基于CA签名证书的语音GW和CUCM之间通过IPsec的安全MGCP通信配置示例

目录

简介

本文档介绍如何根据证书颁发机构(CA)签名的证书，通过互联网协议安全(IPsec)成功保护语音网关(GW)和CUCM（思科统一通信管理器）之间的媒体网关控制协议(MGCP)信令。为了通过MGCP建立安全呼叫，需要单独保护信令和实时传输协议(RTP)流。设置加密RTP流似乎记录得当且非常简单，但安全RTP流不包括安全MGCP信令。如果MGCP信令不安全，则RTP流的加密密钥以明文发送。

先决条件

要求

Cisco 建议您了解以下主题：

- 注册到CUCM的MGCP语音网关，以发送和接收呼叫
- 证书颁发机构代理功能(CAPF)服务已启动，集群设置为混合模式

- GW上的Cisco IOS®映像支持加密安全功能
- 为安全实时传输协议(SRTP)配置的电话和MGCP GW

使用的组件

本文档中的信息基于以下软件和硬件版本：

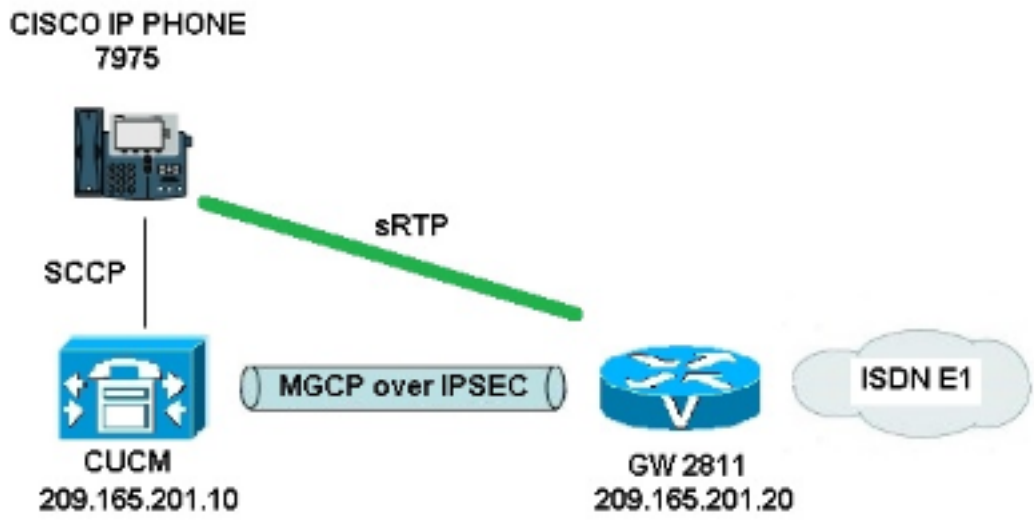
- CUCM — 单节点 — 在联邦信息处理标准(FIPS)模式下运行GGSG（思科全球政府解决方案组）8.6.1.20012-14版
- 7975台运行SCCP75-9-3-1SR2-1S的电话
- GW — 思科2811 - C2800NM-ADVENTERPRISEK9-M，版本15.1(4)M8
- E1 ISDN语音卡 — VWIC2-2MFT-T1/E1 - 2端口RJ-48多路中继

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

注意：使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

网络图



要成功设置CUCM和语音GW之间的IPsec，请完成以下步骤：

1. 在语音GW上配置CA并为语音GW生成CA签名的证书
2. 生成CUCM CA签名的IPsec证书
3. 在CUCM上导入CA、CUCM和语音GW CA证书
4. 在CUCM上配置IPsec隧道设置
5. 在语音GW上配置IPsec隧道设置

1.在语音GW上配置CA并为语音GW生成CA签名证书

第一步，需要在语音GW（Cisco IOS CA服务器）上生成Rivest-Shamir-Addleman(RSA)密钥对：

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

将使用通过简单证书注册协议(SCEP)完成的注册，因此启用HTTP服务器：

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

要在网关上配置CA服务器，需要完成以下步骤：

1. 设置PKI服务器名称。它必须与之前生成的密钥对同名。
   ```
   KRK-UC-2x2811-2(config)#crypto pki server IOS_CA
   ```
2. 指定CA服务器存储所有数据库条目的位置。
   ```
   KRK-UC-2x2811-2(cs-server)#crypto pki server IOS_CA
   ```
3. 配置CA颁发者名称。
   ```
   KRK-UC-2x2811-2(cs-server)#issuer-name cn=IOS
   ```
4. 指定证书服务器颁发的证书中使用的证书撤销列表(CRL)分发点(CDP)，并启用为Cisco IOS从属CA服务器自动授予证书重新注册请求。
   ```
   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. 启用CA服务器。
   ```
   KRK-UC-2x2811-2(cs-server)#no shutdown
   ```

下一步是为CA证书创建信任点，为路由器证书创建本地信任点，其URL注册指向本地HTTP服务器：

```
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
```

要生成由本地CA签名的路由器证书，需要对信任点进行身份验证并注册：

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

之后，路由器的证书由本地CA生成并签名。列出路由器上的证书进行验证。

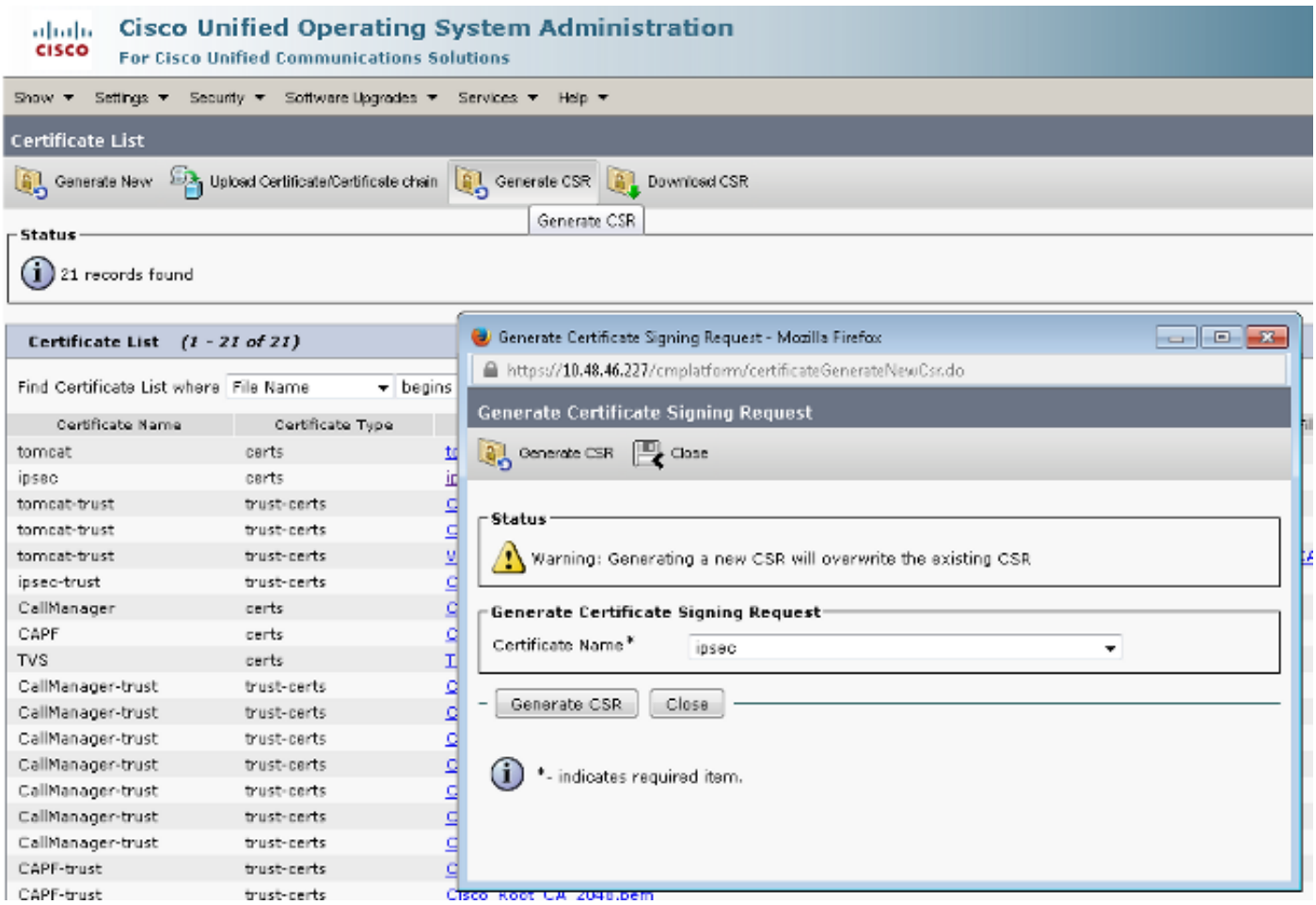
```
KRK-UC-2x2811-2#show crypto ca certificates
Certificate
 Status: Available
 Certificate Serial Number (hex): 02
 Certificate Usage: General Purpose
 Issuer:
   cn=IOS
 Subject:
   Name: KRK-UC-2x2811-2
   cn=KRK-UC-2x2811-2
 CRL Distribution Points:
   http://10.48.46.251/IOS_CA.crl
 Validity Date: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

应列出两个证书。第一个是由本地CA签名的路由器(KRK-UC-2x2811-2)证书，第二个是CA证书。

2.生成CUCM CA签名的IPsec证书

CUCM for IPsec隧道设置使用ipsec.pem证书。默认情况下，此证书是自签名证书，在安装系统时生成。要将其替换为CA签名的证书，首先需要从CUCM OS Admin页面生成IPsec的CSR（证书签名请求）。选择**Cisco Unified OS Administration > Security > Certificate Management > Generate CSR**。



在生成CSR后，需要从CUCM下载CSR，并在GW上根据CA注册。为此，请输入**crypto pki server IOS_CA request pkcs10 terminal base64**命令，并且需要通过终端粘贴签名请求哈希。系统将显示已授予的证书，并需要将其复制并保存为ipsec.pem文件。

```
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+Ilj13D9eG/xxWCBXK7Fy0RJ6Z8yFR+8QzbTc1T2eh3thMTNDO4B
p2M1zJzhvW73W9Cbk5VQ1fE4Oi97v86VA1RZTctISvRoj2ULvnHep1EYF7w/CeT+
BZtPkHunC7AxdNTz5QWPr6W+tAxFvjt3DbbIWZIw5u97PXwhUTEDIWzk6P0CP+s0
Uh1RAi34235D5/fzAgMBAAGjgaowgacwLwYDVR0fBCgwJjAkoCKgIIYeaHR0cDov
LzEwLjQ4LjQ2LjI1MS9JT1NfQ0EuY3JsMAsGA1UdDwQEAwIDuDANBgNVHSUEIDAe
BggrBgEFBQcDAQYIKwYBBQUHAwIGCCsGAQUFBwMFMB8GA1UdIwQYMBaAFJSLP5cn
PL8bIP7VSKLtB6Z1socOMB0GA1UdDgQWBBR4m2eTSyELsdRBW4MRmbNdT2qppTAN
BgkqhkiG9w0BAQQFAAOBgQBuVJ+tVS0JqP4z9TgEeuMbVwn00CTKXz/fCuh6R/50
qq8JhERJGiR/ZHvHRLf+XawhnoE6daPAmE+WkIPtHIIhbMHCbbxG9ffdyaiNXRWy
5sI5XycF1FgYGpTFBYD9M0Lqsw+FIYaT2ZrbOGsx8h6pZoesKqm85RByIUjX4nJK
1g==
```

注意：要解码和检查Base64编码证书的内容，请输入**openssl x509 -in certificate.crt -text -noout**命令。

授予的CUCM证书解码为：

```
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上导入CA、CUCM和语音GW CA证书

CUCM IPsec证书已导出到.pem文件。下一步，需要使用语音GW证书和CA证书完成相同的流程。为此，需要首先在终端上使用**crypto pki export local1 pem terminal**命令显示它们，并将其复制到单独的.pem文件。

```
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证书解码为：

```
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:
```

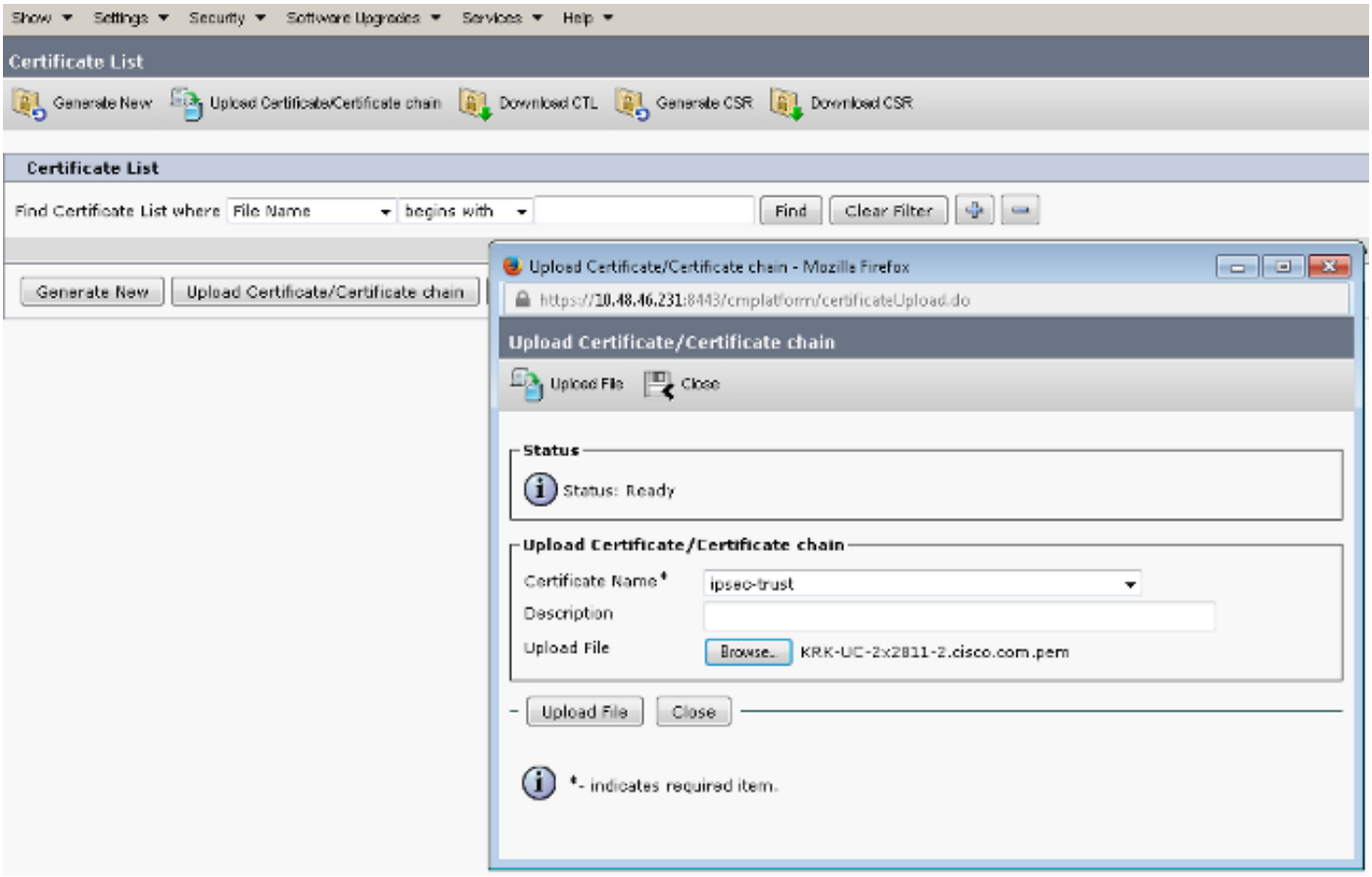
```
        96:62:10:ae:ae:18:9f:a9:35:8b:c4:c3:17:8f:48:f2:9b:6e:
        03:a2:a6:7d:d5:a0:cd:1b:55:70:88:9f:d8:bf:88:b8:d2:df:
        74:cb:ae:56:cd:b6:a9:64:bd:52:eb:9a:be:77:b0:42:2d:0c:
        a9:76:bc:1c:2a:47:52:d1:d7:d3:74:a7:d7:12:cc:96:2e:17:
        9c:45:af:26:9d:97:24:a6:02:81:93:c2:2b:05:f3:3d:2b:e7: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

%通用证书解码为：

```
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
```

将它们另存为.pem文件后，需要将其导入CUCM。选择**Cisco Unified OS Administration > Security > Certificate management > Upload Certificate/Certificate**。

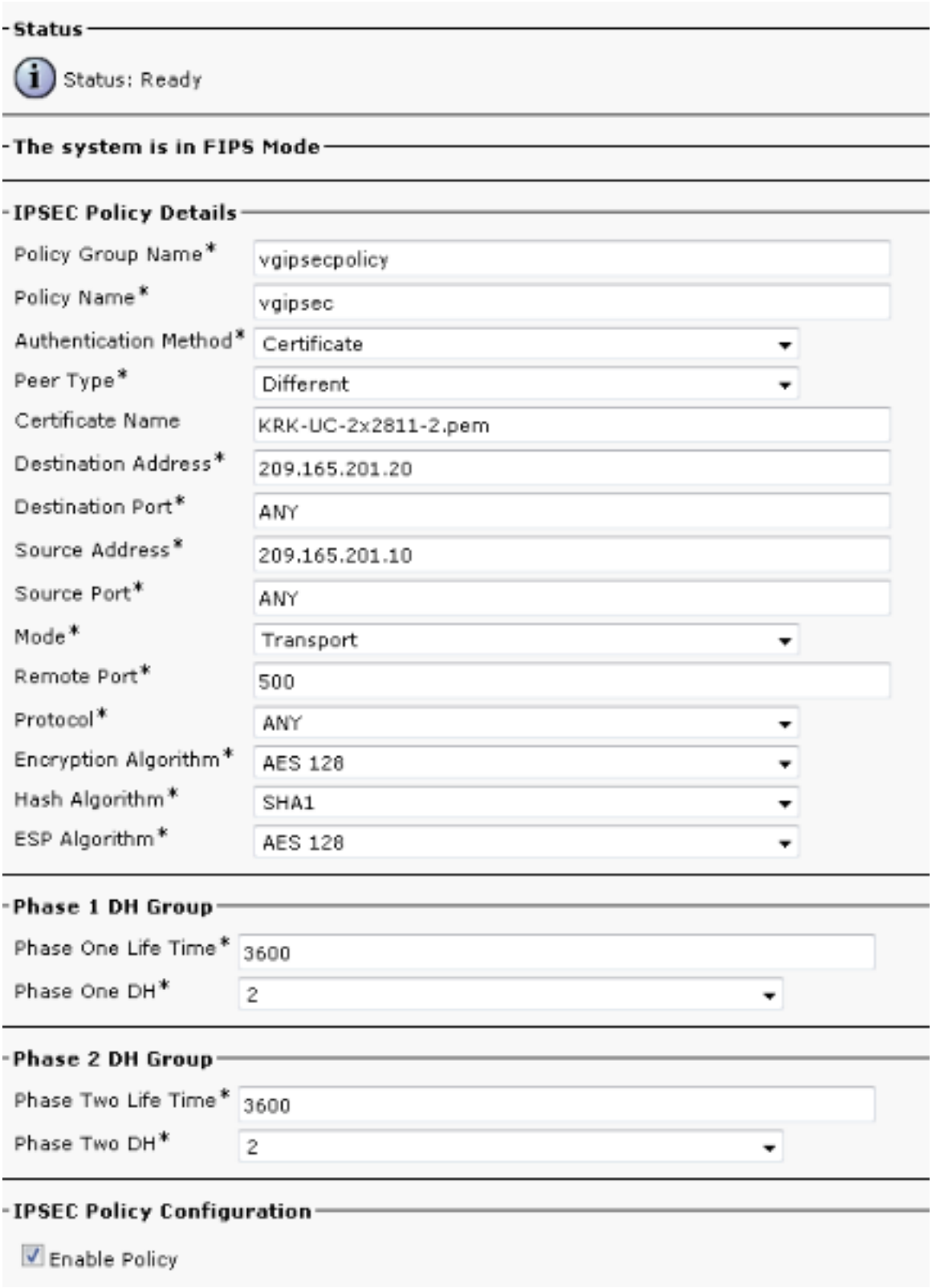
- CUCM证书作为IPsec
- 语音GW证书作为IPsec-trust
- CA证书作为IPsec-trust:



4.在CUCM上配置IPsec隧道设置

下一步是配置CUCM和语音GW之间的IPsec隧道。CUCM上的IPsec隧道配置通过Cisco Unified OS Administration网页(https://<cucm_ip_address>/cmplatform)执行。 选择**Security > IPSEC Configuration > Add new IPsec policy**。

在本示例中，创建了名为“vgipsecpolicy”的策略，该策略基于证书进行身份验证。所有适当的信息都需要填写，并与语音GW上的配置相对应。



注意：语音网关证书名称需要在Certificate Name字段中指定。

5.在语音GW上配置IPsec隧道设置

本示例使用内联注释显示语音GW上的相应配置。

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

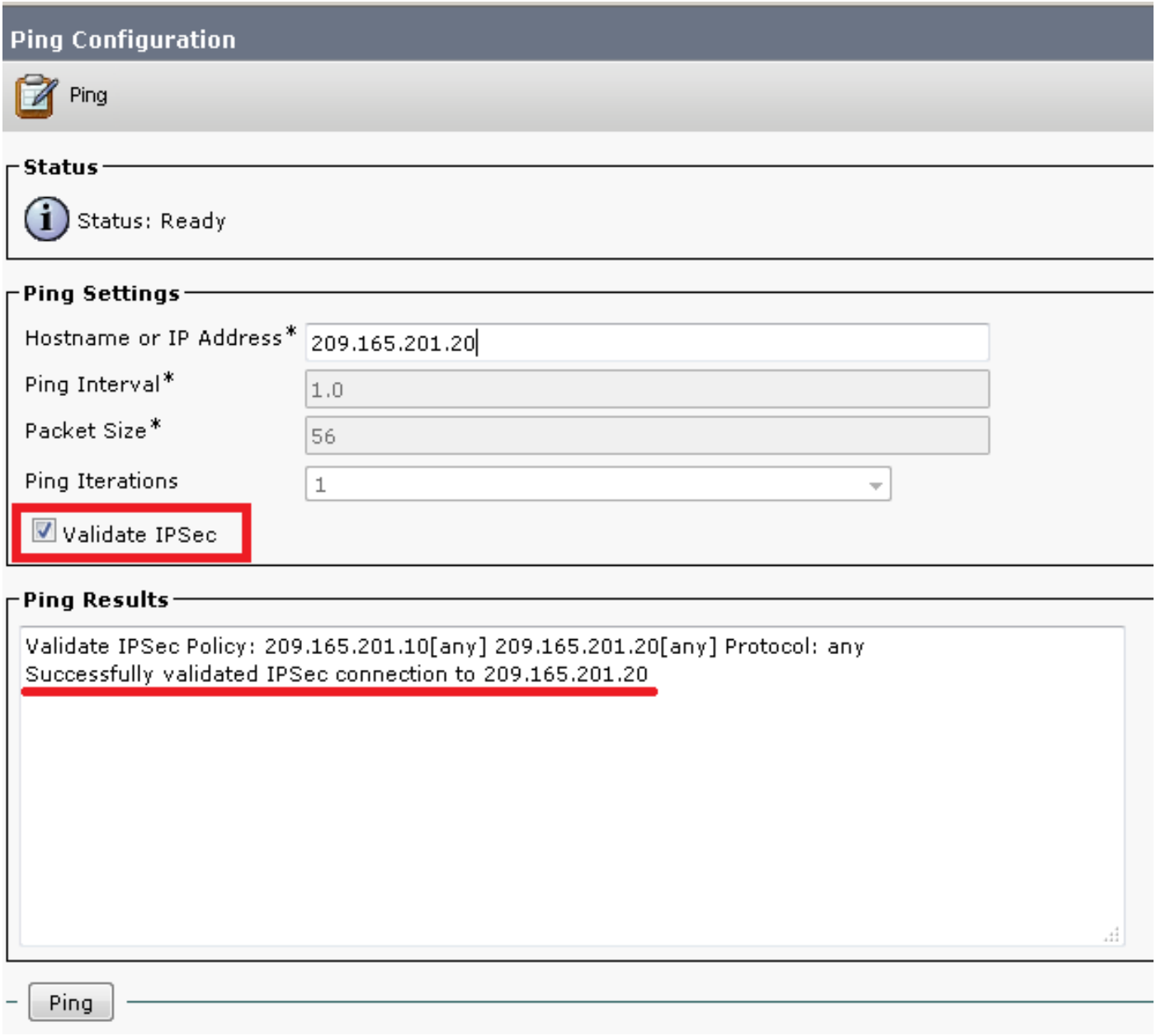
```
 encr aes                  (defines the encryption)
 group 2                   (defines 1024-bit Diffie-Hellman)
 lifetime 57600            (isakmp security association lifetime value)

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
```

验证

使用本部分可确认配置能否正常运行。

验证CUCM端的IPsec隧道状态

在CUCM上验证IPsec隧道状态的最快方法是转至OS Administration页面，然后使用Services > Ping下的**ping**选项。确保选**中验**证IPSec复选框。显然，此处指定的IP地址是GW的IP地址。



注意：有关通过CUCM上的ping功能验证IPsec隧道的信息，请参阅以下Cisco Bug ID:

- Cisco Bug ID CSCuo53813 — 发送ESP（封装安全负载）数据包时验证IPSec Ping结果为空
- Cisco Bug ID CSCud20328 — 验证IPSec策略在FIPS模式下显示错误错误消息

验证语音网关端的IPsec隧道状态

为了验证设置是否运行正常，需要确认两层(互联网安全关联和密钥管理协议(ISAKMP)和IPsec)的安全关联(SA)已正确创建。

要检查ISAKMP的SA是否已创建且工作正常，请在GW上输入**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
```

注意：SA的正确状态应为ACTIVE和QM_IDLE。

第二层是IPsec的SA。它们的状态可以使用show crypto ipsec **sa命令进行**验证。

```
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#
```

注意：入站和出站安全策略索引(SPI)应以ACTIVE状态创建，并且每次通过隧道生成任何流量时，封装/解封和加密/解密的数据包数的计数器应会增加。

最后一步是确认MGCP GW处于注册状态，并且TFTP配置已从CUCM正确下载，且没有任何故障。这可以从以下命令的输出中确认：

```
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#
```

故障排除

本部分提供了可用于对配置进行故障排除的信息。

排除CUCM端的IPsec隧道故障

在CUCM上，没有可维护性服务负责IPsec终止和管理。CUCM使用内置到操作系统的Red Hat IPsec工具包。在Red Hat Linux上运行并终止IPsec连接的守护程序是OpenSwan。

每次在CUCM(OS Administration > Security > IPSEC Configuration)上启用或禁用IPsec策略时，Openswan守护程序都会重新启动。这可在Linux消息日志中观察到。以下行表示重新启动：

```
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
```

每当CUCM上的IPsec连接出现问题时，应检查消息日志中的最后一个条目(输入**file list activelog syslog/messages***命令)以确认Openswan已启动并运行。如果Openswan运行并启动时没有错误，您可以排除IPsec设置故障。负责在Openswan中设置IPsec隧道的守护程序是Pluto。编写Pluto日志是为了保护Red Hat上的日志，可以通过文件get activelog syslog/secure.***命令或通过RTMT收集这些日志：安全日志**。

注意：有关如何通过RTMT收集日志的详细信息，请参阅RTMT文档。

如果根据这些日志难以确定问题的根源，则技术支持中心(TAC)可通过CUCM的根网桥进一步验证IPsec。通过根访问CUCM后，可以使用以下命令检查有关IPsec状态的信息和日志：

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

还可以选择通过根生成Red Hat存储报告。此报告包含Red Hat支持所需的所有信息，以便对操作系统级别的进一步问题进行故障排除：

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

排除语音网关端的IPsec隧道故障

在此站点上，启用以下debug命令后，可以排除IPsec隧道设置的所有阶段故障：

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

注意：IPsec故障排除中提供了排除IPsec故障的详细步骤：了解和使用debug命令。

您可以使用以下debug命令排除MGCP GW问题：

```
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
```