Beheben von SRTP-Entschlüsselungsfehlern und fehlendem Audio in WebEx Contact Center mit AudioCodes-SBC

Inhalt

Problem

Eingehende PSTN-Anrufe an einen Webex Contact Center-Tenant wurden erfolgreich verbunden, hatten aber keine Audioverbindung zwischen Anrufern und Agenten. Der Anruffluss betraf Anbieter A1 Austria über einen AudioCodes-SBC und eine Firewall zum WebEx Contact Center, wobei der Agentenanteil über denselben SBC an Microsoft Teams zurückgeleitet wurde. Sowohl auf der Eingangs-PSTN-Komponente als auch auf der Agentenkomponente fehlte der Ton, sodass die Mitarbeiter nicht mit Anrufern kommunizieren konnten. Dies wirkte sich auf die Anrufbearbeitung im Contact Center aus.

Medienstatistiken haben gezeigt, dass SRTP-Pakete an WebEx gesendet, aber nicht erfolgreich von der Cloud empfangen wurden. Die Analyse ergab folgende Fehlerbedingungen:

- Gesendete Pakete: 1557 (von SBC-Seite)
- Empfangene Pakete: 0
- Entschlüsselungsfehler: 1569
- Nicht vertrauenswürdiges RTP-Protokoll SRTP

SIP-/SDP-Samples zeigten auf jeder Seite unterschiedliche Kryptodeklarationen, wobei das SBC SDP mehrere a=crypto-Leitungen anbot, während Webex 200 OK SDP eine einzelne a=crypto ankündigte: Inline-Parameter AES_CM_128_HMAC_SHA1_80.

Umwelt

- Webex Contact Center-Tenant

- AudioCodes SBC (Mediant VE SBC/v.7.40A.501.392)
- Anbieter A1 Österreich PSTN-Verbindung
- Microsoft Teams für Agenteninfrastruktur
- Firewall zwischen SBC und WebEx Contact Center
- Anrufablauf: PSTN → Provider A1 Österreich → AudioCodes SBC → Firewall → WebEx Contact Center
- Agenten-Leg: WebEx Contact Center → Firewall → SBC → Microsoft Teams

Auflösung

Das Problem wurde durch die Anwendung spezifischer AudioCodes SBC-Mediensicherheitskonfigurationseinstellungen behoben, um die SRTP-Kryptografiefehler zwischen der SIP-Signalisierung und den vom SBC gesendeten Medien zu beheben.

Konfigurationsschritte

Wenden Sie die folgenden AudioCodes SBC-Mediensicherheitsparameter an:

Schritt 1: Konfigurieren der MKI-Größe für SBC erzwingen

Navigieren Sie zum Abschnitt Mediensicherheit, und stellen Sie die Größe des SBC zur Durchsetzung der MKI-Richtlinien ein.

Phase 2: Konfigurieren des SBC zum Entfernen der Verschlüsselungslebensdauer in SDP

SBC "Crypto Lifetime entfernen" in SDP auf Ja festlegen

Validierung

Nach der Übernahme dieser Einstellungen wurde die Audioübertragung für eingehende und ausgehende Anrufe wiederhergestellt. Durch die Testanrufe wurde der ordnungsgemäße Medienfluss zwischen Anrufern und Mitarbeitern über die WebEx Contact Center-Plattform bestätigt.

Fehlerbehebung - Analyse

Das Problem wurde durch Vergleichstests auf den PSTN/SBC-Pfad A1 Austria isoliert. Eine alternative Cloud-PSTN-Verbindung in derselben Organisation zeigte das Audioproblem nicht, und es wurde bestätigt, dass das Problem spezifisch für die AudioCodes-SBC-Konfiguration beim Anbieter A1 Austria war.

Die Paketerfassungs- und Medienstatistiken zeigten eindeutige Hinweise auf SRTP-Entschlüsselungsfehler mit folgenden SIP-/SDP-Aushandlungskonflikten:

SBC INVITE SDP (mit mehreren Verschlüsselungsoptionen):

```
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:WZMYswMS
a=crypto:2 AES_CM_128_HMAC_SHA1_32 inline:27NXBojL
a=crypto:3 AES_256_CM_HMAC_SHA1_80 inline:lWmcbjYR
a=crypto:4 AES_256_CM_HMAC_SHA1_32 inline:TXG/YY/d
```

WebEx 200 OK SDP (Auswahl einer einzelnen Verschlüsselung):

```
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:B3UfL3Ta
```

Ursache

Die Ursache war eine SRTP-Kryptoinkompetenz zwischen der SIP-Signalisierungsaushandlung und den tatsächlichen Medienverschlüsselungsschlüsseln, die vom AudioCodes-SBC verwendet wurden. Der SBC sendete SRTP-Pakete mit falschen Krypto-Schlüsseln, die nicht den vereinbarten Werten der SIP-Signalisierungszentrale entsprachen. Dies führte zu Entschlüsselungsfehlern auf Seiten des WebEx Contact Centers und verhinderte eine erfolgreiche Audiokommunikation trotz erfolgreicher Verbindungsaufbau.

Verwandte Inhalte

- Port-Referenzinformationen für Cisco WebEx Anrufe
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.