CUCM과 VCS 또는 Expressway 컨피그레이션 간의 보안 RTP 예시

목차

소개

이 문서에서는 Cisco VCS(Video Communication Server)와 Cisco CUCM(Unified Communication Manager) 간에 안전한 RTP(Real-time Transport Protocol)를 설정하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- CUCM

- Cisco VCS 또는 Cisco Expressway

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- CUCM
- Cisco VCS 또는 Cisco Expressway

  참고:이 문서에서는 Cisco Expressway 제품을 설명(언급된 경우는 제외)하기 위해 사용하지만, 구축에서 Cisco VCS를 사용하는 경우에도 이 정보가 적용됩니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

조건

- CUCM과 Expressway 간에 라우팅된 SIP(Session Initiation Protocol) 통화
- 미디어 암호화는 Expressway-C와 CUCM 간의 최선형/선택 사항입니다.

설명

CUCM과 VCS/Expressway 간에 라우팅되는 SIP 통화에 대해 최선형 미디어 암호화를 구성하는 데 문제가 보고되었습니다.일반적인 잘못된 컨피그레이션은 SRTP(Secure Real-time Transport Protocol)를 통해 암호화된 미디어의 시그널링에 영향을 미치며, 이는 CUCM과 Expressway 간의 전송이 안전하지 않을 때 최선형 암호화 통화의 실패를 유발합니다.

전송이 안전하지 않은 경우 미디어 암호화 신호를 엿듣는 사람이 읽을 수 있습니다.이 경우 SDP(Session Description Protocol)에서 미디어 암호화 신호 정보가 제거됩니다. 그러나 비보안 연결을 통해 미디어 암호화 신호 신호를 전송(수신)하도록 CUCM을 구성할 수 있습니다.이 잘못된 컨피그레이션은 통화가 트렁크 쪽 또는 CUCM에 대한 회선 측에 따라 두 가지 방법 중 하나로 해결할 수 있습니다.

트렁크측 및 라인측 예

트렁크 쪽:SIP 트렁크는 CUCM에서 Expressway로 구성됩니다.해당 네이버 영역은 Expressway to CUCM에 구성됩니다.VCS 등록(Expressway는 등록자가 아니지만 VCS는 등록됨) 엔드포인트에서 CUCM 등록 엔드포인트를 호출하려면 트렁크가 필요합니다.또 다른 예는 구축에서 H.323 상호 작용을 활성화하는 것입니다.

회선 쪽:회선 측 통화는 트렁크가 아닌 CUCM으로 직접 이동합니다.CUCM에서 모든 등록 및 통화 제어를 제공하는 경우 Expressway에 트렁크가 필요하지 않을 수 있습니다.예를 들어, Expressway가 모바일 및 원격 액세스(MRA)에 대해서만 구축된 경우 외부 엔드포인트에서

CUCM으로 회선 측 통화를 프록시합니다.

완화 전략

CUCM과 Expressway 사이에 SIP 트렁크가 있는 경우 CUCM의 표준화 스크립트는 SDP를 적절하게 재작성하여 최선형 암호화 통화가 거부되지 않도록 합니다.이 스크립트는 CUCM의 이후 릴리스와 함께 자동으로 설치되지만 최선형 암호화 호출이 거부된 경우, 사용자의 CUCM 버전에 대한 최신 vcs-interop 스크립트를 다운로드하여 설치하는 것이 좋습니다.

통화가 CUCM의 라인 쪽으로 이동하면 미디어 암호화가 선택 사항인 경우 CUCM은 `x-cisco-srtp-fallback` 헤더를 볼 수 있습니다.CUCM에 이 헤더가 표시되지 않으면 이 통화는 암호화 필수로 간주됩니다.버전 X8.2에서 이 헤더에 대한 지원이 Expressway에 추가되었으므로 Cisco에서는 MRA(협업 에지)에 X8.2 이상을 권장합니다.

구성

라인측 컨피그레이션

[CUCM]<—best-effort—>[Expressway-C]<—필수—>[Expressway-E]<—필수—>[엔드포인트]

Expressway-C에서 CUCM에 대한 회선 측 통화의 최선 암호화를 활성화하려면 다음을 수행합니다.

- 지원되는 구축/솔루션 사용(예: MRA)
- CUCM에서 혼합 모드 보안 사용
- Expressway와 CUCM이 상호 신뢰(각 상대방의 인증서를 서명하는 CA(Certificate Authority)를 상대방으로부터 신뢰해야 함)
- Expressway 버전 X8.2 이상 사용
- Device Security Mode(디바이스 보안 모드)가 Authenticated(인증) 또는 Encrypted(암호화됨)로 설정된 CUCM에서 보안 전화기 프로파일을 사용합니다. 이러한 모드의 경우 전송 유형은 TLS(Transport Layer Security)입니다.

트렁크측 컨피그레이션

- 지원되는 구축/솔루션 사용
- CUCM에서 혼합 모드 보안 사용
- Expressway와 CUCM이 서로 신뢰하는지 확인합니다(각 상대방의 인증서를 서명하는 CA는 상대방으로부터 신뢰받아야 함).
- Expressway에서 CUCM으로 인접 영역의 전송으로 암호화 모드로 TLS를 선택하는 것이 좋습니다(이러한 값은 라인 측 케이스에 자동으로 미리 입력됨).
- SIP 트렁크 보안 프로필의 인바운드 및 아웃바운드 전송으로 TLS를 선택합니다.
- CUCM에서 Expressway로 SIP 트렁크의 SRTP Allowed(SRTP 허용) 확인(주의 문 참조)
- CUCM 및 Expressway 버전의 올바른 표준화 스크립트를 확인하고 필요한 경우 적용합니다.

주의:SRTP Allowed(SRTP 허용) 확인란을 선택하면 통화 협상 중에 키 및 기타 보안 관련 정보가 노출되지 않도록 암호화된 TLS 프로파일을 사용하는 것이 좋습니다.비보안 프로필을 사용하는 경우 SRTP는 계속 작동합니다.그러나 키는 신호 및 추적에 노출됩니다.이 경우

CUCM과 트렁크의 목적지 측 간의 네트워크 보안을 확인해야 합니다.

미디어 암호화 옵션

없음

암호화는 허용되지 않습니다.암호화가 필요한 통화는 보안될 수 없으므로 실패해야 합니다 .CUCM과 Expressway는 이 케이스에 대한 시그널링에서 일관됩니다.

CUCM과 Expressway 모두 `m=RTP/AVP`를 사용하여 SDP의 미디어를 설명합니다.SDP의 미디어 섹션에 암호화 특성(`no a=crypto...` 줄 없음)이 없습니다.

필수

미디어 암호화가 필요합니다.암호화되지 않은 통화는 항상 실패해야 합니다.대체가 허용되지 않습니다.CUCM과 Expressway는 이 케이스에 대한 시그널링에서 일관됩니다.

CUCM과 Expressway 모두 `m=RTP/SAVP`를 사용하여 SDP의 미디어를 설명합니다.SDP에는 암호화 특성(`a=crypto..` SDP의 미디어 섹션에 있는 행)이 있습니다.

최선의 노력

암호화할 수 있는 통화는 암호화됩니다.암호화를 설정할 수 없는 경우 통화가 암호화되지 않은 미디어로 반환될 수 있습니다.이 경우 CUCM과 Expressway가 일치하지 않습니다.

전송이 TCP(Transmission Control Protocol) 또는 UDP(User Datagram Protocol)인 경우 Expressway는 항상 암호화를 거부합니다. 미디어 암호화를 원하는 경우 CUCM과 Expressway 간의 전송을 보호해야 합니다.

SDP(CUCM에서 기록하는 대로):암호화된 미디어는 `m=RTP/SAVP`로 설명되고 `a=crypto` 라인은 SDP에 기록됩니다.이는 미디어 암호화를 위한 올바른 신호이지만 전송 보안이 안전하지 않을 경우 암호화 라인을 읽을 수 있습니다.

CUCM에 `x-cisco-srtp-fallback` 헤더가 표시되면 통화를 암호화되지 않은 상태로 되돌릴 수 있습니다.이 헤더가 없는 경우 CUCM은 통화에 암호화가 필요하다고 가정합니다(대체를 허용하지 않음).

X8.2부터 Expressway는 CUCM이 라인 측 케이스에서 하는 것과 동일한 방식으로 최선의 노력을 다합니다.

SDP(Expressway에서 트렁크 쪽에 쓰기):암호화된 미디어는 `m=RTP/AVP`로 설명되고 `a=crypto` 라인은 SDP에 기록됩니다.

그러나 a=crypto 라인이 없는 이유는 두 가지가 있습니다.

1. Expressway의 SIP 프록시와의 전송 홉이 안전하지 않을 경우 프록시는 비보안 홉의 노출을 방지하기 위해 암호화 라인을 분리합니다.
2. 자동 응답자가 암호화를 수행할 수 없거나 수행하지 않을 것임을 알리기 위해 암호화 회선을

제거합니다.
CUCM에서 올바른 SIP 정규화 스크립트를 사용하면 이 문제가 완화됩니다.

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

관련 정보

관련 읽기

- Cisco Unified Communications Manager 보안 가이드, 릴리스 10.0(1)
- Optimized Conferencing for Cisco Unified Communications Manager and Cisco VCS Solution Guide(릴리스 2.0)
- Cisco Expressway(SIP 트렁크)를 사용하는 Cisco Unified Communications Manager 구축 설명서(Cisco Expressway X8.2 및 Unified CM 8.6x 및 9.x용)
- Cisco Unified Communications Manager with Cisco VCS(SIP Trunk) 구축 설명서(Cisco VCS X8.2 및 Unified CM 8.6.x 및 9.x용)
- Cisco VCS를 통한 Unified Communications Mobile 및 Remote Access 구축 설명서(Cisco VCS X8.2 및 Cisco Unified CM 9.1(2)SU1 이상)
- Cisco Expressway 구축 가이드를 통한 Unified Communications Mobile and Remote Access(Cisco Expressway X8.2 및 Cisco Unified CM 9.1(2)SU1 이상)
- 기술 지원 및 문서 – Cisco Systems

관련 RFC

- RFC 3261 SIP:세션 시작 프로토콜
- RFC 4566 SDP:세션 설명 프로토콜
- RFC 4568 SDP:보안 설명