Configurar Acceso móvil y remoto a través de Expressway/VCS en una implementación de múltiples dominios

Contenido

Introducción

Este documento describe cómo configurar el Cisco TelePresence Video Communication Server (VCS) para Acceso Remoto Móvil (ARM) cuando se utilizan varios dominios.

La configuración del MRA cuando hay solo un dominio es relativamente sencilla, y usted puede seguir los pasos detallados en la guía de implementación. Cuando la implementación abarca múltiples dominios, se torna más compleja. Este documento no es una guía de configuración, pero describe los aspectos importantes cuando se trata de múltiples dominios. La configuración principal se documenta en la Guía de implementación del Cisco TelePresence Video Communication Server (VCS).

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

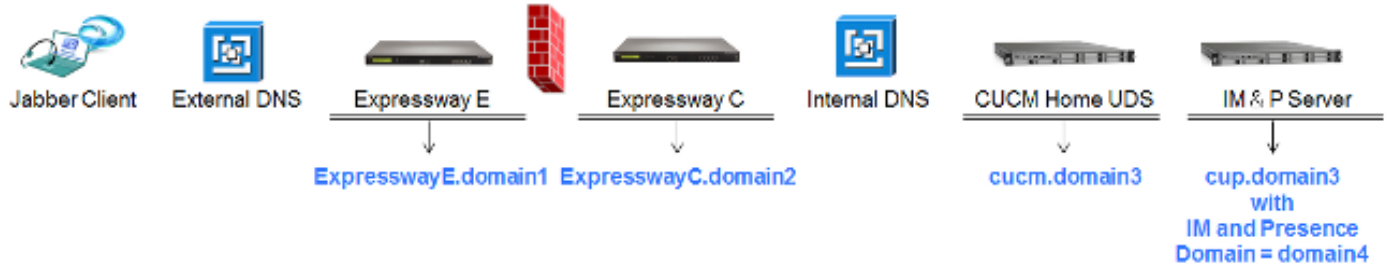
Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

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, make sure that you understand the potential impact of any command.

Configurar

Utilice la información que se describe en esta sección para configurar el VCS.

Diagrama de la red

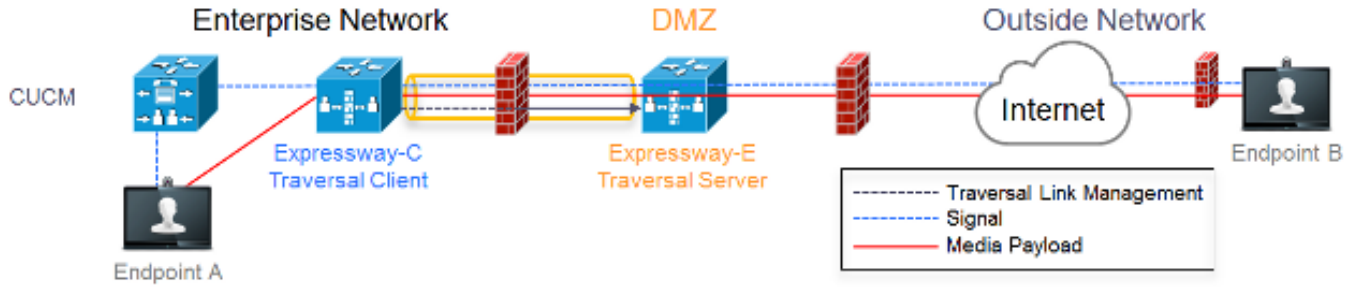


Este es un resumen de los diferentes dominios:

- **Dominio 1: es el dominio Edge que utiliza el cliente para detectar la ubicación del servidor Edge y a través del cual detecta el Servicio de Datos del Usuario (UDS).**
- **Dominio 2 y dominio 3: se utiliza para la detección de servidores.**
- **Dominio 4: este es el dominio de Mensajería Instantánea y Presencia que utiliza el tráfico de la Plataforma Extensible de Comunicaciones (XCP) y del Protocolo Extensible de Mensajería y Presencia (XMPP).**

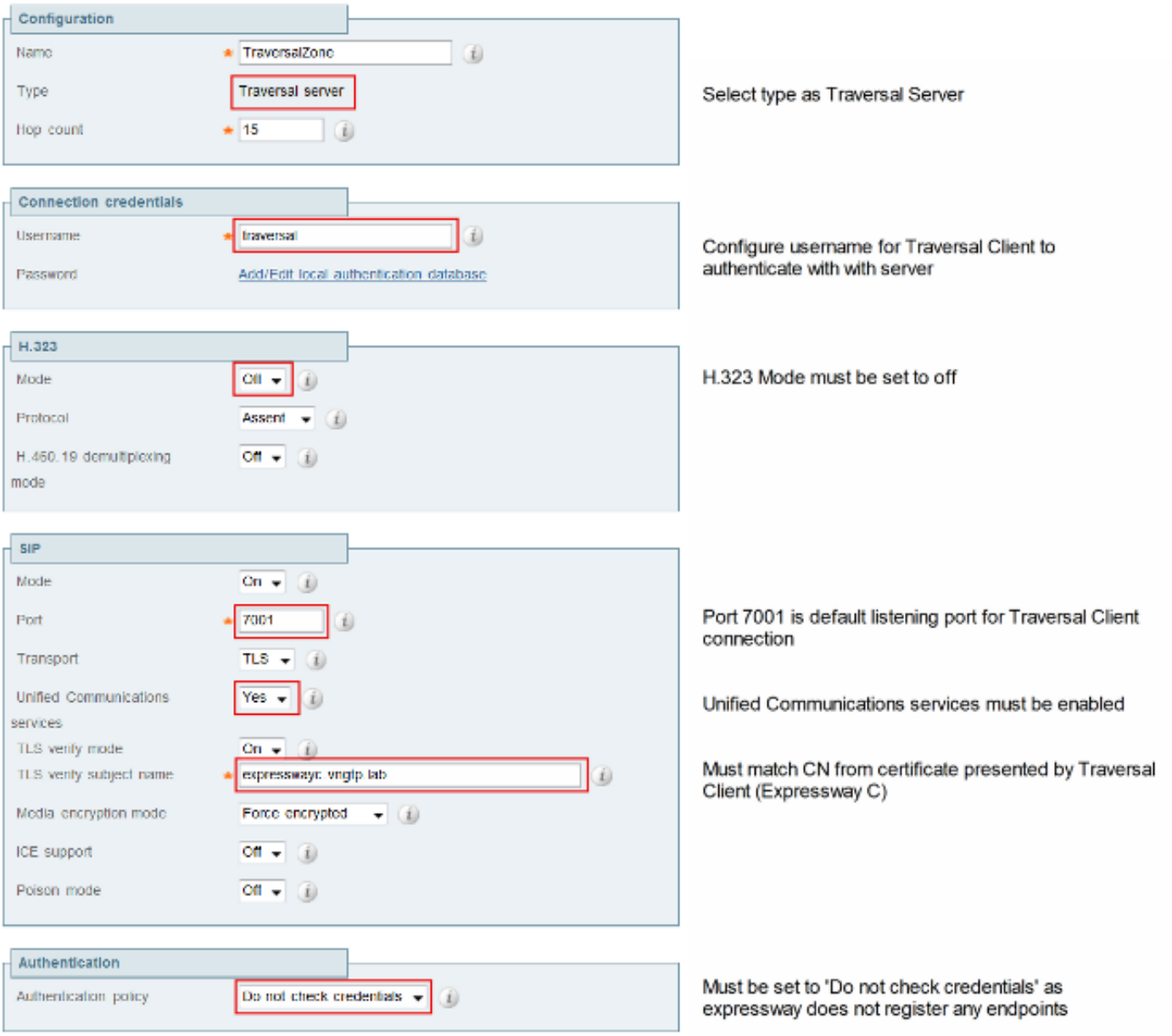
Zona transversal

La zona transversal está formada por un servidor transversal (**expresswayE**), ubicado en la zona desmilitarizada (DMZ), y el cliente transversal (**expresswayC**), ubicado dentro de la red:



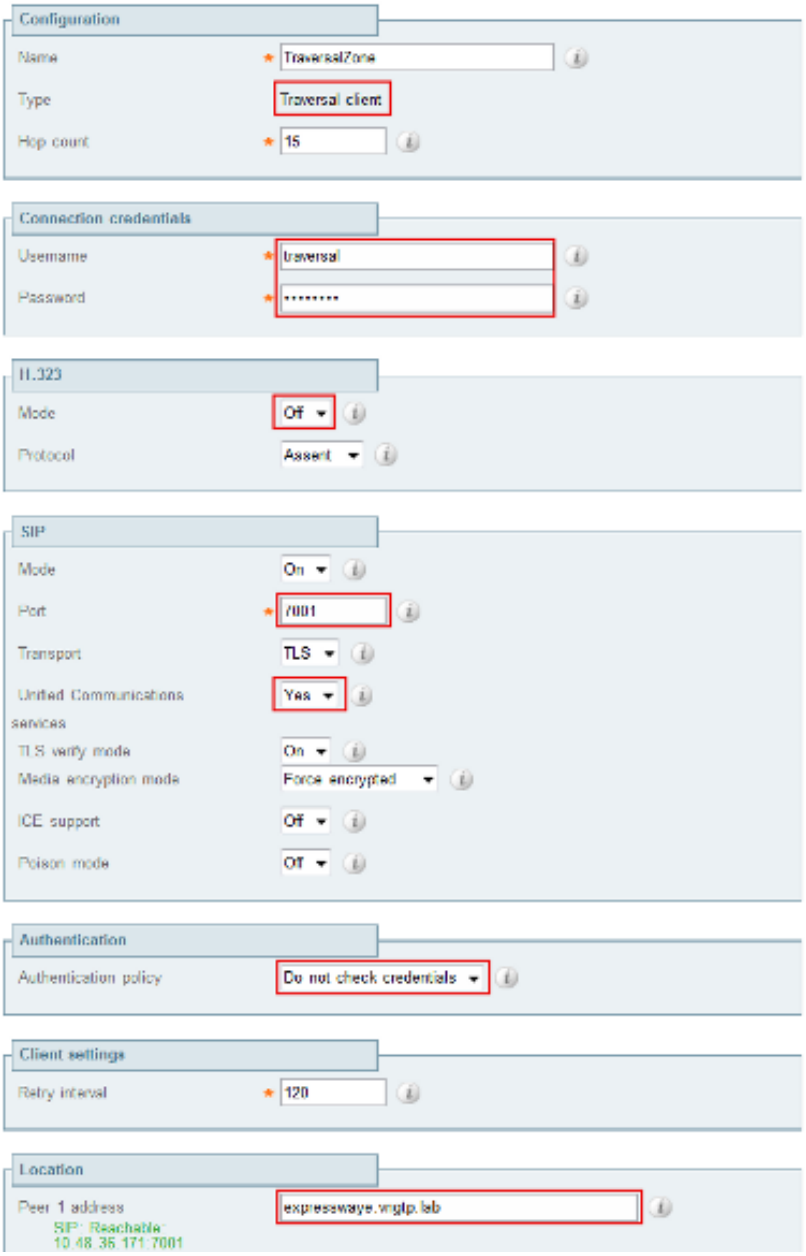
Servidor transversal

El servidor transversal está ubicado en la configuración de zona en Expressway E:



Cliente transversal

El cliente transversal está ubicado en la configuración de zona en Expressway C:



Select Traversal Client as Type

Configure same username and password as added on the Traversal Server (Expressway E)

H.323 mode must be set to off

Destination port Traversal Server is listening on

Unified Communications must be enabled

Must be set to 'Do not check credentials' as expressway does not register any endpoints

Must be FQDN
Must be DNS resolvable
Must match CN from certificate presented by Traversal Server (Expressway E)

Dominio de servicios de voz

El usuario inicia sesión siempre con **userid@domain4**, ya que no debería haber diferencia en la experiencia del usuario tanto afuera como adentro. Esto significa que si el **dominio 1 es diferente del dominio 4**, debe configurar el dominio de los servicios de voz en el cliente Jabber. Esto sucede porque la sección del dominio del inicio de sesión se utiliza para detectar los servicios de Collaboration Edge a través de la búsqueda de registros del Servicio (SRV).

El cliente realiza una consulta de registro de SRV del Sistema de Nombres de Dominios (DNS) para **_collab-edge._tls.<domain>**. Esto implica que, cuando el dominio de la ID de inicio de sesión del usuario es diferente del dominio de Expressway E, debe usar la configuración de dominio del servicio de voz. Jabber utiliza esta configuración para detectar el Collaboration Edge y el UDS.

Hay varias opciones que puede utilizar para completar esta tarea

1. Agregar esto como parámetro al instalar Jabber a través de la Interfaz de Servicios de Medios (MSI):

```
msiexec /i CiscoJabberSetup.msi VOICE_SERVICES_DOMAIN=domain1 CLEAR=1
```

2. Vaya a **%APPDATA% > Cisco > Unified Communications (Comunicaciones Unificadas) > Jabber > CSF > Config**, y cree este **archivo jabber-config-user.xml en el directorio:**

```
<?xml version="1.0" encoding="utf-8"?>
<config version ="1.0">
<Policies> <VoiceServicesDomain>domain1</VoiceServicesDomain>
</Policies>
</config>
```

Nota: Este método es únicamente experimental y no oficialmente compatible con Cisco.

3. Edite el **archivo jabber-config.xml.** Esto requiere que el cliente se registre primero de forma interna. Jabber Config File Generator se puede utilizar para esto:

```
<Policies>
<VoiceServicesDomain>domain1</VoiceServicesDomain>
</Policies>
```

4. Además, los clientes móviles de Jabber se pueden configurar con el Dominio de Servicios de Voz de forma inicial para que no sea necesario que inicien sesión de forma interna en primer lugar. Esto se explica en la Guía de Implementación e Instalación en el capítulo Detección de Servicios. Debe crear una URL de configuración en la cual el usuario deberá hacer clic:
`ciscojabber://provision?ServicesDomain=domain4&VoiceServicesDomain=domain1`

Nota: Se requiere para utilizar el dominio de servicios de voz porque debe asegurarse de realizar la búsqueda de los registros del SRV de Collaboration Edge para el dominio externo (**domain1**).

Registros DNS

Esta sección describe la configuración para los registros DNS internos y externos.

Externo

Tipo	Entrada	Resulta en
Registro SRV	_collab-edge._tls.domain1	ExpresswayE.domain1
Un registro	ExpresswayE.domain1	Dirección IP de ExpresswayE

Es importante tener en cuenta que:

- Los registros SRV proporcionan un Nombre de Dominio Completo (FQDN) y no una dirección IP.
- El FQDN que proporcionan los registros SRV que coinciden con el FQDN real de Expressway-E, o el objetivo de registro SRV es un CNAME y el alias hace referencia a un servidor dentro del mismo dominio como el de Expressway-E (ID de bug de Cisco pendiente CSCuo82526).

Esto es necesario porque Expressway-E establece una cookie en el cliente con su propio dominio (**domain1**), y si no coincide con el dominio proporcionado por el FQDN, el cliente no lo acepta. La ID de bug de Cisco CSCuo83458 se abre como una mejora para este escenario.

Interno

Tipo	Entrada	Resulta en
Registro SRV	_cisco-uds._tcp.domain1	cucm.domain3
Un registro	cucm.domain3	Dirección IP de CUCM

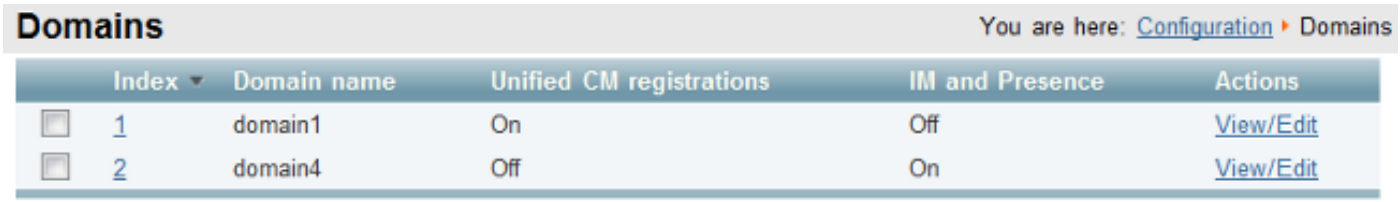
Debido a que el dominio de servicios de voz está establecido en **domain1**, Jabber incrusta el **domain1 en la URL modificada para la detección de configuración de Collaboration Edge (get edge_config**). Una vez recibida, Expressway-C realiza una consulta de registro SRV UDS para **domain1 y proporciona los registros en el mensaje 200 OK.**

Tipo	Entrada	Resulta en
SRV	_cisco-uds._tcp.domain4	cucm.domain3
Un registro	cucm.domain3	Dirección IP de CUCM

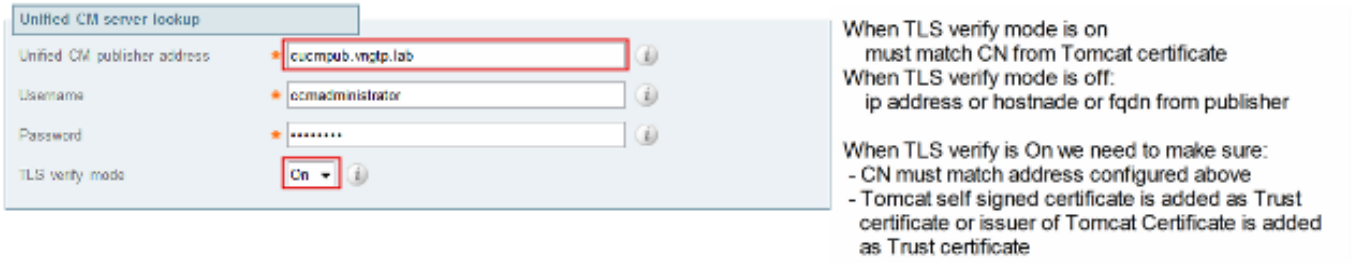
Cuando el cliente está en la red, se requiere la detección del registro SRV UDS para **domain4**.

Dominios SIP en Expressway-C

Debe agregar estos dominios del Protocolo de Inicio de Sesión (SIP) a Expressway-C y habilitarlos para MRA:



Nombre de host/dirección IP de servidores CUCM



Cuando configure los servidores Cisco Unified Communications Manager (CUCM), tendrá dos escenarios posibles:

- Si su Expressway-C (**domain2**) está configurada con el mismo dominio que su servidor CUCM (**domain3**), puede configurar sus servidores CUCM (**System (Sistema) > Servers (Servidores)**) con:

  La dirección IPEl nombre de hostEl FQDN
- Si Expressway-C (**domain2**) está configurada con un dominio diferente del del servidor (**domain3**), entonces debe configurar los servidores CUCM con:

  La dirección IPEl FQDN

Esto es necesario debido a que, cuando Expressway-C detecta los servidores CUCM y se

proporciona el nombre de host, realiza una búsqueda de DNS para **hostname.domain2**, que no funciona si **domain2 y domain3 son diferentes.**

Certificados

Además de los requisitos generales de certificación, se deben agregar algunos detalles a los Nombres Alternativos del Sujeto (SAN) de los certificados:

- Expressway-C

  Se deben agregar los alias del nodo de chat que están configurados en los servidores IM&P. Esto es solo un requisito para las implementaciones federadas destinadas a usar tanto Transport Layer Security (TLS) como chat grupal. Esto se añade automáticamente a la Solicitud de Firma de Certificado (CSR), teniendo en cuenta que ya ha detectado los servidores IM&P.

  Se deben agregar los nombres, en formato FQDN, de todos los perfiles de seguridad telefónica en el CUCM que están configurados para TLS cifrado y que se utilizan para dispositivos que requieren acceso remoto.
  Nota: El formato del FQDN solo se requiere cuando su Autoridad de Certificación (CA) no permite sintaxis de nombre de host en el SAN.
- Expressway-E

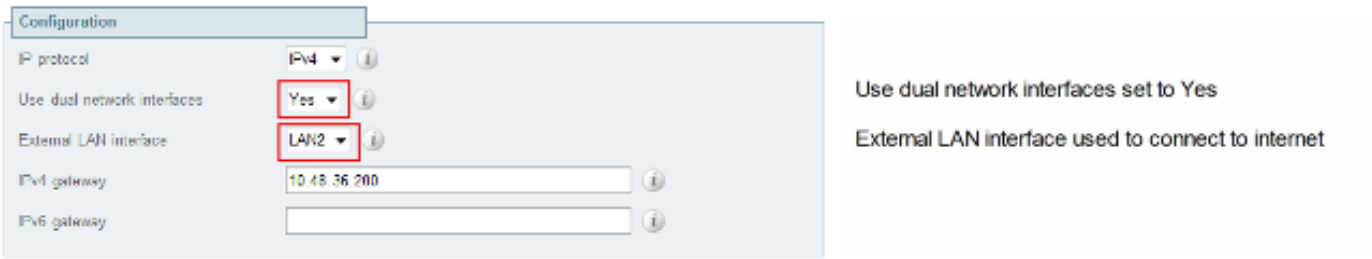
  Se debe agregar el dominio utilizado para la detección de servicios (**domain1**). Dominios federados XMPPSe deben agregar los alias del nodo de chat que están configurados en los servidores IM&P. Esto solo es necesario para las implementaciones XMPP federadas de Comunicaciones Unificadas destinadas a usar tanto el TLS como chat grupal. Esto se puede copiar desde el CSR que se genera en Expressway-C.

NIC dual

Esta sección describe los ajustes de configuración para utilizar las Tarjetas de Interfaz de Red (NIC).

Dos interfaces

Al configurar Expressway-E para usar las interfaces de red duales, es importante garantizar que ambas interfaces estén configuradas y en uso.



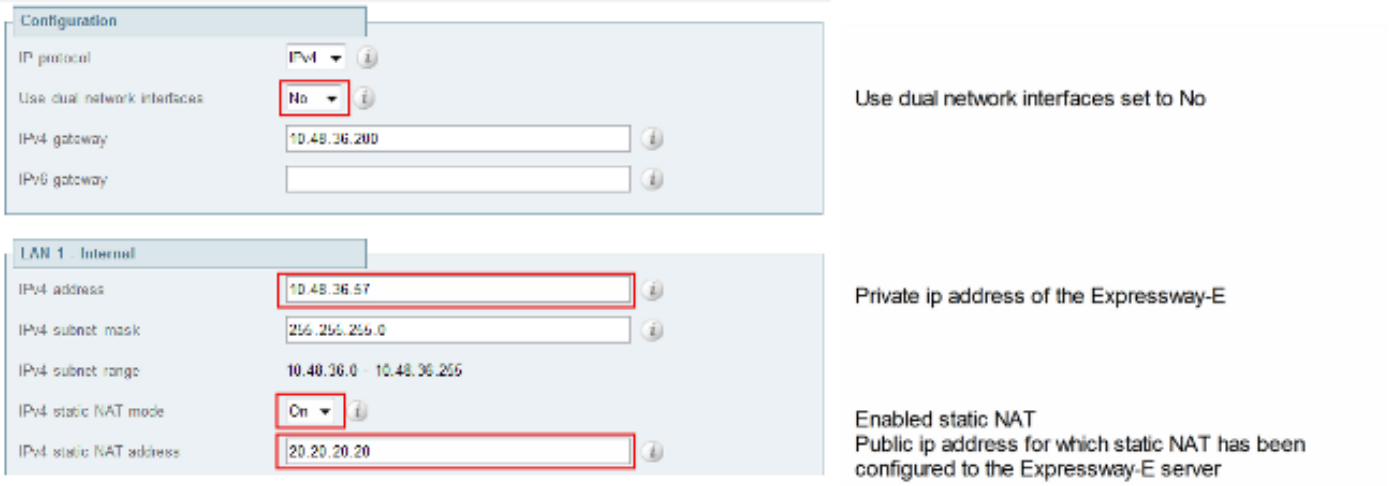
Cuando **Usar interfaces de red duales** se configura con un valor de **Yes**, Expressway-E sólo escucha en la interfaz interna para la comunicación XMPP con Expressway-C. Por lo tanto, debe asegurarse de que esta interfaz está configurada y funciona correctamente.

Una interfaz - Dirección IP pública

Cuando se utiliza solamente una interfaz y configura Expressway-E con una dirección IP pública, no se deben tener en cuenta consideraciones especiales.

Una interfaz - Dirección IP privada

Cuando se utiliza solo una interfaz y configura Expressway-E con una dirección IP privada, debe configurar también la traducción de direcciones de red (NAT):



En este caso, es importante asegurarse de que:

- El firewall permita que Expressway-C envíe tráfico a la dirección IP pública. Esto se conoce como *reflexión NAT*.
- La zona de cliente transversal de Expressway-C está configurada con una dirección de par que coincide con la dirección NAT estática en Expressway-E, que es **20.20.20.20 en este caso.**

  Consejo: En el **Apéndice 4 de la** Guía de Implementación de Configuración Básica del Cisco TelePresence Video Communication Server (VCS) (Control con Expressway) encontrará más información sobre las implementaciones avanzadas de red.

Verificación

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

Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

En esta sección, se detallan algunos escenarios específicos posibles; sin embargo, también puede usar el Collaboration Solutions Analyzer para obtener una vista detallada de todas las

comunicaciones realizadas para intentos de inicio de sesión de MRA e información sobre la solución de problemas en función de sus registros de diagnósticos.

Zona transversal

Cuando la dirección de pares se configura como dirección IP o no coincide con el nombre común (CN), observará estos registros:

```
Event="Outbound TLS Negotiation Error" Service="SIP" Src-ip="10.48.80.161"
Src-port="25697" Dst-ip="10.48.36.171" Dst-port="7001" Detail="Peer's TLS
certificate identity was unacceptable" Protocol="TLS" Common-name="10.48.36.171"
```

Cuando la contraseña es incorrecta, verá lo siguiente en los registros de Expressway-E:

```
Module="network.ldap" Level="INFO": Detail="Authentication credential found in
directory for identity: traversal"

Module="developer.nomodule" Level="WARN" CodeLocation="ppcmains/sip/sipproxy/
SipProxyAuthentication.cpp(686)" Method="SipProxyAuthentication::
checkDigestSAResponse" Thread="0x7f2485cb0700": calculated response does not
match supplied response, calculatedResponse=769c8f488f71eebdf28b61ab1dc9f5e9,
response=319a0bb365decf98c1bb7b3ce350f6ec

Event="Authentication Failed" Service="SIP" Src-ip="10.48.80.161"
Src-port="25723" Detail="Incorrect authentication credential for user"
Protocol="TLS" Method="OPTIONS" Level="1"
```

NIC dual

Cuando NIC dual está habilitada, pero la segunda interfaz no se utiliza o no está conectada, Expressway-C no se puede conectar a Expressway-E para la comunicación XMPP en el Puerto 7400 y los registros de Expressway-C muestran esto:

```
xwayc XCP_JABBERD[23843]: UTCTime="2014-03-25 17:19:45,843" ThreadID=
"139747212576512" Module="Jabber" Level="INFO " CodeLocation="mio.c:1109"
Detail="Connecting on fd 28 to host '10.48.36.171', port 7400"xwayc

XCP_JABBERD[23843]: UTCTime="2014-03-25 17:19:45,847" ThreadID="139747212576512"
Module="Jabber" Level="ERROR" CodeLocation="mio.c:1121" Detail="Unable to
connect to host '10.48.36.171', port 7400:(111) Connection refused"

xwayc XCP_JABBERD[23843]: UTCTime="2014-03-25 17:19:45,847" ThreadID=
"139747406935808" Module="Jabber" Level="ERROR" CodeLocation=
"base_connection.cpp:104" Detail="Failed to connect to component
jabberd-port-1.expresswayc-vngtp-lab"
```

DNS

Cuando el FQDN que proporciona la búsqueda de registro SRV para Collaboration Edge no coincide con el FQDN configurado en Expressway-E, los registros de Jabber muestran este error:

```
WARNING [9134000] - [csf.edge][executeEdgeConfigRequest] XAuth Cookie expiration
time is invalid or not available. Attempting to Failover.
```

```
DEBUG [9134000] - [csf.edge][executeEdgeConfigRequest]Failed to retrieve
EdgeConfig with error:INTERNAL_ERROR
```

En los registros de diagnóstico para Expressway-E podrá observar para qué dominio está configurada la cookie en el mensaje HTTPS:

```
Set-Cookie: X-Auth=1e1111e1-dddb-49e9-ad0d-ab34526e2b00; Expires=Fri,
09 May 2014 20:21:31 GMT; Domain=.vngtp.lab; Path=/; Secure
```

Dominios SIP

Cuando los dominios SIP requeridos no se agregan a Expressway-C, Expressway-C no acepta mensajes para este dominio y en los registros de diagnóstico verá el mensaje **403 Forbidden que se envía al cliente:**

```
ExpresswayE traffic_server[15550]:
Module="network.http.trafficserver" Level="DEBUG": Detail="Sending Response"
Txn-id="2" Dst-ip="10.48.79.80" Dst-port="50314"
HTTPMSG:
|HTTP/1.1 403 Forbidden
Date: Wed, 21 May 2014 14:31:18 GMT
Connection: close
Server: CE_E
Content-Length: 0

ExpresswayE traffic_server[15550]: Event="Sending HTTP error response"
Status="403" Reason="Forbidden" Dst-ip="10.48.79.80" Dst-port="50314"
```