

# Leitfaden zur Fehlerbehebung für Cisco WebEx Hybrid Call Service Connect

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Probleme bei der Anrufeinrichtung](#)

[Gegenseitige TLS-Handshake-Fehler](#)

[Nützliche Tipps zur gemeinsamen TLS-Fehlerbehebung](#)

[Ausgabe 1 Expressway-E vertraut nicht der Zertifizierungsstelle, die das Cisco WebEx Zertifikat signiert hat.](#)

[Ausgabe 2: Falscher Name für TLS-Betreff Verifizierungsname in der Expressway-E Cisco WebEx Hybrid DNS Zone](#)

[Ausgabe 3 Expressway-E sendet keine vollständige Zertifikatskette an Cisco WebEx](#)

[Ausgabe 4: Firewall beendet gegenseitigen TLS-Handshake](#)

[Ausgabe 5 Expressway-E wird von einer öffentlichen Zertifizierungsstelle signiert, aber der Cisco WebEx Control Hub hat alternative Zertifikate geladen](#)

[Ausgabe 6. Expressway ordnet eingehenden Anruf nicht der Cisco WebEx Hybrid DNS-Zone zu.](#)

[Ausgabe 7. Expressway-E verwendet ein selbst signiertes Standardzertifikat.](#)

[Eingehend: Cisco WebEx an Standort](#)

[Ausgabe 1 Cisco WebEx kann den Expressway-E DNS SRV/Hostnamen nicht auflösen.](#)

[Ausgabe 2: Socket-Fehler: Port 5062 ist für Expressway eingehend blockiert](#)

[Ausgabe 3 Socket-Fehler: Expressway-E hört auf Port 5062 nicht zu.](#)

[Ausgabe 4: Expressway-E oder C unterstützen vorinstallierte SIP-Routen-Header nicht](#)

[Ausgabe 5 Die Cisco WebEx App erhält zwei Anrufbenachrichtigungen \(Toasts\).](#)

[Ausgehend: Am Standort zu Cisco WebEx](#)

[Ausgabe 1 Expressway kann die Adresse callservice.ciscopark.com nicht auflösen.](#)

[Ausgabe 2: Port 5062 wird ausgehenden Datenverkehr zu Cisco WebEx blockiert](#)

[Ausgabe 3 Fehlkonfiguration der Expressway Search-Regel](#)

[Ausgabe 4: Expressway CPL-Fehlkonfiguration](#)

[Bidirektional: Cisco WebEx zu standortbasiert oder am Standort zu Cisco WebEx](#)

[Ausgabe 1 IP-Telefon/Collaboration-Endgerät bietet einen anderen Audio-Codec als G.711, G.722 oder AAC-LD.](#)

[Ausgabe 2: Maximale Größe eingehender Nachrichten für Unified CM überschritten](#)

[Anhang](#)

[Expressway-Problembewerkzeug](#)

[Dienstprogramm Muster überprüfen](#)

[Dienstprogramm suchen](#)

[Diagnoseprotokollierung](#)

[Zugehörige Informationen](#)

# Einführung

In diesem Dokument wird die Cisco WebEx Hybrid Call Service Connect-Lösung beschrieben, mit der Ihre bestehende Anrufsteuerungsinfrastruktur von Cisco eine Verbindung zur Cisco Collaboration Cloud herstellen kann, damit diese zusammenarbeiten kann.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Kenntnis des Cisco WebEx Angebots
- Kenntnis der Expressway-Lösung (B2B)
- Kenntnis von Cisco Unified Communications Manager (Unified CM) und seiner Integration mit Expressway
- Unified CM 10.5(2) SU5 oder höher
- Expressway (B2B) Version X8.7.1 oder höher (X8.9.1 wird empfohlen)
- Expressway (Connector-Host) — siehe [Expressway Connector Host Support für Cisco WebEx Hybrid Services](#) für die derzeit unterstützten Versionen

### Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Unified Communications Manager
- Expressdienste
- WebEx für Windows
- WebEx für Mac
- WebEx für iOS
- WebEx für Android
- Cisco Collaboration-Endgeräte
- Collaboration-Desktop-Endgeräte
- IP-Telefone
- Software-Clients

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

## Hintergrundinformationen

Die Lösung bietet folgende Funktionen:

- Verwendung der WebEx App als mobiler Softclient für Audio- und Videoanrufe

- Mit der App können Sie Anrufe von jedem beliebigen Standort aus tätigen und empfangen, als ob Sie sich im Büro aufhielten.
- WebEx, Cisco Jabber oder das Schreibtischtelefon des Telefons verwenden, ohne sich um die Option kümmern zu müssen, die er verwendet
- Anrufverlauf in standortbasierten Telefonen entsperren und Verlauf in WebEx integrieren

Der Umfang dieses Leitfadens deckt Probleme ab, die speziell bei der Hybrid Call Service Connect auftreten. Da Hybrid Call Service Connect über dasselbe Expressway-E/C-Paar wie andere Lösungen wie Mobile und Remote Access und Business-to-Business-Anrufe ausgeführt wird, können Probleme mit den anderen Lösungen die Hybrid Call Service Connect beeinflussen. Für Kunden und Partner, die ein Expressway-Paar zur Verwendung mit Call Service Connect bereitstellen, muss der [Cisco VCS Expressway- und VCS Control Basic Configuration Guide](#) referenziert werden, bevor Sie versuchen, Hybrid Call Service Connect bereitzustellen. In diesem Leitfaden zur Fehlerbehebung werden Firewall-/NAT-Überlegungen sowie das Expressway-Design in Anhang 3 und 4 behandelt. Lesen Sie diese Dokumentation gründlich durch. Darüber hinaus geht dieses Dokument davon aus, dass der Expressway Connector-Host und die Aktivierung des Hybrid Call Service abgeschlossen wurden.

## Probleme bei der Anrufeinrichtung

### Gegenseitige TLS-Handshake-Fehler

Hybrid Call Service Connect nutzt gegenseitige Transport Layer Security (TLS) für die Authentifizierung zwischen Cisco Webex und dem Expressway-E. Dies bedeutet, dass sowohl Expressway-E als auch Cisco WebEx das gegenseitige Zertifikat prüfen und prüfen. Da wechselseitige TLS-Probleme bei der neuen Bereitstellung der Expressway-Server und der Aktivierung von Lösungen wie Hybrid Call Service Connect so weit verbreitet sind, finden Sie in diesem Abschnitt nützliche Informationen und Tipps zur Behebung zertifikatsbasierter Probleme zwischen den Expressways und Cisco WebEx.

Was überprüft Expressway-E?

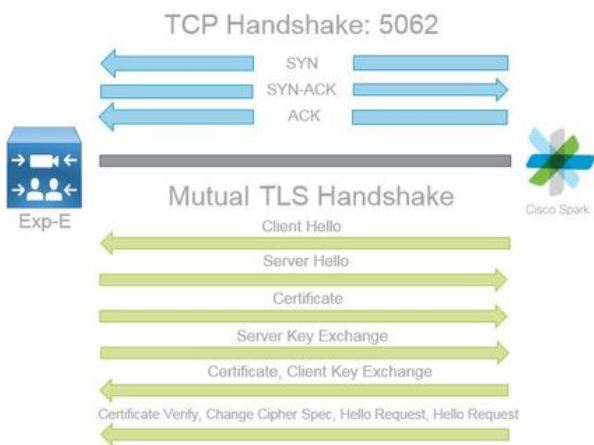
- Wurde das Cisco WebEx Zertifikat von einer öffentlichen Zertifizierungsstelle signiert, die in der Liste der vertrauenswürdigen Zertifizierungsstellen in Expressway-E aufgeführt ist?
- Ist `callservice.ciscospark.com` im Feld Subject Alternate Name (Alternativer Name für Betreff) des Cisco Webex-Zertifikats vorhanden?

Was überprüft Cisco WebEx?

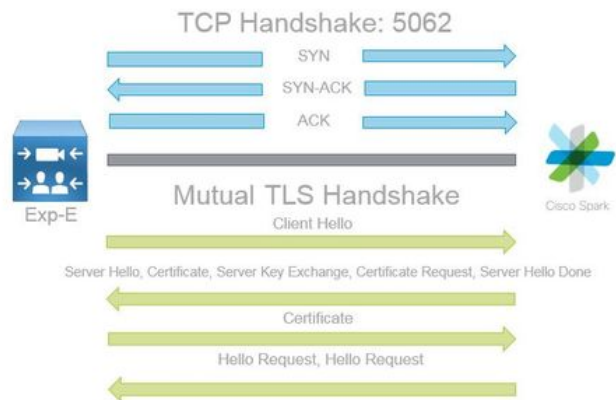
- Wurde das Expressway-E Zertifikat von einer der Public CAs signiert, denen Webex vertraut? ([Cisco WebEx Trusted CA List](#))
- Falls Expressway-E kein öffentlich signiertes Zertifikat verwendet, wurde das Expressway-Zertifikat zusammen mit Root- und Zwischenzertifikaten auf den Cisco Webex Control Hub (<https://admin.ciscospark.com>) hochgeladen?

Dies wird wie im Bild gezeigt erklärt.

## Spark to On Premise



## On Premise to Spark



## Nützliche Tipps zur gemeinsamen TLS-Fehlerbehebung

### 1. Gegenseitiges TLS-Handshake-Decode

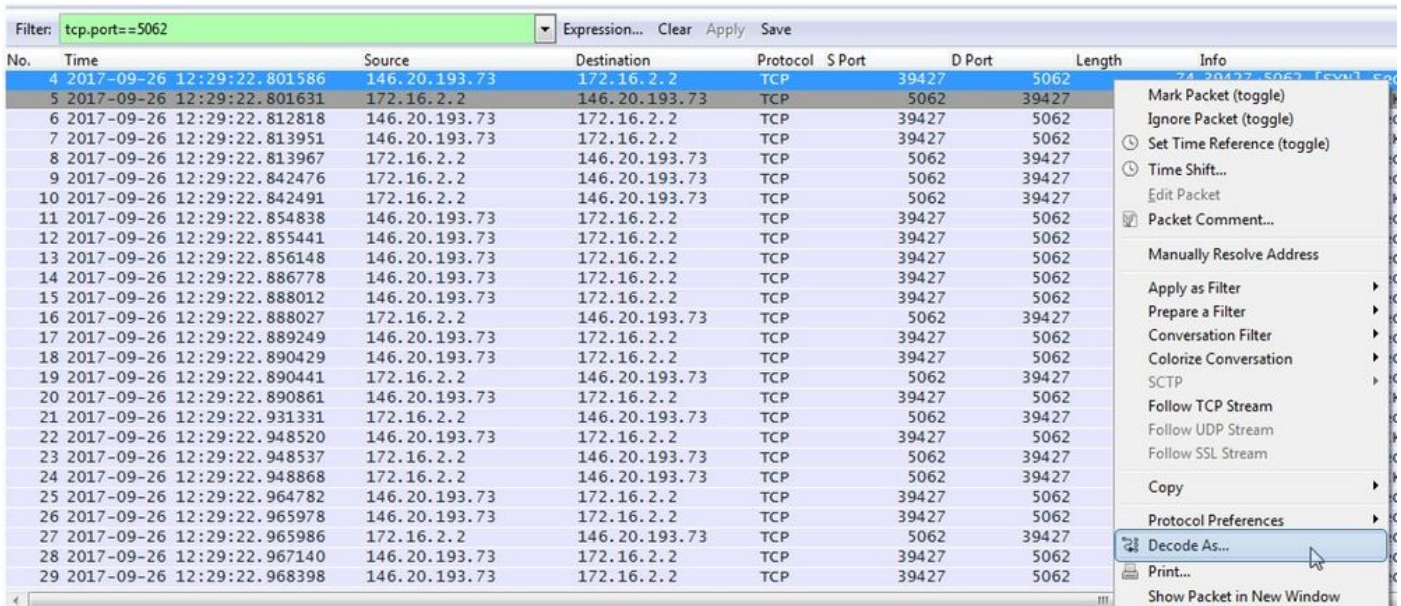
Standardmäßig markiert Wireshark SIP-TLS-Datenverkehr als Port 5061. Das bedeutet, dass Wireshark jedes Mal, wenn Sie einen (gegenseitigen) TLS-Handshake über Port 5062 analysieren möchten, nicht weiß, wie der Datenverkehr ordnungsgemäß entschlüsselt werden kann. Hier ist ein Beispiel für den gegenseitigen TLS-Handshake, der über Port 5062 erfolgt, wie im Bild gezeigt.

| 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    |

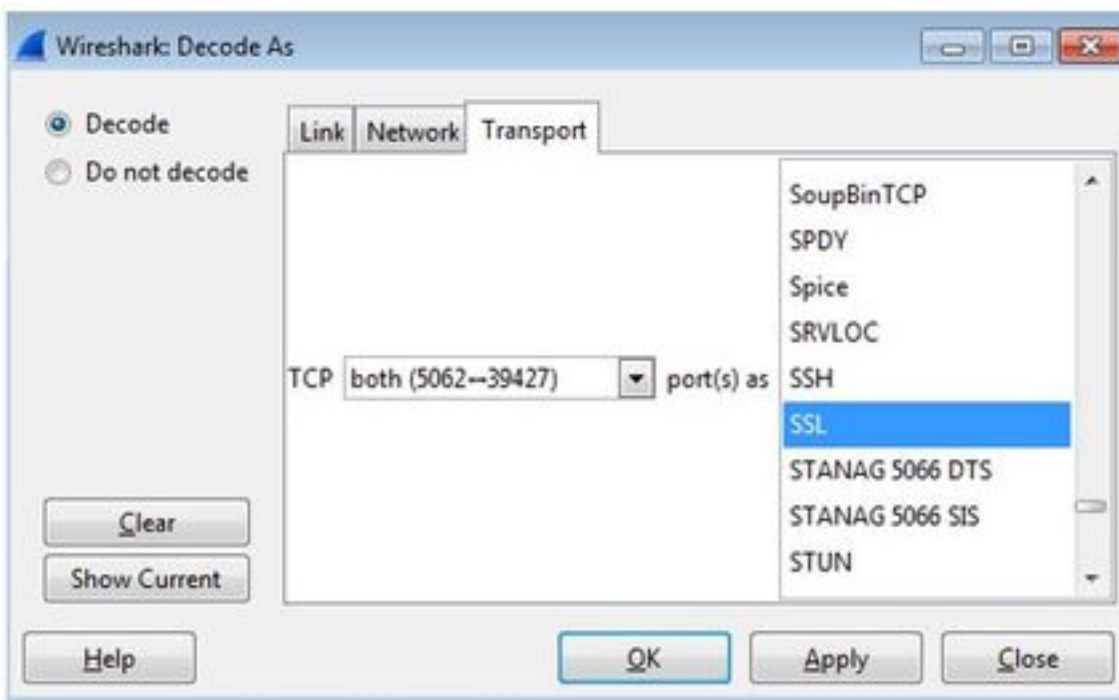
Wie Sie sehen, sieht der Handshake mit den Standardeinstellungen in Wireshark aus. Die Paketnummer 175 ist das Zertifikat, das Expressway an Cisco Webex sendet. Sie können dies jedoch nicht feststellen, ohne dass der Datenverkehr dekodiert wird. Es gibt zwei Methoden, mit denen Sie diesen Datenverkehr decodieren können, sodass Sie die Zertifikatinformationen und alle vorhandenen Fehlermeldungen leichter sehen können.

#### 1a) Deklarieren des Streams als SSL

a) Wenn Sie den Mutual TLS Handshake analysieren, filtern Sie die Erfassung zuerst nach **tcp.port==5062**. Klicken Sie anschließend mit der rechten Maustaste auf das erste Paket im Stream, und wählen Sie **Decode As.. (Als..) aus.** wie im Bild gezeigt.



b) Nach dem **Decode As..** ausgewählt ist, wird eine Liste angezeigt, in der Sie festlegen können, wie der ausgewählte Stream decodiert wird. Wählen Sie in der Liste **SSL aus**, klicken Sie auf **Übernehmen** und schließen Sie das Fenster. An diesem Punkt zeigt der gesamte Stream das Zertifikat und die Fehlermeldungen an, die zum Zeitpunkt des Handshake ausgetauscht wurden, wie im Bild gezeigt.



## 1b) SIP-TLS-Port anpassen

Wenn Sie den SIP-TLS-Port in den Wireshark-Einstellungen auf 5062 einstellen, werden alle Details rund um den Handshake angezeigt, der die Zertifikate enthält. Um diese Änderung vorzunehmen, gehen Sie wie folgt vor:

- Wireshark öffnen
- Navigieren Sie zu **Bearbeiten > Voreinstellungen**.
- Erweitern Sie Protokolle, und wählen Sie **SIP aus**.
- Legen Sie den SIP-TLS-Port auf 5062 fest, und klicken Sie auf **Übernehmen**.



- Setzen Sie den Wert auf 5061 zurück, wenn die Analyse wie im Bild gezeigt abgeschlossen ist.

SIP TCP ports:

SIP TLS Port:

Display raw text for SIP message:

Wenn Sie jetzt dieselbe Erfassung analysieren, werden die Pakete 169 bis 175 decodiert angezeigt. Paket 175 zeigt das Expressway-E-Zertifikat. Wenn Sie das Paket genauer betrachten, werden alle Zertifikatdetails angezeigt, wie im Bild gezeigt.

| 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=28800 Len=0 MSS=1460 SACK_PERM=1 TSval=444315393 TSecr=3875387337 WS=128 |
| 171 | 2017-09-20 14:22:13.304549 | 146.20.193.45 | 172.16.2.2    | TCP      | 48520  | 5062   | 66     | 48520->5062 [ACK] Seq=1 Ack=1 Win=14720 Len=0 TSval=3875387348 TSecr=444315393                                 |
| 172 | 2017-09-20 14:22:13.305898 | 146.20.193.45 | 172.16.2.2    | TLSv1.2  | 48520  | 5062   | 266    | Client Hello   |
| 173 | 2017-09-20 14:22:13.305911 | 172.16.2.2    | 146.20.193.45 | TCP      | 5062   | 48520  | 86     | 5062->48520 [ACK] Seq=1 Ack=201 Win=30080 Len=0 TSval=444315405 TSecr=3875387349                               |
| 174 | 2017-09-20 14:22:13.336342 | 172.16.2.2    | 146.20.193.45 | TLSv1.2  | 5062   | 48520  | 2802   | Server Hello   |

## 2. Wireshark-Filterung

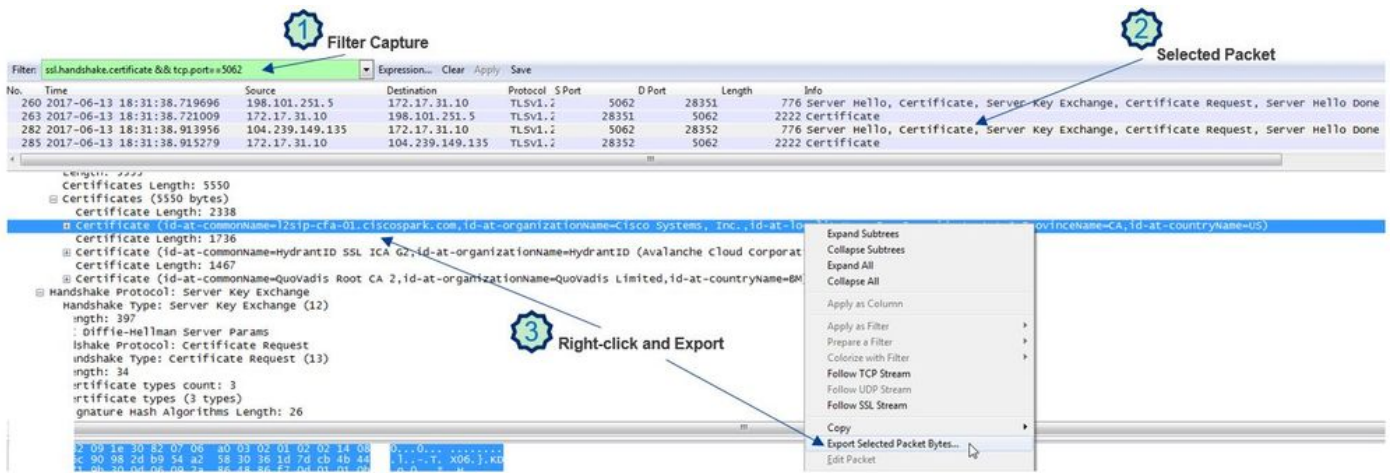
Bei der Analyse von Paketerfassungen geht die Anzahl der Pakete, die bei einer bestimmten Erfassung beobachtet wurden, schnell verloren. Es ist wichtig zu verstehen, welche Art von Datenverkehr Sie am meisten interessiert, damit Sie Wireshark filtern können, um genau das anzuzeigen. Hier sind einige gängige Wireshark-Filter, mit denen Details zu einem gemeinsamen TLS-Handshake abgerufen werden können:

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

## 3. Zertifikat aus Pcap extrahieren

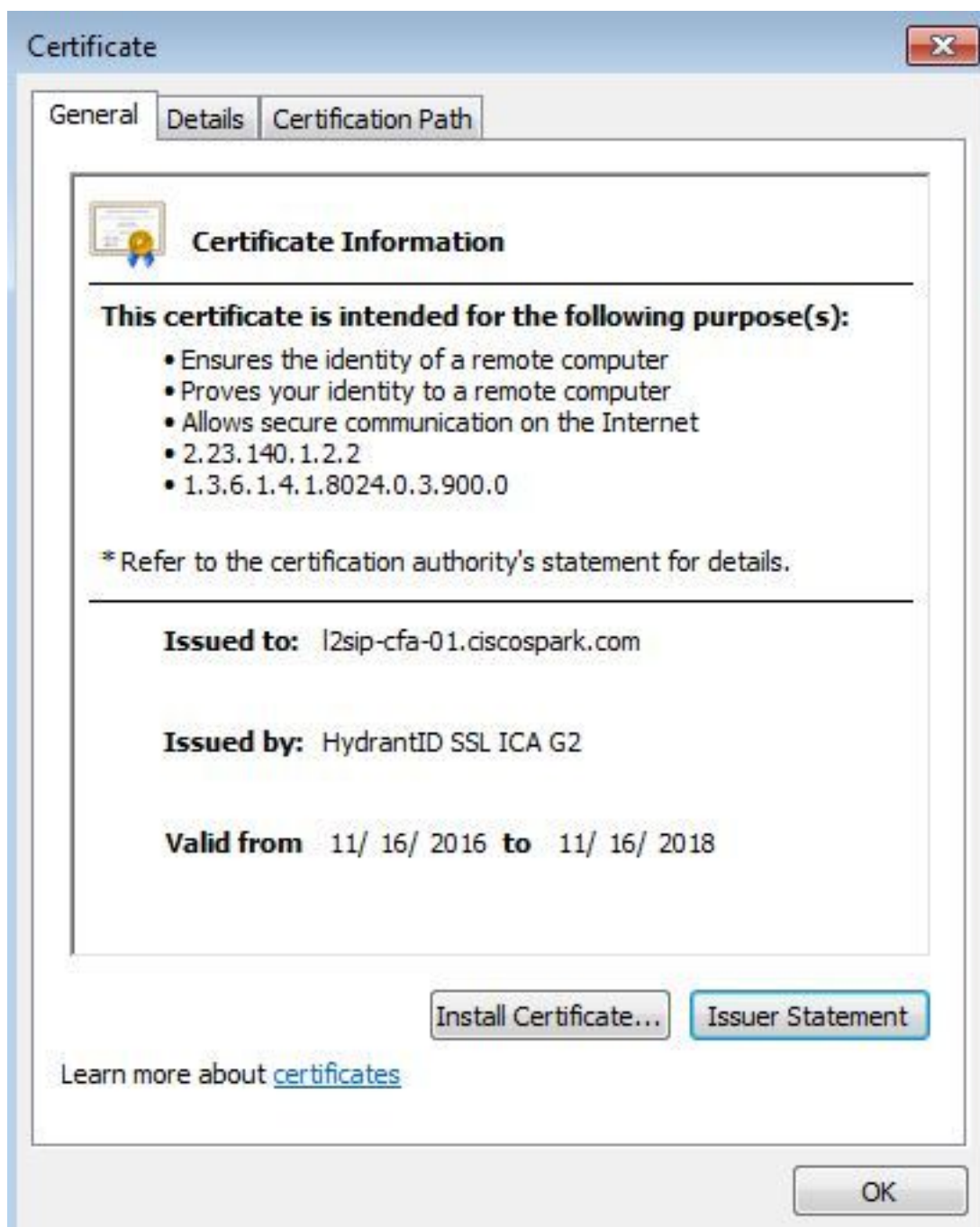
Von Zeit zu Zeit benötigen Sie möglicherweise eine Kopie eines Zertifikats (Server, Root oder Vermittler). Wenn Sie nicht wissen, wo Sie das gesuchte Zertifikat finden, können Sie es direkt aus einer Paketerfassung extrahieren. Hier finden Sie die Schritte zum Abrufen des Cisco WebEx-Zertifikats, das in einem gegenseitigen TLS-Handshake präsentiert wird.

1. Filtern Sie die Paketerfassung mit **ssl.handshake.certificate && tcp.port==5062**.
2. Suchen Sie das Paket, das von der WebEx-Serveradresse stammt und für das im Bereich Info Zertifikat gedruckt ist.
3. Erweitern Sie in den Paketdetails **Secure Socket Layer > TLS Certificate > Handshake Protocol > Certificates**. **Hinweis:** Das untere/letzte Zertifikat in der Kette ist die Root-CA.
4. Klicken Sie mit der rechten Maustaste auf das gewünschte Zertifikat, und wählen Sie **Ausgewählte Paketbyte exportieren...** wie im Bild gezeigt.



5. Speichern Sie die Datei als **.cer**.

6. Doppelklicken Sie auf die gespeicherte Datei, um das Zertifikat zu öffnen, wie im Bild gezeigt.



## 4. Ändern der Expressway-Protokollierungsstufen

Auf dem Expressway stehen zwei Protokollierungsmodule zur Verfügung, die Ihnen helfen können, die Logik des Expressway zu verstehen, wenn Sie die Zertifikate analysieren:

- `Entwickler.ssl`
- `Entwickler.zone.zonemg`

Standardmäßig sind diese Protokollierungsmodule auf die INFO-Stufe eingestellt. Wenn Sie die Einstellung auf eine DEBUG-Ebene festlegen, können Sie die Informationen über die Zertifikatsüberprüfung sowie den Zonenverkehr anzeigen, dem dieser zugeordnet wird. Beide Funktionen sind für den Hybrid Call Service relevant.

Beispiel für Expressway-E, der eine SAN-Prüfung des Cisco Webex-Serverzertifikats durchführt.

```
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"
```

Beispiel für die Expressway-E-Zuordnung der MTLS-Verbindung zur Cisco WebEx Hybrid DNS Zone:

```
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) "
```



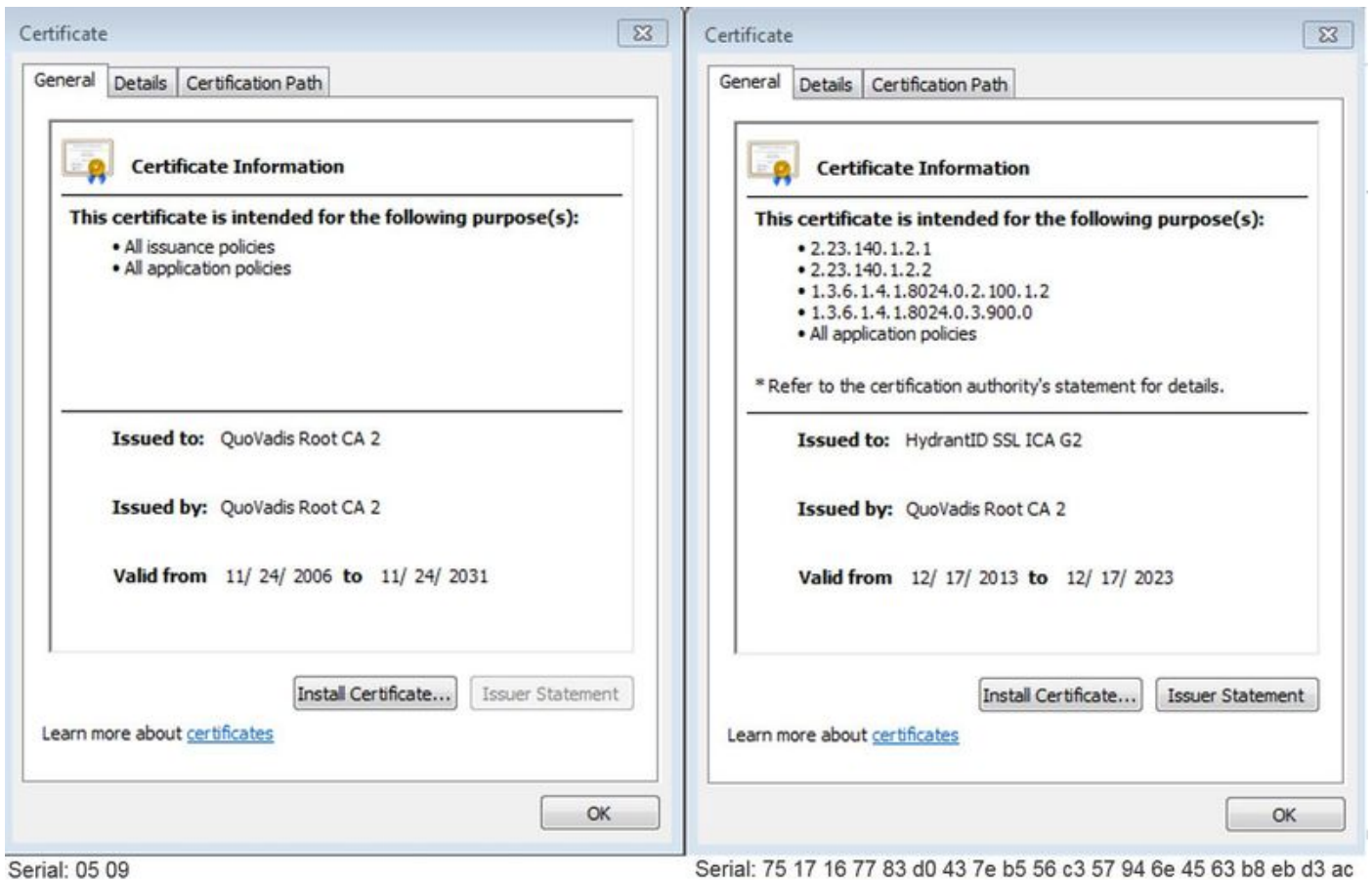
```
Method="ZoneManager::getDNSZoneByTLSVerifySubjectName" Thread="0x7f577f0a0700":
this="0x56408ff81220" getDNSZoneByTLSVerifySubjectName classified subject name
callservice.ciscospark.com into DNS zone Hybrid Call Services DNS
2017-09-22T11:11:19.564-04:00 amer-expressway01 tvcs: UTCTime="2017-09-22 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"
```

Im Folgenden finden Sie eine Liste der häufigsten Probleme im Zusammenhang mit wechselseitigen TLS-Ausfällen zwischen Expressway-E und Cisco WebEx.

**Ausgabe 1 Expressway-E vertraut nicht der Zertifizierungsstelle, die das Cisco WebEx Zertifikat signiert hat.**

Der Cisco WebEx Server, der direkt mit dem Expressway-E kommuniziert, wird als L2SIP-Server bezeichnet. Dieser L2SIP-Server ist von einem zwischengeschalteten Server mit dem gemeinsamen Namen **Hydrant SSL ICA G2** zu signieren. Der Vermittler wird von einer Stammzertifizierungsstelle signiert, die einen gemeinsamen Namen für die **QuoVadis Root CA 2** hat, wie im Bild gezeigt.

**Hinweis:** Dies könnte sich ändern.



Der erste Schritt zur Analyse dieses Datenverkehrs aus der Perspektive der Expressway-Diagnose ist die Suche nach **TCP Connecting**. Nachdem Sie **TCP Connecting** durchsucht haben, suchen Sie nach dem Wert **Dst-port=5062**. Sobald Sie den Bereich in den Protokollen identifizieren, in denen diese Verbindung hergestellt und versucht wurde, können Sie nach dem TLS-Handshake suchen, der im Allgemeinen durch die Protokolleinträge gekennzeichnet ist, die auf Handshake in progress hinweisen.

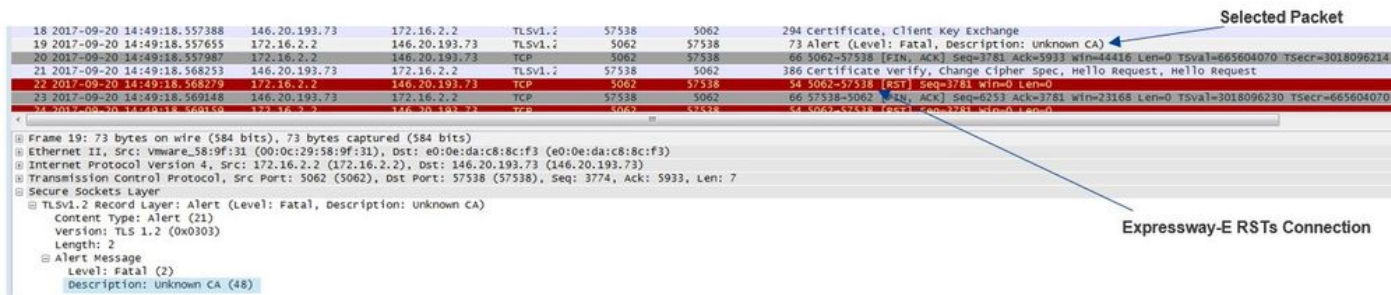
```
2017-09-20T10:49:18.427-04:00 amer-expressway01 tvcs: UTCTime="2017-09-20 14:49:18,426"
Module="developer.ssl" Level="INFO" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(1974) "
Method="::ttssl_continueHandshake" Thread="0x7f29ddefa700": Detail="Handshake in progress"
Reason="want read/write"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

Wenn das Expressway-E den von Cisco WebEx signierten Zertifikaten nicht vertraut, können Sie davon ausgehen, dass das Expressway-E das Zertifikat sofort nach Abschluss des Handshakes zurückweisen kann. Dies kann bei der Expressway-E-Protokollierung durch folgende Protokolleinträge erkannt werden:

```
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="::TTSSL_ErrorOutput" 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"

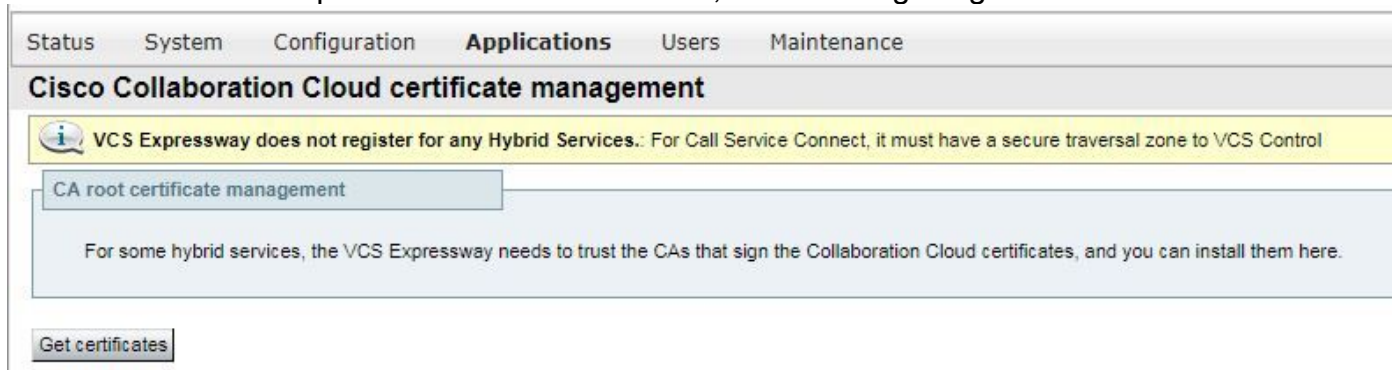
Die Expressway-Fehlermeldung kann leicht in die Irre führen, da sie sich auf ein selbstsigniertes Zertifikat in der Zertifikatkette bezieht. Wireshark erlaubt es Ihnen, sich die Börse genauer anzusehen. Aus der Perspektive der Wireshark-Paketerfassung können Sie deutlich sehen, dass Expressway bei der Vorlage des Zertifikats durch die Webex-Umgebung ein Zertifikat zurückgibt und mit einem Zertifikat mit einem Fehler einer unbekanntenen Zertifizierungsstelle zurückweist, wie im Bild gezeigt.



## Lösung:

Um dieses Problem zu beheben, müssen Sie sicherstellen, dass das Expressway-E den Cisco Webex-Zertifizierungsstellen vertraut. Obwohl Sie diese Zertifikate einfach aus einer Wireshark-Ablaufverfolgung extrahieren und in den Zertifikatsspeicher der Trusted CA auf der Expressway hochladen können, bietet Expressway eine einfachere Methode:

- Melden Sie sich bei Expressway-E an.
- Navigieren Sie zu **Anwendungen > Cloud Certificate Management**.
- Wählen Sie die Option **Zertifikate** abrufen aus, wie im Bild gezeigt.



Zu diesem Zeitpunkt werden die Cisco WebEx Zertifizierungsstellen in den Expressway-E Trusted CA Store hochgeladen (**Maintenance > Security > Trusted CA certificate**).

## Ausgabe 2: Falscher Name für TLS-Betreff Verifizierungsname in der Expressway-E Cisco WebEx Hybrid DNS Zone

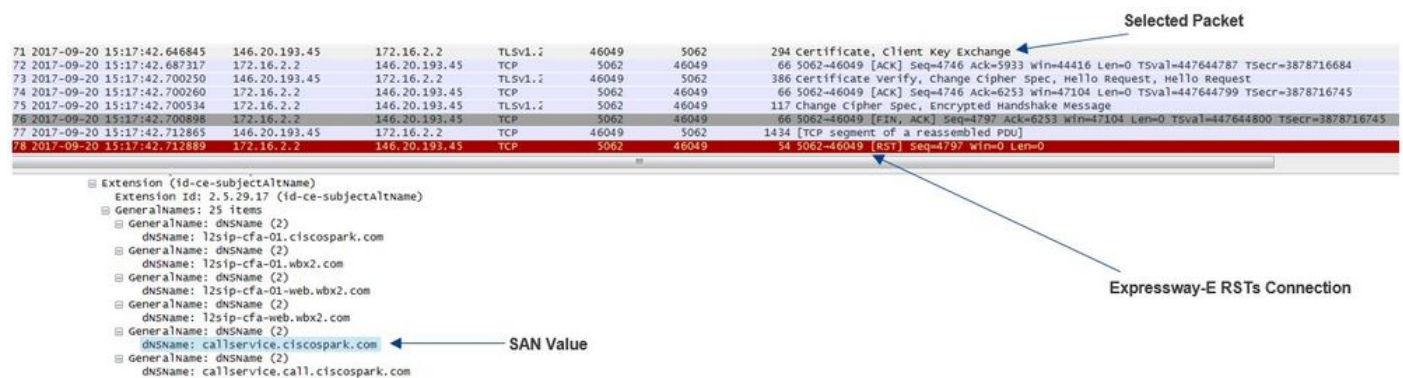
Im Rahmen des gegenseitigen TLS-Handshake verwendet Hybrid Call Service Connect die TLS-Verifizierung. Dies bedeutet, dass der Expressway nicht nur den Cisco Webex CA-Zertifikaten vertraut, sondern auch das Zertifikat durch Überprüfen des Felds "Betreff Alternate Name" (SAN) des Zertifikats überprüft, das präsentiert wird, um sicherzustellen, dass ein Wert wie **callservice.ciscospark.com** vorhanden ist. Wenn dieser Wert nicht vorhanden ist, schlägt der eingehende Anruf fehl.

In diesem speziellen Szenario präsentiert der Cisco WebEx Server sein Zertifikat dem Expressway-E. Das Zertifikat verfügt tatsächlich über 25 verschiedene SANs. Beispiel:

Expressway-E prüft das Zertifikat für das `callservice.ciscopark.com` SAN, findet es aber nicht. Wenn diese Bedingung erfüllt ist, wird in der Diagnoseprotokollierung ein ähnlicher Fehler angezeigt:

```
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"
```

Wenn Sie Wireshark zur Analyse dieses Zertifikatshandshakes verwenden, können Sie feststellen, dass die Expressway-RST-Verbindung kurz nach der Vorlage des Zertifikats von Cisco Webex, wie im Bild gezeigt, erfolgt.



Um die Konfiguration dieses Werts zu bestätigen, können Sie die WebEx Hybrid DNS Zone aufrufen, die für die Lösung konfiguriert wurde. Wenn Sie über die Expressway-E xConfiguration verfügen, können Sie im Abschnitt Zone configuration (Zonenkonfiguration) nachsehen, wie der Name des Betreffs für die TLS-Verifizierung konfiguriert wurde. Beachten Sie bei xConfiguration, dass die Zonen bestellt werden, wobei Zone 1 die erste ist. Hier sehen Sie eine xConfiguration aus der oben analysierten problematischen Umgebung.

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

Wie Sie im Beispiel sehen können, ist der Name des Betreffs für TLS verifizieren auf `callservice.ciscopark.com` anstelle von `callservice.ciscopark.com` festgelegt. (Bitte beachten Sie das zusätzliche "l").

Lösung:

Um dieses Problem zu beheben, muss der Betreffname für die TLS-Überprüfung geändert werden:

- Melden Sie sich bei Expressway-E an.
- Navigieren Sie zu **Konfiguration > Zonen > Zonen**
- Wählen Sie **WebEx Hybrid Services DNS Zone** aus
- Legen Sie den **Betreffnamen für die TLS-Überprüfung auf callservice.ciscopark.com fest.**
- Wählen Sie **Speichern**

**Hinweis:** Informationen zum Protokollierungsverhalten für die Baseline finden Sie hier. In diesem Abschnitt werden die Expressway-Zertifizierung und die Zuordnung zur WebEx

Hybrid DNS Zone beschrieben.

**Hinweis:** Ab dem Expressway-Code x12.5 und später wurde eine neue "Webex" Zone veröffentlicht. Diese WebEx Zone füllt die Konfiguration der Zone aus, die für die Kommunikation mit WebEx erforderlich ist. Das bedeutet, dass Sie nicht mehr den Betreff-Verifizierungsmodus für TLS und den Betreffnamen für TLS-Verifizierung festlegen müssen. Zur Vereinfachung der Konfiguration wird empfohlen, die WebEx Zone zu nutzen, wenn Sie den Expressway-Code x12.5 oder höher ausführen.

### Ausgabe 3 Expressway-E sendet keine vollständige Zertifikatskette an Cisco WebEx

Im Rahmen des gegenseitigen TLS-Handshake muss Cisco WebEx dem Expressway-E-Zertifikat vertrauen. Cisco Webex verfügt über eine vollständige Liste der öffentlichen CAs, denen Cisco vertraut. In der Regel ist ein TLS-Handshake erfolgreich, wenn Ihr Expressway-E-Zertifikat von einer öffentlichen Zertifizierungsstelle signiert wird, die von Cisco WebEx unterstützt wird. Das Expressway-E sendet sein Zertifikat standardmäßig nur während eines TLS-Handshake, obwohl es von einer öffentlichen Zertifizierungsstelle signiert wurde. Um die gesamte Zertifikatskette (Stamm und Zwischenkette) zu senden, müssen diese Zertifikate dem Zertifikatsspeicher der vertrauenswürdigen Zertifizierungsstelle auf dem Expressway-E selbst hinzugefügt werden.

Wenn diese Bedingung nicht erfüllt wird, lehnt Cisco WebEx das Expressway-E-Zertifikat ab. Wenn Sie eine Bedingung beheben, die zu diesem Problem passt, können Sie die Diagnoseprotokolle und tcpdump vom Expressway-E verwenden. Wenn Sie die Expressway-E Diagnoseprotokolle analysieren, sehen Sie einen Fehler, der dem hier ähnelt:

```
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="::TTSSL_ErrorOutput" 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"
```

Wenn Sie dies aus einer Wireshark-Perspektive analysieren, sehen Sie, dass das Expressway-E sein Zertifikat präsentiert. Wenn Sie das Paket erweitern, sehen Sie, dass nur das Serverzertifikat gesendet wird. Cisco WebEx lehnt diesen TLS-Handshake mit einer Fehlermeldung für eine unbekannte CA ab, wie im Bild gezeigt.



Selected Packet

| No. | Time                       | Source        | Destination   | Protocol | Length | Info   |
|-----|----------------------------|---------------|---------------|----------|--------|--|
| 40  | 2017-09-19 15:12:09.610059 | 172.16.2.2    | 146.20.193.45 | TLSv1.2  | 5062   | 33441 2600 Server hello, Certificate, Server Key Exchange, Certificate Request, Server hello Done        |
| 41  | 2017-09-19 15:12:09.664324 | 146.20.193.45 | 172.16.2.2    | TCP      | 5062   | 66 33441-5062 [ACK] Seq=201 Ack=1369 Win=17536 Len=0 TSval=3791983688 TSecr=360911709                    |
| 42  | 2017-09-19 15:12:09.664330 | 146.20.193.45 | 172.16.2.2    | TCP      | 33441  | 73 Alert (Level: Fatal, Description: Certificate Unknown)  |
| 43  | 2017-09-19 15:12:09.664651 | 146.20.193.45 | 172.16.2.2    | TCP      | 33441  | 66 33441-5062 [ACK] Seq=201 Ack=2535 Win=20480 Len=0 TSval=3791983689 TSecr=360911709                    |
| 44  | 2017-09-19 15:12:09.665070 | 146.20.193.45 | 172.16.2.2    | TCP      | 33441  | 78 [TCP Dup ACK 43#1] 33441-5062 [ACK] Seq=201 Ack=2535 Win=20480 Len=0 TSval=3791983707 TSecr=360911709 |
| 45  | 2017-09-19 15:12:09.721427 | 146.20.193.45 | 172.16.2.2    | TLSv1.2  | 33441  | 66 33441-5062 [FIN, ACK] Seq=208 Ack=2535 Win=20480 Len=0 TSval=3791983754 TSecr=360911744               |
| 46  | 2017-09-19 15:12:09.721515 | 146.20.193.45 | 172.16.2.2    | TCP      | 33441  | 66 5062-33441 [FIN, ACK] Seq=209 Ack=2536 Win=20480 Len=0 TSval=3791983754 TSecr=360911821               |
| 47  | 2017-09-19 15:12:09.721758 | 172.16.2.2    | 146.20.193.45 | TCP      | 5062   | 66 33441-5062 [ACK] Seq=209 Ack=2536 Win=20480 Len=0 TSval=3791983779 TSecr=360911821                    |
| 48  | 2017-09-19 15:12:09.731022 | 146.20.193.45 | 172.16.2.2    | TCP      | 33441  | 66 33441-5062 [ACK] Seq=209 Ack=2536 Win=20480 Len=0 TSval=3791983779 TSecr=360911821                    |

Spark Rejects the Handshake "Certificate Unknown" error

```

Frame 40: 3500 bytes on wire (28000 bits): 2600 bytes captured (20800 bits) on 0
Ethernet II, Src: Vmware_58:9f:31 (00:0c:29:58:9f:31), Dst: e0:0e:da:c8:8c:f3 (e0:0e:da:c8:8c:f3)
Internet Protocol Version 4, Src: 172.16.2.2 (172.16.2.2), Dst: 146.20.193.45 (146.20.193.45)
Transmission Control Protocol, Src Port: 5062 (5062), Dst Port: 33441 (33441), Seq: 1, Ack: 201, Len: 2534
Secure Sockets Layer
  TLSv1.2 Record Layer: Handshake Protocol: Server hello
  TLSv1.2 Record Layer: Handshake Protocol: Certificate
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 1722
  Handshake Protocol: Certificate
    Handshake Type: Certificate (11)
    Length: 1718
    Certificates Length: 1715
    Certificates (1715 bytes)
      Certificate Length: 1712
      Certificate (id-at-commonName=amer-expressway01.ciscotac.net,id-at-organizationalUnitName=domain control validated)
        SignedCertificate
          AlgorithmIdentifier (sha256withRSAEncryption)
            padding: 0
            encrypted: 23238dab29a4d921bc432266e5e2faef0e8524bfb44129a7...
  
```

Expressway-E Server Certificate

## Lösung:

Um das Problem in diesem Szenario zu beheben, müssen Sie die Zwischen- und Root-CAs, die an der Signierung des Expressway-E-Zertifikats beteiligt sind, in den Zertifikatsspeicher der Trusted CA hochladen:

- Schritt 1: Melden Sie sich bei Expressway-E an.
- Schritt 2: Navigieren Sie zu **Maintenance > Security > Trusted CA certificate**.
- Schritt 3: Wählen Sie **Datei auswählen** im Menü Hochladen unten in der Benutzeroberfläche aus.
- Schritt 4: Wählen Sie das Zertifizierungsstellenzertifikat aus, das an der Unterzeichnung des Expressway-E beteiligt war.
- Schritt 5: Wählen Sie **CA-Zertifikat anhängen aus**.
- Schritt 6: Wiederholen Sie die Schritte für alle Zertifizierungsstellenzertifikate, die an der Unterzeichnung des Expressway-E-Zertifikats beteiligt sind (Intermediate, Root).
- Schritt 7: Wählen Sie **CA-Zertifikat anhängen aus**.

Nach Abschluss dieses Vorgangs sehen Sie, dass die gesamte Zertifikatkette, die an der Signierung des Expressway-E Server-Zertifikats beteiligt ist, im Schlüsselaustausch enthalten ist. Im Folgenden sehen Sie ein Beispiel für eine Analyse einer Paketerfassung mit Wireshark.

Selected Packet

| No. | Time                       | Source        | Destination   | Protocol | Length | Info   |
|-----|----------------------------|---------------|---------------|----------|--------|--|
| 175 | 2017-09-20 14:22:13.336358 | 172.16.2.2    | 146.20.193.45 | TLSv1.2  | 5062   | 48520 1426 Certificate   |
| 176 | 2017-09-20 14:22:13.354189 | 146.20.193.45 | 172.16.2.2    | TCP      | 48520  | 66 48520-5062 [ACK] Seq=201 Ack=1369 Win=17536 Len=0 TSval=3875387398 TSecr=444315436      |
| 177 | 2017-09-20 14:22:13.354815 | 146.20.193.45 | 172.16.2.2    | TCP      | 48520  | 66 48520-5062 [ACK] Seq=201 Ack=2737 Win=20480 Len=0 TSval=3875387399 TSecr=444315436      |
| 178 | 2017-09-20 14:22:13.355885 | 146.20.193.45 | 172.16.2.2    | TCP      | 48520  | 66 48520-5062 [ACK] Seq=201 Ack=4097 Win=23296 Len=0 TSval=3875387400 TSecr=444315436      |
| 179 | 2017-09-20 14:22:13.355999 | 172.16.2.2    | 146.20.193.45 | TLSv1.2  | 5062   | 715 Server Key Exchange  |
| 180 | 2017-09-20 14:22:13.366930 | 146.20.193.45 | 172.16.2.2    | TCP      | 48520  | 66 48520-5062 [ACK] Seq=201 Ack=4746 Win=26112 Len=0 TSval=3875387411 TSecr=444315455      |
| 197 | 2017-09-20 14:22:13.668592 | 146.20.193.45 | 172.16.2.2    | TLSv1.2  | 48520  | 73 Alert (Level: Fatal, Description: Certificate unknown)                                  |
| 198 | 2017-09-20 14:22:13.668644 | 146.20.193.45 | 172.16.2.2    | TCP      | 48520  | 66 48520-5062 [FIN, ACK] Seq=208 Ack=4746 Win=26112 Len=0 TSval=3875387711 TSecr=444315455 |
| 199 | 2017-09-20 14:22:13.668871 | 172.16.2.2    | 146.20.193.45 | TCP      | 5062   | 66 5062-48520 [FIN, ACK] Seq=4746 Ack=209 Win=30080 Len=0 TSval=444315768 TSecr=3875387711 |
| 200 | 2017-09-20 14:22:13.681586 | 146.20.193.45 | 172.16.2.2    | TCP      | 48520  | 66 48520-5062 [ACK] Seq=209 Ack=4747 Win=26112 Len=0 TSval=3875387725 TSecr=444315768      |

```

Frame 175: 1426 bytes on wire (11408 bits): 1426 bytes captured (11408 bits) on 0
Ethernet II, Src: Vmware_58:9f:31 (00:0c:29:58:9f:31), Dst: e0:0e:da:c8:8c:f3 (e0:0e:da:c8:8c:f3)
Internet Protocol Version 4, Src: 172.16.2.2 (172.16.2.2), Dst: 146.20.193.45 (146.20.193.45)
Transmission Control Protocol, Src Port: 5062 (5062), Dst Port: 48520 (48520), Seq: 2737, Ack: 201, Len: 1360
[2 Reassembled TCP Segments (3938 bytes): #174(2642), #175(1296)]
Secure Sockets Layer
  TLSv1.2 Record Layer: Handshake Protocol: Certificate
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 3933
  Handshake Protocol: Certificate
    Handshake Type: Certificate (11)
    Length: 3929
    Certificates Length: 3926
    Certificates (3926 bytes)
      Certificate Length: 1712
      Certificate (id-at-commonName=amer-expressway01.ciscotac.net,id-at-organizationalUnitName=domain control validated)
        Certificate Length: 1216
      Certificate (id-at-commonName=Go Daddy Secure Certificate Authority - G2,id-at-organizationalUnitName=https://certs.godaddy.com/repository,id-at-organizationName=GoDaddy.com, Inc.,id-at-localityName=)
        Certificate Length: 969
      Certificate (id-at-commonName=Go Daddy Root Certificate Authority - G2,id-at-organizationName=GoDaddy.com, Inc.,id-at-localityName=Scottsdale,id-at-stateOrProvinceName=Arizona,id-at-countryName=US)
        Certificate Length: 1216
  
```

Server  
Intermediate  
Root

## Ausgabe 4: Firewall beendet gegenseitigen TLS-Handshake

Die Expressway-Lösung ist in der Regel mit einer Firewall verbunden. Die Inline-Firewall für die Lösung führt häufig eine eigene Inspektion auf Anwendungsebene durch. Häufig sehen Administratoren bei der Expressway-Lösung unerwünschte Ergebnisse, wenn die Firewall eine Überprüfung auf Anwendungsebene durchführt. Dieses spezielle Problem hilft Ihnen zu erkennen, wenn die

Verbindung durch die Prüfung auf Anwendungsebene einer Firewall plötzlich aufgespielt wird.

Mithilfe der Diagnoseprotokolle vom Expressway können Sie nach dem versuchten Mutual TLS Handshake suchen. Dieser Handshake sollte, wie bereits erwähnt, kurz nach der Herstellung der TCP-Verbindung über Port 5062 erfolgen. Wenn die Firewall die Verbindung beendet, werden diese Fehler in diesem Szenario in der Diagnoseprotokollierung angezeigt.

```
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.ciscopark.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"
```

Was die Paketerfassung betrifft, so wird Ihnen angezeigt, dass das Expressway-E seine Zertifizierung Cisco WebEx präsentiert. Sie sehen, wie ein TCP-RST von Cisco WebEx in Richtung eingehet, wie im Bild gezeigt.

The image shows a Wireshark packet capture. The top part displays a list of packets. Packet 263 is selected, showing a TLSv1.2 Certificate message. Packet 264 is a TCP ACK. Packet 265 is a TLSv1.2 Client Key Exchange, Certificate Verify, Change Cipher Spec, and Encrypted Handshake Message. Packet 266 is a TCP RST, which is highlighted in red and labeled as 'Unexpected RST with no error code'. The packet details pane for packet 266 shows the RST flag set and no error code. The packet bytes pane shows the raw data of the RST packet. On the left, a network diagram shows the path from the Server to the Intermediate and Root nodes.

Auf den ersten Blick denken Sie vielleicht, dass etwas mit dem Expressway-E Zertifikat nicht stimmt. Um dieses Problem zu beheben, müssen Sie zunächst die Antworten auf folgende Fragen ermitteln:

- Wird das Expressway-E von einer öffentlichen Zertifizierungsstelle signiert, der Cisco WebEx vertraut?
- Werden das Expressway-E-Zertifikat und alle Zertifikate, die an der Signierung des Expressway-E-Zertifikats beteiligt sind, manuell auf den Cisco WebEx Control Hub (<https://admin.ciscopark.com>) hochgeladen?

In diesem speziellen Fall sollte der Cisco WebEx Control Hub nicht zum Verwalten der Expressway-E-Zertifikate verwendet werden. Dies bedeutet, dass das Expressway-E-Zertifikat von einer öffentlichen Zertifizierungsstelle signiert werden muss, der Cisco Webex vertraut. Wenn Sie in der Wireshark Capture (wie oben gezeigt) auf dem Zertifikatpaket auswählen, können Sie sehen, dass das Zertifikat von einer öffentlichen Zertifizierungsstelle signiert wurde und dass die gesamte Kette an Cisco Webex gesendet wurde. Daher sollte die Frage nicht mit dem Expressway-E-Zertifikat in Zusammenhang stehen.

Wenn an diesem Punkt eine weitere Isolierung erforderlich ist, können Sie eine Paketerfassung von der externen Schnittstelle der Firewall vornehmen. Der fehlende SSL-Fehler im Diagnoseprotokoll ist jedoch ein wichtiger Datenpunkt. Wenn Sie sich oben erinnern (Issue 3.),

wenn Cisco WebEx dem Expressway-E-Zertifikat nicht vertraut, müssen Sie einen SSL-Trennungsgrund sehen. In dieser Bedingung war kein SSL-Fehler verfügbar.

**Hinweis:** Wenn Sie eine Paketerfassung von der externen Firewall-Schnittstelle durchführen würden, würde in der Cisco WebEx Umgebung kein TCP-RST eingehen.

## Lösung

Für diese spezielle Lösung müssen Sie als Partner oder Kunde auf Ihr Sicherheitsteam vertrauen. Das Team muss untersuchen, ob eine Art von Anwendungsebenenprüfung für die Expressway-Lösung verwendet wird. Ist dies der Fall, sollte diese deaktiviert werden. [In Anhang 4](#) des **VCS Control and Expressway Deployment Guide** wird erläutert, warum es ratsam ist, dass Kunden diese Funktion deaktivieren.

## Ausgabe 5 Expressway-E wird von einer öffentlichen Zertifizierungsstelle signiert, aber der Cisco WebEx Control Hub hat alternative Zertifikate geladen

Diese spezielle Bedingung kann oft auftreten, wenn Sie die Expressway-Lösung von Grund auf neu implementiert haben und das Expressway-E-Zertifikat zunächst nicht von einer öffentlichen Zertifizierungsstelle signiert wurde. In diesem Szenario laden Sie das Expressway-E-Serverzertifikat (das intern signiert wurde) auf den Cisco WebEx Control Hub hoch, damit Sie die gegenseitige TLS-Aushandlung erfolgreich abschließen können. Anschließend erhalten Sie das Expressway-E-Zertifikat, das von einer öffentlichen Zertifizierungsstelle signiert wurde. Vergessen Sie jedoch, das Serverzertifikat aus dem Cisco WebEx Control Hub zu entfernen. Es ist wichtig zu wissen, dass beim Hochladen eines Zertifikats zum Cisco WebEx Control Hub dieses Zertifikat Vorrang vor dem Zertifikat und der Kette hat, die der Expressway während des TLS-Handshake präsentiert.

Aus der Sicht der Expressway-E-Diagnoseprotokollierung kann dieses Problem ähnlich der Protokollierungssignatur aussehen, die erfüllt wird, wenn Cisco WebEx dem Expressway-E-Zertifikat nicht traut - z. B. im Fall des Expressway-E, der seine vollständige Kette nicht sendet, oder im Fall des Expressway-E-Zertifikats, das nicht von einer öffentlichen Zertifizierungsstelle signiert wird, der Cisco Webex vertraut. Im Folgenden finden Sie ein Beispiel für die Expressway-E-Protokollierung beim TLS-Handshake:

```
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""
```

Schauen Sie sich dies aus der Wireshark-Perspektive an, wie Sie hier sehen können, dass das Expressway-E sein Zertifikat in Posten 175 präsentiert. Einige Posten später lehnt die Cisco WebEx Umgebung das Zertifikat mit einem Fehler "Zertifikat unbekannt" ab, wie im Bild gezeigt.



The screenshot shows a network traffic analysis tool interface. At the top, a table of packets is displayed. The selected packet (ID 175) is a TLSv1.2 record containing a certificate. The details pane shows the following information:

- Frame 175: 1426 bytes on wire (11408 bits), 1426 bytes captured (11408 bits)
- Ethernet II, Src: Vmware\_58:9f:31 (00:0c:29:58:9f:31), Dst: e0:0e:da:c8:8c:f3 (e0:0e:da:c8:8c:f3)
- Internet Protocol Version 4, Src: 172.16.2.2 (172.16.2.2), Dst: 146.20.193.45 (146.20.193.45)
- Transmission Control Protocol, Src Port: 5062 (5062), Dst Port: 48520 (48520), Seq: 2737, Ack: 201, Len: 1360
- [2 Reassembled TCP Segments (3938 bytes): #174(2642), #175(1296)]
- Secure Sockets Layer
  - TLSv1.2 Record Layer: Handshake Protocol: certificate
    - Content Type: Handshake (22)
    - Version: TLS 1.2 (0x0303)
    - Length: 3933
    - Handshake Protocol: certificate
      - Handshake Type: Certificate (11)
      - Length: 3929
      - Certificates Length: 3926
      - Certificates (3926 bytes)
        - Certificate Length: 1712
        - Certificate (id-at-commonName=amer-expressway01.ciscotac.net,id-at-organizationalunitName=domain control validated)
        - Certificate Length: 1236
        - Certificate (id-at-commonName=Go Daddy Secure Certificate Authority - G2,id-at-organizationalunitName=http://certs.godaddy.com/repositor,id-at-organizationName=GoDaddy.com, Inc.,id-at-localityName=Scottsdale,id-at-stateOrProvinceName=Arizona,id-at-countryName=US)
        - Certificate Length: 969
        - Certificate (id-at-commonName=Go Daddy Root Certificate Authority - G2,id-at-organizationName=GoDaddy.com, Inc.,id-at-localityName=Scottsdale,id-at-stateOrProvinceName=Arizona,id-at-countryName=US)

A warning message at the bottom right states: "Spark sends a 'Certificate Unknown' Error".

Wenn Sie das Zertifikatpaket auswählen, das der Expressway-E sendet, können Sie die Zertifikatinformationen erweitern, um festzustellen, ob der Expressway-E

1. von einer [Public CA](#) signiert wird, [der Cisco Webex vertraut](#), und
2. schließt die gesamte Kette ein, die an der Signierung beteiligt ist.

In dieser Situation sind beide Bedingungen erfüllt. Das deutet darauf hin, dass das Expressway-E Zertifikat nichts falsch ist.

## Lösung

Schritt 1: Melden Sie sich beim [Cisco WebEx Control Hub an](#).

Schritt 2: Wählen Sie **Services** im linken Bereich aus.

Schritt 3: Wählen Sie **Einstellungen** unter der Hybrid Call Card aus.

Schritt 4: Scrollen Sie zum Abschnitt Call Service Connect, und sehen Sie unter Certificates for Encrypted SIP Calls (Zertifikate für verschlüsselte SIP-Anrufe), ob unerwünschte Zertifikate aufgeführt werden. Wenn ja, klicken Sie auf das Abfaller-Symbol neben dem Zertifikat.

Schritt 5. Wählen Sie **Entfernen aus**.

**Hinweis:** Es ist wichtig, dass die Analyse durchgeführt wird und dass der Kunde die Zertifikate, die auf den WebEx Control Hub hochgeladen wurden, nicht verwendet, bevor er sie entfernt.

Weitere Informationen zum Hochladen Ihres Expressway-E-Zertifikats im Cisco WebEx Control Hub finden Sie [in diesem Abschnitt des Bereitstellungsleitfadens für hybride Anrufe](#).

## Ausgabe 6. Expressway ordnet eingehenden Anruf nicht der Cisco WebEx Hybrid DNS-Zone zu.

Die Zuordnungsfunktion für eingehende TLS arbeitet mit dem Betreffnamen für die TLS-Überprüfung zusammen, die beide in der DNS-Zone für hybride Anrufe konfiguriert sind. In diesem Szenario werden Probleme und Herausforderungen erläutert, die mit dem Expressway vor x12.5 beobachtet wurden. In x12 und später wurde ein neuer Zonentyp implementiert, der als "Webex"-Zone bezeichnet wird. Diese Zone füllt alle erforderlichen Konfigurationen für die Integration mit

WebEx vorab aus. Wenn Sie x12.5 ausführen und WebEx Hybrid Call bereitstellen, wird empfohlen, den **Webex** Zone-Typ zu verwenden, damit die Hybrid Call Services Domain (callservice.webex.com) automatisch für Sie konfiguriert wird. Dieser Wert entspricht dem Betreff Alternate Name des Webex-Zertifikats, das während des Mutual TLS Handshake angezeigt wird, und ermöglicht die Verbindung und eingehende Zuordnung zum Expressway, um erfolgreich zu sein.

Wenn Sie eine Codeversion unter x12.5 verwenden oder die WebEx Zone nicht verwenden, werden Sie mit der unten stehenden Erklärung fortfahren, die veranschaulicht, wie Probleme identifiziert und behoben werden können, bei denen der Expressway den eingehenden Anruf nicht der WebEx Hybrid DNS Zone zuordnet.

Die Funktion gliedert sich in drei Schritte:

1. Expressway-E akzeptiert das Cisco WebEx Zertifikat.
2. Expressway-E prüft das Cisco WebEx-Zertifikat, um festzustellen, ob ein Alternativer Betreff-Name vorhanden ist, der mit dem TLS-Verifizierungsnamen übereinstimmt: callservice.ciscopark.com.
3. Expressway-E ordnet die eingehende Verbindung über die Cisco WebEx Hybrid DNS Zone zu.

Wenn die Authentifizierung nicht erfolgreich ist, bedeutet dies, dass die Zertifikatsvalidierung fehlgeschlagen ist. Der Anruf geht in die Standardzone ein und wird gemäß den für Business-to-Business-Szenarien bereitgestellten Suchregeln weitergeleitet, wenn Business-to-Business auf Expressway-E konfiguriert wird.

Wie bei anderen Szenarien müssen Sie sowohl die Diagnoseprotokollierung als auch die Paketerfassung verwenden, um zu bestimmen, wie dieser Fehler aussieht. Anschließend können Sie mithilfe der Paketerfassung erkennen, welche Seite den RST sendet. Im Folgenden finden Sie ein Beispiel für die TCP-Verbindung, die versucht wird und anschließend eingerichtet wird.

```
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"
```

Nachdem die TCP-Verbindung hergestellt wurde, kann der TLS-Handshake gewährleistet werden. Sie können sehen, kurz nachdem der Handshake beginnt, es schnell Fehler.

```
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"
```

Betrachten Sie diese Situation aus einer Perspektive von pcap, können Sie ein besseres Gefühl von



- der den RST sendet, und
- welche Zertifikate übergeben werden, um festzustellen, ob sie korrekt sind.

Wenn Sie diese Aufnahme analysieren, sehen Sie, dass Expressway-E den RST sendet. Wenn Sie sich das übergebene Cisco WebEx-Zertifikat ansehen, sehen Sie, dass es die gesamte Kette sendet. Darüber hinaus können Sie aufgrund der Fehlermeldung im Diagnoseprotokoll schließen, dass das Expressway-E den öffentlichen CAs von Cisco WebEx nicht vertraut. Andernfalls wird ein Fehler wie "**selbstsigniertes Zertifikat in der Zertifikatskette**" angezeigt. Sie können sich die Paketdetails ansehen, wie im Bild gezeigt.

The image shows a Wireshark capture of a network session. The packet list pane highlights a TCP segment (No. 70) with a Reset (RST) flag, Seq=4798, Win=0, and Len=0, originating from 172.16.2.2. The packet details pane shows the structure of the captured data, including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and the Secure Sockets Layer (SSL/TLS). The TLS handshake details show a Client Key Exchange message followed by a Certificate message containing two certificates: one for 'callservice.ciscopark.com' and another for 'HydrantID SSL ICA G2'.

Durch Klicken auf das Webex-Serverzertifikat und Erweitern des Zertifikats, um die Betreffalternativen Namen (dnsName) anzuzeigen, können Sie überprüfen, ob **callservice.ciscopark.com** aufgeführt ist.

Navigieren Sie zu **Wireshark: Zertifikat > Durchwahl > General Names > GeneralName > NSName: callservice.ciscopark.com**

Damit wird bestätigt, dass das WebEx Zertifikat einwandfrei aussieht.

Sie können jetzt bestätigen, dass der Betreffname der TLS-Überprüfung korrekt ist. Wie bereits erwähnt, können Sie im Abschnitt "Zonenkonfiguration" nach der Konfiguration des Betreffnamens für die TLS-Verifizierung suchen. Eine Anmerkung zur xConfiguration ist, dass die Zonen mit Zone 1 bestellt werden, die erste erstellt wurde. Hier sehen Sie eine xConfiguration aus der oben analysierten problematischen Umgebung. Es ist klar, dass mit dem Betreffnamen "TLS Verified Subject Name" nichts falsch ist.

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

Als Nächstes muss die **eingehende TLS-Zuordnung** überprüft werden. Dadurch wird bestätigt, dass Sie die TLS-Verbindung der WebEx Hybrid DNS Zone richtig zuordnen. Die xConfiguration kann auch zur Analyse verwendet werden. In der xConfiguration heißt die **TLS-Verifizierung der eingehenden Zuordnung DNS ZIP TLS Verify InboundClassification**. Wie Sie in diesem Beispiel sehen können, ist der Wert auf Off (Aus) gesetzt.

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

Da dieser Wert auf Off (Aus) gesetzt ist, bedeutet dies, dass der VCS daran gehindert wird,

eingehende TLS-Verbindungen dieser Zone zuzuordnen. Der Anruf geht somit in die Standardzone ein und wird gemäß den für Business-to-Business-Szenarien bereitgestellten Suchregeln geprüft und weitergeleitet, wenn Business-to-Business auf Expressway-E konfiguriert wird.

## Lösung

Um dies zu erreichen, müssen Sie die eingehende Zuordnung von TLS in der Hybrid Call DNS Zone auf On (Ein) überprüfen. Dies sind die Schritte, die Sie durchführen müssen.

1. Melden Sie sich bei Expressway-E an.
2. Navigieren Sie zu **Konfiguration > Zonen > Zonen**
3. **DNS-Zone** für **Hybrid-Anrufe** auswählen
4. Wählen Sie für die **TLS-Verifizierung der eingehenden Zuordnung On (Ein)** aus.
5. Wählen Sie **Speichern**

**Hinweis:** Informationen zum Protokollierungsverhalten für die Baseline finden Sie unter . In diesem Abschnitt werden die Expressway-Zertifizierung und die Zuordnung zur WebEx Hybrid DNS Zone beschrieben.

## Ausgabe 7. Expressway-E verwendet ein selbst signiertes Standardzertifikat.

Bei einigen neuen Bereitstellungen von Hybrid Call Service Connect wird die Signierung des Expressway-E-Zertifikats übersehen oder es wird davon ausgegangen, dass das Standard-Serverzertifikat verwendet werden kann. Einige Leute denken, dass dies möglich ist, da Sie mit dem Cisco WebEx Control Hub ein benutzerdefiniertes Zertifikat in das Portal laden können. (**Services > Einstellungen (Unter Hybrid Call Card) > Hochladen (unter Zertifikate für verschlüsselte Anrufe)**)

Wenn Sie die Formulierung über die **Zertifikate für verschlüsselte SIP-Anrufe** genau beachten, sehen Sie Folgendes: 'Verwenden Sie Zertifikate aus der Cisco Collaboration Standard-Vertrauensliste, oder laden Sie eigene hoch. Wenn Sie Ihre eigenen verwenden, stellen Sie sicher, dass die Hostnamen in einer verifizierten Domäne sind.' Der Hauptbestandteil dieser Anweisung ist **"Stellen Sie sicher, dass sich Hostnamen in einer verifizierten Domäne befinden."**

Beachten Sie bei der Fehlerbehebung für ein Problem, das mit dieser Bedingung übereinstimmt, dass das Symptom von der Anrufrichtung abhängt. Wenn der Anruf von einem Telefon vor Ort ausgeht, können Sie davon ausgehen, dass die Cisco WebEx App nicht klingelt. Wenn Sie versuchen, den Anruf aus dem Suchverlauf von Expressways zu verfolgen, würden Sie feststellen, dass der Anruf ihn zum Expressway-E führen und dort anhalten würde. Wenn der Anruf von einer Cisco WebEx App stammt und für den Standort bestimmt war, klingelt das Telefon vor Ort nicht. In diesem Fall würden die Expressway-E und Expressway-C Search History nichts anzeigen.

In diesem speziellen Szenario stammt der Anruf von einem Telefon vor Ort. Mithilfe des Expressway-E-Suchverlaufs können Sie feststellen, dass der Anruf beim Server eingegangen ist. An dieser Stelle können Sie die Diagnoseprotokollierung eintauchen, um festzustellen, was passiert ist. Um diese Analyse zu starten, prüfen Sie zunächst, ob über Port 5062 eine TCP-Verbindung hergestellt und versucht wurde. Durch das Durchsuchen der Expressway-E Diagnoseprotokolle nach "TCP Connecting" und das Durchsuchen des Postenelements mit dem Tag "Dst-port=5062" können Sie feststellen, ob die Verbindung hergestellt wird.

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"**

Nachdem Sie bestätigt haben, dass die TCP-Verbindung hergestellt wurde, können Sie den gegenseitigen TLS-Handshake analysieren, der unmittelbar danach erfolgt. Wie Sie hier im Ausschnitt sehen können, schlägt der Handshake fehl, und das Zertifikat ist unbekannt (**Detail="sslv3-Warnzertifikat unbekannt"**)

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"**

Sehen Sie sich die Paketerfassung mit der Expressway-E-Diagnoseprotokollierung genauer an. Sie sehen, dass der Fehler "Certificate Unknown" (Zertifikat unbekannt) aus der Richtung von Cisco WebEx stammt, wie im Bild gezeigt.

| No. | Time                       | Source        | Destination   | Protocol | S Port | D Port | Length | Info   |
|-----|----------------------------|---------------|---------------|----------|--------|--------|--------|--|
| 3   | 2017-09-26 12:18:08.415918 | 146.20.193.45 | 172.16.2.2    | TCP      | 59720  | 5062   | 74     | 59720->5062 [SYN] Seq=0 win=14600 Len=0 MSS=1380 SACK_PERM=1 TSval=91375166 TSecr=0    |
| 4   | 2017-09-26 12:18:08.415941 | 172.16.2.2    | 146.20.193.45 | TCP      | 5062   | 59720  | 74     | 5062->59720 [SYN, ACK] Seq=0 Ack=1 win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=95527050 |
| 5   | 2017-09-26 12:18:08.426317 | 146.20.193.45 | 172.16.2.2    | TCP      | 59720  | 5062   | 66     | 59720->5062 [ACK] Seq=1 Ack=1 win=14720 Len=0 TSval=91375177 TSecr=955270515           |
| 6   | 2017-09-26 12:18:08.427715 | 146.20.193.45 | 172.16.2.2    | TLSv1.2  | 59720  | 5062   | 266    | client Hello   |
| 7   | 2017-09-26 12:18:08.427728 | 172.16.2.2    | 146.20.193.45 | TCP      | 5062   | 59720  | 66     | 5062->59720 [ACK] Seq=1 Ack=201 win=30080 Len=0 TSval=955270527 TSecr=91375178         |
| 8   | 2017-09-26 12:18:08.440978 | 172.16.2.2    | 146.20.193.45 | TLSv1.2  | 5062   | 59720  | 1780   | Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Do   |
| 9   | 2017-09-26 12:18:08.453269 | 146.20.193.45 | 172.16.2.2    | TCP      | 59720  | 5062   | 66     | 59720->5062 [ACK] Seq=201 Ack=1369 win=17536 Len=0 TSval=91375204 TSecr=955270540      |
| 10  | 2017-09-26 12:18:08.453308 | 146.20.193.45 | 172.16.2.2    | TCP      | 59720  | 5062   | 66     | 59720->5062 [ACK] Seq=201 Ack=1715 win=20352 Len=0 TSval=91375204 TSecr=955270540      |
| 11  | 2017-09-26 12:18:08.455698 | 172.16.2.2    | 146.20.193.45 | TLSv1.2  | 59720  | 5062   | 72     | Alert (Level: Fatal, Description: certificate unknown)                                 |

Certificate Unknown  
Sourced from Spark

Wenn Sie das Default Server-Zertifikat von Expressway-E überprüfen, können Sie sehen, dass der 'Common Name' und 'Subject Alternate Names' nicht die 'Verified Domain' enthalten (**rtp.ciscotac.net**). Sie haben dann Beweise dafür, was dieses Problem verursacht, wie im Bild gezeigt wird.

The image shows a network traffic analysis tool displaying a TLS handshake. The 'Selected Packet' is a TLSv1.2 Record Layer: Handshake Protocol: Certificate. The certificate details include a 'Common Name' field with the value 'amer-expressway01'. A red arrow points from this field to a 'Certificate Information' window. This window shows the 'Issued to' field with the same value and a warning: 'Windows does not have enough information to verify this certificate.' The 'Domain Verification' status is 'not verified'.

An diesem Punkt haben Sie festgestellt, dass das Expressway-E Serverzertifikat entweder von einer öffentlichen Zertifizierungsstelle oder einer internen Zertifizierungsstelle signiert werden muss.

## Lösung

Sie haben zwei Möglichkeiten, dieses Problem zu beheben:

1. Lassen Sie das Expressway-E-Zertifikat von einer [öffentlichen Zertifizierungsstelle](#) signieren, [der Cisco WebEx vertraut](#).

Melden Sie sich bei Expressway an. Navigieren Sie zu **Maintenance > Security > Server certificate**. Wählen Sie **CSR erstellen aus**. Geben Sie die erforderlichen Zertifikatsinformationen ein, und stellen Sie sicher, dass das Feld **Zusätzliche alternative Namen** die **Verified Domain** enthält, die im WebEx Control Hub aufgeführt ist. Klicken Sie auf **CSR erstellen**. Stellen Sie die CSR-Anfrage zur Unterzeichnung an eine externe öffentliche Zertifizierungsstelle (Public CA, CA) bereit. Navigieren Sie nach der Rückgabe des Zertifikats zu **Maintenance > Security > Server certificate**. Wählen Sie im Abschnitt **Neues Zertifikat hochladen** neben **Serverzertifikatdatei auswählen** die Option **Datei auswählen** und wählen Sie das **signierte Zertifikat aus**. Wählen Sie **Serverzertifikatdaten hochladen aus**. Navigieren Sie zu **Maintenance > Security > Trusted CA certificate**. Wählen Sie im Abschnitt **Hochladen** neben **Datei mit vertrauenswürdigen CA-Zertifikaten** die Option **Datei auswählen aus**. Wählen Sie alle Root- und Zwischenzertifikate aus, die von der öffentlichen Zertifizierungsstelle bereitgestellt werden. Wählen Sie **Zertifizierungsstellenzertifikat anhängen aus**. Starten Sie den Expressway-E neu.

2. Lassen Sie das Expressway-E-Zertifikat von einer internen Zertifizierungsstelle signieren und laden Sie die interne Zertifizierungsstelle und Expressway-E auf den Cisco WebEx Control Hub hoch.

Beim Expressway anmelden Navigieren Sie zu **Maintenance > Security > Server certificate**. Wählen Sie **CSR erstellen**. Geben Sie die erforderlichen Zertifikatsinformationen ein, um sicherzustellen, dass das Feld **"Zusätzliche alternative Namen"** die **Verified Domain**



enthält, die im WebEx Control Hub aufgeführt ist. Klicken Sie auf **CSR erstellen**. Bereitstellen der CSR-Anfrage an eine öffentliche Zertifizierungsstelle eines Drittanbieters zur Signierung. Navigieren Sie nach der Rückgabe des Zertifikats zu *Maintenance > Security > Server Certificates*. Wählen Sie im *Abschnitt Neues Zertifikat hochladen* neben *Serverzertifikatdatei auswählen* die *Option Datei auswählen* und dann das signierte Zertifikat aus. Wählen Sie **Serverzertifikatdaten hochladen aus**. Navigieren Sie zu **Maintenance > Security > Trusted CA Certificate**. Wählen Sie im *Abschnitt Hochladen* neben **Datei mit vertrauenswürdigen CA-Zertifikaten** die Option **Datei auswählen aus**. Wählen Sie alle Root- und Zwischenzertifikate aus, die von der öffentlichen Zertifizierungsstelle bereitgestellt werden. Wählen Sie **Zertifizierungsstellenzertifikat anhängen aus**. Starten Sie den Expressway-E neu.

2a) Laden Sie das interne CA- und Expressway-E-Zertifikat auf den Cisco WebEx Control Hub hoch.

1. Melden Sie sich als Administrator beim [Cisco WebEx Control Hub](#) an.
2. Wählen Sie **Services aus**.
3. Wählen Sie **Einstellungen** unter der Hybrid Call Service Card aus.
4. Wählen Sie im **Abschnitt Zertifikate für verschlüsselte SIP-Anrufe** die Option **Hochladen aus**.
5. Wählen Sie die Zertifikate Internal CA (Interne CA) und Expressway-E aus.

## Eingehend: Cisco WebEx an Standort

Fast alle eingehenden Cisco WebEx-Angriffe auf Ausfälle vor Ort führen zu demselben gemeldeten Symptom: "Wenn ich von meiner Cisco WebEx-App zur App eines Kollegen rufe, klingelt die App des Kollegen, das Telefon vor Ort jedoch nicht." Zur Fehlerbehebung in diesem Szenario ist es hilfreich, sowohl den Anrufluss als auch die Logik zu verstehen, die beim Tätigen dieses Anrufs auftreten.

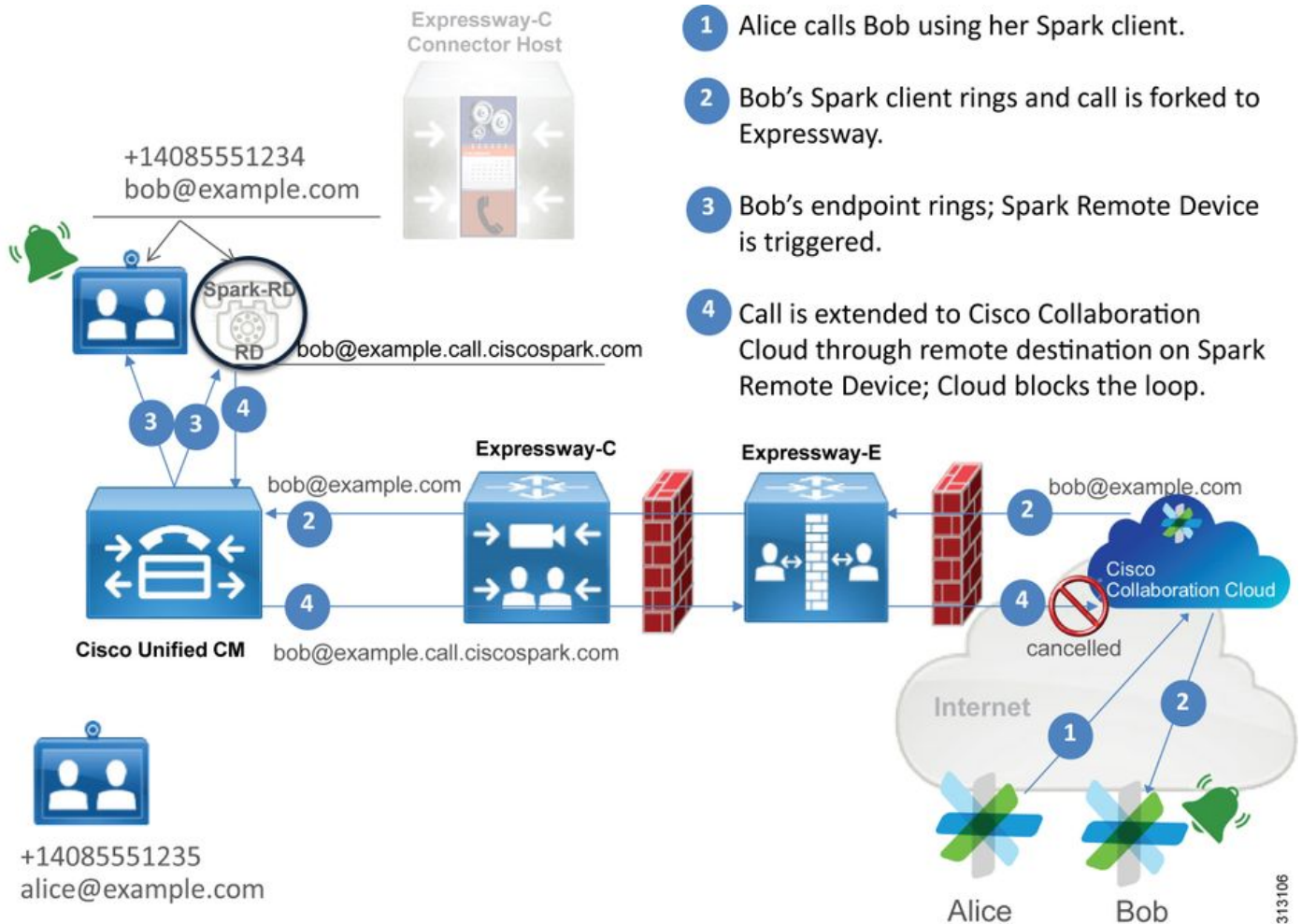
### High-Level-Logik-Fluss

1. Der Anrufer der Cisco WebEx App initiiert den Anruf.
2. Klingelton des angerufenen Teilnehmers
3. Der Anruf wird in die Cisco WebEx Umgebung eingefroren.
4. Die Cisco WebEx Umgebung muss eine DNS-Suche durchführen, die auf dem konfigurierten SIP-Ziel des Kunden im Cisco WebEx Control Hub basiert.
5. Die Cisco WebEx Umgebung versucht, über Port 5062 eine Verbindung zum Expressway herzustellen.
6. Die Cisco WebEx Umgebung versucht, einen TLS-Handshake auf Gegenseitigkeit durchzuführen.
7. Die Cisco WebEx Umgebung sendet eine SIP-INVITE-Nachricht an den Expressway, der an das standortbasierte Collaboration-Endgerät/IP-Telefon weitergeleitet wird.
8. Cisco WebEx und das Unternehmen schließen die SIP-Aushandlung ab
9. Cisco WebEx und das Unternehmen beginnen mit dem Senden und Empfangen von Medien.

### Anrufluss

Navigieren Sie zu **Cisco WebEx-App > Cisco WebEx-Umgebung > Expressway-E > Expressway-C > Standortbasiertes Collaboration Endpoint/IP-Telefon** wie im Bild gezeigt.





Im Folgenden sind einige der häufigsten Probleme aufgeführt, die bei eingehenden Anrufen von Webex zur Infrastruktur vor Ort beobachtet wurden.

### Ausgabe 1 Cisco WebEx kann den Expressway-E DNS SRV/Hostnamen nicht auflösen.

Wenn Sie über Cisco WebEx mit einem standortbasierten Anruffluss nachdenken, ist der erste logische Schritt von Cisco Webex die Kontaktaufnahme mit dem Expressway vor Ort. Wie oben erwähnt, versucht Cisco WebEx, eine Verbindung zum Expressway vor Ort herzustellen, indem es eine SRV-Suche anhand des konfigurierten **SIP-Ziels** durchführt, das auf der Seite **Hybrid Call Service Settings** im [Cisco WebEx Control Hub](#) aufgeführt ist.

Wenn Sie versuchen, eine Fehlerbehebung aus Sicht eines Expressway-E-Diagnoseprotokolls durchzuführen, wird kein Datenverkehr von Cisco WebEx angezeigt. Wenn Sie nach TCP Connecting suchen, wird der Dst-Port=5062 nicht angezeigt. Außerdem wird in Cisco WebEx kein MTLS-Handshake oder SIP-Einladung angezeigt.

In diesem Fall müssen Sie überprüfen, wie das **SIP-Ziel** im Cisco WebEx Control Hub konfiguriert wurde. Sie können auch das **Hybrid Connectivity Test Tool** verwenden, um die Fehlerbehebung zu unterstützen. Das Hybrid Connectivity Test Tool prüft, ob eine gültige DNS-Adresse vorhanden ist, ob Cisco WebEx eine Verbindung zum in der SRV-Suche zurückgegebenen Port herstellen kann und ob der Expressway vor Ort über ein gültiges Zertifikat verfügt, dem Cisco WebEx vertraut.

1. Melden Sie sich beim [Cisco WebEx Control Hub an](#).
2. Services auswählen
3. Wählen Sie den Link Einstellungen in der **Hybrid Call Card** aus.

- Überprüfen Sie im Abschnitt Call Service Connect (Anrufdienst-Connect) die Domäne, die für die öffentliche SIP SRV-Adresse im **SIP**-Zielfeld verwendet wird.
- Wenn der Datensatz korrekt eingegeben wurde, klicken Sie auf **Test**, um festzustellen, ob der Datensatz gültig ist.
- Wie unten abgebildet, können Sie sehen, dass der öffentlichen Domäne kein entsprechender SIP SRV-Datensatz zugeordnet ist, wie im Bild gezeigt.

SIP Destination ⓘ

mtls.rtp.ciscotac.net Test Save

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

Wählen Sie **Testergebnisse anzeigen aus**, und Sie können mehr Details über Fehler sehen, wie im Bild gezeigt.

## Verify SIP Destination

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

Sie können den SRV-Datensatz auch mithilfe von nslookup nachschlagen. Hier sind die Befehle, mit denen Sie überprüfen können, ob das SIP-Ziel vorhanden ist.

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

Wie Sie im Codeblock oben sehen können, wurde der Befehl nslookup initiiert, und der Server ist auf 8.8.8.8 festgelegt, was ein öffentlicher Google DNS-Server ist. Schließlich legen Sie die Datensatztypen für die Suche nach SRV-Datensätzen fest. Anschließend können Sie den vollständigen SRV-Datensatz erstellen, den Sie nachschlagen möchten. Das Endergebnis ist, dass die Anfragen letztendlich das Zeitlimit überschreiten.

## Lösung

- Konfigurieren Sie eine öffentliche SIP SRV-Adresse für das Expressway-E auf der Site, die sie zum Hosten von öffentlichen Domännennamen verwenden.
- Konfigurieren Sie einen Hostnamen, der zur öffentlichen IP-Adresse des Expressway-E aufgelöst wird.

3. Konfigurieren Sie das SIP-Ziel so, dass die in Schritt 1 erstellte Domäne für die SIP SRV-Adresse aufgelistet wird. Melden Sie sich beim [Cisco WebEx Control Hub an.Services](#) auswählenWählen Sie den Link **Einstellungen** in der *Hybrid Call Card aus*.Geben Sie im Abschnitt Call Service Connect (Anrufdienst-Connect) die für die öffentliche SIP-SRV-Adresse verwendete Domäne im Feld **SIP-Ziel ein**. Speichern

**Hinweis:** Wenn der SIP SRV-Datensatz, den Sie verwenden möchten, bereits für die Business-to-Business-Kommunikation verwendet wird, empfehlen wir, eine Teildomäne der Unternehmensdomäne als SIP-Erkennungsadresse im Cisco WebEx Control Hub und folglich einen öffentlichen DNS SRV-Datensatz anzugeben:

Service und Protokoll: \_sips.\_tcp.mtls.example.com  
Priorität: 1  
Gewicht: 10  
Portnummer: 5062  
Ziel: us-expe1.example.com

Die oben genannte Empfehlung stammt direkt aus dem [Cisco WebEx Hybrid Design Guide](#).

#### Alternative Lösung

Wenn der Kunde keinen SIP SRV-Datensatz besitzt (und keinen erstellen möchte), kann er alternativ die durch ":5062" nachgestellte öffentliche IP-Adresse von Expressway auflisten. Dadurch versucht die WebEx Umgebung keine SRV-Suche, sondern stellt eine direkte Verbindung zum **%Expressway\_Pub\_IP%:5062 her**. (Beispiel: 64.102.241.236:5062)

1. Konfigurieren Sie das SIP-Ziel als **%Expressway\_Pub\_IP%:5062**. (Beispiel: 64.102.241.236:5062) Melden Sie sich beim [Cisco WebEx Control Hub an.Services](#) auswählenWählen Sie den Link **Einstellungen** in der *Hybrid Call Card aus*.Geben Sie im Abschnitt Call Service Connect das Feld **%Expressway\_Pub\_IP%:5062** in das Feld **SIP-Ziel ein**. Speichern

Weitere Informationen zur SIP-Zieladresse und/oder zum SRV-Datensatz, der eingerichtet werden muss. Weitere Informationen finden Sie im Abschnitt [Enable Hybrid Call Service Connect for Your Organization](#) im Bereitstellungsleitfaden für Cisco WebEx Hybrid Call Service oder im [Cisco WebEx Hybrid Design Guide](#).

#### Ausgabe 2: Socket-Fehler: Port 5062 ist für Expressway eingehend blockiert

Nach Abschluss der DNS-Auflösung versucht die Cisco WebEx Umgebung, über Port 5062 eine TCP-Verbindung zur IP-Adresse herzustellen, die bei der DNS-Suche zurückgegeben wurde. Diese IP-Adresse ist die öffentliche IP-Adresse des standortbasierten Expressway-E. Wenn die Cisco WebEx Umgebung diese TCP-Verbindung nicht herstellen kann, schlägt der eingehende Anruf an den Standort anschließend fehl. Das Symptom für diese spezielle Situation ist identisch mit fast allen anderen Ausfällen eingehender Cisco WebEx-Anrufe: das Telefon am Standort klingelt nicht.

Wenn Sie dieses Problem mithilfe der Expressway-Diagnoseprotokolle beheben, wird kein Datenverkehr von Cisco WebEx angezeigt. Wenn Sie nach TCP-Verbindung suchen, werden weder Verbindungsversuche für den Dst-Port=5062 noch ein nachfolgender MTLS-Handshake oder SIP-Einladung von Cisco WebEx angezeigt. Da die Expressway-E-Diagnoseprotokollierung in dieser Situation nicht von Nutzen ist, stehen Ihnen einige Überprüfungsverfahren zur

Verfügung:

1. Paketerfassung über die externe Schnittstelle der Firewall
2. Ein Port-Überprüfungsprogramm nutzen
3. Verwenden des Testtools für Hybrid Connectivity

Da das Hybrid Connectivity Test Tool direkt in den Cisco WebEx Control Hub integriert ist und die Cisco WebEx Umgebung simuliert, die versucht, eine Verbindung mit dem Expressway vor Ort herzustellen, ist es die ideale Prüfmethode. So testen Sie die TCP-Verbindung in der Organisation:

1. Melden Sie sich beim [Cisco WebEx Control Hub an](#).
2. Services auswählen
3. Wählen Sie den Link Einstellungen in **der Hybrid Call Card aus**.
4. Stellen Sie im Abschnitt Call Service Connect (Anrufverbindung) sicher, dass der im SIP-Ziel eingeegebene Wert korrekt ist.
5. Klicken Sie auf Test, wie im Bild gezeigt.

SIP Destination ⓘ

64.102.241.236:5062

Test Save

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

6. Da der Test fehlgeschlagen ist, können Sie auf den Link **Testergebnisse anzeigen** klicken, um die Details wie im Bild dargestellt zu überprüfen.

### Verify SIP Destination

IP address lookup

IP  
64.102.241.236

| Test for 64.102.241.236:5062 |               |  |
|------------------------------|---------------|--|
| Tests                        | Result        | Details  |
| Connecting to IP             | Successful    |  |
| Socket test                  | Failed        | TCP Connection failure: Check network connectivity, connection speed, and/or firewall configuration. |
| SSL Handshake                | Not performed |  |
| Ping                         | Not performed |  |

Wie in der Abbildung oben gezeigt, ist der Socket-Test beim Verbindungsversuch mit 64.102.241.236:5062 fehlgeschlagen. Da diese Daten zusätzlich zu den Expressway-Diagnoseprotokollen/-pcaps keine Verbindungsversuche anzeigen, verfügen Sie jetzt über genügend Beweise, um die Firewall-ACL/NAT/Routing-Konfiguration zu untersuchen.

Lösung

Da dieses Problem nicht durch die Cisco WebEx Umgebung oder die standortbasierte



Collaboration-Ausrüstung verursacht wird, müssen Sie sich auf die Firewall-Konfiguration konzentrieren. Da Sie nicht notwendigerweise vorhersagen können, mit welchem Firewall-Typ Sie eine Verbindung herstellen möchten, müssen Sie sich auf jemanden verlassen, der mit dem Gerät vertraut ist. Es ist möglich, dass das Problem mit einer Fehlkonfiguration der Firewall-ACL, NAT oder Routing zusammenhängt.

### Ausgabe 3 Socket-Fehler: Expressway-E hört auf Port 5062 nicht zu.

Diese spezielle Bedingung wird oft falsch diagnostiziert. Häufig wird davon ausgegangen, dass die Firewall die Ursache dafür ist, dass der Datenverkehr über Port 5062 blockiert wird. Zur Fehlerbehebung in dieser speziellen Situation können Sie die Techniken im Szenario "Port 5062 ist eingehend mit dem Expressway blockiert" verwenden. Sie werden feststellen, dass das Hybrid Connectivity Test Tool und jedes andere Tool, das zur Überprüfung der Port-Konnektivität verwendet wird, fehlschlagen. Die erste Annahme besteht darin, dass die Firewall den Datenverkehr blockiert. Die meisten Leute überprüfen dann die Diagnoseprotokollierung vom Expressway-E, um festzustellen, ob sie die TCP-Verbindung sehen können, die versucht, eine Verbindung herzustellen. Sie suchen in der Regel nach einem Protokollposten wie diesem, wie im Bild gezeigt.

```
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"
```

In dieser Bedingung ist der jeweilige Protokolleintrag oben nicht vorhanden. Daher werden viele Menschen die Situation falsch diagnostizieren und annehmen, dass es sich um die Firewall handelt.

Wenn die Diagnoseprotokollierung eine Paketerfassung enthält, können Sie überprüfen, ob die Firewall die Ursache ist. Im Folgenden sehen Sie ein Beispiel für die Paketerfassung aus dem Szenario, in dem das Expressway-E über Port 5062 nicht zuhörte. Diese Erfassung wurde mithilfe von `tcp.port==5062` als angewendeter Filter gefiltert, wie im Bild gezeigt.

The screenshot shows a Wireshark packet capture with the filter `tcp.port==5062`. The capture shows four packets:

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

Annotations in the image:

- A blue arrow points to the filter `tcp.port==5062`.
- A blue arrow points to the info field of packet 55: `74 34351->5062 [SYN] Seq=0 win=14600 Len=0 MSS=1380`, with the text "Spark TCP SYN packet received" above it.
- A blue arrow points to the info field of packet 56: `54 5062->34351 [RST, ACK] Seq=1 Ack=1 win=0 Len=0`, with the text "Immediate RST sent from the Expressway" below it.

Wie Sie in der Paketerfassung sehen können, die über Expressway-E erfolgt ist, wird der Datenverkehr über TCP-Port 5062 nicht von der Firewall blockiert, sondern kommt tatsächlich an. In Paket Nr. 56 können Sie sehen, dass der Expressway-E den RST sofort sendet, nachdem das erste TCP-SYN-Paket angekommen ist. Anhand dieser Informationen können Sie feststellen, dass das Problem auf den Expressway-E, der das Paket empfängt, isoliert ist. Sie müssen das Problem aus der Perspektive von Expressway-E beheben. Berücksichtigen Sie anhand der Beweise mögliche Gründe, warum das Expressway-E das Paket RST durchführen würde. Zwei Möglichkeiten, die diesem Verhalten zuzuschreiben sind, sind:

1. Auf dem Expressway-E sind Firewall-Regeln eingerichtet, die den Datenverkehr blockieren können.



2. Der Expressway-E überwacht keinen gegenseitigen TLS-Datenverkehr und/oder überwacht keinen Datenverkehr über Port 5062.

Die Firewall-Funktionalität von Expressway-E existiert unter *System > Protection > Firewall rules > Configuration*. Bei der Überprüfung in dieser Umgebung war keine Firewall-Konfiguration vorhanden.

Es gibt mehrere Möglichkeiten, zu überprüfen, ob das Expressway-E auf wechselseitigen TLS-Datenverkehr über Port 5062 wartet. Sie können dies entweder über die Webschnittstelle oder die CLI als Stammbenutzer tun.

Wenn Sie **netstat -an** ausgeben, verwenden Sie die **Schnellstraße. | grep ':5062'**, sollten Sie einige Ausgaben ähnlich wie unten sehen.

```
~ # 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
```

Diese Informationen können auch über die Webschnittstelle des Expressway-E erfasst werden. Weitere Informationen finden Sie in den nachfolgenden Schritten.

1. Melden Sie sich bei Expressway-E an.

2. Navigieren Sie zu **Maintenance Tools > Port Usage > Local Inbound Ports (Wartungstools > Portnutzung > Lokale eingehende Ports)**.

3. Nach Typ SIP und IP-Port 5062 suchen. (rot markiert, wie im Bild gezeigt)

| Local inbound ports |                       |          |             |         |           |                           | You are here: <a href="#">Home</a> |
|---------------------|-----------------------|----------|-------------|---------|-----------|---------------------------|------------------------------------|
| Type                | Description           | Protocol | IP address  | IP port | Transport | Actions                   |                                    |
| H.323               | Registration UDP port | H.323    | 192.168.1.6 | 1719    | UDP       | <a href="#">View/Edit</a> |                                    |
| H.323               | Registration UDP port | H.323    | 172.16.2.2  | 1719    | UDP       | <a href="#">View/Edit</a> |                                    |
| SIP                 | TCP port              | SIP      | 192.168.1.6 | 5060    | TCP       | <a href="#">View/Edit</a> |                                    |
| SIP                 | TCP port              | SIP      | 172.16.2.2  | 5060    | TCP       | <a href="#">View/Edit</a> |                                    |
| SIP                 | TLS port              | SIP      | 192.168.1.6 | 5061    | TCP       | <a href="#">View/Edit</a> |                                    |
| SIP                 | TLS port              | SIP      | 172.16.2.2  | 5061    | TCP       | <a href="#">View/Edit</a> |                                    |
| SIP                 | Mutual TLS port       | SIP      | 192.168.1.6 | 5062    | TCP       | <a href="#">View/Edit</a> |                                    |
| SIP                 | Mutual TLS port       | SIP      | 172.16.2.2  | 5062    | TCP       | <a href="#">View/Edit</a> |                                    |

Jetzt, da Sie wissen, was Sie sehen sollten, können Sie das mit der aktuellen Umgebung vergleichen. Aus CLI-Perspektive: Wenn Sie **netstat -an** ausführen | **grep ':5062'** sieht die Ausgabe wie folgt aus:

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

Darüber hinaus zeigt die Web-UU den unter Lokale Eingangsports aufgeführten mutuellen TLS-Port nicht an.

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

Anhand dieser Daten können Sie feststellen, dass das Expressway-E keinen gegenseitigen TLS-Datenverkehr überwacht.

## Lösung

Um dieses Problem zu beheben, müssen Sie sicherstellen, dass der gegenseitige TLS-Modus aktiviert ist und dass der gegenseitige TLS-Port auf dem Expressway-E auf 5062 festgelegt ist:

1. Melden Sie sich bei Expressway-E an.
2. Navigieren Sie zu **Konfiguration > Protokolle > SIP**.
3. Stellen Sie sicher, dass der gegenseitige TLS-Modus auf **Ein** eingestellt ist.
4. Stellen Sie sicher, dass der gegenseitige TLS-Port auf **5062** eingestellt ist.
5. Klicken Sie auf **Speichern** wie im Bild gezeigt.

The screenshot shows the SIP Configuration page. The 'Mutual TLS mode' is set to 'On' and the 'Mutual TLS port' is set to '5062'. Other settings include SIP mode (On), UDP mode (Off), UDP port (5060), TCP mode (On), TCP port (5060), and TLS mode (On).

## Ausgabe 4: Expressway-E oder C unterstützen vorinstallierte SIP-Routen-Header nicht

Mit Hybrid Call Service Connect erfolgt die Anrufweiterleitung basierend auf dem **Routen-Header**. Der Routen-Header wird basierend auf den Informationen aufgefüllt, die der Call Service Aware (Expressway Connector)-Teil der Lösung für Cisco WebEx bereitstellt. Der Host für den Expressway Connector fragt Unified CM für Benutzer ab, die für den Call Service aktiviert sind, und ruft sowohl den **Directory URI** als auch den **Cluster FQDN des Unified CM-Home-Clusters** ab. Sehen Sie sich dieses Beispiel an, indem Sie Alice und Bob verwenden:

| VerzeichnisURI    | Header für Zielroute  |
|-------------------|-----------------------|
| bob@example.com   | emea-cucm.example.com |
| alice@example.com | us-cucm.example.com   |

Wenn Alice oder Bob einen Anruf tätigen, wird der Anruf an den standortbasierten Unified CM weitergeleitet, sodass er an den Cisco WebEx RD verankert werden kann, bevor er an den angerufenen Benutzer weitergeleitet wird.

Wenn Alice Bob anrufen würde, würde der Anruf an *Alice's Unified CM Home Cluster FQDN (us-cucm.example.com)* weitergeleitet. Wenn Sie die SIP-INVITE-Nachricht analysieren, die Cisco Webex eingehend an das Expressway-E sendet, finden Sie die folgenden Informationen im SIP-Header

**URI anfordern** SIP: bob@example.com

**Routen-Header** sip:us-cucm.example.com;lr

Aus der Perspektive des Expressway werden die Suchregeln so konfiguriert, dass der Anruf nicht über den Request URI, sondern über den **Route Header (us-cucm.example.com)** weitergeleitet wird - in diesem Fall über das Unified CM-Home-Cluster von Alice.

Mit diesem Basissatz können Sie die Fehlerbehebung verstehen, wenn die Expressways falsch konfiguriert sind, was dazu führt, dass die obige Logik nicht funktioniert. Da bei fast allen anderen Anrufen, die über die Hybrid Call Service Connect-Verbindung eingehen, *klingselt das Telefon am Standort nicht*.

Bevor Sie die Diagnoseprotokolle auf dem Expressway analysieren, überlegen Sie, wie Sie diesen Anruf identifizieren können:

1. Der SIP-Anforderungs-URI ist der **Verzeichnis-URI des angerufenen Teilnehmers**.
2. Das Feld SIP FROM wird mit dem **anrufenden Teilnehmer** formatiert, der als "**Nachname**" `< sip:WebexDisplayName@subdomain.call.ciscospark.com >` aufgeführt ist.

Anhand dieser Informationen können Sie die Diagnoseprotokolle nach dem **VerzeichnisURI des angerufenen Teilnehmers, dem Vor- und Nachnamen des anrufenden Teilnehmers oder der Cisco WebEx SIP-Adresse des anrufenden Teilnehmers** durchsuchen. Wenn Sie über keine dieser Informationen verfügen, können Sie nach "INVITE SIP:" suchen, in dem alle SIP-Anrufe, die über die Expressway ausgeführt werden, gefunden werden. Sobald Sie die SIP-EINLADUNG für den eingehenden Anruf identifiziert haben, können Sie die SIP-Anruf-ID suchen und kopieren. Nachdem Sie diesen Wert eingegeben haben, können Sie einfach die Diagnoseprotokolle anhand der Anruf-ID durchsuchen, um alle Nachrichten anzuzeigen, die zu diesem Anrufabschnitt gehören.

Eine weitere Möglichkeit, das Routing-Problem zu isolieren, besteht darin zu bestimmen, wie weit der Anruf in das Unternehmen geht. Sie können versuchen, nach den oben auf Expressway-C angegebenen Informationen zu suchen, um festzustellen, ob der Anruf so weit weitergeleitet wurde. In diesem Fall werden Sie wahrscheinlich mit der Untersuchung beginnen.

In diesem Szenario sehen Sie, dass der Expressway-C die INVITE-Nachricht vom Expressway-E erhalten hat.

```
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=35464;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>

Wichtig ist, dass der **Routen-Header (Cluster FQDN)** immer noch intakt ist. Es wird jedoch keine Suchlogik basierend auf dem Route-Header (Cluster FQDN) **cucm.rtp.ciscotac.net** ausgeführt. Stattdessen sehen Sie, dass die Nachricht sofort mit einem **404 Not Found (Nicht gefunden)** abgelehnt wird.

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

Im Vergleich zu einem Arbeitsszenario wird im Arbeitsszenario die Suchlogik basierend auf dem Router Header (Cluster FQDN) ausgeführt

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'"**

Sie sehen dann, dass Expressway-C den Anruf korrekt an den Unified CM weiterleitet (192.168.1.21).

2017-09-22T13:56:02.232-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-22 17:56:02,232"  
Module="network.sip" Level="DEBUG": Action="Sent" Local-ip="192.168.1.5" Local-port="25606" Dst-ip="192.168.1.21" Dst-port="5065" Msg-Hash="866788495063340574"  
SIPMSG:  
|**INVITE sip:jorobb@rtp.ciscotac.net** SIP/2.0  
Via: SIP/2.0/TCP 192.168.1.5:5060;**egress-zone=CUCM11**;branch=z9hG4bK251d6daf044e635607cc13d244b9ea45138220.69ccb8de20a0e853c1313782077f77b5;proxy-call-id=17aa8dc7-422c-42ef-bdd9-b9750fbd0edf;rport  
Via: SIP/2.0/TLS 192.168.1.6:7003;**egress-zone=HybridCallServiceTraversal**;branch=z9hG4bKba323da436b2bc288200d56d11f02d4d272;proxy-call-id=32c76cef-e73c-4911-98d0-e2d2bb6fec77;received=192.168.1.6;rport=7003;**ingress-zone=HybridCallServiceTraversal**  
Via: SIP/2.0/TLS 192.168.1.6:5073;branch=z9hG4bK06cde3f662d53a210b5b4b11b85500c19;x-cisco-local-service=nettle;received=192.168.1.6;rport=42533;ingress-zone=DefaultZone  
Via: SIP/2.0/TLS 64.102.241.236:5061;egress-zone=DefaultZone;branch=z9hG4bK297799f31d0785ff7449e1d7dbe3595b271.2ed90cbcd5b79c6cffad9ecd84cc8337;proxy-call-id=3be87d96-d2e6-4489-b936-8f9cb5ccaa5f;received=172.16.2.2;rport=25005  
Via: SIP/2.0/TLS 192.168.4.146:5062;branch=z9hG4bK043ca6360f253c6abed9b23fbef9819;received=148.62.40.64;rport=36149;ingress-zone=HybridCallServicesDNS  
Via: SIP/2.0/TLS 127.0.0.1:5070;branch=z9hG4bK-353038-8c648a16c2c5d7b85fa5c759d59aa190;rport=47732  
Call-ID: daa1a6fa546ce76591fc464f0a50ee32@127.0.0.1  
CSeq: 1 INVITE

Contact: <sip:192.168.1.6:5073;transport=tls>;call-type=squared  
From: "pstoiano test" <sip:pstoiano-test@dmzlab.call.ciscospark.com>;tag=567490631  
To: <sip:jorobb@rtp.ciscotac.net>  
Max-Forwards: 14  
**Route:**

Record-Route: <sip:proxy-call-id=17aa8dc7-422c-42ef-bdd9-b9750fbd0edf@192.168.1.5:5060;transport=tcp;lr>  
Record-Route: <sip:proxy-call-id=17aa8dc7-422c-42ef-bdd9-b9750fbd0edf@192.168.1.5:5061;transport=tls;lr>  
Record-Route: <sip:proxy-call-id=32c76cef-e73c-4911-98d0-e2d2bb6fec77@192.168.1.6:7003;transport=tls;lr>  
Record-Route: <sip:proxy-call-id=32c76cef-e73c-4911-98d0-e2d2bb6fec77@192.168.1.6:5061;transport=tls;lr>  
Allow: INVITE,ACK,BYE,CANCEL,INFO,OPTIONS,REFER,SUBSCRIBE,NOTIFY  
User-Agent: TANDBERG/4352 (X8.10.2-b2bua-1.0)

Nach Analyse der Diagnoseprotokollierung, die das Problem auf Expressway-C isoliert und einen bestimmten Fehler (404 Not Found), können Sie sich darauf konzentrieren, was diese Art von Verhalten verursachen würde. Folgende Punkte sollten berücksichtigt werden:

1. Anrufe werden über Suchregeln in und aus Zonen auf dem Expressway verschoben.
2. Die Expressways verwenden Logik, die als Preloaded SIP Routen Support (Unterstützung für vorinstallierte SIP-Routen) bezeichnet wird und SIP INVITE-Anfragen verarbeitet, die Router-Header enthalten. Dieser Wert kann in den Zonen (Traversal-Server, Traversal-Client, Neighbor) sowohl auf dem Expressway-C als auch auf dem Expressway-E ein- oder ausgeschaltet werden.

Sie können jetzt die xConfiguration verwenden, um die Konfiguration sowohl auf dem Expressway-E Traversal-Server als auch auf den Expressway-C Client-Zonen anzuzeigen, insbesondere auf den Zonen, die für Hybrid Call Service Connect eingerichtet sind. Zusätzlich zur Zonenkonfiguration können Sie die Suchregeln analysieren, die so konfiguriert sind, dass dieser Anruf von einer Zone an eine andere weitergeleitet wird. Sie wissen auch, dass der Expressway-E den Anruf an den Expressway-C weitergeleitet hat, sodass die Traversal-Serverzonenkonfiguration dort höchstwahrscheinlich korrekt eingerichtet ist.

Um dies zu unterbrechen, teilt uns die folgende xConfig mit, dass der Name dieser Zone als **Hybrid Call Service Traversal** bezeichnet wird. Sie ist vom **TraversalServer**-Zonentyp. Es kommuniziert über den SIP TCP-Port **7003** mit dem Expressway-C.

Der Hauptbestandteil des Hybrid Call Service besteht darin, dass er über vorinstallierte SIP-Routen mit Unterstützung von On verfügen muss. Die Expressway Web Interface nennt diesen Wert **Preloaded SIP routen support**, während die xConfiguration sie als **SIP PreloadedSipRoutes Accept** anzeigt

#### **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 UDPPProbe KeepAliveInterval: "20"
*c xConfiguration Zones Zone 7 TraversalServer UDPPProbe RetryCount: "5"
*c xConfiguration Zones Zone 7 TraversalServer UDPPProbe RetryInterval: "2"
*c xConfiguration Zones Zone 7 Type: "TraversalServer"

```

Sie können auch festlegen, dass dieser Zone Suchregel 3 (WebEx Hybrid) zugeordnet ist. Die Suchregel sendet im Wesentlichen einen "Any"-Alias, der über die DNS-Zone der Hybrid Call Services eingeht und an die Zone oben übergibt, Hybrid Call Service Traversal. Wie erwartet werden sowohl die Zone "Search Rule" (Suchregel) als auch die Zone "Traversal Server" (Traversal-Server) auf dem Expressway-E korrekt konfiguriert.

```

*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"

```

Wenn Sie sich auf die xConfiguration des Expressway-C konzentrieren, können Sie zunächst nach der Traversal Client Zone für WebEx Hybrid suchen. Eine einfache Möglichkeit, diese Nummer zu finden, besteht in der Suche nach der Portnummer, die Sie aus der Expressway-E xConfiguration (SIP-Port: "7003"). So können Sie schnell die richtige Zone in der xConfiguration identifizieren.

Wie zuvor können Sie den Zonennamen (Hybrid Call Service Traversal), den Typ (Traversal Client) und die Konfiguration für die SIP PreloadedSipRoutes Accept (Preloaded SIP Routes Support) erlernen. Wie Sie in dieser xConfiguration sehen können, ist dieser Wert auf Off (Aus) gesetzt. Basierend auf dem Bereitstellungsleitfaden für Cisco WebEx Hybrid Call Services sollte dieser Wert auf On (Ein) eingestellt sein.

Wenn wir die Definition der SIP-Routenunterstützung überprüfen, können wir deutlich sehen, dass Expressway-C eine Nachricht zurückweisen soll, wenn dieser Wert auf Off gesetzt ist UND der INVITE einen Routen-Header enthält: **"Vorgeladene SIP-Routen des Switches unterstützen Off, wenn die Zone SIP-INVITE-Anfragen mit diesem Header ablehnen soll."**

#### 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/11YDd76O/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"
```

An diesem Punkt haben Sie das Problem auf eine Fehlkonfiguration der Expressway-C Traversal Client Zone Konfiguration zurückgeführt. Sie müssen die Unterstützung für vorinstallierte SIP-Routen auf On (Ein) umstellen.

#### Lösung

So stellen Sie die Unterstützung der vorinstallierten SIP-Routen richtig ein:

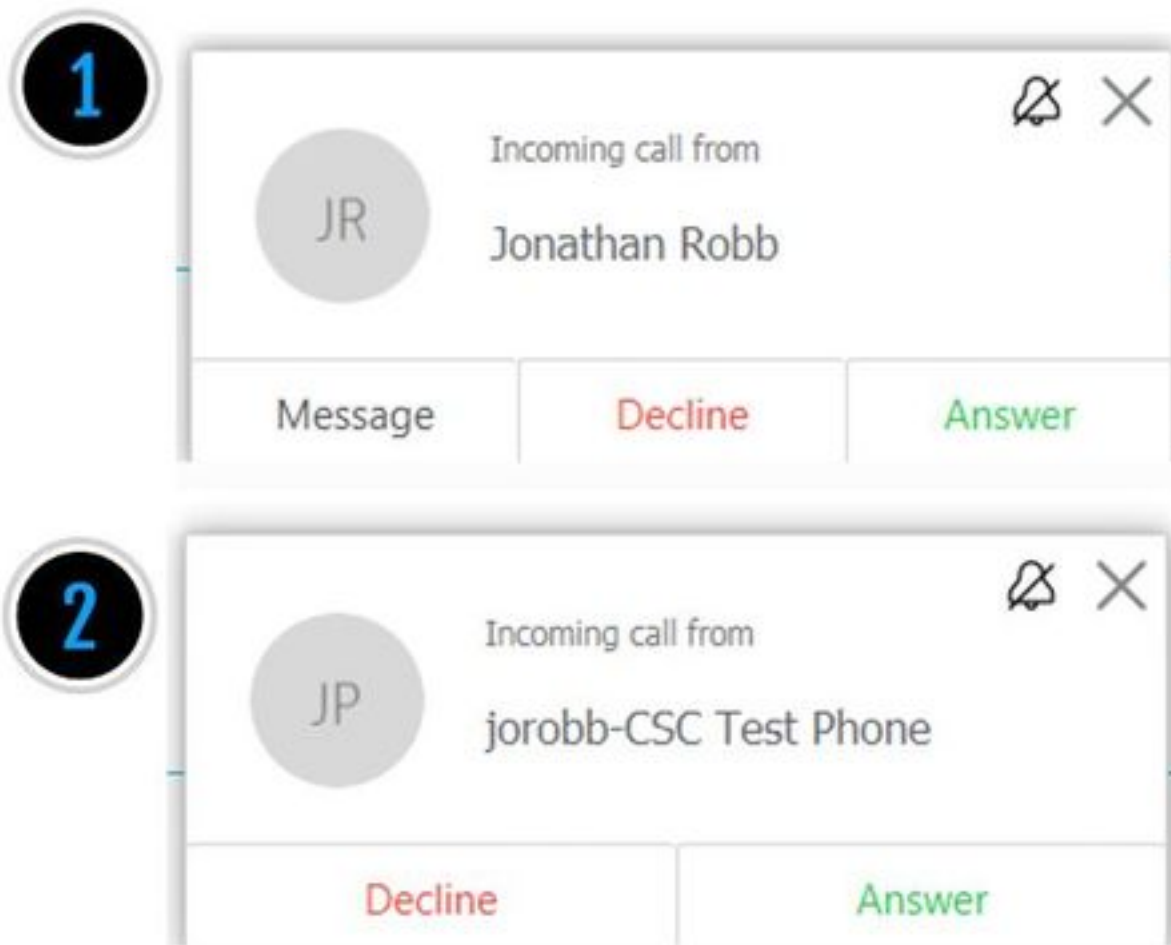
1. Melden Sie sich bei Expressway-C an.
2. Navigieren Sie zu **Konfiguration > Zonen > Zonen**
3. Wählen Sie die Client-Zone für Hybrid Call Service Traversal aus (die Bezeichnung variiert je nach Kunde).
4. Stellen Sie die **Unterstützung für vorinstallierte SIP-Routen auf Ein ein**.
5. Wählen Sie **Speichern**

**Hinweis:** Während dieses Szenario den Ausfall auf dem Expressway-C zeigte, konnten auf dem Expressway-E dieselben Diagnoseprotokollierungsfehler festgestellt werden, wenn die **Unterstützung für vorinstallierte SIP-Routen** in der WebEx Hybrid Call Traversal-Server-Zone deaktiviert war. In diesem Fall hätten Sie nie gesehen, der Anruf erreichte Expressway-C und die Expressway-E wäre für die Ablehnung des Anrufs und das Senden der 404 Not

Found verantwortlich gewesen.

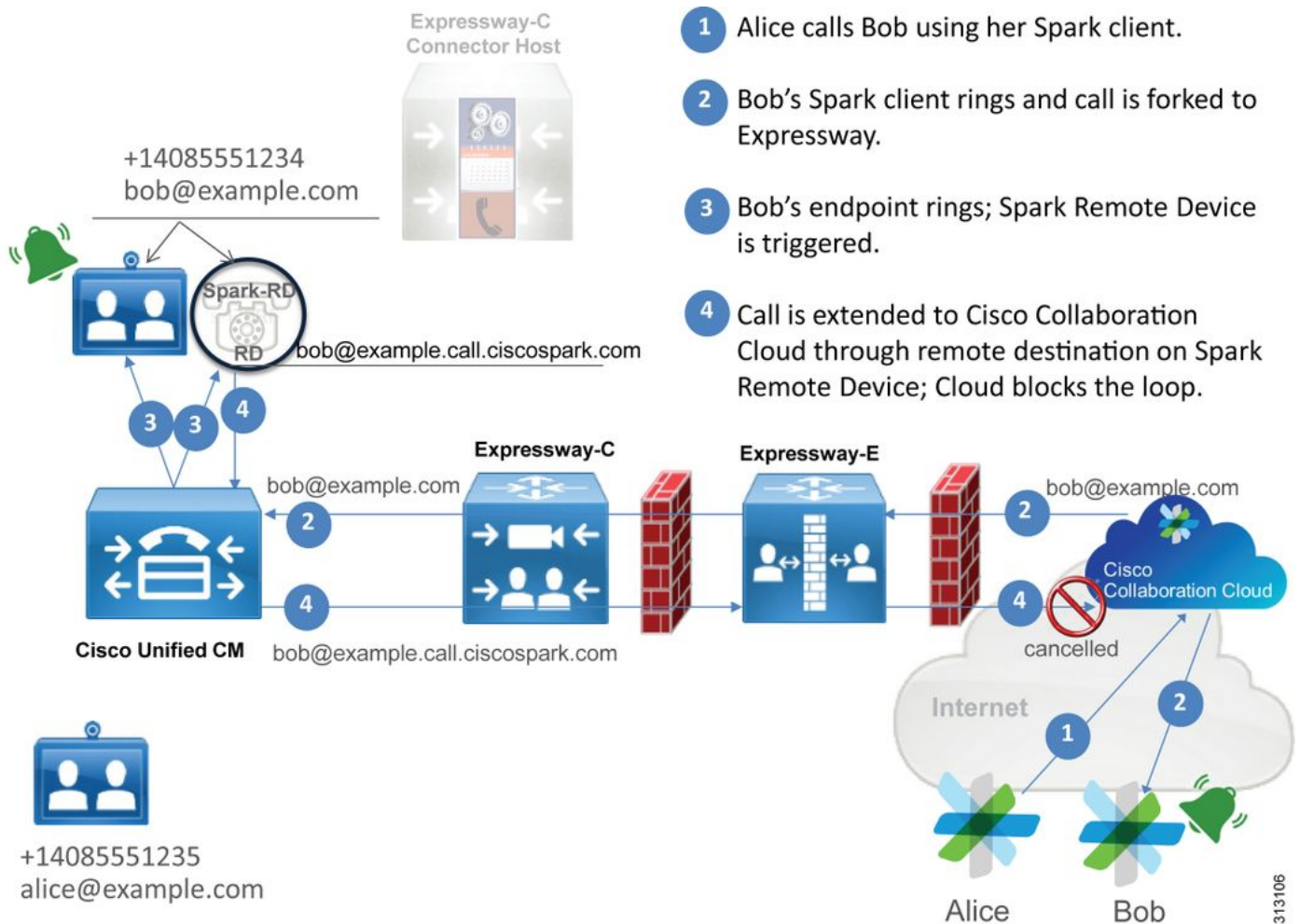
### Ausgabe 5 Die Cisco WebEx App erhält zwei Anrufbenachrichtigungen (Toasts).

Dieses spezielle Problem ist zufällig das einzige eingehende AnrufszENARIO, das nicht dazu führt, dass Anrufe abgebrochen werden. Bei diesem Problem erhält die Person, die den Anruf entgegennimmt (angerufener Teilnehmer), zwei Benachrichtigungen (Toasts) in der Cisco WebEx-App von der Person, die den Anruf getätigt hat (anrufender Teilnehmer). Die erste Benachrichtigung wird von Cisco WebEx generiert, die zweite Benachrichtigung von der standortbasierten Infrastruktur. Im Folgenden finden Sie Beispiele für die beiden Benachrichtigungen, die wie im Bild gezeigt empfangen werden.



Die erste Benachrichtigung (Toast) stammt von der Person, die den Anruf (Anrufer) von der Cisco WebEx Seite initiiert. Die Anrufer-ID in dieser Instanz ist der Anzeigename des Benutzers, der den Anruf initiiert. Die zweite Benachrichtigung (Toast) stammt vom CTI vor Ort oder vom Cisco WebEx RD, der dem Benutzer zugewiesen ist, der den Anruf tätigt. Zunächst scheint dieses Verhalten merkwürdig. Wenn Sie jedoch das Diagramm für eingehende Anrufe (im Cisco WebEx Hybrid Call Design Guide) lesen, ist das Verhalten sinnvoller, wie im Bild gezeigt.





Aus dieser Abbildung können Sie sehen, dass die Alice Bob über ihre Cisco WebEx-App anruft und dass der Anruf am Standort entgegengenommen wird. Dieser Aufruf sollte mit dem Verzeichnis-URI übereinstimmen, der dem Telefon von Bob zugewiesen ist. Das Problem besteht darin, dass bei diesem Design der Directory-URI auch seinem CTI-RD oder Cisco WebEx RD zugewiesen wird. Wenn der Anruf dem CTI-RD oder dem Cisco WebEx RD angeboten wird, wird der Anruf daher zurück an Cisco WebEx gesendet, da auf dem Gerät ein Remote-Ziel für bob@example.call.ciscospark.com konfiguriert ist. Cisco WebEx reagiert mit dieser Situation, indem es den jeweiligen Anrufabschnitt abbricht.

Damit Cisco WebEx den Anrufabschnitt ordnungsgemäß abbrechen kann, musste Cisco WebEx zunächst einen Parameter in den SIP-Header einfügen, nach dem gesucht wird, um den Anruf abzubrechen. Der Parameter, den Cisco Webex in die SIP INVITE-Nachricht einfügt, wird als "**call-type=squared**" bezeichnet und wird in den Contact-Header eingegeben. Wenn dieser Wert aus der Nachricht entfernt wird, versteht Cisco WebEx nicht, wie der Anruf abgebrochen wird.

Anhand dieser Informationen können Sie das zuvor vorgestellte Szenario erneut aufrufen, in dem die Cisco Webex-App des Benutzers zwei Benachrichtigungen (Toasts) erhielt, als der Cisco Webex-Benutzer Jonathan Robb einen Anruf tätigte. Um dieses Problem zu beheben, müssen Sie immer die Diagnoseprotokollierung von Expressway-C und Expressway-E sammeln. Als Ausgangspunkt können Sie die Expressway-E-Protokolle überprüfen, um festzustellen, dass die SIP-INVITE-Nachricht tatsächlich den **Anruftyp=Quadrat-Wert** im Contact-Header des ursprünglichen eingehenden Cisco WebEx INVITEs enthält. Dadurch wird sichergestellt, dass die Firewall die Nachricht nicht manipuliert. Im Folgenden sehen Sie einen Beispielausschnitt der INVITE-Nachricht, die von diesem Szenario aus in den Expressway-E geht.

```
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:

Der Contact-Header hat den **Anruftyp=squared**-Wert. An diesem Punkt muss der Anruf über die Expressway weitergeleitet und aus der WebEx Hybrid Traversal Server-Zone heraus gesendet werden. Wir können die Expressway-E-Protokolle durchsuchen, um zu ermitteln, wie der Anruf aus dem Expressway-E gesendet wurde. Dies gibt uns eine Idee, ob der Expressway-E die INVITE in irgendeiner Weise manipuliert.

```
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=z9hG4bK52aac9a181192566e01b98ae0280bdff858.0e65cdf078cabb269eecb6bce132
8be;proxy-call-id=ec51e8da-e1a3-4210-95c9-494d12debc8;received=172.16.2.2;rport=25016
Via: SIP/2.0/TLS
192.168.5.164:5062;branch=z9hG4bK564cd36d87f3417513c9b559dc666f71;received=146.20.193.73;rport=4
0342;ingress-zone=HybridCallServicesDNS
Via: SIP/2.0/TLS 127.0.0.1:5070;branch=z9hG4bK-3237-5c5060d07ecc546a0bb861ef52a5f507;rport=43306
Call-ID: 6bc0ca8210c0b48df69f38057ec1e48b@127.0.0.1
CSeq: 1 INVITE
Contact: <sip:192.168.1.6:5073;transport=tls> <-- Webex inserted value is now missing
From: "Jonathan Robb"
```

;tag=540300020

To:

Max-Forwards: 15

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

Beachten Sie bei der Überprüfung dieser SIP-INVITE-Nachricht, die vom Expressway-E an den Expressway-C gesendet wird, dass der Contact-Header den **Call-type=squared** fehlt. Eine weitere Anmerkung ist, dass in Zeile 4 die Ausgangszone gleich **HybridCallServiceTraversal** ist. Sie können nun zu dem Schluss kommen, dass die Cisco WebEx App beim Wählen eine zweite Benachrichtigung (Toast) erhält, weil der Expressway-E den **Call-type=squared**-Tag aus dem SIP INVITE-Contact-Header entfernt. Die Frage, die beantwortet werden muss, ist, was die Ursache für diesen entpackten Header sein könnte.

Der Anruf muss über die Hybrid Call Service Traversal weitergeleitet werden, die Sie auf der Expressway eingerichtet haben, damit die Untersuchung beginnen kann. Wenn Sie die xConfiguration haben, können Sie sehen, wie diese Zone konfiguriert wurde. Um die Zone in der xConfiguration zu identifizieren, können Sie einfach den in der Via-Zeile aufgezeichneten Namen verwenden, der in den Protokollen ausgegeben wird. Sie können sehen, dass es als Egress-Zone=HybridCallServiceTraversal bezeichnet wurde. Wenn dieser Name in die Via-Zeile des SIP-Headers gedruckt wird, werden die Leerzeichen entfernt. Der tatsächliche Zonenname aus Sicht von xConfiguration hätte Leerzeichen und wird bei Hybrid Call Service Traversal formatiert.

```
*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"
```

Wenn Sie die Einstellungen für die Hybrid Call Service Traversal festlegen, können Sie nach

möglichen Einstellungen suchen, die sich durch Folgendes auszeichnen:

- SIP PreloadedSIPRoutes Accept: Ein
- SIP-ParameterReservierungsmodus: Aus

Über die Webschnittstelle eines Expressway können Sie sehen, was die Definition dieser Werte ist und was sie tun.

### Unterstützung von vorinstallierten SIP-Routen

Vorinstallierte SIP-Routen des Switches unterstützen On, damit diese Zone SIP-INVITE-Anfragen verarbeiten kann, die den Route-Header enthalten.

Vorinstallierte SIP-Routen des Switches unterstützen Off, wenn die Zone SIP-INVITE-Anfragen mit diesem Header ablehnen soll.

### Beibehaltung von SIP-Parametern

Legt fest, ob der B2BUA der Expressway die über diese Zone gerouteten Parameter in SIP-Anfragen erhält oder umschreibt.

**On behält die SIP Request URI- und Contact-Parameter für das Anforderungsrouting zwischen dieser Zone und dem B2BUA bei.**

**Bietet dem B2BUA die Möglichkeit, die SIP Request URI- und Contact-Parameter von Anfragen Routing zwischen dieser Zone und dem B2BUA umzuschreiben, falls erforderlich.**

Auf der Grundlage dieser Definitionen, der xConfiguration, und da der **call-type=squared**-Wert im "Contact"-Header der SIP-INVITE-Nachricht platziert wird, können Sie daraus schließen, dass der SIP-Parametererhaltungswert in der Hybrid Call Service Traversal-Zone deaktiviert ist, weil das Tag entfernt wird und die Cisco WebEx App doppelte Ringbenachrichtigungen erhält.

### Lösung

Um den Anruftyp=squared-Wert im Contact-Header der SIP INVITE-Nachricht zu erhalten, müssen Sie sicherstellen, dass die Expressways die Beibehaltung der SIP-Parameter für alle an der Anrufverarbeitung beteiligten Zonen unterstützen:

1. Melden Sie sich bei Expressway-E an.
2. Navigieren Sie zu **Konfiguration > Zonen > Zonen**
3. Wählen Sie die Zone aus, die für den Hybrid Traversal Server verwendet wird.
4. Legen Sie den Wert für die Beibehaltung der SIP-Parameter auf **Ein fest**.
5. Speichern Sie die Einstellungen.

#####  
#####

Hinweis: In diesem Beispielszenario war es die WebEx Hybrid Traversal Server-Zone auf dem Expressway-E, die falsch konfiguriert wurde. Beachten Sie, dass der Wert für die Konservierung der SIP-Parameter auf Off (Aus) für den WebEx Hybrid Traversal-Client oder die Nachbarzonen des CUCM eingestellt werden kann. Diese beiden Konfigurationen würden auf dem Expressway-C vorgenommen. Wenn das der Fall wäre, könnten Sie erwarten, dass der Expressway-E den **call-type=squared** Wert an den Expressway-C gesendet hätte und es wäre der Expressway-C-Abbruch gewesen.

### Ausgehend: Am Standort zu Cisco WebEx

Fast jeder Anruf, bei dem ein ausgehender Anruf vor Ort an Cisco WebEx gesendet wird, hat das

gleiche Symptom: "Wenn ich von meinem Unified CM-registrierten Telefon an einen anderen Benutzer anrufe, der für Call Service Connect aktiviert ist, klingelt sein Telefon vor Ort, die Cisco WebEx App hingegen nicht." Um dieses Szenario zu beheben, ist es wichtig, sowohl den Anruffluss als auch die Logik zu verstehen, die beim Tätigen dieses Anrufs auftreten.

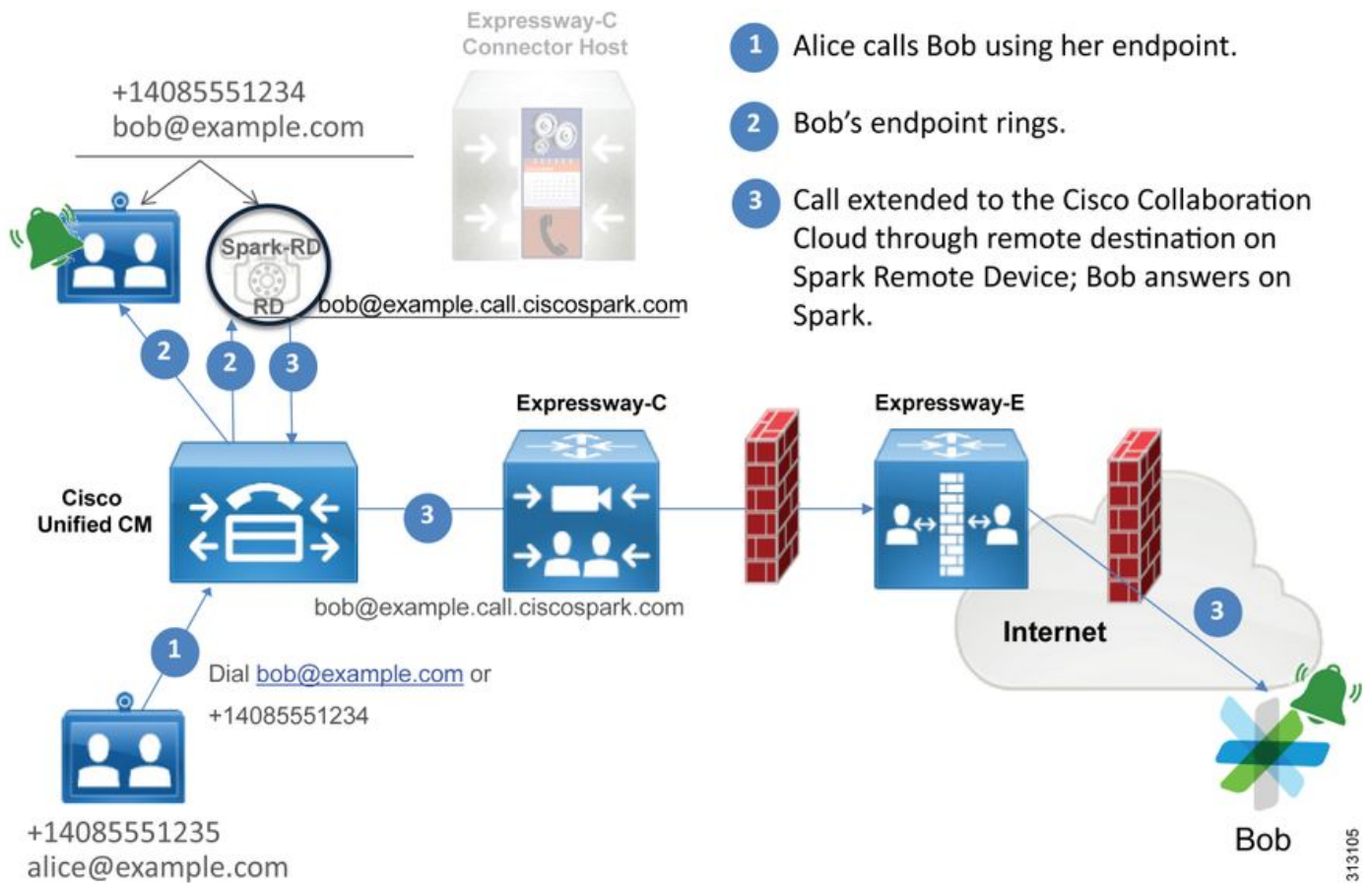
### High-Level-Logik-Fluss

1. Benutzer A führt einen Anruf vom Telefon am Standort zum Verzeichnis-URI von Benutzer B durch
2. Telefon von Benutzer B vor Ort und CTI-RD/Webex-RD akzeptieren den Anruf
3. Das standortbasierte Telefon von Benutzer B klingelt.
4. Der CTI-RD/Webex-RD von Benutzer B leitet diesen Anruf an das Ziel von UserB@example.call.ciscopark.com.
5. Unified CM leitet diesen Anruf an den Expressway-C weiter.
6. Expressway-C sendet den Anruf an die Expressway-E
7. Expressway-E führt eine DNS-Suche in der Domäne callservice.ciscopark.com durch
8. Expressway-E versucht, über Port 5062 eine Verbindung zur Cisco WebEx Umgebung herzustellen.
9. Expressway-E und die Cisco WebEx Umgebung beginnen einen gegenseitigen Handshake
10. Die Cisco WebEx Umgebung leitet den Anruf an die verfügbare Cisco WebEx App von Benutzer B weiter
11. Die verfügbare Cisco WebEx App von Benutzer B klingelt.

### Anruffluss

Navigieren Sie zu **Benutzer B am Standort-Telefon > Unified CM > CTI-RD/Webex-RD > Expressway-C > Expressway-E > Cisco WebEx-Umgebung > Cisco WebEx-App**, wie im Bild gezeigt.





Hinweis: Das Bild wurde aus dem [Cisco WebEx Hybrid Design Guide](#) entnommen.

## Tipps zur Protokollanalyse

Wenn Sie eine Fehlerbehebung für ausgehende gefälschte Anrufe bei Cisco WebEx durchgeführt haben, sollten Sie die Unified CM-, Expressway-C- und Expressway-E-Protokolle sammeln. Durch diese Protokollsätze können Sie sehen, wie der Anruf durch die Umgebung geleitet wird. Eine weitere Möglichkeit, um schnell zu verstehen, wie weit der Anruf in Ihrer Umgebung vor Ort geht, ist der Expressway "Suchverlauf". Über den Verlauf der Expressway-Suche können Sie schnell feststellen, ob der gefälschte Anruf bei Cisco WebEx zum Expressway-C oder E gelangt.

## So verwenden Sie den Suchverlauf:

1. Melden Sie sich bei Expressway-E an.

Testanruf tätigen

Navigieren Sie zu **Status > Suchverlauf**.

Überprüfen Sie, ob ein Anruf mit einer Zieladresse des Webex SIP URI angezeigt wird, die aufgerufen werden soll (user@example.call.ciscopark.com).

Wenn der Suchverlauf den Anruf, der auf den Expressway-E Suchverlauf trifft, nicht anzeigt, wiederholen Sie diesen Vorgang auf dem Expressway-C.

Bevor Sie die Diagnoseprotokolle auf dem Expressway analysieren, überlegen Sie, wie Sie diesen Anruf identifizieren können:

1. Der SIP Request URI ist die SIP-Adresse des Cisco WebEx Benutzers.
2. Das Feld SIP FROM wird so formatiert, dass der anrufende Teilnehmer als "Nachname des Vornamens" <sip:Alias@Domain> aufgeführt wird.

Mit diesen Informationen können Sie die Diagnoseprotokolle nach dem Verzeichnis-URI des

anrufenden Teilnehmers, dem Vor- und Nachnamen des anrufenden Teilnehmers oder der Cisco WebEx SIP-Adresse des angerufenen Teilnehmers durchsuchen. Wenn Sie über keine dieser Informationen verfügen, können Sie unter "INVITE SIP:" nach allen SIP-Anrufen suchen, die über die Expressway ausgeführt werden. Sobald Sie die SIP-EINLADUNG für den ausgehenden Anruf identifiziert haben, können Sie die SIP-Anruf-ID suchen und kopieren. Danach können Sie die Diagnoseprotokolle basierend auf der Anruf-ID durchsuchen, um alle Nachrichten anzuzeigen, die zu diesem Anrufabschnitt gehören.

Im Folgenden sind einige der häufigsten Probleme aufgeführt, die bei ausgehenden Anrufen vom bei Unified CM registrierten Telefon zur Cisco WebEx Umgebung beobachtet wurden, wenn der Anruf an einen Benutzer getätigt wird, der für Call Service Connect aktiviert ist.

### **Ausgabe 1 Expressway kann die Adresse `callservice.ciscospark.com` nicht auflösen.**

Das Standardverfahren für eine Expressway DNS-Zone besteht darin, eine DNS-Suche durchzuführen, die auf der Domäne basiert, die rechts neben einem Request URI angezeigt wird. Um dies zu erklären, betrachten Sie ein Beispiel. Wenn die DNS-Zone einen Aufruf mit dem Request URI `pstojano-test@dmzlab.call.ciscospark.com` empfangen sollte, führt eine typische Expressway DNS Zone die DNS SRV-Suchlogik auf `dmzlab.call.ciscospark.com` aus, die rechts im Request URI steht. Wenn der Expressway dies tun würde, könnten Sie erwarten, dass die folgende Suche und Reaktion auftreten würde.

```
_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
```

Wenn Sie genau hinschauen, sehen Sie, dass die SRV-Datensatzantwort eine Serveradresse und einen Port 5061 und nicht 5062 bereitstellt.

Das bedeutet, dass der gegenseitige TLS-Handshake, der über Port 5062 erfolgt, nicht erfolgt und ein separater Port für die Signalisierung zwischen dem Expressway und Cisco WebEx verwendet wird. Die Herausforderung besteht darin, dass im *Bereitstellungsleitfaden für Cisco WebEx Hybrid Call Services* nicht explizit die Verwendung von Port 5061 erwähnt wird, da in einigen Umgebungen geschäftliche Anrufe nicht möglich sind.

Die Möglichkeit, diese standardmäßige DNS Zone SRV-Suchlogik auf dem Expressway zu überwinden, besteht darin, den Expressway so zu konfigurieren, dass er explizite Suchen durchführt, die auf einem von Ihnen angegebenen Wert basieren.

Wenn Sie diesen Anruf jetzt analysieren, können Sie sich auf den Expressway-E konzentrieren, da Sie (mithilfe des Suchverlaufs) festgestellt haben, dass der Anruf diesen bisher erreicht hat. Beginnen Sie mit der ersten SIP-INVITE, die in den Expressway-E eintrifft, um zu sehen, welche Zone sie übernahm, welche Suchregeln verwendet werden, welche Zone der Anruf ausgeht und welche DNS-Suchlogik auftritt, wenn er korrekt an die DNS-Zone gesendet wird.

```
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-remotecallinfo>;x-cisco-video-traffic-class=DESKTOP  
Remote-Party-ID: "Jonathan Robb"  
<sip:5010@rtp.ciscotac.net>;party=calling;screen=yes;privacy=off  
Contact: <sip:5010@192.168.1.21:5065;transport=tcp>;video;audio  
**From: "Jonathan Robb"**

;tag=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>

In dieser SIP-EINLADUNG können Sie den **Request URI** (pstojo-  
test@dmzlab.call.ciscopark.com), die **Call-ID** (991f7e80-9c11517a-130ac-1501a8c0), **From**  
("Jonathan Robb" <sip:5010@rtp.ciscotac.net) erfassen>), **To** (SIP:pstojo-  
test@dmzlab.call.ciscopark.com) und **User-Agent (Cisco-CUCM11.5)**. Nachdem diese INVITE-  
Nachricht empfangen wurde, muss der Expressway jetzt logische Entscheidungen treffen, um zu  
bestimmen, ob der Anruf an eine andere Zone weitergeleitet werden kann. Der Expressway macht  
dies basierend auf den Suchregeln.

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 'pstojo-test@dmzlab.call.ciscopark.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'"

Auf Basis des obigen Protokollausschnitts können Sie sehen, dass Expressway-E vier Suchregeln analysiert hat, jedoch nur eine (Webex Hybrid - to Webex Cloud) berücksichtigt wurde. Die Suchregel hatte eine Priorität von 90 und wurde für die Hybrid Call Services DNS Zone konzipiert. Nachdem der Anruf an eine DNS-Zone gesendet wurde, können Sie die DNS SRV-Suchvorgänge auf dem Expressway-E überprüfen.

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"

Im obigen Ausschnitt können Sie sehen, dass Expressway-E die SRV-Suche auf der rechten Seite des Request URI (\_sips.\_tcp.dmzlab.call.ciscospark.com) durchgeführt hat und auf den Hostnamen l2sip-cfa-01.wbx2.com und Port 5061 aufgelöst wurde. Der Hostname l2sip-cfa-01.wbx2.com wird auf 146.20.193.64 aufgelöst. Mit diesen Informationen sendet der Expressway als nächsten logischen Schritt ein TCP-SYN-Paket an 146.20.193.64, damit er versuchen kann, den Anruf zu starten. Mithilfe der Expressway-E-Protokollierung können Sie überprüfen, ob dies geschieht.

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"

Im obigen Expressway-E-Diagnoseprotokollierungsausschnitt sehen Sie, dass das Expressway-E versucht, eine Verbindung zum IP 146.20.193.64 herzustellen, der zuvor über den TCP-Port 5061 aufgelöst wurde, aber diese Verbindung ist völlig fehlerhaft. Das Gleiche gilt für die erfasste Paketerfassung.

Expressway-E attempts TCP Connection

| No.   | Time                       | Source      | Destination   | Protocol | S Port | D Port | Length | Info  |
|-------|----------------------------|-------------|---------------|----------|--------|--------|--------|---|
| 3878  | 2017-09-19 17:18:08.801765 | 68.67.59.22 | 172.16.2.2    | TCP      | 25876  | 5061   | 66     | 25876->5061 [FIN, ACK] Seq=1 Ack=1 Win=0 Len=0 Tsva=231154828 TSecr=4109470239                                  |
| 3879  | 2017-09-19 17:18:08.801923 | 172.16.2.2  | 68.67.59.22   | TCP      | 5061   | 25876  | 66     | 5061->25876 [FIN, ACK] Seq=1 Ack=2 Win=0 Len=0 Tsva=4111465862 TSecr=231154828                                  |
| 3882  | 2017-09-19 17:18:08.821153 | 68.67.59.22 | 172.16.2.2    | TCP      | 25876  | 5061   | 66     | 25876->5061 [ACK] Seq=2 Ack=2 Win=362 Len=0 Tsva=231154849 TSecr=4111465862                                     |
| 3109  | 2017-09-19 17:18:51.145130 | 172.16.2.2  | 146.20.193.64 | TCP      | 25010  | 5061   | 66     | 25010->5061 [SYN] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 Tsva=314491012 TSecr=0 WS=128                          |
| 14878 | 2017-09-19 17:18:51.145472 | 172.16.2.2  | 146.20.193.64 | TCP      | 25010  | 5061   | 74     | 25010->5061 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 Tsva=314491012 TSecr=0 WS=128                      |
| 35158 | 2017-09-19 17:18:52.203326 | 172.16.2.2  | 146.20.193.64 | TCP      | 25010  | 5061   | 74     | [TCP Retransmission] 25010->5061 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 Tsva=314491012 TSecr=0 WS=128 |
| 15702 | 2017-09-19 17:18:54.251324 | 172.16.2.2  | 146.20.193.64 | TCP      | 25010  | 5061   | 74     | [TCP Retransmission] 25010->5061 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 Tsva=314491012 TSecr=0 WS=128 |
| 16770 | 2017-09-19 17:18:58.283326 | 172.16.2.2  | 146.20.193.64 | TCP      | 25010  | 5061   | 74     | [TCP Retransmission] 25010->5061 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 Tsva=314491012 TSecr=0 WS=128 |
| 17327 | 2017-09-19 17:19:01.328661 | 172.16.2.2  | 146.20.193.64 | TCP      | 25011  | 5061   | 74     | 25011->5061 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 Tsva=314501193 TSecr=0 WS=128                      |
| 17346 | 2017-09-19 17:19:02.349322 | 172.16.2.2  | 146.20.193.64 | TCP      | 25011  | 5061   | 74     | [TCP Retransmission] 25011->5061 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 Tsva=314501193 TSecr=0 WS=128 |
| 18425 | 2017-09-19 17:19:04.427323 | 172.16.2.2  | 146.20.193.64 | TCP      | 25011  | 5061   | 74     | [TCP Retransmission] 25011->5061 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 Tsva=314501193 TSecr=0 WS=128 |
| 19459 | 2017-09-19 17:19:08.459332 | 172.16.2.2  | 146.20.193.64 | TCP      | 25011  | 5061   | 74     | [TCP Retransmission] 25011->5061 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 Tsva=314501193 TSecr=0 WS=128 |

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

Auf der Grundlage dieser Ergebnisse ist klar, dass der Datenverkehr über Port 5061 nicht erfolgreich ist. Hybrid Call Service Connect ist jedoch für den TCP-Port 5062 und nicht 5061

vorgesehen. Daher müssen Sie sich überlegen, warum Expressway-E keinen SRV-Datensatz löst, der Port 5062 zurückgibt. Um diese Frage zu beantworten, können Sie in der Expressway-E WebEx Hybrid DNS Zone nach möglichen Konfigurationsproblemen suchen.

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

In der xConfiguration des Expressway-E sehen Sie zwei spezielle Werte, die sich auf DNS-Lookups beziehen: **DNSOverride Name** und **DNSOverride Override**. Aufgrund dieser xConfiguration ist DNSOverride Override auf Off (Aus) gesetzt, daher wird der DNSOverride-Name nicht übernommen. Um besser zu verstehen, was diese Werte tun, können Sie die Webbenutzeroberfläche von Expressway verwenden, um die Definition der Werte nachzuschlagen.

### Ändern der DNS-Anforderung (in DNSOverride Override in xConfig)

Leitet ausgehende SIP-Anrufe von dieser Zone an eine manuell angegebene SIP-Domäne statt an die Domäne im gewählten Ziel weiter. Diese Option ist hauptsächlich für die Verwendung mit dem Cisco WebEx Call Service vorgesehen. Siehe [www.cisco.com/go/hybrid-services](http://www.cisco.com/go/hybrid-services).

### Domäne, nach der gesucht werden soll (wird in DNSOverride Name in xConfig übersetzt)

Geben Sie einen FQDN ein, der in DNS gefunden werden soll, anstatt nach der Domäne im ausgehenden SIP-URI zu suchen. Der ursprüngliche SIP URI ist nicht betroffen.

Da Sie jetzt über diese Definitionen verfügen, ist klar, dass diese Werte, wenn sie korrekt festgelegt werden, für unsere DNS-Suchlogik vollkommen relevant sind. Wenn Sie dies mit den Anweisungen aus dem Bereitstellungsleitfaden für Cisco WebEx Hybrid Call Services kombinieren, müssen Sie die DNS-Anforderung ändern auf **On** (Ein) einstellen, und die zu suchende Domäne muss auf **callservice.ciscopark.com** festgelegt werden. Wenn Sie diese Werte ändern, um die richtigen Informationen anzugeben, ist die DNS SRV-Suchlogik völlig anders. Im Folgenden finden Sie einen Auszug von den Vorteilen der Expressway-E-Diagnoseprotokollierung.

```
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.ciscopark.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"
```

## Lösung

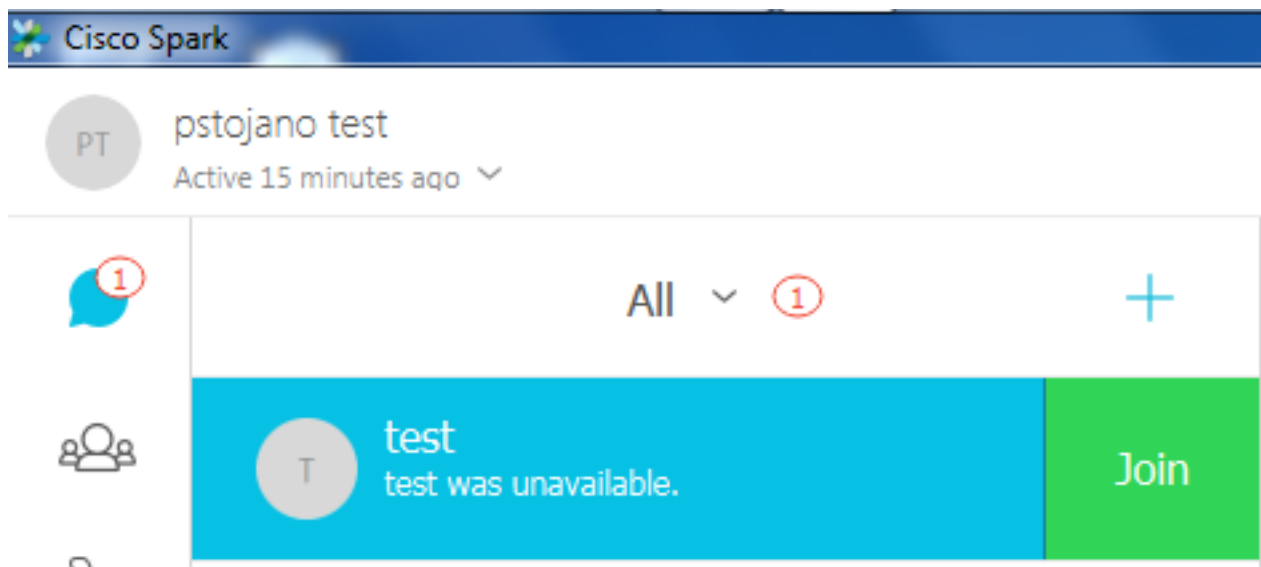
1. Melden Sie sich bei Expressway-E an.
2. Navigieren Sie zu **Konfigurationszonen > Zonen**.
3. Wählen Sie die konfigurierte WebEx Hybrid DNS Zone aus.
4. Stellen Sie die Anforderung DNS ändern auf **Ein ein**.
5. Legen Sie die Domäne für die Suche nach Wert auf **callservice.ciscopark.com fest**.
6. Speichern der Änderungen

**Hinweis:** Wenn auf dem Expressway nur eine DNS-Zone verwendet wird, sollte eine separate DNS-Zone für die Verwendung mit dem Hybrid Call Service konfiguriert werden, der diese Werte nutzen kann.

## Ausgabe 2: Port 5062 wird ausgehenden Datenverkehr zu Cisco WebEx blockiert

Einzigartig an den gefälschten Fehlern ausgehender Anrufe bei Cisco WebEx ist, dass die Cisco WebEx App des angerufenen Teilnehmers eine Schaltfläche "Join" (Verbinden) auf der App anzeigt, obwohl der Client nie klingelt. Wie im obigen Szenario müssen Sie für dieses Problem erneut dieselben Tools und Protokollierungen verwenden, um am besten zu verstehen, wo der Fehler auftritt. Tipps zur Isolierung von Anrufproblemen und zum Analysieren von Protokollen finden Sie im Abschnitt dieses Artikels, wie im Bild gezeigt.

Darstellung der angezeigten Schaltfläche Beitreten



Wie bei Ausgehendem Anruf Ausgabe 1 können Sie die Analyse bei der Expressway-E-Diagnoseprotokollierung starten, da Sie mithilfe des Suchverlaufs auf dem Expressway festgestellt haben, dass der Anruf so weit geht. Beginnen Sie wie bisher mit der ersten INVITE-Nachricht, die vom Expressway-C in das Expressway-E eingeht. Denken Sie daran, dass Sie folgende Dinge suchen möchten:

1. Legt fest, ob der Expressway-E die INVITE-Nachricht empfängt.
2. Legt fest, ob die Suchregellogik den Anruf an die Hybrid-DNS-Zone weiterleitet.
3. Legt fest, ob die DNS-Zone die DNS-Suche und die korrekte Domäne durchführt.

4. Legt fest, ob das System einen TCP-Handshake für Port 5062 versucht und korrekt eingerichtet hat.

5. Ob der gegenseitige TLS-Handshake erfolgreich war

```
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-remotecall:callinfo>;x-cisco-video-traffic-class=DESKTOP
Remote-Party-ID: "Jonathan Robb"
<sip:5010@rtp.ciscotac.net>;party=calling;screen=yes;privacy=off
Contact: <sip:5010@192.168.1.21:5065;transport=tcp>;video;audio
From: "Jonathan Robb"
```

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

To:

```
Max-Forwards: 15
Record-Route: <sip:proxy-call-id=696f6f1c-9abe-47f3-96a4-
e26f649fb76f@192.168.1.5:5061;transport=tls;lr>
Record-Route: <sip:proxy-call-id=696f6f1c-9abe-47f3-96a4-
e26f649fb76f@192.168.1.5:5060;transport=tcp;lr>
Allow: INVITE, OPTIONS, INFO, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY
User-Agent: Cisco-CUCM11.5
Expires: 180
Date: Tue, 19 Sep 2017 14:18:34 GMT
Supported: timer, resource-priority, replaces, X-cisco-srtp-fallback, X-cisco-original-called
Session-Expires: 1800
Min-SE: 1800
Allow-Events: presence
X-TAATag: b2967a3b-93fb-4ca4-b0d7-131f75335684
Session-ID: 75957d4fb66a13e835c10737aa328865;remote=00000000000000000000000000000000
Cisco-Guid: 1783160448-0000065536-000000126-0352430272
Content-Type: application/sdp
Content-Length: 714
<SDP Omitted>
```

Wie Sie oben in der INVITE-Nachricht sehen können, wird die INVITE-Nachricht wie gewohnt empfangen. Dies ist eine "empfangene" Aktion, die von der Expressway-C IP-Adresse ausgeht. Sie können jetzt zur Suchregellogik wechseln.

```

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'"

```

Auf Basis des obigen Protokollausschnitts können Sie sehen, dass das Expressway-E durch vier Suchregeln geparkt wird, jedoch nur eine. (*Webex Hybrid - zur WebEx Cloud*) wurde berücksichtigt. Die Suchregel hatte eine Priorität von 90 und wurde für die Suche nach *DNS-Zone für Hybrid Call Services*. Nachdem der Anruf an eine DNS-Zone gesendet wurde, können Sie die DNS SRV-Suchvorgänge auf dem Expressway-E überprüfen. All das ist völlig normal. Jetzt können Sie sich auf die DNS-Suchlogik konzentrieren.

```

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"

```

Sie können sehen, dass in dieser Instanz der SRV-Datensatz *callservice.ciscospark.com* aufgelöst wurde. Die Antwort sind vier verschiedene gültige Datensätze, die alle Port 5062 verwenden. Dies ist ein normales Verhalten. Jetzt können Sie den TCP-Handshake analysieren, der als Nächstes kommen sollte. Wie bereits zuvor in diesem Dokument erwähnt, können Sie die Diagnoseprotokolle nach "TCP-Verbindung" durchsuchen und nach dem Posten suchen, in dem der *Dst-Port="5062"* aufgeführt ist. Im Folgenden finden Sie ein Beispiel für dieses Szenario:

```

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"

```

Sie können auch die *tcpdump*-Datei verwenden, die im Diagnoseprotokollierungspaket enthalten war, um weitere Informationen über den TCP-Handshake zu erhalten, wie im Bild gezeigt.

Expressway-E attempts TCP Connection twice

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

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

An dieser Stelle können Sie feststellen, dass der Expressway-E den Anruf korrekt weiterleitet. Die

Herausforderung in diesem Szenario besteht darin, dass mit der WebEx Umgebung keine TCP-Verbindung hergestellt werden kann. Dies könnte der Fall sein, weil die WebEx Umgebung nicht auf das TCP-SYN-Paket reagiert. Dies ist jedoch unwahrscheinlich, da der Server, der die Verbindung verarbeitet, von vielen Kunden gemeinsam genutzt wird. Die wahrscheinlichere Ursache in diesem Szenario ist, dass eine Art zwischengeschaltetes Gerät (Firewall, IPS usw.) den Datenverkehr nicht zulässt.

## Lösung

Da das Problem isoliert war, sollten diese Daten dem Netzwerkadministrator des Kunden zur Verfügung gestellt werden. Wenn sie weitere Informationen benötigen, können Sie außerdem eine Erfassung der externen Schnittstelle des Edge-Geräts und/oder der Firewall durchführen, um weitere Nachweise zu erhalten. Aus der Perspektive von Expressway gibt es keine weiteren Aktionen, da sich das Problem nicht auf diesem Gerät befindet.

## Ausgabe 3 Fehlkonfiguration der Expressway Search-Regel

Die Fehlkonfiguration von Suchregeln ist eines der größten Konfigurationsprobleme auf den Expressways. Konfigurationsprobleme bei Suchregeln können bidirektional sein, da Sie Suchregeln für eingehende Anrufe benötigen und Suchregeln für ausgehende Anrufe benötigen. Während Sie dieses Problem durchgehen, werden Sie feststellen, dass Regex-Probleme auf dem Expressway sehr häufig auftreten, aber nicht immer die Ursache für ein Problem mit den Suchregeln sind. In diesem Segment führen Sie einen ausgehenden Anruf durch, der fehlschlägt. Wie alle anderen Szenarien mit gefälschten Anrufen für ausgehende Anrufe sind die Symptome unverändert:

- Die Cisco WebEx App des angerufenen Benutzers zeigt die Schaltfläche "Join" (Verbinden) an.
- Das anrufende Telefon spielte einen Klingelton zurück.
- Das Telefon des angerufenen Benutzers klingelte am Standort.
- Die Cisco WebEx App des angerufenen Benutzers klingelt nie.

Wie alle anderen Szenarien sollten Sie auch CUCM SDL Traces zusammen mit Expressway-C- und E-Diagnoseprotokollen verwenden. Wie zuvor sollten Sie auf das verweisen, um den Suchverlauf zu nutzen, und auf Tipps zum Identifizieren eines Anrufs in den Diagnoseprotokollen. Wie zuvor wurde anhand des Expressway-E Suchverlaufs festgestellt, dass dieser Anruf dort stattfand und fehlschlug. Unten sehen Sie den Beginn der Analyse, für die wir uns die erste SIP-INVITE ansehen, die vom Expressway-C in das Expressway-E geht.

```
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-remotec: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>

Mithilfe der Anruf-ID (**d58f2680-9c91200a-1c7ba-1501a8c0**) aus dem SIP-Header können Sie schnell alle Nachrichten durchsuchen, die diesem Dialog zugeordnet sind. Wenn Sie den dritten Treffer in den Protokollen für die Anruf-ID betrachten, sehen Sie, dass das Expressway-E sofort einen **404 Not Found** an Expressway-C sendet.

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.a81f2992e3863ac202a000a3dd599763;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

Diese Daten zeigen Ihnen zwei Dinge:

1. Expressway-E hat nie versucht, die INVITE an Cisco WebEx zu senden.
2. Der Expressway-E war für die logische Entscheidung verantwortlich, den Anruf mit dem Fehler 404 Not Found (Nicht gefunden) abzulehnen.

Der Fehler 404 Not Found (Nicht gefunden) bedeutet im Allgemeinen, dass die Expressway die Zieladresse nicht finden kann. Da die Expressways mithilfe von Suchregeln Anrufe zwischen sich und in verschiedene Umgebungen weiterleiten, konzentrieren Sie sich zunächst auf die xConfiguration des Expressway-E. In dieser xConfiguration können Sie nach der Suchregel suchen, die den Anruf an die WebEx Hybrid DNS Zone weiterleitet. Um die auf dem Expressway konfigurierten Suchregeln aus Sicht von xConfiguration zu finden, können Sie nach "xConfiguration Zones Policy Search RulesRules" suchen. Dadurch wird eine Liste der Konfiguration von Suchregeln für jede auf dem Expressway erstellte Suchregel angezeigt. Die Anzahl, die nach der "Regel" kommt, erhöht sich basierend auf der zuerst erstellten Suchregel, die als 1 gekennzeichnet wurde. Wenn Sie Schwierigkeiten haben, die Suchregel zu finden. Sie können häufig verwendete Benennungswerte wie "Webex" verwenden, um die Suchregel besser zu finden. Eine weitere Möglichkeit zum Identifizieren der Regel besteht darin, den Wert für Musterzeichenfolge zu ermitteln, der auf ".\*@.\*\.ciscopark\.com" festgelegt ist. Dies ist der Musterstring, der konfiguriert werden soll. (*Annahme, dass die Musterzeichenfolge korrekt konfiguriert ist*)Nachdem Sie die xConfiguration aus diesem Szenario überprüft haben, sehen Sie, dass Suchregel 6 die richtige Regel ist, um den Anruf an Cisco WebEx weiterzuleiten.

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

Um dieses Muster zu testen, können Sie die im Abschnitt beschriebene Funktion Prüfmuster verwenden. Der wichtige Hinweis hierbei ist, dass die folgenden Werte konfiguriert werden sollen:Wartung > Extras > Muster überprüfen

- Alias: %Request URI im ursprünglichen INVITE% (Bsp.: pstojano-



test@dmzlab.call.ciscospark.com)

- Mustertyp: regulär
- Musterzeichenfolge .\*@.\*\ciscospark\com
- Musterverhalten: Urlaub

Wenn der Regex für die Regel richtig eingerichtet ist, sollten Sie das Ergebnis dieses Prüfmusters erfolgreich sehen. Im Folgenden sehen Sie eine Abbildung, die dies zeigt, wie im Bild gezeigt:

The screenshot shows a configuration interface for a search rule. The 'Alias' field contains 'pstoiano-test@dmzlab.call.ciscospark.com'. The 'Pattern' field contains the regex '.\*@.\*\ciscospark\com'. The 'Pattern type' is set to 'Regex' and the 'Pattern behavior' is set to 'Leave'. A 'Check pattern' button is visible. Below the configuration, a 'Result' section shows a green 'Succeeded' status with the message 'Alias matched pattern' and the matched alias 'pstoiano-test@dmzlab.call.ciscospark.com'.

Nachdem Sie nun bestätigen können, dass die Suchregel korrekt vorhanden und konfiguriert ist, können Sie sich die Suchlogik näher ansehen, die der Expressway durchführt, um festzustellen, ob sie das Expressway-E beeinflusst, das den 404 Not Found sendet. Unten sehen Sie ein Beispiel für die Suchregellogik, die der Expressway ausgeführt hat.

```
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 'pstoiano-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 'pstoiano-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 'pstoiano-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)"
```

In diesem Beispiel sehen Sie, dass der Expressway vier Suchregeln verarbeitet hat. Die ersten 3 wurden aus verschiedenen Gründen nicht berücksichtigt, jedoch wurde die vierte berücksichtigt. Interessant ist, dass der Expressway unmittelbar nach der Betrachtung direkt zur DNS-Suchlogik springt. Wenn Sie sich daran erinnern, was wir in der xConfiguration gesehen hatten, wurde die für WebEx Hybrid konfigurierte Suchregel Webex Hybrid genannt - in WebEx Cloud, und sie wurde in dieser Suchregellogik oben nicht einmal berücksichtigt. An dieser Stelle lohnt es sich zu prüfen, wie die durchdachte Suchregel (in DNS) implementiert wurde, damit Sie besser verstehen können, ob sie sich auf die Verwendung der WebEx Hybrid Search-Regel auswirkt. Dazu können

Sie die xConfig-Methode erneut aufrufen und nach der Suchregel mit dem Namen "to DNS" suchen.

```
*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"
```

Nach Überprüfung dieser Suchregel können Sie Folgendes schließen:

- Die Musterzeichenfolge entspricht dem Cisco WebEx Request URI.
- Die Priorität ist auf 100 festgelegt.
- Der Fortschritt (Musterverhalten) ist auf Stopp eingestellt.

Diese Informationen zeigen uns, dass der aufgerufene Cisco WebEx Request URI dieser Regel entspricht und wenn die Regel zugeordnet wurde, würde der Expressway die Suche nach anderen Suchregeln beenden (Berücksichtigen). Mit diesem Verständnis wird die Regelpriorität zu einem Schlüsselfaktor. Die Funktionsweise der Expressway Search-Regel ist die Regel mit der niedrigsten Priorität, die zuerst versucht wird. Im Folgenden sehen Sie ein Beispiel. Suchregel: LokalMusterverhalten: WeiterPriorität 1 Suchregel: NachbarinMusterverhalten: WeiterPriorität 10 Suchregel: DNSMusterverhalten: StoppPriorität 50 In diesem Beispiel wird zuerst die Suchregel mit dem Namen Lokal (1) versucht, und wenn eine Übereinstimmung gefunden wurde, wird sie in Regelnachbarn suchen (10) verschoben, da das Musterverhalten auf Weiter festgelegt ist. Wenn die Suchregel Nachbarn nicht zugeordnet wurde, wird sie weiterhin Regel DNS (50) durchsuchen und als letztes betrachten. Wenn der DNS-Suchregel zugeordnet wurde, wird die Suche beendet, unabhängig davon, ob eine andere Suchregel mit einer Priorität über 50 vorhanden ist, da das Musterverhalten auf Stopp festgelegt wurde. Mit diesem Verständnis können Sie sich die Suchregelprioritäten zwischen den Regeln "zu DNS" und "Webex Hybrid - zu WebEx Cloud" ansehen.

```
*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"
```

Hier sehen Sie, dass die "to DNS"-Regel eine niedrigere Priorität hat als die "Webex Hybrid - to WebEx Cloud"-Regel. Daher wird zuerst die "to DNS"-Regel versucht. Da das Musterverhalten (Progress) auf Stopp eingestellt ist, berücksichtigt Expressway-E niemals die WebEx Hybrid-Regel - die WebEx Cloud-Regel - und der Anruf schlägt letztendlich fehl. Lösung Diese Art von Problem tritt bei Hybrid Call Service Connect immer häufiger auf. Bei der Bereitstellung der Lösung wird häufig eine Regel mit hoher Priorität für die Cisco WebEx-Suche erstellt. Häufig wird diese erstellte Regel nicht aufgerufen, da die vorhandenen Regeln mit niedrigerer Priorität zugeordnet werden. Dies führt zu einem Ausfall. Dieses Problem tritt sowohl bei ein- als auch bei ausgehenden Anrufen von Cisco WebEx auf. Um dieses Problem zu beheben, müssen Sie die

folgenden Schritte ausführen:

1. Melden Sie sich bei Expressway-E an.
2. Navigieren Sie zu Konfiguration > Wählplan > Suchregeln
3. Suchen Sie die WebEx Hybrid Search-Regel, und klicken Sie darauf (*Bsp.: Name: WebEx Hybrid - zu WebEx Cloud*)
4. Legen Sie den Wert für die Priorität auf etwas niedriger als andere Suchregeln fest, das jedoch hoch genug ist, damit sich dies nicht auf andere auswirkt. (*Bsp.: Priorität: 99*)

Die allgemeine Faustregel mit Suchregeln ist, je genauer die Musterzeichenfolge ist, desto niedriger kann sie in der Prioritätenliste der Suchregel platziert werden. Im Allgemeinen wird eine DNS-Zone mit einer Musterzeichenfolge konfiguriert, die alles abfängt, was keine lokale Domäne ist, und sie an das Internet sendet. Aus diesem Grund empfehlen wir, diesen Typ von Suchregel auf eine hohe Priorität festzulegen, damit er zuletzt aufgerufen wird. Ausgabe 4: Expressway CPL-Fehlkonfiguration Die Expressway-Lösung ermöglicht die Verhinderung von Gebührenbetrug, indem die auf dem Server verfügbare CPL-Logik (Call Processing Language) verwendet wird. Wenn die bereitgestellte Expressway-Lösung nur für den Cisco WebEx Hybrid Call Service sowie für den mobilen und Remote-Zugriff verwendet wird, empfehlen wir dringend, die CPL-Richtlinien und -Regeln zu aktivieren und zu implementieren. Während die CPL-Konfiguration auf dem Expressway für Cisco WebEx Hybrid recht einfach ist, kann sie bei falscher Konfiguration Anrufversuche leicht blockieren. In den folgenden Szenarien wird veranschaulicht, wie mithilfe der Diagnoseprotokollierung eine CPL-Fehlkonfiguration identifiziert wird. Wie alle anderen Szenarien mit gefälschten Anrufen nach außen blieben die Symptome unverändert:

- Die Cisco WebEx App des angerufenen Benutzers hat eine Schaltfläche "Join" (Verbinden) angezeigt.
- Das anrufende Telefon spielte einen Klingelton zurück.
- Das Telefon des angerufenen Benutzers klingelte am Standort.
- Die App des angerufenen Benutzers klingelte nie.

Wie alle anderen Szenarien können Sie die CUCM SDL Traces zusammen mit den Expressway-C- und E-Diagnoseprotokollen verwenden. Wie zuvor sollten Sie auf die zum Verwenden des Suchverlaufs und Tipps zum Identifizieren eines Anrufs in den Diagnoseprotokollen. Wie zuvor wurde anhand des Expressway-E Suchverlaufs festgestellt, dass dieser Anruf dort einging und fehlschlug. Unten sehen Sie den Beginn der Analyse, in der Sie sich die erste SIP-INVITE-Nachricht vom Expressway-C in das Expressway-E ansehen können.

```
2017-09-25T16:54:43.722-04:00 amer-expressway01 tvcs: UTCTime="2017-09-25 20:54:43,722"
Module="network.sip" Level="DEBUG": Action="Received" Local-ip="192.168.1.6" Local-port="7003"
Src-ip="192.168.1.5" Src-port="26404" Msg-Hash="17204952472509519266"
SIPMSG:
|INVITE sip:pstojano-test@dmzlab.call.ciscopark.com SIP/2.0
Via: SIP/2.0/TLS 192.168.1.5:5061;egress-
zone=HybridCallServiceTraversal;branch=z9hG4bK781a130d234ed9aaec86834368739430283256.34216c32a0d
e36e16590bae36df388b6;proxy-call-id=3bbb94a-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-remotec: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: 4ffffefed-0512-4067-ac8c-35828f0a1150

Session-ID: 75957d4fb66a13e835c10737aa512577;remote=00000000000000000000000000000000

Cisco-Guid: 3224432896-0000065536-0000000264-0352430272

Content-Type: application/sdp

Content-Length: 714

<SDP Omitted>

Mithilfe der Anruf-ID (c030f100-9c916d13-1cdcb-1501a8c0) aus dem SIP-Header können Sie schnell alle Nachrichten durchsuchen, die diesem Dialog zugeordnet sind. Wenn Sie den dritten Treffer in den Protokollen für die Anruf-ID betrachten, sehen Sie, dass der Expressway-E sofort einen 403 Forbidden an den Expressway-C sendet.

2017-09-25T16:54:43.727-04:00 amer-expressway01 tvcs: UTCTime="2017-09-25 20:54:43,727"

Module="network.sip" Level="DEBUG": Action="Sent" Local-ip="192.168.1.6" Local-port="7003" Dst-ip="192.168.1.5" Dst-port="26404" Msg-Hash="9195436101110134622"

SIPMSG:

|SIP/2.0 403 Forbidden

Via: SIP/2.0/TLS 192.168.1.5:5061;egress-

zone=HybridCallServiceTraversal;branch=z9hG4bK781a130d234ed9aaec86834368739430283256.34216c32a0de36e16590bae36df388b6;proxy-call-id=3bbbf94a-082e-4088-8f5a-

5ea7e82f8aac;received=192.168.1.5;rport=26404;ingress-zone=HybridCallServiceTraversal

Via: SIP/2.0/TCP 192.168.1.21:5065;branch=z9hG4bK1cf344a8b117e;received=192.168.1.21;ingress-zone=CUCM11

Call-ID: c030f100-9c916d13-1cdcb-1501a8c0@192.168.1.21

CSeq: 101 INVITE

From: "Jonathan Robb"

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

To:

;tag=64fe7f9eab37029d

Server: TANDBERG/4135 (X8.10.2)

Warning: 399 192.168.1.6:7003 "Policy Response"

Session-ID: 00000000000000000000000000000000;remote=75957d4fb66a13e835c10737aa512577

Content-Length: 0

Um zu verstehen, warum das Expressway-E diesen Anruf abgelehnt und einen 403 Forbidden-Fehler an den Expressway-C gesendet hat, möchten Sie die Protokolleinträge zwischen dem 403 Forbidden und der ursprünglichen SIP INVITE, die in den Expressway eingegeben wurden, analysieren. Durch Analysieren dieser Protokolleinträge können Sie in der Regel alle logischen Entscheidungen sehen, die getroffen werden. Beachten Sie, dass keine Suchregeln aufgerufen werden, jedoch wird die Call Process Language (CPL)-Logik aufgerufen. Unten sehen Sie einen Ausschnitt davon.

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:

■

Basierend auf der Protokollanalyse oben. Sie können feststellen, dass die CPL den Anruf ablehnt.

2017-09-25T16:54:43.725-04:00 amer-expressway01 tvcs: Event="Search Completed"

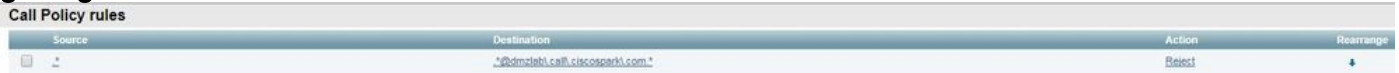
Reason="Forbidden" Service="SIP" Src-alias-type="SIP" Src-alias="5010@rtsp.ciscotac.net" Dst-alias-type="SIP" Dst-alias="sip:pstojano-test@dmzlab.call.ciscospark.com" Call-serial-number="48c80582-ec79-4d89-82e2-e5546f35703c" Tag="4fffefed-0512-4067-ac8c-35828f0a1150" Detail="found:false, searchtype:INVITE, 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"

*Hinweis: In dieser Situation werden Suchregeln nicht aufgerufen, da CPLs, FindMe und Transforms alle vor einer Suchregel verarbeitet werden* In den meisten Fällen können Sie die xConfig des Expressway nutzen, um die Umstände besser zu verstehen. Bei CPLs können die definierten Regeln jedoch nicht angezeigt werden, nur wenn die Richtlinie aktiviert ist. Unten sehen Sie den Teil der xConfig, der zeigt, dass dieses Expressway-E die lokale CPL-Logik verwendet.

\*c xConfiguration Policy AdministratorPolicy Mode: "LocalCPL"

Um die Regelkonfiguration besser zu verstehen, müssen Sie sich beim Expressway-E anmelden und zu Configuration > Call Policy > Rules (Konfiguration > Anrufrichtlinie > Regeln) navigieren, wie im Bild gezeigt.



Wenn Sie diese Konfiguration überprüfen, sehen Sie, dass Folgendes konfiguriert ist: Quelle: .\*Ziel: .\*@dmzlab.call.ciscospark.com.\*Aktion: AblehnenIm Vergleich zu den im [Cisco WebEx Hybrid Call Service Deployment Guide](#) dokumentierten Informationen sehen Sie, dass Quelle und Ziel rückwärts konfiguriert wurden.

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

LösungUm dieses Problem zu beheben, müssen Sie die Konfiguration der CPL-Regel so anpassen, dass die Quelle auf .\*@%Webex\_subdomain%.call.ciscospark.com.\* und das Zielmuster auf .\*

1. Melden Sie sich bei Expressway-E an.
2. Navigieren Sie zu Konfiguration > Anrufrichtlinie > Regeln.
3. Wählen Sie die Regel aus, die für den Cisco WebEx Hybrid Call-Service eingerichtet wurde.
4. Geben Sie das Quellmuster als .\*@%Webex\_subdomain%.call.ciscospark.com ein.\*(Beispiel: .\*@dmzlab.call.ciscospark.com.\*)
5. Geben Sie das Zielmuster als ein.\*
6. Wählen Sie Speichern

Weitere Informationen zur CPL-Implementierung für Webex Hybrid finden Sie im [Cisco WebEx Hybrid Design Guide](#). Bidirektional: Cisco WebEx zu standortbasiert oder am Standort zu Cisco WebEx Ausgabe 1 IP-Telefon/Collaboration-Endgerät bietet einen anderen Audio-Codec als G.711, G.722 oder AAC-LD.Hybrid Call Service Connect unterstützt drei verschiedene Audio-Codex: G.711, G.722 und AAC-LD. Um einen Anruf mit der Cisco WebEx Umgebung erfolgreich einrichten zu können, muss einer dieser Audio-Codex verwendet werden. Die Umgebung am Standort kann so eingerichtet werden, dass sie viele verschiedene Arten von Audio-Codex verwendet. Sie kann jedoch gleichzeitig eingerichtet werden, um sie einzuschränken. Dies kann absichtlich oder unabsichtlich durch die Verwendung von benutzerdefinierten und/oder standardmäßigen Regionseinstellungen auf dem Unified CM geschehen. Für dieses spezielle Verhalten können sich die Protokollierungsmuster je nach Anrufrichtung unterscheiden, und wenn der Unified CM für die Verwendung eines Early- oder Delayed Offer konfiguriert wurde. Im Folgenden finden Sie einige Beispiele für Situationen, in denen sich dieses Verhalten zeigen könnte:

1. Cisco Webex sendet eine eingehende INVITE mit SDP, die G.711, G.722 oder AAC-LD bietet. Der Expressway-C sendet diese Nachricht an Unified CM, aber Unified CM ist so konfiguriert, dass nur G.729 für diesen Anruf zugelassen wird. Daher lehnt Unified CM den Anruf ab, da kein Codec verfügbar ist.



2. Unified CM versucht den ausgehenden Anruf als *Early Offer* (*Early Offer* to Cisco WebEx), d. h. die erste an den Expressway-C gesendete INVITE enthält NUR SDP, das G.729-Audio unterstützt. Cisco WebEx sendet dann ein 200 OK mit SDP, das die Audioübertragung (*m=Audio 0 RTP/SAVP*) ohne Auflösung ausgibt, da G.729 nicht unterstützt wird. Sobald der Expressway-C diese INVITE-Nachricht an den Unified CM übergibt, beendet der Unified CM den Anruf, da kein Codec verfügbar ist.
3. Unified CM versucht den ausgehenden Anruf als *verzögertes Angebot* an Cisco WebEx, d. h. die erste an Expressway-C gesendete INVITE enthält kein SDP. Cisco Webex sendet dann ein 200 OK mit SDP, das alle von Cisco WebEx unterstützten Audio-Codecs enthält. Der Expressway-C sendet diesen 200 OK an Unified CM, aber Unified CM ist nur so konfiguriert, dass G.729 für diesen Anruf zugelassen wird. Daher lehnt Unified CM den Anruf ab, da kein Codec verfügbar ist.

Wenn Sie versuchen, einen Anrufausfall beim Hybrid Call Service Connect zu identifizieren, der zu diesem Problem passt, müssen Sie zusätzlich zu den Unified CM-SDL-Ablaufverfolgungen die Expressway-Protokolle abrufen. Die Protokollausschnitte unten entsprechen Situation 2, in der Unified CM den ausgehenden Anruf als *Early Offer* versucht. Da wir wissen, dass der Anruf an Cisco WebEx weitergeleitet wird, beginnt die Protokollanalyse auf dem Expressway-E. Im Folgenden finden Sie einen Ausschnitt der ersten INVITE-Anfrage für Cisco WebEx. Sie sehen, dass der bevorzugte Audio-Codec auf G.729 (Payload 18) eingestellt ist. Die 101 ist für DTMF und für dieses spezielle Szenario nicht relevant.

```
2017-09-19T10:46:10.488-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 14:46:10,488"
Module="network.sip" Level="DEBUG": Action="Sent" Local-ip="172.16.2.2" Local-port="25034" Dst-
ip="146.20.193.64" Dst-port="5062" Msg-Hash="4309505007645007056"
SIPMSG:
INVITE sip:pstojano-test@dmzlab.call.ciscospark.com SIP/2.0
Via: SIP/2.0/TLS 64.102.241.236:5062;egress-
zone=HybridCallServicesDNS;branch=z9hG4bK323e6b15ad0cbbf409751f67848136fa1115;proxy-call-
id=a3a78ee2-c01b-4741-b29b-55aede256d2;rport
Via: SIP/2.0/TLS 172.16.2.2:5073;branch=z9hG4bK350703fe46645f0acddef05b35adc5c157;x-cisco-local-
service=nettle;received=172.16.2.2;rport=41511;ingress-zone=DefaultZone
Via: SIP/2.0/TLS 192.168.1.6:5061;egress-
zone=DefaultZone;branch=z9hG4bKf71f2bf47233d6ca52b579364594ac6c1114.a402e3f25603f5a77b60b17ea47d
bf72;proxy-call-id=be17a470-0bca-4ad5-8a6c-14872e007efb;received=192.168.1.6;rport=25025
Via: SIP/2.0/TLS 192.168.1.5:5061;egress-
zone=HybridCallServiceTraversal;branch=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-55aede256d2@64.102.241.236:5062;transport=tls;lr>

Record-Route: <sip:proxy-call-id=a3a78ee2-c01b-4741-b29b-55aede256d2@172.16.2.2:5061;transport=tls;lr>

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

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

Supported: X-cisco-srtp-fallback,replaces,timer  
Session-Expires: 1800;refresher=uac  
Min-SE: 500  
X-TAATag: 14a0bd87-1825-4ecf-9f3d-4a23cfa69725  
Session-ID: 75957d4fb66a13e835c10737aa329445;remote=00000000000000000000000000000000  
Content-Type: application/sdp  
Content-Length: 1407

```
v=0
o=tandberg 0 1 IN IP4 64.102.241.236
s=-
c=IN IP4 64.102.241.236
b=AS:384
t=0 0
m=audio 52668 RTP/SAVP 18 101 <-- CUCM is only supporting G.729 for this call
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:.....
a=crypto:2 AES_CM_128_HMAC_SHA1_80 inline:.....
UNENCRYPTED_SRTCP
a=crypto:3 AES_CM_128_HMAC_SHA1_32 inline:.....
a=crypto:4 AES_CM_128_HMAC_SHA1_32 inline:.....
UNENCRYPTED_SRTCP
a=sendrecv
a=rtcp:52669 IN IP4 64.102.241.236
m=video 52670 RTP/SAVP 126 97
b=TIAS:384000
a=rtpmap:126 H264/90000
a=fmtp:126 profile-level-id=42801e;packetization-mode=1;level-asymmetry-allowed=1
a=rtpmap:97 H264/90000
a=fmtp:97 profile-level-id=42801e;packetization-mode=0;level-asymmetry-allowed=1
a=rtcp-fb:* nack pli
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:.....
a=crypto:2 AES_CM_128_HMAC_SHA1_80 inline:.....
UNENCRYPTED_SRTCP
a=crypto:3 AES_CM_128_HMAC_SHA1_32 inline:.....
a=crypto:4 AES_CM_128_HMAC_SHA1_32 inline:.....
UNENCRYPTED_SRTCP
a=sendrecv
a=content:main
a=label:11
a=rtcp:52671 IN IP4 64.102.241.236
```

Als Antwort auf diese erste INVITE-Anfrage antwortet Cisco WebEx mit einer 200 OK-Nachricht. Wenn Sie sich diese Nachricht genauer ansehen, sehen Sie, dass der Audio-Codec auf Null gesetzt wurde. Dies ist problematisch, da der Anruf ohne einen zugewiesenen Audio-Port nicht in der Lage ist, den Stream zu verhandeln.

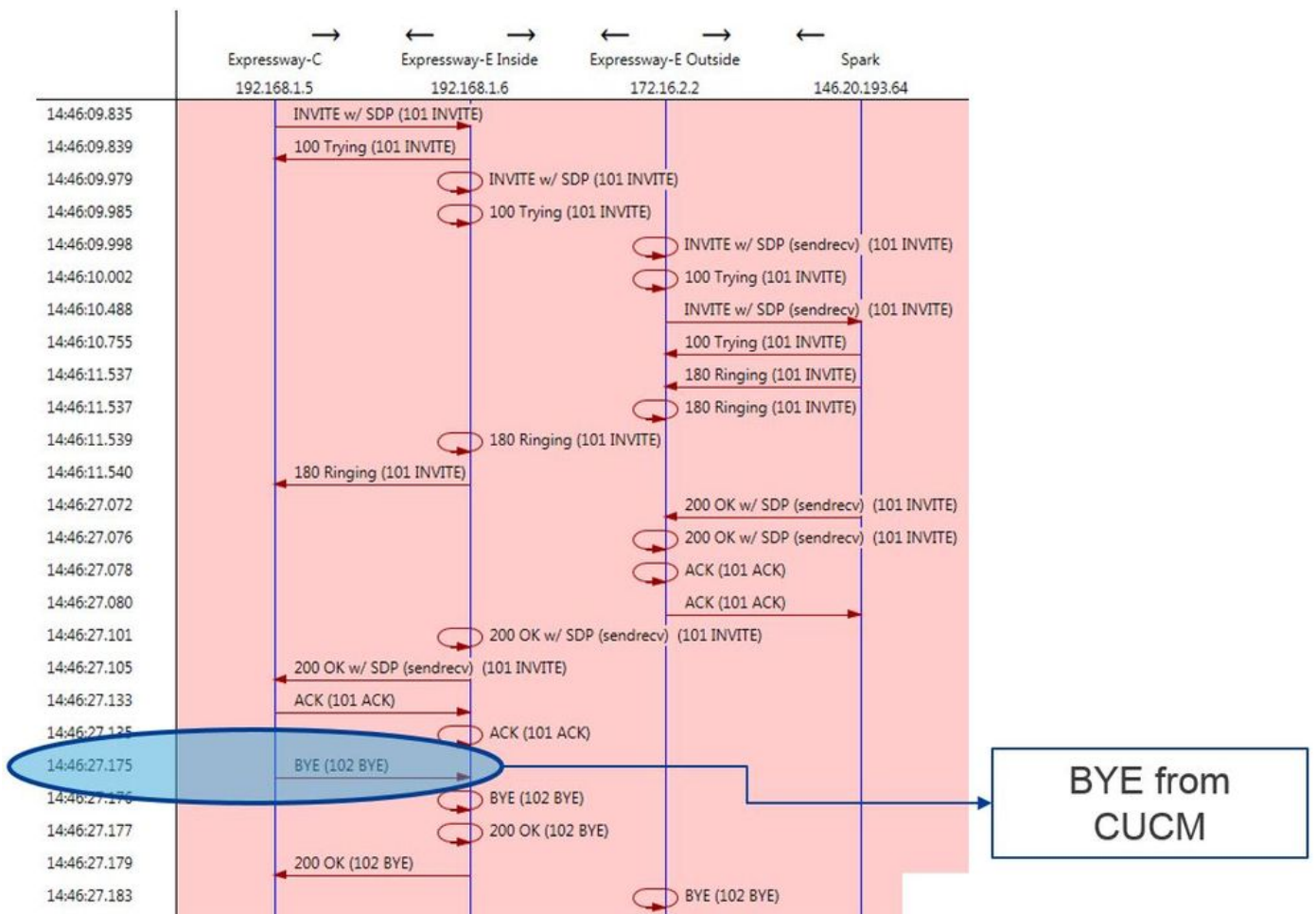
```
2017-09-19T10:46:27.073-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 14:46:27,072"
Module="network.sip" Level="DEBUG": Action="Received" Local-ip="172.16.2.2" Local-port="25034"
Src-ip="146.20.193.64" Src-port="5062" Msg-Hash="5236578200712291002"
SIPMSG:
SIP/2.0 200 OK
Via: SIP/2.0/TLS 64.102.241.236:5062;egress-
zone=HybridCallServicesDNS;branch=z9hG4bK323e6b15ad0cbbf409751f67848136fa1115;proxy-call-
id=a3a78ee2-c01b-4741-b29b-55aedeaa256d2;rport=38245;received=192.168.5.26,SIP/2.0/TLS
172.16.2.2:5073;branch=z9hG4bK350703fe46645f0acdde05b35adc5c157;x-cisco-local-
service=nettle;received=172.16.2.2;rport=41511;ingress-zone=DefaultZone,SIP/2.0/TLS
192.168.1.6:5061;egress-
zone=DefaultZone;branch=z9hG4bKf71f2bf47233d6ca52b579364594ac6c1114.a402e3f25603f5a77b60b17ea47d
bf72;proxy-call-id=be17a470-0bca-4ad5-8a6c-
14872e007efb;received=192.168.1.6;rport=25025,SIP/2.0/TLS 192.168.1.5:5061;egress-
zone=HybridCallServiceTraversal;branch=z9hG4bKf4cfd09d213a88bd2331cef0bc82b540559.494a140082bd
```

66357134b9eed4335df8;proxy-call-id=d4d4e950-babc-45d5-a4a7-c60a8b17a8bd;received=192.168.1.5;rport=26513;ingress-zone=HybridCallServiceTraversal,SIP/2.0/TCP  
192.168.1.21:5065;branch=z9hG4bK12dd82194c4f7;received=192.168.1.21;ingress-zone=CUCM11  
Call-ID: 44bdd400-9c112db1-12d95-1501a8c0@192.168.1.21  
CSeq: 101 INVITE  
Contact: "l2sip-UA" <sip:l2sip-UA@l2sip-cfa-01.wbx2.com:5062;transport=tls>  
From: "Jonathan Robb"

Record-Route: <sip:l2sip-cfa-01.wbx2.com:5062;transport=tls;lr>, <sip:proxy-call-id=a3a78ee2-c01b-4741-b29b-55aede256d2@64.102.241.236:5062;transport=tls;lr>, <sip:proxy-call-id=a3a78ee2-c01b-4741-b29b-55aede256d2@172.16.2.2:5061;transport=tls;lr>  
Allow: INVITE,ACK,CANCEL,BYE,REFER,INFO,OPTIONS,NOTIFY,SUBSCRIBE  
User-Agent: Cisco-L2SIP  
Supported: replaces  
Accept: application/sdp  
Allow-Events: kpml  
Session-ID: ed35426ed3ade6fdc3b058792333df2b;remote=75957d4fb66a13e835c10737aa329445  
Locus: 4711a33f-9d49-11e7-9bf6-dea12d0f2127  
Locus-Type: CALL  
Content-Type: application/sdp  
Content-Length: 503

v=0  
o=linus 0 1 IN IP4 146.20.193.109  
s=-  
c=IN IP4 146.20.193.109  
b=TIAS:384000  
t=0 0  
m=audio 0 RTP/SAVP \* <-- Webex is zeroing this port out  
m=video 33512 RTP/SAVP 108  
c=IN IP4 146.20.193.109  
b=TIAS:384000  
a=content:main  
a=sendrecv  
a=rtpmap:108 H264/90000  
a=fmtp:108 profile-level-id=42001E;packetization-mode=1;max-mps=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

Sie können nun TranslatorX verwenden, um den Rest des Dialogs zu überprüfen. Sie sehen, dass der Dialog selbst mit einem ACK abgeschlossen ist. Das Problem besteht unmittelbar nach Abschluss des Dialogs darin, dass ein BYE aus der Richtung Expressway-C kommt, wie im Bild gezeigt.



Im Folgenden finden Sie ein detailliertes Beispiel für die BYE-Nachricht. Sie sehen eindeutig, dass der Benutzer-Agent Cisco-CUCM11.5 ist. Dies bedeutet, dass die Nachricht vom Unified CM generiert wurde. Ein weiterer Hinweis ist, dass der Ursachencode auf Cause=47 festgelegt ist. Die gemeinsame Übersetzung hierfür ist nicht verfügbar.

```

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

```

Da die Cisco WebEx Komponente den Audio-Codec für dieses Anrufbeispiel mit Null versehen hat, muss der Schwerpunkt auf folgenden Aspekten liegen: a) Die erste INVITE, die an Cisco WebEx gesendet wurde und b) Was war die Logik, mit der Cisco WebEx diesen Port ausgeschaltet

hat?Betrachtet man nun das Einzigartige an der ursprünglichen INVITE, so ist festzustellen, dass sie nur G.729 enthält. In diesem Zusammenhang lesen Sie den Cisco WebEx Hybrid Call Service Deployment Guide und lesen insbesondere das Kapitel Prepare Your Environment (Umgebung vorbereiten), in dem die unterstützten Codecs in Schritt 5 des [Abschnitts Complete the Requirements for Hybrid Call Service Connect](#) aufgerufen werden. Hier sehen wir Folgendes: Cisco WebEx unterstützt die folgenden Codecs:

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

*Hinweis: Der Opus wird nicht vor Ort für den Anruf zu Cisco WebEx Hybrid Call verwendet.* Anhand dieser Informationen können Sie feststellen, dass Unified CM einen nicht unterstützten Audio-Codec sendet. Dies ist der Grund, warum Cisco WebEx den Port deaktiviert. Lösung: Um diese Situation zu beheben, müssen Sie möglicherweise die Regionskonfiguration zwischen dem Cisco Webex RD, der den Anruf vor Ort verankert, und dem SIP-Trunk für den Expressway-C überprüfen. Bestimmen Sie dazu, in welchem Gerätepool sich diese beiden Elemente befinden. Der Gerätepool enthält die Zuordnungen zu den Regionen. So bestimmen Sie den Gerätepool des Expressway-C SIP-Trunks:

1. Melden Sie sich beim Unified CM an.
2. Navigieren Sie zu Gerät > Trunk.
3. Suchen Sie nach dem Trunk-Namen, oder klicken Sie auf Suchen.
4. Wählen Sie den Expressway-C-Trunk aus.
5. Notieren Sie den Namen des Gerätepools.

So bestimmen Sie den Gerätepool des CTI-RD oder Cisco WebEx-RD, der den Anruf übernommen hat:

1. Navigieren Sie zu Gerät > Telefon.
2. Bei der Suche können Sie Device Type (Gerätetyp) aus WebEx oder CTI Remote Device (CTI-Remote-Gerät) auswählen (abhängig davon, was der Kunde verwendet).
3. Notieren Sie den Namen des Gerätepools.

Bestimmen Sie die Region, die jedem Gerätepool zugeordnet ist:

1. Navigieren Sie zu System > Device Pool (System > Gerätepool).
2. Suchen Sie nach dem Gerätepool, der für den Expressway-C SIP-Trunk verwendet wird.
3. Klicken Sie auf den Gerätepool.
4. Notieren Sie den Namen Region.
5. Suchen Sie nach dem Gerätepool, der für den Webex-RD oder CTI-RD verwendet wird.
6. Klicken Sie auf den Gerätepool.
7. Notieren Sie den Namen Region.

Bestimmen der Regionsbeziehung:

1. Navigieren Sie zu System > Region information > Region.
2. Suchen Sie nach einem der angegebenen Regionen.
3. Stellen Sie fest, ob eine Regionsbeziehung zwischen beiden Regionen besteht, die G.729 verwenden.

Wenn Sie an diesem Punkt die Beziehung identifizieren, die G.729 verwendet, müssen Sie die Beziehung zur Unterstützung der unterstützten Audiocodecs anpassen, die von Cisco WebEx verwendet werden, oder einen anderen Gerätepool verwenden, der über eine Region verfügt, die diese unterstützt. In dem oben beschriebenen Szenario wurde Folgendes ermittelt: Expressway-C-Trunk-Region: ReservierungBandbreiteWebex-RD-Region: RTP-GeräteHier sehen Sie eine grafische Darstellung der Beziehung zwischen den RTP-Geräten und den Reservierungsbandbreitenbereichen, wie im Bild gezeigt.



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

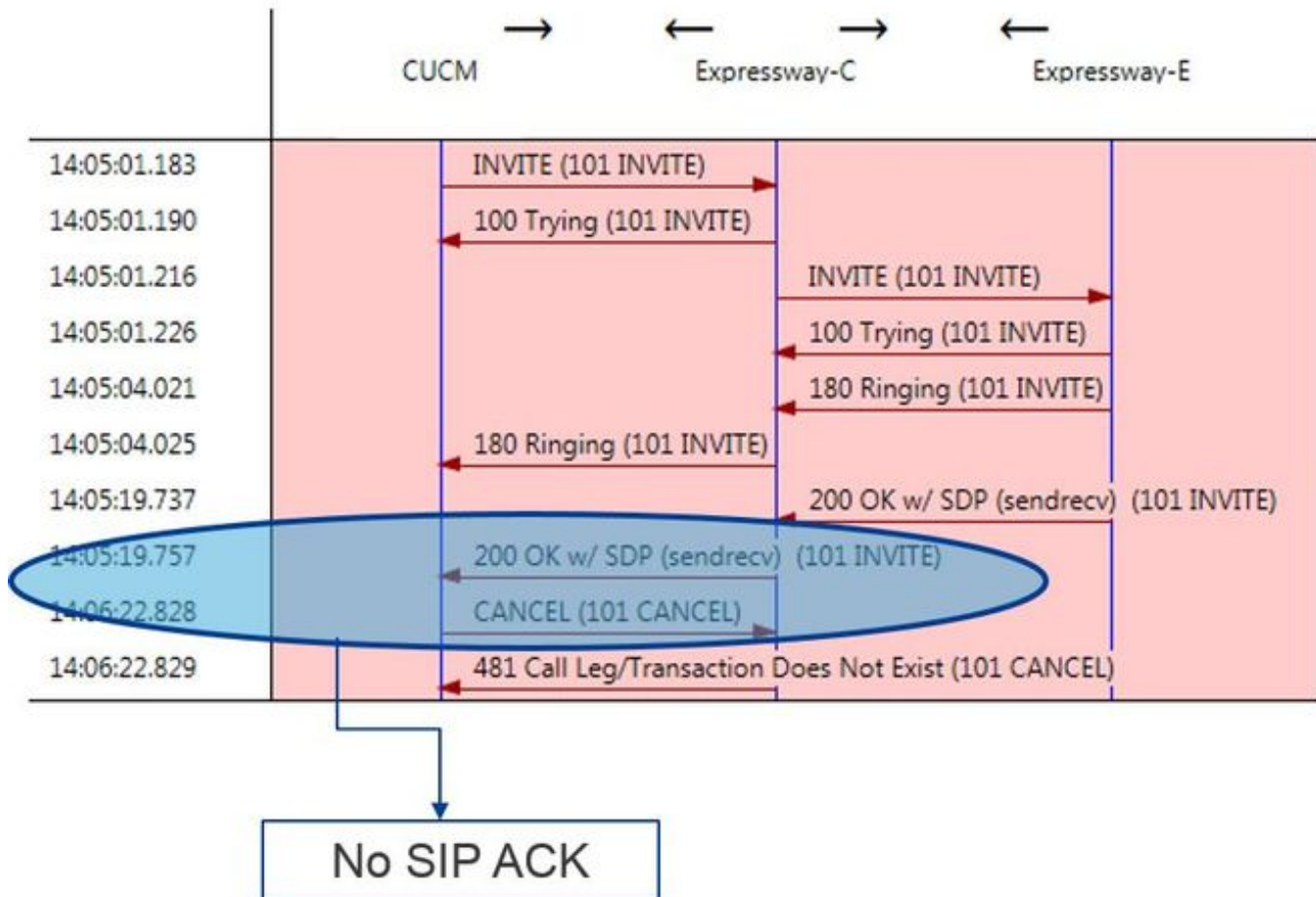
G.729 Not Supported by Spark

Durch Ändern des Gerätepools, in dem sich der Expressway-C-Trunk befunden hat, ändern Sie die Region-Beziehung. Für den neuen Gerätepool wurde die Region auf RTP-Infrastruktur festgelegt. Daher war die neue Regionsbeziehung zwischen dem Cisco Webex-RD und dem Expressway-C-Trunk RTP-Devices und die RTP-Infrastruktur. Wie abgebildet dargestellt, unterstützt diese Beziehung AAC-LD, einen der unterstützten Audio-Codecs für Cisco WebEx, sodass der Anruf korrekt eingerichtet wird. Ausgabe 2: Maximale Größe eingehender Nachrichten für Unified CM überschritten Da Videokommunikation im Unternehmen immer mehr zum Einsatz kommt, ist die Größe der SIP-Nachrichten, die SDP enthalten, erheblich angestiegen. Die Server, die diese Meldungen verarbeiten, müssen so konfiguriert werden, dass sie ein großes Paket akzeptieren können. Bei vielen Anrufsteuerungsservern sind die Standardwerte in Ordnung. Beim Cisco Unified Communications Manager (Unified CM) waren die Standardwerte für die Verarbeitung einer großen SIP-Nachricht mit SDP in früheren Versionen nicht ausreichend. In späteren Versionen von Unified CM wurde die zulässige Wertegröße für eine SIP-Nachricht erhöht. Dieser Wert wird jedoch nur bei Neuinstallationen und nicht bei Upgrades festgelegt. Kunden, die ihre älteren Unified CM-Versionen auf die Unterstützung von Hybrid Call Service Connect erweitern, könnten dadurch von der zu niedrigen maximalen Größe eingehender Nachrichten auf Unified CM betroffen sein. Wenn Sie versuchen, einen Anrufausfall beim Hybrid Call Service Connect zu identifizieren, der zu diesem Problem passt, müssen Sie zusätzlich zu den Unified CM-SDL-Ablaufverfolgungen die Expressway-Protokolle abrufen. Um den Fehler zu identifizieren, müssen Sie zunächst die Vorgänge und dann die Szenarien, in denen der Fehler auftreten kann, verstehen. Um die Frage zu beantworten, was passiert, müssen Sie wissen, dass, sobald der Unified CM eine zu große SIP-Nachricht empfängt, er einfach den TCP-Socket schließt und nicht auf Expressway-C reagiert. Es gibt jedoch viele Situationen und Möglichkeiten, wie dies geschehen kann:

1. Cisco WebEx sendet eine eingehende INVITE mit SDP, die zu groß ist. Der Expressway-C übergibt diese Daten an den Unified CM, und der Unified CM schließt den TCP-Socket. Anschließend wird der SIP-Dialog beendet.
2. Unified CM versucht den ausgehenden Anruf als "Early Offer to WebEx", d. h. die erste an Expressway-C gesendete INVITE enthält SDP. Cisco Webex sendet daraufhin eine 200 OK mit SDP als Antwort, und die 200 OK-Antwort, wenn sie vom Expressway-C an den Unified CM übergeben wird, ist zu groß. Unified CM schließt den TCP-Socket, und der SIP-Dialog wird beendet.
3. Unified CM versucht den ausgehenden Anruf als "Delayed Offer to Webex" (Verzögertes Angebot an Webex) zu verwenden. Das bedeutet, dass der erste INVITE, der an Expressway-C gesendet wird, kein SDP enthält. Cisco Webex sendet dann ein 200 OK mit SDP, und das 200 OK-Angebot ist zu groß, wenn es vom Expressway-C an den Unified CM übergeben wird. Unified CM schließt den TCP-Socket, und der SIP-Dialog wird beendet.

Wenn Sie sich die Expressway-C-Protokolle für diese spezielle Bedingung ansehen, können Sie den Nachrichtenfluss besser verstehen. Wenn Sie ein Programm wie [TranslatorX](#) verwenden, sehen Sie, dass Expressway-C das Cisco WebEx 200 OK mit SDP an Unified CM übergibt. Die Herausforderung besteht darin, dass Unified CM niemals mit einer SIP-ACK zurückantwortet, wie im Bild gezeigt.





Da der Unified CM nicht antwortet, sollten Sie die SDL Traces überprüfen, um zu sehen, wie der Unified CM mit dieser Bedingung umgeht. In diesem Szenario wird vom Unified CM die große Meldung aus dem Expressway-C ignoriert. Ein solches Login-Element wird ausgegeben.

#### 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.
```

Wenn das SIP-Dialogfeld das Zeitlimit überschreitet, sendet Cisco WebEx eine eingehende SIP 603 Decline-Nachricht an den Expressway-E, wie im Protokollbeispiel angegeben.

#### 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
```

Wie bereits erwähnt, gibt es drei verschiedene Szenarien, in denen Sie dieses Verhalten sehen können. Aus Gründen der Übersichtlichkeit entsprachen die in dieser Abbildung gezeigten Protokollbeispiele Situation 3, in der der Anruf als verzögertes Angebot an Cisco WebEx gesendet wurde. Lösung:

1. Melden Sie sich beim Unified CM an.
2. Navigieren Sie zu System > Dienstparameter.
3. Wählen Sie den Server aus, auf dem der Call Manager-Dienst ausgeführt wird.

4. Wählen Sie den Cisco Call Manager-Service aus, wenn Sie zur Auswahl eines Service aufgefordert werden.
5. Wählen Sie die erweiterte Option aus.
6. Ändern Sie unter den Clusterweiten Parameter (Device - SIP) die maximale Größe für eingehende SIP-Nachrichten auf 18.000.
7. Wählen Sie Speichern aus.
8. Wiederholen Sie diesen Vorgang für alle Unified CM-Knoten, auf denen der Cisco Call Manager-Dienst ausgeführt wird.

Hinweis: Damit ein IP-Telefon, ein Collaboration-Endgerät und/oder ein SIP-Trunk diese Einstellung nutzen können, muss dieser neu gestartet werden. Diese Geräte können einzeln neu gestartet werden, um die Auswirkungen auf die Umgebung zu minimieren. Setzen Sie NICHT jedes Gerät auf dem CUCM zurück, es sei denn, Sie wissen, dass dies absolut zulässig

ist. **Anhang** Expressway-Problembewegungsstools Dienstprogramm Muster überprüfen Der Expressway verfügt über ein Dienstprogramm zur Musterprüfung, das nützlich ist, wenn Sie testen möchten, ob ein Muster einem bestimmten Alias entspricht und wie erwartet transformiert wird. Das Dienstprogramm finden Sie auf dem Expressway unter der Menüoption Maintenance > Tools > Check pattern (Wartung > Extras > Muster überprüfen). In der Regel wird dies verwendet, wenn Sie testen möchten, ob der Regex Suchregel einen Alias einer Musterzeichenfolge korrekt zuordnet und dann optional eine erfolgreiche Manipulation der Zeichenfolge durchführen soll. Bei Hybrid Call Service Connect können Sie auch testen, ob der Unified CM-Cluster-FQDN mit der Musterzeichenfolge übereinstimmt, die Sie für den Unified CM-Cluster-FQDN eingerichtet haben. Beachten Sie bei Verwendung dieses Dienstprogramms, dass der Anruf auf Grundlage des im Route Header aufgelisteten Unified CM-Cluster-FQDN-Parameters weitergeleitet wird, nicht auf Basis des Ziel-URI. Wenn z. B. die folgende Einladung in den Expressway kam, testen Sie die Funktion Prüfmuster mit cucm.rtp.ciscotac.net, nicht jorobb@rtp.ciscotac.net.

**SIPMSG:**

```
|INVITE sip:jorobb@rtp.ciscotac.net SIP/2.0
Via: SIP/2.0/TLS 192.168.1.6:7003;egress-
zone=HybridCallServiceTraversal;branch=z9hG4bKcac6d95278590991a2b516cf57e75827371;proxy-call-
id=abcba873-eaae-4d64-83b4-c4541d4e620c;rport
Via: SIP/2.0/TLS 192.168.1.6:5073;branch=z9hG4bK837b03f2cd91b6b19be4fc58edb251bf12;x-cisco-
local-service=nettle;received=192.168.1.6;rport=41913;ingress-zone=DefaultZone
Via: SIP/2.0/TLS 64.102.241.236:5061;egress-
zone=DefaultZone;branch=z9hG4bK524f89592d00ffc45b7b53000271676c370.88b5177ac4d7cfcae1eb8f8be78da
055;proxy-call-id=2db939b2-a49b-4307-8d96-23716a2c090b;received=172.16.2.2;rport=25010
Via: SIP/2.0/TLS
192.168.4.150:5062;branch=z9hG4bK92f9ef952712e6610c3e6b72770c1230;received=148.62.40.63;rport=39
986;ingress-zone=HybridCallServicesDNS
Via: SIP/2.0/TLS 127.0.0.1:5070;branch=z9hG4bK-313634-
3d27a6f914badee6420287903c9c6a45;rport=45939
Call-ID: 3e613afb185751cdf019b056285eb574@127.0.0.1
CSeq: 1 INVITE
Contact: <sip:192.168.1.6:5073;transport=tls>
From: "pstoiano test" <sip:pstoiano-test@dmzlab.call.ciscopark.com>;tag=145765215
To: <sip:jorobb@rtp.ciscotac.net>
Max-Forwards: 15
Route:
```

Führen Sie die folgenden Schritte aus, um das Routen-Header für die Hybrid Call Service Connect-Header mithilfe von Suchmustern zu testen:

1. Navigieren Sie zu Maintenance > Tools > Check pattern.
2. Geben Sie für die Alias den Unified CM-Cluster-FQDN ein.
3. Legen Sie den Mustertyp auf Präfix fest.
4. Legen Sie die Musterzeichenfolge auf Unified CM-Cluster FQDN fest.
5. Legen Sie das Musterverhalten auf Leave (Aus) fest.
6. Wählen Sie Muster überprüfen aus.

Wenn die Suchregeln auf dem Expressway korrekt konfiguriert sind, können Sie erwarten, dass die Ergebnismeldung die Meldung Erfolgreich zurückgibt. Im Folgenden sehen Sie ein Beispiel für einen erfolgreichen Test des Prüfmusters, wie im Bild gezeigt.

### Check pattern

**Alias**

Alias

**Pattern**

Pattern type

Pattern string

Pattern behavior

### Result







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

Der Grund dafür ist, dass Alias (cucm.rtp.ciscotac.net) mit der Prefix pattern String von (cucm.rtp.ciscotac.net) übereinstimmt. Um zu verstehen, wie ein Anruf auf der Grundlage dieser Ergebnisse weitergeleitet wird, können Sie das beschriebene Expressway Locate Utility verwenden. Das Dienstprogramm "Suchen" von Expressway ist nützlich, wenn Sie testen möchten, ob der Expressway einen Anruf auf Basis eines angegebenen Alias an eine bestimmte Zone weiterleiten kann. All dies kann ohne einen echten Anruf abgeschlossen werden. Das Dienstprogramm "Suchen" finden Sie auf der Expressway unter Maintenance > Tools > Locate menu. Es werden einige Anweisungen angezeigt, wie Sie mithilfe der Locate-Funktion auf dem Expressway-C feststellen können, ob der Server einen Anruf basierend auf dem Unified CM-Cluster-FQDN im SIP-Routen-Header weiterleiten kann.

1. Navigieren Sie zu Maintenance > Tools > Locate (Wartung > Tools > Suchen).
2. Geben Sie den Unified CM-Cluster-FQDN im Feld Alias ein.
3. Wählen Sie SIP als Protokoll aus.
4. Wählen Sie Ihre Cisco WebEx Hybrid Traversal Client Zone für die Quelle aus.
5. Wählen Sie Suchen aus.

Am unteren Ende der Benutzeroberfläche werden die Suchergebnisse angezeigt. Im Folgenden sehen Sie ein Beispiel für einen Beispielttest, der mit den entsprechenden Ergebnissen ausgeführt wurde, wie im Bild gezeigt.

## Locate

|               |   |
|---------------|---|
| Locate        |   |
| Alias         | * cucm.rtp.ciscotac.net        |
| Hop count     | * 5                              |
| Protocol      | SIP                              |
| Source        | Hybrid Call Service Traversal  |
| Authenticated | Yes                              |
| Source alias  | <input type="text"/>           |

Locate

Hier sind die Ergebnisse der Locate. Führt sind die Werte von Interesse. Diese Ergebnisse zeigen:

- Die Tatsache, dass die Alias geroutet werden konnten (True)
- Quellinformationen (Zonenname/-typ)
- Zielinformationen (Alias wird weitergeleitet)
- Übereinstimmende Suchregel (Hybrid Call Service Inbound Routing)
- Die Zone, an die der Anruf gesendet wird (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**

**Diagnoseprotokollierung** Wenn Sie bei einem Anruf, der die Expressway-Lösung passiert, ein Problem mit Anrufen oder Medien beheben, müssen Sie die Diagnoseprotokollierung verwenden. Diese Expressway-Funktion gibt einem Techniker eine Menge Informationen für alle logischen Entscheidungen, die der Expressway während des Anrufs durchläuft. Sie können die vollständigen SIP-Nachrichten sehen, wie der Expressway diesen Anruf durchläuft und wie der Expressway die Medienkanäle konfiguriert. Die Diagnoseprotokollierung umfasst eine Reihe von Modulen, die in die Protokollierung eingehen. Die Protokollierungsebenen können so angepasst werden, dass

FATAL, FEHLER, WARN, INFO, DEBUG, TRACE angezeigt wird. Standardmäßig ist alles auf INFO gesetzt, wodurch fast alles erfasst wird, was Sie für die Diagnose eines Problems benötigen. Von Zeit zu Zeit müssen Sie möglicherweise die Protokollierungsebene eines bestimmten Moduls von INFO auf DEBUG anpassen, um ein besseres Verständnis der Vorgänge zu erhalten. In den folgenden Schritten wird veranschaulicht, wie Sie die Protokollierungsebenen des developer.ssl-Moduls anpassen können, das für die Bereitstellung von Informationen für (gegenseitige) TLS-Handshakes verantwortlich ist.

1. Melden Sie sich beim Expressway-Server an (muss sowohl auf dem Expressway-E als auch auf dem C erfolgen).
2. Navigieren Sie zu Maintenance > Diagnostics > Advanced > Support Log Configuration.
3. Scrollen Sie zu dem Modul, das Sie anpassen möchten, in diesem Fall developer.ssl und klicken Sie darauf.
4. Wählen Sie neben dem Parameter Level (Stufe) DEBUG aus dem Menü aus.
5. Klicken Sie auf Speichern.

Jetzt sind Sie bereit, die Diagnoseprotokollierung zu erfassen:

1. Melden Sie sich beim Expressway-Server an (muss sowohl auf dem Expressway-E als auch auf dem C erfolgen).
2. Navigieren Sie zu Maintenance > Diagnostics > Diagnostic logging.
3. Klicken Sie auf Neues Protokoll starten (aktivieren Sie die Option tcpdump).
4. Reproduzieren Sie das Problem.
5. Klicken Sie auf Protokollierung beenden.
6. Klicken Sie auf Protokoll herunterladen.

Für die Expressway-Diagnoseprotokollierung sollten Sie bedenken, dass Sie die Protokollierung sowohl vom Expressway-C als auch vom Expressway-E parallel starten würden: Starten Sie zunächst die Protokollierung auf dem Expressway-E, dann gehen Sie zum Expressway-C und starten Sie es. Anschließend können Sie das Problem reproduzieren. Hinweis: Derzeit enthält das Expressway/VCS Diagnoseprotokoll-Bündel keine Informationen über das Expressway Server-Zertifikat oder die Liste der vertrauenswürdigen Zertifizierungsstellen. Wenn Sie einen Fall haben, in dem eine solche Funktionalität von Vorteil wäre, fügen Sie bitte [diesen Fehler](#)

## bei. Zugehörige Informationen

- [Bereitstellungsleitfaden für Cisco WebEx Hybrid Call Services](#)
- [Cisco WebEx Hybrid-Designleitfaden](#)
- [Administratoranleitung für Cisco Expressway](#)
- [Technischer Support und Dokumentation für Cisco Systeme](#)



## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.