基於CA簽名證書的語音GW和CUCM之間通過IPsec的安全MGCP通訊配置示例

目錄

簡介

本文說明如何根據憑證授權單位(CA)簽署的憑證，透過網際網路通訊協定安全(IPsec)，成功保護語音閘道(GW)和CUCM（思科整合通訊管理員）之間的媒體閘道控制通訊協定(MGCP)訊號傳送。為了通過MGCP建立安全呼叫，需要單獨保護信令和即時傳輸協定(RTP)流。它似乎有很好的文檔記錄，並且設定加密RTP流非常簡單，但安全RTP流不包括安全MGCP信令。如果MGCP信令不安全，則RTP流的加密金鑰將以明文形式傳送。

必要條件

需求

思科建議您瞭解以下主題：

- 註冊到CUCM的MGCP語音網關，用於傳送和接收呼叫
- 證書頒發機構代理功能(CAPF)服務已啟動，群集設定為混合模式

- GW上的Cisco IOS®映像支援加密安全功能
- 為安全即時傳輸協定(SRTP)配置的電話和MGCP GW

採用元件

本文中的資訊係根據以下軟體和硬體版本：

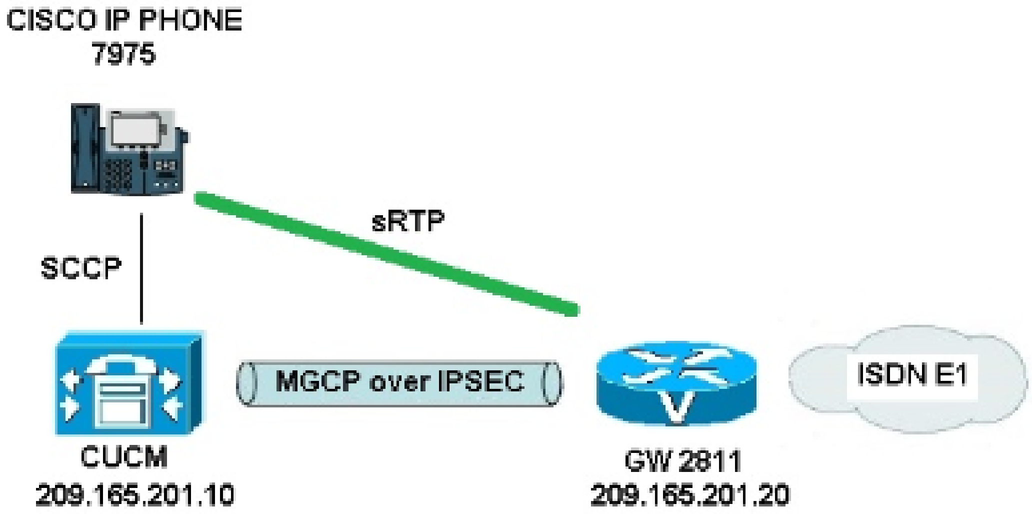
- CUCM — 單節點 — 在聯邦資訊處理標準(FIPS)模式下運行GGSG（思科全球政府解決方案組）版本8.6.1.20012-14
- 運行SCCP75-9-3-1SR2-1S的7975電話
- GW - Cisco 2811 - C2800NM-ADVENTERPRISEK9-M，版本15.1(4)M8
- E1 ISDN語音卡 — VWIC2-2MFT-T1/E1 - 2埠RJ-48 Multiflex中繼

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

設定

附註：使用命令查詢工具(僅供已註冊客戶使用)可獲取本節中使用的命令的更多資訊。

網路圖表



為了成功在CUCM和語音GW之間設定IPsec，請完成以下步驟：

1. 配置語音GW上的CA並為語音GW生成CA簽名的證書
2. 生成CUCM CA簽名的IPsec證書
3. 在CUCM上匯入CA、CUCM和語音GW CA證書
4. 在CUCM上配置IPsec隧道設定
5. 配置語音GW上的IPsec隧道設定

1.在語音GW上配置CA並為語音GW生成CA簽名的證書

第一步，需要在語音GW（Cisco IOS CA伺服器）上生成Rivest-Shamir-Addleman(RSA)金鑰對：

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

將使用通過簡單證書註冊協定(SCEP)完成的註冊，因此啟用HTTP伺服器：

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

要在網關上配置CA伺服器，需要完成以下步驟：

1. 設定PKI伺服器名稱。它必須與之前生成的金鑰對同名。
   ```
   KRK-UC-2x2811-2(config)#crypto pki server IOS_CA
   ```
2. 指定將為CA伺服器儲存所有資料庫條目的位置。
   ```
   KRK-UC-2x2811-2(cs-server)#crypto pki server IOS_CA
   ```
3. 配置CA頒發者名稱。
   ```
   KRK-UC-2x2811-2(cs-server)#issuer-name cn=IOS
   ```
4. 指定要在證書伺服器頒發的證書中使用的證書吊銷清單(CRL)分發點(CDP)，並啟用對Cisco IOS從屬CA伺服器的證書重新註冊請求的自動授予。
   ```
   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. 啟用CA伺服器。
   ```
   KRK-UC-2x2811-2(cs-server)#no shutdown
   ```

下一步是為CA證書建立信任點，為路由器證書建立本地信任點，該信任點的URL註冊指向本地HTTP伺服器：

```
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
```

若要產生由本地CA簽署的路由器憑證，需要驗證信任點並將其註冊：

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

之後，路由器證書將由本地CA生成並簽名。列出路由器上的證書以進行驗證。

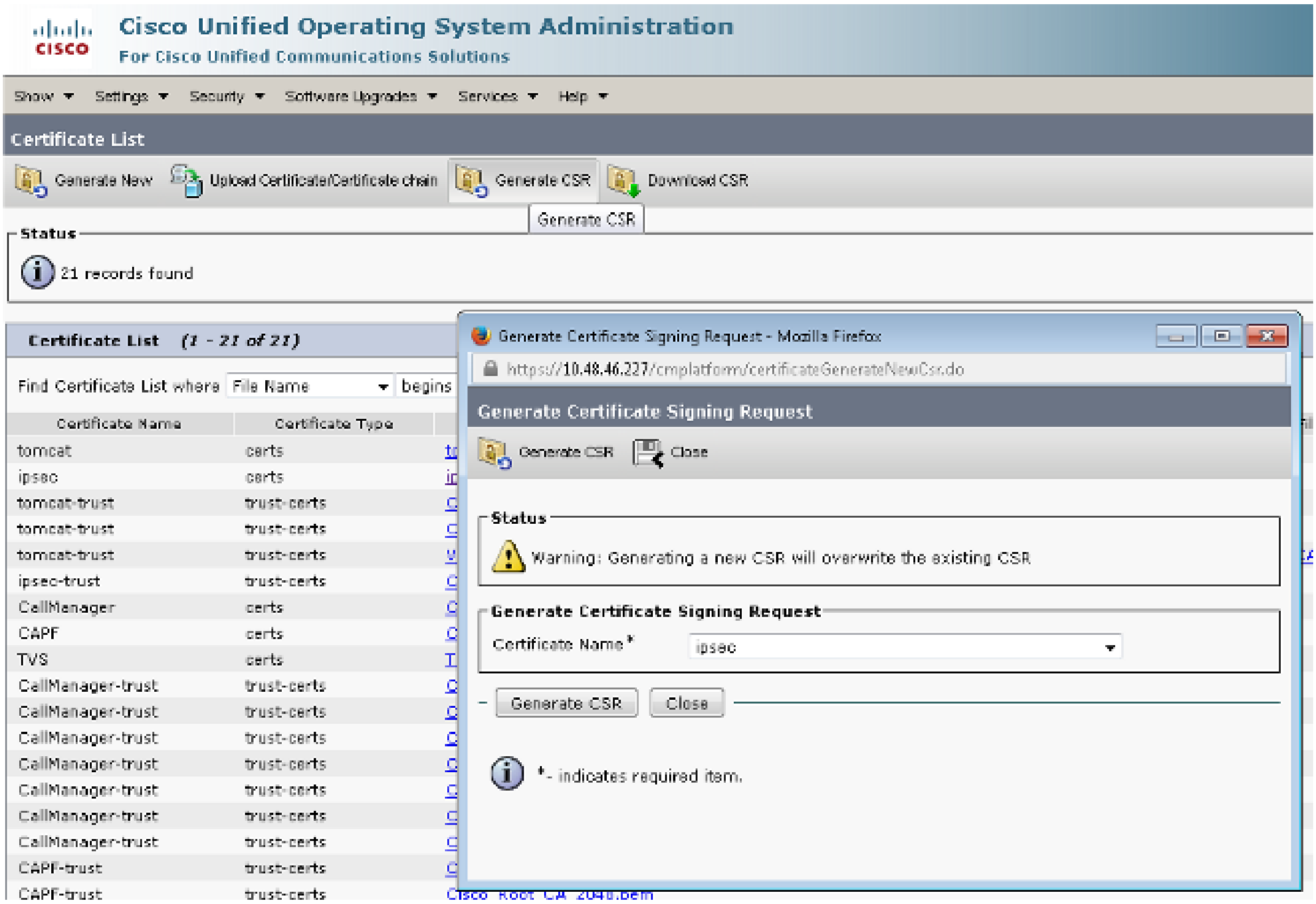
```
KRK-UC-2x2811-2#show crypto ca certificates
Certificate
 Status: Available
 Certificate Serial Number (hex): 02
 Certificate Usage: General Purpose
 Issuer:
   cn=IOS
 Subject:
   Name: KRK-UC-2x2811-2
   cn=KRK-UC-2x2811-2
 CRL Distribution Points:
   http://10.48.46.251/IOS_CA.crl
 Validity Date:
   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
```

應列出兩個證書。第一個是由本地CA簽署的路由器(KRK-UC-2x2811-2)證書，第二個是CA證書。

2.生成CUCM CA簽名的IPsec證書

CUCM for IPsec隧道設定使用ipsec.pem證書。預設情況下，此證書是自簽名的，在安裝系統時生成。若要將其替換為CA簽名的證書，首先需要從CUCM OS管理頁面生成IPsec的CSR（證書簽名請求）。選擇**Cisco Unified OS Administration > Security > Certificate Management > Generate CSR**。


Cisco Unified Operating System Administration
For Cisco Unified Communications Solutions
Show
Settings
Security
Software Upgrades
Services
Help
Certificate List
Generate New
Upload Certificate/Certificate chain
Generate CSR
Download CSR
Generate CSR

Status

21 records found

Certificate List (1 - 21 of 21)

Find Certificate List where File Name begins

Certificate Name	Certificate Type	
tomcat	certs	tc
ipsec	certs	ip
tomcat-trust	trust-certs	C
tomcat-trust	trust-certs	C
tomcat-trust	trust-certs	V
ipsec-trust	trust-certs	C
CallManager	certs	C
CAPF	certs	C
TVS	certs	T
CallManager-trust	trust-certs	C
CallManager-trust	trust-certs	C
CallManager-trust	trust-certs	C
CallManager-trust	trust-certs	C
CallManager-trust	trust-certs	C
CallManager-trust	trust-certs	C
CallManager-trust	trust-certs	C
CAPF-trust	trust-certs	C
CAPF-trust	trust-certs	Cisco Root CA 2048.pem

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

*- indicates required item.

產生CSR後，需要從CUCM下載它並針對GW上的CA進行註冊。為此，請輸入**crypto pki server IOS_CA request pkcs10 terminal base64**命令，並需要通過終端貼上簽名請求雜湊。系統將顯示授予的證書，需要複製證書並將其儲存為ipsec.pem檔案。

```
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==
```

附註：若要解碼和檢查Base64編碼證書的內容，請輸入**openssl x509 -in certificate.crt -text -noout**命令。

授予的CUCM證書將解碼為：

```
Certificate:
Data&colon;
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.在CUCM上匯入CA、CUCM和語音GW CA證書

CUCM IPsec證書已匯出到.pem檔案。下一步，需要完成語音GW證書和CA證書的相同過程。為此，需要首先使用**crypto pki export local1 pem terminal** 命令在終端上顯示這些檔案，並將其複製到單獨的.pem檔案中。

```
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-----
```

% CA證書解碼為：

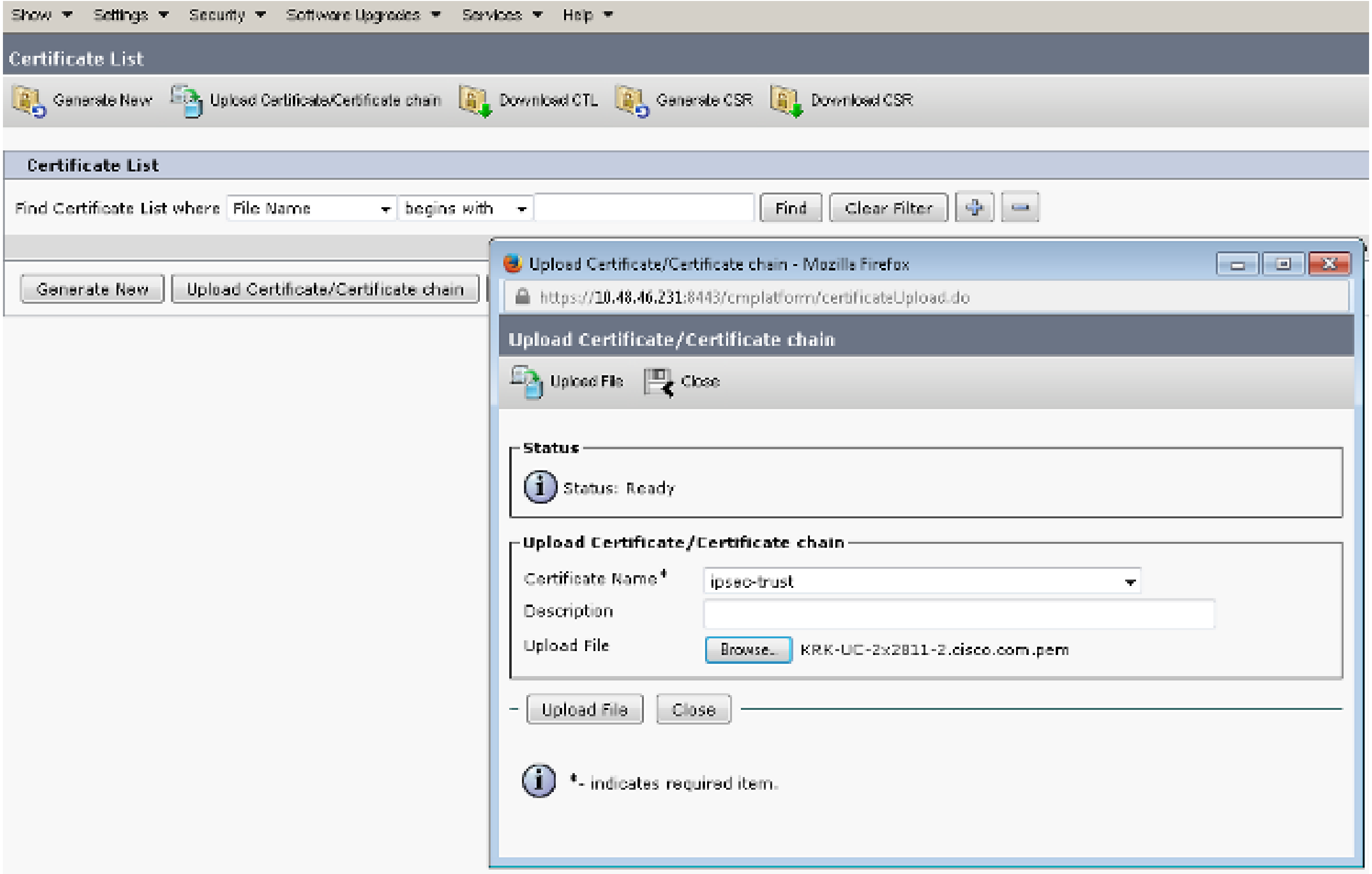
```
Certificate:
   Data&colon;
       Version: 3 (0x2)
       Serial Number: 1 (0x1)
       Signature Algorithm: md5WithRSAEncryption
       Issuer: CN=IOS
       Validity
           Not Before: Nov 21 11:51:12 2014 GMT
           Not After : Nov 20 11:51:12 2017 GMT
       Subject: CN=IOS
       Subject 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
```

% General Purpose Certificate解碼為：

```
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
```

將其另存為.pem檔案後，需要將其匯入CUCM。選擇**Cisco Unified OS Administration > Security > Certificate management > Upload Certificate/Certificate**。

- 作為IPsec的CUCM證書
- 作為IPsec-trust的語音GW證書
- 作為IPsec-trust的CA證書：


Show ▾ Settings ▾ Security ▾ Software Upgrades ▾ Services ▾ Help ▾
Certificate List
Generate New
Upload Certificate/Certificate chain
Download CTL
Generate CSR
Download CSR
Certificate List
Find Certificate List where
File Name
begins with
Find
Clear Filter
Generate New
Upload Certificate/Certificate chain
Upload Certificate/Certificate chain - Mozilla Firefox
https://10.48.46.231:8443/cmplatform/certificateUpload.do
Upload Certificate/Certificate chain
Upload File
Close
Status
Status: Ready
Upload Certificate/Certificate chain
Certificate Name*
Description
Upload File
Browse...
Upload File
Close
*- indicates required item.

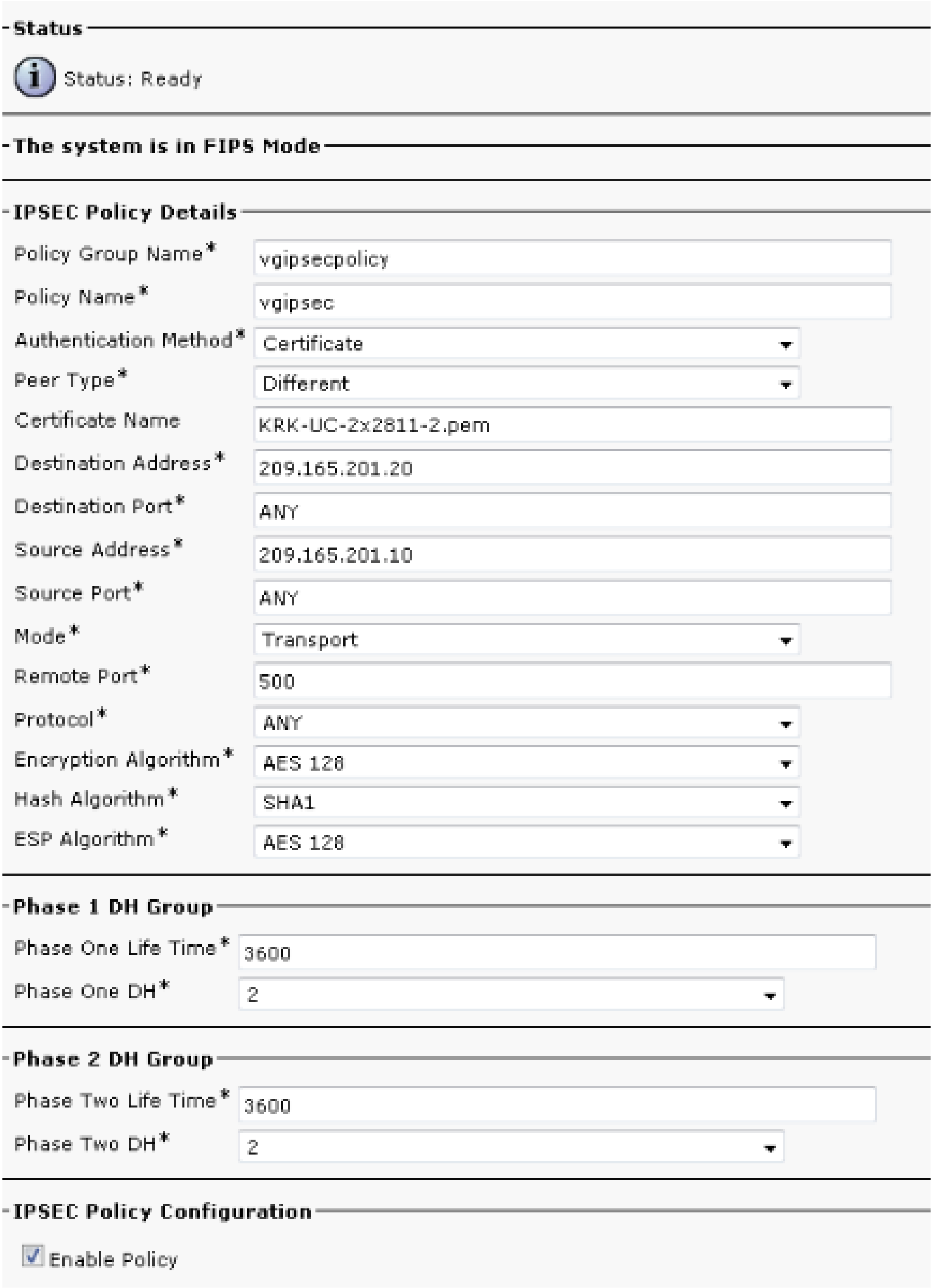
Certificate Name* ipsec-trust

Upload File KRK-UC-2x2811-2.cisco.com.pem

4.在CUCM上配置IPsec隧道設定

下一步是配置CUCM和語音GW之間的IPsec隧道。CUCM上的IPsec隧道配置通過思科統一作業系統管理網頁(https://<cucm_ip_address>/cmplatform)執行。 選擇**Security > IPSEC Configuration > Add new IPsec policy**。

在本示例中，建立了一個名為「vgipsecpolicy」的策略，該策略使用基於證書的身份驗證。需要填寫所有適當資訊並對應於語音GW上的配置。



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

附註：需要在Certificate Name欄位中指定語音網關證書名稱。

5.配置語音GW上的IPsec隧道設定

此示例包含內聯註釋，顯示語音GW上的相應配置。

```
crypto isakmp policy 1     (defines an IKE policy and enters the config-iskmp mode)
```

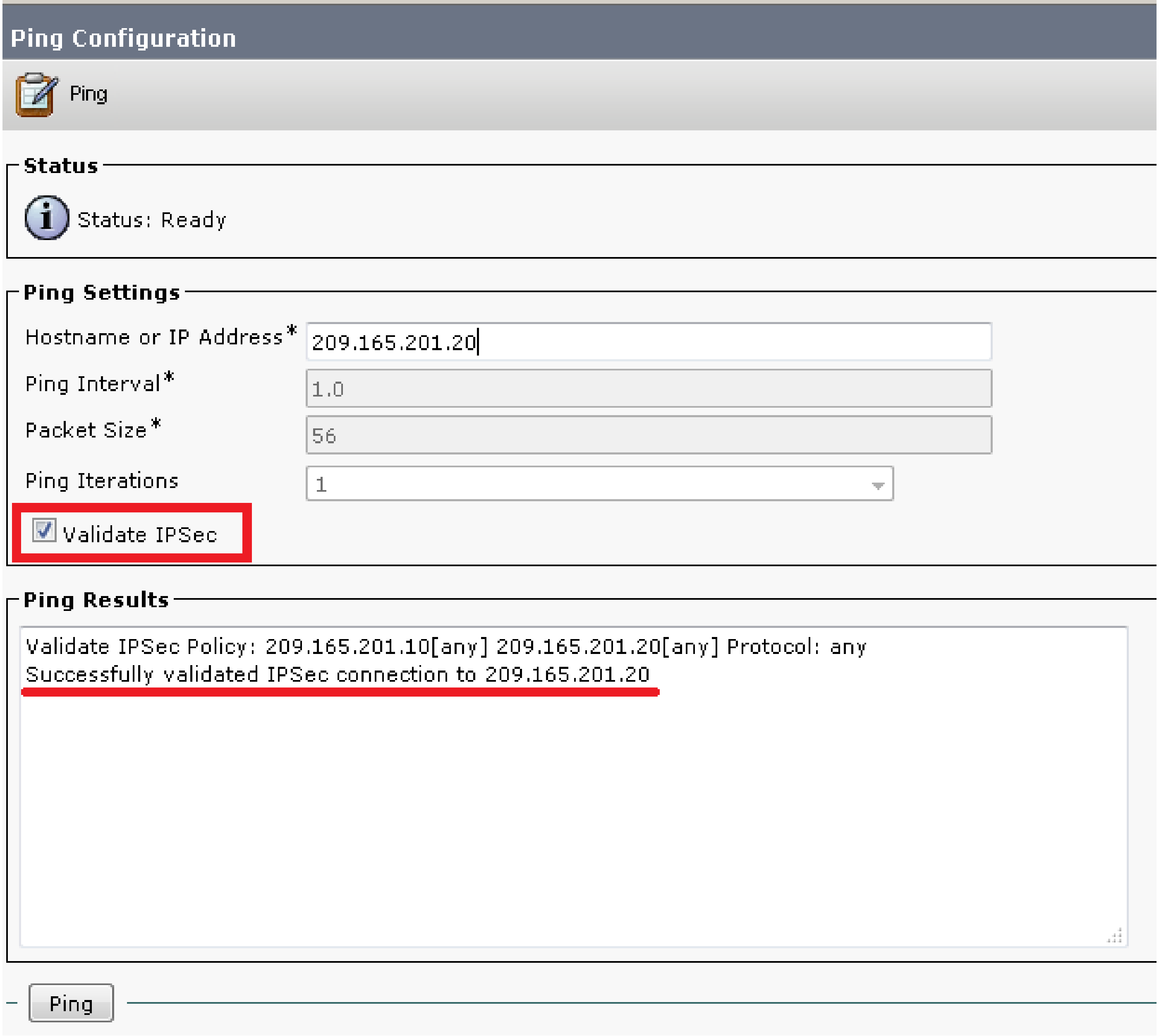
```
 encr aes                 (defines the encryption)
 group 2                  (defines 1024-bit Diffie-Hellman)
 lifetime 57600           (isakmp security association lifetime value)

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
```

驗證

使用本節內容，確認您的組態是否正常運作。

驗證CUCM終端上的IPsec隧道狀態

驗證CUCM上的IPsec隧道狀態的最快方法是轉至OS Administration（作業系統管理）頁面，並使用Services（服務）> Ping(ping)下的**ping**選項。確保選中**Validate IPSec**覈取方塊。顯然，此處指定的IP地址是GW的IP地址。



Status

Status: Ready

Ping Settings

Hostname or IP Address* 209.165.201.20

Ping Interval* 1.0

Packet Size* 56

Ping Iterations 1

☑ 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
```

附註：如需透過CUCM上的ping功能驗證IPsec通道的相關資訊，請參閱以下思科錯誤ID:

— 思科錯誤ID CSCuo53813 — 在傳送ESP（封裝安全負載）資料包時驗證IPSec Ping結果為空
— 思科錯誤ID CSCud20328 — 驗證IPSec策略在FIPS模式下顯示錯誤錯誤消息

驗證語音閘道端上的IPsec通道狀態

為了驗證安裝程式是否運行正常，需要確認是否正確建立了兩個層的安全關聯(SA)(Internet安全關聯和金鑰管理協定(ISAKMP)和IPsec)。

若要檢查是否為ISAKMP建立了SA並且工作正常，請在GW上輸入**show crypto isakmp sa**命令。

```
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
```

附註：SA的正確狀態應為ACTIVE和QM_IDLE。

第二層是用於IPsec的SA。其狀態可以使用**show crypto ipsec sa**命令驗證。

```
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#
```

附註：應在狀態ACTIVE中建立入站和出站安全策略索引(SPI)，並且每當通過隧道生成任何流量時，封裝/解除封裝和加密/解密的資料包數量的計數器應增長。

最後一步是確認MGCP GW處於註冊狀態，並且從CUCM正確下載了TFTP配置並且沒有任何故障。可從以下命令的輸出中確認這一點：

```
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#
```

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

排除CUCM端的IPsec隧道故障

在CUCM上，沒有負責IPsec終止和管理的可維護性服務。CUCM使用內建於作業系統中的Red Hat IPsec工具包。在Red Hat Linux上運行並終止IPsec連線的守護程式是OpenSwan。

每次在CUCM（作業系統管理>安全> IPSEC配置）上啟用或禁用IPsec策略時，都會重新啟動Openswan守護程式。可以在Linux消息日誌中觀察到這種情況。以下行表示重新啟動：

```
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
```

每次CUCM上的IPsec連線發生問題時，都應該檢查消息日誌中的最後一個條目(輸入**file list activivelog syslog/messages***命令)，以確認Openswan已啟動且正在運行。如果Openswan運行且啟動時沒有出現錯誤，您可以對IPsec設定進行故障排除。在Openswan中負責設定IPsec隧道的守護程式是Pluto。編寫冥王星日誌是為了保護Red Hat上的日誌，可以通過**file get activelog syslog/secure.*命令或通過RTMT收集**這些日**志：安全日誌**。

附註：有關如何通過RTMT收集日誌的更多資訊，請參見RTMT文檔。

如果難以根據這些日誌確定問題的來源，則技術支援中心(TAC)可以通過CUCM上的根進一步驗證IPsec。通過根訪問CUCM後，可以使用以下命令檢查有關IPsec狀態的資訊及日誌：

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

還有一個選項可以通過根生成Red Hat sosreport。此報告包含Red Hat支援需要的所有資訊，以便解決作業系統級別上的進一步問題：

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

對語音網關端的IPsec隧道進行故障排除

在此站點上，您可以在啟用以下debug命令後對IPsec隧道設定的所有階段進行故障排除：

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

附註：有關IPsec故障排除的詳細步驟，請參閱IPsec故障排除：瞭解和使用偵錯指令.

您可以使用以下debug指令排除MGCP GW問題：

```
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
```