Configurar o móbil e o Acesso remoto com Expressway/VCS em um desenvolvimento do Multi-domínio

Índice

Introdução

Este documento descreve como configurar o server de comunicação de vídeo do Cisco TelePresence (VC) para o Acesso remoto móvel (MRA) quando os domínios múltiplos são usados.

O MRA estabelecido quando há somente um domínio é relativamente direto, e você pode seguir as etapas que são documentadas no guia de distribuição. Quando o desenvolvimento envolve domínios múltiplos, torna-se mais complexo. Este documento não é um manual de configuração, mas descreve os aspectos importantes quando os domínios múltiplos são involvidos. A configuração principal é documentada no guia de distribuição do server de comunicação de vídeo do Cisco TelePresence (VC).

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

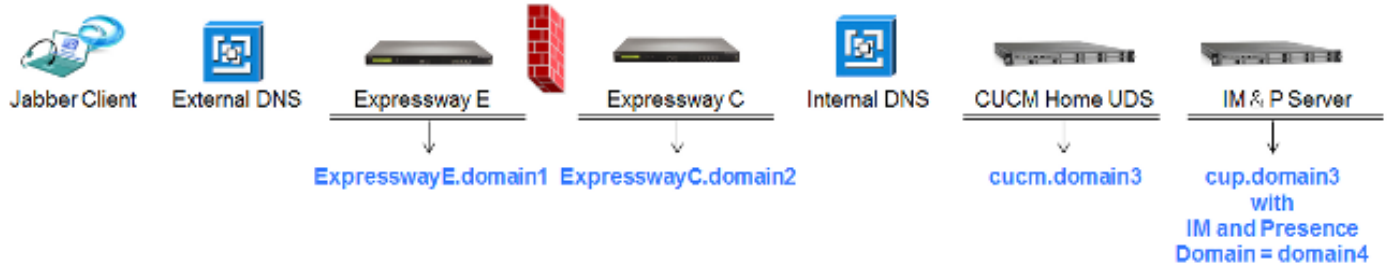
Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Configurar

Use a informação que é descrita nesta seção a fim configurar os VC.

Diagrama de Rede

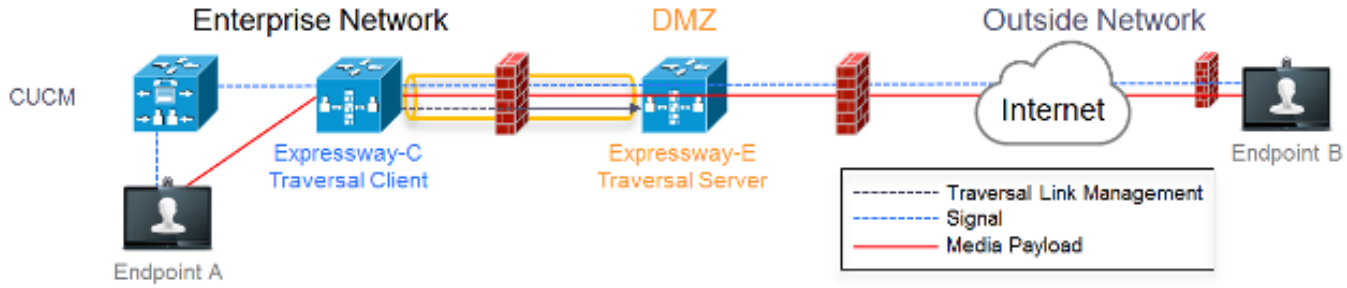


Está aqui uma vista geral curto dos domínios diferentes:

- **domain1** - Este é o domínio de borda que são usados pelo cliente a fim descobrir o lugar do server da borda e com qual descobre o serviço de dados do usuário (UD).
- **domain2 e domain3** - Isto é usado para a descoberta do server.
- **domain4** - Esta é Mensagem e presença instantâneas (o domínio IM&P) que é usado pela plataforma elástico das comunicações (XCP) e pelo tráfego elástico do protocolo da Mensagem e da presença (XMPP).

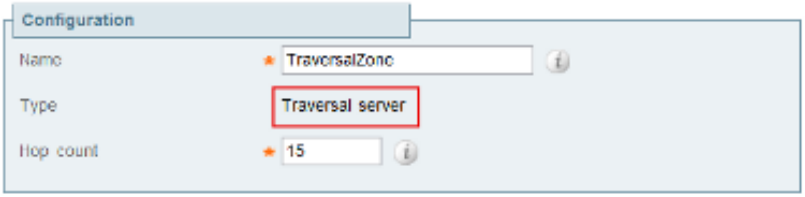
Zona de Traversal

A zona de Traversal consiste no server de Traversal (**expresswayE**), situado no De-Militarized Zone (DMZ), e no cliente de Traversal (**expresswayC**), situado dentro da rede:

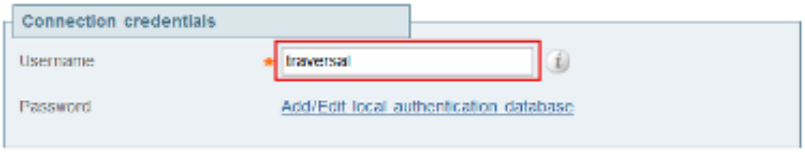


Server de Traversal

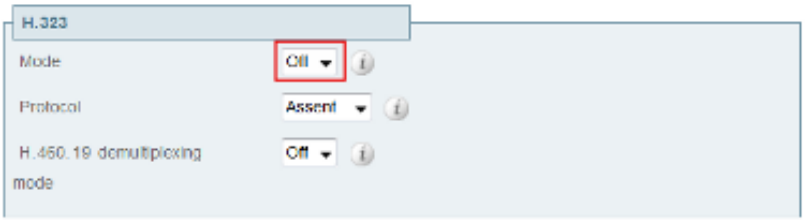
O server de Traversal é ficado situado na configuração da zona na via expressa E:



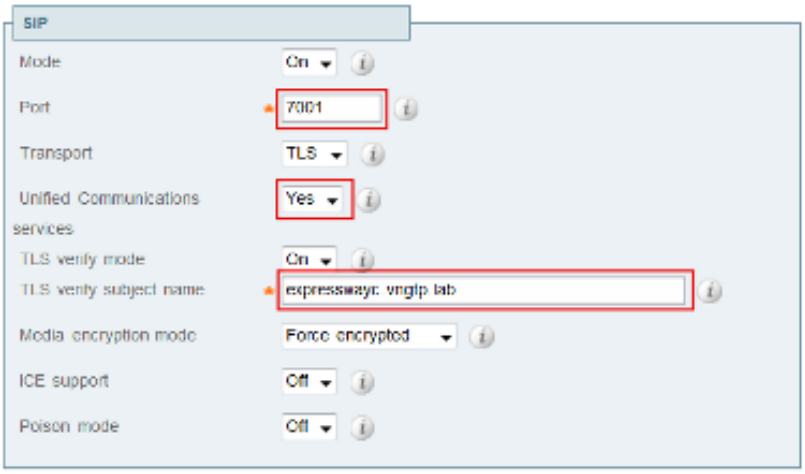
Select type as Traversal Server



Configure username for Traversal Client to authenticate with with server



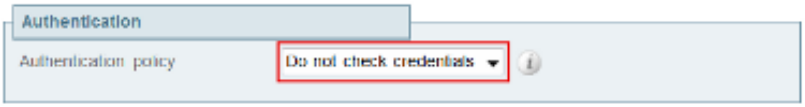
H.323 Mode must be set to off



Port 7001 is default listening port for Traversal Client connection

Unified Communications services must be enabled

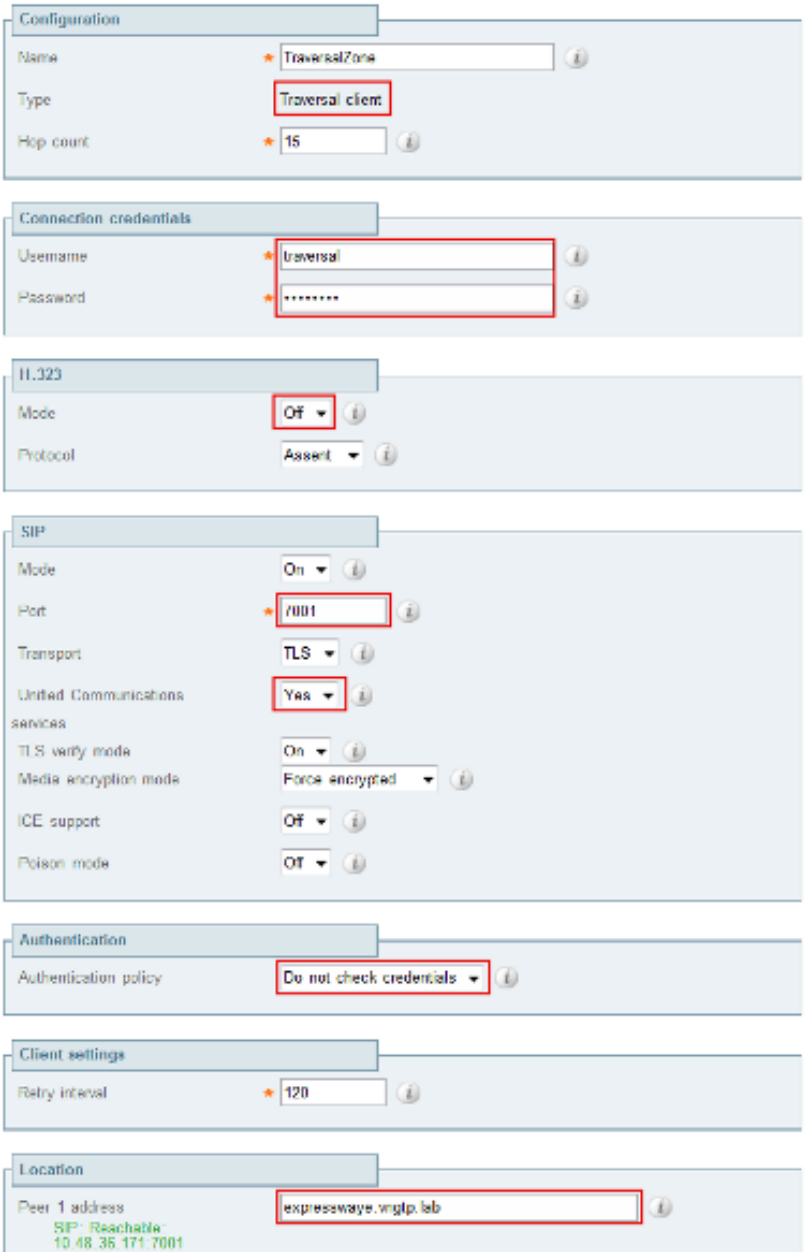
Must match CN from certificate presented by Traversal Client (Expressway C)



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

Cliente de Traversal

O cliente de Traversal é ficado situado na configuração da zona no C da via expressa:



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)

Domínio dos serviços de voz

O usuário entra sempre com **userid@domain4**, porque não deve haver nenhuma diferença na experiência do usuário quando dentro ou fora. Isto significa que se **domain1** é diferente de **domain4**, você deve configurar o domínio dos serviços de voz no cliente do Jabber. Isto é porque a parcela do domínio do início de uma sessão é usada a fim descobrir os serviços de ponta de Colaboração usando consultas do registro do serviço (SRV).

O cliente executa uma pergunta do registro do Domain Name System (DNS) SRV para o **_collab-edge. _tls.<domain>**. Isto implica que quando o domínio do usuário de login - a identificação é diferente do que o domínio da via expressa E, você deve usar a configuração de domínio do serviço de voz. O Jabber usa esta configuração a fim descobrir a borda da Colaboração e os UD.

Há as opções múltiplas que você pode usar a fim terminar esta tarefa:

1. Adicionar isto como um parâmetro quando você instala o Jabber através da relação dos serviços de media (MSI):

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

2. Navegue a **%APPDATA% > Cisco > comunicações unificadas > Jabber > CSF > configuração**, e crie este **arquivo jabber-config-user.xml no** diretório:

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

Nota: Este método experimental é apoiado somente e não oficialmente por Cisco.

3. Edite o **arquivo jabber-config.xml**. Isto exige que o cliente entra internamente primeiramente. O gerador do arquivo de JabberConfig pode ser usado para este:

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

4. Também, os clientes móveis do Jabber podem ser configurados com o domínio dos serviços de voz honesto assim que não precisam de entrar internamente primeiramente. Isto é explicado no desenvolvimento e no Guia de Instalação no capítulo da descoberta do serviço. Você deve criar uma configuração URL que o usuário precise de clicar:
`ciscojabber://provision?ServicesDomain=domain4&VoiceServicesDomain=domain1`

   Nota: Exige-se para usar o domínio dos serviços de voz porque você deve se assegurar de que você execute a consulta para os registros da borda SRV da Colaboração para o domínio exterior (**domain1**).

Registros DNS

Esta seção descreve os ajustes de configuração para os registros externos e dos DN internos.

Externo

Tipo	Entrada	Resoluções a
Registro SRV	_collab-edge._tls.domain1	ExpresswayE.domain1
Um registro	ExpresswayE.domain1	Endereço IP de Um ou Mais Servidores Cisco ICM NT Expressw

Éimportante notar isso:

- Os registros SRV retornam um nome de domínio totalmente qualificado (FQDN) e não um endereço IP de Um ou Mais Servidores Cisco ICM NT.
- O FQDN que é retornado pelos registros SRV deve combinar o FQDN real da via expressa-e, ou o alvo do registro SRV é um CNAME e os pontos do pseudônimo a um server dentro do mesmo domínio que a via expressa-e (identificação de bug Cisco pendente CSCuo82526).

Isto é exigido porque a via expressa-e ajusta um Cookie no cliente com seu próprio domínio (**domain1**), e se isto não combina com o domínio que está retornado pelo FQDN, o cliente não aceita isto. A identificação de bug Cisco CSCuo83458 é aberta como um realce para esta encenação.

Interno

Tipo	Entrada	Resoluções a
Registro SRV	_cisco-uds._tcp.domain1	cucm.domain3
Um registro	cucm.domain3	Endereço IP de Um ou Mais Servidores Cisco ICM NT CUCM

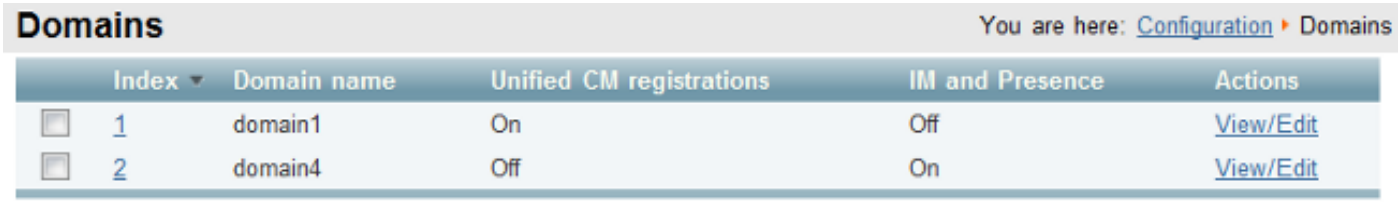
Porque o domínio dos serviços de voz é ajustado a **domain1**, o Jabber encaixa **domain1 na** URL transformada para a descoberta da configuração da borda da Colaboração (**obtenha o edge_config**). Uma vez que recebida, a via expressa-C executa uma pergunta do registro SRV UD para **domain1** e retorna os registros na mensagem de **200 APROVAÇÕES**.

Tipo	Entrada	Resoluções a
SRV	_cisco-uds._tcp.domain4	cucm.domain3
Um registro	cucm.domain3	Endereço IP de Um ou Mais Servidores Cisco ICM NT CUCM

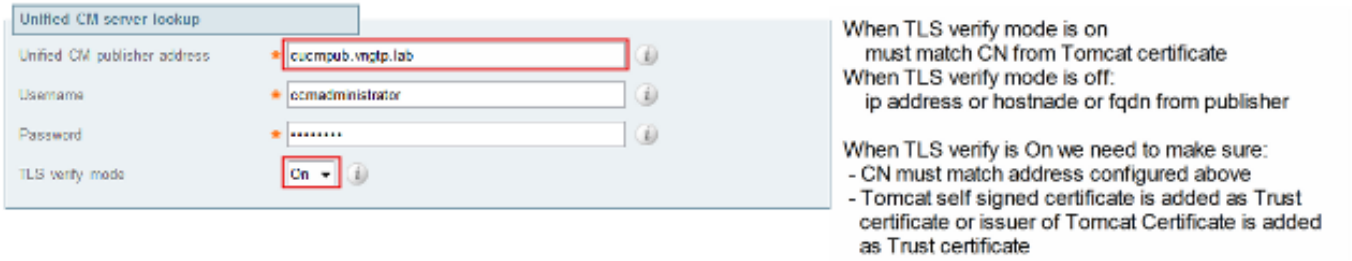
Quando o cliente é on-net, a descoberta do registro SRV UD está exigida para **domain4**.

Domínios do SORVO na via expressa-C

Você deve adicionar estes domínios do Session Initiation Protocol (SIP) na via expressa-C e permiti-los para MRA:



Server do hostname/endereço IP de Um ou Mais Servidores Cisco ICM NT CUCM



Quando você configura os server do gerente das comunicações unificadas de Cisco (CUCM), há duas encenações:

- Se sua via expressa-C (**domain2**) está configurada com o mesmo domínio que seu server CUCM (**domain3**), você pode configurar seus server CUCM (**sistema > server**) com:

  O endereço IP de Um ou Mais Servidores Cisco ICM NTO hostnameO FQDN
- Se a via expressa-C (**domain2**) está configurada com um domínio diferente do que o server CUCM (**domain3**), a seguir você deve configurar os server CUCM com:

  O endereço IP de Um ou Mais Servidores Cisco ICM NTO FQDN

Isto é exigido porque quando a via expressa-C descobre que os server CUCM e o hostname estão retornados, executa uma pesquisa de DNS para **hostname.domain2**, que não trabalha se **domain2** e **domain3** são diferentes.

Certificados

Com exceção das exigências gerais do certificado, algumas coisas devem ser adicionadas aos nomes alternativos sujeitos (SAN) dos Certificados:

- Via expressa-C

  Os pseudônimos do nó do bate-papo que são configurados nos server IM&P devem ser adicionados. Isto é exigido somente para as disposições da federação das comunicações unificadas XMPP que pretendem usar o Transport Layer Security (TLS) e o bate-papo do grupo. Isto é adicionado automaticamente à solicitação de assinatura de certificado (CSR), desde que tem descoberto os server IM&P já.

  Os nomes, no formato FQDN, de todos os perfis de segurança do telefone nos CUCM que são configurados para o TLS cifrado e usados para os dispositivos que exigem o Acesso remoto devem ser adicionados.
  Nota: O formato FQDN é exigido somente quando seu Certificate Authority (CA) não permite a sintaxe do hostname no SAN.
- Via expressa-e

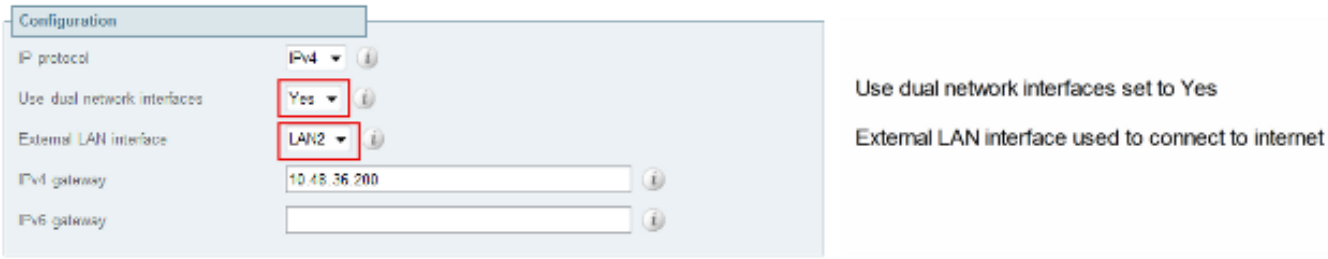
  O domínio usado para a descoberta do serviço (**domain1**) deve ser adicionado. Domínios da federação XMPP.Os pseudônimos do nó do bate-papo que são configurados nos server IM&P devem ser adicionados. Isto é exigido somente para as disposições da federação das comunicações unificadas XMPP que pretendem usar o TLS e o bate-papo do grupo. Estes podem ser copiados do CSR que é gerado na via expressa-C.

NIC dual

Esta seção descreve os ajustes de configuração quando o Network Interface Cards duplo (NIC) é usado.

Duas relações

Quando você configura a via expressa-e a fim usar interfaces de rede duplas, é importante assegurar-se de que ambas as relações estejam configuradas e usadas.



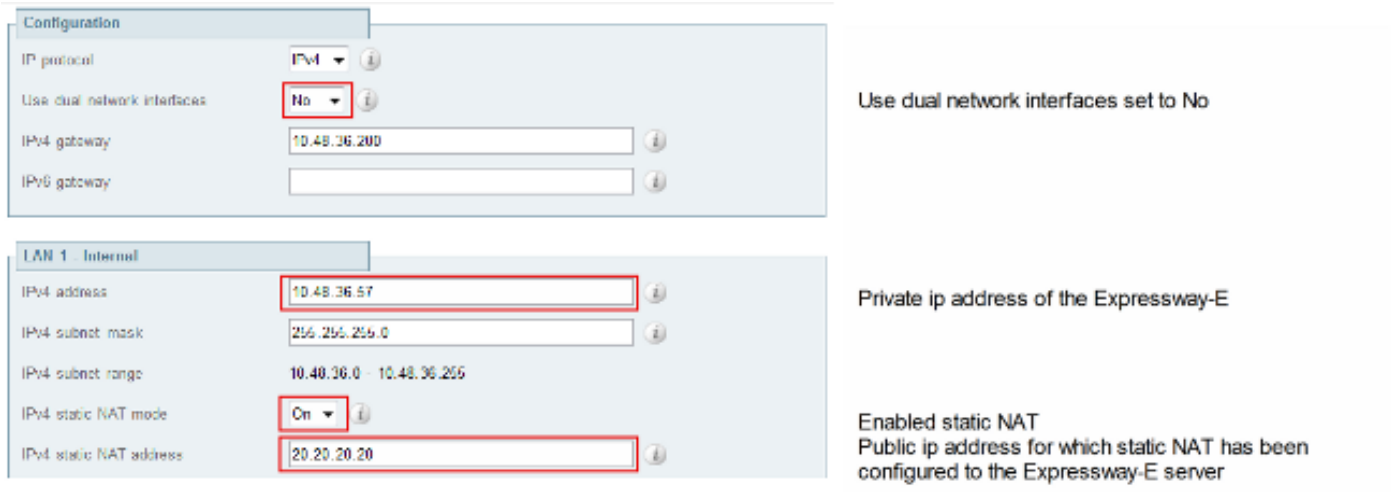
Quando as **interfaces de rede duplas do uso** são configuradas com um valor do **Yes**, a via expressa-e escuta somente na interface interna uma comunicação XMPP com a via expressa-C. Assim, você deve assegurar-se de que esta relação esteja configurada e trabalhe corretamente.

Uma relação - Endereço IP público

Quando somente uma relação está usada, e você configura a via expressa-e com um endereço IP público, nenhuma consideração especial deve ser tomada.

Uma relação - Endereço IP privado

Quando somente uma relação está usada, e você configura a via expressa-e com um endereço IP privado, você deve configurar o endereço da tradução de endereço da rede estática (NAT) também:



Nesta situação, é importante assegurar isso:

- A via expressa-C é permitida pelo Firewall enviar o tráfego ao endereço IP público. Isto é sabido como a *reflexão NAT*.
- A zona do cliente de Traversal na via expressa-C é configurada com um endereço de peer que combine o endereço do NAT estático na via expressa-e, que é **20.20.20.20** neste caso.

  Dica: Mais informação sobre disposições de rede avançada está disponível no **apêndice 4 do** guia de distribuição da configuração básica do server de comunicação de vídeo do Cisco TelePresence (controle com via expressa).

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshooting

Esta seção fornece a informação que você pode se usar a fim pesquisar defeitos sua configuração.

Algumas encenações específicas são cobertas nesta seção, mas você pode igualmente usar o analisador das soluções da Colaboração que fornece uma vista detalhada de toda a comunicação para tentativas de login MRA e da informação de Troubleshooting baseada em seus log de diagnóstico.

Zona de Traversal

Quando o endereço de peer é configurado porque um endereço IP de Um ou Mais Servidores Cisco ICM NT ou o endereço de peer não combinam o Common Name (CN), você vê este nos 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"
```

Quando a senha está incorreta, você vê este nos logs da via expressa-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

Quando o NIC dual é permitido mas a segunda relação não está usada nem está conectada, a via expressa-C não pode conectar à via expressa-e para uma comunicação XMPP na porta 7400, e os logs da via expressa-C mostram este:

```
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

Quando o FQDN que está retornado pela consulta do registro SRV para a borda da Colaboração não combinar o FQDN que está configurado na via expressa-e, a mostra dos logs do Jabber este erro:

```
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
```

Nos log de diagnóstico para a via expressa-e, você pode ver para que domínio o Cookie é ajustado na mensagem HTTPS:

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

Domínios do SORVO

Quando os domínios exigidos do SORVO não são adicionados na via expressa-C, a via expressa-e não aceita mensagens para este domínio e nos log de diagnóstico você vê uma mensagem **proibida 403** que seja enviada ao 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"
```