

# لي م ع و Cisco IOS ت ا ه ج و م ن ي ب IPsec ن ي و ك ت ن ا م ض ل ا ت ا د ا ه ش م ا د خ ت س ا ب Cisco VPN

## المحتويات

- [المقدمة](#)
- [قبل البدء](#)
- [الاصطلاحات](#)
- [المتطلبات الأساسية](#)
- [المكونات المستخدمة](#)
- [التكوين](#)
- [الرسم التخطيطي للشبكة](#)
- [التكوينات](#)
- [التحقق من الصحة](#)
- [استكشاف الأخطاء وإصلاحها](#)
- [معلومات ذات صلة](#)

## المقدمة

يوضح هذا المستند كيفية تكوين نفق IPsec VPN بين موجه Cisco IOS © و عميل Cisco VPN 3.x باستخدام شهادات Entrust. يتم دعم هذه الميزة في برنامج Cisco IOS الإصدار T(8)12.2 والإصدارات الأحدث. كما يسلط مثال التكوين في هذا المستند الضوء على إجراء تسجيل مرجع التصديق (CA) لكل من موجه Cisco IOS و عميل Cisco VPN باستخدام Entrust كخادم CA.

## قبل البدء

### الاصطلاحات

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

### المتطلبات الأساسية

لا توجد متطلبات أساسية خاصة لهذا المستند.

### المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية أدناه.

- موجه Cisco 3640 الذي يشغل برنامج Cisco IOS الإصدار T(8)12.2 (صورة -c3640-ik8o3s-mz.122 IOS: 8.T)
- Cisco VPN Client 4.0.1 على كمبيوتر يعمل بنظام التشغيل Windows 2000

• خادم Entrust CA المستخدم كخادم CA

تم إنشاء المعلومات المقدمة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كنت تعمل في شبكة مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر قبل استخدامه.

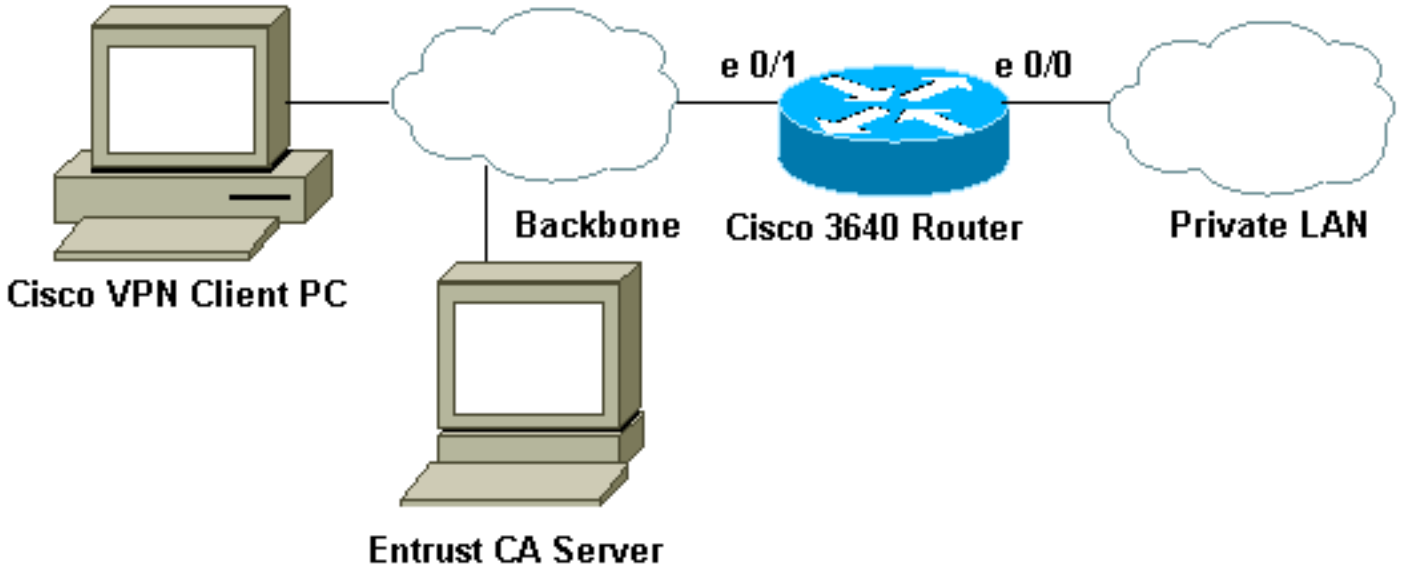
## التكوين

في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

ملاحظة: للعثور على معلومات إضافية حول الأوامر المستخدمة في هذا المستند، استخدم [أداة بحث الأوامر \(للعلماء المسجلين فقط\)](#).

## الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة الموضح في الرسم التخطيطي أدناه.



## التكوينات

يستخدم هذا المستند التكوينات الموضحة أدناه.

- [تكوينات الموجه](#)
- [تسجيل الشهادة لعمل Cisco VPN](#)
- [تكوين اتصال VPN على عمل Cisco VPN](#)

## تكوينات الموجه

- [تسجيل الشهادة على موجه IOS 3640](#)
- [تهيئة 3640](#)

### تسجيل الشهادة على موجه IOS 3640

```
Define a hostname and domain name for the router. ---!  
!--- The fully qualified domain name (FQDN) will be used
```

```

!--- as the identity of the router during certificate
enrollment. 3640(config)#ip domain-name sjpki.com
Generate RSA (encryption and authentication) keys. ---!
3640(config)#crypto key generate rsa
The name for the keys will be: 3640.sjpki.com
Choose the size of the key modulus in the range of 360
to 2048 for your
General Purpose Keys. Choosing a key modulus greater
than 512 may take
.a few minutes

:[How many bits in the modulus [512
[Generating 512 bit RSA keys ...[OK %
Define the CA identity. Note that in Cisco IOS ---!
Software !--- Release 12.2(8)T, the crypto ca trustpoint
command !--- replaces the crypto ca identity command
from previous !--- Cisco IOS versions. So that the
router will try to enroll !--- to the CA server
automatically when its certificates !--- expire, auto-
.enroll was turned on

config)#crypto ca trustpoint SJPKI)3640
ca-trustpoint)# enrollment url http://171.69.89.126)3640
ca-trustpoint)#enrollment mode ra)3640
ca-trustpoint)#crl query ldap://171.69.89.126)3640
ca-trustpoint)#serial-number none)3640
ca-trustpoint)#ip-address none)3640
ca-trustpoint)#password revokeme)3640
ca-trustpoint)#auto-enroll)3640
ca-trustpoint)#usage ike)3640
Retrieves CA and registration authority (RA) !--- ---!
certificates from the CA server. 3640(config)#crypto ca
authen SJPKI
:Certificate has the following attributes
Fingerprint: 0D8E6CF8 C63D7068 3BA4B90A 16054812
Do you accept this certificate? [yes/no]: y %
.Trustpoint CA certificate accepted
#(config)3640
Enroll to CA server and get router's own ---!
certificate. 3640(config)#crypto ca enroll SJPKI
%
.. Start certificate enrollment %

The subject name in the certificate will be: %
3640.sjpki.com
Certificate request sent to Certificate Authority %
.The certificate request fingerprint will be displayed %
The 'show crypto ca certificate' command will also %
.show the fingerprint

config)# Fingerprint: D9CE886E B4B76115)3640
B7149128 6658E7CA

CRYPTO_PKI: status = 102: certificate request :00:58:17
pending
CRYPTO_PKI: status = 102: certificate request :00:58:39
pending
CRYPTO-6-CERTRET: Certificate received from% :00:59:42
Certificate Authority

```

تهينة 3640

version 12.2

```

service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 3640
!
logging buffered 4096 debugging
Define local authentication as the authentication ---!
method !--- for Internet Key Exchange (IKE) XAUTH. !---
Note that "ClientAuth" is the tag associated with the
crypto map. aaa new-model
aaa authentication login ClientAuth local
aaa authorization network ClientAuth local
aaa session-id common
enable secret 5 $1$v49A$bfcGOfwF7qdKQqZxCIN770
!
username vpnclient password 0 cisco123
ip subnet-zero
!
!
ip domain-name sjpki.com
!
ip audit notify log
ip audit po max-events 100
!
crypto ca trustpoint SJPKI
enrollment mode ra
enrollment url http://171.69.89.126:80
usage ike
serial-number none
ip-address none
password 7 1405171D030F2F2621
crl query ldap://171.69.89.126
auto-enroll
crypto ca certificate chain SJPKI
certificate ca 3C9CC54B
308202E4 3082024D A0030201 0202043C 9CC54B30 0D06092A
864886F7 0D010105
0500302D 310B3009 06035504 06130275 73310E30 0C060355
040A1305 63697363
6F310E30 0C060355 040B1305 736A7670 6E301E17 0D303230
33323331 37343132
355A170D 32323033 32333138 31313235 5A302D31 0B300906
03550406 13027573
310E300C 06035504 0A130563 6973636F 310E300C 06035504
0B130573 6A76706E
30819F30 0D06092A 864886F7 0D010101 05000381 8D003081
89028181 00AD0B5B
DACB1B4B 6CBE7138 2A97AA1D A2D3565C 56EE74D7 32A61D4F
7FBA7E53 44A4C8CC
94E16825 99369D85 7B6F5A15 60D9AD92 8AF8800E E3E70E01
757FD5DE 470C4996
A379181A 00709FE5 9C7C5A14 959F77B1 A746F8F7 1F0077FB
99E54DAC 8F3C355F
F36E7511 EF09B23D 52CDCD2F 50E471B7 F1FFCB05 31964497
4E6EB7F4 71020301
0001A382 010F3082 010B3011 06096086 480186F8 42010104
04030200 07304F06
03551D1F 04483046 3044A042 A040A43E 303C310B 30090603
55040613 02757331
0E300C06 0355040A 13056369 73636F31 0E300C06 0355040B
1305736A 76706E31
0D300B06 03550403 13044352 4C31302B 0603551D 10042430
22800F32 30303230

```

355A810F	32303232	30333233	31383131	37343132	33323331	
				32355A30	0B060355	
1D0F0404	03020106	301F0603	551D2304	18301680	14F7931A	
				99D0E447	69928CC0	
A9FF647D	F53E627F	5A301D06	03551D0E	04160414	F7931A99	
				D0E44769	928CC0A9	
FF647DF5	3E627F5A	300C0603	551D1304	05300301	01FF301D	
				06092A86	4886F67D	
10300E1B	0856352E	303A342E	30030204	90300D06	07410004	
				092A8648	86F70D01	
3C6AB8D8	9E3F140D	D5D051AB	7032AF51	03818100	01050500	
				BD357804	4D7FA32C	
EB42D1EA	2AFA1EEF	548C175E	FAB9B4C7	DE0E0744	0916FC71	
				B87768F3	28B605E9	
A054900B	5E249835	3112E7FF	F0B579F5	F06858F8	5940CA9C	
				E0FC4E98	66C50A40	
2ABEAF37	9DB339C0	F98EDC0C	E28C82CD	B2465D46	5E3AB18E	
				0FEEE09A	37D58506	
				72AE135E	3B48662D	
					quit	
				certificate ra-encrypt	3C9CC573	
308202E1	3082024A	A0030201	0202043C	9CC57330	0D06092A	
				864886F7	0D010105	
0500302D	310B3009	06035504	06130275	73310E30	0C060355	
				040A1305	63697363	
6F310E30	0C060355	040B1305	736A7670	6E301E17	0D303230	
				33323332	32353234	
355A170D	30353033	32333233	32323435	5A305631	0B300906	
				03550406	13027573	
310E300C	06035504	0A130563	6973636F	310E300C	06035504	
				0B130573	6A76706E	
03131E65	6E747275	73745650	4E636F6E	06035504	31273025	
				6E656374	6F722045	
6E747275	7374504B	4930819F	300D0609	2A864886	F70D0101	
				01050003	818D0030	
8100AC0B	BA3BC6CF	7C303853	C1C191F6	5CD91A41	81890281	
				2F6143B4	6662D7CB	
A4CD6633	45DBAEC7	7664F88B	D62C5DA9	6087C097	5F498BF5	
				3DDC7ACF	1F4BFA30	
DA112550	841FC5AD	45AEEE65	EA1EB935	473BF5F4	3F6FDE88	
				E05D7097	FD8C4525	
50ECE9F7	4B3EA152	ODDB8867	A7DB5FEB	D7886405	4DCB7486	
				9D8E1E96	5E3495D8	
989017F1	CA7D0203	010001A3	81E43081	E1300B06	03551D0F	
				04040302	0520301B	
0603551D	09041430	12301006	092A8648	86F67D07	441D3103	
				02010130	4F060355	
1D1F0448	30463044	A042A040	A43E303C	310B3009	06035504	
				06130275	73310E30	
0C060355	040A1305	63697363	6F310E30	0C060355	040B1305	
				736A7670	6E310D30	
0B060355	04031304	43524C31	301F0603	551D2304	18301680	
				14F7931A	99D0E447	
69928CC0	A9FF647D	F53E627F	5A301D06	03551D0E	04160414	
				2DDB5231	39027684	
9C982D0D	E4528CBC	CFFB97B3	30090603	551D1304	02300030	
				1906092A	864886F6	
7D074100	040C300A	1B045635	2E300302	04B0300D	06092A86	
				4886F70D	01010505	
001423E0	A88F4F28	FF69BD65	F35FDCD7	BELACB2C	00038181	
				9AF076CD	407D2698	
D9237E02	2026B349	799BD983	C6FE9EB1	41E3728A	0FB37EE2	
				E0CE0071	6194EDF8	
D21A9DED	A7372E20	6FFE0468	014ED8EB	018FBB96	A683B210	

```

A32C0673 D2C2785A
818C8EC8 2B9549EF 356C96BF 8F396064 1F6D7B50 D3354171
ACA45AE7 D550F42A
30922C78 E6
quit
certificate ra-sign 3C9CC574
A0030201 0202043C 9CC57430 0D06092A 30820279 30820310
864886F7 0D010105
0500302D 310B3009 06035504 06130275 73310E30 0C060355
040A1305 63697363
6F310E30 0C060355 040B1305 736A7670 6E301E17 0D303230
33323332 32353234
355A170D 30353033 32333233 32323435 5A305631 0B300906
03550406 13027573
310E300C 06035504 0A130563 6973636F 310E300C 06035504
0B130573 6A76706E
03131E65 6E747275 73745650 4E636F6E 06035504 31273025
6E656374 6F722045
6E747275 7374504B 4930819F 300D0609 2A864886 F70D0101
01050003 818D0030
8100AC87 EF7C0E8E 2120B81F D231EE87 78CB4238 81890281
9F5E5F3B D1D1C9F7
B35993EF 7118104A 26C38AB4 7DDE9B1D 3A685A73 9788A221
AC3199D7 0D91D315
2276DAF7 F58C5A1C 690B3CC8 7C1CBE03 8BD81993 F4644D30
B3388741 A0A0C4FC
BA469358 08C39FA0 152424F9 6E55651C 565B024C A862F557
85D925AA 6074959A
AC8E934B 48090203 010001A3 82011230 82010E30 0B060355
1D0F0404 03020780
302B0603 551D1004 24302280 0F323030 32303332 33323235
3234355A 810F3230
5A301B06 03551D09 04143012 32323435 32393033 30343034
30100609 2A864886
F67D0744 1D310302 0101304F 0603551D 1F044830 463044A0
42A040A4 3E303C31
0B300906 03550406 13027573 310E300C 06035504 0A130563
6973636F 310E300C
0B130573 6A76706E 310D300B 06035504 03130443 06035504
524C3130 1F060355
1D230418 30168014 F7931A99 D0E44769 928CC0A9 FF647DF5
3E627F5A 301D0603
551D0E04 160414AA 2E19FD77 6824DE9B 41DB46FC 15229D09
48D4EF30 09060355
1D130402 30003019 06092A86 4886F67D 07410004 0C300A1B
0456352E 30030204
B0300D06 092A8648 86F70D01 01050500 03818100 9EA074F8
12D60655 181B7E4B
CEC7F891 950F22E3 83344504 CBF49334 3DB683F1 32FE454E
2C3F7B6A 6E80B7F8
5D3B29A0 06AC428B BBAA3381 4209F50C CD8A7D30 4A6842ED
6B683B94 8423E58B
B2E27650 D1104DEB 56678757 7B744187 D99955F7 DF1BCED2
849D4F9A F22CDA7C
203E19C6 125AC104 608E37DF 600F97B9 B4DCF0CE
quit
certificate 3C9CC602
308202C0 30820229 A0030201 0202043C 9CC60230 0D06092A
864886F7 0D010105
0500302D 310B3009 06035504 06130275 73310E30 0C060355
040A1305 63697363
6F310E30 0C060355 040B1305 736A7670 6E301E17 0D303230
34303832 32323534
365A170D 30333034 30383232 35353436 5A304C31 0B300906

```

```
03550406 13027573
310E300C 06035504 0A130563 6973636F 310E300C 06035504
0B130573 6A76706E
311D301B 06092A86 4886F70D 01090216 0E333634 302E736A
706B692E 636F6D30
5C300D06 092A8648 86F70D01 01010500 034B0030 48024100
B7C253B7 B915A629
3CC1514F 39F8BB0A 503D0D10 D9C95D78 106D8944 48D28864
72760A06 859DA91A
0F9304E3 9CA87FFB FA3846FA 5C798970 4D8E6203 FE701A67
02030100 01A38201
0C300B06 03551D0F 04040302 05A03019 0603551D 10308201
11041230 10820E33
3634302E 736A706B 692E636F 6D302B06 03551D10 04243022
800F3230 30323034
5A810F32 30303231 32323031 30353534 32353436 30383232
365A304F 0603551D
1F044830 463044A0 42A040A4 3E303C31 0B300906 03550406
13027573 310E300C
0A130563 6973636F 310E300C 06035504 0B130573 06035504
6A76706E 310D300B
524C3130 1F060355 1D230418 30168014 03130443 06035504
F7931A99 D0E44769
928CC0A9 FF647DF5 3E627F5A 301D0603 551D0E04 16041413
C98FDF5A AEF253F0
84D39E4B 44A10B1F A2622730 09060355 1D130402 30003019
06092A86 4886F67D
0C300A1B 0456352E 30030204 B0300D06 092A8648 07410004
86F70D01 01050500
671FC222 EADDC030 F8053380 5EEE91E5 69D3F5A7 03818100
5AC037F9 539EF9CB
25ECD678 365A954A FFD3141B 17DEEB9F 1DFE6F97 8B8FDD18
47458858 A0517D21
2EE68C30 F359C5F9 647354F8 F92F2346 B999EFB7 029F30FB
AC096829 58DC7E13
EE1FA3F6 BAAF794A 0157B0B1 4935CD3A 7B613B65 940412F8
C6301264 A7E53742 75E1E403
```

quit

*Define Internet Security Association and Key ---!  
Management !--- Protocol (ISAKMP) policy. The IKE  
authentication method !--- "rsa-sig" will be used, but  
it doesn't show up in !--- the configuration since it is  
the default method. crypto isakmp policy 1*

**group 2**

*Use FQDN as the ISAKMP identity. crypto isakmp ---!  
identity hostname !--- Define the VPN group for Cisco  
VPN Client. !--- The VPN group name "sjvpn" matches !---  
the Organizational Unit (OU) name of the client's  
certificate. !--- Access list "acl 100" defines the  
split-tunneling traffic, and !--- "vpnpool" defines the  
IP pool from which the VPN Client !--- receives its IP  
address during the IKE negotiation. crypto isakmp client*

**configuration group sjvpn**

**dns 10.1.1.5**

**wins 10.1.1.5**

**domain sjpki.com**

**pool vpnpool**

**acl 101**

!

*Define crypto map configuration. crypto ipsec --!*

**transform-set myset esp-des esp-md5-hmac**

!

**crypto dynamic-map vpnclient 10**

**set transform-set myset**

```
!
!
crypto map vpn client authentication list ClientAuth
crypto map vpn isakmp authorization list ClientAuth
crypto map vpn client configuration address respond
crypto map vpn 10 ipsec-isakmp dynamic vpnclient
!
!
!
fax interface-type fax-mail
mta receive maximum-recipients 0
!
!
interface Loopback0
ip address 10.1.2.1 255.255.255.0
!
interface Ethernet0/0
ip address 10.1.3.1 255.255.255.0
no keepalive
half-duplex
!
interface Ethernet0/1
ip address 172.16.172.40 255.255.255.240
half-duplex
crypto map vpn
!
interface BRI1/0
no ip address
shutdown
!
interface BRI1/1
no ip address
shutdown
!
interface BRI1/2
no ip address
shutdown
!
interface BRI1/3
no ip address
shutdown
!
interface Serial2/0
no ip address
shutdown
no fair-queue
!
interface Serial2/1
no ip address
shutdown
!
interface Serial2/2
no ip address
shutdown
!
interface Serial2/3
no ip address
shutdown
!
interface Serial3/0
no ip address
shutdown
!
interface Serial3/1
```

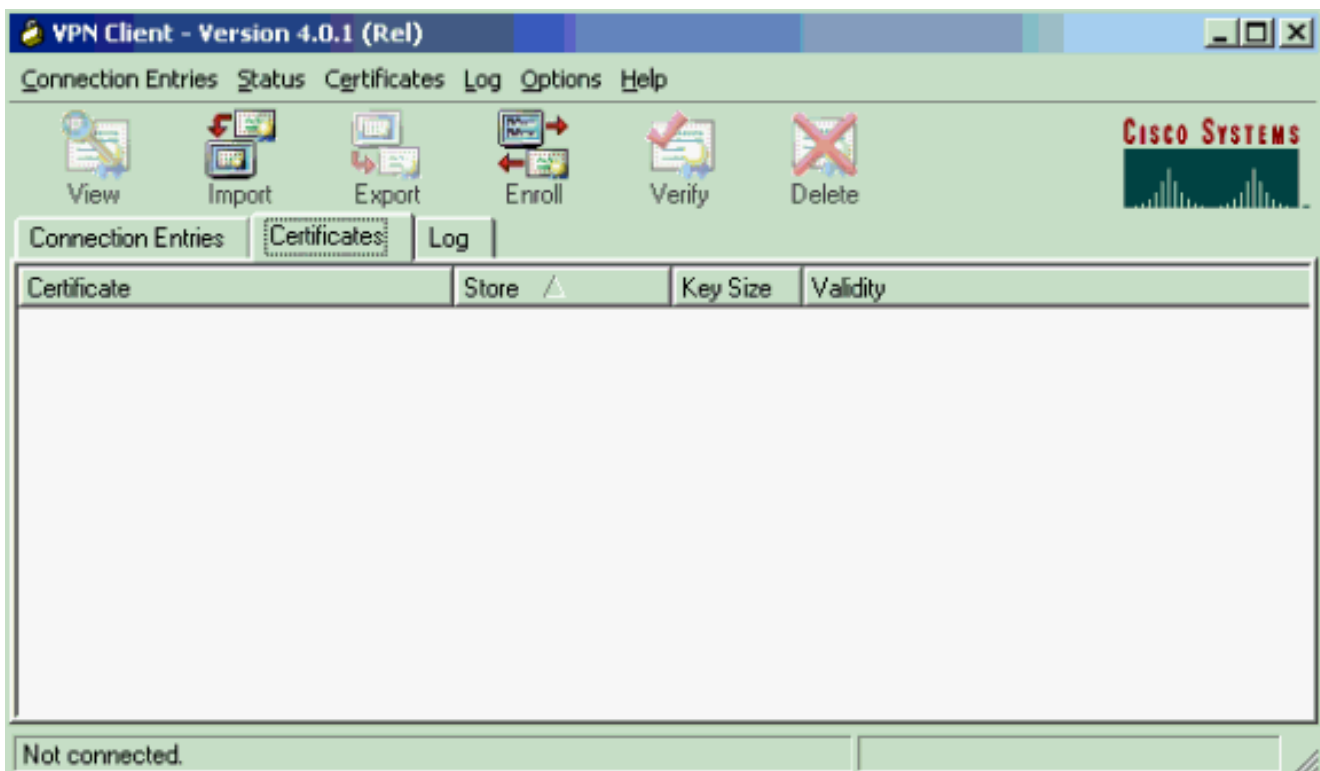


```
no ip address
shutdown
!
interface Serial3/2
no ip address
shutdown
!
interface Serial3/3
no ip address
shutdown
!
ip local pool vpnpool 10.1.1.10 10.1.1.50
ip classless
ip route 0.0.0.0 0.0.0.0 172.16.172.33
no ip http server
ip pim bidir-enable
!
!
access-list 101 permit ip 10.1.0.0 0.0.255.255 10.1.1.0
0.0.0.255
!
call rsvp-sync
!
!
mgcp profile default
!
dial-peer cor custom
!
!
line con 0
line aux 0
line vty 0 4
password cisco
!
!
end
```

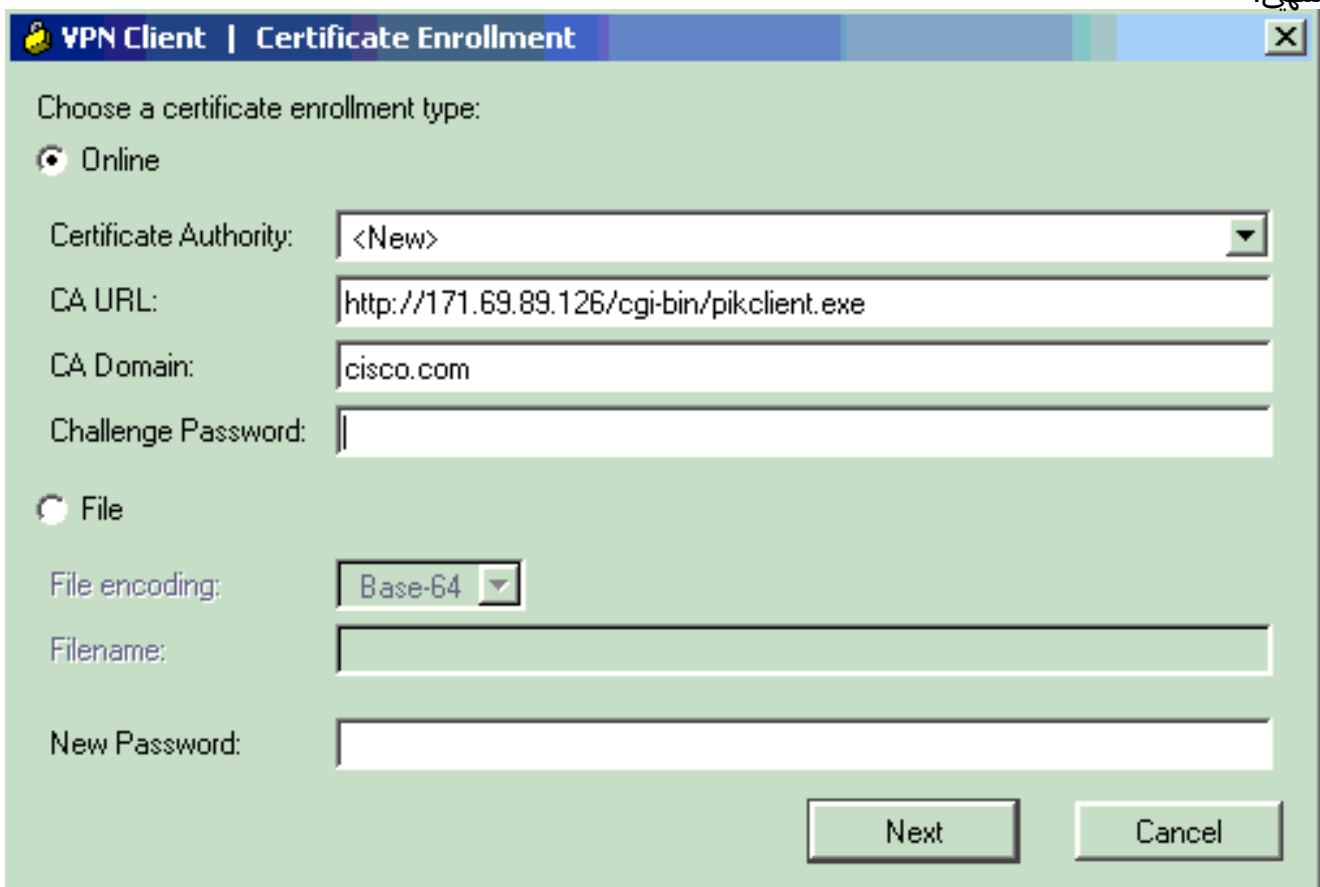
### [تسجيل الشهادة لعمل Cisco VPN](#)

تلتقط الشاشة التالية عرض الإجراءات المستخدمة لتسجيل عميل Cisco VPN لشهادات الضمان. في هذه الحالة، استخدمنا التسجيل المستند إلى الشبكة.

1. أطلقت ال VPN زبون، عينت الشهادات تبويب، وطققة  
يسجل.



2. حدد متصل كنوع تسجيل الشهادة، ثم قم بتعبئة الحقول المناسبة ل URL والمجال وكلمة المرور. طقطقت بعد ذلك عندما تنتهي.



3. أدخل معلوماتك في حقول الترخيص. إذا كنت بحاجة إلى تحرير أي معلومات على الشاشة السابقة، انقر فوق السابق. وإلا، انقر فوق التسجيل عند الانتهاء.

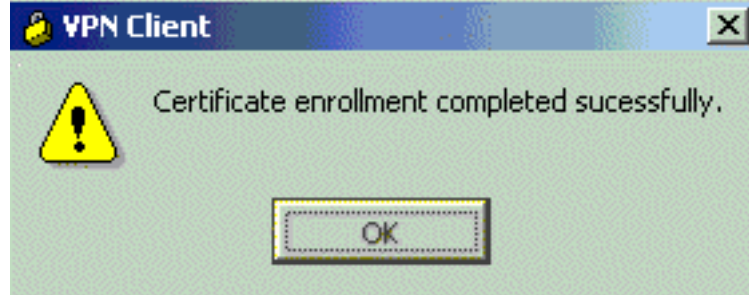
**VPN Client | Certificate Enrollment** [X]

Enter certificate fields, "\*" denotes a required field:

Name [CN]*:	vpncient
Department [OU]:	sjvpn
Company [O]:	Cisco Systems, Inc.
State [ST]:	CA
Country [C]:	US
Email [E]:	
IP Address:	
Domain:	

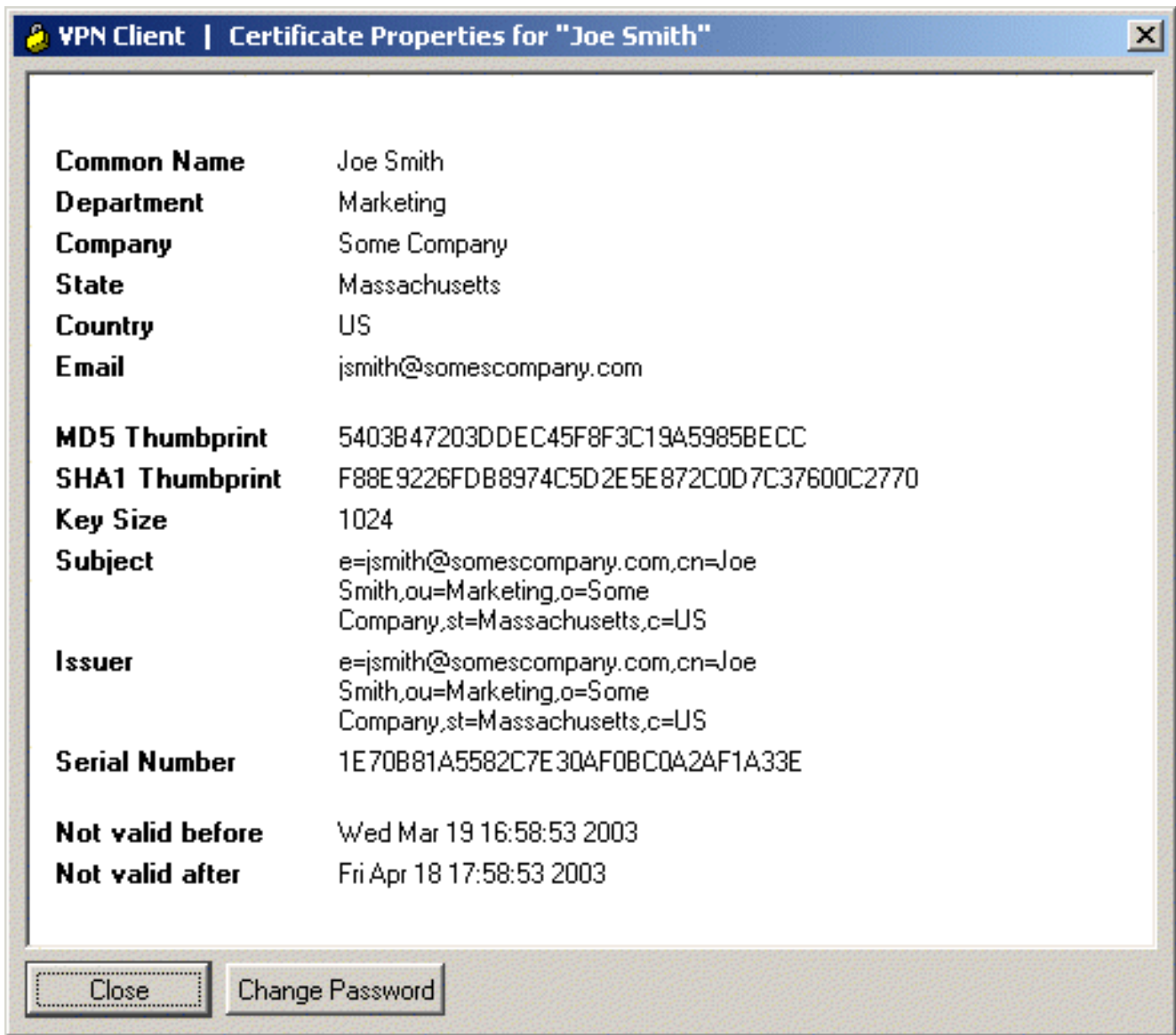
Back Enroll Cancel

4. عندما يؤكد إطار حالة التسجيل طلب التسجيل إلى خادم CA، انقر فوق موافق



للمتابعة.

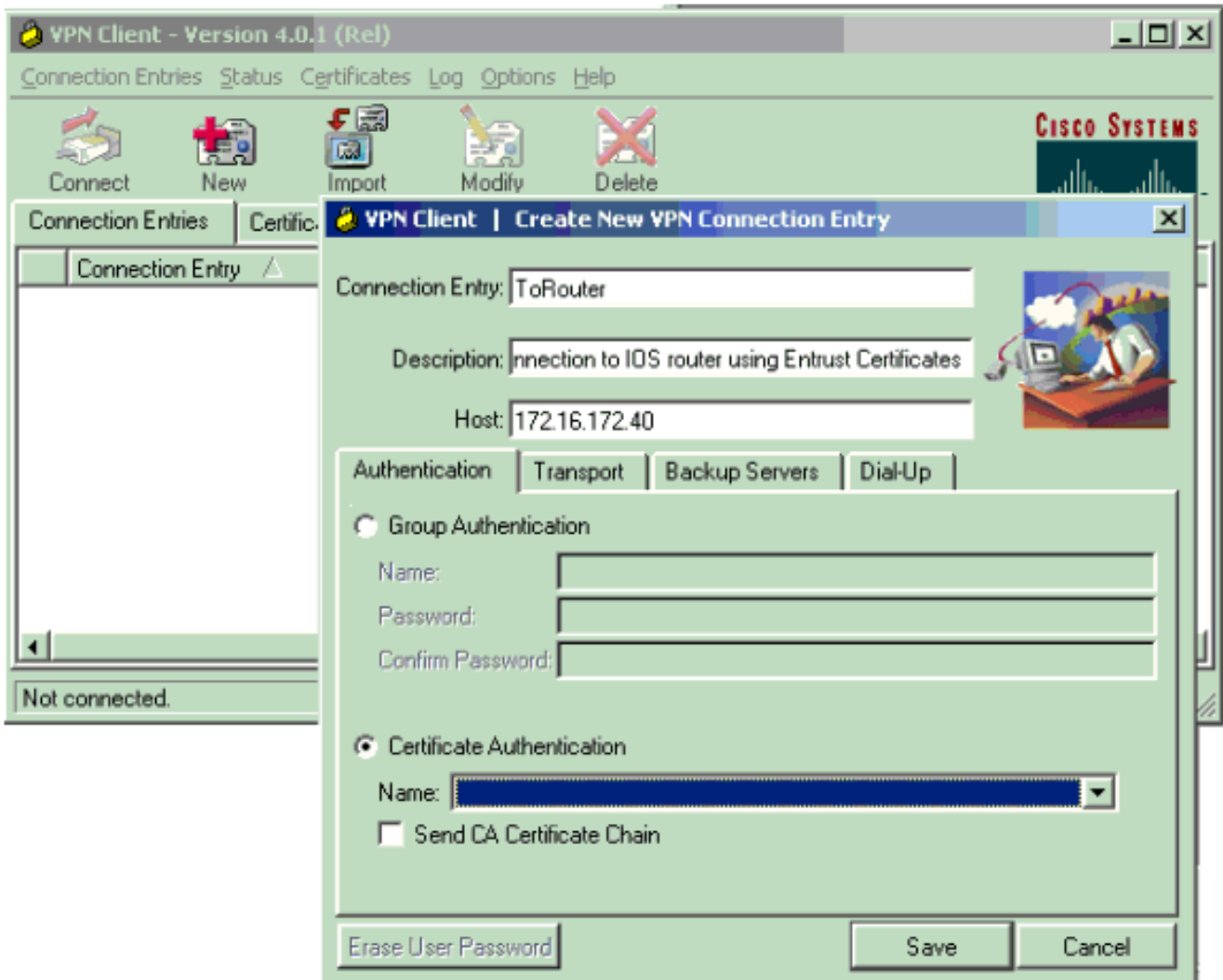
5. بعد التسجيل، يجب أن يتلقى عميل شبكة VPN شهادة شخصية واحدة وشهادة جذر CA وشهادتي RA. تتحقق شاشة الترخيص الرقمي من شهادة عميل VPN. لعرض الشهادة، انتقل إلى الشهادات < عرض. يجب أن تبدو الشهادة مماثلة للمثال التالي.



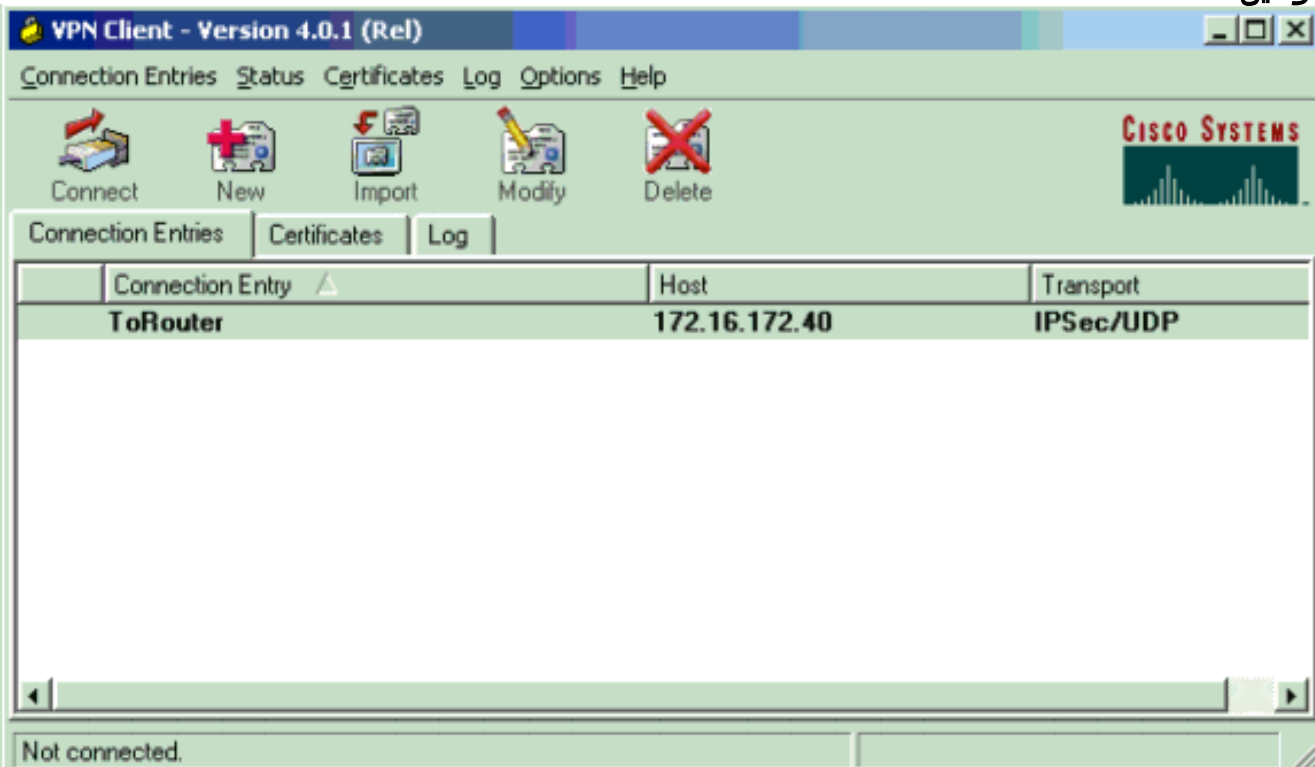
### [تكوين اتصال VPN على عميل VPN Cisco](#)

توضح لقطات الشاشة التالية كيفية تكوين اتصال جديد على عميل VPN Cisco إلى Cisco IOS.

1. قم بتشغيل عميل VPN، وحدد علامة التبويب "إدخالات الاتصال"، ثم انقر فوق جديد لإنشاء اتصال جديد.
2. أدخل اسم الاتصال والوصف وعنوان IP للمضيف. سيتم ملء حقل مصادقة الشهادة تلقائياً بمعلومات على عميل VPN. انقر فوق حفظ عند الانتهاء.



3. للتوصيل، حدد إدخال توصيل جديد ثم انقر على  
توصيل.



[التحقق من الصحة](#)

يوفر هذا القسم معلومات يمكنك إستخدامها للتأكد من أن التكوين يعمل بشكل صحيح.

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

```
3640#show crypto isakmp sa
dst src state conn-id slot
QM_IDLE 1 0 171.69.89.129 172.16.172.40

3640#show crypto ipsec sa

interface: Ethernet0/1
Crypto map tag: vpn, local addr. 172.16.172.40

(local ident (addr/mask/prot/port): (10.1.0.0/255.255.0.0/0/0
(remote ident (addr/mask/prot/port): (10.1.1.11/255.255.255.255/0/0
current_peer: 171.69.89.129
      {}=PERMIT, flags
pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4#
pkts decaps: 17, #pkts decrypt: 17, #pkts verify 17#
pkts compressed: 0, #pkts decompressed: 0#
, pkts not compressed: 0, #pkts compr. failed: 0#
pkts decompress failed: 0, #send errors 0, #recv errors 0#

local crypto endpt.: 172.16.172.40, remote crypto endpt.: 171.69.89.129
path mtu 1500, media mtu 1500
current outbound spi: E73672A9

      :inbound esp sas
      (spi: 0xADA266D3(2913101523
      , transform: esp-des esp-md5-hmac
      { ,in use settings ={Tunnel
      slot: 0, conn id: 2002, flow_id: 3, crypto map: vpn
      (sa timing: remaining key lifetime (k/sec): (4607997/3526
      IV size: 8 bytes
      replay detection support: Y

      :inbound ah sas

      :inbound pcg sas

      :outbound esp sas
      (spi: 0xE73672A9(3879105193
      , transform: esp-des esp-md5-hmac
      { ,in use settings ={Tunnel
      slot: 0, conn id: 2003, flow_id: 4, crypto map: vpn
      (sa timing: remaining key lifetime (k/sec): (4607999/3526
      IV size: 8 bytes
      replay detection support: Y

      :outbound ah sas

      :outbound pcg sas

(local ident (addr/mask/prot/port): (172.16.172.40/255.255.255.255/0/0
(remote ident (addr/mask/prot/port): (10.1.1.11/255.255.255.255/0/0
current_peer: 171.69.89.129
      {}=PERMIT, flags
pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0#
pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0#
```

```

        pkts compressed: 0, #pkts decompressed: 0#
        ,pkts not compressed: 0, #pkts compr. failed: 0#
        pkts decompress failed: 0, #send errors 0, #recv errors 0#

local crypto endpt.: 172.16.172.40, remote crypto endpt.: 171.69.89.129
        path mtu 1500, media mtu 1500
        current outbound spi: 1E04D17C

                :inbound esp sas
                (spi: 0x96D25C98(2530368664
                , 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): (4608000/3527
                IV size: 8 bytes
                replay detection support: Y

                :inbound ah sas

                :inbound pcp sas

                :outbound esp sas
                (spi: 0x1E04D17C(503632252
                , 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): (4608000/3527
                IV size: 8 bytes
                replay detection support: Y

                :outbound ah sas

                :outbound pcp sas

```

3640#show crypto engine connection active

ID	Interface	IP-Address	State	Algorithm	Encrypt	Decrypt
Ethernet0/1	172.16.172.40	set	HMAC_SHA+DES_56_CB	0	0	1
Ethernet0/1	172.16.172.40	set	HMAC_MD5+DES_56_CB	0	0	2000
Ethernet0/1	172.16.172.40	set	HMAC_MD5+DES_56_CB	0	0	2001
Ethernet0/1	172.16.172.40	set	HMAC_MD5+DES_56_CB	0	20	2002
Ethernet0/1	172.16.172.40	set	HMAC_MD5+DES_56_CB	4	0	2003

## استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

فيما يلي إخراج تصحيح الأخطاء لمفاوضات IKE عاملة التي تم تجميعها على موجه Cisco 3640. تم تشغيل تصحيح الأخطاء التالية.

3640#show debug

```

:Cryptographic Subsystem
Crypto ISAKMP debugging is on
Crypto Engine debugging is on

```

Crypto IPSEC debugging is on  
Crypto PKI Trans debugging is on

3640#

```
ISAKMP (0:0): received packet from 171.69.89.129 (N) NEW SA :00:02:30
    ISAKMP: local port 500, remote port 500 :00:02:30
    ISAKMP: Created a peer node for 171.69.89.129 :00:02:30
    ISAKMP (0:1): Setting client config settings 62D99D98 :00:02:30
ISAKMP (0:1): (Re)Setting client xauth list ClientAuth and state :00:02:30
    ISAKMP: Locking CONFIG struct 0x62D99D98 from :00:02:30
    crypto_ikmp_config_initialize_sa, count 1
ISAKMP (0:1): Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH :00:02:30
    Old State = IKE_READY New State = IKE_R_MM1

    ISAKMP (0:1): processing SA payload. message ID = 0 :00:02:30
    ISAKMP (0:1): processing vendor id payload :00:02:30
ISAKMP (0:1): vendor ID seems Unity/DPD but bad major :00:02:30
    ISAKMP (0:1): vendor ID is XAUTH :00:02:30
    ISAKMP (0:1): processing vendor id payload :00:02:30
    ISAKMP (0:1): vendor ID is DPD :00:02:30
    ISAKMP (0:1): processing vendor id payload :00:02:30
    ISAKMP (0:1): vendor ID is Unity :00:02:30
ISAKMP (0:1): Checking ISAKMP transform 1 against priority 1 policy :00:02:30
    ISAKMP: encryption 3DES-CBC :00:02:30
    ISAKMP: hash SHA :00:02:30
    ISAKMP: default group 5 :00:02:30
    ISAKMP: auth XAUTHInitRSA :00:02:30
    ISAKMP: life type in seconds :00:02:30
    ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B :00:02:30
!ISAKMP (0:1): Encryption algorithm offered does not match policy :00:02:30
    ISAKMP (0:1): atts are not acceptable. Next payload is 3 :00:02:30
ISAKMP (0:1): Checking ISAKMP transform 2 against priority 1 policy :00:02:30
    ISAKMP: encryption 3DES-CBC :00:02:30
    ISAKMP: hash MD5 :00:02:30
    ISAKMP: default group 5 :00:02:30
    ISAKMP: auth XAUTHInitRSA :00:02:30
    ISAKMP: life type in seconds :00:02:30
    ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B :00:02:30
!ISAKMP (0:1): Encryption algorithm offered does not match policy :00:02:30
    ISAKMP (0:1): atts are not acceptable. Next payload is 3 :00:02:30
ISAKMP (0:1): Checking ISAKMP transform 3 against priority 1 policy :00:02:30
    ISAKMP: encryption 3DES-CBC :00:02:30
    ISAKMP: hash SHA :00:02:30
    ISAKMP: default group 5 :00:02:30
    ISAKMP: auth RSA sig :00:02:30
    ISAKMP: life type in seconds :00:02:30
    ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B :00:02:30
!ISAKMP (0:1): Encryption algorithm offered does not match policy :00:02:30
    ISAKMP (0:1): atts are not acceptable. Next payload is 3 :00:02:30
ISAKMP (0:1): Checking ISAKMP transform 4 against priority 1 policy :00:02:30
    ISAKMP: encryption 3DES-CBC :00:02:30
    ISAKMP: hash MD5 :00:02:30
    ISAKMP: default group 5 :00:02:30
    ISAKMP: auth RSA sig :00:02:30
    ISAKMP: life type in seconds :00:02:30
    ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B :00:02:30
!ISAKMP (0:1): Encryption algorithm offered does not match policy :00:02:30
    ISAKMP (0:1): atts are not acceptable. Next payload is 3 :00:02:30
ISAKMP (0:1): Checking ISAKMP transform 5 against priority 1 policy :00:02:30
    ISAKMP: encryption 3DES-CBC :00:02:30
    ISAKMP: hash SHA :00:02:30
    ISAKMP: default group 2 :00:02:30
    ISAKMP: auth XAUTHInitRSA :00:02:30
```



ISAKMP: life type in seconds :00:02:30  
ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B :00:02:30  
!ISAKMP (0:1): Encryption algorithm offered does not match policy :00:02:30  
ISAKMP (0:1): atts are not acceptable. Next payload is 3 :00:02:30  
ISAKMP (0:1): Checking ISAKMP transform 6 against priority 1 policy :00:02:30  
ISAKMP: encryption 3DES-CBC :00:02:30  
ISAKMP: hash MD5 :00:02:30  
ISAKMP: default group 2 :00:02:30  
ISAKMP: auth XAUTHInitRSA :00:02:30  
ISAKMP: life type in seconds :00:02:30  
ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B :00:02:30  
!ISAKMP (0:1): Encryption algorithm offered does not match policy :00:02:30  
ISAKMP (0:1): atts are not acceptable. Next payload is 3 :00:02:30  
ISAKMP (0:1): Checking ISAKMP transform 7 against priority 1 policy :00:02:30  
ISAKMP: encryption 3DES-CBC :00:02:30  
ISAKMP: hash SHA :00:02:30  
ISAKMP: default group 2 :00:02:30  
ISAKMP: auth RSA sig :00:02:30  
ISAKMP: life type in seconds :00:02:30  
ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B :00:02:30  
!ISAKMP (0:1): Encryption algorithm offered does not match policy :00:02:30  
ISAKMP (0:1): atts are not acceptable. Next payload is 3 :00:02:30  
ISAKMP (0:1): Checking ISAKMP transform 8 against priority 1 policy :00:02:30  
ISAKMP: encryption 3DES-CBC :00:02:30  
ISAKMP: hash MD5 :00:02:30  
ISAKMP: default group 2 :00:02:30  
ISAKMP: auth RSA sig :00:02:30  
ISAKMP: life type in seconds :00:02:30  
ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B :00:02:30  
!ISAKMP (0:1): Encryption algorithm offered does not match policy :00:02:30  
ISAKMP (0:1): atts are not acceptable. Next payload is 3 :00:02:30  
ISAKMP (0:1): Checking ISAKMP transform 9 against priority 1 policy :00:02:30  
ISAKMP: encryption 3DES-CBC :00:02:30  
ISAKMP: hash SHA :00:02:30  
ISAKMP: default group 1 :00:02:30  
ISAKMP: auth XAUTHInitRSA :00:02:30  
ISAKMP: life type in seconds :00:02:30  
ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B :00:02:30  
!ISAKMP (0:1): Encryption algorithm offered does not match policy :00:02:30  
ISAKMP (0:1): atts are not acceptable. Next payload is 3 :00:02:30  
ISAKMP (0:1): Checking ISAKMP transform 10 against priority 1 policy :00:02:30  
ISAKMP: encryption 3DES-CBC :00:02:30  
ISAKMP: hash MD5 :00:02:30  
ISAKMP: default group 1 :00:02:30  
ISAKMP: auth XAUTHInitRSA :00:02:30  
ISAKMP: life type in seconds :00:02:30  
ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B :00:02:30  
!ISAKMP (0:1): Encryption algorithm offered does not match policy :00:02:30  
ISAKMP (0:1): atts are not acceptable. Next payload is 3 :00:02:30  
ISAKMP (0:1): Checking ISAKMP transform 11 against priority 1 policy :00:02:30  
ISAKMP: encryption 3DES-CBC :00:02:30  
ISAKMP: hash SHA :00:02:30  
ISAKMP: default group 1 :00:02:30  
ISAKMP: auth RSA sig :00:02:30  
ISAKMP: life type in seconds :00:02:30  
ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B :00:02:30  
!ISAKMP (0:1): Encryption algorithm offered does not match policy :00:02:30  
ISAKMP (0:1): atts are not acceptable. Next payload is 3 :00:02:30  
ISAKMP (0:1): Checking ISAKMP transform 12 against priority 1 policy :00:02:30  
ISAKMP: encryption 3DES-CBC :00:02:30  
ISAKMP: hash MD5 :00:02:30  
ISAKMP: default group 1 :00:02:30  
ISAKMP: auth RSA sig :00:02:30  
ISAKMP: life type in seconds :00:02:30

```
ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B :00:02:30
!ISAKMP (0:1): Encryption algorithm offered does not match policy :00:02:30
ISAKMP (0:1): atts are not acceptable. Next payload is 3 :00:02:30
ISAKMP (0:1): Checking ISAKMP transform 13 against priority 1 policy :00:02:30
    ISAKMP: encryption DES-CBC :00:02:30
        ISAKMP: hash SHA :00:02:30
            ISAKMP: default group 5 :00:02:30
                ISAKMP: auth XAUTHInitRSA :00:02:30
                    ISAKMP: life type in seconds :00:02:30
            ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B :00:02:30
        !ISAKMP (0:1): Diffie-Hellman group offered does not match policy :00:02:30
        ISAKMP (0:1): atts are not acceptable. Next payload is 3 :00:02:30
    ISAKMP (0:1): Checking ISAKMP transform 14 against priority 1 policy :00:02:30
        ISAKMP: encryption DES-CBC :00:02:30
            ISAKMP: hash MD5 :00:02:30
                ISAKMP: default group 5 :00:02:30
                    ISAKMP: auth XAUTHInitRSA :00:02:30
                        ISAKMP: life type in seconds :00:02:30
                ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B :00:02:30
            !ISAKMP (0:1): Hash algorithm offered does not match policy :00:02:30
            ISAKMP (0:1): atts are not acceptable. Next payload is 3 :00:02:30
        ISAKMP (0:1): Checking ISAKMP transform 15 against priority 1 policy :00:02:30
            ISAKMP: encryption DES-CBC :00:02:30
                ISAKMP: hash SHA :00:02:30
                    ISAKMP: default group 5 :00:02:30
                        ISAKMP: auth RSA sig :00:02:30
                            ISAKMP: life type in seconds :00:02:30
                    ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B :00:02:30
                !ISAKMP (0:1): Diffie-Hellman group offered does not match policy :00:02:30
                ISAKMP (0:1): atts are not acceptable. Next payload is 3 :00:02:30
            ISAKMP (0:1): Checking ISAKMP transform 16 against priority 1 policy :00:02:30
                ISAKMP: encryption DES-CBC :00:02:30
                    ISAKMP: hash MD5 :00:02:30
                        ISAKMP: default group 5 :00:02:30
                            ISAKMP: auth RSA sig :00:02:30
                                ISAKMP: life type in seconds :00:02:30
                        ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B :00:02:30
                    !ISAKMP (0:1): Hash algorithm offered does not match policy :00:02:30
                    ISAKMP (0:1): atts are not acceptable. Next payload is 3 :00:02:30
                ISAKMP (0:1): Checking ISAKMP transform 17 against priority 1 policy :00:02:30
                    ISAKMP: encryption DES-CBC :00:02:30
                        ISAKMP: hash SHA :00:02:30
                            ISAKMP: default group 2 :00:02:30
                                ISAKMP: auth XAUTHInitRSA :00:02:30
                                    ISAKMP: life type in seconds :00:02:30
                            ISAKMP: life duration (VPI) of 0x0 0x20 0xC4 0x9B :00:02:30
                        ISAKMP (0:1): atts are acceptable. Next payload is 3 :00:02:30
                            CryptoEngine0: generate alg parameter :00:02:30
                                CRYPTO_ENGINE: Dh phase 1 status: 0 :00:02:31
                                    CRYPTO_ENGINE: Dh phase 1 status: 0 :00:02:31
                                        ISAKMP (0:1): processing vendor id payload :00:02:31
                                            ISAKMP (0:1): processing vendor id payload :00:02:31
                                                ISAKMP (0:1): processing vendor id payload :00:02:31
                                                    ISAKMP (0:1): Input = IKE_MSG_INTERNAL, IKE_PROCESS_MAIN_MODE :00:02:31
                                                        Old State = IKE_R_MM1 New State = IKE_R_MM1

ISAKMP (0:1): sending packet to 171.69.89.129 (R) MM_SA_SETUP :00:02:31
ISAKMP (0:1): Input = IKE_MSG_INTERNAL, IKE_PROCESS_COMPLETE :00:02:31
    Old State = IKE_R_MM1 New State = IKE_R_MM2

ISAKMP (0:1): received packet from 171.69.89.129 (R) MM_SA_SETUP :00:02:31
    ISAKMP (0:1): Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH :00:02:31
        Old State = IKE_R_MM2 New State = IKE_R_MM3
```

```
ISAKMP (0:1): processing KE payload. message ID = 0 :00:02:31
    CryptoEngine0: generate alg parameter :00:02:31
ISAKMP (0:1): processing NONCE payload. message ID = 0 :00:02:31
    CryptoEngine0: calculate pkey hmac for conn id 1 :00:02:31
    CryptoEngine0: create ISAKMP SKEYID for conn id 1 :00:02:31
        ISAKMP (0:1): SKEYID state generated :00:02:31
ISAKMP (0:1): Input = IKE_MSG_INTERNAL, IKE_PROCESS_MAIN_MODE :00:02:31
    Old State = IKE_R_MM3 New State = IKE_R_MM3

ISAKMP (0:1): sending packet to 171.69.89.129 (R) MM_KEY_EXCH :00:02:31
ISAKMP (0:1): Input = IKE_MSG_INTERNAL, IKE_PROCESS_COMPLETE :00:02:31
    Old State = IKE_R_MM3 New State = IKE_R_MM4

ISAKMP (0:1): received packet from 171.69.89.129 (R) MM_KEY_EXCH :00:02:31
    ISAKMP (0:1): Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH :00:02:31
        Old State = IKE_R_MM4 New State = IKE_R_MM5

ISAKMP (0:1): processing ID payload. message ID = 0 :00:02:31
ISAKMP (0:1): processing CERT payload. message ID = 0 :00:02:31
    ISAKMP (0:1): processing a CT_X509_SIGNATURE cert :00:02:31
,CRYPTO_PKI: status = 0: poll CRL ldap search: server=171.69.89.126 :00:02:31
    =base=CN = CRL1, OU = sjvpn, O = cisco, C = us, attribute
    scope=2, filter=cn=CRL1 :
        .CRYPTO_PKI: ldap_bind() succeeded :00:02:31
        CRYPTO_PKI: set CRL update timer with delay: 89703 :00:02:32
        CRYPTO_PKI: the current router time: 00:00:39 UTC Apr 9 2002 :00:02:32
            CRYPTO_PKI: the last CRL update time: 23:55:42 UTC Apr 8 2002 :00:02:32
            CRYPTO_PKI: the next CRL update time: 00:55:42 UTC Apr 10 2002 :00:02:32
            CRYPTO_PKI: status = 0: failed to get public key from the storage :00:02:32
            CRYPTO_PKI: status = 65535: failed to get issuer pubkey in cert :00:02:32
            CRYPTO_PKI: status = 0: failed to get public key from the storage :00:02:32
            CRYPTO_PKI: status = 65535: failed to get issuer pubkey in cert :00:02:32
            CRYPTO_PKI: status = 0: failed to get public key from the storage :00:02:32
            CRYPTO_PKI: status = 65535: failed to get issuer pubkey in cert :00:02:32
            CRYPTO_PKI: status = 0: failed to get public key from the storage :00:02:32
            CRYPTO_PKI: status = 65535: failed to get issuer pubkey in cert :00:02:32
            CRYPTO_PKI: transaction GetCRL completed :00:02:32
            CRYPTO_PKI: blocking callback received status: 105 :00:02:32
            CRYPTO_PKI: Certificate verified, chain status= 1 :00:02:32
                ISAKMP (0:1): OU = sjvpn :00:02:32
            ISAKMP (0:1): processing CERT_REQ payload. message ID = 0 :00:02:32
                ISAKMP (0:1): peer wants a CT_X509_SIGNATURE cert :00:02:32
ISAKMP (0:1): peer want cert issued by OU = sjvpn, O = cisco, C = us :00:02:32
                ISAKMP (0:1): processing SIG payload. message ID = 0 :00:02:32
                    Crypto engine 0: RSA decrypt with public key :00:02:32
                    CryptoEngine0: CRYPTO_RSA_PUB_DECRYPT :00:02:32
                    CryptoEngine0: generate hmac context for conn id 1 :00:02:32
                ISAKMP (0:1): processing NOTIFY INITIAL_CONTACT protocol 1 :00:02:32
                    spi 0, message ID = 0, sa = 62D99794
                    ,ISAKMP (0:1): Process initial contact :00:02:32
                        bring down existing phase 1 and 2 SA's
                    ISAKMP (0:1): returning IP addr to the address pool :00:02:32
                    .ISAKMP (0:1): peer does not do paranoid keepalives :00:02:32

                ISAKMP (0:1): SA has been authenticated with 171.69.89.129 :00:02:32
                ISAKMP (0:1): Input = IKE_MSG_INTERNAL, IKE_PROCESS_MAIN_MODE :00:02:32
                    Old State = IKE_R_MM5 New State = IKE_R_MM5

                    ...IPSEC(key_engine): got a queue event :00:02:32
                IPSEC(key_engine_delete_sas): rec'd delete notify from ISAKMP :00:02:32
                    IPSEC(key_engine_delete_sas): delete all SAs :00:02:32
                        shared with 171.69.89.129
                ISAKMP (0:1): SA is doing RSA signature authentication plus XAUTH :00:02:32
                    using id type ID_FQDN
```

```
ISAKMP (1): ID payload :00:02:32
      next-payload : 6
      type : 2
      protocol : 17
      port : 500
      length : 18
ISAKMP (1): Total payload length: 22 :00:02:32
CryptoEngine0: generate hmac context for conn id 1 :00:02:32
  Crypto engine 0: RSA encrypt with private key :00:02:32
  CryptoEngine0: CRYPTO_RSA_PRIV_ENCRYPT :00:02:32
  CryptoEngine0: clear dh number for conn id 1 :00:02:32
ISAKMP (0:1): sending packet to 171.69.89.129 (R) CONF_XAUTH :00:02:32
  CryptoEngine0: generate hmac context for conn id 1 :00:02:32
ISAKMP (0:1): sending packet to 171.69.89.129 (R) CONF_XAUTH :00:02:32
  ISAKMP: Sending phase 1 responder lifetime 86400 :00:02:32

ISAKMP (0:1): Input = IKE_MSG_INTERNAL, IKE_PROCESS_COMPLETE :00:02:32
  Old State = IKE_R_MM5 New State = IKE_P1_COMPLETE

ISAKMP (0:1): Need XAUTH :00:02:32
ISAKMP (0:1): Input = IKE_MSG_INTERNAL, IKE_PHASE1_COMPLETE :00:02:32
Old State = IKE_P1_COMPLETE New State = IKE_XAUTH_AAA_START_LOGIN_AWAIT

ISAKMP: got callback 1 :00:02:32
  ISAKMP/xauth: request attribute XAUTH_TYPE_V2 :00:02:32
  ISAKMP/xauth: request attribute XAUTH_MESSAGE_V2 :00:02:32
  ISAKMP/xauth: request attribute XAUTH_USER_NAME_V2 :00:02:32
  ISAKMP/xauth: request attribute XAUTH_USER_PASSWORD_V2 :00:02:32
  CryptoEngine0: generate hmac context for conn id 1 :00:02:32
  .ISAKMP (0:1): initiating peer config to 171.69.89.129 :00:02:32
    ID = -670289125
ISAKMP (0:1): sending packet to 171.69.89.129 (R) CONF_XAUTH :00:02:32
ISAKMP (0:1): Input = IKE_MSG_FROM_AAA, IKE_AAA_START_LOGIN :00:02:32
Old State = IKE_XAUTH_AAA_START_LOGIN_AWAIT New State = IKE_XAUTH_REQ_SENT

ISAKMP (0:1): received packet from 171.69.89.129 (R) CONF_XAUTH :00:02:36
.ISAKMP (0:1): processing transaction payload from 171.69.89.129 :00:02:36
  message ID = -670289125
  CryptoEngine0: generate hmac context for conn id 1 :00:02:36
  ISAKMP: Config payload REPLY :00:02:36
  ISAKMP/xauth: reply attribute XAUTH_TYPE_V2 unexpected :00:02:36
  ISAKMP/xauth: reply attribute XAUTH_USER_NAME_V2 :00:02:36
  ISAKMP/xauth: reply attribute XAUTH_USER_PASSWORD_V2 :00:02:36
  ISAKMP (0:1): deleting node -670289125 error FALSE :00:02:36
    "reason "done with xauth request/reply exchange
  ISAKMP (0:1): Input = IKE_MSG_FROM_PEER, IKE_CFG_REPLY :00:02:36
Old State = IKE_XAUTH_REQ_SENT New State = IKE_XAUTH_AAA_CONT_LOGIN_AWAIT

ISAKMP: got callback 1 :00:02:36
  CryptoEngine0: generate hmac context for conn id 1 :00:02:36
  .ISAKMP (0:1): initiating peer config to 171.69.89.129 :00:02:36
    ID = -1610220250
ISAKMP (0:1): sending packet to 171.69.89.129 (R) CONF_XAUTH :00:02:36
ISAKMP (0:1): Input = IKE_MSG_FROM_AAA, IKE_AAA_CONT_LOGIN :00:02:36
Old State = IKE_XAUTH_AAA_CONT_LOGIN_AWAIT New State = IKE_XAUTH_SET_SENT

ISAKMP (0:1): received packet from 171.69.89.129 (R) CONF_XAUTH :00:02:36
.ISAKMP (0:1): processing transaction payload from 171.69.89.129 :00:02:36
  message ID = -1610220250
  CryptoEngine0: generate hmac context for conn id 1 :00:02:36
  ISAKMP: Config payload ACK :00:02:36
ISAKMP (0:1): XAUTH ACK Processed :00:02:36
ISAKMP (0:1): deleting node -1610220250 error FALSE :00:02:36
  "reason "done with transaction
```

```
ISAKMP (0:1): Input = IKE_MSG_FROM_PEER, IKE_CFG_ACK :00:02:36
    Old State = IKE_XAUTH_SET_SENT New State = IKE_P1_COMPLETE

ISAKMP (0:1): Input = IKE_MSG_INTERNAL, IKE_PHASE1_COMPLETE :00:02:36
    Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE

ISAKMP (0:1): received packet from 171.69.89.129 (R) QM_IDLE :00:02:36
.ISAKMP (0:1): processing transaction payload from 171.69.89.129 :00:02:36
    message ID = 1789347264
    CryptoEngine0: generate hmac context for conn id 1 :00:02:36
        ISAKMP: Config payload REQUEST :00:02:36
        :ISAKMP (0:1): checking request :00:02:36
            ISAKMP: IP4_ADDRESS :00:02:36
            ISAKMP: IP4_NETMASK :00:02:36
            ISAKMP: IP4_DNS :00:02:36
            ISAKMP: IP4_NBNS :00:02:36
            ISAKMP: ADDRESS_EXPIRY :00:02:36
            ISAKMP: APPLICATION_VERSION :00:02:36
            ISAKMP: UNKNOWN Unknown Attr: 0x7000 :00:02:36
            ISAKMP: UNKNOWN Unknown Attr: 0x7001 :00:02:36
            ISAKMP: DEFAULT_DOMAIN :00:02:36
            ISAKMP: SPLIT_INCLUDE :00:02:36
            ISAKMP: UNKNOWN Unknown Attr: 0x7007 :00:02:36
            ISAKMP: UNKNOWN Unknown Attr: 0x7008 :00:02:36
ISAKMP (0:1): Input = IKE_MSG_FROM_PEER, IKE_CFG_REQUEST :00:02:36
    Old State = IKE_P1_COMPLETE New State = IKE_CONFIG_AUTHOR_AAA_AWAIT

        ISAKMP: got callback 1 :00:02:36
        :ISAKMP (0:1): attributes sent in message :00:02:36
            Address: 0.2.0.0 :00:02:36
        ISAKMP (0:1): allocating address 10.1.1.10 :00:02:36
        ISAKMP: Sending private address: 10.1.1.10 :00:02:36
            (ISAKMP: Unknown Attr: IP4_NETMASK (0x2) :00:02:36
        ISAKMP: Sending IP4_DNS server address: 10.1.1.5 :00:02:36
        ISAKMP: Sending IP4_NBNS server address: 10.1.1.5 :00:02:36
        ISAKMP: Sending ADDRESS_EXPIRY seconds left :00:02:36
            to use the address: 86394
        :ISAKMP: Sending APPLICATION_VERSION string :00:02:36
            Cisco Internetwork Operating System Software
            ,IOS (tm) 3600 Software (C3640-IK803S-M), Version 12.2(8)T
            (RELEASE SOFTWARE (fc2
            TAC Support: http://www.cisco.com/tac
            .Copyright (c) 1986-2002 by cisco Systems, Inc
            Compiled Thu 14-Feb-02 19:36 by ccai
            (ISAKMP: Unknown Attr: UNKNOWN (0x7000) :00:02:36
            (ISAKMP: Unknown Attr: UNKNOWN (0x7001) :00:02:36
        ISAKMP: Sending DEFAULT_DOMAIN default domain name: sjpki.com :00:02:36
        ISAKMP: Sending split include name 101 network 10.1.0.0 :00:02:36
            mask 255.255.0.0, protocol 0, src port 0, dst port 0

            (ISAKMP: Unknown Attr: UNKNOWN (0x7007) :00:02:36
            (ISAKMP: Unknown Attr: UNKNOWN (0x7008) :00:02:36
        CryptoEngine0: generate hmac context for conn id 1 :00:02:36
        .ISAKMP (0:1): responding to peer config from 171.69.89.129 :00:02:36
            ID = 1789347264
        ISAKMP (0:1): sending packet to 171.69.89.129 (R) CONF_ADDR :00:02:36
        " ISAKMP (0:1): deleting node 1789347264 error FALSE reason :00:02:36
        ISAKMP (0:1): Input = IKE_MSG_FROM_AAA, IKE_AAA_GROUP_ATTR :00:02:36
            Old State = IKE_CONFIG_AUTHOR_AAA_AWAIT New State = IKE_P1_COMPLETE

ISAKMP (0:1): received packet from 171.69.89.129 (R) QM_IDLE :00:02:36
    CryptoEngine0: generate hmac context for conn id 1 :00:02:36
    ISAKMP (0:1): processing HASH payload. message ID = -1460041169 :00:02:36
    ISAKMP (0:1): processing SA payload. message ID = -1460041169 :00:02:36
```

**ISAKMP (0:1): Checking IPsec proposal 1 :00:02:36**  
ISAKMP: transform 1, ESP\_3DES :00:02:36  
:ISAKMP: attributes in transform :00:02:36  
ISAKMP: authenticator is HMAC-MD5 :00:02:36  
ISAKMP: encaps is 1 :00:02:36  
ISAKMP: SA life type in seconds :00:02:36  
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B :00:02:36  
validate proposal 0 :00:02:36  
IPSEC(validate\_proposal): transform proposal :00:02:36  
prot 3, trans 3, hmac\_alg 1) not supported)  
ISAKMP (0:1): atts not acceptable. Next payload is 0 :00:02:36  
(ISAKMP (0:1): skipping next ANDED proposal (1 :00:02:36  
ISAKMP (0:1): Checking IPsec proposal 2 :00:02:36  
ISAKMP: transform 1, ESP\_3DES :00:02:36  
:ISAKMP: attributes in transform :00:02:36  
ISAKMP: authenticator is HMAC-SHA :00:02:36  
ISAKMP: encaps is 1 :00:02:36  
ISAKMP: SA life type in seconds :00:02:36  
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B :00:02:36  
validate proposal 0 :00:02:36  
IPSEC(validate\_proposal): transform proposal :00:02:36  
prot 3, trans 3, hmac\_alg 2) not supported)  
ISAKMP (0:1): atts not acceptable. Next payload is 0 :00:02:36  
(ISAKMP (0:1): skipping next ANDED proposal (2 :00:02:36  
ISAKMP (0:1): Checking IPsec proposal 3 :00:02:36  
ISAKMP: transform 1, ESP\_3DES :00:02:36  
:ISAKMP: attributes in transform :00:02:36  
ISAKMP: authenticator is HMAC-MD5 :00:02:36  
ISAKMP: encaps is 1 :00:02:36  
ISAKMP: SA life type in seconds :00:02:36  
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B :00:02:36  
validate proposal 0 :00:02:36  
IPSEC(validate\_proposal): transform proposal :00:02:36  
prot 3, trans 3, hmac\_alg 1) not supported)  
ISAKMP (0:1): atts not acceptable. Next payload is 0 :00:02:36  
ISAKMP (0:1): Checking IPsec proposal 4 :00:02:36  
ISAKMP: transform 1, ESP\_3DES :00:02:36  
:ISAKMP: attributes in transform :00:02:36  
ISAKMP: authenticator is HMAC-SHA :00:02:36  
ISAKMP: encaps is 1 :00:02:36  
ISAKMP: SA life type in seconds :00:02:36  
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B :00:02:36  
validate proposal 0 :00:02:36  
IPSEC(validate\_proposal): transform proposal :00:02:36  
prot 3, trans 3, hmac\_alg 2) not supported)  
ISAKMP (0:1): atts not acceptable. Next payload is 0 :00:02:36  
ISAKMP (0:1): Checking IPsec proposal 5 :00:02:36  
ISAKMP: transform 1, ESP\_DES :00:02:36  
:ISAKMP: attributes in transform :00:02:36  
ISAKMP: authenticator is HMAC-MD5 :00:02:36  
ISAKMP: encaps is 1 :00:02:36  
ISAKMP: SA life type in seconds :00:02:36  
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B :00:02:36  
validate proposal 0 :00:02:36  
.ISAKMP (0:1): atts are acceptable :00:02:36  
ISAKMP (0:1): Checking IPsec proposal 5 :00:02:36  
ISAKMP (0:1): transform 1, IPPCP LZS :00:02:36  
:ISAKMP: attributes in transform :00:02:36  
ISAKMP: encaps is 1 :00:02:36  
ISAKMP: SA life type in seconds :00:02:36  
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B :00:02:36  
IPSEC(validate\_proposal): transform proposal :00:02:36  
prot 4, trans 3, hmac\_alg 0) not supported)  
ISAKMP (0:1): atts not acceptable. Next payload is 0 :00:02:36

```
ISAKMP (0:1): Checking IPsec proposal 6 :00:02:36
      ISAKMP: transform 1, ESP_DES :00:02:36
      :ISAKMP: attributes in transform :00:02:36
      ISAKMP: authenticator is HMAC-SHA :00:02:36
      ISAKMP: encaps is 1 :00:02:36
      ISAKMP: SA life type in seconds :00:02:36
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B :00:02:36
      validate proposal 0 :00:02:36
      IPSEC(validate_proposal): transform proposal :00:02:36
      prot 3, trans 2, hmac_alg 2) not supported)
ISAKMP (0:1): atts not acceptable. Next payload is 0 :00:02:36
      (ISAKMP (0:1): skipping next ANDED proposal (6 :00:02:36
      ISAKMP (0:1): Checking IPsec proposal 7 :00:02:36
      ISAKMP: transform 1, ESP_DES :00:02:36
      :ISAKMP: attributes in transform :00:02:36
      ISAKMP: authenticator is HMAC-MD5 :00:02:36
      ISAKMP: encaps is 1 :00:02:36
      ISAKMP: SA life type in seconds :00:02:36
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B :00:02:36
      validate proposal 0 :00:02:36
      .ISAKMP (0:1): atts are acceptable :00:02:36
      ,IPSEC(validate_proposal_request): proposal part #1 :00:02:36
      ,key eng. msg.) INBOUND local= 172.16.172.40, remote= 171.69.89.129)
      ,(local_proxy= 172.16.172.40/255.255.255.255/0/0 (type=1
      ,(remote_proxy= 10.1.1.10/255.255.255.255/0/0 (type=1
      , protocol= ESP, transform= esp-des esp-md5-hmac
      ,lifedur= 0s and 0kb
      spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
      validate proposal request 0 :00:02:36
ISAKMP (0:1): processing NONCE payload. message ID = -1460041169 :00:02:36
ISAKMP (0:1): processing ID payload. message ID = -1460041169 :00:02:36
ISAKMP (0:1): processing ID payload. message ID = -1460041169 :00:02:36
      ISAKMP (0:1): asking for 1 spis from ipsec :00:02:36
      ,ISAKMP (0:1): Node -1460041169, Input = IKE_MSG_FROM_PEER :00:02:36
      IKE_QM_EXCH
      Old State = IKE_QM_READY New State = IKE_QM_SPI_STARVE

      ...IPSEC(key_engine): got a queue event :00:02:36
      IPSEC(spi_response): getting spi 1289658319 for SA :00:02:36
      from 172.16.172.40 to 171.69.89.129 for prot 3
      (ISAKMP: received ke message (2/1 :00:02:36
      CryptoEngine0: generate hmac context for conn id 1 :00:02:36
      ISAKMP (0:1): sending packet to 171.69.89.129 (R) QM_IDLE :00:02:36
      ,ISAKMP (0:1): Node -1460041169, Input = IKE_MSG_FROM_IPSEC :00:02:36
      IKE_SPI_REPLY
      Old State = IKE_QM_SPI_STARVE New State = IKE_QM_R_QM2

ISAKMP (0:1): received packet from 171.69.89.129 (R) QM_IDLE :00:02:36
      CryptoEngine0: generate hmac context for conn id 1 :00:02:36
      ipsec allocate flow 0 :00:02:36
      ipsec allocate flow 0 :00:02:36
      ISAKMP (0:1): Creating IPsec SAs :00:02:36
      inbound SA from 171.69.89.129 to 172.16.172.40 :00:02:36
      (proxy 10.1.1.10 to 172.16.172.40)
      has spi 0x4CDE9FCF and conn_id 2000 and flags 4 :00:02:36
      lifetime of 2147483 seconds :00:02:36
      outbound SA from 172.16.172.40 to 171.69.89.129 :00:02:36
      (proxy 172.16.172.40 to 10.1.1.10)
      has spi -154514029 and conn_id 2001 and flags C :00:02:36
      lifetime of 2147483 seconds :00:02:36
      ISAKMP (0:1): deleting node -1460041169 error FALSE :00:02:36
      "()"reason "quick mode done (await
      ,ISAKMP (0:1): Node -1460041169, Input = IKE_MSG_FROM_PEER :00:02:36
      IKE_QM_EXCH
```

Old State = IKE\_QM\_R\_QM2 New State = IKE\_QM\_PHASE2\_COMPLETE

```
...IPSEC(key_engine): got a queue event :00:02:36
, : (IPSEC(initialize_sas :00:02:36
,key eng. msg.) INBOUND local= 172.16.172.40, remote= 171.69.89.129)
, (local_proxy= 172.16.172.40/0.0.0.0/0/0 (type=1
, (remote_proxy= 10.1.1.10/0.0.0.0/0/0 (type=1
, protocol= ESP, transform= esp-des esp-md5-hmac
, lifedur= 2147483s and 0kb
spi= 0x4CDE9FCF(1289658319), conn_id= 2000, keysize= 0, flags= 0x4
, : (IPSEC(initialize_sas :00:02:36
,key eng. msg.) OUTBOUND local= 172.16.172.40, remote= 171.69.89.129)
, (local_proxy= 172.16.172.40/0.0.0.0/0/0 (type=1
, (remote_proxy= 10.1.1.10/0.0.0.0/0/0 (type=1
, protocol= ESP, transform= esp-des esp-md5-hmac
, lifedur= 2147483s and 0kb
spi= 0xF6CA4D93(4140453267), conn_id= 2001, keysize= 0, flags= 0xC
, IPSEC(create_sa): sa created :00:02:36
, sa) sa_dest= 172.16.172.40, sa_prot= 50)
, (sa_spi= 0x4CDE9FCF(1289658319
sa_trans= esp-des esp-md5-hmac , sa_conn_id= 2000
, IPSEC(create_sa): sa created :00:02:36
, sa) sa_dest= 171.69.89.129, sa_prot= 50)
, (sa_spi= 0xF6CA4D93(4140453267
sa_trans= esp-des esp-md5-hmac , sa_conn_id= 2001
(ISAKMP: received ke message (4/1 :00:02:36
ISAKMP: Locking CONFIG struct 0x62D99D98 for :00:02:36
crypto_ikmp_config_handle_kei_mess, count 2
ISAKMP (0:1): received packet from 171.69.89.129 (R) QM_IDLE :00:02:37
CryptoEngine0: generate hmac context for conn id 1 :00:02:37
ISAKMP (0:1): processing HASH payload. message ID = 926518983 :00:02:37
ISAKMP (0:1): processing SA payload. message ID = 926518983 :00:02:37
ISAKMP (0:1): Checking IPsec proposal 1 :00:02:37
ISAKMP: transform 1, ESP_3DES :00:02:37
: ISAKMP: attributes in transform :00:02:37
ISAKMP: authenticator is HMAC-MD5 :00:02:37
ISAKMP: encaps is 1 :00:02:37
ISAKMP: SA life type in seconds :00:02:37
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B :00:02:37
validate proposal 0 :00:02:37
IPSEC(validate_proposal): transform proposal :00:02:37
prot 3, trans 3, hmac_alg 1) not supported)
ISAKMP (0:1): atts not acceptable. Next payload is 0 :00:02:37
(ISAKMP (0:1): skipping next ANDed proposal (1 :00:02:37
ISAKMP (0:1): Checking IPsec proposal 2 :00:02:37
ISAKMP: transform 1, ESP_3DES :00:02:37
: ISAKMP: attributes in transform :00:02:37
ISAKMP: authenticator is HMAC-SHA :00:02:37
ISAKMP: encaps is 1 :00:02:37
ISAKMP: SA life type in seconds :00:02:37
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B :00:02:37
validate proposal 0 :00:02:37
IPSEC(validate_proposal): transform proposal :00:02:37
prot 3, trans 3, hmac_alg 2) not supported)
ISAKMP (0:1): atts not acceptable. Next payload is 0 :00:02:37
(ISAKMP (0:1): skipping next ANDed proposal (2 :00:02:37
ISAKMP (0:1): Checking IPsec proposal 3 :00:02:37
ISAKMP: transform 1, ESP_3DES :00:02:37
: ISAKMP: attributes in transform :00:02:37
ISAKMP: authenticator is HMAC-MD5 :00:02:37
ISAKMP: encaps is 1 :00:02:37
ISAKMP: SA life type in seconds :00:02:37
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B :00:02:37
validate proposal 0 :00:02:37
```



```
IPSEC(validate_proposal): transform proposal :00:02:37
    prot 3, trans 3, hmac_alg 1) not supported)
ISAKMP (0:1): atts not acceptable. Next payload is 0 :00:02:37
    ISAKMP (0:1): Checking IPsec proposal 4 :00:02:37
        ISAKMP: transform 1, ESP_3DES :00:02:37
        :ISAKMP: attributes in transform :00:02:37
        ISAKMP: authenticator is HMAC-SHA :00:02:37
        ISAKMP: encaps is 1 :00:02:37
        ISAKMP: SA life type in seconds :00:02:37
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B :00:02:37
    validate proposal 0 :00:02:37
IPSEC(validate_proposal): transform proposal :00:02:37
    prot 3, trans 3, hmac_alg 2) not supported)
ISAKMP (0:1): atts not acceptable. Next payload is 0 :00:02:37
    ISAKMP (0:1): Checking IPsec proposal 5 :00:02:37
        ISAKMP: transform 1, ESP_DES :00:02:37
        :ISAKMP: attributes in transform :00:02:37
        ISAKMP: authenticator is HMAC-MD5 :00:02:37
        ISAKMP: encaps is 1 :00:02:37
        ISAKMP: SA life type in seconds :00:02:37
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B :00:02:37
    validate proposal 0 :00:02:37
    .ISAKMP (0:1): atts are acceptable :00:02:37
    ISAKMP (0:1): Checking IPsec proposal 5 :00:02:37
        ISAKMP (0:1): transform 1, IPsec LZS :00:02:37
        :ISAKMP: attributes in transform :00:02:37
        ISAKMP: encaps is 1 :00:02:37
        ISAKMP: SA life type in seconds :00:02:37
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B :00:02:37
    IPSEC(validate_proposal): transform proposal :00:02:37
    prot 4, trans 3, hmac_alg 0) not supported)
ISAKMP (0:1): atts not acceptable. Next payload is 0 :00:02:37
    ISAKMP (0:1): Checking IPsec proposal 6 :00:02:37
        ISAKMP: transform 1, ESP_DES :00:02:37
        :ISAKMP: attributes in transform :00:02:37
        ISAKMP: authenticator is HMAC-SHA :00:02:37
        ISAKMP: encaps is 1 :00:02:37
        ISAKMP: SA life type in seconds :00:02:37
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B :00:02:37
    validate proposal 0 :00:02:37
IPSEC(validate_proposal): transform proposal :00:02:37
    prot 3, trans 2, hmac_alg 2) not supported)
ISAKMP (0:1): atts not acceptable. Next payload is 0 :00:02:37
    (ISAKMP (0:1): skipping next ANDed proposal (6 :00:02:37
    ISAKMP (0:1): Checking IPsec proposal 7 :00:02:37
        ISAKMP: transform 1, ESP_DES :00:02:37
        :ISAKMP: attributes in transform :00:02:37
        ISAKMP: authenticator is HMAC-MD5 :00:02:37
        ISAKMP: encaps is 1 :00:02:37
        ISAKMP: SA life type in seconds :00:02:37
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xC4 0x9B :00:02:37
    validate proposal 0 :00:02:37
    .ISAKMP (0:1): atts are acceptable :00:02:37
    ,IPSEC(validate_proposal_request): proposal part #1 :00:02:37
    ,key eng. msg.) INBOUND local= 172.16.172.40, remote= 171.69.89.129)
    ,(local_proxy= 10.1.0.0/255.255.0.0/0/0 (type=4
    ,(remote_proxy= 10.1.1.10/255.255.255.255/0/0 (type=1
    , protocol= ESP, transform= esp-des esp-md5-hmac
    ,lifedur= 0s and 0kb
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
    validate proposal request 0 :00:02:37
ISAKMP (0:1): processing NONCE payload. message ID = 926518983 :00:02:37
ISAKMP (0:1): processing ID payload. message ID = 926518983 :00:02:37
ISAKMP (0:1): processing ID payload. message ID = 926518983 :00:02:37
```

```

ISAKMP (0:1): asking for 1 spis from ipsec :00:02:37
,ISAKMP (0:1): Node 926518983, Input = IKE_MSG_FROM_PEER :00:02:37
      IKE_QM_EXCH
Old State = IKE_QM_READY New State = IKE_QM_SPI_STARVE

...IPSEC(key_engine): got a queue event :00:02:37
IPSEC(spi_response): getting spi 1746304572 for SA :00:02:37
      from 172.16.172.40 to 171.69.89.129 for prot 3
      (ISAKMP: received ke message (2/1 :00:02:37
CryptoEngine0: generate hmac context for conn id 1 :00:02:37
ISAKMP (0:1): sending packet to 171.69.89.129 (R) QM_IDLE :00:02:37
,ISAKMP (0:1): Node 926518983, Input = IKE_MSG_FROM_IPSEC :00:02:37
      IKE_SPI_REPLY
Old State = IKE_QM_SPI_STARVE New State = IKE_QM_R_QM2

ISAKMP (0:1): received packet from 171.69.89.129 (R) QM_IDLE :00:02:37
CryptoEngine0: generate hmac context for conn id 1 :00:02:37
      ipsec allocate flow 0 :00:02:37
      ipsec allocate flow 0 :00:02:37
      ISAKMP (0:1): Creating IPsec SAs :00:02:37
      inbound SA from 171.69.89.129 to 172.16.172.40 :00:02:37
      (proxy 10.1.1.10 to 10.1.0.0)
      has spi 0x68167E3C and conn_id 2002 and flags 4 :00:02:37
      lifetime of 2147483 seconds :00:02:37
      outbound SA from 172.16.172.40 to 171.69.89.129 :00:02:37
      (proxy 10.1.0.0 to 10.1.1.10)
      has spi -697634356 and conn_id 2003 and flags C :00:02:37
      lifetime of 2147483 seconds :00:02:37
ISAKMP (0:1): deleting node 926518983 error FALSE :00:02:37
      "()"reason "quick mode done (await
,ISAKMP (0:1): Node 926518983, Input = IKE_MSG_FROM_PEER :00:02:37
      IKE_QM_EXCH
Old State = IKE_QM_R_QM2 New State = IKE_QM_PHASE2_COMPLETE

...IPSEC(key_engine): got a queue event :00:02:37
      , : (IPSEC(initialize_sas :00:02:37
, key eng. msg.) INBOUND local= 172.16.172.40, remote= 171.69.89.129)
      , (local_proxy= 10.1.0.0/255.255.0.0/0/0 (type=4
      , (remote_proxy= 10.1.1.10/0.0.0.0/0/0 (type=1
      , protocol= ESP, transform= esp-des esp-md5-hmac
      , lifedur= 2147483s and 0kb
      spi= 0x68167E3C(1746304572), conn_id= 2002, keysize= 0, flags= 0x4
      , : (IPSEC(initialize_sas :00:02:37
, key eng. msg.) OUTBOUND local= 172.16.172.40, remote= 171.69.89.129)
      , (local_proxy= 10.1.0.0/255.255.0.0/0/0 (type=4
      , (remote_proxy= 10.1.1.10/0.0.0.0/0/0 (type=1
      , protocol= ESP, transform= esp-des esp-md5-hmac
      , lifedur= 2147483s and 0kb
      spi= 0xD66AF1CC(3597332940), conn_id= 2003, keysize= 0, flags= 0xC
      , IPSEC(create_sa): sa created :00:02:37
      , (sa) sa_dest= 172.16.172.40, sa_prot= 50)
      , (sa_spi= 0x68167E3C(1746304572
sa_trans= esp-des esp-md5-hmac , sa_conn_id= 2002
      , IPSEC(create_sa): sa created :00:02:37
      , (sa) sa_dest= 171.69.89.129, sa_prot= 50)
      , (sa_spi= 0xD66AF1CC(3597332940
sa_trans= esp-des esp-md5-hmac , sa_conn_id= 2003

```

## [معلومات ذات صلة](#)

- [صفحات دعم منتجات أمان IP \(IPSec\)](#)
- [الدعم الفني - Cisco Systems](#)

ةمچرتل هذه ل و ح

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