Exemple de configuration de SIP-TLS entre une passerelle SIP IOS et CallManager

Contenu

Introduction

Ce document fournit une configuration d'échantillon pour le cryptage de signalisation de SIP (SIP au-dessus du Transport Layer Security) entre une passerelle de Cisco IOS® et un Cisco Unified CallManager.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Passerelle de Cisco IOS : Cisco 2821, logiciel Release12.4(15)T1 de Cisco IOS avec

l'ensemble de caractéristiques avancé de services d'entreprise
- Cisco CallManager 5.1.2

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Configurez

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Note: Utilisez l'Outil de recherche de commande (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :

Configurations

Ce document utilise les configurations suivantes :

- Téléchargez le certificat Auto-signé par Cisco CallManager
- Configuration de passerelle de SIP de Cisco IOS
- Téléchargez le certificat de passerelle de SIP de Cisco IOS au Cisco Unified CallManager
- Configuration de joncteur réseau de SIP dans le Cisco CallManager

Téléchargez le certificat Auto-signé par Cisco CallManager

Procédez comme suit :

1. Connectez-vous dans la page de gestion de SYSTÈME D'EXPLOITATION de Cisco Unified dans le Cisco CallManager à l'**IP address >/platform_gui/de <ccm de https://**, et choisissez la **Gestion de Sécurité** > de **certificat** > le **téléchargement Certificate/CTL**.
2. Cliquez sur Download **pour posséder le CERT**.
3. **CallManager de** clic comme type de certificat existant.
4. Cliquez sur le **nom de certificat**.
5. Cliquez sur **Continue**.
6. Cliquez avec le bouton droit le **lien CallManager.pem**, et Savelink choisi **comme afin de** télécharger le certificat.

Configuration de passerelle de SIP de Cisco IOS

Configuration de passerelle de SIP IOS

```
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
```

Le certificat de la passerelle de SIP de Cisco IOS de téléchargement au Cisco Unified CallManager

Procédez comme suit :

1. Connectez-vous dans la page de gestion de SYSTÈME D'EXPLOITATION de Cisco Unified dans le Cisco CallManager à l'***IP address >/platform_gui/de <ccm de https://***, et choisissez la **Gestion de Sécurité** > de **certificat** > le **téléchargement Certificate/CTL**.
2. Cliquez sur Upload le **CERT de confiance**.
3. **CallManager-confiance de** clic.

4. Entrez ou parcourez à l'emplacement du certificat de Cisco IOS, fichier the.pem, et cliquez sur Upload.
5. Vérifiez le résultat de téléchargement.

Configuration de joncteur réseau de SIP dans le Cisco CallManager

Procédez comme suit :

1. Connectez-vous dans la page de gestion de SYSTÈME D'EXPLOITATION de Cisco Unified dans le CallManager à l'***IP address >/ccmadmin/de <ccm de https://***. Configurez un profil de Sécurité de joncteur réseau de SIP :**Profil de Sécurité** choisissez le **profil de système >** de **Sécurité >** de **SIP joncteur réseau**.Cliquez sur le **bouton Nouveau d'ajouter** avec les paramètres représentés sur cette figure :
2. Configurez un joncteur réseau de SIP :Choisissez le **périphérique >** le **joncteur réseau**.Cliquez sur le **bouton Nouveau d'ajouter**.**Joncteur réseau** choisi de **SIP** pour le `type de joncteur réseau`, comme affiché :
3. Configurez un modèle d'artère :Choisissez le **routage d'appels >** l'**artère/recherche >** le **modèle d'artère**.Cliquez sur le **bouton Nouveau d'ajouter**, comme affiché :

Vérifiez

Employez cette section afin de confirmer que votre configuration fonctionne correctement à la passerelle de SIP de Cisco IOS.

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes **show**. Employez l'OIT afin d'afficher une analyse de la sortie de la commande show.

- **Affichez à crypto certificat de PKI CCM-SIP-1 bavard**

```
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
```

- Affichez à crypto certificat de PKI le CCM-CERT bavard

```
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
```

- Affichez le détail de tls de TCP de connexion de sip-ua

```
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
```

- **Brief de show call active voice**

```
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
```

Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Commandes de débogage

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes **show**. Employez l'OIT afin d'afficher une analyse de la sortie de la commande show.

Configurez la passerelle de Cisco IOS pour se connecter met au point dans son tampon de journalisation et désactive le **logging console**.

Note: Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

Ce sont les commandes utilisées afin de configurer la passerelle pour enregistrer met au point dans le tampon de journalisation :

- **les horodateurs de service mettent au point la milliseconde date-heure**
- **entretenez l'ordre**
- **no logging console**
- **le logging buffered 5000000 mettent au point**
- **clear log**

Ce sont les commandes utilisées afin de mettre au point la configuration dans ce document :

- **debug isdn q931**
- **debug voip ccapi inout**
- **debug ccsip all**
- **erreurs de debug ssl openssl**
- **msg de debug ssl openssl**
- **états de debug ssl openssl**

Informations connexes

- Assistance technique concernant la technologie vocale
- Assistance concernant les produits vocaux et de communications unifiées
- Dépannage des problèmes de téléphonie IP Cisco
- Support et documentation techniques - Cisco Systems