

# هلجست و Cisco نم 3000 VPN زكرم نيوكت CA مداخلك Cisco IOS هجوم ىلإ

## المحتويات

[المقدمة](#)

[المتطلبات الأساسية](#)

[المتطلبات](#)

[المكونات المستخدمة](#)

[الرسم التخطيطي للشبكة](#)

[الاصطلاحات](#)

[إنشاء زوج مفاتيح RSA وتصديره لخدم الشهادات](#)

[تصدير زوج المفاتيح الذي تم إنشاؤه](#)

[التحقق من زوج المفاتيح الذي تم إنشاؤه](#)

[تمكين خادم HTTP على الموجه](#)

[تمكين خادم CA وتكوينه على الموجه](#)

[تكوين مركز VPN 3000 من Cisco وتسجيله](#)

[التحقق من الصحة](#)

[استكشاف الأخطاء وإصلاحها](#)

[معلومات ذات صلة](#)

## المقدمة

يوضح هذا المستند كيفية تكوين موجه Cisco IOS ® كخادم مرجع شهادات (CA). وبالإضافة إلى ذلك، يوضح كيفية تسجيل مركز Cisco VPN 3000 إلى موجه Cisco IOS للحصول على شهادة جذر ومعرف لمصادقة IPSec.

## المتطلبات الأساسية

### المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

### المكونات المستخدمة

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

• الموجه Cisco 2600 Series Router الذي يعمل ببرامج Cisco IOS Software، الإصدار 12.3(4)T3

• Cisco VPN 3030 Concentrator، الإصدار 4.1.2

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

للحصول على مزيد من المعلومات حول اصطلاحات المستندات، ارجع إلى [اصطلاحات تلميحات Cisco التقنية](#).

## إنشاء زوج مفاتيح RSA وتصديره ل خادم الشهادات

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

```
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 استخدام نفس اسم زوج المفاتيح (تسمية المفتاح) الذي تخطط لاستخدامها ل خادم الشهادة (عبر الأمر `crypto pki server cs-label` الذي تمت تغطيته لاحقاً).

## تصدير زوج المفاتيح الذي تم إنشاؤه

ثم يلزم تصدير المفاتيح إلى ذاكرة الوصول العشوائي غير المتطايرة (NVRAM) أو TFTP (استناداً إلى التكوين الخاص بك). في هذا المثال، يتم استخدام ذاكرة NVRAM. بناء على التطبيق الخاص بك، قد ترغب في استخدام 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 هو موضح هنا:

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

**ملاحظة:** إذا لم تكن ترغب في أن يكون المفتاح قابلاً للتصدير من خادم الشهادات، قم بإستيراده مرة أخرى إلى خادم الشهادات بعد تصديره كزوج مفاتيح غير قابل للتصدير. لذلك، لا يمكن إزالة المفتاح مرة أخرى.

## التحقق من زوج المفاتيح الذي تم إنشاؤه

يمكنك التحقق من زوج المفاتيح الذي تم إنشاؤه من خلال إستدعاء الأمر `show crypto key mypubkey rsa`:

يتم دعم بعض أوامر العرض بواسطة [أداة مترجم الإخراج \(العملاء المسجلون فقط\)](#)، والتي تتيح لك عرض تحليل [إخراج أمر العرض](#).

```
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 AECDD9C 07AD84DD 89020301 0001
```

## تمكين خادم HTTP على الموجه

يُدمع خادم Cisco IOS CA عمليات التسجيل التي تتم عبر بروتوكول تسجيل الشهادة البسيط (SCEP) فقط. وبالتالي، ولجعل هذا ممكناً، يجب أن يقوم الموجه بتشغيل خادم Cisco IOS HTTP المدمج. ولتمكينها، أستخدم الأمر `ip http server`:

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

## تمكين خادم CA وتكوينه على الموجه

اتبع هذا الإجراء.

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

التسمية مع تسمية زوج المفاتيح التي تم إنشاؤها:

```
R1(config)#crypto pki server cisco1
```

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

2. يحدد الأمر قاعدة البيانات url الموقع الذي تتم فيه كتابة جميع إدخلات قاعدة البيانات لخادم CA. إذا لم يتم تحديد هذا الأمر، فسيتم كتابة جميع إدخلات 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 دون 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، فأنت تحتاج أيضا إلى تحديد خادم TFTP خارجي يتم فيه تخزين البيانات عبر الأمر `database url`.

4. قم بتكوين اسم مصدر CA إلى سلسلة DN المحددة. في هذا المثال، يتم استخدام 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 3 سنوات، وفترة بقاء الشهادة الافتراضية هي سنة واحدة. مدة صلاحية الشهادة القصوى أقل من مدة صلاحية شهادة المرجع المصدق (CA) بشهر واحد. على سبيل المثال:

```
R1(cs-server)#lifetime ca-certificate 365
```

```
R1(cs-server)#lifetime certificate 200
```

6. حدد فترة بقاء CRL، بالساعات، التي يتم استخدامها من قبل خادم الشهادات. قيمة الحد الأقصى لعمر الحياة هي 336 ساعة (أسبوعان). القيمة الافتراضية هي 168 ساعة (1 أسبوع).

```
R1(cs-server)#lifetime crl 24
```

7. قم بتعريف نقطة توزيع قائمة إبطال الشهادات (CDP) ليتم استخدامها في الشهادات التي يتم إصدارها بواسطة خادم الشهادات. يجب أن يكون URL HTTP URL. على سبيل المثال، عنوان IP الخاص بالخادم هو `172.18.108.26`.

```
R1(cs-server)#cdp-url http://172.18.108.26/cisco1cdp.cisco1.crl
```

8. قم بتمكين خادم CA بإصدار الأمر `no shutdown`.

```
R1(cs-server)#no shutdown
```

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

## تكوين مركز VPN 3000 من Cisco وتسجيله

اتبع هذا الإجراء.

1. حدد إدارة>إدارة الشهادات واختر انقر هنا لتثبيت شهادة CA لاسترداد الشهادة الجذر من خادم Cisco IOS .CA

Administration | Certificate Management Sunday, 25 January 2004 08:47:49 Refresh

This section lets you view and manage certificates on the VPN 3000 Concentrator. Installation of a CA certificate is required before identity and SSL certificates can be installed.

- [Click here to install a CA certificate](#)
- [Click here to enroll with a Certificate Authority](#)
- [Click here to install a certificate](#)

**Certificate Authorities** [ [View All CRL Caches](#) | [Clear All CRL Caches](#) ] (current: 0, maximum: 20)

Subject	Issuer	Expiration	SCEP Issuer	Actions
No Certificate Authorities				

**Identity Certificates** (current: 0, maximum: 20)

Subject	Issuer	Expiration	Actions
No Identity Certificates			

2. حدد SCEP كطريقة

Administration | Certificate Management | Install | CA Certificate

Choose the method of installation:

- [SCEP \(Simple Certificate Enrollment Protocol\)](#)
- [Cut & Paste Text](#)
- [Upload File from Workstation](#)

[<< Go back to and choose a different type of certificate](#)

للتثبيت.

3. أدخل عنوان URL الخاص بخادم Cisco IOS CA، وهو واصل CA، وانقر فوق إسترداد. ملاحظة: عنوان URL الصحيح في هذا المثال هو <http://14.38.99.99/cgi-bin/pkiclient.exe> (يجب أن تقوم بتضمين المسار الكامل لـ [cgi-/ \(bin/pkiclient.exe\)](http://14.38.99.99/cgi-bin/pkiclient.exe)).

Administration | Certificate Management | Install | CA Certificate | SCEP

Enter the information needed to retrieve the CA certificate via SCEP. Please wait for the operation to complete.

URL

CA Descriptor:  Required for some PKI configurations.

حدد إدارة < إدارة الشهادات للتحقق من تثبيت الشهادة الجذر. يوضح هذا الشكل تفاصيل الشهادة الجذر.

Administration | Certificate Management Sunday, 25 January 2004 08:52:23  
Refresh

This section lets you view and manage certificates on the VPN 3000 Concentrator.

- [Click here to enroll with a Certificate Authority](#)
- [Click here to install a certificate](#)

**Certificate Authorities** [ [View All CRL Caches](#) | [Clear All CRL Caches](#) ] (current: 1, maximum: 20)

Subject	Issuer	Expiration	SCEP Issuer	Actions
cisco1.cisco.com	cisco1.cisco.com	01/20/2005	Yes	<a href="#">View</a>   <a href="#">Configure</a>   <a href="#">Delete</a>   <a href="#">SCEP</a>

**Identity Certificates** (current: 0, maximum: 20)

Subject	Issuer	Expiration	Actions
No Identity Certificates			

4. حدد انقر هنا للتسجيل مع مرجع شهادة للحصول على شهادة المعرف من خادم Cisco IOS .CA

Administration | Certificate Management Sunday, 25 January 2004 08:52:23  
Refresh

This section lets you view and manage certificates on the VPN 3000 Concentrator.

- [Click here to enroll with a Certificate Authority](#)
- [Click here to install a certificate](#)

**Certificate Authorities** [ [View All CRL Caches](#) | [Clear All CRL Caches](#) ] (current: 1, maximum: 20)

Subject	Issuer	Expiration	SCEP Issuer	Actions
cisco1.cisco.com	cisco1.cisco.com	01/20/2005	Yes	<a href="#">View</a>   <a href="#">Configure</a>   <a href="#">Delete</a>   <a href="#">SCEP</a>

**Identity Certificates** (current: 0, maximum: 20)

Subject	Issuer	Expiration	Actions
No Identity Certificates			

5. حدد التسجيل عبر SCEP في cisco1.cisco.com ( cisco1.cisco.com هو CN لخادم Cisco IOS .CA)

Select the enrollment method for the identity certificate. To install a certificate with SCEP, the issuing CA's certificate must also be installed with SCEP. [Click here to install a new CA using SCEP before enrolling.](#)

- [Enroll via PKCS10 Request \(Manual\)](#)
- [Enroll via SCEP at cisco1.cisco.com](#)

[<< Go back to Certificate Management](#)

6. أكمل نموذج التسجيل بإدخال جميع المعلومات التي سيتم تضمينها في طلب الشهادة. بعد إكمال النموذج، انقر فوق تسجيل لبدء طلب التسجيل إلى خادم CA.

Enter the information to be included in the certificate request. Please wait for the operation to finish.

Common Name (CN)	<input type="text" value="rtp-vpn3000"/>	Enter the common name for the VPN 3000 Concentrator to be used in this PKI.
Organizational Unit (OU)	<input type="text" value="TAC"/>	Enter the department.
Organization (O)	<input type="text" value="Cisco"/>	Enter the Organization or company.
Locality (L)	<input type="text" value="RTP"/>	Enter the city or town.
State/Province (SP)	<input type="text" value="NC"/>	Enter the State or Province.
Country (C)	<input type="text" value="US"/>	Enter the two-letter country abbreviation (e.g. United States = US).
Subject AlternativeName (FQDN)	<input type="text"/>	Enter the Fully Qualified Domain Name for the VPN 3000 Concentrator to be used in this PKI.
Subject AlternativeName (E-Mail Address)	<input type="text"/>	Enter the E-Mail Address for the VPN 3000 Concentrator to be used in this PKI.
Challenge Password	<input type="text"/>	Enter and verify the challenge password for this certificate request.
Verify Challenge Password	<input type="text"/>	
Key Size	<input type="text" value="RSA 512 bits"/>	Select the key size for the generated RSA key pair.

بعد النقر فوق تسجيل، يعرض مركز VPN 3000 "تم إنشاء طلب شهادة".

A certificate request has been generated.

SCEP Status: Installed

- [Go to Certificate Management](#)
- [Go to Certificate Enrollment](#)
- [Go to Certificate Installation](#)

ة: يمكن تكوين خادم Cisco IOS CA لمنح الشهادات تلقائياً باستخدام الأمر الفرعي Cisco IOS CA Server. يتم استخدام هذا الأمر لهذا المثال. لمشاهدة تفاصيل شهادة المعرف، حدد إدارة < إدارة الشهادات. الشهادة المعروضة مشابهة لهذا.

Administration | Certificate Management Sunday, 25 January 2004

This section lets you view and manage certificates on the VPN 3000 Concentrator.

- [Click here to enroll with a Certificate Authority](#)
- [Click here to install a certificate](#)

**Certificate Authorities** [[View All CRL Caches](#) | [Clear All CRL Caches](#)] (current: 1, maximum: 20)

Subject	Issuer	Expiration	SCEP Issuer	Actions
cisco1.cisco.com	cisco1.cisco.com	01/20/2005	Yes	<a href="#">View</a>   <a href="#">Configure</a>   <a href="#">Delete</a>   <a href="#">SCEP</a>

**Identity Certificates** (current: 1, maximum: 20)

Subject	Issuer	Expiration	Actions
rtp-vpn3000 at Cisco	cisco1.cisco.com	08/12/2004	<a href="#">View</a>   <a href="#">Renew</a>   <a href="#">Delete</a>

## التحقق من الصحة

راجع قسم [التحقق من زوج المفاتيح الذي تم إنشاؤه](#) للحصول على معلومات التحقق.

## استكشاف الأخطاء وإصلاحها

أحلت لمعلومة يتحرق، يتحرق توصيل مشكلة على ال VPN 3000 مركز أو ip أمن يتحرق - يفهم ويستعمل أمر [.debug](#).

## معلومات ذات صلة

- [صفحة دعم مركز Cisco VPN 3000 Series](#)
- [صفحة دعم عميل Cisco VPN 3000 Series](#)
- [صفحة دعم IPSec](#)
- [الدعم الفني - Cisco Systems](#)



ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت  
ملاعلاء انء مء مء نمة دختسمل معد و تمة مء دقتل ةر شبل او  
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب  
Cisco ةللخت. فرتمة مچرت مء دقء ةللأل ةل فارتحال ةمچرتل عم لاعل او  
ىل إأمءءاد ءوچرلاب ةصوءو تامةرتل هذه ةقء نء اهءل وئس م Cisco  
Systems (رفوتم طبارل) ةل صأل ةل ءل ءن إل دن تسمل