Configure Business to Business Audio and Video Calls Through Expressway Integrated with CUCM

Contents

Introduction
Prerequisites
Requirements
Components Used
Background Information
Configure
Network Diagram
Step 1. SIP trunk between CUCM and Expressway-C
1a. Add a new SIP Trunk Security Profile.
1b. Configure the SIP trunk on CUCM.
1c. Configure a neighbor zone on Expressway-C
1d. Check Certificates
Step 2. Configure traversal zone between Expressway-C and Expressway-E
2a. Traversal zone configuration for B2B traffic on Expressway-C
2b. Traversal zone configuration for B2B traffic on Expressway-E
Step 3. Configure DNS zone on Expressway-E
Step 4. Configure dialplan
4a.Transforms and/or Search Rules on Expressway-C and E
4b. SIP Route pattern(s) in CUCM
4c. For SIP call routing, SRV records must be created on the public DNS servers.
4d. Configure the Cluster Fully Qualified Domain Name in CUCM.
4e. Create a transform on Expressway-C which removes the port from the URI received in the Invite from CUCM.
Step 5. Upload rich media licenses to Expressway
Verify
Troubleshoot
Related Information

Introduction

This document describes how to integrate/configure Business to Business (B2B) deployment for audio and video calls through Expressway integrated with Cisco Unified Call Manager (CUCM).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- 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 phone
- Session Initiation Protocol (SIP)
- Hypertext Transfer Protocol (HTTP)
- eXtensible Messaging and Presence Protocol (XMPP)
- Cisco Unified IM and Presence (IM&P)
- Certificates

Components Used

The information in this document is based on these software and hardware versions:

- Expressway C and E X8.1.1 or later
- Unified Communications Manager (CUCM) 10.0 or later.

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. If your network is live, ensure that you understand the potential impact of any command.

Background Information

These steps explain in detail how to integrate/configure B2B deployment for audio and video calls through Expressway integrated with CUCM to be able to make and receive calls from other companies (domains).

Expressway with the Mobile Remote Access (MRA) feature provides seamless registration of Jabber and TC endpoints located outside the enterprise network as is shown in network diagram.

The same architecture does also provide seamless integration/calls between different enterprises, aka Business to Business integration and this for Audio, Video and IM&P. (B2B)

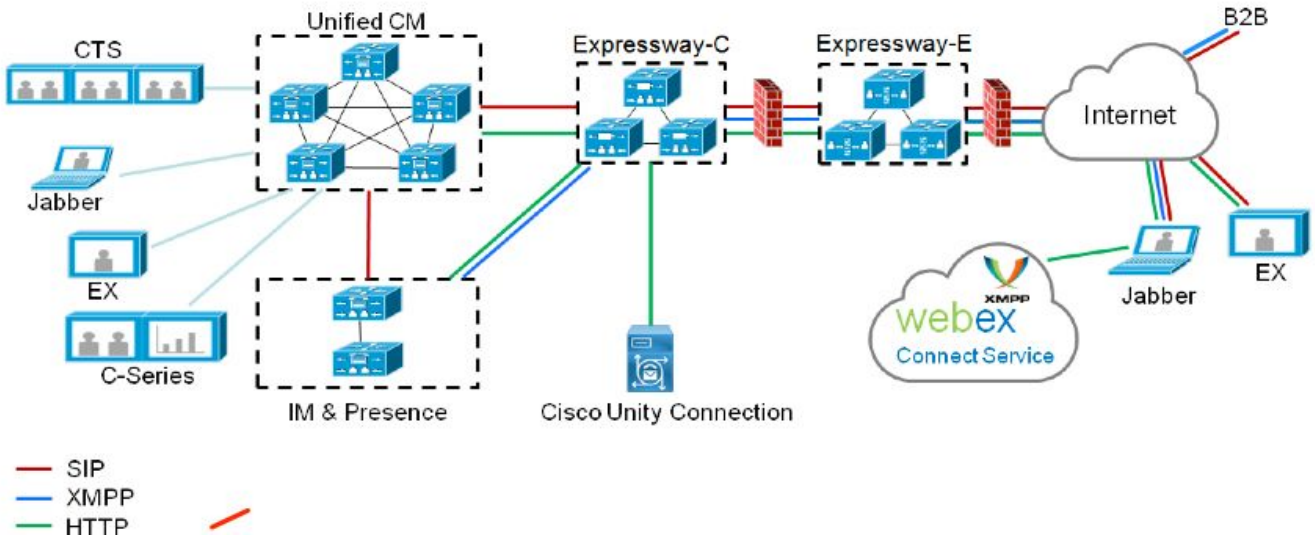
This document does not cover the IM&P part and neither does it cover H.323 integration.

Prior you continue you need to ensure you have the relevant DNS Service (SRV) created for your domain, these records are used by other companies to find the location of your Expressway.

Configure

Network Diagram

This image provides an example of a network diagram



Step 1. SIP trunk between CUCM and Expressway-C

After CUCM discovery is done by Expressway-C, Neighboring zone(s) are automatically configured for each node and transport protocol discovered.

When the CUCM cluster is configured in mixed mode there is 1 zone for Transmission Control Protocol (TCP) for none-secure traffic with destination port 5060 and 1 zone for TLS (Transport Layer Security) for secure traffic with destination port 5061. These ports can not be changed.

The 2 zones are used for all edge calls to and from the edge endpoints.

Inbound calls from the edge endpoints take the route of these auto-added zones and hence target TCP 5060 or TLS 5061 on CUCM.

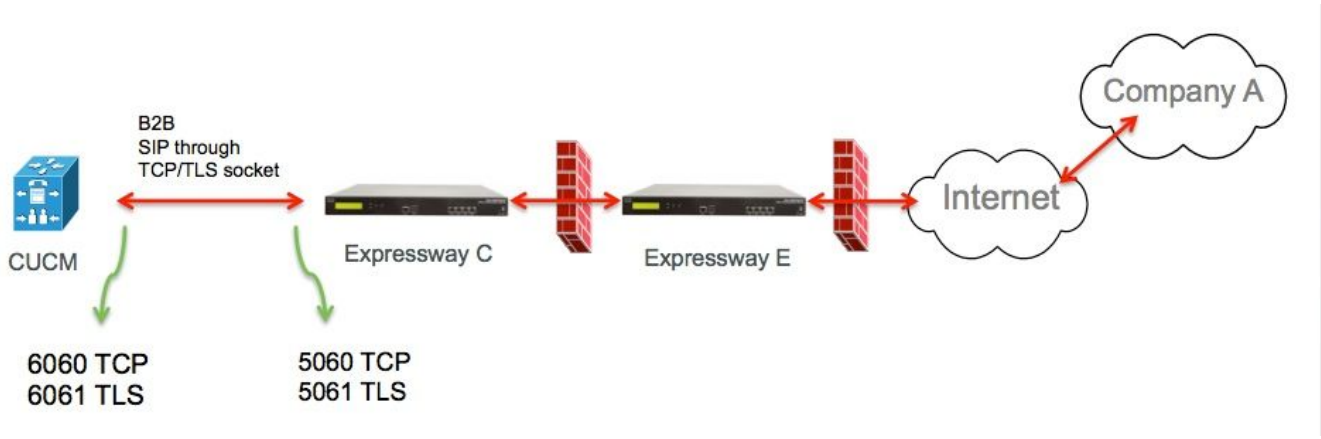
Through the established sockets edge endpoints register and place/receive calls.

For B2B calls, configure a SIP trunk in CUCM that points to Expressway-C where typically CUCM listen on port 5060 or 5061 for inbound traffic from this gateway.

Since edge traffic comes from the same source IP with port 5060/5061, you need to use a different listening port for this trunk in CUCM. Otherwise edge traffic is routed to the SIP trunk device in CUCM and not to the endpoint device (CSF or EX).

For Expressway-C side use ports 5060 and 5061 for Session Initiation Protocol (SIP) TCP/TLS.

An example where CUCM listens on port 6060/6061 for inbound traffic on this trunk is shown in the image



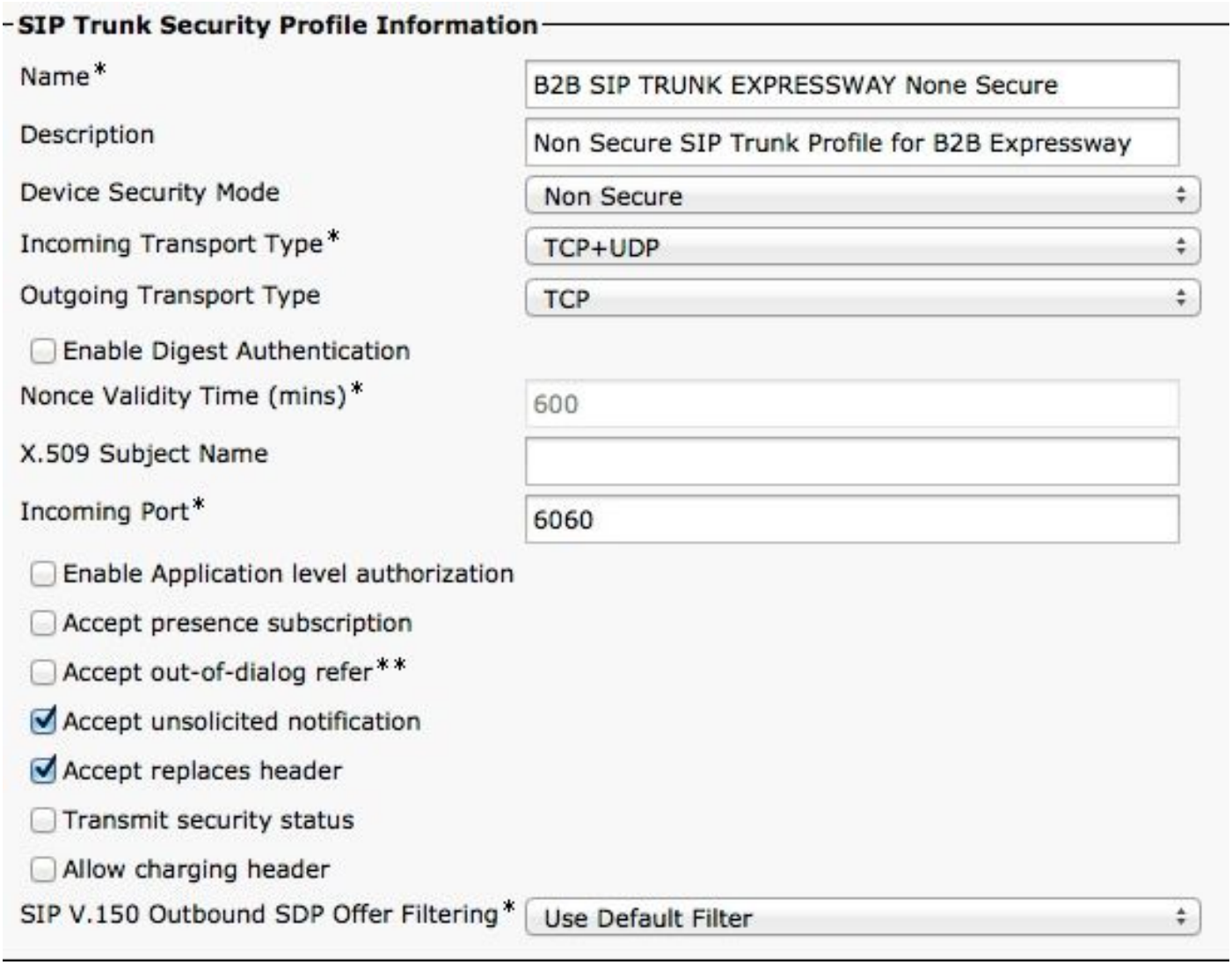
These are the different configuration steps documented for this deployment. Both for secure and non-secure deployments.

1a. Add a new SIP Trunk Security Profile.

From the **CUCM Administration page,** navigate to **> Device > Trunk.**

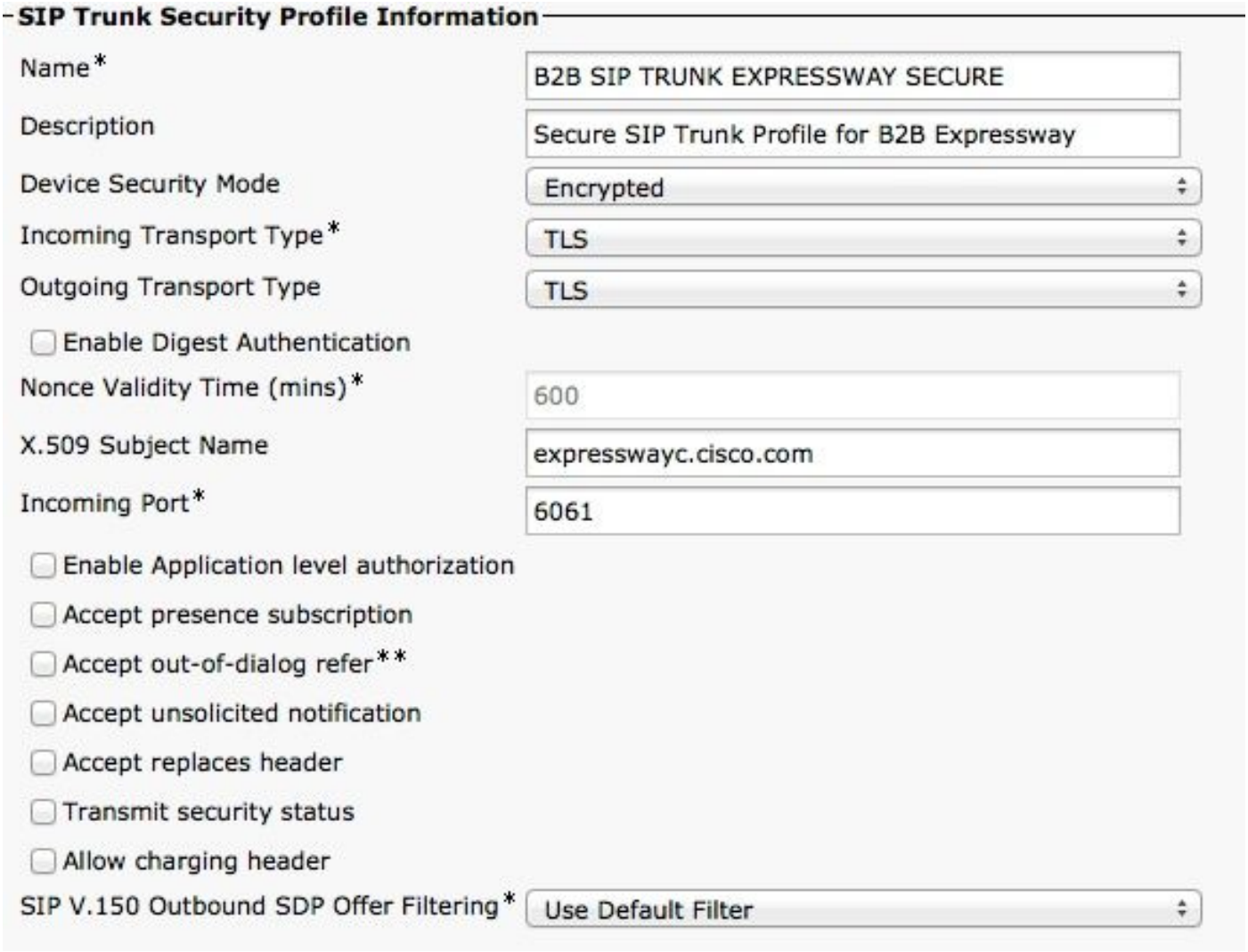
Configure a different Incoming port then 5060/5061, here use 6060 for TCP and 6061 for TLS

Non Secure SIP Trunk profile



Secure SIP Trunk profile

For TLS you also need to configure the X.509 Subject name that matches the CN of the certificate presented by the Expressway-c. In addition also upload the Expressway-C or the CA certificate (which issued the Expressway-C certificate) to the CUCM Certificate trust store.



1b. Configure the SIP trunk on CUCM.

Through this trunk all B2B calls flows to and from CUCM.

The SIP trunk configuration parameters are standard for CUCM with VCS deployments.

Ensure to associate the security profile created in step 1.

1c. Configure a neighbor zone on Expressway-C

A neighbor zone needs to be configured on Expressway-C to target CUCM.

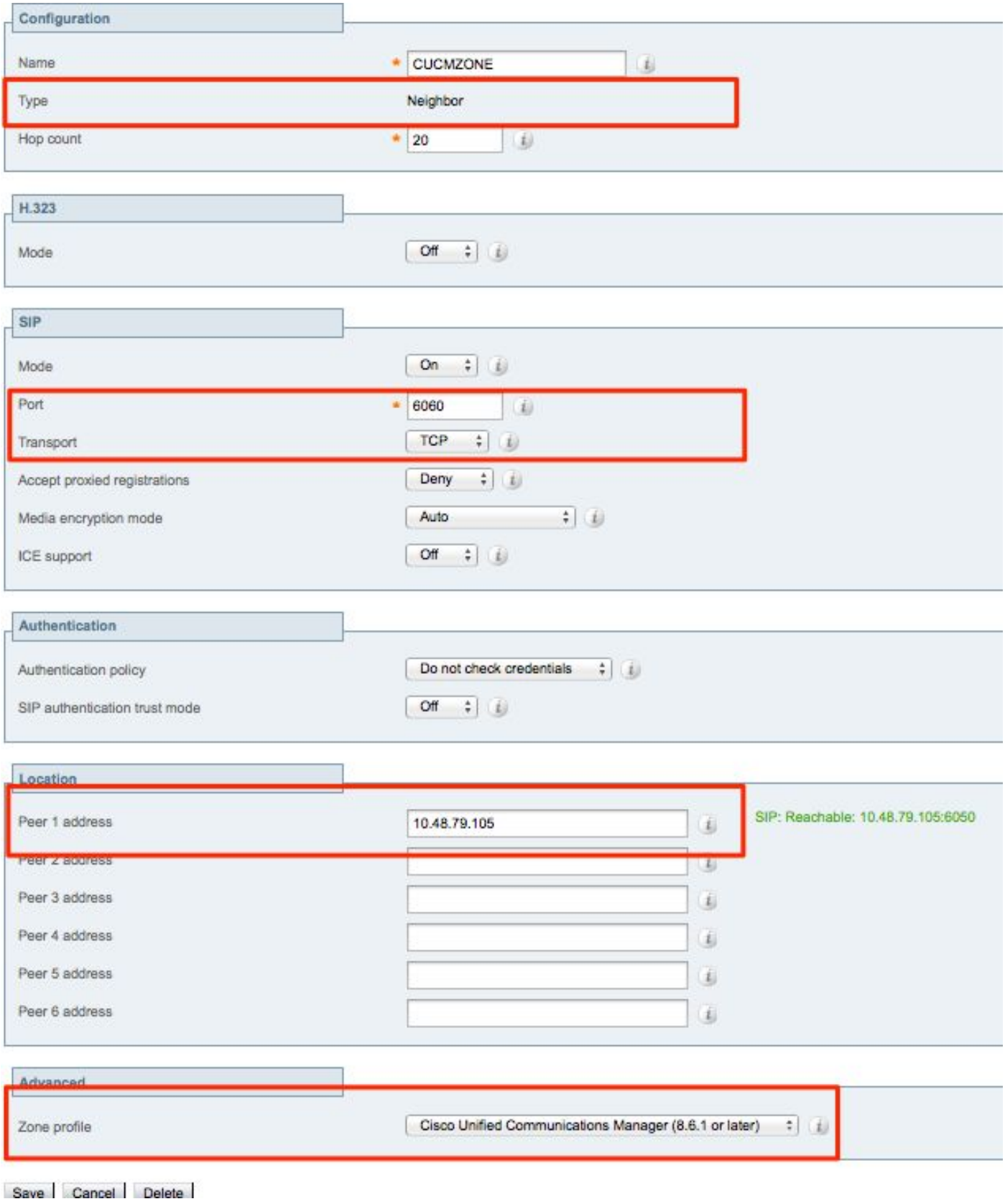
This zone is used to route inbound B2B traffic to CUCM.

The configuration is standard except that you must ensure to configure the destination port corresponds to the listening port configured on the SIP Trunk Security profile assigned to the SIP trunk on CUCM.

In this example the destination port used is 6060 for SIP/TCP and 6061 for SIP/TLS. (refer to step 1) as shown in the image

From Expressway Administration page, navigate to **Configuration > Dial Plan > Transforms y Configuration**

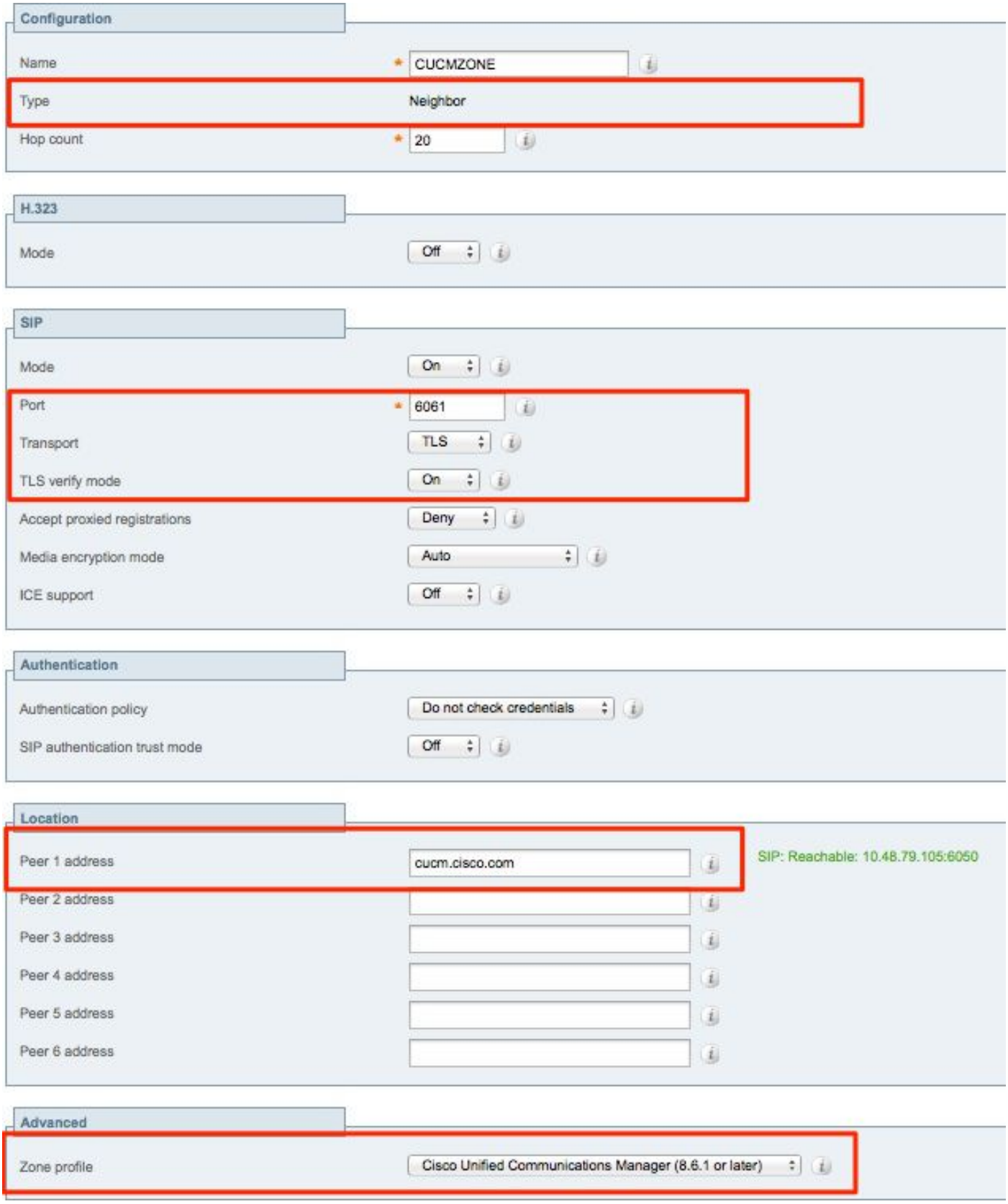
Neighbor zone for SIP TCP:



Neighbor zone for SIP TLS - with TLS verify mode on

When TLS verify mode is set to on you must ensure the **peer address** matches the CN or SAN from the certificate presented by CUCM. Typically with TLS verify mode on you configure the FQDN of the CUCM node for peer address.

From Expressway Administration page, navigate to **Configuration > Dial Plan > Transforms y Configuration**

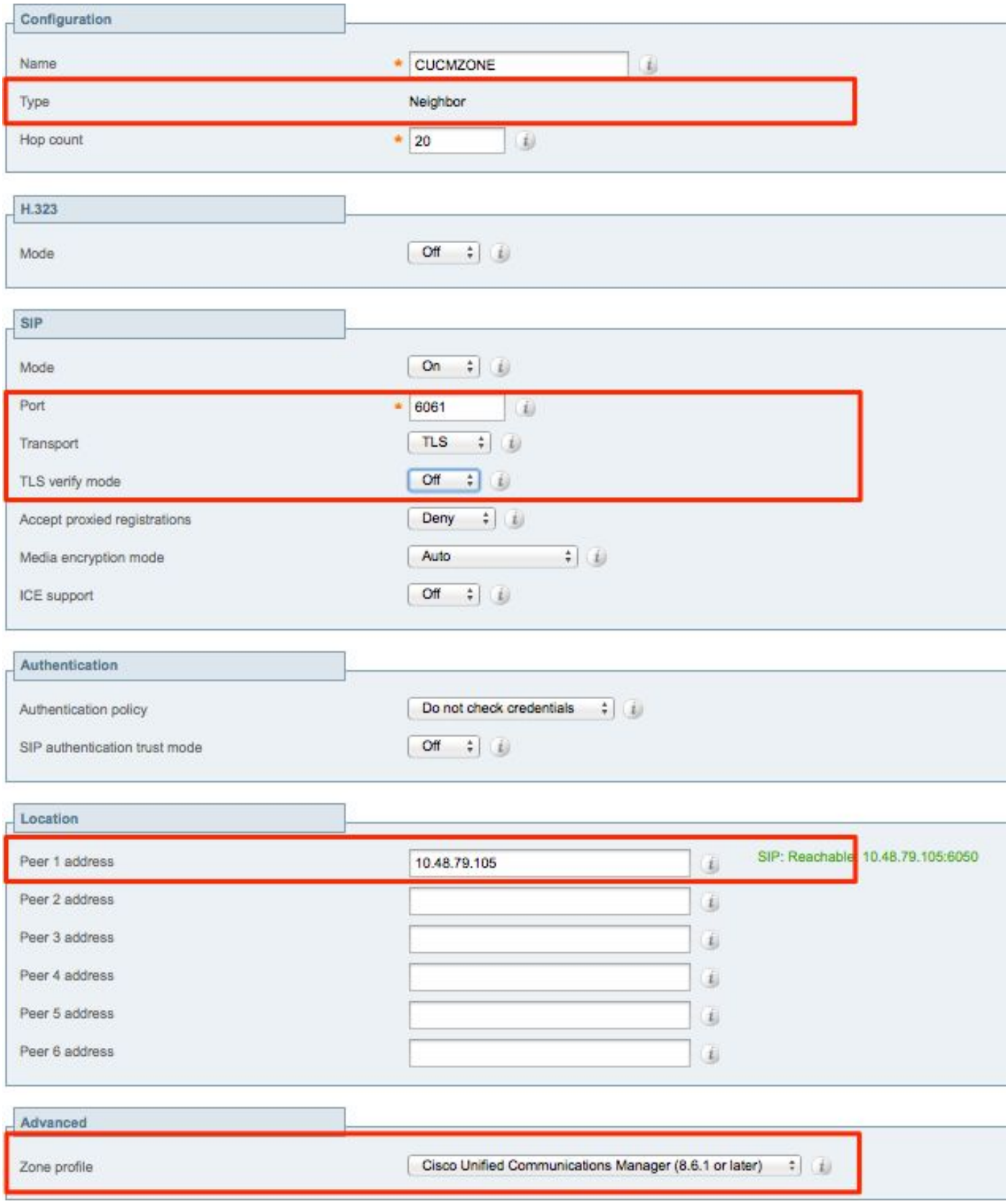


Neighbor zone for SIP TLS - with TLS verify mode off

When TLS verify mode is set to off the peer address can be either the IP address, hostname or Fully Qualified Domain Name (FQDN) of the CUCM node.

From Expressway Administration page, navigate to **Configuration > Dial Plan > Transforms y**

Configuration



1d. Check Certificates

For TLS, ensure that:

- Expressway-C server certificate or CA root (used to sign certificate) is uploaded to the CUCMTrust store on all servers in the CUCM cluster.

- Callmanager certificate or CA root (used to sign certificate) is uploaded to the Trusted CA Certificate list on the Expressway-C server.

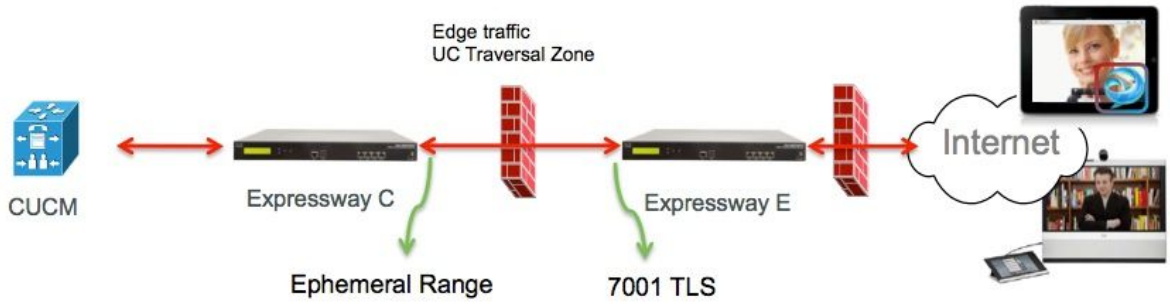
Step 2. Configure traversal zone between Expressway-C and Expressway-E

A separate traversal zone has to be configured to route the B2B traffic between Expressway-C and Expressway-E.

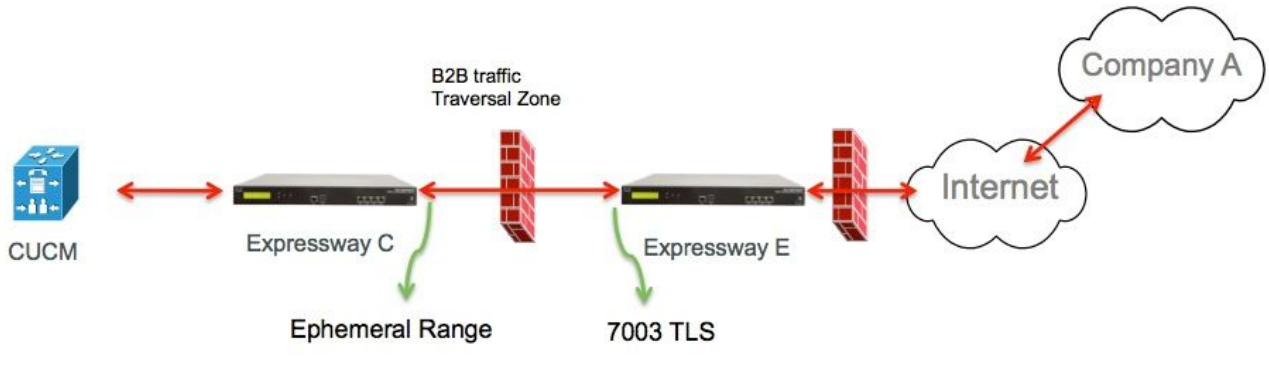
This is a standard traversal zone configuration, but similar as with the SIP trunk on CUCM a different port then the port used by the UC Traversal zone for Edge traffic must be configured.

The standard port for the UC Traversal zone is 7001. For the B2B Traversal zone you can e.g configure 7003.

UC Traversal Zone for edge traffic as shown in the image



Traversal Zone for B2B traffic as shown in the image

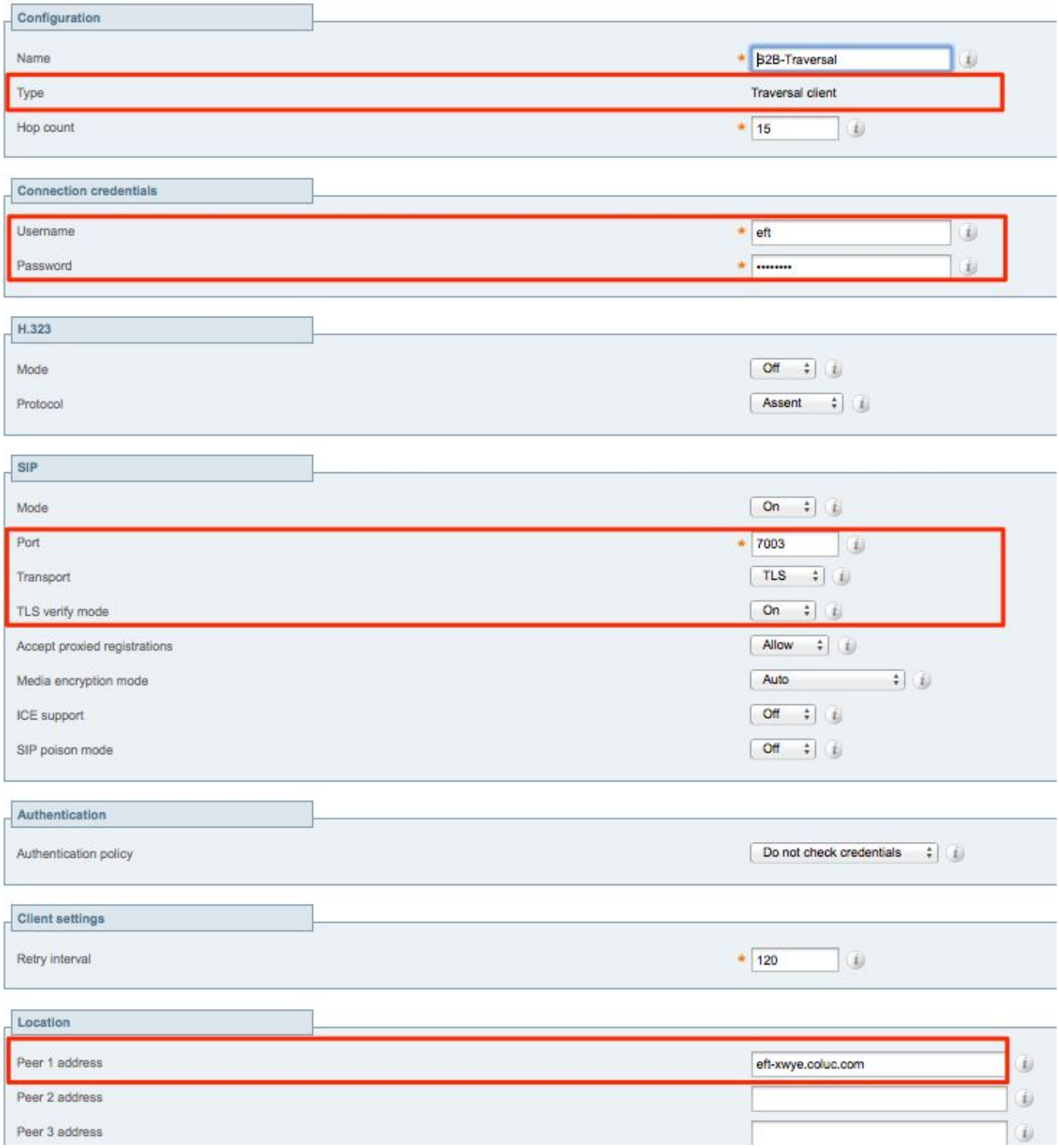


2a. Traversal zone configuration for B2B traffic on Expressway-C

Expressway-C is the traversal zone client, in this example the destination port is 7003

With TLS verify mode set to On ensure the **Peer Address** configured matches the CN or SAN of the presented certificate by Expressway-E

From Expressway Administration page, navigate to **Configuration > Dial Plan > Transforms y Configuration**

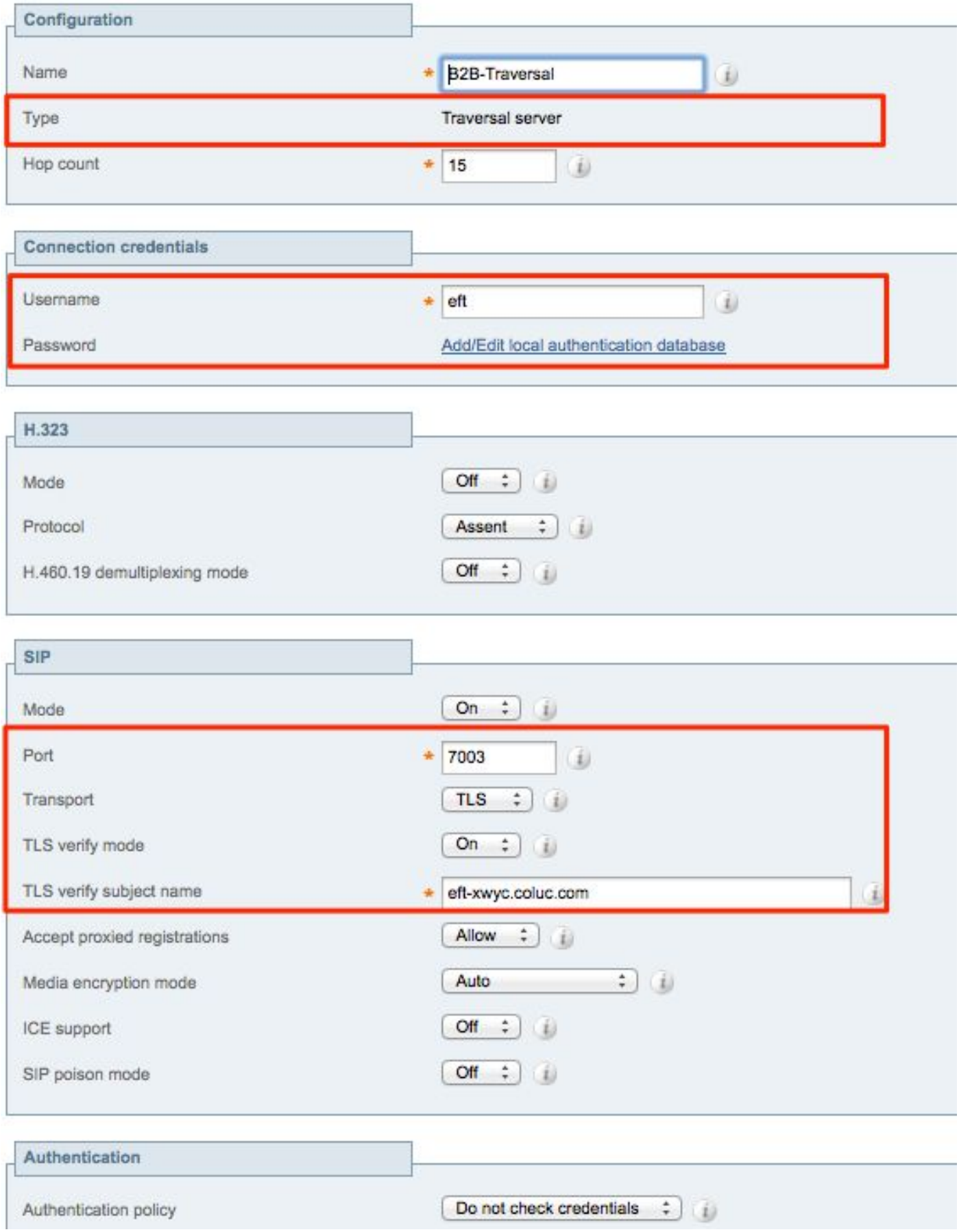


2b. Traversal zone configuration for B2B traffic on Expressway-E

Expressway-E is the traversal zone server, in this example the listening port is 7003.

With TLS verify mode set to On ensure the **TLS verify subject name** configured matches the CN or SAN of the presented certificate by Expressway-C

From Expressway Administration page, navigate to **Configuration > Dial Plan > Transforms y Configuration**



Step 3. Configure DNS zone on Expressway-E

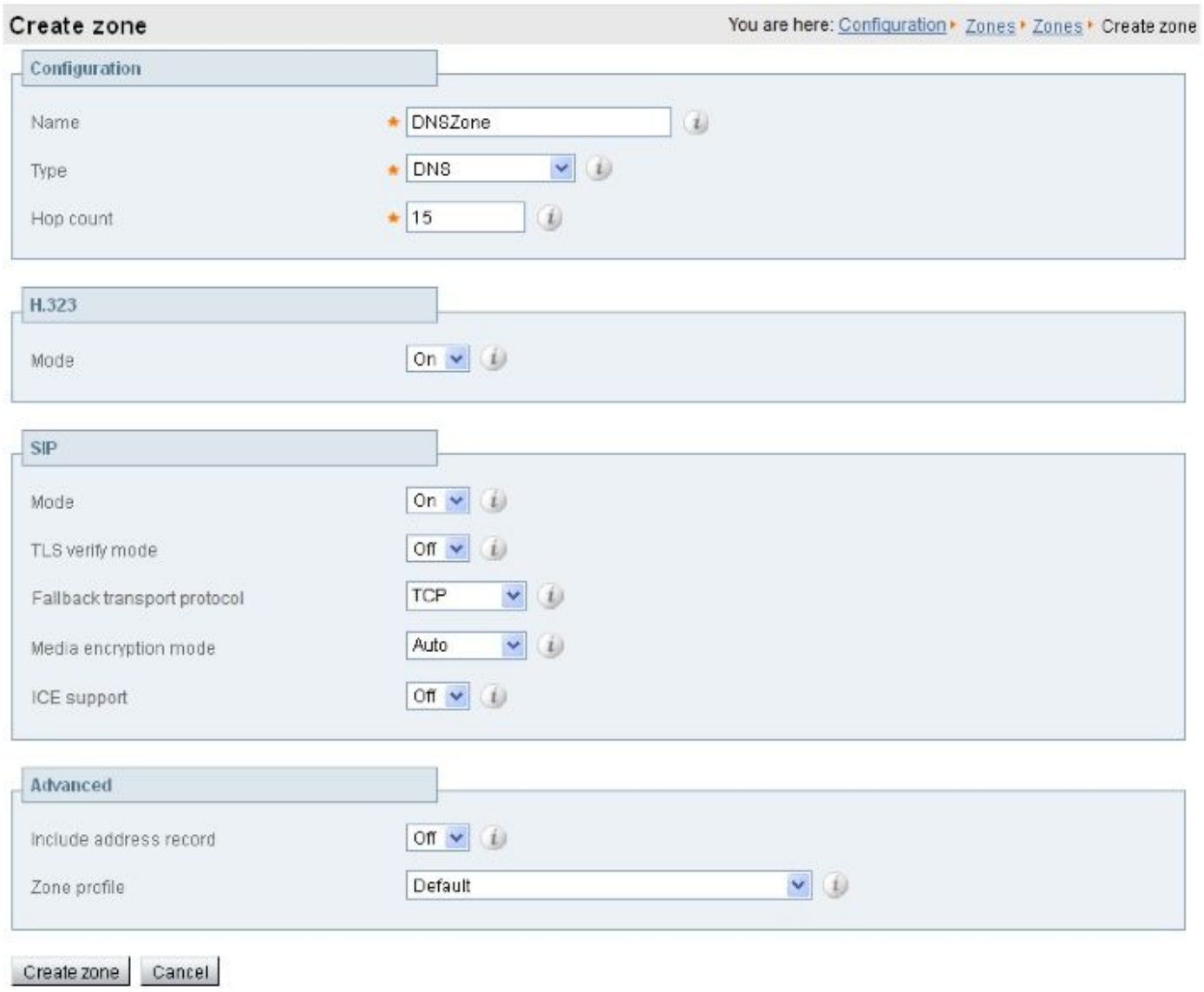
To route the B2B traffic, configure a DNS zone on Expressway-E.

Expressway-E, for traffic destined to this zone performs a DNS SRV lookup for ether _sip or _sips and this for the domain derived from the domain portion of the SIP URI.

The SRV target returned by the DNS server used to route the SIP call to.

The configuration is a standard DNS zone configuration.

From Expressway Administration page, navigate to **Configuration > Zones**



Step 4. Configure dialplan

4a.Transforms and/or Search Rules on Expressway-C and E

From Expressway Administration page, navigate to **Configuration > Dial Plan > Transforms y Configuration > Dial Plan > Transform or Search Rules**

For more information please consult the VCS Deployment guides (Control with Expressway), chapter on 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 Route pattern(s) in CUCM

For more information please consult the CUCM System and Administration guide (Dialplan Deployment guide)

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

4c. For SIP call routing, SRV records must be created on the public DNS servers.

As shown in the image, it lists the required SRV records, as well H323 B2B calls which has not been discussed in this document. Also to note that SIP UDP by default is disabled on 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.

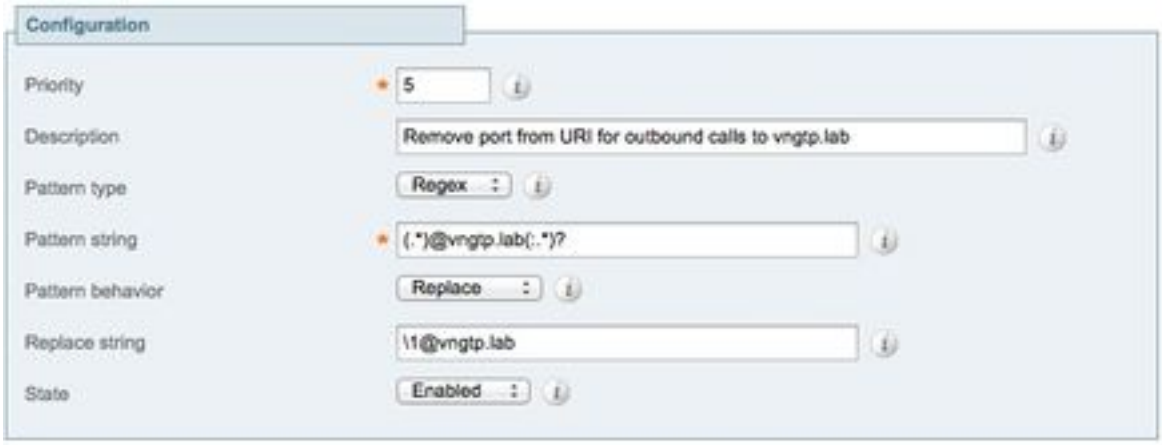
4d. Configure the Cluster Fully Qualified Domain Name in CUCM.

You can enter multiple entries seperated by comma.

4e. Create a transform on Expressway-C which removes the port from the URI received in the Invite from CUCM.

For more info, look for this document: http://www.cisco.com/c/en/us/support/docs/unified-communications/telepresence-video-communication-server-vcs/116729-trouble-cucm-dns-vcs-01.html

From Expressway Administration page, navigate to **Configuration > Dial Plan > Transforms y Configuration > Dial Plan > Transform**



The SRND also contains an extensive chapter on dialplan

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

Step 5. Upload rich media licenses to Expressway

Rich media licenses (aka Traversal Zone licenses) must be uploaded to each Expressway Server.

In case these are missed or due to improper configuration calls are released with this error message: "Call license limit reached: You have reached your license limit of concurrent traversal call licenses"

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Related Information

- Cisco TelePresence Video Communication Server (VCS)