-root.crl
Validity Date:
  start date:18:16:42 PDT Jun 7 2002
  end date:18:26:42 PDT Jun 7 2003
  renew date:16:00:00 PST Dec 31 1969
Associated Trustpoints:MS

CA Certificate
Status:Available
Certificate Serial Number:3AC0A65E9547C2874AAF2468A942D5EE
Certificate Usage:Signature
Issuer:
  CN = msca-root
  O = Cisco Systems
  C = US
Subject:
  CN = msca-root
  O = Cisco Systems
  C = US
CRL Distribution Point:
  http://msca-root/CertEnroll/msca-root.crl
Validity Date:
  start date:16:46:01 PST Feb 13 2002
  end date:16:54:48 PST Feb 13 2007
Associated Trustpoints:MS

Related Documents

Table 9-1 shows documents that contain additional information on Mobile IP Security.

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>CA configuration tasks</td>
<td>The chapter “Configuring Certification Authority Interoperability” in the Cisco IOS Security Configuration Guide, Release 12.2</td>
</tr>
<tr>
<td>Additional certificate and CA commands</td>
<td>The chapter “Certification Authority Interoperability Commands” in the Cisco IOS Security Command Reference, Release 12.2</td>
</tr>
<tr>
<td>Additional ca-trustpoint configuration commands</td>
<td>Trustpoint CLI, Cisco IOS Release 12.2(8)T feature module</td>
</tr>
</tbody>
</table>