Configurare le chiamate audio e video da azienda a azienda tramite Expressway integrato con CUCM

Sommario

Introduzione

Questo documento descrive come integrare/configurare l'implementazione Business to Business (B2B) per chiamate audio e video tramite Expressway integrato con Cisco Unified Call Manager (CUCM).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Expressway-C (Exp-C)
- Expressway-E (Exp-E)
- Cisco Unified Call Manager (CUCM)
- Cisco Unity Connection (CUC)
- Telepresence Video Communication Server-C (VCS-C)
- Jabber phone
- Cisco Telepresence System (CTS)
- EX, telefono
- SIP (Session Initiation Protocol)
- HTTP (Hypertext Transfer Protocol)
- Protocollo XMPP (Extensible Messaging and Presence Protocol)
- Cisco Unified IM and Presence (IM&P)
- Certificati

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Expressway C e E X8.1.1 o versioni successive
- Unified Communications Manager (CUCM) versione 10.0 o successiva.

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

Questi passaggi spiegano in dettaglio come integrare/configurare l'implementazione B2B per le chiamate audio e video attraverso Expressway integrato con CUCM per poter effettuare e ricevere chiamate da altre aziende (domini).

Expressway con la funzione di accesso remoto mobile (MRA, Mobile Remote Access) consente di registrare senza problemi gli endpoint Jabber e TC situati all'esterno della rete aziendale, come illustrato nel diagramma di rete.

La stessa architettura fornisce anche integrazione/chiamate senza interruzioni tra aziende diverse, o integrazione Business-to-Business, e questo per audio, video e IM&P. (B2B)

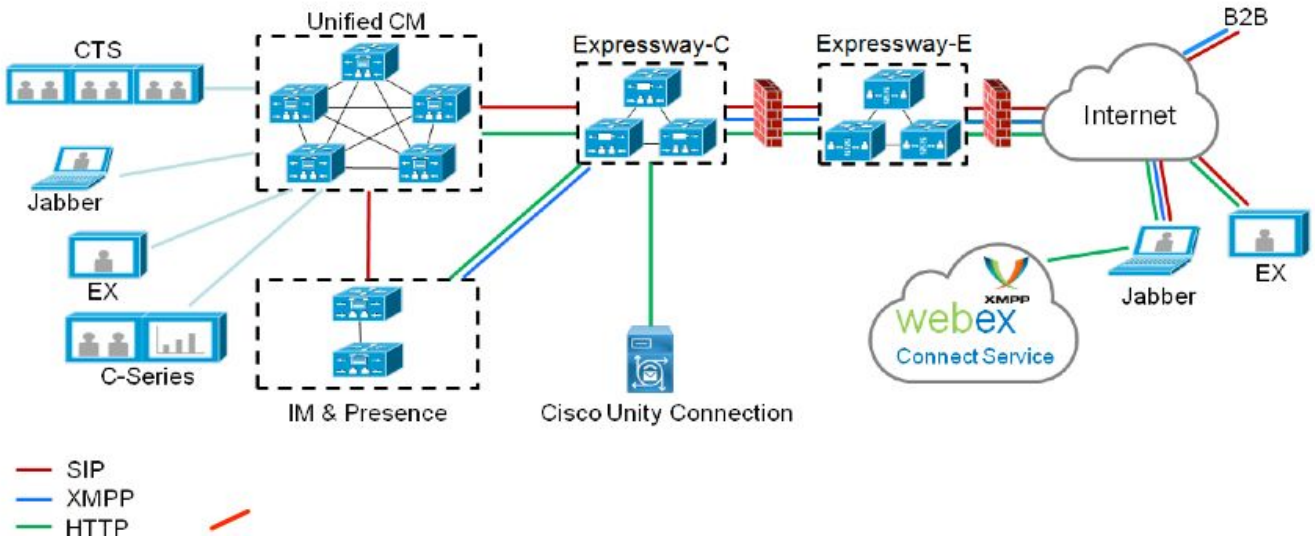
Questo documento non copre la parte IM&P e non copre l'integrazione H.323.

Prima di continuare, è necessario verificare di disporre del servizio DNS (SRV) appropriato creato per il proprio dominio. Questi record vengono utilizzati da altre società per trovare la posizione di Expressway.

Configurazione

Esempio di rete

L'immagine mostra un esempio di diagramma di rete.



Passaggio 1. Trunk SIP tra CUCM e Expressway-C

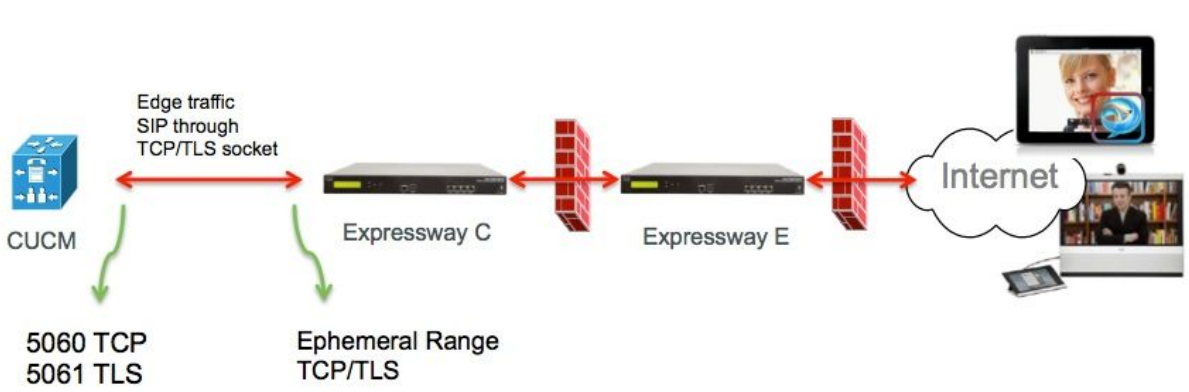
Dopo che il rilevamento CUCM viene eseguito da Expressway-C, le zone adiacenti vengono configurate automaticamente per ogni nodo e viene individuato il protocollo di trasporto.

Quando il cluster CUCM è configurato in modalità mista, esiste una zona per il protocollo TCP (Transmission Control Protocol) per il traffico non protetto con la porta di destinazione 5060 e una zona per TLS (Transport Layer Security) per il traffico protetto con la porta di destinazione 5061. Impossibile modificare le porte.

Le due zone vengono utilizzate per tutte le chiamate di spigolo da e verso i punti finali del bordo.

Le chiamate in entrata dagli endpoint del perimetro prendono il percorso di queste zone ad aggiunta automatica e quindi hanno come destinazione TCP 5060 o TLS 5061 su CUCM.

Tramite le chiamate di registrazione e invio/ricezione degli endpoint di edge sockets stabilite.

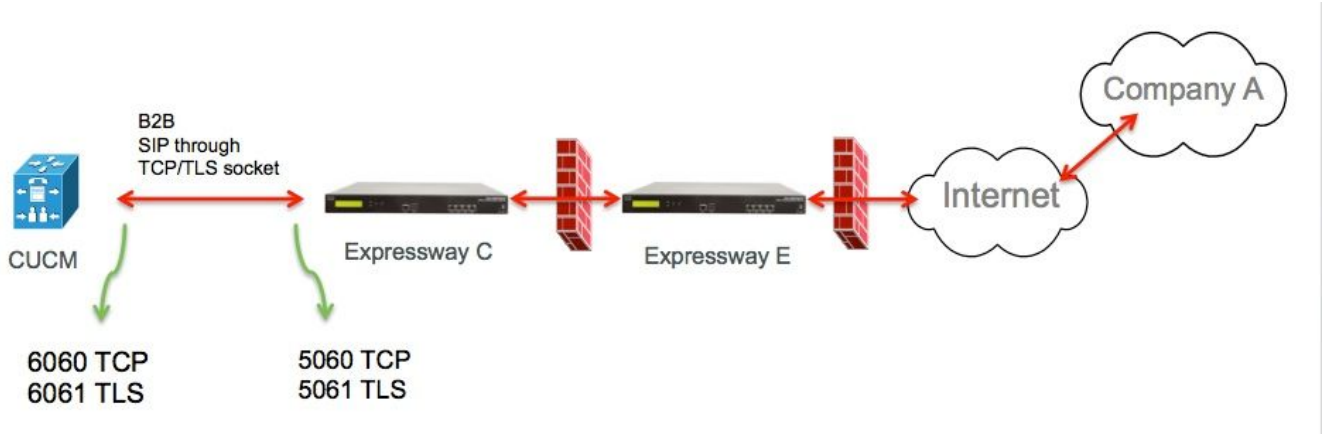


Per le chiamate B2B, configurare un trunk SIP in CUCM che punti a Expressway-C dove in genere CUCM rimane in ascolto sulla porta 5060 o 5061 per il traffico in entrata da questo gateway.

Poiché il traffico ai bordi proviene dallo stesso IP di origine con la porta 5060/5061, è necessario utilizzare una porta di ascolto diversa per questo trunk in CUCM. In caso contrario, il traffico edge viene instradato al dispositivo trunk SIP in CUCM e non al dispositivo endpoint (CSF o EX).

Per Expressway-C, utilizzare le porte 5060 e 5061 per il protocollo TCP/TLS del protocollo SIP (Session Initiation Protocol).

Nell'immagine è riportato un esempio di ascolto di CUCM sulla porta 6060/6061 per il traffico in entrata su questo trunk



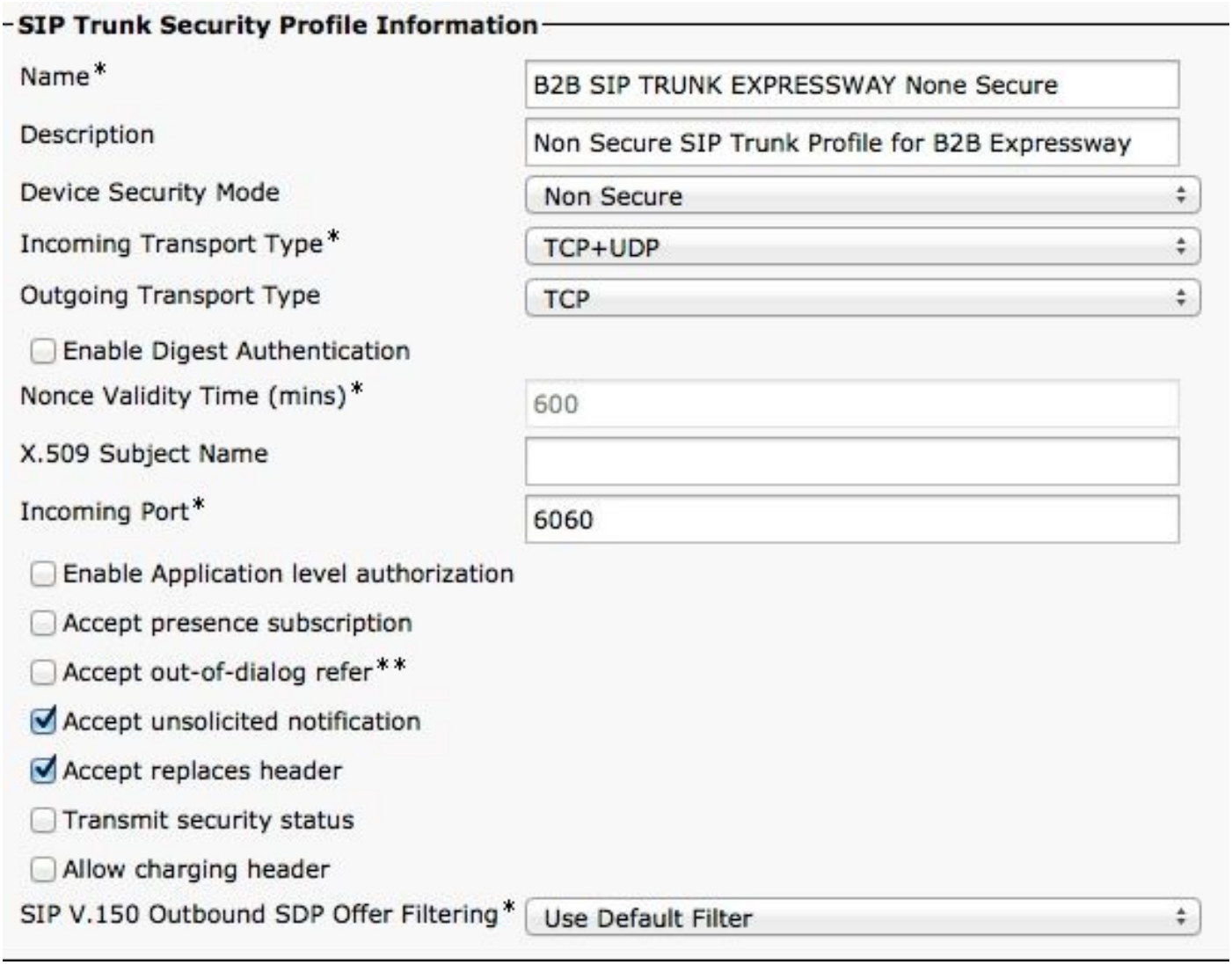
Di seguito sono riportati i diversi passaggi di configurazione documentati per questa distribuzione. Entrambi per installazioni sicure e non sicure.

r. Aggiunge un nuovo profilo di sicurezza trunk SIP.

Dalla **pagina Amministrazione CUCM,** passare a **> Dispositivo > Trunk.**

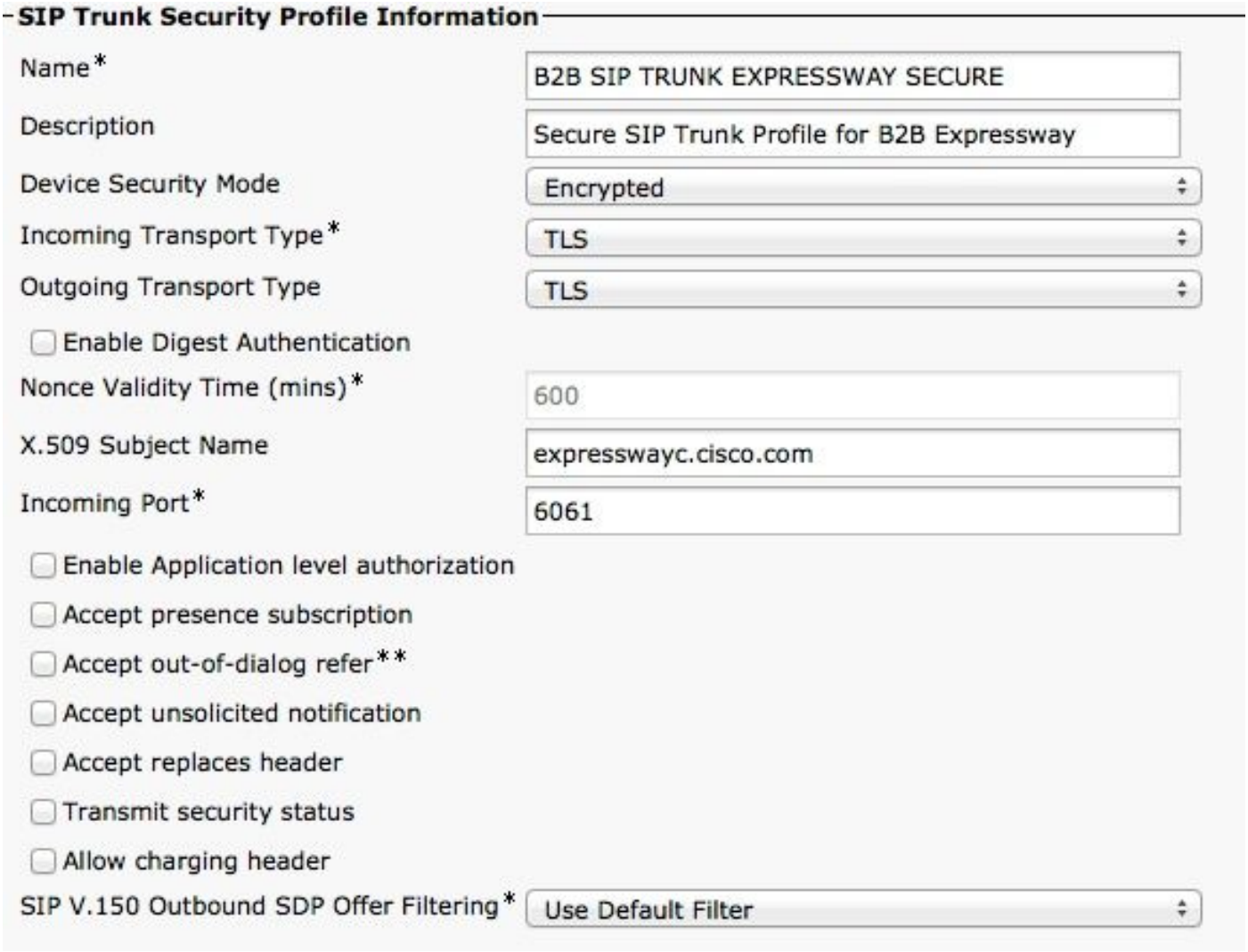
Configurare una porta in ingresso diversa da 5060/5061, dove utilizzare 6060 per TCP e 6061 per TLS

Profilo trunk SIP non sicuro



Profilo trunk SIP protetto

Per TLS è inoltre necessario configurare il nome soggetto X.509 corrispondente al CN del certificato presentato da Expressway-c. Inoltre, caricare Expressway-C o il certificato CA (che ha emesso il certificato Expressway-C) nell'archivio certificati CUCM.



b. Configurare il trunk SIP su CUCM.

Attraverso questo trunk, tutte le chiamate B2B fluiscono da e verso CUCM.

I parametri di configurazione trunk SIP sono standard per le distribuzioni CUCM con VCS.

Accertarsi di associare il profilo di sicurezza creato al passaggio 1.

c. Configurare una zona adiacente su Expressway-C

Ènecessario configurare una zona adiacente su Expressway-C per la destinazione CUCM.

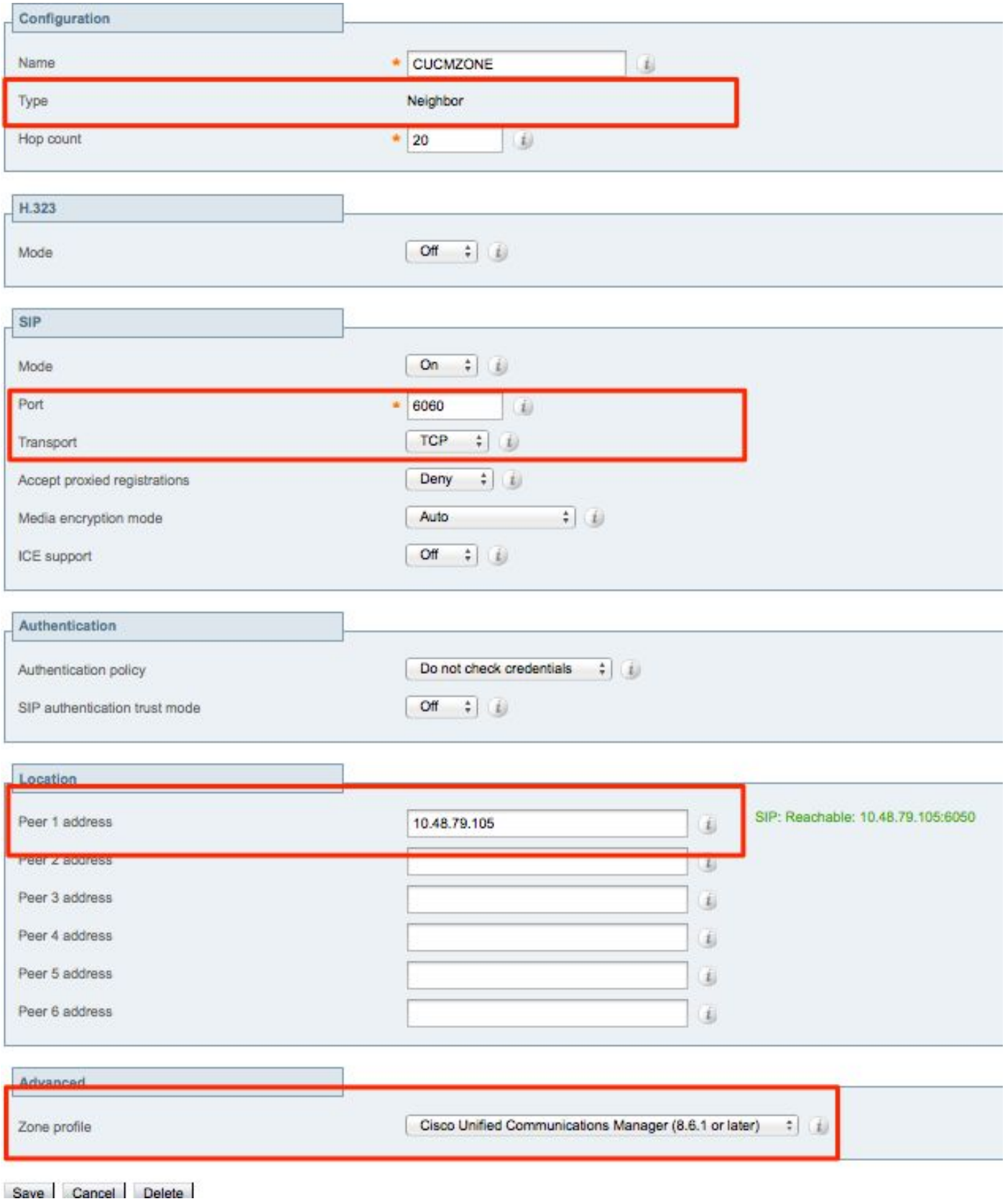
Questa zona viene utilizzata per instradare il traffico B2B in entrata verso CUCM.

La configurazione è standard, con la differenza che è necessario verificare che la porta di destinazione corrisponda alla porta di ascolto configurata nel profilo SIP Trunk Security assegnato al trunk SIP su CUCM.

Nell'esempio, la porta di destinazione utilizzata è 6060 per SIP/TCP e 6061 per SIP/TLS. (fare riferimento al passaggio 1), come mostrato nell'immagine

Dalla pagina Amministrazione di Expressway passare a **Configurazione > Dial Plan > Trasformazioni per configurazione**

Zona adiacente per TCP SIP:

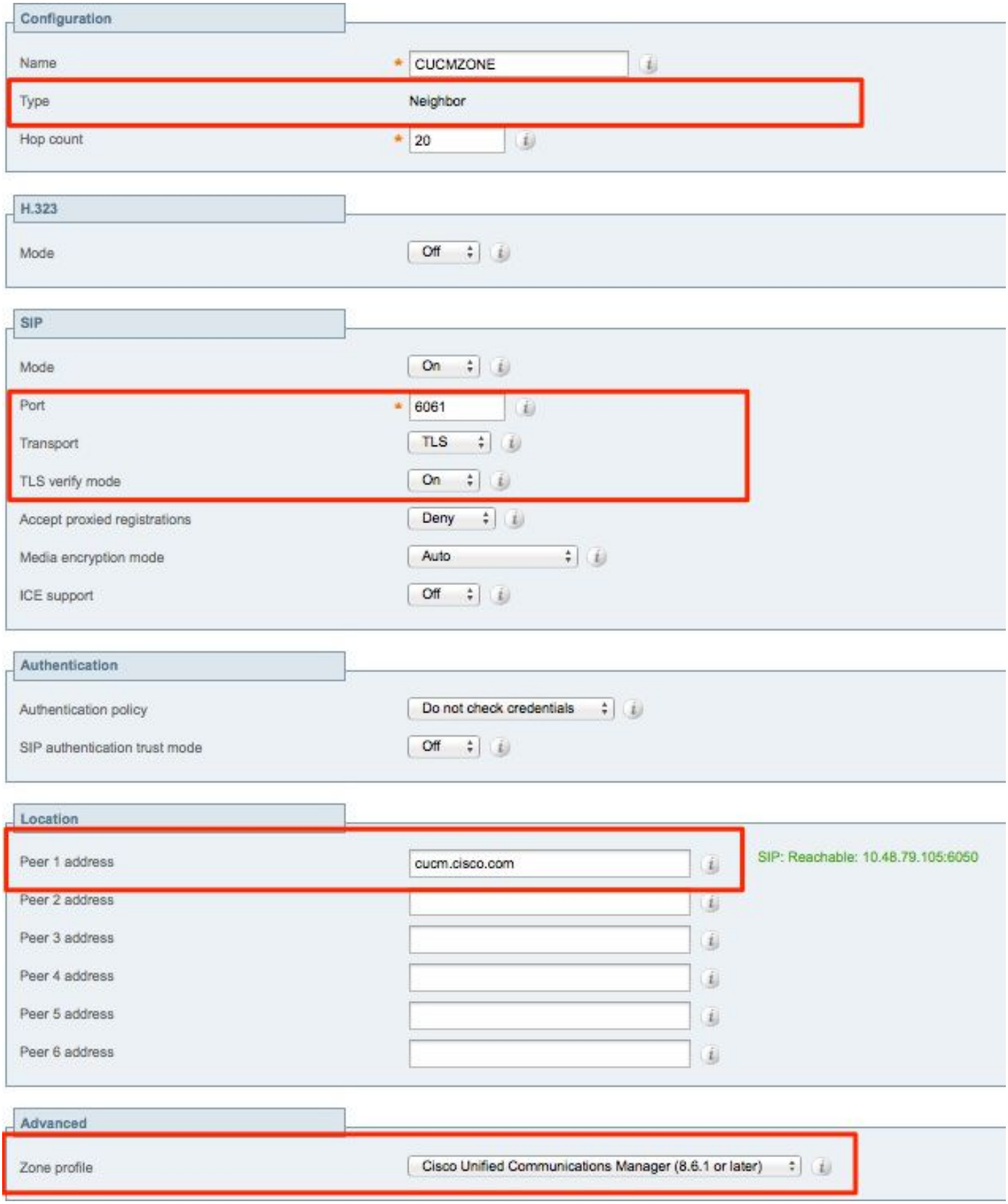


Zona adiacente per SIP TLS - con modalità di verifica TLS attivata

Quando la modalità di verifica TLS è impostata su on, è necessario verificare che l'**indirizzo peer** corrisponda alla CN o alla SAN dal certificato presentato da CUCM. In genere con la modalità di verifica TLS in è possibile configurare il nome di dominio completo (FQDN) del nodo CUCM per l'indirizzo peer.

Dalla pagina Amministrazione di Expressway, passare a **Configurazione > Dial Plan >**

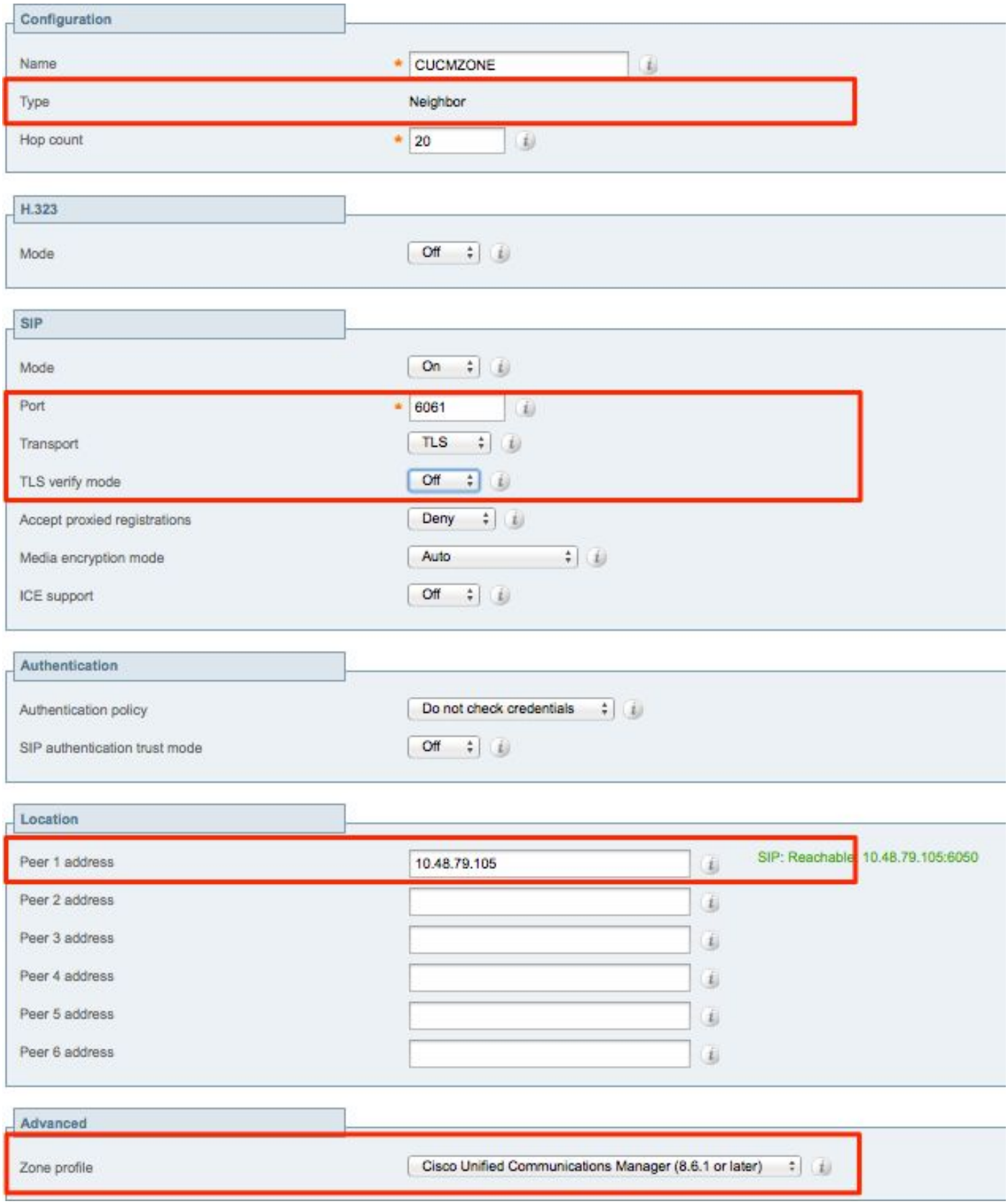
Trasformazioni per configurazione



Zona adiacente per SIP TLS - con modalità di verifica TLS disattivata

Quando la modalità di verifica TLS è impostata su off, l'indirizzo peer può essere l'indirizzo IP, il nome host o il nome di dominio completo (FQDN) del nodo CUCM.

Dalla pagina Amministrazione di Expressway passare a **Configurazione > Dial Plan > Trasformazioni per configurazione**



d. Controlla certificati

Per il TLS, assicurarsi che:

- Il certificato del server Expressway-C o la radice della CA (utilizzata per firmare il certificato) viene caricato nell'archivio CUCMTrust in tutti i server del cluster CUCM.

- Il certificato CallManager o la radice CA (utilizzata per firmare il certificato) viene caricata nell'elenco di certificati CA attendibili sul server Expressway-C.

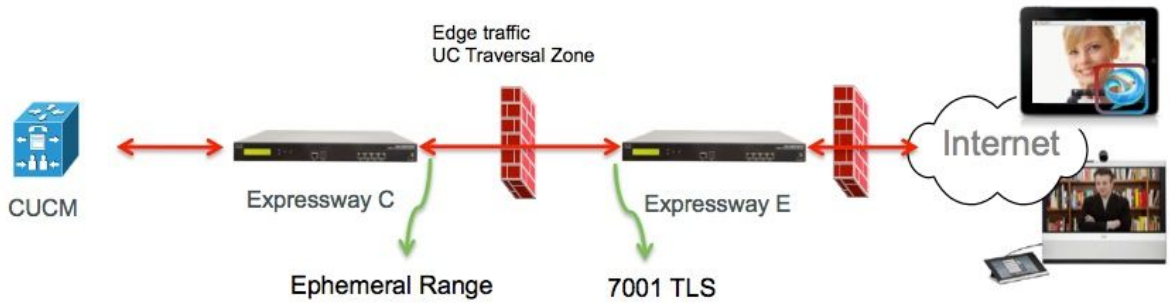
Passaggio 2. Configurare la zona di attraversamento tra Expressway-C ed Expressway-E

Ènecessario configurare una zona di attraversamento separata per instradare il traffico B2B tra Expressway-C ed Expressway-E.

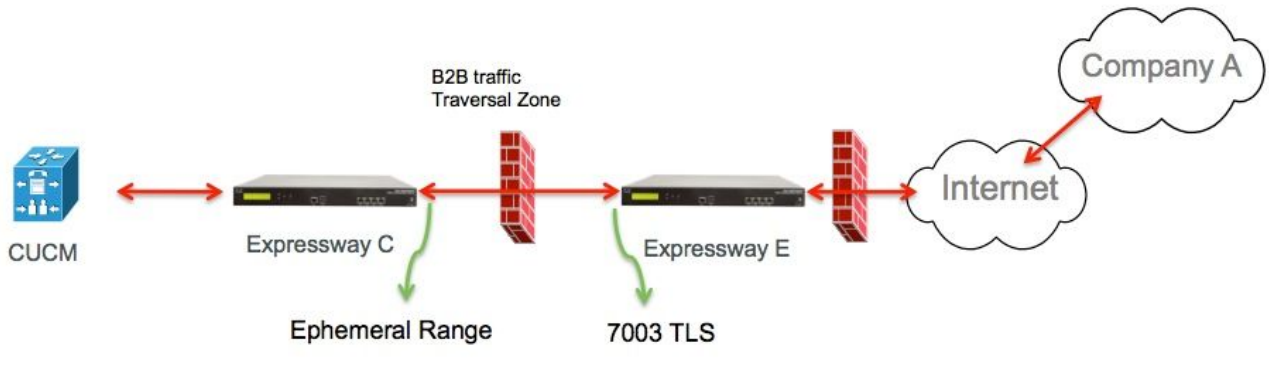
Questa è una configurazione di zona trasversale standard, ma come per il trunk SIP su CUCM è necessario configurare una porta diversa da quella utilizzata dalla zona trasversale UC per il traffico Edge.

La porta standard per la zona di transito UC è 7001. Per la zona B2B Traversal, ad esempio, è possibile configurare 7003.

Zona trasversale UC per il traffico ai bordi, come mostrato nell'immagine



Zona di transito per il traffico B2B, come mostrato nell'immagine

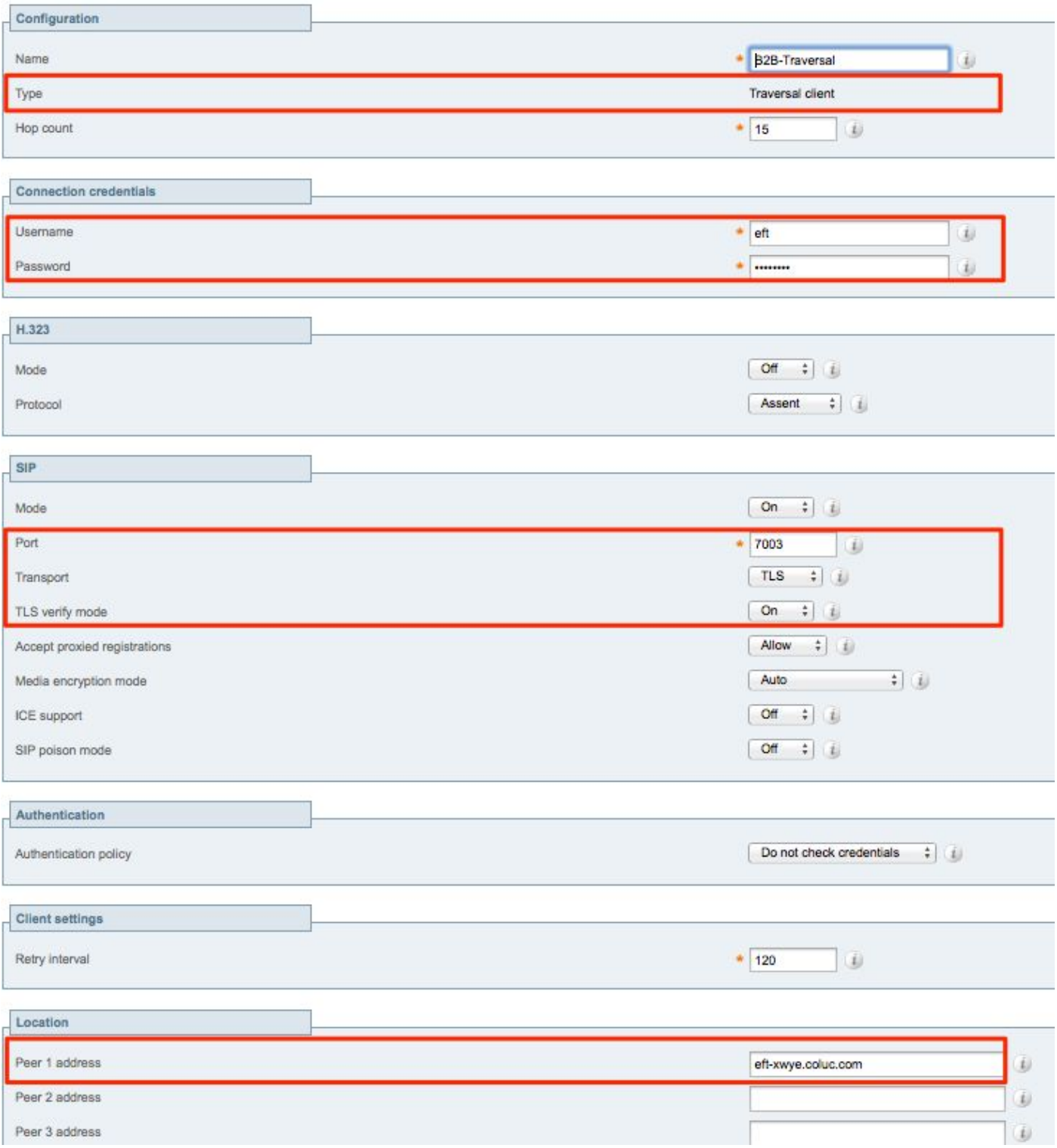


r. Configurazione della zona di transito per il traffico B2B su Expressway-C

Expressway-C è il client della zona trasversale. In questo esempio, la porta di destinazione è 7003

Se la modalità di verifica TLS è impostata su On, verificare che l'**indirizzo peer** configurato corrisponda al CN o alla SAN del certificato presentato da Expressway-E

Dalla pagina Amministrazione di Expressway, passare a **Configurazione > Dial Plan > Trasformazioni per configurazione**

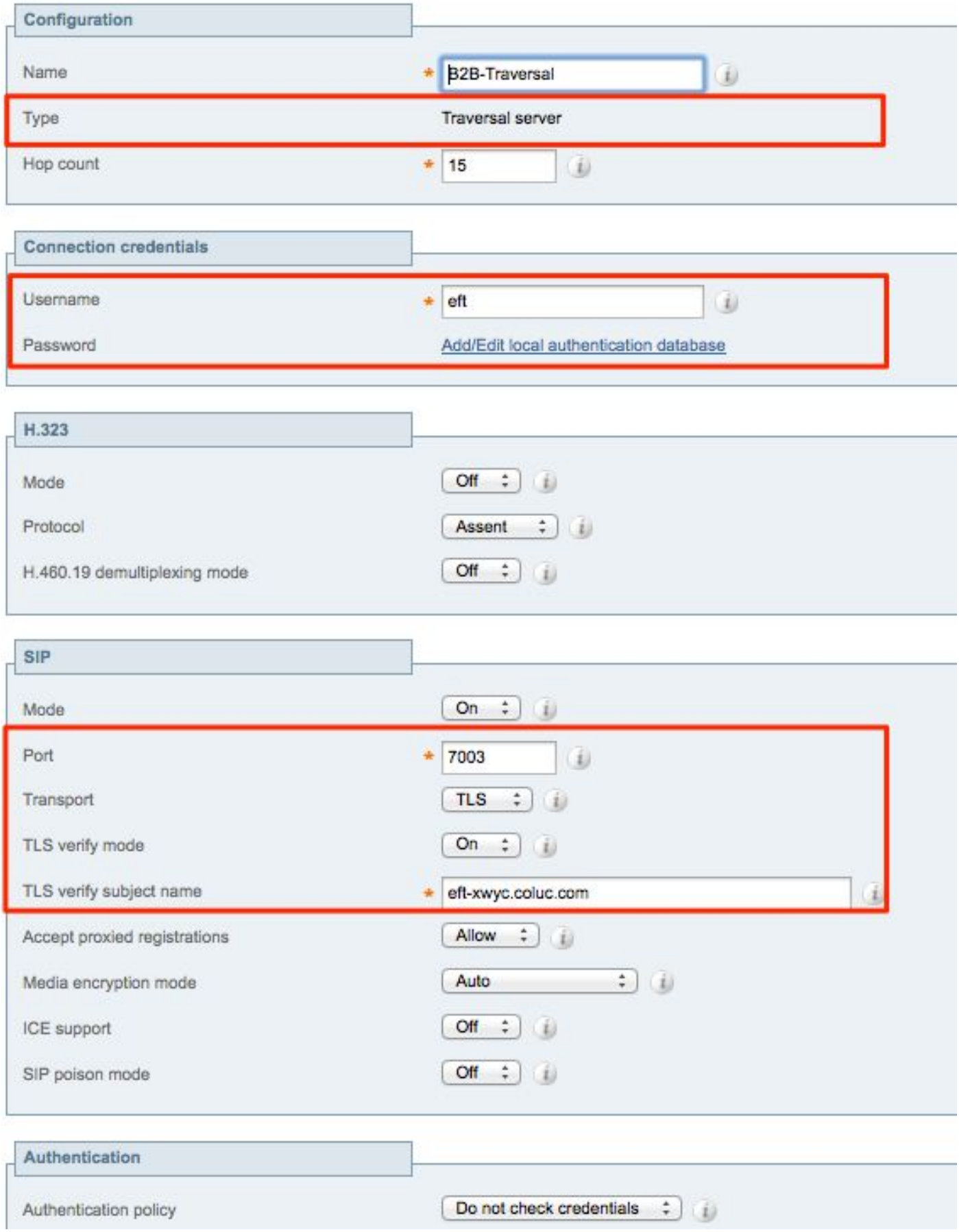


b. Configurazione della zona di transito per il traffico B2B su Expressway-E

Expressway-E è il server della zona trasversale. In questo esempio, la porta di ascolto è 7003.

Se la modalità di verifica TLS è impostata su On, verificare che il **nome soggetto di verifica TLS** configurato corrisponda al CN o alla SAN del certificato presentato da Expressway-C

Dalla pagina Amministrazione di Expressway, passare a **Configurazione > Dial Plan > Trasformazioni per configurazione**



Passaggio 3. Configurare la zona DNS in Expressway-E

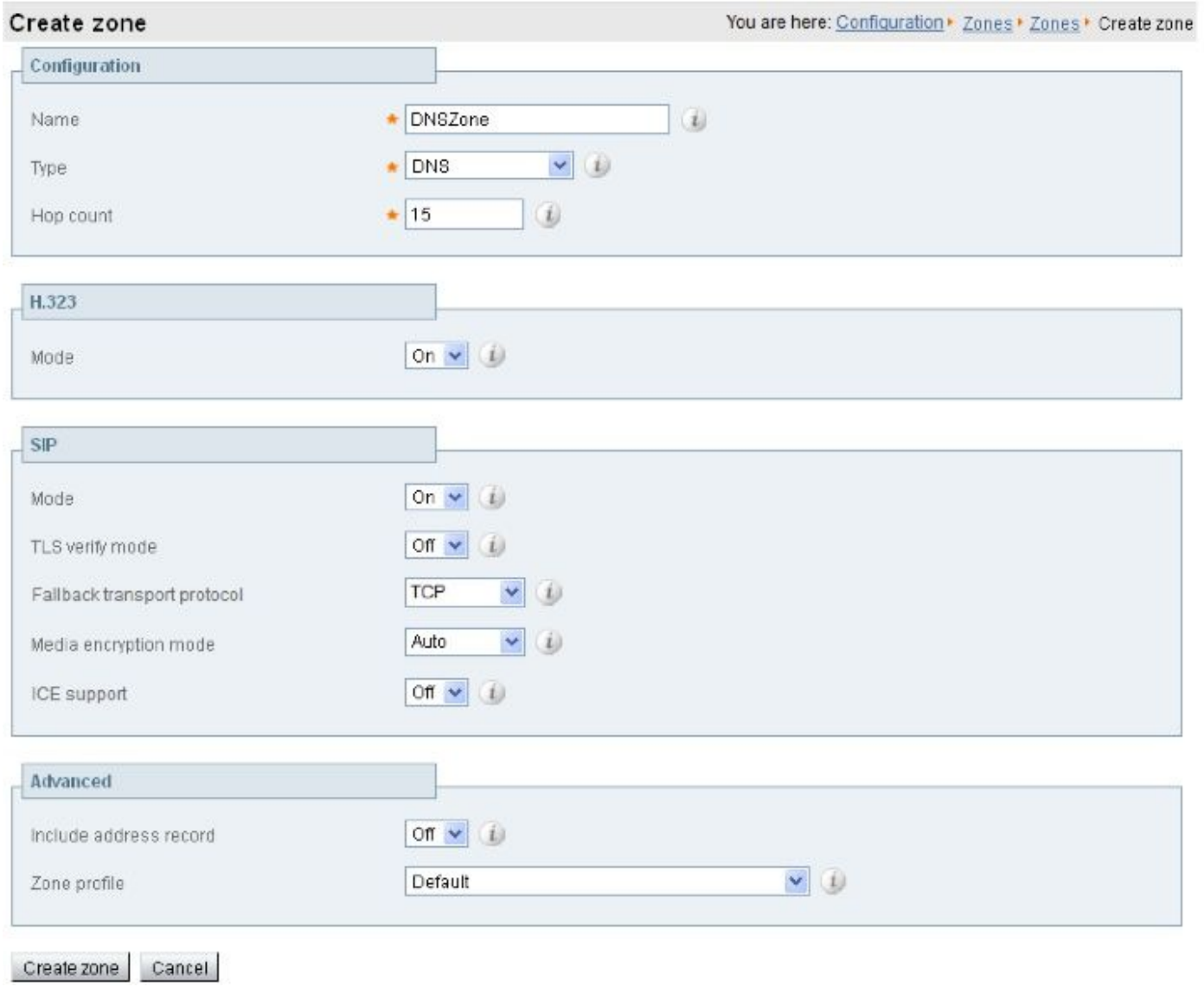
Per indirizzare il traffico B2B, configurare una zona DNS in Expressway-E.

Expressway-E, per il traffico destinato a questa zona, esegue una ricerca DNS SRV per _sip o _sips e questo per il dominio derivato dalla parte dominio dell'URI SIP.

Destinazione SRV restituita dal server DNS utilizzato per instradare la chiamata SIP a.

La configurazione è una configurazione di zona DNS standard.

Dalla pagina Amministrazione di Expressway, passare a **Configurazione > Zone**



Passaggio 4. Configurare il dial plan

a.Trasformazioni e/o regole di ricerca su Expressway-C ed E

Dalla pagina Amministrazione di Expressway passare a **Configurazione > Piano di composizione > Trasformazioni per configurazione > Piano di composizione > Trasforma o Cerca regole**

Per ulteriori informazioni, consultare le guide all'installazione di VCS (Control with Expressway), il capitolo sulla configurazione del routing:

b. SIP Route pattern(s) in CUCM

Per ulteriori informazioni, consultare la Guida all'amministrazione e al sistema CUCM (Dialplan Deployment guide)

c. Per il routing delle chiamate SIP, i record SRV devono essere creati sui server DNS pubblici.

Come mostrato nell'immagine, vengono elencati i record SRV richiesti e le chiamate H323 B2B che non sono state discusse in questo documento. Notare inoltre che SIP UDP è disabilitato per impostazione predefinita in Expressway

DNS SRV records

Name	Service	Protocol	Priority	Weight	Port	Target host
example.com.	h323cs	tcp	10	10	1720	expe.example.com.
example.com.	h323ls	udp	10	10	1719	expe.example.com.
example.com.	sip	tcp	10	10	5060	expe.example.com.
example.com.	sip	udp *	10	10	5060	expe.example.com.
example.com.	sips	tcp	10	10	5061	expe.example.com.

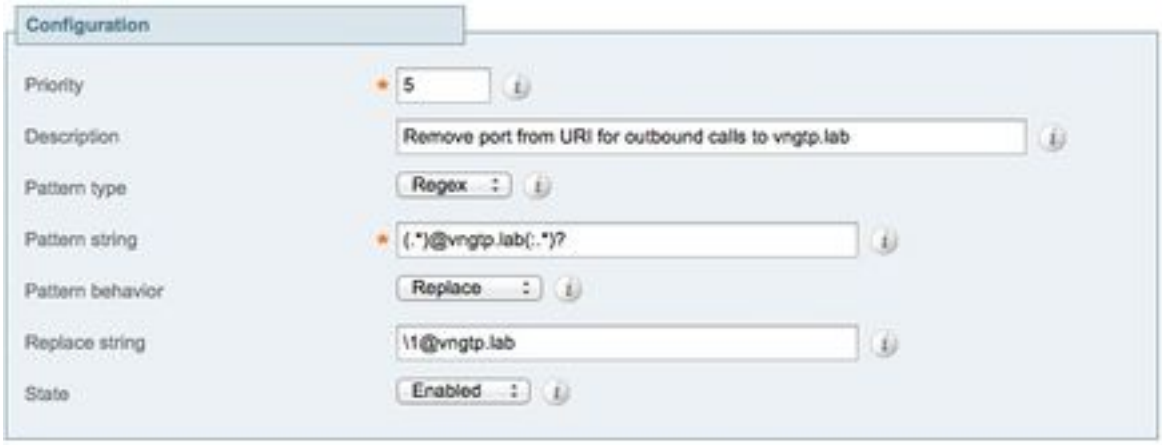
d. Configurare il nome di dominio completo del cluster in CUCM.

Èpossibile immettere più voci separate da una virgola.

e. Creare una trasformazione in Expressway-C che rimuove la porta dall'URI ricevuto nell'invito da CUCM.

Per ulteriori informazioni, cercare questo documento Chiamate da CUCM alla zona DNS su VCS Expressway inviate all'indirizzo IP errato

Dalla pagina Amministrazione di Expressway, passare a **Configurazione > Dial Plan > Trasformazioni per configurazione > Dial Plan > Trasformazione**



Il documento contiene inoltre un capitolo esaustivo sul piano di composizione

Passaggio 5. Caricare le licenze per rich media in Expressway

Le licenze per i rich media (ovvero le licenze per Traversal Zone) devono essere caricate in ogni server Expressway.

Se le chiamate non vengono effettuate o sono dovute a una configurazione errata, viene visualizzato questo messaggio di errore: "Limite licenza chiamata raggiunto: È stato raggiunto il limite di licenze per chiamate trasversali simultanee"

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Per ulteriori informazioni sulla risoluzione dei problemi B2B, fare riferimento a questo documento Risoluzione dei problemi più comuni delle chiamate da business a business tramite Expressway

Informazioni correlate

- Cisco TelePresence Video Communication Server (VCS)
- Documentazione e supporto tecnico – Cisco Systems