Cisco ASA configuration

The Cisco Adaptive Security Appliance (ASA) firewall plays a key role in the security of the Cisco Intercompany Media Engine solution. This section contains information on configuring ASA using the command-line interface, as well as the ASDM, a web-based GUI application.

Proxy configuration guidelines and limits

Context Mode Guidelines

Supported in single context mode only.

Firewall Mode Guidelines

Supported in routed firewall mode only.

I**Pv6 Guidelines**

Does not support IPv6 addresses.

Additional Guidelines and Limitations

Cisco Intercompany Media Engine has the following limitations:

- Fax is not supported. Fax capability needs to be disabled on the SIP trunk.
- Stateful failover of Cisco Unified Intercompany Media Engine is not supported. During failover, existing calls traversing the Cisco Intercompany Media Engine Proxy disconnect; however, new calls successfully traverse the proxy after the failover completes.
- Having Cisco UCMs on more than one of the adaptive security appliance interfaces is not supported with the Cisco Intercompany Media Engine Proxy. Having the Cisco UCMs on one trusted interface is especially necessary in an off path deployment because the adaptive security appliance requires that you specify the listening interface for the mapping service and the Cisco UCMs must be connected on one trusted interface.
- Multipart MIME is not supported.

- Only existing SIP features and messages are supported.
- RTCP is not supported. The adaptive security appliance drops any RTCP traffic sent from the inside interface to the outside interface. The adaptive security appliance does not convert RTCP traffic from the inside interface into SRTP traffic.
- The Cisco Intercompany Media Engine Proxy configured on the adaptive security appliance creates a dynamic SIP trunk for each connection to a remote enterprise. However, you cannot configure a unique subject name for each SIP trunk. The Cisco Intercompany Media Engine Proxy can have only one subject name configured for the proxy.

  Additionally, the subject DN you configure for the Cisco Intercompany Media Engine Proxy match the domain name that has been set for the local Cisco UCM.
- If a service policy rule for the Cisco Intercompany Media Engine Proxy is removed (by using the no service policy command) and reconfigured, the first call traversing the adaptive security appliance will fail. The call fails over to the PSTN because the Cisco UCM does not know the connections are cleared and tries to use the recently cleared IME SIP trunk for the signaling.

  To resolve this issue, you must additionally enter the clear connection all command and restart the adaptive security appliance. If the failure is due to failover, the connections from the primary adaptive security appliance are not synchronized to the standby adaptive security appliance.
- After the clear connection all command is issued on an adaptive security appliance enabled with a UC-IME Proxy and the IME call fails over to the PSTN, the next IME call between an originating and terminating SCCP IP phone completes but does not have audio and is dropped after the signaling session is established.

  An IME call between SCCP IP phones use the IME SIP trunk in both directions. Namely, the signaling from the calling to called party uses the IME SIP trunk. Then, the called party uses the reverse IME SIP trunk for the return signaling and media exchange. However, this connection is already cleared on the adaptive security appliance, which causes the IME call to fail.

  The next IME call (the third call after the clear connection all command is issued), will be completely successful.

  Note This limitation does not apply when the originating and terminating IP phones are configured with SIP.
- The adaptive security appliance must be licensed and configured with enough TLS proxy sessions to handle the IME call volume. See the licensing requirements sections for TLS proxy sessions in the Cisco ASA 5500 Series Configuration Guide using the CLI.

  This limitation occurs because an IME call cannot fall back to the PSTN when there are not enough TLS proxy sessions left to complete the IME call. An IME call between two SCCP IP phones requires the adaptive security appliance to use two TLS proxy sessions to successfully complete the TLS handshake.

  Assume for example, the adaptive security appliance is configured to have a maximum of 100 TLS proxy sessions and IME calls between SCCP IP phones establish 101 TLS proxy sessions. In this example, the next IME call is initiated successfully by the originating SCCP IP phone but fails after the call is accepted by the terminating SCCP IP phone. The terminating IP phone rings and on answering the call, the call hangs due to an incomplete TLS handshake. The call does not fall back to the PSTN.

Proxy CLI configuration

Set up Cisco IME

The following tasks include command line examples based on the noted figure.

To configure a Cisco Intercompany Media Engine for a basic deployment, perform the following tasks.

Procedure

Step 1 Set up one of the following configurations:

- NAT for Cisco UCM. See Set up NAT for Cisco IME, on page 4.
- PAT for the UCM server. See Set up PAT for Cisco UCM server, on page 6.

Step 2 Create access lists for Cisco Intercompany Media Engine Proxy.
See Set up access lists for Cisco IME Proxy, on page 8.

Step 3 Create the media termination address instance for Cisco Intercompany Media Engine Proxy.
See Create media termination instance, on page 9.

Step 4 Create the Cisco Intercompany Media Engine Proxy.
See Create Cisco IME Proxy, on page 11.

Step 5 Create trustpoints and generate certificates for the Cisco Intercompany Media Engine Proxy.
See Create trustpoints and generate certificates, on page 13.

Step 6 Create the TLS proxy.
See Create TLS proxy, on page 15.

Step 7 Configure SIP inspection for the Cisco Intercompany Media Engine Proxy.
See Enable SIP inspection for the Cisco IME Proxy, on page 17.

Step 8 (Optional) Configure TLS within the enterprise.
See Set up TLS in local enterprise, on page 19.

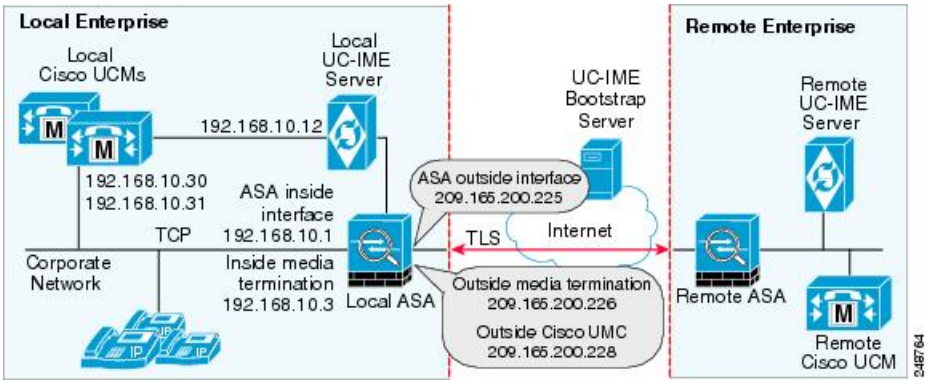
Step 9 (Optional) Configure off path signaling.
See Set up off path signalling, on page 22.

Note You only perform Step 9 when you are configuring the Cisco Intercompany Media Engine Proxy in an off path deployment.

Example for basic (in-line) deployment tasks

The following figure provides an example for a basic deployment of the Cisco Intercompany Media Engine.

Figure 1:



Note Step 1 through Step 8 apply to both basic (in-line) and off path deployments and Step 9 applies only to off path deployment.

Set up NAT for Cisco IME

To configure auto NAT, you first configure an object. You then use the **nat** command in the object configuration mode.

The example command lines in this task are based on a basic (in-line) deployment. Alternatively, you can configure PAT for the Cisco Intercompany Media Engine Proxy. See Set up PAT for Cisco UCM server, on page 6.

To configure auto NAT rules for the Cisco UCM server, complete the following steps:

Procedure

Step 1 Run the following command to set up a network object for the real address of Cisco UCM that you want to translate: `hostname(config)# object network name`

Example:

```
hostname(config)# object network ucm_real_1
```

Step 2 Run the following command to specify the real IP address of the Cisco UCM host for the network object:

```
hostname(config-network-object)# host ip_address
```

Example:

```
hostname(config-network-object)# host 192.168.10.30
```

Step 3 (Optional) Run the following command to provide a description of the network object:

```
hostname(config-network-object)# description string
```

Example:

```
hostname(config-network-object)# description "Cisco UCM #1 Real IP Address"
```

Step 4 Repeat steps 1 through 3 for any other Cisco UCM nodes that you want to translate.

Example:
object ucm_real_2 will contain host 192.168.10.31

Step 5 Run the following command to set up a network object for the outside (translated) addresses of Cisco UCMs:

```
hostname(config)# object network name
```

Example:

```
hostname(config) # object network ucm_map_1
```

Step 6 Run the following command to specify the translated IP address of the Cisco UCM host for the network object:

```
hostname(config-network-object)# host ip_address
```

Example:

```
hostname(config-network-object) # host 209.165.200.227
```

Step 7 (Optional) Run the following command to provide a description of the network object:
hostname(config-network-object)# description string `hostname(config-network-object)# description string`

Example:

```
hostname(config-network-object)# description "Cisco UCM Translated IP Address"
```

Step 8 Repeat steps 5 through 7 for any other Cisco UCM nodes that you want to translate.

Example:
object ucm_map_2 will contain host 209.165.200.228

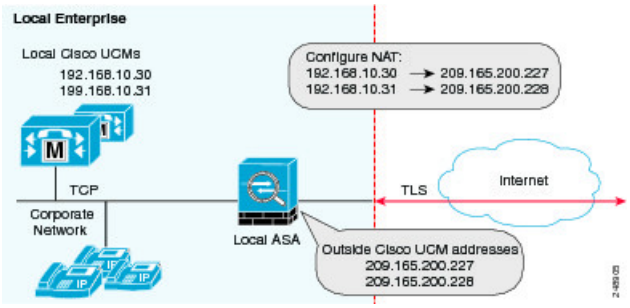
Step 9 Run the following command to specify the address translation on the network objects created in this example

Example:

```
hostname(config)# object network ucm_real_1

hostname(config-network-object)# nat (inside,outside) static ucm_map_1

hostname(config-network-object)# exit

hostname(config)# object network ucm_real_2

hostname(config-network-object)# nat (inside,outside) static ucm_map_2
```

Figure 2: Example for configuring NAT for a deployment

The following figure shows an example for a NAT deployment configuration.



What to Do Next

Create the access lists for the Cisco Intercompany Media Engine Proxy. See Set up access lists for Cisco IME Proxy, on page 8.

Set up PAT for Cisco UCM server

Perform this task as an alternative to configuring NAT for the Cisco Intercompany Media Engine Proxy.

To configure PAT for the Cisco UCM server, complete the following steps:

Procedure

Step 1 Run the following command to set up a network object for inbound Intercompany Media Engine calls:
`hostname(config)# object network name`

Example:
Example: `hostname(config)# object network ucm-pat-config1`

Step 2 Run the following command to specify the real IP address of the Cisco UCM host for the network object:
`hostname(config-network-object)# host ip_address`

Example:
Example: `hostname(config-network-object)# host 192.168.30`

Step 3 Run the following command to provide a description of the network object:
`hostname(config-network-object)# description string`

Example:
Example: `hostname(config-network-object)# description "PAT for Inbound Calls"`

Step 4 Run the following command to set up static PAT for inbound Intercompany Media Engine calls from the port configured on the outside network to the specified port on the inside network:
`hostname(config-network-object)# nat (inside,outside) static mapped_inline_ip service tcp real_port mapped_port`

Example:

Example: `hostname(config-network-object)# nat (inside,outside) static 209.165.200.228 service tcp 5570 5571`

Step 5 Run the following command to exit from the object configuration mode: `hostname(config-network-object)# exit`

Step 6 Run the following command to set up a network object for outbound Intercompany Media Engine calls: `hostname(config)# object network name`

Example:
Example: `hostname(config)# object network ucm-pat-config2`

Step 7 Run the following command to specify the subnet for the network object: `hostname(config-network-object)# subnet ip_address mask`

Example:
Example: `hostname(config-network-object)# host 192.168.10.0 255.255.255.0`

Step 8 Run the following command to provide a description of the network object: `hostname(config-network-object)# description string`

Example:
Example: `hostname(config-network-object)# description "PAT for Outbound Calls"`

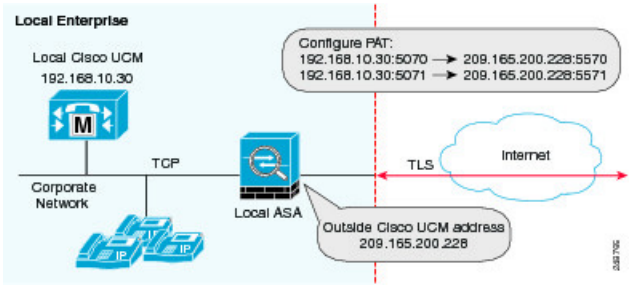
Step 9 Run the following command to set up dy namic PAT for outbound Intercompany Media Engine calls that hides the inside network behind the outside interface address: `hostname(config-network-object)# nat (inside,outside) dynamic ip_address`

Example:
Example: `hostname(config-network-object)# nat (inside,outside) dynamic 209.165.200.228`

Example for configuring PAT for a deployment

The following graphic shows an example PAT deployment configuration.

Note You only perform this step when NAT is not configured for the Cisco UCM server.



Set up access lists for Cisco IME Proxy

To configure access lists for the Cisco Intercompany Media Engine Proxy to reach the Cisco UCM server, perform the following steps.

The example command lines in this task are based on a basic (in-line) deployment. See the example for basic (in-line) deployment tasks graphic for an illustration explaining the example command lines in this task.

Complete the following steps to set up access lists of the Cisco IME Proxy:

Procedure

Step 1 Run the following command to add an Access Control Entry (ACE): `hostname(config)# access-list id extended permit tcp any host ip_address eq port`

Example:
Example: `hostname(config)# access-list incoming extended permit tcp any host 192.168.10.30 eq 5070`
An access list is made up of one or more ACEs with the same access list ID. This ACE provides access control by allowing incoming access for Cisco Intercompany Media Engine connections on the specified port.

In the ip_address argument, provide the real IP address of Cisco UCM.

Step 2 Run the following command to bind the access list to an interface: `hostname(config)# access-group access-list in interface interface_name`

Example:
Example: `hostname(config)# access-group incoming in interface outside`

Step 3 Run the following command to add and ACE to allow inbound SIP traffic: `hostname(config)# access-list id extended permit tcp any host ip_address eq port`

Example:
Example: `hostname(config)# access-list ime-inbound-sip extended permit tcp any host 192.168.10.30 eq 5070`
This ACE allows the adaptive security appliance to allow inbound SIP traffic for Cisco Intercompany Media Engine. This entry is used to classify traffic for the class and policy map.

Note The port that you configure here must match the trunk settings configured on Cisco UCM. See the Cisco Unified Communications Manager documentation for information about this configuration setting.

Step 4 Run the following command to add and ACE to allow outbound SIP traffic: `hostname(config)# access-list id extended permit tcp ip_address mask any range range`

Example:
Example: `hostname(config)# access-list ime-outbound-sip extended permit tcp 192.168.10.30 255.255.255.255 any range 5000 6000`
This ACE allows the adaptive security appliance to allow outbound SIP traffic for Cisco Intercompany Media Engine (in the example, any TCP traffic with source as 192.168.10.30 and destination port range between 5000 and 6000). This entry is used to classify traffic for the class and policy map.

Note Ensure that TCP traffic between Cisco UCM and the Cisco Intercompany Media Engine server does not use this port range (if that connection goes through the adaptive security appliance).

Step 5 Run the following command to add and ACE to allow remote server traffic: `hostname(config)# access-list id permit tcp any host ip_address eq 6084`

Example:
Example: `hostname(config)# access-list ime-traffic permit tcp any host 192.168.10.12 eq 6084`
This ACE allows the adaptive security appliance to allow traffic from the Cisco Intercompany Media Engine server to remote Cisco Intercompany Media Engine servers.

Step 6 Run the following command to add and ACE to allow traffic to the Bootstrap server: `hostname(config)# access-list id permit tcp any host ip_address eq 8470`

Example:
Example: `hostname(config)# access-list ime-bootserver-traffic permit tcp any host 192.168.10.12 eq 8470`
This ACE allows the adaptive security appliance to allow traffic from the Cisco Intercompany Media Engine server to the Bootstrap server for the Cisco Intercompany Media Engine.

What to Do Next

Create the media termination instance on the adaptive security appliance for the Cisco Intercompany Media Engine Proxy. See Create media termination instance, on page 9.

Create media termination instance

Note If you change any Cisco Intercompany Media Engine Proxy settings after you create the media-termination address for the proxy, you must reconfigure the media-termination address by using the no media-termination command, and then reconfiguring it as described in this procedure.

The example command lines in this task are based on a basic (in-line) deployment. See the example for basic (in-line) deployment tasks graphic for an illustration explaining the example command lines in this task.

To create the media termination instance for the Cisco Intercompany Media Engine Proxy, perform the following steps:

Before You Begin

The media termination address you configure must meet these requirements:

- If you decide to configure a media-termination address on interfaces (rather than using a global interface), you must configure a media-termination address on at least two interfaces (the inside and an outside interface) before applying the service policy for the Cisco Intercompany Media Engine Proxy. Otherwise, you will receive an error message when enabling the proxy with SIP inspection.

Note Cisco recommends that you configure the media-termination address for the Cisco Intercompany Media Engine Proxy on interfaces rather than configuring a global media-termination address.

- The Cisco Intercompany Media Engine Proxy can use only one type of media termination instance at a time; for example, you can configure a global media-termination address for all interfaces or configure a media-termination address for different interfaces. However, you cannot use a global media-termination address and media-termination addresses configured for each interface at the same time.

Procedure

Step 1 Run the following command to create the media termination instance that you attach to the Cisco Intercompany Media Engine Proxy: `hostname(config)# media-termination instance_name`

Example:
Example: `hostname(config)# media-termination uc-ime-media-term`

Step 2 Run the following command to set up the media-termination address used by the outside interface of the adaptive security appliance: `hostname(config-media-termination)# address ip_address interface intf_name`

Example:
Examples: `hostname(config-media-termination)# address 209.165.200.228 interface outside`
The outside IP address must be a publicly routable address that is an unused IP address within the address range on that interface.

See Create Cisco IME Proxy, on page 11 for information about the UC-IME proxy settings. See Cisco ASA 5500 Series Configuration Guide using the CLI for information about the no service-policy command.

Step 3 Run the following command to set up a media termination address used by the inside interface of the adaptive security appliance: `hostname(config-media-termination)# address ip_address interface intf_name`

Example:
Examples: `hostname(config-media-termination)# address 192.168.10.3 interface inside`
Note The IP address must be an unused IP address within the same subnet on that interface.

Step 4 (Optional) Run the following command to set up the rtp-min-port and rtp-max-port limits for the Cisco Intercompany Media Engine Proxy: `hostname(config-media-termination)# rtp-min-port port1 rtp-maxport port2`

Example:
Examples: `hostname(config-media-termination)# rtp-min-port 1000 rtp-maxport 2000`
Configure the RTP port range for the media termination point when you need to scale the number of calls that the Cisco Intercompany Media Engine supports.

Where port1 specifies the minimum value for the RTP port range for the media termination point, where port1 can be a value from 1024 to 65535. By default, the value for port1 is 16384.

Where port2 specifies the maximum value for the RTP port range for the media termination point, where port2 can be a value from 1024 to 65535. By default, the value for port2 is 32767.

What to Do Next

Once you have created the media termination instance, create the Cisco Intercompany Media Engine Proxy. See Create Cisco IME Proxy, on page 11.

Create Cisco IME Proxy

The example command lines in this task are based on a basic (in-line) deployment. See the example for basic (in-line) deployment tasks graphic for an illustration explaining the example command lines in this task.

Note You cannot change any of the configuration settings for the Cisco Intercompany Media Engine Proxy described in this procedure when the proxy is enabled for SIP inspection. Remove the Cisco Intercompany Media Engine Proxy from SIP inspection before changing any of the settings described in this procedure.

To create the Cisco Intercompany Media Engine Proxy, complete the following steps.

Procedure

Step 1 Run the following command to configure the Cisco Intercompany Media Engine Proxy: `hostname(config)# uc-ime uc_ime_name`

Example:
Example: `hostname(config)# uc-ime local-ent-ime`
Where `uc_ime_name` is the name of the Cisco Intercompany Media Engine Proxy. The name is limited to 64 characters. Only one Cisco Intercompany Media Engine Proxy can be configured on the adaptive security appliance.

Step 2 Run the following command to specify the media termination instance used by the Cisco Intercompany Media Engine Proxy: `hostname(config-uc-ime)# media-termination mta_instance_name`

Example:
Example: `hostname(config-uc-ime)# media-termination ime-media-term`
Where `mta_instance_name` is the `instance_name` that you created in Step 1 in Create media termination instance, on page 9.

Note You must create the media termination instance before you specify it in the Cisco Intercompany Media Engine Proxy.

Step 3 Run the following command to specify the Cisco UCM server in the enterprise: `hostname(config-uc-ime)# ucm address ip_address trunk-security-mode [nonsecure | secure]`

Example:
Example: `hostname(config-uc-ime)# ucm address 192.168.10.30 trunk-security-mode non-secure`

You must specify the real IP address of the Cisco UCM server. Do not specify a mapped IP address for the server. Where the nonsecure and secure options specify the security mode of the Cisco UCM or cluster of Cisco UCMs.

Note You must include an entry for each Cisco UCM in the cluster with Cisco Intercompany Media Engine that has a SIP trunk enabled.

Specifying secure for Cisco UCM or Cisco UCM cluster indicates that Cisco UCM or Cisco UCM cluster is initiating TLS; therefore, you must configure TLS for components. See Set up TLS in local enterprise, on page 19.

You can specify the secure option in this task or you can update it later while configuring TLS for the enterprise. See Step 11 in Set up TLS in local enterprise, on page 19.

Step 4 Run the following command to set up the ticket epoch and password for Cisco Intercompany Media Engine:

```
hostname(config-uc-ime)# ticket epoch n password password
```

Example:

Example: `hostname(config-uc-ime)# ticket epoch 1 password password1234`

Where `n` is an integer from 1-255. The epoch contains an integer that updates each time that the password is changed. When the proxy is configured the first time and a password entered for the first time, enter 1 for the epoch integer. Each time you change the password, increment the epoch to indicate the new password. You must increment the epoch value each time your change the password.

Typically, you increment the epoch sequentially; however, the adaptive security appliance allows you to choose any value when you update the epoch. If you change the epoch value, the current password is invalidated and you must enter a new password.

Where `password` contains a minimum of 10 and a maximum of 64 printable character from the US-ASCII character set. The allowed characters include 0x21 to 0x73 inclusive, and exclude the space character. We recommend a password of at least 20 characters. Only one password can be configured at a time.

The ticket password is stored onto flash. The output of the show running-config uc-ime command displays ***** instead of the password string.

Note The epoch and password that you configure on the adaptive security appliance must match the epoch and password configured on the Cisco Intercompany Media Engine server. See the Cisco Intercompany Media Engine server documentation for information.

Step 5 (Optional) Run the following command to specify the fallback timers for Cisco Intercompany Media Engine:

```
hostname(config-uc-ime)# fallback monitoring timer timer_millisec | hold-down timer timer_sec
```

Example:

Examples: `hostname(config-uc-ime)# fallback monitoring timer 120 hostname(config-uc-ime)# fallback hold-down timer 30`

Specifying monitoring timer sets the time between which the adaptive security appliance samples the RTP packets received from the Internet. The adaptive security appliance uses the data sample to determine if fallback to the PSTN is needed for a call.

Where `timer_millisec` specifies the length of the monitoring timer. By default, the length is 100 milliseconds for the monitoring timer and the allowed range is 10-600 ms. Specifying hold-down timer sets the amount of time that adaptive security appliance waits before notifying Cisco UCM whether to fall back to PSTN.

Where `timer_sec` specifies the length of the hold-down timer. By default, the length is 20 seconds for the hold-down timer and the allowed range is 10-360 seconds. If you do not use this command to specify fallback timers, the adaptive security appliance uses the default settings for the fallback timers.

Step 6 (Optional) Run the following command to specify the file to use for mid-call PSTN fallback:
`hostname(config-uc-ime)# fallback sensitivity-file file_name`

Example:
Example: `hostname(config-uc-ime)# fallback sensitivity-file ime-fallback-sensitvity.fbs`
Where `file_name` must be the name of a file on disk that includes the .fbs file extension.

The fallback file is used to determine whether the QoS of the call is poor enough for the Cisco Intercompany Media Engine to move the call to the PSTN.

What to Do Next

Install the certificate on the local entity truststore. You could also enroll the certificate with a local CA trusted by the local entity.

Create trustpoints and generate certificates

The example command lines in this task are based on a basic (in-line) deployment. See the example for basic (in-line) deployment tasks graphic for an illustration explaining the example command lines in this task.

Note This task instructs you on how to create trustpoints for the local enterprise and the remote enterprise and how to exchange certificates between these two enterprises. This task does not provide steps for creating trustpoints and exchanging certificates between the local Cisco UCM and the local adaptive security appliance. However, if you require additional security within the local enterprise, you must perform the optional task Set up TLS in local enterprise, on page 19. Performing that task allows for secure TLS connections between the local Cisco UCM and the local adaptive security appliance. The instructions in that task describe how to create trustpoints between the local Cisco UCM and the local adaptive security appliance.

To create the trustpoints and generate certificates, complete the following steps:

Before You Begin

To create a proxy certificate on the adaptive security appliance that is trusted by the remote entity, obtain a certificate from a trusted CA or export it from the remote enterprise adaptive security appliance.

To export the certificate from the remote enterprise, you enter the following command on the remote adaptive security appliance:

```
hostname(config)# crypto ca export trustpoint identity-certificate
```

The adaptive security appliance prompts displays the certificate in the terminal screen. Copy the certificate from the terminal screen. You will need the certificate text in Step 2 of this task.

Procedure

Step 1 Run the following command to creates the RSA keypair that can be used for the trustpoints: `hostname(config)# crypto key generate rsa label key-pair-label modulus size`

Example:
Example: `hostname(config)# crypto key generate rsa label local-ent-key modulus 2048`
On the local adaptive security appliance, creates the RSA keypair that can be used for the trustpoints. This is the keypair and trustpoint for the local entities signed certificate.

The modulus key size that you select depends on the level of security that you want to configure and on any limitations imposed by the CA from which you are obtaining the certificate. The larger the number that you select, the higher the security level will be for the certificate. Most CAs recommend 2048 for the key modulus size; however,

Note GoDaddy requires a key modulus size of 2048.

Step 2 Run the following command to enter the trustpoint configuration mode for the specified trustpoint so that you can create the trustpoint for the local entity: `hostname(config)# crypto ca trustpoint trustpoint_name`

Example:
Example: `hostname(config)# crypto ca trustpoint local_ent`
A trustpoint represents a CA identity and possibly a device identity, based on a certificate issued by the CA. Maximum name length is 128 characters.

Step 3 Run the following command to include the indicated subject DN in the certificate during enrollment: `hostname(config-ca-trustpoint)# subject-name X.500_name`

Example:
Example: `hostname(config-ca-trustpoint)# subject-name cn=Ent-local-domain-name**`

Note The domain name that you enter here must match the domain name that has been set for the local Cisco UCM. For information about how to configure the domain name for Cisco UCM, see the Cisco Unified Communications Manager documentation for information.

Step 4 Run the following command to specify the key pair whose public key is to be certified: `hostname(config-ca-trustpoint)# keypair keyname`

Step 5 Run the following command to indicate that you will use the copy and paste method of enrollment with this trustpoint (also known as manual enrollment): `hostname(config-ca-trustpoint)# enroll terminal`

Example:
Example: `hostname(config-ca-trustpoint)# keypair local-ent-key`

Step 6 Run the following command to exit from the CA Trustpoint configuration mode: `hostname(config-ca-trustpoint)# exit`

Step 7 Run the following command to startthe enrollment process with the CA: `hostname(config)# crypto ca enroll trustpoint`

Example:
Example: `hostname(config)# crypto ca enroll remote-ent % % Start certificate enrollment ... % The subject name in the certificate will be: % cn=enterpriseA % The fully-qualified domain name in the certificate will @ be: ciscoasa % Include the device serial number in the subject name? [yes/no]: no Display Certificate Request to terminal? [yes/no]: yes`
Where `trustpoint` is the same as the value you entered for trust point name in Step 2.

When the trustpoint is configured for manual enrollment (enroll terminal command), the adaptive security appliance writes a base-64-encoded PKCS10 certification request to the console and then displays the CLI prompt. Copy the text from the prompt.

Submit the certificate request to the CA, for example, by pasting the text displayed at the prompt into the certificate signing request enrollment page on the CA website.

When the CA returns the signed identity certificate, proceed to Step 8 in this procedure.

Step 8 Run the following command to import the signed certificate received from the CA in response to a manual enrollment request: `hostname(config)# crypto ca import trustpoint certificate`

Example:
Example: `hostname(config)# crypto ca import remote-ent certificate`
Where `trustpoint` specifies the trust point you created in Step 2. The adaptive security appliance prompts you to paste the base-64 formatted signed certificate onto the terminal.

Step 9 Run the following command to authenticate the third-party identity certificate received from the CA: `hostname(config)# crypto ca authenticate trustpoint`

Example:
Example: `hostname(config)# crypto ca authenticate remote-ent`
The identity certificate is associated with a trustpoint created for the remote enterprise.

The adaptive security appliance prompts you to paste the base-64 formatted identity certificate from the CA onto the terminal.

What to Do Next

Create the TLS proxy for the Cisco Intercompany Media Engine. See the Create TLS proxy, on page 15.

Create TLS proxy

Create TLS proxy instances for the local and remote entity initiated connections respectively. The entity that initiates the TLS connection is in the role of "TLS client." Because the TLS proxy has a strict definition of "client" and "server" proxy, two TLS proxy instances must be defined if either of the entities could initiate the connection.

The example command lines in this task are based on a basic (in-line) deployment. See the example for basic (in-line) deployment tasks graphic for an illustration explaining the example command lines in this task.

To create the TLS proxy, perform the following steps:

Procedure

Step 1 Run the following command to create the TLS proxy for the outbound connection: `hostname(config)# tls-proxy proxy_name`

Example:

Example: `hostname(config)# tls-proxy local_to_remote-ent`

Step 2 Run the following command to specify the trust point and associated certificate for outbound connections: `hostname(config-tlsp)# client trust-point proxy_trustpoint`

Example:
Example: `hostname(config-tlsp)# client trust-point local-ent`
Specifies the trust point and associated certificate that the adaptive security appliance uses in the TLS handshake when the adaptive security appliance assumes the role of the TLS client. The certificate must be owned by the adaptive security appliance (identity certificate).

Where `proxy_trustpoint` specifies the trust point defined by the **crypto ca trustpoint command** in Step 2 in Create trustpoints and generate certificates, on page 13.

Step 3 Run the following command to control the TLS handshake parameter for the cipher suite for outbound connections: `hostname(config-tlsp)# client cipher-suite cipher_suite`

Example:
Example: `hostname(config-tlsp)# client cipher-suite aes128-sha1 aes256-sha1 3des-sha1 null-sha1`
Where `cipher_suite` includes des-sha1, 3des-sha1, aes128-sha1, aes256-sha1, or null-sha1.

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. Use this command to achieve difference ciphers between the two TLS sessions. You should use AES ciphers with the Cisco UCM server.

Step 4 Run the following command to exit from the TLS proxy configuration mode: `hostname(config-tlsp)# exit`

Step 5 Run the following command to create the TLS proxy for inbound connections: `hostname(config)# tls-proxy proxy_name`

Example:
Example: `hostname(config)# tls-proxy remote_to_local-ent`

Step 6 Run the following command to specify the proxy trustpoint certificate presented during TLS handshake for inbound connections: `hostname(config-tlsp)# server trust-point proxy_trustpoint`

Example:
Example: `hostname(config-tlsp)# server trust-point local-ent`
The certificate must be owned by the adaptive security appliance (identity certificate).

Where `proxy_trustpoint` specifies the trust point defined by the **crypto ca trustpoint** command in Step 2 in Create trustpoints and generate certificates, on page 13.

Because the TLS proxy has strict definition of client proxy and server proxy, two TLS proxy instances must be defined if either of the entities could initiate the connection.

Step 7 Run the following command to control the TLS handshake parameter for the cipher suite for inbound connections: `hostname(config-tlsp)# client cipher-suite cipher_suite`

Example:
Example: `hostname(config-tlsp)# client cipher-suite aes128-sha1 aes256-sha1 3des-sha1 null-sha1`
Where `cipher_suite` includes des-sha1, 3des-sha1, aes128-sha1, aes256-sha1, or null-sha1.

Step 8 Run the following command to exit from the TSL proxy configuration mode: `hostname(config-tlsp)# exit`

Step 9 Run the following command to specify the encryption algorithms that the SSL/TLS protocol uses:
`hostname(config)# ssl encryption 3des-sha1 aes128-sha1 [algorithms]`
Specifying the 3des-shal and aes128-shal is required. Specifying other algorithms is optional.

Note The Cisco Intercompany Media Engine Proxy requires that you use strong encryption. You must specify this command when the proxy is licensed using a K9 license.

What to Do Next

Once you have created the TLS proxy, enable it for SIP inspection.

Enable SIP inspection for the Cisco IME Proxy

The example command lines in this task are based on a basic (in-line) deployment. See the example for basic (in-line) deployment tasks graphic for an illustration explaining the example command lines in this task.

Note If you want to change any Cisco Intercompany Media Engine Proxy settings after you enable SIP inspection, you must enter the no service-policy command, and then reconfigure the service policy as described in this procedure. Removing and reconfiguring the service policy does not affect existing calls; however, the first call traversing the Cisco Intercompany Media Engine Proxy will fail. Enter the clear connection command and restart the adaptive security appliance.

To enable SIP inspection for the Cisco Intercompany Media Engine Proxy, complete the following steps:

Procedure

Step 1 Run the following command to define a class for the inbound Cisco Intercompany Media Engine SIP traffic:
`hostname(config)# class-map class_map_name`

Example:
`hostname(config)# class-map ime-inbound-sip`

Step 2 Run the following command to identify the SIP traffic to inspect: `hostname(config-cmap)# match access-list access_list_name`

Example:
`hostname(config-cmap)# match access-list ime-inbound-sip`
Where the `access_list_name` is the access list you created in Step 3 of the task Set up access lists for Cisco IME Proxy, on page 8.

Step 3 Run the following command to exit from the class map configuration mode: `hostname(config-cmap)# exit`

Step 4 Run the following command to define a class for the outbound SIP traffic from Cisco Intercompany Media Engine: `hostname(config)# class-map class_map_name`

Example:

```
hostname(config)# class-map ime-outbound-sip
```

Step 5 Run the following command to identify which outbound SIP traffic to inspect: `hostname(config)# match access-list access_list_name`

Example:

```
hostname(config-cmap)# match access-list ime-outbound-sip
```

Where the `access_list_name` is the access list you created in Step 4 of the task Set up access lists for Cisco IME Proxy, on page 8.

Step 6 Run the following command to exit from the class map configuration mode: `hostname(config-cmap)# exit`

Step 7 Run the following command to define the policy map to which to attach the actions for the class of traffic: `hostname(config)# policy-map name`

Example:

```
hostname(config)# policy-map ime-policy
```

Step 8 Run the following command to assign a class map to the policy map so that you can assign actions to the class map traffic: `hostname(config-pmap)# class classmap_name`

Example:

```
hostname(config-pmap)# class ime-outbound-sip
```

Where `classmap_name` is the name of the SIP class map that you created in Step 1 in this task.

Step 9 Run the following command to enable the TLS proxy and Cisco Intercompany Media Engine Proxy for the specified SIP inspection session: `hostname(config-pmap-c)# inspect sip [sip_map] uc-ime <uc_ime_map> tls-proxy <proxy_name>`

Example:

```
hostname(config-pmap-c)# inspect sip uc-ime local-ent-ime tls-proxy local_to_remote-ent
```

Step 10 `hostname(config-cmap-c)# exit`
Exits from the policy map class configuration mode.

Step 11 Run the following command to assign a class map to the policy map so that you can assign actions to the class map traffic: `hostname(config-pmap)# class class_map_name hostname(config-pmap)# class ime-inbound-sip`
Where `classmap_name` is the name of the SIP class map that you created in Step 4 in this task.

Step 12 Run the following command to Enables the TLS proxy and Cisco Intercompany Media Engine Proxy for the specified SIP inspection session: `hostname(config-pmap-c)# inspect sip [sip_map] uc-ime <uc_ime_map> tls-proxy <proxy_name>`

Example:

```
hostname(config-pmap-c)# inspect sip uc-ime local-ent-ime tls-proxy remote_to_local-ent
```

Step 13 Run the following command to exit from the policy map class configuration mode: `hostname(config-pmap-c)# exit`

Step 14 Run the following command to exit from the policy map configuration mode: `hostname(config-pmap)# exit`

Step 15 Run the following command to enable the service policy for SIP inspection for all interfaces: `hostname(config)# service-policy policymap_name global`

Example:

```
hostname(config)# service-policy ime-policy global
```

Where `policymap_name` is the name of the policy map you created in Step 7 of this task.

See Create Cisco IME Proxy, on page 11 for information about the UC-IME proxy settings. See Cisco ASA 5500 Series Configuration Guide using the CLI for information about the no service-policy command.

What to Do Next

Once you have enabled the TLS proxy for SIP inspection, if necessary, configure TLS within the enterprise. See Set up TLS in local enterprise, on page 19.

Set up TLS in local enterprise

If the transport security for the Cisco Intercompany Media Engine trunk changes on Cisco UCM, it must be changed on the adaptive security appliance as well. A mismatch will result in call failure.

The adaptive security appliance does not support SRTP with non-secure IME trunks. The adaptive security appliance assumes SRTP is allowed with secure trunks. So “SRTP Allowed” must be checked for IME trunks if TLS is used. The adaptive security appliance supports SRTP fallback to RTP for secure IME trunk calls.

To configure TLS within the local enterprise, complete the following steps the local adaptive security appliance:

Before You Begin

On the local Cisco UCM, download the Cisco UCM certificate. See the Cisco Unified Communications Manager documentation for information. You will need this certificate when performing Step 6 of this procedure.

Procedure

Step 1 Run the following command to create an RSA key and trustpoint for the self-signed certificate:

```
hostname(config)# crypto key generate rsa label key-pair-label hostname(config)# crypto ca
trustpoint trustpoint_name hostname(config-ca-trustpoint)# enroll self
hostname(config-ca-trustpoint)# keypair keyname hostname(config-ca-trustpoint)# subject-name
x.500_name
```

Example:

```
hostname(config)# crypto key generate rsa label local-ent-key hostname(config)# crypto ca
trustpoint local-asa hostname(config-ca-trustpoint)# enroll self
hostname(config-ca-trustpoint)# keypair key-local-asa hostname(config-ca-trustpoint)#
subject-name cn=Ent-local-domain-name**., o="Example Corp"
```

Where `key-pair-label` is the RSA key for the local adaptive security appliance.

Where `trustpoint_name` is the trustpoint for the local adaptive security appliance.

Where keyname is key pair for the local adaptive security appliance.

Where `x.500_name` includes the X.500 distinguished name of the local adaptive security appliance, for example, `cn=Ent-local-domain-name**`.

Note The domain name that you enter here must match the domain name that has been set for the local Cisco UCM. For information about how to configure the domain name for Cisco UCM, see the Cisco Unified Communications Manager documentation for more information.

Step 2 Run the following command to exit from Trustpoint Configuration mode: `hostname(config-ca-trustpoint)# exit`

Step 3 Enroll the trustpoint before exporting the identity certificate. `(config mode) crypto ca enroll <trustpoint>` The trustpoint in this case is local-asa.

Step 4 Run the following command to export the certificate you created in Step 1: `hostname(config)# crypto ca export trustpoint identity-certificate`

Example:

```
hostname(config)# crypto ca export local-asa identity-certificate
```

The certificate contents appear on the terminal screen.

Copy the certificate from the terminal screen. This certificate enables Cisco UCM to validate the certificate that the adaptive security appliance sends in the TLS handshake.

On the local Cisco UCM, upload the certificate into the Cisco UCM trust store. See the Cisco Unified Communications Manager documentation for information.

Note The subject name you enter while uploading the certificate to the local Cisco UCM is compared with the X.509 Subject Name field entered on the SIP Trunk Security Profile on Cisco UCM. For example, Ent-local-domain-name was entered in Step 1 of this task; therefore, Ent-local-domain-name should be entered in the Cisco UCM configuration.

Step 5 Run the following command to create a trustpoint for local Cisco UCM: `hostname(config)# crypto ca trustpoint trustpoint_namehostname(config-ca-trustpoint)# enroll terminal`

Example:

```
hostname(config)# crypto ca trustpoint local-ent-ucm hostname(config-ca-trustpoint)# enroll terminal
```

Where `trustpoint_name` is the trustpoint for the local Cisco UCM.

Step 6 Run the following command to exit from Trustpoint Configuration mode: `hostname(config-ca-trustpoint)# exit`

Step 7 Run the following command to import the certificate from local Cisco UCM: `hostname(config)# crypto ca authenticate trustpoint`

Example:

```
hostname(config)# crypto ca authenticate local-ent-ucm
```

Where `trustpoint` is the trust point for the local Cisco UCM.

Paste the certificate downloaded from the local Cisco UCM. This certificate enables the adaptive security appliance to validate the certificate that Cisco UCM sends in the TLS handshake.

Step 8 Run the following command to update the TLS proxy for outbound connections: `hostname(config)# tls-proxy proxy_namehostname(config-tlsp)# server trust-point proxy_trustpoint hostname(config-tlsp)# client trust-point proxy_trustpoint hostname(config-tlsp)# client cipher-suite aes128-sha1 aes256-sha1 3des-sha1 null-sha1`

Example:

```
hostname(config)# tls-proxy local_to_remote-ent hostname(config-tlsp)# server trust-point
local-asa hostname(config-tlsp)# client trust-point local-ent hostname(config-tlsp)# client
cipher-suite aes128-sha1 aes256-sha1 3des-sha1 null-sha1
```

Where `proxy_name` is the name you entered in Step 1 of the task Create TLS proxy, on page 15.

Where `proxy_trustpoint` for the server trust point command is the trust point name for the local adaptive security appliance you entered in Step 1 of this procedure.

Where `proxy_trustpoint` for the client trust point command is the name you entered in Step 2 of the task Create trustpoints and generate certificates, on page 13.

Note In this step, you are creating different trust points for the client and the server.

Step 9 Run the following command to exit from TLS Proxy Configuration mode: `hostname(config-tlsp)# exit`

Step 10 Run the following command to update the TLS proxy for inbound connections: `hostname(config)# tls-proxy proxy_namehostname(config-tlsp)# server trust-point proxy_trustpoint hostname(config-tlsp)# client trust-point proxy_trustpoint hostname(config-tlsp)# client cipher-suite aes128-sha1 aes256-sha1 3des-sha1 null-sha1`

Example:

```
hostname(config)# tls-proxy remote_to_local-ent hostname(config-tlsp)# server trust-point
local-ent hostname(config-tlsp)# client trust-point local-asa hostname(config-tlsp)# client
cipher-suite aes128-sha1 aes256-sha1 3des-sha1 null-sha1
```

Where `proxy_name` is the name you entered in Step 5 of the task Create TLS proxy, on page 15.

Where `proxy_trustpoint` for the server trust point command is the name you entered in Step 2 of the task Create trustpoints and generate certificates, on page 13.

Where `proxy_trustpoint` for the client trust point command is the trust point name for the local adaptive security appliance you entered in Step 1 of this procedure.

Step 11 Run the following command to exit from TLS Proxy Configuration mode: `hostname(config-tlsp)# exit`

Step 12 Run the following command to update the Cisco Intercompany Media Engine Proxy for trunk security mode: `hostname(config)# uc-ime uc_ime_namehostname(config-uc-ime)# ucm address ip_address trunk-security-mode secure`

Example:

```
hostname(config)# uc-ime local-ent-ime hostname(config-uc-ime)# ucm address 192.168.10.30
trunk-security-mode secure
```

Where `uc_ime_name` is the name you entered in Step 1 of the task Create Cisco IME Proxy, on page 11.

Only perform this step if you entered non-secure in Step 3 of the task Create Cisco IME Proxy, on page 11.

What to Do Next

Once you have configured the TLS within the enterprise, if necessary, configure off path signaling for an off path deployment. See Set up off path signalling, on page 22.

Set up off path signalling

Off path signaling requires that outside IP addresses translate to an inside IP address. For the Cisco Intercompany Media Engine Proxy, the adaptive security appliance creates dynamic mappings for external addresses to the internal IP address. For inbound signaling and outbound signaling, address translation must be configured in the following ways.

For inbound signaling, the outside Cisco UCM address has to be routed to the outside interface of the adaptive security appliance. Therefore, you must configure the adaptive security appliance to translate the real Cisco UCM address to the outside address of the adaptive security appliance. The outside address of the adaptive security appliance must be routable. This ensures that the adaptive security appliance receives packets sent to the Cisco UCM.

Configuring this translation means that the source IP address of an inbound signaling packet is translated to the inside interface of the adaptive security appliance. Based the example in this topic, an inbound signaling packet from the remote adaptive security appliance:

Source10.10.0.24	Destination209.165.200.228	Translates to	Source10.10.0.24	Destination192.168.10.30

For outbound signaling, the Cisco UCM does not have an inbound packet with a translated source IP address to which it can reply when the Cisco UCM initiates a connection. To accommodate this situation, you must configure a mapping service on the adaptive security appliance. The mapping service translates the source IP address of future inbound signaling packets.

After you configure off path signaling, the adaptive security appliance mapping service listens on interface “inside” for requests. When it receives a request, it creates a dynamic mapping for the “outside” as the destination address.

In an off path deployment, inbound media packets and outbound media packets are routed based on the media termination address. For information about how the adaptive security appliance uses the media termination address to route media packets, see Create media termination instance, on page 9.

To configure off path signaling for the Cisco Intercompany Media Engine Proxy, perform the following steps:

Procedure

Step 1 Run the following command to create a network object to represent all outside addresses for the off path adaptive security appliance:`hostname(config)# object network name`

Example:
Example: `hostname(config)# object network outside-any`

Step 2 Run the following command to specifies the IP address of the subnet: `hostname(config-network-object)# subnet ip_address`

Example:

Example: `hostname(config-network-object)# subnet 0.0.0.0 0.0.0.0`

Step 3 Run the following command to create a mapping for the Cisco UCM of remote enterprises: `hostname(config-network-object)# nat (outside, inside) dynamic interface`

Step 4 Run the following command to exit from the objects configuration mode: `hostname(config-network-object)# exit`

Step 5 Run the following command to specify the Cisco Intercompany Media Engine Proxy: `hostname(config)# uc-ime uc_ime_name`

Example:
Example: `hostname(config)# uc-ime local-ent-ime`
Specifies the Cisco Intercompany Media Engine Proxy that you created in in the IME proxy creation task.

Where `uc_ime_name` is the name you specified in Step 1 of Create Cisco IME Proxy, on page 11.

Step 6 Run the following command to add the mapping service to the Cisco Intercompany Media Engine Proxy: `hostname(config-uc-ime)# mapping-service listening-interface interface_name [listening-port port] uc-ime-interface uc-ime-interface_name`

Example:
Example: `hostname(config-uc-ime)# mapping-service listening-interface inside listening-port 8060 uc-ime-interface outside`
Adds the mapping service to the Cisco Intercompany Media Engine Proxy for the off-path adaptive security appliance.

Specifies the interface and listening port for the adaptive security appliance mapping service.

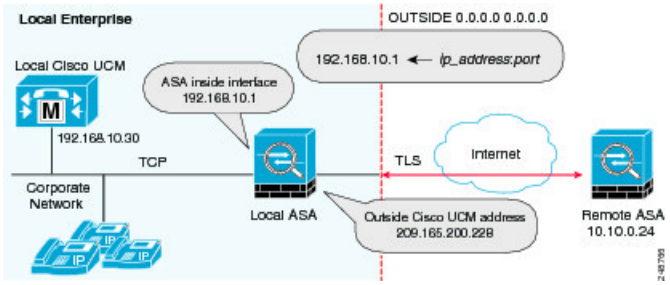
You can only configure one mapping service for the Cisco Intercompany Media Engine Proxy.

Where `interface_name` is the name of the interface on which the adaptive security appliance listens for the mapping requests.

Where port is the TCP port on which the adaptive security appliance listens for the mapping requests. The port number must be between 1024 and 65535 to avoid conflicts with other services on the device, such as Telnet or SSH. By default, the port number is TCP 8060.

Where `uc-ime-interface_name` is the name of the interface that connects to the remote Cisco UCM.

Example off-path signaling in an off-path deployment configuration



Proxy configuration using ASDM

Set up Cisco UC-IMC Proxy using proxy pane

Use the Configure Cisco Intercompany Media Engine (UC-IME) proxy pane to add or edit a Cisco Intercompany Media Engine Proxy instance.

Note The Cisco Intercompany Media Engine Proxy does not appear as an option under the Unified Communications section of the navigation pane unless the license required for this proxy is installed on the adaptive security appliance.

Use this pane to create the proxy instance; however, for the UC-IME proxy to be fully functionally, you must complete additional tasks, such as create the required NAT statements, access lists, and MTA, set up the certificates, create the TLS Proxy, and enable SIP inspection.

Depending on whether the UC-IME proxy is deployed off path or in-line of Internet traffic, you must create the appropriate network objects with embedded NAT/PAT statements for the Cisco UCMs.

Procedure

Step 1 Open the **Configuration** > **Firewall** > **Unified Communications** > **UC-IME Proxy** pane.

Step 2 Select the **Enable Cisco UC-IME** proxy checkbox to enable the feature.

Step 3 In the Unified CM Servers area, enter an IP address or hostname for the Cisco Unified Communications Manager (Cisco UCM) or click the ellipsis to open a dialog and browse for an IP address or hostname.

Step 4 In the **Trunk Security Mode** field, select a security option.
Specifying secure for Cisco UCM or Cisco UCM cluster indicates that Cisco UCM or Cisco UCM cluster is initiating TLS.

Step 5 Click **Add** to add the Cisco UCM for the Cisco Intercompany Media Engine Proxy.
You must include an entry for each Cisco UCM in the cluster with Cisco Intercompany Media Engine that has a SIP trunk enabled.

Step 6 In the **Ticket Epoch** field, enter an integer from 1-255.
The epoch contains an integer that updates each time that the password is changed. When the proxy is configured the first time and a password entered for the first time, enter 1 for the epoch integer. Each time you change the password, increment the epoch to indicate the new password. You must increment the epoch value each time your change the password.

Typically, you increment the epoch sequentially; however, the adaptive security appliance allows you to choose any value when you update the epoch.

If you change the epoch value, the current password is invalidated and you must enter a new password.

Note The epoch and password that you configure in this step on the adaptive security appliance must match the epoch and password that you configure on the Cisco Intercompany Media Engine server. See the Cisco Intercompany Media Engine server documentation for information.

Step 7 In the **Ticket Password** field, enter a minimum of 10 printable character from the US-ASCII character set.

The allowed characters include 0x21 to 0x73 inclusive, and exclude the space character. The ticket password can be up to 64 characters. Confirm the password you entered. Only one password can be configured at a time.

Step 8 Select the **Apply MTA to UC-IME Link** proxy checkbox to associate the media termination address with the Cisco Intercompany Media Engine Proxy.

Note You must create the media termination instance before you associate it with the Cisco Intercompany Media Engine Proxy. If necessary, click the Configure MTA button to configure a media termination address instance.

Step 9 If the Cisco Intercompany Media Engine Proxy is being configured as part of off path deployment, select the **Enable** off path address mapping service checkbox and configure the off path deployment settings:

- In the **Listening Interface** field, select an adaptive security appliance interface. This is the interface on which the adaptive security appliance listens for the mapping requests.
- In the **Port** field, enter a number between 1024 and 65535 as the TCP port on which the adaptive security appliance listens for the mapping requests. The port number must be 1024 or higher to avoid conflicts with other services on the device, such as Telnet or SSH. By default, the port number is TCP 8060.
- In the **UC-IME Interface** field, select an interface. This is the interface that the adaptive security appliance uses to connect to the remote Cisco UCM.

  Note In an off path deployment any existing adaptive security appliance that you have deployed in your environment are not capable of transmitting Cisco Intercompany Media Engine traffic. Off-path signaling requires that outside addresses are translated (using NAT) to an inside IP address. The inside interface address can be used for this mapping service configuration. For the Cisco Intercompany Media Engine Proxy, the adaptive security appliance creates dynamic mappings for external addresses to the internal IP address.

Step 10 In the Fallback area, configure the fallback timer for the Cisco Intercompany Media Engine by specifying the following settings:

- In the **Fallback Sensitivity File** field, enter the path to a file in flash memory that the adaptive security appliance uses for mid-call PSTN fallback. The file name that you enter must be the name of a file on disk that includes the .fbs file extension. Alternatively, click the Browse Flash button to locate and select the file from flash memory.
- In the **Call Quality Evaluation Interval** field, enter a number between 10-600 (in milliseconds). This number controls the frequency at which the adaptive security appliance samples the RTP packets received from the Internet. The adaptive security appliance uses the data sample to determine if fallback to the PSTN is needed for a call. By default, the length is 100 milliseconds for the timer.
- In the **Notification Interval** field, enter a number between 10-360 (in seconds). This number controls the amount of time that the adaptive security appliance waits before notifying Cisco UCM whether to fall back to PSTN. By default, the length is 20 seconds for this timer.

  Note When you change the fallback timer for the Cisco Intercompany Media Engine Proxy, ASDM automatically removes the proxy from SIP inspection and then reapplies SIP inspection when the proxy is re-enabled.

Step 11 Click **Apply** to save the configuration changes for the Cisco Intercompany Media Engine Proxy.

Set up Cisco UC-IMC proxy using Unified Communications Wizard

The wizard automatically creates the necessary TLS proxy, then guides you through creating the Intercompany Media Engine proxy, importing and installing the required certificates, and finally enables the SIP inspection for the Intercompany Media Engine traffic automatically.

The wizard guides you through these steps to create the Cisco Intercompany Media Engine Proxy:

Procedure

Step 1 Select the Intercompany Media Engine Proxy option.

Step 2 Select the topology of the Cisco Intercompany Media Engine Proxy.
The topology value determines whether the adaptive security appliance is an edge firewall with all Internet traffic flowing through it or whether the adaptive security appliance is off the path of the main Internet traffic (referred to as an off path deployment).

Step 3 Specify the private network settings such as the Cisco UCM IP addresses and the ticket settings.

Step 4 Specify the public network settings.

Step 5 Specify the media termination address settings of Cisco UCM.

Step 6 Configure the local-side certificate management.
You must determine the certificates that are exchanged between the local Cisco Unified Communications Manager servers and the adaptive security appliance. The identity certificate that the wizard generates in this step needs to be installed on each Cisco Unified Communications Manager (UCM) server in the cluster with the proxy and each identity certificate from the Cisco UCMs need to be installed on the adaptive security appliance. The certificates are used by the adaptive security appliance and the Cisco UCMs to authenticate each other, respectively, during TLS handshakes. The wizard only supports self-signed certificates for this step.

Step 7 Configure the remote-side certificate management,
You must determine the certificates that are exchanged between the remote server and the adaptive security appliance. In this step, the wizard generates a certificate signing request (CSR). After successfully generating the identity certificate request for the proxy, the wizard prompts you to save the file.

You must send the CSR text file to a certificate authority (CA), for example, by pasting the text file into the CSR enrollment page on the CA website. When the CA returns the Identity Certificate, you must install it on the adaptive security appliance. This certificate is presented to remote servers so that they can authenticate the adaptive security appliance as a trusted server.

This step of the wizard assists you in installing the root certificates of the CA from the remote servers so that the adaptive security appliance can determine that the remote servers are trusted.

The wizard completes by displaying a summary of the configuration created for Cisco Intercompany Media Engine. See the Unified Communications Wizard section in this documentation for more information.