Configurez le mobile et l'Accès à distance par Expressway/VCS dans un déploiement de Multi-domaine

Contenu

Introduction

Ce document décrit comment configurer le serveur de communication vidéo Cisco TelePresence (VCS) pour l'Accès à distance mobile (MRA) quand des plusieurs domaines sont utilisés.

Le MRA a installé quand il y a seulement un domaine est relativement simple, et vous pouvez suivre les étapes qui sont documentées du guide de déploiement. Quand le déploiement implique des plusieurs domaines, il devient plus complexe. Ce document n'est pas un guide de configuration, mais il décrit les importants aspects quand les plusieurs domaines sont impliqués. La configuration principale est documentée du guide de déploiement du serveur de communication vidéo Cisco TelePresence (VCS).

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

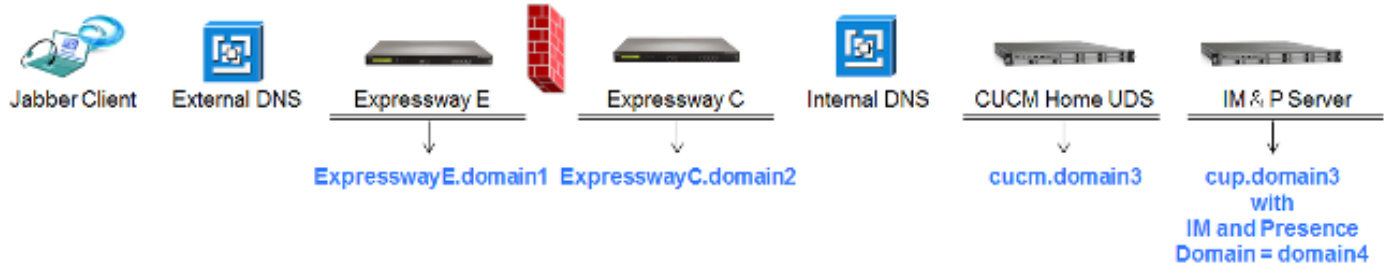
Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Configurez

Utilisez les informations qui sont décrites dans cette section afin de configurer le VCS.

Diagramme du réseau

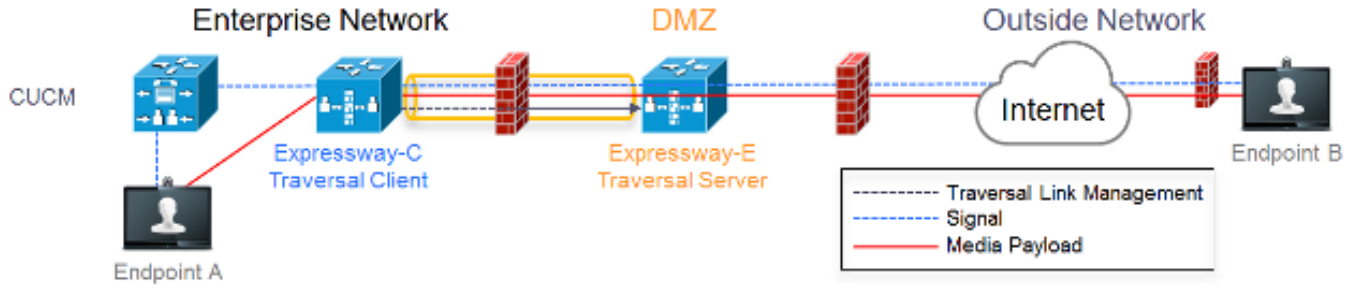


Voici un aperçu court des différents domaines :

- **domain1** - C'est le domaine de périphérie qui est utilisé par le client afin de découvrir l'emplacement du serveur de périphérie et par ce qui il découvre le service de données d'utilisateur (UDS).
- **domain2 et domain3** - Ceci est utilisé pour la détection de serveur.
- **domain4** - C'est Messagerie et présence instantanées (le domaine IM&P) qui est utilisé par la plate-forme extensible de transmissions (XCP) et le trafic extensible de Protocol de Messagerie et de présence (XMPP).

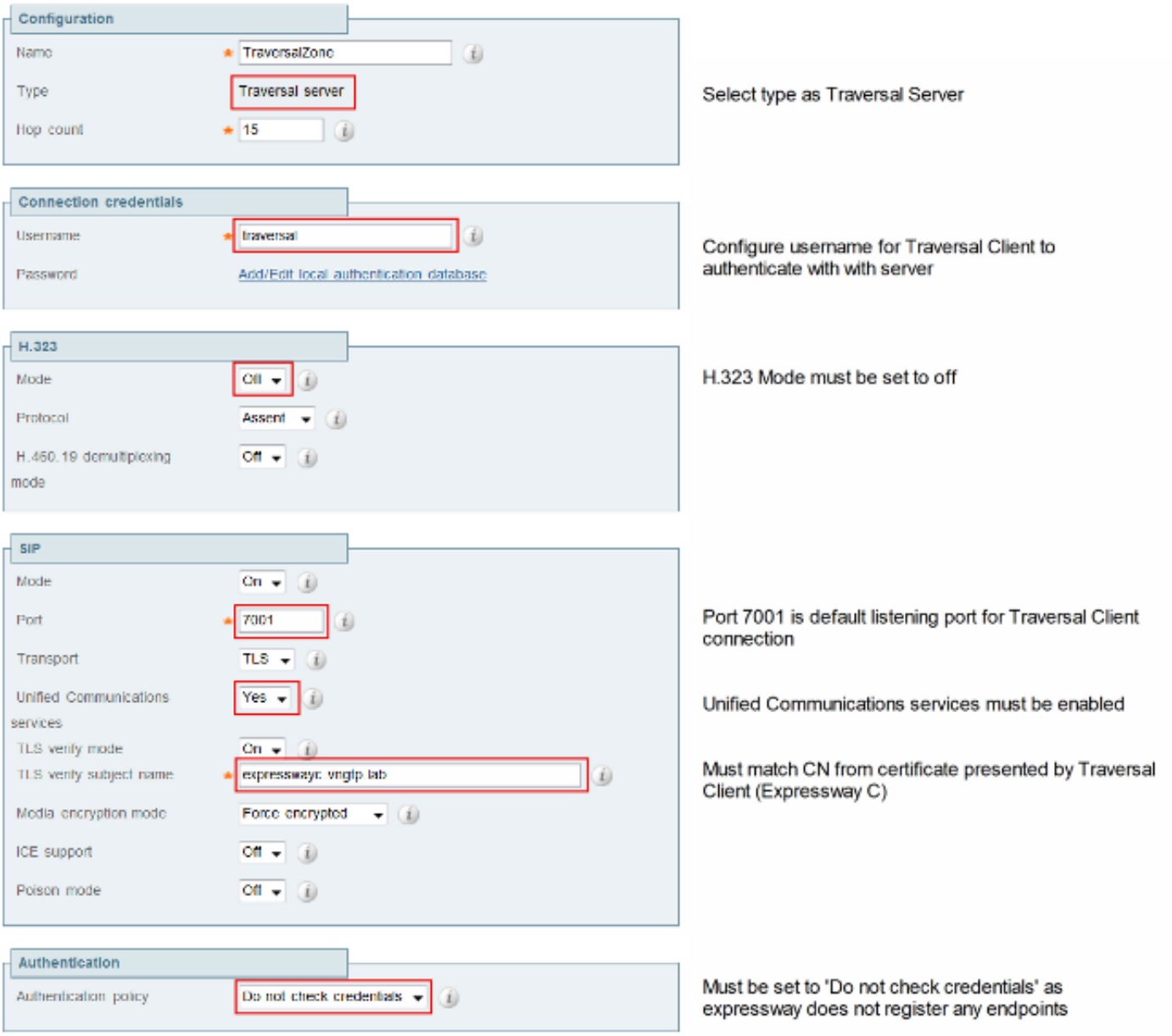
Zone de traversée

La zone de traversée comprend le serveur de traversée (**expresswayE**), situé dans la zone démilitarisée (DMZ), et le client de traversée (**expresswayC**), situé à l'intérieur du réseau :



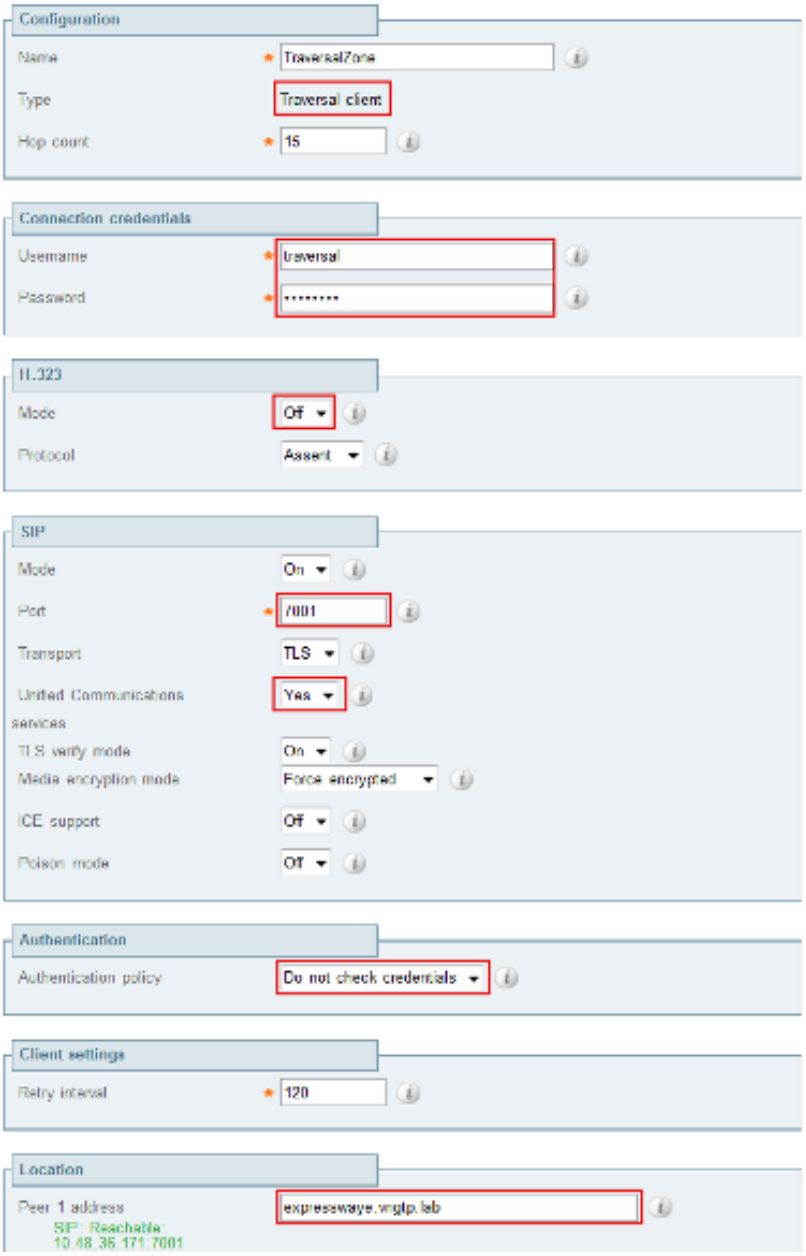
Serveur de traversée

Le serveur de traversée se trouve dans la configuration de zone sur l'autoroute E :



Client de traversée

Le client de traversée se trouve dans la configuration de zone sur le C d'autoroute :



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 vocaux

L'utilisateur ouvre une session toujours avec **userid@domain4**, car il ne devrait y avoir aucune différence dans l'expérience utilisateur quand à l'intérieur ou dehors. Ceci signifie que si **domain1** est différent de **domain4**, vous devez configurer le domaine de services vocaux dans le client de Jabber. C'est parce que la partie de domaine de la procédure de connexion est utilisée afin de découvrir les services de périphérie de Collaboration utilisant des consultations d'enregistrement du service (SRV).

Le client exécute une requête d'enregistrement SRV de Système de noms de domaine (DNS) pour le **_collab-edge. _tls.<domain>**. Ceci implique que quand le domaine de l'user-id de procédure de connexion est différent que le domaine de l'autoroute E, vous devez utiliser la configuration de domaine de service vocal. Le Jabber emploie cette configuration afin de découvrir la périphérie de Collaboration et l'UDS.

Il y a des nombreuses options que vous pouvez employer afin de se terminer cette tâche :

1. Ajoutez ceci comme paramètre quand vous installez le Jabber par l'intermédiaire de l'interface de services de médias (MSI) :

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

2. Naviguez vers **%APPDATA% > Cisco > des transmissions > Jabber > CSF > config unifiés**, et créez ce **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>
```

Remarque: Cette méthode expérimentale et est seulement pas officiellement prise en charge par Cisco.

3. Éditez le **fichier jabber-config.xml**. Ceci exige que le client ouvre une session intérieurement d'abord. Le générateur de fichier de JabberConfig peut être utilisé pour ceci :

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

4. En outre, des clients mobiles de Jabber peuvent être configurés avec le domaine de services vocaux d'avance ainsi ils n'ont pas besoin d'ouvrir une session intérieurement d'abord. Ceci est expliqué dans le déploiement et le guide d'installation dans le chapitre de détection de service. Vous devez créer un configuration url qui les besoins de l'utilisateur de cliquer sur :
`ciscojabber://provision?ServicesDomain=domain4&VoiceServicesDomain=domain1`

   Remarque: On l'exige pour utiliser le domaine de services vocaux parce que vous devez s'assurer que vous exécutez la consultation pour les enregistrements SRV de périphérie de Collaboration pour le domaine extérieur (**domain1**).

Enregistrements DNS

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

Externe

Type	Entrée	Résolutions à
Enregistrement SRV	_collab-edge._tls.domain1	ExpresswayE.domain1
Un enregistrement	ExpresswayE.domain1	Adresse IP ExpresswayE

Il est important de noter cela :

- Les enregistrements SRV renvoient un nom de domaine complet (FQDN) et pas une adresse IP.

- Le FQDN qui est retourné par les enregistrements SRV doit apparier le FQDN d'effectif de l'autoroute-e, ou la cible d'enregistrement SRV est un CNAME et les points de pseudonyme à un serveur dans le même domaine que l'autoroute-e (ID de bogue Cisco en suspens CSCuo82526).

Ceci est exigé parce que l'autoroute-e place un Témoin sur le client avec son propre domaine (**domain1**), et si ceci ne s'assortit pas avec le domaine qui est retourné par le FQDN, le client ne reçoit pas ceci. L'ID de bogue Cisco CSCuo83458 est ouvert comme amélioration pour ce scénario.

Interne

Type	Entrée	Résolutions à
Enregistrement SRV	_cisco-uds._tcp.domain1	cucm.domain3
Un enregistrement	cucm.domain3	Adresse IP CUCM

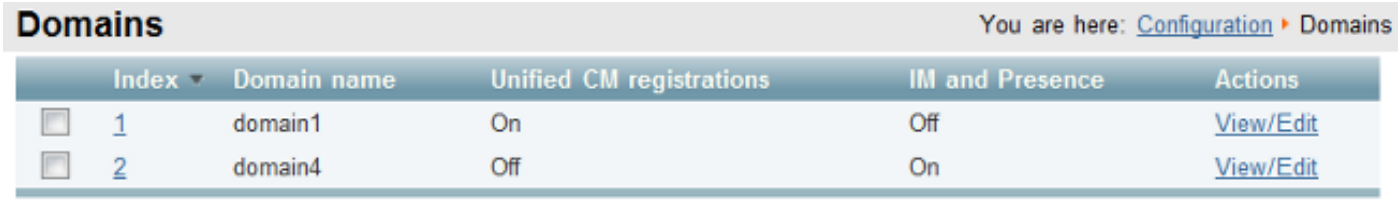
Puisque le domaine de services vocaux est placé à **domain1**, le Jabber encastre **domain1** dans l'URL transformé pour la détection de configuration de périphérie de Collaboration (**obtenez l'edge_config**). Une fois que reçue, l'autoroute-C exécute une requête d'enregistrement SRV UDS pour **domain1** et renvoie les enregistrements dans le message de **200 OKS**.

Type	Entrée	Résolutions à
SRV	_cisco-uds._tcp.domain4	cucm.domain3
Un enregistrement	cucm.domain3	Adresse IP CUCM

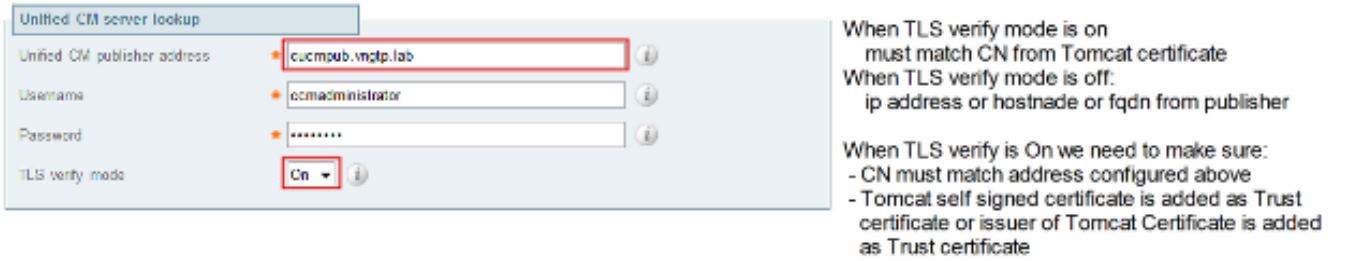
Quand le client est sur le réseau, la détection d'enregistrement SRV UDS est exigée pour **domain4**.

Domaines de SIP sur l'autoroute-C

Vous devez ajouter ces domaines de Protocole SIP (Session Initiation Protocol) sur l'autoroute-C et les activer pour MRA :



Serveurs d'adresse Internet/adresse IP CUCM



Quand vous configurez les serveurs de Cisco Unified Communications Manager (CUCM), il y a deux scénarios :

- Si votre autoroute-C (**domain2**) est configurée avec le même domaine que votre serveur CUCM (**domain3**), vous pouvez configurer vos serveurs CUCM (**système > serveurs**) avec :

  L'adresse IPL'adresse InternetLe FQDN
- Si l'autoroute-C (**domain2**) est configurée avec un domaine différent que le serveur CUCM (**domain3**), alors vous devez configurer les serveurs CUCM avec :

  L'adresse IPLe FQDN

Ceci est exigé parce que quand l'autoroute-C découvre les serveurs CUCM et l'adresse Internet

est retournée, il exécute une consultation de DN pour **hostname.domain2**, qui ne fonctionne pas si **domain2** et **domain3** sont différents.

Certificats

Hormis les conditions requises générales de certificat, quelques choses doivent être ajoutées aux noms secondaires soumis (SAN) des Certificats :

- Autoroute-C

  Les pseudonymes de noeud de conversation qui sont configurés sur les serveurs IM&P doivent être ajoutés. Ceci est seulement exigé pour les déploiements unifiés de fédération des transmissions XMPP qui destinent pour utiliser le Transport Layer Security (TLS) et la discussion de groupe. Ceci est ajouté automatiquement à la demande de signature de certificat (CSR), s'il a déjà découvert les serveurs IM&P.

  Les noms, dans le format FQDN, de tous les profils de degré de sécurité de téléphone dans les CUCM qui sont configurés pour le TLS chiffré et sont utilisés pour les périphériques qui exigent l'Accès à distance doivent être ajoutés.
  Remarque: Le format FQDN est seulement exigé quand votre Autorité de certification (CA) ne permet pas la syntaxe d'adresse Internet dans le SAN.
- Autoroute-e

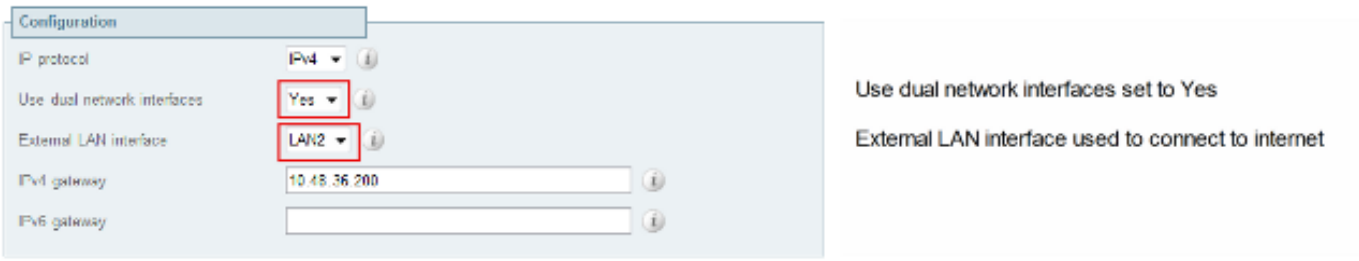
  Le domaine utilisé pour la détection de service (**domain1**) doit être ajouté. Domaines de fédération XMPP.Les pseudonymes de noeud de conversation qui sont configurés sur les serveurs IM&P doivent être ajoutés. Ceci est seulement exigé pour les déploiements unifiés de fédération des transmissions XMPP qui destinent pour utiliser le TLS et la discussion de groupe. Ceux-ci peuvent être copiés du CSR qui est généré sur l'autoroute-C.

Double NIC

Cette section décrit les paramètres de configuration quand les doubles networks interface cards (NIC) sont utilisés.

Deux interfaces

Quand vous configurez l'autoroute-e afin d'utiliser de doubles interfaces réseau, il est important de s'assurer que les deux interfaces sont configurées et utilisées.



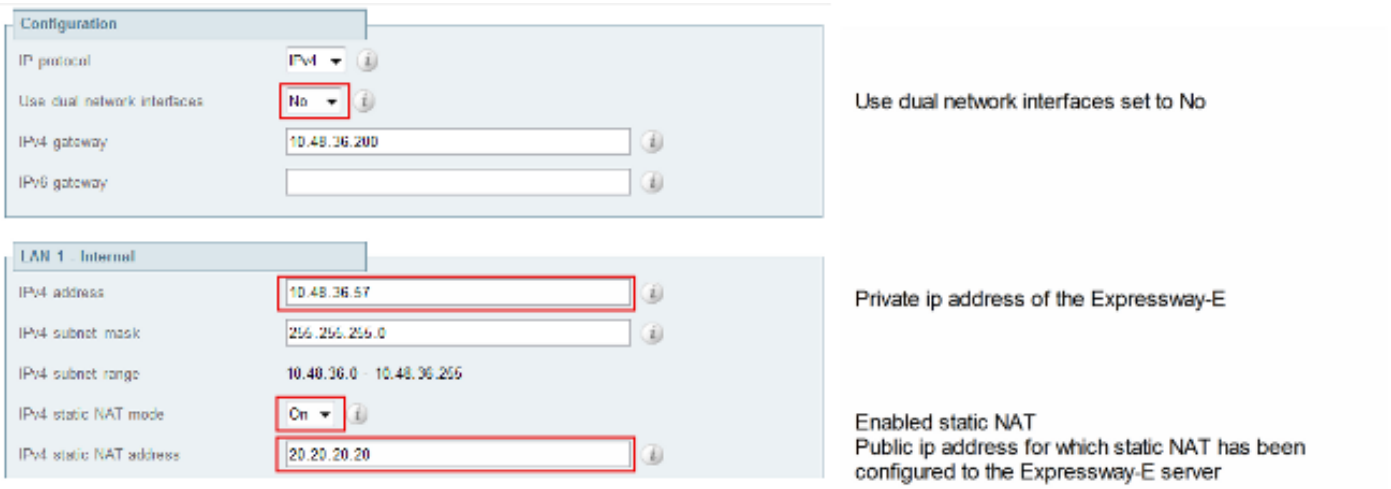
Quand les **doubles interfaces réseau d'utilisation** est configurées avec une valeur d'**oui**, l'autoroute-e écoute seulement sur l'interface interne la transmission XMPP avec l'autoroute-C. Ainsi, vous devez s'assurer que cette interface est configurée et fonctionne correctement.

Une interface - Adresse IP publique

Quand seulement une interface est utilisée, et vous configurez l'autoroute-e avec une adresse IP publique, aucune considération spéciale ne doit être prise.

Une interface - Adresse IP privée

Quand seulement une interface est utilisée, et vous configurez l'autoroute-e avec une adresse IP privée, vous devez configurer l'adresse (NAT) de traduction d'adresses de réseau statique aussi bien :



Dans cette situation, il est important d'assurer cela :

- On permet à l'l'autoroute-C par le Pare-feu pour envoyer le trafic à l'adresse IP publique. Ceci est connu en tant que *réflexion NAT*.
- La zone de client de traversée sur l'autoroute-C est configurée avec une adresse de pair qui apparie l'adresse NAT statique sur l'autoroute-e, qui est **20.20.20.20** dans ce cas.

  Conseil : Plus d'informations sur des déploiements de réseau avancé sont disponibles dans l'**annexe 4 du** guide de déploiement de la configuration de base de serveur de communication vidéo Cisco TelePresence (contrôle avec l'autoroute).

Vérifiez

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

Dépannez

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

Quelques scénarios spécifiques sont couverts dans cette section, mais vous pouvez également utiliser l'analyseur de solutions de Collaboration qui fournit une vue détaillée de toute la transmission pour des tentatives de procédure de connexion MRA et d'information de dépannage

basée sur vos logs diagnostiques.

Zone de traversée

Quand l'adresse de pair est configurée car une adresse IP ou l'adresse de pair n'apparie pas le nom commun (NC), vous voyez ceci dans les logs :

```
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"
```

Quand le mot de passe est incorrect, vous voyez ceci dans les logs d'autoroute-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 le Double-NIC est activé mais la deuxième interface n'est pas utilisée ou est connectée, l'autoroute-C ne peut pas se connecter à l'autoroute-e pour la transmission XMPP sur le port 7400, et les logs d'autoroute-C affichent ceci :

```
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"
```

DN

Quand le FQDN qui est retourné par la consultation d'enregistrement SRV pour la périphérie de Collaboration n'apparie pas le FQDN qui est configuré sur l'autoroute-e, l'exposition de logs de Jabber cette erreur :

```
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 logs diagnostiques pour l'autoroute-e, vous pouvez voir pour quel domaine le Témoin est placé 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 de SIP

Quand les domaines exigés de SIP ne sont pas ajoutés sur l'autoroute-C, l'autoroute-e ne reçoit pas des messages pour ce domaine et dans les logs diagnostiques vous voyez un message **interdit par 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"
```