

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurez](#)

[Diagramme du réseau](#)

[Configuration de CUBE](#)

[Configuration CUCM](#)

[Vérifiez](#)

[Dépannez](#)

[Cisco relatif prennent en charge des discussions de la Communauté](#)

Introduction

Ce document décrit les fondements du Transport Layer Security de Protocole SIP (Session Initiation Protocol) (TLS) et du protocole de transport en temps réel sécurisé (SRTP) au-dessus du Logiciel Cisco Unified Border Element (CUBE) avec un exemple de configuration.

La transmission de voix sécurisée au-dessus du CUBE peut être divisée en deux parts :

- Signalisation sécurisée ? Le CUBE emploie le TLS pour sécuriser la signalisation au-dessus du SIP et de l'
- Médias sécurisés ? SRTP

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Des fichiers de la liste de confiance de certificat de Cisco Unified Communications Manager (CUCM) (CTL) sont créés pour le mode mixte
- Des Téléphones IP sont enregistrés en mode sécurisé (le cryptage)
- Le voip de service vocal de CUBE et la configuration de base de cadran-pair est fait

[Composants utilisés](#)

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

- CUCM 10.5
- CUBE ? 3925E avec IOS 15.3(3)M3
- Cisco IP Communicator (CIPC)

[Informations générales](#)

- TLS - Le TLS et son prédécesseur, Secure Sockets Layer (SSL), sont des protocoles

cryptographiques qui fournissent la sécurité des communications au-dessus de l'Internet.

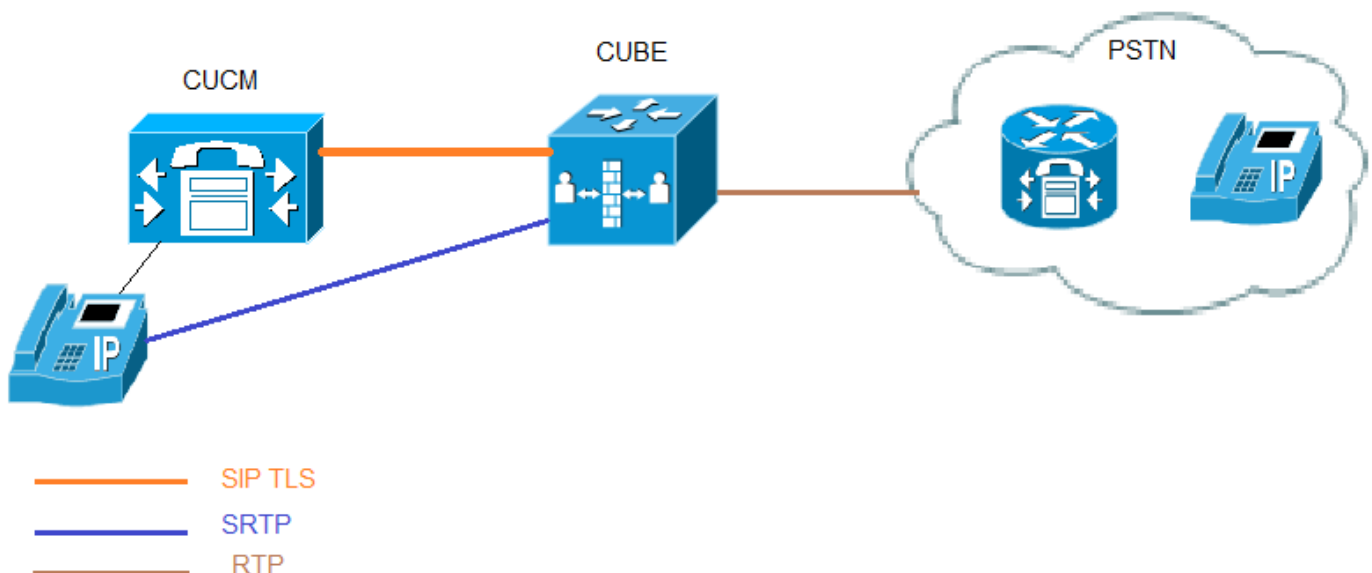
Dans des équivalences en modèle d'interconnexion de systèmes ouverts (OSI), TLS/SSL est initialisé à la couche 5 (la couche session) et puis fonctionne à la couche 6 (la couche présentation). Dans les les deux les modèles, le TLS et le SSL fonctionnent au nom de la couche transport sous-jacente, dont les segments portent des données cryptées.

- Autorité de certification (CA) - L'entité de confiance cette des questions délivre un certificat : Cisco ou une tiers entité.
- Procédure d'authentification de périphérique qui valide l'identité du périphérique et s'assure que l'entité est ce qui être elle prétend avant qu'un rapport soit établi.
- Cryptage - Processus de traduire des données dans le cryptogramme qui assure la confidentialité des données. Seulement le destinataire destiné peut lire les données. Il exige un algorithme de chiffrement et une clé de chiffrement.
- Clés publiques/privées - Clés qui sont utilisées dans le cryptage. Les clés publiques sont largement - des clés disponibles, mais privées sont tenues par leurs détenteurs respectifs. Le cryptage asymétrique combine les deux types.

Configurez

Diagramme du réseau

Dans cette image, l'exemple de configuration pour installer le TLS de SIP et le SRTP entre le téléphone CUCM/IP et le CUBE est affiché. Interréseaux de CUBE entre SRTP et Protocole RTP (Real-Time Transport Protocol)



Configuration de CUBE

1. Configurez l'horloge et le serveur HTTP d'enable

Synchronisez les horloges dans le serveur CA et les points de confiance de client (CUBE/OGW/TGW). Autrement, il y a des questions avec la validité des Certificats délivrés par le serveur CA.

HTTP d'utilisation de points de confiance de client pour recevoir le certificat du CA.

1. Générez une RSA Keypair

Cette étape génère des clés privées et publiques.

Dans cet exemple, le CUBE est juste une étiquette. Il peut être quelque chose.

1. Configurez le serveur IOS CA

Dans cet exemple, le serveur CA est nommé cube-Ca.

1. Créez les points de confiance de PKI pour le cube pour la transmission de TLS.

Dans cet exemple, le nom de point de confiance pour le CUBE est CUBE-TLS. L'adresse IP utilisée dans l'URL d'inscription doit être interface locale sur le CUBE. Le nom du sujet utilisé dans cette étape doit s'assortir sur le nom du sujet X.509 sur le profil de Sécurité de joncteur réseau de SIP CUCM. La pratique recommandée est d'utiliser le nom d'hôte avec le nom de domaine (si le nom de domaine est activé).

Paire de clés RSA d'associé créée dans l'étape 2.

5. Authentifiez le point de confiance avec le serveur CA et recevez le certificat du CA.

```
Secure-CUBE(config)#crypto pki authenticate CUBE-TLS
```

Certificate has the following attributes:

```
Fingerprint MD5: BCEBB5A1 1AC882F7 24BE476D 06537711
```

```
Fingerprint SHA1: CE2FEEA5 42515B33 3EF6A8F6 7E31D6DF 8E32BEB6
```

```
% Do you accept this certificate? [yes/no]: yes
```

```
Trustpoint CA certificate accepted.
```

```
Secure-CUBE(config)#
```

1. Inscrivez-vous le point de confiance avec le serveur CA.

Dans cette étape le CUBE reçoit un certificat signé du CA.

```
Secure-CUBE(config)#crypto pki enroll CUBE-TLS
```

```
%  
% Start certificate enrollment ..  
% Create a challenge password. You will need to verbally provide this  
password to the CA Administrator in order to revoke your certificate.  
For security reasons your password will not be saved in the configuration.  
Please make a note of it.
```

```
Password:
```

```
Re-enter password:
```

```
% The subject name in the certificate will include: CN=Secure-CUBE  
% The fully-qualified domain name will not be included in the certificate  
Request certificate from CA? [yes/no]: yes  
% Certificate request sent to Certificate Authority  
% The 'show crypto pki certificate verbose CUBE-TLS' command will show the fingerprint.
```

```
Secure-CUBE(config)#
```

1. Créez le point de confiance pour le CUCM.

Si le groupe de CallManager a de plusieurs serveurs cm, alors le point de confiance doit être créé pour tous les serveurs, autrement le Basculement pas fonctionne.

```
crypto pki trustpoint cucmpub  
enrollment terminal  
revocation-check none
```

```
crypto pki trustpoint cucmsub  
enrollment terminal  
revocation-check none
```

1. Inscrivez-vous le certificat CUCM POUR CUBER.

Étape 1. Procédure de connexion à l'admin de SYSTÈME D'EXPLOITATION CUCM.

Étape 2. Naviguez vers la **Sécurité > la Gestion > la découverte de certificat**.

Cisco Unified Operating System Administration
For Cisco Unified Communications Solutions

Navigation Cisco Unified OS Administration Go
admin | Search Documentation | About | Logout

Show Settings Security Software Upgrades Services Help

Certificate List

Generate Self-signed Upload Certificate/Certificate chain Download CTL Generate CSR

Status
26 records found

Certificate List (1 - 26 of 26) Rows per Page 50

Find Certificate List where Certificate begins with Find Clear Filter

Certificate	Common Name	Type	Distribution	Issued By	Ex
CallManager	cmpub	Self-signed	cmpub	cmpub	02/
CallManager-trust	Cisco_Root_CA_2048	Self-signed	Cisco_Root_CA_2048	Cisco_Root_CA_2048	05/
CallManager-trust	Cisco_Root_CA_M2	Self-signed	Cisco_Root_CA_M2	Cisco_Root_CA_M2	11/
CallManager-trust	cmsub	Self-signed	cmsub	cmsub	02/
CallManager-trust	CAP-RTP-001	Self-signed	CAP-RTP-001	CAP-RTP-001	02/
CallManager-trust	Cisco_Manufacturing_CA	CA-signed	Cisco_Manufacturing_CA	Cisco_Root_CA_2048	05/
CallManager-trust	CAPF-9a08b5fe	Self-signed	CAPF-9a08b5fe	CAPF-9a08b5fe	02/

Étape 3. Cliquez sur le certificat de **CallManager**, puis téléchargez et sauvegardez le fichier .PEM suivant les indications de cette image.

Certificate Details for cmpub, CallManager

Regenerate Generate CSR Download .PEM File Download .DER File

Status
Status: Ready

Certificate Settings

File Name CallManager.pem
Certificate Purpose CallManager
Certificate Type certs
Certificate Group product-cm
Description(friendly name) Self-signed certificate generated by system

Certificate File Data

```
[
  Version: V3
  Serial Number: 6AA0AECECE947BDCAFCC722310EE83224
  SignatureAlgorithm: SHA1withRSA (1.2.840.113549.1.1.5)
  Issuer Name: L=bangalore, ST=karnataka, CN=cmpub, OU=tac, O=cisco, C=IN
  Validity From: Sat Feb 07 22:39:22 IST 2015
  To: Thu Feb 06 22:39:21 IST 2020
  Subject Name: L=bangalore, ST=karnataka, CN=cmpub, OU=tac, O=cisco, C=IN
  Key: RSA (1.2.840.113549.1.1.1)
  Key value:
  30818902818100d2191a26d52904ae14c3b6eb1a27607d5ca4d85251037db19141e76906d2cfcf5dca3
  097fff569b7c19b9705de7624ca441617d49e08ee21a5d5cb8f3583a1f6089278b971833b6132dd4c77e
  5e81866f2f4386bc16252658e5bf0c37cb844df8a53a7dc034dff225fe7127b0fba88ab96617d01c3026f1
  04eea12492a8572250203010001
  Extensions: 3 present
]
```

Regenerate Generate CSR Download .PEM File Download .DER File

Étape 5. Cliquez sur le bouton **Download .PEM File** pour télécharger le contenu du du COMMENCER LE CERTIFICAT POUR FINIR LE CERTIFICAT .

Fingerprint SHA1: 5D31BEF0 DF2DCA7E 64D40246 89E564DD 9A7F8A01

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported

Secure-CUBE(config)#

1. Assignez le point de confiance pour le sip-ua, ce point de confiance est utilisé pour toute la signalisation de SIP entre le CUBE et le CUCM

Secure-CUBE(config)#**crypto pki authenticate cucmpub**

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

```
-----BEGIN CERTIFICATE-----
MIICoJCCAgugAwIBAgIQaqCuzslHvcr8xyIxDuDgyJDANBgkqhkiG9w0BAQUFADBj
MQswCQYDVQQGEwJlEOMAwGA1UEChMFY2l2Y28xMjE3MjE3MjE3MjE3MjE3MjE3MjE3
A1UEAxMFY2l2Y28xMjE3MjE3MjE3MjE3MjE3MjE3MjE3MjE3MjE3MjE3MjE3MjE3
b3JlMjE3MjE3MjE3MjE3MjE3MjE3MjE3MjE3MjE3MjE3MjE3MjE3MjE3MjE3MjE3
SU4xMjE3MjE3MjE3MjE3MjE3MjE3MjE3MjE3MjE3MjE3MjE3MjE3MjE3MjE3MjE3
MRIwEAYDVQQQIEwlrYXJlYXRha2ExEjAQBGNVBAcTCWJhbmhG9yZTCBnzANBgkq
hkiG9w0BAQEFAAOBjQAwGyKChYEA0hkaJtUpBK4Uw7brGidgfVyk2FJRA32xkUhn
aQbS89dyjCX//Vpt8GblwXeditKRBYX1J4I7iG11cuPNYOh9giSeLlxgzhMt1M
d+XoGGby9DhrwWJSZY5b8MN8uETfilOn3ANN/yJf5xJ7D7qIq5ZhfQHDAm8QTuoS
SSqFciUCAwEAAANXMFUwCwYDVR0PBAQDAgK8MCCGA1UdJQQgMB4GCCsGAQUFBwMB
BggrBgEFBQcDAGYIKwYBBQUHAWUwHQYDVR0OBBYEFDFGq0WCT/OnqwePSnhaknzR0
BconMA0GCSqGSIb3DQEBBQUAA4GBACb9gC0u/picQrv7BeLk2/qFmZ1/zVuXPDOn
wqz4yBMsa7Nk6QmpP5zXKJfXb3iKJPsmRWuUNEe+Df+sx0rUit3oGcF4ce/1ZfV
RKvt461TvA5r9HGxO+KaI8v7BaWeeROBfTboRpkvqRjFt6eIHEtn7+uUicumDASp
SkX08/Ar
-----END CERTIFICATE-----
```

Certificate has the following attributes:
Fingerprint MD5: 92DA2B5B A888784D C53B6C29 2E2B6A3C
Fingerprint SHA1: 5D31BEF0 DF2DCA7E 64D40246 89E564DD 9A7F8A01

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported

Secure-CUBE(config)#

ou transférez le point de confiance peut être configuré pour toute la signalisation de SIP de CUBE.

Secure-CUBE(config)#**crypto pki authenticate cucmpub**

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

```
-----BEGIN CERTIFICATE-----
MIICoJCCAgugAwIBAgIQaqCuzslHvcr8xyIxDuDgyJDANBgkqhkiG9w0BAQUFADBj
MQswCQYDVQQGEwJlEOMAwGA1UEChMFY2l2Y28xMjE3MjE3MjE3MjE3MjE3MjE3MjE3
A1UEAxMFY2l2Y28xMjE3MjE3MjE3MjE3MjE3MjE3MjE3MjE3MjE3MjE3MjE3MjE3
b3JlMjE3MjE3MjE3MjE3MjE3MjE3MjE3MjE3MjE3MjE3MjE3MjE3MjE3MjE3MjE3
SU4xMjE3MjE3MjE3MjE3MjE3MjE3MjE3MjE3MjE3MjE3MjE3MjE3MjE3MjE3MjE3
MRIwEAYDVQQQIEwlrYXJlYXRha2ExEjAQBGNVBAcTCWJhbmhG9yZTCBnzANBgkq
hkiG9w0BAQEFAAOBjQAwGyKChYEA0hkaJtUpBK4Uw7brGidgfVyk2FJRA32xkUhn
aQbS89dyjCX//Vpt8GblwXeditKRBYX1J4I7iG11cuPNYOh9giSeLlxgzhMt1M
d+XoGGby9DhrwWJSZY5b8MN8uETfilOn3ANN/yJf5xJ7D7qIq5ZhfQHDAm8QTuoS
SSqFciUCAwEAAANXMFUwCwYDVR0PBAQDAgK8MCCGA1UdJQQgMB4GCCsGAQUFBwMB
BggrBgEFBQcDAGYIKwYBBQUHAWUwHQYDVR0OBBYEFDFGq0WCT/OnqwePSnhaknzR0
BconMA0GCSqGSIb3DQEBBQUAA4GBACb9gC0u/picQrv7BeLk2/qFmZ1/zVuXPDOn
wqz4yBMsa7Nk6QmpP5zXKJfXb3iKJPsmRWuUNEe+Df+sx0rUit3oGcF4ce/1ZfV
RKvt461TvA5r9HGxO+KaI8v7BaWeeROBfTboRpkvqRjFt6eIHEtn7+uUicumDASp
SkX08/Ar
-----END CERTIFICATE-----
```

SkX08/Ar

-----END CERTIFICATE-----

Certificate has the following attributes:

Fingerprint MD5: 92DA2B5B A888784D C53B6C29 2E2B6A3C

Fingerprint SHA1: 5D31BEF0 DF2DCA7E 64D40246 89E564DD 9A7F8A01

% Do you accept this certificate? [yes/no]: yes

Trustpoint CA certificate accepted.

% Certificate successfully imported

Secure-CUBE(config)#

1. Enable SRTP.

Secure-CUBE(config)#**crypto pki authenticate cucmpub**

Enter the base 64 encoded CA certificate.

End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----

```
MIICoJCCAgugAwIBAgIQaqCuzslHvcr8xyIxDugyJDANBgkqhkiG9w0BAQUFADEj
MQswCQYDVQQGEwJtJTEOMAwGA1UEChMFY2l2Y28xDDAKBgNVBAsTA3RhYzEOMAwG
A1UEAxMFY2l2dWIxEjAQBGNVBAgTCWthcm5hdGFrYTESMBAGA1UEBxMJYmFuZ2Fs
b3JlMB4XDTE1MDIwNzE3MDkyMl0xDTIwMDIwNjE3MDkyMVowYzELMAkGA1UEBhMC
SU4xDjAMBGNVBAoTBWNpc2NvMQwwCgYDVQQLewN0YWMxDjAMBGNVBAMTBWNTcHVi
MRIwEAYDVQQQIEwlrYXJlYXRha2ExEjAQBGNVBACTCWJhbmhG9yZTCBnzANBgkq
hkiG9w0BAQEFAAOBjQAwGyKCGYEA0hkaJtUpBK4Uw7brGidgfVyk2FJRA32xkUhn
aQbS89dyjCX//Vpt8GblwXediTKRBYX1J4I7iG11cuPNYOh9giSeLlxgzhMt1M
d+XoGGby9DhrwWJSZY5b8MN8uETfilOn3ANN/yJf5xJ7D7qIq5ZhfQHDAm8QTuoS
SSqFciUCAwEAAaNXMFUwCwYDVR0PBAQDAgK8MCCGA1UdJQQgMB4GCCsGAQUFBwMB
BggrBgEFBQcDAGYIKwYBBQUHAWUwHQYDVR0OBBYEFDFGq0WCT/OnqwePSnhaknzR0
BconMA0GCSqGSIb3DQEBBQUAA4GBACb9gC0u/picQrv7BeLk2/qFmZ1/zVuXPDOn
wqz4yBMsa7Nk6QmpP5zXKJfXb3iKJPsmRWuUNEe+Df+sx0rUit3oGcF4ce/1ZfV
RKvt461TvA5r9HGxO+KaI8v7BaWeeROBfTboRpkvqRjFt6eIHEtn7+uUicumDASp
SkX08/Ar
```

-----END CERTIFICATE-----

Certificate has the following attributes:

Fingerprint MD5: 92DA2B5B A888784D C53B6C29 2E2B6A3C

Fingerprint SHA1: 5D31BEF0 DF2DCA7E 64D40246 89E564DD 9A7F8A01

% Do you accept this certificate? [yes/no]: yes

Trustpoint CA certificate accepted.

% Certificate successfully imported

Secure-CUBE(config)#

1. Pour l'interconnexion de réseaux SRTP et de RTP, sécurisez le transcoding est exigé.

Si la version IOS est 15.2.2T (CUBE 9.0) ou plus tard puis, transcoding LTI peut être configuré pour réduire la configuration.

Le transcoding LTI n'a pas besoin de la configuration de point de confiance de PKI pour des appels SRTP-RTP

Secure-CUBE(config)#**crypto pki authenticate cucmpub**

Enter the base 64 encoded CA certificate.

End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----

```
MIICoJCCAgugAwIBAgIQaqCuzslHvcr8xyIxDugyJDANBgkqhkiG9w0BAQUFADEj
MQswCQYDVQQGEwJtJTEOMAwGA1UEChMFY2l2Y28xDDAKBgNVBAsTA3RhYzEOMAwG
A1UEAxMFY2l2dWIxEjAQBGNVBAgTCWthcm5hdGFrYTESMBAGA1UEBxMJYmFuZ2Fs
b3JlMB4XDTE1MDIwNzE3MDkyMl0xDTIwMDIwNjE3MDkyMVowYzELMAkGA1UEBhMC
SU4xDjAMBGNVBAoTBWNpc2NvMQwwCgYDVQQLewN0YWMxDjAMBGNVBAMTBWNTcHVi
MRIwEAYDVQQQIEwlrYXJlYXRha2ExEjAQBGNVBACTCWJhbmhG9yZTCBnzANBgkq
hkiG9w0BAQEFAAOBjQAwGyKCGYEA0hkaJtUpBK4Uw7brGidgfVyk2FJRA32xkUhn
aQbS89dyjCX//Vpt8GblwXediTKRBYX1J4I7iG11cuPNYOh9giSeLlxgzhMt1M
d+XoGGby9DhrwWJSZY5b8MN8uETfilOn3ANN/yJf5xJ7D7qIq5ZhfQHDAm8QTuoS
SSqFciUCAwEAAaNXMFUwCwYDVR0PBAQDAgK8MCCGA1UdJQQgMB4GCCsGAQUFBwMB
BggrBgEFBQcDAGYIKwYBBQUHAWUwHQYDVR0OBBYEFDFGq0WCT/OnqwePSnhaknzR0
BconMA0GCSqGSIb3DQEBBQUAA4GBACb9gC0u/picQrv7BeLk2/qFmZ1/zVuXPDOn
wqz4yBMsa7Nk6QmpP5zXKJfXb3iKJPsmRWuUNEe+Df+sx0rUit3oGcF4ce/1ZfV
RKvt461TvA5r9HGxO+KaI8v7BaWeeROBfTboRpkvqRjFt6eIHEtn7+uUicumDASp
SkX08/Ar
```

```
hkiG9w0BAQEFAAOBjQAwwYkCgYEA0hkaJtUpBK4Uw7brGidgfVyk2FJRA32xkUHN
aQbS89dyjCX//Vpt8GblwXediTKRBYX1J4I7iG11cuPNYOh9giSeLlxgzhMt1M
d+XoGGby9DhrwWJSZY5b8MN8uETfilOn3ANN/yJf5xJ7D7qIq5ZhfQHDAm8QTuoS
SSqFciUCAwEAAANXMFUwCwYDVR0PBAQDAgK8MCcGA1UdJQqgMB4GCCsGAQUFBwMB
BggrBgEFBQcDAGYIKwYBBQUHAWUwHQYDVR0OBBYEFdGq0WCt/OnqwePSnhaknzR0
BconMA0GCSqGSIB3DQEBBQUAA4GBACb9gC0u/picQrv7BeLk2/qFmZ1/zVuXPDOn
wqz4yBMsa7Nk6QmpP5zXKJJfXb3iKJPsmRWuUNEe+Df+sx0rUit3oGcF4ce/1ZfV
RKvt461TvA5r9HGxO+KaI8v7BaWeeROBfTboRpkvqRjFt6eIHEtn7+uUicumDASp
SkX08/Ar
```

-----END CERTIFICATE-----

Certificate has the following attributes:

Fingerprint MD5: 92DA2B5B A888784D C53B6C29 2E2B6A3C

Fingerprint SHA1: 5D31BEF0 DF2DCA7E 64D40246 89E564DD 9A7F8A01

% Do you accept this certificate? [yes/no]: yes

Trustpoint CA certificate accepted.

% Certificate successfully imported

Secure-CUBE(config)#

Si l'IOS est au-dessous de 15.2.2T, alors configurez le transcoding de sccp.

Le transcoding de Protocole SCCP (Skinny Call Control Protocol) aurait besoin du point de confiance pour signaler cependant si le même routeur est utilisé pour héberger le transcoding alors que le même point de confiance (CUBE-TLS) peut être utilisé pour le CUBE aussi bien que transcoding.

Secure-CUBE(config)#**crypto pki authenticate cucmpub**

Enter the base 64 encoded CA certificate.

End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----

```
MIICojCAAgugAwIBAgIQaaCuzslHvcr8xyIxDugyJDANBgkqhkiG9w0BAQUFADEj
MQswCQYDVQQGEwJtJjEOMAwGA1UEChMFY2l2Y28xDDAKBgNVBAsTA3RhYzEOMAwG
A1UEAxMFY2l2dWlweXJjAQBgNVBAgTCWthcm5hdGFrYTESMBAGAlUEBxMJYmFuZ2Fs
b3JlMB4XDTE1MDIwNzE3MDkyM1oXDTE1MDIwNzE3MDkyMVowYzELMAkGA1UEBhMC
SU4xDjAMBgNVBAoTBWVnc2NvMQwwCgYDVQQLEwN0YWMxDjAMBgNVBAMTBWVnc2Nv
MRIwEAYDVQQQIEwlrYXJhYXJha2ExEjAQBgNVBAcTCWJhbmdhbG9yZTCBnzANBgkq
hkiG9w0BAQEFAAOBjQAwwYkCgYEA0hkaJtUpBK4Uw7brGidgfVyk2FJRA32xkUHN
aQbS89dyjCX//Vpt8GblwXediTKRBYX1J4I7iG11cuPNYOh9giSeLlxgzhMt1M
d+XoGGby9DhrwWJSZY5b8MN8uETfilOn3ANN/yJf5xJ7D7qIq5ZhfQHDAm8QTuoS
SSqFciUCAwEAAANXMFUwCwYDVR0PBAQDAgK8MCcGA1UdJQqgMB4GCCsGAQUFBwMB
BggrBgEFBQcDAGYIKwYBBQUHAWUwHQYDVR0OBBYEFdGq0WCt/OnqwePSnhaknzR0
BconMA0GCSqGSIB3DQEBBQUAA4GBACb9gC0u/picQrv7BeLk2/qFmZ1/zVuXPDOn
wqz4yBMsa7Nk6QmpP5zXKJJfXb3iKJPsmRWuUNEe+Df+sx0rUit3oGcF4ce/1ZfV
RKvt461TvA5r9HGxO+KaI8v7BaWeeROBfTboRpkvqRjFt6eIHEtn7+uUicumDASp
SkX08/Ar
```

-----END CERTIFICATE-----

Certificate has the following attributes:

Fingerprint MD5: 92DA2B5B A888784D C53B6C29 2E2B6A3C

Fingerprint SHA1: 5D31BEF0 DF2DCA7E 64D40246 89E564DD 9A7F8A01

% Do you accept this certificate? [yes/no]: yes

Trustpoint CA certificate accepted.

% Certificate successfully imported

Secure-CUBE(config)#

Configuration CUCM

1. Certificat IOS de CUBE en exportation à CUCM.

Étape 1. Certificat IOS d'exportation. Copiez le certificat de CA auto-signé et l'enregistrez comme fichier .PEM par exemple, Secure-CUBE.pem


```
Secure-CUBE(config)#crypto pki export CUBE-TLS pem terminal
% CA certificate:
-----BEGIN CERTIFICATE-----
MIIB/TCCA WagAwIBAgIBATANBgkqhkiG9w0BAQQFADASMR AwDgYDVQQDEWJdWJl
LWNhMB4XDTE1MDIxMTEyNTYyMVowXDTE1MDIxMDEyNTYyMVowEjEQMA4GA1UEAxMH
Y3ViZS1jYTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwYkCgYEA tN3gRiUQ409jECyo
xVZzrpBRqj/HOqkVu3iRYp2C2PGRr01vbZvb6IZIh+m4K0Du7gBASUFDAOeidJIF
TCI3+MjUN3grnv1MH321J5tVzAPHj9z7GdD42+gZSoHqOM1FB8z4+VDPzpo xpswI
3TFQHCFNbadF16P5VEFWv+0tHD8CAwEAAAnjMGEwDwYDVR0TAQH/BAUwAwEB/zAO
BgNVHQ8BAf8EBAMCAYYwHwYDVR0jBBgwFoAUnqzvazK/7qXzhkoTiAEFCvsN8rww
HQYDVR0OBBYEFJ6s72syv+6l84ZKE4gBBQr7DFk8MA0GCSqGSIb3DQEBAUAA4GB
AEfnNrB4nls81vz0cqlpuTjID+KVyKRwYNP04zJYWCV7P+m1bpMfC/qh14z5/RzL
e5Bq6NUnxWByLR4gcFjmds1E6NqoNX9S5ryS3xQRkXr0MiXnVngSKELUn22JUw/q
CEnHng0AvcTRv/EBB2XlzYUxG0keiT8K+jv/g7+rmkF5
-----END CERTIFICATE-----
```

```
% General Purpose Certificate:
-----BEGIN CERTIFICATE-----
MIIB7TCCA VagAwIBAgIBAJANBgkqhkiG9w0BAQUFADASMR AwDgYDVQQDEWJdWJl
LWNhMB4XDTE1MDIxMTEyNTYyMVowXDTE1MDIxMDEyNTYyMVowEjEUMBIGA1UEAxML
U2VjdXJlLUNVQkUwZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAJ5C2JnKwtfO
F9bBVYhVwQK8y2c5NMkJKY//pisg+oforvxalPKAXj/jqDkqtDtc3NAMf2A1rk25
f50aaBrNJmq4rfJB1wLyD2a/CzybJg+QB5sVCCHTwk5jf9+YGIMVsivbrf4m+Lqi
OkZ5qxsMa5fEc/fejUsAE8yn4/mmgld/AgMBAAGjTzBNMAsGA1UdDwQEAwIFoDAf
BgNVHSMEGDAWgBSer09rMr/upfOGSh0IAQUK+w3yvDAdBgNVHQ4EFgQUsvUGSpaH
+XIOVvf50imcCHV8HjAwDQYJKoZIhvcNAQEFBQADgYEAYmRHLHxTgIogZYPScPmj
h69GLxXxAOTHHosEbm/vfqk2vbYiHU09AtDDI+kNecSuOGmd7fokJMP9K1xc1i2a
vrr2qwQYqRAh68BwTjWzR3mFAGbDZzwiywv1jJ92ra3EMAUc0sJZSLzGY0+Bj0/E
dEW6JUIOx3NXP2SBN1NMAQ0=
-----END CERTIFICATE-----
```

Secure-CUBE(config)#

Étape 2. Certificat de CA IOS de téléchargement sur CUCM comme CallManager-confiance.

Étape 3. Naviguez vers la **gestion de SYSTÈME D'EXPLOITATION cm > la Gestion de Sécurité > de certificat > le certificat de téléchargement/chaîne de certificat**

Étape 4. Fichier du téléchargement .PEM suivant les indications de cette image.

Upload Certificate/Certificate chain

Upload Close

Status

i Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster

Upload Certificate/Certificate chain

Certificate Purpose* **CallManager-trust**

Description(friendly name)

Upload File **Browse... Secure-CUBE.pem**

Upload Close

i *- indicates required item.

1. Créez le nouveau profil de Sécurité de joncteur réseau de SIP

Étape 1. Sur la gestion cm naviguez les **profils > le fichier de Sécurité** vers le **système > la Sécurité > de SIP joncteur réseau**.

Étape 2. Copiez exister **profil non sécurisé de joncteur réseau de SIP** afin de créer le nouveau profil sécurisé suivant les indications de cette image.

SIP Trunk Security Profile Configuration

Save Delete Copy Reset Apply Config Add New

SIP Trunk Security Profile Information

Name* Secure SIP Trunk Profile

Description Secure SIP Trunk Profile authenticated by null String

Device Security Mode Encrypted

Incoming Transport Type* TLS

Outgoing Transport Type TLS

Enable Digest Authentication

Nonce Validity Time (mins)* 600

X.509 Subject Name Secure-CUBE

Incoming Port* 5061

Enable Application level authorization

Accept presence subscription

Accept out-of-dialog refer**

Accept unsolicited notification

Accept replaces header

Transmit security status

Allow charging header

SIP V.150 Outbound SDP Offer Filtering* Use Default Filter

1. Créez le joncteur réseau de SIP au CUBE

Étape 1. Activez SRTP sur le joncteur réseau de SIP suivant les indications de cette image.

Trunk Configuration

Save Delete Reset Add New

Packet Capture Mode* No Changes

Packet Capture Mode* None

Packet Capture Duration 0

Media Termination Point Required

Retry Video Call as Audio

Path Replacement Support

Transmit UTF-8 for Calling Party Name

Transmit UTF-8 Names in QSIG APDU

Unattended Port

SRTP Allowed When this flag is checked, Encrypted TLS needs to be configured in the network to provide end to end security. Failure to do Consider Traffic on This Trunk Secure*

Consider Traffic on This Trunk Secure* When using both sRTP and TLS

Route Class Signaling Enabled* Default

Use Trusted Relay Point* Default

PSTN Access

Run On All Active Unified CM Nodes

Étape 2. Configurez la destination port 5061 (TLS) et appliquez nouveau sécurisent le profil de Sécurité de joncteur réseau de SIP sur le joncteur réseau de SIP suivant les indications de cette image.

Trunk Configuration Rel

Save Delete Reset Add New

SIP Information

Destination

Destination Address is an SRV

	Destination Address	Destination Address IPv6	Destination Port
1*	10.106.95.155		5061

MTP Preferred Originating Codec*

BLF Presence Group*

SIP Trunk Security Profile*

Rerouting Calling Search Space

Out-Of-Dialog Refer Calling Search Space

SUBSCRIBE Calling Search Space

SIP Profile* [View Details](#)

DTMF Signaling Method*

Vérifiez

```
Secure-CUBE#show sip-ua connections tcp tls detail
```

```
Total active connections : 2
```

```
No. of send failures : 0
```

```
No. of remote closures : 13
```

```
No. of conn. failures : 0
```

```
No. of inactive conn. ageouts : 0
```

```
TLS client handshake failures : 0
```

```
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:10.106.95.151, Connections-Count:2
```

```
Remote-Port Conn-Id Conn-State WriteQ-Size Local-Address
```

```
=====
```

```
5061 16 Established 0 10.106.95.155
```

```
57396 17 Established 0 10.106.95.155
```

```
----- SIP Transport Layer Listen Sockets -----
```

```
Conn-Id Local-Address
```

```
=====
```

```
2 [10.106.95.155]:5061
```

La sortie du brief de show call active voice est capturée quand le transcodeur LTI est utilisé.

```
Secure-CUBE#show call active voice brief
```

```
Telephony call-legs: 0
```

```
SIP call-legs: 2
```

```
H323 call-legs: 0
Call agent controlled call-legs: 0
SCCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 2
1283 : 33 357052840ms.1 (23:57:23.929 IST Sun Feb 15 2015) +2270 pid:3 Answer 3001 active
dur 00:00:08 tx:383/61280 rx:371/59360 dscp:0 media:0 audio tos:0xB8 video tos:0x0
IP 10.106.95.132:17172 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay:
off Transcoded: Yes
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
LostPacketRate:0.00 OutOfOrderRate:0.00
```

```
1283 : 34 357052840ms.2 (23:57:23.929 IST Sun Feb 15 2015) +2270 pid:1 Originate 2001 active
dur 00:00:08 tx:371/60844 rx:383/62812 dscp:0 media:0 audio tos:0xB8 video tos:0x0
IP 10.65.58.24:24584 SRTP: on rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off
Transcoded: Yes
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
LostPacketRate:0.00 OutOfOrderRate:0.00
```

Également quand un appel chiffré par SRTP est fait entre le téléphone IP de Cisco et le CUBE ou la passerelle, une icône de verrouillage est affichée sur le téléphone IP.

Dépannez

Ceux-ci met au point sont utiles pour dépanner des questions PKI/TLS/SIP/SRTP.

```
Secure-CUBE#show call active voice brief
```

```
Telephony call-legs: 0
SIP call-legs: 2
H323 call-legs: 0
Call agent controlled call-legs: 0
SCCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 2
1283 : 33 357052840ms.1 (23:57:23.929 IST Sun Feb 15 2015) +2270 pid:3 Answer 3001 active
dur 00:00:08 tx:383/61280 rx:371/59360 dscp:0 media:0 audio tos:0xB8 video tos:0x0
IP 10.106.95.132:17172 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay:
off Transcoded: Yes
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
LostPacketRate:0.00 OutOfOrderRate:0.00

1283 : 34 357052840ms.2 (23:57:23.929 IST Sun Feb 15 2015) +2270 pid:1 Originate 2001 active
dur 00:00:08 tx:371/60844 rx:383/62812 dscp:0 media:0 audio tos:0xB8 video tos:0x0
IP 10.65.58.24:24584 SRTP: on rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off
Transcoded: Yes
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
LostPacketRate:0.00 OutOfOrderRate:0.00
```