Móvil y Acceso Remoto de la configuración con Expressway/VCS en un despliegue del Multi-dominio

Contenido

Introducción

Este documento describe cómo configurar el servidor del comunicación mediante video del Cisco TelePresence (VCS) para el Acceso Remoto móvil (MRA) cuando se utilizan los dominios múltiples.

El MRA configurado cuando hay solamente un dominio es relativamente directo, y usted puede seguir los pasos que se documentan en el Guía de despliegue. Cuando el despliegue implica los dominios múltiples, llega a ser más complejo. Este documento no es guía de configuración, sino que describe los aspectos importantes cuando los dominios múltiples están implicados. La configuración principal se documenta en el Guía de despliegue del servidor del comunicación mediante video del Cisco TelePresence (VCS).

Prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

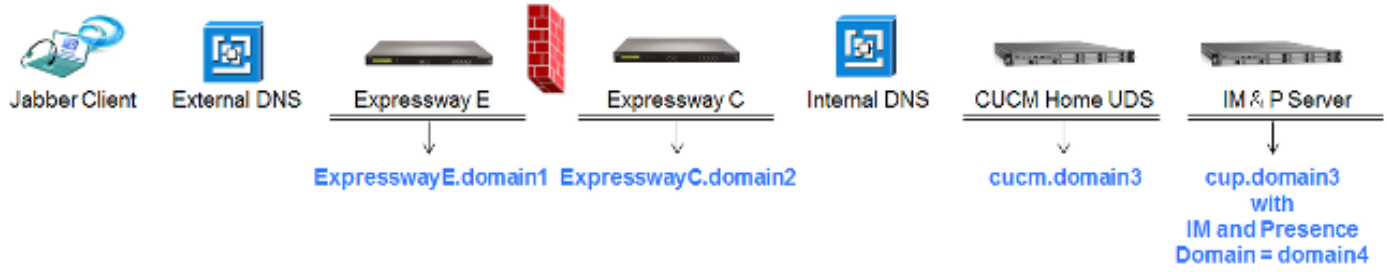
Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Configurar

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

Diagrama de la red

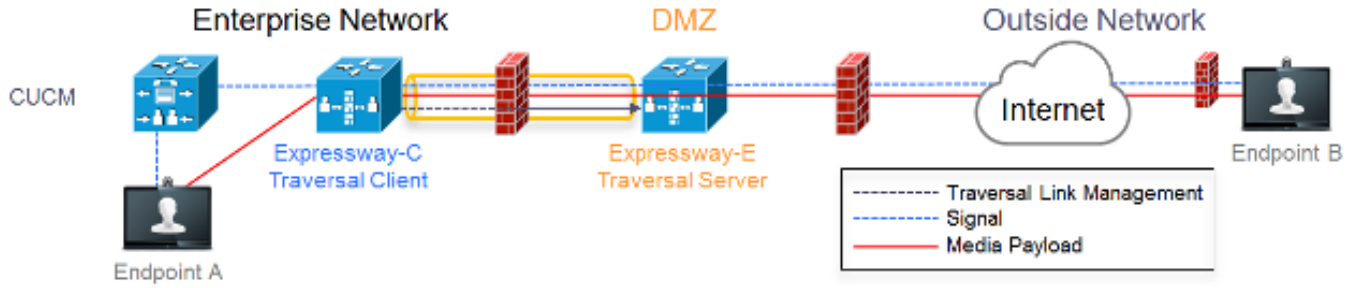


Aquí está una descripción corta de los diversos dominios:

- **domain1** - Éste es el dominio de borde que es utilizado por el cliente para descubrir la ubicación del servidor del borde y con cuál descubre el servicio de datos del usuario (UD).
- **domain2 y domain3** - Esto se utiliza para la detección del servidor.
- **domain4** - Ésta es Mensajería y presencia instantáneas (el dominio IM&P) que es utilizado por la plataforma extensible de las comunicaciones (XCP) y el tráfico extensible de la Mensajería y del protocolo de la presencia (XMPP).

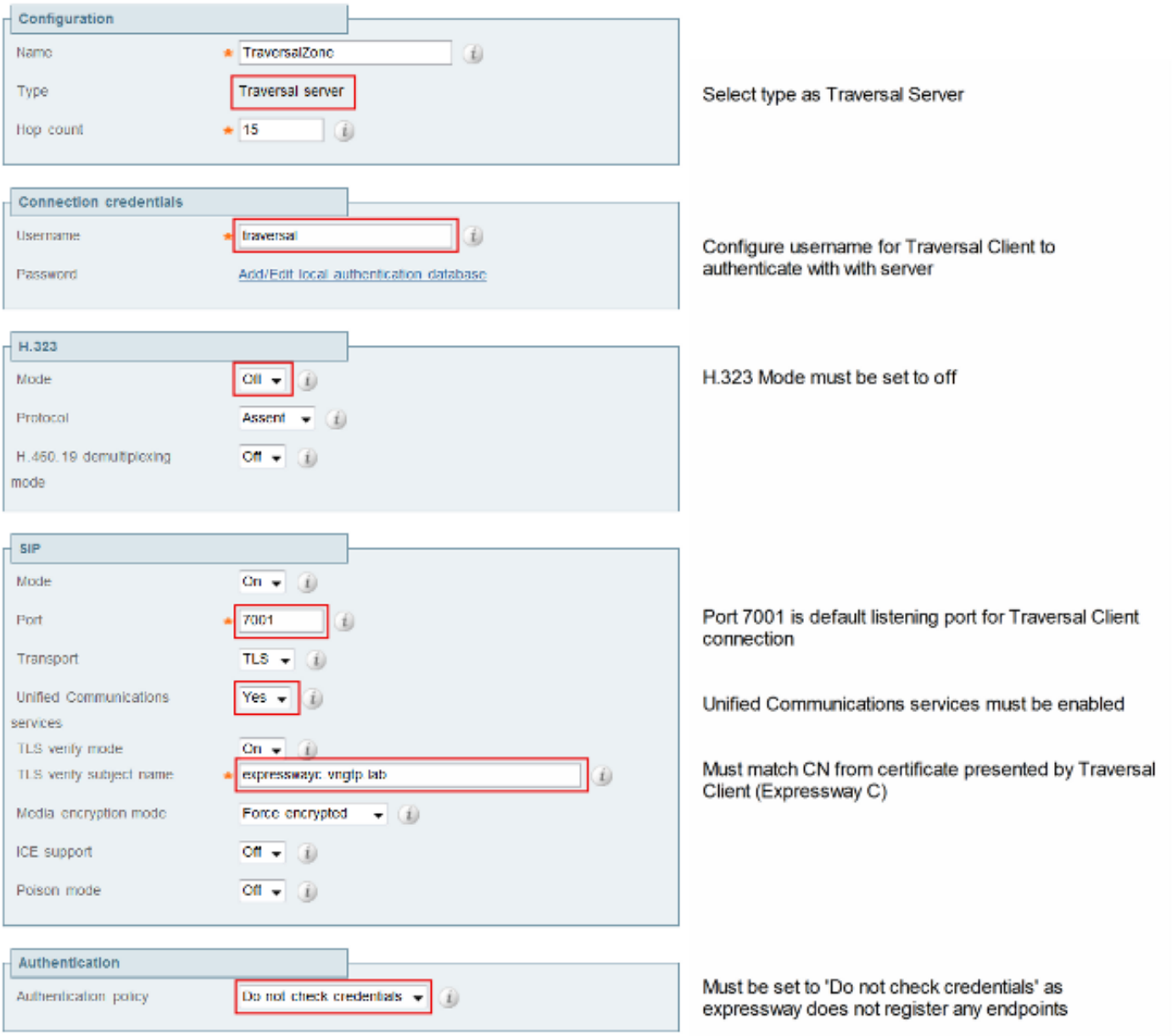
Zona del Traversal

La zona del Traversal consiste en el servidor del Traversal (**expresswayE**), situado en el De-Militarized Zone (DMZ), y el cliente del Traversal (**expresswayC**), situado dentro de la red:



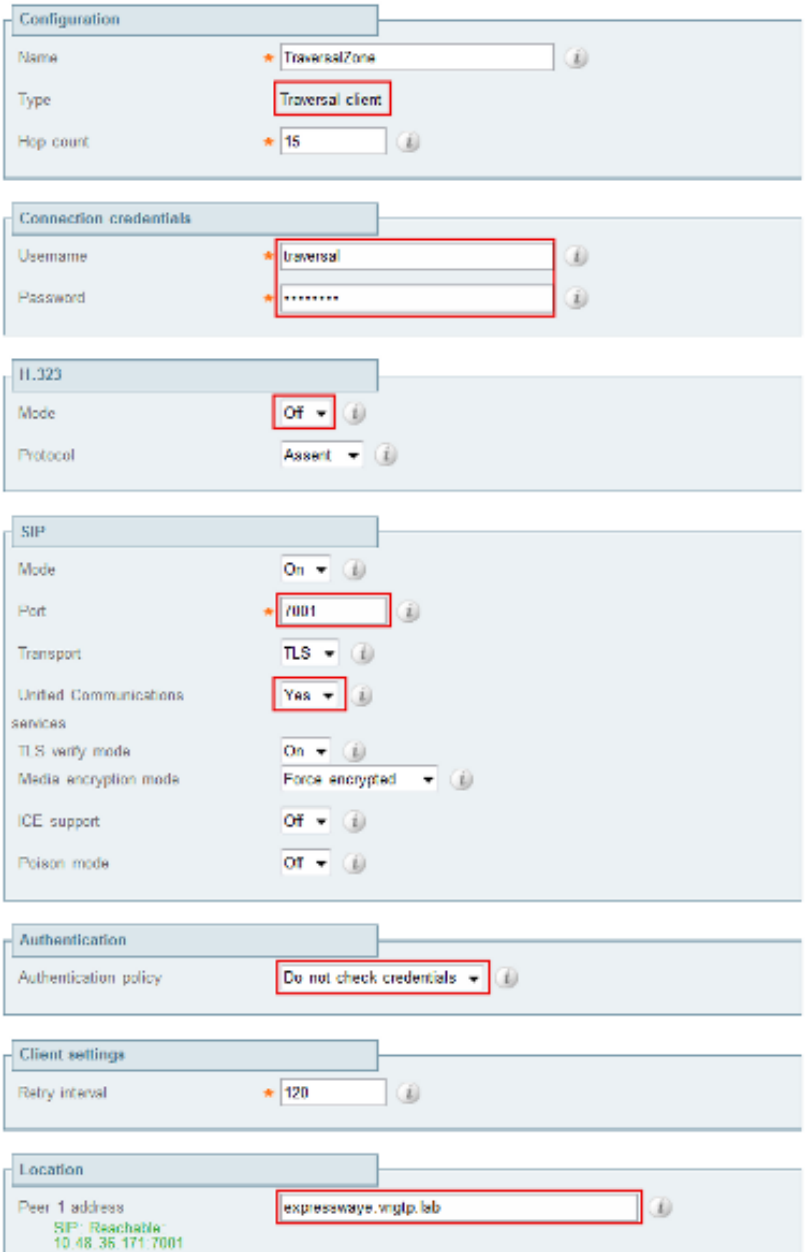
Servidor del Traversal

El servidor del Traversal está situado en la configuración de la zona en la autopista E:



Cliente del Traversal

El cliente del Traversal está situado en la configuración de la zona en el C de la autopista:



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 los servicios de voz

El usuario abre una sesión siempre con **userid@domain4**, pues no debe haber diferencia en la experiencia del usuario cuando interno o externo. Esto significa que si **domain1** es diferente de **domain4**, usted debe configurar el dominio de los servicios de voz en el cliente del Jabber. Esto es porque la porción del dominio del login se utiliza para descubrir los servicios perimetrales de Colaboración usando las operaciones de búsqueda del expediente del servicio (SRV).

El cliente realiza una interrogación del expediente del Domain Name System (DNS) SRV para el **_collab-edge. _tls.<domain>**. Esto implica que cuando el dominio de la identificación del usuario del login es diferente que el dominio de la autopista E, usted debe utilizar el servicio de voz Domain Configuration (Configuración del dominio). El Jabber utiliza esta configuración para descubrir el borde de la Colaboración y los UD.

Hay las opciones múltiples que usted puede utilizar para completar esta tarea:

1. Agregue esto como parámetro cuando usted instala el Jabber vía la interfaz de los servicios de media (MSI):

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

2. Navegue hasta el **%APPDATA% > Cisco > las Comunicaciones unificadas > Jabber > CFS > los 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 experimental es soportado solamente y no oficialmente por Cisco.

3. Edite el **archivo jabber-config.xml**. Esto requiere que el cliente abra una sesión internamente primero. El generador del archivo de JabberConfig se puede utilizar para esto:

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

4. También, los clientes móviles del Jabber pueden ser configurados con el dominio de los servicios de voz francamente así que no necesitan iniciar sesión internamente primero. Esto se explica en el despliegue y la guía de instalación en el capítulo de la detección del servicio. Usted debe crear una configuración URL que el usuario necesite hacer clic:
`ciscojabber://provision?ServicesDomain=domain4&VoiceServicesDomain=domain1`

   Nota: Se requiere para utilizar el dominio de los servicios de voz porque usted debe asegurarse de que usted realice las operaciones de búsqueda para los expedientes del borde SRV de la Colaboración para el dominio exterior (**domain1**).

Expedientes DNS

Esta sección describe los ajustes de la configuración para el externo y los expedientes de los DN internos.

Externo

Tipo	Entrada	Resoluciones a
Expediente SRV	_collab-edge._tls.domain1	ExpresswayE.domain1
Un expediente	ExpresswayE.domain1	Dirección IP ExpresswayE

Es importante observar eso:

- Los expedientes SRV vuelven un nombre de dominio completo (FQDN) y no una dirección IP.
- El FQDN que es vuelto por los expedientes SRV debe hacer juego el FQDN real de la autopista-e, o la blanco del expediente SRV es un CNAME y las puntas del alias a un servidor dentro del mismo dominio que la autopista-e (Id. de bug Cisco pendiente CSCuo82526).

Se requiere esto porque la autopista-e fija un Cookie en el cliente con su propio dominio (**domain1**), y si esto no hace juego con el dominio que es vuelto por el FQDN, el cliente no valida esto. El Id. de bug Cisco CSCuo83458 se abre como mejora para este escenario.

Interno

Tipo	Entrada	Resoluciones a
Expediente SRV	_cisco-uds._tcp.domain1	cucm.domain3

Un expediente	cucm.domain3	Dirección IP CUCM

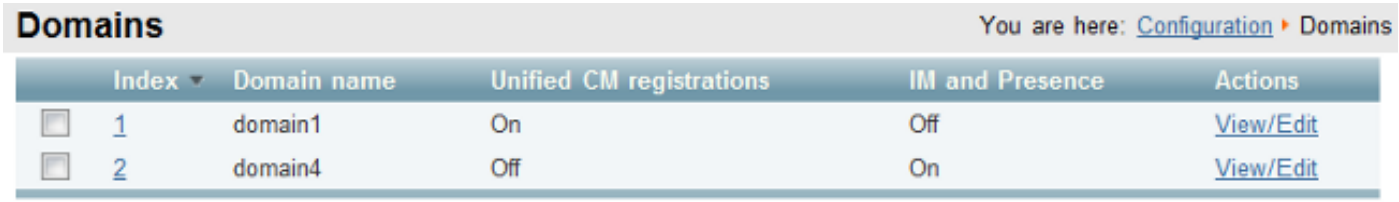
Porque el dominio de los servicios de voz se fija a **domain1**, el Jabber integra **domain1** en el URL transformado para la detección de la configuración del borde de la Colaboración (**consiga el edge_config**). Una vez que está recibida, la autopista-C realiza una interrogación del expediente SRV UD para **domain1** y vuelve los expedientes en el mensaje de **200 AUTORIZACIONES**.

Tipo	Entrada	Resoluciones a
SRV	_cisco-uds._tcp.domain4	cucm.domain3
Un expediente	cucm.domain3	Dirección IP CUCM

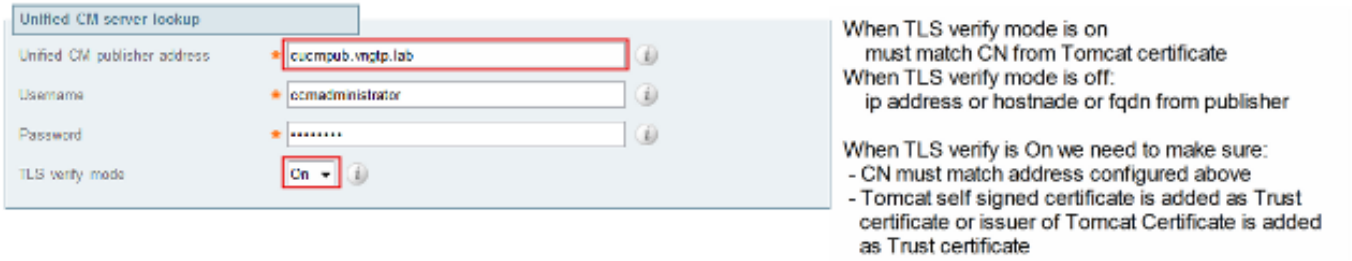
Cuando el cliente es en red, la detección de registro SRV UD se requiere para **domain4**.

Dominios del SORBO en la autopista-C

Usted debe agregar estos dominios del Session Initiation Protocol (SIP) en la autopista-C y habilitarlos para MRA:



Servidores del nombre de host/de la dirección IP CUCM



Cuando usted configura los servidores del administrador de las Comunicaciones unificadas de Cisco (CUCM), hay dos escenarios:

- Si su autopista-C (**domain2**) se configura con el mismo dominio que su servidor CUCM (**domain3**), usted puede configurar sus servidores CUCM (**sistema > servidores**) con:

  La dirección IPEl nombre de hostEl FQDN
- Si la autopista-C (**domain2**) se configura con un diverso dominio que el servidor CUCM (**domain3**), después usted debe configurar los servidores CUCM con:

  La dirección IPEl FQDN

Se requiere esto porque cuando la autopista-C descubre que los servidores CUCM y el nombre de host está vueltos, realiza una búsqueda de DNS para **hostname.domain2**, que no trabaja si **domain2** y **domain3** son diferentes.

Certificados

Independientemente de los requisitos generales del certificado, algunas cosas se deben agregar a los nombres alternos sujetos (SAN) de los Certificados:

- Autopista-C

  Los alias del nodo de la charla que se configuran en los servidores IM&P deben ser agregados. Esto se requiere solamente para las implementaciones de la federación de las Comunicaciones unificadas XMPP que se preponen utilizar Transport Layer Security (TLS) y la charla del grupo. Esto se agrega automáticamente al pedido de firma de certificado (CSR), con tal que haya descubierto los servidores IM&P ya.

  Los nombres, en el formato FQDN, de todos los perfiles de seguridad del teléfono en los CUCM que se configuran para TLS cifrado y se utilizan para los dispositivos que requieren el Acceso Remoto deben ser agregados.
  Nota: El formato FQDN se requiere solamente cuando su Certificate Authority (CA) no permite el sintaxis del nombre de host en el SAN.
- Autopista-e

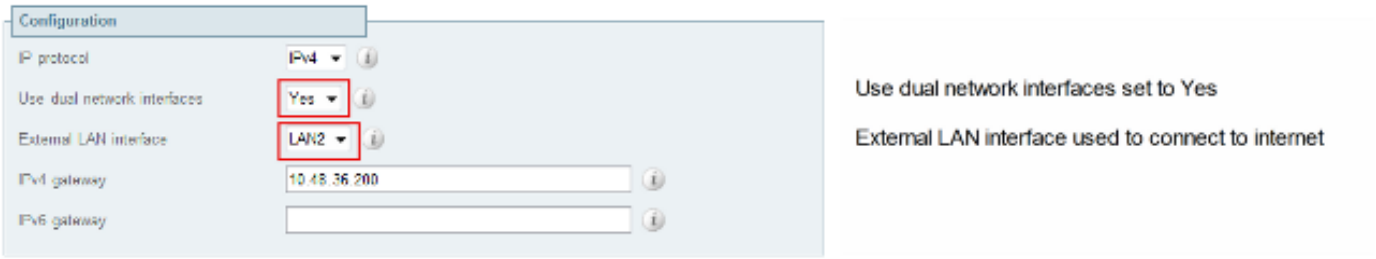
  El dominio usado para la detección del servicio (**domain1**) debe ser agregado. Dominios de la federación XMPP.Los alias del nodo de la charla que se configuran en los servidores IM&P deben ser agregados. Esto se requiere solamente para las implementaciones de la federación de las Comunicaciones unificadas XMPP que se preponen utilizar TLS y la charla del grupo. Éstos se pueden copiar del CSR que se genera en la autopista-C.

NIC dual

Esta sección describe los ajustes de la configuración cuando se utiliza el Network Interface Cards dual (NIC).

Dos interfaces

Cuando usted configura la autopista-e para utilizar las interfaces de la red duales, es importante asegurarse de que ambas interfaces están configuradas y utilizadas.



Cuando las **interfaces de la red duales del uso** se configuran con un valor del **sí**, la autopista-e escucha solamente en la interfaz interna la comunicación XMPP con la autopista-C. Así, usted debe asegurarse de que esta interfaz esté configurada y trabaje correctamente.

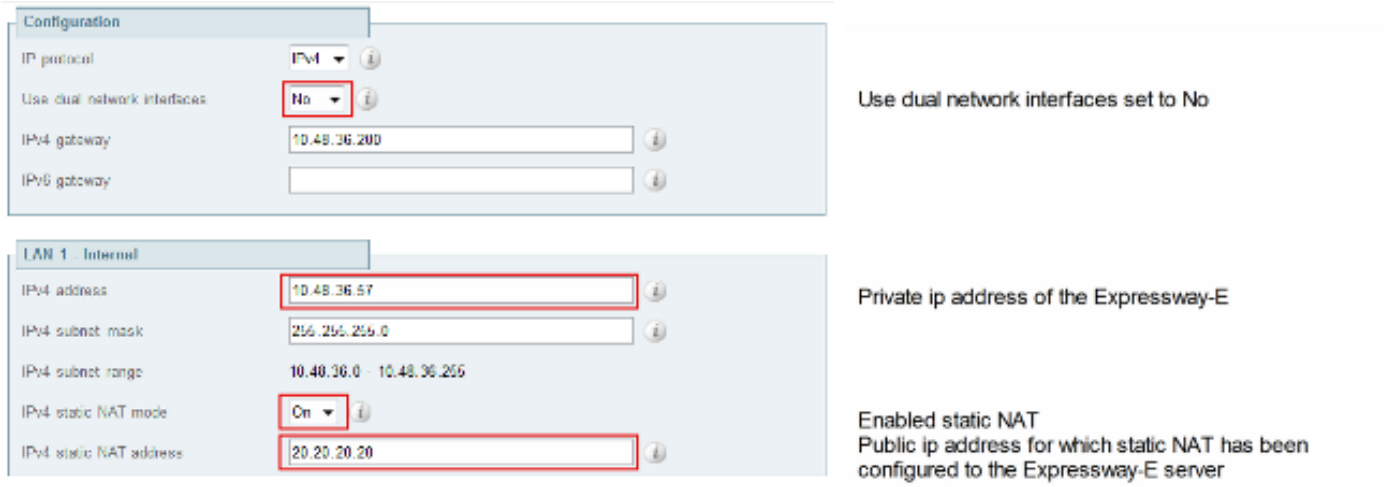
Una interfaz - IP Address público

Cuando se utiliza solamente una interfaz, y usted configura la autopista-e con un IP Address

público, ningunas Consideraciones especiales deben ser tomadas.

Una interfaz - IP Address privado

Cuando se utiliza solamente una interfaz, y usted configura la autopista-e con un IP Address privado, usted debe configurar el direccionamiento de la traducción de dirección de red estática (NAT) también:



En esta situación, es importante asegurar eso:

- La autopista-C es permitida por el Firewall enviar el tráfico al IP Address público. Esto se conoce como *reflexión NAT*.

- La zona del cliente del Traversal en la autopista-C se configura con una dirección de peer que haga juego el direccionamiento NAT estática en la autopista-e, que es **20.20.20.20** en este caso.

  Consejo: Más información sobre las implementaciones de red avanzada está disponible en el **apéndice 4 del** Guía de despliegue de la configuración básica del servidor del comunicación mediante video del Cisco TelePresence (control con la autopista).

Verificación

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

Troubleshooting

Esta sección proporciona la información que usted puede utilizar para resolver problemas su configuración.

Algunos escenarios específicos se cubren en esta sección, pero usted puede también utilizar el analizador de las soluciones de la Colaboración que proporciona una vista detallada de toda la comunicación para los intentos de inicio de sesión MRA y de la información de Troubleshooting basada en sus registros de diagnóstico.

Zona del Traversal

Cuando configuran a la dirección de peer pues una dirección IP o la dirección de peer no hace juego el Common Name (CN), usted ve esto en los 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, usted ve esto en los registros de la autopista-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 se habilita el NIC dual pero la segunda interfaz no se utiliza ni está conectada, la autopista-C no puede conectar con la autopista-e para la comunicación XMPP sobre el puerto 7400, y los registros de la autopista-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 es vuelto por las operaciones de búsqueda del expediente SRV para el borde de la Colaboración no hace juego el FQDN que se configura en la autopista-e, la demostración de los registros del Jabber 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 la autopista-e, usted puede ver para qué dominio se fija el 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 del SORBO

Cuando los dominios requeridos del SORBO no se agregan en la autopista-C, la autopista-e no valida los mensajes para este dominio y en los registros de diagnóstico usted ve un mensaje **prohibido 403** que se envíe 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"
```