Configuring SIP Support for SRTP

First Published: June 29, 2007
Last Updated: August 5, 2009

This module contains information about configuring Session Initiation Protocol (SIP) support for the Secure Real-time Transport Protocol (SRTP). SRTP is an extension of the Real-time Transport Protocol (RTP) Audio/Video Profile (AVP) and ensures the integrity of RTP and Real-Time Control Protocol (RTCP) packets that provide authentication, encryption, and the integrity of media packets between SIP endpoints.

SIP support for SRTP was introduced in Cisco IOS Release 12.4(15)T. In this and later releases, you can configure the handling of secure RTP calls on both a global level and on an individual dial peer basis on Cisco IOS voice gateways. You can also configure the gateway (or dial peer) either to fall back to (nonsecure) RTP or to reject (fail) the call for cases where an endpoint does not support SRTP.

The option to allow negotiation between SRTP and RTP endpoints was added for Cisco IOS Release 12.4(20)T and later releases, as was interoperability of SIP support for SRTP on Cisco IOS voice gateways with Cisco Unified Communications Manager. In Cisco IOS Release 12.4(22)T and later releases, you can configure SIP support for SRTP on Cisco Unified Border Elements (Cisco UBEs), as well.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the “Feature Information for Configuring SIP Support for SRTP” section on page 16.

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.
Configuring SIP Support for SRTP

Contents

• Prerequisites for Configuring SIP Support for SRTP, page 2
• Restrictions for Configuring SIP Support for SRTP, page 2
• Information About Configuring SIP Support for SRTP, page 2
• How to Configure SIP Support for SRTP, page 9
• Configuring SRTP and SRTP Fallback on a Dial Peer, page 12
• Additional References, page 14
• Feature Information for Configuring SIP Support for SRTP, page 16
• Glossary, page 18

Prerequisites for Configuring SIP Support for SRTP

• Establish a working IP network and configure VoIP.

Note

For information about configuring VoIP, see Enhancements to the Session Initiation Protocol for VoIP on Cisco Access Platforms.

• Ensure that the gateway has voice functionality configured for SIP.
• Ensure that your Cisco router has adequate memory.
• As necessary, configure the router to use Greenwich Mean Time (GMT). SIP requires that all times be sent in GMT. SIP INVITE messages are sent in GMT. However, the default for routers is to use Coordinated Universal Time (UTC). To configure the router to use GMT, issue the clock timezone command in global configuration mode and specify GMT.

Restrictions for Configuring SIP Support for SRTP

• The SIP gateway does not support codecs other than those listed in the table titled “SIP Codec Support by Platform and Cisco IOS Release” in the “Enhanced Codec Support for SIP Using Dynamic Payloads” section of the Configuring SIP QoS Features module.
• SIP requires that all times be sent in GMT.

Information About Configuring SIP Support for SRTP

The SIP Support for SRTP features use encryption to secure the media flow between two SIP endpoints. Cisco IOS voice gateways and Cisco Unified Border Elements use the Digest method for user authentication and, typically, they use Transport Layer Security (TLS) for signaling authentication and encryption.
To provide more flexibility, TLS signaling encryption is no longer required for SIP support of SRTP in Cisco IOS Release 12.4(22)T and later releases. Secure SIP (SIPS) is still used to establish and determine TLS but TLS is no longer a requirement for SRTP, which means calls established with SIP only (and not SIPS) can still successfully negotiate SRTP without TLS signaling encryption. This also means you could configure encryption using a different protocol, such as IPsec.

However, Cisco does not recommend configuring SIP support for SRTP without TLS signaling encryption because doing so compromises the intent of forcing media encryption (SRTP).

When TLS is used, the cryptographic parameters required to successfully negotiate SRTP rely on the cryptographic attribute in the Session Description Protocol (SDP). To ensure the integrity of cryptographic parameters across a network, SRTP uses the SIPS schema (sips:example.com). If the Cisco IOS voice gateway or Cisco Unified Border Element is configured to use TLS encryption and sends an invite to an endpoint that cannot provide TLS support, that endpoint rejects the INVITE message. For cases like these, you can configure the gateway or Cisco UBE either to fall back to an RTP-only call or to reject the call.

The SIP support for SRTP features provide the following security benefits:

- Confidentiality of RTP packets—protects packet-payloads from being read by unapproved entities but does so without authorized entities having to enter a secret encryption key.
- Message authentication of RTP packets—protects the integrity of the packet against forgery, alteration, or replacement.
- Replay protection—protects the session address against denial of service attacks.

Table 1 describes the security level of SIP INVITE messages according to which of the four possible combinations of TLS and SRTP is configured.

### Table 1 TLS-SRTP Combinations

<table>
<thead>
<tr>
<th>TLS</th>
<th>SRTP</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>On</td>
<td>On</td>
<td>Signaling and media are secure.</td>
</tr>
<tr>
<td>Off</td>
<td>On</td>
<td>Signaling is insecure:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- If you use the <code>srtp fallback</code> command, the gateway sends an RTP-only SDP.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- If you do not configure the <code>srtp fallback</code> command, the call fails and the gateway does not send an INVITE message.</td>
</tr>
</tbody>
</table>

**Note** In Cisco IOS Release 12.4(20)T and later releases (and, for Cisco UBEs, in Cisco IOS Release 12.4(22)T and later releases), calls established with SRTP only (and not SIPS) will succeed even if the `srtp fallback` command is not configured.

<table>
<thead>
<tr>
<th>TLS</th>
<th>SRTP</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>On</td>
<td>Off</td>
<td>RTP-only call.</td>
</tr>
<tr>
<td>Off</td>
<td>Off</td>
<td>Signaling and media are not secure.</td>
</tr>
</tbody>
</table>

### Cryptographic Parameters

RFC 3711 defines the SRTP cryptographic parameters, including valid syntax and values for attribute `a=crypto` (see Table 2). Some of these parameters are declarative and apply only to the send direction of the declarer, while others are negotiable and apply to both send and receive directions.
The following shows the cryptographic attribute syntax:
```
a=crypto:<tag> <crypto-suite> <key-params> [session-params]
```

Table 2 summarizes the syntax for the cryptographic attribute.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Optional</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tag</td>
<td>No</td>
<td>The tag attribute is a unique decimal number used as an identifier for a particular cryptographic attribute to determine which of the several offered cryptographic attributes was chosen by the answerer.</td>
</tr>
<tr>
<td>crypto-suite</td>
<td>No</td>
<td>The crypto-suite attribute defines the encryption and authentication algorithm. Cisco IOS voice gateways and Cisco UBEs support default suite AES_CM_128_HMAC_SHA1_32 (AES-CM encryption with a 128-bit key and HMAC-SHA1 message authentication with a 32-bit tag).</td>
</tr>
<tr>
<td>key-params</td>
<td>No</td>
<td>“inline:” &lt;key</td>
</tr>
<tr>
<td>session-params</td>
<td>Yes</td>
<td>The session-params attribute is specific to a given transport and is optional. The gateway does not generate any session-params in an outgoing INVITE message, nor will the SDP library parse them.</td>
</tr>
</tbody>
</table>

### SDP Negotiation

To allow calls to succeed between endpoints that do not support SRTP, you can enable SIP support for SRTP by configuring the `srtp` command but you can also enable fall back to the RTP mechanism in cases where SRTP is not supported by one or both endpoints. To configure a Cisco IOS voice gateway or Cisco Unified Border Element to fall back to RTP when SRTP is not supported, configure the `srtp fallback` command either globally or for an individual dial peer.

When the `srtp` command is enabled, the offer SDP in the INVITE message has only one m line for the RTP/SAVP (RTP/Secure AVP) transport type. If a called endpoint does not support SRTP, the call fails with a 4xx error. However, if you configure the `srtp fallback` command, the gateway generates another INVITE message with an RTP-only offer instead of simply allowing the call to fail.

**Note** In Cisco IOS Release 12.4(20)T and later releases (and, for Cisco UBEs, in Cisco IOS Release 12.4(22)T and later releases), calls established with SRTP only (and not SIPS) will succeed even if the `srtp fallback` command is not configured.

When the gateway or Cisco Unified Border Element is the called endpoint, it will accept an offer with an m line value of SRTP-only, RTP-only, or both SRTP and RTP. For calls with two m lines (SRTP and RTP), the negotiation depends on the configuration of the inbound dial peer or global configuration. Only one m line negotiates—the port number in the other m line is set to 0.

Table 3 summarizes the behavior of the gateway during negotiation.
Configuring SIP Support for SRTP

Information About Configuring SIP Support for SRTP

The following example shows an offer SDP with two m lines that use the cryptographic attribute for the RTP/SAVP media transport type:

```
v=0
o=CiscoSystemsSIP-GW-UserAgent 7826 3751 IN IP4 172.18.193.98
s=SIP Call
c=IN IP4 172.18.193.98
t=0 0
m=audio 1789 RTP/AVP 0
a=rtpmap:0 PCMU/8000
m=audio 51372 RTP/SAVP 0
a=rtpmap:0 PCMU/8000
a=crypto:1 AES_CM_128_HMAC_SHA1_32
inline:d0RmdmcmVCspeEc3QGZiNWpVLFJhQX1cfHAWJSoj|2^20|1:32
```

The following example shows the corresponding answer SDP with SRTP supported:

```
v=0
o=CiscoSystemsSIP-GW-UserAgent 7826 3751 IN IP4 172.18.193.98
s=SIP Call
c=IN IP4 172.18.193.98
t=0 0
m=audio 0 RTP/AVP 0
a=rtpmap:0 PCMU/8000
m=audio 49170 RTP/SAVP 0
a=rtpmap:0 PCMU/8000
a=crypto:1 AES_CM_128_HMAC_SHA1_32
inline:NzB4d1BINUAvLEw6UzF3WSdFcGdUJShpX1Zj|2^20|1:32
```

Table 3  Gateway Behavior During Negotiations

<table>
<thead>
<tr>
<th>Dial Peer Configuration</th>
<th>INVITE Message Received with SRTP</th>
<th>INVITE Message Received with SRTP and RTP</th>
<th>INVITE Message Received with RTP</th>
</tr>
</thead>
<tbody>
<tr>
<td>SRTP only</td>
<td>SRTP call.</td>
<td>SRTP call, port number in m line of RTP set to 0.</td>
<td>488 (unacceptable media).</td>
</tr>
<tr>
<td>SRTP with fallback</td>
<td>SRTP call.</td>
<td>SRTP call, port number in m line of RTP set to 0.</td>
<td>RTP call, port number in m line of SRTP set to 0.</td>
</tr>
<tr>
<td>No SRTP</td>
<td>488 (unacceptable media).</td>
<td>RTP call, port number in m line of SRTP set to 0.</td>
<td>RTP call.</td>
</tr>
</tbody>
</table>

The following example shows an offer SDP with two m lines that use the cryptographic attribute for the RTP/SAVP media transport type:

```
v=0
o=CiscoSystemsSIP-GW-UserAgent 7826 3751 IN IP4 172.18.193.98
s=SIP Call
c=IN IP4 172.18.193.98
t=0 0
m=audio 1789 RTP/AVP 0
a=rtpmap:0 PCMU/8000
m=audio 51372 RTP/SAVP 0
a=rtpmap:0 PCMU/8000
a=crypto:1 AES_CM_128_HMAC_SHA1_32
inline:d0RmdmcmVCspeEc3QGZiNWpVLFJhQX1cfHAWJSoj|2^20|1:32
```

Call Control and Signaling

SIP uses the SRTP library to receive cryptographic keys. If you configure SRTP for the call and cryptographic context is supported, SDP offers the cryptographic parameters. If the cryptographic parameters are negotiated successfully, the parameters are downloaded to the DSP, which encrypts and decrypts the packets. The sender encrypts the payload by using the AES algorithm and builds an authentication tag, which is encapsulated to the RTP packet. The receiver verifies the authentication tag and then decrypts the payload.
Default and Recommended SRTP Settings

Table 4 lists the default and recommended SRTP settings.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
<th>Recommended Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key derivation rate</td>
<td>0</td>
<td>0—Rekeying is supported</td>
</tr>
<tr>
<td>Master key length</td>
<td>128 bits</td>
<td>128 bits</td>
</tr>
<tr>
<td>Master salt key length</td>
<td>112 bits</td>
<td>112 bits</td>
</tr>
<tr>
<td>MKI indicator</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>MKI length</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PRF</td>
<td>AES_CM</td>
<td>128</td>
</tr>
<tr>
<td>Session authentication key length</td>
<td>128</td>
<td>128</td>
</tr>
<tr>
<td>Session encryption key length</td>
<td>128 bits</td>
<td>128 bits</td>
</tr>
<tr>
<td>Session salt key length</td>
<td>112</td>
<td>112</td>
</tr>
<tr>
<td>SRTP authentication</td>
<td>HMAC-SHA1</td>
<td>HMAC-SHA1</td>
</tr>
<tr>
<td>SRTCP authentication</td>
<td>HMAC-SHA1</td>
<td>HMAC-SHA1</td>
</tr>
<tr>
<td>SRTP cipher</td>
<td>AES_CM</td>
<td>AES_CM</td>
</tr>
<tr>
<td>SRTCP cipher</td>
<td>AES_CM</td>
<td>NULL</td>
</tr>
<tr>
<td>SRTP HMAC tag length</td>
<td>80</td>
<td>32 (voice)—Supported</td>
</tr>
<tr>
<td></td>
<td></td>
<td>80 (other)—Not supported</td>
</tr>
<tr>
<td>SRTCP HMAC tag length</td>
<td>80</td>
<td>80</td>
</tr>
<tr>
<td>SRTP packets maximum lifetime</td>
<td>$2^{48}$ packets</td>
<td>$2^{48}$ packets</td>
</tr>
<tr>
<td>SRTCP packets maximum lifetime</td>
<td>$2^{31}$ packets</td>
<td>$2^{31}$ packets</td>
</tr>
<tr>
<td>SRTP replay-window size</td>
<td>64</td>
<td>64—Not supported</td>
</tr>
<tr>
<td>SRTCP replay-window size</td>
<td>64</td>
<td>64—Not supported</td>
</tr>
</tbody>
</table>

Before an SRTP session can be established on a Cisco IOS voice gateway or Cisco UBE, the following cryptographic information must be exchanged in SDP between the two endpoints:

- Crypto suite—crypto algorithm \{AES_CM_128_HMAC_SHA1_32\} and the supported codec list \{g711, G729, G729a\}. There could be one or more crypto suites. Cisco IOS Release 12.4(15)T supports only one crypto suite.
- Crypto context—16-byte master key and a 14-byte master salt.

Generating Master Keys

The SRTP library provides an application program interface (API), srtp_generate_master_key, to generate a random master key. For encryption and authentication purposes, the key length is 128 bits (master key and session keys). Additionally, RFC 3711 introduces “salting keys”—master salts and sessions salts—and strongly recommends the use of a master salt in the key derivation of session keys. The salting keys (salts) are used to fight against pre-computation and time-memory tradeoff attacks.
The master salt (also known as the n-bit SRTP key) prevents off-line key-collision attacks on the key derivation and, when used, must be random (but can be public). The master salt is derived from the master key and is used in the key derivation of session keys. Session salts, in turn, are used in encryption to counter various attacks against additive stream ciphers. All salting keys (master salt and session salts) are 112 bits.

**SRTP Offer and Answer Exchange**

If you configure the gateway for SRTP (globally or on an individual dial peer) and end-to-end TLS, an outgoing INVITE message has cryptographic parameters in the SDP.

If you use the `srtp fallback` command and the called endpoint does not support SRTP (offer is rejected with a 4xx class error response), the gateway or Cisco Unified Border Element sends an RTP offer SDP in a new INVITE request. If you do not configure the `srtp fallback` command, the call fails.

---

**Note**

In Cisco IOS Release 12.4(20)T and later releases (and, for Cisco UBEs, in Cisco IOS Release 12.4(22)T and later releases), calls established with SRTP only (and not SIPS) will succeed even if the `srtp fallback` command is not configured.

When a gateway or Cisco Unified Border Element receives an SRTP offer, negotiation is based on the inbound dial peer if specified and, if not, the global configuration. If multiple cryptographic attributes are offered, the gateway selects an SRTP offer it supports (AES_CM_128_HMAC_SHA1_32). The cryptographic attribute will include the following:

- The tag and same crypto suite from the accepted cryptographic attribute in the offer.
- A unique key the gateway generates from the SRTP library API.
- Any negotiated session parameters and its own set of declarative parameters, if any.

If this cryptographic suite is not in the list of offered attributes, or if none of the attributes are valid, the SRTP negotiation fails. If the INVITE message contains an alternative RTP offer, the gateway (or Cisco UBE) negotiates and the call falls back to (nonsecure) RTP mode. If there is no alternative offer and the SRTP negotiation fails, the INVITE message is rejected with a 488 error (Not Acceptable Media).

**Rekeying Rules**

There is no rekeying on an SRTP stream. A REINVITE/UPDATE message is used in an established SIP call to update media-related information (codec, destination address, and port number) or other features, such as call-hold. A new key need only be generated if the offer SDP has a new connection address or port. Because the source connection address and port do not change, the gateway or Cisco UBE will not generate a new master key after a key has been established for an SRTP session.
Call-Feature Interactions

This section describes call-feature interactions when SIP Support for SRTP features are configured.

Call Hold

If a gateway receives a call hold REINVITE message after an initial call setup is secured, the gateway places the existing SRTP stream on hold, and its answer in the 200 OK message depends on the offer SDP. If there is a cryptographic attribute in the offer, the gateway responds with a cryptographic attribute in its answer.

Signaling Forking

A proxy can fork an INVITE message that contains an SRTP offer, which can result in multiple SRTP streams until a 200 OK message is received. Because the gateway always honors the last answer, the gateway deletes previous SRTP streams and creates a new stream to the latest endpoint. Other endpoints might also stream to the gateway, but because the DSP knows only the last streams’s cryptographic suite and key, authentication on these packets fails, and the packets are dropped.

Call Redirection

A gateway redirects a call when an INVITE message, sent to a proxy or redirect server, results in a 3xx response with a list of redirected contact addresses. The gateway handles a 3xx response based on the schema in the contact of a 3xx message. If the message is SIP, and you configure the call for SRTP with fallback, the gateway offers an SRTP-only redirected INVITE message. If you configure for SRTP only, the offer is SRTP only.

If the schema is SIP, and you use the `srtp fallback` command to configure the call for RTP with fallback, the INVITE message has an RTP offer. If you do not configure the `srtp fallback` command, the call fails.

Note

In Cisco IOS Release 12.4(20)T and later releases (and, for Cisco UBEs, in Cisco IOS Release 12.4(22)T and later releases), calls established with SRTP only (and not SIPS) will succeed even if the `srtp fallback` command is not configured.

Call Transfer

The SIP Support for SRTP feature interaction with call transfer depends on your outbound dial peer or global configuration. During a call transfer, the gateway sends an INVITE message to establish the connection to the transfer target. The gateway includes an SRTP offer in the INVITE message if the outbound dial peer or global configuration includes the SRTP offer.

T.38 Fax

The T.38 transport supported is User Datagram Protocol (UDP). A T.38 call is initiated as a voice call, which can be RTP or SRTP, and when it switches to T.38 fax mode, the fax call is not secure. When the fax is switched back to voice, the call returns to its initial voice state.

Conferencing Calls

For conferencing calls, the incoming INVITE message does not match any inbound dial peer and the message body is sent to the application in a container. The conferencing application performs the necessary negotiation and replies through PROGRESS or CONNECT events.
How to Configure SIP Support for SRTP

Before configuring SIP support for SRTP on a gateway or Cisco Unified Border Element, it is strongly recommended you first configure SIPS either globally or on an individual dial peer basis. The configuration on a dial peer overrides the global configuration.

This section contains the following configurations:
- Configuring SIPS Globally, page 9 (optional)
- Configuring SIPS on a Dial Peer, page 10 (optional)
- Configuring SRTP and SRTP Fallback Globally, page 11 (required)
- Configuring SRTP and SRTP Fallback on a Dial Peer, page 12 (optional)

Configuring SIPS Globally

To configure secure SIP (SIPS) globally on a Cisco IOS voice gateway or Cisco Unified Border Element, perform the following steps.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. voice service {pots | voatm | vofr | voip}
4. sip
5. url sips
6. exit

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 1    | enable            | Enables privileged EXEC mode.  
|      |                   | • Enter your password if prompted. |
| 2    | configure terminal| Enters global configuration mode. |
| 3    | voice service {pots | voatm | vofr | voip} | Enters voice service configuration mode. |
| 4    | sip               | Enters SIP configuration mode. |

**Example:**

Router> enable
Router# configure terminal
Router(config)# voice service voip
Router(config)# sip
Configuring SIP Support for SRTP

1. **Configuring SIPS on a Dial Peer**

   To configure secure SIP (SIPS) on an individual dial peer, perform the following steps.

   **SUMMARY STEPS**
   
   1. `enable`
   2. `configure terminal`
   3. `dial-peer voice tag {pots | vofr | voip}`
   4. `voice-class sip url sips`
   5. `exit`

   **DETAILED STEPS**
   
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> <code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><code>Router&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> `dial-peer voice tag {pots</td>
<td>vofr</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router(config)# dial-peer voice 111 voip</code></td>
<td></td>
</tr>
</tbody>
</table>
Configuring SIP Support for SRTP

How to Configure SIP Support for SRTP

To configure SRTP and SRTP fallback behavior globally on a Cisco IOS voice gateway or Cisco Unified Border Element, perform the following steps.

SUMMARY STEPS

1. enable
2. configure terminal
3. voice service {pots | voatm | vofr | voip}
4. srtp
5. srtp fallback
6. exit

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>Example: Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> voice service {pots</td>
<td>voatm</td>
</tr>
<tr>
<td>Example: Router(config)# voice service voip</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> srtp</td>
<td>Configures secure RTP calls.</td>
</tr>
<tr>
<td>Example: Router(conf-voi-serv)# srtp</td>
<td></td>
</tr>
</tbody>
</table>
Configuring SIP Support for SRTP

How to Configure SIP Support for SRTP

1. To configure SRTP and SRTP fallback behavior on an individual dial peer that overrides the global SRTP configuration, perform the following steps.

<table>
<thead>
<tr>
<th>SUMMARY STEPS</th>
<th>DETAILED STEPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. enable</td>
<td>Step 1: enable</td>
</tr>
<tr>
<td>2. configure terminal</td>
<td>Step 2: configure terminal</td>
</tr>
<tr>
<td>3. dial-peer voice tag {pots</td>
<td>vofr</td>
</tr>
<tr>
<td>4. srtp</td>
<td>Step 4: srtp</td>
</tr>
<tr>
<td>5. srtp fallback</td>
<td></td>
</tr>
<tr>
<td>6. exit</td>
<td>Step 6: exit</td>
</tr>
</tbody>
</table>

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Step 3 dial-peer voice tag {pots</td>
<td>vofr</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Step 4 srtp</td>
<td>Configures secure RTP calls.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>

**Command or Action**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 5 srtp fallback</td>
<td>Configures a fallback to RTP calls in case secure RTP calls fail due to lack of support from an endpoint.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Step 6 exit</td>
<td>Exits the current mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
### Configuration Examples for Configuring SIP Support for SRTP

The following example shows how to configure SIPS globally on a Cisco IOS voice gateway or Cisco Unified Border Element:

```
Router> enable
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# url sips
Router(conf-serv-sip)# exit
```

The following example shows how to configure SIPS on dial peer 111:

```
Router> enable
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# dial-peer voice 111 voip
Router(config-dial-peer)# voice-class sip url sips
Router(config-dial-peer)# exit
```

The following example shows how to configure SRTP with fallback to RTP globally on a Cisco IOS voice gateway or Cisco Unified Border Element:

```
Router> enable
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# voice service voip
Router(conf-voi-serv)# sip
Router(conf-voi-serv)# srtp
Router(conf-voi-serv)# exit
```

The following example shows how to configure for SRTP with fallback to RTP on dial peer 111:

```
Router> enable
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# dial-peer voice 111 voip
Router(config-dial-peer)# srtp
Router(config-dial-peer)# srtp fallback
Router(config-dial-peer)# exit
```

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>srtp fallback</td>
<td>Configures a fallback to RTP calls in case secure RTP calls fail due to lack of support from an endpoint.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-dial-peer)# srtp fallback</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>exit</td>
<td>Exits the current mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config-dial-peer)# exit</td>
<td></td>
</tr>
</tbody>
</table>
Additional References

The following sections provide references related to configuring the SIP Support for SRTP features.

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS dial peer overview</td>
<td>Dial Peer Overview</td>
</tr>
<tr>
<td>Cisco IOS dial technologies command information</td>
<td>Cisco IOS Dial Technologies Command Reference</td>
</tr>
<tr>
<td>Cisco IOS SIP features, listed by release</td>
<td>SIP Features Roadmap</td>
</tr>
<tr>
<td>Cisco IOS SIP overview and related documents</td>
<td>Overview of SIP</td>
</tr>
<tr>
<td>Cisco IOS software configuration guides</td>
<td>• Cisco IOS Dial Technologies Configuration Guide</td>
</tr>
<tr>
<td></td>
<td>• Cisco IOS SIP Configuration Guide</td>
</tr>
<tr>
<td></td>
<td>Note To locate the configuration guide specific to</td>
</tr>
<tr>
<td></td>
<td>your Cisco IOS software release, choose the Cisco</td>
</tr>
<tr>
<td></td>
<td>IOS and NX-OS Software category on the Product</td>
</tr>
<tr>
<td></td>
<td>Support page and navigate according to your release</td>
</tr>
<tr>
<td>Cisco IOS voice command information</td>
<td>Cisco IOS Voice Command Reference</td>
</tr>
<tr>
<td>Cisco IOS voice configuration information</td>
<td>Cisco IOS Voice Configuration Library</td>
</tr>
<tr>
<td>Cisco Unified Border Element configuration</td>
<td>Cisco Unified Border Element Configuration Guide</td>
</tr>
<tr>
<td>information</td>
<td></td>
</tr>
<tr>
<td>Cisco Unified CME command information</td>
<td>Cisco Unified Communications Manager Express Command Reference</td>
</tr>
<tr>
<td>Cisco Unified CME configuration information</td>
<td>Cisco Unified CME Support Documentation Home Page</td>
</tr>
</tbody>
</table>

RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>draft-ietf-mmusic-sdescriptions-08.txt</td>
<td>Session Description Protocol Security Descriptions for Media Streams</td>
</tr>
<tr>
<td>RFC 3263</td>
<td>Session Initiation Protocol (SIP): Locating SIP Servers</td>
</tr>
<tr>
<td>RFC 3711</td>
<td>The Secure Real-time Transport Protocol (SRTP)</td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases,</td>
</tr>
<tr>
<td></td>
<td>and feature sets, use Cisco MIB Locator found at the following URL:</td>
</tr>
<tr>
<td></td>
<td><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>
Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including</td>
<td><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></td>
</tr>
<tr>
<td>documentation and tools for troubleshooting and resolving technical issues</td>
<td></td>
</tr>
<tr>
<td>with Cisco products and technologies.</td>
<td></td>
</tr>
<tr>
<td>To receive security and technical information about your products, you can</td>
<td></td>
</tr>
<tr>
<td>subscribe to various services, such as the Product Alert Tool (accessed from</td>
<td></td>
</tr>
<tr>
<td>Field Notices), the Cisco Technical Services Newsletter, and Really Simple</td>
<td></td>
</tr>
<tr>
<td>Syndication (RSS) Feeds.</td>
<td></td>
</tr>
<tr>
<td>Access to most tools on the Cisco Support website requires a Cisco.com user</td>
<td></td>
</tr>
<tr>
<td>ID and password.</td>
<td></td>
</tr>
</tbody>
</table>
Feature Information for Configuring SIP Support for SRTP

Table 5 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.2(1) or Cisco IOS Releases 12.2(1) or 12.0(3)S or a later release appear in the table.

For information on a feature in this technology that is not documented here, see the Cisco IOS SIP Features Roadmap module at http://www.cisco.com/en/US/docs/ios/voice/sip/configuration/guide/sip_cg-roadmap.html.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note

Table 5 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release. Unless noted otherwise, subsequent releases of that Cisco IOS software release also support that feature.

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP Support for SRTP</td>
<td>12.4(15)T</td>
<td>This feature introduces SIP support for supplementary services features, such as call hold, call transfer, call waiting, and call conference (3WC) using hook flash (HF) for FXS phones on Cisco IOS voice gateways. The following commands were introduced or modified: srtp, srtp fallback.</td>
</tr>
<tr>
<td>SIP SRTP Fallback to Nonsecure RTP</td>
<td>12.4(15)XY 12.4(20)T</td>
<td>This feature extends the existing SRTP to RTP fallback on Cisco IOS voice gateways to support a delayed offer and adds support for SRTP over SIP. The following commands were introduced or modified: srtp negotiate, voice-class sip srtp negotiate.</td>
</tr>
<tr>
<td>Interworking of Secure RTP calls for SIP and H323</td>
<td>12.4(20)T</td>
<td>This feature provides an option for a Secure RTP (SRTP) call to be connected from H323 to SIP and from SIP to SIP. Additionally, this feature extends SRTP fallback support from the Cisco IOS voice gateway to the Cisco Unified Border Element. This feature uses no new or modified commands.</td>
</tr>
</tbody>
</table>
### Table 5  Feature Information for Configuring SIP Support for SRTP (continued)

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
</table>
| SIP SRTP Fallback to Nonsecure RTP for Cisco Unified Border Elements         | 12.4(22)T | This feature adds support for both SRTP to RTP fallback with a delayed offer and SRTP over SIP to the Cisco Unified Border Element.  
This feature uses no new or modified commands.                                |
| Cisco Unified Border Element Support for SRTP-RTP Internetworking            | 12.4(22)YB | This feature provides the ability to support interworking between SRTP on one IP leg and RTP on another IP leg of a Cisco Unified Border Element.  
The following command was introduced or modified: **tls**.                      |
Glossary

AVP—Audio/Video Profile.
CAC—Call Admission Control.
CME—Communications Manager Express.
CVP—Customer Voice Portal.
GW—gateway.
ISDN—Integrated Services Digital Network.
MIME—Multipurpose Internet Mail Extensions.
m line—The media-level section of an SDP session begins and ends with an “m” line that confines the information about the media stream.
MOH—music on hold.
OGW—originating gateway (ingress gateway).
PBX—Private Branch Exchange.
PINX—private integrated services network exchange.
PISN—private integrated services network.
QoS—quality of service.
QSIG—Q Signaling protocol.
RSVP—Resource Reservation Protocol.
RTP—Real-time Transport Protocol.
SDP—Session Description Protocol.
SIP—Session Initiation Protocol.
SRTP—Secure Real-time Transport Protocol.
TDM—time-division multiplexing.
TGW—terminating gateway (egress gateway).
UA—user agent.
UDP—User Datagram Protocol.
URI—uniform resource identifier.