Configurez l’accès mobile et à distance grâce à Expressway/VCS dans un déploiement multidomaine

Contenu

Introduction

Ce document décrit comment configurer le Serveur de communication vidéo (VCS) Cisco TelePresence pour un accès à distance mobile (MRA) lorsque plusieurs domaines sont utilisés.

La configuration du MRA lorsqu’il n’y a qu’un seul domaine est relativement simple, et vous pouvez suivre les étapes indiquées dans le guide de déploiement. Lorsque le déploiement touche plusieurs domaines, il devient plus complexe. Le présent document n’est pas un guide de configuration, mais il décrit tout de même les aspects importants dont il faut tenir compte lorsque plusieurs domaines sont concernés. La configuration principale est indiquée dans le guide de déploiement du serveur de communication vidéo Cisco TelePresence.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

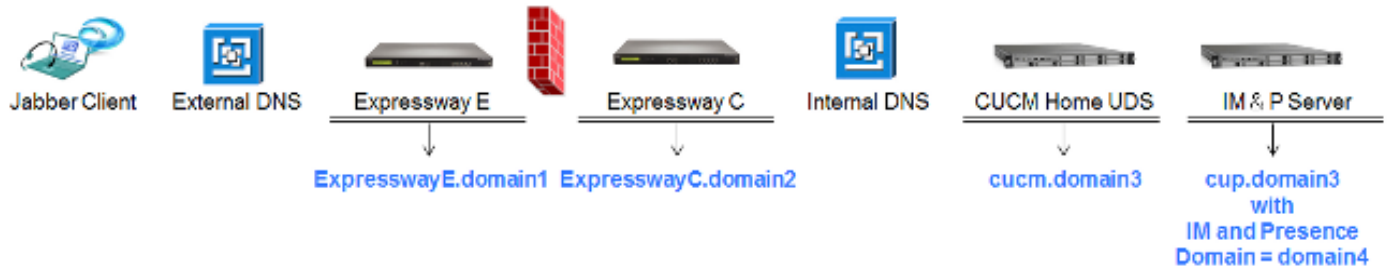
Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

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.

Configuration

Utilisez les renseignements décrits dans la présente section pour configurer le VCS.

Diagramme du réseau

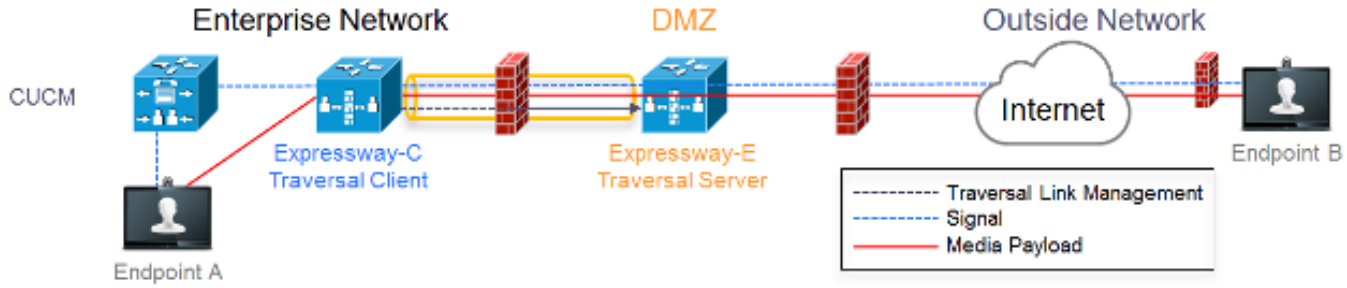


Voici un bref aperçu des différents domaines :

- **Domaine1 – C'est le domaine Edge qui est utilisé par le client afin de découvrir l'emplacement du serveur Edge et par lequel il découvre le Service de données utilisateur (SDU).**
- **Domaines 2 et 3 – Ils sont utilisés pour découvrir les serveurs.**
- **Domaine 4 – Il s'agit du domaine de messagerie instantanée et de présence (IM&P), qui est utilisé par la plateforme extensible de communications (XCP) et du trafic du protocole Messagerie et présence extensibles (XMPP).**

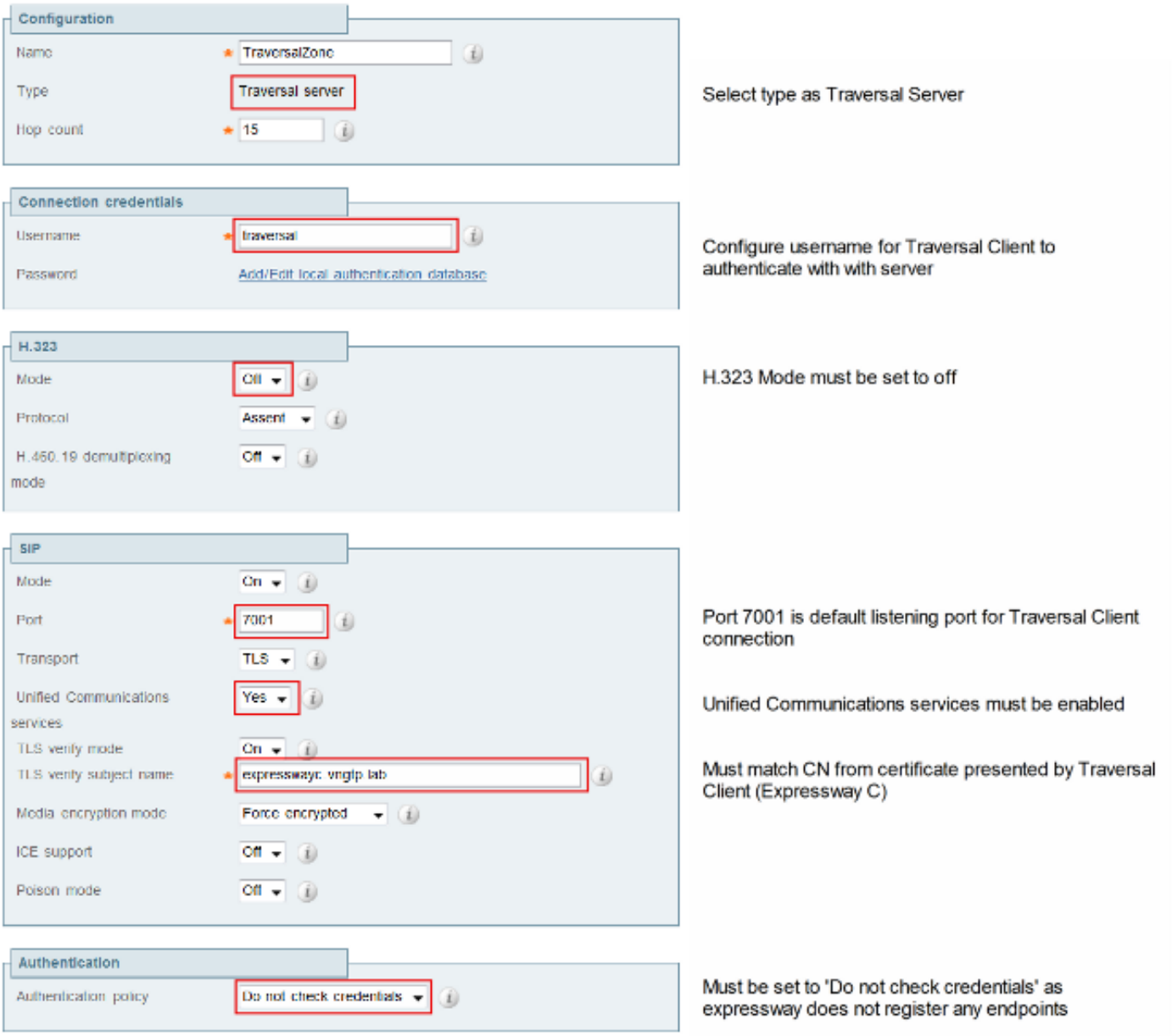
Zone de traversée

La zone de traversée comprend le serveur de traversée (**Expressway-E**), situé dans la zone démilitarisée (DMZ), et le client de traversée (**Expressway-C**), situé dans le réseau :



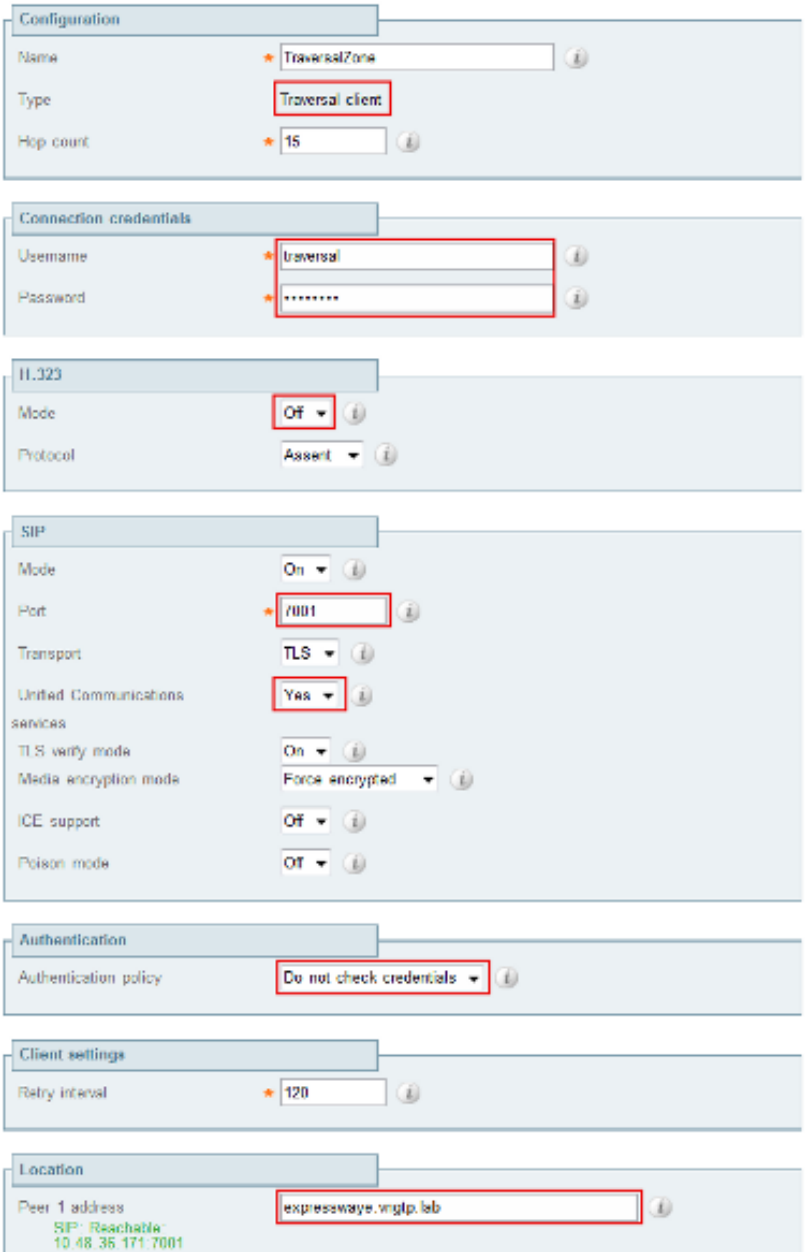
Serveur de traversée

Le serveur de traversée se trouve dans la zone de configuration de l'Expressway-E :



Client de traversée

Le client de traversée est situé dans la zone de configuration de l'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)

Domaine de services téléphoniques

L'utilisateur se connecte toujours par **userid@domain4**, car il ne devrait y avoir aucune différence dans l'expérience utilisateur, que ce soit à l'intérieur ou à l'extérieur. Cela signifie que si le **domaine 1 est différent du domaine 4**, vous devriez configurer le domaine des services téléphoniques dans le client Jabber. C'est que la partie domaine de la connexion est utilisée pour découvrir les services de collaboration Edge à l'aide des requêtes d'enregistrements.

Le client effectue une requête d'enregistrement SRV du DNS pour **_collab-edge._tls.<domain>**. Cela signifie que, lorsque le domaine de l'identifiant de connexion de l'utilisateur est différent du domaine de l'Expressway-E, vous devez alors utiliser la configuration du domaine des services téléphoniques. Jabber utilise cette configuration pour découvrir le Collaboration Edge et l'UDS.

Vous pouvez utiliser plusieurs options pour réaliser cette tâche :

1. Ajouter ce qui suit comme paramètre lorsque vous installez Jabber par l'interface de services multimédias (MSI) :

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

2. Accédez à **%APPDATA% > Cisco > Unified Communications > Jabber > CSF > Config** et créer le fichier **jabber-config-user.xml dans le répertoire :**

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

Note: Cette méthode est en essai seulement et n'est pas officiellement prise en charge par Cisco.

3. Modifier le fichier **jabber-config.xml.** Ainsi, le client se connecte d'abord à l'interne. Le [générateur de fichiers de configuration Jabber] peut être utilisé pour ceci :

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

4. Aussi, les clients mobiles de Jabber peuvent être configurés d'avance grâce au domaine des services téléphoniques; ils n'ont donc pas à se connecter d'abord à l'interne. Cette procédure est expliquée dans le guide de déploiement et d'installation au chapitre [« Découverte du service ».] Vous devez créer une URL de configuration sur laquelle l'utilisateur devra cliquer : `ciscojabber://provision?ServicesDomain=domain4&VoiceServicesDomain=domain1`

Note: Il est nécessaire d'utiliser le domaine des services téléphoniques, parce que vous devez vous assurer que vous effectuez une requête pour les enregistrements SRV de Collaboration Edge pour le domaine extérieur (**domaine 1**).

Enregistrements DNS

Cette section décrit les paramètres de configuration des enregistrements DNS externes et internes.

Externe

Type	Entrée	Mène à
Enregistrement SRV	_collab-edge_tls.domain1	ExpresswayE.domain1
Un enregistrement	ExpresswayE.domain1	Adresse IP Expressway-E

Il importe de noter que :

- Les enregistrements SRV renvoient un nom de domaine complètement qualifié (FQDN) et non une adresse IP.

- Le FQDN retourné par les enregistrements SRV doit correspondre au FQDN réel de l'Expressway-E, ou la cible d'enregistrement SRV désigne un CNAME et le nom en question représente un serveur dans le même domaine que l'Expressway-E (bogue de Cisco CSCuo82526 en attente).

Ceci est nécessaire, car l'Expressway-E configure un témoin sur le client avec son propre

domaine (**domaine 1**), et s'il ne correspond pas au domaine retourné par le FQDN, le client ne l'accepte pas. Le bogue de Cisco [CSCuo83458 est ouvert à titre d'amélioration pour ce scénario.]

Interne

Type	Entrée	Mène à
Enregistrement SRV	_cisco-uds._tcp.domain1	cucm.domain3
Un enregistrement	cucm.domain3	CUCM de l'adresse IP

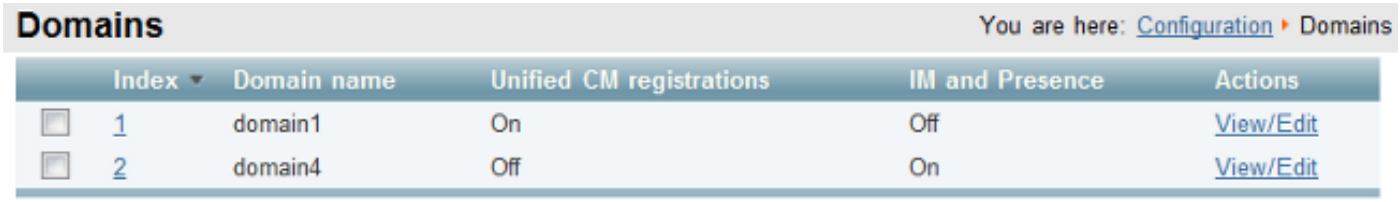
Vu que le domaine des services téléphoniques est configuré selon le **domaine 1**, Jabber intègre le **domaine 1 dans l'URL transformée pour découvrir la configuration de Collaboration Edge (obtenir edge_config**). Une fois reçue, l'Expressway-C effectue une requête d'enregistrements SRV UDS pour le **domaine 1 et renvoie les enregistrements dans le message 200 OK.**

Type	Entrée	Mène à
SRV	_cisco-uds._tcp.domain4	cucm.domain3
Un enregistrement	cucm.domain3	CUCM de l'adresse IP

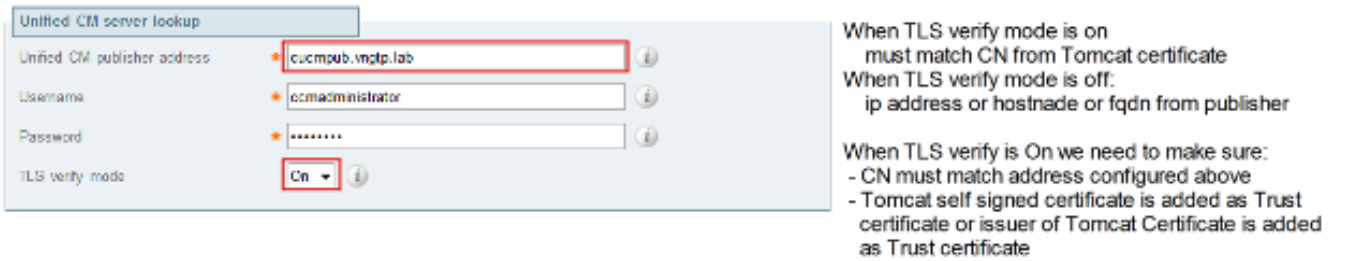
Lorsque le client est sur Internet, il faut découvrir les enregistrements SRV UDS pour le **domaine 4**.

Domaines du SIP sur Expressway-C

Vous devez ajouter les domaines de protocole d'ouverture de session (SIP) sur l'Expressway-C et autoriser un MRA :



Serveurs de l'adresse IP ou du nom d'hôte du CUCM



Lorsque vous configurez les serveurs de solutions Cisco Unified Communications Manager (CUCM), il existe deux scénarios :

- Si votre Expressway-C (**domaine 2**) est configuré selon le même domaine que votre serveur CUCM (**domaine 3**), vous pouvez configurer vos serveurs CUCM (**système > serveurs**) grâce à :

  l'adresse IPle nom d'hôtele FQDN
- Si l'Expressway-C (**domaine 2**) est configuré selon un domaine différent de celui du serveur

CUCM (**domaine 3**), vous devez donc configurer les serveurs CUCM grâce à :

l'adresse IPle FQDN

Ceci est nécessaire, car lorsque l'Expressway-C détecte les serveurs CUCM, retournant ainsi le nom d'hôte, le système effectue une requête DNS pour **hostname.domain2**, ce qui ne fonctionne pas si **le domaine 2 et le domaine 3 sont différents.**

Certificats

Hormis les exigences générales des certificats, il faut ajouter quelques petites choses aux autres noms des sujets (SAN) des certificats :

- Expressway-C

  Le pseudo des nœuds de clavardage configurés sur les serveurs IM&P doit être ajouté. C'est nécessaire seulement pour les déploiements de la fédération des communications unifiées XMPP qui ont l'intention d'utiliser le Transport Layer Security (TLS) et le clavardage de groupe. L'ajout se fait automatiquement pour la demande de signature de certificat (CSR), à condition que les serveurs IM&P aient été détectés.

  Les noms, dans le format FQDN, de tous les profils de sécurité téléphonique dans les CUCM configurés pour le TLS chiffré et qui servent aux appareils nécessitant un accès à distance doivent être ajoutés.
  Note: Le format du FQDN est seulement nécessaire lorsque votre autorité de certification (CA) n'autorise pas la syntaxe du nom d'hôte dans les SAN.
- Expressway-E

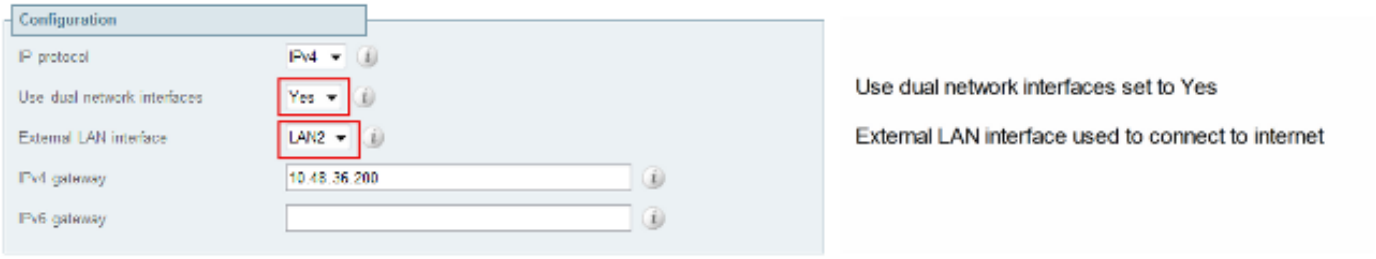
  Le domaine utilisé pour la découverte de service (**domaine 1**) doit être ajouté. Domaines de la fédération des XMPP.Le pseudo des nœuds de clavardage configurés sur les serveurs IM&P doit être ajouté. C'est nécessaire seulement pour les déploiements de la fédération des communications unifiées XMPP qui ont l'intention d'utiliser le TLS et le clavardage de groupe. Ils peuvent être copiés à partir de la CSR générée sur l'Expressway-C.

Double NIC

Cette section décrit les paramètres de configuration lorsque deux cartes d'interface réseau (NIC) sont utilisées.

Deux interfaces

Lorsque vous configurez l'Expressway-E pour utiliser les deux interfaces réseau, il importe de s'assurer que les deux interfaces sont configurées et utilisées.



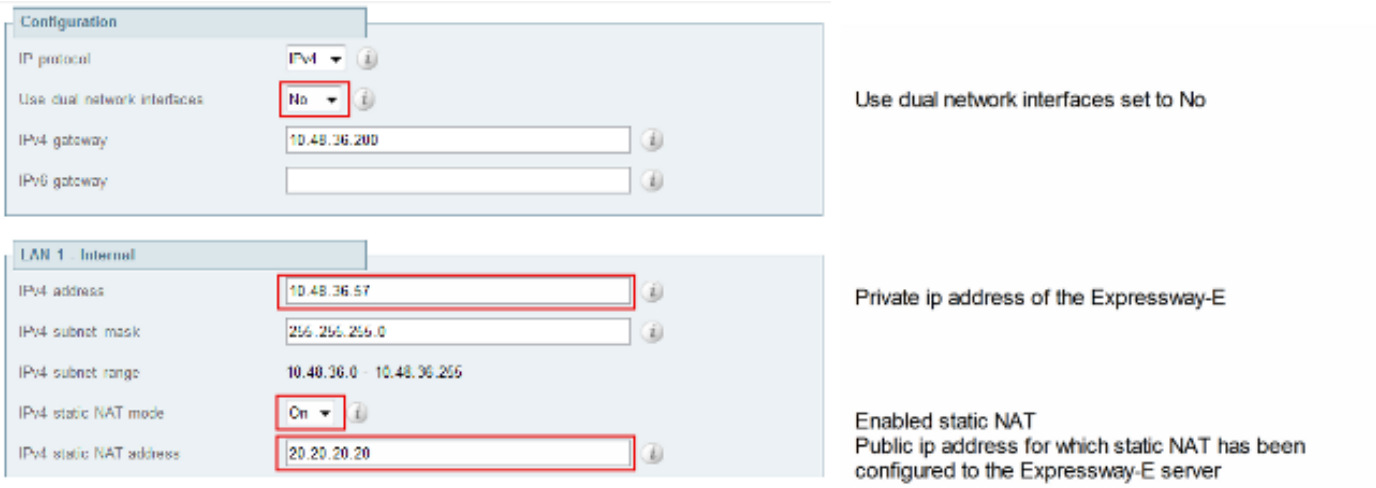
Lorsque la valeur **Use dual network interfaces** est configurée avec **Yes**, l'Expressway-E n'écoute que l'interface interne pour la communication XMPP avec l'Expressway-C. Par conséquent, vous devez vous assurer que cette interface est configurée et fonctionne correctement.

Une interface – adresse IP publique

Lorsqu'une seule interface est utilisée et que vous configurez l'Expressway-E en utilisant une adresse IP publique, vous n'avez à tenir compte d'aucune considération particulière.

Une interface – adresse IP privée

Lorsqu'une seule interface est utilisée et que vous configurez l'Expressway-E en utilisant une adresse IP privée, vous devez également configurer l'adresse statique de traduction d'adresses réseau (NAT) :



Dans ce cas, il importe de veiller à ce qui suit :

- Le pare-feu autorise l'Expressway-C à laisser passer le trafic vers l'adresse IP publique. Il s'agit de ce qu'on appelle la *réflexion NAT*.
- La zone du client de traversée sur l'Expressway-C est configurée au moyen d'une adresse d'un pair qui correspond à l'adresse statique de NAT sur l'Expressway-E, soit, dans la présente situation, **20.20.20.20.**

  Astuce : Vous aurez plus de renseignements sur les déploiements de réseaux avancés dans **l'annexe 4 du** Guide de déploiement de la configuration de base du serveur de communication vidéo Cisco TelePresence (contrôle avec Expressway).

Vérification

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Des scénarios précis sont traités dans la présente section, mais vous pouvez également utiliser l'analyseur de solutions de collaboration, qui offre un affichage détaillé des communications liées aux tentatives de connexion MRA et des données de dépannage reposant sur les journaux de diagnostic.

Zone de traversée

Lorsque l'adresse d'un pair est configurée comme une adresse IP ou si elle ne correspond pas au nom commun (CN), vous verrez ce qui suit dans les journaux :

```
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"
```

Lorsque le mot de passe est incorrect, vous verrez ce qui suit dans les journaux 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"
```

Double NIC

Quand la fonction double NIC est activée, mais si la deuxième interface n'est pas utilisée ou connectée, l'Expressway-C ne parviendra pas à se connecter à l'Expressway-E aux fins des communications de XMPP sur le port 7400, et donc les journaux Expressway-C afficheront ce qui suit :

```
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

Si le FQDN qui est retourné à la suite d'une requête des enregistrements SRV pour Collaboration Edge ne correspond pas au FQDN configuré sur l'Expressway-E, les journaux de Jabber afficheront l'erreur suivante :

```
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
```

Dans les journaux de diagnostic pour l'Expressway-E, vous pouvez voir pour quel domaine le témoin est configuré dans le message HTTPS :

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

Domaines SIP

Lorsque les domaines SIP requis ne sont pas ajoutés sur l'Expressway-C, l'Expressway-E n'accepte pas les messages pour ce domaine, et vous verrez dans les journaux de diagnostic le message d'erreur 403 qui est envoyé au client :

```
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"
```