MRA/Expressway에 대한 ActiveControl 활성화

목차

소개

이 문서에서는 MRA(Mobile and Remote Access) 클라이언트 및 온프레미스 엔드포인트에서 Expressway를 통한 Webex Meetings로의 통화에 대해 ActiveControl 프로토콜을 활성화하는 다양한 옵션에 대해 설명합니다. MRA는 VPN(Virtual Private Network-less) Jabber 및 엔드포인트 기능을 위한 구축 솔루션입니다. 이 솔루션을 통해 최종 사용자는 전 세계 어디서나 내부 엔터프라이즈 리소스에 연결할 수 있습니다. ActiveControl 프로토콜은 회의 로스터, 비디오 레이아웃 변경, 뮤팅 및 녹음 옵션과 같은 런타임 기능을 통해 더욱 풍부한 회의 경험을 제공할 수 있는 Cisco 독점 프로토콜입니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Expressway(MRA 및 B2B 통화)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Expressway X12.5
- Cisco Meeting Server(CMS) 2.9
- Cisco Unified Communications Manager 12.5

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

명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

이 문서에서는 Cisco Meeting Server(CMS)에 대한 MRA 클라이언트 연결에 대해 주로 살펴보지만 Webex Meetings에 연결할 때와 같은 다른 유형의 플랫폼 또는 연결에도 동일하게 적용됩니다. 다음 유형의 통화 흐름에 대해 동일한 논리를 적용할 수 있습니다.

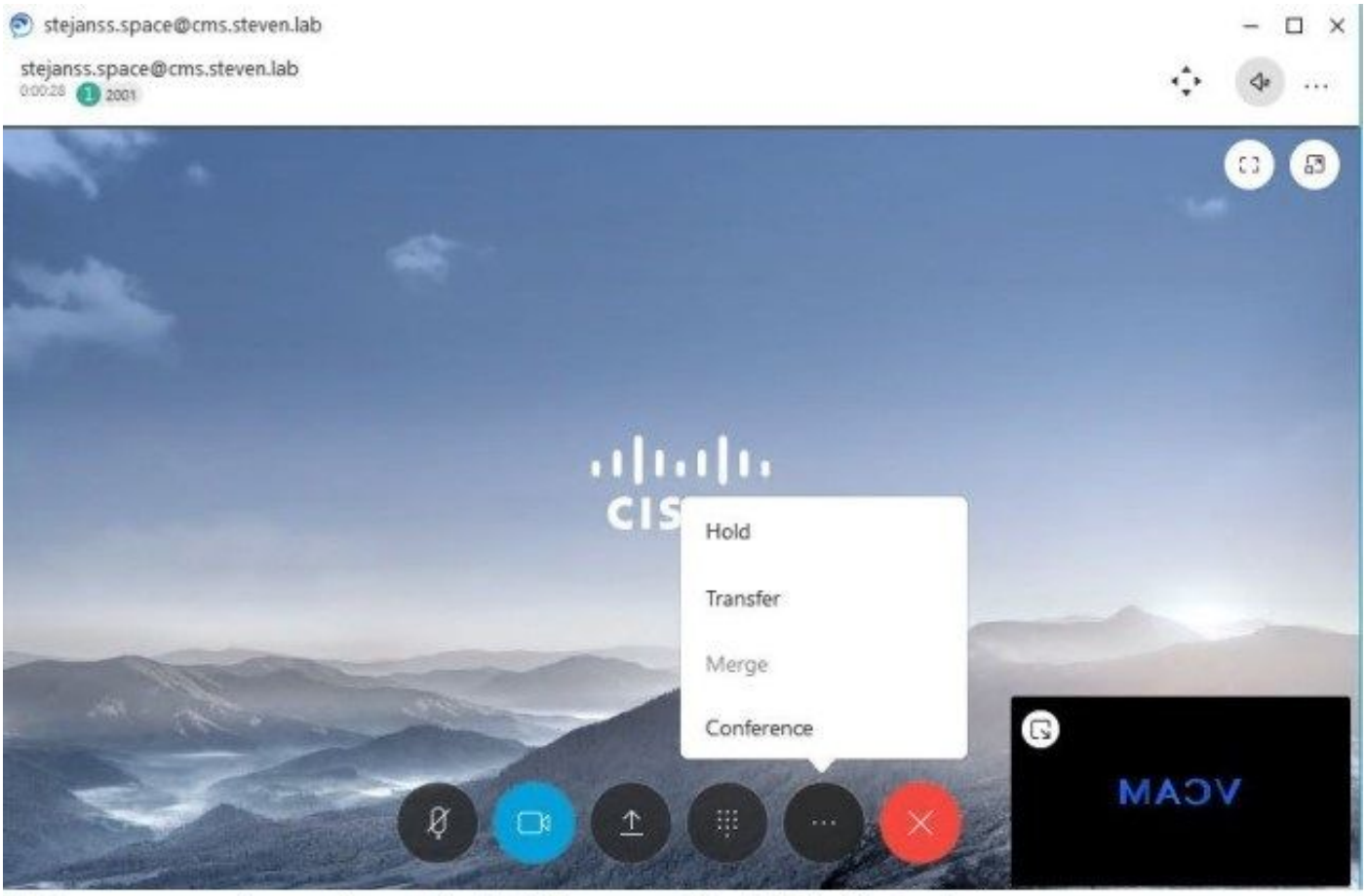
- 엔드포인트 - CUCM - Expressway-C - Expressway-E - Webex Meeting
- MRA 엔드포인트 - (Expressway-E - Expressway-C) - CUCM - Expressway-C - Expressway-E - Webex Meeting

  참고: Webex Meetings에서 지원하는 ActiveControl의 기능은 현재 CMS의 기능과 다르며 제한된 하위 집합에 불과합니다.

Cisco Meeting Server 플랫폼은 회의 참가자에게 외부 애플리케이션 또는 운영자가 필요 없이 ActiveControl을 통해 회의 엔드포인트에서 직접 회의 환경을 제어할 수 있는 기능을 제공합니다. ActiveControl은 Cisco 디바이스에서 iX 미디어 프로토콜을 사용하며 통화의 SIP 메시징의 일부로 협상됩니다. CMS 버전 2.5부터 사용되는 주요 기능은 다음과 같습니다(엔드포인트 유형 및 사용 중인 소프트웨어 버전에 따라 다를 수 있음).

- 미팅에 연결된 모든 참가자 목록(명부 목록 또는 참가자 목록) 보기
- 다른 참가자 음소거 또는 음소거 해제
- 미팅에서 다른 참가자 추가 또는 제거
- 모임 녹음/녹화 시작 또는 중지
- 참가자의 중요도
- 미팅에서 현재 발언자인 참가자의 표시자입니다.
- 현재 모임에서 콘텐츠 또는 프레젠테이션을 공유하고 있는 참가자의 표시기입니다.
- 모임 잠금 또는 잠금 해제

첫 번째 이미지에서는 ActiveControl이 없는 CMS 공간에 전화를 건 Jabber 클라이언트의 사용자 보기가 표시되고, 두 번째 이미지에서는 Jabber가 CMS 서버와 ActiveControl을 협상할 수 있는 기능이 더 풍부한 사용자 보기가 표시됩니다.



Jabber user experience when calling to CMS space without ActiveControl

Jabber user experience when calling to CMS space with ActiveControl

ActiveControl은 SIP(Session Initiation Protocol) 호출의 SDP(Session Description Protocol)에서 협상되는 iX 프로토콜을 사용하여 전송되는 XML 기반 프로토콜입니다. Cisco 프로토콜(eXtensible Conference Control Protocol(XCCP))이며 SIP에서만 협상합니다(따라서 연동된 통화에는 ActiveControl이 없음). 데이터 전송을 위해 UDP/UDT(UDP 기반 Data Transfer Protocol)를 활용합니다. DTLS(Datagram TLS)를 통해 보안 협상이 이루어집니다. DTLS는 UDP 연결을 통한 TLS로 간주할 수 있습니다. 협상의 차이에 대한 일부 샘플이 여기에 표시됩니다.

암호화되지 않음

m=application xxxxx UDP/UDT/IX *****
a=ixmap:11 **xccp**

암호화됨(최선형 - 암호화를 시도하지만 암호화되지 않은 연결로의 대체를 허용)

m=application xxxx UDP/UDT/IX *****

a=ixmap:2 **xccp**

a=**fingerprint**:sha-1 xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:

암호화(강제 암호화 - 암호화되지 않은 연결로의 대체를 허용하지 않음)

m=application xxxx UDP/**DTLS**/UDT/IX *****

a=ixmap:2 **xccp**

a=**fingerprint**:sha-1 xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:

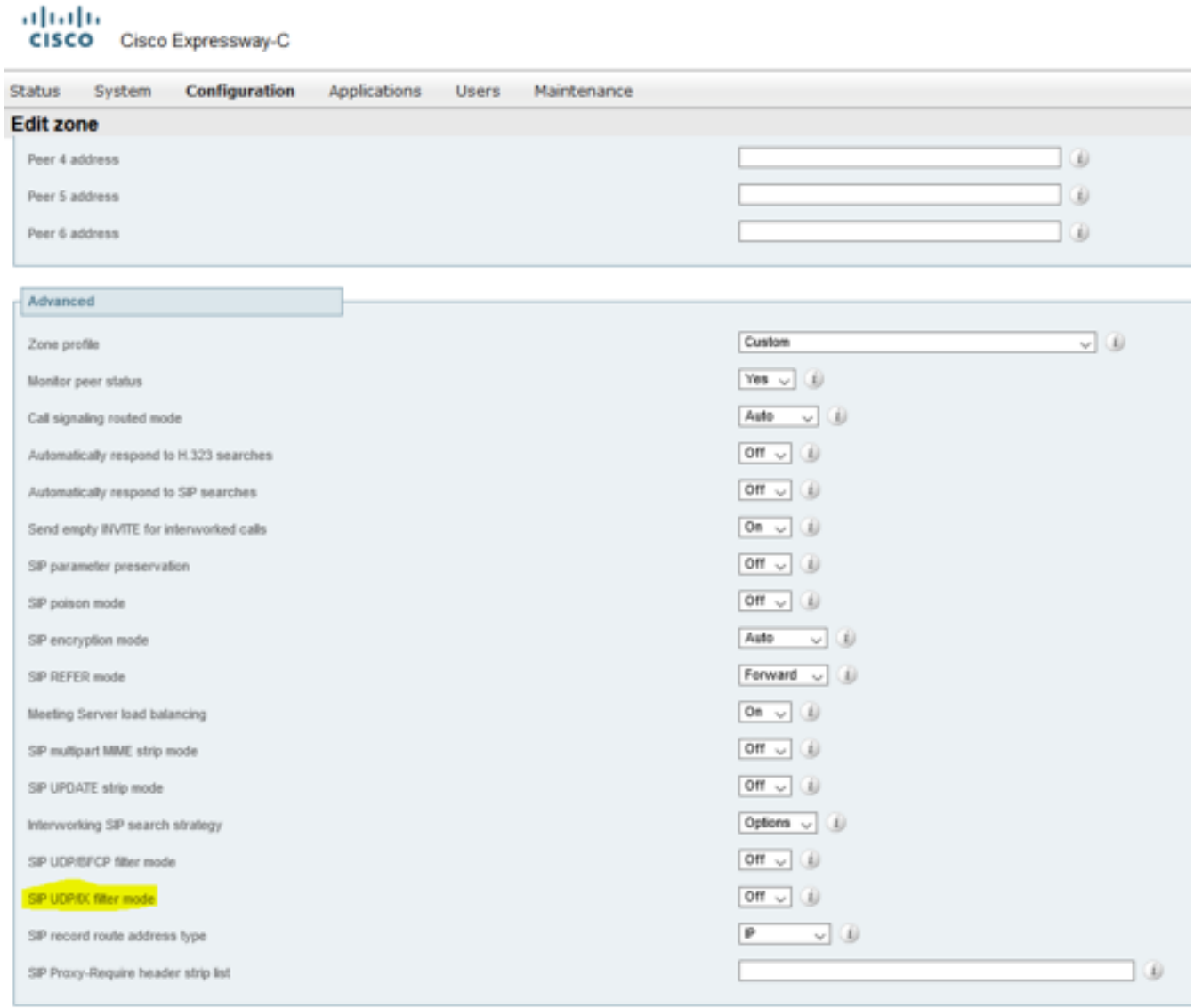
다음과 같이 전체 ActiveControl 지원에 필요한 몇 가지 최소 소프트웨어 버전이 있습니다.

- Jabber 버전 12.5 이상(릴리스 정보)
- CMS ActiveControl 가이드에 따라 CE 엔드포인트 8.3 이상, 9.6.2 이상 권장(Webex 도움말 링크에 따라 Webex의 경우 CE9.3.1 이상)
- CUCM 10.5 이상(Jabber 12.5 ActiveControl 지원)(11.5(1) 이상(Webex의 경우 링크 기준)
- CMS ActiveControl 가이드에 따라 CMS 2.1 이상, 2.5 이상 권장
- Expressway X12.5 이상(릴리스 노트)을 통해 암호화되지 않은 MRA 클라이언트 지원 가능

몇 가지 컨피그레이션 옵션을 고려해야 합니다.

- CUCM에서 관련 SIP 트렁크(Expressway-C 및 CMS)가 'Allow iX Application Media'(iX 애플리케이션 미디어 허용)가 선택된 SIP 프로필로 구성되어 있는지 확인합니다

- CMS에서는 기본적으로 2.1 이상에서 활성화되지만 sipUDT를 false로 설정할 수 있는 compatibilityProfile을 통해 비활성화할 수 있습니다
- Advanced(고급) 설정의 Zone(영역) 컨피그레이션에 있는 Expressway에서 'Custom(맞춤형)' 영역 프로필을 사용하는 경우 iX가 통과하도록 허용하려면 *SIP UDP/IX 필터 모드*가 'Off(해제)'로 설정되어 있는지 확인합니다



문제

일반 정보

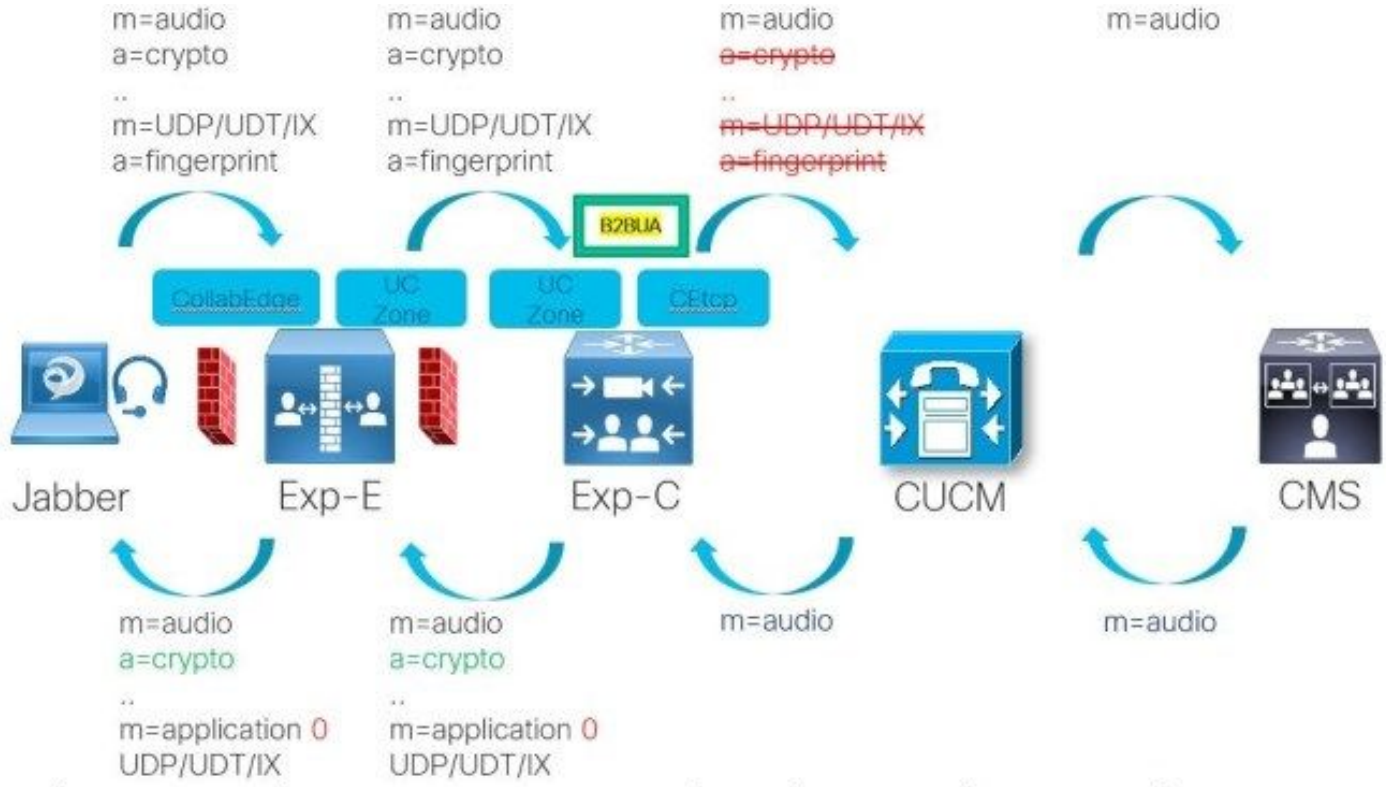
ActiveControl은 다른 미디어 채널과는 다르게 안전하게 협상되고 있습니다. 예를 들어 오디오 및 비디오와 같은 다른 미디어 채널의 경우 SDP에는 이 채널에 사용할 암호화 키를 원격지에 알리는 데 사용되는 암호화 줄이 추가됩니다. 따라서 RTP(Real-time Transport Protocol) 채널을 안전하게 만들 수 있으므로 SRTP(Secure RTP)로 간주할 수 있습니다. iX 채널의 경우 DTLS 프로토콜을 사용하여 XCCP 미디어 스트림을 암호화하므로 다른 메커니즘을 사용합니다.

Expressway 소프트웨어는 DTLS 프로토콜을 종료하지 않습니다. 이는 Expressway 릴리스 노트의 *Unsupported* Functionality(지원되지 않는 *기능) 아래*의 Limitations(제한) 섹션에 표시됩니다.

- Expressway does not terminate DTLS. We do not support DTLS for securing media and SRTP is used to secure calls. Attempts to make DTLS calls through Expressway will fail. The DTLS protocol is inserted in the SDP but only for traversing the encrypted iX protocol.

X12.5 이전 Expressway 버전

X12.5 이전의 Expressway 버전을 실행할 때, 안전하지 않은 TCP 영역을 따라 전달되는 암호화된 iX 채널을 사용하여 들어오는 연결이 있는 경우 Expressway는 일반 미디어 채널의 암호화 라인과 전체 iX 채널을 모두 분리합니다. MRA 클라이언트에서 Expressway-C로의 연결이 안전한 것을 확인할 수 있는 CMS 공간에 연결된 MRA 클라이언트에 대해 시각적으로 표시됩니다. 그런 다음 디바이스의 CUCM에 설정된 전화기 보안 프로파일에 따라 암호화되지 않은(그리고 CEtcp 영역을 통해 전송된) 상태이거나 암호화되어(그리고 CEtls 영역을 통해 전송된) 상태입니다. 이미지에 표시된 대로 암호화되지 않은 경우 Expressway-C가 모든 미디어 채널의 암호화 회선을 제거하고 DTLS 프로토콜을 종료할 수 없으므로 전체 iX 미디어 채널도 제거하는 것을 볼 수 있습니다. 이는 CEtcp 영역에 대한 영역 컨피그레이션이 미디어 암호화 'Force unencrypted'로 설정되어 있기 때문에 B2BUA(Back-To-Back User Agent)를 통해 발생합니다. SDP 회신을 수신할 때 반대 방향으로(미디어 암호화 '강제 적용'을 사용하는 UC 접근 영역을 통해) SDP는 일반 미디어 라인에 대한 암호화 라인을 추가하고 iX 채널에 대한 포트를 0으로 설정하여 ActiveControl 협상을 수행하지 않습니다. 내부적으로 클라이언트가 CUCM에 직접 등록되면 CUCM이 미디어 경로에 자신을 넣지 않으므로 암호화된 iX 미디어 채널과 암호화되지 않은 iX 미디어 채널을 모두 허용합니다.



Media negotiation when using Expressway versions lower than X12.5 and CEtcp SIP trunk

Expressway를 통한 통화 연결과 Webex Meetings에 동일한 종류의 논리가 적용됩니다. Expressway 서버(X12.5 이전)가 DTLS 연결 정보만 전달하지만 자체 종료하지 않고 새 세션을 시작하거나 다른 호출 레그에 있는 미디어 채널을 암호화/암호 해독하므로 전체 경로가 안전하게 끝나야 합니다.

X12.5 이상의 Expressway 버전

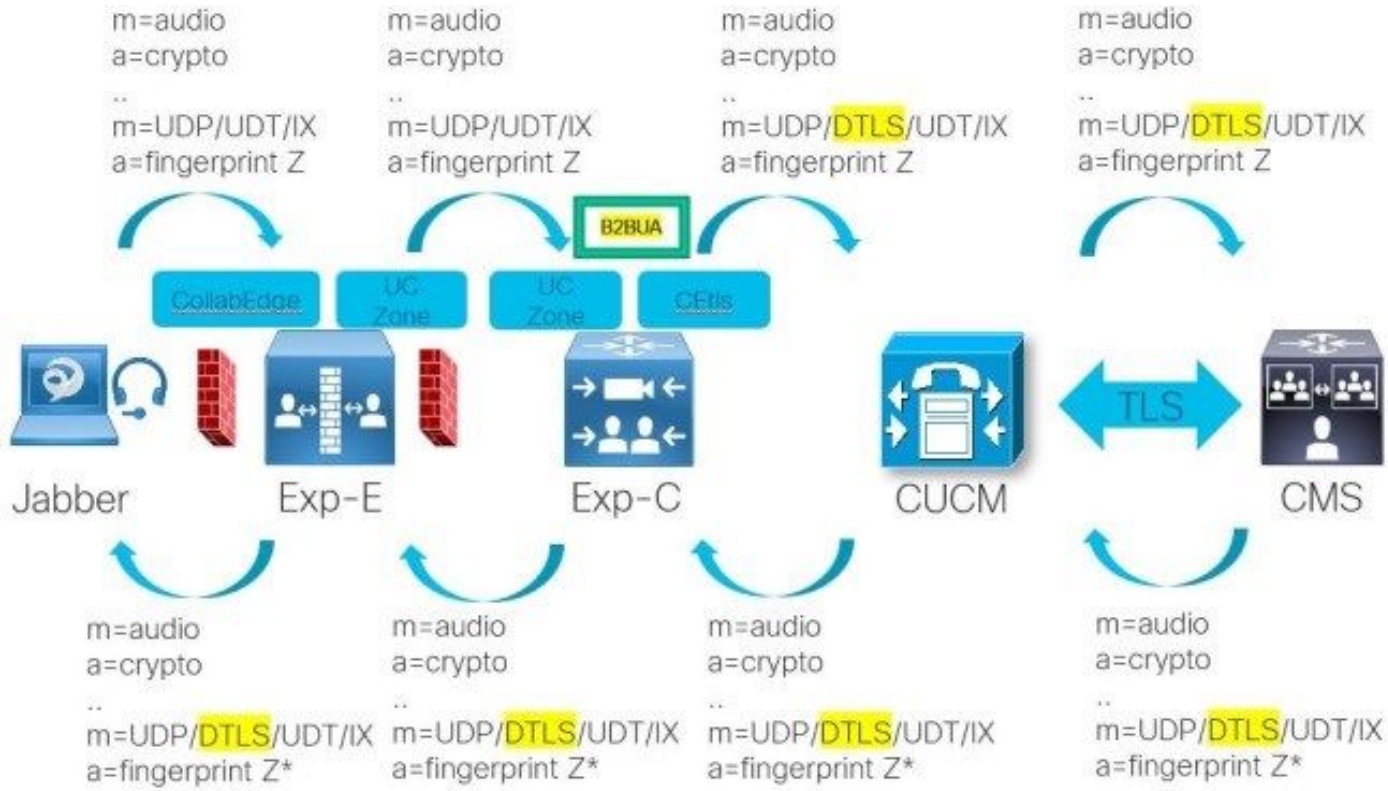
Expressway 버전 X12.5 이상을 실행하는 경우, iX 채널을 계속 협상할 수 있도록 TCP 영역 연결을 통해 강제 암호화(UDP/DTLS/UDT/IX)로 iX 채널을 전달하는 것과 마찬가지로 원격 끝에서도 암호화를 사용하는 경우에만 동작이 변경되었습니다. Expressway는 DTLS 세션을 종료하지 않고 패스스루에서만 작동하므로 암호화를 시행하므로 원격 끝점에서 DTLS 세션을 시작/종료합니다. 암호화 라인은 보안을 위해 TCP 연결을 통해 제거됩니다. 이러한 동작 변경은 'MRA: Support for Encrypted iX (for ActiveControl)' 섹션에 나와 있는 릴리스 노트에서 다룹니다. 그 후 발생하는 사항은 CUCM 버전에 따라 달라집니다. 12.5(1)SU1에서 해당 동작이 변경되어 iX 채널뿐만 아니라 안전하지 않은 수신 연결에서도 전달할 수 있게 되었습니다. CMS에 보안 TLS SIP 트렁크가 있는 경우에도 12.5(1)SU1 미만의 CUCM 버전을 실행할 경우 iX 채널을 제거한 후 CMS로 전달하므로 결국 CUCM에서 Expressway-C로 포트가 0으로 출력됩니다.

MRA: Support for Encrypted iX (for ActiveControl)

ActiveControl over MRA is already supported with encrypted phone profiles. This feature will allow MRA video endpoints and Jabber clients with non-secure phone security profiles to negotiate ActiveControl so that users can see roster lists, layouts, and other iX-dependent ActiveControl features in video meetings.

There are no configuration or interface changes for this feature. However, you may need to rediscover your Cisco Unified Communications Manager servers after you upgrade the Expressway.

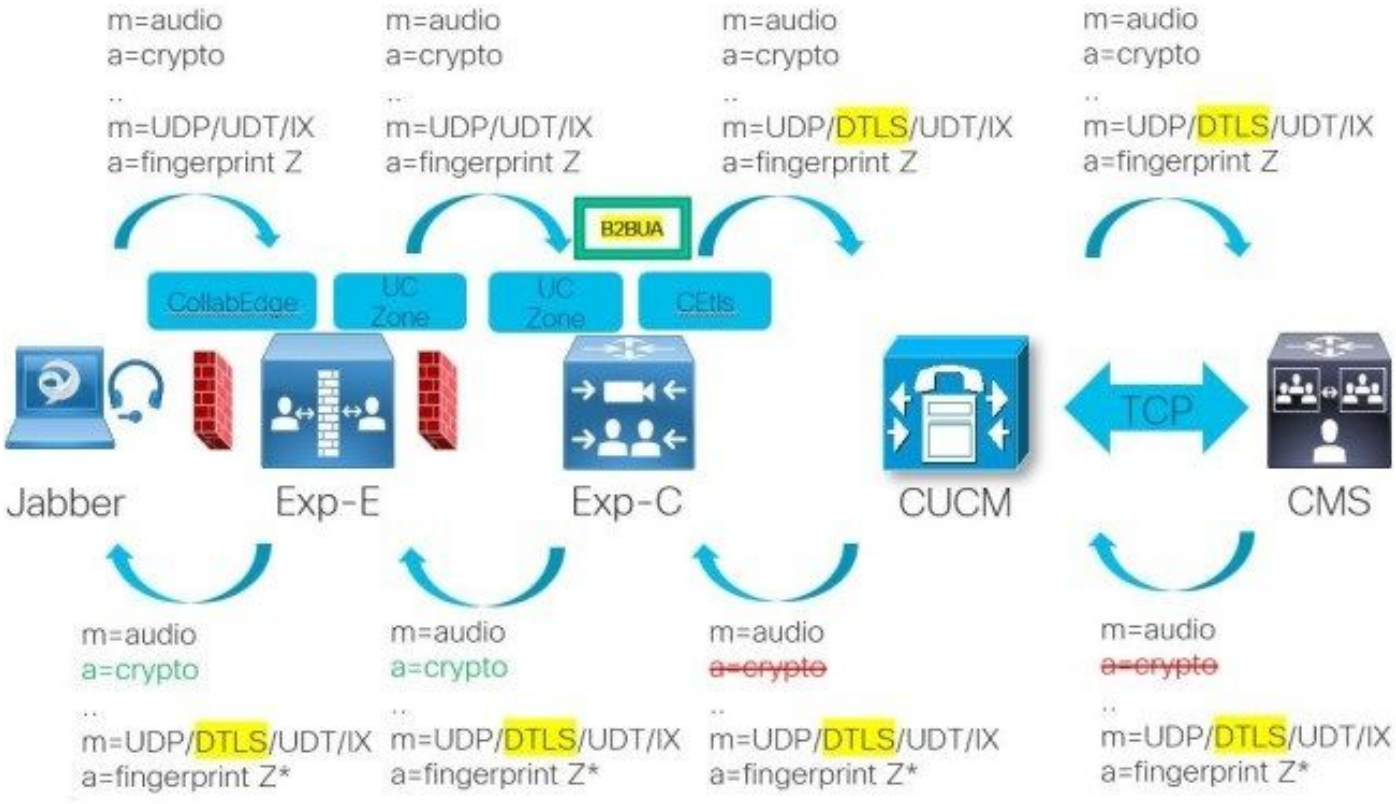
엔드 투 엔드 보안 통화 시그널링 및 미디어 경로를 통해 iX 채널을 (MRA) 클라이언트와 컨퍼런싱 솔루션(CMS 또는 Webex Meeting) 간에 직접 협상(Expressway 서버의 다른 홉을 통해 전달)할 수 있습니다. 이 그림에서는 CMS 공간에 연결된 MRA 클라이언트의 동일한 통화 흐름을 보여 주지만, 이제 CUCM에 보안 전화기 보안 프로파일이 구성되어 있고 CMS에 보안 TLS SIP 트렁크가 구성되어 있습니다. 경로가 엔드 투 엔드 보안 상태이며 DTLS 핑거프린트 매개변수가 전체 경로를 따라 방금 전달되었음을 확인할 수 있습니다.



Media negotiation when using Expressway and CEtls SIP trunk with TLS SIP trunk to CMS

보안 디바이스 보안 프로필을 설정하려면 혼합 모드에서 CUCM을 설정해야 하며, 이는 번거로운 프로세스일 수 있습니다(또한 보안 온프레미스 커뮤니케이션을 위해 CAPF(Certificate Authority Proxy Function)가 필요하기 때문에 작동할 때도 있음). 따라서 이 문서에서 다루는 대로 MRA 및 Expressway에 대한 ActiveControl의 일반적인 가용성을 지원하기 위해 여기에서 보다 편리한 다른 솔루션을 제공할 수 있습니다.

CMS 서버에 대한 보안 TLS SIP 트렁크는 필요하지 않습니다. CUCM(SIP 트렁크에 SRTP 허용 옵션이 설정되어 있다고 가정)이 항상 iX 채널 및 암호화 회선의 수신 보안 SIP 연결에서 전달되지만 CMS는 iX 채널에 대한 암호화(ActiveControl의 경우 허용)로 다시 응답합니다(SIP **미디어 암호화**가 CMS에서 [설정] > [통화 설정]에서 *허용되거나* 강제 적용되도록 설정되어 있다고 가정**). 그러나 이 미지에 따라** 암호화 회선을 제거하기 때문에 다른 미디어 채널에 대한 암호화가 없습니다**.** Expressway 서버는 연결의 해당 부분을 계속 보호하기 위해 암호화 회선에 다시 추가할 수 있지만(iX는 여전히 DTLS를 통해 최종 클라이언트 간에 직접 협상됨), 이는 보안 관점에서 이상적이지 않으므로 컨퍼런스 브리지에 보안 SIP 트렁크를 설정하는 것이 좋습니다. SIP **트렁크**에서 SRTP Allowed(SRTP 허용)를 선택하지 않으면 CUCM이 암호화 회선을 제거하고 보안 iX 협상도 실패합니다.



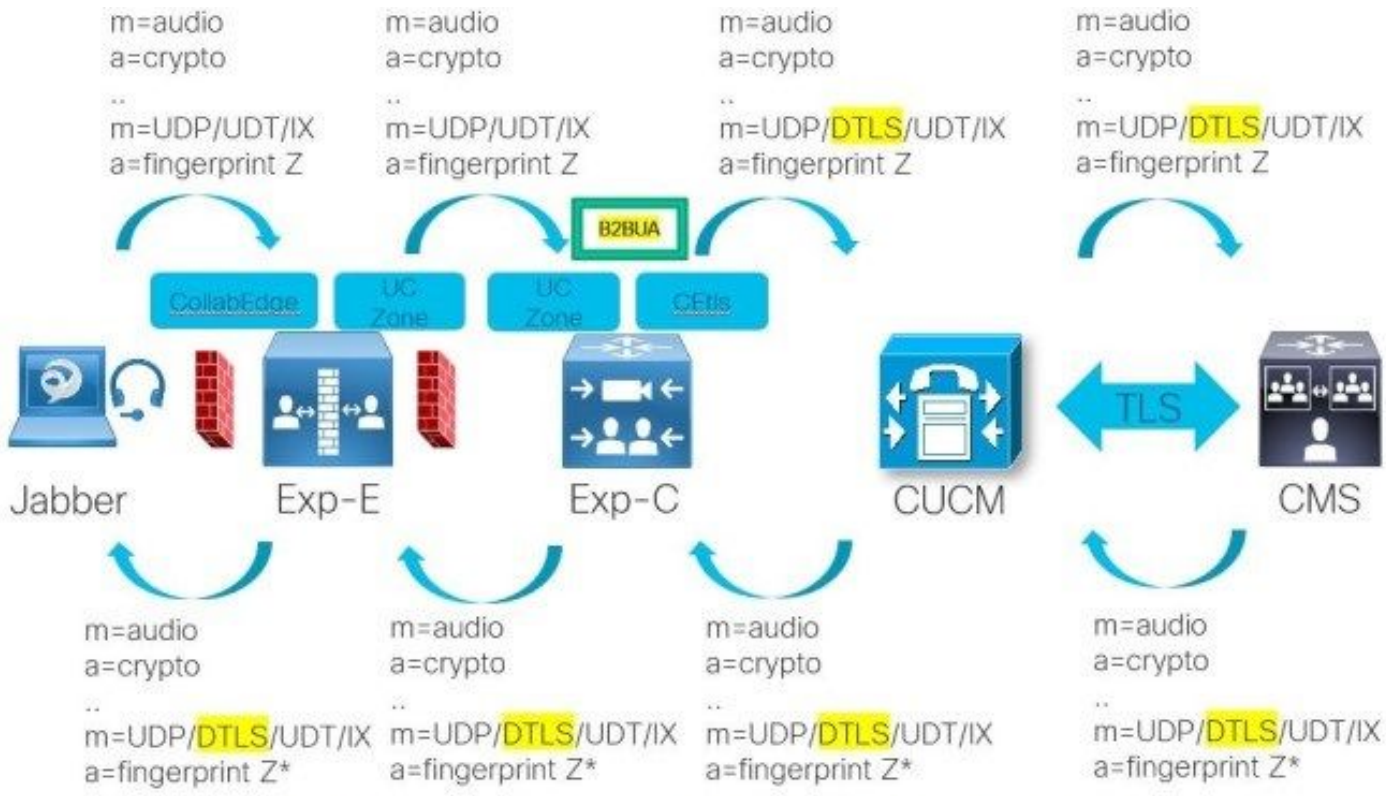
Media negotiation when using Expressway and CEtls SIP trunk with TCP SIP trunk to CMS

솔루션

다양한 요구 사항 및 다양한 찬성과 반대 의견으로 사용 가능한 몇 가지 다른 옵션이 있습니다. 각각의 내용은 좀 더 상세한 단원에 제시되어 있다. 다른 옵션은 다음과 같습니다.

1. 엔드포인트용 보안 전화기 보안 프로파일(혼합 모드 CUCM)
2. Jabber용 SIP OAuth
3. 안전하지 않은 전화 보안 프로필을 위한 암호화된 iX 채널(CUCM 12.5(1)SU1 이상)

솔루션 1: 엔드포인트용 보안 전화 보안 프로파일(혼합 모드 CUCM)



Media negotiation when using Expressway and CEtls SIP trunk with TLS SIP trunk to CMS

사전 요구 사항:

- 혼합 모드의 CUCM

프로:

- 모든 CUCM 버전에서 작동
- 모든 클라이언트 장치에서 작동

단언:

- 혼합 모드에서 CUCM 구성 필요(및 온프레미스 엔드포인트에서 CAPF 작업 필요)

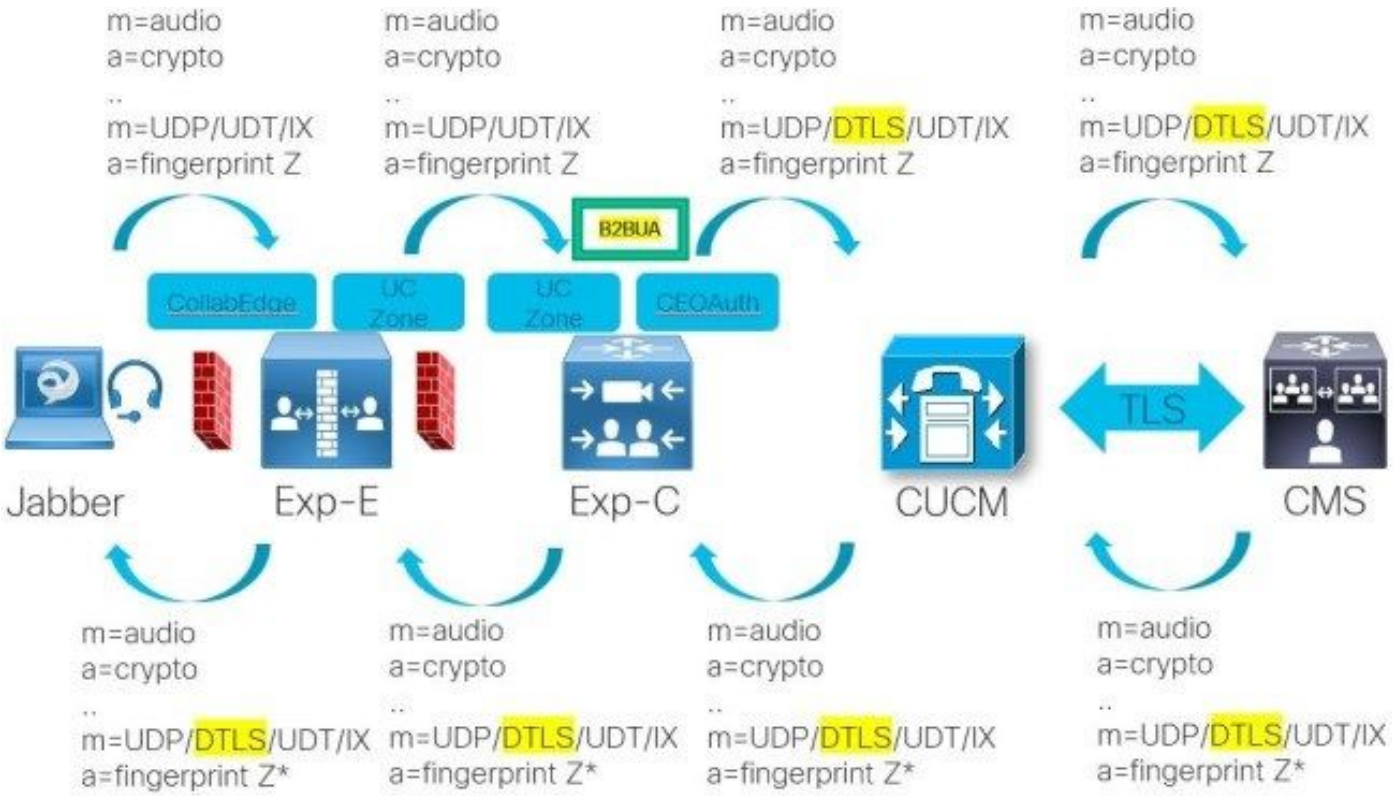
이 방법은 Problem(문제) 섹션에서 다루는 방법이며, 엔드 투 엔드 암호화 통화 신호 및 미디어 경로가 있는지 확인하는 끝에도 적용됩니다. 다음 문서에 따라 CUCM을 혼합 모드로 설정해야 합니다.

MRA 클라이언트의 경우 CAPF 작업이 필요하지 않지만 Collaboration Edge TC 기반 엔드포인트 컨피그레이션 예에서 강조 표시된 대로 Expressway-C 서버 인증서의 주체 대체 이름 중 하나와 일치하는 이름을 가진 보안 전화 보안 프로필을 사용하여 추가 컨피그레이션 단계를 수행해야 합니다(CE 기반 엔드포인트 및 Jabber 클라이언트에도 적용됨).

온프레미스 엔드포인트 또는 Jabber 클라이언트에서 Webex Meeting에 연결할 때 CAPF 작업을 수행하여 클라이언트를 CUCM에 안전하게 등록해야 합니다. 이는 Expressway가 DTLS 협상을 통과하고 직접 처리할 수 없는 엔드 투 엔드 보안 통화 흐름을 보장하기 위해 필요합니다.

통화를 엔드 투 엔드 보안을 유지하려면 모든 관련 SIP 트렁크(Webex Meeting 통화의 경우 Expressway-C로, CMS 컨퍼런스 통화의 경우 CMS로)가 보안 SIP 트렁크 보안 프로필과 함께 TLS를 사용하는 보안 SIP 트렁크인지 확인합니다.

솔루션 2: Jabber용 SIP OAuth



Media negotiation when using Expressway and CEOAuth SIP trunk with TLS SIP trunk to CMS

사전 요구 사항:

- Cisco Jabber 12.5 이상(릴리스 정보)
- OAuth(Refresh *Login Flow*)가 활성화된 CUCM 버전 12.5 이상(*릴리스 정보*)
- Expressway X12.5.1 이상(릴리스 정보) - 새로 고침*이 활성화된 OAuth 토큰으로* 권한 부여

프로:

- 매번 갱신 CAPF 없이 온프레미스 및 오프프레미스 간 보안 등록 및 손쉬운 전환 가능
- 혼합 모드에서 CUCM을 설정할 필요가 없음

단언:

- Jabber에만 해당되며 TC/CE 엔드포인트에는 해당되지 않음

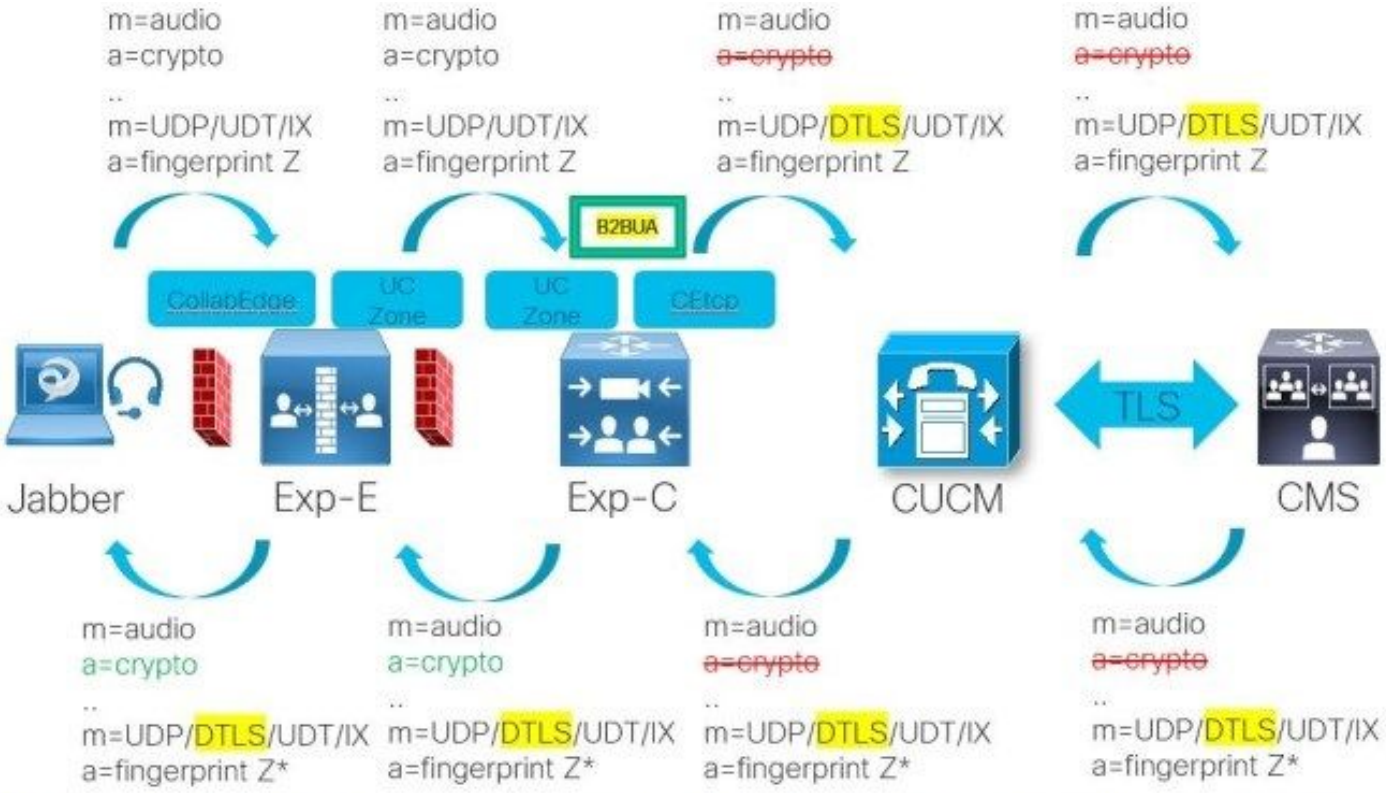
SIP OAuth 모드에서는 보안 환경에서 Cisco Jabber 인증에 OAuth 새로 고침 토큰을 사용할 수 있습니다. 솔루션 1의 CAPF 요구 사항 없이 안전한 신호 처리 및 미디어를 지원합니다. CUCM 클러스터 및 Jabber 엔드포인트에서 OAuth 기반 권한 부여가 활성화된 경우 SIP 등록 중에 토큰 검증이 완료됩니다.

CUCM의 컨피그레이션은 기능 컨피그레이션 가이드에 설명되어 있으며 Enterprise Parameters(엔터프라이즈 매개변수)에서 OAuth with Refresh Login Flow(새로 고침 로그인 플로우 포함)가 이미 활성화되어 있어야 합니다. MRA에서도 이를 활성화하려면 Expressway-C 서버의 Configuration(구성) > Unified Communication(Unified **통신) > Unified CM Servers(Unified CM 서버)**에서 CUCM 노드를 새로 고쳐야 합니다. 그러면 Configuration(**구성) > Zones(영역) > Zones(영역)**에서 이제 자동으로 생성된 CEOAuth 영역도 볼 수 있습니다. 또한 Configuration(컨피그레이션) **> Unified Communication(유니파이드 커뮤니케이션) > Configuration(컨피그레이션)**에서 Authorize **by OAuth token with refresh(새로 고침**으로 OAuth 토큰에 **의해** 권한 부여가 활성화되었는지 확인합니다.

이 컨피그레이션을 사용하면 신호 및 미디어에 대해 유사한 엔드 투 엔드 보안 통화 연결을 얻을 수 있으므로 Expressway는 해당 트래픽 자체를 종료하지 않으므로 DTLS 협상을 통해 전달하기만 합니다. 이는 이전 솔루션과 비교할 때 유일한 차이점이 CUCM이 보안 전화기 보안 프로필과 혼합 모

드에서 작동할 때 TLS를 통한 보안 디바이스 등록이 아닌 SIP OAuth를 사용하므로 CEtls 영역이 아니라 Expressway-C에서 CUCM으로 CEOAuth 영역을 사용하는 것이 CEtls 영역과 비교했을 때의 차이점이며, 이 점을 제외하면 모두 동일하게 유지됩니다.

솔루션 3: 안전하지 않은 전화 보안 프로필을 위한 암호화된 iX 채널(CUCM 12.5(1)SU1 이상)



Media negotiation when using Expressway on version higher than X12.5 and CEtcp SIP trunk to CUCM running a version of 12.5(1)SU1 or higher and a TLS SIP trunk to CMS

사전 요구 사항:

- CUCM 버전 12.5(1)SU1 이상(릴리스 정보)
- Expressway X12.5.1 이상(릴리스 정보)

프로:

- 혼합 모드에서 CUCM을 설정할 필요가 없음
- 안전한 엔드 투 엔드 통신을 설정할 필요가 없음
- Jabber 및 TC/CE 엔드포인트 모두에 적용 가능

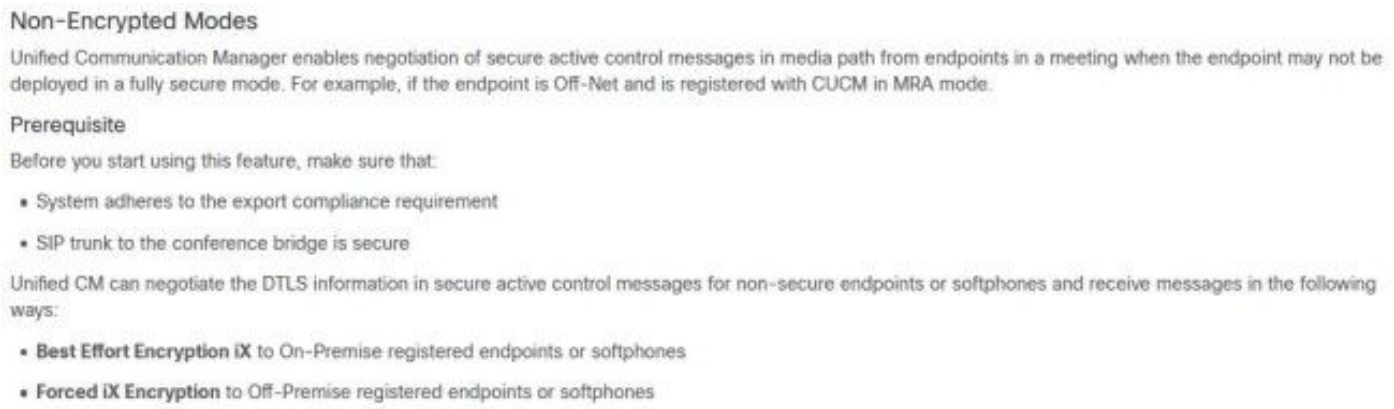
단언:

- CUCM 업그레이드 필요
- CUCM 제한 버전만 지원됩니다.

CUCM 12.5(1)SU1에서 모든 SIP 회선 디바이스에 대해 iX 암호화 협상을 지원하므로, 비보안 엔드포인트 또는 소프트폰에 대해 보안 ActiveControl 메시지에서 DTLS 정보를 협상할 수 있습니다. TCP를 통해 최선형 iX 암호화를 전송하므로 CUCM에 대한 비보안 TCP 연결(TLS가 아님)에도 불구하고 전화기에서 암호화된 iX 채널을 종단 간에 유지할 수 있습니다.

'Encrypted iX Channel' 섹션 아래의 CUCM 12.5(1)SU1의 보안 가이드에서는 시스템이 수출 규정을 준수하고 컨퍼런스 브리지에 대한 SIP 트렁크가 안전하다는 전제 조건으로 비보안 디바이스의

비암호화 모드, 최선형 및 강제 iX 암호화를 협상할 수 있음을 보여줍니다.



Non-Encrypted Modes

Unified Communication Manager enables negotiation of secure active control messages in media path from endpoints in a meeting when the endpoint may not be deployed in a fully secure mode. For example, if the endpoint is Off-Net and is registered with CUCM in MRA mode.

Prerequisite

Before you start using this feature, make sure that:

- System adheres to the export compliance requirement
- SIP trunk to the conference bridge is secure

Unified CM can negotiate the DTLS information in secure active control messages for non-secure endpoints or softphones and receive messages in the following ways:

- **Best Effort Encryption iX** to On-Premise registered endpoints or softphones
- **Forced iX Encryption** to Off-Premise registered endpoints or softphones

CUCM의 경우:

- Export restricted CUCM(제한 없음)을 사용해야 합니다.
- **System > Licensing > License Management**에서 "Export-Controlled Functionality"를 allowed로 설정해야 합니다.
- SIP 트렁크에는 "SRTP **Allowed**" 옵션이 활성화되어 있어야 합니다(트렁크 자체가 안전한지 안전하지 않은지 여부와 관계 없음).

CMS:

- callbridge에는 암호화가 포함된 라이센스가 있어야 합니다(따라서 callBridgeNoEncryption 라이센스가 없음).
- webadmin의 Configuration(**구성) > Call Settings(통화 설정)** 아래에서 **SIP 미디어 암호화**를 **allowed**(또는 **required)로** 설정해야 합니다.

이미지에서 Expressway-C가 SDP를 통해 암호화 회선 없이 CUCM으로 전송할 때까지 연결이 보호됨을 확인할 수 있지만 iX 미디어 채널은 여전히 포함되어 있습니다. 따라서 오디오/비디오/.. 의 일반 미디어는 암호화 회선으로 보호되지 않지만 iX 미디어 채널에 대한 보안 연결이 설정되어 있으므로 Expressway에서 DTLS 연결을 종료할 필요가 없습니다. 따라서 ActiveControl은 안전하지 않은 전화 보안 프로필을 사용하더라도 클라이언트와 컨퍼런스 브리지 간에 직접 협상할 수 있습니다. 이전 버전의 CUCM에서는 흐름이 달라지고 ActiveControl이 협상되지 않습니다. iX 채널을 통해 CMS로 전달되지 않기 때문입니다. 해당 부분이 이미 제거되었기 때문입니다.

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.