Konfigurationsbeispiel für sicheres RTP zwischen CUCM und VCS oder Expressway

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie ein sicheres Real-Time Transport Protocol (RTP) zwischen dem Cisco Video Communication Server (VCS) und Cisco Unified Communication Manager (CUCM) einrichten.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- CUCM
- Cisco VCS oder Cisco Expressway

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- CUCM
- Cisco VCS oder Cisco Expressway

  Hinweis: In diesem Artikel werden die Cisco Expressway-Produkte zur Erläuterung verwendet (sofern nicht anders angegeben). Die Informationen gelten jedoch auch, wenn bei Ihrer Bereitstellung das Cisco VCS verwendet wird.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Hintergrundinformationen

Bedingungen

- SIP-Anrufe (Session Initiation Protocol) zwischen CUCM und Expressway
- Medienverschlüsselung ist bestmöglich/optional zwischen Expressway-C und CUCM

Beschreibung

Es wurden Schwierigkeiten bei der Konfiguration der bestmöglichen Medienverschlüsselung für SIP-Anrufe gemeldet, die zwischen CUCM und VCS/Expressway geroutet werden. Eine häufig vorkommende Fehlkonfiguration wirkt sich auf die Signalisierung verschlüsselter Medien über Secure Real-time Transport Protocol (SRTP) aus, was zum Ausfall von verschlüsselten Best-Effort-Anrufen führt, wenn die Übertragung zwischen CUCM und Expressway nicht sicher ist.

Wenn die Übertragung nicht sicher ist, kann die Medienverschlüsselungssignalisierung von einem Abhörer gelesen werden. In diesem Fall werden die Signalisierungsinformationen zur Medienverschlüsselung aus dem Session Description Protocol (SDP) entfernt. Es ist jedoch möglich, CUCM so zu konfigurieren, dass Medienverschlüsselungssignalisierung über eine ungesicherte Verbindung gesendet (und empfangen wird) wird. Sie können diese Fehlkonfiguration auf zwei Arten umgehen, je nachdem, ob es sich um geroutete Trunk-seitige oder leitungsseitige Anrufe zum CUCM handelt.

Beispiele für Trunk- und Leitungssysteme

Trunk-seitig: Ein SIP-Trunk wird auf dem CUCM zu Expressway konfiguriert. Auf dem Expressway

zum CUCM wird eine entsprechende Nachbarzone konfiguriert. Sie benötigen einen Trunk, wenn Sie VCS-registrierte Endpunkte (Expressway ist kein Registrar, aber VCS ist) für den Anruf von CUCM-registrierten Endpunkten benötigen. Ein weiteres Beispiel wäre die Aktivierung der H.323-Interworking-Funktion in Ihrer Bereitstellung.

Leitungsseitig: Leitungsseitige Anrufe werden direkt an den CUCM weitergeleitet, nicht über einen Trunk. Wenn alle Registrierungs- und Anrufsteuerungsfunktionen vom CUCM bereitgestellt werden, ist für Ihre Bereitstellung möglicherweise kein Trunk zu Expressway erforderlich. Wenn beispielsweise Expressway ausschließlich für den mobilen und Remote-Zugriff (MRA) bereitgestellt wird, werden die leitungsseitigen Anrufe von externen Endpunkten an den CUCM weitergeleitet.

Eindämmungsstrategie

Wenn ein SIP-Trunk zwischen CUCM und Expressway vorhanden ist, wird das SDP von einem Normalisierungs-Skript im CUCM entsprechend umgeschrieben, sodass der Best-Effort-Verschlüsselungsaufruf nicht abgelehnt wird. Dieses Skript wird automatisch zusammen mit späteren Versionen von CUCM installiert. Wenn Sie jedoch bestmögliche verschlüsselte Anrufe zurückgewiesen haben, empfiehlt Cisco, das neueste VCS-Interop-Skript für Ihre CUCM-Version herunterzuladen und zu installieren.

Wenn der Anruf an die Leitung zum CUCM weitergeleitet wird, erwartet CUCM, dass der `x-cisco-srtp-Fallback-`Header angezeigt wird, wenn die Medienverschlüsselung optional ist. Wenn der CUCM diesen Header nicht sieht, wird der Anruf als verschlüsselt betrachtet. Die Unterstützung für diesen Header wurde Expressway in Version X8.2 hinzugefügt. Cisco empfiehlt daher X8.2 oder höher für MRA (Collaboration Edge).

Konfiguration

Leitungsseitige Konfiguration

[CUCM]<—Best Effort—>[Expressway-C]<—obligatorisch—>[Expressway-E]<—obligatorisch—>[Endpunkt]

So aktivieren Sie die bestmögliche Verschlüsselung von leitungsseitigen Anrufen von Expressway-C zum CUCM:

- Verwendung einer unterstützten Bereitstellung/Lösung (z. B. MRA)
- Sicherheit im gemischten Modus für CUCM verwenden
- Stellen Sie sicher, dass Expressway und CUCM einander vertrauen (die Zertifizierungsstelle (Certificate Authority, CA), die die Zertifikate der einzelnen Parteien unterzeichnet, muss von der anderen Partei als vertrauenswürdig gelten).
- Expressway-Version X8.2 oder höher verwenden
- Verwenden Sie sichere Telefonprofile auf dem CUCM, wobei der Gerätesicherheitsmodus auf "Authenticated" (Authentifiziert) oder "Encrypted" (Verschlüsselt) gesetzt ist. Bei diesen Modi lautet der Transporttyp "Transport Layer Security (TLS)".

Trunk-seitige Konfiguration

- Unterstützte Bereitstellung/Lösung
- Sicherheit im gemischten Modus für CUCM verwenden
- Stellen Sie sicher, dass Expressway und CUCM einander vertrauen (die Zertifizierungsstelle, die die Zertifikate der einzelnen Parteien unterzeichnet, muss von der anderen Partei als vertrauenswürdig gelten).
- Wählen Sie Best Effort als Verschlüsselungsmodus und TLS als Transport im Nachbarbereich von Expressway zum CUCM aus (diese Werte werden automatisch im leitungsseitigen Fall vorab eingetragen).
- Wählen Sie TLS als Eingangs- und Ausgangs-Transport im SIP-Trunk-Sicherheitsprofil aus.
- Überprüfung der zulässigen SRTP-Verbindungen (siehe die "Caution"-Anweisung) auf dem SIP-Trunk vom CUCM zum Expressway
- Suchen Sie nach dem richtigen Normalisierungs-Skript für Ihre Versionen von CUCM und Expressway, und wenden Sie es ggf. an.

> **Vorsicht:** Wenn Sie das Kontrollkästchen SRTP Allowed (Zulässige SRTP-Protokolle) aktivieren, empfiehlt Cisco die Verwendung eines verschlüsselten TLS-Profils, damit Schlüssel und andere sicherheitsrelevante Informationen bei Anrufverhandlungen nicht verfügbar gemacht werden. Wenn Sie ein nicht sicheres Profil verwenden, funktioniert SRTP weiterhin. Die Schlüssel werden jedoch in Signalisierung und Traces verfügbar gemacht. In diesem Fall müssen Sie die Sicherheit des Netzwerks zwischen dem CUCM und der Zielseite des Trunks sicherstellen.

Medienverschlüsselungsoptionen

Keine

Die Verschlüsselung ist nicht zulässig. Anrufe, die verschlüsselt werden müssen, sollten fehlschlagen, da sie nicht sicher sind. CUCM und Expressway sind in diesem Fall konsistent in der Signalisierung.

CUCM und Expressway verwenden beide `m=RTP/AVP`, um die Medien im SDP zu beschreiben. Es gibt keine Kryptoattribute (no `a=crypto...` Zeilen in den Medienabschnitten des SDP).

Mandatory (Obligatorisch)

Eine Medienverschlüsselung ist erforderlich. Unverschlüsselte Anrufe sollten immer fehlschlagen. Es ist kein Fallback zulässig. CUCM und Expressway sind in diesem Fall konsistent in der Signalisierung.

CUCM und Expressway verwenden beide `m=RTP/SAVP`, um die Medien im SDP zu beschreiben. Das SDP verfügt über Kryptoattribute (`a=crypto...` Zeilen in den Medienabschnitten des SDP).

Bester Aufwand

Anrufe, die verschlüsselt werden können, werden verschlüsselt. Wenn die Verschlüsselung nicht eingerichtet werden kann, können und sollten Anrufe auf unverschlüsselte Medien zurückfallen. CUCM und Expressway sind in diesem Fall inkonsistent.

Expressway verweigert immer die Verschlüsselung, wenn es sich bei dem Transport um Transmission Control Protocol (TCP) oder User Datagram Protocol (UDP) handelt. Wenn Sie Medienverschlüsselung benötigen, müssen Sie den Transport zwischen CUCM und Expressway sichern.

SDP (wie CUCM schreibt): Verschlüsselte Medien werden als `m=RTP/SAVP` beschrieben und `a=crypto` Zeilen werden in das SDP geschrieben. Dies ist die richtige Signalisierung für die Medienverschlüsselung, aber die Kryptozeilen sind lesbar, wenn die Übertragung nicht sicher ist.

Wenn der CUCM den `x-cisco-srtp-fallback`-Header sieht, kann der Anruf auf unverschlüsselt zurückfallen. Wenn dieser Header nicht vorhanden ist, geht CUCM davon aus, dass der Anruf verschlüsselt werden muss (ein Fallback ist nicht möglich).

Ab X8.2 arbeitet Expressway genauso wie CUCM im Line-Side-Fall.

SDP (wie Expressway auf Trunk-Seite schreibt): Verschlüsselte Medien werden als `m=RTP/AVP` und `a=crypto` Zeilen in das SDP geschrieben.

Es gibt jedoch zwei Gründe, warum die a=crypto-Zeilen fehlen könnten:

1. Wenn ein Transport-Hop zum oder vom SIP-Proxy auf dem Expressway nicht sicher ist, entfernt der Proxy die Krypto-Linien, um zu verhindern, dass diese auf dem unsicheren Hop verfügbar sind.
2. Der Anrufer entfernt die Kryptozeilen, um zu signalisieren, dass er keine Verschlüsselung durchführen kann oder will.

Durch die Verwendung des korrekten SIP-Normalisierungsskripts für CUCM wird dieses Problem behoben.

Überprüfung

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

Zugehörige Lektüre

- Cisco Unified Communications Manager Security Guide, Version 10.0(1)
- Optimierte Konferenzlösungen für Cisco Unified Communications Manager und Cisco VCS Lösungsleitfaden (Version 2.0)
- Implementierungsleitfaden für Cisco Unified Communications Manager mit Cisco Expressway (SIP-Trunk) (für Cisco Expressway X8.2 und Unified CM 8.6x und 9.x)
- Bereitstellungsleitfaden für Cisco Unified Communications Manager mit Cisco VCS (SIP-Trunk) (Für Cisco VCS X8.2 und Unified CM 8.6.x und 9.x)
- Unified Communications Mobile und Remote Access über Cisco VCS Implementierungsleitfaden (für Cisco VCS X8.2 und Cisco Unified CM 9.1(2)SU1 oder höher)
- Unified Communications Mobile und Remote Access über Cisco Expressway Deployment Guide (Für Cisco Expressway X8.2 und Cisco Unified CM 9.1(2)SU1 oder höher)
- Technischer Support und Dokumentation für Cisco Systeme

Zugehörige RFCs

- RFC 3261 SIP: Session Initiation Protocol
- RFC 4566 SDP: Session Description Protocol
- RFC 4568 SDP: Sicherheitsbeschreibungen