TLS Proxy Configuration on the Cisco Adaptive Security Appliance

This section explains the TLS Proxy Configuration on the Cisco Adaptive Security Appliance.

TLS Proxy

The Cisco Adaptive Security Applianc acts as a TLS proxy between the IM and Presence Serivce and the external server. This allows the Cisco Adaptive Security Applianc to proxy TLS messages on behalf of the server (that initiates the TLS connection), and route the TLS messages from the proxy to the client. The TLS proxy decrypts, inspects and modifies the TLS messages as required on the incoming leg, and then re-encrypts traffic on the return leg.

Note Before configuring the TLS proxy, you must configure the Cisco Adaptive Security Applianc security certificates between the Cisco Adaptive Security Applianc and the IM and Presence Serivce, and between the Cisco Adaptive Security Applianc and the external server. Complete the procedures in the following sections to accomplish this:

- Security Certificate Exchange Between IM and Presence Service and Cisco Adaptive Security Appliance
- Security Certificate Exchange Between Cisco Adaptive Security Appliance and Microsoft Access Edge (External Interface) with Microsoft CA

Related Information

Common Cisco Adaptive Security Appliance Problems and Recommended Actions

Access List Configuration Requirements

This section lists the access list configuration requirements for a single IM and Presence Service deployment.

Note

- For each access list, you must configure a corresponding class-map, and configure an entry in the policy-map global policy.
- You can check the peer auth listener port on the IM and Presence Service by logging in to **Cisco Unified Communications Manager IM and Presence Administration** and choosing **System** > **Application Listeners**.

Table 1: Single IM and Presence Service Access List Configuration Requirements

Item	Description
Deployment Scenario: An IM and Presence Service node federating with one or more external domains	
Configuration Requirement:	Configure the following two access lists for each external domain that IM and Presence Service is federates with: • Configure an access list to allow the IM and Presence Service to send messages to the external domain on port 5061. • Configure an access list to allow the IM and Presence Service to receive messages from the external domain on port 5061. If you use the Cisco Adaptive Security Appliance Release 8.3, use the actual port that IM and Presence Service listens on for SIP federation (check the peer auth listener port on IM and Presence Service).
Configuration Example:	**access-list** *ent_imp_to_external_server* **extended permit tcp host** *routing_imp_private_address* **host** *external_public_address* **eq 5061** Cisco Adaptive Security Appliance Release 8.2: **access-list** *ent_external_server_to_imp* **extended permit tcp host** *external_public_address* **host** *imp_public_address* **eq 5061** Cisco Adaptive Security Appliance Release 8.3: **access-list** *ent_external_server_to_imp* **extended permit tcp host** *external_public_address* **host** *imp_private_address* **eq 5061** **Note** In the access list above 5061 is the port that the IM and Presence Service listens on for SIP messaging. If the IM and Presence Service listens on port 5062, specify 5062 in the access list.
Deployment Scenario: Intercluster deployment. This also applies to a multinode deployment.	

Item	Description
Configuration Requirement:	Configure the following two access lists for each intercluster IM and Presence Service node. • Configure an access list to allow the IM and Presence Service to send messages to the external domain on port 5061. • Configure an access list to allow the IM and Presence Service to receive messages from the external domain on the arbitrary port 5061. If you use Cisco Adaptive Security Appliance Release 8.3, use the actual port that the IM and Presence Service listens on for SIP federation (check the peer auth listener port on the IM and Presence Service).
Configuration Example:	**access-list** *ent_intercluster_imp_to_external_server* **extended permit tcp host** *intercluster_imp_private_address* **host external public address eq 5061** Cisco Adaptive Security Appliance Release 8.2: **access-list** *ent_external_server_to_intercluster_imp* **extended permit tcp host** *external_public_address* **host** *imp* **public address eq** *arbitrary_port* Cisco Adaptive Security Appliance Release 8.3: *ent_external_server_to_intercluster_imp* **extended permit tcp host** *external_public_address* **host** *imp_private_address* **eq** *5061* In the access list above, 5061 is the port that the IM and Presence Service listens on for SIP messaging. If the IM and Presence Service listens on port 5062, specify 5062 in the access list.

Related Information

Sample Cisco Adaptive Security Appliance Configuration

Configure TLS Proxy Instances

Associate Access List with TLS Proxy Instance Using Class Maps

Enable TLS Proxy

Configure TLS Proxy Instances

For this integration, you need to create two TLS proxy instances. The first TLS proxy handles the TLS connections initiated by the IM and Presence Service, where the IM and Presence Service is the client and the external domain is the server. In this case, the Cisco Adaptive Security Appliance acts as the TLS server facing the "client" which is the IM and Presence Service. The second TLS Proxy handles the TLS connections initiated by the external domain, where the external domain is the client and where the IM and Presence Service is the server.

The TLS proxy instance defines “trustpoints” for both the server and the client. The direction from which the TLS handshake is initiated determines the trustpoint defined in the server and client commands:

- If the TLS handshake initiates from the IM and Presence Service to the external domain, the server command specifies the trustpoint that contains the Cisco Adaptive Security Appliance self-signed certificate. The client command specifies the trustpoint that contains the Cisco Adaptive Security Appliance

certificate that is used in the TLS handshake between Cisco Adaptive Security Appliance and the external domain.

- If the handshake initiates from the external domain to the IM and Presence Service, the server command specifies the trustpoint that contains the Cisco Adaptive Security Appliance certificate the TLS handshake uses between the Cisco Adaptive Security Appliance and the external domain. The client command specifies the trustpoint that contains the Cisco Adaptive Security Appliance self-signed certificate.

Before you begin

- Complete the steps in Access List Configuration Requirements, on page 2.

Procedure

Step 1 Enter configuration mode:

```
> Enable
> <password>
> configure terminal
```

Step 2 Create a TLS proxy instance for TLS connections initiated by the IM and Presence Service. This example creates a TLS proxy instance called imp_to_external:

```
tls-proxy ent_imp_to_external
server trust-point imp_proxy
client trust-point trustpoint_name
client cipher-suite aes128-sha1 aes256-sha1 3des-sha1 null-sha1
```

Step 3 Create a TLS proxy instance for TLS connections initiated by a external domain. This example creates a TLS proxy instance called external_to_imp:

```
tls-proxy ent_external_to_imp
server trust-point trustpoint_name
client trust-point imp_proxy
client cipher-suite aes128-sha1 aes256-sha1 3des-sha1 null-sha1
```

What to do next

Associate Access List with TLS Proxy Instance Using Class Maps, on page 5

Associate Access List with TLS Proxy Instance Using Class Maps

Using the class map command, you need to associate a TLS Proxy instance to each of the external domain access lists you defined previously.

Before you begin

Complete the steps in Configure TLS Proxy Instances.

Procedure

Step 1 Enter configuration mode:

```
> Enable
> <password>
> configure terminal
```

Step 2 Associate each of your access lists with the TLS proxy instance that the class map uses. The TLS proxy you select depends on whether the class-map is for messages from the IM and Presence Service to an external domain, or from an external domain to the IM and Presence Service.

In the example below, the access list for messages sent from the IM and Presence Service to an external domain is associated with the TLS proxy instance for TLS connections initiated by the IM and Presence Service called “ent_imp_to_external”:

```
class-map ent_imp_to_external match access-list ent_imp_to_external
```

In the example below, the access list for messages sent from an external domain to the IM and Presence Service is associated with the TLS proxy instance for TLS connections initiated by the external server called "ent_external_to_imp":

```
class-map ent_external_to_imp match access-list ent_external_to_imp
```

Step 3 If you are have an intercluster IM and Presence Service deployment, configure a class map for each IM and Presence Service node, and associate this with the appropriate access-list for the server that you defined previously, for example:

```
class-map ent_second_imp_to_external match access-list ent_second_imp_to_external
class-map ent_external_to_second_imp match access-list ent_external_to_second_imp
```

What to do next

Enable TLS Proxy, on page 6

Enable TLS Proxy

Using the policy map command, you need to enable the TLS proxy for each class map you created in the previous section.

Note You cannot use a High security sip-inspect policy map on Cisco Adaptive Security Appliance for a federated deployment because the configuration fails. You must use a Low/Medium security policy map.

Before you begin

Complete the steps in Associate Access List with TLS Proxy Instance Using Class Maps.

Procedure

Step 1 Enter configuration mode:

```
> Enable
> <password>
> configure terminal
```

Step 2 Define the sip-inspect policy map, for example:

```
policy-map type inspect sip sip_inspectParameters
```

Step 3 Define the global policy map, for example:

```
policy-map global_policy class ent_cup_to_external inspect sip sip_inspect tls-proxy
ent_cup_to_external
```

Configure Cisco Adaptive Security Appliance for an Intercluster Deployment

For an intercluster IM and Presence Service deployment, you must perform the following configuration on the Cisco Adaptive Security Appliance for each additional IM and Presence Service node.

Procedure

Step 1 Create an additional access list for the IM and Presence Service.

Step 2 Generate and import the Cisco Adaptive Security Appliance security certificate onto the IM and Presence Service node.

Step 3 Generate and import the IM and Presence Service security certificate onto Cisco Adaptive Security Appliance.

Step 4 Configure a class map for each external domain.

Step 5 Include the class maps in the global policy map.

Related Information

Security Certified Exchange Between IM and Presence Service and Cisco Adaptive Security Appliance

Associate Access List with TLS Proxy Instance Using Class Maps

Enable TLS Proxy

Intercluster and Multinode Deployments