XMPP Federation Between CUPS and Other Servers

Contents

Introduction

This document describes the steps used in order to configure Extensible Messaging and Presence Protocol (XMPP) federation between the Cisco Unified Presence Server (CUPS) and other servers.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on Cisco Unified Presence (CUP) Release 8.x.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Background Information

CUPS supports federation for only these servers:

- IBM Sametime Server Releases 8.2 and 8.5
- Cisco WebEx Connect Release 6
- GoogleTalk
- CUP Release 8.x
- Servers that are XMPP Standards Compliant

The XMPP message flow between two clients registered with two XMPP servers is:

XMPP Client (Google Talk or WebEx Connect) > **TCP: 5222** > **XMPP Server** (Google Server or WebEx Connect Server) > **TCP: 5269** > **ASA** (firewall) > **TCP: 5269** > **CUPS** > **TCP: 5222** > **CUPS XMPP Client** (Jabber or CUPS)

> **Note**: Not all Jabber clients support federated contact.

The assumptions for this document are:

- The CUPS domain is **cupdomain.com**.
- The CUPS User IM Address is **cupuser1@cupdomain.com**.
- The XMPP Server domain is **gmail.com**.
- The XMPP User IM Address is **jdoe1@gmail.com**.

This is what happens when federation occurs:

1. When **jdoe1@gmail.com** is added to the **cupuser1** Contact List, CUPS becomes aware.
2. CUPS sends a **_xmpp-server._tcp.gmail.com** Domain Name System (DNS) query to the DNS server specified in CUPS. This is found with the **show network eth0 details** command, and is typically a local DNS server.
3. The local DNS server forwards the DNS query to the public DNS server, which has an entry for **_xmpp-server._tcp.gmail.com** because the contact IM has the **gmail.com** domain, and returns values for the Fully Qualified Domain Name (FQDN)/IP address of the Google server to the local DNS server. The values are then sent to CUPS.
4. Now CUP knows where to send the presence subscription request, and requests present status to the XMPP server IP address retrieved in the previous step (for user **jdoe1@gmail.com** on **TCP Port 5369**).
5. The request must pass through the Cisco Adaptive Security Appliance (ASA) firewall to the public XMPP server (Google) on **TCP Port 5269**.

> **Note**: This process is reversed when **jdoe1@gmail.com** adds **cupuser1@cupdomain.com** to his/her contact list.

Configure

This section describes a simple overview of federation configuration:

1. Configure a **DNS SRV** record on the public DNS server (the company that hosts the CUPS company website or the internet service provider). If the **DNS SRV** is created for the FQDN of CUPS, then a **DNS** "**A**" record must be created in order to resolve the **DNS A** record to the

CUPS public IP address.

This is an example of the **DNS SRV** record and **DNS A** record for CUPS:

DNS SRV record: **_xmpp-server._tcp.cupdomain.com** points to **cup1.cupdomain.com** (this assumes that **cup1** is the CUPS hostname). The priority weight can be **0**.DNS A record: **cup1.cupdomain.com** points to the public IP of the ASA for CUPS.

2. Configure the firewall to have a Network Address Translation (NAT) that translates the CUPS IP to a public IP, or configure a Port Address Translation (PAT) on the ASA that translates the CUPS IP and **TCP Port 5269** to a public IP with **TCP Port 5269**.
3. Ensure that the CUPS domain is not a registered domain with the XMPP server. For example, **cupdomain.com** should not be registered with Google Apps or with WebEx service.
4. Enable XMPP federation on CUPS. For Google it is TCP, and for WebEx it is Transport Layer Security (TLS) Optional with **no client side certificate** checked.
5. Start the XMPP federation service on CUPS.

Verify

Complete these steps in order to verify that incoming traffic passes through the ASA for **TCP Port 5269**.

1. Obtain a PC that is not connected to the local network as Cisco Unified Presence Server, but connected to an outside network and coming into the ASA.
2. Open up a command prompt and type:
   ```
   telnet <CiscoUnifiedPresenceServer_outside_NAT'ed_IP> 5269
   ```
   If this action produces a blank screen, then the configuration on the ASA is correct.
3. Check that the CUPS internal IP address is telnet-able. From an internal PC, open a command promt and enter:
   ```
   telnet <CiscoUnifiedPresenceServer_Internal_IP> 5269
   ```
   If this fails, it means that CUPS XMPP federation is not configured or that XMPP federation service is not enabled.

> **Note**: If any of the previous steps fail, you must troubleshoot the firewall log.

Additionally, you must discover if the CUPS domain is registered with WebEx or Gmail. If there is a registered domain with Gmail or WebEx, the CUPS XMPP federation log must be analyzed. It informs you of an unexpected dial-back resonse. In this case, the Google or WebEx support team must be contacted in order to remove the CUPS domain from their subscription service.

> **Note**: Windows 7 does not come with the telnet application by default; it must be installed via **Control Panel > Programs and Features > Turn Windows feature on or off > Telnet Client**.

Troubleshoot

Complete these steps in order to troubleshoot the configuration:

1. In order to check that the XMPP records are properly created on the public DNS server, open a command prompt and enter:
   ```
   nslookup
   set type=SRV
   _xmpp-server._tcp.cupdomain.com
   ```
   Note: This step gives results for the CUPS public IP address that is configured on the ASA for CUPS. If you encounter trouble with this step, talk to the website provider or internet service provider who created the **DNS SRV** record.
2. In order to check that the ASA operates properly and does not block traffic, open a command prompt from a PC that belongs to the same network as CUPS and complete these steps:

   Check the outgoing traffic through the ASA for **TCP Port 5269**. In order to do this, you must verify the XMPP server IP address with these commands:
   ```
   nslookup
   set type=SRV
   _xmpp-server._tcp.gmail.com
   ```
   Note: The output from these commands gives multiple IP addresses that serve the gmail.com domain for XMPP federation.Open a new command prompt and enter:
   ```
   telnet <gmail_server_ip> 5269
   ```
   If this produces a blank screen, then the ASA passes outgoing traffic.

Related Information

- **Configuring Cisco Unified Presence for XMPP Federation**
- **Technical Support & Documentation - Cisco Systems**