

Cisco Webex Hybrid Call Service Connect 트러블슈팅 가이드

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[통화 설정 문제](#)

[상호 TLS 핸드셰이크 실패](#)

[유용한 상호 TLS 문제 해결 팁](#)

[문제점 1. Expressway-E는 Cisco Webex 인증서에 서명한 CA\(Certificate Authority\)를 신뢰하지 않습니다.](#)

[문제 2. Expressway-E Cisco Webex Hybrid DNS 영역의 TLS 주체 검증 이름 오류](#)

[문제 3. Expressway-E는 전체 인증서 체인을 Cisco Webex로 전송하지 않습니다.](#)

[문제 4. 방화벽이 상호 TLS 핸드셰이크를 종료합니다.](#)

[문제점 5. Expressway-E는 공용 CA에서 서명되었지만 Cisco Webex Control Hub에는 대체 인증서가 로드되었습니다.](#)

[문제점 6. Expressway가 인바운드 통화를 Cisco Webex Hybrid DNS 영역에 매핑하지 않습니다.](#)

[문제 7. Expressway-E는 기본 자체 서명 인증서를 사용합니다.](#)

[인바운드: Cisco Webex에서 온프레미스](#)

[문제 1. Cisco Webex에서 Expressway-E DNS SRV/호스트 이름을 확인할 수 없습니다.](#)

[문제 2. 소켓 실패: 포트 5062가 Expressway로의 인바운드입니다.](#)

[문제 3. 소켓 실패: Expressway-E가 포트 5062에서 수신 대기 중이 아님](#)

[문제 4. Expressway-E 또는 C는 사전 로드된 SIP 경로 헤더를 지원하지 않습니다.](#)

[문제점 5. Cisco Webex 앱에서 2개의 통화 알림\(토스트\)을 받고 있습니다.](#)

[아웃바운드: 온프레미스-Cisco Webex](#)

[문제 1. Expressway에서 callservice.ciscospark.com 주소를 확인할 수 없습니다.](#)

[문제 2. 포트 5062가 Cisco Webex로의 아웃바운드 차단됨](#)

[문제 3. Expressway 검색 규칙 구성 오류](#)

[문제 4. Expressway CPL 컨피그레이션 오류](#)

[양방향: Cisco Webex에서 온프레미스 또는 온프레미스에서 Cisco Webex로](#)

[문제점 1. IP Phone/Collaboration Endpoint는 G.711, G.722 또는 AAC-LD 이외의 오디오 코덱을 제공합니다.](#)

[문제 2. Unified CM 최대 수신 메시지 크기 초과](#)

[부록](#)

[Expressway 문제 해결 도구](#)

[패턴 확인 유틸리티](#)

[유틸리티 찾기](#)

[진단 로깅](#)

[관련 정보](#)

소개

이 문서에서는 기존 Cisco 통화 제어 인프라를 Cisco Collaboration 클라우드에 연결하여 함께 사용할 수 있도록 하는 Cisco Webex Hybrid Call Service Connect 솔루션에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco Webex 오퍼에 대한 지식
- Expressway 솔루션 지식(B2B)
- Cisco Unified CM(Communications Manager)에 대한 지식 및 Expressway와의 통합
- Unified CM 10.5(2) SU5 이상
- Expressway(B2B) 버전 X8.7.1 이상(X8.9.1 권장)
- Expressway(커넥터 호스트) - 현재 지원되는 버전에 대해서는 [Cisco Webex Hybrid Services에 대한 Expressway Connector 호스트 지원](#)을 참조하십시오.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Unified Communications Manager
- 고속도로
- Windows용 Webex
- Mac용 Webexfor
- Webexfor iOS
- Android용 Webex
- Cisco 협업 엔드포인트
- 협업 데스크 엔드포인트
- IP 전화
- 소프트웨어 클라이언트

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

배경 정보

이 솔루션은 다음과 같은 기능을 제공합니다.

- Webex 앱을 오디오 및 비디오 통화를 위한 모바일 소프트웨어 클라이언트로 사용
- 사무실에 있는 것처럼 어디에서나 전화를 걸고 받을 수 있도록 앱을 사용합니다.
- Webex, Cisco Jabber 또는 해당 데스크폰을 사용하여 통화할 수 있습니다. 어떤 옵션을 사용하든 걱정할 필요 없음
- 온프레미스 전화에서 통화 기록 잠금 해제 및 Webex에서 해당 기록 통합

이 가이드의 범위는 하이브리드 통화 서비스 연결에 고유한 문제를 다루는 것입니다. Hybrid Call Service Connect는 모바일 및 원격 액세스, 비즈니스 대 비즈니스 통화와 같은 다른 솔루션과 동일한 Expressway E & C 쌍을 통해 실행되므로 다른 솔루션과 관련된 문제는 Hybrid Call Service Connect에 영향을 미칠 수 있습니다. Call Service Connect와 함께 사용하기 위해 Expressway 쌍을 구축하는 고객 및 파트너의 경우 Hybrid Call Service Connect를 구축하기 전에 [Cisco VCS Expressway 및 VCS Control Basic Configuration Guide](#)를 참조해야 합니다. 이 트러블슈팅 가이드는 부록 3 및 4의 Expressway 설계와 함께 방화벽/NAT 고려 사항을 다룹니다. 이 설명서를 자세히 검토하십시오. 또한 이 문서에서는 Expressway 커넥터 호스트 및 하이브리드 통화 서비스 활성화를 완료한 것으로 가정합니다.

통화 설정 문제

상호 TLS 핸드셰이크 실패

Hybrid Call Service Connect는 Cisco Webex와 Expressway-E 간의 인증을 위해 상호 전송 계층 보안(상호 TLS)을 사용합니다. 즉, Expressway-E와 Cisco Webex가 모두 존재하는 인증서를 확인하고 검사합니다. Expressway 서버를 새로 구축하고 Hybrid Call Service Connect와 같은 솔루션을 활성화하는 동안 상호 TLS 문제가 매우 일반적이기 때문에 이 섹션에서는 Expressway와 Cisco Webex 간의 인증서 기반 문제를 해결하는 데 유용한 정보와 팁을 제공합니다.

Expressway-E는 무엇을 확인합니까?

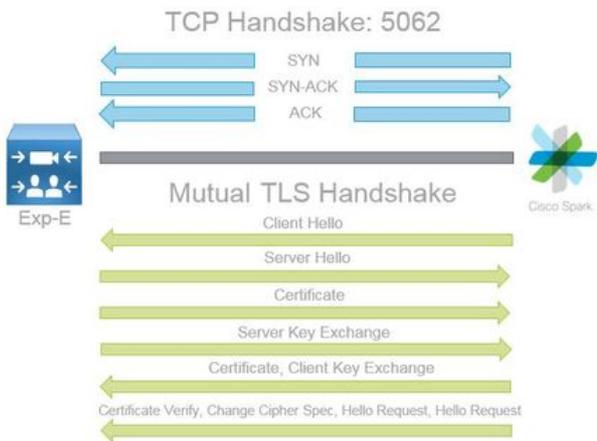
- Expressway-E Trusted CA 목록에 나열된 공용 CA에서 Cisco Webex 인증서가 서명되었습니까?
- Cisco Webex 인증서의 주체 대체 이름 필드에 `callservice.ciscospark.com`이 있습니까?

Cisco Webex는 무엇을 확인합니까?

- Webex가 신뢰하는 공용 CA 중 하나에서 Expressway-E 인증서에 서명했습니까?([Cisco Webex Trusted CA List](#))
- Expressway-E가 공개적으로 서명된 인증서를 사용하지 않는 경우 Cisco Webex Control Hub(<https://admin.ciscospark.com>)에 업로드된 루트 및 중간 인증서와 함께 Expressway 인증서가 되었습니까?

이는 이미지에 표시된 대로 설명됩니다.

Spark to On Premise



On Premise to Spark



유용한 상호 TLS 문제 해결 팁

1. 상호 TLS 핸드셰이크 디코드

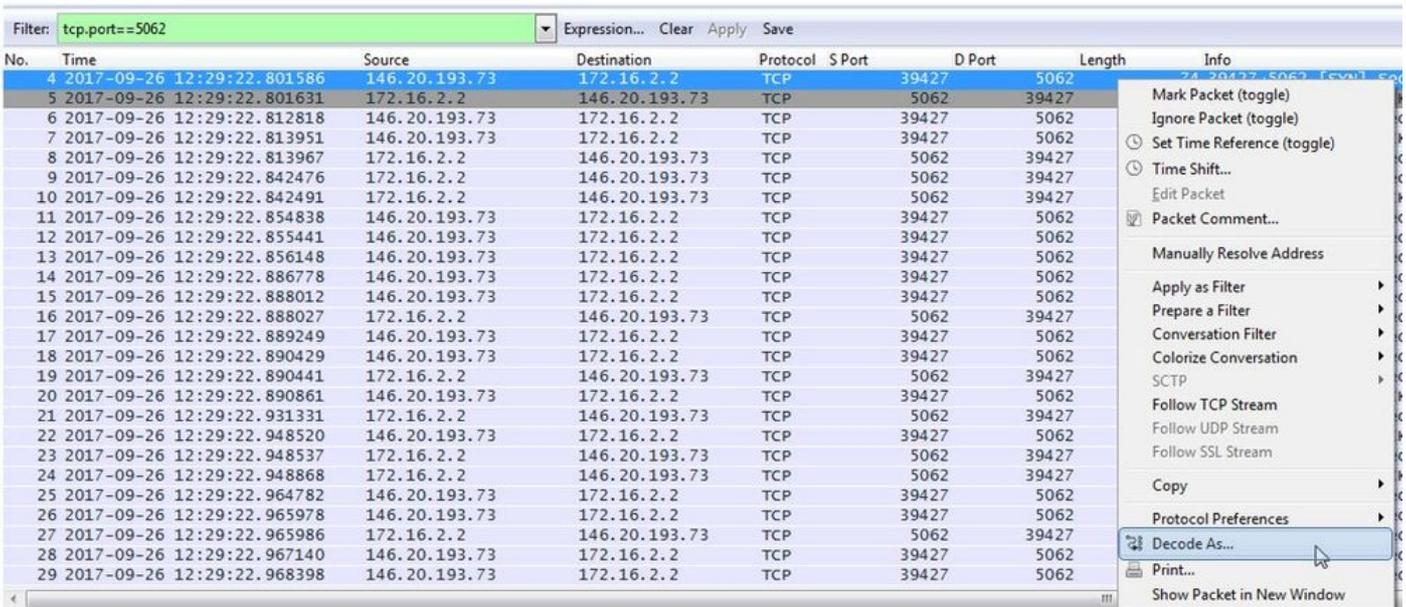
기본적으로 Wireshark는 SIP TLS 트래픽을 포트 5061로 표시합니다. 즉, 포트 5062를 통해 발생하는 (상호) TLS 핸드셰이크를 분석하려는 경우 Wireshark는 트래픽을 제대로 디코딩하는 방법을 알지 못합니다. 다음은 이미지에 표시된 대로 포트 5062에서 발생하는 Mutual TLS 핸드셰이크의 예입니다.

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

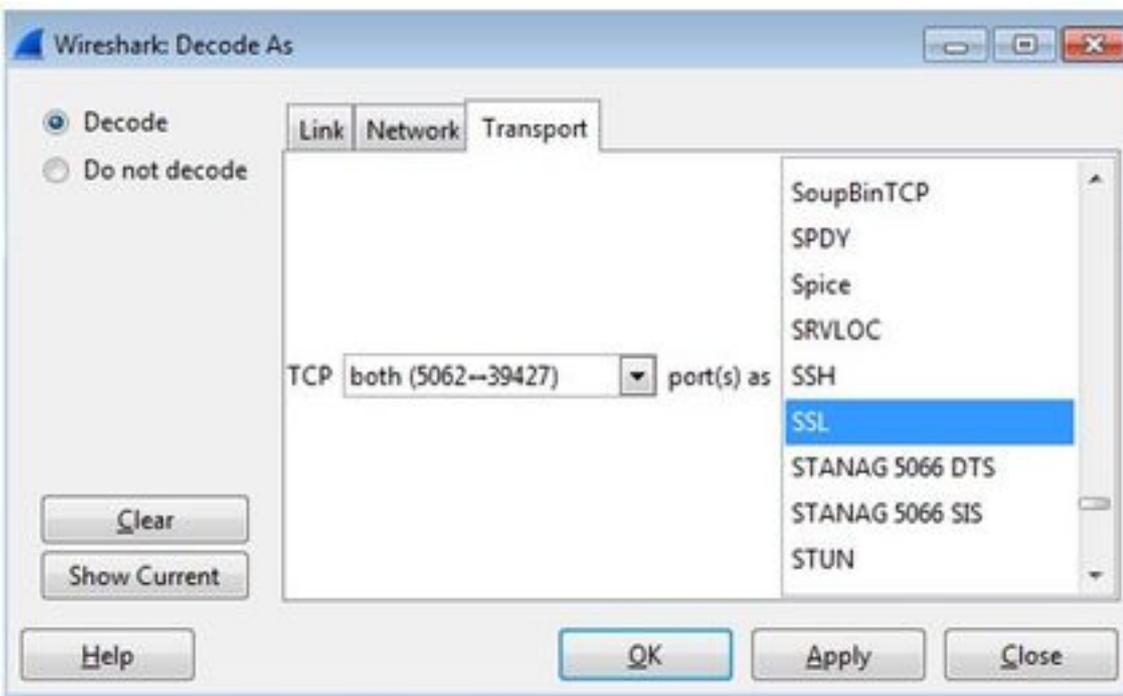
보시다시피 Wireshark의 기본 설정을 사용하여 핸드셰이크가 표시되는 방식입니다.패킷 번호 175는 Expressway가 Cisco Webex에 전송하는 인증서입니다.그러나 트래픽을 디코딩하지 않으면 확인할 수 없습니다.인증서 정보 및 존재하는 오류 메시지를 보다 쉽게 볼 수 있도록 이 트래픽을 디코딩하는 두 가지 방법을 사용할 수 있습니다.

1a. 스트림을 SSL로 분류

a. Mutual TLS 핸드셰이크를 분석할 때 먼저 **tcp.port==5062**로 캡처를 필터링합니다. 그런 다음 스트림에서 첫 번째 패킷을 마우스 오른쪽 단추로 클릭하고 **다음으로 디코드...**를 선택합니다. 이미지에 표시된 것처럼



b. Decode As... 옵션을 선택하면 선택한 스트림을 디코딩하는 방법을 선택할 수 있는 목록이 표시 됩니다. 목록에서 SSL을 선택하고 Apply(적용)를 클릭하고 창을 닫습니다. 이 시점에서 전체 스트림은 이미지에 표시된 대로 핸드셰이크 시점에 교환된 인증서 및 오류 메시지를 표시합니다.



1b. SIP TLS 포트 조정

Wireshark 환경 설정에서 SIP TLS 포트를 5062로 조정하면 인증서를 포함한 핸드셰이크를 둘러싼 모든 세부 정보를 볼 수 있습니다. 이 변경을 수행하려면

- 오픈 Wireshark
- Edit(편집) > Preferences(기본 설정)로 이동합니다.
- Protocols(프로토콜)를 확장하고 SIP를 선택합니다.
- SIP TLS 포트를 5062로 설정하고 Apply(적용)를 클릭합니다.
- 이미지에 표시된 대로 분석이 완료되면 값을 5061로 다시 설정합니다.

SIP TCP ports:

SIP TLS Port:

Display raw text for SIP message:

지금 동일한 캡처를 분석하면 패킷 169~175가 디코딩된 것을 볼 수 있습니다. 패킷 175는 Expressway-E 인증서를 표시하고, 패킷을 드릴다운하면 이미지에 표시된 대로 모든 인증서 세부 정보를 볼 수 있습니다.

No.	Time	Source	Destination	Protocol	S Port	D Port	Length	Info
169	2017-09-20 14:22:13.293817	146.20.193.45	172.16.2.2	TCP	48520	5062	74	48520->5062 [SYN] Seq=0 Win=14600 Len=0 MSS=1380 SACK_PERM=1 TSval=3875387337 TSecr=0 WS=128
170	2017-09-20 14:22:13.293846	172.16.2.2	146.20.193.45	TCP	5062	48520	74	5062->48520 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=444315393 TSecr=3875387337 WS=128
171	2017-09-20 14:22:13.304549	146.20.193.45	172.16.2.2	TCP	48520	5062	66	48520->5062 [ACK] Seq=1 Ack=1 Win=14720 Len=0 TSval=3875387348 TSecr=444315393
172	2017-09-20 14:22:13.305898	146.20.193.45	172.16.2.2	TLSv1.2	48520	5062	268	Client Hello
173	2017-09-20 14:22:13.305911	172.16.2.2	146.20.193.45	TCP	5062	48520	66	5062->48520 [ACK] Seq=1 Ack=201 Win=30080 Len=0 TSval=444315405 TSecr=3875387349
174	2017-09-20 14:22:13.336342	172.16.2.2	146.20.193.45	TLSv1.2	5062	48520	2802	Server Hello
175	2017-09-20 14:22:13.336358	172.16.2.2	146.20.193.45	TLSv1.2	5062	48520	1426	Certificate

2. Wireshark 필터링

패킷 캡처를 분석할 때 지정된 캡처에서 관찰된 엄청난 양의 패킷으로 손실되기 쉽습니다. Wireshark를 필터링하여 표시할 수 있도록 가장 관심 있는 트래픽 유형을 이해하는 것이 중요합니다. 다음은 상호 TLS 핸드셰이크에 대한 세부 정보를 얻는 데 사용할 수 있는 몇 가지 일반적인 Wireshark 필터입니다.

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

3. PCAP에서 인증서 추출

때때로 인증서(서버, 루트 또는 중개자)의 사본을 가져와야 할 수 있습니다. 검색할 인증서를 찾을 위치를 모르는 경우 패킷 캡처에서 직접 인증서를 추출할 수 있습니다. 다음은 상호 TLS 핸드셰이크에 표시되는 Cisco Webex 인증서를 가져오는 방법입니다.

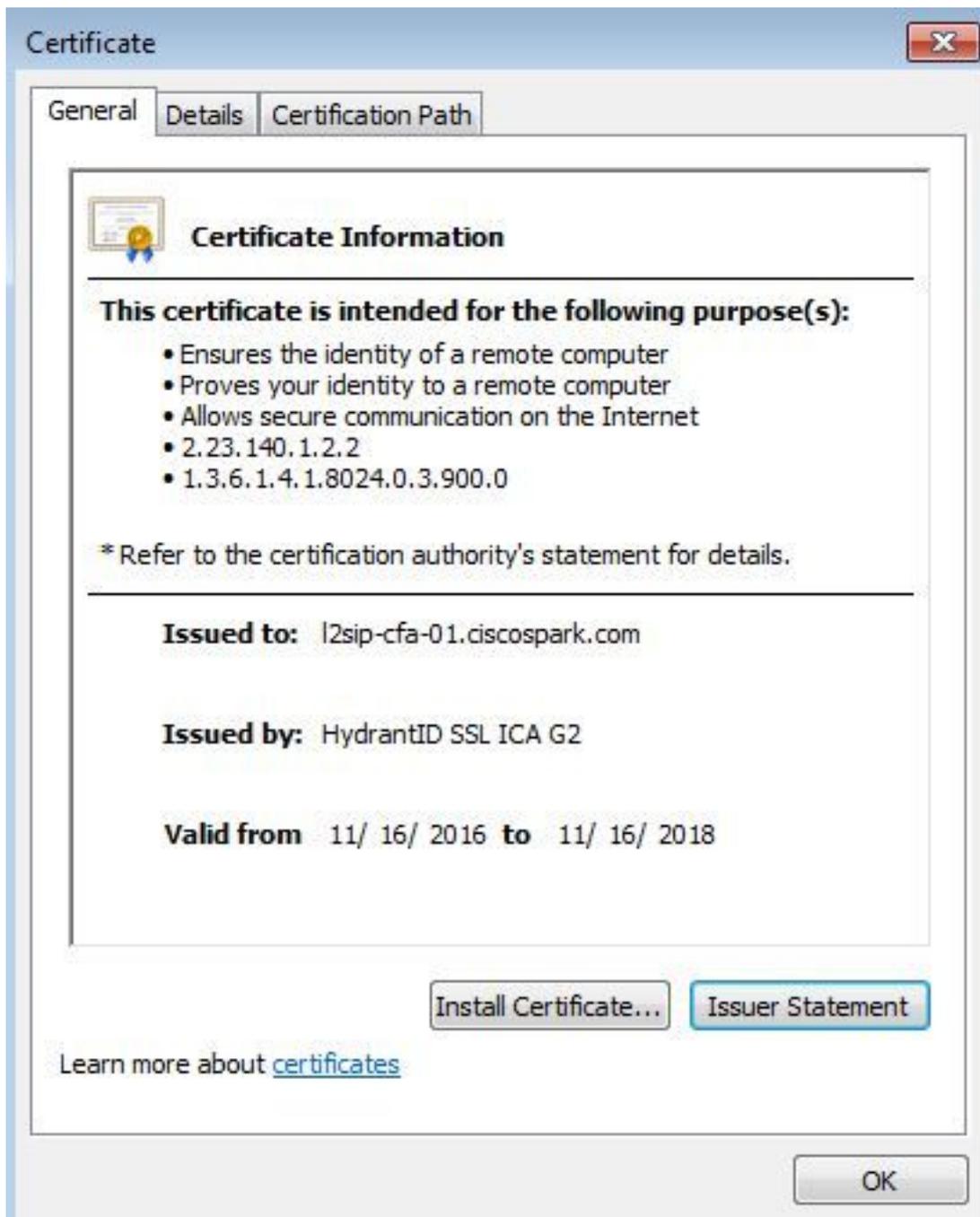
1. **ssl.handshake.certificate && tcp.port==5062**로 패킷 캡처 필터링
2. Webex 서버 주소에서 소싱되고 Info(정보) 섹션에 Certificate(인증서)가 인쇄된 패킷을 찾습니다.
3. 패킷 세부 정보에서 **Secure Socket Layer > TLS Certificate > Handshake Protocol > Certificates**를 확장합니다. 참고: 체인의 맨 아래/마지막 인증서는 루트 CA입니다.
4. 관심 있는 인증서를 마우스 오른쪽 버튼으로 클릭하고 이미지에 표시된 대로 **Export Selected Packet Bytes...**를 선택합니다.

The image shows the Wireshark interface with the following elements:

- Filter Capture:** A filter expression `ssl.handshake.certificate && tcp.port==5062` is applied to the capture.
- Selected Packet:** Packet 285 is selected, showing details for the TLS Certificate.
- Right-click and Export:** A context menu is open over the certificate details, with the option `Export Selected Packet Bytes...` highlighted.

5. 파일을 .cer로 저장합니다.

6. 저장된 파일을 두 번 클릭하여 이미지에 표시된 대로 인증서를 엽니다.



4. Expressway 로깅 레벨 조정

인증서를 분석할 때 Expressway가 수행하는 논리를 더 잘 이해할 수 있도록 Expressway에서 두 개의 로깅 모듈을 사용할 수 있습니다.

- 개발자.ssl
- developer.zone.zonemg

기본적으로 이러한 로깅 모듈은 INFO 레벨로 설정됩니다. DEBUG 레벨로 설정하면 발생하는 인증서 검사에 대한 정보와 어떤 영역 트래픽이 매핑되는지 확인할 수 있습니다. 이 두 기능은 모두 하이브리드 통화 서비스와 관련이 있습니다.

Cisco Webex의 서버 인증서에 대한 SAN 검사를 수행하는 Expressway-E의 예.

```
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""
```

MTLS 연결을 Cisco Webex Hybrid DNS 영역에 매핑하는 Expressway-E의 예:

```
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" Identities="{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-
```

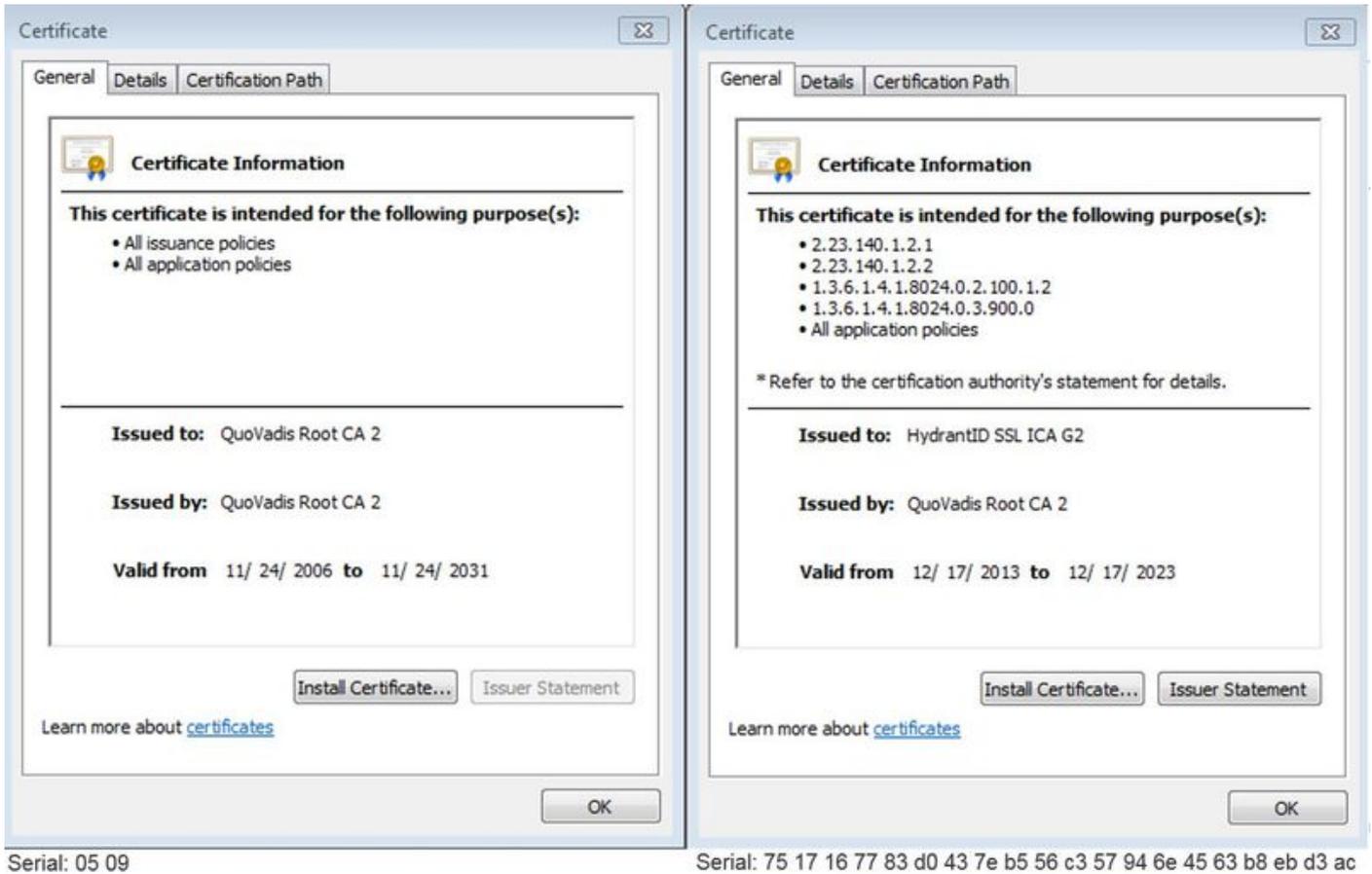
web.wbx2.com, Alt-DNS: l2sip-cfa-web.wbx2.com, Alt-DNS: callservice.ciscospark.com, **Alt-DNS: callservice.call.ciscospark.com**, Alt-DNS: l2sip-a-Webexcall.ciscospark.com, Alt-DNS: l2sip-prod-11-dfw-public.wbx2.com, Alt-DNS: l2sip-prod-12-dfw-public.wbx2.com, Alt-DNS: l2sip-l2sipproda1-294-riad-public.wbx2.com, 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"

다음은 Expressway-E와 Cisco Webex 간의 상호 TLS 장애와 관련된 가장 일반적인 문제 목록입니다.

문제점 1. Expressway-E는 Cisco Webex 인증서에 서명한 CA(Certificate Authority)를 신뢰하지 않습니다.

Expressway-E와 직접 통신하는 Cisco Webex 서버를 L2SIP 서버라고 합니다. 이 L2SIP 서버는 일반 이름 Hydrant SSL ICA G2를 사용하는 중간 서버에서 서명합니다. 이 중개자는 이미지에 표시된 대로 QuoVadis Root CA 2의 공통 이름을 가진 루트 인증 기관에서 서명합니다.

참고: 이 문제는 변경될 수 있습니다.



Expressway 진단 관점에서 이 트래픽을 분석하는 첫 번째 단계는 **TCP 연결**을 검색하는 것입니다. **TCP Connecting**을 검색한 후 **Dst-port=5062** 값을 찾습니다. 이 연결이 시도되고 설정된 로그에서 영역을 식별한 다음 일반적으로 Handshake in progress(핸드셰이크 진행 중)를 나타내는 로그 항목으로 표시되는 TLS 핸드셰이크를 찾을 수 있습니다.

```
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"
```

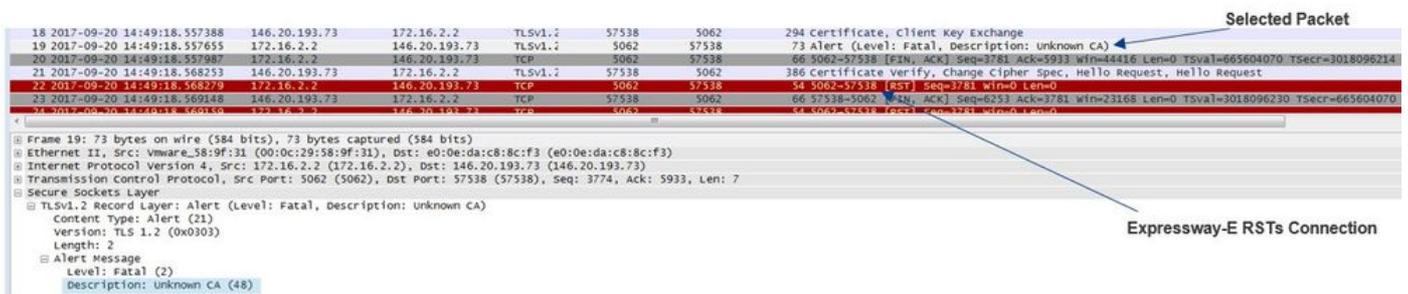
Expressway-E가 Cisco Webex 서명 인증서를 신뢰하지 않을 경우 핸드셰이크가 완료된 후 Expressway-E가 인증서를 즉시 거부할 수 있습니다.이 로그 항목은 다음 로그 항목을 통해 Expressway-E 로깅에서 확인할 수 있습니다.

```
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"
```

Expressway 오류 메시지는 인증서 체인의 자체 서명 인증서를 참조하므로 약간 잘못 인식할 수 있습니다.Wireshark를 사용하면 교환을 자세히 볼 수 있습니다.Wireshark 패킷 캡처 분석 관점에서 Webex 환경이 인증서를 제시하면 Expressway가 돌아서서 이미지에 표시된 대로 알 수 없는 CA 오류가 있는 인증서로 거부한다는 것을 명확하게 확인할 수 있습니다.



해결책:

이 문제를 해결하려면 Expressway-E가 Cisco Webex 인증 기관을 신뢰하는지 확인해야 합니다 .Wireshark 추적에서 이러한 인증서를 추출하여 Expressway의 신뢰할 수 있는 CA 인증서 저장소에 업로드하면 되지만 Expressway는 더 간단한 방법을 제공합니다.

- Expressway-E에 로그인
- Applications(애플리케이션) > Cloud Certificate management(클라우드 인증서 관리)로 이동합니다.
- 이미지에 표시된 대로 인증서 가져오기 옵션을 선택합니다.

Status System Configuration **Applications** Users Maintenance

Cisco Collaboration Cloud certificate management

VCS Expressway does not register for any Hybrid Services. For Call Service Connect, it must have a secure traversal zone to VCS Control

CA root certificate management

For some hybrid services, the VCS Expressway needs to trust the CAs that sign the Collaboration Cloud certificates, and you can install them here.

[Get certificates](#)

이때 Cisco Webex 인증 기관은 Expressway-E Trusted CA 저장소(Maintenance > Security > Trusted CA certificate)에 업로드됩니다.

문제 2. Expressway-E Cisco Webex Hybrid DNS 영역의 TLS 주체 검증 이름 오류

Hybrid Call Service Connect는 상호 TLS 핸드셰이크의 일부로 TLS 확인을 사용합니다. 즉, Expressway는 Cisco Webex CA 인증서를 신뢰할 수 있을 뿐 아니라 제공된 인증서의 SAN(Subject Alternate Name) 필드를 확인하여 **callservice.ciscospark.com**과 같은 값이 있는지 확인합니다. 이 값이 없으면 인바운드 통화가 실패합니다.

이 특정 시나리오에서 Cisco Webex 서버는 Expressway-E에 인증서를 제공합니다. 인증서에는 실제로 25개의 다른 SAN이 있습니다. Expressway-E가 **callservice.ciscospark.com** SAN에 대해 인증서를 확인하지만 이를 찾지 못하는 경우를 생각해 보십시오. 이 조건이 충족되면 진단 로깅 내에서 이와 유사한 오류가 표시됩니다.

```
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"
```

Wireshark를 사용하여 이 인증서 핸드셰이크를 분석할 경우, Cisco Webex가 인증서를 제시하면 Expressway RST가 이미지에 표시된 대로 바로 후에 연결을 확인할 수 있습니다.

Selected Packet

No.	Time	Source	Destination	Protocol	Length	Info
71	2017-09-20 15:17:42.646845	146.20.193.45	172.16.2.2	TLSv1.2	46049	5062 294 Certificate, Client Key Exchange
72	2017-09-20 15:17:42.687317	172.16.2.2	146.20.193.45	TCP	5062	46049 66 5062-46049 [ACK] Seq=4746 Ack=5933 win=44416 Len=0 TSval=447644787 TSecr=3878716684
73	2017-09-20 15:17:42.700250	146.20.193.45	172.16.2.2	TLSv1.2	46049	5062 386 Certificate Verify, Change cipher spec, Hello Request, Hello Request
74	2017-09-20 15:17:42.700260	172.16.2.2	146.20.193.45	TCP	5062	46049 66 5062-46049 [ACK] Seq=4746 Ack=6253 win=47104 Len=0 TSval=447644799 TSecr=3878716745
75	2017-09-20 15:17:42.700534	172.16.2.2	146.20.193.45	TLSv1.2	5062	46049 117 Change cipher Spec, Encrypted Handshake Message
76	2017-09-20 15:17:42.700898	172.16.2.2	146.20.193.45	TCP	5062	46049 66 5062-46049 [FIN, ACK] Seq=4797 Ack=6253 win=47104 Len=0 TSval=447644800 TSecr=3878716745
77	2017-09-20 15:17:42.712865	146.20.193.45	172.16.2.2	TCP	46049	5062 1434 [TCP segment of a reassembled PDU]
78	2017-09-20 15:17:42.712889	172.16.2.2	146.20.193.45	TCP	5062	46049 54 5062-46049 [RST] Seq=4797 Win=0 Len=0

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

Expressway-E RSTs Connection

이 값의 컨피그레이션을 확인하려면 솔루션에 대해 구성된 Webex Hybrid DNS 영역으로 이동할 수 있습니다. Expressway-E xConfiguration이 있는 경우 Zone Configuration(영역 컨피그레이션) 섹션을 찾아 TLS 확인 주체 이름이 구성된 방법을 확인할 수 있습니다. xConfiguration의 경우 영역 1이 첫 번째인 영역 순서가 지정됩니다. 위에 분석된 문제의 환경의 xConfiguration입니다.

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

예제에서 볼 수 있듯이 TLS Verify Subject Name(TLS 확인 주체 이름)은 callservice.ciscopark.com 대신 **callservice.ciscopark.com**으로 설정됩니다.(추가 "/" 참고)

해결책:

이 문제를 해결하려면 TLS 확인 주체 이름을 수정해야 합니다.

- Expressway-E에 로그인
- Configuration(컨피그레이션) > Zones(영역) > Zones(영역)로 이동합니다.
- Webex Hybrid Services DNS 영역 선택
- TLS 확인 주체 이름을 callservice.ciscopark.com으로 설정
- 저장 선택

참고:기본 로깅 동작은 을 참조하십시오.이 섹션에서는 Expressway가 인증서 확인을 수행하고 Webex Hybrid DNS 영역에 매핑하는 방법을 보여 줍니다.

참고:Expressway 코드 x12.5 이상 버전에서는 새 "Webex" 영역이 해제되었습니다.이 Webex 영역은 Webex와의 통신에 필요한 영역의 컨피그레이션을 미리 채웁니다.즉, TLS 주체 검증 모드 및 TLS 주체 이름을 설정할 필요가 없습니다.구성 간소화를 위해 x12.5 이상의 Expressway 코드를 실행 중인 경우 Webex 영역을 활용하는 것이 좋습니다.

문제 3. Expressway-E는 전체 인증서 체인을 Cisco Webex로 전송하지 않습니다.

상호 TLS 핸드셰이크의 일부로 Cisco Webex는 Expressway-E 인증서를 신뢰해야 합니다.Cisco Webex에는 신뢰할 수 있는 퍼블릭 CA의 전체 목록이 있습니다.일반적으로 Cisco Webex에서 지원하는 공용 CA에서 Expressway-E 인증서를 서명하면 TLS 핸드셰이크가 성공합니다.설계상, Expressway-E는 공용 CA에서 서명했지만 TLS 핸드셰이크 중에 인증서를 전송합니다.인증서의 전체 체인(루트 및 중간)을 전송하려면 해당 인증서를 Expressway-E 자체의 신뢰할 수 있는 CA 인증서 저장소에 추가해야 합니다.

이 조건이 충족되지 않으면 Cisco Webex는 Expressway-E 인증서를 거부합니다.이 문제와 일치하는 조건을 트러블슈팅할 때 Expressway-E에서 진단 로그 및 tcpdump를 사용할 수 있습니다. Expressway-E 진단 로그를 분석할 때 다음과 유사한 오류가 표시됩니다.

```
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"
```

Wireshark의 관점에서 이 정보를 분석할 경우 Expressway-E가 인증서를 제시한다는 것을 알 수 있습니다.패킷을 확장하면 서버 인증서만 전송된다는 것을 확인할 수 있습니다.Cisco Webex는 이미 지에 표시된 대로 알 수 없는 CA 오류 메시지와 함께 이 TLS 핸드셰이크를 거부합니다.

Selected Packet

2600 Server hello, Certificate, Server Key Exchange, Certificate Request, Server hello Done

73 alert (Level: Fatal, Description: Certificate Unknown)

Spark Rejects the Handshake "Certificate Unknown" error

Expressway-E Server Certificate

id-at-commonName=amer-expressway01.ciscotac.net,id-at-organizationalUnitName=domain control validated

signedCertificate

algorithmIdentifier (sha256withRSAEncryption)

padding: 0

encrypted: 23238dab294d921bc43226e5e2faef0e8524bfb44129a7...

해결책:

이 시나리오에서 문제를 해결하려면 Expressway-E 인증서 서명에 관련된 중간 및 루트 CA를 신뢰할 수 있는 CA 인증서 저장소에 업로드해야 합니다.

1단계. Expressway-E에 로그인합니다.

2단계. Maintenance(유지 관리) > Security(보안) > Trusted CA certificate(신뢰할 수 있는 CA 인증서)로 이동합니다.

3단계. UI 하단의 Upload(업로드) 메뉴에서 Choose File(파일 선택)을 선택합니다.

4단계. Expressway-E 서명과 관련된 CA 인증서를 선택합니다.

5단계. CA 인증서 추가를 선택합니다.

6단계. Expressway-E 인증서(중간, 루트) 서명에 관련된 모든 CA 인증서에 대해 단계를 반복합니다.

7단계. CA 인증서 추가를 선택합니다.

이 프로세스가 완료되면 키 교환에 포함된 Expressway-E 서버 인증서 서명과 관련된 인증서의 전체 체인이 표시됩니다.다음은 Wireshark를 사용하여 패킷 캡처를 분석할 경우 어떤 것이 보이는지 보여주는 샘플입니다.

Selected Packet

1426 Certificate

66 48520-5062 [ACK] Seq=201 Ack=1369 win=17536 Len=0 TSval=3875387398 TSecr=444315436

66 48520-5062 [ACK] Seq=201 Ack=2737 win=20480 Len=0 TSval=3875387399 TSecr=444315436

66 48520-5062 [ACK] Seq=201 Ack=4097 win=23296 Len=0 TSval=3875387400 TSecr=444315436

715 Server Key Exchange

66 48520-5062 [ACK] Seq=201 Ack=4746 win=26112 Len=0 TSval=3875387411 TSecr=444315455

73 alert (Level: Fatal, Description: certificate unknown)

66 48520-5062 [FIN, ACK] Seq=208 Ack=4746 win=26112 Len=0 TSval=3875387711 TSecr=444315455

66 5062-48520 [FIN, ACK] Seq=4746 Ack=209 win=20080 Len=0 TSval=444315768 TSecr=3875387711

66 48520-5062 [ACK] Seq=209 Ack=4747 win=26112 Len=0 TSval=3875387725 TSecr=444315768

Server

Intermediate

Root

1426 bytes captured (11408 bits) on interface 0

Ethernet II, Src: Vmware_S8:9f:31 (00:0c:29:58:9f:31), Dst: e0:0e:da:c8:8c:f3 (e0:0e:da:c8:8c:f3)

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

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

[2 Reassembled TCP Segments (3938 bytes) = #174(264), #175(1296)]

Secure Sockets Layer

Handshake Protocol: Certificate

Content Type: Handshake (22)

Version: TLS 1.2 (0x0303)

Length: 3929

Handshake Protocol: Certificate

Handshake Type: Certificate (11)

Length: 3929

Certificates Length: 3926

Certificates (3926 bytes)

Certificate Length: 1712

Certificate (id-at-commonName=amer-expressway01.ciscotac.net,id-at-organizationalUnitName=domain control validated)

Certificate Length: 1236

Certificate (id-at-commonName=Go Daddy Secure Certificate Authority - G2,id-at-organizationalUnitName=http://certs.godaddy.com/repositor,id-at-organizationName=GoDaddy.com, Inc.,id-at-localityName=)

Certificate Length: 969

Certificate (id-at-commonName=Go Daddy Root Certificate Authority - G2,id-at-organizationName=GoDaddy.com, Inc.,id-at-localityName=Scottsdale,id-at-stateOrProvinceName=Arizona,id-at-countryName=US)

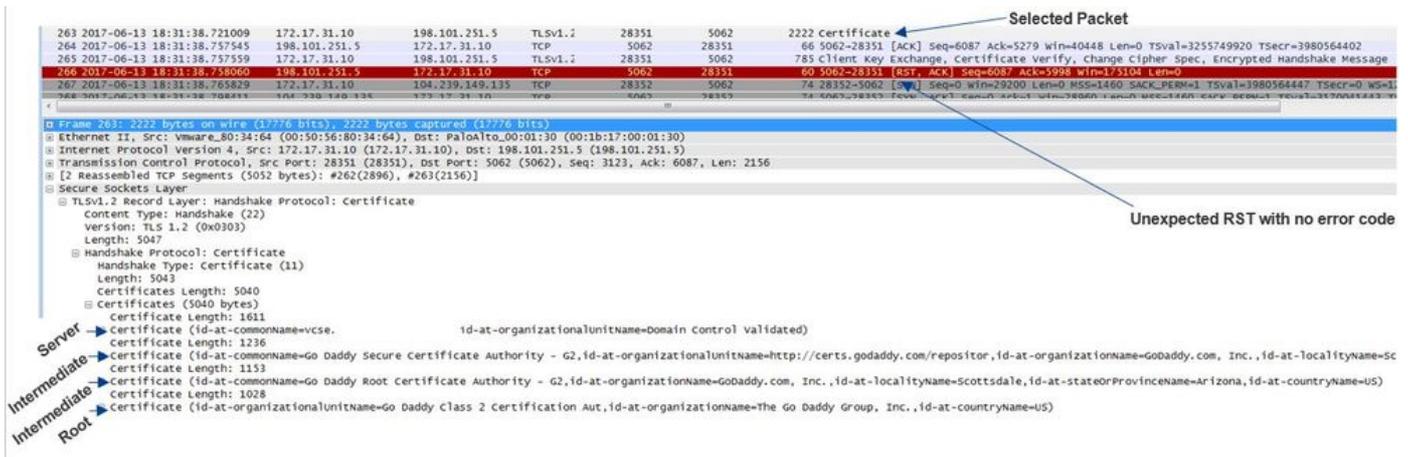
문제 4. 방화벽이 상호 TLS 핸드셰이크를 종료합니다.

Expressway 솔루션은 일반적으로 방화벽과 상호 작용합니다.솔루션의 인라인 방화벽은 몇 가지 유형의 애플리케이션 레이어 검사를 실행하는 경우가 많습니다.Expressway 솔루션에서 방화벽이 애플리케이션 레이어 검사를 실행할 때 관리자는 원치 않는 결과를 보게 됩니다.이 특정 문제는 방화벽의 애플리케이션 레이어 검사가 갑자기 연결을 끊었던 시기를 파악하는 데 도움이 됩니다.

Expressway에서 진단 로그를 사용하여 시도한 Mutual TLS 핸드셰이크를 찾을 수 있습니다. 앞서 언급한 대로 이 핸드셰이크는 포트 5062를 통해 TCP 연결이 설정된 직후에 와야 합니다. 이 시나리오에서는 방화벽이 연결을 끊으면 진단 로깅 내에서 이러한 오류가 표시됩니다.

```
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"
```

패킷 캡처 관점에서 Expressway-E는 Cisco Webex에 인증서를 제공합니다. 이미지에 표시된 대로 Cisco Webex의 방향에서 TCP RST가 오는 것을 볼 수 있습니다.



첫눈에 Expressway-E 인증서에 문제가 있다고 생각할 수 있습니다. 이 문제를 해결하려면 먼저 다음 질문에 대한 답을 결정해야 합니다.

- Expressway-E는 Cisco Webex가 신뢰하는 공용 CA에 의해 서명됩니까?
- Expressway-E 인증서 및 Expressway-E 인증서 서명과 관련된 모든 인증서가 Cisco Webex Control Hub(<https://admin.ciscospark.com>)에 자동으로 업로드됩니까?

이 특정 상황에서 솔루션은 Cisco Webex Control Hub를 사용하여 Expressway-E 인증서를 관리하지 않았습니다. 즉, Cisco Webex가 신뢰하는 공용 CA에서 Expressway-E 인증서를 서명해야 합니다. Wireshark 캡처에서 Certificate(인증서) 패킷(위 그림 참조)을 선택하면 인증서가 공용 CA에서 서명되었으며 전체 체인이 Cisco Webex로 전송되었음을 확인할 수 있습니다. 따라서 이 문제는 Expressway-E 인증서와 관련해서는 안 됩니다.

이 시점에서 추가적인 격리가 필요한 경우, 패킷이 방화벽의 외부 인터페이스에서 캡처될 수 있습니다. 그러나 진단 로그에 SSL 오류가 없는 것은 중요한 데이터 포인트입니다. 위(문제 3.)를 상기할 때 Cisco Webex가 Expressway-E 인증서를 신뢰하지 않는 경우 SSL 연결 해제 사유 유형을 확인해야 합니다. 이 조건에서 사용 가능한 SSL 오류가 없습니다.

참고: 방화벽 외부 인터페이스에서 패킷 캡처를 가져오려는 경우 Cisco Webex 환경에서 TCP RST가 들어오는 것을 볼 수 없습니다.

솔루션

이 특정 솔루션의 경우 파트너 또는 고객은 보안 팀에 의존해야 합니다. 이 팀은 Expressway 솔루션

에 대해 어떤 종류의 애플리케이션 레이어 검사를 사용하는지, 사용하는지 여부를 조사해야 하며, 사용한다면 이를 비활성화해야 합니다. VCS Control and Expressway 구축 설명서의 [부록 4](#)에서는 고객이 이 기능을 끄는 것이 권장되는 이유에 대해 설명합니다.

문제점 5. Expressway-E는 공용 CA에서 서명되었지만 Cisco Webex Control Hub에는 대체 인증서가 로드되었습니다.

이 특정 조건은 Expressway 솔루션을 처음부터 배포하고 공용 CA에서 서명한 Expressway-E 인증서가 없을 때 발생할 수 있습니다. 이 시나리오에서는 상호 TLS 협상을 성공적으로 완료할 수 있도록 내부적으로 서명된 Expressway-E 서버 인증서를 Cisco Webex Control Hub에 업로드합니다. 그런 다음 공용 CA에서 서명한 Expressway-E 인증서를 얻지만 Cisco Webex Control Hub에서 서버 인증서를 제거하는 것을 잊습니다. 인증서가 Cisco Webex Control Hub에 업로드될 때 해당 인증서가 TLS 핸드셰이크 중에 Expressway에서 제공하는 인증서보다 우선권을 가지고 있다는 것을 알아야 합니다.

Expressway-E 진단 로깅 관점에서 이 문제는 Cisco Webex가 Expressway-E 인증서를 신뢰하지 않을 때 충족되는 로깅 시그니처와 유사하게 보일 수 있습니다. 예를 들어, Expressway-E가 전체 체인을 전송하지 않거나 Cisco Webex가 신뢰하는 공용 CA에서 Expressway-E 인증서를 서명하지 않는 경우입니다. 다음은 TLS 핸드셰이크 중 Expressway-E 로깅에서 기대할 수 있는 예시입니다.

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

Wireshark의 관점에서 Expressway-E가 해당 인증서를 행 항목 175에 표시하는 것을 확인할 수 있습니다. 나중에 몇 개의 행 항목이 있으면 Cisco Webex 환경에서 인증서에 알 수 없는 인증서 오류가 있는 인증서를 거부합니다(이미지에 표시됨).

The screenshot shows a Wireshark capture of a TLS handshake. Packet 175 is selected, showing a 'Certificate' message. The details pane shows the certificate chain: Server (Certificate), Intermediate (Certificate), and Root (Certificate). An annotation points to the error message: 'Spark sends a "Certificate Unknown" Error'.

Expressway-E에서 전송하는 인증서 패킷을 선택할 경우 인증서 정보를 확장하여 Expressway-E가

1. [Cisco Webex](#)가 [신뢰하는 공용 CA에](#) 의해 서명되었으며,

2. 이(가) 서명에 포함된 전체 체인을 포함합니다.

이 경우 두 조건 모두 충족됩니다. 이는 Expressway-E 인증서에 문제가 없음을 나타냅니다.

솔루션

1단계. [Cisco Webex Control Hub에 로그인합니다.](#)

2단계. 왼쪽 창에서 서비스를 선택합니다.

3단계. Hybrid Call Card(하이브리드 통화 카드) 아래에서 Settings(설정)를 선택합니다.

4단계. Call Service Connect(통화 서비스 연결) 섹션으로 스크롤하여 Certificates for Encrypted SIP Calls(암호화된 SIP 통화용 인증서) 아래에서 원하지 않는 인증서가 나열되는지 확인합니다. 그런 경우 인증서 옆에 있는 휴지통 아이콘을 클릭합니다.

5단계. 제거를 선택합니다.

참고: 분석이 수행되어야 하며, 고객이 Webex Control Hub에 업로드된 인증서를 제거하기 전에 사용하지 않는 것으로 확인되어야 합니다.

Cisco Webex Control Hub에서 Expressway-E 인증서 업로드에 대한 자세한 내용은 [Hybrid Call Deployment Guide의 이 섹션을](#) 참조하십시오.

문제점 6. Expressway가 인바운드 통화를 Cisco Webex Hybrid DNS 영역에 매핑하지 않습니다.

인바운드 TLS 매핑 기능은 TLS 확인 주체 이름과 함께 작동하며, 둘 다 하이브리드 통화 DNS 영역에 구성됩니다. 이 시나리오에서는 x12.5 이전 Expressway에서 관찰된 문제와 과제를 설명합니다. x12 이상에서는 "Webex" 영역이라고 하는 새로운 영역 유형이 구현되었습니다. 이 영역은 Webex와의 통합에 필요한 모든 컨피그레이션을 미리 채웁니다. x12.5를 실행하고 Webex Hybrid Call을 구축하는 경우 Webex Zone 유형을 사용하여 Hybrid Call Services Domain(callservice.webex.com)이 자동으로 구성되도록 하는 것이 좋습니다. 이 값은 Mutual TLS 핸드셰이크 중에 표시되는 Webex 인증서의 Subject Alternate Name(주체 대체 이름)과 일치하며 Expressway에 대한 연결 및 인바운드 매핑이 성공하도록 허용합니다.

x12.5 아래의 코드 버전을 사용하고 있거나 Webex 영역을 사용하고 있지 않은 경우 Expressway가 인바운드 통화를 Webex Hybrid DNS 영역에 매핑하지 않는 문제를 식별하고 수정하는 방법을 설명하는 아래 설명을 계속 진행합니다.

이 기능은 3단계 프로세스로 분할됩니다.

1. Expressway-E는 Cisco Webex 인증서를 수락합니다.

2. Expressway-E는 Cisco Webex 인증서를 검사하여 TLS 확인 주체 이름과 일치하는 주체 대체 이름이 있는지 확인합니다. callservice.ciscopark.com.

3. Expressway-E는 Cisco Webex Hybrid DNS 영역을 통해 인바운드 연결을 매핑합니다.

인증이 실패하면 인증서 유효성 검사에 실패했음을 의미합니다. Expressway-E에서 Business-to-Business가 구성된 경우 통화가 기본 영역으로 진입하고 B2B 시나리오에 대해 제공된 검색 규칙에 따라 라우팅됩니다.

다른 시나리오와 마찬가지로, 진단 로깅 및 패킷 캡처를 모두 사용하여 이 오류의 모양을 확인한 다

음 패킷 캡처를 사용하여 RST를 전송하는 측면을 확인해야 합니다.다음은 시도되고 설정되는 TCP 연결의 샘플입니다.

```
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"
```

이제 TCP 연결이 설정되었으므로 TLS 핸드셰이크가 발생할 수 있습니다.핸드셰이크가 시작된 후 바로 확인할 수 있으며, 빠르게 오류가 발생합니다.

```
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"
```

pcap(pcap) 관점에서 이 상황을 살펴보면

- RST를 전송하는
- 올바른 인증서를 확인하기 위해 전달되는 인증서

이 특정 캡처를 분석할 때 Expressway-E가 RST를 전송함을 확인할 수 있습니다.전달된 Cisco Webex 인증서를 보면 전체 체인을 전송하는 것을 알 수 있습니다.또한 진단 로그의 오류 메시지를 기반으로 Expressway-E가 Cisco Webex Public CA를 신뢰하지 않는 시나리오를 제외할 수 있습니다.그렇지 않으면 "인증서 체인의 자체 서명 인증서"와 같은 오류가 표시됩니다. 이미지에 표시된 대로 패킷 세부 정보를 볼 수 있습니다.

The screenshot shows a packet capture in Wireshark. The top table lists several packets, with packet 70 highlighted in red, indicating a TCP segment with a RST flag. The packet details pane shows the following structure:

- Ethernet II, Src: e0:0e:da:c8:8c:f3 (e0:0e:da:c8:8c:f3), Dst: Vmware_58:9f:31 (00:0c:29:58:9f:31)
- Internet Protocol Version 4, Src: 148.62.40.52 (148.62.40.52), Dst: 172.16.2.2 (172.16.2.2)
- Transmission Control Protocol, Src Port: 44205 (44205), Dst Port: 5062 (5062), Seq: 5673, Ack: 4746, Len: 228
- [5 Reassembled TCP segments (5700 bytes): #54(1368), #56(1368), #59(1368), #60(1368), #62(228)]
- Secure Sockets Layer
 - TLSv1.2 Record Layer: Handshake Protocol: Multiple Handshake Messages
 - Content Type: Handshake (22)
 - Version: TLS 1.2 (0x0303)
 - Length: 5695
 - Handshake Protocol: Certificate
 - Handshake Type: Certificate (11)
 - Length: 5553
 - Certificates Length: 5550
 - Certificates (5550 bytes)
 - Certificate Length: 2338
 - Certificate (id-at-commonName=l2sip-cfa-01.ciscospark.com,id-at-organizationName=Cisco Systems, Inc.,id-at-localityName=San Jose,id-at-stateOrProvinceName=CA,id-at-countryName=US) Certificate Length: 1736
 - Certificate (id-at-commonName=HydrantID SSL ICA G2,id-at-organizationName=HydrantID (Avalanche Cloud Corporation),id-at-countryName=US) Certificate Length: 1467
 - Certificate (id-at-commonName=Quovadis Root CA 2,id-at-organizationName=Quovadis Limited,id-at-countryName=BM)

A blue arrow points to the RST packet in the packet list, and a red arrow points to the 'Expressway-E sends the RST' text in the details pane.

Webex 서버 인증서를 클릭하고 확장하면 Subject Alternate Names (dnsName)(주체 대체 이름 (dnsName)을 확인하여 callservice.ciscospark.com이 나열되었는지 확인할 수 있습니다.

Wireshark로 이동합니다.인증서 > 내선 번호 > 일반 이름 > 일반 이름 > dnsName:callservice.ciscospark.com

이는 Webex 인증서가 정상이라는 것을 완벽하게 확인합니다.

이제 TLS Verify Subject Name(TLS 확인 주체 이름)이 올바른지 확인할 수 있습니다. 앞서 언급한 대로 xConfiguration이 있는 경우 Zone Configuration(영역 컨피그레이션) 섹션을 참조하여 TLS 확인 주체 이름이 어떻게 구성되었는지 확인할 수 있습니다. xConfiguration에 대해 주목해야 할 한 가지는 영역 1과 함께 영역을 주문하는 것이 첫 번째 생성이라는 것입니다. 위에 분석된 문제의 환경의 xConfiguration입니다. TLS Verify Subject Name(TLS 확인 주체 이름)에 문제가 없는 것은 분명합니다.

```
*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"
```

다음으로 조사해야 하는 것은 **TLS 확인 인바운드 매핑**입니다. TLS 연결을 Webex Hybrid DNS 영역에 올바르게 매핑하는지 확인합니다. xConfiguration을 활용하여 이러한 정보를 분석할 수도 있습니다. xConfiguration에서 **TLS 확인 인바운드 매핑**은 **DNS ZIP TLS Verify InboundClassification**이라고 합니다. 이 예에서 볼 수 있듯이 이 값은 Off로 설정됩니다.

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

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

이 값이 Off로 설정된 경우 이는 VCS가 인바운드 TLS 연결을 이 영역에 매핑하려고 시도하지 못하도록 하는 것을 의미합니다. 따라서 Expressway-E에서 Business-to-Business가 구성된 경우 Business-to-Business 시나리오에 대해 제공된 검색 규칙에 따라 통화가 기본 영역으로 들어가서 확인 및 라우팅됩니다.

솔루션

이를 해결하려면 하이브리드 통화 DNS 영역에서 TLS 확인 인바운드 매핑을 켜기로 설정해야 합니다. 이를 완료하는 단계는 다음과 같습니다.

1. Expressway-E에 로그인
2. Configuration(컨피그레이션) > Zones(영역) > Zones(영역)로 이동합니다.
3. 하이브리드 통화 DNS 영역 선택
4. TLS 확인 인바운드 매핑에 대해 On(켜기)을 선택합니다.
5. 저장 선택

참고: 기본 로깅 동작은 를 참조하십시오. 이 섹션에서는 Expressway가 인증서 확인을 수행하고 Webex Hybrid DNS 영역에 매핑하는 방법을 보여 줍니다.

문제 7. Expressway-E는 기본 자체 서명 인증서를 사용합니다.

하이브리드 통화 서비스 연결의 일부 신규 구축에서 Expressway-E 인증서 서명은 무시되거나 기본 서버 인증서를 사용할 수 있다고 간주됩니다. Cisco Webex Control Hub를 사용하면 사용자 지정 인증서를 포털에 로드할 수 있기 때문에 이것이 가능하다고 생각하는 사람도 있습니다. (Services(서비스) > Settings(Hybrid Call Card(하이브리드 호출 카드 아래) > Upload(암호화된 통화의 인증서 아래))

암호화된 SIP 통화에 대한 인증서에 대한 문구에 자세히 주의를 기울이면 다음 내용이 표시됩니다. 'Cisco Collaboration 기본 신뢰 목록에서 제공된 인증서를 사용하거나 직접 업로드하십시오. 사용자 이름을 사용하는 경우 호스트 이름이 확인된 도메인에 있는지 확인하십시오.' 이 문의 핵심 요소는 "호스트 이름이 확인된 도메인에 있는지 확인"입니다.

이 조건과 일치하는 문제를 트러블슈팅할 때 증상이 통화 방향에 따라 달라집니다. 온-프레미스 전화로 통화가 시작된 경우 Cisco Webex 앱이 올리지 않을 것으로 예상할 수 있습니다. 또한 Expressway Search History(Expressway 검색 기록)에서 통화를 추적하려고 하면 통화가 Expressway-E로 전송되어 거기서 중지됩니다. 통화가 Cisco Webex 앱에서 시작되어 프레미스 대상으로 지정된 경우 온프레미스 전화가 올리지 않습니다. 이 경우 Expressway-E와 Expressway-Search History에는 아무것도 표시되지 않습니다.

이 특정 시나리오에서는 온-프레미스 전화기에서 통화가 시작되었습니다. Expressway-E Search History를 사용하여 통화가 서버에 연결되었는지 확인할 수 있습니다. 이 시점에서 진단 로깅을 통해 발생한 상황을 확인할 수 있습니다. 이 분석을 시작하려면 먼저 포트 5062를 통해 TCP 연결이 시도되고 설정되었는지 확인합니다. Expressway-E 진단 로그에서 "TCP Connecting"을 검색하고 "Dst-port=5062"라는 태그를 사용하여 행 항목을 검색하면 연결이 설정되는지 확인할 수 있습니다.

```
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"
```

이제 TCP 연결이 설정되었음을 확인했으므로 즉시 발생하는 상호 TLS 핸드셰이크를 분석할 수 있습니다. 여기 코드 조각에서 볼 수 있듯이 핸드셰이크가 실패하고 인증서를 알 수 없습니다 (Detail="sslv3 알린 인증서 알 수 없음").

```
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"
```

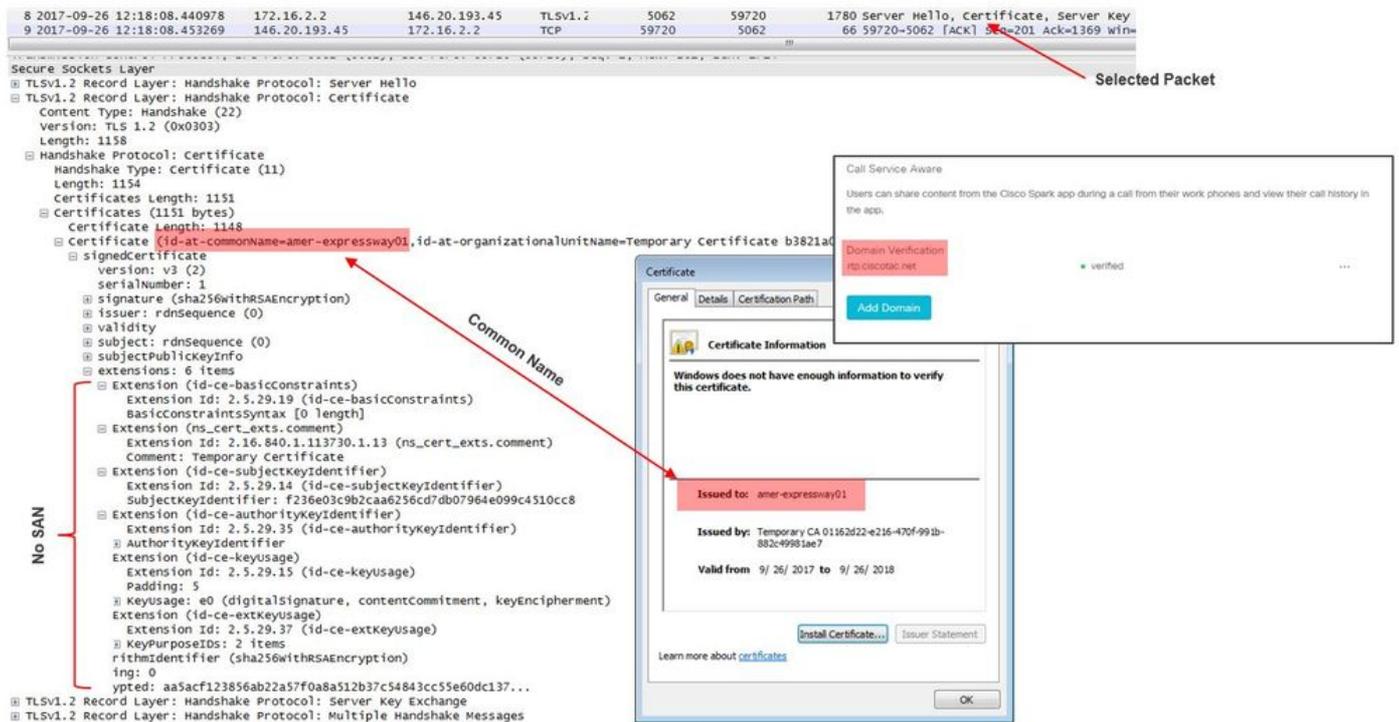
```
2017-09-26T08:18:08.455-04:00 amer-expressway01 tvcs: UTCTime="2017-09-26 12:18:08,455"
Module="network.tcp" Level="DEBUG": Src-ip="146.20.193.45" Src-port="59720" Dst-ip="172.16.2.2"
Dst-port="5062" Detail="TCP Connection Closed" Reason="Got EOF on socket"
```

Expressway-E 진단 로깅과 함께 제공된 패킷 캡처를 자세히 살펴보면, 이미지에 표시된 것처럼 Certificate Unknown(알 수 없는 인증서) 오류가 Cisco Webex의 방향에서 소싱되고 있음을 확인할 수 있습니다.

No.	Time	Source	Destination	Protocol	S Port	D Port	Length	Info
3	2017-09-26 12:18:08.415918	146.20.193.45	172.16.2.2	TCP	59720	5062	74	59720->5062 [SYN] Seq=0 win=14600 Len=0 MSS=1380 SACK_PERM=1 TSval=91375166 TSecr=0
4	2017-09-26 12:18:08.415941	172.16.2.2	146.20.193.45	TCP	5062	59720	74	5062->59720 [SYN, ACK] Seq=0 Ack=1 win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=95527051
5	2017-09-26 12:18:08.426317	146.20.193.45	172.16.2.2	TCP	59720	5062	66	59720->5062 [ACK] Seq=1 Ack=1 win=14720 Len=0 TSval=91375177 TSecr=955270515
6	2017-09-26 12:18:08.427715	146.20.193.45	172.16.2.2	TLSv1.2	59720	5062	266	client Hello
7	2017-09-26 12:18:08.427728	172.16.2.2	146.20.193.45	TCP	5062	59720	66	5062->59720 [ACK] Seq=1 Ack=201 win=30080 Len=0 TSval=955270527 TSecr=91375178
8	2017-09-26 12:18:08.440978	172.16.2.2	146.20.193.45	TLSv1.2	5062	59720	1780	Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Do
9	2017-09-26 12:18:08.453269	146.20.193.45	172.16.2.2	TCP	59720	5062	66	59720->5062 [ACK] Seq=201 Ack=1369 win=17536 Len=0 TSval=91375204 TSecr=955270540
10	2017-09-26 12:18:08.453308	146.20.193.45	172.16.2.2	TCP	59720	5062	66	59720->5062 [ACK] Seq=201 Ack=1715 win=20352 Len=0 TSval=91375204 TSecr=955270540
11	2017-09-26 12:18:08.455698	146.20.193.45	172.16.2.2	TLSv1.2	59720	5062	73	Alert (Level: Fatal, Description: Certificate Unknown)

Certificate Unknown Sourced from Spark

Expressway-E에서 기본 서버 인증서를 검사할 경우 'Common Name' 및 'Subject Alternate Names'에 'Verified Domain'(rtp.ciscotac.net)이 포함되지 않음을 확인할 수 있습니다. 그러면 이미지에 표시된 대로 이 문제의 원인에 대한 증거가 표시됩니다.



이 시점에서 Expressway-E 서버 인증서를 공용 CA 또는 내부 CA에서 서명해야 함을 확인했습니다

솔루션

이 문제를 해결하려면 두 가지 옵션이 있습니다.

- Expressway-E 인증서를 [Cisco Webex](#)가 신뢰하는 [공용 CA에서 서명하도록 합니다](#). Expressway에 로그인합니다.Maintenance(유지 관리) > Security(보안) > Server certificate(서버 인증서)로 이동합니다.Generate CSR을 선택합니다.필요한 인증서 정보를 입력하고 Additional alternative names(추가 대체 이름) 필드에 Webex Control Hub에 나열된 Verified Domain(확인된 도메인)이 포함되어 있는지 확인합니다.Generate CSR(CSR 생성)을 클릭합니다.서드파티 퍼블릭 CA에 CSR을 제공하여 서명합니다.인증서가 반환되면 Maintenance(유지 관리) > Security(보안) > Server certificates(서버 인증서)로 이동합니다.Select the server certificate file(서버 인증서 파일 선택) 옆에 있는 Upload New Certificate(새 인증서 업로드) 섹션에서 Choose File(파일 선택)을 선택하고 서명된 인증서를 선택합니다.Upload server certificate data를 선택합니다.Maintenance(유지 관리) > Security(보안) > Trusted CA certificate(신뢰할 수 있는 CA 인증서)로 이동합니다.Select the file contains trusted CA certificates(신뢰할 수 있는 CA 인증서가 포함된 파일 선택) 옆의 Upload(업로드) 섹션에서 Choose File(파일 선택)을 선택합니다.공용 CA에서 제공하는 루트 및 중간 CA 인증서를 선택합니다.Append CA certificate(CA 인증서 추가)를 선택합니다.Expressway-E를 다시 시작합니다.
- 내부 CA에서 Expressway-E 인증서를 서명한 다음 내부 CA 및 Expressway-E를 Cisco Webex Control Hub에 업로드합니다. Expressway에 로그인Maintenance(유지 관리) > Security(보안) > Server certificate(서버 인증서)로 이동합니다.CSR 생성 선택Additional alternative names 필드에 Webex Control Hub에 나열된 Verified Domain이 포함되도록 필요한 인증서 정보를 입력합니다.Generate CSR(CSR

생성)을 클릭합니다.서드파티 퍼블릭 CA에 CSR 제공인증서가 반환되면 Maintenance(유지 관리) > Security(보안) > Server certificates(서버 인증서)로 이동합니다.Select the server certificate file(서버 인증서 파일 선택) 옆에 있는 Upload New Certificate(새 인증서 업로드) 섹션에서 Choose File(파일 선택)을 선택하고 서명된 인증서를 선택합니다.서버 인증서 데이터 업로드 선택Maintenance(유지 관리) > Security(보안) > Trusted CA certificate(신뢰할 수 있는 CA 인증서)로 이동합니다.Select the file contains trusted CA certificates(신뢰할 수 있는 CA 인증서가 포함된 파일 선택) 옆의 Upload(업로드) 섹션에서 Choose File(파일 선택)을 선택합니다.공용 CA에서 제공하는 루트 및 중간 CA 인증서를 선택합니다.Append CA certificate(CA 인증서 추가)를 선택합니다.Expressway-E를 다시 시작합니다.

2a.Cisco Webex Control Hub에 내부 CA 및 Expressway-E 인증서 업로드

1. 관리자로 [Cisco Webex Control Hub](#)에 로그인합니다.
2. 서비스를 선택합니다.
3. 하이브리드 통화 서비스 카드 아래에서 설정을 선택합니다.
4. Certificates for Encrypted SIP Calls(암호화된 SIP 통화용 인증서) 섹션에서 Upload(업로드)를 선택합니다.
5. 내부 CA 및 Expressway-E 인증서를 선택합니다.

인바운드: Cisco Webex에서 온프레미스

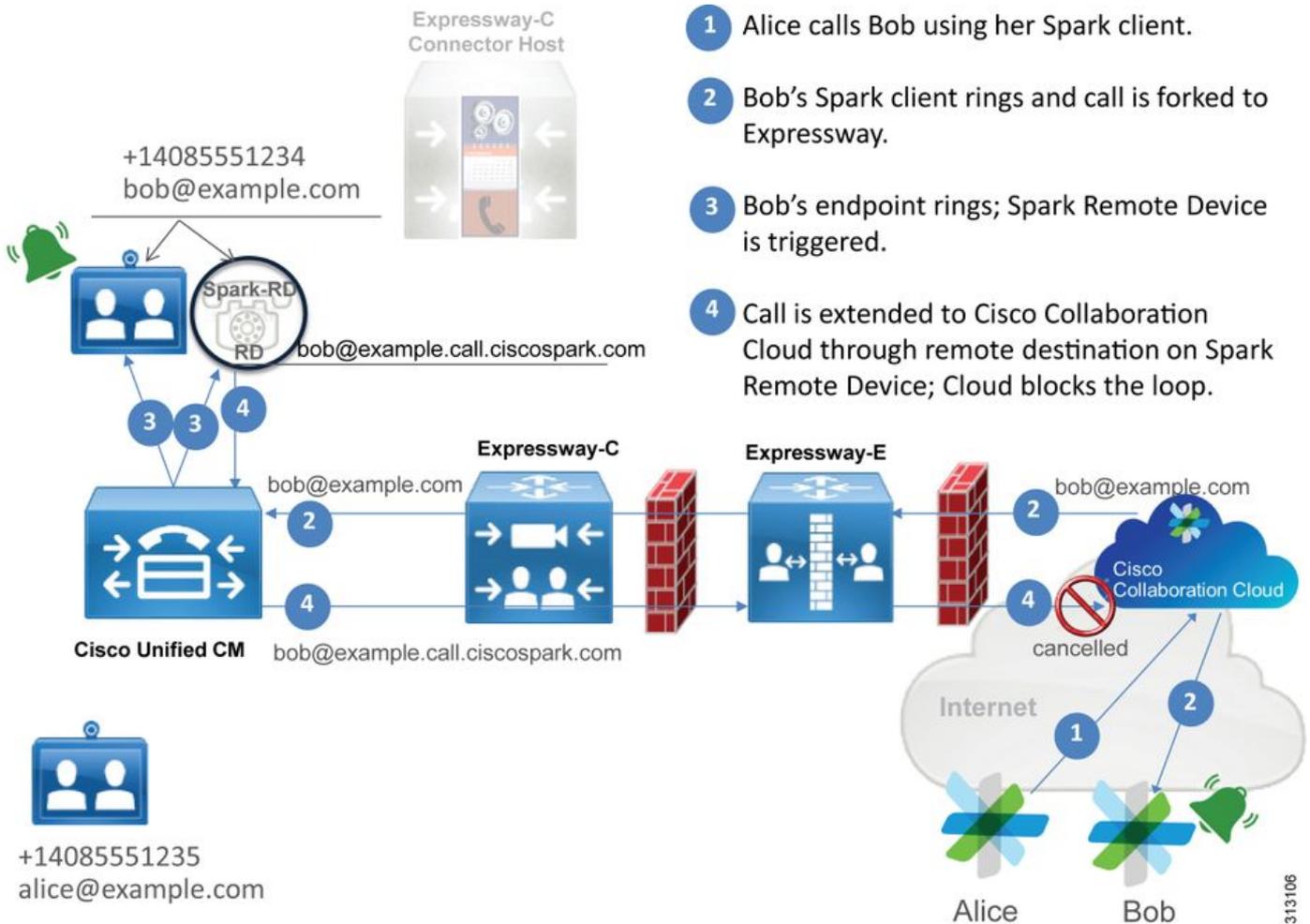
온프레미스 장애에 대한 거의 모든 인바운드 Cisco WebEx는 동일한 증상을 나타냅니다."Cisco Webex 앱에서 다른 동료의 앱으로 전화를 걸면 동료의 앱이 울렸지만 온프레미스 전화는 울리지 않습니다." 이 시나리오를 트러블슈팅하려면 이 유형의 통화가 발신될 때 발생하는 통화 흐름과 논리를 모두 이해하는 것이 도움이 됩니다.

하이 레벨 로직 흐름

1. Cisco Webex 앱 발신자가 통화를 시작합니다.
2. 전화한 상대방의 앱 링
3. 통화가 Cisco Webex 환경에 연결됨
4. Cisco Webex 환경은 Cisco Webex Control Hub에서 고객이 구성한 SIP 대상에 따라 DNS 조회를 수행해야 합니다.
5. Cisco Webex 환경은 포트 5062를 통해 Expressway에 연결하려고 시도합니다
6. Cisco Webex 환경은 상호 TLS 핸드셰이크를 수행하려고 시도합니다
7. Cisco Webex 환경은 온프레미스 협업 엔드포인트/IP 전화기로 전달되는 SIP INVITE를 Expressway로 전송합니다
8. Cisco Webex와 기업은 SIP 협상을 완료합니다.
9. Cisco Webex와 기업은 미디어를 보내고 받기 시작합니다.

통화 흐름

이미지에 표시된 대로 Cisco Webex app > Cisco Webex environment > Expressway-E > Expressway-C > On-Premises Collaboration Endpoint/IP Phone으로 이동합니다.



- 1 Alice calls Bob using her Spark client.
- 2 Bob's Spark client rings and call is forked to Expressway.
- 3 Bob's endpoint rings; Spark Remote Device is triggered.
- 4 Call is extended to Cisco Collaboration Cloud through remote destination on Spark Remote Device; Cloud blocks the loop.

다음은 Webex에서 온-프레미스 인프라로의 인바운드 통화에서 관찰된 몇 가지 일반적인 문제입니다.

문제 1. Cisco Webex에서 Expressway-E DNS SRV/호스트 이름을 확인할 수 없습니다.

Cisco Webex에서 온프레미스 통화 흐름에 대해 생각할 때 Cisco Webex의 첫 번째 논리적 단계는 온프레미스 Expressway에 연결하는 방법입니다. 위에서 설명한 대로 Cisco Webex는 [Cisco Webex Control Hub](#)의 **Hybrid Call Service Settings** 페이지에 나열된 구성된 **SIP Destination**에 따라 SRV 조회를 수행하여 온-프레미스 Expressway에 연결을 시도합니다.

Expressway-E 진단 로그 관점에서 이 문제를 해결하려고 시도하면 Cisco Webex의 트래픽이 표시되지 않습니다. TCP Connecting을 검색하려고 하면 Dst-port=5062가 표시되지 않으며, Cisco Webex에서 후속 MTLS 핸드셰이크 또는 SIP Invite가 표시되지 않습니다.

이 경우 Cisco Webex Control Hub에서 **SIP Destination**이 어떻게 구성되었는지 확인해야 합니다. 또한 **Hybrid Connectivity Test Tool**을 사용하여 트러블슈팅을 지원할 수 있습니다. 하이브리드 연결 테스트 도구는 유효한 DNS 주소가 있는지, Cisco Webex가 SRV 조회에서 반환된 포트에 연결할 수 있는지, 온-프레미스 Expressway에 Cisco Webex가 신뢰하는 유효한 인증서가 있는지 확인합니다.

1. [Cisco Webex Control Hub에 로그인](#)
2. 서비스 선택
3. 하이브리드 통화 카드에서 설정을 선택합니다.
4. Call Service Connect(통화 서비스 연결) 섹션에서 SIP Destination(SIP 대상) 필드에서 공용 SIP SRV 주소에 사용되는 도메인을 확인합니다.

5. 레코드를 올바르게 입력한 경우 **테스트**를 클릭하여 레코드가 유효한지 확인합니다.
6. 아래 그림과 같이, 퍼블릭 도메인에 해당 SIP SRV 레코드가 연결되어 있지 않음을 확인할 수 있습니다.

SIP Destination ⓘ

Test
Save

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

테스트 결과 보기를 선택하면 이미지에 표시된 대로 실패한 내용에 대한 자세한 정보를 볼 수 있습니다.

Verify SIP Destination ✕

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

또 다른 방법으로 nslookup을 사용하여 SRV 레코드를 조회할 수도 있습니다. 다음은 SIP 대상이 있는지 확인하기 위해 실행할 수 있는 명령입니다.

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

위의 코드 블록에서 볼 수 있듯이 nslookup 명령이 시작된 후 서버는 공용 Google DNS 서버인 8.8.8.8으로 설정됩니다. 마지막으로 레코드 유형을 SRV 레코드로 조회하도록 설정합니다. 그런 다음 조회하려는 전체 SRV 레코드를 실행할 수 있습니다. 결과적으로 요청이 시간 초과됩니다.

솔루션

1. 공용 도메인 이름을 호스트하는 데 사용하는 사이트의 Expressway-E에 대한 공용 SIP SRV 주소를 구성합니다.
2. Expressway-E의 공용 IP 주소로 확인할 호스트 이름을 구성합니다.
3. 1단계에서 생성한 SIP SRV 주소에 사용되는 도메인을 나열하도록 SIP 대상을 구성합니다. [Cisco Webex Control Hub](#)에 [로그인합니다](#). 서비스 **선택 하이브리드 통화 카드**에서 **설정 링크 선택** Call Service Connect(통화 서비스 연결) 섹션에서 공용 SIP SRV 주소에 사용되는 도메인을 SIP Destination(SIP 대상) 필드에 입력합니다. 저장 선택

참고:사용하려는 SIP SRV 레코드가 B2B 통신에 이미 활용되고 있는 경우 다음과 같이 기업 도메인의 하위 도메인을 Cisco Webex Control Hub의 SIP 검색 주소로 지정하고 그 결과 공용

DNS SRV 레코드를 지정하는 것이 좋습니다.

서비스 및 프로토콜: _sips._tcp.mtls.example.com

우선 순위:1

무게:10

포트 번호:5062

대상:us-expe1.example.com

위의 권장 사항은 [Cisco Webex Hybrid Design Guide](#)에서 직접 가져왔습니다.

대체 솔루션

고객이 SIP SRV 레코드를 가지고 있지 않으며(생성할 계획이 없는 경우) ":5062"로 접미사를 붙인 Expressway 공용 IP 주소를 나열할 수도 있습니다. 이렇게 하면 Webex 환경에서 SRV 조회를 시도하지 않고 **%Expressway_Pub_IP%:5062**에 직접 연결합니다(예:64.102.241.236:5062)

1. SIP 대상을 **%Expressway_Pub_IP%:5062**로 포맷하도록 구성합니다. (예: 64.102.241.236:5062) [Cisco Webex Control Hub](#)에 [로그인합니다](#). 서비스 선택 **하이브리드 통화 카드**에서 **설정 링크 선택** Call Service Connect(통화 서비스 연결) 섹션에서 **SIP Destination(SIP 대상)** 필드에 **%Expressway_Pub_IP%:5062**를 입력합니다. 저장 선택
설정해야 하는 SIP 대상 주소 및/또는 SRV 레코드에 대한 자세한 내용은 다음을 참조하십시오. Cisco Webex [Hybrid Call](#) Service 구축 가이드 또는 [Cisco Webex Hybrid Design Guide](#)의 Enable Hybrid Call Service Connect for Your Organization 섹션을 [참조하십시오](#).

문제 2. 소켓 실패:포트 5062가 Expressway로의 인바운드입니다.

DNS 확인이 완료되면 Cisco Webex 환경에서 DNS 조회 중에 반환된 IP 주소에 대해 포트 5062를 통한 TCP 연결을 설정하려고 시도합니다.이 IP 주소는 온-프레미스 Expressway-E의 공용 IP 주소가 됩니다.Cisco Webex 환경에서 이 TCP 연결을 설정할 수 없는 경우, 그 후 프리미엄 인바운드 통화가 실패합니다.이 특정 상태에 대한 증상은 다른 모든 Cisco Webex 인바운드 통화 실패와 동일합니다.온-프레미스 전화가 울리지 않습니다.

Expressway 진단 로그를 사용하여 이 문제를 해결하는 경우 Cisco Webex에서 어떤 트래픽도 표시되지 않습니다.TCP Connecting을 검색하려고 하면 Dst-port=5062에 대한 연결 시도가 표시되지 않으며 Cisco Webex에서 후속 MTLN 핸드셰이크 또는 SIP Invite가 표시되지 않습니다.이 상황에서는 Expressway-E 진단 로깅을 사용할 수 없으므로 몇 가지 확인 방법이 있습니다.

1. 방화벽 외부 인터페이스에서 패킷 캡처 가져오기
2. 포트 확인 유틸리티 활용
3. 하이브리드 연결 테스트 도구 사용

하이브리드 연결 테스트 도구는 Cisco Webex Control Hub에 바로 내장되어 있으며 온프레미스 Expressway에 연결하려는 Cisco Webex 환경을 시뮬레이션하므로 가장 이상적인 검증 방법입니다.조직에 대한 TCP 연결을 테스트하려면

1. [Cisco Webex Control Hub에 로그인](#)
2. 서비스 선택
3. 하이브리드 통화 카드에서 **설정을 선택합니다**.
4. Call Service Connect(통화 서비스 연결) 섹션에서 SIP Destination(SIP 대상)에 입력한 값이 올바른지 확인합니다.
5. 이미지에 표시된 대로 Test(테스트)를 클릭합니다.

SIP Destination ?

64.102.241.236:5062

Test

Save

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

6. 테스트가 실패했으므로 **테스트 결과 보기** 링크를 눌러 이미지에 표시된 대로 상세내역을 확인할 수 있습니다.

Verify SIP Destination ✕

IP address lookup

IP

64.102.241.236

Test for 64.102.241.236:5062

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

위 이미지에서 관찰한 것처럼 64.102.241.236:5062에 연결하려고 시도했을 때 소켓 테스트가 실패했음을 확인할 수 있습니다. Expressway 진단 로그/pcaps에 연결 시도가 표시되지 않는 데이터 외에도 방화벽 ACL/NAT/라우팅 컨피그레이션을 조사할 수 있는 충분한 증거가 있습니다.

솔루션

이 문제는 Cisco Webex 환경 또는 온프레미스 협업 장비에서 발생하는 것이 아니므로 방화벽 구성에 주력해야 합니다. 상호 작용할 방화벽의 유형을 반드시 예측할 수는 없으므로 해당 장치에 대해 잘 알고 있는 사람에게 의존해야 합니다. 방화벽 ACL, NAT 또는 라우팅 컨피그레이션 오류 등과 관련된 문제가 있을 수 있습니다.

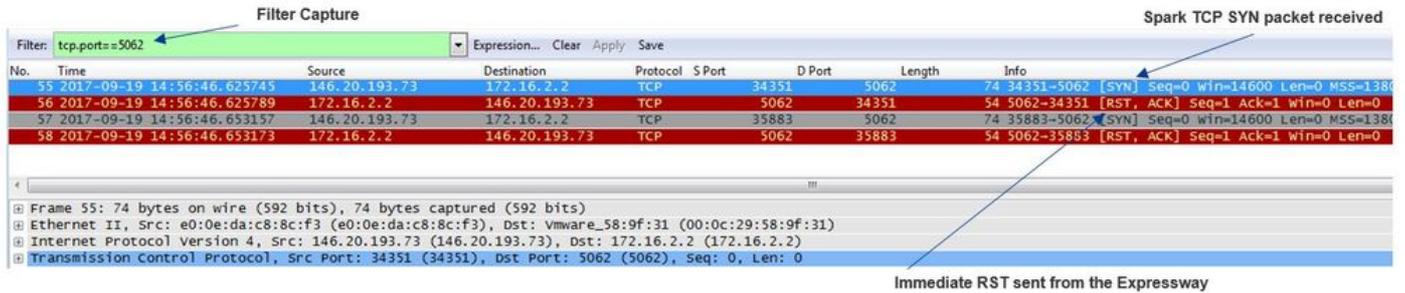
문제 3. 소켓 실패: Expressway-E가 포트 5062에서 수신 대기 중이 아님

이 특정 상황은 종종 잘못 진단됩니다. 방화벽이 포트 5062를 통한 트래픽이 차단되는 이유인 것으로 간주되는 경우가 많습니다. 이 특정 문제를 해결하려면 위의 "Port 5062 is blocked inbound to the Expressway" 시나리오에서 기술을 사용할 수 있습니다. Hybrid Connectivity Test 툴과 포트 연결을 확인하는 데 사용되는 다른 툴이 실패합니다. 첫 번째 가정은 방화벽이 트래픽을 차단하고 있다는 것입니다. 그런 다음 대부분의 사용자는 Expressway-E에서 진단 로깅을 다시 확인하여 설정하려는 TCP 연결을 볼 수 있는지 확인합니다. 일반적으로 이미지에 표시된 것과 같은 로그 라인 항목을 찾습니다.

```
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"
```

이 경우 위의 특정 로그 항목이 존재하지 않습니다. 따라서 많은 사람들이 상태를 잘못 진단하고 방화벽이라고 가정합니다.

패킷 캡처가 진단 로깅에 포함된 경우 방화벽이 원인이 아닌지 확인할 수 있습니다. 다음은 Expressway-E가 포트 5062를 통해 수신하지 못한 시나리오의 패킷 캡처 샘플입니다. 이 캡처는 이미지에 표시된 대로 적용된 필터로 `tcp.port==5062`를 사용하여 필터링됩니다.



Expressway-E에서 가져온 패킷 캡처에서 볼 수 있듯이 tcp 포트 5062를 통한 트래픽은 방화벽에 의해 차단되지 않고 실제로 도달하고 있습니다. 패킷 번호 56에서 Expressway-E가 초기 TCP SYN 패킷이 도착한 직후 RST를 전송하고 있음을 확인할 수 있습니다. 이 정보를 사용하여 문제가 패킷을 수신하는 Expressway-E로 격리되었다고 결론 내릴 수 있습니다. Expressway-E 관점에서 문제를 해결해야 합니다. 증거를 고려한다면 Expressway-E가 패킷을 RST하는 이유에 대한 가능한 이유를 고려하십시오. 이 동작에 영향을 미칠 수 있는 두 가지 가능성은 다음과 같습니다.

1. Expressway-E에는 트래픽을 차단할 수 있는 일부 유형의 방화벽 규칙이 설정되어 있습니다.
2. Expressway-E가 상호 TLS 트래픽을 수신하지 않거나 포트 5062를 통한 트래픽을 수신하지 않습니다.

Expressway-E의 방화벽 기능은 *System > Protection > Firewall rules > Configuration* 아래에 있습니다. 이 환경을 체크 인할 때 방화벽 구성이 없습니다.

Expressway-E가 포트 5062를 통해 Mutual TLS 트래픽을 수신하는지 확인하는 여러 가지 방법이 있습니다. 이 작업은 웹 인터페이스 또는 CLI를 통해 루트 사용자로 수행할 수 있습니다.

Expressway의 루트에서 `netstat -an`을 실행하는 경우 `| grep ':5062'`, 아래 표시된 것과 비슷한 출력을 얻을 수 있습니다.

```
~ # 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 :::5062             :::*                 LISTEN
```

이 정보는 Expressway-E의 웹 인터페이스를 통해 캡처할 수도 있습니다. 이 정보를 수집하려면 아래 단계를 참조하십시오.

1. Expressway-E에 로그인합니다.
2. 유지 관리 도구 > 포트 사용량 > 로컬 인바운드 포트에 이동합니다.
3. 유형 SIP 및 IP 포트 5062를 검색합니다(이미지에 표시된 대로 빨간색으로 강조 표시됨).

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

이제 무엇을 봐야 하는지 알고 있으므로 현재 환경과 비교할 수 있습니다. CLI의 관점에서 netstat -an을 실행할 때 | grep ':5062', 출력은 다음과 같습니다.

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

또한 웹 UI는 로컬 인바운드 포트 아래에 나열된 Mutual TLS 포트를 표시하지 않습니다

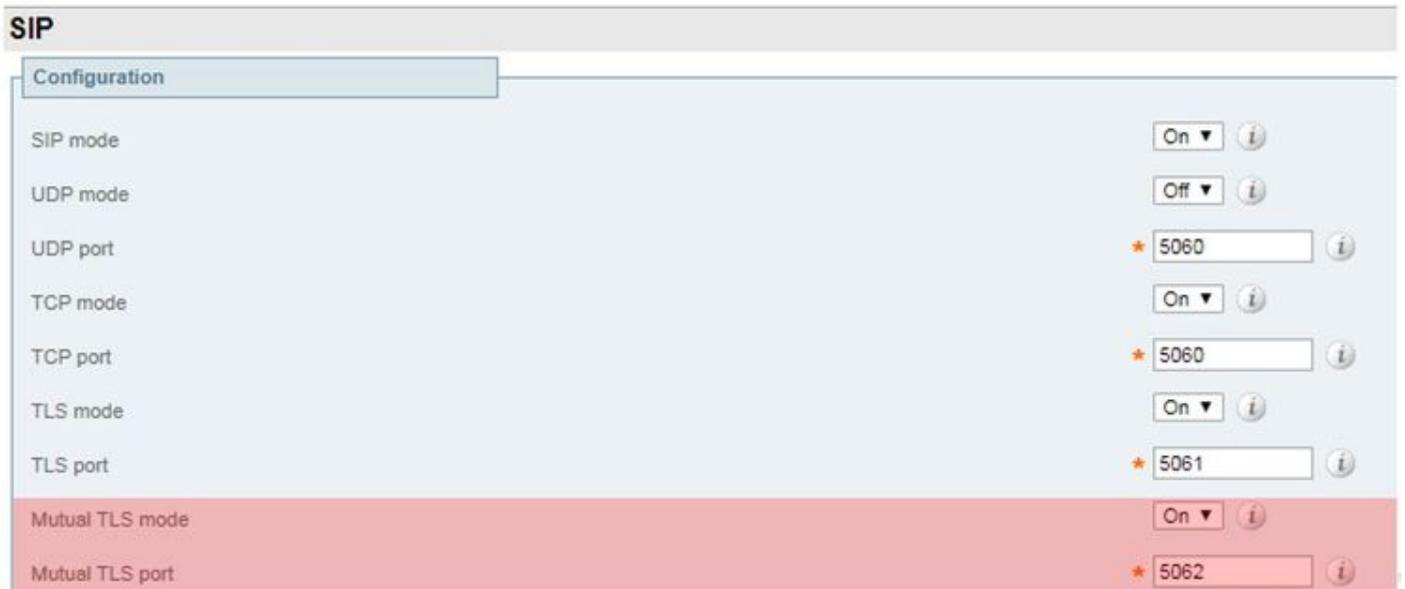
Type	Description	Protocol	IP address	IP port	Transport
H.323	Call signaling port range	H.323	192.168.1.6	15000-19999	TCP
H.323	Call signaling port range	H.323	172.16.2.2	15000-19999	TCP
H.323	Registration UDP port	H.323	192.168.1.6	1719	UDP
H.323	Registration UDP port	H.323	172.16.2.2	1719	UDP
SIP	TCP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

이 데이터를 사용하면 Expressway-E가 Mutual TLS 트래픽을 수신하지 않는다고 결론 내릴 수 있습니다.

솔루션

이 문제를 해결하려면 Mutual TLS 모드가 활성화되었고 Expressway-E에서 Mutual TLS 포트가 5062로 설정되었는지 확인해야 합니다.

1. Expressway-E에 로그인
2. Configuration(컨피그레이션) > Protocols(프로토콜) > SIP로 이동합니다.
3. Mutual TLS 모드가 On으로 설정되어 있는지 확인합니다.
4. Mutual TLS 포트가 5062로 설정되었는지 확인합니다.
5. 이미지에 표시된 대로 저장을 클릭합니다.



문제 4. Expressway-E 또는 C는 사전 로드된 SIP 경로 헤더를 지원하지 않습니다.

하이브리드 통화 서비스 연결을 사용하면 **경로 헤더**를 기반으로 통화 라우팅이 수행됩니다. 경로 헤더는 솔루션의 Call Service Aware(Expressway Connector) 부분이 Cisco Webex에 제공하는 정보를 기반으로 채워집니다. Expressway 커넥터 호스트는 Unified CM을 쿼리하여 Call Service에 대해 활성화되고 **디렉터리 URI**와 **Unified CM 홈 클러스터의 클러스터 FQDN**을 모두 가져옵니다. Alice와 Bob을 사용하여 다음 예를 참조하십시오.

디렉터리 URI	대상 경로 헤더
bob@example.com	emea-cucm.example.com
alice@example.com	us-cucm.example.com

Alice 또는 Bob이 전화를 걸면 통화가 온-프레미스 Unified CM으로 라우팅되므로 전화를 받은 사용자에게 라우팅하기 전에 해당 통화가 Cisco WebexRD에 고정될 수 있습니다.

Alice가 Bob에게 전화를 걸 경우 통화는 *Alice의 Unified CM 홈 클러스터 FQDN(us-cucm.example.com)*으로 라우팅됩니다. Cisco Webex가 Expressway-E로 인바운드를 전송하는 SIP INVITE를 분석하면 SIP 헤더 내에서 다음 정보를 찾을 수 있습니다

요청 URI sip:bob@example.com
경로 헤더 sip:us-cucm.example.com;lr

Expressway 관점에서 검색 규칙은 요청 URI가 아니라 **Route Header(us-cucm.example.com)**(이 경우 Alice의 Unified CM 홈 클러스터)에서 통화를 라우팅하도록 구성됩니다.

이 기반 집합을 사용하면 Expressway가 잘못 구성된 상황을 해결할 수 있으며, 이 경우 위의 논리가 작동하지 않습니다. 다른 거의 모든 인바운드 하이브리드 통화 서비스 연결 통화 설정 실패와 마찬가지로 온프레미스 전화기가 울리지 않는다는 증상이 나타납니다.

Expressway에서 진단 로그를 분석하기 전에 이 통화를 식별하는 방법을 고려하십시오.

1. SIP 요청 URI는 수신자의 디렉터리 URI가 됩니다.
2. SIP FROM 필드는 **Calling Party(발신자)**가 "First Name Last Name" <sip:WebexDisplayName@subdomain.call.ciscospark.com>으로 나열된 형식으로 지정됩니다.

이 정보를 사용하여 발신자의 디렉터리 URI, 발신자의 이름과 성 또는 발신자의 Cisco Webex SIP 주소로 진단 로그를 검색할 수 있습니다. 이 정보가 없는 경우 Expressway를 통해 실행 중인 모든 SIP 호출을 찾는 "INVITE SIP:"를 검색할 수 있습니다. 인바운드 통화에 대한 SIP INVITE를 식별한 다음 SIP 통화 ID를 찾아 복사할 수 있습니다. 이 값이 있으면 통화 ID를 기반으로 진단 로그를 검색하여 이 통화 레그와 연결된 모든 메시지를 볼 수 있습니다.

라우팅 문제를 격리할 수 있는 또 다른 방법은 통화가 엔터프라이즈로 얼마나 멀리 이동하는지 확인하는 것입니다. Expressway-C에 위에 표시된 정보를 검색하여 통화가 그렇게 라우팅되었는지 확인할 수 있습니다. 만약 그렇다면, 여러분은 그곳에서 조사를 시작하고 싶을 것입니다.

이 시나리오에서는 Expressway-C가 Expressway-E에서 INVITE를 수신했음을 확인할 수 있습니다.

```
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
```


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

작업 시나리오와 비교했을 때 작업 시나리오에서 라우터 헤더(클러스터 FQDN)를 기반으로 검색 논
리가 수행되고 있음을 확인할 수 있습니다

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'"**
그러면 Expressway-C가 통화를 Unified CM(192.168.1.21)으로 올바르게 전달하는 것을 확인할 수 있습니다.

2017-09-22T13:56:02.232-04:00 rtp12-tpdmz-118-VCSC tvcs: UTCTime="2017-09-22 17:56:02,232"
Module="network.sip" Level="DEBUG": Action="Sent" Local-ip="192.168.1.5" Local-port="25606" Dst-ip="192.168.1.21" Dst-port="5065" Msg-Hash="866788495063340574"
SIPMSG:
|INVITE sip:jorobb@rtp.ciscotac.net SIP/2.0
Via: SIP/2.0/TCP 192.168.1.5:5060;egress-zone=CUCM11;branch=z9hG4bK251d6daf044e635607cc13d244b9ea45138220.69ccb8de20a0e853c1313782077f77b5;proxy-call-id=17aa8dc7-422c-42ef-bdd9-b9750fbd0edf;rport
Via: SIP/2.0/TLS 192.168.1.6:7003;egress-zone=HybridCallServiceTraversal;branch=z9hG4bKba323da436b2bc288200d56d11f02d4d272;proxy-call-id=32c76cef-e73c-4911-98d0-e2d2bb6fec77;received=192.168.1.6;rport=7003;ingress-zone=HybridCallServiceTraversal
Via: SIP/2.0/TLS 192.168.1.6:5073;branch=z9hG4bK06cde3f662d53a210b5b4b11b85500c19;x-cisco-local-service=nettle;received=192.168.1.6;rport=42533;ingress-zone=DefaultZone
Via: SIP/2.0/TLS 64.102.241.236:5061;egress-zone=DefaultZone;branch=z9hG4bK297799f31d0785ff7449e1d7dbe3595b271.2ed90cbcd5b79c6cffad9ecd84cc8337;proxy-call-id=3be87d96-d2e6-4489-b936-8f9cb5ccaa5f;received=172.16.2.2;rport=25005
Via: SIP/2.0/TLS 192.168.4.146:5062;branch=z9hG4bK043ca6360f253c6abed9b23fbfeff9819;received=148.62.40.64;rport=36149;ingress-zone=HybridCallServicesDNS
Via: SIP/2.0/TLS 127.0.0.1:5070;branch=z9hG4bK-353038-8c648a16c2c5d7b85fa5c759d59aa190;rport=47732
Call-ID: daa1a6fa546ce76591fc464f0a50ee32@127.0.0.1
CSeq: 1 INVITE
Contact: <sip:192.168.1.6:5073;transport=tls>;call-type=squared
From: "pstoiano test" <sip:pstoiano-test@dmzlab.call.ciscopark.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)

Expressway-C에 문제를 격리하고 특정 오류(404 찾을 수 없음)를 발생시킨 진단 로깅을 분석한 후에는 이러한 유형의 동작을 발생시킬 수 있는 요소에 집중할 수 있습니다.고려해야 할 몇 가지 사항은 다음과 같습니다.

1. 통화는 검색 규칙을 통해 Expressway의 영역 내부 및 외부로 이동합니다.
2. Expressway는 라우터 헤더를 포함하는 SIP INVITE 요청을 처리하는 Preloaded SIP 경로 지원이라는 논리를 사용합니다.이 값은 Expressway-C 및 Expressway-E의 영역(Traversal 서버, Traversal 클라이언트, Neighbor)에서 설정 또는 해제할 수 있습니다.

이제 xConfiguration을 사용하여 Expressway-E Traversal 서버 및 Expressway-C 클라이언트 영역, 특히 Hybrid Call Service Connect에 대해 설정된 컨피그레이션을 볼 수 있습니다.영역 컨피그레이션 외에도 이 통화를 한 영역에서 다른 영역으로 통과하도록 구성된 검색 규칙을 분석할 수 있습니다.또한 Expressway-E가 Expressway-C로 통화를 전달하여 Traversal 서버 영역 컨피그레이션이 올바르게 설정되었을 가능성이 높습니다.

이 문제를 해결하려면 아래 xConfig에서 이 영역의 이름을 **Hybrid Call Service Traversal**이라고 합니다.TraversalServer 영역 유형의 유형입니다.SIP TCP 포트 7003을 통해 Expressway-C에 통신합니다.

Hybrid Call Service의 핵심 요소는 On(켜기) SIP 경로 지원을 미리 로드해야 한다는 것입니다. Expressway 웹 인터페이스는 이 값을 **Preloaded SIP 경로 지원**을 호출하는 반면 xConfiguration은 이를 SIP PreloadedSipRoutes Accept로 표시합니다.

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"

```

이 영역에 검색 규칙 3(Webex Hybrid)이 연결되어 있는지 확인할 수도 있습니다. 기본적으로 Search Rule은 Hybrid Call Services의 DNS 영역을 통해 들어오는 "Any" 별칭을 보내고 이를 위의 Hybrid Call Service Traversal 영역으로 전달합니다. 예상대로 Expressway-E의 Search Rule(검색 규칙)과 Traversal Server(통과 서버) 영역이 모두 올바르게 구성됩니다.

```

*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"

```

Expressway-C의 xConfiguration에 주력하는 경우 먼저 Webex Hybrid의 Traversal Client 영역을 찾을 수 있습니다. Expressway-E xConfiguration(SIP 포트:"7003") 따라서 xConfiguration에서 올바른 영역을 신속하게 식별할 수 있습니다.

전과 같이 Zone Name(Hybrid Call Service Traversal), Type(Traversal Client) 및 SIP PreloadedSipRoutes Accept(사전 로드된 SIP 경로 지원)에 대해 구성된 내용을 배울 수 있습니다. 이 xConfiguration에서 볼 수 있듯이 이 값은 Off로 설정됩니다. Cisco Webex Hybrid Call Services용 구축 가이드를 기반으로 이 값을 On으로 설정해야 합니다.

또한 사전 로드된 SIP 경로 지원의 정의를 확인하면 이 값이 Off로 설정되어 있고 INVICEe에 경로 헤더가 포함되어 있는 경우 Expressway-C에서 메시지를 거부해야 한다는 것을 명확히 확인할 수 있습니다. "이 헤더가 포함된 SIP INVITE 요청을 영역에서 거부하도록 하려면 Switch Preloaded SIP routes support Off를 사용합니다."

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/1lYDd760/6KrHGA7g8bJs="
*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"

```

이 시점에서 Expressway-C Traversal 클라이언트 영역 컨피그레이션의 잘못된 컨피그레이션으로 문제를 격리했습니다. Preloaded SIP 경로 지원을 On으로 전환해야 합니다.

솔루션

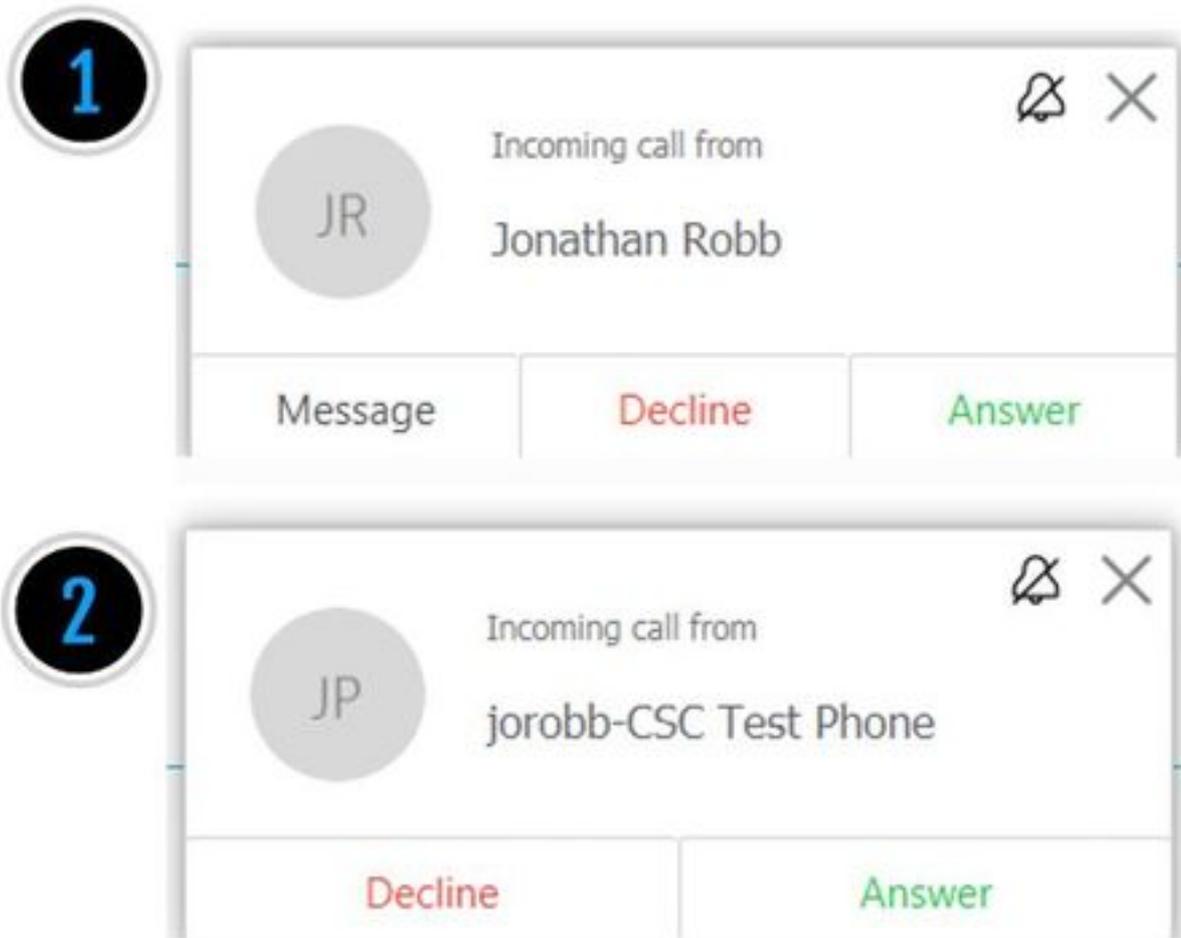
사전 로드된 SIP 경로 지원을 올바르게 설정하려면

1. Expressway-C에 로그인
2. Configuration(컨피그레이션) > Zones(영역) > Zones(영역)로 이동합니다.
3. Hybrid Call Service Traversal 클라이언트 영역을 선택합니다(이름은 고객마다 다를 수 있음).
4. Preloaded SIP 경로 지원을 On으로 설정
5. 저장 선택

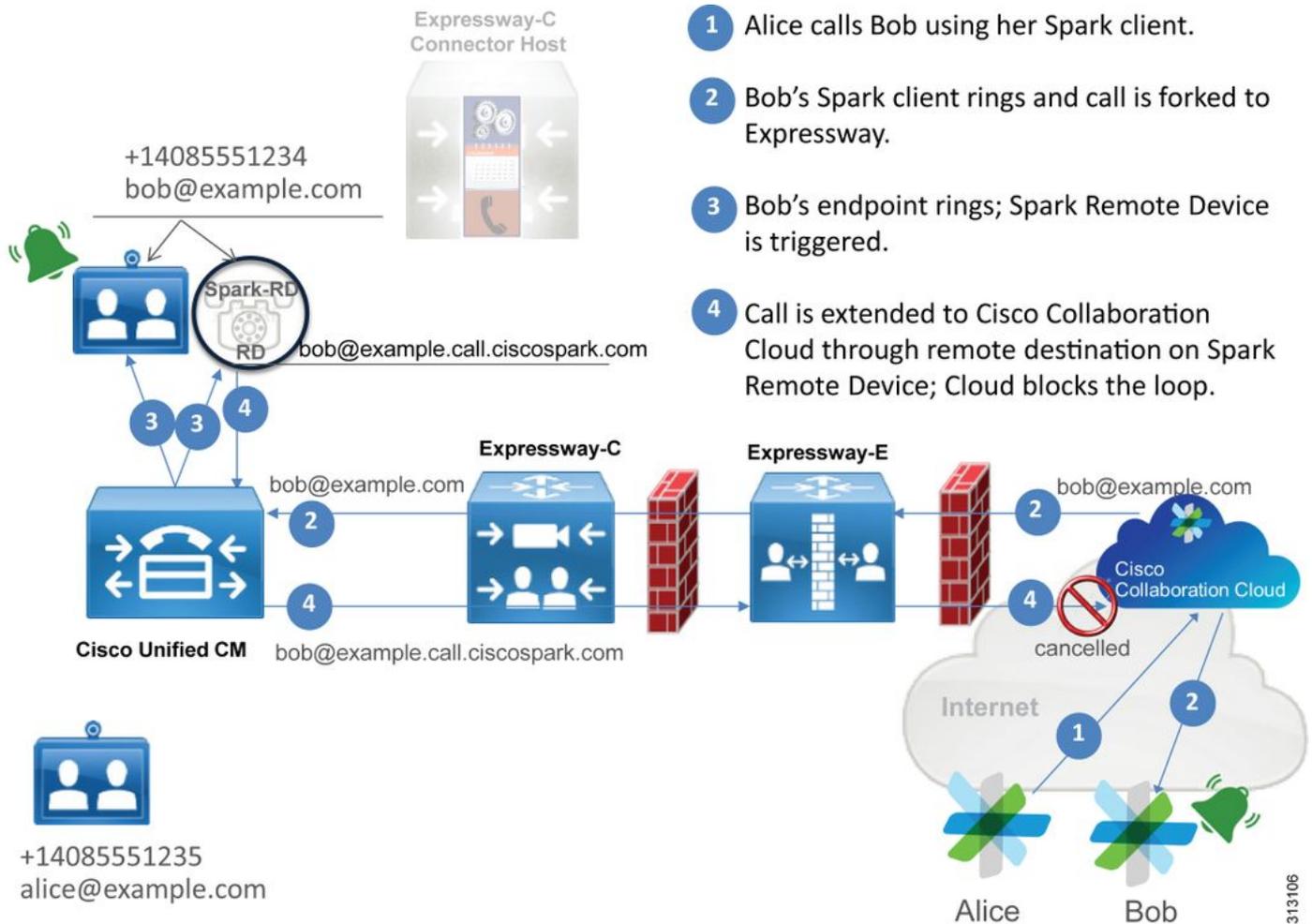
참고: 이 시나리오에서는 Expressway-C의 실패를 보여주었지만, Webex Hybrid Call Traversal Server 영역에서 사전 로드된 SIP 경로 지원이 해제된 경우 Expressway-E에서 동일한 진단 로깅 오류를 볼 수 있습니다. 이 경우 Expressway-C에 통화가 도달하는 것을 본 적이 없을 것이며 Expressway-E는 통화를 거부하고 404 Not Found를 전송하는 역할을 담당했을 것입니다.

문제점 5. Cisco Webex 앱에서 2개의 통화 알림(토스트)을 받고 있습니다.

이 특정 문제는 통화가 끊기지 않는 유일한 인바운드 통화 시나리오입니다. 이 문제와 관련하여 전화를 받은 사람(수신자)이 전화를 건 사람(발신자)으로부터 Cisco Webex 앱에서 2개의 알림(토스트)을 받고 있습니다. 첫 번째 알림은 Cisco Webex에서 생성되며 두 번째 알림은 온프레미스 인프라에서 제공됩니다. 다음은 이미지에 표시된 대로 수신되는 두 알림의 샘플입니다.



첫 번째 알림(toast)은 Cisco Webex 측에서 통화를 개시하는 사람(발신자)의 것입니다. 이 인스턴스의 발신 ID는 해당 통화를 시작하는 사용자의 표시 이름입니다. 두 번째 알림(toast)은 전화를 거는 사용자에게 할당된 온-프레미스 CTI 또는 Cisco Webex RD에서 제공됩니다. 처음에, 이 행동은 이상하게 보인다. 그러나 Cisco Webex Hybrid Call Design Guide에서 인바운드 통화 다이어그램을 검토할 경우 이미지에 표시된 것처럼 동작이 더 적합합니다.



이 그림에서 Alice가 Cisco Webex 앱에서 Bob에게 전화를 걸고 있으며 통화가 온프레미스로 전달되고 있음을 확인할 수 있습니다. 이 통화는 Bob의 전화기에 할당된 디렉터리 URI와 일치해야 합니다. 문제는 이 설계에서 디렉터리 URI가 CTI-RD 또는 Cisco Webex RD에도 할당된다는 점입니다. 따라서 CTI-RD 또는 Cisco Webex RD에 통화가 제공되면 해당 디바이스에 bob@example.call.ciscospark.com에 대해 구성된 원격 대상이 있기 때문에 통화가 Cisco Webex로 다시 전송됩니다. Cisco Webex가 이러한 상황을 처리하는 방식은 특정 통화 레그를 취소한다는 것입니다.

Cisco Webex가 통화 레그를 올바르게 취소하려면 Cisco Webex는 처음에는 지정된 레그를 취소하려고 하는 매개변수를 SIP 헤더에 넣어야 했습니다. Cisco Webex가 SIP INVITE에 삽입하는 매개변수를 "call-type=squared"라고 하며 이 값은 Contact 헤더에 입력됩니다. 이 값이 메시지에서 제거되면 Cisco Webex는 통화를 취소하는 방법을 알지 못합니다.

이 정보를 통해 Cisco Webex 사용자 Jonathan Robb이 전화를 걸었을 때 사용자의 Cisco Webex 앱이 2개의 알림(토스트)을 수신한 앞에서 설명한 시나리오를 다시 살펴볼 수 있습니다. 이러한 유형의 문제를 해결하려면 항상 Expressway-C 및 Expressway-E에서 진단 로깅을 수집해야 합니다. 시작점으로, Expressway-E 로그를 검토하여 SIP INVITE가 실제로 최초 Cisco Webex INVITE가 인바운드될 때 보낸 연락처 헤더에 있는 call-type=squared 값이 있는지 확인할 수 있습니다. 이렇게 하면 방화벽에서 어떤 방식으로든 메시지를 조작하지 않습니다. 다음은 이 시나리오에서 Expressway-E로 인바운드되는 INVITE의 샘플 조각입니다.

```
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:

Contact 헤더에 **call-type=제곱** 값이 있습니다.이 시점에서 통화를 Expressway를 통해 라우팅하고 Webex Hybrid Traversal Server 영역에서 전송해야 합니다.Expressway-E 로그를 검색하여 Expressway-E에서 통화가 전송된 방법을 확인할 수 있습니다.그러면 Expressway-E가 어떤 식으로든 INVITE를 조작하는지 알 수 있습니다.

2017-09-19T14:01:48.468-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 18:01:48,468"
Module="network.sip" Level="DEBUG": **Action="Sent"** Local-ip="192.168.1.6" Local-port="7003" Dst-ip="192.168.1.5" Dst-port="26686" Msg-Hash="1847271284712495612"

SIPMSG:

INVITE sip:pstojano-test@rtp.ciscotac.net SIP/2.0
Via: SIP/2.0/TLS 192.168.1.6:7003;**egress-zone=HybridCallServiceTraversal**;branch=z9hG4bKec916b02b6d469abad0a30b93753f4b0859;proxy-call-id=d7372034-85d1-41f8-af84-dffed6d1a9a9;rport
Via: SIP/2.0/TLS 192.168.1.6:5073;branch=z9hG4bKd91699370129b4c10d09e269525de00c2;x-cisco-local-service=nettle;received=192.168.1.6;rport=43119;ingress-zone=DefaultZone
Via: SIP/2.0/TLS 64.102.241.236:5061;egress-zone=DefaultZone;branch=z9hG4bK52aac9a181192566e01b98ae0280bdf858.0e65cdf078cabb269e6cb6bce1328be;proxy-call-id=ec51e8da-e1a3-4210-95c9-494d12debc8;received=172.16.2.2;rport=25016
Via: SIP/2.0/TLS
192.168.5.164:5062;branch=z9hG4bK564cd36d87f3417513c9b559dc666f71;received=146.20.193.73;rport=40342;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>

Expressway-E에서 Expressway-C로 전송되는 이 SIP INVITE를 검토할 때 Contact 헤더에 **call-type=squared**가 없습니다.하나 더 지적할 것은 라인 항목 4에서 이그레스 영역이

HybridCallServiceTraversal과 동일하다는 것입니다. 이제 Cisco Webex 앱이 전화를 걸 때 두 번째 알림(toast)을 받는 이유는 Expressway-E가 SIP INVITE Contact 헤더에서 **call-type=squared** 태그를 제거했기 때문이라고 결론을 수 있습니다. 답변할 질문은 이 헤더 제거 원인이 무엇인지에 대한 것입니다.

통화가 Expressway에서 설정한 하이브리드 통화 서비스 통과를 통해 라우팅되어야 하므로 조사를 시작할 수 있습니다. xConfiguration이 있는 경우 이 영역이 어떻게 구성되었는지 확인할 수 있습니다. xConfiguration에서 Zone을 식별하려면 로그에 인쇄되는 Via 행에 기록된 이름을 사용하면 됩니다. 위에서 egress-zone=HybridCallServiceTraversal이라고 하는 것을 볼 수 있습니다. 이 이름이 SIP 헤더의 Via 줄에 인쇄되면 공백이 제거됩니다. xConfiguration(x컨피그레이션) 관점에서 실제 영역 이름은 공백을 포함하며 하이브리드 통화 서비스 통과에서 포맷됩니다.

```
*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"
```

Hybrid Call Service Traversal에 대해 식별된 설정을 사용하여 다음과 같이 눈에 띄는 잠재적인 설정을 찾을 수 있습니다.

- SIP PreloadedSIPRoutes Accept:켜짐
- SIP 매개 변수만 유지 모드:꺼짐

Expressway의 웹 인터페이스를 사용하면 이러한 값의 정의 및 작업을 확인할 수 있습니다.

사전 로드된 SIP 경로 지원

Switch Preloaded SIP routes support On을 사용하면 이 영역에서 Route 헤더가 포함된 SIP INVITE 요청을 처리할 수 있습니다.

영역에 이 헤더가 포함된 SIP INVITE 요청을 거부하도록 하려면 Switch Preloaded SIP routes support Off를 사용합니다.

SIP 매개 변수 보존

Expressway의 B2BUA가 이 영역을 통해 라우팅된 SIP 요청의 매개 변수를 보존할지 또는 다시 쓰는지 결정합니다.

이 영역과 B2BUA 간의 라우팅 요청의 SIP 요청 URI 및 연락처 매개변수를 보존합니다.

필요한 경우 B2BUA에서 이 영역과 B2BUA 간에 라우팅되는 요청의 SIP 요청 URI 및 연락처 매개 변수를 재작성할 수 있습니다.

이러한 정의에 따라 xConfiguration과 **call-type=제공** 값이 SIP INVITE의 "Contact" 헤더에 배치된다는 점을 통해 Hybrid Call Service Traversal 영역에서 SIP 매개 변수 보존 값을 Off로 설정하면 태그가 제거되고 Cisco Webex 앱에서 이중 벨소리 알림을 받고 있다는 결론을 내릴 수 있습니다.

솔루션

SIP INVITE의 Contact 헤더에 **call-type=제공** 값을 유지하려면 Expressway가 통화를 처리하는 모든 영역에 대해 SIP 매개 변수 보존을 지원하는지 확인해야 합니다.

1. Expressway-E에 로그인
2. Configuration(컨피그레이션) > **Zones(영역)** > **Zones(영역)**로 이동합니다.
3. 하이브리드 접근 서버에 사용 중인 영역 선택
4. SIP 매개 변수 보존 값을 On으로 **설정**
5. 설정을 저장합니다.

#####

참고:이 시나리오에서는 Expressway-E의 Webex Hybrid Traversal Server 영역이 잘못 구성되었습니다.Webex Hybrid Traversal 클라이언트 또는 CUCM 인접 영역에서 SIP 매개변수 보존 값을 Off로 설정할 수 있다는 점에 유의하십시오.이 두 컨피그레이션은 모두 Expressway-C에서 수행됩니다. 이 경우 Expressway-E가 **call-type=squared** 값을 Expressway-C로 전송했을 것이며 Expressway-C에서 이 값을 분리했을 것입니다.

아웃바운드:온프레미스-Cisco Webex

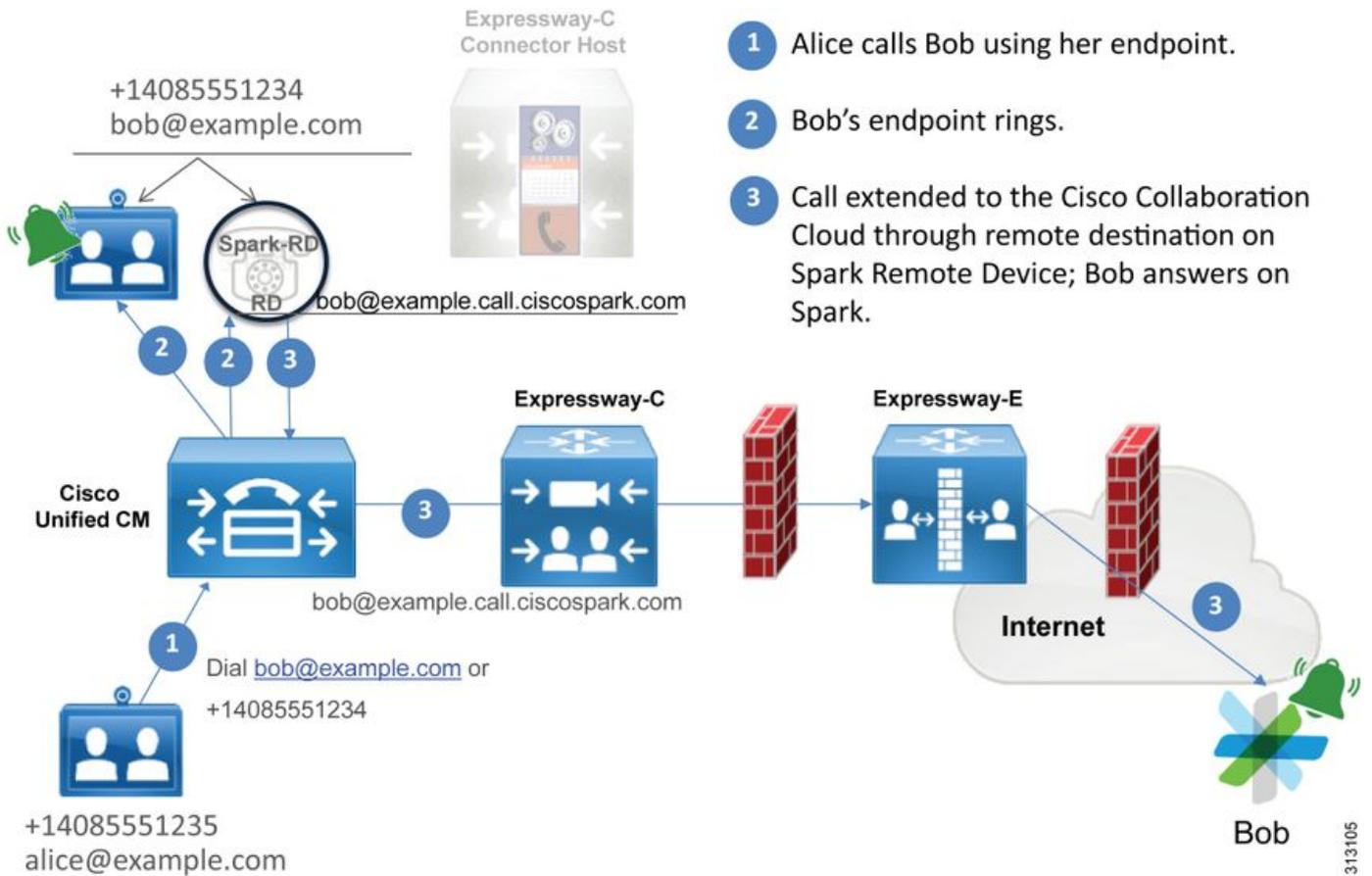
Cisco Webex에 대한 아웃바운드 온프레미스(on-premises)와 관련된 거의 모든 통화 장애에 동일한 증상이 보고됩니다."Unified CM 등록 전화기에서 Call Service Connect를 사용할 수 있는 다른 사용자로 전화를 걸면 해당 사용자의 온프레미스 전화가 울렸지만 Cisco Webex 앱은 울리지 않습니다." 이 시나리오를 트러블슈팅하려면 이 유형의 통화가 발신될 때 발생하는 통화 흐름과 논리를 모두 이해하는 것이 중요합니다.

하이 레벨 로직 흐름

1. 사용자 A가 온 프레미스 전화기에서 사용자 B의 디렉토리 URI로 전화를 겁니다.
2. 사용자 B의 온-프레미스 전화 및 CTI-RD/Webex-RD에서 통화 수락
3. 사용자 B의 온-프레미스 전화기가 울리기 시작
4. 사용자 B의 CTI-RD/Webex-RD는 이 통화를 목적지(UserB@example.call.ciscospark.com)으로 전환합니다.
5. Unified CM은 이 통화를 Expressway-C로 전달합니다.
6. Expressway-C는 통화를 Expressway-E로 보냅니다.
7. Expressway-E는 callservice.ciscospark.com 도메인에서 DNS 조회를 수행합니다.
8. Expressway-E는 포트 5062를 통해 Cisco Webex 환경에 연결하려고 시도합니다.
9. Expressway-E와 Cisco Webex 환경에서 상호 핸드셰이크를 시작합니다.
10. Cisco Webex 환경은 사용자 B의 사용 가능한 Cisco Webex 앱으로 통화를 전달합니다.
11. 사용자 B의 사용 가능한 Cisco Webex 앱이 울리기 시작합니다.

통화 흐름

이미지에 표시된 대로 **User B on-prem phone > Unified CM > CTI-RD/Webex-RD > Expressway-C > Expressway-E > Cisco Webex environment > Cisco Webex app**로 이동합니다.



참고: [Cisco Webex Hybrid Design Guide](#)에서 이미지를 가져왔습니다.

로그 분석 팁

Cisco Webex로의 아웃바운드 포워드된 통화가 실패한 문제를 해결하는 경우 Unified CM, Expressway-C 및 Expressway-E 로그를 수집해야 합니다. 이러한 로그 집합을 확보하면 통화가 환경을 통해 전달되는 방식을 확인할 수 있습니다. 온-프레미스 환경에서 통화가 얼마나 멀리 연결되는지 쉽게 알 수 있는 또 다른 방법은 Expressway "검색 기록"을 사용하는 것입니다. Expressway Search History(Expressway 검색 기록)를 사용하면 Cisco Webex에 대한 포크된 통화가 Expressway-C 또는 E에 연결되는지 확인할 수 있습니다.

검색 기록을 사용하려면 다음을 수행할 수 있습니다.

1. Expressway-E에 로그인

테스트 호출

Status(상태) > Search History(검색 기록)로 이동합니다.

호출해야 하는 Webex SIP URI의 대상 주소가 있는 통화가 있는지 확인합니다

(user@example.call.ciscospark.com).

검색 기록에 Expressway-E 검색 히스토리 통화가 표시되지 않으면 Expressway-C에서 이 프로세스를 반복합니다

Expressway에서 진단 로그를 분석하기 전에 이 통화를 식별하는 방법을 고려하십시오.

1. SIP 요청 URI는 Cisco Webex 사용자의 SIP 주소가 됩니다.

2. SIP FROM 필드는 발신자가 "First Name Last Name" < sip:Alias@Domain>으로 표시되도록

형식이 지정됩니다.

이 정보를 사용하여 발신자의 디렉토리 URI, 발신자의 이름과 성 또는 발신자의 Cisco Webex SIP 주소로 진단 로그를 검색할 수 있습니다. 이 정보가 없는 경우 Expressway를 통해 실행 중인 모든 SIP 통화를 찾는 "INVITE SIP:"를 검색할 수 있습니다. 아웃바운드 통화에 대한 SIP INVITE를 확인했으면 SIP Call-ID를 찾아 복사할 수 있습니다. 이 작업을 수행한 후에는 통화 ID를 기반으로 진단 로그를 검색하여 이 통화 레그와 연결된 모든 메시지를 볼 수 있습니다.

다음은 Call Service Connect를 사용할 수 있는 사용자에게 전화를 걸 때 Unified CM 등록 전화기에서 Cisco Webex 환경으로의 아웃바운드 통화에서 가장 일반적인 몇 가지 문제입니다.

문제 1. Expressway에서 callservice.ciscospark.com 주소를 확인할 수 없습니다.

Expressway DNS 영역의 표준 운영 절차는 요청 URI의 오른쪽 및 측면에 표시되는 도메인을 기반으로 DNS 조회를 수행하는 것입니다. 이를 설명하려면 예를 들어 보십시오. DNS 영역이 **pstojano-test@dmzlab.call.ciscospark.com**의 요청 URI가 있는 통화를 받아야 하는 경우 일반적인 Expressway DNS 영역은 요청 URI의 오른쪽의 **dmzlab.call.ciscospark.com**에서 DNS SRV 조회 논리를 수행합니다. Expressway에서 이 작업을 수행하는 경우 다음 조회 및 응답이 발생할 것으로 예상할 수 있습니다.

```
_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
```

자세히 살펴보면 SRV 레코드 응답에서 서버 주소 및 포트 5061을 제공하지만 5062는 제공하지 않습니다.

즉, 포트 5062를 통해 발생하는 Mutual TLS 핸드셰이크가 발생하지 않으며 Expressway와 Cisco Webex 간의 시그널링에 별도의 포트가 사용됩니다. 문제는 *Cisco Webex Hybrid Call Services*용 구축 가이드가 포트 5061의 사용을 명시적으로 호출하지 않는다는 것입니다. 일부 환경에서는 비즈니스 통화를 허용하지 않기 때문입니다.

Expressway에서 이 표준 DNS 영역 SRV 조회 논리를 통과하는 방법은 사용자가 제공한 값을 기반으로 명시적 검색을 수행하도록 Expressway를 구성하는 것입니다.

이제 이 특정 통화를 분석할 때 통화가 이렇게 진행되었음을 (검색 기록 사용) 결정했으므로 Expressway-E에 집중할 수 있습니다. Expressway-E로 들어오는 첫 번째 SIP INVITE부터 시작하여 들어오는 영역, 사용 중인 검색 규칙, 통화가 나가는 영역, DNS 영역으로 올바르게 전송된 경우 어떤 DNS 조회 논리가 발생하는지 확인합니다.

```
2017-09-19T13:18:50.562-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 17:18:50,556"  
Module="network.sip" Level="DEBUG": Action="Received" Local-ip="192.168.1.6" Local-port="7003"  
Src-ip="192.168.1.5" Src-port="26686" Msg-Hash="4341754241544006348"  
SIPMSG:  
|INVITE sip:pstojano-test@dmzlab.call.ciscospark.com SIP/2.0  
Via: SIP/2.0/TLS 192.168.1.5:5061;egress-  
zone=HybridCallServiceTraversal;branch=z9hG4bK6d734eaf7a6d733bd1e79705b7445ebb46175.1d33be65c99c  
56898f85df813f1db3a7;proxy-call-id=47454c92-2b30-414a-b7fe-aff531296bcf;rport  
Via: SIP/2.0/TCP 192.168.1.21:5065;branch=z9hG4bK13187594dd412;received=192.168.1.21;ingress-  
zone=CUCM11  
Call-ID: 991f7e80-9c11517a-130ac-1501a8c0@192.168.1.21  
CSeq: 101 INVITE
```

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

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

To:

Max-Forwards: 15
Record-Route: <sip:proxy-call-id=47454c92-2b30-414a-b7fe-aff531296bcf@192.168.1.5:5061;transport=tls;lr>
Record-Route: <sip:proxy-call-id=47454c92-2b30-414a-b7fe-aff531296bcf@192.168.1.5:5060;transport=tcp;lr>
Allow: INVITE,OPTIONS,INFO,BYE,CANCEL,ACK,PRACK,UPDATE,REFER,SUBSCRIBE,NOTIFY
User-Agent: Cisco-CUCM11.5
Expires: 180
Date: Tue, 19 Sep 2017 17:18:50 GMT
Supported: timer,resource-priority,replaces,X-cisco-srtp-fallback,X-cisco-original-called
Session-Expires: 1800
Min-SE: 1800
Allow-Events: presence
X-TAATag: 2272025a-ce36-49d0-8d93-cb6a5e90ffe0
Session-ID: 75957d4fb66a13e835c10737aa332675;remote=00000000000000000000000000000000
Cisco-Guid: 2568978048-0000065536-0000000148-0352430272
Content-Type: application/sdp
Content-Length: 714

<SDP Omitted>

이 SIP INVITE에서 요청 URI(pstojano-test@dmzlab.call.ciscospark.com), 통화 ID(991f7e80-9c11517a-130ac-1501a8c0), From ("Jonathan Rob" <sip:5010@rtp.ciscotac.net>) 및 (pstojano-test@dmzlab.call.ciscospark.com)을 수집할 수 있습니다. 사용자 에이전트(Cisco-CUCM11.5). 이 INVITE가 수신되면 Expressway는 통화를 다른 Zone으로 라우팅할 수 있는지 여부를 결정하기 위해 논리 결정을 내려야 합니다.Expressway는 검색 규칙에 따라 이 작업을 수행합니다.

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'"

위의 로그 조각에 따라 Expressway-E가 네 개의 검색 규칙을 통해 구문 분석되었지만 단 하나의 (Webex Hybrid - to Webex Cloud)만 고려되었습니다.검색 규칙은 우선 순위가 90이고 하이브리드 통화 서비스 DNS 영역으로 이동하도록 지정되었습니다.통화가 DNS 영역으로 전송되므로 Expressway-E에서 발생하는 DNS SRV 조회를 검토할 수 있습니다

```

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"

```

위의 코드 조각에서 Expressway-E가 요청 URI(_sips._tcp.dmzlab.call.ciscospark.com)의 오른쪽에 있는 SRV 조회를 수행했으며 l2sip-cfa-01.wbx2.com 및 포트 5061의 호스트 이름으로 확인되었음을 확인할 수 있습니다. 호스트 이름 l2sip-cfa-01.wbx2.com은 146.20.193.64으로 확인됩니다. 이 정보를 사용하여 Expressway에서 수행할 다음 논리적 단계는 TCP SYN 패킷을 146.20.193.64에 전송하여 통화를 설정하려고 시도하는 것입니다. Expressway-E 로깅에서 이러한 문제가 발생하는지 검토할 수 있습니다.

```

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"

```

위의 Expressway-E 진단 로깅 조각에서 Expressway-E가 이전에 TCP 포트 5061을 통해 해결되었던 IP 146.20.193.64에 연결하려고 시도하지만 이 연결이 완전히 실패하는 것을 확인할 수 있습니다. 수집된 패킷 캡처에서도 동일한 내용을 볼 수 있습니다.

Expressway-E attempts TCP Connection

No.	Time	Source	Destination	Protocol	S Port	D Port	Length	Info
3878	2017-09-19 17:18:08.801765	68.67.59.22	172.16.2.2	TCP	25876	5061	66	25876->5061 [FIN, ACK] Seq=1 Ack=1 win=0 Len=0 TSval=231154828 TSecr=4109470239
3879	2017-09-19 17:18:08.801923	172.16.2.2	68.67.59.22	TCP	5061	25876	66	5061->25876 [FIN, ACK] Seq=2 Ack=2 win=0 Len=0 TSval=4111465862 TSecr=231154828
3882	2017-09-19 17:18:08.822153	68.67.59.22	172.16.2.2	TCP	25876	5061	66	25876->5061 [ACK] Seq=2 Ack=2 win=362 Len=0 TSval=231154849 TSecr=4111465862
8109	2017-09-19 17:18:25.110830	192.33.146.113	172.16.2.2	TCP	50714	5061	60	50714->5061 [RST, ACK] Seq=1 Ack=1 win=312 Len=0
14878	2017-09-19 17:18:51.145472	172.16.2.2	146.20.193.64	TCP	25010	5061	74	25010->5061 [SYN] Seq=0 win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=314491012 TSecr=0 WS=128
15158	2017-09-19 17:18:52.203226	172.16.2.2	146.20.193.64	TCP	25010	5061	74	[TCP Retransmission] 25010->5061 [SYN] Seq=0 win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=314491012 TSecr=0 WS=128
15302	2017-09-19 17:18:54.231224	172.16.2.2	146.20.193.64	TCP	25010	5061	74	[TCP Retransmission] 25010->5061 [SYN] Seq=0 win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=314491012 TSecr=0 WS=128
15470	2017-09-19 17:18:55.283326	172.16.2.2	146.20.193.64	TCP	25010	5061	74	[TCP Retransmission] 25010->5061 [SYN] Seq=0 win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=314491012 TSecr=0 WS=128
15577	2017-09-19 17:19:01.328621	172.16.2.2	146.20.193.64	TCP	25011	5061	74	25011->5061 [SYN] Seq=0 win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=314501195 TSecr=0 WS=128
17846	2017-09-19 17:19:02.379327	172.16.2.2	146.20.193.64	TCP	25011	5061	74	[TCP Retransmission] 25011->5061 [SYN] Seq=0 win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=314501195 TSecr=0 WS=128
18425	2017-09-19 17:19:04.427323	172.16.2.2	146.20.193.64	TCP	25011	5061	74	[TCP Retransmission] 25011->5061 [SYN] Seq=0 win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=314501195 TSecr=0 WS=128
19459	2017-09-19 17:19:08.499322	172.16.2.2	146.20.193.64	TCP	25011	5061	74	[TCP Retransmission] 25011->5061 [SYN] Seq=0 win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=314501195 TSecr=0 WS=128

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

이러한 결과에 따르면 포트 5061을 통한 트래픽이 성공하지 못하는 것은 분명합니다. 그러나 Hybrid Call Service Connect는 5061이 아닌 TCP 포트 5062를 사용하기 위한 것입니다. 따라서 Expressway-E에서 포트 5062를 반환하는 SRV 레코드를 확인하지 않는 이유를 고려해야 합니다. 이 질문에 답하기 위해 Expressway-E Webex Hybrid DNS 영역에서 가능한 구성 문제를 찾을 수 있습니다.

```

*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"
```

Expressway-E의 xConfiguration에서 DNS 조회와 관련된 두 가지 특별한 관심 값이 있음을 확인할 수 있습니다. **DNSOverride Name** 및 **DNSOverride Override**. 이 xConfiguration을 기반으로 DNSOverride Override가 Off로 설정되어 있으므로 DNSOverride Name이 적용되지 않습니다. 이러한 값이 수행하는 작업을 더 잘 이해하려면 Expressway 웹 UI를 사용하여 값의 정의를 조회할 수 있습니다.

DNS 요청 수정(xConfig에서 DnsOverride Override로 변환)

이 영역에서 발신 SIP 통화를 다이얼된 대상의 도메인 대신 수동으로 지정된 SIP 도메인으로 라우팅합니다. 이 옵션은 주로 Cisco Webex Call Service와 함께 사용하기 위한 것입니다. www.cisco.com/go/hybrid-services을 [참조하십시오](#).

검색할 도메인(xConfig에서 DnsOverride Name으로 변환)

아웃바운드 SIP URI에서 도메인을 검색하는 대신 DNS에서 찾을 FQDN을 입력합니다. 원래 SIP URI는 영향을 받지 않습니다.

이제 이러한 정의가 있으므로 올바르게 설정되면 이러한 값이 DNS 조회 로직과 전적으로 관련이 있습니다. Cisco Webex Hybrid Call Services용 구축 가이드의 문장과 이 정보를 결합할 경우 Modify DNS Request(DNS 요청 수정)가 On(켜기)으로 설정되어 있고 검색할 도메인을 **callservice.ciscospark.com**으로 설정해야 합니다. 올바른 정보를 지정하기 위해 이러한 값을 변경하면 DNS SRV 조회 논리가 완전히 달라지게 됩니다. 아래는 Expressway-E 진단 로깅 관점에서 기대할 수 있는 것의 일부입니다

```
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"
```

솔루션

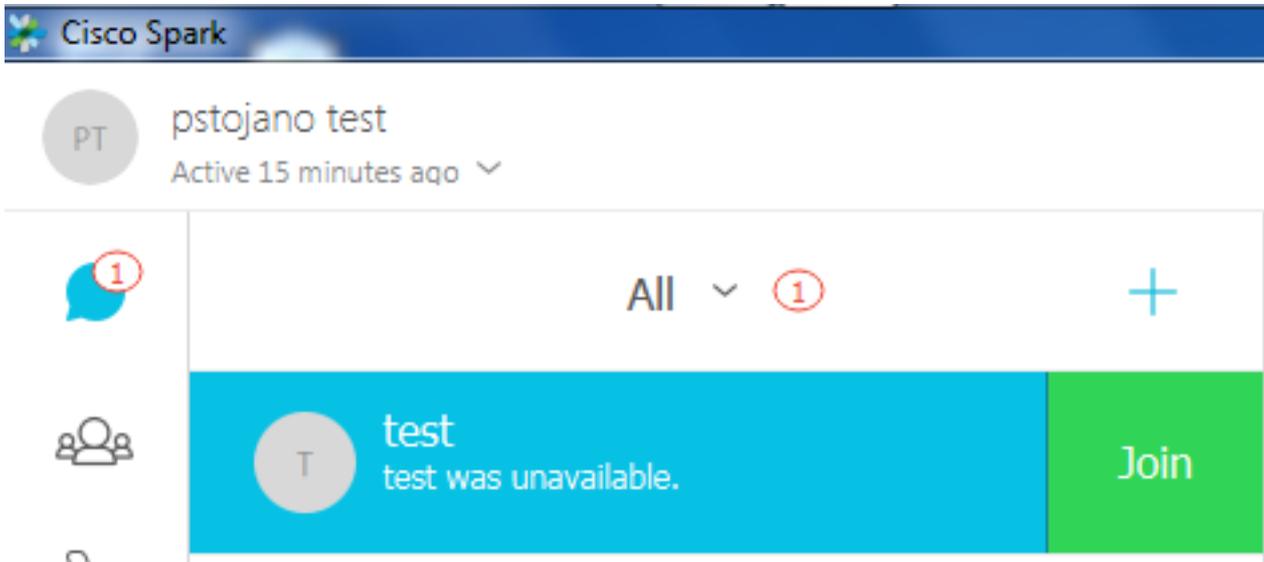
1. Expressway-E에 로그인
2. Configuration Zones(컨피그레이션 영역) > Zones(영역)로 이동합니다.
3. 구성된 Webex Hybrid DNS 영역 선택
4. Modify DNS request(DNS 수정 요청)를 On으로 설정
5. 값을 검색할 도메인을 callservice.ciscospark.com으로 설정합니다.
6. 변경 내용 저장

참고: Expressway에 DNS 영역이 하나만 사용되는 경우 이러한 값을 활용할 수 있는 하이브리드 통화 서비스와 함께 사용할 별도의 DNS 영역을 구성해야 합니다.

문제 2. 포트 5062가 Cisco Webex로의 아웃바운드 차단됨

Cisco Webex에 대한 포크된 아웃바운드 통화 실패에 대해 고유한 한 가지는 전화를 건 사람이 전화를 건 적이 없음에도 불구하고 전화한 상대방의 Cisco Webex 앱이 해당 앱에 Join(가입) 버튼을 표시한다는 점입니다. 위의 시나리오와 같이 이 문제와 관련하여 오류가 발생한 위치를 가장 잘 파악하려면 동일한 톨과 로깅을 다시 사용해야 합니다. 통화 문제 격리 및 로그 분석에 대한 팁은 이미지에 표시된 대로 이 문서의 섹션을 참조하십시오.

표시되는 조인 단추의 그림



아웃바운드 통화 문제 #1과 마찬가지로 Expressway의 검색 기록을 사용하여 통화가 그렇게 멀리까지 이동하는지 확인했으므로 Expressway-E 진단 로깅에서 분석을 시작할 수 있습니다. 이전과 같이 Expressway-C에서 Expressway-E로 들어오는 초기 INVITE로 시작합니다. 찾을 사항은 다음과 같습니다.

1. Expressway-E가 INVITE를 수신하는지 여부
2. 검색 규칙 논리가 하이브리드 DNS 영역으로 통화를 전달할지 여부
3. DNS 영역이 DNS 조회를 수행하는지, 올바른 도메인에서 수행되는지 여부
4. 시스템이 포트 5062에 대한 TCP 핸드셰이크를 시도하여 올바르게 설정했는지 여부
5. 상호 TLS 핸드셰이크의 성공 여부

```
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:pstoiano-test@dmzlab.call.ciscospark.com SIP/2.0
Via: SIP/2.0/TLS 192.168.1.5:5061;egress-
zone=HybridCallServiceTraversal;branch=z9hG4bK57d8d5c823824bcddfd62f6ff7e09f9939482.899441b6d60c
444e4ed58951d07b5224;proxy-call-id=696f6f1c-9abe-47f3-96a4-e26f649fb76f;rport
Via: SIP/2.0/TCP 192.168.1.21:5065;branch=z9hG4bK12d4b77c97a64;received=192.168.1.21;ingress-
zone=CUCM11
Call-ID: 6a48de80-9c11273a-12d08-1501a8c0@192.168.1.21
CSeq: 101 INVITE
Call-Info: <urn:x-cisco-remotecall:callinfo>;x-cisco-video-traffic-class=DESKTOP
Remote-Party-ID: "Jonathan Robb"
<sip:5010@rtp.ciscotac.net>;party=calling;screen=yes;privacy=off
Contact: <sip:5010@192.168.1.21:5065;transport=tcp>;video;audio
From: "Jonathan Robb"
```

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

To:

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

위 INVITE에서 볼 수 있듯이 INVITE는 정상적으로 수신됩니다. 이는 "수신" 작업이며 Expressway-C IP 주소에서 가져옵니다. 이제 검색 규칙 로직으로 이동할 수 있습니다.

```
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'"
```

위의 로그 조각을 기반으로 Expressway-E가 4개의 검색 규칙을 통해 구문 분석되었지만 단 한 개의 검색 규칙만 분석되었음을 확인할 수 있습니다 (*Webex Hybrid - Webex Cloud*) 고려되었습니다. Search Rule은 우선 순위가 90이고 하이브리드 통화 서비스 DNS 영역. 통화가 DNS 영역으로 전송되므로 Expressway-E에서 발생하는 DNS SRV 조회를 검토할 수 있습니다. 이 모든 것은 완전히 정상입니다. 이제 DNS Lookup 로직에 집중할 수 있습니다

```
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:'12sip-cfa-02.wbx2.com' Port:'5062' Priority:'5' TTL:'300' Weight:'10' (SRV)  
Hostname:'12sip-cfa-01.wbx2.com' Port:'5062' Priority:'5' TTL:'300' Weight:'10' (SRV) Number of  
relevant records retrieved: 4"
```

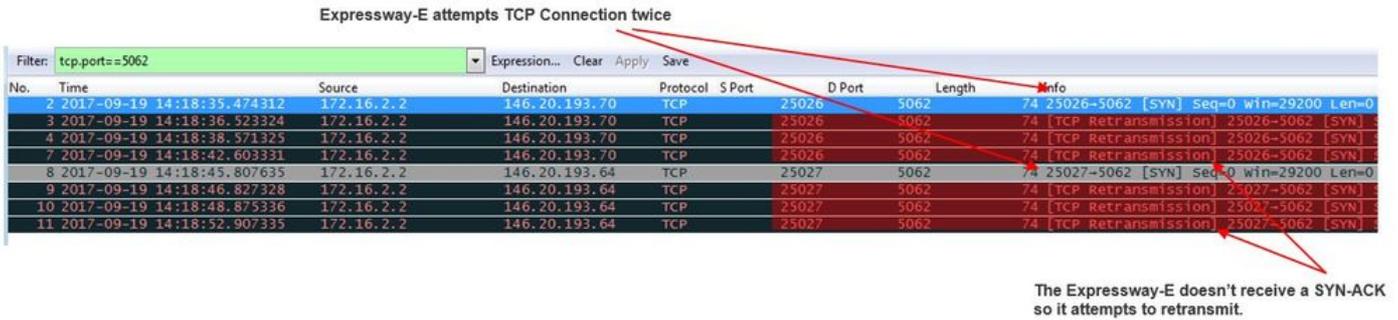
이 인스턴스에서 callservice.ciscospark.com SRV 레코드가 확인되었음을 확인할 수 있습니다. 응답은 4개의 서로 다른 유효한 레코드이며 모두 포트 5062를 사용합니다. 이는 정상적인 동작입니다. 이

제 다음에 올 TCP 핸드셰이크를 분석할 수 있습니다. 문서에서 앞서 언급한 대로 진단 로그에서 "TCP 연결"을 검색하고 Dst-port="5062"를 나열하는 라인 항목을 찾을 수 있습니다. 다음은 이 시나리오에서 볼 수 있는 샘플입니다.

```
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"
```

또한 진단 로깅 번들에 포함된 tcpdump를 사용하여 이미지에 표시된 대로 TCP 핸드셰이크에 대한 자세한 정보를 얻을 수 있습니다.

Expressway-E attempts TCP Connection twice



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

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

이 시점에서 Expressway-E가 통화를 올바르게 라우팅하고 있다고 결론지을 수 있습니다. 이 시나리오의 문제는 Webex 환경에서 TCP 연결을 설정할 수 없다는 것입니다. Webex 환경이 TCP SYN 패킷에 응답하지 않기 때문에 이러한 문제가 발생할 수 있지만, 연결을 처리하는 서버가 많은 고객 간에 공유되는 경우에는 이러한 문제가 발생할 수 있습니다. 이 시나리오에서 발생할 가능성이 높은 원인은 중간 장치(방화벽, IPS 등)의 유형이 트래픽을 허용하지 않는 것입니다.

솔루션

문제가 격리되었으므로 이 데이터는 고객의 네트워크 관리자에게 제공해야 합니다. 또한 추가 정보가 필요한 경우 에지 디바이스 및/또는 방화벽의 외부 인터페이스에서 캡처를 해제하여 추가 증거를 얻을 수 있습니다. Expressway의 관점에서, 이 문제는 해당 디바이스에 상주하지 않으므로 더 이상 수행할 작업이 없습니다.

문제 3. Expressway 검색 규칙 구성 오류

검색 규칙 잘못된 컨피그레이션은 Expressway에서 가장 큰 컨피그레이션 관련 문제 중 하나입니다. 인바운드 통화에 대한 검색 규칙이 필요하고 아웃바운드 통화에 대한 검색 규칙이 필요하기 때문에 검색 규칙 구성 문제는 양방향일 수 있습니다. 이 문제를 살펴보면 Expressway에서는 regex 문제가 매우 일반적이지만 검색 규칙 문제의 원인이 항상 아닌 것을 알 수 있습니다. 이 특정 세그먼트에서는 장애가 발생한 아웃바운드 통화를 살펴봅니다. 다른 모든 아웃바운드 포킹된 통화 시나리오와 마찬가지로, 증상은 그대로 유지됩니다.

- Called 사용자의 Cisco Webex 앱이 Join(참가) 단추를 표시했습니다.
- 전화기에서 벨소리를 재생하고 있었습니다.
- 전화한 사용자의 온-프레미스 전화가 울리고 있습니다.
- 전화를 건 사용자의 Cisco Webex 앱은 울리지 않음

다른 모든 시나리오와 마찬가지로 Expressway-C 및 E 진단 로그와 함께 CUCM SDL 추적을 활용하고자 합니다. 이전과 마찬가지로, 검색 히스토리 활용 및 진단 로그에서 통화를 식별하는 팁을 참조해야 합니다. 이전과 마찬가지로 Expressway-E 검색 기록을 사용하여 이 통화가 해당 통화를 거

치고 실패했음을 확인했습니다.아래는 Expressway-C에서 Expressway-E로 들어오는 초기 SIP INVITE를 살펴보는 분석의 시작입니다.

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

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

To:

```
Max-Forwards: 15
Record-Route: <sip:proxy-call-id=f79b8631-947b-46d4-a888-
911bf0150bfe@192.168.1.5:5061;transport=tls;lr>
Record-Route: <sip:proxy-call-id=f79b8631-947b-46d4-a888-
911bf0150bfe@192.168.1.5:5060;transport=tcp;lr>
Allow: INVITE,OPTIONS,INFO,BYE,CANCEL,ACK,PRACK,UPDATE,REFER,SUBSCRIBE,NOTIFY
User-Agent: Cisco-CUCM11.5
Expires: 180
Date: Mon, 25 Sep 2017 15:26:02 GMT
Supported: timer,resource-priority,replaces,X-cisco-srtp-fallback,X-cisco-original-called
Session-Expires: 1800
Min-SE: 1800
Allow-Events: presence
X-TAATag: 8e8c014d-5d01-4581-8108-5cb096778fc5
Session-ID: 75957d4fb66a13e835c10737aa505813;remote=00000000000000000000000000000000
Cisco-Guid: 3582928512-0000065536-000000240-0352430272
Content-Type: application/sdp
Content-Length: 714
```

<SDP Omitted>

SIP 헤더에서 Call-ID(d58f2680-9c91200a-1c7ba-1501a8c0)를 사용하여 이 대화 상자에 연결된 모든 메시지를 빠르게 검색할 수 있습니다.Expressway-E가 Expressway-C에 대해 로그에서 세 번째 적중 사항을 볼 때 Expressway-E가 즉시 404 Not Found(404 찾을 수 없음)를 전송합니다.

```
2017-09-25T11:26:13.286-04:00 amer-expressway01 tvcs: UTCTime="2017-09-25 15:26:13,286"
Module="network.sip" Level="DEBUG": Action="Sent" Local-ip="192.168.1.6" Local-port="7003" Dst-
ip="192.168.1.5" Dst-port="25675" Msg-Hash="12372154521012287279"
SIPMSG:
|SIP/2.0 404 Not Found
```

Via: SIP/2.0/TLS 192.168.1.5:5061;egress-zone=HybridCallServiceTraversal;branch=z9hG4bK1c7bf93ff08014ca5e00bb0b5f8b184b272412.a81f2992e3863ac202a000a3dd599763;proxy-call-id=f79b8631-947b-46d4-a888-911bf0150bfe;received=192.168.1.5;rport=25675;ingress-zone=HybridCallServiceTraversal
Via: SIP/2.0/TCP 192.168.1.21:5065;branch=z9hG4bK1c8c419938648;received=192.168.1.21;ingress-zone=CUCM11
Call-ID: d58f2680-9c91200a-1c7ba-1501a8c0@192.168.1.21
CSeq: 101 INVITE
From: "Jonathan Robb"

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

To:

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

이 데이터는 다음 두 가지를 알려줍니다.

1. Expressway-E는 Cisco Webex에 INVITE를 보내지 않았습니다.
2. Expressway-E는 404 Not Found(404 찾을 수 없음) 오류가 있는 통화를 거부하기 위한 로직 결정을 내린 책임자입니다.

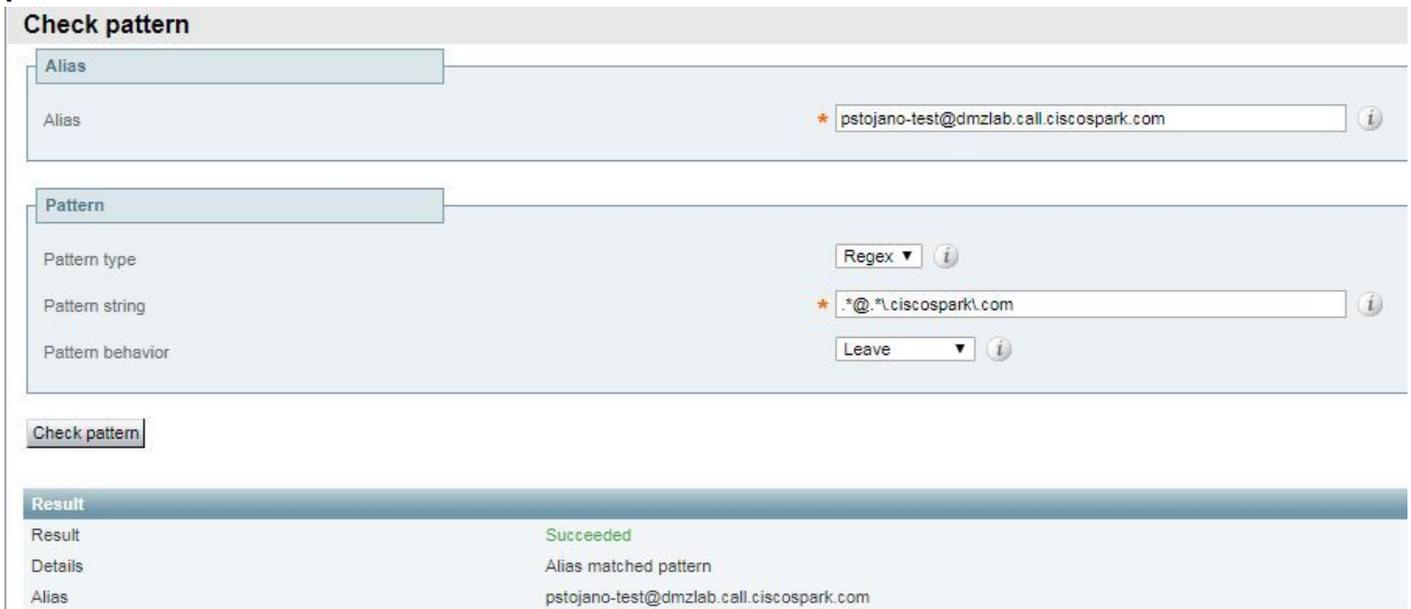
404 Not Found 오류는 일반적으로 Expressway에서 대상 주소를 찾을 수 없음을 의미합니다. Expressway는 검색 규칙을 사용하여 자신과 다른 환경 간에 통화를 라우팅하기 때문에 Expressway-E의 xConfiguration에 초점을 맞추어 시작합니다. 이 xConfiguration 내에서 Webex Hybrid DNS 영역으로 통화를 전달할 검색 규칙을 찾을 수 있습니다. xConfiguration(x컨피그레이션) 관점에서 Expressway에 구성된 검색 규칙을 찾으려면 "xConfiguration Zones Policy SearchRules Rule(xConfiguration 영역 정책 검색 규칙)"을 검색할 수 있습니다. 이렇게 하면 Expressway에 생성된 각 검색 규칙에 대한 검색 규칙 컨피그레이션 목록이 표시됩니다. "Rule" 뒤에 오는 숫자는 1로 먼저 생성된 검색 규칙에 따라 증가합니다. 검색 규칙을 찾는 데 문제가 있는 경우 "Webex"와 같이 일반적으로 사용되는 이름 지정 값을 사용하여 검색 규칙을 더 잘 찾을 수 있습니다. 규칙을 식별하는 또 다른 방법은 ".*@.*\ciscopark.com"으로 설정된 Pattern String 값을 찾는 것입니다. 구성할 패턴 문자열입니다. (패턴 문자열이 올바르게 구성된 것으로 가정)이 시나리오에서 xConfiguration을 검토한 후 Search Rule 6이 Cisco Webex에 통화를 전달하는 올바른 규칙임을 확인할 수 있습니다.

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

이 패턴을 테스트하기 위해 에 설명된 Check 패턴 기능을 사용할 수 있습니다. 여기서 중요한 사항은 다음 값을 구성하라는 것입니다. 유지 관리 > 도구 > 패턴 확인

- 별칭: 초기 INVITE%에서 %URI 요청(예: pstojano-test@dmzlab.call.ciscopark.com)
- 패턴 유형: 레게스
- 패턴 문자열: .*@.*\..ciscopark\..com
- 패턴 동작: 나가기

규칙에 대한 Regex가 올바르게 설정된 경우 이 Check 패턴 Succeeded의 결과를 확인해야 합니다. 다음은 이미지에 표시된 것처럼 이를 보여 주는 그림입니다



검색 규칙이 있고 올바르게 구성되었는지 확인할 수 있으므로 Expressway가 수행 중인 검색 논리를 자세히 확인하여 404 Not Found를 보내는 Expressway-E에 영향을 미치는지 확인할 수 있습니다. 다음은 Expressway가 수행하는 검색 규칙 로직의 샘플입니다.

```

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.ciscopark.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.ciscopark.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.ciscopark.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.ciscopark.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.ciscopark.com" Type="SRV (IPv4 and IPv6)"

```

이 샘플에서는 Expressway가 4개의 검색 규칙을 처리한 것을 확인할 수 있습니다. 첫 3회는 여러 이유로 고려되지 않았지만 4일은 고려됐다. 흥미로운 데이터는 Expressway가 DNS 조회 로직으로 직진되는 즉시 발생합니다. xConfiguration에서 확인한 내용을 기억하면 Webex Hybrid에 대해 구성된 검색 규칙의 이름이 Webex Hybrid - Webex Cloud로 지정되었으며 위의 이 검색 규칙 로직에서도 고려되지 않았습니다. 여기서 Webex Hybrid Search 규칙의 사용에 영향을 미치는지 더 잘 이해할 수 있도록 DNS에 대해 고려된 검색 규칙이 어떻게 구현되었는지 살펴볼 필요가 있습니다. 이를 위

해 이번에는 "to DNS"라는 검색 규칙을 찾아 xConfig를 다시 살펴볼 수 있습니다.

```
*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"
```

이 검색 규칙을 검토한 후 다음을 완료할 수 있습니다.

- 패턴 문자열은 Cisco Webex 요청 URI와 일치합니다.
- 우선 순위는 100으로 설정됩니다.
- Progress(Pattern behavior)가 Stop(중지)으로 설정됩니다.

이 정보에 따르면, 호출되는 Cisco Webex Request URI가 이 규칙과 일치하며, 규칙이 일치하면 Expressway에서 다른 검색 규칙을 검색(고려 중)하지 않습니다. 이러한 이해를 통해 Rule Priority가 핵심 요소가 됩니다. Expressway 검색 규칙 우선 순위가 가장 낮은 우선 순위 규칙이 먼저 시도됩니다. 다음은 예입니다. 검색 규칙: 로컬패턴 동작: 계속우선 순위 1 검색 규칙: 네이퍼패턴 동작: 계속우선 순위 10 검색 규칙: DNS패턴 동작: 중지우선 순위 50이 예에서 Local(1)이라는 검색 규칙을 먼저 시도하며 일치하는 항목이 발견되면 Pattern(패턴) 동작이 Continue(계속)로 설정되어 있으므로 Search rule Neighbor(1)로 이동합니다. 검색 규칙 Neighbor가 일치하지 않으면 Search Rule DNS(50)로 계속 이동하여 마지막으로 고려합니다. Search Rule DNS가 일치하면 Pattern(패턴) 동작이 Stop(중지)으로 설정되었으므로 우선 순위가 50보다 높은 다른 검색 규칙이 있는지 여부에 관계없이 검색이 중지됩니다. 이러한 이해를 통해 "DNS"와 "Webex Hybrid - to Webex Cloud(Webex Cloud)" 규칙 사이의 검색 규칙 우선 순위를 살펴볼 수 있습니다.

```
*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"
```

여기서 "DNS로" 규칙의 우선 순위가 "Webex Hybrid - to Webex Cloud" 규칙보다 낮으므로 "DNS로" 규칙이 먼저 시도됩니다. 패턴 동작(진행)이 중지(Stop)로 설정된 경우 Expressway-E는 Webex Hybrid - Webex Cloud 규칙을 고려하지 않으며 통화가 궁극적으로 실패합니다. 솔루션 이러한 유형의 문제는 Hybrid Call Service Connect에서 점점 더 흔해지고 있습니다. 솔루션이 구축된 경우, 사람들은 Cisco Webex 검색에 사용할 우선 순위가 높은 규칙을 자주 생성합니다. 우선 순위가 낮은 기존 규칙이 일치하고 있어 생성된 이 규칙이 호출되지 않는 경우가 많으며, 이로 인해 오류가 발생합니다. 이 문제는 Cisco Webex에 대한 인바운드 및 아웃바운드 통화 모두에서 발생합니다. 이 문제를 해결하려면 다음 단계를 수행해야 합니다.

1. Expressway-E에 로그인
2. Configuration(구성) > Dial Plan(다이얼 플랜) > Search rules(검색 규칙)로 이동합니다.
3. Webex Hybrid Search 규칙을 찾아 클릭합니다.(예: 이름: Webex Hybrid - Webex Cloud)
4. 우선 순위 값을 다른 검색 규칙보다 낮은 값으로 설정하고 다른 사용자에게 영향을 주지 않도록 충분히 높입니다.(예: 우선 순위: 99)

Search 규칙이 있는 thumb의 일반적인 규칙은 Pattern 문자열보다 구체적이며 Search rule priority(검색 규칙 우선 순위) 목록에 배치할 수 있습니다. 일반적으로 DNS 영역은 로컬 도메인이 아닌 모든 항목을 catch하여 인터넷으로 보내는 Pattern 문자열로 구성됩니다. 이 때문에 해당 유형의 검색 규칙이 마지막으로 호출되도록 우선 순위를 높게 설정하는 것이 좋습니다. 문제 4.

Expressway CPL 컨피그레이션 오류 Expressway 솔루션은 서버에서 사용 가능한 CPL(Call Processing Language) 논리를 사용하여 요금 사기 완화를 허용합니다. 구축 중인 Expressway 솔루션이 Cisco Webex Hybrid Call Service 및 Mobile & Remote Access에만 사용되는 경우 CPL 정책 및 규칙을 활성화하고 구현하는 것이 좋습니다. Cisco Webex Hybrid용 Expressway의 CPL 구성은 매우 간단하지만, 잘못 구성하면 통화 시도를 쉽게 차단할 수 있습니다. 아래 시나리오에서는 진단 로깅을 사용하여 CPL 컨피그레이션 오류를 식별하는 방법을 보여줍니다. 다른 모든 발신 포킹된 통화 시나리오와 마찬가지로, 증상은 동일하게 유지되었습니다.

- 호출된 사용자의 Cisco Webex 앱에서 Join(참가) 버튼을 제공했습니다.
- 전화기에서 벨이 울리고 있었다
- 전화한 사용자의 은-프리미스 전화가 울리고 있습니다.
- 호출한 사용자의 앱은 울리지 않음

다른 모든 시나리오와 마찬가지로 Expressway-C 및 E 진단 로그와 함께 CUCM SDL 추적을 사용할 수 있습니다. 이전과 마찬가지로 을 참조하십시오. 이전과 마찬가지로 Expressway-E 검색 기록을 사용하여 이 통화가 도착하고 실패했음을 확인했습니다. 다음은 Expressway-C에서 Expressway-E로 들어오는 초기 SIP INVITE를 볼 수 있는 분석의 시작입니다.

```
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=z9hG4bK781a130d234ed9aaec86834368739430283256.34216c32a0d
e36e16590bae36df388b6;proxy-call-id=3bbbf94a-082e-4088-8f5a-5ea7e82f8aac;rport
Via: SIP/2.0/TCP 192.168.1.21:5065;branch=z9hG4bK1cf344a8b117e;received=192.168.1.21;ingress-
zone=CUCM11
Call-ID: c030f100-9c916d13-1cdcb-1501a8c0@192.168.1.21
CSeq: 101 INVITE
Call-Info: <urn:x-cisco-remotecall:callinfo>;x-cisco-video-traffic-class=DESKTOP
Remote-Party-ID: "Jonathan Robb"
<sip:5010@rtp.ciscotac.net>;party=calling;screen=yes;privacy=off
Contact: <sip:5010@192.168.1.21:5065;transport=tcp>;video;audio
From: "Jonathan Robb"
```

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

To:

```
Max-Forwards: 15
Record-Route: <sip:proxy-call-id=3bbbf94a-082e-4088-8f5a-
5ea7e82f8aac@192.168.1.5:5061;transport=tls;lr>
Record-Route: <sip:proxy-call-id=3bbbf94a-082e-4088-8f5a-
5ea7e82f8aac@192.168.1.5:5060;transport=tcp;lr>
Allow: INVITE,OPTIONS,INFO,BYE,CANCEL,ACK,PRACK,UPDATE,REFER,SUBSCRIBE,NOTIFY
User-Agent: Cisco-CUCM11.5
Expires: 180
Date: Mon, 25 Sep 2017 20:54:43 GMT
Supported: timer,resource-priority,replaces,X-cisco-srtp-fallback,X-cisco-original-called
Session-Expires: 1800
Min-SE: 1800
```

Allow-Events: presence
X-TAATag: 4ffffefed-0512-4067-ac8c-35828f0a1150
Session-ID: 75957d4fb66a13e835c10737aa512577;remote=00000000000000000000000000000000
Cisco-Guid: 3224432896-0000065536-0000000264-0352430272
Content-Type: application/sdp
Content-Length: 714

<SDP Omitted>

SIP 헤더에서 Call-ID(c030f100-9c916d13-1cdcb-1501a8c0)를 사용하여 이 대화 상자에 연결된 모든 메시지를 빠르게 검색합니다. Expressway-E가 Expressway-C에 대해 로그에 세 번째 히트를 표시하는 경우 Expressway-E가 즉시 Expressway-C에 403 Forbidden을 전송한다는 것을 확인할 수 있습니다.

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

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

To:

;tag=64fe7f9eab37029d

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

Expressway-E가 이 통화를 거부하고 Expressway-C에 403 금지된 오류를 보낸 이유를 이해하려면 Expressway-C에 입력된 원래 SIP INVITE와 403 금지됨 사이의 로그 항목을 분석하려고 합니다. 이러한 로그 항목을 분석하면 일반적으로 실행 중인 모든 논리 결정을 볼 수 있습니다. 호출되는 검색 규칙은 표시되지 않지만 호출되는 CPL(Call Process Language) 로직도 볼 수 있습니다. 아래는 그러한 것의 일부입니다.

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:

위의 로그 분석을 기반으로 합니다.CPL이 통화를 거부하도록 결정할 수 있습니다.

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="4ffffefed-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"

참고:이 경우 CPL, FindMe 및 Transforms가 모두 검색 규칙 이전에 처리되므로 검색 규칙이 호출되는 것을 볼 수 없습니다.대부분의 경우 Expressway의 xConfig를 활용하여 상황을 더 잘 이해할 수 있습니다.그러나 CPL의 경우 정책이 활성화된 경우에만 정의된 규칙을 볼 수 없습니다.다음은 이 Expressway-E가 로컬 CPL 논리를 사용한다는 것을 보여주는 xConfig 부분입니다.

*c xConfiguration Policy AdministratorPolicy Mode: "LocalCPL"

규칙 컨피그레이션을 더 잘 이해하려면 Expressway-E에 로그인하고 이미지에 표시된 대로 Configuration > Call Policy > Rules로 이동해야 합니다

Source	Destination	Action	Rearrange
	@dmzlab.call.ciscospark.com	Reject	

이 컨피그레이션을 검토할 때 다음이 구성된 것을 확인할 수 있습니다.출처: *대상: .*@dmzlab.call.ciscospark.com.*작업:거부 [Cisco Webex Hybrid Call Service](#) 구축 [가이드](#)에 설명된 것과 비교할 때 소스 및 대상이 뒤로 구성된 것을 확인할 수 있습니다

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

솔루션이 문제를 해결하려면 소스가 .*@%Webex_subdomain%.call.ciscospark.com.*(으)로 설정되고 대상 패턴이 *

1. Expressway-E에 로그인
2. Configuration(컨피그레이션) > Call Policy(통화 정책) > Rules(규칙)로 이동합니다.
3. Cisco Webex Hybrid Call 서비스에 대해 설정된 규칙을 선택합니다.
4. 소스 패턴을 .*@%Webex_subdomain%.call.ciscospark.com.*(예: .*@dmzlab.call.ciscospark.com.*)
5. Destination Pattern(대상 패턴)을 다음으로 입력합니다.*
6. 저장 선택

Webex Hybrid용 CPL 구현에 대한 자세한 내용은 [Cisco Webex Hybrid Design Guide](#)를 참조하십시오.

오. 양방향: Cisco Webex에서 온프레미스 또는 온프레미스에서 Cisco Webex로 문제점 1. IP Phone/Collaboration Endpoint는 G.711, G.722 또는 AAC-LD 이외의 오디오 코덱을 제공합니다. Hybrid Call Service Connect는 다음과 같은 세 가지 오디오 코덱을 지원합니다. G.711, G.722 및 AAC-LD. Cisco Webex 환경에서 성공적으로 통화를 설정하려면 이러한 오디오 코덱을 사용해야 합니다. 온프레미스 환경은 다양한 유형의 오디오 코덱을 사용하도록 설정할 수 있지만 동시에 이를 제한하도록 설정할 수 있습니다. 이는 Unified CM에서 사용자 지정 및/또는 기본 영역 설정을 사용하여 의도적 또는 의도하지 않게 발생할 수 있습니다. 이러한 특정 동작의 경우 통화 방향과 Unified CM이 Early 또는 Delayed Offer를 사용하도록 구성된 경우 로깅 패턴이 다를 수 있습니다. 다음은 이 동작이 자체적으로 나타날 수 있는 몇 가지 상황에 대한 예입니다.

1. Cisco Webex는 G.711, G.722 또는 AAC-LD를 제공하는 인바운드 INVITE를 SDP와 함께 보냅니다. Expressway-C는 이 메시지를 Unified CM으로 전송하지만 Unified CM은 이 통화에 대해 G.729만 허용하도록 구성되어 있습니다. 따라서 Unified CM은 사용 가능한 코덱이 없기 때문에 통화를 거부합니다.
2. Unified CM은 아웃바운드 통화를 Cisco Webex에 대한 Early Offer로 시도합니다. 즉, Expressway-C로 전송된 초기 INVITE에는 G.729 오디오를 지원하는 SDP만 포함됩니다. 그런 다음 Cisco Webex는 G.729를 지원하지 않으므로 오디오를 제로로 내보내는 SDP를 사용하여 200OK를 보냅니다(*m=audio 0 RTP/SAVP*). Expressway-C가 이 INVITE를 Unified CM에 전달하면 사용할 수 없는 코덱이 있기 때문에 Unified CM이 통화를 종료합니다.
3. Unified CM은 아웃바운드 통화를 Expressway-C로 보낸 초기 INVITE에 SDP가 포함되지 않음을 Cisco Webex에 대한 지연된 제안으로 시도합니다. 그런 다음 Cisco Webex가 지원하는 모든 오디오 코덱이 포함된 SDP가 포함된 200OK를 전송합니다. Expressway-C는 이 200 확인을 Unified CM으로 전송하지만 Unified CM은 이 통화에 대해 G.729만 허용하도록 구성되어 있습니다. 따라서 Unified CM은 사용 가능한 코덱이 없기 때문에 통화를 거부합니다.

이 문제와 일치하는 Hybrid Call Service Connect 통화 오류를 식별하려는 경우 Unified CM SDL 추적 외에 Expressway 로그를 가져와야 합니다. Unified CM이 아웃바운드 통화를 *Early Offer*로 시도하는 경우 일치 상황 #2 아래에 있는 로그 코드 조각이 있습니다. 통화가 Cisco Webex로 연결된다는 사실을 알고 있으므로 로그 분석이 Expressway-E에서 시작됩니다. 다음은 Cisco Webex에 대한 초기 INVITE의 일부입니다. 기본 오디오 코덱이 G.729(페이로드 18)로 설정되어 있음을 확인할 수 있습니다. 101은 DTMF용이며 이 특정 시나리오는 관련이 없습니다.

```
2017-09-19T10:46:10.488-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 14:46:10,488"
Module="network.sip" Level="DEBUG": Action="Sent" Local-ip="172.16.2.2" Local-port="25034" Dst-
ip="146.20.193.64" Dst-port="5062" Msg-Hash="4309505007645007056"
SIPMSG:
INVITE sip:pstojano-test@dmzlab.call.ciscospark.com SIP/2.0
Via: SIP/2.0/TLS 64.102.241.236:5062;egress-
zone=HybridCallServicesDNS;branch=z9hG4bK323e6b15ad0cbbf409751f67848136fa1115;proxy-call-
id=a3a78ee2-c01b-4741-b29b-55aede256d2;rport
Via: SIP/2.0/TLS 172.16.2.2:5073;branch=z9hG4bK350703fe46645f0acddef05b35adc5c157;x-cisco-local-
service=nettle;received=172.16.2.2;rport=41511;ingress-zone=DefaultZone
Via: SIP/2.0/TLS 192.168.1.6:5061;egress-
zone=DefaultZone;branch=z9hG4bKf71f2bf47233d6ca52b579364594ac6c1114.a402e3f25603f5a77b60b17ea47d
bf72;proxy-call-id=be17a470-0bca-4ad5-8a6c-14872e007efb;received=192.168.1.6;rport=25025
Via: SIP/2.0/TLS 192.168.1.5:5061;egress-
zone=HybridCallServiceTraversal;branch=z9hG4bKf4cf4d09d213a88bd2331cef0bc82b540559.494a140082bd
66357134b9eed4335df8;proxy-call-id=d4d4e950-babc-45d5-a4a7-
c60a8b17a8bd;received=192.168.1.5;rport=26513;ingress-zone=HybridCallServiceTraversal
Via: SIP/2.0/TCP 192.168.1.21:5065;branch=z9hG4bK12dd82194c4f7;received=192.168.1.21;ingress-
zone=CUCM11
Call-ID: 44bdd400-9c112db1-12d95-1501a8c0@192.168.1.21
CSeq: 101 INVITE
Remote-Party-ID: "Jonathan Robb" <sip:5010@rtp.ciscotac.net>;privacy=off;screen=no;party=calling
Contact: <sip:172.16.2.2:5073;transport=tls>;video;audio
From: "Jonathan Robb"
```

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

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

이 초기 INVITE에 대한 응답으로 Cisco Webex는 200 OK 메시지로 응답합니다. 이 메시지를 자세히 살펴보면 오디오 코덱이 0으로 분리되어 있음을 확인할 수 있습니다. 이는 문제가 됩니다. 오디오 포트가 할당되지 않으면 통화가 해당 스트림을 협상할 수 없기 때문입니다.

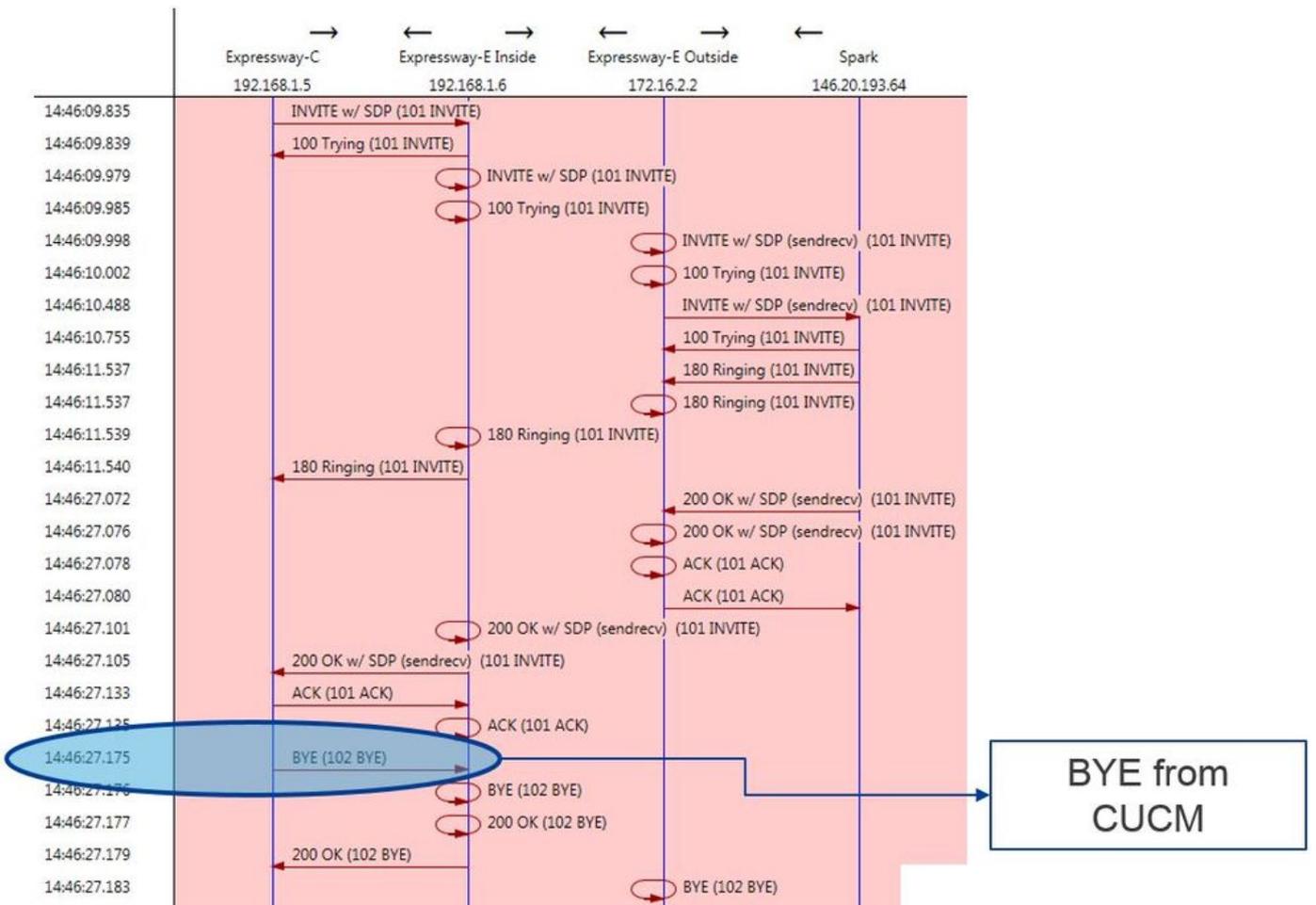
2017-09-19T10:46:27.073-04:00 amer-expressway01 tvcs: UTCTime="2017-09-19 14:46:27,072"
Module="network.sip" Level="DEBUG": Action="Received" Local-ip="172.16.2.2" Local-port="25034"
Src-ip="146.20.193.64" Src-port="5062" Msg-Hash="5236578200712291002"
SIPMSG:
SIP/2.0 200 OK

Via: SIP/2.0/TLS 64.102.241.236:5062;egress-
zone=HybridCallServicesDNS;branch=z9hG4bK323e6b15ad0cbbf409751f67848136fa1115;proxy-call-
id=a3a78ee2-c01b-4741-b29b-55aede256d2;rport=38245;received=192.168.5.26,SIP/2.0/TLS
172.16.2.2:5073;branch=z9hG4bK350703fe46645f0acdddef05b35adc5c157;x-cisco-local-
service=nettle;received=172.16.2.2;rport=41511;ingress-zone=DefaultZone,SIP/2.0/TLS
192.168.1.6:5061;egress-
zone=DefaultZone;branch=z9hG4bKf71f2bf47233d6ca52b579364594ac6c1114.a402e3f25603f5a77b60b17ea47d
bf72;proxy-call-id=be17a470-0bca-4ad5-8a6c-
14872e007efb;received=192.168.1.6;rport=25025,SIP/2.0/TLS 192.168.1.5:5061;egress-
zone=HybridCallServiceTraversal;branch=z9hG4bKf4cf4d09d213a88bd2331cef0bc82b540559.494a140082bd
66357134b9eed4335df8;proxy-call-id=d4d4e950-babc-45d5-a4a7-
c60a8b17a8bd;received=192.168.1.5;rport=26513;ingress-
zone=HybridCallServiceTraversal,SIP/2.0/TCP
192.168.1.21:5065;branch=z9hG4bK12dd82194c4f7;received=192.168.1.21;ingress-zone=CUCM11
Call-ID: 44bdd400-9c112db1-12d95-1501a8c0@192.168.1.21
CSeq: 101 INVITE
Contact: "l2sip-UA" <sip:l2sip-UA@l2sip-cfa-01.wbx2.com:5062;transport=tls>
From: "Jonathan Robb"

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

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

이제 TranslatorX를 사용하여 대화 상자의 나머지 부분을 검토할 수 있습니다.대화 상자 자체가
ACK로 완료되었음을 확인할 수 있습니다.이 문제는 대화 상자가 완료되면 즉시 이미지에 표시된
대로 Expressway-C 방향에서 BYE가 발생합니다



다음은 BYE 메시지의 자세한 샘플입니다. User-Agent가 Cisco-CUCM11.5임을 명확히 알 수 있습니다. 즉, Unified CM에서 메시지가 생성되었음을 의미합니다. 또 다른 지적해야 할 것은 이유 코드가 cause=47로 설정되어 있다는 것입니다. 이 경우 일반적으로 사용할 수 있는 리소스가 없습니다.

```

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-
79e26f48eabc-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

```

Cisco Webex 구성 요소가 이 통화 샘플에 대한 오디오 코덱을 0으로 분리했으므로 다음 사항에 중점을 두어야 합니다. a. Cisco Webex로 전송된 초기 INVITE 및 b. Cisco Webex가 해당 포트를 제로 아웃하는 데 사용한 논리는 무엇입니까? 이제 초기 INVITE의 고유한 특성을 살펴보면 G.729만 포함되어 있습니다. 이를 알고 있는 경우 Cisco Webex Hybrid Call Service 구축 가이드를 검토하고

Prepare Your Environment 장을 검토합니다. 여기서 Completes [The Preferences for Hybrid Call Service Connect](#) 섹션의 5단계에서 지원되는 특정 코덱을 호출합니다. 여기에서 다음과 같은 내용을 확인할 수 있습니다. Cisco Webex는 다음 코덱을 지원합니다.

- 오디오 - G.711, G.722, AAC-LD
- 비디오 - H.264

참고: Opus는 Cisco Webex Hybrid Call에 대한 통화의 온프레미스 레그에서 사용되지 않습니다. 이 정보를 통해 Unified CM이 지원되지 않는 오디오 코덱을 전송하고 있다는 결론을 내릴 수 있습니다. 이 때문에 Cisco Webex가 포트를 비웁니다. 해결책: 이러한 특정 상황을 해결하려면 온프레미스에 통화를 고정하는 Cisco Webex RD와 Expressway-C에 대한 SIP 트렁크 간의 지역 컨피그레이션을 검토해야 할 수 있습니다. 이렇게 하려면 해당 두 요소가 있는 디바이스 풀을 결정합니다. 디바이스 풀은 영역에 대한 매핑을 포함합니다. Expressway-C SIP 트렁크의 디바이스 풀을 확인하려면

1. Unified CM에 로그인합니다.
2. Device(디바이스) > Trunk(트렁크)로 이동합니다.
3. 트렁크 이름을 검색하거나 찾기를 클릭합니다.
4. Expressway-C 트렁크를 선택합니다.
5. 디바이스 풀의 이름을 기록합니다.

통화를 라우팅한 CTI-RD 또는 Cisco Webex-RD의 디바이스 풀을 확인하려면 다음을 수행합니다.

1. Device(디바이스) > Phone(전화기)으로 이동합니다.
2. 검색할 때 Device Type contains Webex 또는 CTI Remote Device(Webex 또는 CTI 원격 디바이스 포함)를 선택할 수 있습니다(고객의 사용 방식에 따라 다름).
3. 디바이스 풀의 이름을 기록합니다.

각 디바이스 풀에 연결된 지역을 확인합니다.

1. System(시스템) > Device Pool(디바이스 풀)으로 이동합니다.
2. Expressway-C SIP 트렁크에 사용되는 디바이스 풀을 검색합니다.
3. Device Pool(디바이스 풀)을 클릭합니다.
4. 지역 이름을 기록합니다.
5. Webex-RD 또는 CTI-RD에 사용되는 장치 풀을 검색합니다.
6. Device Pool(디바이스 풀)을 클릭합니다.
7. 지역 이름을 기록합니다.

지역 관계 결정:

1. 시스템 > 영역 정보 > 영역으로 이동합니다.
2. 식별된 지역 중 하나를 검색합니다.
3. G.729를 사용하는 두 지역 간에 지역 관계가 있는지 확인합니다.

이 시점에서 G.729를 사용 중인 관계를 식별한 경우 Cisco Webex가 이 기능을 지원하는 리전이 있는 다른 장치 풀을 사용하거나 사용하는 지원되는 오디오 코덱을 지원하도록 관계를 조정해야 합니다. 위에 설명된 시나리오에서 다음을 확인했습니다. Expressway-C 트렁크 영역: 예약대역폭 Webex-RD 지역: RTP-디바이스 이 그림은 RTP-Devices와 ReservingBandwidth 영역 간의 관계를 그림으로 나타낸 것입니다

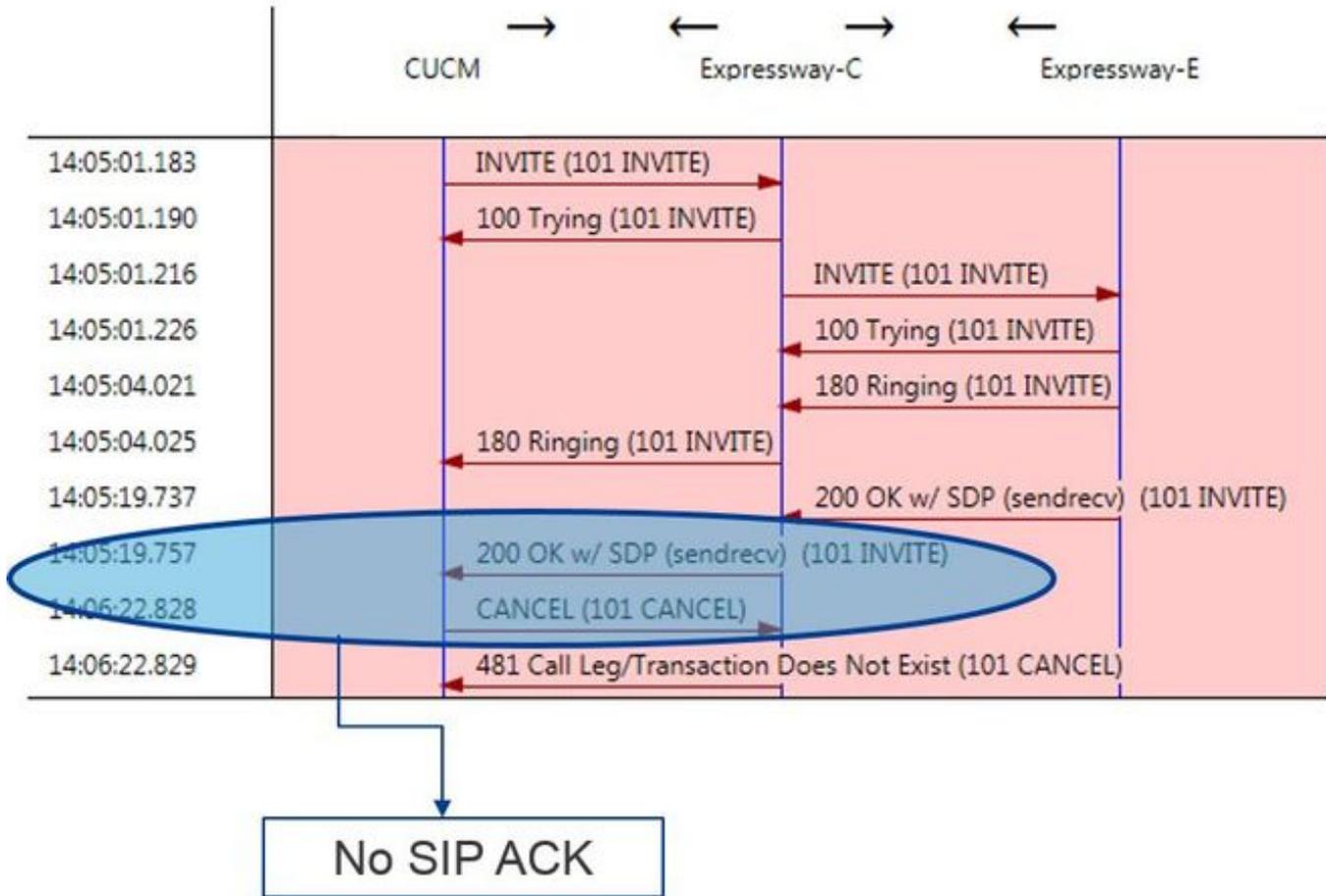
Region	Audio Codec Preference List	Maximum Audio Bit Rate	Maximum Session Bit Rate for Video Calls	Maximum Session Bit Rate for Immersive Video Calls
Default	Use System Default (Factory Default low loss)	256 kbps (L16, AAC-LD)	32000 kbps	32000 kbps
ReservingBandwidth	Use System Default (Factory Default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

Expressway-C 트렁크가 있던 디바이스 풀을 변경하면 지역 관계가 변경됩니다. 새 디바이스 풀에는 RTP-Infrastructure로 설정된 Region이 있으므로 Cisco Webex-RD와 Expressway-C 트렁크 간의 새로운 지역 관계는 RTP-Devices와 RTP-Infrastructure였습니다. 그림과 같이 이 관계는 Cisco

Webex에서 지원되는 오디오 코덱인 AAC-LD를 지원하므로 통화가 올바르게 설정된다는 것을 확인할 수 있습니다. 문제 2. Unified CM 최대 수신 메시지 크기 초과기업 내에서 비디오가 더욱 보편화됨에 따라 SDP가 포함된 SIP 메시지의 크기가 상당히 증가했습니다. 이러한 메시지를 처리하는 서버는 큰 패킷을 수용할 수 있도록 구성해야 합니다. 많은 통화 제어 서버에서 기본값은 괜찮습니다. Cisco Unified CM(Unified Communications Manager)에서는 이전 릴리스에서 SDP를 포함하는 큰 SIP 메시지를 처리하는 기본값이 사용되지 않았습니다. Unified CM의 이후 릴리스에서는 SIP 메시지에 허용되는 값 크기가 증가했지만 이 값은 업그레이드가 아니라 새 설치에만 설정됩니다. 이와 함께 Unified CM의 이전 릴리스를 Hybrid Call Service Connect를 지원하도록 업그레이드하는 고객은 Unified CM의 Max Incoming Message Size(최대 수신 메시지 크기)가 너무 낮을 수 있습니다. 이 문제와 일치하는 Hybrid Call Service Connect 통화 오류를 식별하려는 경우 Unified CM SDL 추적 외에 Expressway 로그를 가져와야 합니다. 장애를 식별하려면 먼저 어떤 일이 발생하는지 파악하고 장애가 발생할 수 있는 시나리오의 유형을 파악합니다. Unified CM이 너무 큰 SIP 메시지를 수신하면 TCP 소켓을 닫고 Expressway-C에 응답하지 않는다는 사실을 알아야 합니다. 이와 함께 다음과 같은 다양한 상황과 방법이 발생할 수 있습니다.

1. Cisco Webex는 너무 큰 SDP가 포함된 인바운드 INVITE를 보냅니다. Expressway-C는 이를 Unified CM으로 전달하고 Unified CM은 TCP 소켓을 닫고 SIP 대화 상자가 시간 초과됩니다.
2. Unified CM은 Webex에 대한 초기 오퍼(Early Offer to Webex)로 아웃바운드 통화를 시도합니다. 즉, Expressway-C로 전송된 초기 INVITE에 SDP가 포함됩니다. 그런 다음 Cisco Webex는 SDP가 포함된 200OK를 응답하고 Expressway-C에서 Unified CM으로 전달되는 200OK 응답이 너무 큼니다. Unified CM이 TCP 소켓을 닫으면 SIP 대화 상자가 시간 초과됩니다.
3. Unified CM은 발신 통화를 Webex에 대한 지연된 오퍼(Delayed Offer to Webex)로 시도합니다. 즉, Expressway-C로 전송된 초기 INVITE에 SDP가 포함되지 않습니다. 그런 다음 Cisco Webex는 Expressway-C에서 Unified CM으로 전달되는 200OK를 SDP와 함께 전송하고 200OK 오퍼가 너무 큼니다. Unified CM이 TCP 소켓을 닫으면 SIP 대화 상자가 시간 초과됩니다.

Expressway-C 로그를 통해 이 특정 조건을 확인하면 메시지 흐름을 이해할 수 있습니다. TranslatorX와 같은 프로그램을 사용할 경우 Expressway-C가 Cisco Webex 200 OK(SDP 포함)를 Unified CM으로 통과하고 있음을 알 수 있습니다. 문제는 Unified CM이 이미지에 표시된 대로 SIP ACK로 응답하지 않는다는 것입니다



Unified CM은 응답하지 않는 책임자이므로 SDL 추적을 검토하여 Unified CM이 이 조건을 어떻게 처리하는지 확인할 필요가 있습니다. 이 시나리오에서는 Unified CM이 Expressway-C의 큰 메시지를 무시한다는 것을 알 수 있습니다. 이와 같은 로그 라인 항목이 인쇄됩니다.

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.

```

SIP 대화 상자가 시간 초과되면 Cisco Webex는 로그 샘플에 표시된 대로 Expressway-E에 인바운드 SIP 603 거부 메시지를 보냅니다.

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

```

앞서 언급한 대로, 이 동작을 볼 수 있는 세 가지 시나리오가 있습니다. 명확성을 위해 이 그림에 제공된 로그 샘플은 통화가 Cisco Webex로 Delayed 오퍼로 아웃바운드된 상황 3과 일치합니다. 해결책:

1. Unified CM에 로그인합니다.
2. System(시스템) > Service Parameters(서비스 매개변수)로 이동합니다.
3. Call Manager 서비스를 실행 중인 서버를 선택합니다.
4. 서비스 선택을 묻는 메시지가 나타나면 Cisco Call Manager 서비스를 선택합니다.

5. 고급 옵션을 선택합니다.
6. Clusterwide Parameters (Device - SIP)(클러스터 수준 매개변수(디바이스 - SIP) 설정 아래에서 SIP Max Incoming Message Size(SIP 최대 수신 메시지 크기)를 18000으로 변경합니다.
7. 저장을 선택합니다.
8. Cisco Call Manager 서비스를 실행 중인 모든 Unified CM 노드에 대해 이 프로세스를 반복합니다.

참고: IP Phone, Collaboration 엔드포인트 및/또는 SIP Trunk에서 이 설정을 사용하려면 다시 시작해야 합니다. 이러한 장치는 환경에 미치는 영향을 최소화하기 위해 개별적으로 다시 시작할 수 있습니다. CUCM에서 모든 장치를 재설정하지 마십시오. CUCM에서 모든 장치를 재설정하는 것이 절대적으로 허용될 수 있음을 모르는 경우 재설정하지 마십시오. **부록 Expressway 문제 해결 도구패턴 확인 유틸리티** Expressway에는 패턴이 특정 별칭과 일치하는지 테스트하고 예상대로 변형되는지 여부를 테스트할 때 유용한 패턴 검사 유틸리티가 있습니다. 이 유틸리티는 Expressway에서 Maintenance(유지 관리) > Tools(도구) > Check pattern(패턴 확인) 메뉴 옵션의 아래에 있습니다. 가장 일반적으로, 검색 규칙 regex가 패턴 문자열에 대한 별칭과 제대로 일치하는지 테스트한 다음 선택적으로 문자열을 성공적으로 조작할 수 있도록 하려는 경우에 사용됩니다. 하이브리드 통화 서비스 연결의 경우 Unified CM 클러스터 FQDN이 Unified CM 클러스터 FQDN에 대해 설정한 패턴 문자열과 일치하는지 테스트할 수도 있습니다. 이 유틸리티를 사용할 때 통화가 대상 URI가 아니라 경로 헤더에 나열된 Unified CM 클러스터 FQDN 매개변수를 기반으로 라우팅된다는 점에 유의하십시오. 예를 들어 다음 초대가 Expressway에 들어온 경우 jorobb@rtp.ciscotac.net이 아닌 cucm.rtp.ciscotac.net에 대해 Check 패턴 기능을 테스트합니다.

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

확인 패턴을 사용하여 하이브리드 통화 서비스 연결 경로 헤더 검색 규칙 라우팅을 테스트하려면 다음 단계를 수행합니다.

1. Maintenance(유지 관리) > Tools(도구) > Check pattern(패턴 확인)으로 이동합니다.
2. 별칭에 Unified CM 클러스터 FQDN을 입력합니다.
3. Pattern Type(패턴 유형)을 Prefix(접두사)로 설정합니다.
4. 패턴 문자열을 Unified CM 클러스터 FQDN으로 설정합니다.
5. Pattern(패턴) 동작을 Leave(나가기)로 설정합니다.
6. 패턴 확인을 선택합니다.

Expressway의 검색 규칙이 올바르게 구성된 경우 Results return a Succeeded 메시지를 볼 수 있습니다. 다음은 이미지에 표시된 대로 성공적인 검사 패턴 테스트의 예입니다

Check pattern

Alias

Alias

Pattern

Pattern type Prefix

Pattern string

Pattern behavior Leave

Result

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

이 별칭이 성공한 이유는 이 별칭(cucm.rtp.ciscotac.net)이 접두사 패턴 문자열 (cucm.rtp.ciscotac.net)과 일치하기 때문입니다. 이러한 결과에 따라 통화가 라우팅되는 방법을 이해하려면 설명된 Expressway Locate 유틸리티를 사용할 수 있습니다. 유틸리티 찾기 Expressway의 Locate 유틸리티는 지정된 별칭을 기반으로 Expressway가 특정 영역으로 통화를 라우팅할 수 있는지 여부를 테스트하려는 경우에 유용합니다. 이 모든 작업은 실제 전화를 걸지 않고도 완료할 수 있습니다. Locate 유틸리티는 Expressway의 Maintenance(유지 관리) > Tools(툴) > Locate(찾기) 메뉴 아래에서 찾을 수 있습니다. Expressway-C에서 Locate(찾기) 기능을 사용하여 서버가 SIP Route 헤더에 있는 Unified CM Cluster FQDN을 기반으로 통화를 라우팅할 수 있는지 확인하는 방법에 대한 몇 가지 지침을 확인할 수 있습니다.

1. Maintenance(유지 관리) > Tools(툴) > Locate(찾기)로 이동합니다.
2. Alias(별칭) 필드에 Unified CM Cluster FQDN을 입력합니다.
3. SIP를 Protocol로 선택합니다.
4. 소스에 대한 Cisco Webex Hybrid Traversal 클라이언트 영역을 선택합니다.
5. Locate(찾기)를 선택합니다.

인터페이스의 맨 아래에 검색 결과가 표시됩니다. 다음은 이미지에 표시된 것과 같이 일치하는 결과를 사용하여 실행된 샘플 테스트의 예입니다

Locate

Locate

Alias

Hop count

Protocol SIP

Source Hybrid Call Service Traversal

Authenticated Yes

Source alias

다음은 Locate(찾기)의 결과입니다. 볼드가 관심의 가치이다. 다음과 같은 결과가 표시됩니다.

- 별칭을 라우팅할 수 있다는 사실(True)
- 소스 정보(영역 이름/유형)
- 대상 정보(라우팅 중인 별칭)

- 일치하는 검색 규칙(하이브리드 통화 서비스 인바운드 라우팅)
- 통화를 전송할 영역(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

진단 로깅 Expressway 솔루션을 통과하는 통화에 대한 통화 또는 미디어 문제를 해결할 때는 언제든지 진단 로깅을 사용해야 합니다. 이 Expressway 기능을 사용하면 엔지니어가 통화를 통과하면서 Expressway가 거치는 모든 로직 결정에 대한 정보를 세부적으로 볼 수 있습니다. 전체 본문 SIP 메시지, Expressway가 해당 통화를 전달하는 방법 및 Expressway가 미디어 채널을 설정하는 방법을 확인할 수 있습니다. 진단 로깅에는 여러 개의 다른 모듈이 포함되어 있습니다. 로깅 수준을 조정하여 치명적, 오류, 경고, 정보, 디버그, 추적을 표시할 수 있습니다. 기본적으로 모든 것이 INFO로 설정되어 문제 진단에 필요한 거의 모든 것을 캡처합니다. 때때로 특정 모듈의 로깅 수준을 INFO에서 DEBUG로 조정하여 현재 상황을 더 잘 파악해야 할 수도 있습니다. 아래 단계에서는 (상호) TLS 핸드셰이크에 대한 정보를 제공하는 developer.ssl 모듈의 로깅 레벨을 조정하는 방법을 설명합니다.

1. Expressway 서버에 로그인합니다(Expression-E와 C 모두에서 수행해야 함).
2. Maintenance(유지 관리) > Diagnostics(진단) > Advanced(고급) > Support Log Configuration(지원 로그 컨피그레이션)으로 이동합니다.
3. 이 인스턴스에서 조정할 모듈로 스크롤하여 developer.ssl을 클릭합니다.
4. Level 매개 변수 옆의 메뉴에서 DEBUG를 선택합니다.
5. 저장을 클릭합니다.

이제 진단 로깅을 캡처할 준비가 되었습니다.

1. Expressway 서버에 로그인합니다(Expression-E와 C 모두에서 수행해야 함).
2. Maintenance(유지 관리) > Diagnostics(진단) > Diagnostic logging(진단 로깅)으로 이동합니다.
3. Start New Log(새 로그 시작)를 클릭합니다(tcpdump 옵션을 선택해야 합니다).
4. 문제를 재현합니다.

5. Stop Logging(로깅 중지)을 클릭합니다.

6. Download Log를 클릭합니다.

Expressway 진단 로깅의 경우 Expressway-C와 Expressway-E 모두에서 로깅을 병렬로 시작해야 합니다. 먼저 Expressway-E에서 로깅을 시작한 다음 Expressway-C로 이동하여 시작합니다. 그 시점에서 문제를 재현할 수 있습니다. 참고: 현재 Expressway/VCS 진단 로그 번들에는 Expressway 서버 인증서 또는 신뢰할 수 있는 CA 목록에 대한 정보가 포함되어 있지 않습니다. 이 기능이 유용할

케이스가 있는 경우 [이 결합](#)에 케이스를 첨부하십시오. **관련 정보**

- [Cisco Webex Hybrid Call Services 구축 설명서](#)
- [Cisco Webex Hybrid 설계 가이드](#)
- [Cisco Expressway 관리자 가이드](#)
- [기술 지원 및 문서 - Cisco Systems](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.