تكوين موجه Cisco IOS وتسجيله إلى موجه Cisco IOS آخر تم تكوينه كخادم CA

المحتويات

المقدمة

يوضح هذا المستند كيفية تكوين موجه Cisco IOS® كخادم مرجع شهادات (CA). وبالإضافة إلى ذلك، يوضح كيفية تسجيل موجه Cisco IOS آخر للحصول على شهادة جذر ومعرف لمصادقة IPsec من خادم CA.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

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

- موجهات Cisco 2600 Series التي تشغل برنامج Cisco IOS الإصدار 12.3(4)T3.

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.

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

إنشاء زوج مفاتيح RSA وتصديره لخادم الشهادات

تتمثل الخطوة الأولى في إنشاء زوج مفاتيح RSA الذي يستخدمه خادم Cisco IOS CA. على الموجه (R1)، قم بإنشاء مفاتيح RSA كما يوضح هذا الإخراج:

```
R1(config)#crypto key generate rsa general-keys label cisco1 exportable
The name for the keys will be: cisco1
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
.a few minutes

:[How many bits in the modulus [512
[Generating 512 bit RSA keys ...[OK %

#(R1(config
Jan 22 09:51:46.116: %SSH-5-ENABLED: SSH 1.99 has been enabled*
```

ملاحظة: يجب إستخدام نفس اسم زوج المفاتيح (*تسمية المفتاح*) الذي تخطط لاستخدامها لخادم الشهادة (عبر الأمر **crypto pki server *cs-label* الذي تمت تغطيته لاحقا).**

تصدير زوج المفاتيح الذي تم إنشاؤه

قم بتصدير المفاتيح إلى ذاكرة الوصول العشوائي غير المتطايرة (NVRAM) أو TFTP (استنادا إلى التكوين الخاص بك). في هذا المثال، يتم إستخدام ذاكرة NVRAM. استنادا إلى التطبيق الخاص بك، قد ترغب في إستخدام خادم TFTP منفصل لتخزين معلومات الشهادة الخاصة بك.

```
R1(config)#crypto key export rsa cisco1 pem url nvram: 3des cisco123

Key name: cisco1 %
Usage: General Purpose Key
...Exporting public key
?[Destination filename [cisco1.pub
Writing file to nvram:cisco1.pub
```

```
...Exporting private key
?[Destination filename [cisco1.prv
  Writing file to nvram:cisco1.prv
#(R1(config
```

إذا كنت تستخدم خادم TFTP، فيمكنك إعادة إستيراد زوج المفاتيح الذي تم إنشاؤه كما يوضح هذا الأمر:

```
crypto key import rsa key-label pem [usage-keys] {terminal | url url} [exportable] passphrase
```

ملاحظة: إذا لم تكن ترغب في أن يكون المفتاح قابلا للتصدير من خادم الشهادات، قم باستيراده مرة أخرى إلى خادم الشهادات بعد تصديره كزوج مفاتيح غير قابل للتصدير. بهذه الطريقة، لا يمكن إزالة المفتاح مرة أخرى.

التحقق من زوج المفاتيح الذي تم إنشاؤه

قم بإصدار الأمر **show crypto key mypubkey rsa** للتحقق من زوج المفاتيح الذي تم إنشاؤه.

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر **show**. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مُخرَج الأمر **show** .

```
R1#show crypto key mypubkey rsa
Key pair was generated at: 09:51:45 UTC Jan 22 2004 %
Key name: cisco1
Usage: General Purpose Key
.Key is exportable
:Key Data
305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00CC2DC8 ED26163A
B3642376 FAA91C2F 93A3825B 3ABE6A55 C9DD3E83 F7B2BD56 126E0F11 50552843
    7F7CA4DA 3EC3E2CE 0F42BD6F 4C585385 3C43FF1E 04330AE3 37020301 0001
Key pair was generated at: 09:51:54 UTC Jan 22 2004 %
Key name: cisco1.server
Usage: Encryption Key
.Key is exportable
:Key Data
307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00EC5578 025D3066
72149A35 32224BC4 3E41DD68 38B08D39 93A1AA43 B353F112 1E56DA42 49741698
EBD02905 FE4EC392 7174EEBF D82B4475 2A2D7DEC 83E277F8 AEC590BE 124E00E1
    C1607433 5C7BC549 D532D18C DD0B7AE3 AECDDE9C 07AD84DD 89020301 0001
```

تمكين خادم HTTP على الموجه

يدعم خادم Cisco IOS CA عمليات التسجيل التي تتم عبر بروتوكول تسجيل الشهادة البسيط (SCEP) فقط. وبالتالي، ولجعل هذا ممكنا، يجب أن يقوم الموجه بتشغيل خادم Cisco IOS HTTP المدمج. أستخدم الأمر **ip http server** من أجل تمكينه:

```
R1(config)#ip http server
```

تمكين خادم CA وتكوينه على الموجه

أكمل الخطوات التالية:

1. من المهم جدا تذكر أنه يجب على خادم الشهادات إستخدام نفس اسم زوج المفاتيح الذي أنشأته يدويا.تتطابق

التسمية مع تسمية زوج المفاتيح التي تم إنشاؤها:
```
R1(config)#crypto pki server cisco1
```

بعد تمكين خادم ترخيص، يمكنك إستخدام القيم الافتراضية المكونة مسبقا أو تحديد قيم عبر CLI لوظائف خادم الترخيص.

2. يحدد الأمر **قاعدة البيانات url** الموقع الذي تتم فيه كتابة جميع إدخالات قاعدة البيانات لخادم CA. إذا لم يتم تحديد هذا الأمر، فسيتم كتابة جميع إدخالات قاعدة البيانات إلى Flash.
```
:R1(cs-server)#database url nvram
```

ملاحظة: إذا كنت تستخدم خادم TFTP، فيجب أن يكون عنوان URL هو **tftp://<ip_address>/directory**.

3. تكوين مستوى قاعدة البيانات:
```
R1(cs-server)#database level minimum
```

يتحكم هذا الأمر في نوع البيانات المخزنة في قاعدة بيانات تسجيل الشهادة:**الحد الأدنى**—يتم تخزين معلومات كافية فقط لمتابعة إصدار شهادات جديدة بدون تعارض. القيمة الافتراضية.**الأسماء**- بالإضافة إلى المعلومات المقدمة في المستوى الأدنى، الرقم التسلسلي واسم الموضوع لكل شهادة.**Complete**—بالإضافة إلى المعلومات المتوفرة في الحد الأدنى ومستويات الأسماء، تتم كتابة كل شهادة صادرة إلى قاعدة البيانات.**ملاحظة:** تنتج الكلمة الأساسية **الكاملة** قدرا كبيرا من المعلومات. إذا تم إصدارها، فيجب عليك أيضا تحديد خادم TFTP خارجي يتم فيه تخزين البيانات عبر الأمر **url لقاعدة البيانات**.

4. قم بتكوين اسم مصدر CA إلى سلسلة DN المحددة. على هذا المثال، يتم إستخدام CN (الاسم الشائع) من cisco1.cisco.com و L (المنطقة المحلية) من RTP و C (البلد) من US:
```
R1(cs-server)#issuer-name CN=cisco1.cisco.com L=RTP C=US
```

5. تحديد مدة صلاحية شهادة المرجع المصدق أو الشهادة بالأيام.تتراوح القيم الصالحة من *يوم واحد إلى 1825 يوما*. العمر الافتراضي لشهادة المرجع المصدق هو ثلاث سنوات، وفترة بقاء الشهادة الافتراضية هي سنة واحدة. مدة صلاحية الشهادة القصوى *أقل* بشهر واحد من مدة صلاحية شهادة المرجع المصدق. على سبيل المثال:
```
R1(cs-server)#lifetime ca-certificate 365
R1(cs-server)#lifetime certificate 200
```
6. حدد فترة بقاء CRL، بالساعات، التي يتم إستخدامها من قبل خادم الشهادات. القيمة القصوى لفترة الحياة هي **336 ساعة** (أسبوعان). القيمة الافتراضية هي **168 ساعة** (أسبوع واحد).
```
R1(cs-server)#lifetime crl 24
```

7. قم بتعريف نقطة توزيع قائمة إبطال الشهادات (CDP) لاستخدامها في الشهادات التي يتم إصدارها بواسطة خادم الشهادات.يجب أن يكون URL HTTP URL. على سبيل المثال، كان لدى الخادم عنوان IP بقيمة 172.18.108.26:
```
R1(cs-server)#cdp-url http://172.18.108.26/cisco1cdp.cisco1.crl
```

8. أصدرت ال **ما من إيقاف عمل** أمر in order to مكنت ال CA نادل:
```
R1(cs-server)#no shutdown
```

ملاحظة: قم بإصدار هذا الأمر فقط بعد تكوين خادم الشهادات بالكامل.

تكوين موجه IOS الثاني (R2) وتسجيله إلى خادم الشهادات

اتبع هذا الإجراء.

1. قم بتكوين اسم المضيف واسم المجال وإنشاء مفاتيح RSA على R2.أستخدم الأمر **hostname** لتكوين اسم المضيف للموجه ليكون R2:
```
Router(config)#hostname R2
```

```
#(R2(config
```

لاحظ أن اسم المضيف للموجه قد تغير مباشرة بعد إدخال الأمر **hostname**.أستخدم الأمر **ip domain-name** لتكوين اسم المجال على الموجه:

```
R2(config)#ip domain-name cisco.com
```

أستخدم الأمر **crypto key generate rsa** لإنشاء زوج المفاتيح R2:

```
R2(config)#crypto key generate rsa
The name for the keys will be: R2.cisco.com
Choose the size of the key modulus in the range of 360 to 2048 for your
 General Purpose Keys. Choosing a key modulus greater than 512 may take
.a few minutes

:[How many bits in the modulus [512
[Generating 512 bit RSA keys ...[OK %
```

2. استعملت هذا أمر في شامل تشكيل أسلوب in order to أعلنت إلى ال CA أن أنت ينبغي استعملت (cisco ios CA في هذا مثال) وعينت صفة ل ال trustPoint CA:

```
crypto ca trustpoint cisco
 enrollment retry count 5
enrollment retry period 3
enrollment url http://14.38.99.99:80
revocation-check none
```

ملاحظة: يقوم الأمر **crypto ca trustPoint** بتوحيد الأمر **crypto ca identity الموجود** والأمر **crypto ca trusted-root**، وبالتالي توفير الوظائف المجمعة بموجب أمر واحد.

أستخدم الأمر Cisco) **crypto ca authentication cisco** هي تسمية trustPoint) لاسترداد الشهادة الجذر من خادم CA:

```
R2(config)#crypto ca authenticate cisco
```

4. أستخدم الأمر Cisco) **crypto ca login cisco** هي تسمية TrustPoint) للتسجيل وإنشاء:

```
R2(config)#crypto ca enroll cisco
```

بعد التسجيل بنجاح إلى خادم Cisco IOS CA، يجب أن ترى الشهادات الصادرة باستخدام الأمر **show crypto ca certificates**. هذا هو مخرج الأمر. يعرض الأمر معلومات الشهادة التفصيلية، والتي تتوافق مع المعلمات التي تم تكوينها في خادم Cisco IOS CA:

```
R2#show crypto ca certificates
                                Certificate
                            Status: Available
                 Certificate Serial Number: 02
               Certificate Usage: General Purpose
                                        :Issuer
                          cn=cisco1.cisco.com
                                       l=RTP
                                        c=US
                                      :Subject
                            Name: R2.cisco.com
                          hostname=R2.cisco.com
                                :CRL Distribution Point
        http://172.18.108.26/cisco1cdp.cisco1.crl
                                    :Validity Date
          start date: 15:41:11 UTC Jan 21 2004
           end   date: 15:41:11 UTC Aug 8 2004
           renew date: 00:00:00 UTC Jan 1 1970
                   Associated Trustpoints: cisco

                                 CA Certificate
                            Status: Available
                 Certificate Serial Number: 01
```

```
Certificate Usage: Signature
                    :Issuer
          cn=cisco1.cisco.com
                      l=RTP
                       c=US
                   :Subject
          cn=cisco1.cisco.com
                      l=RTP
                       c=US
                :Validity Date
    start date: 15:39:00 UTC Jan 21 2004
    end   date: 15:39:00 UTC Jan 20 2005
      Associated Trustpoints: cisco
```

5. دخلت هذا أمر in order to أنقذت المفتاح إلى متواصل flash ذاكرة:

```
hostname(config)#write memory
```

6. دخلت هذا أمر in order to أنقذت التشكيل:

```
hostname#copy run start
```

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر **show**. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مُخرَج الأمر **show** .

- **إظهار شهادات التشفير**—يعرض الشهادات.
- **show crypto key mypubkey rsa**—يعرض زوج المفاتيح.

```
Key pair was generated at: 09:28:16 EST Jan 30 2004 %!
                    Key name: ese-ios-ca!
                Usage: General Purpose Key !
                        .Key is exportable !
                               :Key Data !
    30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00AF2198  !
    C56F1A8F 5AC501FF ADFB1489 1F503F91 CA3C3FA3 9FB2C150 FFCBF815 2AA73060  !
    E79AF510 E292C171 C6804B45 0CAAD4AF 5834AB85 B204208B 3960D20D 9B51AF7B  !
    ACF12D3D F5BC6EAE 77186AE9 1471F5A4 443CE5B5 1336EC33 5FEB3398 002C15EE  !
9F8FD331 83490D8A 983FBBE1 9E72A130 121A3B97 A3ACD147 C37DA3D6 77020301 0001  !
Key pair was generated at: 09:28:17 EST Jan 30 2004 %!
                Key name: ese-ios-ca.server!
                    Usage: Encryption Key !
                        .Key is exportable !
                               :Key Data !
    307C300D 06092A86 4886F70D 01010105 00036B00 30680261 0096456A 01AEC6A5  !
    0049CCA7 B41B675E 5317328D DF879CAE DB96A739 26F2A03E 09638A7A 99DFF8E9  !
    18F7635D 6FB6EE27 EF93B3DE 336C148A 6A7A91CB 6A5F7E1B E0084174 2C22B3E2  !
        3ABF260F 5C4498ED 20E76948 9BC2A360 1C799F8C 1B518DD8 D9020301 0001  !
```

- **crypto pki server ese-ios-ca info crl**—يعرض قائمة إلغاء الشهادة (CRL).

```
                                    :Certificate Revocation List !
 Issuer: cn=ese-ios-ca,ou=ESE,o=Cisco Systems Inc,l=Raleigh,st=NC    !
                            This Update: 09:58:27 EST Jan 30 2004    !
                            Next Update: 09:58:27 EST Jan 31 2004    !
                                    Number of CRL entries: 0    !
                                        CRL size: 300 bytes    !
```

- **طلبات معلومات PKI server ese-ios-ca**—يعرض طلبات التسجيل المعلقة.

```
                                    :Enrollment Request Database !
        ReqID  State      Fingerprint                       SubjectName !
```

```
! ------------------------------------------------------------
```

- **show crypto pki server**— يعرض حالة خادم البنية الأساسية للمفتاح العام (PKI) الحالية.

```
! Certificate Server status: enabled, configured
!                                 Granting mode is: manual
!                       Last certificate issued serial number: 0x1
!       CA certificate expiration timer: 10:58:20 EDT Jun 21 2005
!               CRL NextUpdate timer: 09:58:26 EST Jan 31 2004
!                                 :Current storage dir: nvram
!    Database Level: Names - subject name data written as .cnm
```

- **منح *تسمية خادم transAction-id*** **{Crypto PKI { all | }**—يمنح جميع طلبات SCEP أو طلبات محددة.
- **رفض خادم *transAction-id*** **{Crypto PKI *CS-Label* { all | }**—يرفض جميع طلبات SCEP أو طلبات SCEP المحددة.
- **يتم إنشاء كلمة مرور Crypto PKI server cs-label [*دقيقة*>**— يقوم بإنشاء كلمة مرور مرة واحدة (OTP) لطلب SCEP (دقائق - طول الوقت (بالدقائق) الذي تكون فيه كلمة المرور صالحة. النطاق الصالح يتراوح من 1 إلى 1440 دقيقة. الافتراضي هو 60 دقيقة.**ملاحظة:** يكون OTP واحد فقط صالحا في كل مرة. إن خلقت آخر OTP يكون، ال OTP سابق لم يعد صالح.
- **crypto pki server *cs-label* revoke *certificate-serial-number* —يلغي الشهادة بناء على رقمها التسلسلي.**
- **طلب [pem Crypto PKI server *cs-label pkcs10* {url *url* | *terminal*}]**—يضيف يدويا إما طلب تسجيل الشهادة base64 أو PEM PKCS10 إلى قاعدة بيانات الطلب.
- **crypto pki server *cs-label* info crl**—يعرض المعلومات المتعلقة بحالة CRL الحالي.
- **طلب معلومات التسمية *CS-Label* لخادم crypto pki** —يعرض جميع طلبات تسجيل الشهادة المعلقة.

راجع قسم التحقق من زوج المفاتيح الذي تم إنشاؤه في هذا المستند للحصول على معلومات تحقق إضافية.

استكشاف الأخطاء وإصلاحها

راجع أستكشاف أخطاء أمان IP وإصلاحها - فهم أوامر تصحيح الأخطاء واستخدامها للحصول على معلومات أستكشاف الأخطاء وإصلاحها.

ملاحظة: في العديد من الحالات، يمكنك حل المشاكل عند حذف خادم CA وإعادة تعريفه.

معلومات ذات صلة

- مفاوضة IPSec/بروتوكولات IKE
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).