Overview of this Integration

June 18, 2013

Basic Federated Network

This integration enables Cisco Unified Presence users in one enterprise domain to exchange availability information and Instant Messaging (IM) with users in foreign domains. Cisco Unified Presence uses different protocols to federate with different foreign domains.

Cisco Unified Presence uses the standard Session Initiation Protocol (SIP RFC 3261) to federate with:

- Microsoft Office Communications Server Release 2 (OCS R2), OCS 2007, Microsoft Lync 2010

Note Only Cisco Unified Presence Release 8.5(2) or later supports interdomain federation with Microsoft Lync. For Cisco Unified Presence Release 8.5(2) or later, any reference to interdomain federation with OCS also includes Microsoft Lync, unless explicitly stated otherwise.

- AOL SIP Access Gateway (SAG)

Note Only Cisco Unified Presence Release 8.5.x or later supports interdomain federation with AOL.

SIP federation with AOL enables Cisco Unified Presence users to federate with the following users:

  - Users of AOL public communities, for example, aim.com, aol.com.

  - Users of an enterprise whose domain is hosted by AOL.
  - Users of a foreign enterprise that federate with AOL. Cisco Unified Presence could use AOL as a clearing house to federate with these foreign enterprises.

Cisco Unified Presence uses the Extensible Messaging and Presence Protocol (XMPP) to federate with:

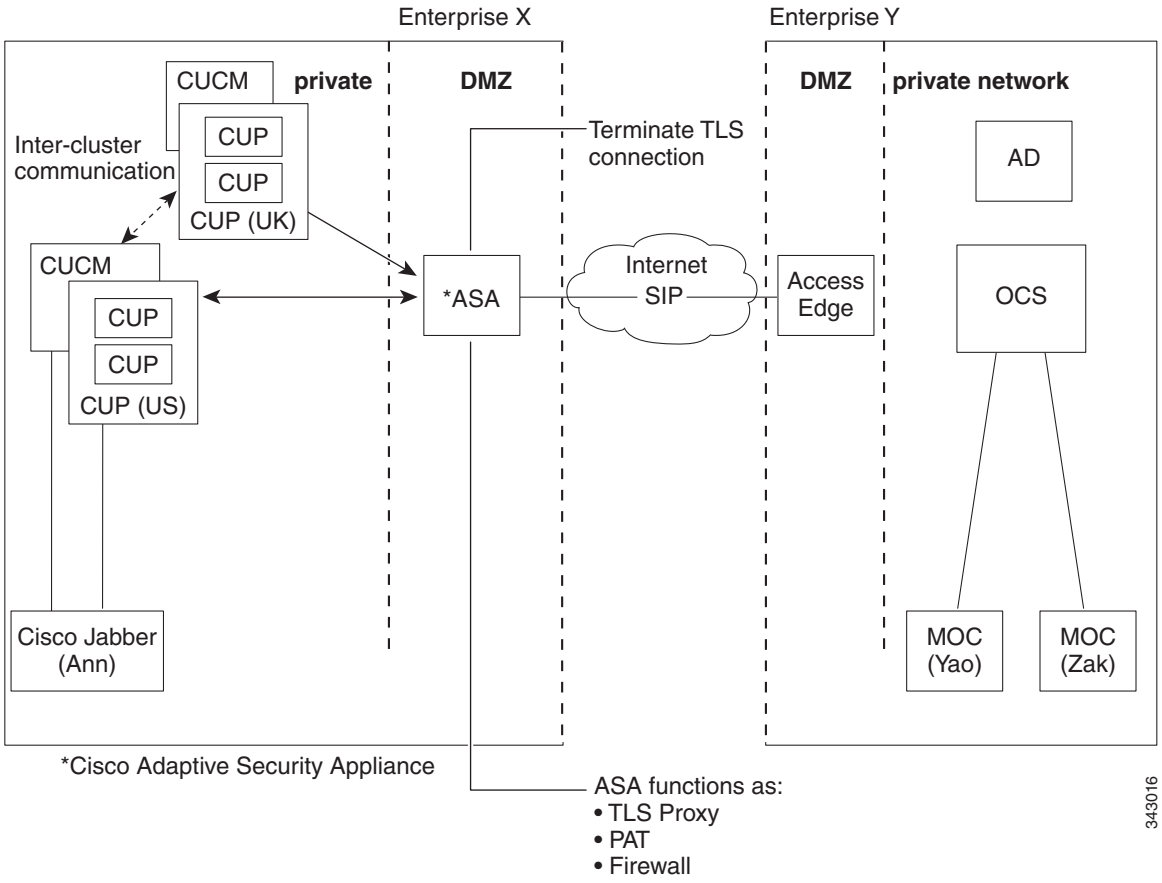
- IBM Sametime Server 8.2 and 8.5
- Cisco Webex Connect Release 6
- GoogleTalk
- Cisco Unified Presence Release 8.x
- Any other server that is XMPP Standards compliant

Note

- Cisco Unified Presence does *not* support federation between a Cisco Unified Presence Release 8.x enterprise, and a Cisco Unified Presence Release 7.0(x) enterprise.
- Cisco Unified Presence supports XMPP federation with GoogleTalk over TCP. XMPP federation with GoogleTalk over TLS is not supported.

Figure 1-1 provides an example of a SIP federated network between Cisco Unified Presence enterprise deployment and Microsoft OCS enterprise deployment.

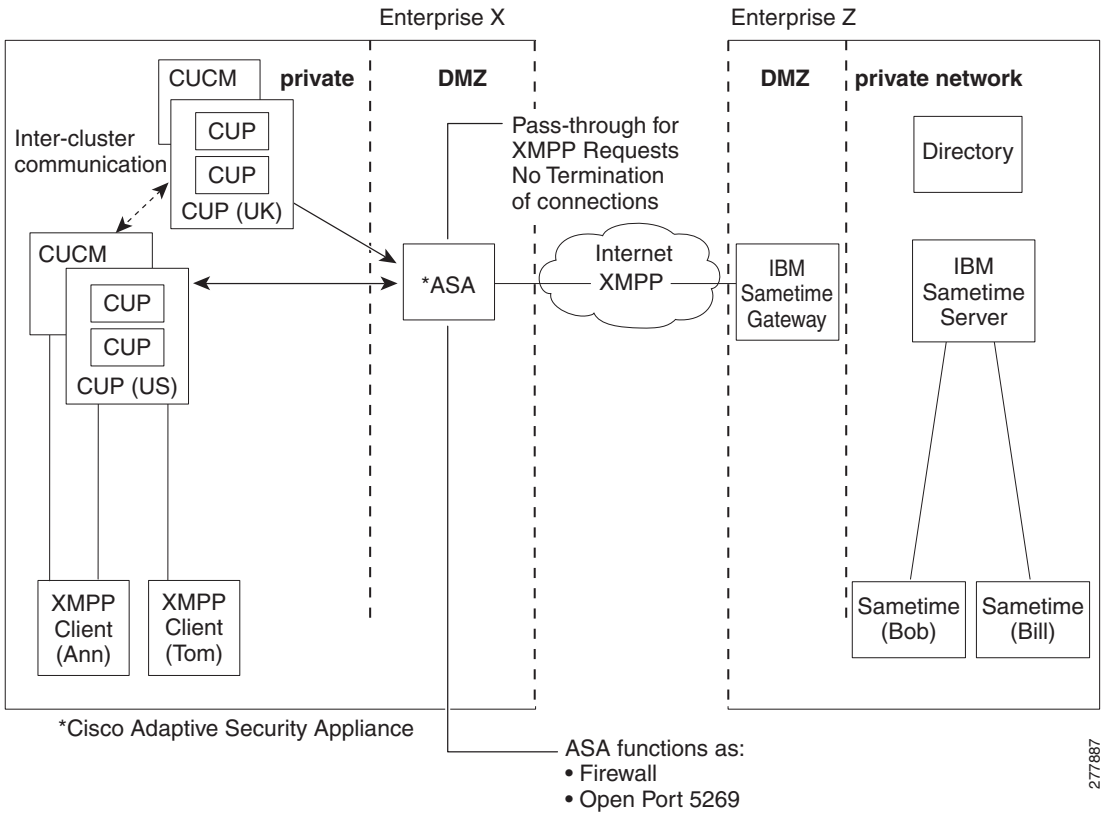
Figure 1-1 Basic SIP Federated Network between Cisco Unified Presence and Microsoft OCS



In Figure 1-1, each internal enterprise domain interconnects over the public internet using its DMZ edge server using a secure TLS connection. Within the internal Cisco Unified Presence enterprise deployment, the Cisco Adaptive Security Appliance provides firewall, Port Address Translation (PAT) and TLS proxy functionality. The Cisco Adaptive Security Appliance routes all incoming traffic initiated from the foreign domain to a designated Cisco Unified Presence server.

Figure 1-2 provides an example of an XMPP federated network between Cisco Unified Presence 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.

Figure 1-2 Basic XMPP Federated Network between Cisco Unified Presence and IBM Sametime



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

About SIP Federation with AOL

Intercluster Deployments and SIP Federation with AOL

If you have an intercluster deployment that contains Cisco Unified Presence Release 7.x nodes, and Cisco Unified Presence Release 8.5 (and later) nodes, you can only configure the Cisco Unified Presence Release 8.5 (and later) nodes to federate with AOL.

Note the following points:

- An AOL user may see availability status of a Cisco Unified Presence Release 7.x intercluster contact. The Available state displays correctly, but all other states display as offline.

- A Cisco Unified Presence Release 7.x intercluster user cannot see the availability status of AOL contacts.
- AOL users and Cisco Unified Presence Release 7.x intercluster contacts cannot exchange instant messages.
- We recommend that you do *not* configure AOL as a federated domain on Cisco Unified Presence Release 7.x. This configuration is *not* supported. Consequently, on Cisco Unified Presence Release 7.x, Cisco Unified Personal Communicator users cannot add federated AOL contacts.

Limitation with AOL Federation

Users in the AOL community (aol.com, aim.com) can use an existing email address as their screen name in AOL. This is existing email address that the user holds with any other public email provider, for example gmail.com, yahoo.com, msn.com and so on. In this scenario AOL expects a mapped JID when it addresses these users,, for example user(gmail.com)@aol.com, and similarly AOL sends out a modified JID.

For example, AOL addresses the user with this screenname‘user@gmail.com’ as follows:

```
SUBSCRIBE sip:user(gmail.com)@aol.com SIP/2.0
From: sip:user@cisco.com;tag=
To: sip:user(gmail.com)@aol.com
```

AOL sends out this modified JID for this user:

```
SUBSCRIBE sip:user@cisco.com SIP/2.0
From: sip:user(gmail.com)@aol.com ;tag=
To: sip:user@cisco.com
```

If you deploy SIP federation with AOL, Cisco Unified Presence does not support these AOL users whose screen names are an email address, and not a userID.

Note that AOL routing is different to OCS routing in that AOL does not obey the SIP record-route;all requests from AOL are sent to the routing Cisco Unified Presence server, even if the original request was initiated from one of the other Cisco Unified Presence nodes. As a result, when you configure AOL federation, the federation routing Cisco Unified Presence may experience more load than it would when it federates with OCS.

About Intercluster and Multi-node Deployments

- SIP Federation Deployments, page 1-6
- XMPP Federation Deployments, page 1-6

Note Any configuration procedures in this document that relate to intercluster Cisco Unified Presence deployments, you can also apply these procedures to multi-node Cisco Unified Presence deployments.

SIP Federation Deployments

In an intercluster and a multi-node cluster Cisco Unified Presence deployment, when a foreign domain initiates a new session, Cisco Adaptive Security Appliance routes all messages to a Cisco Unified Presence server that is designated for routing purposes. If the Cisco Unified Presence routing server does not host the recipient user, it routes the message via intercluster communication to the appropriate Cisco Unified Presence server within the cluster. The system routes all responses that are associated with this request through the routing Cisco Unified Presence server.

Any Cisco Unified Presence server can initiate a message to a foreign domain via Cisco Adaptive Security Appliance. On OCS, when the foreign domain replies to these messages, the replies are sent directly back to the Cisco Unified Presence server that initiated the message via Cisco Adaptive Security Appliance. You enable this behavior when you configure Port Address Translation (PAT) on Cisco Adaptive Security Appliance. However, for AOL federation, all responses will be routed through the routing Cisco Unified Presence routing server. We recommend that you configure PAT on Cisco Adaptive Security Appliance as PAT is required for the 200 ok response messages.

Related Topics

- About Port Address Translation (PAT), page 6-3
- Intercluster Deployments and SIP Federation with AOL, page 1-4

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 Cisco Unified Presence node that is enabled for XMPP Federation. All incoming requests from foreign domains will be routed to the node running XMPP federation, based on the published SRV record. Internally Cisco Unified Presence reroutes the requests to the correct node for the user. Cisco Unified Presence also routes all outgoing requests via the node running XMPP federation.

You can also publish multiple DNS SRV records, for example, for scale purposes, or if you have multiple Cisco Unified Presence 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 Cisco Unified Presence enterprise domain. As a result, Cisco Unified Presence can route incoming requests to any one of the published nodes that you enable for XMPP federation.

In an intercluster and a multi-node cluster Cisco Unified Presence deployment, when a foreign 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; Cisco Unified Presence can route the request to any of the servers that DNS publishes. Internally Cisco Unified Presence reroutes the requests to the correct node for the user. Cisco Unified Presence 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, Cisco Unified Presence routes all incoming requests via that single node, rather than load-balancing the incoming requests across the nodes running XMPP federation. Cisco Unified Presence will load-balance outgoing requests and send outgoing request via any of the nodes running XMPP federation within the cluster.

About High Availability and Federation

High Availability for SIP Federation

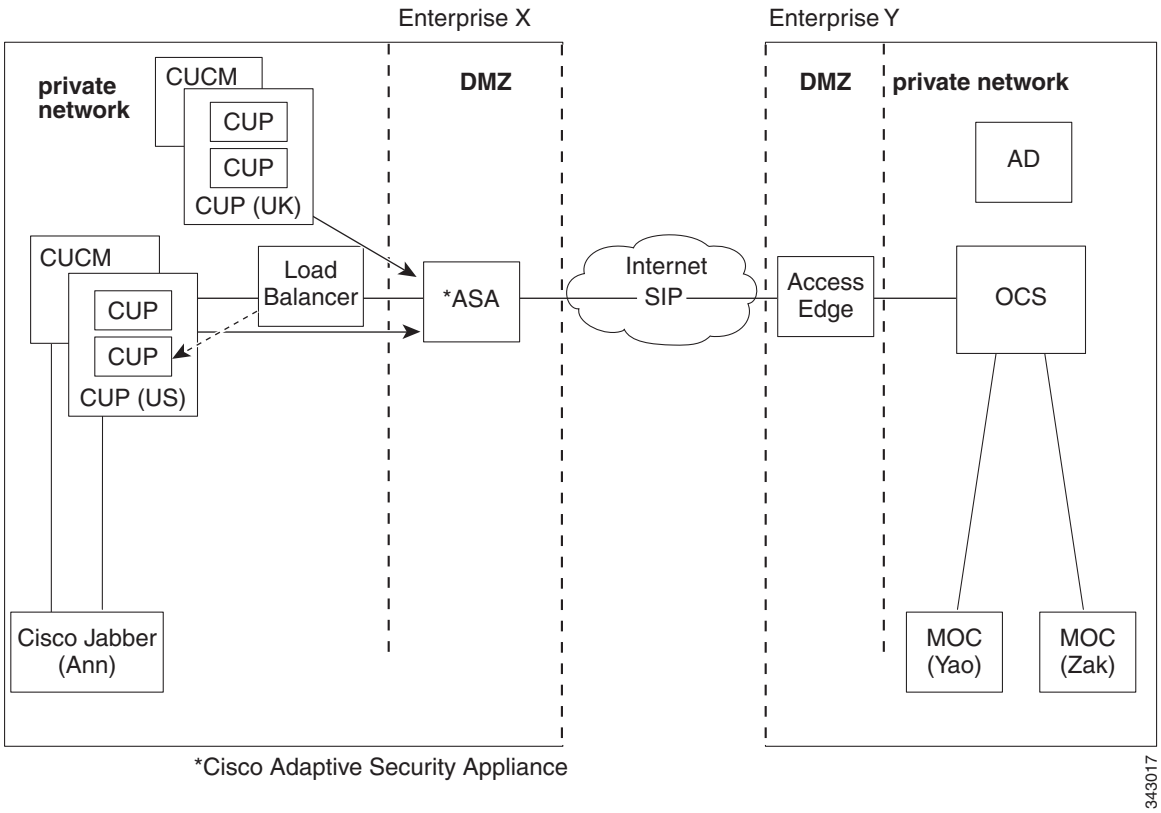
Note Only Cisco Unified Presence Release 8.5 or later supports high availability.

If you are federating with a Microsoft OCS enterprise, 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 OCS, you must incorporate a load balancer between the Cisco Unified Presence server and Cisco Adaptive Security Appliance, as shown in Figure 1-3. 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. Currently only the Cisco CSS11506 Content Services Switch supports TLS.

Similarly, in order to achieve high availability when federating with AOL, you must incorporate a load balancer between the Cisco Unified Presence server and Cisco Adaptive Security Appliance, as shown in Figure 1-3.

Figure 1-3 Federated Network between Cisco Unified Presence and Microsoft OCS with High Availability



Related Topic

Configuring the Load Balancer for Redundancy for SIP Federation, page 10-1

High Availability for XMPP Federation

Note Only Cisco Unified Presence Release 8.5 or later supports high availability.

High availability for XMPP federation differs from the high availability model for other Cisco Unified Presence 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 Cisco Unified Presence 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

Cisco Unified Presence evenly load balances outbound requests from users within that cluster across all the XMPP federation enabled nodes in the cluster. If any node fails, Cisco Unified Presence 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 a foreign domain to discover the local Cisco Unified Presence deployment, a DNS SRV record must be published on a public DNS server. This record resolves to an XMPP federation enabled node. The foreign domain then connects to the resolved address.

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

These records provide a choice of DNS SRV records for the local deployment. If an XMPP federation enabled node fails, the foreign system will have other options from which to connect to the local Cisco Unified Presence Deployment.

Note

- Each published DNS SRV records must have the same priority and weight. This will allow for an spread of load across all published records, and will also allow for the foreign 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 a Cisco Unified Presence server in an XMPP federation deployment, you can publish multiple DNS SRV records for chat node aliases also. This will allow the foreign 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

Cisco Unified Presence Releases 8.5 and later do *not* support high availability for interdomain federation between a Cisco Unified Presence 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 Cisco Unified Presence in an IBM Sametime federation deployment. If users have failed over to the backup node due to critical services failing, but the Cisco UP 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.

GoogleTalk Federation

Cisco Unified Presence Releases 8.5 and later do *not* support high availability for interdomain federation between a Cisco Unified Presence enterprise and GoogleTalk.

Related Topics

- How to Configure DNS for XMPP Federation, page 11-5
- Turning on XMPP Federation on a Node, page 11-2

Cisco Adaptive Security Appliance Deployment Options

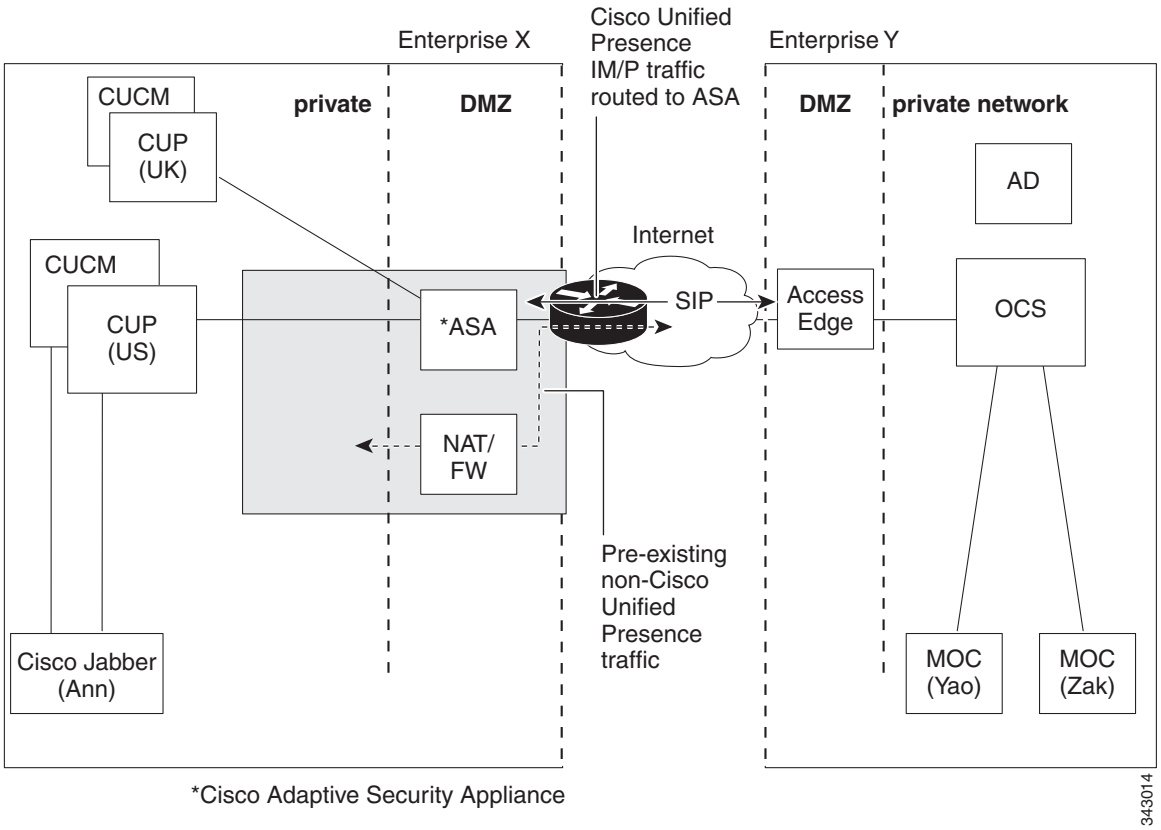
Within the internal Cisco Unified Presence enterprise deployment, the Cisco Adaptive Security Appliance provides firewall, Port Address Translation (PAT) and TLS proxy functionality in the DMZ to terminate the incoming connections from the public internet, and permit traffic from specific federated domains.

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.

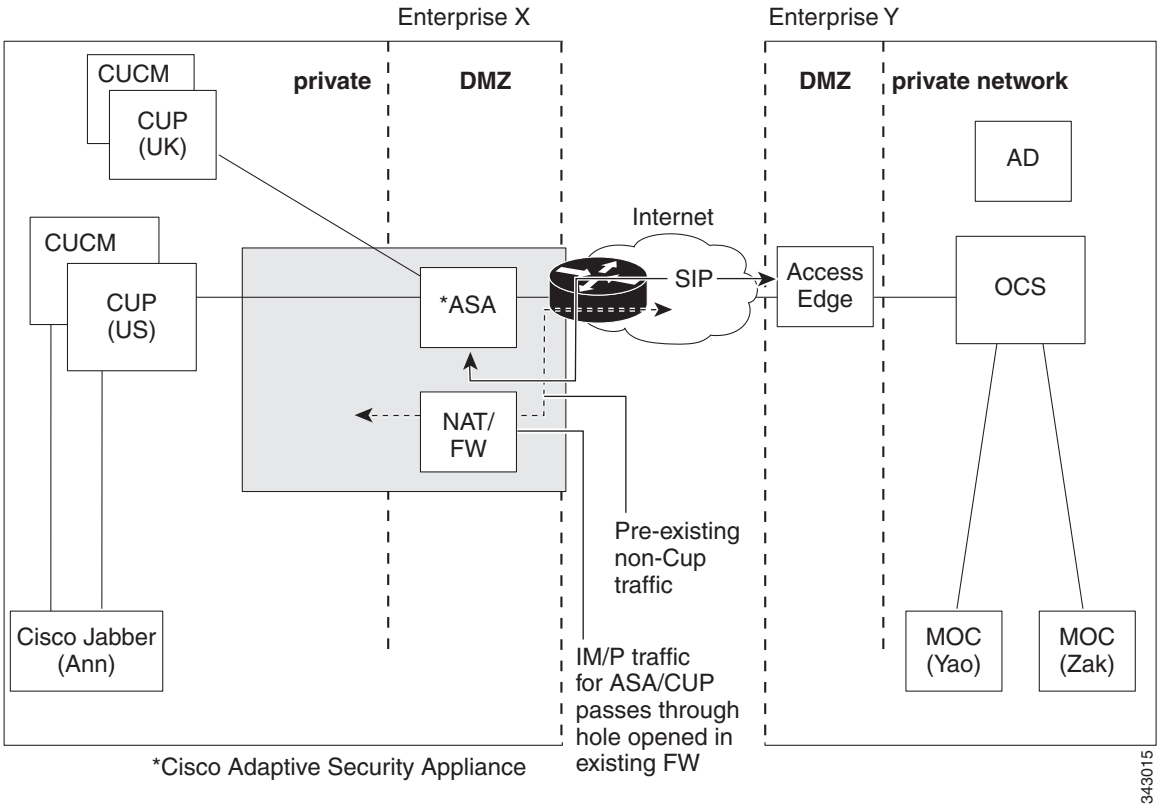
You can deploy the Cisco Adaptive Security Appliance as the enterprise firewall that protects Instant Messaging (IM) traffic, Presence traffic and other traffic, as illustrated in Figure 1-1 and Figure 1-4. This is the most cost-effective deployment, and the one we recommend for new and existing networks. You can also deploy the Cisco Adaptive Security Appliance in parallel to the existing firewall, as illustrated in Figure 1-4. In this deployment Cisco Adaptive Security Appliance handles the IM and Presence traffic between Cisco Unified Presence and the public internet, and the pre-existing traffic continues to use any existing firewall. In Figure 1-4 Cisco Adaptive Security Appliance is also deployed as a gateway for the Cisco Unified Presence server, which means that you do not require a separate router to direct traffic to Cisco Adaptive Security Appliance.

Figure 1-4 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 Cisco Unified Presence to reach the Cisco Adaptive Security Appliance, as illustrated in Figure 1-5. In this type of deployment the Cisco Adaptive Security Appliance is functioning as a gateway for the Cisco Unified Presence server.

Figure 1-5 Cisco ASA 5500 Deployed Behind Existing NAT/Firewall



Availability Subscriptions and Blocking Levels

All new availability subscriptions from “x@foreigndomain.com” to “user@local.com”are sent via the Cisco Adaptive Security Appliance, as illustrated in Figure 1-6. Cisco Adaptive Security Appliance checks the inbound SIP subscriptions against the list of permitted foreign domains. If the domain is not permitted, Cisco Adaptive Security Appliance denies the availability subscription.

Note In an XMPP federation deployment, Cisco Adaptive Security Appliance does not perform any domain checks.

On receipt of the inbound subscription, Cisco Unified Presence verifies that the foreign domain is one of the permitted federated domains that you define at the administration level on the Cisco Unified Presence server. 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, Cisco Unified Presence denies the subscription (without contacting the local user).

If the subscription is from a permitted domain, Cisco Unified Presence 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 availability subscription. Cisco Unified Presence then accepts the incoming subscription and places it in a pending state.

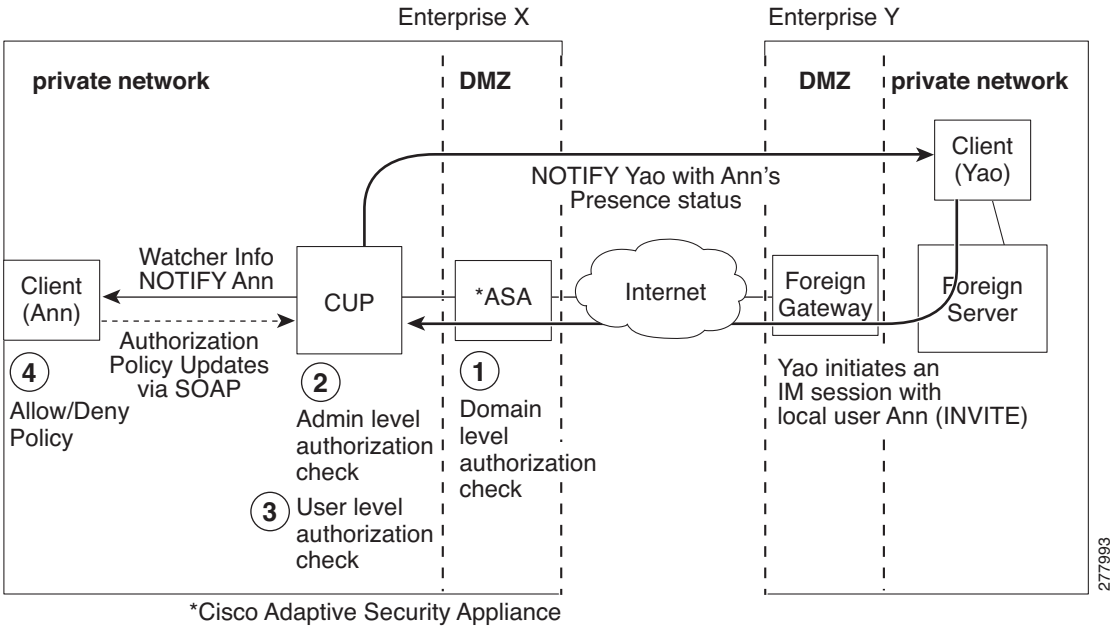
Cisco Unified Presence notifies the local user that "x@foreigndomain.com" wants to watch their availability by sending the client application a notification message for the subscription. This triggers a dialog box on the client application that enables the local user to allow or deny the subscription.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

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 Cisco Unified Presence User Options interface.

A deny decision is handled using polite blocking, which means that the availability state of the user appears offline on the foreign client. If the local user allows the subscription, Cisco Unified Presence sends availability updates to the foreign watcher.

The user can also block subscriptions on a per user and a per domain basis. This can be configured via the Cisco Unified Presence User Options interface, and the Cisco Jabber client.

Figure 1-6 Inbound SIP Presence Message Flow

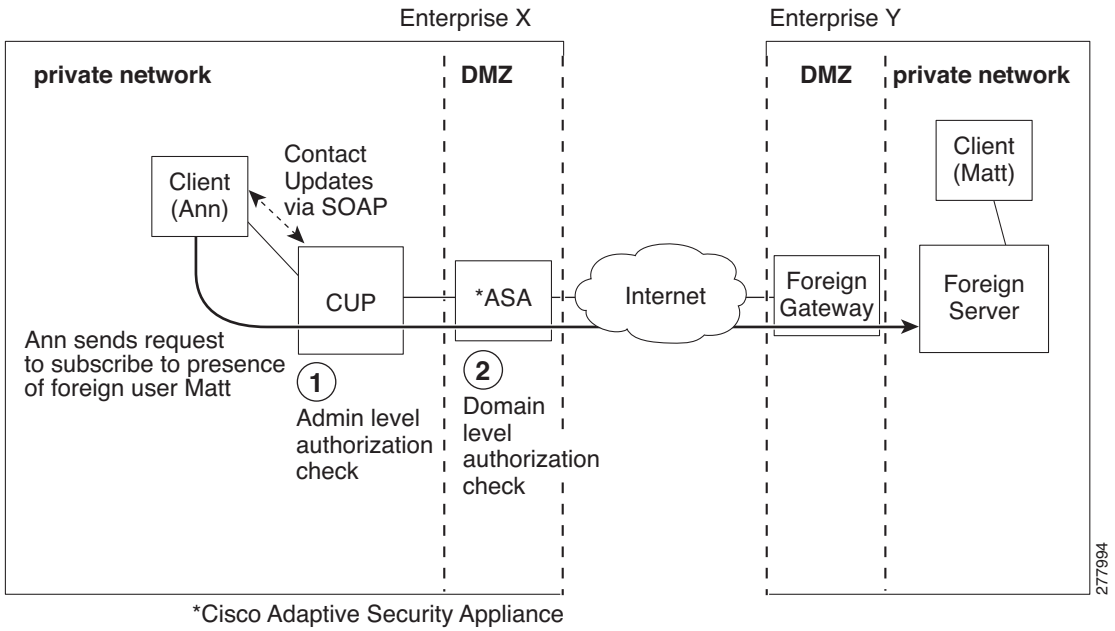


Cisco Unified Presence sends all outgoing subscriptions through Cisco Adaptive Security Appliance, and Cisco Adaptive Security Appliance forwards these subscriptions to the foreign domain. Cisco Unified Presence sends an outgoing subscription even if an active subscription already exists between a different local user to the same foreign user in the same foreign domain. Figure 1-7 illustrates an outgoing availability subscription flow.

The foreign user is added to the contact list on the client application and the Cisco Unified Presence User Options interface as "user@foreigndomain.com".

Note The domain level authentication check is not applied on Cisco Adaptive Security Appliance for XMPP federation.

Figure 1-7 Outbound Presence Request Flow



Note

- Microsoft OCS performs a refresh subscribe every one hour and 45 minutes. Therefore, if a Cisco Unified Presence server restarts, the maximum duration a Microsoft Office Communicator client will be without the availability status of Cisco Unified Presence contacts is approximately two hours.
- If Microsoft OCS restarts, the maximum duration a Cisco Unified Presence client will be without availability status of Microsoft Office Communicator contacts is approximately two hours.

Related Topics

- About Availability State Mappings, page 1-14
- About Instant Messaging, page 1-21

About Availability State Mappings

- Availability State Mappings for Microsoft OCS, page 1-15
- Availability State Mappings for Microsoft Lync, page 1-16
- Availability State Mappings for AOL Instant Messenger, page 1-18
- Availability State Mappings for XMPP Federation, page 1-18

Availability State Mappings for Microsoft OCS

Table 1-1 shows the availability mapping states from Microsoft Office Communicator to Cisco Unified Presence, third-party XMPP clients and Cisco Unified Personal Communicator.

Table 1-1 Availability Mapping States from Microsoft Office Communicator

Microsoft Office Communicator Setting	Third-party XMPP Client Setting (connected to Cisco Unified Presence)	Cisco Unified Personal Communicator Release 7.x Setting	Cisco Unified Personal Communicator Release 8.x Setting
Available	Available	Available	Available
Busy	Away	Away	Busy
Do Not Disturb	Away	Away	Busy
Be Right Back	Away	Away	Away
Away	Away	Away	Away
Offline	Offline	Offline	Offline

In Table 1-1, 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 will show the "Away" icon with no text. Other XMPP clients will render the "Away" icon with "Busy" text annotation alongside.

Table 1-2 shows the availability mapping states from Cisco Unified Personal Communicator Release 7.x to Microsoft Office Communicator.

Table 1-2 Availability Mapping States from Cisco Unified Personal Communicator Release 7.x

Cisco Unified Personal Communicator Release 7.x Setting	Microsoft Office Communicator Setting
Available	Available
Away	Away
Do Not Disturb	Busy
Offline	Offline
Invisible	Away

Table 1-3 shows the availability mapping states from Cisco Unified Personal Communicator Release 8.x to Microsoft Office Communicator.

Table 1-3 Availability Mapping States from Cisco Unified Personal Communicator Release 8.x

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

Table 1-4 shows the availability mapping states from third-party XMPP clients, that are connected to Cisco Unified Presence, to Microsoft Office Communicator.

Table 1-4 Availability Mapping States from Third-party XMPP Client

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

Related Topics

Availability Subscriptions and Blocking Levels, page 1-12

Availability State Mappings for Microsoft Lync

Table 1-5 shows the availability mapping states from Microsoft Lync to Cisco Unified Presence, third-party XMPP clients and Cisco Unified Personal Communicator.

Table 1-5 Availability Mapping States from Microsoft Lync

Microsoft Lync Setting	Third-party XMPP Client Setting (connected to Cisco Unified Presence)	Cisco Unified Personal Communicator Release 7.x Setting	Cisco Unified Personal Communicator Release 8.x Setting
Available	Available	Available	Available
Busy	Away	Away	Busy
Do Not Disturb	Away	Away	Busy
Be Right Back	Away	Away	Away
Away	Away	Away	Away
Offline	Offline	Offline	Offline

In Table 1-5, 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 will show the "Away" icon with no text. Other XMPP clients will render the "Away" icon with "Busy" text annotation alongside.

Table 1-6 shows the availability mapping states from Cisco Unified Personal Communicator Release 7.x to a Lync client.

Table 1-6 Availability Mapping States from Cisco Unified Personal Communicator Release 7.x

Cisco Unified Personal Communicator Release 7.x Setting	Microsoft Lync Setting
Available	Available
Away	Away
Do Not Disturb	Busy
Offline	Offline
Invisible	Away

Table 1-7 shows the availability mapping states from Cisco Unified Personal Communicator Release 8.x to a Lync client.

Table 1-7 Availability Mapping States from Cisco Unified Personal Communicator Release 8.x

Cisco Unified Personal Communicator Release 8.x Setting	Microsoft Lync Setting
Available	Available
Busy	Busy
Do Not Disturb	Busy
Offline	Offline

Table 1-8 shows the availability mapping states from third-party XMPP clients, that are connected to Cisco Unified Presence, to a Lync client.

Table 1-8 Availability Mapping States from Third-party XMPP Client

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

Related Topics

Availability Subscriptions and Blocking Levels, page 1-12

Availability State Mappings for AOL Instant Messenger

Table 1-9 shows the availability mapping states from AOL Instant Messenger to Cisco Unified Personal Communicator.

Table 1-9 Availability Mapping States from AOL Instant Messenger to Cisco Unified Personal Communicator

AOL Instant Messenger Setting	Cisco Unified Personal Communicator Release 7.x Setting	Cisco Unified Personal Communicator Release 8.x Setting
Available	Available	Available
Away	Away	Away
Invisible	Offline	Offline
Offline	Offline	Offline

Table 1-10 shows the availability mapping states from Cisco Unified Personal Communicator to AOL Instant Messenger.

Table 1-10 Availability Mapping States from Cisco Unified Personal Communicator to AOL Instant Messenger

Cisco Unified Personal Communicator Release 7.x Setting	Cisco Unified Personal Communicator Release 8.x Setting	AOL Instant Messenger
Available	Available	Available
Do Not Disturb	Do Not Disturb	Away
Away	Busy	Away
Idle	Idle	Away
Offline	Offline	Offline

Related Topics

Availability Subscriptions and Blocking Levels, page 1-12

Availability State Mappings for XMPP Federation

Table 1-11 shows the availability mapping states from IBM Sametime 8.2 to a third-party XMPP client on Cisco Unified Presence, and to Cisco Unified Personal Communicator.

Table 1-11 Availability Mapping States from IBM Sametime 8.2 client

IBM Sametime Client Setting	Third-party XMPP Client Setting (connected to Cisco Unified Presence)	Cisco Unified Personal Communicator Setting Release 7.x	Cisco Unified Personal Communicator Setting Release 8.x
Available	Available	Available	Available with status message
Do Not Disturb	Do Not Disturb	Do Not Disturb	Do Not Disturb with status message

Table 1-11 Availability Mapping States from IBM Sametime 8.2 client (continued)

IBM Sametime Client Setting	Third-party XMPP Client Setting (connected to Cisco Unified Presence)	Cisco Unified Personal Communicator Setting Release 7.x	Cisco Unified Personal Communicator Setting Release 8.x
Available with status "In a meeting"	Available with status "In a meeting"	Available with status "In a meeting"	Available with status message
Away	Away	Away	Away with status message
Offline	Offline	Offline	Offline

Table 1-12 shows the availability mapping states from webex Connect to a third-party XMPP client on Cisco Unified Presence, and to Cisco Unified Personal Communicator.

Table 1-12 Availability Mapping States from Webex Connect

Webex Connect Setting	Third-party XMPP Client Setting (connected to Cisco Unified Presence)	Cisco Unified Personal Communicator Setting Release 7.x	Cisco Unified Personal Communicator Setting Release 8.x
Available	Available	Available	Available
Do Not Disturb	Do Not Disturb	Do Not Disturb	Do Not Disturb
Away with status "In a meeting"	Available with status "In a meeting"	Away with status "In a meeting"	Away with status "In a meeting"
Away	Away	Away	Away
Offline	Offline	Offline	Offline

Table 1-13 shows the availability mapping states from Cisco Unified Personal Communicator Release 7.x to other federated clients.

Table 1-13 Availability Mapping States from Cisco Unified Personal Communicator Release 7.x

Cisco Unified Personal Communicator Release 7.x Setting	Federated Cisco Unified Personal Communicator Release 7.x Setting	Federated Cisco Unified Personal Communicator Release 8.x Setting	Federated Third-party XMPP Client Setting (connected to Cisco Unified Presence)	Webex Connect Client Setting	IBM Sametime Client Server
Available	Available	Available	Available	Available	Available
Do Not Disturb	Do Not Disturb	Do Not Disturb	Do Not Disturb	Do Not Disturb	Do Not Disturb
Away	Away	Away	Away	Away	Away
Idle	Idle	Idle	Away with status "Idle"	Away with status "Idle"	Extended Away
Offline	Offline	Offline	Offline	Offline	Offline

Table 1-14 shows the availability mapping states from Cisco Unified Personal Communicator Release 8.x to other federated clients.

Table 1-14 Availability Mapping States from Cisco Unified Personal Communicator Release 8.x

Cisco Unified Personal Communicator Release 8.x Setting	Federated Cisco Unified Personal Communicator Release 7.x Setting	Federated Cisco Unified Personal Communicator Release 8.x Setting	Federated Third-party XMPP Client Setting (connected to Cisco Unified Presence)	Webex Connect Client Setting	IBM Sametime Client Server
Available	Available	Available	Available	Available	Available
Do Not Disturb	Do Not Disturb	Do Not Disturb	Do Not Disturb	Do Not Disturb	Do Not Disturb
Busy	Away	Busy	Away	Idle	Away
Idle	Idle	Idle	Idle	Idle	Idle
Offline	Offline	Offline	Offline	Offline	Offline

Table 1-15 shows the availability mapping states from a third-party XMPP client on Cisco Unified Presence to other federated clients.

Table 1-15 Availability Mapping States from XMPP Client Connected to Cisco Unified Presence

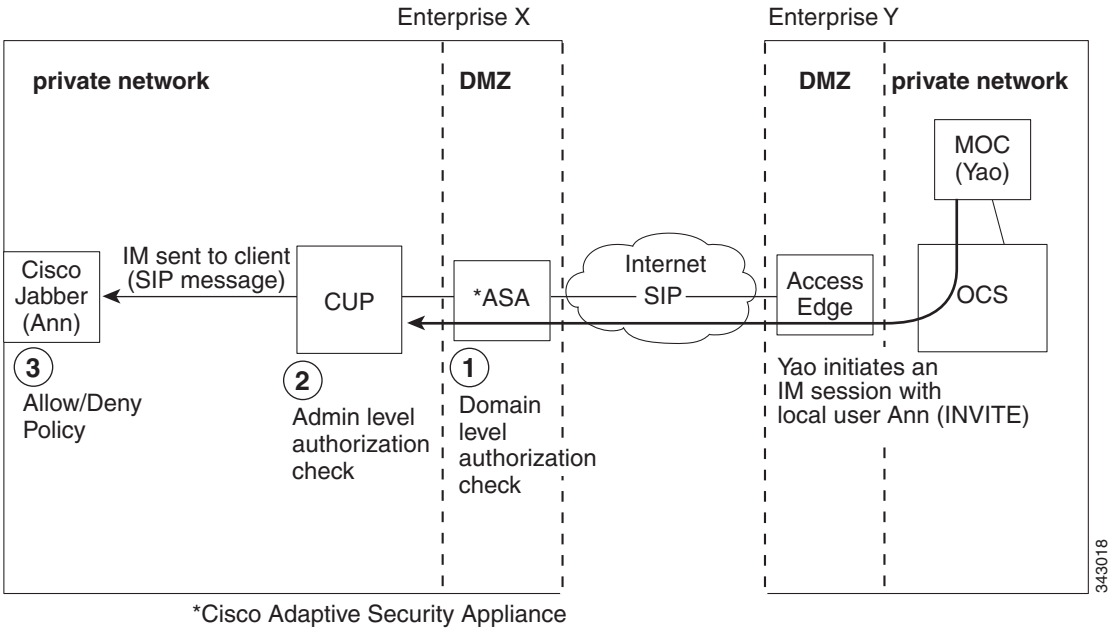
Third-party XMPP Client Setting (connected to Cisco Unified Presence)	Federated Cisco Unified Personal Communicator Release 7.x Setting	Federated Cisco Unified Personal Communicator Release 8.x Setting	Federated XMPP Client Setting (connected to Cisco Unified Presence)	Webex Connect Client Setting	IBM Sametime Client Server
Available	Available	Available	Available	Available	Available
Do Not Disturb	Do Not Disturb	Do Not Disturb	Do Not Disturb	Do Not Disturb	Do Not Disturb
Away	Away	Away	Away	Away	Away
Extended Away	Away	Away	Extended Away	Extended Away	Away
Away with status “Idle”	Idle	Idle	Away with status “Idle”	Away with status “Idle”	Away with status “Idle”
Offline	Offline	Offline	Offline	Offline	Offline

About Instant Messaging

Instant Message Flow for SIP Federation

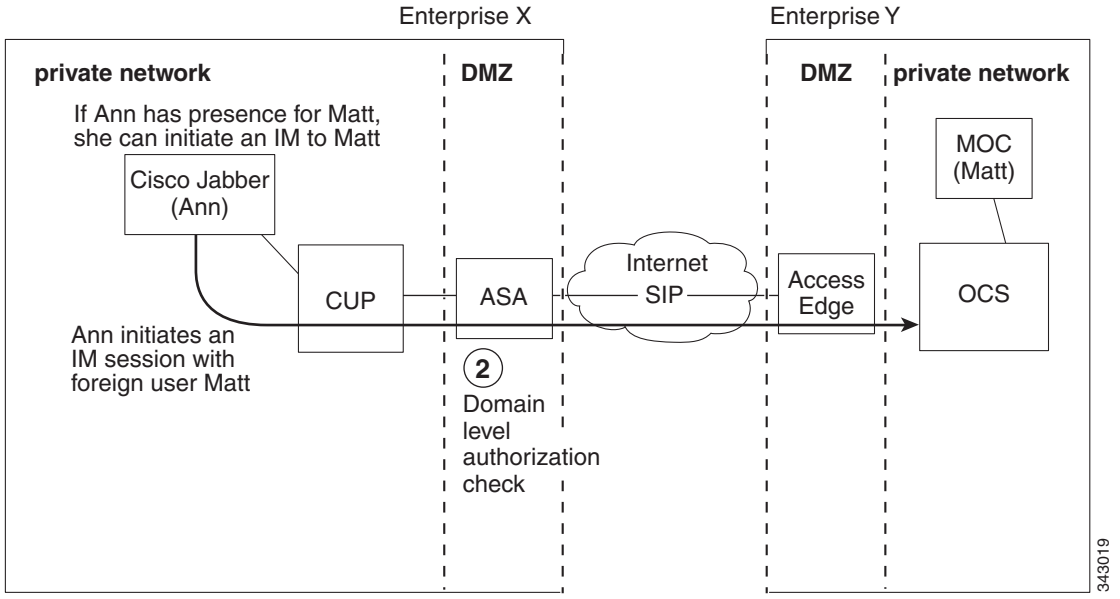
Instant Messages (IMs) that are sent between two enterprise deployments use Session Mode. When a user in a foreign domain sends an IM to a local user in the Cisco Unified Presence domain, the foreign server sends an INVITE message, as illustrated in Figure 1-8. Cisco Adaptive Security Appliance forwards the INVITE message to Cisco Unified Presence. Cisco Unified Presence replies with a 200 OK message to the foreign server, and the foreign server sends a SIP MESSAGE containing the text data. Cisco Unified Presence forwards the text data to the client application of the local user, using the appropriate protocol.

Figure 1-8 Inbound Instant Messaging Flow



When a local user in the Cisco Unified Presence domain sends an IM to a user in a foreign domain, the IM is sent to the Cisco Unified Presence server. If no existing IM session is established between these two users, Cisco Unified Presence sends an INVITE message to the foreign domain to establish a new session. Figure 1-9 illustrates this flow. Cisco Unified Presence 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 1-9 Outbound Instant Message Flow



Note Cisco Unified Presence does not support a three-way IM session (group chat) with a Microsoft OCS contact.

Related Topic

Availability Subscriptions and Blocking Levels, page 1-12

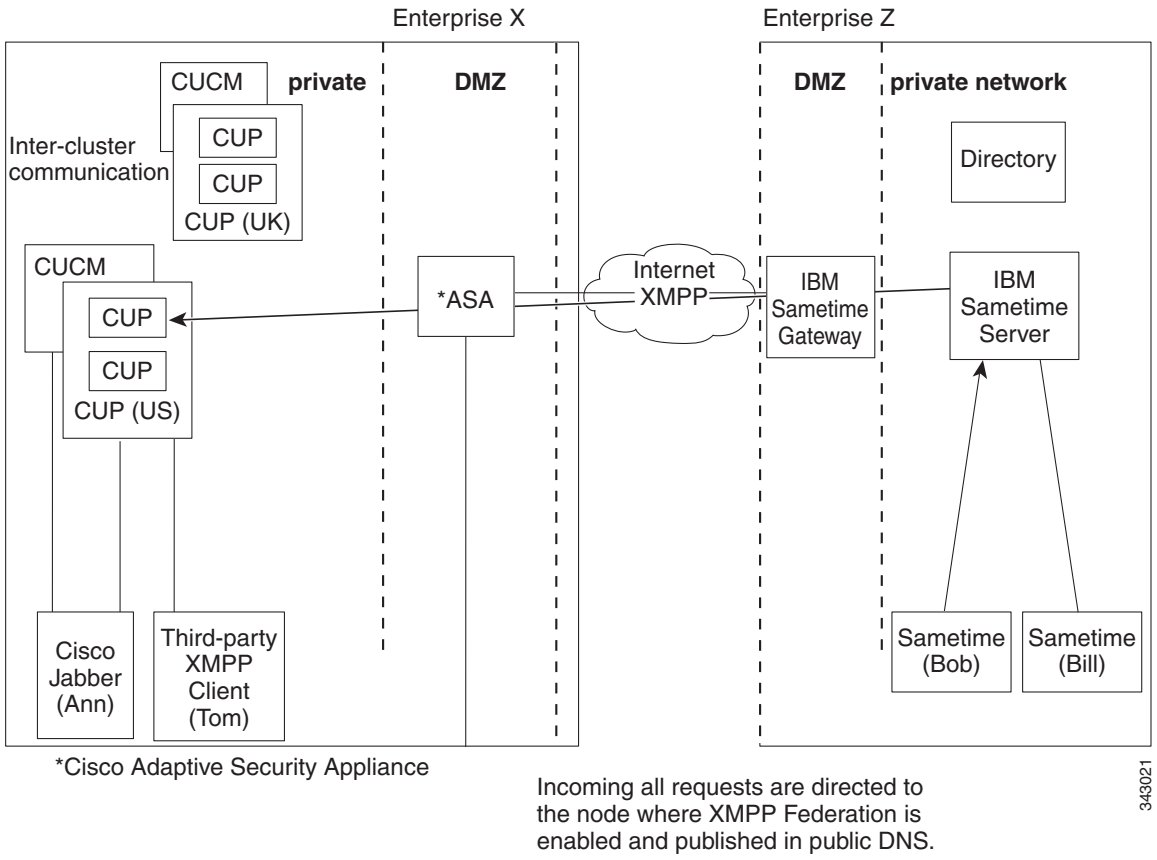
Availability and Instant Message Flow for XMPP Federation

The flow of incoming and outgoing availability and IM requests for XMPP federation can vary in a multi-node Cisco Unified Presence deployment.

In a multi-node 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).

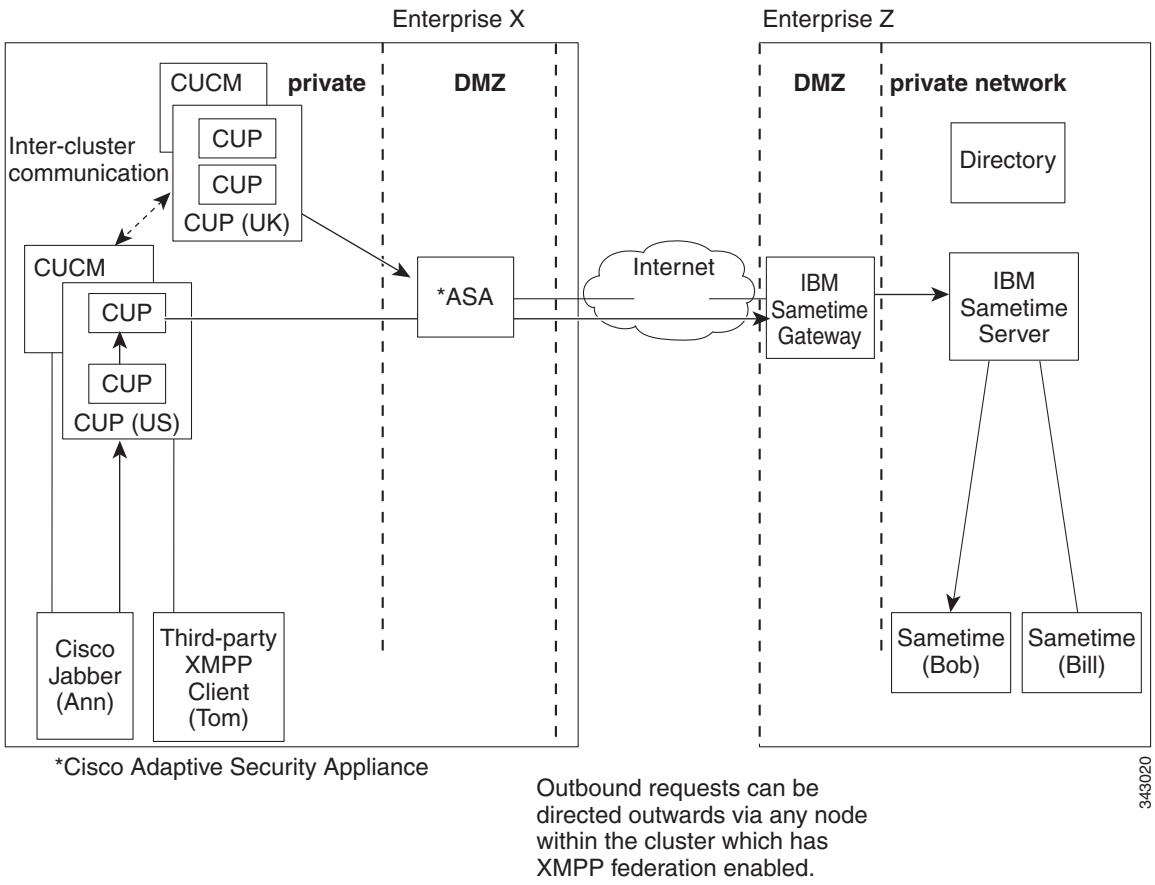
If you only publish a single DNS SRV record, the system routes all inbound requests to that single node, and internally Cisco Unified Presence routes the traffic to the correct node using intercluster routing, as illustrated in Figure 1-10. If you publish multiple DNS SRV records, depending on how you configure the SRV records, the system could load-balance inbound requests across each node.

Figure 1-10 XMPP Inbound Request Flow



Cisco Unified Presence 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 Figure 1-11.

Figure 1-11 XMPP Outbound Request Flow



Related Topic

High Availability for XMPP Federation, page 1-8

Federation and Subdomains

Cisco Unified Presence supports the following subdomain scenarios:

- Cisco Unified Presence belongs to a subdomain of the foreign domain. For example, Cisco Unified Presence belongs to the subdomain "cup.cisco.com". Cisco Unified Presence federates with a foreign enterprise that belongs to the domain "cisco.com". In this case, the Cisco Unified Presence user is assigned the URI "*cupuser*@cup.cisco.com", and the foreign user has the URI "*foreignuser*@cisco.com".
- Cisco Unified Presence belongs to a parent domain, and the foreign enterprise belongs to a subdomain of that parent domain. For example, Cisco Unified Presence belongs to the domain "cisco.com". Cisco Unified Presence federates with a foreign enterprise that belongs to the subdomain "foreign.cisco.com". In this case, the Cisco Unified Presence user is assigned the URI "*cupuser*@cisco.com", and the foreign user is assigned the URI "*foreignuser*@foreign.cisco.com".

- Cisco Unified Presence and the foreign enterprise each belong to different subdomains, but both of these subdomains belong to the same parent domain. For example, Cisco Unified Presence belongs to the subdomain "cup.cisco.com" and the foreign enterprise belongs to the subdomain "foreign.cisco.com". Both of these subdomains belong to the parent domain "cisco.com". In this case, the Cisco Unified Presence user is assigned the URI "*cupuser*@cup.cisco.com" and the foreign 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, Cisco Unified Presence users or foreign 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 "cup.cisco.com" or "foreign.cisco.com", and may have the URI "*cupuser*@cup.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. The Cisco Jabber user must add these users as external (federated) contacts so that the Cisco Unified Presence applies the correct domain and not the local domain.

Note Cisco Unified Presence also supports the scenarios above if you configure federation between two Cisco Unified Presence enterprise deployments.