TLS Proxy for Encrypted Voice Inspection

This chapter describes how to configure the TLS Proxy so that the system can inspect encrypted voice connections.

This chapter includes the following sections:

Information About the TLS Proxy for Encrypted Voice Inspection

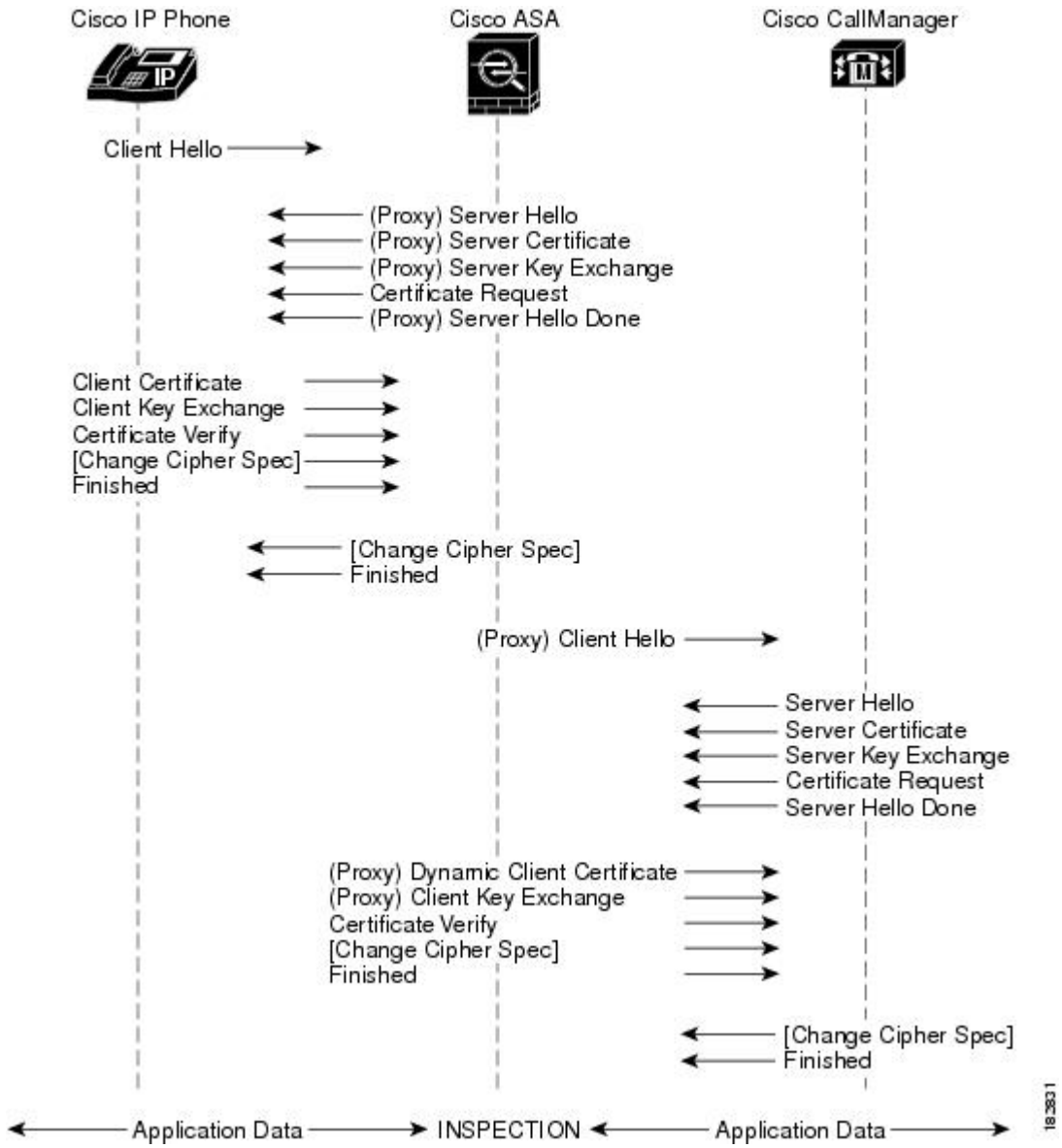
End-to-end encryption often leaves network security appliances “blind” to media and signaling traffic, which can compromise access control and threat prevention security functions. This lack of visibility can result in a lack of interoperability between the firewall functions and the encrypted voice, leaving businesses unable to satisfy both of their key security requirements.

The ASA is able to intercept and decrypt encrypted signaling from Cisco encrypted endpoints to the Cisco Unified Communications Manager (Cisco UCM), and apply the required threat protection and access control. It can also ensure confidentiality by re-encrypting the traffic onto the Cisco UCM servers.

Typically, the ASA TLS Proxy functionality is deployed in campus unified communications network. This solution is ideal for deployments that utilize end to end encryption and firewalls to protect Unified Communications Manager servers.

The security appliance in the following figure serves as a proxy for both client and server, with Cisco IP Phone and Cisco UCM interaction.

Figure 1: TLS Proxy Flow



Decryption and Inspection of Unified Communications Encrypted Signaling

With encrypted voice inspection, the security appliance decrypts, inspects and modifies (as needed, for example, performing NAT), and re-encrypts voice signaling traffic while all of the existing VoIP inspection functions for SIP are preserved. Once voice signaling is decrypted, the plain text signaling message is passed to the existing inspection engines.

The security appliance acts as a TLS proxy between the Cisco IP Phone and Cisco UCM. The proxy is transparent for the voice calls between the phone and the Cisco UCM. Cisco IP Phones download a Certificate Trust List from the Cisco UCM before registration which contains identities (certificates) of the devices that the phone should trust, such as TFTP servers and Cisco UCM servers. To support server proxy, the CTL file must contain the certificate that the security appliance creates for the Cisco UCMs.

To proxy calls on behalf of the Cisco IP Phone, the security appliance presents a certificate that the Cisco UCM can verify, which is a Local Dynamic Certificate for the phone, issued by the certificate authority on the security appliance.

TLS proxy is supported by the Cisco Unified CallManager Release 5.1 and later. You should be familiar with the security features of the Cisco UCM. For background and detailed description of Cisco UCM security, see the Cisco Unified CallManager documentation.

Supported Cisco UCM and IP Phones for the TLS Proxy

Cisco Unified Communications Manager

The following releases of the Cisco Unified Communications Manager are supported with the TLS proxy:

- Cisco Unified CallManager Version 5.1
- Cisco Unified Communications Manager 6.1
- Cisco Unified Communications Manager 7.0
- Cisco Unified Communications Manager 8.0
- Cisco Unified Communications Manager 8.6
- Cisco Unified Communications Manager 10.5

Cisco Unified IP Phones

The following IP phones are supported with the TLS proxy:

- Cisco Unified IP Phone 7985
- Cisco Unified IP Phone 7975
- Cisco Unified IP Phone 7971
- Cisco Unified IP Phone 7970
- Cisco Unified IP Phone 7965
- Cisco Unified IP Phone 7962
- Cisco Unified IP Phone 7961
- Cisco Unified IP Phone 7961G-GE
- Cisco Unified IP Phone 7960
- Cisco Unified IP Phone 7945
- Cisco Unified IP Phone 7942
- Cisco Unified IP Phone 7941
- Cisco Unified IP Phone 7941G-GE
- Cisco Unified IP Phone 7940
- Cisco Unified Wireless IP Phone 7921
- Cisco Unified Wireless IP Phone 7925

- Cisco Unified IP Conference Phone 8831
- Cisco IP Communicator (CIPC) for softphones

Incorporating the Firewall into the Unified Communications System

Configuring the ASA is not enough to fully incorporate the firewall into the Cisco Unified Communications system. You must also add the ASA to the Certificate Trust List (CTL) using the Cisco Certificate Trust List Client, which is part of the Unified Communications Manager.

When you configure a firewall in the CTL file, you can secure a ASA firewall as part of a secure Cisco Unified Communications Manager system. The Cisco CTL Client displays the firewall certificate as a "CCM" certificate.

When configured correctly, the ASA receives the CTL file from the CTL provider. However, the ASA does not store the raw CTL file in the flash, rather, it parses the CTL file and installs the appropriate trustpoints.

For detailed information on how to add the ASA as a firewall to the Unified Communications Manager system, look for information on the CTL Client Setup in the *Security Guide for Cisco Unified Communications Manager* for the software version you are using. You can find the documents at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-call%20manager/products-maintenance-guides-list.html.

Also see the Security Guide for information on installing, exporting, and creating UCM-side certificates. You will need to import the ASA certificate into UCM.

Configuring the TLS Proxy for Encrypted Voice Inspection (CLI)

The following procedure explains the end-to-end process for enabling inspection of encrypted voice traffic.

Before you begin

Prerequisites for the TLS Proxy for Encrypted Voice Inspection

Before configuring TLS proxy, the following prerequisites are required:

- You must set clock on the security appliance before configuring TLS proxy. To set the clock manually and display clock, use the **clock set** and **show clock** commands. We recommend that the security appliance use the same NTP server as the Cisco Unified CallManager cluster. TLS handshake may fail due to certificate validation failure if clock is out of sync between the security appliance and the Cisco Unified CallManager server.
- 3DES-AES license is needed to interoperate with the Cisco Unified CallManager. AES is the default cipher used by the Cisco Unified CallManager and Cisco IP Phone.

Step 1 (Optional) Set the maximum number of TLS proxy sessions to be supported by the security appliance. For example:

Example:

```
ciscoasa(config)# tls-proxy maximum-sessions 1200
```

The default and maximum differ by device model. This command controls the memory size reserved for cryptographic applications such as TLS proxy. Crypto memory is reserved at the time of system boot. If you increase the number, you must reboot the system to reserve the additional memory.

Step 2 Create the Proxy Trustpoint for the Unified Call Manager Cluster

Step 3 Create the Internal Local CA to Sign Local Dynamic Certificates for Phones

Step 4 Create a CTL Provider

Step 5 Create the TLS Proxy

Step 6 Enable TLS Proxy for SIP Inspection

Step 7 Export the local CA certificate (ldc_server) and install it as a trusted certificate on the Cisco UCM server.

a. Use the following command to export the certificate if a trust-point with proxy-ldc-issuer is used as the signer of the dynamic certificates, for example:

```
ciscoasa(config)# crypto ca export ldc_server identity-certificate
```

b. For the embedded local CA server LOCAL-CA-SERVER, use the following command to display the certificate, which you can then copy and paste to a text file. For example:

```
ciscoasa(config)# show ca server certificate
```

c. Import the certificate into UCM. For detailed information, see the *Security Guide for Cisco Unified Communications Manager* for the software version you are using. You can find the documents at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-managercallmanager/products-maintenance-guides-list.html.

Step 8 Run the CTL Client application to add the server proxy certificate (ccm_proxy) to the CTL file and install the CTL file on the security appliance.

For more information, see Incorporating the Firewall into the Unified Communications System.

Create the Proxy Trustpoint for the Unified Call Manager Cluster

The Cisco UCM proxy certificate could be self-signed or issued by a third-party CA. The certificate is exported to the CTL client. The following procedure shows how to create a self-signed proxy.

The ASA uses this proxy when authenticating with the phones. The ASA acts as the server in place of the Call Manager.

Step 1 Create the RSA keypair for the trustpoint.

crypto key generate rsa label *key-pair-label* **modulus** *size*

Cisco UCM releases 10.5.2su3 and earlier allow a maximum key of 1024 bits. The default is 2048, so you need to include the **modulus** keyword.

Example:

```
ciscoasa(config)# crypto key generate rsa label ccm_proxy_key modulus 1024
INFO: The name for the keys will be: ccm_proxy_key
Keypair generation process begin. Please wait...
ciscoasa(config)#
```

Step 2 Create the proxy trustpoint for the Unified Call Manager cluster.

crypto ca trustpoint *trustpoint_name*

You enter trustpoint configuration mode, where you can configure the trustpoint characteristics.

Example:

```
ciscoasa(config)# crypto ca trustpoint ccm_proxy
```

Step 3 Generate a self-signed certificate.

enrollment self

Example:

```
ciscoasa(config-ca-trustpoint)# enrollment self
```

Step 4 Do not to include a fully qualified domain name (FQDN) in the Subject Alternative Name extension of the certificate during enrollment.

fqdn none

Example:

```
ciscoasa(config-ca-trustpoint)# fqdn none
```

Step 5 Specify a subject DN in the certificate during enrollment.

subject-name *X.500_name*

Cisco IP Phones require certain fields from the X.509v3 certificate to be present to validate the certificate by consulting the CTL file. Consequently, the **subject-name** entry must be configured for a proxy certificate trustpoint. The subject name must be composed of the ordered concatenation of the CN, OU and O fields. The CN field is mandatory; the others are optional.

If you use multiple attributes, separate them with a semicolon. Use one of the following forms:

- CN=xxx;OU=yyy;O=zzz
- CN=xxx;OU=yyy
- CN=xxx;O=zzz
- CN=xxx

Example:

```
ciscoasa(config-ca-trustpoint)# subject-name cn=EJW-SV-1-Proxy
```

Step 6 Specify the key pair you created for the trustpoint.

keypair *keyname*

Example:

```
ciscoasa(config-ca-trustpoint)# keypair ccm_proxy_key
```

Step 7 Enroll the trustpoint.

crypto ca enroll *trustpoint_name*

Example:

```
ciscoasa(config-ca-trustpoint)# crypto ca enroll ccm_proxy
WARNING: The certificate enrollment is configured with an fqdn
that differs from the system fqdn. If this certificate will be
used for VPN authentication this may cause connection problems.

Would you like to continue with this enrollment? [yes/no]: yes
```

```
% The fully-qualified domain name will not be included in the certificate

% Include the device serial number in the subject name? [yes/no]: no

Generate Self-Signed Certificate? [yes/no]: yes
ciscoasa(config)#
```

Create the Internal Local CA to Sign Local Dynamic Certificates for Phones

Create an internal local CA to sign the LDC for Cisco IP Phones. This local CA is a regular self-signed trustpoint with **proxy-ldc-issuer** enabled. The ASA presents these certificates to the Call Manager server on behalf of the phones, securing the connection between the ASA and the Call Manager.

You can alternatively use the embedded local CA LOCAL-CA-SERVER on the ASA to issue the LDC, but this is not recommended.

Step 1 Create the RSA keypair for the local CA.

crypto key generate rsa label *key-pair-label* **modulus** *size*

Cisco UCM releases 10.5.2su3 and earlier allow a maximum key of 1024 bits. The default is 2048, so you need to include the **modulus** keyword.

Example:

```
ciscoasa(config)# crypto key generate rsa label ldc_signer_key modulus 1024
INFO: The name for the keys will be: ldc_signer_key
Keypair generation process begin. Please wait...
ciscoasa(config)#
```

Step 2 Create the proxy trustpoint for the local Certificate Authority (CA) for signing local dynamic certificates.

crypto ca trustpoint *trustpoint_name*

You enter trustpoint configuration mode, where you can configure the trustpoint characteristics.

Example:

```
ciscoasa(config)# crypto ca trustpoint ldc_server
```

Step 3 Generate a self-signed certificate.

enrollment self

Example:

```
ciscoasa(config-ca-trustpoint)# enrollment self
```

Step 4 Define the CA as one that can issue local dynamic certificates (LDC).

proxy-ldc-issuer

You can configure this option for a local CA only if you also specify **enrollment self**.

The ASA generates a local dynamic certificate for each phone that registers with the Call Manager. When the phone unregisters, the dynamic certificate is automatically deleted. These certificates do not appear in the running configuration; they are created and destroyed as needed.

Example:

```
ciscoasa(config-ca-trustpoint)# proxy-ldc-issuer
```

Step 5 Add a fully qualified domain name (FQDN) in the Subject Alternative Name extension of the certificate during enrollment.

fqdn *name*

Example:

```
ciscoasa(config-ca-trustpoint)# fqdn my-ldc-ca.example.com
```

Step 6 Specify a subject DN in the certificate during enrollment.

subject-name *X.500_name*

The CN field is mandatory; the others are optional. If you use multiple attributes, separate them with a semicolon. Use one of the following forms:

- CN=xxx;OU=yyy;O=zzz
- CN=xxx;OU=yyy
- CN=xxx;O=zzz
- CN=xxx

Example:

```
ciscoasa(config-ca-trustpoint)# subject-name cn=FW_LDC_SIGNER_172_23_45_200
```

Step 7 Specify the key pair you created for the local CA.

keypair *keyname*

Example:

```
ciscoasa(config-ca-trustpoint)# keypair ldc_signer_key
```

Step 8 Enroll the trustpoint.

crypto ca enroll *trustpoint_name*

Example:

```
ciscoasa(config-ca-trustpoint)# crypto ca enroll ldc_server
WARNING: The certificate enrollment is configured with an fqdn
that differs from the system fqdn. If this certificate will be
used for VPN authentication this may cause connection problems.

Would you like to continue with this enrollment? [yes/no]: yes

% The fully-qualified domain name in the certificate will be:
my-ldc-ca.example.com

% Include the device serial number in the subject name? [yes/no]: no

Generate Self-Signed Certificate? [yes/no]: yes
ciscoasa(config)#
```

Create a CTL Provider

Create a CTL Provider in preparation for a connection from the CTL Client.

Step 1 Create the Certificate Trust List (CTL) provider.

ctl-provider *ctl_name*

You enter CTL provider configuration mode, where you can configure the provider characteristics.

Example:

```
ciscoasa(config)# ctl-provider my_ctl
```

Step 2 Specify the addresses of the CTL clients that should be able to connect with the CTL provider on the ASA.

client interface *if_name ipv4_address*

Where *if_name* is the interface through which the client can be reached, and the IPv4 address is the address of the workstation on which the CTL client is installed. Enter this command as many times as needed to identify all CTL clients that you want to allow.

Example:

```
ciscoasa(config-ctl-provider)# client interface inside address 172.23.45.1
```

Step 3 Specify the username and password for client authentication.

client username *name* **password** *password* **[encrypted]**

The username and password must be the username and password for Cisco UCM administration. Specify the optional **encrypted** keyword if the password is encrypted (in which case it must be 16 characters).

Example:

```
ciscoasa(config-ctl-provider)# client username CCMAdministrator
password XXXXXX
```

Step 4 Export the proxy trustpoint you created for the Cisco UCM server to the CTL client.

export certificate *trustpoint_name*

The certificate will be added to the Certificate Trust List file composed by the CTL client and subsequently distributed to all the phones that download the CTL file. Specify the name of the trustpoint you created in Create the Proxy Trustpoint for the Unified Call Manager Cluster. This ensures that each phone has the server certificate the ASA uses to authenticate the connection.

Example:

```
ciscoasa(config-ctl-provider)# export certificate ccm_proxy
```

Step 5 If necessary, change the port on which the CTL provider listens.

service port *number*

The default port number listened to by the CTL Provider is TCP 2444, which is the default CTL port on the Cisco UCM. If you changed this port in the Cisco UCM, you must specify the port on this command so that the CTL Provider can communicate with the CTL client. The port must be in the range 2000-9999.

Example:

```
ciscoasa(config-ctl-provider)# service port 2445
```

Step 6 Enable the CTL provider to parse the CTL file from the CTL client and install trustpoints for entries from the CTL file.

ctl install

Trustpoints installed by this command have names prefixed with "_internal_CTL_<ctl_name>."

Example:

```
ciscoasa(config-ctl-provider)# ctl install
```

Create the TLS Proxy

Create the TLS proxy to handle the encrypted signaling.

Step 1 Create the RSA keypair for the local CA.

crypto key generate rsa label *key-pair-label* **modulus** *size*

Cisco UCM releases 10.5.2su3 and earlier allow a maximum key of 1024 bits. The default is 2048, so you need to include the **modulus** keyword.

Example:

```
ciscoasa(config)# crypto key generate rsa label phone_common modulus 1024
INFO: The name for the keys will be: phone_common
Keypair generation process begin. Please wait...
ciscoasa(config)#
```

Step 2 Create the TLS proxy.

tls-proxy *name*

You enter TLS proxy configuration mode, where you can configure the proxy characteristics.

Example:

```
ciscoasa(config)# tls-proxy my_proxy
```

Step 3 Specify the proxy trustpoint certificate to present during the TLS handshake with phone clients.

server trust-point *proxy_trustpoint*

Specify the name of the trustpoint you created in Create the Proxy Trustpoint for the Unified Call Manager Cluster.

The **server** command configures the proxy parameters for the original TLS server. In other words, the parameters for the ASA to act as the server during a TLS handshake the TLS clients.

Example:

```
ciscoasa(config-tlsp)# server trust-point ccm_proxy
```

Step 4 Specify the local CA trustpoint to provide the local dynamic certificates.

client ldc issuer *ca_trustpoint_name*

Specify the name of the local CA you created in Create the Internal Local CA to Sign Local Dynamic Certificates for Phones. This trustpoint must include the proxy-ldc-issuer command or be the default local CA server (LOCAL-CA-SERVER).

Example:

```
ciscoasa(config-tlsp)# client ldc issuer ldc_server
```

Step 5 Specify the key pair you created for the local dynamic certificates.

client ldc key-pair *keyname*

Example:

```
ciscoasa(config-tlsp)# client ldc key-pair phone_common
```

Step 6 (Optional.) Configure the cipher suite to use when the proxy acts as a client to the Cisco UCM.

client cipher-suite *cipher_suite*

For client proxy (the proxy acts as a TLS client to the server), the user-defined cipher suite replaces the default cipher suite, or the one defined by the **ssl encryption** command. You can use this command to achieve difference ciphers between the two TLS sessions. You should use AES ciphers with the CallManager server. Separate multiple options with spaces.

Example:

```
ciscoasa(config-tlsp)# client cipher-suite aes128-sha1 aes256-sha1
```

Step 7 (Optional.) Configure the cipher suite to use when the proxy acts as a server to the phones.

If you do not define the ciphers the TLS proxy can use, the proxy server uses the global cipher suite defined by the **ssl cipher** command. By default, the global cipher level is medium, which means all ciphers are available except for NULL-SHA, DES-CBC-SHA, and RC4-MD5. Specify the **server cipher-suite** command only if you want to use a different suite than the one generally available on the ASA. Separate multiple options with spaces.

To set the minimum TLS version for all SSL server connections on the ASA, see the **ssl server-version**command. The default is TLS v1.0.

Example:

```
ciscoasa(config-tlsp)# server cipher-suite aes128-sha1 aes256-sha1
```

Enable TLS Proxy for SIP Inspection

Configure the required service policies to enable encrypted voice inspection for SIP.

Because secure protocols use different ports than the regular unencrypted versions, you need to configure unique classes for TLS proxy inspection.

- Secure SIP (SIPS) uses TCP/UDP 5061 (rather than SIP's 5060).

The inspection_default class filters on the unencrypted ports only.

The following procedure explains how to create these classes and add the TLS proxy inspections to the existing global_policy policy map. Alternatively, you can create service policies for specific interfaces.

For more detailed information on how to configure service policies, see the firewall configuration guide.

Before you begin

You can configure inspection policy maps to customize the inspection. If you do not want to use the default settings for the inspections, configure the inspection policy maps before configuring the service policy. For details on customizing SIP, see the firewall configuration guide. The following procedure assumes you are using the default settings.

Step 1 Create the class for secure SIP.

Because SIP endpoints can use TCP or UDP, you cannot create a simple port match for the class. Instead, create a service group for TCP/5061 and UDP/5061, then use that object in an ACL.

a. Create a service object group for TCP/UDP 5061.

```
ciscoasa(config)# object-group service sec_sip_ports
ciscoasa(config-service-object-group)# service-object
tcp-udp destination eq 5061
```

b. Create an ACL that matches secure SIP traffic for all addresses.

```
ciscoasa(config)# access-list sec_sip_acl extended permit
object-group sec_sip_ports any any
ciscoasa(config)# show access-list
access-list sec_sip_acl; 2 elements; name hash: 0x46fa3345
access-list sec_sip_acl line 1 extended permit object-group
sec_sip_ports any any (hitcnt=0) 0x04ff39a5
access-list sec_sip_acl line 1 extended permit
tcp any any eq 5061 (hitcnt=0) 0x23e41037
access-list sec_sip_acl line 1 extended permit
udp any any eq 5061 (hitcnt=0) 0x511cfebe
```

c. Create the class map using an ACL match.

```
ciscoasa(config)# class-map sec_sip
ciscoasa(config-cmap)# match access-list sec_sip_acl
```

Step 2 Edit the global_policy policy map.

```
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)#
```

Step 3 Add the Secure SIP class and configure SIP inspection with the TLS proxy.

```
ciscoasa(config-pmap)# class sec_sip
ciscoasa(config-pmap-c)# inspect sip tls-proxy my_proxy
```

Step 4 Verify the global_policy policy map now has the expected content.

In the following output, you can see that the running configuration performs SIP inspection without the TLS proxy on the unencrypted default ports that match the inspection_default class. Then, the TLS proxy inspections appear for the correct sec_sip class for the encrypted ports.

```
ciscoasa(config-pmap-c)# show run policy-map global_policy
!
policy-map global_policy
class inspection_default
inspect dns migrated_dns_map_1
inspect ftp
inspect ip-options
inspect netbios
inspect rsh
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect xdmcp
inspect sip
inspect skinny
class sec_sip
```

```
inspect sip tls-proxy my_proxy
!
```

Step 5 Enable the global_policy service policy to implement your changes.

```
ciscoasa(config-pmap-c)# service-policy global_policy global
```

Configuring the TLS Proxy for Encrypted Voice Inspection (ASDM)

The following procedure explains the end-to-end process for enabling inspection of encrypted voice traffic using ASDM.

Step 1 Create the Proxy Trustpoint for the Unified Call Manager Cluster (ASDM).

Step 2 Create the Internal Local CA to Sign Local Dynamic Certificates for Phones (ASDM)

Step 3 Create a CTL Provider (ASDM)

Step 4 Create the TLS Proxy (ASDM)

Step 5 Enable TLS Proxy for SIP Inspection

Step 6 Export the local CA certificate (ldc_server) and install it as a trusted certificate on the Cisco UCM server.

a. Choose **Configuration** > **Firewall** > **Advanced** > **Certificate Management** > **Identity Certificates**

b. Select the LDC trustpoint and click **Export**.

c. Specify a file name and click **Export Certificate**.

d. Import the certificate into UCM. For detailed information, see the *Security Guide for Cisco Unified Communications Manager* for the software version you are using. You can find the documents at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-managercallmanager/products-maintenance-guides-list.html.

Step 7 Run the CTL Client application to add the server proxy certificate (ccm_proxy) to the CTL file and install the CTL file on the security appliance.

For more information, see Incorporating the Firewall into the Unified Communications System.

Create the Proxy Trustpoint for the Unified Call Manager Cluster (ASDM)

The Cisco UCM proxy certificate could be self-signed or issued by a third-party CA. The certificate is exported to the CTL client. The following procedure shows how to create a self-signed proxy.

The ASA uses this proxy when authenticating with the phones. The ASA acts as the server in place of the Call Manager.

Step 1 Choose **Device Management** > **Certificate Management** > **Identity Certificates**then click the **Add** button.

Step 2 Enter a Trustpoint Name. For example, **ccm_proxy**.

Step 3 Choose **Add a New Identity Certificate**.

Step 4 For **Key Pair**, create a new key pair:

a. Click **New**.

b. Select **RSA** as the key type.

c. Select **Enter New Key Pair Name**, then enter a name. For example, **ccm_proxy_key**.

d. For **Size**, select **1024**.

Cisco UCM releases 10.5.2su3 and earlier allow a maximum key of 1024 bits.

e. For **Usage**, select **General Purpose**.

f. Click **Generate Now**.

The key is generated and you are returned to the Add Identity Certificate dialog box with the new key automatically selected.

Step 5 For **Certificate Subject DN**, specify a subject DN.

Cisco IP Phones require certain fields from the X.509v3 certificate to be present to validate the certificate by consulting the CTL file. Consequently, you must configure a subject DN for a proxy certificate trustpoint. The subject name must be composed of the ordered concatenation of the CN, OU and O fields. The CN field is mandatory; the others are optional.

If you use multiple attributes, separate them with a semicolon. Use one of the following forms:

- CN=xxx;OU=yyy;O=zzz
- CN=xxx;OU=yyy
- CN=xxx;O=zzz
- CN=xxx

For example, **cn=EJW-SV-1-Proxy**.

Step 6 Choose **Generate Self-Signed Certificate**.

Note Do not select the Act as local certificate authority and issue dynamic certificates for TLS proxy option for this trustpoint.

Step 7 Click the **Advanced** button, and clear the **FQDN** field on the Certificate Parameters tab. Click **OK**.

Do not to include a fully qualified domain name (FQDN) in the Subject Alternative Name extension of the certificate during enrollment.

Step 8 Click **Add Certificate**.

Create the Internal Local CA to Sign Local Dynamic Certificates for Phones (ASDM)

Create an internal local CA to sign the LDC for Cisco IP Phones. This local CA is a regular self-signed trustpoint with the ability to issue local dynamic certificates. The ASA presents these certificates to the Call Manager server on behalf of the phones, securing the connection between the ASA and the Call Manager.

You can alternatively use the embedded local CA (LOCAL-CA-SERVER) on the ASA to issue the LDC, but this is not recommended.

Step 1 Choose **Device Management** > **Certificate Management** > **Identity Certificates** then click the **Add** button.

Step 2 Enter a Trustpoint Name. For example, **ldc_server**.

Step 3 Choose **Add a New Identity Certificate**.

Step 4 For **Key Pair**, create a new key pair:

a. Click **New**.

b. Select **RSA** as the key type.

c. Select **Enter New Key Pair Name**, then enter a name. For example, **ldc_signer_key**.

d. For **Size**, select **1024**.

Cisco UCM releases 10.5.2su3 and earlier allow a maximum key of 1024 bits.

e. For **Usage**, select **General Purpose**.

f. Click **Generate Now**.

The key is generated and you are returned to the Add Identity Certificate dialog box with the new key automatically selected.

Step 5 For **Certificate Subject DN**, specify a subject DN.

The CN field is mandatory; the others are optional. If you use multiple attributes, separate them with a semicolon. Use one of the following forms:

- CN=xxx;OU=yyy;O=zzz
- CN=xxx;OU=yyy
- CN=xxx;O=zzz
- CN=xxx

For example, **cn=FW_LDC_SIGNER_172_23_45_200**.

Step 6 Choose **Generate Self-Signed Certificate**.

Step 7 Choose the **Act as local certificate authority and issue dynamic certificates for TLS proxy** option.

The ASA generates a local dynamic certificate for each phone that registers with the Call Manager. When the phone unregisters, the dynamic certificate is automatically deleted. These certificates do not appear in the running configuration; they are created and destroyed as needed.

Step 8 Click the **Advanced** button, and enter an fully-qualified domain name in the **FQDN** field on the Certificate Parameters tab. Click **OK**.

For example, **my-ldc-ca.example.com**.

Step 9 Click **Add Certificate**.

Create a CTL Provider (ASDM)

Create a CTL Provider in preparation for a connection from the CTL Client.

Step 1 Select **Configuration** > **Firewall** > **Unified Communications** > **CTL Provider**

Step 2 Click **Add** to create a new provider, or select a provider and click **Edit**.

Step 3 Enter a **CTL Provider Name**. For example, **my_ctl**.

Step 4 In **Certificate to be Exported**, select the proxy trustpoint you created for the Cisco UCM server to the CTL client.

The certificate will be added to the Certificate Trust List file composed by the CTL client and subsequently distributed to all the phones that download the CTL file. Specify the name of the trustpoint you created in Create the Proxy Trustpoint for the Unified Call Manager Cluster (ASDM). This ensures that each phone has the server certificate the ASA uses to authenticate the connection.

For example, select **ccm_proxy**.

Step 5 Specify the addresses of the CTL clients that should be able to connect with the CTL provider on the ASA.

For each client, select the interface through which the client can be reached, and then enter the IPv4 address of the workstation on which the CTL client is installed. Click **Add>>** to add it to the list of clients. For example, **inside 172.23.45.1**.

Repeat the process as many times as needed to identify all CTL clients that you want to allow.

Step 6 Click **More Options**, and specify the username and password for client authentication.

The username and password must be the username and password for Cisco UCM administration. For example, CCMAdministrator, password XXXXXX.

Step 7 If necessary, change the port on which the CTL provider listens in the **Port Number** field.

The default port number listened to by the CTL Provider is TCP 2444, which is the default CTL port on the Cisco UCM. If you changed this port in the Cisco UCM, you must specify the port on this command so that the CTL Provider can communicate with the CTL client. The port must be in the range 2000-9999.

Step 8 Ensure that the **Parse the CTL File Provided by the CTL Client and Install Trustpoints** option is selected.

The system installs trustpoints for entries from the CTL file. Trustpoints installed from the file have names prefixed with "_internal_CTL_<ctl_name>." If you disable this option, you must manually import and install each Call Manager server and CAPF certificate.

Step 9 Click **OK**.

Create the TLS Proxy (ASDM)

Create the TLS proxy to handle the encrypted signaling. The following procedure explains how to configure the proxy for encrypted SIP inspection.

Step 1 Select **Configuration** > **Firewall** > **Unified Communications** > **TLS Proxy**.

Step 2 (Optional) Set the maximum number of TLS proxy sessions to be supported by the security appliance.

The default and maximum differ by device model. The **Maximum TLS Sessions** option controls the memory size reserved for cryptographic applications such as TLS proxy. Crypto memory is reserved at the time of system boot. If you increase the number, you must reboot the system to reserve the additional memory.

To change the default, select **Specify the Maximum Number of TLS Proxy Sessions that the ASA Needs to Support**, and enter the maximum number of sessions. These fields are below the table of TLS proxies.

Step 3 Click **Add** to create a new TLS proxy, or select a proxy and click **Edit**.

When you create a new proxy, you are taken through a wizard to configure the required properties. When editing an existing proxy, the wizard steps are presented as separate tabs. The following steps assume you are adding a new proxy.

Step 4 Enter a name for the proxy in **TLS Proxy Name**. For example, **my_proxy**. Click **Next**.

Step 5 Configure the options to use when the ASA acts as the TLS server for the phone clients.

For encrypted SIP inspection as explained in this procedure, the ASA acts as a proxy for Cisco Unified Call Manager. However, you could also configure the proxy for a Cisco Unified Presence Server (CUPS), or when configuring MMP inspection for a Cisco Unified Mobility Advantage (CUMA) server.

a. In **Server Proxy Certificate**, select the trustpoint you created in Create the Proxy Trustpoint for the Unified Call Manager Cluster (ASDM). For example, ccm_proxy.

The server proxy configures the proxy parameters for the original TLS server. In other words, the parameters for the ASA to act as the server during a TLS handshake the TLS clients.

If you have not already created the identity certificate, you can click **Manage** to add it.

b. (Optional.) You can define the security algorithms (ciphers) that the server can use by moving them from the available algorithms to the active algorithms list. If you do not specify ciphers, the default system ciphers are used. You can move the algorithms up or down to change their relative priority.

c. (Optional.) Click **Install TLS Server's Certificate** to install the Call Manager certificate. Because this certificate will be installed from the CTL file, you do not need to install it. However, if you are not installing trustpoints from the CTL file, obtain the certificate from the Call Manager server and install it now.

d. Select **Enable client authentication during TLS Proxy handshake**. You would deselect this option only for testing purposes, or for MMP inspection.

For MMP inspection, used for Unified Mobility Advantage (CUMA), the client is not able to present a certificate, so authentication is not possible.

e. Click **Next**.

Step 6 Configure the options to use when the ASA acts as the TLS client for the original TLS server.

For encrypted SIP inspection as explained in this procedure, the ASA acts as a proxy for IP phones. However, you could also configure the proxy for a Microsoft LCS/OCS client for Cisco Unified Presence Federation, or when configuring MMP inspection for a Cisco Unified Mobility Advantage (CUMA) client.

a. Choose the **Specify the Internal Certificate Authority to Sign the Local Dynamic Certificates for Phones**.

The other options are used for other types of inspection:

- **Configure the proxy client to use clear text to communicate with the remote TCP server**. This option configures TLS offload for Diameter inspection, for use when the ASA is in the same data center as the Diameter server.
- **Specify the proxy certificate for TLS Client**. This option is for use when the client is also a server (in the case of Presence Federation), or when you want to use a single certificate to represent all clients (in Diameter inspection).

b. In **Certificate**, select the LDC issuer you created in Create the Internal Local CA to Sign Local Dynamic Certificates for Phones (ASDM). For example, **ldc_server**. This trustpoint must include the **proxy-ldc-issuer** command. If you have not created this trustpoint yet, click **Manage** and create it now.

Alternatively, if you want to use the default local CA server (LOCAL-CA-SERVER), select **Certificate Authority Server**.

c. For **Key-Pair Name**, click **New** and create a new RSA general purpose key pair, size 1024. (Cisco UCM releases 10.5.2su3 and earlier allow a maximum key of 1024 bits.) Give the key a new name, for example, **phone_common**. When you click **Generate Now**, the key is generated and you are returned to the wizard with the new key pair selected.

d. (Optional.) You can define the security algorithms (ciphers) to use when the proxy acts as a client to the Cisco UCM. Move the allowed ciphers from the available algorithms to the active algorithms list. These ciphers replace the original ones from the hello message. If you do not specify ciphers, the default system ciphers are used. You can move the algorithms up or down to change their relative priority. You can select the null cipher if you are confident communication with the Call Manager server is secure (for example, the server is in the same data center as the ASA).

e. Click **Next**.

Step 7 The final step of the wizard explains the additional steps you must perform. Click **Finish**.

Enable TLS Proxy for SIP Inspection (ASDM)

Configure the required service policies to enable encrypted voice inspection for SIP.

Because secure protocols use different ports than the regular unencrypted versions, you need to configure unique classes for TLS proxy inspection.

- Secure SIP (SIPS) uses TCP/UDP 5061 (rather than SIP's 5060).

The inspection_default class filters on the unencrypted ports only.

The following procedure explains how to create these classes and add the TLS proxy inspections to the existing global_policy policy map. Alternatively, you can create service policies for specific interfaces.

For more detailed information on how to configure service policies, see the firewall configuration guide.

Before you begin

You can configure inspection policy maps to customize the inspection. If you do not want to use the default settings for the inspections, configure the inspection policy maps before configuring the service policy. For

details on customizing SIP, see the firewall configuration guide. The following procedure assumes you are using the default settings.

Step 1 Choose **Configuration** > **Firewall** > **Service Policy**.

Step 2 Create the service policy for secure SIP.

a. Click **Add** > **Add Service Policy Rule**.

b. Select **Global** and click **Next**.

c. Choose **Create a New Class** and enter a class name, for example, **sec_sip**.

d. Choose **Source and Destination IP Address (Uses ACL)**.

Because SIP endpoints can use TCP or UDP, you cannot create a simple port match for the class. Instead, create a service group for TCP/5061 and UDP/5061, then use that object in an ACL.

e. Click **Next** to define the ACL.

f. Select the following ACL options:

- **Action = Match**.
- **Source** = any
- **Destination** = any

g. For **Destination Service**, click the ... button to open the Browse Service dialog box.

h. Click **Add** > **Service Group** , and configure the following:

- **Group Name** = Something meaningful, such as **sec_sip_ports**.
- Select **Create New Member**, select **tcp-udp** for **Service Type**, enter 5061 for **Destination Port/Range**, then click **Add>>**.
- Click **OK** to save the object. This returns you to the Browse Service dialog box.

i. Double-click the object you just created to select it and click **OK**.

The Add Service Policy Rule - Traffic Match dialog box should now show your object selected in the Destination Service field for the ACL.

j. Click **Next**.

k. On the **Rule Actions** > **Protocol Inspection** tab, select **SIP** and click the associated **Configure** button.

l. Configure the following SIP inspection options:

- If you configured an inspection map to customize SIP inspection, choose **Select a SIP Inspection Map**, then select your map. Otherwise, leave **Use the Default SIP Inspection Map** selected.
- Select **Enable Encrypted Traffic Inspection**, then select the TLS proxy you configured for SIP inspection.

m. Click **OK** to save the SIP inspection options.

n. Click **Finish** to save the SIP inspection service policy.

Step 3 Click **Apply** to write the new policies to the device.

Verifying TLS Proxy Setup for a Phone

You can verify that encrypted voice inspection is working by logging into the CLI and setting up tls-proxy debugging.

You can enable TLS proxy debug flags along with SSL syslogs to debug TLS proxy connection problems. For example, use the following commands to enable TLS proxy-related debug and syslog output only:

```
ciscoasa(config)# debug inspect tls-proxy events
ciscoasa(config)# debug inspect tls-proxy errors
ciscoasa(config)# logging enable
ciscoasa(config)# logging timestamp
ciscoasa(config)# logging list loglist message 711001
ciscoasa(config)# logging list loglist message 725001-725014
ciscoasa(config)# logging list loglist message 717001-717038
ciscoasa(config)# logging buffer-size 1000000
ciscoasa(config)# logging buffered loglist
ciscoasa(config)# logging debug-trace
```

The following is sample output reflecting a successful TLS proxy session setup for a SIP phone:

```
ciscoasa(config)# show log

Apr 17 2007 23:13:47: %ASA-6-725001: Starting SSL handshake with client
outside:133.9.0.218/49159 for TLSv1 session.
Apr 17 2007 23:13:47: %ASA-7-711001: TLSP cbad5120: Set up proxy for Client
outside:133.9.0.218/49159 <-> Server inside:195.168.2.201/5061
Apr 17 2007 23:13:47: %ASA-7-711001: TLSP cbad5120: Using trust point 'local_ccm' with the
Client, RT proxy cbae1538
Apr 17 2007 23:13:47: %ASA-7-711001: TLSP cbad5120: Waiting for SSL handshake from Client
outside:133.9.0.218/49159.
Apr 17 2007 23:13:47: %ASA-7-725010: Device supports the following 4 cipher(s).
Apr 17 2007 23:13:47: %ASA-7-725011: Cipher[1] : RC4-SHA
Apr 17 2007 23:13:47: %ASA-7-725011: Cipher[2] : AES128-SHA
Apr 17 2007 23:13:47: %ASA-7-725011: Cipher[3] : AES256-SHA
Apr 17 2007 23:13:47: %ASA-7-725011: Cipher[4] : DES-CBC3-SHA
Apr 17 2007 23:13:47: %ASA-7-725008: SSL client outside:133.9.0.218/49159 proposes the
following 2 cipher(s).
Apr 17 2007 23:13:47: %ASA-7-725011: Cipher[1] : AES256-SHA
Apr 17 2007 23:13:47: %ASA-7-725011: Cipher[2] : AES128-SHA
Apr 17 2007 23:13:47: %ASA-7-725012: Device chooses cipher : AES128-SHA for the SSL
session with client outside:133.9.0.218/49159
Apr 17 2007 23:13:47: %ASA-7-725014: SSL lib error. Function: SSL23_READ Reason: ssl
handshake failure
Apr 17 2007 23:13:47: %ASA-7-717025: Validating certificate chain containing 1
certificate(s).
Apr 17 2007 23:13:47: %ASA-7-717029: Identified client certificate within certificate
chain. serial number: 01, subject name: cn=SEP0017593F50A8.
Apr 17 2007 23:13:47: %ASA-7-717030: Found a suitable trustpoint
_internal_ejw-sv-2_cn=CAPF-08a91c01 to validate certificate.
Apr 17 2007 23:13:47: %ASA-6-717022: Certificate was successfully validated. serial
number: 01, subject name: cn=SEP0017593F50A8.
Apr 17 2007 23:13:47: %ASA-6-717028: Certificate chain was successfully validated with
warning, revocation status was not checked.
Apr 17 2007 23:13:47: %ASA-6-725002: Device completed SSL handshake with client
outside:133.9.0.218/49159
Apr 17 2007 23:13:47: %ASA-6-725001: Starting SSL handshake with server
inside:195.168.2.201/5061 for TLSv1 session.
```

```
Apr 17 2007 23:13:47: %ASA-7-725009: Device proposes the following 2 cipher(s) to server
inside:195.168.2.201/5061
Apr 17 2007 23:13:47: %ASA-7-725011: Cipher[1] : AES128-SHA
Apr 17 2007 23:13:47: %ASA-7-725011: Cipher[2] : AES256-SHA
Apr 17 2007 23:13:47: %ASA-7-711001: TLSP cbad5120: Generating LDC for client
'cn=SEP0017593F50A8', key-pair 'phone_common', issuer 'LOCAL-CA-SERVER', RT proxy cbae1538
Apr 17 2007 23:13:47: %ASA-7-711001: TLSP cbad5120: Started SSL handshake with Server
Apr 17 2007 23:13:47: %ASA-7-711001: TLSP cbad5120: Data channel ready for the Client
Apr 17 2007 23:13:47: %ASA-7-725013: SSL Server inside:195.168.2.201/5061 choose cipher :
AES128-SHA
Apr 17 2007 23:13:47: %ASA-7-717025: Validating certificate chain containing 1
certificate(s).
Apr 17 2007 23:13:47: %ASA-7-717029: Identified client certificate within certificate
chain. serial number: 76022D3D9314743A, subject name: cn=EJW-SV-2.inside.com.
Apr 17 2007 23:13:47: %ASA-6-717022: Certificate was successfully validated. Certificate
is resident and trusted, serial number: 76022D3D9314743A, subject name:
cn=EJW-SV-2.inside.com.
Apr 17 2007 23:13:47: %ASA-6-717028: Certificate chain was successfully validated with
revocation status check.
Apr 17 2007 23:13:47: %ASA-6-725002: Device completed SSL handshake with server
inside:195.168.2.201/5061
Apr 17 2007 23:13:47: %ASA-7-711001: TLSP cbad5120: Data channel ready for the Server
```

Monitoring the TLS Proxy

Use the **show tls-proxy** commands with different options to check the active TLS proxy sessions. In ASDM, you can issue the commands through the **Tools** > **Command Line Interface** dialog box. The following are some sample outputs:

```
ciscoasa(config-tlsp)# show tls-proxy
Maximum number of sessions: 1200
TLS-Proxy 'sip_proxy': ref_cnt 1, seq# 3
Server proxy:
Trust-point: local_ccm
Client proxy:
Local dynamic certificate issuer: LOCAL-CA-SERVER
Local dynamic certificate key-pair: phone_common
Cipher suite: aes128-sha1 aes256-sha1
Run-time proxies:
Proxy 0xcbae1538: Class-map: sip_ssl, Inspect: sip
Active sess 1, most sess 3, byte 3456043
ciscoasa(config-tlsp)# show tls-proxy session count
2 in use, 4 most used
ciscoasa(config-tlsp)# show tls-proxy session
2 in use, 4 most used
outside 133.9.0.218:49159 inside 195.168.2.201:5061 P:0xcbae1538(sip_proxy) S:0xcbad5120
byte 8786
ciscoasa(config-tlsp)# show tls-proxy session detail
2 in use, 4 most used
outside 133.9.0.218:49159 inside 195.168.2.201:5061 P:0xcbae1538(sip_proxy) S:0xcbad5120
byte 8786
Client: State SSLOK Cipher AES128-SHA Ch 0xca55e398 TxQSize 0 LastTxLeft 0 Flags 0x1
Server: State SSLOK Cipher AES128-SHA Ch 0xca55e378 TxQSize 0 LastTxLeft 0 Flags 0x9
Local Dynamic Certificate
Status: Available
Certificate Serial Number: 2b
Certificate Usage: General Purpose
Public Key Type: RSA (1024 bits)
Issuer Name:
cn=F1-ASA.default.domain.invalid
Subject Name:
```

```
cn=SEP0017593F50A8
Validity Date:
start date: 23:13:47 PDT Apr 16 2007
end date: 23:13:47 PDT Apr 15 2008
Associated Trustpoints:
```

Feature History for the TLS Proxy for Encrypted Voice Inspection

The following table lists the release history for this feature.

Table 1: Feature History for Cisco Phone Proxy

Feature Name	Releases	Feature Information
TLS Proxy	8.0(2)	The TLS proxy feature was introduced.
SIP, SCCP, and TLS Proxy support for IPv6	9.3(1)	You can now inspect IPv6 traffic when using SIP, SCCP, and TLS Proxy (using SIP or SCCP). We did not modify any commands. We did not modify any ASDM screens.
Support for Cisco Unified Communications Manager 8.6	9.3(1)	The ASA now interoperates with Cisco Unified Communications Manager Version 8.6 (including SCCPv21 support). We did not modify any commands. We did not modify any ASDM screens.
SIP support for Trust Verification Services, NAT66, CUCM 10.5, and model 8831 phones.	9.3(2)	You can now configure Trust Verification Services servers in SIP inspection. You can also use NAT66. SIP inspection has been tested with CUCM 10.5. We added the **trust-verification-server** parameter command. (ASDM) We added Trust Verification Services Server support to the SIP inspection policy map.

Feature Name	Releases	Feature Information
Support for TLSv1.2 in TLS proxy and Cisco Unified Communications Manager 10.5.2.	9.7(1)	You can now use TLSv1.2 with TLS proxy for encrypted SIP or SCCP inspection with the Cisco Unified Communications Manager 10.5.2. The TLS proxy supports the additional TLSv1.2 cipher suites added as part of the **client cipher-suite** command. We modified the following commands: **client cipher-suite**. (ASDM) We did not modify any screens.
Support for setting the TLS proxy server SSL cipher suite.	9.8(1)	You can now set the SSL cipher suite when the ASA acts as a TLS proxy server. Formerly, you could only set global settings for the ASA using the ssl-cipher command. In ASDM, this is on the **Configuration** > **Device Management** > **Advanced** > **SSL Settings** > **Encryption** page We added the following command: **server cipher-suite**. (ASDM) We modified the following pages: **Configuration** > **Firewall** > **Unified Communications** > **TLS Proxy Add/Edit** dialog boxes, **Server Configuration** page.
TLS proxy deprecated for SCCP (Skinny) inspection.	9.13(1)	The **tls-proxy** keyword, and support for SCCP/Skinny encrypted inspection, was deprecated. The keyword will be removed from the **inspect skinny** command in a future release.