Main page: Cisco Unified Presence, Release 7.x

Contents

Previous Topic

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

- Supported Interdomain Federation Integrations
- Hardware Requirements
- Software Requirements
- Preparation for this Integration
- Prerequisite Configuration Tasks for this Integration

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:

- a Microsoft Office Communications Server (OCS), or
- a Microsoft Live Communications Server (LCS), or
- a Cisco Unified Presence enterprise deployment in a foreign domain

The complete procedure for setting up a federated network between a Cisco Unified Presence enterprise deployment, and a Microsoft OCS enterprise deployment is provided. Use this document as a guide for setting up a federation between Cisco Unified Presence and one of the supported foreign domains listed above.

Note: If you are federating between one Cisco Unified Presence enterprise and another, you follow the same procedures outlined in this document (ignoring the Microsoft-specific sections). Note that when you are configuring a Federated Domain entry on the Cisco Unified Presence server for this integration, you need to select the integration type "**CUP to CUP**".

Related Topics

- Getting More Information

Hardware Requirements

Cisco Hardware

- MCS 7825/35/45 Server running Cisco Unified Presence
- MCS 7825/35/45 Server running Cisco Unified Communications Manager
- Two DNS servers within the Cisco Unified Presence enterprise
- Cisco Adaptive Security Appliance 5500 Series
- (Optional) Cisco CSS11506 Content Services Switch

  Note: When selecting a **Cisco Adaptive Security Appliance** model: http://www.cisco.com/en/US/products/ps6120/prod_models_home.html. The TLS Proxy component is available on all 5500 models.

- The **Cisco CSS 11500 Content Services Switch** must have a SSL Accelerator Module installed.

Microsoft Hardware

Refer to the *Microsoft Office Communications Server 2007 Planning Guide* for server platform requirements.

- A server running either LCS 2005 or OCS 2007

- Access Edge server
- Windows Active Directory® Node
- DNS server within the Microsoft OCS enterprise deployment

Related Topics

- Getting More Information

Software Requirements

Cisco Software

- Cisco Unified Presence Server Version 7.0
- Cisco Unified Communications Manager Server Version 6.X+
- Cisco Unified Personal Communicator v7.0
- Cisco Adaptive Security Appliance Version v8.0.4(x) (for Cisco Unified Presence 7.0(3) or earlier)
- Cisco Adaptive Security Appliance Version v8.2(x) (for Cisco Unified Presence 7.0(4) or later)
- Cisco Adaptive Security Device Manager (ASDM) v6.1(3)

Microsoft Software

- Microsoft OCS 2007 Server Standard or Enterprise, Microsoft OCS 2007 Release 2, or Microsoft LCS 2005 Server Standard or Enterprise
- Microsoft Office Communicator 2005 (LCS) or 2007(OCS)
- Microsoft Active Directory

Related Topics

- Getting More Information

Preparation for this Integration

It is essential that you plan carefully for this integration. Consider the items described in this section before commencing any configuration for this integration.

- Routing Configuration
- Redundancy/High Availability
- DNS Configuration
- Certificate Authority (CA) Server

Routing Configuration

You need to consider how you are going to set up routing in your federated network. Consider how messages destined for a foreign domain address are routed 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.

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

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

Related Topics

- Cisco Adaptive Security Appliance Deployment Options
- Configuring Cisco Adaptive Security Appliance for this Integration
- Getting More Information

Public IP Address

For this integration you will require a publicly accessible IP address for the public Cisco Unified Presence address. If you do not have an IP address to assign, you can use the outside interface of the Cisco Adaptive Security Appliance as the public Cisco Unified Presence address provided you are only using the Cisco Adaptive Security Appliance for Presence and IM traffic.

Related Topics

- External and Internal Interface Configuration
- Getting More Information

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 here:

http://www.cisco.com/en/US/products/hw/contnetw/ps792/products_installation_and_configuration_guides_list.ht

Related Topics

- Failover on Cisco Adaptive Security Appliance
- Configuring the Load Balancer for Redundancy
- Getting More Information

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. The Microsoft enterprise deployment requires this because Cisco Unified Presence is configured 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.

Related Topics

- Getting More Information

Certificate Authority (CA) Server

The Cisco Adaptive Security Appliance in the Cisco Unified Presence enterprise deployment, and the Access Edge Server in the Microsoft enterprise deployment, will share IM and Presence over a secure SSL/TLS connection. Each enterprise deployment must present a certificate that is signed by an external CA, and each enterprise deployment may be 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.

Related Topics

- Getting More Information

Prerequisite Configuration Tasks for this Integration

Before you begin, ensure that you have performed the prerequisite configuration tasks specific to the integration you are deploying as described in the table below.

Table: Prerequisite configuration tasks

Prerequisite	CUP to CUP	CUP to OCS/LCS	Documentation Reference
A Cisco Unified Presence server that is installed and configured 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 Cisco Unified Personal Communicator is receiving presence states from the Cisco Unified Presence server.	Yes	Yes	http://www.cisco.com/en/US/products/ps6837/tsd_products_support_series_home.

The Cisco Unified Presence server must be correctly deployed 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.	Yes	Yes	
A Cisco Adaptive Security Appliance that is installed and configured correctly. Ensure that you have the performed the following basic configuration checks on the Cisco Adaptive Security Appliance: 1. Gained access to the Cisco Adaptive Security Appliance either via console though a hyperterminal, or via the web-based Adaptive Security Device Manager (ASDM). 2. Obtained 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	Yes	Yes	The complete set of Cisco Adaptive Security Appliance documentation is available http://www.cisco.com/en/US/products/ps6120/tsd_products_support_series_home. The *Cisco Adaptive Security Appliance Command Line Reference Guides* are avail http://www.cisco.com/en/US/products/ps6120/tsd_products_support_reference_gu The *Cisco Adaptive Security Appliance Configuration Guide* is available at this UR http://www.cisco.com/en/US/products/ps6120/tsd_products_support_configure.htm The *ASDM 6.0 User Guide* is available here: http://www.cisco.com/en/US/products/ps6120/tsd_products_support_maintain_and

information. 3. Upgraded the software (if necessary). 4. Configured 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. Checked 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.			
A Microsoft OCS or LCS server that is installed, configured properly and running without any issues. The Microsoft OCS or LCS server must be configured for Federation.	No	Yes	For details on installing, configuring and deploying Microsoft OCS, refer to the fol http://office.microsoft.com/en-us/communicationsserver/FX101729111033.aspx
A Microsoft Access Edge server (OCS) or Access Proxy server (LCS) that is installed, configured properly and running without any issues.	No	Yes	For details on installing, configuring and deploying Microsoft LCS, refer to the fol http://office.microsoft.com/en-us/communicationsserver/FX011526591033.aspx

Related Topics

- Failover on Cisco Adaptive Security Appliance
- External and Internal Interface Configuration
- Configuring Static Routes