Configurer les appels audio et vidéo interentreprises (business-to-business) au moyen d'Expressway intégré à CUCM

Contenu

Introduction

Ce document décrit comment intégrer et configurer le déploiement interentreprises (B2B) des appels audio et vidéo par l'entremise d'Expressway et intégré au Cisco Unified Call Manager (CUCM).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Expressway-C (Exp-C)
- Expressway-E (Exp-E)
- Cisco Unified Call Manager (CUCM)
- Cisco Unity Connection (CUC)
- Téléprésence par Video Communication Server-C (VCS-C)
- Téléphone Jabber
- Cisco Telepresence System (CTS)
- Téléphone EX
- Session Initiation Protocol (SIP)
- Hypertext Transfer Protocol (HTTP)
- eXtensible Messaging and Presence Protocol (XMPP)
- Cisco Unified IM and Presence (IM&P)
- Certificats

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Expressway C et E X8.1.1 ou ultérieur
- Unified Communications Manager (CUCM) 10.0 ou ultérieur.

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Les étapes suivantes décrivent de manière détaillée comment intégrer et configurer le déploiement interentreprises (B2B) des appels audio et vidéo par l'entremise d'Expressway intégré au CUCM dans le but de faire et de recevoir des appels d'autres entreprises (domaines).

Expressway avec la fonction d'accès distant mobile (MRA) permet l'enregistrement transparent des terminaux Jabber et TC situés en dehors du réseau de l'entreprise, comme le montre le schéma de réseau.

La même architecture assure également une intégration/des appels fluides entre différentes entreprises (intégration d'entreprise à entreprise, par exemple pour les applications audio, vidéo et IM&P). (B2B)

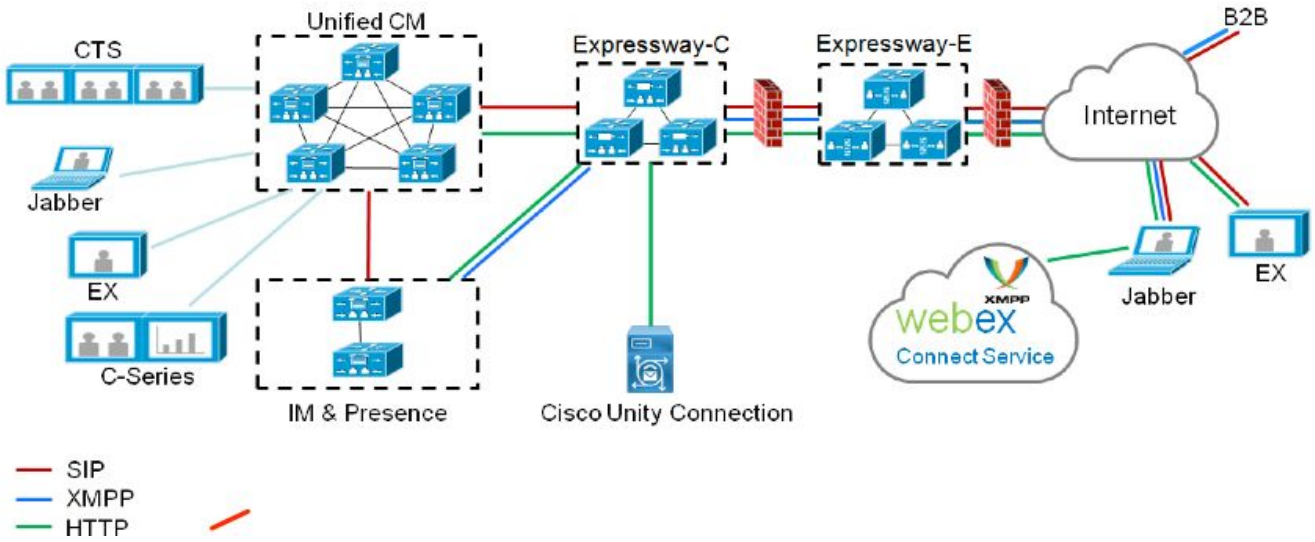
Ce document ne couvre pas la partie IM&P, ni l'intégration H.323.

Avant de continuer, vous devez vous assurer que le service DNS (SRV) approprié a été créé pour votre domaine. Ces enregistrements sont utilisés par d'autres sociétés pour trouver l'emplacement de votre Expressway.

Configuration

Diagramme du réseau

Cette illustration donne un exemple de diagramme de réseau



Étape 1. Liaison SIP entre CUCM et Expressway-C

Une fois la détection CUCM effectuée par Expressway-C, les zones voisines sont automatiquement configurées pour chaque noeud et le protocole de transport est découvert.

Lorsque le cluster CUCM est configuré en mode mixte, il existe une zone pour le protocole TCP (Transmission Control Protocol) pour le trafic non sécurisé avec le port de destination 5060 et une zone pour TLS (Transport Layer Security) pour le trafic sécurisé avec le port de destination 5061. Ces ports ne peuvent pas être modifiés.

Les deux zones sont utilisées pour tous les appels de périphérie vers et depuis les points d'extrémité de périphérie.

Les appels entrants provenant des points d’extrémité Edge prennent la route de ces zones ajoutées automatiquement et ciblent conséquemment les ports TCP 5060 ou TLS 5061 du CUCM.

Les points d’extrémités Edge enregistrent et font ou reçoivent des appels par les interfaces de connexion établies.

Pour les appels B2B, configurez une liaison SIP dans CUCM qui pointe vers Expressway-C où CUCM écoute généralement le trafic entrant de cette passerelle sur le port 5060 ou 5061.

Puisque le trafic Edge vient de la même source IP sur les ports 5060/5061, vous devez utiliser un autre port de réception pour cette ligne principale dans CUCM. Sinon, le trafic de périphérie est acheminé vers le périphérique de liaison SIP dans CUCM et non vers le périphérique de point d'extrémité (CSF ou EX).

Du côté de Expressway-C, utilisez les ports 5060 et 5061 pour le SIP (Session Initiation Protocol) TCP/TLS.

Cette illustration décrit un cas où CUCM reçoit le trafic entrant sur les ports 6060/6061 sur cette ligne principale.

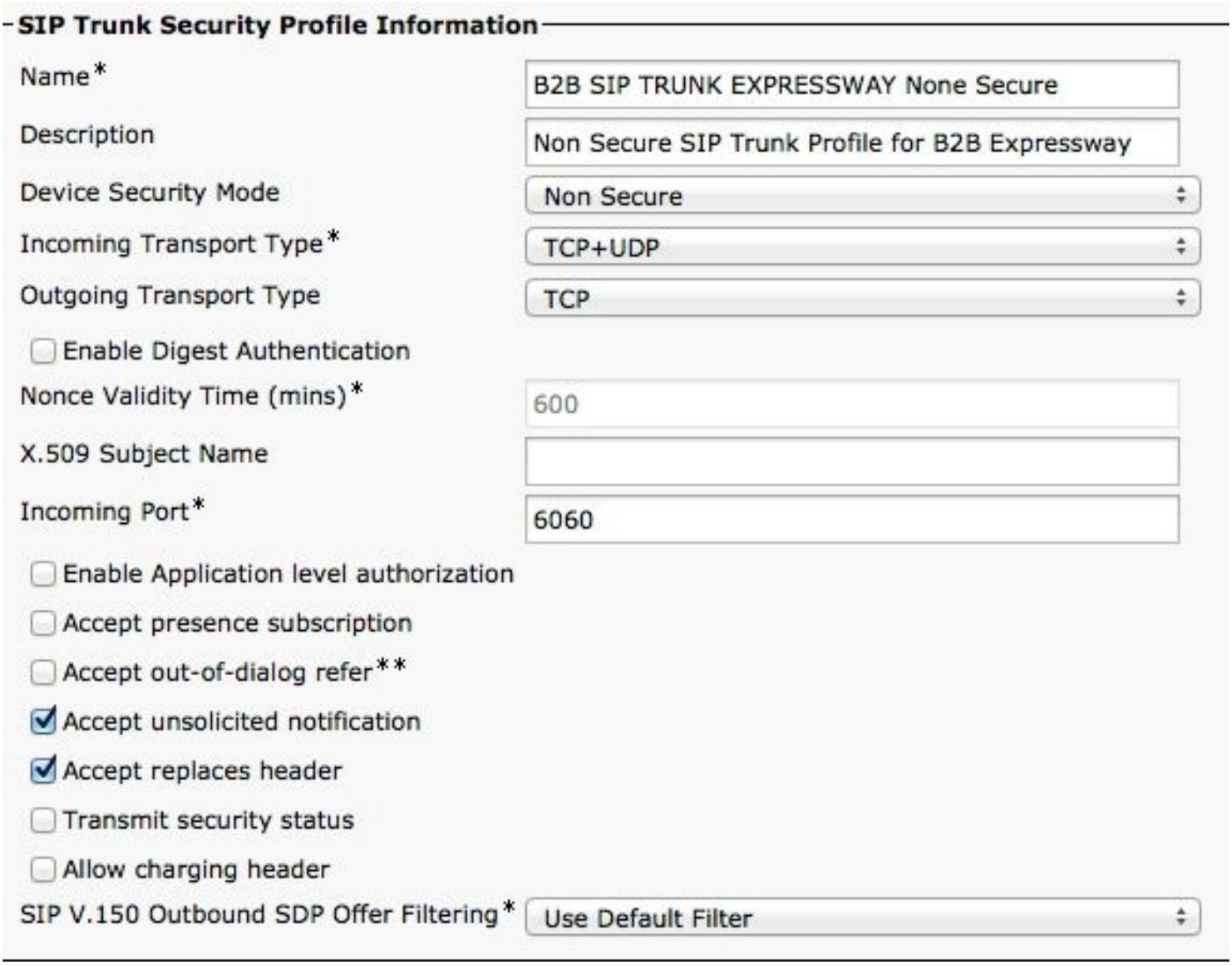
Voici les étapes de configuration pour ce déploiement. Convient aux déploiements sécurisés et non sécurisés.

a. Ajouter un nouveau profil de sécurité de la ligne principale SIP

Dans le **page d'administration de CUCM, naviguez jusqu'à > Device > Trunk.**

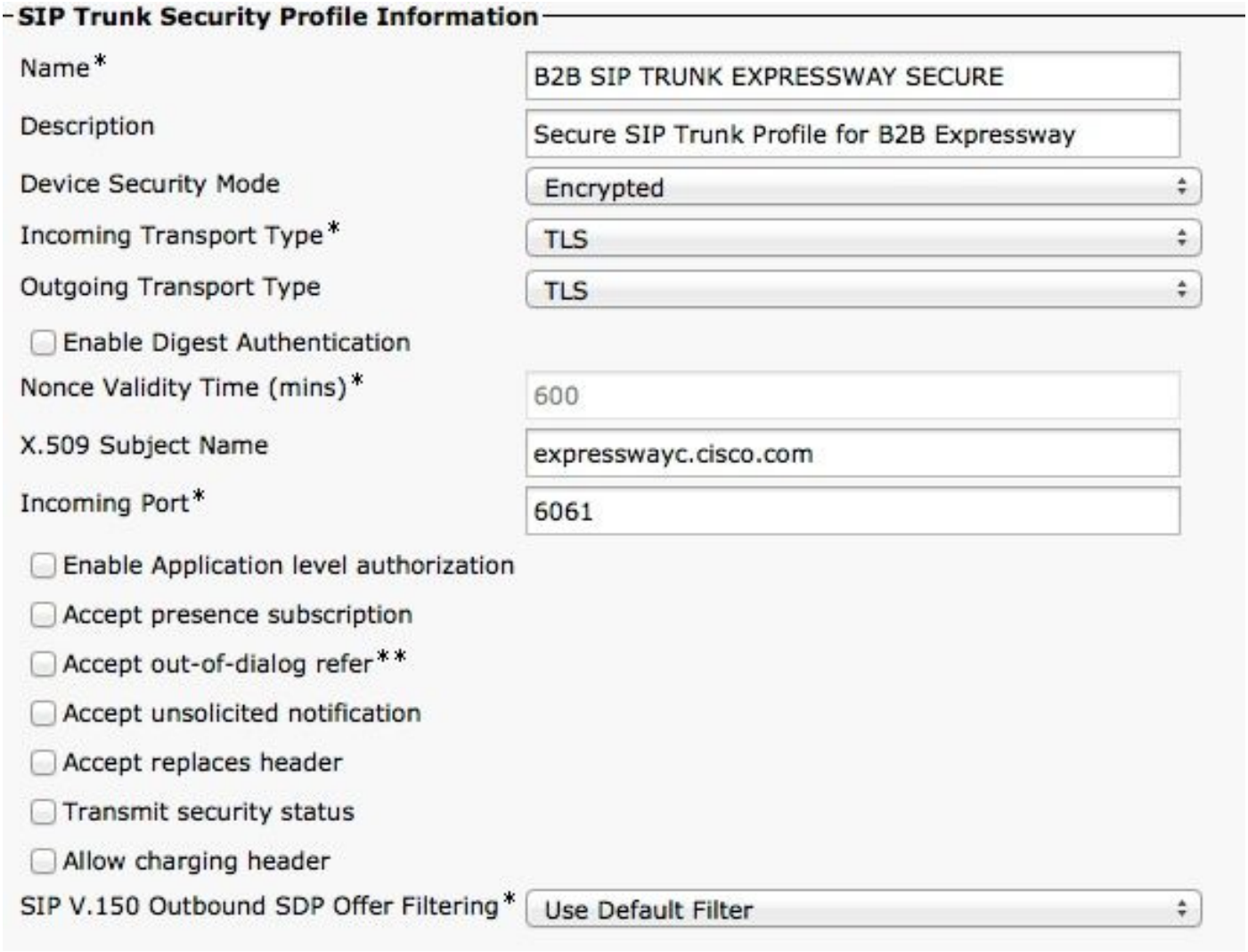
Configurez un port entrant différent de 5060/5061, ici utilisez 6060 pour TCP et 6061 pour TLS

Profil de ligne principale SIP non sécurisée



Profil de la ligne principale SIP sécurisée

Pour TLS, vous devez aussi configurer le Subject name X.509 qui correspond au CN du certificat présenté à Expressway-C. En outre, téléchargez également l'Expressway-C ou le certificat CA (qui a délivré le certificat Expressway-C) dans le magasin de fiducie de certificat CUCM.



b. Configurez la ligne principale SIP sur CUCM.

Par cette liaison, tous les appels B2B circulent à destination et en provenance de CUCM.

Les paramètres de configuration de ligne principale SIP sont standard pour CUCM avec les déploiements VCS.

Assurez-vous d'associer le profil de sécurité créé à l'étape 1.

c. Configurer une zone voisine sur Expressway-C

Une zone voisine doit être configurée sur Expressway-C pour cibler CUCM.

Cette zone est utilisée pour acheminer le trafic B2B entrant au CUCM.

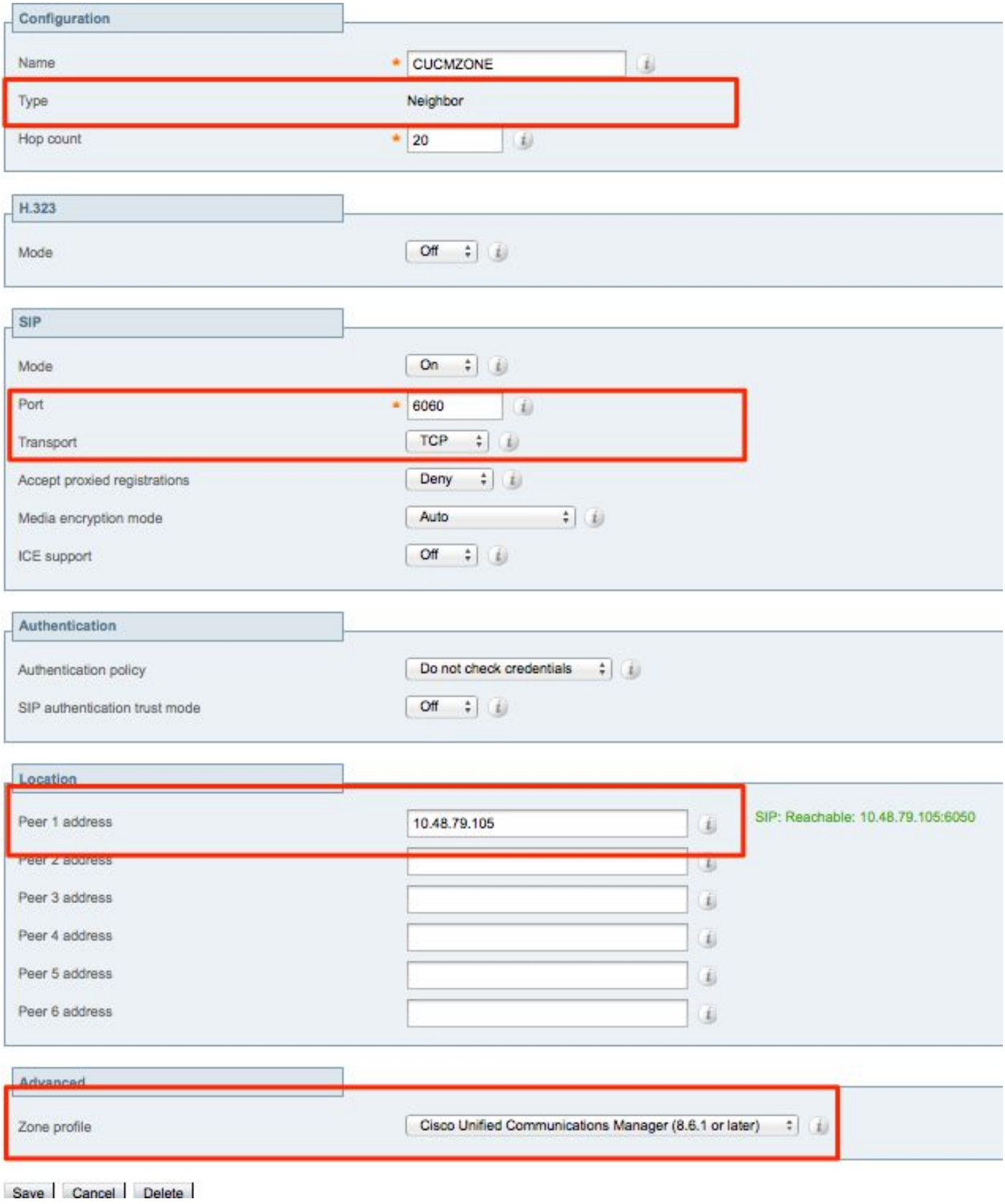
La configuration est standard, sauf que vous devez vous assurer de configurer le port de destination pour qu'il corresponde au port d'entrée configuré dans le profil de sécurité de la ligne

principale SIP affecté à la ligne principale SIP sur CUCM.

Dans cet exemple, le port de destination utilisé est 6060 pour SIP/TCP et 6061 pour SIP/TLS. (reportez-vous à l'étape 1), comme indiqué dans l'illustration

Àpartir de la page Expressway Administration, accédez à **Configuration > Dial Plan > Transforms y Configuration**

Zone voisine pour TCP SIP :

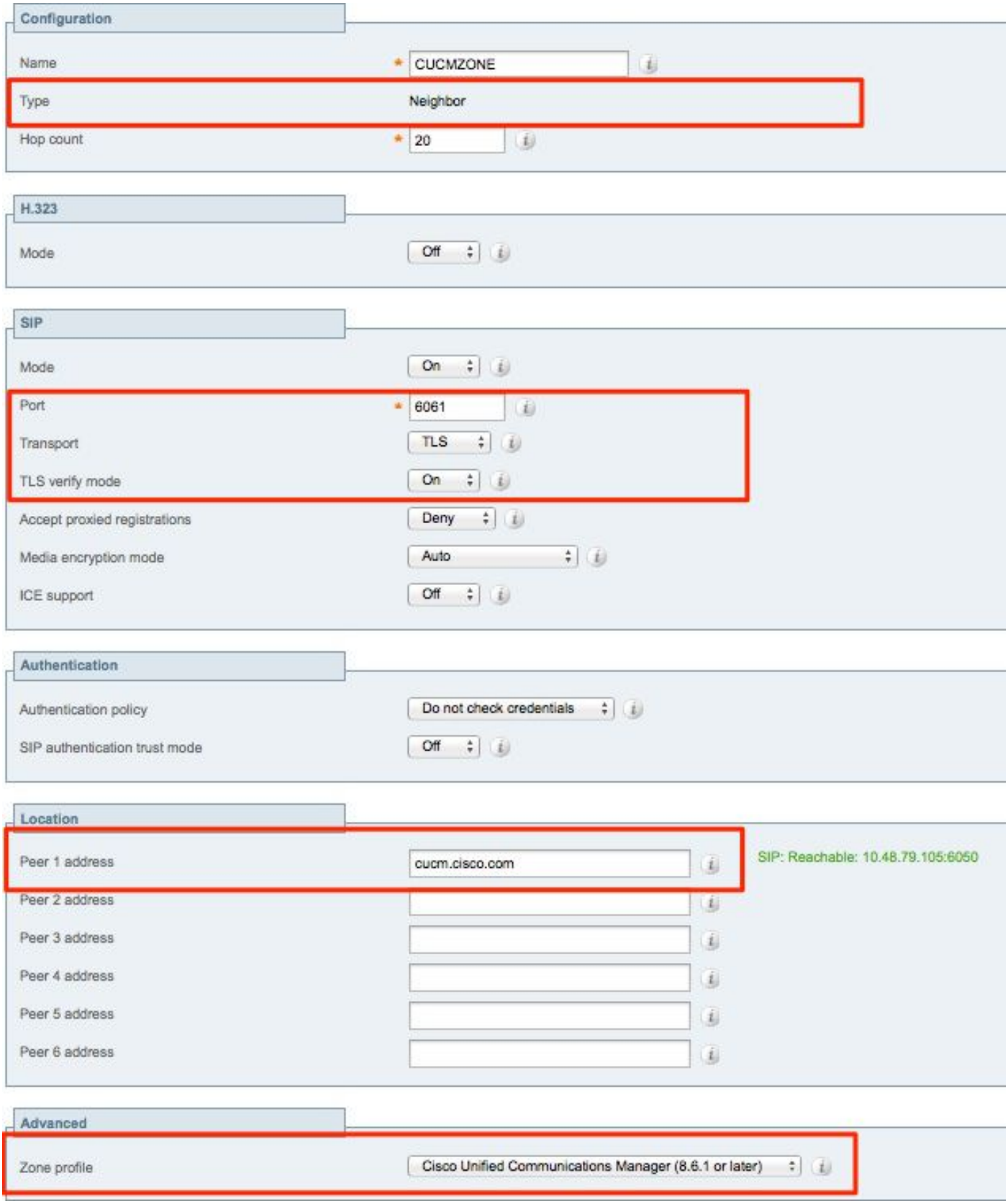


Zone voisine pour TLS SIP - avec le mode de vérification TLS activé

Lorsque le mode de vérification TLS est activé, vous devez vous assurer l'**adresse homologue correspond au CN ou au SAN du certificat présenté par CUCM.** En règle générale, avec le mode de vérification TLS, vous configurez le nom de domaine complet (FQDN) du noeud CUCM pour l'adresse homologue.

Àpartir de la page Expressway Administration, accédez à **Configuration > Dial Plan > Transforms**

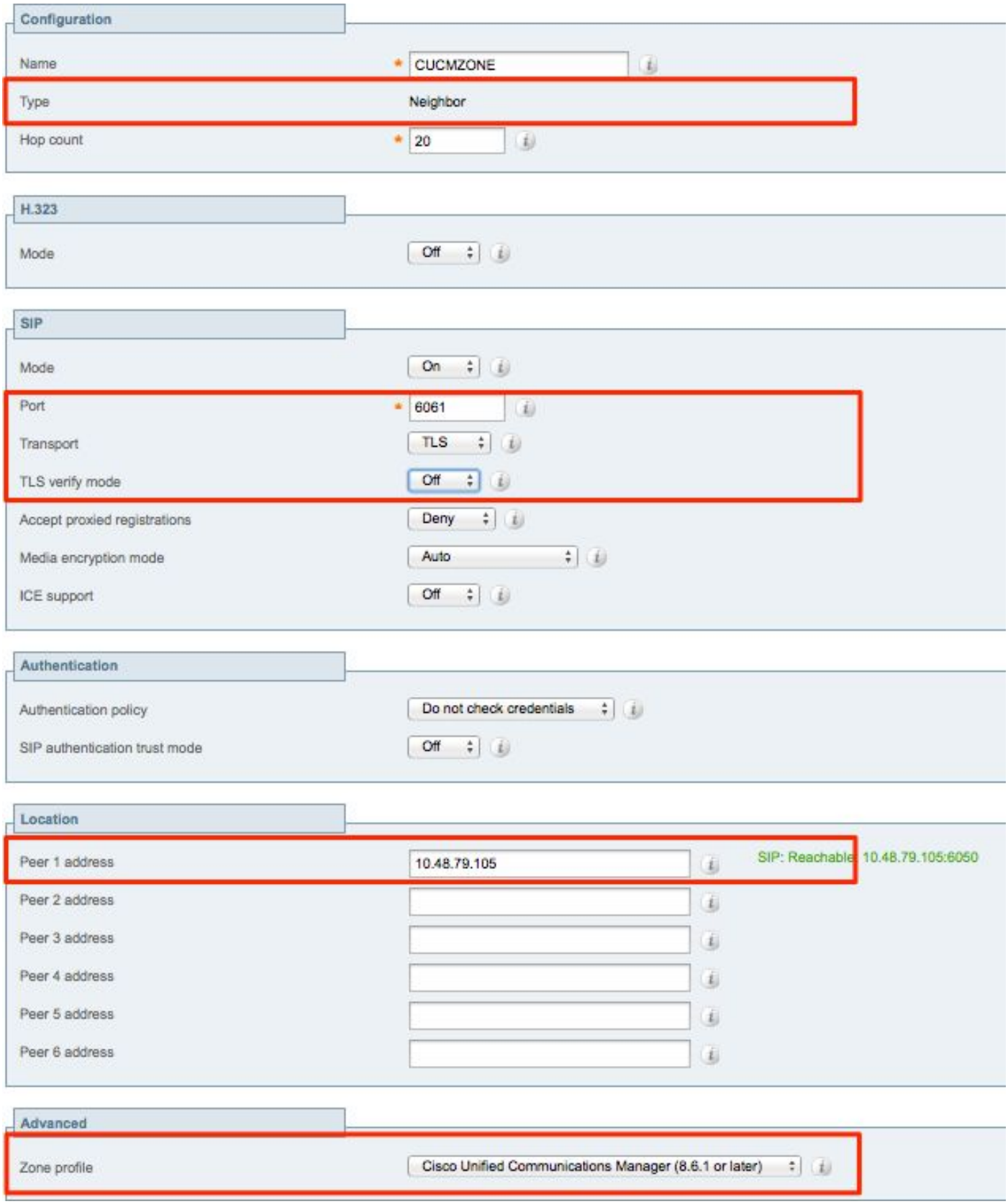
y Configuration.



Zone voisine pour TLS SIP, avec le mode de vérification TLS désactivé

Lorsque le mode de vérification TLS est désactivé, l'adresse homologue peut être l'adresse IP, le nom d'hôte ou le nom de domaine complet du noeud CUCM.

Àpartir de la page Expressway Administration, accédez à **Configuration > Dial Plan > Transforms y Configuration**



d. Vérifier les certificats

Pour le TLS, assurez-vous que :

- Le certificat du serveur Expressway-C ou la racine du CA (utilisée pour signer le certificat) est téléversé dans le dépôt CUCM sur tous les serveurs du groupe.

- Le certificat CallManager ou la racine du CA (utilisée pour signer le certificat) est téléversé dans liste de certificats du CA du Trusted CA sur le serveur Expressway-C.

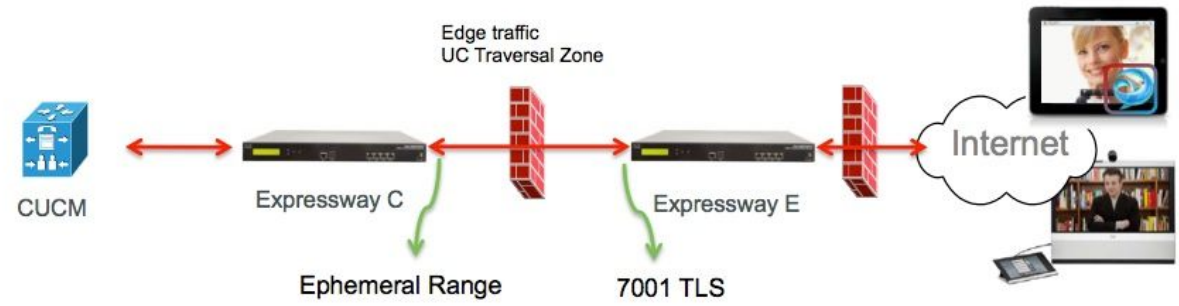
Étape 2. Configurer une zone de traverse entre Expressway-C et Expressway-E

Un horaire que la traversée distincts doit être configuré pour le trafic de route le B2B entre Expressway-C et Expressway E.

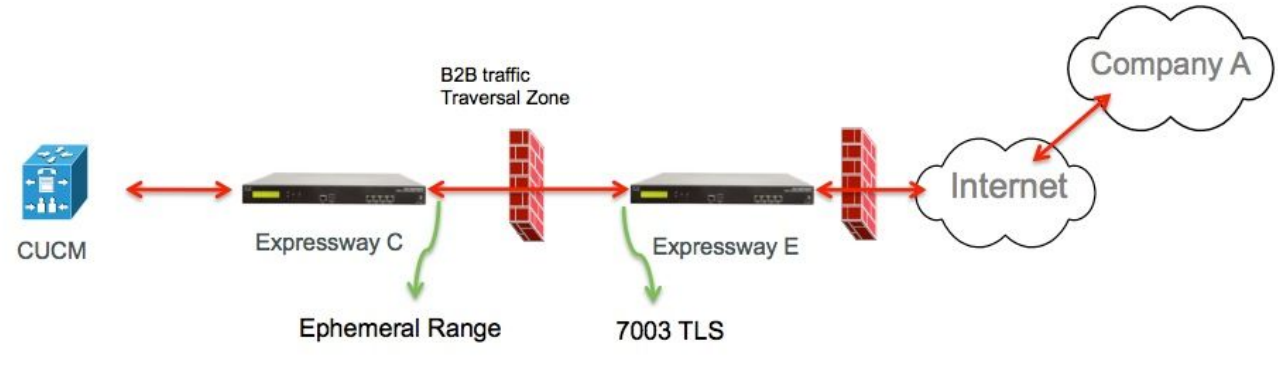
Il s'agit d'une configuration standard de zone de traverse, mais pour la ligne principale SIP du CUCM, un port différent du port utilisé par la zone de traverse UC pour le trafic Edge doit être configuré.

Le port standard pour la zone de traverse UC est 7001. Pour la zone de traversée B2B, vous pouvez par exemple configurer 7003.

La zone de traverse UC pour le trafic Edge est décrite dans l'illustration suivante



La zone de traverse pour le trafic B2B est décrite dans l'illustration suivante



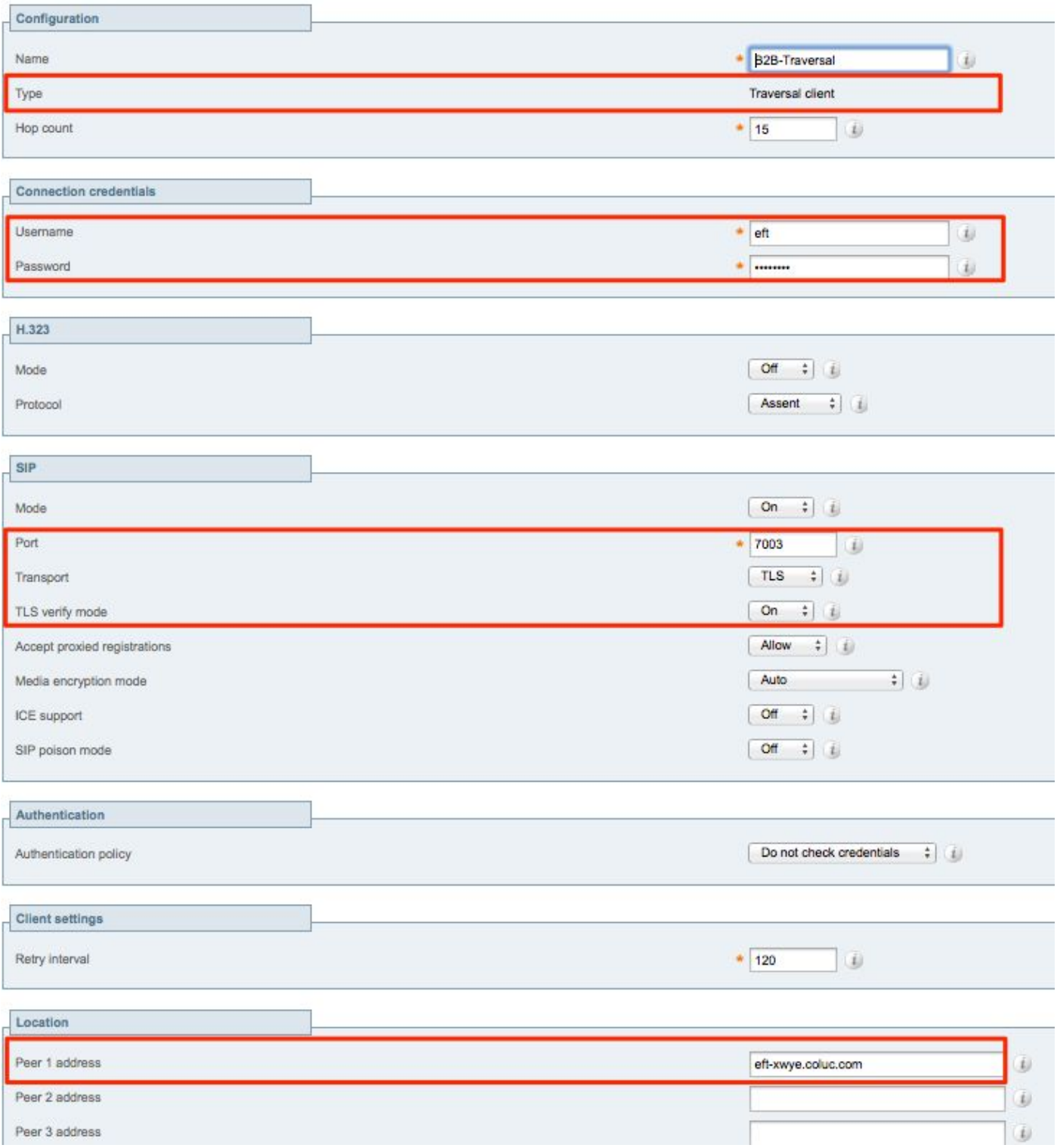
a. Configuration d'une zone de traverse pour le trafic B2B sur Expressway-C

Expressway-C est le client de zone de traversée, dans cet exemple, le port de destination est

7003

Avec le mode de vérification TLS activé, assurez-vous que l'**adresse homologue configurée correponde au CN ou au SAN du certificat présenté par Expressway-E**

Àpartir de la page Expressway Administration, accédez à **Configuration > Dial Plan > Transforms y Configuration.**

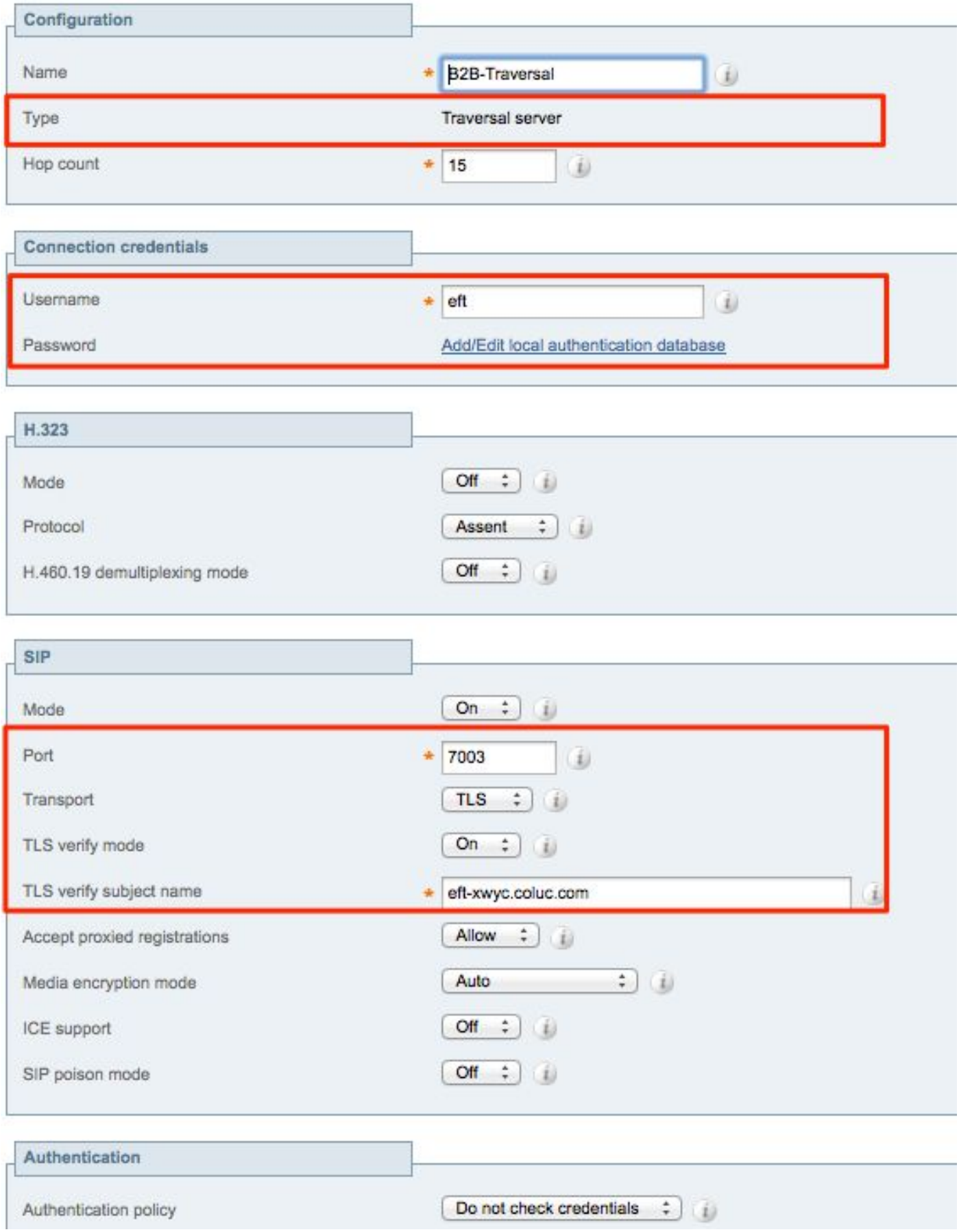


b. Configuration d'une zone de traverse pour le trafic B2B sur Expressway-E

Expressway-E est le serveur de zone de traversée, dans cet exemple, le port d'écoute est 7003.

Avec le mode de vérification TLS activé, assurez-vous que le **TLS verify subject name configuré correspond au CN ou au SAN du certificat présenté par Expressway-C**

Àpartir de la page Expressway Administration, accédez à **Configuration > Dial Plan > Transforms y Configuration.**



Étape 3. Configurer la zone DNS sur Expressway-E

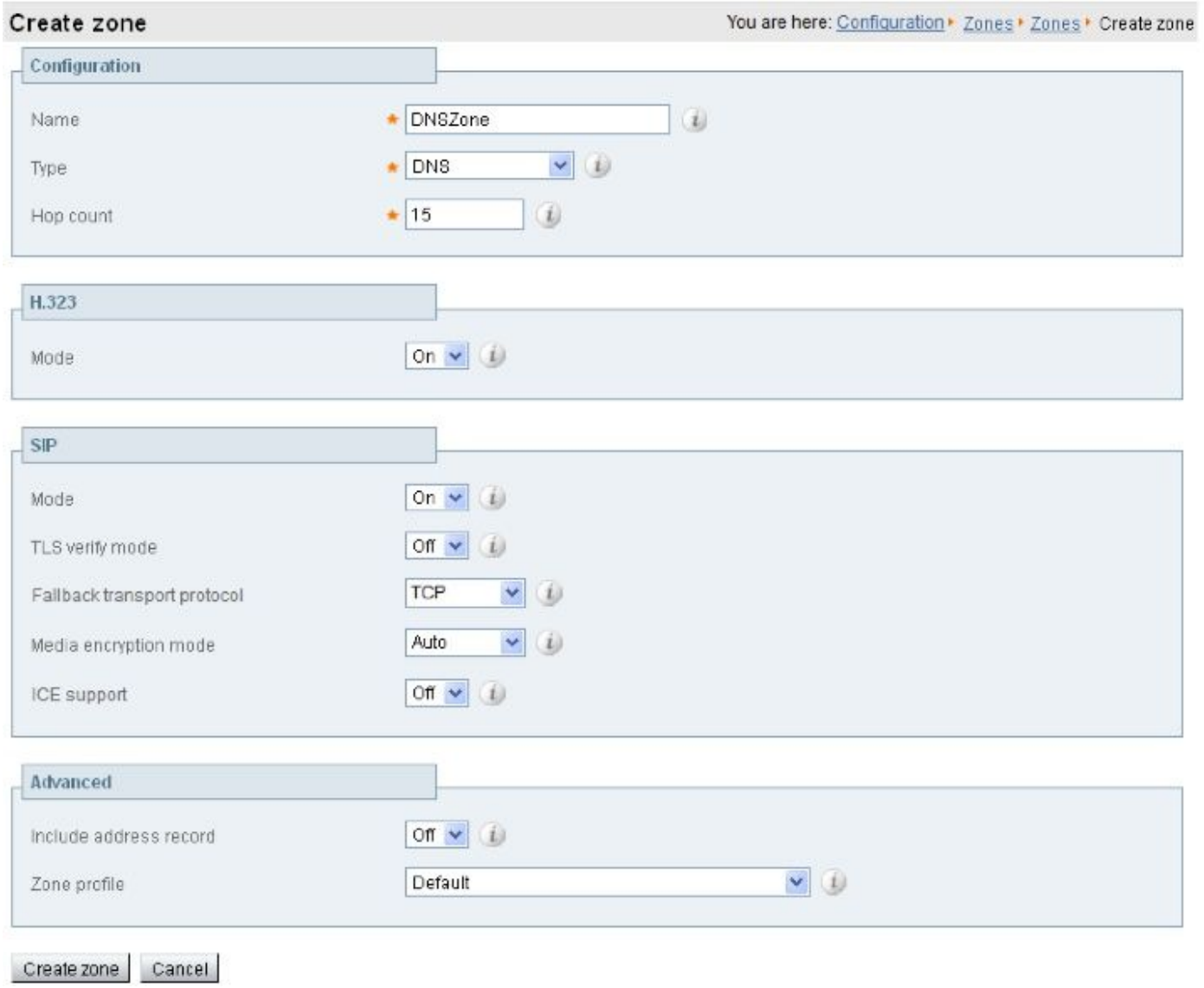
Pour router le trafic B2B, configurez une zone DNS sur Expressway-E.

Expressway-E, pour le trafic destiné à cette zone, effectue une recherche DNS SRV pour les protocoles ther _sip ou _sips et ceci pour le domaine dérivé de la partie domaine de l'URI SIP.

La cible SRV retournée par le serveur DNS utilisée pour acheminer l'appel SIP.

La configuration est une configuration standard de zone DNS.

Àpartir de la page Expressway Administration, accédez à **Configuration > Zones.**



Étape 4. Configurer le plan de numérotation

a.Transforme et/ou recherche de règles sur Expressway-C et E

Àpartir de la page Administration d'Expressway, accédez à **Configuration > Dial Plan > Transforms y Configuration > Dial Plan > Transform or Search Rules**

Pour plus d'informations, consultez les guides de déploiement VCS (Control with Expressway), le chapitre sur la configuration du routage :

b. Schéma(s) de routage SIP dans CUCM

Pour de plus amples renseignements, veuillez consulter le guide d'administration du système CUCM (Dialplan Deployment)

c. Pour le routage d'appels SIP, les enregistrements SRV doivent être créés sur les serveurs DNS publics.

Comme l'illustre l'image, il répertorie les enregistrements SRV requis, ainsi que les appels H323 B2B qui n'ont pas été traités dans ce document. Notez également que le UDP SIP est désactivé par défaut sur 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.

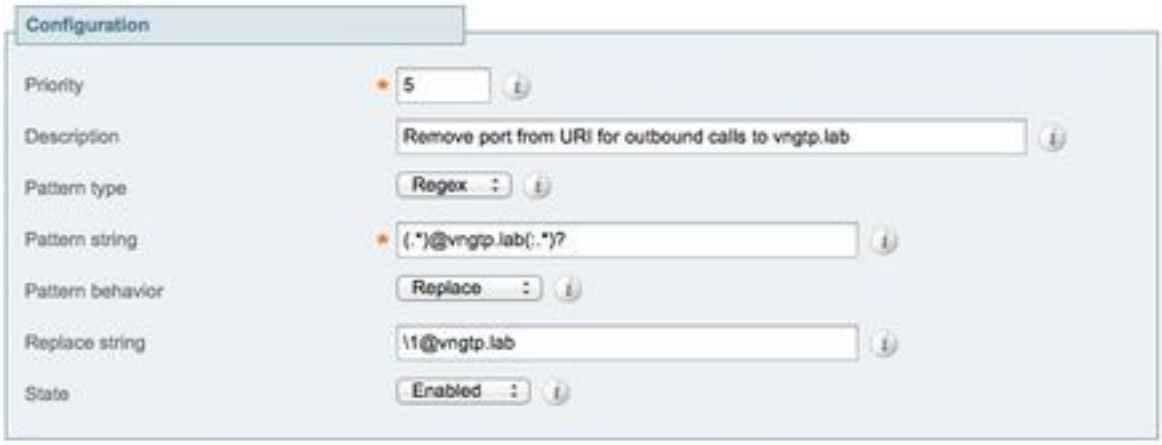
d. Configurer le nom complet du domaine du groupe (cluster) dans CUCM.

Vous pouvez saisir plusieurs entrées séparées par une virgule.

e. Créer une transformation sur Expressway-C qui permet de supprimer le port de l'URI reçu dans l'invitation de CUCM.

Pour plus d'informations, recherchez ce document Appels de CUCM vers la zone DNS sur VCS Expressway envoyés à une adresse IP incorrecte

Àpartir de la page d'administration d'Expressway, naviguez jusqu'à Configuration > Dial Plan > Transforms y Configuration > Dial Plan > Transform



Le SRND contient également un chapitre complet au sujet de Dialplan

Étape 5. Télécharger des licences multimédia sur Expressway

Les licences multimédias (alias Traversal Zone licences) doivent être téléversées sur chaque serveur Expressway.

En cas d'absence ou de configuration incorrecte, les appels sont libérés avec ce message d'erreur : « Limite de licence d'appel atteinte : You have reached your license limit of concurrent traversal call licenses »

Vérification

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Pour plus d'informations sur le dépannage B2B, reportez-vous à ce document Dépannage des problèmes les plus courants pour les appels entre entreprises via Expressway

Informations connexes

- Serveur de communication vidéo (VCS) Cisco TelePresence
- Support et documentation techniques - Cisco Systems