Mobiele en Remote Access instellen via snelweg/VCS in een multi-domein-implementatie

Inhoud

[Inleiding](#)
[Voorwaarden](#)
[Vereisten](#)
[Gebruikte componenten](#)
[Configureren](#)
[Netwerkdiagram](#)
[Traversal Zone](#)
[Verkeersserver](#)
[Verkeerclient](#)
[Domain voor spraakservices](#)
[DNS-records](#)
[SIP-domein op expresse-C](#)
[Hostnaam/IP-Address CUCM Server](#)
[Certificaten](#)
[Dubbele NIC](#)
[Twee interfaces](#)
[Eén interface - openbaar IP-adres](#)
[Eén interface - Private IP-adres](#)
[Verifiëren](#)
[Problemen oplossen](#)
[Traversal Zone](#)
[Dubbele NIC](#)
[DNS](#)
[SIP-domein](#)

Inleiding

Dit document beschrijft hoe u de Cisco TelePresence Video Communication Server (VCS) voor Mobile Remote Access (MRA) moet configureren wanneer er meerdere domeinen worden gebruikt.

De MRA is ingesteld wanneer er slechts één domein is, en u kunt de stappen volgen die in de implementatiegids gedocumenteerd zijn. Wanneer de implementatie meerdere domeinen betreft, wordt het complexer. Dit document is geen configuratiehandleiding, maar beschrijft de belangrijke aspecten wanneer er meerdere domeinen bij betrokken zijn. De hoofdconfiguratie is gedocumenteerd in de Cisco TelePresence Video Communication Server (VCS)-implementatiegids.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

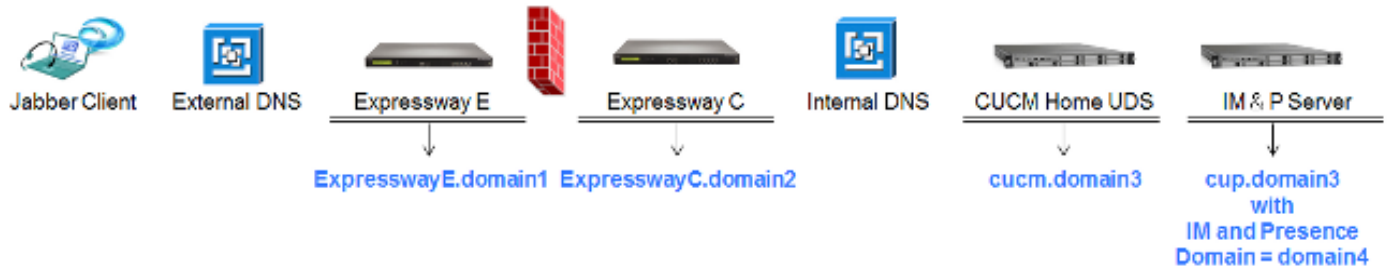
Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Configureren

Gebruik de informatie die in dit gedeelte wordt beschreven om de VCS te configureren.

Netwerkdiagram

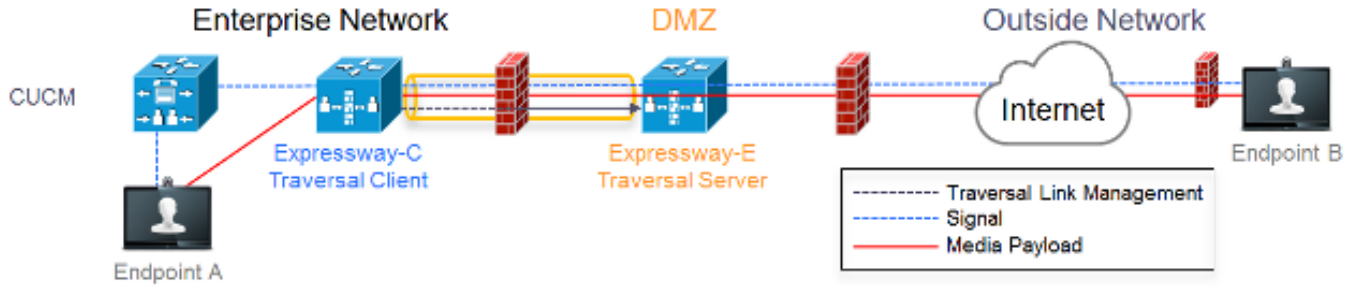


Hier volgt een kort overzicht van de verschillende domeinen:

- **domain1** - Dit is het Edge-domein dat door de client wordt gebruikt om de locatie van de Edge-server te ontdekken en door deze de User Data Service (UDS) te ontdekken.
- **domein2 en domein3** - Dit wordt gebruikt voor het opsporen van servers.
- **domain4** - Dit is het Instant Messaging and Presence (IM&P)-domein dat wordt gebruikt door Extensible Communications Platform (XCP) en Extensible Messaging and Presence Protocol (XMPP).

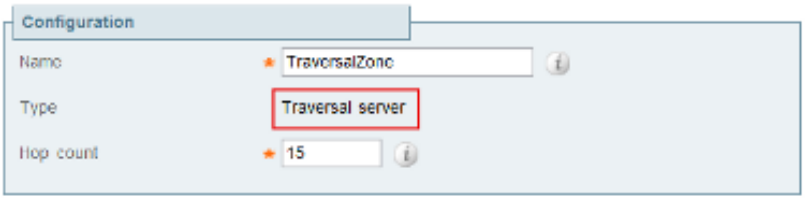
Traversal Zone

De Traversal Zone bestaat uit de Traversal Server (**snelwegE**), gelegen in de de-Militarized Zone (DMZ) en de Traversal Client (**snelwegC**), gelegen in het netwerk:

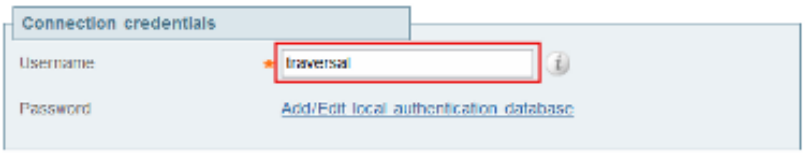


Verkeersserver

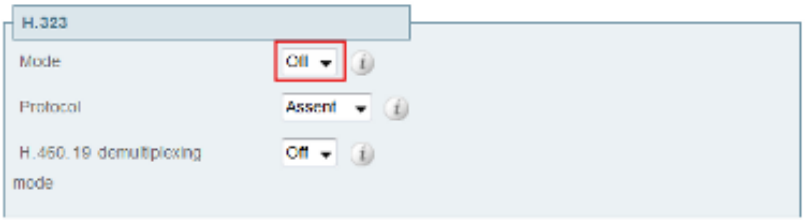
De Traversal Server bevindt zich in de configuratie van de zone op sneltoets E:



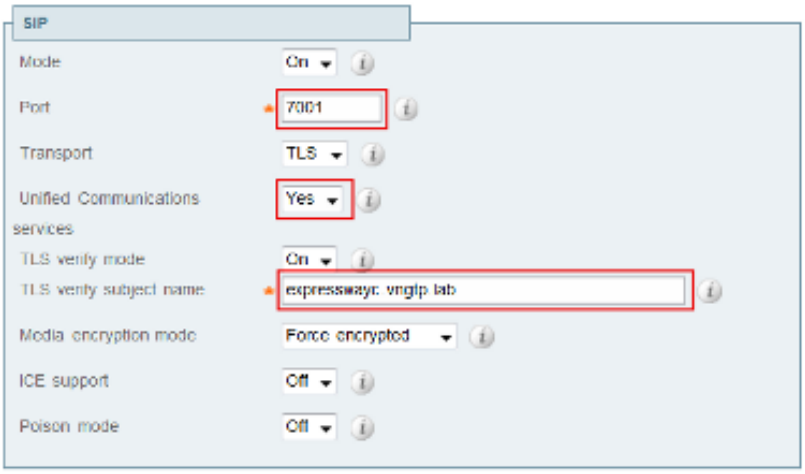
Select type as Traversal Server



Configure username for Traversal Client to authenticate with with server



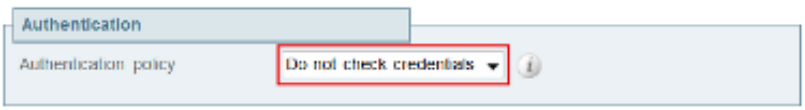
H.323 Mode must be set to off



Port 7001 is default listening port for Traversal Client connection

Unified Communications services must be enabled

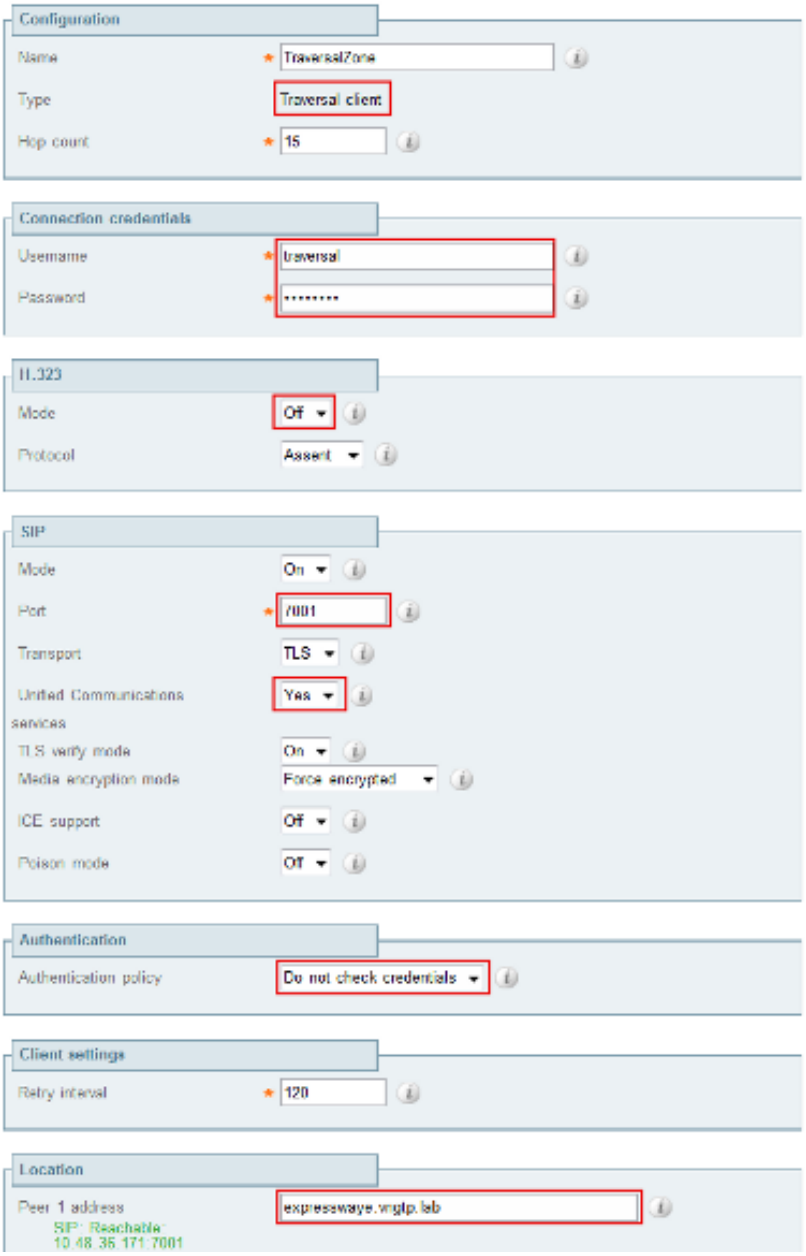
Must match CN from certificate presented by Traversal Client (Expressway C)



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

Verkeerclient

De Traversal Client bevindt zich in de zone-configuratie op expressweg 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)

Domain voor spraakservices

De gebruiker logt altijd in met **userid@domain4**, aangezien er geen verschil in gebruikerservaring zou moeten zijn binnen of buiten. Dit betekent dat als **domain1** anders is dan **domain4**, u het Voice Services-domein in de Jabber-client moet configureren. Dit komt doordat het domeingedeelte van de inlognaam wordt gebruikt om de Collaboration Edge-services te ontdekken met behulp van de Service (SRV)-record.

De client voert een Domain Name System (DNS)-record query uit voor **_collab-edge._tls.<domein>**. Dit impliceert dat wanneer het domein van de inloggebruiker-ID anders is dan het domein van de expressweg E, u de configuratie van het Voice Service domein moet gebruiken. Jabber gebruikt deze configuratie om de Collaboration Edge en de UDS te ontdekken.

Er zijn meerdere opties die u kunt gebruiken om deze taak te voltooien:

1. Voeg dit toe als een parameter wanneer u Jabber via de Media Services Interface (MSI) installeert:

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

2. Navigeren in **%APPDATA% > Cisco > Unified Communications > Jabber > CSF > Config** en maken dit **jabber-**configuratie**-user.xml**-bestand in de map:

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

Opmerking: Deze methode is alleen experimenteel en niet officieel ondersteund door Cisco.

3. Bewerk het bestand **jabber-klaar.xml**. Dit vereist dat de cliënt eerst intern inlogt. De generator Jabber Config kan hiervoor worden gebruikt:

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

4. Ook kunnen mobiele klanten Jabber met het Domein van de Diensten van de Spraak van tevoren worden gevormd zodat zij niet hoeven eerst intern in te loggen. Dit wordt uitgelegd in de installatiegids en de installatiehandleiding in het hoofdstuk Service Discovery. U moet een configuratie-URL maken waarop de gebruiker moet klikken:
`ciscojabber://provision?ServicesDomain=domain4&VoiceServicesDomain=domain1`

Opmerking: Het is vereist om het domein van de spraakservices te gebruiken omdat u moet verzekeren dat u de raadpleging voor de Collaboration Edge SRV records voor het externe domein (**domein1**) uitvoert.

DNS-records

In dit gedeelte worden de configuratie-instellingen voor de externe en interne DNS-records beschreven.

Extern

Type	Toegang	Oplossingen op
SRV-record	_collab-edge._tls.domain1	ExpresswayE.domain1
Een record	ExpresswayE.domain1	IP-adresomzetting

Het is belangrijk op te merken dat:

- De SRV records geven een Full Qualified Domain Name (FQDN) en geen IP-adres terug.
- De FQDN die door de SRV records wordt teruggegeven moet overeenkomen met de eigenlijke FQDN van de expressway-E, of het SRV record target is een CNAME en de alias wijst naar een server binnen hetzelfde domein als de Expressway-E (hangend Cisco bug ID CSCuo82526).

Dit is vereist omdat de Expressway-E een koekje op de cliënt met zijn eigen domein (**domein1**) vastlegt, en als dit niet overeenkomt met het domein dat door FQDN wordt geretourneerd, accepteert de cliënt dit niet. Cisco bug-ID CSCuo83458 wordt geopend als een verbetering voor dit scenario.

Intern

Type	Toegang	Oplossingen op
SRV-record	_cisco-uds._tcp.domain1	cucm.domein3
Een record	cucm.domein3	IP-adres CUCM

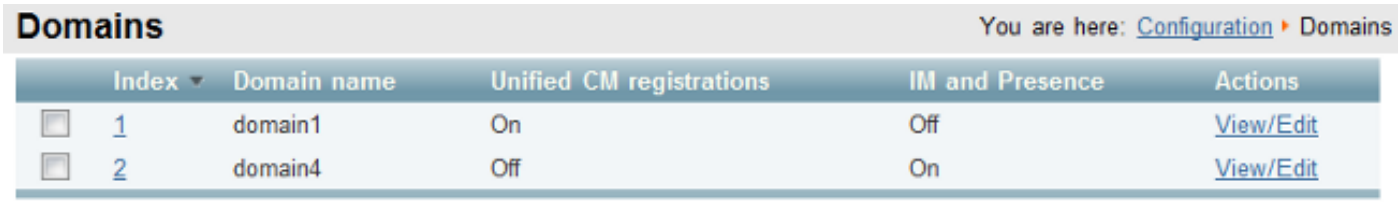
Omdat het domein van de spraakservices is ingesteld op **domain1**, combineert Jabber **domein1** in de getransformeerde URL voor de configuratie discovery van de Collaboration Edge (**get edge_fig**). Zodra ontvangen, voert Expressway-C een SRV UDS-opnametoewijzing voor **domein1** uit en geeft de records in het **200 OK-**bericht terug.

Type	Toegang	Oplossingen op
SRV	_cisco-uds._tcp.domain4	cucm.domein3
Een record	cucm.domein3	IP-adres CUCM

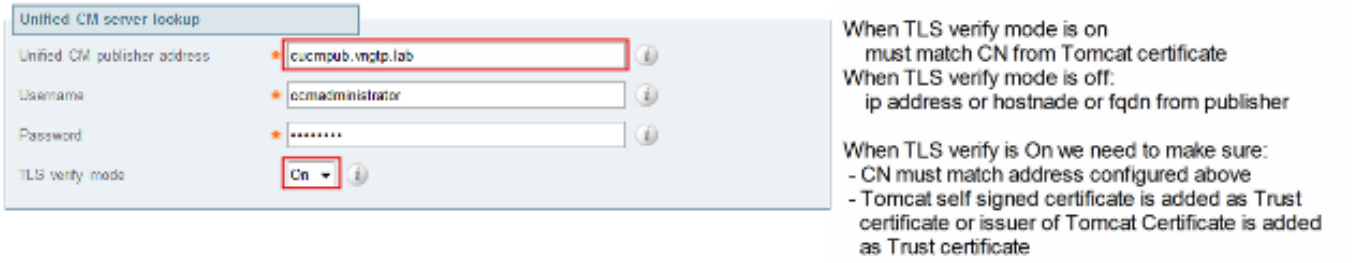
Wanneer de client on-net is, is de SRV UDS record discovery vereist voor **domain4**.

SIP-domein op expresse-C

U moet deze domeinen van het Session Initiation Protocol (SIP) in de Expressway-C toevoegen en ze voor MRA inschakelen:



Hostnaam/IP-Address CUCM Server



Wanneer u de Cisco Unified Communications Manager (CUCM)-servers configureren zijn er twee scenario's:

- Als uw Expressway-C (**domein2**) is geconfigureerd met hetzelfde domein als uw CUCM-server (**domein3**), kunt u uw CUCM-servers (**Systeem > servers**) configureren met:

  Het IP-adresDe hostnameDe FQDN
- Als Expressway-C (**domain2**) is ingesteld met een ander domein dan de CUCM-server (**domein3**), dan moet u de CUCM-servers configureren met:

  Het IP-adresDe FQDN

Dit is vereist omdat wanneer de Expressway-C de CUCM servers ontdekt en de hostname wordt teruggegeven, het een DNS raadpleging voor **hostname.domain2** uitvoert, wat niet werkt als

domain2 en **domain3** anders zijn.

Certificaten

Naast de algemene certificatievereisten, moeten er enkele dingen worden toegevoegd aan de Onderwerp Alternate Names (SAN's) van de certificaten:

- snelweg-C

  De aliases van het babbelknooppunt die worden ingesteld op de IM&P-servers moeten worden toegevoegd. Dit is alleen vereist voor de Unified Communications XMPP-federaties die van plan zijn zowel op Transport Layer Security (TLS) als groepschat te gebruiken. Dit wordt automatisch toegevoegd aan het CSR-verzoek (certificaataanvraag), mits de IM&P-servers al zijn ontdekt.

  De namen, in FQDN-formaat, van alle telefoonbeveiligingsprofielen in CUCM die voor versleuteld TLS zijn geconfigureerd en die worden gebruikt voor apparaten die externe toegang vereisen, moeten worden toegevoegd.
  Opmerking: Het FQDN-formaat is alleen vereist wanneer uw certificaatautoriteit (CA) geen hostname in SAN toestaat.
- snelweg-E

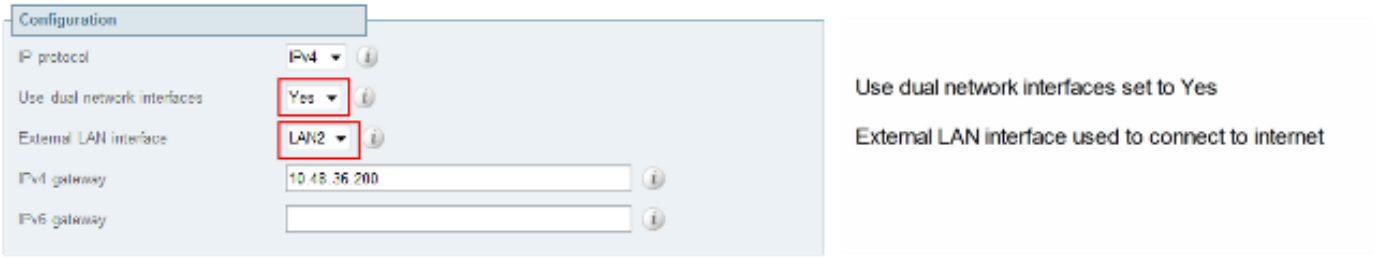
  Het domein dat wordt gebruikt voor de ontdekking van service (**domein1**) moet worden toegevoegd. domeinen van de XMPP Federatie.De aliases van het babbelknooppunt die worden ingesteld op de IM&P-servers moeten worden toegevoegd. Dit is alleen vereist voor Unified Communications XMPP-federaties die zowel TLS als groepschatten willen gebruiken. Deze kunnen worden gekopieerd van de CSR die op de Expressway-C wordt gegenereerd.

Dubbele NIC

In dit gedeelte worden de configuratie-instellingen beschreven bij gebruik van dubbele netwerkinterfacekaarten (NIC's).

Twee interfaces

Wanneer u de Expressway-E instelt om dubbele netwerkinterfaces te gebruiken, is het belangrijk om ervoor te zorgen dat beide interfaces worden geconfigureerd en gebruikt.



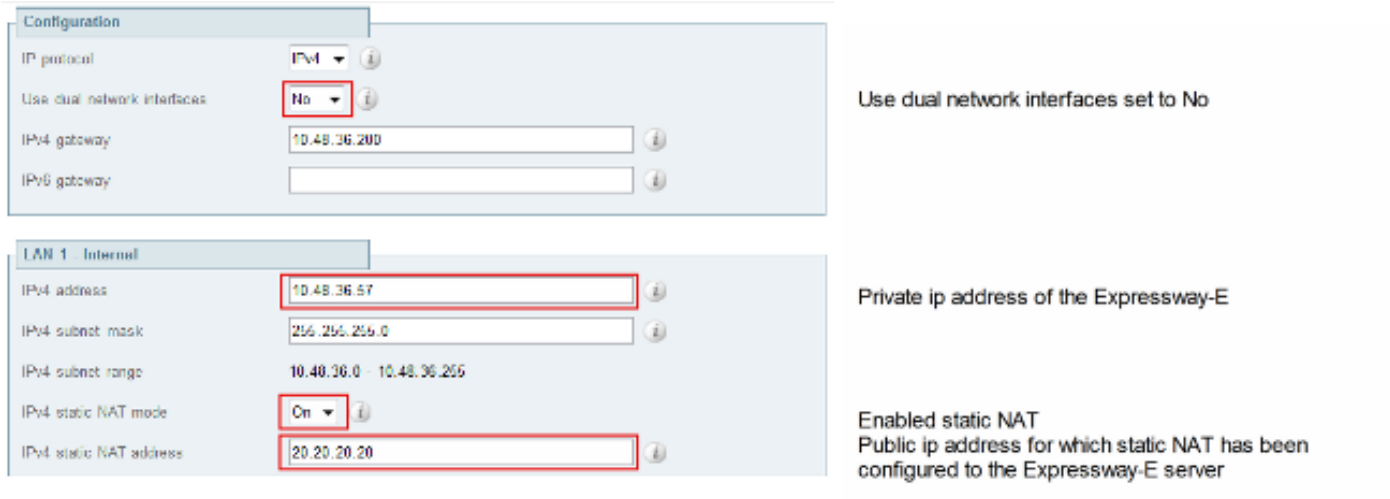
Wanneer de **Use dual network interfaces** is geconfigureerd met een waarde van **Ja**, luistert de Expressway-E alleen op de interne interface voor XMPP communicatie met de Expressway-C. Dus moet u ervoor zorgen dat deze interface is geconfigureerd en correct werkt.

Eén interface - openbaar IP-adres

Wanneer slechts één interface wordt gebruikt, en u vormt de Expressway-E met een openbaar IP-adres, moeten er geen speciale overwegingen worden genomen.

Eén interface - Private IP-adres

Wanneer slechts één interface wordt gebruikt en u de Expressway-E met een privaat IP-adres configureren moet u ook het statische adres voor netwerkadresomzetting (NAT) configureren:



In deze situatie is het belangrijk ervoor te zorgen dat:

- De firewall staat expressway-C toe om verkeer naar het openbare IP-adres te sturen. Dit staat bekend als *NAT reflectie*.
- De verplaatsen-clientzone in de snelweg-C is ingesteld met een peer-adres dat overeenkomt met het statische NAT-adres in de expressway-E, dat in dit geval **20.20.20**.20 is.

  Tip: Meer informatie over geavanceerde netwerkimplementaties is beschikbaar in **Bijlage 4** van de Cisco TelePresence Video Communication Server Basic Configuration (Control met Expressway) Deployment Guide.

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Deze sectie verschaft informatie die u kunt gebruiken om problemen met uw configuratie op te lossen.

Sommige specifieke scenario's worden in deze sectie behandeld, maar u kunt ook de Collaboration Solutions Analyzer gebruiken die een gedetailleerde weergave biedt van alle communicatie voor inlogpogingen en informatie over probleemoplossing op basis van uw diagnostische logbestanden.

Traversal Zone

Wanneer het peer-adres is ingesteld als een IP-adres of het peer-adres niet overeenkomt met de Common Name (CN), dan zie u dit in de logbestanden:

```
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"
```

Wanneer het wachtwoord niet correct is, ziet u dit in de documenten 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"
```

Dubbele NIC

Wanneer Dual-NIC is ingeschakeld maar de tweede interface niet wordt gebruikt of aangesloten, kan Expressway-C geen verbinding maken met de Expressway-E voor XMPP-communicatie in Port 7400 en de Expressway-C-logs tonen dit:

```
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

Wanneer de FQDN die door de SRV record lookup for Collaboration Edge wordt teruggezonden niet overeenkomt met de FQDN die in de Expressway-E is geconfigureerd, tonen de Jabber-logboeken deze fout:

```
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
```

In de diagnostische logbestanden voor Expressway-E kunt u zien voor welk domein het koekje in het HTTPS-bericht is ingesteld:

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

SIP-domein

Wanneer de vereiste SIP-domeinen niet zijn toegevoegd op de Expressway-C, accepteert de Expressway-E geen berichten voor dit domein en in de diagnostische logbestanden ziet u een **403 Verboden** bericht dat naar de client wordt verzonden:

```
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"
```