CA 서명 인증서 컨피그레이션을 기반으로 IPsec을 통한 음성 GW와 CUCM 간의 보안 MGCP 통신 예

목차

소개

이 문서에서는 CA(Certificate Authority) 서명 인증서를 기반으로 IPsec(Internet Protocol Security)를 통해 GW(Voice Gateway Control Protocol)와 CUCM(Cisco Unified Communications Manager) 간의 MGCP(Media Gateway Control Protocol) 신호를 성공적으로 보호하는 방법에 대해 설명합니다.MGCP를 통해 보안 통화를 설정하려면 신호 처리 및 RTP(Real-time Transport Protocol) 스트림을 별도로 보호해야 합니다.문서화가 잘 되어 있고 암호화된 RTP 스트림을 설정하는 것이 매우 간단한 것처럼 보이지만, 보안 RTP 스트림에는 보안 MGCP 시그널링이 포함되지 않습니다.MGCP 신호 처리가 보안되지 않으면 RTP 스트림에 대한 암호화 키가 암호화되지 않은 상태로 전송됩니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 통화를 보내고 받기 위해 CUCM에 등록된 MGCP 음성 게이트웨이
- CAPF(Certificate Authority Proxy Function) 서비스가 시작되었으며 클러스터가 혼합 모드로 설정되었습니다.
- GW의 Cisco IOS® 이미지는 암호화 보안 기능을 지원합니다.
- SRTP(Secure Real-time Transport Protocol)용으로 구성된 전화기 및 MGCP GW

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

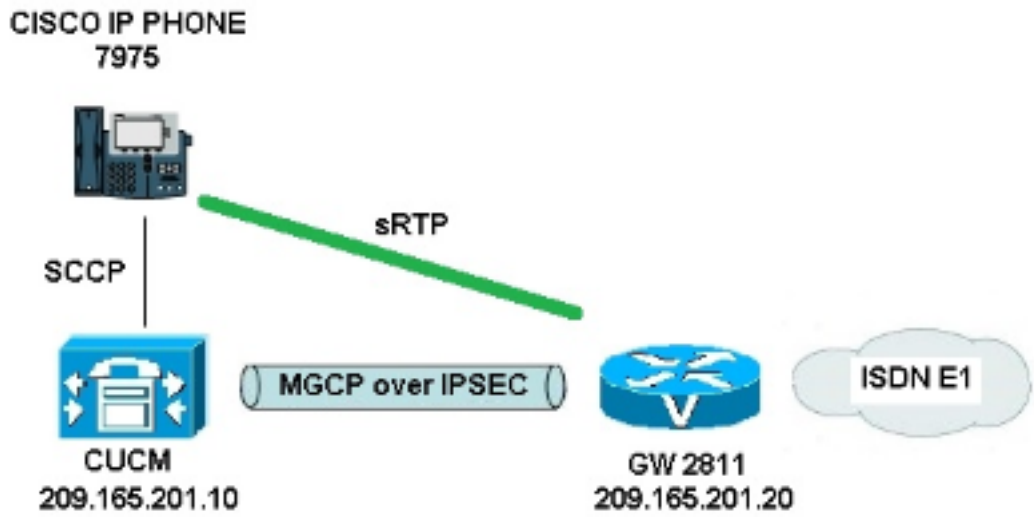
- CUCM - 단일 노드 - FIPS(Federal Information Processing Standard) 모드에서 GSG(Cisco의 Global Government Solutions Group) 버전 8.6.1.20012-14를 실행합니다.
- SCCP75-9-3-1SR2-1S를 실행하는 7975 전화기
- GW - Cisco 2811 - C2800NM-ADVENTERPRISEK9-M, 버전 15.1(4)M8
- E1 ISDN 음성 카드 - VWIC2-2MFT-T1/E1 - 2포트 RJ-48 Multiflex Trunk

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

> **참고:**이 섹션에 사용된 명령에 대한 자세한 내용을 보려면 Command Lookup Tool(등록된 고객만 해당)을 사용합니다.

네트워크 다이어그램



CUCM과 음성 GW 간에 IPsec을 성공적으로 설정하려면 다음 단계를 완료하십시오.

1. 음성 GW에서 CA를 구성하고 음성 GW용 CA 서명 인증서를 생성합니다.
2. CUCM CA 서명 IPsec 인증서 생성

3. CUCM에서 CA, CUCM 및 음성 GW CA 인증서 가져오기
4. CUCM에서 IPsec 터널 설정 구성
5. 음성 GW에서 IPsec 터널 설정 구성

1. 음성 GW에서 CA를 구성하고 음성 GW용 CA 서명 인증서 생성

첫 번째 단계로, 음성 GW(Cisco IOS CA 서버)에서 Rivest-Shamir-Addleman(RSA) 키 쌍을 생성해야 합니다.

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

SCEP(Simple Certificate Enrollment Protocol)를 통해 완료된 등록이 사용되므로 HTTP 서버를 활성화합니다.

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

게이트웨이에 CA 서버를 구성하려면 다음 단계를 완료해야 합니다.

1. PKI 서버 이름을 설정합니다.이전에 생성한 키 쌍과 이름이 같아야 합니다.
   ```
   KRK-UC-2x2811-2(config)#crypto pki server IOS_CA
   ```
2. CA 서버에 대해 모든 데이터베이스 항목을 저장할 위치를 지정합니다.
   ```
   KRK-UC-2x2811-2(cs-server)#crypto pki server IOS_CA
   ```
3. CA 발급자 이름을 구성합니다.
   ```
   KRK-UC-2x2811-2(cs-server)#issuer-name cn=IOS
   ```
4. 인증서 서버에서 발급한 인증서에 사용할 CRL(Certificate Revocation List) 배포 지점(CDP)을 지정하고 Cisco IOS 하위 CA 서버에 대해 인증서 재등록 요청을 자동으로 부여할 수 있습니다.
   ```
   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. CA 서버를 활성화합니다.
   ```
   KRK-UC-2x2811-2(cs-server)#no shutdown
   ```

다음 단계는 로컬 HTTP 서버를 가리키는 URL 등록을 사용하여 라우터 인증서에 대한 CA 인증서 및 로컬 신뢰 지점을 생성하는 것입니다.

```
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
```

로컬 CA에서 서명한 라우터의 인증서를 생성하려면 신뢰 지점을 인증하고 등록해야 합니다.

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

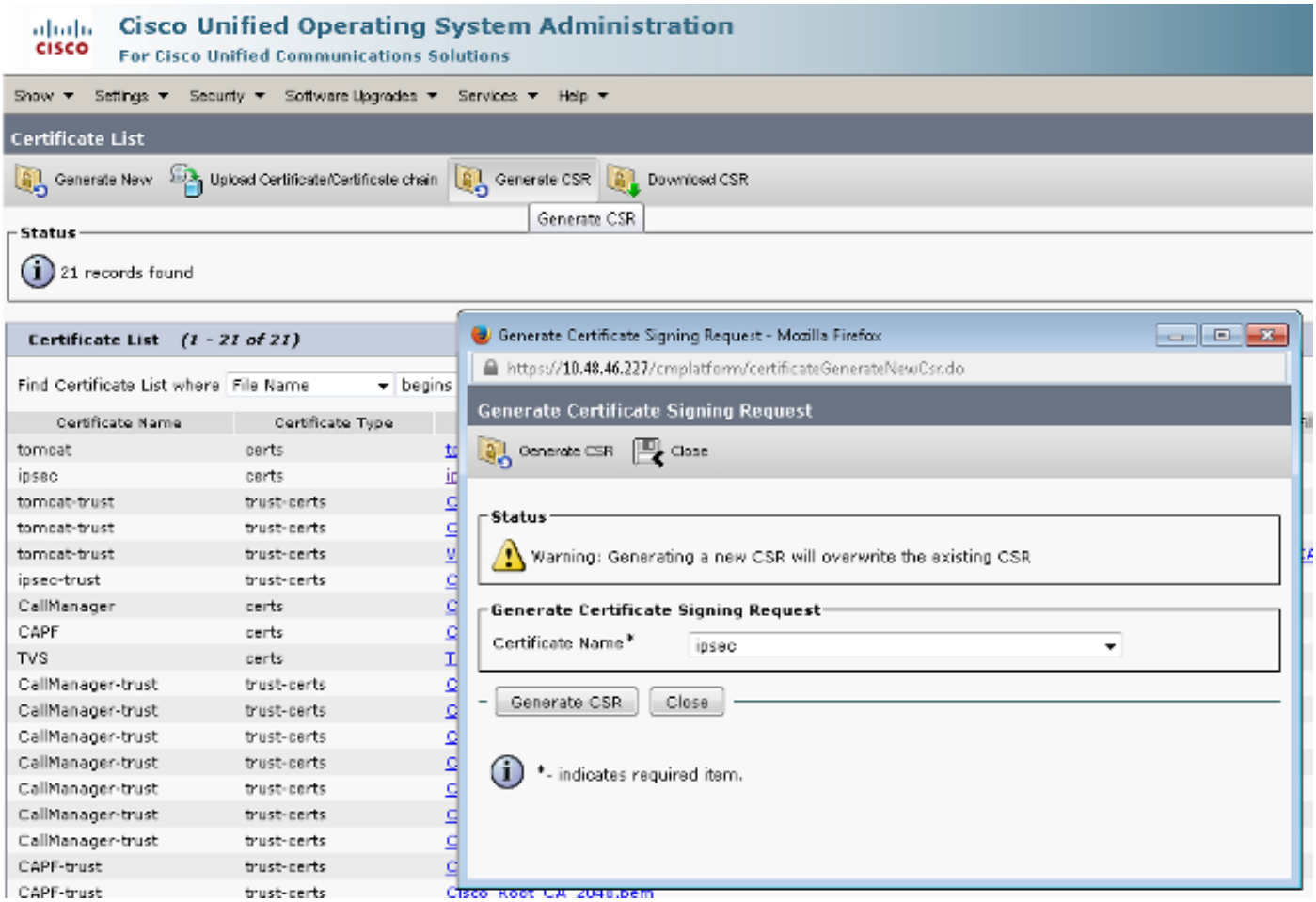
그런 다음 로컬 CA에서 라우터의 인증서를 생성하고 서명합니다.확인을 위해 라우터에 인증서를 나열합니다.

```
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
```

두 개의 인증서가 나열되어야 합니다.첫 번째는 로컬 CA에서 서명한 라우터의 (KRK-UC-2x2811-2) 인증서이고 두 번째는 CA 인증서입니다.

2. CUCM CA 서명 IPsec 인증서 생성

IPsec 터널용 CUCM은 ipsec.pem 인증서를 사용합니다.기본적으로 이 인증서는 시스템이 설치될 때 자체 서명되어 생성됩니다.CA 서명 인증서로 교체하려면 먼저 CUCM OS 관리 페이지에서 IPsec에 대한 CSR(Certificate Sign Request)을 생성해야 합니다.Cisco **Unified OS Administration > Security > Certificate Management > Generate CSR을 선택합니다**.



CSR이 생성된 후에는 CUCM에서 다운로드하여 GW의 CA에 등록해야 합니다.이렇게 하려면 crypto pki **서버 IOS_CA request pkcs10 terminal base64** 명령을 입력하고 서명 요청 해시를 터미널을 통해 붙여넣어야 합니다.부여된 인증서가 표시되고 ipsec.pem 파일로 복사하여 저장해야 합니다.

```
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==
```

참고: Base64로 인코딩된 인증서의 내용을 디코딩하고 확인하려면 openssl **x509 -in certificate.crt -text -noout** 명령을 입력합니다.

부여된 CUCM 인증서는 다음과 같이 디코딩됩니다.

```
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. CUCM에서 CA, CUCM 및 음성 GW CA 인증서 가져오기

CUCM IPsec 인증서가 이미 .pem 파일로 내보내졌습니다.다음 단계로 음성 GW 인증서 및 CA 인증서와 동일한 프로세스를 완료해야 합니다.이렇게 하려면 먼저 crypto pki export local1 pem terminal 명령을 사용하여 터미널에 표시하고 별도의 .pem 파일에 복사해야 합니다.

```
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 인증서가 디코딩됩니다.

```
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
```

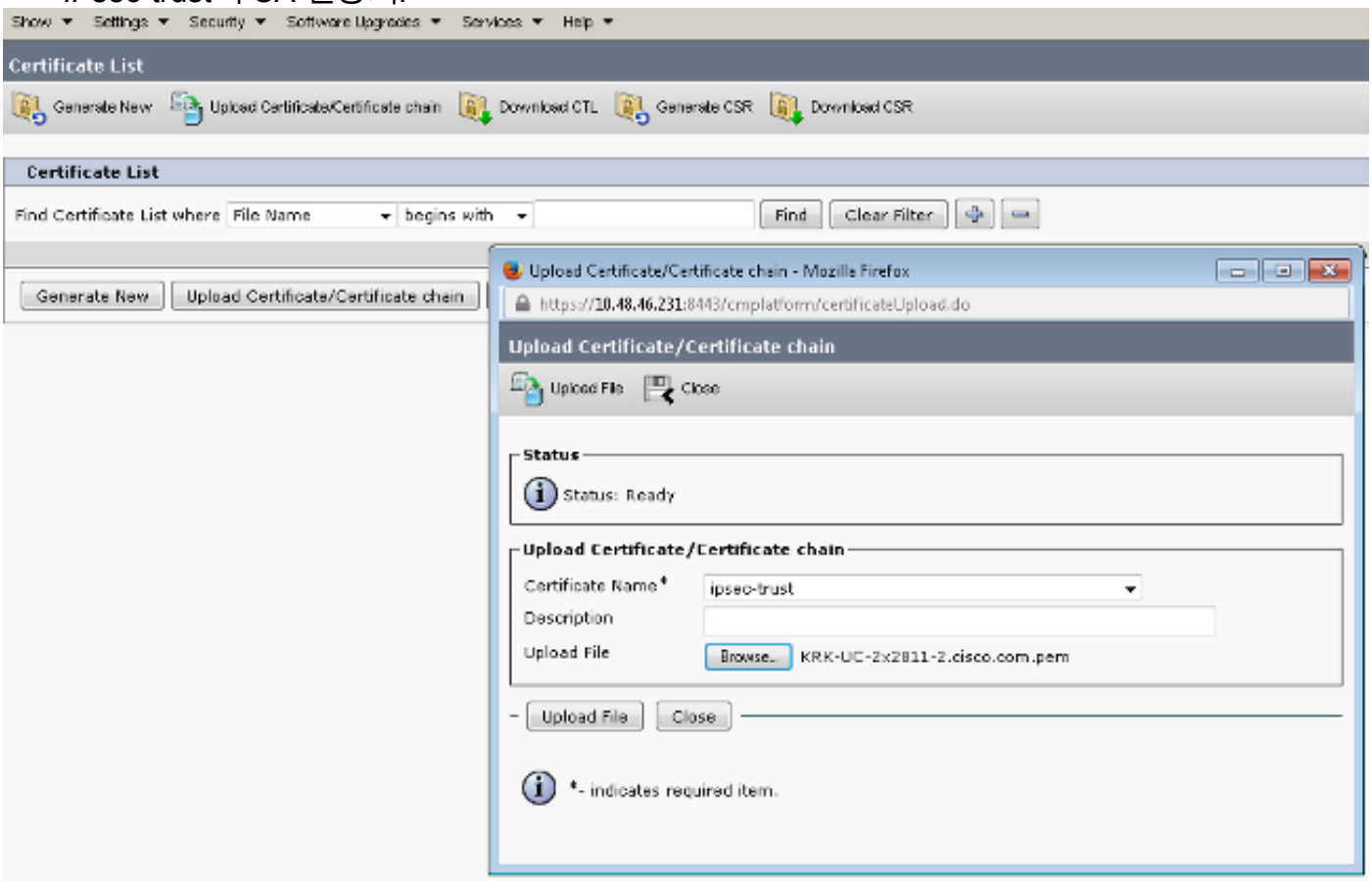
% General Purpose Certificate는 다음 용도로 디코딩됩니다.

```
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
```

.pem 파일로 저장한 후에는 CUCM으로 가져와야 합니다.Cisco **Unified OS Administration > Security > Certificate management > Upload Certificate/Certificate**를 선택합니다.

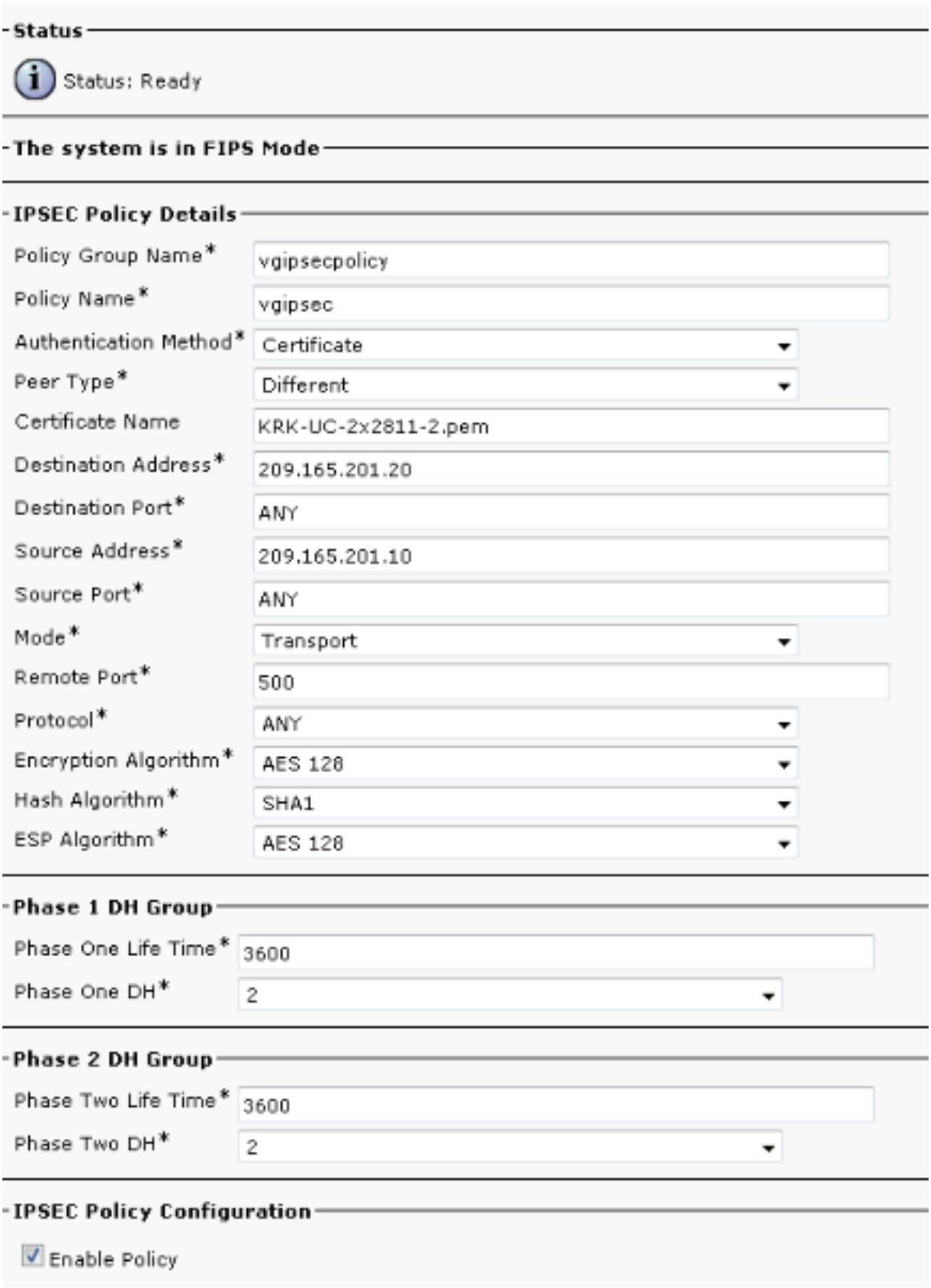
- IPsec으로 CUCM 인증서
- 음성 GW 인증서를 IPsec-trust로 사용
- IPsec-trust의 CA 인증서:



4. CUCM에서 IPsec 터널 설정 구성

다음 단계는 CUCM과 음성 GW 간의 IPsec 터널 컨피그레이션입니다.CUCM의 IPsec 터널 구성은 Cisco Unified OS 관리 웹 페이지(https://<cucm_ip_address>/cmplatform)를 통해 수행됩니다. Security **> IPSEC Configuration > Add new IPsec policy를 선택합니다**.

이 예에서는 인증서 기반 인증으로 "vgipsecpolicy"라는 정책이 생성되었습니다.모든 적절한 정보를 입력하고 음성 GW의 컨피그레이션에 일치해야 합니다.



참고: Certificate Name(인증서 이름) 필드에 음성 게이트웨이 인증서 이름을 지정해야 합니다.

5. 음성 GW에서 IPsec 터널 설정을 구성합니다.

이 예에서는 인라인 코멘트와 함께 음성 GW의 해당 컨피그레이션을 표시합니다.

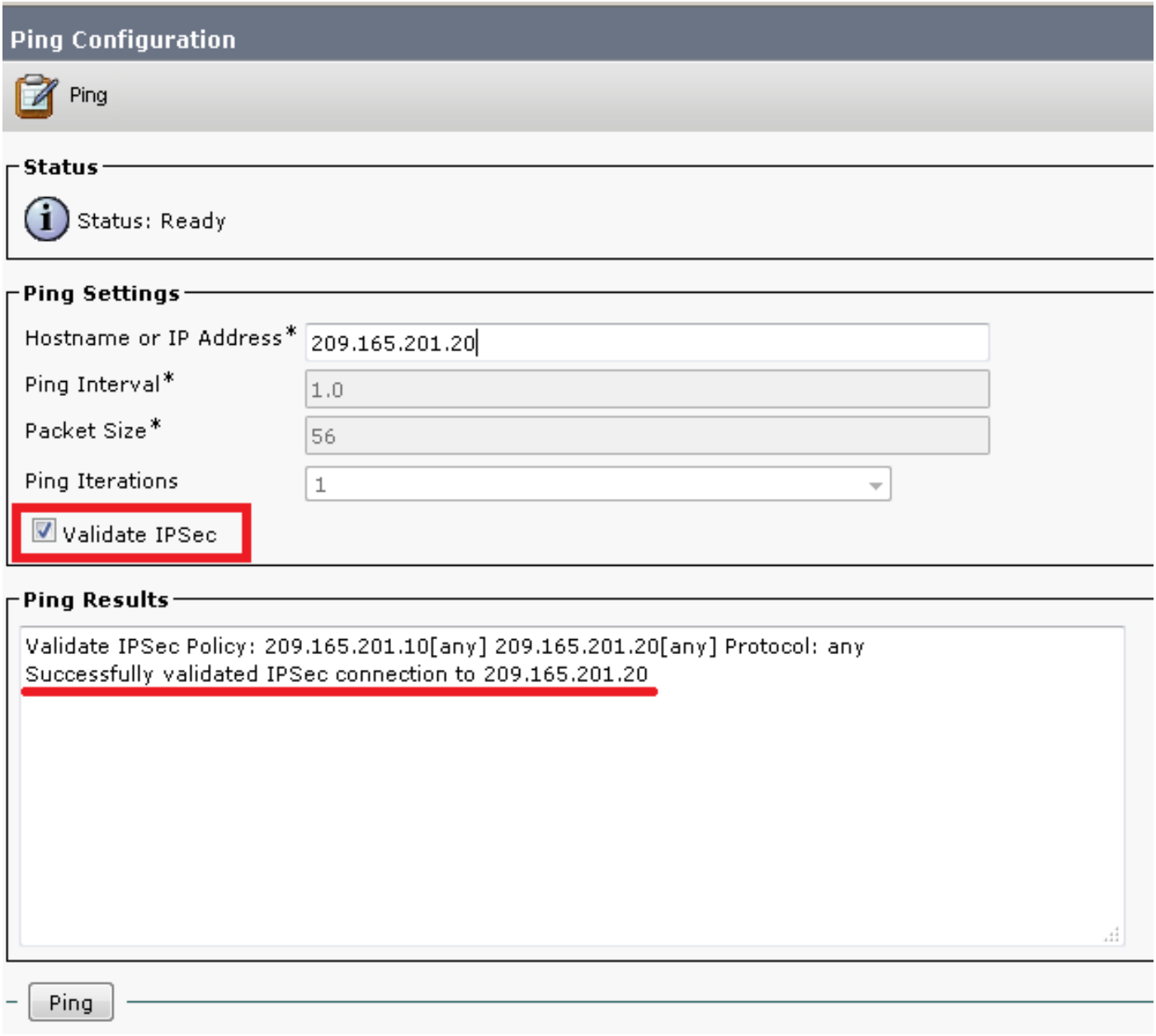
```
crypto isakmp policy 1    (defines an IKE policy and enters the config-iskmp mode)
 encr aes                 (defines the encryption)
 group 2                  (defines 1024-bit Diffie-Hellman)
 lifetime 57600           (isakmp security association lifetime value)

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
```

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

CUCM 끝의 IPsec 터널 상태 확인

CUCM에서 IPsec 터널 상태를 확인하는 가장 빠른 방법은 OS Administration(OS 관리) 페이지로 이동하여 Services(서비스) > Ping(핑)에서 **ping** 옵션을 사용하는 것입니다.Validate IPSec(**IPSec 검증**) 확인란이 선택되었는지 확인합니다.여기에 지정된 IP 주소는 GW의 IP 주소입니다.



참고:CUCM의 ping 기능을 통한 IPsec 터널 검증에 대한 자세한 내용은 다음 Cisco 버그 ID를 참조하십시오.

- Cisco 버그 ID CSCuo53813 - ESP(보안 페이로드 캡슐화) 패킷이 전송될 때 IPSec Ping 결과를 비워 둡니다.
- Cisco 버그 ID CSCud20328 - IPSec 정책 유효성 검사에 FIPS 모드에서 잘못된 오류 메시지가 표시됨

음성 게이트웨이 끝의 IPsec 터널 상태 확인

설정이 제대로 실행되는지 확인하려면 두 레이어(ISAKMP(Internet Security Association) 및 IPsec(Key Management Protocol) 모두에 대한 SA(Security Associations)가 올바르게 생성되었는지 확인해야 합니다.

ISAKMP용 SA가 생성되어 제대로 작동하는지 확인하려면 GW에 **show crypto isakmp sa** 명령을 입력합니다.

```
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
```

참고:SA의 적절한 상태는 ACTIVE 및 QM_IDLE여야 합니다.

두 번째 레이어는 IPsec용 SA입니다.해당 상태는 show crypto ipsec sa 명령으로 **확인할** 수 있습니다.

```
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#
```

참고:인바운드 및 아웃바운드 SPI(Security Policy Indexes)는 상태 ACTIVE에서 생성해야 하며, 캡슐화/역캡슐화 및 암호화/암호 해독된 패킷 수에 대한 카운터는 터널을 통한 트래픽이 생성될 때마다 증가해야 합니다.

마지막 단계는 MGCP GW가 등록된 상태이고 TFTP 컨피그레이션이 CUCM에서 장애 없이 올바르게 다운로드되었는지 확인하는 것입니다.다음 명령의 출력에서 확인할 수 있습니다.

```
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#
```

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

CUCM 끝의 IPsec 터널 문제 해결

CUCM에서는 IPsec 종료 및 관리를 담당하는 서비스 가용성 서비스가 없습니다.CUCM은 운영 체제에 내장된 Red Hat IPsec 툴 패키지를 사용합니다.Red Hat Linux에서 실행되고 IPsec 연결을 종료하는 데몬은 OpenSwan입니다.

CUCM(OS Administration > Security > IPSEC Configuration)에서 IPsec 정책이 활성화되거나 비활성화될 때마다 Openswan 데몬이 다시 시작됩니다.이는 Linux 메시지 로그에서 확인할 수 있습니다.재시작은 다음 행으로 표시됩니다.

```
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
```

CUCM에서 IPsec 연결에 문제가 있을 때마다 Openswan이 작동 및 실행되는지 확인하기 위해 메시지 로그의 마지막 항목을 확인해야 합니다(**file list activelog syslog/messages*** 명령 입력).Openswan이 실행되어 오류 없이 시작되면 IPsec 설정 문제를 해결할 수 있습니다.Openswan에서 IPsec 터널 설정을 담당하는 데몬은 Pluto입니다.명왕성 로그는 Red Hat에서 로그를 보호하기 위해 작성되며 **파일 get activelog syslog/secure.*** 명령 또는 RTMT를 통해 수집할 수 **있습니다.보안 로그**.

> **참고:**RTMT를 통해 로그를 수집하는 방법에 대한 자세한 내용은 RTMT 문서를 참조하십시오.

이러한 로그를 기반으로 문제의 원인을 파악하기 어려운 경우 CUCM의 루트를 통해 TAC(Technical Assistance Center)에서 IPsec을 추가로 확인할 수 있습니다.루트를 통해 CUCM에 액세스하면 다음 명령으로 IPsec 상태에 대한 정보 및 로그를 확인할 수 있습니다.

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

루트를 통해 Red Hat sos 보고서를 생성하는 옵션도 있습니다.이 보고서에는 운영 체제 수준에서 추가 문제를 해결하기 위해 Red Hat 지원에 필요한 모든 정보가 포함되어 있습니다.

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

음성 게이트웨이 끝의 IPsec 터널 문제 해결

이 사이트에서 다음 debug 명령을 활성화한 후 IPsec 터널 설정의 모든 단계를 해결할 수 있습니다.

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

> **참고:**IPsec 트러블슈팅을 위한 자세한 단계는 IPsec 트러블슈팅에서 확인할 수 있습니다.디버그 명령 이해 및 사용.

다음 debug 명령으로 MGCP GW 문제를 해결할 수 있습니다.

```
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
```