

# Configuration IPSec entre les routeurs Cisco IOS et le client VPN Cisco à l'aide des certificats Entrust

## Contenu

[Introduction](#)

[Avant de commencer](#)

[Conventions](#)

[Conditions préalables](#)

[Composants utilisés](#)

[Configurez](#)

[Diagramme du réseau](#)

[Configurations](#)

[Vérifiez](#)

[Dépannez](#)

[Informations connexes](#)

## [Introduction](#)

Ce document explique comment configurer un tunnel VPN d'IPSec entre un routeur de Cisco IOS® et un Client VPN Cisco 3.x utilisant confiez aux Certificats. Cette caractéristique est prise en charge dans des versions de logiciel 12.2(8)T et ultérieures de Cisco IOS. L'exemple de configuration dans ce document met en valeur également la procédure d'inscription de l'autorité de certification (CA) pour le routeur Cisco IOS et l'utilisation de Client VPN Cisco confient en tant que serveur CA.

## [Avant de commencer](#)

### [Conventions](#)

Pour plus d'informations sur les conventions des documents, référez-vous aux [Conventions utilisées pour les conseils techniques de Cisco](#).

### [Conditions préalables](#)

Aucune condition préalable spécifique n'est requise pour ce document.

### [Composants utilisés](#)

Les informations dans ce document sont basées sur les versions de logiciel et de matériel ci-

dessous.

- Une version de logiciel courante 12.2(8)T (image de Cisco IOS de routeur de Cisco 3640 IOS : c3640-ik8o3s-mz.122-8.T)
- Un Client VPN Cisco 4.0.1 sur le Windows 2000 courant PC
- Un serveur de la confiance CA utilisé en tant que serveur CA

Les informations présentées dans ce document ont été créées à partir de périphériques dans un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si vous travaillez dans un réseau opérationnel, assurez-vous de bien comprendre l'impact potentiel de toute commande avant de l'utiliser.

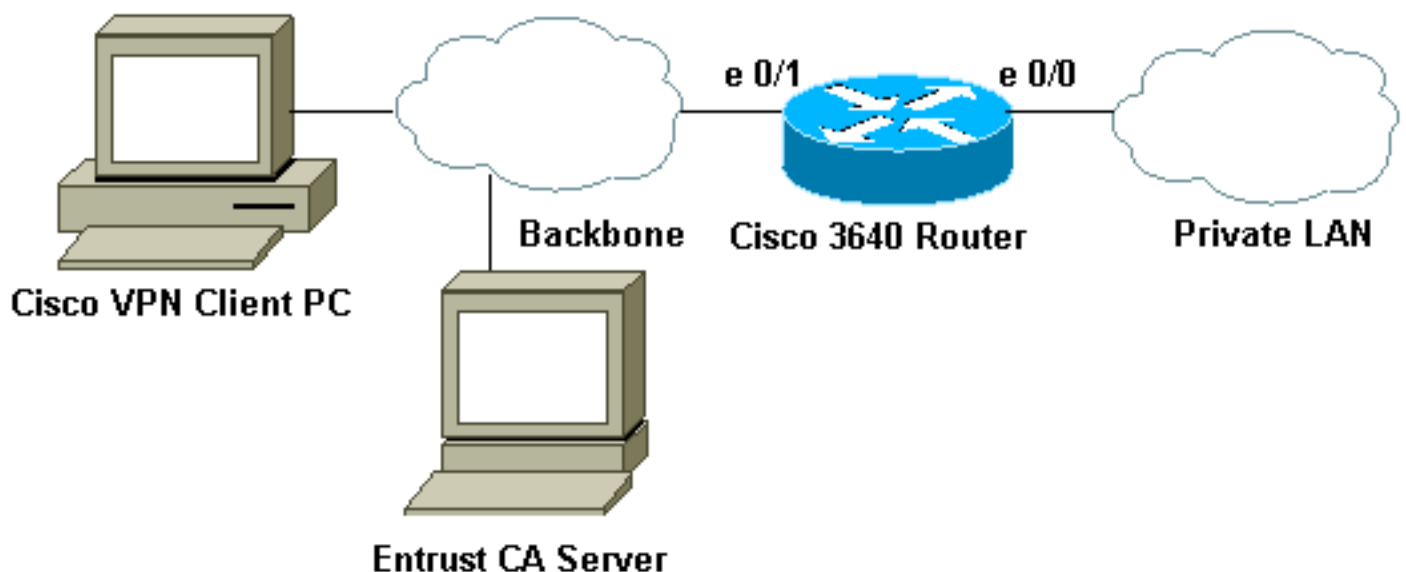
## Configurez

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

**Remarque:** Pour obtenir des informations supplémentaires sur les commandes utilisées dans ce document, utilisez l'[Outil de recherche de commande](#) ([clients enregistrés](#) seulement).

## Diagramme du réseau

Ce document utilise la configuration réseau indiquée dans le diagramme suivant :



## Configurations

Ce document utilise les configurations présentées ci-dessous.

- [Configurations de routeur](#)
- [Inscription de certificat pour le Client VPN Cisco](#)
- [Configurer une connexion VPN sur le Client VPN Cisco](#)

## Configurations de routeur

- [Inscription de certificat sur le routeur 3640 IOS](#)
- [Configuration 3640](#)

## Inscription de certificat sur le routeur 3640 IOS

```

!--- 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.
3640(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 !--- 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.
3640(config)# !--- 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. 3640(config)# Fingerprint: D9CE886E
B4B76115 B7149128 6658E7CA 00:58:17: CRYPTO_PKI: status
= 102: certificate request pending 00:58:39: CRYPTO_PKI:
status = 102: certificate request pending 00:59:42:
%CRYPTO-6-CERTRET: Certificate received from Certificate
Authority

```

## Configuration 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$bfGOfwF7qdKQqZxCIN770 ! 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 31964497 F36E7511 EF09B23D 52CDCD2F 50E471B7
F1FFCB05 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 33323331
37343132 355A810F 32303232 30333233 31383131 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 07410004 10300E1B 0856352E 303A342E 30030204
90300D06 092A8648 86F70D01 01050500 03818100 3C6AB8D8
9E3F140D D5D051AB 7032AF51 BD357804 4D7FA32C EB42D1EA
2AFA1EEF 548C175E FAB9B4C7 DE0E0744 0916FC71 B87768F3
28B605E9 A054900B 5E249835 3112E7FF F0B579F5 F06858F8
5940CA9C E0FC4E98 66C50A40 2ABEAF37 9DB339C0 F98EDC0C
E28C82CD B2465D46 5E3AB18E 0FEEEE09A 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 31273025 06035504 03131E65
6E747275 73745650 4E636F6E 6E656374 6F722045 6E747275
7374504B 4930819F 300D0609 2A864886 F70D0101 01050003
818D0030 81890281 8100AC0B BA3BC6CF 7C303853 C1C191F6
5CD91A41 2F6143B4 6662D7CB A4CD6633 45DBAEC7 7664F88B
D62C5DA9 6087C097 5F498BF5 3DDC7ACF 1F4BFA30 DA112550
841FC5AD 45AEFE65 EA1EB935 473BF5F4 3F6FDE88 E05D7097
FD8C4525 50ECE9F7 4B3EA152 0DDB8867 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	00038181	001423E0	A88F4F28	FF69BD65	F35FDCD7
BE1ACB2C	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	30820310	30820279	A0030201	0202043C
9CC57430	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
31273025	06035504	03131E65	6E747275	73745650	4E636F6E
6E656374	6F722045	6E747275	7374504B	4930819F	300D0609
2A864886	F70D0101	01050003	818D0030	81890281	8100AC87
EF7C0E8E	2120B81F	D231EE87	78CB4238	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	0F3223030
32303332	33323235	3234355A	810F3230	30343034	32393033
32323435	5A301B06	03551D09	04143012	30100609	2A864886
F67D0744	1D310302	0101304F	0603551D	1F044830	463044A0
42A040A4	3E303C31	0B300906	03550406	13027573	310E300C
06035504	0A130563	6973636F	310E300C	06035504	0B130573
6A76706E	310D300B	06035504	03130443	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	10308201	0C300B06
03551D0F	04040302	05A03019	0603551D	11041230	10820E33
3634302E	736A706B	692E636F	6D302B06	03551D10	04243022
800F3230	30323034	30383232	32353436	5A810F32	30303231
32323031	30353534	365A304F	0603551D	1F044830	463044A0
42A040A4	3E303C31	0B300906	03550406	13027573	310E300C
06035504	0A130563	6973636F	310E300C	06035504	0B130573
6A76706E	310D300B	06035504	03130443	524C3130	1F060355
1D230418	30168014	F7931A99	D0E44769	928CC0A9	FF647DF5
3E627F5A	301D0603	551D0E04	16041413	C98FDF5A	AEF253F0

```

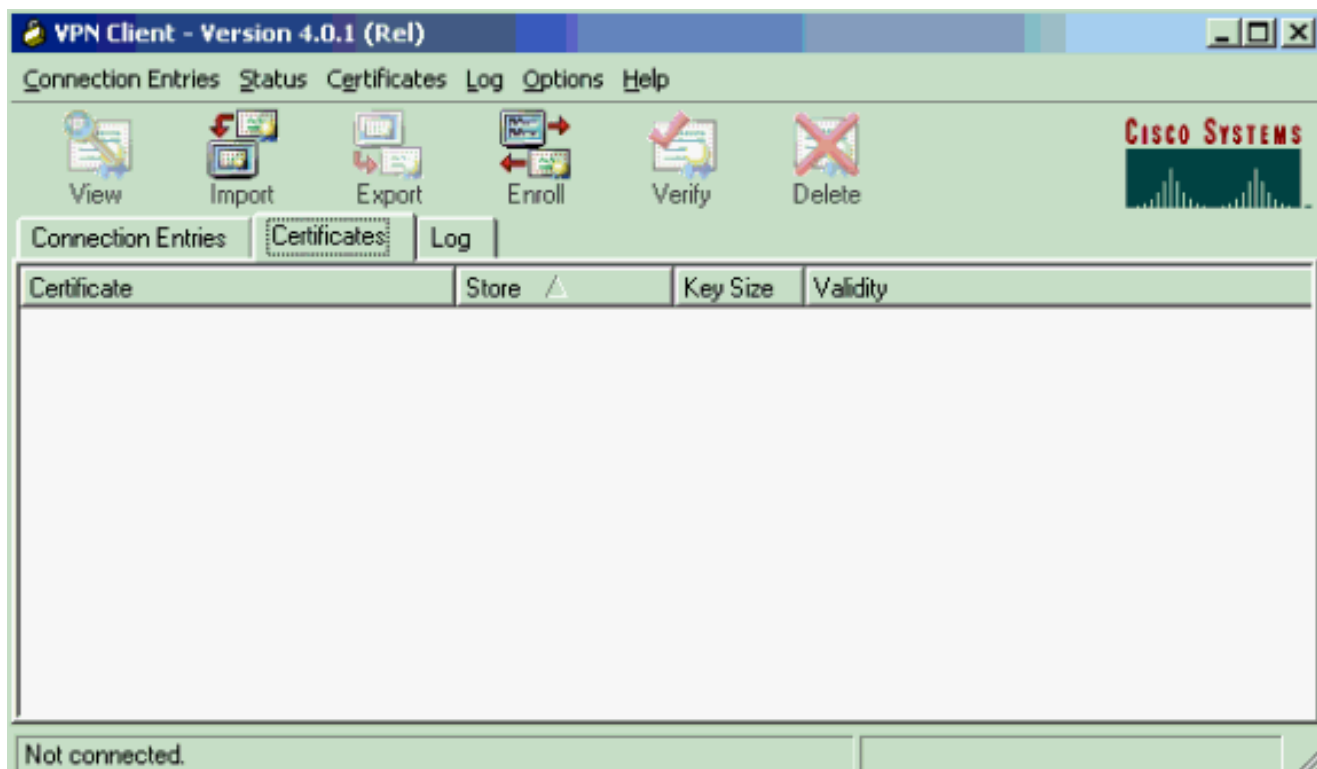
84D39E4B 44A10B1F A2622730 09060355 1D130402 30003019
06092A86 4886F67D 07410004 0C300A1B 0456352E 30030204
B0300D06 092A8648 86F70D01 01050500 03818100 671FC222
EADDC030 F8053380 5EEE91E5 69D3F5A7 5AC037F9 539EF9CB
25ECD678 365A954A FFD3141B 17DEEB9F 1DFE6F97 8B8FDD18
47458858 A0517D21 2EE68C30 F359C5F9 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

```

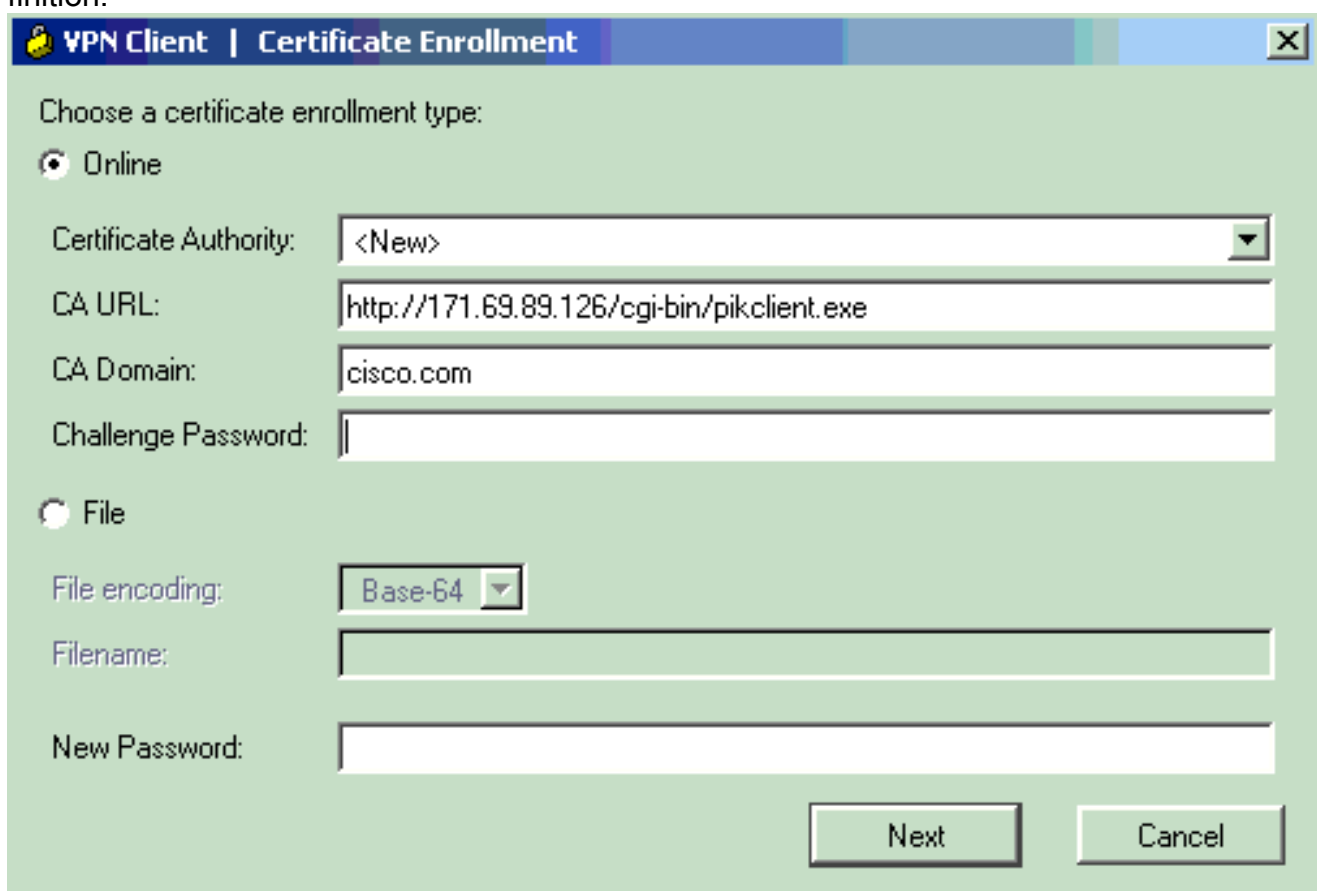
## Inscription de certificat pour le Client VPN Cisco

Les captures d'écran suivantes expliquent les procédures utilisées pour s'inscrire le Client VPN Cisco pour des Certificats Entrust. Dans ce cas, nous avons utilisé l'inscription Fondé(e) sur le réseau.

1. Lancez le client vpn, sélectionnez l'onglet de Certificats, et le clic s'inscrivent.



2. Sélectionnez **en ligne** comme type d'inscription de certificat, puis complétez les champs appropriés pour l'URL, le domaine, et le mot de passe. Cliquez sur Next quand vous êtes de finition.



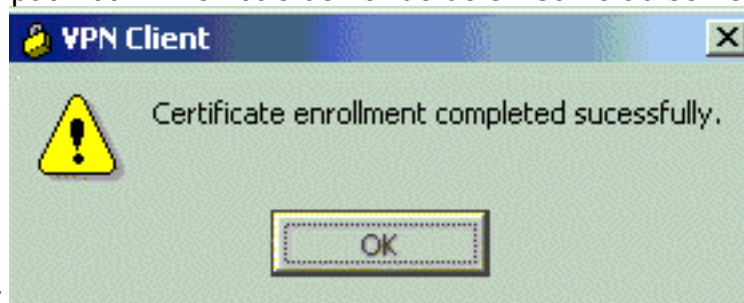
3. Écrivez vos informations dans les domaines de certificat. Si vous devez éditer n'importe quelles informations sur l'écran antérieur, cliquez sur **de retour**. Autrement, le clic **s'inscrivent** quand vous êtes de finition.

The screenshot shows a dialog box titled "VPN Client | Certificate Enrollment". It contains a form with the following fields and values:

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

At the bottom of the dialog box, there are three buttons: "Back", "Enroll", and "Cancel".

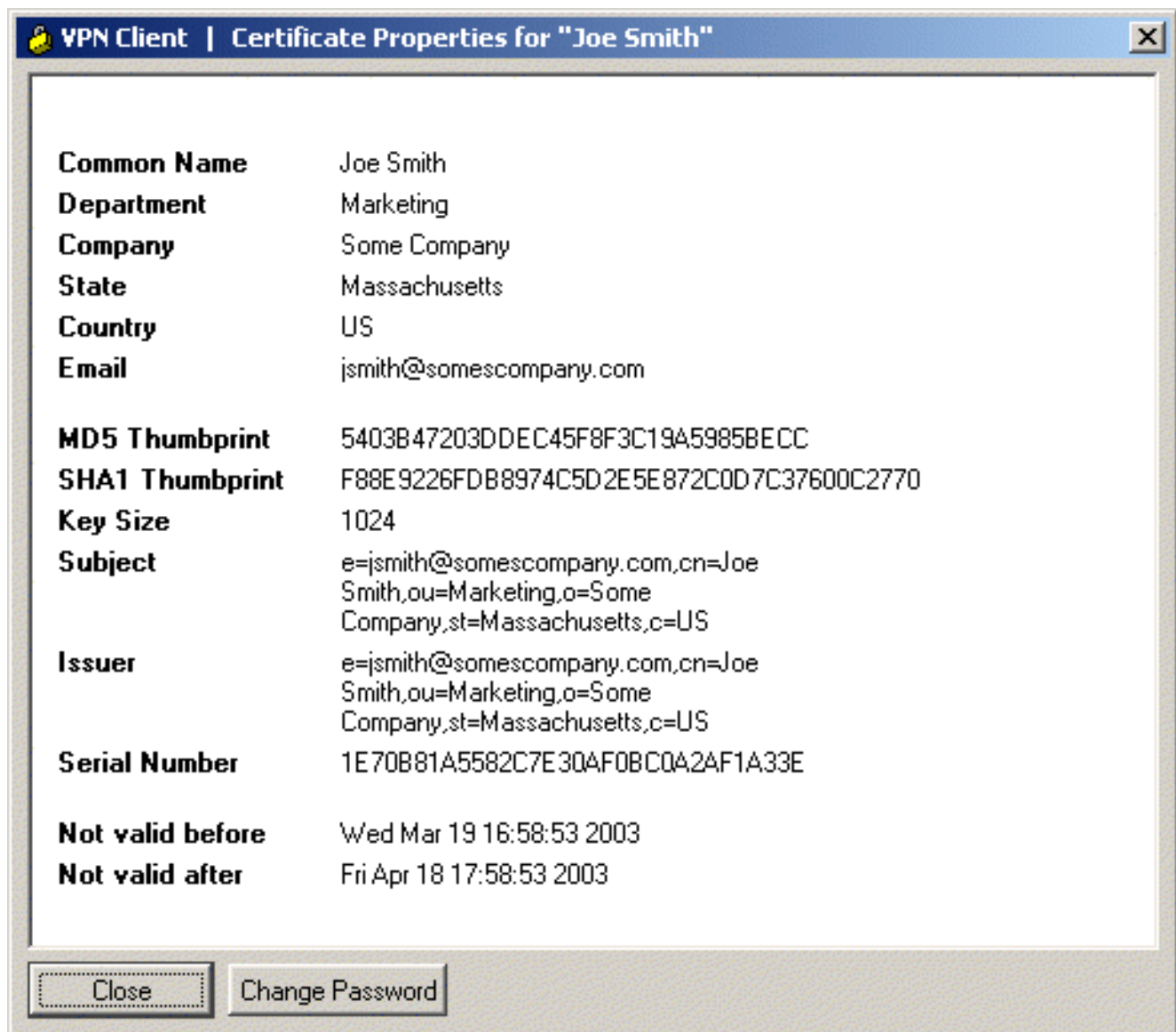
4. Quand la fenêtre d'état d'inscription confirme votre demande de s'inscrire au serveur CA,



cliquez sur OK pour continuer.

5. Après l'inscription, le client vpn devrait recevoir un certificat personnel, un certificat racine CA, et deux Certificats de RA. L'écran de certificat numérique vérifie le certificat de client vpn. Pour visualiser le certificat, allez aux **Certificats > à la vue**. Le certificat devrait sembler semblable à l'exemple suivant.

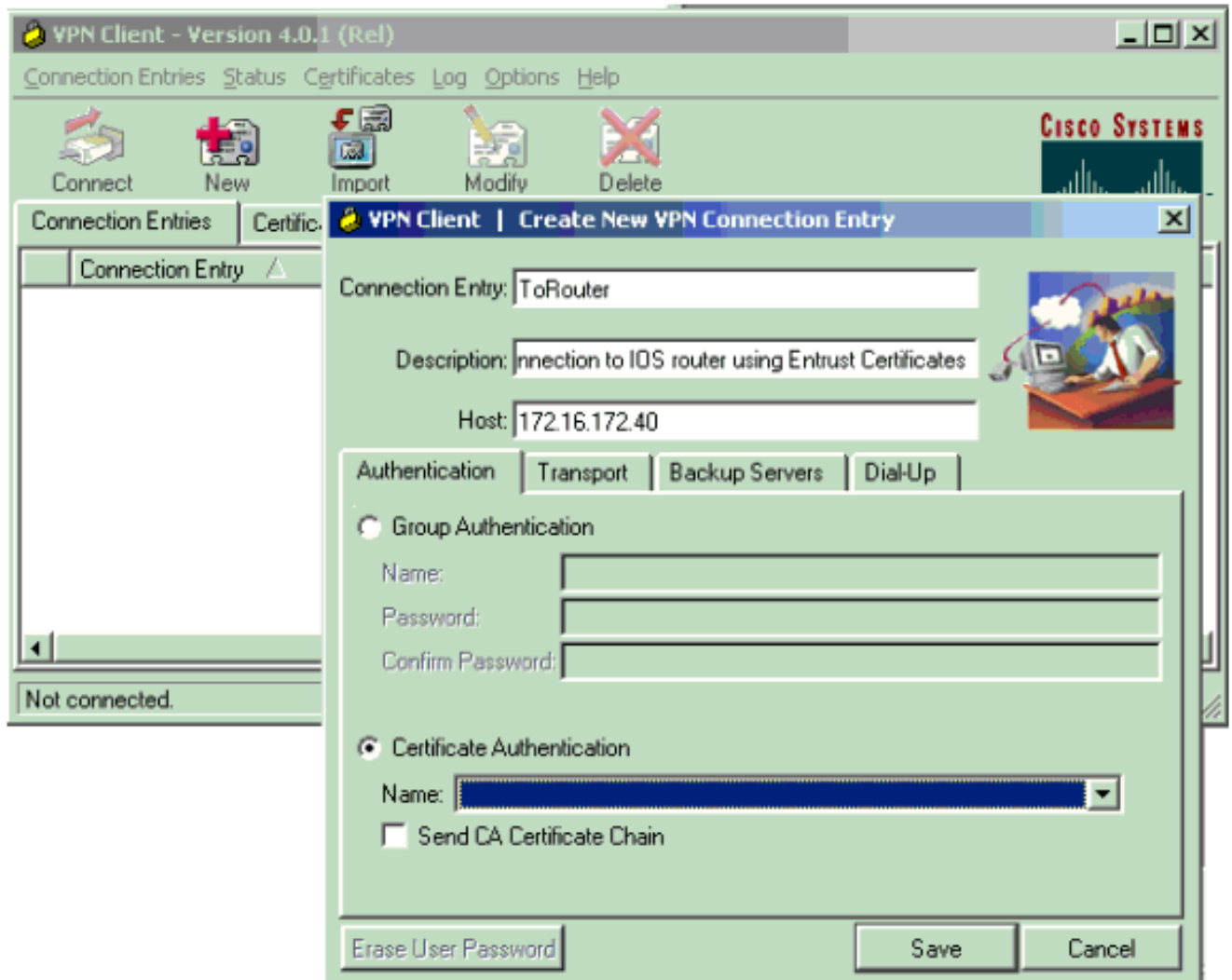




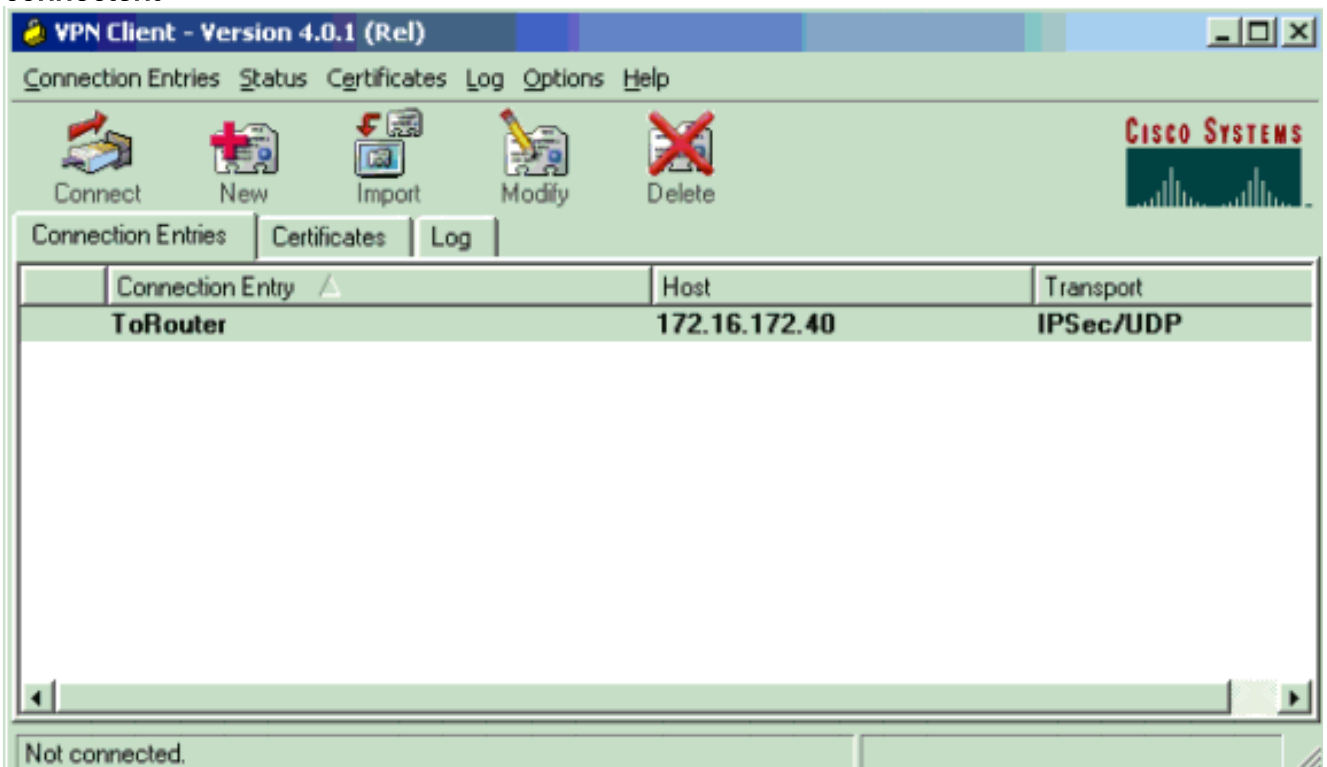
### [Configurer une connexion VPN sur le Client VPN Cisco](#)

Les captures d'écran suivantes expliquent comment configurer une nouvelle connexion sur le Client VPN Cisco au routeur Cisco IOS.

1. Lancez le client vpn, sélectionnez l'onglet d'entrées de connexion, et cliquez sur New pour créer une nouvelle connexion.
2. Écrivez le nom de la connexion, la description, et l'adresse IP d'hôte. Le champ d'authentification de certificat sera automatiquement rempli avec les informations sur le client vpn. **Sauvegarde de clic** quand vous êtes de finition.



3. Pour se connecter, sélectionnez la nouvelle entrée de connexion et puis cliquez sur **se connectent**.



[Vérifiez](#)

Cette section présente des informations que vous pouvez utiliser pour vous assurer que votre configuration fonctionne correctement.

Certaines commandes **show** sont prises en charge par l'[Output Interpreter Tool \(clients enregistrés\)](#) uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

- 3640#**show crypto isakmp sa** dst src state conn-id slot 172.16.172.40 171.69.89.129 QM\_IDLE 1 0
- 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 pcp 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 pcp 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 1 Ethernet0/1 172.16.172.40 set HMAC\_SHA+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 0 2002 Ethernet0/1 172.16.172.40 set HMAC\_MD5+DES\_56\_CB 0 20 2003 Ethernet0/1 172.16.172.40 set HMAC\_MD5+DES\_56\_CB 4 0

## [Dépannez](#)

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Est ci-dessous la sortie de débogage d'une négociation fonctionnante d'IKE collectée sur le routeur de Cisco 3640. Ce qui suit met au point a été activé.

```
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# 00:02:30: 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 crypto_ikmp_config_initialize_sa, count 1 00:02:30: ISAKMP (0:1): Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH Old State = IKE_READY New State = IKE_R_MM1 00:02:30: 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): 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 00:02:31: 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 Old State = IKE\_R\_MM1 New State = IKE\_R\_MM1 00:02:31: 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 Old State = IKE\_R\_MM1 New State = IKE\_R\_MM2 00:02:31: 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 Old State = IKE\_R\_MM2 New State = IKE\_R\_MM3 00:02:31: 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 Old State = IKE\_R\_MM3 New State = IKE\_R\_MM3 00:02:31: 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 Old State = IKE\_R\_MM3 New State = IKE\_R\_MM4 00:02:31: 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 Old State = IKE\_R\_MM4 New State = IKE\_R\_MM5 00:02:31: 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, base=CN = CRL1, OU = sjvnp, O = cisco, C = us, attribute= : scope=2, filter=cn=CRL1 00:02:31: CRYPTO\_PKI: ldap\_bind() succeeded. 00:02:32: 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: 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 = sjvnp 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 = sjvnp, 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 spi 0, message ID = 0, sa = 62D99794 00:02:32: ISAKMP (0:1): Process initial contact, bring down existing phase 1 and 2 SA's 00:02:32: 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 Old State = IKE\_R\_MM5 New State = IKE\_R\_MM5 00:02:32: 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 shared with 171.69.89.129 00:02:32: ISAKMP (0:1): SA is doing RSA signature authentication plus XAUTH using id type ID\_FQDN 00:02:32: ISAKMP (1):

ID payload next-payload : 6 type : 2 protocol : 17 port : 500 length : 18 00:02:32: 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 Old State = IKE\_R\_MM5 New State = IKE\_P1\_COMPLETE **00:02:32: ISAKMP (0:1):  
Need XAUTH** 00:02:32: ISAKMP (0:1): Input = IKE\_MSG\_INTERNAL, IKE\_PHASE1\_COMPLETE Old State =  
IKE\_P1\_COMPLETE New State = IKE\_XAUTH\_AAA\_START\_LOGIN\_AWAIT 00:02:32: 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. ID = -670289125 00:02:32: 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 Old State =  
IKE\_XAUTH\_AAA\_START\_LOGIN\_AWAIT New State = IKE\_XAUTH\_REQ\_SENT 00:02:36: 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. message ID = -670289125 00:02:36: 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 reason "done with xauth request/reply exchange" 00:02:36: ISAKMP (0:1):  
Input = IKE\_MSG\_FROM\_PEER, IKE\_CFG\_REPLY Old State = IKE\_XAUTH\_REQ\_SENT New State =  
IKE\_XAUTH\_AAA\_CONT\_LOGIN\_AWAIT 00:02:36: 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. ID = -1610220250 00:02:36: 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 Old State =  
IKE\_XAUTH\_AAA\_CONT\_LOGIN\_AWAIT New State = IKE\_XAUTH\_SET\_SENT 00:02:36: 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. message ID = -1610220250 00:02:36: 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 reason "done with transaction"  
**00:02:36: ISAKMP (0:1): Input = IKE\_MSG\_FROM\_PEER, IKE\_CFG\_ACK Old State = IKE\_XAUTH\_SET\_SENT  
New State = IKE\_P1\_COMPLETE** 00:02:36: ISAKMP (0:1): Input = IKE\_MSG\_INTERNAL,  
IKE\_PHASE1\_COMPLETE Old State = IKE\_P1\_COMPLETE New State = IKE\_P1\_COMPLETE 00:02:36: 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. message ID = 1789347264 00:02:36: 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 Old State = IKE\_P1\_COMPLETE New State  
= IKE\_CONFIG\_AUTHOR\_AAA\_AWAIT 00:02:36: 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 to use the address: 86394 00:02:36: ISAKMP: Sending APPLICATION\_VERSION string:  
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 00:02:36: 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 mask 255.255.0.0, protocol 0, src port 0, dst port 0 00:02:36: 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. ID = 1789347264 **00:02:36: 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 Old State =  
IKE\_CONFIG\_AUTHOR\_AAA\_AWAIT New State = IKE\_P1\_COMPLETE 00:02:36: 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 (prot 3, trans 3, hmac\_alg 1) not supported 00:02:36: 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 (prot 3, trans 3, hmac\_alg 2) not supported 00:02:36: 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 (prot 3, trans 3, hmac\_alg 1) not supported 00:02:36: 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 (prot 3, trans 3, hmac\_alg 2) not supported 00:02:36: 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 (prot 4, trans 3, hmac\_alg 0) not supported 00:02:36: 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 (prot 3, trans 2, hmac\_alg 2) not supported 00:02:36: 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, (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 00:02:36: 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, IKE\_QM\_EXCH Old State = IKE\_QM\_READY New State = IKE\_QM\_SPI\_STARVE 00:02:36: IPSEC(key\_engine): got a queue event... 00:02:36: IPSEC(spi\_response): getting spi 1289658319 for SA from 172.16.172.40 to 171.69.89.129 for prot 3 00:02:36: 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, IKE\_SPI\_REPLY Old State = IKE\_QM\_SPI\_STARVE New State = IKE\_QM\_R\_QM2 00:02:36: 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 (proxy 10.1.1.10 to 172.16.172.40) 00:02:36: 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 (proxy 172.16.172.40 to 10.1.1.10) 00:02:36: 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 reason "quick mode done (await())"  
00:02:36: ISAKMP (0:1): Node -1460041169, Input = IKE\_MSG\_FROM\_PEER, IKE\_QM\_EXCH Old State =  
IKE\_QM\_R\_QM2 New State = IKE\_QM\_PHASE2\_COMPLETE 00:02:36: IPSEC(key\_engine): got a queue  
event... 00:02:36: IPSEC(initialize\_sas): , (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 00:02:36:  
IPSEC(initialize\_sas): , (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 00:02:36: IPSEC(create\_sa): sa  
created, (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 00:02:36: IPSEC(create\_sa): sa created, (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 00:02:36: ISAKMP: received ke message (4/1) 00:02:36: ISAKMP: Locking CONFIG  
struct 0x62D99D98 for crypto\_ikmp\_config\_handle\_kei\_mess, count 2 00:02:37: 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 (prot 3,  
trans 3, hmac\_alg 1) not supported 00:02:37: 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 (prot 3,  
trans 3, hmac\_alg 2) not supported 00:02:37: 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 (prot 3,  
trans 3, hmac\_alg 1) not supported 00:02:37: 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 (prot 3, trans 3, hmac\_alg 2) not supported 00:02:37: 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, IPPCP 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 (prot 4, trans 3, hmac\_alg 0) not supported 00:02:37: 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 (prot 3, trans 2, hmac\_alg 2)  
not supported 00:02:37: 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, (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 00:02:37: 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, IKE_QM_EXCH Old State
= IKE_QM_READY New State = IKE_QM_SPI_STARVE 00:02:37: IPSEC(key_engine): got a queue event...
00:02:37: IPSEC(spi_response): getting spi 1746304572 for SA from 172.16.172.40 to 171.69.89.129
for prot 3 00:02:37: 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, IKE_SPI_REPLY Old State =
IKE_QM_SPI_STARVE New State = IKE_QM_R_QM2 00:02:37: 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 (proxy 10.1.1.10 to 10.1.0.0) 00:02:37:
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 (proxy 10.1.0.0 to 10.1.1.10) 00:02:37: 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 reason "quick mode done (await())" 00:02:37: ISAKMP
(0:1): Node 926518983, Input = IKE_MSG_FROM_PEER, IKE_QM_EXCH Old State = IKE_QM_R_QM2 New
State = IKE_QM_PHASE2_COMPLETE 00:02:37: IPSEC(key_engine): got a queue event... 00:02:37:
IPSEC(initialize_sas): , (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 00:02:37: IPSEC(initialize_sas): ,
(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 00:02:37: IPSEC(create_sa): sa created, (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 00:02:37: IPSEC(create_sa): sa created, (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
```

## [Informations connexes](#)

- [Pages de support produit de sécurité IP \(IPSec\)](#)
- [Support technique - Cisco Systems](#)