

Konfigurieren des SRTP-RTP-Interworking auf CUBE

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Zusätzlicher Service-Support](#)

[Konfigurationen](#)

[Überprüfung](#)

[Fehlerbehebung](#)

Einleitung

In diesem Dokument wird ein schrittweiser Prozess zur Konfiguration des SRTP-RTP Interworking für CUBE beschrieben.

Voraussetzungen

Anforderungen

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

- Cisco Unified Border Element (CUBE)
- Session Initiation Protocol (SIP)
- Transport Layer Security (TLS)
- Real-Time Transport Protocol (RTP)
- Secure Media - Secure Real-time Transport Protocol (SRTP)

Verwendete Komponenten

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

- Cisco Unified Border Element (CUBE)
- Cisco IOS XE - Version 17.6 und höher
- Cisco C8200-1N-4T

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 Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Die Funktion zur Unterstützung von SRTP-RTP-Interworking in Cisco Unified Border Element (CUBE) verbindet SRTP-Unternehmensdomänen mit SIP-Trunks von RTP-SIP-Anbietern. SRTP-RTP-Interworking verbindet RTP-Unternehmensnetzwerke mit SRTP über ein externes Netzwerk zwischen Unternehmen. Dadurch wird eine flexible, sichere Business-to-Business-Kommunikation ermöglicht, ohne dass statische IPsec-Tunnel erforderlich sind oder SRTP im Unternehmen bereitgestellt werden muss.

Wichtige Informationen zum SRTP-RTP-Interworking auf CUBE:

1. Verschlüsselung und Entschlüsselung: CUBE kann Datenströme von und zu SRTP- und RTP-Netzwerken verschlüsseln und entschlüsseln.
2. TLS-Unterstützung: Transport Layer Security (TLS) kann zwischen dem SCCP-Server und dem SCCP-Client aktiviert oder deaktiviert werden. Standardmäßig ist TLS aktiviert, um SRTP-Schlüssel zu schützen.
3. Ergänzende Dienste: In Cisco IOS Version 15.2(1) wurde die Funktion erweitert, um zusätzliche Dienste auf CUBE zu unterstützen.
4. Transkodierung: SRTP-RTP Internetworking ist für normale und universelle Transcoder verfügbar, die über SCCP-Messaging aufgerufen werden.
5. Fallback Handling (Handhabung von Fallbacks): Wenn einer der Anrufendpunkte SRTP nicht unterstützt, kann der Anruf auf RTP-RTP zurückgreifen oder fehlschlagen, je nach Konfiguration. Dieser Fallback tritt nur auf, wenn der SRTP-Fallback-Befehl auf dem entsprechenden DFÜ-Peer konfiguriert ist.
6. Bereitstellung: SRTP-RTP-Interworking kann auf Benutzer-zu-Netzwerk-Schnittstellen (UNI) und Netzwerk-zu-Netzwerk-Schnittstellen (NNI) bereitgestellt werden.

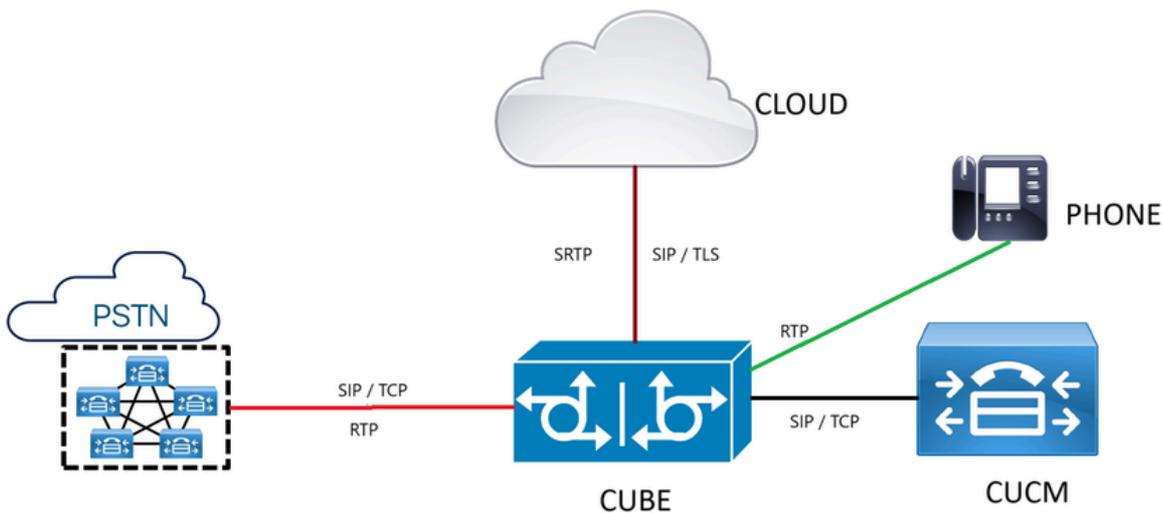


Anmerkung:

- Für Plattformen, die auf Cisco IOS-Versionen ausgeführt werden, sind DSP-Ressourcen erforderlich.
- Für Plattformen, die auf Cisco IOS XE-Versionen ausgeführt werden, sind keine DSP-Ressourcen erforderlich.

Konfigurieren

Netzwerkdiagramm



Zusätzlicher Service-Support

Unterstützt werden folgende Zusatzleistungen:

- Änderung des Mittleren Anrufcodecs mit Codec-Konfiguration der Sprachklasse
- Halten und Wiederaufnahmen von Anrufen auf Basis von Reinvite
- Warteschleifenmusik (Music on Hold, MoH), die vom Cisco Unified Communications Manager (Cisco UCM) aufgerufen wird, bei der sich der Anrufabschnitt zwischen SRTP und RTP für eine Quelle für Warteschleifenmusik ändert
- Weiterleiten und Weiterleiten von Anrufen auf Basis von Reinvite
- Anrufweiterleitung basierend auf einer REFER-Nachricht, mit lokaler Nutzung oder Weiterleitung der REFER-Nachricht auf dem CUBE
- Anrufweiterleitung basierend auf einer 302-Nachricht, mit lokaler Nutzung oder Weitergabe der 302-Nachricht auf dem CUBE
- T.38 Fax Switchover
- Fax-Passthrough-Switchover

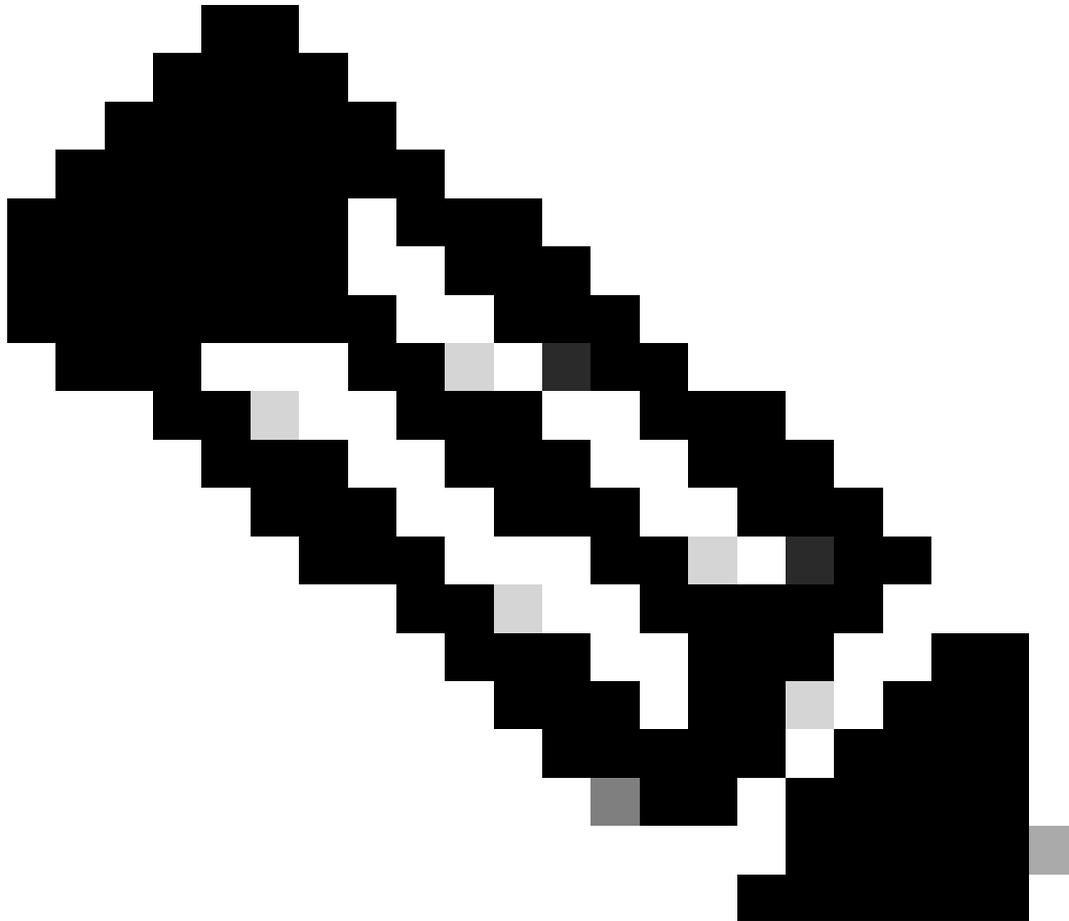
Bei Anrufübertragungen mit REFER- und 302-Nachrichten (Nachrichten, die lokal auf CUBE verbraucht werden) wird die End-to-End-Medienneuverhandlung von CUBE nur initiiert, wenn Sie den Befehl `additional-service media-renegotiate` im VoIP-Konfigurationsmodus für Sprachdienste konfigurieren.

Für jeden Anruffluss, bei dem auf demselben SIP-Anrufabschnitt ein Switchover von RTP zu SRTP stattfindet, muss der `medienneu` ausgehandelte Ergänzungsdienstbefehl im globalen Modus oder im VoIP-Konfigurationsmodus für Sprachdienste aktiviert werden, um sicherzustellen, dass Zweiwege-Audio zur Verfügung steht.

Beispiele für Anrufflüsse:

- RTP - SRTP-Übertragung auf CUCM-Seite
- Nicht sicheres Warteschleifenmusik wird während des sicheren Halten oder Fortsetzens von Anrufen wiedergegeben

Wenn von den Endpunkten aus zusätzliche Services aufgerufen werden, kann der Anruf während der Anrufdauer zwischen SRTP und RTP wechseln. Cisco empfiehlt daher, solche SIP-Trunks für das SRTP-Fallback zu konfigurieren.



Hinweis: Ab Cisco IOS XE Everest Version 16.5.1b sind diese Verschlüsselungs-Suites standardmäßig für die SRTP-Komponente aktiviert:

- AEAD_AES_256_GCM
- AEAD_AES_128_GCM
- AES_CM_128_HMAC_SHA1_80
- AES_CM_128_HMAC_SHA1_32

Konfigurationen

Schritt 1: Aktivieren Sie SRTP, und konfigurieren Sie Dial-Peer für die SRTP-Strecke: Dies ist die Strecke, für die SRTP erforderlich ist.

```
dial-peer voice <Tag> voip
```

Beschreibung Eingehender SRTP-DFÜ-Peer

```
destination-pattern <Muster>
```

Sitzungsprotokoll sipv2

```
session target ipv4:<SRTP-Peer-IP-Adresse>
```

Sprachklasse-Codec 1

SRTP

```
dtmf-relay rtp-nte
```

IP QoS DSCP CS3-Signalisierung

!

Schritt 2: Konfigurieren des Dial-Peer für den RTP-Abschnitt: Dies ist der Abschnitt, für den RTP erforderlich ist.

```
dial-peer voice <Tag> voip
```

description Ausgehender RTP-DFÜ-Peer

```
destination-pattern <Muster>
```

Sitzungsprotokoll sipv2

```
session target ipv4:<RTP-Peer-IP-Adresse>
```

Sprachklasse-Codec 1

```
dtmf-relay rtp-nte
```

IP QoS DSCP CS3-Signalisierung

!

Schritt 3: Krypto-Authentifizierung konfigurieren

Schritte zum Konfigurieren von CUBE zur Unterstützung einer SRTP-Verbindung mithilfe der AES_CM_128_HMAC_SHA1_80-Verschlüsselungs-Suite

- Konfiguration der DFÜ-Peer-Ebene

```
dial-peer voice <Tag> voip
```

Sprachklasse sip srtp-auth sha1-80

!

- Konfiguration auf globaler Ebene

Sprachdienst voip

Schluck

srtp-auth sha1-80

!

- Konfiguration auf Sprachklassenebene

Sprachklasse srtp-crypto 3000

crypto 1 AES_CM_128_HMAC_SHA1_80

crypto 2 AES_CM_128_HMAC_SHA1_32

!

Schritt 4: SRTP-Fallback aktivieren: Sie können SRTP mit der Fallback-Option konfigurieren, sodass ein Anruf auf RTP zurückgreifen kann, wenn SRTP vom anderen Anrufer nicht unterstützt wird. Die SRTP-Fallback-Funktion muss aktiviert werden, damit nicht sichere ergänzende Services wie Warteschleifenmusik, Anrufweiterleitung und Anrufweiterleitung unterstützt werden können.

- Im Dial-Peer-Konfigurationsmodus

dial-peer voice <Tag> voip

SRTP-Fallback (für die Zusammenarbeit mit anderen Geräten als Cisco Unified Communications Manager)

Oder

voice-class sip srtp negotiation cisco (Aktivieren Sie diese CLI zusammen mit dem Befehl srtp fallback zur Unterstützung des SRTP-Fallbacks mit Cisco Unified Communications Manager)

- Im globalen VoIP SIP-Konfigurationsmodus

Sprachdienst voip

Schluck

SRTP-Fallback (für die Zusammenarbeit mit anderen Geräten als Cisco Unified Communications Manager)

Oder

srtp negotiate cisco (Aktivieren Sie diese CLI zusammen mit dem Befehl srtp fallback, um

SRTP-Fallback mit Cisco Unified Communications Manager zu unterstützen)

Beispielkonfiguration:

Nachfolgend finden Sie eine konsolidierte Beispielkonfiguration:

Sprachklasse srtp-crypto 300

crypto 1 AES_CM_128_HMAC_SHA1_80

crypto 2 AES_CM_128_HMAC_SHA1_32

!

dial-peer voice 100 voip

Beschreibung Eingehender SRTP-DFÜ-Peer

Zielmuster 1234

Sitzungsprotokoll sipv2

session target ipv4:192.0.2.1

Sprachklasse-Codec 1

Sprachklasse SIP SRTP

dtmf-relay rtp-nte

SRTP

Sprachklasse sip srtp-crypto 300

IP QoS DSCP CS3-Signalisierung

!

dial-peer voice 200 voip

description Ausgehender RTP-DFÜ-Peer

Zielmuster 5678

Sitzungsprotokoll sipv2

session target ipv4:192.0.2.2

Sprachklasse-Codec 1

dtmf-relay rtp-nte

IP QoS DSCP CS3-Signalisierung

!

Überprüfung

Führen Sie den Befehl während eines aktiven Anrufs aus, um die SRTP- und RTP-Komponenten zu überprüfen.

```
CUBE# show call active voice brief
```

```
Telefonie-Rufnummern: 0
```

```
SIP-Anrufabschnitte: 2
```

```
H323-Anrufabschnitte: 0
```

```
Call Agent gesteuerte Call-Beine: 0
```

```
SCCP-Anrufabschnitte: 0
```

```
Multicast-Anrufabschnitte: 0
```

```
Gesamtzahl der Anrufabschnitte: 2
```

```
0 : 1 12:49:45.256 IST Fr Okt 19 2024.1 +29060 pid:1 Antwort 10008001 verbunden
```

```
dur 00:01:19 tx:1653/271092 rx:2831/464284 dscp:0 media:0
```

```
IP XX.XX.XX.XX:7892 SRTP: on rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay:  
off
```

```
inaktive Medien erkannt:n Mediensteuerung rcvd:n/a Zeitstempel:n/a
```

```
Anruf mit langer Dauer erkannt:n Anrufdauer mit langer Dauer:n/ein Zeitstempel:n/a
```

```
0:2 12:49:45.256 IST Fr Okt 19 2024.2 +29060 pid:22 Ursprungs 20009001 verbunden
```

```
dur 00:01:19 tx:2831/452960 rx:1653/264480 dscp:0 media:0
```

```
IP XX.XX.XX.XX:7893 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay:  
off
```

```
inaktive Medien erkannt:n Mediensteuerung rcvd:n/a Zeitstempel:n/a
```

```
Anruf mit langer Dauer erkannt:n Anrufdauer mit langer Dauer:n/ein Zeitstempel:n/a
```

Fehlerbehebung

Sie müssen diese Debug- und Protokolldateien sammeln, um festzustellen, ob es Probleme mit der Interworking-Funktion gibt.

- debug ccsip all
- debuggen voip ccapi inout
- debugging voip srtp packet
- debugging voip srtp error
- debuggen voip srtp session
- Paketerfassung

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.