

Comunicação MGCP segura entre voz GW e CUCM via IPsec com base no exemplo de configuração de certificados assinados pela CA

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de Rede](#)

[1. Configurar a CA no GW de voz e gerar um certificado assinado pela AC para GW de voz](#)

[2. Gerar um certificado IPsec assinado por CA do CUCM](#)

[3. Importar certificados CA, CUCM e CA GW de voz no CUCM](#)

[4. Configurar as configurações de túnel IPsec no CUCM](#)

[5. Configurar a configuração do túnel IPsec no GW de voz](#)

[Verificar](#)

[Verifique o status do túnel IPsec na extremidade do CUCM](#)

[Verifique o status do túnel IPsec na extremidade do gateway de voz](#)

[Troubleshoot](#)

[Solucionar problemas do túnel IPsec na extremidade do CUCM](#)

[Solucionar problemas do túnel IPsec na extremidade do gateway de voz](#)

Introduction

Este documento descreve como proteger com êxito a sinalização do Media Gateway Control Protocol (MGCP) entre um gateway de voz (GW) e o CUCM (Cisco Unified Communications Manager) via Internet Protocol Security (IPsec), com base em certificados assinados pela Autoridade de Certificação (CA). Para configurar uma chamada segura via MGCP, a sinalização e os fluxos do protocolo de transporte em tempo real (RTP) precisam ser protegidos separadamente. Parece bem documentado e bastante simples configurar fluxos RTP criptografados, mas um fluxo RTP seguro não inclui sinalização MGCP segura. Se a sinalização MGCP não estiver segura, as chaves de criptografia para o fluxo RTP serão enviadas em branco.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Gateway de voz MGCP registrado no CUCM para enviar e receber chamadas
- Serviço de função de proxy da autoridade de certificação (CAPF) iniciado, cluster definido para modo misto
- A imagem do Cisco IOS® no GW suporta recurso de segurança de criptografia
- Telefones e MGCP GW configurados para Secure Real-Time Transport Protocol (SRTP)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

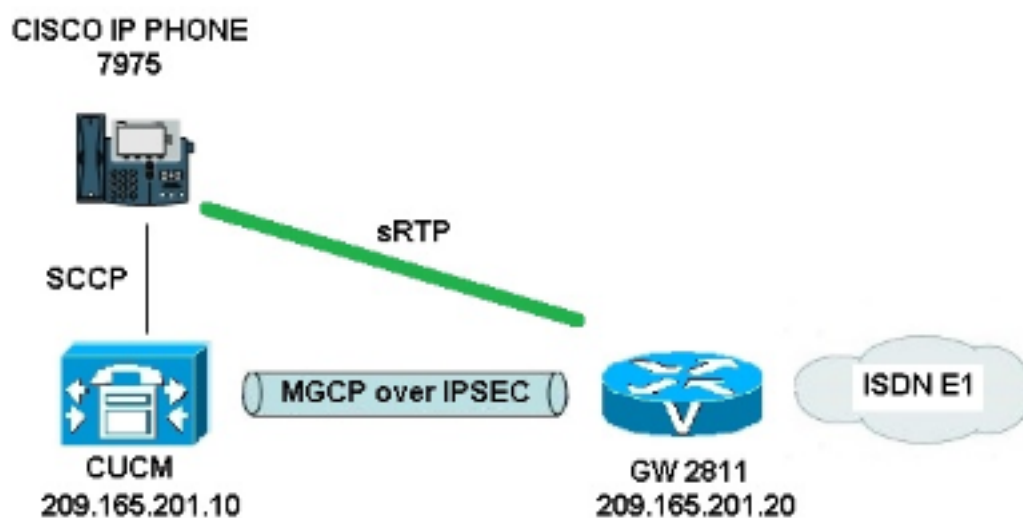
- CUCM - nó único - executa o GGSG (Global Government Solutions Group) versão 8.6.1.2012-14 no modo FIPS (Federal Information Processing Standard)
- Telefones 7975 que executam SCCP75-9-3-1SR2-1S
- GW - Cisco 2811 - C2800NM-ADVENTERPRISEK9-M, Versão 15.1(4)M8
- Placa de voz E1 ISDN - VWIC2-2MFT-T1/E1 - Tronco Multiflex RJ-48 de 2 portas

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.

Configurar

Note: Use a [Command Lookup Tool \(somente clientes registrados\)](#) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede



Para configurar com êxito o IPsec entre o CUCM e o GW de voz, faça o seguinte:

1. Configurar a CA no GW de voz e gerar um certificado assinado por CA para GW de voz
2. Gerar um certificado IPsec assinado por CA do CUCM

3. Importar certificados CA, CUCM e CA GW de voz no CUCM
4. Definir configurações de túnel IPsec no CUCM
5. Configurar a configuração do túnel IPsec no GW de voz

1. Configurar a CA no GW de voz e gerar um certificado assinado pela AC para GW de voz

Como primeiro passo, o par de chaves Rivest-Shamir-Addleman (RSA) precisa ser gerado no GW de voz (servidor de CA do Cisco IOS):

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

As inscrições concluídas via Simple Certificate Enrollment Protocol (SCEP) serão usadas, portanto, ative o servidor HTTP:

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

Para configurar o Servidor CA em um gateway, estas etapas precisam ser concluídas:

1. Defina o nome do servidor PKI. Ele precisa ter o mesmo nome do par de chaves gerado anteriormente.

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

2. Especifique o local onde todas as entradas do banco de dados serão armazenadas para o servidor CA.

```
KRK-UC-2x2811-2(cs-server)#crypto pki server IOS_CA
```

3. Configure o nome do emissor da CA.

```
KRK-UC-2x2811-2(cs-server)#issuer-name cn=IOS
```

4. Especifique um ponto de distribuição (CDP) da lista de revogação de certificados (CRL) a ser usado em certificados emitidos pelo servidor de certificados e habilite a concessão automática de solicitações de registro de certificado para um servidor de CA subordinado do Cisco IOS.

```
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. Ative o servidor CA.

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

A próxima etapa é criar um ponto de confiança para o certificado CA e um ponto de confiança local para o certificado do roteador com uma inscrição de URL que aponte para um servidor 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
```

Para gerar o certificado do roteador assinado pela CA local, o ponto de confiança precisa ser autenticado e inscrito:

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

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

Depois disso, o certificado do roteador é gerado e assinado pela CA local. Liste o certificado no roteador para verificação.

```
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

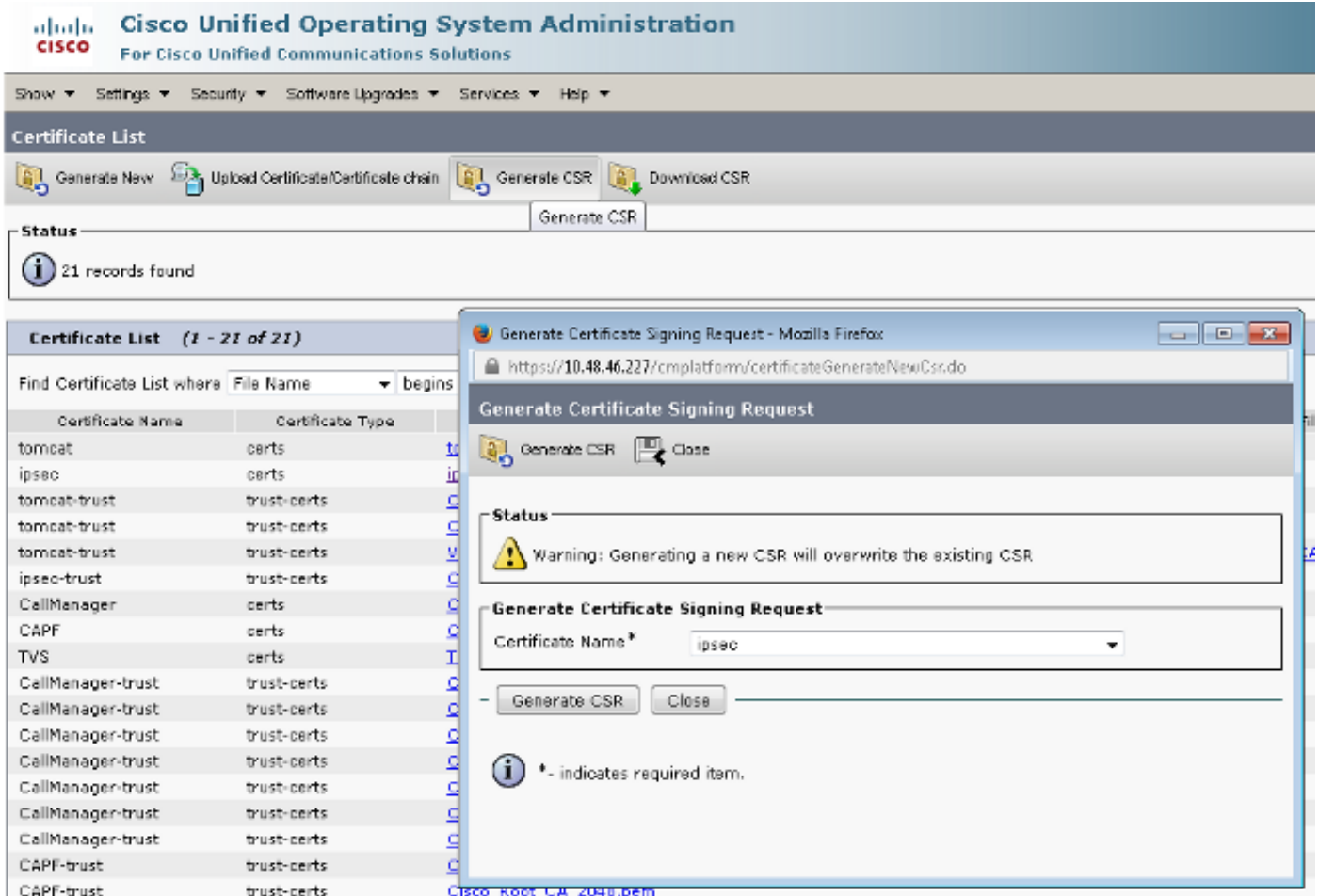
Associated Trustpoints: local1 IOS_CA

Storage: nvram:IOS#1CA.cer

Dois certificados devem ser listados. O primeiro é um certificado de roteador (KRK-UC-2x2811-2) assinado pela CA local e o segundo é um certificado CA.

2. Gerar um certificado IPsec assinado por CA do CUCM

A configuração do túnel CUCM para IPsec usa um certificado ipsec.pem. Por padrão, esse certificado é autoassinado e gerado quando o sistema é instalado. Para substituí-lo por um certificado assinado por CA, primeiro é necessário gerar um CSR (Certificate Sign Request) para IPsec da página de administração do SO CUCM. Escolha **Cisco Unified OS Administration > Security > Certificate Management > Generate CSR**.



Depois que o CSR é gerado, ele precisa ser baixado do CUCM e inscrito no CA no GW. Para fazer isso, insira o comando `crypto pki server IOS_CA request pkcs10 terminal base64` e o hash de requisição de sinal precisa ser colado via terminal. O certificado concedido é exibido e precisa ser copiado e salvo como o arquivo `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-----
MIIDNjCCAh4CAQAwgaxkCzAJBgNVBAYTAlBMMQ4wDAYDVQQIEwVjaXNjbzEOMAwG
A1UEBxMFY21zY28xDjAMBgNVBAoTBWNPc2NvMQ4wDAYDVQQLEwVjaXNjbzEPMA0G
A1UEAxMQQ1VDTUIxMUMkRwYDVQQFE0A1NjY2OWY5MjgzNWZmZWQ1MDg0YjI5MTU4
NjcwMDBmMGI2NjliYjYkYjYwZmZmNDNmM2QzOWFhNGQxMzZmMjZlMjZlMjZlMjZl
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAKfHxvcov4vFmK+3+dQShW3s3SszAYBQ19
0JDBiC4eDRmrdq0V2dkn9UpLUX9OH7V0Oe/8wmHqYwoxFZ5a6B5qRRkc010/ub2
u1l1QCw+nQ6QizGdNhdne0NYY4r3odF4CkrtYAJA4PUSce1tWxfiJY5dw/Xhv8cVg
gVyxctESemfMhUfvEM203NU9nod7YTEzQzuAadjNcyc4blu91vQm5OVUNXxODov
e7/0lQNUWU3LSEr0aI9lC75x3qdRGBe8Pwnk/gWbT5B7pwuMXTU8+UFj6+lvrQM
Rb47dw22yFmSMObvez18IVExAyFs50j9Aj/rNFIdUQIt+Nt+Q+f38wIDAQABOEcw
RQYJKoZIhvcNAQkOMTgwNjAnBgNVHUSIEIDAeBggrBgEFBQcDAQYIKwYBBQUHAWIG
CCsGAQUFBwMFMAsgA1UdDwQEAwIDuANBgkqhkiG9w0BAQUFAAOCAQEADgAR40l
oQ4z2yqgSsICAZ2hQA3Vztp6aOI+0PSyMfihGS//3V3tALEZL2+t0Y5elKsBea72
sieKjpSikXjNaj+SiYlaYy4siVw5EKQD3Ii4Qv115BvuniZXvBiBQUw+SpBLbeNi
xwIgrYELrFywQZBeZodFqnSKN9X1isXe6oU9GXux7uwgXwCXMF/azutbio14Fgf
qUF00GzkhtEapJA6c5RzaxG/0uDukY+4z1eSSsXzFhBTifk3RfJA+I7Na1zQBIEJ
2IOJdiZnn0HWVr5C5eZ7VnQuNdiC/qn3uUfvNVRZo8iCDq3tRv7dr/n64jdKsHEM
lk6P8gp9993cJw==
quit
% Granted certificate:
```

```
MIIDXTCCAsagAwIBAgIBBTANBgkqhkiG9w0BAQQFADAOMQwwCgYDVQQDEwNJT1Mw
HhcNMtUwMTA4MTIwMTAwWhcNMtYwMTA4MTIwMTAwWjCBqTELMakGAlUEBhMCUEwx
DjAMBgNVBAgTBWNpc2NvMQ4wDAYDVQQHEwVjaXNjbzEOMAwGA1UEChMFY21zY28x
DjAMBgNVBAStBWNpc2NvMQ8wDQYDVQQDEwZDVUNNQjExSTBHBgNVBAUTQDU2NjY5
ZjkyODMlZmZlZDUwODRlMjkxNTg2NzAwMGYwYjY2OWJiN2RhZmE0M2YzZDM5YWE0
ZDEzMzVlOWUyNTMwgwEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC8fG9
yi/i8WYr7f51BKFBbezdlMBgFDX3QkMGihzh4NGZ2urRXZ2Sf1SktTH04ftXQ57/z
CYepjCjEVnlroHmpFGRw7XT+5va6XVALD6dDpCJkZ02F2d7Q1hjiveh0XgKSulgA
kDg9Rjx7W1bF+Iljl3D9eG/xxWCBXK7Fy0RJ6Z8yFR+8QzbTc1T2eh3thMTND04B
p2M1zJzhvW73W9CbK5VQ1fE40i97v86VA1RZTctISvRoj2ULvnHep1EYF7w/CeT+
BZtPkHunC7AxdNTz5QWPr6W+tAxFvjt3DbbIWZlw5u97PXwhUTEDIWzk6P0CP+s0
Uh1RAi34235D5/fzAgMBAAGjgaowgacwLwYDVR0fBCgwJjAkoCKgIIYeaHR0cDov
LzEwLjQ4LjQ2LjI1MS9JT1NfQ0EuY3JsMAsGAlUdDwQEAwIDuDanBgNVHSUEIDAe
BggrBgEFBQcDAQYIKwYBBQUHAWIGCCsGAQUFBwMFMB8GAlUdIwQYMBaAFJSLP5cn
PL8bIP7VSKLtB6Z1socOMB0GAlUdDgQWBBR4m2eTSyELsdRBW4MRmbNdT2qppTAN
BgkqhkiG9w0BAQQFAAOBggQBuVJ+tVS0JqP4z9TgEeuMbVwn00CTKXz/fCuh6R/50
qq8JhERJGiR/ZHvHRLf+XawhnoE6daPAmE+WkIPtHIhbMHCbbxG9ffdyaiNXRWy
5sI5XycF1FgYGpTFBYD9M0Lqsw+FIYaT2ZrbOGsx8h6pZoesKqm85RByIUjX4nJK
lg==
```

Note: Para decodificar e verificar o conteúdo do certificado codificado Base64, insira o comando **openssl x509 -in certificate.crt -text -noout**.

O certificado CUCM concedido decodifica para:

```
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. Importar certificados CA, CUCM e CA GW de voz no CUCM

O certificado CUCM IPsec já foi exportado para um arquivo .pem. Como próxima etapa, o mesmo processo precisa ser concluído com o certificado GW de voz e o certificado CA. Para fazer isso, eles precisam ser exibidos primeiro em um terminal com o comando **crypto pki export local1 pem terminal** e copiados para arquivos .pem separados.

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

```
% CA certificate:
```

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

```
MIIB9TCCA6AwIBAgIBATANBgkqhkiG9w0BAQQFADAOMQwwCgYDVQQDEwNJT1Mw
HhcNMTQxMTIwMTE1MTEyWWhcNMTcxMTIwMTE1MTEyWjAOMQwwCgYDVQQDEwNJT1Mw
gZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAK6Cd2yxUywtbgBE1kZUsP6eaZVv
6YfpEbFptyt6ptRdpxgJOYI3InEP3wewtmEPNeTJL8+a/W7MDUemm3t/NlWBO6T2
m9Bp6k0FNOBXMKeDfTSqOKey7WfLASE/Pbq8M+JMpeMWz8xnMboYOb66rY8igZFz
k1tRPlIMsf5r01tnAgMBAAGjYzBhMA8GA1UdEwEB/wQFMAMBAf8wDgYDVR0PAQH/
BAQDAgGGMB8GA1UdIwQYMBAAwFJSLP5cnPL8bIP7VSKLtB6Z1socOMB0GA1UdDgQW
BBSUiz+XJzy/GyD+1Uii7QemdbKHDjANBgkqhkiG9w0BAQQFAA0BgQCUMC1SFV1S
TSS1Exbm9i2D4HOWYhCurhifqTWLxMMXj0jym24DoqZ91aDNGlVwiJ/Yv4i40t90
y65WzbpZL1S65q+d7BCLQypdrwcKkdS0dfTdKfXESyWLhecRa8mnZckpgKBk8Ir
Bfm9K+caXkfhPEPa644UzV9++OKMKhtDuQ==
```

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

```
% General Purpose Certificate:
```

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

```
MIIB2zCCAUSgAwIBAgIBAJANBgkqhkiG9w0BAQUFADAOMQwwCgYDVQQDEwNJT1Mw
HhcNMTQxMTIwMTE1MTEyWWhcNMTUxMTIwMTE1MTEyWjAAMRgwFgYDVQQDEw9LUkst
VUMtMngyODExLTlWXdANBgkqhkiG9w0BAQEFAANLADBIAGApGWIN1nAAAtKLVMoj
mZVkQFgI8LrHD6zSrlaKgAJh1u+H/mnRQq5rqtIpekDdPoowST9Rxc5CJmB4spT
VWkYkwIDAQABo4GAMH4wLwYDVR0fBCgwJjAkoCKgIIYeHR0cDovLzEwLjQ4LjQ2
LjI1MS9JT1NfQ0EuY3JSMASGA1UdDwQEAwIFoDafBgNVHSMEGDAWgBSUiz+XJzy/
GyD+1Uii7QemdbKHDjAdBgNVHQ4EFgQUtAWc61K5nYGgWqKAI IOLMlphfqIwDQYJ
KoZIhvcNAQEFBQADgYEAjdfLh+N3yc3RykCig9B0aAIXWZPmaqLF9v9R75zc+f8x
zbSIzovBhnU0eu0j1hnIghyymjeELjTEh6uQrWUN2ElW1yphmxk1jN5q0t+vfdr
+yepS04pFor9R0d7IWg6e/1hFDEep9hbvzrVwQHCjzeY0rVrPcLl126k5oauMwTs=
```

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

O certificado % CA decodifica para:

Certificate:

Data:

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

O % certificado de finalidade geral decodifica para:

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
```

Depois que são salvos como arquivos .pem, eles precisam ser importados para o CUCM. Escolha **Cisco Unified OS Administration > Security > Certificate management > Upload Certificate/Certificate**.

- Certificado CUCM como IPsec
- Certificado GW de voz como IPsec-trust
- Certificado CA como confiável de IPsec:

The screenshot shows the Cisco Unified OS Administration web interface. The main page is titled 'Certificate List' and includes a search bar and several action 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, displaying the following information:

- Status:** Ready
- Upload Certificate/Certificate chain:**
 - Certificate Name*: ipsec-trust
 - Description: (empty text box)
 - Upload File: (Browse... button) KRK-UC-2x2811-2.cisco.com.pem


At the bottom of the dialog, there are 'Upload File' and 'Close' buttons, and a note: 'i* indicates required item.'

4. Configurar as configurações de túnel IPsec no CUCM

A próxima etapa é a configuração do túnel IPsec entre o CUCM e o GW de voz. A configuração do túnel IPsec no CUCM é executada através da página da Web do Cisco Unified OS Administration (https://<cucm_ip_address>/cmplatform). Escolha **Segurança > Configuração IPSEC > Adicionar nova política IPsec**.

Neste exemplo, uma política chamada "vgipsecpolicy" foi criada, com autenticação baseada em certificados. Todas as informações apropriadas precisam ser preenchidas e correspondem à configuração no GW de voz.

- 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: O nome do certificado do gateway de voz precisa ser especificado no campo Nome do certificado.

5. Configurar a configuração do túnel IPsec no GW de voz

Este exemplo, com comentários em linha, apresenta a configuração correspondente em um GW de voz.

```

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

```

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Verifique o status do túnel IPsec na extremidade do CUCM

A maneira mais rápida de verificar o status do túnel IPsec no CUCM é ir até a página Administração do SO e usar a opção **ping** em Serviços > Ping. Verifique se a caixa de seleção **Validar IPSec** está marcada. Obviamente, o endereço IP especificado aqui é o endereço IP do 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

Note: Consulte estes IDs de bug da Cisco para obter informações sobre a validação do túnel IPsec através do recurso de ping no CUCM:

- ID de bug da Cisco [CSCuo53813](#) - Validar resultados de Ping de IPsec em branco quando pacotes ESP (Encapsulating Security Payload) são enviados
- O bug da Cisco ID [CSCud20328](#) - Validate IPsec Policy mostra uma mensagem de erro incorreta no modo FIPS

Verifique o status do túnel IPsec na extremidade do gateway de voz

Para verificar se a configuração é executada corretamente ou não, é necessário confirmar que as Associações de Segurança (SAs) para ambas as camadas (ISAKMP) e IPsec foram criadas corretamente.

Para verificar se o SA de ISAKMP foi criado e funciona corretamente, insira o comando **show crypto isakmp sa** no 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: O status correto do SA deve ser ACTIVE e QM_IDLE.

A segunda camada é SAs para IPsec. Seu status pode ser verificado com o comando **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: Os Índices de Política de Segurança (SPIs) de entrada e saída devem ser criados no status ATIVO e os contadores para o número de pacotes encapsulados/desencapsulados e criptografados/descriptografados devem crescer toda vez que qualquer tráfego através de um túnel é gerado.

A última etapa é confirmar se o GW MGCP está no estado registrado e se a configuração TFTP foi baixada corretamente do CUCM sem falhas. Isso pode ser confirmado a partir da saída destes comandos:

```
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#
```

Troubleshoot

Esta seção disponibiliza informações para a solução de problemas de configuração.

Solucionar problemas do túnel IPsec na extremidade do CUCM

No CUCM, não há serviço de manutenção responsável pela terminação e gerenciamento de IPsec. O CUCM usa um pacote de ferramentas Red Hat IPsec incorporado ao sistema operacional. O daemon executado no Red Hat Linux e que termina a conexão IPsec é o OpenSwan.

Toda vez que a política de IPsec é ativada ou desativada no CUCM (OS Administration > Security > IPSEC Configuration), o daemon Openswan é reiniciado. Isso pode ser observado no registro de mensagens do Linux. Uma reinicialização é indicada pelas seguintes linhas:

```
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
```

Sempre que houver um problema com a conexão IPsec no CUCM, as últimas entradas no registro de mensagens devem ser verificadas (insira o comando **file list ativelog syslog/messages***) para confirmar se o Openswan está ativo e em execução. Se o Openswan for executado e iniciado sem erros, você poderá solucionar problemas de configuração do IPsec. O daemon responsável pela configuração de túneis IPsec em Openswan é Plutão. Os registros de plug-ins são escritos para proteger os registros no Red Hat e podem ser obtidos através do comando **get ativelog syslog/secure.*** ou através da **RTMT: Registros de segurança**.

Note: Mais informações sobre como coletar registros via RTMT podem ser encontradas na [documentação da RTMT](#).

Se for difícil determinar a origem do problema com base nesses registros, o IPsec pode ser verificado ainda mais pelo Technical Assistance Center (TAC) através da raiz no CUCM. Depois de acessar o CUCM pela raiz, as informações e os registros sobre o status do IPsec podem ser verificados com estes comandos:

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

Também há uma opção para gerar um relatório de sosde Red Hat pela raiz. Este relatório contém todas as informações exigidas pelo suporte da Red Hat para solucionar problemas adicionais no nível do sistema operacional:

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

Solucionar problemas do túnel IPsec na extremidade do gateway de voz

Neste site, você pode solucionar problemas de todas as fases da configuração do túnel IPsec depois de habilitar estes comandos de depuração:

```
debug crypto ipsec
```



```
debug crypto isakmp
```

Note: As etapas detalhadas para solucionar problemas de IPsec são encontradas em [Troubleshooting de IPsec: Entendendo e usando comandos debug](#).

Você pode solucionar problemas do MGCP GW com estes comandos debug:

```
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
```