

Konfigurationsbeispiel für die sichere MGCP-Kommunikation zwischen Sprach-GW und CUCM über IPsec auf Basis von CA Signed Certificates

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfiguration](#)

[Netzwerkdigramm](#)

[1. Konfigurieren der CA auf dem Sprach-GW und Generieren eines Zertifikats mit CA-Signierung für Sprach-GW](#)

[2. Generieren eines IPsec-Zertifikats mit CUCM-CA-Vorzeichen](#)

[3. CA-, CUCM- und Sprach-GW-Zertifizierungsstellen-Zertifikate auf CUCM importieren](#)

[4. Konfigurieren der IPsec-Tunneleinstellungen auf CUCM](#)

[5. Konfigurieren der IPsec-Tunneleinstellung auf dem Sprach-GW](#)

[Überprüfung](#)

[Überprüfen des IPsec-Tunnelstatus am CUCM-Ende](#)

[Überprüfen Sie den IPsec-Tunnelstatus am Voice Gateway-Ende.](#)

[Fehlerbehebung](#)

[Fehlerbehebung für den IPsec-Tunnel am CUCM-Ende](#)

[Fehlerbehebung beim IPsec-Tunnel am Voice Gateway-Ende](#)

Einführung

In diesem Dokument wird beschrieben, wie die MGCP-Signalisierung (Media Gateway Control Protocol) zwischen einem Sprach-Gateway (GW) und dem CUCM (Cisco Unified Communications Manager) mithilfe von IPsec (Internet Protocol Security), basierend auf Zertifikaten der Zertifizierungsstelle (Certificate Authority, CA), erfolgreich gesichert wird. Um einen sicheren Anruf über MGCP einzurichten, müssen Signalisierungs- und RTP-Streams (Real-time Transport Protocol) separat gesichert werden. Es scheint gut dokumentiert zu sein und ist relativ einfach, verschlüsselte RTP-Streams einzurichten. Ein sicherer RTP-Stream beinhaltet jedoch keine sichere MGCP-Signalisierung. Wenn die MGCP-Signalisierung nicht gesichert ist, werden die Verschlüsselungsschlüssel für den RTP-Stream unverschlüsselt gesendet.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- MGCP-Voice-Gateway für CUCM registriert, um Anrufe zu senden und zu empfangen
- CAPF-Dienst (Certificate Authority Proxy Function) gestartet, Cluster auf den gemischten Modus festgelegt.
- Cisco IOS[®] Image auf GW unterstützt Verschlüsselungssicherheitsfunktionen
- Telefone und MGCP-GW für Secure Real-Time Transport Protocol (SRTP) konfiguriert

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

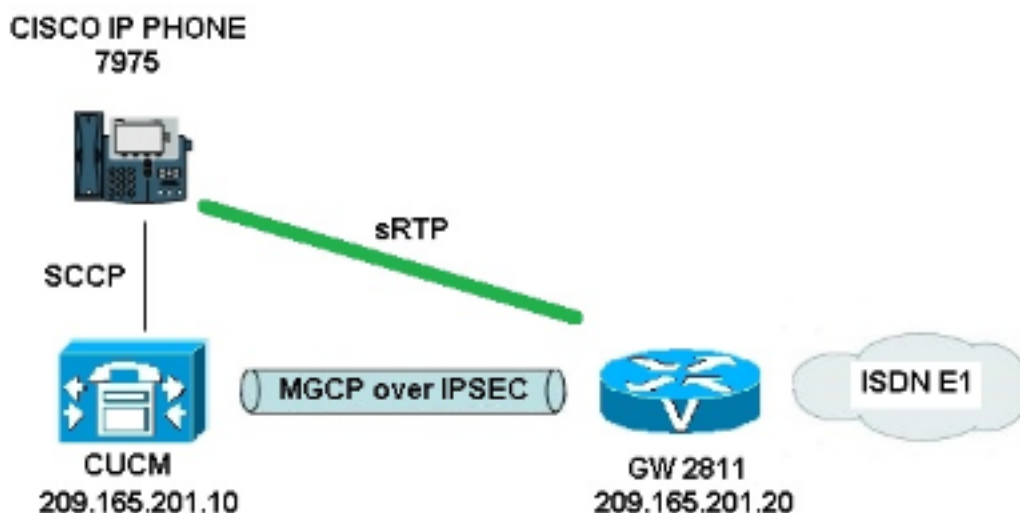
- CUCM - ein Knoten - führt GGSG (Cisco Global Government Solutions Group) Version 8.6.1.2012-14 im FIPS-Modus (Federal Information Processing Standard) aus
- 7975 Telefone mit SCCP75-9-3-1SR2-1S
- GW - Cisco 2811 - C2800NM-ADVENTERPRISEK9-M, Version 15.1(4)M8
- E1 ISDN-Sprachkarte - VWIC2-2MFT-T1/E1 - 2-Port RJ-48 Multiflex-Trunk

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Konfiguration

Hinweis: Verwenden Sie das [Command Lookup Tool](#) (nur [registrierte](#) Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm



Gehen Sie wie folgt vor, um IPsec zwischen CUCM und Sprach-GW erfolgreich einzurichten:

1. Konfigurieren der CA auf dem Sprach-GW und Generieren eines Zertifikats mit CA-Signierung für Sprach-GW
2. Generieren eines IPsec-Zertifikats mit CUCM-CA-Vorzeichen
3. CA-, CUCM- und Sprach-GW CA-Zertifikate auf CUCM importieren
4. Konfigurieren der IPsec-Tunneleinstellungen auf CUCM
5. Konfigurieren der IPsec-Tunneleinstellung auf dem Sprach-GW

1. Konfigurieren der CA auf dem Sprach-GW und Generieren eines Zertifikats mit CA-Signierung für Sprach-GW

In einem ersten Schritt muss das Rivest-Shamir-Addleman (RSA)-Schlüsselpaar auf dem Sprach-GW (Cisco IOS CA-Server) generiert werden:

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

Die über das Simple Certificate Enrollment Protocol (SCEP) abgeschlossenen Anmeldungen werden verwendet. Aktivieren Sie daher den HTTP-Server:

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

Um den CA Server auf einem Gateway zu konfigurieren, müssen die folgenden Schritte ausgeführt werden:

1. Legen Sie den PKI-Servernamen fest. Der Name muss mit dem zuvor generierten Schlüsselpaar übereinstimmen.

```
KRK-UC-2x2811-2(config)#crypto pki server IOS_CA
```
2. Geben Sie den Speicherort an, an dem alle Datenbankeinträge für den CA-Server gespeichert werden.

```
KRK-UC-2x2811-2(cs-server)#crypto pki server IOS_CA
```
3. Konfigurieren Sie den Namen des CA-Emittenten.

```
KRK-UC-2x2811-2(cs-server)#issuer-name cn=IOS
```
4. Geben Sie einen CRL-Verteilungspunkt (Certificate Revocation List) für Zertifikate an, der in Zertifikaten verwendet wird, die vom Zertifikatsserver ausgestellt werden, und ermöglichen Sie die automatische Erteilung von Zertifikatswiedereinschreibung-Anträgen für einen untergeordneten CA-Server von Cisco IOS.

```
KRK-UC-2x2811-2(cs-server)#cdp-url http://209.165.201.10/IOS_CA.crl
```

```
KRK-UC-2x2811-2(cs-server)#grant auto
```
5. Aktivieren Sie den CA-Server.

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

Im nächsten Schritt werden ein Vertrauenspunkt für das CA-Zertifikat und ein lokaler Vertrauenspunkt für das Router-Zertifikat mit einer URL-Registrierung erstellt, die auf einen lokalen HTTP-Server zeigt:

```
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)#rsa keypair 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
```

Um das von der lokalen Zertifizierungsstelle signierte Zertifikat des Routers zu generieren, muss der Vertrauenspunkt authentifiziert und registriert werden:

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

Danach wird das Zertifikat des Routers erstellt und von der lokalen Zertifizierungsstelle signiert. Listen Sie das Zertifikat auf dem Router zur Überprüfung auf.

```
KRK-UC-2x2811-2#show crypto ca certificates
```

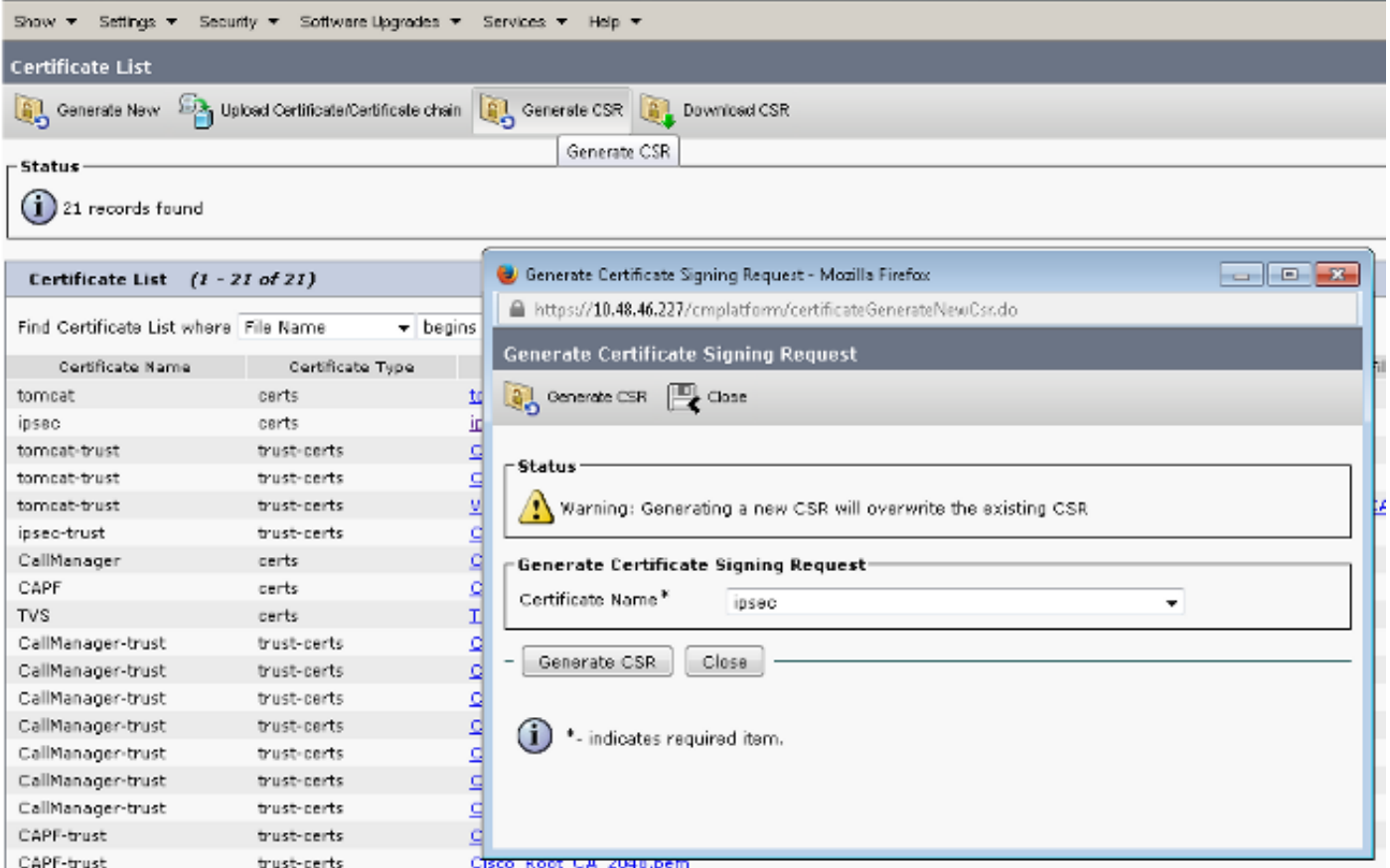
```
Certificate
Status: Available
Certificate Serial Number (hex): 02
Certificate Usage: General Purpose
Issuer:
  cn=IOS
Subject:
  Name: KRK-UC-2x2811-2
  cn=KRK-UC-2x2811-2
CRL Distribution Points:
  http://10.48.46.251/IOS_CA.crl
Validity Date:
  start date: 13:05:01 CET Nov 21 2014
  end   date: 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
```

Es sollten zwei Zertifikate aufgeführt werden. Das erste ist ein Router-Zertifikat (KRK-UC-2x2811-2), das von der lokalen Zertifizierungsstelle signiert wird, und das zweite Zertifikat ist das Zertifizierungsstellenzertifikat.

2. Generieren eines IPsec-Zertifikats mit CUCM-CA-Vorzeichen

Die Einrichtung des CUCM für IPsec-Tunnels verwendet ein ipsec.pem-Zertifikat. Dieses Zertifikat wird standardmäßig selbst signiert und bei der Installation des Systems generiert. Um es durch ein Zertifikat mit CA-Vorzeichen zu ersetzen, muss zunächst ein CSR (Certificate Sign Request) für IPsec von der CUCM-OS-Admin-Seite generiert werden. Wählen Sie **Cisco Unified OS Administration > Security > Certificate Management > Generate CSR** aus.



Nachdem der CSR generiert wurde, muss er vom CUCM heruntergeladen und für die CA auf dem GW registriert werden. Geben Sie dazu den Befehl **crypto pki server IOS_CA request pkcs10 terminal base64** ein, und der Hash für die Zeichenanforderung muss über Terminal eingefügt werden. Das erteilte Zertifikat wird angezeigt und muss als ipsec.pem-Datei kopiert und gespeichert werden.

```
CRK-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-----
MIIDNjCCA4CAQAwgaxkCzAJBgNVBAYTAlBMMQ4wDAYDVQQIEwVjaXNjbzEOMAwG
A1UEBxMFY2l2Y28xODJAMBgNVBAoTBWVnc2NvMjNvMjNvMjNvMjNvMjNvMjNvMjNv
A1UEAxMGMGQ1VDTUIxMkxwY28xODJAMBgNVBAYTAlBMMQ4wDAYDVQQIEwVjaXNjbzE
NjcwMDBmMGI2NjliYjYkYjYwZmVudVQwFE0A1NjY2OWY5Mjg5Mjg5Mjg5Mjg5Mjg5
NjcwMDBmMGI2NjliYjYkYjYwZmVudVQwFE0A1NjY2OWY5Mjg5Mjg5Mjg5Mjg5Mjg5
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAKfHxvcov4vFmK+3+dQShW3s3SszAYBQ19
0JDBiic4eDRmdrq0V2dKn9UpLUx90H7V0Oe/8wmHqYwoxFZ5a6B5qRRkc010/ub2
ul1QCw+nQ6QizGdNhdne0NYY4r3odF4CkrtYAJA4PUScelTwxfiJY5dw/Xhv8cVg
gVyxctESemfMhUfvEM203NU9nod7YTEzQzuAadjNcyc4blu91vQm5OVUNXxODov
e7/0lQNUWU3LSEr0aI9lC75x3qRgBe8Pwnk/gWbT5B7pwuwMXTU8+UFj6+1vrQM
Rb47dw22yFmSMObvez18IVExAyFs50j9Aj/rNFidUQIt+Nt+Q+f38wIDAQABoEcw
RQYJKoZIhvcNAQkOMTgwNjAnBgNVHSUEIDAEBggrBgEFBQcDAQYIKwYBBQUHAWIG
CCsGAQUFBwMFMAsGA1UdDwQEAwIDuANBgkqhkiG9w0BAQUFAAOCAQEADgAR40l
oQ4z2yqgSsICAZ2hQA3Vztp6aOI+0PSyMfihGS//3V3tALEZL2+t0Y5elKsBea72
sieKjpSikXjNaj+Siy1aYy4siVw5EKQD3Ii4Qv115BvuniZXvBiBQuW+SpBLbeNi
xwIgrYELrFywQZBeZodFqnSKN9XlisXe6oU9GXux7uwgXwkCXMF/azutbiol4Fgf
qUF00GzkhTEapJA6c5RzaxG/0uDuKY+4z1eSSsXzFhBTifk3RfJA+I7Na1zQBIEJ
2IOJdiZnn0HWVr5C5eZ7VnQuNdiC/qn3uUfvNVRZo8iCDq3tRv7dr/n64jdKsHEM
lk6P8gp9993cJw==
quit
```

% Granted certificate:

```
MIIDXTCCAsagAwIBAgIBBTANBgkqhkiG9w0BAQQFADAOMQwwCgYDVQQDEwNJT1Mw
HhcNMUwMTA4MTIwMTAwWhcNMUwMTA4MTIwMTAwWjCBqTELMAkGALUEBhMCUEwx
DjAMBgNVBAgTBWNpc2NvMQ4wDAYDVQQHEwVjaXNjbzEOMAwGA1UEChMFY21zY28x
DjAMBgNVBAStBWNpc2NvMQ8wDQYDVQQDEwZDVUNNQjExSTBHbgNVBAUTQDU2NjY5
ZjkyODMlZmZlZDUwODRlMjkxNTg2NzAwMGYwYjY2OWJiN2RhZmE0M2YzZDM5YWE0
ZDEzMzVlOWUyNTMwgGEMAA0GCSqSIB3DQEBAQUAA4IBDwAwggEKAoIBAQC8fG9
yi/i8WYr7f51BKFbezdLMBgFDX3QkMGihzh4NGZ2urRXZ2Sf1SktTH04ftXQ57/z
CYepjCjEVnlroHmpFGRw7XT+5va6XVALD6dDpCJkZ02F2d7Q1hjiveh0XgKSu1gA
kDg9RjX7W1bF+Iljl3D9eG/xxWCBXK7Fy0RJ6Z8yFR+8QzbTc1T2eh3thMTND04B
p2M1zJzhvW73W9CbK5VQ1fE40i97v86VA1RZTctISvRoj2ULvnHep1EYF7w/CeT+
BZtPkHunC7AxdNTz5QWPr6W+tAxFvjt3DbbIWZlw5u97PXwhUTEDIWzk6P0CP+s0
Uh1RAi34235D5/fzAgMBAAGjgaowgacwLwYDVR0fBCgwJjAkoCKgIIYeaHR0cDov
LzEwLjQ4LjQ2LjI1MS9JT1NfQ0EuY3JsMAsGALUdDwQEAwIDuDanBgNVHSUEIDAe
BggrBgEFBQcDAQYIKwYBBQUHAWIGCCsGAQUFBwMFMB8GA1UdIwQYMBaAFJSLP5cn
PL8bIP7VSKLtB6Z1socOMB0GA1UdDgQWBRR4m2eTSyELsdRBW4MRmbNdT2qppTAN
BgkqhkiG9w0BAQQFAA0BgQBvVJ+tVS0JqP4z9TgEeuMbVwn00CTKXz/fCuh6R/50
qq8JhERJGiR/ZHvHRLf+XawhnoE6daPAme+WkIPtHIhbMHCbbxG9ffdyaiNXRWy
5sI5XycF1FgYGpTFBYD9M0Lqsw+FIYaT2ZrbOGsx8h6pZoesKqm85RByIUjX4nJK
lg==
```

Hinweis: Um den Inhalt des Base64-kodierten Zertifikats zu dekodieren und zu überprüfen, geben Sie den Befehl **openssl x509 -in certificate.crt -text -noout** ein.

Das erteilte CUCM-Zertifikat decodiert an:

```
Certificate:
Data:
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. CA-, CUCM- und Sprach-GW-Zertifizierungsstellen-Zertifikate auf CUCM importieren

Das CUCM-IPsec-Zertifikat wird bereits in eine .pem-Datei exportiert. Im nächsten Schritt muss derselbe Prozess mit dem Sprach-GW-Zertifikat und dem Zertifizierungsstellenzertifikat abgeschlossen werden. Dazu müssen sie zuerst in einem Terminal mit dem Befehl **crypto pki local1 pem terminal** angezeigt und in separate .pem-Dateien kopiert werden.

```
KRK-UC-2x2811-2(config)#crypto pki export local1 pem terminal
% CA certificate:
-----BEGIN CERTIFICATE-----
MIIB9TCCA6AwIBAgIBATANBgkqhkiG9w0BAQQFADAOMQwwCgYDVQQDEwNJT1Mw
HhcNMTQxMTE1MTEyWWhcNMTQxMTE1MTEyWjAOMQwwCgYDVQQDEwNJT1Mw
gZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAK6Cd2yxUywtbgBELkZUSP6eaZVv
6YfpEbFptyt6ptRdpxgjoYI3InEP3ewwtmEPNeTJL8+a/WMDUemm3t/NlWBO6T2
m9Bp6k0FNOBXMKeDfTSqOKey7WfLASE/Pbq8M+JMpeMWz8xnMboYOb66rY8igZFz
k1tRPlIMSf5r01tnAgMBAAGjYzBhMA8GA1UdEwEB/wQFMAMBAf8wDgYDVDR0PAQH/
BAQDAGGMB8GA1UdIwQYMBAAwFJSLP5cnPL8bIP7VSKLtB6Z1socOMB0GA1UdDgQW
BBSUiz+XJzy/GyD+1Uii7QemdbKHDjANBgkqhkiG9w0BAQQFAA0BgQCUMC1SFV1S
TSS1Exbm9i2D4HOWYhCurhifqTWLxMMXj0jym24DoqZ91aDNG1VwiJ/Yv4i40t90
y65WzbapZL1S65q+d7BCLQypdrwcKkdS0dfTdKfXESyWLheCRa8mnZckpgKBk8Ir
Bfm9K+caXkfhPEPa644UzV9++OKMKhtDuQ==
-----END CERTIFICATE-----

% General Purpose Certificate:
-----BEGIN CERTIFICATE-----
MIIB2zCCAUSgAwIBAgIBAJANBgkqhkiG9w0BAQUFADAOMQwwCgYDVQQDEwNJT1Mw
HhcNMTQxMTE1MTEyWWhcNMTQxMTE1MTEyWjAAMRgwFgYDVQQDEw9LUkst
VUMtMngyODEXLTlWXdANBgkqhkiG9w0BAQEFAANLADBIAGkEApGWINlnAAtKLVMoj
mZVkQFgI8LrHD6zSrlaKGAJhlu+H/mnRQQ5rqiTipekDdPoowST9RxC5CJmB4spT
VWkYkwIDAQABo4GAMH4wLwYDVROfBCgwJjAkoCKgIIYeHR0cDovLzEwLjQ4LjQ2
LjI1MS9JT1NfQ0EuY3JSMASgALUdDwQEAWIFoDAfBgNVHSMEGDAWgBSUiz+XJzy/
GyD+1Uii7QemdbKHDjAdBgNVHQ4EFgQUtAWc61K5nYGgWqKaiIOLMlphfqIwDQYJ
KoZIhvcNAQEFBQADgYEAjdFlh+N3yc3RykCig9B0aAIXWZPmaqLF9v9R75zc+f8x
zbSIzoVbBhnUOeuOj1hnIghyMjeELjTEh6uQrWUN2ElW1ypfmxk1jN5q0t+vfdr
+yepS04pFor9RoD7IWg6e/1hFDEep9hBvzrVwQHCjzeY0rVrPcLl26k5oauMwTs=
```

-----END CERTIFICATE-----

Das Zertifikat % CA decodiert an:

Certificate:

Data:

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

Das %-Zertifikat für allgemeine Zweckbestimmung dekodiert:

Certificate:

Data:

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:

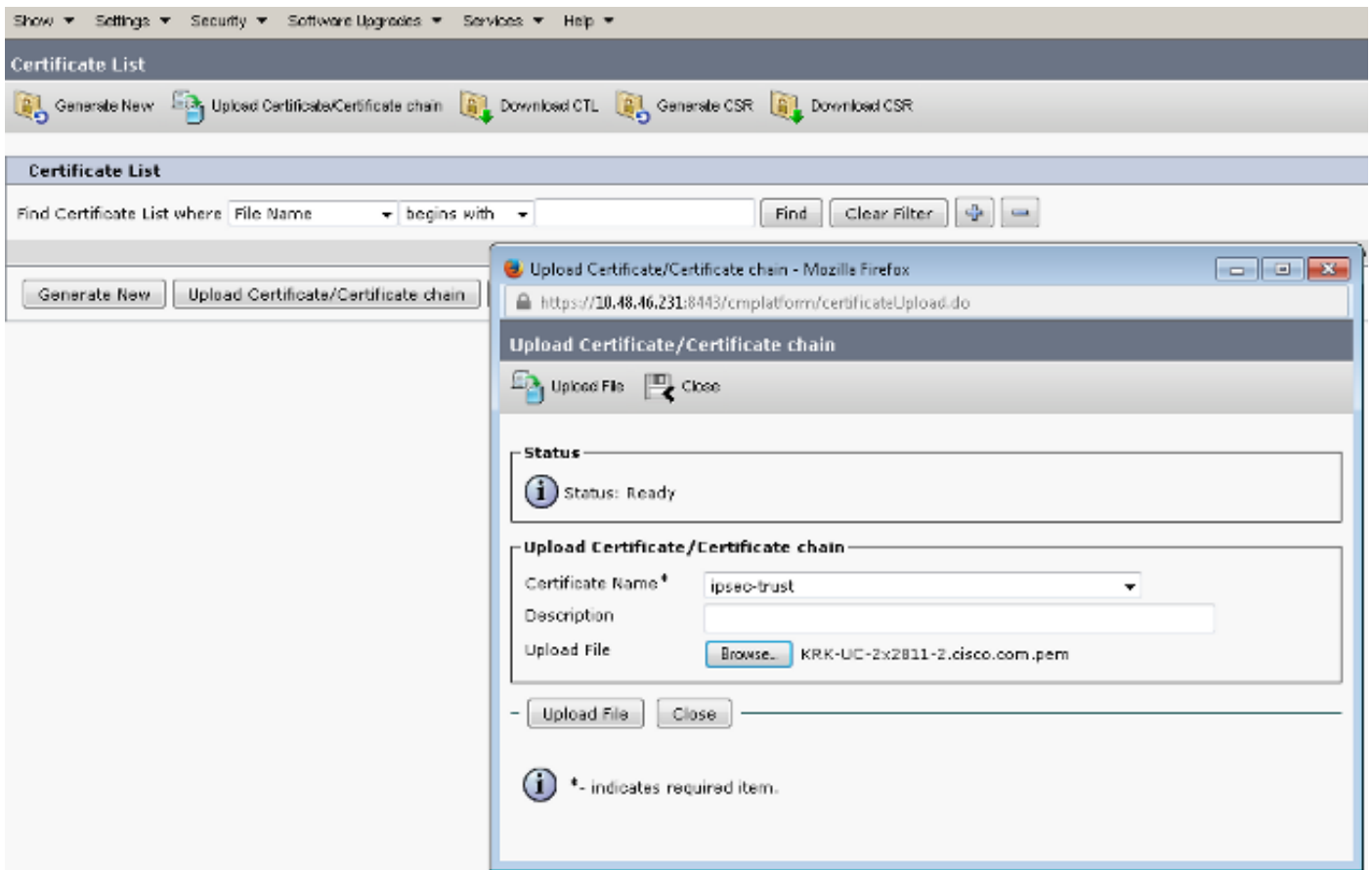
B4:05:9C:EB:52:B9:9D:81:A0:5A:A2:80:88:83:8B:32:5A:61:7E:A2

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

Nachdem sie als .pem-Dateien gespeichert wurden, müssen sie in CUCM importiert werden.
Wählen Sie **Cisco Unified OS Administration > Security > Certificate Management > Upload Certificate/Certificate** aus.

- CUCM-Zertifikat als IPsec
- Sprach-GW-Zertifikat als IPsec-Trust
- CA-Zertifikat als IPsec-trust:




4. Konfigurieren der IPsec-Tunneleinstellungen auf CUCM

Der nächste Schritt ist die Konfiguration des IPsec-Tunnels zwischen CUCM und dem Sprach-GW. Die IPsec-Tunnelkonfiguration auf CUCM wird über die Cisco Unified OS Administration-Webseite (https://<cucm_ip_address>/cmplatform) durchgeführt. Wählen Sie **Security > IPSEC Configuration > Add new IPsec policy** aus.

In diesem Beispiel wurde eine Richtlinie mit dem Namen "vgipsecpolicy" erstellt, deren Authentifizierung auf Zertifikaten basiert. Alle entsprechenden Informationen müssen ausgefüllt werden und entsprechen der Konfiguration auf dem Sprach-GW.

- Status

 Status: Ready

- The system is in FIPS Mode

- IPSEC Policy Details

Policy Group Name*	<input type="text" value="vgipsecpolicy"/>
Policy Name*	<input type="text" value="vgipsec"/>
Authentication Method*	<input type="text" value="Certificate"/>
Peer Type*	<input type="text" value="Different"/>
Certificate Name	<input type="text" value="KRK-UC-2x2811-2.pem"/>
Destination Address*	<input type="text" value="209.165.201.20"/>
Destination Port*	<input type="text" value="ANY"/>
Source Address*	<input type="text" value="209.165.201.10"/>
Source Port*	<input type="text" value="ANY"/>
Mode*	<input type="text" value="Transport"/>
Remote Port*	<input type="text" value="500"/>
Protocol*	<input type="text" value="ANY"/>
Encryption Algorithm*	<input type="text" value="AES 128"/>
Hash Algorithm*	<input type="text" value="SHA1"/>
ESP Algorithm*	<input type="text" value="AES 128"/>

- Phase 1 DH Group

Phase One Life Time*	<input type="text" value="3600"/>
Phase One DH*	<input type="text" value="2"/>

- Phase 2 DH Group

Phase Two Life Time*	<input type="text" value="3600"/>
Phase Two DH*	<input type="text" value="2"/>

- IPSEC Policy Configuration

Enable Policy

Hinweis: Der Name des Sprach-Gateway-Zertifikats muss im Feld Zertifikatname angegeben werden.

5. Konfigurieren der IPsec-Tunneleinstellung auf dem Sprach-GW

In diesem Beispiel wird mit Inline-Kommentaren die entsprechende Konfiguration auf einem Sprach-GW dargestellt.

```

crypto isakmp policy 1      (defines an IKE policy and enters the config-isakmp 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 crypto map on the interface)

access-list 130 permit ip host 209.165.201.20 host 209.165.201.10

```

Überprüfung

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Überprüfen des IPsec-Tunnelstatus am CUCM-Ende

Der schnellste Weg, den IPsec-Tunnelstatus auf dem CUCM zu überprüfen, ist die Seite für die Betriebssystemverwaltung, und verwenden Sie die **Ping**-Option unter Dienste > Ping. Stellen Sie sicher, dass das Kontrollkästchen **IPSec validieren** aktiviert ist. Offensichtlich ist die hier angegebene IP-Adresse die IP-Adresse des GW.

Ping Configuration



Ping

Status



Status: Ready

Ping Settings

Hostname or IP Address*	<input type="text" value="209.165.201.20"/>
Ping Interval*	<input type="text" value="1.0"/>
Packet Size*	<input type="text" value="56"/>
Ping Iterations	<input type="text" value="1"/>
<input checked="" type="checkbox"/> 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
```

Ping

Hinweis: Weitere Informationen zur Validierung des IPsec-Tunnels über die Ping-Funktion auf dem CUCM finden Sie unter diesen Cisco Bug-IDs:

- Cisco Bug ID [CSCuo53813](#) - Validieren Sie die Leerlaufergebnisse des IPsec-Pings, wenn ESP-Pakete (Encapsulating Security Payload) gesendet werden.
- Cisco Bug-ID [CSCud20328](#) - IPsec-Richtlinie validieren zeigt falsche Fehlermeldung im FIPS-Modus an

Überprüfen Sie den IPsec-Tunnelstatus am Voice Gateway-Ende.

Um zu überprüfen, ob die Konfiguration ordnungsgemäß ausgeführt wird, muss bestätigt werden, dass die Sicherheitszuordnungen (SAs) für beide Ebenen (Internet Security Association und Key Management Protocol (ISAKMP) und IPsec) ordnungsgemäß erstellt wurden.

Um zu überprüfen, ob der SA für ISAKMP erstellt wurde und korrekt funktioniert, geben Sie den Befehl `show crypto isakmp sa` auf dem GW ein.

```
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
```

Hinweis: Der richtige Status für den SA sollte "ACTIVE" und "QM_IDLE" lauten.

Die zweite Ebene sind SAs für IPsec. Ihr Status kann mit dem Befehl **show crypto ipsec sa** überprüft werden.

```
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 pcg sas:
KRK-UC-2x2811-2#

Hinweis: Eingehende und ausgehende Sicherheitsrichtlinienindizes (Security Policy Indexes, SPIs) sollten mit dem Status ACTIVE erstellt werden. Zähler für die Anzahl der eingekapselten/entkapselten und verschlüsselten/entschlüsselten Pakete sollten bei jedem Generieren von Datenverkehr über einen Tunnel wachsen.

Der letzte Schritt besteht in der Bestätigung, dass sich das MGCP-GW im registrierten Zustand befindet und die TFTP-Konfiguration fehlerfrei vom CUCM heruntergeladen wurde. Dies kann anhand der Ausgabe der folgenden Befehle bestätigt werden:

```
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#
```

Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration

verwenden können.

Fehlerbehebung für den IPsec-Tunnel am CUCM-Ende

Auf dem CUCM gibt es keinen Service für die IPsec-Terminierung und -Verwaltung. CUCM verwendet ein im Betriebssystem integriertes Red Hat IPsec-Toolpaket. Der Daemon, der unter Red Hat Linux läuft und die IPsec-Verbindung beendet, ist OpenSwan.

Bei jeder Aktivierung oder Deaktivierung der IPsec-Richtlinie auf dem CUCM (OS Administration > Security > IPSEC Configuration) wird der OpenWAN-Daemon neu gestartet. Dies kann im Linux-Nachrichtenprotokoll beobachtet werden. Ein Neustart wird durch folgende Zeilen angezeigt:

```
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
```

Jedes Mal, wenn ein Problem mit der IPsec-Verbindung auf dem CUCM auftritt, sollten die letzten Einträge im Nachrichtenprotokoll überprüft werden (geben Sie die **Dateiliste `active` `log` `syslog/messages*`** Befehl ein), um zu bestätigen, dass Openswan aktiv ist und ausgeführt wird. Wenn Openswan ohne Fehler ausgeführt und gestartet wird, können Sie die IPsec-Konfiguration beheben. Der für die Einrichtung von IPsec-Tunneln in Openswan verantwortliche Daemon ist Pluto. Pluto-Protokolle werden geschrieben, um Protokolle auf Red Hat zu sichern, und sie können über die **Datei `"get active` `log` `syslog/secure"` gesammelt werden.*** Befehl oder über **RTMT: Sicherheitsprotokolle**.

Hinweis: Weitere Informationen zum Erfassen von Protokollen über das RTMT finden Sie in der [RTMT-Dokumentation](#).

Wenn es schwierig ist, anhand dieser Protokolle die Ursache des Problems zu ermitteln, kann IPsec vom Technical Assistance Center (TAC) über das Root auf dem CUCM weiter verifiziert werden. Wenn Sie über Root auf den CUCM zugreifen, können Informationen und Protokolle zum IPsec-Status mithilfe der folgenden Befehle überprüft werden:

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

Es gibt auch eine Option, einen Red Hat-SOSreport über root zu generieren. Dieser Bericht enthält alle Informationen, die Red Hat-Support benötigt, um weitere Probleme auf Betriebssystemebene zu beheben:

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

Fehlerbehebung beim IPsec-Tunnel am Voice Gateway-Ende

Auf dieser Site können Sie nach Aktivierung der folgenden Debugbefehle alle Phasen der Einrichtung des IPsec-Tunnels beheben:


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

Hinweis: Detaillierte Schritte zur Fehlerbehebung für IPsec finden Sie in der [IPsec-Fehlerbehebung: Verstehen und Verwenden von Debugbefehlen](#).

Mithilfe der folgenden Debugbefehle können Sie MGCP-GW-Probleme beheben:

```
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
```