CHAPTER 8

Configuring the Load Balancer for Redundancy

January 26, 2009

About the Load Balancer

For redundancy and high-availability purposes, you can incorporate a load balancer into the federated network. Cisco recommends the Cisco CSS 11500 Content Services Switch, which is placed between the Cisco Unified Presence server and the Cisco Adaptive Security Appliance (see Figure 1-2 on page 1-4).

The load balancer terminates incoming TLS connections from Cisco Adaptive Security Appliance, and initiates a new TLS connection to route the content to the appropriate backend Cisco Unified Presence server.

Updating the Cisco Unified Presence Servers

When using a load balancer for redundancy, you must update settings on the Cisco Unified Presence publisher and subscriber nodes.

Procedure

Task	Procedure
Update the federation routing parameter	Select **Cisco Unified Presence Administration > System > Service Parameters** > **Cisco UP SIP Proxy** from the Service menu and enter these values: • **Virtual IP Address**—enter the virtual IP address set on the load balancer • **Server Name**—set to the FQDN of the load balancer • **Federation Routing CUP FQDN**—set to the FQDN of the load balancer.
Create a new TLS peer subject	1. Select **Cisco Unified Presence Administration > System > Security > TLS Peer Subjects**. 2. Click **Add New** and enter these values: • **Peer Subject Name**— enter the external FQDN of the load balancer • **Description**—enter the name of the load balancer
Add the TLS peer to the TLS peer subjects list	1. Select **Cisco Unified Presence Administration > System > Security > TLS Context Configuration**. 2. Click **Find**. 3. Click **Default_Cisco_UPS_SIP_Proxy_Peer_Auth_TLS_Context**. 4. Move the load balancer federation-TLS peer subject for the load balancer to the selected TLS peer subjects list.

Related Topics

- Configuring the Federation Routing Parameter, page 3-3
- Creating a new TLS Peer Subject, page 3-3
- Adding the TLS Peer to the Selected TLS Peer Subjects List, page 3-4
- How to Exchange Certificates Using CA-Signed Certificates, page C-3

How to Update the Cisco Adaptive Security Appliance

When using a load balancer, the foreign domain still sends messages to the public CUP address, but the Cisco Adaptive Security Appliance maps that address to a virtual IP address on the load balancer. Thus, when the Cisco Adaptive Security Appliance receives messages from the foreign domain, it forwards it to the load balancer. The load balancer then passes it on to the appropriate Cisco Unified Presence servers.

To support this configuration, you must make some changes to the Cisco Adaptive Security Appliance:

- Updating the Static PAT Messages, page 8-3
- Updating the Access Lists, page 8-4
- Updating the TLS Proxy Instances, page 8-5

Updating the Static PAT Messages

You must update the static PAT messages to include the load balancer details.

Procedure

Task	Configuration Example
Changes Required for Cisco Unified Presence Publisher	
Change the static PAT to use an arbitrary, unused port for the public CUP address.	Change: `static (inside,outside) tcp <Public CUP IP address> 5061 <Routing CUP private IP address> 5062 netmask 255.255.255.255` to: `static (inside,outside) tcp <Public CUP IP address> 55061 <Routing CUP/Publisher private IP address> 5062 netmask 255.255.255.255`
Add a new static PAT to allow messages sent to the public Cisco Unified Presence address to be forwarded to the virtual port address (on whichever port the load balancer is listening for TLS messages).	`static (inside,outside) tcp <Public CUP address> 5061 <Load Balancer VIP> 5062 netmask 255.255.255.255.`
Changes Required for Cisco Unified Presence Subscriber	
Add a new access list for the load balancer virtual IP address. You must add an access list for each foreign domain that Cisco Unified Presence needs to access.	`access-list ent_lber_to_foreign_ocs extended permit tcp host <subscriber private ip address> host <foreign domain public IP address> 5061`
Add a new access list for a foreign domain to initiate messages to a Cisco Unified Presence server when the load balancer virtual IP address is in place. You must add an access list for each foreign domain that needs to access Cisco Unified Presence.	`access-list ent_lcs_to_lber_routgcup extended permit tcp host <foreign domain public ip address> host <cup public ip address> 65061`

Related Topics

- Configuring the Static IP Routes, page 5-2
- About Port Address Translation (PAT), page 5-3

Updating the Access Lists

To support the load balancer, you also need to update the access lists on the Cisco Adaptive Security Appliance specific to your deployment scenario.

Procedure

Deployment Scenario	Task	Configuration Example
A Cisco Unified Presence server federating with one or more foreign domains	Add a new access list for the new load balancer virtual IP address. You must add an access list for each foreign domain that Cisco Unified Presence needs to access.	Publisher: access-list ent_lber_to_foreign_ocs extended permit tcp host <Virtual IP address> host <foreign domain public IP address> 5061 Subscriber: access-list ent_lber_to_foreign_ocs extended permit tcp host <subscriber private ip address> host <foreign domain public IP address> 5061
	Add a new access list for a foreign domain to initiate messages to a Cisco Unified Presence server when the load balancer virtual IP address is in place. You must add an access list for each foreign domain that needs to access Cisco Unified Presence.	Publisher: access-list ent_lcs_to_lber_routgcup extended permit tcp host <foreign domain public ip address> host <cup public ip address> eq 55061 Subscriber: access-list ent_lcs_to_lber_routgcup extended permit tcp host <foreign domain public ip address> host <cup public ip address> eq 65061
	For each access list, add a new class to incorporate the new access list.	class ent_lber_to_foreign_ocs match access-list ent_lber_to_foreign_ocs
	For each class, make an entry in the policy-map global_policy for messages initiated by Cisco Unified Presence.	policy-map global_policy class ent_lber_to_foreign_ocs inspect sip sip_inspect tls-proxy ent_cup_to_foreign
	For each class, make an entry in the policy-map global_policy for messages initiated on a foreign domain.	policy-map global_policy class ent_lcs_to_lber_routgcup inspect sip sip_inspect tls-proxy ent_foreign_to_cup
Cisco Unified Presence to Cisco Unified Presence Federation, where the foreign domain has added one or more intercluster Cisco Unified Presence servers	The foreign domain ASA must allow access to the arbitrary ports which have been chosen for our local domain publisher and the subscriber.	access-list ent_cup_to_foreignPubcupwlber extended permit tcp host <foreign domain private CUP address> host <public CUP address of our local domain> 55061 access-list ent_cup_to_foreignSubcupwlber extended permit tcp host <foreign domain private CUP address> host <public CUP address of our local domain> 65061
	For each access list, add a new class to incorporate the new access list.	
	For each class, make an entry in the policy-map global_policy.	

Related Topics

- Access List Configuration Requirements, page 6-2

Updating the TLS Proxy Instances

Update the TLS proxy instances on the Cisco Adaptive Security Appliance.

Procedure

Task	Configuration Example

Update TLS-PROXY	Change
	`tls-proxy ent_foreign_to_cup`
	` server trust-point msoft_publicfqdn`
	` client trust-point cup_proxy`
	` client cipher-suite aes128-sha1 aes256-sha1 3des-sha1 null-sha1`
	`!`
	`tls-proxy ent_cup_to_foreign`
	` server trust-point cup_proxy`
	` client trust-point msoft_publicfqdn`
	` client cipher-suite aes128-sha1 aes256-sha1 3des-sha1 null-sha1`
	to:
	`tls-proxy ent_foreign_to_cup`
	` server trust-point msoft_publicfqdn`
	` client trust-point msoft_publicfqdn`
	` client cipher-suite aes128-sha1 aes256-sha1 3des-sha1 null-sha1`
	`!`
	`tls-proxy ent_cup_to_foreign`
	` server trust-point msoft_publicfqdn`
	` client trust-point msoft_publicfqdn`
	` client cipher-suite aes128-sha1 aes256-sha1 3des-sha1 null-sha1`

Related Topics

- Configuring the TLS Proxy Instances, page 6-3

How to Update the CA-Signed Security Certificates

When adding the load balancer to the configuration, you must also generate CA-signed security certificates between the load balancer and the Cisco Adaptive Security Appliance and Cisco Unified Presence server as described in these sections:

- Configuring the Security Certificate between the Load Balancer and the Cisco Adaptive Security Appliance, page 8-6
- Configuring the Security Certificate between the Load Balancer and the Cisco Unified Presence Server, page 8-7

Configuring the Security Certificate between the Load Balancer and the Cisco Adaptive Security Appliance

This topic provides an overview of the required steps for configuring the security certificate between the load balancer and the Cisco Adaptive Security Appliance. For details, refer to Cisco CSS 11500 Content Services Switch documentation: http://www.cisco.com/en/US/products/hw/contnetw/ps792/products_installation_and_configuration_guides_list.html

Procedure

Task	Procedure
Generate CA-signed certificate for the load balancer on the Cisco Adaptive Security Appliance.	Use the `crypto ca enroll` command and specify the FQDN of the load balancer.
Import the CA-signed certificate from the Cisco Adaptive Security Appliance to the load balancer..	Use the `copy ssl` command.
Generate a CA-signed certificate for the Cisco Adaptive Security Appliance on the load balancer..	These steps provide an overview but refer to the *CSS SSL Configuration Guide* for details: **1.** Enter global configuration mode (`config`). **2.** Generate the RSA key pair used in the exhange (`ssl genrsa`). **3.** Associate the generated RSA key pair with a file (`ssl associate`) **4.** Generate the Certificate Signing Request (`ssl gencsr`). **5.** Obtain a root CA certificate from the CA. **6.** Transfer the CSR to the CA. **7.** Re-import the signed cert into the load balancer (`copy ssl` and `ssl associate`).
Import the CA-signed certificate from the load balancer to the Cisco Adaptive Security Appliance	Use the `crypto ca trustpoint` command. To verify that the certificate was imported, use the `show crypto ca certificate` command.

Related Topics

- Configuring the Certificate on Cisco Adaptive Security Appliance using SCEP Enrollment, page 4-6
- Importing the Cisco Unified Presence Certificate onto Cisco Adaptive Security Appliance, page 4-4
- How to Configure Security Certificate Exchange Between Cisco Adaptive Security Appliance and Microsoft Access Edge (External Interface) Using a Microsoft CA, page 4-5
- How to Exchange Certificates Using CA-Signed Certificates, page C-3

Configuring the Security Certificate between the Load Balancer and the Cisco Unified Presence Server

This topic provides an overview of the required steps for configuring the security certificate between the load balancer and the Cisco Unified Presence nodes.

Procedure

Task	Procedure
Generate a CA-signed certificate on both the publisher and subscriber nodes.	Need to add xref to the procedure
Import the CA-signed certificates (from the publisher and subscriber nodes) to the load balancer	Use the `copy ssl` and `ssl associate` commands.

Related Topics

- How to Exchange Certificates Using CA-Signed Certificates, page C-3

Updating the Microsoft Components

You must update some Microsoft components with the load balancer details.

Procedure

Task	Procedure
Update all instances of the FQDN to correspond to the load balancer FQDN.	
Update the domain name in the IM Provider list with the load balancer.	1. Select **Start > Administrative Tools > Computer Management** on the external Access Edge server. 2. Right-click **Microsoft Office Communications Server 2007** in the left pane. 3. Click the **IM Provider** tab. 4. Click **Add**. 5. Check **Allow the IM service provider**. Define the network address of the IM service provider as the public FQDN of the Load Balancer

Related Topics

- Configuring the Microsoft Components for Federation, page 7-1

Configuring the Load Balancer

This topic gives an overview of the necessary tasks for configuring the Cisco CSS 11500 Content Services Switch for this integration. The Cisco CSS 11500 Content Services Switch must have an SSL Accelerator Module installed and configured in back-end SSL mode.For detailed information on each task, refer to the Cisco CSS 11500 Content Services Switch documentation at the following URL:

http://www.cisco.com/en/US/products/hw/contnetw/ps792/products_installation_and_configuration_guides_list.html

Procedure

Task	Additional Notes
Configure certificate exchange between Cisco CSS 11500 Content Services Switch and Cisco Unified Presence.	• CA or self-signed certificates can be used in the SSL module. • You need to generate a certificate for the Cisco CSS 11500 Content Services Switch, and import this onto the remote server. • You need to import the certificate from the remote server onto the Cisco CSS 11500 Content Services Switch.
Configure certificate exchange between Cisco CSS 11500 Content Services Switch and Cisco Adaptive Security Appliance.	
You must define a virtual SSL server in an SSL proxy list for an SSL module to properly process and terminate SSL communications from the client and initiate a HTTP connection to the server.	• You must specify the IP address and port number that the Cisco Adaptive Security Appliance points to. • You must specify the name of the existing certificate and key pair for the Cisco Adaptive Security Appliance.
Create a Back-End SSL server entry in SSL Proxy List for each Cisco Unified Presence server.	• You must specify the Cisco Unified Presence server address. Note that the Cisco Unified Presence servers (back-end servers) must be on a different subnet than the VIP address. • The back-end server connection can be a different TLS cipher suite than the front-end, or can be TCP. • You must specify the port to receive the TLS traffic on the Cisco CSS 11500 Content Services Switch. • You must specify the port to send the TLS traffic to the Cisco Unified Presence servers.
Create an SSL service for SSL termination for each Cisco Unified Presence server.	• When specifying the keepalive port, ensure that the port number is the same as those you configured for the Back-End SSL server entries. • The keepalive message type value should be ‘tcp’.
Create the SSL module.	• You must specify the physical slot number of the SSL module. Use the CSS command ‘show chassis’ to retrieve this slot number. • In the SSL module you must associate a Cisco Unified Presence server with an SSL service, for example add ssl-proxy-list called **ssl_list1**.

Task	Additional Notes
Create an internal content rule to route the decrypted data from the ASA to CUP server.	
Create content rule to route TLS data to the SSL module for decryption and load-balancing.	
Create a NAT association between the VIP and the back-end Cisco Unified Presence servers.	
When using a Cisco CSS 11500 Content Services Switch directly between Cisco Unified Presence and Microsoft OCS (no Cisco Adaptive Security Appliance), you must be able to resolve the certificate Subject Common Name for the Cisco Unified Presence server to Cisco Unified Presence IP address from OCS. Also each Cisco Unified Presence server Subject Common Name must be in the OCS host authorization list.	