

CUCM و Voice GW نيب نم آل MGCP لاصتا تاداهش ل نيوكت لاثم ل اذانت سا IPsec ربع CA نم ةعقوم ل

المحتويات

[المقدمة](#)

[المتطلبات الأساسية](#)

[المتطلبات](#)

[المكونات المستخدمة](#)

[التكوين](#)

[الرسم التخطيطي للشبكة](#)

[1. قم بتكوين CA على Voice GW وإنشاء شهادة موقعة من CA ل Voice GW](#)

[2. إنشاء شهادة IPsec موقعة من CUCM](#)

[3. إستيراد شهادات CA و CUCM و GW على CUCM](#)

[4. تكوين إعدادات نفق IPsec على CUCM](#)

[5. قم بتكوين إعداد نفق IPsec على Voice GW](#)

[التحقق من الصحة](#)

[التحقق من حالة نفق IPsec على نهاية CUCM](#)

[التحقق من حالة نفق IPsec على نهاية العبارة الصوتية](#)

[استكشاف الأخطاء وإصلاحها](#)

[أستكشاف أخطاء نفق IPsec وإصلاحها في نهاية CUCM](#)

[أستكشاف أخطاء نفق IPsec وإصلاحها على نهاية عبارة الصوت](#)

المقدمة

يصف هذا المستند كيفية تأمين إرسال إشارات بروتوكول التحكم في عبارة الوسائط (MGCP) بنجاح بين عبارة الصوت (GW) و (CUCM (Cisco Unified Communications Manager) عبر أمان بروتوكول الإنترنت (IPsec)، استنادا إلى الشهادات الموقعة من مرجع الشهادة (CA). من أجل إعداد مكالمة آمنة عبر بروتوكول MGCP، يلزم تأمين تدفقات بروتوكول النقل في الوقت الفعلي (RTP) بشكل منفصل. يبدو أنه موثق جيدا وبسيط للغاية لإعداد تدفقات RTP المشفرة، ولكن لا يتضمن تدفق RTP الآمن إرسال إشارات MGCP الآمنة. إذا لم يتم تأمين إرسال إشارات MGCP، يتم إرسال مفاتيح التشفير لتدفق RTP في الوضوح.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- عبارة الصوت MGCP المسجلة إلى CUCM لإرسال المكالمات واستقبالها
- تم بدء خدمة "وظيفة وكيل المرجع المصدق" (CAPF)، وتم تعيين نظام المجموعة على الوضع المختلط
- تدعم صورة Cisco IOS® على GW ميزة أمان التشفير
- تم تكوين الهواتف و MGCP GW لبروتوكول نقل الوقت الفعلي الآمن (SRTP)

المكونات المستخدمة

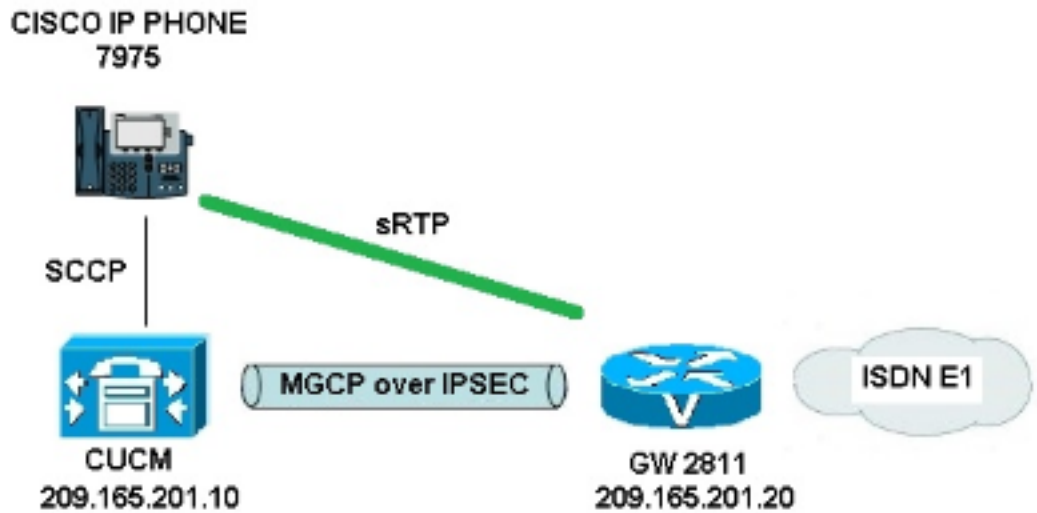
تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- CUCM - عقدة واحدة - تشغيل GGSG (مجموعة الحلول الحكومية العالمية من Cisco) الإصدار 14-8.6.1.20012 في وضع معيار معالجة المعلومات الفيدرالية (FIPS)
- هواتف 7975 التي تشغيل SCCP75-9-3-1SR2-1S
- بطاقة الصوت E1 ISDN - VWIC2-2MFT-T1/E1 - 2-Port RJ-48 Multiflex Trunk - Cisco 2811 - C2800nm-Adterprisek9-M - الإصدار M8(4)15.1، GW
- تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

التكوين

ملاحظة: أستخدم أداة بحث الأوامر (للعلماء المسجلين فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

الرسم التخطيطي للشبكة



من أجل إعداد IPsec بنجاح بين CUCM و GW الصوتي، أكمل الخطوات التالية:

1. قم بتكوين المرجع المصدق على GW الصوتي وإنشاء شهادة موقعة من CA ل GW الصوتي
2. إنشاء شهادة IPsec موقعة من CUCM
3. إستيراد شهادات CA و CUCM و CA GW على CUCM
4. تكوين إعدادات نفق IPsec على CUCM
5. تكوين إعدادات نفق IPsec على GW الصوتي

1. قم بتكوين CA على Voice GW وإنشاء شهادة موقعة من CA ل Voice GW

كخطوة أولى، يلزم إنشاء زوج مفاتيح (RSA) (Rivest-Shamir-Addleman) على خادم Cisco IOS CA:

```
KRK-UC-2x2811-2#crypto key generate rsa general-keys label IOS_CA exportable
سيتم استخدام عمليات التسجيل التي تم إكمالها عبر بروتوكول تسجيل الشهادة البسيط (SCEP)، لذا قم بتمكين خادم
:HTTP
```

```
KRK-UC-2x2811-2#ip http server
لتكوين خادم CA على بوابة، يلزم إكمال هذه الخطوات:
```

1. قم بتعيين اسم خادم PKI. يجب أن يكون نفس اسم زوج المفاتيح الذي تم إنشاؤه مسبقاً.

```
KRK-UC-2x2811-2(config)#crypto pki server IOS_CA
```

2. حدد الموقع الذي سيتم فيه تخزين كافة إدخلات قاعدة البيانات لخادم CA.

```
KRK-UC-2x2811-2(cs-server)#crypto pki server IOS_CA
```

3. قم بتكوين اسم مصدر CA.

```
KRK-UC-2x2811-2(cs-server)#issuer-name cn=IOS
```

4. حدد نقطة توزيع قائمة إبطال الشهادات (CDP) (CRL) ليتم استخدامها في الشهادات التي يتم إصدارها بواسطة خادم الشهادات وتمكين منح طلبات إعادة تسجيل الشهادة تلقائياً لخادم CA التابع ل 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. قم بتمكين خادم CA.

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

تتمثل الخطوة التالية في إنشاء TrustPoint لشهادة CA ونقطة ثقة محلية لشهادة الموجه مع تسجيل URL الذي يشير إلى خادم HTTP محلي:

```
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
```

لإنشاء شهادة الموجه الموقعة من المرجع المصدق المحلي، يلزم مصادقة جهة الاتصال وتسجيلها:

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

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

بعد ذلك، يتم إنشاء شهادة الموجه وتوقيعها من قبل المرجع المصدق المحلي. قم بسرد الشهادة على الموجه للتحقق.

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

```
Certificate
```

```
Status: Available
```

```
Certificate Serial Number (hex): 02
```

```
Certificate Usage: General Purpose
```

```
:Issuer
```

```
cn=IOS
```

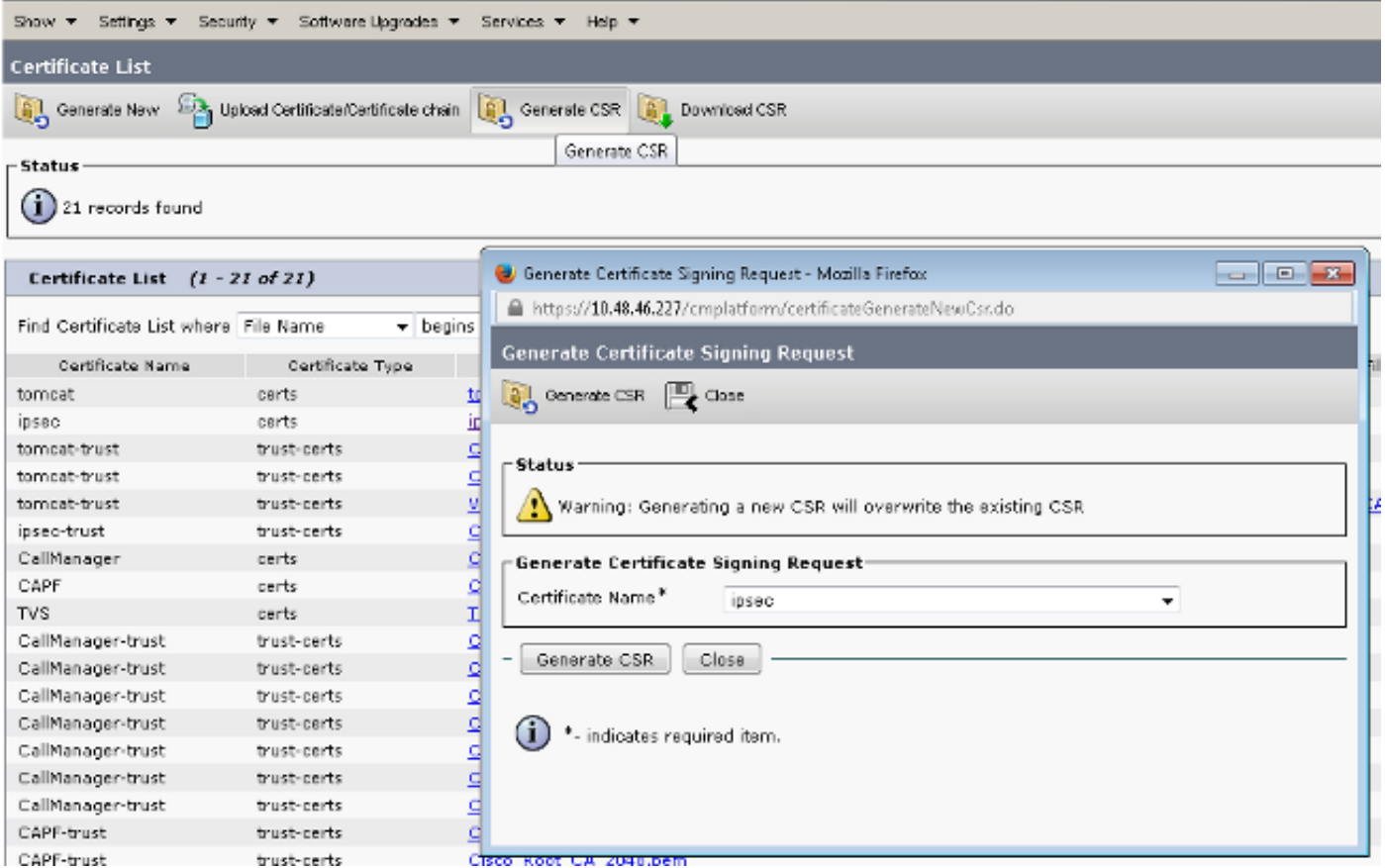
```
:Subject
Name: KRK-UC-2x2811-2
cn=KRK-UC-2x2811-2
:CRL Distribution Points
http://10.48.46.251/IOS_CA.crl
:Validity Date
start date: 13:05:01 CET Nov 21 2014
end date: 13:05:01 CET Nov 21 2015
Associated Trustpoints: local1
Storage: nvram:IOS#2.cer
```

```
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
```

يجب إدراج شهادتين. الأول هو شهادة جهاز توجيه (KRK-UC-2x2811-2) موقعة من المرجع المصدق المحلي، والثاني شهادة CA.

2. إنشاء شهادة IPsec موقعة من CUCM

يستخدم CUCM الخاص بإعداد نفق IPsec شهادة IPsec.pem. بشكل افتراضي، تكون هذه الشهادة موقعة ذاتيا ويتم إنشاؤها عند تثبيت النظام. لاستبدالها بشهادة موقعة من CA، يلزم أولا إنشاء CSR (طلب توقيع الشهادة) ل IPsec من صفحة إدارة CUCM OS. اختر إدارة نظام التشغيل الموحدة من Cisco < الأمان < إدارة الشهادات < إنشاء CSR.



بعد إنشاء CSR، يجب تنزيلها من CUCM وتسجيلها مقابل CA على GW. للقيام بذلك، أدخل الأمر `crypto pki server IOS_CA request pkcs10 terminal base64` وبلزم لصق تجزئة طلب التوقيع عبر terminal. يتم عرض الشهادة الممنوحة وبلزم نسخها وحفظها كملف `ipsec.pem`.

```
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-----
MIIDNjCCA4CAQAwgaxkCzAJBgNVBAYTA1BMMQ4wDAYDVQQIEwVjaXNjbzEOMAwG
A1UEBxMFY21zY28xDjAMBgNVBAoTBWNpc2NvMQ4wDAYDVQQLEwVjaXNjbzEPMA0G
A1UEAxMGQ1VDTUlxMUKwRwYDVQFE0A1NjY2OWY5MjgzNWZmZWZmZWZmZWZmZWZm
NjcwMDBmMGI2NjliYjdkYWZhNDNmM2QzOWFhNGQxMzZmZmZmZmZmZmZmZmZmZmZm
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEakfHxvcov4vFmK+3+dQShW3s3SzAYBQ19
0JDBiIc4eDRmdrq0V2dkn9UpLUx9OH7V0Oe/8wmHqYwoxFZ5a6B5qRRkc010/ub2
ullQCw+nQ6QiZGdNhdne0NYY4r3odF4CkrtYAJA4PUSce1tWxfiJY5dw/Xhv8cVg
gVyuxctESemfMhUfvEM203NU9nod7YTEzQzuAadjNcyc4blu91vQm5OVUNXxODov
e7/OlQNUWU3LSEr0aI9lC75x3qdRGe8Pwnk/gWbT5B7pwuwMXTU8+UFj6+lvrQM
Rb47dw22yFmSMObvez18IVExAyFs50j9Aj/rNFIdUQIt+Nt+Q+f38wIDAQABOEcw
RQYJKoZIhvcNAQkOMTgwNjAnBgNVHSUEIDAEBggrBgEFBQcDAQYIKwYBBQUHAWIG
CCsGAQUFBwMFMA5GAlUdDwQEAWIDuANBgkqhkiG9w0BAQUFAAOCAQEADgAR40l
oQ4z2yqgSsICAZ2hQA3Vztp6aOI+0PSyMfihGS//3V3tALEZL2+t0Y5e1KsBea72
sieKjpSikXjNa+SiYlaYy4siVw5EKQD3Ii4Qv115BvuniZXvBiBQUw+SpBLbeNi
xwIgrYELrFywQZBeZ0dFqnSKN9XlisXe6oU9GXux7uwgXwCXMF/azutbiol4Fgf
qUF00GzkhtEapJA6c5RzaxG/OuDuKY+4z1eSSsXzFhBTifk3RfJA+I7Na1zQBIEJ
2IOJdiZnn0HWVr5C5eZ7VnQuNdiC/qn3uUfvNVRZo8iCDq3tRv7dr/n64jdKsHEM
==lk6P8gp9993cJw
quit
:Granted certificate %
MIIDXTCCAasagAwIBAgIBBTANBgkqhkiG9w0BAQQFADAOMQwwCgYDVQQDEwNUTlMw
```

```
HhcNMTUwMTA4MTIwMTAwWhcNMTYwMTA4MTIwMTAwWjCBqTELMAkGA1UEBhMCUEwX
DjAMBgNVBAGTBWNpc2NvMQ4wDAYDVQOHEwVjaXNjbzEOMAwGA1UEChMFY2l2Y28x
DjAMBgNVBAsTBWNpc2NvMQ8wDQYDVQQDEwZDVUNNQjExSTBHBG9NVBAUTQDU2NjY5
ZjkyODMlZmZlZDUwODRiMjkxNTg2NzAwMGYwYyY2OWJiN2RhZmE0M2YzZDM5YWE0
ZDEzMzVlOWUyNTMwgG9EiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCRC8fG9
yi/i8WYr7f51BKfBezdlMBgFDX3QkMGInzh4NGZ2urRXZ2Sf1SktTH04ftXQ57/z
CYepjCjEVnlroHmpFGRw7XT+5va6XVALD6dDpCJkZ02F2d7Q1hjiveh0XgKSulga
kDg9RJx7W1bF+I1j13D9eG/xxWCBXK7Fy0RJ6Z8yFR+8QzbTc1T2eh3thMTND04B
+p2M1zJzhvW73W9Cbk5VQ1fE40i97v86VA1RZTctISvRoJ2ULvnHep1EYF7w/CeT
BZtPkHunC7AxdNTz5QWPr6W+tAxFvjt3DbbIwZIW5u97PXwhUTEDIWzk6P0CP+s0
Uh1RAi34235D5/fzAgMBAAGjgaowgacwLwYDVR0fBCgwJjAkoCKgIIYeaHR0cDov
LzEwLjQ4LjQ2LjI1MS9JT1NfQ0EuY3JsMAsGA1UdDwQEAwIDuDanBgNVHVSUEIDAe
BggrBgEFBQcDAQYIKwYBBQUHAWIGCCsGAQUFBwMFMB8GA1UdIwQYMBaAFJSLP5cn
PL8bIP7VSKLtb6Z1socOMB0GA1UdDgQWBRR4m2eTSyELsdRBW4MRmbNdT2qppTAN
BgkqhkiG9w0BAQQFAA0BgQBvVJ+tVS0JqP4z9TgEeuMbVwn00CTKXz/fCuh6R/50
qq8JhERJGiR/ZHvHRLf+XawhnoE6daPAmE+WkIPtHIhbmHChbbxG9ffdyainXRWY
5sI5XycF1FgYGpTFBYD9M0Lqsw+FIYaT2ZrbOGsx8h6pZoesKqm85RByIUjX4nJK
==lg
```

ملاحظة: من أجل فك ترميز وفحص محتوى شهادة Base64 المرمزة، أدخل الأمر -in openssl x509 -text -noout .certificate.crt

يتم فك ترميز شهادة CUCM الممنوحة ل:

```
: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
:f1:f1:bd:ca:2f:e2:f1:66:2b:ed:fe:75:04:00:91
:a1:5b:7b:37:4b:30:18:05:0d:7d:d0:90:c1:88:87
:ba:b4:57:67:64:9f:d5:29:2d:4c:38:78:34:66:76
: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
:e2:bd:e8:74:5e:02:92:bb:58:00:90:38:3d:44:18
: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
:d3:73:54:f6:7a:1d:ed:84:c4:cd:0c:ee:01:a7:36
:cc:9c:e1:bd:6e:f7:5b:d0:9b:93:95:50:d5:63:35
: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
:e6:ef:7b:3d:7c:21:51:31:03:21:6c:e4:e8:92:30
: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
: f2:1e:a9:66:87:ac:2a:a9:bc:e5:10:72:21:48:d7:e2:72:31
4a:d6

```

3. إستيراد شهادات CA و CUCM و GW CA على CUCM

تم تصدير شهادة IPsec CUCM بالفعل إلى ملف pem. وكخطوة تالية، يلزم إكمال نفس العملية بشهادة GW الصوتية وشهادة CA. للقيام بذلك، يلزم عرضها أولاً على وحدة طرفية باستخدام الأمر `crypto pki export local1 pem terminal` ونسخها لفصل ملفات pem.

```

KRK-UC-2x2811-2(config)#crypto pki export local1 pem terminal
:CA certificate %
-----BEGIN CERTIFICATE-----
MIIB9TCCA6AwIBAgIBATANBgkqhkiG9w0BAQQFADAOMQwwCgYDVQQDEwNJTlMw
HhcNMTQxMTIwMTEyMTEyWhcNMTQxMTIwMTEyMTEyWjAOMQwwCgYDVQQDEwNJTlMw
gZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAK6Cd2yxUywtbgBELkZUsP6eaZVv
6YfpEbFptyt6ptRdpxgjOYI3InEP3wewtmEPNeTJL8+a/W7MDUemm3t/NlWBO6T2
m9Bp6k0FNOBXMKEDfTSqOKEy7WfLASE/Pbq8M+JMpeMWz8xnMboYOb66rY8igZFz
/kltRPLIMsf5r01tnAgMBAAGjYzBhMA8GALUdEwEB/wQFMAMBAf8wDgYDVVR0PAQH
BAQDAgGMB8GALUdIwQYMBaAFJSLP5cnPL8bIP7VSKLtB6Z1socOMB0GALUdDgQW
BBSUiz+XJzy/GyD+1Uii7QemdbKHDjANBgkqhkiG9w0BAQQFAA0BgQCUMC1SFVLS
TSS1Exbm9i2D4HOWYhCurhifqTWLxMMXj0jym24DoqZ91aDNG1VwiJ/Yv4i40t90
y65WzbapZL1S65q+d7BCLQypdrwKkdS0dfTdkfXESyWLhecRa8mnZckpgKbk8Ir
==BfM9K+caXkfhPEPa644UzV9++OKMKhtDuQ
-----END CERTIFICATE-----

:General Purpose Certificate %
-----BEGIN CERTIFICATE-----
MIIB2zCCAUSgAwIBAgIBAJANBgkqhkiG9w0BAQUFADAOMQwwCgYDVQQDEwNJTlMw
HhcNMTQxMTIwNTAxWhcNMTUxMTIwNTAxWjAaMRGwFgYDVQQDEw9LUkst
VUMtMngyODExLTlWMDANBgkqhkiG9w0BAQEFAANLADBIAAEApGWINlnAAATKLVMoj
mZVkJQFgI8LrHD6zSrlaKgaJh1U+H/mnRQQ5rqitIpekDdPooWST9RxC5CJmB4spT
VWkYkwIDAQBo4GAMH4wLwYDVR0fBCgwJjAkoCKGjIIYeaHR0cDovLzEwLjQ4LjQ2
/LjI1MS9JTlNfQ0EuY3JsMAsGALUdDwQEAwIFoDAFbgNVHSMEGDAWgBSUiz+XJzy
GyD+1Uii7QemdbKHDjAdBgNVHQ4EFgQUtAwc61K5nYGGwQkAiIOLMlphfQIwDQYJ
KoZIhvcNAQEFBQADgYEAjDflH+N3yc3RykCig9B0aAIXWZPmaqL9v9R75zc+f8x
zbSIzoVbBhnUOeu0j1hnIghyMjeELjTEh6uQrWUN2ElW1ypfmxk1jN5q0t+vfdR
=yepS04pFor9RoD7IWg6e/1hFDEep9hBvzrVwQHCjzeY0rVrPcLl26k5oauMwTs+
-----END CERTIFICATE-----

```

يتم فك ترميز % CA للشهادة إلى:

```

: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
:ae:82:77:6c:b1:53:2c:2d:6e:00:44:96:46:54:00
: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
:e0:57:30:a7:83:7d:34:aa:38:a1:32:ed:67:cb:34
:bf:3d:ba:bc:33:e2:4c:a5:e3:16:cf:cc:67:01:27
:ba:18:39:be:ba:ad:8f:22:81:91:73:93:5b:51:31
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
:ae:ae:18:9f:a9:35:8b:c4:c3:17:8f:48:f2:9b:6e:96:62:10
:a2:a6:7d:d5:a0:cd:1b:55:70:88:9f:d8:bf:88:b8:d2:df:03
:cb:ae:56:cd:b6:a9:64:bd:52:eb:9a:be:77:b0:42:2d:0c:74
: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
b9:43

```

يتم فك ترميز % شهادة الغرض العام إلى:

```

: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
:a4:65:88:37:59:c0:02:d2:8b:54:c3:a3:99:95:00
:f0:ba:c7:0f:ac:d2:ae:56:8a:80:02:64:40:58:08
:61:95:4f:87:fe:69:d1:41:0e:6b:aa:2b:48:a5:e9

```



```

:fa:28:c1:24:fd:47:10:b9:08:99:81:e2:ca:03:74
53:55:69:18:93
(Exponent: 65537 (0x10001
:X509v3 extensions
:X509v3 CRL Distribution Points
URI:http://10.48.46.251/IOS_CA.crl

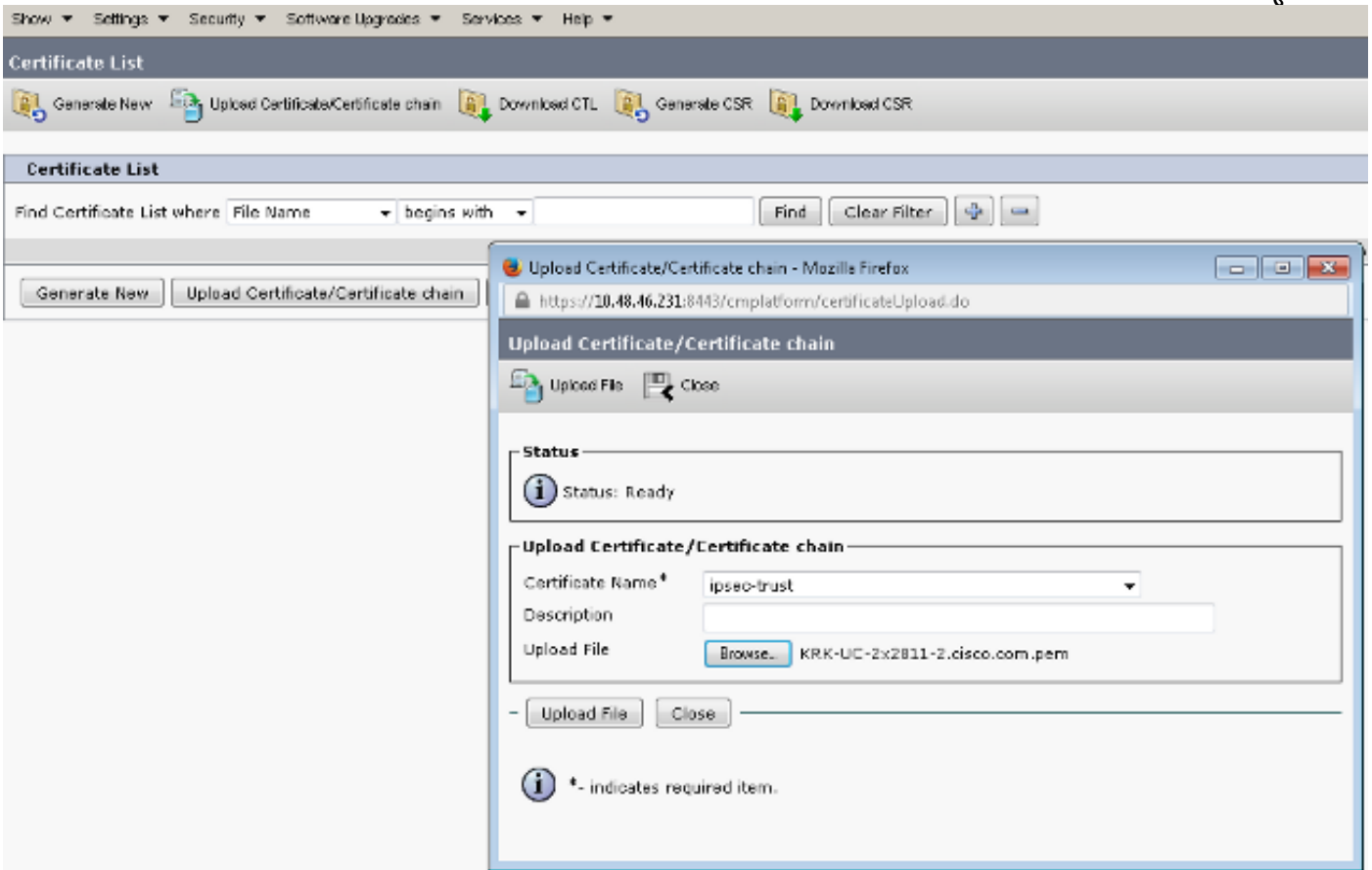
:X509v3 Key Usage
Digital Signature, Key Encipherment
:X509v3 Authority Key Identifier
keyid:94:8B:3F:97:27:3C:BF:1B:20:FE:D5:48:A2:ED:07:A6:75:B2:87:0E

: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
:e6:6a:a2:c5:f6:ff:51:ef:9c:dc:f9:ff:31:cd:b4:88:59:93
:ce:85:5b:06:19:d4:39:eb:8e:8f:58:67:22:01:f2:c8:c8:de
:b8:d3:12:1e:ae:42:b5:94:37:61:25:5b:5c:a9:7e:6c:64:10
:d6:33:79:ab:4b:7e:bd:f7:51:fb:27:a9:4b:4e:29:16:8a:fd
:fb:21:68:3a:7b:fd:61:14:31:1e:a7:d8:41:bf:3a:d5:46:80
:c1:01:c2:8f:37:98:d2:b5:6b:3d:c2:e5:db:a9:39:a1:ab:8c
c1:3b

```

بعد حفظها كملفات pem، يجب إستيرادها إلى CUCM. أخطر إدارة نظام التشغيل الموحدة من Cisco < الأمان > إدارة الشهادات < تحميل الشهادة/الشهادة.


- شهادة CUCM ك IPsec
- شهادة GW الصوتية كتقنة IPsec
- شهادة CA كتقنة IPsec.



4. تكوين إعدادات نفق IPsec على CUCM

تتمثل الخطوة التالية في تكوين نفق IPsec بين CUCM و GW الصوتي. يتم إجراء تكوين نفق IPsec على CUCM عبر صفحة الويب الخاصة بإدارة نظام التشغيل الموحد من (Cisco (https://<cucm_ip_address>/cmplatform).
أختر التأمين < تكوين IPsec > إضافة سياسة IPsec جديدة.

في هذا المثال، تم إنشاء سياسة تسمى "vgipsecpolicy"، مع مصادقة تستند إلى شهادات. كل المعلومات المناسبة تحتاج أن يكون ملئت وبطابق التشكيل على الصوت GW.

- Status -	
	Status: Ready
- The system is in FIPS Mode -	
- IPSEC Policy Details -	
Policy Group Name*	vgipsecpolicy
Policy Name*	vgipsec
Authentication Method*	Certificate
Peer Type*	Different
Certificate Name	KRK-UC-2x2811-2.pem
Destination Address*	209.165.201.20
Destination Port*	ANY
Source Address*	209.165.201.10
Source Port*	ANY
Mode*	Transport
Remote Port*	500
Protocol*	ANY
Encryption Algorithm*	AES 128
Hash Algorithm*	SHA1
ESP Algorithm*	AES 128
- Phase 1 DH Group -	
Phase One Life Time*	3600
Phase One DH*	2
- Phase 2 DH Group -	
Phase Two Life Time*	3600
Phase Two DH*	2
- IPSEC Policy Configuration -	
<input checked="" type="checkbox"/>	Enable Policy

ملاحظة: يلزم تحديد اسم شهادة العبارة الصوتية في حقل اسم الشهادة.

5. قم بتكوين إعداد نفق IPsec على Voice GW

يعرض هذا المثال، مع التعليقات في السطر، التكوين المطابق على GW الصوتي.

```
(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
```

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

التحقق من حالة نفق IPsec على نهاية CUCM

أسرع طريقة للتحقق من حالة نفق IPsec على CUCM هي الانتقال إلى صفحة إدارة OS واستخدام خيار ping ضمن الخدمات < إختبار الاتصال. تأكد من تحديد خانة الاختيار **التحقق من IPsec**. من الواضح أن عنوان IP المحدد هنا هو عنوان IP الخاص بـ 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

ملاحظة: راجع معرفات أخطاء Cisco هذه للحصول على معلومات حول التحقق من صحة نفق IPsec عبر ميزة اختبار الاتصال على CUCM:

- معرف تصحيح الأخطاء من Cisco [CSCuo53813](#) - التحقق من نتائج اختبار الاتصال IPsec فارغة عند إرسال حزم ESP (حمولة أمان التضمين)
- معرف تصحيح الأخطاء من Cisco [CSCud20328](#) - التحقق من صحة نهج IPsec يظهر رسالة خطأ غير صحيحة في وضع FIPS

التحقق من حالة نفق IPsec على نهاية العبارة الصوتية

للتحقق مما إذا كان الإعداد يعمل بشكل صحيح أم لا، يلزم التأكد من إنشاء اقترانات الأمان (SAs) لكلا الطبقتين (اقتران أمان الإنترنت وبروتوكول إدارة المفاتيح (ISAKMP) و IPsec) بشكل صحيح.

للتحقق من إنشاء SA ل ISAKMP والعمل بشكل صحيح، أدخل الأمر `show crypto isakmp sa` على GW.

```
dst src state conn-id status
QM_IDLE 1539 ACTIVE 209.165.201.10 209.165.201.20
```

IPv6 Crypto ISAKMP SA

ملاحظة: يجب أن تكون الحالة الصحيحة ل SA نشطة و QM_IDLE.

الطبقة الثانية هي شبكات SA ل IPsec. يمكن التحقق من حالتها باستخدام الأمر `show crypto ipSec`.

```
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 pcg 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#
```

ملاحظة: يجب إنشاء فهارس سياسة الأمان الواردة والصادرة (SPIs) في الحالة "نشط"، كما يجب أن تنمو

عدادات عدد الحزم التي تم تغليفها/فك كبسلة وتشفيرها/فك تشفيرها كل مرة يتم فيها إنشاء أي حركة مرور عبر نفق.

الخطوة الأخيرة هي تأكيد أن MGCP GW في الحالة المسجلة وأن تكوين TFTP تم تنزيله بشكل صحيح من CUCM دون أي حالات فشل. هذا يستطیع كنت أكدت من الإنتاج من هذا أمر:

```
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#
```

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

أستكشاف أخطاء نفق IPsec وإصلاحها في نهاية CUCM

لا توجد على CUCM خدمة قابلة الصيانة مسؤولة عن إنهاء IPsec وإدارته. يستخدم CUCM حزمة أدوات Red Hat

IPsec المضمنة في نظام التشغيل. البرنامج الخفي الذي يعمل على Red Hat Linux وينتهي من اتصال IPsec هو OpenSwan.

في كل مرة يتم فيها تمكين نهج IPsec أو تعطيله على CUCM (إدارة OS < الأمان < تكوين IPsec)، تتم إعادة تشغيل البرنامج الخفي OpenWAN. يمكن ملاحظة ذلك في سجل رسائل لينوكس. تشير هذه السطور إلى إعادة التشغيل:

```
...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
```

في كل مرة تكون هناك مشكلة في اتصال IPsec على CUCM، يجب التحقق من الإدخالات الأخيرة في سجل الرسائل (أدخل الأمر قائمة الملفات **activefield syslog/messages**) لتأكيد تشغيل OpenWAN. إذا تم تشغيل OpenWAN وبدء تشغيله دون حدوث أخطاء، فيمكنك استكشاف أخطاء إعداد IPsec وإصلاحها. إن الأداة المساعدة المسؤولة عن إعداد أنفاق IPsec في OpenSSWAN هي Pluto. تتم كتابة سجلات Pluto لتأمين السجلات على Red Hat، ويمكن تجميعها عبر الملف **get activelog syslog/secure**. الأمر أو عبر RTMT: سجلات الأمان.

ملاحظة: يمكن العثور على مزيد من المعلومات حول كيفية تجميع السجلات عبر RTMT في [وئائق RTMT](#).

إذا كان من الصعب تحديد مصدر المشكلة استناداً إلى هذه السجلات، يمكن التحقق من IPsec بشكل إضافي بواسطة مركز المساعدة التقنية (TAC) عبر الجذر على CUCM. بعد الوصول إلى CUCM عبر الجذر، يمكن التحقق من المعلومات والسجلات حول حالة IPsec باستخدام الأوامر التالية:

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

وهناك أيضاً خيار لإنشاء تقرير Red Hat Sosreport عبر الجذر. يحتوي هذا التقرير على جميع المعلومات المطلوبة من قبل دعم Red Hat لاستكشاف المشاكل الأخرى وإصلاحها على مستوى نظام التشغيل:

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

أستكشاف أخطاء نفق IPsec وإصلاحها على نهاية عبارة الصوت

على هذا الموقع، يمكنك استكشاف أخطاء جميع مراحل إعداد نفق IPsec وإصلاحها بعد تمكين أوامر تصحيح الأخطاء التالية:

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

ملاحظة: تم العثور على الخطوات التفصيلية لاستكشاف أخطاء IPsec وإصلاحها في [أستكشاف أخطاء IPsec وإصلاحها: فهم أوامر تصحيح الأخطاء واستخدامها](#).

أنت يستطيع تحربت MGCP GW مشكلة مع هذا يضبط أمر:

```
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
```


ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا اذ ه Cisco ت مچرت
م ل ا ل ا ا ن ا ع مچ ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل و
ا م ك ة ق ي ق د ن و ك ت ن ل ة ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن ت س م ل ا