Overview of this Integration

This section provdes an overview of the integration.

Basic Federated Network

This integration enables the IM and Presence Service users from within any domain that IM and Presence Service manages to exchange availability information and Instant Messaging (IM) with users in external domains. The IM and Presence Service uses different protocols to federate with different external domains.

The IM and Presence Service uses the standard Session Initiation Protocol (SIP RFC 3261) to federate with:

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

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

IM and Presence Service uses the Extensible Messaging and Presence Protocol (XMPP) to federate with:

- IBM Sametime Server 8.2 and 8.5
- Cisco WebEx Messenger

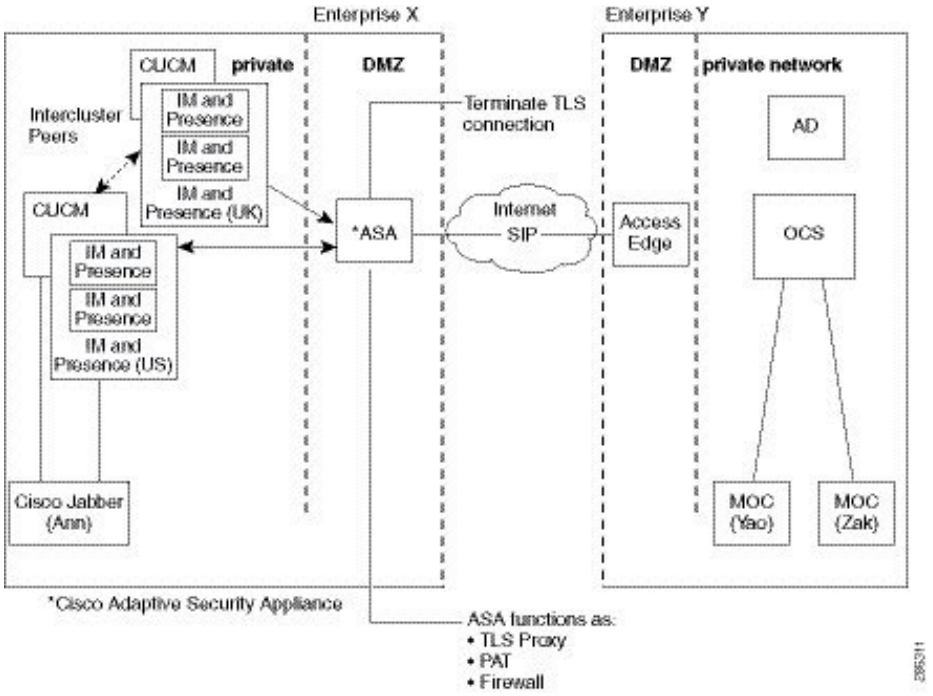
- IM and Presence Service 9.x and up
- Any other server that is XMPP Standards compliant

Note If you wish to enable XMPP federation with an external domain, ensure that the external domain was not previously configured as a SIP federated domain on the IM and Presence Service.

Example: An IM and Presence deployment with example.com was historically configured as a SIP based federation. But example.com has now added XMPP support, so the local administrator instead wishes to enable an XMPP based federation. To allow this, the local administrator must first delete example.com as a SIP federated domain on the IM and Presence Service.

The following figure provides an example of a SIP federated network between IM and Presence Service enterprise deployment and Microsoft S4B/Lync enterprise deployment.

Figure 1: Basic SIP Federated Network Between IM and Presence Service and Microsoft S4B/Lync

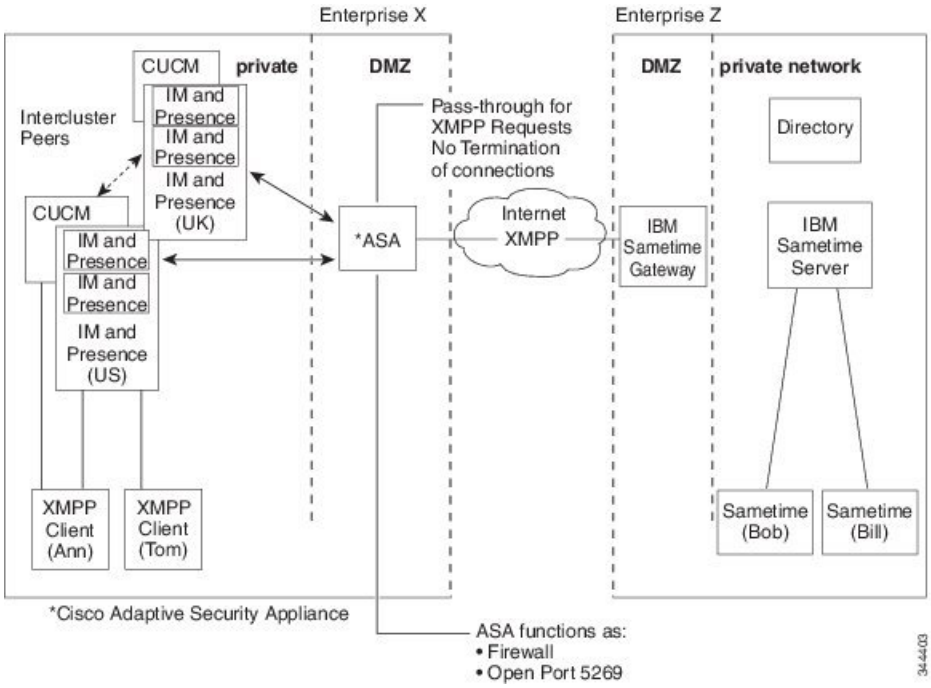


This example shows the messaging flows for a multi-cluster IM and Presence Service deployment where SIP Federation is enabled in one cluster only. A single routing node receives all incoming IMs from the Expressway-C and reroutes the IM to the correct node in either cluster. Outgoing IMs can be sent to the Expressway-C from any node in either cluster.

In the figure, each internal enterprise domain interconnects over the public internet using its DMZ edge server using a secure TLS connection. Within the internal IM and Presence Service enterprise deployment, the Cisco Adaptive Security Appliance provides firewall, Port Address Translation (PAT), and TLS proxy functionality. The Cisco Expressway-C routes all incoming traffic initiated from the external domain to a designated IM and Presence Service node.

The following figure provides an example of a multi-cluster XMPP federated network between IM and Presence Service enterprise deployment and an IBM Sametime enterprise deployment. TLS is optional for XMPP federation. Cisco Adaptive Security Appliance acts only as a firewall for XMPP federation; it does not provide TLS proxy functionality or PAT for XMPP federation. IMs can be sent and received from any node that has Federation enabled. However, Federation must be configured in parallel in both clusters.

Figure 2: Basic XMPP Federated Network Between IM and Presence Service and IBM Sametime



There are two DNS servers within the internal IM and Presence Service enterprise deployment. One DNS server hosts the IM and Presence Service private address. The other DNS server hosts the IM and Presence Service public address and DNS SRV records for SIP federation (_sipfederationtls), and XMPP federation (_xmpp-server) with the IM and Presence Service. The DNS server that hosts the IM and Presence Service public address is located in the local DMZ.

Intercluster and Multinode Deployments

Note Any configuration procedures in this document that relate to intercluster IM and Presence Service deployments, you can also apply these procedures to multinode IM and Presence Service deployments.

SIP Federation Deployments

In an intercluster and a multinode cluster IM and Presence Service deployment, when an external domain initiates a new session, Cisco Expressway-C routes all messages to an IM and Presence Service node that is designated for routing purposes. If the IM and Presence Service routing node does not host the recipient user, it routes the message through intercluster communication to the appropriate IM and Presence Service node

within the cluster. The system routes all responses that are associated with this request through the routing IM and Presence Service node.

Any IM and Presence Service node can initiate a message to an external domain through Cisco Expressway-C. On Microsoft S4B/Lync, when the external domain replies to these messages, the replies are sent directly back to the IM and Presence Service node that initiated the message through the Cisco Expressway-C You enable this behavior when you configure Port Address Translation (PAT) on the Cisco Expressway-C. We recommend that you configure PAT on the Cisco Expressway-C as PAT is required for the 200 OK response messages.

Related Information - Port Address Translation (PAT)

XMPP Federation Deployments

For a single cluster, you only need to enable XMPP federation on one node in the cluster. A single DNS SRV record is published for the enterprise in the public DNS. This DNS SRV record maps to the IM and Presence Service node that is enabled for XMPP Federation. All incoming requests from external domains are routed to the node running XMPP federation, based on the published SRV record. Internally the IM and Presence Service reroutes the requests to the correct node for the user. The IM and Presence Service also routes all outgoing requests through the node running XMPP federation.

You can also publish multiple DNS SRV records, for example, for scale purposes, or if you have multiple IM and Presence Service clusters and you must enable XMPP federation at least once per cluster. Unlike SIP federation, XMPP federation does not require a single point of entry for the IM and Presence Service enterprise domain. As a result, the IM and Presence Service can route incoming requests to any one of the published nodes that you enable for XMPP federation.

In an intercluster and a multinode cluster IM and Presence Service deployment, when an external XMPP federated domain initiates a new session, it performs a DNS SRV lookup to determine where to route the request. If you publish multiple DNS SRV records, the DNS lookup returns multiple results; IM and Presence Service can route the request to any of the servers that DNS publishes. Internally the IM and Presence Service reroutes the requests to the correct node for the user. The IM and Presence Service routes outgoing requests to any of the nodes running XMPP federation within the cluster.

If you have multiple nodes running XMPP federation, you can still choose to publish only one node in the public DNS. With this configuration, the IM and Presence Service routes all incoming requests through that single node, rather than load balancing the incoming requests across the nodes running XMPP federation. The IM and Presence Service load-balances outgoing requests and sends outgoing requests to any of the nodes running XMPP federation within the cluster.

High Availability and Federation

This section expalins the concept of high availability and federation.

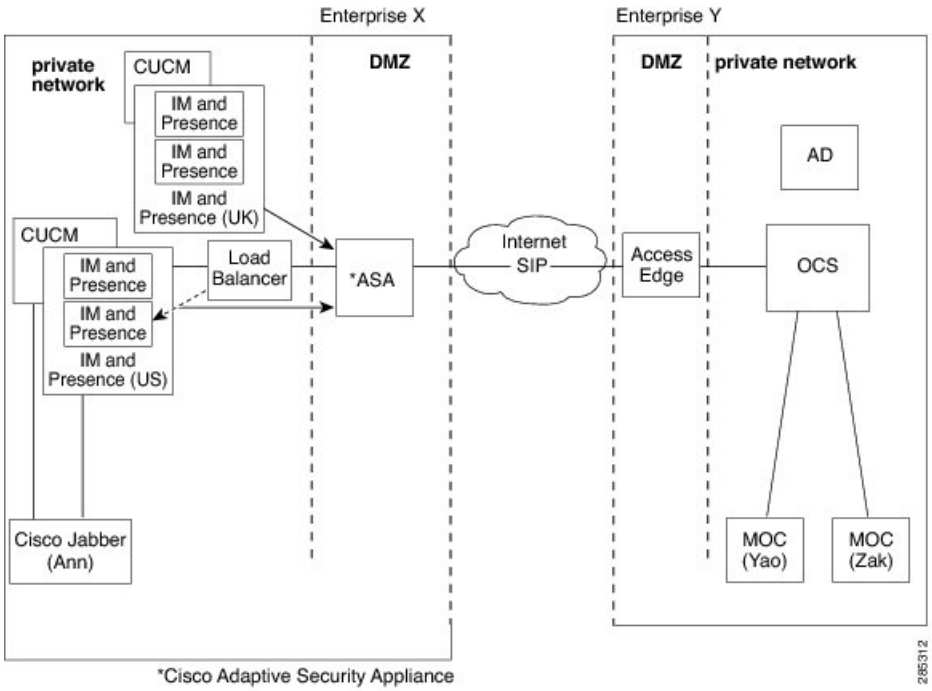
High Availability for SIP Federation

Note Only the IM and Presence Service, Release 8.5 or later supports high availability.

If you are federating with a Microsoft S4B/Lync, the Microsoft Access Edge server only supports the return of a single hostname and server address in the DNS SRV lookup. Also the Microsoft Access Edge server only supports the manual provisioning of a single IP address.

Therefore, in order to achieve high availability when federating with Microsoft S4B/Lync, you must incorporate a load balancer between the IM and Presence Service node and Cisco Expressway-C, as shown in the following figure. The load balancer terminates incoming TLS connections from Cisco Expressway-C, and initiates a new TLS connection to route the content to the appropriate backend IM and Presence Service.

Figure 3: Federated Network Between the IM and Presence Service and Microsoft S4B/Lync with High Availability



Related Information -

Load Balancer Configuration for Redundancy for SIP Federation

High Availability for XMPP Federation

High availability for XMPP federation differs from the high availability model for other IM and Presence Service features because it is not tied to the two node sub-cluster model.

To provide high availability for XMPP federation, you must enable two or more IM and Presence Service nodes in your cluster for XMPP federation; having multiple nodes enabled for XMPP federation not only adds scale but it also provides redundancy in the event that any node fails.

High Availability for Outbound Request Routing

The IM and Presence Service evenly load balances outbound requests from users within that cluster across all the XMPP federation enabled nodes in the cluster. If any node fails, the IM and Presence Service dynamically spreads the outbound traffic across the remaining active nodes within the cluster.

High Availability for Inbound Request Routing

An additional step is required to provide high availability for inbound request routing. To allow an external domain to discover the local IM and Presence Service deployment, a DNS SRV record must be published on a public DNS server. This record resolves to an XMPP federation enabled node. The external domain then connects to the resolved address.

To provide high availability in this model, multiple DNS SRV records must be published for the local IM and Presence Service deployment. Each of these records resolve to one of the XMPP Federation enabled nodes within the local IM and Presence Service deployment.

These records provide a choice of DNS SRV records for the local deployment. If an XMPP federation enabled node fails, the external system has other options from which to connect to the local IM and Presence Service deployment.

Note

- Each published DNS SRV records must have the same priority and weight. This allows a spread of load across all published records, and also allows the external system to correctly reconnect to one of the other nodes with a DNS SRV record in the event of a failure.
- DNS SRV records may be published for all or just a subset of XMPP federation enabled nodes. The greater the number of records published, the greater the redundancy in the system for inbound request handling.
- If you configure the Chat feature on an IM and Presence Service node in an XMPP federation deployment, you can publish multiple DNS SRV records for chat node aliases also. This allows the external system to find another inbound route to that specific chat node through another XMPP federation node, should any XMPP Federation enabled node fail. Note that this is not high availability for the Chat feature itself, but an extension of the XMPP Federation high availability feature for inbound requests addressed to chat node aliases.

IBM Sametime Federation

IM and Presence Service Release 9.0 does not support high availability for Interdomain federation between an IM and Presence Service enterprise and an IBM Sametime enterprise and an IBM Sametime enterprise. This is because IBM Sametime does not retry other records that are returned in a DNS SRV lookup. It only tries the first DNS SRV record found, and if the connection attempt fails, it does not retry to lower weighted nodes.

Note There is one situation where XMMP Federation high availability may appear to occur on the IM and Presence Service in an IBM Sametime federation deployment. If users have failed over to the backup node due to critical services failing, but the Cisco XCP XMPP Federation Connection Manager remains running on the primary node. In this case, incoming traffic is still directed to the primary node, and then redirected to the backup node using the router to router connection. However, in this scenario XMPP Federation has not failed and can continue to operate as normal.

Related Information -

DNS Configuration for XMPP Federation

Turn On XMPP Federation on a Node

Cisco Adaptive Security Appliance Deployment Options

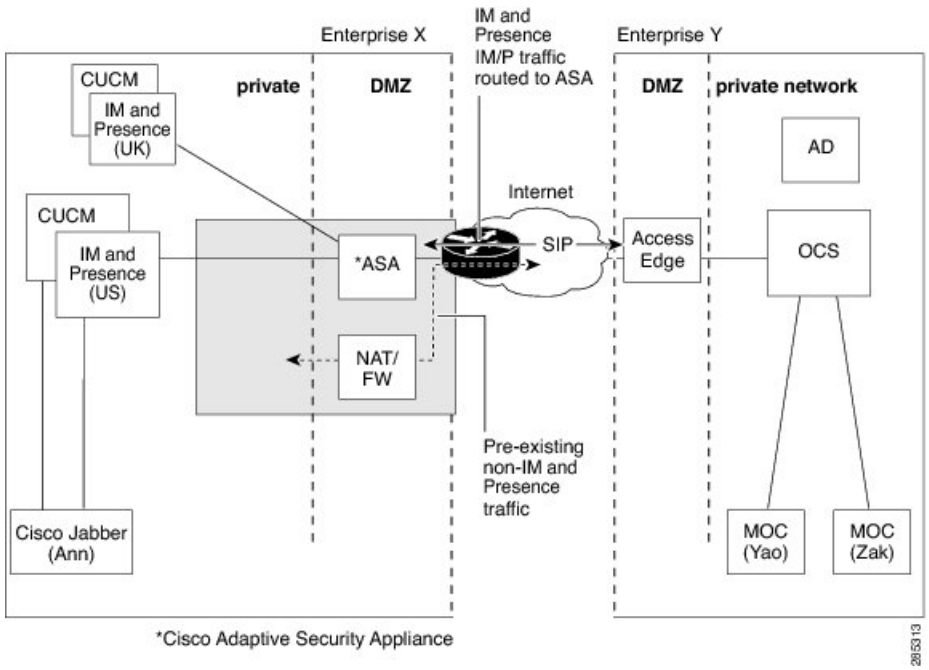
Within the internal IM and Presence Service enterprise deployment, the Cisco Adaptive Security Appliance provides firewall, Port Address Translation (PAT) and TLS proxy functionality in the DMZ to terminate the incoming connections from the public internet, and permit traffic from specific federated domains.

Note In an XMPP federation deployment, Cisco Adaptive Security Appliance provides firewall functionality only. If you already deploy a firewall, you do not require an extra Cisco Adaptive Security Appliance for XMPP federation.

You can deploy the Cisco Adaptive Security Appliance in a number of different ways, depending on your existing network and the type of firewall functionality you want to deploy. This section contains only an overview of the deployment models we recommend. For further details please refer to the deployment guidelines in the Cisco Adaptive Security Appliance documentation. The Cisco Adaptive Security Appliance deployment options we describe here apply to SIP federation only.

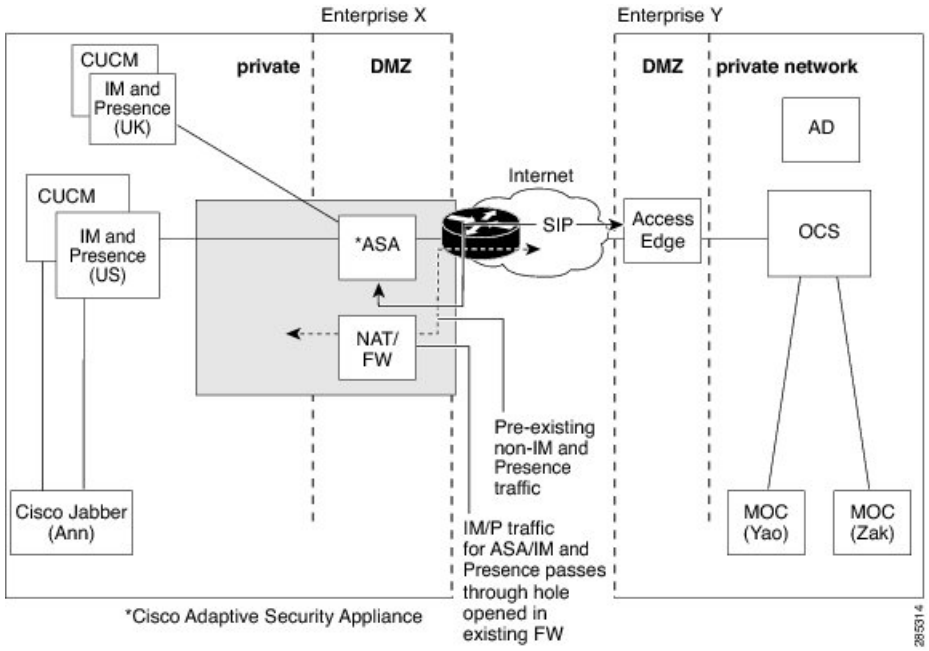
You can deploy the Cisco Adaptive Security Appliance as the enterprise firewall that protects Instant Messaging (IM) traffic, Availability traffic, and other traffic as illustrated in the following figures. This is the most cost-effective deployment, and the one we recommend for new and existing networks. You can also deploy the Cisco Adaptive Security Appliance in parallel to the existing firewall, as illustrated in the following figure. In this deployment Cisco Adaptive Security Appliance handles the IM and Presence Service traffic between IM and Presence Service and the public internet, and the pre-existing traffic continues to use any existing firewall. In the following figure Cisco Adaptive Security Appliance is also deployed as a gateway for the IM and Presence Service node, which means that you do not require a separate router to direct traffic to Cisco Adaptive Security Appliance.

Figure 4: Cisco ASA 5500 Deployed in Parallel to Existing NAT/Firewall



You can also deploy the Cisco Adaptive Security Appliance behind an existing firewall. In this case, you configure the existing firewall to allow traffic destined for the IM and Presence Service to reach the Cisco Adaptive Security Appliance, as illustrated in the following figure. In this type of deployment the CiscoAdaptive Security Appliance is functioning as a gateway for the IM and Presence Service node.

Figure 5: Cisco ASA 5500 Deployed Behind Existing NAT/Firewall



Presence Subscriptions and Blocking Levels

All new presence subscriptions from `x@externaldomain.com` to `user@local.com`are sent by the Cisco Expressway-C, as shown in the following figure. The Cisco Expressway-C checks the inbound SIP subscriptions against the list of permitted external domains. If the domain is not permitted, the Cisco Expressway-C denies the presence subscription.

Note In an XMPP federation deployment, the Cisco Expressway-C does not perform any domain checks.

On receipt of the inbound subscription, the IM and Presence Service verifies that the external domain is one of the permitted federated domains that you define at the administration level on the IM and Presence Service node. For SIP federation, you configure a federated domain. For XMPP federation, you define the administrator policy for XMPP federation. If the subscription is not from a permitted domain, the IM and Presence Service denies the subscription (without contacting the local user).

If the subscription is from a permitted domain, the IM and Presence Service checks the authorization policies of the local user to verify that the local user has not previously blocked or allowed either the federated domain or the user sending the presence subscription. The IM and Presence Service then accepts the incoming subscription and places it in a pending state.

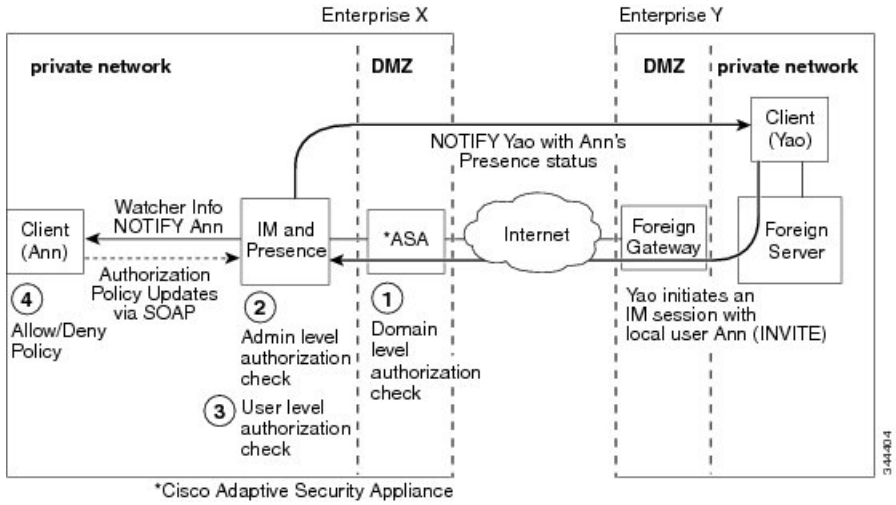
The IM and Presence Service notifies the local user that `x@externaldomain.com` wants to watch their presence by sending the client application a notification message for the subscription. This triggers a dialog box on the client application that enables the local user to allow or deny the subscription. Once the user has made an authorization decision, the client application communicates that decision back to the IM and Presence Service. The authorization decision is added to the policy list of the user stored on the IM and Presence Service.

Note Third-party XMPP clients do not update the policy list of the user, they just accept the subscription. The user can manually update their privacy list in the IM and Presence Service User Options interface.

A deny decision is handled using polite blocking, which means that the presence state of the user appears offline on the external client. If the local user allows the subscription, the IM and Presence Service sends presence updates to the external watcher.

The user can also block subscriptions on a per user and a per domain basis. This can be configured by the Cisco Jabber client.

Figure 6: Inbound SIP Presence Message Flow

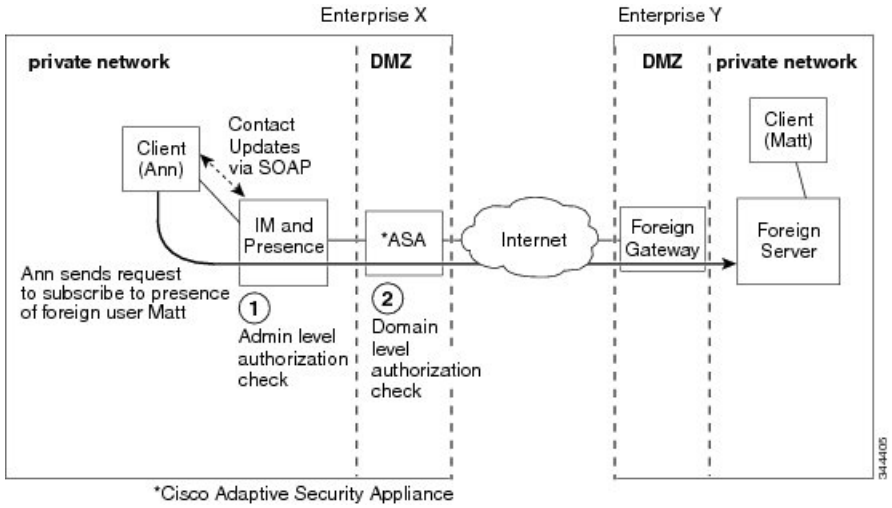


The IM and Presence Service sends all outgoing subscriptions through the Cisco Expressway-C, the Cisco Expressway-C then forwards these subscriptions to the external domain. The IM and Presence Service sends an outgoing subscription even if an active subscription already exists between a different local user to the same external user in the same external domain. The following figure illustrates an outgoing presence subscription flow.

The external user is added to the contact list on the client application and the **IM and Presence Service User Options** interface as `user@externaldomain.com`.

Note The domain level authentication check is not applied on the Cisco Expressway-C for XMPP federation.

Figure 7: Outbound Presence Request Flow



Note

- Microsoft S4B/Lync performs a refresh subscribe every one hour and 45 minutes. Therefore, if an IM and Presence Service node restarts, the maximum duration a Microsoft S4B/Lync client is without the presence status of the IM and Presence Service contacts is approximately two hours.
- If Microsoft S4B/Lync restarts, the maximum duration an IM and Presence Service client is without presence status of Microsoft S4B/Lync contacts is approximately two hours.

Related Information -

Availability State Mappings

Instant Messaging

Availability State Mappings

This section explains the various concepts of availability state mappings.

Availability State Mappings for Microsoft OCS

The following table shows the availability mapping states from Microsoft Office Communicator to the IM and Presence Service, third-party XMPP clients and Cisco Jabber.

Table 1: Availability Mapping States from Microsoft Office Communicator

Microsoft Office Communicator Setting	Third-party XMPP Client Setting (connected to IM and Presence Service)	Cisco Jabber Release 8.x Setting
Available	Available	Available

Microsoft Office Communicator Setting	Third-party XMPP Client Setting (connected to IM and Presence Service)	Cisco Jabber Release 8.x Setting
Busy	Away	Busy
Do Not Disturb	Away	Busy
Be Right Back	Away	Away
Away	Away	Away
Offline	Offline	Offline

In the table, Microsoft Office Communicator "Busy" and "Do Not Disturb" states map to "Away" with a status text of "Busy" on a third-party XMPP client. XMPP clients differ in how they render this "Away" status, for example, certain XMPP clients show the "Away" icon with no text. Other XMPP clients render the "Away" icon with "Busy" text annotation alongside.

The following table shows the availability mapping states from Cisco Jabber Release 8.x to Microsoft Office Communicator.

Table 2: Availability Mapping States from Cisco Jabber Release 8.x

Cisco Jabber Release 8.x Setting	Microsoft Office Communicator Setting
Available	Available
Busy	Busy
Do Not Disturb	Busy
Offline	Offline

The following table shows the availability mapping states from third-party XMPP clients that are connected to IM and Presence Service to Microsoft Office Communicator.

Table 3: Availability Mapping States from Third-party XMPP Client

Third-party XMPP Client Setting (connected to IM and Presence Service)	Microsoft Office Communicator Setting
Available	Available
Away	Away
Extended Away	Away
Do Not Disturb	Busy
Offline	Offline

Related Information

Presence Subscriptions and Blocking Levels

Availability State Mappings for Microsoft Lync

The following table shows the availability mapping states from Microsoft Lync to the IM and Presence Service, third-party XMPP clients, and Cisco Jabber.

Table 4: Availability Mapping States from Microsoft Lync

Microsoft Lync Setting	Third-party XMPP Client Setting (connected to IM and Presence Service)	Cisco Jabber Release 8.x Setting
Available	Available	Available
Busy	Away	Busy
Do Not Disturb	Away	Busy
Be Right Back	Away	Away
Away	Away	Away
Offline	Offline	Offline

In the table, Lync Client "Busy" and "Do Not Disturb" states map to "Away" with a status text of "Busy" on a third-party XMPP client. XMPP clients differ in how they render this "Away" status, for example, certain XMPP clients show the "Away" icon with no text. Other XMPP clients render the "Away" icon with "Busy" text annotation alongside.

The following table shows the availability mapping states from Cisco Jabber Release 8.x to a Lync client.

Table 5: Availability Mapping States from Cisco Jabber Release 8.x

Cisco Jabber Release 8.x Setting	Microsoft Lync Setting
Available	Available
Busy	Busy
Do Not Disturb	Busy
Offline	Offline

The following table shows the availability mapping states from third-party XMPP clients, that are connected to the IM and Presence Service, to a Lync client.

Table 6: Availability Mapping States from a Third-party XMPP Client

Third-party XMPP Client Setting (connected to IM and Presence Service)	Microsoft Lync Setting
Available	Available
Away	Away
Extended Away	Away
Do Not Disturb	Busy
Offline	Offline

Related Information -

Presence Subscriptions and Blocking Levels

Availability State Mappings for XMPP Federation

The following table shows the availability mapping states from IBM Sametime 8.2 to a third-party XMPP client on the IM and Presence Service, and to Cisco Jabber.

Table 7: Availability Mapping States from IBM Sametime 8.2 Client

IBM Sametime Client Setting	Third-party XMPP Client Setting (connected to IM and Presence Service)	Cisco Jabber Setting Release 8.x
Available	Available	Available with status message
Do Not Disturb	Do Not Disturb	Do Not Disturb with status message
Available with status “In a meeting”	Available with status “In a meeting”	Available with status message
Away	Away	Away with status message
Offline	Offline	Offline

The following table shows the availability mapping states from webex Connect to a third-party XMPP client on the IM and Presence Service and to Cisco Jabber.

Table 8: Availability Mapping States from Webex Connect

Webex Connect Setting	Third-party XMPP Client Setting (connected to IM and Presence Service)	Cisco Jabber Setting Release 8.x
Available	Available	Available
Do Not Disturb	Do Not Disturb	Do Not Disturb

Webex Connect Setting	Third-party XMPP Client Setting (connected to IM and Presence Service)	Cisco Jabber Setting Release 8.x
Away with status “In a meeting”	Available with status “In a meeting”	Away with status “In a meeting”
Away	Away	Away
Offline	Offline	Offline

The following table shows the availability mapping states from Cisco Jabber Release 8.x to other federated clients.

Table 9: Availability Mapping States from Cisco Jabber Release 8.x

Cisco Jabber Release 8.x Setting	Federated Cisco Jabber Release 8.x Setting	Federated Third-party XMPP Client Setting (connected toIM and Presence Service)	Webex Connect Client Setting	IBM Sametime Client Server
Available	Available	Available	Available	Available
Do Not Disturb	Do Not Disturb	Do Not Disturb	Do Not Disturb	Do Not Disturb
Busy	Busy	Away	Idle	Away
Idle	Idle	Idle	Idle	Idle
Offline	Offline	Offline	Offline	Offline

The following table shows the availability mapping states from a third-party XMPP client on the IM and Presence Service to other federated clients.

Table 10: Availability Mapping States from XMPP Client Connected to the IM and Presence Service

Third-party XMPP Client Setting (connected to IM and Presence Service)	Federated Cisco Jabber Release 8.x Setting	Federated XMPP Client Setting (connected to IM and Presence Service)	Webex Connect Client Setting	IBM Sametime Client Server
Available	Available	Available	Available	Available
Do Not Disturb	Do Not Disturb	Do Not Disturb	Do Not Disturb	Do Not Disturb
Away	Away	Away	Away	Away
Extended Away	Away	Extended Away	Extended Away	Away
Away with status “Idle”	Idle	Away with status “Idle”	Away with status “Idle”	Away with status “Idle”

Third-party XMPP Client Setting (connected to IM and Presence Service)	Federated Cisco Jabber Release 8.x Setting	Federated XMPP Client Setting (connected to IM and Presence Service)	Webex Connect Client Setting	IBM Sametime Client Server
Offline	Offline	Offline	Offline	Offline

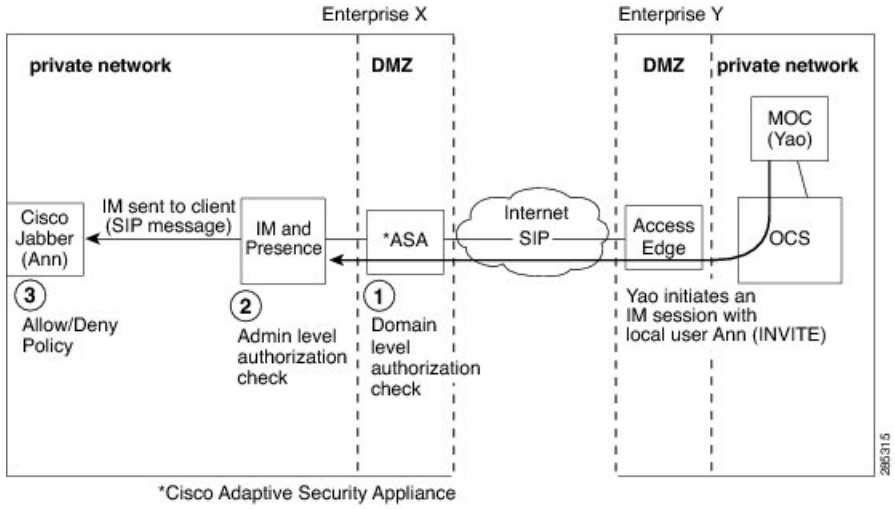
Instant Messaging

This section explains the following -

Instant Message Flow for SIP Federation

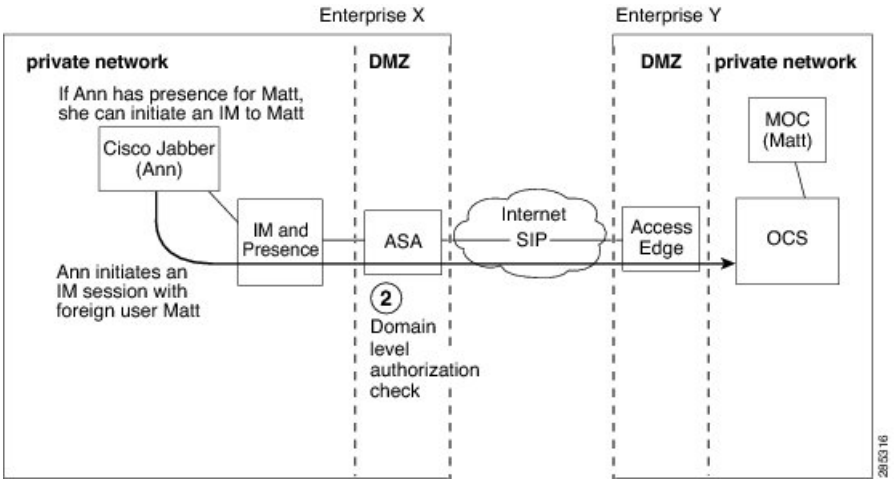
Instant Messages (IMs) that are sent between two enterprise deployments use Session Mode. When a user in an external domain sends an IM to a local user in the IM and Presence Service domain, the external server sends an INVITE message, as illustrated in the following figure. The Expressway-C forwards the INVITE message to IM and Presence Service. The IM and Presence Service replies with a 200 OK message to the external server, and the external server sends a SIP MESSAGE containing the text data. The IM and Presence Service forwards the text data to the client application of the local user, using the appropriate protocol.

Figure 8: Inbound Instant Messaging Flow



When a local user in the IM and Presence Service domain sends an IM to a user in a external domain, the IM is sent to the IM and Presence Service node. If no existing IM session is established between these two users, the IM and Presence Service sends an INVITE message to the external domain to establish a new session. The following figure illustrates this flow. the IM and Presence Service uses this session for any subsequent MESSAGE traffic from either of these two users. Note that users of Cisco Jabber and third-party XMPP clients can initiate an IM even if they do not have availability.

Figure 9: Outbound Instant Message Flow



Note The IM and Presence Service does not support a three-way IM session (group chat) with a Microsoft S4B/Lync contact.

Related Information -

Presence Subscriptions and Blocking Levels

Availability and Instant Message Flow for XMPP Federation

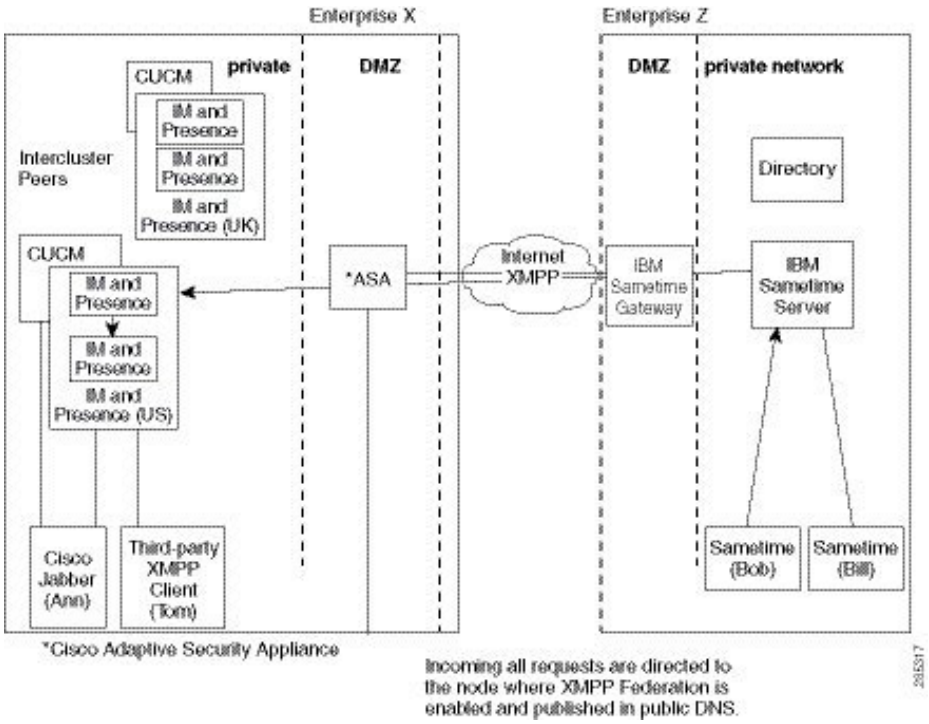
The flow of incoming and outgoing availability and IM requests for XMPP federation can vary in a multinode IM and Presence Service deployment.

In a multinode deployment, you can enable XMPP federation on each node in the cluster, or just on a single node in a cluster. In addition, you can decide to publish only a single DNS SRV record, or publish multiple DNS SRV records (one record for each node on which you enable XMPP Federation).

If you only publish a single DNS SRV record, the system routes all inbound requests to that single node, and internally the IM and Presence Service routes the traffic to the correct node using intercluster routing, as illustrated in the following figure. If you publish multiple DNS SRV records, depending on how you configure the SRV records, the system could load-balance inbound requests across each node.

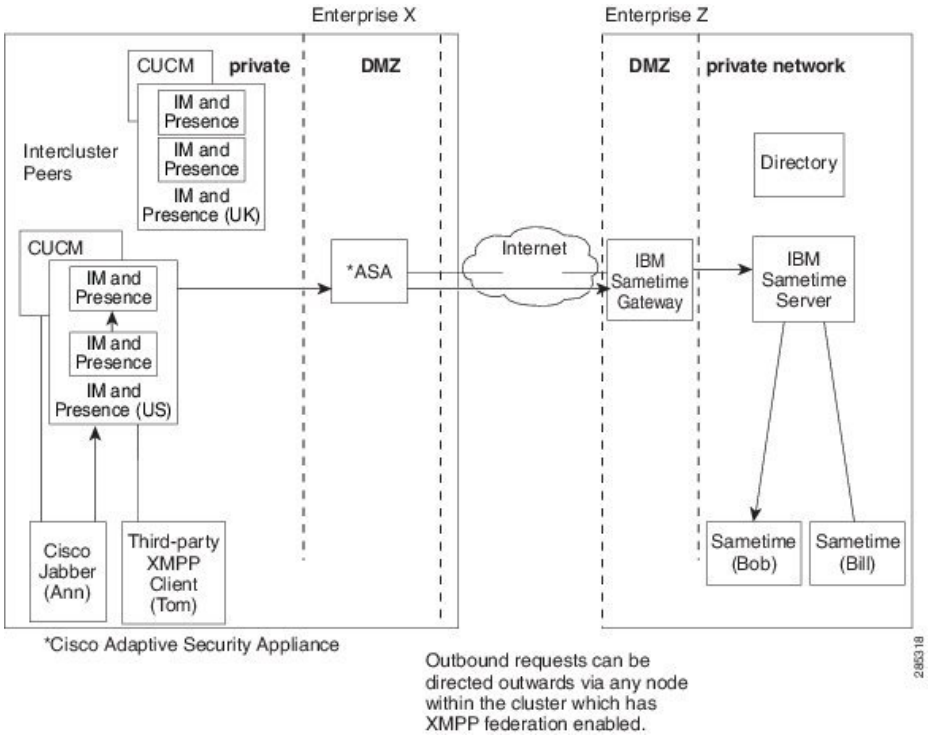
In this diagram, which shows the inbound message flow for a multi-cluster XMPP Federated network, Federation is enabled in both clusters. The inbound message goes directly to a Federation-enabled node in the destination cluster. The Federation-enabled node reroutes the message to the appropriate cluster node.

Figure 10: XMPP Inbound Request Flow



The IM and Presence Service routes outbound requests to any node in the cluster on which you enable XMPP Federation, even if that node is not the home node for the user that initiates the request, as illustrated in the following figure. In this diagram, Federation is enabled in both peer clusters, but the outbound flow does not hit the peer cluster.

Figure 11: XMPP Outbound Request Flow



Related Information -

High Availability for XMPP Federation

Federation in Deployments with Multiple Domains

Federation is fully supported in IM and Presence Service deployments with multiple domains provided the remote domain is not managed by the local IM and Presence Service deployment.

You must create DNS records for all local domains to enable Federation for all users in the local cluster.

For XMPP federation, the cup-xmpp security certificate must have all local domains included as Subject Alt Names.

Federation and Subdomains

The IM and Presence Service supports the following subdomain scenarios:

- The IM and Presence Service belongs to a subdomain of the external domain. For example, theIM and Presence Service belongs to the subdomain "imp.cisco.com". The IM and Presence Service federates with an external enterprise that belongs to the domain "cisco.com". In this case, the IM and Presence Service user is assigned the URI "impuser@imp.cisco.com", and the external user has the URI "foreignuser@cisco.com".

- The IM and Presence Service belongs to a parent domain, and the external enterprise belongs to a subdomain of that parent domain. For example, the IM and Presence Service belongs to the domain "cisco.com". The IM and Presence Service federates with a external enterprise that belongs to the subdomain "foreign.cisco.com". In this case, the IM and Presence Service user is assigned the URI "impuser@cisco.com", and the external user is assigned the URI "foreignuser@foreign.cisco.com".
- The IM and Presence Service and the external enterprise each belong to different subdomains, but both of these subdomains belong to the same parent domain. For example, the IM and Presence Service belongs to the subdomain "cup.cisco.com" and the external enterprise belongs to the subdomain "foreign.cisco.com". Both of these subdomains belong to the parent domain "cisco.com". In this case, the IM and Presence Service user is assigned the URI "impuser@cup.cisco.com" and the external user is assigned the URI "foreignuser@foreign.cisco.com".

If you federate with subdomains, you only need to configure separate DNS domains; there is no requirement to split your Active Directory. If you configure federation within the enterprise, the IM and Presence Service users or external users can belong to the same Active Directory domain. For example, in the third scenario above, the Active Directory can belong to the parent domain "cisco.com". You can configure all users under the "cisco.com" domain in Active Directory, even though a user may belong to the subdomain "imp.cisco.com" or "foreign.cisco.com", and may have the URI "impuser@imp.cisco.com" or "foreignuser@foreign.cisco.com".

Note that even though an LDAP search from Cisco Jabber may return users in the other domain, or subdomain, a Cisco Jabber user cannot add these federated users from the LDAP lookup on Cisco Jabber. TheCisco Jabber user must add these users as external (federated) contacts so that the IM and Presence Service applies the correct domain and not the local domain.

Note The IM and Presence Service also supports the scenarios above if you configure federation between two IM and Presence Service enterprise deployments.