Load Balancer Configuration for Redundancy for SIP Federation

This section explains the Load Balancer Configuration for Redundancy for SIP Federation.

About the Load Balancer

For redundancy and high availability purposes, you can incorporate a load balancer into the federated network. The load balancer is placed between the IM and Presence Service node and the Cisco Adaptive Security Appliance (see High Availability for SIP Federation).

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 IM and Presence Service node.

IM and Presence Service Node Updates

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

Procedure

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

Cisco Adaptive Security Appliance Updates

When using a load balancer, the external domain still sends messages to the public IM and Presence Service 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 external domain, it forwards it to the load balancer. The load balancer then passes it on to the appropriate IM and Presence Service nodes.

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

Static PAT Message Updates

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

Procedure

Task	Cisco Adaptive Security Appliance Release 8.2 Command	Cisco Adaptive Security App
Changes Required for the IM and Presence Service Publisher		

Task	Cisco Adaptive Security Appliance Release 8.2 Command	Cisco Adaptive Security
Change the static PAT to use an arbitrary, unused port for the public IM and Presence Service address.	Change: **static (inside,outside) tcp** *public_imp_ip_address 5061 routing_imp_private_ip_address 5062* **netmask** *255.255.255.255* to: **static (inside,outside) tcp** *public_imp_ip_address 55061 routing_imp_publisher_ private_ip_address 5062* **netmask** *255.255.255.255*	Change: **object service** *obj_tc 5061* **nat (inside,outside)** *obj_host_routing_imp_ obj_host_public_imp_i obj_tcp_source_eq_506* to **object service** *obj_tc 55061* **nat (inside,outside)** *obj_host_routing_imp_ obj_host_public_imp_i obj_tcp_source_eq_550*
Add a new static PAT to allow messages sent to the public IM and Presence Service 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_imp_address 5061 load_balancer_vip 5062* **netmask** *255.255.255.255*	**object network** *obj_hc routing_imp_private_a* **object service** *obj_tc 5061* **nat (inside,outside)** *obj_host_public_imp_i obj_tcp_source_eq_506*
Changes Required for IM and Presence Service Subscriber		
Add a new access list for the load balancer virtual IP address. You must add an access list for each external domain that IM and Presence Service needs to access.	**access-list** *ent_lber_to_external_ocs* **extended permit tcp host** *external_domain_public_ip_address 5061* **access-list** *ent_lcs_to_lber_routg_imp* **extended permit tcp hos** *imp_public_ip_address 65061*	
Add a new access list for a **extended permit tcp hos**external domain to initiate messages to a IM and Presence Service server when the load balancer virtual IP address is in place. You must add an access list for each external domain that needs to access IM and Presence Service.		

Related Topics

Configure Static IP Routes
Port Address Translation (PAT)

Access List Updates

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

Note The IM and Presence Service public IP address refers to the public IP address of the IM and Presence Service domain as configured on the Cisco Adaptive Security Appliance, and as it appears in the DNS record. This record shows the FQDN of the load balancer containing the public IP of the Cisco Adaptive Security Appliance.

Procedures

Deployment Scenario: An IM and Presence Service node federating with one or more external domains

Task	Configuration Example
Add a new access list for the new load balancer virtual IP address. You must add an access list for each external domain that IM and Presence Service needs to access.	Publisher: Cisco Adaptive Security Appliance Release 8.2 and 8.3 Commar **access-list** *ent_lber_to_external_ocs* **extended permit t** **host** *external_domain_public_ip_address* **eq 5061**
Add a new access list for an external domain to initiate messages to a IM and Presence Service node when the load balancer virtual IP address is in place. You must add an access list for each external domain that needs to access IM and Presence Service.	Publisher: Cisco Adaptive Security Appliance Release 8.2 Command: **access-list** *ent_lcs_to_lber_routgimp* **extended permit t** *external_domain_public_ip_address* **host** *imp_public_ip_a* Cisco Adaptive Security Appliance Release 8.3 Command: **access-list** *ent_external_server_to_lb* **extended permit** *external_public_address* **host** *loadbalancer_virtual_ip_a*
For each access list, add a new class to incorporate the new access list.	**class** *ent_lber_to_external_ocs* **match access-list** *ent_l*
For each class, make an entry in the policy-map global_policy for messages initiated by the IM and Presence Service.	**policy-map global_policy class** *ent_lber_to_external_oc* **tls-proxy** *ent_imp_to_external*
For each class, make an entry in the policy-map global_policy for messages initiated on an external domain.	**policy-map global_policy class** *ent_lcs_to_lber_routgim* **tls-proxy** *ent_external_to_imp*

Deployment Scenario:IM and Presence Service to IM and Presence Service Federation, where the external domain has added one or more intercluster IM and Presence Service nodes

Task	Configuration Example
The external domain Adaptive Security Appliance must allow access to the arbitrary ports that were selected for our local domain publisher and subscriber.	**access-list** *ent_imp_to_externalPubimpwlber* **extended pe** *external_domain_private_imp_address* **host** *public_imp_ad* **access-list** *ent_imp_to_externalSubimpwlber* **extended pe** *external_domain_private_imp_address* **host** *public_imp_ad*

Task	Configuration Example
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 Information -

Access List Configuration Requirements

TLS Proxy Instance Updates

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

Procedure

Change:

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

to:

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

Related Topics

Configure TLS Proxy Instances

CA-Signed Security Certificate Updates

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

Security Certificate Configuration Between the Load Balancer and 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.

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 FQDI
Import the CA-signed certificate from the Cisco Adaptive Security Appliance to the load balancer.	Refer to your load balancer documentation.
Generate a CA-signed certificate for the Cisco Adaptive Security Appliance on the load balancer.	Refer to your load balancer documentation.
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 cry` command.

Related Information -

Configure a Certificate on the Cisco Adaptive Security Appliance Using SCEP

Import an IM and Presence Service Certificate into the Cisco Adaptive Security Appliance

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

Security Certificate Configuration Between the Load Balancer and IM and Presence Service Node

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

Task	Procedure
Generate a CA-signed certificate on both the publisher and subscriber nodes.	Follow the instructions to exchange certificates using CA-signed cert
Import the CA-signed certificates (from the publisher and subscriber nodes) to the load balancer	Refer to your load balancer documentation.

Microsoft Component Updates

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. On the external Access Edge server, choose **Start** > **Administ** **Computer Management**. 2. In the left pane, right-click **Microsoft Office Communications** 3. Click the **IM Provider** tab. 4. Click **Add**. 5. Check the check box for **Allow the IM service provider**. Define the network address of the IM service provider as the pub the load balancer

Related Topics

External Server Component Configuration for SIP Federation