IOS SIP ゲートウェイと CallManager の間の SIP-TLS の設定例

目次

はじめに

このドキュメントでは、Cisco IOS® ゲートウェイと Cisco Unified CallManager の間の SIP シグナリングの暗号化（SIP over Transport Layer Security）の設定例を紹介します。

前提条件

要件

このドキュメントに関しては個別の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco IOS ゲートウェイ： Cisco 2821、高度なエンタープライズ サービス機能が設定された Cisco IOS ソフトウェア リリース 12.4(15) T1
- Cisco CallManager 5.1.2

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメン

トで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注: このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。

設定

このドキュメントでは、次の設定を使用します。

- Cisco CallManager 自己署名証明書のダウンロード
- Cisco IOS SIP ゲートウェイの設定
- Cisco Unified CallManager への Cisco IOS SIP ゲートウェイ証明書のアップロード
- Cisco CallManager での SIP トランク設定

Cisco CallManager 自己署名証明書のダウンロード

次の手順を実行します。

1. **https://<ccm ip address>/platform_gui/** で Cisco CallManager の Cisco Unified OS 管理ページにログインし、[Security] > [Certificate Management] > [Download Certificate/CTL] を選択します。
2. [Download Own Cert] をクリックします。
3. 既存の証明書タイプとして [CallManager] をクリックします。
4. [Certificate Name] をクリックします。
5. [Continue] をクリックします。
6. [CallManager.pem link] を右クリックし、[Savelink] を選択して証明書をダウンロードします。

Cisco IOS SIP ゲートウェイの設定

IOS SIP ゲートウェイの設定
`maui-soho-01#`

!--- Enable IP TCP MTU Path Discovery. ip tcp path-mtu-discovery *!--- Configure NTP Server.* ntp server 172.18.108.15 *!--- Upload the CCM Certificate to Cisco IOS Gateway.* crypto pki trustpoint CCM-Cert enrollment terminal revocation-check none *!--- Download the Cisco CallManager certificate, and paste !--- the contents of the certificate, pem format.* Router(config)#crypto ca authenticate CCM-Cert Enter the base 64 encoded CA certificate. End with a blank line or the word "quit" on a line by itself -----BEGIN CERTIFICATE-----
MIICIjCCAYugAwIBAgIIS4xQN3bIZUowDQYJKoZIhvcNAQEFBQAwFzEV
MBMGA1UE
AxMMUlRQTVMtQ0NNLTUxMB4XDTA3MDcyMzIzMjI0OVoXDTEyMDcyMzIz
MjI0OVow
FzEVMBMGA1UEAxMMUlRQTVMtQ0NNLTUxMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCB
iQKBgQD6HIRcgDXQmO/EWosnaMBaoqjzARIR0erx31uR9WOiaZqsgRY+
Am5/E3FG
n1nJ/4NVmA45z1Q54vK0WULXgMBGANGHnBZFCNiJOiNeBfiEh1LGGMre
VTLFqKB/
lNAMtTppc0AVyYFjAAcJtZfUGxolZCanY5TWfmlwGBMIDhnqQQIDAQAB
o3cwdTAL
BgNVHQ8EBAMCArwwJwYDVR0lBCAwHgYIKwYBBQUHAwEGCCsGAQUFBwMC
BggrBgEF
BQcDBTAeBgNVHREEFzAVhhNzaXA6Q049UlRQTVMtQ0NNLTUxMB0GA1Ud
DgQWBBQr
pCXbwcRZ09AkO7V0HgHihiKpZzANBgkqhkiG9w0BAQUFAAOBgQAvNQqa
VKKoZxUD
HCBIA292qZSsOht859FY3UJkWfGD+kjlGhjgjlxEQcaJOa7pDlorzH+H
QIjFpcv6
1cl0tOdOrs2L6IAGd9e5DQ3qDwWxaB7TIsBPTkv9FLVURnKtJtVHbqjM
d+AAtsDl /DV5TbDUdre6Org1mn4uaMdrYzt1kQ== -----END CERTIFICATE----- Certificate has the following attributes: Fingerprint MD5: 1EF154E3 70E40379 1C7003B9 B29E111B Fingerprint SHA1: CAFA0F83 B04B2E65 71104B73 64BF6AEB ABE9EED9 % Do you accept this certificate? [yes/no]: yes Trustpoint CA certificate accepted. % Certificate successfully imported *!--- Configure a trustpoint in order to generate the self-signed !--- certificate of the Gateway.* crypto pki trustpoint CCM-SIP-1 enrollment selfsigned fqdn none subject-name CN=SIP-GW revocation-check none rsakeypair CCM-SIP-1 Router(config)#crypto ca enroll CCM-SIP-1 % The fully-qualified domain name will not be included in the certificate % Include the router serial number in the subject name? [yes/no]: no % Include an IP address in the subject name? [no]: no Generate Self Signed Router Certificate? [yes/no]: yes Router Self Signed Certificate successfully created *!— View the certificate in PEM format, and copy the Self-signed CA certificate !--- (output starting from “----BEGIN” to “CERTIFICATE-----“) to a file named SIP-GW.pem* Router(config)#crypto pki export CCM-SIP-1 pem terminal % Self-signed CA certificate: -----BEGIN CERTIFICATE-----
MIIBhDCCAS6gAwIBAgIBATANBgkqhkiG9w0BAQQFADARMQ8wDQYDVQQD
EwZTSVAt
R1cwHhcNMDcwOTA1MjAwMTA3WhcNMjAwMTAxMDAwMDAwWjARMQ8wDQYD
VQQDEwZT
SVAtR1cwXDANBgkqhkiG9w0BAQEFAANLADBIAkEAzgvQDbs9BgdrxxXW
1S/h4CZC
6JcMbBrhyO/VWOLWVe6BCFG+baJjUdYtyyvaMnlyeeVEh0/MuqCfsDo8
TvJJKwID
AQABo3EwbzAPBgNVHRMBAf8EBTADAQH/MBwGA1UdEQQVMBOCEUYzNDAu
MjguMjUt

```
MjgwMC0yMB8GA1UdIwQYMBaAFF6gnOpo7VY8BHL4mbSvwNxCKi62MB0G
A1UdDgQW
BBReoJzqaO1WPARy+Jm0r8DcQioutjANBgkqhkiG9w0BAQQFAANBAHhn
QS4EKcP6
IBVdtA4CM/74qCjhtsu/jciaIe90BXs56wrj7ZC4m1sIMzDAHfsl7dJl
B2IOw9Sk s980Np7dLJU= -----END CERTIFICATE----- %
General Purpose Certificate: -----BEGIN CERTIFICATE-----
MIIBhDCCAS6gAwIBAgIBATANBgkqhkiG9w0BAQQFADARMQ8wDQYDVQQD
EwZTSVAt
R1cwHhcNMDcwOTA1MjAwMTA3WhcNMjAwMTAxMDAwMDAwWjARMQ8wDQYD
VQQDEwZT
SVAtR1cwXDANBgkqhkiG9w0BAQEFAANLADBIAkEAzgvQDbs9BgdrxxXW
1S/h4CZC
6JcMbBrhyO/VWOLWVe6BCFG+baJjUdYtyyvaMnlyeeVEh0/MuqCfsDo8
TvJJKwID
AQABo3EwbzAPBgNVHRMBAf8EBTADAQH/MBwGA1UdEQQVMBOCEUYzNDAu
MjguMjUt
MjgwMC0yMB8GA1UdIwQYMBaAFF6gnOpo7VY8BHL4mbSvwNxCKi62MB0G
A1UdDgQW
BBReoJzqaO1WPARy+Jm0r8DcQioutjANBgkqhkiG9w0BAQQFAANBAHhn
QS4EKcP6
IBVdtA4CM/74qCjhtsu/jciaIe90BXs56wrj7ZC4m1sIMzDAHfsl7dJl
B2IOw9Sk s980Np7dLJU= -----END CERTIFICATE----- !---
Configure the SIP stack in the Cisco IOS GW to use the
self-signed !--- certificate of the router in order to
establish a SIP TLS connection from/to !--- Cisco
CallManager. sip-ua crypto signaling remote-addr
172.18.110.84 255.255.255.255 trustpoint CCM-SIP-1
strict-cipher !--- Configure the T1 PRI. controller T1
1/0/0 framing esf linecode b8zs pri-group timeslots 1-24
!--- Configure the ISDN switch type and incoming-voice
under the D-channel !--- interface. interface
Serial1/0/0:23 no ip address encapsulation hdlc isdn
switch-type primary-ni isdn incoming-voice voice no cdp
enable !--- Configure a POTS dial-peer that is used as
an inbound dial-peer for calls !--- that come in across
the T1 PRI line. dial-peer voice 2 pots description PSTN
PRI Circuit destination-pattern 9T incoming called-
number . direct-inward-dial port 1/0/0:23 !--- Configure
an outbound voip dial-peer in order to route calls to
the !--- Cisco CallManager. dial-peer voice 3 voip
destination-pattern 75... session protocol sipv2 session
target ipv4:172.18.110.84:5061 session transport tcp tls
dtmf-relay rtp-nte codec g711ulaw
```

Cisco Unified CallManager への Cisco IOS SIP ゲートウェイ証明書のアップロード

次の手順を実行します。

1. **https://<ccm *ip address*>/platform_gui/** で Cisco CallManager の Cisco Unified OS 管理ページにログインし、[Security] > [Certificate Management] > [Upload Certificate/CTL] を選択します。
2. [Upload Trust Cert] をクリックします。
3. [CallManager-trust] をクリックします。
4. Cisco IOS 証明書、the.pem ファイルの場所を入力または参照し、[Upload] をクリックします。
5. アップロード結果を検証します。

Cisco CallManager での SIP トランク設定

次の手順を実行します。

1. **https://<ccm *ip address*>/ccmadmin/** で CallManager の Cisco Unified OS 管理ページにログインします。 SIP トランク セキュリティ プロファイルを設定します。[System] > [Security Profile] > [SIP Trunk Security Profile] を選択します。次の図に示すパラメータの [Add New] ボタンをクリックします。
2. SIP トランクを設定します。[Choose Device] > [Trunk]を選択します。[Add New] ボタンをクリックします。次に示すように、**トランクタイプ**を SIP トランクにします。
3. ルート パターンを設定します。[Call Routing] > [Route/Hunt] > [Route Pattern] を選択します。次に示すように、[Add New] ボタンをクリックします。

確認

この項では、Cisco IOS SIP ゲートウェイで設定が適切に機能するかどうかを確認できます。

Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

- **Show crypto pki certificate verbose CCM-SIP-1**

```
Router Self-Signed Certificate

  Status: Available

  Version: 3

  Certificate Serial Number: 0x1

  Certificate Usage: General Purpose

  Issuer:

    cn=SIP-GW

  Subject:

    Name: SIP-GW

    cn=SIP-GW

  Validity Date:

    start date: 16:01:07 EST Sep 5 2007

    end   date: 20:00:00 EST Dec 31 2019

  Subject Key Info:

    Public Key Algorithm: rsaEncryption

    RSA Public Key: (512 bit)

  Signature Algorithm: MD5 with RSA Encryption

  Fingerprint MD5: 3F9612FB C0E435F1 F445B5C4 0344E6A9

  Fingerprint SHA1: E6520255 B799818F C1067042 1A7E2EE9 4DDFD0C8
```

```
X509v3 extensions:
  X509v3 Subject Key ID: 5EA09CEA 68ED563C 0472F899 B4AFC0DC 422A2EB6
  X509v3 Basic Constraints:
      CA: TRUE
  X509v3 Subject Alternative Name:
      F340.28.25-2800-2
  X509v3 Authority Key ID: 5EA09CEA 68ED563C 0472F899 B4AFC0DC 422A2EB6
  Authority Info Access:
Associated Trustpoints: CCM-SIP-1
```

- Show crypto pki certificate verbose CCM-Cert

```
CA Certificate
  Status: Available
  Version: 3
  Certificate Serial Number: 0x4B8C503776C8654A
  Certificate Usage: General Purpose
  Issuer:
    cn=RTPMS-CCM-51
  Subject:
    cn=RTPMS-CCM-51
  Validity Date:
    start date: 19:22:49 EST Jul 23 2007
    end   date: 19:22:49 EST Jul 23 2012
  Subject Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (1024 bit)
  Signature Algorithm: SHA1 with RSA Encryption
  Fingerprint MD5: 1EF154E3 70E40379 1C7003B9 B29E111B
  Fingerprint SHA1: CAFA0F83 B04B2E65 71104B73 64BF6AEB ABE9EED9
  X509v3 extensions:
    X509v3 Key Usage: BC000000
      Digital Signature
      Key Encipherment
```

```
      Data Encipherment

      Key Agreement

      Key Cert Sign

    X509v3 Subject Key ID: 2BA425DB C1C459D3 D0243BB5 741E01E2 8622A967

    X509v3 Subject Alternative Name:

    Authority Info Access:

  Associated Trustpoints: CCM-Cert
```

- Show sip-ua connection tcp tls detail

```
Total active connections      : 2

No. of send failures          : 0

No. of remote closures        : 0

No. of conn. failures         : 2

No. of inactive conn. ageouts : 0

Max. tls send msg queue size of 0, recorded for 0.0.0.0:0

TLS client handshake failures : 2

TLS server handshake failures : 0


---------Printing Detailed Connection Report---------

Note:

 ** Tuples with no matching socket entry

    - Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port>'

      to overcome this error condition

 ++ Tuples with mismatched address/port entry

    - Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port>

   id <connid>' to overcome this error condition


Remote-Agent:172.18.110.84, Connections-Count:2

  Remote-Port Conn-Id Conn-State  WriteQ-Size

  =========== ======= =========== ===========

         5061       1 Established           0

        51180       2 Established           0
```

- show call active voice brief

```
11F0 : 7 8990160ms.1 +2670 pid:20001 Answer 7960 active

 dur 00:00:10 tx:483/83076 rx:510/81600

 Tele 1/0/0:23 (228) [1/0/0.1] tx:9660/9660/0ms g711ulaw noise:0 acom:0  i/0:0/0 dBm


11F0 : 8 8990980ms.1 +1840 pid:3 Originate 75001 active

 dur 00:00:10 tx:483/1246360336 rx:513/82080

 IP 14.50.202.26:28232 SRTP: off rtt:0ms pl:4720/1ms lost:0/0/0 delay:0/0/0ms

 g711ulaw TextRelay: off media inactive detected:n media contrl rcvd:n/a

 timestamp:n/a long duration call detected:n long duration call

 duration:n/a timestamp:n/a


Telephony call-legs: 1

SIP call-legs: 1

H323 call-legs: 0

Call agent controlled call-legs: 0

SCCP call-legs: 0

Multicast call-legs: 0

Media call-legs: 0

Total call-legs: 2
```

トラブルシューティング

このセクションでは、設定のトラブルシューティングに役立つ情報を提供します。

debug コマンド

Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

Cisco IOS ゲートウェイを設定して、ロギング バッファにデバッグ情報を記録し、**logging console** を無効にするようにします。

注: debug コマンドを使用する前に、『**debug コマンドの重要な情報**』を参照してください。

ゲートウェイがロギング バッファにデバッグを格納するよう設定するには、次のコマンドを使用します。

- **service timestamps debug datetime msec**

- service sequence
- no logging console
- logging buffered 5000000 debug
- clear log

このドキュメントの設定をデバッグするには、次のコマンドを使用します。

- debug isdn q931
- debug voip ccapi inout
- debug ccsip all
- debug ssl openssl errors
- debug ssl openssl msg
- debug ssl openssl states

関連情報

- 音声に関する技術サポート
- 音声とユニファイド コミュニケーションに関する製品サポート
- Cisco IP Telephony のトラブルシューティング
- テクニカル サポートとドキュメント – Cisco Systems