



SRTP-SRTP Pass-Through

SRTP-SRTP pass-through feature allows pass-through of encrypted media from one call-leg to the other.

- [Feature Information for Support of SRTP-SRTP Pass-Through Calls, on page 1](#)
- [Information About SRTP-SRTP Pass-Through, on page 2](#)
- [Configure Pass-Through of Unsupported Crypto Suites for a Specific Dial Peer, on page 3](#)
- [Configure Pass-Through of Unsupported Crypto Suites Globally, on page 5](#)
- [Configuration Examples for SRTP-SRTP Pass-Through, on page 6](#)

Feature Information for Support of SRTP-SRTP Pass-Through Calls

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://cfng.cisco.com/>. An account on Cisco.com is not required.

Table 1: Feature Information for SRTP-SRTP Pass-Through

Feature Name	Releases	Feature Information
Support for SRTP-SRTP Basic calls	12.4.15XZ	This feature introduced support for basic SRTP-SRTP pass-through calls.
Support for AES_CM_128_HMAC_SHA1_80 crypto suite	Cisco IOS 15.4(1)T Cisco IOS XE 3.11S	Support AES_CM_128_HMAC_SHA1_80 crypto suite on the Session Initiation Protocol (SIP) Trunk interface was introduced. The following commands were introduced or modified: show sip-ua srtp , srtp-auth and voice-class sip srtp-auth .

Feature Name	Releases	Feature Information
Enhanced Support for SRTP-SRTP Pass-Through	Cisco IOS 15.6(1)T Cisco IOS XE 3.17S	Introduced support for pass-through of the following unsupported crypto suites: <ul style="list-style-type: none"> • AEAD_AES_128_GCM • AEAD_AES_256_GCM • AEAD_AES_128_CCM • AEAD_AES_256_CCM <p>The srtp command was modified to add pass-thru keyword.</p>

Information About SRTP-SRTP Pass-Through

Cisco Unified Border Element supports SIP calls between endpoints using Transport Layer Security (TLS) for SIP signaling encryption and Secure Real-Time Protocol (SRTP) to provide RTP media encryption. However, these two encryption mechanisms may not be deployed simultaneously, depending on the required call flow invoked on the associated configuration.

The following are conditions of the SRTP Passthrough feature:

- SRTP Passthrough must be configured on both legs of the call. If the target adjacency does not support SRTP Passthrough, then the call is rejected by error message 415 (Unsupported Media Type).
- "m= .. RTP/SAVP .." and a="crypto:..." fields coming in on an Invite from one adjacency are passed on in an Invite to the target adjacency.
- "m= ...RTP/SAVP..." is a required field in the Invite to trigger SRTP Passthrough behavior in the SBC.

Pass-Through of Unsupported Crypto Suites



Note Effective from Cisco IOS XE Everest Release 16.5.1b, CUBE supports AEAD_AES_128_GCM and AEAD_AES_256_GCM crypto-suites. For more information, see [SRTP-SRTP Interworking](#).

CUBE supports transparent passthrough of all (supported and unsupported) crypto suites.

Until Cisco IOS Release 15.6(1)T and Cisco IOS XE Release 3.17S, CUBE and DSP supported SRTP pass-through only for AES_CM_128_HMAC_SHA1_80 crypto suite.

From Cisco IOS Release 15.6(1)T and Cisco IOS XE Release 3.17S onwards, CUBE supports pass-through of the following unsupported crypto suites:

- AEAD_AES_128_GCM
- AEAD_AES_256_GCM
- AEAD_AES_128_CCM

- AEAD_AES_256_CCM

CUBE has the ability to pass across crypto attributes (containing any unsupported crypto suites) as well as media packets (encrypted with unsupported crypto suites).

If SRTP pass-thru feature is enabled, media interworking will not be supported. Ensure that you have symmetric configuration on both the incoming and outgoing dial-peers to avoid media-related issues.

Configure Pass-Through of Unsupported Crypto Suites for a Specific Dial Peer

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice tag voip**
4. **destination-pattern string**
5. **session protocol sipv2**
6. **sessiontarget ipv4: destination-address**
7. **incoming called-number string**
8. **srtp pass-thru**
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 pass-thru**
14. **codec codec**
15. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	dial-peer voice tag voip Example: <pre>Device(config)# dial-peer voice 201 voip</pre>	Defines a particular dial peer, to specify the method of voice encapsulation, and enters dial peer voice configuration mode. <ul style="list-style-type: none"> In the example, the following parameters are set: <ul style="list-style-type: none"> Dial peer 201 is defined. VoIP is shown as the method of encapsulation.
Step 4	destination-pattern string Example: <pre>Device(config-dial-peer)# destination-pattern 5550111</pre>	Specifies either the prefix or the full E.164 telephone number to be used for a dial peer string. <ul style="list-style-type: none"> In the example, 5550111 is specified as the pattern for the telephone number.
Step 5	session protocol sipv2 Example: <pre>Device(config-dial-peer)# session protocol sipv2</pre>	Specifies a session protocol for calls between local and remote routers using the packet network. <ul style="list-style-type: none"> In the example, the sipv2 keyword is configured so that the dial peer uses the IETF SIP.
Step 6	sessiontarget ipv4: destination-address Example: <pre>Device(config-dial-peer)# session target ipv4:10.13.25.102</pre>	Designates a network-specific address to receive calls from a VoIP or VoIPv6 dial peer. <ul style="list-style-type: none"> In the example, the IP address of the dial peer to receive calls is configured as 10.13.25.102.
Step 7	incoming called-number string Example: <pre>Device(config-dial-peer)# incoming called-number 5550111</pre>	Specifies a digit string that can be matched by an incoming call to associate the call with a dial peer. <ul style="list-style-type: none"> In the example, 5550111 is specified as the pattern for the E.164 or private dialing plan telephone number.
Step 8	srtp pass-thru Example: <pre>Device(config-dial-peer)# srtp pass-thru</pre>	Enables transparent passthrough of all crypto suites for a specific dial peer.
Step 9	codec codec Example: <pre>Device(config-dial-peer)# codec g711ulaw</pre>	Specifies the voice coder rate of speech for the dial peer. <ul style="list-style-type: none"> In the example, G.711 mu-law at 64,000 bps, is specified as the voice coder rate for speech.
Step 10	end Example: <pre>Device(config-dial-peer)#end</pre>	Exits dial peer voice configuration mode.

	Command or Action	Purpose
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. <ul style="list-style-type: none"> • In the example, the following parameters are set: <ul style="list-style-type: none"> • 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 pass-thru Example: Device(config-dial-peer)# srtp pass-thru	Enables transparent passthrough of all crypto suites for a specific dial peer.
Step 14	codec codec Example: Device(config-dial-peer)# codec g711ulaw	Specifies the voice coder rate of speech for the dial peer. <ul style="list-style-type: none"> • 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.

Configure Pass-Through of Unsupported Crypto Suites Globally

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **srtp pass-thru**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.

	Command or Action	Purpose
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	voice service voip Example: Device(config)# voice service voip	Enters VoIP voice-service configuration mode.
Step 4	srtp pass-thru Example: Device(config-dial-peer)# srtp pass-thru	Enables transparent passthrough of all crypto suites globally.
Step 5	end Example: Device(config-dial-peer)# end	Exits dial peer voice configuration mode.

Configuration Examples for SRTP-SRTP Pass-Through

Example for SRTP=SRTP Pass-Through

```
enable
configure terminal
dial-peer voice 201 voip
destination-pattern 5550111
session protocol sipv2
session target ipv4:10.13.25.102
incoming called-number 5550111
srtp
codec g711ulaw
end

dial-peer voice 200 voip
destination-pattern 5550111
session protocol sipv2
session target ipv4:10.13.25.101
incoming called-number 5550111
srtp
codec g711ulaw
end
```

Example for Pass-Through of Unsupported Crypto Suites for a specific dial peer

```
enable
configure terminal
```

```
dial-peer voice 201 voip
destination-pattern 5550111
session protocol sipv2
session target ipv4:10.13.25.102
incoming called-number 5550111
srtp pass-thru
codec g711ulaw
end
```

```
dial-peer voice 200 voip
destination-pattern 5550111
session protocol sipv2
session target ipv4:10.13.25.101
incoming called-number 5550111
srtp pass-thru
codec g711ulaw
end
```

Example for Pass-Through of Unsupported Crypto Suites Globally

```
enable
configure terminal
voice service voip
srtp pass-thru
end
```

