Secure RTP tussen CUCM en VCS of voorbeeld voor configuratie van snelwegen

Inhoud

Inleiding

Dit document beschrijft hoe u een beveiligd Real-time Transport Protocol (RTP) kunt instellen tussen de Cisco Video Communication Server (VCS) en Cisco Unified Communications Manager (CUCM).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- CUCM
- Cisco VCS of Cisco-snelweg

Gebruikte componenten

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

- CUCM
- Cisco VCS of Cisco-snelweg

  Opmerking: Dit artikel gebruikt de producten van de Uitdrukbaan van Cisco voor uitleg (behalve waar vermeld), maar de informatie is ook van toepassing als uw plaatsing de VCS van Cisco gebruikt.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

Voorwaarden

- Session Initiation Protocol (SIP)-gesprekken tussen CUCM en Express
- Media-encryptie is de best-inspanning / optioneel tussen Expressway-C en CUCM

Beschrijving

Er zijn problemen gemeld voor de configuratie van best-energie media-encryptie voor SIP-oproepen die tussen CUCM en VCS/Expressway worden verzonden. Een veel voorkomende fout-configuratie heeft invloed op het signaleren van versleutelde media via Secure Real-time Transport Protocol (SRTP), wat een storing veroorzaakt van best-inspanning versleutelde oproepen wanneer het transport tussen CUCM en Expressway niet veilig is.

Als het transport niet veilig is, kan het media encryptie-signaal worden gelezen door een luisteraar. In dit geval wordt de informatie over mediaconcentratie-signalering verwijderd uit het Session Description Protocol (SDP). Het is echter mogelijk om CUCM te configureren dat u media-encryptie-signalering via een onbeveiligde verbinding wilt verzenden (en verwachten te ontvangen). Je kunt op één of twee manieren rond deze wanconfiguratie werken, afhankelijk van of de oproepen aan de achterkant van de romp of aan de kant van de lijn aan CUCM worden gestuurd.

Voorbeelden van trunks en lijnen

Kant: Een SIP-romp is op CUCM in de richting van expresse ingesteld. Een corresponderende buurzone wordt ingesteld op de snelweg naar CUCM. U hebt een romp nodig als u VCS-

Geregistreerd (Expressway is geen registrator, maar VCS is) endpoints om CUCM-geregistreerde endpoints te bellen. Een ander voorbeeld zou zijn om H.323 interworking in uw plaatsing mogelijk te maken.

Lijnzijde: De lijn-zij vraag gaat rechtstreeks naar CUCM, niet via een boomstam. Als alle registratie en Call controle door CUCM wordt verstrekt, zou uw plaatsing geen boomstam aan Expressway kunnen nodig hebben. Bijvoorbeeld, als Expressway puur voor Mobile en Remote Access (MRA) wordt ingezet, volgt deze de line-side gesprekken van externe endpoints naar CUCM.

Beperkingsstrategie

Als er een SIP-romp is tussen CUCM en Expressway, schrijft een normalisatie-script op CUCM de SDP correct opnieuw zodat de best-inspanning coderingsoproep niet wordt afgewezen. Dit script wordt automatisch geïnstalleerd met latere releases van CUCM, maar als u gecodeerde oproepen van het best-inspanning hebt verworpen, raadt Cisco u aan het laatste vcs-interpop script voor uw versie van CUCM te downloaden en te installeren.

Als het gesprek van line naar CUCM gaat, verwacht CUCM de `x-cisco-srtp-back-`header te zien als de mediaconcentratie optioneel is. Als CUCM deze header niet ziet, is de oproep verplicht tot codering. Ondersteuning van deze header is toegevoegd aan Expressway in versie X8.2, dus Cisco raadt X8.2 aan of hoger voor MRA (samenwerkingsrand).

Configureren

Configuratie aan één kant

[CUCM]<—best-inspanning—>[Expressway-C]<—verplicht—>[Expressway-E]<—verplicht—>[Endpoint]

Zo maakt u een optimaal gebruik van encryptie van line-side gesprekken van Expressway-C naar CUCM:

- Gebruik een ondersteunde toepassing / oplossing (bijvoorbeeld MRA)
- Beveiliging in gemengde modus gebruiken op CUCM
- Zorg ervoor dat Expressway en CUCM elkaar vertrouwen (de certificaatautoriteit (CA) die de certificaten van elke partij teken moet worden vertrouwd door de andere partij)
- Gebruik versie X8.2 of hoger van Expresway
- Gebruik beveiligde telefoonprofielen op CUCM, waarbij de apparaatbeveiligingsmodus is ingesteld op Verificeerd of Versleuteld - voor deze modi is het transporttype Transport Layer Security (TLS)

Configuratie met Trunk-zijde

- Gebruik een ondersteunde toepassing / oplossing
- Beveiliging in gemengde modus gebruiken op CUCM
- Zorg ervoor dat Expressway en CUCM elkaar vertrouwen (CA die de certificaten van elke partij teken moet worden vertrouwd door de andere partij)

- Kies de beste inspanning als encryptiemodus en TLS als het transport op de buurzone van Expressway naar CUCM (deze waarden worden automatisch voorbevolkt in de line-side case)
- Selecteer TLS als het inkomende en uitgaande transport op het SIP-stam veiligheidsprofiel
- Controleer SRTP toegestaan (zie de waarschuwing) op de SIP-stam van CUCM naar Express
- Controleer op, en pas indien nodig het juiste normalisatie script toe voor uw versies van CUCM en Expressway

Voorzichtig: Als u het vakje SRTP Toegestaan aanvinkt, raadt Cisco sterk aan dat u een versleuteld TLS-profiel gebruikt zodat de toetsen en andere security-gerelateerde informatie niet worden blootgesteld tijdens Call onderhandelingen. Als u een niet-beveiligd profiel gebruikt, zal SRTP nog steeds werken. De toetsen worden echter blootgesteld aan signalering en sporen. In dat geval, moet u de veiligheid van het netwerk tussen CUCM en de bestemmingskant van de boomstam verzekeren.

Opties voor mediaconcentratie

None

Encryptie is niet toegestaan. Roepingen die encryptie vereisen zouden moeten mislukken omdat zij niet veilig kunnen zijn. CUCM en Expressway zijn consistent in het signaleren voor deze case.

CUCM en Expressway gebruiken `m=RTP/AVP` om de media in de SDP te beschrijven. Er zijn geen cryptoeigenschappen (geen `a=crypto...` lijnen in de media secties van de SDP).

Verplicht

Media-encryptie is vereist. Niet-gecodeerde oproepen moeten altijd falen; een reserve is niet toegestaan . CUCM en Expressway zijn consistent in het signaleren voor deze case.

CUCM en Expressway gebruiken beide `m=RTP/SAVP` om de media in de SDP te beschrijven. De SDP heeft crypto eigenschappen (`a=crypto...` lijnen in de media secties van de SDP).

Beste inspanning

De oproepen die kunnen worden versleuteld zijn versleuteld. Als encryptie niet kan worden vastgesteld, zou de vraag kunnen en moeten terugvallen op niet gecodeerde media. CUCM en Expressway zijn in dit geval niet consistent.

Express weigert altijd encryptie als het transport Transmission Control Protocol (TCP) of User Datagram Protocol (UDP) is. U moet het transport tussen CUCM en Expressway beveiligen als u media-encryptie wilt.

SDP (zoals CUCM schrijft): Versleutelde media worden beschreven als `m=RTP/SAVP` en `a=crypto`-lijnen worden in de SDP geschreven. Dit is de juiste signalering voor mediaconcentratie, maar de cryptoverbindingen zijn leesbaar als het transport niet veilig is.

Als CUCM de `x-cisco-srtp-back` header ziet, kan deze worden teruggestuurd naar niet-versleuteld.

Als deze header ontbreekt, wordt met CUCM aangenomen dat er een codering nodig is (dit staat geen back-up toe).

Sinds X8.2 doet Expressway het best zoals CUCM dat doet in het line-side geval.

SDP (zoals Expressway schrijft boomkant): Versleutelde media worden beschreven als `m=RTP/AVP` en `a=crypto`-lijnen worden naar de SDP geschreven.

Er zijn echter twee redenen dat de a=crypto lijnen afwezig zouden kunnen zijn:

1. Wanneer een transportwop naar of van de SIP-proxy op de expressweg niet veilig is, stript de proxy de crypto-lijnen om te voorkomen dat deze op de onveilige hop blootstaan.
2. De antwoordende partij schrapt de crypto lijnen om te signaleren dat het geen encryptie kan of zal doen.

Het gebruik van het juiste SIP-normalisatie-script op CUCM vermindert dit probleem.

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Gerelateerde informatie

Verwante tekst

- Cisco Unified Communications Manager security handleiding, release 10.0(1)
- Geoptimaliseerde conferencing voor Cisco Unified Communications Manager en Cisco VCS Solution Guide (release 2.0)
- Cisco Unified Communications Manager met implementatiegids van Cisco Express (SIP Trunk) (voor Cisco Express X8.2 en Unified CM 8.6x en 9.x)
- Cisco Unified Communications Manager met Cisco VCS (SIP Trunk)-implementatiegids (voor Cisco VCS X8.2 en Unified CM 8.6.x en 9.x)
- Unified Communications mobiele en externe toegang via de Cisco VCS-implementatiegids (voor Cisco VCS X8.2 en Cisco Unified CM 9.1(2)SU1 of hoger)
- Unified Communications mobiele en externe toegang via de Cisco-implementatiegids voor snelwegen van Cisco X8.2 en Cisco Unified CM 9.1(2)SU1 of hoger)
- Technische ondersteuning en documentatie – Cisco Systems

Verwante RFC's

- RFC 3261 SIP: Session Initiation-protocol

- RFC 4566 SDP: Session Description Protocol
- RFC 4568 SDP: Security beschrijvingen