Configurar llamadas de audio y video interempresariales mediante Expressway integrado con CUCM

Contenido

Introducción

Este documento describe cómo integrar/configurar la implementación interempresarial (B2B) para las llamadas de audio y video mediante Expressway integrado con Cisco Unified Call Manager (CUCM).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Expressway-C (Exp-C)
- Expressway-E (Exp-E)
- Cisco Unified Call Manager (CUCM)
- Cisco Unity Connection (CUC)
- Servidor-C de comunicación por video (VCS-C) de TelePresence
- Teléfono Jabber
- Cisco TelePresence System (CTS)
- Teléfono EX
- Protocolo de inicio de sesión (SIP)
- HTTP (Hypertext Transfer Protocol)
- Protocolo extensible de mensajería y comunicación de presencia (XMPP)
- Cisco Unified IM and Presence (IM&P)
- Certificados

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Expressway C y E X8.1.1 o posterior
- Unified Communications Manager (CUCM) 10.0 o posterior

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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Estos pasos explican en detalle cómo integrar/configurar la implementación B2B de audio y videollamadas mediante Expressway integrado en CUCM para realizar y recibir llamadas de otras empresas (dominios).

Expressway con la función de acceso remoto móvil (MRA) proporciona un registro sin problemas de los terminales Jabber y TC ubicados fuera de la red empresarial, como se muestra en el diagrama de red.

La misma arquitectura también proporciona integración/llamadas fluidas entre diferentes empresas, también conocida como integración entre empresas, y esto para audio, vídeo e IM&P. (B2B)

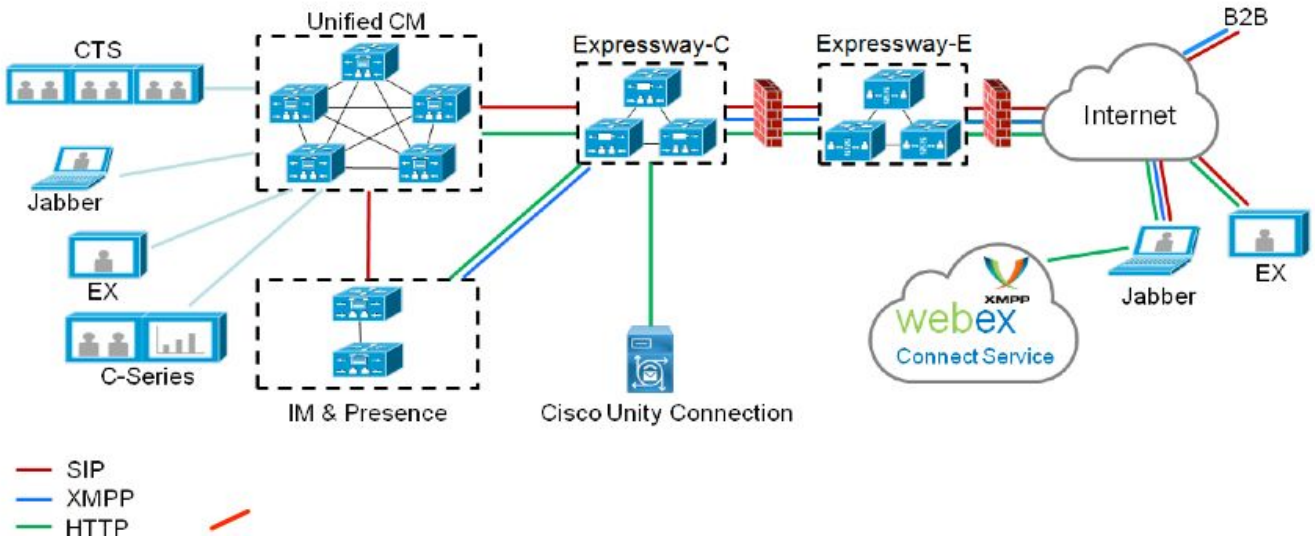
Este documento no cubre la parte correspondiente a IM&P ni la integración de H.323.

Antes de continuar, debe asegurarse de que se ha creado el servicio DNS (SRV) correspondiente para su dominio, otros fabricantes utilizan estos registros para buscar la ubicación de Expressway.

Configurar

Diagrama de la red

Esta imagen proporciona un ejemplo de un diagrama de red.



Paso 1. Enlace troncal SIP entre CUCM y Expressway-C

Después de que Expressway-C realiza la detección de CUCM, las zonas vecinas se configuran automáticamente para cada nodo y se detecta el protocolo de transporte.

Cuando el clúster de CUCM se configura en modo mixto, hay una zona para el protocolo de control de transmisión (TCP) para el tráfico no seguro con el puerto de destino 5060 y una zona para TLS (seguridad de la capa de transporte) para el tráfico seguro con el puerto de destino 5061. No se pueden cambiar estos puertos.

Las dos zonas se utilizan para todas las llamadas de borde hacia y desde los extremos de borde.

Las llamadas entrantes de los terminales perimetrales toman la ruta de estas zonas agregadas automáticamente y, por lo tanto, el TCP 5060 o la TLS 5061 en CUCM.

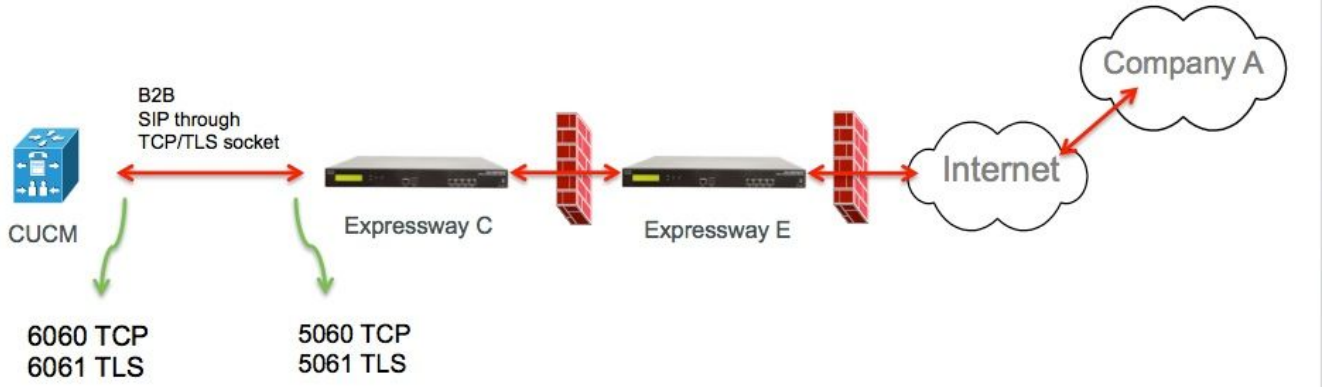
A través de los sockets establecidos, los terminales perimetrales registran y realizan/reciben llamadas.

Para las llamadas B2B, configure un troncal SIP en CUCM que apunte a Expressway-C, donde normalmente CUCM escucha el puerto 5060 o 5061 para el tráfico entrante de este gateway.

Dado que el tráfico perimetral proviene de la misma fuente IP con los puertos 5060/5061, debe utilizar un puerto de escucha distinto para el enlace troncal en CUCM. De lo contrario, el tráfico de borde se enruta al dispositivo troncal SIP en CUCM y no al dispositivo terminal (CSF o EX).

Por el lado de Expressway-C, use los puertos 5060 y 5061 para el TCP o la TLS del protocolo de inicio de sesión (SIP).

En la imagen se muestra un ejemplo donde CUCM escucha el puerto 6060/6061 para el tráfico entrante en este enlace troncal.



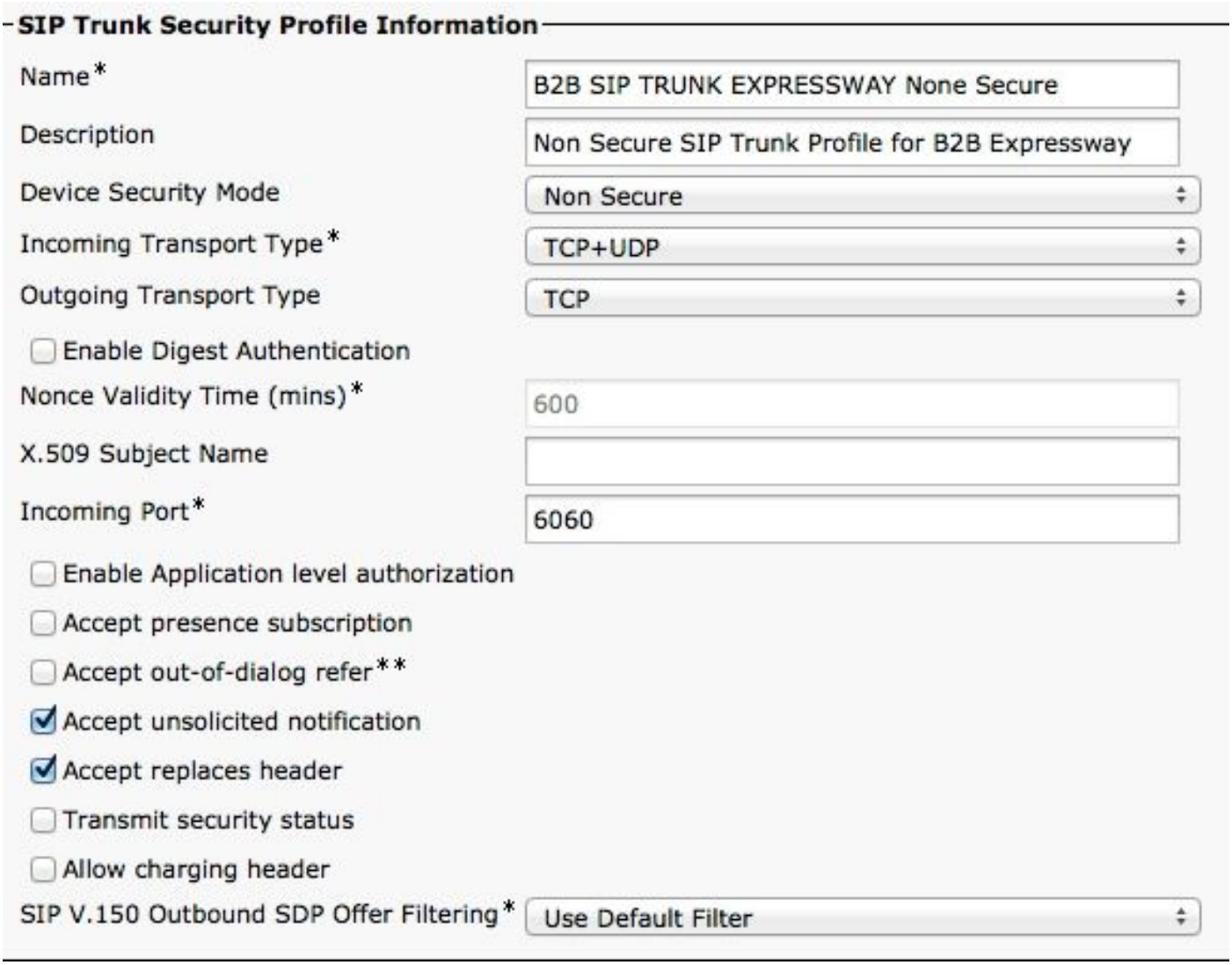
Estos son los diferentes pasos de configuración documentados para la implementación. Tanto para las implementaciones seguras como no seguras.

a. Agregue un nuevo perfil de seguridad de enlace troncal SIP

Desde la **página de administración de CUCM, navegue hasta > Dispositivo > Enlace troncal.**

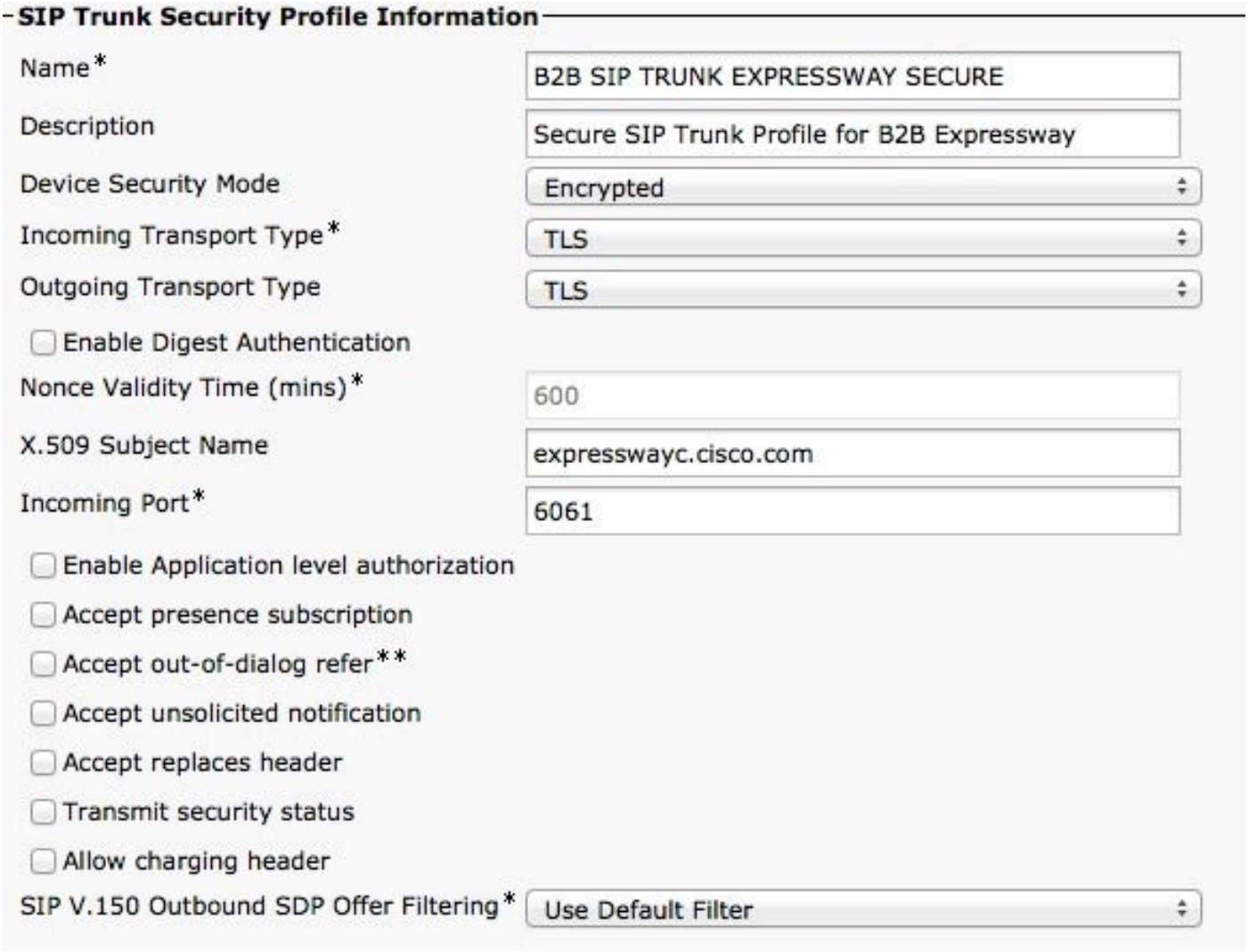
Configure un puerto de entrada diferente al 5060/5061, aquí use 6060 para TCP y 6061 para TLS

Perfil de enlace troncal SIP no seguro



Perfil de enlace troncal SIP seguro

Para la TLS además debe configurar el nombre de asunto X.509 que coincida con el CN del certificado presentado por Expressway-C. Además, cargue también el certificado de Expressway-C o CA (que emitió el certificado de Expressway-C) en el almacén de confianza de certificados de CUCM.



b. Configure el enlace troncal SIP en CUCM

A través de este enlace troncal, todas las llamadas B2B fluyen hacia y desde CUCM.

Los parámetros de configuración del enlace troncal SIP son estándar para CUCM con implementaciones de VCS.

Asegúrese de asociar el perfil de seguridad que se creó en el Paso 1.

c. Configure una zona de vecino en Expressway-C

Debe configurarse una zona de vecino en Expressway-C al destino de CUCM.

Esta zona se utiliza para enrutar el tráfico B2B entrante a CUCM.

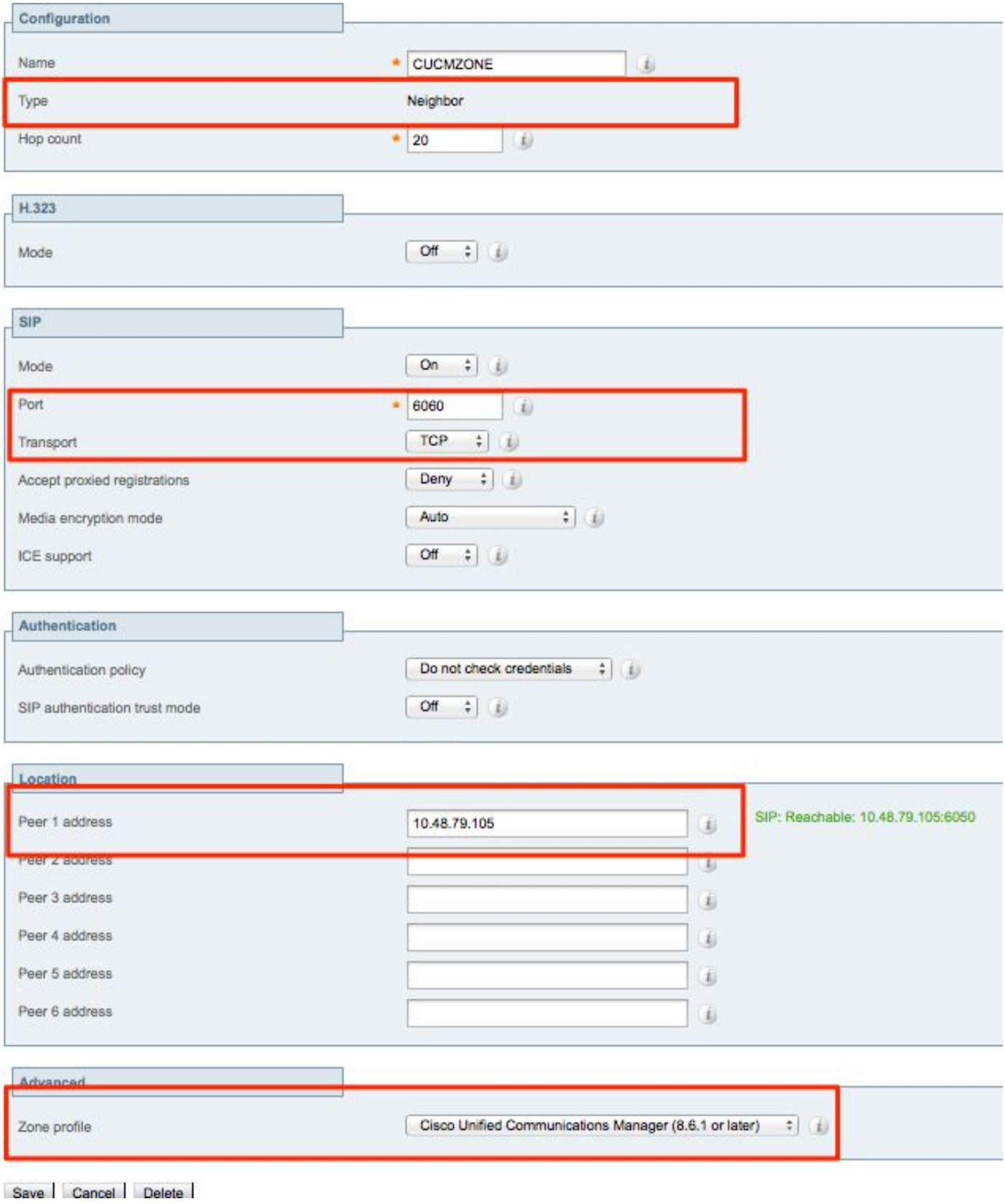
La configuración es estándar, excepto que debe asegurarse de configurar el puerto de destino correspondiente al puerto de escucha configurado en el perfil de seguridad del enlace troncal SIP

asignado al enlace troncal SIP en CUCM.

En este ejemplo, el puerto de destino utilizado es 6060 para SIP/TCP y 6061 para SIP/TLS. (Consulte el Paso 1, como se muestra en la imagen).

En la página Administración de Expressway, vaya a **Configuración > Plan de marcación > Transformación y configuración**

Zona de vecino para el TCP del SIP

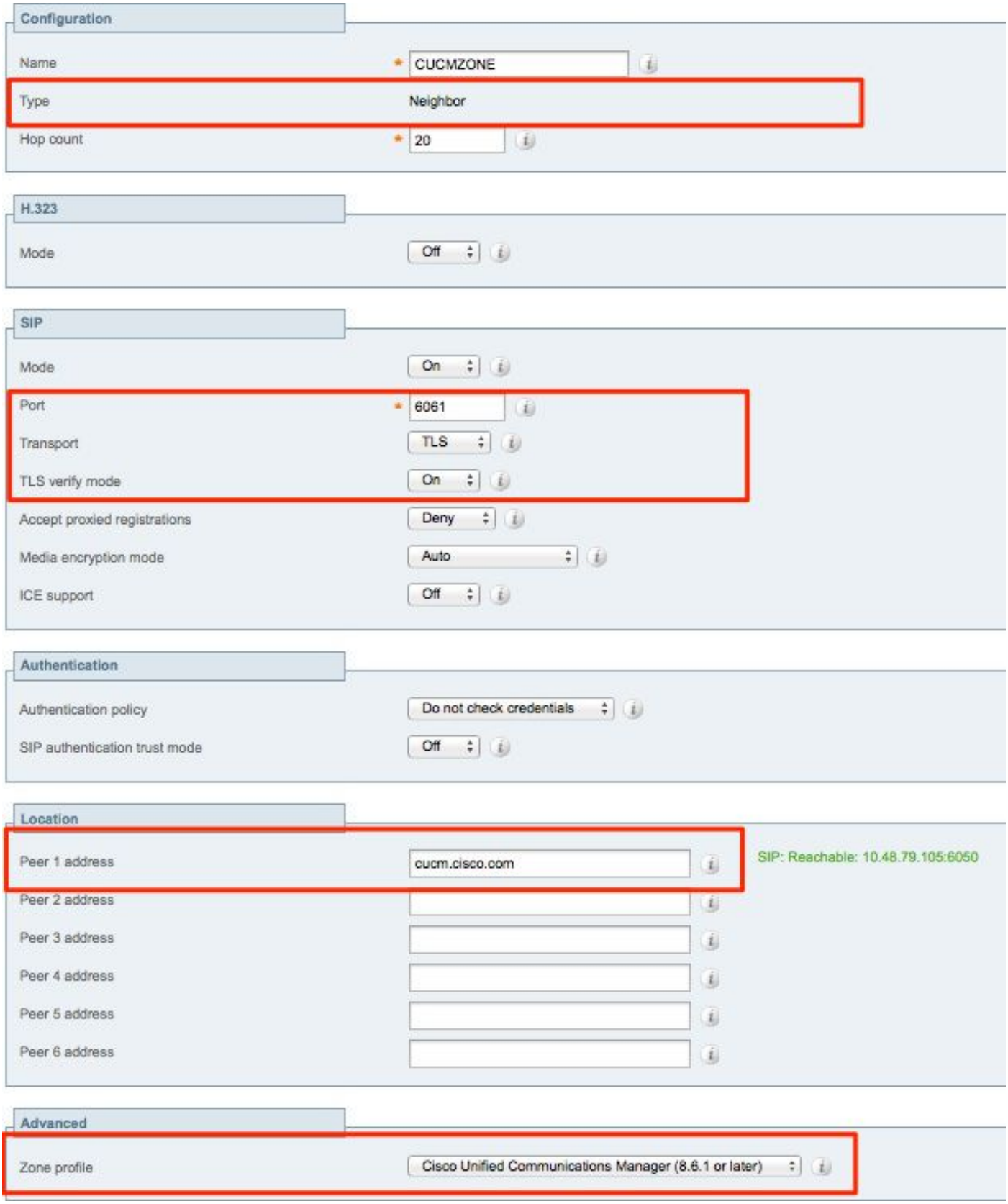


Zona de vecino para la TLS del SIP con modo de verificación de TLS activado

Con el modo de verificación de TLS activado, debe asegurarse de que la **dirección homóloga coincida con el CN o SAN del certificado presentado por CUCM.** Normalmente, con el modo de verificación de TLS se configura el nombre de dominio completo (FQDN) del nodo CUCM para la dirección de peer.

En la página de administración de Expressway, vaya a **Configuración > Plan de marcación >**

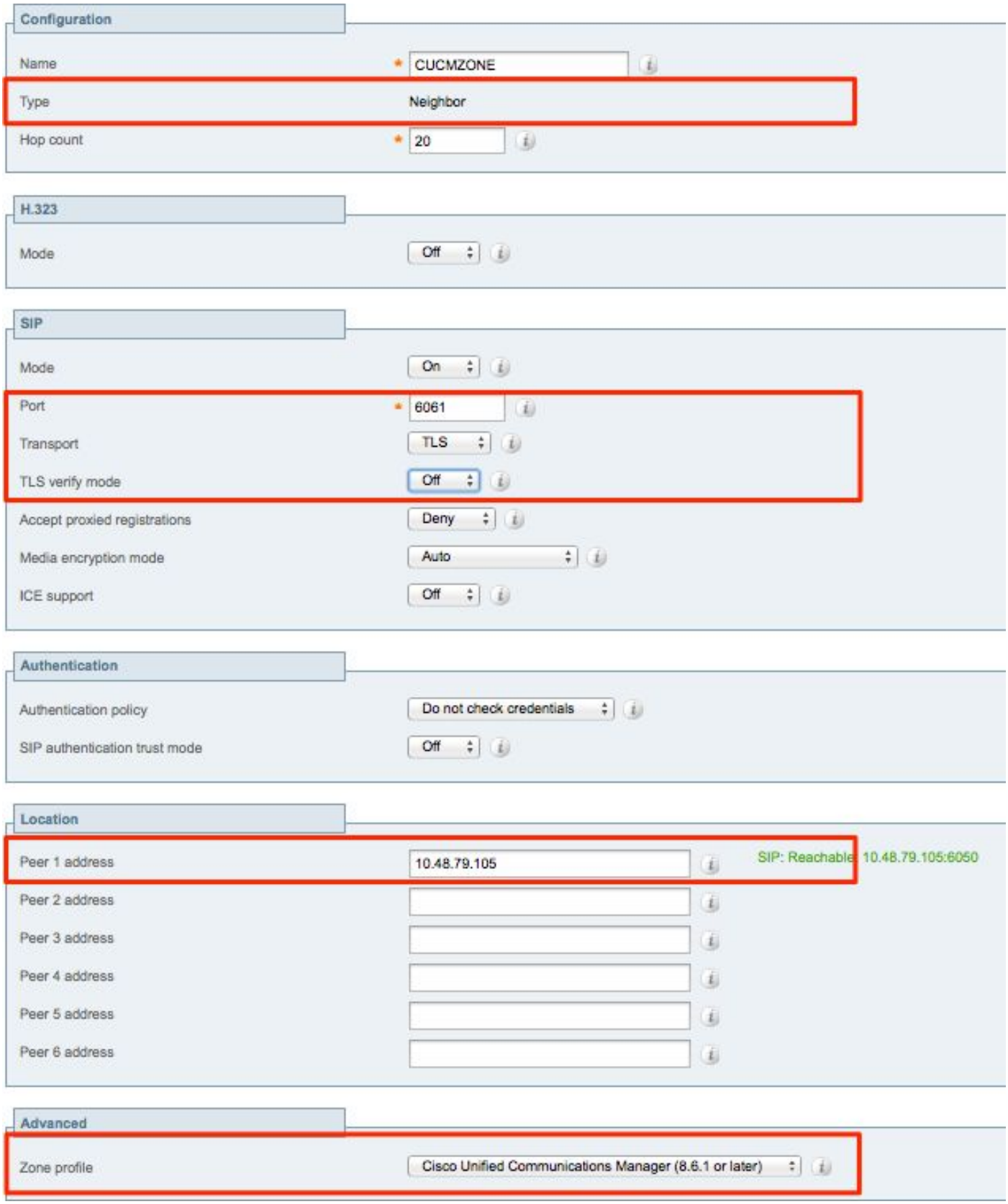
Transformación y configuración



Zona de vecino para la TLS del SIP con modo de verificación de TLS desactivado

Cuando el modo de verificación de TLS se establece en off, la dirección de peer puede ser la dirección IP, el nombre de host o FQDN del nodo CUCM.

En la página Administración de Expressway, vaya a **Configuración > Plan de marcación > Transformación y configuración**



d. Verificación de certificaciones

Para la TLS, asegúrese de que:

- El certificado de servidor de Expressway-C o la raíz de CA (que se usó para firmar el certificado) se cargue en el almacén de confianza de CUCM en todos los servidores del clúster de CUCM.

- El certificado de CallManager o la raíz de CA (que se usó para firmar el certificado) se cargue en la lista de certificados de CA de confianza en el servidor de Expressway-C.

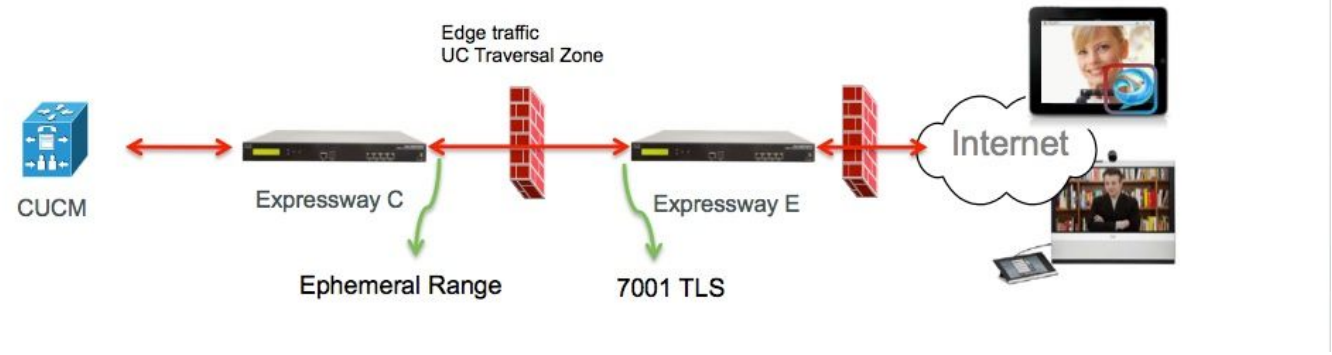
Paso 2. Configuración de la zona transversal entre Expressway-C y Expressway-E

Una zona transversal independiente debe configurarse para enrutar el tráfico B2B entre Expressway-C y Expressway-E.

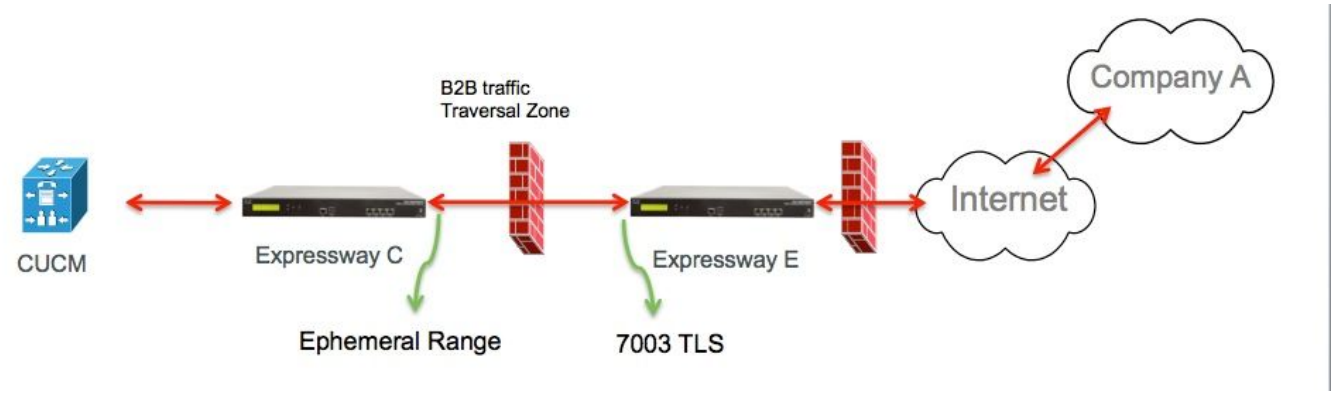
Se trata de una configuración de zona transversal estándar, que es similar al enlace troncal SIP de CUCM en un puerto diferente; luego debe configurarse el puerto que usa la zona transversal de UC para el tráfico perimetral de CUCM.

El puerto estándar de la zona transversal UC es 7001. Para la zona transversal B2B, puede, por ejemplo, configurar 7003.

Zona transversal UC para el tráfico perimetral, como se muestra en la imagen:



Zona transversal para el tráfico B2B, como se muestra en la imagen:

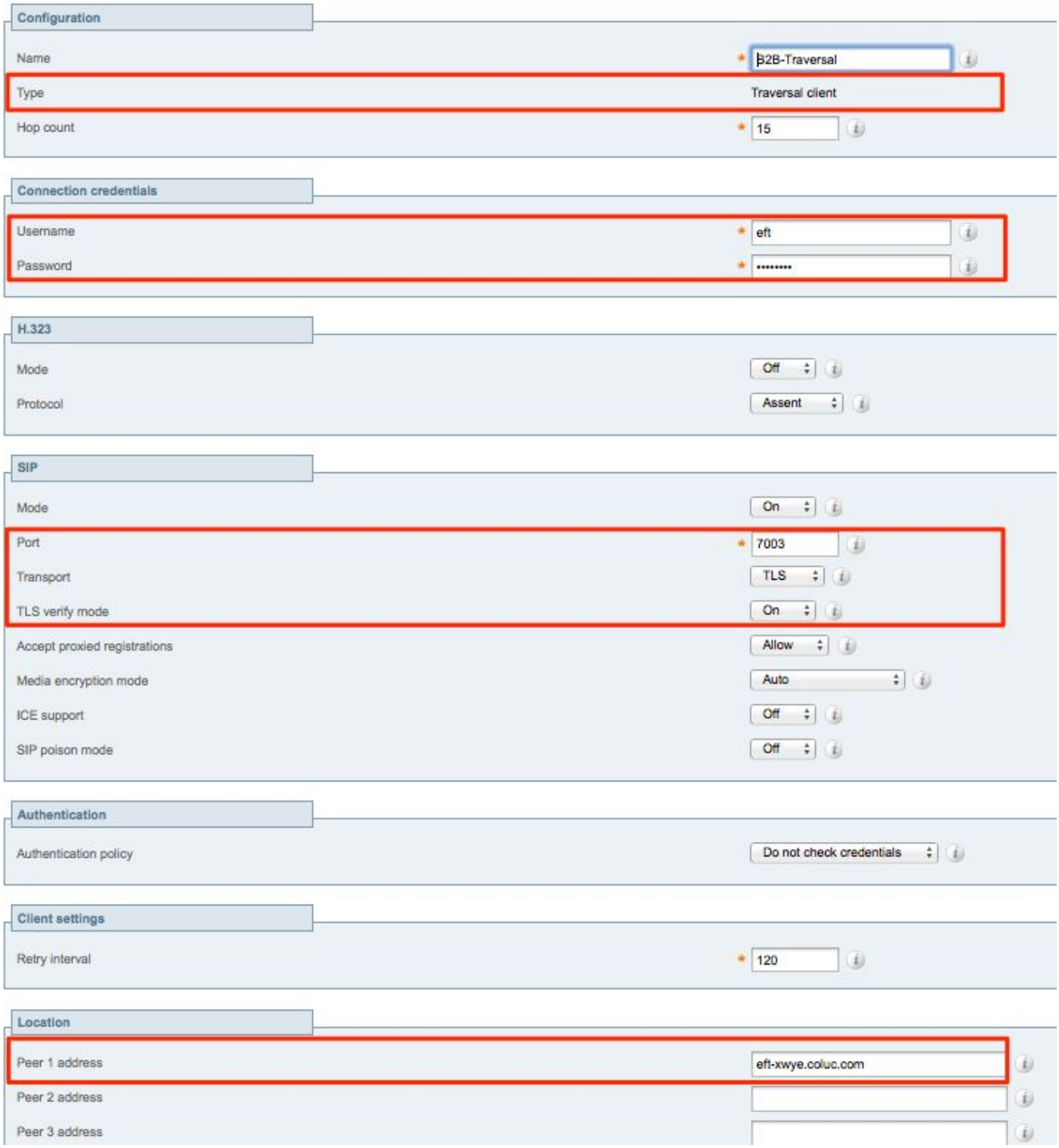


a. Configure la zona transversal para el tráfico B2B en Expressway-C

Expressway-C es el cliente de zona transversal, en este ejemplo, el puerto de destino es 7003

Con el modo de verificación de TLS activado, debe asegurarse de que la **dirección homóloga configurada coincida con el CN o SAN del certificado presentado por Expressway-E.**

En la página de administración de Expressway, vaya a **Configuración > Plan de marcación > Transformación y configuración**

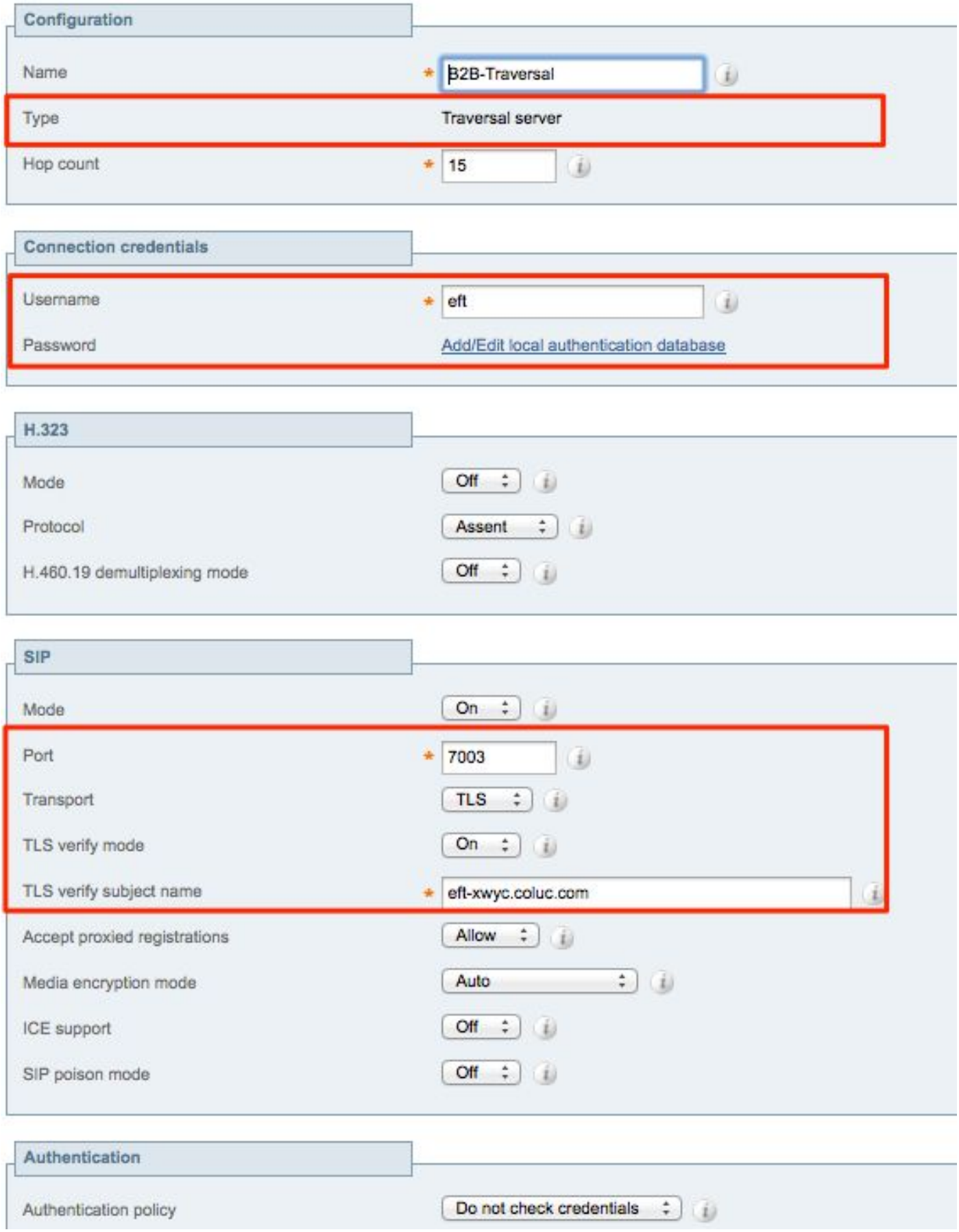


b. Configure la zona transversal para el tráfico B2B en Expressway-E

Expressway-E es el servidor de zona transversal, en este ejemplo, el puerto de escucha es 7003.

Con el modo de verificación de TLS activado, debe asegurarse de que el **nombre de asunto de verificación de la TLS configurado coincida con el CN o SAN del certificado presentado por Expressway-C.**

En la página de administración de Expressway, vaya a **Configuración > Plan de marcación > Transformación y configuración**



Paso 3. Configuración de la zona DNS en Expressway-E

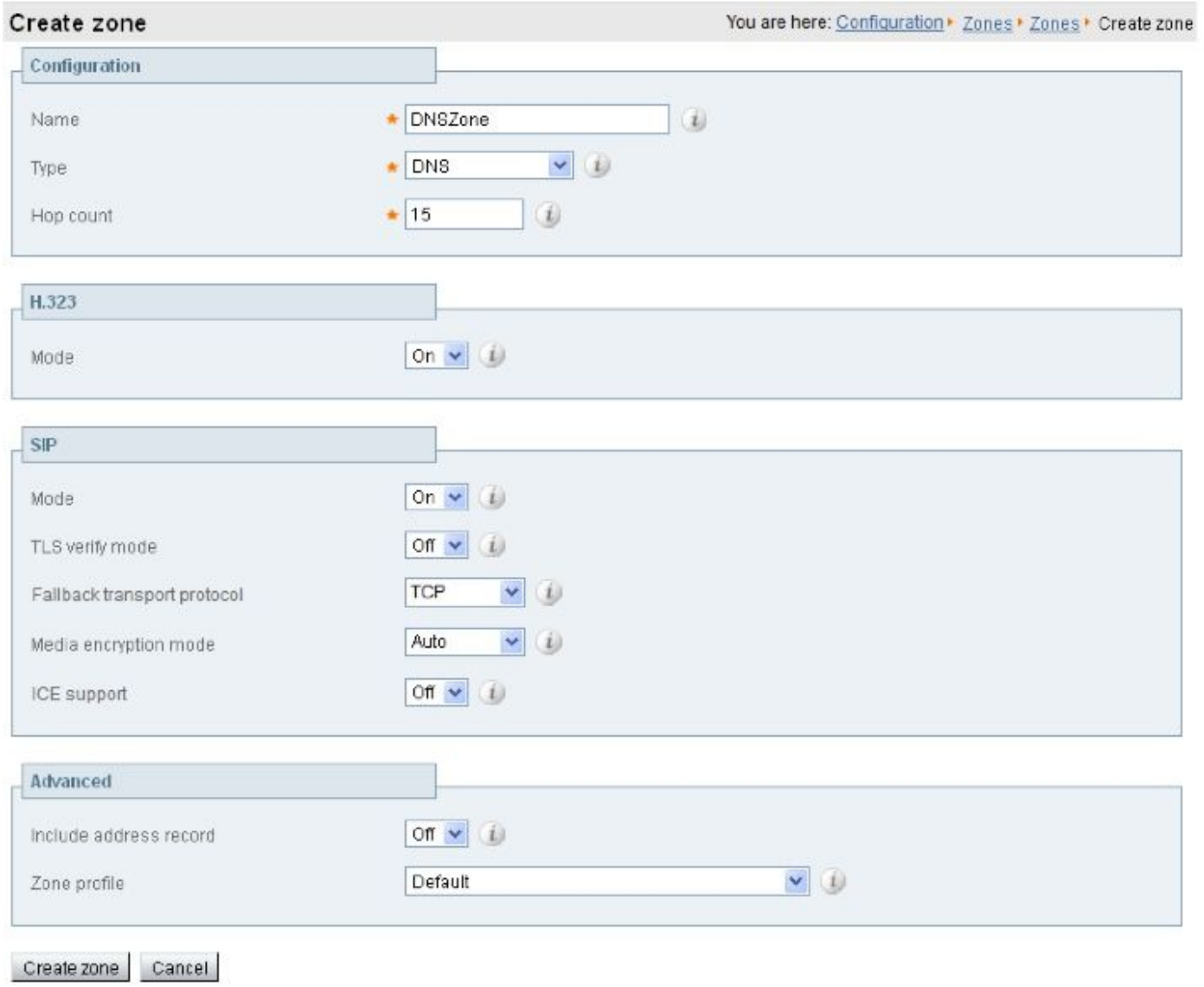
Para rutear, el tráfico B2B, configure una zona DNS en Expressway-E.

Expressway-E, para el tráfico destinado a esta zona, realiza una búsqueda DNS SRV para tanto _sip o _sips y esto para el dominio derivado de la parte de dominio del URI SIP.

El destino SRV devuelto por el servidor DNS se usa para enrutar la llamada al SIP.

La configuración es una configuración de zona DNS estándar.

Desde la página de administración de Expressway, vaya a **Configuración > Zonas**



Paso 4. Configurar plan de marcación

a. Reglas de transformación o búsqueda en Expressway-C y E

Desde la página de administración de Expressway, vaya a **Configuración > Plan de marcación > Transformación y configuración > Plan de marcación > Reglas de transformación o búsqueda**

Para obtener más información, consulte las guías de implementación de VCS (Control con Expressway), el capítulo sobre configuración de routing:

b. Patrones de enrutamiento del SIP en CUCM

Para obtener más información, consulte la guía de administración del sistema CUCM (Guía de implementación del plan de marcación):

c. Para el enrutamiento de llamadas del SIP, se deben crear registros SRV en los servidores DNS públicos.

Como se muestra en la imagen, enumera los registros SRV requeridos, así como las llamadas B2B H323 que no se han tratado en este documento. También tenga en cuenta que el UDP del SIP se desactivada de forma predeterminada en 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.

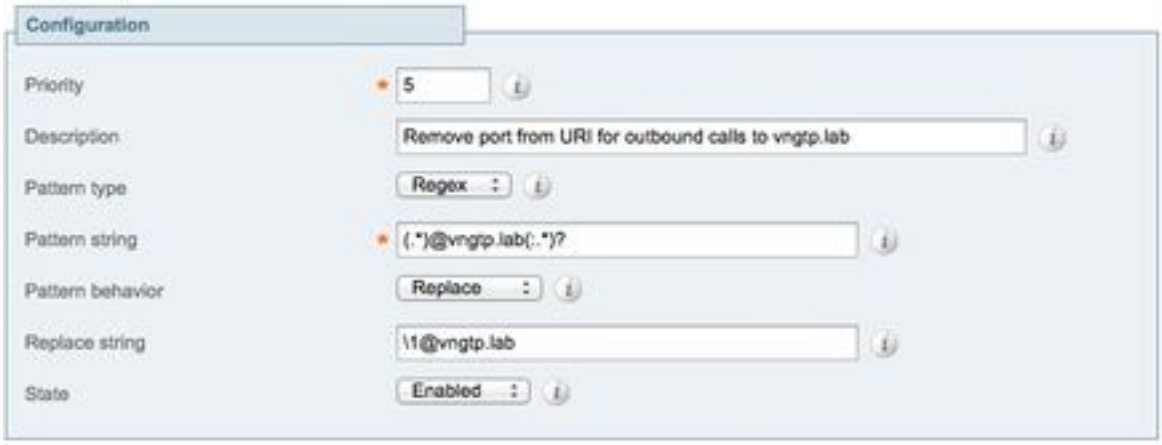
d. Configure el nombre de dominio completamente calificado del clúster de CUCM.

Puede introducir varias entradas separadas por una coma.

e. Cree una transformación en Expressway-C que quite el puerto del URI recibido en la invitación de CUCM.

Para obtener más información, busque este documento Llamadas de CUCM a zona DNS en VCS Expressway enviadas a dirección IP incorrecta

En la página de administración de Expressway, vaya a Configuración > Plan de marcación > Transformación y configuración > Plan de marcación > Transformar



El SRND también contiene un amplio capítulo sobre el plan de marcación.

Paso 5. Cargar licencias multimedia enriquecidas en Expressway

Las licencias de medios enriquecidos (también conocidas como licencias de zona transversal) deben cargarse en cada servidor de Expressway.

En caso de que se pierdan o debido a una configuración incorrecta, se liberan llamadas con este mensaje de error: "Se ha alcanzado el límite de licencia de llamada: ha alcanzado el límite de licencia de las licencias de llamadas transversales simultáneas".

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshoot

Para obtener más información sobre la resolución de problemas B2B, consulte este documento Solución de problemas más comunes para llamadas de empresa a empresa a través de Expressway

Información Relacionada

- Cisco TelePresence Video Communication Server (VCS)
- Soporte Técnico y Documentación - Cisco Systems