

Guia de solução de problemas para Cisco Webex Hybrid Call Service Connect

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Problemas de configuração de chamada](#)

[Falhas de Handshake TLS mútuo](#)

[Dicas úteis de solução de problemas de TLS mútuo](#)

[Problema 1. O Expressway-E não confia na autoridade de certificação \(CA\) que assinou o certificado do Cisco Webex](#)

[Problema 2. Nome incorreto para verificação de assunto TLS no Expressway-E Zona DNS híbrida do Cisco Webex](#)

[Problema 3. O Expressway-E não envia a cadeia de certificado completa para o Cisco Webex](#)

[Problema 4. O firewall encerra o handshake TLS mútuo](#)

[Problema 5. O Expressway-E é assinado por CA pública, mas o Cisco Webex Control Hub tem certificados alternativos carregados](#)

[Problema 6. O Expressway não está mapeando a chamada de entrada para a zona DNS híbrida do Cisco Webex](#)

[Problema 7. O Expressway-E usa o certificado autoassinado padrão](#)

[Entrada: Cisco Webex para o local](#)

[Problema 1. O Cisco Webex não consegue resolver o nome de host/SRV DNS Expressway-E](#)

[Problema 2. Falha no soquete: A porta 5062 está bloqueada na entrada para o Expressway](#)

[Problema 3. Falha no soquete: O Expressway-E não está escutando na porta 5062](#)

[Problema 4. O Expressway-E ou C não suporta cabeçalhos de rota SIP pré-carregados](#)

[Problema 5. O aplicativo Cisco Webex está recebendo duas notificações de chamada \(brindes\)](#)

[Saída: No local para o Cisco Webex](#)

[Problema 1. O Expressway não consegue resolver o endereço callservice.ciscopark.com](#)

[Problema 2. A porta 5062 está bloqueada para saída do Cisco Webex](#)

[Problema 3. Erro de configuração da regra de pesquisa do Expressway](#)

[Problema 4. Configuração incorreta de CPL do Expressway](#)

[Bidirecional: Cisco Webex para o local ou Local para o Cisco Webex](#)

[Problema 1. O IP Phone/Collaboration Endpoint está oferecendo um codec de áudio diferente de G.711, G.722 ou AAC-LD.](#)

[Problema 2. Tamanho máximo de mensagem de entrada do Unified CM excedido](#)

[Appendix](#)

[Ferramentas de identificação e solução de problemas do Expressway](#)

[Utilitário de verificação de padrão](#)

[Localize o utilitário](#)

[Registro de diagnóstico](#)

Introduction

Este documento descreve a solução Cisco Webex Hybrid Call Service que permite à infraestrutura de controle de chamada atual da Cisco se conectar à Cisco Collaboration Cloud para que elas possam funcionar juntas.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento da oferta Cisco Webex
- Conhecimento da solução Expressway (B2B)
- Conhecimento do Cisco Unified Communications Manager (Unified CM) e da integração com dele com o Expressway
- Unified CM 10.5(2) SU5 ou posterior.
- Expressway (B2B) versão X8.7.1 ou posterior (X8.9.1 é recomendado)
- Expressway (Connector Host) — consulte [Suporte ao host do Expressway Connector para Cisco Webex Hybrid Services](#) para as versões atualmente suportadas

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Unified Communications Manager
- Expressways
- Webex para Windows
- Webexfor Mac
- Webexpara iOS
- Webex para Android
- Endpoints de colaboração da Cisco
- Endpoints de mesa de colaboração
- Telefones IP
- Clientes de software

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

A solução oferece estes recursos:

- Usar o aplicativo Webex como um cliente de software móvel para chamadas de áudio e vídeo

- Use o aplicativo para fazer e receber chamadas de qualquer lugar, como se estivesse no escritório
- Use Webex, Cisco Jabber ou seu telefone de mesa para ligar, sem precisar se preocupar com a opção que usam
- Desbloquear o histórico de chamadas em telefones locais e integrar esse histórico no Webex

O escopo deste guia é abranger questões exclusivas do Hybrid Call Service Connect. Como o Hybrid Call Service Connect é executado no mesmo par Expressway E & C de outras soluções, como acesso móvel e remoto e chamadas Business to Business, os problemas com as outras soluções podem afetar o Hybrid Call Service Connect. Para clientes e parceiros que implantam um par Expressway para usar com o Call Service Connect, o [Guia de Configuração Básica do Cisco VCS Expressway e do VCS Control deve ser consultado antes que você tente implantar o Hybrid Call Service Connect](#). Este guia de solução de problemas aborda as considerações sobre Firewall/NAT junto com o design do Expressway no Apêndice 3 e 4. Revise esta documentação completamente. Além disso, este documento presume que a ativação do host conector do Expressway e do Hybrid Call Service activation foram concluídas.

Problemas de configuração de chamada

Falhas de Handshake TLS mútuo

O Hybrid Call Service Connect usa TLS mútuo (segurança de camada de transporte mútua) para autenticação entre o Cisco Webex e o Expressway-E. Isso significa que o Expressway-E e o Cisco Webex verificam e inspecionam os certificados apresentados. Como os problemas de TLS mútuo são tão comuns durante as novas implantações dos servidores Expressway e a ativação de soluções como o Hybrid Call Service Connect, esta seção fornece informações e dicas úteis para a solução de problemas baseados em certificado entre o Expressways e o Cisco Webex.

O que o Expressway-E verifica?

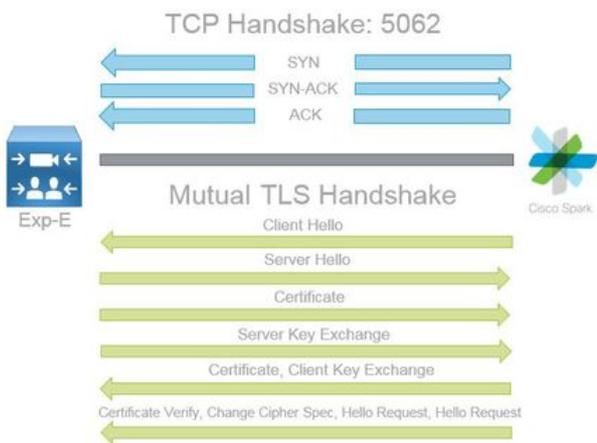
- O certificado do Cisco Webex foi assinado por uma CA pública presente na lista de CAs confiáveis no Expressway-E?
- `callservice.ciscopark.com` está presente no campo de nome alternativo de assunto do certificado do Cisco Webex?

O que o Cisco Webex verifica?

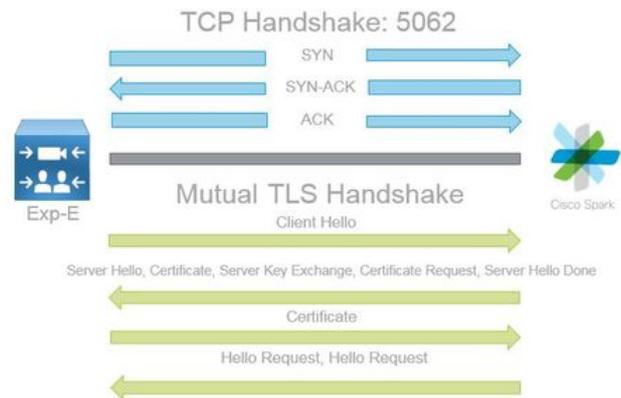
- Se o certificado Expressway-E foi assinado por uma das CAs públicas de confiança do Webex? ([Lista de CAs confiáveis do Cisco Webex](#))
- Caso o Expressway-E não use um certificado assinado publicamente, o certificado do Expressway, juntamente com os certificados raiz e intermediários foram carregados no Cisco Webex Control Hub (<https://admin.ciscopark.com>)?

Isso é explicado como mostrado na imagem.

Spark to On Premise



On Premise to Spark



Dicas úteis de solução de problemas de TLS mútuo

1. Decodificar Handshake TLS mútuo

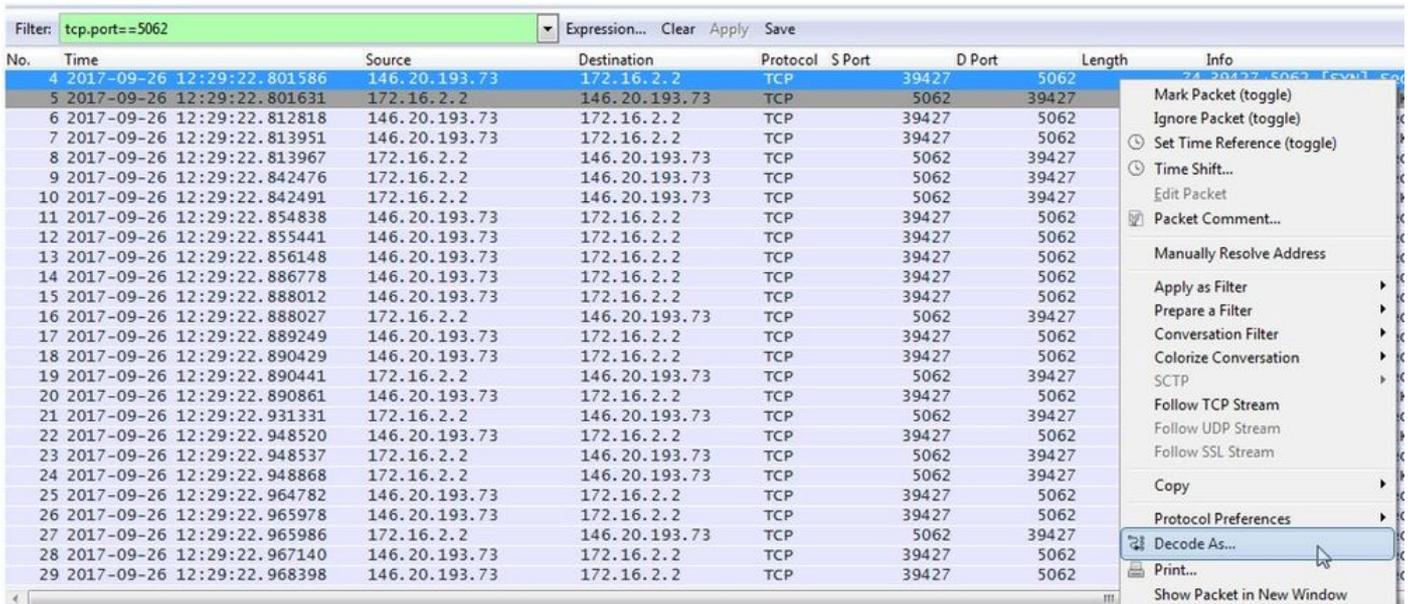
Por padrão, o Wireshark marca o tráfego SIP TLS como porta 5061. O que isso significa é que sempre que você quiser analisar um handshake TLS (mútuo) que ocorre na porta 5062, o Wireshark não saberá como decodificar o tráfego corretamente. Este é um exemplo do handshake TLS mútuo que acontece pela porta 5062 como mostrado na imagem.

No.	Time	Source	Destination	Protocol	S Port	D Port	Length	Info
169	2017-09-20 14:22:13.293817	146.20.193.45	172.16.2.2	TCP	48520	5062	74	48520->5062 [SYN] Seq=0 Win=14600 Len=0 MSS=1380 SACK_PERM=1 TSval=3875387337 TSecr=0 WS=128
170	2017-09-20 14:22:13.293846	172.16.2.2	146.20.193.45	TCP	5062	48520	74	5062->48520 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=444315393 TSecr=
171	2017-09-20 14:22:13.304549	146.20.193.45	172.16.2.2	TCP	48520	5062	66	48520->5062 [ACK] Seq=1 Ack=1 Win=14720 Len=0 TSval=3875387348 TSecr=444315393
172	2017-09-20 14:22:13.305898	146.20.193.45	172.16.2.2	TCP	48520	5062	266	48520->5062 [PSH, ACK] Seq=1 Ack=1 Win=14720 Len=200 TSval=3875387349 TSecr=444315393
173	2017-09-20 14:22:13.305911	172.16.2.2	146.20.193.45	TCP	5062	48520	66	5062->48520 [ACK] Seq=1 Ack=201 Win=30080 Len=0 TSval=444315405 TSecr=3875387349
174	2017-09-20 14:22:13.336342	172.16.2.2	146.20.193.45	TCP	5062	48520	2802	5062->48520 [ACK] Seq=1 Ack=201 Win=30080 Len=2736 TSval=444315436 TSecr=3875387349
175	2017-09-20 14:22:13.336358	172.16.2.2	146.20.193.45	TCP	5062	48520	1426	5062->48520 [PSH, ACK] Seq=2737 Ack=201 Win=30080 Len=1360 TSval=444315436 TSecr=3875387349

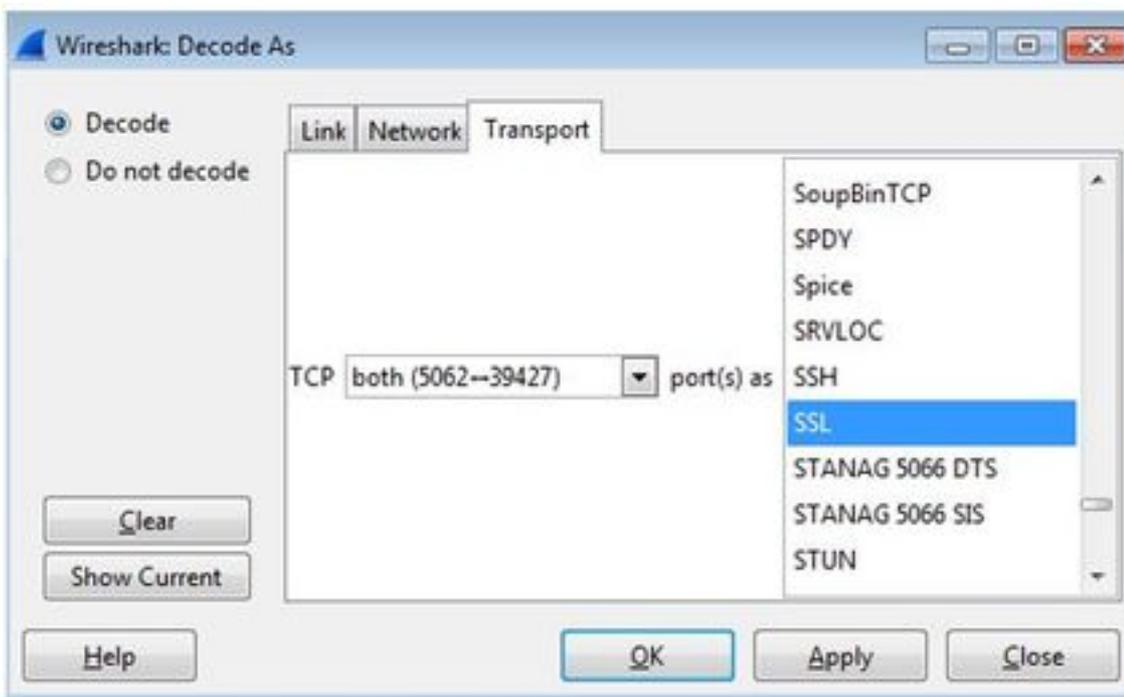
Como você pode ver, essa é a aparência do handshake com as configurações padrão no Wireshark. O pacote de número 175 é o certificado que o Expressway envia para o Cisco Webex. No entanto, não é possível determinar isso sem a decodificação do tráfego. Há dois métodos que podem ser usados para decodificar esse tráfego para que você possa ver com mais facilidade as informações do certificado e as mensagens de erro presentes.

1 bis. Decodificar o fluxo como SSL

a. Ao analisar o handshake TLS mútuo, primeiro filtre a captura por **tcp.port==5062**. Depois disso, clique com o botão direito do mouse no primeiro pacote no fluxo e selecione **Decodificar como...** conforme mostrado na imagem.



b. Uma vez **decodificado como...** estiver selecionada, você verá uma lista na qual poderá selecionar como Decodificar o fluxo selecionado. Na lista, selecione **SSL**, clique em **Apply** e feche a janela. Nesse ponto, o fluxo completo mostra o certificado e as mensagens de erro trocadas no momento do handshake como mostrado na imagem.



1 ter. Ajustar a porta SIP TLS

Quando você ajusta a porta SIP TLS como 5062 nas preferências do Wireshark, será possível ver todos os detalhes que cercam o handshake e isso inclui os certificados. Para fazer essa alteração:

- Abra o Wireshark
- Acesse **Editar > Preferências**
- Expanda Protocolos e selecione **SIP**
- Configure a porta SIP TLS como 5062 e clique em **Aplicar**
- Defina o valor de volta para 5061 quando a análise for concluída como mostrado na imagem.

SIP TCP ports:

SIP TLS Port:

Display raw text for SIP message:

Se analisar a mesma captura agora, você verá os pacotes 169 a 175 decodificados. O pacote 175 mostra o certificado Expressway-E e, se você detalhar o pacote, verá todos os detalhes do certificado como mostrado na imagem.

No.	Time	Source	Destination	Protocol	S Port	D Port	Length	Info
169	2017-09-20 14:22:13.293817	146.20.193.45	172.16.2.2	TCP	48520	5062	74	48520->5062 [SYN] Seq=0 Win=14600 Len=0 MSS=1380 SACK_PERM=1 TSval=3875387337 TSecr=0 WS=128
170	2017-09-20 14:22:13.293846	172.16.2.2	146.20.193.45	TCP	5062	48520	74	5062->48520 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=444315393 TSecr=3875387337 WS=128
171	2017-09-20 14:22:13.304549	146.20.193.45	172.16.2.2	TCP	48520	5062	66	48520->5062 [ACK] Seq=1 Ack=1 Win=14720 Len=0 TSval=3875387348 TSecr=444315393
172	2017-09-20 14:22:13.305898	146.20.193.45	172.16.2.2	TLSv1.2	48520	5062	266	Client Hello
173	2017-09-20 14:22:13.305911	172.16.2.2	146.20.193.45	TCP	5062	48520	66	5062->48520 [ACK] Seq=1 Ack=201 Win=30080 Len=0 TSval=444315405 TSecr=3875387349
174	2017-09-20 14:22:13.336342	172.16.2.2	146.20.193.45	TLSv1.2	5062	48520	2802	Server Hello
175	2017-09-20 14:22:13.336358	172.16.2.2	146.20.193.45	TLSv1.2	5062	48520	1426	Certificate

2. Filtragem do Wireshark

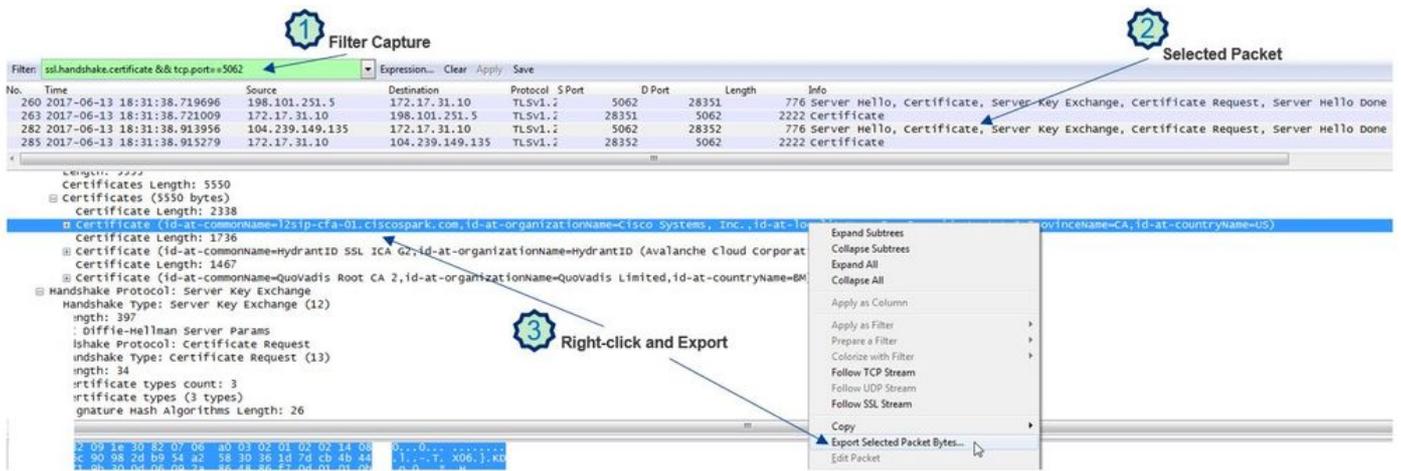
Ao analisar as capturas de pacote, é fácil se perder na quantidade de pacotes existentes em uma determinada captura. É importante entender qual o tipo de tráfego interessa mais para que seja possível filtrar o Wireshark para exibi-lo. Estes são alguns filtros comuns do Wireshark que podem ser usados para obter detalhes sobre um handshake TLS mútuo:

- tcp.port==5062
- ssl && tcp.port==5062
- ssl.handshake.certificate && tcp.port==5062

3. Extrair o certificado de Pcap

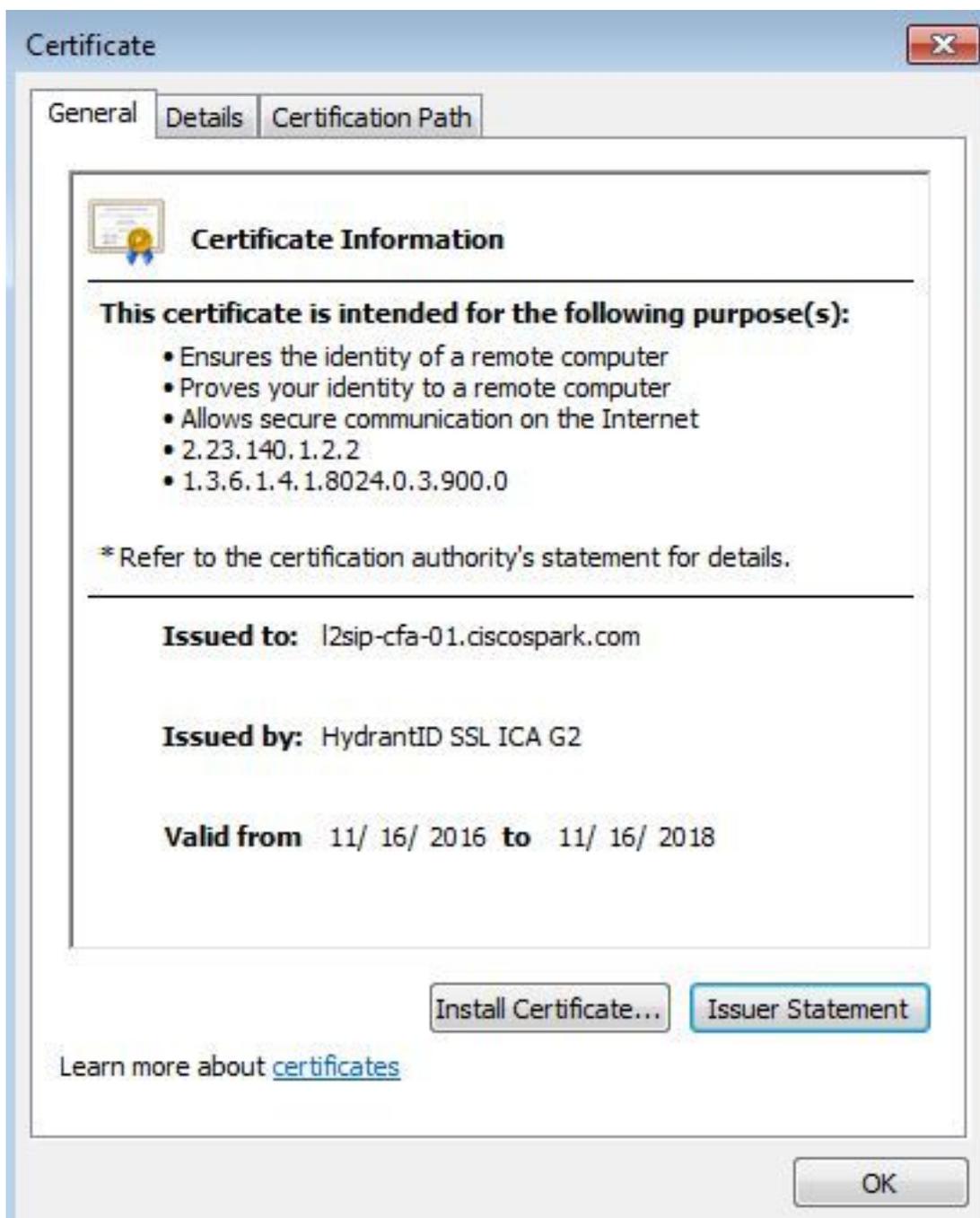
De tempos em tempos, talvez seja necessário obter uma cópia de um certificado (servidor, raiz ou intermediário). Caso não saiba onde encontrar o certificado que está buscando, é possível extrair-lo direto da captura de pacotes. Estas são as etapas de como obter o certificado Cisco Webex que é apresentado em um handshake TLS mútuo.

1. Filtre a captura de pacotes com **ssl.handshake.certificate && tcp.port==5062**
2. Localize o pacote obtido do endereço de servidor do Webex e tem Certificado na seção de Informações.
3. Nos detalhes do pacote, expanda **Secure Socket Layer > TLS Certificate > Handshake Protocol > Certificados**. **Note:** O certificado no final da cadeia é o CA raiz.
4. Clique com o botão direito do mouse no certificado de interesse e selecione **Exportar bytes de pacote selecionados...** conforme mostrado na imagem.



5. Salve o arquivo como a .cer.

6. Clique suas vezes no arquivo salvo para abrir o certificado conforme mostrado na imagem.



4. Ajuste os níveis de log do Expressway

Dois módulos de log estão disponíveis no Expressway e eles podem ajudá-lo a entender melhor a lógica executada pelo Expressway ao analisar os certificados:

- developer.ssl
- developer.zone.zonemg

Por padrão, esses módulos de log são definidos com um nível de informações. Quando definido para um nível de DEPURAÇÃO, você poderá começar a ver as informações sobre a inspeção de certificado que acontece juntamente com para qual zona de tráfego ele é mapeado. Ambas essas funções são relevantes para o Hybrid Call Service.

O exemplo do Expressway-E que faz uma inspeção de SAN no certificado de servidor do Cisco Webex.

```
2017-09-22T11:11:19.485-04:00 amer-expressway01 tvcs: UTCTime="2017-09-22 15:11:19,485"
Module="developer.ssl" Level="INFO" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(1974) "
Method="::ttssl_continueHandshake" Thread="0x7f576cbee700": Detail="Handshake in progress"
Reason="want read/write"
2017-09-22T11:11:19.564-04:00 amer-expressway01 tvcs: UTCTime="2017-09-22 15:11:19,564"
Module="developer.ssl" Level="DEBUG" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(1960) "
Method="::ttssl_continueHandshake" Thread="0x7f576cbee700": Detail="Handshake succeeded"
2017-09-22T11:11:19.564-04:00 amer-expressway01 tvcs: UTCTime="2017-09-22 15:11:19,564"
Module="developer.ssl" Level="DEBUG" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(1629) "
Method="::TTSSL_retrieveCommonName" Thread="0x7f576cbee700": Detail="Found common name in peer
certificate" CommonName="l2sip-cfa-01.ciscospark.com"
2017-09-22T11:11:19.564-04:00 amer-expressway01 tvcs: UTCTime="2017-09-22 15:11:19,564"
Module="developer.ssl" Level="DEBUG" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(1654) "
Method="::TTSSL_retrieveAltNames" Thread="0x7f576cbee700": Detail="Found DNS alt-name in peer
certificate" AltName="l2sip-cfa-01.ciscospark.com"
2017-09-22T11:11:19.564-04:00 amer-expressway01 tvcs: UTCTime="2017-09-22 15:11:19,564"
Module="developer.ssl" Level="DEBUG" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(1654) "
Method="::TTSSL_retrieveAltNames" Thread="0x7f576cbee700": Detail="Found DNS alt-name in peer
certificate" AltName="l2sip-cfa-01.wbx2.com"
2017-09-22T11:11:19.564-04:00 amer-expressway01 tvcs: UTCTime="2017-09-22 15:11:19,564"
Module="developer.ssl" Level="DEBUG" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(1654) "
Method="::TTSSL_retrieveAltNames" Thread="0x7f576cbee700": Detail="Found DNS alt-name in peer
certificate" AltName="l2sip-cfa-01-web.wbx2.com"
2017-09-22T11:11:19.564-04:00 amer-expressway01 tvcs: UTCTime="2017-09-22 15:11:19,564"
Module="developer.ssl" Level="DEBUG" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(1654) "
Method="::TTSSL_retrieveAltNames" Thread="0x7f576cbee700": Detail="Found DNS alt-name in peer
certificate" AltName="l2sip-cfa-web.wbx2.com"
2017-09-22T11:11:19.564-04:00 amer-expressway01 tvcs: UTCTime="2017-09-22 15:11:19,564"
Module="developer.ssl" Level="DEBUG" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(1654) "
Method="::TTSSL_retrieveAltNames" Thread="0x7f576cbee700": Detail="Found DNS alt-name in peer
certificate" AltName="callservice.ciscospark.com"
2017-09-22T11:11:19.564-04:00 amer-expressway01 tvcs: UTCTime="2017-09-22 15:11:19,564"
Module="developer.ssl" Level="DEBUG" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(1654) "
Method="::TTSSL_retrieveAltNames" Thread="0x7f576cbee700": Detail="Found DNS alt-name in peer
certificate" AltName="callservice.call.ciscospark.com"
```

Exemplo do Expressway-E mapeando a conexão MTLs para a zona DNS do Cisco Webex Hybrid:

```
2017-09-22T11:11:19.564-04:00 amer-expressway01 tvcs: UTCTime="2017-09-22 15:11:19,564"
Module="developer.zone.zonemgr" Level="DEBUG"
```

```

CodeLocation="ppcmains/oak/zones/ZoneManager.cpp(1226) "
Method="ZoneManager::getDNSZoneByTLSVerifySubjectName" Thread="0x7f577f0a0700":
this="0x56408ff81220" getDNSZoneByTLSVerifySubjectName classified subject name
callservice.ciscospark.com into DNS zone Hybrid Call Services DNS
2017-09-22T11:11:19.564-04:00 amer-expressway01 tvcs: UTCTime="2017-09-22 15:11:19,564"
Module="developer.zone.zonemgr" Level="DEBUG"
CodeLocation="ppcmains/oak/zones/ZoneManager.cpp(1183) "
Method="ZoneManager::getDNSZoneByTLSVerifySubjectNameList" Thread="0x7f577f0a0700":
this="0x56408ff81220" Detail="Searched for DNS Zones by Subject Name" Found="True"
Candidates="l2sip-cfa-01.ciscospark.coml2sip-cfa-01.ciscospark.coml2sip-cfa-01.wbx2.coml2sip-
cfa-01-web.wbx2.coml2sip-cfa-web.wbx2.comcallservice.ciscospark.com" MatchedZone="Hybrid Call
Services DNS" MatchedIdentity="callservice.ciscospark.com"
2017-09-22T11:11:19.564-04:00 amer-expressway01 tvcs: UTCTime="2017-09-22 15:11:19,564"
Module="developer.zone.zonemgr" Level="DEBUG"
CodeLocation="ppcmains/oak/zones/ZoneManager.cpp(1054) "
Method="ZoneManager::getZoneByIdentities" Thread="0x7f577f0a0700": this="0x56408ff81220"
Detail="getZoneByIdentities, match complete" Identitites="{CN: l2sip-cfa-01.ciscospark.com, Alt-
DNS: l2sip-cfa-01.ciscospark.com, Alt-DNS: l2sip-cfa-01.wbx2.com, Alt-DNS: l2sip-cfa-01-
web.wbx2.com, Alt-DNS: l2sip-cfa-web.wbx2.com, Alt-DNS: callservice.ciscospark.com, Alt-DNS:
callservice.call.ciscospark.com, Alt-DNS: l2sip-a-Webexcall.ciscospark.com, Alt-DNS: l2sip-prod-
11-dfw-public.wbx2.com, Alt-DNS: l2sip-prod-12-dfw-public.wbx2.com, Alt-DNS: l2sip-l2sipproda1-
294-riad-public.wbx2.com, Alt-DNS: l2sip-l2sipproda1-817-riad-public.wbx2.com, Alt-DNS: l2sip-
l2sip-prod-wpsjc-web.ciscospark.com, Alt-DNS: l2sip-l2sip-prod-wpsjc-web.wbx2.com, Alt-DNS:
l2sip-l2sip-prod-wpdfw-web.ciscospark.com, Alt-DNS: l2sip-l2sip-prod-wpdfw-web.wbx2.com, Alt-
DNS: l2sip-cfa-02.wbx2.com, Alt-DNS: Webexcmr-wpa.ciscospark.com, Alt-DNS: Webexcmr-
wpb.ciscospark.com, Alt-DNS: Webexcmr-wpc.ciscospark.com, Alt-DNS: l2sip-wpa-01.wbx2.com, Alt-
DNS: l2sip-wpa-02.wbx2.com, Alt-DNS: l2sip-wpb-01.wbx2.com, Alt-DNS: l2sip-wpb-02.wbx2.com, Alt-
DNS: l2sip-wpc-01.wbx2.com, Alt-DNS: l2sip-wpc-02.wbx2.com}" MatchMechanism="DNSZoneMatch"
MatchedZone="Hybrid Call Services DNS"

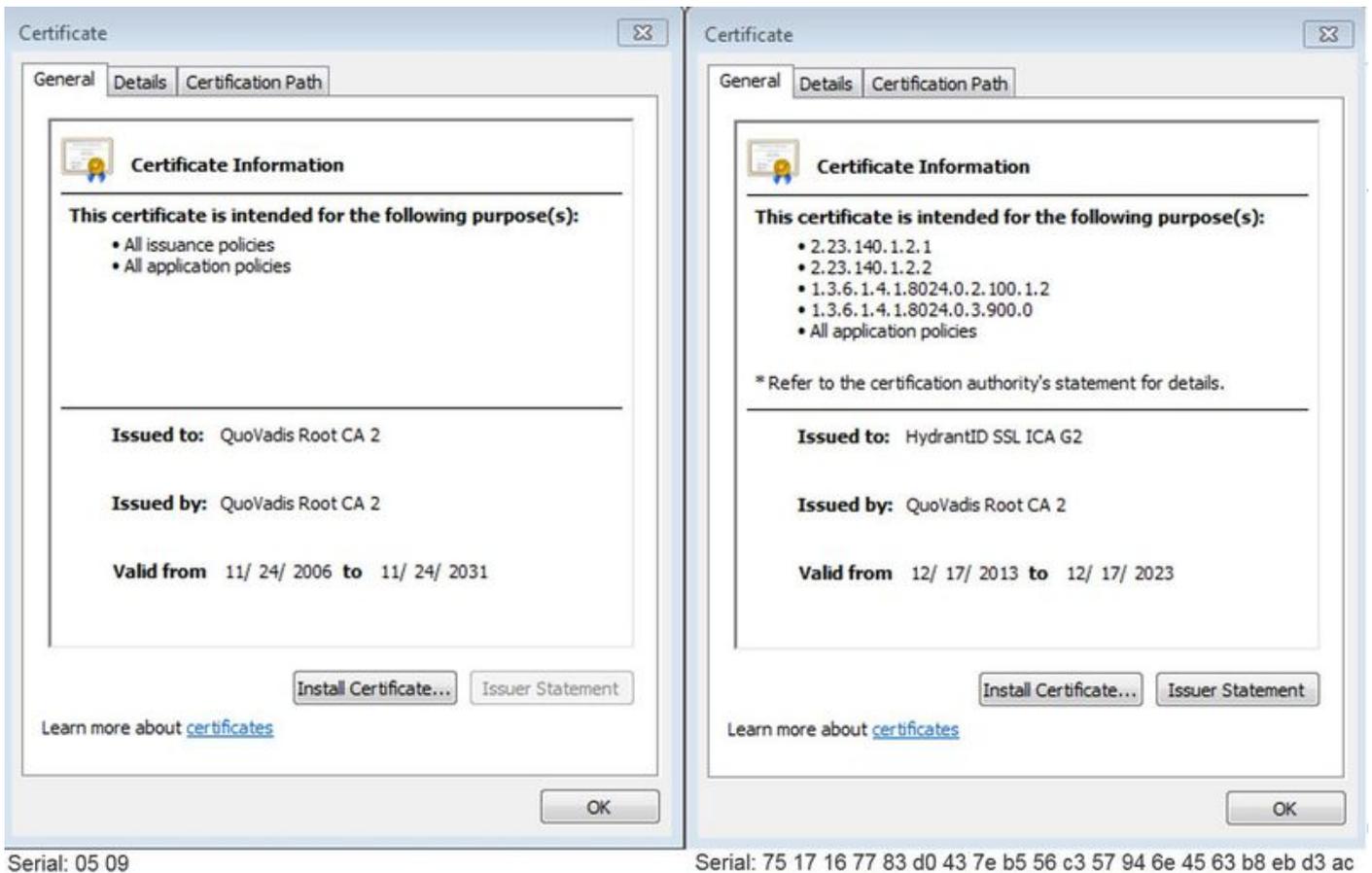
```

Esta é uma lista dos problemas mais comuns relacionados a falhas de TLS mútuo entre o Expressway-E e o Cisco Webex.

Problema 1. O Expressway-E não confia na autoridade de certificação (CA) que assinou o certificado do Cisco Webex

O servidor Cisco Webex que está em comunicação direta com o Expressway-E é chamado de servidor L2SIP. Este servidor L2SIP deve ser assinado por um servidor intermediário com um nome comum de **Hydrant SSL ICA G2**. O intermediário é assinado por uma Certificate Authority raiz que tem um nome comum de **QuoVadis Root CA 2** como mostrado na imagem.

Note: Isso pode estar sujeito a alteração.



A primeira etapa para analisar esse tráfego pela perspectiva de diagnóstico do Expressway é pesquisar por **Conexão TCP**. Depois que pesquisar por **Conexão TCP**, você buscará pelo valor **Dst-port=5062**. Depois de identificar a área nos logs nas quais a conexão foi tentada e estabelecida, é possível buscar pelo handshake TLS que normalmente é indicado pelas entradas de log que mostram handshake em andamento.

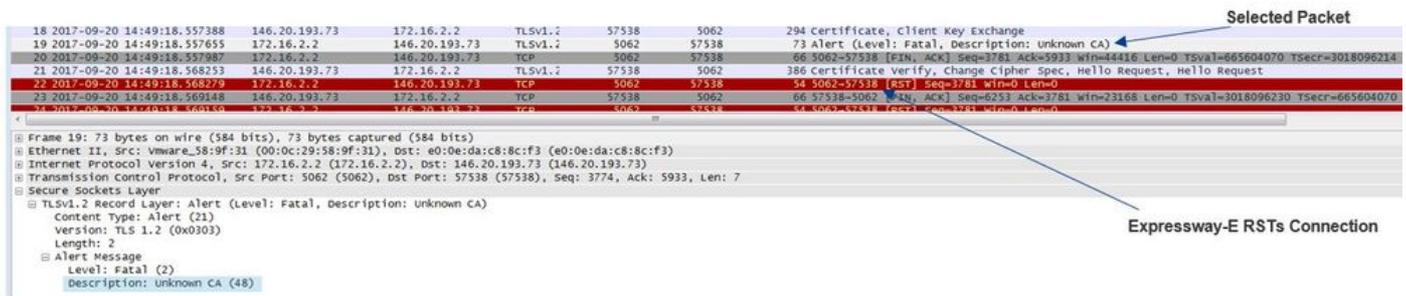
```
2017-09-20T10:49:18.427-04:00 amer-expressway01 tvcs: UTCTime="2017-09-20 14:49:18,426"
Module="developer.ssl" Level="INFO" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(1974) "
Method="::ttssl_continueHandshake" Thread="0x7f29ddefa700": Detail="Handshake in progress"
Reason="want read/write"
```

Caso o Expressway-E não confie em certificados assinados pelo Cisco Webex, é possível que o Expressway-E rejeite o certificado imediatamente após a conclusão do handshake. Isso pode ser percebido nos logs do Expressway-E por essas entradas de log:

```
2017-09-20T10:49:18.724-04:00 amer-expressway01 tvcs: Event="Inbound TLS Negotiation Error"
Service="SIP" Src-ip="146.20.193.73" Src-port="58531" Dst-ip="172.16.2.2" Dst-port="5062"
Detail="self signed certificate in certificate chain" Protocol="TLS" Level="1" UTCTime="2017-09-20 14:49:18,724"
2017-09-20T10:49:18.724-04:00 amer-expressway01 tvcs: UTCTime="2017-09-20 14:49:18,724"
Module="developer.ssl" Level="ERROR" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(68) "
Method="::TTSSLErrorOutput" Thread="0x7f29ddefa700": TTSSL_continueHandshake: Failed to
establish SSL connection iResult="-1" error="1" bServer="true"
localAddress="['IPv4' 'TCP' '172.16.2.2:5062']" remoteAddress="['IPv4' 'TCP' '146.20.193.73:58531']"
ssl_error_reason="error:14089086:SSL routines:ssl3_get_client_certificate:certificate verify
failed"
2017-09-20T10:49:18.724-04:00 amer-expressway01 tvcs: UTCTime="2017-09-20 14:49:18,724"
Module="network.tcp" Level="DEBUG": Src-ip="146.20.193.73" Src-port="58531" Dst-ip="172.16.2.2"
Dst-port="5062" Detail="TCP Connection Closed" Reason="self signed certificate in certificate
chain"
```

A mensagem de erro do Expressway pode induzir em erro um pouco porque se refere a um

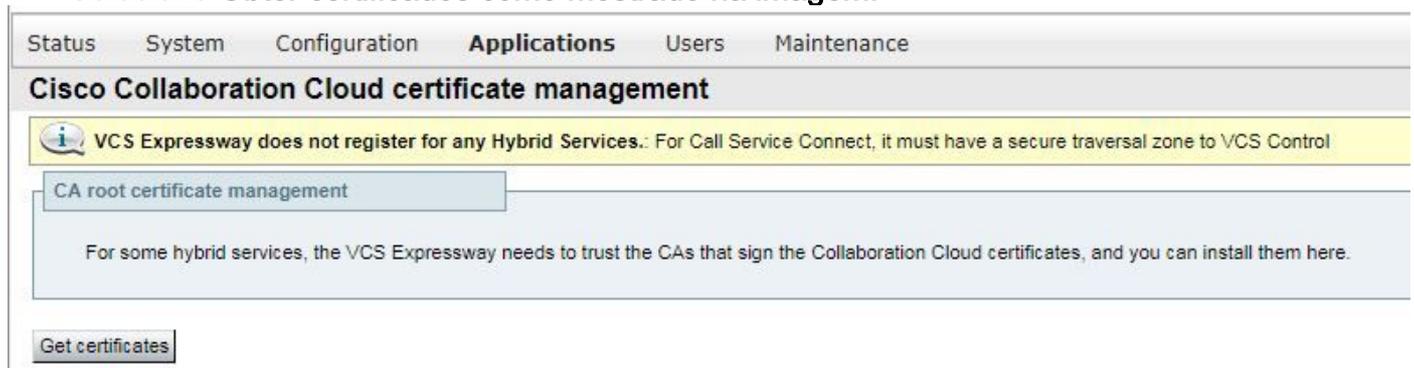
certificado autoassinado na cadeia de certificados. O Wireshark permite que você veja mais atentamente a troca. Da perspectiva da análise de captura de pacotes do Wireshark, você pode ver claramente que quando o ambiente do Webex apresenta seu certificado, o Expressway se vira e rejeita com um certificado com um erro de CA desconhecido como mostrado na imagem.



Solução:

Para resolver a situação, é preciso assegurar que o Expressway-E confie na Certificate Authority do Cisco Webex. Ainda que você possa simplesmente extrair esses certificados do rastreamento do Wireshark e carregá-los no armazenamento de certificado CA confiável no Expressway, o Expressway oferece um método mais simples:

- Faça login no Expressway-E
- Navegue até **Aplicativos > Gerenciamento de certificado de nuvem**
- Selecione **Obter certificados** como mostrado na imagem.



Nesse ponto, a Certificate Authority do Cisco Webex é carregada no armazenamento de CA confiável do Expressway-E (**Manutenção > Segurança > Certificado CA confiável**).

Problema 2. Nome incorreto para verificação de assunto TLS no Expressway-E Zona DNS híbrida do Cisco Webex

Como parte do handshake TLS mútuo, o Hybrid Call Service Connect usa a verificação TLS. Isso significa que, além de confiar nos certificados da CA do Cisco Webex, o Expressway verifica o certificado ao verificar o campo de nome alternativo de assunto (SAN) que é apresentado para assegurar que ele tenha um valor como **callservice.ciscospark.com** presente. Se esse valor não estiver presente, a chamada de entrada falhará.

Neste cenário específico, o servidor Cisco Webex apresenta seu certificado ao Expressway-E. O certificado, na verdade, tem 25 SANs diferentes. Considere o caso no qual o Expressway-E verifica o certificado para ver se há o SAN **callservice.ciscospark.com**, mas não o encontra. Quando essa condição for cumprida, será possível ver um erro semelhante a este no log de diagnóstico:

```

2017-09-20T11:17:42.701-04:00 amer-expressway01 tvcs: Event="Inbound TLS Negotiation Error"
Service="SIP" Src-ip="146.20.193.45" Src-port="46049" Dst-ip="172.16.2.2" Dst-port="5062"
Detail="Peer's TLS certificate identity was unacceptable" Protocol="TLS" Level="1"
UTCTime="2017-09-20 15:17:42,700"
2017-09-20T11:17:42.701-04:00 amer-expressway01 tvcs: UTCTime="2017-09-20 15:17:42,700"
Module="network.tcp" Level="DEBUG": Src-ip="146.20.193.45" Src-port="46049" Dst-ip="172.16.2.2"
Dst-port="5062" Detail="TCP Connection Closed" Reason="Peer's TLS certificate identity was
unacceptable"

```

Se você usar o Wireshark para analisar esse handshake de certificado, será possível encontrá-lo depois que o Cisco Webex apresentar o certificado, o Expressway redefine a conexão logo depois, como mostrado na imagem.

The screenshot shows a network traffic capture in Wireshark. The top part displays a list of packets, with packet 76 selected. The details pane for packet 76 shows the following information:

- Extension (id-ce-subjectAltName)
 - Extension Id: 2.5.29.17 (id-ce-subjectAltName)
 - GeneralNames: 25 items
 - GeneralName: dnsName (2)
 - dnsName: l2sip-cfa-01.ciscospark.com
 - GeneralName: dnsName (2)
 - dnsName: l2sip-cfa-01.wbx2.com
 - GeneralName: dnsName (2)
 - dnsName: l2sip-cfa-01-web.wbx2.com
 - GeneralName: dnsName (2)
 - dnsName: l2sip-cfa-web.wbx2.com
 - GeneralName: dnsName (2)
 - dnsName: callservice.ciscospark.com (SAN Value)
 - GeneralName: dnsName (2)
 - dnsName: callservice.call.ciscospark.com

Para confirmar a configuração deste valor, é possível acessar a zona DNS do Webex Hybrid que foi configurada para a solução. Se tiver o Expressway-E xConfiguration, é possível buscar pela seção de configuração da zona de forma a determinar como o TLS verifica se o nome do assunto foi configurado. No xConfiguration, observe que as zonas são organizadas com a Zona 1 em primeiro lugar. Esta é uma configuração do ambiente problemático analisado acima.

```

*c xConfiguration Zones Zone 6 DNS SIP TLS Verify Mode: "On"
*c xConfiguration Zones Zone 6 DNS SIP TLS Verify Subject Name: "callservice.ciscospark.com"

```

Como você pode ver no exemplo, TLS Verify Subject Name (Nome do assunto de verificação TLS) está definido como **callservice.ciscospark.com** em vez de **callservice.ciscospark.com**. (anote o "l" extra).

Solução:

Para resolver o problema, a Verificação de TLS do nome de assunto precisa ser modificada:

- Faça login no Expressway-E
- Navegue até **Configuração > Zonas > Zonas**
- Selecione **Zona DNS do Webex Hybrid Services**
- Defina o **Verificação de TLS do nome de assunto como callservice.ciscospark.com**
- Selecione **Salvar**

Note: Consulte para ver o comportamento de log de linha de base. Esta seção mostra o Expressway realizando a verificação de certificado e o mapeamento da zona DNS híbrida do Webex.

Note: A partir do código Expressway x12.5 e posterior, uma nova zona "Webex" foi lançada. Essa zona Webex preenche previamente a configuração da zona necessária para comunicação com o Webex. Isso significa que você não precisa mais definir o TLS Subject

Verify Mode (Modo de verificação de assunto TLS) e TLS Verify Subject Name (Verificar nome do assunto TLS). Para simplificar a configuração, é recomendável aproveitar a zona do Webex se você estiver executando x12.5 ou posterior do código do Expressway.

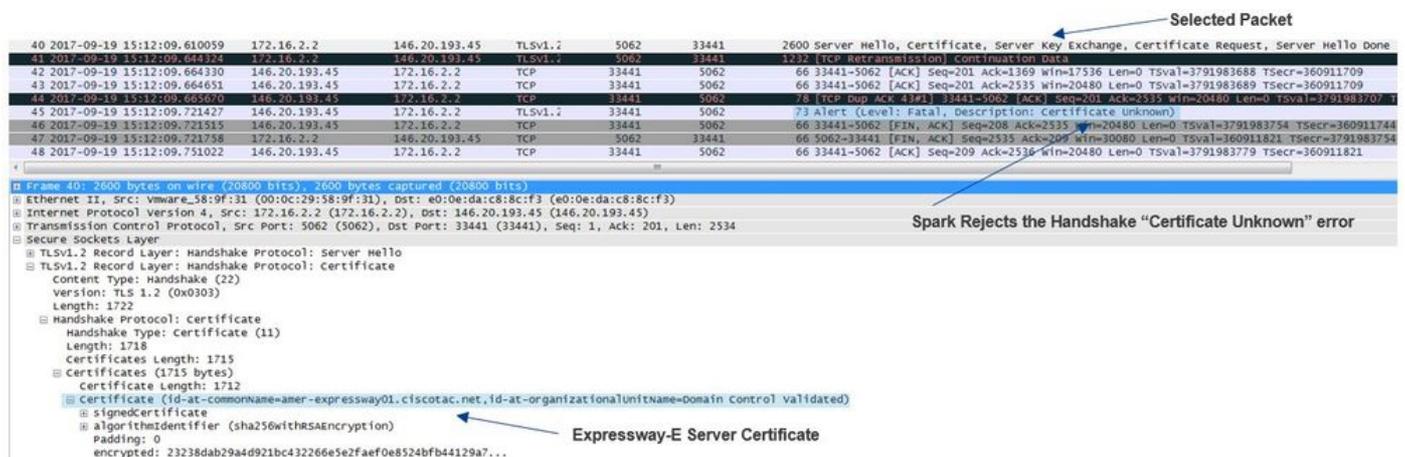
Problema 3. O Expressway-E não envia a cadeia de certificado completa para o Cisco Webex

Como parte do handshake de TLS mútuo, o Cisco Webex precisa confiar no certificado Expressway-E. O Cisco Webex tem uma lista completa de CAs públicas nas quais ele confia. Normalmente, um handshake de TLS é bem-sucedido quando seu certificado Expressway-E é assinado por uma CA pública compatível com o Cisco Webex. Por design, o Expressway-E envia seu certificado somente durante um handshake TLS, apesar de ser assinado por uma CA pública. Para enviar a cadeia completa de certificados (raiz e intermediária), esses certificados devem ser adicionados ao armazenamento de certificados CA confiáveis no próprio Expressway-E.

Caso a condição não seja atendida, o Cisco Webex rejeitará o certificado Expressway-E. Quando você realiza a solução de problemas que corresponde a esse problema, é possível usar os logs de diagnóstico e o tcpdump do Expressway-E. Ao analisar os logs de diagnóstico do Expressway-E, você verá um erro semelhante a este:

```
2017-09-19T11:12:09.721-04:00 amer-expressway01 tvcs: Event="Inbound TLS Negotiation Error"
Service="SIP" Src-ip="146.20.193.45" Src-port="33441" Dst-ip="172.16.2.2" Dst-port="5062"
Detail="sslv3 alert certificate unknown" Protocol="TLS" Level="1" UTCTime="2017-09-19
15:12:09,721"
2017-09-19T11:12:09.721-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 15:12:09,721"
Module="developer.ssl" Level="ERROR" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(68)"
Method=":TTSSLErrorOutput" Thread="0x7fc67c6ec700": TTSSL_continueHandshake: Failed to
establish SSL connection iResult="0" error="1" bServer="true"
localAddress="['IPv4' 'TCP' '172.16.2.2:5062']" remoteAddress="['IPv4' 'TCP' '146.20.193.45:33441']"
ssl_error_reason="error:14094416:SSL routines:ssl3_read_bytes:sslv3 alert certificate unknown"
2017-09-19T11:12:09.721-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 15:12:09,721"
Module="network.tcp" Level="DEBUG": Src-ip="146.20.193.45" Src-port="33441" Dst-ip="172.16.2.2"
Dst-port="5062" Detail="TCP Connection Closed" Reason="Got EOF on socket"
```

Se analisar pela perspectiva do Wireshark, você verá que o Expressway-E apresenta o certificado. Caso expanda o pacote, você verá que apenas o certificado do servidor será enviado. O Cisco Webex rejeita este handshake TLS com uma mensagem de erro de CA desconhecido como mostrado na imagem.



Solução:

Para lidar com o problema nesse cenário, é preciso carregar as CAs raiz e intermediárias

envolvidas na assinatura do certificado Expressway-E para o armazenamento de certificados CA confiável:

Etapa 1. Faça login no Expressway-E.

Etapa 2. Navegue até **Manutenção > Segurança > Certificado CA confiável**.

Etapa 3. Selecione **Escolher arquivo** no menu Carregar próximo à parte inferior da IU.

Etapa 4. Escolha o certificado CA envolvido na assinatura do Expressway-E.

Etapa 5. Selecione **Anexar certificado CA**.

Etapa 6. Repita as etapas para todos os certificados CA envolvidos na assinatura do certificado Expressway-E (Intermediário, Raiz).

Passo 7. Selecione **Anexar certificado CA**.

Quando esse processo for concluído, você verá a cadeia completa de certificados envolvida na assinatura do certificado de servidor Expressway-E inclusa na troca da chave. Esta é uma amostra do que você veria caso estivesse analisando uma captura de pacotes com o Wireshark.

Selected Packet

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------------------------|---------------|---------------|----------|--------|--|
| 175 | 2017-09-20 14:22:13.336358 | 172.16.2.2 | 146.20.193.45 | TLSv1.2 | 5062 | 48520 → 1426 Certificate |
| 176 | 2017-09-20 14:22:13.354189 | 146.20.193.45 | 172.16.2.2 | TCP | 48520 | 5062 → 66 48520-5062 [ACK] Seq=201 Ack=1369 win=17536 Len=0 TSval=3875387398 TSecr=444315436 |
| 177 | 2017-09-20 14:22:13.354815 | 146.20.193.45 | 172.16.2.2 | TCP | 48520 | 5062 → 66 48520-5062 [ACK] Seq=201 Ack=2737 win=20480 Len=0 TSval=3875387399 TSecr=444315436 |
| 178 | 2017-09-20 14:22:13.355985 | 146.20.193.45 | 172.16.2.2 | TCP | 48520 | 5062 → 66 48520-5062 [ACK] Seq=201 Ack=4097 win=23296 Len=0 TSval=3875387400 TSecr=444315436 |
| 179 | 2017-09-20 14:22:13.355999 | 172.16.2.2 | 146.20.193.45 | TLSv1.2 | 5062 | 48520 → 715 Server Key Exchange |
| 180 | 2017-09-20 14:22:13.366930 | 146.20.193.45 | 172.16.2.2 | TCP | 48520 | 5062 → 66 48520-5062 [ACK] Seq=201 Ack=4746 win=26112 Len=0 TSval=3875387411 TSecr=444315455 |
| 197 | 2017-09-20 14:22:13.668592 | 146.20.193.45 | 172.16.2.2 | TLSv1.2 | 48520 | 5062 → 73 Alert (Level: Fatal, Description: Certificate unknown) |
| 198 | 2017-09-20 14:22:13.668644 | 146.20.193.45 | 172.16.2.2 | TCP | 48520 | 5062 → 66 48520-5062 [FIN, ACK] Seq=208 Ack=4746 win=26112 Len=0 TSval=3875387711 TSecr=444315455 |
| 199 | 2017-09-20 14:22:13.668871 | 172.16.2.2 | 146.20.193.45 | TCP | 5062 | 48520 → 66 5062-48520 [FIN, ACK] Seq=4746 Ack=209 win=30080 Len=0 TSval=444315768 TSecr=3875387711 |
| 200 | 2017-09-20 14:22:13.681586 | 146.20.193.45 | 172.16.2.2 | TCP | 48520 | 5062 → 66 48520-5062 [ACK] Seq=209 Ack=4747 win=26112 Len=0 TSval=3875387725 TSecr=444315768 |

Frame 175: 1426 bytes on wire (11408 bits), 1426 bytes captured (11408 bits) on interface 0

Ethernet II, Src: Vmware_S8:19f:31 (00:0c:29:58:19:f3), Dst: e0:0e:da:c8:fc:f3 (e0:0e:da:c8:fc:f3)

Internet Protocol Version 4, Src: 172.16.2.2 (172.16.2.2), Dst: 146.20.193.45 (146.20.193.45)

Transmission Control Protocol, Src Port: 5062 (5062), Dst Port: 48520 (48520), Seq: 2737, Ack: 201, Len: 1360

[2 Reassembled TCP Segments (3938 bytes): #174(2642), #175(1296)]

Secure Sockets Layer

- TLV1.2 Record Layer: Handshake Protocol: Certificate
 - Content Type: handshake (22)
 - Version: TLS 1.2 (0x0303)
 - Length: 3933
 - Handshake Protocol: certificate
 - Handshake Type: certificate (11)
 - Length: 3929
 - Certificates Length: 3926
 - Certificates (3926 bytes)
 - Certificate Length: 1712
 - Certificate (id-at-commonName=amer-expressway01.ciscotac.net, id-at-organizationalUnitName=bonain control validated)
 - Certificate (id-at-commonName=go daddy Secure Certificate Authority - G2, id-at-organizationalUnitName=http://certs.godaddy.com/repositor, id-at-organizationName=GoDaddy.com, Inc., id-at-localityName=Intermediate)
 - Certificate Length: 969
 - Certificate (id-at-commonName=Go Daddy Root Certificate Authority - G2, id-at-organizationName=GoDaddy.com, Inc., id-at-localityName=Scottsdale, id-at-stateOrProvinceName=Arizona, id-at-countryName=US)

Problema 4. O firewall encerra o handshake TLS mútuo

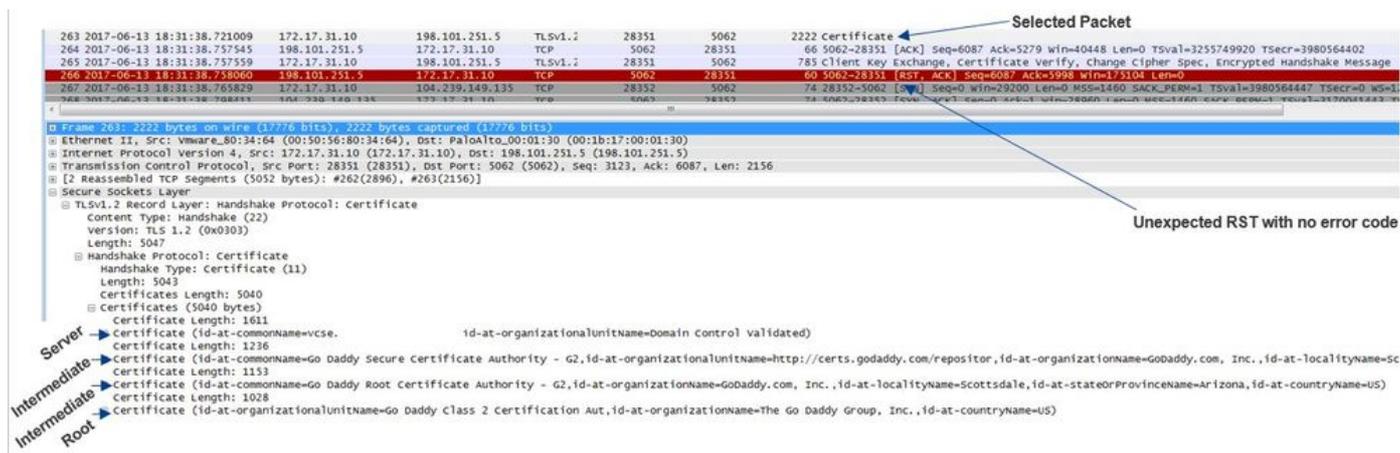
A solução Expressway geralmente faz a interface com um firewall. Diversas vezes, o firewall em linha da solução funciona em algum tipo de inspeção de camada de aplicação. Frequentemente com a solução Expressway, quando o firewall executa a inspeção da camada de aplicação, os administradores veem resultados indesejáveis. Esse problema específico ajuda você a identificar quando a inspeção de uma camada de aplicação do firewall encerra a conexão abruptamente.

Com o uso dos logs de diagnóstico do Expressway, é possível buscar pelo handshake de TLS mútuo. Esse handshake, como mencionado anteriormente, deve acontecer logo depois que a conexão TCP for estabelecida pela porta 5062. Neste cenário, quando o firewall encerra a conexão, você verá esses erros no log de diagnóstico.

```
Thread="0x7f6496669700": TTSSL_continueHandshake: Failed to establish SSL connection iResult="-1" error="5" bServer="false" localAddress="[ 'IPv4' 'TCP' '172.17.31.10:28351' ]"  
2017-06-13T13:31:38.760-05:00 vcse tvcs: Event="Outbound TLS Negotiation Error" Service="SIP"  
Src-ip="172.17.31.10" Src-port="28351" Dst-ip="198.101.251.5" Dst-port="5062" Detail="No SSL error available, probably remote disconnect" Protocol="TLS" Common-name="callservice.ciscospark.com" Level="1" UTCTime="2017-06-13 18:31:38,758"  
2017-06-13T13:31:38.760-05:00 vcse tvcs: UTCTime="2017-06-13 18:31:38,758" Module="network.tcp" Level="DEBUG": Src-ip="172.17.31.10" Src-port="28351" Dst-ip="198.101.251.5" Dst-port="5062" Detail="TCP Connection Closed" Reason="Got EOF on socket"
```

Pela perspectiva da captura de pacotes, você verá que o Expressway-E apresenta o certificado

para o Cisco Webex. Você verá um TCP RST chegando pela direção do Cisco Webex, conforme mostrado na imagem.



A princípio, você pode achar que algo está errado com o certificado Expressway-E. Para solucionar esse problema, você primeiro precisará determinar as respostas para essas perguntas:

- O Expressway-E foi assinado por uma CA pública de confiança do Cisco Webex?
- O certificado Expressway-E e quaisquer certificados envolvidos na assinatura do certificado Expressway-E carregado manualmente para o Cisco Webex Control Hub (<https://admin.ciscospark.com/>)?

Nessa condição específica, a solução foi não usar o Cisco Webex Control Hub para gerenciar os certificados Expressway-E. Isso significa que o certificado do Expressway-E precisa ser assinado por uma CA pública de confiança do Cisco Webex. Ao selecionar o pacote de certificados na captura do Wireshark (como mostrado acima), você poderá ver que o certificado foi assinado por uma CA pública e que a cadeia completa foi enviada para o Cisco Webex. Portanto, o problema não estaria relacionado ao certificado do Expressway-E.

Nesse ponto, caso seja necessário mais isolamento, é possível tirar uma captura de pacote da interface externa do firewall. No entanto, a falta de erro SSL no log de diagnóstico é um ponto de dados importante. Se você lembrar do mostrado acima (Problema 3.), *caso o Cisco Webex não confie no certificado do Expressway-E, será necessário ver algum tipo de razão pela desconexão de SSL*. Nessa condição não havia erro SSL disponível.

Note: Se você fosse obter uma captura de pacotes da interface externa do firewall, não veria um TCP RST oriundo do ambiente do Cisco Webex.

Solução

Nesta solução específica, você, como parceiro ou cliente, precisa confiar em sua equipe de segurança. A equipe precisa investigar se algum tipo de inspeção de camada de aplicação é usada na solução Expressway e, em caso afirmativo, isso deverá ser desativado. [O Apêndice 4 do Guia de implantação de VCS Control e Expressway explica porque é recomendável que os clientes desativem essa funcionalidade.](#)

Problema 5. O Expressway-E é assinado por CA pública, mas o Cisco Webex Control Hub tem certificados alternativos carregados

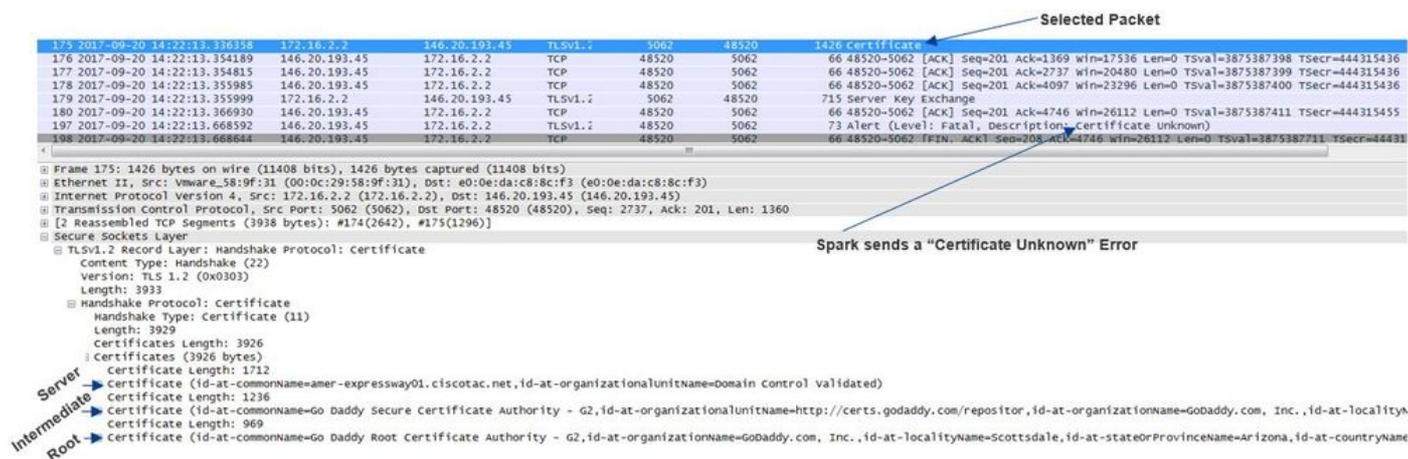
Essa condição específica pode acontecer normalmente quando você implantou a solução

Expressway do zero e não é necessário que o certificado do Expressway-E seja assinado inicialmente por uma CA pública. O que acontece neste cenário é que você carrega o certificado do servidor Expressway-E (que foi assinado internamente) no Cisco Webex Control Hub para que seja possível concluir a negociação de TLS mútuo com êxito. Posteriormente, você acaba por obter o certificado do Expressway-E assinado por uma CA pública, no entanto, esquece de remover o certificado do servidor do Cisco Webex Control Hub. É importante saber que quando um certificado é carregado no Cisco Webex Control Hub, esse certificado tem prioridade sobre esse certificado e essa cadeia que o Expressway apresenta durante o handshake TLS.

Do ponto de vista do log de diagnóstico do Expressway-E, esse problema pode parecer semelhante à assinatura de registro encontrada quando o Cisco Webex não confia no certificado do Expressway-E — por exemplo, o caso do Expressway-E não enviar sua cadeia completa ou o certificado do Expressway-E não estar sendo assinado por uma CA pública confiável pelo Cisco Webex. Abaixo está um exemplo do que você pode esperar dos logs Expressway-E durante o handshake TLS:

```
2017-09-20T10:22:13.669-04:00 amer-expressway01 tvcs: Event="Inbound TLS Negotiation Error"
Service="SIP" Src-ip="146.20.193.45" Src-port="48520" Dst-ip="172.16.2.2" Dst-port="5062"
Detail="sslv3 alert certificate unknown" Protocol="TLS" Level="1" UTCTime="2017-09-20
14:22:13,668"
2017-09-20T10:22:13.669-04:00 amer-expressway01 tvcs: UTCTime="2017-09-20 14:22:13,668"
Module="developer.ssl" Level="ERROR" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(68)"
Method=":TTSSL_ErrorOutput" Thread="0x7f4a2c16f700": TTSSL_continueHandshake: Failed to
establish SSL connection iResult="0" error="1" bServer="true"
localAddress="['IPv4','TCP','172.16.2.2:5062']" remoteAddress="['IPv4','TCP','146.20.193.45:48520']"
ssl_error_reason="error:14094416:SSL routines:ssl3_read_bytes:sslv3 alert certificate unknown"
2017-09-20T10:22:13.669-04:00 amer-expressway01 tvcs: UTCTime="2017-09-20 14:22:13,668"
Module="network.tcp" Level="DEBUG": Src-ip="146.20.193.45" Src-port="48520" Dst-ip="172.16.2.2"
Dst-port="5062" Detail="TCP Connection Closed" Reason="Got EOF on socket"
```

Observe isso pela perspectiva do Wireshark, é possível ver aqui que o Expressway-E apresenta o certificado no item de linha 175. Alguns itens de linha mais abaixo, o ambiente do Cisco Webex rejeita o certificado com um erro de certificado desconhecido, como mostrado na imagem.



Se você selecionar o pacote de certificados que o Expressway-E envia, será possível expandir as informações do certificado para determinar se o Expressway-E

1. foi assinado por uma [CA pública de confiança do Cisco Webex](#) e
2. está incluso na cadeia completa envolvida na assinatura.

Nessa situação, ambas as condições são atendidas. Isso sugere que não há nada errado com o certificado Expressway-E.

Solução

Etapa 1. Faça login no [Cisco Webex Control Hub](#).

Etapa 2. Selecione **Serviços** no painel esquerdo.

Etapa 3. Escolha **Settings** na placa Hybrid Call.

Etapa 4. Vá até a seção Call Service Connect e procure em Certificados para chamadas SIP criptografadas para ver se os certificados indesejados estão listados. Se sim, clique no ícone de lixeira ao lado do certificado.

etapa 5. Selecione **Remove**.

Note: É importante que a análise seja conduzida e que seja determinado que o cliente não está usando os certificados carregados no Webex Control Hub antes de removê-los.

Para obter mais informações sobre como carregar o certificado do Expressway-E no Cisco Webex Control Hub, confira [esta seção no Guia de Implantação do Hybrid Call](#).

Problema 6. O Expressway não está mapeando a chamada de entrada para a zona DNS híbrida do Cisco Webex

O recurso de mapeamento do TLS de entrada funciona em conjunto com a Verificação de TLS do nome do assunto, com ambas configuradas na Zona DNS do Hybrid Call. Esse cenário articula problemas e desafios observados com o Expressway antes de x12.5. No x12 e posteriormente, um novo tipo de zona foi implementado chamado de zona "Webex". Essa zona preenche previamente toda a configuração necessária para a integração com o Webex. Se você estiver executando o x12.5 e implantando o Webex Hybrid Call, é recomendável usar o tipo de zona **Webex** para que o Hybrid Call Services Domain (callservice.webex.com) seja configurado automaticamente para você. Esse valor corresponde ao nome alternativo do assunto do certificado Webex que é apresentado durante o handshake TLS mútuo e permite que a conexão e o mapeamento de entrada para o Expressway sejam bem-sucedidos.

Se você estiver usando uma versão de código abaixo de x12.5 ou não estiver usando a zona Webex, prossiga com a explicação abaixo que demonstra como identificar e corrigir problemas em que o Expressway não está mapeando a chamada de entrada para a zona DNS Webex Hybrid.

O recurso se divide em um processo de três etapas:

1. O Expressway-E aceita o certificado do Cisco Webex.
2. O Expressway-E inspeciona o certificado do Cisco Webex para determinar se há um nome de assunto alternativo que corresponda à verificação de TLS de nome de assunto: callservice.ciscopark.com.
3. O Expressway-E mapeia a conexão de entrada pela zona DNS do Cisco Webex Hybrid.

Caso a autenticação não seja bem-sucedida, isso significa que a validação do certificado falhou. A chamada entra na Zona padrão e é roteada de acordo com as regras de pesquisa fornecidas nos cenários de empresa para empresa, caso empresa para empresa esteja configurado no

Expressway-E.

Como nos outros cenários, é preciso usar o log de diagnóstico e as capturas de pacotes para determinar como é essa falha e usar a captura de pacotes para ver qual lado está enviando o RST. Esta é uma amostra da conexão TCP sendo tentada e estabelecida.

```
2017-09-22T10:09:56.471-04:00 amer-expressway01 tvcs: UTCTime="2017-09-22 14:09:56,471"
Module="network.tcp" Level="DEBUG": Src-ip="148.62.40.52" Src-port="44205" Dst-ip="172.16.2.2"
Dst-port="5062" Detail="TCP Connecting"
2017-09-22T10:09:56.471-04:00 amer-expressway01 tvcs: UTCTime="2017-09-22 14:09:56,471"
Module="network.tcp" Level="DEBUG": Src-ip="148.62.40.52" Src-port="44205" Dst-ip="172.16.2.2"
Dst-port="5062" Detail="TCP Connection Established"
```

Agora que a conexão TCP foi estabelecida, o handshake TLS pode continuar. Você pode ver que logo após o início do handshake, rapidamente acontece um erro.

```
2017-09-22T10:09:57.044-04:00 amer-expressway01 tvcs: UTCTime="2017-09-22 14:09:57,044"
Module="developer.ssl" Level="INFO" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(1974)"
Method=":ttssl_continueHandshake" Thread="0x7f044e7cc700": Detail="Handshake in progress"
Reason="want read/write"
2017-09-22T10:09:57.123-04:00 amer-expressway01 tvcs: Event="Inbound TLS Negotiation Error"
Service="SIP" Src-ip="148.62.40.52" Src-port="44205" Dst-ip="172.16.2.2" Dst-port="5062"
Detail="Peer's TLS certificate identity was unacceptable" Protocol="TLS" Level="1"
UTCTime="2017-09-22 14:09:57,123"
2017-09-22T10:09:57.123-04:00 amer-expressway01 tvcs: UTCTime="2017-09-22 14:09:57,123"
Module="network.tcp" Level="DEBUG": Src-ip="148.62.40.52" Src-port="44205" Dst-ip="172.16.2.2"
Dst-port="5062" Detail="TCP Connection Closed" Reason="Peer's TLS certificate identity was unacceptable"
```

Observe a situação pela perspectiva pcap e será possível obter uma ideia melhor de quem

- está enviando o RST e de
- quais certificados estão sendo passados para determinar se eles estão corretos.

Ao analisar essa captura específica, será possível ver que o Expressway-E envia o RST. Quando você observa o certificado Cisco Webex que é passado, é possível ver que ele envia a cadeia completa. Além disso, você pode concluir que, de acordo com a mensagem de erro no log de diagnóstico, é possível descartar o cenário no qual o Expressway-E não confia nas CAs públicas do Cisco Webex. Do contrário, você verá um erro como "certificado autoassinado na cadeia de certificados". Você pode detalhar o pacote como mostrado na imagem.

| No. | Time | Source | Destination | Protocol | S Port | D Port | Length | Info |
|-----|----------------------------|--------------|--------------|----------|--------|--------|--------|--|
| 60 | 2017-09-22 14:09:57.038603 | 148.62.40.52 | 172.16.2.2 | TCP | 44205 | 5062 | 44205 | 1444 [TCP segment of a reassembled PDU] |
| 61 | 2017-09-22 14:09:57.038610 | 172.16.2.2 | 148.62.40.52 | TCP | 5062 | 44205 | 44205 | 66 5062-44205 [ACK] Seq=4746 Ack=5673 win=41728 Len=0 TSval=100928489 TSe |
| 62 | 2017-09-22 14:09:57.039488 | 148.62.40.52 | 172.16.2.2 | TLSv1.2 | 44205 | 5062 | 5062 | 294 certificate, Client Key Exchange |
| 63 | 2017-09-22 14:09:57.080318 | 172.16.2.2 | 148.62.40.52 | TCP | 5062 | 44205 | 44205 | 66 5062-44205 [ACK] Seq=4746 Ack=5901 win=44416 Len=0 TSval=100928531 TSe |
| 64 | 2017-09-22 14:09:57.122634 | 148.62.40.52 | 172.16.2.2 | TLSv1.2 | 44205 | 5062 | 5062 | 386 Certificate Verify, Change Cipher Spec, Hello Request, Hello Request |
| 65 | 2017-09-22 14:09:57.122648 | 172.16.2.2 | 148.62.40.52 | TCP | 5062 | 44205 | 44205 | 66 5062-44205 [ACK] Seq=4746 Ack=6221 win=47104 Len=0 TSval=100928573 TSe |
| 66 | 2017-09-22 14:09:57.122947 | 172.16.2.2 | 148.62.40.52 | TLSv1.2 | 5062 | 44205 | 44205 | 117 Change Cipher Spec, Encrypted Handshake Message |
| 67 | 2017-09-22 14:09:57.123364 | 172.16.2.2 | 148.62.40.52 | TCP | 5062 | 44205 | 44205 | 66 5062-44205 [FIN, ACK] Seq=4797 Ack=6221 win=47104 Len=0 TSval=100928573 TSe |
| 68 | 2017-09-22 14:09:57.164863 | 148.62.40.52 | 172.16.2.2 | TCP | 44205 | 5062 | 5062 | 66 44205-5062 [ACK] Seq=6221 Ack=4797 win=26624 Len=0 TSval=128002473 TSe |
| 69 | 2017-09-22 14:09:57.170866 | 148.62.40.52 | 172.16.2.2 | TCP | 44205 | 5062 | 44205 | 1434 [TCP segment of a reassembled PDU] |
| 70 | 2017-09-22 14:09:57.170889 | 172.16.2.2 | 148.62.40.52 | TCP | 5062 | 44205 | 54 | 5062-44205 [RST] Seq=4798 win=0 Len=0 |

Selected Packet

4 Frame 62: 294 bytes on wire (2352 bits), 294 bytes captured (2352 bits)

- Ethernet II, Src: e0:0e:da:c8:8c:f3 (e0:0e:da:c8:8c:f3), Dst: vmware_58:9f:31 (00:0c:29:58:9f:31)
- Internet Protocol Version 4, Src: 148.62.40.52 (148.62.40.52), Dst: 172.16.2.2 (172.16.2.2)
- Transmission Control Protocol, Src Port: 44205 (44205), Dst Port: 5062 (5062), Seq: 5673, Ack: 4746, Len: 228
- [5 Reassembled TCP Segments (3700 bytes): #54(1368), #56(1368), #59(1368), #60(1368), #62(228)]
- Secure Sockets Layer
 - TLSv1.2 Record Layer: Handshake Protocol: Multiple Handshake Messages
 - Content Type: Handshake (22)
 - Version: TLS 1.2 (0x0303)
 - Length: 5695
 - Handshake Protocol: Certificate
 - Handshake Type: Certificate (11)
 - Length: 5553
 - Certificates Length: 5550
 - Certificates (5550 bytes)
 - Certificate Length: 2338
 - Certificate (id-at-commonName=12sip-cfa-01.ciscospark.com,id-at-organizationName=Cisco Systems, Inc.,id-at-localityName=San Jose,id-at-stateOrProvinceName=CA,id-at-countryName=US)
 - Certificate Length: 1736
 - Certificate (id-at-commonName=HydrantID SSL ICA G2,id-at-organizationName=HydrantID (Avalanche Cloud Corporation),id-at-countryName=US)
 - Certificate Length: 1467
 - Certificate (id-at-commonName=Quovadis Root CA 2,id-at-organizationName=Quovadis Limited,id-at-countryName=BM)
 - Handshake Protocol: Client Key Exchange

Clique no certificado do servidor Webex e expanda-o para ver os nomes alternativos do assunto

(dnsName) é possível verificar para garantir que **callservice.ciscospark.com** está listado.

Navegue até Wireshark: **Certificado > Extensão > Nomes gerais > GeneralName > dNSName: callservice.ciscospark.com**

Isso confirma totalmente que o certificado Webex está correto.

Agora você pode confirmar que a verificação TLS de nome do assunto está correta. Como mencionado, caso tenha a xConfiguration, é possível buscar a seção de configuração da zona para determinar como a verificação TLS de nome do assunto foi configurada. Algo a se observar sobre a xConfiguration é que as zonas são organizadas com a Zona 1 como a primeira criada. Esta é uma configuração do ambiente problemático analisado acima. Está claro que não há nada errado com a verificação TLS de nome do assunto.

```
*c xConfiguration Zones Zone 6 DNS SIP TLS Verify Mode: "On"
```

```
*c xConfiguration Zones Zone 6 DNS SIP TLS Verify Subject Name: "callservice.ciscospark.com"
```

O próximo item a ser investigado é a **verificação TLS de mapeamento de entrada**. Isso confirma se você está mapeando corretamente a conexão TLS para a zona DNS do Webex Hybrid. O xConfiguration também pode ser usado para analisar isso. No xConfiguration, o **mapeamento de entrada de verificação TLS é chamado de verificação TLS de DNS ZIP InboundClassification**. Como você pode ver neste exemplo, o valor está definido como Desligado.

```
*c xConfiguration Zones Zone 6 DNS SIP TLS Verify InboundClassification: "Off"
```

```
*c xConfiguration Zones Zone 6 Name: "Hybrid Call Services DNS"
```

Como esse valor está definido como Desligado, isso significa que o VCS não consegue tentar mapear conexões de entrada TLS nesta zona. A chamada entra na Zona padrão e é verificada e roteada de acordo com as regras de pesquisa fornecidas nos cenários de empresa para empresa, caso empresa para empresa esteja configurado no Expressway-E.

Solução

Para lidar com isso, é necessário definir o mapeamento de entrada de verificação TLS na zona DNS do Hybrid Call como Ligado. Estas são as etapas para concluir essa etapa.

1. Faça login no Expressway-E
2. Navegue até **Configuração > Zonas > Zonas**
3. Selecione **Zona DNS do Hybrid Call**
4. Em **Mapeamento de entrada de verificação TLS**, escolha **Ligado**
5. Selecione **Salvar**

Note: Consulte para obter informações sobre o comportamento de registro de linha de base. Esta seção mostra o Expressway realizando a verificação de certificado e o mapeamento da zona DNS híbrida do Webex.

Problema 7. O Expressway-E usa o certificado autoassinado padrão

Em algumas novas implantações do Hybrid Call Service Connect, a assinatura do certificado Expressway-E é desconsiderada ou acredita-se que o certificado de servidor padrão pode ser usado. Algumas pessoas acham que isso é possível porque o Cisco Webex Control Hub permite carregar um certificado no portal. (**Serviços > Configurações (no cartão Hybrid Call) > Carregar**

(em Certificados para chamadas criptografadas))

Se você prestar atenção ao enunciado de **Certificados para chamadas SIP criptografadas**, você **verá isto**: 'Usar certificados fornecidos pela lista confiável padrão do Cisco Collaboration ou carregar uma própria. Se você usar uma própria, assegure que os nomes de host estejam em um domínio verificado.' A parte importante dessa declaração é **"assegure que os nomes de host estejam em um domínio verificado."**

Ao solucionar um problema que corresponda a essa condição, tenha em mente que o sintoma dependerá da direção da chamada. Se a chamada tiver sido originada por um telefone no local, é possível que o aplicativo Cisco Webex não toque. Além disso, se você tentou rastrear a chamada pelo histórico de pesquisa do Expressway, descobrirá que a chamada seria feita para o Expressway-E e pararia ali. Se a chamada tiver sido originada de um aplicativo Cisco Webex e tivesse como destino o local, o telefone no local não tocaria. Nesse caso, o histórico de pesquisa do Expressway-E e do Expressway-C não mostraria nada.

Nesse cenário específico, a chamada originou-se em um telefone no local. Usando o histórico de pesquisa do Expressway-E, é possível determinar que a chamada chegou ao servidor. Nesse momento, é possível analisar o log de diagnóstico para determinar o que aconteceu. Para iniciar essa análise, primeiro observe para ver se houve uma tentativa de conexão TCP bem-sucedida na porta 5062. Ao pesquisar os logs de diagnóstico do Expressway-E por "conexão TCP" e buscar o item de linha com a tag "Dst-port=5062", *será possível determinar se a conexão foi bem-sucedida.*

```
2017-09-26T08:18:08.428-04:00 amer-expressway01 tvcs: UTCTime="2017-09-26 12:18:08,426"
Module="network.tcp" Level="DEBUG": Src-ip="146.20.193.45" Src-port="59720" Dst-ip="172.16.2.2"
Dst-port="5062" Detail="TCP Connecting"
```

```
2017-09-26T08:18:08.428-04:00 amer-expressway01 tvcs: UTCTime="2017-09-26 12:18:08,426"
Module="network.tcp" Level="DEBUG": Src-ip="146.20.193.45" Src-port="59720" Dst-ip="172.16.2.2"
Dst-port="5062" Detail="TCP Connection Established"
```

Agora que você confirmou que a conexão TCP foi estabelecida, será possível analisar o handshake TLS mútuo que acontece imediatamente depois. Como é possível ver neste trecho, o handshake falhou e o certificado é desconhecido (**Detail="sslv3 alert certificate unknown"**)

```
2017-09-26T08:18:08.441-04:00 amer-expressway01 tvcs: UTCTime="2017-09-26 12:18:08,441"
Module="developer.ssl" Level="INFO" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(1974) "
Method="::ttssl_continueHandshake" Thread="0x7f930adab700": Detail="Handshake in progress"
Reason="want read/write"
```

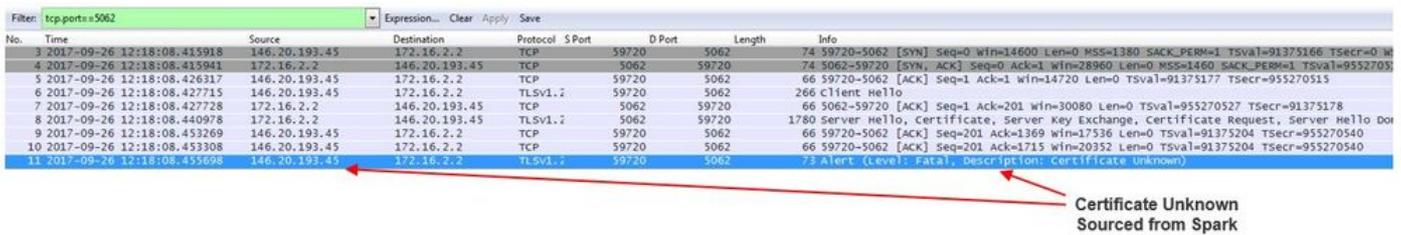
```
2017-09-26T08:18:08.455-04:00 amer-expressway01 tvcs: Event="Inbound TLS Negotiation Error"
Service="SIP" Src-ip="146.20.193.45" Src-port="59720" Dst-ip="172.16.2.2" Dst-port="5062"
Detail="sslv3 alert certificate unknown" Protocol="TLS" Level="1" UTCTime="2017-09-26
12:18:08,455"
```

```
2017-09-26T08:18:08.455-04:00 amer-expressway01 tvcs: UTCTime="2017-09-26 12:18:08,455"
Module="developer.ssl" Level="DEBUG" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(1997) "
Method="::ttssl_continueHandshake" Thread="0x7f930adab700": Detail="Handshake Failed"
Reason="want error ssl"
```

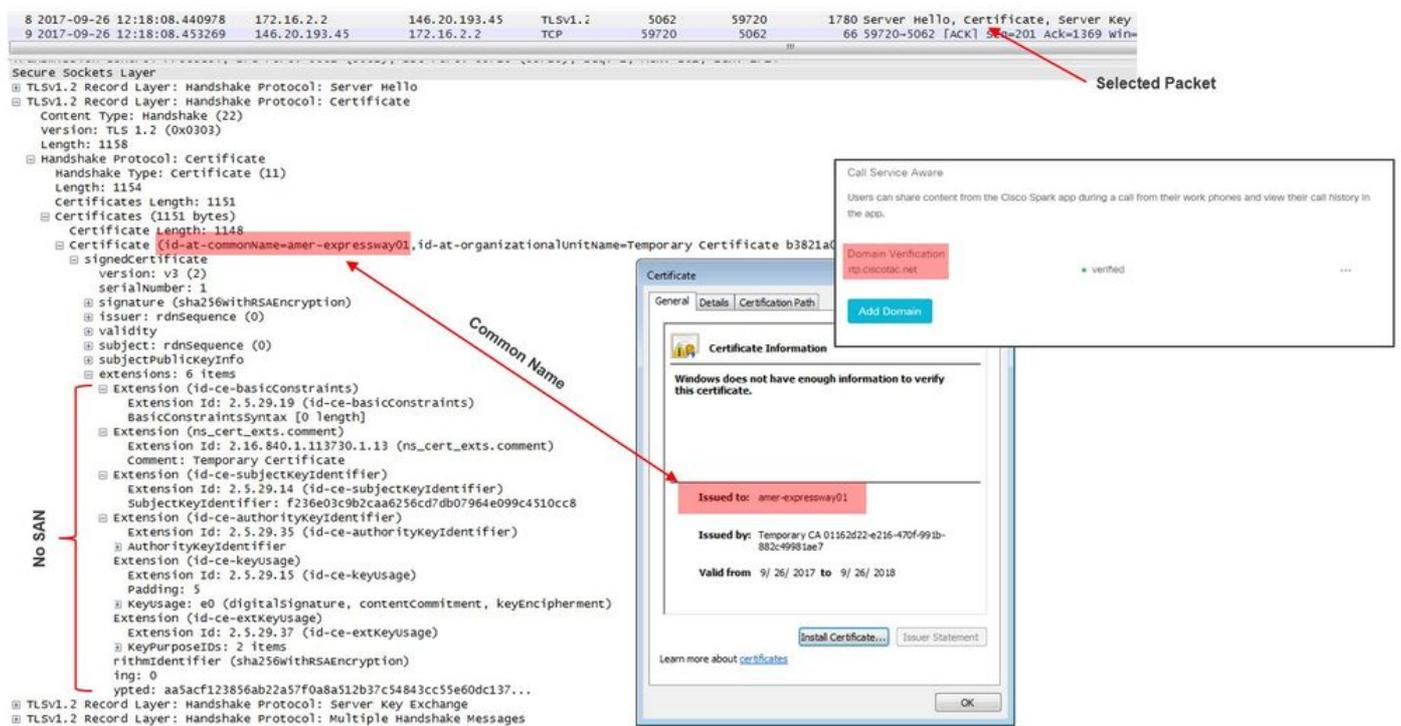
```
2017-09-26T08:18:08.455-04:00 amer-expressway01 tvcs: UTCTime="2017-09-26 12:18:08,455"
Module="developer.ssl" Level="ERROR" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(68) "
Method="::TTSSL_ErrorOutput" Thread="0x7f930adab700": TTSSL_continueHandshake: Failed to
establish SSL connection iResult="0" error="1" bServer="true"
localAddress="['IPv4','TCP','172.16.2.2:5062']" remoteAddress="['IPv4','TCP','146.20.193.45:59720']"
ssl_error_reason="error:14094416:SSL routines:ssl3_read_bytes:sslv3 alert certificate unknown"
```

```
2017-09-26T08:18:08.455-04:00 amer-expressway01 tvcs: UTCTime="2017-09-26 12:18:08,455"
Module="network.tcp" Level="DEBUG": Src-ip="146.20.193.45" Src-port="59720" Dst-ip="172.16.2.2"
Dst-port="5062" Detail="TCP Connection Closed" Reason="Got EOF on socket"
```

Observe com mais atenção a captura de pacotes fornecida no log de diagnóstico do Expressway-E e será possível ver que o erro de certificado desconhecido está se originando da direção do Cisco Webex, como mostrado na imagem.



Se você inspecionar o certificado de servidor padrão do Expressway-E, verá que "Nome comum" e "Nomes alternativos do assunto" não contêm o "Domínio verificado" (`rtp.ciscotac.net`). Você então terá evidência do que causa esse problema, como mostrado na imagem.



Nesse ponto, você determinou que o certificado de servidor Expressway-E precisa ser assinado por uma CA pública ou interna.

Solução

Para resolver o problema existem duas opções:

1. Assinar o certificado Expressway-E com uma [CA pública de confiança do Cisco Webex](#). Faça login no Expressway. Navegue até **Manutenção > Segurança > Certificado de servidor**. Selecione **Gerar CSR**. Insira as informações de certificado obrigatórias e assegure-se de que o campo **Nomes alternativos adicionais** contenha o **Domínio verificado** listado no **Webex Control Hub**. Clique em **Gerar CSR**. Forneça o CSR a uma CA pública de terceiros para ser assinado. Depois que o certificado for devolvido, navegue até **Manutenção > Segurança > Certificados de servidor**. Na seção **Carregar novo certificado** ao lado de **Selecionar** o arquivo de certificado, selecione **Escolher arquivo** e selecione o certificado assinado. Selecione **Carregar dados do certificado de servidor**. Navegue até **Manutenção > Segurança > Certificado CA confiável**. Na seção **Carregar** ao lado de **Selecionar** o arquivo

que contém certificados CA confiáveis selecione Escolher arquivo.Selecione qualquer certificado CA raiz e intermediário oferecido pela CA pública.Selecione **Anexar certificado CA.**Reinicie o Expressway-E.

2. Assinar o certificado Expressway-E com uma CA interna e carregar a CA interna e o Expressway-E no Cisco Webex Control Hub.

Faça login no ExpresswayNavegue até **Manutenção > Segurança > Certificado de servidor.**Selecione **Gerar CSR**Insira as informações de certificado obrigatórias e assegure-se de que o campo *Nomes alternativos adicionais contenha o Domínio verificado listado no Webex Control Hub.*Clique em **Gerar CSR**Forneça o CSR a uma CA pública de terceiros para ser assinadoDepois que o certificado for devolvido, navegue até *Manutenção > Segurança > Certificados de servidor*Na seção *Carregar novo certificado ao lado de Selecionar o arquivo de certificado*, selecione **Escolher arquivo e selecione o certificado assinado.**Selecione **Carregar dados do certificado de servidor**Navegue até **Manutenção > Segurança > Certificado CA confiável.**Na seção *Carregar ao lado de Selecionar o arquivo que contém certificados CA confiáveis selecione Escolher arquivo.*Selecione qualquer certificado CA raiz e intermediário oferecido pela CA pública.Selecione **Anexar certificado CA.**Reinicie o Expressway-E.

- 2a. Carregue o CA interno e o certificado do Expressway-E no Cisco Webex Control Hub
 1. Efetue login no [Cisco Webex Control Hub](#) como administrador.
 2. Selecione Services.
 3. Selecione **Configurações** no cartão Hybrid Call Service.
 4. Na seção **Certificados de chamadas SIP criptografadas**, selecione **Carregar**.
 5. Escolha os certificados CA internos e Expressway-E.

Entrada: Cisco Webex para o local

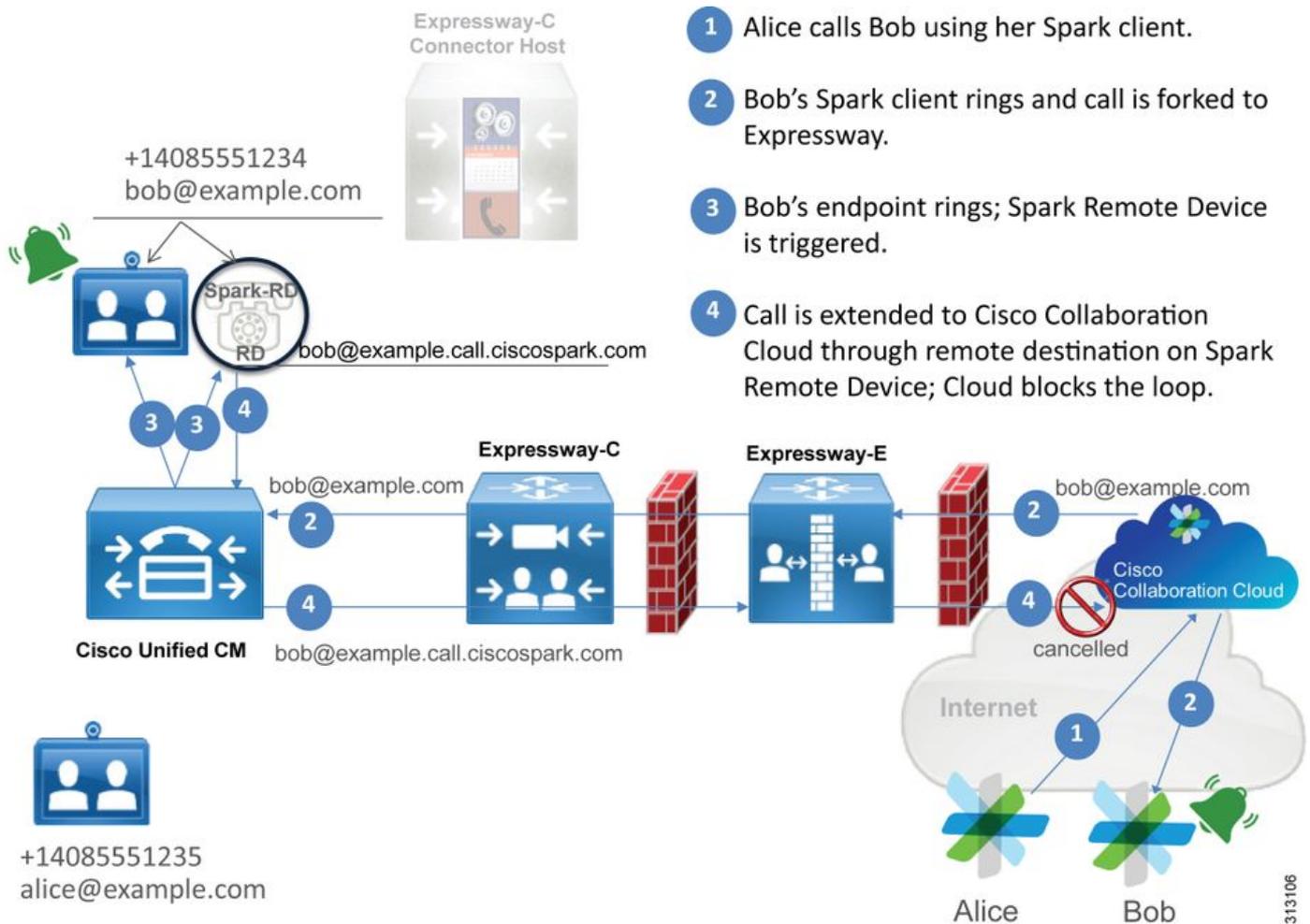
Praticamente todas as falhas de entrada Cisco Webex para o local resulta na indicação do mesmo sintoma: "Quando ligo do aplicativo Cisco Webex para o aplicativo de outro colega, o aplicativo dele toca, mas o telefone do local não". Para solucionar o problema nessa situação, você achará útil entender tanto o fluxo de chamadas quanto a lógica que acontece quando esse tipo de chamada é feita.

Fluxo de lógica de alto nível

1. A parte que liga pelo aplicativo Cisco Webex inicia a chamada
2. O aplicativo do destinatário da chamada toca
3. A chamada é bifurcada para o ambiente Cisco Webex
4. O ambiente Cisco Webex deve executar uma busca de DNS com base no destino SIP configurado no Cisco Webex Control Hub
5. O ambiente Cisco Webex tenta se conectar ao Expressway pela porta 5062
6. O ambiente Cisco Webex tenta fazer um handshake TLS mútuo
7. O ambiente Cisco Webex envia um CONVITE SIP para o Expressway, que passa para o endpoint de colaboração/telefone IP do local
8. O Cisco Webex e a empresa concluem a negociação SIP
9. O Cisco Webex e a empresa começam a enviar e receber mídia.

Fluxo de chamada

Navegue até Aplicativo Cisco Webex > Ambiente Cisco Webex > Expressway-E > Expressway-C > Telefone IP/endpoint de colaboração no local como mostrado na imagem.



Estes são alguns dos problemas comuns com as chamadas de entrada do Webex para a infraestrutura no local.

Problema 1. O Cisco Webex não consegue resolver o nome de host/SRV DNS Expressway-E

Ao considerar o fluxo de chamadas Cisco Webex para o local, a primeira etapa lógica do Cisco Webex trata-se de como entrar em contato com o Expressway no local. Como observado acima, o Cisco Webex tentará conectar-se ao Expressway no local executando uma busca SRV com base no **Destino SIP configurado que está listado na página [Configurações do Hybrid Call Service no Cisco Webex Control Hub](#)**.

Caso tente solucionar o problema dessa situação pela perspectiva do log de diagnóstico do Expressway-E você não verá tráfego do Cisco Webex. Se tentar buscar pela Conexão TCP, você não verá Dst-port=5062 nem nenhum handshake MTLS ou convite SIP subsequente do Cisco Webex.

Caso esta seja a situação, será necessário verificar como o **Destino SIP foi configurado no Cisco Webex Control Hub**. Você também pode usar a **Ferramenta de teste de conectividade do Hybrid para ajudar na solução de problemas**. A ferramenta de teste de conectividade do Hybrid verifica se há um endereço DNS válido, se o Cisco Webex pode se conectar à porta retornada na busca SRV e se o Expressway no local tem um certificado válido no qual o Cisco Webex confia.

1. Faça login no Cisco Webex Control Hub
2. Selecionar serviços
3. Selecione o link Configurações no cartão do Hybrid Call.

4. Na seção Ligar para Service Connect, verifique o domínio usado como endereço SRV SIP público no campo de destino SIP.
5. Se o registro tiver sido inserido corretamente, clique em **Testar para ver se o registro é válido**.
6. Como mostrado abaixo, é possível ver claramente que o domínio público não tem um registro SRV de SIP associado a ele como mostrado na imagem.

SIP Destination ⓘ

mtls.rtp.ciscotac.net Test Save

✖ Your SIP Destination is not configured correctly. [View test results](#)

selecione **Exibir resultados do teste** e você poderá ver mais detalhes sobre o que falhou, como mostrado na imagem.

Verify SIP Destination

DNS Lookup failed. Check that a DNS or SRV record exists for your SIP Destination and that it resolves to one or more valid IP addresses.

Como outra abordagem, também é possível buscar o registro SRV usando nslookup. Estes são os comandos que podem ser executados para verificar se o destino SIP existe.

```
C:\Users\pstoiano>nslookup
> server 8.8.8.8
Default Server: google-public-dns-a.google.com
Address: 8.8.8.8
> set type=SRV
> _sips._tcp.mtls.rtp.ciscotac.net
Server: google-public-dns-a.google.com
Address: 8.8.8.8
DNS request timed out.
timeout was 2 seconds.
DNS request timed out.
timeout was 2 seconds.
*** Request to google-public-dns-a.google.com timed-out
```

Como é possível ver no bloco de código acima, o comando nslookup foi iniciado e o servidor é definido como 8.8.8.8 que é um servidor DNS público do Google. Por fim, você define os tipos de registro para buscar os registros SRV. Nesse ponto, será possível emitir o registro SRV completo que deseja buscar. O resultado líquido é que as solicitações acabam atingindo o tempo limite.

Solução

1. Configure um endereço SRV SIP público para o Expressway-E no local usado para hospedar nomes de domínio público.
2. Configure um nome de host que será resolvido para o endereço IP público do Expressway-E
3. Configure o destino SIP para listar o domínio usado pelo endereço SRV SIP criado na Etapa 1. Faça login no [Cisco Webex Control Hub](#) Selecione **Serviços** Selecione o link **Configurações**

no *cartão de chamada híbrida* Na seção Ligar para Service Connect, insira o domínio usado como endereço SRV SIP público no campo de **destino SIP**. Selecione Salvar

Note: Se o registro SRV SIP que gostaria de usar já esteja sendo aproveitado nas comunicações entre empresas, recomendamos especificar um subdomínio do domínio corporativo como o endereço de detecção SIP no Cisco Webex Control Hub e, conseqüentemente, um registro SRV DNS público, como a seguir:

Serviço e protocolo: _sips._tcp.mtls.example.com

Prioridade: 1

Importância: 10

Número de porta: 5062

Destino: us-expe1.example.com

A recomendação acima foi obtida diretamente do [Guia de design do Cisco Webex Hybrid](#).

Solução alternativa

Caso o cliente não tenha um registro SRV SIP (e não planeje criar um), eles podem listar alternativamente o endereço IP público do Expressway com o sufixo ":5062". Ao fazer isso, o ambiente Webex não tentará uma busca SRV, mas sim se conectar diretamente ao **%Expressway_Pub_IP%:5062**. (Exemplo: 64.102.241.236:5062)

1. Configure o destino SIP a ser formatado como **%Expressway_Pub_IP%:5062**. (Exemplo: 64.102.241.236:5062) Faça login no [Cisco Webex Control Hub](#) Selecione **Serviços** Selecione o link **Configurações no cartão de chamada híbrida** Na seção Ligar para o Service Connect, insira **%Expressway_Pub_IP%:5062 no campo de destino SIP**. Selecione Salvar

Para obter mais informações sobre o endereço de destino SIP e/ou registro SRV que precisam ser configurados. Consulte a seção [Habilitar Hybrid Call Service Connect para sua empresa do Guia de implantação do serviço Cisco Webex Hybrid Call](#) ou o [Guia de Design do Cisco Webex Hybrid](#).

Problema 2. Falha no soquete: A porta 5062 está bloqueada na entrada para o Expressway

Depois que a resolução de DNS for concluída, o ambiente Cisco Webex tentará estabelecer uma conexão TCP pela porta 5062 para o endereço IP que foi retornado durante a busca de DNS. Esse endereço IP será o endereço IP público do Expressway-E no local. Se o ambiente Cisco Webex não conseguir estabelecer esta conexão TCP, a chamada de entrada para o local vai falhar. O sintoma dessa condição específica é o mesmo que praticamente qualquer outra falha de chamada de entrada do Cisco Webex: o telefone no local não toca.

Se estiver solucionando esse problema usando os logs de diagnóstico do Expressway, você não verá nenhum tráfego do Cisco Webex. Se tentar buscar pela Conexão TCP, você não verá tentativas de conexão de Dst-port=5062 ou nenhum handshake MTLS ou convite SIP subsequente do Cisco Webex. Como os logs de diagnóstico do Expressway-E não são úteis nessa situação, você terá alguns métodos possíveis de verificação:

1. Obter uma captura de pacotes da interface externa do firewall
2. Use o utilitário de verificação de porta
3. Use a ferramenta Hybrid Connectivity Test

Como a ferramenta Hybrid Connectivity Test é integrada ao Cisco Webex Control Hub e simula o

ambiente Cisco Webex tentando se conectar ao Expressway no local, ela é o melhor método de identificação disponível. Para testar a conectividade TCP na empresa:

1. Faça login no Cisco Webex Control Hub
2. Selecionar serviços
3. Selecione o link Configurações no cartão do Hybrid Call
4. Na seção Ligar para o Service Connect, verifique se o valor inserido em destino SIP está correto
5. Clique em Testar como mostrado na imagem.

SIP Destination ⓘ

64.102.241.236:5062

Test Save

✖ Your SIP Destination is not configured correctly. [View test results](#)

6. Como o teste falhou, é possível clicar no link **Exibir resultados do teste para verificar os detalhes como mostrado na imagem.**

Verify SIP Destination

IP address lookup

IP
64.102.241.236

Test for 64.102.241.236:5062

| Tests | Result | Details |
|------------------|---------------|--|
| Connecting to IP | Successful | |
| Socket test | Failed | TCP Connection failure: Check network connectivity, connection speed, and/or firewall configuration. |
| SSL Handshake | Not performed | |
| Ping | Not performed | |

Como observado na imagem acima, é possível ver que o teste de soquete falhou ao tentar se conectar a 64.102.241.236:5062. Ter esses dados além dos pcaps/logs de diagnóstico do Expressway não mostra nenhuma tentativa de conexão, você agora tem evidência suficiente para investigar a configuração do firewall ACL/NAT/roteamento.

Solução

Como esse problema específico não é causado pelo ambiente Cisco Webex ou pelo equipamento de colaboração no local, você precisa se concentrar na configuração do firewall. Como você não pode necessariamente prever o tipo de firewall com que vai interagir, será necessário confiar em alguém que tenha familiaridade com o dispositivo. É possível que esse problema possa estar relacionado a um problema de configuração de firewall ACL, NAT ou roteamento.

Problema 3. Falha no soquete: O Expressway-E não está escutando na porta 5062

Essa condição específica frequentemente é diagnosticada incorretamente. Muitas vezes, assume-se que o firewall é a causa do bloqueio no tráfego pela porta 5062. Para solucionar esse problema específico, é possível usar as técnicas no cenário "Entrada da porta 5062 bloqueada no Expressway" acima. Você verá que a ferramenta Hybrid Connectivity Test e qualquer outra ferramenta usada para verificar a conectividade das portas vai falhar. A primeira suposição é que o firewall está bloqueando o tráfego. A maioria das pessoas vai verificar duplamente o log de diagnóstico do Expressway-E para determinar se conseguem ver a conexão TCP tentando ser estabelecida. Eles vão obter uma visão geral de um item de linha do log, como mostrado na imagem.

```
2017-09-19T14:01:46.462-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 18:01:46,461"  
Module="network.tcp" Level="DEBUG": Src-ip="146.20.193.73" Src-port="40342" Dst-ip="172.16.2.2"  
Dst-port="5062" Detail="TCP Connecting"
```

Nessa condição, a entrada de log específica acima não existirá. Portanto, muitas pessoas vão diagnosticar incorretamente a condição e vão presumir que é o firewall.

Se uma captura de pacotes for incluída com o log de diagnóstico, será possível ver que o firewall não é a causa. Abaixo está uma amostra de captura de pacotes desse cenário no qual o Expressway-E não estava acompanhando pela porta 5062. Essa captura filtrada usando `tcp.port==5062` como o filtro aplicado como mostrado na imagem.

| No. | Time | Source | Destination | Protocol | S Port | D Port | Length | Info |
|-----|----------------------------|---------------|---------------|----------|--------|--------|--------|--|
| 55 | 2017-09-19 14:56:46.625745 | 146.20.193.73 | 172.16.2.2 | TCP | 34351 | 5062 | 74 | 34351->5062 [SYN] Seq=0 win=14600 Len=0 MSS=1380 |
| 56 | 2017-09-19 14:56:46.625789 | 172.16.2.2 | 146.20.193.73 | TCP | 5062 | 34351 | 54 | 5062->34351 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 57 | 2017-09-19 14:56:46.653157 | 146.20.193.73 | 172.16.2.2 | TCP | 35883 | 5062 | 74 | 35883->5062 [SYN] Seq=0 win=14600 Len=0 MSS=1380 |
| 58 | 2017-09-19 14:56:46.653173 | 172.16.2.2 | 146.20.193.73 | TCP | 5062 | 35883 | 54 | 5062->35883 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |

Annotations: Spark TCP SYN packet received (pointing to packet 55), Immediate RST sent from the Expressway (pointing to packet 56).

Como é possível ver na captura de pacotes obtida pelo Expressway-E, o tráfego pela porta tcp 5062 não será bloqueado pelo firewall e, na verdade, está chegando. No pacote número 56, é possível ver que o Expressway-E está enviando o RST imediatamente depois da chegada do pacote TCP SYN inicial. Com essas informações, é possível concluir que o problema está isolado do Expressway-E recebendo o pacote; você precisa solucionar o problema pela perspectiva do Expressway-E. Com as evidências, considere possíveis razões pelas quais o Expressway-E faria RST no pacote. Duas possibilidades que poderiam ser atribuídas a esse comportamento são:

1. O Expressway-E tem algum tipo de regras de firewall configuradas que podem estar bloqueando o tráfego
2. O Expressway-E não está ouvindo em busca de tráfego TLS mútuo e/ou não está ouvindo em busca de tráfego pela porta 5062.

A funcionalidade de firewall do Expressway-E existe em *System > Protection > Firewall rules > Configuration* (Sistema > Proteção > Regras de firewall > Configuração). Quando isso foi verificado nesse ambiente, não havia configuração de firewall.

Há várias maneiras de verificar se o Expressway-E está ouvindo o tráfego TLS mútuo pela porta 5062. Você pode fazer isso pela interface da Web ou pelo CLI como usuário raiz.

Pela raiz do Expressway, se você emitir `netstat -an | grep ':5062'`, você deve obter alguma saída semelhante à que você vê abaixo.

```

~ # netstat -an | grep ':5062'
tcp        0      0 172.16.2.2:5062      0.0.0.0:*           LISTEN  <--  Outside
Interface
tcp        0      0 192.168.1.6:5062     0.0.0.0:*           LISTEN  <--  Inside Interface
tcp        0      0 127.0.0.1:5062      0.0.0.0:*           LISTEN
tcp        0      0 :::1:5062            :::*                 LISTEN

```

Essas informações também podem ser obtidas pela interface da Web do Expressway-E. Consulte as etapas abaixo para reunir essas informações

1. Faça login no Expressway-E
2. Navegue até **Maintenance Tools > Port usage > Local inbound ports (Ferramentas de manutenção > Utilização de porta > Portas de entrada locais)**
3. Procure por tipo SIP e porta de IP 5062. (destacado em vermelho como mostrado na imagem)

| Type | Description | Protocol | IP address | IP port | Transport | Actions |
|-------|-----------------------|----------|-------------|---------|-----------|---------------------------|
| H.323 | Registration UDP port | H.323 | 192.168.1.6 | 1719 | UDP | View/Edit |
| H.323 | Registration UDP port | H.323 | 172.16.2.2 | 1719 | UDP | View/Edit |
| SIP | TCP port | SIP | 192.168.1.6 | 5060 | TCP | View/Edit |
| SIP | TCP port | SIP | 172.16.2.2 | 5060 | TCP | View/Edit |
| SIP | TLS port | SIP | 192.168.1.6 | 5061 | TCP | View/Edit |
| SIP | TLS port | SIP | 172.16.2.2 | 5061 | TCP | View/Edit |
| SIP | Mutual TLS port | SIP | 192.168.1.6 | 5062 | TCP | View/Edit |
| SIP | Mutual TLS port | SIP | 172.16.2.2 | 5062 | TCP | View/Edit |

Agora que você sabe o que deveria ver, será possível comparar ao ambiente atual. Pela perspectiva do CLI, quando executa `netstat -an | grep ':5062'`, a saída é assim:

```

~ # netstat -an | grep ':5062'
tcp        0      0 127.0.0.1:5062      0.0.0.0:*           LISTEN
tcp        0      0 :::1:5062            :::*                 LISTEN
~ #

```

Além disso, a interface da Web não mostra a porta TLS mútua listada nas portas de entrada locais

| Type | Description | Protocol | IP address | IP port | Transport |
|-------|---------------------------|----------|-------------|-------------|-----------|
| H.323 | Call signaling port range | H.323 | 192.168.1.6 | 15000-19999 | TCP |
| H.323 | Call signaling port range | H.323 | 172.16.2.2 | 15000-19999 | TCP |
| H.323 | Registration UDP port | H.323 | 192.168.1.6 | 1719 | UDP |
| H.323 | Registration UDP port | H.323 | 172.16.2.2 | 1719 | UDP |
| SIP | TCP port | SIP | 192.168.1.6 | 5060 | TCP |
| SIP | TCP port | SIP | 172.16.2.2 | 5060 | TCP |
| SIP | TLS port | SIP | 192.168.1.6 | 5061 | TCP |
| SIP | TLS port | SIP | 172.16.2.2 | 5061 | TCP |

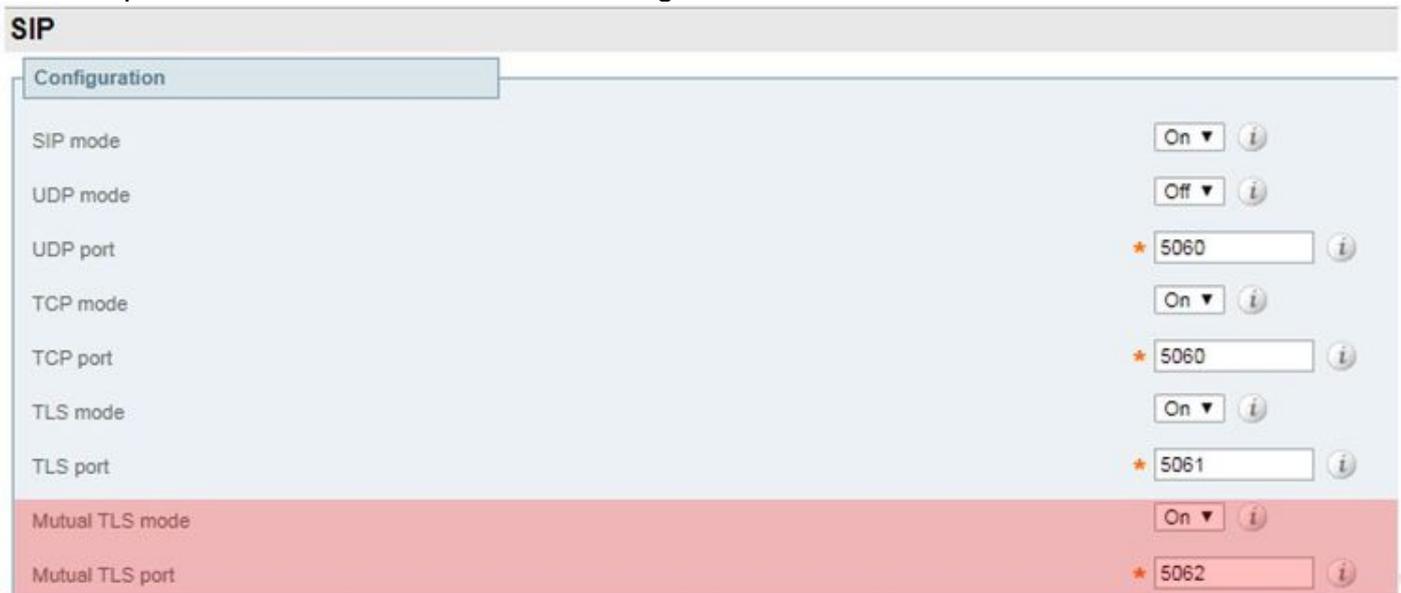
Com esses dados, é possível concluir que o Expressway-E não está acompanhando em busca de tráfego TLS mútuos.

Solução

Para resolver esse problema, é necessário garantir que o modo de TLS mútuos esteja ativado e que a porta de TLS mútuos esteja definida como 5062 no Expressway-E:

1. Faça login no Expressway-E
2. Navegue até **Configuration > Protocols > SIP (Configuração > Protocolos > SIP)**
3. Assegure-se de que o TLS mútuos esteja definido como **Ligado**
4. Certifique-se de que a porta de TLS mútuos esteja definida como **5062**

5. Clique em **Salvar** como mostrado na imagem.



Problema 4. O Expressway-E ou C não suporta cabeçalhos de rota SIP pré-carregados

No Hybrid Call Service Connect, o roteamento de chamada é realizado com base no **cabeçalho da rota**. O cabeçalho da rota é preenchido como base nas informações que a parte Call Service Aware (Expressway Connector) da solução oferece ao Cisco Webex. O host do conector do Expressway consulta o Unified CM em busca de usuários que estão ativados para o Call Service e obtém tanto a **URI do diretório** e o **FQDN do cluster do cluster inicial do Unified CM**. Consulte este exemplo, usando Alice e Bob:

| URI do diretório | Cabeçalho de rota de destino |
|-------------------|------------------------------|
| bob@example.com | emea-cucm.example.com |
| alice@example.com | us-cucm.example.com |

Se Alice ou Bob fizerem uma chamada, a chamada será roteada para o Unified CM no local para que possa ser ancorada no Cisco WebexRD antes de direcionar para o usuário chamado.

Se Alice estivesse ligando para Bob, a chamada seria roteada para o *FQDN do cluster inicial do Unified CM de Alice (us-cucm.example.com)*. Se você analisar o CONVITE SIP enviado pelo Cisco Webex envia a entrada para o Expressway-E, verá as seguintes informações no cabeçalho SIP

URI da solicitação sip: bob@example.com
Cabeçalho de rota sip:us-cucm.example.com;lr

Do ponto de vista do Expressway, as regras de pesquisa são configuradas para rotear a chamada não pelo URI de solicitação, mas sim pelo **cabeçalho da rota (us-cucm.example.com)** — neste caso, o cluster inicial do Unified CM de Alice.

Com esse conjunto básico, é possível entender situações de solução de problemas nas quais os Expressways são configurados incorretamente, o que faz com que a lógica acima não funcione. Como em praticamente todas as falhas de configuração de chamada de entrada do Hybrid Call Service Connect, o sintoma é que o *telefone no local não toca*.

Antes de analisar os logs de diagnóstico no Expressway, considere como identificar esta chamada:

1. A URI de solicitação SIP será a **URI de diretório do destinatário da chamada**.
2. O campo SIP FROM será formatado com o **chamador** listado como **"Nome Sobrenome"**
<sip:WebexDisplayName@subdomain.call.ciscospark.com>

Com essas informações é possível pesquisar os logs de diagnóstico por **URI de diretório do destinatário da chamada, Nome e sobrenome do chamador ou endereço SIP do Cisco Webex do chamador**. Se você não tiver nenhuma dessas informações, poderá pesquisar em **"CONVITE SIP:"**, que localiza todas as chamadas SIP em execução no Expressway. Depois de identificar o CONVITE SIP da chamada de entrada, é possível localizar e copiar a ID de chamada do SIP. Depois que tiver esse valor, você poderá apenas pesquisar nos logs de diagnóstico com base na ID de chamada para ver todas as mensagens correlacionadas a esse log de chamada.

Outra coisa que ajudará a isolar o problema de roteamento é determinar a distância que a chamada percorre na empresa. Você pode tentar pesquisar as informações acima no Expressway-C para ver se a chamada foi roteada até ali. Em caso afirmativo, você provavelmente deverá começar a investigação por aqui.

Neste cenário, é possível ver que o Expressway-C recebeu o CONVITE do Expressway-E.

```
2017-09-19T14:16:15.836-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-19 18:16:15,830"
Module="network.sip" Level="DEBUG": Action="Received" Local-ip="192.168.1.5" Local-port="26847"
Src-ip="192.168.1.6" Src-port="7003" Msg-Hash="11449260850208794722"
SIPMSG:
|INVITE sip:jorobb@rtp.ciscotac.net SIP/2.0
Via: SIP/2.0/TLS 192.168.1.6:7003;egress-
zone=HybridCallServiceTraversal;branch=z9hG4bKc81c6c4dddef7ed6be5bdce9868fb019913;proxy-call-
id=a82052ef-6fd7-4506-8173-e73af6655b5d;rport
Via: SIP/2.0/TLS 192.168.1.6:5073;branch=z9hG4bKb0eba6d700dfdf761a8ad97fff3c240124;x-cisco-
local-service=nettle;received=192.168.1.6;rport=43119;ingress-zone=DefaultZone
Via: SIP/2.0/TLS 64.102.241.236:5061;egress-
zone=DefaultZone;branch=z9hG4bK6fe399bae58fb0d70c9d69b8e37e13e5912.4248943487bff4af6f649b586c769
6bb;proxy-call-id=f2d15853-c81f-462f-b3e5-c08124f344a3;received=172.16.2.2;rport=25016
Via: SIP/2.0/TLS
192.168.5.66:5062;branch=z9hG4bK0f455ca79cf1b0af5637333aa5286436;received=146.20.193.45;rport=35
464;ingress-zone=HybridCallServicesDNS
Via: SIP/2.0/TLS 127.0.0.1:5070;branch=z9hG4bK-383039-
8f0d64025c04d23b6d5e1d5142db46ec;rport=52706
Call-ID: 9062bca7eca2afe71b4a225048ed5101@127.0.0.1
CSeq: 1 INVITE
Contact: <sip:192.168.1.6:5073;transport=tls>;call-type=squared
From: "pstoiano test"

;tag=872524918
To: <sip:jorobb@rtp.ciscotac.net>
Max-Forwards: 15
Route:
```

```
Record-Route: <sip:proxy-call-id=a82052ef-6fd7-4506-8173-
e73af6655b5d@192.168.1.6:7003;transport=tls;lr>
Record-Route: <sip:proxy-call-id=a82052ef-6fd7-4506-8173-
e73af6655b5d@192.168.1.6:5061;transport=tls;lr>
```

O item mais importante é que o **cabeçalho da rota (FQDN do cluster)** ainda está intacto. No

entanto, não há lógica de pesquisa realizada com base no cabeçalho da rota (FQDN do cluster) **cucm.rtp.ciscotac.net**. Em vez disso, você verá a mensagem sendo rejeitada imediatamente com um erro **404 Não encontrado**.

```
2017-09-19T14:16:15.836-04:00 rtp12-tpdmz-118-VCSC tvcs: Event="Call Attempted" Service="SIP"
Src-ip="192.168.1.6" Src-port="7003" Src-alias-type="SIP" Src-alias="sip:pstojoano-
test@dmzlab.call.ciscospark.com" Dst-alias-type="SIP" Dst-alias="sip:jorobb@rtp.ciscotac.net"
Call-serial-number="a3e44231-f62a-4e95-a70e-253701a89515" Tag="73c276e2-3917-4a0c-9fc5-
ddde83b49fd0" Protocol="TLS" Auth="NO" Level="1" UTCTime="2017-09-19 18:16:15,832"
2017-09-19T14:16:15.836-04:00 rtp12-tpdmz-118-VCSC tvcs: Event="Search Attempted" Service="SIP"
Src-alias-type="SIP" Src-alias="pstojoano-test@dmzlab.call.ciscospark.com" Dst-alias-type="SIP"
Dst-alias="sip:jorobb@rtp.ciscotac.net" Call-serial-number="a3e44231-f62a-4e95-a70e-
253701a89515" Tag="73c276e2-3917-4a0c-9fc5-ddde83b49fd0" Detail="searchtype:INVITE" Level="1"
UTCTime="2017-09-19 18:16:15,834"
2017-09-19T14:16:15.836-04:00 rtp12-tpdmz-118-VCSC tvcs: Event="Search Completed" Reason="Not
Found" Service="SIP" Src-alias-type="SIP" Src-alias="pstojoano-test@dmzlab.call.ciscospark.com"
Dst-alias-type="SIP" Dst-alias="sip:jorobb@rtp.ciscotac.net" Call-serial-number="a3e44231-f62a-
4e95-a70e-253701a89515" Tag="73c276e2-3917-4a0c-9fc5-ddde83b49fd0" Detail="found:false,
searchtype:INVITE, Info:Policy Response" Level="1" UTCTime="2017-09-19 18:16:15,835"
2017-09-19T14:16:15.836-04:00 rtp12-tpdmz-118-VCSC tvcs: Event="Call Rejected" Service="SIP"
Src-ip="192.168.1.6" Src-port="7003" Src-alias-type="SIP" Src-alias="sip:pstojoano-
test@dmzlab.call.ciscospark.com" Dst-alias-type="SIP" Dst-alias="sip:jorobb@rtp.ciscotac.net"
Call-serial-number="a3e44231-f62a-4e95-a70e-253701a89515" Tag="73c276e2-3917-4a0c-9fc5-
ddde83b49fd0" Detail="Not Found" Protocol="TLS" Response-code="404" Level="1" UTCTime="2017-09-
19 18:16:15,835"
2017-09-19T14:16:15.836-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-19 18:16:15,830"
Module="network.sip" Level="INFO": Action="Received" Local-ip="192.168.1.5" Local-port="26847"
Src-ip="192.168.1.6" Src-port="7003" Detail="Receive Request Method=INVITE, CSeq=1, Request-
URI=sip:jorobb@rtp.ciscotac.net, Call-ID=9062bca7eca2afe71b4a225048ed5101@127.0.0.1, From-
Tag=872524918, To-Tag=, Msg-Hash=11449260850208794722, Local-
SessionID=daf7c278732bb5a557fb57925dffcbf7, Remote-SessionID=00000000000000000000000000000000"
2017-09-19T14:16:15.836-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-19 18:16:15,836"
Module="network.sip" Level="INFO": Action="Sent" Local-ip="192.168.1.5" Local-port="26847" Dst-
ip="192.168.1.6" Dst-port="7003" Detail="Sending Response Code=404, Method=INVITE, CSeq=1,
To=sip:jorobb@rtp.ciscotac.net, Call-ID=9062bca7eca2afe71b4a225048ed5101@127.0.0.1, From-
Tag=872524918, To-Tag=96b9a0eaf669a590, Msg-Hash=254718822158415175, Local-
SessionID=00000000000000000000000000000000, Remote-SessionID=daf7c278732bb5a557fb57925dffcbf7"

2017-09-19T14:16:15.836-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-19 18:16:15,836"
Module="network.sip" Level="DEBUG": Action="Sent" Local-ip="192.168.1.5" Local-port="26847" Dst-
ip="192.168.1.6" Dst-port="7003" Msg-Hash="254718822158415175"
SIPMSG:
|SIP/2.0 404 Not Found
Via: SIP/2.0/TLS 192.168.1.6:7003;egress-
zone=HybridCallServiceTraversal;branch=z9hG4bKc81c6c4dddef7ed6be5bdce9868fb019913;proxy-call-
id=a82052ef-6fd7-4506-8173-e73af6655b5d;received=192.168.1.6;rport=7003;ingress-
zone=HybridCallServiceTraversal
Via: SIP/2.0/TLS 192.168.1.6:5073;branch=z9hG4bK0eba6d700dfdf761a8ad97fff3c240124;x-cisco-
local-service=nettle;received=192.168.1.6;rport=43119;ingress-zone=DefaultZone
Via: SIP/2.0/TLS 64.102.241.236:5061;egress-
zone=DefaultZone;branch=z9hG4bK6fe399bae58fb0d70c9d69b8e37e13e5912.4248943487bff4af6f649b586c769
6bb;proxy-call-id=f2d15853-c81f-462f-b3e5-c08124f344a3;received=172.16.2.2;rport=25016
Via: SIP/2.0/TLS
192.168.5.66:5062;branch=z9hG4bK0f455ca79cf1b0af5637333aa5286436;received=146.20.193.45;rport=35
464;ingress-zone=HybridCallServicesDNS
Via: SIP/2.0/TLS 127.0.0.1:5070;branch=z9hG4bK-383039-
8f0d64025c04d23b6d5e1d5142db46ec;rport=52706
Call-ID: 9062bca7eca2afe71b4a225048ed5101@127.0.0.1
CSeq: 1 INVITE
From: "pstojoano test"
```

;tag=872524918
To: <sip:jorobb@rtp.ciscotac.net>;tag=96b9a0eaf669a590
Server: TANDBERG/4135 (X8.10.2)
Warning: 399 192.168.1.5:5061 "Policy Response"
Session-ID: 00000000000000000000000000000000;remote=daf7c278732bb5a557fb57925dffcbf7
Content-Length: 0

Em comparação com o cenário em funcionamento, você verá que nesse cenário que a lógica de pesquisa está sendo realizada com base no cabeçalho da rota (FQDN do cluster)

```
2017-09-22T13:56:02.215-04:00 rtp12-tpdmz-118-VCSC tvcs: Event="Search Attempted" Service="SIP"
Src-alias-type="SIP" Src-alias="pstojano-test@dmzlab.call.ciscospark.com" Dst-alias-type="SIP"
Dst-alias="sip:jorobb@rtp.ciscotac.net" Call-serial-number="17aa8dc7-422c-42ef-bdd9-
b9750fbd0edf" Tag="8bd936da-f2ab-4412-96df-d64558f7597b" Detail="searchtype:INVITE" Level="1"
UTCTime="2017-09-22 17:56:02,215"
2017-09-22T13:56:02.218-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-22 17:56:02,217"
Module="network.cpl" Level="DEBUG": Remote-ip="192.168.1.6" Remote-port="7003" Detail="CPL:
<routed> "
2017-09-22T13:56:02.218-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-22 17:56:02,218"
Module="network.cpl" Level="DEBUG": Remote-ip="192.168.1.6" Remote-port="7003" Detail="CPL:
<location clear="yes" url="sip:cucm.rtp.ciscotac.net;lr" diversion="" dest-url-for-
message="sip:jorobb@rtp.ciscotac.net" sip-route-set="" dest-service=""> added
sip:cucm.rtp.ciscotac.net;lr to location set "
2017-09-22T13:56:02.218-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-22 17:56:02,218"
Module="network.cpl" Level="DEBUG": Remote-ip="192.168.1.6" Remote-port="7003" Detail="CPL:
<proxy stop-on-busy="no" timeout="0"/> "
2017-09-22T13:56:02.218-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-22 17:56:02,218"
Module="network.search" Level="DEBUG": Detail="Search rule 'Inbound MS to CMS' did not match
destination alias 'cucm.rtp.ciscotac.net;lr'"
2017-09-22T13:56:02.218-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-22 17:56:02,218"
Module="network.search" Level="DEBUG": Detail="Search rule 'multiway' did not match destination
alias 'cucm.rtp.ciscotac.net;lr'"
2017-09-22T13:56:02.218-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-22 17:56:02,218"
Module="network.search" Level="DEBUG": Detail="Search rule 'WebEx Search Rule' did not match
destination alias 'cucm.rtp.ciscotac.net;lr'"
2017-09-22T13:56:02.218-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-22 17:56:02,218"
Module="network.search" Level="DEBUG": Detail="Search rule 'ISDN Inbound' ignored due to source
filtering"
2017-09-22T13:56:02.218-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-22 17:56:02,218"
Module="network.search" Level="DEBUG": Detail="Search rule 'recalls into CMS' did not match
destination alias 'cucm.rtp.ciscotac.net;lr'"
2017-09-22T13:56:02.218-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-22 17:56:02,218"
Module="network.search" Level="DEBUG": Detail="Search rule 'CEtcp-rtp12-tpdmz-118-ucmpub' did
not match destination alias 'cucm.rtp.ciscotac.net;lr'"
2017-09-22T13:56:02.218-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-22 17:56:02,218"
Module="network.search" Level="DEBUG": Detail="Search rule 'Conference Factory' did not match
destination alias 'cucm.rtp.ciscotac.net;lr'"
2017-09-22T13:56:02.218-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-22 17:56:02,219"
Module="network.search" Level="DEBUG": Detail="Search rule 'Inbound B2B Calling' did not match
destination alias 'cucm.rtp.ciscotac.net;lr'"
2017-09-22T13:56:02.218-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-22 17:56:02,219"
Module="network.search" Level="DEBUG": Detail="Search rule 'Calls to Cisco Webex' did not match
destination alias 'cucm.rtp.ciscotac.net;lr'"
2017-09-22T13:56:02.218-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-22 17:56:02,219"
Module="network.search" Level="DEBUG": Detail="Considering search rule 'as is local' towards
target 'LocalZone' at priority '1' with alias 'cucm.rtp.ciscotac.net;lr'"
2017-09-22T13:56:02.219-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-22 17:56:02,219"
```

Module="network.search" Level="DEBUG": Detail="Considering search rule 'Hybrid Call Service Inbound Routing' towards target 'CUCM11' at priority '2' with alias 'cucm.rtp.ciscotac.net;lr'"

Você então verá que o Expressway-C encaminha corretamente a chamada para o Unified CM (192.168.1.21).

2017-09-22T13:56:02.232-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-22 17:56:02,232"
Module="network.sip" Level="DEBUG": Action="Sent" Local-ip="192.168.1.5" Local-port="25606" Dst-ip="192.168.1.21" Dst-port="5065" Msg-Hash="866788495063340574"

SIPMSG:

| INVITE sip:jorobb@rtp.ciscotac.net SIP/2.0

Via: SIP/2.0/TCP 192.168.1.5:5060;egress-zone=CUCM11;branch=z9hG4bK251d6daf044e635607cc13d244b9ea45138220.69ccb8de20a0e853c1313782077f77b5;proxy-call-id=17aa8dc7-422c-42ef-bdd9-b9750fbd0edf;rport

Via: SIP/2.0/TLS 192.168.1.6:7003;egress-zone=HybridCallServiceTraversal;branch=z9hG4bKba323da436b2bc288200d56d11f02d4d272;proxy-call-id=32c76cef-e73c-4911-98d0-e2d2bb6fec77;received=192.168.1.6;rport=7003;ingress-zone=HybridCallServiceTraversal

Via: SIP/2.0/TLS 192.168.1.6:5073;branch=z9hG4bK06cde3f662d53a210b5b4b11b85500c19;x-cisco-local-service=nettle;received=192.168.1.6;rport=42533;ingress-zone=DefaultZone

Via: SIP/2.0/TLS 64.102.241.236:5061;egress-zone=DefaultZone;branch=z9hG4bK297799f31d0785ff7449e1d7dbe3595b271.2ed90cbcd5b79c6cffad9ecd84cc8337;proxy-call-id=3be87d96-d2e6-4489-b936-8f9cb5ccaa5f;received=172.16.2.2;rport=25005

Via: SIP/2.0/TLS 192.168.4.146:5062;branch=z9hG4bK043ca6360f253c6abed9b23fbef9819;received=148.62.40.64;rport=36149;ingress-zone=HybridCallServicesDNS

Via: SIP/2.0/TLS 127.0.0.1:5070;branch=z9hG4bK-353038-8c648a16c2c5d7b85fa5c759d59aa190;rport=47732

Call-ID: daa1a6fa546ce76591fc464f0a50ee32@127.0.0.1

CSeq: 1 INVITE

Contact: <sip:192.168.1.6:5073;transport=tls>;call-type=squared

From: "pstoiano test" <sip:pstoiano-test@dmzlab.call.ciscospark.com>;tag=567490631

To: <sip:jorobb@rtp.ciscotac.net>

Max-Forwards: 14

Route:

Record-Route: <sip:proxy-call-id=17aa8dc7-422c-42ef-bdd9-b9750fbd0edf@192.168.1.5:5060;transport=tcp;lr>

Record-Route: <sip:proxy-call-id=17aa8dc7-422c-42ef-bdd9-b9750fbd0edf@192.168.1.5:5061;transport=tls;lr>

Record-Route: <sip:proxy-call-id=32c76cef-e73c-4911-98d0-e2d2bb6fec77@192.168.1.6:7003;transport=tls;lr>

Record-Route: <sip:proxy-call-id=32c76cef-e73c-4911-98d0-e2d2bb6fec77@192.168.1.6:5061;transport=tls;lr>

Allow: INVITE,ACK,BYE,CANCEL,INFO,OPTIONS,REFER,SUBSCRIBE,NOTIFY

User-Agent: TANDBERG/4352 (X8.10.2-b2bua-1.0)

Com a análise do log de diagnóstico que isolou o problema no Expressway-C e um erro específico (404 não encontrado), você pode se concentrar no que causaria esse tipo de comportamento. Algumas coisas a considerar são as seguintes:

1. As chamadas entram e saem de zonas no Expressway com base nas regras de pesquisa.
2. Os Expressways usam a lógica chamada suporte a rotas SIP pré-carregadas que processa solicitações de CONVITE SIP que contêm cabeçalho de roteador. Esse valor pode ser ativado ou desativado nas zonas (servidor de passagem, cliente de passagem, vizinho) no Expressway-C e no Expressway-E.

Você agora pode usar o xConfiguration para visualizar a configuração no servidor de passagem

Expressway-E e nas zonas de cliente do Expressway-C, especificamente as que são configuradas no Hybrid Call Service Connect. Além da configuração de zona, é possível analisar as regras de pesquisa configuradas para passar essa chamada de uma zona para outra. Você também sabe que o Expressway-E passou a chamada para o Expressway-C então a configuração da zona de servidor de passagem lá provavelmente está configurada corretamente.

Para detalhar isso, o xConfig informa o nome da zona como **Hybrid Call Service Traversal**. É do tipo de zona **TraversalServer**. Ele se comunica com o Expressway-C pela porta TCP SIP **7003**.

A parte mais importante do Hybrid Call Service é que ele precisa ter o suporte a rotas SIP pré-carregadas ativado. A interface Web do Expressway chama esse valor **Suporte a rotas SIP pré-carregadas enquanto a xConfiguration será exibida como SIP PreloadedSipRoutes Accept**

Expressway-E

```
*c xConfiguration Zones Zone 7 Name: "Hybrid Call Service Traversal"
*c xConfiguration Zones Zone 7 TraversalServer Authentication Mode: "DoNotCheckCredentials"
*c xConfiguration Zones Zone 7 TraversalServer Authentication UserName: "hybridauth"
*c xConfiguration Zones Zone 7 TraversalServer Collaboration Edge: "Off"
*c xConfiguration Zones Zone 7 TraversalServer H323 H46019 Demultiplexing Mode: "Off"
*c xConfiguration Zones Zone 7 TraversalServer H323 Port: "6007"
*c xConfiguration Zones Zone 7 TraversalServer H323 Protocol: "Assent"
*c xConfiguration Zones Zone 7 TraversalServer Registrations: "Allow"
*c xConfiguration Zones Zone 7 TraversalServer SIP Media AesGcm Support: "Off"
*c xConfiguration Zones Zone 7 TraversalServer SIP Media Encryption Mode: "Auto"
*c xConfiguration Zones Zone 7 TraversalServer SIP Media ICE Support: "Off"
*c xConfiguration Zones Zone 7 TraversalServer SIP Multistream Mode: "On"
*c xConfiguration Zones Zone 7 TraversalServer SIP ParameterPreservation Mode: "On"
*c xConfiguration Zones Zone 7 TraversalServer SIP Poison Mode: "Off"
*c xConfiguration Zones Zone 7 TraversalServer SIP Port: "7003"
*c xConfiguration Zones Zone 7 TraversalServer SIP PreloadedSipRoutes Accept: "On"
*c xConfiguration Zones Zone 7 TraversalServer SIP Protocol: "Assent"
*c xConfiguration Zones Zone 7 TraversalServer SIP TLS Verify Mode: "On"
*c xConfiguration Zones Zone 7 TraversalServer SIP TLS Verify Subject Name: "rtp12-tpdmz-118-
VCSC.rtp.ciscotac.net"
*c xConfiguration Zones Zone 7 TraversalServer SIP Transport: "TLS"
*c xConfiguration Zones Zone 7 TraversalServer TCPProbe KeepAliveInterval: "20"
*c xConfiguration Zones Zone 7 TraversalServer TCPProbe RetryCount: "5"
*c xConfiguration Zones Zone 7 TraversalServer TCPProbe RetryInterval: "2"
*c xConfiguration Zones Zone 7 TraversalServer UDPProbe KeepAliveInterval: "20"
*c xConfiguration Zones Zone 7 TraversalServer UDPProbe RetryCount: "5"
*c xConfiguration Zones Zone 7 TraversalServer UDPProbe RetryInterval: "2"
*c xConfiguration Zones Zone 7 Type: "TraversalServer"
```

Você também pode determinar que essa zona tem a regra de pesquisa 3 (Webex Hybrid) vinculada. Essencialmente a regra de pesquisa está enviando um alias "Any" que passa pela zona DNS do Hybrid Call Services e passando-a pela zona acima, Hybrid Call Service Traversal. Conforme esperado, tanto a regra de pesquisa quanto a zona do servidor de passagem no Expressway-E estão configuradas corretamente.

```
*c xConfiguration Zones Policy SearchRules Rule 3 Authentication: "No"
*c xConfiguration Zones Policy SearchRules Rule 3 Description: "Calls to VCS-C"
*c xConfiguration Zones Policy SearchRules Rule 3 Mode: "AnyAlias"
*c xConfiguration Zones Policy SearchRules Rule 3 Name: "Webex Hybrid"
*c xConfiguration Zones Policy SearchRules Rule 3 Pattern Behavior: "Strip"
*c xConfiguration Zones Policy SearchRules Rule 3 Pattern Replace:
*c xConfiguration Zones Policy SearchRules Rule 3 Pattern String:
*c xConfiguration Zones Policy SearchRules Rule 3 Pattern Type: "Prefix"
*c xConfiguration Zones Policy SearchRules Rule 3 Priority: "15"
```

```
*c xConfiguration Zones Policy SearchRules Rule 3 Progress: "Stop"
*c xConfiguration Zones Policy SearchRules Rule 3 Protocol: "SIP"
*c xConfiguration Zones Policy SearchRules Rule 3 SIPTrafficType: "Any"
*c xConfiguration Zones Policy SearchRules Rule 3 Source Mode: "Named"
*c xConfiguration Zones Policy SearchRules Rule 3 Source Name: "Hybrid Call Services DNS"
*c xConfiguration Zones Policy SearchRules Rule 3 State: "Enabled"
*c xConfiguration Zones Policy SearchRules Rule 3 SystemGenerated: "No"
*c xConfiguration Zones Policy SearchRules Rule 3 Target Name: "Hybrid Call Service Traversal"
*c xConfiguration Zones Policy SearchRules Rule 3 Target SIPVariant: "Any"
*c xConfiguration Zones Policy SearchRules Rule 3 Target Type: "Zone"
```

Se você se concentrar na xConfiguration do Expressway-C, é possível começar procurando pela zona de passagem de cliente do Webex Hybrid. Uma maneira fácil de encontrar isso é pesquisar no número da porta que obteve na xConfiguration Expressway-E (Porta SIP: "7003"). Isso o ajudará a identificar rapidamente a zona correta na xConfiguration.

Como anteriormente, é possível obter o nome da zona (Hybrid Call Service Traversal), o tipo (cliente de passagem) e o que foi configurado em SIP PreloadedSipRoutes Accept (suporte a rotas SIP pré-carregadas). Como é possível ver nesta xConfiguration, o valor está definido como Desligado. De acordo com o Guia de Implantação do Cisco Webex Hybrid Call Services, o valor deverá ser definido como Ligado.

Além disso, se verificarmos a definição do suporte de rotas SIP pré-carregados, veremos claramente que o Expressway-C REJEITARÁ a mensagem caso o valor esteja definido como Desligado E o CONVITE contenha um cabeçalho de rota: **"Desative o suporte de rotas SIP pré-carregada se desejar que a zona rejeite as solicitações de CONVITE SIP que contém esse cabeçalho."**

Expressway-C

```
*c xConfiguration Zones Zone 6 Name: "Hybrid Call Service Traversal"
*c xConfiguration Zones Zone 6 TraversalClient Accept Delegated Credential Checks: "Off"
*c xConfiguration Zones Zone 6 TraversalClient Authentication Mode: "DoNotCheckCredentials"
*c xConfiguration Zones Zone 6 TraversalClient Authentication Password:
"{cipher}qeh8eq+fuVY1GHGgRLder/1lYDd76O/6KrHGA7g8bJs="
*c xConfiguration Zones Zone 6 TraversalClient Authentication UserName: "hybridauth"
*c xConfiguration Zones Zone 6 TraversalClient Collaboration Edge: "Off"
*c xConfiguration Zones Zone 6 TraversalClient H323 Port: "1719"
*c xConfiguration Zones Zone 6 TraversalClient H323 Protocol: "Assent"
*c xConfiguration Zones Zone 6 TraversalClient Peer 1 Address: "amer-expressway01.ciscotac.net"
*c xConfiguration Zones Zone 6 TraversalClient Peer 2 Address:
*c xConfiguration Zones Zone 6 TraversalClient Peer 3 Address:
*c xConfiguration Zones Zone 6 TraversalClient Peer 4 Address:
*c xConfiguration Zones Zone 6 TraversalClient Peer 5 Address:
*c xConfiguration Zones Zone 6 TraversalClient Peer 6 Address:
*c xConfiguration Zones Zone 6 TraversalClient Registrations: "Allow"
*c xConfiguration Zones Zone 6 TraversalClient RetryInterval: "120"
*c xConfiguration Zones Zone 6 TraversalClient SIP Media AesGcm Support: "Off"
*c xConfiguration Zones Zone 6 TraversalClient SIP Media Encryption Mode: "Auto"
*c xConfiguration Zones Zone 6 TraversalClient SIP Media ICE Support: "Off"
*c xConfiguration Zones Zone 6 TraversalClient SIP Multistream Mode: "On"
*c xConfiguration Zones Zone 6 TraversalClient SIP ParameterPreservation Mode: "On"
*c xConfiguration Zones Zone 6 TraversalClient SIP Poison Mode: "Off"
*c xConfiguration Zones Zone 6 TraversalClient SIP Port: "7003"
*c xConfiguration Zones Zone 6 TraversalClient SIP PreloadedSipRoutes Accept: "Off"
*c xConfiguration Zones Zone 6 TraversalClient SIP Protocol: "Assent"
*c xConfiguration Zones Zone 6 TraversalClient SIP TLS Verify Mode: "On"
*c xConfiguration Zones Zone 6 TraversalClient SIP TURN Server Address:
*c xConfiguration Zones Zone 6 TraversalClient SIP TURN Server Port:
*c xConfiguration Zones Zone 6 TraversalClient SIP Transport: "TLS"
*c xConfiguration Zones Zone 6 Type: "TraversalClient"
```

Nesse ponto você terá isolado o problema para uma configuração incorreta da configuração de zona cliente de passagem do Expressway-C. Você precisa ativar o suporte a rotas SIP pré-carregado.

Solução

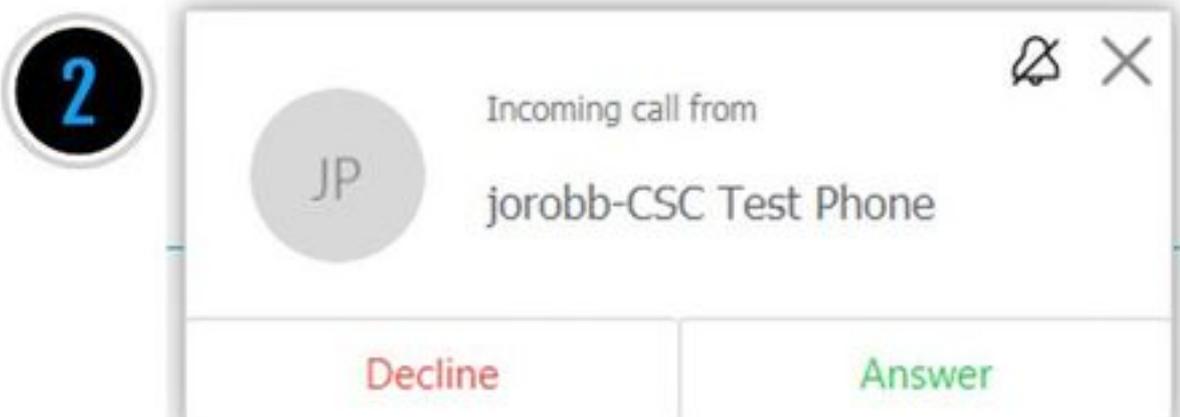
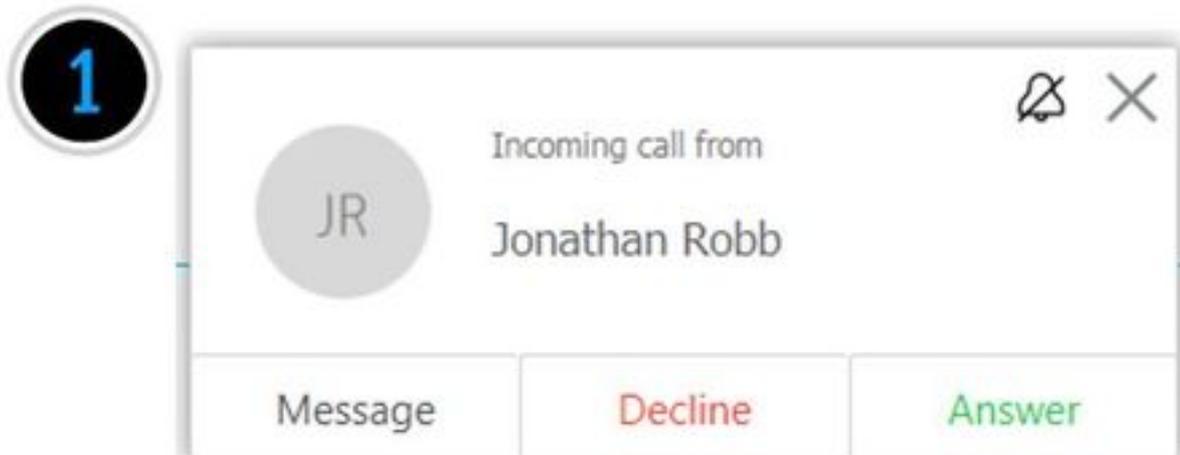
Para definir corretamente o suporte a rotas SIP pré-carregadas:

1. Faça login no Expressway-C
2. Navegue até **Configuração > Zonas > Zonas**
3. Selecione a zona de passagem do Hybrid Call Service (o nome vai variar de cliente para cliente)
4. Ajuste o **Suporte a rotas SIP pré-carregadas** como **Ligado**
5. Selecione **Salvar**

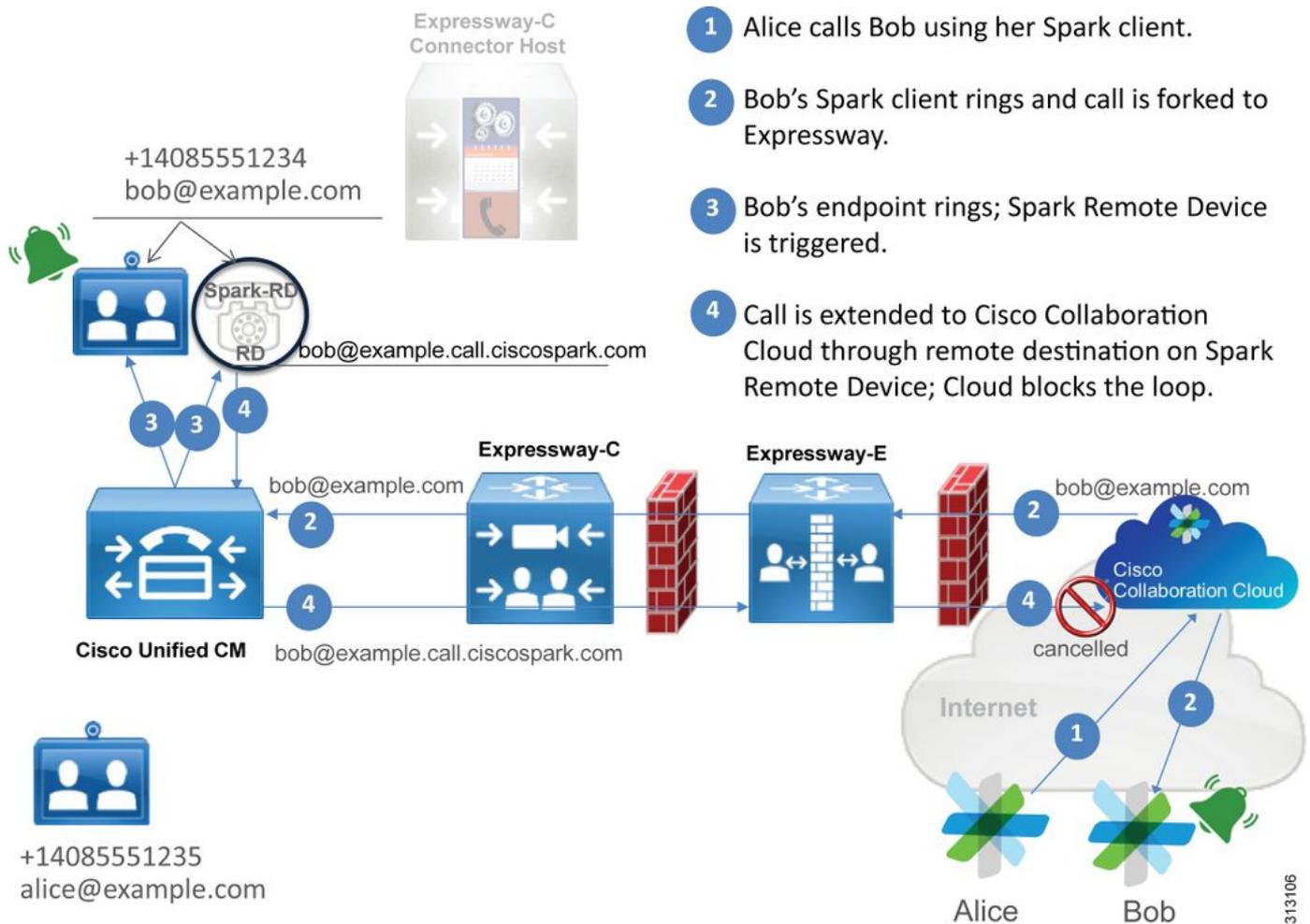
Note: Ainda que esse cenário tenha demonstrado a falha no Expressway-C, os mesmos erros de log de diagnóstico podem ser observados no Expressway-E caso o **Suporte a rotas SIP pré-carregadas estivesse desligado na zona de servidor de passagem do Webex Hybrid Call**. Nesse caso, você não veria a chamada chegar ao Expressway-C e o Expressway-E teria sido responsável por rejeitar a chamada e enviar o erro de 404 não encontrado.

Problema 5. O aplicativo Cisco Webex está recebendo duas notificações de chamada (brindes)

Esse problema específico é o único cenário de chamada de entrada que não resulta na queda da chamada. Nesse caso, a pessoa que recebe a chamada (destinatário da chamada) está recebendo duas notificações no aplicativo do Cisco Webex da pessoa que fez a chamada (chamador). A primeira notificação é gerada pelo Cisco Webex e a segunda notificação vem da infraestrutura no local. A seguir encontram-se exemplos das duas notificações que são recebidas como mostrado na imagem.



A primeira notificação vem da pessoa que iniciou a chamada (chamador) no lado do Cisco Webex. A ID de chamada nessa instância é o nome de exibição do usuário que inicia a chamada. A segunda notificação vem do RD Cisco Webex ou do CTI no local que está atribuído ao usuário chamador. A princípio, esse comportamento parece peculiar. No entanto, se você analisar o diagrama de chamada de entrada (do Guia de design do Cisco Webex Hybrid Call), o comportamento faz mais sentido como mostrado na imagem.



Na ilustração, você pode ver que Alice está ligando para Bob pelo aplicativo Cisco Webex e a chamada está sendo distribuída para o local. Esta chamada deve corresponder à URI de diretório atribuída ao telefone de Bob. O problema é que, com esse design, a URI do diretório também é atribuída ao CTI-RD ou RD do Cisco Webex dele. Portanto, quando a chamada é enviada para o CTI-RD ou RD Cisco Webex, a chamada é enviada de volta para o Cisco Webex porque o dispositivo tem um Destino remoto configurado como bob@example.call.ciscospark.com. A forma como o Cisco Webex lida com essa situação é que ele cancela esse segmento de camada específico.

Para que o Cisco Webex cancele corretamente o segmento de chamada, o Cisco Webex inicialmente precisava colocar um parâmetro no cabeçalho SIP que seria buscado para cancelar o segmento de chamada específico. O parâmetro que o Cisco Webex insere no CONVITE SIP é chamado **"call-type=squared"** e esse valor é inserido no cabeçalho do contato. Se esse valor for retirado da mensagem, o Cisco Webex não entende como cancelar a chamada.

Com essas informações, é possível revisitar o cenário apresentado anteriormente, no qual o aplicativo do Cisco Webex do usuário estava recebendo duas notificações quando o usuário do Cisco Webex Jonathan Robb estava fazendo uma chamada. Para solucionar esse tipo de problema, você sempre precisará coletar logs de diagnóstico do Expressway-C e do Expressway-E. Como ponto de partida, você pode revisar os logs do Expressway-E para determinar que o CONVITE SIP na verdade tem o valor **call-type=squared presente no cabeçalho de contato do CONVITE inicial do Cisco Webex enviado**. Isso vai garantir que o firewall não esteja manipulando a mensagem de nenhuma forma. A seguir está um exemplo de trecho do CONVITE que chega ao Expressway-E neste cenário.

```
2017-09-19T14:01:48.140-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 18:01:48,140"
Module="network.sip" Level="DEBUG": Action="Received" Local-ip="172.16.2.2" Local-port="5062"
Src-ip="146.20.193.73" Src-port="40342" Msg-Hash="11658696457333185909"
SIPMSG:
|INVITE sip:pstojano-test@rtp.ciscotac.net SIP/2.0
Via: SIP/2.0/TLS 192.168.5.164:5062;branch=z9hG4bK564cd36d87f3417513c9b559dc666f71,SIP/2.0/TLS
127.0.0.1:5070;branch=z9hG4bK-3237-5c5060d07ecc546a0bb861ef52a5f507;rport=43306
Call-ID: 6bc0ca8210c0b48df69f38057ec1e48b@127.0.0.1
CSeq: 1 INVITE
Contact: "l2sip-UA" <sip:l2sip-UA@l2sip-cfa-01.wbx2.com:5062;transport=tls>;call-type=squared
<-- Webex inserted value
From: "Jonathan Robb"
```

```
;tag=540300020
```

To:

O cabeçalho do contato tem o calor **call-type=squared** . Nesse momento, a chamada deve passar pelo Expressway e ser enviada para a zona de servidor de passagem do Webex Hybrid. Podemos pesquisar nos logs do Expressway-E para determinar como a chamada foi enviada para o Expressway-E. Isso nos dará uma ideia de se o Expressway-E está manipulando o CONVITE de qualquer forma.

```
2017-09-19T14:01:48.468-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 18:01:48,468"
Module="network.sip" Level="DEBUG": Action="Sent" Local-ip="192.168.1.6" Local-port="7003" Dst-
ip="192.168.1.5" Dst-port="26686" Msg-Hash="1847271284712495612"
SIPMSG:
INVITE sip:pstojano-test@rtp.ciscotac.net SIP/2.0
Via: SIP/2.0/TLS 192.168.1.6:7003;egress-
zone=HybridCallServiceTraversal;branch=z9hG4bKec916b02b6d469abad0a30b93753f4b0859;proxy-call-
id=d7372034-85d1-41f8-af84-dffed6d1a9a9;rport
Via: SIP/2.0/TLS 192.168.1.6:5073;branch=z9hG4bKd91699370129b4c10d09e269525de00c2;x-cisco-local-
service=nettle;received=192.168.1.6;rport=43119;ingress-zone=DefaultZone
Via: SIP/2.0/TLS 64.102.241.236:5061;egress-
zone=DefaultZone;branch=z9hG4bK52aac9a181192566e01b98ae0280bdf858.0e65cdf078cabb269eecb6bce132
8be;proxy-call-id=ec51e8da-e1a3-4210-95c9-494d12debc8;received=172.16.2.2;rport=25016
Via: SIP/2.0/TLS
192.168.5.164:5062;branch=z9hG4bK564cd36d87f3417513c9b559dc666f71;received=146.20.193.73;rport=4
0342;ingress-zone=HybridCallServicesDNS
Via: SIP/2.0/TLS 127.0.0.1:5070;branch=z9hG4bK-3237-5c5060d07ecc546a0bb861ef52a5f507;rport=43306
Call-ID: 6bc0ca8210c0b48df69f38057ec1e48b@127.0.0.1
CSeq: 1 INVITE
Contact: <sip:192.168.1.6:5073;transport=tls> <-- Webex inserted value is now missing
From: "Jonathan Robb"
```

```
;tag=540300020
```

To:

Max-Forwards: 15

Route: <sip:cucm.rtp.ciscotac.net;lr>

Ao revisar o CONVITE SIP que está sendo enviado do Expressway-E para o Expressway-C, observe que o cabeçalho de contato não tem o valor **call-type=squared**. Uma outra coisa a apontar é que, no item de linha 4, você pode ver que a zona de saída é igual a **HybridCallServiceTraversal**. Agora você pode concluir que a razão pela qual o aplicativo Cisco Webex está recebendo uma segunda notificação quando chamado é porque o Expressway-E está retirando a tag **call-type=squared** do cabeçalho de contato do CONVITE SIP. A pergunta a responder é o que poderia estar causando essa retirada do cabeçalho.

A chamada deve passar pelo servidor de passagem do Hybrid Call Service Traversal configurado no Expressway para que seja um bom lugar para iniciar a investigação. Caso tenha o xConfiguration, será possível ver como essa zona foi configurada. Para identificar a zona no xConfiguration, é possível usar o nome registrado na linha Via impressa nos logs. Você pode ver acima que era chamada de egress-zone=HybridCallServiceTraversal. Quando esse nome é impresso na linha Via do cabeçalho SIP, os espaços são removidos. O nome real da zona pela perspectiva do xConfiguration teria espaços e seria formatado no servidor de passagem do Hybrid Call Service.

```
*c xConfiguration Zones Zone 7 TraversalServer Authentication Mode: "DoNotCheckCredentials"
*c xConfiguration Zones Zone 7 TraversalServer Authentication UserName: "hybridauth"
*c xConfiguration Zones Zone 7 TraversalServer Collaboration Edge: "Off"
*c xConfiguration Zones Zone 7 TraversalServer H323 H46019 Demultiplexing Mode: "Off"
*c xConfiguration Zones Zone 7 TraversalServer H323 Port: "6007"
*c xConfiguration Zones Zone 7 TraversalServer H323 Protocol: "Assent"
*c xConfiguration Zones Zone 7 TraversalServer Registrations: "Allow"
*c xConfiguration Zones Zone 7 TraversalServer SIP Media AesGcm Support: "Off"
*c xConfiguration Zones Zone 7 TraversalServer SIP Media Encryption Mode: "Auto"
*c xConfiguration Zones Zone 7 TraversalServer SIP Media ICE Support: "Off"
*c xConfiguration Zones Zone 7 TraversalServer SIP Multistream Mode: "On"
*c xConfiguration Zones Zone 7 TraversalServer SIP ParameterPreservation Mode: "Off" <--
Possible Suspect Value
*c xConfiguration Zones Zone 7 TraversalServer SIP Poison Mode: "Off"
*c xConfiguration Zones Zone 7 TraversalServer SIP Port: "7003"
*c xConfiguration Zones Zone 7 TraversalServer SIP PreloadedSipRoutes Accept: "On" <--
Possible Suspect Value
*c xConfiguration Zones Zone 7 TraversalServer SIP Protocol: "Assent"
*c xConfiguration Zones Zone 7 TraversalServer SIP TLS Verify Mode: "On"
*c xConfiguration Zones Zone 7 TraversalServer SIP TLS Verify Subject Name: "rtp12-tpdmz-118-
VCSC.rtp.ciscotac.net"
*c xConfiguration Zones Zone 7 TraversalServer SIP Transport: "TLS"
*c xConfiguration Zones Zone 7 TraversalServer TCPProbe KeepAliveInterval: "20"
*c xConfiguration Zones Zone 7 TraversalServer TCPProbe RetryCount: "5"
*c xConfiguration Zones Zone 7 TraversalServer TCPProbe RetryInterval: "2"
*c xConfiguration Zones Zone 7 TraversalServer UDPProbe KeepAliveInterval: "20"
*c xConfiguration Zones Zone 7 TraversalServer UDPProbe RetryCount: "5"
*c xConfiguration Zones Zone 7 TraversalServer UDPProbe RetryInterval: "2"
*c xConfiguration Zones Zone 7 Name: "Hybrid Call Service Traversal"
```

Com as configurações identificadas para o servidor de passagem do Hybrid Call Service, você poderá procurar por possíveis configurações que se destaquem, como:

- SIP PreloadedSIPRoutes Accept: Ligado
- SIP ParameterPreservatoin Mode: Off

Usando a interface da Web de qualquer Expressway, é possível ver qual é a definição desses valores e o que eles fazem.

Suporta a rotas SIP pré-carregadas

Ative o suporte a rotas pré-carregadas para permitir que essa zona processe as solicitações de CONVITE SIP que contenham o cabeçalho de rota.

Desative o suporte de rotas SIP pré-carregadas se desejar que a zona rejeite as solicitações de CONVITE SIP que contêm esse cabeçalho.

Preservação de parâmetro SIP

Determina se o B2BUA do Expressway preserva ou reescreve os parâmetros em solicitações SIP roteadas por essa zona.

Ligado preserva a URI de solicitação de SIP e os parâmetros de contato das solicitações que passam entre essa zona e o B2BUA.

Desligado permite que o B2BUA reescreva a URI da solicitação SIP e os parâmetros de contato das solicitações que passam entre essa zona e o B2BUA, se necessário.

Com base nessas definições, a xConfiguration, e o valor **call-type=squared** são colocados no cabeçalho "Contato" do CONVITE SIP, é possível concluir que, a preservação de parâmetro desligada na zona de passagem do Hybrid Call Service é a razão pela qual a tag está sendo retirada e o aplicativo Cisco Webex está recebendo notificações de toque dobradas.

Solução

Para preservar o valor **call-type=squared** no cabeçalho de contato do CONVITE SIP, é preciso garantir que os Expressways suportem a preservação do parâmetro SIP em todas as zonas envolvidas no tratamento da chamada:

1. Faça login no Expressway-E
2. Navegue até **Configuração > Zonas > Zonas**
3. Selecione a zona que está sendo usada para o servidor de passagem Hybrid
4. Defina o valor de preservação de parâmetro SIP como **Ligado**
5. Salve as configurações.

#####

Note: Neste cenário de exemplo, a zona do servidor de passagem do Webex Hybrid estava configurada incorretamente. Tenha em mente que é totalmente possível que o valor de preservação do parâmetro SIP seja definido como desligado no cliente de passagem do Webex Hybrid ou nas zonas vizinhas do CUCM. Ambas configurações seriam feitas no Expressway-C. Se esse fosse o caso, você poderia esperar que o Expressway-E enviasse o valor **call-type=squared** para o Expressway-C e ele teria sido o Expressway-C removendo-o.

Saída: No local para o Cisco Webex

Praticamente todas as falhas de saída do local para o Cisco Webex resultam na indicação do mesmo sintoma: "Quando ligo de meu telefone registrado no Unified CM para outro usuário que está habilitado para Call Service Connect, o telefone no local dele toca, mas o aplicativo Cisco Webex não." Para solucionar esse cenário, é importante entender a lógica e o fluxo de chamadas que acontecem quando esse tipo de chamada é feito.

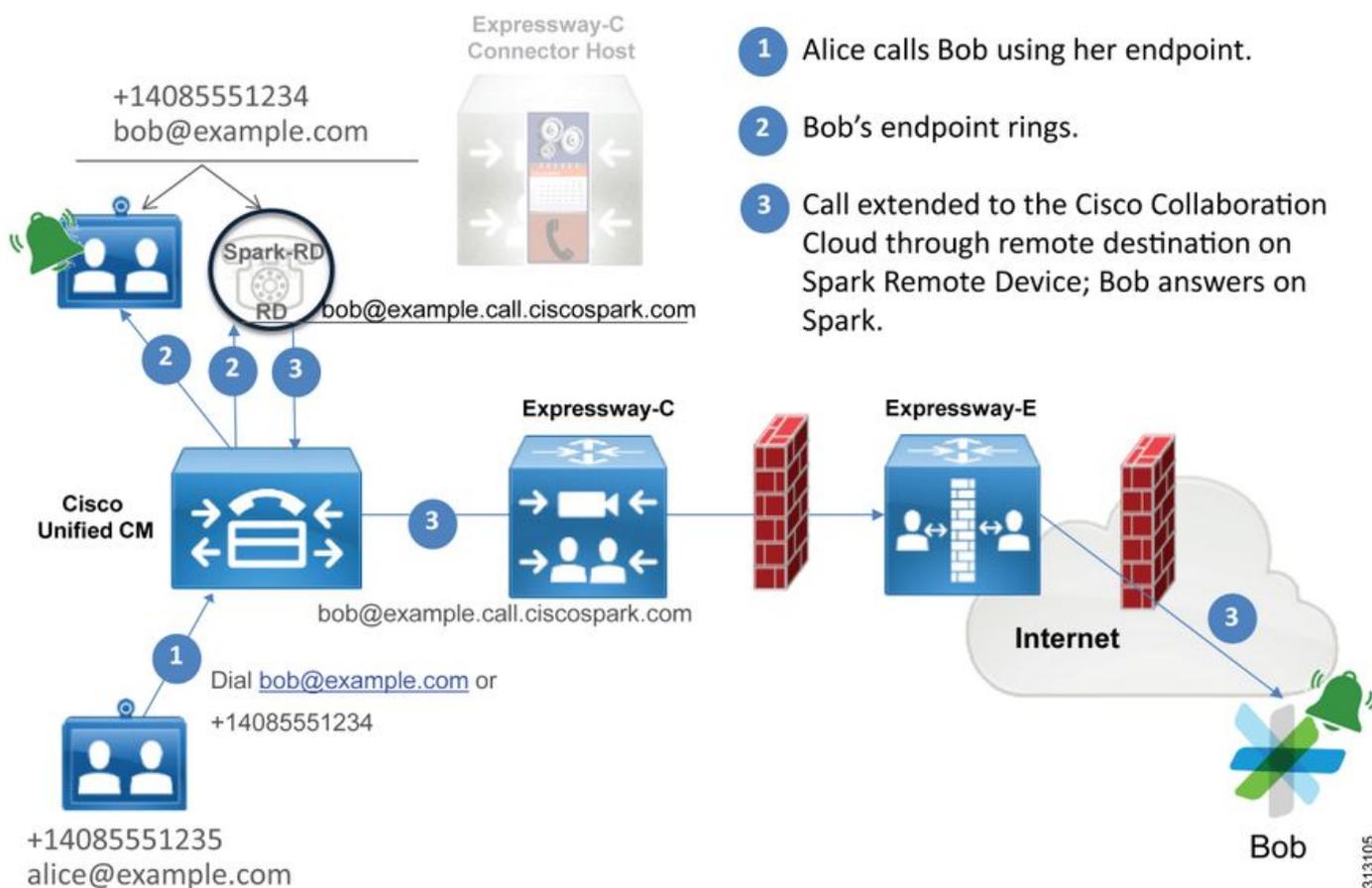
Fluxo de lógica de alto nível

1. O usuário A faz uma chamada do telefone no local para a URI de diretório do usuário B
2. O telefone no local do usuário B e o CTI-RD/Webex-RD aceitam a chamada

3. O telefone no local do usuário B começa a tocar
4. O CTI-RD/Webex-RD do usuário B distribui a chamada para o destino UserB@example.call.ciscospark.com
5. O Unified CM passa a chamada para o Expressway-C
6. O Expressway-C envia a chamada para o Expressway-E
7. O Expressway-E realiza uma busca de DNS no domínio callservice.ciscospark.com
8. O Expressway-E tenta se conectar ao ambiente Cisco Webex pela porta 5062.
9. O Expressway-E e o ambiente Cisco Webex iniciam um handshake mútuo
10. O ambiente do Cisco Webex passa a chamada para o aplicativo Cisco Webex do usuário B disponível
11. O aplicativo Cisco Webex do usuário B disponível começa a tocar.

Fluxo de chamada

Navegue até **Telefone no local do usuário B > Unified CM > CTI-RD/Webex-RD > Expressway-C > Expressway-E > Ambiente Cisco Webex > Aplicativo Cisco Webex** como mostrado na imagem.



Note: A imagem foi retirada do [Guia de design do Cisco Webex Hybrid](#).

Dicas de análise de log

Caso estivesse solucionando problemas em um cenário no qual as chamadas de saída distribuídas para o Cisco Webex estivessem falhando, você deveria coletar os logs do Unified CM, Expressway-C e Expressway-E. Com esses dois conjuntos de logs, é possível ver como a chamada está passando pelo ambiente. Outra maneira rápida de entender qual a distância percorrida pela chamada em seu ambiente local é usar o "Histórico de pesquisa" do Expressway. O histórico de pesquisa do Expressway vai permitir rapidamente que você veja que a chamada

distribuída para o Cisco Webex está chegando ao Expressway-C ou E.

Para usar o histórico de pesquisa, é possível executar as seguintes etapas:

1. Faça login no Expressway-E

Faça uma chamada de teste

Navegue até **Status > Histórico de pesquisa**

Verifique se você vê uma chamada que tem um endereço de destino da URI SIP do Webex que deveria chamar (user@example.call.ciscopark.com)

Se o histórico de pesquisa não mostrar a chamada chegando ao histórico de pesquisa do Expressway-E, repita o processo no Expressway-C

Antes de analisar os logs de diagnóstico no Expressway, considere como identificar esta chamada:

1. A URI da solicitação SIP será o endereço SIP do usuário do Cisco Webex

2. O campo SIP FROM será formatado para que a parte chamadora seja listada como "Nome Sobrenome" <sip:Alias@Domain>

Com essas informações é possível pesquisar os logs de diagnóstico por URI de diretório do chamador, Nome e sobrenome do chamador ou endereço SIP do Cisco Webex do destinatário da chamada. Se você não tiver nenhuma dessas informações, poderá fazer uma pesquisa em "**CONVITE SIP:**", que localizará todas as chamadas SIP executadas no Expressway. Depois de identificar o CONVITE SIP da chamada de saída, é possível localizar e copiar a **ID de chamada** do SIP. Depois que tiver esse valor, você poderá apenas pesquisar nos logs de diagnóstico com base na ID de chamada para ver todas as mensagens correlacionadas a esse segmento de chamada.

Estes são alguns dos problemas mais comuns observados nas chamadas de saída do telefone registrado no Unified CM para o ambiente Cisco Webex quando a chamada é feita para um usuário habilitado para o Call Service Connect.

Problema 1. O Expressway não consegue resolver o endereço callservice.ciscopark.com

O procedimento operacional padrão de uma zona DNS do Expressway é executar buscas de DNS com base no domínio que aparece no lado direito de uma URI de solicitação. Para explicar isso, considere um exemplo. Se a zona DNS fosse receber uma chamada que tinha uma URI de solicitação **pstojano-test@dmzlab.call.ciscopark.com**, uma zona DNS Expressway típica faria a lógica de busca SRV DNS no **dmzlab.call.ciscopark.com** que **está do lado direito da URI de solicitação**. Caso o Expressway fosse fazer isso, seria esperado que a seguinte busca e resposta acontecesse.

```
_sips._tcp.dmzlab.call.ciscopark.com.  
Response: 5 10 5061 12sip-cfa-01.wbx2.com.  
12sip-cfa-01.wbx2.com  
Response: 146.20.193.64
```

Se você observar com atenção, verá que a resposta do registro SRV está fornecendo um endereço de servidor e a porta 5061, não a 5062.

Isso significa que o handshake TLS mútuo que acontece pela porta 5062 não acontecerá e uma porta separada será usada para sinalizar entre o Expressway e o Cisco Webex. O desafio disso é que o *Guia de implantação do Cisco Webex Hybrid Call Services* não indica explicitamente o uso

da porta 5061, já que alguns ambientes não permitem ligações entre empresas.

A forma de superar essa lógica de busca SRV da zona DNS padrão no Expressway é configurar o Expressway para que ele explicitamente as pesquisas com base em um valor fornecido.

Agora ao analisar essa chamada específica, será possível se concentrar no Expressway-E, pois você determinou (usando o histórico de pesquisa) que a chamada chegou até aqui. Comece com o primeiro CONVITE SIP que acompanha o Expressway-E para ver por qual zona ela chegou, quais regras de pesquisa estão sendo usadas, por qual zona a chamada saiu e, se enviada corretamente para a zona DNS, que lógica de busca de DNS acontece.

```
2017-09-19T13:18:50.562-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 17:18:50,556"
Module="network.sip" Level="DEBUG": Action="Received" Local-ip="192.168.1.6" Local-port="7003"
Src-ip="192.168.1.5" Src-port="26686" Msg-Hash="4341754241544006348"
SIPMSG:
|INVITE sip:pstojano-test@dmzlab.call.ciscospark.com SIP/2.0
Via: SIP/2.0/TLS 192.168.1.5:5061;egress-
zone=HybridCallServiceTraversal;branch=z9hG4bK6d734eaf7a6d733bd1e79705b7445ebb46175.1d33be65c99c
56898f85df813f1db3a7;proxy-call-id=47454c92-2b30-414a-b7fe-aff531296bcf;rport
Via: SIP/2.0/TCP 192.168.1.21:5065;branch=z9hG4bK13187594dd412;received=192.168.1.21;ingress-
zone=CUCM11
Call-ID: 991f7e80-9c11517a-130ac-1501a8c0@192.168.1.21
CSeq: 101 INVITE
Call-Info: <urn:x-cisco-remotecall:callinfo>;x-cisco-video-traffic-class=DESKTOP
Remote-Party-ID: "Jonathan Robb"
<sip:5010@rtp.ciscotac.net>;party=calling;screen=yes;privacy=off
Contact: <sip:5010@192.168.1.21:5065;transport=tcp>;video;audio
From: "Jonathan Robb"

;tag=332677~c9cc7ddc-9592-49e8-a13c-79e26f48eebc-30106860
To:

Max-Forwards: 15
Record-Route: <sip:proxy-call-id=47454c92-2b30-414a-b7fe-
aff531296bcf@192.168.1.5:5061;transport=tls;lr>
Record-Route: <sip:proxy-call-id=47454c92-2b30-414a-b7fe-
aff531296bcf@192.168.1.5:5060;transport=tcp;lr>
Allow: INVITE,OPTIONS,INFO,BYE,CANCEL,ACK,PRACK,UPDATE,REFER,SUBSCRIBE,NOTIFY
User-Agent: Cisco-CUCM11.5
Expires: 180
Date: Tue, 19 Sep 2017 17:18:50 GMT
Supported: timer,resource-priority,replaces,X-cisco-srtp-fallback,X-cisco-original-called
Session-Expires: 1800
Min-SE: 1800
Allow-Events: presence
X-TAATag: 2272025a-ce36-49d0-8d93-cb6a5e90ffe0
Session-ID: 75957d4fb66a13e835c10737aa332675;remote=00000000000000000000000000000000
Cisco-Guid: 2568978048-0000065536-000000148-0352430272
Content-Type: application/sdp
Content-Length: 714
```

<SDP Omitted>

Neste CONVITE SIP, você pode reunir a URI de solicitação (pstojoano-test@dmzlab.call.ciscospark.com), a ID de chamada (991f7e80-9c11517a-130ac-1501a8c0), De ("Jonathan Robb" <sip:5010@rtp.ciscotac.net>) To (sip:pstojoano-test@dmzlab.call.ciscospark.com) e User-Agent (Cisco-CUCM11.5). Depois que este CONVITE for recebido, o Expressway agora precisam tomar decisões lógicas para determinar se ele pode rotear a chamada para outra zona. O Expressway fará isso com base nas regras de pesquisa.

```
2017-09-19T13:18:50.564-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 17:18:50,564"
Module="network.search" Level="DEBUG": Detail="Search rule 'B2B calls to VCS-C' did not match
destination alias 'pstojoano-test@dmzlab.call.ciscospark.com'"
2017-09-19T13:18:50.564-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 17:18:50,564"
Module="network.search" Level="DEBUG": Detail="Search rule 'Webex Hybrid' ignored due to source
filtering"
2017-09-19T13:18:50.564-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 17:18:50,564"
Module="network.search" Level="DEBUG": Detail="Search rule 'Calls to Webex' did not match
destination alias 'pstojoano-test@dmzlab.call.ciscospark.com'"
2017-09-19T13:18:50.564-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 17:18:50,564"
Module="network.search" Level="DEBUG": Detail="Considering search rule 'Webex Hybrid - to Webex
Cloud' towards target 'Hybrid Call Services DNS' at priority '90' with alias 'pstojoano-
test@dmzlab.call.ciscospark.com'"
```

Com base no trecho de log acima, será possível ver que o Expressway-E foi analisado por quatro regras de pesquisa, no entanto, apenas um (Webex Hybrid para Webex Cloud) foi considerado. A regra de pesquisa teve uma prioridade de 90 e foi direcionada para a zona DNS dos serviços Hybrid Call. Agora que a chamada está sendo enviada para uma zona DNS, é possível revisar as buscas SRV DNS que acontecem no Expressway-E

```
2017-09-19T13:18:50.565-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 17:18:50,565"
Module="network.dns" Level="DEBUG": Detail="Sending DNS query"
Name="dmzlab.call.ciscospark.com" Type="NAPTR (IPv4 and IPv6)"
2017-09-19T13:18:50.718-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 17:18:50,718"
Module="network.dns" Level="DEBUG": Detail="Sending DNS query"
Name="_sips._tcp.dmzlab.call.ciscospark.com" Type="SRV (IPv4 and IPv6)"
2017-09-19T13:18:50.795-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 17:18:50,795"
Module="network.dns" Level="DEBUG": Detail="Resolved hostname to:
['IPv4' 'TCP' '146.20.193.64:5061'] (A/AAAA) Hostname:'l2sip-cfa-01.wbx2.com' Port:'5061'
Priority:'5' TTL:'300' Weight:'10' (SRV) Number of relevant records retrieved: 2"
```

No trecho acima, é possível ver que o Expressway-E realizou a busca SRV com base no lado direito da URI de solicitação (_sips._tcp.dmzlab.call.ciscospark.com) e foi resolvido para um nome de host de l2sip-cfa-01.wbx2.com e porta 5061. O nome de host l2sip-cfa-01.wbx2.com é resolvido para 146.20.193.64. Com essas informações, a próxima etapa lógica que o Expressway vai cumprir é enviar um pacote SYN TCP para 146.20.193.64 para tentar configurar a chamada. No log do Expressway-E, é possível analisar para ver se isso está acontecendo.

```
2017-09-19T13:18:51.145-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 17:18:51,145"
Module="network.tcp" Level="DEBUG": Src-ip="172.16.2.2" Src-port="25010" Dst-ip="146.20.193.64"
Dst-port="5061" Detail="TCP Connecting"
2017-09-19T13:19:01.295-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 17:19:01,289"
Module="network.tcp" Level="ERROR": Src-ip="172.16.2.2" Src-port="25010" Dst-ip="146.20.193.64"
Dst-port="5061" Detail="TCP Connection Failed"
```

No trecho de log de diagnóstico do Expressway-E acima, você poderá ver que o Expressway-E está tentando se conecta ao IP 146.20.193.64 que foi resolvido anteriormente pela porta TCP 5061, no entanto, essa conexão está claramente falhando. O mesmo pode ser visto na captura de

pacotes coletada.

Expressway-E attempts TCP Connection

| No. | Time | Source | Destination | Protocol | S Port | D Port | Length | Info |
|-------|----------------------------|-------------|---------------|----------|--------|--------|--------|---|
| 3878 | 2017-09-19 17:18:08.801765 | 68.67.59.22 | 172.16.2.2 | TCP | 25876 | 5061 | 66 | 25876->5061 [FIN, ACK] Seq=1 Ack=1 Win=362 Len=0 TSval=231154828 TSecr=4109470239 |
| 3879 | 2017-09-19 17:18:08.801923 | 172.16.2.2 | 68.67.59.22 | TCP | 5061 | 25876 | 66 | 5061->25876 [FIN, ACK] Seq=1 Ack=1 Win=287 Len=0 TSval=4111463862 TSecr=231154828 |
| 3882 | 2017-09-19 17:18:08.822153 | 68.67.59.22 | 172.16.2.2 | TCP | 25876 | 5061 | 66 | 25876->5061 [ACK] Seq=2 Ack=2 Win=362 Len=0 TSval=231154849 TSecr=4111463862 |
| 3109 | 2017-09-19 17:18:51.103310 | 172.16.2.2 | 172.16.2.2 | TCP | 5061 | 5061 | 66 | 5061->5061 [EST, ACK] Seq=0 Ack=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 TSval=314491012 TSecr=0 WS=128 |
| 14878 | 2017-09-19 17:18:51.145472 | 172.16.2.2 | 146.20.193.64 | TCP | 25010 | 5061 | 74 | 25010->5061 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=314491012 TSecr=0 WS=128 |
| 15158 | 2017-09-19 17:18:52.203326 | 172.16.2.2 | 146.20.193.64 | TCP | 25010 | 5061 | 74 | [TCP Retransmission] 25010->5061 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=314 |
| 15702 | 2017-09-19 17:18:54.251324 | 172.16.2.2 | 146.20.193.64 | TCP | 25010 | 5061 | 74 | [TCP Retransmission] 25010->5061 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=314 |
| 16770 | 2017-09-19 17:18:58.283326 | 172.16.2.2 | 146.20.193.64 | TCP | 25010 | 5061 | 74 | [TCP Retransmission] 25010->5061 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=314 |
| 17577 | 2017-09-19 17:19:01.328621 | 172.16.2.2 | 146.20.193.64 | TCP | 25011 | 5061 | 74 | 25011->5061 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=314501195 TSecr=0 WS=128 |
| 17648 | 2017-09-19 17:19:02.819322 | 172.16.2.2 | 146.20.193.64 | TCP | 25011 | 5061 | 74 | [TCP Retransmission] 25011->5061 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=314 |
| 18425 | 2017-09-19 17:19:04.427323 | 172.16.2.2 | 146.20.193.64 | TCP | 25011 | 5061 | 74 | [TCP Retransmission] 25011->5061 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=314 |
| 19459 | 2017-09-19 17:19:08.459332 | 172.16.2.2 | 146.20.193.64 | TCP | 25011 | 5061 | 74 | [TCP Retransmission] 25011->5061 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=314 |

The Expressway-E doesn't receive a SYN-ACK so it retries the SYN packet again 3 times

Com base nesses resultados, fica claro que o tráfego pela porta 5061 não está funcionando. No entanto, o Hybrid Call Service Connect pretendia usar a porta TCP 5062, não a 5061. Portanto, você precisa considerar o motivo pelo qual o Expressway-E não está resolvendo um registro SRV que retornaria a porta 5062. Para tentar responder a essa pergunta, você pode buscar possíveis problemas de configuração na zona DNS Webex Hybrid do Expressway-E.

- *c xConfiguration Zones Zone 6 Name: "Hybrid Call Services DNS"
- *c xConfiguration Zones Zone 6 DNS SIP Authentication Trust Mode: "Off"
- *c xConfiguration Zones Zone 6 DNS SIP Default Transport: "TLS"
- *c xConfiguration Zones Zone 6 DNS SIP DnsOverride Name: "ciscopark.com"
- *c xConfiguration Zones Zone 6 DNS SIP DnsOverride Override: "Off"
- *c xConfiguration Zones Zone 6 DNS SIP Media AesGcm Support: "Off"
- *c xConfiguration Zones Zone 6 DNS SIP Media Encryption Mode: "On"
- *c xConfiguration Zones Zone 6 DNS SIP Media ICE Support: "Off"
- *c xConfiguration Zones Zone 6 DNS SIP ParameterPreservation Mode: "Off"
- *c xConfiguration Zones Zone 6 DNS SIP Poison Mode: "Off"
- *c xConfiguration Zones Zone 6 DNS SIP PreloadedSipRoutes Accept: "On"
- *c xConfiguration Zones Zone 6 DNS SIP Record Route Address Type: "IP"
- *c xConfiguration Zones Zone 6 DNS SIP SearchAutoResponse: "Off"
- *c xConfiguration Zones Zone 6 DNS SIP TLS Verify InboundClassification: "On"
- *c xConfiguration Zones Zone 6 DNS SIP TLS Verify Mode: "On"
- *c xConfiguration Zones Zone 6 DNS SIP TLS Verify Subject Name: "callservice.ciscopark.com"
- *c xConfiguration Zones Zone 6 DNS SIP UDP BFCP Filter Mode: "Off"
- *c xConfiguration Zones Zone 6 DNS SIP UDP IX Filter Mode: "Off"

Na xConfiguration do Expressway-E, você pode ver que a dois valores específicos de interesse que se relacionam às buscas de DNS: **DnsOverride Name** e **DnsOverride Override**. Com base na xConfiguration, o DnsOverride Override é definido como Desligado, portanto, o DnsOverride Name não aconteceria. Para entender melhor o que esses valores fazem, você pode usar a interface da Web do Expressway para buscar a definição dos valores.

Modificar a solicitação DNS (se converte em DnsOverride Override no xConfig)

Roteia chamadas SIP de saída dessa zona para um domínio SIP especificado manualmente em vez do domínio no destino discado. Essa opção destina-se primariamente para uso com o Cisco Webex Call Service. Consulte www.cisco.com/go/hybrid-services.

Domínio para pesquisar (converte-se em DnsOverride Name na xConfig)

Insira um FQDN para encontrar um DNS em vez de pesquisar pelo domínio na URI de SIP de saída. A URI original do SIP não é afetada.

Agora que você tem essas definições, fica claro que eles, se definidos corretamente, seriam totalmente relevantes para a lógica de busca do DNS. Se você combinar isso com as instruções do Guia de implantação do Cisco Webex Hybrid Call Services, descobrirá que a solicitação de modificação de DNS deve estar definida como **On** e o domínio a ser pesquisado deve estar

definido como **callservice.ciscospark.com**. Se você fosse alterar esses valores para especificar as informações corretas, a lógica de busca SRV de DNS seria totalmente diferente. A seguir você verá um trecho do que pode esperar da perspectiva de log de diagnóstico do Expressway-E

```
2017-09-19T10:18:35.048-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 14:18:35,048"
Module="network.dns" Level="DEBUG": Detail="Sending DNS query"
Name="_sips._tcp.callservice.ciscospark.com" Type="SRV (IPv4 and IPv6)"
2017-09-19T10:18:35.126-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 14:18:35,126"
Module="network.dns" Level="DEBUG": Detail="Resolved hostname to:
['IPv4','TCP','146.20.193.70:5062'] (A/AAAA) ['IPv4','TCP','146.20.193.64:5062'] (A/AAAA)
Hostname:'l2sip-cfa-02.wbx2.com' Port:'5062' Priority:'5' TTL:'300' Weight:'10' (SRV)
Hostname:'l2sip-cfa-01.wbx2.com' Port:'5062' Priority:'5' TTL:'300' Weight:'10' (SRV) Number of
relevant records retrieved: 4"
```

Solução

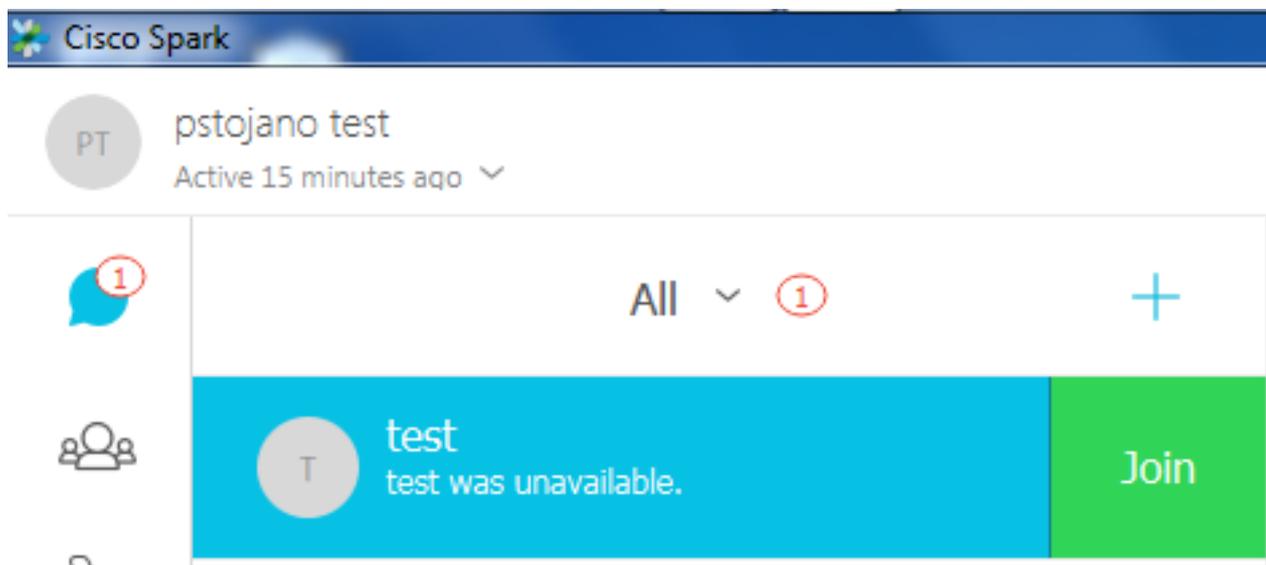
1. Faça login no Expressway-E
2. Navegue até **Configuração > Zonas > Zonas**
3. Selecione a zona DNS do Webex Hybrid que foi configurada
4. Defina a solicitação de modificação do DNS como **Ligado**
5. Defina o domínio para pesquisar pelo valor de **callservice.ciscospark.com**
6. Salve as alterações

Note: Caso haja apenas uma zona DNS sendo usada no Expressway, uma zona DNS separada deve ser configurada para ser usada com o Hybrid Call Service que pode aproveitar esses valores.

Problema 2. A porta 5062 está bloqueada para saída do Cisco Webex

Algo exclusivo a respeito das falhas de distribuição das chamadas de saída para o Cisco Webex é que o aplicativo Cisco Webex do destinatário da chamada apresentará um botão Ingressar no aplicativo, ainda que o cliente nunca toque. Como no cenário acima, nesse problema você novamente precisaria usar as mesmas ferramentas e logs para entender melhor onde há a falha. Para obter dicas sobre isolar os problemas de chamada e analisar logs, consulte a seção deste artigo como mostrado na imagem.

Ilustração da apresentação do botão Ingressar



Como com o problema de chamada de saída nº 1, é possível iniciar a análise no log de diagnóstico do Expressway-E, pois você usou o histórico de pesquisa no Expressway para determinar se a camada está percorrendo essa distância. Como antes, comece com o CONVITE inicial que entra no Expressway-E do Expressway-C. Lembre-se que as coisas que você deseja procurar são:

1. Se o Expressway-E recebe o CONVITE
2. Se a lógica da regra de pesquisa passa a chamada para a zona DNS do Hybrid
3. Se a zona DNS realiza a busca DNS e se o faz no domínio correto
4. Se o sistema tentou e estabeleceu corretamente um handshake TCP na porta 5062
5. Se o handshake TLS mútuo foi bem-sucedido

```
2017-09-19T10:18:35.023-04:00 amer-expressway01 tvcs: UTCtime="2017-09-19 14:18:35,017"
Module="network.sip" Level="DEBUG": Action="Received" Local-ip="192.168.1.6" Local-port="7003"
Src-ip="192.168.1.5" Src-port="26513" Msg-Hash="3732376649380137405"
SIPMSG:
|INVITE sip:pstojano-test@dmzlab.call.ciscospark.com SIP/2.0
Via: SIP/2.0/TLS 192.168.1.5:5061;egress-
zone=HybridCallServiceTraversal;branch=z9hG4bK57d8d5c823824bcd62f6ff7e09f9939482.899441b6d60c
444e4ed58951d07b5224;proxy-call-id=696f6f1c-9abe-47f3-96a4-e26f649fb76f;rport
Via: SIP/2.0/TCP 192.168.1.21:5065;branch=z9hG4bK12d4b77c97a64;received=192.168.1.21;ingress-
zone=CUCM11
Call-ID: 6a48de80-9c11273a-12d08-1501a8c0@192.168.1.21
CSeq: 101 INVITE
Call-Info: <urn:x-cisco-remotecall:callinfo>;x-cisco-video-traffic-class=DESKTOP
Remote-Party-ID: "Jonathan Robb"
<sip:5010@rtp.ciscotac.net>;party=calling;screen=yes;privacy=off
Contact: <sip:5010@192.168.1.21:5065;transport=tcp>;video;audio
From: "Jonathan Robb"

;tag=328867~c9cc7ddc-9592-49e8-a13c-79e26f48eebc-30106829
To:

Max-Forwards: 15
Record-Route: <sip:proxy-call-id=696f6f1c-9abe-47f3-96a4-
e26f649fb76f@192.168.1.5:5061;transport=tls;lr>
Record-Route: <sip:proxy-call-id=696f6f1c-9abe-47f3-96a4-
e26f649fb76f@192.168.1.5:5060;transport=tcp;lr>
Allow: INVITE, OPTIONS, INFO, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY
User-Agent: Cisco-CUCM11.5
Expires: 180
Date: Tue, 19 Sep 2017 14:18:34 GMT
Supported: timer, resource-priority, replaces, X-cisco-srtp-fallback, X-cisco-original-called
Session-Expires: 1800
Min-SE: 1800
Allow-Events: presence
X-TAATag: b2967a3b-93fb-4ca4-b0d7-131f75335684
Session-ID: 75957d4fb66a13e835c10737aa328865;remote=00000000000000000000000000000000
Cisco-Guid: 1783160448-0000065536-0000000126-0352430272
Content-Type: application/sdp
Content-Length: 714
<SDP Omitted>
```

Como é possível ver no CONVITE acima, o CONVITE é recebido normalmente. Esta é uma ação "recebida" e está se originando no endereço IP do Expressway-C. Você agora pode mover-se para a lógica de regra de pesquisa

```
2017-09-19T10:18:35.023-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 14:18:35,022"
Module="network.search" Level="DEBUG": Detail="Search rule 'B2B calls to VCS-C' did not match
destination alias 'pstojano-test@dmzlab.call.ciscospark.com'"
2017-09-19T10:18:35.023-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 14:18:35,022"
Module="network.search" Level="DEBUG": Detail="Search rule 'Webex Hybrid' ignored due to source
filtering"
2017-09-19T10:18:35.023-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 14:18:35,022"
Module="network.search" Level="DEBUG": Detail="Search rule 'Calls to Webex' did not match
destination alias 'pstojano-test@dmzlab.call.ciscospark.com'"
2017-09-19T10:18:35.023-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 14:18:35,022"
Module="network.search" Level="DEBUG": Detail="Considering search rule 'Webex Hybrid - to Webex
Cloud' towards target 'Hybrid Call Services DNS' at priority '90' with alias 'pstojano-
test@dmzlab.call.ciscospark.com'"
```

Com base no trecho de log acima, você pode ver que o Expressway-E foi analisado por quatro regras de pesquisa, no entanto, apenas uma (*Webex Hybrid - para Webex Cloud*) foi considerado. A regra de pesquisa tinha uma prioridade de 90 e estava prevista para ir para o *Zona DNS de serviços de chamada híbrida*. Agora que a chamada está sendo enviada para uma zona DNS, é possível revisar as buscas SRV DNS que acontecem no Expressway-E. Tudo isso é totalmente normal. Agora é possível se concentrar na lógica de busca do DNS

```
2017-09-19T10:18:35.048-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 14:18:35,048"
Module="network.dns" Level="DEBUG": Detail="Sending DNS query"
Name="_sips._tcp.callservice.ciscospark.com" Type="SRV (IPv4 and IPv6)"
2017-09-19T10:18:35.126-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 14:18:35,126"
Module="network.dns" Level="DEBUG": Detail="Resolved hostname to:
['IPv4','TCP','146.20.193.70:5062'] (A/AAAA) ['IPv4','TCP','146.20.193.64:5062'] (A/AAAA)
Hostname:'l2sip-cfa-02.wbx2.com' Port:'5062' Priority:'5' TTL:'300' Weight:'10' (SRV)
Hostname:'l2sip-cfa-01.wbx2.com' Port:'5062' Priority:'5' TTL:'300' Weight:'10' (SRV) Number of
relevant records retrieved: 4"
```

Você pode ver claramente isso nessa instância, que o registro SRV callservice.ciscospark.com é resolvido. A resposta são quatro registros diferentes válidos, todos usando a porta 5062. Este é um comportamento normal. Nesse momento, é possível analisar o handshake TCP que deve vir a seguir. Como mencionado anteriormente no documento, é possível pesquisar os logs de diagnóstico por "Conexão TCP" e buscar o item de linha que lista Dst-port="5062". A seguir encontra-se uma amostra do que você verá nesse cenário:

```
2017-09-19T10:18:35.474-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 14:18:35,474"
Module="network.tcp" Level="DEBUG": Src-ip="172.16.2.2" Src-port="25026" Dst-ip="146.20.193.70"
Dst-port="5062" Detail="TCP Connecting"
2017-09-19T10:28:35.295-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 14:28:35,289"
Module="network.tcp" Level="ERROR": Src-ip="172.16.2.2" Src-port="25026" Dst-ip="146.20.193.70"
Dst-port="5062" Detail="TCP Connection Failed"
```

Você também pode usar o tcpdump que foi incluído no pacote de log de diagnóstico para obter algumas informações mais detalhadas sobre o handshake TCP como mostrado na imagem.

Expressway-E attempts TCP Connection twice

| No. | Time | Source | Destination | Protocol | S Port | D Port | Length | Info |
|-----|----------------------------|------------|---------------|----------|--------|--------|--------|---|
| 2 | 2017-09-19 14:18:35.474312 | 172.16.2.2 | 146.20.193.70 | TCP | 25026 | 5062 | 74 | 25026->5062 [SYN] Seq=0 win=29200 Len=0 |
| 3 | 2017-09-19 14:18:36.523324 | 172.16.2.2 | 146.20.193.70 | TCP | 25026 | 5062 | 74 | [TCP Retransmission] 25026->5062 [SYN] |
| 4 | 2017-09-19 14:18:38.571325 | 172.16.2.2 | 146.20.193.70 | TCP | 25026 | 5062 | 74 | [TCP Retransmission] 25026->5062 [SYN] |
| 7 | 2017-09-19 14:18:42.603331 | 172.16.2.2 | 146.20.193.70 | TCP | 25026 | 5062 | 74 | [TCP Retransmission] 25026->5062 [SYN] |
| 8 | 2017-09-19 14:18:45.807635 | 172.16.2.2 | 146.20.193.64 | TCP | 25027 | 5062 | 74 | 25027->5062 [SYN] Seq=0 win=29200 Len=0 |
| 9 | 2017-09-19 14:18:46.827328 | 172.16.2.2 | 146.20.193.64 | TCP | 25027 | 5062 | 74 | [TCP Retransmission] 25027->5062 [SYN] |
| 10 | 2017-09-19 14:18:48.875336 | 172.16.2.2 | 146.20.193.64 | TCP | 25027 | 5062 | 74 | [TCP Retransmission] 25027->5062 [SYN] |
| 11 | 2017-09-19 14:18:52.907335 | 172.16.2.2 | 146.20.193.64 | TCP | 25027 | 5062 | 74 | [TCP Retransmission] 25027->5062 [SYN] |

The Expressway-E doesn't receive a SYN-ACK so it attempts to retransmit.

Nesse ponto, é possível concluir que o Expressway-E está roteando a chamada corretamente. O desafio nesse cenário é que a conexão TCP não pode ser estabelecida no ambiente Webex. Isso pode estar acontecendo porque o ambiente Webex não está respondendo ao pacote SYN TCP, no entanto, isso seria improvável, considerando que o servidor que manipula a conexão é compartilhado entre vários clientes. A causa mais provável nesse cenário é que algum tipo de dispositivo intermediário (firewall, IPS etc) não está permitindo a saída do tráfego.

Solução

Como o problema foi isolado, esses dados podem ser fornecidos pelo administrador de rede do cliente. Além disso, caso precise de mais informações, é possível tirar uma captura da interface externa do dispositivo de borda e/ou do firewall para obter mais provas. Pela perspectiva do Expressway, não há mais ações a realizar já que o problema está no dispositivo.

Problema 3. Erro de configuração da regra de pesquisa do Expressway

Os problemas de configuração de regra de pesquisa é um dos maiores problemas relacionados à configuração nos Expressways. Os problemas de configuração de regra de pesquisa podem ser bidirecionais, pois você precisa das regras de pesquisa para as chamadas de entrada e para as chamadas de saída. Quando você analisa o problema, descobre que, ainda que os problemas de regex sejam bastante comuns no Expressway, eles nem sempre são a causa de um problema de regra de pesquisa. Neste segmento específico, você vai analisar uma chamada de saída que está falhando. Como em todos os outros cenários de distribuição de chamada de saída, os sintomas continuam os mesmos:

- O aplicativo Cisco Webex do destinatário da chamada apresentou um botão Ingressar
- O telefone do chamador estava reproduzindo um toque
- O telefone do destinatário da chamada no local estava tocando
- O aplicativo Cisco Webex do destinatário da chamada nunca tocou

Como em todos os outros cenários, você também vai querer aproveitar os rastreamentos SDL do CUCM juntamente com os logs de diagnóstico do Expressway-C e E. Como anteriormente, você deve consultar o histórico de pesquisa e as dicas para identificar uma chamada nos logs de diagnóstico. Como anteriormente, foi determinado usando o histórico de pesquisa do Expressway-E que essa chamada estava chegando ao destino e falhando. A seguir, está o início da análise que observamos na chegada do CONVITE SIP inicial no Expressway-E pelo Expressway-C.

```
2017-09-25T11:26:02.959-04:00 amer-expressway01 tvcs: UTCTime="2017-09-25 15:26:02,959"
Module="network.sip" Level="DEBUG": Action="Received" Local-ip="192.168.1.6" Local-port="7003"
Src-ip="192.168.1.5" Src-port="25675" Msg-Hash="1536984498381728689"
SIPMSG:
|INVITE sip:pstojano-test@dmzlab.call.ciscospark.com SIP/2.0
```

Via: SIP/2.0/TLS 192.168.1.5:5061;egress-
zone=HybridCallServiceTraversal;branch=z9hG4bK1c7bf93ff08014ca5e00bb0b5f8b184b272412.a81f2992e38
63ac202a000a3dd599763;proxy-call-id=f79b8631-947b-46d4-a888-911bf0150bfe;rport
Via: SIP/2.0/TCP 192.168.1.21:5065;branch=z9hG4bK1c8c419938648;received=192.168.1.21;ingress-
zone=CUCM11
Call-ID: d58f2680-9c91200a-1c7ba-1501a8c0@192.168.1.21
CSeq: 101 INVITE
Call-Info: <urn:x-cisco-remotecall:callinfo>;x-cisco-video-traffic-class=DESKTOP
Remote-Party-ID: "Jonathan Robb"
<sip:5010@rtp.ciscotac.net>;party=calling;screen=yes;privacy=off
Contact: <sip:5010@192.168.1.21:5065;transport=tcp>;video;audio
From: "Jonathan Robb"

tag=505817~c9cc7ddc-9592-49e8-a13c-79e26f48eebc-30106972

To:

Max-Forwards: 15
Record-Route: <sip:proxy-call-id=f79b8631-947b-46d4-a888-
911bf0150bfe@192.168.1.5:5061;transport=tls;lr>
Record-Route: <sip:proxy-call-id=f79b8631-947b-46d4-a888-
911bf0150bfe@192.168.1.5:5060;transport=tcp;lr>
Allow: INVITE, OPTIONS, INFO, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY
User-Agent: Cisco-CUCM11.5
Expires: 180
Date: Mon, 25 Sep 2017 15:26:02 GMT
Supported: timer, resource-priority, replaces, X-cisco-srtp-fallback, X-cisco-original-called
Session-Expires: 1800
Min-SE: 1800
Allow-Events: presence
X-TAATag: 8e8c014d-5d01-4581-8108-5cb096778fc5
Session-ID: 75957d4fb66a13e835c10737aa505813;remote=00000000000000000000000000000000
Cisco-Guid: 3582928512-0000065536-0000000240-0352430272
Content-Type: application/sdp
Content-Length: 714

<SDP Omitted>

Usando a ID de chamada (**d58f2680-9c91200a-1c7ba-1501a8c0**) do cabeçalho SIP, você pode pesquisar rapidamente todas as mensagens associadas a esse diálogo. Ao analisar a terceira ocorrência da ID de chamada nos logs, é possível ver que o Expressway-E envia imediatamente um erro **404 não encontrado para o Expressway-C**.

2017-09-25T11:26:13.286-04:00 amer-expressway01 tvcs: UTCTime="2017-09-25 15:26:13,286"
Module="network.sip" Level="DEBUG": **Action="Sent"** Local-ip="192.168.1.6" Local-port="7003" Dst-
ip="192.168.1.5" Dst-port="25675" Msg-Hash="12372154521012287279"

SIPMSG:

|SIP/2.0 404 Not Found

Via: SIP/2.0/TLS 192.168.1.5:5061;egress-
zone=HybridCallServiceTraversal;branch=z9hG4bK1c7bf93ff08014ca5e00bb0b5f8b184b272412.a81f2992e38
63ac202a000a3dd599763;proxy-call-id=f79b8631-947b-46d4-a888-
911bf0150bfe;received=192.168.1.5;rport=25675;ingress-zone=HybridCallServiceTraversal
Via: SIP/2.0/TCP 192.168.1.21:5065;branch=z9hG4bK1c8c419938648;received=192.168.1.21;ingress-
zone=CUCM11
Call-ID: d58f2680-9c91200a-1c7ba-1501a8c0@192.168.1.21
CSeq: 101 INVITE

From: "Jonathan Robb"

;tag=505817~c9cc7ddc-9592-49e8-a13c-79e26f48eebc-30106972

To:

Server: TANDBERG/4135 (X8.10.2) Warning: 399 192.168.1.6:7003 "Policy Response"
Session-ID: 00000000000000000000000000000000;remote=75957d4fb66a13e835c10737aa505813 Content-
Length: 0

Esses dados informam duas coisas:

1. O Expressway-E nunca tentou enviar o CONVITE para o Cisco Webex
2. O Expressway-E foi a parte responsável por tomar a decisão lógica de rejeitar a chamada com um erro 404 não encontrado.

Um erro 404 não encontrado normalmente significa que o Expressway não foi capaz de encontrar o endereço de destino. Como os Expressways usam regras de pesquisa para rotear chamadas entre si e para diferentes ambientes, comece se concentrando na xConfiguration do Expressway-E. Nessa xConfiguration, é possível buscar a regra de pesquisa que deve passar a chamada para a zona DNS Webex Hybrid. Para localizar as regras de pesquisa configuradas no Expressway pela perspectiva do xConfiguration, é possível pesquisar por "Regra de pesquisa de política de zonas de xConfiguration". Ao fazer isso, você verá uma lista de configuração de Regras de pesquisa para cada regra de pesquisa criada no Expressway. O número que vem depois de "Regra" aumentará com base na regra de pesquisa que foi criada primeiro marcada como 1. Se tiver problemas para encontrar a regra de pesquisa. Você pode usar valores de nome usados normalmente como "Webex" para localizar melhor a regra de pesquisa. Outra maneira de identificar a regra é encontrar o valor da String de Padrão definido como ".*@.*\.ciscopark\.com". Esta é a string de padrão que deverá ser configurada. (*Supondo que a string de padrão esteja configurada corretamente*)Depois de analisar a xConfiguration neste cenário, será possível ver que a Regra de pesquisa 6 é a regra correta para passar a chamada para o Cisco Webex.

```
*c xConfiguration Zones Policy SearchRules Rule 6 Authentication: "No"
*c xConfiguration Zones Policy SearchRules Rule 6 Description: "Outbound calls to Webex"
*c xConfiguration Zones Policy SearchRules Rule 6 Mode: "AliasPatternMatch"
*c xConfiguration Zones Policy SearchRules Rule 6 Name: "Webex Hybrid - to Webex Cloud"
*c xConfiguration Zones Policy SearchRules Rule 6 Pattern Behavior: "Leave"
*c xConfiguration Zones Policy SearchRules Rule 6 Pattern Replace:
*c xConfiguration Zones Policy SearchRules Rule 6 Pattern String: ".*@.*\.ciscopark\.com"
*c xConfiguration Zones Policy SearchRules Rule 6 Pattern Type: "Regex"
*c xConfiguration Zones Policy SearchRules Rule 6 Priority: "101"
*c xConfiguration Zones Policy SearchRules Rule 6 Progress: "Stop"
*c xConfiguration Zones Policy SearchRules Rule 6 Protocol: "SIP"
*c xConfiguration Zones Policy SearchRules Rule 6 SIPTrafficType: "Any"
*c xConfiguration Zones Policy SearchRules Rule 6 Source Mode: "Named"
*c xConfiguration Zones Policy SearchRules Rule 6 Source Name: "Hybrid Call Service Traversal"
*c xConfiguration Zones Policy SearchRules Rule 6 State: "Enabled"
*c xConfiguration Zones Policy SearchRules Rule 6 SystemGenerated: "No"
*c xConfiguration Zones Policy SearchRules Rule 6 Target Name: "Hybrid Call Services DNS"
*c xConfiguration Zones Policy SearchRules Rule 6 Target SIPVariant: "Any"
*c xConfiguration Zones Policy SearchRules Rule 6 Target Type: "Zone"
```

Para testar esse padrão, podemos usar a função de verificação de padrão descrita em. O importante aqui é que gostaríamos que os seguintes valores fossem configurados:Manutenção > Ferramentas > Verificar padrão

- Alias: %URI da solicitação no CONVITE inicial% (Ex: pstojano-test@dmzlab.call.ciscospark.com)
- Tipo de padrão: Regex
- String de padrão .*@\.*\ciscospark\com
- Comportamento padrão: Sair

Se o Regex da regra estiver configurada corretamente, deverá ver o resultado bem-sucedido da verificação do padrão. A seguir há uma ilustração demonstrando isso como mostrado na imagem:

Check pattern

Alias: pstojano-test@dmzlab.call.ciscospark.com

Pattern type: **Regex**

Pattern string: .*@\.*\ciscospark\com

Pattern behavior: **Leave**

Check pattern

Result

Result: **Succeeded**

Details: Alias matched pattern

Alias: pstojano-test@dmzlab.call.ciscospark.com

Agora que você consegue confirmar que a regra de pesquisa está presente e configurada corretamente, é possível observar melhor a lógica de pesquisa sendo executada pelo Expressway para determinar se ela está afetando o Expressway-E que está enviando o erro 404 não encontrado. A seguir há uma amostra da lógica de regra de pesquisa sendo executada pelo Expressway.

```
2017-09-25T11:26:02.966-04:00 amer-expressway01 tvcs: UTCTime="2017-09-25 15:26:02,966"
Module="network.search" Level="DEBUG": Detail="Search rule 'B2B calls to VCS-C' did not match
destination alias 'pstojano-test@dmzlab.call.ciscospark.com'"
2017-09-25T11:26:02.966-04:00 amer-expressway01 tvcs: UTCTime="2017-09-25 15:26:02,966"
Module="network.search" Level="DEBUG": Detail="Search rule 'Webex Hybrid' ignored due to source
filtering"
2017-09-25T11:26:02.966-04:00 amer-expressway01 tvcs: UTCTime="2017-09-25 15:26:02,966"
Module="network.search" Level="DEBUG": Detail="Search rule 'Calls to Webex' did not match
destination alias 'pstojano-test@dmzlab.call.ciscospark.com'"
2017-09-25T11:26:02.967-04:00 amer-expressway01 tvcs: UTCTime="2017-09-25 15:26:02,967"
Module="network.search" Level="DEBUG": Detail="Considering search rule 'to DNS' towards target
'DNS' at priority '100' with alias 'pstojano-test@dmzlab.call.ciscospark.com'"

2017-09-25T11:26:02.968-04:00 amer-expressway01 tvcs: UTCTime="2017-09-25 15:26:02,968"
Module="network.dns" Level="DEBUG": Detail="Sending DNS query" Name="dmzlab.call.ciscospark.com"
Type="NAPTR (IPv4 and IPv6)"
2017-09-25T11:26:02.982-04:00 amer-expressway01 tvcs: UTCTime="2017-09-25 15:26:02,982"
Module="network.dns" Level="DEBUG": Detail="Could not resolve hostname"
2017-09-25T11:26:02.982-04:00 amer-expressway01 tvcs: UTCTime="2017-09-25 15:26:02,982"
Module="network.dns" Level="DEBUG": Detail="Sending DNS query"
Name="_sips._tcp.dmzlab.call.ciscospark.com" Type="SRV (IPv4 and IPv6)"
```

Nesta amostra, você pode ver que o Expressway processou quatro regras de pesquisa. Os 3 primeiros não foram considerados por diversas razões, no entanto, o 4º foi considerado. O dado importante é que imediatamente depois da consideração o Expressway segue diretamente para a lógica de busca DNS. Caso lembre-se do que vimos na xConfiguration, a regra de pesquisa configurada no Webex Hybrid chamava-se Webex Hybrid - para Webex Cloud e não foi considerada na lógica de regra de pesquisa acima. Nesse ponto, vale a pena observar como a

regra de pesquisa considerada (para DNS) foi implementada para que você possa entender melhor se ela está afetando o uso da regra de pesquisa do Webex Hybrid. Para fazer isso, é possível visitar a xConfig, dessa vez buscando pela regra de pesquisa chamada "para DNS"

```
*c xConfiguration Zones Policy SearchRules Rule 1 Authentication: "No"
*c xConfiguration Zones Policy SearchRules Rule 1 Description:
*c xConfiguration Zones Policy SearchRules Rule 1 Mode: "AliasPatternMatch"
*c xConfiguration Zones Policy SearchRules Rule 1 Name: "to DNS"
*c xConfiguration Zones Policy SearchRules Rule 1 Pattern Behavior: "Leave"
*c xConfiguration Zones Policy SearchRules Rule 1 Pattern Replace:
*c xConfiguration Zones Policy SearchRules Rule 1 Pattern String: "(?!.*%localdomains%.*$).*"
*c xConfiguration Zones Policy SearchRules Rule 1 Pattern Type: "Regex"
*c xConfiguration Zones Policy SearchRules Rule 1 Priority: "100"
*c xConfiguration Zones Policy SearchRules Rule 1 Progress: "Stop"
*c xConfiguration Zones Policy SearchRules Rule 1 Protocol: "Any"
*c xConfiguration Zones Policy SearchRules Rule 1 SIPTrafficType: "Any"
*c xConfiguration Zones Policy SearchRules Rule 1 Source Mode: "Any"
*c xConfiguration Zones Policy SearchRules Rule 1 Source Name: "Please Select"
*c xConfiguration Zones Policy SearchRules Rule 1 State: "Enabled"
*c xConfiguration Zones Policy SearchRules Rule 1 SystemGenerated: "No"
*c xConfiguration Zones Policy SearchRules Rule 1 Target Name: "DNS"
*c xConfiguration Zones Policy SearchRules Rule 1 Target SIPVariant: "Any"
*c xConfiguration Zones Policy SearchRules Rule 1 Target Type: "Zone"
```

Depois de revisar essa regra de pesquisa, será possível concluir o seguinte:

- A string de padrão corresponderia À URI de solicitação do Cisco Webex
- A prioridade é definida como 100
- O progresso (comportamento do padrão) fica definido como Parar.

Essas informações nos dizem que a URI de solicitação do Cisco Webex sendo chamada corresponderia a essa regra e, se a regra correspondesse ao Expressway, pararia de pesquisar (Considerando) outras regras de pesquisa. Com esse entendimento, a prioridade de regras se torna um fator essencial. A forma como a prioridade de regra de pesquisa do Expressway funciona é que a regra de prioridade mais baixa é tentada primeiro. A seguir, está um exemplo. Regra de pesquisa: LocalComportamento padrão: ContinuarPrioridade 1 Regra de pesquisa: VizinhoComportamento padrão: ContinuarPrioridade 10 Regra de pesquisa: DNSComportamento padrão: PararPrioridade 50 Neste exemplo, a regra de pesquisa chamada Local (1) seria tentada primeiro e, se fosse encontrada uma correspondência, ela seria movida para a regra de pesquisa Vizinho (10) devido ao comportamento padrão definido como Continuar. Se a regra de pesquisa Vizinho não tiver correspondências, ela ainda continuará para a regra de pesquisa DNS (50) e a considerará como a última. Caso a regra de pesquisa DNS tiver correspondência, a pesquisa seria interrompida independentemente de se havia outra regra de pesquisa com uma prioridade superior a 50, pois o comportamento do padrão foi definido como Parar. Com esse entendimento, é possível observar as prioridades de regra de pesquisa entre as regras "para DNS" e "Webex Hybrid para Webex Cloud".

```
*c xConfiguration Zones Policy SearchRules Rule 1 Name: "to DNS"
*c xConfiguration Zones Policy SearchRules Rule 1 Priority: "100"
*c xConfiguration Zones Policy SearchRules Rule 1 Progress: "Stop"

*c xConfiguration Zones Policy SearchRules Rule 6 Name: "Webex Hybrid - to Webex Cloud"
*c xConfiguration Zones Policy SearchRules Rule 6 Priority: "101"
*c xConfiguration Zones Policy SearchRules Rule 6 Progress: "Stop"
```

Aqui, você pode ver que a regra "para DNS" tem uma prioridade mais baixa do que a regra "Webex Hybrid - para Webex Cloud" — portanto, a regra "para DNS" será tentada primeiro. Considerando que o comportamento do padrão (Progresso) está definido como Parar, o Expressway-E nunca considera que a regra Webex Hybrid - para Webex Cloud e a chamada acaba falhando. Solução Esse tipo de problema é cada vez mais comum no Hybrid Call Service Connect. Muitas vezes, quando a solução é implantada, as pessoas criam uma regra de alta prioridade a ser usada para pesquisas do Cisco Webex. Muitas vezes essa regra que é criada

não está sendo chamada devido a regras de prioridade mais baixa existentes sendo correspondidas e isso resulta em uma falha. Esse problema acontece em chamadas de entrada e saída do Cisco Webex. Para resolver isso, você precisará seguir estas etapas:

1. Faça login no Expressway-E
2. Navegue até Configuração > Plano de discagem > Regras de pesquisa
3. Localize a regra de pesquisa Webex Hybrid e clique nela (Ex: Nome: Webex Hybrid - para Webex Cloud)
4. Defina o valor de prioridade para algo abaixo de outras regras de pesquisa, mas alto o suficiente que não vai afetar as outras. (Ex: Prioridade: 99)

A regra geral das regras de pesquisa é que quanto mais específica é a string de padrão, mais baixo ela pode ser colocada na lista de prioridades de regras de pesquisa. Normalmente uma zona DNS é configurada com uma string de padrão que vai obter qualquer coisa que não seja um domínio local e enviá-las para a Internet. Por isso, recomendamos que você defina esse tipo de regra de pesquisa para uma prioridade alta, para que ela seja chamada por último. Problema 4. Configuração incorreta de CPL do ExpresswayA solução Expressway permite a mitigação de fraude de tarifas usando a lógica de linguagem de processamento de chamadas (CPL) disponível no servidor. Se a solução Expressway sendo implantada estiver sendo usada apenas para o Cisco Webex Hybrid Call Service e acesso remoto e móvel, é altamente recomendável que as regras e a política de CPL sejam ativadas e implementadas. Enquanto a configuração de CPL no Expressway para Cisco Webex Hybrid seja relativamente simples, se houver problemas e configuração ele poderá bloquear tentativas de chamada com facilidade. Os cenários abaixo mostram como usar o log de diagnóstico e identificar um problema de configuração de CPL. Como em todos os outros cenários de distribuição de chamada de saída, os sintomas continuam os mesmos:

- O aplicativo Cisco Webex do destinatário da chamada apresentou um botão Ingressar
- O telefone do chamador estava reproduzindo um toque
- O telefone do destinatário da chamada no local estava tocando
- O aplicativo do destinatário da chamada nunca tocou

Como em todos os outros cenários, você pode usar os rastreamentos SDL do CUCM juntamente com os logs de diagnóstico do Expressway-C e E. Como antes, você deve consultar o para usar o Histórico de pesquisa e dicas para identificar uma chamada nos logs de diagnóstico. Como anteriormente, foi determinado usando o histórico de pesquisa do Expressway-E que essa chamada estava chegando ao destino e falhando. A seguir está o início da análise que você pode observar na chegada do CONVITE SIP inicial no Expressway-E pelo Expressway-C.

```
2017-09-25T16:54:43.722-04:00 amer-expressway01 tvcs: UTCTime="2017-09-25 20:54:43,722"
Module="network.sip" Level="DEBUG": Action="Received" Local-ip="192.168.1.6" Local-port="7003"
Src-ip="192.168.1.5" Src-port="26404" Msg-Hash="17204952472509519266"
SIPMSG:
|INVITE sip:pstojano-test@dmzlab.call.ciscopark.com SIP/2.0
Via: SIP/2.0/TLS 192.168.1.5:5061;egress-
zone=HybridCallServiceTraversal;branch=z9hG4bK781a130d234ed9aaec86834368739430283256.34216c32a0d
e36e16590bae36df388b6;proxy-call-id=3bbbf94a-082e-4088-8f5a-5ea7e82f8aac;rport
Via: SIP/2.0/TCP 192.168.1.21:5065;branch=z9hG4bK1cf344a8b117e;received=192.168.1.21;ingress-
zone=CUCM11
Call-ID: c030f100-9c916d13-1cdcb-1501a8c0@192.168.1.21
CSeq: 101 INVITE
Call-Info: <urn:x-cisco-remotecallinfo>;x-cisco-video-traffic-class=DESKTOP
Remote-Party-ID: "Jonathan Robb"
<sip:5010@rtp.ciscotac.net>;party=calling;screen=yes;privacy=off
Contact: <sip:5010@192.168.1.21:5065;transport=tcp>;video;audio
From: "Jonathan Robb"
```

;tag=512579~c9cc7ddc-9592-49e8-a13c-79e26f48eebc-30107000

To:

Max-Forwards: 15
Record-Route: <sip:proxy-call-id=3bbbf94a-082e-4088-8f5a-5ea7e82f8aac@192.168.1.5:5061;transport=tls;lr>
Record-Route: <sip:proxy-call-id=3bbbf94a-082e-4088-8f5a-5ea7e82f8aac@192.168.1.5:5060;transport=tcp;lr>
Allow: INVITE, OPTIONS, INFO, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY
User-Agent: Cisco-CUCM11.5
Expires: 180
Date: Mon, 25 Sep 2017 20:54:43 GMT
Supported: timer, resource-priority, replaces, X-cisco-srtp-fallback, X-cisco-original-called
Session-Expires: 1800
Min-SE: 1800
Allow-Events: presence
X-TAATag: 4ffffefed-0512-4067-ac8c-35828f0a1150
Session-ID: 75957d4fb66a13e835c10737aa512577;remote=00000000000000000000000000000000
Cisco-Guid: 3224432896-0000065536-0000000264-0352430272
Content-Type: application/sdp
Content-Length: 714

<SDP Omitted>

Com a ID de chamada (c030f100-9c916d13-1cdcb-1501a8c0) no cabeçalho SIP, você pesquisa rapidamente todas as mensagens associadas a este diálogo. Ao analisar a terceira ocorrência da ID de chamada nos logs, é possível ver que o Expressway-E envia imediatamente um erro 403 proibido para o Expressway-C.

2017-09-25T16:54:43.727-04:00 amer-expressway01 tvcs: UTCTime="2017-09-25 20:54:43,727"
Module="network.sip" Level="DEBUG": Action="Sent" Local-ip="192.168.1.6" Local-port="7003" Dst-ip="192.168.1.5" Dst-port="26404" Msg-Hash="9195436101110134622"
SIPMSG:
|SIP/2.0 403 Forbidden
Via: SIP/2.0/TLS 192.168.1.5:5061;egress-zone=HybridCallServiceTraversal;branch=z9hG4bK781a130d234ed9aaec86834368739430283256.34216c32a0de36e16590bae36df388b6;proxy-call-id=3bbbf94a-082e-4088-8f5a-5ea7e82f8aac;received=192.168.1.5;rport=26404;ingress-zone=HybridCallServiceTraversal
Via: SIP/2.0/TCP 192.168.1.21:5065;branch=z9hG4bK1cf344a8b117e;received=192.168.1.21;ingress-zone=CUCM11
Call-ID: c030f100-9c916d13-1cdcb-1501a8c0@192.168.1.21
CSeq: 101 INVITE
From: "Jonathan Robb"

;tag=512579~c9cc7ddc-9592-49e8-a13c-79e26f48eebc-30107000

To:

;tag=64fe7f9eab37029d
Server: TANDBERG/4135 (X8.10.2)
Warning: 399 192.168.1.6:7003 "Policy Response"
Session-ID: 00000000000000000000000000000000;remote=75957d4fb66a13e835c10737aa512577
Content-Length: 0

Para entender porque o Expressway-E negou essa chamada e enviou um erro 403 proibido para o Expressway-C, você deverá analisar as entradas de log entre o 403 proibido e o CONVITE SIP

original que foi inserido no Expressway. Ao analisar essas entradas de log, você normalmente poderá ver todas as decisões de lógica sendo tomadas. Observe que você não vê regras de pesquisa sendo chamadas, mas vê a lógica de linguagem de processo de chamada (CPL) sendo chamada. Abaixo encontra-se um trecho disso.

```
2017-09-25T16:54:43.725-04:00 amer-expressway01 tvcs: UTCTime="2017-09-25 20:54:43,725"  
Module="network.cpl" Level="DEBUG": Remote-ip="192.168.1.5" Remote-port="26404" Detail="CPL:
```

```
2017-09-25T16:54:43.725-04:00 amer-expressway01 tvcs: UTCTime="2017-09-25 20:54:43,725"  
Module="network.cpl" Level="DEBUG": Remote-ip="192.168.1.5" Remote-port="26404" Detail="CPL:
```

```
2017-09-25T16:54:43.725-04:00 amer-expressway01 tvcs: UTCTime="2017-09-25 20:54:43,726"  
Module="network.cpl" Level="DEBUG": Remote-ip="192.168.1.5" Remote-port="26404" Detail="CPL:
```

```
2017-09-25T16:54:43.725-04:00 amer-expressway01 tvcs: UTCTime="2017-09-25 20:54:43,726"  
Module="network.cpl" Level="DEBUG": Remote-ip="192.168.1.5" Remote-port="26404" Detail="CPL:
```

Com base na análise de log acima, você pode fazer a determinação de que a CPL está rejeitando a chamada.

```
2017-09-25T16:54:43.725-04:00 amer-expressway01 tvcs: Event="Search Completed"  
Reason="Forbidden" Service="SIP" Src-alias-type="SIP" Src-alias="5010@rtp.ciscotac.net" Dst-  
alias-type="SIP" Dst-alias="sip:pstojano-test@dmzlab.call.ciscospark.com" Call-serial-  
number="48c80582-ec79-4d89-82e2-e5546f35703c" Tag="4ffefed-0512-4067-ac8c-35828f0a1150"  
Detail="found:false, searchtype:INVITE, Info:Policy Response" Level="1" UTCTime="2017-09-25  
20:54:43,726"
```

```
2017-09-25T16:54:43.725-04:00 amer-expressway01 tvcs: Event="Call Rejected" Service="SIP" Src-  
ip="192.168.1.5" Src-port="26404" Src-alias-type="SIP"
```

Note: Nessa situação, você não verá as regras de pesquisa sendo chamadas porque CPLs, FindMe e Transforms são todos processados antes de uma regra de pesquisa Na maioria das circunstâncias, é possível aproveitar a xConfig do Expressway para entender melhor as circunstâncias. No entanto, nas CPLs, não é possível ver as regras que estão definidas, apenas se a política estiver ativada. Abaixo está uma parte de xConfig que nos mostra que esse Expressway-E está usando a lógica de CPL local.

```
*c xConfiguration Policy AdministratorPolicy Mode: "LocalCPL"
```

Para entender melhor a configuração de regra, será necessário fazer login no Expressway-E e navegar até Configuração > Política de chamadas > Regras como mostrado na imagem.



| Source | Destination | Action | Rearrange |
|------------------------------|------------------------------|--------|-----------|
| *@dmzlab.call.ciscospark.com | *@dmzlab.call.ciscospark.com | Reject | |

Ao revisar essas configurações, será possível ver que o seguinte está configurado: Fonte: .*Destino: .*@dmzlab.call.ciscospark.com.* Ação: Reject Em comparação com o que foi documentado no [Guia de implantação do Cisco Webex Hybrid Call Service](#), você pode ver que a origem e o destino foram configurados ao contrário.

| Field | Setting |
|---------------------|---|
| Source Type | From address |
| Rule applies to | Unauthenticated callers |
| Source pattern | .*@example\.call\.ciscopark\.com.* , where example is your company's subdomain. |
| Destination pattern | .* |
| Action | Reject |

Solução Para resolver esse problema, você precisa reajustar a configuração da regra CPL para que a Origem seja definida como **.*@%Webex_subdomain%\.call\.ciscopark\.com.*** e o Padrão de Destino seja **.***

1. Faça login no Expressway-E
2. Navegue até Configuração > Política de chamadas > Regras
3. Selecione a regra que foi configurada no serviço Cisco Webex Hybrid Call
4. Digite o padrão de origem como **.*@%Webex_subdomain%\.call\.ciscopark\.com.*** (Ex: **.*@dmzlab\.call\.ciscopark\.com.***)
5. Insira o padrão de destino como **.***
6. Selecione Salvar

Para obter mais informações sobre a implementação de CPL para Webex Hybrid, consulte o [Guia de design do Cisco Webex Hybrid](#). Bidirecional: Cisco Webex para o local ou Local para o Cisco Webex

Problema 1. O IP Phone/Collaboration Endpoint está oferecendo um codec de áudio diferente de G.711, G.722 ou AAC-LD. O Hybrid Call Service Connect é compatível com três codecs de áudio diferentes: G.711, G.722 e AAC-LD. Para estabelecer uma chamada com êxito no ambiente do Cisco Webex, um desses codecs de áudio deve ser usado. O ambiente no local pode ser configurado para usar diversos tipos de codecs de áudio, mas, ao mesmo tempo, ele pode ser configurado para restringi-los. Isso pode acontecer intencionalmente ou não usando-se configurações de região personalizadas e/ou padrão no Unified CM. Nesse comportamento específico, os padrões de log podem ser diferentes com base na direção da chamada se o Unified CM tiver sido configurado para usar oferta antecipada ou atrasada. A seguir encontram-se exemplos de algumas situações diferentes nas quais esse comportamento pode aparecer:

1. O Cisco Webex envia um CONVITE c/ SDP de entrada que oferece G.711, G.722 ou AAC-LD. O Expressway-C envia essa mensagem para o Unified CM, mas o Unified CM está configurado para permitir apenas G.729 nesta chamada. Sendo assim, o Unified CM rejeitará a chamada, pois não há codec disponível.
2. O Unified CM tenta a chamada de saída como uma *oferta antecipada para o Cisco Webex, o que significa que o CONVITE inicial enviado para o Expressway-C conterà o SDP com suporte SOMENTE ao áudio G.729*. O Cisco Webex envia um 200 OK c/SDP que zera o áudio (*m=audio 0 RTP/SAVP*) porque não é compatível com G.729. Depois que o Expressway-C passar esse CONVITE para o Unified CM, o Unified CM encerra a chamada, pois não há um codec disponível.
3. O Unified CM tenta a chamada de saída como *oferta atrasada para o Cisco Webex, o que significa que o CONVITE inicial enviado para o Expressway-C não conterà o SDP*. O Cisco Webex então envia o 200 OK c/SDP contendo todos os codecs de áudio compatíveis com o Cisco Webex. O Expressway-C envia esse 200 OK para o Unified CM, mas o Unified CM está configurado para permitir apenas G.729 nesta chamada. Sendo assim, o Unified CM rejeitará a chamada, pois não há codec disponível.

Caso esteja tentando identificar uma falha de chamada de conexão de Hybrid Call Service que corresponda a esse problema, será necessário obter os logs do Expressway além de traços SDL do Unified CM. Os trechos de log de exemplo abaixo correspondem à situação nº 2, na qual o Unified CM está tentando a chamada de saída como *oferta antecipada*. Como sabemos que a chamada está saindo do Cisco Webex, a análise de log começa no Expressway-E. Aqui está um trecho do CONVITE inicial para o Cisco Webex. Você pode ver que o codec de áudio preferencial está definido como G.729 (Payload 18). O 101 destina-se ao DTMF e, para esse cenário específico, não é relevante.

```
2017-09-19T10:46:10.488-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 14:46:10,488"
Module="network.sip" Level="DEBUG": Action="Sent" Local-ip="172.16.2.2" Local-port="25034" Dst-
ip="146.20.193.64" Dst-port="5062" Msg-Hash="4309505007645007056"
SIPMSG:
INVITE sip:pstojano-test@dmzlab.call.ciscospark.com SIP/2.0
Via: SIP/2.0/TLS 64.102.241.236:5062;egress-
zone=HybridCallServicesDNS;branch=z9hG4bK323e6b15ad0cbbf409751f67848136fa1115;proxy-call-
id=a3a78ee2-c01b-4741-b29b-55aede256d2;rport
Via: SIP/2.0/TLS 172.16.2.2:5073;branch=z9hG4bK350703fe46645f0acddef05b35adc5c157;x-cisco-local-
service=nettle;received=172.16.2.2;rport=41511;ingress-zone=DefaultZone
Via: SIP/2.0/TLS 192.168.1.6:5061;egress-
zone=DefaultZone;branch=z9hG4bKf71f2bf47233d6ca52b579364594ac6c1114.a402e3f25603f5a77b60b17ea47d
bf72;proxy-call-id=be17a470-0bca-4ad5-8a6c-14872e007efb;received=192.168.1.6;rport=25025
Via: SIP/2.0/TLS 192.168.1.5:5061;egress-
zone=HybridCallServiceTraversal;branch=z9hG4bKf4cfd09d213a88bd2331cef0bc82b540559.494a140082bd
66357134b9eed4335df8;proxy-call-id=d4d4e950-babc-45d5-a4a7-
c60a8b17a8bd;received=192.168.1.5;rport=26513;ingress-zone=HybridCallServiceTraversal
Via: SIP/2.0/TCP 192.168.1.21:5065;branch=z9hG4bK12dd82194c4f7;received=192.168.1.21;ingress-
zone=CUCM11
Call-ID: 44bdd400-9c112db1-12d95-1501a8c0@192.168.1.21
CSeq: 101 INVITE
Remote-Party-ID: "Jonathan Robb" <sip:5010@rtp.ciscotac.net>;privacy=off;screen=no;party=calling
Contact: <sip:172.16.2.2:5073;transport=tls>;video;audio
From: "Jonathan Robb"
```

```
Max-Forwards: 14
Record-Route: <sip:proxy-call-id=a3a78ee2-c01b-4741-b29b-
55aede256d2@64.102.241.236:5062;transport=tls;lr>
Record-Route: <sip:proxy-call-id=a3a78ee2-c01b-4741-b29b-
55aede256d2@172.16.2.2:5061;transport=tls;lr>
Allow: INVITE,ACK,BYE,CANCEL,INFO,OPTIONS,REFER,SUBSCRIBE,NOTIFY
User-Agent: TANDBERG/4352 (X8.10.2-b2bua-1.0)
Supported: X-cisco-srtp-fallback,replaces,timer
Session-Expires: 1800;refresher=uac
Min-SE: 500
X-TAATag: 14a0bd87-1825-4ecf-9f3d-4a23cfa69725
Session-ID: 75957d4fb66a13e835c10737aa329445;remote=00000000000000000000000000000000
Content-Type: application/sdp
Content-Length: 1407
```

```
v=0
o=tandberg 0 1 IN IP4 64.102.241.236
s=-
c=IN IP4 64.102.241.236
b=AS:384
t=0 0
m=audio 52668 RTP/SAVP 18 101 <-- CUCM is only supporting G.729 for this call
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:101 telephone-event/8000
```

a=fmtp:101 0-15
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:.....
a=crypto:2 AES_CM_128_HMAC_SHA1_80 inline:.....
UNENCRYPTED_SRTCP
a=crypto:3 AES_CM_128_HMAC_SHA1_32 inline:.....
a=crypto:4 AES_CM_128_HMAC_SHA1_32 inline:.....
UNENCRYPTED_SRTCP
a=sendrecv
a=rtcp:52669 IN IP4 64.102.241.236
m=video 52670 RTP/SAVP 126 97
b=TIAS:384000
a=rtpmap:126 H264/90000
a=fmtp:126 profile-level-id=42801e;packetization-mode=1;level-asymmetry-allowed=1
a=rtpmap:97 H264/90000
a=fmtp:97 profile-level-id=42801e;packetization-mode=0;level-asymmetry-allowed=1
a=rtcp-fb:* nack pli
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:.....
a=crypto:2 AES_CM_128_HMAC_SHA1_80 inline:.....
UNENCRYPTED_SRTCP
a=crypto:3 AES_CM_128_HMAC_SHA1_32 inline:.....
a=crypto:4 AES_CM_128_HMAC_SHA1_32 inline:.....
UNENCRYPTED_SRTCP
a=sendrecv
a=content:main
a=label:11
a=rtcp:52671 IN IP4 64.102.241.236

Em resposta a esse CONVITE inicial, o Cisco Webex responde com uma mensagem 200 OK. Se você observar esta mensagem com mais atenção, verá que o codec de áudio estava zerado. Isso é problemático, pois, sem uma porta de áudio atribuída, a chamada não poderá negociar o fluxo.

2017-09-19T10:46:27.073-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 14:46:27,072"
Module="network.sip" Level="DEBUG": Action="Received" Local-ip="172.16.2.2" Local-port="25034"
Src-ip="146.20.193.64" Src-port="5062" Msg-Hash="5236578200712291002"
SIPMSG:
SIP/2.0 200 OK
Via: SIP/2.0/TLS 64.102.241.236:5062;egress-
zone=HybridCallServicesDNS;branch=z9hG4bK323e6b15ad0cbbf409751f67848136fa1115;proxy-call-
id=a3a78ee2-c01b-4741-b29b-55aede256d2;rport=38245;received=192.168.5.26,SIP/2.0/TLS
172.16.2.2:5073;branch=z9hG4bK350703fe46645f0acdddef05b35adc5c157;x-cisco-local-
service=nettle;received=172.16.2.2;rport=41511;ingress-zone=DefaultZone,SIP/2.0/TLS
192.168.1.6:5061;egress-
zone=DefaultZone;branch=z9hG4bKf71f2bf47233d6ca52b579364594ac6c1114.a402e3f25603f5a77b60b17ea47d
bf72;proxy-call-id=be17a470-0bca-4ad5-8a6c-
14872e007efb;received=192.168.1.6;rport=25025,SIP/2.0/TLS 192.168.1.5:5061;egress-
zone=HybridCallServiceTraversal;branch=z9hG4bKf4cfd09d213a88bd2331cef0bc82b540559.494a140082bd
66357134b9eed4335df8;proxy-call-id=d4d4e950-babc-45d5-a4a7-
c60a8b17a8bd;received=192.168.1.5;rport=26513;ingress-
zone=HybridCallServiceTraversal,SIP/2.0/TCP
192.168.1.21:5065;branch=z9hG4bK12dd82194c4f7;received=192.168.1.21;ingress-zone=CUCM11
Call-ID: 44bdd400-9c112db1-12d95-1501a8c0@192.168.1.21
CSeq: 101 INVITE
Contact: "l2sip-UA" <sip:l2sip-UA@l2sip-cfa-01.wbx2.com:5062;transport=tls>
From: "Jonathan Robb"

Record-Route: <sip:l2sip-cfa-01.wbx2.com:5062;transport=tls;lr>, <sip:proxy-call-id=a3a78ee2-
c01b-4741-b29b-55aede256d2@64.102.241.236:5062;transport=tls;lr>, <sip:proxy-call-id=a3a78ee2-
c01b-4741-b29b-55aede256d2@172.16.2.2:5061;transport=tls;lr>
Allow: INVITE,ACK,CANCEL,BYE,REFER,INFO,OPTIONS,NOTIFY,SUBSCRIBE
User-Agent: Cisco-L2SIP
Supported: replaces

```

Accept: application/sdp
Allow-Events: kpml
Session-ID: ed35426ed3ade6fdc3b058792333df2b;remote=75957d4fb66a13e835c10737aa329445
Locus: 4711a33f-9d49-11e7-9bf6-dea12d0f2127
Locus-Type: CALL
Content-Type: application/sdp
Content-Length: 503

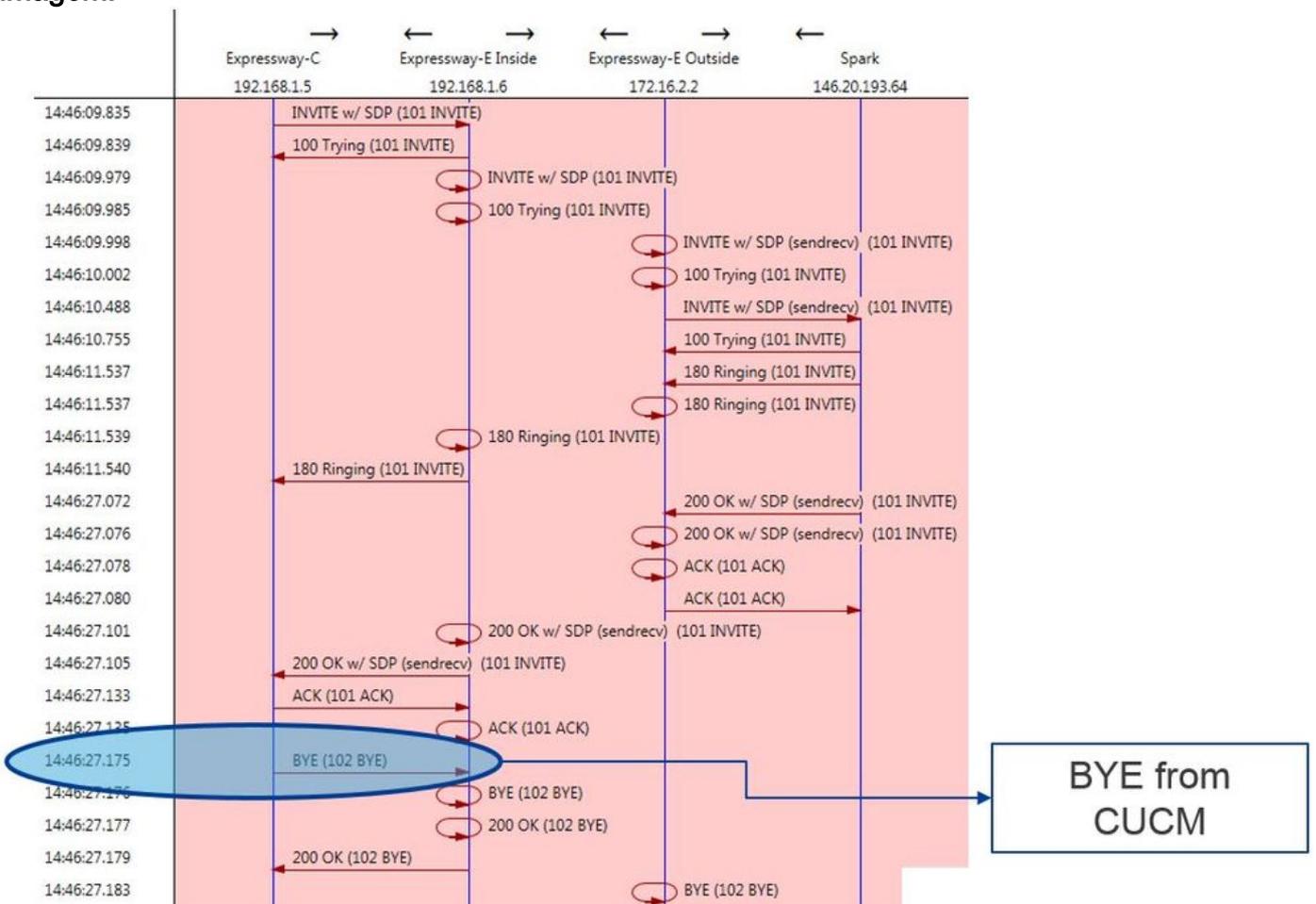
```

```

v=0
o=linus 0 1 IN IP4 146.20.193.109
s=-
c=IN IP4 146.20.193.109
b=TIAS:384000
t=0 0
m=audio 0 RTP/SAVP *      <-- Webex is zeroing this port out
m=video 33512 RTP/SAVP 108
c=IN IP4 146.20.193.109
b=TIAS:384000
a=content:main
a=sendrecv
a=rtpmap:108 H264/90000
a=fmtp:108 profile-level-id=42001E;packetization-mode=1;max-mbps=40500;max-fs=1620;max-fps=3000;max-br=10000;max-dpb=3037;level-asymmetry-allowed=1
a=rtcp-fb:* nack pli
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:.....
a=label:200

```

Você agora pode usar o TradutorX para analisar o restante do diálogo. Você pode ver que a caixa de diálogo em si é preenchida por um ACK. O problema ocorre imediatamente após a conclusão do diálogo, há um BYE que vem da direção do Expressway-C, como mostrado na imagem.



Aqui está um exemplo detalhado da mensagem BYE. Você pode ver claramente que o Agente do usuário é Cisco-CUCM11.5, que significa que a mensagem foi gerada pelo Unified CM. Outro

item a apontar é que o código de razão está definido como cause=47. A conversão comum disso é Nenhum recurso disponível.

```
2017-09-19T10:46:27.175-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 14:46:27,175"
Module="network.sip" Level="DEBUG": Action="Received" Local-ip="192.168.1.6" Local-port="7003"
Src-ip="192.168.1.5" Src-port="26513" Msg-Hash="237943800593485079"
SIPMSG:
BYE sip:192.168.1.6:5071;transport=tls SIP/2.0
Via: SIP/2.0/TLS 192.168.1.5:5061;egress-
zone=HybridCallServiceTraversal;branch=z9hG4bK90a666b3461356f8cd605cec91e4538240575.494a140082bd
66357134b9eed4335df8;proxy-call-id=d4d4e950-babc-45d5-a4a7-c60a8b17a8bd;rport
Via: SIP/2.0/TCP 192.168.1.21:5065;branch=z9hG4bK12ddd10269d39;received=192.168.1.21;ingress-
zone=CUCM11
Call-ID: 44bdd400-9c112db1-12d95-1501a8c0@192.168.1.21
CSeq: 102 BYE
From: "Jonathan Robb" <sip:5010@rtp.ciscotac.net>;tag=329447~c9cc7ddc-9592-49e8-a13c-
79e26f48eebc-30106833
To: <sip:pstojano-test@dmzlab.call.ciscospark.com>;tag=f3734601fb0eb541
Max-Forwards: 69
Route: <sip:proxy-call-id=be17a470-0bca-4ad5-8a6c-
14872e007efb@192.168.1.6:7003;transport=tls;lr>, <sip:proxy-call-id=be17a470-0bca-4ad5-8a6c-
14872e007efb@192.168.1.6:5061;transport=tls;lr>
User-Agent: Cisco-CUCM11.5
Date: Tue, 19 Sep 2017 14:46:09 GMT
X-TAA:Tag: 14a0bd87-1825-4ecf-9f3d-4a23cfa69725
Reason: Q.850 ;cause=47
Session-ID: 75957d4fb66a13e835c10737aa329445;remote=ed35426ed3ade6fdc3b058792333df2b
Content-Length: 0
```

Como o componente do Cisco Webex zerou o codec de áudio nessa amostra de chamada, o foco deve ficar no:a. CONVITE inicial que foi enviado para o Cisco Webex eb. qual foi a lógica usada pelo Cisco Webex para zerar a porta.Agora, observando o que é exclusivo sobre o CONVITE inicial, o que podemos notar é que ele contém apenas G.729. Sabendo disso, analise o Guia de implantação do Cisco Webex Hybrid Call Service e revise especificamente o capítulo Preparação do ambiente, no qual a etapa 5 da [seção Complete os pré-requisitos do Hybrid Call Service Connect mostrando os codecs específicos compatíveis](#). Então veríamos isto:O Cisco Webex é compatível com os seguintes codecs:

- Áudio — G.711, G.722, AAC-LD
- Vídeo — H.264

Note: O Opus não é usado no segmento local da chamada para o Cisco Webex Hybrid Call. Com essas informações em mãos, é possível concluir que o Unified CM está enviando um codec de áudio não compatível, que é a razão pela qual o Cisco Webex está zerando a porta. Solução:Para lidar com essa situação específica, talvez seja necessário revisar a configuração de região entre o Cisco Webex RD que ancora a chamada no local e o Tronco SIP para o Expressway-C. Para fazer isso, determine em qual Pool de Dispositivos esses dois elementos estão. O pool de dispositivos contém os mapeamentos de regiões. Para determinar o pool de dispositivos do tronco SIP do Expressway-C:

1. Faça login no Unified CM.
2. Navegue até Dispositivo > Tronco.
3. Procure o nome do tronco ou clique em Localizar.
4. Selecione o tronco do Expressway-C.
5. Registre o nome do pool de dispositivos.

Para determinar o pool de dispositivos do CTI-RD ou do Cisco Webex-RD que ancorou a chamada:

1. Navegue até Dispositivo > Telefone.
2. Ao pesquisar, você pode selecionar Tipo de dispositivo que contém Webex ou dispositivo remoto CTI (dependendo do que o cliente está usando).

3. Registre o nome do pool de dispositivos.

Determine a região conectada a cada pool de dispositivos:

1. Navegue até System > Device Pool.
2. Procure pelo pool de dispositivos usado para o tronco SIP do Expressway-C.
3. Clique em Device Pool.
4. Registre o nome da região.
5. Procure pelo pool de dispositivos usado no Webex-RD ou CTI-RD.
6. Clique em Device Pool.
7. Registre o nome da região.

Determine o relacionamento regional:

1. Navegue até Sistema > Informações de região > Região.
2. Pesquisa em uma das regiões identificadas.
3. Determine se há uma relação de região entre as duas regiões que estão usando G.729.

Nesse momento, se você identificar o relacionamento que está usando G.729, você precisará ajustar o relacionamento para comportar os codecs de áudio compatíveis que o Cisco Webex usa ou usar um pool de recursos diferente que tenha uma região que comporte isso. No cenário documentado acima, determinamos o seguinte: Região do tronco do Expressway-C: Reserva de largura de banda Região Webex-RD: Dispositivos RTP Aqui está uma ilustração gráfica da relação entre as regiões RTP-Devices e ReservingBandwidth, como mostrado na imagem.

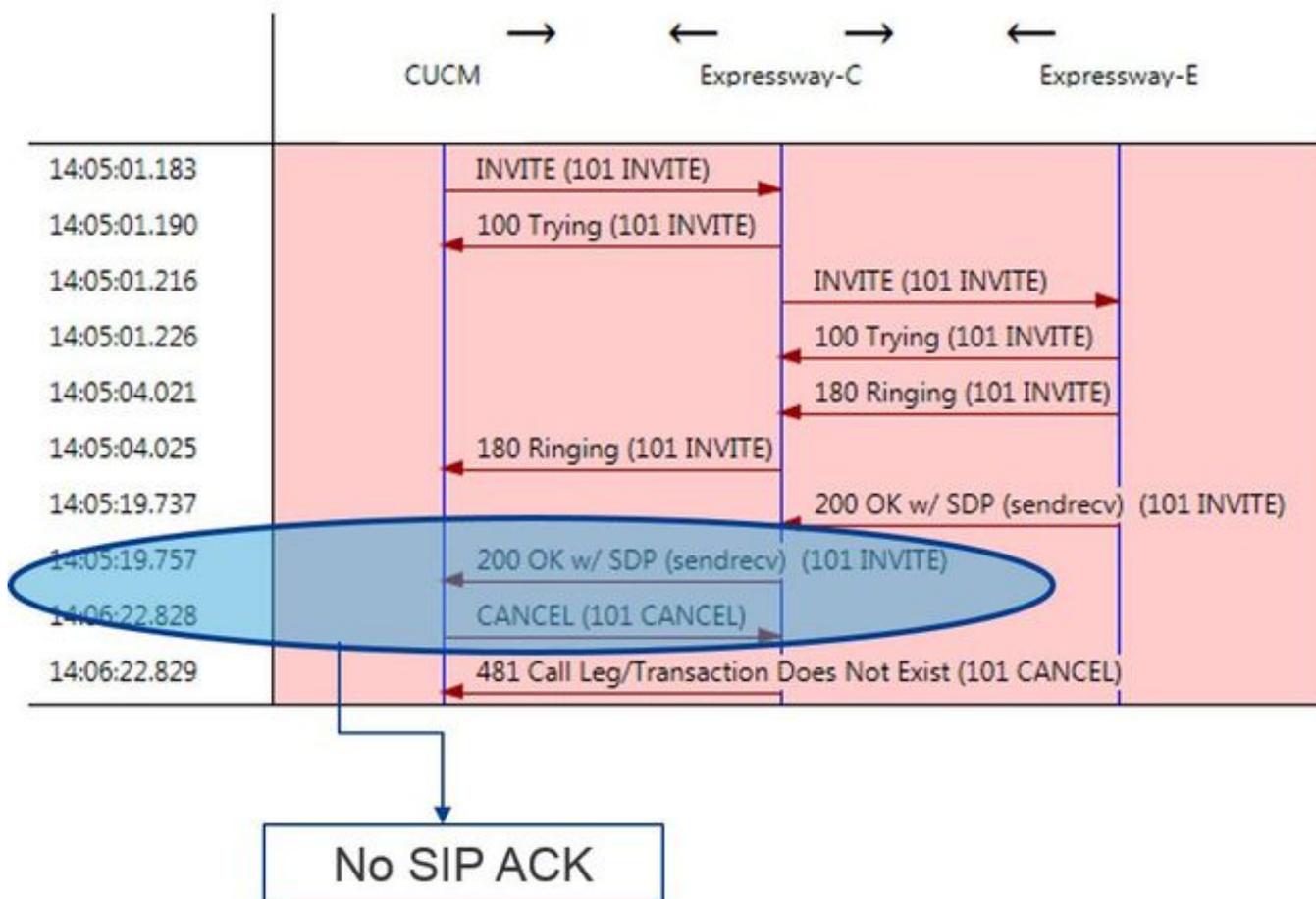
| Region | Audio Codec Preference List | Maximum Audio Bit Rate | Maximum Session Bit Rate for Video Calls | Maximum Session Bit Rate for Immersive Video Calls |
|--------------------|---|------------------------|--|--|
| Default | Use System Default (Factory Default low loss) | 256 kbps (L16, AAC-LD) | 32000 kbps | 32000 kbps |
| ReservingBandwidth | Use System Default (Factory Default low loss) | 8 kbps (G.729) | 384 kbps | 384 kbps |
| RTP-Devices | Use System Default (Factory Default low loss) | 256 kbps (L16, AAC-LD) | 32000 kbps | 32000 kbps |
| RTP-Infrastructure | Use System Default (Factory Default low loss) | 256 kbps (L16, AAC-LD) | 32000 kbps | 32000 kbps |

G.729 Not Supported by Spark

Ao alterar o pool de recursos em que estava o tronco do Expressway-C, você altera o relacionamento da região. O novo pool de recursos tem uma região definida como infraestrutura RTP portanto, o novo relacionamento de região entre o Cisco Webex-RD e o tronco Expressway-C era dispositivos RTP e infraestrutura RTP. Como mostrado na figura, você pode ver que essa relação suporta AAC-LD, que é um dos codecs de áudio suportados pelo Cisco Webex e, portanto, a chamada será configurada corretamente. Problema 2. Tamanho máximo de mensagem de entrada do Unified CM excedido Como o vídeo se tornou mais predominante na empresa, o tamanho das mensagens de SIP que contêm o SDP cresceu substancialmente. Os servidores que processam essas mensagens devem ser configurados de forma que possam aceitar um pacote grande. Em vários servidores de controle de chamada, não há problema em usar os valores padrão. No Cisco Unified Communications Manager (Unified CM), havia problemas com os valores padrão para lidar com uma grande mensagem SIP que continham SDP nas versões anteriores. Em versões posteriores do Unified CM, o tamanho do valor permitido para uma mensagem SIP foi aumentado, no entanto, esse valor é definido somente em novas instalações, não em atualizações. Dessa forma, os clientes que estão atualizando suas versões mais antigas do Unified CM para oferecer suporte ao Hybrid Call Service Connect podem ser afetados pelo tamanho máximo da mensagem de entrada no Unified CM ser muito baixo. Caso esteja tentando identificar uma falha de chamada de conexão de Hybrid Call Service que corresponda a esse problema, será necessário obter os logs do Expressway além de traços SDL do Unified CM. Para identificar a falha, primeiro, entenda o que acontece e, em seguida, os tipos de cenários em que a falha pode ocorrer. Para responder à pergunta sobre o que acontece, você deve saber que quando o Unified CM recebe uma mensagem SIP muito grande, ele simplesmente fecha o soquete TCP e não responde ao Expressway-C. Com isso, há diversas situações nas quais isso pode acontecer:

1. O Cisco Webex envia um CONVITE de entrada c/SDP que é grande demais. O Expressway-C passa isso para o Unified CM e o Unified CM fecha o soquete TCP e a caixa de diálogo SIP vai atingir o tempo limite.
2. O Unified CM tenta a chamada de saída como oferta antecipada para o Webex, o que significa que o CONVITE inicial enviado para o Expressway-C vai conter o SDP. O Cisco Webex então envia um 200 OK c/SDP em resposta e a resposta 200 OK quando passada do Expressway-C para o Unified CM é grande demais. O Unified CM fecha o soquete TCP e a caixa de diálogo SIP expira.
3. O Unified CM tenta a chamada de saída como oferta atrasada para o Webex, o que significa que o CONVITE inicial enviado para o Expressway-C não conterá o SDP. O Cisco Webex então envia um 200 OK c/SDP e a oferta 200 OK quando passada do Expressway-C para o Unified CM é grande demais. O Unified CM fecha o soquete TCP e a caixa de diálogo SIP expira.

Examinar os logs do Expressway-C nessa condição específica o ajuda a entender o fluxo de mensagens. Se você usasse um programa como [TranslatorX](#), você poderia ver que o Expressway-C está passando o Cisco Webex 200 OK c/ SDP para o Unified CM. O desafio é que o Unified CM nunca responde com um ACK de SIP como mostrado na imagem.



Como o Unified CM é a parte responsável por não responder, vale a pena revisar os rastreamentos SDL para ver como o Unified CM está lidando com essa condição. O que você encontraria neste cenário é que o Unified CM ignora a mensagem grande do Expressway-C. Um item de linha como este será impresso.

CUCM Traces

```
53138762.000 |09:05:19.762 |AppInfo |SIPSocketProtocol(5,100,14,707326)::handleReadComplete
send SdlReadRsp: size 5000
```

```

53138763.000 |09:05:19.762 |SdlSig |SdlReadRsp |wait
|SIPTcp(5,100,71,1) |SdlTCPConnection(5,100,14,707326)
|5,100,14,707326.4^10.36.100.140^^ |*TraceFlagOverrode
53138763.001 |09:05:19.762 |AppInfo |SIPTcp - SdlRead bufferLen=5000
53138763.002 |09:05:19.762 |AppInfo |//SIP/Stack/Error/0x0/httpish_cache_header_val: DROPPING
unregistered header Locus: c904ecb1-d286-11e6-bfdf-b60ed914549d
53138763.003 |09:05:19.762 |AppInfo |//SIP/Stack/Info/0x0/httpish_msg_process_network_msg:
Content Length 4068, Bytes Remaining 3804
53138763.004 |09:05:19.762 |AppInfo |//SIP/Stack/Info/0x0/ccsip_process_network_message:
process_network_msg: not complete
53138763.005 |09:05:19.762 |AppInfo |SIPTcp - Ignoring large message from %Expressway-
C_IP%:[5060]. Only allow up to 5000 bytes. Resetting connection.

```

Depois que a caixa de diálogo SIP expirar, o Cisco Webex enviará uma mensagem Inbound SIP 603 Decline para o Expressway-E, conforme observado na amostra de log.

Expressway-E Traces

```

2017-01-04T09:05:40.645-05:00 vcs-expressway tvcs: UTCTime="2017-01-04 14:05:40,645"
Module="network.sip" Level="DEBUG": Action="Received" Local-ip="%Exp-E%" Local-port="25150" Src-
ip="%Webex_IP%" Src-port="5062" Msg-Hash="2483073756671246315" SIPMSG: SIP/2.0 603 Decline

```

Como mencionado, há três cenários diferentes nos quais você pode ver esse comportamento. Para fins de clareza, as amostras de log fornecidas nesta ilustração correspondeu à situação 3 na qual a chamada foi enviada para o Cisco Webex como uma oferta atrasada. Solução:

1. Faça login no Unified CM.
2. Navegue até System > Service Parameters.
3. Selecione o servidor que está executando o serviço Call Manager.
4. Escolha o serviço Cisco Call Manager quando solicitado para uma seleção de Serviço.
5. Selecione a opção Avançado.
6. Em Configurações de parâmetro geral de cluster (dispositivo - SIP), altere o Tamanho máximo da mensagem de entrada SIP para 18000.
7. Selecione Salvar.
8. Repita esse processo para cada nó do Unified CM que está executando o serviço Cisco Call Manager.

Note: Para que um telefone IP, endpoint de colaboração e/ou tronco de SIP para aproveitar essa configuração, ela precisa ser reiniciada. Esses dispositivos podem ser reiniciados individualmente para minimizar o impacto no ambiente. NÃO reinicie todos os dispositivos no CUCM, a menos

que você saiba que é absolutamente aceitável fazer isso.

Appendix Ferramentas de identificação e solução de problemas do Expressway

Utilitário de verificação de padrão O Expressway tem um utilitário de verificação de padrões que é útil quando você deseja testar se um padrão corresponde a um determinado alias e se é transformado da maneira esperada. O utilitário pode ser encontrado no Expressway na opção de menu Manutenção > Ferramentas > Padrão de verificação. Mais comumente, isso é usado se você quiser testar se seu regex de regra de pesquisa vai corresponder corretamente um alias a uma string de padrão e, opcionalmente, executar a manipulação bem-sucedida da string. No Hybrid Call Service Connect, também é possível testar se o FQDN do cluster do Unified CM vai corresponder à string de padrão configurada para o FQDN do cluster do Unified CM. Ao usar este utilitário, lembre-se de que a chamada será roteada com base no parâmetro de FQDN do cluster do Unified CM listado no cabeçalho da rota, não na URI de destino. Por exemplo, se o convite a seguir chegar no Expressway, teste a funcionalidade de padrão de verificação em relação a cucm.rtp.ciscotac.net, não a jorobb@rtp.ciscotac.net.

```

SIPMSG:
|INVITE sip:jorobb@rtp.ciscotac.net SIP/2.0
Via: SIP/2.0/TLS 192.168.1.6:7003;egress-
zone=HybridCallServiceTraversal;branch=z9hG4bKcac6d95278590991a2b516cf57e75827371;proxy-call-
id=abcba873-eaae-4d64-83b4-c4541d4e620c;rport
Via: SIP/2.0/TLS 192.168.1.6:5073;branch=z9hG4bK837b03f2cd91b6b19be4fc58edb251bf12;x-cisco-
local-service=nettle;received=192.168.1.6;rport=41913;ingress-zone=DefaultZone

```

```
Via: SIP/2.0/TLS 64.102.241.236:5061;egress-  
zone=DefaultZone;branch=z9hG4bK524f89592d00ffc45b7b53000271676c370.88b5177ac4d7cfcae1eb8f8be78da  
055;proxy-call-id=2db939b2-a49b-4307-8d96-23716a2c090b;received=172.16.2.2;rport=25010  
Via: SIP/2.0/TLS  
192.168.4.150:5062;branch=z9hG4bK92f9ef952712e6610c3e6b72770c1230;received=148.62.40.63;rport=39  
986;ingress-zone=HybridCallServicesDNS  
Via: SIP/2.0/TLS 127.0.0.1:5070;branch=z9hG4bK-313634-  
3d27a6f914badee6420287903c9c6a45;rport=45939  
Call-ID: 3e613afb185751cdf019b056285eb574@127.0.0.1  
CSeq: 1 INVITE  
Contact: <sip:192.168.1.6:5073;transport=tls>  
From: "pstoiano test" <sip:pstoiano-test@dmzlab.call.ciscospark.com>;tag=145765215  
To: <sip:jorobb@rtp.ciscotac.net>  
Max-Forwards: 15  
Route:
```

Para usar o padrão de verificação para testar o roteamento da regra de pesquisa do cabeçalho do Hybrid Call Service Connect Route, siga estas etapas:

1. Navegue até Manutenção > Ferramentas > Verificar padrão.
2. Para o Alias, insira o FQDN do cluster do Unified CM.
3. Defina o Tipo de Padrão como Prefixo.
4. Defina a string de padrão como FQDN do cluster do Unified CM.
5. Defina o comportamento do padrão como Leave.
6. Selecione Verificar padrão.

Se as regras de pesquisa no Expressway estiverem configuradas corretamente, é possível esperar ver os resultados retornarem uma mensagem de êxito. Aqui está um exemplo de um teste de padrão de verificação bem-sucedido como mostrado na imagem.

Check pattern

Alias:

Pattern type:

Pattern string:

Pattern behavior:

Result

| | |
|---------|-----------------------|
| Result | Succeeded |
| Details | Alias matched pattern |
| Alias | cucm.rtp.ciscotac.net |

Isso é bem-sucedido porque esse Alias (cucm.rtp.ciscotac.net) corresponde à string do padrão de prefixo de (cucm.rtp.ciscotac.net). Para entender como uma chamada é roteada com base nesses resultados, você pode usar o Utilitário de localização do Expressway descrito. Localize o utilitário de localização do Expressway é útil se você deseja testar se o Expressway consegue rotear uma chamada para uma determinada zona com base em um determinado alias. Tudo isso pode ser concluído sem precisar fazer uma chamada real. O utilitário de localização pode ser encontrado no Expressway no menu Manutenção > Ferramentas > Localizar. Você verá algumas

instruções sobre como usar a funcionalidade Localizar no Expressway-C para determinar se o servidor pode rotear uma chamada com base no FQDN do cluster do Unified CM encontrado no cabeçalho da Rota SIP.

1. Navegue até Manutenção > Ferramentas > Localizar.
2. Insira o FQDN do cluster do Unified CM no campo Alias.
3. Selecione SIP como o Protocolo.
4. Selecione sua zona cliente de passagem do Cisco Webex Hybrid para a origem.
5. Selecione Localizar.

Na parte inferior da interface, você agora verá os resultados da pesquisa. Aqui está um exemplo do teste de exemplo que foi executado com os resultados correspondentes, como mostrado na imagem.

The screenshot shows the 'Locate' interface with the following fields and values:

- Alias: cucm.rtp.ciscotac.net
- Hop count: 5
- Protocol: SIP
- Source: Hybrid Call Service Traversal
- Authenticated: Yes
- Source alias: (empty)

Aqui estão os resultados da Localização. Os valores de interesse são negados. Esses resultados mostram:

- O fato de que o alias não pôde ser roteado (verdadeiro)
- Informações de origem (nome/tipo da zona)
- Informações de destino (alias sendo roteado)
- A regra de pesquisa sendo correspondida (roteamento de entrada do serviço Hybrid Call)
- A zona para a qual a chamada seria enviada (CUCM11)

```
Search (1)
State: Completed
Found: True
Type: SIP (OPTIONS)
SIPVariant: Standards-based
CallRouted: True
CallSerial Number: ae73fb64-c305-457a-b7b3-59ea9688c630
Tag: 473a5b19-9a37-40bf-bbee-6f7bc94e7c77
Source (1)
Authenticated: True
Aliases (1)
Alias (1)
Type: Url
Origin: Unknown
Value: xcom-locate
Zone (1)
Name: Hybrid Call Service Traversal
Type: TraversalClient
Path (1)
Hop (1)
Address: 127.0.0.1
Destination (1)
Alias (1)
Type: Url
Origin: Unknown
```

Value: sip:cucm.rtp.ciscotac.net
StartTime: 2017-09-24 09:51:18
Duration: 0.01
SubSearch (1)
Type: Transforms
Action: Not Transformed
ResultAlias (1)
Type: Url
Origin: Unknown
Value: cucm.rtp.ciscotac.net
SubSearch (1)
Type: Admin Policy
Action: Proxy
ResultAlias (1)
Type: Url
Origin: Unknown
Value: cucm.rtp.ciscotac.net
SubSearch (1)
Type: FindMe
Action: Proxy
ResultAlias (1)
Type: Url
Origin: Unknown
Value: cucm.rtp.ciscotac.net
SubSearch (1)
Type: Search Rules
SearchRule (1)
Name: as is local
Zone (1)
Name: LocalZone
Type: Local
Protocol: SIP
Found: False
Reason: Not Found
StartTime: 2017-09-24 09:51:18
Duration: 0
Gatekeeper (1)
Address: 192.168.1.5:0
Alias (1)
Type: Url
Origin: Unknown
Value: cucm.rtp.ciscotac.net
Zone (2)
Name: LocalZone
Type: Local
Protocol: H323
Found: False
Reason: Not Found
StartTime: 2017-09-24 09:51:18
Duration: 0
Gatekeeper (1)
Address: 192.168.1.5:0
Alias (1)
Type: Url
Origin: Unknown
Value: cucm.rtp.ciscotac.net
SearchRule (2)
Name: Hybrid Call Service Inbound Routing
Zone (1)
Name: CUCM11
Type: Neighbor
Protocol: SIP
Found: True
StartTime: 2017-09-24 09:51:18

Duration: 0
Gatekeeper (1)
Address: 192.168.1.21:5065
Alias (1)
Type: Url
Origin: Unknown
Value: cucm.rtp.ciscotac.net

Registro de diagnóstico Sempre que estiver solucionando problemas de chamada ou de mídia de uma chamada que passa pela solução Expressway será preciso usar o log de diagnóstico. Esse recurso do Expressway oferece aos engenheiros informações detalhadas de todas as decisões de lógica pelas quais o Expressway está passando conforme a chamada passa. Você poderá ver o corpo completo das mensagens de SIP, como o Expressway passa a chamada e como o Expressway define os canais de mídia. O log de diagnóstico tem diversos módulos diferentes que o alimentam. Os níveis de log podem ser ajustados para mostrar FATAL, ERROR, WARN, INFO, DEBUG, TRACE. Por padrão, tudo está definido como INFO, que captura quase tudo o que você precisa para diagnosticar um problema. De tempos em tempos, poderá ser necessário ajustar um nível de log de um determinado módulo de INFO para DEBUG para obter um melhor entendimento do que está acontecendo. As etapas abaixo mostram como é possível ajustar os níveis de log do módulo developer.ssl que é responsável por oferecer informações para handshakes TLS (mútuos).

1. Faça login no servidor Expressway (Deve ser feito no Expressway-E e C).
2. Navegue até Manutenção > Diagnóstico > Avançado > Configuração do Log de Suporte.
3. Role até o módulo que gostaria de ajustar nessa instância developer.ssl e clique nele.
4. Ao lado do parâmetro Nível, escolha DEBUG no menu.
5. Click Save.

Nesse momento você estará preparado para obter o log de diagnóstico:

1. Faça login no servidor Expressway (deve ser feito no Expressway-E e C).
2. Navegue até Manutenção > Diagnóstico > Log de diagnóstico.
3. Clique em Start New Log (Certifique-se de marcar a opção tcpdump).
4. Reproduza o problema.
5. Clique em Parar registro.
6. Clique em Download Log.

No log de diagnóstico do Expressway, tenha em mente que você poderia começar o log do Expressway-C e do Expressway-E em paralelo: primeiro, inicie o registro no Expressway-E, em seguida, vá até Expressway-C e inicie-o. Nesse ponto, é possível reproduzir o problema. Note: Atualmente, o pacote de log de diagnóstico do Expressway/VCS não contém informações sobre o certificado do Expressway Server ou a lista de CAs confiáveis. Se tiver um caso no qual ter essa

funcionalidade seja útil, anexe seu caso a [este defeito](#). **Informações Relacionadas**

- [Guia de implantação dos serviços Cisco Webex Hybrid Call](#)
- [Guia de design do Cisco Webex Hybrid](#)
- [Guia do administrador do Cisco Expressway](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.