Konfiguration von Business-to-Business-Audio- und Videoanrufen über Expressway, integriert in CUCM

Inhalt

Einführung

Dieses Dokument beschreibt die Integration/Konfiguration der B2B-Bereitstellung (Business to Business) für Audio- und Videoanrufe über Expressway in Cisco Unified Call Manager (CUCM).

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- 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-Telefon
- Cisco TelePresence System (CTS)
- EX-Telefon
- Session Initiation Protocol (SIP)
- Hypertext Transfer Protocol (HTTP)
- XMPP (eXtensible Messaging and Presence Protocol)
- Cisco Unified IM und Presence (IM&P)
- Zertifikate

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Expressway C und E X8.1.1 oder spätere Version
- Unified Communications Manager (CUCM) 10.0 oder höher

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

In diesen Schritten wird detailliert erläutert, wie B2B-Bereitstellungen für Audio- und Videoanrufe über Expressway, integriert in CUCM, integriert werden, um Anrufe von anderen Unternehmen (Domänen) tätigen und empfangen zu können.

Expressway mit der Mobile Remote Access (MRA)-Funktion ermöglicht die nahtlose Registrierung von Jabber- und TC-Endgeräten außerhalb des Unternehmensnetzwerks, wie im Netzwerkdiagramm dargestellt.

Dieselbe Architektur bietet auch eine nahtlose Integration/Anrufe zwischen verschiedenen Unternehmen, d. h. Business-to-Business-Integration und diese für Audio, Video und IM&P. (B2B)

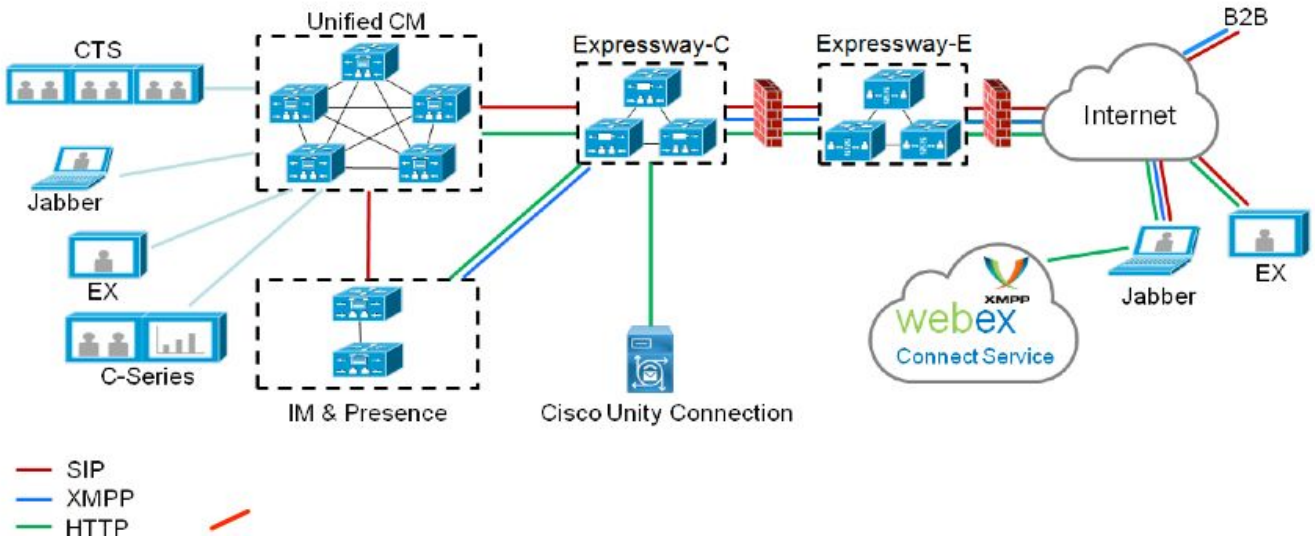
Dieses Dokument behandelt weder den IM&P-Teil noch die H.323-Integration.

Bevor Sie fortfahren können, müssen Sie sicherstellen, dass Sie den für Ihre Domäne relevanten DNS Service (SRV) erstellt haben, diese Datensätze werden von anderen Unternehmen verwendet, um den Speicherort Ihres Expressway zu finden.

Konfigurieren

Netzwerkdiagramm

Dieses Bild enthält ein Beispiel für ein Netzwerkdiagramm.



Schritt 1: SIP-Trunk zwischen CUCM und Expressway-C

Nachdem die CUCM-Erkennung durch Expressway-C durchgeführt wurde, werden die benachbarten Zonen automatisch für jeden Knoten und jedes erkannte Transportprotokoll konfiguriert.

Wenn das CUCM-Cluster im gemischten Modus konfiguriert ist, gibt es eine Zone für Transmission Control Protocol (TCP) für ungesicherten Datenverkehr mit Zielport 5060 und eine Zone für TLS (Transport Layer Security) für sicheren Datenverkehr mit Zielport 5061. Diese Ports können nicht geändert werden.

Die beiden Zonen werden für alle Edge-Anrufe an und von den Edge-Endpunkten verwendet.

Eingehende Anrufe von den Edge-Endpunkten nehmen die Route dieser automatisch hinzugefügten Zonen ein und zielen daher auf TCP 5060 oder TLS 5061 auf CUCM ab.

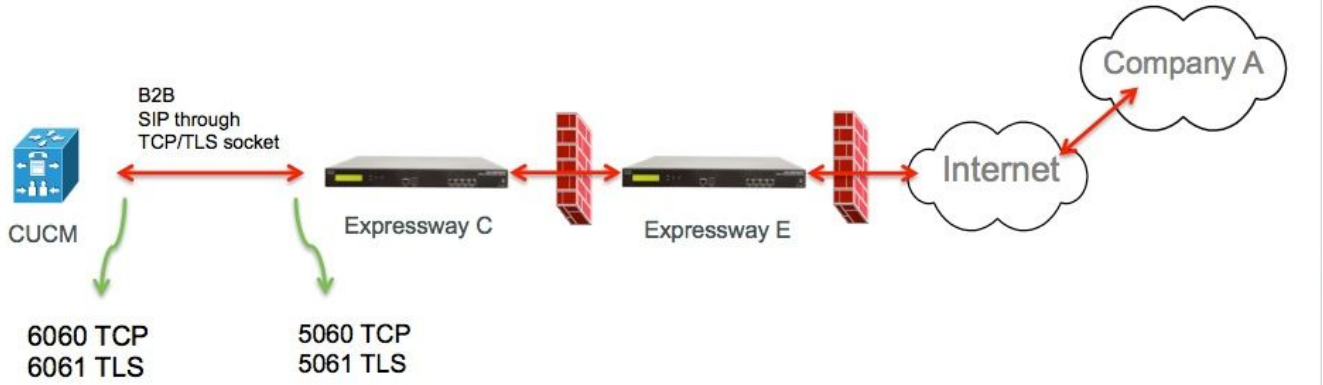
Über die etablierten Sockets Edge-Endpunkte können Anrufe registriert und getätigt/empfangen werden.

Konfigurieren Sie für B2B-Anrufe einen SIP-Trunk in CUCM, der auf Expressway-C zeigt, wobei der CUCM-Verkehr von diesem Gateway aus in der Regel auf Port 5060 oder 5061 überwacht.

Da Edge-Datenverkehr von derselben Quell-IP mit Port 5060/5061 stammt, müssen Sie für diesen Trunk in CUCM einen anderen Überwachungsport verwenden. Andernfalls wird Edge-Datenverkehr zum SIP-Trunk-Gerät im CUCM und nicht zum Endgerät (CSF oder EX) geroutet.

Für Expressway-C-seitige Verwendung der Ports 5060 und 5061 für Session Initiation Protocol (SIP) TCP/TLS.

Ein Beispiel, in dem CUCM auf Port 6060/6061 eingehenden Datenverkehr auf diesem Trunk überwacht, wird im Bild angezeigt.



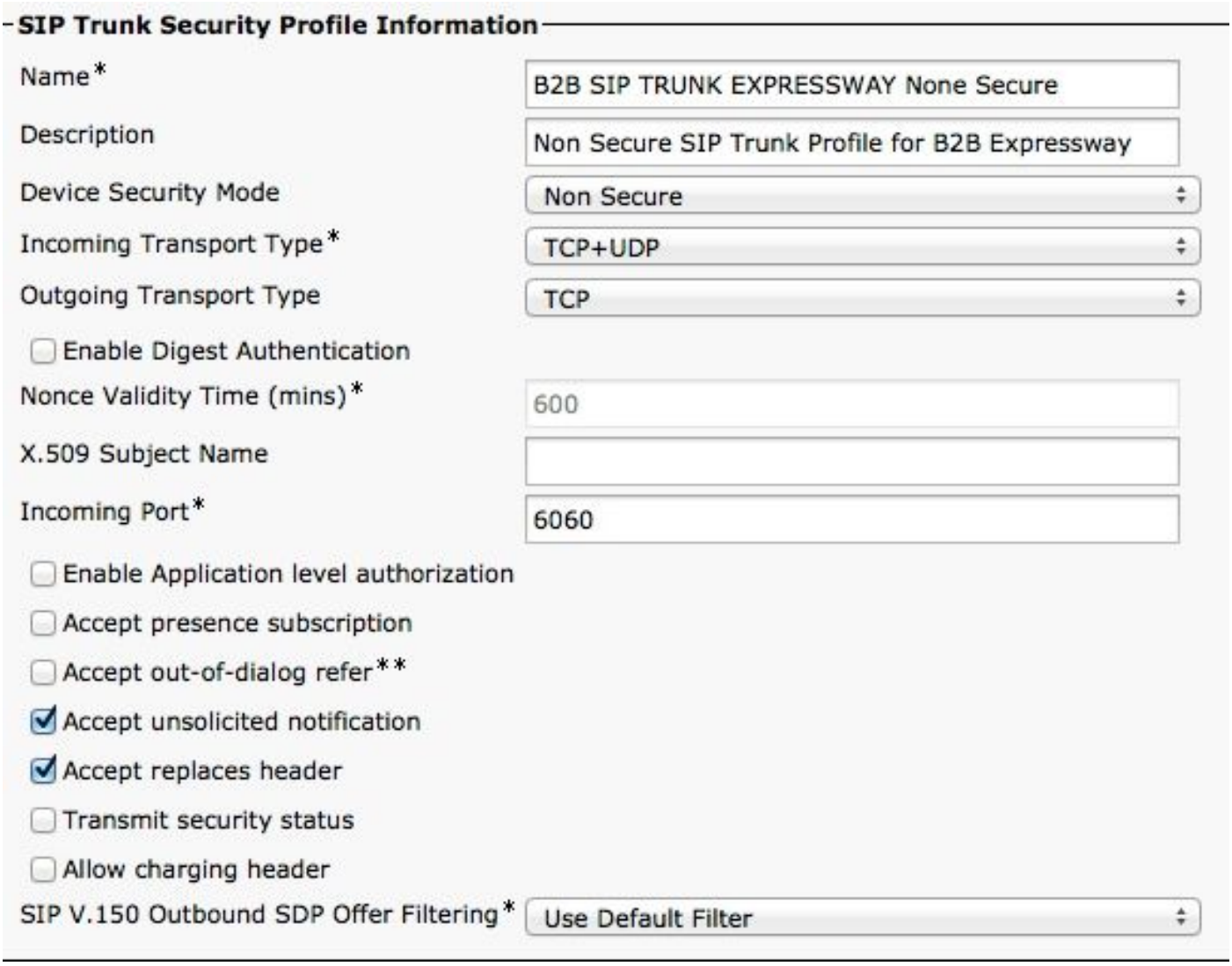
Dies sind die verschiedenen Konfigurationsschritte, die für diese Bereitstellung dokumentiert sind. Sowohl für sichere als auch für nicht sichere Bereitstellungen.

1a) Fügen Sie ein neues SIP-Trunk-Sicherheitsprofil hinzu.

Navigieren Sie auf der **CUCM-Verwaltungsseite** zu **> Device > Trunk.**

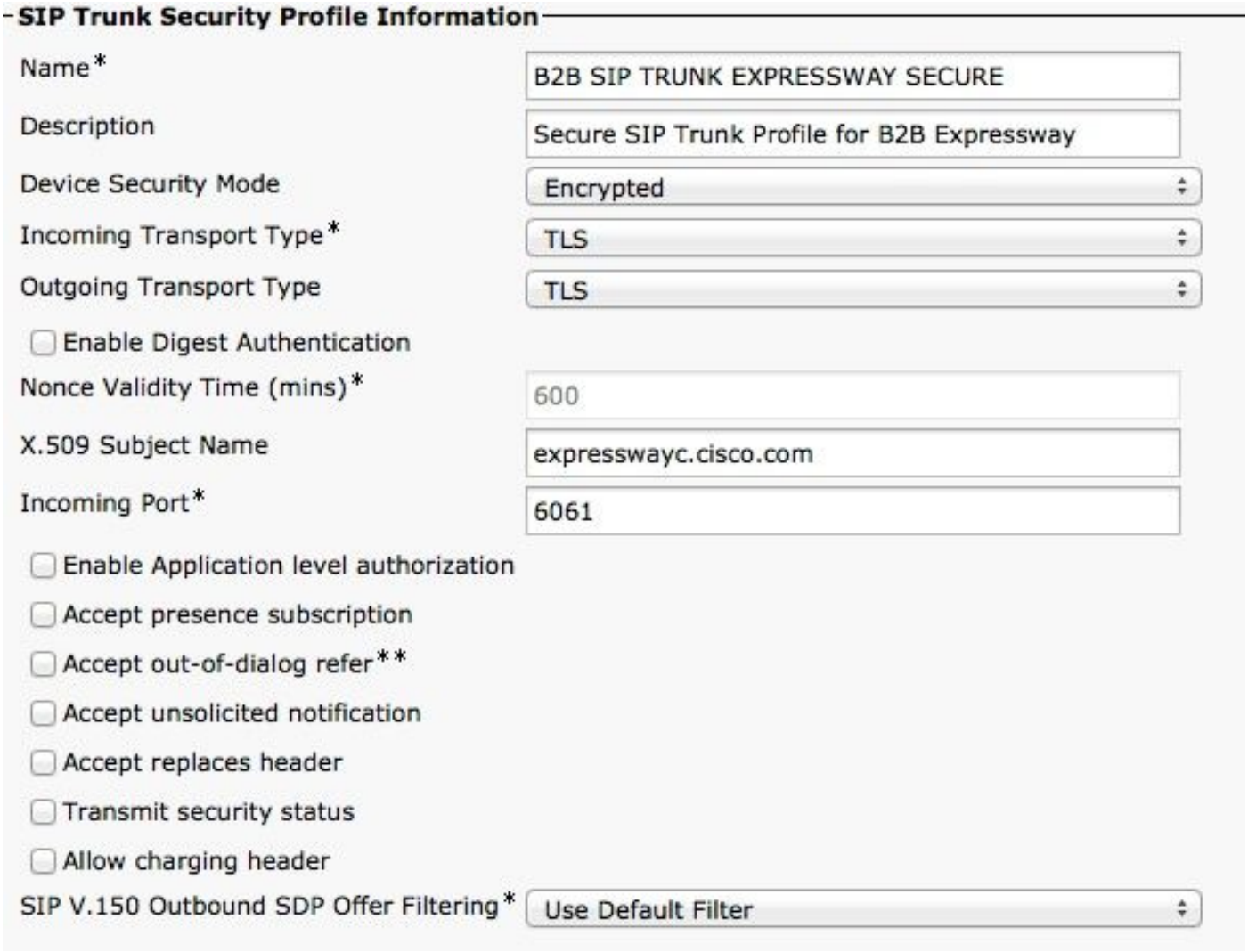
Konfigurieren Sie einen anderen eingehenden Port als 5060/5061, verwenden Sie hier 6060 für TCP und 6061 für TLS.

Nicht sicheres SIP-Trunk-Profil



Sicheres SIP-Trunk-Profil

Für TLS müssen Sie auch den X.509-Betreffnamen konfigurieren, der mit dem CN des Zertifikats übereinstimmt, das vom Expressway-c bereitgestellt wird. Zusätzlich laden Sie das Expressway-C- oder das CA-Zertifikat (das das Expressway-C Zertifikat ausgestellt hat) in den CUCM Certificate Trust Store hoch.



1b) Konfigurieren des SIP-Trunks auf dem CUCM

Über diesen Trunk werden alle B2B-Anrufe vom und zum CUCM weitergeleitet.

Die Konfigurationsparameter für SIP-Trunks sind standardmäßig für CUCM mit VCS-Bereitstellungen vorgesehen.

Stellen Sie sicher, dass das in Schritt 1 erstellte Sicherheitsprofil zugeordnet wird.

1c) Konfigurieren einer Nachbarzone auf Expressway-C

Für den CUCM muss auf Expressway-C eine Nachbarzone konfiguriert werden.

Diese Zone wird verwendet, um eingehenden B2B-Datenverkehr an CUCM weiterzuleiten.

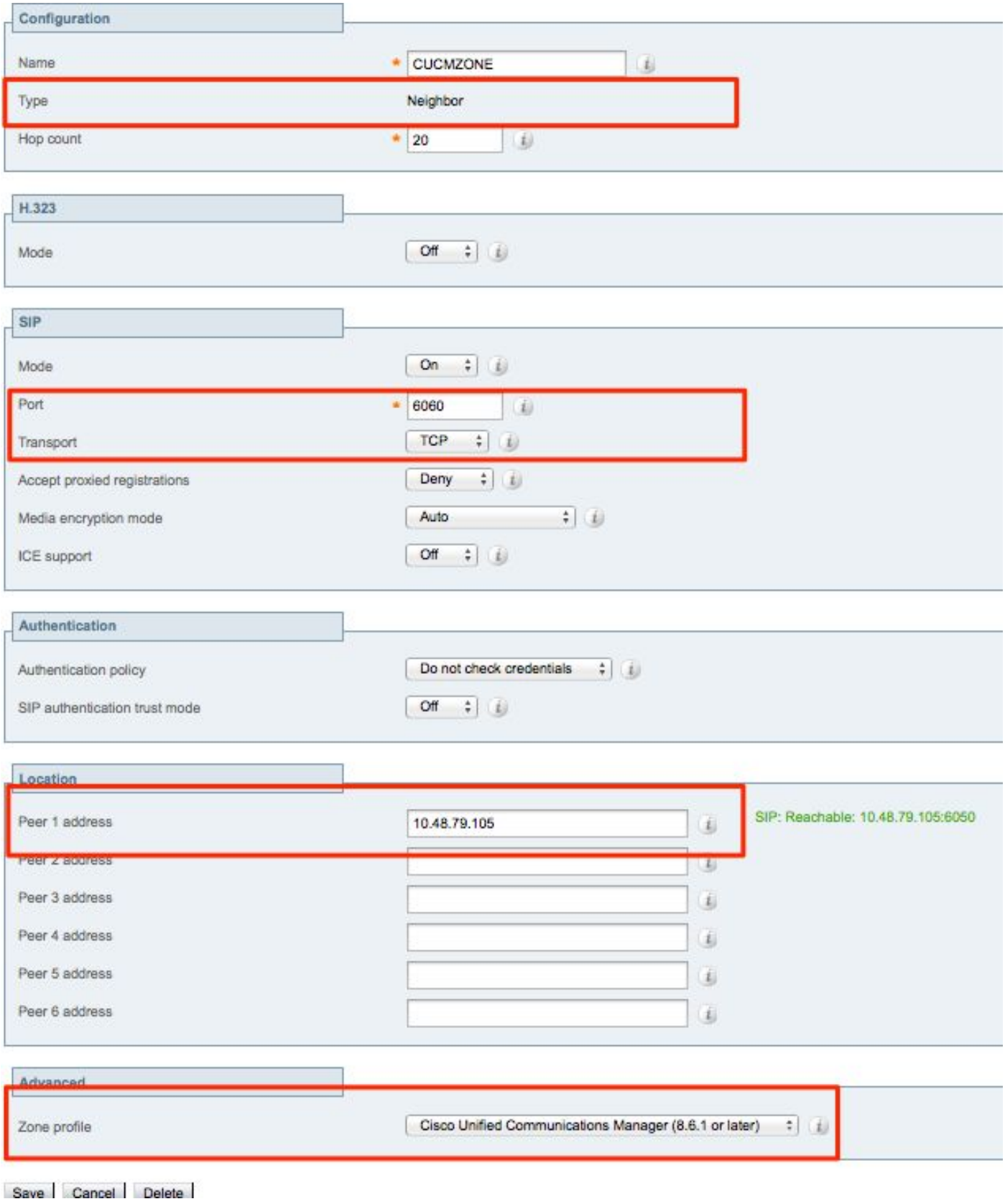
Die Konfiguration ist standardmäßig, jedoch muss sichergestellt werden, dass der Zielport dem Überwachungsport entspricht, der im SIP-Trunk-Sicherheitsprofil konfiguriert wurde, das dem SIP-

Trunk auf dem CUCM zugewiesen wurde.

In diesem Beispiel wird der Zielport 6060 für SIP/TCP und 6061 für SIP/TLS verwendet. (siehe Schritt 1), wie im Bild gezeigt

Navigieren Sie auf der Seite Expressway Administration (Expressway-Administration) zu **Konfiguration > Wählplan > Konfiguration ändern**

Nachbarzone für SIP TCP:

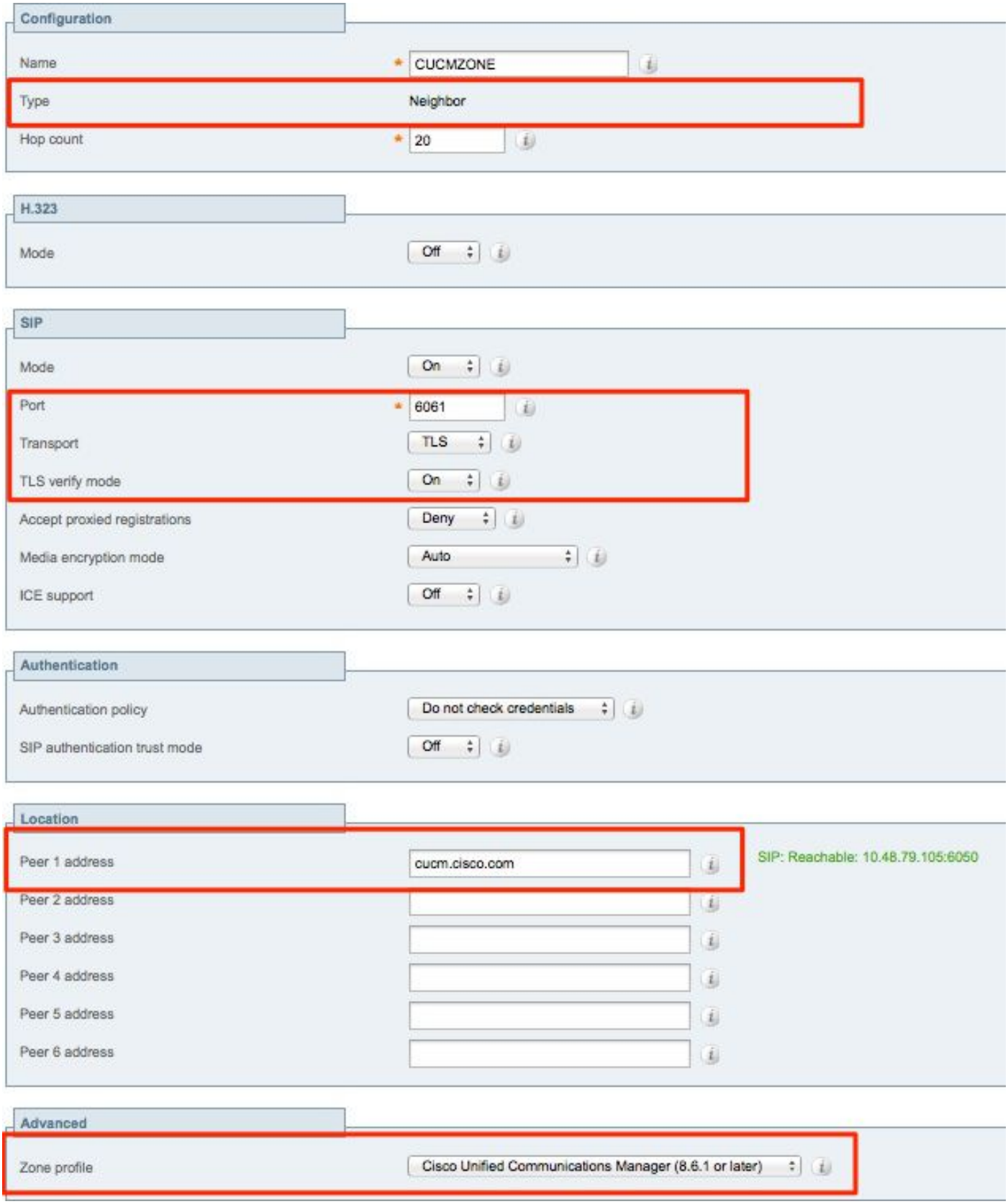


Nachbarzone für SIP TLS - mit TLS-Verifizierungsmodus aktiviert

Wenn der TLS-Überprüfungsmodus auf "On" (Ein) festgelegt ist, müssen Sie sicherstellen, dass die **Peer-Adresse** mit dem CN oder SAN aus dem vom CUCM vorgelegten Zertifikat übereinstimmt. In der Regel wird der FQDN des CUCM-Knotens im TLS-Überprüfungsmodus für die Peer-Adresse konfiguriert.

Navigieren Sie auf der Seite "Expressway Administration" zu **Configuration > Dial Plan >**

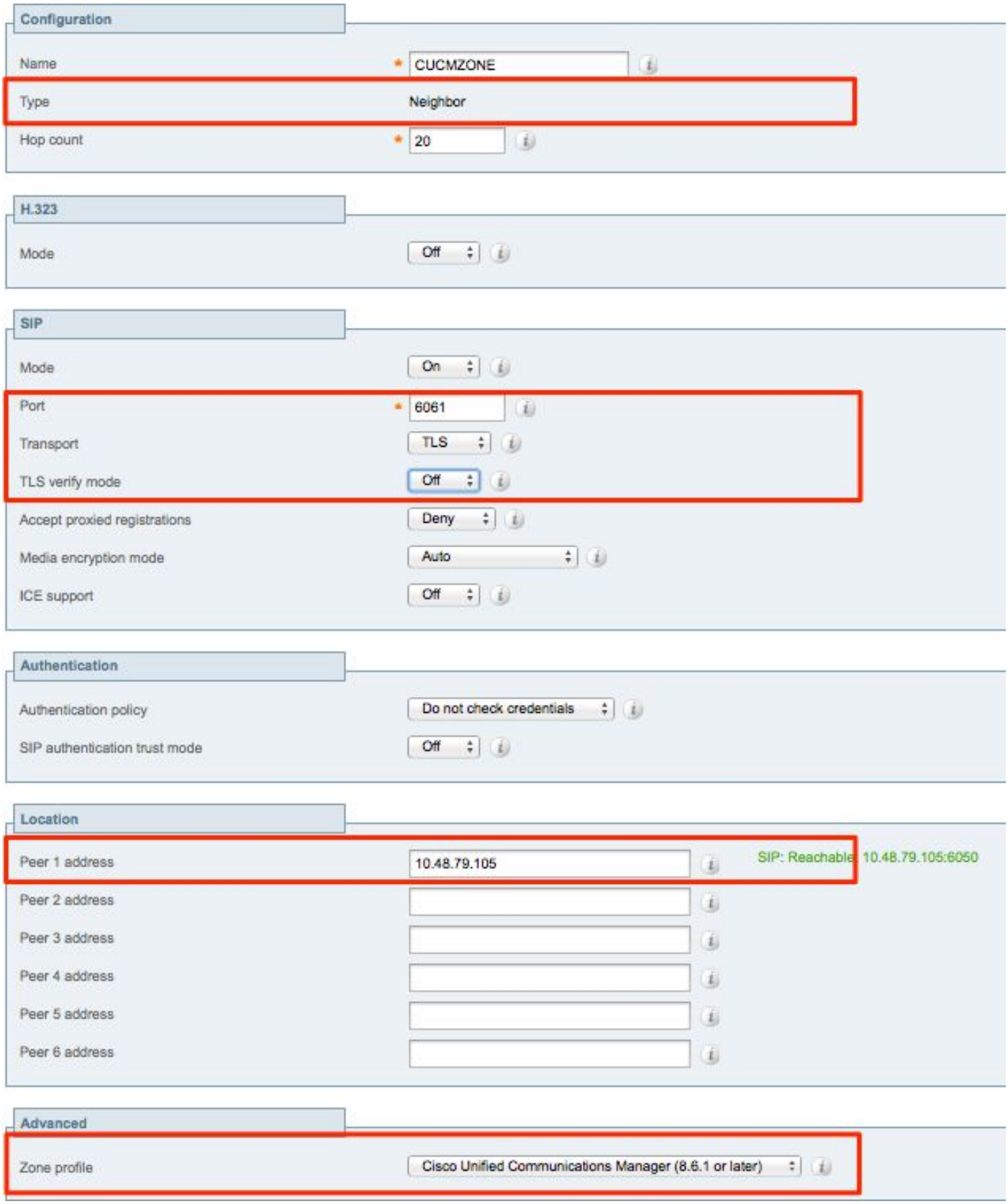
Transforms y Configuration.



Nachbarzone für SIP TLS - mit TLS-Verifizierungs-Modus aus

Wenn der TLS-Verifizierungsmodus auf die Peer-Adresse festgelegt ist, kann es sich entweder um die IP-Adresse, den Hostnamen oder den Fully Qualified Domain Name (FQDN) des CUCM-Knotens handeln.

Navigieren Sie auf der Seite Expressway Administration (Expressway-Administration) zu **Konfiguration > Wählplan > Konfiguration ändern**



1d. Zertifikate überprüfen

Für TLS müssen Sie Folgendes sicherstellen:

- Expressway-C-Serverzertifikat oder CA-Root (zum Signieren des Zertifikats) wird in den CUCMTrust-Speicher auf allen Servern im CUCM-Cluster hochgeladen.

- Das Callmanager-Zertifikat oder der CA-Root (zum Signieren des Zertifikats) wird auf dem Expressway-C-Server in die Liste der vertrauenswürdigen Zertifizierungsstellen hochgeladen.

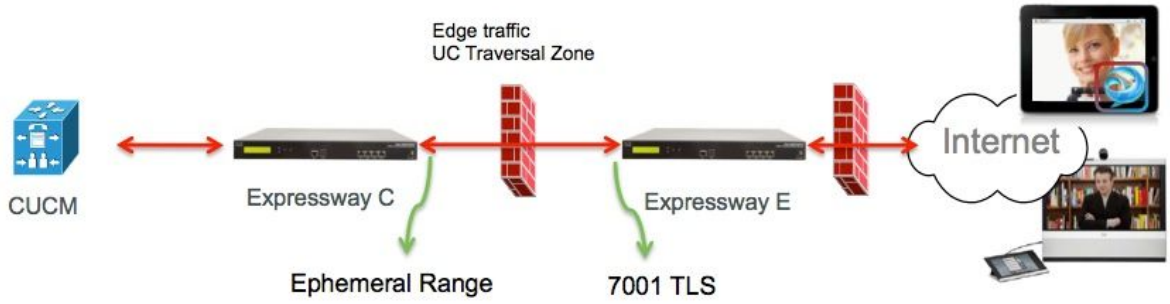
Schritt 2: Konfiguration der Traversal Zone zwischen Expressway-C und Expressway-E

Für die Weiterleitung des B2B-Datenverkehrs zwischen Expressway-C und Expressway-E muss eine separate Traversal Zone konfiguriert werden.

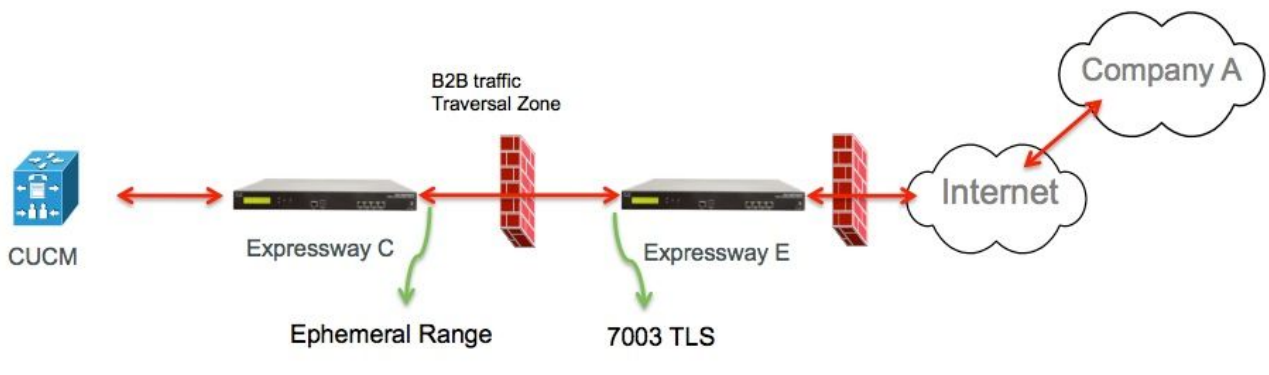
Dies ist eine standardmäßige Konfiguration der Traversal-Zone, aber ähnlich wie bei dem SIP-Trunk auf dem CUCM muss ein anderer Port als der Port konfiguriert werden, der von der UC Traversal-Zone für Edge-Datenverkehr verwendet wird.

Der Standardport für die UC Traversal-Zone ist 7001. Für die B2B-Traversal-Zone können Sie z.B. 7003 konfigurieren.

UC Traversal Zone für Edge-Datenverkehr, wie im Bild gezeigt



Traversal Zone für B2B-Datenverkehr, wie im Bild gezeigt

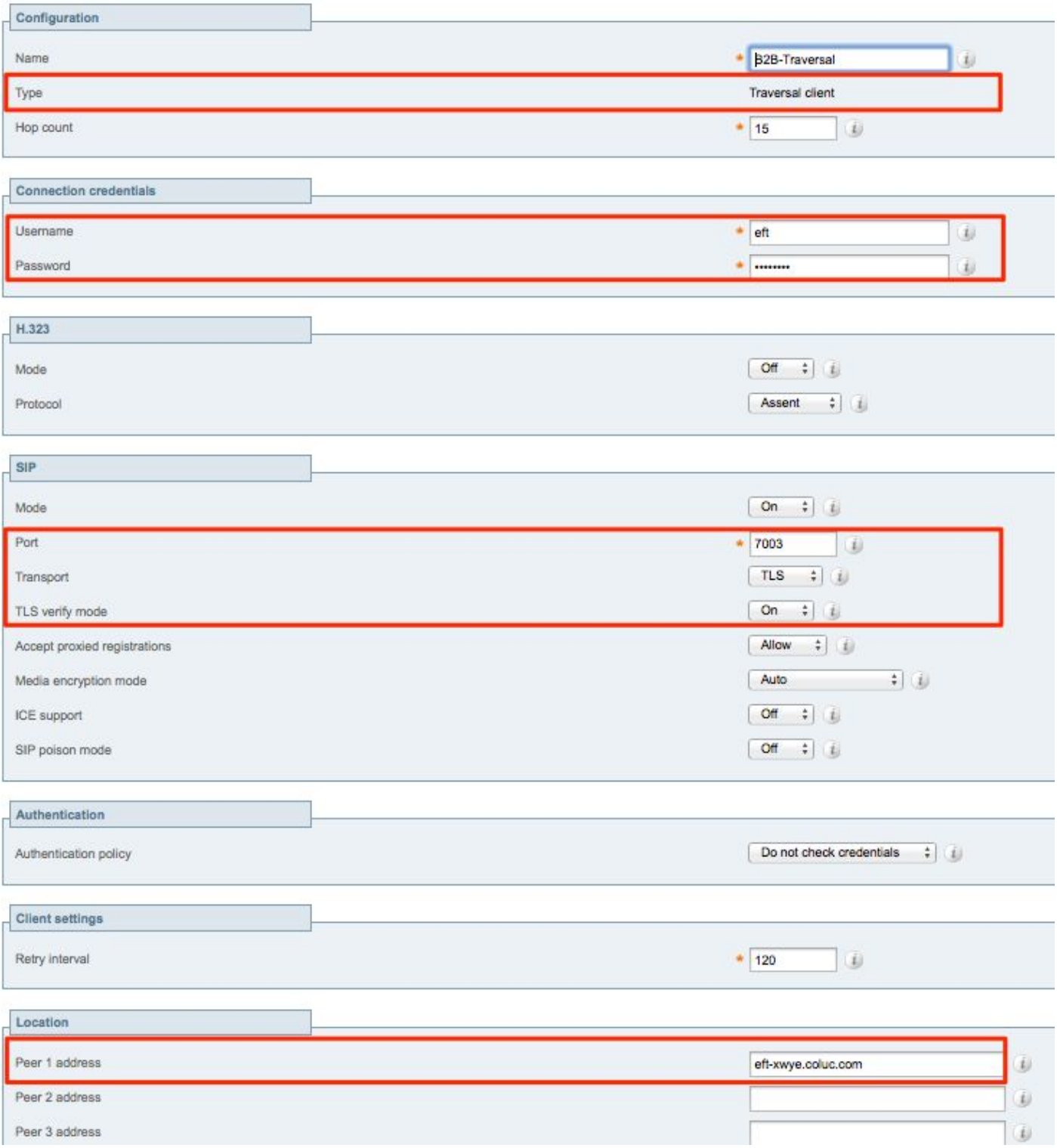


2a) Konfiguration der Traversal-Zone für B2B-Datenverkehr auf Expressway-C

Expressway-C ist der Traversal-Zone-Client, in diesem Beispiel ist der Zielport 7003.

Der TLS-Verifizierungsmodus ist auf On (Ein) gesetzt, um sicherzustellen, dass die konfigurierte **Peer-Adresse** mit dem CN oder SAN des angegebenen Zertifikats von Expressway-E übereinstimmt.

Navigieren Sie auf der Seite "Expressway Administration" zu **Configuration > Dial Plan > Transforms y Configuration.**

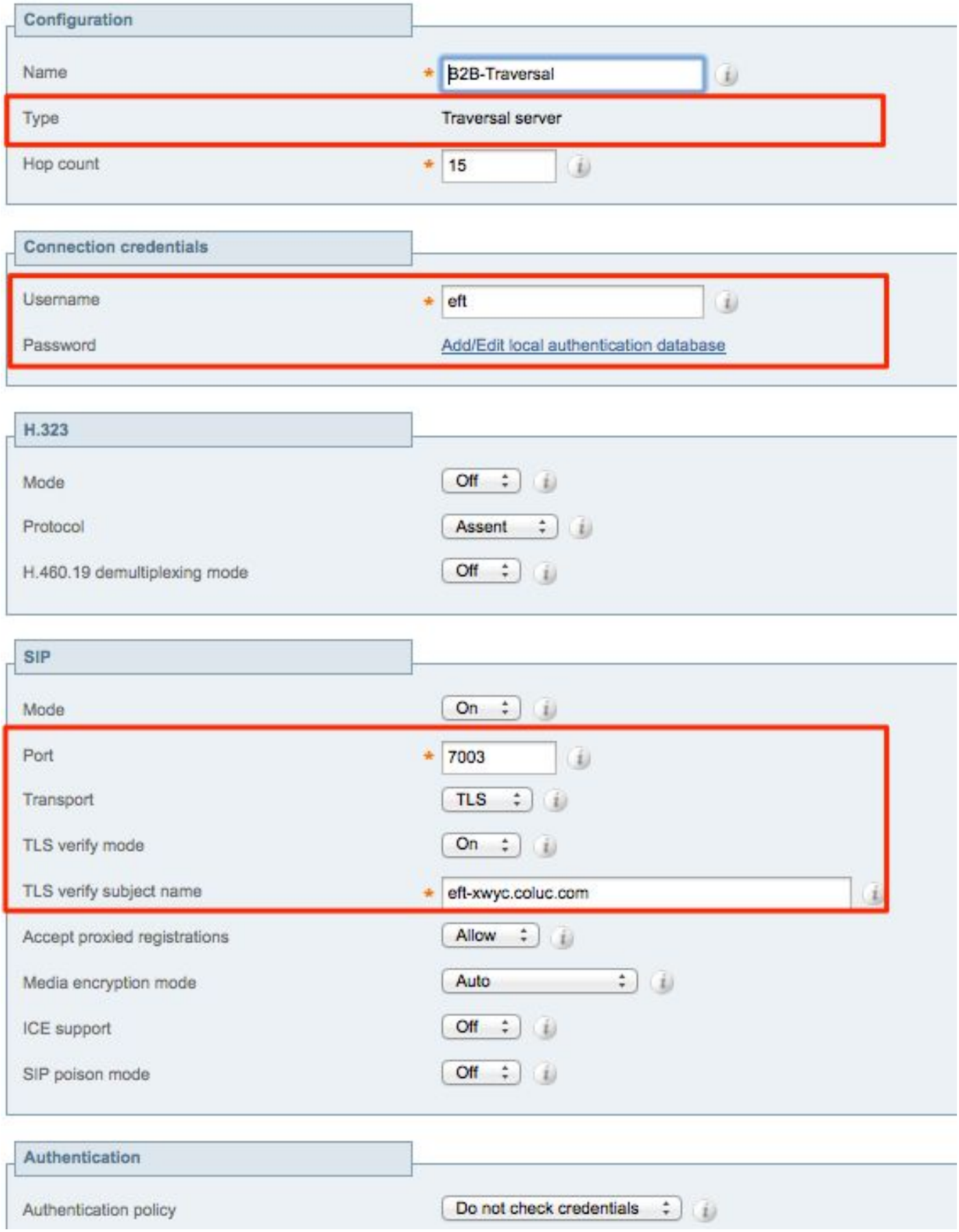


2b) Konfiguration der Traversal-Zone für B2B-Datenverkehr auf Expressway-E

Expressway-E ist der Traversal-Zone-Server, in diesem Beispiel ist der Überwachungsport 7003.

Der TLS-Verifizierungsmodus ist auf On (Ein) gesetzt, um sicherzustellen, dass der konfigurierte **Betreffname** dem CN oder SAN des von Expressway-C präsentierten Zertifikats entspricht.

Navigieren Sie auf der Seite "Expressway Administration" zu **Configuration > Dial Plan > Transforms y Configuration.**



Schritt 3: Konfigurieren der DNS-Zone für Expressway-E

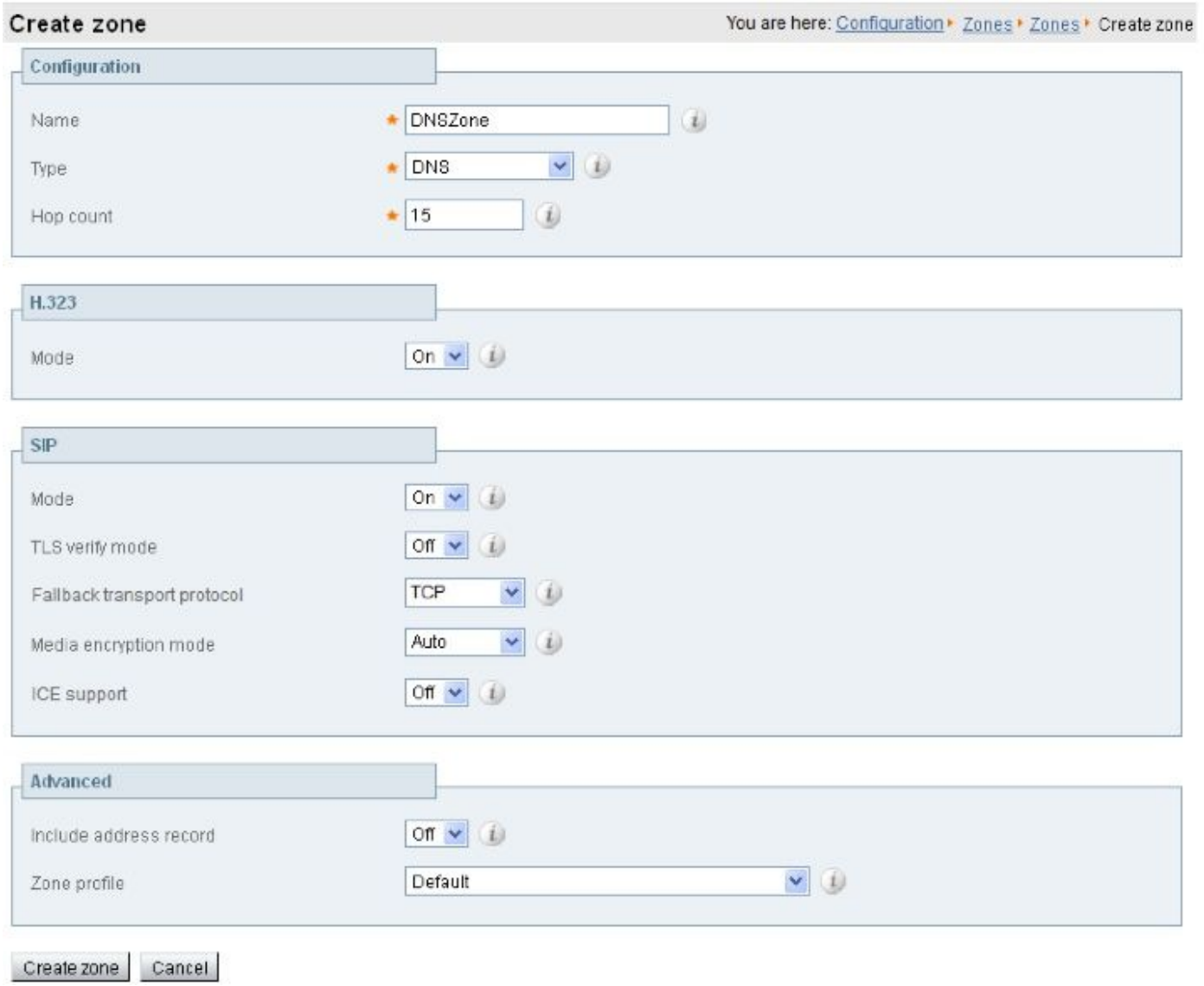
Um den B2B-Datenverkehr zu routen, konfigurieren Sie eine DNS-Zone auf Expressway-E.

Expressway-E führt für Datenverkehr, der für diese Zone bestimmt ist, eine DNS-SRV-Suche nach _sip oder _sips durch, und zwar für die Domäne, die vom Domänen-Teil der SIP-URI abgeleitet ist.

Das SRV-Ziel, das vom DNS-Server zurückgegeben wird, an den der SIP-Anruf weitergeleitet wird.

Die Konfiguration ist eine Standard-DNS-Zonenkonfiguration.

Navigieren Sie auf der Expressway Administration-Seite zu **Configuration > Zones (Konfiguration > Zonen).**



Schritt 4: Wählplan konfigurieren

4a.Transformation und/oder Suchregeln auf Expressway-C und E

Navigieren Sie auf der Seite Expressway Administration (Expressway-Administration) zu **Konfiguration > Wählplan > Umwandeln in Konfiguration > Wählplan > Umwandeln oder Suchregeln**

Weitere Informationen finden Sie in den VCS Deployment Guides (Control with Expressway), Kapitel "Routing Configuration:

http://www.cisco.com/c/en/us/support/unified-communications/telepresence-video-communication-server-vcs/products-installation-and-configuration-guides-list.html

4b) SIP-Routenmuster in CUCM

Weitere Informationen finden Sie im CUCM-System- und Administrationsleitfaden (Leitfaden zur Bereitstellung eines Nummernplans).

http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html

4c. Für die SIP-Anrufweiterleitung müssen SRV-Datensätze auf den öffentlichen DNS-Servern erstellt werden.

Wie im Bild gezeigt, werden die erforderlichen SRV-Datensätze sowie H323 B2B-Anrufe aufgeführt, die in diesem Dokument nicht behandelt wurden. Beachten Sie außerdem, dass SIP UDP auf Expressway standardmäßig deaktiviert ist.

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.

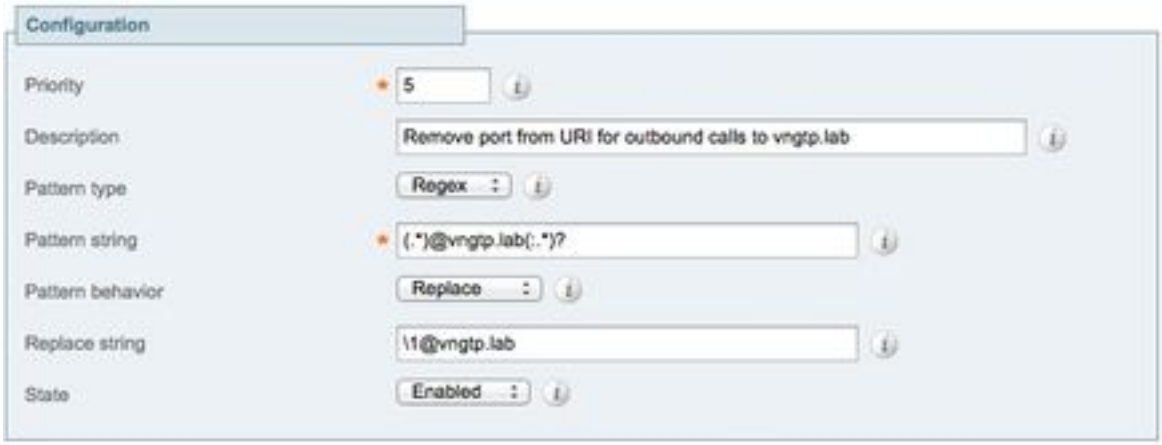
4d. Konfigurieren Sie den vollständig qualifizierten Domänennamen des Clusters in CUCM.

Sie können mehrere Einträge durch Kommas voneinander getrennt eingeben.

(4e) Erstellen Sie eine Transformation auf Expressway-C, die den Port aus dem URI entfernt, der in der Einladung vom CUCM empfangen wurde.

Weitere Informationen finden Sie in diesem Dokument:
http://www.cisco.com/c/en/us/support/docs/unified-communications/telepresence-video-communication-server-vcs/116729-trouble-cucm-dns-vcs-01.html

Navigieren Sie auf der Seite "Expressway Administration" zu **Configuration > Dial Plan > Transform y Configuration > Dial Plan > Transform**



Das SRND enthält außerdem ein umfangreiches Kapitel zum Wählplan.

http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-implementation-design-guides-list.html

Schritt 5: Rich Media-Lizenzen auf Expressway hochladen

Rich Media-Lizenzen (auch Traversal Zone-Lizenzen genannt) müssen auf jeden Expressway-Server hochgeladen werden.

Falls diese verpasst wurden oder aufgrund von nicht ordnungsgemäßen Konfigurationsanrufen weitergeleitet werden, erhalten Sie folgende Fehlermeldung: "Call license limit erreicht: Sie haben die Lizenzgrenze für Lizenzen für gleichzeitige Anrufe mit mehreren Benutzern erreicht."

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- Cisco TelePresence Video Communication Server (VCS)