Guía de solución de problemas para Cisco Webex Hybrid Call Service Connect

Contenido

Introducción

Este documento describe la solución Hybrid Call Service Connect de Cisco Webex, que permite que la infraestructura existente de control de llamadas de Cisco se conecte a Cisco Collaboration Cloud para que puedan funcionar juntos.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimientos sobre la oferta de Cisco Webex
- Conocimientos sobre la solución de Expressway (B2B)
- Conocimientos sobre Cisco Unified Communications Manager (Unified CM) y su integración con Expressway
- Unified CM 10.5 (2) SU5 o posterior.
- Expressway (B2B) versión X8.7.1 o posterior (se recomienda X8.9.1)
- Expressway (host de conector): consulte Soporte de host de conector de Expressway para los servicios híbridos de Cisco Webex para las versiones compatibles actualmente

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco Unified Communications Manager
- Expressway
- Webex para Windows
- Webexfor Mac
- Webexfor iOS
- Webex para Android
- Terminales de colaboración de Cisco
- Terminales de escritorio de colaboración
- Teléfonos 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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

La solución ofrece estas funciones:

- Utilice la aplicación Webex como cliente de software móvil para llamadas de audio y vídeo
- Use la aplicación para hacer y recibir llamadas desde cualquier lugar, tal y como si estuviera

en la oficina
- Utilice Webex, Cisco Jabber o su teléfono de escritorio para llamar, sin tener que preocuparse por la opción que utilicen
- Desbloquee el historial de llamadas en los teléfonos de las instalaciones e integre dicho historial en Webex

Esta guía cubre los problemas exclusivos de Hybrid Call Service Connect. Dado que Hybrid Call Service Connect se ejecuta en el mismo par de Expressway E & C que otras soluciones como el acceso móvil y remoto y las llamadas de empresa a empresa, los problemas con las otras soluciones pueden afectar a Hybrid Call Service Connect. Los clientes y partners que implementan un par de Expressway para su uso con Call Service Connect deben consultar la guía de configuración básica de VCS Expressway y VCS Control de Cisco antes de intentar implementar Hybrid Call Service Connect. Esta guía de resolución de problemas trata las consideraciones de firewall/NAT junto con el diseño de Expressway en los Apéndice 3 y 4. Revise detenidamente esta documentación. Además, en este documento se supone que ya se realizó la activación del host de conector de Expressway y de Hybrid Call Service.

Problemas de configuración de llamada

Errores de intercambio mutuo de señales TLS

Hybrid Call Service Connect usa la seguridad de capa de transporte mutua (TLS mutua) para la autenticación entre Cisco Webex y Expressway-E. Esto significa que Expressway-E y Cisco Webex comprueban e inspeccionan el certificado que presentan el uno al otro. Dado que los problemas mutuos de TLS son tan frecuentes durante las nuevas implementaciones de los servidores de Expressway y la habilitación de soluciones como Hybrid Call Service Connect, esta sección proporciona información útil y consejos para resolver problemas basados en certificados entre Expressway y Cisco Webex.

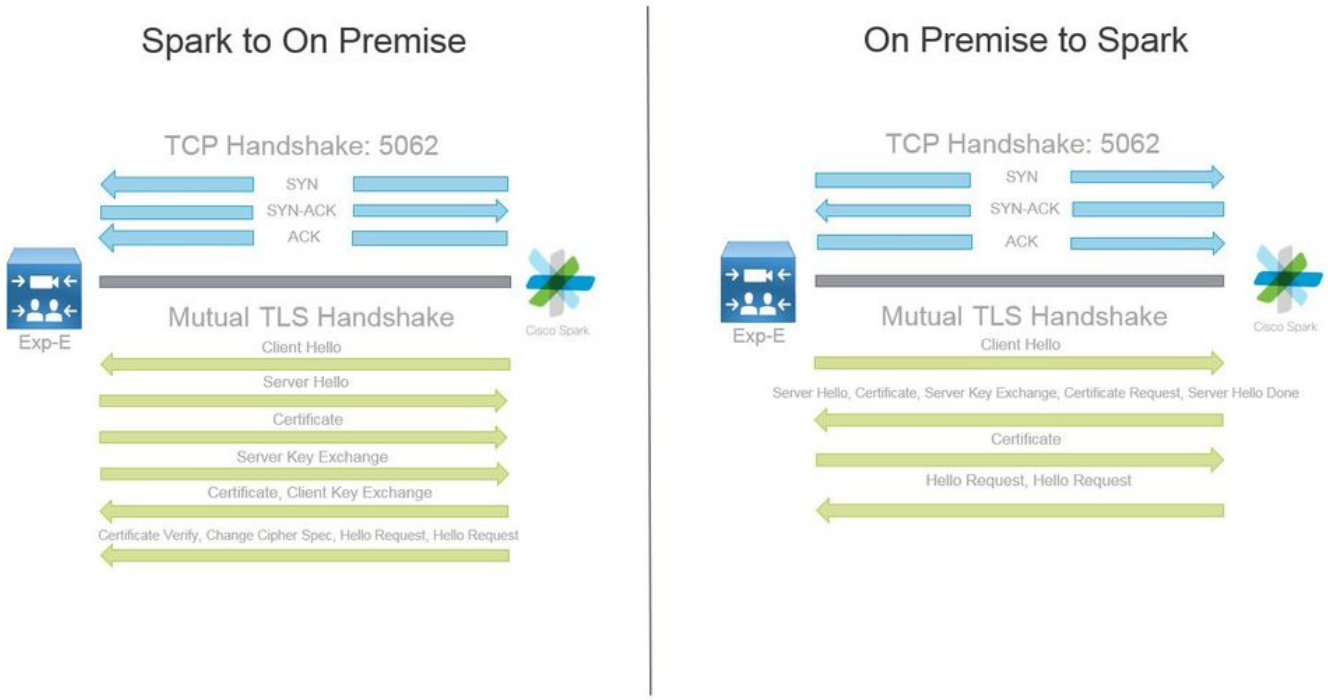
¿Qué comprueba Expressway-E?

- ¿El certificado de Cisco Webex estaba firmado por una CA pública que aparece en la lista de CA de confianza de Expressway-E?
- ¿callservice.ciscospark.com está presente en el campo Nombre alternativo del asunto del certificado de Cisco Webex?

¿Qué comprueba Cisco Webex?

- Si el certificado de Expressway-E está firmado por una de las CA públicas de confianza de Webex? (Lista de CA de confianza de Cisco Webex)
- Si Expressway-E no usa un certificado con firma púbica, ¿el certificado de Expressway y los certificados intermedios y de raíz se cargaron en Cisco Webex Control Hub (https://admin.ciscospark.com)?

Esto se explica como se muestra en la imagen.



Consejos útiles para solucionar problemas de intercambio mutuo de señales TLS

1. Decodificación del intercambio mutuo de señales TLS

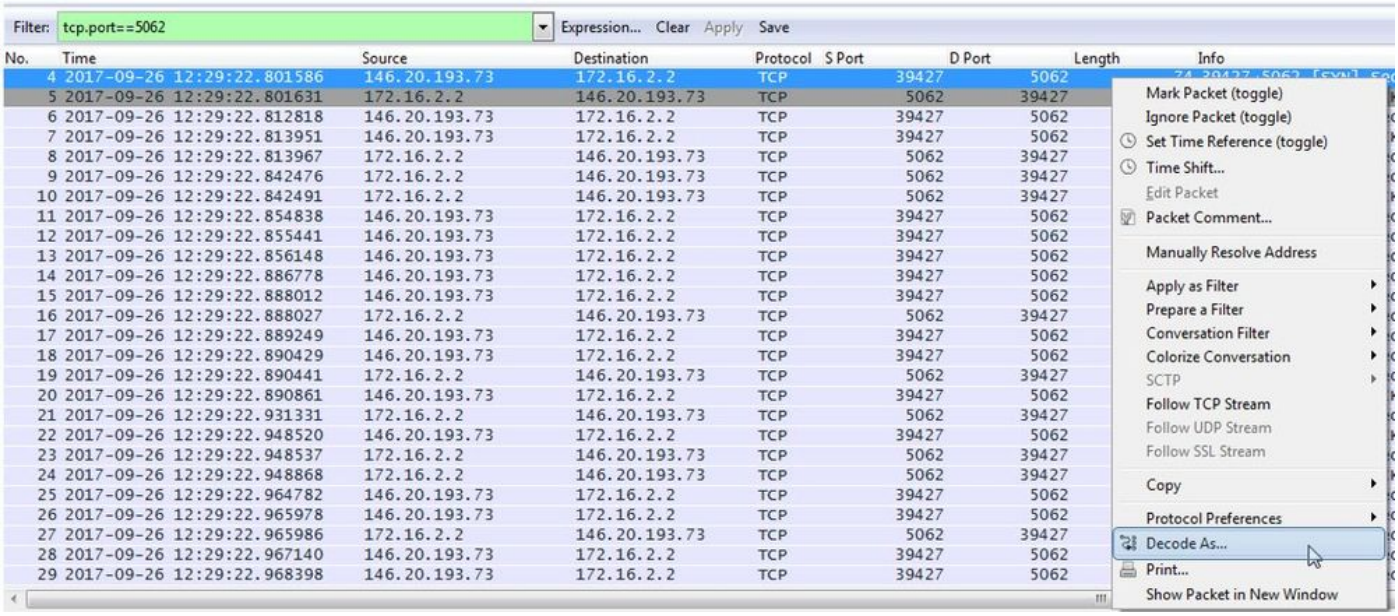
De forma predeterminada, Wireshark marca el tráfico de TLS de SIP como el puerto 5061. Esto significa que cada vez que desee analizar un intercambio de señales TLS (mutuo) que se produce en el puerto 5062, Wireshark no sabrá cómo descodificar el tráfico correctamente. Este es un ejemplo del intercambio mutuo de señales TLS que se realiza a través del puerto 5062, como se muestra en la imagen.

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

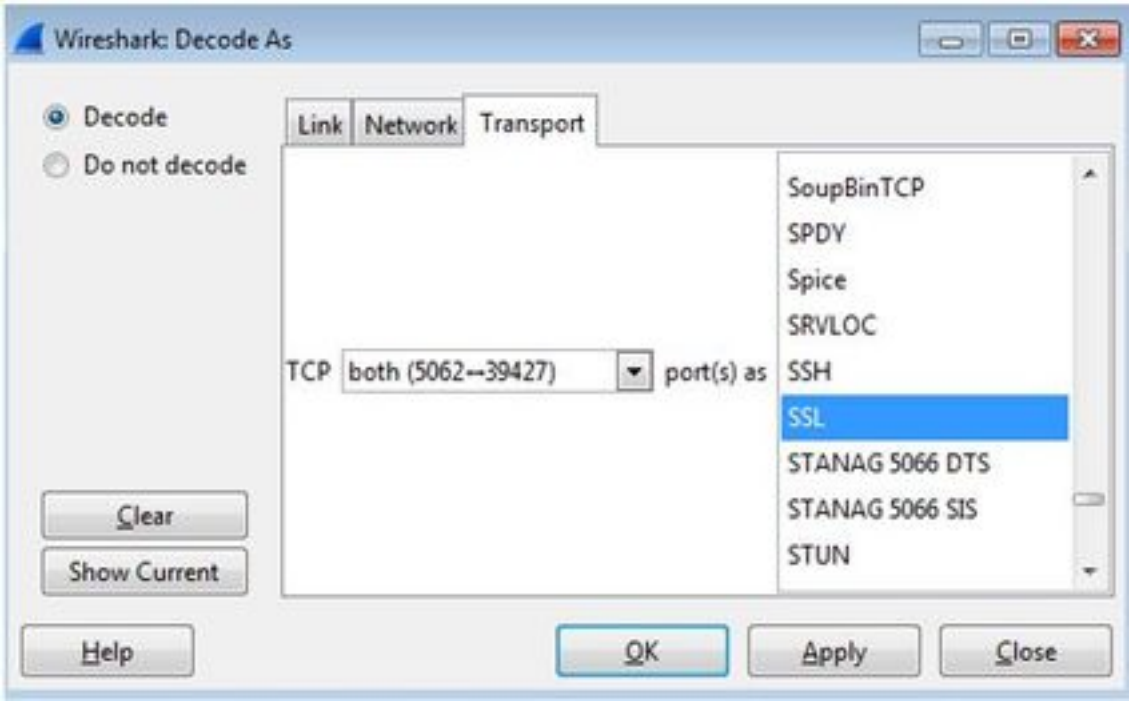
Como se puede ver, este es el aspecto del intercambio de señales con la configuración predeterminada de Wireshark. El paquete número 175 es el certificado que Expressway envía a Cisco Webex. Sin embargo, no se puede determinar eso sin decodificar el tráfico. Puede usar dos métodos para decodificar este tráfico a fin de simplificar la visualización de la información del certificado y los mensajes de error presentes.

1 bis. Decodificar la secuencia como SSL

a. Al analizar el intercambio mutuo de señales TLS, primero filtre la captura por **tcp.port==5062**. Después de esto, haga clic con el botón derecho del ratón en el primer paquete de la secuencia y seleccione **Decodificar como...** como se muestra en la imagen.



b. Una vez que el **Decode As...** Si selecciona esta opción, verá una lista en la que puede seleccionar cómo decodificar la secuencia seleccionada. En la lista, seleccione **SSL,** haga clic en **Aplicar** y cierre la ventana. En este punto, toda la secuencia muestra el certificado y los mensajes de error que se intercambiaron en el momento del intercambio de señales, como se muestra en la imagen.

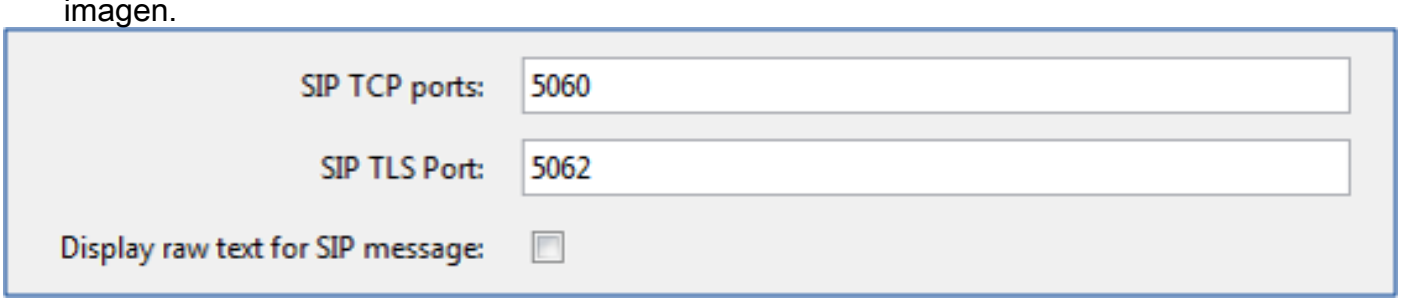


1 ter. Ajustar el puerto de TLS de SIP

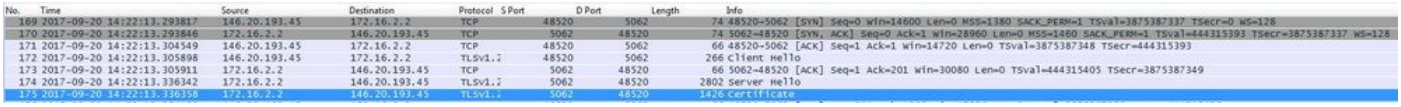
Una vez que ajuste el puerto de TLS de SIP en 5062 en las preferencias de Wireshark, podrá ver todos los detalles del intercambio de señales, incluidos los certificados. Para hacer este cambio:

- Abra Wireshark
- Vaya a **Editar > Preferencias**
- Expanda Protocolos y seleccione **SIP**
- Defina el puerto de TLS de SIP en 5062 y haga clic en **Aplicar**
- Vuelva a establecer el valor en 5061 cuando se complete el análisis, como se muestra en la

imagen.



Si analiza la misma captura ahora, verá los paquetes 169 a 175 decodificados. El paquete 175 muestra el certificado de Expressway-E y, si se explora en profundidad el paquete, podrá ver todos los detalles del certificado como se muestra en la imagen.



2. Filtro de Wireshark

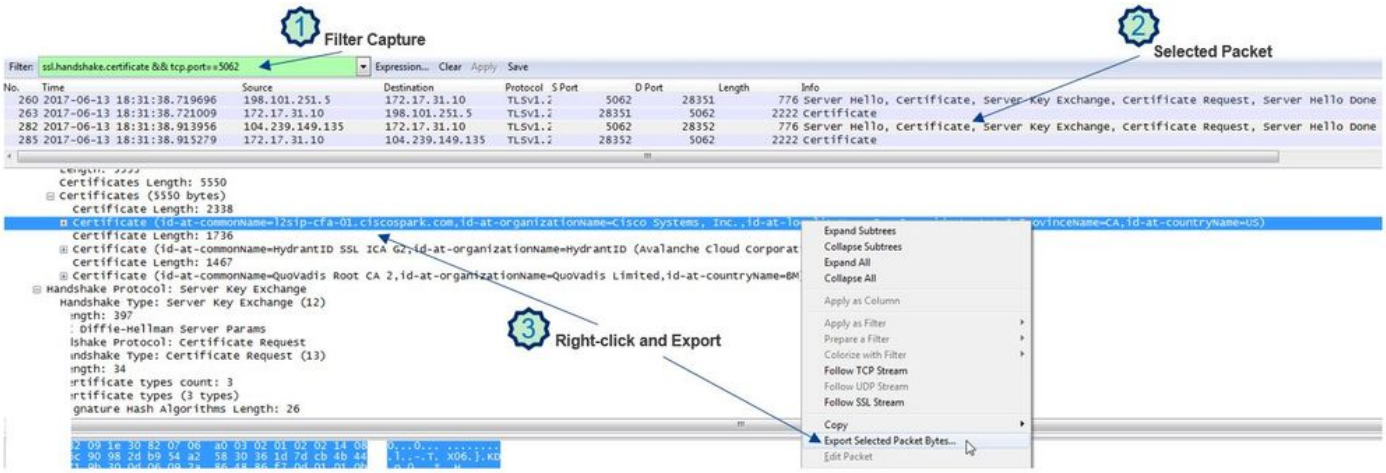
Al analizar las capturas de paquetes, es fácil perderse por la gran cantidad de paquetes que se observan en una determinada captura. Es importante tener en cuenta el tipo de tráfico que más le interesa para filtrar Wireshark a fin de que muestre eso solo. A continuación se detallan algunos filtros comunes de Wireshark que pueden usarse para obtener detalles acerca de un intercambio mutuo de señales de TLS:

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

3. Extraiga el certificado de Pcap

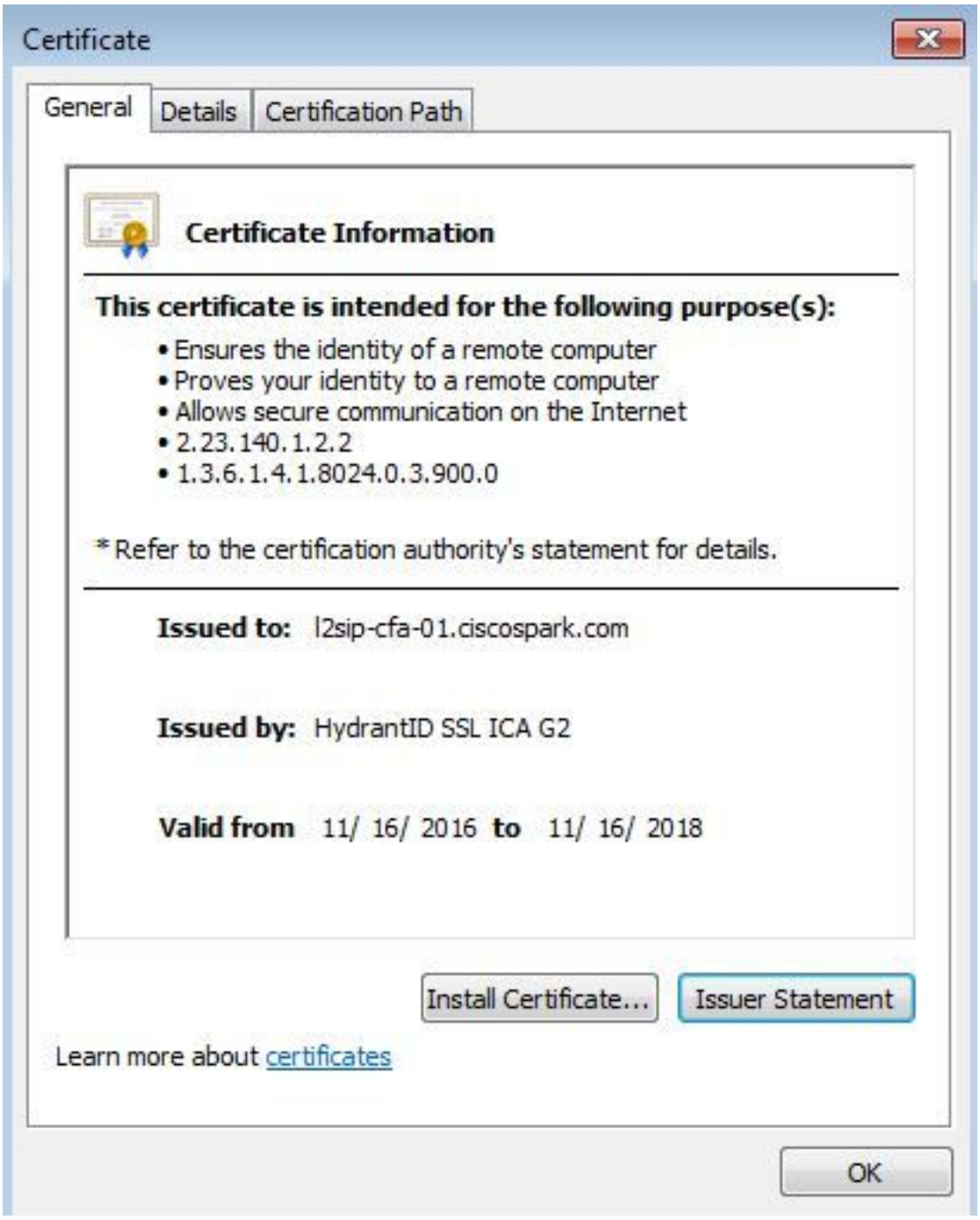
De vez en cuando, puede que necesite obtener una copia de un certificado (servidor, raíz o intermediario). Si no sabe dónde encontrar el certificado que está buscando, lo puede extraer directamente desde una captura de paquetes. Estos son los pasos para extraer el certificado de Cisco Webex que se presenta en un intercambio mutuo de señales de TLS.

1. Filtre la captura de paquetes con **ssl.handshake.certificate && tcp.port==5062**
2. Encuentre el paquete que proviene de la dirección del servidor de Webex y dice "Certificate" en la sección de información.
3. En los detalles del paquete, expanda **Secure Socket Layer > TLS Certificate > Handshake Protocol > Certificates**. **Nota:** El último certificado de la cadena es la CA de raíz.
4. Haga clic con el botón derecho del ratón en el certificado de interés y seleccione **Exportar bytes de paquete seleccionados**... como se muestra en la imagen.



5. Guarde el archivo con la extensión .cer.

6. Haga doble clic en el archivo guardado para abrir el certificado como se muestra en la imagen.



4. Ajustar los niveles de registro de Expressway

Los dos módulos de registro disponibles en Expressway pueden ayudarle a comprender mejor cuál es la lógica que aplica Expressway al analizar los certificados:

- developer.ssl
- developer.zone.zonemg

De forma predeterminada, estos módulos de registro están configurados en el nivel INFO. Cuando se los configura en el nivel DEBUG, se puede comenzar a ver la información sobre la inspección de certificados que se realiza, junto con el tráfico de zona al que se lo asigna. Ambas de estas funciones son relevantes para Hybrid Call Service.

Ejemplo del Expressway-E que lleva a cabo una inspección de SAN del certificado de servidor de 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"
```

Ejemplo de la asignación de Expressway-E de la conexión MTLS a la zona de DNS híbrido de Cisco Webex:

```
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"
```

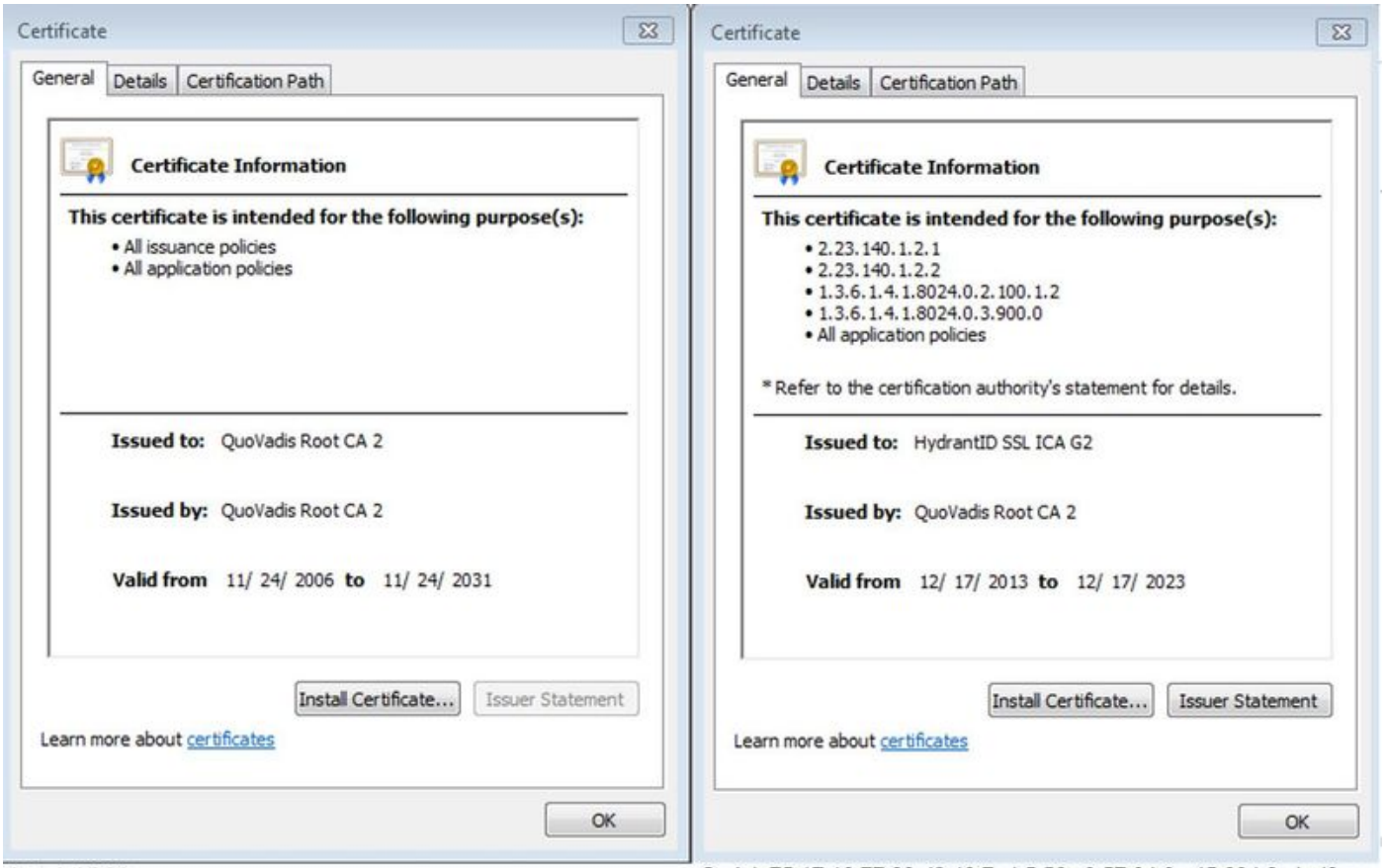
CodeLocation="ppcmains/oak/zones/ZoneManager.cpp(1226)"
Method="ZoneManager::getDNSZoneByTLSVerifySubjectName" Thread="0x7f577f0a0700":
this="0x56408ff81220" **getDNSZoneByTLSVerifySubjectName classified subject name callservice.ciscospark.com into DNS zone Hybrid Call Services DNS**
2017-09-22T11:11:19.564-04:00 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"**

A continuación se presenta una lista de los problemas más comunes relacionados con las fallas mutuas de TLS entre Expressway-E y Cisco Webex.

Problema 1. Expressway-E no confía en la autoridad de certificados (CA) que firmó el certificado de Cisco Webex

El servidor de Cisco Webex que se encuentra en comunicación directa con Expressway-E se denomina servidor L2SIP. Este servidor L2SIP debe tener la firma de un servidor intermediario con un nombre común de **Hydrant SSL ICA G2**. El intermediario tiene la firma de una autoridad de certificación de raíz que tiene un nombre común de **QuoVadis Root CA 2**, como se muestra en la imagen.

> **Nota:** Esto podría estar sujeto a cambios.



El primer paso para analizar este tráfico desde la perspectiva de diagnóstico de Expressway es buscar **Conectando TCP**. Después de buscar **Conectando TCP**, deberá buscar el valor **Dst-port=5062.** Una vez que haya identificado el área de los registros donde se ha intentado y establecido esta conexión, puede buscar el intercambio de señales de TLS que normalmente se identifica en las entradas de registro como intercambio de señales en curso.

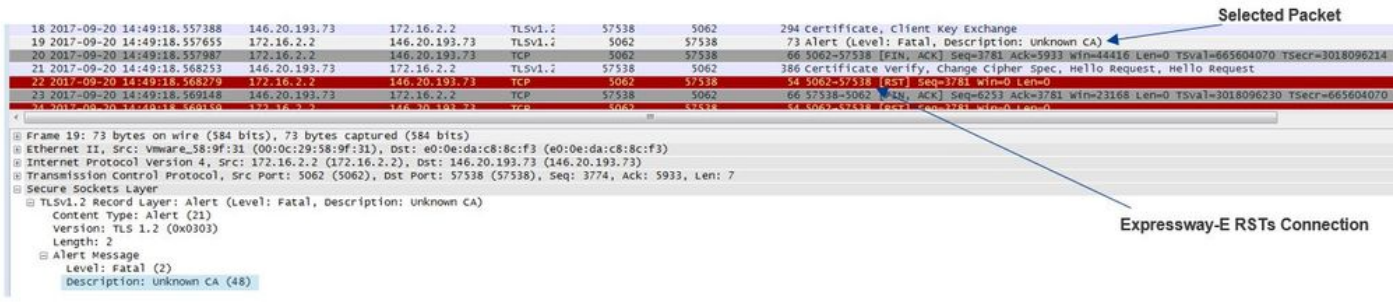
```
2017-09-20T10:49:18.427-04:00 amer-expressway01 tvcs: UTCTime="2017-09-20 14:49:18,426"
Module="developer.ssl" Level="INFO" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(1974)"
Method="::ttssl_continueHandshake" Thread="0x7f29ddefa700":  Detail="Handshake in progress"
Reason="want read/write"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

Si Expressway-E no confía en los certificados firmados de Cisco Webex, Expressway-E puede rechazar el certificado inmediatamente después de que se complete el intercambio de señales. Esto se puede observar en estas entradas del registro de Expressway-E:

```
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"
```

El mensaje de error de Expressway puede inducir a error ligeramente porque se refiere a un

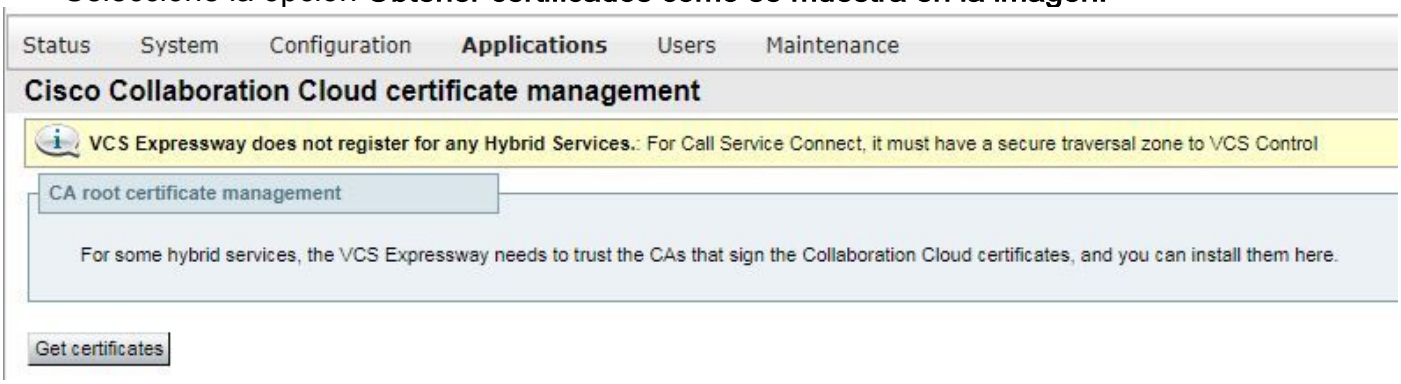
certificado autofirmado en la cadena de certificados. Wireshark le permite echar un vistazo al intercambio. Desde la perspectiva del análisis de captura de paquetes de Wireshark, puede ver claramente que cuando el entorno de Webex presenta su certificado, Expressway se da la vuelta y rechaza con un certificado con un error de CA desconocido como se muestra en la imagen.



Solución:

Para resolver esta situación, debe asegurarse de que Expressway-E confíe en las autoridades de certificados de Cisco Webex. Aunque podría simplemente extraer estos certificados de un seguimiento de Wireshark y cargarlos en el almacén de certificados de CA de confianza en Expressway, Expressway ofrece un método más sencillo:

- Inicie sesión en Expressway-E
- Vaya a **Aplicaciones > Administración de certificados en la nube**
- Seleccione la opción **Obtener certificados como se muestra en la imagen.**



En este momento, se cargan las autoridades de certificados de Cisco Webex en el almacén de CA de confianza de Expressway-E **(Mantenimiento > Seguridad > Certificado de CA de confianza)**.

Problema 2. Nombre incorrecto para el nombre de verificación del asunto TLS en la zona de DNS híbrido de Cisco Webex de Expressway-E

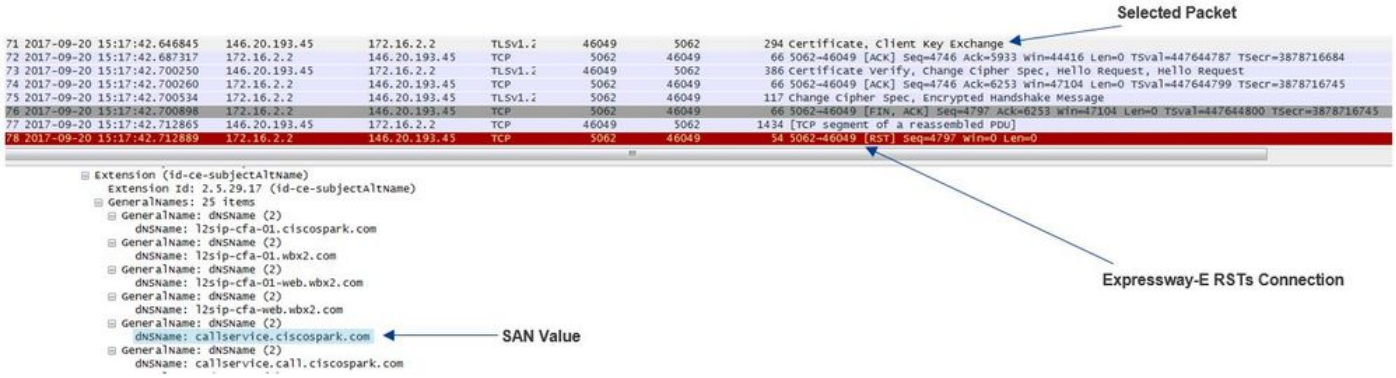
Como parte del intercambio mutuo de señales de TLS, Hybrid Call Service Connect usa la verificación de TLS. Esto significa que, además de confiar en los certificados de CA de Cisco Webex, Expressway comprueba el certificado al verificar el campo de nombre alternativo de asunto (SAN) del certificado que se presenta para asegurarse de que tenga un valor como **callservice.ciscospark.com presente.** Si este valor no está presente, se produce un error en la llamada entrante.

En esta situación concreta, el servidor de Cisco Webex presenta su certificado a Expressway-E. El certificado tiene 25 SAN diferentes. Analicemos el caso en que Expressway-E comprueba el certificado para encontrar el SAN de callservice.ciscospark.com, pero no puede encontrar esa información. Cuando se cumple esta condición, puede ver un error similar a este en el registro 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"
```

Si usa Wireshark para analizar el intercambio de señales de este certificado, puede encontrar esto después de que Cisco Webex presenta su certificado; Expressway reinicia la conexión poco después, como se muestra en la imagen.



Para confirmar la configuración de este valor, puede ir a la zona de DNS híbrido de Webex que se ha configurado para la solución. Si tiene la xConfiguration de Expressway-E, puede buscar la sección de configuración de zona para determinar la configuración del nombre de asunto de verificación de TLS. Para la xConfiguration, tenga en cuenta que las zonas se ordenan con la zona 1 en primer lugar. Esta es una xConfiguration del entorno problemático analizado anteriormente.

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

Como puede ver en el ejemplo, el nombre de asunto de verificación de TLS se establece en **calllservice.ciscospark.com** en lugar de **callservice.ciscospark.com**. (observe la "l" adicional).

Solución:

Para resolver este problema, debe modificar el nombre de asunto de verificación de TLS:

- Inicie sesión en Expressway-E
- Vaya a **Configuración > Zonas > Zonas**
- Seleccione **Zona de DNS de servicios híbridos de Webex**
- Establezca el **Nombre de asunto ed verificación de TLS en callservice.ciscospark.com**
- Seleccione **Save (Guardar).**

Nota: Consulte el comportamiento de registro de referencia. Esta sección muestra la verificación de certificados de Expressway y la asignación a la zona de DNS híbrido de Webex.

Nota: A partir del código de Expressway x12.5 y posteriores, se ha lanzado una nueva zona

"Webex". Esta zona de Webex rellena previamente la configuración de la zona requerida para la comunicación a Webex. Esto significa que ya no tendrá que establecer el modo de verificación de asunto de TLS y el nombre de asunto de verificación de TLS. Para simplificar la configuración, se recomienda aprovechar la zona de Webex si está ejecutando x12.5 o una versión posterior del código de Expressway.

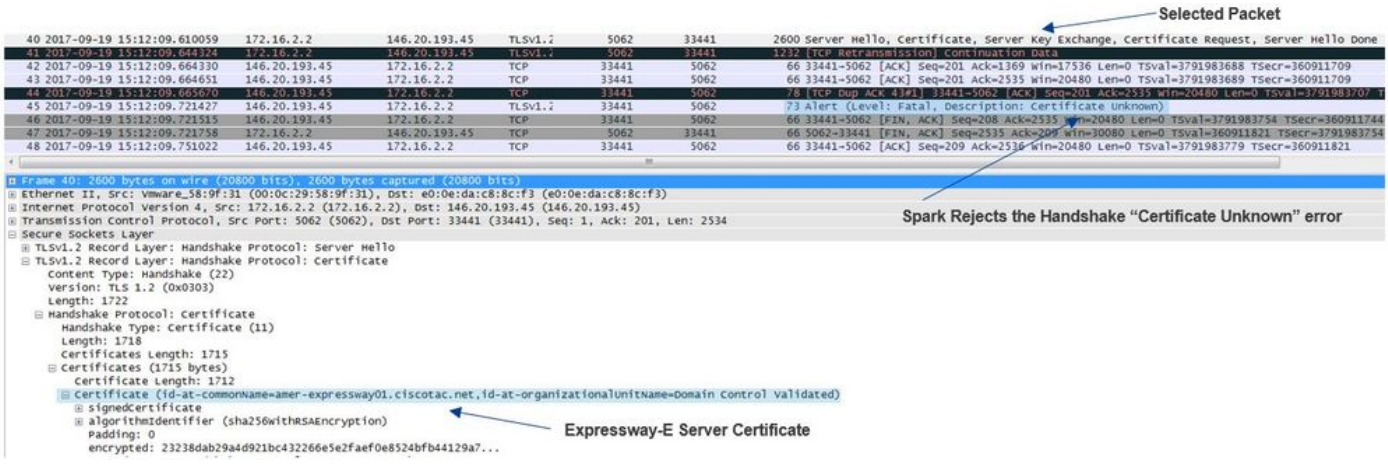
Problema 3. Expressway-E no envía la cadena de certificado completa a Cisco Webex

Como parte del intercambio mutuo de señales de TLS, Cisco Webex debe confiar en el certificado de Expressway-E. Cisco Webex tiene una lista completa de CA públicas de confianza. Por lo general, un intercambio de señales de TLS es exitoso cuando el certificado de Expressway-E está firmado por una CA pública que es compatible con Cisco Webex. Por diseño, Expressway-E sólo envía su certificado durante un intercambio de señales TLS a pesar de que está firmado por una CA pública. Para enviar la cadena completa de certificados (raíz e intermedia), estos certificados deben agregarse al almacén de certificados de CA de confianza en el Expressway-E mismo.

Si no se cumple esta condición, Cisco Webex rechaza el certificado de Expressway-E. Al solucionar una situación que coincide con este problema, puede usar los registros de diagnóstico y tcpdump de Expressway-E. Al analizar los registros de diagnóstico de Expressway-E, verá un error similar 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"
```

Si analiza esto desde la perspectiva de Wireshark, verá que Expressway-E presenta su certificado. Si expande el paquete, puede ver que se envía solo el certificado del servidor. Cisco Webex rechaza este intercambio de señales de TLS con un mensaje de error de CA desconocida, como se muestra en la imagen.

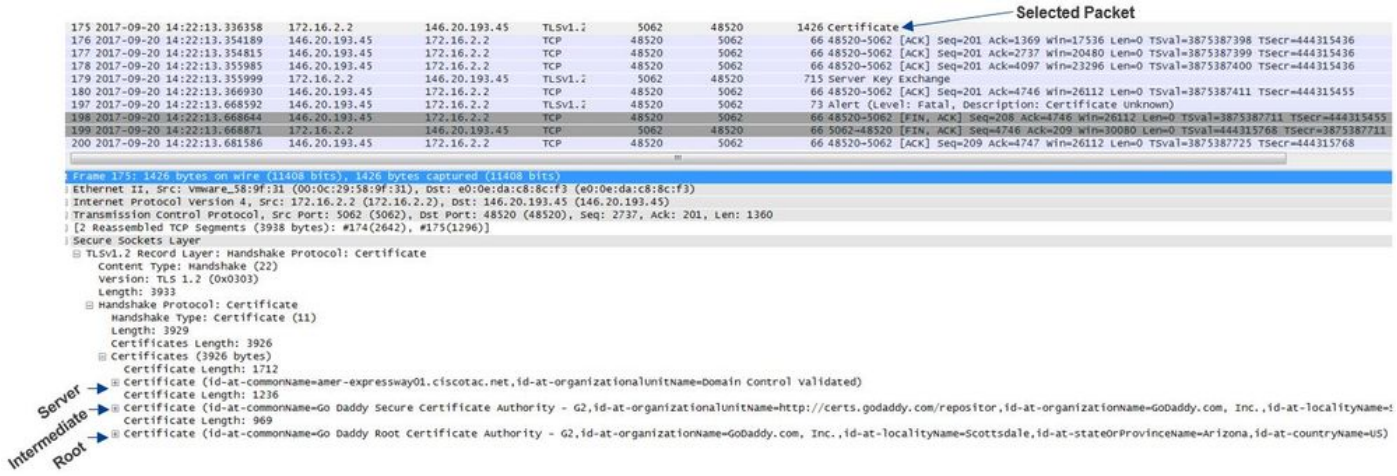


Solución:

Para solucionar el problema en esta situación, debe cargar la CA intermedia y de raíz que participan en la firma del certificado de Expressway-E en el almacén de certificados de CA de confianza:

Paso 1. Inicie sesión en Expressway-E.
Paso 2. Vaya a **Mantenimiento > Seguridad > Certificado de CA de confianza**.
Paso 3. Seleccione **Elegir archivo** en el menú Cargar cerca de la parte inferior de la interfaz de usuario.
Paso 4. Elija el certificado CA que participó en la firma de Expressway-E.
Paso 5. Seleccione **Agregar certificado de CA**.
Paso 6. Repita los pasos para todos los certificados de CA involucrados en la firma del certificado de Expressway-E (intermedio, raíz).
Paso 7. Seleccione **Agregar certificado de CA**.

Una vez terminado este proceso, verá la cadena completa de certificados involucrados en la firma del certificado de servidor de Expressway-E incluido en el intercambio de claves. Este es un ejemplo de lo que vería si analiza una captura de paquetes con Wireshark.



Problema 4. El firewall finaliza el intercambio mutuo de señales TLS

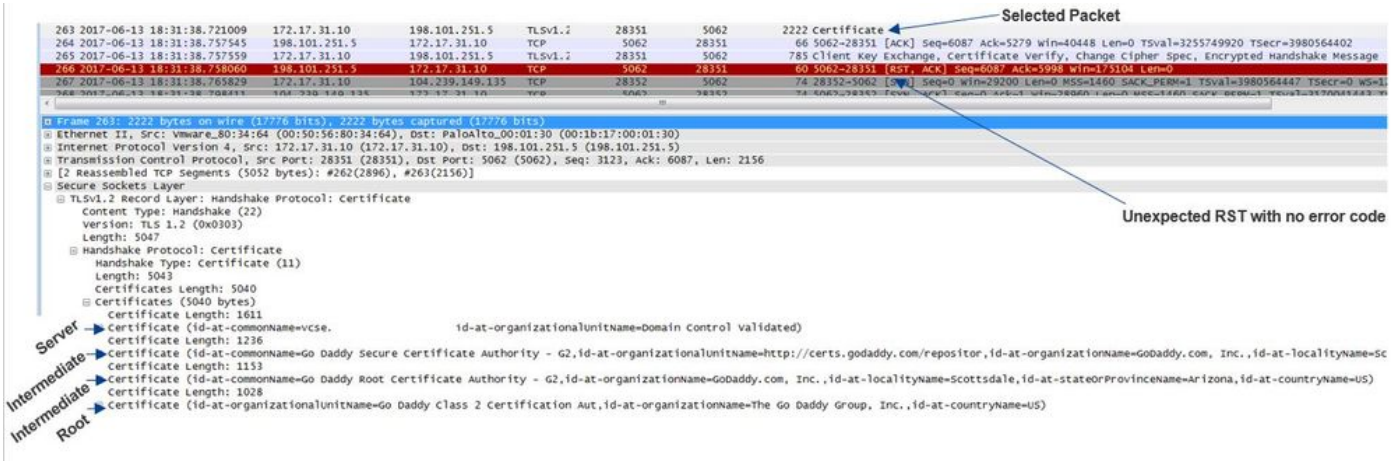
La solución de Expressway normalmente interactúa con un firewall. Muchas veces, el cortafuegos en línea de la solución ejecuta algún tipo de inspección de capa de aplicaciones. A menudo con la solución Expressway, cuando el firewall realiza la inspección de la capa de aplicación, los administradores ven resultados no deseados. Este problema concreto ayuda a identificar cuando la inspección de capa de aplicaciones de un cortafuegos repentinamente interrumpe la conexión.

Mediante el uso de los registros de diagnóstico de Expressway, puede buscar el intento de intercambio mutuo de señales TLS. Este intercambio de señales, como se mencionó antes, debe figurar poco después de que se estableció la conexión TCP a través del puerto 5062. En esta situación, cuando el cortafuegos interrumpe la conexión, verá estos errores en el registro 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"
```

Desde una perspectiva de captura de paquetes, verá que Expressway-E presenta su certificado a Cisco Webex. Verá un RST de TCP procedente de la dirección de Cisco Webex, como se muestra en la imagen.



En un principio, puede pensar que algo va mal con el certificado de Expressway-E. Para solucionar este problema, primero debe determinar las respuestas a estas preguntas:

- ¿Expressway-E está firmado por una CA pública de confianza para Cisco Webex?
- ¿El certificado de Expressway-E y cualquier certificado involucrado en la firma del certificado de Expressway-E se cargaron manualmente en Cisco Webex Control Hub (https://admin.ciscospark.com)?

En este caso en particular, la solución era no usar Cisco Webex Control Hub para administrar los certificados de Expressway-E. Esto significa que el certificado de Expressway-E debe estar firmado por una CA pública de confianza para Cisco Webex. Mediante la selección en el paquete de certificados de la captura de Wireshark (como se muestra antes), puede comprobar que el certificado está firmado por una CA pública y que se ha enviado la cadena completa a Cisco Webex. Por lo tanto, el problema no debe estar relacionado con el certificado de Expressway-E.

A esta altura, si se necesita más aislamiento, podría tomar una captura de paquetes de la interfaz externa del cortafuegos. Sin embargo, la falta de error de SSL en el registro de diagnóstico es un punto de datos importante. Como se menciona en el punto anterior (problema 3)*, si Cisco Webex no confía en el certificado de Expressway-E, debe ver algún tipo de motivo de desconexión de SSL.* En esta situación, no había ningún error de SSL disponible.

> **Nota:** Si obtuviera una captura de paquetes de la interfaz externa del cortafuegos, no vería una RST de TCP proveniente del entorno de Cisco Webex.

Solución

Para esta solución en particular, como partner o cliente debe confiar en su equipo de seguridad. El equipo debe investigar si se usa algún tipo de inspección de capa de aplicaciones para la solución de Expressway y, si se usa, se la debe deshabilitar. El apéndice 4 de la **Guía de implementación de VCS Control y Expressway explica por qué se recomienda que los clientes desactiven esta función.**

Problema 5. Expressway-E está firmado por la CA pública pero Cisco Webex Control Hub tiene

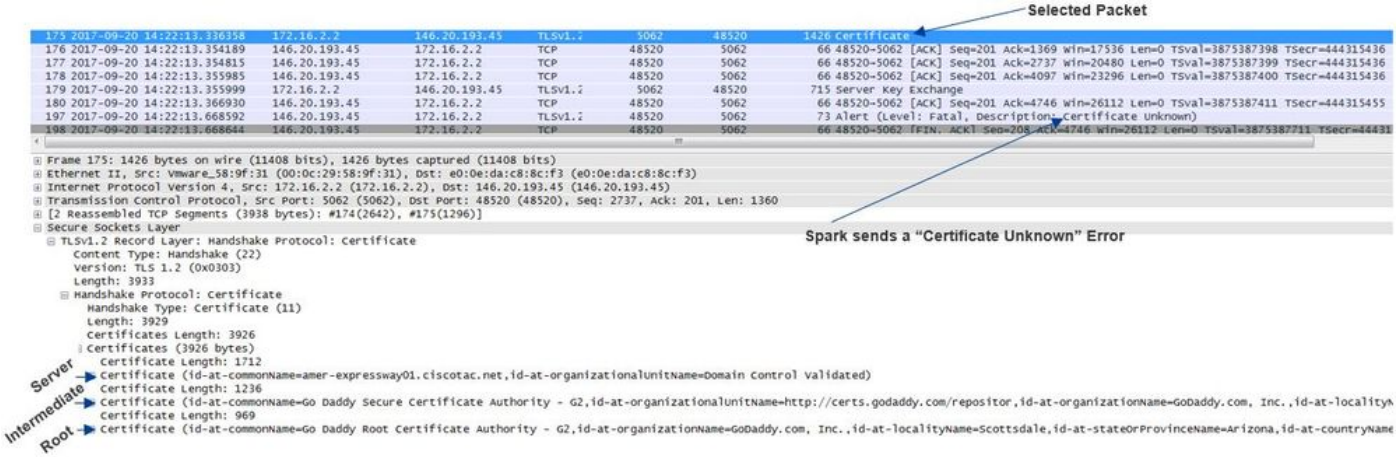
cargados otros certificados

Esta condición en particular suele ocurrir cuando se implementa la solución de Expressway desde el principio y no se tiene el certificado de Expressway-E firmado por una CA pública inicialmente. En esta situación, se carga el certificado de servidor de Expressway-E (que se ha firmado internamente) en Cisco Webex Control Hub para que la negociación mutua de TLS pueda completarse correctamente. Posteriormente, hace firmar el certificado de Expressway-E por una CA pública, pero se olvida de quitar el certificado del servidor desde Cisco Webex Control Hub. Es importante saber que, cuando se carga un certificado en Cisco Webex Control Hub, ese certificado tiene prioridad sobre el certificado y la cadena que Expressway presenta durante el intercambio de señales de TLS.

Desde la perspectiva del registro de diagnóstico de Expressway-E, este problema puede parecer similar a la firma de registro que se cumple cuando Cisco Webex no confía en el certificado de Expressway-E; por ejemplo, en el caso de que Expressway-E no envíe su cadena completa o de que el certificado de Expressway-E no esté firmado por una CA pública en la que confía Cisco Webex. A continuación se muestra un ejemplo de lo que puede esperar en ver en el registro de Expressway-E durante el intercambio de señales 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="::TTSSLErrorOutput" 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"
```

Si analiza esto desde la perspectiva de Wireshark, puede ver que Expressway-E presenta su certificado en el artículo de línea 175. Algunos elementos de línea más tarde, el entorno de Cisco Webex rechaza el certificado con un error de certificado desconocido, como se muestra en la imagen.



Si selecciona el paquete de certificado que envía Expressway-E, puede ampliar la información del certificado para determinar si Expressway-E

1. está firmado por una CA pública de confianza para Cisco Webex, y

2. incluye la cadena completa involucrada en la firma.

En esta situación, se cumplen ambas condiciones. Esto sugiere que no hay ningún problema con el certificado de Expressway-E.

Solución

Paso 1. Inicie sesión en Cisco Webex Control Hub.
Paso 2. Seleccione **Services** en el panel izquierdo.

Paso 3. Elija **Settings** en la tarjeta de llamada híbrida.

Paso 4. Desplácese hasta la sección Conexión del servicio de llamadas y busque en Certificados para llamadas SIP cifradas para ver si se muestran los certificados no deseados. Si es así, haga clic en el icono de papelera junto al certificado.

paso 5. Seleccione **Remove**.

> **Nota:** Es importante que se lleve a cabo el análisis y se determine que el cliente no usa los certificados cargados en Webex Control Hub antes de quitarlos.

Para obtener más información acerca de la carga del certificado de Expressway-E en Cisco Webex Control Hub, consulte esta sección de la Guía de implementación de llamadas híbridas.

Problema 6. Expressway no asigna llamadas entrantes a la zona de DNS híbrido de Cisco Webex

La función de asignación de TLS entrantes opera conjuntamente con la verificación de nombre de asunto de TLS y ambas se configuran en la zona de DNS de llamada híbrida. Este escenario articula los problemas y desafíos observados con Expressway antes de x12.5. En x12 y posterior se implementó un nuevo tipo de zona denominado zona "Webex". Esta zona rellena previamente toda la configuración necesaria para la integración con Webex. Si está ejecutando x12.5 e implementando una llamada híbrida de Webex, es recomendable utilizar el tipo de zona **Webex** para que el dominio de servicios de llamadas híbridas (callservice.webex.com) se configure automáticamente para usted. Este valor coincide con el nombre alternativo del asunto del certificado de Webex que se presenta durante el intercambio mutuo de señales TLS y permite que la conexión y la asignación entrante a Expressway se realicen correctamente.

Si utiliza una versión de código inferior a x12.5 o no utiliza la zona de Webex, deberá continuar con la siguiente explicación que muestra cómo identificar y corregir los problemas en los que Expressway no asigna la llamada entrante a la zona de DNS híbrido de Webex.

La función se divide en un proceso de tres pasos:

1. Expressway-E acepta el certificado de Cisco Webex.
2. Expressway-E examina el certificado de Cisco Webex para determinar si hay un nombre alternativo del asunto que coincida con la verificación de nombre de asunto de TLS: callservice.ciscospark.com.
3. Expressway-E asigna la conexión entrante a través de la zona de DNS híbrido de Cisco Webex.

Si la autenticación no tiene éxito, esto significa que falló la validación del certificado. La llamada entra en la zona predeterminada y se enruta según las reglas de búsqueda proporcionadas para situaciones interempresariales, si están configuradas en Expressway-E.

Al igual que en las demás situaciones, debe usar tanto el registro de diagnóstico como las capturas de paquetes para determinar el aspecto de este error y, a continuación, usar la captura de paquetes para ver qué lado está enviando el RST. Este es un ejemplo del intento y posterior establecimiento de la conexión TCP.

```
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"
```

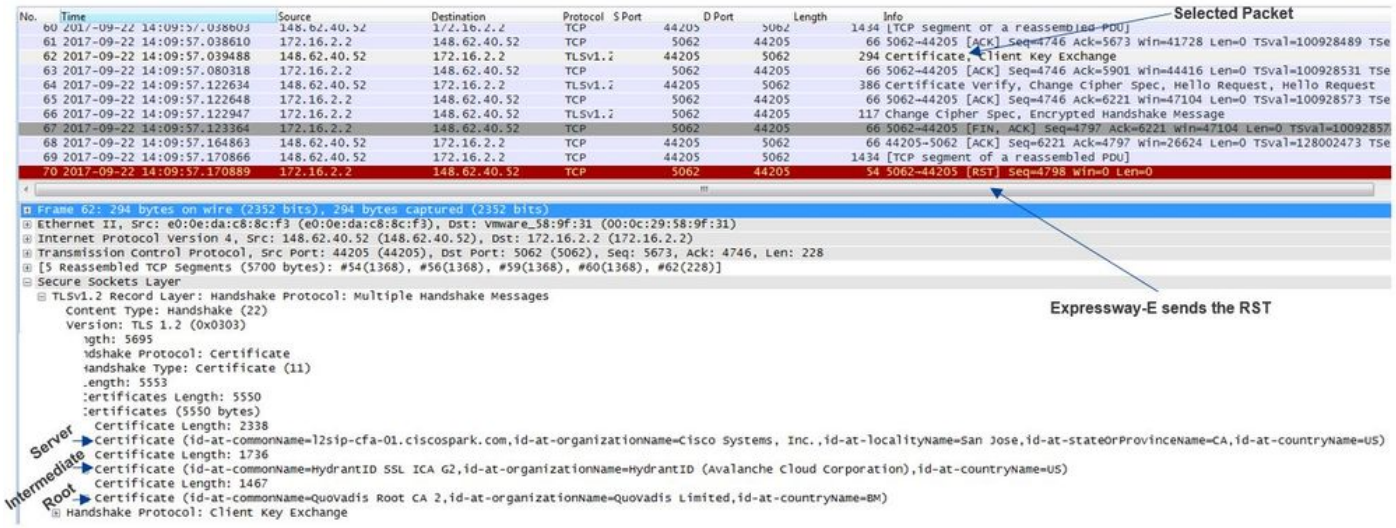
Una vez que se haya establecido la conexión TCP, puede producirse el intercambio de señales TLS. Puede ver que apenas se inicia el intercambio de señales, se detiene por errores rápidamente.

```
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"
```

Si analiza esta situación desde la perspectiva de pcap, puede obtener una mejor idea de

- quién envía el RST, y
- qué certificados se intercambian para determinar si son correctos.

Al analizar esta captura concreta, puede ver que Expressway-E envía el RST. Al observar el certificado de Cisco Webex que se transmite, puede ver que envía la cadena completa. Además, puede concluir que, según el mensaje de error del registro de diagnóstico, puede descartar la situación en la que Expressway-E no confía en las CA públicas de Cisco Webex. De lo contrario, verá un error como "certificado autofirmado en la cadena de certificado". Puede profundizar en los detalles del paquete, como se muestra en la imagen.



Al hacer clic en el certificado de servidor de Webex y expandirlo para ver los nombres alternativos del asunto (dnsName), puede asegurarse de que **callservice.ciscospark.com esté en la lista.**

Vaya a Wireshark: **Certificado > Extensión > Nombres generales > GeneralName > dNSName: callservice.ciscospark.com**

Esto confirma definitivamente que el certificado de Webex es correcto.

Ahora puede confirmar que el nombre de asunto de verificación de TLS es correcto. Según lo mencionado antes, si tiene la xConfiguration, puede buscar la sección de configuración de zona para determinar la configuración del nombre de asunto de verificación de TLS. Un aspecto de xConfiguration que se debe tener en cuenta es que las zonas se ordenan con la zona 1 en primer lugar. Esta es una xConfiguration del entorno problemático analizado anteriormente. Está claro que no hay ningún problema con el nombre de asunto de verificación de TLS.

```
*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"
```

Lo siguiente que se debe investigar es la **asignación entrante de verificación de TLS**. Esto confirma si está asignando correctamente la conexión de TLS a la zona de DNS híbrido de Webex. Puede usar xConfiguration para analizar esto también. En xConfiguration, la **asignación entrante de verificación de TLS se denomina DNS ZIP TLS Verify InboundClassification**. Como puede ver en este ejemplo, se establece el valor en Off.

```
*c xConfiguration Zones Zone 6 DNS SIP TLS Verify InboundClassification: "Off"
*c xConfiguration Zones Zone 6 Name: "Hybrid Call Services DNS"
```

Dado que este valor se establece en Off, esto significa que se impide que VCS intente asignar las conexiones TLS entrantes a esta zona. La llamada entra en la zona predeterminada, y se la comprueba y enruta según las reglas de búsqueda proporcionadas para situaciones interempresariales, si están configuradas en Expressway-E.

Solución

Para esto, es preciso configurar la opción de asignación entrante de verificación de TLS en la zona de DNS híbrido de llamadas en On. Estos son los pasos para hacerlo.

1. Inicie sesión en Expressway-E

2. Vaya a **Configuración > Zonas > Zonas**
3. Seleccione **Zona de DNS híbrido de llamadas**
4. Para la **asignación entrante de verificación de TLS**, seleccione **On**
5. Seleccione **Save (Guardar).**

Nota: Consulte para obtener información sobre el comportamiento de registro de la línea de base. Esta sección muestra la verificación de certificados de Expressway y la asignación a la zona de DNS híbrido de Webex.

Problema 7. Expressway-E utiliza el certificado firmado automáticamente predeterminado

En algunas instalaciones nuevas de Hybrid Call Service Connect, la firma del certificado de Expressway-E se pasa por alto o se considera que se puede usar el certificado de servidor predeterminado. Algunas personas consideran que esto es posible debido a que Cisco Webex Control Hub permite cargar un certificado personalizado en el portal. (**Servicios > Configuración (bajo la tarjeta de llamadas híbridas**) **> Cargar (en Certificados para llamadas cifradas**))

Si se presta mucha atención a los términos sobre los **certificados para llamadas SIP cifradas, verá esto:** "Use los certificados proporcionados en la lista de confianza predeterminada de Cisco Collaboration o cargue sus propios certificados. Si usa sus propios certificados, asegúrese de que los nombres de host se encuentren en un dominio verificado". La parte clave de esa instrucción es **"asegúrese de que los nombres de host se encuentren en un dominio verificado".**

Cuando solucione un problema que coincida con esta condición, tenga en cuenta que el síntoma dependerá de la dirección de la llamada. Si la llamada se originó en un teléfono en las instalaciones, puede esperar que la aplicación Cisco Webex no timbre. Además, si se ha intentado realizar el seguimiento de la llamada desde el historial de búsqueda de Expressway, encontrará que la llamada llegó a Expressway-E y se detuvo allí. Si la llamada se originó en una aplicación de Cisco Webex y está destinada a las instalaciones, el teléfono en las instalaciones no timbra. En ese caso, el historial de búsqueda de Expressway-E y Expressway-C no mostrarían nada.

En esta situación en particular, la llamada se originó en un teléfono en las instalaciones. Con el historial de búsqueda de Expressway-E, es posible determinar si la llamada llegó al servidor. En este momento, puede profundizar en el registro de diagnóstico para determinar qué ha ocurrido. Para iniciar este análisis, compruebe en primer lugar si se ha intentado y establecido una conexión de TCP a través del puerto 5062. Si busca "Conexión de TCP" en los registros de diagnóstico de Expressway-E y busca del artículo de línea con la etiqueta "Dst-port=5062"*, puede determinar si se establece la conexión.*

```
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"
```

Una vez que haya confirmado que se estableció la conexión de TCP, puede analizar el intercambio mutuo de señales TLS que ocurre inmediatamente después. Como se puede ver en este fragmento, el intercambio de señales falla y el certificado se desconoce **(detalle = "sslv3 alert certificateunknown")**

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"**

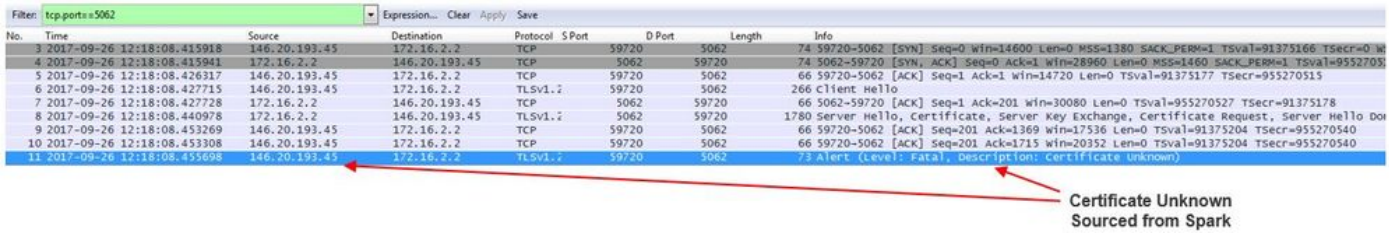
2017-09-26T08:18:08.455-04:00 amer-expressway01 tvcs: Event="Inbound TLS Negotiation Error" Service="SIP" Src-ip="146.20.193.45" Src-port="59720" Dst-ip="172.16.2.2" **Dst-port="5062"** Detail="sslv3 alert certificate unknown" Protocol="TLS" Level="1" UTCTime="2017-09-26 12:18:08,455"

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"**

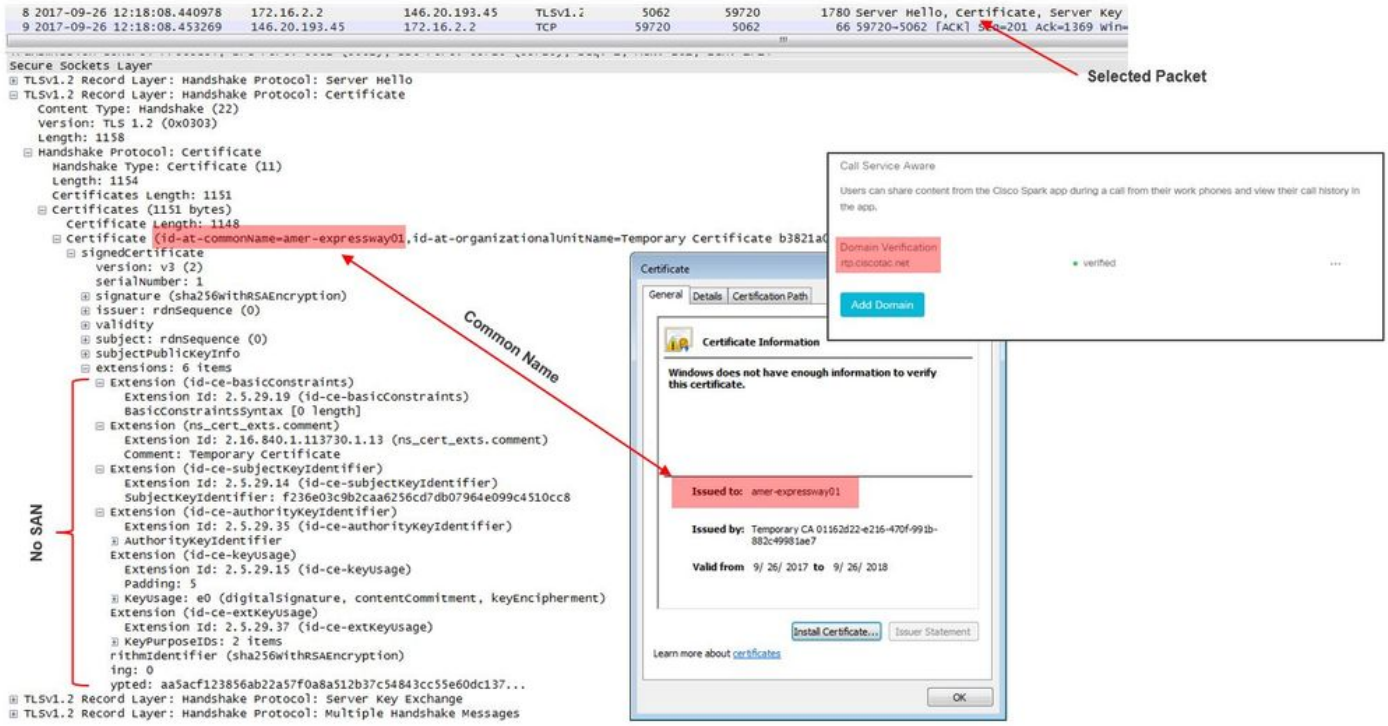
2017-09-26T08:18:08.455-04:00 amer-expressway01 tvcs: UTCTime="2017-09-26 12:18:08,455" Module="developer.ssl" Level="ERROR" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(68)" Method="::TTSSLErrorOutput" Thread="0x7f930adab700": **TTSSL_continueHandshake: Failed to establish SSL connection** iResult="0" 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"**

Si analiza en más detalle la captura de paquetes proporcionada con el registro de diagnóstico de Expressway-E, puede ver que el error de certificado desconocido proviene de Cisco Webex, como se muestra en la imagen.



Si inspecciona el certificado del servidor predeterminado de Expressway-E, podrá ver que el 'Nombre común' y los 'Nombres alternativos de asunto' no contienen el 'Dominio verificado' **(rtp.ciscotac.net).** Con esto tiene pruebas acerca de las causas de este problema, como se muestra en la imagen.



En este punto, ha determinado que el certificado de servidor de Expressway-E tiene que estar firmado por una CA pública o una CA interna.

Solución

Para resolver este problema, tiene dos opciones:

1. Haga que el certificado de Expressway-E tenga la firma de una [CA pública de confianza para Cisco Webex](#).
   Inicie sesión en Expressway-E.Vaya a **Mantenimiento > Seguridad > Certificado de servidor**.Seleccione **Generar CSR**.Introduzca la información necesaria del certificado y asegúrese de que el campo **Nombres alternativos adicionales contenga el Dominio verificado en la lista de Webex Control Hub.**Haga clic en **Generar CSR**.Envíe la CSR a una CA pública externa para que la firme.Al recibir el certificado de vuelta, vaya a **Mantenimiento > Seguridad > Certificados de servidor**.En la sección **Cargar certificado nuevo junto a Seleccione el archivo del certificado de servidor**, seleccione **Elegir archivo y seleccione el certificado firmado**.Seleccione **Cargar datos del certificado de servidor**.Vaya a **Mantenimiento > Seguridad > Certificado de CA de confianza**.En la sección **Cargar** junto a **Seleccione el archivo que contiene los certificados de CA de confianza , seleccione Elegir archivo**.Seleccione cualquier certificado de CA de raíz o intermedia proporcionados por la CA pública.Seleccione **Agregar certificado de CA**.Reinicie Expressway-E.
2. Haga que una CA interna firme el certificado de Expressway-E y, a continuación, cargue la CA interna y Expressway-E en Cisco Webex Control Hub.
   Inicie sesión en Expressway.Vaya a **Mantenimiento > Seguridad > Certificado de servidor**.Seleccione **Generar CSR.**Introduzca la información necesaria del certificado y asegúrese de que el campo *Nombres alternativos adicionales contenga el* **Dominio verificado en la lista de Webex Control Hub.**Haga clic en **Generar CSR.**Envíe la CSR a una CA pública externa para que la firme.Al recibir el certificado de vuelta, vaya a *Mantenimiento > Seguridad > Certificados de servidor.*En la sección *Cargar certificado nuevo junto a* **Seleccione el archivo del certificado de servidor**, seleccione **Elegir archivo y seleccione el**

certificado firmado. Seleccione **Cargar datos del certificado de servidor.**Vaya a **Mantenimiento > Seguridad > Certificado de CA de confianza.**En la sección **Cargar junto a Seleccione el archivo que contiene los certificados de CA de confianza , seleccione Elegir archivo**.Seleccione cualquier certificado de CA de raíz o intermedia proporcionados por la CA pública.Seleccione **Agregar certificado de CA**.Reinicie Expressway-E.

2a. Cargue el certificado de CA interna y Expressway-E en Cisco Webex Control Hub.

1. Inicie sesión en Cisco Webex Control Hub como administrador.
2. Seleccione Servicies (Servicios).
3. Seleccione **Settings** en la tarjeta Hybrid Call Service.
4. En la sección **Certificados para llamadas SIP cifradas, seleccione Cargar**.
5. Elija los certificados de CA interna y Expressway-E.

Entrantes: Cisco Webex en las instalaciones

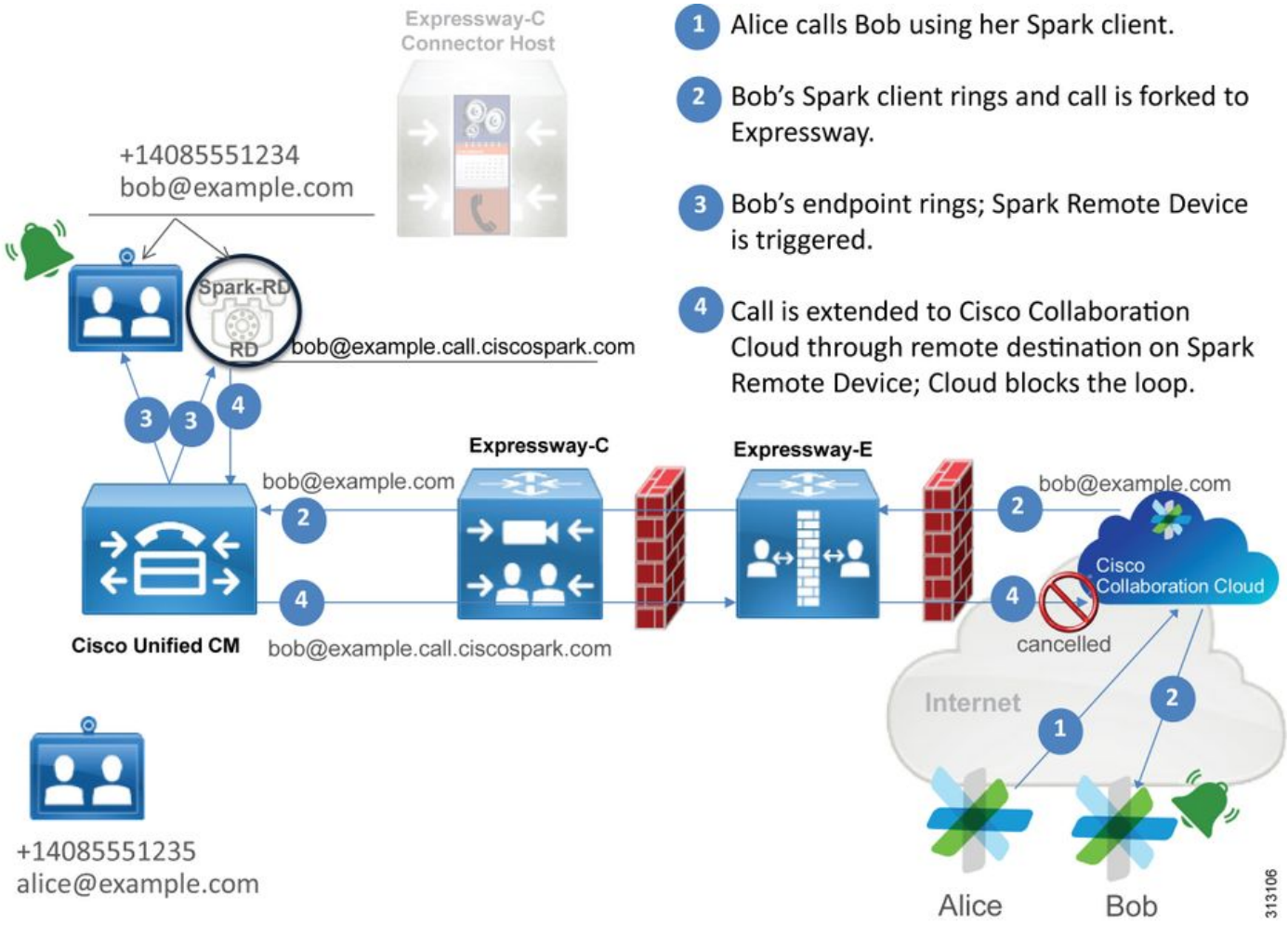
Casi todas las fallas entrantes de Cisco Webex a las instalaciones causan el mismo síntoma informado: "Cuando llamo desde mi aplicación de Cisco Webex a la aplicación de otro compañero, la aplicación de mi compañero timbra, pero el teléfono en las instalaciones no". Para solucionar problemas en estas situaciones, le resultará útil comprender el flujo de llamadas y la lógica que se produce cuando se realiza este tipo de llamada.

Flujo de lógica de alto nivel

1. La aplicación de Cisco Webex de la persona que llama inicia la llamada
2. La aplicación de la persona a la que llaman suena
3. La llamada se bifurca al entorno de Cisco Webex
4. El entorno de Cisco Webex debe llevar a cabo una búsqueda de DNS en función del destino SIP configurado del cliente en Cisco Webex Control Hub.
5. El entorno de Cisco Webex intenta conectarse a Expressway a través del puerto 5062
6. El entorno de Cisco Webex intenta realizar un intercambio mutuo de señales TLS
7. El entorno de Cisco Webex envía un SIP INVITE a Expressway, que lo envía al terminal de colaboración o al teléfono IP en las instalaciones
8. Cisco Webex y la empresa completan la negociación de SIP
9. Cisco Webex y la empresa empiezan a enviar y recibir medios.

Flujo de llamada

Vaya a la aplicación Cisco Webex > Entorno de Cisco Webex > Expressway-E > Expressway-C > Terminal de colaboración o teléfono IP en las instalaciones, como se muestra en la imagen.



Estos son algunos de los problemas comunes observados con las llamadas entrantes de Webex a la infraestructura en las instalaciones.

Problema 1. Cisco Webex no puede resolver el SRV/nombre de host DNS de Expressway-E

Cuando piense en el flujo de llamadas de Cisco Webex a las instalaciones, el primer paso lógico de Cisco Webex es ponerse en contacto con Expressway en las instalaciones. Como se indica anteriormente, Cisco Webex intentará conectarse a Expressway en las instalaciones mediante una búsqueda de SRV basada en el **Destino SIP configurado que aparece en la** página de configuración de Hybrid Call Service en Cisco Webex Control Hub.

Si intenta resolver esta situación desde una perspectiva de registro de diagnóstico de Expressway-E, no verá el tráfico de Cisco Webex. Si intenta buscar las conexiones TCP, no verá Dst-port=5062, ni verá cualquier intercambio de señales MTLS o invitación SIP posteriores de Cisco Webex.

En esta situación, debe comprobar la configuración del **Destino SIP en Cisco Webex Control Hub.** También puede usar la **Herramienta de prueba de conectividad híbrida para asistir en la solución de problemas.** La herramienta de prueba de conectividad híbrida comprueba si hay una dirección válida de DNS, si Cisco Webex puede conectarse al puerto devuelto en la búsqueda de SRV, y si Expressway en las instalaciones tiene un certificado válido y de confianza para Cisco Webex.

1. Inicie sesión en Cisco Webex Control Hub.
2. Seleccione Servicios
3. Seleccione el vínculo Configuración en la tarjeta de llamada híbrida.

4. En la sección Conexión del servicio de llamada, compruebe el dominio utilizado para la dirección de SRV de SIP en el campo Destino de SIP.
5. Si el registro se introdujo correctamente, haga clic en **Probar para ver si el registro es válido.**
6. Como se muestra a continuación, puede ver claramente que el dominio público no tiene un registro SRV SIP correspondiente asociado, como se muestra en la imagen.

Seleccione **Ver resultados de prueba** y podrá ver más detalles sobre lo que falló, como se muestra en la imagen.

Otro enfoque es buscar el registro SRV con nslookup. Estos son los comandos que puede ejecutar para comprobar si existe el destino de SIP.

```
C:\Users\pstojano>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 se puede ver en el bloque de código anterior, primero se inicia el comando nslookup y, a continuación, el servidor se establece en 8.8.8.8, que es un servidor de DNS público de Google. Por último, se configuran los tipos de registro para buscar en los registros de SRV. En ese momento, puede emitir el registro SRV completo que desea buscar. El resultado neto es que las solicitudes agotan el tiempo de espera.

Solución

1. Configure una dirección SRV SIP pública para Expressway-E en el sitio que se usa para alojar los nombres de dominio públicos.
2. Configure un nombre de host que se resuelva en la dirección IP pública de Expressway-E
3. Configure el destino de SIP para que incluya el dominio que se usa para la dirección SRV SIP creada en el paso 1. Inicie sesión en Cisco Webex Control Hub.Seleccione

Servicios. Seleccione el vínculo **Configuración en la** *tarjeta de llamada híbrida.*En la sección Conexión del servicio de llamada, introduzca el dominio utilizado para la dirección de SRV de SIP en el campo **Destino de SIP.** Seleccione Save (Guardar).

Nota: Si el registro SRV SIP que le gustaría usar ya se usa para las comunicaciones interempresariales, le recomendamos que especifique un subdominio del dominio corporativo como la dirección de detección de SIP en Cisco Webex Control Hub y, por tanto, un registro público de SRV de DNS, como se indica a continuación:

Servicio y protocolo: _sips._tcp.mtls.example.com
Prioridad: 1
Peso: 10
Número de puerto: 5062
Objetivo: us-expe1.example.com

La recomendación anterior se obtuvo directamente de la Guía de diseño híbrido de Cisco Webex.

Solución alternativa

Si el cliente no tiene un registro SRV SIP presente (y no piensa crear uno), como alternativa puede incluir la dirección IP pública de Expressway con el sufijo ": 5062". Al hacerlo, el entorno de Webex no intentará una búsqueda de SRV, sino que en su lugar se conectará directamente a **%Expressway_Pub_IP%:5062**. (Ejemplo: 64.102.241.236:5062)

1. Configure el destino de SIP con el formato **%Expressway_Pub_IP%:5062**. *(Ejemplo: 64.102.241.236:5062)* Inicie sesión en Cisco Webex Control Hub.Seleccione **Servicios.**Seleccione el vínculo **Configuración en la** *tarjeta de llamada híbrida.*En la sección Conexión del servicio de llamada, introduzca **%Expressway_Pub_IP%:5062 en el campo Destino de SIP.** Seleccione Save (Guardar).

Para obtener más información sobre la dirección de destino de SIP o un registro de SRV que debe configurarse. Consulte la sección Habilite Hybrid Call Service Connect para su organización de la Guía de implementación de Cisco Webex Hybrid Call Service o la Guía de diseño híbrido de Cisco Webex.

Problema 2. Falla de socket: El puerto 5062 entrante a Expressway está bloqueado

Una vez terminada la resolución de DNS, el entorno de Cisco Webex intentará establecer una conexión TCP a través del puerto 5062 a la dirección IP devuelta durante la búsqueda de DNS. Esta dirección IP será la dirección IP pública de Expressway-E en las instalaciones. Si el entorno de Cisco Webex es incapaz de establecer esta conexión TCP, la llamada entrante a las instalaciones también fallará. El síntoma para este caso en particular es el mismo que para casi todos las demás fallas de llamada entrante de Cisco Webex: el teléfono en las instalaciones no suena.

Si está solucionando este problema con los registros de diagnóstico de Expressway, no verá nada de tráfico de Cisco Webex. Si intenta buscar las conexiones TCP, no verá intentos de conexión para Dst-port=5062, ni verá cualquier intercambio de señales MTLS o invitación SIP posteriores de Cisco Webex. Dado que el registro de diagnóstico de Expressway-E no sirve en esta situación, dispone de otros posibles métodos de verificación:

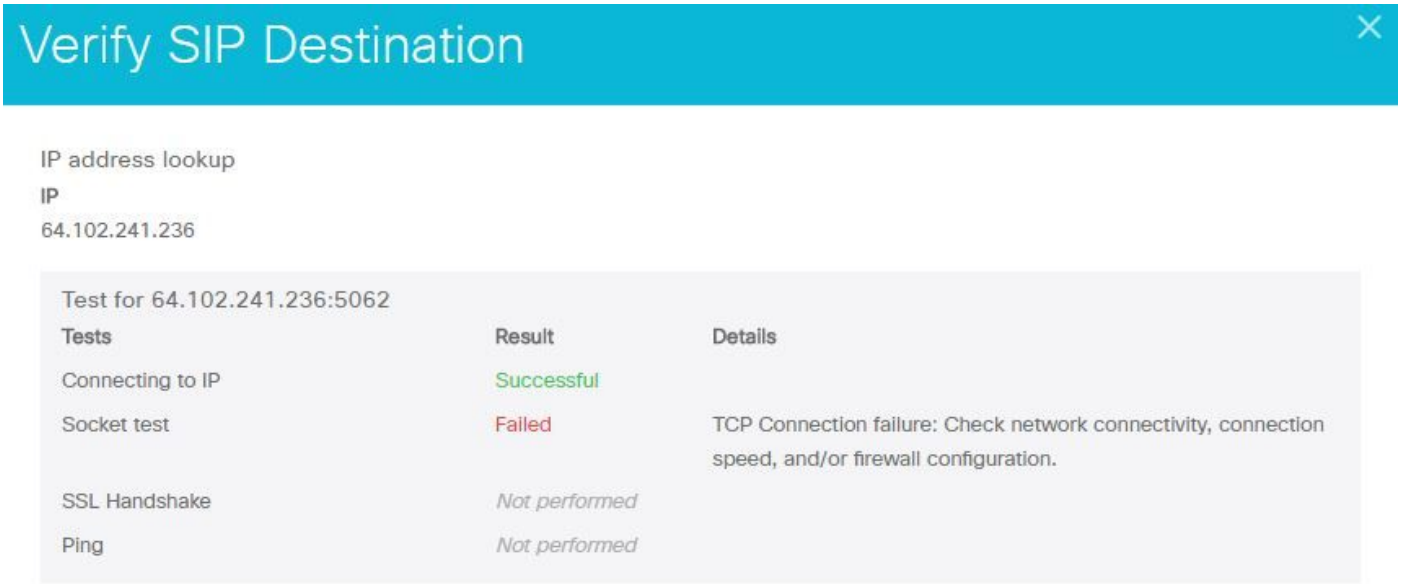
1. Obtenga una captura de paquetes de la interfaz externa del cortafuegos

2. Use una utilidad de comprobación de puertos
3. Use la herramienta de prueba de conectividad híbrida

Dado que la herramienta de prueba de conectividad híbrida está integrada directamente en Cisco Webex Control Hub y simula el entorno de Cisco Webex mientras intenta conectarse a Expressway en las instalaciones, es el mejor método de verificación disponible. Para comprobar la conectividad de TCP en la organización:

1. Inicie sesión en Cisco Webex Control Hub.
2. Seleccione Servicios
3. Seleccione el vínculo Configuración en la tarjeta de llamada híbrida
4. En la sección de conexión del servicio de llamadas, asegúrese de que el valor introducido en el destino de SIP sea correcto
5. Haga clic en Probar, como se muestra en la imagen.

6. Dado que la prueba ha fallado, puede hacer clic en el vínculo **Ver resultados de prueba para comprobar los detalles, como se muestra en la imagen.**



Como se observa en la imagen anterior, puede ver que ha fallado la prueba de Socket al intentar conectarse a 64.102.241.236:5062. Como estos datos ni los registros de diagnóstico/pcaps de Expressway no muestran ningún intento de conexión, tiene pruebas suficientes para investigar la configuración de enrutamiento/ACL/NAT del cortafuegos.

Solución

Puesto que este problema concreto no surge del entorno de Cisco Webex ni del equipo de colaboración en las instalaciones, deberá centrarse en la configuración de cortafuegos. Dado que no se puede predecir el tipo de cortafuegos con el que deberá interactuar, debe confiar en alguien que esté familiarizado con el dispositivo. Es posible que el problema esté relacionado con un error

de configuración de enrutamiento, ACL o NAT del cortafuegos.

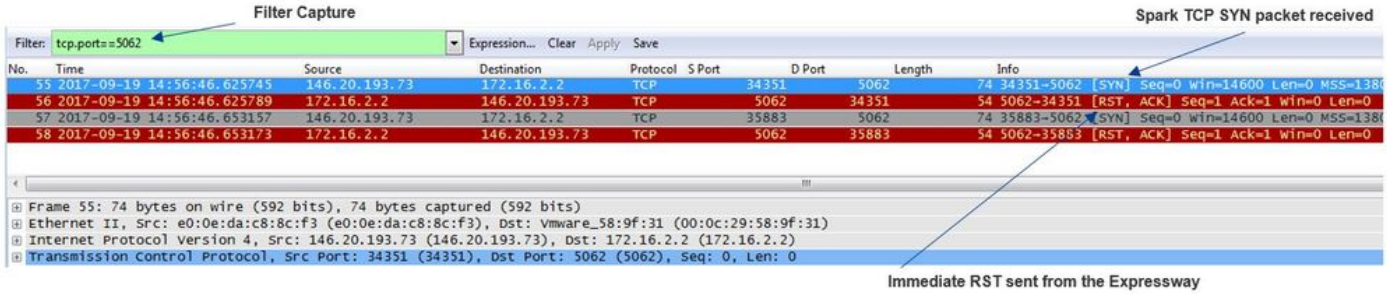
Problema 3. Falla de socket: Expressway-E no tiene detección en el puerto 5062

Esta situación en particular se suele diagnosticar incorrectamente. Muchas veces se supone que el cortafuegos es la causa del bloqueo del tráfico del puerto 5062. Para solucionar esta situación concreta, puede usar las técnicas de la situación anterior donde el "Puerto 5062 entrante a Expressway está bloqueado". Verá que la herramienta de prueba de conectividad híbrida y cualquier otra herramienta de comprobación de la conectividad de puerto no funcionarán. La primera suposición es que el cortafuegos está bloqueando el tráfico. La mayoría de las personas volverá a comprobar el registro de diagnóstico de Expressway-E para determinar si pueden ver la conexión TCP tratando de establecerse. Por lo general, buscarán un artículo de línea de registro como este, como se muestra en la imagen.

```
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"
```

En esta situación, la entrada de registro anterior no existe. Por lo tanto, muchas personas harán un diagnóstico incorrecto de la situación y supondrán que se debe al cortafuegos.

Si una captura de paquetes se incluye con el registro de diagnóstico, puede comprobar que el servidor de seguridad no es la causa. A continuación encontrará un ejemplo de captura de paquetes de la situación en la que Expressway-E no escucha a través del puerto 5062. En esta captura se filtra con tcp.port==5062 como el filtro aplicado, como se muestra en la imagen.



Como se puede ver en la captura de paquetes que se obtuvo de Expressway-E, al tráfico del puerto tcp 5062 no lo está bloqueando el cortafuegos, sino que está llegando correctamente. En el paquete número 56, puede ver que Expressway-E envía el RST inmediatamente después de que ha llegado el paquete SYN TCP inicial. Con esta información, puede concluir que el problema se encuentra en el Expressway-E que recibe el paquete; debe solucionar el problema desde la perspectiva de Expressway-E. Con estas pruebas, considere las posibles razones por las que Expressway-E restablece (RST) el paquete. Dos posibilidades que pueden causar este comportamiento son:

1. Expressway-E tiene algún tipo de reglas de cortafuegos configuradas que podrían estar bloqueando el tráfico

2. Expressway-E no detecta el tráfico de TLS mutuo o no detecta el tráfico del puerto 5062.

La función de cortafuegos de Expressway-E se encuentra en *Sistema > Protección > Reglas de cortafuegos > Configuración*. Cuando se comprobó esto en este entorno, no había ninguna configuración de cortafuegos presente.

Hay varias formas de comprobar si Expressway-E está detectando el tráfico de TLS mutuo a través del puerto 5062. Puede hacerlo a través de la interfaz Web o de la CLI como usuario raíz.

En la raíz de Expressway, si emite **netstat -an | grep ':5062' ,** debería obtener una salida similar a la que ve a continuación.

```
~ # 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
```

Esta información también se pueden capturar a través de la interfaz web de Expressway-E. Consulte los siguientes pasos para recopilar esta información

1. Inicie sesión en Expressway-E

2. Vaya a **Herramientas de mantenimiento > Uso de puertos > Puertos entrantes locales**

3. Busque el tipo SIP y el puerto IP 5062. (destacados en rojo como se muestra en la imagen)

Ahora que ya sabe qué debería ver, puede comparar eso con el entorno actual. Desde la perspectiva de la CLI, cuando se ejecuta **netstat -an | grep ':5062' ,** la salida es similar a la siguiente:

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

Además, el UU web no muestra el puerto de TLS mutuo que figura en Puertos entrantes locales

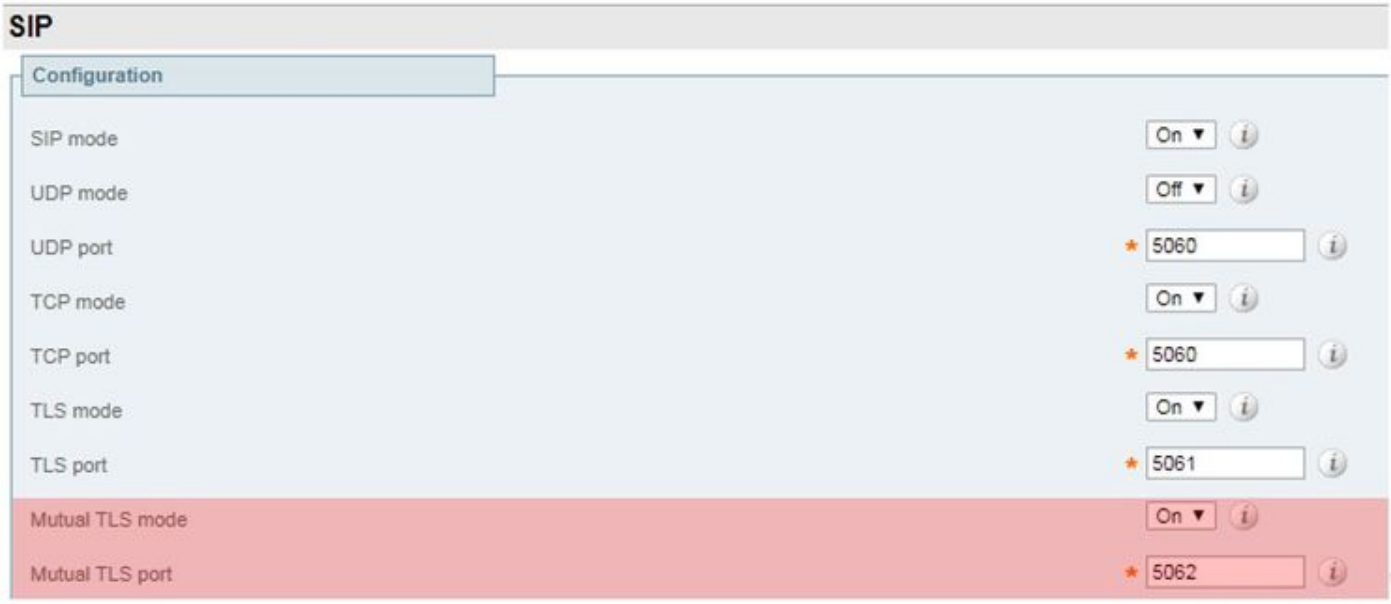
Con estos datos, puede concluir que Expressway-E no está detectando el tráfico de TLS mutuo.

Solución

Para resolver este problema, debe asegurarse de que el modo de TLS mutuo esté habilitado y que el puerto de TLS mutuo esté configurado en 5062 en Expressway-E:

1. Inicie sesión en Expressway-E

2. Vaya a **Configuración > Protocolos > SIP**
3. Asegúrese de que el modo de TLS mutuo esté configurado en **On**
4. Asegúrese de que el puerto de TLS mutuo se establezca en **5062**
5. Haga clic en **Guardar** como se muestra en la imagen.



Problema 4. Expressway-E o C no admite encabezados de ruta SIP precargados

Con Hybrid Call Service Connect, el enrutamiento de llamadas se realiza en función del **encabezado de enrutamiento**. El encabezado de enrutamiento se completa en función de la información que proporciona a Cisco Webex la parte de la solución que reconoce los servicios de llamadas (conector de Expressway). El host del conector de Expressway solicita a Unified CM los usuarios que están habilitados para el servicio de llamada y extrae sus **URI de directorio y FQDN del clúster del clúster de inicio de Unified CM**. Consulte estos ejemplos sobre Alice y Bob:

URI de directorio	Encabezado de enrutamiento de destino
bob@example.com	emea-cucm.example.com
alice@example.com	us-cucm.example.com

Si Alice o Bob realizan una llamada, la llamada se enruta a su Unified CM en las instalaciones, de modo que pueda anclarse a Cisco WebexRD antes de enrutarla al usuario destinatario de la llamada.

Si Alice llama a Bob, la llamada se enrutaría al *FQDN del clúster de inicio de Unified CM de Alice (us-cucm.example.com).* Si se analiza la SIP INVITE entrante que Cisco Webex envía a Expressway-E, encontrará la siguiente información en el encabezado de SIP

URI de la solicitud	sip: bob@example.com
Encabezado de enrutamiento	sip:us-cucm.example.com;lr

Desde la perspectiva de Expressway, las reglas de búsqueda se configuran para enrutar la llamada no por el URI de solicitud, sino por el **encabezado de ruta (us-cucm.example.com);** en este caso, el clúster principal de Unified CM de Alice.

Una vez establecida esta base, puede comprender las situaciones problemáticas en las que Expressway está mal configurado, lo que impide el funcionamiento de la lógica anterior. Al igual que casi todas las otras fallas de configuración de llamadas entrantes de Hybrid Call Service

Connect, el síntoma es que *no suena el teléfono en las instalaciones*.

Antes de analizar los registros de diagnóstico en Expressway, tenga en cuenta cómo identificar esta llamada:

1. La URI de la solicitud de SIP será la **URI de directorio** *del destinatario de la llamada.*
2. El campo SIP FROM se formateará con la **persona que llama** que se muestra como **"Nombre Apellido" <sip:WebexDisplayName@subdomain.call.ciscospark.com>**

Con esta información, puede buscar en los registros de diagnóstico por **URI de directorio del destinatario de la llamada, nombre y apellido de la persona que llama o dirección de SIP de Cisco Webex de la persona que llama**. Si no dispone de esta información, puede buscar en "**INVITE SIP:**", que localiza todas las llamadas SIP que se ejecutan en Expressway. Una vez que haya identificado SIP INVITE para la llamada entrante, puede buscar y copiar el ID de llamada SIP. Una vez que tenga este valor, simplemente puede buscar los registros de diagnóstico en función del ID de llamada para ver todos los mensajes que coincidan con este segmento de llamada.

Otra manera de aislar el problema de enrutamiento es determinar hasta dónde va la llamada en la empresa. Puede intentar buscar la información indicada anteriormente en Expressway-C para ver si la llamada se enrutó hasta allí. De ser así, es probable que desee iniciar la investigación por allí.

En esta situación, puede ver que Expressway-C ha recibido INVITE de 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: "pstojano 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>
```

Lo importante es que el **encabezado de enrutamiento (FQDN del clúster) sigue intacto.** No obstante, ninguna lógica de búsqueda se realiza en función del encabezado de enrutamiento (FQDN del clúster) **cucm.rtp.ciscotac.net**. Verá que el mensaje se rechaza inmediatamente con un error **404 no 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:pstojano-
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="pstojano-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="pstojano-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:pstojano-
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=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
From: "pstojano 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
```

En comparación con una situación de trabajo, en la situación de trabajo la lógica de búsqueda se realiza en función del encabezado de enrutamiento (FQDN del clúster)

```
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'"**

Entonces puede ver que Expressway-C desvía la llamada correctamente a 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=z9hG4bK297799f31d0785ff7449e1d7dbe3595b271.2ed90cbed5b79c6cffad9ecd84cc8337;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=z9hG4bK043ca6360f253c6abed9b23fbeff9819;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: "pstojano test" <sip:pstojano-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)

Una vez analizado el registro de diagnóstico que aisló el problema en Expressway-C y un error específico (404 no encontrado), puede centrarse en la posible causa de este tipo de comportamiento. Algunos aspectos que debe tener en cuenta son:

1. Las llamadas pasan dentro y fuera de las zonas de Expressway mediante las reglas de

búsqueda.

2. Expressway usa una lógica llamada soporte para enrutamiento SIP precargado que procesa las solicitudes SIP INVITE que tienen encabezado de enrutamiento. Este valor se puede activar o desactivar en las zonas (servidor transversal, cliente transversal, vecino) en Expressway-C y Expressway-E.

Ahora puede usar xConfiguration para ver la configuración del servidor transversal de Expressway-E y las zonas de cliente de Expressway-C, específicamente las configuraciones para Hybrid Call Service Connect. Además de la configuración de zona, puede analizar las reglas de búsqueda configuradas para transmitir esta llamada de una zona a otra. También sabrá que Expressway-E pasó la llamada a Expressway-C, por lo que lo más probable es que la configuración de zona de servidor transversal esté configurada correctamente.

Para desglosar esto, la xConfig siguiente indica que el nombre de esta zona es **Hybrid Call Service Traversal**. El tipo de zona es **TraversalServer.** Se comunica a Expressway-C a través del puerto TCP SIP **7003**.

La pieza clave del servicio de Hybrid Call Service es que debe activarse el soporte de enrutamiento SIP precargado. La interfaz web de Expressway denomina a este valor **soporte para enrutamiento SIP precargado, mientras que xConfiguration lo denomina 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"
```

También se puede determinar que esta zona tiene la regla de búsqueda 3 (Webex híbrida) ligada a ella. En esencia, la regla de búsqueda envía un alias "Any" que proviene de la zona de DNS de Hybrid Call Services y lo transfiere a la zona anterior, Hybrid Call Service Traversal. Según lo esperado, la regla de búsqueda y la zona del servidor transversal de Expressway-E están configuradas correctamente.

```
*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"
```

Si se centra en xConfiguration de Expressway-C, puede empezar por buscar la zona de cliente transversal para los servicios híbridos de Webex. Un método sencillo para encontrarla es buscar en el número de puerto que aprendió en xConfiguration de Expressway-E (**Puerto SIP: "7003"**). Esto ayuda a identificar rápidamente la zona correcta en xConfiguration.

Como antes, puede aprender el nombre de la zona (Hybrid Call Service Traversal), el tipo (cliente transversal), y lo que se ha configurado para SIP PreloadedSipRoutes Accept (soporte para enrutamiento SIP precargado). Como se puede ver en esta xConfiguration, este valor se establece en Off. Según la Guía de implementación de Cisco Webex Hybrid Call Services, este valor debe establecerse en On.

Además, si analizamos la definición de soporte de enrutamiento SIP precargado, podremos ver claramente que Expressway-C debe rechazar un mensaje si este valor se establece en Off e INVITE contiene un encabezado de enrutamiento: "**El soporte de enrutamiento SIP precargado debe estar en Off si desea que la zona rechace las solicitudes SIP INVITE que contengan este encabezado**".

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"
```

A esta altura, ya aisló el problema a una mala configuración de la zona de cliente transversal de Expressway-C. Debe activar el soporte de enrutamiento SIP precargado.

Solución

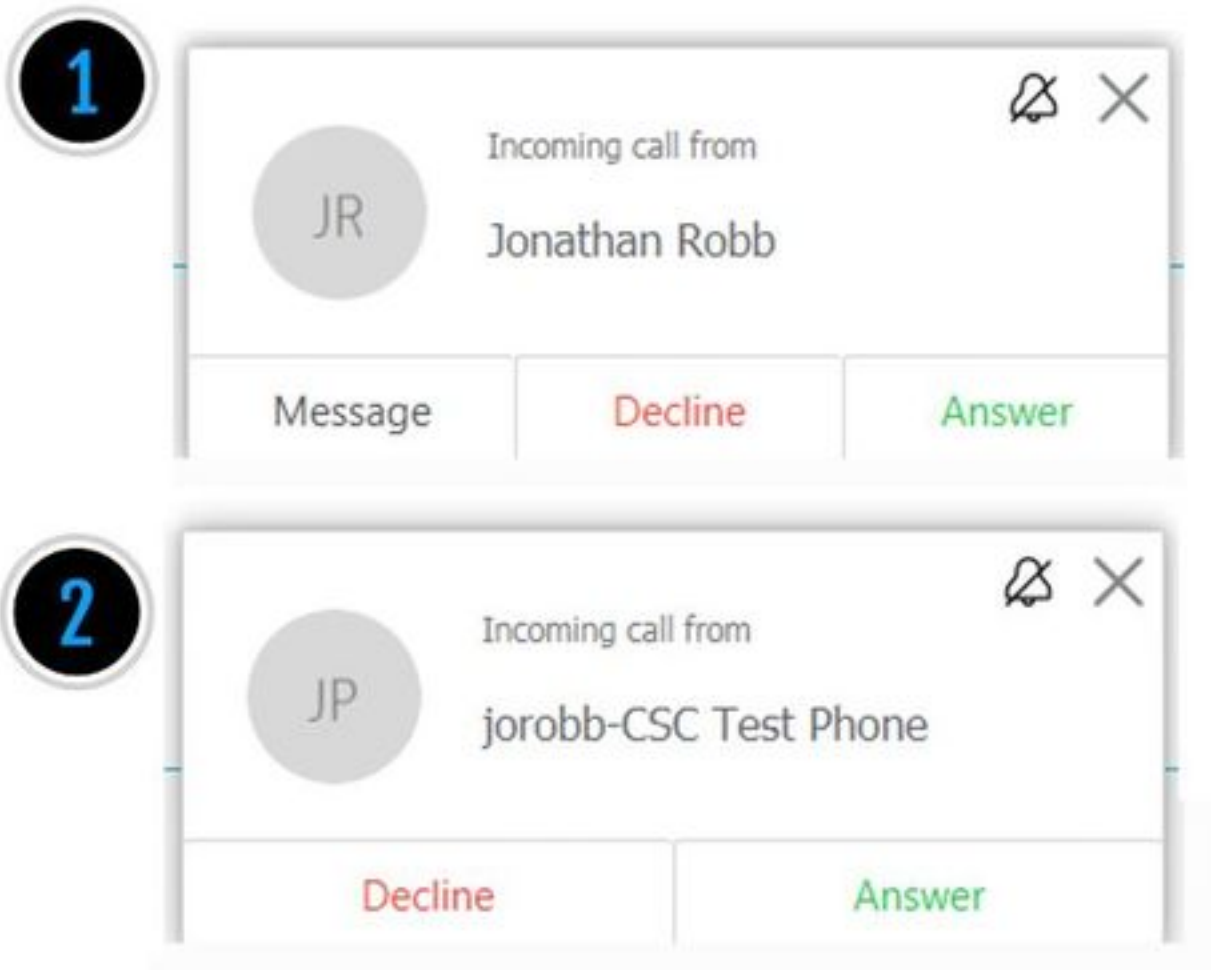
Para configurar correctamente el soporte de enrutamiento SIP precargado:

1. Inicie sesión en Expressway-C
2. Vaya a **Configuración > Zonas > Zonas**
3. Seleccione la zona de cliente transversal de Hybrid Call Service (la nomenclatura varía de un cliente a otro)
4. Configure el **Soporte de enrutamiento SIP precargado** en **On**
5. Seleccione **Save (Guardar).**

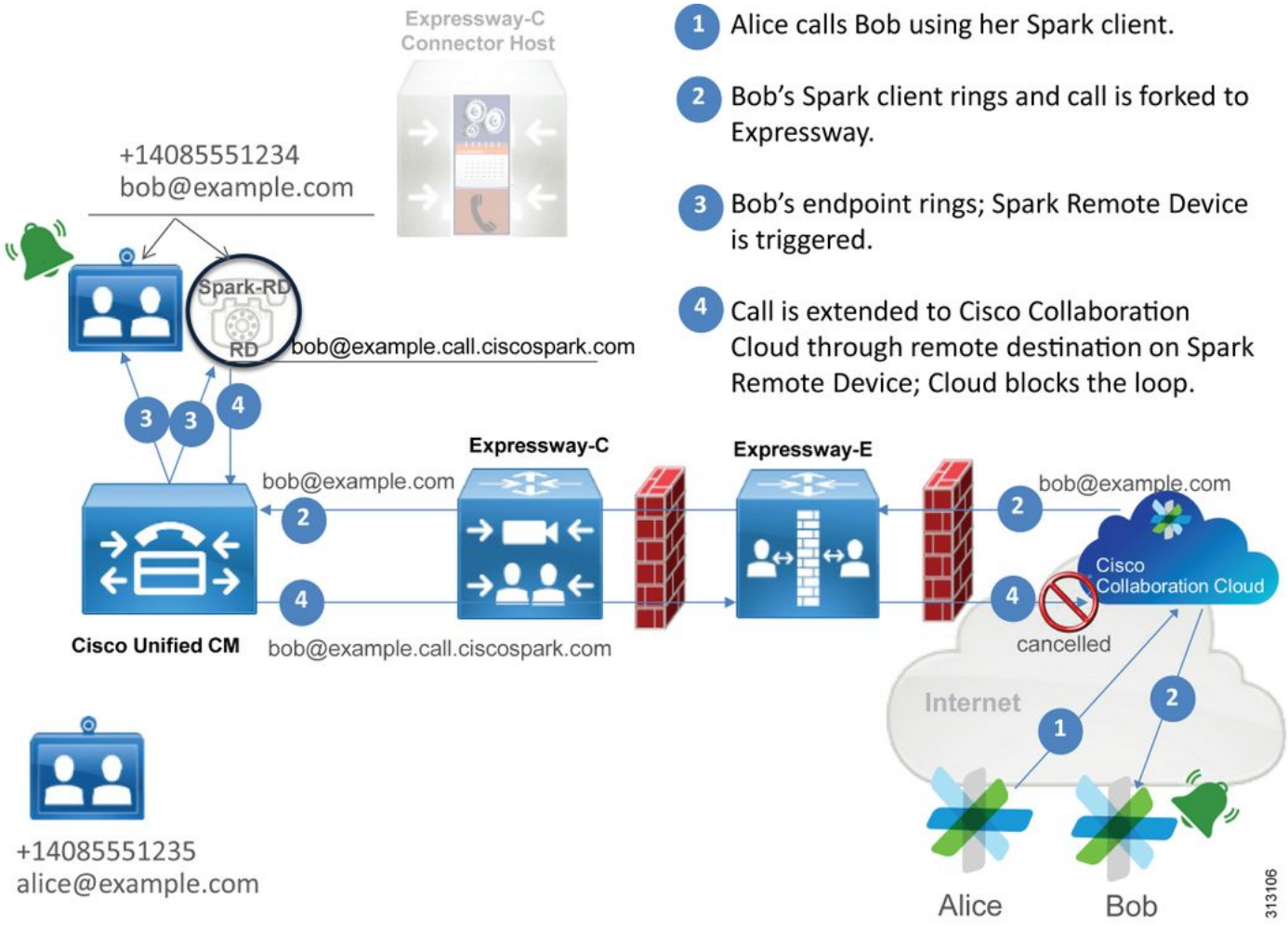
Nota: Mientras que esta situación demostró una falla en Expressway-C, se pueden observar los mismos errores de registro de diagnóstico en Expressway-E si el **soporte de enrutmiento SIP precargado estaba en Off en la zona de servidor transversal de llamadas híbridas de Webex.** En ese caso, nunca hubiera visto a la llamada llegar a Expressway-C y Expressway-E habría sido responsable de rechazar la llamada y enviar el error 404 no encontrado.

Problema 5. La aplicación Cisco Webex está recibiendo dos notificaciones de llamada (toasts)

Este problema en particular es la única situación de llamada entrante en la que no se corta la llamada. Para este problema, la persona que recibe la llamada (destinatario de la llamada) recibe dos notificaciones (mensajes emergentes) en la aplicación Cisco Webex de la persona que hizo la llamada (persona que llama). La primera notificación se genera en Cisco Webex y la segunda notificación proviene de la infraestructura en las instalaciones. A continuación se muestran ejemplos de las dos notificaciones recibidas, como se muestra en la imagen.



La primera notificación (mensaje emergente) es de la persona que inicia la llamada (persona que llama) del lado de Cisco Webex. El ID de la llamada en esta instancia es el nombre en pantalla del usuario que inicia esa llamada. La segunda notificación (mensaje emergente) proviene de la CTI de las instalaciones o del Cisco Webex RD asignado al usuario que realiza la llamada. En primer lugar, este comportamiento parece raro. Sin embargo, si analiza el diagrama de llamada entrante (tomado de la Guía de diseño de llamadas híbridas de Cisco Webex), el comportamiento cobra más sentido, como se muestra en la imagen.



En la ilustración, puede ver que Alice llama a Bob desde su aplicación Cisco Webex y que la llamada se bifurca hasta llegar a las instalaciones. En esta llamada debe coincidir el URI de directorio asignado al teléfono de Bob. El problema es que, con este diseño, el URI de directorio también está asignado a su CTI-RD o Cisco Webex RD. Por lo tanto, cuando la llamada se ofrece a CTI-RD o Cisco Webex RD, la llamada se envía de vuelta a Cisco Webex debido a que el dispositivo tiene un destino remoto configurado para bob@example.call.ciscospark.com. Cisco Webex responde a esta situación cancelando el segmento de llamada en particular.

Para que Cisco Webex cancele correctamente el segmento de llamada, Cisco Webex inicialmente debía colocar un parámetro en el encabezado SIP que buscaría para cancelar ese segmento determinado. El parámetro que Cisco Webex inserta en SIP INVITE se denomina **"call-type=squared" y este valor se ingresa en el encabezado del contacto.** Si se elimina este valor del mensaje, Cisco Webex no sabe cómo cancelar la llamada.

Con esta información, puede volver a analizar la situación anterior en la que la aplicación de Cisco Webex del usuario recibía dos notificaciones (mensajes emergentes) cuando el usuario de Cisco Webex Jonathan Robb realizaba una llamada. Para solucionar problemas de este tipo, siempre debe recopilar el registro de diagnóstico de Expressway-C y Expressway-E. Como punto de partida, puede revisar los registros de Expressway-E para determinar que SIP INVITE en realidad tenga el valor **call-type=squared presente en el encabezado de contacto de la INVITE inicial de Cisco Webex entrantes.** Esto garantizará que el cortafuegos no manipula el mensaje de ninguna forma. A continuación hay un fragmento de ejemplo de INVITE entrante a Expressway-E en esta situación.

```
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:
```

El encabezado de contacto tiene el valor **call-type=squaredpresente.** A esta altura, la llamada debe enrutarse mediante Expressway y enviarse fuera de la zona del servidor transversal híbrido de Webex. Podemos buscar en los registros de Expressway-E para determinar cómo se envió la llamada fuera de Expressway-E. Esto nos dará una idea de si Expressway-E está manipulando INVITE de alguna 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=z9hG4bK52aac9a181192566e01b98ae0280bdff858.0e65cdfe078cabb269eecb6bce132
8be;proxy-call-id=ec51e8da-e1a3-4210-95c9-494d12debcd8;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>
```

Al revisar esta SIP INVITE que se envía desde Expressway-E a Expressway-C, tenga en cuenta que falta **call-type=squared** en el encabezado de contacto. Algo más para mencionar es que en el elemento de línea 4, puede ver que la zona de salida es igual a **HybridCallServiceTraversal**. Ahora puede concluir que el motivo por el que la aplicación Cisco Webex está recibiendo una segunda notificación (mensaje emergente) después del marcado es que Expressway-E elimina la etiqueta **call-type=squared del encabezado de contacto SIP INVITE.** La pregunta que se debe responder es cuál podría ser la causa de este encabezado sin etiqueta.

La llamada debe pasar por Hybrid Call Service Traversal configurado en Expressway, por lo que ese es un buen lugar para iniciar la investigación. Si tiene xConfiguration, puede ver cómo se ha configurado esta zona. Para identificar la zona en xConfiguration, puede usar el nombre registrado en la línea de Via que se imprime en los registros. Puede ver que antes se llamaba egress-zone=HybridCallServiceTraversal. Cuando este nombre se imprime en la línea de Via del encabezado SIP, se eliminan los espacios. El nombre de zona real desde la perspectiva de xConfiguration tendría espacios y el formato de 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: "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"
```

Una vez identificada la configuración de Hybrid Call Service Traversal, puede buscar configuraciones posibles que se destaquen, tales como:

- SIP PreloadedSIPRoutes Accept: Encendido
- SIP ParameterPreservatoin Mode: Desactivado

Con la interfaz web de cualquier Expressway, puede ver la definición de estos valores y qué hacen.

Soporte de enrutamiento SIP precargado

Active el soporte de enrutamiento SIP precargado para permitir que esta zona procese solicitudes SIP INVITE con el encabezado de enrutamiento.

El soporte de enrutamiento SIP precargado debe estar desactivado si desea que la zona rechace las solicitudes SIP INVITE que contengan este encabezado.

Conservación de parámetros SIP

Determina si B2BUA de Expressway conserva o modifica los parámetros en las solicitudes SIP que se enrutan a través de esta zona.

Si se activa esta función, se conservan los parámetros de URI y contacto de solicitud SIP de las solicitudes que se enrutan entre esta zona y B2BUA.
Si se desactiva esta función, B2BUA puede modificar los parámetros de URI y contacto de solicitud SIP de las solicitudes que se enrutan entre esta zona y B2BUA, de ser necesario.
A partir de estas definiciones, xConfiguration y el valor **call-type=squared que se coloca en el encabezado "Contacto" de SIP INVITE, puede concluir que la desactivación del valor de conservación del parámetro SIP en la zona de Hybrid Call Service Traversal es el motivo por el que se elimina la etiqueta y la aplicación Cisco Webex está recibiendo notificaciones de timbre dobles.**

Solución

Para mantener el valor de call-type=squared en el encabezado de contacto de SIP INVITE, debe asegurarse de que Expressway admita la conservación de parámetros SIP para todas las zonas involucradas en la gestión de la llamada:

1. Inicie sesión en Expressway-E
2. Vaya a **Configuración > Zonas > Zonas**
3. Seleccione la zona que se usa para el servidor transversal híbrido
4. Establezca el valor de conservación de parámetros SIP en **On**
5. Guarde las configuraciones.

##########

Nota: En esta situación de ejemplo, la zona de servidor transversal híbrido de Webex en Expressway-E estaba mal configurada. Tenga en cuenta que es totalmente posible que el valor de conservación de parámetros SIP esté desactivado en el cliente transversal híbrido de Webex o en las zonas vecinas de CUCM. Ambas configuraciones se harían en Expressway-C. Si ese fuera el caso, podría esperar que Expressway-E hubiera enviado el valor **call-type=squared** a Expressway-C y que Expressway-C lo hubiera quitado.

Salientes: De las instalaciones a Cisco Webex

Casi todas las fallas de llamadas relacionadas con señales salientes en las instlaciones a Cisco Webex causan el mismo síntoma informado: "Cuando llamo desde mi teléfono registrado en Unified CM a otro usuario habilitado para la conexión del servicio de llamada, su teléfono en las instalaciones suena, pero su aplicación Cisco Webex no". Para solucionar problemas en esta situación, es importante comprender el flujo de llamadas y la lógica que se produce cuando se realiza este tipo de llamada.

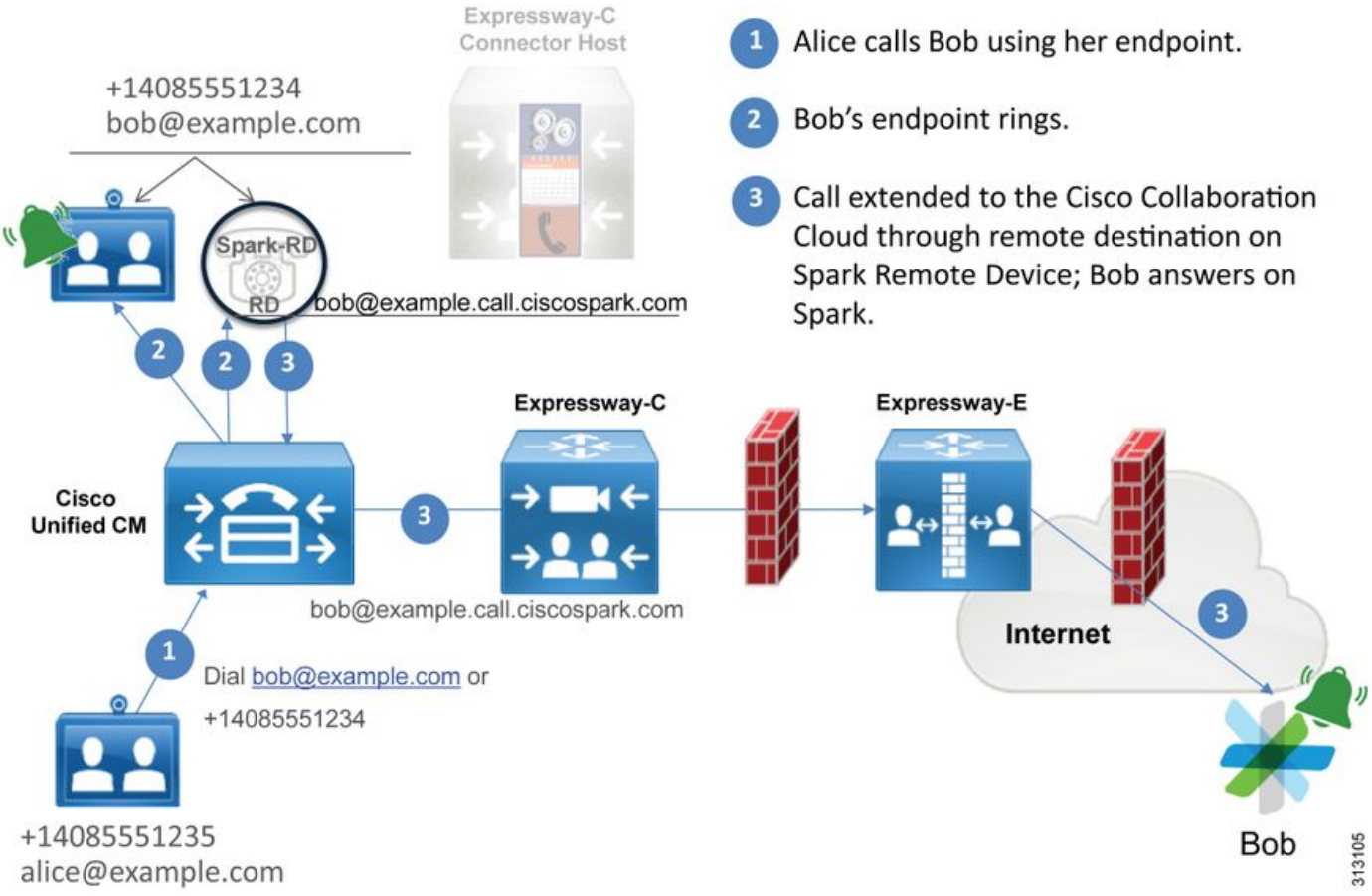
Flujo de lógica de alto nivel

1. El usuario A realiza una llamada desde su teléfono en las instalaciones al URI de directorio del usuario B

2. El teléfono en las instalaciones y CTI-RD/Webex-RD del usuario B aceptan la llamada
3. El teléfono en las instalaciones del usuario B empieza a sonar
4. El CTI-RD/Webex-RD del usuario B bifurca esta llamada al destino de UserB@example.call.ciscospark.com
5. Unified CM pasa esta llamada a Expressway-C
6. Expressway-C envía la llamada a Expressway-E
7. Expressway-E realiza una búsqueda de DNS en el dominio callservice.ciscospark.com
8. Expressway-E intenta conectarse al entorno de Cisco Webex a través del puerto 5062.
9. Expressway-E y el entorno de Cisco Webex inician un intercambio mutuo de señales
10. El entorno de Cisco Webex transfiere la llamada a la aplicación Cisco Webex disponible del usuario B
11. La aplicación Cisco Webex disponible del usuario B empieza a sonar.

Flujo de llamada

Vaya al **teléfono en las instalaciones del usuario B > Unified CM > CTI-RD/Webex-RD > Expressway-C > Expressway-E > Entorno de Cisco Webex > Aplicación Cisco Webex**, como se muestra en la imagen.



Nota: La imagen se obtuvo de la Guía de diseño híbrido de Cisco Webex.

Consejos de análisis de registros

Si estaba solucionando una situación en la que fallaban las llamadas bifurcadas salientes a Cisco WebEx, debe recopilar los registros de Unified CM, Expressway-C y Expressway-E. Con estos conjuntos de registros, puede ver cómo la llamada pasa a través del entorno. Otra forma rápida de comprender hasta dónde llega la llamada dentro de su entorno en las instalaciones es usar el

"Historial de búsqueda" de Expressway. El historial de búsqueda de Expressway rápidamente le permitirá ver si la llamada bifurcada saliente de Cisco WebEx está llegando a Expressway-C o E.

Para usar el historial de búsqueda, puede hacer lo siguiente:

1. Inicie sesión en Expressway-E
   Realice una llamada de prueba
   Vaya a **Estado > Historial de búsqueda**
   Compruebe si puede ver una llamada con una dirección de destino de la URI del SIP de Webex que se debería llamar (user@example.call.ciscospark.com)
   Si el historial de búsqueda no muestra la llamada cuando llega al historial de búsqueda de Expressway-E, repita este proceso en Expressway-C

Antes de analizar los registros de diagnóstico en Expressway, tenga en cuenta cómo identificar esta llamada:

1. La URI del SIP de la solicitud será la dirección SIP del usuario de Cisco Webex
2. Se formateará el campo SIP FROM para que la persona que llama aparezca como "Nombre Apellido" <sip:Alias@Domain>

Con esta información, puede buscar en los registros de diagnóstico por URI de directorio de la persona que llama, nombre y apellido de la persona que llama o dirección de SIP de Cisco Webex del destinatario de la llamada. Si no dispone de esta información, puede realizar una búsqueda en "**INVITE SIP:**", que localizará todas las llamadas SIP que se ejecutan en Expressway. Una vez que haya identificado SIP INVITE para la llamada entrante, puede buscar y copiar el **ID de llamada** SIP. Una vez que tenga este valor, simplemente puede buscar los registros de diagnóstico en función del ID de llamada para ver todos los mensajes que coincidan con este segmento de llamada.

Estos son algunos de los problemas más comunes observados con las llamadas salientes del teléfono registrado en Unified CM al entorno de Cisco Webex cuando se realiza la llamada a un usuario que está habilitado para la conexión del servicio de llamada.

Problema 1. Expressway no puede resolver la dirección callservice.ciscospark.com

El procedimiento operativo estándar para una zona de DNS de Expressway es hacer una búsqueda de DNS basada en el dominio que se muestra en la parte derecha de la URI de la solicitud. Para explicar esto, considere un ejemplo. Si la zona de DNS recibiera una llamada con una URI de solicitud de **pstojano-test@dmzlab.call.ciscospark.com**, una zona de DNS típica de Expressway aplicaría la lógica de búsqueda de SRV de DNS en **dmzlab.call.ciscospark.com, que está del lado derecho de la URI de la solicitud.** Si Expressway fuera a hacer esto, podría esperar que se se produzcan las siguientes búsqueda y respuesta.

```
_sips._tcp.dmzlab.call.ciscospark.com.
Response: 5 10 5061 l2sip-cfa-01.wbx2.com.
l2sip-cfa-01.wbx2.com
Response: 146.20.193.64
```

Si observa detenidamente, verá que la respuesta de registro SRV proporciona una dirección de servidor y el puerto 5061, no 5062.

Esto significa que no se producirá el intercambio mutuo de señales TLS a través del puerto 5062 y se usará otro puerto para la señalización entre Expressway y Cisco Webex. El desafío de esto

es que la *Guía de implementación de Cisco Webex Hybrid Call Services* no indica explícitamente el uso del puerto 5061 debido a que algunos entornos no permiten llamadas interempresariales.

La manera de superar esta lógica estándar de búsqueda de SRV de zona de DNS en Expressway es configurar Expressway para que haga búsquedas explícitas basadas en un valor que usted proporciona.

Al analizar esta llamada concreta, puede centrarse en Expressway-E debido a que determinó (con el historial de búsqueda) que la llamada llegó hasta este punto. Empiece por el primer SIP INVITE que llega a Expressway-E para ver de qué zona proviene, qué reglas de búsqueda se usan, a qué zona va la llamada y, si se la envía correctamente a la zona de DNS, qué lógica de búsqueda de DNS se aplica.

```
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-remotecc: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: 2568978048-0000065536-0000000148-0352430272
```

```
Content-Type: application/sdp
Content-Length: 714

<SDP Omitted>
```

En este SIP INVITE, puede recopilar el URI de solicitud (pstojano-test@dmzlab.call.ciscospark.com), el **ID de llamada** (991f7e80-9c11517a-130ac-1501a8c0), **De** ("Jonathan Robb" <sip:5010@rtp.ciscotac.net>), To (sip:pstojano-test@dmzlab.call.ciscospark.com) y **User-Agent** (Cisco-CUCM11.5). Después de recibido este INVITE, Expressway ahora debe tomar decisiones de lógica para determinar si puede enrutar la llamada a otra zona. Expressway hace esto en función de las reglas de búsqueda.

```
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 'pstojano-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 'pstojano-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 'pstojano-
test@dmzlab.call.ciscospark.com'"
```

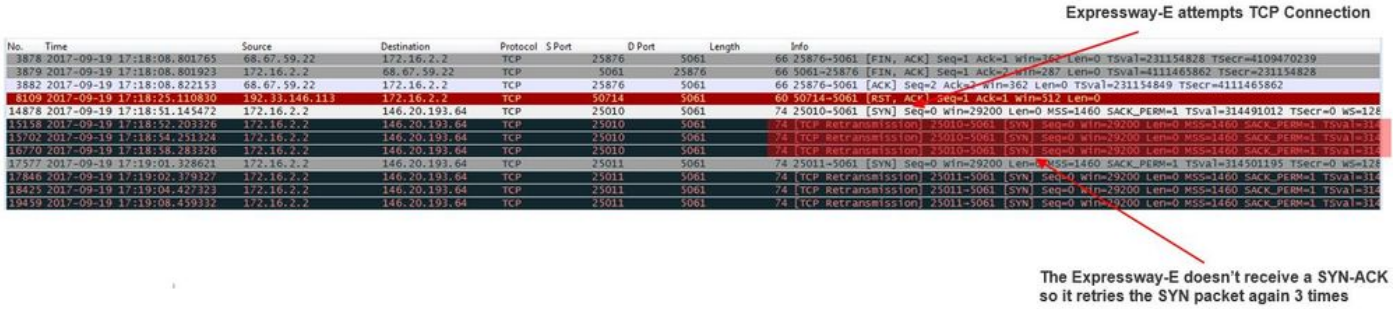
Según el fragmento de registro anterior, puede ver que Expressway-E analizó cuatro reglas de búsqueda, pero solo se consideró una *(*de Webex híbrido a Webex Cloud*).* La regla de búsqueda tiene una prioridad de 90 y se ha diseñado para ir a la zona de DNS de servicios de llamadas híbrido. Ahora que la llamada se envía a una zona de DNS, puede revisar las búsquedas de SRV de DNS que se producen en 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"
```

En el fragmento anterior, puede ver que Expressway-E realizó la búsqueda de SRV basada en el lado derecho del URI de la solicitud (_sips._tcp.dmzlab.call.ciscospark.com) y se ha resuelto por el nombre de host l2sip-cfa-01.wbx2.com y el puerto 5061. El nombre de host l2sip-cfa-01.wbx2.com se resuelve en 146.20.193.64. Con esta información, el siguiente paso lógico que aplicará Expressway es enviar un paquete SYN de TCP a 146.20.193.64 para intentar configurar la llamada. En el registro de Expressway-E, puede comprobar si esto sucede.

```
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"
```

En el fragmento de registro de diagnóstico de Expressway-E anterior, puede ver que Expressway-E está intentando conectarse a la dirección IP 146.20.193.64 que se ha resuelto anteriormente a través del puerto TCP 5061, pero esta conexión falla directamente. Esto mismo puede verse en la captura de paquetes recopilada.



En función de estos resultados, está claro que el tráfico del puerto 5061 no está fluyendo correctamente. Sin embargo, Hybrid Call Service Connect pensaba usar el puerto TCP 5062, no el puerto 5061. Por lo tanto, debe pensar por qué Expressway-E no resuelve un registro de SRV que devolvería el puerto 5062. Para intentar responder esta pregunta, puede buscar posibles problemas de configuración en la zona de DNS híbrido de Webex de 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: "ciscospark.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.ciscospark.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"
```

En xConfiguration de Expressway-E, puede ver que hay dos valores de interés en particular relacionados con las búsquedas de DNS: **DNSOverride Name y DNSOverride Override**. Según esta xConfiguration, DNSOverride Override se configura en Off, por lo tanto, DNSOverride Name no surtiría efecto. Para comprender mejor qué hacen estos valores, puede usar la interfaz de usuario web de Expressway para buscar la definición de los valores.

Modificar la solicitud de DNS *(se traduce a DnsOverride Override en xConfig)*

Enruta las llamadas SIP salientes de esta zona a un dominio de SIP especificado manualmente en vez de usar el dominio del destino marcado. Esta opción está pensada principalmente para usarse con el servicio de llamada de Cisco Webex. Consulte www.cisco.com/go/hybrid-services.

El dominio para buscar (se traduce a DnsOverride Name en xConfig)

Introduzca un FQDN para buscar en DNS en lugar de buscar el dominio en el URI del SIP saliente. URI del SIP original no se ve afectado.

Ahora que ya tiene estas definiciones, está claro que, si estos valores se configuran

correctamente, serían completamente relevantes para la lógica de búsqueda de DNS. Si se une a esto con las instrucciones de la Guía de implementación de Cisco Webex Hybrid Call Services, se encontrará con que la solicitud de modificación de DNS debe estar configurada en **On** y el dominio para buscar debe estar configurado en **callservice.ciscospark.com**. Si fuera a cambiar estos valores para especificar la información correcta, la lógica de búsqueda de SRV de DNS sería completamente diferente. A continuación encontrará un fragmento de lo que se puede esperar desde la perspectiva de registro de diagnóstico de 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"
```

Solución

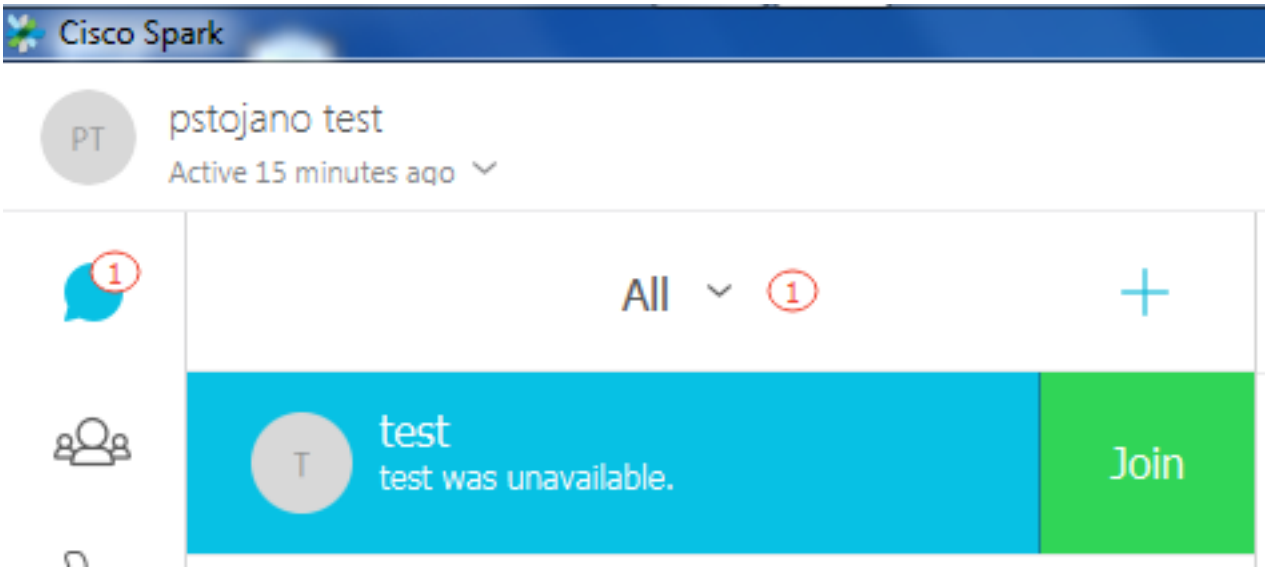
1. Inicie sesión en Expressway-E
2. Vaya a **Zonas de configuración > Zonas**
3. Seleccione la zona de DNS híbrido de Webex configurada
4. Establezca la solicitud de modificación de DNS en **On**
5. Establezca el valor del dominio para buscar en **callservice.ciscospark.com**
6. Guarde los cambios.

> **Nota:** Si hay una sola zona de DNS en uso en Expressway, se debe configurar otra zona de DNS independiente para utilizarse con Hybrid Call Service para aprovechar estos valores.

Problema 2. El puerto 5062 está bloqueado de salida a Cisco Webex

Un aspecto único de los errores de llamadas salientes bifurcadas a Cisco WebEx es que la aplicación Cisco Webex del destinatario de la llamada presentará un botón Unirse en su aplicación aunque el cliente nunca suene. Como la situación anterior, para este problema otra vez tendrá que usar las mismas herramientas y el mismo registro para comprender mejor dónde se encuentra el error. Para leer algunas sugerencias acerca de cómo aislar problemas de llamada y analizar los registros, consulte la sección de este artículo como se muestra en la imagen.

Ilustración del botón Unirse que se presenta



Al igual que para el problema 1 con las llamadas salientes, puede iniciar el análisis en el registro de diagnóstico de Expressway-E, debido a que usó el historial de búsqueda de Expressway para determinar que la llamada está llegando hasta allí. Como antes, comience con la INVITE inicial que entra en Expressway-E desde Expressway-C. Recuerde que las cosas que desea buscar son:

1. Si Expressway-E recibe la INVITE
2. Si la lógica de las reglas de búsqueda transfiere la llamada a la zona de DNS híbrido
3. Si la zona de DNS realiza la búsqueda de DNS y si lo hace en el dominio correcto
4. Si el sistema ha intentado y establecido correctamente un intercambio de señales TCP para el puerto 5062
5. Si el intercambio mutuo de señales TLS tuvo éxito

```
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=z9hG4bK57d8d5c823824bcddfd62f6ff7e09f9939482.899441b6d60c
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-remotecc: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 se puede ver en la INVITE anterior, la INVITE se recibe de manera normal. Se trata de una acción de "recibida" que procede de la dirección IP de Expressway-C. Ya puede pasar a la lógica de las reglas de búsqueda

```
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'"
```

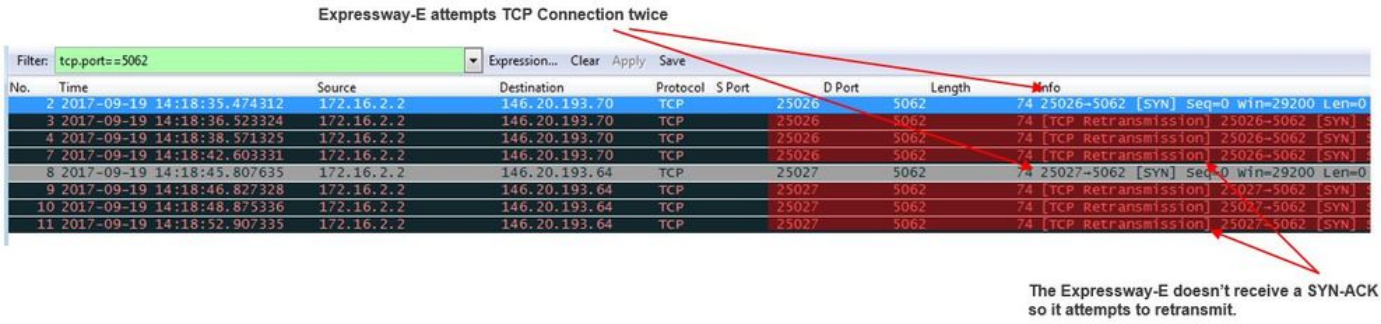
Según el fragmento de registro anterior, puede ver que Expressway-E analizó cuatro reglas de búsqueda, aunque solo una *(Webex híbrido: a Webex Cloud)* fue considerado. La regla de búsqueda tenía una prioridad de 90 y estaba dirigida a la *Zona DNS de servicios de llamadas híbridos*. Ahora que se envía la llamada a una zona DNS, puede revisar las búsquedas de SRV de DNS que se producen en la Expressway-E. Todo esto es completamente normal. Ahora puede centrarse en la lógica de búsqueda de 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"
```

Puede ver claramente que en este caso, el registro SRV callservice.ciscospark.com se ha resuelto. La respuesta son cuatro registros válidos diferentes que usan el puerto 5062. Esto es normal. A esta altura, ya puede analizar el intercambio de señales TCP que debería venir a continuación. Como se menciona anteriormente en el documento, puede buscar la "Conexión TCP" en los registros de diagnóstico y buscar el elemento de línea que muestra Dst-port="5062". A continuación se presenta un ejemplo de lo que verá en esta situación:

```
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"
```

También puede usar el tcpdump incluido con el paquete de registro de diagnóstico para obtener información más detallada sobre el intercambio de señales TCP, como se muestra en la imagen.



A esta altura, puede concluir que Expressway-E enruta la llamada correctamente. El desafío en esta situación es que no se puede establecer una conexión TCP con el entorno de Webex. Esto puede deberse a que el entorno de Webex no responde al paquete SYN de TCP, pero esto sería poco probable, ya que el servidor que maneja la conexión se comparte entre muchos clientes. La causa más probable de esta situación es algún tipo de dispositivo intermediario (cortafuegos, IPS, etc.) que no permite el tráfico de salida.

Solución

Debido a que el problema se ha aislado, se deben proporcionar estos datos al administrador de redes del cliente. Además, si necesitan más información, puede realizar una captura de la interfaz externa del dispositivo de extremo o del cortafuegos como prueba adicional. Desde la perspectiva de Expressway, no se puede tomar ninguna acción adicional porque el problema no se encuentra en ese dispositivo.

Problema 3. Error de configuración de regla de búsqueda de Expressway

Los errores de configuración de reglas de búsqueda son uno de los principales errores de configuración de Expressways. Los problemas de configuración de reglas de búsqueda pueden ser bidireccionales, ya que se necesitan reglas de búsqueda para las llamadas entrantes y para las llamadas salientes. A medida que analice este problema, descubrirá que los problemas de regex son bastante comunes en Expressway, pero no son siempre la causa de un problema de regla de búsqueda. En este segmento en particular, analizará una llamada saliente que provoca un error. Al igual que en todas las situaciones de llamadas bifurcadas salientes, los síntomas son los mismos:

- La aplicación Cisco Webex del destinatario de la llamada presenta el botón Unirse
- El teléfono de la llamada reproduce una señal de llamada
- El teléfono en las instalaciones del destinatario de la llamada estaba sonando
- La aplicación Cisco Webex del destinatario de la llamada nunca sonó

Al igual que en todas las demás situaciones, también querrá aprovechar los rastros de SDL de CUCM junto con los registros de diagnóstico de Expressway-C y E. Como antes, debe consultar para aprovechar el historial de búsqueda y las sugerencias para identificar una llamada en los

registros de diagnóstico. Como antes, se ha determinado con el historial de búsqueda de Expressway-E que esta llamada llega hasta allí y falla. A continuación se muestra el comienzo del análisis en el que se estudia la SIP INVITE inicial que llega a Expressway-E de 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-remotecc: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>
```

Con el ID de llamada (**d58f2680-9c91200a-1c7ba-1501a8c0**) del encabezado SIP, puede buscar rápidamente todos los mensajes asociados a este diálogo. Al observar el tercer resultado de los registros de ID de llamada, puede ver que Expressway-E inmediatamente envía un error **404 no encontrado a 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
```

Estos datos indican dos cosas:

1. Expressway-E nunca intentó enviar la INVITE a Cisco Webex
2. Expressway-E fue el responsable de tomar la decisión lógica de rechazar la llamada con un error 404 no encontrado.

Un error 404 no encontrado generalmente significa que Expressway no puede encontrar la dirección de destino. Dado que Expressway usa reglas de búsqueda para enrutar las llamadas entre sí y los diferentes entornos, empiece por centrarse en la xConfiguration de Expressway-E. Dentro de este xConfiguration, puede buscar la regla de búsqueda que debería transferir la llamada a la zona de DNS híbrido de Webex. Para buscar las reglas de búsqueda configuradas en Expressway desde la perspectiva de xConfiguration, puede buscar "Reglas de búsqueda de políticas de zonas de xConfiguration". Al hacerlo, verá una lista de configuración de reglas de búsqueda para cada regla de búsqueda creada en Expressway. El número que se incluye después de la regla aumenta en función de la regla de búsqueda que se creó por primera vez, que se marca con el 1. Si tiene problemas para encontrar la regla de búsqueda, puede usar valores de nombre utilizados habitualmente, como "*Webex*", para encontrar la regla de búsqueda. Otra forma de identificar la regla es encontrar el valor de la cadena de patrón que se establece en ".*@.*\.ciscospark\.com". Esta es la cadena de patrón que se supone que debe configurar. *(Suponiendo que la cadena de patrón se ha configurado correctamente)*Después de revisar la xConfiguration de esta situación, puede ver que la regla de búsqueda 6 es la regla correcta para transferir la llamada a Cisco Webex.

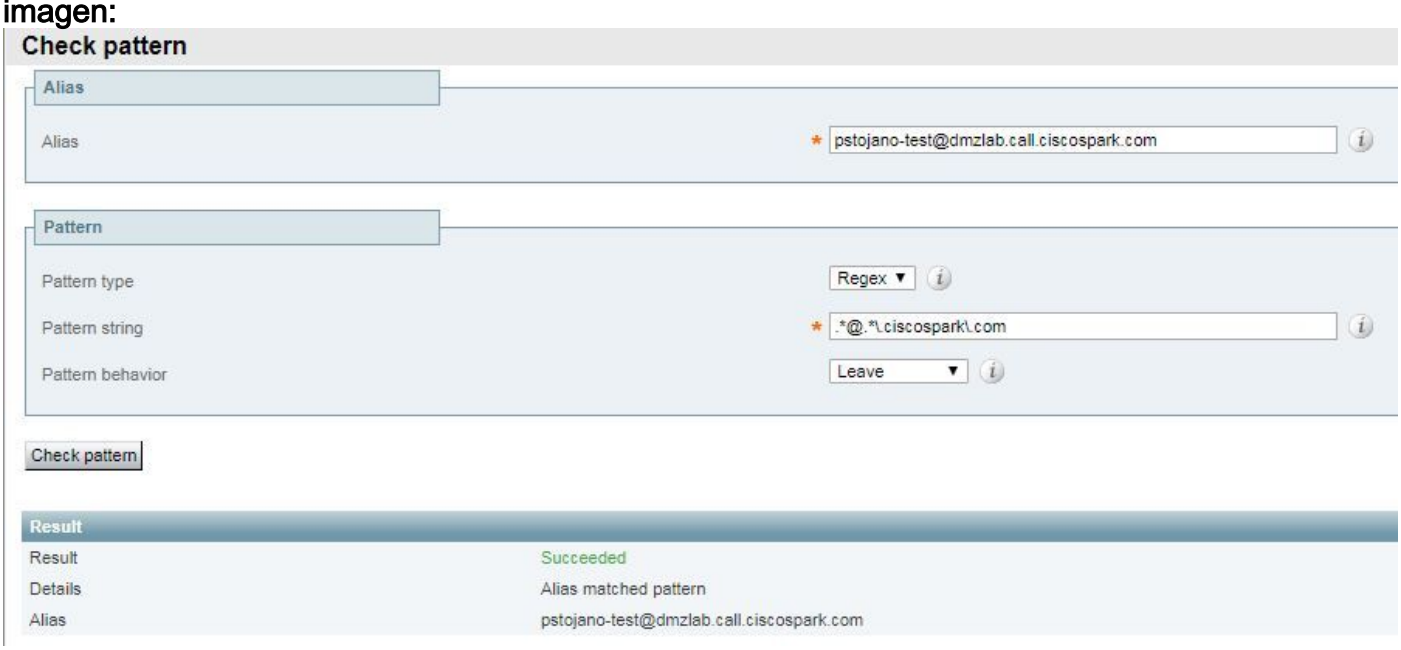
```
*c xConfiguration Zones Policy SearchRules Rule 6 Authentication: "No"
*c xConfiguration Zones Policy SearchRules Rule 6 Description: "Outbound calls to Webex"
*c xConfiguration Zones Policy SearchRules Rule 6 Mode: "AliasPatternMatch"
*c xConfiguration Zones Policy SearchRules Rule 6 Name: "Webex 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: ".*@.*\.ciscospark\.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 comprobar este patrón, podemos usar la función de comprobación de patrón que se describe en. Lo importante aquí es que queremos configurar los siguientes valores:Mantenimiento > Herramientas > Patrón de comprobación

- Alias: URI de la solicitud %Request en la invitación INVITE% inicial (Ej.: pstojano-test@dmzlab.call.ciscospark.com)
- Tipo de patrón: Regex
- Cadena de patrón .*@.*\.ciscospark\.com
- Comportamiento de patrón: Salir

Si el Regex de la regla se ha configurado correctamente, debería ver el resultado de este patrón de verificación con éxito. A continuación hay una ilustración que demuestra como se muestra en la
imagen:



Ahora que confirmó que la regla de búsqueda está presente y configurada correctamente, puede analizar en más detalle la lógica de búsqueda que usa Expressway para determinar si afecta a Expressway-E que envía el error 404 no encontrado. A continuación hay un ejemplo de la lógica de reglas de búsqueda que Expressway estaba usando.

```
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)"
```

En este ejemplo, puede ver que Expressway procesó cuatro reglas de búsqueda. No se consideran las primeras tres por diversos motivos, sin embargo, se considera la cuarta. El dato interesante es que inmediatamente después de la consideración, Expressway salta directamente a la lógica de búsqueda de DNS. Si recuerda lo que hemos visto en xConfiguration, la regla de búsqueda configurada para Webex híbrido se denominaba Webex híbrido a Webex Cloud y ni siquiera se la consideraba en la lógica de regla de búsqueda anterior. A esta altura, es importante examinar cómo se ha implementado la regla de búsqueda considerada (al DNS) para comprender mejor si afecta el uso de la regla de búsqueda de Webex híbrido. Para ello, puede revisar xConfig para buscar la regla de búsqueda denominada "a 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"
```

Después de revisar esta regla de búsqueda, puede concluir lo siguiente:

- La cadena de patrón coincidiría con el URI de la solicitud de Cisco Webex
- La prioridad está establecida en 100
- El progreso (comportamiento del patrón) se establece en Detener.

Esta información nos indica que la URI de la solicitud de Cisco Webex a la que se llama coincidiría con esta regla y, si la regla encuentra coincidencias, Expressway detendría la búsqueda de otras reglas de búsqueda. Con este dato, la prioridad de las reglas se convierte en un factor clave. La prioridad de regla de búsqueda de Expressway se aplica intentando usar la regla de prioridad más baja primero. Aquí tiene un ejemplo.Regla de búsqueda: LocalComportamiento de patrón: ContinúePrioridad 1Regla de búsqueda: VecinoComportamiento de patrón: ContinúePrioridad 10Regla de búsqueda: DNSComportamiento de patrón: DetenerPrioridad 50En este ejemplo, la regla de búsqueda denominada Local (1) se intentaría primero y, si se encuentra una coincidencia, pasaría a la regla de búsqueda vecina (10) debido a que el comportamiento de patrón está configurado en Continuar. Si no coincide con la regla de búsqueda vecina, pasa a la regla de búsqueda de DNS (50) y considera eso en último lugar. Si se encontró una coincidencia con la regla de búsqueda de DNS, la búsqueda se detiene, independientemente de si hay otra regla de búsqueda con una prioridad superior a 50, porque el comportamiento del patrón estaba configurado en Detener. Con esto en mente, puede analizar las prioridades de regla de búsqueda entre las reglas "a DNS" y "Webex híbrido a 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"
```

Aquí puede ver que la regla "a DNS" tiene una prioridad menor que la regla "Webex híbrido - a Webex Cloud"; por lo tanto, la regla "a DNS" se probará primero. Dado que el comportamiento de patrón (Progreso) se establece en Detener, Expressway-E no considera nunca la regla Webex híbrido a Webex Cloud y la llamada termina fallando. SoluciónEste tipo de problema es cada vez más común con Hybrid Call Service Connect. Muchas veces cuando se implementa la solución, las personas crean una regla de alta prioridad para usar en las búsquedas de Cisco Webex. Muchas veces esta regla que se crea no se invoca debido a que hay reglas de menor prioridad que coinciden y producen un error. Este problema se produce en las llamadas entrantes y salientes a Cisco Webex. Para resolver este problema, debe seguir estos pasos:

1. Inicie sesión en Expressway-E
2. Vaya a Configuración > Plan de marcación > Reglas de búsqueda
3. Busque la regla de búsqueda de Webex híbrido y haga clic en ella *(Ej.: Nombre: WebEx híbrido a Webex Cloud)*
4. Establezca el valor de prioridad en un valor inferior que las otras reglas de búsqueda, pero lo suficientemente alto como para que no afecte a los demás. *(Ej.: Prioridad: 99)*

La regla general para las reglas de búsqueda es que cuanto más específica es la cadena de patrón, más baja se puede ubicar en la lista de prioridades de regla de búsqueda. Por lo general, una zona de DNS se configura con una cadena de patrón que captura todo lo que no es un dominio local y lo envía a Internet. Debido a esto, se recomienda que configure ese tipo de regla de búsqueda con una prioridad alta para que se invoque última. Problema 4. error de configuración de CPL de ExpresswayLa solución de Expressway permite mitigar el fraude telefónico con la lógica de lenguaje de procesamiento de llamadas (CPL) disponible en el servidor. Si la solución de Expressway que se implementará solo se usa para Cisco Webex Hybrid Call Service y Mobile & Remote Access, se recomienda encarecidamente que la política y las reglas de CPL estén habilitadas e implementadas. La configuración de CPL en Expressway para Cisco Webex híbrido es bastante sencilla, pero si la configuración es incorrecta, puede bloquear fácilmente los intentos de llamada. Las situaciones siguientes muestran cómo usar el registro de diagnóstico para identificar un error de configuración de CPL.Al igual que en todas las situaciones de llamadas bifurcadas salientes, los síntomas son los mismos:

- La aplicación Cisco Webex del destinatario de la llamada presenta el botón Unirse
- El teléfono de la llamada reproduce una señal de llamada
- El teléfono en las instalaciones del destinatario de la llamada estaba sonando
- La aplicación del destinatario de la llamada nunca sonó

Al igual que en todas las demás situaciones, puede usar los rastros de SDL de CUCM junto con los registros de diagnóstico de Expressway-C y E. Como antes, debe hacer referencia al para utilizar el historial de búsqueda y consejos para identificar una llamada en los registros de diagnóstico. Como antes, se ha determinado con el historial de búsqueda de Expressway-E que esta llamada llega hasta allí y falla. A continuación se muestra el comienzo del análisis en el que se estudia la SIP INVITE inicial que llega a Expressway-E de 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.ciscospark.com SIP/2.0
 Via: SIP/2.0/TLS 192.168.1.5:5061;egress-
zone=HybridCallServiceTraversal;branch=z9hG4bK781a130d234ed9aaec868343687394302832 56.34216c32a0d
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-remotecc: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=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: 4fffefed-0512-4067-ac8c-35828f0a1150
 Session-ID: 75957d4fb66a13e835c10737aa512577;remote=00000000000000000000000000000000
 Cisco-Guid: 3224432896-0000065536-0000000264-0352430272
 Content-Type: application/sdp
 Content-Length: 714

<SDP Omitted>
```

Con el ID de llamada (c030f100-9c916d13-1cdcb-1501a8c0) del encabezado SIP, puede buscar rápidamente entre todos los mensajes asociados con este cuadro de diálogo. Al observar el tercer resultado de los registros de ID de llamada, puede ver que Expressway-E inmediatamente envía un error 403 no permitido a 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="91954361011l0134622"
 SIPMSG:
 |SIP/2.0 403 Forbidden
 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;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 comprender por qué Expressway-E rechazó esta llamada y envió un error 403 no permitido a Expressway-C, debe analizar las entradas de registro entre el error 403 no permitido y la SIP INVITE original que llegó a Expressway. Al analizar estas entradas de registro, por lo general, puede ver todas las decisiones de lógica que se realizan. Tenga en cuenta que no se ven las reglas de búsqueda que se invocan, pero se ve la lógica de idioma de proceso llamada (CPL) que se invoca. A continuación hay un fragmento de esto.

```
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:
```

```
        "
```

Según el análisis de registro anterior, puede tomar la determinación de que el CPL rechaza la llamada.

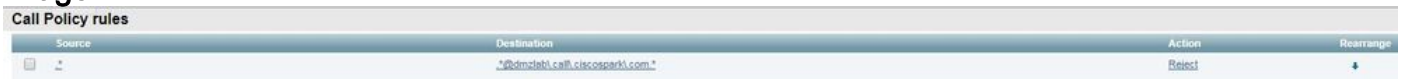
```
2017-09-25T16:54:43.725-04:00 amer-expressway01 tvcs: Event="Search Completed"
Reason="Forbidden" Service="SIP" Src-alias-type="SIP" Src-alias="5010@rtp.ciscotac.net" Dst-
alias-type="SIP" Dst-alias="sip:pstojano-test@dmzlab.call.ciscospark.com" Call-serial-
number="48c80582-ec79-4d89-82e2-e5546f35703c" Tag="4fffefed-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"
```

*Nota: En esta situación, no verá las reglas de búsqueda que se invocan porque los CPL, FindMe y las transformaciones se procesan antes que una regla de búsqueda*En la mayoría de los casos, puede aprovechar la xConfig de Expressway para comprender mejor las circunstancias. Sin embargo, para las CPL, no puede ver las reglas que se han establecido, solo si la política está activada. A continuación, encontrará la parte de xConfig que muestra que Expressway-E está usando la lógica de CPL Local.

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

Para comprender mejor la configuración de reglas, deberá iniciar sesión en Expressway-E y diríjase a Configuración > Política de llamadas > Reglas, como se muestra en la

imagen.



Al revisar esta configuración, puede ver la siguiente configuraciónFuente: .*Destino: .*@dmzlab\.call\.ciscospark\.com.*Acción: RechazarEn comparación con lo que se ha documentado en la *Guía de implementación de Cisco Webex Hybrid Call Service*, puede ver que el Origen y Destino se configuraron al
revés.

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

SoluciónPara resolver este problema, debe reajustar la configuración de la regla CPL para que el origen esté configurado en .*@%Webex_subdomain%\.call\.ciscospark\.com.* y el patrón de destino sea .*

1. Inicie sesión en Expressway-E
2. Vaya a Configuración > Política de llamadas > Reglas
3. Seleccione la regla configurada para el servicio de llamada de Cisco Webex híbrido
4. Introduzca el patrón de origen como .*@%Webex_subdomain%\.call\.ciscospark\.com.*(Ejemplo: .*@dmzlab\.call\.ciscospark\.com.*)
5. Introduzca el patrón de destino como .*
6. Seleccione Save (Guardar).

Para obtener más información sobre la implementación de CPL para Webex híbrido, consulte la Guía de diseño de Cisco Webex híbrido. Bidireccionales: De Cisco Webex a las instalaciones o de las instalaciones a Cisco Webex Problema 1. El terminal de colaboración/teléfono IP ofrece un códec de audio distinto de G.711, G.722 o AAC-LD.Hybrid Call Service Connect es compatible con tres códecs de audio diferentes: G.722, G.711 y AAC-LD. Para establecer correctamente una llamada con el entorno de Cisco Webex, se debe usar uno de estos códecs de audio. El entorno en las instalaciones puede configurarse para que use varios tipos de códecs de audio, pero también puede configurarse para restringirlos. Esto puede suceder de forma intencional o sin intención por el uso de ajustes regionales personalizados o predeterminados en Unified CM. Para este comportamiento específico, los patrones de registro pueden diferir en función de la dirección de la llamada y si Unified CM se ha configurado para usar la oferta anticipada o diferida. A continuación se muestran ejemplos de algunas situaciones diferentes donde se podría presentar este comportamiento:

1. Cisco Webex envía un mensaje INVITE entrante con SDP que ofrece G.711, G.722, o AAC-LD. Expressway-C envía este mensaje a Unified CM, pero Unified CM está configurado para permitir solo G.729 para esta llamada. Por lo tanto, Unified CM rechaza la llamada debido a que no hay ningún códec disponible.
2. Unified CM intenta la llamada saliente como *oferta anticipada a Cisco Webex, lo que significa que la INVITE inicial enviada a Expressway-C tendrá SDP ONLY compatible con audio G.729.* Cisco Webex envía un 200 OK con SDP que elimina el audio (*m=audio 0*

RTP/SAVP) porque no admite G.729. Una vez que Expressway-C pasa este mensaje INVITE a Unified CM, Unified CM finaliza la llamada porque no hay un códec disponible.

3. Unified CM intenta la llamada saliente como *oferta diferida a Cisco Webex, lo que significa que la INVITE inicial enviada a Expressway-C no tendrá SDP.* Cisco Webex envía un 200 OK con SDP que contiene todos los códecs de audio compatibles que admite Cisco Webex. Expressway-C envía este mensaje 200 OK a Unified CM, pero Unified CM solo está configurado para permitir G.729 para esta llamada. Por lo tanto, Unified CM rechaza la llamada debido a que no hay ningún códec disponible.

Si está tratando de identificar un error de llamada de Hybrid Call Service Connect que coincida con este problema, debe obtener los registros de Expressway además de los rastros de SDL de Unified CM. Los fragmentos de registro de ejemplo que encontrará a continuación coinciden con la situación 2, donde Unified CM está intentando la llamada saliente como *oferta anticipada*. Como sabemos que la llamada está saliendo a Cisco WebEx, el análisis de registro se inicia en Expressway-E.A continuación se muestra un fragmento de la INVITE inicial a Cisco Webex. Puede ver que el códec de audio preferido está configurado en G.729 (carga útil 18). El 101 es para DTMF y en esta situación en particular no es 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-55aedea256d2;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=z9hG4bKfcf4cfd09d213a88bd2331cef0bc82b540559.494a140082bd
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-
55aedea256d2@64.102.241.236:5062;transport=tls;lr>
Record-Route: <sip:proxy-call-id=a3a78ee2-c01b-4741-b29b-
55aedea256d2@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
```

En respuesta a este mensaje INVITE inicial, Cisco Webex responde con un mensaje 200 OK. Si analiza este mensaje más detenidamente, puede ver que el códec de audio se pone a cero. Esto es problemático porque sin un puerto de audio asignado, la llamada no podrá negociar esa transmisión.

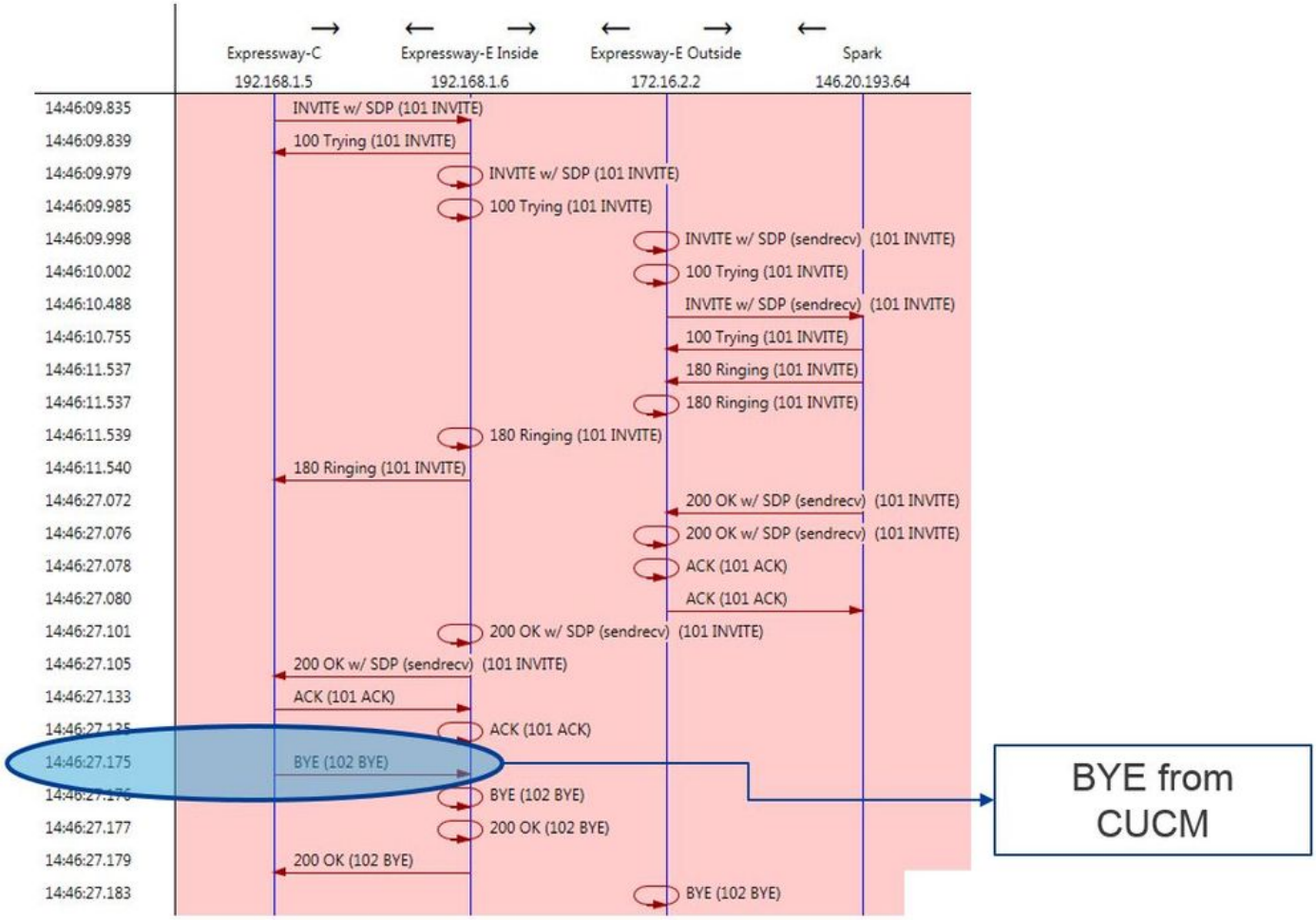
```
2017-09-19T10:46:27.073-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 14:46:27,072"
Module="network.sip" Level="DEBUG":  Action="Received" Local-ip="172.16.2.2" Local-port="25034"
Src-ip="146.20.193.64" Src-port="5062" Msg-Hash="5236578200712291002"
SIPMSG:
SIP/2.0 200 OK
Via: SIP/2.0/TLS 64.102.241.236:5062;egress-
zone=HybridCallServicesDNS;branch=z9hG4bK323e6b15ad0cbbf409751f67848136fa1115;proxy-call-
id=a3a78ee2-c01b-4741-b29b-55aedea256d2;rport=38245;received=192.168.5.26,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,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=z9hG4bKfcf4cfd09d213a88bd2331cef0bc82b540559.494a140082bd
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-55aedea256d2@64.102.241.236:5062;transport=tls;lr>,<sip:proxy-call-id=a3a78ee2-
c01b-4741-b29b-55aedea256d2@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
```

Ahora puede usar TranslatorX para revisar el resto del cuadro de diálogo. Puede ver que el cuadro de diálogo se completa con un ACK. El problema se produce inmediatamente después de que se complete el diálogo, hay un BYE que viene de la dirección de Expressway-C, como se muestra en la
imagen.



Aquí hay un ejemplo detallado del mensaje BYE. Puede ver claramente que el agente usuario es Cisco-CUCM11.5, lo que significa que el mensaje se generó en Unified CM. Otro aspecto que se puede destacar es que el código de motivo está configurado en cause=47. La traducción común para esto es Ningún recurso disponible.

```
2017-09-19T10:46:27.175-04:00 amer-expressway01 tvcs: UCTCTime="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-TAATag: 14a0bd87-1825-4ecf-9f3d-4a23cfa69725
Reason: Q.850 ;cause=47
Session-ID: 75957d4fb66a13e835c10737aa329445;remote=ed35426ed3ade6fdc3b058792333df2b
Content-Length: 0
```

Debido a que el componente de Cisco Webex puso a cero el códec de audio para este ejemplo de llamada, el enfoque debe estar en:a. el mensaje INVITE inicial enviado a Cisco Webex yb. la lógica de Cisco Webex utilizada para poner en cero ese puerto.Al observar qué hace único al

mensaje INVITE inicial, se observa que solo contiene G.729. Con esta información, revise la Guía de implementación de Cisco Webex Hybrid Call Service y consulte específicamente el capítulo de preparación del entorno; en el paso 5 de la sección Complete los requisitos previos para Hybrid Call Service Connect, se mencionan los códecs específicos que son compatibles. Allí vería esto:Cisco Webex es compatible con los siguientes códecs:

- Audio: G.711, G.722, AAC-LD
- Video: H.264

Nota: El Opus no se utiliza en el segmento en las instalaciones de la llamada para la llamada híbrida de Cisco Webex. Con esta información, puede concluir que Unified CM está enviando un códec de audio no compatible que hace que Cisco Webex ponga a cero el puerto. Solución:Para abordar esta situación concreta, es posible que deba revisar la configuración regional entre Cisco Webex RD que está anclando la llamada en las instalaciones y el troncal SIP para Expressway-C. Para ello, determine en qué grupo de dispositivos se encuentran estos dos elementos. El grupo de dispositivos contiene las asignaciones a las regiones. Para determinar el grupo de dispositivos de la línea troncal SIP de Expressway-C:

1. Inicie sesión en Unified CM.
2. Vaya a Dispositivo > Troncal.
3. Busque el nombre del enlace troncal o haga clic en Buscar.
4. Seleccione la línea troncal de Expressway-C.
5. Registre el nombre del grupo de dispositivos.

Para determinar el grupo de dispositivos de CTI-RD o Cisco Webex-RD que ancló la llamada:

1. Vaya a Device > Phone.
2. Al buscar, puede seleccionar Device Type (Tipo de dispositivo) que contiene Webex o CTI Remote Device (Dispositivo remoto CTI) (en función de lo que esté utilizando el cliente).
3. Registre el nombre del grupo de dispositivos.

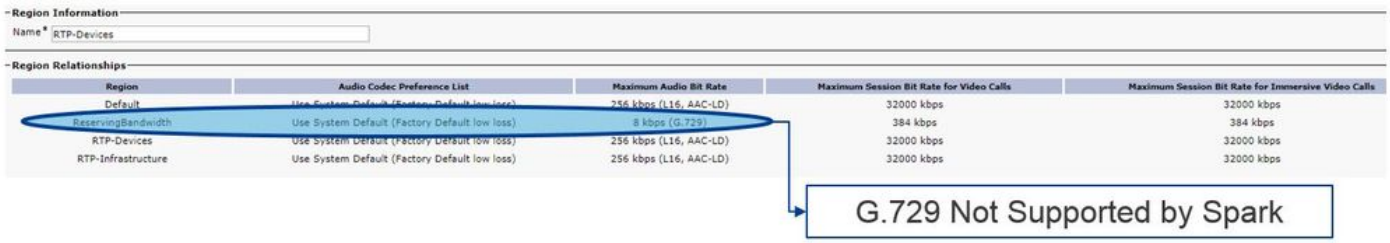
Determine la región conectada a cada grupo de dispositivos:

1. Vaya a System > Device Pool.
2. Busque el grupo de dispositivos que se usa para las líneas troncales SIP de Expressway-C.
3. Haga clic en el grupo de dispositivos.
4. Registre el nombre Región.
5. Busque el grupo de dispositivos que se usa para Webex-RD o CTI-RD.
6. Haga clic en el grupo de dispositivos.
7. Registre el nombre Región.

Determine la relación regional:

1. Vaya a System > Region information > Region.
2. Busque en una de las regiones identificadas.
3. Determine si existe una relación de región entre ambas regiones que utilizan G.729.

A esta altura, si identifica la relación que usa G.729, deberá ajustar la relación para que admita los códecs de audio compatibles que Cisco Webex usa o usar otro grupo de dispositivos con una región que admita esto. En la situación que se describe anteriormente, se determina lo siguiente:Región de enlace troncal de Expressway-C: ReservingBandwidthRegión de WebEx: Dispositivos de RTPA continuación, se muestra una ilustración gráfica de la relación entre las regiones de dispositivos RTP y Ancho de banda reservado, como se muestra en la imagen.



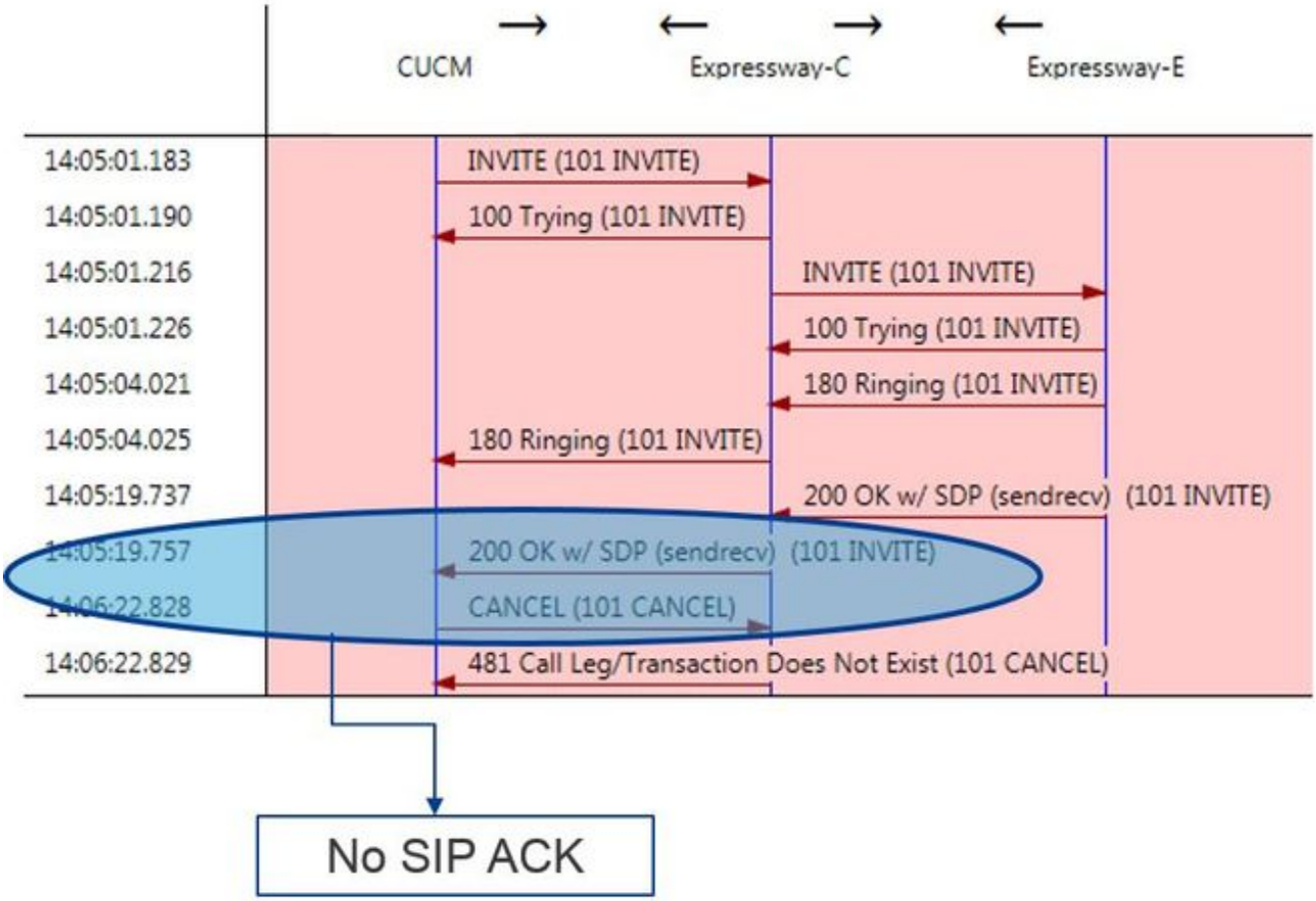
Al cambiar el grupo de dispositivos donde estaba el enlace troncal de Expressway-C, cambia la relación de la región. El nuevo grupo de dispositivos tenía una región establecida en infraestructura de RTP, por lo tanto, la nueva relación de región entre Cisco Webex-RD y el enlace troncal de Expressway-C era de dispositivos de RTP e infraestructura de RTP. Como se muestra, puede ver que esta relación es compatible con AAC-LD, que es uno de los códecs de audio compatibles con Cisco Webex, por lo que la llamada se configurará correctamente. Problema 2. Se ha superado el tamaño máximo de mensajes entrantes de Unified CMDebido a que el video se ha vuelto más frecuente en la empresa, el tamaño de los mensajes SIP que contienen SDP ha aumentado considerablemente. Los servidores que procesan estos mensajes deben configurarse de tal manera que puedan aceptar un paquete grande. En muchos servidores de control de llamadas, los valores predeterminados están bien. Con Cisco Unified Communications Manager (Unified CM), los valores predeterminados de versiones anteriores para manejar un mensaje SIP grande con SDP no eran aptos. En las versiones posteriores de Unified CM, se ha aumentado el tamaño de valor permitido para un mensaje SIP, aunque este valor sólo se establece en las instalaciones nuevas, no en las actualizaciones. Con esto, sin embargo, los clientes que estén actualizando sus versiones anteriores de Unified CM para admitir Hybrid Call Service Connect podrían verse afectados por el tamaño máximo de mensajes entrantes en Unified CM, que es demasiado bajo.Si está tratando de identificar un error de llamada de Hybrid Call Service Connect que coincida con este problema, debe obtener los registros de Expressway además de los rastros de SDL de Unified CM. Para identificar la falla, primero, entienda qué sucede y luego los tipos de escenarios en los que puede ocurrir la falla.Para responder a la pregunta de qué sucede, debe saber que una vez que Unified CM recibe un mensaje SIP demasiado grande, simplemente cierra el socket TCP y no responde a Expressway-C.Dicho esto, hay muchas formas y situaciones en las que puede ocurrir esto:

1. Cisco Webex envía un mensaje INVITE entrante con SDP que es demasiado grande. Expressway-C pasa esto a Unified CM y Unified CM cierra el socket TCP y el cuadro de diálogo de SIP agota el tiempo de espera.

2. Unified CM intenta la llamada saliente como oferta anticipada a Cisco Webex, lo que significa que la INVITE inicial enviada a Expressway-C tendrá SDP. Cisco Webex envía un 200 OK con SDP de respuesta y la respuesta de 200 OK cuando pasa de Expressway-C a Unified CM es demasiado grande. Unified CM cierra el socket TCP y el cuadro de diálogo SIP agota el tiempo de espera.

3. Unified CM intenta la llamada saliente como oferta diferida a Webex, lo que significa que la INVITE inicial enviada a Expressway-C no tendrá SDP. Cisco Webex envía un 200 OK con SDP y la oferta de 200 OK cuando pasa de Expressway-C a Unified CM es demasiado grande. Unified CM cierra el socket TCP y el cuadro de diálogo SIP agota el tiempo de espera.

Buscar esta condición en particular en los registros de Expressway-C ayuda a entender el flujo de mensajes. Si utilizara un programa como TranslatorX, podría ver que Expressway-C está pasando el Cisco Webex 200 OK con SDP a Unified CM. El desafío es que Unified CM nunca responde con una ACK de SIP, como se muestra en la imagen.



Como Unified CMi es responsable de no responder, es importante revisar los rastros de SDL para ver cómo Unified CM maneja esta condición. Lo que encontraría en esta situación es que Unified CM ignora el mensaje grande de Expressway-C. Se imprimirá un elemento lógico como este.

```
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.
```

Una vez que se agote el tiempo de espera del diálogo SIP, Cisco Webex enviará un mensaje de rechazo de SIP 603 entrante a Expressway-E, como se indica en el ejemplo de registro.

```
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 se ha mencionado, hay tres escenarios diferentes en los que puede ver este comportamiento. Para mayor claridad, estos ejemplos de registro coinciden con la situación 3, donde la llamada saliente se envió a Cisco Webex como oferta diferida. Solución:

1. Inicie sesión en Unified CM.
2. Vaya a System > Service Parameters.
3. Seleccione el servidor que está ejecutando el servicio de Call Manager.
4. Elija el servicio Cisco Call Manager cuando se le solicite una selección de Servicio.

5. Seleccione la opción avanzada.
6. En los parámetros clusterwide (dispositivo - SIP), cambie el Tamaño máximo de mensaje SIP entrante a 18000.
7. Seleccione Guardar.
8. Repita este proceso para cada nodo de Unified CM que esté ejecutando el servicio Call Manager de Cisco.

Nota: Para que un teléfono IP, un terminal de colaboración o un enlace troncal SIP aproveche esta configuración, se lo debe reiniciar. Estos dispositivos se pueden reiniciar individualmente para minimizar el impacto en el entorno. NO reinicie todos los dispositivos de CUCM a menos que sepa que es absolutamente aceptable hacerlo.

AppendixHerramientas para la resolución de problemas de Expressway

Compruebe la utilidad del patrónExpressway tiene una utilidad de comprobación de patrones que es útil cuando desea comprobar si un patrón coincide con un alias determinado y se transforma de forma esperada. La utilidad puede encontrarse en Expressway en la opción de menú Mantenimiento > Herramientas > Verificar patrón. Normalmente, esto se utiliza si desea comprobar si el regex de regla de búsqueda va a coincidir correctamente con un alias en una cadena de patrón y, opcionalmente, realizar correctamente la manipulación de la cadena. Para Hybrid Call Service Connect, también puede probar que el FQDN de clúster de Unified CM coincidirá con la cadena de patrón configurada para el FQDN de clúster de Unified CM. Al usar esta utilidad, recuerde que la llamada se enrutará en función del parámetro de FQDN de clúster de Unified CM que aparecen en el encabezado de enrutamiento, no en el URI de destino. Por ejemplo, si la invitación siguiente llega a Expressway, pruebe la función de verificación de patrón con cucm.rtp.ciscotac.net, no con jorobb@rtp.ciscotac.net.

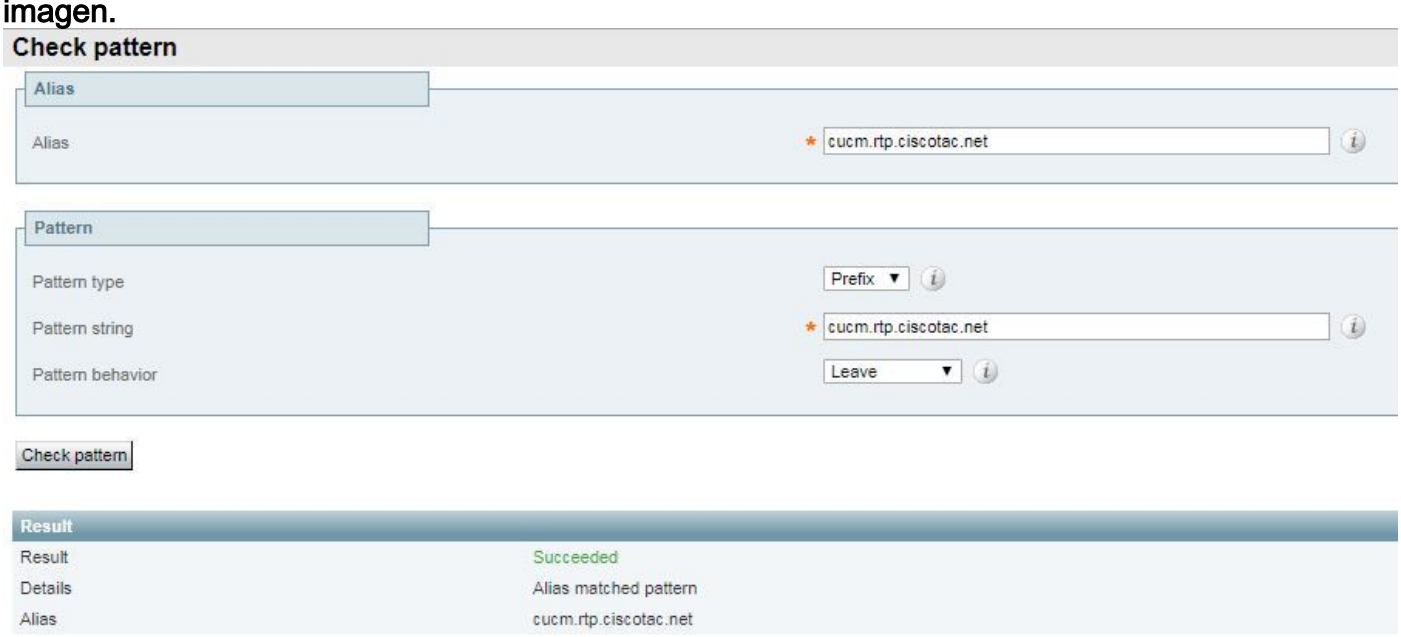
```
SIPMSG:
|INVITE sip:jorobb@rtp.ciscotac.net SIP/2.0
Via: SIP/2.0/TLS 192.168.1.6:7003;egress-
zone=HybridCallServiceTraversal;branch=z9hG4bKcac6d95278590991a2b516cf57e75827371;proxy-call-
id=abcba873-eaae-4d64-83b4-c4541d4e620c;rport
Via: SIP/2.0/TLS 192.168.1.6:5073;branch=z9hG4bK837b03f2cd91b6b19be4fc58edb251bf12;x-cisco-
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: "pstojano test" <sip:pstojano-test@dmzlab.call.ciscospark.com>;tag=145765215
To: <sip:jorobb@rtp.ciscotac.net>
Max-Forwards: 15
Route:
```

Para utilizar Check pattern para probar el ruteo de regla de búsqueda de encabezado de Hybrid Call Service Connect Route, siga estos pasos:

1. Vaya a Mantenimiento > Herramientas > Patrón de comprobación.
2. Para Alias, introduzca el FQDN de clúster de Unified CM.
3. Establezca el Tipo de patrón en Prefijo.
4. Establezca la cadena de patrón en FQDN de clúster de Unified CM.

5. Establezca el comportamiento del patrón en Leave.
6. Seleccione Patrón de verificación.

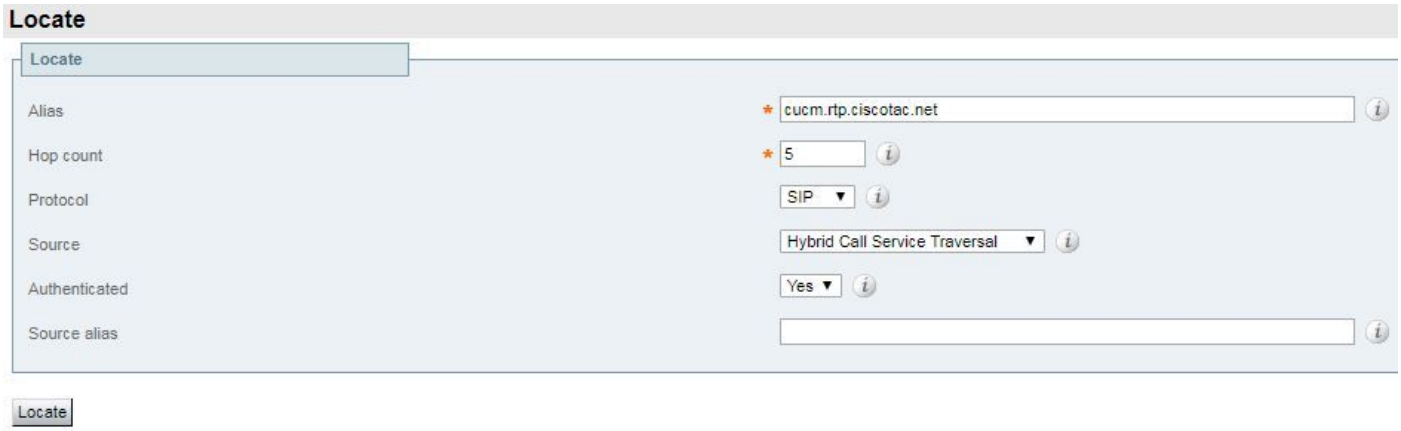
Si las reglas de búsqueda de Expressway están configuradas correctamente, puede esperar que los resultados devuelvan un mensaje de éxito. A continuación se muestra un ejemplo de una prueba de patrón de comprobación correcta, como se muestra en la imagen.



La razón por la que esto es exitoso es que este Alias (cucm.rtp.ciscotac.net) coincide con la cadena de patrón de prefijo de (cucm.rtp.ciscotac.net). Para comprender cómo se enruta una llamada en función de estos resultados, puede utilizar la utilidad de localización de Expressway descrita.Busque la utilidadLa utilidad de localización de Expressway es útil si desea comprobar si Expressway puede enrutar una llamada a una zona determinada con un alias especificado. Todo esto se puede completar sin tener que realizar una llamada real. La utilidad de localización puede encontrarse en Expressway en la opción de menú Mantenimiento > Herramientas > Localizar. Verá algunas instrucciones sobre cómo utilizar la función Localizar de Expressway-C para determinar si el servidor puede enrutar una llamada basándose en el FQDN de clúster de Unified CM que se encuentra en el encabezado de ruta SIP.

1. Vaya a Mantenimiento > Herramientas > Localizar.
2. Introduzca el FQDN del clúster de Unified CM en el campo Alias.
3. Seleccione SIP como el protocolo.
4. Seleccione su zona de cliente transversal híbrido de Cisco Webex para el origen.
5. Seleccione Localizar.

En la parte inferior de la interfaz, ahora verá los resultados de búsqueda. A continuación se muestra un ejemplo de la prueba de ejemplo que se ejecutó con los resultados coincidentes, como se muestra en la imagen.



Estos son los resultados de Localizar. Los Bolded son los valores de interés. Estos resultados muestran:

- El hecho de que el Alias se haya podido enrutar (verdadero)
- Información de origen (nombre/tipo de zona)
- Información de destino (alias al que se enruta)
- Regla de búsqueda de coincidencia (enrutamiento entrante de (Hybrid Call Service)
- La zona a la que se enviará la llamada (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
```

Registros de diagnósticoSiempre que solucione un problema de llamada o de medios de una llamada que atraviesa la solución de Expressway, debe usar el registro de diagnóstico. Esta capacidad de Expressway ofrece a los ingenieros información muy detallada sobre todas las decisiones de lógica que toma Expressway a medida que se procesa la llamada. Puede ver los mensajes SIP de cuerpo completo, la manera en que Expressway procesa esa llamada y la forma en que Expressway configura los canales de medios. El registro de diagnóstico tiene varios

módulos diferentes que lo alimentan. Los niveles de registro pueden ajustarse para mostrar mensajes FATAL (GRAVE), ERROR, WARN (ADVERTENCIA), INFO, DEBUG (DEPURACIÓN), TRACE (RASTREO). De forma predeterminada, todo se establece en INFO, que captura casi todo lo que necesita para diagnosticar un problema. A veces, necesitará ajustar un nivel de registro de un módulo concreto de INFO a DEBUG para comprender mejor lo que sucede. Los pasos siguientes muestran cómo puede ajustar los niveles de registro del módulo developer.ssl que es responsable de proporcionar información para los intercambios (mutuos) de señales TLS.

1. Inicie sesión en el servidor de Expressway (debe realizarse tanto en Expressway-E como en C).
2. Vaya a Mantenimiento > Diagnóstico > Avanzado > Configuración de registro de soporte.
3. Desplácese hasta el módulo que le gustaría ajustar, en este caso, developer.ssl y haga clic en él.
4. Junto al parámetro Level, elija DEBUG en el menú.
5. Click Save.

A esta altura, ya está preparado para capturar el registro de diagnóstico:

1. Inicie sesión en el servidor de Expressway (debe realizarse tanto en Expressway-E como en C).
2. Vaya a Mantenimiento > Diagnóstico > Registro de diagnóstico.
3. Haga clic en Iniciar nuevo registro (Asegúrese de marcar la opción tcpdump).
4. Reproduzca el problema.
5. Haga clic en Detener registro.
6. Haga clic en Descargar registro.

Para el registro de diagnóstico de Expressway, tenga en cuenta que el registro se inicia desde Expressway-C y Expressway-E en paralelo: en primer lugar, inicie el registro en Expressway-E y, a continuación, vaya a Expressway-C y comience con él. En ese momento, ya podrá reproducir el problema.Nota: Actualmente, el paquete de registro de diagnóstico de Expressway/VCS no contiene información sobre el certificado de servidor de Expressway o la lista de CA de confianza. Si dispone de un caso en el que esta función puede resultar útil, adjunte su caso a este defecto.

Información Relacionada

- Guía de implementación de Cisco Webex Hybrid Call Services
- Guía de diseño de Cisco Webex híbrido
- Guía del administrador de Cisco Expressway
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).