IPsec による音声 GW および CUCM 間の保護された MGCP コミュニケーションは CA 署名入り認証 設定例に基づいていました

目次

概要

このドキュメントでは、認証局（CA ）署名付き証明書に基づき、IPSec（Internet Protocol Security）を介して、音声ゲートウェイ（GW）と CUCM（Cisco Unified Communications Manager）間の Media Gateway Control Protocol（MGCP）シグナリングを正しく保護する方法を説明します。 MGCP を介して保護されたコールを設定するには、シグナリングのストリームと Real-time Transport Protocol（RTP）のストリームを個別に保護する必要があります。 暗号化された RTP ストリームを設定する手法がよく説明されているため単純であるように思えるかもしれませんが、セキュアな RTP ストリームには、セキュアな MGCP シグナリングが含まれません。 MGCP シグナリングがセキュアでない場合、RTP ストリームの暗号化キーがクリア テキストで送信されます。

前提条件

要件

次の項目に関する知識が推奨されます。

- コールを送受信するために CUCM に登録されている MGCP 音声ゲートウェイ
- 認証局プロキシ機能（CAPF）の開始済みサービス、および混合モードに設定されたクラスタ
- 暗号化セキュリティ機能をサポートするゲートウェイに関する Cisco IOS® のイメージ
- Secure Real-Time Transport Protocol（SRTP）用に設定された電話および MGCP ゲートウェイ

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

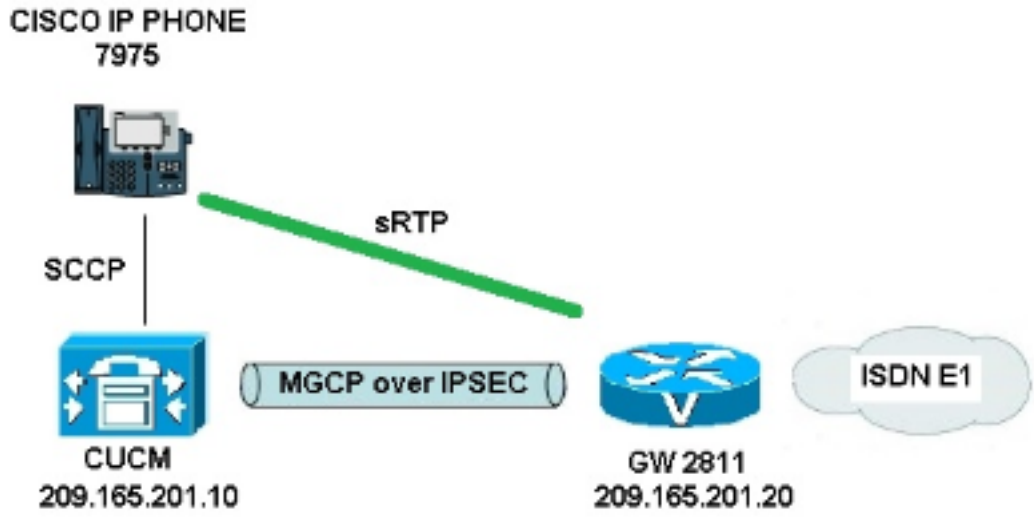
- CUCM（単一ノード）：連邦情報処理標準（FIPS）モードで GGSG（シスコ グローバル ガバメント ソリューション グループ）8.6.1.20012-14 を実行する CUCM
- SCCP75-9-3-1SR2-1S を実行する 7975 電話
- GW - Cisco 2811：C2800NM-ADVENTERPRISEK9-M、バージョン 15.1(4)M8
- E1 ISDN 音声カード（VWIC2-2MFT-T1/E1）：2 ポート RJ-48 マルチフレックス トランク

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

設定

> **注:** このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

ネットワーク図



CUCM および音声ゲートウェイ間で IPSec を正しく設定するには、次の手順を実行します。

1. 音声ゲートウェイ上に CA を設定し、音声ゲートウェイ用 CA 署名付き証明書を生成する
2. CUCM CA 署名付き IPSec 証明書を生成する
3. CUCM で CA、CUCM、音声ゲートウェイ CA 証明書をインポートする
4. CUCM で IPsec トンネル設定を設定する
5. 音声ゲートウェイで IPsec トンネル設定を設定する

1. 音声ゲートウェイの CA を設定し、音声ゲートウェイ用 CA 署名付き証明書を生成する

最初のステップとして、音声ゲートウェイ（Cisco IOS CA サーバ）に Rivest-Shamir-Addleman（RSA）キー ペアを生成する必要があります。

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

Simple Certificate Enrollment Protocol（SCEP）によって実行された登録が使用されるため、HTTP サーバをイネーブルにします。

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

ゲートウェイに CA サーバを設定するには、次の手順を実行する必要があります。

1. PKI サーバ名を設定します。 これは、先ほどの手順でキー ペアが生成したのと同一の名前である必要があります。
   ```
   KRK-UC-2x2811-2(config)#crypto pki server IOS_CA
   ```
2. CA サーバのすべてのデータベース エントリが保存される場所を指定します。
   ```
   KRK-UC-2x2811-2(cs-server)#crypto pki server IOS_CA
   ```
3. CA 発行者名を設定します。
   ```
   KRK-UC-2x2811-2(cs-server)#issuer-name cn=IOS
   ```
4. 証明書サーバが発行する証明書に使用される証明書失効リスト（CRL）分散ポイント（CDP）を指定し、Cisco IOS 下位 CA サーバに対して証明再登録要求の自動付与をイネーブルにします。
   ```
   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 サーバをイネーブルにします。
   ```
   KRK-UC-2x2811-2(cs-server)#no shutdown
   ```

次に、CA 証明書のトラストポイントと、ルータ証明書のローカル トラストポイントを作成し、ローカル HTTP サーバを指す URL を登録します。

```
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
```

ローカル CA によって署名されたルータの証明書を生成するには、トラストポイントの認証と登録が必要です。

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

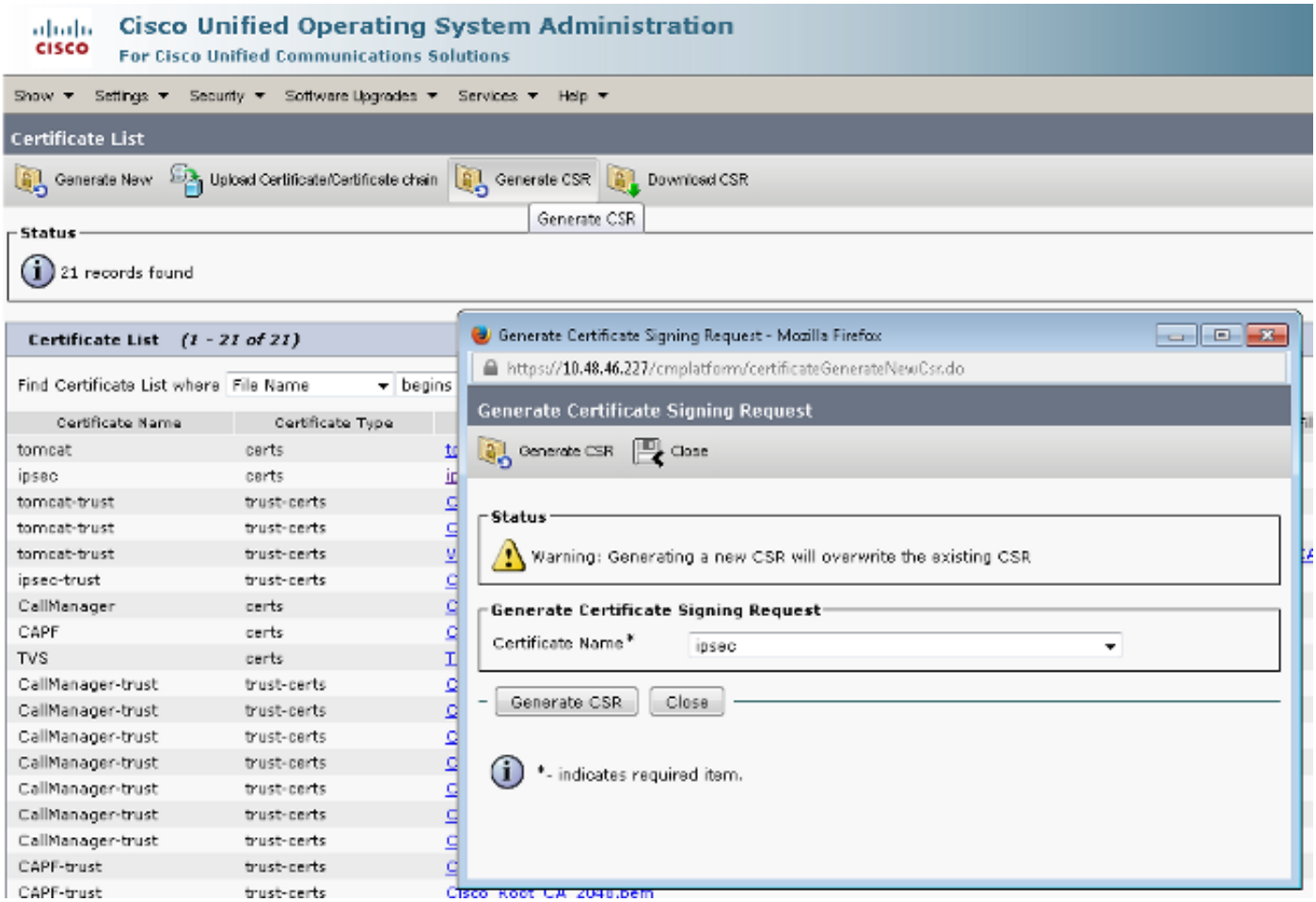
その後、ルータの証明書が口ーカル CA によって生成され、署名されます。確認のためにルータの証明書を一覧表示します。

```
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
```

2 つの証明書が一覧表示されます。 最初のものは口ーカル CA によって署名されたルータ（KRK-UC-2x2811-2）の証明書で、もう 1 つは CA 証明書です。

2. CUCM CA 署名付き IPSec 証明書の生成

IPSec トンネル セットアップ用の CUCM は ipsec.pem 証明書を使用します。 デフォルトでは、この証明書は自己署名型の証明書で、システムのインストール時に生成されます。 これを CA 署名付き証明書と交換するには、まず、CUCM の OS 管理ページから IPSec 用の証明書署名要求（CSR）を生成する必要があります。 [CiscoUnified OS Administration] > [Security] > [Certificate Management] > [Generate CSR] の順に選択します。



CSR は、生成した後で CUCM からダウンロードし、GW の CA に対して登録する必要があります。 そのために、**crypto pki server IOS_CA request pkcs10 terminal base64** コマンドを入力し、署名要求ハッシュを端末から貼り付ける必要があります。 付与された証明書を表示し、コピーして、ipsec.pem ファイルとして保存する必要があります。

```
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==
```

注: Base64 で暗号化された証明書の内容を複合化して確認するには、**openssl x509 -in certificate.crt -text -noout** コマンドを入力します。

付与された CUCM 証明書は次のように複合化されます。

```
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. CUCM での CA、CUCM、音声ゲートウェイ CA 証明書のインポート

CUCM IPsec 証明書はすでに .pem ファイルにエクスポートされています。 次のステップとして、音声ゲートウェイ証明書と CA 証明書についても同じ手順を実行する必要があります。 そのためには、まず **crypto pki export local1 pem terminal** コマンドを使用してそれらを端末に表示し、別個の .pem ファイルにコピーする必要があります。

```
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 証明書は次のように複合化されます。

```
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
```

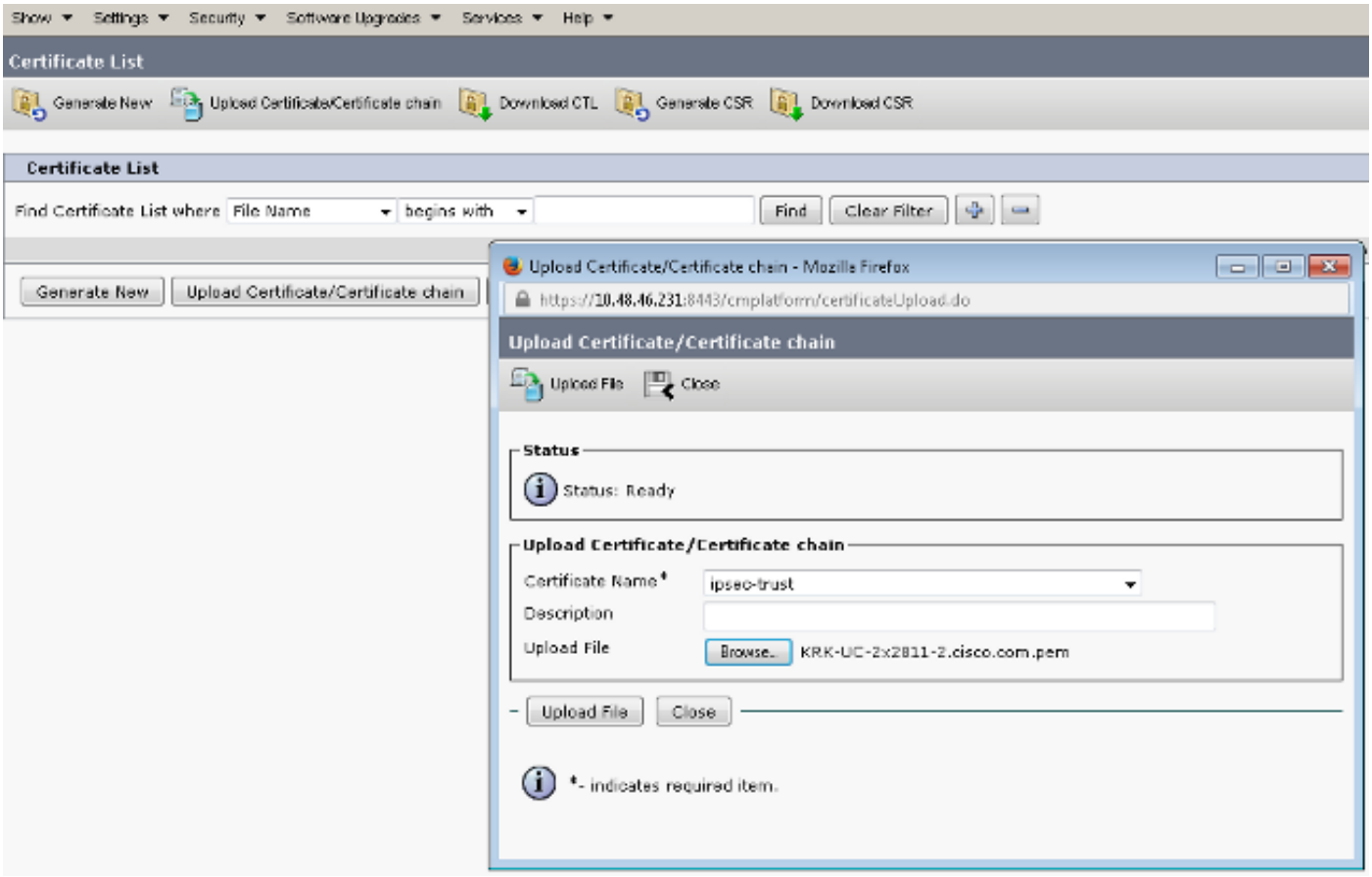
```
TSS1ExbM9i2D4HOWYhCurhifqTWLxMMXj0jym24DoqZ91aDNG1VwiJ/Yv4i40t90
y65WzbapZL1S65q+d7BCLQypdrwcKkdS0dfTdKfXEsyWLhecRa8mnZckpgKBk8Ir
BfM9K+caXkfhPEPa644UzV9++OKMKhtDuQ==
-----END CERTIFICATE-----

% 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-----
```

% 汎用証明書は次のように複合化されます。

```
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-----
```

.pem ファイルとしてこれらを保存した後、CUCM にインポートする必要があります。 [Cisco Unified OS Administration] > [Security] > [Certificate management] > [Upload Certificate/Certificate] の順に選択します。

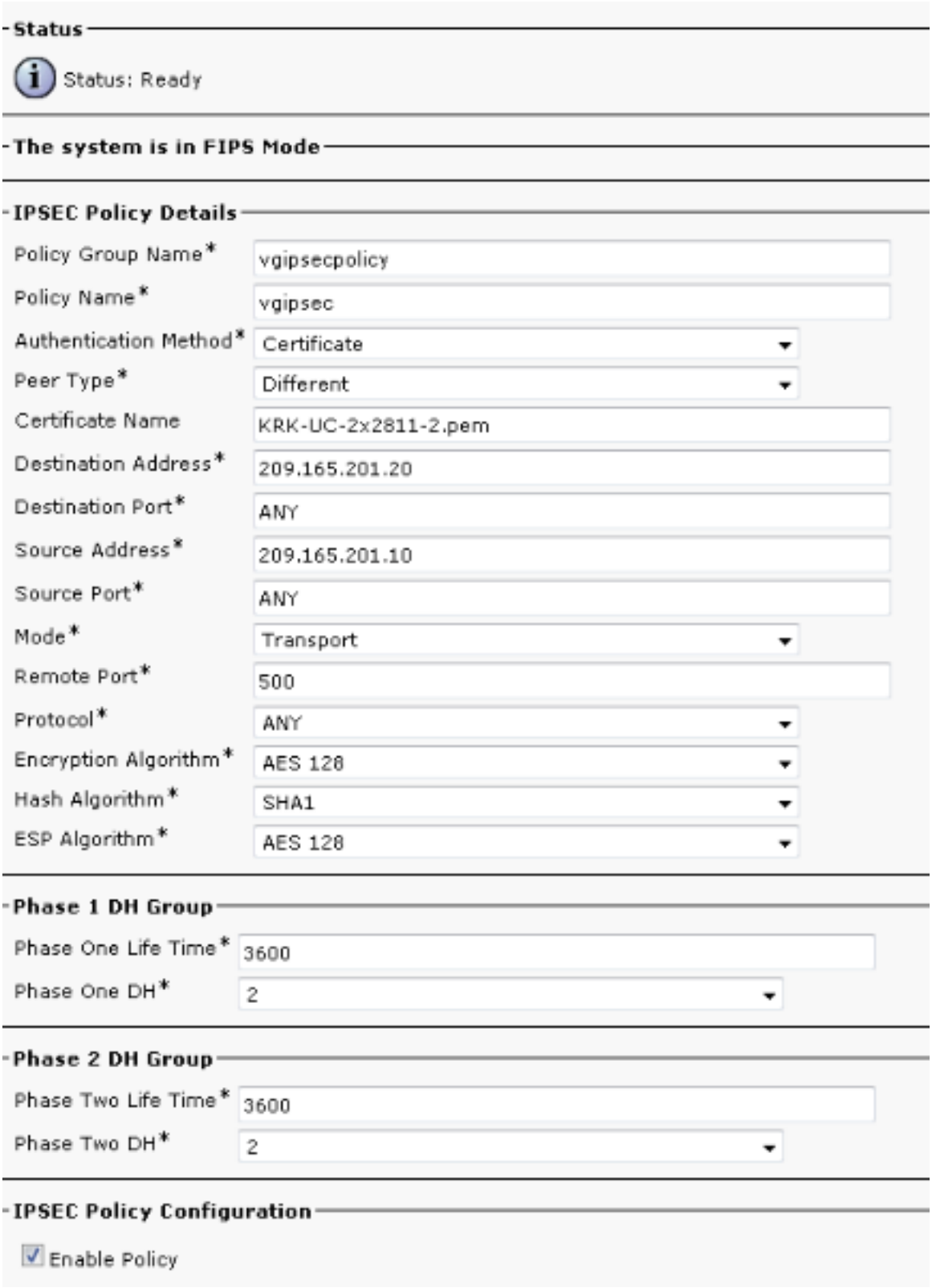
- CUCM 証明書を IPsec として
- 音声ゲートウェイ証明書を IPsec-trust として
- CA 証明書を IPsec-trust として



4. CUCM での IPsec トンネル設定の設定

次に、CUCM と音声ゲートウェイとの間に IPSec トンネルを設定します。 CUCM の IPsec トンネル設定は、Cisco Unified OS の管理 Web ページ（ https://<cucm_ip_address>/cmplatform ）で行われます。 [Security] > [IPSEC Configuration] > [Add new IPsec policy] の順に選択します。

この例では、「vgipsecpolicy」という名前のポリシーが作成され、証明書に基づいて認証が設定されています。 必要な情報をすべて入力する必要があります。これらの情報は、音声ゲートウェイの設定に対応している必要があります。



注: 音声ゲートウェイの証明書名を [Certificate Name] フィールドで指定する必要があります。

5. 音声ゲートウェイでの IPsec トンネル設定の設定

この例では、インライン コメントを使用して、音声ゲートウェイ上の対応する設定を示しています。

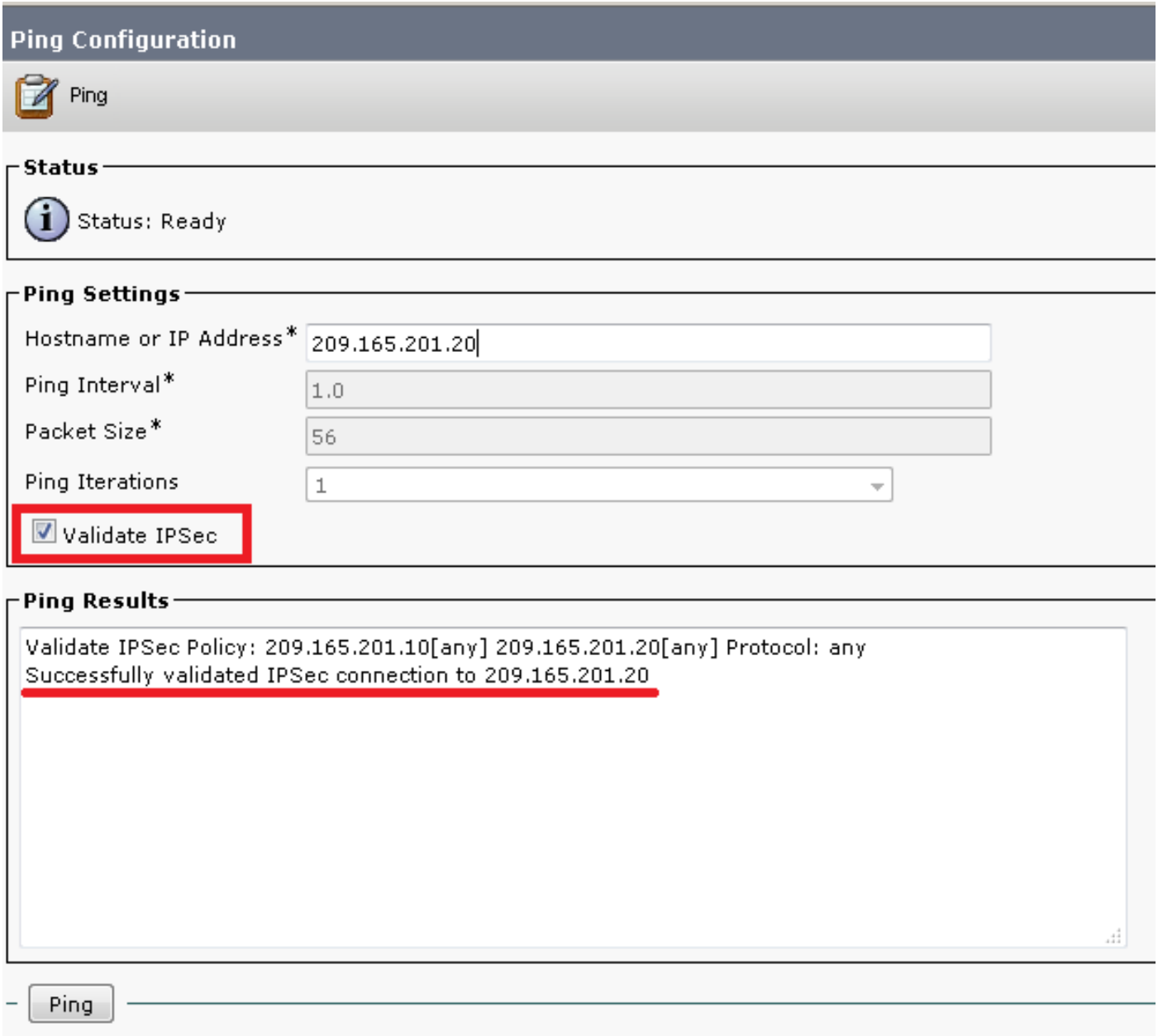
```
crypto isakmp policy 1    (defines an IKE policy and enters the config-iskmp mode)
 encr aes                 (defines the encryption)
 group 2                  (defines 1024-bit Diffie-Hellman)
 lifetime 57600           (isakmp security association lifetime value)

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
```

確認

このセクションでは、設定が正常に機能していることを確認します。

CUCM 側の IPsec トンネル ステータスの確認

CUCM の IPsec トンネルのステータスを最も迅速に確認する方法は、[OS Administration] ページに移動し、[Services] > [Ping] の順に移動して、ping オプションを使用することです。 [Validate IPSec] チェックボックスがオンになっていることを確認します。 当然、ここで指定されている IP アドレスはゲートウェイの IP アドレスです。



注: CUCM で ping 機能を使用して IPsec トンネルを検証する方法については、次の Cisco Bug ID を参照してください。

- Cisco Bug ID CSCuo53813：ESP（セキュリティ ペイロードのカプセル化）パケットが送信されるとき、Validate IPSec Ping を実行した結果が空白になる
- Cisco Bug ID CSCud20328：Validate IPSec Policy で FIPS モードの誤ったエラー メッセージが表示される

音声ゲートウェイ側の IPsec トンネル ステータスの確認

セットアップが正しく実行されるかどうかを確認するには、両方のレイヤ（Internet Security Association and Key Management Protoco（ISAKMP）および IPsec）のセキュリティ アソシエーション（SA）が正しく作成されていることを確認する必要があります。

ISAKMP の SA が作成され、正しく動作することを確認するには、ゲートウェイで **show crypto isakmp sa** コマンドを入力します。

```
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: SA の適切なステータスは「ACTIVE」および「QM_IDLE」です。

2 番目の層は、IPSec の SA です。 そのステータスは、**show crypto ipsec sa** コマンドで確認できます。

```
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: インバウンドおよびアウトバウンドのセキュリティ ポリシー インデックス (SPI) は、ステータスが「ACTIVE」の時に作成する必要があります。また、カプセル化およびカプセル化解除されたパケット数、および暗号化および復号化されたパケット数は、トンネル経由のトラフィックが生成されるたびに増加します。

最後に、MGCP ゲートウェイが登録済みの状態であり、TFTP 設定が CUCM から問題なく正常にダウンロードされたことを確認します。 これは、次のコマンドの出力で確認できます。

```
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#
```

トラブルシューティング

このセクションでは、設定のトラブルシューティングに役立つ情報を提供します。

CUCM 側の IPsec トンネルのトラブルシューティング

CUCM 側については、IPSec の終了と管理に関する有用性サービスはありません。 CUCM は、オペレーティング システムに組み込まれている Red Hat IPsec ツールのパッケージを使用します。 Red Hat Linux で動作し、IPSec 接続を終了するデーモンは、OpenSwan です。

CUCM 上で IPsec ポリシーを有効または無効にするたびに（[OS Administration] > [Security] > [IPSEC Configuration]）、Openswan デーモンが再起動します。 この情報は Linux メッセージ ログで確認できます。 再起動は次の行で示されます。

```
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#
```

CUCM の IPSec 接続に問題があるたびに、Openswan が稼働することを確認するために、メッセージ ログの最後のエントリを確認する必要があります（**file list activelog syslog/messages*** コマンドを入力）。 Openswan がエラーなしで動作し開始される場合、IPsec 設定をトラブルシューティングできます。 Openswan の IPsec トンネルのセットアップに関するデーモンは Pluto です。 Pluto のログは、Red Hat のログを保護する目的で記述されており、**file get activelog syslog/secure? コマンドか、RTMT: Security Logs** を使用して収集できます。

注: RTMT を使用してログを収集する方法の詳細については、『RTMT documentation』に記載されています。

これらのログに基づいて問題の原因を判別することは困難ですが、IPSec は CUCM のルートから、テクニカル アシスタンス センター（TAC）でさらに検証できます。 ルートから CUCM にアクセスした後、次のコマンドを使用して、IPsec のステータスに関する情報およびログを確認できます。

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

また、ルートから Red Hat の sosreport を生成することもできます。 このレポートには、オペレーティング システム レベルの問題のトラブルシューティングで Red Hat サポートが必要とするすべての情報が含まれます。

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

音声ゲートウェイ側の IPsec トンネルのトラブルシューティング

このサイトから、次の debug コマンドを有効にした後、IPSec トンネル セットアップのすべてのフェーズをトラブルシューティングできます。

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

注: IPSec のトラブルシューティング手順の詳細は、『IPSec のトラブルシューティング：debug コマンドの説明と使用』に記載されています。

次の debug コマンドを使用して、MGCP ゲートウェイの問題をトラブルシューティングできます。

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