Federazione XMPP tra CUPS e altri server

Sommario

Introduzione

In questo documento viene descritto come configurare la federazione XMPP (Extensible Messaging and Presence Protocol) tra Cisco Unified Presence Server (CUPS) e altri server.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il riferimento delle informazioni contenute in questo documento è Cisco Unified Presence (CUP) release 8.x.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

CUPS supporta la federazione solo per questi server:

- IBM Sametime Server release 8.2 e 8.5
- Cisco WebEx Connect release 6
- GoogleTalk
- CUP release 8.x
- Server conformi agli standard XMPP

Il flusso di messaggi XMPP tra due client registrati con due server XMPP è:

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

Nota: Non tutti i client Jabber supportano il contatto federato.

I presupposti per l'utilizzo di questo documento sono:

- Il dominio CUPS è **cupdomain.com**.
- L'indirizzo IM dell'utente CUPS è **cupuser1@cupdomain.com**.
- Il dominio del server XMPP è **gmail.com**.
- L'indirizzo IM dell'utente XMPP è **jdoe1@gmail.com**.

Questo è ciò che accade quando si verifica la federazione:

1. Quando **jdoe1@gmail.com** viene aggiunto all'elenco contatti **cupuser1**, CUPS viene informato.
2. CUPS invia una query DNS **_xmpp-server._tcp.gmail.com** al server DNS specificato in CUPS. Questa condizione viene rilevata con il comando **show network eth0 details** e in genere è un server DNS locale.
3. Il server DNS locale inoltra la query DNS al server DNS pubblico, che dispone di una voce per **_xmpp-server._tcp.gmail.com** perché il contatto IM ha il dominio **gmail.com** e restituisce i valori per il nome di dominio completo (FQDN)/indirizzo IP del server Google al server DNS locale. I valori vengono quindi inviati a CUPS.
4. Ora CUP sa dove inviare la richiesta di abbonamento alla presenza e richiede lo stato attuale all'indirizzo IP del server XMPP recuperato nel passaggio precedente (per l'utente **jdoe1@gmail.com** sulla **porta TCP 5369**).
5. La richiesta deve passare attraverso il firewall di Cisco Adaptive Security Appliance (ASA) al server XMPP pubblico (Google) sulla **porta TCP 5269**.

   Nota: Questo processo viene annullato quando **jdoe1@gmail.com** aggiunge **cupuser1@cupdomain.com** al suo elenco di contatti.

Configurazione

In questa sezione viene descritta una semplice panoramica della configurazione della federazione:

1. Configurare un record **DNS SRV** nel server DNS pubblico, ovvero la società che ospita il sito Web della società CUPS o il provider di servizi Internet. Se il **DNS SRV** viene creato per il nome di dominio completo (FQDN) di CUPS, è necessario creare un record **"A" DNS per**

risolvere il record DNS A nell'indirizzo IP pubblico CUPS.

Questo è un esempio dei record DNS SRV e DNS A per CUPS:

Record DNS SRV: _xmpp-server._tcp.cupdomain.com punta a cup1.cupdomain.com (ciò presuppone che cup1 sia il nome host CUPS). Il fattore di priorità può essere 0.Record A DNS: cup1.cupdomain.com punta all'IP pubblico dell'ASA per CUPS.

2. Configurare il firewall in modo che abbia un NAT (Network Address Translation) che traduca l'indirizzo IP CUPS in un indirizzo IP pubblico, oppure configurare un PAT (Port Address Translation) sull'appliance ASA che traduca l'indirizzo IP e la porta TCP 5269 in un indirizzo IP pubblico con la porta TCP 5269.
3. Verificare che il dominio CUPS non sia un dominio registrato con il server XMPP. Ad esempio, cupdomain.com non deve essere registrato con Google Apps o con il servizio WebEx.
4. Abilita federazione XMPP su CUPS. Per Google è TCP e per WebEx è TLS (Transport Layer Security) Facoltativo, senza alcun certificato lato client controllato.
5. Avviare il servizio federativo XMPP su CUPS.

Verifica

Completare questa procedura per verificare che il traffico in entrata passi attraverso l'ASA per la porta TCP 5269.

1. Ottenere un PC non connesso alla rete locale come Cisco Unified Presence Server, ma connesso a una rete esterna e in entrata nell'appliance ASA.
2. Aprire un prompt dei comandi e digitare:
   telnet

   Se l'azione genera uno schermo vuoto, la configurazione dell'ASA è corretta.
3. Verificare che l'indirizzo IP interno CUPS sia telnet. Da un PC interno, aprire una richiesta di comando ed immettere:
   telnet

   Se l'operazione non riesce, significa che la federazione XMPP CUPS non è configurata o che il servizio federativo XMPP non è abilitato.

Nota: Se una delle operazioni precedenti ha esito negativo, è necessario risolvere il problema del registro del firewall.

Inoltre, è necessario verificare se il dominio CUPS è registrato con WebEx o Gmail. Se esiste un dominio registrato con Gmail o WebEx, è necessario analizzare il registro di federazione CUPS XMPP. Fornisce informazioni su una risposta remota imprevista. In questo caso, è necessario

contattare il team di supporto di Google o WebEx per rimuovere il dominio CUPS dal servizio di abbonamento.

> **Nota:** Windows 7 non viene fornito con l'applicazione telnet per impostazione predefinita. deve essere installato tramite **Pannello di controllo > Programmi e funzionalità > Attivazione o disattivazione della funzionalità Windows > Client Telnet**.

Risoluzione dei problemi

Per risolvere i problemi relativi alla configurazione, completare la procedura seguente:

1. Per verificare che i record XMPP siano stati creati correttamente nel server DNS pubblico, aprire un prompt dei comandi e immettere:
   ```
   nslookup
   set type=SRV
   _xmpp-server._tcp.cupdomain.com
   ```
   Nota: Questo passo fornisce i risultati per l'indirizzo IP pubblico CUPS configurato sull'appliance ASA per CUPS. In caso di problemi con questo passaggio, rivolgersi al provider del sito Web o del servizio Internet che ha creato il record **DNS SRV**.
2. Per verificare che l'ASA funzioni correttamente e non blocchi il traffico, aprire un prompt dei comandi da un PC che appartiene alla stessa rete di CUPS e completare i seguenti passaggi:

   Controllare il traffico in uscita attraverso l'ASA per verificare la **porta TCP 5269**. A tale scopo, è necessario verificare l'indirizzo IP del server XMPP con questi comandi:
   ```
   nslookup
   set type=SRV
   _xmpp-server._tcp.gmail.com
   ```
   Nota: L'output di questi comandi fornisce più indirizzi IP che servono il dominio gmail.com per la federazione XMPP.Aprire un nuovo prompt dei comandi e immettere:
   ```
   telnet
   ```

   Se viene visualizzata una schermata vuota, l'ASA trasmette il traffico in uscita.

Informazioni correlate

- Configurazione di Cisco Unified Presence per XMPP Federation
- Documentazione e supporto tecnico – Cisco Systems