Planning for this Integration

June 18, 2013

Supported Interdomain Federation Integrations

This document describes the configuration steps for setting up a federated network between Cisco Unified Presence server and a foreign domain.

The supported foreign domains that a Cisco Unified Presence server can federate with are:

- Microsoft Office Communications Server Releases 2007, R2, Microsoft Lync 2010 over SIP

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 over SIP
- Cisco Webex Connect Release 6.x over XMPP
- IBM Sametime Server Release 8.2, 8.5 over XMPP
- GoogleTalk over XMPP
- Cisco Unified Presence Release 8.x over XMPP

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

Related Topics

- Hardware Requirements, page 2-2

- Software Requirements, page 2-2

Hardware Requirements

Cisco Hardware

- Cisco Unified Presence server. For Cisco Unified Presence hardware support, refer to the Cisco Unified Presence compatibility matrix
- Cisco Unified Communications Manager server. For Cisco Unified Communications Manager hardware support, refer to the Cisco Unified Communications Manager compatibility matrix
- Two DNS servers within the Cisco Unified Presence enterprise
- Cisco Adaptive Security Appliance 5500 Series
- (Optional) Cisco CSS11506 Content Services Switch

Note

- We only recommend the Cisco Adaptive Security Appliance for SIP federation as it provides the TLS proxy functionality. For XMPP federation, any firewall is sufficient.
- When selecting a **Cisco Adaptive Security Appliance** model, go to: http://www.cisco.com/en/US/products/ps6120/prod_models_home.html. The TLS proxy component is available on all 5500 models.
- Make sure you use the correct version of Cisco Adaptive Security Appliance software for your deployment. If you are configuring a new interdomain federation deployment, refer to the Cisco Unified Presence compatibility matrix for the correct version of Cisco Adaptive Security Appliance software.

Related Topics

- *Hardware and Software Compatibility Information for Cisco Unified Presence:* http://www.cisco.com/en/US/products/ps6837/products_device_support_tables_list.html
- *Cisco Unified Communications Manager Hardware Compatibility Matrix:* http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_device_support_tables_list.html
- Software Requirements, page 2-2

Software Requirements

Note You require Cisco Unified Presence Release 8.5 or later to configure SIP federation with AOL.

Cisco Software

- Cisco Unified Presence Server Release 8.6(x)
- Cisco Unified Communications Manager Server Release 6.x+
- Cisco Adaptive Security Appliance v8.3(1)

- Cisco Adaptive Security Device Manager (ASDM) v6.3
- Supported SIP client:
  - Cisco Unified Personal Communicator Release 7.x (7.03.13742 or later)
- Supported XMPP clients:
  - Cisco Unified Personal Communicator Release 8.5
  - Cisco Jabber for Mac
  - Cisco Jabber for Windows
  - Cisco Jabber IM for Mobile (iPhone, Android, Blackberry)
  - Cisco Jabber for iPad
  - Cisco Jabber for Cius

Microsoft Software for SIP Federation

- Microsoft Lync 2010
- Microsoft OCS 2007 Release 2 Server Standard or Enterprise
- Microsoft Office Communicator 2007 Release 2
- Microsoft Active Directory

AOL Software for SIP Federation

- AOL SIP Access Gateway (SAG)
- AOL Instant Messenger Release 7.2.6.1 or later

Software for XMPP Federation

- Cisco Webex Connect Release 6.x
- IBM Sametime Server Release 8.2
- GoogleTalk

Related Topic

Hardware Requirements, page 2-2

About Integration Preparation

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

Routing Configuration

Consider how you are going to set up routing in your federated network. Consider how you route messages that are destined for a foreign domain address from Cisco Unified Presence through the Cisco Adaptive Security Appliance to the foreign domain. You could consider deploying a routing entity (router, switch or gateway) between the Cisco Unified Presence enterprise deployment and Cisco Adaptive Security Appliance. The routing entity routes messages to the Cisco Adaptive Security Appliance, and Cisco Adaptive Security Appliance routes these messages to the foreign domain.

You can also deploy Cisco Adaptive Security Appliance as a gateway between Cisco Unified Presence and the foreign domain. If you use Cisco Adaptive Security Appliance as a gateway for Cisco Unified Presence, within your local enterprise deployment you must consider how Cisco Unified Communications Manager, and the Cisco Unified Presence client will access the Cisco Unified Presence server. If Cisco Unified Communications Manager and the Cisco Unified Presence clients are in a different subnet from Cisco Unified Presence, they will need to access the Cisco Unified Presence using Cisco Adaptive Security Appliance.

If you deploy Cisco Adaptive Security Appliance behind an existing firewall in your network, consider how you route traffic to Cisco Adaptive Security Appliance and to Cisco Unified Presence. On the existing firewall, configure routes and access lists to route traffic to the public Cisco Unified Presence address. You must also configure routes to the foreign domain using the existing firewall.

Related Topics

- Cisco Adaptive Security Appliance Deployment Options, page 1-10
- Configuring Cisco Adaptive Security Appliance for SIP Federation, page 6-1

Public IP Address

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

For SIP federation with Microsoft OCS R2, you require a single public IP address, even if you deploy multiple Cisco Unified Presence servers. Cisco Adaptive Security Appliance routes the requests from OCS to the correct Cisco Unified Presence server using Port Address Translation (PAT).

For XMPP federation, you can choose to either expose a public IP address for each Cisco Unified Presence server on which you enable XMPP federation, or expose a single public IP address:

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

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

Related Topics

- External and Internal Interface Configuration, page 6-1
- DNS Configuration, page 2-6

Public FQDN

For SIP federation, request messages are routed based on the FQDN. Therefore, the FQDN of the routing Cisco Unified Presence server (publisher) must be publicly resolvable.

AOL SIP Access Gateway

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

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

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

Server Name: sip.oscar.aol.com

Server Port: 5061

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

Note

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

Redundancy/High Availability

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

If you wish to make your Cisco Unified Presence federation capability highly available you can deploy a load balancer in front of your designated (federation) Cisco Unified Presence cluster. Cisco recommends you use the Cisco CSS 11500 Content Services Switch.

The Cisco CSS 11500 Content Services Switch documentation is available at the following URL: http://www.cisco.com/en/US/products/hw/contnetw/ps792/products_installation_and_configuration_guides_list.html

DNS Configuration

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

For SIP federation with Microsoft OCS R2, you must publish the DNS SRV record **_sipfederationtls**. The Microsoft enterprise deployment requires this record because you configure Cisco Unified Presence as a Public IM Provider on the Access Edge server. In the external enterprise deployment, in order for Cisco Unified Presence to discover the Microsoft domain, a DNS SRV record must exist that points to this external domain. If the Cisco Unified Presence server cannot discover the Microsoft domain using DNS SRV, you must configure a static route on Cisco Unified Presence that points to the *public interface* of this external domain.

For AOL federation, AOL publishes the DNS SRV record **_sipfederationtls_tcp.aol.com** in their public DNS server for the domain ‘aol.com’. This resolves to sip.oscar.aol.com which is the AOL SIP Access Gateway.

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

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

Related Topics

- Routing SIP Requests for SIP Federation with AOL, page 4-7
- Verifying or Changing the Default Federation Routing Domain for SIP Federation with AOL, page 4-8

Certificate Authority (CA) Server

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

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

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

About Prerequisite Configuration Tasks for this Integration

Prerequisite Configuration for Cisco Unified Presence

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

1. Install and configure Cisco Unified Presence as described in the *Deployment Guide for Cisco Unified Presence.*

   At this point, perform the following checks to ensure that your Cisco Unified Presence is operating properly:

- Run the Cisco Unified Presence Troubleshooter.
- Check that you can add local contacts to Cisco Unified Presence.
- Check that your clients are receiving availability states from the Cisco Unified Presence server.

2. Configure Cisco Unified Presence server with a Cisco Unified Communications Manager (CUCM) server as described in the *Deployment Guide for Cisco Unified Presence*. Ensure that the Cisco Unified Presence server is working without any issues.

Related Topics

- *Deployment Guide for Cisco Unified Presence: http://www.cisco.com/en/US/products/ps6837/tsd_products_support_series_home.html*
- Prerequisite Configuration for Cisco Adaptive Security Appliance, page 2-8

Prerequisite Configuration for Cisco Adaptive Security Appliance

Note

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

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

1. Access Cisco Adaptive Security Appliance either via console though a hyperterminal, or via the web-based Adaptive Security Device Manager (ASDM).
2. Obtain the appropriate licenses for Cisco Adaptive Security Appliance. Note that you will require a license for the TLS proxy on Cisco Adaptive Security Appliance. Contact your Cisco representative for license information.
3. Upgrade the software (if necessary).
4. Configure the hostname using the command:

   ```
   (config)# hostname name
   ```
5. Set the timezone, date and time in ASDM by selecting **Device Setup > System Time > Clock**, or via the CLI using the **clock set** command. Note the following:

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

6. Check the Cisco ASA 5500 modes. The Cisco ASA 5500 is configured to use single mode and routed mode by default.

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

  ```
  (config)# show mode
  ```
- Check the current firewall mode. This is routed mode by default.

  ```
  (config)# show firewall
  ```
- Set up the external and internal interfaces.
- Set up the basic IP routes.

Related Topics:

- Cisco Adaptive Security Appliance documentation: http://www.cisco.com/en/US/products/ps6120/tsd_products_support_series_home.html
- Cisco Adaptive Security Appliance Command Line Reference Guides: http://www.cisco.com/en/US/products/ps6120/tsd_products_support_reference_guides.html
- Cisco Adaptive Security Appliance Configuration Guide: http://www.cisco.com/en/US/products/ps6120/tsd_products_support_configure.html

- *ASDM 6.0 User Guide*: http://www.cisco.com/en/US/products/ps6120/tsd_products_support_maintain_and_operate.html
- External and Internal Interface Configuration, page 6-1
- Configuring the Static IP Routes, page 6-2
- Prerequisite Configuration for Cisco Unified Presence, page 2-7