SRTP-SRTP Interworking

Cisco Unified Border Element (CUBE) supports secure calls between two networks having different cipher suites. SRTP-SRTP interworking is supported for audio and video calls.

Feature Information for SRTP-SRTP Interworking

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 https://cfnng.cisco.com/. An account on Cisco.com is not required.

Table 1: Feature Information for SRTP-SRTP Interworking

Feature Name	Releases	Feature Information
Security Readiness Criteria (SRC)—Modified the command **show sip-ua calls**.	Cisco IOS XE Gibraltar Release 16.11.1a	Command **show sip-ua calls** is modified to display local crypto key and remote cryto key.
Support for SRTP-SRTP interworking	Cisco IOS XE Everest 16.5.1b	This feature allows secure calls between two enterprises using different cipher suites. Supported cipher suites are as follows: • AEAD_AES_256_GCM • AEAD_AES_128_GCM • AES_CM_128_HMAC_SHA1_80 • AES_CM_128_HMAC_SHA1_32

Prerequisites for SRTP-SRTP Interworking

- Cisco IOS XE Everest Release 16.5.1b or later

Note SRTP-SRTP Interworking feature is not supported on Cisco ISR G2 Series Routers.

Restrictions for SRTP-SRTP Interworking

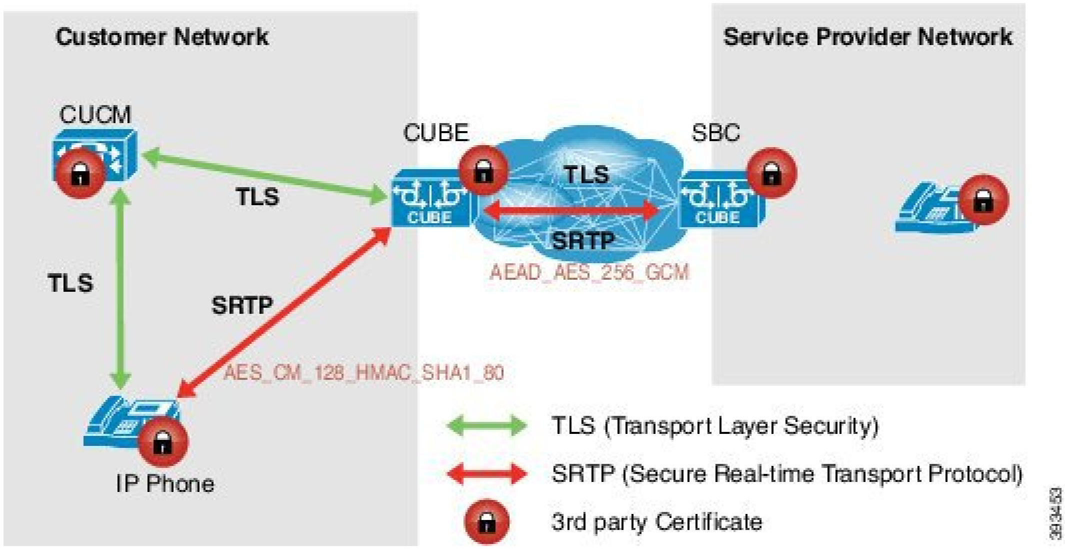
- Asymmetric SRTP fallback configuration is not supported
- Call Progress Analysis (CPA) is not supported
- Transcoding calls are not supported
- SRTCP-RTCP interworking is not supported
- More than one audio and video m-line is not supported
- Unified CME and Unified SRST flows and SIP-TDM flows are not supported
- GCM ciphers with extension header are not supported

Information About SRTP-SRTP Interworking

From Cisco IOS XE Everest Release 16.5.1b onwards, when SRTP is enabled, by default Cisco Unified Border Element supports secure calls between networks using different cipher suites. The cipher suites that are supported for SRTP-SRTP interworking with default preference order are as follows:

- AEAD_AES_256_GCM
- AEAD_AES_128_GCM
- AES_CM_128_HMAC_SHA1_80
- AES_CM_128_HMAC_SHA1_32

Figure 1: SRTP-SRTP Interworking



CUBE allows you to change the list of preference order of the cipher-suites. Cipher-suite preference can be configured globally (under **voice service voip** >> **sip**), on a voice class tenant, or on a dial peer.

The preference range is 1–4, where 1 represents highest preference. CUBE offers SRTP cipher-suites in SDP offer based on the preference configured. For SDP answer, the highest configured preference cipher suite that matches the offer from peer is selected.

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 that is enabled in global or voice service VoIP configuration mode to ensure that there is 2-way audio.

Example call-flows:

- RTP-RTP flow switching to SRTP-RTP.
- Nonsecure MOH being played during secure call hold or resume.
- RTP-SRTP flow switching to SRTP- SRTP.

When supplementary services are invoked from the endpoints, 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 Enabling SRTP Fallback, on page 9.

How to Configure SRTP-SRTP Interworking

Configuring SRTP

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. **srtp**
9. **codec** *codec*
10. **end**
11. **dial-peer voice** *tag* **voip**
12. Repeat Steps 4, 5, 6, and 7 to configure a second dial peer.
13. **srtp**
14. **codec** *codec*
15. **exit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Device> enable`	• 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.
Step 6	**session target ipv4:***destination-address* **Example:** `Device(config-dial-peer)# session target ipv4:10.13.25.102`	Designates an IP 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	**srtp** **Example:** `Device(config-dial-peer)# srtp`	Specifies that SRTP is used to enable secure calls for the dial peer.
Step 9	**codec** *codec*	Specifies the voice coder rate of speech for the dial peer.

	Command or Action	Purpose
	Example: `Device(config-dial-peer)# codec g711ulaw`	• In the example, G.711 mu-law at 64,000 bps, is specified as the voice coder rate for speech.
Step 10	**end** **Example:** `Device(config-dial-peer)#end`	Exits dial peer voice configuration mode.

Step 11	**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 12	Repeat Steps 4, 5, 6, and 7 to configure a second dial peer.	--
Step 13	**srtp** **Example:** `Device(config-dial-peer)# srtp`	Specifies that SRTP is used to enable secure calls for the dial peer.
Step 14	**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 15	**exit** **Example:** `Device(config-dial-peer)# exit`	Exits dial peer voice configuration mode.

Configuring Cipher Suite Preference (optional)

Note No additional configurations are required if you want to configure the default preference order. Use the following procedure for changing the default preference.

SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **voice class srtp-crypto** *tag*
4. **crypto** *preference cipher-suite*
5. **exit**

DETAILED STEPS

Procedure

	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	**voice class srtp-crypto** *tag* **Example:** `Device(config)# voice class srtp-crypto 100`	Enters voice class configuration mode and assign an identification tag for a srtp-crypto voice class.
Step 4	**crypto** *preference cipher-suite* **Example:** `Device(config-class)# crypto 1 AEAD_AES_256_GCM`	Specifies the preference for an SRTP cipher-suite that will be offered by Cisco Unified Border Element (CUBE) in the SDP in offer and answer. You can configure a maximum of four preferences.
Step 5	**exit** **Example:** `Device(config-class)# exit`	Exists the present configuration mode.

Example

What to do next

Assign SRTP Crypto voice class globally, or on a voice-class tenant, or on a dial-peer. For more information, see Applying Crypto Suite Selection Preference (optional), on page 7.

Applying Crypto Suite Selection Preference (optional)

Before you begin

- Ensure that an srtp voice-class is created using the **voice class srtp-crypto** *crypto-tag* command

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Apply crypto suite selection preference
    - In global configuration mode:
        - **voice service voice**
        - **sip**
        - **srtp-crpto** *crypto-tag*
    - In voice class tenant configuration mode:
        - **voice class tenant** *tag*
        - **srtp-crypto** *crypto-tag*
    - In dial-peer configuration mode:
        - **dial-peer voice** *tag* **voip**
        - **voice-class sip srtp-crypto** *crypto-tag*
4. **end**

DETAILED STEPS

Procedure

	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	Apply crypto suite selection preference
	• In global configuration mode:
	  • **voice service voice**
	  • **sip**
	  • **srtp-crpto** *crypto-tag*
	• In voice class tenant configuration mode:
	  • **voice class tenant** *tag*
		Assigns previously configured crypto-suite selection preference.
		The *cryptp-tag* maps to the tag created using the **voice class srtp-crypto** command available in global configuration mode.

	Command or Action	Purpose

	• **srtp-crypto** *crypto-tag*
	• In dial-peer configuration mode:
	• **dial-peer voice** *tag* **voip**
	• **voice-class sip srtp-crypto** *crypto-tag*
	Example:
	In global configuration mode:
	`Device> enable`
	`Device# configure terminal`
	`Device(config)# voice service voice`
	`Device(conf-voi-serv)# sip`
	`Device(conf-serv-sip)# srtp-crypto 102`
	In voice class tenant configuration mode:
	`Device> enable`
	`Device# configure terminal`
	`Device(config)# voice class tenant 100`
	`Device(conf-serv-sip)# srtp-crypto 102`
	In dial-peer configuration mode:
	`Device> enable`
	`Device# configure terminal`
	`Device(config)# dial-peer voice 300 voip`
	`Device(config-dial-peer)# voice-class sip`
	`srtp-crypto 102`	

Step 4	**end** **Example:** `Device(config-dial-peer)# exit`	Exits the present configuration mode.

Enabling 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

Procedure

	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**	Enables call fallback to nonsecure mode.

	Command or Action	Purpose

	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:
	
	`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`	

	Command or Action	Purpose
	`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.

Configuration Examples

Example: Configuring SRTP-SRTP Interworking

The following example shows how to configure support for SRTP-SRTP interworking. In this example, the incoming call leg preference is set to AEAD_AES_256_GCM crypto-suite and the outgoing call leg preference is set to AES_CM_128_HMAC_SHA1_80 crypto-suite.

Configure SRTP:

```
Device> enable
Device# configure terminal
Device(config)# dial-peer voice 300 voip
Device(config-dial-peer)# description "inbound dialpeer for 81560"
Device(config-dial-peer)# session protocol sipv2
Device(config-dial-peer)# incoming called-number 81560
Device(config-dial-peer)# srtp
Device(config-dial-peer)# codec g711ulaw
Device(config-dial-peer)# end

Device(config)# dial-peer voice 400 voip
Device(config-dial-peer)# destination-pattern 81560
Device(config-dial-peer)# description "outbound dialpeer for 81560"
Device(config-dial-peer)# session protocol sipv2
Device(config-dial-peer)# session target ipv4:10.13.25.102
Device(config-dial-peer)# srtp
Device(config-dial-peer)# codec g711ulaw
```

Create a voice class srtp-crypto 100 and assign AEAD_AES_256_GCM crypto-suite with highest preference:

```
Device(config)# voice class srtp-crypto 100
Device(config-class)# crypto 1 AEAD_AES_256_GCM
```

Assign srtp-crypto 100 on incoming dial-peer:

```
Device(config)# dial-peer voice 300 voip
Device(config-dial-peer)# voice-class sip srtp-crypto 100
Device(config-dial-peer)# codec g711ulaw
Device(config-dial-peer)# srtp
```

Create a voice class srtp-crypto 103 and assign AES_CM_128_HMAC_SHA1_80 crypto-suite with highest preference:

```
Device> enable
Device# configure terminal
Device(config)# voice class srtp-crypto 103
Device(config-class)# crypto 1 AES_CM_128_HMAC_SHA1_80
```

Assign srtp-crypto 103 on outgoing dial-peer:

```
Device(config)# dial-peer voice 400 voip
Device(config-dial-peer)# voice-class sip srtp-crypto 103
Device(config-dial-peer)# codec g711ulaw
Device(config-dial-peer)# srtp
```

```
Device# show sip-ua calls
Total SIP call legs:2, User Agent Client:1, User Agent Server:1
SIP UAC CALL INFO
Call 1
SIP Call ID                : 706E9625-C4FB11E6-8008AFC8-C0129831@10.25.15.63
   State of the call       : STATE_ACTIVE (7)
   Substate of the call    : SUBSTATE_NONE (0)
   Calling Number          : 61230
   Called Number           : 81560
   Called URI              :
   Bit Flags               : 0xC04018 0x80000100 0x80
   CC Call ID              : 2
   Local UUID              : d5173c8551b25b06820edc687e50ab90
   Remote UUID             : 2e9094e33b815992a519f82abfae09d2
   Source IP Address (Sig ): 10.25.16.63
   Destn SIP Req Addr:Port : [10.13.25.102]:14560
   Destn SIP Resp Addr:Port: [10.13.25.102]:14560
   Destination Name        :
   Number of Media Streams : 1
   Number of Active Streams: 1
   RTP Fork Object         : 0x0
   Media Mode              : flow-through
   Media Stream 1
     State of the stream      : STREAM_ACTIVE
     Stream Call ID           : 2
     Stream Type              : voice+dtmf (1)
     Stream Media Addr Type   : 1
     Negotiated Codec         : g711ulaw (80 bytes)
     Codec Payload Type       : 0
     Negotiated Dtmf-relay    : rtp-nte
     Dtmf-relay Payload Type  : 101
     QoS ID                   : -1
     Local QoS Strength       : BestEffort
     Negotiated QoS Strength  : BestEffort
     Negotiated QoS Direction : None
     Local QoS Status         : None
     Media Source IP Addr:Port: [10.25.15.63]:8002
     Media Dest IP Addr:Port  : [10.13.25.102]:14240
     Local Crypto Suite       :  AES_CM_128_HMAC_SHA1_80
     Remote Crypto Suite      :  AES_CM_128_HMAC_SHA1_80
     Local Crypto Key         : bTQqZXbgFJddA1hE9wJGV3aKxo5vPV+Z1234tVb2
     Remote Crypto Key        : bTQqZXbgFJddA1hE9wJGV3aKxo5vPV+Z9876tVb2
   Mid-Call Re-Assocation Count: 0
   SRTP-RTP Re-Assocation DSP Query Count: 0
```

```
Options-Ping    ENABLED:NO    ACTIVE:NO
   Number of SIP User Agent Client(UAC) calls: 1

SIP UAS CALL INFO
Call 1
SIP Call ID                : 1-8614@10.41.50.13
   State of the call       : STATE_ACTIVE (7)
   Substate of the call    : SUBSTATE_NONE (0)
   Calling Number          : 61230
   Called Number           : 81560
   Called URI              : sip:81560@10.13.25.102:5060
   Bit Flags               : 0xC0401C 0x10000100 0x4
   CC Call ID              : 1
   Local UUID              : 2e9094e33b815992a519f82abfae09d2
   Remote UUID             : d5173c8551b25b06820edc687e50ab90
   Source IP Address (Sig ): 10.25.15.63
   Destn SIP Req Addr:Port : [10.41.50.13]:14450
   Destn SIP Resp Addr:Port: [10.41.50.13]:14450
   Destination Name        : 10.41.50.13
   Number of Media Streams : 1
   Number of Active Streams: 1
   RTP Fork Object         : 0x0
   Media Mode              : flow-through
   Media Stream 1
     State of the stream      : STREAM_ACTIVE
     Stream Call ID           : 1
     Stream Type              : voice+dtmf (0)
     Stream Media Addr Type   : 1
     Negotiated Codec         : g711ulaw (80 bytes)
     Codec Payload Type       : 0
     Negotiated Dtmf-relay    : rtp-nte
     Dtmf-relay Payload Type  : 101
     QoS ID                   : -1
     Local QoS Strength       : BestEffort
     Negotiated QoS Strength  : BestEffort
     Negotiated QoS Direction : None
     Local QoS Status         : None
     Media Source IP Addr:Port: [10.25.15.63]:8000
     Media Dest IP Addr:Port  : [10.41.50.13]:14670
     Local Crypto Suite       :  AEAD_AES_256_GCM
     Remote Crypto Suite      :  AEAD_AES_256_GCM (
                                 AEAD_AES_256_GCM
                                 AEAD_AES_128_GCM )
     Local Crypto Key         : bTQqZXbgFJddA1hE9wJGV3aKxo5vPV+Z8765tVb2
     Remote Crypto Key        : bTQqZXbgFJddA1hE9wJGV3aKxo5vPV+Z2345tVb2
   Mid-Call Re-Assocation Count: 0
   SRTP-RTP Re-Assocation DSP Query Count: 0


Options-Ping    ENABLED:NO    ACTIVE:NO
   Number of SIP User Agent Server(UAS) calls: 1
```

Example: Changing the Cipher-Suite Preference

Specify SRTP cipher-suite preference:

```
Device> enable
Device# configure terminal
Device(config)# voice class srtp-crypto 100
Device(config-class)# crypto 1 AEAD_AES_256_GCM
Device(config-class)# crypto 2 AEAD_AES_128_GCM
```

```
Device(config-class)# crypto 4 AES_CM_128_HMAC_SHA1_32
```

The following is the snippet of **show running-config** command output showing the cipher-suite preference:

```
Device# show running-config
voice class srtp-crypto 100
crypto 1 AEAD_AES_256_GCM
crypto 2 AEAD_AES_128_GCM
crypto 4 AES_CM_128_HMAC_SHA1_32
```

If you want to change the preference 4 to AES_CM_128_HMAC_SHA1_80, execute the following command:

```
Device(config-class)# crypto 4 AES_CM_128_HMAC_SHA1_80
```

The following is the snippet of **show running-config** command output showing the change in cipher-suite:

```
Device# show running-config
voice class srtp-crypto 100
crypto 1 AEAD_AES_256_GCM
crypto 2 AEAD_AES_128_GCM
crypto 4 AES_CM_128_HMAC_SHA1_80
```

If you want to change the preference of AES_CM_128_HMAC_SHA1_80 to 3, execute the following commands:

```
Device(config-class)# no crypto 4
Device(config-class)# crypto 3 AES_CM_128_HMAC_SHA1_80
```

The following is the snippet of **show running-config** command output showing the cipher-suite preference overwritten:

```
Device# show running-config
voice class srtp-crypto 100
crypto 1 AEAD_AES_256_GCM
crypto 2 AEAD_AES_128_GCM
crypto 3 AES_CM_128_HMAC_SHA1_80
```