Configuring Secure SCCP Analog Endpoints over TLS with Cisco Unified Communications Manager

First Published: November 19, 2010
Last Updated: June 29, 2015

This module describes how the Secure Skinny Client Control Protocol (SCCP) enhances SCCP telephony control (STC) application (STCAPP) Foreign Exchange Station (FXS) security analog endpoints through secure signaling and media encryption using Transport Layer Security (TLS). This feature is supported for analog SCCP endpoints that are controlled by the Cisco Unified Communications Manager (Cisco Unified CM) only.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the "Feature Information for Secure SCCP Analog Endpoints over TLS with Cisco Unified CM" section on page 224.

Finding Support Information for Platforms and Cisco IOS Software Images

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.

Contents

Prerequisites for Secure SCCP Analog Endpoints over TLS with Cisco Unified CM

Secure SCCP Analog Endpoints over TLS with Cisco Unified CM require the following software component:

- Cisco Unified CM 8.5 or later

Cisco IOS Voice Gateway

- Cisco IOS Release 15.1(3)T or a later version
- Cisco voice gateway is set up and configured for operation. For information, see the appropriate Cisco configuration documentation.
- Analog FXS voice ports are set up and configured for operation. For information, see *Cisco IOS Voice Port Configuration Guide*.
- SCCP and the STCAPP are enabled on the Cisco voice gateway. For configuration information, see *Configuring FXS Ports for Basic Calls*.

Restrictions for Secure SCCP Analog Endpoints over TLS with Cisco Unified CM

- This feature supports only the following Cisco IOS platforms:
  - Cisco ISR 1861/2801/2811/2821/2851/3825/3845
  - Cisco ISR G2 2901/2911/2921/2951/3925/3945/3925E/3945E
  - Cisco VG202/VG204/VG224

Benefits of Secure SCCP Analog Endpoints over TLS with Cisco Unified CM

The Secure SCCP enhances STCAPP FXS analog endpoints through signaling integrity and media encryption using TLS and Secured Real-time Transport Protocol (SRTP) with Cisco Unified CM.

This feature provides parity with incumbent time-division multiplexing systems.

Information About Secure SCCP Analog Endpoints over TLS with Cisco Unified CM

To enable SCCP supplementary features on analog phones connected to FXS ports on a Cisco voice gateway, you should understand the following concept:

Secure SCCP Analog Endpoints over TLS with Cisco Unified CM

In a nonsecure Cisco Unified CM-gateway environment, the SCCP connection between the Cisco Unified CM and the Cisco IOS Voice Gateway is established through a TCP connection on port 2000 and media between the gateway and the Cisco Unified CM is RTP. Since these connections are not encrypted, hackers create damage by disrupting signaling or by listening to the media connection.

The Secure SCCP over TLS feature enhances STCAPP security endpoints by using an existing Cisco IOS Public Key Infrastructure (PKI) to manage security certificates on Cisco IOS Voice Gateways and connect to the Cisco Unified CM.

This feature aims to provide call signaling integrity and media encryption in the IP telephony environment through the following:

- SCCP signaling authentication, integrity and encryption using TLS, page 215
- Media protection by SRTP, page 216

SCCP signaling authentication, integrity and encryption using TLS

Dynamic, secure SCCP signaling per media channel instead of secure signaling through the IPSEC tunnel, which is complex to configure in large-scale deployments, complements the secure media through SRTP and avoids the complexity necessary to setup static IPSEC tunnels.

Signaling can be secured by implementing a secure TLS connection between multiple IOS SCCP Analog Voice Gateways and the Cisco Unified CM through the following steps:

- Establish an identity for the STCAPP by getting a digital security certificate (that contains public keys used for encryption and digital signatures) from a root Certificate Authority (CA) server used by both the Cisco Unified CM and the STCAPP.

  Note Since the gateway is running the Cisco IOS with a PKI subsystem there is no need for a proxy function called the Certificate Authority Proxy Function (CAPF) to issue certificates. For Cisco Unified CM, any third-party CA supporting standards based on the Simple Certificate Exchange Protocol (SCEP) or a dedicated Cisco IOS router acts as a CA server. The Cisc o Unified CM can also get a certificate from the Cisco IOS CA server using built-in support to manually request and import certificates from external CAs. Each Cisco IOS Voice Gateway receives its own security certificate from the Cisco IOS CA server through PKI autoprovisioning to allow large-scale deployments.

- Establish an identity for the gateway and Cisco Unified CM by getting a certificate from the same root CA. The TLS uses a standard handshake with mutual authentication. The gateway and the Cisco Unified CM authenticate each other by exchanging and validating the certificates during the TLS handshake. In addition to the standard TLS handshake, the Cisco Unified CM also examines the device name or MAC address from the gateway's certificate Subject field.

  Note Registration is rejected and an error message indicating a mismatch in the configuration is received when a secure gateway attempts to register with a nonsecure Cisco Unified CM or a nonsecure gateway attempts to register with a secure Cisco Unified CM.

Theoretically, up to 24 certificates can be issued to each of the 24 analog phones on the Cisco VG224 Voice Gateway. However, only one certificate is issued to a single VG224 box with all the analog phones sharing this certificate while establishing TLS connection to the Cisco Unified CM. The reasons for this are:

- Each analog port with its own certificate consumes a large amount of NVRAM memory, which is limited on Cisco IOS platforms.
- There is no significant enhancement in security with individual certificates for each analog port because of the single data path between Cisco Unified CM and the gateway.

Media protection by SRTP

SRTP is used to encrypt the call control signaling and the media streams from one end to the other for IP endpoints. For media encryption, the two analog endpoints controlled by the Cisco Unified CM exchange keys used to encrypt and decrypt the call control signaling packets. The transmission end has a key (tx key) used to encrypt the packets while the receiving end has a similar key (rx key) required to decrypt the packets. To decrypt the packets properly, the receiving end's "rx key" must be similar to the transmitter's "tx key".

Media protection involves the following:

- Security keys generation and the distribution, page 216
- Media security through digital signal processor (DSP) programming using security keys, page 216

Security keys generation and the distribution

The security keys are generated at the Cisco Unified CM and distributed to the SCCP analog endpoints as part of the SCCP signaling messages over the TLS protocol.

Media security through digital signal processor (DSP) programming using security keys

The SCCP FXS analog endpoints using the PVDM2 and PVDM3 packet voice DSP modules are supported.

To achieve media security through SRTP with secure capable end points, the SRTP keys are exchanged before the media really starts or the commands are sent to the endpoints.

The DSP is programmed by the Cisco IOS to use SRTP after the DSP is put in voice mode. A DSP channel (associated with a call leg) toggles from secure to nonsecure modes and vice versa when supplementary services are used. The DSP is reprogrammed based on the instructions from the application. The reprogramming of the DSP occurs after the DSP is reset and put in voice mode.

How to Configure Secure SCCP Analog Endpoints over TLS with Cisco Unified CM

Note This document does not contain details about configuring Cisco Unified CM or an IOS CA server. See the documentation for these products for installation and configuration instructions.

To enable dynamic, secure SCCP signaling to complement secure media through SRTP on a Cisco voice gateway connected to a Cisco Unified CM, perform the following tasks:

- Creating a Trustpoint on a Cisco IOS Voice Gateway, page 217
- Configuring Secure SCCP Analog Endpoints over TLS with Cisco Unified CM, page 220

Creating a Trustpoint on a Cisco IOS Voice Gateway

To create a security trustpoint on a Cisco IOS gateway, perform the following steps:

Note While using Cisco Voice Gateway 3xx Series (VG 310, VG 320, VG 350), activate securityK9 licenses for enabling secure SRTP Calls.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint** *label*
4. **enrollment url** *ca-url*
5. **serial-number** [**none**]
6. **fqdn** [***name*** | **none**]
7. **ip-address none**
8. **subject-name cn=***AA:BB:CC:DD:EE*
9. **revocation-check** [**none**]
10. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**crypto pki trustpoint** *label* **Example:** `Router(config)# crypto pki trustpoint VG224`	Specifies a trustpoint that your registration authority mode certificate server should use and enters CA-trustpoint configuration mode. • *label*—Name for the trustpoint and registration authority.
Step 4	**enrollment url** *ca-url* **Example:** `Router(ca-trustpoint)# enrollment url http://1.4.32.7:80`	Specifies the enrollment URL of the issuing CA certificate server (root certificate server). • *ca-url*—URL of the router on which the root CA has been installed.
Step 5	**serial-number** [**none**] **Example:** `Router(ca-trustpoint)# serial-number none`	Specifies whether the router serial number should be included in the certificate request. • **none**—(Optional) Specifies that a serial number will not be included in the certificate request.
Step 6	**fqdn** [*name* | **none**} **Example:** `Router(ca-trustpoint)# fqdn none`	Specifies a fully qualified domain name to be included in the certificate request. • ***name***—FQDN that will be included as "unstructured Name" in the certificate request. • **none**—Router FQDN will not be included in the certificate request.
Step 7	**ip-address none** **Example:** `Router(ca-trustpoint)# ip-address none`	Specifies a dotted IP address or an interface to be included as "unstructuredAddress" in the certificate request. • **none**—Specifies that an IP address is not to be included in the certificate request.
Step 8	**subject-name cn=***AA:BB:CC:DD:EE* **Example:** `Router(ca-trustpoint)# subject-name cn=11:22:22:11:11`	Specifies the subject name in the certificate request. • **cn=***AA:BB:CC:DD:EE*—last 10 digit of SCCP Interface MAC address

	Command or Action	Purpose
Step 9	**revocation-check** [**none**] **Example:** `Router(ca-trustpoint)# revocation-check none`	Checks the revocation status of a certificate and specifies a method to check the status. • **none**—(Optional) Certificate checking is not required.
Step 10	**exit** **Example:** `Router(config)# exit`	Exits CA-trustpoint configuration mode.

Configuring Secure SCCP Analog Endpoints over TLS with Cisco Unified CM

Note This document does not contain details about configuring STCAPP. For more information, see the "Enabling SCCP on the Voice Gateway" section on page 21.

To configure secure SCCP analog endpoints, perform the following steps on the Cisco IOS voice gateway:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **stcapp security trustpoint** *line*
4. **stcapp security** *mode* {**authenticated** | **encrypted** | **none**}
5. **stcapp**
6. **dial-peer voice** *tag* **pots**
7. **security mode** [**authenticated** | **encrypted** | **none**]
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**stcapp security trustpoint** *line* **Example:** `Router(config)# stcapp security trustpoint VG204`	Enables security for STCAPP endpoints and specifies the trustpoint to be used for setting up the TLS connection. • *line*—Security trustpoint for the STCAPP endpoint.

	Command or Action	Purpose
Step 4	**stcapp security** *mode* {**authenticat4ed** | **encrypted** | **none**} **Example:** `Router(config)# stcapp security mode encrypted`	Enables STCAPP endpoints and specifies the global security mode to be used for setting up the TLS connection. • **authenticated**—Security mode is authenticated and enables SCCP signaling between the voice gateway andthe Cisco Unified CM through the secure TLS connection. • **encrypted**—Security mode is encrypted. STCAPP endpoints are encrypted using data encryptionthrough SRTP. • **none**—Security mode is disabled. Defaults to global configuration mode.
Step 5	**stcapp** **Example:** `Router(config)# stcapp`	Enables the STCAPP feature. **Note** Both the stcapp security trustpoint and the stcapp security mode must be entered to enable security for the STCAPP endpoints.
Step 6	**dial-peer voice** *tag* **pots** **Example:** `Router(config)# dial-peer voice 1 pots`	(Optional) Enters dial peer voice configuration mode. • *tag*—Digits that define a particular dial peer. Range: 1 to 2147483647. • **pots**—Indicates that this is a POTS peer that uses VoIP encapsulation on the IP backbone.
Step 7	**security mode** [**authenticated** |**encrypted** | **none**] **Example:** `Router(config-dialpeer)# security mode encrypted`	(Optional) Enables dial-peer level STCAPP endpoint security and overrides global configuration. • **authenticated**—Enables STCAPP endpoints using signaling authentication. • **encrypted**—Enables STCAPP endpoints using data encryption. • **none**—Disables dial-peer-level STCAPP endpoint security configuration and defaults to global level configuration.
Step 8	**end** **Example:** `Router(config-dialpeer)# end`	Exits dial-peer configuration mode and returns to privileged EXEC mode.

Configuration Examples for Secure SCCP Analog Endpoints over TLS with Cisco Unified CM

This section provides the following configuration examples:

- Example: Configuring a Cisco IOS CA Server, page 222
- Example: Configuring a Cisco IOS VG224 Voice Gateway, page 222

Example: Configuring a Cisco IOS CA Server

The following example shows how to configure a Cisco IOS CA server, where the IP address of the CA server is entered as the enrollment url:

```
Router# show run
.
.
.
crypto pki server cserver1
 grant auto
!
crypto pki trustpoint cserver1
 enrollment url http://1.4.32.7:80
 revocation-check crl
 rsakeypair cserver1
```

Example: Configuring a Cisco IOS VG224 Voice Gateway

The following example shows how to configure a Cisco IOS VG224 Voice Gateway, where the IP address of the CA server is entered as the enrollment url:

```
Router# show run
.
.
.
crypto pki trustpoint VG224
 enrollment url http://1.4.32.7:80
 serial-number none
 fqdn none
 ip-address none
 mac-address FastEthernet0/0
 revocation-check none
!
stcapp security trustpoint VG224
stcapp security mode encrypted
stcapp
```

Additional References

The following sections provide references related to SCCP analog phone support for FXS ports on the Cisco voice gateway.

Related Documents

Related Topic	Document Title
Cisco Unified Communications Manager	*Cisco Unified Communications Manager*
Cisco Unified Communications Manager Express	*Cisco Unified Communications Manager Express*
Cisco IOS debugging	*Cisco IOS Debug Command Reference*
Cisco IOS voice commands	*Cisco IOS Voice Command Reference*
Cisco IOS voice configuration	*Cisco IOS Voice Configuration Library*
Cisco voice gateway	• *Cisco VG200 Series Gateway* • *Cisco 1800 Series Integrated Services Routers* • *Cisco 2800 Series Integrated Services Routers* • *Cisco 3800 Series Integrated services Routers* • *Cisco Unified 500 Series*
Conferencing and transcoding resources	• "Configuring Enhanced Conferencing and Transcoding for Voice Gateway Routers" chapter in the *Cisco Unified CallManager and Cisco IOS Interoperability Guide*. • *Cisco CallManager and IOS Gateway DSP Farm Configuration Example*

RFCs

RFC	Title
RFC 2246	The TLS Protocol Version 1.0

Technical Assistance

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

Feature Information for Secure SCCP Analog Endpoints over TLS with Cisco Unified CM

Table 1 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 15.1(3)T or a later release appear in the table.

For information on a feature in this technology that is not documented here, see the "Supplementary Services Features Roadmap" section on page 1.

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

Table 1 Feature Information for Secure SCCP Analog Endpoints over TLS with Cisco Unified CM

Feature Name	Releases	Feature Information
Secure SCCP Analog Endpoints over TLS with Cisco Unified CM	15.1(3)T	Enhances STCAPP FXS security analog endpoints through secure signaling and media encryption using TLS. This feature is supported for analog SCCP endpoints that are controlled by the Cisco Unified CM only. The following sections provide information about this feature: • Information About Secure SCCP Analog Endpoints over TLS with Cisco Unified CM, page 214 • How to Configure Secure SCCP Analog Endpoints over TLS with Cisco Unified CM, page 217. No new commands were introduced by this feature.