Configure SRTP-RTP Interworking on CUBE

Contents

Introduction

This document describes a step-by-step process on how to configure SRTP-RTP Interworking on CUBE.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- 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)

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Unified Border Element (CUBE)
- Cisco IOS XE - 17.6 and later releases
- Cisco C8200-1N-4T

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

The Cisco Unified Border Element (CUBE) Support for SRTP-RTP Interworking feature connects SRTP

enterprise domains to RTP SIP provider SIP trunks. SRTP-RTP interworking connects RTP enterprise networks with SRTP over an external network between businesses. This provides flexible secure business-to-business communications without the need for static IPsec tunnels or the need to deploy SRTP within the enterprise.

Key points about SRTP-RTP interworking on CUBE include:

1. Encryption and Decryption: CUBE can encrypt and decrypt data streams to and from SRTP and RTP networks.
2. TLS Support: Transport Layer Security (TLS) can be enabled or disabled between the SCCP server and the SCCP client. By default, TLS is enabled to protect SRTP keys.
3. Supplementary Services: In Cisco IOS Release 15.2(1), the feature was extended to support supplementary services on CUBE.
4. Transcoding: SRTP-RTP internetworking is available with normal and universal transcoders, invoked using SCCP messaging.
5. Fallback Handling: If one of the call endpoints does not support SRTP, the call can fall back to RTP-RTP or fail, depending on the configuration. This fallback occurs only if the srtp fallback command is configured on the respective dial peer.
6. Deployment: SRTP to RTP interworking can be deployed on User to Network Interfaces (UNI) and Network to Network Interfaces (NNI).
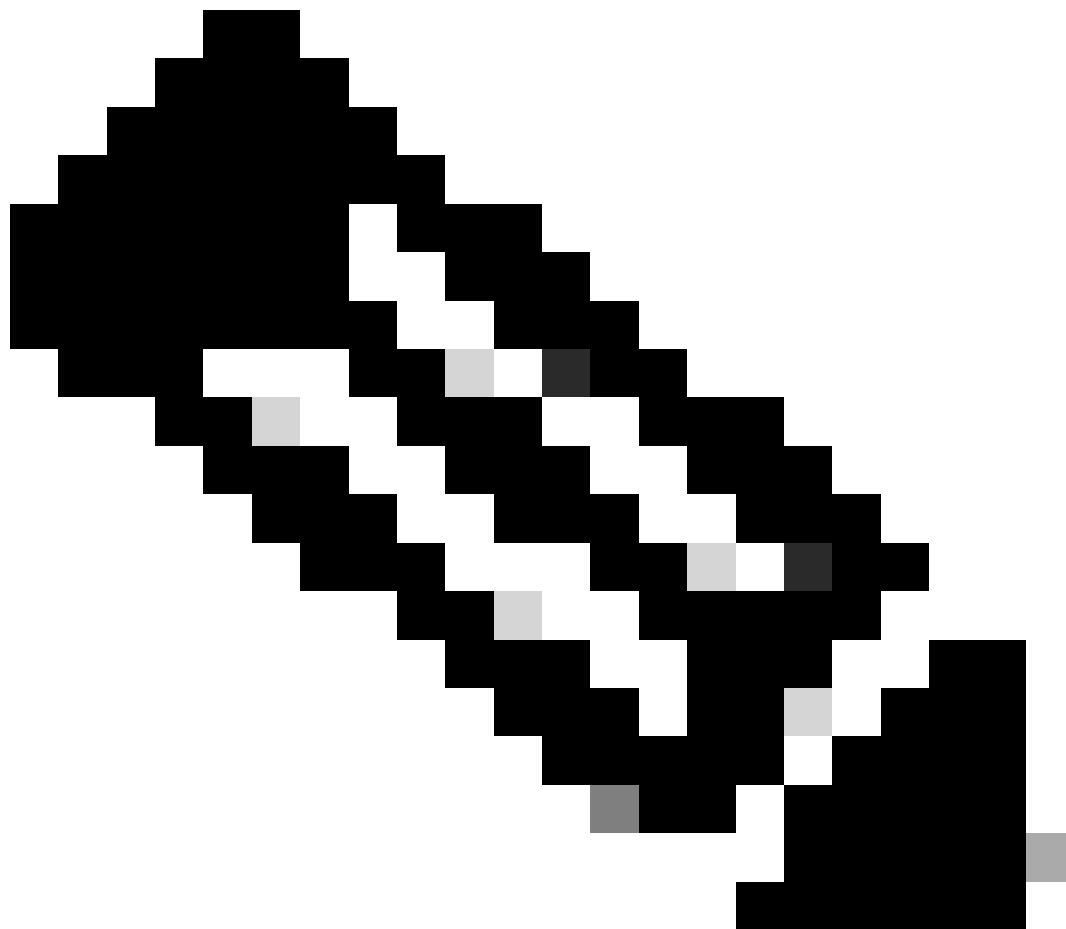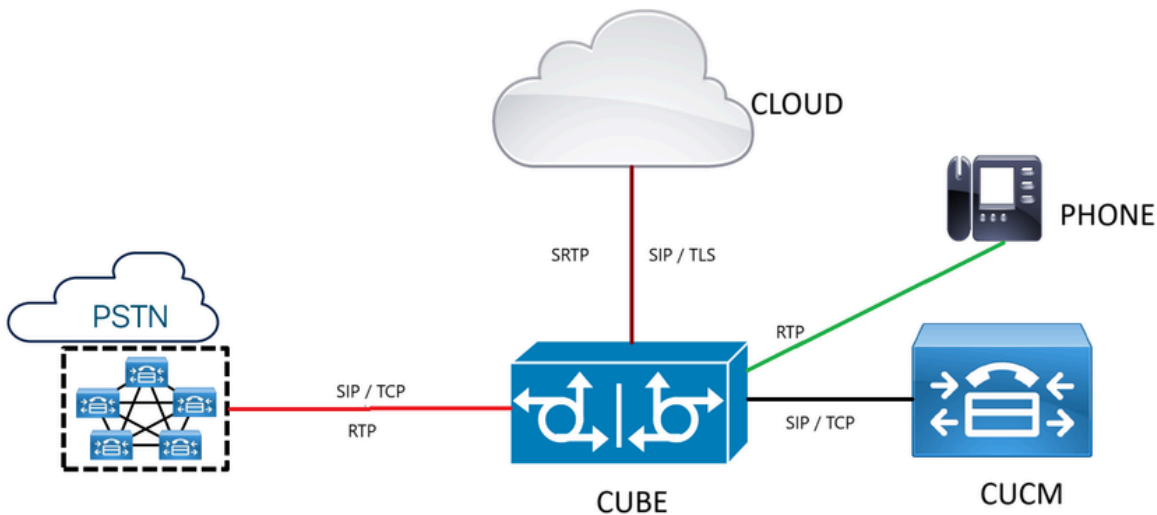
- DSP resources are required for platforms running on Cisco IOS Releases.
- Platforms running on Cisco IOS XE Releases do not require DSP resources.

Configure

Network Diagram

Supplementary Services Support

The supplementary services supported are :

- Midcall codec change with voice class codec configuration
- Reinvite-based call hold and resume
- Music on hold (MoH) invoked from the Cisco Unified Communications Manager (Cisco UCM), where the call leg changes between SRTP and RTP for an MoH source
- Reinvite-based call forward and call transfer
- Call transfer based on a REFER message, with local consumption or pass-through of the REFER message on the CUBE
- Call forward based on a 302 message, with local consumption or pass-through of the 302 message on the CUBE
- T.38 fax switchover
- Fax pass-through switchover

For call transfers involving REFER and 302 messages (messages that are locally consumed on CUBE), end-to-end media renegotiation is initiated from CUBE only when you configure the **supplementary-service media-renegotiate** command in voice service voip configuration mode.

Any call-flow wherein there is a switchover from RTP to SRTP on the same SIP call-leg requires the **supplementary-service media-renegotiate** command enabled in global or voice service voip configuration mode to ensure there is 2-way audio.

Example call-flows:

- RTP -SRTP transfer on CUCM side
- Non-secure MOH being played during secure call hold or resume

When supplementary services are invoked from the end points, the call can switch between SRTP and RTP during the call duration. Hence, Cisco recommends that you configure such SIP trunks for SRTP fallback.
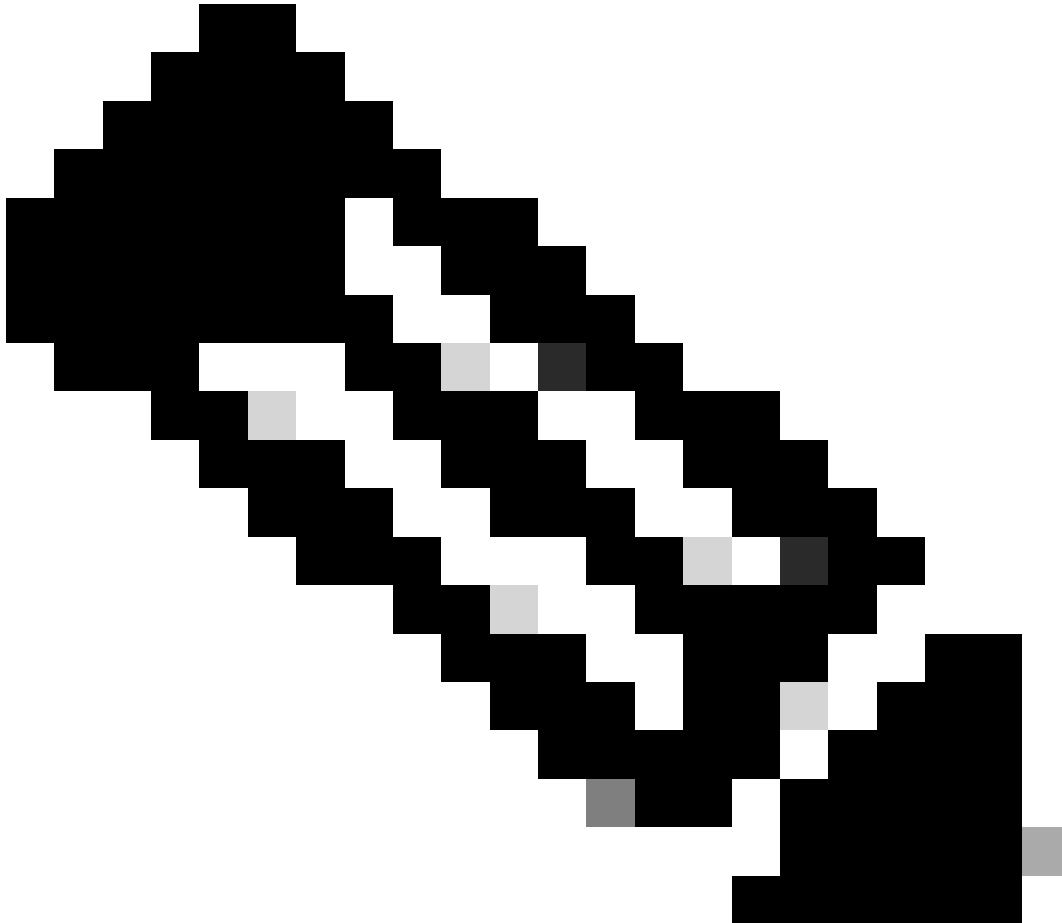
Note: From Cisco IOS XE Everest Release 16.5.1b onward, these crypto suites are enabled by default on the SRTP leg:

- AEAD_AES_256_GCM
- AEAD_AES_128_GCM
- AES_CM_128_HMAC_SHA1_80
- AES_CM_128_HMAC_SHA1_32

Configurations

Step 1. Enable SRTP and configure Dial-Peer for the SRTP leg**:** This is the leg where SRTP is required.

dial-peer voice <tag> voip

```
  description Incoming SRTP Dial-Peer

  destination-pattern <pattern>

  session protocol sipv2

  session target ipv4:<SRTP-Peer-IP-Address>

  voice-class codec 1

  srtp

  dtmf-relay rtp-nte

  ip qos dscp cs3 signaling

  !
```

Step 2. Configure Dial-Peer for the RTP leg: This is the leg where RTP is required.

```
  dial-peer voice <tag> voip

   description Outgoing RTP Dial-Peer

   destination-pattern <pattern>

   session protocol sipv2

   session target ipv4:<RTP-Peer-IP-Address>

   voice-class codec 1

   dtmf-relay rtp-nte

   ip qos dscp cs3 signaling

   !
```

Step 3. Configure Crypto Authentication

Steps to configure CUBE to support an SRTP connection using the AES_CM_128_HMAC_SHA1_80 crypto suite

- Dial-peer level configuration

```
  dial-peer voice <tag> voip

     voice-class sip srtp-auth sha1-80

   !
```

- Global Level configuration

```
  voice service voip

   sip
```

srtp-auth sha1-80

!

- Voice class level configuration

voice class srtp-crypto 3000

crypto 1 AES_CM_128_HMAC_SHA1_80

crypto 2 AES_CM_128_HMAC_SHA1_32

!

Step 4. Enable SRTP Fallback: You can configure SRTP with the fallback option so that a call can fall back to RTP if SRTP is not supported by the other call end. Enabling SRTP fallback is required for supporting nonsecure supplementary services such as MoH, call forward, and call transfer.

- In dial-peer configuration mode

dial-peer voice <tag> voip

srtp fallback (for interworking with devices other than Cisco Unified Communications Manager)

or

voice-class sip srtp negotiate cisco (Enable this CLI along with srtp fallback command to support SRTP fallback with Cisco Unified Communications Manager)

- In global VoIP SIP configuration mode

voice service voip

sip

srtp fallback (for interworking with devices other than Cisco Unified Communications Manager)

or

srtp negotiate cisco (Enable this CLI along with srtp fallback command to support SRTP fallback with Cisco Unified Communications Manager)

Example Configuration:

Here is a consolidated example configuration:

voice class srtp-crypto 300

crypto 1 AES_CM_128_HMAC_SHA1_80

crypto 2 AES_CM_128_HMAC_SHA1_32

!

dial-peer voice 100 voip

description Incoming SRTP Dial-Peer

```
  destination-pattern 1234

  session protocol sipv2

  session target ipv4:192.0.2.1

  voice-class codec 1

  voice-class sip srtp

  dtmf-relay rtp-nte

  srtp

  voice-class sip srtp-crypto 300

  ip qos dscp cs3 signaling

!
dial-peer voice 200 voip

  description Outgoing RTP Dial-Peer

  destination-pattern 5678

  session protocol sipv2

  session target ipv4:192.0.2.2

  voice-class codec 1

  dtmf-relay rtp-nte

  ip qos dscp cs3 signaling

!
```

Verify

Execute the command during an active call to verify SRTP and RTP legs.

CUBE# show call active voice brief

Telephony call-legs: 0

SIP call-legs: 2

H323 call-legs: 0

Call agent controlled call-legs: 0

SCCP call-legs: 0

ulticast call-legs: 0

Total call-legs: 2

0   : 1 12:49:45.256 IST Fri Oct 19 2024.1 +29060 pid:1 Answer 10008001 connected

 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

 media inactive detected:n media contrl rcvd:n/a timestamp:n/a

 long duration call detected:n long duration call duration:n/a timestamp:n/a

0   : 2 12:49:45.256 IST Fri Oct 19 2024.2 +29060 pid:22 Originate 20009001 connected

 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

 media inactive detected:n media contrl rcvd:n/a timestamp:n/a

 long duration call detected:n long duration call duration:n/a timestamp:n/a

Troubleshoot

You need to collect these debugs and logs in order to investigate if there are any issues with interworking.

- debug ccsip all
- debug voip ccapi inout
- debug voip srtp packet
- debug voip srtp error
- debug voip srtp session
- Packet captures