Preparation for this Integration

This section explains the preparations to be made for this integration.

Supported Interdomain Federation Integrations

This document describes the configuration steps for setting up a federated network between IM and Presence Service the node and an external domain.

The supported external domains that an IM and Presence Service node can federate with are:

- Microsoft Office 365 over SIP (business to business)
- Microsoft Skype for Business 2015 over SIP (business to business)
- Microsoft Lync 2010 and 2013 over SIP

Note The IM and Presence Service supports interdomain federation with Microsoft Lync/S4B. Any reference to interdomain federation with Microsoft Lync/S4B also includes Microsoft Office 365, unless explicitly stated otherwise.

- Cisco WebEx Messenger over XMPP
- IBM Sametime Server Release 8.2, 8.5 over XMPP
- IM and Presence Service Release 9.x and later over XMPP

Note If you federate between one IM and Presence Service enterprise and another, follow the procedures that describe how to configure XMPP Federation.

Related Information -

Hardware Requirements

Software Requirements

Presence Web Service API Support

The Presence Web Service is an open interface that allows client applications to share user presence information with IM and Presence Service. Third party developers use this interface to build client applications that can send and retrieve updates about the presence state of a user. Note the following restrictions about Presence Web Service API support:

- For interdomain federation over SIP, you can use the Presence Web Service API to obtain rich presence information from non-Cisco clients, but basic presence for non-Cisco clients is not supported.
- For interdomain federation over XMPP, you cannot use the Presence Web Service API to obtain presence information from non-Cisco clients.

For more information about the Presence Web Service, see the *IM and Presence Service Developer Guide* at https://developer.cisco.com/site/collaboration/call-control/unified-presence/documentation/index.gsp.

Hardware Requirements

Cisco Hardware

- IM and Presence Service node. For IM and Presence Service hardware support, refer to the IM and Presence Service compatibility matrix
- Cisco Unified Communications Manager node. For Cisco Unified Communications Manager hardware support, refer to the Cisco Unified Communications Manager compatibility matrix
- Two DNS servers within the IM and Presence Service enterprise
- Cisco Expressway-C 5500 Series
- We only recommend the Cisco Expressway-C for SIP federation as it provides the TLS proxy functionality. For XMPP federation, any firewall is sufficient.
- When selecting a Cisco Expressway-C model, go to: http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_models_home.html. The TLS proxy component is available on all 5500 models.
- Make sure you use the correct version of Cisco Expressway-C software for your deployment. If you are configuring a new interdomain federation deployment, refer to the IM and Presence Service compatibility matrix for the correct version of Cisco Expressway-C software.

Related Information -

Compatibility Information

Software Requirements

Software Requirements

Cisco Software

- IM and Presence Service
- Cisco Unified Communications Manager
- Cisco Adaptive Security Appliance v8.3(1) or later
- Cisco Adaptive Security Device Manager (ASDM) v6.3 or later
- Supported XMPP clients:
  - Cisco Unified Personal Communicator Release 8.5
  - Cisco Jabber for Mac
  - Cisco Jabber for Windows
  - Cisco Jabber IM for Mobile (iPhone, Android, Blackberry)
  - Cisco Jabber for iPad
  - Cisco Jabber for Cius

Microsoft Software for SIP Federation

- Microsoft Office 365 (business to business)
- Microsoft Skype for Business Server 2015, Standard Edition or Enterprise Edition
- Microsoft Lync 2013 or 2010, Standard Edition or Enterprise Edition

Software for XMPP Federation

- Cisco WebEx Messenger
- IBM Sametime Server Release 8.2

Related Topic -

Hardware Requirements

Integration Preparation

It is essential that you plan carefully for this integration. Read the items in this section before you commence any configuration for this integration.

Routing Configuration

Consider how you are going to set up routing in your federated network. Consider how you route messages that are destined for an external domain address from IM and Presence Service through the Cisco Expressway-C to the external domain. You could consider deploying a routing entity (router, switch or gateway) between the IM and Presence Service enterprise deployment and Cisco Expressway-C. The routing entity routes messages to the Cisco Expressway-C, and Cisco Expressway-C routes these messages to the external domain.

You can also deploy Cisco Expressway-C as a gateway between the IM and Presence Service and the external domain. If you use the Cisco Expressway-C as a gateway for the IM and Presence Service, within your local enterprise deployment, you must consider how the Cisco Unified Communications Maanger, and the IM and Presence Service client access the IM and Presence Service node. If the Cisco Unified Communications Maanger and the IM and Presence Service clients are in a different subnet from the IM and Presence Service, they must access the IM and Presence Service using the Cisco Expressway-C.

If you deploy the Cisco Expressway-C behind an existing firewall in your network, consider how you route traffic to the Cisco Expressway-C and to the IM and Presence Service. On the existing firewall, configure routes and access lists to route traffic to the public IM and Presence Service address. You must also configure routes to the external domain using the existing firewall.

Related Information

Cisco Adaptive Security Appliance Deployment Options

Public IP Address

For SIP federation, you require a publicly accessible IP address for the public IM and Presence Service address. If you do not have an IP address that you can assign, use the outside interface of the Cisco Expressway-C as the public IM and Presence Service address (once you only use the Cisco Expressway-C for availability and IM traffic).

For XMPP federation, you can choose to either expose a public IP address for each IM and Presence Service node on which you enable XMPP federation, or expose a single public IP address:

- If you expose multiple IP addresses, you use NAT on Cisco Expressway-C to convert the public addresses to private addresses. For example, you can use NAT to convert the public addresses x.x.x.x:5269 and y.y.y.y:5269 to the private addresses a.a.a.a:5269 and b.b.b.b:5269 respectively.
- If you expose a single IP address, you use PAT on Cisco Expressway-C to map to the correct IM and Presence Service node. For example, the public IP address in your deployment is x.x.x.x, and there are multiple DNS SRV records for _xmpp-server. Each record has a different port, but all records resolve to x.x.x.x. The external servers sends requests to x.x.x.x:5269, x.x.x.x:15269, x.x.x.x.25269 through the Cisco Expressway-C. The Cisco Expressway-C performs PAT on the IP addresses, whereby it maps each address to the corresponding internal IP address for each IM and Presence Service node.

  For example, the public IP address x.x.x.x:5269 maps to the private IP address a.a.a.a:5269, the public IP address x.x.x.x:15269 maps to the private IP address b.b.b.b.b:5269, and the public IP address x.x.x.x:25269 maps to the private IP address c.c.c.c:5269, and so on. All IP addresses map internally to the same port (5269) on the IM and Presence Service.

Related Information -

External and Internal Interface Configuration

DNS Configuration

Public FQDN

For SIP federation, request messages are routed based on the FQDN. Therefore, the FQDN of the routing IM and Presence Service node (publisher) must be publicly resolvable.

AOL SIP Access Gateway

The AOL SIP Access Gateway provides federated services, which permit a company's SIP/SIMPLE-based instant messaging servers to communicate with other instant messaging users on the network. Using the AOL SIP Access Gateway, it is possible for users of a company's SIP/SIMPLE-based messaging server to obtain availability information for, and hold conversations with, public users of the AIM or AOL services. The AOL SIP Access Gateway also enables users of the AIM or AOL systems to send instant messages and to display availability information for users of the company's internal SIP/SIMPLE-based system.

The AOL SIP Access Gateway acts as the front end to a translator for internal AOL protocols. All communications between the company server and AOL uses SIP. The AOL SIP Access Gateway handles the translation into the protocols needed by internal AOL systems. It is not necessary to add any translation capabilities to external servers; from that perspective the AOL protocols are hidden. If the company server communicates using SIP/SIMPLE, it should still be possible to connect to AOL through the AOL SIP Access Gateway.

The AOL SIP Access Gateway supports connections by TLS over TCP only. The AOL SIP Access Gateway server should be defined within your instant messaging servers or proxies with this address:

Server Name: `sip.oscar.aol.com`

Server Port: 5061

The server name `sip.oscar.aol.com` resolves to 205.188.153.55 & 64.12.162.248.

Note

- If you configure these IP addresses statically anywhere in your network, we recommend that you periodically check with AOL for potential changes to these addresses.
- We recommend that you ping the FQDN of AOL SIP Access Gateway (sip.oscar.aol.com) to confirm the IP address as it may be subject to change, for example **`ping sip.oscar.aol.com`**.

Redundancy/High Availability

You need to consider how you are going to configure redundancy in your federated network. The Cisco Expressway-C supports redundancy by providing the Active/Standby (A/S) deployment model.

If you wish to make your IM and Presence Service federation capability highly available you can deploy a load balancer in front of your designated (federation) IM and Presence Service cluster.

DNS Configuration

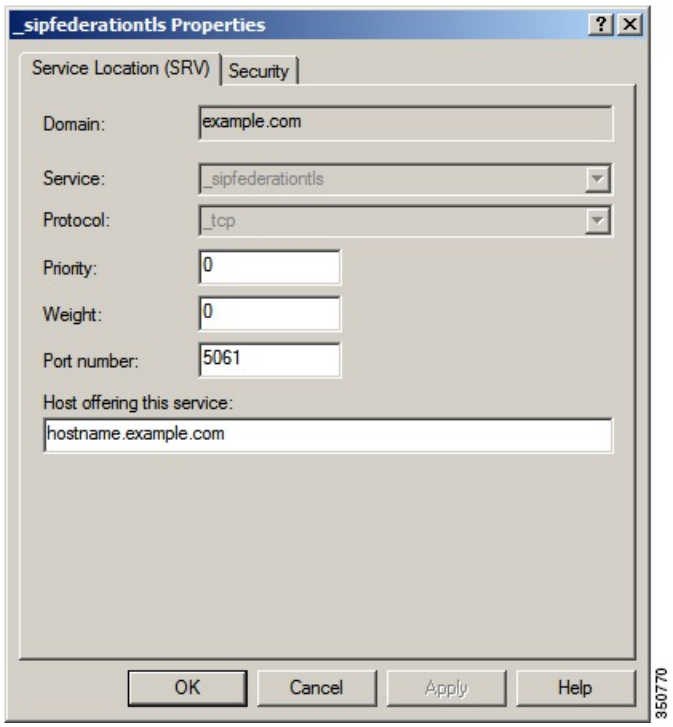
In the local IM and Presence Service enterprise deployment, the IM and Presence Service must publish a DNS SRV record for the IM and Presence Service domain to make it possible for other domains to discover the IM and Presence Service node through DNS SRV. The DNS SRV records reside on the DNS server in the enterprise DMZ.

If the local IM and Presence Service deployment is managing multiple domains, you must publish a DNS SRV record for each local domain. The DNS SRV record you publish for each local domain should resolve to the same public FQDN IP address.

For SIP federation with Microsoft S4B/Lync, you must publish the DNS SRV record "_sipfederationtls". The Microsoft enterprise deployment requires this record because you configure the IM and Presence Service as a Public IM Provider on the Access Edge server. In the external enterprise deployment, in order for the IM and Presence Service to discover the Microsoft domain, a DNS SRV record must exist that points to this external domain. If the IM and Presence Service node cannot discover the Microsoft domain using DNS SRV, you must configure a static route on the IM and Presence Service that points to the public interface of this external domain.

See the following figure for a sample DNS configuration for the DNS SRV record "_sipfederationtls_tcp.example.com" .

Figure 1: DNS SRV for "_sipfederationtls"

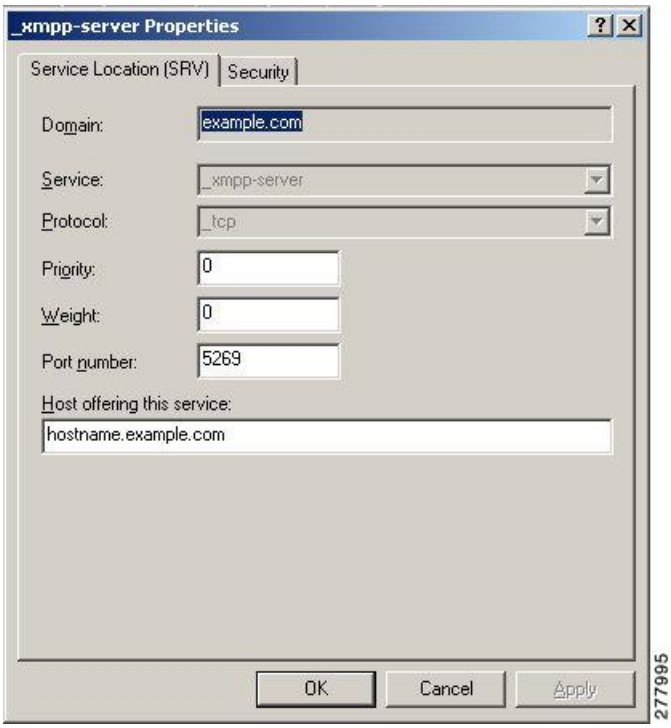


Because DNS SRV records are publicly resolvable, if you turn on DNS forwarding in the local enterprise, DNS queries retrieve information about public domains outside of the local enterprise. If the DNS queries rely completely on DNS information within the local enterprise (you do not turn on DNS forwarding in the local enterprise), you must publish DNS SRV record/FQDN/IP address that points to the external domain. Alternatively. you can configure static routes.

For XMPP federation, you must publish the DNS SRV record "_xmpp-server". This record enables federated XMPP domains to discover the IM and Presence Service domain so users in both domains can exchange IM and availability information over XMPP. Similarly, external domains must publish the _xmpp-server record in their public DNS server to enable theIM and Presence Service to discover the external domain.

See the following figure for a sample DNS configuration for the DNS SRV record "_xmpp-server".

Figure 2: DNS SRV for "_xmpp-server"



Certificate Authority Server

For SIP federation, the Cisco Adaptive Security Appliance in the IM and Presence Service enterprise deployment, and the external enterprise deployment, share IM and availability over a secure SSL/TLS connection.

Each enterprise deployment must present a certificate that is signed by an external Certificate Authority (CA), however each enterprise deployment may using a different CA. Therefore each enterprise deployment must download the root certificate from the external CA of the other enterprise deployment to achieve a mutual trust between the two enterprise deployments.

For XMPP federation, you can choose whether or not to configure a secure TLS connection. If you configure TLS, on the IM and Presence Service you need to upload the root certificate of the Certificate Authority (CA) that signs the certificate of the external enterprise. This certificate must exist in the certificate trust store on the IM and Presence Service because the Cisco Expressway-C does not terminate the TLS connections for XMPP federation; Cisco Expressway-C acts as a firewall for XMPP federation.

Prerequisite Configuration Tasks for this Integration

This chapter explains the various prerequisite configuration tasks to be performed for this preparation.

Configure the IM and Presence Service for Integration

Note These prerequisite tasks apply to both SIP and XMPP federation.

Procedure

Step 1 Install and configure the IM and Presence Service.

At this point, perform the following checks to ensure that your IM and Presence Service is operating properly:

- Run the IM and Presence Service System Configuration Troubleshooter.
- Check that you can add local contacts to the IM and Presence Service.
- Check that your clients are receiving availability states from the IM and Presence Service node.

Step 2 Configure the IM and Presence Service node with Cisco Unified Communications Manager a node as described in *Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*. Ensure that the IM and Presence Service node is working and issue free.

Related Information -

Configure the Cisco Adaptive Security Appliance for Integration

Configure the Cisco Adaptive Security Appliance for Integration

Note
- For SIP federation, you require the Cisco Adaptive Security Appliance.
- For XMPP federation, you require a firewall. You can use any firewall, including the Cisco Adaptive Security Appliance for basic firewall/NAT/PAT functionality. For XMPP federation you do not use the Cisco Adaptive Security Appliance for TLS proxy functionality.

Install and configure the Cisco Adaptive Security Appliance. Perform the following basic configuration checks on the Cisco Adaptive Security Appliance:

Procedure

Step 1 Access the Cisco Adaptive Security Appliance either through a console, hyperterminal, or the web-based Adaptive Security Device Manager (ASDM).

Step 2 Obtain the appropriate licenses for the Cisco Adaptive Security Appliance. Note that a license is required for the TLS proxy on the Cisco Adaptive Security Appliance. Contact your Cisco representative for license information.

Step 3 Upgrade the software (if necessary).

Step 4 Configure the hostname using the command:

```
(config)# hostname name
```

Step 5 Set the timezone, date and time in ASDM by choosing **Device Setup** > **System Time** > **Clock**, or through the CLI using the **clock set** command. Note the following:

- Set the clock on the Cisco Adaptive Security Appliance 5500 before configuring the TLS proxy.
- We recommend that the Cisco Adaptive Security Appliance use the same NTP server as the IM and Presence Service cluster. The TLS connections may fail due to certificate validation failure if the clock is out of sync between the Cisco Adaptive Security Appliance and the IM and Presence Service node.
- To view the NTP server address, use the command **ntp server** *server_address*, and the command **show ntp associat | status** to view the status of the NTP server.

Step 6 Check the Cisco Adaptive Security Appliance 5500 modes. The Cisco Adaptive Security Appliance 5500 is configured to use single mode and routed mode by default.

- Check the current mode. This value is single mode by default.

  ```
  (config)# show mode
  ```

- Check the current firewall mode. This is routed mode by default.

  ```
  (config)# show firewall
  ```

- Set up the external and internal interfaces.
- Set up the basic IP routes.

Related Information -

External and Internal Interface Configuration

Configure Static IP Routes

Configure the IM and Presence Service for Integration