

# لائحة مداخلت سواب Cisco IOS ةداهش ليجست ةنسح م ل ليجست ل رماو نيوكت

## المحتويات

- [المقدمة](#)
- [المتطلبات الأساسية](#)
- [المتطلبات](#)
- [المكونات المستخدمة](#)
- [الاصطلاحات](#)
- [معلومات أساسية](#)
- [التكوين](#)
- [الرسم التخطيطي للشبكة](#)
- [التكوينات](#)
- [التحقق من الصحة](#)
- [إعادة إنشاء زوج مفاتيح RSA](#)
- [عندما لا يكون زوج مفاتيح RSA موجودا](#)
- [عند انتهاء صلاحية شهادة الهوية](#)
- [استكشاف الأخطاء وإصلاحها](#)
- [أوامر استكشاف الأخطاء وإصلاحها](#)
- [تصحيح الأخطاء على الموجهات](#)
- [معلومات ذات صلة](#)

## المقدمة

يوضح هذا المستند استخدام أوامر التسجيل التلقائي للشهادة المحسنة. هذه الميزة هي تحسين يستهدف تسهيل إدارة الشهادات على الموجهات. تقدم ميزة التسجيل التلقائي للشهادة خمسة أوامر فرعية جديدة إلى الأمر `crypto ca trustPoint`. هذه الأوامر هي `(ip-address (ca-trustPoint` و `(password (ca-trustPoint` و `serial-number` و `subject-name` و `use`. توفر هذه الأوامر خيارات جديدة لطلبات الشهادات وتسمح للمستخدمين بتحديد حقول في التكوين بدلا من الاضطرار إلى المرور عبر المطالبات. ومع ذلك، يبقى سلوك المطالبة هو السلوك الافتراضي إذا لم يتم تمكين هذه الميزة. يمكن للمستخدمين تحميل جميع المعلومات الضرورية مسبقا في التكوين. وهذا يسمح لكل موجه بالحصول على شهادته تلقائيا عند التمهييد.

تقوم "سلطات التصديق لنقطة الثقة" (CAs) بدمج واستبدال وظائف هوية و CAs الجذر الموثوق به. وبالتالي، يهمل الأمر `crypto ca trustPoint` هوية التشفير و `crypto ca trusted-root` الأوامر. كما تتم مناقشة أوامر وصف التسجيل التلقائي وإعادة الإنشاء و `rsa-key` في هذا المستند.

ارجع إلى [كيفية الحصول على شهادة رقمية من مرجع مصدق Microsoft Windows باستخدام ASDM على ASA](#) لمعرفة المزيد حول نفس السيناريو مع PIX/ASA 7.x.

ارجع إلى [تكوين مركز Cisco VPN 3000 4.7.x للحصول على شهادة رقمية وشهادة SSL](#) لمعرفة المزيد حول نفس السيناريو مع مركز Cisco VPN 3000 Series Concentrator.

# المتطلبات الأساسية

## المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

## المكونات المستخدمة

تنطبق المعلومات الواردة في هذا المستند على إصدارات البرامج والمكونات المادية التالية.

• الموجهات 7204 و 2611 و 1720 من Cisco

• خوادم الشهادات المستقلة ل Microsoft

• برنامج IOS® الإصدار 12.2(12.10)T و 12.2.11T من Cisco

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.

## الاصطلاحات

راجع [اصطلاحات تلمحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.](#)

## معلومات أساسية

بالإضافة إلى أوامر تسجيل الشهادة، تتم مناقشة مختلف أوامر تحسين تسجيل الشهادة هذه:

- **crypto ca trustPoint** — يعلن المرجع المصدق الذي يجب أن يستخدمه الموجه.
- **اسم الموضوع [x.500-name]** — يحدد اسم الموضوع في طلب الشهادة. إذا لم يتم استخدام الأمر الفرعي **subject-name**، بشكل افتراضي، يتم استخدام اسم المجال المؤهل بالكامل (FQDN) للموجه. ويتم استخدام هذا في وضع تكوين **ca-trustPoint**. على سبيل المثال، تتسبب اسم **X.500** هو اسم الموضوع **OU=Rome**، **O=Italy**.
- **عنوان IP (عنوان interface | IP)** — يحدد عنوان IP منقطع أو واجهة يتم تضمينها في طلب الشهادة. ويتم استخدام هذا في وضع تكوين **ca-trustPoint**.
- **كلمة السر خيط** — يعين الإبطال كلمة للشهادة. ويتم استخدام هذا في وضع تكوين **ca-trustPoint**. بما أن قائمة إبطال الشهادة (CRL) غير مستخدمة في هذا المستند، فإنه يتم تعيين جميع كلمات المرور على "بلا".
- **الرقم التسلسلي [none]** — يحدد ما إذا كان يجب تضمين رقم تسلسلي في طلب الشهادة. ويتم استخدام هذا في وضع تكوين **ca-trustPoint**.
- **أسلوب الاستخدام 1 [method2، method3]** — يحدد الاستخدام المقصود للشهادة. الخيارات المتاحة هي **(Internet Key Exchange (IKE و SSL-client و SSL-server)**. الاستخدام في هذا المستند هو **IKE**. ويتم استخدام هذا في وضع تكوين **ca-trustPoint**.
- **التسجيل التلقائي [regenerate]** — الطلب التلقائي لشهادة موجه من المرجع المصدق التي تستخدم المعلومات في التكوين. يقوم هذا الأمر بإنشاء مفتاح **(Rivest-Shamir-Adelman (RSA** جديد فقط في حالة عدم وجود مفتاح جديد مع التسمية المطلوبة. يتم استخدام هذا الأمر في وضع تكوين **ca-trustPoint**، للتحقق من شهادات الموجه منتهية الصلاحية. نقطة ثقة يتم تكوينها لمحاولات التسجيل التلقائي لإعادة التسجيل عند انتهاء صلاحية شهادة الموجه. من مزايا هذا الأمر أن بعض فئات **CA** تتطلب مفتاحاً جديداً لإعادة التسجيل للعمل. لذلك، يتم استخدام الأمر الفرعي لإنشاء مفتاح جديد. يتم إجراء التسجيل التلقائي عند بدء التشغيل لأي مرجع مصدق من نوع **TrustPoint** تم تكوينه ولا يحتوي على شهادة صالحة. عند انتهاء صلاحية الشهادة التي يتم إصدارها بواسطة مرجع مصدق ثقة (تم تكوينه للتسجيل التلقائي)، يتم طلب شهادة جديدة. على الرغم من أن هذه الميزة لا توفر

تجديد الشهادة بسلاسة، إلا أنها توفر إسترداد غير مراقب من انتهاء صلاحية.

• استخدام هذا الأمر في وضع تكوين ca-trustPoint. في كثير من الحالات، يمكن طلب موجه للتسجيل باستخدام خوادم شهادات متعددة. ومع ذلك، يمكن أن يكون لكل خادم مرجع مصدق متطلبات نهج مختلفة (مثل طول المفتاح). يسمح هذا الأمر الفرعي بإقران أزواج مفاتيح RSA من أحجام مختلفة لشهادات الهوية من خوادم CA المختلفة. إذا لم يتم استخدام الأمر الفرعي، فسيتم استخدام الموجه FQDN بشكل افتراضي. يتم إنشاء تسمية المفتاح أثناء التسجيل إذا لم تكن موجودة بالفعل أو إذا تم إصدار أمر إعادة إنشاء التسجيل التلقائي. حدد حجم المفتاح لإنشاء المفتاح وحدد حجم مفتاح التشفير لطلب تشفير منفصل، مفاتيح التوقيع، والشهادات. على سبيل المثال:

```
2611-VPN(config)#crypto ca trustpoint caserver2
2611-VPN(ca-trustpoint)#rsa-keypair tacvpn 512 512
```

**ملاحظة:** بشكل افتراضي، تطلب ميزة التسجيل التلقائي شهادة جديدة عند انتهاء صلاحية الشهادة القديمة. يمكن فقد الاتصال أثناء خدمة الطلب لأنه يتم حذف أزواج الشهادات والمفتاح الحالية مباشرة بعد إنشاء المفتاح الجديد. لا يحتوي المفتاح الجديد على شهادة لمطابقته حتى تكتمل العملية، ولا يمكن إنشاء إتصالات IKE الواردة حتى يتم إصدار الشهادة الجديدة. تتيح ميزة "إعادة توجيه المفاتيح لتجديد الشهادة" التي إدخالها في الإصدار 12.3(7)T من برنامج Cisco IOS Software إمكانية إجراء طلب تجديد الشهادة قبل انتهاء صلاحية الشهادة والاحتفاظ بالمفتاح القديم والشهادة إلى أن تتوفر الشهادة الجديدة. للحصول على معلومات إضافية حول هذه الميزة، ارجع إلى [إعادة توجيه المفتاح لتجديد الشهادة](#).

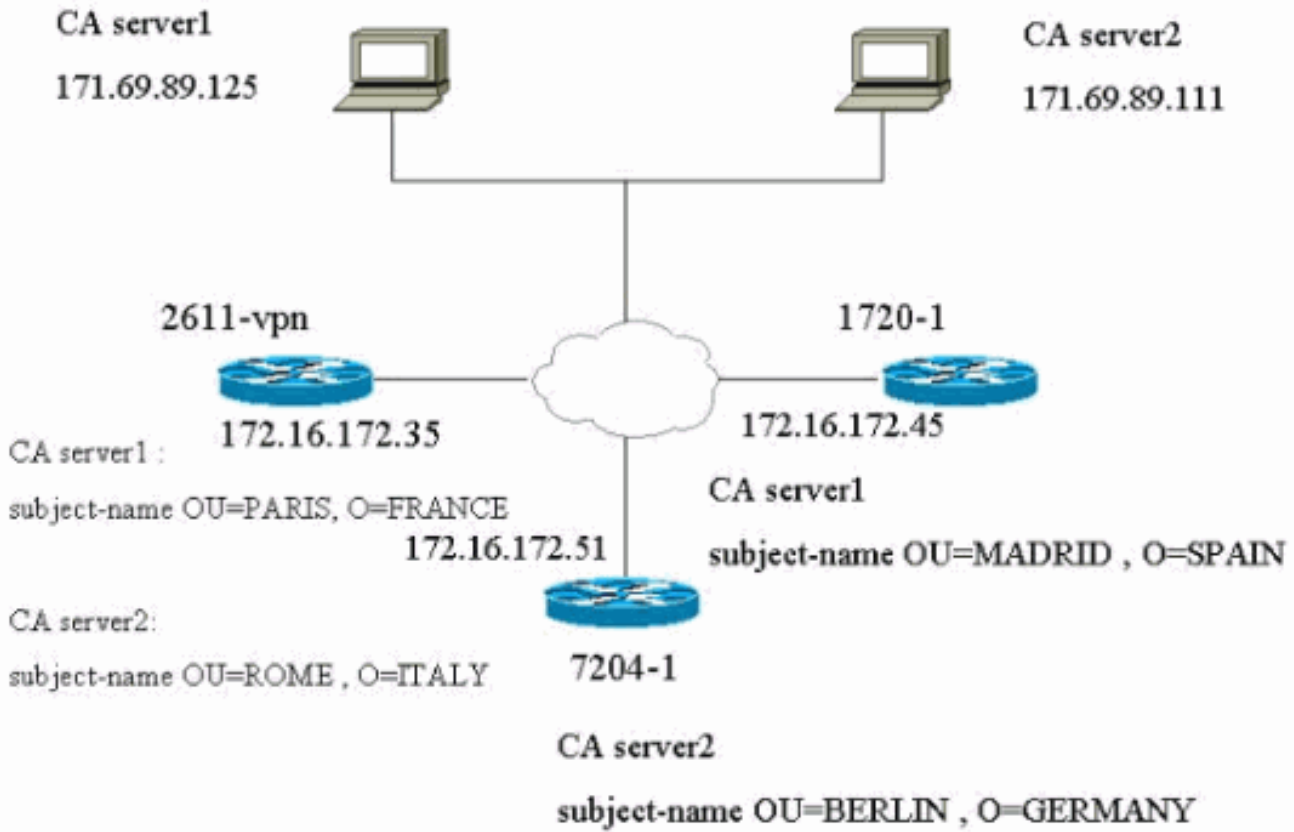
## التكوين

يقدم لك هذا القسم معلومات تكوين الميزات التي يصفها هذا المستند.

**ملاحظة:** استخدم [أداة بحث الأوامر](#) (للعلماء [المسجلين](#) فقط) للعثور على مزيد من المعلومات حول الأوامر المستخدمة في هذا المستند.

## الرسم التخطيطي للشبكة

يوضح الرسم التخطيطي للشبكة الموجهات المستخدمة في المختبر، وخوادم CA، واسم موضوع شهادات الهوية التي تم الحصول عليها من الموجه من خادمي CA.



## التكوينات

يستخدم هذا المستند هذه التكوينات. ال VPN-2611 مسحاج تحديد الصرة أي يكون سجلت في على حد سواء CA نادل 1 و CA نادل 2. تم تسجيل الموجه 1-2611 مع خادم CA1 وتم تسجيل الموجه 1-7204 مع خادم CA2.

- تكوين موجه صرة VPN-2611 والشهادات الخاصة به من خادمي CA مختلفين
- تكوين الموجه 1-1720 والشهادات من خادم CA 1
- تكوين الموجه 1-7204 والشهادات من خادم CA2

### تكوين موجه صرة VPN-2611 والشهادات الخاصة به من خادمي CA مختلفين

```

show verify
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-IK8S-M), Version
,12.2(12.10)T
MAINTENANCE INTERIM SOFTWARE
TAC Support: http://www.cisco.com/tac
.Copyright (c) 1986-2002 by cisco Systems, Inc
Compiled Fri 27-Sep-02 21:25 by ccai
Image text-base: 0x80008098, data-base: 0x819B8124

ROM: System Bootstrap, Version 11.3(2)XA4, RELEASE
(SOFTWARE (fc1
ROM: C2600 Software (C2600-IK8S-M), Version

```

,12.2(12.10)T

MAINTENANCE INTERIM SOFTWARE

2611-VPN uptime is 18 hours, 16 minutes  
System returned to ROM by reload  
System restarted at 04:00:46 UTC Sun Oct 27 2002  
"System image file is "flash:c2600-ik8s-mz.122-12.10.t

cisco 2611 (MPC860) processor (revision 0x203) with  
59392K/6144K  
.bytes of memory  
(Processor board ID JAD03456979 (1914264035  
M860 processor: part number 0, mask 49  
.Bridging software  
.X.25 software, Version 3.0.0  
(Ethernet/IEEE 802.3 interface(s 2  
(Low-speed serial(sync/async) network interface(s 4  
(Virtual Private Network (VPN) Module(s 1  
.32K bytes of non-volatile configuration memory  
16384K bytes of processor board System flash  
(Read/Write

Configuration register is 0x2102

2611-VPN#**show run**  
...Building configuration

Current configuration : 15431 bytes  
!  
Last configuration change at 22:09:05 UTC Sun Oct 27 2002  
!  
version 12.2  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
!  
hostname 2611-VPN  
!  
memory-size iomem 10  
ip subnet-zero  
!  
ip domain name cisco.com  
ip host caserver2 171.69.89.111  
ip host caserver1 171.69.89.125  
!  
!  
**crypto ca trustpoint caserver1**  
**enrollment retry period 5**  
**enrollment mode ra**  
**enrollment url**  
**http://171.69.89.125:80/certsrv/mscep/mscep.dll**  
**usage ike**  
**serial-number**  
**fqdn 2611-vpn.cisco.com**  
**ip-address Ethernet0/0**  
**password 7 1107160B12**  
**subject-name OU=PARIS O=FRANCE**  
**crl optional**  
**rsakeypair ciscovpn**  
**auto-enroll regenerate**  
!

```

crypto ca trustpoint caserver2
  enrollment retry period 5
  enrollment mode ra
  enrollment url
http://171.69.89.111:80/certsrv/mscep/mscep.dll
  usage ike
  serial-number
  fqdn 2611-vpn.cisco.com
  ip-address Ethernet0/0
  password 7 130B181C0E
  subject-name OU=ROME O=ITALY
  rsakeypair tacvpn
  auto-enroll regenerate
crypto ca certificate chain caserver1
certificate ca 0E7EC1B68A2F14BD4C4515AF44C45732
308202BE 30820268 A0030201 0202100E 7EC1B68A 2F14BD4C
4515AF44 C4573230
0D06092A 864886F7 0D010105 05003076 310B3009 06035504
06130255 53310B30
Certificate is abbreviated for easier viewing. quit ---!
certificate 6103EE0A0000000000038 3082040F 308203B9
A0030201 02020A61 03EE0A00 00000000 38300D06 092A8648
86F70D01 01050500 3076310B 30090603 55040613 02555331
0B300906 03550408 13024341 3111300F 06035504 07130853
616E204A 6F736531 16301406 0355040A !--- Certificate is
abbreviated for easier viewing. quit certificate
6104020F00000000000039 3082040F 308203B9 A0030201 02020A61
04020F00 00000000 39300D06 092A8648 86F70D01 01050500
3076310B 30090603 55040613 02555331 0B300906 03550408
13024341 3111300F 06035504 07130853 616E204A 6F736531
16301406 0355040A !--- Certificate is abbreviated for
easier viewing. quit crypto ca certificate chain
caserver2
certificate 3DAA9059000000000033
308203CF 30820379 A0030201 02020A3D AA905900 00000000
33300D06 092A8648
86F70D01 01050500 3061310B 30090603 55040613 02555331
13301106 03550408
130A6361 6C69666F 726E6961 3111300F 06035504 07130873
616E206A 6F736531
Certificate is abbreviated for easier viewing. quit ---!
certificate 3DAA867D000000000032 308203CF 30820379
A0030201 02020A3D AA867D00 00000000 32300D06 092A8648
86F70D01 01050500 3061310B 30090603 55040613 02555331
13301106 03550408 130A6361 6C69666F 726E6961 3111300F
06035504 07130873 616E206A 6F736531 !--- Certificate is
abbreviated for easier viewing. quit certificate ca
3E34CD199392A0914621EA778B13F357 30820284 3082022E
A0030201 0202103E 34CD1993 92A09146 21EA778B 13F35730
0D06092A 864886F7 0D010105 05003061 310B3009 06035504
06130255 53311330 11060355 0408130A 63616C69 666F726E
69613111 300F0603 55040713 0873616E !--- Certificate is
abbreviated for easier viewing. quit ! crypto isakmp
policy 10 hash md5 crypto isakmp identity hostname ! !
crypto ipsec transform-set myset esp-des esp-md5-hmac !
crypto map vpn 10 ipsec-isakmp set peer 172.16.172.45
set transform-set myset match address 101 crypto map vpn
20 ipsec-isakmp set peer 172.16.172.51 set transform-set
myset match address 102 crypto map vpn 30 ipsec-isakmp
set peer 172.16.172.53 set transform-set myset match
address 103 ! mta receive maximum-recipients 0 ! ! ! !
interface Ethernet0/0 ip address 172.16.172.35
255.255.255.240 half-duplex crypto map vpn ! interface
Ethernet0/1 ip address 192.168.4.1 255.255.255.0 half-

```

```
duplex ! interface Serial1/0 no ip address shutdown !
interface Serial1/1 no ip address shutdown ! interface
Serial1/2 no ip address shutdown ! interface Serial1/3
no ip address shutdown ! ip classless ip route 0.0.0.0
0.0.0.0 172.16.172.33 ip http server ! access-list 101
    permit ip 192.168.4.0 0.0.0.255 20.1.1.0 0.0.0.255
access-list 102 permit ip 192.168.4.0 0.0.0.255 3.3.3.0
    0.0.0.255 access-list 103 permit ip 192.168.4.0
    0.0.0.255 200.1.1.0 0.0.0.255 access-list 169 deny ip
    host 172.16.172.60 any access-list 169 deny ip host
    172.16.172.61 any access-list 169 deny ip host
    172.16.172.62 any access-list 169 permit ip any any !
call rsvp-sync ! ! mgcp profile default ! ! ! dial-peer
cor custom ! ! ! ! ! line con 0 line aux 0 line vty 0 4
login ! ! end
```

## تكوين الموجه 1-1720 والشهادات من خادم CA 1

```
show verify
Cisco Internetwork Operating System Software
IOS (tm) C1700 Software (C1700-K9SY7-M), Version
    12.2(11)T, RELEASE
    (SOFTWARE (fc1
    TAC Support: http://www.cisco.com/tac
    .Copyright (c) 1986-2002 by cisco Systems, Inc
    Compiled Wed 31-Jul-02 12:28 by ccai
Image text-base: 0x80008124, data-base: 0x80D1654C
ROM: System Bootstrap, Version 12.0(3)T, RELEASE
    (SOFTWARE (fc1

    uptime is 18 hours, 50 minutes 1720-1
System returned to ROM by reload at 12:03:01 UTC Fri Oct
    25 2002
    System restarted at 03:28:54 UTC Sun Oct 27 2002
"System image file is "flash:c1700-k9sy7-mz.122-11.T.bin

cisco 1720 (MPC860T) processor (revision 0x601) with
    44237K/4915K bytes
    .of memory
Processor board ID JAD0449013N (791802990), with
    hardware revision
    0000
MPC860T processor: part number 0, mask 32
    .Bridging software
    .X.25 software, Version 3.0.0
    (Ethernet/IEEE 802.3 interface(s 1
    (FastEthernet/IEEE 802.3 interface(s 1
    (Serial network interface(s 1
    (Virtual Private Network (VPN) Module(s 1
    WIC T1-DSU
    .32K bytes of non-volatile configuration memory
    16384K bytes of processor board System flash
    ((Read/Write

Configuration register is 0x2102

1720-1#show run
...Building configuration
```

```

Current configuration : 8177 bytes
!
Last configuration change at 21:05:50 UTC Sun Oct 27 2002
NVRAM config last updated at 04:03:16 UTC Tue Oct 26 2004
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname 1720-1
!
!
username cisco password 0 cisco
ip subnet-zero
!
!
no ip domain lookup
ip domain name tac.com
ip host caserver1 171.69.89.125
!
!

crypto ca trustpoint caserver1
enrollment retry count 5
enrollment retry period 2
enrollment mode ra
enrollment url
http://171.69.89.125:80/certsrv/mscep/mscep.dll
usage ike
serial-number
ip-address FastEthernet0
subject-name OU=MADRID O=SPAIN
crl optional
rsaкеypair ipsecpki
auto-enroll 100 regenerate
crypto ca certificate chain caserver1
certificate ca 0E7EC1B68A2F14BD4C4515AF44C45732
308202BE 30820268 A0030201 0202100E 7EC1B68A 2F14BD4C
4515AF44
C4573230
0D06092A 864886F7 0D010105 05003076 310B3009 06035504
06130255
53310B30
Certificate is abbreviated for easier viewing. quit ---!
certificate 611652F7000000000003A 30820407 308203B1
A0030201 02020A61 1652F700 00000000 3A300D06 092A8648
86F70D01 01050500 3076310B 30090603 55040613 02555331
0B300906 03550408 !--- Certificate is abbreviated for
easier viewing. quit certificate 61165F5B000000000003B
30820407 308203B1 A0030201 02020A61 165F5B00 00000000
3B300D06 092A8648 86F70D01 01050500 3076310B 30090603
55040613 02555331 0B300906 03550408 !--- Certificate is
abbreviated for easier viewing. quit ! crypto isakmp
policy 10 hash md5 crypto isakmp identity hostname ! !
crypto ipsec transform-set myset esp-des esp-md5-hmac
crypto map vpn 10 ipsec-isakmp set peer 172.16.172.35
set transform-set myset match address 102 ! ! ! !
interface Loopback0 ip address 20.1.1.1 255.255.255.0 !

```



```
interface Ethernet0 no ip address shutdown half-duplex !
interface FastEthernet0 ip address 172.16.172.45
255.255.255.240 speed auto crypto map vpn ! interface
Serial0 no ip address no keepalive shutdown ! ip
classless ip route 0.0.0.0 0.0.0.0 172.16.172.33 ip http
server ! ! access-list 1 permit 10.1.1.0 0.0.0.255
access-list 102 permit ip 20.1.1.0 0.0.0.255 192.168.4.0
0.0.0.255 ! ! line con 0 line aux 0 line vty 0 4 login !
ntp clock-period 17179867 ntp master 1 end
```

## تكوين الموجه 1-7204 والشهادات من خادم CA2

```
show verify
Cisco Internetwork Operating System Software
IOS (tm) 7200 Software (C7200-JK903S-M), Version
,12.2(11)T1
(RELEASE SOFTWARE (fc2
TAC Support: http://www.cisco.com/tac
.Copyright (c) 1986-2002 by cisco Systems, Inc
Compiled Sat 28-Sep-02 12:29 by ccai
Image text-base: 0x60008940, data-base: 0x61D72000
ROM: System Bootstrap, Version 12.1(20000824:081033)
[dbeazley-cosmos_e_LATEST
DEVELOPMENT SOFTWARE ,[101

uptime is 1 hour, 16 minutes 7204-1
System returned to ROM by reload at 23:22:25 PST Sat Oct
25 2003
System restarted at 21:07:06 PST Sat Oct 26 2002
System image file is "slot0:c7200-jk9o3s-mz.122-
"11.T1.bin

cisco 7204VXR (NPE300) processor (revision D) with
122880K/40960K bytes
.of memory
Processor board ID 23663249
R7000 CPU at 262Mhz, Implementation 39, Rev 2.1, 256KB
L2, 2048KB L3
Cache
slot VXR midplane, Version 2.3 4

Last reset from power-on
.Bridging software
.X.25 software, Version 3.0.0
SuperLAT software (copyright 1990 by Meridian Technology
.(Corp
.TN3270 Emulation software
(Ethernet/IEEE 802.3 interface(s 4
(HSSI network interface(s 1
.125K bytes of non-volatile configuration memory

20480K bytes of Flash PCMCIA card at slot 0 (Sector size
.(128K
.(4096K bytes of Flash internal SIMM (Sector size 256K
Configuration register is 0x2102

7204-1#show run
```

```

...Building configuration

Current configuration : 8245 bytes
!
version 12.2
service timestamps debug datetime
service timestamps log datetime
no service password-encryption
service udp-small-servers
service tcp-small-servers
no service dhcp
!
hostname 7204-1
!
boot system flash slot
boot system flash slot0:c7200-jk9o3s-mz.122-11.T1.bin
logging buffered 50000 debugging
enable secret 5 $1$l0d0$bXKx.l0gHbotsggIli0UL0
enable password tajmahal
!
username cisco password 0 cisco
clock timezone PST -7
ip subnet-zero
!

no ip domain lookup
ip domain name cisco.com
ip host caserver2 171.69.89.111
!
!
ip vrf test
no ip cef
ip audit notify log
ip audit po max-events 100
!
crypto ca trustpoint caserver2
enrollment retry period 2
enrollment mode ra
enrollment url
http://171.69.89.111:80/certsrv/mscep/mscep.dll
usage ike
serial-number
ip-address none
password 7 151C040201
subject-name OU=BERLIN O=GERMANY
crl optional
rsakeypair ciscotac
auto-enroll regenerate
crypto ca certificate chain caserver2
certificate 3DA1D131000000000031
308203AA 30820354 A0030201 02020A3D A1D13100 00000000
31300D06
092A8648
86F70D01 01050500 3061310B 30090603 55040613 02555331
13301106
03550408
Certificate is abbreviated for easier viewing. quit ---!
certificate 3DA1C8FA0000000000030 308203AA 30820354
A0030201 02020A3D A1C8FA00 00000000 30300D06 092A8648
86F70D01 01050500 3061310B 30090603 55040613 02555331
13301106 03550408 !--- Certificate is abbreviated for
easier viewing. quit certificate ca

```

```
3E34CD199392A0914621EA778B13F357 30820284 3082022E
A0030201 0202103E 34CD1993 92A09146 21EA778B 13F35730
0D06092A 864886F7 0D010105 05003061 310B3009 06035504
06130255 53311330 !--- Certificate is abbreviated for
easier viewing. quit ! crypto isakmp policy 10 hash md5
crypto isakmp identity hostname ! crypto ipsec
transform-set myset esp-des esp-md5-hmac ! crypto map
vpn 10 ipsec-isakmp set peer 172.16.172.35 set
transform-set myset match address 101 ! ! ! voice call
carrier capacity active ! ! ! ! interface Ethernet1/0 no
ip address duplex half ! interface Ethernet1/1 ip
address 172.16.172.51 255.255.255.240 no ip redirects
duplex half crypto map vpn ! interface Ethernet1/2 ip
address 3.3.3.2 255.255.255.0 no keepalive duplex half !
interface Ethernet1/3 no ip address duplex half !
interface Hssi4/0 ip address 200.1.1.1 255.255.255.0
load-interval 30 fair-queue 64 16 0 hssi dce serial
restart_delay 0 clockrate 1524705 ! ip classless ip
route 0.0.0.0 0.0.0.0 172.16.172.49 no ip http server ip
pim bidir-enable ! ! access-list 101 permit ip 3.3.3.0
0.0.0.255 192.168.4.0 0.0.0.255 ! snmp-server community
public RO snmp-server enable traps tty ! ! call rsvp-
sync ! ! mgcp profile default ! dial-peer cor custom ! !
! ! gatekeeper shutdown ! ! line con 0 exec-timeout 0 0
line aux 0 line vty 0 4 privilege level 15 password
cisco login line vty 5 15 login ! no scheduler max-task-
time ! end 7204-1# 7204-1# 7204-1#show crypto ca
```

**certificate**  
Certificate

Status: Available

Certificate Serial Number: 3DA1D131000000000031

Certificate Usage: Encryption

:Issuer

CN = vpn

OU = cisco

O = tac

L = san jose

ST = california

C = US

:Subject

**Name: 7204-1.cisco.com**

**Serial Number: 01691291**

**"OU = "BERLIN O=GERMANY**

OID.1.2.840.113549.1.9.2 = 7204-1.cisco.com

OID.2.5.4.5 = 1691291

:CRL Distribution Point

<http://tac-2hq8cg5ti0h/CertEnroll/vpn.crl>

**:Validity Date**

**start date: 17:16:57 PST**

**Oct 26 2002**

**end date: 17:26:57**

**PST Oct 26 2003**

**renew date: 17:26:55 PST**

**Oct 26 2003**

**Associated Trustpoints: caserver2**

Certificate

Status: Available

Certificate Serial Number: 3DA1C8FA000000000030

Certificate Usage: Signature

:Issuer

CN = vpn

OU = cisco

O = tac  
L = san jose  
ST = california  
C = US  
**:Subject**  
**Name: 7204-1.cisco.com**  
**Serial Number: 01691291**  
**"OU = "BERLIN O=GERMANY**  
OID.1.2.840.113549.1.9.2 = 7204-1.cisco.com  
OID.2.5.4.5 = 1691291  
:CRL Distribution Point  
http://tac-2hq8cg5ti0h/CertEnroll/vpn.crl  
:Validity Date  
start date: 17:16:55 PST Oct 26 2002  
end date: 17:26:55 PST Oct 26 2003  
**Associated Trustpoints: caserver2**

CA Certificate  
Status: Available  
Certificate Serial Number:  
3E34CD199392A0914621EA778B13F357  
Certificate Usage: Signature  
:Issuer  
CN = vpn  
OU = cisco  
O = tac  
L = san jose  
ST = california  
C = US  
:Subject  
CN = vpn  
OU = cisco  
O = tac  
L = san jose  
ST = california  
C = US  
:CRL Distribution Point  
http://tac-2hq8cg5ti0h/CertEnroll/vpn.crl  
:Validity Date  
start date: 21:19:50 PST Dec 6 2001  
end date: 21:29:42 PST Dec 6 2003  
Associated Trustpoints: caserver2

7204-1#**show crypto key mypubkey rsa**  
Key pair was generated at: 13:55:35 PST Oct 25 2002 %  
**Key name: ciscotac**  
**Usage: Signature Key**  
:Key Data  
305C300D 06092A86 4886F70D 01010105 00034B00 30480241  
0099BC9C  
175AD748  
C991D24E 4F328960 997CADCB E665B876 4C53E2A0 449CA082  
4C503E05  
87604F32  
EECDF7B5 5CA0ADB6 2C664F9D 883EBAD6 671C6A8F A0C5D9EE  
23020301  
0001  
Key pair was generated at: 13:55:35 PST Oct 25 2002 %  
**Key name: ciscotac**  
**Usage: Encryption Key**  
:Key Data  
305C300D 06092A86 4886F70D 01010105 00034B00 30480241

```

00D4FE8A
3DE940E6
42277A82 87DDDA45 A0F77AE4 AF47D91F BA134F65 92886D3B
7489BEBB
DE650EA1
029A5A5C 72F39FCA A83BC018 246B0D1D 270DBC2F B9B29587
21020301
0001
Key pair was generated at: 22:07:13 PST Oct 26 2002 %
Key name: ciscotac.server
Usage: Encryption Key
:Key Data
307C300D 06092A86 4886F70D 01010105 00036B00 30680261
00E47825
7E60D6AC
4C078368 925191FD 2B2AAC50 6A6D6AF1 8A01C9B6 D21C4C80
05DD8277
D63F60B1
01A2DDCF 407BE088 D333FE1D 4F5DE892 47970454 A50C54EC
B962FEE4
A9BF5197
4C2B0656 503E0045 BB3168C4 2228155A B6BF0385 0B493FC5
79020301
0001
7204-1#
7204-1#
7204-1#
7204-1#

```

## التحقق من الصحة

توفر هذه الأقسام تأكيداً لما إذا كان التكوين يعمل عند إصدار أوامر **show** هذه أم لا. تتحقق هذه الأوامر من CA وإذا كانت شهادات الهوية (شهادات الموجه) قد تم إصدارها بواسطة خادم CA.

تدعم **أداة مترجم الإخراج (للعلماء المسجلين فقط) بعض أوامر show**. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مخرج الأمر **show**.

- **show crypto ca certificate** — يعرض معلومات حول الشهادات، وشهادة المرجع المصدق، وأي شهادات مرجع تسجيل. استخدم الأمر **show crypto ca certificates** في وضع EXEC.
  - **crypto ca** — مصادقة مرجع التصديق (إسترداد شهادة المرجع المصدق). استخدم الأمر **crypto ca authentication** في وضع التكوين العام.
  - **show crypto key mypubkey rsa** — يعرض مفاتيح RSA العامة للموجه. استخدم الأمر **show crypto key mypubkey rsa** في وضع EXEC.
  - **show crypto isakmp sa** — يعرض جميع اقترانات أمان تبادل مفتاح الإنترنت الحالية (SAs) في نظير. استخدم الأمر **show crypto isakmp sa** في وضع EXEC.
  - **show crypto ipSec** — يعرض الإعدادات المستخدمة من قبل IPsec SAs الحالية. استخدم الأمر **show crypto ipSec sa** في وضع EXEC.
  - **show clock** — يعرض وقت النظام الحالي على الموجه.
  - **تعيين التقويم س:م:س يوم السنة** - تعيين وقت نظام التقويم. لمزيد من المعلومات حول الساعات المختلفة وتعيين مصادر الوقت الخارجية على الموجه، ارجع إلى [تنفيذ إدارة النظام الأساسية](#).
- للحصول على أوامر إضافية متعلقة بقابلية التشغيل البيئي ل CA و IPsec و IKE، ارجع إلى [SR: الجزء 4: أمان IP وتشفير أوامر التوافق ل مرجع الشهادات](#).

هذا المخرج من الأمر **show crypto ca certificate**.

2611-VPN#show crypto ca certificate

Certificate  
Status: Available  
Certificate Serial Number: 3DAA9059000000000033  
Certificate Usage: Encryption  
:Issuer  
CN = vpn  
OU = cisco  
O = tac  
L = san jose  
ST = california  
C = US  
:Subject

*The received certificate from CA server2 contains the !--- FQDN, IP address, and subject ---!  
name. The renew date !--- states when the next enroll date is. Name: 2611-vpn.cisco.com*

**IP Address: 172.16.172.35**  
**Serial Number: 721959E3**  
**"OU = "ROME O=ITALY**  
OID.1.2.840.113549.1.9.2 = 2611-vpn.cisco.com  
OID.1.2.840.113549.1.9.8 = 172.16.172.35  
OID.2.5.4.5 = 721959E3  
:CRL Distribution Point  
<http://tac-2hq8cg5ti0h/CertEnroll/vpn.crl>  
:Validity Date  
**start date: 00:26:30 UTC Oct 27 2002**  
**end date: 00:36:30 UTC Oct 27 2003**  
**renew date: 00:36:28 UTC Oct 27 2003**  
**Associated Trustpoints: caserver2**

Certificate  
Status: Available  
Certificate Serial Number: 3DAA867D0000000000032  
Certificate Usage: Signature  
:Issuer  
CN = vpn  
OU = cisco  
O = tac  
L = San Jose ST = California C = US  
:Subject

**Name: 2611-vpn.cisco.com**  
**IP Address: 172.16.172.35**  
**Serial Number: 721959E3**  
**"OU = "ROME O=ITALY**  
OID.1.2.840.113549.1.9.2 = 2611-vpn.cisco.com  
OID.1.2.840.113549.1.9.8 = 172.16.172.35  
OID.2.5.4.5 = 721959E3  
:CRL Distribution Point  
<http://tac-2hq8cg5ti0h/CertEnroll/vpn.crl>  
:Validity Date  
**start date: 00:26:28 UTC Oct 27 2002**  
**end date: 00:36:28 UTC Oct 27 2003**  
**Associated Trustpoints: caserver2**

CA Certificate  
Status: Available  
Certificate Serial Number: 3E34CD199392A0914621EA778B13F357  
Certificate Usage: Signature  
:Issuer  
CN = vpn  
OU = cisco  
O = tac  
L = San Jose ST = California C = US

:Subject  
CN = vpn  
OU = cisco  
O = tac  
L = San Jose ST = California C = US  
:CRL Distribution Point  
<http://tac-2hq8cg5ti0h/CertEnroll/vpn.crl>  
:Validity Date  
start date: 04:19:50 UTC Dec 7 2001  
end date: 04:29:42 UTC DEC 7 2003  
Associated Trustpoints: caserver2

CA Certificate  
Status: Available  
Certificate Serial Number: 0E7EC1B68A2F14BD4C4515AF44C45732  
Certificate Usage: Signature  
:Issuer  
CN = SJVPNTAC-CAServer  
OU = TAC-VPN-SJ  
O = Cisco Systems  
L = San Jose  
ST = CA  
C = US  
:Subject  
CN = SJVPNTAC-CAServer  
OU = TAC-VPN-SJ  
O = Cisco Systems  
L = San Jose  
ST = CA  
C = US  
:CRL Distribution Point  
<http://ca-server/CertEnroll/SJVPNTAC-CAServer.crl>  
:Validity Date  
start date: 20:52:48 UTC Sep 17 2002  
end date: 21:02:37 UTC Sep 17 2017  
Associated Trustpoints: caserver1

Certificate  
Status: Available  
Certificate Serial Number: 6103EE0A0000000000038  
Certificate Usage: Signature  
:Issuer  
CN = SJVPNTAC-CAServer  
OU = TAC-VPN-SJ  
O = Cisco Systems  
L = San Jose  
ST = CA  
C = US  
:Subject  
**Name: 2611-vpn.cisco.com**  
**IP Address: 172.16.172.35**  
**Serial Number: 721959E3**  
**"OU = "PARIS O=FRANCE**  
OID.1.2.840.113549.1.9.2 = 2611-vpn.cisco.com  
OID.1.2.840.113549.1.9.8 = 172.16.172.35  
OID.2.5.4.5 = 721959E3  
:CRL Distribution Point  
<http://ca-server/CertEnroll/SJVPNTAC-CAServer.crl>  
:Validity Date  
start date: 03:33:05 UTC Oct 26 2002  
end date: 03:43:05 UTC Oct 26 2003  
**Associated Trustpoints: caserver1**

Certificate

Status: Available  
Certificate Serial Number: 6104020F000000000039  
Certificate Usage: Encryption  
:Issuer  
CN = SJPNTAC-CAServer  
OU = TAC-VPN-SJ  
O = Cisco Systems  
L = San Jose  
ST = CA  
C = US  
:Subject

*The received certificate from CA server2 contains the !--- FQDN, IP address, and subject ---!  
name. The renew date !--- states when the next enroll date is. Name: 2611-vpn.cisco.com*

**IP Address: 172.16.172.35**  
**Serial Number: 721959E3**  
**"OU = "PARIS O=FRANCE**

OID.1.2.840.113549.1.9.2 = 2611-vpn.cisco.com  
OID.1.2.840.113549.1.9.8 = 172.16.172.35  
OID.2.5.4.5 = 721959E3  
:CRL Distribution Point  
http://ca-server/CertEnroll/SJPNTAC-CAServer.crl  
:Validity Date  
**start date: 03:33:10 UTC Oct 26 2002**  
**end date: 03:43:10 UTC Oct 26 2003**  
**renew date: 03:43:05 UTC Oct 26 2003**  
**Associated Trustpoints: caserver1**

2611-VPN#show crypto key mypubkey rsa  
Key pair was generated at: 00:14:06 UTC Mar 1 1993 %  
**Key name: ciscovpn**  
**Usage: Signature Key**

:Key Data  
305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00A2DE57 2C7A4555  
BF87D3CC 4A260DBF 56574554 472FC72C 0461A35B E41B5B53 BE81A47E 264A68D7  
27E4E301 2AF04B1C E472F70B 74DF38A0 6EB286F9 01020301 0001 08662555

Key pair was generated at: 00:14:10 UTC Mar 1 1993 %  
Key name: ciscovpn  
Usage: **Encryption Key**

:Key Data  
305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00D10224 8CBEC2D7  
B517DF99 7363717D 6F6CA0F1 83FB7874 E60BB169 CD4AD9CA 92E04143 16D4D253  
5CBF212F FF6268A5 329AB988 2655568C 8EC19017 6F4A4C86 43020301 0001

Key pair was generated at: 00:14:59 UTC Mar 1 1993 %  
**Key name: tacvpn**  
**Usage: Signature Key**

:Key Data  
305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00AB2884 22A070D0  
A8C84C3E CD45A382 F4CDB158 5B31B624 5C92632C 5DC1977E 686E1C18 DA16BE57  
6FBA9518 4D2F01B8 0D59528D 447014D3 02D5A631 84E54CD4 FB020301 0001

Key pair was generated at: 00:15:00 UTC Mar 1 1993 %  
Key name: tacvpn  
Usage: **Encryption Key**

:Key Data  
305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00AB7576 9D0A2D65  
7BB9B465 AF227B73 2B83AFD6 3791FA54 3A2DB845 55E4540F 35972460 B87C613E  
82DBC4D2 51E6F9A7 07164C57 B02D28B8 93F8D50F D5C3444F 01020301 0001

Key pair was generated at: 22:02:57 UTC Oct 27 2002 %  
Key name: ciscovpn.server  
Usage: Encryption Key

:Key Data  
307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00D42A5E 4C9D27F1  
195CC537 7CF9E390 935DFBA3 2DA01B3B C5E50620 57B902A3 50876FA1 1A9D83FD  
0EB437F7 E0568EB7 830A46FA E9D9BA4F 3E8B132D F24A08B8 E2154944 36829D64  
E48077EF 224BF142 A3A92672 F0BC57F5 063EF64A 8B775979 CD020301 0001



## RSA إعادة إنشاء زوج مفاتيح

توضح هذه الأوامر على الموجه 1-7204 كيفية استخدام أمر إعادة إنشاء التسجيل التلقائي و **rsa-key**. يوضح الشكل تسلسل الأحداث بعد إعلان CA على الموجه وبعد إصدار الأمر **crypto ca authentication ca server**. يعمل الأمر **auto-login** فقط بعد مصادقة المرجع المصدق. بمجرد مصادقة المرجع المصدق، يتم تسجيل الموجه تلقائياً مع خادم CA. لا تحتاج إلى إصدار الأمر **crypto ca enroll ca server**. بمجرد انتهاء صلاحية شهادة الهوية، يقوم الموجه بالتسجيل تلقائياً مع خادم CA. مع إدخال هذا الأمر، لا توجد حاجة للتسجيل يدوياً مع خادم CA بمجرد انتهاء صلاحية شهادة الهوية (الموجه).

لا تحتاج إلى استخدام مصدر وقت خارجي (خادم NTP) على الموجه إذا قمت بتعيين نظام التقويم على الموجه باستخدام الأمر **مجموعة التقويم** لتعيين الوقت الصحيح. يؤدي إعادة تحميل الموجه إلى مزامنة ساعة النظام مع النظام ذي الصلة.

**ملاحظة:** لا يتوفر الأمر **set** التقويم على الموجهات 1700 و 2600. استخدام مصدر وقت خارجي على هذه الموجهات.

تم تكوين CA على الموجه. يوضح هذا الإخراج التسجيل التلقائي لشهادات الهوية وإعادة إنشاء زوج مفاتيح RSA على الموجه 1-7204. وهذا الناتج جريء في مجالات معينة للتأكيد على معلومات مهمة.

```
crypto ca trustpoint caserver2
  enrollment retry period 2
  enrollment mode ra
enrollment url http://171.69.89.111:80/certsrv/mscep/mscep.dll
  usage ike
  serial-number
  ip-address none
  password 7 151C040201
subject-name OU=BERLIN O=GERMANY
  crl optional
  rsa-keypair ciscotac
  auto-enroll regenerate
```

*Execute this command to authenticate the CA by obtaining !--- the CA's self-signed ---! certificate which contains the CA's public key. Because !--- the CA signs its own certificate, the CA's public key should be manually !--- authenticated by contacting the CA administrator to compare the CA certificate's !--- fingerprint. Note that after you execute the command the router immediately !--- enrolls with the CA server to obtain its identity certificate. 7204-*

```
1(config)#crypto ca authenticate caserver2
:Certificate has the following attributes
Fingerprint: A1E8B61A FD1A66D6 2DE35501 99C43D83
:[Do you accept this certificate? [yes/no %
:Oct 27 06:45:09: CRYPTO_PKI: Sending CA Certificate Request
GET /certsrv/mscep/mscep.dll/pkiclient.exe?operation=GetCACert&message=caserver2
HTTP/1.0
```

```
Oct 27 06:45:09: CRYPTO_PKI: can not resolve server name/IP address
Oct 27 06:45:09: CRYPTO_PKI: Using unresolved IP Address 171.69.89.111
Oct 27 06:45:09: CRYPTO_PKI: http connection opened
:Oct 27 06:45:10: CRYPTO_PKI: HTTP response header
HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Sun, 27 Oct 2002 02:19:09 GMT
Content-Length: 2811
Content-Type: application/x-x509-ca-ra-cert
```

.Content-Type indicates we have received CA and RA certificates  
(Oct 27 06:45:10: CRYPTO\_PKI:crypto\_process\_ca\_ra\_cert(trustpoint=caserver2

```
:(Oct 27 06:45:10: CRYPTO_PKI:CA and RA certs (cert data
    0A F7 06 09 2A 86 48 86 F7 0D 01 07 02 82 30
    A0
    hex data omitted
    0B 73 6A 76 70 6E 70 y 13 03
.Trustpoint CA certificate accepted
    config)#6B 69 2D 72 61 30 81)7204-1
    9F 30 0D 06 09 2A 86 48 86 F7 0D 01 01 01
    00 05
    hex data omitted
    A9 13 93 1E E6 E1 E4 30 07 31 00
= Oct 27 06:45:10: CRYPTO_PKI: InsertCertData: subject name
    0B 30 09 06 03 55 04 06 13 02 55 53 31 61 30
    31
    hex data omitted
    6E 70 76
= Oct 27 06:45:10: CRYPTO_PKI: InsertCertData: issuer name
    0B 30 09 06 03 55 04 06 13 02 55 53 31 61 30
    31
    hex data omitted
    6E 70 76
Oct 27 06:45:10: CRYPTO_PKI: InsertCertData: serial number = 3E
    CD 19 93 92 A0 91 46 21 EA 77 8B 13 F3 57 34
= Oct 27 06:45:10: CRYPTO_PKI: InsertCertData: subject name
    1E 06 09 2A 86 48 86 F7 0D 30 20 31 83 81 30
    01
    hex data omitted
    6B 69 2D 72 61 70
= Oct 27 06:45:10: CRYPTO_PKI: InsertCertData: issuer name
    0B 30 09 06 03 55 04 06 13 02 55 53 31 61 30
    31
    hex data omitted
    6E 70 76
Oct 27 06:45:10: CRYPTO_PKI: InsertCertData: serial number = 14
    6C F2 85 00 00 00 00 00 09
Oct 27 06:45:10: CRYPTO_PKI: WARNING: Certificate, private key or CRL
    was not found while selecting CRL
= Oct 27 06:45:10: CRYPTO_PKI: InsertCertData: subject name
    1E 06 09 2A 86 48 86 F7 0D 30 20 31 83 81 30
    01
    hex data omitted
    6B 69 2D 72 61 70
= Oct 27 06:45:10: CRYPTO_PKI: InsertCertData: issuer name
    0B 30 09 06 03 55 04 06 13 02 55 53 31 61 30
    31
    hex data omitted
    6E 70 76
Oct 27 06:45:10: CRYPTO_PKI: InsertCertData: serial number = 14
    6C F1 A9 00 00 00 00 00 08
Oct 27 06:45:10: CRYPTO_PKI: WARNING: Certificate, private key or CRL
    was not found while selecting CRL
= Oct 27 06:45:10: CRYPTO_PKI: InsertCertData: subject name
    0B 30 09 06 03 55 04 06 13 02 55 53 31 61 30
    31
    hex data omitted
    6E 70 76
= Oct 27 06:45:10: CRYPTO_PKI: InsertCertData: issuer name
    0B 30 09 06 03 55 04 06 13 02 55 53 31 61 30
    31
    hex data omitted
    6E 70 76
Oct 27 06:45:10: CRYPTO_PKI: InsertCertData: serial number = 3E
    CD 19 93 92 A0 91 46 21 EA 77 8B 13 F3 57 34
Oct 27 06:45:10: CRYPTO_PKI: transaction GetCACert completed
```

```

.Oct 27 06:45:10: CRYPTO_PKI: CA certificate received
      Oct 27 06:45:10: CRYPTO_PKI: CA certificate
.received
()Oct 27 06:45:10: CRYPTO_PKI: crypto_pki_authenticate_tp_cert
Oct 27 06:45:10: CRYPTO_PKI: trustpoint caserver2 authentication status
      2 =
= Oct 27 06:45:12: CRYPTO_PKI: InsertCertData: subject name
      0B 30 09 06 03 55 04 06 13 02 55 53 31 61 30
      31
      hex data omitted
      6E 70 76
= Oct 27 06:45:12: CRYPTO_PKI: InsertCertData: issuer name
      0B 30 09 06 03 55 04 06 13 02 55 53 31 61 30
      31
      hex data omitted
      6E 70 76
Oct 27 06:45:12: CRYPTO_PKI: InsertCertData: serial number = 3E
      CD 19 93 92 A0 91 46 21 EA 77 8B 13 F3 57 34
(Oct 27 06:45:12: CRYPTO_PKI: crypto_process_ra_certs(trust_point=caserver2

      Time to Re-enroll trust_point caserver2 7204-1#%
Can not select my full public key (ciscotac)% Start certificate enrollment
      ..
The subject name in the certificate will %
      be: OU=BERLIN O=GERMANY
The subject name in the certificate will %
      be: 7204-1.cisco.com
The serial number in the certificate will %
      be: 01691291
Certificate request sent to Certificate %
      Authority
The certificate request fingerprint will %
      .be displayed
The 'show crypto ca certificate' command %
      .will also show the fingerprint
      :Signing Certificate Reqeust Fingerprint
      E92A4B6C D213B9A9 4AD07064 23BFABA1
:Oct 27 06:46:32: CRYPTO_PKI: Sending CA Certificate Request
GET /certsrv/mscep/mscep.dll/pkiclient.exe?operation=GetCACert&message=caserver2
      HTTP/1.0

Oct 27 06:46:32: CRYPTO_PKI: can not resolve server name/IP address
Oct 27 06:46:32: CRYPTO_PKI: Using unresolved IP Address 171.69.89.111
Oct 27 06:46:32: CRYPTO_PKI: http connection opened
:Oct 27 06:46:33: CRYPTO_PKI: HTTP response header
      HTTP/1.1 200 OK
      Server: Microsoft-IIS/5.0
      Date: Sun, 27 Oct 2002 02:20:32 GMT
      Content-Length: 2811
      Content-Type: application/x-x509-ca-ra-cert

.Content-Type indicates we have received CA and RA certificates
(Oct 27 06:46:33: CRYPTO_PKI:crypto_process_ca_ra_cert(trustpoint=caserver2
      :(Oct 27 06:46:33: CRYPTO_PKI:CA and RA certs (cert data
      0A F7 06 09 2A 86 48 86 F7 0D 01 07 02 82 30
      A0
      hex data omitted
      Encryption Certi0A 06 03
      6E 30 1E 17 0D 30 32 70 76 03 13 03 04 55
      39 30
      hex data omitted
      A9 13 93 1E E6 E1 E4 30 07 31 00
= Oct 27 06:46:33: CRYPTO_PKI: InsertCertData: subject name
      0B 30 09 06 03 55 04 06 13 02 55 53 31 61 30

```

31  
hex data omitted  
6E 70 76  
= Oct 27 06:46:33: CRYPTO\_PKI: InsertCertData: issuer name  
0B 30 09 06 03 55 04 06 13 02 55 53 31 61 30  
31  
hex data omitted  
6E 70 76  
Oct 27 06:46:33: CRYPTO\_PKI: InsertCertData: serial number = 3E  
CD 19 93 92 A0 91 46 21 EA 77 8B 13 F3 57 34  
= Oct 27 06:46:33: CRYPTO\_PKI: InsertCertData: subject name  
1E 06 09 2A 86 48 86 F7 0D 30 20 31 83 81 30  
01  
hex data omitted  
6B 69 2D 72 61 70  
= Oct 27 06:46:33: CRYPTO\_PKI: InsertCertData: issuer name  
0B 30 09 06 03 55 04 06 13 02 55 53 31 61 30  
31  
hex data omitted  
6E 70 76  
Oct 27 06:46:33: CRYPTO\_PKI: InsertCertData: serial number = 14  
6C F2 85 00 00 00 00 09  
Oct 27 06:46:33: CRYPTO\_PKI: WARNING: Certificate, private key or CRL  
was not found while selecting CRL  
= Oct 27 06:46:33: CRYPTO\_PKI: InsertCertData: subject name  
1E 06 09 2A 86 48 86 F7 0D 30 20 31 83 81 30  
01  
hex data omitted  
6B 69 2D 72 61 70  
= Oct 27 06:46:33: CRYPTO\_PKI: InsertCertData: issuer name  
0B 30 09 06 03 55 04 06 13 02 55 53 31 61 30  
31  
hex data omitted  
6E 70 76  
Oct 27 06:46:33: CRYPTO\_PKI: InsertCertData: serial number = 14  
6C F1 A9 00 00 00 00 08  
Oct 27 06:46:33: CRYPTO\_PKI: WARNING: Certificate, private key or CRL  
was not found while selecting CRL  
= Oct 27 06:46:33: CRYPTO\_PKI: InsertCertData: subject name  
1E 06 09 2A 86 48 86 F7 0D 30 20 31 83 81 30  
01  
hex data omitted  
6B 69 2D 72 61 70  
= Oct 27 06:46:33: CRYPTO\_PKI: InsertCertData: issuer name  
0B 30 09 06 03 55 04 06 13 02 55 53 31 61 30  
31  
hex data omitted  
6E 70 76  
Oct 27 06:46:33: CRYPTO\_PKI: InsertCertData: serial number = 14  
6C F1 A9 00 00 00 00 08  
= Oct 27 06:46:33: CRYPTO\_PKI: InsertCertData: subject name  
1E 06 09 2A 86 48 86 F7 0D 30 20 31 83 81 30  
01  
hex data omitted  
6B 69 2D 72 61 70  
= Oct 27 06:46:33: CRYPTO\_PKI: InsertCertData: issuer name  
0B 30 09 06 03 55 04 06 13 02 55 53 31 61 30  
31  
hex data omitted  
6E 70 76  
Oct 27 06:46:33: CRYPTO\_PKI: InsertCertData: serial number = 14  
6C F2 85 00 00 00 00 09  
= Oct 27 06:46:33: CRYPTO\_PKI: InsertCertData: subject name  
0B 30 09 06 03 55 04 06 13 02 55 53 31 61 30

```

31
hex data omitted
6E 70 76
= Oct 27 06:46:33: CRYPTO_PKI: InsertCertData: issuer name
0B 30 09 06 03 55 04 06 13 02 55 53 31 61 30
31
hex data omitted
6E 70 76
Oct 27 06:46:33: CRYPTO_PKI: InsertCertData: serial number = 3E
CD 19 93 92 A0 91 46 21 EA 77 8B 13 F3 57 34
(Oct 27 06:46:33: CRYPTO_PKI: crypto_process_ra_certs(trust_point=caserver2
Oct 27 06:46:33: CRYPTO_PKI: transaction PKCSReq completed
:Oct 27 06:46:33: CRYPTO_PKI: status
Oct 27 06:46:33: CRYPTO_PKI: All sockets are closed for trustpoint
.caserver2
Oct 27 06:46:33: CRYPTO_PKI:Write out pkcs#10 content:319
3B 30 81 E6 02 01 00 30 4C 31 19 01 82 30
17 30
hex data omitted
FB EE 80 3D 5D 62 B9 BD 85 24 03 49 6D 2C
98
...Oct 27 06:46:33: CRYPTO_PKI:Enveloped Data for trustpoint caserver2
2A 86 48 86 F7 0D 01 07 03 A0 80 09 06 80 30
30
hex data omitted
00 00 00 00
Oct 27 06:46:33: CRYPTO_PKI:Signed Data for trustpoint caserver2 (1410
(bytes
2A 86 48 86 F7 0D 01 07 02 A0 09 06 80 30
30 80
hex data omitted
00 00
Oct 27 06:46:33: CRYPTO_PKI: can not resolve server name/IP address
Oct 27 06:46:33: CRYPTO_PKI: Using unresolved IP Address 171.69.89.111
Oct 27 06:46:33: CRYPTO_PKI: http connection opened
Oct 27 06:46:35: CRYPTO_PKI:Write out pkcs#10 content:319
3B 30 81 E6 02 01 00 30 4C 31 19 01 82 30
17 30
hex data omitted
A0 F6 FB F3 9F E3 3C AF AB BE 24 9F 30 11
10
:ificate Request Fingerprint
3B7DB296 E21FCDD8 3B4E29D4 A472A4A7
...Oct 27 06:47:03: CRYPTO_PKI:Enveloped Data for trustpoint caserver2
2A 86 48 86 F7 0D 01 07 03 A0 80 09 06 80 30
30
hex data omitted
00 00 00 00
Oct 27 06:47:03: CRYPTO_PKI:Signed Data for trustpoint caserver2 (1410
(bytes
2A 86 48 86 F7 0D 01 07 02 A0 09 06 80 30
30 80
hex data omitted
B1 B3 DB 54 0F F9 4A 5D 56 45 00 00 00 00
00
00 00
Oct 27 06:47:03: CRYPTO_PKI: can not resolve server name/IP address
Oct 27 06:47:03: CRYPTO_PKI: Using unresolved IP Address 171.69.89.111
Oct 27 06:47:03: CRYPTO_PKI: http connection opened
Oct 27 06:47:05: CRYPTO_PKI: received msg of 1930 bytes
:Oct 27 06:47:05: CRYPTO_PKI: HTTP response header
```

HTTP/1.1 200 OK  
Server: Microsoft-IIS/5.0  
Date: Sun, 27 Oct 2002 02:20:35 GMT  
Content-Length: 1784  
Content-Type: application/x-pki-message

Oct 27 06:47:05: CRYPTO\_PKI:Received pki message (PKCS7) for trustpoint  
caserver2: 1784 bytes  
F4 06 09 2A 86 48 86 F7 0D 01 07 02 06 82 30  
A0  
hex data omitted  
4E 15 B3 43 58 17 42 73  
= Oct 27 06:47:05: CRYPTO\_PKI: InsertCertData: subject name  
1E 06 09 2A 86 48 86 F7 0D 30 20 31 83 81 30  
01  
hex data omitted  
6B 69 2D 72 61 70  
= Oct 27 06:47:05: CRYPTO\_PKI: InsertCertData: issuer name  
0B 30 09 06 03 55 04 06 13 02 55 53 31 61 30  
31  
hex data omitted  
6E 70 76  
Oct 27 06:47:05: CRYPTO\_PKI: InsertCertData: serial number = 14  
6C F1 A9 00 00 00 00 00 08  
Oct 27 06:47:05: CRYPTO\_PKI: WARNING: Certificate, private key or CRL  
was not found while selecting CRL  
:Oct 27 06:47:05: CRYPTO\_PKI: signed attr: pki-message-type  
33 01 13  
Oct 27 06:47:05: CRYPTO\_PKI: signed attr: pki-status: 13  
30 01  
:Oct 27 06:47:05: CRYPTO\_PKI: signed attr: pki-recipient-nonce  
C3 F3 B9 FA 5B B6 C0 D9 55 1D B6 46 10 04  
E6 57  
7E 67  
:Oct 27 06:47:05: CRYPTO\_PKI: signed attr: pki-transaction-id  
33 37 37 35 38 32 39 31 34 36 33 33 20 13  
38 43  
37 31 38 46 45 32 41 30 35 46 35 46 34 39  
35 33  
37 32  
Oct 27 06:47:05: CRYPTO\_PKI: status = 100: certificate is granted  
Oct 27 06:47:05: CRYPTO\_PKI:Verified signed data for trustpoint caserver2  
:(bytes 1217)  
BD 06 09 2A 86 48 86 F7 0D 01 07 04 82 30  
A0 03  
hex data omitted  
BE  
:Oct 27 06:47:05: CRYPTO\_PKI:Decrypted enveloped content  
D9 06 09 2A 86 48 86 F7 0D 01 07 03 82 30  
A0 02  
hex data omitted  
AF 15 F0 AD BF 22 7A 41 72 49 5D 31 00  
= Oct 27 06:47:05: CRYPTO\_PKI: InsertCertData: subject name  
4E 31 10 30 0E 06 03 55 04 05 13 07 31 36 30  
39  
hex data omitted  
4C 49 4E 20 4F 3D 47 45 52 4D 41 52 45 42  
4E 59  
= Oct 27 06:47:05: CRYPTO\_PKI: InsertCertData: issuer name  
0B 30 09 06 03 55 04 06 13 02 55 53 31 61 30  
31  
hex data omitted  
6E 70 76

```
Oct 27 06:47:05: CRYPTO_PKI: InsertCertData: serial number = 61
                                C6 69 00 00 00 00 34 11
Oct 27 06:47:05: CRYPTO_PKI: WARNING: Certificate, private key or CRL
                                was not found while selecting CRL
= Oct 27 06:47:05: CRYPTO_PKI: InsertCertData: subject name
                                4E 31 10 30 0E 06 03 55 04 05 13 07 31 36 30
                                                                39
                                                                hex data omitted
                                4C 49 4E 20 4F 3D 47 45 52 4D 41 52 45 42
                                                                4E 59
= Oct 27 06:47:05: CRYPTO_PKI: InsertCertData: issuer name
                                0B 30 09 06 03 55 04 06 13 02 55 53 31 61 30
                                                                31
                                                                hex data omitted
                                                                6E 70 76
Oct 27 06:47:05: CRYPTO_PKI: InsertCertData: serial number = 61
                                C6 69 00 00 00 00 34 11
Oct 27 06:47:05: %CRYPTO-6-CERTRET: Certificate
                                received from Certificate Authority
Oct 27 06:47:15: CRYPTO_PKI: received msg of 1930 bytes
:Oct 27 06:47:15: CRYPTO_PKI: HTTP response header
                                HTTP/1.1 200 OK
                                Server: Microsoft-IIS/5.0
                                Date: Sun, 27 Oct 2002 02:21:05 GMT
                                Content-Length: 1784
                                Content-Type: application/x-pki-message

Oct 27 06:47:15: CRYPTO_PKI:Received pki message (PKCS7) for trustpoint
                                caserver2: 1784 bytes
                                F4 06 09 2A 86 48 86 F7 0D 01 07 02 06 82 30
                                                                A0
                                                                hex data omitted
                                3A AD 1F 3B 2F 99 37 79
= Oct 27 06:47:15: CRYPTO_PKI: InsertCertData: subject name
                                1E 06 09 2A 86 48 86 F7 0D 30 20 31 83 81 30
                                                                01
                                                                hex data omitted
                                6B 69 2D 72 61 70
= Oct 27 06:47:15: CRYPTO_PKI: InsertCertData: issuer name
                                0B 30 09 06 03 55 04 06 13 02 55 53 31 61 30
                                                                31
                                                                hex data omitted
                                                                6E 70 76
Oct 27 06:47:15: CRYPTO_PKI: InsertCertData: serial number = 14
                                6C F1 A9 00 00 00 00 08
Oct 27 06:47:15: CRYPTO_PKI: WARNING: Certificate, private key or CRL
                                was not found while selecting CRL
:Oct 27 06:47:15: CRYPTO_PKI: signed attr: pki-message-type
                                                                33 01 13
Oct 27 06:47:15: CRYPTO_PKI: signed attr: pki-status: 13
                                                                30 01
:Oct 27 06:47:15: CRYPTO_PKI: signed attr: pki-recipient-nonce
                                D6 56 C7 8C CB 3D A3 E7 B6 84 F8 66 10 04
                                                                EE 80
                                                                18 65
:Oct 27 06:47:15: CRYPTO_PKI: signed attr: pki-transaction-id
                                43 31 37 39 45 36 30 36 33 46 33 33 20 13
                                                                34 35
                                35 42 30 46 42 46 30 36 34 36 32 39 46 34
                                                                39 37
                                                                32 35
Oct 27 06:47:15: CRYPTO_PKI: status = 100: certificate is granted
Oct 27 06:47:15: CRYPTO_PKI:Verified signed data for trustpoint caserver2
```

```

:(bytes 1217)
BD 06 09 2A 86 48 86 F7 0D 01 07 04 82 30
A0 03
hex data omitted
7A 43 16 55 C5 57 97 DF FE D4 3A 0C 14 24
5D D1
96
:Oct 27 06:47:15: CRYPTO_PKI:Decrypted enveloped content
D9 06 09 2A 86 48 86 F7 0D 01 07 03 82 30
A0 02
hex data omitted
AC A9 92 C8 2D F8 24 31 00 71 57 01 94
= Oct 27 06:47:15: CRYPTO_PKI: InsertCertData: subject name
4E 31 10 30 0E 06 03 55 04 05 13 07 31 36 30
39
hex data omitted
4C 49 4E 20 4F 3D 47 45 52 4D 41 52 45 42
4E 59
= Oct 27 06:47:15: CRYPTO_PKI: InsertCertData: issuer name
0B 30 09 06 03 55 04 06 13 02 55 53 31 61 30
31
hex data omitted
6E 70 76
Oct 27 06:47:15: CRYPTO_PKI: InsertCertData: serial number = 61
3C 0A 00 00 00 00 00 35 12
Oct 27 06:47:15: CRYPTO_PKI: WARNING: Certificate, private key or CRL
was not found while selecting CRL
= Oct 27 06:47:15: CRYPTO_PKI: InsertCertData: subject name
4E 31 10 30 0E 06 03 55 04 05 13 07 31 36 30
39
hex data omitted
4C 49 4E 20 4F 3D 47 45 52 4D 41 52 45 42
4E 59
= Oct 27 06:47:15: CRYPTO_PKI: InsertCertData: issuer name
0B 30 09 06 03 55 04 06 13 02 55 53 31 61 30
31
hex data omitted
6E 70 76
Oct 27 06:47:15: CRYPTO_PKI: InsertCertData: serial number = 61
3C 0A 00 00 00 00 00 35 12
Oct 27 06:47:15: CRYPTO_PKI: All enrollment requests completed for trustpoint
.caserver2
Oct 27 06:47:15: CRYPTO_PKI: All enrollment requests completed for
.trustpoint caserver2
Oct 27 06:47:15: CRYPTO_PKI: WARNING: Certificate, private key or CRL
was not found while selecting CRL
Oct 27 06:47:15: CRYPTO_PKI: All enrollment
.requests completed for trustpoint caserver2
7204-1#
7204-1#
View detailed information on certificate. 7204-1#show crypto ca certificate ---!
Certificate
Status: Available
Certificate Serial Number: 61123C0A000000000035
Certificate Usage: Encryption
:Issuer
CN = vpn
OU = cisco
O = tac
L = san jose
ST = california
C = US
:Subject
Name: 7204-1.cisco.com

```



Serial Number: 01691291  
"OU = "BERLIN O=GERMANY  
OID.1.2.840.113549.1.9.2  
cisco.com.7204-1 =  
OID.2.5.4.5 = 1691291  
:CRL Distribution Point  
http://tac-2hq8cg5ti0h/CertEnroll/vpn.crl  
:Validity Date  
start date: 19:11:05  
PST Oct 26 2002  
:end date  
PST Oct 27 2002 19:21:05  
renew date: 19:20:35  
PST Oct 27 2002

*Note that the certificate issued here is only !--- valid for a day. The router !--- auto- ---!  
enrolls at the renew date given. Associated Trustpoints: caserver2*

Certificate  
Status: Available  
Certificate Serial Number: 6111C66900000000034  
Certificate Usage: Signature  
:Issuer  
CN = vpn  
OU = cisco  
O = tac  
L = san jose  
ST = california  
C = US  
:Subject

Name: 7204-1.cisco.com  
Serial Number: 01691291  
"OU = "BERLIN O=GERMANY  
OID.1.2.840.113549.1.9.2  
cisco.com.7204-1 =  
OID.2.5.4.5 = 1691291  
:CRL Distribution Point  
http://tac-2hq8cg5ti0h/CertEnroll/vpn.crl  
:Validity Date  
start date: 19:10:35 PST  
Oct 26 2002  
end date: 19:20:35 PST Oct  
2002 27

**Associated Trustpoints: caserver2**

CA Certificate  
Status: Available  
Certificate Serial Number: 3E34CD199392A0914621EA778B13F357  
Certificate Usage: Signature  
:Issuer  
CN = vpn  
OU = cisco  
O = tac  
L = san jose  
ST = california  
C = US  
:Subject

CN = vpn  
OU = cisco  
O = tac  
L = san jose  
ST = california  
C = US  
:CRL Distribution Point  
http://tac-2hq8cg5ti0h/CertEnroll/vpn.crl  
:Validity Date  
start date: 21:19:50 PST Dec 6 2001

end date: 21:29:42 PST Dec 6 2003  
Associated Trustpoints: caserver2

7204-1#show cry key mypubkey rsa  
Key pair was generated at: 13:55:35 PST %  
Oct 25 2002

*Note that the RSA key pairs are regenerated once the router !--- has reenrolled for the ---! certificates.* Key name: ciscotac Usage: Signature Key Key Data: 305C300D 06092A86 4886F70D 01010105 00034B00 30480241 0099BC9C 175AD748 C991D24E 4F328960 997CADCB E665B876 4C53E2A0 449CA082 4C503E05 87604F32 EECDF7B5 5CA0ADB6 2C664F9D 883EBAD6 671C6A8F A0C5D9EE 23020301 0001 % Key pair was generated at: 13:55:35 PST Oct 25 2002 Key name: ciscotac Usage: Encryption Key Key Data: 305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00D4FE8A 3DE940E6 42277A82 87DDDA45 A0F77AE4 AF47D91F BA134F65 92886D3B 7489BEBB DE650EA1 029A5A5C 72F39FCA A83BC018 246B0D1D 270DBCf2 B9B29587 21020301 0001 % Key pair was generated at: 22:07:13 PST Oct 26 2002 Key name: ciscotac.server Usage: Encryption Key Key Data: 307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00E47825 7E60D6AC 4C078368 925191FD 2B2AAC50 6A6D6AF1 8A01C9B6 D21C4C80 05DD8277 D63F60B1 01A2DDCF 407BE088 D333FE1D 4F5DE892 47970454 A50C54EC B962FEE4 A9BF5197 4C2B0656 503E0045 BB3168C4 2228155A B6BF0385 0B493FC5 79020301 0001 7204-1# *!--- The router configuration with the certificates.* 7204-1#show run

```
...Building configuration
Current configuration : 8367 bytes
!
Last configuration change at 23:45:33 PST Sat Oct 26 2002 !
NVRAM config last updated at 23:43:25 PST Sat Oct 26 2002 !
!
version 12.2
service timestamps debug datetime
service timestamps log datetime
no service password-encryption
service udp-small-servers
service tcp-small-servers
no service dhcp
!
hostname 7204-1
!
boot system flash slot
boot system flash slot0:c7200-jk9o3s-mz.122-11.T1.bin
logging buffered 50000 debugging
enable secret 5 $1$GdwM$YPQYieph20DPAhQeNvHa30
enable password ipsecpki
!
username cisco password 0 cisco
clock timezone PST -7
ip subnet-zero
!
!
no ip domain lookup
ip domain name cisco.com
ip host caserver2 171.69.89.111
!
!
ip vrf test
no ip cef
ip audit notify log
ip audit po max-events 100
!
crypto ca trustpoint caserver2
enrollment retry period 2
enrollment mode ra
enrollment url http://171.69.89.111:80/certsrv/mscep/mscep.dll
usage ike
serial-number
ip-address none
```

```

password 7 151C040201
subject-name OU=BERLIN O=GERMANY
crl optional
rsakeypair ciscotac
auto-enroll regenerate
crypto ca certificate chain caserver2
certificate 61123C0A000000000035
308203AA 30820354 A0030201 02020A61 123C0A00 00000000 35300D06
092A8648
86F70D01 01050500 3061310B 30090603 55040613 02555331 13301106
03550408
Certificate is abbreviated for easier viewing. quit certificate 6111C669000000000034 ---!
308203AA 30820354 A0030201 02020A61 11C66900 00000000 34300D06 092A8648 86F70D01 01050500
3061310B 30090603 55040613 02555331 13301106 03550408 !--- Certificate is abbreviated for easier
viewing. quit certificate ca 3E34CD199392A0914621EA778B13F357 30820284 3082022E A0030201
0202103E 34CD1993 92A09146 21EA778B 13F35730 0D06092A 864886F7 0D010105 05003061 310B3009
06035504 06130255 53311330 !--- Certificate is abbreviated for easier viewing. quit ! crypto
isakmp policy 10 hash md5 crypto isakmp identity hostname ! ! crypto ipsec transform-set myset
esp-des esp-md5-hmac ! crypto map vpn 10 ipsec-isakmp set peer 172.16.172.35 set transform-set
myset match address 101 ! ! ! voice call carrier capacity active ! ! ! ! ! ! ! ! ! ! !
interface Ethernet1/0 no ip address duplex half ! interface Ethernet1/1 ip address 172.16.172.51
255.255.255.240 no ip redirects duplex half crypto map vpn ! interface Ethernet1/2 ip address
3.3.3.2 255.255.255.0 no keepalive duplex half ! interface Ethernet1/3 no ip address duplex half
! interface Hssi4/0 ip address 200.1.1.1 255.255.255.0 load-interval 30 fair-queue 64 16 0 hssi
dce serial restart_delay 0 clockrate 1524705 ! ip classless ip route 0.0.0.0 0.0.0.0
172.16.172.49 no ip http server ip pim bidir-enable ! ! access-list 101 permit ip 3.3.3.0
0.0.0.255 192.168.4.0 0.0.0.255 ! snmp-server community public RO snmp-server enable traps tty !
! call rsvp-sync ! ! mgcp profile default ! dial-peer cor custom ! ! ! ! gatekeeper shutdown ! !
line con 0 exec-timeout 0 0 line aux 0 line vty 0 4 privilege level 15 password cisco login line
vty 5 15 login ! no scheduler max-task-time ! end !--- The system clock is used to view the
time. 7204-1#show clock
PST Sat Oct 26 2002 23:54:39.059
7204-1#show clock
PST Sat Oct 26 2002 23:58:08.127
7204-1#show clock
PST Sat Oct 26 2002 19:35:57.227*
7204-1#
7204-1#
7204-1#
7204-1#show crypto ca certificate
CA Certificate
Status: Available
Certificate Serial Number: 3E34CD199392A0914621EA778B13F357
Certificate Usage: Signature
:Issuer
CN = vpn
OU = cisco
O = tac
L = san jose
ST = california
C = US
:Subject
CN = vpn
OU = cisco
O = tac
L = san jose
ST = california
C = US
:CRL Distribution Point
http://tac-2hq8cg5ti0h/CertEnroll/vpn.crl
:Validity Date
start date: 21:19:50 PST Dec 6 2001
end date: 21:29:42 PST Dec 6 2003
Associated Trustpoints: caserver2

```

```
Certificate
Status: Available
Certificate Serial Number: 6111C66900000000034
Certificate Usage: Signature
:Issuer
CN = vpn
OU = cisco
O = tac
L = san jose
ST = california
C = US
:Subject
Name: 7204-1.cisco.com
Serial Number: 01691291
"OU = "BERLIN O=GERMANY
OID.1.2.840.113549.1.9.2 = 7204-1.cisco.com
OID.2.5.4.5 = 1691291
:CRL Distribution Point
http://tac-2hq8cg5ti0h/CertEnroll/vpn.crl
:Validity Date
start date: 19:10:35 PST Oct 26 2002
end date: 19:20:35 PST Oct 27 2002
Associated Trustpoints: caserver2
```

```
Certificate
Status: Available
Certificate Serial Number: 61123C0A000000000035
Certificate Usage: Encryption
:Issuer
CN = vpn
OU = cisco
O = tac
L = san jose
ST = california
C = US
:Subject
Name: 7204-1.cisco.com
Serial Number: 01691291
"OU = "BERLIN O=GERMANY
OID.1.2.840.113549.1.9.2 = 7204-1.cisco.com
OID.2.5.4.5 = 1691291
:CRL Distribution Point
http://tac-2hq8cg5ti0h/CertEnroll/vpn.crl
:Validity Date
start date: 19:11:05 PST Oct 26 2002
end date: 19:21:05 PST Oct 27 2002
renew date: 19:20:35 PST Oct 27 2002
Associated Trustpoints: caserver2
```

```
The system clock is used to view the time. 7204-1#show clock ---!
PST Sat Oct 26 2002 19:38:33.387*
7204-1#show clock
PST Sat Oct 26 2002 19:38:34.735*
7204-1#
7204-1#
7204-1#
7204-1#show clock
PST Sat Oct 26 2002 19:45:09.735*
7204-1#show clock
7204-1#show clock
PST Sun Oct 27 2002 17:28:30.662*
7204-1#show clock
PST Sun Oct 27 2002 17:28:48.646*
7204-1#
7204-1#show clock
PST Sun Oct 27 2002 17:41:15.410*
```

```
7204-1#
7204-1#show clock
PST Sun Oct 27 2002 18:08:45.430*
7204-1#show clock
PST Sun Oct 27 2002 18:24:54.702*
7204-1#show clock
PST Sun Oct 27 2002 18:37:13.322*
show clock 7204-1#
PST Sun Oct 27 2002 18:47:53.270*
show clock 7204-1#
PST Sun Oct 27 2002 18:58:56.202*
show clock 7204-1#
PST Sun Oct 27 2002 19:10:27.746*
show clock 7204-1#
PST Sun Oct 27 2002 19:10:31.254*
show clock 7204-1#
PST Sun Oct 27 2002 19:10:32.658*
show clock 7204-1#
PST Sun Oct 27 2002 19:15:44.054*
show clock 7204-1#
PST Sun Oct 27 2002 19:15:48.054*
show clock 7204-1#
PST Sun Oct 27 2002 19:15:49.606*
7204-1#show clock
PST Sun Oct 27 2002 19:17:02.882*
7204-1#show clock
PST Sun Oct 27 2002 19:17:15.722*
7204-1#
7204-1#
7204-1#
show clock
PST Sun Oct 27 2002 19:17:26.038*
7204-1#show clock
PST Sun Oct 27 2002 19:17:27.170*
7204-1#show clock
PST Sun Oct 27 2002 19:17:28.418*
7204-1#show clock
PST Sun Oct 27 2002 19:18:50.650*
7204-1#show debug
:Cryptographic Subsystem
Crypto PKI Msg debugging is on
Crypto PKI Trans debugging is on
7204-1#
7204-1#
PST Sun Oct 27 2002 19:19:16.574*
7204-1#show clock
PST Sun Oct 27 2002 19:19:22.202*
7204-1#show clock
PST Sun Oct 27 2002 19:19:23.762*
7204-1#show clock
PST Sun Oct 27 2002 19:19:25.354*
7204-1#show clock
PST Sun Oct 27 2002 19:19:28.202*
7204-1#show clock
PST Sun Oct 27 2002 19:19:34.482*
7204-1#show clock
PST Sun Oct 27 2002 19:19:53.118*
7204-1#show clock
PST Sun Oct 27 2002 19:19:55.014*
7204-1#show clock
PST Sun Oct 27 2002 19:20:28.654*
7204-1#show clock
PST Sun Oct 27 2002 19:20:32.770*
```

*The certificate renew date is 19:20:35 PST !--- Oct 27 2002. At the following time the ---!*

```

router automatically enrolls !--- with CA server2 in order to obtain another identity
certificate !--- before the current identity certificate expires. The router also !---
regenerates the RSA key pair. 7204-1#show clock
PST Sun Oct 27 2002 19:20:34.182*
7204-1#show clock
Time to re-enroll
trust_point caserver2
Can not select my full public
(key (ciscotac
PST Sun Oct 27 19:20:35.314*
2002
Start certificate enrollment 7204-1#%
..
The subject name in the certificate will %
be: OU=BERLIN O=GERMANY
The subject name in the certificate will %
be: 7204-1.cisco.com
The serial number in the certificate will %
be: 01691291
Certificate request sent to Certificate %
Authority
The certificate request fingerprint will %
.be displayed
The 'show crypto ca certificate' command %
.will also show the fingerprint
Oct 28 02:20:35: %SSH-5-DISABLED: SSH 1.5 has been disabled*
Oct 28 02:20:35: %CRYPTO-6-AUTOGEN: Generated new 512 bit key pair*
:Signing Certificate Reqeust Fingerprint
2EF6D7F3 AF5B4491 E254E6D0 229878CF
Oct 28 02:20:35: %SSH-5-ENABLED: SSH 1.5 has been enabled*
Oct 28 02:20:36: %CRYPTO-6-AUTOGEN: Generated new 512 bit key pair*
:Oct 28 02:20:36: CRYPTO_PKI:Insert Selfsigned Certificate*
4A 30 81 F5 02 20 35 45 35 42 44 43 01 82 30
39
hex data omitted
9F 2C DB 5F FA DC A2 DC E3 49 6D 28 C8 F8
= Oct 28 02:20:36: CRYPTO_PKI: InsertCertData: subject name*
1F 30 1D 06 09 2A 86 48 86 F7 0D 01 31 21 30
09
2D 31 2E 63 69 73 63 34 30 32 37 10 16 02
6F 2E
= 1 number
36 41 38 45 32 30 45 39 43 44 42 35 45 35
31 42
34 45 43 45 46 45 31 33 42 32 45 46 39 45
46 38
:Oct 28 02:20:36: CRYPTO_PKI: Sending CA Certificate Request*
GET /certsrv/mscep/mscep.dll/pkiclient.exe?operation=GetCACert&message=caserver2
HTTP/1.0
6F 6D 63
= Oct 28 02:20:36: CRYPTO_PKI: InsertCertData: issuer name*
1F 30 1D 06 09 2A 86 48 86 F7 0D 31 21 30
09 01
2D 31 2E 63 69 73 63 34 30 32 37 10 16 02
6F 2E
6F 6D 63
Oct 28 02:20:36: CRYPTO_PKI: InsertCertData: seria*
:Encryption Certificate Request Fingerprint
58D999C4 BA8F34FD F5C10A30 81D7A054
Oct 28 02:20:36: CRYPTO_PKI: can not resolve server name/IP address*
Oct 28 02:20:36: CRYPTO_PKI: Using unresolved IP Address 171.69.89.111*
Oct 28 02:20:36: CRYPTO_PKI: http connection opened*
:Oct 28 02:20:36: CRYPTO_PKI: HTTP response header*
HTTP/1.1 200 OK

```

Server: Microsoft-IIS/5.0  
Date: Mon, 28 Oct 2002 02:20:43 GMT  
Content-Length: 2811  
Content-Type: application/x-x509-ca-ra-cert

.Content-Type indicates we have received CA and RA certificates  
Oct 28 02:20:36: CRYPTO\_PKI:crypto\_process\_ca\_ra\_cKI:CA and RA certs\*

:(cert data)  
0A F7 06 09 2A 86 48 86 F7 0D 01 07 02 82 30  
A0

(0A E8 30 82 0A E4ert(trustpoint=caserver2 82

Oct 28 02:20:36: CRYPTO\_P 02 01 01 31 00 30 0B 06 09\*

hex data omitted

A9 13 93 1E E6 E1 E4 30 07 31 00

= Oct 28 02:20:36: CRYPTO\_PKI: InsertCertData: subject name\*

0B 30 09 06 03 55 04 06 13 02 55 53 31 61 30

31

hex data omitted

6E 70 76

= Oct 28 02:20:36: CRYPTO\_PKI: InsertCertData: issuer name\*

0B 30 09 06 03 55 04 06 13 02 55 53 31 61 30

31

hex data omitted

6E 70 76

= Oct 28 02:20:36: CRYPTO\_PKI: InsertCertData: serial number\*

3E 34 CD 19 93 92 A0 91 46 21 EA 77 8B 13 F3 57

= Oct 28 02:20:36: CRYPTO\_PKI: InsertCertData: subject name\*

1E 06 09 2A 86 48 86 F7 0D 30 20 31 83 81 30

01

hex data omitted

6B 69 2D 72 61 70

= Oct 28 02:20:36: CRYPTO\_PKI: InsertCertData: issuer name\*

0B 30 09 06 03 55 04 06 13 02 55 53 31 61 30

31

hex data omitted

6E 70 76

= Oct 28 02:20:36: CRYPTO\_PKI: InsertCertData: serial number\*

6C F2 85 00 00 00 00 09 14

Oct 28 02:20:36: CRYPTO\_PKI: WARNING: Certificate, private key or CRL\*

was not found while selecting CRL

= Oct 28 02:20:36: CRYPTO\_PKI: InsertCertData: subject name\*

1E 06 09 2A 86 48 86 F7 0D 30 20 31 83 81 30

01

hex data omitted

6B 69 2D 72 61 70

= Oct 28 02:20:36: CRYPTO\_PKI: InsertCertData: issuer name\*

0B 30 09 06 03 55 04 06 13 02 55 53 31 61 30

31

hex data omitted

6E 70 76

= Oct 28 02:20:36: CRYPTO\_PKI: InsertCertData: serial number\*

6C F1 A9 00 00 00 00 08 14

Oct 28 02:20:36: CRYPTO\_PKI: WARNING: Certificate, private key or CRL\*

was not found while selecting CRL

= Oct 28 02:20:36: CRYPTO\_PKI: InsertCertData: subject name\*

1E 06 09 2A 86 48 86 F7 0D 30 20 31 83 81 30

01

hex data omitted

6B 69 2D 72 61 70

= Oct 28 02:20:36: CRYPTO\_PKI: InsertCertData: issuer name\*

0B 30 09 06 03 55 04 06 13 02 55 53 31 61 30

31

hex data omitted

```

6E 70 76
= Oct 28 02:20:36: CRYPTO_PKI: InsertCertData: serial number*
6C F1 A9 00 00 00 00 08 14
= Oct 28 02:20:36: CRYPTO_PKI: InsertCertData: subject name*
1E 06 09 2A 86 48 86 F7 0D 30 20 31 83 81 30
01
hex data omitted
6B 69 2D 72 61 70
= Oct 28 02:20:36: CRYPTO_PKI: InsertCertData: issuer name*
0B 30 09 06 03 55 04 06 13 02 55 53 31 61 30
31
hex data omitted
6E 70 76
= Oct 28 02:20:36: CRYPTO_PKI: InsertCertData: serial number*
6C F2 85 00 00 00 00 09 14
= Oct 28 02:20:36: CRYPTO_PKI: InsertCertData: subject name*
0B 30 09 06 03 55 04 06 13 02 55 53 31 61 30
31
hex data omitted
6E 70 76
= Oct 28 02:20:36: CRYPTO_PKI: InsertCertData: issuer name*
0B 30 09 06 03 55 04 06 13 02 55 53 31 61 30
31
hex data omitted
6E 70 76
= Oct 28 02:20:36: CRYPTO_PKI: InsertCertData: serial number*
3E 34 CD 19 93 92 A0 91 46 21 EA 77 8B 13 F3 57
(Oct 28 02:20:36: CRYPTO_PKI: crypto_process_ra_certs(trust_point=caserver2*
Oct 28 02:20:36: CRYPTO_PKI: transaction PKCSReq completed*
:Oct 28 02:20:36: CRYPTO_PKI: status*
Oct 28 02:20:36: CRYPTO_PKI:Write out pkcs#10 content:319*
3B 30 81 E6 02 01 00 30 4C 31 19 01 82 30
17 30
hex data omitted
9A 0E DE 86 AB 85 DD 67 79 6B 67 1F 2B 53
51
...Oct 28 02:20:36: CRYPTO_PKI:Enveloped Data for trustpoint caserver2*
2A 86 48 86 F7 0D 01 07 03 A0 80 09 06 80 30
30
hex data omitted
00 00 00 00
Oct 28 02:20:36: CRYPTO_PKI:Signed Data for trustpoint caserver2 (1410*
(bytes
2A 86 48 86 F7 0D 01 07 02 A0 09 06 80 30
30 80
hex data omitted
00 00
Oct 28 02:20:36: CRYPTO_PKI: can not resolve server name/IP address*
Oct 28 02:20:36: CRYPTO_PKI: Using unresolved IP Address 171.69.89.111*
Oct 28 02:20:36: CRYPTO_PKI: http connection opened*
Oct 28 02:20:38: CRYPTO_PKI:Write out pkcs#10 content:319*
3B 30 81 E6 02 01 00 30 4C 31 19 01 82 30
17 30
hex data omitted
1E 74 00 9F A9 C1 ED 00 3C 7F 72 E3 61 D5
84
...Oct 28 02:20:38: CRYPTO_PKI:Enveloped Data for trustpoint caserver2*
2A 86 48 86 F7 0D 01 07 03 A0 80 09 06 80 30
30
hex data omitted
5A 0B 69 47 5E C6 23 4C 00 00 00 00 08 04
00 00
00 00 00 00
Oct 28 02:20:38: CRYPTO_PKI:Signed Data for trustpoint caserver2 (1410*
```



```
(bytes
2A 86 48 86 F7 0D 01 07 02 A0 09 06 80 30
30 80
hex data omitted
9F 8D B4 5F 00 00 00 00 87 84 93 05 86 65
00 00
00 00
Oct 28 02:20:38: CRYPTO_PKI: can not resolve server name/IP address*
Oct 28 02:20:38: CRYPTO_PKI: Using unresolved IP Address 171.69.89.111*
Oct 28 02:20:39: CRYPTO_PKI: http connection opened*
Oct 28 02:20:40: %AMDP2_FE-5-LATECOLL: Ethernet1/1 transmit error*
,Oct 28 02:20:41: %SCHED-3-STUCKTMR: Sleep with expired timer 63B997A8*
.(time 0x51A21B4 (00:00:00 ago
Process= "Crypto PKI RECV ", ipl= 4, pid= 92-
Traceback= 6064AD0C 6064B0C8 607237BC 60725E60 60796C00 6079C2B0 61CCF6D4-
61CC9838 61CC9944 61CC864C 60630A98 60630A84
Oct 28 02:20:41: CRYPTO_PKI: received msg of 1930 bytes*
:Oct 28 02:20:41: CRYPTO_PKI: HTTP response header*
HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Mon, 28 Oct 2002 02:20:46 GMT
Content-Length: 1784
Content-Type: application/x-pki-message

Oct 28 02:20:41: CRYPTO_PKI:Received pki message (PKCS7) for trustpoint*
caserver2: 1784 bytes
F4 06 09 2A 86 48 86 F7 0D 01 07 02 06 82 30
A0
hex data omitted
A0 82 04 AE 30 82 04 AA 02 01 00 31 81 9E
81 30
Oct 28 02:20:41: %CRYPTO-6-CERTRET: Certificate received from Certificate*
Authority
Oct 28 02:20:51: CRYPTO_PKI: received msg of 1930 bytes*
:Oct 28 02:20:51: CRYPTO_PKI: HTTP response header*
HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Mon, 28 Oct 2002 02:20:49 GMT
Content-Length: 1784
Content-Type: application/x-pki-message

Oct 28 02:20:51: CRYPTO_PKI:Received pki message (PKCS7) for trustpoint*
caserver2: 1784 bytes
F4 06 09 2A 86 48 86 F7 0D 01 07 02 06 82 30
A0
hex data omitted
ED 9F 4E 20 DB 91 A7 55
= Oct 28 02:20:51: CRYPTO_PKI: InsertCertData: subject name*
1E 06 09 2A 86 48 86 F7 0D 30 20 31 83 81 30
01
hex data omitted
6B 69 2D 72 61 70
= Oct 28 02:20:51: CRYPTO_PKI: InsertCertData: issuer name*
0B 30 09 06 03 55 04 06 13 02 55 53 31 61 30
31
hex data omitted
6E 70 76
= Oct 28 02:20:51: CRYPTO_PKI: InsertCertData: serial number*
6C F1 A9 00 00 00 00 08 14
Oct 28 02:20:51: CRYPTO_PKI: WARNING: Certificate, private key or CRL*
was not found while selecting CRL
:Oct 28 02:20:51: CRYPTO_PKI: signed attr: pki-message-type*
```

```

33 01 13
Oct 28 02:20:51: CRYPTO_PKI: signed attr: pki-status: 13*
30 01
:Oct 28 02:20:51: CRYPTO_PKI: signed attr: pki-recipient-nonce*
CE AB A0 E3 52 BD BF 95 D9 F8 DB 1A 10 04
D9 07
FA C6
:Oct 28 02:20:51: CRYPTO_PKI: signed attr: pki-transaction-id*
31 30 42 42 33 37 43 43 35 43 31 35 20 13
41 38
32 44 31 42 30 39 43 39 39 34 39 35 35 33
38 37
30 31
:Oct 28 02:20:51: CRYPTO_PKI: status = 100*
certificate is granted
Oct 28 02:20:51: CRYPTO_PKI:Verified signed*
:(data for trustpoint caserver2 (1217 bytes
BD 06 09 2A 86 48 86 F7 0D 01 07 04 82 30
A0 03
hex data omitted
3A 74 B6 8F F8 E5 29
Oct 28 02:20:52: CRYPTO_PKI: WARNING: Certificate, private key or*
CRL was not found while selecting CRL
Oct 28 02:21:02: CRYPTO_PKI: All enrollment*
.requests completed for trustpoint caserver2
7204-1#
7204-1#
7204-1#show crypto ca certificate
Certificate
Status: Available
Certificate Serial Number: 053859FC000000000039
Certificate Usage: Encryption
:Issuer
CN = vpn
OU = cisco
O = tac
L = san jose
ST = california
C = US
:Subject
Name: 7204-1.cisco.com
Serial Number: 01691291
"OU = "BERLIN O=GERMANY
OID.1.2.840.113549.1.9.2
cisco.com.7204-1 =
OID.2.5.4.5 = 1691291
:CRL Distribution Point
http://tac-2hq8cg5ti0h/CertEnroll/vpn.crl
:Validity Date
start date: 19:10:49 PST
2002
end date: 19:20:49
PST Oct 28 2002
renew date: 19:20:46 PST
Oct 28 2002
Associated Trustpoints: caserver2
Certificate
Status: Available
Certificate Serial Number: 05384E3F0000000000038
Certificate Usage: Signature
:Issuer
CN = vpn
OU = cisco

```

*Another identity certificate is !--- received and the renew date is now different. Oct 27 ---!*

```

O = tac
L = san jose
ST = california
C = US
:Subject
Name: 7204-1.cisco.com
Serial Number: 01691291
"OU = "BERLIN O=GERMANY
OID.1.2.840.113549.1.9.2 = 7204-1.cisco.com
OID.2.5.4.5 = 1691291
:CRL Distribution Point
http://tac-2hq8cg5ti0h/CertEnroll/vpn.crl
:Validity Date
start date: 19:10:46 PST Oct 27 2002
end date: 19:20:46 PST Oct 28 2002
Associated Trustpoints: caserver2
CA Certificate
Status: Available
Certificate Serial Number: 3E34CD199392A0914621EA778B13F357
Certificate Usage: Signature
:Issuer
CN = vpn
OU = cisco
O = tac
L = san jose
ST = california
C = US
:Subject
CN = vpn
OU = cisco
O = tac
L = san jose
ST = california
C = US
:CRL Distribution Point
http://tac-2hq8cg5ti0h/CertEnroll/vpn.crl
:Validity Date
start date: 21:19:50 PST Dec 6 2001
end date: 21:29:42 PST Dec 6 2003
Associated Trustpoints: caserver2

```

```

show crypto key mypubkey rsa 7204-1#
%
```

*The RSA key pair was regenerated at the time of !--- certificate auto-enroll. Key pair was ---!*  
**generated at: 19:20:35 PST  
Oct 27 2002**

```

Key name: ciscotac
Usage: Signature Key
:Key Data
305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00A540B1
062AEF70
081605F2 F81402EE A52DEAF4 05462747 CCE21BCC 8A1A21B0 C7BDF333
90728D48
68D46B81 19FC15EE 33045A3F 7BE50D85 FDD9F3DE 55E29F6F 67020301
0001
Key pair was generated at: 19:20:35 PST Oct 27 2002 %

```

```

Key name: ciscotac
Usage: Encryption Key
:Key Data
305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00A9F8A8
4E5AA9AF
22D9B0E0 B3754D5A 4387995D 23B09D8F E9AB70B7 CDF A126A 63A25EAF
055065EB

```

```

C076B36B 5A034A9D CE82206B 031C8231 B85DE829 E35FF874 39020301
                                0001
Key pair was generated at: 19:20:36 PST Oct 27 2002 %
Key name: ciscotac.server
Usage: Encryption Key
      :Key Data
307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00E47825
                                7E60D6AC
4C078368 925191FD 2B2AAC50 6A6D6AF1 8A01C9B6 D21C4C80 05DD8277
                                D63F60B1
01A2DDCF 407BE088 D333FE1D 4F5DE892 47970454 A50C54EC B962FEE4
                                A9BF5197
4C2B0656 503E0045 BB3168C4 2228155A B6BF0385 0B493FC5 79020301
                                0001
                                7204-1#
                                7204-1#
                                7204-1#

```

```

The router configuration with the new identity certificates. 7204-1# 7204-1#show run ---!
...Building configuration
Current configuration : 8245 bytes
!
version 12.2
service timestamps debug datetime
service timestamps log datetime
no service password-encryption
service udp-small-servers
service tcp-small-servers
no service dhcp
!
hostname 7204-1
!
boot system flash slot
boot system flash slot0:c7200-jk9o3s-mz.122-11.T1.bin
logging buffered 50000 debugging
enable secret 5 $1$GdwM$YPQYieph20DPAhQeNvHa30
enable password ipsecpki
!
username cisco password 0 cisco
clock timezone PST -7
ip subnet-zero
!
!
no ip domain lookup
ip domain name cisco.com
ip host caserver2 171.69.89.111
!
!
ip vrf test
no ip cef
ip audit notify log
ip audit po max-events 100
!
crypto ca trustpoint caserver2
enrollment retry period 2
enrollment mode ra
enrollment url http://171.69.89.111:80/certsrv/mscep/mscep.dll
usage ike
serial-number
ip-address none
password 7 094241071C
subject-name OU=BERLIN O=GERMANY
crl optional
rsa-keypair ciscotac
auto-enroll regenerate

```

```
crypto ca certificate chain caserver2
certificate 053859FC000000000039
308203AA 30820354 A0030201 02020A05 3859FC00 00000000 39300D06
092A8648
```

```
Certificate is abbreviated for easier viewing. quit certificate 05384E3F0000000000038 ---!
308203AA 30820354 A0030201 02020A05 384E3F00 00000000 38300D06 092A8648 86F70D01 01050500
3061310B 30090603 55040613 02555331 13301106 03550408 !--- Certificate is abbreviated for easier
viewing. quit certificate ca 3E34CD199392A0914621EA778B13F357 30820284 3082022E A0030201
0202103E 34CD1993 92A09146 21EA778B 13F35730 0D06092A 864886F7 0D010105 05003061 310B3009
06035504 06130255 53311330 !--- Certificate is abbreviated for easier viewing. quit ! crypto
isakmp policy 10 hash md5 crypto isakmp identity hostname - ! ! crypto ipsec transform-set myset
esp-des esp-md5-hmac ! crypto map vpn 10 ipsec-isakmp set peer 172.16.172.35 set transform-set
myset match address 101 ! ! ! voice call carrier capacity active ! ! interface Ethernet1/0 no ip
address duplex half ! interface Ethernet1/1 ip address 172.16.172.51 255.255.255.240 no ip
redirects duplex half crypto map vpn !interface Ethernet1/2 ip address 3.3.3.2 255.255.255.0 no
keepalive duplex half ! interface Ethernet1/3 no ip address duplex half ! interface Hssi4/0 ip
address 200.1.1.1 255.255.255.0 load-interval 30 fair-queue 64 16 0 hssi dce serial
restart_delay 0 clockrate 1524705 ! ip classless ip route 0.0.0.0 0.0.0.0 172.16.172.49 no ip
http server ip pim bidir-enable ! ! access-list 101 permit ip 3.3.3.0 0.0.0.255 192.168.4.0
0.0.0.255 ! snmp-server community public RO snmp-server enable traps tty ! ! call rsvp-sync ! !
mgcp profile default ! dial-peer cor custom ! ! ! ! gatekeeper shutdown ! ! line con 0 exec-
timeout 0 0 line aux 0 line vty 0 4 privilege level 15 password cisco login line vty 5 15 login
! no scheduler max-task-time ! end 7204-1# 7204-1#
```

يعرض هذا الإخراج الأمر **show crypto ca certificate** على الموجه 1-1720 الذي يعرض إعادة إنشاء مفتاح RSA.

```
1720-1#
1720-1#show crypto ca certificate
CA Certificate
Status: Available
Certificate Serial Number: 0E7EC1B68A2F14BD4C4515AF44C45732
Certificate Usage: Signature
:Issuer
CN = SJVPNTAC-CAServer
OU = TAC-VPN-SJ
O = Cisco Systems
L = San Jose
ST = CA
C = US
:Subject
CN = SJVPNTAC-CAServer
OU = TAC-VPN-SJ
O = Cisco Systems
L = San Jose
ST = CA
C = US
:CRL Distribution Point
http://ca-server/CertEnroll/SJVPNTAC-CAServer.crl
:Validity Date
start date: 20:52:48 UTC Sep 17 2002
end date: 21:02:37 UTC Sep 17 2017
Associated Trustpoints: caserver1
```

```
Certificate
Status: Available
Certificate Serial Number: 611652F7000000000003A
Certificate Usage: Signature
:Issuer
CN = SJVPNTAC-CAServer
OU = TAC-VPN-SJ
O = Cisco Systems
L = San Jose
ST = CA
```

```
C = US
:Subject
Name: 1720-1.tac.com
IP Address: 172.16.172.45
Serial Number: 2F31F46E
"OU = "MADRID O=SPAIN
OID.1.2.840.113549.1.9.2 = 1720-1.tac.com
OID.1.2.840.113549.1.9.8 = 172.16.172.45
OID.2.5.4.5 = 2F31F46E
:CRL Distribution Point
http://ca-server/CertEnroll/SJVPNTAC-CAServer.crl
:Validity Date
start date: 03:53:11 UTC Oct 26 2002
end date: 04:03:11 UTC Oct 26 2003
Associated Trustpoints: caserver1
```

```
Certificate
Status: Available
Certificate Serial Number: 61165F5B000000000003B
Certificate Usage: Encryption
:Issuer
CN = SJVPNTAC-CAServer
OU = TAC-VPN-SJ
O = Cisco Systems
L = San Jose
ST = CA
C = US
:Subject
```

```
Name: 1720-1.tac.com
IP Address: 172.16.172.45
Serial Number: 2F31F46E
"OU = "MADRID O=SPAIN
OID.1.2.840.113549.1.9.2 = 1720-1.tac.com
OID.1.2.840.113549.1.9.8 = 172.16.172.45
OID.2.5.4.5 = 2F31F46E
:CRL Distribution Point
http://ca-server/CertEnroll/SJVPNTAC-CAServer.crl
:Validity Date
start date: 03:53:14 UTC Oct 26 2002
end date: 04:03:14 UTC Oct 26 2003
renew date: 04:03:11 UTC Oct 26 2003
Associated Trustpoints: caserver1
```

يعرض هذا الإخراج الأمر **show crypto key** على الموجة 1-1720.

```
1720-1#show crypto key mypubkey rsa
Key pair was generated at: 00:49:35 UTC Mar 1 1993 %
Key name: ipsecpki
Usage: Signature Key
:Key Data
305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00D3D4B1 CC3DC9DE
04373E6C F3ADA37B DBE56BD4 C9945889 E24626DF D0CC45FE 7CBA196C 1DB10C15
EE6332F8 A614561E 991549DD 787E4D7C 30ECC465 B0D67BEA E1020301 0001
Key pair was generated at: 00:49:36 UTC Mar 1 1993 %
Key name: ipsecpki
Usage: Encryption Key
:Key Data
305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00C6D61D D126D546
678D5C7D A99E9D22 E2B7C82E 72D69478 3A241FE9 A5F5B761 81A6A85D 9389FD03
D27D58CF 21122EF5 8B3F4278 B2C71C58 DD0E5485 B00A02AE 0B020301 0001
Key pair was generated at: 21:30:31 UTC Oct 27 2002 %
Key name: ipsecpki.server
```

**Usage: Encryption Key**

:Key Data

```

307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00DB0878 020052BA
BE67DEBF 001DA215 D6EB8CA9 8DD5B077 A27809D7 792166C4 5F1F2AD4 F4BE813B
087E1747 4677570B 7F692A78 D897951A B37A1A0B 1E167044 F6ADA763 67AECAE6
BF2D9AF3 0EA492B5 1E601EAF 7E280B80 091A2D89 2116685A 59020301 0001

```

**عندما لا يكون زوج مفاتيح RSA موجودا**

إذا لم يكن زوج مفاتيح RSA موجودا أثناء التسجيل التلقائي، فسيتم إنشاء زوج من مفاتيح الأغراض العامة والاستخدام تلقائياً أثناء التسجيل، كما يظهر هذا الإخراج. يبدأ هذا المثال بدون تكوين شهادة على الموجه 1-7204 ولا يتم إنشاء زوج مفاتيح RSA.

**show run**

```

...Building configuration
Current configuration : 1828 bytes
!
version 12.2
service timestamps debug datetime
service timestamps log datetime
no service password-encryption
service udp-small-servers
service tcp-small-servers
no service dhcp
!
hostname 7204-1
!
boot system flash slot
boot system flash slot0:c7200-jk9o3s-mz.122-11.T1.bin
logging buffered 50000 debugging
enable secret 5 $1$GdwM$YPQYieph20DPAhQeNvHa30
enable password ipsecpki
!
username cisco password 0 cisco
clock timezone PST -7
ip subnet-zero
!
!
no ip domain lookup
ip domain name cisco.com
ip host caserver2 171.69.89.111
!
!
ip vrf test
no ip cef
ip audit notify log
ip audit po max-events 100
!
crypto isakmp policy 10
hash md5
crypto isakmp identity hostname
!
!
crypto ipsec transform-set myset esp-des esp-md5-hmac
!
crypto map vpn 10 ipsec-isakmp
set peer 172.16.172.35
set transform-set myset
match address 101
!
!

```

```
voice call carrier capacity active
!
!
interface Ethernet1/0
no ip address
duplex half
!
interface Ethernet1/1
ip address 172.16.172.51 255.255.255.240
no ip redirects
duplex half
crypto map vpn
!
interface Ethernet1/2
ip address 3.3.3.2 255.255.255.0
no keepalive
duplex half
!
interface Ethernet1/3
no ip address
duplex half
!
interface Hssi4/0
ip address 200.1.1.1 255.255.255.0
load-interval 30
fair-queue 64 16 0
hssi dce
serial restart_delay 0
clockrate 1524705
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.16.172.49
no ip http server
ip pim bidir-enable
!
!
access-list 101 permit ip 3.3.3.0 0.0.0.255 192.168.4.0 0.0.0.255
!
snmp-server community public RO
snmp-server enable traps tty
!
!
call rsvp-sync
!
!
mgcp profile default
!
dial-peer cor custom
!
!
!
!
gatekeeper
shutdown
!
!
line con 0
exec-timeout 0 0
line aux 0
line vty 0 4
privilege level 15
password cisco
login
line vty 5 15
```



```

login
!
no scheduler max-task-time
!
end

7204-1#show clock
PST Mon Oct 28 2002 17:18:44.780*
7204-1#conf t
7204-1#show crypto key mypubkey rsa
7204-1#show cry key mypubkey rsa
An RSA key pair has not been generated. 7204-1#show cry key mypubkey rsa ---!
7204-1#
7204-1#
7204-1#
7204-1#
7204-1#configure terminal
Defining the CA server communication parameters. Enter configuration commands, one per ---!
line. End with CNTL/Z. 7204-1(config)#crypto ca trustpoint caserver2
ca-trustpoint)# enrollment retry period 2)7204-1
ca-trustpoint)# enrollment mode ra)7204-1
ca-trustpoint)# enrollment url http://171.69.89.111:80/certsrv/mscep/mscep.dll)7204-1
ca-trustpoint)# usage ike)7204-1
ca-trustpoint)# serial-number)7204-1
ca-trustpoint)# ip-address none)7204-1
ca-trustpoint)# password 7 030A540503)7204-1
ca-trustpoint)# subject-name OU=BERLIN O=GERMANY)7204-1
ca-trustpoint)# crl optional)7204-1
ca-trustpoint)# rsakeypair ciscotac)7204-1
ca-trustpoint)# auto-enroll regenerate)7204-1
#(ca-trustpoint)7204-1
ca-trustpoint)#^Z)7204-1
7204-1#
7204-1#
7204-1#
7204-1#
7204-1#
7204-1#
Oct 29 00:19:39: %SYS-5-CONFIG_I: Configured from console by consolesh*
clo
7204-1#show clock
PST Mon Oct 28 2002 17:19:42.656*
7204-1#show run
...Building configuration
Current configuration : 2131 bytes
!
version 12.2
service timestamps debug datetime
service timestamps log datetime
no service password-encryption
service udp-small-servers
service tcp-small-servers
no service dhcp
!
hostname 7204-1
!
boot system flash slot
boot system flash slot0:c7200-jk9o3s-mz.122-11.T1.bin
logging buffered 50000 debugging
enable secret 5 $1$GdwM$YPQYieph20DPAhQeNvHa30
enable password ipsecpki
!
username cisco password 0 cisco
clock timezone PST -7
ip subnet-zero

```

```

!
!
no ip domain lookup
ip domain name cisco.com
ip host caserver2 171.69.89.111
!
!
ip vrf test
no ip cef
ip audit notify log
ip audit po max-events 100
!
crypto ca trustpoint caserver2
enrollment retry period 2
enrollment mode ra
enrollment url http://171.69.89.111:80/certsrv/mscep/mscep.dll
usage ike
serial-number
ip-address none
password 7 000A1C0801
subject-name OU=BERLIN O=GERMANY
crl optional
rsakeypair ciscotac
auto-enroll regenerate
crypto isakmp policy 10
hash md5
crypto isakmp identity hostname
!
!
crypto ipsec transform-set myset esp-des esp-md5-hmac
!
crypto map vpn 10 ipsec-isakmp
set peer 172.16.172.35
set transform-set myset
match address 101
!
!
!
voice call carrier capacity active
!
!
!
!
!
!
!
!
!
!
!
7204-1#debug crypto pki transactions
Crypto PKI Trans debugging is on
7204-1#
7204-1#configure terminal
.Enter configuration commands, one per line. End with CNTL/Z
config)#crypto ca authenticate)7204-1
caserver2
:Certificate has the following attributes
Fingerprint: A1E8B61A FD1A66D6 2DE35501 99C43D83
:[Do you accept this certificate? [yes/no %
:Oct 29 00:20:56: CRYPTO_PKI: Sending CA Certificate Request*
GET /certsrv/mscep/mscep.dll/pkiclient.exe?operation=GetCACert&message=caserver2
HTTP/1.0
Oct 29 00:20:56: CRYPTO_PKI: can not resolve server name/IP address*
Oct 29 00:20:56: CRYPTO_PKI: Using unresolved IP Address 171.69.89.111*
Oct 29 00:20:56: CRYPTO_PKI: http connection opened*
:Oct 29 00:20:56: CRYPTO_PKI: HTTP response header*

```

HTTP/1.1 200 OK  
Server: Microsoft-IIS/5.0  
Date: Tue, 29 Oct 2002 00:21:02 GMT  
Content-Length: 2811  
Content-Type: application/x-x509-ca-ra-cert

.Content-Type indicates we have received CA and RA certificates

```
Y
.Trustpoint CA certificate accepted
#(config)7204-1
(Oct 29 00:20:56: CRYPTO_PKI:crypto_process_ca_ra_cert(trustpoint=caserver2*
Oct 29 00:20:56: CRYPTO_PKI: WARNING: Certificate, private key or CRL*
was not found while selecting CRL
Oct 29 00:20:56: CRYPTO_PKI: WARNING: Certificate, private key or CRL*
was not found while selecting CRL
Oct 29 00:20:56: CRYPTO_PKI: transaction GetCACert completed*
Oct 29 00:20:56: CRYPTO_PKI: CA certificate*
.received
.Oct 29 00:20:56: CRYPTO_PKI: CA certificate received*
()Oct 29 00:20:56: CRYPTO_PKI: crypto_pki_authenticate_tp_cert*
Oct 29 00:20:56: CRYPTO_PKI: trustpoint caserver2 authentication status*
2 =
(Oct 29 00:20:58: CRYPTO_PKI: crypto_process_ra_certs(trust_point=caserver2*
#(config)7204-1
```

```
7204-1#show crypto key mypubkey rsa
The RSA key pair has not yet been generated. !--- Only the CA has been authenticated. 7204- ---!
1#show crypto ca certificate
```

```
Only the CA certificate has been received. CA Certificate Status: Available Certificate ---!
Serial Number: 3E34CD199392A0914621EA778B13F357 Certificate Usage: Signature Issuer: CN = vpn OU
= cisco O = tac L = san jose ST = california C = US Subject: CN = vpn OU = cisco O = tac L = san
jose ST = california C = US CRL Distribution Point: http://tac-2hq8cg5ti0h/CertEnroll/vpn.crl
Validity Date: start date: 21:19:50 PST Dec 6 2001 end date: 21:29:42 PST Dec 6 2003 Associated
Trustpoints: caserver2
```

```
Time to Re-enroll trust_point caserver2 7204-1#
(Can not select my full public key (ciscotac
(Can not select my full public key (ciscotac
%(Can not select my full public key (ciscotac
.. Start certificate enrollment %
The subject name in the certificate will %
be: OU=BERLIN O=GERMANY
The subject name in the certificate will %
be: 7204-1.cisco.com
The serial number in the certificate will %
be: 01691291
Certificate request sent to Certificate %
Authority
The certificate request fingerprint will %
.be displayed
The 'show crypto ca certificate' command %
.will also show the fingerprint
```

```
key mypubkey
rsa Fingerprint: 6FD37B13 7329725C B524C666 2CFB08BB
Oct 29 00:22:13: %SSH-5-ENABLED: SSH 1.5 has been enabled*
Oct 29 00:22:13: %CRYPTO-6-AUTOGEN: Generated new 512 bit key pair*
:Oct 29 00:22:13: CRYPTO_PKI: Sending CA Certificate Request*
GET /certsrv/mscep/mscep.dll/pkiclient.exe?operation=GetCACert&message=caserver2
HTTP/1.0
Oct 29 00:22:13: CRYPTO_PKI: can not resolve server name/IP address*
Oct 29 00:22:13: CRYPTO_PKI: Using unresolved IP Address 171.69.89.111*
Oct 29 00:22:13: CRYPTO_PKI: http connection opened*
:Oct 29 00:22:14: CRYPTO_PKI: HTTP response header*
HTTP/1.1 200 OK
```

Server: Microsoft-IIS/5.0  
Date: Tue, 29 Oct 2002 00:22:20 GMT  
Content-Length: 2811  
Content-Type: application/x-x509-ca-ra-cert

.Content-Type indicates we have received CA and RA certificates  
(Oct 29 00:22:14: CRYPTO\_PKI:crypto\_process\_ca\_ra\_cert(trustpoint=caserver2\*  
Oct 29 00:22:14: CRYPTO\_PKI: WARNING: Certificate, private key or CRL\*  
was not found while selecting CRL  
Oct 29 00:22:14: CRYPTO\_PKI: WARNING: Certificate, private key or CRL\*  
was not found while selecting CRL  
(Oct 29 00:22:14: CRYPTO\_PKI: crypto\_process\_ra\_certs(trust\_point=caserver2\*  
Oct 29 00:22:14: CRYPTO\_PKI: transaction PKCSReq completed\*  
:Oct 29 00:22:14: CRYPTO\_PKI: status\*  
Oct 29 00:22:14: CRYPTO\_PKI: All sockets are closed for trustpoint\*  
.caserver2  
Oct 29 00:22:14: CRYPTO\_PKI: can not resolve server name/IP address\*  
Oct 29 00:22:14: CRYPTO\_PKI: Using unresolved IP Address 171.69.89.111\*  
Oct 29 00:22:14: CRYPTO\_PKI: http connection opened\*  
Oct 29 00:22:16: CRYPTO\_PKI: received msg of 1930 bytes\*  
:Oct 29 00:22:16: CRYPTO\_PKI: HTTP response header\*  
HTTP/1.1 200 OK  
Server: Microsoft-IIS/5.0  
Date: Tue, 29 Oct 2002 00:22:22 GMT  
Content-Length: 1784  
Content-Type: application/x-pki-message

Oct 29 00:22:16: CRYPTO\_PKI: WARNING: Certificate, private key or CRL\*  
was not found while selecting CRL  
Oct 29 00:22:16: CRYPTO\_PKI: status = 100: certificate is granted\*  
Oct 29 00:22:16: CRYPTO\_PKI: WARNING: Certificate, private key or\*  
CRL was not found while selecting CRL  
Oct 29 00:22:16: **CRYPTO\_PKI: All enrollment\*  
.requests completed for trustpoint caserver2**  
Oct 29 00:22:16: CRYPTO\_PKI: All enrollment requests completed for\*  
.trustpoint caserver2  
Oct 29 00:22:16: %CRYPTO-6-CERTRET: Certificate received from Certificate\*  
Authority  
Oct 29 00:22:16: **CRYPTO\_PKI: All enrollment\*  
.requests completed for trustpoint caserver2**  
.Oct 29 00:22:16: %CRYPTO-4-NOAUTOSAVE: Configuration was modified\*  
Issue "write memory" to save new certificate  
Oct 29 00:22:16: CRYPTO\_PKI: WARNING: Certificate, private key or\*  
CRL was not found while selecting CRL  
Oct 29 00:22:16: CRYPTO\_PKI: All enrollment requests completed for\*  
.trustpoint caserver2  
**Key pair was generated at: 17:22:13 PST %  
Oct 28 2002  
Key name: ciscotac  
Usage: General Purpose Key  
:Key Data  
305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00B05722  
43B43599  
A2506398 A2205406 755D3AA2 9888FD4C 76CF3C78 CA91BA4A 5EDB4BF8  
121A924D  
A093D24C 282085BD 3ED9AD76 4CD8C7AD 0EA5582C 70D4E5AF FD020301  
0001  
Key pair was generated at: 17:22:13 PST Oct 28 2002 %  
Key name: ciscotac.server  
Usage: Encryption Key  
:Key Data  
307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00CE8A87**

0698C6DF  
D13D7CF8 C5504394 24D23E0E 2B8367AE 11E6F5AF BD5B6A27 11E63F99  
EB768894  
A234A6FD 54B90A93 F352B551 08FC32E7 5D0B1F68 2E42974A 4BEB7A9C  
EA989DD1  
35267E59 D1C84CC5 DA436E72 8BAB6B3B 60D0AB62 129FAB02 1F020301  
0001  
7204-1#  
7204-1#  
7204-1#

7204-1#show crypto key mypubkey rsa

Key pair was generated at: 17:22:13 PST Oct 28 2002 %

Key name: ciscotac

*As defined in the configuration, a general !--- purpose RSA key pair.* Usage: General ---!

Purpose Key was generated during auto-enrollment. Key Data: 305C300D 06092A86 4886F70D 01010105

00034B00 30480241 00B05722 43B43599 A2506398 A2205406 755D3AA2 9888FD4C 76CF3C78 CA91BA4A

5EDB4BF8 121A924D A093D24C 282085BD 3ED9AD76 4CD8C7AD 0EA5582C 70D4E5AF FD020301 0001 % Key pair

was generated at: 17:22:13 PST Oct 28 2002 Key name: ciscotac.server Usage: Encryption Key Key

Data: 307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00CE8A87 0698C6DF D13D7CF8 C5504394

24D23E0E 2B8367AE 11E6F5AF BD5B6A27 11E63F99 EB768894 A234A6FD 54B90A93 F352B551 08FC32E7

5D0B1F68 2E42974A 4BEB7A9C EA989DD1 35267E59 D1C84CC5 DA436E72 8BAB6B3B 60D0AB62 129FAB02

1F020301 0001 7204-1# 7204-1# 7204-1# 7204-1#show crypto ca certificate

Certificate

Status: Available

Certificate Serial Number: 09F246B800000000003C

Certificate Usage: General Purpose

:Issuer

CN = vpn

OU = cisco

O = tac

L = san jose

ST = california

C = US

:Subject

Name: 7204-1.cisco.com

Serial Number: 01691291

"OU = "BERLIN O=GERMANY

OID.1.2.840.113549.1.9.2 = 7204-1.cisco.com

OID.2.5.4.5 = 1691291

:CRL Distribution Point

<http://tac-2hq8cg5ti0h/CertEnroll/vpn.crl>

:Validity Date

start date: 17:12:22 PST Oct 28 2002

end date: 17:22:22 PST Oct 29 2002

Associated Trustpoints: caserver2

CA Certificate

Status: Available

Certificate Serial Number: 3E34CD199392A0914621EA778B13F357

Certificate Usage: Signature

:Issuer

CN = vpn

OU = cisco

O = tac

L = san jose

ST = california

C = US

:Subject

CN = vpn

OU = cisco

O = tac

L = san jose

ST = california

C = US

:CRL Distribution Point

```
http://tac-2hq8cg5ti0h/CertEnroll/vpn.crl
:Validity Date
start date: 21:19:50 PST Dec 6 2001
end date: 21:29:42 PST Dec 6 2003
Associated Trustpoints: caserver2
```

```
7204-1#
```

```
7204-1#
```

```
Generates an RSA usage-key pair. 7204-1# 7204-1# 7204-1#show run ---!
```

```
...Building configuration
Current configuration : 2139 bytes
!
version 12.2
service timestamps debug datetime
service timestamps log datetime
no service password-encryption
service udp-small-servers
service tcp-small-servers
no service dhcp
!
hostname 7204-1
!
boot system flash slot
boot system flash slot0:c7200-jk9o3s-mz.122-11.T1.bin
logging buffered 50000 debugging
enable secret 5 $1$GdwM$YPQYieph20DPAhQeNvHa30
enable password ipsecpki
!
username cisco password 0 cisco
clock timezone PST -7
ip subnet-zero
!
no ip domain lookup
ip domain name cisco.com
ip host caserver2 171.69.89.111
!
!
ip vrf test
no ip cef
ip audit notify log
ip audit po max-events 100
!
crypto ca trustpoint caserver2
enrollment retry period 2
enrollment mode ra
enrollment url http://171.69.89.111:80/certsrv/mscep/mscep.dll
usage ike
serial-number
ip-address none
password 7 0608002F49
subject-name OU=BERLIN O=GERMANY
crl optional
rsakeypair ciscotac 512 512
```

```
The RSA key pair defined is for usage-keys. auto-enroll regenerate crypto isakmp policy 10 ---!
hash md5 crypto isakmp identity hostname ! ! crypto ipsec transform-set myset esp-des esp-md5-
hmac ! crypto map vpn 10 ipsec-isakmp set peer 172.16.172.35 set transform-set myset match
address 101 ! ! ! voice call carrier capacity active ! ! interface Ethernet1/0 no ip address
duplex half ! interface Ethernet1/1 ip address 172.16.172.51 255.255.255.240 no ip redirects
duplex half crypto map vpn ! interface Ethernet1/2 ip address 3.3.3.2 255.255.255.0 no keepalive
duplex half ! interface Ethernet1/3 no ip address duplex half ! interface Hssi4/0 ip address
200.1.1.1 255.255.255.0 load-interval 30 fair-queue 64 16 0 hssi dce serial restart_delay 0
clockrate 1524705 ! ip classless ip route 0.0.0.0 0.0.0.0 172.16.172.49 no ip http server ip pim
bidir-enable ! ! access-list 101 permit ip 3.3.3.0 0.0.0.255 192.168.4.0 0.0.0.255 ! snmp-server
community public RO snmp-server enable traps tty ! ! call rsvp-sync ! ! mgcp profile default !
```



```

#(config)7204-1
config)#% Time to Re-enroll trust_point)7204-1
caserver2
(Can not select my full public key (ciscotac
(Can not select my full public key (ciscotac
%(Can not select my full public key (ciscotac
.. Start certificate enrollment
The subject name in the certificate will %
be: OU=BERLIN O=GERMANY
The subject name in the certificate will %
be: 7204-1.cisco.com
The serial number in the certificate will %
be: 01691291
Certificate request sent to Certificate %
Authority
The certificate request fingerprint will %
.be displayed
The 'show crypto ca certificate' command %
.will also show the fingerprint
Oct 29 00:29:10: %CRYPTO-6-AUTOGEN: Generated new 512 bit key pair*
:Signing Certificate Reqeust Fingerprint
D3EA83A5 B255CDA0 C65BF99D 4C1A978B
Oct 29 00:29:10: %SSH-5-ENABLED: SSH 1.5 has been enabled*
Oct 29 00:29:10: %CRYPTO-6-AUTOGEN: Generated new 512 bit key pair*
:Oct 29 00:29:10: CRYPTO_PKI: Sending CA Certificate Request*
GET /certsrv/mscep/mscep.dll/pkiclient.exe?operation=GetCACert&message;=caserver2
HTTP/1.0

Oct 29 00:29:10: CRYPTO_PKI: can not resolve server name/IP address*
Oct 29 00:29:10: CRYPTO_PKI: Using unresolved IP Address 171.69.89.111*
Oct 29 00:29:11: CRYPTO_PKI: http connection opened*
:Oct 29 00:29:11: CRYPTO_PKI: HTTP response header*
HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Tue, 29 Oct 2002 00:29:17 GMT
Content-Length: 2811
Content-Type: application/x-x509-ca-ra-cert

.Content-Type indicates we have received CA and RA certificates
(Oct 29 00:29:11: CRYPTO_PKI:crypto_process_ca_ra_cert(trustpoint=caserver2*
Oct 29 00:29:11: CRYPTO_PKI: WARNING: Certificate, private key or CRL*
was not found while selecting CRL
Oct 29 00:29:11: CRYPTO_PKI: WARNING: Certificate, private key or CRL*
was not found while selecting CRL
(Oct 29 00:29:11: CRYPTO_PKI: crypto_process_ra_certs(trust_point=caserver2*
Oct 29 00:29:11: CRYPTO_PKI: transaction PKCSReq completed*
:Oct 29 00:29:11: CRYPTO_PKI: status*
Oct 29 00:29:11: CRYPTO_PKI: All sockets are closed for trustpoint*
.caserver2
Oct 29 00:29:11: CRYPTO_PKI: can not resolve server name/IP address*
Oct 29 00:29:11: CRYPTO_PKI: Using unresolved IP Address 171.69.89.111*
Oct 29 00:29:11: CRYPTO_PKI: http connection opened*
:Encryption Certificate Request Fingerprint
3258F1D9 0412BFA8 2FD14FBC B7345089
Oct 29 00:29:13: CRYPTO_PKI: can not resolve server name/IP address*
Oct 29 00:29:13: CRYPTO_PKI: Using unresolved IP Address 171.69.89.111*
Oct 29 00:29:13: CRYPTO_PKI: http connection opened*
Oct 29 00:29:15: CRYPTO_PKI: received msg of 1930 bytes*
:Oct 29 00:29:15: CRYPTO_PKI: HTTP response header*
HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Tue, 29 Oct 2002 00:29:19 GMT
```



Content-Length: 1784  
Content-Type: application/x-pki-message

Oct 29 00:29:15: CRYPTO\_PKI: WARNING: Certificate, private key or CRL\*  
was not found while selecting CRL  
Oct 29 00:29:15: CRYPTO\_PKI: status = 100: certificate is granted\*  
Oct 29 00:29:15: CRYPTO\_PKI: WARNING: Certificate, private key or\*  
CRL was not found while selecting CRL  
Oct 29 00:29:15: %CRYPTO-6-CERTRET: Certificate received from Certificate\*  
Authority  
Oct 29 00:29:25: CRYPTO\_PKI: received msg of 1930 bytes\*  
:Oct 29 00:29:25: CRYPTO\_PKI: HTTP response header\*  
HTTP/1.1 200 OK  
Server: Microsoft-IIS/5.0  
Date: Tue, 29 Oct 2002 00:29:21 GMT  
Content-Length: 1784  
Content-Type: application/x-pki-message

Oct 29 00:29:25: CRYPTO\_PKI: WARNING: Certificate, private key or CRL\*  
was not found while selecting CRL  
Oct 29 00:29:25: CRYPTO\_PKI: status = 100: certificate is granted\*  
Oct 29 00:29:25: CRYPTO\_PKI: WARNING: Certificate, private key or\*  
CRL was not found while selecting CRL  
**Oct 29 00:29:25: CRYPTO\_PKI: All enrollment\*  
.requests completed for trustpoint caserver2**  
**Oct 29 00:29:25: CRYPTO\_PKI: All enrollment\*  
.requests completed for trustpoint caserver2**  
**Oct 29 00:29:25: %CRYPTO-6-CERTRET: Certificate\*  
received from Certificate Authority**  
**Oct 29 00:29:25: CRYPTO\_PKI: All enrollment\*  
.requests completed for trustpoint caserver2**  
.Oct 29 00:29:25: %CRYPTO-4-NOAUTOSAVE: Configuration was modified\*  
Issue "write memory" to save new certificate  
Oct 29 00:29:25: CRYPTO\_PKI: WARNING: Certificate, private key or\*  
CRL was not found while selecting CRL  
Oct 29 00:29:25: CRYPTO\_PKI: All enrollment requests completed for\*  
.trustpoint caserver2  
#(config)7204-1  
config)#^Z)7204-1  
7204-1#  
7204-1#  
7204-1#  
7204-1#  
Oct 29 00:30:32: %SYS-5-CONFIG\_I: Configured from console by console\*  
7204-1#

*An RSA usage-key pair was generated.* 7204-1#show crypto key mypubkey rsa ----!  
**Key pair was generated at: 17:29:10 PST %  
Oct 28 2002**  
Key name: ciscotac  
Usage: Signature Key  
:Key Data  
305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00E29E58  
FD93989D  
F6997DA1 D191123C 661FEB81 789522EE 0CB8D5AD 8A4E9DED E5CDCFDC  
78829A68  
41962AD9 5D51AA21 F1C31271 23A7EA4D 6F632CD1 2CFD95C9 D3020301  
0001  
Key pair was generated at: 17:29:10 PST Oct 28 2002 %  
Key name: ciscotac  
Usage: Encryption Key  
:Key Data  
305C300D 06092A86 4886F70D 01010105 00034B00 30480241 009FB6F5  
73B9C0D7  
0BF59C1F 579606A6 E4CEE4AD 8BC307B9 3EC3955B 5FA1B355 665750E2

EC09F8EF  
2B5F1D72 0E2FDB8B 0AA16911 492A749F 08113C64 6A203BB7 A9020301  
0001  
Key pair was generated at: 17:29:11 PST Oct 28 2002 %  
Key name: ciscotac.server  
Usage: Encryption Key  
:Key Data  
307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00CE8A87  
0698C6DF  
D13D7CF8 C5504394 24D23E0E 2B8367AE 11E6F5AF BD5B6A27 11E63F99  
EB768894  
A234A6FD 54B90A93 F352B551 08FC32E7 5D0B1F68 2E42974A 4BEB7A9C  
EA989DD1  
35267E59 D1C84CC5 DA436E72 8BAB6B3B 60D0AB62 129FAB02 1F020301  
0001  
7204-1#  
7204-1#  
7204-1#

7204-1#**show crypto ca certificate**

Certificate  
Status: Available  
Certificate Serial Number: 09F8AC9500000000003E  
Certificate Usage: Encryption  
:Issuer  
CN = vpn  
OU = cisco  
O = tac  
L = san jose  
ST = california  
C = US  
:Subject  
Name: 7204-1.cisco.com  
Serial Number: 01691291  
"OU = "BERLIN O=GERMANY  
OID.1.2.840.113549.1.9.2 = 7204-1.cisco.com  
OID.2.5.4.5 = 1691291  
:CRL Distribution Point  
<http://tac-2hq8cg5ti0h/CertEnroll/vpn.crl>  
:Validity Date  
start date: 17:19:21 PST Oct 28 2002  
end date: 17:29:21 PST Oct 29 2002  
renew date: 17:29:19 PST Oct 29 2002  
Associated Trustpoints: caserver2

Certificate  
Status: Available  
Certificate Serial Number: 09F8A45E00000000003D  
Certificate Usage: Signature  
:Issuer  
CN = vpn  
OU = cisco  
O = tac  
L = san jose  
ST = california  
C = US  
:Subject  
Name: 7204-1.cisco.com  
Serial Number: 01691291  
"OU = "BERLIN O=GERMANY  
OID.1.2.840.113549.1.9.2 = 7204-1.cisco.com  
OID.2.5.4.5 = 1691291  
:CRL Distribution Point  
<http://tac-2hq8cg5ti0h/CertEnroll/vpn.crl>  
:Validity Date  
start date: 17:19:19 PST Oct 28 2002

```

end date: 17:29:19 PST Oct 29 2002
Associated Trustpoints: caserver2
CA Certificate
Status: Available
Certificate Serial Number: 3E34CD199392A0914621EA778B13F357
Certificate Usage: Signature
:Issuer
CN = vpn
OU = cisco
O = tac
L = san jose
ST = california
C = US
:Subject
CN = vpn
OU = cisco
O = tac
L = san jose
ST = california
C = US
:CRL Distribution Point
http://tac-2hq8cg5ti0h/CertEnroll/vpn.crl
:Validity Date
start date: 21:19:50 PST Dec 6 2001
end date: 21:29:42 PST Dec 6 2003
Associated Trustpoints: caserver2
7204-1#

```

## عند انتهاء صلاحية شهادة الهوية

لا تحتوي الشبكة الخاصة الظاهرية (VPN) طراز 2611 على مصدر وقت خارجي تم تكوينه ويتم استخدام ساعة النظام لتعقب الوقت. يتم إعلان خادم CA2 على الموجه، ويصادق خادم CA، ويسجل موجه VPN-2611 تلقائياً مع خادم CA لشهادات الهوية الخاصة به. تم تكوين خادم CA لإصدار شهادات هوية صالحة ليوم واحد فقط. بمجرد انتهاء صلاحية الشهادة، يتم تسجيل الموجه تلقائياً مع خادم CA ويتم عرض تسلسل الأحداث في هذا الإخراج.

```

2611-VPN#clock set 19:30:00 26 oct 2002
Sets the system clock. 2611-VPN# 2611-VPN(config)#crypto ca trustpoint caserver2 ---!
Declares the CA server communication parameters. 2611-VPN(ca-trustpoint)# enrollment retry ---!
period 5
2611-VPN(ca-trustpoint)# enrollment mode ra
/2611-VPN(ca-trustpoint)# enrollment url url http://171.69.89.111:80/certsrv/mscep
mscep.dll
2611-VPN(ca-trustpoint)# usage ike
2611-VPN(ca-trustpoint)# serial-number
2611-VPN(ca-trustpoint)# fqdn 2611-vpn.cisco.com
2611-VPN(ca-trustpoint)# ip-address Ethernet0/0
2611-VPN(ca-trustpoint)# password 7 12170A1917
2611-VPN(ca-trustpoint)# subject-name OU=ROME O=ITALY
2611-VPN(ca-trustpoint)# crl optional
2611-VPN(ca-trustpoint)# rsakeypair tacvpn
2611-VPN(ca-trustpoint)# auto-enroll regenerate
#(2611-VPN(ca-trustpoint
:Oct 26 19:30:53.772: CRYPTO_PKI:Insert Selfsigned Certificate
4E 30 81 F9 02 20 38 42 33 34 38 41 01 82 30
44
Hex data omitted
AF 16 7B C1 4E 61 99 24 86 55 30 0D 96 91
4D 47
62 70
= Oct 26 19:30:53.820: CRYPTO_PKI: InsertCertData: subject name

```

```
1F 06 09 2A 86 48 86 F7 0D 01 30 21 31 23 30
09
2D 76 70 6E 2E 63 69 31 31 36 32 12 16 02
63 73
6F 2E 63 6F 6D
= Oct 26 19:30:53.828: CRYPTO_PKI: InsertCertData: issuer name
1F 06 09 2A 86 48 86 F7 0D 01 30 21 31 23 30
09
2D 76 70 6E 2E 63 69 31 31 36 32 12 16 02
63 73
6F 2E 63 6F 6D
= Oct 26 19:30:53.832: CRYPTO_PKI: InsertCertData: serial number
32 34 34 38 39 38 39 44 41 38 34 33 42 38
34 44
46 36 46 34 42 39 39 43 33 32 39 30 46 45
39 30
2611-VPN(config)#crypto ca authenticate caserver2
Authenticates the CA server. Certificate has the following attributes: Fingerprint: ---!
A1E8B61A FD1A66D6 2DE35501 99C43D83 % Do you accept this certificate? [yes/no]: Oct 26
19:31:10.936: CRYPTO_PKI: Sending CA Certificate Request: GET
/certsrv/mscep/mscep.dll/pkiclient.exe?operation=GetCACert&message;=caserver2 HTTP/1.0 Oct 26
19:31:10.940: CRYPTO_PKI: can not resolve server name/IP address Oct 26 19:31:10.940:
CRYPTO_PKI: Using unresolved IP Address 171.69.89.111 Oct 26 19:31:10.944: CRYPTO_PKI: http
connection opened Oct 26 19:31:11.401: CRYPTO_PKI: HTTP response header: HTTP/1.1 200 OK Server:
Microsoft-IIS/5.0 Date: Sun, 27 Oct 2002 02:30:22 GMT Content-Length: 2811 Content-Type:
application/x-x509-ca-ra-cert Content-Type indicates we have received CA
.and RA certificates
(Oct 26 19:31:11.405: CRYPTO_PKI:crypto_process_ca_ra_cert(trustpoint=caserver2
:(Oct 26 19:31:11.405: CRYPTO_PKI:CA and RA certs (cert data
0A F7 06 09 2A 86 48 86 F7 0D 01 07 02 82 30
A0
hex data omitted
0A 13 05 63 69 73 63 6F 31 0C 30 0A 04 55
06y
.Trustpoint CA certificate accepted
2611-VPN(config)# 03
0B 13 03 74 61 63 31 14 30 12 06 03 04 55
04 55
hex data omitted
A9 13 93 1E E6 E1 E4 30 07 31 00
= Oct 26 19:31:11.801: CRYPTO_PKI: InsertCertData: subject name
0B 30 09 06 03 55 04 06 13 02 55 53 31 61 30
31
hex data omitted
6E 70 76
= Oct 26 19:31:11.813: CRYPTO_PKI: InsertCertData: issuer name
0B 30 09 06 03 55 04 06 13 02 55 53 31 61 30
31
hex data omitted
6E 70 76
= Oct 26 19:31:11.825: CRYPTO_PKI: InsertCertData: serial number
3E 34 CD 19 93 92 A0 91 46 21 EA 77 8B 13 F3 57
= Oct 26 19:31:11.865: CRYPTO_PKI: InsertCertData: subject name
1E 06 09 2A 86 48 86 F7 0D 30 20 31 83 81 30
01
hex data omitted
6B 69 2D 72 61 70
= Oct 26 19:31:11.885: CRYPTO_PKI: InsertCertData: issuer name
0B 30 09 06 03 55 04 06 13 02 55 53 31 61 30
31
hex data omitted
6E 70 76
= Oct 26 19:31:11.897: CRYPTO_PKI: InsertCertData: serial number
6C F2 85 00 00 00 00 09 14
```

```
Oct 26 19:31:11.901: CRYPTO_PKI: WARNING: Certificate, private key or
                                CRL was not found while selecting CRL
= Oct 26 19:31:11.941: CRYPTO_PKI: InsertCertData: subject name
                                1E 06 09 2A 86 48 86 F7 0D 30 20 31 83 81 30
                                                                01
                                                                hex data omitted
                                                                6B 69 2D 72 61 70
= Oct 26 19:31:11.957: CRYPTO_PKI: InsertCertData: issuer name
                                0B 30 09 06 03 55 04 06 13 02 55 53 31 61 30
                                                                31
                                                                hex data omitted
                                                                6E 70 76
= Oct 26 19:31:11.969: CRYPTO_PKI: InsertCertData: serial number
                                6C F1 A9 00 00 00 00 08 14
Oct 26 19:31:11.977: CRYPTO_PKI: WARNING: Certificate, private key or
                                CRL was not found while selecting CRL
= Oct 26 19:31:11.981: CRYPTO_PKI: InsertCertData: subject name
                                0B 30 09 06 03 55 04 06 13 02 55 53 31 61 30
                                                                31
                                                                hex data omitted
                                                                6E 70 76
= Oct 26 19:31:11.998: CRYPTO_PKI: InsertCertData: issuer name
                                0B 30 09 06 03 55 04 06 13 02 55 53 31 61 30
                                                                31
                                                                hex data omitted
                                                                6E 70 76
= Oct 26 19:31:12.010: CRYPTO_PKI: InsertCertData: serial number
                                3E 34 CD 19 93 92 A0 91 46 21 EA 77 8B 13 F3 57
Oct 26 19:31:12.014: CRYPTO_PKI: transaction GetCACert completed
Oct 26 19:31:12.014: CRYPTO_PKI: CA certificate
                                .received
.Oct 26 19:31:12.014: CRYPTO_PKI: CA certificate received
( )Oct 26 19:31:12.030: CRYPTO_PKI: crypto_pki_authenticate_tp_cert
                                Oct 26 19:31:12.030: CRYPTO_PKI: trustpoint caserver2
                                authentication status = 2
= Oct 26 19:31:13.837: CRYPTO_PKI: InsertCertData: subject name
                                0B 30 09 06 03 55 04 06 13 02 55 53 31 61 30
                                                                31
                                                                hex data omitted
                                                                6E 70 76
= Oct 26 19:31:13.849: CRYPTO_PKI: InsertCertData: issuer name
                                0B 30 09 06 03 55 04 06 13 02 55 53 31 61 30
                                                                31
                                                                hex data omitted
                                                                6E 70 76
= Oct 26 19:31:13.861: CRYPTO_PKI: InsertCertData: serial number
                                3E 34 CD 19 93 92 A0 91 46 21 EA 77 8B 13 F3 57
Time to Re-enroll trust_point caserver2 %
%(Can not select my full public key (tacvpn
.. Start certificate enrollment
The subject name in the certificate will %
be: OU=ROME O=ITALY
The fully-qualified domain name in the certificate %
will be: 2611-vpn.cisco.com
The subject name in the certificate will %
be: 2611-vpn.cisco.com
The serial number in the certificate will %
be: 721959E3% Certificate request sent to Certificate Authority
The certificate request fingerprint will %
.be displayed
The 'show crypto ca certificate' command %
.will also show the fingerprint
:Signing Certificate Reqeust Fingerprint
00599B4B 62BAAE44 1706AF6E CD689B5D
```

:Oct 26 19:32:43.532: CRYPTO\_PKI: Sending CA Certificate Request  
GET /certsrv/mscep/mscep.dll/pkiclient.exe?operation=GetCACert&message;=caserver2  
HTTP/1.0

Oct 26 19:32:43.532: CRYPTO\_PKI: can not resolve server name/IP address  
Oct 26 19:32:43.532: CRYPTO\_PKI: Using unresolved IP Address 171.69.89.111

Oct 26 19:32:43.540: CRYPTO\_PKI: http connection opened

:Oct 26 19:32:44.032: CRYPTO\_PKI: HTTP response header  
HTTP/1.1 200 OK

Server: Microsoft-IIS/5.0

Date: Sun, 27 Oct 2002 02:31:55 GMT

Content-Length: 2811

Content-Type: application/x-x509-ca-ra-cert

.Content-Type indicates we have received CA and RA certificates  
(Oct 26 19:32:44.032: CRYPTO\_PKI:crypto\_process\_ca\_ra\_cert(trustpoint=caserver2

:(Oct 26 19:32:44.032: CRYPTO\_PKI:CA and RA certs (cert data

0A F7 06 09 2A 86 48 86 F7 0D 01 07 02 82 30  
A0

hex data omitted

6C 69 66 6F 72 6E 69 61 31 11 3 61

:Encryption Certificate Request Fingerprint

798894EE 357D6023 FD4F6C4E 75BF9611

hex data omitted

A9 13 93 1E E6 E1 E4 30 07 31 00

= Oct 26 19:32:44.489: CRYPTO\_PKI: InsertCertData: subject name

0B 30 09 06 03 55 04 06 13 02 55 53 31 61 30

31

hex data omitted

6E 70 76

= Oct 26 19:32:44.505: CRYPTO\_PKI: InsertCertData: issuer name

0B 30 09 06 03 55 04 06 13 02 55 53 31 61 30

31

hexdata omitted

6E 70 76

= Oct 26 19:32:44.517: CRYPTO\_PKI: InsertCertData: serial number

3E 34 CD 19 93 92 A0 91 46 21 EA 77 8B 13 F3 57

= Oct 26 19:32:44.557: CRYPTO\_PKI: InsertCertData: subject name

1E 06 09 2A 86 48 86 F7 0D 30 20 31 83 81 30

01

hex data omitted

6B 69 2D 72 61 70

= Oct 26 19:32:44.573: CRYPTO\_PKI: InsertCertData: issuer name

0B 30 09 06 03 55 04 06 13 02 55 53 31 61 30

31

hex data omitted

6E 70 76

= Oct 26 19:32:44.589: CRYPTO\_PKI: InsertCertData: serial number

6C F2 85 00 00 00 00 09 14

Oct 26 19:32:44.593: CRYPTO\_PKI: WARNING: Certificate, private key or

CRL was not found while selecting CRL

= Oct 26 19:32:44.641: CRYPTO\_PKI: InsertCertData: subject name

1E 06 09 2A 86 48 86 F7 0D 30 20 31 83 81 30

01

hex data omitted

6B 69 2D 72 61 70

= Oct 26 19:32:44.657: CRYPTO\_PKI: InsertCertData: issuer name

0B 30 09 06 03 55 04 06 13 02 55 53 31 61 30

31

hex data omitted

6E 70 76

= Oct 26 19:32:44.669: CRYPTO\_PKI: InsertCertData: serial number

```

        6C F1 A9 00 00 00 00 08 14
Oct 26 19:32:44.677: CRYPTO_PKI: WARNING: Certificate, private key or
        CRL was not found while selecting CRL
    = Oct 26 19:32:44.681: CRYPTO_PKI: InsertCertData: subject name
        1E 06 09 2A 86 48 86 F7 0D 30 20 31 83 81 30
        01
        hex data omitted
        6B 69 2D 72 61 70
    = Oct 26 19:32:44.697: CRYPTO_PKI: InsertCertData: issuer name
        0B 30 09 06 03 55 04 06 13 02 55 53 31 61 30
        31
        hex data omitted
        6F 31 0C 30 0A 06 03 55 04 03 13 63 73 69 63
        03
        6E 70 76
    = Oct 26 19:32:44.710: CRYPTO_PKI: InsertCertData: serial number
        6C F1 A9 00 00 00 00 08 14
    = Oct 26 19:32:44.718: CRYPTO_PKI: InsertCertData: subject name
        1E 06 09 2A 86 48 86 F7 0D 30 20 31 83 81 30
        01
        hex data omitted
        6B 69 2D 72 61 70
    = Oct 26 19:32:44.730: CRYPTO_PKI: InsertCertData: issuer name
        0B 30 09 06 03 55 04 06 13 02 55 53 31 61 30
        31
        hex data omitted
        6E 70 76
    = Oct 26 19:32:44.742: CRYPTO_PKI: InsertCertData: serial number
        6C F2 85 00 00 00 00 09 14
    = Oct 26 19:32:44.750: CRYPTO_PKI: InsertCertData: subject name
        0B 30 09 06 03 55 04 06 13 02 55 53 31 61 30
        31
        hex data omitted
        6E 70 76
    = Oct 26 19:32:44.762: CRYPTO_PKI: InsertCertData: issuer name
        0B 30 09 06 03 55 04 06 13 02 55 53 31 61 30
        31
        hex data omitted
        6E 70 76
    = Oct 26 19:32:44.774: CRYPTO_PKI: InsertCertData: serial number
        3E 34 CD 19 93 92 A0 91 46 21 EA 77 8B 13 F3 57
(Oct 26 19:32:44.778: CRYPTO_PKI: crypto_process_ra_certs(trust_point=caserver2
    Oct 26 19:32:44.782: CRYPTO_PKI: transaction PKCSReq completed
        :Oct 26 19:32:44.782: CRYPTO_PKI: status
    Oct 26 19:32:44.974: CRYPTO_PKI:Write out pkcs#10 content:347
        31 67 30 00 01 02 01 01 82 30 57 01 82 30
        30 15
        hex data omitted
        E0 7C A2 40 42 6B 87 AA 59 25 01
...Oct 26 19:32:45.102: CRYPTO_PKI:Enveloped Data for trustpoint caserver2
        2A 86 48 86 F7 0D 01 07 03 A0 80 09 06 80 30
        30
        hex data omitted
        00 00 00 00
    Oct 26 19:32:45.383: CRYPTO_PKI:Signed Data for trustpoint caserver2
        (bytes 1448)
        2A 86 48 86 F7 0D 01 07 02 A0 09 06 80 30
        30 80
        hex data omitted
        00 00 00 00 00 00 00 00
    Oct 26 19:32:45.571: CRYPTO_PKI: can not resolve server name/IP address
    Oct 26 19:32:45.571: CRYPTO_PKI: Using unresolved IP Address 171.69.89.111
    Oct 26 19:32:45.579: CRYPTO_PKI: http connection opened
    Oct 26 19:32:47.779: CRYPTO_PKI:Write out pkcs#10 content:347
```

```
31 67 30 00 01 02 01 01 82 30 57 01 82 30
30 15
hex data omitted
C0 71 E0 1C B9 47 E7 DB 0E 8A 61
...Oct 26 19:32:47.907: CRYPTO_PKI:Enveloped Data for trustpoint caserver2
2A 86 48 86 F7 0D 01 07 03 A0 80 09 06 80 30
30
hex data omitted
00 00 00 00
Oct 26 19:32:48.191: CRYPTO_PKI:Signed Data for trustpoint caserver2
(bytes 1448)
2A 86 48 86 F7 0D 01 07 02 A0 09 06 80 30
30 80
hex data omitted
00 00 00 00 00 00 00 00
Oct 26 19:32:48.380: CRYPTO_PKI: can not resolve server name/IP address
Oct 26 19:32:48.380: CRYPTO_PKI: Using unresolved IP Address 171.69.89.111
Oct 26 19:32:48.452: CRYPTO_PKI: http connection opened
Oct 26 19:32:50.483: CRYPTO_PKI: received msg of 1972 bytes
:Oct 26 19:32:50.483: CRYPTO_PKI: HTTP response header
HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Sun, 27 Oct 2002 02:31:59 GMT
Content-Length: 1826
Content-Type: application/x-pki-message

Oct 26 19:32:50.487: CRYPTO_PKI:Received pki message (PKCS7) for trustpoint
caserver2: 1826 bytes
1E 06 09 2A 86 48 86 F7 0D 01 07 02 07 82 30
A0
hex data omitted

FE 23 71 08 04 82 80
:Oct 26 19:32:51.465: %CRYPTO-6-CERTRET
Certificate received from Certificate Authority
Oct 26 19:33:11.469: CRYPTO_PKI: received msg of 1972 bytes
:Oct 26 19:33:11.469: CRYPTO_PKI: HTTP response header
HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Sun, 27 Oct 2002 02:32:02 GMT
Content-Length: 1826
Content-Type: application/x-pki-message

Oct 26 19:33:11.473: CRYPTO_PKI:Received pki message (PKCS7) for trustpoint
caserver2: 1826 bytes
1E 06 09 2A 86 48 86 F7 0D 01 07 02 07 82 30
A0
hex data omitted
25 54
= Oct 26 19:33:11.734: CRYPTO_PKI: InsertCertData: subject name
1E 06 09 2A 86 48 86 F7 0D 30 20 31 83 81 30
01
hex data omitted

6B 69 2D 72 61 70
= Oct 26 19:33:11.750: CRYPTO_PKI: InsertCertData: issuer name
0B 30 09 06 03 55 04 06 13 02 55 53 31 61 30
31
hex data omitted

6E 70 76
= Oct 26 19:33:11.762: CRYPTO_PKI: InsertCertData: serial number
```



```

6C F1 A9 00 00 00 00 08 14
Oct 26 19:33:11.770: CRYPTO_PKI: WARNING: Certificate, private key or
CRL was not found while selecting CRL
:Oct 26 19:33:11.842: CRYPTO_PKI: signed attr: pki-message-type
33 01 13
:Oct 26 19:33:11.842: CRYPTO_PKI: signed attr: pki-status
30 01 13
:Oct 26 19:33:11.846: CRYPTO_PKI: signed attr: pki-recipient-nonce
E0 59 89 15 0A E0 C5 2D 2B 44 82 72 10 04
7B E7
4D EF
:Oct 26 19:33:11.850: CRYPTO_PKI: signed attr: pki-transaction-id
32 41 41 33 32 41 37 39 37 32 45 41 20 13
45 44
34 30 37 36 45 35 39 34 38 45 37 38 32 30
38 33
30 34
Oct 26 19:33:11.854: CRYPTO_PKI: status = 100: certificate is granted
Oct 26 19:33:11.854: CRYPTO_PKI:Verified signed data for trustpoint
:(caserver2 (1259 bytes
E7 06 09 2A 86 48 86 F7 0D 01 07 04 82 30
A0 03
hex data omitted
1B D5 43 D5 E3 88 F6 F5 D5 09 45
:Oct 26 19:33:12.191: CRYPTO_PKI:Decrypted enveloped content
FE 06 09 2A 86 48 86 F7 0D 01 07 03 82 30
A0 02
hex data omitted
DD C1 E0 03 85 EC B3 E9 B0 63 3D FF F2 54
C9 7F

= Oct 26 19:33:12.355: CRYPTO_PKI: InsertCertData: subject name
6B 31 11 30 0F 06 03 55 04 05 13 08 37 32 30
31
hex data omitted
0C 52 4F 4D 45 20 4F 3D 49 54 41 4C 59
= Oct 26 19:33:12.371: CRYPTO_PKI: InsertCertData: issuer name
0B 30 09 06 03 55 04 06 13 31 61 30
31 53 55 02
hex data omitted
6E 70 76
= Oct 26 19:33:12.383: CRYPTO_PKI: InsertCertData: serial number
1C 41 E0 00 00 00 00 00 37 61
Oct 26 19:33:12.391: CRYPTO_PKI: WARNING: Certificate, private key or
CRL was not found while selecting CRL
= Oct 26 19:33:12.407: CRYPTO_PKI: InsertCertData: subject name
6B 31 11 30 0F 06 03 55 04 05 13 08 37 32 30
31
1C 30 1A 06 09 31 33 45 39 35 39
Oct 26 19:33:12.459: CRYPTO_PKI: WARNING: Certificate, private key
or CRL was not found while selecting CRL
Oct 26 19:33:22.503: CRYPTO_PKI: All enrollment
.requests completed for trustpoint caserver2

```

```

2611-VPN#show crypto ca certificate
Certificate
Status: Available
Certificate Serial Number: 611C41E00000000000037
Certificate Usage: Encryption
:Issuer
CN = vpn
OU = cisco
O = tac
L = san jose

```

ST = california

C = US

:Subject

**Name: 2611-vpn.cisco.com**

*The subject name, IP address, and serial !--- numbers of the certificate issued by CA ---!*

**server2. IP Address: 172.16.172.35**

**Serial Number: 721959E3**

**"OU = "ROME O=ITALY**

**OID.1.2.840.113549.1.9.2**

**2611-vpn.cisco.com =**

**OID.1.2.840.113549.1.9.8**

**172.16.172.35 =**

**OID.2.5.4.5 = 721959E3**

**:CRL Distribution Point**

**http://tac-2hq8cg5ti0h/CertEnroll/vpn.crl**

**:Validity Date**

**start date: 02:22:02 UTC**

**Oct 27 2002**

**end date: 02:32:02**

**UTC Oct 28 2002**

*CA server2 issued a certificate with a !--- validity period of one day. !--- The renew date ---!*

*indicates the time for reenrollment !--- with the CA server. renew date: 02:31:59 UTC*

**Oct 28 2002**

**Associated Trustpoints: caserver2**

Certificate

Status: Available

Certificate Serial Number: 611C3624000000000036

Certificate Usage: Signature

:Issuer

CN = vpn

OU = cisco

O = tac

L = san jose

ST = california

C = US

:Subject

**Name: 2611-vpn.cisco.com**

**IP Address: 172.16.172.35**

**Serial Number: 721959E3**

**"OU = "ROME O=ITALY**

**OID.1.2.840.113549.1.9.2 = 2611-vpn.cisco.com**

**OID.1.2.840.113549.1.9.8 = 172.16.172.35**

**OID.2.5.4.5 = 721959E3**

**:CRL Distribution Point**

**http://tac-2hq8cg5ti0h/CertEnroll/vpn.crl**

**:Validity Date**

**start date: 02:21:59 UTC Oct 27 2002**

**end date: 02:31:59 UTC Oct 28 2002**

**Associated Trustpoints: caserver2**

CA Certificate

Status: Available

Certificate Serial Number: 3E34CD199392A0914621EA778B13F357

Certificate Usage: Signature

:Issuer

CN = vpn

OU = cisco

O = tac

L = san jose

ST = california

C = US

:Subject

CN = vpn

OU = cisco

O = tac  
L = san jose  
ST = california  
C = US  
:CRL Distribution Point  
http://tac-2hq8cg5ti0h/CertEnroll/vpn.crl  
:Validity Date  
start date: 04:19:50 UTC Dec 7 2001  
end date: 04:29:42 UTC Dec 7 2003  
Associated Trustpoints: caserver2  
CA Certificate  
Status: Available  
Certificate Serial Number: 0E7EC1B68A2F14BD4C4515AF44C45732  
Certificate Usage: Signature  
:Issuer  
CN = SJVPNTAC-CAServer  
OU = TAC-VPN-SJ  
O = Cisco Systems  
L = San Jose  
ST = CA  
C = US  
:Subject  
CN = SJVPNTAC-CAServer  
OU = TAC-VPN-SJ  
O = Cisco Systems  
L = San Jose  
ST = CA  
C = US  
:CRL Distribution Point  
http://ca-server/CertEnroll/SJVPNTAC-CAServer.crl  
:Validity Date  
start date: 20:52:48 UTC Sep 17 2002  
end date: 21:02:37 UTC Sep 17 2017  
**Associated Trustpoints: caserver1**  
Certificate  
Status: Available  
Certificate Serial Number: 6103EE0A0000000000038  
Certificate Usage: Signature  
:Issuer  
CN = SJVPNTAC-CAServer  
OU = TAC-VPN-SJ  
O = Cisco Systems  
L = San Jose  
ST = CA  
C = US  
:Subject  
**Name: 2611-vpn.cisco.com**  
**IP Address: 172.16.172.35**  
**Serial Number: 721959E3**  
**"OU = "PARIS O=FRANCE**  
OID.1.2.840.113549.1.9.2 = 2611-vpn.cisco.com  
OID.1.2.840.113549.1.9.8 = 172.16.172.35  
OID.2.5.4.5 = 721959E3  
:CRL Distribution Point  
http://ca-server/CertEnroll/SJVPNTAC-CAServer.crl  
:Validity Date  
start date: 03:33:05 UTC Oct 26 2002  
end date: 03:43:05 UTC Oct 26 2003  
**Associated Trustpoints: caserver1**  
Certificate  
Status: Available  
Certificate Serial Number: 6104020F0000000000039  
Certificate Usage: Encryption  
:Issuer

CN = SJVPNTAC-CAServer  
OU = TAC-VPN-SJ  
O = Cisco Systems  
L = San Jose  
ST = CA  
C = US  
:Subject  
Name: 2611-vpn.cisco.com  
IP Address: 172.16.172.35  
Serial Number: 721959E3  
"OU = "PARIS O=FRANCE  
OID.1.2.840.113549.1.9.2 = 2611-vpn.cisco.com  
OID.1.2.840.113549.1.9.8 = 172.16.172.35  
OID.2.5.4.5 = 721959E3  
:CRL Distribution Point  
http://ca-server/CertEnroll/SJVPNTAC-CAServer.crl  
**:Validity Date**  
**start date: 03:33:10 UTC**  
**Oct 26 2002**  
**end date: 03:43:10**  
**UTC Oct 26 2003**  
**renew date: 03:43:05 UTC**  
**Oct 26 2003**  
**Associated Trustpoints: caserver1**

2611-VPN#show crypto key mypubkey rsa  
Key pair was generated at: 00:14:06 UTC %  
Mar 1 1993

Key name: ciscovpn  
Usage: Signature Key

:Key Data

305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00A2DE57  
2C7A4555  
BF87D3CC 4A260DBF 56574554 472FC72C 0461A35B E41B5B53 BE81A47E  
264A68D7  
27E4E301 2AF04B1C E472F70B 74DF38A0 6EB286F9 01020301 08662555  
0001

Key pair was generated at: 00:14:10 UTC Mar 1 1993 %

Key name: ciscovpn

Usage: Encryption Key

:Key Data

305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00D10224  
8CBEC2D7  
B517DF99 7363717D 6F6CA0F1 83FB7874 E60BB169 CD4AD9CA 92E04143  
16D4D253  
5CBF212F FF6268A5 329AB988 2655568C 8EC19017 6F4A4C86 43020301  
0001

Key pair was generated at: 00:14:59 UTC Mar 1 1993 %

*The RSA key pair is generated during !--- the next auto reenroll . Key name: tacvpn ---!  
This key pair was generated before the system !--- clock was set, hence the 1993 date. ---!*

Usage: Signature Key

:Key Data

305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00AB2884  
22A070D0  
A8C84C3E CD45A382 F4CDB158 5B31B624 5C92632C 5DC1977E 686E1C18  
DA16BE57  
6FBA9518 4D2F01B8 0D59528D 447014D3 02D5A631 84E54CD4 FB020301  
0001

Key pair was generated at: 00:15:00 UTC Mar 1 1993 %

Key name: tacvpn

Usage: Encryption Key

:Key Data

305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00AB7576

```
9D0A2D65
7BB9B465 AF227B73 2B83AFD6 3791FA54 3A2DB845 55E4540F 35972460
B87C613E
82DBC4D2 51E6F9A7 07164C57 B02D28B8 93F8D50F D5C3444F 01020301
0001
Key pair was generated at: 22:02:57 UTC Oct 27 2002 %
Key name: ciscovpn.server
Usage: Encryption Key
:Key Data
307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00D42A5E
4C9D27F1
195CC537 7CF9E390 935DFBA3 2DA01B3B C5E50620 57B902A3 50876FA1
1A9D83FD
0EB437F7 E0568EB7 830A46FA E9D9BA4F 3E8B132D F24A08B8 E2154944
36829D64
E48077EF 224BF142 A3A92672 F0BC57F5 063EF64A 8B775979 CD020301
0001
#2611-VPN
#2611-VPN
2611-VPN# show clock
UTC Sun Oct 27 2002 19:29:20.304
#2611-VPN
#2611-VPN
#2611-VPN
```

*The certificate from CA server2 expired and the router is !--- reenrolling automatically ---!  
without user intervention.* 2611-VPN# Time to Re-enroll trust\_point caserver2 Can not select my

```
.. full public key (tacvpn)% Start certificate enrollment
The subject name in the certificate will %
be: OU=ROME O=ITALY
```

```
The fully-qualified domain name in the certificate %
will be: 2611-vpn.cisco.com
```

```
The subject name in the certificate will %
be: 2611-vpn.cisco.com
```

```
The serial number in the certificate will %
be: 721959E3% Certificate request sent to Certificate Authority
```

```
The certificate request fingerprint will %
.be displayed
```

```
The 'show crypto ca certificate' command %
.will also show the fingerprint
```

```
Oct 28 02:32:01.210: %CRYPTO-6-AUTOGEN: Generated new 512 bit key pair
Oct 28 02:32:02.924: %CRYPTO-6-AUTOGEN: Generated new 512 bit key pair
:Oct 28 02:32:02.944: CRYPTO_PKI: Sending CA Certificate Request
GET /certsrv/mscep/mscep.dll/pkiclient.exe?operation=GetCACert&message;=caserver2
HTTP/1.0
```

```
Oct 28 02:32:02.944: CRYPTO_PKI: can not resolve server name/IP address
Oct 28 02:32:02.944: CRYPTO_PKI: Using unresolved IP Address 171.69.89.111
:Signing Certificate Reqeust Fingerprint
99E260CF 476B54E1 B6486AF3 98FD0F02
```

```
Oct 28 02:32:02.952: CRYPTO_PKI: http connection opened
:Oct 28 02:32:03.461: CRYPTO_PKI: HTTP response header
HTTP/1.1 200 OK
```

```
Server: Microsoft-IIS/5.0
Date: Mon, 28 Oct 2002 09:31:15 GMT
Content-Length: 2811
```

```
Content-Type: application/x-x509-ca-ra-cert
```

```
.Content-Type indicates we have received CA and RA certificates
(Oct 28 02:32:03.461: CRYPTO_PKI:crypto_process_ca_ra_cert(trustpoint=caserver2
```

```
:(Oct 28 02:32:03.461: CRYPTO_PKI:CA and RA certs (cert data
0A F7 06 09 2A 86 48 86 F7 0D 01 07 02 82 30
```

```
A0
```

```
hex data omitted
```

```
9D B4 04 E9 46 13 45 37 10 59 AE B1 F7 39 00
```

```
C1
D3 F2 DB 0C 95 5A F7 C9 F 73
:Encryption Certificate Request Fingerprint
BE1C5800 A6F895FF AC8DBAF9 0DED9356
A9 13 93 1E E6 E1 E4 30 07 31
00
hex data omitted
= Oct 28 02:32:03.922: CRYPTO_PKI: InsertCertData: subject name
0B 30 09 06 03 55 04 06 13 02 55 53 31 61 30
31
hex data omitted
6E 70 76
= Oct 28 02:32:03.934: CRYPTO_PKI: InsertCertData: issuer name
0B 30 09 06 03 55 04 06 13 02 55 53 31 61 30
31
0A 63 61 6C 69 13 08 04 55 03 06 11 30 13
6F 66
6E 69 61 31 11 30 0F 06 03 55 04 07 13 72
73 08
6E 20 6A 6F 73 65 31 0C 30 0A 06 03 55 61
0A 04
0E 30 0C 06 03 55 04 0B 31 63 61 74 03 13
05 13
6F 31 0C 30 0A 06 03 55 04 03 63 73 69 63
03 13
6E 70 76
= Oct 28 02:32:03.946: CRYPTO_PKI: InsertCertData: serial number
3E 34 CD 19 93 92 A0 91 46 21 EA 77 8B 13 F3 57
= Oct 28 02:32:03.990: CRYPTO_PKI: InsertCertData: subject name
1E 06 09 2A 86 48 86 F7 0D 30 20 31 83 81 30
01
hex data omitted
6B 69 2D 72 61 70
= Oct 28 02:32:04.006: CRYPTO_PKI: InsertCertData: issuer name
0B 30 09 06 03 55 04 06 13 02 55 53 31 61 30
31
hex data omitted
6E 70 76
= Oct 28 02:32:04.018: CRYPTO_PKI: InsertCertData: serial number
6C F2 85 00 00 00 00 09 14
Oct 28 02:32:04.026: CRYPTO_PKI: WARNING: Certificate, private key or
CRL was not found while selecting CRL
= Oct 28 02:32:04.066: CRYPTO_PKI: InsertCertData: subject name
1E 06 09 2A 86 48 86 F7 0D 30 20 31 83 81 30
01
hex data omitted
6B 69 2D 72 61 70
= Oct 28 02:32:04.082: CRYPTO_PKI: InsertCertData: issuer name
0B 30 09 06 03 55 04 06 13 02 55 53 31 61 30
31
0A 63 61 6C 69 13 08 04 55 03 06 11 30 13
6F 66
6E 69 61 31 11 30 0F 06 03 55 04 07 13 72
73 08
6E 20 6A 6F 73 65 31 0C 30 0A 06 03 55 61
0A 04
0E 30 0C 06 03 55 04 0B 31 63 61 74 03 13
05 13
6F 31 0C 30 0A 06 03 55 04 03 63 73 69 63
03 13
6E 70 76
= Oct 28 02:32:04.094: CRYPTO_PKI: InsertCertData: serial number
6C F1 A9 00 00 00 00 08 14
```



```
...Oct 28 02:32:04.527: CRYPTO_PKI:Enveloped Data for trustpoint caserver2
      2A 86 48 86 F7 0D 01 07 03 A0 80 09 06 80 30
      30
      hex data omitted
      B2 72 10 92 09 AF 00 00 00 00 00 29 69 08 04
      00
      00 00 00 00
Oct 28 02:32:04.807: CRYPTO_PKI:Signed Data for trustpoint caserver2
      (bytes 2129)
      2A 86 48 86 F7 0D 01 07 02 A0 09 06 80 30
      30 80
      hex data omitted
      F0 20 30 3F 15 41 BD A6 F5 00 00 00 00 00
      00
      00
Oct 28 02:32:05.080: CRYPTO_PKI: can not resolve server name/IP address
Oct 28 02:32:05.084: CRYPTO_PKI: Using unresolved IP Address 171.69.89.111
Oct 28 02:32:05.088: CRYPTO_PKI: http connection opened
Oct 28 02:32:07.292: CRYPTO_PKI:Write out pkcs#10 content:347
      31 67 30 00 01 02 01 01 82 30 57 01 82 30
      30 15
      0B 13 0C 52 4F 4D 45 20 4F 04 55 03 06 13
      3D 49
      hex data omitted
      A5 FF 13 4A CF B0 2B 0C A8 7D BF
...Oct 28 02:32:07.416: CRYPTO_PKI:Enveloped Data for trustpoint caserver2
      2A 86 48 86 F7 0D 01 07 03 A0 80 09 06 80 30
      30
      hex data omitted
      00 00 00 00
Oct 28 02:32:07.716: CRYPTO_PKI:Signed Data for trustpoint caserver2
      (bytes 2129)
      2A 86 48 86 F7 0D 01 07 02 A0 09 06 80 30
      30 80
      hex data omitted
      0A F2 8F 78 FB 4E 6B C2 CB 00 00 00 00 00
      00
      00
Oct 28 02:32:07.989: CRYPTO_PKI: can not resolve server name/IP address
Oct 28 02:32:07.989: CRYPTO_PKI: Using unresolved IP Address 171.69.89.111
Oct 28 02:32:08.049: CRYPTO_PKI: http connection opened
Oct 28 02:32:10.064: CRYPTO_PKI: received msg of 2012 bytes
      :Oct 28 02:32:10.064: CRYPTO_PKI: HTTP response header
      HTTP/1.1 200 OK
      Server: Microsoft-IIS/5.0
      Date: Mon, 28 Oct 2002 09:31:20 GMT
      Content-Length: 1866
      Content-Type: application/x-pki-message

Oct 28 02:32:10.064: CRYPTO_PKI:Received pki message (PKCS7) for trustpoint
      caserver2: 1866 bytes
      2A 86 48 86 F7 0D 01 07 02 09 06 46 07 82 30
      A0
      hex data omitted
      6D DB 94 FF 71 DD A0 E6 1B E9 31 66 76 D2 5C
      FC
      :Oct 28 02:32:11.070: %CRYPTO-6-CERTRET
Certificate received from Certificate Authority
Oct 28 02:32:31.075: CRYPTO_PKI: received msg of 2012 bytes
      :Oct 28 02:32:31.075: CRYPTO_PKI: HTTP response header
      HTTP/1.1 200 OK
      Server: Microsoft-IIS/5.0
      Date: Mon, 28 Oct 2002 09:31:23 GMT
```



Content-Length: 1866  
Content-Type: application/x-pki-message

```
Oct 28 02:32:31.079: CRYPTO_PKI:Received pki message (PKCS7) for trustpoint
                                caserver2: 1866 bytes
                                2A 86 48 86 F7 0D 01 07 02 09 06 46 07 82 30
                                                                A0
                                hex data omitted
                                4B D4 80 86 DC 91 FF F2 C8 30 CF 20 42 07 95
                                                                BE
                                BA F2 B1 6A 9A 24 FC 46 35 61
= Oct 28 02:32:31.343: CRYPTO_PKI: InsertCertData: subject name
                                1E 06 09 2A 86 48 86 F7 0D 30 20 31 83 81 30
                                                                01
                                hex data omitted
                                6B 69 2D 72 61 70
= Oct 28 02:32:31.359: CRYPTO_PKI: InsertCertData: issuer name
                                0B 30 09 06 03 55 04 06 13 02 55 53 31 61 30
                                                                31
                                hex data omitted
                                6E 70 76
= Oct 28 02:32:31.375: CRYPTO_PKI: InsertCertData: serial number
                                6C F1 A9 00 00 00 00 00 08 14
Oct 28 02:32:31.379: CRYPTO_PKI: WARNING: Certificate, private key or
                                CRL was not found while selecting CRL
:Oct 28 02:32:31.451: CRYPTO_PKI: signed attr: pki-message-type
                                33 01 13
:Oct 28 02:32:31.455: CRYPTO_PKI: signed attr: pki-status
                                30 01 13
:Oct 28 02:32:31.455: CRYPTO_PKI: signed attr: pki-recipient-nonce
                                0C CF 22 65 E3 50 72 E0 0C 59 42 A2 10 04
                                                                6F 54
                                                                1F 6B
:Oct 28 02:32:31.459: CRYPTO_PKI: signed attr: pki-transaction-id
                                39 33 42 37 35 36 32 38 31 36 39 34 20 13
                                                                34 33
                                32 36 33 42 31 42 33 43 44 33 34 38 45 44
                                                                46 41
                                                                33 34
:Oct 28 02:32:31.467: CRYPTO_PKI
                                status = 100: certificate is granted
Oct 28 02:32:31.467: CRYPTO_PKI:Verified signed data for trustpoint
                                :(caserver2 (1299 bytes)
                                0F 06 09 2A 86 48 86 F7 0D 01 07 05 82 30
                                                                A0 03
                                hex data omitted
                                0B 7E 8B 1F 53 17 7E 13 BC 62 9A 3E F5 13 44
                                                                D6
                                                                2C CE 8F
:Oct 28 02:32:31.800: CRYPTO_PKI:Decrypted enveloped content
                                FE 06 09 2A 86 48 86 F7 0D 01 07 03 82 30
                                                                A0 02
                                hex data omitted
                                EF 3D 6E 15 63 C3 3C F9 79 54 BA 6D 57 68 5B
                                                                43
                                                                00 31
= Oct 28 02:32:31.988: CRYPTO_PKI: InsertCertData: subject name
                                6B 31 11 30 0F 06 03 55 04 05 13 08 37 32 30
                                                                31
                                hex data omitted
                                0C 52 4F 4D 45 20 4F 3D 49 54 41 4C 59
= Oct 28 02:32:32.000: CRYPTO_PKI: InsertCertData: issuer name
```

0B 30 09 06 03 55 04 06 13 02 55 53 31 61 30  
31  
hex data omitted  
6F 31 0C 30 0A 06 03 55 04 03 13 63 73 69 63  
03  
6E 70 76

= Oct 28 02:32:32.016: CRYPTO\_PKI: InsertCertData: serial number 06  
:# Oct 28 02:32:32.116: CRYPTO\_PKI:removing superceded cert serial  
611C41E0000000000037  
:# Oct 28 02:32:32.120: CRYPTO\_PKI:removing superceded cert serial  
611C3624000000000036

**:Oct 28 02:32:42.121: CRYPTO\_PKI**

**.All enrollment requests completed for trustpoint caserver2**

**2611-VPN#show crypto key mypubkey rsa**

Key pair was generated at: 00:14:06 UTC Mar 1 1993 %

Key name: ciscovpn

Usage: Signature Key

:Key Data

305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00A2DE57  
2C7A4555

BF87D3CC 4A260DBF 56574554 472FC72C 0461A35B E41B5B53 BE81A47E  
264A68D7

27E4E301 2AF04B1C E472F70B 74DF38A0 6EB286F9 01020301 08662555  
0001

Key pair was generated at: 00:14:10 UTC Mar 1 1993 %

Key name: ciscovpn

Usage: Encryption Key

:Key Data

305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00D10224  
8CBEC2D7

B517DF99 7363717D 6F6CA0F1 83FB7874 E60BB169 CD4AD9CA 92E04143  
16D4D253

5CBF212F FF6268A5 329AB988 2655568C 8EC19017 6F4A4C86 43020301  
0001

Key pair was generated at: 02:32:01 UTC Oct 28 2002 %

**Key name: tacvpn**

**Usage: Signature Key**

:Key Data

305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00BFC0C4  
6217E11E

96447AE7 3579A8AC 0E3354BD 54080ABD 32A94C9D CAF0009A DD441CD4  
7962C6E8

82A6C63D DCBF454A 342B0815 3C7FF706 583316D3 ABF7E53D 51020301  
0001

*The RSA key pair was regenerated with the !--- reenroll of the identity certificate. % Key ---!*

**pair was generated at: 02:32:02**

**UTC Oct 28 2002**

**Key name: tacvpn**

**Usage: Encryption Key**

:Key Data

305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00E65D19  
513BCF3C

486F722E 9E9EB410 E26A8BA0 F492C824 AF276EB4 53F5D22C 5BE90B52  
91889E0E

C896DF08 E4D3A899 B8F6C8CE 9884B4EE 49C787D5 DFFC9907 29020301  
0001

Key pair was generated at: 11:33:57 UTC Oct 28 2002 %

Key name: ciscovpn.server

Usage: Encryption Key

:Key Data

307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00BBD14F  
A16AE1D8

98D25643 0A5BCA1B BE3809DA EED3672B A0CA07F3 E221A31C 3D64B59B

62A145B1  
82BE03D5 5D7FA248 064BA826 CFC35CAB 330CDCDD 8994F95D 450580DC  
2B003FE1  
EB834755 AC083989 4F058F63 2E00CD3A 720075F2 500D38DE C1020301  
0001

2611-VPN# **show crypto ca certificate**

Certificate

Status: Available

Certificate Serial Number: 06C28C8B00000000003B

Certificate Usage: Encryption

:Issuer

CN = vpn

OU = cisco

O = tac

L = san jose

ST = california

C = US

**:Subject**

**Name: 2611-vpn.cisco.com**

**IP Address: 172.16.172.35**

**Serial Number: 721959E3**

**"OU = "ROME O=ITALY**

OID.1.2.840.113549.1.9.2 = 2611-vpn.cisco.com

OID.1.2.840.113549.1.9.8 = 172.16.172.35

OID.2.5.4.5 = 721959E3

:CRL Distribution Point

<http://tac-2hq8cg5ti0h/CertEnroll/vpn.crl>

**:Validity Date**

**start date: 09:21:23**

**UTC Oct 28 2002**

*The CA server2 issued a new !--- identity certificate with a new renew date. end date: ---!*

**09:31:23**

**UTC Oct 29 2002**

**renew date: 09:31:20**

**UTC Oct 29 2002**

**Associated Trustpoints: caserver2**

Certificate

Status: Available

Certificate Serial Number: 06C2807F000000000003A

Certificate Usage: Signature

:Issuer

CN = vpn

OU = cisco

O = tac

L = san jose

ST = california

C = US

**:Subject**

**Name: 2611-vpn.cisco.com**

**IP Address: 172.16.172.35**

**Serial Number: 721959E3**

**"OU = "ROME O=ITALY**

**OID.1.2.840.113549.1.9.2**

**2611-vpn.cisco.com =**

**OID.1.2.840.113549.1.9.8**

**172.16.172.35 =**

**OID.2.5.4.5 = 721959E3**

:CRL Distribution Point/

<http://tac-2hq8cg5ti0h/CertEnroll/vpn.crl>

**:Validity Date**

**start date: 09:21:20 UTC Oct 28 2002**

**end date: 09:31:20 UTC Oct 29 2002**

**Associated Trustpoints: caserver2**

CA Certificate

Status: Available  
Certificate Serial Number: 3E34CD199392A0914621EA778B13F357  
Certificate Usage: Signature  
:Issuer  
CN = vpn  
OU = cisco  
O = tac  
L = san jose  
ST = california  
C = US  
:Subject  
CN = vpn  
OU = cisco  
O = tac  
L = san jose  
ST = california  
C = US  
:CRL Distribution Point  
http://tac-2hq8cg5ti0h/CertEnroll/vpn.crl  
:Validity Date  
start date: 04:19:50 UTC Dec 7 2001  
end date: 04:29:42 UTC Dec 7 2003

**Associated Trustpoints: caserver2**

CA Certificate  
Status: Available  
Certificate Serial Number: 0E7EC1B68A2F14BD4C4515AF44C45732  
Certificate Usage: Signature  
:Issuer  
CN = SJVPNTAC-CAServer  
OU = TAC-VPN-SJ  
O = Cisco Systems  
L = San Jose  
ST = CA  
C = US  
:Subject  
CN = SJVPNTAC-CAServer  
OU = TAC-VPN-SJ  
O = Cisco Systems  
L = San Jose  
ST = CA  
C = US  
:CRL Distribution Point  
http://ca-server/CertEnroll/SJVPNTAC-CAServer.crl  
:Validity Date  
start date: 20:52:48 UTC Sep 17 2002  
end date: 21:02:37 UTC Sep 17 2017

**Associated Trustpoints: caserver1**

Certificate  
Status: Available  
Certificate Serial Number: 6103EE0A0000000000038  
Certificate Usage: Signature  
:Issuer  
CN = SJVPNTAC-CAServer  
OU = TAC-VPN-SJ  
O = Cisco Systems  
L = San Jose  
ST = CA  
C = US  
:Subject

**Name: 2611-vpn.cisco.com**

**IP Address: 172.16.172.35**

**Serial Number: 721959E3**

**"OU = "PARIS O=FRANCE**

OID.1.2.840.113549.1.9.2 = 2611-vpn.cisco.com

```
OID.1.2.840.113549.1.9.8 = 172.16.172.35
OID.2.5.4.5 = 721959E3
:CRL Distribution Point
http://ca-server/CertEnroll/SJVPNTAC-CAServer.crl
:Validity Date
start date: 03:33:05 UTC Oct 26 2002
end date: 03:43:05 UTC Oct 26 2003
Associated Trustpoints: caserver1
Certificate
Status: Available
Certificate Serial Number: 6104020F000000000039
Certificate Usage: Encryption
:Issuer
CN = SJVPNTAC-CAServer
OU = TAC-VPN-SJ
O = Cisco Systems
L = San Jose
ST = CA
C = US
:Subject
Name: 2611-vpn.cisco.com
IP Address: 172.16.172.35
Serial Number: 721959E3
"OU = "PARIS O=FRANCE
OID.1.2.840.113549.1.9.2
2611-vpn.cisco.com =
OID.1.2.840.113549.1.9.8
172.16.172.35 =
OID.2.5.4.5 = 721959E3
:CRL Distribution Point
http://ca-server/CertEnroll/SJVPNTAC-CAServer.crl
:Validity Date
start date: 03:33:10 UTC Oct 26 2002
end date: 03:43:10 UTC Oct 26 2003
renew date: 03:43:05 UTC Oct 26 2003
Associated Trustpoints: caserver1
```

*Router with the new certificate !--- after automatic reenrollment. 2611-VPN#show run ---!*

```
...Building configuration
Current configuration : 15523 bytes
!
Last configuration change at 19:31:48 UTC Sat Oct 26 2002 !
NVRAM config last updated at 23:37:39 UTC Sun Oct 27 2002 !
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname 2611-VPN
!
!
memory-size iomem 10
ip subnet-zero
!
!
ip domain name cisco.com
ip host caserver2 171.69.89.111
ip host caserver1 171.69.89.125
!
!
crypto ca trustpoint caserver1
enrollment retry period 5
enrollment mode ra
enrollment url http://171.69.89.125:80/certsrv/mscep/mscep.dll
```

```

usage ike
serial-number
fqdn 2611-vpn.cisco.com
ip-address Ethernet0/0
password 7 011D090A5E
subject-name OU=PARIS O=FRANCE
crl optional
rsa-keypair ciscovpn
auto-enroll regenerate
!
crypto ca trustpoint caserver2
enrollment retry period 5
enrollment mode ra
enrollment url http://171.69.89.111:80/certsrv/mscep/mscep.dll
usage ike
serial-number
fqdn 2611-vpn.cisco.com
ip-address Ethernet0/0
password 7 151C040201
subject-name OU=ROME O=ITALY
crl optional
rsa-keypair tacvpn
auto-enroll regenerate
crypto ca certificate chain caserver1
certificate ca 0E7EC1B68A2F14BD4C4515AF44C45732
308202BE 30820268 A0030201 0202100E 7EC1B68A 2F14BD4C 4515AF44
C4573230
0D06092A 864886F7 0D010105 05003076 310B3009 06035504 06130255
53310B30
Certificate is abbreviated for easier viewing. quit certificate 6103EE0A0000000000038 ---!
3082040F 308203B9 A0030201 02020A61 03EE0A00 00000000 38300D06 092A8648 86F70D01 01050500
3076310B 30090603 55040613 02555331 0B300906 03550408 !--- Certificate is abbreviated for easier
viewing. quit certificate 6104020F0000000000039 3082040F 308203B9 A0030201 02020A61 04020F00
00000000 39300D06 092A8648 86F70D01 01050500 3076310B 30090603 55040613 02555331 0B300906
03550408 !--- Certificate is abbreviated for easier viewing. quit crypto ca certificate chain
caserver2 certificate 06C28C8B000000000003B 308203CF 30820379 A0030201 02020A06 C28C8B00 00000000
3B300D06 092A8648 86F70D01 01050500 3061310B 30090603 55040613 02555331 13301106 03550408 !---
Certificate is abbreviated for easier viewing. 97363 quit certificate 06C2807F000000000003A
308203CF 30820379 A0030201 02020A06 C2807F00 00000000 3A300D06 092A8648 !--- Certificate is
abbreviated for easier viewing. quit certificate ca 3E34CD199392A0914621EA778B13F357 30820284
3082022E A0030201 0202103E 34CD1993 92A09146 21EA778B 13F35730 0D06092A 864886F7 0D010105
05003061 310B3009 06035504 06130255 53311330 !--- Certificate is abbreviated for easier viewing.
quit ! crypto isakmp policy 10 hash md5 crypto isakmp identity hostname ! ! crypto ipsec
transform-set myset esp-des esp-md5-hmac ! crypto map vpn 10 ipsec-isakmp set peer 172.16.172.45
set transform-set myset match address 101 crypto map vpn 20 ipsec-isakmp set peer 172.16.172.51
set transform-set myset match address 102 crypto map vpn 30 ipsec-isakmp set peer 172.16.172.53
set transform-set myset match address 103 ! ! ! ! ! ! ! ! ! ! mta receive maximum-recipients
0 ! ! ! ! interface Ethernet0/0 ip address 172.16.172.35 255.255.255.240 half-duplex crypto map
vpn interface Ethernet0/1 ip address 192.168.4.1 255.255.255.0 half-duplex ! interface Serial1/0
no ip address shutdown ! interface Serial1/1 no ip address shutdown ! interface Serial1/2 no ip
address shutdown ! interface Serial1/3 no ip address shutdown ! ip classless ip route 0.0.0.0
0.0.0.0 172.16.172.33 ip http server ! ! access-list 101 permit ip 192.168.4.0 0.0.0.255
20.1.1.0 0.0.0.255 access-list 102 permit ip 192.168.4.0 0.0.0.255 3.3.3.0 0.0.0.255 access-list
103 permit ip 192.168.4.0 0.0.0.255 200.1.1.0 0.0.0.255 access-list 169 deny ip host
172.16.172.60 any access-list 169 deny ip host 172.16.172.61 any access-list 169 deny ip host
172.16.172.62 any access-list 169 permit ip any any ! call rsvp-sync ! ! mgcp profile default !
! ! dial-peer cor custom ! line con 0 exec-timeout 0 0 line aux 0 line vty 0 4 login ! ! end
#2611-VPN

```

## استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

## أوامر استكشاف الأخطاء وإصلاحها

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

ملاحظة: قبل إصدار أوامر debug، راجع [المعلومات المهمة في أوامر تصحيح الأخطاء](#).

- debug crypto pki transaction
- debug crypto pki messages
- debug crypto ipSec
- debug crypto isakmp

## تصحيح الأخطاء على الموجهات

يتم عرض تصحيح أخطاء IKE و IPsec من الموجهات الثلاثة في هذا الإخراج. أثناء مفاوضات IKE مع نظير IPsec، يجب أن يحدد الموجه 2600 خادم CA الذي سيتم استخدامه. في سيناريو الاختبار، قام الطرازان 1-1720 و 7204 ببدء نفق IPsec إلى موجه الشبكة الخاصة الظاهرية (VPN) طراز 2600.

يعرض هذا الإخراج تصحيح أخطاء IKE/ IPsec على الموجه VPN-2611 باستخدام أوامر `show crypto`.

```
2611-VPN#show debug
```

```
:Cryptographic Subsystem
Crypto ISAKMP debugging is on
Crypto IPSEC debugging is on

Debugs on the router when the 1720-1 router has initiated !--- an IPsec tunnel to the ---!
router. Oct 27 22:20:23.337: ISAKMP (0:0): received packet from 172.16.172.45 dport 500 sport
500 (N) NEW SA Oct 27 22:20:23.337: ISAKMP: local port 500, remote port 500 Oct 27 22:20:23.341:
ISAKMP (0:408): Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH Oct 27 22:20:23.341: ISAKMP (0:408): Old
State = IKE_READY New State = IKE_R_MM1 Oct 27 22:20:23.341: ISAKMP (0:408): processing SA
payload. message ID = 0 Oct 27 22:20:23.341: ISAKMP (0:408): Checking ISAKMP transform 1 against
priority 10 policy Oct 27 22:20:23.341: ISAKMP: encryption DES-CBC Oct 27 22:20:23.341: ISAKMP:
hash MD5 Oct 27 22:20:23.345: ISAKMP: default group 1 Oct 27 22:20:23.345: ISAKMP: auth RSA sig
Oct 27 22:20:23.345: ISAKMP: life type in seconds Oct 27 22:20:23.345: ISAKMP: life duration
(VPI) of 0x0 0x1 0x51 0x80 Oct 27 22:20:23.345: ISAKMP (0:408): atts are acceptable. Next
payload is 3 Oct 27 22:20:23.389: ISAKMP (0:408): Input = IKE_MSG_INTERNAL,
IKE_PROCESS_MAIN_MODE Oct 27 22:20:23.389: ISAKMP (0:408): Old State = IKE_R_MM1 New State =
IKE_R_MM1 Oct 27 22:20:23.389: ISAKMP (0:408): sending packet to 172.16.172.45 my_port 500
peer_port 500 (R) MM_SA_SETUP Oct 27 22:20:23.393: ISAKMP (0:408): Input = IKE_MSG_INTERNAL,
IKE_PROCESS_COMPLETE Oct 27 22:20:23.393: ISAKMP (0:408): Old State = IKE_R_MM1 New State =
IKE_R_MM2 Oct 27 22:20:23.538: ISAKMP (0:408): received packet from 172.16.172.45 dport 500
sport 500 (R) MM_SA_SETUP Oct 27 22:20:23.538: ISAKMP (0:408): Input = IKE_MSG_FROM_PEER,
IKE_MM_EXCH Oct 27 22:20:23.538: ISAKMP (0:408): Old State = IKE_R_MM2 New State = IKE_R_MM3 Oct
27 22:20:23.542: ISAKMP (0:408): processing KE payload. message ID = 0 Oct 27 22:20:23.582:
ISAKMP (0:408): processing NONCE payload. message ID = 0 Oct 27 22:20:23.626: ISAKMP (0:408):
SKEYID state generated Oct 27 22:20:23.630: ISAKMP (0:408): processing CERT_REQ payload. message
ID = 0 Oct 27 22:20:23.630: ISAKMP (0:408): peer wants a CT_X509_SIGNATURE cert Oct 27
,22:20:23.634: ISAKMP (0:408): peer want cert issued by CN = SJVPNTAC-CAServer
,OU = TAC-VPN-SJ
,O = Cisco Systems

L = San Jose, ST = CA, C = US
The router has determined that the !--- IPsec peer sends a certificate !--- that CA server1 ---!
has issued. Oct 27 22:20:23.642: ISAKMP (0:408): Choosing trustpoint caserver1 as issuer
Oct 27 22:20:23.642: ISAKMP (0:408): processing vendor id payload
Oct 27 22:20:23.642: ISAKMP (0:408): vendor ID is Unity
```

```
Oct 27 22:20:23.642: ISAKMP (0:408): processing vendor id payload
Oct 27 22:20:23.646: ISAKMP (0:408): vendor ID is DPD
Oct 27 22:20:23.646: ISAKMP (0:408): processing vendor id payload
!Oct 27 22:20:23.646: ISAKMP (0:408): speaking to another IOS box
,Oct 27 22:20:23.646: ISAKMP (0:408): Input = IKE_MSG_INTERNAL
IKE_PROCESS_MAIN_MODE
Oct 27 22:20:23.646: ISAKMP (0:408): Old State = IKE_R_MM3 New State = IKE_R_MM3

Oct 27 22:20:23.666: ISAKMP (0:408): sending packet to 172.16.172.45
(my_port 500 peer_port 500 (R
MM_KEY_EXCH
Oct 27 22:20:23.670: ISAKMP (0:408): Input = IKE_MSG_INTERNAL, IKE_PROCESS_COMPLETE
Oct 27 22:20:23.670: ISAKMP (0:408): Old State = IKE_R_MM3 New State = IKE_R_MM4

Oct 27 22:20:24.207: ISAKMP (0:408): received packet from 172.16.172.45
(dport 500 sport 500 (R
MM_KEY_EXCH
Oct 27 22:20:24.219: ISAKMP (0:408): Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH
Oct 27 22:20:24.219: ISAKMP (0:408): Old State = IKE_R_MM4 New State = IKE_R_MM5

Oct 27 22:20:24.223: ISAKMP (0:408): processing ID payload. message ID = 0
Oct 27 22:20:24.223: ISAKMP (408): Process ID payload
type : 2
FQDN name : 1720-1.tac.com
protocol : 17
port : 500
length : 14
Oct 27 22:20:24.223: ISAKMP (0:408): processing CERT payload. message ID = 0
Oct 27 22:20:24.223: ISAKMP (0:408): processing a CT_X509_SIGNATURE cert
Oct 27 22:20:24.267: ISAKMP (0:408): peer's pubkey isn't cached
Oct 27 22:20:24.319: ISAKMP (0:408): cert approved with warning
Subject name of 1720-1 router's !--- certificates from CA server1. !--- FQDN of 1720-1. Oct ---!
27 22:20:24.383: ISAKMP (0:408): OU = MADRID O=SPAIN
Oct 27 22:20:24.419: ISAKMP (0:408): processing SIG payload. message ID = 0
= Oct 27 22:20:24.419: ISAKMP (408): sa->peer.name = , sa->peer.id.id.id_fqdn.fqdn
tac.com.1720-1
Oct 27 22:20:24.475: ISAKMP (0:408): processing NOTIFY INITIAL_CONTACT protocol 1
spi 0, message ID = 0, sa = 82F6FE80
Oct 27 22:20:24.475: ISAKMP (0:408): Process initial contact, bring down existing phase
and 2 SA's 1

with local 172.16.172.35 remote 172.16.172.45
Oct 27 22:20:24.479: ISAKMP (0:408): SA has been authenticated with 172.16.172.45
Oct 27 22:20:24.479: ISAKMP (0:408): Input = IKE_MSG_INTERNAL, IKE_PROCESS_MAIN_MODE
Oct 27 22:20:24.479: ISAKMP (0:408): Old State = IKE_R_MM5 New State = IKE_R_MM5

...Oct 27 22:20:24.479: IPSEC(key_engine): got a queue event
Oct 27 22:20:24.483: ISAKMP (0:408): SA is doing RSA signature authentication using
id type ID_FQDN
Oct 27 22:20:24.483: ISAKMP (408): ID payload
next-payload : 6
type : 2
FQDN name : 2611-vpn.cisco.com
protocol : 17
port : 0
length : 22
Oct 27 22:20:24.483: ISAKMP (408): Total payload length: 26
Oct 27 22:20:24.495: ISKAMP: growing send buffer from 1024 to 3072
Oct 27 22:20:24.507: ISAKMP (0:408): using the caserver1 trustpoint's
keypair to sign
Oct 27 22:20:24.956: ISAKMP (0:408): sending packet to 172.16.172.45
(my_port 500 peer_port 500 (R
MM_KEY_EXCH
,Oct 27 22:20:24.956: ISAKMP (0:408): Input = IKE_MSG_INTERNAL
```



```

                                                    IKE_PROCESS_COMPLETE
= Oct 27 22:20:24.956: ISAKMP (0:408): Old State = IKE_R_MM5 New State
                                                    IKE_P1_COMPLETE

,Oct 27 22:20:24.960: ISAKMP (0:408): Input = IKE_MESG_INTERNAL
                                                    IKE_PHASE1_COMPLETE
Oct 27 22:20:24.960: ISAKMP (0:408): Old State = IKE_P1_COMPLETE
New State = IKE_P1_COMPLETE

Oct 27 22:20:25.168: ISAKMP (0:408): received packet from 172.16.172.45
(dport 500 sport 500 (R
Q_M_IDLE
Oct 27 22:20:25.172: ISAKMP: set new node -2090109070 to Q_M_IDLE
Oct 27 22:20:25.192: ISAKMP (0:408): processing HASH payload. message ID = -2090109070
Oct 27 22:20:25.192: ISAKMP (0:408): processing SA payload. message ID = -2090109070
Oct 27 22:20:25.192: ISAKMP (0:408): Checking IPsec proposal 1
Oct 27 22:20:25.192: ISAKMP: transform 1, ESP_DES
:Oct 27 22:20:25.192: ISAKMP: attributes in transform
Oct 27 22:20:25.192: ISAKMP: encaps is 1
Oct 27 22:20:25.192: ISAKMP: SA life type in seconds
Oct 27 22:20:25.196: ISAKMP: SA life duration (basic) of 3600
Oct 27 22:20:25.196: ISAKMP: SA life type in kilobytes
Oct 27 22:20:25.196: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0
Oct 27 22:20:25.196: ISAKMP: authenticator is HMAC-MD5
.Oct 27 22:20:25.196: ISAKMP (0:408): atts are acceptable
,Oct 27 22:20:25.196: IPSEC(validate_proposal_request): proposal part #1
,key eng. msg.) INBOUND local= 172.16.172.35, remote= 172.16.172.45)
,(local_proxy= 192.168.4.0/255.255.255.0/0/0 (type=4
,(remote_proxy= 20.1.1.0/255.255.255.0/0/0 (type=4
, protocol= ESP, transform= esp-des esp-md5-hmac
,lifedur= 0s and 0kb
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x2
Oct 27 22:20:25.200: ISAKMP (0:408): processing NONCE payload. message ID = -2090109070
Oct 27 22:20:25.200: ISAKMP (0:408): processing ID payload. message ID = -2090109070
Oct 27 22:20:25.204: ISAKMP (0:408): processing ID payload. message ID = -2090109070
Oct 27 22:20:25.204: ISAKMP (0:408): asking for 1 spis from ipsec
,Oct 27 22:20:25.204: ISAKMP (0:408): Node -2090109070, Input = IKE_MESG_FROM_PEER
IKE_QM_EXCH
= Oct 27 22:20:25.204: ISAKMP (0:408): Old State = IKE_QM_READY New State
IKE_QM_SPI_STARVE
...Oct 27 22:20:25.204: IPSEC(key_engine): got a queue event
Oct 27 22:20:25.208: IPSEC(spi_response): getting spi 2951036365 for SA
from 172.16.172.35 to 172.16.172.45 for prot 3
(Oct 27 22:20:25.208: ISAKMP: received ke message (2/1
Oct 27 22:20:25.493: ISAKMP (0:408): sending packet to 172.16.172.45
(my_port 500 peer_port 500 (R
Q_M_IDLE
,Oct 27 22:20:25.493: ISAKMP (0:408): Node -2090109070, Input = IKE_MESG_FROM_IPSEC
IKE_SPI_REPLY
= Oct 27 22:20:25.493: ISAKMP (0:408): Old State = IKE_QM_SPI_STARVE New State
IKE_QM_R_QM2
Oct 27 22:20:25.577: ISAKMP (0:408): received packet from 172.16.172.45 dport 500
(sport 500 (R
Q_M_IDLE
Oct 27 22:20:25.669: ISAKMP (0:408): Creating IPsec SAs
Oct 27 22:20:25.669: inbound SA from 172.16.172.45 to 172.16.172.35
(proxy 20.1.1.0 to 192.168.4.0)
Oct 27 22:20:25.669: has spi 0xAFE53DCD and conn_id 420 and flags 2
Oct 27 22:20:25.669: lifetime of 3600 seconds
Oct 27 22:20:25.669: lifetime of 4608000 kilobytes
Oct 27 22:20:25.669: has client flags 0x0
Oct 27 22:20:25.673: outbound SA from 172.16.172.35 to 172.16.172.45
(proxy 192.168.4.0 to 20.1.1.0)
Oct 27 22:20:25.673: has spi 563992317 and conn_id 421 and flags A
```

```

Oct 27 22:20:25.673: lifetime of 3600 seconds
Oct 27 22:20:25.673: lifetime of 4608000 kilobytes
Oct 27 22:20:25.673: has client flags 0x0
Oct 27 22:20:25.673: ISAKMP (0:408): deleting node -2090109070 error FALSE reason
"()quick mode done (await"
,Oct 27 22:20:25.673: ISAKMP (0:408): Node -2090109070, Input = IKE_MSG_FROM_PEER
IKE_QM_EXCH
= Oct 27 22:20:25.677: ISAKMP (0:408): Old State = IKE_QM_R_QM2 New State
IKE_QM_PHASE2_COMPLETE
...Oct 27 22:20:25.677: IPSEC(key_engine): got a queue event
, :(Oct 27 22:20:25.677: IPSEC(initialize_sas
,key eng. msg.) INBOUND local= 172.16.172.35, remote= 172.16.172.45)
,(local_proxy= 192.168.4.0/255.255.255.0/0/0 (type=4
,(remote_proxy= 20.1.1.0/255.255.255.0/0/0 (type=4
, protocol= ESP, transform= esp-des esp-md5-hmac
,lifedur= 3600s and 4608000kb
spi= 0xAF53DCD(2951036365), conn_id= 420, keysize= 0, flags= 0x2
, :(Oct 27 22:20:25.681: IPSEC(initialize_sas
,key eng. msg.) OUTBOUND local= 172.16.172.35, remote= 172.16.172.45)
,(local_proxy= 192.168.4.0/255.255.255.0/0/0 (type=4
,(remote_proxy= 20.1.1.0/255.255.255.0/0/0 (type=4
, protocol= ESP, transform= esp-des esp-md5-hmac
,lifedur= 3600s and 4608000kb
spi= 0x219DD6FD(563992317), conn_id= 421, keysize= 0, flags= 0xA
Oct 27 22:20:25.681: IPSEC(add mtree): src 192.168.4.0, dest 20.1.1.0, dest_port 0
,Oct 27 22:20:25.681: IPSEC(create_sa): sa created
,sa) sa_dest= 172.16.172.35, sa_prot= 50)
,(sa_spi= 0xAF53DCD(2951036365
sa_trans= esp-des esp-md5-hmac , sa_conn_id= 420
,Oct 27 22:20:25.685: IPSEC(create_sa): sa created
,sa) sa_dest= 172.16.172.45, sa_prot= 50)
,(sa_spi= 0x219DD6FD(563992317
sa_trans= esp-des esp-md5-hmac , sa_conn_id= 421
Oct 27 22:20:26.070: ISAKMP (0:407): purging SA., sa=82F7ADE0, delme=82F7ADE0
#2611-VPN
#2611-VPN
#2611-VPN
#2611-VPN

```

*Debugs on the router when the 7204-1 router has initiated !--- an IPsec tunnel to the ---!*

```

router. Oct 27 22:32:02.740: ISAKMP (0:0): received packet from 172.16.172.51 dport 500 sport
500 (N) NEW SA Oct 27 22:32:02.740: ISAKMP: local port 500, remote port 500 Oct 27 22:32:02.740:
ISAKMP (0:412): Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH Oct 27 22:32:02.744: ISAKMP (0:412): Old
State = IKE_READY New State = IKE_R_MM1 Oct 27 22:32:02.744: ISAKMP (0:412): processing SA
payload. message ID = 0 Oct 27 22:32:02.744: ISAKMP (0:412): Checking ISAKMP transform 1 against
priority 10 policy Oct 27 22:32:02.744: ISAKMP: encryption DES-CBC Oct 27 22:32:02.744: ISAKMP:
hash MD5 Oct 27 22:32:02.744: ISAKMP: default group 1 Oct 27 22:32:02.748: ISAKMP: auth RSA sig
Oct 27 22:32:02.748: ISAKMP: life type in seconds Oct 27 22:32:02.748: ISAKMP: life duration
(VPI) of 0x0 0x1 0x51 0x80 Oct 27 22:32:02.748: ISAKMP (0:412): atts are acceptable. Next
payload is 3 Oct 27 22:32:02.792: ISAKMP (0:412): Input = IKE_MSG_INTERNAL,
IKE_PROCESS_MAIN_MODE Oct 27 22:32:02.792: ISAKMP (0:412): Old State = IKE_R_MM1 New State =
IKE_R_MM1 Oct 27 22:32:02.792: ISAKMP (0:412): sending packet to 172.16.172.51 my_port 500
peer_port 500 (R) MM_SA_SETUP Oct 27 22:32:02.796: ISAKMP (0:412): Input = IKE_MSG_INTERNAL,
IKE_PROCESS_COMPLETE Oct 27 22:32:02.796: ISAKMP (0:412): Old State = IKE_R_MM1 New State =
IKE_R_MM2 Oct 27 22:32:02.820: ISAKMP (0:412): received packet from 172.16.172.51 dport 500
sport 500 (R) MM_SA_SETUP Oct 27 22:32:02.820: ISAKMP (0:412): Input = IKE_MSG_FROM_PEER,
IKE_MM_EXCH Oct 27 22:32:02.824: ISAKMP (0:412): Old State = IKE_R_MM2 New State = IKE_R_MM3 Oct
27 22:32:02.824: ISAKMP (0:412): processing KE payload. message ID = 0 Oct 27 22:32:02.868:
ISAKMP (0:412): processing NONCE payload. message ID = 0 Oct 27 22:32:02.908: ISAKMP (0:412):
SKEYID state generated Oct 27 22:32:02.912: ISAKMP (0:412): processing CERT_REQ payload. message
ID = 0 Oct 27 22:32:02.912: ISAKMP (0:412): peer wants a CT_X509_SIGNATURE cert Oct 27
,22:32:02.916: ISAKMP (0:412): peer want cert issued by CN = vpn
,OU = cisco, O = tac

```

L = san jose, ST = california, C = US

The router has determined that the !--- IPsec peer is sending a certificate !--- that CA ---!  
server2 has issued.

```
Oct 27 22:32:02.924: ISAKMP (0:412): Choosing trustpoint caserver2 as issuer
Oct 27 22:32:02.928: ISAKMP (0:412): processing vendor id payload
Oct 27 22:32:02.928: ISAKMP (0:412): vendor ID is Unity
Oct 27 22:32:02.928: ISAKMP (0:412): processing vendor id payload
Oct 27 22:32:02.928: ISAKMP (0:412): vendor ID is DPD
Oct 27 22:32:02.928: ISAKMP (0:412): processing vendor id payload
!Oct 27 22:32:02.928: ISAKMP (0:412): speaking to another IOS box
,Oct 27 22:32:02.932: ISAKMP (0:412): Input = IKE_MSG_INTERNAL
IKE_PROCESS_MAIN_MODE
Oct 27 22:32:02.932: ISAKMP (0:412): Old State = IKE_R_MM3 New State = IKE_R_MM3
Oct 27 22:32:02.952: ISAKMP (0:412): sending packet to 172.16.172.51 my_port 500
peer_port 500
R) MM_KEY_EXCH)
,Oct 27 22:32:02.952: ISAKMP (0:412): Input = IKE_MSG_INTERNAL
IKE_PROCESS_COMPLETE
Oct 27 22:32:02.952: ISAKMP (0:412): Old State = IKE_R_MM3 New State = IKE_R_MM4
Oct 27 22:32:03.016: ISAKMP (0:412): received packet from 172.16.172.51 dport 500
sport 500
R) MM_KEY_EXCH)
Oct 27 22:32:03.032: ISAKMP (0:412): Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH
Oct 27 22:32:03.032: ISAKMP (0:412): Old State = IKE_R_MM4 New State = IKE_R_MM5
Oct 27 22:32:03.032: ISAKMP (0:412): processing ID payload. message ID = 0
Oct 27 22:32:03.032: ISAKMP (412): Process ID payload
type : 2
FQDN name : 7204-1.cisco.com
protocol : 17
port : 500
length : 16
Oct 27 22:32:03.032: ISAKMP (0:412): processing CERT payload. message ID = 0
Oct 27 22:32:03.036: ISAKMP (0:412): processing a CT_X509_SIGNATURE cert
Oct 27 22:32:03.076: ISAKMP (0:412): peer's pubkey isn't cached
Oct 27 22:32:03.129: ISAKMP (0:412): cert approved with warning
Subject name of 7204-1 router's certificate issued by CA server2. Oct 27 22:32:03.189: ---!
ISAKMP (0:412): OU = BERLIN O=GERMANY
Oct 27 22:32:03.229: ISAKMP (0:412): processing SIG payload. message ID = 0
FQDN of 7204-1. Oct 27 22:32:03.229: ISAKMP (412): sa->peer.name = , sa- ---!
= >peer_id.id.id_fqdn.fqdn
cisco.com.7204-1
Oct 27 22:32:03.265: ISAKMP (0:412): processing NOTIFY INITIAL_CONTACT protocol 1
spi 0, message ID = 0, sa = 82F69D84
Oct 27 22:32:03.269: ISAKMP (0:412): Process initial contact, bring down existing phase 1
and 2 SA's with local
remote 172.16.172.51 172.16.172.35
Oct 27 22:32:03.269: ISAKMP (0:412): SA has been authenticated with 172.16.172.51
Oct 27 22:32:03.269: ISAKMP (0:412): Input = IKE_MSG_INTERNAL, IKE_PROCESS_MAIN_MODE
Oct 27 22:32:03.269: ISAKMP (0:412): Old State = IKE_R_MM5 New State = IKE_R_MM5
...Oct 27 22:32:03.269: IPSEC(key_engine): got a queue event
Oct 27 22:32:03.273: ISAKMP (0:412): SA is doing RSA signature authentication
using id type ID_FQDN
Oct 27 22:32:03.273: ISAKMP (412): ID payload
next-payload : 6
type : 2
FQDN name : 2611-vpn.cisco.com
protocol : 17
port : 0
length : 22
```

Oct 27 22:32:03.273: ISAKMP (412): Total payload length: 26  
Oct 27 22:32:03.285: ISKAMP: growing send buffer from 1024 to 3072  
Oct 27 22:32:03.297: ISAKMP (0:412): using the caserver2 trustpoint's keypair to sign  
Oct 27 22:32:03.762: ISAKMP (0:412): sending packet to 172.16.172.51 my\_port 500  
peer\_port 500  
R) MM\_KEY\_EXCH)  
Oct 27 22:32:03.762: ISAKMP (0:412): Input = IKE\_MSG\_INTERNAL, IKE\_PROCESS\_COMPLETE  
Oct 27 22:32:03.766: ISAKMP (0:412): Old State = IKE\_R\_MM5 New State = IKE\_P1\_COMPLETE  
  
Oct 27 22:32:03.766: ISAKMP (0:412): Input = IKE\_MSG\_INTERNAL, IKE\_PHASE1\_COMPLETE  
= Oct 27 22:32:03.766: ISAKMP (0:412): Old State = IKE\_P1\_COMPLETE New State  
IKE\_P1\_COMPLETE  
  
Oct 27 22:32:03.790: ISAKMP (0:412): received packet from 172.16.172.51 dport 500  
sport 500  
R) QM\_IDLE)  
Oct 27 22:32:03.790: ISAKMP: set new node 1631242332 to QM\_IDLE  
Oct 27 22:32:03.810: ISAKMP (0:412): processing HASH payload. message ID = 1631242332  
Oct 27 22:32:03.810: ISAKMP (0:412): processing SA payload. message ID = 1631242332  
Oct 27 22:32:03.810: ISAKMP (0:412): Checking IPsec proposal 1  
Oct 27 22:32:03.810: ISAKMP: transform 1, ESP\_DES  
:Oct 27 22:32:03.810: ISAKMP: attributes in transform  
Oct 27 22:32:03.810: ISAKMP: encaps is 1  
Oct 27 22:32:03.814: ISAKMP: SA life type in seconds  
Oct 27 22:32:03.814: ISAKMP: SA life duration (basic) of 3600  
Oct 27 22:32:03.814: ISAKMP: SA life type in kilobytes  
Oct 27 22:32:03.814: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0  
Oct 27 22:32:03.814: ISAKMP: authenticator is HMAC-MD5  
.Oct 27 22:32:03.814: ISAKMP (0:412): atts are acceptable  
,Oct 27 22:32:03.818: IPSEC(validate\_proposal\_request): proposal part #1  
,key eng. msg.) INBOUND local= 172.16.172.35, remote= 172.16.172.51)  
,(local\_proxy= 192.168.4.0/255.255.255.0/0/0 (type=4  
,(remote\_proxy= 3.3.3.0/255.255.255.0/0/0 (type=4  
, protocol= ESP, transform= esp-des esp-md5-hmac  
,lifedur= 0s and 0kb  
spi= 0x0(0), conn\_id= 0, keysize= 0, flags= 0x2  
Oct 27 22:32:03.818: ISAKMP (0:412): processing NONCE payload. message ID = 1631242332  
Oct 27 22:32:03.822: ISAKMP (0:412): processing ID payload. message ID = 1631242332  
Oct 27 22:32:03.822: ISAKMP (0:412): processing ID payload. message ID = 1631242332  
Oct 27 22:32:03.822: ISAKMP (0:412): asking for 1 spis from ipsec  
,Oct 27 22:32:03.822: ISAKMP (0:412): Node 1631242332, Input = IKE\_MSG\_FROM\_PEER  
IKE\_QM\_EXCH  
= Oct 27 22:32:03.822: ISAKMP (0:412): Old State = IKE\_QM\_READY New State  
IKE\_QM\_SPI\_STARVE  
...Oct 27 22:32:03.822: IPSEC(key\_engine): got a queue event  
Oct 27 22:32:03.826: IPSEC(spi\_response): getting spi 3365950736 for SA  
from 172.16.172.35 to 172.16.172.51 for prot 3  
(Oct 27 22:32:03.826: ISAKMP: received ke message (2/1  
Oct 27 22:32:04.090: ISAKMP (0:412): sending packet to 172.16.172.51 my\_port 500  
peer\_port 500  
R) QM\_IDLE)  
= Oct 27 22:32:04.094: ISAKMP (0:412): Node 1631242332, Input  
IKE\_MSG\_FROM\_IPSEC, IKE\_SPI\_REPLY  
= Oct 27 22:32:04.094: ISAKMP (0:412): Old State = IKE\_QM\_SPI\_STARVE New State  
IKE\_QM\_R\_QM2  
Oct 27 22:32:04.102: ISAKMP (0:412): received packet from 172.16.172.51  
dport 500 sport 500  
R) QM\_IDLE)  
Oct 27 22:32:04.190: ISAKMP (0:412): Creating IPsec SAs  
Oct 27 22:32:04.190: inbound SA from 172.16.172.51 to 172.16.172.35  
(proxy 3.3.3.0 to 192.168.4.0)  
Oct 27 22:32:04.190: has spi 0xC8A05510 and conn\_id 422 and flags 2  
Oct 27 22:32:04.190: lifetime of 3600 seconds  
Oct 27 22:32:04.190: lifetime of 4608000 kilobytes

```

Oct 27 22:32:04.190: has client flags 0x0
Oct 27 22:32:04.194: outbound SA from 172.16.172.35 to 172.16.172.51
    ( proxy 192.168.4.0 to 3.3.3.0)
Oct 27 22:32:04.194: has spi -788374095 and conn_id 423 and flags A
    Oct 27 22:32:04.194: lifetime of 3600 seconds
    Oct 27 22:32:04.194: lifetime of 4608000 kilobytes
    Oct 27 22:32:04.194: has client flags 0x0
Oct 27 22:32:04.194: ISAKMP (0:412): deleting node 1631242332 error FALSE
    reason "quick mode done
        "())await)
    = Oct 27 22:32:04.194: ISAKMP (0:412): Node 1631242332, Input
        IKE_MSG_FROM_PEER, IKE_QM_EXCH
= Oct 27 22:32:04.198: ISAKMP (0:412): Old State = IKE_QM_R_QM2 New State
    IKE_QM_PHASE2_COMPLETE
    ...Oct 27 22:32:04.198: IPSEC(key_engine): got a queue event
        , :(Oct 27 22:32:04.198: IPSEC(initialize_sas
, key eng. msg.) INBOUND local= 172.16.172.35, remote= 172.16.172.51)
        ,(local_proxy= 192.168.4.0/255.255.255.0/0/0 (type=4
        ,(remote_proxy= 3.3.3.0/255.255.255.0/0/0 (type=4
        , protocol= ESP, transform= esp-des esp-md5-hmac
        ,lifedur= 3600s and 4608000kb
        spi= 0xC8A05510(3365950736), conn_id= 422, keysize= 0, flags= 0x2
        , :(Oct 27 22:32:04.202: IPSEC(initialize_sas
, key eng. msg.) OUTBOUND local= 172.16.172.35, remote= 172.16.172.51)
        ,(local_proxy= 192.168.4.0/255.255.255.0/0/0 (type=4
        ,(remote_proxy= 3.3.3.0/255.255.255.0/0/0 (type=4
        , protocol= ESP, transform= esp-des esp-md5-hmac
        ,lifedur= 3600s and 4608000kb
        spi= 0xD1025DB1(3506593201), conn_id= 423, keysize= 0, flags= 0xA
Oct 27 22:32:04.202: IPSEC(add mtree): src 192.168.4.0, dest 3.3.3.0, dest_port 0

,Oct 27 22:32:04.202: IPSEC(create_sa): sa created
    ,sa) sa_dest= 172.16.172.35, sa_prot= 50)
        ,(sa_spi= 0xC8A05510(3365950736
    sa_trans= esp-des esp-md5-hmac , sa_conn_id= 422
,Oct 27 22:32:04.206: IPSEC(create_sa): sa created
    ,sa) sa_dest= 172.16.172.51, sa_prot= 50)
        ,(sa_spi= 0xD1025DB1(3506593201
    sa_trans= esp-des esp-md5-hmac , sa_conn_id= 423
        #2611-VPN
        #2611-VPN
        2611-VPN#show crypto en conn ac

```

```

ID Interface
IP-Address State Algorithm
Encrypt Decrypt
Ethernet0/0 411
set HMAC_MD5+DES_56_CB 172.16.172.35
    0 0
Ethernet0/0 412
set HMAC_MD5+DES_56_CB 172.16.172.35
    0 0
Ethernet0/0 420
set HMAC_MD5+DES_56_CB 172.16.172.35
    8 0
Ethernet0/0 421
set HMAC_MD5+DES_56_CB 172.16.172.35
    0 8
Ethernet0/0 422
set HMAC_MD5+DES_56_CB 172.16.172.35
    9 0
Ethernet0/0 423
set HMAC_MD5+DES_56_CB 172.16.172.35
    0 9

```

#2611-VPN  
#2611-VPN  
#2611-VPN  
#2611-VPN

2611-VPN#**show crypto map**

Crypto Map "vpn" 10 ipsec-isakmp  
Peer  
172.16.172.45 =  
Extended  
IP access list 101

access-list 101 permit ip 192.168.4.0 0.0.0.255 20.1.1.0 0.0.0.255  
Current  
peer: 172.16.172.45  
Security  
association lifetime: 4608000 kilobytes/3600 seconds  
PFS  
Y/N): N)  
Transform  
}=sets

,myset

{

Crypto Map "vpn" 20 ipsec-isakmp  
Peer  
172.16.172.51 =  
Extended  
IP access list 102

access-list 102 permit ip 192.168.4.0 0.0.0.255 3.3.3.0 0.0.0.255  
Current  
peer: 172.16.172.51  
Security  
association lifetime: 4608000 kilobytes/3600 seconds  
PFS  
Y/N): N)  
Transform  
}=sets

,myset

{

Crypto Map "vpn" 30 ipsec-isakmp  
Peer = 172.16.172.53  
Extended  
IP access list 103

access-list 103 permit ip 192.168.4.0 0.0.0.255 200.1.1.0 0.0.0.255  
Current  
peer: 172.16.172.53  
Security  
association lifetime: 4608000 kilobytes/3600 seconds  
PFS  
Y/N): N)  
Transform  
}=sets

,myset

{

Interfaces

:using crypto map vpn

Ethernet0/0

2611-VPN#**show crypto isa sa**

```

dst
src
state conn-id
slot
172.16.172.51 172.16.172.35
QM_IDLE
0 412
172.16.172.45 172.16.172.35
QM_IDLE
0 411
2611-VPN#show crypto ipsec sa
interface: Ethernet0/0
Crypto map tag: vpn, local
addr. 172.16.172.35
:(local ident (addr/mask/prot/port
(192.168.4.0/255.255.255.0/0/0)
:(remote ident (addr/mask/prot/port
(200.1.1.0/255.255.255.0/0/0)
current_peer: 172.16.172.53:500
{,PERMIT, flags={origin_is_acl
:pkts encaps: 0, #pkts encrypt#
pkts digest 0# ,0
:pkts decaps: 0, #pkts decrypt#
pkts verify 0# ,0
pkts compressed: 0, #pkts#
decompressed: 0
pkts not compressed: 0, #pkts#
compr. failed: 0
,pkts not decompressed: 0#
pkts decompress failed: 0#
send errors 0, #recv errors#
0
:.local crypto endpt
remote crypto endpt.: 172.16.172.53 ,172.16.172.35
path mtu 1500, media
mtu 1500
:current outbound spi
0
:inbound esp sas
:inbound ah sas
:inbound pcp sas
:outbound esp sas
:outbound ah sas
:outbound pcp sas
:(local ident (addr/mask/prot/port
(192.168.4.0/255.255.255.0/0/0)
:(remote ident (addr/mask/prot/port
(3.3.3.0/255.255.255.0/0/0)
current_peer: 172.16.172.51:500
{,PERMIT, flags={origin_is_acl
:pkts encaps: 9, #pkts encrypt#
pkts digest 9# ,9
:pkts decaps: 9, #pkts decrypt#
pkts verify 9# ,9
pkts compressed: 0, #pkts#
decompressed: 0
pkts not compressed: 0, #pkts#
compr. failed: 0
,pkts not decompressed: 0#
pkts decompress failed: 0#
send errors 0, #recv errors#
0
:.local crypto endpt
remote crypto endpt.: 172.16.172.51 ,172.16.172.35

```

```

path mtu 1500, media
mtu 1500
:current outbound spi
D1025DB1
:inbound esp sas
 spi: 0xC8A05510(3365950736
:transform
, esp-des esp-md5-hmac
in
{ ,use settings ={Tunnel
:slot
conn id: 422, flow_id: 3, crypto map: vpn ,0
sa
(timing: remaining key lifetime (k/sec): (4607998/3519
IV
size: 8 bytes
replay
detection support: Y
:inbound ah sas
:inbound pcp sas
:outbound esp sas
 spi: 0xD1025DB1(3506593201
:transform
, esp-des esp-md5-hmac
in
{ ,use settings ={Tunnel
:slot
conn id: 423, flow_id: 4, crypto map: vpn ,0
sa
(timing: remaining key lifetime (k/sec): (4607998/3519
IV
size: 8 bytes
replay
detection support: Y
:outbound ah sas
:outbound pcp sas
:(local ident (addr/mask/prot/port
(192.168.4.0/255.255.255.0/0/0)
:(remote ident (addr/mask/prot/port
(20.1.1.0/255.255.255.0/0/0)
current_peer: 172.16.172.45:500
{,PERMIT, flags={origin_is_acl
:pkts encaps: 8, #pkts encrypt#
pkts digest 8# ,8
:pkts decaps: 8, #pkts decrypt#
pkts verify 8# ,8
pkts compressed: 0, #pkts#
decompressed: 0
pkts not compressed: 0, #pkts#
compr. failed: 0
,pkts not decompressed: 0#
pkts decompress failed: 0#
send errors 0, #recv errors#
0
:.local crypto endpt
remote crypto endpt.: 172.16.172.45 ,172.16.172.35
path mtu 1500, media
mtu 1500
:current outbound spi
5F57E177
:inbound esp sas
 spi: 0xC7DB301B(3353030683
:transform
, esp-des esp-md5-hmac

```



```

in
{ ,use settings ={Tunnel
:slot
conn id: 420, flow_id: 1, crypto map: vpn ,0
sa
(timing: remaining key lifetime (k/sec): (4607998/3410
IV
size: 8 bytes
replay
detection support: Y
:inbound ah sas
:inbound pcg sas
:outbound esp sas
(spi: 0x5F57E177(1599594871
:transform
, esp-des esp-md5-hmac
in
{ ,use settings ={Tunnel
:slot
conn id: 421, flow_id: 2, crypto map: vpn ,0
sa
(timing: remaining key lifetime (k/sec): (4607998/3409
IV
size: 8 bytes
replay
detection support: Y
:outbound ah sas
:outbound pcg sas
#2611-VPN
#2611-VPN

```

يعرض هذا الإخراج تصحيح أخطاء IKE/ IPsec على الموجه 1-1720 باستخدام أوامر `show crypto`. يقوم هذا الإخراج ببدء نفق IPsec إلى موجه VPN-2611.

```

, : (Oct 27 22:21:04.994: IPSEC(sa_request
,key eng. msg.) OUTBOUND local= 172.16.172.45, remote= 172.16.172.35)
,(local_proxy= 20.1.1.0/255.255.255.0/0/0 (type=4
,(remote_proxy= 192.168.4.0/255.255.255.0/0/0 (type=4
, protocol= ESP, transform= esp-des esp-md5-hmac
,lifedur= 3600s and 4608000kb
=spi= 0x219DD6FD(563992317), conn_id= 0, keysize
flags= 0x400C ,0
(Oct 27 22:21:04.998: ISAKMP: received ke message (1/1
Oct 27 22:21:04.998: ISAKMP: local port 500, remote port 500
Oct 27 22:21:05.002: ISAKMP (0:3): Input = IKE_MSG_FROM_IPSEC, IKE_SA_REQ_MM
Oct 27 22:21:05.002: ISAKMP (0:3): Old State = IKE_READY New
State = IKE_I_MM1
Oct 27 22:21:05.002: ISAKMP (0:3): beginning Main Mode exchange
Oct 27 22:21:05.002: ISAKMP (0:3): sending packet to 172.16.172.35
I) MM_NO_STATE)
Oct 27 22:21:05.062: ISAKMP (0:3): received packet from 172.16.172.35
I) MM_NO_STATE)
Oct 27 22:21:05.062: ISAKMP (0:3): Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH
Oct 27 22:21:05.066: ISAKMP (0:3): Old State = IKE_I_MM1 New
State = IKE_I_MM2
Oct 27 22:21:05.066: ISAKMP (0:3): processing SA payload. message ID
0 =
Oct 27 22:21:05.066: ISAKMP (0:3): Checking ISAKMP transform 1 against
priority 10 policy
Oct 27 22:21:05.066: ISAKMP: encryption
DES-CBC
Oct 27 22:21:05.066: ISAKMP: hash MD5
Oct 27 22:21:05.066: ISAKMP: default

```

```

                                group 1
                                Oct 27 22:21:05.066: ISAKMP: auth RSA
                                sig
                                Oct 27 22:21:05.066: ISAKMP: life type
                                in seconds
                                Oct 27 22:21:05.070: ISAKMP: life duration
                                VPI) of 0x0 0x1 0x51 0x80)
                                Oct 27 22:21:05.070: ISAKMP (0:3): atts are acceptable. Next payload
                                is 0
Oct 27 22:21:05.190: ISAKMP (0:3): Input = IKE_MSG_INTERNAL, IKE_PROCESS_MAIN_MODE
                                Oct 27 22:21:05.190: ISAKMP (0:3): Old State = IKE_I_MM2 New
                                State = IKE_I_MM2
                                .Oct 27 22:21:05.202: ISAKMP (0:3): sending packet to 172.16.172.35
                                I) MM_SA_SETUP)
Oct 27 22:21:05.202: ISAKMP (0:3): Input = IKE_MSG_INTERNAL, IKE_PROCESS_COMPLETE
                                Oct 27 22:21:05.202: ISAKMP (0:3): Old State = IKE_I_MM2 New
                                State = IKE_I_MM3
                                Oct 27 22:21:05.338: ISAKMP (0:3): received packet from 172.16.172.35
                                I) MM_SA_SETUP)
Oct 27 22:21:05.342: ISAKMP (0:3): Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH
                                Oct 27 22:21:05.342: ISAKMP (0:3): Old State = IKE_I_MM3 New
                                State = IKE_I_MM4
                                Oct 27 22:21:05.342: ISAKMP (0:3): processing KE payload. message ID
                                0 =
                                Oct 27 22:21:05.466: ISAKMP (0:3): processing NONCE payload. message
                                ID = 0
                                Oct 27 22:21:05.490: ISAKMP (0:3): SKEYID state generated
Oct 27 22:21:05.490: ISAKMP (0:3): processing CERT_REQ payload. message
                                ID = 0
                                Oct 27 22:21:05.490: ISAKMP (0:3): peer wants a CT_X509_SIGNATURE cert
                                ,Oct 27 22:21:05.494: ISAKMP (0:3): peer want cert issued by CN = vpn
                                OU = cisco, O = tac, L = san jose, ST = california, C = US
Oct 27 22:21:05.498: ISAKMP (0:3): processing CERT_REQ payload. message
                                ID = 0
                                Oct 27 22:21:05.498: ISAKMP (0:3): peer wants a CT_X509_SIGNATURE cert
                                Oct 27 22:21:05.502: ISAKMP (0:3): peer want
                                ,cert issued by CN = SJVPNTAC-CAServer, OU = TAC-VPN-SJ, O = Cisco Systems
                                L = San Jose, ST = CA, C = US
                                Oct 27 22:21:05.506: ISAKMP (0:3): Choosing
                                trustpoint caserver1 as issuer
                                Oct 27 22:21:05.506: ISAKMP (0:3): processing vendor id payload
                                Oct 27 22:21:05.506: ISAKMP (0:3): vendor ID is Unity
                                Oct 27 22:21:05.510: ISAKMP (0:3): processing vendor id payload
                                Oct 27 22:21:05.510: ISAKMP (0:3): vendor ID is DPD
                                Oct 27 22:21:05.510: ISAKMP (0:3): processing vendor id payload
                                !Oct 27 22:21:05.510: ISAKMP (0:3): speaking to another IOS box
                                Oct 27 22:21:05.510: ISAKMP (0:3): processing vendor id payload
                                !!!Oct 27 22:21:05.510: I
                                Success rate is 60 percent (3/5), round-trip min/avg/max = 4/5/8 ms
                                1720-1#SAKMP (0:3): Input = IKE_MSG_INTERNAL, IKE_PROCESS_MAIN_MODE
                                Oct 27 22:21:05.510: ISAKMP (0:3): Old State = IKE_I_MM4 New
                                State = IKE_I_MM4
                                Oct 27 22:21:05.514: ISAKMP (0:3): Send initial contact
Oct 27 22:21:05.514: ISAKMP (0:3): SA is doing RSA signature authentication
                                using id type ID_FQDN
                                Oct 27 22:21:05.514: ISAKMP (3): ID payload
                                next-payload : 6
                                type
                                2 :
                                protocol
                                17 :
                                port
                                500 :
                                length

```

18 :

Oct 27 22:21:05.514: ISAKMP (3): Total payload length: 22  
Oct 27 22:21:05.530: ISKAMP: growing send buffer from 1024 to 3072  
Oct 27 22:21:05.538: ISAKMP (0:3): using the caserver1 trustpoint's  
keypair to sign  
Oct 27 22:21:05.870: ISAKMP (0:3): sending packet to 172.16.172.35  
I) MM\_KEY\_EXCH)  
Oct 27 22:21:05.870: ISAKMP (0:3): Input = IKE\_MSG\_INTERNAL, IKE\_PROCESS\_COMPLETE  
Oct 27 22:21:05.874: ISAKMP (0:3): Old State = IKE\_I\_MM4 New  
State = IKE\_I\_MM5  
Oct 27 22:21:06.630: ISAKMP (0:3): received packet from 172.16.172.35  
I) MM\_KEY\_EXCH)  
Oct 27 22:21:06.638: ISAKMP (0:3): Input = IKE\_MSG\_FROM\_PEER, IKE\_MM\_EXCH  
Oct 27 22:21:06.638: ISAKMP (0:3): Old State = IKE\_I\_MM5 New  
State = IKE\_I\_MM6  
Oct 27 22:21:06.638: ISAKMP (0:3): processing ID payload. message ID  
0 =  
Oct 27 22:21:06.638: ISAKMP (0:3): processing CERT payload. message  
ID = 0  
Oct 27 22:21:06.638: ISAKMP (0:3): processing a CT\_X509\_SIGNATURE cert  
Oct 27 22:21:06.670: ISAKMP (0:3): peer's pubkey isn't cached  
Oct 27 22:21:06.714: ISAKMP (0:3): cert approved with warning  
Oct 27 22:21:06.762: ISAKMP (0:3): **OU = PARIS**  
-----> **O=FRANCE**  
The certificate subject name from 2621-VPN router  
Oct 27 22:21:06.794: ISAKMP (0:3): processing SIG payload. message  
ID = 0  
Oct 27 22:21:06.794: ISAKMP (3): **sa->peer.name**  
**sa->peer\_id.id.id\_fqdn.fqdn = 2611-vpn.cisco.com , =**  
Oct 27 22:21:06.818: ISAKMP (0:3): SA has been  
**authenticated with 172.16.172.35**  
Oct 27 22:21:06.822: ISAKMP (0:3): Input = IKE\_MSG\_INTERNAL, IKE\_PROCESS\_MAIN\_MODE  
Oct 27 22:21:06.822: ISAKMP (0:3): Old State = IKE\_I\_MM6 New  
State = IKE\_I\_MM6  
Oct 27 22:21:06.822: ISAKMP (0:3): Input = IKE\_MSG\_INTERNAL, IKE\_PROCESS\_COMPLETE  
Oct 27 22:21:06.826: ISAKMP (0:3): Old State = IKE\_I\_MM6 New  
State = IKE\_P1\_COMPLETE  
Oct 27 22:21:06.826: ISAKMP (0:3): beginning Quick Mode exchange, M-ID  
of -2090109070  
Oct 27 22:21:06.834: ISAKMP (0:3): sending packet to 172.16.172.35  
I) QM\_IDLE)  
,Oct 27 22:21:06.838: ISAKMP (0:3): Node -2090109070, Input = IKE\_MSG\_INTERNAL  
IKE\_INIT\_QM  
Oct 27 22:21:06.838: ISAKMP (0:3): Old State = IKE\_QM\_READY New  
State = IKE\_QM\_I\_QM1  
Oct 27 22:21:06.838: ISAKMP (0:3): Input = IKE\_MSG\_INTERNAL, IKE\_PHASE1\_COMPLETE  
Oct 27 22:21:06.838: ISAKMP (0:3): Old State = IKE\_P1\_COMPLETE  
New State = IKE\_P1\_COMPLETE  
Oct 27 22:21:07.162: ISAKMP (0:3): received packet from 172.16.172.35  
I) QM\_IDLE)  
Oct 27 22:21:07.174: ISAKMP (0:3): processing HASH payload. message  
ID = -2090109070  
Oct 27 22:21:07.174: ISAKMP (0:3): processing SA payload. message ID  
-2090109070 =  
Oct 27 22:21:07.174: ISAKMP (0:3): Checking IPsec proposal 1  
Oct 27 22:21:07.174: ISAKMP: transform 1, ESP\_DES  
:Oct 27 22:21:07.174: ISAKMP: attributes in transform  
Oct 27 22:21:07.174: ISAKMP: encaps is  
1  
Oct 27 22:21:07.174: ISAKMP: SA life  
type in seconds  
Oct 27 22:21:07.174: ISAKMP: SA life  
duration (basic) of 3600  
Oct 27 22:21:07.174: ISAKMP: SA life

```
type in kilobytes
Oct 27 22:21:07.178: ISAKMP: SA life
duration (VPI) of 0x0 0x46 0x50 0x0
Oct 27 22:21:07.178: ISAKMP: authenticator
is HMAC-MD5
.Oct 27 22:21:07.178: ISAKMP (0:3): atts are acceptable
Oct 27 22:21:07.178: IPSEC(validate_proposal_request): proposal part
,#1
,key eng. msg.) INBOUND local= 172.16.172.45, remote= 172.16.172.35)
,(local_proxy= 20.1.1.0/255.255.255.0/0/0 (type=4
,(remote_proxy= 192.168.4.0/255.255.255.0/0/0 (type=4
, protocol= ESP, transform= esp-des esp-md5-hmac
,lifedur= 0s and 0kb
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
Oct 27 22:21:07.182: ISAKMP (0:3): processing NONCE payload. message
ID = -2090109070
Oct 27 22:21:07.182: ISAKMP (0:3): processing ID payload. message ID
-2090109070 =
Oct 27 22:21:07.182: ISAKMP (0:3): processing ID payload. message ID
-2090109070 =
Oct 27 22:21:07.230: ISAKMP (0:3): Creating IPsec SAs
:Oct 27 22:21:07.230
inbound SA from 172.16.172.35 to 172.16.172.45
(proxy 192.168.4.0 to 20.1.1.0)
:Oct 27 22:21:07.230
has spi 0x219DD6FD and conn_id 200 and flags 4
:Oct 27 22:21:07.234
lifetime of 3600 seconds
:Oct 27 22:21:07.234
lifetime of 4608000 kilobytes
:Oct 27 22:21:07.234
outbound SA from 172.16.172.45 to 172.16.172.35
proxy 20.1.1.0 to 192.168.4.0)
(
:Oct 27 22:21:07.234
has spi -1343930931 and conn_id 201 and flags C
:Oct 27 22:21:07.234
lifetime of 3600 seconds
:Oct 27 22:21:07.234
lifetime of 4608000 kilobytes
...Oct 27 22:21:07.234: IPSEC(key_engine): got a queue event
, :(Oct 27 22:21:07.234: IPSEC(initialize_sas
,key eng. msg.) INBOUND local= 172.16.172.45, remote= 172.16.172.35)
,(local_proxy= 20.1.1.0/255.255.255.0/0/0 (type=4
,(remote_proxy= 192.168.4.0/255.255.255.0/0/0 (type=4
, protocol= ESP, transform= esp-des esp-md5-hmac
,lifedur= 3600s and 4608000kb
=spi= 0x219DD6FD(563992317), conn_id= 200, keysize
flags= 0x4 , 0
, :(Oct 27 22:21:07.238: IPSEC(initialize_sas
,key eng. msg.) OUTBOUND local= 172.16.172.45, remote= 172.16.172.35)
,(local_proxy= 20.1.1.0/255.255.255.0/0/0 (type=4
,(remote_proxy= 192.168.4.0/255.255.255.0/0/0 (type=4
, protocol= ESP, transform= esp-des esp-md5-hmac
,lifedur= 3600s and 4608000kb
=spi= 0xAFE53DCD(2951036365), conn_id= 201, keysize
flags= 0xC , 0
,Oct 27 22:21:07.238: IPSEC(create_sa): sa created
,(sa sa_dest= 172.16.172.45, sa_prot= 50)
,(sa_spi= 0x219DD6FD(563992317
sa_trans= esp-des esp-md5-hmac , sa_conn_id= 200
,Oct 27 22:21:07.242: IPSEC(create_sa): sa created
,(sa sa_dest= 172.16.172.35, sa_prot= 50)
,(sa_spi= 0xAFE53DCD(2951036365
```

```

sa_trans= esp-des esp-md5-hmac , sa_conn_id= 201
Oct 27 22:21:07.246: ISAKMP (0:3): sending packet to 172.16.172.35
                                I) QM_IDLE)
Oct 27 22:21:07.246: ISAKMP (0:3): deleting node -2090109070 error
                                " FALSE reason
,Oct 27 22:21:07.246: ISAKMP (0:3): Node -2090109070, Input = IKE_MSG_FROM_PEER
                                IKE_QM_EXCH
Oct 27 22:21:07.246: ISAKMP (0:3): Old State = IKE_QM_I_QM1 New
                                State = IKE_QM_PHASE2_COMPLETE
Oct 27 22:21:07.710: ISAKMP (0:2): purging SA., sa=8182AB8C, delme=8182AB8C

```

```

1720-1# show crypto map 1720-1#
Crypto Map "vpn" 10 ipsec-isakmp
Peer = 172.16.172.35
Extended IP access list
102

```

```

access-list 102 permit ip 20.1.1.0 0.0.0.255 192.168.4.0 0.0.0.255
Current peer: 172.16.172.35
:Security association lifetime
kilobytes/3600 seconds 4608000
PFS (Y/N): N
,Transform sets={ myset
{
Interfaces using crypto
:map vpn

```

```

1720-1#show crypto en conn ac
Oct 27 22:21:57.246: ISAKMP (0:3): purging node -2090109070onn ac
ID Interface IP-Address
State Algorithm
Encrypt Decrypt
<none> 3
none> set>
HMAC_MD5+DES_56_CB
0 0
FastEthernet0 172.16.172.45 set 200
HMAC_MD5+DES_56_CB
8 0
FastEthernet0 172.16.172.45 set 201
HMAC_MD5+DES_56_CB
0 8

```

```

1720-1#show crypto isa sa
dst
src
state conn-id
slot
QM_IDLE 172.16.172.45 172.16.172.35
0 3

```

```

1720-1#show crypto ipsec sa
interface: FastEthernet0
Crypto map tag: vpn, local addr. 172.16.172.45
(local ident (addr/mask/prot/port): (20.1.1.0/255.255.255.0/0/0
(remote ident (addr/mask/prot/port): (192.168.4.0/255.255.255.0/0/0
current_peer: 172.16.172.35
{,PERMIT, flags={origin_is_acl
pkts encaps: 8, #pkts encrypt: 8, #pkts digest#
8
pkts decaps: 8, #pkts decrypt: 8, #pkts verify#
8
pkts compressed: 0, #pkts decompressed: 0#
,pkts not compressed: 0, #pkts compr. failed: 0#

```

```

pkts decompress failed: 0#
send errors 2, #recv errors 0#
local crypto endpt.: 172.16.172.45, remote
crypto endpt.: 172.16.172.35
path mtu 1500, media mtu 1500
current outbound spi: AFE53DCD
:inbound esp sas
(spi: 0x219DD6FD(563992317
transform: esp-des esp-md5-hmac
,
,in use settings ={Tunnel
{
:slot: 0, conn id: 200, flow_id
crypto map: vpn ,1
(sa timing: remaining key lifetime (k/sec): (4607998/3530
IV size: 8 bytes
:replay detection support
Y
:inbound ah sas
:inbound pcp sas
:outbound esp sas
(spi: 0xAFE53DCD(2951036365
transform: esp-des esp-md5-hmac
,
,in use settings ={Tunnel
{
:slot: 0, conn id: 201, flow_id
crypto map: vpn ,2
sa timing: remaining key
(lifetime (k/sec): (4607998/3521
IV size: 8 bytes
:replay detection support
Y
:outbound ah sas
:outbound pcp sas
1720-1#
1720-1#

```

يوضح هذا الإخراج تصحيح أخطاء IKE/ IPsec على الموجه 1-7204 باستخدام أوامر **show crypto** التي تبدأ بنفق IPsec إلى موجه VPN-2611.

```

, : (Oct 27 05:24:23: IPSEC(sa_request
,key eng. msg.) OUTBOUND local= 172.16.172.51, remote= 172.16.172.35)
,(local_proxy= 3.3.3.0/255.255.255.0/0/0 (type=4
,(remote_proxy= 192.168.4.0/255.255.255.0/0/0 (type=4
, protocol= ESP, transform= esp-des esp-md5-hmac
,lifedur= 3600s and 4608000kb
=spi= 0xD1025DB1(3506593201), conn_id= 0, keysize
flags= 0x400C ,0
(Oct 27 05:24:23: ISAKMP: received ke message (1/1
Oct 27 05:24:23: ISAKMP: local port 500, remote port 500
Oct 27 05:24:23: ISAKMP (0:1): Input = IKE_MSG_FROM_IPSEC, IKE_SA_REQ_MM
Oct 27 05:24:23: ISAKMP (0:1): Old State = IKE_READY New State
IKE_I_MM1 =
Oct 27 05:24:23: ISAKMP (0:1): beginning Main Mode exchange
(Oct 27 05:24:23: ISAKMP (0:1): sending packet to 172.16.172.35 (I
MM_NO_STATE
(Oct 27 05:24:23: ISAKMP (0:1): received packet from 172.16.172.35 (I
MM_NO_STATE
Oct 27 05:24:23: ISAKMP (0:1): Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH
Oct 27 05:24:23: ISAKMP (0:1): Old State = IKE_I_MM1 New State
IKE_I_MM2 =

```

Oct 27 05:24:23: ISAKMP (0:1): processing SA payload. message ID = 0  
Oct 27 05:24:23: ISAKMP (0:1): Checking ISAKMP transform 1 against  
priority 10 policy  
Oct 27 05:24:23: ISAKMP: encryption DES-CBC  
Oct 27 05:24:23: ISAKMP: hash MD5  
Oct 27 05:24:23: ISAKMP: default group  
1  
Oct 27 05:24:23: ISAKMP: auth RSA sig  
Oct 27 05:24:23: ISAKMP: life type in  
seconds  
Oct 27 05:24:23: ISAKMP: life duration  
VPI) of 0x0 0x1 0x51 0x80)  
Oct 27 05:24:23: ISAKMP (0:1): atts are acceptable. Next payload is  
0  
Oct 27 05:24:23: ISAKMP (0:1): Input = IKE\_MSG\_INTERNAL, IKE\_PROCESS\_MAIN\_MODE  
!!!!.Oct 27  
Success rate is 80 percent (4/5), round-trip min/avg/max = 4/8/16 ms  
ISAKMP (0:1): Old State = IKE\_I\_MM2 New State :05:24:23 7204-1#  
IKE\_I\_MM2 =

Oct 27 05:24:23: ISAKMP (0:1): sending packet to 172.16.172.35 (I) MM\_SA\_SETUP  
Oct 27 05:24:23: ISAKMP (0:1): Input = IKE\_MSG\_INTERNAL, IKE\_PROCESS\_COMPLETE  
Oct 27 05:24:23: ISAKMP (0:1): Old State = IKE\_I\_MM2 New State  
IKE\_I\_MM3 =

(Oct 27 05:24:23: ISAKMP (0:1): received packet from 172.16.172.35 (I  
MM\_SA\_SETUP  
Oct 27 05:24:23: ISAKMP (0:1): Input = IKE\_MSG\_FROM\_PEER, IKE\_MM\_EXCH  
Oct 27 05:24:23: ISAKMP (0:1): Old State = IKE\_I\_MM3 New State  
IKE\_I\_MM4 =

Oct 27 05:24:23: ISAKMP (0:1): processing KE payload. message ID = 0  
Oct 27 05:24:23: ISAKMP (0:1): processing NONCE payload. message ID  
0 =  
Oct 27 05:24:23: ISAKMP (0:1): SKEYID state generated  
Oct 27 05:24:23: ISAKMP (0:1): processing CERT\_REQ payload. message  
ID = 0  
Oct 27 05:24:23: ISAKMP (0:1): peer wants a CT\_X509\_SIGNATURE cert  
Oct 27 05:24:23: ISAKMP (0:1): **peer want cert**  
**, issued by CN = vpn, OU = cisco, O = tac, L = san jose, ST = california**  
**C = US**  
Oct 27 05:24:23: CRYPTO\_PKI: **Trust-Point caserver2**  
**picked up**  
Oct 27 05:24:23: ISAKMP (0:1): **Choosing trustpoint**  
**caserver2 as issuer**  
Oct 27 05:24:23: ISAKMP (0:1): processing CERT\_REQ payload. message  
ID = 0  
Oct 27 05:24:23: ISAKMP (0:1): peer wants a CT\_X509\_SIGNATURE cert  
Oct 27 05:24:23: ISAKMP (0:1): **peer want cert**  
**issued by CN = SJPNTAC-CAServer, OU = TAC-VPN-SJ, O = Cisco Systems, L**  
**San Jose, ST = CA, C = US =**  
Oct 27 05:24:23: ISAKMP (0:1): processing vendor id payload  
Oct 27 05:24:23: ISAKMP (0:1): vendor ID is Unity  
Oct 27 05:24:23: ISAKMP (0:1): processing vendor id payload  
Oct 27 05:24:23: ISAKMP (0:1): vendor ID is DPD  
Oct 27 05:24:23: ISAKMP (0:1): processing vendor id payload  
!Oct 27 05:24:23: ISAKMP (0:1): speaking to another IOS box  
Oct 27 05:24:23: ISAKMP (0:1): processing vendor id payload  
Oct 27 05:24:23: ISAKMP (0:1): Input = IKE\_MSG\_INTERNAL, IKE\_PROCESS\_MAIN\_MODE

```
Oct 27 05:24:23: ISAKMP (0:1): Old State = IKE_I_MM4 New State
                                         IKE_I_MM4 =

Oct 27 05:24:23: ISAKMP (0:1): Send initial contact
Oct 27 05:24:23: ISAKMP (0:1): SA is doing RSA signature authentication
                                         using id type ID_FQDN
Oct 27 05:24:23: ISAKMP (1): ID payload
                                         next-payload : 6
                                         type
                                         2 :
                                         protocol
                                         17 :
                                         port
                                         500 :
                                         length
                                         20 :
Oct 27 05:24:23: ISAKMP (1): Total payload length: 24
Oct 27 05:24:23: ISAKMP (0:1): using the caserver2 trustpoint's keypair
                                         to sign
Oct 27 05:24:23: ISKAMP: growing send buffer from 1024 to 3072
(Oct 27 05:24:23: ISAKMP (0:1): sending packet to 172.16.172.35 (I
                                         MM_KEY_EXCH
Oct 27 05:24:23: ISAKMP (0:1): Input = IKE_MSG_INTERNAL, IKE_PROCESS_COMPLETE
Oct 27 05:24:23: ISAKMP (0:1): Old State = IKE_I_MM4 New State
                                         IKE_I_MM5 =

(Oct 27 05:24:24: ISAKMP (0:1): received packet from 172.16.172.35 (I
                                         MM_KEY_EXCH
Oct 27 05:24:24: ISAKMP (0:1): Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH
Oct 27 05:24:24: ISAKMP (0:1): Old State = IKE_I_MM5 New State
                                         IKE_I_MM6 =

Oct 27 05:24:24: ISAKMP (0:1): processing ID payload. message ID = 0
Oct 27 05:24:24: ISAKMP (0:1): processing CERT payload. message ID
                                         0 =
Oct 27 05:24:24: ISAKMP (0:1): processing a CT_X509_SIGNATURE cert
Oct 27 05:24:24: ISAKMP (0:1): peer's pubkey isn't cached
Oct 27 05:24:24: CRYPTO_PKI: WARNING: Certificate, private key or CRL
                                         was not found while selecting CRL

.Oct 27 05:24:24: CRYPTO_PKI: cert revocation status unknown
The subject name of the certificate from the 2611-VPN router !--- obtained from CA server2. ---!
Oct 27 05:24:24: ISAKMP (0:1): cert approved with warning
Oct 27 05:24:24: ISAKMP (0:1): OU = ROME O=ITALY

Oct 27 05:24:24: ISAKMP (0:1): processing SIG payload. message ID = 0
Oct 27 05:24:24: ISAKMP (1): sa->peer.name
                                         sa->peer_id.id.id_fqdn.fqdn = 2611-vpn.cisco.com , =
Oct 27 05:24:24: ISAKMP (0:1): SA has been authenticated with 172.16.172.35
Oct 27 05:24:24: ISAKMP (0:1): Input = IKE_MSG_INTERNAL, IKE_PROCESS_MAIN_MODE
Oct 27 05:24:24: ISAKMP (0:1): Old State = IKE_I_MM6 New State
                                         IKE_I_MM6 =

Oct 27 05:24:24: ISAKMP (0:1): Input = IKE_MSG_INTERNAL, IKE_PROCESS_COMPLETE
Oct 27 05:24:24: ISAKMP (0:1): Old State = IKE_I_MM6 New State
                                         IKE_P1_COMPLETE =

Oct 27 05:24:24: ISAKMP (0:1): beginning Quick Mode exchange, M-ID of
```



```
1631242332
(Oct 27 05:24:24: ISAKMP (0:1): sending packet to 172.16.172.35 (I
QM_IDLE
,Oct 27 05:24:24: ISAKMP (0:1): Node 1631242332, Input = IKE_MSG_INTERNAL
IKE_INIT_QM

Oct 27 05:24:24: ISAKMP (0:1): Old State = IKE_QM_READY New State
IKE_QM_I_QM1 =

Oct 27 05:24:24: ISAKMP (0:1): Input = IKE_MSG_INTERNAL, IKE_PHASE1_COMPLETE
Oct 27 05:24:24: ISAKMP (0:1): Old State = IKE_P1_COMPLETE New
State = IKE_P1_COMPLETE

(Oct 27 05:24:24: ISAKMP (0:1): received packet from 172.16.172.35 (I
QM_IDLE
Oct 27 05:24:24: ISAKMP (0:1): processing HASH payload. message ID
1631242332 =
= Oct 27 05:24:24: ISAKMP (0:1): processing SA payload. message ID
1631242332
Oct 27 05:24:24: ISAKMP (0:1): Checking IPsec proposal 1
Oct 27 05:24:24: ISAKMP: transform 1, ESP_DES
:Oct 27 05:24:24: ISAKMP: attributes in transform
Oct 27 05:24:24: ISAKMP: encaps is 1
Oct 27 05:24:24: ISAKMP: SA life type
in seconds
Oct 27 05:24:24: ISAKMP: SA life duration
basic) of 3600)
Oct 27 05:24:24: ISAKMP: SA life type
in kilobytes
Oct 27 05:24:24: ISAKMP: SA life duration
VPI) of 0x0 0x46 0x50 0x0)
Oct 27 05:24:24: ISAKMP: authenticator
is HMAC-MD5
.Oct 27 05:24:24: ISAKMP (0:1): atts are acceptable
,Oct 27 05:24:24: IPSEC(validate_proposal_request): proposal part #1
,key eng. msg.) INBOUND local= 172.16.172.51, remote= 172.16.172.35)
,(local_proxy= 3.3.3.0/255.255.255.0/0/0 (type=4
,(remote_proxy= 192.168.4.0/255.255.255.0/0/0 (type=4
, protocol= ESP, transform= esp-des esp-md5-hmac
,lifedur= 0s and 0kb
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
Oct 27 05:24:24: ISAKMP (0:1): processing NONCE payload. message ID
1631242332 =
= Oct 27 05:24:24: ISAKMP (0:1): processing ID payload. message ID
1631242332
= Oct 27 05:24:24: ISAKMP (0:1): processing ID payload. message ID
1631242332
Oct 27 05:24:24: ISAKMP (0:1): Creating IPsec SAs
Oct 27 05:24:24: inbound
SA from 172.16.172.35 to 172.16.172.51
(proxy 192.168.4.0 to 3.3.3.0)
Oct 27 05:24:24: has
spi 0xD1025DB1 and conn_id 2000 and flags 4
Oct 27 05:24:24: lifetime
of 3600 seconds
Oct 27 05:24:24: lifetime
of 4608000 kilobytes
Oct 27 05:24:24: outbound
SA from 172.16.172.51 to 172.16.172.35 (proxy 3.3.3.0
( to 192.168.4.0
Oct 27 05:24:24: has
```

```
spi -929016560 and conn_id 2001 and flags C
Oct 27 05:24:24: lifetime
of 3600 seconds
Oct 27 05:24:24: lifetime
of 4608000 kilobytes
(Oct 27 05:24:24: ISAKMP (0:1): sending packet to 172.16.172.35 (I
QM_IDLE
Oct 27 05:24:24: ISAKMP (0:1): deleting node 1631242332 error FALSE
" " reason
,Oct 27 05:24:24: ISAKMP (0:1): Node 1631242332, Input = IKE_MSG_FROM_PEER
IKE_QM_EXCH
```

```
Oct 27 05:24:24: ISAKMP (0:1): Old State = IKE_QM_I_QM1 New State
IKE_QM_PHASE2_COMPLETE =
```

```
...Oct 27 05:24:24: IPSEC(key_engine): got a queue event
, : (Oct 27 05:24:24: IPSEC(initialize_sas
,key eng. msg.) INBOUND local= 172.16.172.51, remote= 172.16.172.35)
,(local_proxy= 3.3.3.0/255.255.255.0/0/0 (type=4
,(remote_proxy= 192.168.4.0/255.255.255.0/0/0 (type=4
, protocol= ESP, transform= esp-des esp-md5-hmac
,lifedur= 3600s and 4608000kb
=spi= 0xD1025DB1(3506593201), conn_id= 2000, keysize
flags= 0x4 ,0
, : (Oct 27 05:24:24: IPSEC(initialize_sas
,key eng. msg.) OUTBOUND local= 172.16.172.51, remote= 172.16.172.35)
,(local_proxy= 3.3.3.0/255.255.255.0/0/0 (type=4
,(remote_proxy= 192.168.4.0/255.255.255.0/0/0 (type=4
, protocol= ESP, transform= esp-des esp-md5-hmac
,lifedur= 3600s and 4608000kb
=spi= 0xC8A05510(3365950736), conn_id= 2001, keysize
flags= 0xC ,0
,Oct 27 05:24:24: IPSEC(create_sa): sa created
,sa) sa_dest= 172.16.172.51, sa_prot= 50)
,(sa_spi= 0xD1025DB1(3506593201
sa_trans= esp-des esp-md5-hmac , sa_conn_id= 2000
,Oct 27 05:24:24: IPSEC(create_sa): sa created
,sa) sa_dest= 172.16.172.35, sa_prot= 50)
,(sa_spi= 0xC8A05510(3365950736
sa_trans= esp-des esp-md5-hmac , sa_conn_id= 2001
7204-1#
7204-1#
7204-1#
7204-1#
7204-1#
```

```
7204-1#show crypto isa sa
dst
src
state conn-id
slot
QM_IDLE 172.16.172.51 172.16.172.35
0 1
```

```
7204-1#show crypto en conn ac
```

```
ID Interface IP-Address
State Algorithm
Encrypt Decrypt
<none> 1
none> set>
```

```
HMAC_MD5+DES_56_CB 0
0
Ethernet1/1 172.16.172.51 2000
set HMAC_MD5+DES_56_CB
9 0
Ethernet1/1 172.16.172.51 2001
set HMAC_MD5+DES_56_CB
0 9
```

7204-1#**show crypto ipsec sa**

```
interface: Ethernet1/1
Crypto map tag: vpn, local addr. 172.16.172.51

(local ident (addr/mask/prot/port): (3.3.3.0/255.255.255.0/0/0)
(remote ident (addr/mask/prot/port): (192.168.4.0/255.255.255.0/0/0)
current_peer: 172.16.172.35
{,PERMIT, flags={origin_is_acl
pkts encaps: 13, #pkts encrypt: 13, #pkts digest#
13
pkts decaps: 13, #pkts decrypt: 13, #pkts verify#
13
pkts compressed: 0, #pkts decompressed: 0#
,pkts not compressed: 0, #pkts compr. failed: 0#
pkts decompress failed: 0#
send errors 32, #recv errors 0#

local crypto endpt.: 172.16.172.51, remote
crypto endpt.: 172.16.172.35
path mtu 1500, media mtu 1500
current outbound spi: C8A05510

:inbound esp sas
(spi: 0xD1025DB1(3506593201)
transform: esp-des esp-md5-hmac
,
,in use settings ={Tunnel
{
,slot: 0, conn id: 2000
flow_id: 1, crypto map: vpn
(sa timing: remaining key lifetime (k/sec): (4607998/3435
IV size: 8 bytes
:replay detection support
Y

:inbound ah sas

:inbound pcp sas

:outbound esp sas
(spi: 0xC8A05510(3365950736)
transform: esp-des esp-md5-hmac
,
,in use settings ={Tunnel
{
,slot: 0, conn id: 2001
```

```
flow_id: 2, crypto map: vpn
sa timing: remaining key
(lifetime (k/sec): (4607998/3435
IV size: 8 bytes
:replay detection support
Y
```

```
:outbound ah sas
```

```
:outbound pcp sas
```

```
show crypto en conf 7204-1#
```

```
:crypto engine name
unknown
:crypto engine type
software
```

```
serial number: 01691291
crypto engine state: installed
crypto engine in slot: N/A
```

```
platform: predator crypto_engine
```

```
:Encryption Process Info
input queue
size: 500
input
queue top: 26
input
queue bot: 26
:input queue count
0
```

```
:Crypto Adjacency Counts
Lock Count: 0
Unlock Count: 0
```

```
7204-1#show crypto map
Crypto Map "vpn" 10 ipsec-isakmp
Peer = 172.16.172.35
Extended IP access list
101
```

```
access-list 101 permit ip 3.3.3.0 0.0.0.255 192.168.4.0 0.0.0.255
Current peer: 172.16.172.35
:Security association lifetime
kilobytes/3600 seconds 4608000
PFS (Y/N): N
,Transform sets={ myset
{
Interfaces using crypto
:map vpn
Ethernet1/1
```

## معلومات ذات صلة

- مرجع أمر أمان Cisco IOS، الإصدار 12.2
- دليل تكوين أمان IOS، الإصدار 12.2 من Cisco
- كيفية تكوين IPsec من شبكة LAN إلى شبكة LAN بين موجه و PIX باستخدام الشهادات الرقمية
- مفاوضة IPsec/بروتوكول IKE
- الدعم التقني والمستندات - Cisco Systems

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا ذه Cisco ت مچرت  
م ل ا ل اء ان ا ع مچ ي ف ن ي م دخت س م ل ل م عد ي و ت ح م م ي دقت ل ة ي ر ش ب ل و  
امك ة ق ي ق د ن و ك ت ن ل ة ي ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ال 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 ال ا ة مچرت ل ا ع م ل ا ح ل ا و ه  
ي ل ا م اء ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا هذه 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