

# Beveiligde MGCP-communicatie tussen Voice GW en CUCM via IPsec gebaseerd op CA-ondertekende Configuratievoorbeeld voor certificaten

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Netwerkdigram](#)

[1. Configureer de CA in de Voice GW en genereer een CA-ondertekend certificaat voor spraak GW](#)

[2. Generate een CUCM CA-ondertekend IPsec-certificaat](#)

[3. Importeer CA, CUCM en Voice GW CA-certificaten op CUCM](#)

[4. Het configureren van IPsec-tunnelinstellingen op CUCM](#)

[5. Het configureren van de IPsec-tunnelinstelling op de Voice GW](#)

[Verifiëren](#)

[Controleer de IPsec-tunnelstatus op het CUCM-einde](#)

[Controleer de IPsec-tunnelstatus in het einde van de spraakgateway](#)

[Problemen oplossen](#)

[Probleemoplossing voor de IPsec-tunnels in het CUCM-einde](#)

[Probleemoplossing voor de IPsec-tunnels in het einde van de spraakgateway](#)

## Inleiding

Dit document beschrijft hoe u Media Gateway Control Protocol (MGCP) (MGCP) signalering kunt beveiligen tussen een spraakgateway (GW) en CUCM (Cisco Unified Communications Manager) via Internet Protocol Security (IPsec), gebaseerd op certificaten van de certificaatautoriteit (CA). Om een beveiligde oproep via MGCP op te zetten, moeten signalering en realtime Transport Protocol (RTP)-stromen afzonderlijk worden beveiligd. Het lijkt goed gedocumenteerd en vrij eenvoudig te zijn om versleutelde RTP-stromen in te stellen, maar een beveiligde RTP-stream bevat geen beveiligde MGCP-signalering. Als de MGCP-signalering niet is beveiligd, worden de encryptiesleutels voor de RTP-stream in het display verzonden.

## Voorwaarden

## Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- MGCP spraagateway geregistreerd op CUCM om oproepen te verzenden en ontvangen
- Service van certificeringsinstanties Proxy (CAPF) gestart, cluster ingesteld op gemengde modus
- Cisco IOS<sup>®</sup> afbeelding op GW ondersteunt crypto security functie
- Telefoons en MGCP GW ingesteld voor Secure Real-time Transport Protocol (SRTP)

## Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

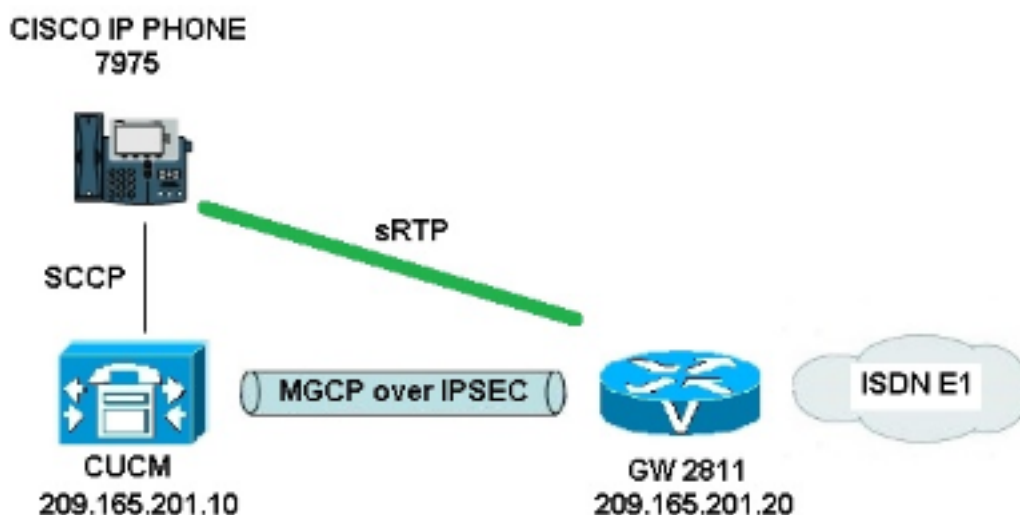
- CUCM - één knooppunt - voert GSG (Cisco's Global Government Solutions Group) versie 8.6.1.2012-14 uit in de modus Federal Information Processing Standard (FIPS)
- 7975 telefoons die SCCP75-9-3-1SR2-1S draaien
- GW - Cisco 2811 - C2800NM-ADVENTERPRISEK9-M, versie 15.1(4)M8
- E1 ISDN-spraakkaart - VWIC2-12MFT-T1/E1 - 2-poorts RJ-48 Multiflex Trunk

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

## Configureren

**Opmerking:** Gebruik de [Command Lookup Tool \(alleen voor geregistreeerde gebruikers\) voor meer informatie over de opdrachten die in deze sectie worden gebruikt.](#)

## Netwerkdigram



Voltooi de volgende stappen om IPsec tussen CUCM en Voice GW met succes in te stellen:

1. Configureer de CA op de spraak GW en genereer een CA-ondertekend certificaat voor spraak GW
2. Een door CUCM CA ondertekend IPsec-certificaat genereren
3. CA, CUCM en Voice GW CA-certificaten importeren op CUCM
4. IPsec-tunnelinstellingen configureren op CUCM
5. Configuratie van de IPsec-tunnelinstelling op de spraak GW

## 1. Configureer de CA in de Voice GW en genereer een CA-ondertekend certificaat voor spraak GW

Als eerste stap moet het sleutelbaar Rivest-Shamir-Add (RSA) worden gegenereerd op de spraak-GW (Cisco IOS CA server):

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

Invoeringen die via Simple certificaatinschrijving Protocol (SCEP) zijn voltooid, worden gebruikt, zodat de HTTP-server kan worden gebruikt:

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

Om de CA Server op een gateway te configureren moeten deze stappen worden voltooid:

1. Stel de PKI servernaam in. Het moet dezelfde naam hebben als het sleutelbaar dat eerder gegenereerd is.  

```
KRK-UC-2x2811-2 (config)#crypto pki server IOS_CA
```
2. Specificeer de locatie waar alle databases worden opgeslagen voor de CA-server.  

```
KRK-UC-2x2811-2 (cs-server)#crypto pki server IOS_CA
```
3. Configureer de naam van de CA-emittent.  

```
KRK-UC-2x2811-2 (cs-server)#issuer-name cn=IOS
```
4. Specificeer een certificeringslijst (CRL) van certificaten die worden gebruikt in certificaten die door de certificaatserver worden uitgegeven en waardoor automatische verlening van certificaten opnieuw kan worden aangevraagd voor een Cisco IOS ondergeschikte CA-server.  

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

```
KRK-UC-2x2811-2 (cs-server)#grant auto
```
5. Schakel de CA-server in.  

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

De volgende stap is om een betrouwbaar punt voor het certificaat van CA en een lokaal trustpunt voor het routercertificaat met een URL te creëren die aan een lokale HTTP server wijst:

```
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)#rsa keypair 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
```

Om het certificaat van de router te genereren dat door lokale CA wordt ondertekend moet het betrouwbaar punt geauthenticeerd worden en ingeschreven worden:

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

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

Daarna wordt het certificaat van de router gegenereerd en ondertekend door de lokale CA. Maak een lijst van het certificaat op de router ter verificatie.

```
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

Twee certificaten dienen te worden vermeld. Het eerste is het certificaat van een router (KRK-UC-2x2811-2), ondertekend door de lokale CA en het tweede is CA certificaat.

## 2. Generate een CUCM CA-ondertekend IPsec-certificaat

De CUCM voor IPsec-tunnelversie gebruikt een ipsec.pem-certificaat. Dit certificaat is standaard zelf ondertekend en gegenereerd wanneer het systeem is geïnstalleerd. Om deze te vervangen door een CA-ondertekend certificaat, moet eerst een CSR (certificaataanvraag) voor IPsec uit de CUCM OS Admin-pagina worden gegenereerd. Kies **Cisco Unified OS-beheer > Beveiliging > certificaatbeheer > Generate CSR**.

Show Settings Security Software Upgrades Services Help

### Certificate List

Generate New Upload Certificate/Certificate chain Generate CSR Download CSR

Status

21 records found

Certificate Name	Certificate Type
tomcat	certs
ipsec	certs
tomcat-trust	trust-certs
tomcat-trust	trust-certs
tomcat-trust	trust-certs
ipsec-trust	trust-certs
CallManager	certs
CAPF	certs
TVS	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

Generate Certificate Signing Request - Mozilla Firefox

https://10.48.46.227/cmplatform/certificateGenerateNewCsr.do

#### Generate Certificate Signing Request

Generate CSR Close

Status

**Warning:** Generating a new CSR will overwrite the existing CSR

Generate Certificate Signing Request

Certificate Name\* ipsec

Generate CSR Close

\* indicates required item.

Nadat het CSR gegenereerd is, moet het van CUCM worden gedownload en tegen de CA in de GW worden ingeschreven. Om dat te doen, voer de **crypto server IOS\_CA** verzoek om **pkcs10 terminal base64** opdracht in en de de hak van de gebarentaanvraag moet via terminal worden geplakt. Het toegekende certificaat wordt weergegeven en moet worden gekopieerd en opgeslagen als het ipsec.pem-bestand.

```
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-----
MIIDNjCCA4CAQAwgaxkCzAJBgNVBAYTA1BMMQ4wDAYDVQQIEwVjaXNjbzEOMAwG
A1UEBxMFY2lzY28xDjAMBgNVBAoTBWNpc2NvMQ4wDAYDVQQLEwVjaXNjbzEPMA0G
A1UEAxMQQ1VDTUIxMkxwRwYDVQQFE0A1NjY2OWY5MjgzNWZmZWZmZWZmZWZmZWZm
NjcwMDBmMGI2NjliYjYkYXZhdnNDNmM2QzOWFhNGQxMzZlMjZlMjZlMjZlMjZlMjZl
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAKfHxvcov4vFmK+3+dQShW3s3SzAYBQ19
0JDBIic4eDRmdrq0V2dKn9UpLUx90H7V0Oe/8wmHqYwoxFZ5a6B5qRRkc010/ub2
ul1QCw+nQ6QiZGdNhdne0NYY4r3odF4CkrtYAJA4PUSce1tWxfiJY5dw/Xhv8cVg
gVyxctESemfMhUfvEM203NU9nod7YTEzQzuAadjNcyc4blu91vQm5OVUNXxODov
e7/O1QNUWU3LSEr0aI9lC75x3qdRGBe8Pwnk/gWbT5B7pwuwMXTU8+UFj6+1vrQM
Rb47dw22yFmSMObvez18IVExAyFs50j9Aj/rNFidUQIt+Nt+Q+f38wIDAQABoEcw
RQYJKoZIhvcNAQkOMTgwNjAnBgNVHSUEIDAEBggrBgEFBQcDAQYIKwYBBQUHAWIG
CCsGAQUFBwMFMA5GA1UdDwQEAwIDuANBgkqhkiG9w0BAQUFAAOCAQEADgAR40l
oQ4z2yqgSsICAZ2hQA3Vztp6aOI+0PSyMfihGS//3V3tALEZL2+t0Y5elKsBea72
sieKjpSikXjNaj+Siy1aYy4siVw5EKQD3Ii4Qv115BvuniZXvBiQUw+SpBLbeNi
xwIgrYELrFywQZBeZodFqnSKN9XlisXe6oU9GXux7uwgXwkCXMF/azutbiol4Fgf
qUF00GzkhtEapJA6c5RzaxG/0uDuKY+4z1eSSsXzFhBTifk3RfJA+I7Na1zQBIEJ
2IOJdiZnn0HWVr5C5eZ7VnQuNdiC/qn3uUfvNVRZo8iCdQ3tRv7dr/n64jdKsHEM
lk6P8gp9993cJw==
quit
```

% Granted certificate:

```
MIIDXTCCAsagAwIBAgIBBTANBgkqhkiG9w0BAQQFADAOMQwwCgYDVQQDEwNJT1Mw
HhcNMTUwMTA4MTIwMTAwWhcNMTYwMTA4MTIwMTAwWjCBqTELMAkGA1UEBhMCUEwx
DjAMBgNVBAgTBWNpc2NvMQ4wDAYDVQQHEwVjaXNjbzEOMAwGA1UEChMFY21zY28x
DjAMBgNVBAStBWNpc2NvMQ8wDQYDVQQDEwZDVUNNQjExSTBHBgNVBAUTQDU2NjY5
ZjkyODM1ZmZlZDUwODRimjxNtG2NzAwMGYwYjY2OWJiN2RhZmE0M2YzZDM5YWE0
ZDEzMzVlOWUyNTMwgGEMAA0GCSqSIB3DQEBAQUAA4IBDwAwggEKAoIBAQC8fG9
yi/i8WYr7f51BKFbezDLMBgFDX3QkMGihzh4NGZ2urRXZ2Sf1SktTH04ftXQ57/z
CYepjCjEVnlroHmpFGRw7XT+5va6XVALD6dDpCJkZ02F2d7Q1hjhiveh0XgKSu1gA
kDg9RjX7W1bF+Ilj13D9eG/xxWCBXK7Fy0RJ6Z8yFR+8QzbTc1T2eh3thMTND04B
p2M1zJzhvW73W9Cbk5VQ1fE4Oi97v86VA1RZTctISvRoj2ULvnHep1EYF7w/CeT+
BZtPkHunC7AxdNTz5QWPr6W+tAxFvj3DbbIWZlw5u97PXwhUTEDIWzk6P0CP+s0
Uh1RAi34235D5/fzAgMBAAGjgaowgacwLwYDVR0fBCgwJjAkoCKgIIYeaHR0cDov
LzEwLjQ4LjQ2LjI1MS9JT1NfQ0EuY3JsMAsGA1UdDwQEAwIDuDanBgNVHSUEIDAe
BggrBgEFBQcDAQYIKwYBBQUHAWIGCCsGAQUFBwMFMB8GA1UdIwQYBAAFJSLP5cn
PL8bIP7VSKLtB6Z1socOMB0GA1UdDgQWBRR4m2eTSyELsdRBW4MRmbNdT2qppTAN
BgkqhkiG9w0BAQQFAAOBQBuVJ+TVS0JqP4z9TgEeuMbVwn00CTKXz/fCuh6R/50
qq8JhERJGiR/ZHvHRLf+XawhnoE6daPAmE+WkIPtHIhbmhMChbxG9ffdyaiNXRWy
5sI5XycF1FgYGpTFBYD9M0Lqsw+FIYaT2ZrbOGsx8h6pZoesKqm85RByIUjX4nJK
1g==
```

**Opmerking:** Om de inhoud van het Base64 gecodeerde certificaat te decoderen en te controleren, voert u de **openssl x509 -in certificaat.crt -text** - noout opdracht in.

Het toegekende CUCM-certificaat besluit:

```
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. Importeer CA, CUCM en Voice GW CA-certificaten op CUCM

Het CUCM IPsec-certificaat wordt al geëxporteerd naar een .pem-bestand. Als volgende stap moet hetzelfde proces worden voltooid met het Voice GW-certificaat en het CA-certificaat. Om dat te doen, moeten ze eerst op een terminal worden weergegeven met de **crypto pki opdracht om lokale1 pem terminal uit te voeren** en gekopieerd worden om .pem bestanden te scheiden.

```
KRK-UC-2x2811-2 (config)#crypto pki export local1 pem terminal
% CA certificate:
-----BEGIN CERTIFICATE-----
MIIB9TCCA6AwIBAgIBATANBgkqhkiG9w0BAQQFADAOMQwwCgYDVQQDEwNJT1Mw
HhcNMTQxMTE1MTEyWWhcNMTc4MTIwMTE1MTEyWjAOMQwwCgYDVQQDEwNJT1Mw
gZ8wDQYJKoZIhvcNAQEBBQADGy0AMIGJAoGBAK6Cd2yxUywtbgBElkZUsP6eaZVv
6YfpEbFptyt6ptRdpxgjOYI3InEP3wewtmEPNeTJL8+a/W7MDUemm3t/NlWBO6T2
m9Bp6k0FNOBXMKeDfTsQOKey7WfLASE/Pbq8M+JMpeMWz8xnMboYOb66rY8igZFz
k1tRPlIMsf5r01tnAgMBAAGjYzBhMA8GA1UdEwEB/wQFMAMBAf8wDgYDVR0PAQH/
BAQDAgGGMB8GA1UdIwQYMBAAJFJSLP5cnPL8bIP7VSKLtB6Z1socOMB0GA1UdDgQW
BBSUiz+XJzy/GyD+1Ui7QemdbKHDjANBgkqhkiG9w0BAQQFAAOBgQCUMC1SFV1S
TSS1Exbm9i2D4HOWYhCurhifqTWLxMMXj0jym24DoqZ91aDNG1VwiJ/Yv4i40t90
y65WzbpZL1S65q+d7BCLQypdrwcKkdS0dfTdkfXESyWLhecRa8mnZckpgKBk8Ir
Bfm9K+caXkfhPEPa644UzV9++OKMKhtDuQ==
-----END CERTIFICATE-----

% General Purpose Certificate:
-----BEGIN CERTIFICATE-----
MIIB2zCCAUSgAwIBAgIBAJANBgkqhkiG9w0BAQUFADAOMQwwCgYDVQQDEwNJT1Mw
HhcNMTQxMTE1MTEyWWhcNMTUxMTE1MTEyWjAAMRgwFgYDVQQDEw9LUkst
VUMtMngyODExLTUwXDNANBgkqhkiG9w0BAQEFAANLADBIaKEApGWIN1nAAAtKLVMoj
mZVqQFgI8LrHD6zSrlaKgaJh1u+H/mnRQQ5rqi tIpekDdPoowST9RxC5CJmB4spT
VWkYkwIDAQABo4GAMH4wLwYDVR0fBCgwJjAkoCKgIIYeHR0cDovLzEwLjQ4LjQ2
LjI1MS9JT1NfQ0EuY3JsmASGA1UdDwQEAwIFoDafBgNVHSMEGDAWgBSUiz+XJzy/
GyD+1Ui7QemdbKHDjAdBgNVHQ4EFgQUtAWc61K5nYGgWqKAiIOLMlphfqIwDQYJ
KoZIhvcNAQEFBQADgYEAJdf1h+N3yc3RykCig9B0aAIXWZPmaqLF9v9R75zc+f8x
zbSiZoVbBhnUOeuOj1hnIghyymjeELjTEh6uQrWUN2ElW1ypfmxk1jn5q0t+vfdr
+yepS04pFor9R0d7IWg6e/1hFDEep9hBvzrVwQHCjzeY0rVrPcLl26k5oauMwTs=
-----END CERTIFICATE-----
```

## Het % CA-certificaat besluit tot:

### Certificate:

Data&colon;

Version: 3 (0x2)

Serial Number: 1 (0x1)

Signature Algorithm: md5WithRSAEncryption

Issuer: CN=IOS

Validity

Not Before: Nov 21 11:51:12 2014 GMT

Not After : Nov 20 11:51:12 2017 GMT

Subject: CN=IOS

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (1024 bit)

Modulus (1024 bit):

00:ae:82:77:6c:b1:53:2c:2d:6e:00:44:96:46:54:  
b0:fe:9e:69:95:6f:e9:87:e9:11:b1:69:b7:2b:7a:  
a6:d4:5d:a7:18:23:39:82:37:22:71:0f:df:07:b0:  
b6:61:0f:35:e4:c9:2f:cf:9a:fd:6e:cc:0d:47:a6:  
9b:7b:7f:36:55:81:3b:a4:f6:9b:d0:69:ea:4d:05:  
34:e0:57:30:a7:83:7d:34:aa:38:a1:32:ed:67:cb:  
01:27:bf:3d:ba:bc:33:e2:4c:a5:e3:16:cf:cc:67:  
31:ba:18:39:be:ba:ad:8f:22:81:91:73:93:5b:51:  
3e:52:0c:49:fe:6b:3b:5b:67

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Basic Constraints: critical

CA:TRUE

X509v3 Key Usage: critical

Digital Signature, Certificate Sign, CRL Sign

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:

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

Signature Algorithm: md5WithRSAEncryption

94:30:2d:52:15:59:52:4d:24:b5:13:16:cc:f6:2d:83:e0:73:  
96:62:10:ae:ae:18:9f:a9:35:8b:c4:c3:17:8f:48:f2:9b:6e:  
03:a2:a6:7d:d5:a0:cd:1b:55:70:88:9f:d8:bf:88:b8:d2:df:  
74:cb:ae:56:cd:b6:a9:64:bd:52:eb:9a:be:77:b0:42:2d:0c:  
a9:76:bc:1c:2a:47:52:d1:d7:d3:74:a7:d7:12:cc:96:2e:17:  
9c:45:af:26:9d:97:24:a6:02:81:93:c2:2b:05:f3:3d:2b:e7:  
1a:5e:47:e1:3c:43:da:eb:8e:14:cd:5f:7e:f8:e2:8c:2a:1b:  
43:b9

## Het certificaat voor algemene doeleinden van % bepaalt:

### Certificate:

Data&colon;

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

Nadat ze als .pem-bestanden zijn opgeslagen, moeten ze naar CUCM worden geïmporteerd. Kies **Cisco Unified OS-beheer > Beveiliging > certificaatbeheer > Uploadcertificaat/certificaat.**

- CUCM-certificaat als IPsec
- Voice GW-certificaat als IPsec-vertrouwen
- CA-certificaat als IPsec-trust:

The screenshot shows the Cisco Unified OS Management interface. The main window displays the 'Certificate List' page with a search bar and several buttons: 'Generate New', 'Upload Certificate/Certificate chain', 'Download CTL', 'Generate CSR', and 'Download CSR'. An 'Upload Certificate/Certificate chain' dialog box is open in the foreground, showing the 'Status' as 'Ready'. The 'Certificate Name' is set to 'ipsec-trust'. The 'Upload File' field contains the file path 'KRK-UC-2x2811-2.cisco.com.pem'. The dialog box also includes 'Upload File' and 'Close' buttons and a note: '\* - indicates required item.'


## 4. Het configureren van IPsec-tunnelinstellingen op CUCM

De volgende stap is het configureren van de IPsec-tunnel tussen CUCM en de spraakgateway. De IPsec-tunnelconfiguratie op CUCM wordt uitgevoerd via de Cisco Unified OS-beheerwebpagina ([https://<cucm\\_ip\\_adres>/com](https://<cucm_ip_adres>/com)). Kies **Beveiliging > IPSEC Configuration > Add new IPsec-beleid**.

In dit voorbeeld werd een beleid gecreëerd dat "vgp secpolicy" werd genoemd, met authenticatie gebaseerd op certificaten. Alle relevante informatie moet worden ingevuld en dient overeen te komen met de configuratie op de spraak-GW.

---

**- Status**

 Status: Ready

---

**- The system is in FIPS Mode**

---

**- IPSEC Policy Details**

Policy Group Name*	<input type="text" value="vgipsecpolicy"/>
Policy Name*	<input type="text" value="vgipsec"/>
Authentication Method*	<input type="text" value="Certificate"/>
Peer Type*	<input type="text" value="Different"/>
Certificate Name	<input type="text" value="KRK-UC-2x2811-2.pem"/>
Destination Address*	<input type="text" value="209.165.201.20"/>
Destination Port*	<input type="text" value="ANY"/>
Source Address*	<input type="text" value="209.165.201.10"/>
Source Port*	<input type="text" value="ANY"/>
Mode*	<input type="text" value="Transport"/>
Remote Port*	<input type="text" value="500"/>
Protocol*	<input type="text" value="ANY"/>
Encryption Algorithm*	<input type="text" value="AES 128"/>
Hash Algorithm*	<input type="text" value="SHA1"/>
ESP Algorithm*	<input type="text" value="AES 128"/>

---

**- Phase 1 DH Group**

Phase One Life Time*	<input type="text" value="3600"/>
Phase One DH*	<input type="text" value="2"/>

---

**- Phase 2 DH Group**

Phase Two Life Time*	<input type="text" value="3600"/>
Phase Two DH*	<input type="text" value="2"/>

---

**- IPSEC Policy Configuration**

Enable Policy

**Opmerking:** De naam van het certificaat van spraakgateway moet in het veld Naam van het certificaat worden gespecificeerd.

## 5. Het configureren van de IPsec-tunnelinstelling op de Voice GW

Dit voorbeeld, met inline commentaren, presenteert de overeenkomstige configuratie op een stemGW.

```
crypto isakmp policy 1      (defines an IKE policy and enters the config-iskmp 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 creypto map on the interface)

access-list 130 permit ip host 209.165.201.20 host 209.165.201.10
```

## Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

## Controleer de IPsec-tunnelstatus op het CUCM-einde

De snelste manier om de IPsec-tunnelstatus op CUCM te controleren is naar de pagina OS-beheer te gaan en de optie ping onder Services > Ping te gebruiken. Zorg ervoor dat het vakje **IPSec-wissen** is ingeschakeld. Duidelijk, is het IP adres dat hier vermeld is het IP adres van de GW.

## Ping Configuration



Ping

### 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

**Opmerking:** Zie deze Cisco bug ID's voor informatie over de validatie van de IPsec-tunnel via de ping-functie op CUCM:

- Cisco bug-ID [CSCuo53813](#) - valideren IPsec Ping resultaten blanco wanneer ESP (Encapsulation Security Payload)-pakketten worden verzonden
- Cisco bug-ID [CSCud20328](#) - validerend IPsec-beleid toont onjuiste foutmelding in FIPS-modus

## Controleer de IPsec-tunnelstatus in het einde van de spraakgateway

Om te verifiëren of de setup-instelling goed werkt of niet, moet worden bevestigd dat de Security Associations (SA's) voor beide lagen (Internet Security Association en Key Management Protocol (ISAKMP) en IPsec) correct zijn gemaakt.

Om te controleren of de SA voor ISAKMP gecreëerd is en correct werkt, voer de **show crypto isakmp sa** opdracht in op de 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
```

**Opmerking:** De juiste status voor de SA zou ACTIVE en QM\_IDLE moeten zijn.

De tweede laag is SAs voor IPsec. Hun status kan worden geverifieerd met de **show crypto ipsec als** opdracht.

```
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#

**Opmerking:** Inbound and outbound Security Policy Indexes (SPI's) moet worden gemaakt in status-actief en tellers voor het aantal ingekapselde/gedecapsuleerde en gecodeerde/gedecrypteerde pakketten moeten groeien telkens wanneer er verkeer via een tunnel wordt gegenereerd.

De laatste stap is te bevestigen dat de MGCP GW in de geregistreerde toestand is en dat de TFTP-configuratie correct van CUCM is gedownload zonder dat er fouten zijn gemaakt. Dit kan worden bevestigd vanuit de uitvoer van deze opdrachten:

```
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#
```

## Problemen oplossen

Deze sectie verschaft informatie die u kunt gebruiken om problemen met uw configuratie op te

lossen.

## Probleemoplossing voor de IPsec-tunnels in het CUCM-einde

Op CUCM is er geen service die verantwoordelijk is voor de beëindiging en het beheer van IPsec. CUCM gebruikt een Rood Hat IPsec-hulppakket dat in het besturingssysteem is ingebouwd. De daemon die op Red Hat Linux draait en de IPsec-verbinding beëindigt is OpenSwan.

Elke keer dat het IPsec-beleid is ingeschakeld of uitgeschakeld op CUCM (OS-beheer > Security > IPSEC-configuratie), wordt de Openswan-pagina opnieuw gestart. Dit kan worden waargenomen in het Linux-berichtenlog. Een herstart is geïndiceerd door deze lijnen:

```
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.e15PAE...
Nov 16 13:50:32 cucmipsec daemon 3 ipsec_setup: ...Openswan IPsec started
```

Telkens wanneer er een probleem is met de IPsec-verbinding op CUCM, moeten de laatste items in het berichtenlog worden gecontroleerd (voer de opdracht **bestands list actief syslog/berichten\*** in) om te bevestigen dat Openswan in bedrijf is en actief is. Als Openswan zonder fouten draait en gestart is, kunt u de IPsec-instelling problemen oplossen. De daemon die verantwoordelijk is voor het instellen van IPsec-tunnels in Openswan is Pluto. Pluto-logs worden geschreven om boomstammen te beveiligen op Red Hat, en ze kunnen worden verzameld via het **bestand om activelog syslog/security te verkrijgen.\*** opdracht of via RTMT: **Beveiligingslogboek**.

**Opmerking:** Meer informatie over het verzamelen van logbestanden via de RTMT is te vinden in de [RTMT - documentatie](#).

Als het lastig is de bron van het probleem te bepalen op basis van deze bestanden, kan IPsec verder worden geverifieerd door het Technical Assistance Center (TAC) via de basis op het CUCM. Nadat u CUCM via root hebt benaderd, kunnen informatie en logbestanden over de IPsec-status met deze opdrachten worden gecontroleerd:

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

Er is ook een optie om via root een 'Red Hat'-rapport op te stellen. Dit rapport bevat alle informatie die door de ondersteuning van Red Hat vereist is om verdere problemen op het niveau van het besturingssysteem op te lossen:

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

## Probleemoplossing voor de IPsec-tunnels in het einde van de spraakgateway

Op deze site kunt u alle fasen van de installatie van de IPsec-tunnel opnieuw instellen nadat u deze debug-opdrachten hebt ingeschakeld:

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

**Opmerking:** Gedetailleerde stappen om IPsec-problemen op te lossen zijn gevonden in [IPsec-probleemoplossing: Opdrachten begrijpen en gebruiken debug](#).

U kunt problemen met MGCP GW-problemen oplossen bij deze debug-opdrachten:

```
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
```