SRTP-RTP Interworking

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.

- Feature Information for SRTP-RTP Interworking, on page 1
- Prerequisites for SRTP-RTP Interworking, on page 2
- Restrictions for SRTP-RTP Interworking, on page 2
- Information About SRTP-RTP Interworking, on page 2
- How to Configure Support for SRTP-RTP Interworking, on page 6
- Configuration Examples for SRTP-RTP Interworking, on page 13

Feature Information for SRTP-RTP 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 www.cisco.com/go/cfn. An account on Cisco.com is not required.

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified Border Element Support for SRTP-RTP Interworking</td>
<td>12.4(22)YB , 15.0(1)M Cisco IOS XE 3.1S</td>
<td>This feature allows secure to non-secure enterprise calls. Support for SRTP-RTP interworking between one or multiple Cisco Unified Border Elements is enabled for SIP-SIP audio calls.</td>
</tr>
<tr>
<td>Supplementary Services Support on CUBE for SRTP-RTP Calls</td>
<td>Cisco IOS 15.2(1)T Cisco IOS XE 3.7S</td>
<td>The SRTP-RTP Interworking feature was enhanced to support supplementary services for SRTP-RTP calls.</td>
</tr>
</tbody>
</table>
Feature Information

Releases | Feature Information
--- | ---
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 for SRTP-RTP Interworking

• SRTP-RTP interworking is supported with Cisco Unified CallManager 7.0 and later releases.
• DSP resources are required for platforms running on Cisco IOS Releases. For more information on configuring DSP resources, see Transcoding.
• Platforms running on Cisco IOS XE Releases do not require DSP resources.

Restrictions for SRTP-RTP Interworking

• Asymmetric SRTP fallback configuration is not supported.
• Dial peer hunting is not supported.
• Video calls are not supported on platforms running on Cisco IOS Releases.
• More than one video m-line is not supported.
• DTMF interworking is not supported on ISR G2 (2900, 3900) series routers. It is supported only on platforms running on Cisco IOS XE Releases.

Information About SRTP-RTP Interworking

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

Support for SRTP-RTP Interworking

The Cisco Unified Border Element Support for SRTP-RTP Interworking feature connects SRTP Cisco Unified CallManager domains with the following:

• RTP Cisco Unified CallManager domains. Domains that do not support SRTP or have not been configured for SRTP, as shown in the figure below.
• RTP Cisco applications or servers. For example, Cisco Unified MeetingPlace, Cisco WebEx, or Cisco Unity, which do not support SRTP, or have not been configured for SRTP, or are resident in a secure data center, as shown in the figure below.
• RTP to third-party equipment. For example, IP trunks to PBXs or virtual machines, which do not support SRTP.
The Cisco Unified Border Element 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, as shown in the figure below.

SRTP-RTP interworking also connects SRTP enterprise networks with static IPsec over external networks, as shown in the figure below.

SRTP-RTP interworking on the CUBE in a network topology uses single-pair key generation. Existing audio and dual-tone multifrequency (DTMF) transcoding is used to support voice calls. SRTP-RTP interworking support is provided in both flow-through and high-density mode. There is no impact on SRTP-SRTP pass-through calls.

SRTP is configured on one dial peer using the `srtp` and `srtp fallback` commands. RTP is configured 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.
Using 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 Call 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 Call Manager (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.

- CUCM 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 is not supported up to Cisco IOS 15.5(3)M Release and Cisco IOS XE Everest 16.4.1 Release.

- From Cisco IOS XE Everest 16.5.1b Release onwards, SRTP-SRTP interworking is supported and therefore SRTP-RTP chain is not required.
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 Enabling SRTP Fallback.
How to Configure Support for SRTP-RTP Interworking

Configuring SRTP-RTP Interworking Support

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 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
- Enter your password if prompted. |
| **Example:** Device> enable |
| **Step 2** configure terminal | Enters global configuration mode. |
| **Example:** Device# configure terminal |
| **Step 3** dial-peer voice tag 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. |
| **Example:** Device(config)# dial-peer voice 201 voip |
| **Step 4** destination-pattern string | 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. |
| **Example:** Device(config-dial-peer)# destination-pattern 5550111 |
| **Step 5** 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. |
| **Example:** Device(config-dial-peer)# session protocol sipv2 |
| **Step 6** session target ipv4: destination-address | 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. |
| **Example:** Device(config-dial-peer)# session target ipv4:10.13.25.102. |
| **Step 7** incoming called-number string | 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. |
| **Example:** Device(config-dial-peer)# incoming called-number 5550111 |
| **Step 8** codec codec | 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. |
<p>| <strong>Example:</strong> Device(config-dial-peer)# codec codec |</p>
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device(config-dial-peer)# codec g711ulaw</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> end</td>
<td>Exits dial peer voice configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-dial-peer)#end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong> dial-peer voice tag voip</td>
<td>Defines a particular dial peer, to specify the method of voice encapsulation, and enters dial peer voice configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# dial-peer voice 200 voip</td>
<td></td>
</tr>
<tr>
<td>• In the example, the following parameters are set:</td>
<td></td>
</tr>
<tr>
<td>• Dial peer 200 is defined.</td>
<td></td>
</tr>
<tr>
<td>• VoIP is shown as the method of encapsulation.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong> Repeat Steps 4, 5, 6, and 7 to configure a second dial peer.</td>
<td>--</td>
</tr>
<tr>
<td><strong>Step 12</strong> srtp</td>
<td>Specifies that SRTP is used to enable secure calls for the dial peer.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-dial-peer)# srtp</td>
<td></td>
</tr>
<tr>
<td><strong>Step 13</strong> codec codec</td>
<td>Specifies the voice coder rate of speech for the dial peer.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-dial-peer)# codec g711ulaw</td>
<td></td>
</tr>
<tr>
<td>• In the example, G.711 mu-law at 64,000 bps, is specified as the voice coder rate for speech.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 14</strong> exit</td>
<td>Exits dial peer voice configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config-dial-peer)# exit</td>
<td></td>
</tr>
</tbody>
</table>

**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.

**SUMMARY STEPS**

1. enable
2. configure terminal
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><strong>enable</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Device&gt; enable</td>
<td>Enables privileged EXEC mode.&lt;br&gt;• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2</td>
<td><strong>configure terminal</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Device# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>
| Step 3 | Execute the commands based on your configuration mode<br>• In dial-peer configuration mode:<br>  ```
dial-peer voice tag voip
voice-class sip srtp-auth {sha1-32 | sha1-80 | system}
  ```<br>• In global VoIP SIP configuration mode:<br>  ```
voice service voip
sip
srtp-auth {sha1-32 | sha1-80}
  ```<br>**Example:**<br>Device(config)# dial-peer voice 15 voip<br>Device(config-dial-peer)# voice-class sip srtp-auth sha1-80<br>**Example:**<br>Device(config)# voice service voip<br>Device(conf-voi-serv)# sip<br>Device(conf-serv-sip)# srtp-auth sha1-80 | Configures an SRTP connection on CUBE using the preferred crypto suite.<br>• The default value is **sha1-32**. |
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**

---

**Table: Purpose of Commands**

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>end</strong></td>
<td>Ends the current configuration session and returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
| **Example:** | Device(conf-serv-sip)# end | }
# DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> Enter one of the following commands:</td>
<td>Enables call fallback to nonsecure mode.</td>
</tr>
<tr>
<td>• In dial-peer configuration mode</td>
<td></td>
</tr>
<tr>
<td>dial-peer</td>
<td></td>
</tr>
<tr>
<td>voice</td>
<td></td>
</tr>
<tr>
<td>tag</td>
<td></td>
</tr>
<tr>
<td>voip</td>
<td></td>
</tr>
<tr>
<td>srtp</td>
<td></td>
</tr>
<tr>
<td>fallback (for interworking with devices other than Cisco Unified Communications Manager)</td>
<td></td>
</tr>
<tr>
<td>or</td>
<td></td>
</tr>
<tr>
<td>voice-class sip srtp</td>
<td></td>
</tr>
<tr>
<td>negotiate cisco (Enable this CLI along with srtp fallback command to support SRTP fallback with Cisco Unified Communications Manager)</td>
<td></td>
</tr>
<tr>
<td>• In global VoIP SIP configuration mode</td>
<td></td>
</tr>
<tr>
<td>voice service voip</td>
<td></td>
</tr>
<tr>
<td>sip</td>
<td></td>
</tr>
<tr>
<td>srtp</td>
<td></td>
</tr>
<tr>
<td>fallback (for interworking with devices other than Cisco Unified Communications Manager)</td>
<td></td>
</tr>
<tr>
<td>or</td>
<td></td>
</tr>
<tr>
<td>srtp</td>
<td></td>
</tr>
<tr>
<td>negotiate cisco (Enable this CLI along with srtp fallback command to support SRTP fallback with Cisco Unified Communications Manager)</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device(config)# dial-peer voice 10 voip</td>
<td></td>
</tr>
<tr>
<td>Device(config-dial-peer)# srtp fallback</td>
<td></td>
</tr>
</tbody>
</table>
### Troubleshooting Tips

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

- debug ccsip all
- debug voip ccsapi inout

### Verifying SRTP-RTP Supplementary Services Support

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:**

```bash
Device(conf-voi-serv)# exit
```
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 12:45.256 IST Fri Jun 3 2011.1 +29060 pid:1 Answer 10008001 connected
dur 00:01:19 tx:1653/464284 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 ctrl rlcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a
```

Configuration Examples for SRTP-RTP Interworking

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
```
Example: Configuring Crypto Authentication

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 Cisco UBE 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 Cisco UBE 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(config-voi-serv)# sip
Device(config-serv-sip)# srtp-auth sha1-80
Device(config-serv-sip)# end
```