Comunicación MGCP asegurada entre la Voz GW y CUCM vía el IPSec basado en el ejemplo de configuración de los certificados firmados de CA

Contenido

Introducción
prerrequisitos
Requisitos
Componentes Utilizados
Configurar
Diagrama de la red
1. Configure CA en la Voz GW y genere a certificado firmado por CA para la Voz GW
2. Genere un certificado CA-firmado CUCM del IPSec
3. Importe CA, CUCM, y los Certificados de la Voz GW CA en CUCM
4. Configure las configuraciones del túnel IPsec en CUCM
5. Configure la configuración del túnel IPsec en la Voz GW
Verificación
Verifique el estatus del túnel IPsec en el extremo CUCM
Verifique el estatus del túnel IPsec en el extremo del gateway de voz
Troubleshooting
Resuelva problemas el túnel IPsec en el extremo CUCM
Resuelva problemas el túnel IPsec en el extremo del gateway de voz

Introducción

Este documento describe cómo asegurar con éxito el Media Gateway Control Protocol (MGCP) que señala entre un gateway de voz (GW) y CUCM (administrador de las Comunicaciones unificadas de Cisco) vía la seguridad de protocolos en Internet (IPSec), sobre la base de los certificados firmados del Certificate Authority (CA). Para configurar una llamada asegurada vía el MGCP, la señalización y las secuencias del Real-Time Transport Protocol (RTP) necesitan ser aseguradas por separado. Parece ser bien documentado y muy simple configurar las secuencias cifradas RTP, pero una secuencia segura RTP no incluye la señalización segura MGCP. Si la señalización MGCP no se asegura, las claves de encripción para la secuencia RTP se envían en el claro.

Prerequisites

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Gateway de voz MGCP registrado a CUCM para enviar y recibir las llamadas
- El servicio de la función de proxy del Certificate Authority (CAPF) comenzó, cluster fijado al mezclado-MODE
- La imagen del ® del Cisco IOS en el GW soporta la función de seguridad crypto
- Teléfonos y MGCP GW configurados para el protocolo Real-Time Transport seguro (SRTP)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

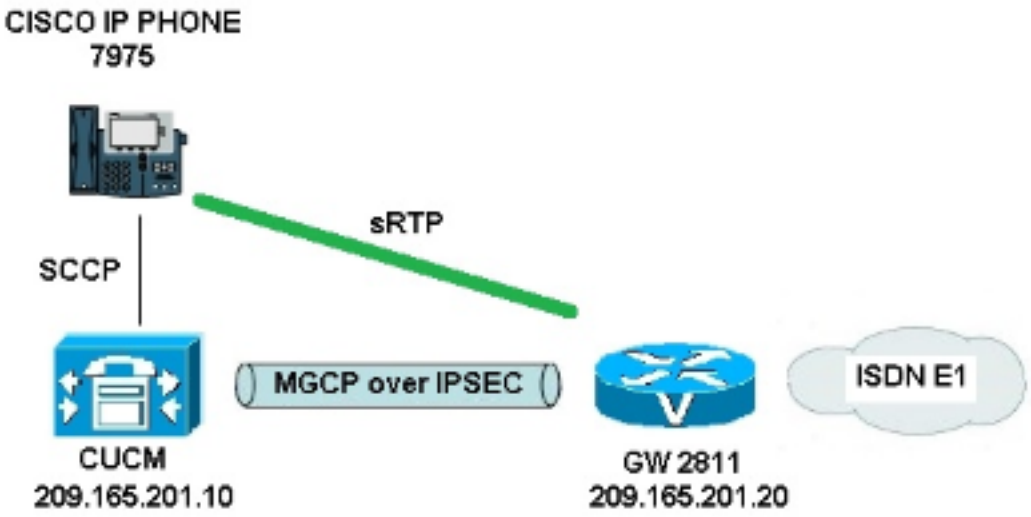
- CUCM - nodo único - versión 8.6.1.20012-14 de los funcionamientos GGSG (grupo global de las soluciones del gobierno de Cisco) en el modo del Estándar de procesamiento de la información federal (FIP)
- 7975 teléfonos que ejecutan SCCP75-9-3-1SR2-1S
- GW - Cisco 2811 - C2800NM-ADVENTERPRISEK9-M, versión 15.1(4)M8
- Placa de voz del e1 ISDN - VWIC2-2MFT-T1/E1 - troncal de multiflex RJ-48 2 puerto

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Configurar

> **Note**: Use la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.

Diagrama de la red



Para configurar con éxito el IPSec entre CUCM y expresar el GW, complete estos pasos:

1. Configure CA en la Voz GW y genere a certificado firmado por CA para la Voz GW
2. Genere un certificado CA-firmado CUCM del IPSec
3. Importe CA, CUCM, y los Certificados de la Voz GW CA en CUCM
4. Configure las configuraciones del túnel IPsec en CUCM
5. Configure la configuración del túnel IPsec en la Voz GW

1. Configure CA en la Voz GW y genere a certificado firmado por CA para la Voz GW

En primer lugar, el par clave del Rivest-Shamir-Addleman (RSA) necesita ser generado en la Voz GW (servidor de CA del Cisco IOS):

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

Las inscripciones completadas vía el protocolo simple certificate enrollment (SCEP) serán utilizadas, así que habilitan al servidor HTTP:

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

Para configurar el servidor de CA en un gateway, estos pasos necesitan ser completados:

1. Fije el nombre de servidor pki. Necesita ser el mismo nombre que el par clave generó previamente.
   ```
   KRK-UC-2x2811-2(config)#crypto pki server IOS_CA
   ```
2. Especifique la ubicación en donde todas las entradas de la base de datos serán salvadas para el servidor de CA.
   ```
   KRK-UC-2x2811-2(cs-server)#crypto pki server IOS_CA
   ```
3. Configure el nombre del emisor de CA.
   ```
   KRK-UC-2x2811-2(cs-server)#issuer-name cn=IOS
   ```
4. Especifique un punto de distribución del Listas de revocación de certificados (CRL) (CDP) que se utilizará en los Certificados que son publicados por el servidor de certificados y concesión automática del permiso del reenrollment del certificado pide para un servidor subordinado de CA del 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. Habilite el servidor de CA.

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

El siguiente paso es crear un trustpoint para el certificado de CA y un trustpoint local para el certificado del router con una inscripción URL esas puntas a un 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 generar el certificado del router firmado por CA local, el trustpoint necesita ser autenticado y ser alistado:

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

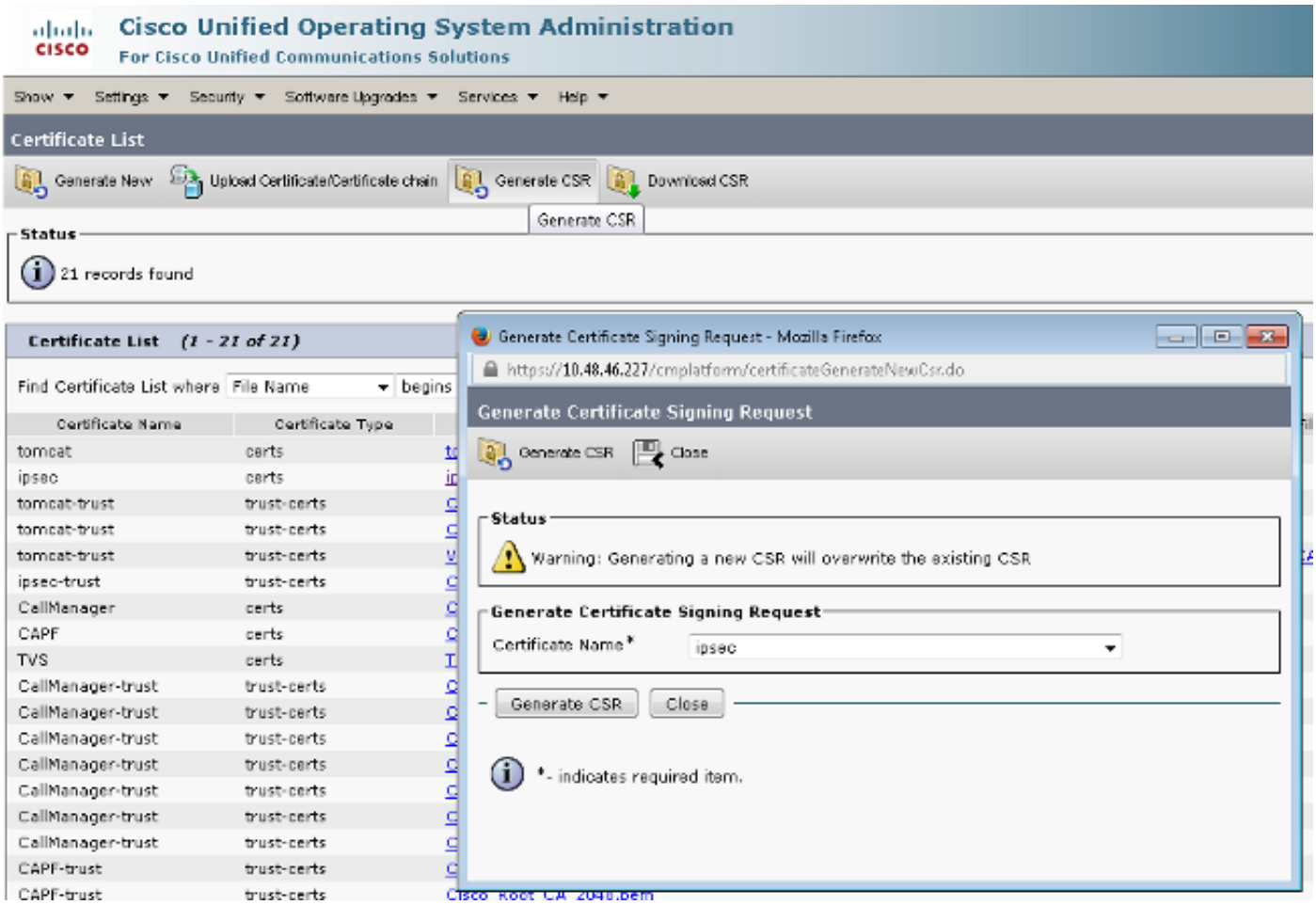
Después de ese, el certificado del router es generado y firmado por la lista local CA el certificado en el router para la verificación.

```
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
```

Dos Certificados deben ser mencionados. Primer es el certificado de un router (KRK-UC-2x2811-2) firmado por CA local y segundo es certificado de CA.

2. Genere un certificado CA-firmado CUCM del IPSec

El CUCM para la configuración del túnel IPsec utiliza un certificado ipsec.pem. Por abandono, uno mismo-se firma y se genera este certificado cuando el sistema está instalado. Para substituirlo por certificado firmado por CA, primero un CSR (petición de la muestra del certificado) para el IPSec de la página de administración CUCM OS necesita ser generado. Elija el **Certificate Management (Administración de certificados) del > Security (Seguridad) de la administración de** CiscoUnified **OS > generan el CSR.**



Después de que se genere el CSR, necesita ser descargado de CUCM y ser alistado contra CA en el GW. Para hacer eso, ingrese el comando **terminal crypto del base64 de la petición pkcs10 del servidor pki IOS_CA** y el hash de la petición de la muestra necesita ser pegado vía la terminal. El certificado concedido se visualiza y necesita ser copiado y ser guardado como el archivo 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-----
MIIDNjCCAh4CAQAwgakxCzAJBgNVBAYTAlBMMQ4wDAYDVQQIEwVjaXNjbzEOMAwG
A1UEBxMFY2lzY28xDjAMBgNVBAoTBWNpc2NvMQ4wDAYDVQQLEwVjaXNjbzEPMA0G
A1UEAxMGQ1VDTUIxMUkwRwYDVQQFE0A1NjY2OWY5MjgzNWZmZWQ1MDg0YjI5MTU4
NjcwMDBmMGI2NjliYjdkYWZhNDNmM2QzOWFhNGQxMzM1ZTllMjUzMIIBIjANBgkq
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAkfHxvcov4vFmK+3+dQShW3s3SzAYBQ19
0JDBiIc4eDRmdrq0V2dkn9UpLUx9OH7V0Oe/8wmHqYwoxFZ5a6B5qRRkcO10/ub2
```

```
ul1QCw+nQ6QiZGdNhdne0NYY4r3odF4CkrtYAJA4PUSce1tWxfiJY5dw/Xhv8cVg
gVyuxctESemfMhUfvEM203NU9nod7YTEzQzuAadjNcyc4b1u91vQm5OVUNXxODov
e7/OlQNUWU3LSEr0aI9lC75x3qdRGBe8Pwnk/gWbT5B7pwuwMXTU8+UFj6+lvrQM
Rb47dw22yFmSMObvez18IVExAyFs5Oj9Aj/rNFIdUQIt+Nt+Q+f38wIDAQABoEcw
RQYJKoZIhvcNAQkOMTgwNjAnBgNVHSUEIDAeBggrBgEFBQcDAQYIKwYBBQUHAwIG
CCsGAQUFBwMFMAsGA1UdDwQEAwIDuDANBgkqhkiG9w0BAQUFAAOCAQEAQDgAR4Ol
oQ4z2yqgSsICAZ2hQA3Vztp6aOI+0PSyMfihGS//3V3tALEZL2+t0Y5elKsBea72
sieKjpSikXjNaj+SiY1aYy4siVw5EKQD3Ii4Qvl15BvuniZXvBiBQuW+SpBLbeNi
xwIgrYELrFywQZBeZOdFqnSKN9XlisXe6oU9GXux7uwgXwkCXMF/azutbiol4Fgf
qUF00GzkhtEapJA6c5RzaxG/0uDuKY+4z1eSSsXzFhBTifk3RfJA+I7Na1zQBIEJ
2IOJdiZnn0HWVr5C5eZ7VnQuNdiC/qn3uUfvNVRZo8iCDq3tRv7dr/n64jdKsHEM
lk6P8gp9993cJw==
quit
% Granted certificate:
MIIDXTCCAsagAwIBAgIBBTANBgkqhkiG9w0BAQQFADAOMQwwCgYDVQQDEwNJT1Mw
HhcNMTUwMTA4MTIwMTAwWhcNMTYwMTA4MTIwMTAwWjCBqTELMAkGA1UEBhMCUEwx
DjAMBgNVBAgTBWNpc2NvMQ4wDAYDVQQHEwVjaXNjbzEOMAwGA1UEChMFY2lzY28x
DjAMBgNVBAsTBWNpc2NvMQ8wDQYDVQQDEwZDVUNNQjExSTBHBgNVBAUTQDU2NjY5
ZjkyODM1ZmZlZDUwODRiMjkxNTg2NzAwMGYwYjY2OWJiN2RhZmE0M2YzZDM5YWE0
ZDEzMzVlOWUyNTMwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCR8fG9
yi/i8WYr7f51BKFbezdLMBgFDX3QkMGIhzh4NGZ2urRXZ2Sf1SktTH04ftXQ57/z
CYepjCjEVnlroHmpFGRw7XT+5va6XVALD6dDpCJkZ02F2d7Q1hjiveh0XgKSu1gA
kDg9RJx7W1bF+Iljl3D9eG/xxWCBXK7Fy0RJ6Z8yFR+8QzbTc1T2eh3thMTNDO4B
p2M1zJzhvW73W9Cbk5VQ1fE4Oi97v86VA1RZTctISvRoj2ULvnHep1EYF7w/CeT+
BZtPkHunC7AxdNTz5QWPr6W+tAxFvjt3DbbIWZIw5u97PXwhUTEDIWzk6P0CP+s0
Uh1RAi34235D5/fzAgMBAAGjgaowgacwLwYDVR0fBCgwJjAkoCKgIIYeaHR0cDov
LzEwLjQ4LjQ2LjI1MS9JT1NfQ0EuY3JsMAsGA1UdDwQEAwIDuDAnBgNVHSUEIDAe
BggrBgEFBQcDAQYIKwYBBQUHAwIGCCsGAQUFBwMFMB8GA1UdIwQYMBaAFJSLP5cn
PL8bIP7VSKLtB6Z1socOMB0GA1UdDgQWBBR4m2eTSyELsdRBW4MRmbNdT2qppTAN
BgkqhkiG9w0BAQQFAAOBgQBuVJ+tVS0JqP4z9TgEeuMbVwn00CTKXz/fCuh6R/50
qq8JhERJGiR/ZHvHRLf+XawhnoE6daPAmE+WkIPtHIIhbMHCbbxG9ffdyaiNXRWy
5sI5XycF1FgYGpTFBYD9M0Lqsw+FIYaT2ZrbOGsx8h6pZoesKqm85RByIUjX4nJK
1g==
```

Note: Para decodificar y marcar el contenido del base64 codificaron el certificado, ingrese el **openssl x509 - en certificate.crt - texto - el noout ordena**.

El certificado concedido CUCM decodifica a:

```
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-----
MIIDNjCCAh4CAQAwgakxCzAJBgNVBAYTAlBMMQ4wDAYDVQQIEwVjaXNjbzEOMAwG
A1UEBxMFY2lzY28xDjAMBgNVBAoTBWNpc2NvMQ4wDAYDVQQLEwVjaXNjbzEPMA0G
A1UEAxMGQ1VDTUIxMUkwRwYDVQQFE0A1NjY2OWY5MjgzNWZmZWQ1MDg0YjI5MTU4
NjcwMDBmMGI2NjliYjdkYWZhNDNmM2QzOWFhNGQxMzM1ZTllMjUzMIIBIjANBgkq
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAkfHxvcov4vFmK+3+dQShW3s3SzAYBQ19
0JDBiIc4eDRmdrq0V2dkn9UpLUx9OH7V0Oe/8wmHqYwoxFZ5a6B5qRRkcO10/ub2
ul1QCw+nQ6QiZGdNhdne0NYY4r3odF4CkrtYAJA4PUSce1tWxfiJY5dw/Xhv8cVg
gVyuxctESemfMhUfvEM203NU9nod7YTEzQzuAadjNcyc4b1u91vQm5OVUNXxODov
e7/OlQNUWU3LSEr0aI9lC75x3qdRGBe8Pwnk/gWbT5B7pwuwMXTU8+UFj6+lvrQM
Rb47dw22yFmSMObvez18IVExAyFs5Oj9Aj/rNFIdUQIt+Nt+Q+f38wIDAQABoEcw
RQYJKoZIhvcNAQkOMTgwNjAnBgNVHSUEIDAeBggrBgEFBQcDAQYIKwYBBQUHAwIG
CCsGAQUFBwMFMAsGA1UdDwQEAwIDuDANBgkqhkiG9w0BAQUFAAOCAQEAQDgAR4Ol
oQ4z2yqgSsICAZ2hQA3Vztp6aOI+0PSyMfihGS//3V3tALEZL2+t0Y5elKsBea72
sieKjpSikXjNaj+SiY1aYy4siVw5EKQD3Ii4Qvl15BvuniZXvBiBQuW+SpBLbeNi
xwIgrYELrFywQZBeZOdFqnSKN9XlisXe6oU9GXux7uwgXwkCXMF/azutbiol4Fgf
qUF00GzkhtEapJA6c5RzaxG/0uDuKY+4z1eSSsXzFhBTifk3RfJA+I7Na1zQBIEJ
```

```
2IOJdiZnn0HWVr5C5eZ7VnQuNdiC/qn3uUfvNVRZo8iCDq3tRv7dr/n64jdKsHEM
lk6P8gp9993cJw==
quit
% Granted certificate:
MIIDXTCCAsagAwIBAgIBBTANBgkqhkiG9w0BAQQFADAOMQwwCgYDVQQDEwNJT1Mw
HhcNMTUwMTA4MTIwMTAwWhcNMTYwMTA4MTIwMTAwWjCBqTELMAkGA1UEBhMCUEwx
DjAMBgNVBAgTBWNpc2NvMQ4wDAYDVQQHEwVjaXNjbzEOMAwGA1UEChMFY2lzY28x
DjAMBgNVBAsTBWNpc2NvMQ8wDQYDVQQDEwZDVUNNQjExSTBHBgNVBAUTQDU2NjY5
ZjkyODM1ZmZlZDUwODRiMjkxNTg2NzAwMGYwYjY2OWJiN2RhZmE0M2YzZDM5YWE0
ZDEzMzVlOWUyNTMwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCR8fG9
yi/i8WYr7f51BKFbezdLMBgFDX3QkMGIhzh4NGZ2urRXZ2Sf1SktTH04ftXQ57/z
CYepjCjEVnlroHmpFGRw7XT+5va6XVALD6dDpCJkZ02F2d7Q1hjiveh0XgKSu1gA
kDg9RJx7W1bF+Iljl3D9eG/xxWCBXK7Fy0RJ6Z8yFR+8QzbTc1T2eh3thMTNDO4B
p2M1zJzhvW73W9Cbk5VQ1fE4Oi97v86VA1RZTctISvRoj2ULvnHep1EYF7w/CeT+
BZtPkHunC7AxdNTz5QWPr6W+tAxFvjt3DbbIWZIw5u97PXwhUTEDIWzk6P0CP+s0
Uh1RAi34235D5/fzAgMBAAGjgaowgacwLwYDVR0fBCgwJjAkoCKgIIYeaHR0cDov
LzEwLjQ4LjQ2LjI1MS9JT1NfQ0EuY3JsMAsGA1UdDwQEAwIDuDAnBgNVHSUEIDAe
BggrBgEFBQcDAQYIKwYBBQUHAwIGCCsGAQUFBwMFMB8GA1UdIwQYMBaAFJSLP5cn
PL8bIP7VSKLtB6Z1socOMB0GA1UdDgQWBBR4m2eTSyELsdRBW4MRmbNdT2qppTAN
BgkqhkiG9w0BAQQFAAOBgQBuVJ+tVS0JqP4z9TgEeuMbVwn00CTKXz/fCuh6R/50
qq8JhERJGiR/ZHvHRLf+XawhnoE6daPAmE+WkIPtHIIhbMHCbbxG9ffdyaiNXRWy
5sI5XycF1FgYGpTFBYD9M0Lqsw+FIYaT2ZrbOGsx8h6pZoesKqm85RByIUjX4nJK
1g==
```

3. Importación CA, CUCM, y Certificados de la Voz GW CA en CUCM

El certificado del IPSec CUCM se exporta ya a un archivo del .pem. Como siguiente paso, el mismo proceso necesita ser completado con el certificado de la Voz GW y el certificado de CA. Para hacer eso, necesitan primero ser visualizados en una terminal con el **comando terminal crypto PEM del local1 de la exportación del pki** y ser copiados para separar los archivos del .pem.

```
KRK-UC-2x2811-2(config)#crypto pki export local1 pem terminal
% CA certificate:
-----BEGIN CERTIFICATE-----
MIIB9TCCAV6gAwIBAgIBATANBgkqhkiG9w0BAQQFADAOMQwwCgYDVQQDEwNJT1Mw
HhcNMTQxMTIxMTE1MTEyWhcNMTcxMTIwMTE1MTEyWjAOMQwwCgYDVQQDEwNJT1Mw
gZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAK6Cd2yxUywtbgBElkZUsP6eaZVv
6YfpEbFptyt6ptRdpxgjOYI3InEP3wewtmEPNeTJL8+a/W7MDUemm3t/NlWBO6T2
m9Bp6k0FNOBXMKeDfTSqOKEy7WfLASe/Pbq8M+JMpeMWz8xnMboYOb66rY8igZFz
k1tRPlIMSf5rO1tnAgMBAAGjYzBhMA8GA1UdEwEB/wQFMAMBAf8wDgYDVR0PAQH/
BAQDAgGGMB8GA1UdIwQYMBaAFJSLP5cnPL8bIP7VSKLtB6Z1socOMB0GA1UdDgQW
BBSUiz+XJzy/GyD+1Uii7QemdbKHDjANBgkqhkiG9w0BAQQFAAOBgQCUMC1SFVlS
TSS1ExbM9i2D4HOWYhCurhifqTWLxMMXj0jym24DoqZ91aDNG1VwiJ/Yv4i40t90
y65WzbapZL1S65q+d7BCLQypdrwcKkdS0dfTdKfXEsyWLhecRa8mnZckpgKBk8Ir
BfM9K+caXkfhPEPa644UzV9++OKMKhtDuQ==
-----END CERTIFICATE-----

% General Purpose Certificate:
-----BEGIN CERTIFICATE-----
MIIB2zCCAUSgAwIBAgIBAjANBgkqhkiG9w0BAQUFADAOMQwwCgYDVQQDEwNJT1Mw
HhcNMTQxMTIxMTIwNTAxWhcNMTUxMTIxMTIwNTAxWjAaMRgwFgYDVQQDEw9LUkst
VUMtMngyODExLTIwXDANBgkqhkiG9w0BAQEFAANLADBIAkEApGWIN1nAAtKLVMOj
mZVkQFgI8LrHD6zSrlaKgAJhlU+H/mnRQQ5rqitIpekDdPoowST9RxC5CJmB4spT
VWkYkwIDAQABo4GAMH4wLwYDVR0fBCgwJjAkoCKgIIYeaHR0cDovLzEwLjQ4LjQ2
LjI1MS9JT1NfQ0EuY3JsMAsGA1UdDwQEAwIFoDAfBgNVHSMEGDAWgBSUiz+XJzy/
GyD+1Uii7QemdbKHDjAdBgNVHQ4EFgQUtAWc61K5nYGgWqKAiIOLMlphfqIwDQYJ
KoZIhvcNAQEFBQADgYEAjDflH+N3yc3RykCig9B0aAIXWZPmaqLF9v9R75zc+f8x
zbSIzoVbBhnUOeuOj1hnIgHyyMjeELjTEh6uQrWUN2ElW1ypfmxk1jN5q0t+vfdR
+yepS04pFor9RoD7IWg6e/1hFDEep9hBvzrVwQHCjzeY0rVrPcLl26k5oauMwTs=
-----END CERTIFICATE-----
```

El % del certificado de CA decodifica a:

```
KRK-UC-2x2811-2(config)#crypto pki export local1 pem terminal
% CA certificate:
-----BEGIN CERTIFICATE-----
MIIB9TCCAV6gAwIBAgIBATANBgkqhkiG9w0BAQQFADAOMQwwCgYDVQQDEwNJT1Mw
HhcNMTQxMTIxMTE1MTEyWhcNMTcxMTIwMTE1MTEyWjAOMQwwCgYDVQQDEwNJT1Mw
gZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAK6Cd2yxUywtbgBElkZUsP6eaZVv
6YfpEbFptyt6ptRdpxgjOYI3InEP3wewtmEPNeTJL8+a/W7MDUemm3t/NlWBO6T2
m9Bp6k0FNOBXMKeDfTSqOKEy7WfLASe/Pbq8M+JMpeMWz8xnMboYOb66rY8igZFz
k1tRPlIMSf5rO1tnAgMBAAGjYzBhMA8GA1UdEwEB/wQFMAMBAf8wDgYDVR0PAQH/
BAQDAgGGMB8GA1UdIwQYMBaAFJSLP5cnPL8bIP7VSKLtB6Z1socOMB0GA1UdDgQW
BBSUiz+XJzy/GyD+1Uii7QemdbKHDjANBgkqhkiG9w0BAQQFAAOBgQCUMC1SFVlS
TSS1ExbM9i2D4HOWYhCurhifqTWLxMMXj0jym24DoqZ91aDNG1VwiJ/Yv4i40t90
y65WzbapZL1S65q+d7BCLQypdrwcKkdS0dfTdKfXEsyWLhecRa8mnZckpgKBk8Ir
BfM9K+caXkfhPEPa644UzV9++OKMKhtDuQ==
-----END CERTIFICATE-----

% General Purpose Certificate:
-----BEGIN CERTIFICATE-----
MIIB2zCCAUSgAwIBAgIBAjANBgkqhkiG9w0BAQUFADAOMQwwCgYDVQQDEwNJT1Mw
HhcNMTQxMTIxMTIwNTAxWhcNMTUxMTIxMTIwNTAxWjAaMRgwFgYDVQQDEw9LUkst
VUMtMngyODExLTIwXDANBgkqhkiG9w0BAQEFAANLADBIAkEApGWIN1nAAtKLVMOj
mZVkQFgI8LrHD6zSrlaKgAJhlU+H/mnRQQ5rqitIpekDdPoowST9RxC5CJmB4spT
VWkYkwIDAQABo4GAMH4wLwYDVR0fBCgwJjAkoCKgIIYeaHR0cDovLzEwLjQ4LjQ2
LjI1MS9JT1NfQ0EuY3JsMAsGA1UdDwQEAwIFoDAfBgNVHSMEGDAWgBSUiz+XJzy/
GyD+1Uii7QemdbKHDjAdBgNVHQ4EFgQUtAWc61K5nYGgWqKAiIOLMlphfqIwDQYJ
KoZIhvcNAQEFBQADgYEAjDflH+N3yc3RykCig9B0aAIXWZPmaqLF9v9R75zc+f8x
zbSIzoVbBhnUOeuOj1hnIgHyyMjeELjTEh6uQrWUN2ElW1ypfmxk1jN5q0t+vfdR
+yepS04pFor9RoD7IWg6e/1hFDEep9hBvzrVwQHCjzeY0rVrPcLl26k5oauMwTs=
-----END CERTIFICATE-----
```

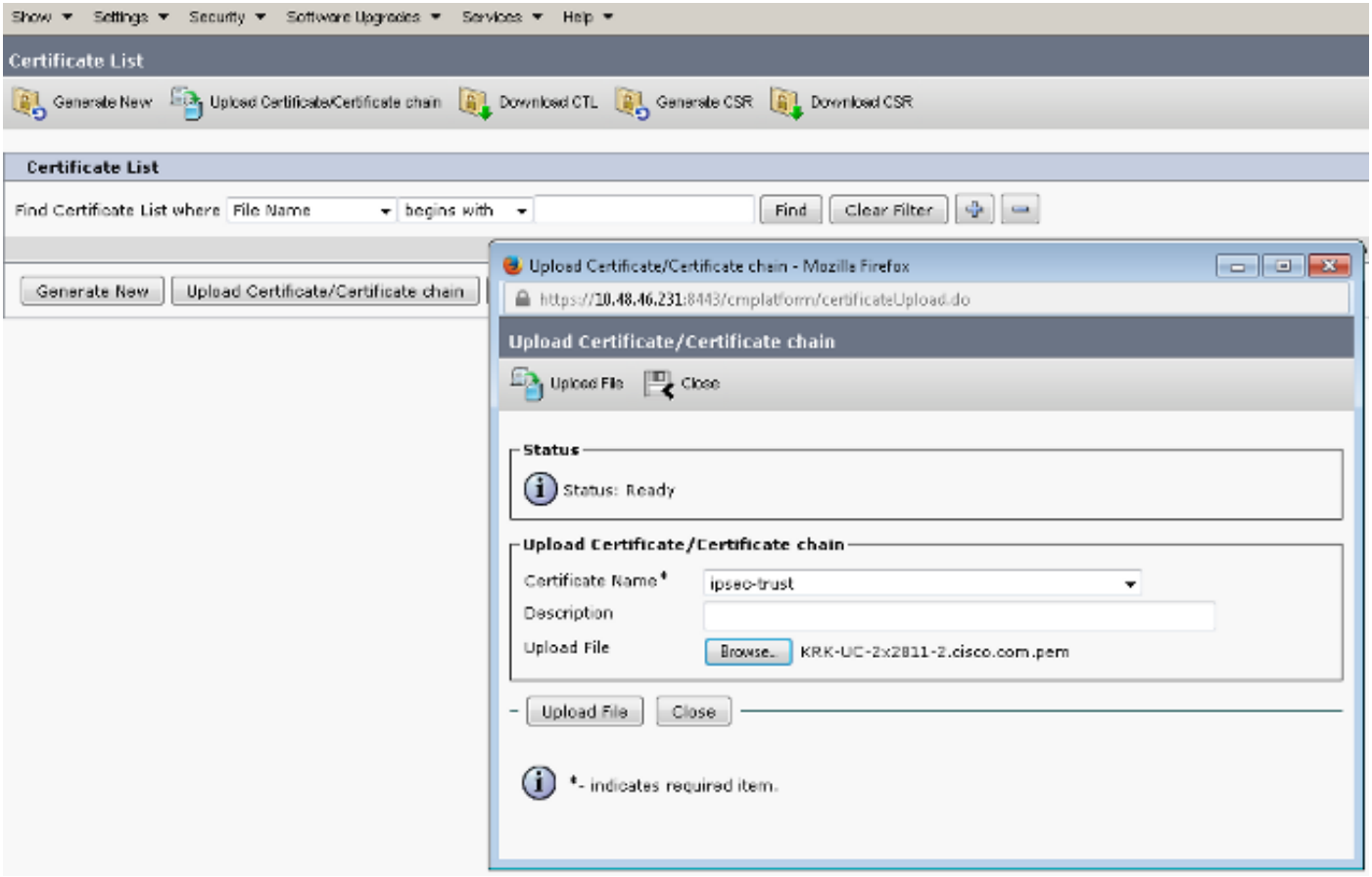
El % del certificado de fines generales decodifica a:

```
KRK-UC-2x2811-2(config)#crypto pki export local1 pem terminal
% CA certificate:
-----BEGIN CERTIFICATE-----
MIIB9TCCAV6gAwIBAgIBATANBgkqhkiG9w0BAQQFADAOMQwwCgYDVQQDEwNJT1Mw
HhcNMTQxMTIxMTE1MTEyWhcNMTcxMTIwMTE1MTEyWjAOMQwwCgYDVQQDEwNJT1Mw
gZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAK6Cd2yxUywtbgBElkZUsP6eaZVv
6YfpEbFptyt6ptRdpxgjOYI3InEP3wewtmEPNeTJL8+a/W7MDUemm3t/NlWBO6T2
m9Bp6k0FNOBXMKeDfTSqOKEy7WfLASe/Pbq8M+JMpeMWz8xnMboYOb66rY8igZFz
k1tRPlIMSf5rO1tnAgMBAAGjYzBhMA8GA1UdEwEB/wQFMAMBAf8wDgYDVR0PAQH/
BAQDAgGGMB8GA1UdIwQYMBaAFJSLP5cnPL8bIP7VSKLtB6Z1socOMB0GA1UdDgQW
BBSUiz+XJzy/GyD+1Uii7QemdbKHDjANBgkqhkiG9w0BAQQFAAOBgQCUMC1SFVlS
TSS1ExbM9i2D4HOWYhCurhifqTWLxMMXj0jym24DoqZ91aDNG1VwiJ/Yv4i40t90
y65WzbapZL1S65q+d7BCLQypdrwcKkdS0dfTdKfXEsyWLhecRa8mnZckpgKBk8Ir
BfM9K+caXkfhPEPa644UzV9++OKMKhtDuQ==
-----END CERTIFICATE-----

% General Purpose Certificate:
-----BEGIN CERTIFICATE-----
MIIB2zCCAUSgAwIBAgIBAjANBgkqhkiG9w0BAQUFADAOMQwwCgYDVQQDEwNJT1Mw
HhcNMTQxMTIxMTIwNTAxWhcNMTUxMTIxMTIwNTAxWjAaMRgwFgYDVQQDEw9LUkst
VUMtMngyODExLTIwXDANBgkqhkiG9w0BAQEFAANLADBIAkEApGWIN1nAAtKLVMOj
mZVkQFgI8LrHD6zSrlaKgAJhlU+H/mnRQQ5rqitIpekDdPoowST9RxC5CJmB4spT
VWkYkwIDAQABo4GAMH4wLwYDVR0fBCgwJjAkoCKgIIYeaHR0cDovLzEwLjQ4LjQ2
LjI1MS9JT1NfQ0EuY3JsMAsGA1UdDwQEAwIFoDAfBgNVHSMEGDAWgBSUiz+XJzy/
GyD+1Uii7QemdbKHDjAdBgNVHQ4EFgQUtAWc61K5nYGgWqKAiIOLMlphfqIwDQYJ
KoZIhvcNAQEFBQADgYEAjDflH+N3yc3RykCig9B0aAIXWZPmaqLF9v9R75zc+f8x
zbSIzoVbBhnUOeuOj1hnIgHyyMjeELjTEh6uQrWUN2ElW1ypfmxk1jN5q0t+vfdR
```

```
+yepS04pFor9RoD7IWg6e/1hFDEep9hBvzrVwQHCjzeY0rVrPcLl26k5oauMwTs=
-----END CERTIFICATE-----
```

Después de que se guarden como archivos del .pem, necesitan ser importados a CUCM. Elija el **Certificate Management (Administración de certificados) del > Security (Seguridad) de la administración OS > el certificado de la carga/el certificado unificados Cisco**.

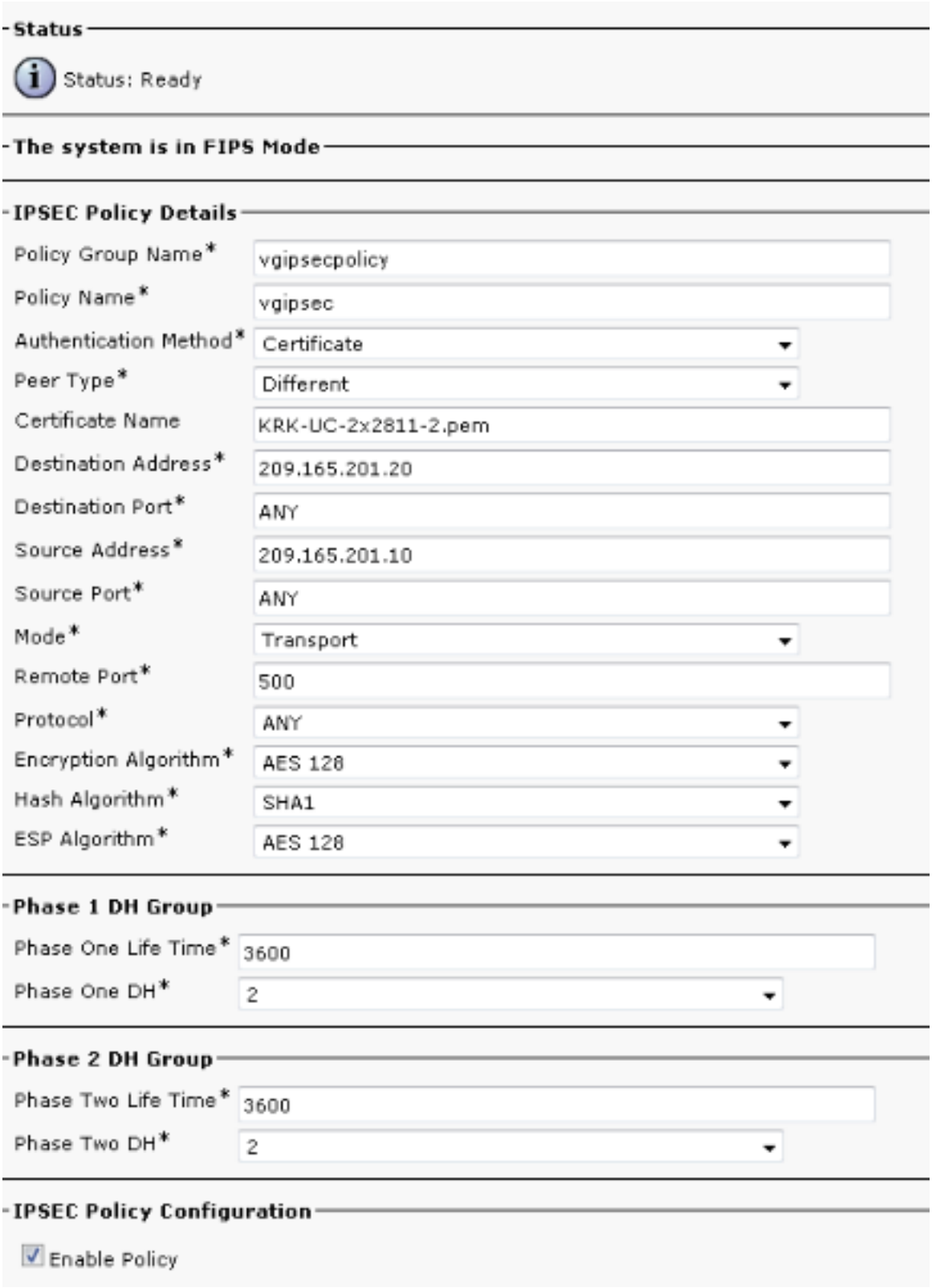
- Certificado CUCM como IPSec
- Certificado de la Voz GW como IPSec-confianza
- Certificado de CA como IPSec-confianza:



4. Configuraciones del túnel IPsec de la configuración en CUCM

El siguiente paso es configuración del túnel IPsec entre CUCM y la Voz GW. La configuración del túnel IPsec en CUCM se realiza vía la página Web de administración unificada Cisco OS (https://<cucm_ip_address>/cmplatform). Elija la **nueva directiva del IPSec de la Seguridad > de la configuración IPSec > Add**.

En este ejemplo, una directiva llamada “vgipsecpolicy” fue creada, con la autenticación basada en los Certificados. Todas las informaciones necesitas apropiadas de ser completado y corresponden a la configuración en la Voz GW.



Note: El nombre del certificado del gateway de voz necesita ser especificado en el campo de nombre del certificado.

5. Configure la configuración del túnel IPsec en la Voz GW

Este ejemplo, con los comentarios en línea, presenta la configuración correspondiente en una Voz GW.

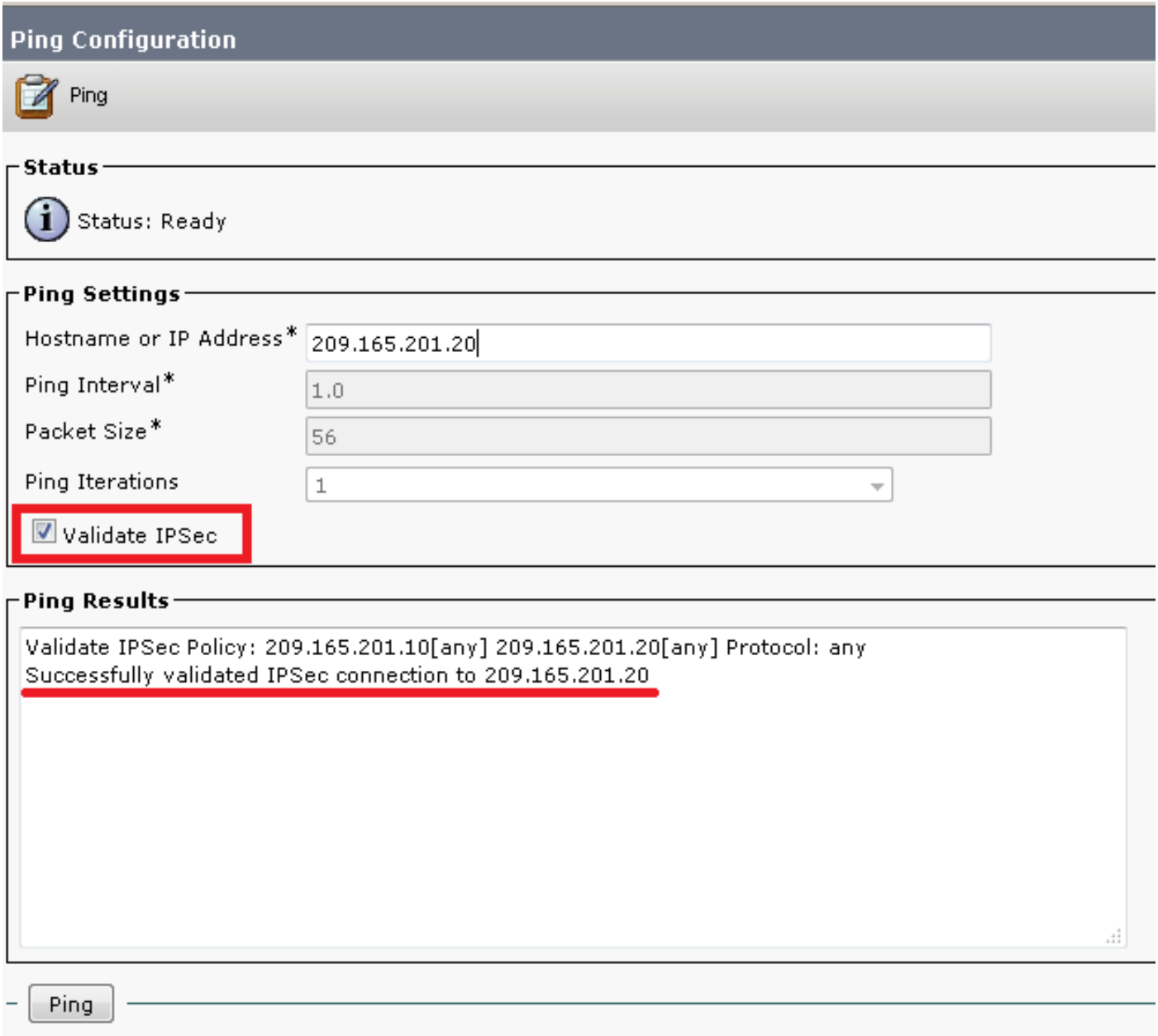
```
crypto isakmp policy 1    (defines an IKE policy and enters the config-iskmp mode)
 encr aes                 (defines the encryption)
 group 2                  (defines 1024-bit Diffie-Hellman)
 lifetime 57600           (isakmp security association lifetime value)

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
```

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

Verifique el estatus del túnel IPsec en el extremo CUCM

La manera más rápida de verificar el estatus del túnel IPsec en CUCM es va a la página de administración OS y utiliza la opción del **ping** bajo los servicios > ping. Asegúrese que la casilla de verificación del **IPSec del validar** esté marcada. Obviamente, la dirección IP especificada aquí es la dirección IP del GW.



Note: Vea este bug Cisco ID para la información sobre la validación del túnel IPsec vía la característica del ping en CUCM:

- Id. de bug Cisco CSCuo53813 - Valide el espacio en blanco de los resultados del ping del IPSec cuando se envían los paquetes ESP (Encapsulating Security Payload)
- Id. de bug Cisco CSCud20328 - Valide el mensaje de error incorrecto de las demostraciones de la política IPSec en el modo FIP

Verifique el estatus del túnel IPsec en el extremo del gateway de voz

Para verificar si la configuración se ejecute muy bien o no, necesita ser confirmado que crean a las asociaciones de seguridad (SA) para las capas (asociación de la seguridad de Internet y administración de claves Protoco (ISAKMP) y IPSec) correctamente.

Para marcar si el SA para el ISAKMP se crea y trabaja correctamente, ingrese el **comando show crypto isakmp sa** en el 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: El estatus apropiado para el SA debe ser ACTIVO y QM_IDLE.

La segunda capa es SA para el IPSec. Su estatus se puede verificar con el **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**: Los índices entrantes y salientes de la política de seguridad (SPI) se deben crear en el ACTIVE del estatus, y los contadores para el número de paquetes encapsulado/decapsulated y cifrado/desencriptado deben crecer cada vez que cualquier tráfico vía un túnel se genera.

El paso más reciente es confirmar que el MGCP GW está en el estado registrado y la configuración de TFTP fue descargada correctamente de CUCM sin ningunos errores. Esto se puede confirmar de la salida de estos 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#
```

Troubleshooting

Esta sección proporciona la información que usted puede utilizar para resolver problemas su

configuración.

Resuelva problemas el túnel IPsec en el extremo CUCM

En CUCM no hay servicio de la utilidad responsable de la terminación y de la Administración del IPSec. CUCM utiliza un paquete de las herramientas del IPSec del Red Hat incorporado al sistema operativo. La daemon que se ejecuta en Red Hat Linux y termina conexión IPSec es OpenSwan.

Cada vez que la directiva del IPSec se habilita o se inhabilita en CUCM (> Security (Seguridad) > configuración IPSec de la administración OS), se recomienza la daemon de Openswan. Esto se puede observar en el registro de mensajes de Linux. Un reinicio es indicado por estas líneas:

```
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#
```

Cada vez que hay un problema con conexión IPSec encendido el CUCM, las entradas más recientes del registro de mensajes se deben marcar (ingrese el comando del **Syslog/del messages* del activelog de la lista del archivo**) para confirmar que Openswan es ascendente y se

ejecuta. Si Openswan se ejecuta y comenzó sin los errores, usted puede resolver problemas la configuración del IPSec. La daemon responsable de la configuración de los túneles IPsec en Openswan es Plutón. Los registros de Plutón se escriben para asegurar abren una sesión el Red Hat, y pueden ser recolectados vía el **archivo consiguen el** comando del **Syslog/secure.* del activelog** o vía **RTMT: Registros de seguridad**.

> **Note**: Más información sobre cómo recolectar los registros vía RTMT se puede encontrar en RTMT la documentación.

Si es difícil determinar la fuente del problema basado en estos registros, el IPSec se puede verificar más lejos por el Centro de Asistencia Técnica (TAC) vía la raíz en el CUCM. Después de que usted acceda CUCM vía la raíz, la información y los registros sobre el estatus del IPSec se pueden marcar con estos comandos:

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

Hay también una opción para generar un sosreport del Red Hat vía la raíz. Este informe contiene toda la información requerida por el soporte del Red Hat para resolver problemas otros problemas en el nivel del sistema de funcionamiento:

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

Resuelva problemas el túnel IPsec en el extremo del gateway de voz

En este sitio, usted puede resolver problemas todas las fases de configuración del túnel IPsec después de que usted habilite estos comandos debug:

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

> **Note**: Los pasos detallados para resolver problemas el IPSec se encuentran en el Troubleshooting de IPSec: Entendiendo y con los comandos debug.

Usted puede resolver problemas los problemas MGCP GW con estos comandos debug:

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