Expressway x15.5로 클라이언트 EKU 일몰 탐색

소개

이 문서에서는 Cisco Expressway x15.5로 클라이언트 EKU 일몰을 탐색하는 방법에 대해 설명합니다.

배경 정보

디지털 인증서는 신뢰할 수 있는 CA(Certificate Authority)에서 발급하는 전자 자격 증명으로, 인증, 데이터 무결성 및 기밀성을 보장하여 서버와 클라이언트 간의 통신을 보호합니다. 이러한 인증서에는 용도를 정의하는 EKU(Extended Key Usage) 필드가 포함되어 있습니다.

- 서버 인증 EKU(id-kp-serverAuth)는 서버가 ID를 증명하기 위해 인증서를 제공할 때 사용됩니다.
- 클라이언트 인증 EKU(id-kp-clientAuth)는 양 당사자가 서로 인증하는 mTLS(mutual TLS) 연결에 사용됩니다.

기존에는 단일 인증서에 서버 및 클라이언트 인증 EKU를 모두 포함할 수 있으므로 이중 용도로 사용할 수 있습니다. 이 점은 Cisco Expressway와 같이 서로 다른 연결 시나리오에서 서버와 클라이언트 역할을 모두 수행하는 제품에 특히 중요합니다.

문제 정의

Chrome 루트 프로그램 정책 변경

2026년 6월부터 Chrome 루트 프로그램 정책은 Chrome 루트 저장소에 포함된 루트 CA(Certificate Authority) 인증서를 제한하여 다목적 루트를 단계적으로 축소하여 모든 PKI(public-key infrastructure) 계층을 정렬하여 TLS 서버 인증 사용 사례만 제공합니다.

주요 정책 요구 사항

- 공용 루트 CA는 서버 인증(id-kp-serverAuth)에 대해서만 EKU(Extended Key Usage)를 어설션해야 합니다.
- 이러한 인증서에 클라이언트 인증 EKU를 포함하는 것은 금지됩니다.

- 공용 서버 TLS 인증서에 대한 혼합 사용 루트 CA가 더 이상 없습니다.
- 시행 일정: 2026년 6월

공용 CA 응답 일정

- 2025년 10월: 많은 공용 CA(DigiCert, Sectigo, SSL)가 기본적으로 서버 전용 인증서를 발급하기 시작했습니다.
- 2026년 5월: 공용 CA 서버가 클라이언트 인증 EKU 인증 발급을 중지합니다.
- 2026년 6월: Chrome Root Program Policy가 완전히 유효해짐

참고: 이 정책은 공용 CA에서 발급한 인증서에만 적용됩니다. 개인 PKI 및 자체 서명 인증서는 이 정책의 영향을 받지 않습니다.

Expressway에서 클라이언트 EKU의 일몰이 미치는 영향에 대해 읽으려면 공용 CA 인증서에서 Expressway for Client Auth EKU Sunset을 참조하십시오.

Expressway 릴리스 x15.5(솔루션 포함)

Expressway x15.5

Expressway x15.5는 모든 공공 인증 기관에서 클라이언트 EKU의 일몰로 인해 발생하는 문제에 대한 제안 된 수정 사항이 있습니다. 이는 글로벌 문제이며 공용 PKI 인증서를 사용하도록 선택한 모든 벤더/구축에 영향을 미칩니다.

이전 릴리스인 x15.4에는 관리자가 Expressway E에서 서버 EKU 전용 인증서(클라이언트 EKU 없음)를 업로드할 수 있는 CLI 명령 스위치가 있었습니다.

xConfiguration XCP TLS 인증서 CVS EnableServerEkuUpload: On

참고: 이 명령은 x15.5에서 더 이상 사용되지 않습니다.

X15.5 인증서 저장소 추가

x15.5에는 두 개의 인증서 저장소가 있습니다.

1. 서버 인증서 저장소

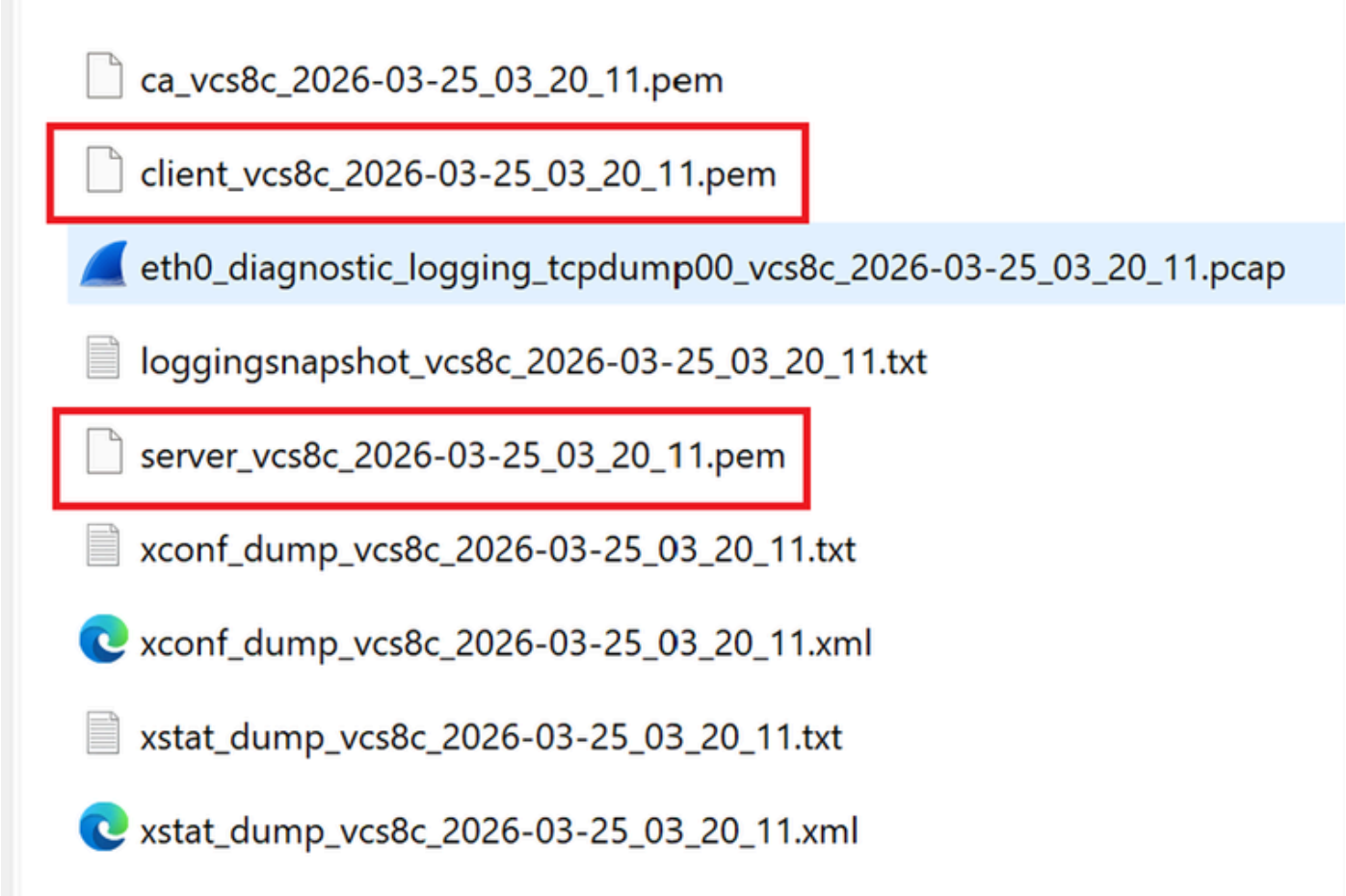
2. 클라이언트 인증서 저장소

Expressway(단일 Nic 또는 이중 Nic): 두 Expressway 인터페이스는 필요에 따라 2개의 인증서 저장소를 사용할 수 있습니다.

예:

- Expressway가 TLS 핸드셰이크 중에 클라이언트 역할을 할 때 클라이언트 인증서가 표시됩니다.
- Expressway가 TLS 핸드셰이크 중에 서버 역할을 하는 경우 서버 인증서가 표시됩니다.

참고: 두 인증서 저장소(클라이언트 및 서버) 모두 동일한 신뢰할 수 있는 CA 라이브러리를 사용합니다. 서버 및 클라이언트 인증서를 서명한 CA가 트러스트 저장소에 올바르게 업로드되었는지 확인합니다. 이제 진단 로그에 서버 인증서 및 클라이언트 인증서가 PEM 파일 형식으로 포함됩니다.



X15.4 또는 이전 버전에서 X15.5로 업그레이드

업그레이드를 수행하면 x15.4 또는 이전 버전의 서버 인증서가 x15.5의 클라이언트 인증서 저장소로 복사됩니다. x15.5의 클라이언트 및 서버 인증서 저장소에는 동일한 인증서가 있습니다.

스크린샷 예제

15.4의 Expressway 서버, 현재 서버 인증서 일련 번호 46:df:76:aa:00:00:00:00:29

인증서:

버전: 3개(0x2)

일련 번호:

46:df:76:aa:00:00:00:00:00:29

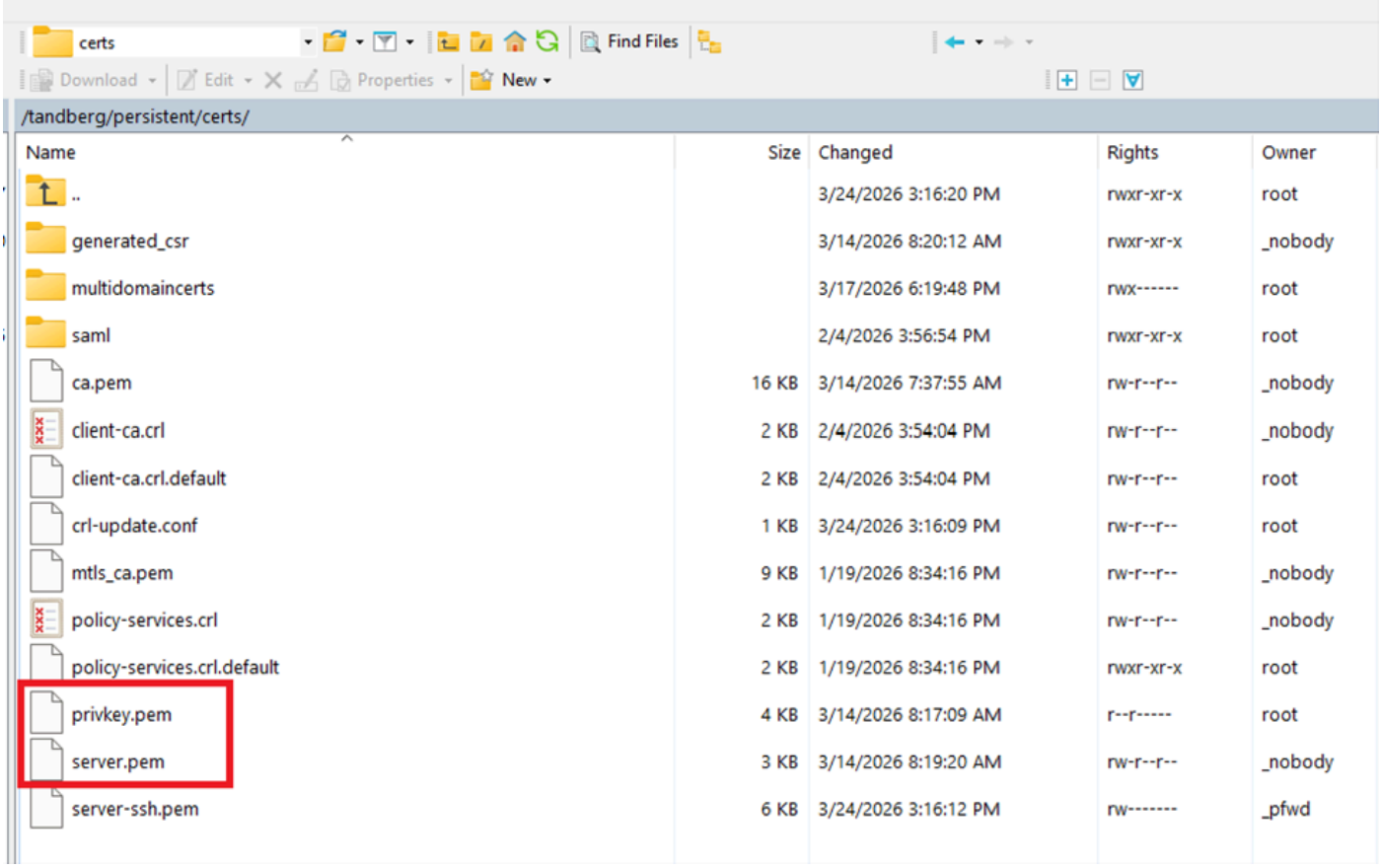
유효성

다음 날짜 이전: 3월 14일 02시 37분 40초 2026 GMT

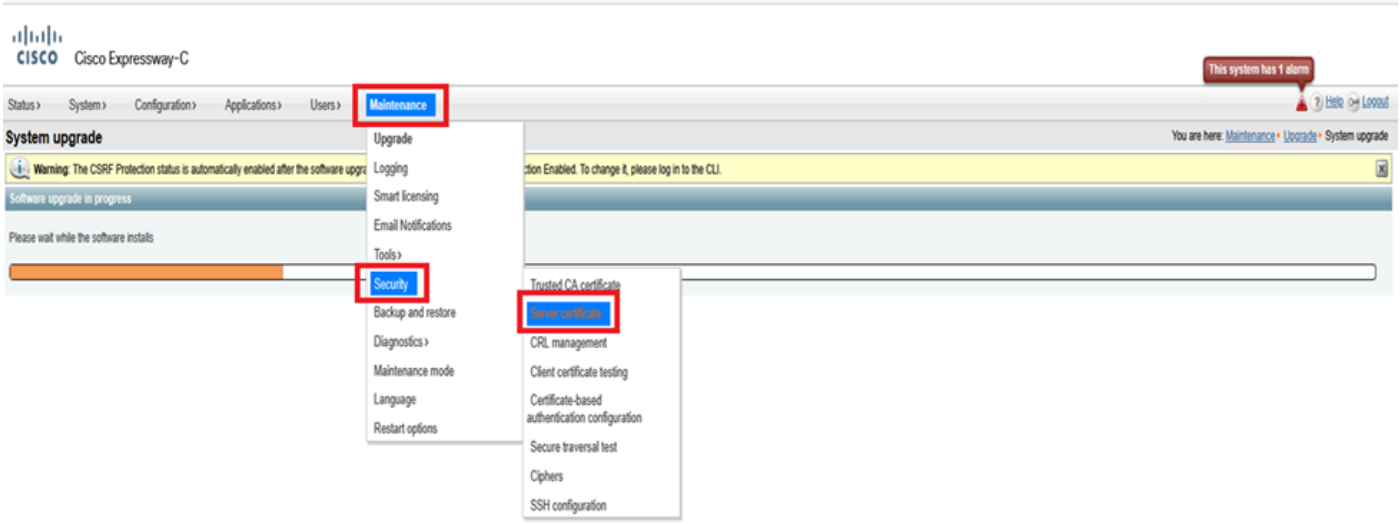
다음 이후 아님: 3월 14일 02시 47분 40초 2028 GMT

제목: C = IN, ST = KA, L = KA, O = Cisco, OU = TAc, CN = cluster.s.com

x15.4의 Expressway 파일 시스템 persistent/cert 디렉토리:



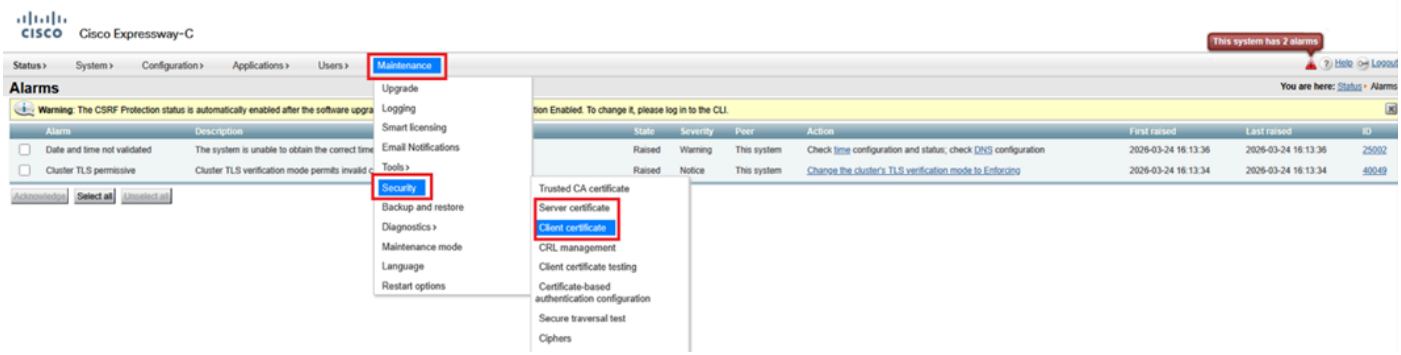
x15.4의 Expressway 메뉴(Maintenance(유지 관리) > Security(보안) > Server certificate(서버 인증서))(서버 인증서 필드만 표시됨):



x15.5로 성공적으로 업그레이드한 후

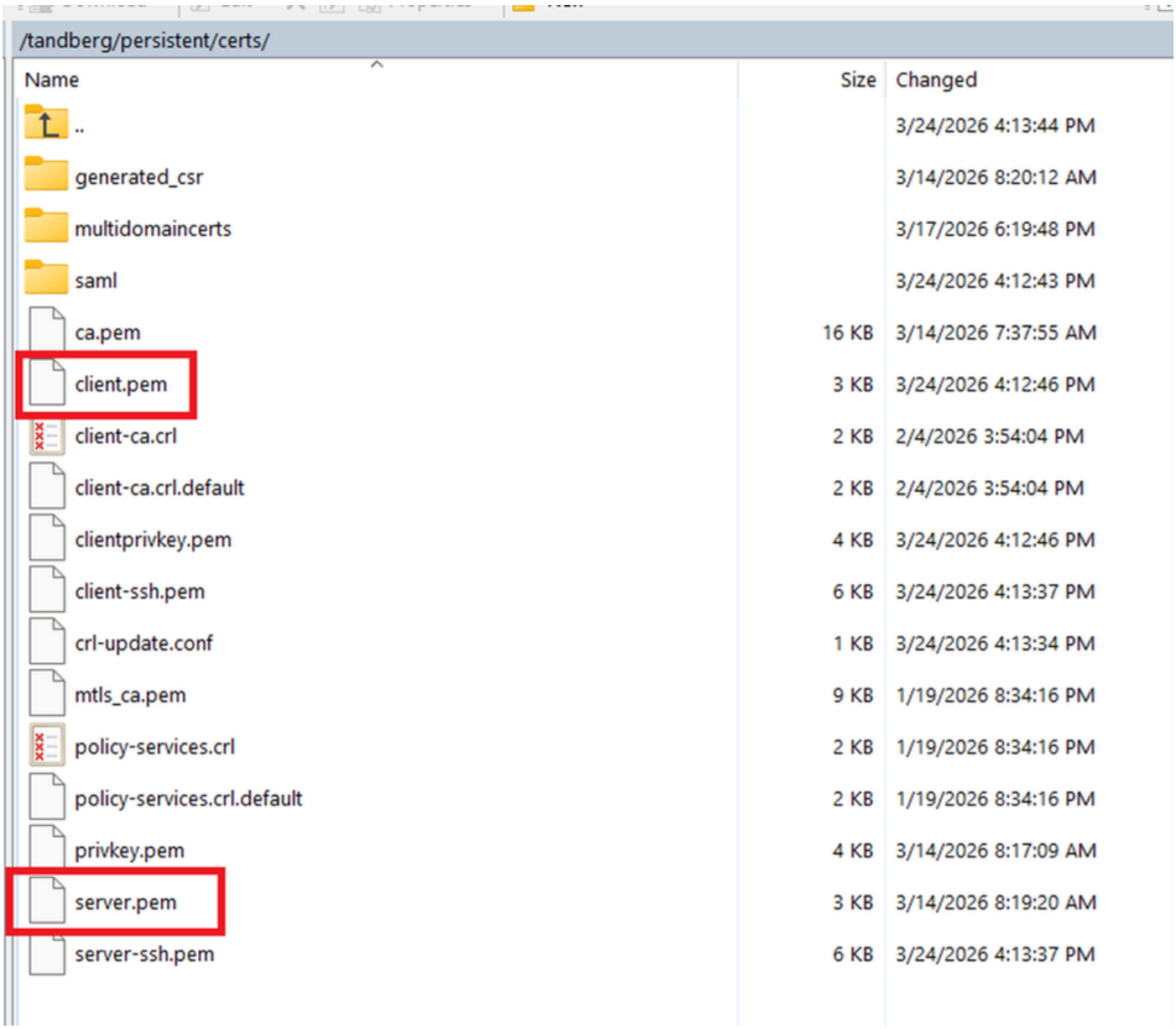
여기에서 Maintenance(유지 관리) > Security(보안) > client certificate and server certificates(클라이언트 인증서 및 서버 인증서)의 2가지 인증서 옵션을 볼 수 있습니다. x15.5로 업그레이드한 후 x15.4의 서버 인증서가 x15.5의 클라이언트 인증서 저장소로 복사되었으므로 웹 관리자의 서버 및

클라이언트 인증서 포털에서 모두 동일한 인증서를 표시합니다.



x15.5 기존 인증서 및 개인 키로 업그레이드 후 클라이언트 인증서 저장소로 복사되었습니다.

x15.5의 Expressway 파일 시스템 persistent/cert 디렉토리:



TLS 핸드셰이크 중 X15.5 EKU 확인

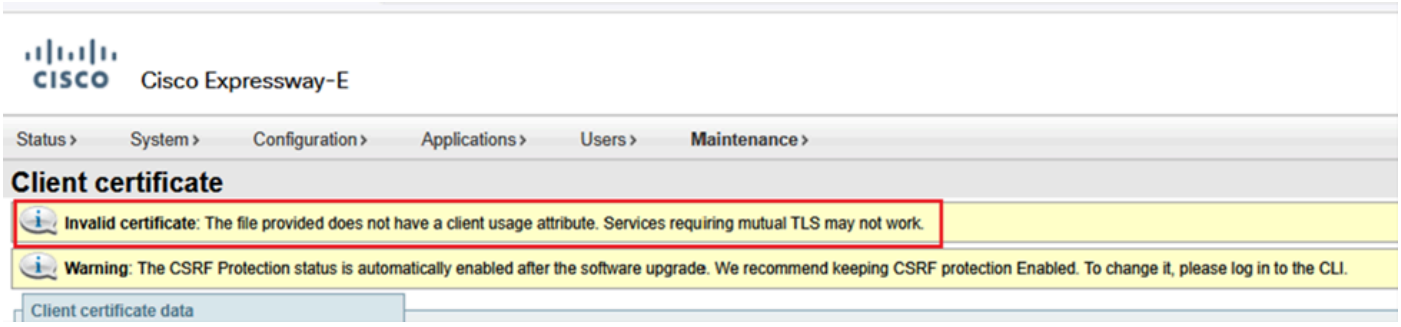
x15.5에서는 TLS 핸드셰이크 중에 EKU(Extended Key Usage)를 확인하는 새 CLI 명령이 도입되었습니다. 기본값은 "ON"입니다. 명령 집합은 Expressway Core 및 Edge에서 유효합니다.

명령 집합은 Expressway에 대한 모든 인바운드 SIP TLS 연결을 검사합니다. (인바운드 클라이언트 Hello/인증서가 제공됨). "ON"을 설정하면 TLS 개시자가 제공한 인증서에 인증서에 클라이언트 EKU가 포함되어 있는지 확인합니다. 꺼진 경우 검사를 우회합니다. 그러나 서버 EKU가 인증서에 있는지 확인합니다.

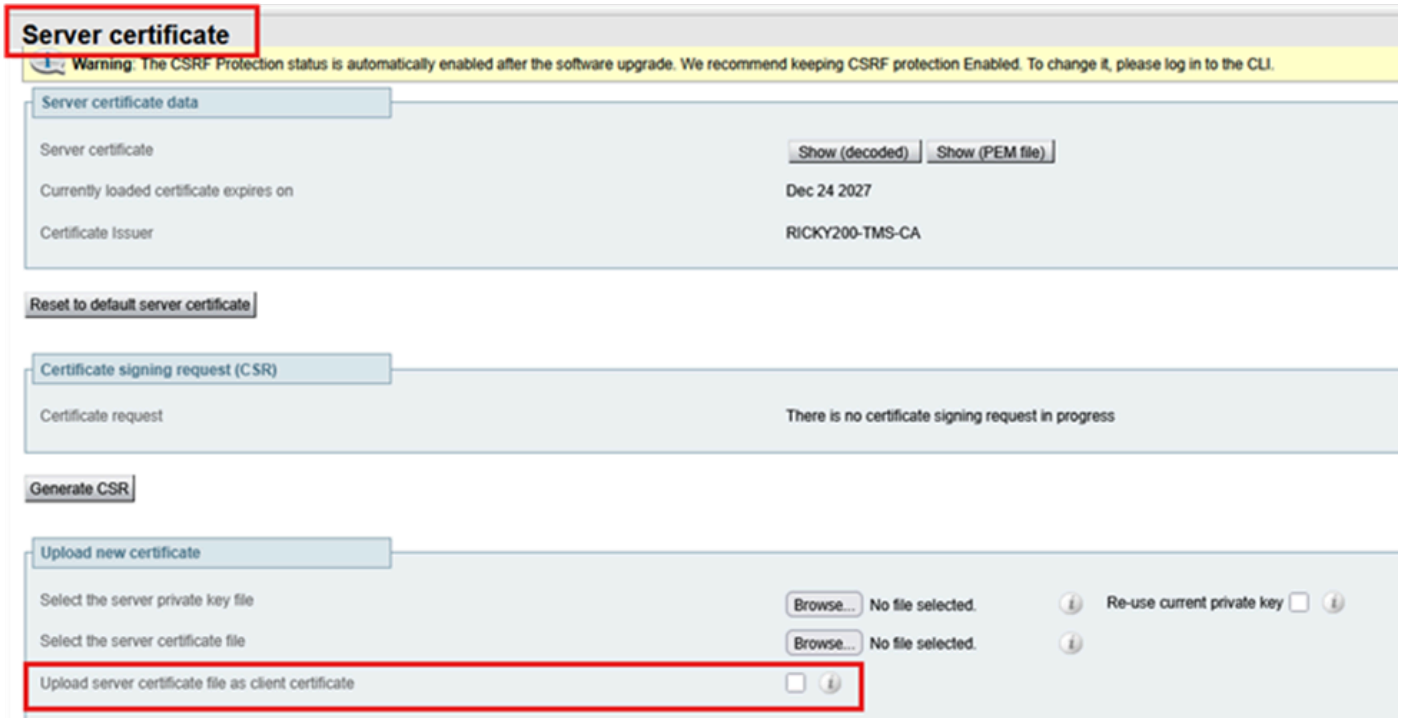
xconfiguration SIP TLS 인증서 ExtendedKeyUsage 확인 모드: 켜기/끄기:

참고: 클라이언트 인증서를 생성하고 클라이언트 EKU가 포함되지 않은 CSR에 서명하는 경우(공용 CA 서명 인증서의 예), 클라이언트 인증서 저장소에서 이 인증서를 수동으로 업로드할 수 없습니다. 따라서 CSR에 서명하여 생성된 인증서에 항상 클라이언트 EKU가 포함되어 있는지 확인해야 합니다(클라이언트 EKU를 삽입하기 위해 전용 CA를 사용할 수 있음).

팁: 이 오류는 클라이언트 인증서 저장소에서 클라이언트 EKU가 없는 CSR 서명 인증서를 업로드하려고 할 때 분명해집니다.



그러나 서버 인증서 저장소를 통해 서버 EKU만 있는(클라이언트 EKU 없음) 인증서를 업로드하도록 선택하고 서버 인증서 파일 업로드를 클라이언트 인증서로 선택하면 인증서가 클라이언트 인증서 저장소에 복사됩니다. Expressway-Edge에서 사설 CA 서명 인증서를 사용하지 않으려는 관리자는 서버 인증서 저장소에서 클라이언트 인증서 저장소로 서버 EKU만 복사하도록 선택할 수 있습니다.

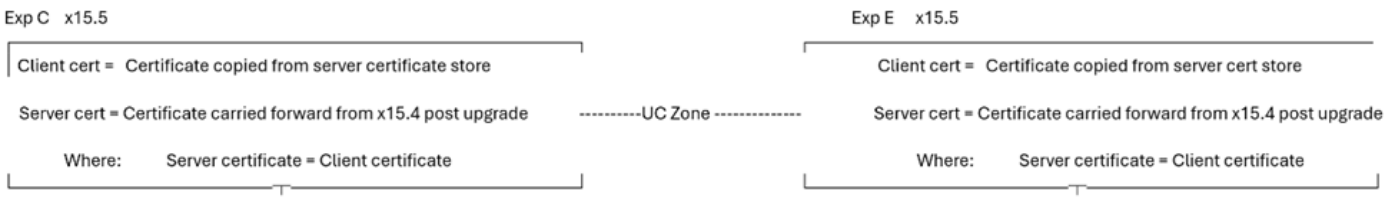


여러 인증서 저장소, 여러 구축 시나리오

현재 Expressway에는 두 개의 인증서 저장소가 있으므로 여러 가지 인증서 저장 시나리오가 있습니다.

조건 1: 업그레이드

Expressway가 x15.4에서 업그레이드되거나 x15.5 이전인 경우 이 조건은 true입니다. x15.4 버전의 기존 인증서는 두 개의 인증서 저장소에 복사됩니다. x15.5 클라이언트 및 서버에서는 인증서가 동일합니다.

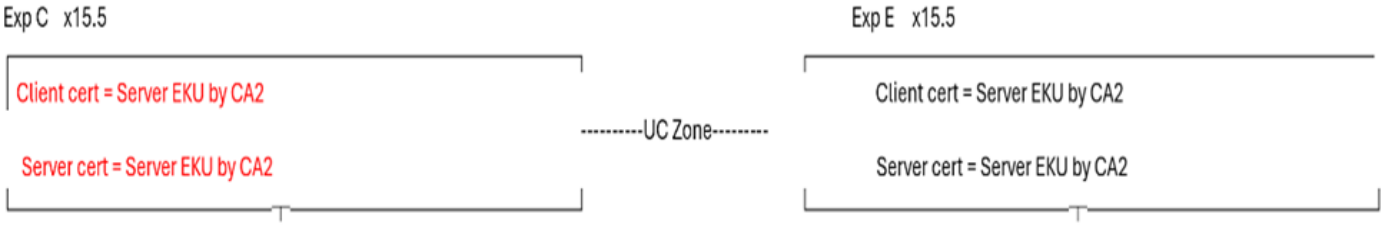


조건 2: 관리자가 x15.5에 새 인증서를 설치할 때(기존 인증서가 만료됨)

CA 1 = 내부 CA

CA 2 = 공용 CA

다음 그림에서 Expressway Core는 서버 EKU가 CA 2(공용 CA)에서만 서명된 클라이언트 인증서와 서버 EKU가 CA 2(공용 CA)에서만 서명된 서버 인증서를 가지고 있습니다. 마찬가지로 Expressway E에는 CA2(공용 CA)에서 서명한 서버 EKU가 있는 클라이언트 인증서와 CA2(공용 CA)에서만 서명한 서버 EKU가 있는 서버 인증서가 있습니다.



Expressway 코어 서버 인증서에 클라이언트 EKU, Unified communications 접근 영역, MRA가 없으면 WebRTC 프록시가 작동하지 않습니다. Expressway Core 서버 인증서에 클라이언트 EKU가 있는지 확인합니다. 이는 사용자가 공용 CA의 모든 인증서를 서명하도록 선택하는 일반적인 사용 사례입니다. 공용 CA는 인증서에 클라이언트 EKU를 포함하지 않으므로 Unified Communications 접근 영역이 활성화됩니다.

UC 영역을 활성화하려면 Expressway E에서 EKU 검사를 끄는 것이 좋습니다. 그러면 UC 영역이 나타납니다. 그러나 SSH 터널은 비활성 상태로 유지됩니다. 현재 2222의 SSH 터널 통신에는 클라이언트 EKU의 검증이 필요합니다.

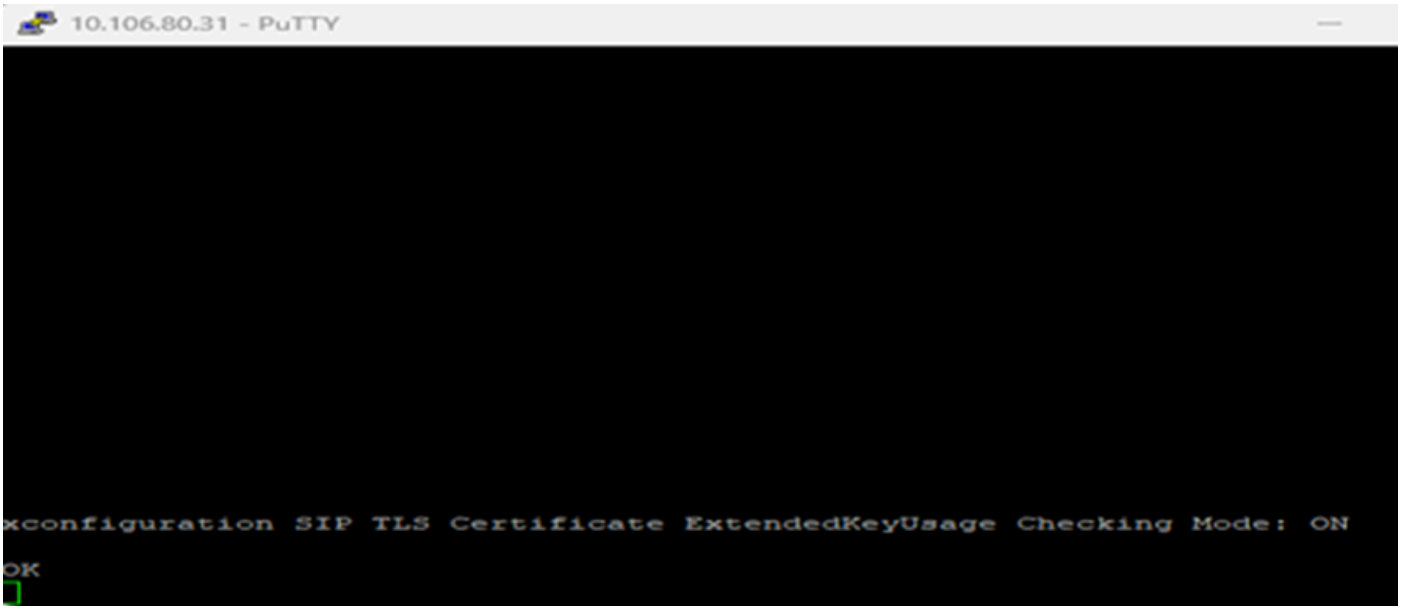
MRA 클라이언트 로그인 및 WebRTC 프록시 기능은 작동하지 않습니다. 프라이빗 CA에 의지해야 할 수도 있습니다.

테스트 사례 1

- Expressway E에서 EKU 검사가 "ON"인 경우
- Expressway Core의 클라이언트 및 서버 인증서에 서버 EKU만 있는 경우
- UC 영역 상태가 실패함

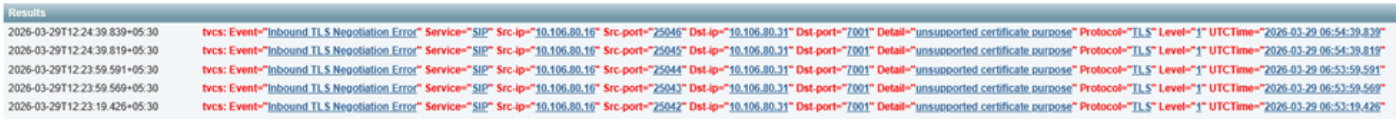
Expressway-Edge ExtendedKeyUsage 확인 켜짐

xconfiguration SIP TLS 인증서 ExtendedKeyUsage 확인 모드: On:



통합 통신 영역 오류:

Expressway E 로그는 10.106.80.16 = Expressway Core, 10.106.80.31 = Expressway Edge인 위치를 보여줍니다.

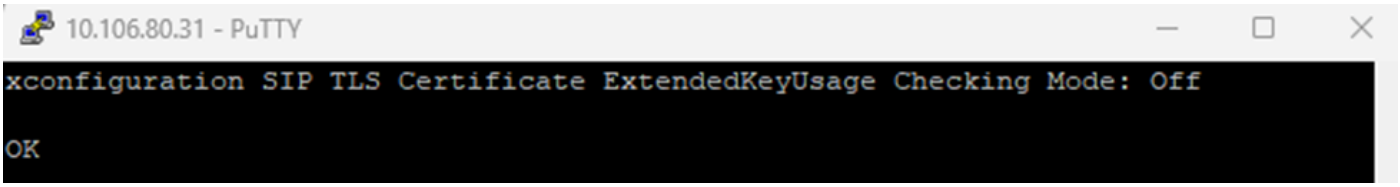


테스트 사례 2

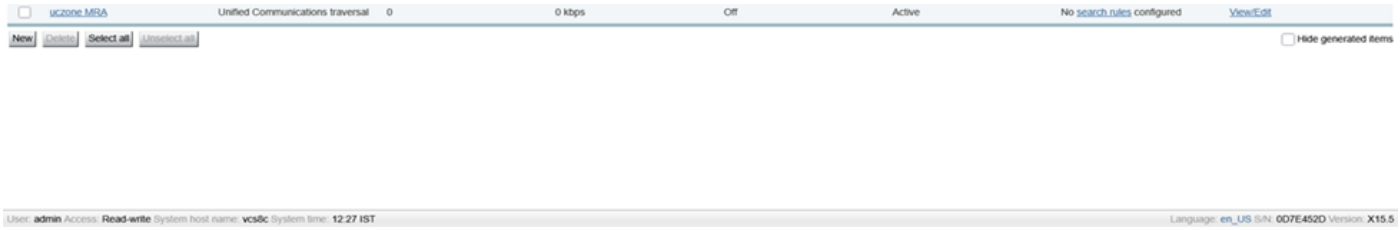
- Expressway E에서 EKU 체크가 꺼진 경우
- Expressway Core의 클라이언트 및 서버 인증서에 서버 전용 EKU가 있는 경우
- UC 영역 상태가 활성입니다.

Expressway E에서 EKU 검사를 끕니다.

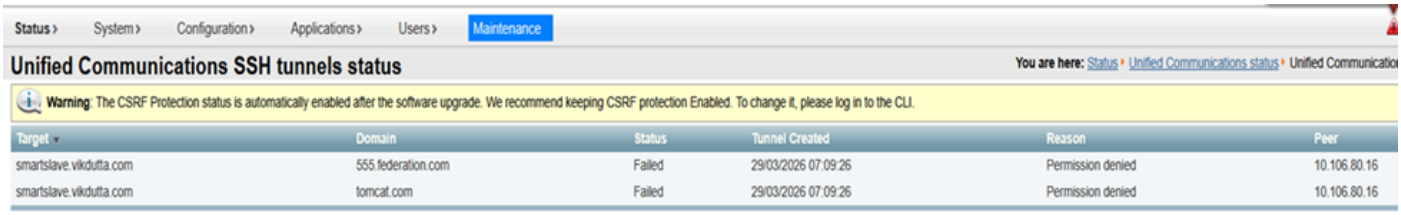
xconfiguration SIP TLS 인증서 ExtendedKeyUsage 확인 모드: 끄기



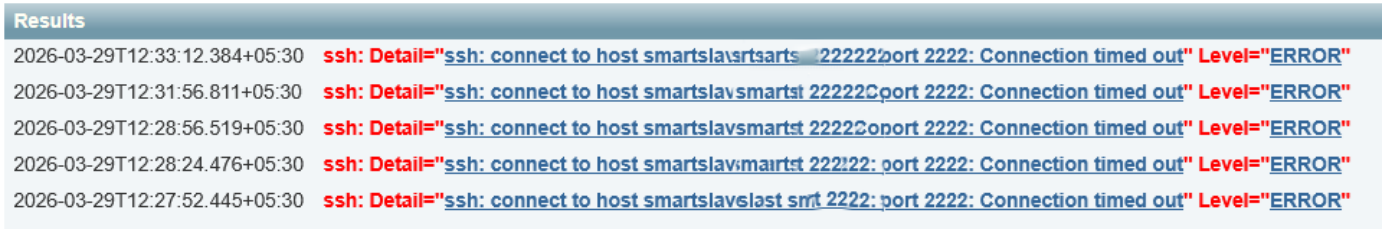
Unified communication zone Active(통합 통신 영역 활성):



그러나 ssh 터널이 여전히 실패했습니다.



Expressway 이벤트 로그



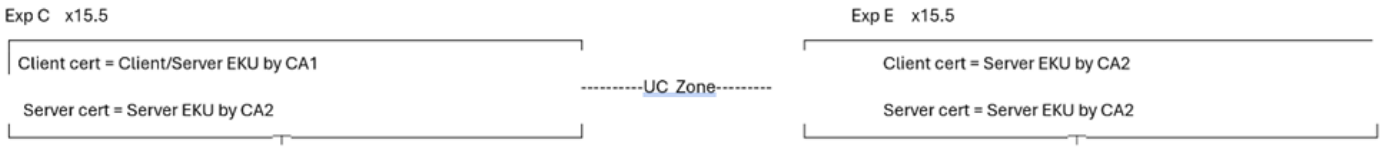
조건 2.1: 성공 사례

CA 1 = 내부 CA

CA 2 = 공용 CA

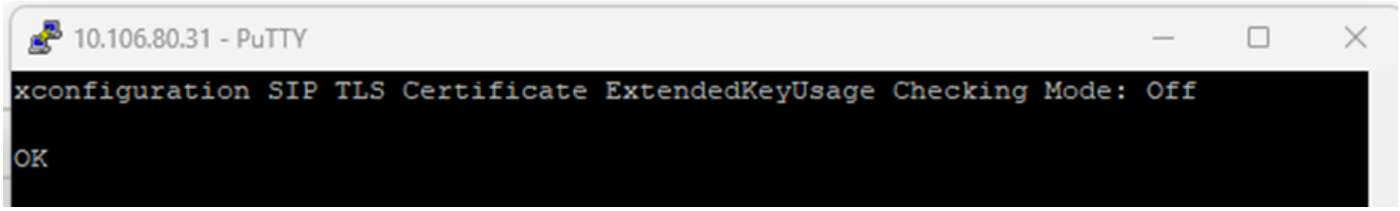
- 여기서 Expressway 코어 클라이언트 인증서는 CA 1(내부 CA)에서 서명되며 클라이언트/서버 EKU를 모두 포함합니다.
- Expressway 코어 서버 인증서는 CA 2 공용 CA에서 서명하며 서버 EKU만 포함합니다.
- Expressway 에지 서버 인증서는 CA 2 공용 CA에서 서명하며 서버 EKU만 포함합니다.

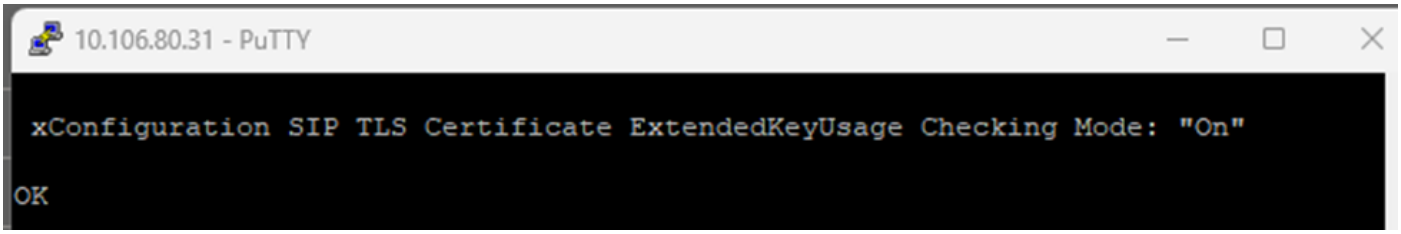
- Expressway Edge 클라이언트 인증서는 CA 2 공용 CA에서 서명하며 서버 EKU만 포함합니다.



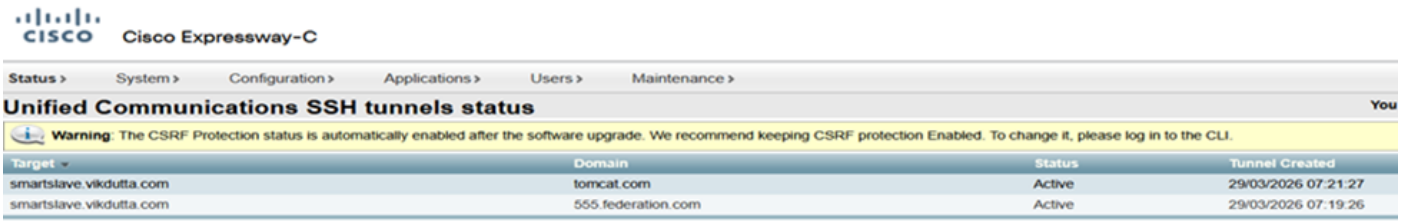
이 조건은 성공 사례입니다. EKU 확인 모드가 ON/OFF인지 여부에 관계없이 Unified Communication 영역과 SSH 터널이 모두 활성화됩니다. MRA 클라이언트가 작동합니다.

Expressway Edge EKU 체크가 OFF 또는 ON인지 여부는 중요하지 않습니다. Expressway 코어 클라이언트 인증서에 클라이언트 EKU가 포함되어 있습니다.

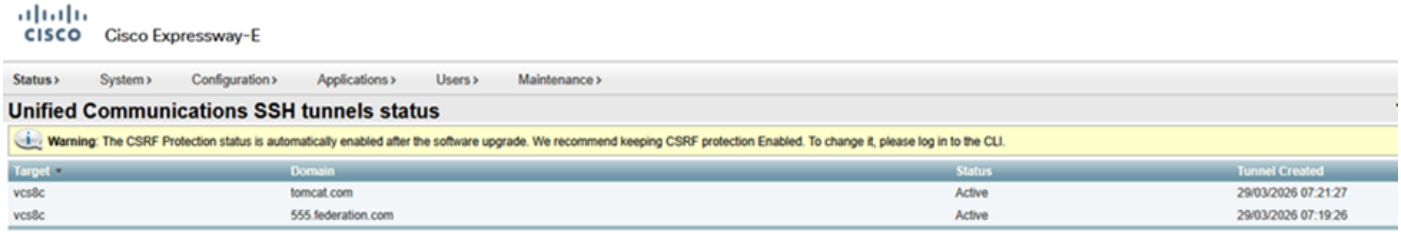




Expressway 코어 활성 SSH 터널:

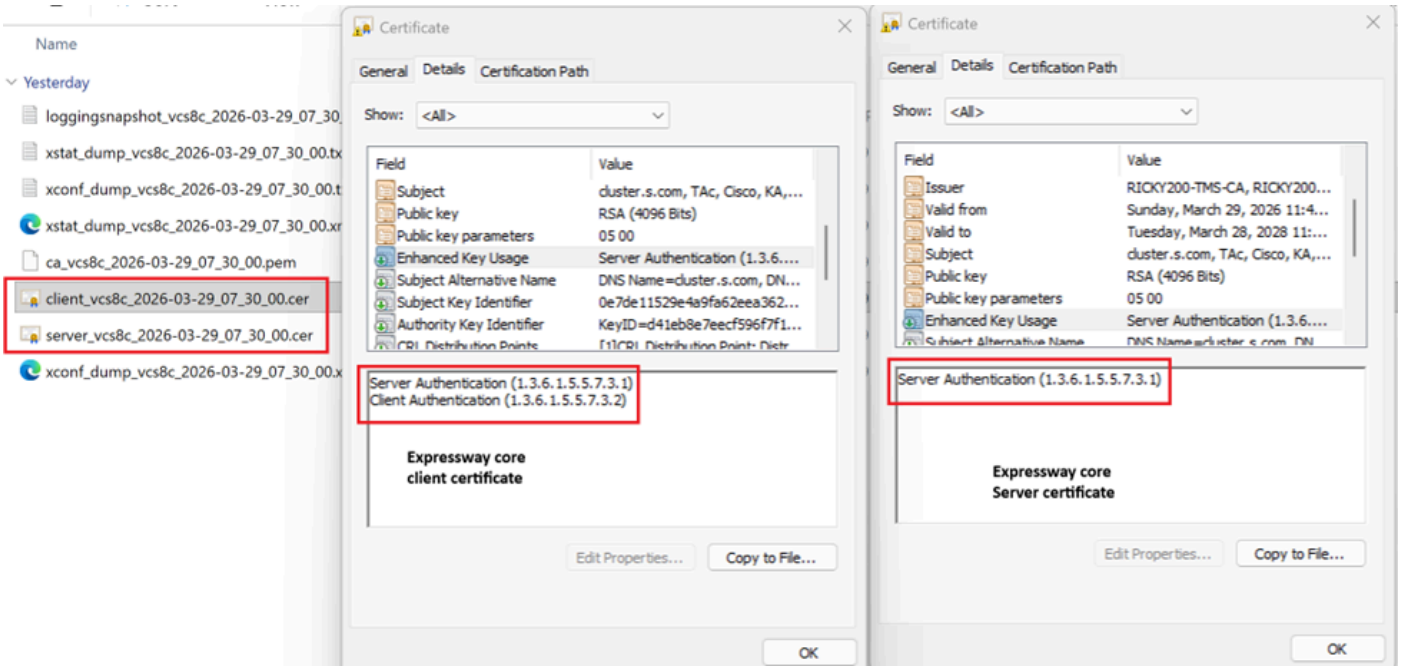


Expressway Edge Active의 SSH 터널

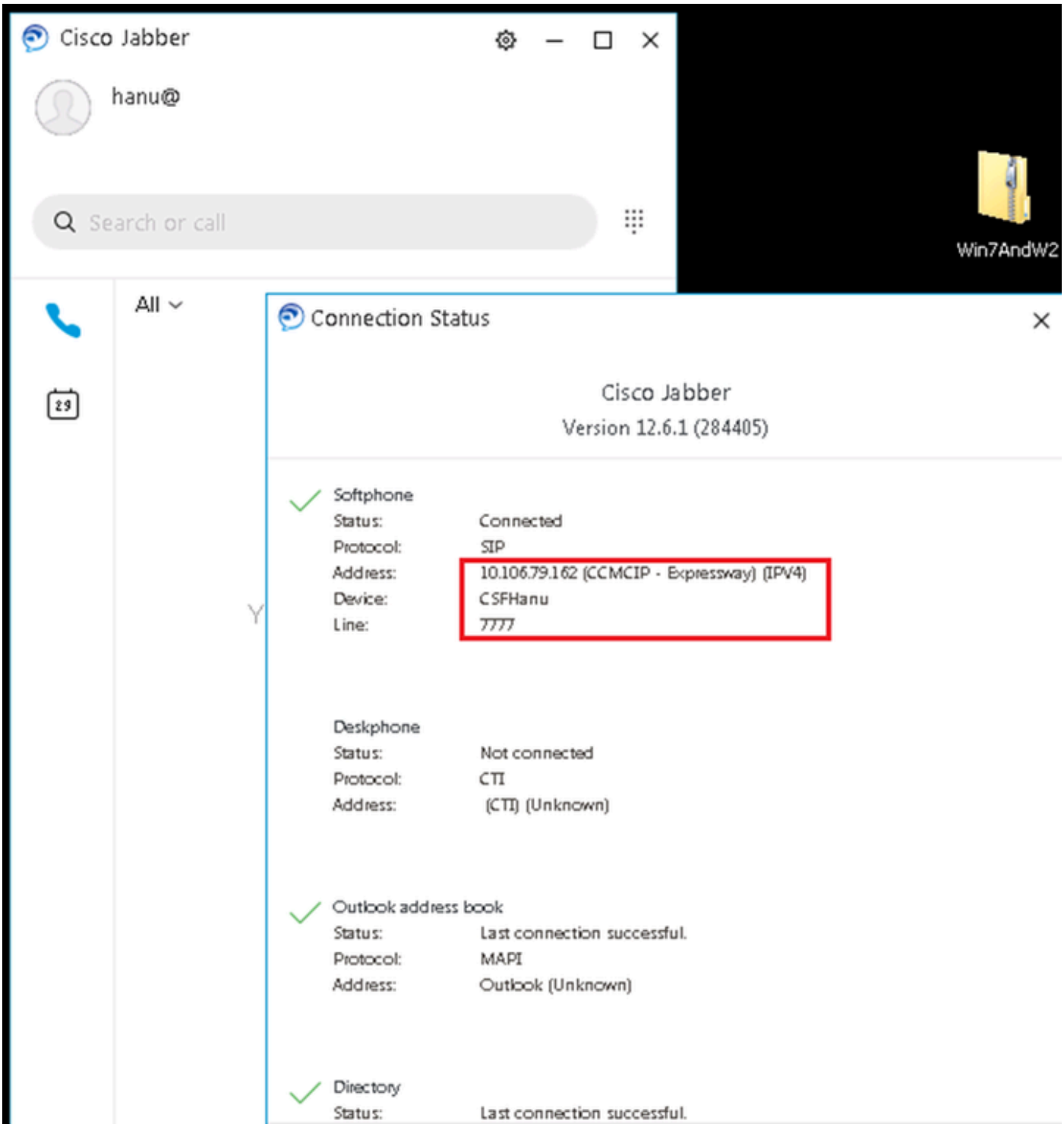


Unified Communication MRA 영역 상태 활성:

- Expressway-Core 클라이언트 인증서에는 서버 EKU 및 클라이언트 EKU가 있습니다.
- Expressway 코어 서버 인증서에는 서버 EKU만 있습니다.



MRA 클라이언트가 로그인하고 등록됨:

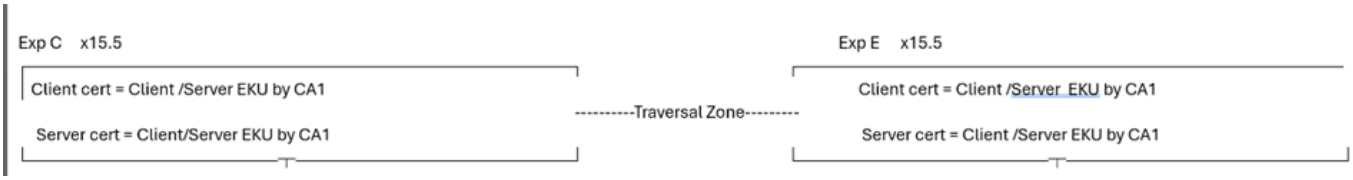


참고: MRA 및 WebRTC 프록시가 작동할 수 있도록 인증서에 있는 EKU를 비교하고 기록해 둡니다. 작동 중인 구축과 작동하지 않는 구축의 비교입니다.

조건 3: 프라이빗 CA로 모든 인증서 서명

CA 1 = 내부 CA

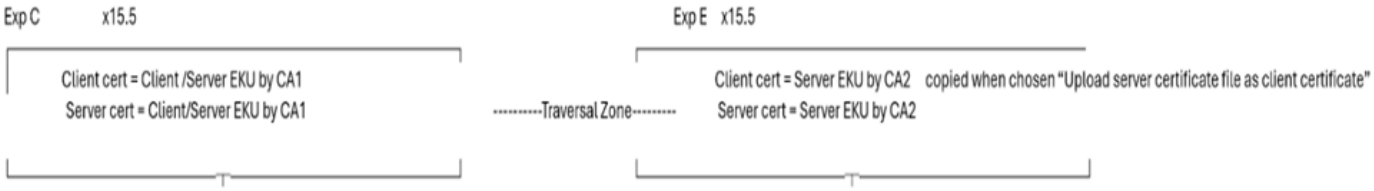
CA 2 = 공용 CA



조건 3에서 모든 인증서는 내부 CA(CA1)에 의해 서명됩니다.

- Expressway-E에서 TLS 연결을 전송할 때 CA 1 루트/중간자를 원단 엔티티와 교환해야 합니다. far-end에 기능이 없거나 개인 CA 인증서 업로드를 허용하지 않는 경우 TLS 연결이 실패합니다.
- MRA 클라이언트는 프라이빗 인증서가 OS 신뢰 저장소에 없는 경우 팝업을 수락하기 위해 인증서를 가져옵니다.

조건 4: Expressway Edge에는 서버 EKU만 있는 공용 인증서가 있습니다.



조건 4에서 Expressway 핵심 클라이언트 및 서버 인증서는 서명된 내부 CA이며 클라이언트와 서버 EKU가 모두 있습니다. Expressway E 서버 인증서는 서명된 공용 CA이며 서버 EKU만 있습니다. 서버 인증서가 클라이언트 인증서 저장소로 복사됩니다. 클라이언트 인증서로 서버 인증서 파일 업로드를 선택합니다.

조건 4에서 TLS 연결이 원엔드로 설정될 때 Expressway -E가 TLS 클라이언트 hello를 전송하는 경우 원엔드는 클라이언트 EKU 검사를 비활성화해야 합니다(클라이언트 인증서에 클라이언트 인증 EKU가 없기 때문). 그렇지 않으면 TLS 연결이 실패합니다.

사용자 구축 및 활용 사례에 따라 현장에서 더 많은 조건이나 시나리오가 있을 수 있으며, 제한된 생각의 흐름 때문에 모두 다룰 수 없습니다. 그러나 기억해야 할 점은 다음과 같습니다.

- # TLS 핸드셰이크 중에 Expressway가 클라이언트가 되면 클라이언트 인증서가 피어에 표시됩니다.
- #IF 핸드셰이크 중에 Expressway가 서버가 됩니다. 서버 인증서가 피어에 표시됩니다.

이러한 검사 사례와 함께 이러한 추론이 확립되었다.

시나리오 1

이 시나리오에서 Expressway는 Webex와의 MTLS 핸드셰이크 중에 클라이언트 인증서를 제공합니다.

Webex 회의 영상 통화:

샘플 통화 흐름 Jabber -à CUCM -à Exp Core —à Exp Edge —à Webex

10.106.80.31= Expressway 에지

163.129.37.33 = Webex

2026-03-24T11:54:26.106+00:00 smartslave tvcs: UTCTime="2026-03-24 11:54:26,106" 모듈 ="network.sip" 수준="디버그": Action="보냄" Local-ip="10.106.80.31" Local-port="25002" Dst-ip="163.129.37.33" Dst-port="5061"

Expressway Edge에는 이 일련 번호(2f0000004c869c77c8981becde00000000004c)가 있는 클라이언트 인증서가 있습니다.

Expressway Edge는 TLS 협상 중에 'Webex'에 클라이언트 hello를 전송한 다음 클라이언트 인증서를 전송합니다.

일련 번호 2f0000004c869c77c8981becde00000000004c:

1. Expressway Edge는 mTLS 협상 중에 'Webex'에 클라이언트 hello(pkt= 13699)를 전송합니다.

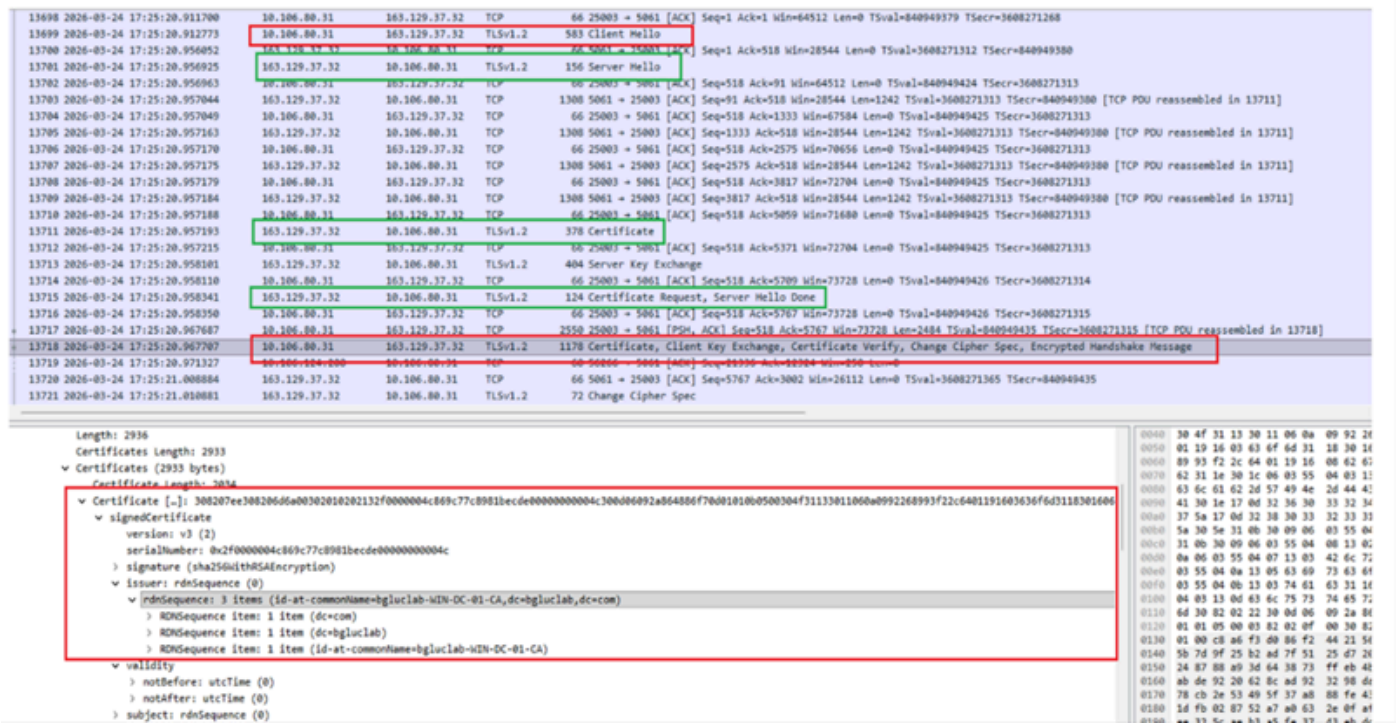
2. Webex에서 Expressway Edge로 서버 hello를 보냅니다(pkt=13701).

3. Webex가 인증서를 Expressway Edge로 보냅니다(pkt=13711).

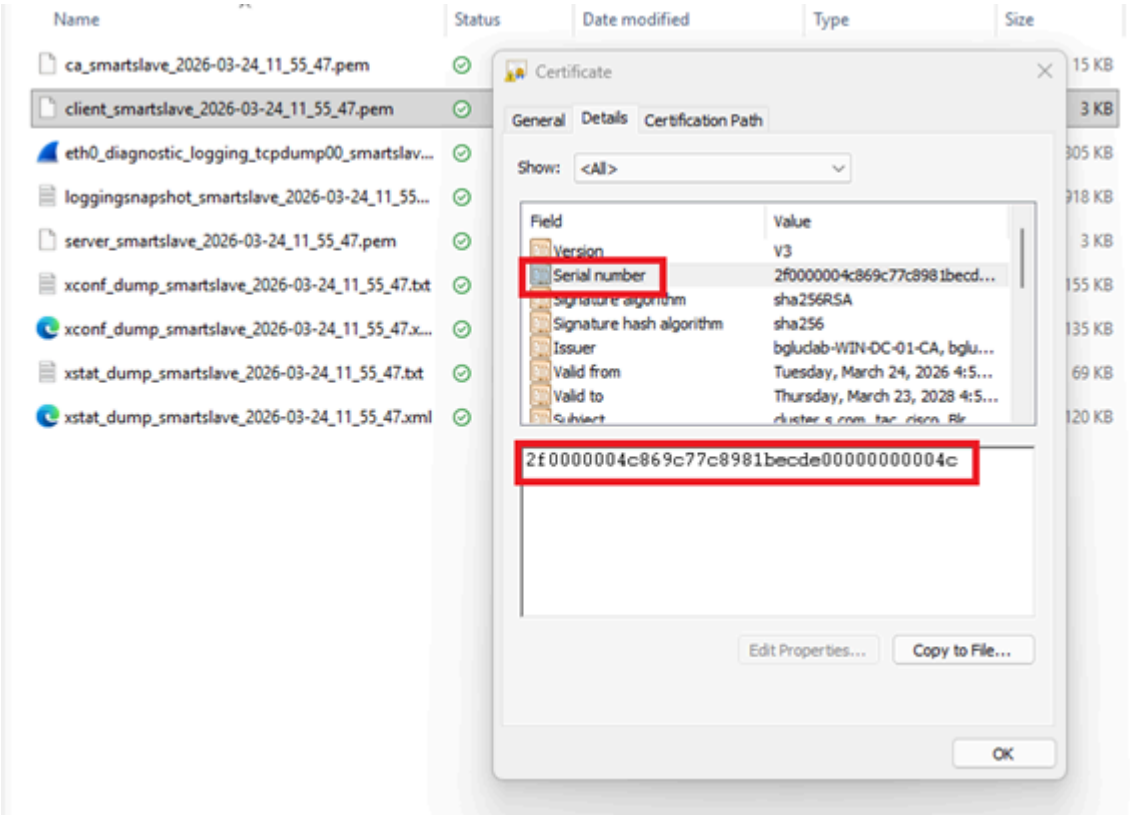
4. Webex에서 Expressway 에지 인증서 "CertificateRequest"(pkt=13715)를 요청합니다.

5. Expressway Edge가 인증서를 Webex에 보냅니다(pkt=13718).

(스크린샷)



Expressway 에지의 클라이언트 인증서:



시나리오 2

Expressway는 mTLS 핸드셰이크 중에 서버 엔터티가 되어 서버 인증서를 제공합니다.

Expressway가 서버 인증서를 제공하는 경우 Expressway에는 확인 이름이 ON인 5061 이상의 보안 네이버 영역이 있습니다.

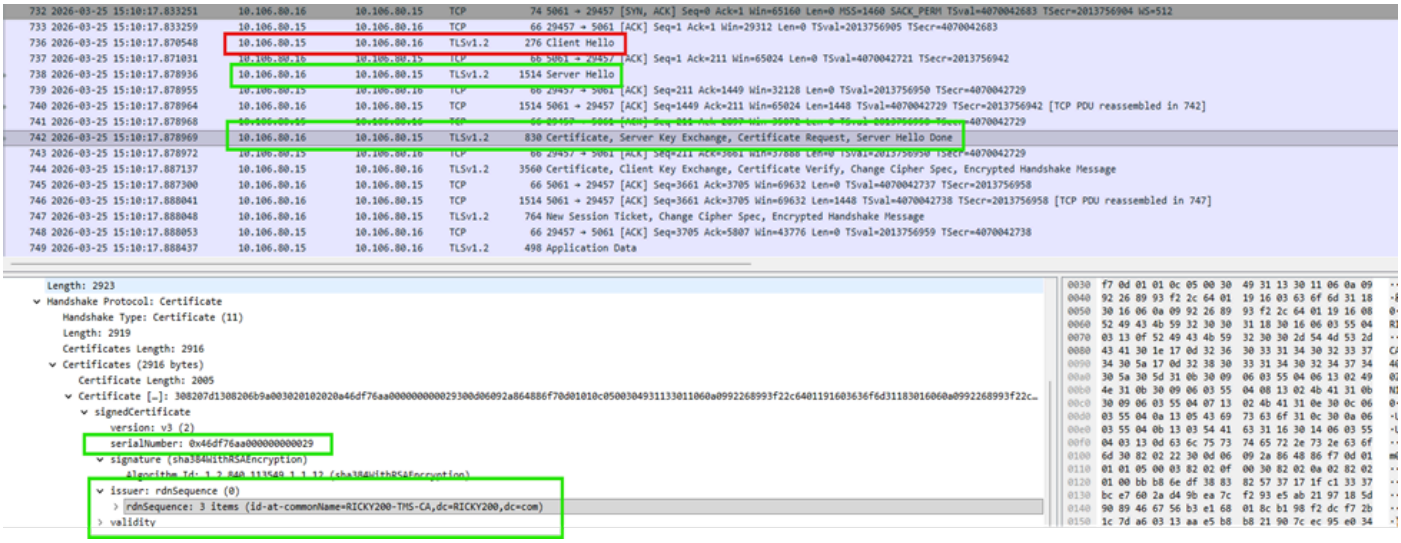
Expressway 노드 x15.5와 Expressway 노드 x8.11.4 간의 보안 네이버 영역:

10.106.80.15 (x8.11.4) sends a client hello to 10.106.80.16 (x15.5) (pkt=736)

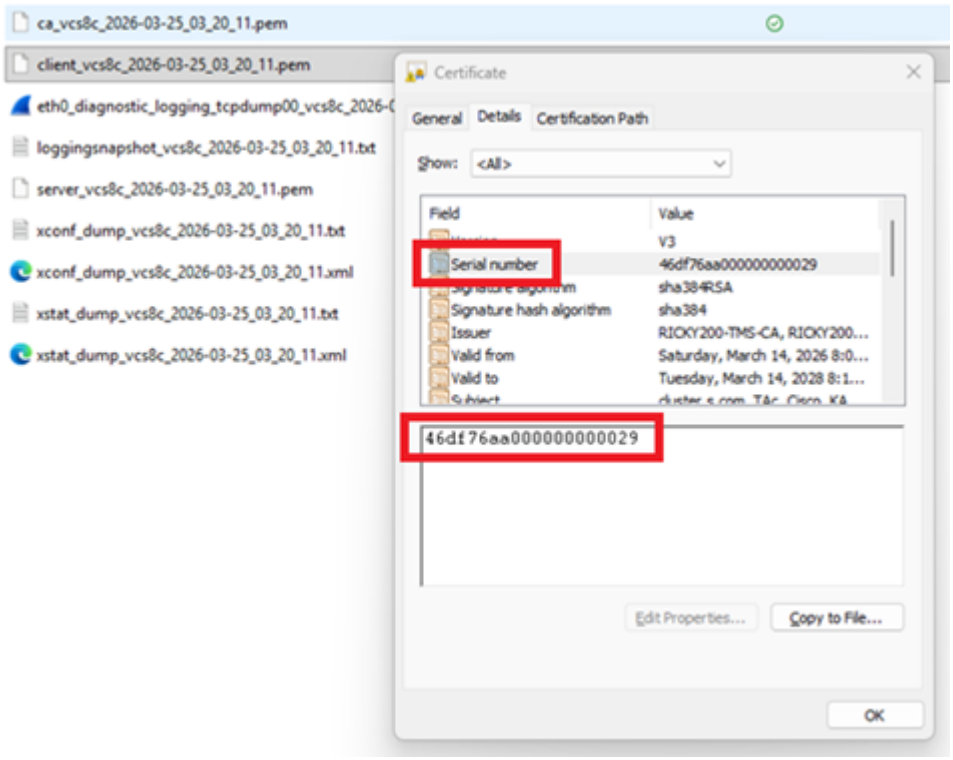
10.106.80.16 sends a server hello to 10.106.80.15 (pkt=738)

10.106.80.16 (x15.5) presents its server cert during TLS handshake (pkt=742) and requests client's cert

10.106.80.15 (x8.11.4) sends client certificate (pkt=744)



이 스크린샷은 서버 인증서를 일련 번호와 일치하는지 보여줍니다.

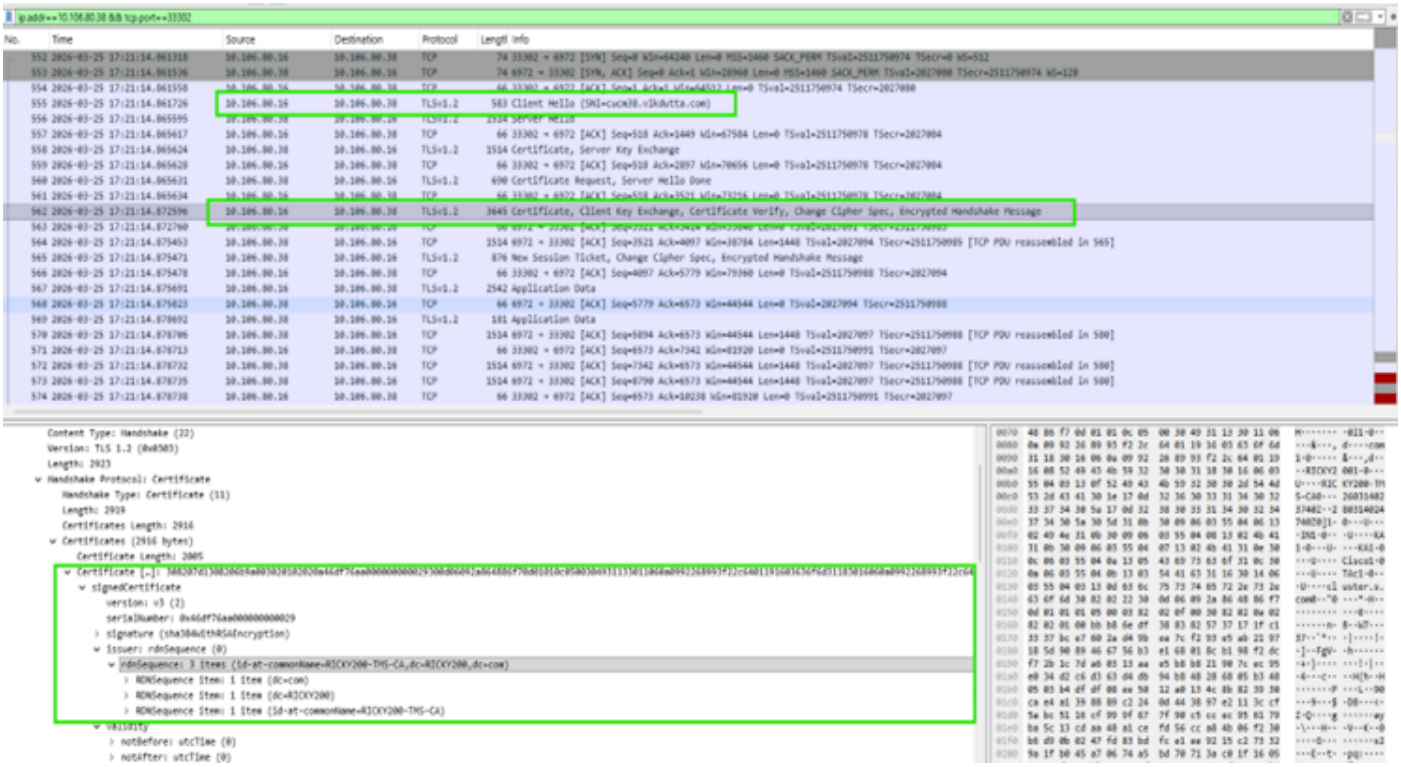


테스트 케이스 3: MRA 클라이언트는 로그인을 위해 프로비저닝되며 워크플로에는 Expressway Core와 CUCM 간의 트래픽 서버 인증서 검증이 포함됩니다.

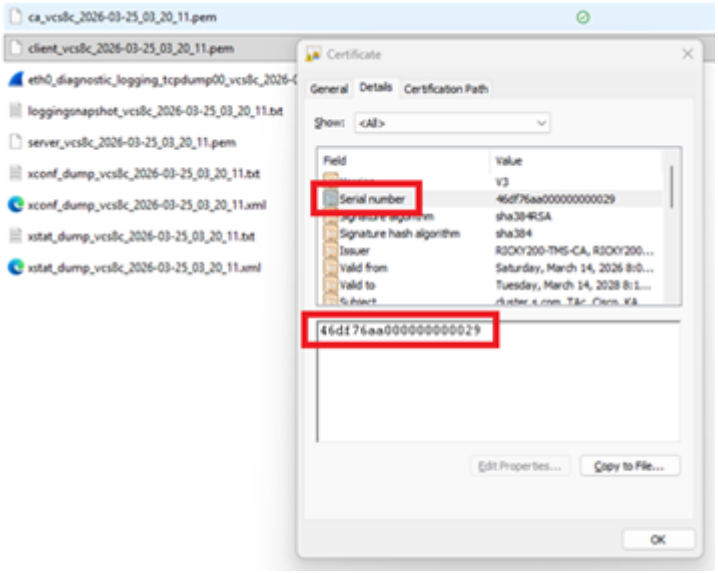
10.106.80.16 = Expressway Core x15.5

10.106.80.38 = CUCM

- Exp C 16은 6972 TFTP에서 클라이언트 hello를 전송합니다.
- Exp C 16은 TLS 핸드셰이크 중에 클라이언트 인증서를 전송합니다.



Expressway 코어 클라이언트 인증서:



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.