SRTP-RTP Internetworking

- Overview, on page 1
- Prerequisites, on page 5
- Restrictions, on page 5
- Configure SRTP-RTP Interworking, on page 5
- Configure Crypto Authentication, on page 8
- Enable SRTP Fallback, on page 10
- Verify SRTP-RTP, on page 13

Overview

The Cisco Unified Border Element (CUBE) Support for SRTP-RTP Interworking feature allows secure network to non-secure network calls and provides operational enhancements for Session Initiation Protocol (SIP) trunks from Cisco Unified Call Manager and Cisco Unified Call Manager Express. Support for Secure Real-Time Transport Protocol (SRTP) to Real-Time Transport Protocol (RTP) interworking in a network is enabled for SIP-SIP audio calls.

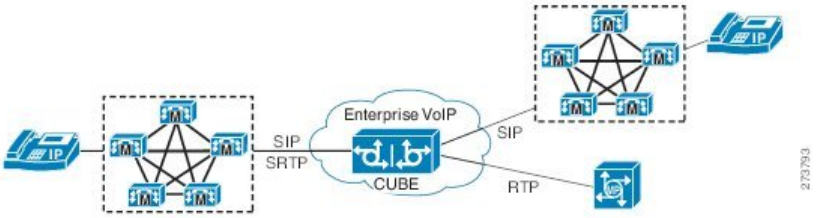
To configure support for SRTP-RTP interworking, you should understand the following concepts:

Support for SRTP-RTP Interworking

The CUBE Support for SRTP-RTP Interworking feature connects SRTP Cisco Unified Call Manager domains with the following:

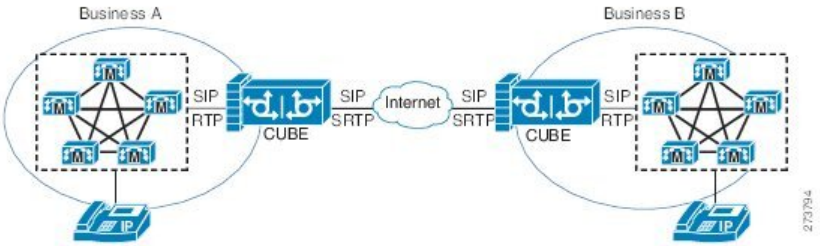
- RTP Cisco Unified Call Manager domains. Domains that do not support SRTP or is not configured for SRTP.
- RTP Cisco applications or servers. For example, Cisco Unified Meeting Place, Cisco WebEx, or Cisco Unity, which do not support SRTP, or is not configured for SRTP, or are resident in a secure data center.
- RTP to third-party equipment. For example, IP trunks to PBXs or virtual machines, which do not support SRTP.

Figure 1: SRTP Domain Connections



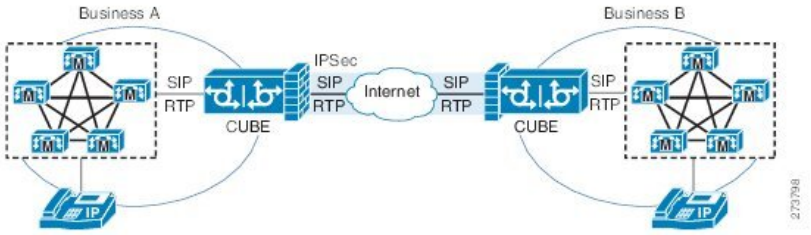
The CUBE support for SRTP-RTP Interworking feature connects SRTP enterprise domains to RTP SIP provider SIP trunks. SRTP-RTP interworking connects RTP enterprise networks with SRTP over an external network between businesses. This provides flexible and secure business-to-business communications without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

Figure 2: Secure Business-to-Business Communications



SRTP-RTP interworking also connects SRTP enterprise networks with static IPsec over external networks.

Figure 3: SRTP Enterprise Network Connections



SRTP-RTP interworking on the CUBE in a network topology uses single-pair keygen. Existing audio and dual-tone multifrequency (DTMF) transcoding supports voice calls. There is no impact on SRTP-SRTP pass-through calls.

Use the **srtp** and **srtp fallback** commands to configure SRTP on one dial peer. Configure the RTP on the other dial peer. The dial peer configuration takes precedence over the global configuration on the CUBE.

Fallback handling occurs if one of the call endpoints does not support SRTP. The call can fall back to RTP-RTP, or the call can fail, depending on the configuration. Fallback takes place only if the **srtp fallback** command is configured on the respective dial peer. RTP-RTP fallback occurs when no transcoding resources are available for SRTP-RTP interworking.

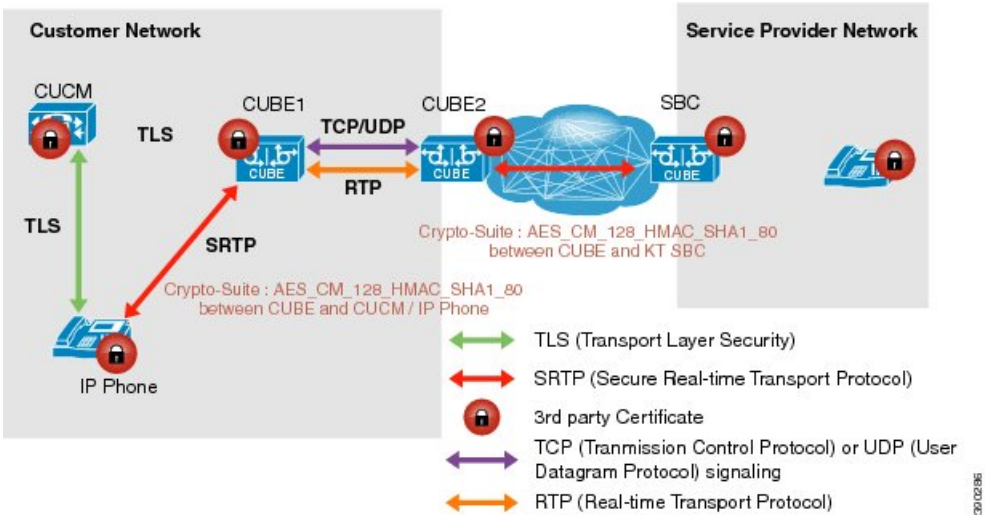
Use SRTP-RTP Chain for Interworking Between AES_CM_128_HMAC_SHA1_32 and AES_CM_128_HMAC_SHA1_80 Crypto Suites

A single Cisco Unified Communications Manager (CUCM) device cannot terminate a Secure Real-Time Transport Protocol (SRTP) connection with an IP Phone using the AES_CM_128_HMAC_SHA1_32 crypto suite and initiate an SRTP connection with an external CUBE device with the AES_CM_128_HMAC_SHA1_80 crypto suite at the same time.

For Cisco Unified Communications Manager (Cisco Unified Communications Manager) and IP Phone devices that support only AES_CM_128_HMAC_SHA1_32 crypto suite, the interim SRTP-RTP interworking solution that is described below can be implemented.

- Cisco Unified Communications Manager or IP Phone side:
  - An SRTP connection using the AES_CM_128_HMAC_SHA1_32 crypto suite exists between the IP phone and CUBE1.
  - An RTP connection exists between CUBE1 and CUBE2.
- SIP trunk side—An SRTP connection using the AES_CM_128_HMAC_SHA1_80 crypto suite is initiated by CUBE2 here. In the image below, CUBE2 is the border element on the Customer Network and SBC is the border element on the Service Provider Network.

Figure 4: SRTP-RTP Interworking Supporting AES_CM_128_HMAC_SHA1_32 Crypto Suite



Note

- AES_CM_128_HMAC_SHA1_32 to AES_CM_128_HMAC_SHA1_80 interworking does not support to Cisco IOS XE Everest 16.4.1 Release.
- SRTP-SRTP interworking supports from Cisco IOS XE Everest 16.5.1b Release onwards, and therefore does not require an SRTP-RTP chain.

Supplementary Services Support

The following supplementary services are supported:

- 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.

Note 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. For information on configuring SRTP fallback, refer Enable SRTP Fallback, on page 10 .

Feature Information

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for SRTP-RTP Interworking

Feature Name	Releases	Feature Information
Support for AEAD_AES_GCM_256 and AEAD_AES_GCM_128 crypto-suites	Cisco IOS XE Everest 16.5.1b	AEAD_AES_GCM_256 and AEAD_AES_GCM_128 crypto suites were added to support SRTP-RTP interworking.

Prerequisites

- SRTP-RTP interworking is supported with Cisco Unified Call Manager 7.0 and later releases.
- Platforms running on Cisco IOS XE Releases do not require DSP resources.

Restrictions

- More than one video m-line is not supported.
- GCM ciphers with extension header are not supported.

Configure SRTP-RTP Interworking

Note From Cisco IOS XE Everest Release 16.5.1b onwards, the following 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

Use the following procedure for changing the default preference list.

Perform the task in this section to enable SRTP-RTP interworking support between one or multiple Cisco Unified Border Elements for SIP-SIP audio calls. In this task, RTP is configured on the incoming call leg and SRTP is configured on the outgoing call leg.

Note This feature is available only on Cisco IOS XE images with security package.

SUMMARY STEPS

1. **enable**

2. **configure terminal**
3. **dial-peer voice** *tag* **voip**
4. **destination-pattern** *string*
5. **session protocol sipv2**
6. **session target ipv4:** *destination-address*
7. **incoming called-number** *string*
8. **codec** *codec*
9. **end**
10. **dial-peer voice** *tag* **voip**
11. Repeat Steps 4, 5, 6, and 7 to configure a second dial peer.
12. **srtp**
13. **codec** *codec*
14. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**dial-peer voice** *tag* **voip** **Example:** `Device(config)# dial-peer voice 201 voip`	Defines a particular dial peer, to specify the method of voice encapsulation, and enters dial peer voice configuration mode. • In the example, the following parameters are set: • Dial peer 201 is defined. • VoIP is shown as the method of encapsulation.
Step 4	**destination-pattern** *string* **Example:** `Device(config-dial-peer)# destination-pattern 5550111`	Specifies either the prefix or the full E.164 telephone number to be used for a dial peer string. • In the example, 5550111 is specified as the pattern for the telephone number.
Step 5	**session protocol sipv2** **Example:** `Device(config-dial-peer)# session protocol sipv2`	Specifies a session protocol for calls between local and remote routers using the packet network. • In the example, the **sipv2** keyword is configured so that the dial peer uses the SIP protocol.

	Command or Action	Purpose
Step 6	**session target ipv4:** *destination-address* **Example:** `Device(config-dial-peer)# session target ipv4:10.13.25.102.`	Designates an IPv4 destination address where calls will be sent. • In the example, calls matching this outbound dial-peer will be sent to 10.13.25.102.
Step 7	**incoming called-number** *string* **Example:** `Device(config-dial-peer)# incoming called-number 5550111`	Specifies a digit string that can be matched by an incoming call to associate the call with a dial peer. • In the example, 5550111 is specified as the pattern for the E.164 or private dialing plan telephone number.
Step 8	**codec** *codec* **Example:** `Device(config-dial-peer)# codec g711ulaw`	Specifies the voice coder rate of speech for the dial peer. • In the example, G.711 mu-law at 64,000 bps, is specified as the voice coder rate for speech.
Step 9	**end** **Example:** `Device(config-dial-peer)#end`	Exits dial peer voice configuration mode.

Step 10	**dial-peer voice** *tag* **voip**
	Example:
	`Device(config)# dial-peer voice 200 voip`
		Defines a particular dial peer, to specify the method of voice encapsulation, and enters dial peer voice configuration mode.
		• In the example, the following parameters are set:
		  • Dial peer 200 is defined.
		  • VoIP is shown as the method of encapsulation.

Step 11	Repeat Steps 4, 5, 6, and 7 to configure a second dial peer.	--
Step 12	**srtp** **Example:** `Device(config-dial-peer)# srtp`	Specifies that SRTP is used to enable secure calls for the dial peer.
Step 13	**codec** *codec* **Example:** `Device(config-dial-peer)# codec g711ulaw`	Specifies the voice coder rate of speech for the dial peer. • In the example, G.711 mu-law at 64,000 bps, is specified as the voice coder rate for speech.
Step 14	**exit** **Example:** `Device(config-dial-peer)# exit`	Exits dial peer voice configuration mode.

Example: SRTP-RTP Interworking

The following example shows how to configure support for SRTP-RTP interworking. In this example, the incoming call leg is RTP and the outgoing call leg is SRTP.

```
%SYS-5-CONFIG_I: Configured from console by console
dial-peer voice 201 voip
 destination-pattern 5550111
 session protocol sipv2
 session target ipv4:10.13.25.102
 incoming called-number 5550112
 codec g711ulaw
!
dial-peer voice 200 voip
 destination-pattern 5550112
 session protocol sipv2
 session target ipv4:10.13.2.51
 incoming called-number 5550111
 srtp
 codec g711ulaw
```

Configure Crypto Authentication

Note Effective Cisco IOS XE Everest Releases 16.5.1b, **srtp-auth** command is deprecated. Although this command is still available in Cisco IOS XE Everest software, executing this command does not cause any configuration changes. Use **voice class srtp-crypto** command to configure the preferred cipher-suites for the SRTP call leg (connection). For more information, see SRTP-SRTP Interworking.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Execute the commands based on your configuration mode
   - In dial-peer configuration mode:

     dial-peer voice *tag* **voip**

     voice-class sip srtp-auth {**sha1-32** | **sha1-80** | **system**}
   - In global VoIP SIP configuration mode:

     voice service voip

     sip

     srtp-auth {**sha1-32** | **sha1-80**}
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

Step 3	Execute the commands based on your configuration mode
	• In dial-peer configuration mode:
	dial-peer voice *tag* **voip**
	voice-class sip srtp-auth {**sha1-32** | **sha1-80** | **system**}
	• In global VoIP SIP configuration mode:
	voice service voip
	sip
	srtp-auth {**sha1-32** | **sha1-80**}
	Example:
	`Device(config)# dial-peer voice 15 voip`
	`Device(config-dial-peer)# voice-class sip srtp-auth sha1-80`
	Example:
	`Device(config)# voice service voip`
	`Device(conf-voi-serv)# sip`
	`Device(conf-serv-sip)# srtp-auth sha1-80`
		Configures an SRTP connection on CUBE using the preferred crypto suite.
		• The default value is **sha1-32**.

Step 4	**end** **Example:** `Device(conf-serv-sip)# end`	Ends the current configuration session and returns to privileged EXEC mode.

Example: Configuring Crypto Authentication

Note Effective Cisco IOS XE Everest Releases 16.5.1b, **srtp-auth** command is deprecated. Although this command is still available in Cisco IOS XE Everest software, executing this command does not cause any configuration changes. Use **voice class srtp-crypto** command to configure the preferred cipher-suites for the SRTP call leg (connection). For more information, see SRTP-SRTP Interworking.

Example: Configuring Crypto Authentication (Dial Peer Level)

The following example shows how to configure CUBE to support an SRTP connection using the AES_CM_128_HMAC_SHA1_80 crypto suite at the dial peer level:

```
Device> enable
Device# configure terminal
Device(config)# dial-peer voice 15 voip
Device(config-dial-peer)# voice-class sip srtp-auth sha1-80
Device(config-dial-peer)# end
```

Example: Configuring Crypto Authentication (Global Level)

The following example shows how to configure CUBE to support an SRTP connection using the AES_CM_128_HMAC_SHA1_80 crypto suite at the global level:

```
Device> enable
Device# configure terminal
Device(config)# voice service voip
Device(conf-voi-serv)# sip
Device(conf-serv-sip)# srtp-auth sha1-80
Device(conf-serv-sip)# end
```

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.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Enter one of the following commands:
   - 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)

4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	Enter one of the following commands: • 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**	Enables call fallback to nonsecure mode.

	Command or Action	Purpose

	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:
	
	`Device(config)# dial-peer voice 10 voip`
	`Device(config-dial-peer)# srtp fallback`
	
	Example:
	
	`Device(config)# dial-peer voice 10 voip`
	`Device(config-dial-peer)# voice-class sip srtp negotiate`
	`Cisco`
	
	Example:
	
	`Device(config)# voice service voip`
	`Device(config)# sip`
	`Device(conf-voi-serv)# srtp fallback`
	
	Example:
	
	`Device(config)# voice service voip`
	`Device(config)# sip`
	`Device(conf-voi-serv)# srtp negotiate cisco`	

Step 4	**exit** **Example:** `Device(conf-voi-serv)# exit`	Exits present configuration mode and enters privileged EXEC mode.

Troubleshooting Tips

The following commands help in troubleshooting SRTP-RTP supplementary services support:

- **debug ccsip all**
- **debug voip ccapi inout**

Verify SRTP-RTP

Perform this task to verify the configuration for SRTP-RTP supplementary services support.

SUMMARY STEPS

1. **enable**
2. **show call active voice brief**

DETAILED STEPS

Step 1 enable

Enables privileged EXEC mode.

Example:

```
Device> enable
```

Step 2 show call active voice brief

Displays call information for voice calls in progress.

Example:

```
Device# 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: 2
ulticast call-legs: 0
Total call-legs: 4
0    : 1 12:49:45.256 IST Fri Jun 3 2011.1 +29060 pid:1 Answer 10008001 connected
 dur 00:01:19 tx:1653/271092 rx:2831/464284 dscp:0 media:0
 IP 10.45.40.40:7892 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 Jun 3 2011.2 +29060 pid:22 Originate 20009001 connected
 dur 00:01:19 tx:2831/452960 rx:1653/264480 dscp:0 media:0
 IP 10.45.40.40:7893 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

0    : 3 12:50:14.326 IST Fri Jun 3 2011.1 +0 pid:0 Originate  connecting
 dur 00:01:19 tx:2831/452960 rx:1653/264480 dscp:0 media:0
 IP 10.45.34.252:2000 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

0    : 5 12:50:14.326 IST Fri Jun 3 2011.2 +0 pid:0 Originate  connecting
 dur 00:01:19 tx:1653/271092 rx:2831/464284 dscp:0 media:0
 IP 10.45.34.252:2000 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
```