CHAPTER 6

Configuring the TLS Proxy on Cisco Adaptive Security Appliance

January 26, 2009

Note For up to date release information on configuring the TLS proxy, please refer to the Cisco Adaptive Security Appliance Configuration Guide at the following URL: http://www.cisco.com/en/US/products/ps6120/tsd_products_support_configure.html

TLS Proxy

Cisco Adaptive Security Appliance acts as a TLS proxy between the Cisco Unified Presence and the foreign server. This allows Cisco Adaptive Security Appliance 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 Appliance security certificates between Cisco Adaptive Security Appliance and Cisco Unified Presenceo, and Cisco Adaptive Security Appliance and the foreign server. Complete the procedures in the following sections to accomplish this:

- How to Configure Security Certificate Exchange Between Cisco Unified Presence and Cisco Adaptive Security Appliance, page 4-1
- How to Configure Security Certificate Exchange Between Cisco Adaptive Security Appliance and Microsoft Access Edge (External Interface) Using a Microsoft CA, page 4-5

Related Topics

Common Cisco Adaptive Security Appliance Problems and Recommended Actions, page 10-1.

Access List Configuration Requirements

Table 6-1 lists the access list configuration requirements for a single Cisco Unified Presence 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 Cisco Unified Presence by selecting **Cisco Unified Presence Administration > System > Application Listeners**.

Table 6-1 .Access List Configuration Requirements

Deployment Scenario	Configuration Requirement	Configuration Example

A Cisco Unified Presence server federating with one or more foreign domains	Configure the following two access lists for each foreign domain that Cisco Unified Presence is federates with:
	• Configure an access list to allow Cisco Unified Presence to send messages to the foreign domain on port 5061.
	• Configure an access list to allow Cisco Unified Presence to receive messages from the foreign domain on port 5061.
		`access-list ent_cup_to_foreign_server extended permit tcp host <routing cup private address> host <foreign public address> eq 5061`
		
		`access-list ent_foreign_server_to_cup extended permit tcp host <foreign public address> host < CUP public address> eq 5061`

Deployment Scenario	Configuration Requirement	Configuration Example

Intercluster deployment
 	
(This also applies to a multi-node deployment)
	Configure the following two access lists for each intercluster Cisco Unified Presence server.
	• Configure an access list to allow Cisco Unified Presence to send messages to the foreign domain on port (5061).
	• Configure an access list to allow Cisco Unified Presence to receive messages from the foreign domain on the arbitrary port.
		`access-list ent_intercluster_cup_to_foreign_server extended permit tcp host <intercluster cup private address> host <foreign public address> eq 5061`
		
		`access-list ent_foreign_server_to_intercluster_cup extended permit tcp host <foreign public address> host <cup public address> eq <arbitrary port>`

Cisco Unified Presence to Cisco Unified Presence Federation, where the foreign domain has added one or more intercluster Cisco Unified Presence servers	There are two configuration options:
	• For each intercluster Cisco Unified Presence server in the foreign domain, configure an access list to allow the local Cisco Unified Presence to send messages to the intercluster Cisco Unified Presence on the arbitrary port. Note that if you use this configuration option, you must retrieve the arbitrary port number from the system administrator of the foreign enterprise deployment.
	• Configure an access list to allow the local Cisco Unified Presence server access *any* port in the foreign domain.
		`access-list ent_cup_to_foreign_intercluster_cup extended permit tcp host <private routing cup> host <foreign company public cup address> eq <arbitrary port>.`
		
		`access-list ent_cup_to_foreign_interclustercup extended permit tcp host <private routing cup> host <foreign public cup address>`

Related Topics

- Sample Cisco Adaptive Security Appliance Configuration, page A-1
- Configuring the TLS Proxy Instances, page 6-3
- Associating an Access List with a TLS Proxy Instance Using Class Maps, page 6-4
- Enabling the TLS Proxy, page 6-5

Configuring the TLS Proxy Instances

For this integration, you need to create two TLS proxy instances. The first TLS proxy handles the TLS connections initiated by Cisco Unified Presence, where Cisco Unified Presence is the client and the foreign domain is the server. In this case, the Cisco Adaptive Security Appliance acts as the TLS server facing the "client" which is Cisco Unified Presence. The second TLS Proxy handles the TLS connections initiated by the foreign domain, where the foreign domain is the client and Cisco Unified Presence 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 Cisco Unified Presence to the foreign 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 foreign domain.
- If the handshake initiates from the foreign domain to Cisco Unified Presence, the server command specifies the trustpoint that contains the Cisco Adaptive Security Appliance certificate the TLS handshake uses between Cisco Adaptive Security Appliance and the foreign 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, page 6-2.

Procedure

Step 1 Enter config mode:

```
>Enable
>password
>config t
```

Step 2 Create a TLS proxy instance for TLS connections initiated by Cisco Unified Presence. This example creates a TLS proxy instance called cup_to_foreign:

```
tls-proxy ent_cup_to_foreign
server trust-point cup_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 foreign domain. This example creates a TLS proxy instance called foreign_to_cup:

```
tls-proxy ent_foreign_to_cup
server trust-point <trustpoint_name>
client trust-point cup_proxy
client cipher-suite aes128-sha1 aes256-sha1 3des-sha1 null-sha1
```

What To Do Next

Associating an Access List with a TLS Proxy Instance Using Class Maps, page 6-4

Associating an Access List with a TLS Proxy Instance Using Class Maps

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

Before You Begin

Complete the steps in Configuring the TLS Proxy Instances, page 6-3

Procedure

Step 1 Enter config mode:

```
>Enable
>password
>config t
```

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 Cisco Unified Presence to a foreign domain, or from a foreign domain to Cisco Unified Presence.

In the example below, the access list for messages sent from Cisco Unified Presence to a foreign domain is associated with the TLS proxy instance for TLS connections initiated by Cisco Unified Presence called “ent_cup_to_foreign”:

```
class-map ent_cup_to_foreign
    match access-list ent_cup_to_foreign
```

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

```
class-map ent_second_cup_to_foreign
    match access-list ent_second_cup_to_foreign
```

What To Do Next

Enabling the TLS Proxy, page 6-5

Enabling the 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 will fail. You must use a Low/Medium security policy map.

Before You Begin

Complete the steps in Associating an Access List with a TLS Proxy Instance Using Class Maps, page 6-4

Procedure

Step 1 Enter config mode:

```
>Enable
>password
>config t
```

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

```
policy-map type inspect sip sip_inspect
    Parameters
        !SIP Inspection Parameters
```

Step 3 Define the global policy map, for example:

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

Configuring Cisco Adaptive Security Appliance for an Intercluster Deployment

For an intercluster Cisco Unified Presence deployment, you must perform the following configuration on the Cisco Adaptive Security Appliance for **each additional** Cisco Unified Presence server.

Procedure

Step 1 Create an additional access list for the Cisco Unified Presence server.

Step 2 Generate and import the Cisco Adaptive Security Appliance security certificate onto the Cisco Unified Presence server.

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

Step 4 Configure a class map for each foreign domain.

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

Related Topics

- How to Configure Security Certificate Exchange Between Cisco Unified Presence and Cisco Adaptive Security Appliance, page 4-1
- How to Configure Security Certificate Exchange Between Cisco Unified Presence and Cisco Adaptive Security Appliance, page 4-1
- Associating an Access List with a TLS Proxy Instance Using Class Maps, page 6-4
- Enabling the TLS Proxy, page 6-5
- Intercluster and Multi-node Deployment, page 1-2