

通过多域部署的Expressway/VCS配置莫比尔和远程访问

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[网络图](#)

[穿越区域](#)

[穿越服务器](#)

[穿越客户端](#)

[语音服务域](#)

[DNS记录](#)

[在ExpresswayC的SIP域](#)

[主机名/IP地址CUCM服务器](#)

[证书](#)

[双NIC](#)

[两个接口](#)

[一个接口-公网IP地址](#)

[一个接口-专用IP地址](#)

[验证](#)

[故障排除](#)

[穿越区域](#)

[双NIC](#)

[DNS](#)

[SIP域](#)

简介

本文描述如何配置思科网真视频通信服务器(VCS)移动远程访问的(MRA)，当使用时多个域。

MRA设置，当只有一个域是相对直接的时，并且您能遵从在部署指南描述的步骤。当部署介入多个域时，变得更加复杂。本文不是配置指南，但是描述重要方面，当多个域是包含的时。主要配置在[思科网真视频通信服务器\(VCS\)部署指南](#)描述。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

请使用在此部分描述为了配置VCS的信息。

网络图

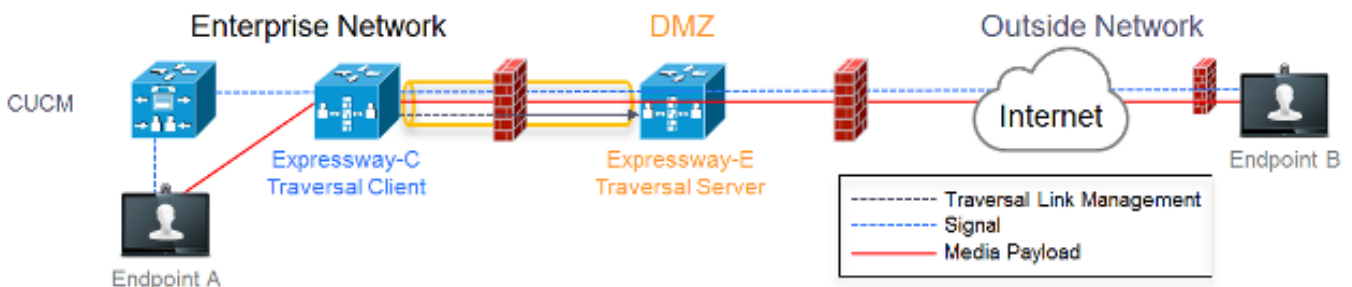


这是不同的域的一短的概述：

- **domain1** -这是由客户端使用为了发现边缘服务器位置，并且通过的边缘域哪些发现用户数据服务(UDS)。
- **domain2和domain3** -这使用服务器发现。
- **domain4** -这是瞬时消息传送和在线状态(由可扩展通信平台的IM&P)域(XCP)和可扩展消息传送和在线状态协议(XMPP)流量使用。

穿越区域

穿越区域包括穿越服务器(**expresswayE**)，查找在非敏感区域(DMZ)和穿越客户端(**expresswayC**)，查找在网络里面：



穿越服务器

穿越服务器在Expressway E的区域配置里查找：

Configuration

Name ⓘ

Type

Hop count ⓘ

Select type as Traversal Server

Connection credentials

Username ⓘ

Password [Add/Edit local authentication database](#)

Configure username for Traversal Client to authenticate with with server

H.323

Mode ⓘ

Protocol ⓘ

H.460.19 demultiplexing mode ⓘ

H.323 Mode must be set to off

SIP

Mode ⓘ

Port ⓘ

Transport ⓘ

Unified Communications services ⓘ

TLS verify mode ⓘ

TLS verify subject name ⓘ

Media encryption mode ⓘ

ICE support ⓘ

Poison mode ⓘ

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)

Authentication

Authentication policy ⓘ

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

穿越客户端

穿越客户端在Expressway C的区域配置里查找：

<p>Configuration</p> <p>Name <input type="text" value="TraversalZone"/></p> <p>Type <input type="text" value="Traversal client"/></p> <p>Hop count <input type="text" value="15"/></p>	Select Traversal Client as Type
<p>Connection credentials</p> <p>Username <input type="text" value="traversal"/></p> <p>Password <input type="password" value="*****"/></p>	Configure same username and password as added on the Traversal Server (Expressway E)
<p>H.323</p> <p>Mode <input type="text" value="Off"/></p> <p>Protocol <input type="text" value="Assent"/></p>	H.323 mode must be set to off
<p>SIP</p> <p>Mode <input type="text" value="On"/></p> <p>Port <input type="text" value="/1001"/></p> <p>Transport <input type="text" value="TLS"/></p> <p>Unified Communications services <input type="text" value="Yes"/></p> <p>TLS verify mode <input type="text" value="On"/></p> <p>Media encryption mode <input type="text" value="Force encrypted"/></p> <p>ICE support <input type="text" value="Off"/></p> <p>Poison mode <input type="text" value="Off"/></p>	Destination port Traversal Server is listening on Unified Communications must be enabled
<p>Authentication</p> <p>Authentication policy <input type="text" value="Do not check credentials"/></p>	Must be set to 'Do not check credentials' as expressway does not register any endpoints
<p>Client settings</p> <p>Retry interval <input type="text" value="120"/></p>	Must be FQDN Must be DNS resolvable Must match CN from certificate presented by Traversal Server (Expressway E)
<p>Location</p> <p>Peer 1 address <input type="text" value="expresswaye.vmgtp.lab"/></p> <p><small>SIP: Reachable 10.48.35.171:7001</small></p>	

语音服务域

因为不应该有在用户体验的差异，当内部或外部时，用户总是登录与userid@domain4。这意味着，如果domain1是与domain4不同，您必须配置在Jabber客户端的语音服务域。这是因为使用服务(SRV)记录查找，登录的域部分用于为了发现协作边缘服务。

客户端执行_collab-edge的。_tls.<domain>一域名系统(DNS) SRV记录查询。这暗示，当从登录用户ID的域跟域与Expressway E不同时，您必须使用语音服务域配置。Jabber使用此配置为了发现协作边缘和UDS。

有您能使用为了完成此任务的多个选项：

1. 请添加此作为参数，当您通过媒体服务接口时(MSI)安装Jabber：

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

2. 导航到%APPDATA% > Cisco>统一通信> Jabber > CSFS >config，并且创建在目录的此Jabber设置user.xml文件：

```
<?xml version="1.0" encoding="utf-8"?>
```

```
<config version = "1.0">
<Policies> <VoiceServicesDomain>domain1</VoiceServicesDomain>
</Policies>
</config>
```

注意： 试验思科只和不正式支持此方法。

3. 编辑Jabberconfig.xml文件。这要求客户端登录内部地首先。 [JabberConfig文件生成器](#)可以用于此：

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

4. 并且，移动Jabber客户端可以配置与语音服务域在最前面，因此他们不需要内部地首先登陆。这在部署和安装指南解释在[服务发现号](#)章节。您必须创建用户需要点击的配置URL：

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

注意： 它要求使用语音服务域，因为您必须保证您执行协作边缘SRV记录的查找外部域的(domain1)。

DNS记录

此部分描述外部和内部DNS记录的配置设置。

外部

类型	条目	解决
SRV记录	_collab-edge._tls.domain1	ExpresswayE.domain1
一个记录	ExpresswayE.domain1	IP地址ExpresswayE

注释那是重要的：

- SRV记录返回完全合格的域名(FQDN)而不是IP地址。
- 由SRV记录返回的FQDN必须匹配Expressway的实际FQDN E或者SRV记录目标是一CNAME和别名点对于一个服务器在域内和ExpresswayE (待定Cisco Bug ID [CSCuo82526](#))一样。

这要求，因为ExpresswayE设置在客户端的一Cookie有其自己的域的(domain1)，并且，如果这不配比与由FQDN返回的域，客户端不认可它。Cisco Bug ID [CSCuo83458](#)打开作为此方案的一增强。

内部

类型	条目	解决
SRV记录	_cisco-uds._tcp.domain1	cucm.domain3
一个记录	cucm.domain3	IP地址CUCM

由于语音服务域设置为domain1，Jabber在协作边缘配置发现的变换的URL嵌入domain1 (请获得edge_config)。一旦接收，ExpresswayC执行domain1的一SRV UDS记录查询并且返回在200 OK消息的记录。

类型	条目	解决
SRV	_cisco-uds._tcp.domain4	cucm.domain3
一个记录	cucm.domain3	IP地址CUCM

当客户端是网内时，SRV UDS记录发现为domain4要求。

在ExpresswayC的SIP域

您必须添加在ExpresswayC的这些会话初始化协议(SIP)域和为MRA启用他们：

Domains					You are here: Configuration > Domains
Index	Domain name	Unified CM registrations	IM and Presence	Actions	
<input type="checkbox"/> 1	domain1	On	Off	View/Edit	
<input type="checkbox"/> 2	domain4	Off	On	View/Edit	

主机名/IP地址CUCM服务器

Unified CM server lookup

Unified CM publisher address: ⓘ

Username: ⓘ

Password: ⓘ

TLS verify mode: ⓘ

When TLS verify mode is on must match CN from Tomcat certificate
When TLS verify mode is off: ip address or hostname or fqdn from publisher

When TLS verify is On we need to make sure:
- CN must match address configured above
- Tomcat self signed certificate is added as Trust certificate or issuer of Tomcat Certificate is added as Trust certificate

当您配置Cisco Unified Communications Manager (CUCM)时服务器，有两个方案：

- 如果您的ExpresswayC (domain2)配置与域和您的CUCM服务器(domain3)一样，您能配置您的CUCM服务器(系统>服务器)与：

IP地址主机名FQDN

- 如果ExpresswayC (domain2)比CUCM服务器(domain3)配置与一个不同的域，则您必须配置CUCM服务器与：

IP地址FQDN

这要求，因为，当ExpresswayC发现CUCM服务器时，并且主机名返回，执行hostname.domain2的DNS查找，不工作，如果domain2和domain3不同的。

证书

除一般证书需求外，必须添加一些工作到附属的替代名称(SAN)证书：

- ExpresswayC

在IM&P服务器配置的聊天节点别名必须添加。这为打算使用传输层安全的统一通信XMPP联邦部署只要求(TLS)和组聊天。假设已经，发现IM&P服务器这自动地被添加到证书签名请求(CSR)。

的所有在CUCM的电话安全配置文件必须添加名称，在FQDN格式，为已加密TLS配置和使用设备要求远程访问。

注意：当您的Certificate Authority (CA)不允许在SAN时的主机名语法FQDN格式只要求。

- ExpresswayE

必须添加用于服务发现的域(domain1)。XMPP联邦域。在IM&P服务器配置的聊天节点别名必须添加。这为统一通信XMPP打算使用两个TLS和分组聊天的联邦部署只要求。这些可以从在ExpresswayC生成的CSR复制。

双NIC

此部分描述配置设置，当使用双重网络接口界面卡(NIC)时。

两个接口

当您配置ExpresswayE为了使用双重网络接口时，请注意两个接口配置并且使用。

The screenshot shows the 'Configuration' tab of the Expressway interface. The 'IP protocol' is set to 'IPv4'. The 'Use dual network interfaces' dropdown is set to 'Yes'. The 'External LAN interface' dropdown is set to 'LAN2'. The 'IPv4 gateway' is set to '10.48.36.200'. The 'IPv6 gateway' is empty. To the right, there are two informational messages: 'Use dual network interfaces set to Yes' and 'External LAN interface used to connect to internet'.

当使用双重网络接口配置与值是时，ExpresswayE在XMPP通信的内部接口只侦听与ExpresswayC。因此，您必须保证此接口正确地配置并且工作。

一个接口-公网IP地址

当仅使用时一个接口，并且您配置与公网IP地址的ExpresswayE，不必采取特别注意事项。

一个接口-专用IP地址

当仅使用时一个接口，并且您配置与专用IP地址的ExpresswayE，您必须配置静态网络地址转换(NAT)地址：

The screenshot shows the 'Configuration' tab of the Expressway interface. The 'IP protocol' is set to 'IPv4'. The 'Use dual network interfaces' dropdown is set to 'No'. The 'IPv4 gateway' is set to '10.48.36.200'. The 'IPv6 gateway' is empty. Below this is the 'LAN 1 - Internal' section. The 'IPv4 address' is set to '10.48.36.57'. The 'IPv4 subnet mask' is set to '255.255.255.0'. The 'IPv4 subnet range' is set to '10.48.36.0 - 10.48.36.255'. The 'IPv4 static NAT mode' dropdown is set to 'On'. The 'IPv4 static NAT address' is set to '20.20.20.20'. To the right, there are three informational messages: 'Use dual network interfaces set to No', 'Private ip address of the Expressway-E', and 'Enabled static NAT Public ip address for which static NAT has been configured to the Expressway-E server'.

在这种情况下，以保证那是重要的：

- ExpresswayC由防火墙允许发送流量到公网IP地址。这叫作NAT反射。

- ExpresswayC的穿越客户端区域配置与匹配在ExpresswayE的静态NAT地址，在这种情况下是20.20.20.20的对等地址。

提示：关于高级网络部署的更多信息是可用的在[思科网真视频通信服务器基本配置\(有Expressway的控制\)部署指南的附录4](#)。

验证

当前没有可用于此配置的验证过程。

故障排除

本部分提供了可用于对配置进行故障排除的信息。

一些特定方案在此部分报道，但是您能也使用为MRA登录尝试提供根据您的诊断记录的所有通信和故障排除信息详细信息的[协作解决方案分析器](#)。

穿越区域

当对等地址配置时，因为IP地址或对等地址不匹配共同名称(CN)，您在日志看到此：

```
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"
```

当密码不正确时，您在ExpresswayE日志看到此：

```
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"
```

双NIC

当双NIC启用时，但是没有使用第二个接口也没有连接，ExpresswayC不能连接到XMPP通信的ExpresswayE在波尔特7400，并且ExpresswayC日志显示此：

```
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

当FQDN由的协作边缘的时SRV记录查找返回不匹配在ExpresswayE配置的FQDN， Jabber日志显示此错误：

```
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
```

在ExpresswayE的诊断记录，您能为哪个域看到Cookie在HTTPS消息设置：

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

SIP域

当需要的SIP域在ExpresswayC时没有被添加， ExpresswayE不接受此域的消息，并且在诊断记录您看到传送给客户端的**403禁止**信息：

```
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"
```