Konfiguration des mobilen und Remote-Zugriffs über Expressway/VCS in einer Bereitstellung mit mehreren Domänen

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie der Cisco TelePresence Video Communication Server (VCS) für den mobilen Remote-Zugriff (MRA) konfiguriert wird, wenn mehrere Domänen verwendet werden.

Die MRA-Einrichtung, wenn nur eine Domäne vorhanden ist, ist relativ einfach. Sie können die im Bereitstellungsleitfaden dokumentierten Schritte befolgen. Wenn die Bereitstellung mehrere Domänen umfasst, wird sie komplexer. Dieses Dokument ist kein Konfigurationsleitfaden, aber es beschreibt die wichtigen Aspekte, wenn mehrere Domänen beteiligt sind. Die Hauptkonfiguration ist im Cisco TelePresence Video Communication Server (VCS) Deployment Guide dokumentiert.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

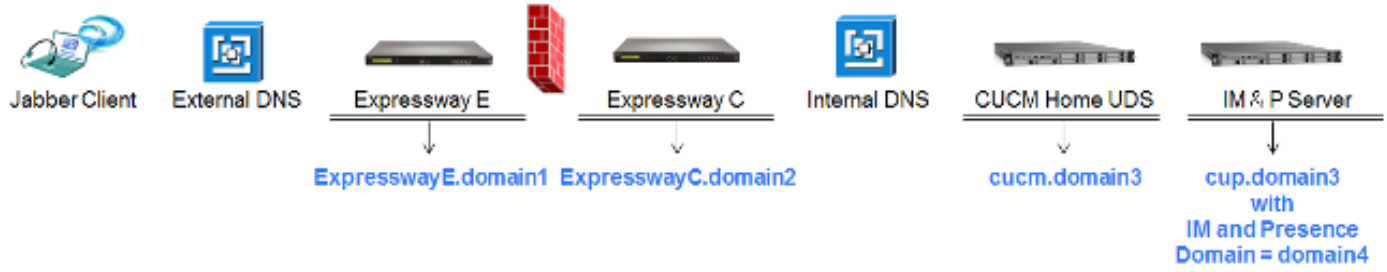
Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

Verwenden Sie die in diesem Abschnitt beschriebenen Informationen, um den VCS zu konfigurieren.

Netzwerkdiagramm

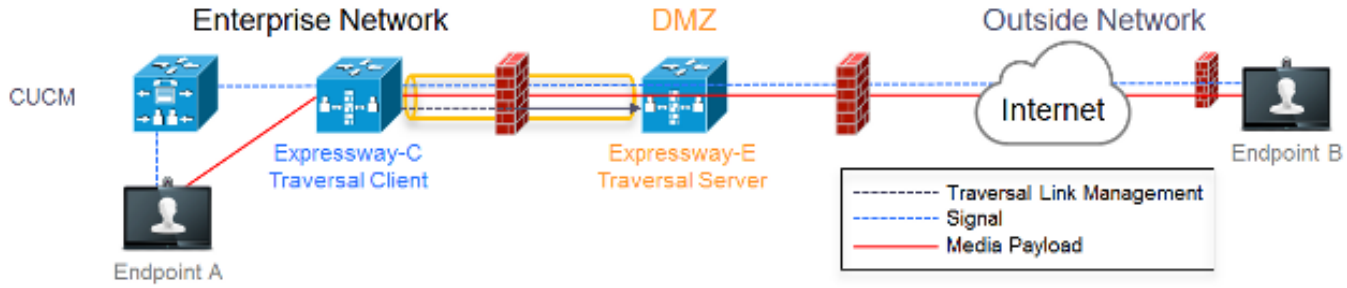


Im Folgenden finden Sie eine kurze Übersicht über die verschiedenen Domänen:

- **domain1** - Dies ist die Edge-Domäne, die vom Client verwendet wird, um den Standort des Edge-Servers zu ermitteln und den User Data Service (UDS) zu ermitteln.
- **domain2 und domain3**: wird zur Servererkennung verwendet.
- **domain4** - Dies ist die Instant Messaging- und Presence-Domäne (IM&P), die von XCP (Extensible Communications Platform)- und XMPP-Datenverkehr (Extensible Messaging and Presence Protocol) verwendet wird.

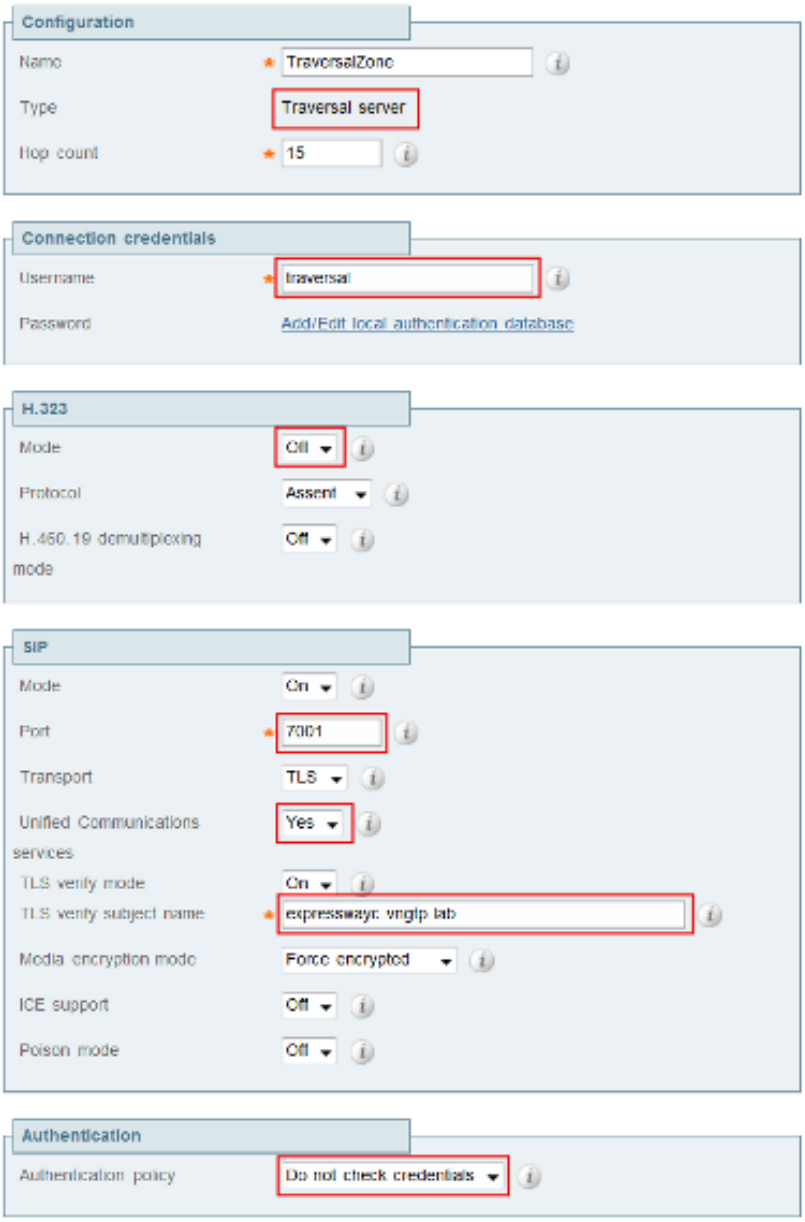
Traversal Zone

Die Traversal Zone besteht aus dem Traversal Server (**ExpresswayE**) in der De-Militarized Zone (DMZ) und dem Traversal Client (**ExpresswayC**) im Netzwerk:



Traversal-Server

Der Traversal-Server befindet sich in der Zonenkonfiguration auf der Expressway 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

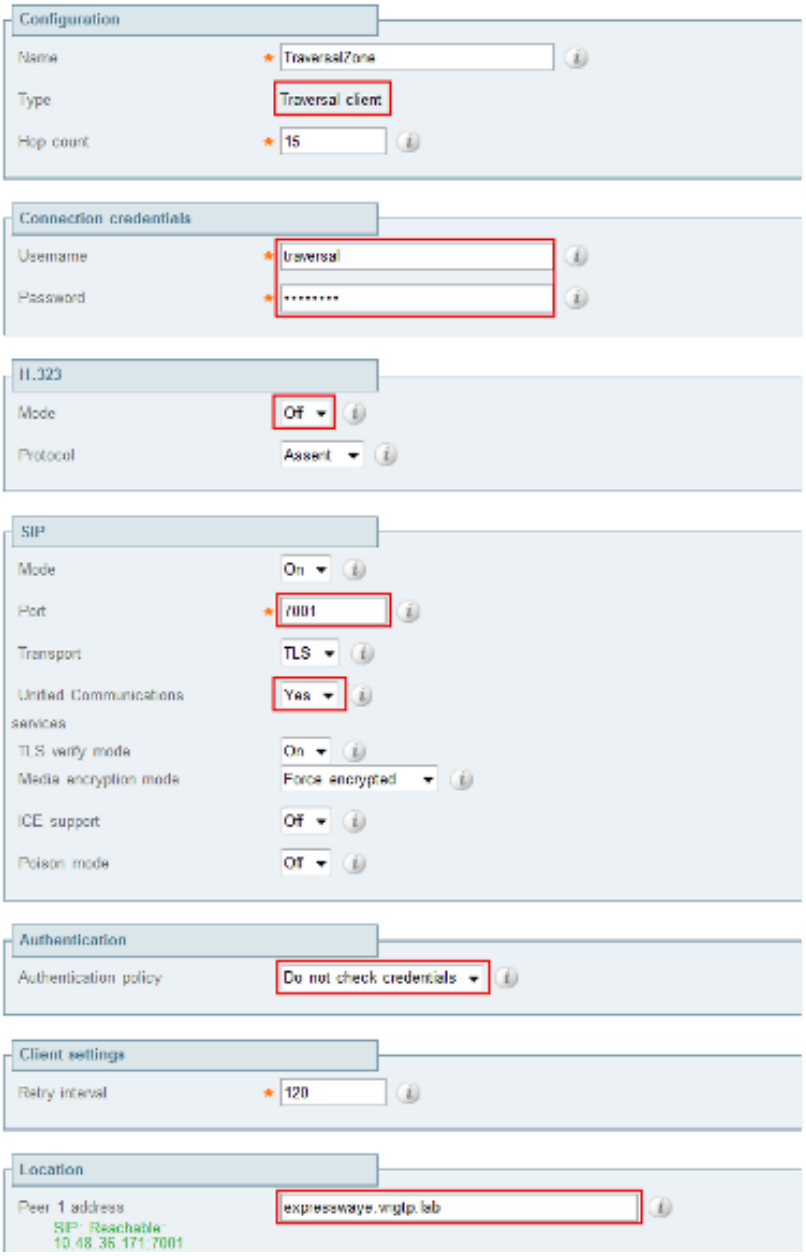
Unified Communications services must be enabled

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

Traversal-Client

Der Traversal Client befindet sich in der Zonenkonfiguration auf der 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)

Voice Services-Domäne

Der Benutzer meldet sich immer bei **userid@domain4** an, da es innerhalb und außerhalb des Netzwerks keine Unterschiede beim Anwendererlebnis geben sollte. Dies bedeutet, dass Sie die Sprachdienstdomäne im Jabber-Client konfigurieren müssen, wenn **domain1** sich von **domain4** unterscheidet. Der Grund hierfür ist, dass der Domänenteil der Anmeldung verwendet wird, um die Collaboration Edge-Services mithilfe der SRV-Datensatzsuche zu ermitteln.

Der Client führt eine DNS-Abfrage (Domain Name System) der SRV-Datensätze für **_collab-edge._tls.<domain>** durch. Dies bedeutet, dass Sie die Domänenkonfiguration für Sprachdienste verwenden müssen, wenn die Domäne aus der Anmelde-Benutzer-ID von der Domäne des Expressway E abweicht. Jabber verwendet diese Konfiguration, um den Collaboration Edge und den UDS zu ermitteln.

Sie können mehrere Optionen verwenden, um diese Aufgabe durchzuführen:

1. Fügen Sie dies als Parameter hinzu, wenn Sie Jabber über das Media Services Interface (MSI) installieren:

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

2. Navigieren Sie zu **%APPDATA% > Cisco > Unified Communications > Jabber > CSF > Config**, und erstellen Sie diese **Jabber-config-user.xml-**Datei im Verzeichnis:

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

Hinweis: Diese Methode ist nur experimentell und wird nicht offiziell von Cisco unterstützt.

3. Bearbeiten Sie die Datei **jabber-config.xml**. Dies erfordert, dass sich der Client zuerst intern anmeldet. Der Jabber Config File Generator kann hierfür verwendet werden:

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

4. Darüber hinaus können mobile Jabber-Clients mit der Voice Services-Domäne vorab konfiguriert werden, sodass sie sich nicht zuerst intern anmelden müssen. Dies wird im Bereitstellungs- und Installationshandbuch im Kapitel Serviceerkennung erläutert. Sie müssen eine Konfigurations-URL erstellen, auf die der Benutzer klicken muss:

```
ciscojabber://provision?ServicesDomain=domain4&VoiceServicesDomain=domain1
```

Hinweis: Es ist erforderlich, die Voice-Services-Domäne zu verwenden, da Sie sicherstellen müssen, dass Sie die Suche nach den Collaboration Edge SRV-Datensätzen für die externe Domäne (**Domäne1**) durchführen.

DNS-Einträge

In diesem Abschnitt werden die Konfigurationseinstellungen für die externen und internen DNS-Datensätze beschrieben.

Extern

Typ	Eintrag	Auflöst auf
SRV-Datensatz	_collab-edge._tls.domain1	ExpresswayE.Domain1
Ein Datensatz	ExpresswayE.Domain1	IP-Adresse ExpresswayE

Folgendes ist wichtig:

- Die SRV-Datensätze geben einen vollqualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) und keine IP-Adresse zurück.
- Der FQDN, der von den SRV-Datensätzen zurückgegeben wird, muss mit dem tatsächlichen FQDN des Expressway-E übereinstimmen, oder das SRV-Aufzeichnungsziel ist ein CNAME und der Alias verweist auf einen Server in derselben Domäne wie der Expressway-E (ausstehend Cisco Bug ID CSCuo82526).

Dies ist erforderlich, da das Expressway-E ein Cookie auf dem Client mit seiner eigenen Domäne

(**domain1**) setzt, und wenn dies nicht mit der vom FQDN zurückgegebenen Domäne übereinstimmt, akzeptiert der Client dies nicht. Die Cisco Bug-ID CSCuo83458 wird als Erweiterung für dieses Szenario geöffnet.

Intern

Typ	Eintrag	Auflöst auf
SRV-Datensatz	_cisco-uds_tcp.domain1	cucm.domain3
Ein Datensatz	cucm.domain3	IP-Adresse CUCM

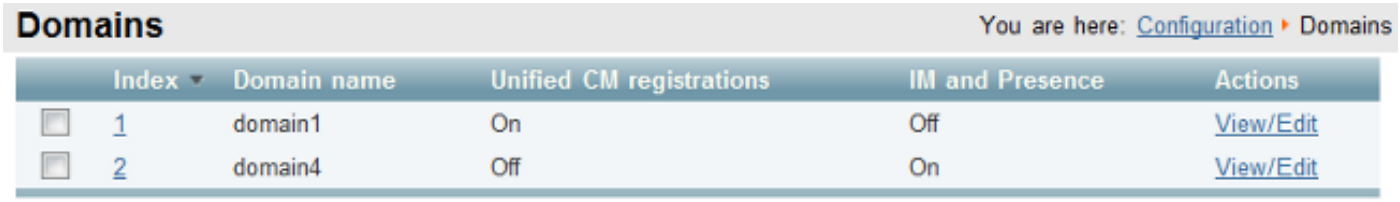
Da die Voice-Services-Domäne auf **domain1** festgelegt ist, fügt Jabber **domain1** zur Konfigurationserkennung des Collaboration Edge in die umgewandelte URL ein (**get edge_config**). Nach dem Empfang führt der Expressway-C eine SRV UDS-Datensatzabfrage für **domain1** durch und gibt die Datensätze in der **200 OK**-Nachricht zurück.

Typ	Eintrag	Auflöst auf
SRV	_cisco-uds_tcp.domain4	cucm.domain3
Ein Datensatz	cucm.domain3	IP-Adresse CUCM

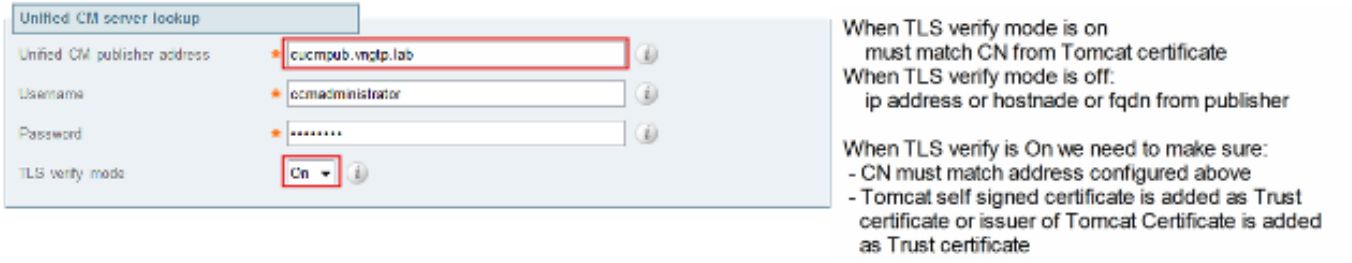
Wenn der Client im Netzwerk ist, ist die SRV UDS-Datensatzerkennung für **Domäne4** erforderlich.

SIP-Domänen auf Expressway-C

Sie müssen diese SIP-Domänen (Session Initiation Protocol) auf dem Expressway-C hinzufügen und für MRA aktivieren:



Hostname/IP-Adresse CUCM-Server



Wenn Sie die Cisco Unified Communications Manager-Server (CUCM) konfigurieren, gibt es zwei Szenarien:

- Wenn Ihr Expressway-C (**domain2**) mit der gleichen Domäne wie Ihr CUCM-Server (**domain3**) konfiguriert ist, können Sie Ihre CUCM-Server (**System > Server**) wie folgt konfigurieren:

  Die IP-AdresseDer HostnameFQDN
- Wenn der Expressway-C (**domain2**) mit einer anderen Domäne als der CUCM-Server (**domain3**) konfiguriert ist, müssen Sie die CUCM-Server wie folgt konfigurieren:

Die IP-AdresseFQDN

Dies ist erforderlich, da Expressway-C, wenn er die CUCM-Server erkennt und den Hostnamen zurückgibt, eine DNS-Suche nach **hostname.domain2** durchführt, die nicht funktioniert, wenn sich **domain2** und **domain3** unterscheiden.

Zertifikate

Neben den allgemeinen Zertifikatsanforderungen müssen den Subject Alternate Names (SAN) der Zertifikate einige Dinge hinzugefügt werden:

- Expressway-C

  Die auf den IM&P-Servern konfigurierten Chat-Knoten-Aliase müssen hinzugefügt werden. Dies ist nur bei Unified Communications XMPP-Verbundbereitstellungen erforderlich, die sowohl Transport Layer Security (TLS) als auch Group Chat verwenden möchten. Dies wird automatisch dem CSR (Certificate Signing Request) hinzugefügt, sofern die IM&P-Server bereits erkannt wurden.

  Es müssen die Namen aller Telefonsicherheitsprofile im CUCM im FQDN-Format hinzugefügt werden, die für verschlüsselte TLS konfiguriert sind und für Geräte verwendet werden, die Remote-Zugriff erfordern.
  Hinweis: Das FQDN-Format ist nur erforderlich, wenn Ihre Zertifizierungsstelle (Certificate Authority, CA) die Hostnamensyntax im SAN nicht zulässt.
- Expressway-E

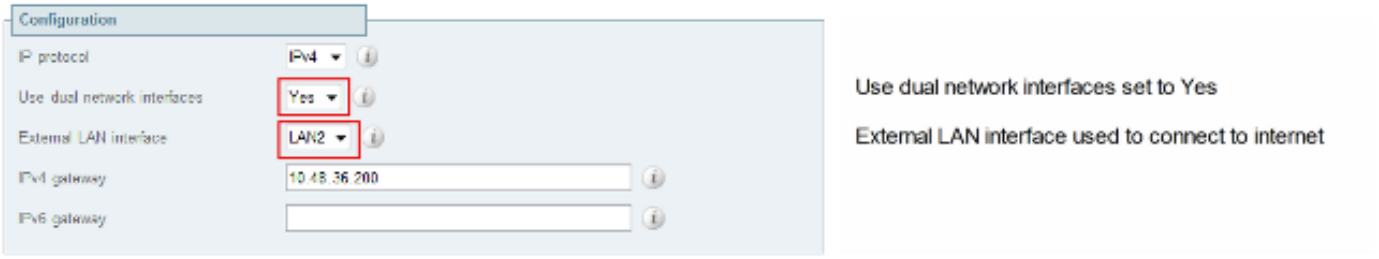
  Die Domäne, die für die Diensterkennung (**domain1**) verwendet wird, muss hinzugefügt werden. XMPP Federation-Domänen.Die auf den IM&P-Servern konfigurierten Chat-Knoten-Aliase müssen hinzugefügt werden. Dies ist nur bei Bereitstellungen im Verbund mit Unified Communications XMPP erforderlich, die sowohl TLS als auch Gruppen-Chat verwenden möchten. Diese können aus dem CSR kopiert werden, der auf dem Expressway-C generiert wird.

Dual-NIC

In diesem Abschnitt werden die Konfigurationseinstellungen beschrieben, wenn zwei Netzwerkschnittstellenkarten (NICs) verwendet werden.

Zwei Schnittstellen

Wenn Sie Expressway-E für die Verwendung von dualen Netzwerkschnittstellen konfigurieren, ist es wichtig, sicherzustellen, dass beide Schnittstellen konfiguriert und verwendet werden.



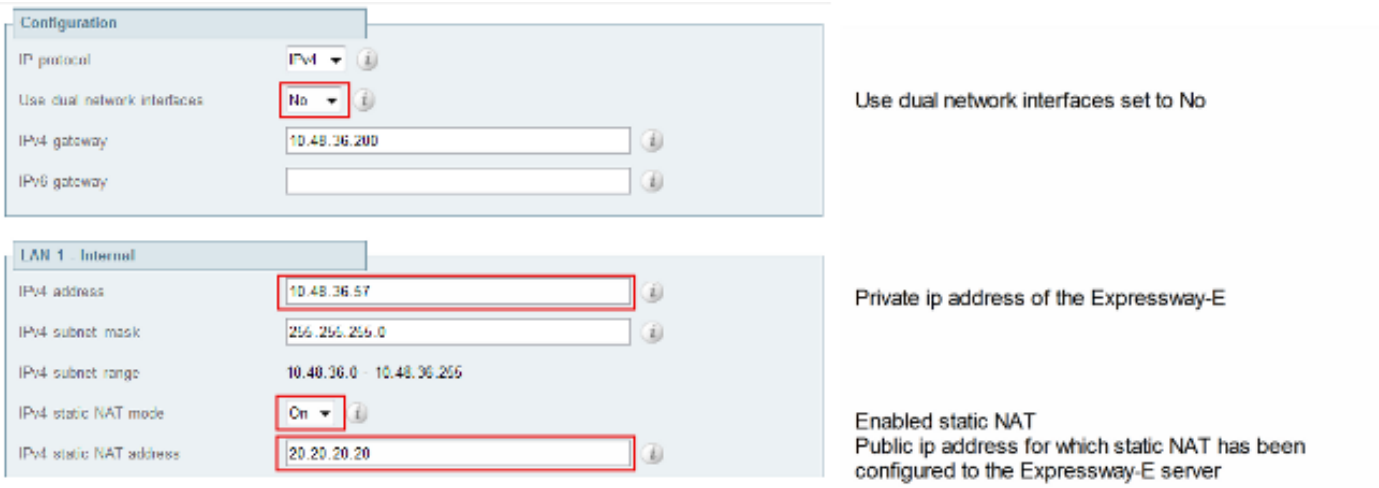
Wenn die **Doppelnetzwerkschnittstellen verwenden** mit dem Wert **Ja** konfiguriert ist, überwacht der Expressway-E nur die interne Schnittstelle für die XMPP-Kommunikation mit dem Expressway-C. Daher müssen Sie sicherstellen, dass diese Schnittstelle konfiguriert ist und ordnungsgemäß funktioniert.

Eine Schnittstelle - Öffentliche IP-Adresse

Wenn nur eine Schnittstelle verwendet wird und Sie das Expressway-E mit einer öffentlichen IP-Adresse konfigurieren, müssen keine besonderen Überlegungen angestellt werden.

Eine Schnittstelle - Private IP-Adresse

Wenn nur eine Schnittstelle verwendet wird und Sie das Expressway-E mit einer privaten IP-Adresse konfigurieren, müssen Sie auch die statische Network Address Translation (NAT)-Adresse konfigurieren:



In dieser Situation ist es wichtig sicherzustellen, dass

- Der Expressway-C darf von der Firewall Datenverkehr an die öffentliche IP-Adresse senden. Dies wird als *NAT-Reflektion* bezeichnet.
- Die Traversal-Client-Zone auf dem Expressway-C wird mit einer Peer-Adresse konfiguriert, die der statischen NAT-Adresse auf dem Expressway-E entspricht, die in diesem Fall **20.20.20.20** ist.

Tipp: Weitere Informationen zu erweiterten Netzwerkbereitstellungen finden Sie in **Anhang 4** des Cisco TelePresence Video Communication Server Basic Configuration (Control with Expressway) Deployment Guide.

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

Einige spezifische Szenarien werden in diesem Abschnitt behandelt, Sie können jedoch auch den Collaboration Solutions Analyzer verwenden, der eine detaillierte Ansicht aller Kommunikationsvorgänge für MRA-Anmeldeversuche und Informationen zur Fehlerbehebung auf der Grundlage Ihrer Diagnoseprotokolle bereitstellt.

Traversal Zone

Wenn die Peer-Adresse als IP-Adresse konfiguriert ist oder die Peer-Adresse nicht mit dem Common Name (CN) übereinstimmt, wird dies in den Protokollen angezeigt:

```
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"
```

Wenn das Kennwort falsch ist, sehen Sie dies in den Expressway-E-Protokollen:

```
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"
```

Dual-NIC

Wenn Dual-NIC aktiviert ist, aber die zweite Schnittstelle nicht verwendet oder verbunden wird, kann Expressway-C keine Verbindung zum Expressway-E für die XMPP-Kommunikation auf Port 7400 herstellen. Die Expressway-C-Protokolle zeigen Folgendes:

```
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

Wenn der FQDN, der von der SRV-Datensatzsuche für den Collaboration Edge zurückgegeben wird, nicht mit dem FQDN übereinstimmt, der auf dem Expressway-E konfiguriert wurde, zeigen die Jabber-Protokolle den folgenden Fehler an:

```
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 den Diagnoseprotokollen für Expressway-E können Sie sehen, für welche Domäne das Cookie in der HTTPS-Nachricht festgelegt ist:

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

SIP-Domänen

Wenn die erforderlichen SIP-Domänen nicht zum Expressway-C hinzugefügt werden, akzeptiert der Expressway-E keine Nachrichten für diese Domäne. In den Diagnoseprotokollen wird eine **403 Forbidden-**Meldung angezeigt, die an den Client gesendet wird:

```
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"
```