

Exemple de configuration de la communication MGCP sécurisée entre GW voix et CUCM via IPsec en fonction des certificats signés CA

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Configuration](#)

[Diagramme du réseau](#)

[1. Configurez l'autorité de certification sur la passerelle vocale et générez un certificat signé par l'autorité de certification pour la passerelle vocale](#)

[2. Générer un certificat IPsec signé par l'autorité de certification CUCM](#)

[3. Importer des certificats CA, CUCM et GW voix sur CUCM](#)

[4. Configurer les paramètres du tunnel IPsec sur CUCM](#)

[5. Configurer le paramètre de tunnel IPsec sur la passerelle vocale](#)

[Vérification](#)

[Vérifier l'état du tunnel IPsec sur la fin CUCM](#)

[Vérification de l'état du tunnel IPsec sur l'extrémité de la passerelle vocale](#)

[Dépannage](#)

[Dépannage du tunnel IPsec sur l'extrémité CUCM](#)

[Dépannage du tunnel IPsec sur l'extrémité de la passerelle vocale](#)

Introduction

Ce document décrit comment sécuriser avec succès la signalisation MGCP (Media Gateway Control Protocol) entre une passerelle vocale (GW) et CUCM (Cisco Unified Communications Manager) via IPsec (Internet Protocol Security), en fonction des certificats signés par l'autorité de certification (CA). Pour configurer un appel sécurisé via MGCP, les flux RTP (Real-time Transport Protocol) et de signalisation doivent être sécurisés séparément. Il semble bien documenté et assez simple de configurer des flux RTP chiffrés, mais un flux RTP sécurisé n'inclut pas la signalisation MGCP sécurisée. Si la signalisation MGCP n'est pas sécurisée, les clés de chiffrement du flux RTP sont envoyées en clair.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Passerelle vocale MGCP enregistrée auprès de CUCM afin d'envoyer et de recevoir des appels
- Démarrage du service CAPF (Certificate Authority Proxy Function), cluster défini en mode mixte
- L'image Cisco IOS® sur GW prend en charge la fonction de sécurité de chiffrement
- Téléphones et MGCP GW configurés pour le protocole SRTP (Secure Real-Time Transport Protocol)

Components Used

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

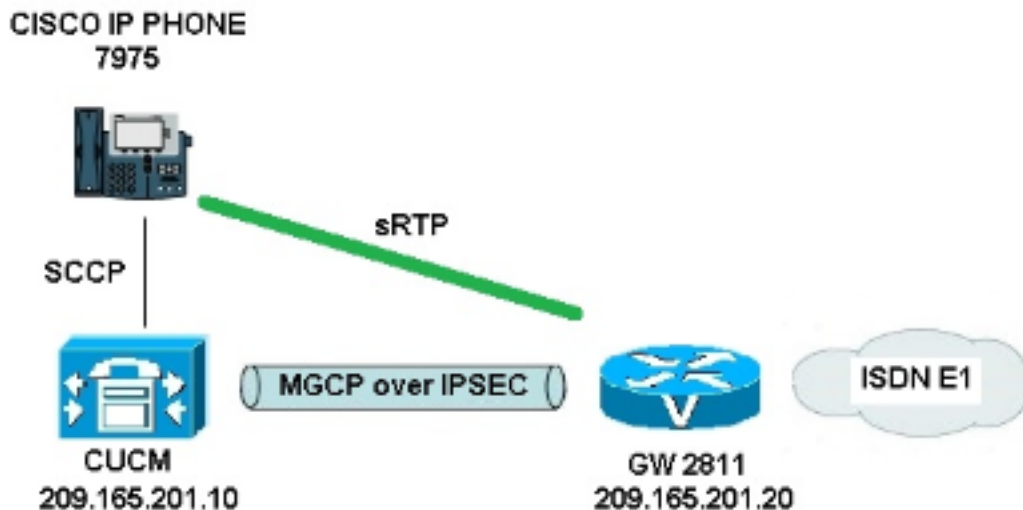
- CUCM - noeud unique - exécute GGSG (Global Government Solutions Group de Cisco) version 8.6.1.2012-14 en mode Federal Information Processing Standard (FIPS).
- Téléphones 7975 qui exécutent SCCP75-9-3-1SR2-1S
- GW - Cisco 2811 - C2800NM-ADVENTERPRISEK9-M, version 15.1(4)M8
- Carte vocale RNIS E1 - VWIC2-2MFT-T1/E1 - Liaison Multiflex RJ-48 à 2 ports

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configuration

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

Diagramme du réseau



Afin de configurer correctement IPsec entre CUCM et voix GW, procédez comme suit :

1. Configurez l'autorité de certification sur la passerelle vocale et générez un certificat signé par l'autorité de certification pour la passerelle vocale
2. Générer un certificat IPsec signé par l'autorité de certification CUCM
3. Importer des certificats CA, CUCM et GW voix sur CUCM
4. Configurer les paramètres de tunnel IPsec sur CUCM
5. Configurer le paramètre de tunnel IPsec sur la passerelle vocale

1. Configurez l'autorité de certification sur la passerelle vocale et générez un certificat signé par l'autorité de certification pour la passerelle vocale

Dans un premier temps, la paire de clés Rivest-Shamir-Addleman (RSA) doit être générée sur la passerelle vocale (serveur Cisco IOS CA) :

```
KRK-UC-2x2811-2#crypto key generate rsa general-keys label IOS_CA exportable
```

Les inscriptions terminées via le protocole SCEP (Simple Certificate Enrollment Protocol) seront utilisées, donc activez le serveur HTTP :

```
KRK-UC-2x2811-2#ip http server
```

Pour configurer le serveur AC sur une passerelle, ces étapes doivent être effectuées :

1. Définissez le nom du serveur PKI. Il doit porter le même nom que la paire de clés générée précédemment.

```
KRK-UC-2x2811-2(config)#crypto pki server IOS_CA
```
2. Spécifiez l'emplacement où toutes les entrées de base de données seront stockées pour le serveur AC.

```
KRK-UC-2x2811-2(cs-server)#crypto pki server IOS_CA
```
3. Configurez le nom de l'émetteur CA.

```
KRK-UC-2x2811-2(cs-server)#issuer-name cn=IOS
```
4. Spécifiez un point de distribution de liste de révocation de certificats (CRL) à utiliser dans les certificats émis par le serveur de certificats et activez l'octroi automatique de demandes d'inscription de certificat pour un serveur d'autorité de certification subordonné Cisco IOS.

```
KRK-UC-2x2811-2(cs-server)#crl-url http://209.165.201.10/IOS_CA.crl
```

```
KRK-UC-2x2811-2(cs-server)#grant auto
```

5. Activez le serveur AC.

```
KRK-UC-2x2811-2 (cs-server) #no shutdown
```

L'étape suivante consiste à créer un point de confiance pour le certificat CA et un point de confiance local pour le certificat du routeur avec une inscription d'URL qui pointe vers un serveur HTTP local :

```
KRK-UC-2x2811-2 (config) #crypto pki trustpoint IOS_CA
```

```
KRK-UC-2x2811-2 (ca-trustpoint) #revocation-check crl
```

```
KRK-UC-2x2811-2 (ca-trustpoint) #rsakeypair IOS_CA
```

```
KRK-UC-2x2811-2 (config) #crypto pki trustpoint local1
```

```
KRK-UC-2x2811-2 (ca-trustpoint) #enrollment url http://209.165.201.10:80
```

```
KRK-UC-2x2811-2 (ca-trustpoint) #serial-number none
```

```
KRK-UC-2x2811-2 (ca-trustpoint) #fqdn none
```

```
KRK-UC-2x2811-2 (ca-trustpoint) #ip-address none
```

```
KRK-UC-2x2811-2 (ca-trustpoint) #subject-name cn=KRK-UC-2x2811-2
```

```
KRK-UC-2x2811-2 (ca-trustpoint) #revocation-check none
```

Afin de générer le certificat du routeur signé par l'autorité de certification locale, le point de confiance doit être authentifié et inscrit :

```
KRK-UC-2x2811-2 (config) #crypto pki authenticate local1
```

```
KRK-UC-2x2811-2 (config) #crypto pki enroll local1
```

Ensuite, le certificat du routeur est généré et signé par l'autorité de certification locale. Indiquez le certificat sur le routeur pour vérification.

```
KRK-UC-2x2811-2 #show crypto ca certificates
```

Certificate

Status: Available

Certificate Serial Number (hex): 02

Certificate Usage: General Purpose

Issuer:

cn=IOS

Subject:

Name: KRK-UC-2x2811-2

cn=KRK-UC-2x2811-2

CRL Distribution Points:

http://10.48.46.251/IOS_CA.crl

Validity Date:

start date: 13:05:01 CET Nov 21 2014

end date: 13:05:01 CET Nov 21 2015

Associated Trustpoints: local1

Storage: nvram:IOS#2.cer

CA Certificate

Status: Available

Certificate Serial Number (hex): 01

Certificate Usage: Signature

Issuer:

cn=IOS

Subject:

cn=IOS

Validity Date:

start date: 12:51:12 CET Nov 21 2014

end date: 12:51:12 CET Nov 20 2017

Associated Trustpoints: local1 IOS_CA

Storage: nvram:IOS#1CA.cer

Deux certificats doivent être répertoriés. Le premier est un certificat de routeur (KRK-UC-2x2811-

2) signé par l'autorité de certification locale et le second est un certificat d'autorité de certification.

2. Générer un certificat IPsec signé par l'autorité de certification CUCM

Le CUCM pour le tunnel IPsec configuré utilise un certificat ipsec.pem. Par défaut, ce certificat est autosigné et généré lorsque le système est installé. Afin de le remplacer par un certificat signé par une autorité de certification, il faut d'abord générer un CSR (Certificate Sign Request) pour IPsec à partir de la page d'administration du système d'exploitation CUCM. Choisissez **Cisco Unified OS Administration > Security > Certificate Management > Generate CSR**.

The screenshot shows the Cisco Unified Operating System Administration interface. The main page displays a 'Certificate List' with 21 records found. A modal dialog box titled 'Generate Certificate Signing Request - Mozilla Firefox' is open, showing a warning: 'Warning: Generating a new CSR will overwrite the existing CSR'. The 'Certificate Name' field is set to 'ipsec'. The 'Generate CSR' button is visible.

Find Certificate List where	File Name	begins
tomcat	certs	
ipsec	certs	
tomcat-trust	trust-certs	
tomcat-trust	trust-certs	
tomcat-trust	trust-certs	
ipsec-trust	trust-certs	
CallManager	certs	
CAPF	certs	
TWS	certs	
CallManager-trust	trust-certs	
CallManager-trust	trust-certs	
CallManager-trust	trust-certs	
CallManager-trust	trust-certs	
CallManager-trust	trust-certs	
CallManager-trust	trust-certs	
CallManager-trust	trust-certs	
CallManager-trust	trust-certs	
CAPF-trust	trust-certs	
CAPF-trust	trust-certs	

Une fois le CSR généré, il doit être téléchargé à partir de CUCM et inscrit à l'autorité de certification sur la GW. Pour ce faire, entrez la commande **crypto pki server IOS_CA request pkcs10 terminal base64** et le hachage de la demande de signature doit être collé via terminal. Le certificat accordé est affiché et doit être copié et enregistré en tant que fichier ipsec.pem.

```
KRK-UC-2x2811-2#crypto pki server IOS_CA request pkcs10 terminal base64  
PKCS10 request in base64 or pem
```

```
% Enter Base64 encoded or PEM formatted PKCS10 enrollment request.  
% End with a blank line or "quit" on a line by itself.  
-----BEGIN CERTIFICATE REQUEST-----  
MIIDNjCCA4h4CAQAwgaxkCzAJBgNVBAYTA1BMMQ4wDAYDVQQIEwVjaXNjbzEOMAwG  
A1UEBxMFMFY21zY28xDjAMBgNVBAoTBWVnc2NvMQ4wDAYDVQQLEwVjaXNjbzEPMA0G  
A1UEAxMGMQ1VDTUIxMUkwRwYDVQQFE0A1NjY2OWY5MjgzNWZmZWQ1MDg0YjI5MTU4  
NjcwMDBmMGI2NjliYjYkYjYwZmZlNDNmMzQzOWFhNGQxMzZlMTU1MjUzMIIBIjANBgkq  
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEakfHxvcov4vFmK+3+dQShW3s3SsZAYBQ19  
0JDBiIc4eDRmrdq0V2dkn9UpLUx9OH7V0Oe/8wmHqYwoxFZ5a6B5qRRkc010/ub2
```

```
ul1QCw+nQ6QiZGdNhdne0NYY4r3odF4CkrtYAJA4PUSceltWxfiJY5dw/Xhv8cVg
gVyuxctESemfMhUfvEM203NU9nod7YTEzQzuAadjNcyc4blu91vQm5OVUNXxODov
e7/OlQNUWU3LSEr0aI9lC75x3qdRgBe8Pwnk/gWbT5B7pwuwMXTU8+UFj6+lvrQM
Rb47dw22yFmSMObvez18IVExAyFs50j9Aj/rNFIdUQIt+Nt+Q+f38wIDAQABoEcw
RQYJKoZIhvcNAQkOMTgwNjAnBgNVHSUEIDAEBggrBgEFBQCDAQYIKwYBBQUHAWIG
CCsGAQUFBwMFMAsgA1UdDwQEAwIDuDanBgkqhkiG9w0BAQUFAAOCAQEAQDgAR4O1
oQ4z2yqgSsICAZ2hQA3Vztp6aOI+0PSyMfihGS//3V3tALEZL2+t0Y5elKsBea72
sieKjpSikXjNaj+SiY1aYy4siVw5EKQD3Ii4Qv115BvuniZXvBiBQUw+SpBLbeNi
xwIgrYELrFyWQZBeZodFqnSKN9X1isXe6oU9GXux7uWgXwkCXMF/azutbio14Fgf
qUF00GzkhtEapJA6c5RzaxG/0uDuKY+4z1eSSsXzFhBTifk3RfJA+I7Na1zQBIEJ
2IOJdiZnn0HWVr5C5eZ7VnQuNdiC/qn3uUfvNVRZo8iCDq3tRv7dr/n64jdKsHEM
lk6P8gp9993cJw==
```

quit

% Granted certificate:

```
MIIDXTCCAsagAwIBAgIBBTANBgkqhkiG9w0BAQQFADAOMQwwCgYDVQQDEwNJT1Mw
HhcNMtUwMTA4MTIwMTAwWhcNMtYwMTA4MTIwMTAwWjCBQTELMAKGA1UEBhMCUEwx
DjAMBgNVBAgTBWNpc2NvMQ4wDAYDVQQHEwVjaXNjbzEOMAwGA1UEChMFY2lzY28x
DjAMBgNVBAStBWNpc2NvMQ8wDQYDVQQDEwZDVUNNQjExSTBHBGNVBAUTQDU2NjY5
ZjkyODM1ZmZlZDUwODRimjknNTg2NzAwMGYwYjY2OWJiN2RhZmE0M2YzZDM5YWE0
ZDEzMzVlOUYyNTMwgwEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC8fG9
yi/i8WYr7f51BKFbezdlMBgFDX3QkMGihzh4NGZ2urRXZ2Sf1SktTH04ftXQ57/z
CYepjCjEVnlroHmpFGRw7XT+5va6XVALD6dDpCJkZ02F2d7Q1hjhiveh0XgKSu1gA
kDg9Rjx7W1bF+Ilj13D9eG/xxWCBXK7Fy0Rj6Z8yFR+8QzbTc1T2eh3thMTND04B
p2M1zJzhvW73W9Cbk5VQ1fe40i97v86VA1RZTctISvRoj2ULvnHep1EYF7w/CeT+
BZtPkHunC7AxdNTz5QWPr6W+tAxFvj3DbbIWZlw5u97PXwhUTEDIWzk6P0CP+s0
Uh1RAi34235D5/fzAgMBAAGjgaowgacwLwYDVR0fBCgwJjAkoCKgIIYeaHR0cDov
LzEwLjQ4LjQ2LjI1MS9JT1NfQ0EuY3JsMAsGA1UdDwQEAwIDuDanBgNVHSUEIDAE
BggrBgEFBQCDAQYIKwYBBQUHAWIGCCsGAQUFBwMFMB8GA1UdIwQYMBaAFJSLP5cn
PL8bIP7VSKLtbB6Z1socOMB0GA1UdDgQWBRR4m2eTSyELsdRBW4MRmbNdT2qppTAN
BgkqhkiG9w0BAQQFAAOBgQBvVJ+tvS0JqP4z9TgEeuMbVwn00CTKXz/fCuh6R/50
qq8JhERJGiR/ZHvHRLf+XawhnoE6daPAmE+WkIPtHIhbmhCbbxG9ffdyaiNXRWy
5sI5XycF1FgYGpTFBYD9M0Lqsw+FIYaT2ZrbOGsx8h6pZoesKqm85RByIUjX4nJK
1g==
```

Note: Afin de décoder et vérifier le contenu du certificat codé Base64, entrez la commande **openssl x509 -in certificate.crt -text -noout**.

Le certificat CUCM accordé décode :

```
Certificate:
Data:
Version: 3 (0x2)
Serial Number: 5 (0x5)
Signature Algorithm: md5WithRSAEncryption
Issuer: CN=IOS
Validity
Not Before: Jan 8 12:01:00 2015 GMT
Not After : Jan 8 12:01:00 2016 GMT
Subject: C=PL, ST=cisco, L=cisco, O=cisco, OU=cisco,
CN=CUCMB1/serialNumber=56669f92835ffed5084b2915867000f0b669bb7dafa43f3d39aa4d1335e9e253
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (2048 bit)
Modulus (2048 bit):
00:91:f1:f1:bd:ca:2f:e2:f1:66:2b:ed:fe:75:04:
a1:5b:7b:37:4b:30:18:05:0d:7d:d0:90:c1:88:87:
38:78:34:66:76:ba:b4:57:67:64:9f:d5:29:2d:4c:
7d:38:7e:d5:d0:e7:bf:f3:09:87:a9:8c:28:c4:56:
79:6b:a0:79:a9:14:64:70:ed:74:fe:e6:f6:ba:5d:
50:0b:0f:a7:43:a4:22:64:67:4d:85:d9:de:d0:d6:
18:e2:bd:e8:74:5e:02:92:bb:58:00:90:38:3d:44:
```

```
9c:7b:5b:56:c5:f8:89:63:97:70:fd:78:6f:f1:c5:
60:81:5c:ae:c5:cb:44:49:e9:9f:32:15:1f:bc:43:
36:d3:73:54:f6:7a:1d:ed:84:c4:cd:0c:ee:01:a7:
63:35:cc:9c:e1:bd:6e:f7:5b:d0:9b:93:95:50:d5:
f1:38:3a:2f:7b:bf:ce:95:03:54:59:4d:cb:48:4a:
f4:68:8f:65:0b:be:71:de:a7:51:18:17:bc:3f:09:
e4:fe:05:9b:4f:90:7b:a7:0b:b0:31:74:d4:f3:e5:
05:8f:af:a5:be:b4:0c:45:be:3b:77:0d:b6:c8:59:
92:30:e6:ef:7b:3d:7c:21:51:31:03:21:6c:e4:e8:
fd:02:3f:eb:34:52:1d:51:02:2d:f8:db:7e:43:e7:
f7:f3
```

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 CRL Distribution Points:

URI:http://10.48.46.251/IOS_CA.crl

X509v3 Key Usage:

Digital Signature, Key Encipherment, Data Encipherment, Key Agreement

X509v3 Extended Key Usage:

TLS Web Server Authentication, TLS Web Client Authentication,

IPSec End System

X509v3 Authority Key Identifier:

keyid:94:8B:3F:97:27:3C:BF:1B:20:FE:D5:48:A2:ED:07:A6:75:B2:87:0E

X509v3 Subject Key Identifier:

78:9B:67:93:4B:21:0B:B1:D4:41:5B:83:11:99:B3:5D:4F:6A:A9:A5

Signature Algorithm: md5WithRSAEncryption

6e:54:9f:ad:55:2d:09:a8:fe:33:f5:38:04:7a:e3:1b:57:09:

f4:d0:24:ca:5f:3f:df:0a:e8:7a:47:fe:74:aa:af:09:84:44:

49:1a:24:7f:64:7b:c7:44:b7:fe:5d:ac:21:9e:81:3a:75:a3:

c0:98:4f:96:90:83:ed:1c:82:21:6c:c1:c2:6d:bc:46:f5:f7:

dd:c9:a8:8d:5d:15:b2:e6:c2:39:5f:27:05:d4:58:18:1a:94:

c5:05:80:fd:33:42:ea:b3:0f:85:21:86:93:d9:9a:db:38:6b:

31:f2:1e:a9:66:87:ac:2a:a9:bc:e5:10:72:21:48:d7:e2:72:

4a:d6

3. Importer des certificats CA, CUCM et GW voix sur CUCM

Le certificat IPsec CUCM est déjà exporté vers un fichier .pem. À l'étape suivante, le même processus doit être terminé avec le certificat GW voix et le certificat CA. Pour ce faire, ils doivent d'abord être affichés sur un terminal avec la commande **crypto pki export local1 pem terminal** et copiés dans des fichiers .pem séparés.

```
KRK-UC-2x2811-2 (config)#crypto pki export local1 pem terminal
```

```
% CA certificate:
```

```
-----BEGIN CERTIFICATE-----
```

```
MIIB9TCCA6gAwIBAgIBATANBgkqhkiG9w0BAQQFADAOMQwwCgYDVQQDEwNJT1Mw
HhcNMTEyMTIwMTE1MTEyWhcNMTEyMTIwMTE1MTEyWjAOMQwwCgYDVQQDEwNJT1Mw
gZ8wDQYJKoZIhvcNAQEBBQADGy0AMIGJAoGBAK6Cd2yxUywtbgBE1kZUsP6eaZVv
6YfpEbFptyt6ptRdpxgjOYI3InEP3wewtmEPNeTJL8+a/W7MDUemm3t/NlWBO6T2
m9Bp6k0FN0BXMKeDfTSqOKey7WfLASE/Pbq8M+JMpeMWz8xnMboYOb66rY8igZFz
k1tRPlIMsf5r01tnAgMBAAGjYzBhMA8GA1UdEwEB/wQFMAMBAf8wDgYDVR0PAQH/
BAQDAgGMB8GA1UdIwQYMBAAJFJSLP5cNPL8bIP7VSKLtB6Z1socOMB0GA1UdDgQW
BBSUiz+XJzy/GyD+1Ui7QemdbKHDjANBgkqhkiG9w0BAQQFAAOBgQCUMC1SFV1S
TSS1Exbm9i2D4HOWYhCurhifqTWLxMMXj0jym24DoqZ91aDNG1VwiJ/Yv4i40t90
y65WzbpZL1S65q+d7BCLQypdrwcKkdS0dfTdKfXESyWLhecRa8mnZckpgKBk8Ir
Bfm9K+caXkfhPEPa644UzV9++OKMKhtDuQ==
```

```
-----END CERTIFICATE-----
```


Certificate:

Data:

Version: 3 (0x2)

Serial Number: 2 (0x2)

Signature Algorithm: sha1WithRSAEncryption

Issuer: CN=IOS

Validity

Not Before: Nov 21 12:05:01 2014 GMT

Not After : Nov 21 12:05:01 2015 GMT

Subject: CN=KRK-UC-2x2811-2

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (512 bit)

Modulus (512 bit):

00:a4:65:88:37:59:c0:02:d2:8b:54:c3:a3:99:95:

64:40:58:08:f0:ba:c7:0f:ac:d2:ae:56:8a:80:02:

61:95:4f:87:fe:69:d1:41:0e:6b:aa:2b:48:a5:e9:

03:74:fa:28:c1:24:fd:47:10:b9:08:99:81:e2:ca:

53:55:69:18:93

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 CRL Distribution Points:

URI:http://10.48.46.251/IOS_CA.crl

X509v3 Key Usage:

Digital Signature, Key Encipherment

X509v3 Authority Key Identifier:

keyid:94:8B:3F:97:27:3C:BF:1B:20:FE:D5:48:A2:ED:07:A6:75:B2:87:0E

X509v3 Subject Key Identifier:

B4:05:9C:EB:52:B9:9D:81:A0:5A:A2:80:88:83:8B:32:5A:61:7E:A2

Signature Algorithm: sha1WithRSAEncryption

8c:37:e5:1f:e3:77:c9:cd:d1:ca:40:a2:83:d0:74:68:02:17:

59:93:e6:6a:a2:c5:f6:ff:51:ef:9c:dc:f9:ff:31:cd:b4:88:

ce:85:5b:06:19:d4:39:eb:8e:8f:58:67:22:01:f2:c8:c8:de:

10:b8:d3:12:1e:ae:42:b5:94:37:61:25:5b:5c:a9:7e:6c:64:

d6:33:79:ab:4b:7e:bd:f7:51:fb:27:a9:4b:4e:29:16:8a:fd:

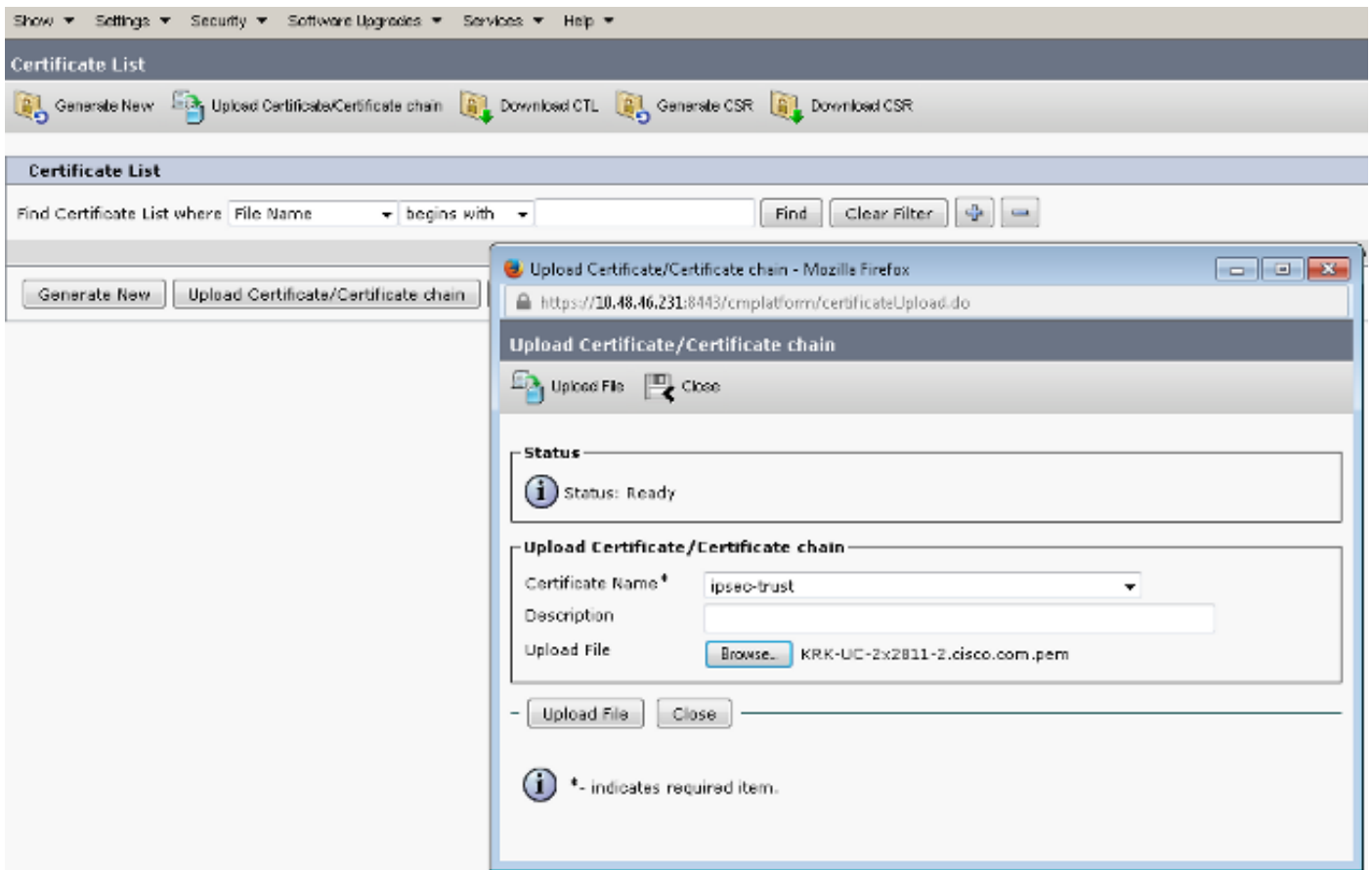
46:80:fb:21:68:3a:7b:fd:61:14:31:1e:a7:d8:41:bf:3a:d5:

c1:01:c2:8f:37:98:d2:b5:6b:3d:c2:e5:db:a9:39:a1:ab:8c:

c1:3b

Une fois enregistrés en tant que fichiers .pem, ils doivent être importés dans CUCM. Choisissez **Cisco Unified OS Administration > Security > Certificate management > Upload Certificate/Certificate**.

- Certificat CUCM en tant qu'IPsec
- Certificat GW voix en tant qu'IPsec-trust
- Certificat CA en tant qu'approbation IPsec :




4. Configurer les paramètres du tunnel IPsec sur CUCM

L'étape suivante est la configuration du tunnel IPsec entre CUCM et la passerelle vocale. La configuration du tunnel IPsec sur CUCM est effectuée via la page Web d'administration de Cisco Unified OS (https://<cucm_ip_address>/cmplatform). Choisissez **Security > IPSEC Configuration > Add new IPsec policy**.

Dans cet exemple, une stratégie appelée « vgipsecpolicy » a été créée, avec une authentification basée sur des certificats. Toutes les informations appropriées doivent être renseignées et correspondre à la configuration de la passerelle vocale.

- Status

 Status: Ready

- The system is in FIPS Mode

- IPSEC Policy Details

Policy Group Name*	vgipsecpolicy
Policy Name*	vgipsec
Authentication Method*	Certificate ▼
Peer Type*	Different ▼
Certificate Name	KRK-UC-2x2811-2.pem
Destination Address*	209.165.201.20
Destination Port*	ANY
Source Address*	209.165.201.10
Source Port*	ANY
Mode*	Transport ▼
Remote Port*	500
Protocol*	ANY ▼
Encryption Algorithm*	AES 128 ▼
Hash Algorithm*	SHA1 ▼
ESP Algorithm*	AES 128 ▼

- Phase 1 DH Group

Phase One Life Time*	3600
Phase One DH*	2 ▼

- Phase 2 DH Group

Phase Two Life Time*	3600
Phase Two DH*	2 ▼

- IPSEC Policy Configuration

Enable Policy

Note: Le nom du certificat de la passerelle vocale doit être spécifié dans le champ Nom du certificat.

5. Configurer le paramètre de tunnel IPsec sur la passerelle vocale

Cet exemple, avec des commentaires en ligne, présente la configuration correspondante sur un GW voix.

```

crypto isakmp policy 1      (defines an IKE policy and enters the config-isakmp mode)
  encr aes                 (defines the encryption)
  group 2                  (defines 1024-bit Diffie-Hellman)
  lifetime 57600           (isakmp security association lifetime value)

crypto isakmp identity dn   (defines DN as the ISAKMP identity)
crypto isakmp keepalive 10  (enable sending dead peer detection (DPD)
keepalive messages to the peer)
crypto isakmp aggressive-mode disable (to block all security association
and ISAKMP aggressive mode requests)

crypto ipsec transform-set cm3 esp-aes esp-sha-hmac (set of a combination of
security protocols
and algorithms that are
acceptable for use)
  mode transport
crypto ipsec df-bit clear
no crypto ipsec nat-transparency udp-encapsulation
!
crypto map cm3 1 ipsec-isakmp (selects data flows that need security
processing, defines the policy for these flows
and the crypto peer that traffic needs to go to)
  set peer 209.165.201.10
  set security-association lifetime seconds 28800
  set transform-set cm3
  match address 130

interface FastEthernet0/0
  ip address 209.165.201.20 255.255.255.224
  duplex auto
  speed auto
  crypto map cm3 (enables crypto map on the interface)

access-list 130 permit ip host 209.165.201.20 host 209.165.201.10

```

Vérification

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Vérifier l'état du tunnel IPsec sur la fin CUCM

La façon la plus rapide de vérifier l'état du tunnel IPsec sur CUCM est d'accéder à la page d'administration du système d'exploitation et d'utiliser l'option **ping** sous Services > Ping. Vérifiez que la case **Valider IPSec** est cochée. Évidemment, l'adresse IP spécifiée ici est l'adresse IP du GW.

Ping Configuration



Status



Status: Ready

Ping Settings

Hostname or IP Address*	<input type="text" value="209.165.201.20"/>
Ping Interval*	<input type="text" value="1.0"/>
Packet Size*	<input type="text" value="56"/>
Ping Iterations	<input type="text" value="1"/>
<input checked="" type="checkbox"/> Validate IPsec	

Ping Results

```
Validate IPsec Policy: 209.165.201.10[any] 209.165.201.20[any] Protocol: any  
Successfully validated IPsec connection to 209.165.201.20
```

Ping

Note: Reportez-vous à ces ID de bogue Cisco pour obtenir des informations sur la validation du tunnel IPsec via la fonctionnalité ping sur CUCM :

- ID de bogue Cisco [CSCuo53813](#) - Valider les résultats de la commande ping IPsec vides lors de l'envoi de paquets ESP (Encapsulating Security Payload)
- ID de bogue Cisco [CSCud20328](#) - La validation de la stratégie IPsec affiche un message d'erreur incorrect en mode FIPS

Vérification de l'état du tunnel IPsec sur l'extrémité de la passerelle vocale

Afin de vérifier si l'installation fonctionne correctement ou non, il faut confirmer que les associations de sécurité (SA) pour les deux couches (Internet Security Association and Key Management Protocol (ISAKMP) et IPsec) sont créées correctement.

Afin de vérifier si la SA pour ISAKMP est créée et fonctionne correctement, entrez la commande **show crypto isakmp sa** sur le GW.

```
KRK-UC-2x2811-2#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst src state conn-id status
209.165.201.20 209.165.201.10 QM_IDLE 1539 ACTIVE

IPv6 Crypto ISAKMP SA
```

Note: L'état correct pour l'association de sécurité doit être ACTIVE et QM_IDLE.

La deuxième couche est les SA pour IPsec. Leur état peut être vérifié avec la commande **show crypto ipsec sa**.

```
KRK-UC-2x2811-2#show crypto ipsec sa

interface: FastEthernet0/0
Crypto map tag: cm3, local addr 209.165.201.20

protected vrf: (none)
local ident (addr/mask/prot/port): (209.165.201.20/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (209.165.201.10/255.255.255.255/0/0)
current_peer 209.165.201.10 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 769862, #pkts encrypt: 769862, #pkts digest: 769862
#pkts decaps: 769154, #pkts decrypt: 769154, #pkts verify: 769154
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 211693, #recv errors 0

local crypto endpt.: 209.165.201.20, remote crypto endpt.: 209.165.201.10
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
current outbound spi: 0xA9FA5FAC(2851757996)
PFS (Y/N): N, DH group: none

inbound esp sas:
spi: 0x9395627(154752551)
transform: esp-aes esp-sha-hmac ,
in use settings ={Transport, }
conn id: 3287, flow_id: NETGX:1287, sibling_flags 80000006, crypto map: cm3
sa timing: remaining key lifetime (k/sec): (4581704/22422)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0xA9FA5FAC(2851757996)
transform: esp-aes esp-sha-hmac ,
in use settings ={Transport, }
conn id: 3288, flow_id: NETGX:1288, sibling_flags 80000006, crypto map: cm3
sa timing: remaining key lifetime (k/sec): (4581684/22422)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE

outbound ah sas:
```

outbound pcp sas:
KRK-UC-2x2811-2#

Note: Les index de stratégie de sécurité (SPI) entrants et sortants doivent être créés dans l'état ACTIVE, et les compteurs du nombre de paquets encapsulés/décapsulés et chiffrés/décryptés doivent augmenter chaque fois qu'un trafic via un tunnel est généré.

La dernière étape consiste à confirmer que le GW MGCP est à l'état enregistré et que la configuration TFTP a été téléchargée correctement à partir de CUCM sans aucune défaillance. Ceci peut être confirmé à partir du résultat de ces commandes :

```
KRK-UC-2x2811-2#show ccm-manager
MGCP Domain Name: KRK-UC-2x2811-2.cisco.com
Priority Status Host
=====
Primary Registered 209.165.201.10
First Backup None
Second Backup None

Current active Call Manager: 10.48.46.231
Backhaul/Redundant link port: 2428
Failover Interval: 30 seconds
Keepalive Interval: 15 seconds
Last keepalive sent: 09:33:10 CET Mar 24 2015 (elapsed time: 00:00:01)
Last MGCP traffic time: 09:33:10 CET Mar 24 2015 (elapsed time: 00:00:01)
Last failover time: None
Last switchback time: None
Switchback mode: Graceful
MGCP Fallback mode: Not Selected
Last MGCP Fallback start time: None
Last MGCP Fallback end time: None
MGCP Download Tones: Disabled
TFTP retry count to shut Ports: 2

Backhaul Link info:
Link Protocol: TCP
Remote Port Number: 2428
Remote IP Address: 209.165.201.10
Current Link State: OPEN
Statistics:
Packets recvd: 0
Recv failures: 0
Packets xmitted: 0
Xmit failures: 0
PRI Ports being backhauled:
Slot 0, VIC 1, port 0
FAX mode: disable
Configuration Error History:
KRK-UC-2x2811-2#

KRK-UC-2x2811-2#show ccm-manager config-download
Configuration Error History:
KRK-UC-2x2811-2#
```

Dépannage

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

Dépannage du tunnel IPsec sur l'extrémité CUCM

Sur CUCM, il n'existe aucun service de maintenance responsable de la terminaison et de la gestion IPsec. CUCM utilise un package d'outils Red Hat IPsec intégré au système d'exploitation. Le démon qui s'exécute sur Red Hat Linux et termine la connexion IPsec est OpenSwan.

Chaque fois que la stratégie IPsec est activée ou désactivée sur CUCM (Administration du système d'exploitation > Sécurité > Configuration IPSEC), le démon Openswan est redémarré. Ceci peut être observé dans le journal des messages Linux. Un redémarrage est indiqué par les lignes suivantes :

```
Nov 16 13:50:17 cucmipsec daemon 3 ipsec_setup: Stopping Openswan IPsec...
Nov 16 13:50:25 cucmipsec daemon 3 ipsec_setup: ...Openswan IPsec stopped
(...)
Nov 16 13:50:26 cucmipsec daemon 3 ipsec_setup: Starting Openswan IPsec
U2.6.21/K2.6.18-348.4.1.el5PAE...
Nov 16 13:50:32 cucmipsec daemon 3 ipsec_setup: ...Openswan IPsec started
```

Chaque fois qu'il y a un problème avec la connexion IPsec sur CUCM, les dernières entrées du journal des messages doivent être vérifiées (entrez la commande **file list activelog syslog/messages***) afin de confirmer que Openswan est actif et s'exécute. Si Openswan s'exécute et a démarré sans erreur, vous pouvez dépanner la configuration IPsec. Le démon responsable de la configuration des tunnels IPsec dans Openswan est Pluto. Les journaux Pluto sont écrits afin de sécuriser les journaux sur Red Hat, et ils peuvent être rassemblés via le **fichier get activelog syslog/secure.*** ou via **RTMT : Journaux de sécurité**.

Note: Vous trouverez plus d'informations sur la façon de collecter des journaux via le RTMT dans la [documentation RTMT](#).

S'il est difficile de déterminer la source du problème à partir de ces journaux, IPsec peut être vérifié plus avant par le centre d'assistance technique (TAC) via root sur le CUCM. Une fois que vous avez accédé à CUCM via la racine, les informations et les journaux sur l'état IPsec peuvent être vérifiés à l'aide des commandes suivantes :

```
ipsec verify (used to identify the status of Pluto daemon and IPSec)
ipsec auto --status
ipsec auto --listall
```

Il existe également une option permettant de générer un rapport Red Hat sosreport via root. Ce rapport contient toutes les informations requises par le support de Red Hat afin de résoudre d'autres problèmes au niveau du système d'exploitation :

```
sosreport -batch - output file will be available in /tmp folder
```

Dépannage du tunnel IPsec sur l'extrémité de la passerelle vocale

Sur ce site, vous pouvez dépanner toutes les phases de la configuration du tunnel IPsec après avoir activé ces commandes de débogage :

```
debug crypto ipsec
debug crypto isakmp
```


Note: Des étapes détaillées pour dépanner IPsec sont disponibles dans [Dépannage IPsec : Présentation et utilisation des commandes de débogage.](#)

Vous pouvez dépanner les problèmes MGCP GW avec les commandes de débogage suivantes :

```
debug ccm-manager config download all
debug ccm-manager backhaul events
debug ccm-manager backhaul packets
debug ccm-manager errors
debug ccm-manager events
debug mgcp packet
debug mgcp events
debug mgcp errors
debug mgcp state
debug isdn q931
```