Main page: Cisco Unified Presence, Release 7.x

Contents

Previous Topic

- Configuring Cisco Unified Presence Release 7.x for Interdomain Federation

- About the Integration Components

- Cisco Adaptive Security Appliance Deployment Options

- About Federated Presence and Instant Messaging

- Federation and Subdomains

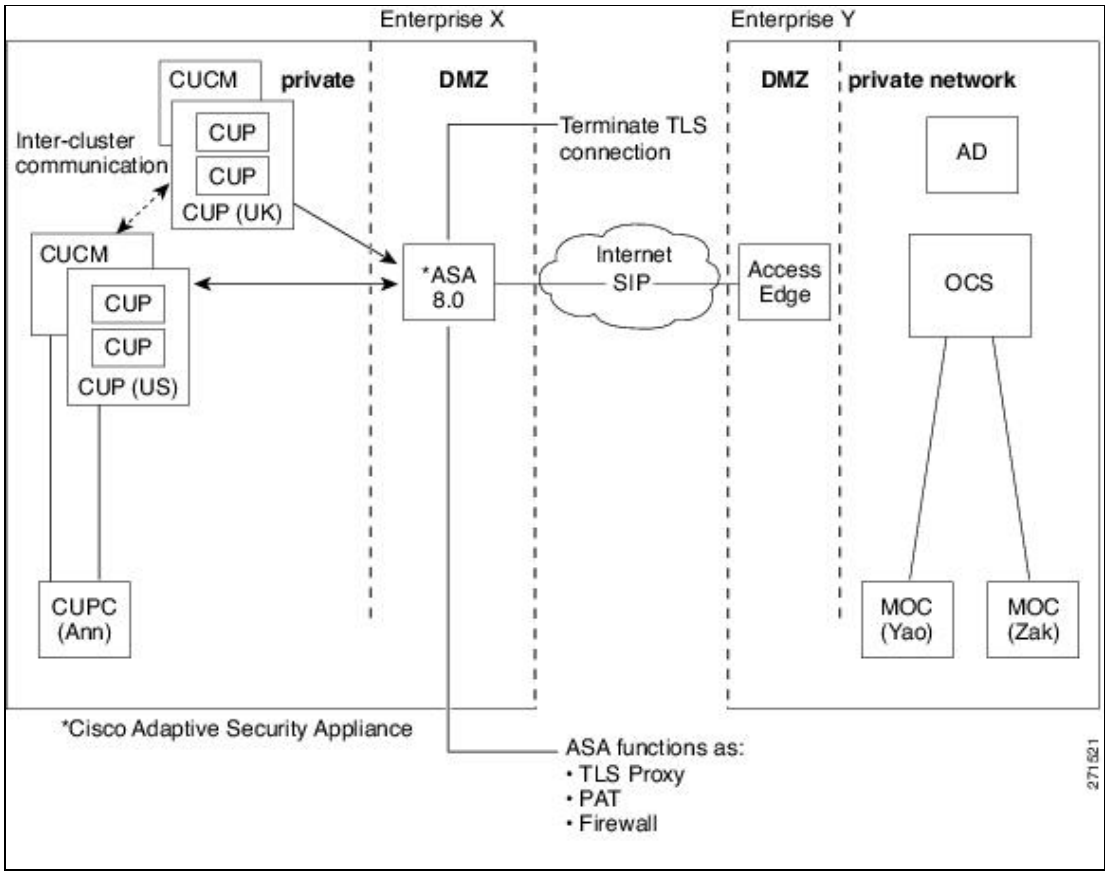
About the Integration Components

- Basic Federated Network
- Intercluster and Multi-node Deployment
- High Availability

Basic Federated Network

This integration enables Cisco Unified Presence users in one enterprise domain to exchange presence information and Instant Messaging (IM) with Microsoft Office Communications Server (OCS) or Live Communications Server (LCS) users, or Cisco Unified Presence users, in a foreign domain. See Figure: Basic Federated Network between Cisco Unified Presence and Microsoft OCS for an example of a basic example of a federated network between Cisco Unified Presence enterprise deployment and Microsoft OCS enterprise deployment.

Figure: Basic Federated Network between Cisco Unified Presence and Microsoft OCS



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.

There are two DNS servers within the internal Cisco Unified Presence enterprise deployment; one DNS server hosts the Cisco Unified Presence private address, and the other DNS server hosts the Cisco Unified Presence public address and a DNS SRV record for federating with Cisco Unified Presence. The DNS server that hosts the Cisco Unified Presence public address is located in the local DMZ.

Related Topics

- Getting More Information

Intercluster and Multi-node Deployment

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. This second Cisco Unified Presence server replies to the Cisco Unified Presence routing server; it does not reply directly to the Cisco Adaptive Security Appliance.

Any Cisco Unified Presence server can initiate a message to a foreign domain via Cisco Adaptive Security Appliance. 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.

Note: Any configuration procedures described in this document that relate to intercluster Cisco Unified Presence deployments can also be applied to multi-node Cisco Unified Presence deployments.

Related Topics

- Getting More Information

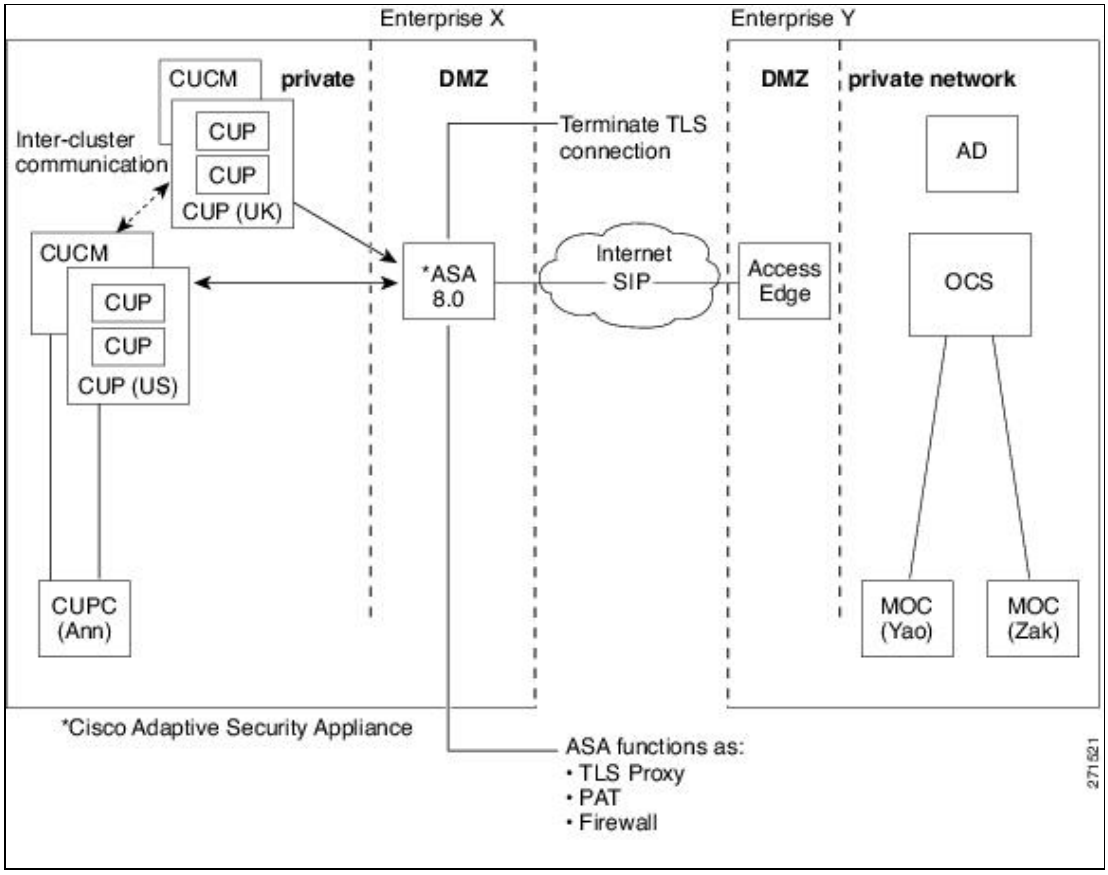
High Availability

If you are federating between one Cisco Unified Presence enterprise and another Cisco Unified Presence enterprise, you can achieve high availability by configuring multiple DNS SRV entries so the partner enterprise can failover to the backup server address. However, when 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 a Microsoft OCS enterprise, you must incorporate a load balancer between the Cisco Unified Presence server and Cisco Adaptive Security Appliance, as shown in Figure: Federated Network between Cisco Unified Presence and Microsoft OCS with High Availability. 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.

Figure: Federated Network between Cisco Unified Presence and Microsoft OCS with High Availability



Related Topics

- Configuring the Load Balancer for Redundancy
- Getting More Information

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.

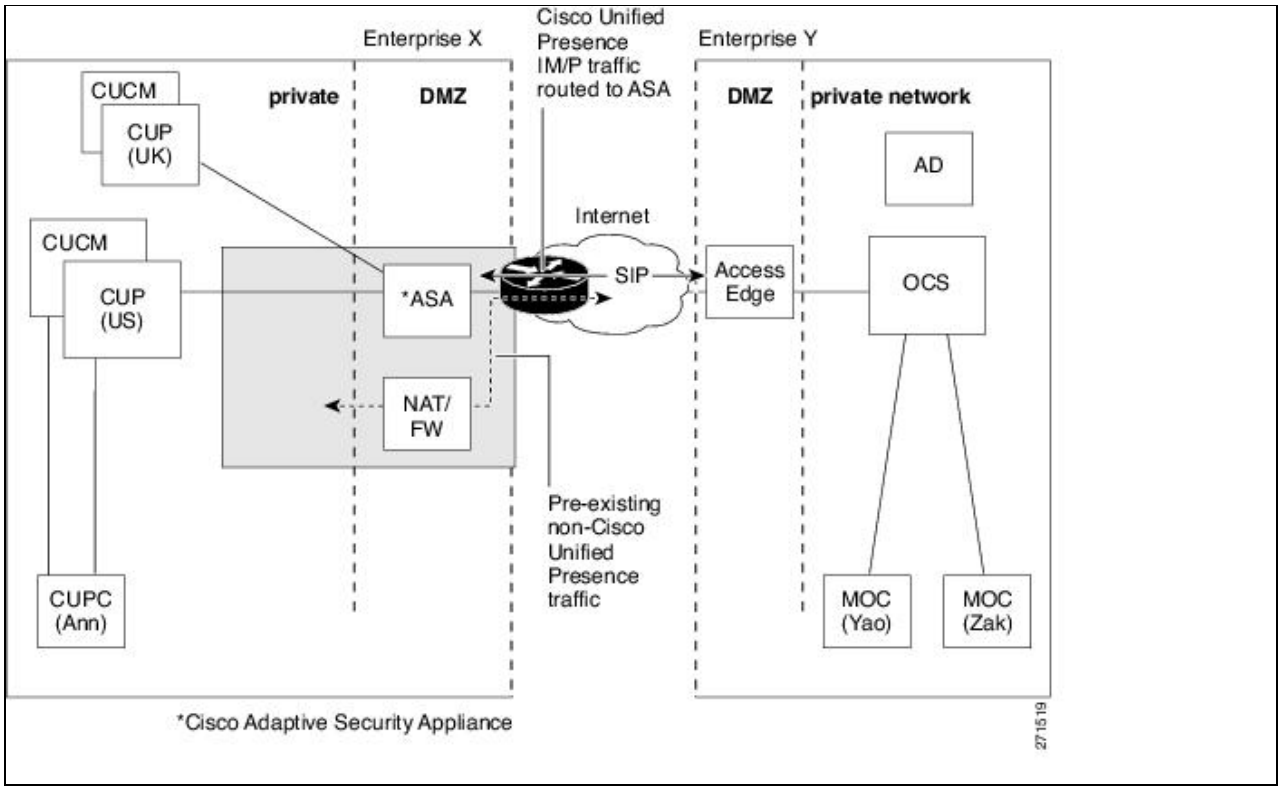
You can deploy the Cisco Adaptive Security Appliance in a number of different ways, depending on your existing network and the type of firewall functionality you desire. This section contains only an overview of the deployment models we recommend. For further details please refer to the deployment guidelines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

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: Basic Federated Network between Cisco Unified Presence and Microsoft OCS and Figure: Cisco ASA 5500 Deployed in Parallel to

Existing NAT/Firewall. This is the most cost-effective deployment, and the one we recommend for new and existing networks.

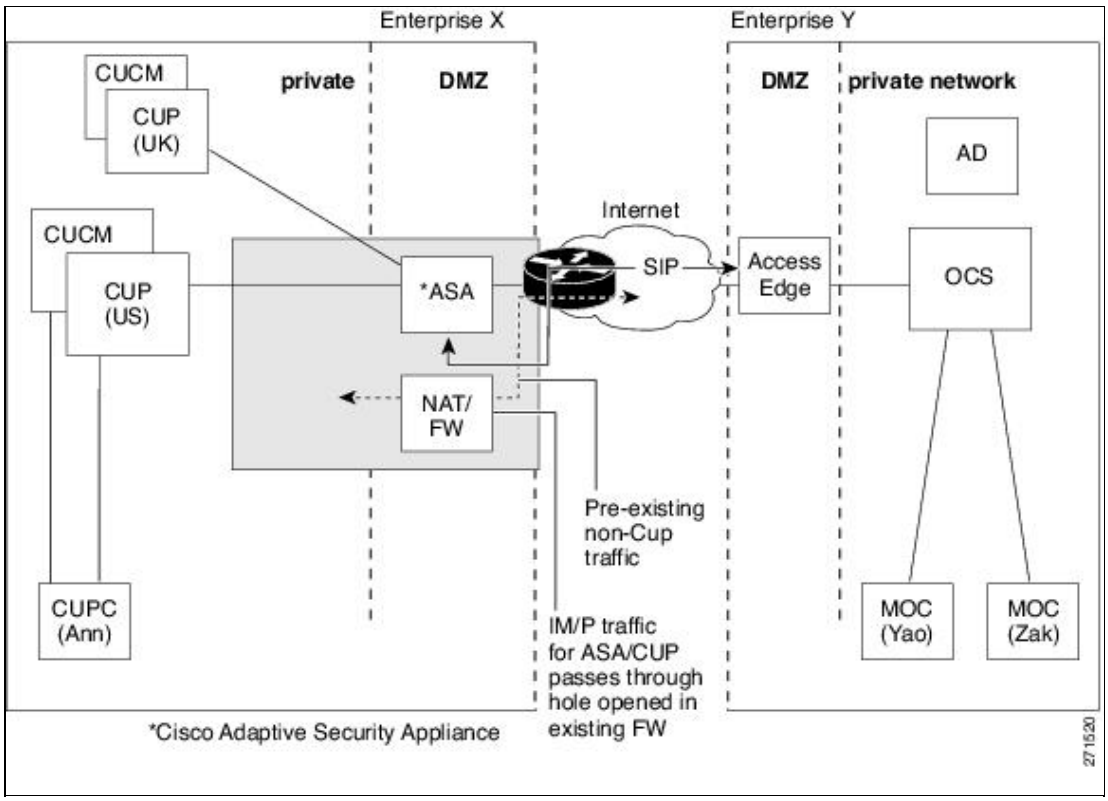
You can also deploy the Cisco Adaptive Security Appliance in parallel to the existing firewall, as illustrated in Figure: Cisco ASA 5500 Deployed in Parallel to Existing NAT/Firewall. In this deployment Cisco Adaptive Security Appliance handles the IM and Presence traffic between Cisco Unified Presence and the public internet, and the pre-existing traffic continues to use any existing firewall. In Figure: Cisco ASA 5500 Deployed in Parallel to Existing NAT/Firewall Cisco Adaptive Security Appliance is also deployed as a gateway for the Cisco Unified Presence server, which means that a separate router is not required to direct traffic to Cisco Adaptive Security Appliance.

Figure: 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, the existing firewall is configured to allow traffic destined for Cisco Unified Presence to reach the Cisco Adaptive Security Appliance, as illustrated in Figure: Cisco ASA 5500 Deployed Behind Existing NAT/Firewall. In this type of deployment the Cisco Adaptive Security Appliance is functioning as a gateway for the Cisco Unified Presence server.

Figure: Cisco ASA 5500 Deployed Behind Existing NAT/Firewall



Related Topics

- Getting More Information

About Federated Presence and Instant Messaging

- Presence Subscriptions and Blocking Levels
- Presence State Mappings
- Instant Messaging

Presence Subscriptions and Blocking Levels

All new presence subscriptions from "x@foreigndomain.com" to "user@local.com"are sent via the Cisco Adaptive Security Appliance, as illustrated in Figure: Inbound Presence Message Flow. Cisco Adaptive Security Appliance checks the inbound subscription against the list of permitted foreign domains. If the domain is not permitted, Cisco Adaptive Security Appliance denies the presence subscription.

On receipt of the inbound subscription, Cisco Unified Presence verifies that the foreign domain is one of the permitted (white-listed) domains defined at the administration level on the Cisco Unified Presence server. 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 presence subscription. Cisco Unified Presence then accepts the incoming subscription and places it in a pending state.

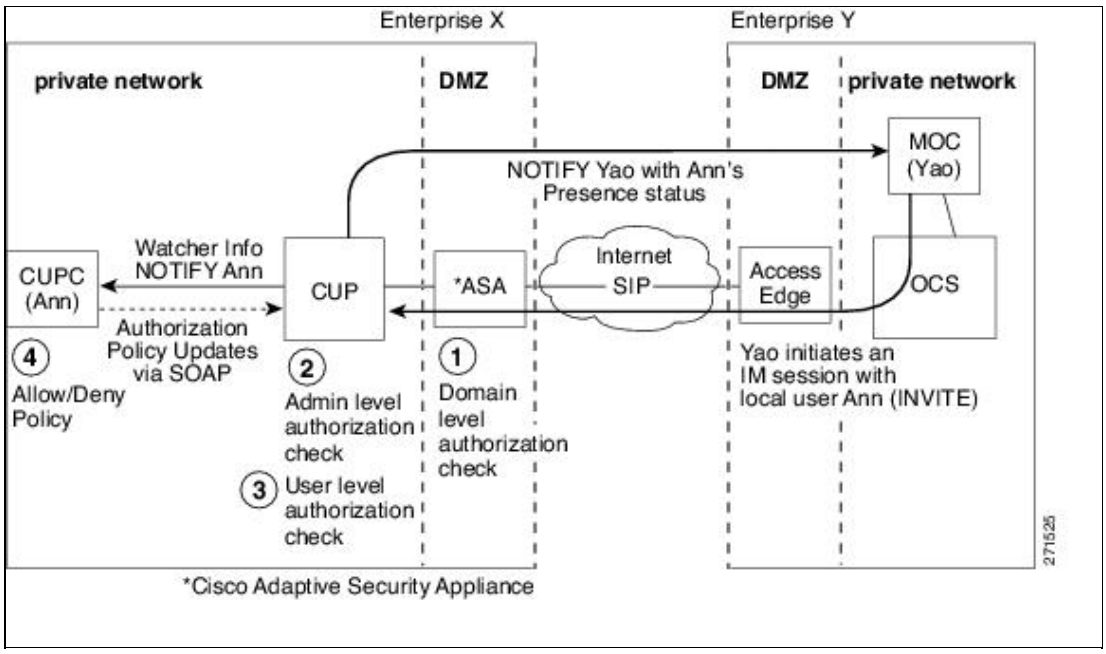
Cisco Unified Presence notifies the local user that "x@foreigndomain.com" wishes to watch their presence by sending the client application a NOTIFY message for the subscription (provided the client has subscribed for the Presence Watcher Info Package). This triggers a dialog box on the client application 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 via the SOAP interface. The authorization decision is added to the policy list of the user stored on Cisco Unified Presence.

A deny decision is handled using polite blocking, which means that the presence state of the user appears offline on the foreign client. If the local user allows the subscription, Cisco Unified Presence sends a presence NOTIFY message to `x@foreign.com'.

The user can also block subscriptions on a per user and a per domain basis. This can be configured via the Cisco Unified Presence end user GUI, and the Cisco Unified Personal Communicator client.

Note: The SOAP interface used to manage the contact and preference information for a user on Cisco Unified Presence is called the Client Configuration Web Service. For details on this web service, please refer to the *Developer Guide for Cisco Unified Presence Release 7.0*.

Figure: Inbound Presence Message Flow

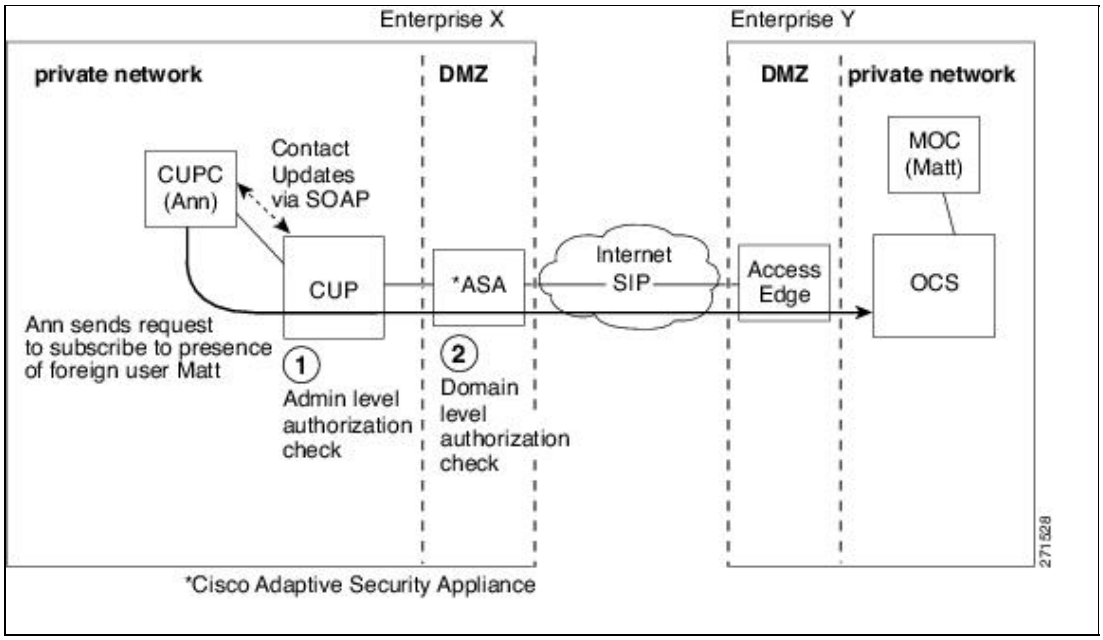


All outgoing subscriptions from Cisco Unified Presence are sent via Cisco Adaptive Security Appliance and

are forwarded to the foreign domain. An outgoing subscription is sent even if an active subscription already exists between a different local user to the same foreign user in the same foreign domain. Figure: Outbound Presence Message Flow illustrates an outgoing presence subscription flow.

The foreign user is added to the contacts on the client application (Cisco Unified Personal Communicator) and the Cisco Unified Presence end user GUI window as "user@foreigndomain.com". Cisco Unified Personal Communicator encodes auxiliary contact information about the foreign contact and stores it on the Cisco Unified Presence server via the SOAP interface.

Figure: Outbound Presence Message Flow



Notes:

- The OCS server 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 presence status of Cisco Unified Presence contacts is one hour and 45 minutes.
- If the OCS server restarts, the maximum duration a Cisco Unified Presence client will be without presence status of Microsoft Office Communicator contacts is two hours.
- If you are federating between one Cisco Unified Presence domain and another, if a Cisco Unified Presence restarts, the maximum duration a Cisco Unified Personal Communicator client in a foreign Cisco Unified Presence domain will be without the presence status of local Cisco Unified Presence contacts is two hours.

Related Topics

- Presence State Mappings
- Instant Messaging
- Getting More Information

Federated Presence State Mappings

The table below shows the presence mapping states from Microsoft Office Communicator to Cisco Unified Presence and Cisco Unified Personal Communicator.

Table: Presence Mapping States from Microsoft Office Communicator

Microsoft Office Communicator Setting	Cisco Unified Presence Reachability	Cisco Unified Personal Communicator Setting
Available	Available	Available
Busy	Busy	Away
Do Not Disturb	Busy - Microsoft OCS does not send DND to a federated domain.	Away
Be Right Back	Away	Away
Offline	Unavailable	Offline
Away	Away	Away

Similarly Table: Presence Mapping States from Cisco Unified Personal Communicator shows the presence mapping states from Cisco Unified Personal Communicator to Cisco Unified Presence and Microsoft Office Communicator.

Table: Presence Mapping States from Cisco Unified Personal Communicator

Microsoft Office Communicator Setting	Cisco Unified Presence Reachability	Cisco Unified Personal Communicator Setting
Available	Available	Available
Away	Away	Away
Do Not Disturb	Do Not Disturb	Busy
Offline	Unavailable	Offline

Related Topics

- Presence Subscriptions and Blocking Levels
- Instant Messaging
- Getting More Information

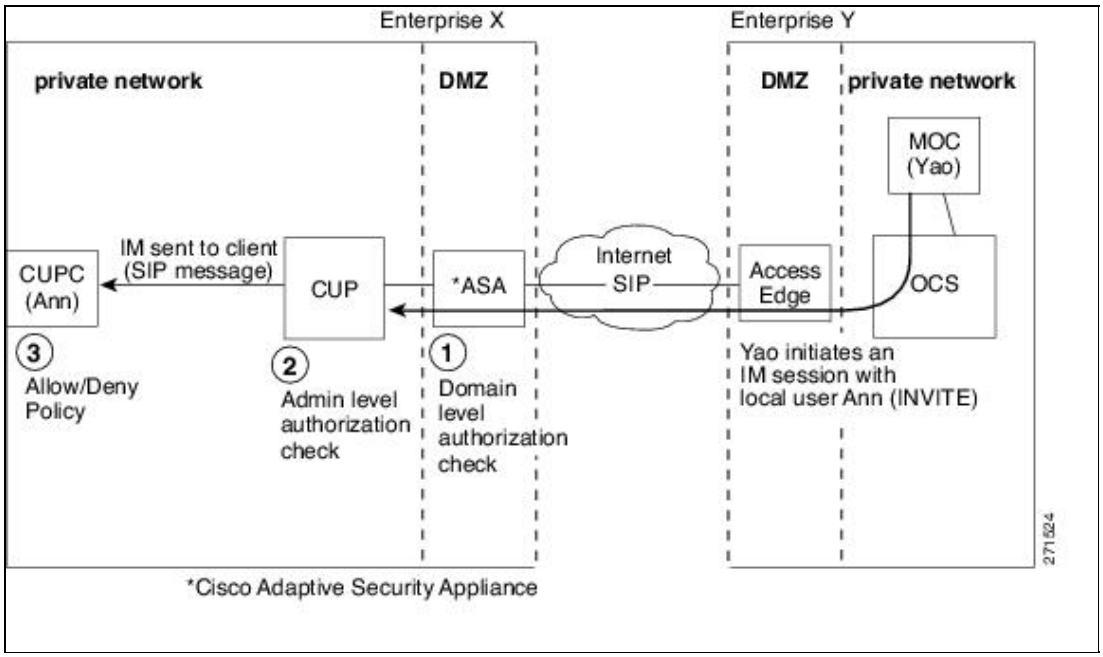
Instant Messaging

Instant Messages (IMs) that are sent between two enterprise deployments use Session Mode. IMs that are sent between Cisco Unified Presence and the client application (Cisco Unified Personal Communicator) use Pager 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: Inbound Instant Messaging Flow. The 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 sends the SIP MESSAGE to the client application for the local user.

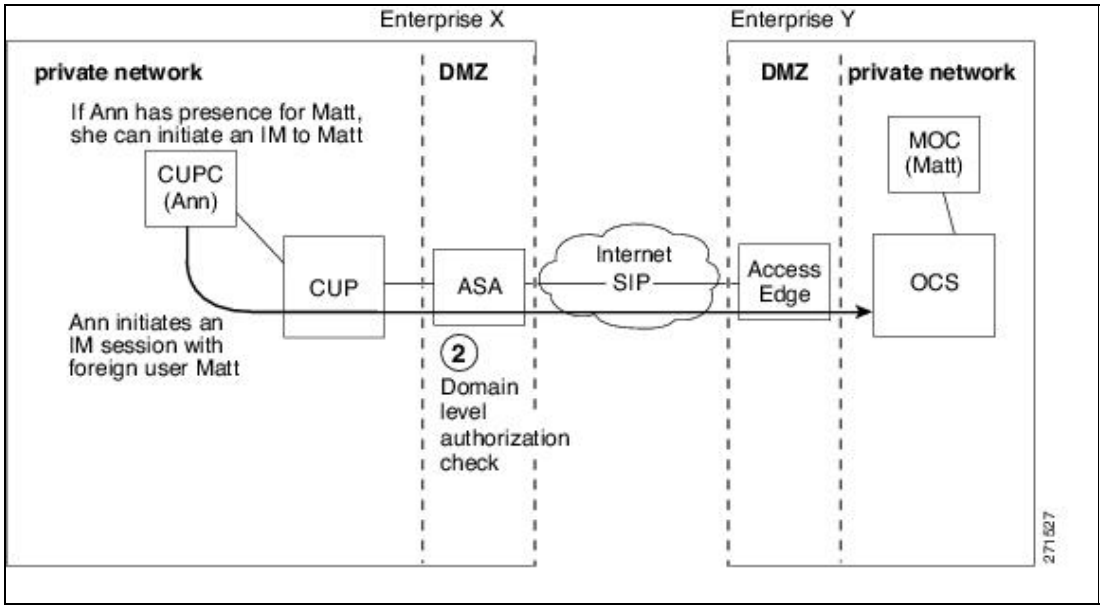
Figure: Inbound Instant Messaging Flow



When a local user in the Cisco Unified Presence domain sends an IM to a user in a foreign domain, it is sent to the IM controller running on the Cisco Unified Presence server. If no existing IM session is established between these two users, the IM controller sends an INVITE message to the foreign domain to establish a new session. Figure: Outbound Instant Message Flow illustrates this flow. This session is used for any subsequent MESSAGE traffic from either of these two users.

This session establishment also takes place when federating between two Cisco Unified Presence domains. Note that inbound IMs are first set up as session mode IMs using an INVITE message, but these IMs are converted into pager mode (a SIP session) on the Cisco Unified Presence server.

Figure: Outbound Instant Message Flow



Note: A three-way IM session (group chat) with a federated party is not supported.

Related Topics

- Presence Subscriptions and Blocking Levels
- Presence State Mappings
- Getting More Information

Federation and Subdomains

The following subdomain scenarios are supported:

- Cisco Unified Presence belongs to a subdomain of the OCS domain. For example, Cisco Unified Presence belongs to the subdomain "cup.cisco.com", and Cisco Unified Presence is federating with OCS which belongs to the domain "cisco.com". In this case, the Cisco Unified Personal Communicator user is assigned the SIP URI "*cupuser*@cup.cisco.com", and the OCS user has the SIP URI "*ocsuser*@cisco.com".

- Cisco Unified Presence belongs to a parent domain, and OCS belongs to a subdomain of that parent domain. For example, Cisco Unified Presence belongs to the domain"cisco.com", and Cisco Unified Presence is federating with OCS which belongs to the subdomain"ocs.cisco.com". In this case, the Cisco Unified Personal Communicator user is assigned the SIP URI "*cupuser*@cisco.com", and the OCS user is assigned the SIP URI "*ocsuser*@ocs.cisco.com".

- Cisco Unified Presence and OCS 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 OCS belongs to the subdomain "ocs.cisco.com". Both of these subdomains belong to the parent domain "cisco.com". In this case, the Cisco Unified Personal Communicator user is assigned the SIP URI "*cupuser*@cup.cisco.com" and the OCS user is assigned the SIP URI "*ocsuser*@ocs.cisco.com".

If you are federating with subdomains, you only need to configure separate DNS domains; there is no requirement to split your Active Directory. Cisco Unified Presence users or OCS users can belong to the same Active Directory domain. For example, in the third scenario described 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 "ocs.cisco.com", and may have the SIP URI "*cupuser*@cup.cisco.com " or "*ocsuser*@ocs.cisco.com".

Note: The above scenarios are also supported if you are federating between two Cisco Unified Presence enterprise deployments.

Related Topics

- Getting More Information