Handleiding voor probleemoplossing voor Cisco Webex Hybride Call Service Connect

Inhoud

Inleiding
Voorwaarden
Vereisten
Gebruikte componenten
Achtergrondinformatie
Problemen met gespreksopbouw
TMS-handshake-mislukkingen
Handige wederzijdse TLS-tips voor probleemoplossing
Uitgave 1. Expressway-E is geen Trust certificaatautoriteit (CA) die het Cisco Webex-certificaat heeft ondertekend
Probleem 2. Onjuiste naam voor TLS Onderwerp Controleer naam op Expressway-E Cisco Webex hybride DNS-zone
Vraag 3. Expressway-E stuurt geen volledige certificaatketen naar Cisco Webex
4. Firewall beëindigt wederzijdse TLS-handdruk
Vak 5. Expressway-E wordt ondertekend door openbare CA, maar Cisco Webex Control Hub heeft alternatieve certificaten geladen
Uitgave 6. Expressway is geen Toewijzing van inkomende oproep aan Cisco Webex Hybrid DNS Zone
Uitgave 7. Sneltoets-E gebruikt standaard zelfgetekend certificaat
Inkomend: Cisco Webex naar locaties
Probleem 1. Cisco Webex kan niet de snelweg-E DNS SRV/hostname oplossen
Afdeling 2: Socketfalen: Port 5062 is ingesloten in een expresse-ingang
Uitgifte 3. Socketfalen: Expressway-E staat niet op poort 5062
Vraag 4. E of C ondersteunen vooraf geladen SIP-routekoppen niet
Vraag 5. Cisco Webex-app ontvangt twee gespreksmeldingen (kantelingen)
Uitgaand: Premises aan Cisco Webex
Vraag 1. Expressway is niet in staat om het adres callservice.ciscospark.com op te lossen
Eigen 2. Port 5062 is geblokkeerd naar Cisco Webex
Kwestie 3. Onjuiste configuratie van de standaard voor snelwegen
4. Misconfiguratie van de CPL-uitdrukking
Bidirectioneel: Cisco Webex aan inbedrijfstelling of aan inbedrijfstelling bij Cisco Webex
Vraag 1. IP-telefoon/collaboration-endpoint biedt een audio-codec aan die niet gelijk is aan G.711, G.722 of AAC-LD.
Uitgave 2. Unified CM Max. inkomende berichtgrootte overschreden
Bijlage
Hulpmiddelen voor probleemoplossing
Patronenhulpprogramma controleren
Hulpprogramma lokaliseren
Diagnostische vastlegging

Gerelateerde informatie

Inleiding

Dit document beschrijft de Cisco Webex Hybrid Call Service Connect-oplossing die uw bestaande Cisco Call Control-infrastructuur toestaat om verbinding te maken met de Cisco Collaboration Cloud, zodat ze kunnen samenwerken.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Kennis van het Cisco Webex-aanbod
- Kennis van de oplossing van snelwegen (B2B)
- Kennis van Cisco Unified Communications Manager (Unified CM) en de integratie ervan met Express
- Unified CM 10.5(2) SU5 of hoger.
- Uitdrukking (B2B) versie X8.7.1 of hoger (X8.9.1 wordt aanbevolen)
- Sneltoets (Connectorhost) — zie Uitdrukconnector Host Support voor Cisco Webex Hybrid Services voor de momenteel ondersteunde versies

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Unified Communications Manager
- snelwegen
- Webex voor Windows
- Webex voor Mac
- Webexfor iOS
- Webex voor Android
- Cisco Collaboration-endpoints
- Endpoints voor samenwerking via bureaublad
- IP-telefoons
- Softwareclients

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Achtergrondinformatie

De oplossing biedt deze mogelijkheden:

- Gebruik de Webex-app als mobiele zachte client voor audio- en videogesprekken
- Gebruik de app om overal gesprekken te maken en te ontvangen, alsof ze op kantoor waren
- Gebruik Webex, Cisco Jabber of hun schrijftelefoon om te bellen zonder de noodzaak om zich zorgen te maken over de gebruikte optie
- Ontgrendel de vraaggeschiedenis in telefoons op het bedrijf en integreer die geschiedenis in Webex

Het bereik van deze handleiding is gericht op onderwerpen die uniek zijn voor Hybrid Call Service Connect. Aangezien Hybride Call Service Connect over hetzelfde E & C-paar van de Uitdrukker loopt als andere oplossingen zoals Mobiele en Remote Access en Business to Business-oproepen, kunnen problemen met de andere oplossingen de hybride Call Service Connect beïnvloeden. Voor klanten en partners die een expressroutepaar voor gebruik met Call Service Connect opstellen, moet de Cisco VCS Expressway en VCS Control Basic Configuration-handleiding worden vermeld voordat u probeert om Hybrid Call Service Connect te implementeren. Deze handleiding voor probleemoplossing bevat firewalls/NAT-overwegingen en snelontwerp in zowel bijlage 3 als bijlage 4. Bekijk deze documentatie aandachtig. Bovendien wordt er in dit document van uitgegaan dat de host van de expressconnector en de activering van de hybride gespreksservice zijn voltooid.

Problemen met gespreksopbouw

TMS-handshake-mislukkingen

Hybrid Call Service Connect gebruikt security transportlaag (wederzijds TLS) voor verificatie tussen Cisco Webex en de Expressway-E. Dit betekent dat zowel de Expressway-E als Cisco Webex controleren en het certificaat controleren dat elkaar aanwezig is. Aangezien wederzijdse TLS-problemen zo vaak voorkomen tijdens nieuwe implementaties van de sneltoetsen en de mogelijkheden voor oplossingen zoals Hybrid Call Service Connect, biedt deze sectie nuttige informatie en tips voor het oplossen van op certificaten gebaseerde problemen tussen de snelheden en Cisco Webex.

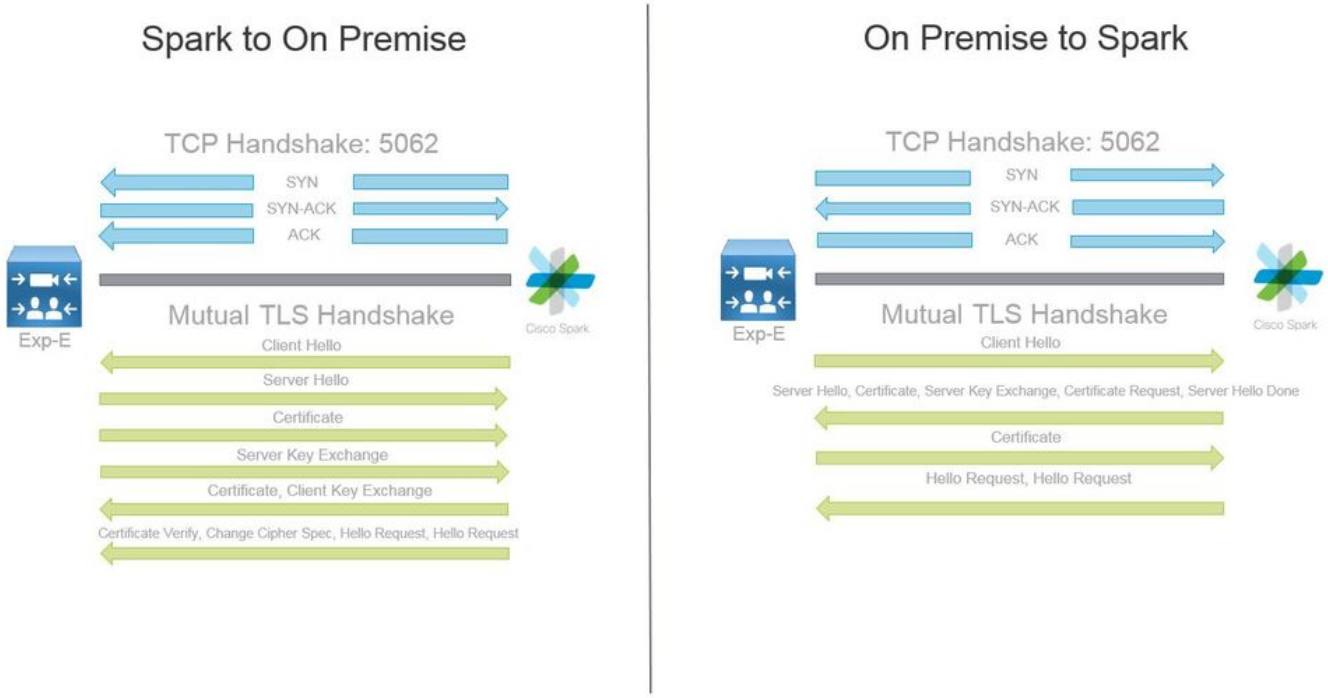
Wat controleert de expressway-E?

- Was het Cisco Webex-certificaat ondertekend door een openbare CA die in de lijst van Vertrouwde expressweg-E CA is opgenomen?
- Is callservice.ciscospark.com aanwezig in het veld Alternatieve naam voor onderwerp van het Cisco Webex-certificaat?

Wat controleert Cisco Webex?

- Is het expressway-E-certificaat ondertekend door een van de openbare CA's die Webex vertrouwt? (Cisco Webex Trusted CA-lijst)
- Als Expressway-E geen publiekelijk ondertekend certificaat gebruikt, was het expressopecertificaat samen met enige wortel- en intermediaire certificaten geüpload naar de Cisco Webex Control Hub (https://admin.ciscospark.com)?

Dit wordt uitgelegd zoals in de afbeelding.



Handige wederzijdse TLS-tips voor probleemoplossing

1. Onderlinge TLS-handdruk decoderen

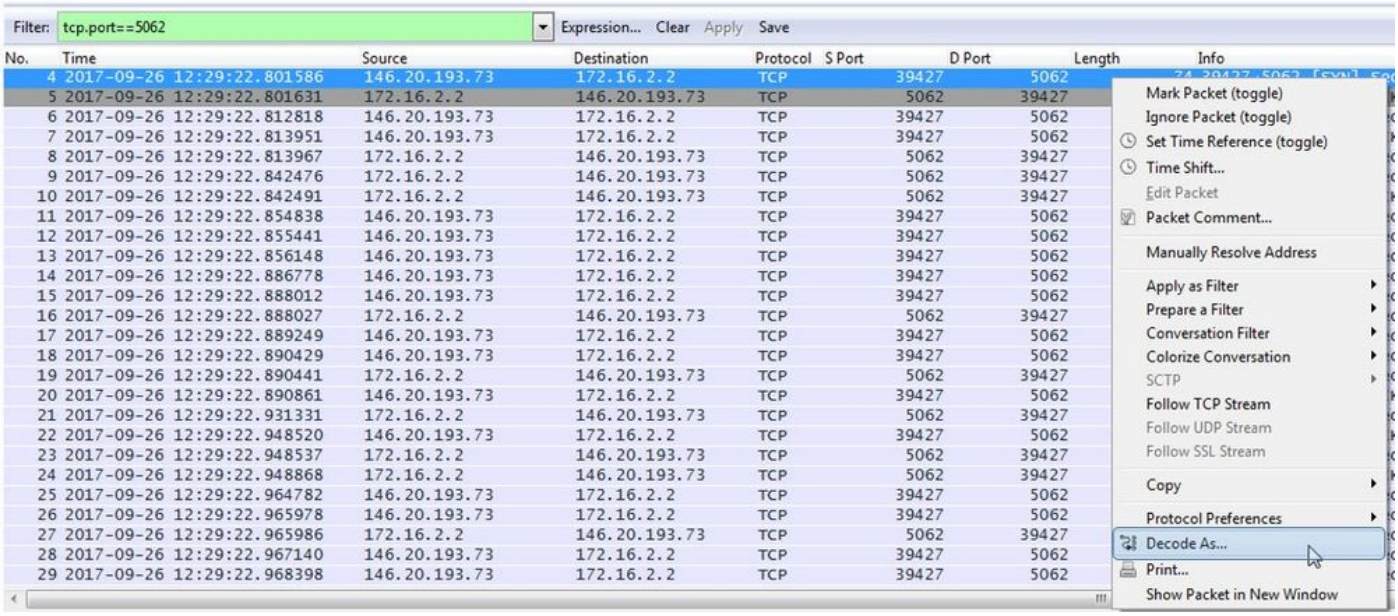
Standaard wordt met Wireshark het SIP TLS-verkeer aangeduid als poort 5061. Dit betekent dat elke keer dat u een (wederzijdse) TLS-handdruk wilt analyseren die zich via poort 5062 voordoet, Wireshark niet zal weten hoe u het verkeer goed moet decoderen. Hier is een voorbeeld van de wederzijdse TLS handdruk die over poort 5062 plaatsvindt zoals in de afbeelding wordt getoond.

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

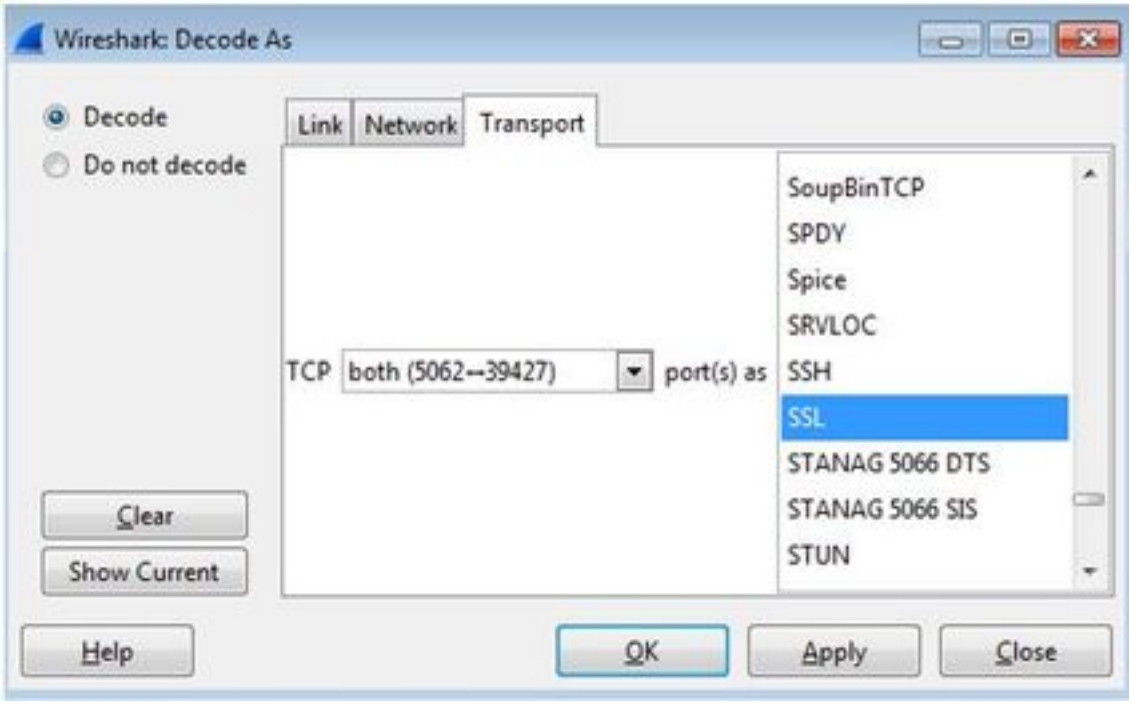
Zoals u kunt zien, is dit hoe de handdruk er uitziet met de standaardinstellingen van Wireshark. Packet-nummer 175 is het certificaat dat de sneltoets wordt verzonden naar Cisco Webex. Maar dat kun je niet bepalen zonder dat het verkeer wordt gedecodeerd. Er zijn twee methoden die u kunt gebruiken om de decode van dit verkeer te gebruiken zodat u de certificaatinformatie en de eventuele foutmeldingen gemakkelijker kunt zien.

1 bis. De stream als SSL decoderen

a. Wanneer u de handdruk van het wederzijdse TLS analyseert, eerst filtert u de opname door **tcp.port==5062**. Klik vervolgens met de rechtermuisknop op het eerste pakket in de stream en selecteer **Decode als...** zoals in de afbeelding wordt weergegeven.



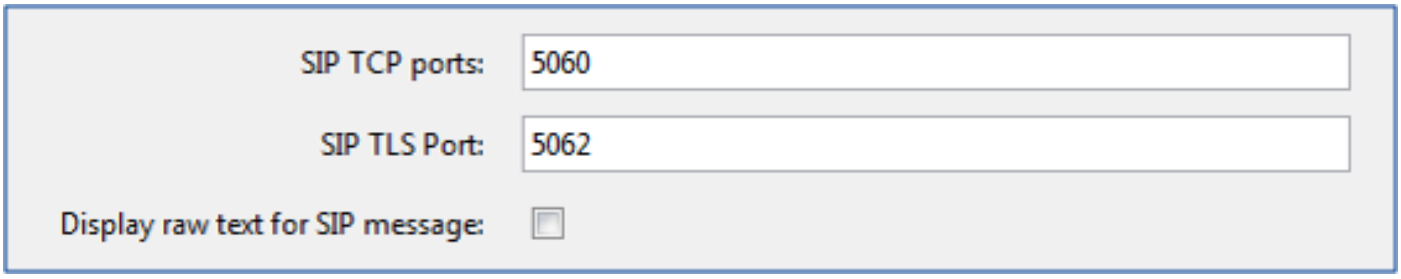
b. Zodra de optie **Decode As...** is geselecteerd, ziet u een lijst waarin u kunt selecteren hoe u de geselecteerde stream kunt decoderen. Selecteer in de lijst **SSL en** klik op **Toepassen** en sluit het venster. Op dit punt toont de gehele stream het certificaat en de foutmeldingen die werden uitgewisseld tijdens de handdruk zoals in de afbeelding.



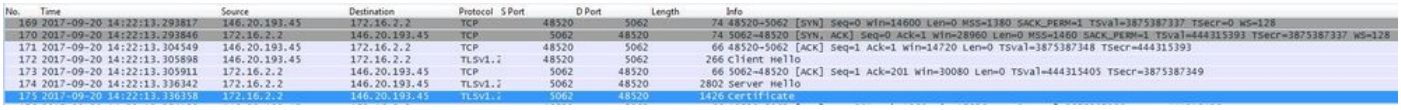
1 ter. SIP-TLS-poort aanpassen

Wanneer u de SIP TLS poort naar 5062 aanpast in de Voorkeuren voor draadloos harden, kunt u dan alle details zien die de handdruk omringen, die de certificaten omvat. Zo wijzigt u dit:

- Open Wireshark
- Navigeren in om **uit** te **werken > Voorkeuren**
- Protocollen uitvouwen en **SIP** selecteren
- Stel de SIP-TLS-poort in op 5062 en klik op **Toepassen**
- Stel de waarde terug op 5061 wanneer de analyse is voltooid zoals in de afbeelding.



Als u dezelfde opname nu analyseert, ziet u pakketten 169-175 gedecodeerd. Packet 175 toont het sneltoets-E certificaat en als u op het pakket boort, kunt u alle certificeringsgegevens zien zoals in de afbeelding.



2. Filtering draadloos haai

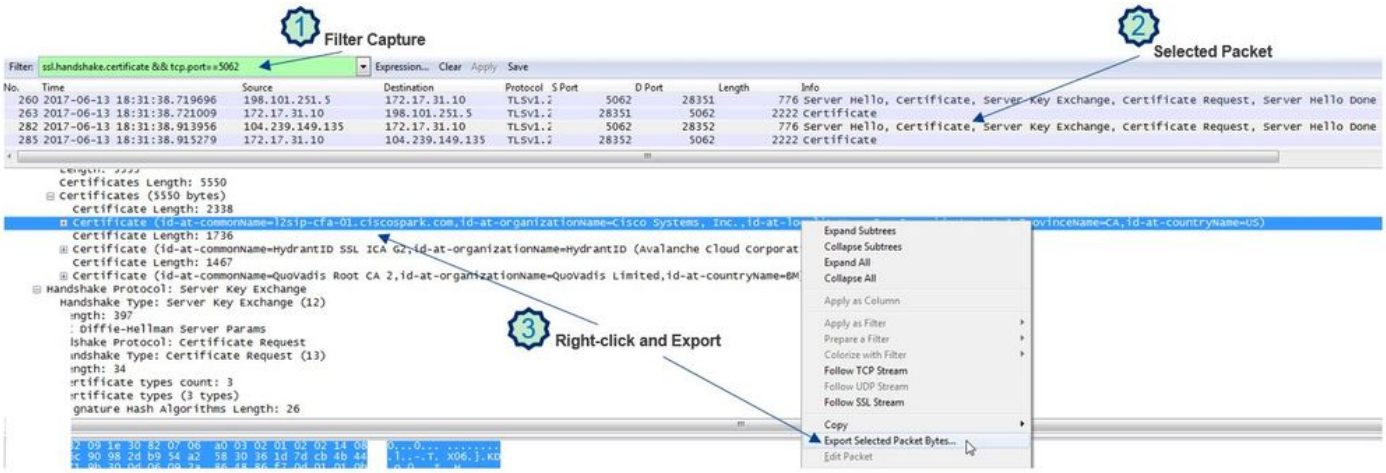
Wanneer u pakketvastlegging analyseert, is het gemakkelijk om te verliezen in de hoeveelheid pakketten die in een bepaalde opname worden waargenomen. Het is belangrijk om te begrijpen welk soort verkeer je het meest interesseert zodat je Wireshark kan filteren om dat weer te geven. Hier zijn een aantal veelvoorkomende Wireshark filters die kunnen worden gebruikt om meer informatie te krijgen over een linker-handdruk:

- TCP.poort==5062
- ssl && tcp.port==5062
- ssl.handshake.ertificaat & tcp.port==5062

3. Contractcertificaat aan dop

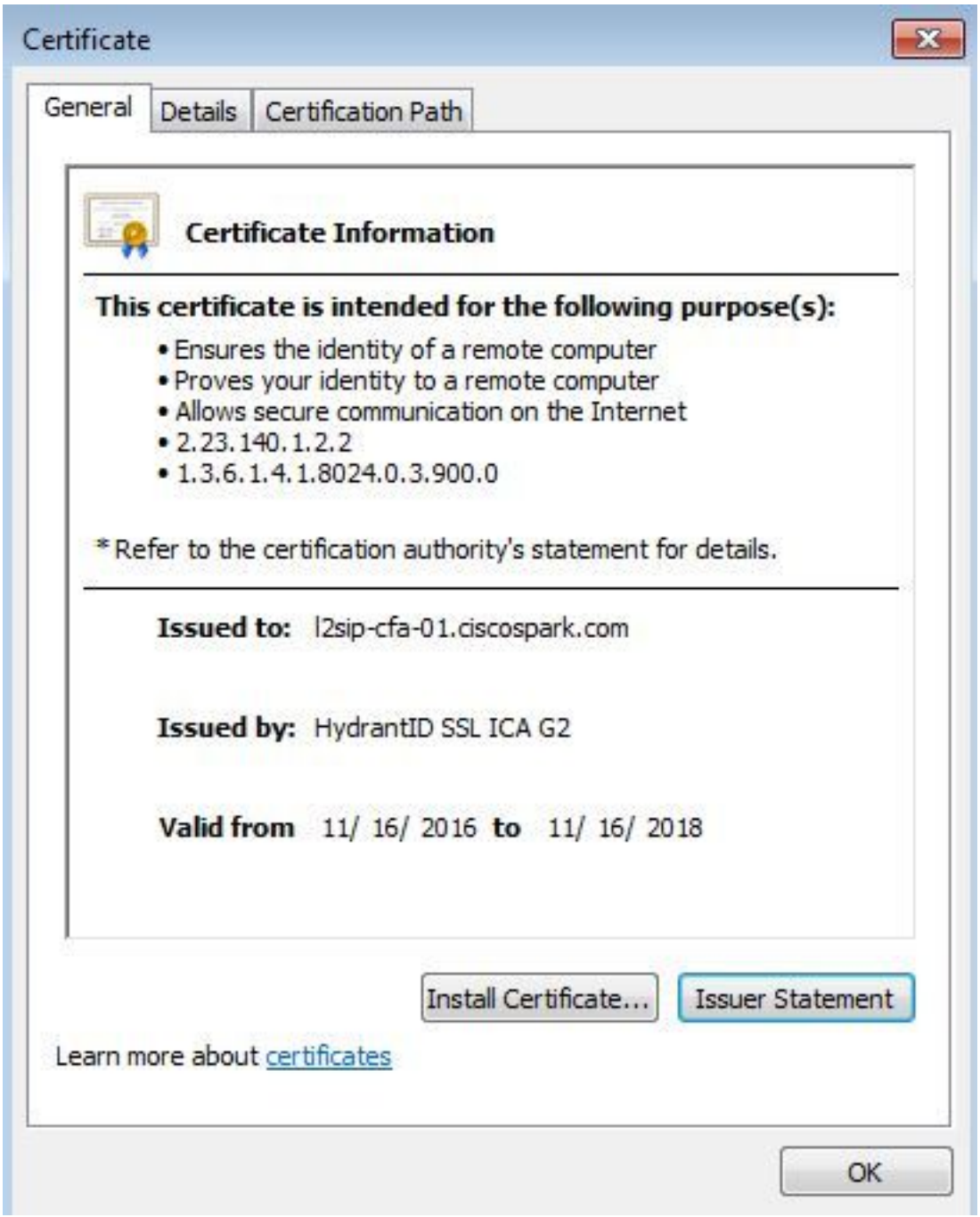
Van tijd tot tijd kunt u een kopie van een certificaat nodig hebben (server, wortel, of tussenpersoon). Als u niet weet waar u het certificaat wilt vinden dat u zoekt, kunt u het rechtstreeks uit een pakketvastlegging halen. Dit zijn de stappen voor het trekken van het Cisco Webex-certificaat dat bij een wederzijdse TLS-handdruk wordt weergegeven.

1. Het pakkettransport filteren met **ssl.handshake.ertificaat en tcp.port==5062**
2. Pak het pakket op dat afkomstig is van het Webex-serveradres en is certificaatafgedrukt in het gedeelte Info.
3. In de pakketgegevens **vouwt** u **Secure Socket Layer > TLS Certificate > Handshake Protocol > Certificaten uit**. **Opmerking:** Het bodem/laatste certificaat in de keten is de wortel CA.
4. Klik met de rechtermuisknop op het certificaat van belangstelling en selecteer **Geselecteerde Packet Bytes**... exporteren zoals in de afbeelding.



5. Sla het bestand op als **een .cer**.

6. Dubbelklik op het opgeslagen bestand om het certificaat te openen zoals in de afbeelding.



4. Instellen van niveaus voor automatische vastlegging

Er zijn twee logmodules beschikbaar op de expressway die u helpen beter te begrijpen welke logica de snelweg hanteert wanneer u de certificaten analyseert:

- ontwikkelaar.ssl
- ontwikkelaar.zone.zonemg

Standaard worden deze logmodules ingesteld op een INFO-niveau. Wanneer het wordt ingesteld op een DEBUG niveau, kunt u de informatie beginnen te zien over de certificateninspectie die gebeurt, samen met welke zone verkeer in kaart wordt gebracht. Beide functies zijn relevant voor de hybride gespreksservice.

Voorbeeld van de Expressway-E die een SAN-inspectie van Cisco Webex's servercertificaat uitvoert.

```
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"
```

Voorbeeld van de snelweg-E-mapping van de MTLS-verbinding naar de Cisco Webex hybride 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"
```

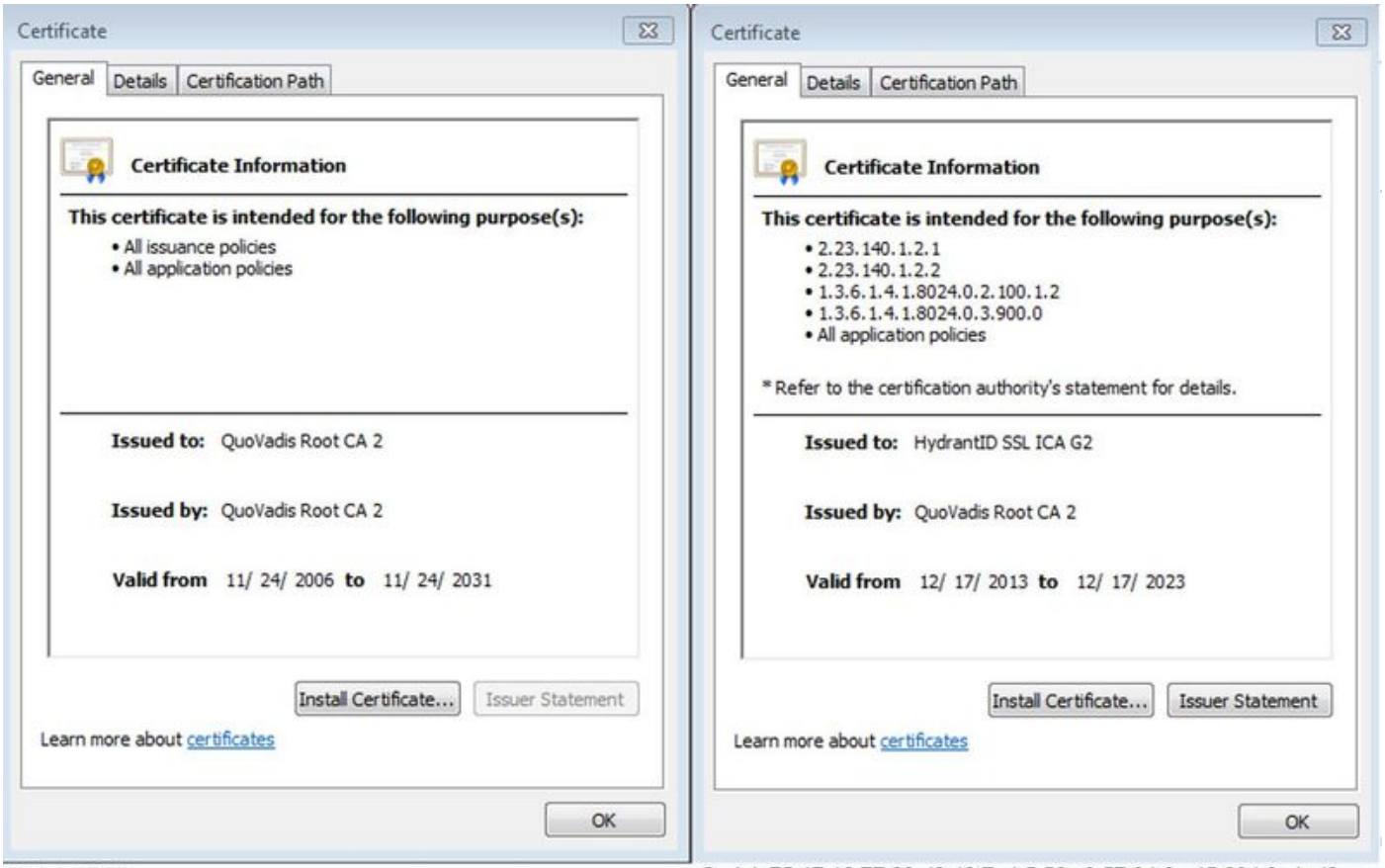
CodeLocation="ppcmains/oak/zones/ZoneManager.cpp(1226)"
Method="ZoneManager::getDNSZoneByTLSVerifySubjectName" Thread="0x7f577f0a0700":
this="0x56408ff81220" **getDNSZoneByTLSVerifySubjectName classified subject name callservice.ciscospark.com into DNS zone Hybrid Call Services DNS**
2017-09-22T11:11:19.564-04:00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

Hier is een lijst van de meest gebruikelijke kwesties die betrekking hebben op wederzijdse TLS-fouten tussen de snelweg-E en Cisco Webex.

Uitgave 1. Expressway-E is geen Trust certificaatautoriteit (CA) die het Cisco Webex-certificaat heeft ondertekend

De Cisco Webex-server die in directe communicatie met de snelweg-E staat, wordt een L2SIP-server genoemd. Deze L2SIP-server moet door een intermediaire server met een algemene naam van **Hydrant SSL ICA G2** worden ondertekend. De intermediair is ondertekend door een basiscertificeringsinstantie die een gezamenlijke naam van **QuoVadis Root CA 2 heeft** zoals in de afbeelding wordt getoond.

> **Opmerking:** Dit kan veranderen.



De eerste stap om dit verkeer vanuit het diagnostische perspectief van de snelweg te analyseren is naar **TCP-verbinding** te zoeken. Nadat u **TCP-verbinding hebt** gezocht, zult u de **DST-port=5062** waarde zoeken. Nadat u het gebied in de logbestanden hebt geïdentificeerd waar deze verbinding is gepoogd en ingesteld, kunt u vervolgens de TLS Handshake zoeken, die over het algemeen wordt aangegeven door de logitems die Handshake in uitvoering aangeven.

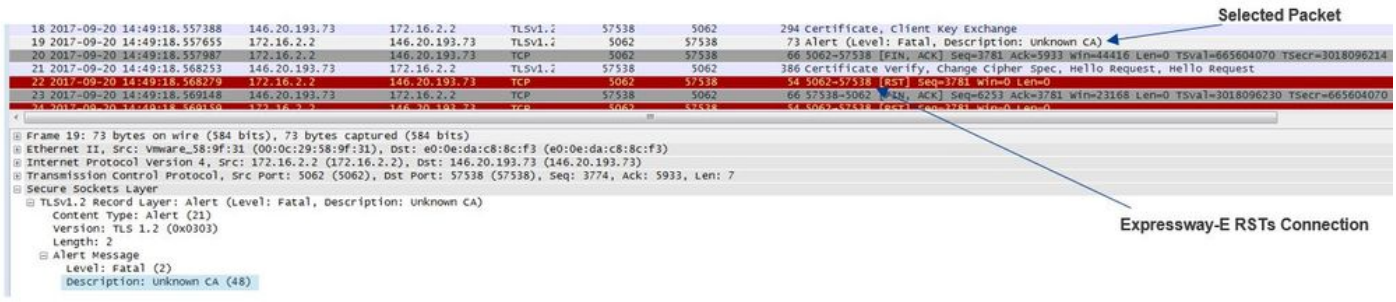
```
2017-09-20T10:49:18.427-04:00 amer-expressway01 tvcs: UTCTime="2017-09-20 14:49:18,426"
Module="developer.ssl" Level="INFO" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(1974)"
Method="::ttssl_continueHandshake" Thread="0x7f29ddefa700":  Detail="Handshake in progress"
Reason="want read/write"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

Als de Expressway-E de Cisco Webex getekende certificaten niet vertrouwt, kunt u verwachten dat de Expressway-E het certificaat onmiddellijk na voltooiing van de handdruk kan verwerpen. Dit kan in het logbestand Expressway-E worden gevonden in deze logitems:

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

De foutmelding Expressway kan iets misleiden omdat deze verwijst naar een zelf-ondertekend

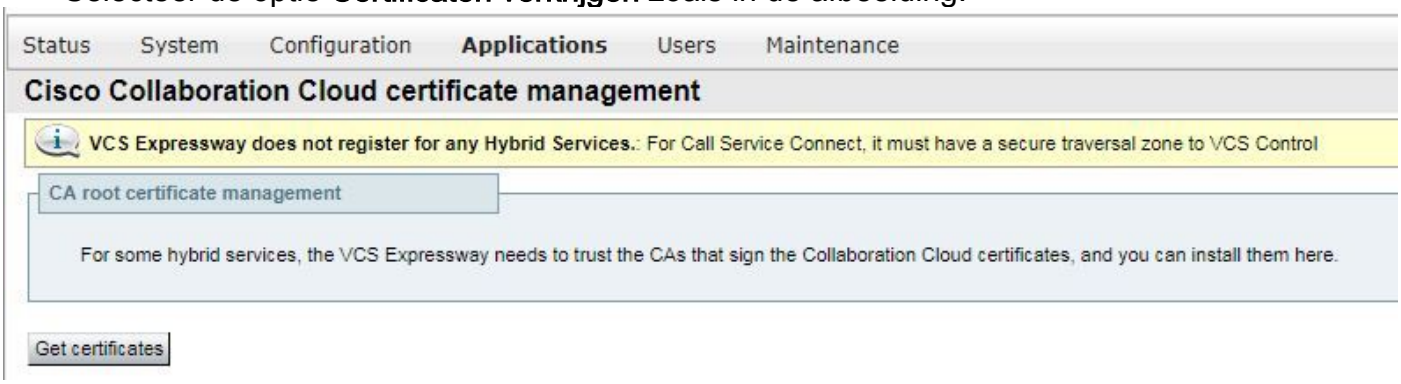
certificaat in de certificeringsketen. Wireshark laat je de uitwisseling nader bekijken. Vanuit een perspectief van de analyse van de pakketvastlegging van Wireshark kunt u duidelijk zien dat wanneer de Webex-omgeving zijn certificaat presenteert, expressway zich omdraait en met een certificaat met een Onbekende CA-fout zoals in de afbeelding wordt weergegeven.



Oplossing:

Om deze situatie op te lossen, moet u ervoor zorgen dat de Expressway-E de Cisco Webex-certificeringsinstanties vertrouwt. Terwijl u deze certificaten eenvoudig uit een Wireshark spoor kunt halen en ze naar de Trusted CA certificatenwinkel op de Expressway kunt uploaden, biedt de Expressway een eenvoudiger methode:

- Inloggen bij de sneltoets
- Navigatie in naar **toepassingen > Cloud certificaatbeheer**
- Selecteer de optie **Certificaten verkrijgen** zoals in de afbeelding.



Op dit punt worden de Cisco Webex-certificeringsinstanties geüpload naar de Express-E Trusted CA-winkel **(Onderhoud > Security > Trusted CA-certificaat)**.

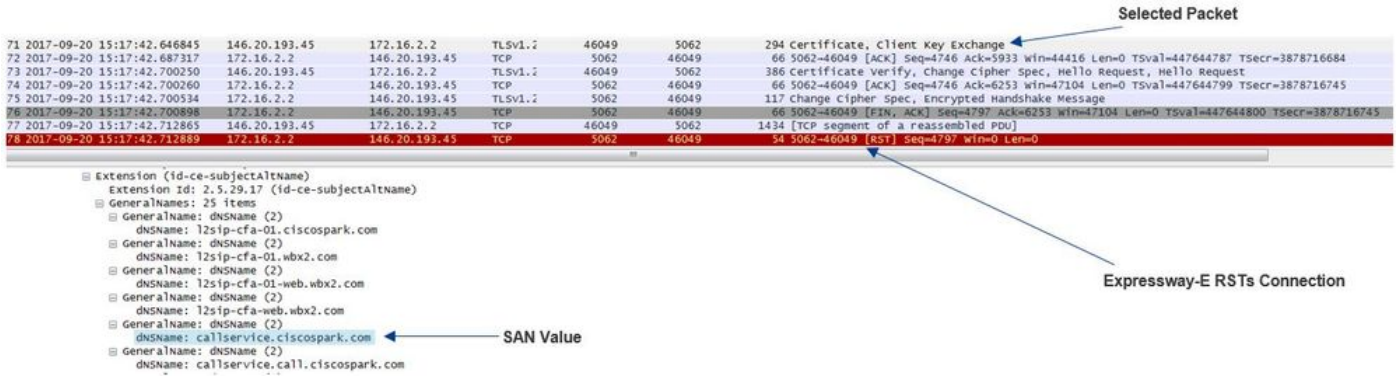
Probleem 2. Onjuiste naam voor TLS Onderwerp Controleer naam op Expressway-E Cisco Webex hybride DNS-zone

Als onderdeel van de wederzijdse TLS-handdruk maakt de hybride Call Service Connect gebruik van TLS Verificatie. Dit betekent dat, naast het vertrouwen op de Cisco Webex CA certificaten, de Expressway het certificaat controleert door het veld Onderwerp Alternate Name (SAN) van het certificaat te controleren dat wordt aangeboden om er zeker van te zijn dat de waarde zoals **callservice.ciscospark.com** aanwezig is. Als deze waarde niet aanwezig is, mislukt de inkomende vraag.

In dit specifieke scenario, stelt de Cisco Webex server zijn certificaat aan de Expressway-E voor. Het certificaat heeft 25 verschillende SAN's. Neem het geval in waar de Expressway-E het certificaat voor de callservice.ciscospark.com SAN controleert maar dat niet vindt. Als aan deze voorwaarde is voldaan, kan je een fout zien die hierop lijkt in de diagnostische houtkap:

```
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"
```

Als u Wireshark gebruikt om deze certificaathanddruk te analyseren, kunt u vinden dat nadat Cisco Webex zijn certificaat presenteert, de Expressway RSTs de verbinding kort na zoals in de afbeelding wordt weergegeven.



Om de configuratie van deze waarde te bevestigen, kunt u naar de Webex Hybrid DNS Zone gaan die voor de oplossing is geconfigureerd. Als u de Express-E-configuratie hebt, kunt u naar het gedeelte Zone-configuratie zoeken om te bepalen hoe het TLS de onderwerpregel heeft geconfigureerd. Let er voor xConfiguration op dat de zones worden besteld met Zone 1 als eerste. Hier volgt een xConfiguration van de problematische omgeving die hierboven wordt geanalyseerd.

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

Zoals u in het voorbeeld kunt zien TLS Controleer de Onderwerp Naam is ingesteld op **calllservice.ciscospark.com** in plaats van **callservice.ciscospark.com**. (noteer het extra "l").

Oplossing:

Om dit probleem op te lossen, moet de TLS verify-naam worden gewijzigd:

- Inloggen bij de sneltoets
- Navigeren in **configuratie > Zones > Zones**
- Selecteer **Webex Hybride services DNS-zone**
- Stel het **TLS**-type **in** op **CallService.ciscospark.com**
- Selecteer **Opslaan**

Opmerking: Zie de basis voor basisloginggedrag. In deze sectie wordt de snelweg weergegeven die certificatie uitvoert en wordt de Webex Hybrid DNS Zone in kaart gebracht.

Opmerking: Vanaf expresswegcode x12.5 en later is er een nieuwe "Webex"-zone vrijgegeven. Deze Webex-zone vult de configuratie van de zone in die nodig is voor communicatie naar Webex. Dit betekent dat u niet langer de TLS Onderwerp Verificatiemodus hoeft in te stellen en TLS Controleer Onderwerp Naam. Voor vereenvoudiging van de configuratie is het aanbevolen om de Webex-zone te benutten als u

x12.5 of hoger van de expressway-code gebruikt.

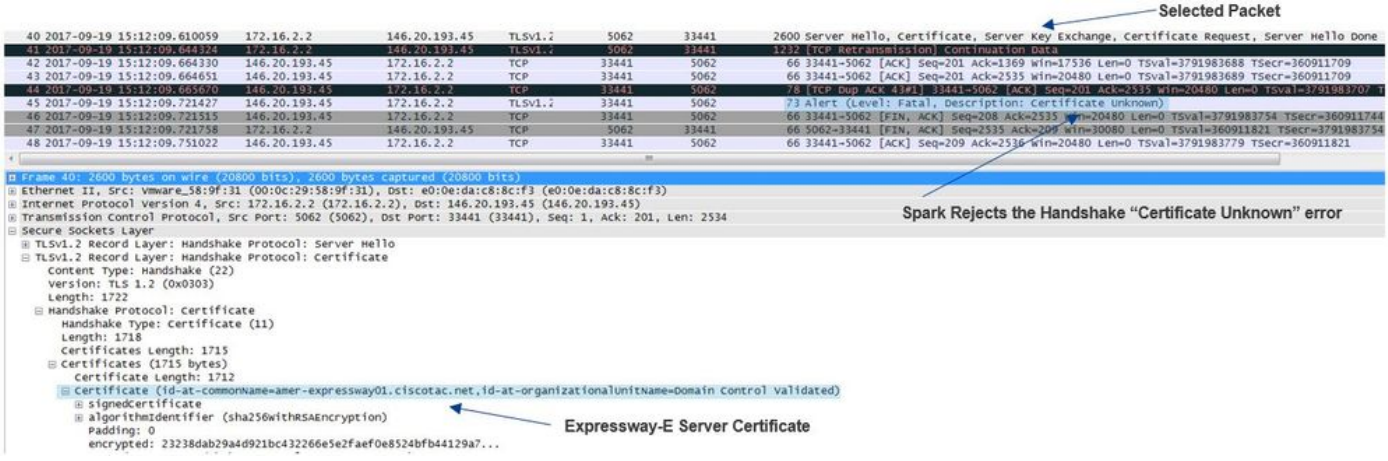
Vraag 3. Expressway-E stuurt geen volledige certificaatketen naar Cisco Webex

Als deel van de wederzijdse lenshanddruk, moet Cisco Webex het certificaat van de Uitdrukkracht-E vertrouwen. Cisco Webex heeft een volledige lijst van openbare CA's waarop het vertrouwen heeft. Meestal is een TLS-handdruk geslaagd wanneer uw sneltoets-E certificaat is ondertekend door een openbaar CA dat door Cisco Webex wordt ondersteund. Door het ontwerp stuurt de Expressway-E alleen het certificaat via een TLS-handdruk, ondanks dat het is ondertekend door een openbare CA. Om de volledige keten van certificaten (wortel en tussenproduct) te verzenden, moeten deze certificaten worden toegevoegd aan de Trusted CA-certificaatwinkel op de Expressway-E zelf.

Als aan deze voorwaarde niet is voldaan, verwerpt Cisco Webex het certificaat Expressway-E. Wanneer u een voorwaarde problemen oplost die dit probleem aanpast, kunt u de diagnostische loglogs en de voump van de Expressway-E gebruiken. Wanneer je de diagnostische logs van Expressway-E analyseert, zie je een fout die hier lijkt:

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

Als je dit analyseert vanuit een Wireshark perspectief, zie je dat de Expressway-E zijn certificaat presenteert. Als u het pakket uitbreidt, kunt u zien dat alleen het servercertificaat wordt verzonden. Cisco Webex wijst deze TLS-handdruk vervolgens af met een Onbekend CA-foutbericht zoals in de afbeelding.



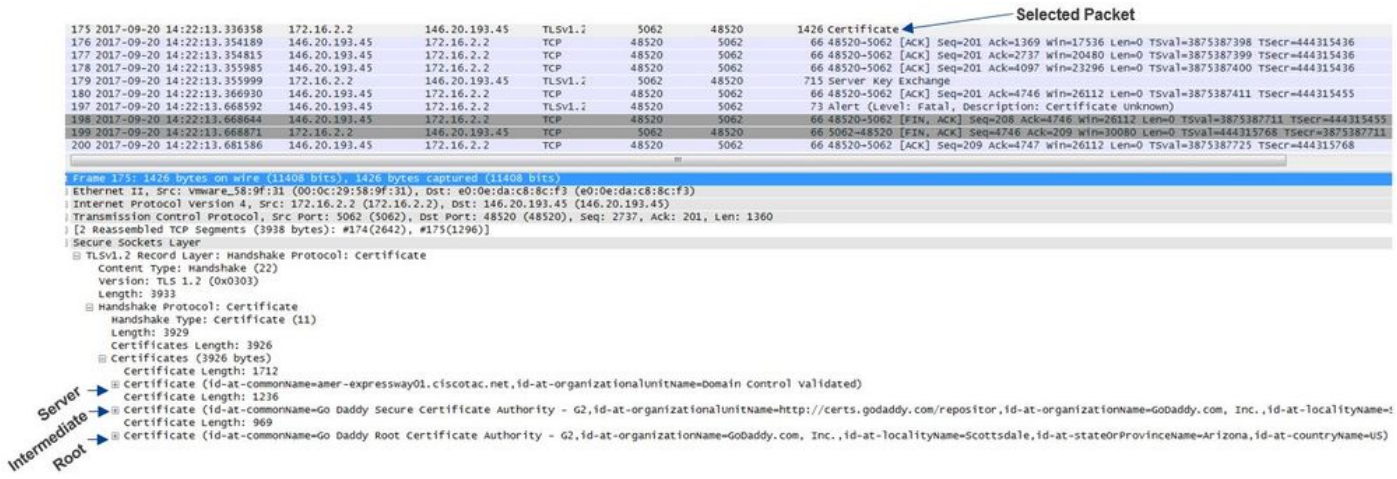
Oplossing:

Om de kwestie in dit scenario aan te pakken moet u de intermediaire en de wortel CA's uploaden die bij de ondertekening van het certificaat van Expressway-E aan de Trusted CA certificslag

betrokken zijn:

Stap 1. Meld u aan bij de sneltoets.
Stap 2. Navigeer naar **onderhoud > Beveiliging > Vertrouwd CA-certificaat**.
Stap 3. Selecteer **Bestand** onder het menu Upload in de buurt van de onderkant van de UI.
Stap 4. Kies het CA-certificaat dat betrokken was bij de ondertekening van de snelweg-E.
Stap 5. Selecteer **CA-certificaat toevoegen**.
Stap 6. Herhaal stappen voor alle CA-certificaten die betrokken zijn bij de ondertekening van het Expressway-E-certificaat (Intermediate, Root).
Stap 7. Selecteer **CA-certificaat toevoegen**.

Nadat dit proces is voltooid, ziet u dat de volledige keten van certificaten betrokken bij het ondertekenen van het Expressway-E server certificaat dat in de key exchange is opgenomen. Hier is een voorbeeld van wat je zou zien als je een pakketvastlegging met Wireshark analyseert.



4. Firewall beëindigt wederzijdse TLS-handdruk

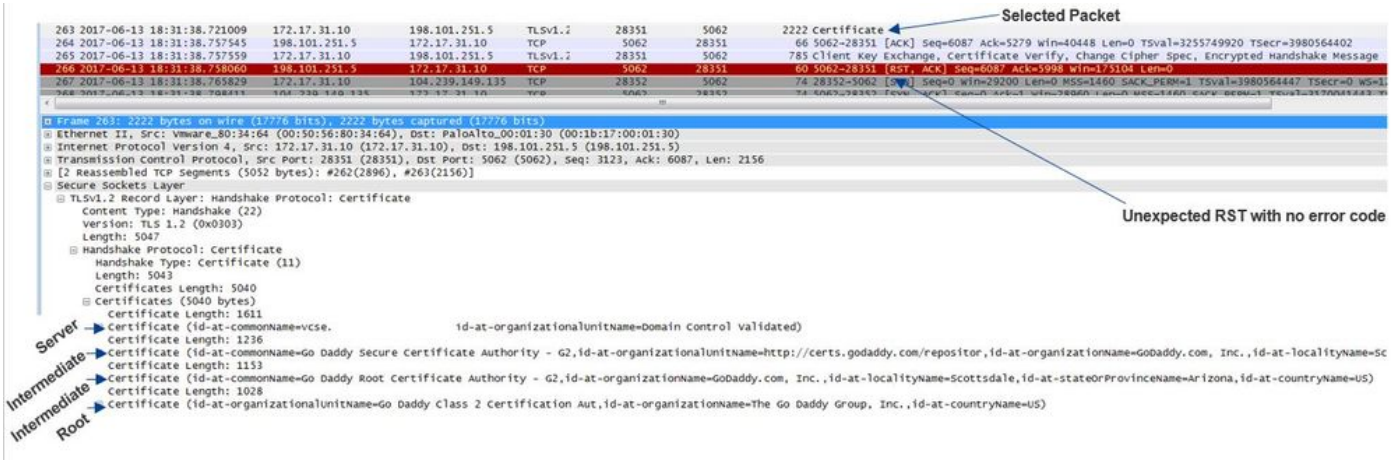
De oplossing van de Uitdrukking interfaces met een firewall. Vaak loopt de inline firewall voor de oplossing één of ander type van toepassing laaginspectie. Vaak met de oplossing van de Uitdrukbaan, wanneer de firewall de controle van de toepassingslaag in werking stelt, zien de beheerders ongewenste resultaten. Dit specifieke probleem helpt u te identificeren wanneer de controle van de toepassingslaag van een firewall de verbinding abrupt heeft verstoord.

Met het gebruik van de diagnostische logbestanden van de Expressway, kunt u de poging tot wederzijdse TLS handdruk zoeken. Deze handdruk, zoals eerder vermeld, zou kort moeten komen nadat de TCP-verbinding via poort 5062 tot stand is gebracht. In dit scenario, wanneer de firewall de verbinding onderbreekt, zie je deze fouten in de diagnostische houtkap.

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

Vanuit een perspectief van de pakketvastlegging, zult u zien dat de Expressway-E zijn certificaat aan Cisco Webex presenteert. U ziet een TCP RST vanuit de richting van Cisco Webex komen

zoals in de afbeelding.



Op het eerste gezicht denk je misschien dat er iets mis is met het Expressway-E-certificaat. Om dit probleem op te lossen, moet u eerst de antwoorden op deze vragen bepalen:

- Is de snelweg-E ondertekend door een publiek CA dat Cisco Webex vertrouwt?
- Is het sneltoets-E certificaat en alle certificaten betrokken bij de ondertekening van het snelwegcertificaat E handmatig geüpload naar de Cisco Webex Control Hub (https://admin.ciscospark.com)?

In deze specifieke voorwaarde was de oplossing niet om de WebEx Control Hub van Cisco te gebruiken om de certificaten van de Uitdrukking te beheren. Dit betekent dat het sneltoets-E certificaat moet worden ondertekend door een openbaar CA dat Cisco Webex vertrouwt. Door op het certificaatpakket in de WinShark-opname te selecteren (zoals hierboven wordt geïllustreerd), kunt u zien dat het certificaat door een openbare CA is ondertekend en dat de volledige keten naar Cisco Webex is verzonden. Daarom moet de afgifte niet gerelateerd zijn aan het E-certificaat.

Als u op dit punt nog meer isolatie nodig hebt, kunt u een pakketopname vanuit de externe interface van de firewall uitvoeren. Het gebrek aan SSL-fout in het diagnostische logbestand is echter een belangrijk gegeven. Als u zich hierboven herinnert (Vraag 3.), als Cisco Webex het Expressway-E certificaat niet vertrouwt, moet u een of ander type SSL zien dat de verbinding verbroken maakt. In deze conditie was er geen SSL-fout beschikbaar.

> **Opmerking:** Als u een pakketvastlegging van de firewall buiten interface zou krijgen, zou u geen TCP RST zien binnenkomen vanuit de Cisco Webex-omgeving.

Oplossing

Voor deze specifieke oplossing moet u als partner of klant vertrouwen op uw veiligheidsteam. Het team moet onderzoeken of ze een soort van toepassing-laaginspectie gebruiken voor de expressievloeistof-oplossing en als ze dat zijn, moet dit worden uitgeschakeld. Bijlage 4 van de **VCS Control and Expressway Deployment Guide** legt uit waarom klanten deze functie aangeraden zijn.

Vak 5. Expressway-E wordt ondertekend door openbare CA, maar Cisco Webex Control Hub heeft alternatieve certificaten geladen

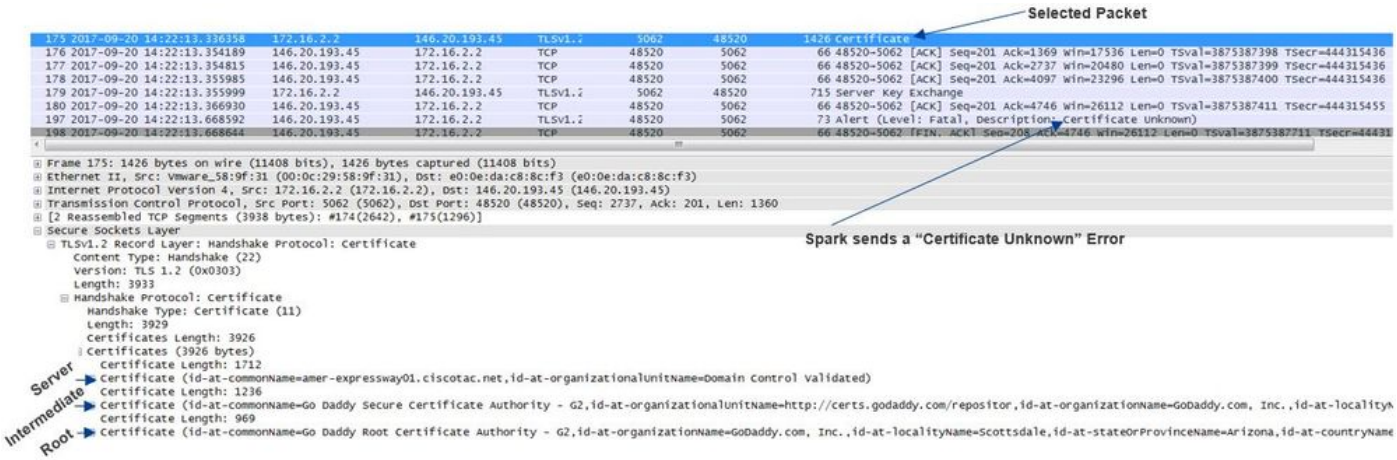
Deze specifieke voorwaarde kan vaak voorkomen wanneer u de oplossing van de Uitdrukking vanuit het niets uitwerkte en u hebt niet het certificaat van de Uitdrukking-E aanvankelijk door een

openbaar CA ondertekend. Wat in dit scenario gebeurt is dat u het E-servercertificaat (dat intern is getekend) uploaden naar de Cisco Webex Control Hub zodat u de TLS-onderhandeling met succes kunt voltooien. Daarna krijgt u het Expressway-E-certificaat dat door een openbare CA is ondertekend, maar u vergeet het servercertificaat uit de Cisco Webex Control Hub te verwijderen. Het is belangrijk om te weten dat wanneer een certificaat wordt geüpload naar de Cisco Webex Control Hub, dat certificaat voorrang heeft op welk certificaat en de expressway tijdens de TLS-handdruk toont.

Vanuit een diagnostisch blogperspectief van Expressway-E kan deze kwestie op de houtkap lijken die wordt bereikt wanneer Cisco Webex het expressway-E-certificaat niet vertrouwt — bijvoorbeeld het geval van de Expressway-E die zijn volledige keten niet stuurt of het expressway-E-certificaat dat niet wordt ondertekend door een openbaar CA dat Cisco Webex vertrouwt. Hieronder zie je een voorbeeld van wat je kunt verwachten in de expressway-E logging tijdens de TLS handdruk:

```
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"
```

Bekijk dit vanuit het perspectief van Wireshark u hier kunt zien dat de Expressway-E het certificaat presenteert in lijnitem 175. Een paar lijnpunten later wijst de Cisco Webex-omgeving het certificaat af met een onbekende fout van het certificaat zoals in de afbeelding.



Als u het certificaatpakket selecteert dat de sneltoets indrukt-E verstuurt, kunt u de certificaatinformatie uitbreiden om te bepalen of de sneltoets-E

1. is ondertekend door een publiek CA dat Cisco Webex vertrouwt, en

2. haar gehele keten omvat die bij de ondertekening betrokken is .

In deze situatie is aan beide voorwaarden voldaan. Dit suggereert dat er niets mis is met het

Expressway-E certificaat.

Oplossing

Stap 1. Meld u aan bij de Cisco Webex Control Hub.
Stap 2. Selecteer **Services** in het linker deelvenster.

Stap 3. Kies **Instellingen** onder de hybride gesprekskaart.

Stap 4. Scrolt naar het gedeelte Call Service Connect en kijk onder de Certificaten voor Versleutelde SIP-oproepen om te zien of er ongewenste certificaten zijn opgenomen. Als dit het geval is, klikt u op het pictogram afval naast het certificaat.

stap 5. Selecteer **Verwijderen**.

> **Opmerking:** Het is belangrijk dat de analyse wordt uitgevoerd en dat wordt vastgesteld dat de klant niet de certificaten gebruikt die aan de Webex Control Hub zijn geüpload voordat deze worden verwijderd.

Voor meer informatie over het uploaden van uw expressway-E certificaat in de Cisco Webex Control Hub, controleer dit gedeelte van de Hybrid Call Deployment Guide.

Uitgave 6. Expressway is geen Toewijzing van inkomende oproep aan Cisco Webex Hybrid DNS Zone

De functie Inbound TLS mapping werkt in combinatie met de TLS verify-naam, die beide op de hybride Call DNS-zone zijn ingesteld. Dit scenario schetst kwesties en uitdagingen die vóór x12.5 met de snelweg werden waargenomen. In x12 en later werd een nieuw soort zone geïmplementeerd, de "Webex"-zone. Deze zone vult alle benodigde configuratie voor de integratie met Webex voor. Als u x12.5 uitvoert en Webex Hybrid Call implementeert, is het raadzaam het **Webex** Zone-type te gebruiken zodat het domein van de Hybrid Call Services (callservice.webex.com) voor u automatisch wordt geconfigureerd. Deze waarde komt overeen met de Onderwerp Alternate Name van het Webex certificaat dat tijdens de Mutual TLS handshake wordt aangeboden en dat de verbinding en inkomende mapping naar de expressway in staat stelt om te slagen.

Als u een codeversie onder x12.5 gebruikt of de Webex-zone niet gebruikt, wilt u de onderstaande uitleg gebruiken die aantoont hoe u problemen kunt identificeren en corrigeren waarbij de expressway de inkomende aanroep naar de Webex hybride DNS-zone niet in kaart brengt.

Deze optie is in drie stappen verdeeld:

1. Expressway-E accepteert het Cisco Webex-certificaat.
2. Expressway-E inspecteert het Cisco Webex-certificaat om te bepalen of er een Onderwerp Alternatieve naam is die overeenkomt met de TLS verify-onderwerpnaam: callservice.ciscospark.com.
3. Expressway-E brengt de inkomende verbinding door de Cisco Webex Hybrid DNS Zone in kaart.

Indien de echtheidscontrole geen succes heeft, betekent dit dat de certificatie niet is geslaagd. De oproep gaat in de Standaardzone in en wordt routeerd volgens de zoekregels die voor business-

to-business scenario's zijn voorzien, als business-to-business is ingesteld op Expressway-E.

Net zoals de andere scenario's, moet u zowel de diagnostische houtkap als pakketvastlegging gebruiken om te bepalen hoe deze fout eruit ziet, dan gebruik de pakketvastlegging om te zien welke kant de RST stuurt. Hier is een voorbeeld van de TCP verbinding die wordt geprobeerd, dan het vestigen.

```
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"
```

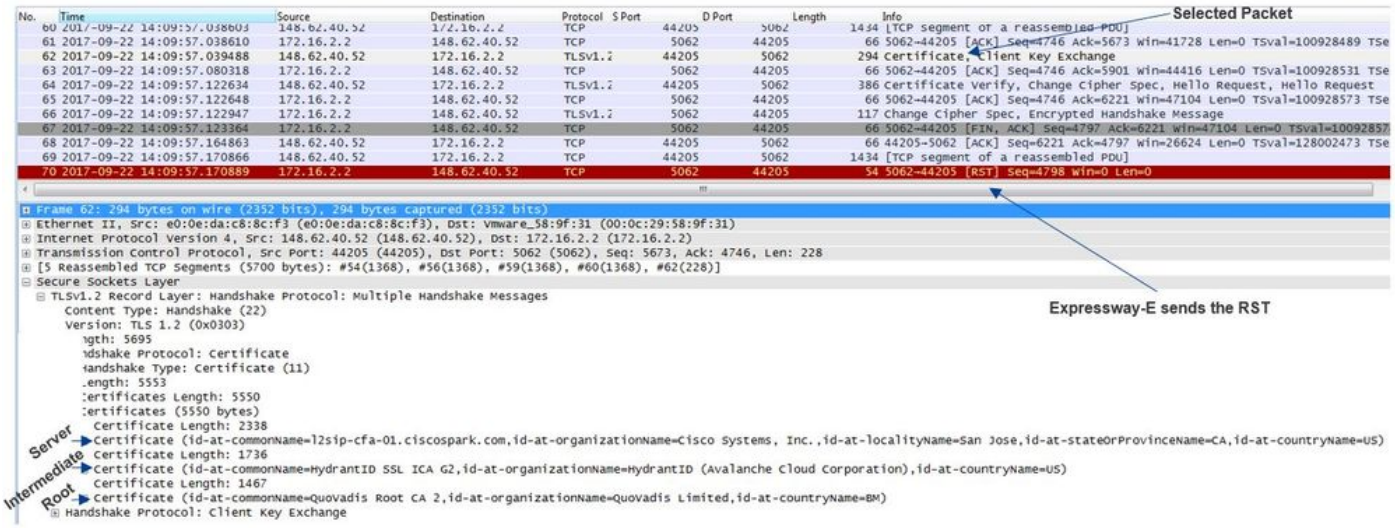
Nu de TCP verbinding tot stand is gebracht, kan de TLS Handshake worden uitgevoerd. Je kunt zien kort nadat de handdruk begint, het komt snel uit.

```
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"
```

Kijk naar deze situatie vanuit het perspectief van het glb, je kan een beter gevoel krijgen

- wie de RST stuurt, en
- welke certificaten worden afgegeven om na te gaan of zij juist zijn .

Wanneer je deze specifieke opname analyseert, kan je zien dat de Expressway-E de RST stuurt. Wanneer u het Cisco Webex-certificaat bekijkt dat wordt doorgegeven, kunt u zien dat het de volledige keten verstuurt. Daarnaast kunt u concluderen dat op basis van de foutmelding in het diagnostische logbestand, u het scenario kunt uitsluiten waar de Expressway-E de Cisco Webex openbare CA's niet vertrouwt. Anders ziet u een fout zoals "**zichzelf getekend certificaat in certificeringsketen**". U kunt in de pakketgegevens graven zoals in de afbeelding.



Door op het Webex Server certificaat te klikken en het uit te breiden om de Onderwerp Alternate Names (dnsName) te zien kunt u verifiëren om ervoor te zorgen dat het **callservice.ciscospark.com** vermeld heeft.

Navigeren in naar **Wireshark: certificaatnummer > Verlenging > Algemene namen > Algemene naam > Naam: callservice.ciscospark.com**

Dit bevestigt volledig dat het Webex-certificaat er prima uitziet.

U kunt nu bevestigen dat het TLS Controleer Onderwerp Naam correct is. Zoals vermeld kunt u, als u de xConfiguration hebt, naar het gedeelte Zone-configuratie zoeken om te bepalen hoe het TLS verify-onderwerpnaam is geconfigureerd. Een ding om op te merken over de xConfiguration is dat de zones besteld worden met Zone 1 de eerste is het creëren. Hier volgt een xConfiguration van de problematische omgeving die hierboven wordt geanalyseerd. Het is duidelijk dat er niets mis is met de TLS verify-naam.

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

Het volgende dat moet worden onderzocht is het **TLS verify-kaart**. Dit bevestigt als u de TLS-verbinding naar de Webex hybride DNS-zone correct in kaart brengt. De xConfiguration is bedoeld voor de analyse van dit probleem. In de xConfiguration wordt **TLS verify-**kaart **DNS ZIP-TLS** genoemd**, verify-classificatie**. Zoals u in dit voorbeeld kunt zien wordt de waarde op Uit ingesteld.

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

Gezien het feit dat deze waarde op Off is ingesteld, betekent dit dat de VCS verhinderd wordt om inkomende TLS-verbindingen naar deze zone in kaart te brengen. De oproep gaat dus naar de Default Zone en wordt gecontroleerd en routeerd volgens de zoekregels die voor business-to-business-scenario's zijn voorzien, indien business-to-business is ingesteld op Expressway-E..

Oplossing

Om dit aan te pakken moet u de TLS om inkomende mapping op de Hybrid Call DNS Zone op Aan te zetten instellen. Hier zijn de stappen om dat te voltooien.

1. Inloggen bij de sneltoets
2. Navigeren in **configuratie > Zones > Zones**
3. Selecteer **Hybride Call DNS-zone**
4. Kies **op TLS voor** controle van **inkomende mapping**
5. Selecteer **Opslaan**

> **Opmerking:** Zie het voor uitgangswaarde houtkapgedrag. In deze sectie wordt de snelweg weergegeven die certificatie uitvoert en wordt de Webex Hybrid DNS Zone in kaart gebracht.

Uitgave 7. Sneltoets-E gebruikt standaard zelfgetekend certificaat

Bij sommige nieuwe implementaties van Hybrid Call Service Connect wordt het ondertekenen van het Expressway-E-certificaat over het hoofd gezien of wordt aangenomen dat het standaard server-certificaat kan worden gebruikt. Sommige mensen denken dat dit mogelijk is omdat de Cisco Webex Control Hub u een aangepast certificaat in het portal laat laden. (**Services >**

Instellingen (onder Hybride Call Card) > Upload (onder Certificaten voor versleutelde oproepen)

Als u aandachtig kijkt naar de formulering van de certificaten voor versleutelde SIP-oproepen, ziet u dit: 'Gebruik certificaten die worden geleverd vanuit de standaard Cisco Collaboration-vertrouwenslijst of uploaden uw eigen certificaten. Als u uw eigen naam gebruikt, zorg er dan voor dat de hostnamen op een geverifieerd domein staan.' Het sleutelstuk in die verklaring is "Controleer of hostname op een geverifieerd domein staat."

Wanneer u een probleem oplossen dat met deze voorwaarde overeenkomt, houd in gedachten dat het symptoom van de richting van de vraag afhankelijk zal zijn. Als de oproep afkomstig is van een mobiele telefoon, kunt u verwachten dat de Cisco Webex-app niet zal bellen. Als je de oproep uit de zoekgeschiedenis van snelwegen trachtte op te sporen, zou je ook zien dat de oproep tot de expressway-E zou leiden en daar zou stoppen. Als de oproep afkomstig is van een Cisco Webex-app en bestemd is voor het gebouw, belt de telefoon niet op het kantoor. In dat geval zou de veteranengeschiedenis van de snelweg-E en de snelweg-C niets laten zien.

In dit specifieke scenario kwam de oproep van een telefoon in het bedrijf. Met behulp van de Expressway-E Search History kunt u bepalen dat de oproep tot de server is gemaakt. Op dit punt kun je in de diagnostische houtkap duiken om te bepalen wat er gebeurde. Om deze analyse te beginnen, kijk eerst of een TCP verbinding werd geprobeerd en gevestigd over haven 5062. Door in de diagnostische logbestanden van Expressway-E te zoeken naar "TCP-verbinding" en het doorzoeken van de regeloptie met de tag "Dst-port=5062", kunt u bepalen of de verbinding tot stand is gebracht.

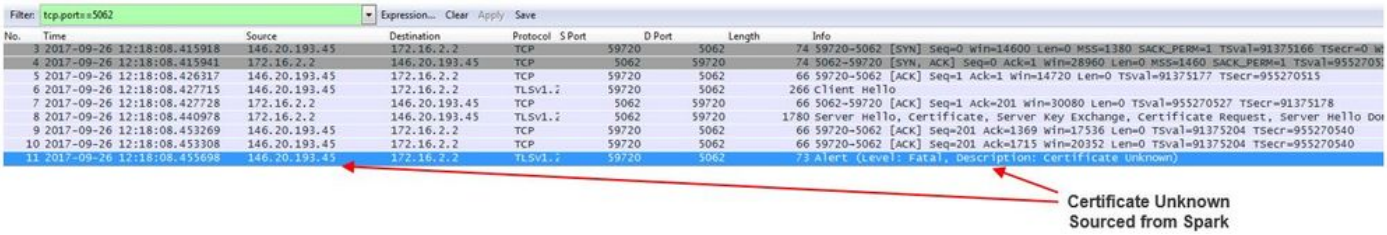
```
2017-09-26T08:18:08.428-04:00 amer-expressway01 tvcs: UTCTime="2017-09-26 12:18:08,426"
Module="network.tcp" Level="DEBUG":  Src-ip="146.20.193.45" Src-port="59720" Dst-ip="172.16.2.2"
Dst-port="5062" Detail="TCP Connecting"
2017-09-26T08:18:08.428-04:00 amer-expressway01 tvcs: UTCTime="2017-09-26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

Nu u de TCP-verbinding hebt bevestigd, kunt u de wederzijdse TLS-handdruk analyseren die direct daarna plaatsvindt. Zoals u in het hoofdstuk kunt zien, faalt de handdruk en is het certificaat onbekend (Detail="sslv3 alarmcertificaat onbekend")

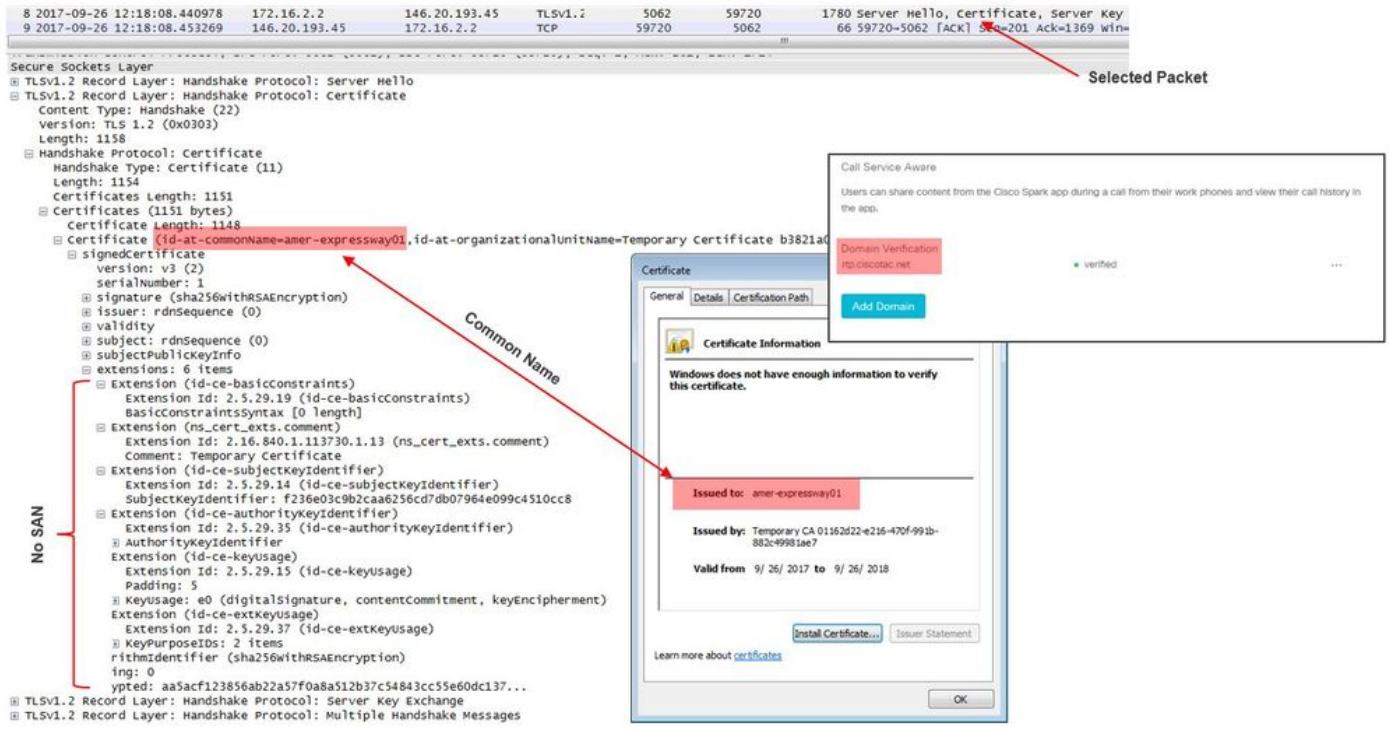
```
2017-09-26T08:18:08.441-04:00 amer-expressway01 tvcs: UTCTime="2017-09-26 12:18:08,441"
Module="developer.ssl" Level="INFO" CodeLocation="ppcmains/ssl/ttssl/ttssl_openssl.cpp(1974)"
Method="::ttssl_continueHandshake" Thread="0x7f930adab700":  Detail="Handshake in progress"
Reason="want read/write"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

Neem een kijkje bij de pakketvastlegging die bij de diagnostische vastlegging Expressway-E is meegeleverd, kunt u zien dat de onbekende fout van het Certificaat afkomstig is van de richting van Cisco Webex zoals in de afbeelding.



Als u het certificaat van de Standaard Server van de Expressway-E inspecteert, kunt u zien dat de 'Common Name' en 'Onderwerp Alternate Names' niet het 'Verified Domain' **(rtp.ciscotac.net)** bevatten. U hebt dan bewijs over wat de oorzaak van dit probleem is zoals in de afbeelding wordt getoond.



Op dit punt, bepaalde u dat het de Server certificaat van de Uitdrukking-E moet worden ondertekend door of een Openbaar CA of een Interne CA.

Oplossing

U hebt twee opties om dit probleem op te lossen:

1. Zorg ervoor dat het E-certificaat wordt ondertekend door een publiek CA dat Cisco Webex vertrouwt.
   Log in op de sneltoets.Navigeer naar **Onderhoud > Beveiliging > Server certificaat**.Selecteer **CSR genereren**.Voer de gewenste certificaatinformatie in en controleer of het veld **Aanvullende alternatieve namen** het **geverifieerde domein** bevat dat in de Webex Control Hub is opgenomen.Klik op **Generate CSR**.Laat de CSR aan een derde partij openbare CA ter beschikking voor ondertekening.Navigeer bij terugkeer van het certificaat naar **Onderhoud > Security > Server certificaten**.**Selecteer** in het gedeelte **Upload New Certificate** naast **het bestand van het servercertificaat**, selecteer **Bestand kiezen** en selecteer het **ondertekende**

certificaat.Selecteer **de gegevens van het uploadcertificaat**.Navigeer naar **Onderhoud > Beveiliging > Vertrouwd CA-certificaat**.Selecteer in het gedeelte **Upload** naast **Selecteer het bestand met vertrouwde CA-certificaten** en selecteer **Bestand kiezen**.Selecteer alle basis- en intermediaire CA-certificaten die door de openbare CA zijn geleverd.Selecteer **CA-certificaat toevoegen**.Start de snelweg opnieuw.

2. Zorg dat het sneltoets-E certificaat wordt ondertekend door een interne CA en uploaden vervolgens de interne CA en Expressway-E naar de Cisco Webex Control Hub. Inloggen in de sneltoetsNavigeer naar **Onderhoud > Beveiliging > Server certificaat**.Selecteer **Generate CSR**Voer de gewenste certificaatinformatie in die garandeert dat het *veld Aanvullende alternatieve namen* het **geverifieerde domein** in de Webex Control Hub bevatKlik op **Generate CSR**CSR leveren aan een derde partij, publiek CA voor ondertekeningNavigeer bij terugkeer van het certificaat naar *Onderhoud > Security > Server certificatenSelecteer* in het *gedeelte* Upload *New Certificate* naast *het bestand van het servercertificaat*, selecteer **Bestand kiezen** en selecteer het ondertekende certificaatSelecteer **de gegevens van het uploadcertificaat**Navigatie naar **onderhoud > Beveiliging > Vertrouwd CA-certificaat**Selecteer in het gedeelte **Upload** naast **Selecteer het bestand met vertrouwde CA-certificaten** en selecteer **Bestand kiezen**.Selecteer alle basis- en intermediaire CA-certificaten die door de openbare CA zijn geleverd.Selecteer **CA-certificaat toevoegen**.Start de snelweg opnieuw.

2 bis. Upload het interne CA en snelheden-E certificaat naar de Cisco Webex Control Hub

1. Log in op de Cisco Webex Control Hub als beheerder.
2. Selecteer **Services**.
3. Selecteer **Instellingen** onder de knop Hybride gespreksservicekaart.
4. Selecteer **Upload** in **de sectie Certificaten voor versleutelde SIP-oproepen**.
5. Kies de interne CA- en E-certificaten.

Inkomend: Cisco Webex naar locaties

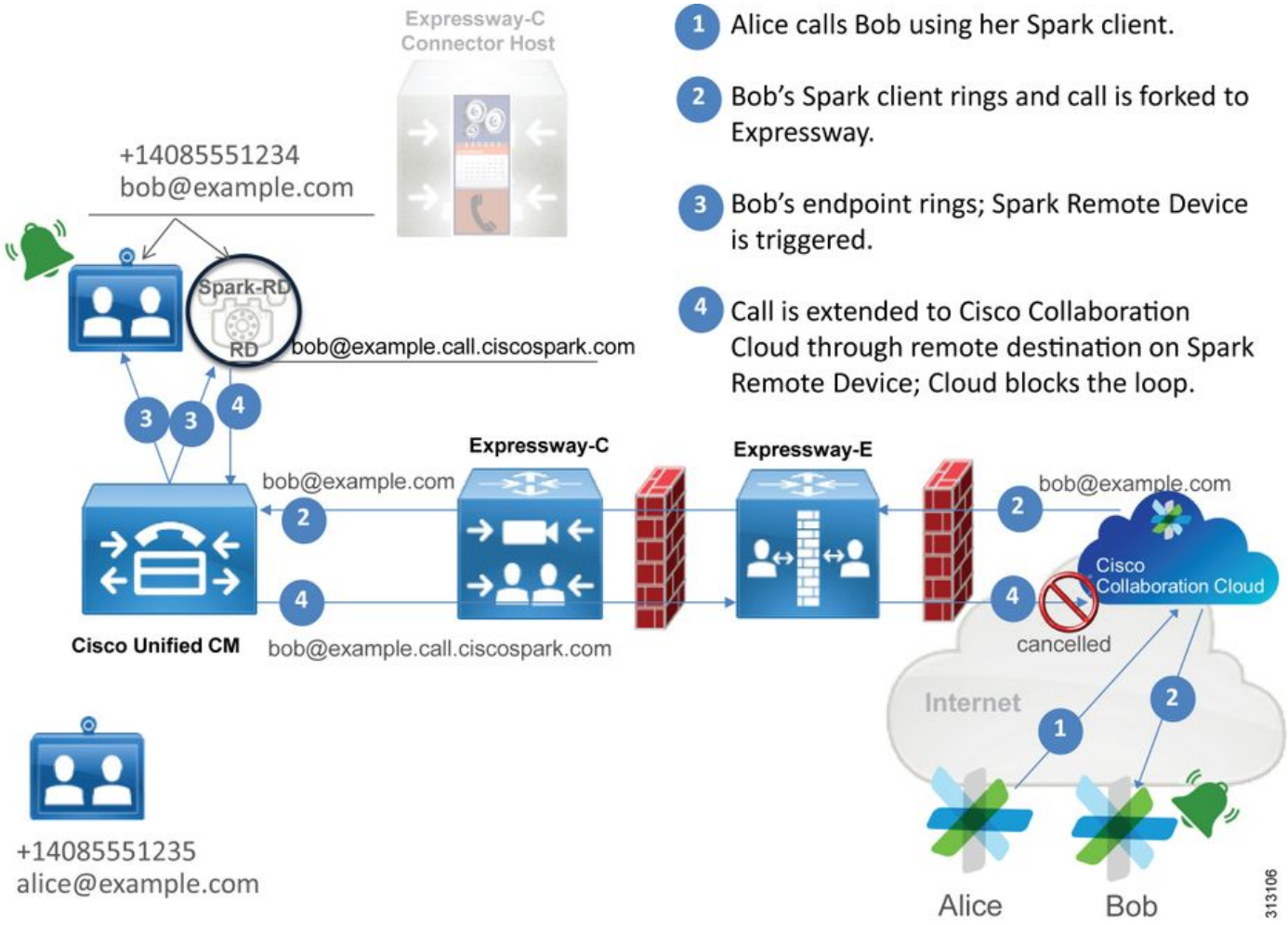
Bijna elke inkomende Cisco Webex naar onbedrijfsmatige mislukking resulteert in hetzelfde gerapporteerde symptoom: "Wanneer ik van mijn Cisco Webex-app naar de app van een andere collega bel, gaat de app van de collega wel maar niet naar de mobiele telefoon." Om dit scenario problemen op te lossen, zult u het behulpzaam vinden om zowel de vraagstroom als de logica te begrijpen die voorkomen wanneer dit type van vraag wordt geplaatst.

Logic-doorloop op hoog niveau

1. De oproep van Cisco Webex-app is gestart
2. De app van de opgeroepen partij
3. De oproep is gericht aan de Cisco Webex-omgeving
4. De Cisco Webex-omgeving moet een DNS-upgrade uitvoeren op basis van de geconfigureerde SIP-bestemming van de klant in de Cisco Webex-controlehub
5. De Cisco Webex-omgeving probeert verbinding te maken met de snelweg via poort 5062
6. De Cisco Webex-omgeving probeert een wederzijdse TLS-handdruk uit te voeren
7. De Cisco Webex-omgeving verstuurt een SIP-verbinding naar de sneltoets, die wordt doorgegeven naar het collaboration-endpoints/IP-telefoon
8. Cisco Webex en de onderneming voltooien de SIP-onderhandeling
9. Cisco Webex en de onderneming beginnen met het verzenden en ontvangen van media.

Call Flow

Navigeer naar **Cisco Webex-app > Cisco Webex-omgeving > Expressway-E > On-Premises Collaboration-endpoint/IP-telefoon** zoals in de afbeelding getoond.



Hier zijn een aantal van de vaak voorkomende problemen waargenomen bij inkomende oproepen van Webex naar de infrastructuur op locatie.

Probleem 1. Cisco Webex kan niet de snelweg-E DNS SRV/hostname oplossen

Wanneer u aan de Cisco Webex nadenkt om aan te bellen stroom te geven, is de eerste logische stap van Cisco Webex hoe u contact opneemt met de expressway. Zoals hierboven vermeld, zal Cisco Webex proberen om verbinding te maken met de sneltoets op het kantoorgebouw door een SRV-raadpleging uit te voeren op basis van de geconfigureerde **SIP-bestemming** die in de pagina **Hybrid Call Service Settings** in de Cisco Webex-controlehub is opgenomen.

Als u probeert deze situatie vanuit een diagnostisch logperspectief van Expressway-E te oplossen, ziet u geen verkeer vanuit Cisco Webex. Als u probeert om TCP te zoeken verbinden, zou u Dst-port=5062 niet zien, noch zou u een volgende MTLS handdruk of SIP Invite van Cisco Webex zien.

Als dit de situatie is, moet u controleren hoe de **SIP-bestemming** is geconfigureerd in de Cisco Webex Control Hub. U kunt ook het **Hybrid Connectivity Test Tool** gebruiken om bij de probleemoplossing te helpen. Het Hybrid Connectivity Test Tool controleert als er een geldig DNS-adres is, als Cisco Webex verbinding kan maken met de poort die in de SRV-raadpleging is teruggekeerd en als de expressway op het bedrijf een geldig certificaat heeft dat Cisco Webex vertrouwt.

1. Inloggen op [de Cisco Webex Control Hub]
2. SelecteerServices
3. Selecteer de instellingslink in **de hybride gesprekskaart**.
4. Controleer in het vak Call Service Connect het domein dat wordt gebruikt voor het openbare SIP SRV-adres in **het** veld SIP-bestemming.
5. Als de record correct is ingevoerd, klikt u op **Test** om te zien of de record geldig is.
6. Zoals hieronder wordt weergegeven, kunt u duidelijk zien dat het publieke domein geen corresponderende SIP SRV record heeft gekoppeld aan de afbeelding.

Selecteer **testresultaten bekijken** en u kunt meer details zien over het mislukken zoals in de afbeelding.

Als een andere benadering, kunt u het SRV record ook opzoeken door nslookup te gebruiken. Hier zijn de opdrachten die u kunt uitvoeren om te controleren of de SIP-bestemming bestaat.

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

Zoals u in het bovenstaande codeponeringsblok kunt zien, is de opdracht nslookup gestart en is de server ingesteld op 8.8.8.8, een openbare Google DNS-server. Ten slotte, stelt u de record types in om naar SRV records te kijken. Op dat punt kunt u dan het volledige SRV-record uitgeven dat u wilt opzoeken. Het nettoresultaat is dat de verzoeken uiteindelijk worden ingetrokken.

Oplossing

1. Configureer een openbaar SIP SRV-adres voor de sneltoets-E op de site die zij gebruiken om openbare domeinnamen te host.
2. Configuratie van een hostname die aan het openbare IP adres van Expressway-E zal

oplossen

3. Configureer de SIP-bestemming om een lijst te maken van het domein dat wordt gebruikt voor het SIP SRV-adres dat in Stap 1 is aangemaakt. Log in op Cisco Webex Control HubSelecteer **Services**Selecteer de koppeling **Instellingen** in de *hybride telefoonkaart*In het gedeelte Call Service Connect specificeert u het domein dat voor het openbare SIP SRV-adres in het veld **SIP-bestemming** wordt gebruikt. Selecteer Opslaan

   Opmerking: Als het SIP SRV-record dat u wilt gebruiken al actief is op het gebied van bedrijfscommunicatie, raden we aan om een subdomein van het bedrijfsdomein te specificeren als het SIP-zoekadres in Cisco Webex Control Hub, en vervolgens een openbaar DNS SRV-record, als volgt:

Service- en -protocol: _sips._tcp.mtls.example.com
Prioriteit: 1
Gewicht: 10
Poortnummer: 5062
Doel: us-expe1.example.com

De bovenstaande aanbeveling is rechtstreeks afkomstig van de Cisco Webex Hybrid Design Guide.

Alternatieve oplossing

Als de klant geen SIP SRV record heeft (en niet van plan is er een te maken), kunnen zij anders een lijst maken van het openbare IP-adres expressway dat wordt aangevuld met ":5062". Door dit te doen, zal de Webex-omgeving geen SRV raadpleging proberen maar rechtstreeks verbinden met de **%Expressway_Pub_IP%:5062**. (Voorbeeld: 64.102.241.236:5062)

1. Configureer de SIP-bestemming die wordt geformatteerd als **%Expressway_Pub_IP%:5062**. *(Voorbeeld: 64.102.241.236:5062)* Log in op Cisco Webex Control HubSelecteer **Services**Selecteer de koppeling **Instellingen** in de *hybride telefoonkaart*Voer in het vak Call Service Connect de **%Expressway_Pub_IP%:5062** in het veld **SIP-bestemming in**. Selecteer Opslaan

Voor meer informatie over het SIP-adres en/of SRV-record die moet worden ingesteld. Raadpleeg het gedeelte Hybrid Call Service Connect voor uw organisatie van de Cisco Webex Hybrid Call Service Deployment Guide of de Cisco Webex Hybrid Design Guide.

Afdeling 2: Socketfalen: Port 5062 is ingesloten in een expresse-ingang

Nadat de DNS-resolutie is voltooid, probeert de Cisco Webex-omgeving om een TCP-verbinding via poort 5062 naar het IP-adres te creëren dat tijdens de DNS-raadpleging is teruggekeerd. Dit IP-adres wordt het openbare IP-adres van de expressway-E. Als de Cisco Webex-omgeving deze TCP-verbinding niet kan opzetten, wordt de oproep naar het gebouw vervolgens mislukt. Het symptoom voor deze specifieke conditie is hetzelfde als bijna elke andere Cisco Webex-inbound-falen: de telefoon in de ruimte niet belt .

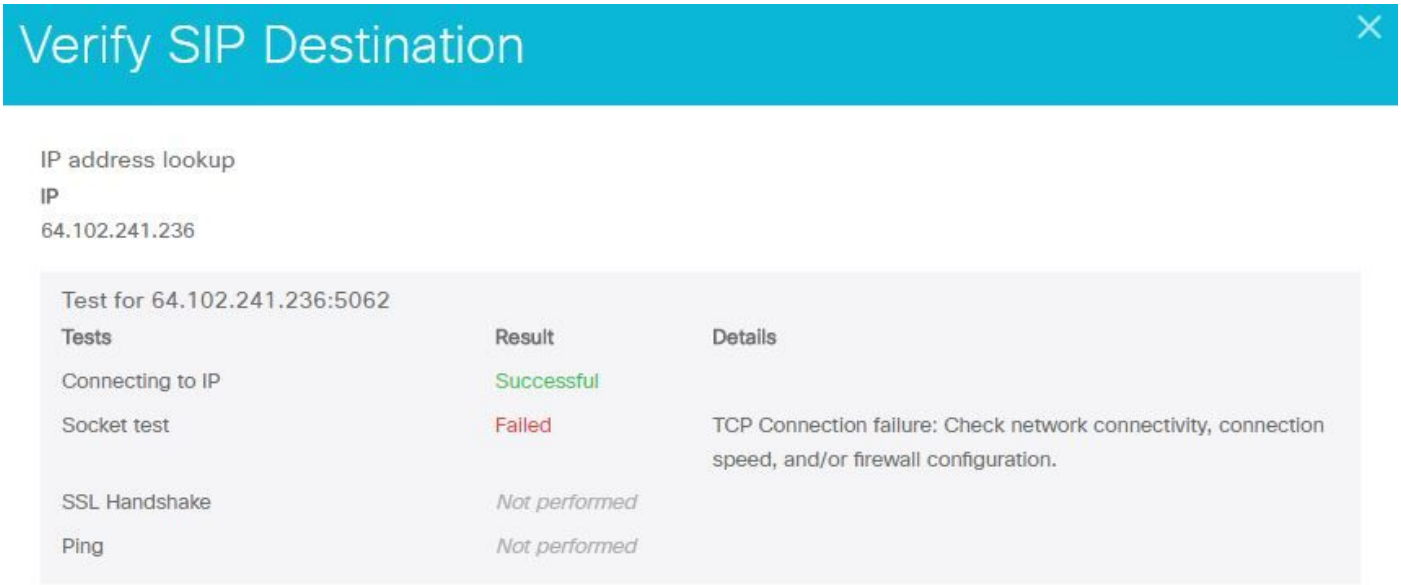
Als u problemen oplossen bij dit probleem met behulp van de diagnostische logbestanden van de snelweg, zult u geen verkeer van Cisco Webex zien. Als u probeert om TCP te zoeken verbinden, zou u geen verbindingspogingen zien voor st-port=5062, noch zou u een volgende MTLS handdruk of SIP Invite van Cisco Webex zien. Aangezien de diagnostische registratie van expressway-E in deze situatie niet nuttig is, hebt u een paar mogelijke verificatiemethoden:

1. Krijg een pakketvastlegging van de externe interface van de firewall
2. Levering van een havencontrolevoorziening
3. Gebruik het testgereedschap voor hybride connectiviteit

Aangezien het gereedschap Hybrid Connectivity Test direct in de Cisco Webex Control Hub is ingebouwd en de Cisco Webex-omgeving simuleert die probeert aan te sluiten op de expressway, is dit de meest ideale verificatiemethode die beschikbaar is. U kunt de TCP-connectiviteit in de organisatie als volgt testen:

1. Inloggen op de Cisco Webex Control Hub
2. SelecteerServices
3. Selecteer de instellingslink in **de hybride gesprekskaart**
4. In het vak Call Service Connect dient u er zeker van te zijn dat de waarde die in de SIP-bestemming is ingevoerd, juist is
5. Klik op Test zoals in de afbeelding.

6. Aangezien de test heeft gefaald, kunt u op de link **Testresultaten bekijken** klikken om de gegevens in de afbeelding te controleren.



Zoals u in de afbeelding hierboven kunt zien, is de Socket-test mislukt bij uw poging om verbinding te maken met 64.102.241.236:5062. Als u deze gegevens naast de diagnostische logbestanden/patches voor expressway hebt, die geen verbindingspogingen tonen, hebt u nu voldoende bewijs om de configuratie van firewalls ACL/NAT/routing te onderzoeken.

Oplossing

Aangezien dit specifieke probleem niet veroorzaakt wordt door de Cisco Webex-omgeving of de collaboration-apparatuur op gebouwen, moet u zich richten op de firewallconfiguratie. Aangezien u niet noodzakelijkerwijs het type firewall kunt voorspellen waarmee u wordt geconfronteerd, moet u

vertrouwen op iemand met vertrouwdheid met het apparaat. Het is mogelijk dat het probleem gerelateerd kan zijn aan een firewall ACL, NAT of een routingfout.

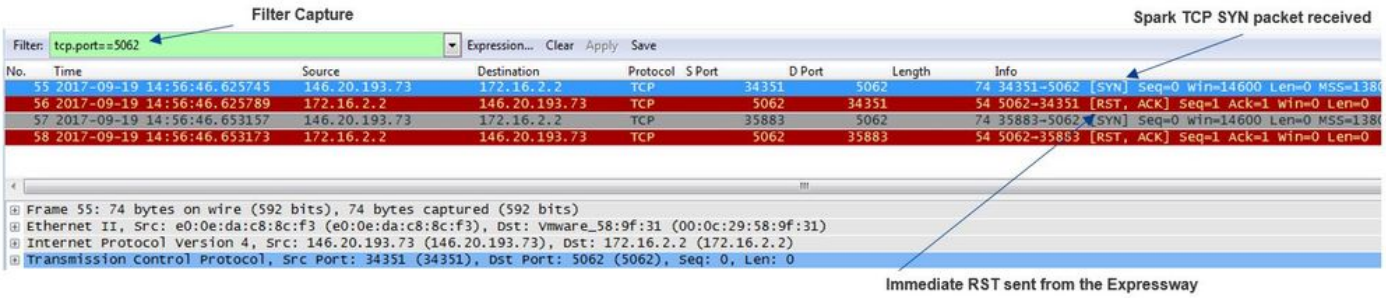
Uitgifte 3. Socketfalen: Expressway-E staat niet op poort 5062

Deze specifieke aandoening wordt vaak niet correct gediagnosticeerd. Vaak wordt aangenomen dat de firewall de oorzaak is van waarom het verkeer over poort 5062 wordt geblokkeerd. Om deze specifieke situatie op te lossen, kunt u de technieken gebruiken in "Port 5062 is geblokkeerd binnenin het bovenstaande scenario "Expressway". U zult ontdekken dat het gereedschap Hybrid Connectivity Test en elk ander gereedschap dat wordt gebruikt om de poortconnectiviteit te controleren zullen mislukken. De eerste veronderstelling is dat de firewall het verkeer blokkeert. De meeste mensen zullen dan de diagnostische houtkap van de Uitdrukkingsweg-E controleren om te bepalen of zij de TCP verbinding kunnen zien die probeert te vestigen. Ze zullen in het algemeen een loglijnitem zoeken zoals dit in de afbeelding.

```
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 deze voorwaarde bestaat de hierboven vermelde specifieke loggegevens niet. Daarom zullen veel mensen een verkeerde diagnose stellen van de aandoening en ervan uitgaan dat het de firewall is.

Als de pakketvastlegging in de diagnostische vastlegging is opgenomen, kunt u controleren of de firewall niet de oorzaak is. Hieronder staat een voorbeeld van pakketvastlegging uit het scenario waarin de Expressway-E niet luisterde via poort 5062. Deze opname wordt gefilterd door gebruik van tcp.port==5062 als het toegepaste filter zoals in de afbeelding.



Zoals u kunt zien in de pakketvastlegging die door de sneltoets E is gegenereerd, wordt het verkeer via TCP poort 5062 niet geblokkeerd door de firewall, maar komt in feite aan. In pakketnummer 56 kunt u zien dat de snelweg-E de RST onmiddellijk na het eerste TCP SYN-pakket verzenden. Met deze informatie kunt u concluderen dat de kwestie geïsoleerd is aan de expressway-E die het pakket ontvangt; U moet het probleem oplossen vanuit het standpunt van de snelweg. Gezien het bewijsmateriaal, bedenk mogelijke redenen waarom de Expressway-E het pakje zou REST. Twee mogelijkheden die aan dit gedrag kunnen worden toegeschreven zijn:

1. De Expressway-E heeft een of ander type firewallregels die het verkeer kunnen blokkeren

2. De snelweg-E luistert niet naar wederzijds TLS-verkeer en/of luistert niet naar verkeer via poort 5062.

De firewallfunctionaliteit van de Expressway-E bestaat onder *System > Protection > Firewall rules > Configuration*. Toen dit in deze omgeving werd gecontroleerd, was er geen firewallconfiguratie aanwezig.

Er zijn verschillende manieren om te verifiëren of de snelweg-E naar Mutual TLS traffic over poort 5062 luistert. U kunt dit doen door de Web Interface of de CLI als wortelgebruiker.

Vanuit de wortel van de snelweg, als u **netstat** afgeeft **-an | grep ':5062' ,** moet u wat output krijgen die vergelijkbaar is met wat u hieronder ziet.

```
~ # 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
```

Deze informatie kan ook worden opgenomen via de webinterface van de sneltoets E. Zie de onderstaande stappen om deze informatie te verzamelen

1. Inloggen bij de expressweg-E

2. Navigatie naar **onderhoudstools > poortgebruik > Lokale inkomende poorten**

3. Zoeken naar poort van het type SIP en IP 5062. (rood gemarkeerd zoals in de afbeelding)

Nu je weet wat je moet zien, kan je dat vergelijken met de huidige omgeving. Vanuit het CLI-perspectief, wanneer je **netstat** gebruikt **-an | grep ':5062'** ziet de output er zo uit:

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

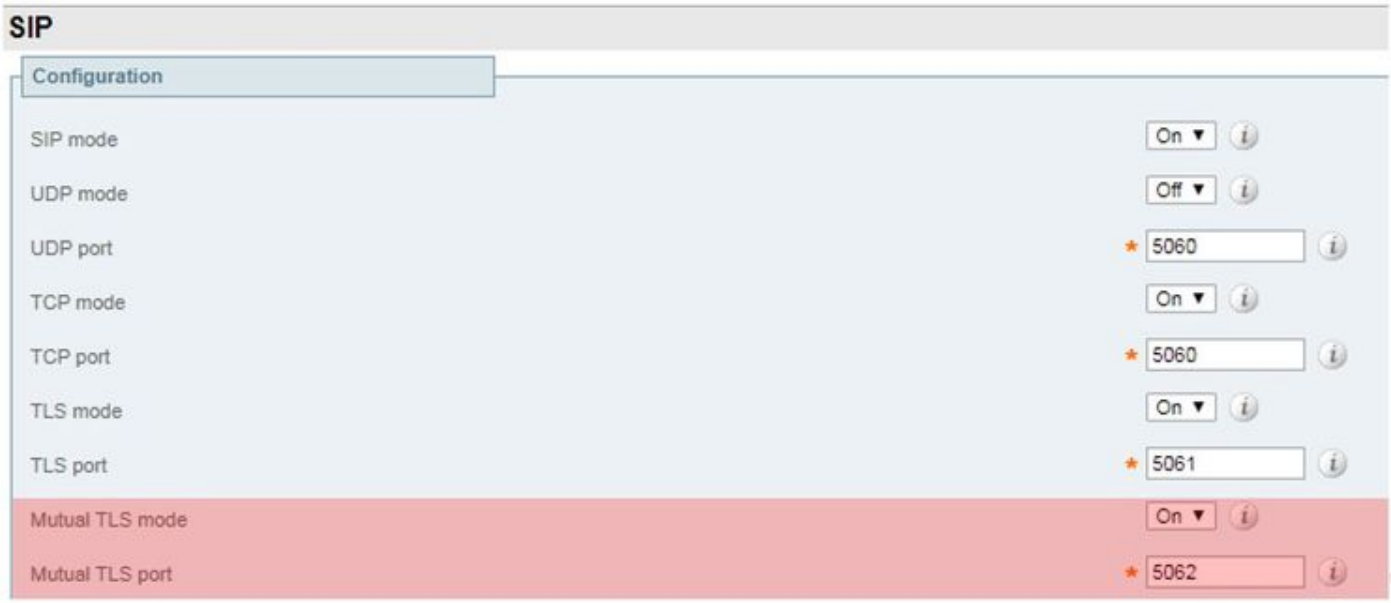
Daarnaast toont web UU de Mutual TLS poort niet die is opgenomen in de lijst van lokale inkomende poorten

Met deze gegevens kunt u concluderen dat de Expressway-E niet luistert naar Mutual TLS-verkeer.

Oplossing

Om dit probleem op te lossen, moet u ervoor zorgen dat de Mutual TLS-modus is ingeschakeld en dat de Mutual TLS-poort is ingesteld op 5062 in de Expressway-E:

1. Inloggen bij de sneltoets
2. Navigatie in naar **Configuration > Protocols > SIP**
3. Zorg ervoor dat de multi-TLS-modus is ingesteld op **Aan**
4. Zorg ervoor dat de wederzijdse TLS-poort is ingesteld op **5062**
5. Klik op **Opslaan** zoals in de afbeelding.



Vraag 4. E of C ondersteunen vooraf geladen SIP-routekoppen niet

Met de Hybrid Call Service Connect wordt de oproeproutering uitgevoerd op basis van **routekop**. De routekop is bevolkt op basis van de informatie die het gedeelte Call Service Aware (Express Connector) van de oplossing levert aan Cisco Webex. De host van de expressway-connector vraagt Unified CM voor gebruikers die zijn ingeschakeld voor de Call Service en trekt zowel hun **directory URI** als de **Cluster FQDN van hun Unified CM-thuiscluster**. Zie dit voorbeeld, gebruik Alice en Bob:

Map URI	**Routekop voor bestemming**
bob@example.com	emea-cucm.example.com
alice@example.com	us-cucm.example.com

Als Alice of Bob een gesprek voert, wordt de oproep naar hun Unified CM-vestigingen gestuurd, zodat deze op hun Cisco WebexRD kan worden geankerd voordat u de oproep naar de opgeroepen gebruiker stuurt.

Als Alice Bob moest bellen, zou de oproep naar *Alice's Unified CM Home Cluster FQDN (us-cucm.voorbeeldcom)* leiden. Als u de SIP INVITE analyseert die Cisco Webex naar de expressway-E stuurt, vindt u de volgende informatie in de SIP-header

URI aanvragen stap: bob@example.com
Routekop sip:us-cucm.voorbeeldcom;lr

Vanuit het perspectief van de Uitvoer worden de regels van het Zoeken ingesteld om de oproep niet door de URI van het verzoek maar eerder de **Kop van de Route (us-cucm.voorbeeldcom) te** leiden — in dit geval Alice's Unified CM home cluster.

Met deze stichting ingesteld, kunt u problemen oplossen situaties begrijpen waar de snelwegen verkeerd zijn ingesteld, waardoor de bovenstaande logica niet werkt. Zoals bijna elke andere

inkomende Hybrid Call Service Connect setup-storing is het symptoom dat *de telefoon op zijn terrein niet belt*.

Alvorens u de diagnostische logbestanden op de Expressway analyseert, moet u bedenken hoe u deze oproep kunt identificeren:

1. De URI van het SIP-verzoek is de **directory URI** *van* **de opgeroepen partij.**
2. Het veld SIP VANAF is opgemaakt van de **bellenpartij** die is opgenomen in de lijst **met "Voornaam en voornaam" <sip:WebexDisplayName@subdomain.call.ciscospark.com>**

Met deze informatie kunt u de diagnostische logbestanden doorzoeken in **Directory URI van genaamd Party, First and Last Name of Calling Party, of Cisco Webex SIP Address of the Calling Party**. Als u geen van deze informatie hebt, kunt u op "**INVITE SIP:**" zoeken**:**" die alle SIP-oproepen plaatst die over de expressway lopen. Nadat u SIP INVITE voor de inkomende vraag hebt geïdentificeerd, kunt u de plaats van de SIP Vraag ID vinden en kopiëren. Nadat u deze waarde hebt, kunt u de diagnostische logbestanden op basis van de Call-ID gewoon doorzoeken om alle berichten te zien die correleren met deze gesprekspartner.

Een ander ding om het routingprobleem te isoleren is te bepalen hoe ver de vraag in de onderneming gaat. U kunt proberen om de informatie te vinden die hierboven op de Expressway-C vermeld staat om te zien of de oproep zover verstuurd is. Zo ja, dan zult u waarschijnlijk uw onderzoek daar willen starten.

In dit scenario ziet u dat de Expressway-C het INVITE van de Expressway-E heeft ontvangen.

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



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

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

Belangrijk is dat de **routeheader (Cluster FQDN)** nog intact is. Er wordt echter geen zoeklogica uitgevoerd op basis van de routeheader (Cluster FQDN) **cucm.rtp.ciscotac.net**. Je ziet het bericht meteen verworpen worden met een **404 Not found**.

```
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
```

Vergeleken met een werkscenario zou u zien dat in het werkscenario de zoeklogica wordt uitgevoerd op basis van de Router Header (Cluster FQDN)

```
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'"**

U kunt dan zien dat Expressway-C correct de oproep naar Unified CM (192.168.1.21) doorgeeft.

2017-09-22T13:56:02.232-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-22 17:56:02,232" Module="network.sip" Level="DEBUG": Action="Sent" Local-ip="192.168.1.5" Local-port="25606" Dst-ip="192.168.1.21" Dst-port="5065" Msg-Hash="866788495063340574"
SIPMSG:
|**INVITE sip:jorobb@rtp.ciscotac.net** SIP/2.0
Via: SIP/2.0/TCP 192.168.1.5:5060;**egress-zone=CUCM11**;branch=z9hG4bK251d6daf044e635607cc13d244b9ea45138220.69ccb8de20a0e853c1313782077f77b5;proxy-call-id=17aa8dc7-422c-42ef-bdd9-b9750fbd0edf;rport
Via: SIP/2.0/TLS 192.168.1.6:7003;**egress-zone=HybridCallServiceTraversal**;branch=z9hG4bKba323da436b2bc288200d56d11f02d4d272;proxy-call-id=32c76cef-e73c-4911-98d0-e2d2bb6fec77;received=192.168.1.6;rport=7003;**ingress-zone=HybridCallServiceTraversal**
Via: SIP/2.0/TLS 192.168.1.6:5073;branch=z9hG4bK06cde3f662d53a210b5b4b11b85500c19;x-cisco-local-service=nettle;received=192.168.1.6;rport=42533;ingress-zone=DefaultZone
Via: SIP/2.0/TLS 64.102.241.236:5061;egress-zone=DefaultZone;branch=z9hG4bK297799f31d0785ff7449e1d7dbe3595b271.2ed90cbed5b79c6cffad9ecd84cc8337;proxy-call-id=3be87d96-d2e6-4489-b936-8f9cb5ccaa5f;received=172.16.2.2;rport=25005
Via: SIP/2.0/TLS 192.168.4.146:5062;branch=z9hG4bK043ca6360f253c6abed9b23fbeff9819;received=148.62.40.64;rport=36149;ingress-zone=HybridCallServicesDNS
Via: SIP/2.0/TLS 127.0.0.1:5070;branch=z9hG4bK-353038-8c648a16c2c5d7b85fa5c759d59aa190;rport=47732
Call-ID: daa1a6fa546ce76591fc464f0a50ee32@127.0.0.1
CSeq: 1 INVITE
Contact: <sip:192.168.1.6:5073;transport=tls>;call-type=squared
From: "pstojano test" <sip:pstojano-test@dmzlab.call.ciscospark.com>;tag=567490631
To: <sip:jorobb@rtp.ciscotac.net>
Max-Forwards: 14
Route:

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

Na analyse van de diagnostische houtkap die het probleem geïsoleerd heeft aan de Expressway-C en een specifieke fout (404 Not Found) kan je je concentreren op wat dit soort gedrag zou veroorzaken. Enkele overwegingen zijn:

1. De oproepen worden in en uit zones op de snelweg verplaatst door middel van zoekregels.
2. De expressways gebruiken logica die wordt genoemd Voorgeladen SIP routeondersteuning

die SIP INVITE verzoeken verwerkt die routerheader bevatten. Deze waarde kan in de Zones (Traversal Server, Traversal client, buurman) aan of uit worden gezet op zowel expressway-C als Expressway-E.

U kunt de xConfiguration gebruiken om de configuratie op zowel de Expressway-E Traversal server als de Expressway-C client zones te bekijken, in het bijzonder de zones die zijn ingesteld voor Hybrid Call Service Connect. Naast de configuratie van de Zone, kunt u de regels van het Zoeken analyseren die zijn ingesteld om deze oproep van de ene zone naar de andere door te geven. U weet ook dat de Expressway-E de aanroep aan de Expressway-C heeft doorgegeven zodat de Traversal server zone configuratie daar waarschijnlijk correct is ingesteld.

Om dit te onderbreken, vertelt de xConfig hieronder dat de naam van deze zone **Hybrid Call Service Traversal** wordt genoemd. Het is van het **TraversalServer** zone type. Het communiceert met de Expressway-C over SIP TCP poort **7003**.

Het belangrijkste stuk voor de Hybride Call Service is dat deze SIP-routeondersteuning op moet hebben vooraf geladen. De interface Expressway Web roept deze waarde **Voorgeladen SIP-routeondersteuning op**, terwijl de xConfiguration het zal weergeven zoals **SIP PreloadedSipRoutes Accepteren**

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

U kunt ook bepalen dat deze Zone zoekregel 3 (Webex Hybrid) aan deze regel heeft gekoppeld. De zoekregel stuurt in wezen een 'Any'-alias die door de DNS-zone van de hybride Call Services komt en doorgeeft aan de hierboven genoemde zone, Hybrid Call Service Traversal. Zoals verwacht, worden zowel de zone van de Zoeken als de Transversal Server op de snelweg-E correct ingesteld.

```
*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"
```

Als u zich richt op de xConfiguration van de Expressway-C, kunt u starten door te zoeken naar de Traversal Client-zone voor Webex Hybrid. Eén makkelijke manier om dit te vinden is door te zoeken in het poortnummer dat u hebt geleerd van de SIP-poort (SIP-poort): "7003"). Dit helpt u snel de juiste zone in de xConfiguration-instelling te identificeren.

Zoals eerder kunt u de Zone Name (Hybrid Call Service Traversal), het Type (Traversal Client) en wat is ingesteld voor de SIP PreloadedRoues Accept (vooraf ingestelde SIP-routeondersteuning). Zoals u in deze xConfiguration kunt zien, wordt deze waarde ingesteld op Uit. Gebaseerd op de plaatsingsgids voor de Hybride Bel van Cisco Webex, moet deze waarde op On worden ingesteld.

Daarnaast kunnen we, als we de definitie van de voorgeladen SIP-routes controleren, duidelijk zien dat Expressway-C een bericht moet OPNIEUW-JECT hebben als deze waarde op Off is ingesteld EN INVITe een routeheader bevat: "SIP-routeondersteuning via Switch Preloaded Off, als u wilt dat de zone SIP INVITE-verzoeken met deze header afwijst."

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

```
*c xConfiguration Zones Zone 6 TraversalClient SIP TLS Verify Mode: "On"
*c xConfiguration Zones Zone 6 TraversalClient SIP TURN Server Address:
*c xConfiguration Zones Zone 6 TraversalClient SIP TURN Server Port:
*c xConfiguration Zones Zone 6 TraversalClient SIP Transport: "TLS"
*c xConfiguration Zones Zone 6 Type: "TraversalClient"
```

Op dit punt heb je het probleem geïsoleerd aan een verkeerde configuratie van de configuratie van de Expressway-C Traversal-clientzone. U moet de ondersteuning van de voorgeladen SIP-routes naar On wijzigen.

Oplossing

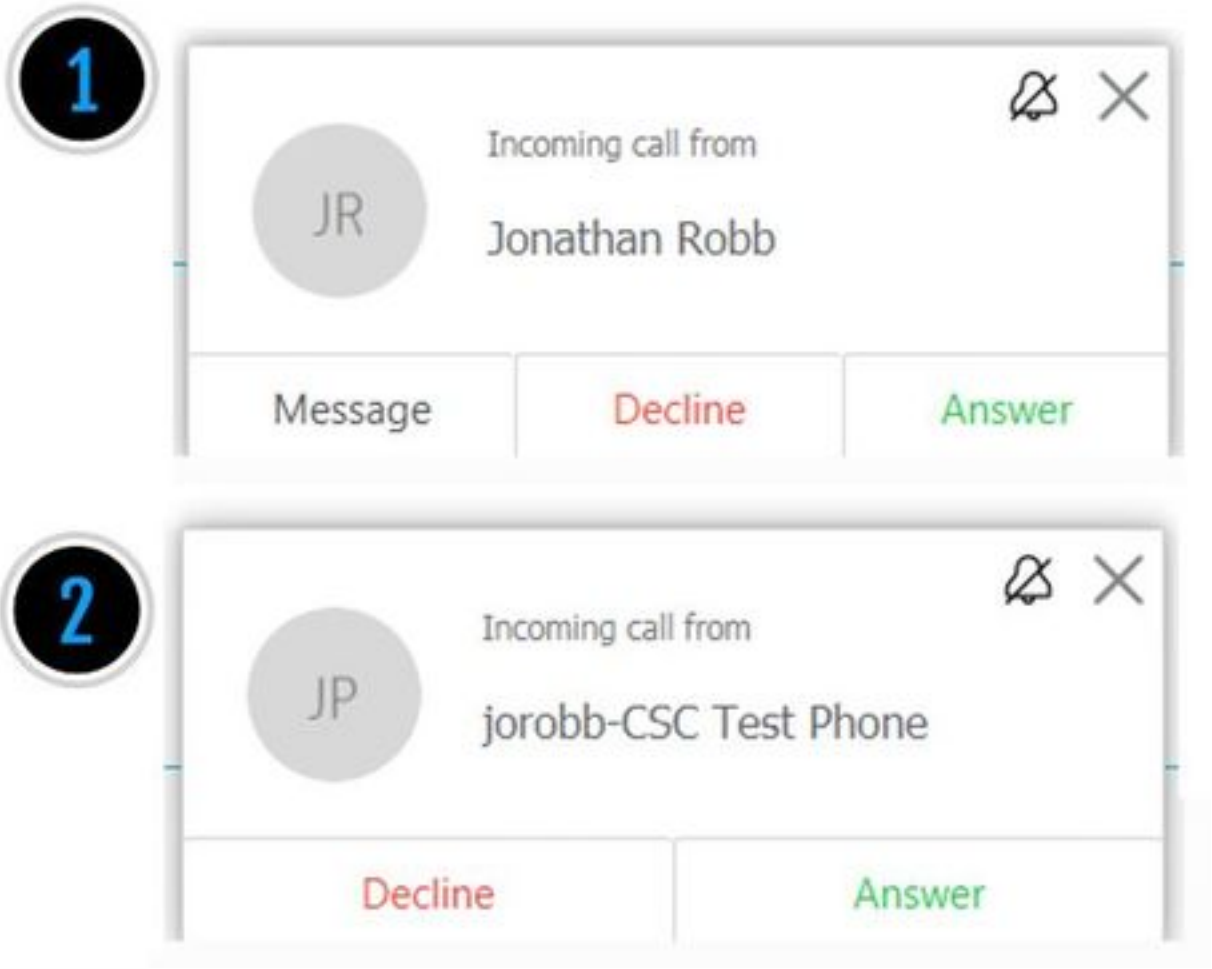
U kunt de ondersteuning van vooraf ingestelde SIP-routes als volgt instellen:

1. Inloggen bij sneltoets-C
2. Navigeren in **configuratie > Zones > Zones**
3. Selecteer de gebruikerszone van de Hybride Call Service Traversal (de naam zal van klant tot klant verschillen)
4. Stel de **ondersteuning van vooraf ingestelde SIP-routes** in op **On**
5. Selecteer **Opslaan**

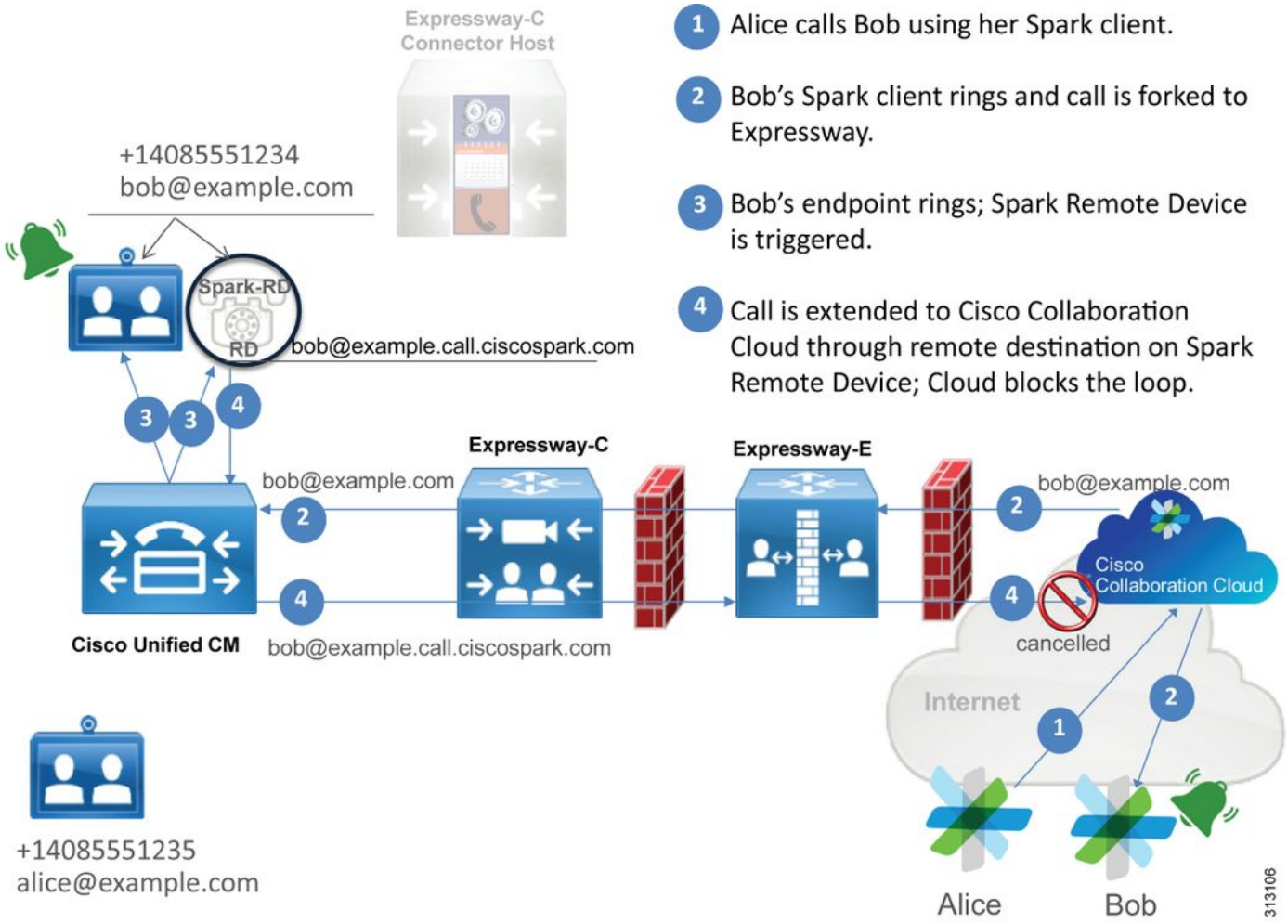
Opmerking: Terwijl dit scenario de mislukking op de Expressway-C aantoonde, konden de zelfde diagnostische logfouten worden waargenomen op de Expressway-E als de **Voorgeladen SIP routeondersteuning** uit was op de Webex Hybrid Call Traversal Server-zone. In dat geval zou je de oproep nooit bij de Expressway-C hebben gezien en de Expressway-E zou verantwoordelijk zijn geweest voor het afwijzen van de oproep en het verzenden van de 404 Not Found.

Vraag 5. Cisco Webex-app ontvangt twee gespreksmeldingen (kantelingen)

Dit specifieke probleem is toevallig het enige inkomende oproepende scenario dat niet in het afzetten van de vraag resulteert. Voor dit probleem ontvangt de persoon die de oproep ontvangt (de zogeheten partij) twee kennisgevingen (berichten) in de Cisco Webex-app van de persoon die de oproep had geplaatst (oproepende partij). Het eerste bericht wordt gegenereerd door Cisco Webex en het tweede bericht komt van de infrastructuur op uw locatie. Hieronder staan monsters van de twee ontvangen kennisgevingen, zoals weergegeven in de afbeelding.



Het eerste bericht (toast) is van de persoon die de vraag (kijkend partij) van de kant van Cisco Webex initieert. De oproepende ID in deze instantie is de Display Name van de gebruiker die de oproep initieert. Het tweede bericht (toast) komt van het bedrijf CTI of Cisco Webex RD dat wordt toegewezen aan de gebruiker die de vraag maakt. In het begin lijkt dit gedrag eigenaardig. Als u echter het inkomende aanroepschema (van de Hybride Call Design Guide van Cisco Webex) bekijkt, is het gedrag logischer zoals in de afbeelding te zien.



Uit de afbeelding kan je zien dat Alice Bob van haar Cisco Webex-app belt en dat de oproep tot het indienen van voorstellen naar het pand wordt gestuurd. Deze vraag moet overeenkomen met de URI van de Map die aan de telefoon van Bob is toegewezen. Het probleem is dat met dit ontwerp, de directory URI ook wordt toegewezen aan zijn CTI-RD of Cisco Webex RD. Daarom, wanneer de oproep aan CTI-RD of Cisco Webex RD wordt aangeboden, wordt de vraag teruggestuurd naar Cisco Webex omdat het apparaat een Remote Destination die voor bob@example.call.ciscospark.com wordt geconfigureerd heeft. De manier waarop Cisco Webex deze situatie behandelt is dat het de specifieke telefoonboog annuleert.

Om Cisco Webex te kunnen annuleren moet Cisco Webex eerst een parameter in de SIP header plaatsen die nodig is om dat bepaalde been te annuleren. De parameter Cisco Webex invoegen in SIP INVITE wordt **"call-type=squared"** genoemd en deze waarde wordt ingevoerd in de Contactheader. Als deze waarde van het bericht wordt gestript, begrijpt Cisco Webex niet hoe u de oproep kunt annuleren.

Met deze informatie kunt u het eerder gepresenteerde scenario bekijken waar de Cisco Webex-app van de gebruiker twee meldingen (tips) ontving toen Cisco Webex-gebruiker Jonathan Robb belde. Om dit type probleem op te lossen, zult u altijd diagnostische houtkap van de Expressway-C en Expressway-E moeten verzamelen. Als startpunt kunt u de sneltoetsen Expressway-E bekijken om te bepalen dat SIP INVITE in feite de **Call-type=squared** waarde heeft die aanwezig is in de contactkop van de eerste Cisco Webex INVITE die binnensteekt. Dit zal ervoor zorgen dat de firewall het bericht op geen enkele manier manipuleert. Hieronder zie je een voorbeeld van het INVITE dat vanuit dit scenario naar de expressway-E komt.

```
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:
```

De contactkop heeft de aanwezige **call-type=squared** waarde. Op dit punt moet de oproep door de sneltoets lopen en uit de zone van de Webex Hybrid Traversal Server worden verstuurd. We kunnen de sneltoetsen Expressway-E doorzoeken om te bepalen hoe de oproep vanuit de expressway-E werd verstuurd. Dit zal ons een idee geven als de Expressway-E de INVITE op een of andere manier manipuleert.

```
2017-09-19T14:01:48.468-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 18:01:48,468"
Module="network.sip" Level="DEBUG":  Action="Sent" Local-ip="192.168.1.6" Local-port="7003" Dst-
ip="192.168.1.5" Dst-port="26686" Msg-Hash="1847271284712495612"
SIPMSG:
INVITE sip:pstojano-test@rtp.ciscotac.net SIP/2.0
Via: SIP/2.0/TLS 192.168.1.6:7003;egress-
zone=HybridCallServiceTraversal;branch=z9hG4bKec916b02b6d469abad0a30b93753f4b0859;proxy-call-
id=d7372034-85d1-41f8-af84-dffed6d1a9a9;rport
Via: SIP/2.0/TLS 192.168.1.6:5073;branch=z9hG4bKd91699370129b4c10d09e269525de00c2;x-cisco-local-
service=nettle;received=192.168.1.6;rport=43119;ingress-zone=DefaultZone
Via: SIP/2.0/TLS 64.102.241.236:5061;egress-
zone=DefaultZone;branch=z9hG4bK52aac9a181192566e01b98ae0280bdff858.0e65cdfe078cabb269eecb6bce132
8be;proxy-call-id=ec51e8da-e1a3-4210-95c9-494d12debcd8;received=172.16.2.2;rport=25016
Via: SIP/2.0/TLS
192.168.5.164:5062;branch=z9hG4bK564cd36d87f3417513c9b559dc666f71;received=146.20.193.73;rport=4
0342;ingress-zone=HybridCallServicesDNS
Via: SIP/2.0/TLS 127.0.0.1:5070;branch=z9hG4bK-3237-5c5060d07ecc546a0bb861ef52a5f507;rport=43306
Call-ID: 6bc0ca8210c0b48df69f38057ec1e48b@127.0.0.1
CSeq: 1 INVITE
Contact: <sip:192.168.1.6:5073;transport=tls>     <-- Webex inserted value is now missing
From: "Jonathan Robb"




        ;tag=540300020
To:
```

```
Max-Forwards: 15
Route: <sip:cucm.rtp.ciscotac.net;lr>
```

Wanneer u deze SIP INVITE bespreekt die van de sneltoets-E naar de sneltoets expressievloer-C wordt verzonden, let op dat de contactkop het **aanroepen-type=squared** mist. Een ander ding om op te wijzen is dat in lijn item 4, je kunt zien dat de spanning-zone gelijk is aan **HybridCallServiceTraversal**. U kunt nu concluderen dat de reden dat de Cisco Webex-app een tweede melding (toast) krijgt wanneer deze wordt geselecteerd, is vanwege het **verwijderen** van de **Call-type=squared** tag van de SIP INVITE Contact header. De vraag die moet worden beantwoord is wat de oorzaak zou kunnen zijn van deze gestripte kop.

De oproep moet via de Hybrid Call Service Traversal lopen die u op de Expressway hebt ingesteld, zodat dit een goede plek is om het onderzoek te starten. Als u de xConfiguration hebt, kunt u zien hoe deze zone is ingesteld. Om de Zone in de xConfiguration te identificeren, kunt u de naam gebruiken die in de Via-lijn is opgenomen en in de logbestanden wordt afgedrukt. Je kunt zien dat het hierboven heet egress-zone=HybridCallServiceTraversal. Wanneer deze naam in de Via lijn van de SIP-header is afgedrukt, worden de spaties verwijderd. De echte naam van de zone vanuit het perspectief van de xConfiguration heeft spaties en is opgemaakt bij de Transversal voor de Hybrid Call Service.

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

Met de instellingen die voor de Hybrid Call Service Traversal zijn geïdentificeerd, kunt u op zoek gaan naar mogelijke instellingen die opvallen, zoals:

- Voorgeladen SIPSIPRoutes aanvaarden: Aan
- SIP-parameterBehoud-modus: Uit

Met behulp van de web interface van elke expressway, kun je zien wat de definitie van deze waarden is en wat ze doen.

Ondersteuning van voorgeprogrammeerde SIP-routers

Ondersteuning van SIP-routes voor overzetten op om deze zone in staat te stellen SIP INVITE-verzoeken te verwerken die de routekop bevatten.

Ondersteuning van SIP-routebeheer voor overzetten als u wilt dat de zone SIP INVITE-verzoeken met deze header afwijst.

SIP-parameterbehoud

Bepaalt of de B2BUA van de Uitdrukkwaliteit de parameters in SIP verzoeken bewaart of herschrijft die via deze zone worden geleid.

Hiermee behoudt u de URI van de SIP-aanvraag en de Contactparameters van verzoeken die tussen deze zone en de B2BUA worden verzonden.
OffHiermee kan de B2BUA de SIP-aanvraagURI herschrijven en contactparameters van verzoeken die tussen deze zone en de B2BUA worden verzonden, indien nodig.
Gebaseerd op deze definities, de xConfiguration, en dat de **call-type=squared** waarde wordt geplaatst in de "Contact"-header van de SIP INVITE, kunt u concluderen dat het hebben van de SIP-parameter-waarde voor het behoud van de waarde Off in de traversal van de hybride Call Service de reden is dat tag wordt gestript en dat de Cisco Webex-app dubbele ringmeldingen krijgt.

Oplossing

Om de Call-type=squared waarde in de Contact header van de SIP INVITE te handhaven, moet u ervoor zorgen dat de expressievormen SIP-parameter behoud bieden voor alle zones die betrokken zijn bij de verwerking van de oproep:

1. Inloggen bij de sneltoets
2. Navigeren in **configuratie > Zones > Zones**
3. Selecteer de zone die wordt gebruikt voor de hybride traversale server
4. Stel de waarde voor het behoud van de SIP-parameter in op **On**
5. De instellingen opslaan.

##
Opmerking: In dit voorbeeldscenario was het de Hybrid Traversal Server-zone van Webex op de Expressway-E die verkeerd was geconfigureerd. Houd in gedachten dat het volledig mogelijk is dat de SIP-waarde voor het behoud van parameter op Off wordt ingesteld op Off in de Webex Hybrid Traversal client of CUCM buurzones. Beide formaties zouden worden uitgevoerd op de Expressway-C. Als dat het geval was, zou je kunnen verwachten dat de Expressway-E de **call-type=squared** waarde naar de Expressway-C zou hebben gestuurd en het zou de Expressway-C zijn geweest die het zou verwijderen.

Uitgaand: Premises aan Cisco Webex

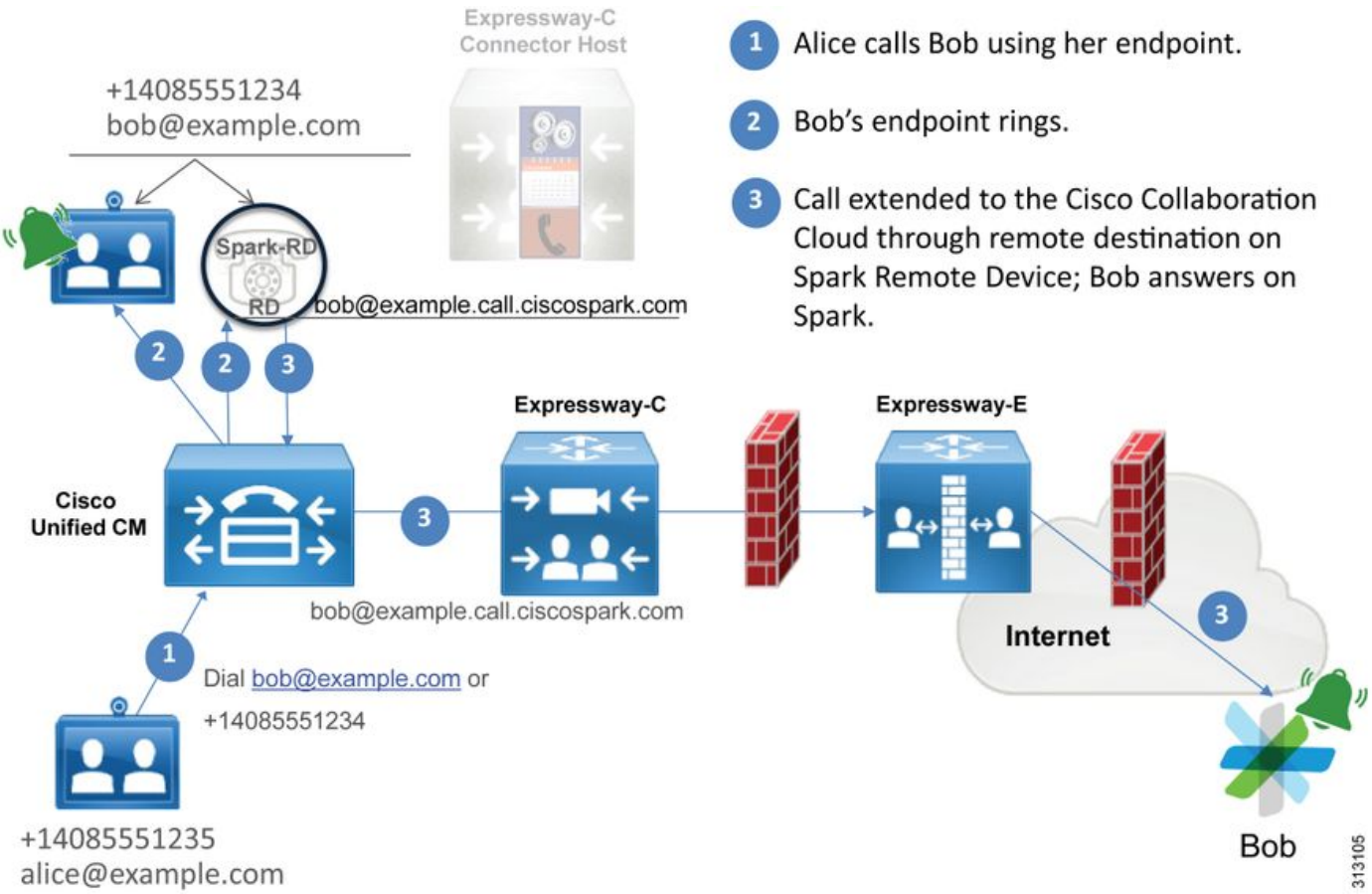
Bijna elke fout in oproepen bij uitgaande ondersteuning van Cisco Webex leidt tot hetzelfde gerapporteerde symptoom: "Wanneer ik van mijn Unified CM-geregistreerde telefoon naar een andere gebruiker roep die is ingeschakeld voor Call Service Connect, gaat hun mobiele telefoon naar het bedrijf, maar hun Cisco Webex-app niet." Om dit scenario problemen op te lossen, is het belangrijk om zowel de vraagstroom als de logica te begrijpen die plaatsvinden wanneer dit type vraag wordt geplaatst.

Logic-doorloop op hoog niveau

1. Gebruiker A roept vanuit hun telefoon op voorstappen naar de directory URI van Gebruiker B
2. Gebruiker B's ter plaatse en CTI-RD/Webex-RD accepteert de oproep
3. De telefoon van de gebruiker begint bij de ringen
4. CTI-RD/Webex-RD van de gebruiker, die deze oproep doet naar de bestemming van UserB@example.call.ciscospark.com
5. Unified CM geeft deze oproep tot de sneltoets-C door
6. Expressway-C stuurt de oproep naar de snelweg-E
7. Expressway-E voert een DNS-raadpleging uit in het domein CallService.ciscospark.com
8. Expressway-E probeert verbinding te maken met de Cisco Webex-omgeving via poort 5062.
9. Expresway-E en de Cisco Webex-omgeving beginnen een wederzijdse handdruk
10. De Cisco Webex-omgeving geeft de oproep door naar de beschikbare Cisco Webex-app van gebruiker B
11. Gebruiker B's beschikbare Cisco Webex-app begint te bellen.

CallFlow

Navigeer naar **Gebruiker B on-prem telefoon > Unified CM > CTI-RD/Webex-RD > Expressway-C > Expressway-E > Cisco Webex-omgeving > Cisco Webex-app** zoals in de afbeelding getoond.



Opmerking: De afbeelding is getrokken uit de Cisco Webex Hybrid Design Guide.

Tips voor loganalyse

Als u problemen oplossen bij een situatie waarin de uitgaande geforceerde oproepen naar Cisco Webex mislukken, wilt u de Unified CM, Expressway-C en Expressway-E logbestanden

verzamelen. Door deze stammen te hebben, kunt u zien hoe de oproep door de omgeving gaat. Een andere snelle manier om te begrijpen hoe ver de oproep in uw omgeving komt is de "zoekgeschiedenis" van de snelweg te gebruiken. De geschiedenis van het zoeken van de snelweg zal u snel toestaan om te zien of de geforkeerde vraag naar Cisco Webex aan de autosnelweg-C of E begint.

U kunt de zoekgeschiedenis als volgt gebruiken:

1. Inloggen bij de sneltoets
   Plaats een testoproep
   navigeren naar **status > zoekgeschiedenis**
   Controleer of u een oproep ziet die een doeladres van de Webex SIP URI heeft dat moet worden opgeroepen (user@example.call.ciscospark.com)
   Als de zoekgeschiedenis niet de vraag toont die de expressweg-E zoekgeschiedenis aanslaat, herhaal dit proces dan op de sneltoets-C

Alvorens u de diagnostische logbestanden op de Expressway analyseert, moet u bedenken hoe u deze oproep kunt identificeren:

1. De URI van het SIP-verzoek is het SIP-adres van de Cisco Webex-gebruiker
2. Het veld SIP VANUIT is opgemaakt zodat de bellenpartij in de lijst staat met "Voornaam en achternaam" <sip:Alias@Domain>

Met deze informatie kunt u de diagnostische logbestanden doorzoeken via Directory URI of Calling Party, First and Last Name of Calling Party, of Cisco Webex SIP Address of the Call Party. Als u geen van deze informatie hebt, kunt u een zoekopdracht op "**INVITE SIP:**" uitvoeren om alle SIP-oproepen te lokaliseren die over de expressway lopen. Zodra u SIP INVITE voor de Uitgaande vraag hebt geïdentificeerd, kunt u de plaats van de **Vraag-ID** van SIP **plaatsen** en kopiëren. Nadat je dit hebt, kan je de diagnostische logbestanden gewoon doorzoeken op basis van de **Call-ID** om alle berichten te zien die correleren met deze callleg.

Hier zijn een aantal van de meest gebruikelijke kwesties die met uitgaande oproepen van de Unified CM-geregistreerde telefoon naar de Cisco Webex-omgeving worden gesignaleerd wanneer de oproep wordt gedaan aan een gebruiker die voor Call Service Connect is ingeschakeld.

Vraag 1. Expressway is niet in staat om het adres callservice.ciscospark.com op te lossen

De standaardprocedure voor een DNS-zone van een snelweg is om een DNS-raadpleging uit te voeren op basis van het domein dat aan de rechterkant van een URI van een aanvraag verschijnt. Om dit te verklaren, denk aan een voorbeeld. Als de DNS-zone een oproep zou ontvangen die een aanvraag URI van **pstojano-test@dmzlab.call.ciscospark.com** had, dan zou een typische DNS-zone van Expressway de DNS SRV-Lookup-logica uitvoeren op **dmzlab.call.ciscospark.com,** wat de rechterkant van het verzoek URI is. Als de Expressway dit zou doen, kon je verwachten dat de volgende raadpleging en reactie zouden plaatsvinden.

```
_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
```

Als u goed kijkt, ziet u dat de SRV record respons een serveradres en poort 5061 aanbiedt, niet 5062.

Dit betekent dat de wederzijdse TLS-handdruk die via poort 5062 plaatsvindt niet zal plaatsvinden en dat een afzonderlijke poort wordt gebruikt voor het signaleren tussen de sneltoets en Cisco Webex. De uitdaging hiermee is dat de *Invoergids voor de Hybride Call Services van Cisco Webex* het gebruik van port 5061 niet expliciet uitroept omdat sommige omgevingen geen zaken toestaan om zaken te bellen.

De manier om voorbij deze standaard DNS Zone SRV lookup-logica op de Expressway te werken is door de expressway te configureren zodat deze expliciete zoekopdrachten uitvoert op basis van een waarde die u verschaft.

Wanneer u deze bepaalde oproep analyseert, kunt u zich concentreren op de Expressway-E omdat u heeft bepaald (met behulp van zoekgeschiedenis) dat de oproep tot nu toe heeft geleid. Start met de eerste SIP INVITE die in de Expressway-E komt om te zien welke zone het binnenliep, welke zoekregels worden gebruikt, welke Zone de oproep uitgaat en welke DNS lookup-logica optreedt als je correct naar de DNS-zone wordt verzonden.

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




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




 Max-Forwards: 15
 Record-Route: <sip:proxy-call-id=47454c92-2b30-414a-b7fe-
aff531296bcf@192.168.1.5:5061;transport=tls;lr>
 Record-Route: <sip:proxy-call-id=47454c92-2b30-414a-b7fe-
aff531296bcf@192.168.1.5:5060;transport=tcp;lr>
 Allow: INVITE,OPTIONS,INFO,BYE,CANCEL,ACK,PRACK,UPDATE,REFER,SUBSCRIBE,NOTIFY
 User-Agent: Cisco-CUCM11.5
 Expires: 180
 Date: Tue, 19 Sep 2017 17:18:50 GMT
 Supported: timer,resource-priority,replaces,X-cisco-srtp-fallback,X-cisco-original-called
 Session-Expires: 1800
 Min-SE: 1800
 Allow-Events: presence
```

```
X-TAATag: 2272025a-ce36-49d0-8d93-cb6a5e90ffe0
Session-ID: 75957d4fb66a13e835c10737aa332675;remote=00000000000000000000000000000000
Cisco-Guid: 2568978048-0000065536-0000000148-0352430272
Content-Type: application/sdp
Content-Length: 714

<SDP Omitted>
```

In deze SIP INVITE, kunt u de **URI** (**Application URI**), de **Call-ID** (991f7e80-9c1517a-130ac-1501a8c0), **From** ("Jonathan Robb" **<**sip:5010@rtp.ciscotac.net **To** (SIP:pstojano-test@dmzlab.call.ciscospark.com) en **User-Agent (Cisco-CUCM11.5).** Nadat deze INVITE is ontvangen, moet de snelweg nu een logisch besluit nemen om te bepalen of hij de oproep naar een andere zone kan sturen. De sneltoets zal dit doen op basis van zoekregels.

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

Op basis van het logfragment hierboven kunt u zien dat de Expressway-E is geparseerd met vier zoekregels, maar er is slechts één *(*Webex Hybrid - naar Webex Cloud*)* overwogen. De zoekregel had een prioriteit van 90 en was bedoeld om naar de DNS-zone voor hybride gespreksservices te gaan. Nu de vraag naar een DNS-zone wordt verzonden, kunt u de DNS SRV-favorieten die op de Expressway-E plaatsvinden opnieuw bekijken

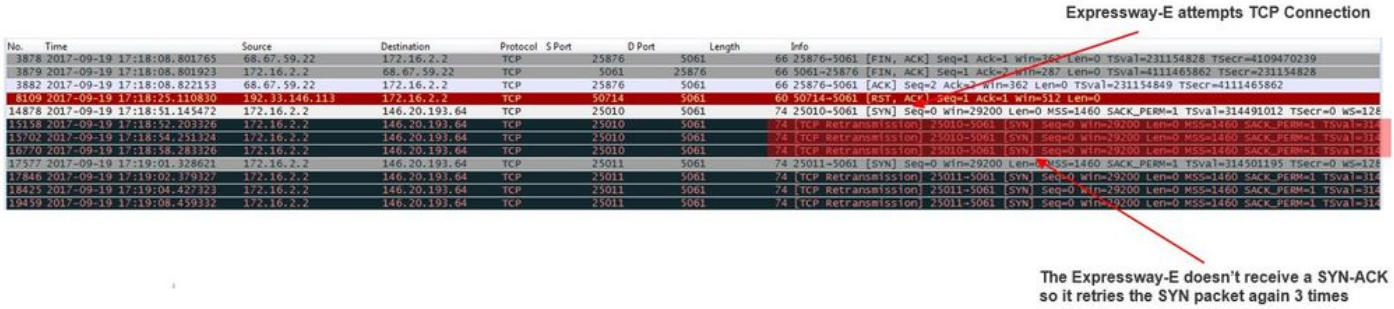
```
2017-09-19T13:18:50.565-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 17:18:50,565"
Module="network.dns" Level="DEBUG":  Detail="Sending DNS query"
Name="dmzlab.call.ciscospark.com" Type="NAPTR (IPv4 and IPv6)"
2017-09-19T13:18:50.718-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 17:18:50,718"
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"
```

In het bovenstaande fragment kunt u zien dat de Expressway-E de SRV-raadpleging heeft uitgevoerd aan de rechterkant van de URI met het verzoek (_sips._tcp.dmzlab.call.ciscospark.com) en dat de functie is opgelost aan een hostname van l2sip-cfa-01.wbx2.com en poort 5061. De hostname l2sip-cfa-01.wbx2.com lost op tot 146.20.193.64. Met deze informatie is de volgende logische stap die de Expressway zal nemen om een TCP SYN-pakket naar 146.20.193.64 te verzenden zodat het kan proberen om de oproep in te stellen. Van de Expressway-E-logging kunt u bekijken of dit gebeurt.

```
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"
```

In het bovenstaande diagnostische logingfragment van Expressway-E kunt u zien dat de Expressway-E probeert verbinding te maken met het IP 146.20.193.64 dat eerder werd opgelost via TCP-poort 5061, maar deze verbinding schiet volledig tekort. Dit kan ook worden gezien in het kader van de pakketvastlegging die is verzameld.



Op basis van deze resultaten is het duidelijk dat het verkeer over port 5061 niet slaagt. Hybride Call Service Connect is echter bedoeld om TCP-poort 5062 en niet 5061 te gebruiken. Daarom moet u bedenken waarom het niet de Expressway-E is die een SRV record oplost die port 5062 zou teruggeven. Om die vraag te beantwoorden kunt u naar mogelijke configuratieproblemen op de Expressway-E Webex hybride DNS-zone zoeken.

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

In de xConfiguration van de Expressway-E kunt u zien dat er twee speciale waarden voor de DNS-raadpleging zijn: **DNSOverify-naam en DNSOverify-correctie**. Gebaseerd op deze xConfiguration is de DNSOque Override ingesteld op Off, daarom zou de DNSOverify-naam niet van kracht worden. Om beter te begrijpen wat deze waarden doen, kunt u het Web UI van de Uitdrukking gebruiken om de definitie van de waarden omhoog te kijken.

DNS-aanvraag wijzigen *(vertaalt naar DNSOverride in xConfig)*

Routes uitgaande SIP-oproepen van deze zone naar een handmatig gespecificeerd SIP-domein in plaats van het domein in de gedialineerde bestemming. Deze optie is voornamelijk bedoeld voor gebruik met Cisco Webex Call Service. Zie www.cisco.com/go/hybrid-services.

Domain om naar *te* zoeken *(vertaalt naar DNSOverride Name in xConfig)*

Voer een FQDN in om in DNS in plaats van het zoeken naar het domein in de uitgaande SIP URI

te vinden. De oorspronkelijke SIP URI wordt niet gewijzigd.

Nu u deze definities hebt, is het duidelijk dat deze waarden als deze correct zijn ingesteld volledig relevant zijn voor onze DNS lookup-logica. Als u dit koppelt met de verklaringen van de plaatsingsgids voor de Hybride Call Services van Cisco Webex, zou u zien dat het DNS-verzoek wijzigen op **On** moet worden ingesteld en dat het domein om naar te zoeken op **callservice.ciscospark.com** moet worden ingesteld. Als u deze waarden zou veranderen om de juiste informatie te specificeren, zou de DNS SRV lookup-logica volledig anders zijn. Hieronder staat een fragment van wat je zou kunnen verwachten vanuit het perspectief van de Expressway-E diagnostische houtkap

```
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"
```

Oplossing

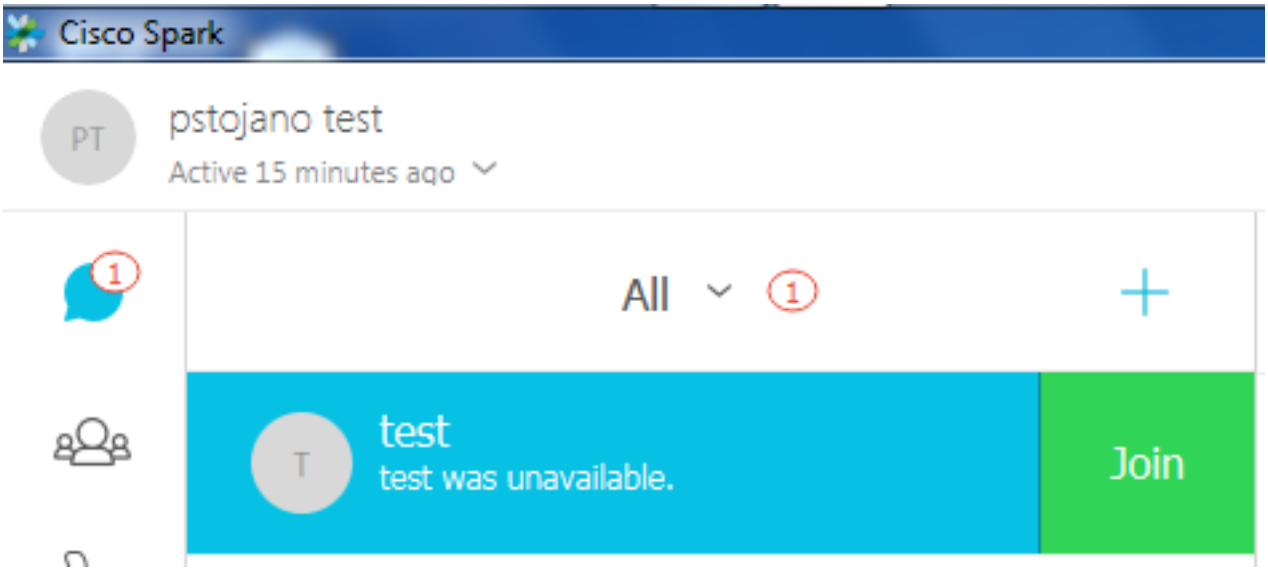
1. Inloggen bij de sneltoets
2. Navigeren in naar **Configuratiezones > Zones**
3. Selecteer de optie Webex Hybrid DNS-zone die is geconfigureerd
4. Stel het DNS-verzoek wijzigen in op **On**
5. Stel het domein in om naar waarde te zoeken op **callservice.ciscospark.com**
6. De wijzigingen opslaan

Opmerking: Als er op de snelweg slechts één DNS-zone wordt gebruikt, moet een afzonderlijke DNS-zone worden geconfigureerd voor gebruik met de hybride Call-service om gebruik te maken van deze waarden.

Eigen 2. Port 5062 is geblokkeerd naar Cisco Webex

Een ding dat uniek is aan de geforceerde uitbellen die uitvallen voor Cisco Webex is dat de app Cisco Webex van de opgeroepen partij een gezamenlijke knop op hun app presenteert alhoewel de client nooit ringen. Zoals het scenario hierboven, zal u voor deze kwestie opnieuw de zelfde gereedschappen en het registreren moeten gebruiken om te begrijpen waar de mislukking bestaat. Zie het gedeelte van dit artikel zoals in de afbeelding voor tips over het isoleren van gespreksproblemen en het analyseren van logbestanden.

Illustratie van de gezamenlijke toets die wordt gepresenteerd



Net zoals Uitgaande Call Issue #1 kan je de analyse starten bij de Expressway-E diagnostiek, omdat je de Search History op de expressway hebt gebruikt om te bepalen dat de oproep zo ver komt. Zoals eerder, begin met de eerste INVITE die in de Expressway-E van de Expressway-C komt. Vergeet niet dat je wilt zoeken naar:

1. of de expressway-E de INVITE ontvangt
2. Of de logica van de Zoeken de vraag naar de hybride DNS-zone doorgeeft
3. Of de DNS-zone het DNS-opnameproces uitvoert en op het juiste domein
4. Of het systeem een TCP-handshake voor Port 5062 heeft geprobeerd en juist heeft ingesteld
5. Of de Mutual TLS Handshake is geslaagd

```
2017-09-19T10:18:35.023-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 14:18:35,017"
Module="network.sip" Level="DEBUG":  Action="Received" Local-ip="192.168.1.6" Local-port="7003"
Src-ip="192.168.1.5" Src-port="26513" Msg-Hash="3732376649380137405"
 SIPMSG:
 |INVITE sip:pstojano-test@dmzlab.call.ciscospark.com SIP/2.0
 Via: SIP/2.0/TLS 192.168.1.5:5061;egress-
zone=HybridCallServiceTraversal;branch=z9hG4bK57d8d5c823824bcddfd62f6ff7e09f9939482.899441b6d60c
444e4ed58951d07b5224;proxy-call-id=696f6f1c-9abe-47f3-96a4-e26f649fb76f;rport
 Via: SIP/2.0/TCP 192.168.1.21:5065;branch=z9hG4bK12d4b77c97a64;received=192.168.1.21;ingress-
zone=CUCM11
 Call-ID: 6a48de80-9c11273a-12d08-1501a8c0@192.168.1.21
 CSeq: 101 INVITE
 Call-Info: <urn:x-cisco-remotecc:callinfo>;x-cisco-video-traffic-class=DESKTOP
 Remote-Party-ID: "Jonathan Robb"
<sip:5010@rtp.ciscotac.net>;party=calling;screen=yes;privacy=off
 Contact: <sip:5010@192.168.1.21:5065;transport=tcp>;video;audio
 From: "Jonathan Robb"



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



 Max-Forwards: 15
 Record-Route: <sip:proxy-call-id=696f6f1c-9abe-47f3-96a4-
```

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

Zoals u in het bovenstaande INVITE kunt zien, wordt het INVITE als normaal ontvangen. Dit is een "ontvangen" actie en het komt van het IP-adres Expressway-C. U kunt nu overgaan op Zoekregel Logic

```
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'"
```

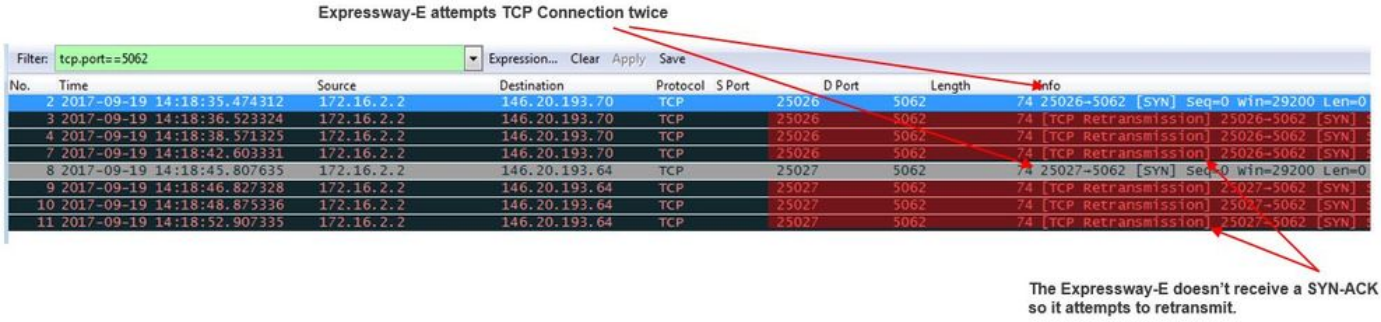
Gebaseerd op het logfragment hierboven, kunt u zien dat de Expressway-E door vier zoekregels is geparseerd maar slechts één regel *(Webex hybride - naar Webex Cloud)* werd overwogen. De zoekregel had een prioriteit van 90 en was bedoeld om naar de *DNS-zone voor hybride Call Services*. Nu de vraag naar een DNS Zone wordt verzonden, kunt u de DNS SRV-favorieten bekijken die op de Expressway-E plaatsvinden. Dit is allemaal heel normaal. U kunt zich nu richten op de DNS-opnamelogica

```
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"
```

U kunt duidelijk zien dat in dit geval het callservice.ciscospark.com SRV-record is opgelost. Het antwoord is vier verschillende geldige records die allemaal haven 5062 gebruiken. Dit is normaal gedrag. Op dit punt kan je nu de TCP handdruk analyseren die hierna zou moeten komen. Zoals eerder vermeld in het document, kunt u de diagnostische logbestanden naar "TCP verbinden" zoeken en naar het lijnitem zoeken dat de Dst-port="5062" toont. Hieronder zie je een voorbeeld van wat je in dit scenario ziet:

```
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"
```

U kunt ook de TCP-handdruk gebruiken die met de diagnostische logbundel was meegeleverd om meer gedetailleerde informatie te krijgen over de TCP-handdruk zoals in de afbeelding wordt weergegeven.



Op dit punt, kunt u concluderen dat de Expressway-E de vraag correct routeert. De uitdaging in dit scenario is dat een TCP verbinding niet met de Webex omgeving kan worden gevestigd. Dit zou kunnen gebeuren omdat de Webex-omgeving niet reageert op het TCP SYN-pakket maar dit is onwaarschijnlijk omdat de server die de verbinding verwerkt, wordt gedeeld tussen vele klanten. De waarschijnlijker oorzaak in dit scenario is een of ander type intermediair apparaat (firewall, IPS, enz.) dat het verkeer niet uit staat.

Oplossing

Omdat de kwestie geïsoleerd was, zouden deze gegevens aan de netwerkbeheerder van de klant moeten worden verstrekt. Daarnaast kunt u, als u meer informatie nodig hebt, de externe interface van het randapparaat en/of de firewall voor verder bewijs afdrukken. Vanuit het standpunt van de snelweg, is er geen verdere actie te ondernemen aangezien de kwestie niet op dat apparaat ligt.

Kwestie 3. Onjuiste configuratie van de standaard voor snelwegen

Onjuiste configuratie van de zoekregel is een van de grootste configuratie-gerelateerde problemen op de snelwegen. De configuratiekwesties van de zoekregel kunnen bidirectioneel zijn, omdat u zoekregels voor inkomende oproepen nodig hebt en u zoekregels voor uitgaande oproepen nodig hebt. Terwijl je door deze kwestie loopt, zul je ontdekken dat regex-kwesties vrij algemeen zijn op de expressweg, maar niet altijd de oorzaak zijn van een zoekregel-kwestie. In dit specifieke segment, zal je door een uitgaande roep lopen die faalt. Zoals al onze andere uitgaande geforceerde call scenario's, blijven de symptomen hetzelfde:

- De geroepen app Cisco Webex aangeboden
- De beltelefoon speelde een ring terug
- De telefoon van de opgeroepen gebruiker belde
- De app Cisco Webex van de genoemde gebruiker is nooit gebeld

Zoals alle andere scenario's, zult u ook CUCM SDL sporen samen met Expressway-C en E diagnostische logs willen gebruiken. Zoals eerder, zou u de voor hefboomgeschiedenis en tips van het hefboomeffect van de Geschiedenis van het Onderzoek moeten verwijzen voor het identificeren van een vraag in de diagnostische logboeken. Zoals eerder, werd het bepaald aan de

hand van de Expressway-E Search History dat deze oproep het daar maakte en faalde. Hieronder staat het begin van de analyse waarvoor we kijken naar de eerste SIP INVITE die vanuit de expressway-E in de Expressway-C komt.

```
2017-09-25T11:26:02.959-04:00 amer-expressway01 tvcs: UTCTime="2017-09-25 15:26:02,959"
Module="network.sip" Level="DEBUG":  Action="Received" Local-ip="192.168.1.6" Local-port="7003"
Src-ip="192.168.1.5" Src-port="25675" Msg-Hash="1536984498381728689"
 SIPMSG:
 |INVITE sip:pstojano-test@dmzlab.call.ciscospark.com SIP/2.0
 Via: SIP/2.0/TLS 192.168.1.5:5061;egress-
zone=HybridCallServiceTraversal;branch=z9hG4bK1c7bf93ff08014ca5e00bb0b5f8b184b272412.a81f2992e38
63ac202a000a3dd599763;proxy-call-id=f79b8631-947b-46d4-a888-911bf0150bfe;rport
 Via: SIP/2.0/TCP 192.168.1.21:5065;branch=z9hG4bK1c8c419938648;received=192.168.1.21;ingress-
zone=CUCM11
 Call-ID: d58f2680-9c91200a-1c7ba-1501a8c0@192.168.1.21
 CSeq: 101 INVITE
 Call-Info: <urn:x-cisco-remotecc:callinfo>;x-cisco-video-traffic-class=DESKTOP
 Remote-Party-ID: "Jonathan Robb"
<sip:5010@rtp.ciscotac.net>;party=calling;screen=yes;privacy=off
 Contact: <sip:5010@192.168.1.21:5065;transport=tcp>;video;audio
 From: "Jonathan Robb"




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




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

<SDP Omitted>
```

Met behulp van de Call-ID (**d58f2680-9c91200a-1c7ba-1501a8c0**) van de SIP-header kunt u snel alle berichten zoeken die bij deze dialoog horen. Wanneer je kijkt naar de derde hit in de blogs voor de Call-ID, zie je dat de Expressway-E direct een **404 Not** to the Expressway-C verstuurt.

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

```
 |SIP/2.0 404 Not Found
 Via: SIP/2.0/TLS 192.168.1.5:5061;egress-
zone=HybridCallServiceTraversal;branch=z9hG4bK1c7bf93ff08014ca5e00bb0b5f8b184b272412.a81f2992e38
63ac202a000a3dd599763;proxy-call-id=f79b8631-947b-46d4-a888-
911bf0150bfe;received=192.168.1.5;rport=25675;ingress-zone=HybridCallServiceTraversal
 Via: SIP/2.0/TCP 192.168.1.21:5065;branch=z9hG4bK1c8c419938648;received=192.168.1.21;ingress-
zone=CUCM11
 Call-ID: d58f2680-9c91200a-1c7ba-1501a8c0@192.168.1.21
 CSeq: 101 INVITE
 From: "Jonathan Robb"




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




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

Deze gegevens vertellen je twee dingen:

1. De sneltoets heeft nooit geprobeerd om INVITE naar Cisco Webex te sturen
2. De Expressway-E was de verantwoordelijke partij voor het nemen van het logische besluit om de oproep te verwerpen met een 404 Not Found-fout.

Een fout van 404 niet gevonden betekent over het algemeen dat de snelweg niet in staat is om het doeladres te vinden. Aangezien de snelheden zoekregels gebruiken om oproepen tussen zichzelf en verschillende omgevingen te verplaatsen, begin door te focussen op de xConfiguration van de expressway-E. Binnen deze xConfiguration kunt u de zoekregel zoeken die de oproep naar de Webex Hybrid DNS Zone moet doorgeven. Om de zoekregels te vinden die op de sneltoets vanuit het xConfiguration-perspectief zijn ingesteld, kunt u naar "xConfiguration Zones Policy SearchRegels" zoeken door dit te doen, ziet u een lijst met de configuratie van de zoekregel voor elke zoekregel die op de expressway is gemaakt. Het nummer dat na de 'Regel' komt, wordt verhoogd op basis van de zoekregel die eerst werd gemaakt, die wordt gemarkeerd 1. Als je moeite hebt de zoekregel te vinden. U kunt veel gebruikte naamgevingswaarden zoals "*Webex*" gebruiken om de zoekregel beter te vinden. Een andere manier om de regel te identificeren is het vinden van de waarde van de Pattern String die is ingesteld op ".*@.*\.ciscospark\.com". Dat is de Patronenreeks die verondersteld wordt te worden geconfigureerd. *(aangenomen dat de Patronenstring correct is geconfigureerd)*Na het bekijken van de xConfiguration van dit scenario, kunt u zien dat Search Rule 6 de juiste regel is om de vraag naar Cisco Webex toe te passen.

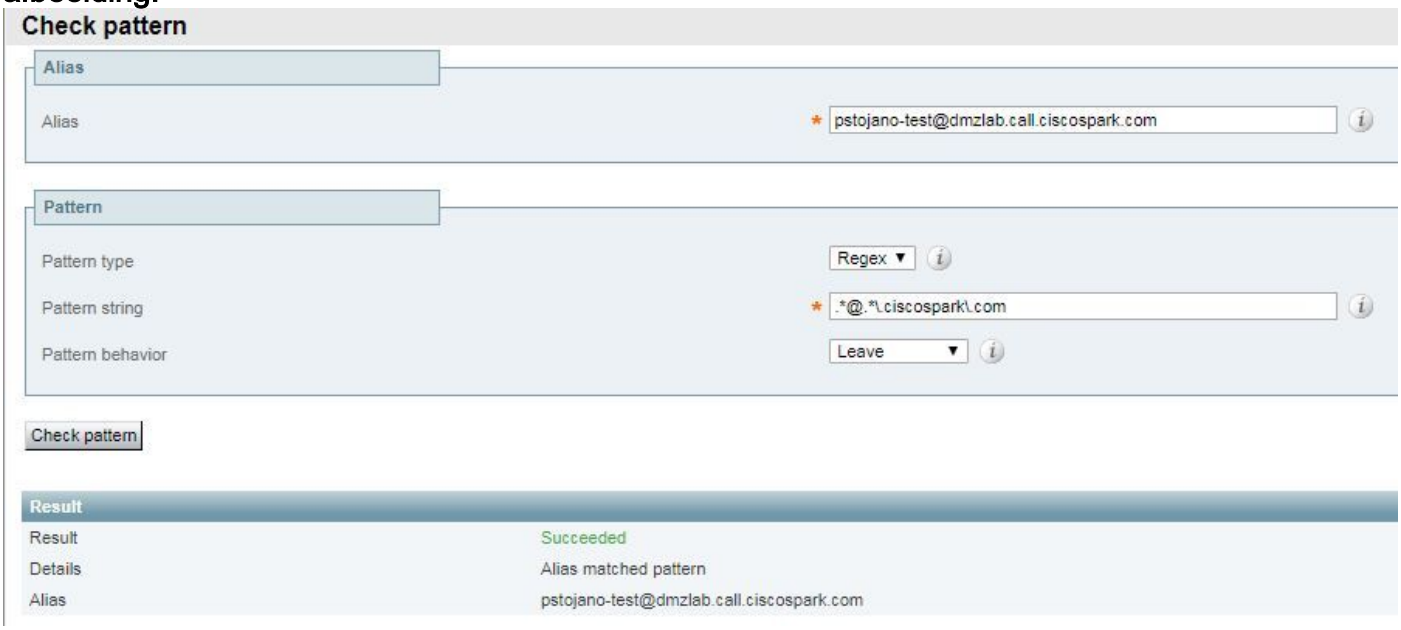
```
*c xConfiguration Zones Policy SearchRules Rule 6 Authentication: "No"
*c xConfiguration Zones Policy SearchRules Rule 6 Description: "Outbound calls to Webex"
*c xConfiguration Zones Policy SearchRules Rule 6 Mode: "AliasPatternMatch"
*c xConfiguration Zones Policy SearchRules Rule 6 Name: "Webex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

```
*c xConfiguration Zones Policy SearchRules Rule 6 State: "Enabled"
*c xConfiguration Zones Policy SearchRules Rule 6 SystemGenerated: "No"
*c xConfiguration Zones Policy SearchRules Rule 6 Target Name: "Hybrid Call Services DNS"
*c xConfiguration Zones Policy SearchRules Rule 6 Target SIPVariant: "Any"
*c xConfiguration Zones Policy SearchRules Rule 6 Target Type: "Zone"
```

Om dit patroon te testen, kunnen we de functie Patroon controleren gebruiken die in het document wordt beschreven. De belangrijke oproep hier is dat we de volgende waarden willen configureren:Onderhoud > Gereedschappen > Controleer het patroon

- Alias: %Verzoek URI in eerste INVITE% (Ex: leaving pstojano-test@dmzlab.call.ciscospark.com)
- Patroontype: Regex
- Patroonstring.*@\.ciscospark\.com
- Patroongedrag: vertrekken

Als Regex voor de regel correct is ingesteld, moet u het resultaat van dit patroon van de controle Success zien. Hieronder zie je een afbeelding die dit aantoont zoals in de afbeelding:



Nu u kunt bevestigen dat de zoekregel aanwezig en correct ingesteld is, kunt u dichter in de zoeklogica kijken dat de snelweg uitvoert om te bepalen of het de expressway-E beïnvloedt die de 404 Not Found verstuurt. Hieronder zie je een voorbeeld van de zoekregel logica die de Expressway uitvoerde.

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

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

```
Name="_sips._tcp.dmzlab.call.ciscospark.com" Type="SRV (IPv4 and IPv6)"
```

In deze steekproef kan je zien dat de snelweg vier zoekregels verwerkt. De eerste 3 werden om verschillende redenen niet in aanmerking genomen, maar de vierde werd wel in overweging genomen. Het interessante is dat onmiddellijk na het overwegen van de Expressway recht springt naar DNS lookup-logica. Als u zich herinnert wat we in de xConfiguration hadden gezien, werd de zoekregel die voor Webex Hybrid was ingesteld, Webex Hybrid genoemd - naar Webex Cloud en werd deze regel niet eens in deze zoekregel logica hierboven overwogen. Op dit punt is het de moeite waard om te onderzoeken hoe de overwogen zoekregel (naar DNS) is geïmplementeerd, zodat u beter kunt begrijpen of deze van invloed is op het gebruik van de Hybrid Webex-zoekregel. Om dat te doen, kunt u de xConfig dit keer opnieuw bekijken op zoek naar de zoekregel met de naam "DNS"

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

Na het bekijken van deze zoekregel kunt u het volgende concluderen:

- De patroonstring zou overeenkomen met Cisco Webex Application URI
- De prioriteit is vastgesteld op 100
- De Progress (Patronengedrag) wordt ingesteld op Stop.

Wat deze informatie ons vertelt is dat de URI van het Cisco Webex-verzoek dat wordt opgeroepen deze regel zou evenaren en als de regel was aangepast zou de Expressway niet meer zoeken (Gezien) andere zoekregels. Met dit begrip wordt de prioriteit van de regels een sleutelfactor. De manier waarop de voorrang van de regel van het Onderzoek van de snelweg werkt is de laagste prioritaire regel wordt eerst gepoogd. Hieronder zie je een voorbeeld.Zoekregel: LokaalPatroongedrag: DoorgaanPrioriteit 1Zoekregel: buurvrouwPatroongedrag: DoorgaanPrioriteit 10Zoekregel: DNSPatroongedrag: StoppenPrioriteit 50In dit voorbeeld, zou eerst de zoekregel genaamd Local (1) worden geprobeerd en als een match werd gevonden zou deze overgaan op Search Rule buurman (10) vanwege het Patroontgedrag dat wordt ingesteld op Doorgaan. Als de zoekregel buurman niet was aangepast, zal deze toch DNS (50) van de Zoekregel blijven zoeken en dat als laatste beschouwen. Als Zoekregel DNS is aangepast, zal de zoekfunctie stoppen ongeacht of er een andere zoekregel is met een prioriteit hoger dan 50, omdat Patroongedrag is ingesteld op Stop. Met dit begrip kunt u de prioriteiten van de Zoeken tussen de regels "DNS" en "Webex Hybrid - to Webex Cloud" bekijken.

```
*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 ziet u dat de "to DNS"-regel een lagere prioriteit heeft dan de "Webex Hybrid - to Webex

Cloud"-regel — en daarom wordt de "to DNS"-regel eerst geprobeerd. Gezien het feit dat het Patronengedrag (Progress) is ingesteld om op te houden, overweegt de Expressway-E nooit de Webex Hybrid - naar de Webex Cloud-regel en is de oproep uiteindelijk mislukt. OplossingDit type probleem komt steeds vaker voor bij een verbinding met de hybride gesprekservice. Vaak wanneer de oplossing wordt uitgevoerd, creëren mensen een hoge prioriteit om voor de onderzoeken van Cisco Webex te gebruiken. Vaak wordt deze regel niet ingeroepen door bestaande lagere prioriteitsregels. Ze worden aangepast en resulteert in een mislukking. Dit probleem gebeurt op zowel inkomende als uitgaande oproepen naar Cisco Webex. Om dit op te lossen, moet u deze stappen volgen:

1. Inloggen bij de sneltoets
2. Navigeren in configuratie > Kiesschema > Zoeken regels
3. Vind de Hybride Webex-zoekregel en klik op deze *(bijvoorbeeld: Name: Webex hybride - tot Webex Cloud)*
4. Stel de prioriteitswaarde in op iets lager dan andere zoekregels, toch hoog genoeg, zodat het geen impact heeft op anderen. *(Ex: Prioriteit: 99)*

De algemene regel van duim met de regels van het Zoeken is meer specifiek de "Pattern string", hoe lager het kan worden geplaatst in de prioriteitenlijst van de Zoeken. Over het algemeen wordt een DNS Zone ingesteld met een Patronenreeks die alles gaat vangen dat geen lokaal domein is en het naar het internet stuurt. Daarom raden we u aan om dat type zoekregel op een hoge prioriteit in te stellen zodat deze als laatste wordt ingeroepen. 4. Misconfiguratie van de CPL-uitdrukkingDe oplossing van de Uitdrukking maakt het mogelijk om te compenseren voor Toll Fraud door gebruik te maken van de logica van de Verwerkingstaal (CPL) van de Vraag die op de server beschikbaar is. Als de oplossing van de Uitdrukking die wordt opgesteld slechts voor de Hybride de Dienst van de Vraag van Cisco Webex en Mobiel & Externe Toegang wordt gebruikt, adviseren wij sterk dat het beleid en de regels van de CPL worden toegelaten en ten uitvoer gelegd. Terwijl de configuratie van CPL op de Uitdrukking voor de Hybride van Cisco Webex vrij eenvoudig is, als zij misplaatst is kan zij makkelijk vraagpogingen van het gebeuren blokkeren. De scenario's hieronder tonen u hoe u de diagnostische houtkap gebruikt om een misconfiguratie van CPL te identificeren.Zoals alle andere uitgaande geforkeerde call scenario's, bleven de symptomen hetzelfde:

- De app Cisco Webex van de opgeroepen gebruiker heeft een gezamenlijke knop gepresenteerd
- De telefoon speelde een ring terug
- De telefoon die de gebruiker ter plekke had belde
- De app van de opgeroepen gebruiker is nooit gebeld

Zoals alle andere scenario's, kunt u de sporen van CUCM SDL samen met Expressway-C en E diagnostische logbestanden gebruiken. Zoals voorheen, dient u de voor het gebruik van zoekgeschiedenis en tips voor het identificeren van een vraag in de diagnostische logbestanden. Zoals eerder, werd het bepaald aan de hand van de Expressway-E Search Geschiedenis dat deze oproep daar aankwam en faalde. Hieronder staat het begin van de analyse waarin je een blik kunt werpen op de eerste SIP INVITE die vanuit de expressway-E in de Expressway-C komt.

```
2017-09-25T16:54:43.722-04:00 amer-expressway01 tvcs: UTCTime="2017-09-25 20:54:43,722"
Module="network.sip" Level="DEBUG":  Action="Received" Local-ip="192.168.1.6" Local-port="7003"
Src-ip="192.168.1.5" Src-port="26404" Msg-Hash="17204952472509519266"
 SIPMSG:
 |INVITE sip:pstojano-test@dmzlab.call.ciscospark.com SIP/2.0
 Via: SIP/2.0/TLS 192.168.1.5:5061;egress-
zone=HybridCallServiceTraversal;branch=z9hG4bK781a130d234ed9aaec868343687394302832 56.34216c32a0d
e36e16590bae36df388b6;proxy-call-id=3bbbf94a-082e-4088-8f5a-5ea7e82f8aac;rport
 Via: SIP/2.0/TCP 192.168.1.21:5065;branch=z9hG4bK1cf344a8b117e;received=192.168.1.21;ingress-
zone=CUCM11
 Call-ID: c030f100-9c916d13-1cdcb-1501a8c0@192.168.1.21
 CSeq: 101 INVITE
```

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




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




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

<SDP Omitted>
```

Met de Call-ID (c030f100-9c916d13-1cdcb-1501a8c0) van de SIP-header zoekt u snel alle berichten die bij dit dialoogvenster horen. Wanneer je kijkt naar de derde hit in de blogs voor de Call-ID, zie je dat de Expressway-E direct een 403 Verboden naar de Expressway-C stuurt.

```
2017-09-25T16:54:43.727-04:00 amer-expressway01 tvcs: UTCTime="2017-09-25 20:54:43,727"
Module="network.sip" Level="DEBUG":  Action="Sent" Local-ip="192.168.1.6" Local-port="7003" Dst-
ip="192.168.1.5" Dst-port="26404" Msg-Hash="91954361011l0134622"
 SIPMSG:
 |SIP/2.0 403 Forbidden
 Via: SIP/2.0/TLS 192.168.1.5:5061;egress-
zone=HybridCallServiceTraversal;branch=z9hG4bK781a130d234ed9aaec868343687394302832S6.34216c32a0d
e36e16590bae36df388b6;proxy-call-id=3bbbf94a-082e-4088-8f5a-
5ea7e82f8aac;received=192.168.1.5;rport=26404;ingress-zone=HybridCallServiceTraversal
 Via: SIP/2.0/TCP 192.168.1.21:5065;branch=z9hG4bK1cf344a8b117e;received=192.168.1.21;ingress-
zone=CUCM11
 Call-ID: c030f100-9c916d13-1cdcb-1501a8c0@192.168.1.21
 CSeq: 101 INVITE
 From: "Jonathan Robb"




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

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

Om te begrijpen waarom de Expressway-E deze oproep ontkende en een 403 Verboden fout naar de Expressway-C stuurde, wil je de loggegevens analyseren tussen de 403 Verboden en de oorspronkelijke SIP INVITE die in de Expressway is ingevoerd. Door deze logingangen te analyseren, kan je doorgaans alle logische beslissingen zien die worden genomen. Merk op dat u geen zoekregels ziet die worden aangehaald, maar u ziet de CPL-logica (Call Processing Language) gebruiken. Hieronder staat een fragment uit de video.

```
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:
```

```
          "
```

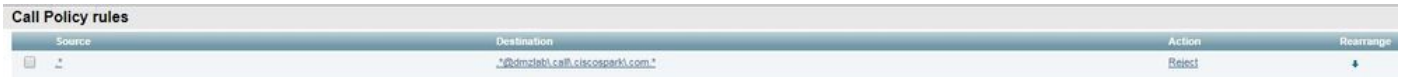
Gebaseerd op de hierboven beschreven loganalyse. u kunt bepalen dat de CPL de oproep afwijst.

```
2017-09-25T16:54:43.725-04:00 amer-expressway01 tvcs: Event="Search Completed"
Reason="Forbidden" Service="SIP" Src-alias-type="SIP" Src-alias="5010@rtp.ciscotac.net" Dst-
alias-type="SIP" Dst-alias="sip:pstojano-test@dmzlab.call.ciscospark.com" Call-serial-
number="48c80582-ec79-4d89-82e2-e5546f35703c" Tag="4fffefed-0512-4067-ac8c-35828f0a1150"
Detail="found:false, searchtype:INVITE, Info:Policy Response" Level="1" UTCTime="2017-09-25
20:54:43,726"
2017-09-25T16:54:43.725-04:00 amer-expressway01 tvcs: Event="Call Rejected" Service="SIP" Src-
ip="192.168.1.5" Src-port="26404" Src-alias-type="SIP"
```

*Opmerking: In deze situatie ziet u Zoekregels niet worden aangehaald omdat CPL's, FindMe en Transforms allemaal worden verwerkt vóór een zoekregel*Onder de meeste omstandigheden, kunt u de xConfig van de expressweg gebruiken om de omstandigheden beter te begrijpen. Echter, voor CPLs kunt u de Regels niet zien die worden bepaald, slechts als het beleid wordt toegelaten. Hieronder zie je het gedeelte van de xConfig dat ons toont dat deze Expressway-E de lokale CPL-logica gebruikt.

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

Om de regelconfiguratie beter te begrijpen, moet u in de sneltoets indrukken-E inloggen en naar Configuration > Call Policy > Regels navigeren zoals in de afbeelding.



Tijdens het bekijken van deze configuratie kunt u zien dat het volgende is ingesteldBron: .*Bestemming: .*@dmzlab\.call\.ciscospark\.com.*Actie: afwijzenVergeleken met wat in de *Cisco Webex Hybrid Call Service Deployment Guide* is gedocumenteerd, kunt u zien dat de Bron en de Bestemming achterin zijn
geconfigureerd.

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

OplossingOm dit probleem op te lossen, moet u de CPL regelconfiguratie aanpassen zodat de Bron wordt ingesteld op .*@%Webex_subdomein%\.ciscospark\.com.* en het Destination Pattern is .*

1. Inloggen bij de sneltoets
2. Navigeren in configuratie > Call Policy > Regels
3. Selecteer de regel die is ingesteld voor de Hybride Cisco Webex-gespreksservice
4. Voer het bronpatroon in als .*@%Webex_subdomein%\.call\.ciscospark\.com.*(Ex: .*@dmzlab\.call\.ciscospark\.com).
5. Voer het bestemmingspatroon in als .*
6. Selecteer Opslaan

Raadpleeg de Cisco Webex Hybrid Design Guide voor meer informatie over de CPL-implementatie voor Webex Hybrid. Bidirectioneel: Cisco Webex aan inbedrijfstelling of aan inbedrijfstelling bij Cisco Webex Vraag 1. IP-telefoon/collaboration-endpoint biedt een audio-codec aan die niet gelijk is aan G.711, G.722 of AAC-LD.Hybride Call Service Connect ondersteunt drie verschillende audio-codecs: G.711, G.722 en AAC-LD. Om een gesprek met de Cisco Webex-omgeving op te zetten, moet een van deze audio-codecs worden gebruikt. De omgeving in de fabriek kan worden ingesteld om veel soorten audio-codecs te gebruiken maar tegelijkertijd kan worden ingesteld om ze te beperken. Dit kan opzettelijk of onbedoeld gebeuren door het gebruik van aangepaste en/of standaardinstellingen voor gebieden op de Unified CM. Voor dit specifieke gedrag kunnen de houtkappatronen verschillen op basis van de richting van de oproep en als de Unified CM is ingesteld om vroege of vertraagde aanbiedingen te gebruiken. Hieronder zie je wat voorbeelden van situaties waarin dit gedrag zich zou kunnen voordoen:

1. Cisco Webex stuurt een inkomende INVITE met SDP die G.711, G.722 of AAC-LD biedt. De snelweg-C stuurt dit bericht naar Unified CM maar Unified CM is ingesteld om G.729 alleen toe te staan voor deze oproep. Dus, Unified CM wijst het gesprek af omdat er geen codec beschikbaar is.
2. Unified CM probeert de uitgaande vraag zoals *vroege offer* aan Cisco Webex te bieden. Dit betekent de eerste INVITE die naar de Expressway-C wordt verstuurd, zal SDP ALLEEN SDP bevatten dat G.729-audio ondersteunt. Cisco Webex verstuurt vervolgens een 200 OK met SDP die de audio (*m=audio 0 RTP/SAVP*) uitlekt omdat het G.729 niet ondersteunt. Zodra de Expressway-C deze INVITE aan Unified CM doorgeeft, beëindigt Unified CM de oproep omdat er geen beschikbare codec is.

3. Unified CM probeert de uitgaande vraag zoals *vertraagd* aanbod aan Cisco Webex te doen wat betekent dat de eerste INVITE die naar de snelweg-C wordt verstuurd geen SDP zal bevatten. Cisco Webex verstuurt vervolgens een 200 OK met SDP die alle ondersteunde audio-codecs van Cisco Webex bevat. De snelweg-C verstuurt deze 200 OK naar Unified CM maar Unified CM is alleen ingesteld om G.729 alleen toe te staan voor deze oproep. Dus, Unified CM wijst het gesprek af omdat er geen codec beschikbaar is.

Als u probeert een storing in de oproepen van de Hybride Call Service Connect te identificeren die deze kwestie aansluit, moet u de expresslogboeken naast Unified CM SDL sporen krijgen. De logopnamen van het voorbeeld hieronder komen overeen met situatie #2 waarin Unified CM de uitgaande oproep als *vroege aanbieding* probeert. Omdat we weten dat de oproep naar Cisco Webex gaat, begint de loganalyse op de Expressway-E.Hier volgt een fragment van de eerste INVITE-bewerking op Cisco Webex. U kunt zien dat de favoriete audio-codec is ingesteld op G.729 (payload 18). De 101 is voor DTMF en voor dit specifieke scenario is dat niet 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-55aedea256d2;rport
Via: SIP/2.0/TLS 172.16.2.2:5073;branch=z9hG4bK350703fe46645f0acddef05b35adc5c157;x-cisco-local-
service=nettle;received=172.16.2.2;rport=41511;ingress-zone=DefaultZone
Via: SIP/2.0/TLS 192.168.1.6:5061;egress-
zone=DefaultZone;branch=z9hG4bKf71f2bf47233d6ca52b579364594ac6c1114.a402e3f25603f5a77b60b17ea47d
bf72;proxy-call-id=be17a470-0bca-4ad5-8a6c-14872e007efb;received=192.168.1.6;rport=25025
Via: SIP/2.0/TLS 192.168.1.5:5061;egress-
zone=HybridCallServiceTraversal;branch=z9hG4bKfcf4cfd09d213a88bd2331cef0bc82b540559.494a140082bd
66357134b9eed4335df8;proxy-call-id=d4d4e950-babc-45d5-a4a7-
c60a8b17a8bd;received=192.168.1.5;rport=26513;ingress-zone=HybridCallServiceTraversal
Via: SIP/2.0/TCP 192.168.1.21:5065;branch=z9hG4bK12dd82194c4f7;received=192.168.1.21;ingress-
zone=CUCM11
Call-ID: 44bdd400-9c112db1-12d95-1501a8c0@192.168.1.21
CSeq: 101 INVITE
Remote-Party-ID: "Jonathan Robb" <sip:5010@rtp.ciscotac.net>;privacy=off;screen=no;party=calling
Contact: <sip:172.16.2.2:5073;transport=tls>;video;audio
From: "Jonathan Robb"
Max-Forwards: 14
Record-Route: <sip:proxy-call-id=a3a78ee2-c01b-4741-b29b-
55aedea256d2@64.102.241.236:5062;transport=tls;lr>
Record-Route: <sip:proxy-call-id=a3a78ee2-c01b-4741-b29b-
55aedea256d2@172.16.2.2:5061;transport=tls;lr>
Allow: INVITE,ACK,BYE,CANCEL,INFO,OPTIONS,REFER,SUBSCRIBE,NOTIFY
User-Agent: TANDBERG/4352 (X8.10.2-b2bua-1.0)
Supported: X-cisco-srtp-fallback,replaces,timer
Session-Expires: 1800;refresher=uac
Min-SE: 500
X-TAATag: 14a0bd87-1825-4ecf-9f3d-4a23cfa69725
Session-ID: 75957d4fb66a13e835c10737aa329445;remote=00000000000000000000000000000000
Content-Type: application/sdp
Content-Length: 1407

v=0
o=tandberg 0 1 IN IP4 64.102.241.236
s=-
```

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

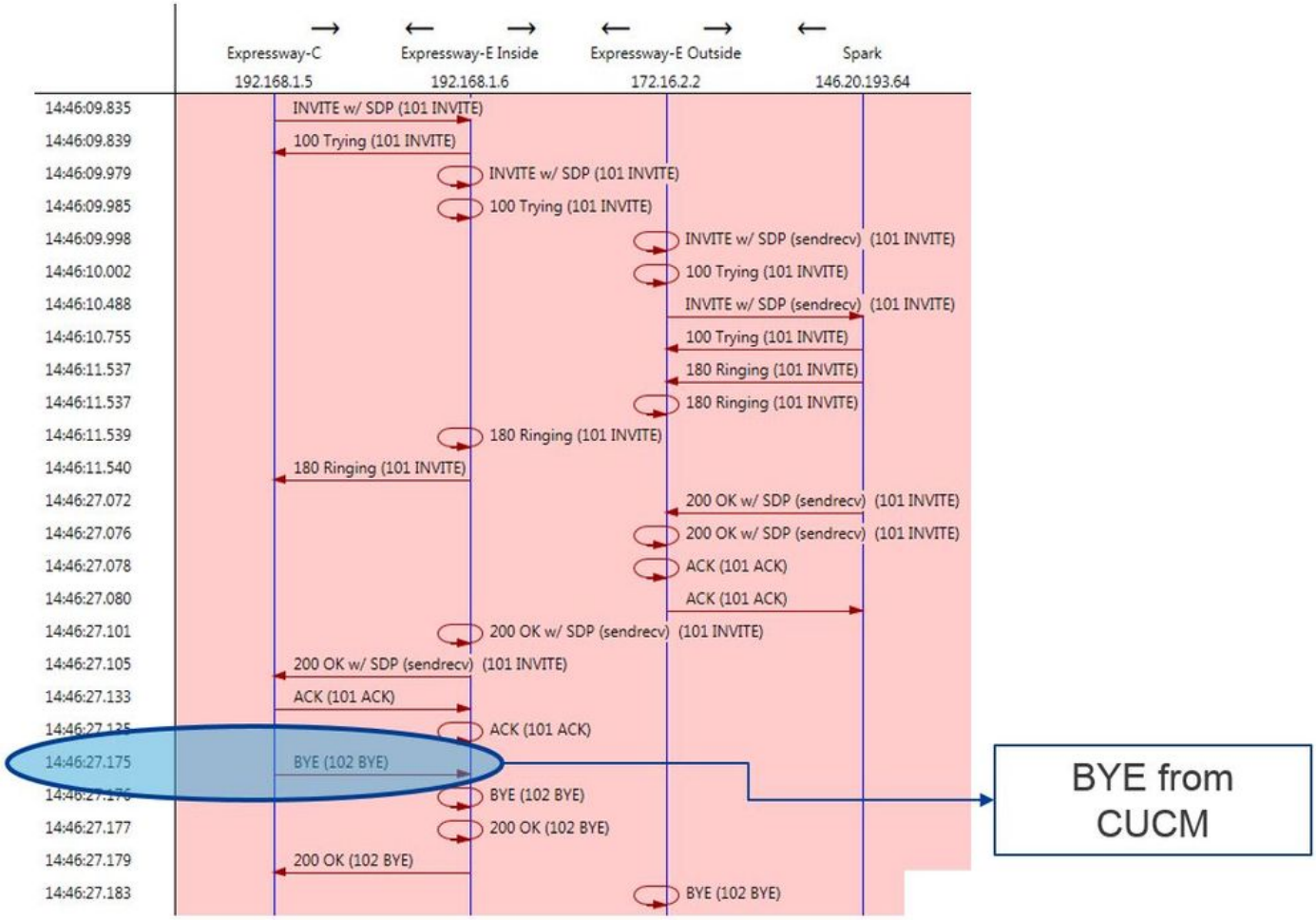
In antwoord op deze eerste INVITE reageert Cisco Webex met een 200 OK-bericht. Als u nader naar dit bericht kijkt, kunt u zien dat de audio-codec op nul is gezet. Dit is een probleem omdat zonder een audio poort die is toegewezen, de oproep niet in staat zal zijn om die stroom te onderhandelen.

```
2017-09-19T10:46:27.073-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 14:46:27,072"
Module="network.sip" Level="DEBUG":  Action="Received" Local-ip="172.16.2.2" Local-port="25034"
Src-ip="146.20.193.64" Src-port="5062" Msg-Hash="5236578200712291002"
SIPMSG:
SIP/2.0 200 OK
Via: SIP/2.0/TLS 64.102.241.236:5062;egress-
zone=HybridCallServicesDNS;branch=z9hG4bK323e6b15ad0cbbf409751f67848136fa1115;proxy-call-
id=a3a78ee2-c01b-4741-b29b-55aedea256d2;rport=38245;received=192.168.5.26,SIP/2.0/TLS
172.16.2.2:5073;branch=z9hG4bK350703fe46645f0acddef05b35adc5c157;x-cisco-local-
service=nettle;received=172.16.2.2;rport=41511;ingress-zone=DefaultZone,SIP/2.0/TLS
192.168.1.6:5061;egress-
zone=DefaultZone;branch=z9hG4bKf71f2bf47233d6ca52b579364594ac6c1114.a402e3f25603f5a77b60b17ea47d
bf72;proxy-call-id=be17a470-0bca-4ad5-8a6c-
14872e007efb;received=192.168.1.6;rport=25025,SIP/2.0/TLS 192.168.1.5:5061;egress-
zone=HybridCallServiceTraversal;branch=z9hG4bKfcf4cfd09d213a88bd2331cef0bc82b540559.494a140082bd
66357134b9eed4335df8;proxy-call-id=d4d4e950-babc-45d5-a4a7-
c60a8b17a8bd;received=192.168.1.5;rport=26513;ingress-
zone=HybridCallServiceTraversal,SIP/2.0/TCP
192.168.1.21:5065;branch=z9hG4bK12dd82194c4f7;received=192.168.1.21;ingress-zone=CUCM11
Call-ID: 44bdd400-9c112db1-12d95-1501a8c0@192.168.1.21
CSeq: 101 INVITE
Contact: "l2sip-UA" <sip:l2sip-UA@l2sip-cfa-01.wbx2.com:5062;transport=tls>
From: "Jonathan Robb"
```

```
Record-Route: <sip:l2sip-cfa-01.wbx2.com:5062;transport=tls;lr>,<sip:proxy-call-id=a3a78ee2-
c01b-4741-b29b-55aedea256d2@64.102.241.236:5062;transport=tls;lr>,<sip:proxy-call-id=a3a78ee2-
c01b-4741-b29b-55aedea256d2@172.16.2.2:5061;transport=tls;lr>
Allow: INVITE,ACK,CANCEL,BYE,REFER,INFO,OPTIONS,NOTIFY,SUBSCRIBE
User-Agent: Cisco-L2SIP
Supported: replaces
Accept: application/sdp
Allow-Events: kpml
Session-ID: ed35426ed3ade6fdc3b058792333df2b;remote=75957d4fb66a13e835c10737aa329445
Locus: 4711a33f-9d49-11e7-9bf6-dea12d0f2127
Locus-Type: CALL
Content-Type: application/sdp
Content-Length: 503

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

U kunt TranslatorX nu gebruiken om de rest van het dialoogvenster te bekijken. U kunt zien dat het dialoogvenster zelf wordt voltooid met een ACK. Het probleem is direct nadat het dialoogvenster is voltooid, er is een BYE die afkomstig is uit de richting van de expressway-C zoals in de
afbeelding.



Hier volgt een gedetailleerd voorbeeld van het BYE-bericht. U kunt duidelijk zien dat de User-Agent Cisco-CUCM11.5 is, wat betekent dat het bericht door de Unified CM is gegenereerd. Een ander ding om op te merken is dat de Reason-code is ingesteld om=47 te veroorzaken. De algemene vertaling hiervoor is geen bron beschikbaar.

```
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
```

Omdat de component Cisco Webex de audio-codec voor deze Callmonster op nul heeft gezet, moet de nadruk op:a. Het eerste INVITE dat naar Cisco Webex is verzonden enb. Wat was de logica die Cisco Webex gebruikte om die poort op nul te stellen.Bekijk nu wat uniek is aan de

eerste INVITE wat opgemerkt kan worden is dat het alleen G.729 bevat. Wanneer u dit weet, bekijk dan de Cisco Webex Hybrid Call Service Deployment Guide en herzie specifiek het hoofdstuk Voorbereiden van uw omgeving, waar stap 5 van de Complete de vereisten voor de hybride Call Service Connect-sectie de specifieke codecs aanwijst die worden ondersteund. Daar zouden we dit zien:Cisco Webex ondersteunt de volgende codecs:

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

Opmerking: Opus wordt niet gebruikt op het onuitgangspunt van de vraag voor de Hybride Vraag van Cisco Webex. Met deze informatie kunt u tot de conclusie komen dat Unified CM een niet-ondersteunde audio-codec verzenden die de reden is dat Cisco Webex de poort op nul zet. Oplossing:Om deze specifieke situatie aan te pakken, kunt u de regionale configuratie tussen de Cisco Webex RD die de oproep op gebouwen en de SIP Trunk voor de snelweg-C verankerd heeft moeten herzien. Om dit te doen, moet u bepalen in welke apparaatpool deze twee elementen zich bevinden. De apparaatpool bevat de tekeningen van de regio's. U kunt het kinderslot van de sneltoets indrukken-C SIP als volgt bepalen:

1. Meld u aan bij de Unified CM.
2. Navigeer naar apparaat > Trunk.
3. Zoek de Trunk-naam of klik op Zoeken.
4. Selecteer de autosnelweg-C romp.
5. Registreer de naam van het apparaat.

U kunt de apparaatpool van de CTI-RD of Cisco Webex-RD die de oproep bevestigde, als volgt bepalen:

1. Navigeren naar apparaat > telefoon.
2. Bij het zoeken kunt u Apparaattype selecteren bevat Webex of CTI Remote Devices (afhankelijk van wat de klant gebruikt).
3. Registreer de naam van het apparaat.

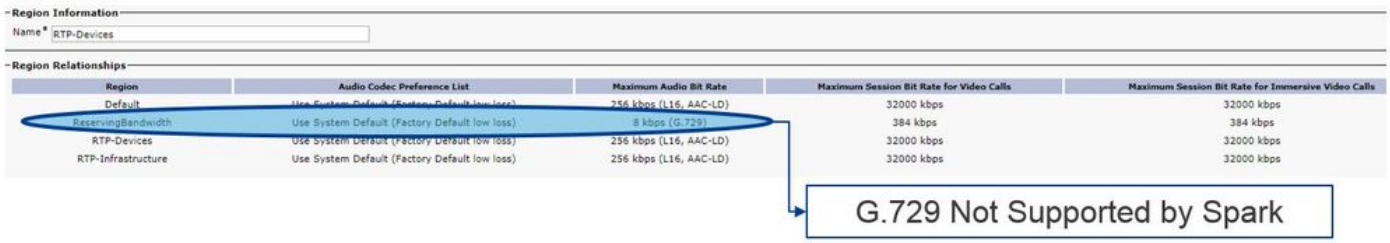
Bepaal het gebied dat aan elk apparaat is bevestigd:

1. Navigeren in op Systeem > Apparaatpool.
2. Zoek naar de apparaatpool die gebruikt wordt voor de snelweg-C SIP Trunk.
3. Klik op het apparaatpaneel.
4. Noteer de naam van het gebied.
5. Zoek de apparaatpool die gebruikt wordt voor Webex-RD of CTI-RD.
6. Klik op het apparaatpaneel.
7. Noteer de naam van het gebied.

Bepaal de regionale relatie:

1. Navigeer naar Systeem > Gebiedsinformatie > Gebied.
2. Zoeken op een van de genoemde regio's.
3. Bepaal of er een regionaal verband is tussen beide regio's die G.729 gebruiken.

Op dit punt, als u de relatie identificeert die G.729 gebruikt, zult u de relatie moeten aanpassen om de ondersteunde audio codecs te ondersteunen die Cisco Webex gebruikt of een andere Apparaatpool moet gebruiken die dit ondersteunt. In het hierboven beschreven scenario werd het volgende bepaald:gebied met snelweg-C Trunk: ReserveringBandbreedteWebex-RD regio: RTP-apparatenHier is een grafische illustratie van het verband tussen de RTP-apparaten en de ReservingBandwidth-regio's zoals in de
afbeelding.



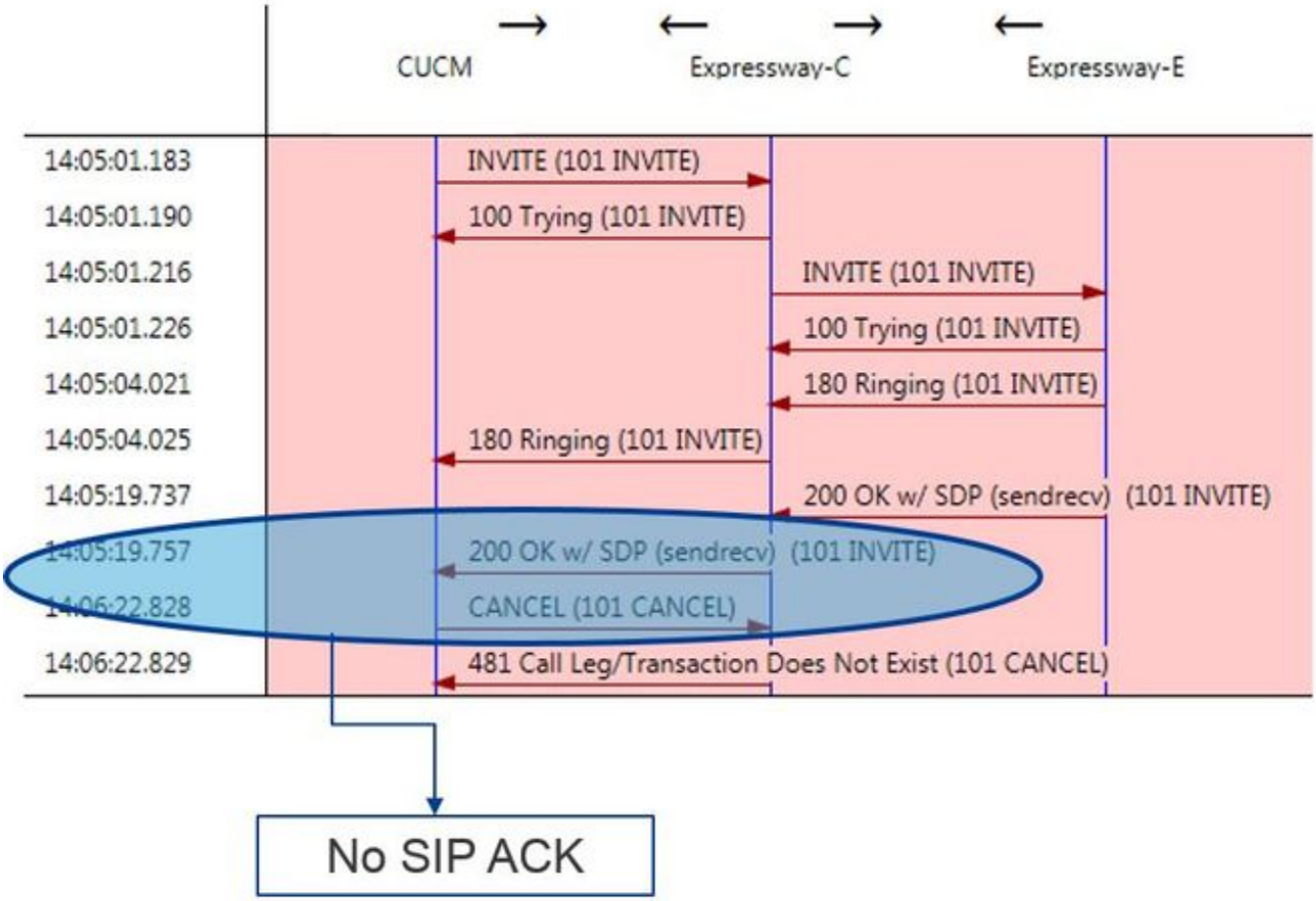
Door de apparaatpool te veranderen, veranderde u de verhouding van het gebied. De nieuwe apparaatpool had een regio die op RTP-infrastructuur was ingesteld. Daarom was de nieuwe gebiedsrelatie tussen de Cisco Webex-RD en Expressway-C-stam RTP-apparaten en RTP-infrastructuur. Als u het beeld bekijkt, kunt u deze relatie zien met de ondersteuning van AAC-LD, een van de ondersteunde audio-codecs voor Cisco Webex en zo stelt de oproep correct in. Uitgave 2. Unified CM Max. inkomende berichtgrootte overschredenOmdat video meer overheersend is geworden binnen de onderneming, is de grootte van SIP berichten die SDP bevatten substantieel toegenomen. De servers die deze berichten verwerken moeten zodanig zijn geconfigureerd dat zij een groot pakket kunnen accepteren. Op veel Call Control servers zijn de standaardwaarden prima. Met de Cisco Unified Communications Manager (Unified CM) zijn de standaardwaarden om een groot SIP-bericht met SDP te verwerken in eerdere releases niet beschikbaar. In latere releases van Unified CM is de waarde die voor een SIP-bericht is toegestaan, toegenomen. Deze waarde wordt echter alleen op nieuwe installaties ingesteld en niet op upgrades. Dit gezegd hebbende, kunnen klanten die hun oudere versies van Unified CM aan het verbeteren zijn om de verbinding van de Hybrid Call Service te steunen beïnvloed worden door de Max Inkomend Berichtgrootte op Unified CM die te laag is.Als u probeert een Hybrid Call Service Connect-gespreksstoring te identificeren die deze kwestie aansluit, moet u de expresslogboeken naast Unified CM SDL-sporen krijgen. Om de mislukking te identificeren, eerst begrijpen wat er gebeurt en dan het soort scenario's waarin de mislukking kan voorkomen.Om de vraag te beantwoorden van wat er gebeurt, moet u weten dat wanneer Unified CM een te groot SIP bericht ontvangt, het eenvoudigweg de TCP socket sluit en niet reageert op de Expressway-C.Dit gezegd hebbende zijn er veel situaties en manieren waarop dit zou kunnen gebeuren:

1. Cisco Webex stuurt een inkomende INVITE met SDP die te groot is. De snelweg-C geeft dit aan Unified CM door en Unified CM sluit de TCP socket en het SIP-dialoogvenster verschijnt dan.

2. Unified CM probeert de uitgaande verbinding aan te bieden zoals Voortijdig aan Webex, wat betekent dat de eerste INVITE die naar de Expressway-C wordt verstuurd SDP zal bevatten. Cisco Webex stuurt vervolgens een O/SDP-antwoord van 200 OK en de OK-reactie van 200 OK wanneer deze van de sneltoets C naar de Unified CM wordt doorgegeven is te groot. Unified CM sluit de TCP socket en het SIP-dialoogvenster verschijnt dan buiten.

3. Unified CM probeert de uitgaande oproep zoals vertraagd aan Webex te doen, wat betekent dat de eerste INVITe die naar de expressway-C wordt gestuurd geen SDP zal bevatten. Cisco Webex stuurt dan een O/O-bestand van 200 OK en het bod van 200 OK wanneer de overdracht van de sneltoets-C naar de Unified CM te groot is. Unified CM sluit de TCP socket en het SIP-dialoogvenster verschijnt dan buiten.

Wanneer u de sneltoetsen Expressway-C doorkijkt voor deze toestand, kunt u de berichtstroom begrijpen. Als u een programma zoals TranslatorX wilt gebruiken, kunt u zien dat Expressway-C de Cisco Webex 200 OK met SDP doorgeeft aan Unified CM. De uitdaging is dat de Unified CM nooit meer reageert met een SIP-ACK zoals in de afbeelding.



Aangezien Unified CM de verantwoordelijke partij is voor het niet reageren, is het de moeite waard om de SDL-sporen te bekijken om te zien hoe Unified CM met deze conditie omgaat. Wat u in dit scenario zou vinden is dat de Unified CM het grote bericht van de Expressway-C negeert. Een logline-optie zoals deze wordt afgedrukt.

```
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.
```

Nadat het SIP-dialoogvenster is verstuurd, stuurt Cisco Webex een bericht van ininkomende SIP 603 afname naar de expressway-E zoals in de logsteekproef vermeld.

```
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
```

Zoals gezegd zijn er drie verschillende scenario's waarin je dit gedrag kan zien. Voor de duidelijkheid kwamen de logmonsters die in deze illustratie worden meegeleverd, overeen met situatie 3 waarin de oproep naar Cisco Webex werd verzonden zoals het vertraagde aanbod. Oplossing:

1. Meld u aan bij de Unified CM.
2. Navigeer naar Systeem > Servicecategorieën.

3. Selecteer de server die de Call Manager-service voert.
4. Kies de Cisco Call Manager-service wanneer dit wordt gevraagd voor een keuze voor de service.
5. Selecteer de geavanceerde optie.
6. Wijzig onder de instellingen Devices device - SIP de grootte van het SIP Max-inkomende bericht in 18000.
7. Selecteer Opslaan.
8. Herhaal dit proces voor elk Unified CM-knooppunt dat de Cisco Call Manager-service biedt.

Opmerking: Om een IP-telefoon te kunnen gebruiken, moet het Collaboration-endpoints en/of SIP-trunk opnieuw worden gestart. Deze apparaten kunnen afzonderlijk worden herstart om de invloed op het milieu te minimaliseren. Stel NIET elk apparaat op de CUCM opnieuw in, tenzij u weet dat dit absoluut aanvaardbaar is.

BijlageHulpmiddelen voor probleemoplossing

PatronenhulpprogrammaControlerenDe Expressway heeft een voorziening voor patrooncontrole die handig is wanneer je wilt testen of een patroon overeenkomt met een bepaald alias en op een verwachte manier getransformeerd wordt. Het hulpprogramma kan gevonden worden op de snelweg onder het kopje Onderhoud > Gereedschappen > Patronenmenu controleren. Meestal, wordt dit gebruikt als je wilt testen of je zoekregel regex een alias correct zal vergelijken met een patroonstring en dan naar keuze succesvolle manipulatie van de string uitvoeren. Voor Hybride Call Service Connect kunt u ook testen dat de Unified CM Cluster FQDN overeenkomt met de Patronenstring die u hebt ingesteld voor de Unified CM-cluster FQDN. Wanneer u deze voorziening gebruikt, bedenk dan dat de oproep zal leiden op basis van de Unified CM Cluster FQDN-parameter die in de routeheader is vermeld, niet op basis van de doelcode. Bijvoorbeeld, als, de volgende uitnodiging in de Expressway kwam, test de het patroon van de Controle tegen cucm.rtp.ciscotac.net, niet jorobb@rtp.ciscotac.net.

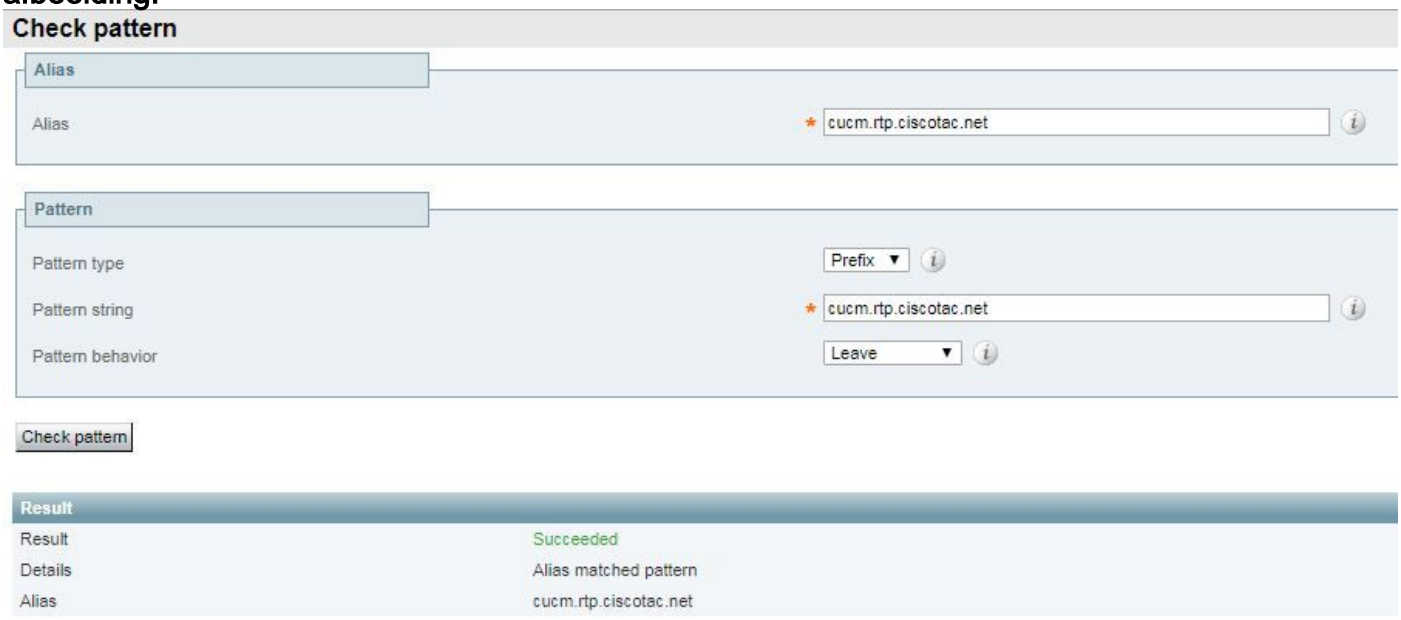
```
SIPMSG:
|INVITE sip:jorobb@rtp.ciscotac.net SIP/2.0
Via: SIP/2.0/TLS 192.168.1.6:7003;egress-
zone=HybridCallServiceTraversal;branch=z9hG4bKcac6d95278590991a2b516cf57e75827371;proxy-call-
id=abcba873-eaae-4d64-83b4-c4541d4e620c;rport
Via: SIP/2.0/TLS 192.168.1.6:5073;branch=z9hG4bK837b03f2cd91b6b19be4fc58edb251bf12;x-cisco-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

Om het patroon van de Controle te gebruiken om de het radiogolven van de de kopader van de Hybride Vraag van de Dienst Connect te testen, volgt deze stappen:

1. Navigeer naar Onderhoud > Gereedschappen > Controleer het patroon.
2. Voer voor de alias de Unified CM Cluster FQDN in.

3. Stel het Patroontype in op Prefixeren.
4. Stel de Patronenreeks in op Unified CM Cluster FQDN.
5. Stel het Patroontgedrag in om te vertrekken.
6. Selecteer Het patroon controleren.

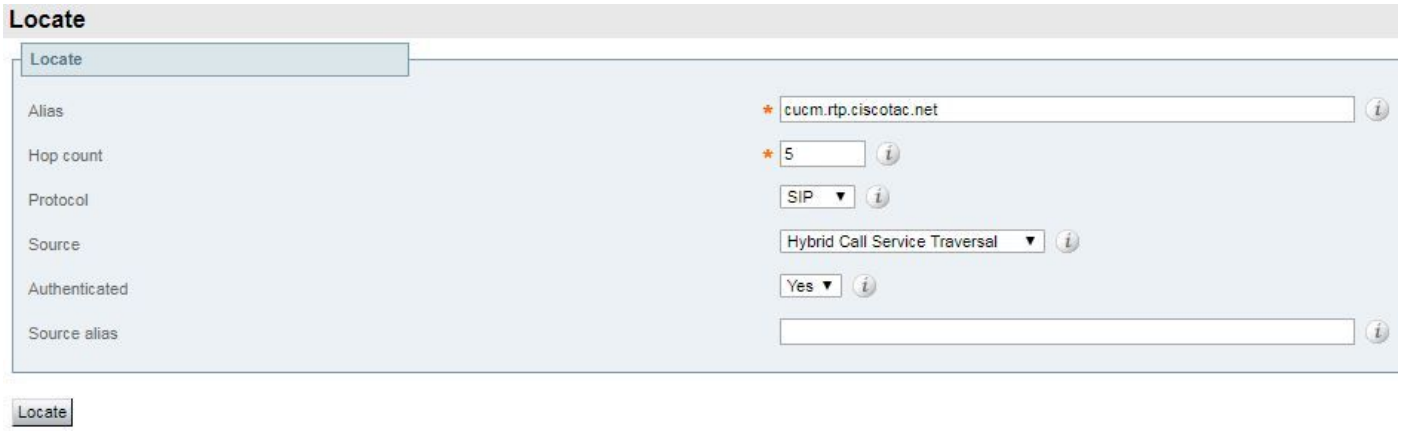
Als de zoekregels op de expressway correct zijn ingesteld, kunt u verwachten dat de Resultaten een Success bericht teruggeven. Hier is een voorbeeld van een succesvolle test van het patroon controleren zoals in de
afbeelding.



De reden dat dit succesvol is, is dat deze Alias (cucm.rtp.ciscotac.net) de prefixpatroon string van (cucm.rtp.ciscotac.net) aanpast. Om te begrijpen hoe een vraag op deze resultaten wordt routed, kunt u het beschreven hulpprogramma van de Plaats van de expressweg gebruiken.Hulpprogramma lokaliserenDe Locate voorziening van de Expressway is nuttig als je wilt testen of de Expressway een oproep naar een bepaalde Zone kan sturen op basis van een bepaald alias. Dit alles kan worden voltooid zonder dat je echt hoeft te bellen. U vindt het programma Lokaliseren in de snelweg van de sneltoets onder Onderhoud > Gereedschappen > Lokaliseren in het menu. U zult instructies zien op hoe u de Locate functionaliteit op de Expressway-C kunt gebruiken om te bepalen of de server een verbinding kan maken gebaseerd op de Unified CM Cluster FQDN die in de SIP-routekop is gevonden.

1. Navigeer naar Onderhoud > Gereedschappen > Lokaliseren.
2. Voer de Unified CM Cluster FQDN in in het veld alias.
3. Selecteer SIP als het protocol.
4. Selecteer uw Cisco Webex Hybrid Traversal Client Zone voor de bron.
5. Selecteer Lokaliseren.

Onder in de interface ziet u nu de zoekresultaten. Hier is een voorbeeld van de voorbeeldtest die met de bijbehorende resultaten is uitgevoerd zoals in de
afbeelding.



Dit zijn de resultaten van de Locate. Geboldeerd zijn de waarden van belang. Deze resultaten tonen:

- Het feit dat de Alias kon worden routeerd (True)
- Broninformatie (naam van het gebied/type)
- Bestemmingsinformatie (ook bekend als routinematig)
- Zoekregel die wordt aangepast (hybride gespreksservice inkomende routing)
- De zone waarnaar de oproep zal worden verstuurd (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
```

Diagnostische vastleggingElke keer dat u een probleem met betrekking tot een roeping of een mediaprobleem oplost voor een vraag die de oplossing van de Uitdrukking overbrengt, moet u de diagnostische houtkap gebruiken. Deze expressway-mogelijkheid geeft een ingenieur een groot detail van informatie voor alle logische beslissingen die de expressway neemt als de oproep doorgaat. U kunt de volledige tekst SIP-berichten zien, hoe de snelweg van de expressweg doorloopt en hoe de Expressway de mediakanalen instelt. De diagnostische houtkap heeft een

aantal verschillende modules die er in voeden. De houtkap kan worden aangepast om FATAAL, FOUT, WAARSCHUWING, INFO, DEBUG, TRACE weer te geven. Standaard wordt alles ingesteld op INFORMATIE waarin bijna alles wordt opgenomen wat u nodig hebt om een probleem te diagnosticeren. Van tijd tot tijd moet u misschien het logniveau van een bepaalde module van INFO naar DEBUG aanpassen om een beter begrip van wat er gebeurt te krijgen. De onderstaande stappen illustreren hoe u de logniveaus van de developer.ssl-module kunt aanpassen die verantwoordelijk is voor het leveren van informatie over (wederzijdse) TLS-handleidingen.

1. Meld u aan bij de sneltoets van de sneltoets (dit moet zowel op de sneltoets indrukken-E als op de toets C gebeuren).
2. Navigeer naar Onderhoud > Diagnostiek > Geavanceerd > Ondersteunde logconfiguratie.
3. Rol naar de module die u wilt aanpassen, in dit geval developer.ssl en klik op.
4. Kies DEBUG in het menu naast de parameter Niveau.
5. Klik op Opslaan.

Op dit moment ben je bereid om de diagnostische houtkap op te nemen:

1. Log in op de snelwegserver (dit moet zowel op de sneltoets als op de sneltoets C gebeuren).
2. Navigeer naar Onderhoud > Diagnostiek > Diagnostische vastlegging.
3. Klik op Start Nieuw logbestand (Zorg dat u de optie TCP-pomp controleert).
4. Reproduceer het probleem.
5. Klik op Stop vastlegging.
6. Klik op Downloadlogboek.

Voor de diagnostische houtkap van de snelweg, houd in gedachten dat u de houtkap van zowel expressway-C als Expressway-E parallel zou starten: eerst, start de houtkap op de snelweg-E, dan ga je naar de snelweg-C en start het. Op dat moment kun je het probleem dan reproduceren.Opmerking: Op dit moment bevat de diagnostische logbundel Expressway/VCS geen informatie over het certificaat voor sneldrukserver of de lijst Trusted CA. Als u een geval hebt waarin deze functie nuttig zou zijn, kunt u uw zaak aan dit defect hechten.

Gerelateerde informatie

- Invoergids voor Cisco Webex hybride gespreksservices
- Cisco Webex-handleiding voor hybride ontwerpen
- Cisco-toegangsbeheerdershandleiding
- Technische ondersteuning en documentatie – Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.