Configuration des autorités de certification à identité multiple sur les routeurs Cisco IOS

Contenu

Introduction

Ce document décrit comment configurer des Routeurs de Cisco IOS® pour prendre en charge les autorités de certification de multiple-identité (CA). Dans certaines situations, comme un projet commun entre deux sociétés ou deux unités commerciales, les Routeurs sur chaque (qui s'inscrivent aux CAs différents qui n'ont aucune relations de confiance) besoin latéral de communiquer utilisant IPSec VPN. Le routeur de périphérie pourrait devoir avoir deux ensembles de certificats d'identité à communiquer avec des Routeurs sur les deux domaines CA. Ce document décrit explique comment s'inscrire un routeur de Cisco à différents serveurs CA pour obtenir de plusieurs certificats d'identité ; la vérification est fournie utilisant un exemple simple.

Conditions préalables

Conditions requises

La caractéristique est introduite dans la version de logiciel 12.2(2)T de Cisco IOS®. Les versions antérieures du logiciel ne pourront pas utiliser la configuration illustrée dans ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de

logiciel suivantes :

- Routeurs de Cisco 7200 avec le Logiciel Cisco IOS version 12.2(4)T1
- Serveur de Microsoft CA sur le serveur de Windows 2000
- Confiez au serveur CA sur serveur windows nt

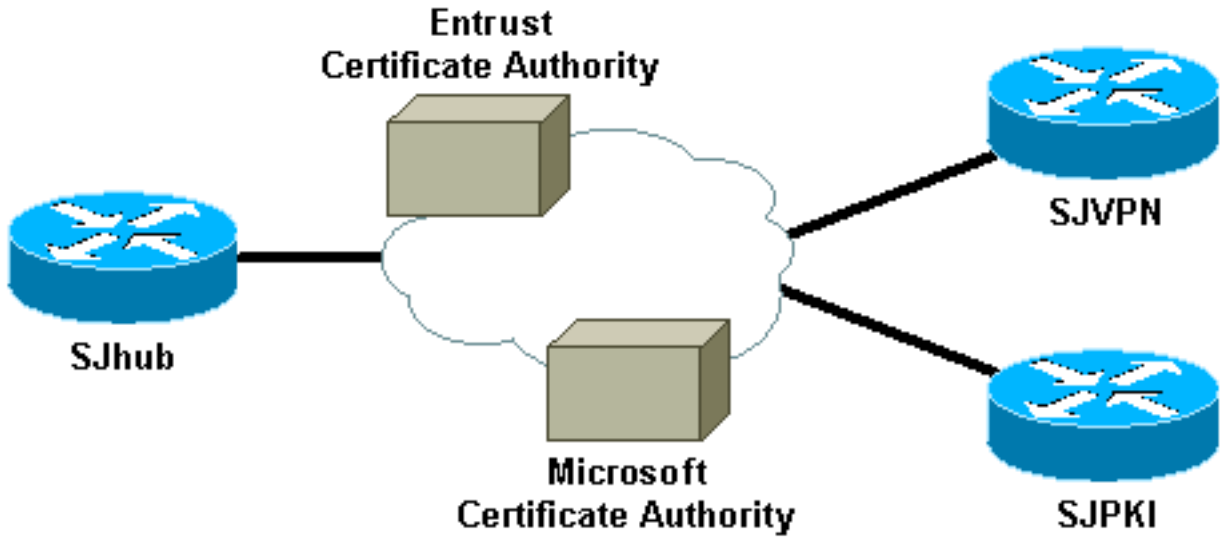
Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous aux Conventions relatives aux conseils techniques Cisco.

Diagramme du réseau

Dans le diagramme affiché ci-dessous, SJhub, SJVPN, et SJPKI sont trois Routeurs de Cisco 7200 se connectant au réseau fédérateur. SJhub est le routeur concentrateur, avec des Certificats de multiple-identité des serveurs de la confiance CA et du Microsoft CA qui résident dans le réseau fédérateur. SJVPN s'inscrit au serveur de la confiance CA, et SJPKI s'inscrit à Microsoft CA le serveur.



Configurer le routeur Cisco IOS pour obtenir de plusieurs Certificats

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).

Remarque: Une partie du résultat présenté dans la procédure ci-dessous a été enveloppée aux plusieurs lignes pour des raisons d'espace.

1. Générez les clés RSA sur le routeur.SJhub#**configure terminal** Enter configuration commands, one per line. End with CNTL/Z. SJhub(config)#**ip domain-name sjtac.com** SJhub(config)#**crypto key generate rsa** The name for the keys will be: SJhub.sjtac.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 RSA keys ... [OK]
2. Définissez le premier crypto ca identity sur le routeur. Le serveur utilisé ici est un serveur de la confiance CA.SJhub(config)#**crypto ca identity EntrustPKI** SJhub(ca-identity)#**enrollment url http://171.69.89.16** SJhub(ca-identity)#**enrollment mode ra** SJhub(ca-identity)#**query url ldap://171.69.89.16** SJhub(ca-identity)#**exit**
3. Obtenez le CA et les Certificats d'autorité d'enregistrement (RA) et inscrivez-vous le routeur à la confiance CA.SJhub(config)#**crypto ca authenticate EntrustPKI** Certificate has the following attributes: Fingerprint: 1FCDF2C8 2DEDA6AC 4819D4C4 B4CFF2F5 % Do you accept this certificate? [yes/no]: y SJhub(config)#**crypto ca enroll EntrustPKI** % % Start certificate enrollment .. % Create a challenge password. You will need to verbally provide this password to the CA Administrator in order to revoke your certificate. For security reasons your password will not be saved in the configuration. Please make a note of it. Password: Re-enter password: % The subject name in the certificate will be: SJhub.sjtac.com % Include the router serial number in the subject name? [yes/no]: n % Include an IP address in the subject name? [yes/no]: n Request certificate from CA? [yes/no]: y % Certificate request sent to Certificate Authority % The certificate request fingerprint will be displayed. % The 'show crypto ca certificate' command will also show the fingerprint. SJhub(config)# Fingerprint: B530BB30 70D2C565 E6F20A88 BB86A75A
4. Vérifiez les Certificats.SJhub#**show crypto ca certificates** Certificate Status: Available Certificate Serial Number: 3B2FD63F Key Usage: General Purpose Issuer: OU = sjvpn O = cisco C = us Subject Name Contains: Name: SJhub.sjtac.com CRL Distribution Point: CN = CRL1, OU = sjvpn, O = cisco, C = us Validity Date: start date: 21:48:52 UTC Jan 9 2002 end date: 22:18:52 UTC Jan 9 2003 Associated Identity: EntrustPKI RA Signature Certificate Status: Available Certificate Serial Number: 3B2FD319 Key Usage: Signature Issuer: OU = sjvpn O = cisco C = us Subject: CN = First Officer OU = sjvpn O = cisco C = us CRL Distribution Point: CN = CRL1, OU = sjvpn, O = cisco, C = us Validity Date: start date: 22:03:31 UTC Jun 19 2001 end date: 22:33:31 UTC Jun 19 2004 Associated Identity: EntrustPKI RA KeyEncipher Certificate Status: Available Certificate Serial Number: 3B2FD318 Key Usage: Encryption Issuer: OU = sjvpn O = cisco C = us Subject: CN = First Officer OU = sjvpn O = cisco C = us CRL Distribution Point: CN = CRL1, OU = sjvpn, O = cisco, C = us Validity Date: start date: 22:03:31 UTC Jun 19 2001 end date: 22:33:31 UTC Jun 19 2004 Associated Identity: EntrustPKI CA Certificate Status: Available Certificate Serial Number: 3B2FD307 Key Usage: General Purpose Issuer: OU = sjvpn O = cisco C = us Subject: OU = sjvpn O = cisco C = us CRL Distribution Point: CN = CRL1, OU = sjvpn, O = cisco, C = us Validity Date: start date: 22:02:40 UTC Jun 19 2001 end date: 22:32:40 UTC Jun 19 2021 Associated Identity: EntrustPKI
5. Définissez le crypto ca identity du deuxième CA sur le routeur. Un serveur de Microsoft CA est utilisé ici.SJhub(config)#**crypto ca identity MicrosoftCA** SJhub(ca-identity)#**enrollment url http://171.69.89.182:80/certsrv/mscep/mscep.$** SJhub(ca-identity)#**enrollment mode ra** SJhub(ca-identity)#**query url ldap://171.69.89.182** SJhub(ca-identity)#**exit**
6. Obtenez les Certificats CA et de RA du serveur de Microsoft CA.SJhub(config)#**crypto ca authenticate MicrosoftCA** Certificate has the following attributes: Fingerprint: 5FC47E85 9A2724A2 7242F172 BFB87F7E % Do you accept this certificate? [yes/no]: y
7. Inscrivez-vous à Microsoft CA le serveur et obtenez le certificat d'identité du routeur.SJhub(config)#**crypto ca enroll MicrosoftCA** % % Start certificate enrollment .. % Create a challenge password. You will need to verbally provide this password to the CA Administrator in order to revoke your certificate. For security reasons your password will not be saved in the configuration. Please make a note of it. Password: Re-enter password: % The subject name in the certificate will be: SJhub.sjtac.com % Include the router serial number in the subject name? [yes/no]: n % Include an IP address in the subject name? [yes/no]: n Request certificate from CA? [yes/no]: y % Certificate request sent to Certificate Authority % The certificate request fingerprint will be displayed. % The 'show crypto ca certificate' command will also show the fingerprint. SJhub(config)# Fingerprint: 4046052F 2D32A725 235D55E9 694DF3EA
8. Vérifiez les Certificats. Vous devriez voir deux ensembles de Certificats.SJhub#**show crypto ca certificates** Certificate Status: Available Certificate Serial Number: 132BD14C000000000000B

```
Key Usage: General Purpose Issuer: CN = SJPKICA OU = SJPKI O = SJTAC L = SAN JOSE ST = CA C
= US Subject Name Contains: Name: SJhub.sjtac.com CRL Distribution Point:
ldap:///CN=SJPKICA,CN=sjvpnmspki,CN=CDP,CN=Public%20Key%20Services, CN=Services,
CN=Configuration,DC=sjpki, DC=com?certificateRevocationList?base?
objectclass=cRLDistributionPoint Validity Date: start date: 18:36:23 UTC Jan 13 2002 end
date: 18:36:23 UTC Jan 13 2004 Associated Identity: MicrosoftCA RA Signature Certificate
Status: Available Certificate Serial Number: 054E60AD000000000002 Key Usage: Signature
Issuer: CN = SJPKICA OU = SJPKI O = SJTAC L = SAN JOSE ST = CA C = US Subject: CN = SJVPNRA
OU = SJPKI O = SJTAC L = SAN JOSE ST = CA C = US CRL Distribution Point:
ldap:///CN=SJPKICA,CN=sjvpnmspki,CN=CDP,CN=Public%20Key%20Services,
CN=Services,CN=Configuration,DC=sjpki, DC=com?certificateRevocationList?base?
objectclass=cRLDistributionPoint Validity Date: start date: 01:59:27 UTC Jan 11 2002 end
date: 01:59:27 UTC Jan 11 2004 Associated Identity: MicrosoftCA RA KeyEncipher Certificate
Status: Available Certificate Serial Number: 054E63CE000000000003 Key Usage: Encryption
Issuer: CN = SJPKICA OU = SJPKI O = SJTAC L = SAN JOSE ST = CA C = US Subject: CN = SJVPNRA
OU = SJPKI O = SJTAC L = SAN JOSE ST = CA C = US CRL Distribution Point:
ldap:///CN=SJPKICA,CN=sjvpnmspki,CN=CDP,CN=Public%20Key%20Services,
CN=Services,CN=Configuration,DC=sjpki, DC=com?certificateRevocationList?base?
objectclass=cRLDistributionPoint Validity Date: start date: 01:59:28 UTC Jan 11 2002 end
date: 01:59:28 UTC Jan 11 2004 Associated Identity: MicrosoftCA CA Certificate Status:
Available Certificate Serial Number: 091B47AEE8CFE2A94D3E8B38F292F5AF Key Usage: General
Purpose Issuer: CN = SJPKICA OU = SJPKI O = SJTAC L = SAN JOSE ST = CA C = US Subject: CN =
SJPKICA OU = SJPKI O = SJTAC L = SAN JOSE ST = CA C = US CRL Distribution Point:
ldap:///CN=SJPKICA,CN=sjvpnmspki,CN=CDP,CN=Public%20Key%20Services,
CN=Services,CN=Configuration,DC=sjpki, DC=com?certificateRevocationList?base?
objectclass=cRLDistributionPoint Validity Date: start date: 01:51:39 UTC Jan 11 2002 end
date: 02:00:04 UTC Jan 11 2007 Associated Identity: MicrosoftCA CA Certificate Status:
Available Certificate Serial Number: 3B2FD307 Key Usage: General Purpose Issuer: OU = sjvpn
O = cisco C = us Subject: OU = sjvpn O = cisco C = us CRL Distribution Point: CN = CRL1, OU
= sjvpn, O = cisco, C = us Validity Date: start date: 22:02:40 UTC Jun 19 2001 end date:
22:32:40 UTC Jun 19 2021 Associated Identity: EntrustPKI RA KeyEncipher Certificate Status:
Available Certificate Serial Number: 3B2FD318 Key Usage: Encryption Issuer: OU = sjvpn O =
cisco C = us Subject: CN = First Officer OU = sjvpn O = cisco C = us CRL Distribution
Point: CN = CRL1, OU = sjvpn, O = cisco, C = us Validity Date: start date: 22:03:31 UTC Jun
19 2001 end date: 22:33:31 UTC Jun 19 2004 Associated Identity: EntrustPKI RA Signature
Certificate Status: Available Certificate Serial Number: 3B2FD319 Key Usage: Signature
Issuer: OU = sjvpn O = cisco C = us Subject: CN = First Officer OU = sjvpn O = cisco C = us
CRL Distribution Point: CN = CRL1, OU = sjvpn, O = cisco, C = us Validity Date: start date:
22:03:31 UTC Jun 19 2001 end date: 22:33:31 UTC Jun 19 2004 Associated Identity: EntrustPKI
Certificate Status: Available Certificate Serial Number: 3B2FD63F Key Usage: General
Purpose Issuer: OU = sjvpn O = cisco C = us Subject Name Contains: Name: SJhub.sjtac.com
CRL Distribution Point: CN = CRL1, OU = sjvpn, O = cisco, C = us Validity Date: start date:
21:48:52 UTC Jan 9 2002 end date: 22:18:52 UTC Jan 9 2003 Associated Identity: EntrustPKI
```

Vérifiez

Cette section emploie une configuration simple pour vérifier comment les Routeurs IOS traitent de plusieurs certificats d'identité. Le schéma de réseau ci-dessus affiche trois 7200 Routeurs formant un topologie de réseau hub-and-spoke. Le routeur concentrateur (SJhub) a deux certificats d'identité — un d'un serveur de la confiance CA et un d'un serveur de Microsoft CA. Le routeur en étoile (SJVPN) fait confier un certificat d'identité de la même chose au serveur CA, et à l'autre routeur en étoile (SJPKI) a un certificat d'identité du même serveur de Microsoft CA. Dans cet exemple, le routeur concentrateur simule le point joignant de deux sociétés dans un projet commun ; avec l'aide du support de la multiple-identité CA, le hub peut communiquer avec l'un ou l'autre de côté quoique les rais soient inscrits au CAs différent.

Exemples de configuration

Les configurations de tous les Routeurs sont répertoriées ci-dessous comme référence.

- SJhub
- SJVPN
- SJPKI

SJhub (routeur concentrateur)

```
SJhub#write terminal Building configuration... Current
configuration : 19665 bytes ! ! Last configuration
change at 18:40:55 UTC Sun Jan 13 2002 ! NVRAM config
last updated at 18:41:45 UTC Sun Jan 13 2002 ! version
12.2 no parser cache service timestamps debug uptime
service timestamps log uptime no service password-
encryption ! hostname SJhub ! enable password cisco ! ip
subnet-zero ip cef ! ! ip telnet source-interface
Loopback88 no ip domain-lookup ip domain-name sjtac.com
! ip audit notify log ip audit po max-events 100 ip ssh
time-out 120 ip ssh authentication-retries 3 ! crypto ca
identity EntrustPKI enrollment mode ra enrollment url
http://171.69.89.16:80 query url ldap://171.69.89.16 !
crypto ca identity MicrosoftCA enrollment mode ra
enrollment url
http://171.69.89.182:80/certsrv/mscep/mscep.dll query
url ldap://171.69.89.182 crl optional crypto ca
certificate chain EntrustPKI certificate ca 3B2FD307
308202E4 3082024D A0030201 0202043B 2FD30730 0D06092A
864886F7 0D010105 0500302D 310B3009 06035504 06130275
73310E30 0C060355 040A1305 63697363 6F310E30 0C060355
040B1305 736A7670 6E301E17 0D303130 36313932 32303234
305A170D 32313036 31393232 33323430 5A302D31 0B300906
03550406 13027573 310E300C 06035504 0A130563 6973636F
310E300C 06035504 0B130573 6A76706E 30819F30 0D06092A
864886F7 0D010101 05000381 8D003081 89028181 00E8C25B
EDF4A6EE A352B142 C16578F4 FBDAF45E 4F2F7733 8D2B8879
96138C63 1DB713BF 753BF845 2D7E600F AAF4D75B 9E959513
BB13FF13 36696F48 86C464F2 CF854A66 4F8E83F8 025F216B
A44D4BB2 39ADD1A5 1BCCF812 09A19BDC 468EEAE1 B6C2A378
69C81348 1A9CD61C 551216F2 8B168FBB 94CBEF37 E1D9A8F7
80BBC17F D1020301 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 30303130 36313932 32303234
305A810F 32303231 30363139 32323332 34305A30 0B060355
1D0F0404 03020106 301F0603 551D2304 18301680 1446C160
9CDBEA53 EE80A480 601A9658 3B0DF80D 2F301D06 03551D0E
04160414 46C1609C DBEA53EE 80A48060 1A96583B 0DF80D2F
300C0603 551D1304 05300301 01FF301D 06092A86 4886F67D
07410004 10300E1B 0856352E 303A342E 30030204 90300D06
092A8648 86F70D01 01050500 03818100 7E3DBAC4 8CAE7D5A
B19C0625 8780D222 F965A1A2 C0C25B84 CBC5A203 BF50FAC4
9656699A 52D8CB46 40776237 87163118 8F3C0F47 D2CAA36B
6AB34F99 AB71269E 78C0AC10 DA0B9EC5 AE448B46 701254CF
3EBC64C1 5DBB2EE5 56C0140B B0C83497 D79FB148 80018F51
3A4B6174 590B85AA 9CE3B391 629406AA 7CE9CC0D 01593E6B
quit certificate ra-encrypt 3B2FD318 308202D0 30820239
A0030201 0202043B 2FD31830 0D06092A 864886F7 0D010105
0500302D 310B3009 06035504 06130275 73310E30 0C060355
040A1305 63697363 6F310E30 0C060355 040B1305 736A7670
6E301E17 0D303130 36313932 32303333 315A170D 30343036
31393232 33333331 5A304531 0B300906 03550406 13027573
310E300C 06035504 0A130563 6973636F 310E300C 06035504
0B130573 6A76706E 31163014 06035504 03130D46 69727374
```

```
204F6666 69636572 30819F30 0D06092A 864886F7 0D010101
05000381 8D003081 89028181 00BFC427 727E15E9 30CB1BCB
C0EFFB2F 3E4916D4 EC365F57 C13D1356 6388E66D 7BCCBCB9
04DA2E7C C9639F31 AF15E7B1 E698A33C 0EB447E4 B3B72EC8
766EADCF 9883E612 AD782E39 B0603A90 0322CE78 D6735E07
BDC022F1 1164EC9E 31FC5309 9AA9DC1D 69ECC316 8727A6CB
ADCFB488 FF904D6D 9D9E5778 05B24D4B BB5B4F5F 4D020301
0001A381 E43081E1 300B0603 551D0F04 04030205 20301B06
03551D09 04143012 30100609 2A864886 F67D0744 1D310302
0100304F 0603551D 1F044830 463044A0 42A040A4 3E303C31
0B300906 03550406 13027573 310E300C 06035504 0A130563
6973636F 310E300C 06035504 0B130573 6A76706E 310D300B
06035504 03130443 524C3130 1F060355 1D230418 30168014
46C1609C DBEA53EE 80A48060 1A96583B 0DF80D2F 301D0603
551D0E04 16041400 A7C3DD9F 9FAB0A25 E1485FC7 DB88A63F
78CE4830 09060355 1D130402 30003019 06092A86 4886F67D
07410004 0C300A1B 0456352E 30030204 B0300D06 092A8648
86F70D01 01050500 03818100 69105382 0BE0BA59 B0CD2652
9C6A4585 940C7882 DCEB1D1E 610B8525 0C032A76 2C8758C2
F5CA1EF4 B946848A C49047D5 6D1EF218 FA082A00 16CCD9FC
42DF3B05 A8EF2AAD 151637DE 67885BB2 BA0BB6A1 308F63FF
21C3CB00 9272257A 3C292645 FD62D486 C247F067 301C2FEE
5CF6D12B 6CFA1DAA E74E8B8E 5B017A2E 5BB6C5F9 quit
certificate ra-sign 3B2FD319 308202FF 30820268 A0030201
0202043B 2FD31930 0D06092A 864886F7 0D010105 0500302D
310B3009 06035504 06130275 73310E30 0C060355 040A1305
63697363 6F310E30 0C060355 040B1305 736A7670 6E301E17
0D303130 36313932 32303333 315A170D 30343036 31393232
33333331 5A304531 0B300906 03550406 13027573 310E300C
06035504 0A130563 6973636F 310E300C 06035504 0B130573
6A76706E 31163014 06035504 03130D46 69727374 204F6666
69636572 30819F30 0D06092A 864886F7 0D010101 05000381
8D003081 89028181 00E85434 395790E9 416ED13D 72F1A411
333A0984 66B8F68A 0ECA7E2B CBC40C39 A21E2D8A 5F94772D
69846720 73227891 E43D46B6 B2D1DDC5 385C5135 DB2075F1
4D252ACF AC80DA4C 2111946F 26F7193B 8EA1CA66 8332D2A1
5310B2D7 07C985A8 0B44CE37 BC95EAFF C328D4C6 73B3B35E
0F6D25F5 DCAC6AFA 2DAAD6D1 47BB3396 E1020301 0001A382
01123082 010E300B 0603551D 0F040403 02078030 2B060355
1D100424 3022800F 32303031 30363139 32323033 33315A81
0F323030 33303732 37303233 3333315A 301B0603 551D0904
14301230 1006092A 864886F6 7D07441D 31030201 00304F06
03551D1F 04483046 3044A042 A040A43E 303C310B 30090603
55040613 02757331 0E300C06 0355040A 13056369 73636F31
0E300C06 0355040B 1305736A 76706E31 0D300B06 03550403
13044352 4C31301F 0603551D 23041830 16801446 C1609CDB
EA53EE80 A480601A 96583B0D F80D2F30 1D060355 1D0E0416
04147BD2 620C611F 3AC69FB3 155FD8F9 8A7CF353 3A583009
0603551D 13040230 00301906 092A8648 86F67D07 4100040C
300A1B04 56352E30 030204B0 300D0609 2A864886 F70D0101
05050003 8181003A A6431D7D 1979DDF9 CC99D8F8 CC987F67
DBF67280 2A9418E9 C6255B08 DECDE1C2 50FCB1A6 544F1D51
C214162E E2403DAB 2F1294C4 841240ED FD6F799C 130A0B24
AC74DD74 C60EB5CD EC648631 E0B88B3F 3D19A2E1 6492958E
9F64746E 45C080AE E5A6C245 7827D7B1 380A6FE8 A01D9022
7F52AD9C B596743A 853549C5 771DA2 quit certificate
3B2FD63F 308202C2 3082022B A0030201 0202043B 2FD63F30
0D06092A 864886F7 0D010105 0500302D 310B3009 06035504
06130275 73310E30 0C060355 040A1305 63697363 6F310E30
0C060355 040B1305 736A7670 6E301E17 0D303230 31303932
31343835 325A170D 30333031 30393232 31383532 5A304D31
0B300906 03550406 13027573 310E300C 06035504 0A130563
6973636F 310E300C 06035504 0B130573 6A76706E 311E301C
06092A86 4886F70D 01090216 0F534A68 75622E73 6A746163
```

```
2E636F6D 305C300D 06092A86 4886F70D 01010105 00034B00
30480241 00B5C0D3 B5DC7620 0C08953F E10C3391 8E262A72
2F5268F2 E53EEC89 BA7A1634 A736B835 77C5F7DF 72255DF2
CE121603 30CA8A2B 7C1E41D5 4983C9E6 5901198E 0F020301
0001A382 01113082 010D300B 0603551D 0F040403 0205A030
1A060355 1D110413 3011820F 534A6875 622E736A 7461632E
636F6D30 2B060355 1D100424 3022800F 32303032 30313039
32313438 35325A81 0F323030 32303932 32313031 3835325A
304F0603 551D1F04 48304630 44A042A0 40A43E30 3C310B30
09060355 04061302 7573310E 300C0603 55040A13 05636973
636F310E 300C0603 55040B13 05736A76 706E310D 300B0603
55040313 0443524C 31301F06 03551D23 04183016 801446C1
609CDBEA 53EE80A4 80601A96 583B0DF8 0D2F301D 0603551D
0E041604 14FBE38B 58E5868B 65C3AED1 5CE7C8E9 6658815B
1C300906 03551D13 04023000 30190609 2A864886 F67D0741
00040C30 0A1B0456 352E3003 0204B030 0D06092A 864886F7
0D010105 05000381 81001732 4B19CE9F 5EDA454B D782B240
D9FEC161 215AC65E 4DD449B9 022ADDE6 489D5125 949BA7E7
68B61D2C 3E6F0871 4A9E1DC0 95EBCB11 875CE3BD 649D5BC0
E85B77AD 8541DBC9 2904DA65 0BF441D7 A2BEBD12 0EA438D2
AB6B8AFC 2E25AB87 B0C277C0 7B5C521A A5B8989B 7D854F3A
619393D1 CF666429 E2AE8615 03EE4DD7 13BB quit crypto ca
certificate chain MicrosoftCA certificate
132BD14C00000000000B 3082044C 308203F6 A0030201 02020A13
2BD14C00 00000000 0B300D06 092A8648 86F70D01 01050500
305F310B 30090603 55040613 02555331 0B300906 03550408
13024341 3111300F 06035504 07130853 414E204A 4F534531
0E300C06 0355040A 1305534A 54414331 0E300C06 0355040B
1305534A 504B4931 10300E06 03550403 1307534A 504B4943
41301E17 0D303230 31313331 38333632 335A170D 30343031
31333138 33363233 5A302031 1E301C06 092A8648 86F70D01
0902130F 534A6875 622E736A 7461632E 636F6D30 5C300D06
092A8648 86F70D01 01010500 034B0030 48024100 B5C0D3B5
DC76200C 08953FE1 0C33918E 262A722F 5268F2E5 3EEC89BA
7A1634A7 36B83577 C5F7DF72 255DF2CE 12160330 CA8A2B7C
1E41D549 83C9E659 01198E0F 02030100 01A38202 D1308202
CD300B06 03551D0F 04040302 05A0301D 0603551D 0E041604
14FBE38B 58E5868B 65C3AED1 5CE7C8E9 6658815B 1C308198
0603551D 23048190 30818D80 14231557 4F054052 81E113C7
E86D83CB F233B71C B1A163A4 61305F31 0B300906 03550406
13025553 310B3009 06035504 08130243 41311130 0F060355
04071308 53414E20 4A4F5345 310E300C 06035504 0A130553
4A544143 310E300C 06035504 0B130553 4A504B49 3110300E
06035504 03130753 4A504B49 43418210 091B47AE E8CFE2A9
4D3E8B38 F292F5AF 301D0603 551D1101 01FF0413 3011820F
534A6875 622E736A 7461632E 636F6D30 81C60603 551D1F04
81BE3081 BB3081B8 A081B5A0 81B28681 AF6C6461 703A2F2F
2F434E3D 534A504B 4943412C 434E3D73 6A76706E 6D73706B
692C434E 3D434450 2C434E3D 5075626C 69632532 304B6579
25323053 65727669 6365732C 434E3D53 65727669 6365732C
434E3D43 6F6E6669 67757261 74696F6E 2C44433D 736A706B
692C4443 3D636F6D 3F636572 74696669 63617465 5265766F
63617469 6F6E4C69 73743F62 6173653F 6F626A65 6374636C
6173733D 63524C44 69737472 69627574 696F6E50 6F696E74
3081B706 082B0601 05050701 010481AA 3081A730 81A40608
2B060105 05073002 8681976C 6461703A 2F2F2F43 4E3D534A
504B4943 412C434E 3D414941 2C434E3D 5075626C 69632532
304B6579 25323053 65727669 6365732C 434E3D53 65727669
6365732C 434E3D43 6F6E6669 67757261 74696F6E 2C44433D
736A706B 692C4443 3D636F6D 3F634143 65727469 66696361
74653F62 6173653F 6F626A65 6374636C 6173733D 63657274
69666963 6174696F 6E417574 686F7269 7479300C 0603551D
130101FF 04023000 30130603 551D2504 0C300A06 082B0601
05050802 02303F06 092B0601 04018237 14020432 1E300049
```

```
00500053 00450043 0049006E 00740065 0072006D 00650064
00690061 00740065 004F0066 0066006C 0069006E 0065300D
06092A86 4886F70D 01010505 00034100 39A41B77 72A2EF4D
300D69AE 399894E8 8DBFADFF AC8D9FEA 81755872 BE242CD9
231932FE 3B4D370C F7E4DD76 2DA6E0C1 B6BA26CA 9955858B
95430434 0DD7C88E quit certificate ra-sign
054E60AD000000000002 308204A0 3082044A A0030201 02020A05
4E60AD00 00000000 02300D06 092A8648 86F70D01 01050500
305F310B 30090603 55040613 02555331 0B300906 03550408
13024341 3111300F 06035504 07130853 414E204A 4F534531
0E300C06 0355040A 1305534A 54414331 0E300C06 0355040B
1305534A 504B4931 10300E06 03550403 1307534A 504B4943
41301E17 0D303230 31313130 31353932 375A170D 30343031
31313031 35393237 5A305F31 0B300906 03550406 13025553
310B3009 06035504 08130243 41311130 0F060355 04071308
53414E20 4A4F5345 310E300C 06035504 0A130553 4A544143
310E300C 06035504 0B130553 4A504B49 3110300E 06035504
03130753 4A56504E 52413081 9F300D06 092A8648 86F70D01
01010500 03818D00 30818902 818100E2 61FD62D2 64BED93E
7DBF1FDE 52F0D811 479A4F4E 48E56811 83ED9285 F2A3907B
F236F508 43742D4A E89A76EF 3CB98722 D0A7DC1F 432F386C
721A3379 D50B7EA7 43C07AD0 AA6C087D FDA7BDBF 0BA92FA3
711A7F54 FBCAFBF6 633FCEFA AA9D9A8D 2C79550F 99314B3E
FC97F764 BC6D6D67 D79A7292 A679B42F 4B5C083F 0AA6C902
03010001 A38202A2 3082029E 300B0603 551D0F04 04030207
80301506 03551D25 040E300C 060A2B06 01040182 37140201
303B0609 2B060104 01823714 02042E1E 2C004500 6E007200
6F006C00 6C006D00 65006E00 74004100 67006500 6E007400
4F006600 66006C00 69006E00 65301D06 03551D0E 04160414
09AD6911 B0F87B73 06A2ECAE 24853CA4 DBB12A9E 30819806
03551D23 04819030 818D8014 2315574F 05405281 E113C7E8
6D83CBF2 33B71CB1 A163A461 305F310B 30090603 55040613
02555331 0B300906 03550408 13024341 3111300F 06035504
07130853 414E204A 4F534531 0E300C06 0355040A 1305534A
54414331 0E300C06 0355040B 1305534A 504B4931 10300E06
03550403 1307534A 504B4943 41821009 1B47AEE8 CFE2A94D
3E8B38F2 92F5AF30 81C60603 551D1F04 81BE3081 BB3081B8
A081B5A0 81B28681 AF6C6461 703A2F2F 2F434E3D 534A504B
4943412C 434E3D73 6A76706E 6D73706B 692C434E 3D434450
2C434E3D 5075626C 69632532 304B6579 25323053 65727669
6365732C 434E3D53 65727669 6365732C 434E3D43 6F6E6669
67757261 74696F6E 2C44433D 736A706B 692C4443 3D636F6D
3F636572 74696669 63617465 5265766F 63617469 6F6E4C69
73743F62 6173653F 6F626A65 6374636C 6173733D 63524C44
69737472 69627574 696F6E50 6F696E74 3081B706 082B0601
05050701 010481AA 3081A730 81A40608 2B060105 05073002
8681976C 6461703A 2F2F2F43 4E3D534A 504B4943 412C434E
3D414941 2C434E3D 5075626C 69632532 304B6579 25323053
65727669 6365732C 434E3D53 65727669 6365732C 434E3D43
6F6E6669 67757261 74696F6E 2C44433D 736A706B 692C4443
3D636F6D 3F634143 65727469 66696361 74653F62 6173653F
6F626A65 6374636C 6173733D 63657274 69666963 6174696F
6E417574 686F7269 7479300D 06092A86 4886F70D 01010505
00034100 2CEFFC7E B2C42AED 167FA630 AB3F9460 5E12B77F
07BC860A 48A5DBDB E942F9B8 1B053148 05A70A17 B2EF37D4
F4234622 DD59571B F8D8AF09 2B54D40C 9145302D quit
certificate ra-encrypt 054E63CE000000000003 3082048E
30820438 A0030201 02020A05 4E63CE00 00000000 03300D06
092A8648 86F70D01 01050500 305F310B 30090603 55040613
02555331 0B300906 03550408 13024341 3111300F 06035504
07130853 414E204A 4F534531 0E300C06 0355040A 1305534A
54414331 0E300C06 0355040B 1305534A 504B4931 10300E06
03550403 1307534A 504B4943 41301E17 0D303230 31313130
31353932 385A170D 30343031 31313031 35393238 5A305F31
```

```
0B300906 03550406 13025553 310B3009 06035504 08130243
41311130 0F060355 04071308 53414E20 4A4F5345 310E300C
06035504 0A130553 4A544143 310E300C 06035504 0B130553
4A504B49 3110300E 06035504 03130753 4A56504E 52413081
9F300D06 092A8648 86F70D01 01010500 03818D00 30818902
818100C6 E17A9C97 9CD883ED CCE68AAD DA4AF518 1D1B0056
EAE19CF7 40A1CBA7 622A83DB 4131898F 5FC662A6 5486D0FB
CE253DE5 26A85487 27CCC45C 54803AB6 F5644F21 6967296A
B075E6A3 0392704C 862A3344 8F15F512 FE86F257 6465A4C5
B265DBA5 EBA53F19 D488839E 5881EA32 2943CDF2 2D03B889
5E47A30B C908D29B 64656102 03010001 A3820290 3082028C
300B0603 551D0F04 04030205 20301506 03551D25 040E300C
060A2B06 01040182 37140201 30290609 2B060104 01823714
02041C1E 1A004300 45005000 45006E00 63007200 79007000
74006900 6F006E30 1D060355 1D0E0416 04148F6F 02D57617
E11F78D2 48547776 FE42DBE3 D8CC3081 98060355 1D230481
9030818D 80142315 574F0540 5281E113 C7E86D83 CBF233B7
1CB1A163 A461305F 310B3009 06035504 06130255 53310B30
09060355 04081302 43413111 300F0603 55040713 0853414E
204A4F53 45310E30 0C060355 040A1305 534A5441 43310E30
0C060355 040B1305 534A504B 49311030 0E060355 04031307
534A504B 49434182 10091B47 AEE8CFE2 A94D3E8B 38F292F5
AF3081C6 0603551D 1F0481BE 3081BB30 81B8A081 B5A081B2
8681AF6C 6461703A 2F2F2F43 4E3D534A 504B4943 412C434E
3D736A76 706E6D73 706B692C 434E3D43 44502C43 4E3D5075
626C6963 2532304B 65792532 30536572 76696365 732C434E
3D536572 76696365 732C434E 3D436F6E 66696775 72617469
6F6E2C44 433D736A 706B692C 44433D63 6F6D3F63 65727469
66696361 74655265 766F6361 74696F6E 4C697374 3F626173
653F6F62 6A656374 636C6173 733D6352 4C446973 74726962
7574696F 6E506F69 6E743081 B706082B 06010505 07010104
81AA3081 A73081A4 06082B06 01050507 30028681 976C6461
703A2F2F 2F434E3D 534A504B 4943412C 434E3D41 49412C43
4E3D5075 626C6963 2532304B 65792532 30536572 76696365
732C434E 3D536572 76696365 732C434E 3D436F6E 66696775
72617469 6F6E2C44 433D736A 706B692C 44433D63 6F6D3F63
41436572 74696669 63617465 3F626173 653F6F62 6A656374
636C6173 733D6365 72746966 69636174 696F6E41 7574686F
72697479 300D0609 2A864886 F70D0101 05050003 41008FE9
45687473 3798A614 D3A41747 D357B72B 8D286162 91A7B519
B100159E CF283215 28DE4504 EBB55282 247A9164 DC6B8185
63F159DC 18F6541B E289FC37 EC74 quit certificate ca
091B47AEE8CFE2A94D3E8B38F292F5AF 3082032C 308202D6
A0030201 02021009 1B47AEE8 CFE2A94D 3E8B38F2 92F5AF30
0D06092A 864886F7 0D010105 0500305F 310B3009 06035504
06130255 53310B30 09060355 04081302 43413111 300F0603
55040713 0853414E 204A4F53 45310E30 0C060355 040A1305
534A5441 43310E30 0C060355 040B1305 534A504B 49311030
0E060355 04031307 534A504B 49434130 1E170D30 32303131
31303135 3133395A 170D3037 30313131 30323030 30345A30
5F310B30 09060355 04061302 5553310B 30090603 55040813
02434131 11300F06 03550407 13085341 4E204A4F 5345310E
300C0603 55040A13 05534A54 4143310E 300C0603 55040B13
05534A50 4B493110 300E0603 55040313 07534A50 4B494341
305C300D 06092A86 4886F70D 01010105 00034B00 30480241
00AEC268 0C6388F1 404A2E97 3C94742D 37070BE0 368069BF
C98A7AB3 E81131A5 DDC3E41F B9D9EB66 AF504D65 2BD2864C
87260696 8AAFF871 88A80301 1500F11D 63020301 0001A382
016C3082 01683013 06092B06 01040182 37140204 061E0400
43004130 0B060355 1D0F0404 03020146 300F0603 551D1301
01FF0405 30030101 FF301D06 03551D0E 04160414 2315574F
05405281 E113C7E8 6D83CBF2 33B71CB1 30820100 0603551D
1F0481F8 3081F530 81B8A081 B5A081B2 8681AF6C 6461703A
2F2F2F43 4E3D534A 504B4943 412C434E 3D736A76 706E6D73
```

```
706B692C 434E3D43 44502C43 4E3D5075 626C6963 2532304B
65792532 30536572 76696365 732C434E 3D536572 76696365
732C434E 3D436F6E 66696775 72617469 6F6E2C44 433D736A
706B692C 44433D63 6F6D3F63 65727469 66696361 74655265
766F6361 74696F6E 4C697374 3F626173 653F6F62 6A656374
636C6173 733D6352 4C446973 74726962 7574696F 6E506F69
6E743038 A036A034 86326874 74703A2F 2F736A76 706E6D73
706B692E 736A706B 692E636F 6D2F4365 7274456E 726F6C6C
2F534A50 4B494341 2E63726C 30100609 2B060104 01823715
01040302 0100300D 06092A86 4886F70D 01010505 00034100
735977DF 7822B944 96A50106 722108F0 1A60EF86 EFEDA9ED
2C7C9174 5EF48909 B4A66A08 226FBD11 3F20BA61 C556182A
8E914788 AE6C5363 A769805F 9E2F6458 quit ! crypto isakmp
policy 1 hash md5 ! crypto isakmp identity hostname
crypto isakmp keepalive 10 ! ! crypto ipsec transform-
set myset esp-des esp-md5-hmac crypto mib ipsec flowmib
history tunnel size 200 crypto mib ipsec flowmib history
failure size 200 ! crypto map vpn 10 ipsec-isakmp set
peer 172.16.172.52 set transform-set myset match address
101 crypto map vpn 20 ipsec-isakmp set peer
172.16.172.10 set transform-set myset match address 102
! ! interface Loopback1 ip address 20.1.1.1
255.255.255.0 ! interface Loopback88 no ip address !
interface FastEthernet0/0 no ip address no keepalive
shutdown duplex half media-type MII ! interface
Ethernet4/0 ip address 172.16.172.69 255.255.255.240 ip
route-cache same-interface no ip mroute-cache duplex
half crypto map vpn ! interface Ethernet4/1 no ip
address duplex half ! interface Ethernet4/2 no ip
address shutdown duplex half ! interface Ethernet4/3 no
ip address shutdown duplex half ! ip default-gateway
172.16.172.65 ip classless ip route 0.0.0.0 0.0.0.0
172.16.172.65 ip http server ip pim bidir-enable !
access-list 101 permit ip 20.1.1.0 0.0.0.255 50.1.1.0
0.0.0.255 access-list 102 permit ip 20.1.1.0 0.0.0.255
10.1.1.0 0.0.0.255 ! ! call rsvp-sync ! ! mgcp profile
default ! dial-peer cor custom ! ! ! ! gatekeeper
shutdown ! ! line con 0 exec-timeout 0 0 line aux 0 line
vty 0 4 password cisco login line vty 5 15 login ! no
scheduler max-task-time ! end
```

SJVPN (routeur en étoile inscrit pour confier au serveur CA)

```
SJVPN#write terminal Building configuration... Current
configuration : 8980 bytes ! ! Last configuration change
at 10:28:19 UTC Sun Jan 13 2002 ! NVRAM config last
updated at 10:28:20 UTC Sun Jan 13 2002 ! version 12.2
service timestamps debug uptime service timestamps log
uptime no service password-encryption service udp-small-
servers service tcp-small-servers no service dhcp !
hostname SJVPN ! enable password cisco ! ip subnet-zero
ip cef ! ! no ip domain-lookup ip domain-name sjvpn.com
! ip audit notify log ip audit po max-events 100 ip ssh
time-out 120 ip ssh authentication-retries 3 ! crypto ca
identity EntrustPKI enrollment mode ra enrollment url
http://171.69.89.16:80 query url ldap://171.69.89.16
crypto ca certificate chain EntrustPKI certificate ca
3B2FD307 308202E4 3082024D A0030201 0202043B 2FD30730
0D06092A 864886F7 0D010105 0500302D 310B3009 06035504
06130275 73310E30 0C060355 040A1305 63697363 6F310E30
0C060355 040B1305 736A7670 6E301E17 0D303130 36313932
32303234 305A170D 32313036 31393232 33323430 5A302D31
0B300906 03550406 13027573 310E300C 06035504 0A130563
6973636F 310E300C 06035504 0B130573 6A76706E 30819F30
```

```
0D06092A 864886F7 0D010101 05000381 8D003081 89028181
00E8C25B EDF4A6EE A352B142 C16578F4 FBDAF45E 4F2F7733
8D2B8879 96138C63 1DB713BF 753BF845 2D7E600F AAF4D75B
9E959513 BB13FF13 36696F48 86C464F2 CF854A66 4F8E83F8
025F216B A44D4BB2 39ADD1A5 1BCCF812 09A19BDC 468EEAE1
B6C2A378 69C81348 1A9CD61C 551216F2 8B168FBB 94CBEF37
E1D9A8F7 80BBC17F D1020301 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 30303130 36313932
32303234 305A810F 32303231 30363139 32323332 34305A30
0B060355 1D0F0404 03020106 301F0603 551D2304 18301680
1446C160 9CDBEA53 EE80A480 601A9658 3B0DF80D 2F301D06
03551D0E 04160414 46C1609C DBEA53EE 80A48060 1A96583B
0DF80D2F 300C0603 551D1304 05300301 01FF301D 06092A86
4886F67D 07410004 10300E1B 0856352E 303A342E 30030204
90300D06 092A8648 86F70D01 01050500 03818100 7E3DBAC4
8CAE7D5A B19C0625 8780D222 F965A1A2 C0C25B84 CBC5A203
BF50FAC4 9656699A 52D8CB46 40776237 87163118 8F3C0F47
D2CAA36B 6AB34F99 AB71269E 78C0AC10 DA0B9EC5 AE448B46
701254CF 3EBC64C1 5DBB2EE5 56C0140B B0C83497 D79FB148
80018F51 3A4B6174 590B85AA 9CE3B391 629406AA 7CE9CC0D
01593E6B quit certificate ra-encrypt 3B2FD318 308202D0
30820239 A0030201 0202043B 2FD31830 0D06092A 864886F7
0D010105 0500302D 310B3009 06035504 06130275 73310E30
0C060355 040A1305 63697363 6F310E30 0C060355 040B1305
736A7670 6E301E17 0D303130 36313932 32303333 315A170D
30343036 31393232 33333331 5A304531 0B300906 03550406
13027573 310E300C 06035504 0A130563 6973636F 310E300C
06035504 0B130573 6A76706E 31163014 06035504 03130D46
69727374 204F6666 69636572 30819F30 0D06092A 864886F7
0D010101 05000381 8D003081 89028181 00BFC427 727E15E9
30CB1BCB C0EFFB2F 3E4916D4 EC365F57 C13D1356 6388E66D
7BCCBCB9 04DA2E7C C9639F31 AF15E7B1 E698A33C 0EB447E4
B3B72EC8 766EADCF 9883E612 AD782E39 B0603A90 0322CE78
D6735E07 BDC022F1 1164EC9E 31FC5309 9AA9DC1D 69ECC316
8727A6CB ADCFB488 FF904D6D 9D9E5778 05B24D4B BB5B4F5F
4D020301 0001A381 E43081E1 300B0603 551D0F04 04030205
20301B06 03551D09 04143012 30100609 2A864886 F67D0744
1D310302 0100304F 0603551D 1F044830 463044A0 42A040A4
3E303C31 0B300906 03550406 13027573 310E300C 06035504
0A130563 6973636F 310E300C 06035504 0B130573 6A76706E
310D300B 06035504 03130443 524C3130 1F060355 1D230418
30168014 46C1609C DBEA53EE 80A48060 1A96583B 0DF80D2F
301D0603 551D0E04 16041400 A7C3DD9F 9FAB0A25 E1485FC7
DB88A63F 78CE4830 09060355 1D130402 30003019 06092A86
4886F67D 07410004 0C300A1B 0456352E 30030204 B0300D06
092A8648 86F70D01 01050500 03818100 69105382 0BE0BA59
B0CD2652 9C6A4585 940C7882 DCEB1D1E 610B8525 0C032A76
2C8758C2 F5CA1EF4 B946848A C49047D5 6D1EF218 FA082A00
16CCD9FC 42DF3B05 A8EF2AAD 151637DE 67885BB2 BA0BB6A1
308F63FF 21C3CB00 9272257A 3C292645 FD62D486 C247F067
301C2FEE 5CF6D12B 6CFA1DAA E74E8B8E 5B017A2E 5BB6C5F9
quit certificate ra-sign 3B2FD319 308202FF 30820268
A0030201 0202043B 2FD31930 0D06092A 864886F7 0D010105
0500302D 310B3009 06035504 06130275 73310E30 0C060355
040A1305 63697363 6F310E30 0C060355 040B1305 736A7670
6E301E17 0D303130 36313932 32303333 315A170D 30343036
31393232 33333331 5A304531 0B300906 03550406 13027573
310E300C 06035504 0A130563 6973636F 310E300C 06035504
0B130573 6A76706E 31163014 06035504 03130D46 69727374
204F6666 69636572 30819F30 0D06092A 864886F7 0D010101
```

```
05000381 8D003081 89028181 00E85434 395790E9 416ED13D
72F1A411 333A0984 66B8F68A 0ECA7E2B CBC40C39 A21E2D8A
5F94772D 69846720 73227891 E43D46B6 B2D1DDC5 385C5135
DB2075F1 4D252ACF AC80DA4C 2111946F 26F7193B 8EA1CA66
8332D2A1 5310B2D7 07C985A8 0B44CE37 BC95EAFF C328D4C6
73B3B35E 0F6D25F5 DCAC6AFA 2DAAD6D1 47BB3396 E1020301
0001A382 01123082 010E300B 0603551D 0F040403 02078030
2B060355 1D100424 3022800F 32303031 30363139 32323033
33315A81 0F323030 33303732 37303233 3333315A 301B0603
551D0904 14301230 1006092A 864886F6 7D07441D 31030201
00304F06 03551D1F 04483046 3044A042 A040A43E 303C310B
30090603 55040613 02757331 0E300C06 0355040A 13056369
73636F31 0E300C06 0355040B 1305736A 76706E31 0D300B06
03550403 13044352 4C31301F 0603551D 23041830 16801446
C1609CDB EA53EE80 A480601A 96583B0D F80D2F30 1D060355
1D0E0416 04147BD2 620C611F 3AC69FB3 155FD8F9 8A7CF353
3A583009 0603551D 13040230 00301906 092A8648 86F67D07
4100040C 300A1B04 56352E30 030204B0 300D0609 2A864886
F70D0101 05050003 8181003A A6431D7D 1979DDF9 CC99D8F8
CC987F67 DBF67280 2A9418E9 C6255B08 DECDE1C2 50FCB1A6
544F1D51 C214162E E2403DAB 2F1294C4 841240ED FD6F799C
130A0B24 AC74DD74 C60EB5CD EC648631 E0B88B3F 3D19A2E1
6492958E 9F64746E 45C080AE E5A6C245 7827D7B1 380A6FE8
A01D9022 7F52AD9C B596743A 853549C5 771DA2 quit
certificate 3B2FD65B 308202C2 3082022B A0030201 0202043B
2FD65B30 0D06092A 864886F7 0D010105 0500302D 310B3009
06035504 06130275 73310E30 0C060355 040A1305 63697363
6F310E30 0C060355 040B1305 736A7670 6E301E17 0D303230
31313132 30313630 385A170D 30333031 31313230 34363038
5A304D31 0B300906 03550406 13027573 310E300C 06035504
0A130563 6973636F 310E300C 06035504 0B130573 6A76706E
311E301C 06092A86 4886F70D 01090216 0F534A56 504E2E73
6A76706E 2E636F6D 305C300D 06092A86 4886F70D 01010105
00034B00 30480241 00EC4BE5 44E6ABC4 404BBBAD FE61E486
F2F85AC5 751EAC1D E68BD930 09958131 A977BA90 13BFD94D
297E41CA 23CDB0A3 EC38A296 49F61BBE 8037C94E F7FF6F35
29020301 0001A382 01113082 010D300B 0603551D 0F040403
0205A030 1A060355 1D110413 3011820F 534A5650 4E2E736A
76706E2E 636F6D30 2B060355 1D100424 3022800F 32303032
30313131 32303136 30385A81 0F323030 32303932 34303834
3630385A 304F0603 551D1F04 48304630 44A042A0 40A43E30
3C310B30 09060355 04061302 7573310E 300C0603 55040A13
05636973 636F310E 300C0603 55040B13 05736A76 706E310D
300B0603 55040313 0443524C 31301F06 03551D23 04183016
801446C1 609CDBEA 53EE80A4 80601A96 583B0DF8 0D2F301D
0603551D 0E041604 14494FC9 CE8C0C8E 2B078D54 EF43111B
3F1FAAB2 8A300906 03551D13 04023000 30190609 2A864886
F67D0741 00040C30 0A1B0456 352E3003 0204B030 0D06092A
864886F7 0D010105 05000381 81006C96 16AB6674 1FF8D1AB
27FA7384 0C08272A 8D68C826 8F80006B 0C146105 2FB8BDF9
CCC85262 2133F1EF FC7AA2F9 48191740 86AFC27C EF5AD773
768C5597 A953316B 839617FE 210B1195 3E5CD64A B643ADFC
43A57C8E 1D56BD39 5812109B 2C8301E1 BC30A6E1 8E634030
1851AC22 CD941F9C 65F21608 0229AFB4 126FD11A 6825 quit !
crypto isakmp policy 1 hash md5 ! crypto isakmp identity
hostname crypto isakmp keepalive 10 ! ! crypto ipsec
transform-set myset esp-des esp-md5-hmac crypto mib
ipsec flowmib history tunnel size 200 crypto mib ipsec
flowmib history failure size 200 ! crypto map vpn 10
ipsec-isakmp set peer 172.16.172.69 set transform-set
myset match address 101 ! ! ! ! ! ! ! ! controller ISA
3/1 ! ! ! ! interface Ethernet1/0 ip address
172.16.172.52 255.255.255.248 no ip redirects duplex
half crypto map vpn ! interface Ethernet1/1 ip address
```

50.1.1.1 255.255.255.0 no ip redirects duplex half ! interface Ethernet1/2 no ip address shutdown duplex half ! interface Ethernet1/3 no ip address shutdown duplex half ! ip classless ip route 0.0.0.0 0.0.0.0 172.16.172.49 no ip http server ip pim bidir-enable ! access-list 101 permit ip 50.1.1.0 0.0.0.255 20.1.1.0 0.0.0.255 ! snmp-server community public RO ! call rsvp-sync ! ! mgcp profile default ! dial-peer cor custom ! ! ! ! gatekeeper shutdown ! ! line con 0 exec-timeout 0 0 line aux 0 line vty 0 4 password cisco no login line vty 5 15 login ! no scheduler max-task-time ! end SJVPN#**show crypto ca certificates** CA Certificate Status: Available Certificate Serial Number: 3B2FD307 Key Usage: General Purpose Issuer: OU = sjvpn O = cisco C = us Subject: OU = sjvpn O = cisco C = us CRL Distribution Point: CN = CRL1, OU = sjvpn, O = cisco, C = us Validity Date: start date: 22:02:40 UTC Jun 19 2001 end date: 22:32:40 UTC Jun 19 2021 Associated Identity: EntrustPKI RA KeyEncipher Certificate Status: Available Certificate Serial Number: 3B2FD318 Key Usage: Encryption Issuer: OU = sjvpn O = cisco C = us Subject: CN = First Officer OU = sjvpn O = cisco C = us CRL Distribution Point: CN = CRL1, OU = sjvpn, O = cisco, C = us Validity Date: start date: 22:03:31 UTC Jun 19 2001 end date: 22:33:31 UTC Jun 19 2004 Associated Identity: EntrustPKI RA Signature Certificate Status: Available Certificate Serial Number: 3B2FD319 Key Usage: Signature Issuer: OU = sjvpn O = cisco C = us Subject: CN = First Officer OU = sjvpn O = cisco C = us CRL Distribution Point: CN = CRL1, OU = sjvpn, O = cisco, C = us Validity Date: start date: 22:03:31 UTC Jun 19 2001 end date: 22:33:31 UTC Jun 19 2004 Associated Identity: EntrustPKI Certificate Status: Available Certificate Serial Number: 3B2FD65B Key Usage: General Purpose Issuer: OU = sjvpn O = cisco C = us Subject Name Contains: Name: SJVPN.sjvpn.com CRL Distribution Point: CN = CRL1, OU = sjvpn, O = cisco, C = us Validity Date: start date: 20:16:08 UTC Jan 11 2002 end date: 20:46:08 UTC Jan 11 2003 Associated Identity: EntrustPKI

SJPKI (routeur en étoile inscrit au serveur de Microsoft CA)

SJPKI#**write terminal** Building configuration... Current configuration : 12452 bytes ! ! Last configuration change at 18:40:41 UTC Sun Jan 13 2002 ! NVRAM config last updated at 18:42:15 UTC Sun Jan 13 2002 ! version 12.2 service timestamps debug uptime service timestamps log uptime no service password-encryption service udp-small-servers service tcp-small-servers ! hostname SJPKI ! ! ip subnet-zero ip cef ! ! ip domain-name sjtac ! ip audit notify log ip audit po max-events 100 ip ssh time-out 120 ip ssh authentication-retries 3 ! crypto ca identity MicrosoftPKI enrollment mode ra enrollment url http://171.69.89.182:80/certsrv/mscep/mscep.dll query url ldap://171.69.89.182 crl optional ! ! crypto ca certificate chain MicrosoftPKI certificate ca 091B47AEE8CFE2A94D3E8B38F292F5AF 3082032C 308202D6 A0030201 02021009 1B47AEE8 CFE2A94D 3E8B38F2 92F5AF30 0D06092A 864886F7 0D010105 0500305F 310B3009 06035504 06130255 53310B30 09060355 04081302 43413111 300F0603 55040713 0853414E 204A4F53 45310E30 0C060355 040A1305 534A5441 43310E30 0C060355 040B1305 534A504B 49311030 0E060355 04031307 534A504B 49434130 1E170D30 32303131 31303135 3133395A 170D3037 30313131 30323030 30345A30

```
5F310B30 09060355 04061302 5553310B 30090603 55040813
02434131 11300F06 03550407 13085341 4E204A4F 5345310E
300C0603 55040A13 05534A54 4143310E 300C0603 55040B13
05534A50 4B493110 300E0603 55040313 07534A50 4B494341
305C300D 06092A86 4886F70D 01010105 00034B00 30480241
00AEC268 0C6388F1 404A2E97 3C94742D 37070BE0 368069BF
C98A7AB3 E81131A5 DDC3E41F B9D9EB66 AF504D65 2BD2864C
87260696 8AAFF871 88A80301 1500F11D 63020301 0001A382
016C3082 01683013 06092B06 01040182 37140204 061E0400
43004130 0B060355 1D0F0404 03020146 300F0603 551D1301
01FF0405 30030101 FF301D06 03551D0E 04160414 2315574F
05405281 E113C7E8 6D83CBF2 33B71CB1 30820100 0603551D
1F0481F8 3081F530 81B8A081 B5A081B2 8681AF6C 6461703A
2F2F2F43 4E3D534A 504B4943 412C434E 3D736A76 706E6D73
706B692C 434E3D43 44502C43 4E3D5075 626C6963 2532304B
65792532 30536572 76696365 732C434E 3D536572 76696365
732C434E 3D436F6E 66696775 72617469 6F6E2C44 433D736A
706B692C 44433D63 6F6D3F63 65727469 66696361 74655265
766F6361 74696F6E 4C697374 3F626173 653F6F62 6A656374
636C6173 733D6352 4C446973 74726962 7574696F 6E506F69
6E743038 A036A034 86326874 74703A2F 2F736A76 706E6D73
706B692E 736A706B 692E636F 6D2F4365 7274456E 726F6C6C
2F534A50 4B494341 2E63726C 30100609 2B060104 01823715
01040302 0100300D 06092A86 4886F70D 01010505 00034100
735977DF 7822B944 96A50106 722108F0 1A60EF86 EFEDA9ED
2C7C9174 5EF48909 B4A66A08 226FBD11 3F20BA61 C556182A
8E914788 AE6C5363 A769805F 9E2F6458 quit certificate ra-
encrypt 054E63CE000000000003 3082048E 30820438 A0030201
02020A05 4E63CE00 00000000 03300D06 092A8648 86F70D01
01050500 305F310B 30090603 55040613 02555331 0B300906
03550408 13024341 3111300F 06035504 07130853 414E204A
4F534531 0E300C06 0355040A 1305534A 54414331 0E300C06
0355040B 1305534A 504B4931 10300E06 03550403 1307534A
504B4943 41301E17 0D303230 31313130 31353932 385A170D
30343031 31313031 35393238 5A305F31 0B300906 03550406
13025553 310B3009 06035504 08130243 41311130 0F060355
04071308 53414E20 4A4F5345 310E300C 06035504 0A130553
4A544143 310E300C 06035504 0B130553 4A504B49 3110300E
06035504 03130753 4A56504E 52413081 9F300D06 092A8648
86F70D01 01010500 03818D00 30818902 818100C6 E17A9C97
9CD883ED CCE68AAD DA4AF518 1D1B0056 EAE19CF7 40A1CBA7
622A83DB 4131898F 5FC662A6 5486D0FB CE253DE5 26A85487
27CCC45C 54803AB6 F5644F21 6967296A B075E6A3 0392704C
862A3344 8F15F512 FE86F257 6465A4C5 B265DBA5 EBA53F19
D488839E 5881EA32 2943CDF2 2D03B889 5E47A30B C908D29B
64656102 03010001 A3820290 3082028C 300B0603 551D0F04
04030205 20301506 03551D25 040E300C 060A2B06 01040182
37140201 30290609 2B060104 01823714 02041C1E 1A004300
45005000 45006E00 63007200 79007000 74006900 6F006E30
1D060355 1D0E0416 04148F6F 02D57617 E11F78D2 48547776
FE42DBE3 D8CC3081 98060355 1D230481 9030818D 80142315
574F0540 5281E113 C7E86D83 CBF233B7 1CB1A163 A461305F
310B3009 06035504 06130255 53310B30 09060355 04081302
43413111 300F0603 55040713 0853414E 204A4F53 45310E30
0C060355 040A1305 534A5441 43310E30 0C060355 040B1305
534A504B 49311030 0E060355 04031307 534A504B 49434182
10091B47 AEE8CFE2 A94D3E8B 38F292F5 AF3081C6 0603551D
1F0481BE 3081BB30 81B8A081 B5A081B2 8681AF6C 6461703A
2F2F2F43 4E3D534A 504B4943 412C434E 3D736A76 706E6D73
706B692C 434E3D43 44502C43 4E3D5075 626C6963 2532304B
65792532 30536572 76696365 732C434E 3D536572 76696365
732C434E 3D436F6E 66696775 72617469 6F6E2C44 433D736A
706B692C 44433D63 6F6D3F63 65727469 66696361 74655265
766F6361 74696F6E 4C697374 3F626173 653F6F62 6A656374
```

```
636C6173 733D6352 4C446973 74726962 7574696F 6E506F69
6E743081 B706082B 06010505 07010104 81AA3081 A73081A4
06082B06 01050507 30028681 976C6461 703A2F2F 2F434E3D
534A504B 4943412C 434E3D41 49412C43 4E3D5075 626C6963
2532304B 65792532 30536572 76696365 732C434E 3D536572
76696365 732C434E 3D436F6E 66696775 72617469 6F6E2C44
433D736A 706B692C 44433D63 6F6D3F63 41436572 74696669
63617465 3F626173 653F6F62 6A656374 636C6173 733D6365
72746966 69636174 696F6E41 7574686F 72697479 300D0609
2A864886 F70D0101 05050003 41008FE9 45687473 3798A614
D3A41747 D357B72B 8D286162 91A7B519 B100159E CF283215
28DE4504 EBB55282 247A9164 DC6B8185 63F159DC 18F6541B
E289FC37 EC74 quit certificate ra-sign
054E60AD000000000002 308204A0 3082044A A0030201 02020A05
4E60AD00 00000000 02300D06 092A8648 86F70D01 01050500
305F310B 30090603 55040613 02555331 0B300906 03550408
13024341 3111300F 06035504 07130853 414E204A 4F534531
0E300C06 0355040A 1305534A 54414331 0E300C06 0355040B
1305534A 504B4931 10300E06 03550403 1307534A 504B4943
41301E17 0D303230 31313130 31353932 375A170D 30343031
31313031 35393237 5A305F31 0B300906 03550406 13025553
310B3009 06035504 08130243 41311130 0F060355 04071308
53414E20 4A4F5345 310E300C 06035504 0A130553 4A544143
310E300C 06035504 0B130553 4A504B49 3110300E 06035504
03130753 4A56504E 52413081 9F300D06 092A8648 86F70D01
01010500 03818D00 30818902 818100E2 61FD62D2 64BED93E
7DBF1FDE 52F0D811 479A4F4E 48E56811 83ED9285 F2A3907B
F236F508 43742D4A E89A76EF 3CB98722 D0A7DC1F 432F386C
721A3379 D50B7EA7 43C07AD0 AA6C087D FDA7BDBF 0BA92FA3
711A7F54 FBCAFBF6 633FCEFA AA9D9A8D 2C79550F 99314B3E
FC97F764 BC6D6D67 D79A7292 A679B42F 4B5C083F 0AA6C902
03010001 A38202A2 3082029E 300B0603 551D0F04 04030207
80301506 03551D25 040E300C 060A2B06 01040182 37140201
303B0609 2B060104 01823714 02042E1E 2C004500 6E007200
6F006C00 6C006D00 65006E00 74004100 67006500 6E007400
4F006600 66006C00 69006E00 65301D06 03551D0E 04160414
09AD6911 B0F87B73 06A2ECAE 24853CA4 DBB12A9E 30819806
03551D23 04819030 818D8014 2315574F 05405281 E113C7E8
6D83CBF2 33B71CB1 A163A461 305F310B 30090603 55040613
02555331 0B300906 03550408 13024341 3111300F 06035504
07130853 414E204A 4F534531 0E300C06 0355040A 1305534A
54414331 0E300C06 0355040B 1305534A 504B4931 10300E06
03550403 1307534A 504B4943 41821009 1B47AEE8 CFE2A94D
3E8B38F2 92F5AF30 81C60603 551D1F04 81BE3081 BB3081B8
A081B5A0 81B28681 AF6C6461 703A2F2F 2F434E3D 534A504B
4943412C 434E3D73 6A76706E 6D73706B 692C434E 3D434450
2C434E3D 5075626C 69632532 304B6579 25323053 65727669
6365732C 434E3D53 65727669 6365732C 434E3D43 6F6E6669
67757261 74696F6E 2C44433D 736A706B 692C4443 3D636F6D
3F636572 74696669 63617465 5265766F 63617469 6F6E4C69
73743F62 6173653F 6F626A65 6374636C 6173733D 63524C44
69737472 69627574 696F6E50 6F696E74 3081B706 082B0601
05050701 010481AA 3081A730 81A40608 2B060105 05073002
8681976C 6461703A 2F2F2F43 4E3D534A 504B4943 412C434E
3D414941 2C434E3D 5075626C 69632532 304B6579 25323053
65727669 6365732C 434E3D53 65727669 6365732C 434E3D43
6F6E6669 67757261 74696F6E 2C44433D 736A706B 692C4443
3D636F6D 3F634143 65727469 66696361 74653F62 6173653F
6F626A65 6374636C 6173733D 63657274 69666963 6174696F
6E417574 686F7269 7479300D 06092A86 4886F70D 01010505
00034100 2CEFFC7E B2C42AED 167FA630 AB3F9460 5E12B77F
07BC860A 48A5DBDB E942F9B8 1B053148 05A70A17 B2EF37D4
F4234622 DD59571B F8D8AF09 2B54D40C 9145302D quit
certificate 0961EAC400000000000A 30820444 308203EE
```

```
A0030201 02020A09 61EAC400 00000000 0A300D06 092A8648
86F70D01 01050500 305F310B 30090603 55040613 02555331
0B300906 03550408 13024341 3111300F 06035504 07130853
414E204A 4F534531 0E300C06 0355040A 1305534A 54414331
0E300C06 0355040B 1305534A 504B4931 10300E06 03550403
1307534A 504B4943 41301E17 0D303230 31313132 30353931
375A170D 30343031 31313230 35393137 5A301C31 1A301806
092A8648 86F70D01 0902130B 534A504B 492E736A 74616330
5C300D06 092A8648 86F70D01 01010500 034B0030 48024100
C7FB363F 410E22E5 1B5649A6 8948CC05 D8A58518 A3633227
F6908EE1 7809600F 80771B65 09316FA0 DCB317D3 7FB6D7DF
BBAC418D 2D8E2ABA 418A49AE 7961560D 02030100 01A38202
CD308202 C9300B06 03551D0F 04040302 05A0301D 0603551D
0E041604 142C9F6B 2DAFF8F8 C040121B B78AA486 0CD207E0
DF308198 0603551D 23048190 30818D80 14231557 4F054052
81E113C7 E86D83CB F233B71C B1A163A4 61305F31 0B300906
03550406 13025553 310B3009 06035504 08130243 41311130
0F060355 04071308 53414E20 4A4F5345 310E300C 06035504
0A130553 4A544143 310E300C 06035504 0B130553 4A504B49
3110300E 06035504 03130753 4A504B49 43418210 091B47AE
E8CFE2A9 4D3E8B38 F292F5AF 30190603 551D1101 01FF040F
300D820B 534A504B 492E736A 74616330 81C60603 551D1F04
81BE3081 BB3081B8 A081B5A0 81B28681 AF6C6461 703A2F2F
2F434E3D 534A504B 4943412C 434E3D73 6A76706E 6D73706B
692C434E 3D434450 2C434E3D 5075626C 69632532 304B6579
25323053 65727669 6365732C 434E3D53 65727669 6365732C
434E3D43 6F6E6669 67757261 74696F6E 2C44433D 736A706B
692C4443 3D636F6D 3F636572 74696669 63617465 5265766F
63617469 6F6E4C69 73743F62 6173653F 6F626A65 6374636C
6173733D 63524C44 69737472 69627574 696F6E50 6F696E74
3081B706 082B0601 05050701 010481AA 3081A730 81A40608
2B060105 05073002 8681976C 6461703A 2F2F2F43 4E3D534A
504B4943 412C434E 3D414941 2C434E3D 5075626C 69632532
304B6579 25323053 65727669 6365732C 434E3D53 65727669
6365732C 434E3D43 6F6E6669 67757261 74696F6E 2C44433D
736A706B 692C4443 3D636F6D 3F634143 65727469 66696361
74653F62 6173653F 6F626A65 6374636C 6173733D 63657274
69666963 6174696F 6E417574 686F7269 7479300C 0603551D
130101FF 04023000 30130603 551D2504 0C300A06 082B0601
05050802 02303F06 092B0601 04018237 14020432 1E300049
00500053 00450043 0049006E 00740065 0072006D 00650064
00690061 00740065 004F0066 0066006C 0069006E 0065300D
06092A86 4886F70D 01010505 00034100 377A0F69 2909A243
11F41B30 4F3B125F DDE22145 0BEA2BF1 4E030C8E B82DCFF9
3639C047 AF40A0A7 EE0FF252 71E48C82 4AA309C4 9343BFB6
2C9C2D81 FE788AF3 quit ! crypto isakmp policy 1 hash md5
! crypto isakmp identity hostname crypto isakmp
keepalive 10 ! ! crypto ipsec transform-set myset esp-
des esp-md5-hmac crypto mib ipsec flowmib history tunnel
size 200 crypto mib ipsec flowmib history failure size
200 ! crypto map vpn 10 ipsec-isakmp set peer
172.16.172.69 set transform-set myset match address 101
! ! ! ! ! ! ! ! controller ISA 2/1 ! ! ! ! interface
Ethernet1/0 ip address 172.16.172.10 255.255.255.240 ip
broadcast-address 172.16.172.0 no ip redirects duplex
half crypto map vpn ! interface Ethernet1/1 ip address
10.1.1.2 255.255.255.0 ip broadcast-address 10.1.1.0
duplex half ! interface Ethernet1/2 no ip address ip
broadcast-address 0.0.0.0 shutdown duplex half !
interface Ethernet1/3 no ip address ip broadcast-address
0.0.0.0 shutdown duplex half ! router ospf 1 log-
adjacency-changes redistribute static subnets network
10.1.1.0 0.0.0.255 area 0 ! ip classless ip route
0.0.0.0 0.0.0.0 172.16.172.1 no ip http server ip pim
```

```
bidir-enable ! access-list 101 permit ip 10.1.1.0
0.0.0.255 20.1.1.0 0.0.0.255 ! route-map tftp permit 10
match ip address 150 ! ! call rsvp-sync ! ! mgcp profile
default ! dial-peer cor custom ! ! ! ! gatekeeper
shutdown ! ! line con 0 exec-timeout 0 0 line aux 0 line
vty 0 4 login line vty 5 15 login ! ! end SJPKI#show
crypto ca cert CA Certificate Status: Available
Certificate Serial Number:
091B47AEE8CFE2A94D3E8B38F292F5AF Key Usage: General
Purpose Issuer: CN = SJPKICA OU = SJPKI O = SJTAC L =
SAN JOSE ST = CA C = US Subject: CN = SJPKICA OU = SJPKI
O = SJTAC L = SAN JOSE ST = CA C = US CRL Distribution
Point:
ldap:///CN=SJPKICA,CN=sjvpnmspki,CN=CDP,CN=Public%20Key%
20Services,
CN=Services,CN=Configuration,DC=sjpki,DC=com?
certificateRevocationList?base?objectclass=cRLDistributi
onPoint Validity Date: start date: 01:51:39 UTC Jan 11
2002 end date: 02:00:04 UTC Jan 11 2007 Associated
Identity: MicrosoftPKI RA KeyEncipher Certificate
Status: Available Certificate Serial Number:
054E63CE000000000003 Key Usage: Encryption Issuer: CN =
SJPKICA OU = SJPKI O = SJTAC L = SAN JOSE ST = CA C = US
Subject: CN = SJVPNRA OU = SJPKI O = SJTAC L = SAN JOSE
ST = CA C = US CRL Distribution Point:
ldap:///CN=SJPKICA,CN=sjvpnmspki,CN=CDP,CN=Public%20Key%
20Services,
CN=Services,CN=Configuration,DC=sjpki,DC=com?
certificateRevocationList?base?objectclass=cRLDistributi
onPoint Validity Date: start date: 01:59:28 UTC Jan 11
2002 end date: 01:59:28 UTC Jan 11 2004 Associated
Identity: MicrosoftPKI RA Signature Certificate Status:
Available Certificate Serial Number:
054E60AD000000000002 Key Usage: Signature Issuer: CN =
SJPKICA OU = SJPKI O = SJTAC L = SAN JOSE ST = CA C = US
Subject: CN = SJVPNRA OU = SJPKI O = SJTAC L = SAN JOSE
ST = CA C = US CRL Distribution Point:
ldap:///CN=SJPKICA,CN=sjvpnmspki,CN=CDP,CN=Public%20Key%
20Services,
CN=Services,CN=Configuration,DC=sjpki,DC=com?
certificateRevocationList?base?objectclass=cRLDistributi
onPoint Validity Date: start date: 01:59:27 UTC Jan 11
2002 end date: 01:59:27 UTC Jan 11 2004 Associated
Identity: MicrosoftPKI Certificate Status: Available
Certificate Serial Number: 0961EAC400000000000A Key
Usage: General Purpose Issuer: CN = SJPKICA OU = SJPKI O
= SJTAC L = SAN JOSE ST = CA C = US Subject Name
Contains: Name: SJPKI.sjtac CRL Distribution Point:
ldap:///CN=SJPKICA,CN=sjvpnmspki,CN=CDP,CN=Public%20Key%
20Services,
CN=Services,CN=Configuration,DC=sjpki,DC=com?
certificateRevocationList?base?objectclass=cRLDistributi
onPoint Validity Date: start date: 20:59:17 UTC Jan 11
2002 end date: 20:59:17 UTC Jan 11 2004 Associated
Identity: MicrosoftPKI
```

Dépannez

Dépannage des commandes

Vous pouvez utiliser quelques commandes de débogage liées IPSec IOS de voir comment la

négociation d'Échange de clés Internet (IKE) fonctionne avec de plusieurs certificats d'identité.

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.

Remarque: Avant d'émettre des commandes de **débogage**, référez-vous aux informations importantes sur des commandes de debug.

- **debug crypto isakmp**—Affichage de messages d'événements IKE.
- **debug crypto ipsec** — Affiche des événements IPsec.
- **transaction de PKI de debug crypto** — Messages de débogage d'affichages pour le suivi de l'interaction (type de message) entre le CA et le routeur.
- **message de PKI de debug crypto** — Messages de débogage d'affichages pour les détails de l'interaction (vidage mémoire de message) entre le CA et le routeur.

Certificats d'un serveur de la confiance CA

Ce qui suit met au point a été collecté sur SJVPN et SJhub. Typiquement, essais SJVPN pour initier le tunnel d'IPSec au routeur concentrateur SJhub. SJhub envoie une charge utile CERT_REQ pour chaque domaine CA qu'elle la prend en charge. Chaque **charge utile CERT_REQ** contient le nom unique (DN) de l'émetteur des Certificats. Essais SJVPN puis pour tracer le DN dans le CERT_REQ et pour envoyer ses propres Certificats à SJhub.

Dans les exemples ci-dessous, le routeur de SJhub envoie ses Certificats basés sur le **CERT_REQ** envoyé par le routeur SJVPN. Des Certificats du serveur de la confiance CA sont utilisés.

- Debugs collectés sur SJVPN
- Debugs collectés sur SJhub
- Liste des révocations de certificat (CRL) cachant sur les Routeurs

Debugs collectés sur SJVPN

```
00:02:24: IPSEC(sa_request): ,
(key eng. msg.) src= 172.16.172.52, dest= 172.16.172.69,
src_proxy= 50.1.1.0/255.255.255.0/0/0 (type=4),
dest_proxy= 20.1.1.0/255.255.255.0/0/0 (type=4),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 3600s and 4608000kb,
spi= 0xFA8261EB(4202848747), conn_id= 0, keysize= 0, flags= 0x4004
00:02:24: ISAKMP: received ke message (1/1)
00:02:24: ISAKMP: local port 500, remote port 500
00:02:24: ISAKMP (0:2): Input = IKE_MESG_FROM_IPSEC, IKE_SA_REQ_MM
Old State = IKE_READY New State = IKE_I_MM1
00:02:24: ISAKMP (0:2): beginning Main Mode exchange
00:02:24: ISAKMP (0:2): sending packet to 172.16.172.69 (I) MM_NO_STATE
00:02:24: ISAKMP (0:2): received packet from 172.16.172.69 (I) MM_NO_STATE
00:02:24: ISAKMP (0:2): Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
Old State = IKE_I_MM1 New State = IKE_I_MM2

00:02:24: ISAKMP (0:2): processing SA payload. message ID = 0
00:02:24: ISAKMP (0:2): Checking ISAKMP transform 1
   against priority 1 policy
00:02:24: ISAKMP: encryption DES-CBC
00:02:24: ISAKMP: hash MD5
```

00:02:24: ISAKMP: default group 1
00:02:24: ISAKMP: auth RSA sig
00:02:24: ISAKMP: life type in seconds
00:02:24: ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80
00:02:24: ISAKMP (0:2): atts are acceptable. Next payload is 0
00:02:24: ISAKMP (0:2): SA is doing RSA signature authentication
   using id type ID_FQDN
00:02:24: ISAKMP (0:2): Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
Old State = IKE_I_MM2 New State = IKE_I_MM2

00:02:24: ISAKMP (0:2): sending packet to 172.16.172.69 (I) MM_SA_SETUP
00:02:24: ISAKMP (0:2): Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
Old State = IKE_I_MM2 New State = IKE_I_MM3

00:02:24: ISAKMP (0:2): received packet from 172.16.172.69 (I) MM_SA_SETUP
00:02:24: ISAKMP (0:2): Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
.ld State = IKE_I_MM3 New State = IKE_I_MM4

00:02:24: ISAKMP (0:2): processing KE payload. message ID = 0
00:02:24: ISAKMP (0:2): processing NONCE payload. message ID = 0
00:02:24: ISAKMP (0:2): SKEYID state generated
00:02:24: ISAKMP (0:2): processing CERT_REQ payload. message ID = 0 00:02:24: ISAKMP (0:2): peer wants a CT_X509_SIGNATURE cert 00:02:24: ISAKMP (0:2): peer want cert issued by CN = SJPKICA, OU = SJPKI, O = SJTAC, L = SAN JOSE, ST = CA, C = US 00:02:24: ISAKMP (0:2): can't find router cert for signature! 00:02:24: ISAKMP (2): issuer name is not a trusted root. 00:02:24: ISAKMP (0:2): processing CERT_REQ payload. message ID = 0 00:02:24: ISAKMP (0:2): peer wants a CT_X509_SIGNATURE cert 00:02:24: ISAKMP (0:2): peer want cert issued by OU = sjvpn, O = cisco, C = us 00:02:24: ISAKMP (0:2): processing vendor id payload 00:02:24: ISAKMP (0:2): speaking to another IOS box! 00:02:24: ISAKMP (0:2): Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE Old State = IKE_I_MM4 New State = IKE_I_MM4 00:02:24: ISAKMP (2): ID payload next-payload : 6 type : 2 protocol : 17 port : 500 length : 19 00:02:24: ISAKMP (2): Total payload length: 23 00:02:24: ISAKMP (0:2): sending packet to 172.16.172.69 (I) MM_KEY_EXCH 00:02:24: ISAKMP (0:2): Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE Old State = IKE_I_MM4 New State = IKE_I_MM5 . 00:02:26: ISAKMP (0:2): received packet from 172.16.172.69 (I) MM_KEY_EXCH 00:02:26: ISAKMP (0:2): Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH Old State = IKE_I_MM5 New State = UNKNOWN 00:02:26: ISAKMP (0:2): processing ID payload. message ID = 0 **00:02:26: ISAKMP (0:2): processing CERT payload. message ID = 0 00:02:26: ISAKMP (0:2): processing a CT_X509_SIGNATURE cert 00:02:26: CRYPTO_PKI: status = 0: poll CRL 00:02:27: CRYPTO_PKI: ldap_bind() succeeded. 00:02:27: CRYPTO_PKI: set CRL update timer with delay: 46206 00:02:27: CRYPTO_PKI: the current router time: 13:07:32 UTC Jan 14 2002 00:02:27: CRYPTO_PKI: the last CRL update time: 00:57:38 UTC Jan 14 2002 00:02:27: CRYPTO_PKI: the next CRL update time: 01:57:38 UTC Jan 15 2002 00:02:27: CRYPTO_PKI: status = 0: failed to get public key from the storage 00:02:27: CRYPTO_PKI: status = 65535: failed to get issuer pubkey in cert 00:02:27: CRYPTO_PKI: status = 0: failed to get public key from the storage 00:02:27: CRYPTO_PKI: status = 65535: failed to get issuer pubkey in cert 00:02:27: CRYPTO_PKI: status = 0: failed to get public key from the storage 00:02:27: CRYPTO_PKI: status = 65535: failed to get issuer pubkey in cert 00:02:28: CRYPTO_PKI: transaction GetCRL completed 00:02:28: CRYPTO_PKI: blocking callback received status: 105 00:02:28: CRYPTO_PKI: Certificate verified, chain status= 1 00:02:28: ISAKMP (0:2): processing SIG payload. message ID = 0 00:02:28: ISAKMP (2): sa->peer.name = , sa->peer_id.id.id_fqdn.fqdn = SJhub.sjtac.com** 00:02:28: ISAKMP:received payload type 14 00:02:28: ISAKMP (0:2): processing keep alive: proposal=10/2 sec., actual=10/2 sec. 00:02:28: ISA.!! Success rate is 40 percent (2/5), round-trip min/avg/max = 1/2/4 ms SJVPN#KMP (0:2): peer knows about the keepalive extension mechanism. 00:02:28: ISAKMP (0:2): read keepalive extended attribute VPI: /0x2/0x4 00:02:28: ISAKMP (0:2): peer keepalives capabilities: 0x1 **00:02:28: ISAKMP (0:2): SA has been authenticated with 172.16.172.69** 00:02:28: ISAKMP (0:2): Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE Old State = UNKNOWN New State = UNKNOWN 00:02:28: ISAKMP (0:2): Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE Old State = UNKNOWN New State = IKE_P1_COMPLETE 00:02:28: ISAKMP (0:2): beginning Quick Mode exchange, M-ID of -304515331 00:02:28: ISAKMP (0:2): sending packet to 172.16.172.69 (I) QM_IDLE 00:02:28: ISAKMP (0:2): Node -304515331, Input = IKE_MESG_INTERNAL, IKE_INIT_QM Old State = IKE_QM_READY New State = IKE_QM_I_QM1 00:02:28: ISAKMP (0:2): Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE 00:02:28: ISAKMP (0:2): received packet from 172.16.172.69 (I) QM_IDLE 00:02:28: ISAKMP (0:2): processing HASH payload. message ID = -304515331 00:02:28: ISAKMP (0:2): processing SA payload. message ID = -304515331 00:02:28: ISAKMP (0:2): Checking IPSec proposal 1 00:02:28: ISAKMP: transform 1, ESP_DES 00:02:28: ISAKMP:

```
attributes in transform: 00:02:28: ISAKMP: encaps is 1 00:02:28: ISAKMP: SA life type in seconds
00:02:28: ISAKMP: SA life duration (basic) of 3600 00:02:28: ISAKMP: SA life type in kilobytes
00:02:28: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0 00:02:28: ISAKMP: authenticator is
HMAC-MD5 00:02:28: ISAKMP (0:2): atts are acceptable. 00:02:28:
IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) dest= 172.16.172.69, src=
172.16.172.52, dest_proxy= 20.1.1.0/255.255.255.0/0/0 (type=4), src_proxy=
50.1.1.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform= esp-des esp-md5-hmac , lifedur=
0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4 00:02:28: ISAKMP (0:2): processing
NONCE payload. message ID = -304515331 00:02:28: ISAKMP (0:2): processing ID payload. message ID
= -304515331 00:02:28: ISAKMP (0:2): processing ID payload. message ID = -304515331 00:02:28:
ISAKMP (0:2): Creating IPSec SAs 00:02:28: inbound SA from 172.16.172.69 to 172.16.172.52 (proxy
20.1.1.0 to 50.1.1.0) 00:02:28: has spi 0xFA8261EB and conn_id 2029 and flags 4 00:02:28:
lifetime of 3600 seconds 00:02:28: lifetime of 4608000 kilobytes 00:02:28: outbound SA from
172.16.172.52 to 172.16.172.69 (proxy 50.1.1.0 to 20.1.1.0 ) 00:02:28: has spi 206728450 and
conn_id 2030 and flags 4 00:02:28: lifetime of 3600 seconds 00:02:28: lifetime of 4608000
kilobytes 00:02:28: IPSEC(key_engine): got a queue event... 00:02:28: IPSEC(initialize_sas): ,
(key eng. msg.) dest= 172.16.172.52, src= 172.16.172.69, dest_proxy= 50.1.1.0/255.255.255.0/0/0
(type=4), src_proxy= 20.1.1.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform= esp-des esp-
md5-hmac , lifedur= 3600s and 4608000kb, spi= 0xFA8261EB(4202848747), conn_id= 2029, keysize= 0,
flags= 0x4 00:02:28: IPSEC(initialize_sas): , (key eng. msg.) src= 172.16.172.52, dest=
172.16.172.69, src_proxy= 50.1.1.0/255.255.255.0/0/0 (type=4), dest_proxy=
20.1.1.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform= esp-des esp-md5-hmac , lifedur=
3600s and 4608000kb, spi= 0xC526D02(206728450), conn_id= 2030, keysize= 0, flags= 0x4 00:02:28:
IPSEC(create_sa): sa created, (sa) sa_dest= 172.16.172.52, sa_prot= 50, sa_spi=
0xFA8261EB(4202848747), sa_trans= esp-des esp-md5-hmac , sa_conn_id= 2029 00:02:28:
IPSEC(create_sa): sa created, (sa) sa_dest= 172.16.172.69, sa_prot= 50, sa_spi=
0xC526D02(206728450), sa_trans= esp-des esp-md5-hmac , sa_conn_id= 2030 00:02:28: ISAKMP (0:2):
sending packet to 172.16.172.69 (I) QM_IDLE 00:02:28: ISAKMP (0:2): deleting node -304515331
error FALSE reason "" 00:02:28: ISAKMP (0:2): Node -304515331, Input = IKE_MESG_FROM_PEER,
IKE_QM_EXCH Old State = IKE_QM_I_QM1 New State = IKE_QM_PHASE2_COMPLETE 00:02:36: ISAKMP (0:2):
received packet from 172.16.172.69 (I) QM_IDLE 00:02:36: ISAKMP (0:2): processing HASH payload.
message ID = -2051070354 00:02:36: ISAKMP (0:2): processing NOTIFY ITS_ALIVE protocol 1 spi 0,
message ID = -2051070354, sa = 62DF2768 00:02:36: ISAKMP (0:2): deleting node -2051070354 error
FALSE reason "informational (in) state 1" 00:02:36: ISAKMP (0:2): Input = IKE_MESG_FROM_PEER,
IKE_INFO_NOTIFY Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE 00:02:36: ISAKMP (0:2):
sending packet to 172.16.172.69 (I) QM_IDLE 00:02:36: ISAKMP (0:2): purging node -739583249
00:02:36: ISAKMP (0:2): Input = IKE_MESG_FROM_PEER, IKE_MESG_KEEP_ALIVE Old State =
IKE_P1_COMPLETE New State = IKE_P1_COMPLETE
```

Debugs collectés sur SJhub

```
00:02:18: ISAKMP (0:0): received packet from 172.16.172.52 (N) NEW SA
00:02:18: ISAKMP: local port 500, remote port 500
00:02:18: ISAKMP (0:2): Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
Old State = IKE_READY New State = IKE_R_MM1
00:02:18: ISAKMP (0:2): processing SA payload. message ID = 0
00:02:18: ISAKMP (0:2): Checking ISAKMP transform 1 against priority 1 policy
00:02:18: ISAKMP: encryption DES-CBC
00:02:18: ISAKMP: hash MD5
00:02:18: ISAKMP: default group 1
00:02:18: ISAKMP: auth RSA sig
00:02:18: ISAKMP: life type in seconds
00:02:18: ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80
00:02:18: ISAKMP (0:2): atts are acceptable. Next payload is 3
00:02:18: ISAKMP (0:2): Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
Old State = IKE_R_MM1 New State = IKE_R_MM1

00:02:18: ISAKMP (0:2): SA is doing RSA signature authentication
   using id type ID_FQDN
00:02:18: ISAKMP (0:2): sending packet to 172.16.172.52 (R) MM_SA_SETUP
00:02:18: ISAKMP (0:2): Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
Old State = IKE_R_MM1 New State = IKE_R_MM2
```

```
00:02:18: ISAKMP (0:2): received packet from 172.16.172.52 (R) MM_SA_SETUP
00:02:18: ISAKMP (0:2): Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
Old State = IKE_R_MM2 New State = IKE_R_MM3

00:02:18: ISAKMP (0:2): processing KE payload. message ID = 0
00:02:19: ISAKMP (0:2): processing NONCE payload. message ID = 0
00:02:19: ISAKMP (0:2): SKEYID state generated
```

00:02:19: ISAKMP (0:2): processing CERT_REQ payload. message ID = 0 00:02:19: ISAKMP (0:2): peer wants a CT_X509_SIGNATURE cert 00:02:19: ISAKMP (0:2): peer want cert issued by OU = sjvpn, O = cisco, C = us 00:02:19: ISAKMP (0:2): processing vendor id payload 00:02:19: ISAKMP (0:2): speaking to another IOS box! 00:02:19: ISAKMP (0:2): Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE Old State = IKE_R_MM3 New State = IKE_R_MM3 00:02:19: ISAKMP (0:2): sending packet to 172.16.172.52 (R) MM_KEY_EXCH 00:02:19: ISAKMP (0:2): Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE Old State = IKE_R_MM3 New State = IKE_R_MM4 00:02:19: ISAKMP (0:2): received packet from 172.16.172.52 (R) MM_KEY_EXCH 00:02:19: ISAKMP (0:2): Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH Old State = IKE_R_MM4 New State = IKE_R_MM5 00:02:19: ISAKMP (0:2): processing ID payload. message ID = 0 **00:02:19: ISAKMP (0:2): processing CERT payload. message ID = 0 00:02:19: ISAKMP (0:2): processing a CT_X509_SIGNATURE cert 00:02:19: CRYPTO_PKI: status = 0: poll CRL 00:02:19: CRYPTO_PKI: ldap_bind() succeeded. 00:02:20: CRYPTO_PKI: set CRL update timer with delay: 49920 00:02:20: CRYPTO_PKI: the current router time: 12:05:38 UTC Jan 14 2002 00:02:20: CRYPTO_PKI: the last CRL update time: 00:57:38 UTC Jan 14 2002 00:02:20: CRYPTO_PKI: the next CRL update time: 01:57:38 UTC Jan 15 2002 00:02:20: CRYPTO_PKI: status = 0: failed to get public key from the storage 00:02:20: CRYPTO_PKI: status = 65535: failed to get issuer pubkey in cert 00:02:20: CRYPTO_PKI: status = 0: failed to get public key from the storage 00:02:20: CRYPTO_PKI: status = 65535: failed to get issuer pubkey in cert 00:02:20: CRYPTO_PKI: status = 0: failed to get public key from the storage 00:02:20: CRYPTO_PKI: status = 65535: failed to get issuer pubkey in cert 00:02:20: CRYPTO_PKI: status = 0: failed to get public key from the storage 00:02:20: CRYPTO_PKI: status = 65535: failed to get issuer pubkey in cert 00:02:20: CRYPTO_PKI: status = 0: failed to get public key from the storage 00:02:20: CRYPTO_PKI: status = 65535: failed to get issuer pubkey in cert 00:02:20: CRYPTO_PKI: status = 0: failed to get public key from the storage 00:02:20: CRYPTO_PKI: status = 65535: failed to get issuer pubkey in cert 00:02:21: CRYPTO_PKI: transaction GetCRL completed 00:02:21: CRYPTO_PKI: blocking callback received status: 105 00:02:21: CRYPTO_PKI: Certificate verified, chain status= 1 00:02:21: ISAKMP (0:2): processing SIG payload. message ID = 0 00:02:21: ISAKMP (2): sa->peer.name = , sa->peer_id.id.id_fqdn.fqdn = SJVPN.sjvpn.com** 00:02:21: ISAKMP:received payload type 14 00:02:21: ISAKMP (0:2): processing keep alive: proposal=10/2 sec., actual=10/2 sec. 00:02:21: ISAKMP (0:2): peer knows about the keepalive extension mechanism. 00:02:21: ISAKMP (0:2): read keepalive extended attribute VPI: /0x2/0x4 00:02:21: ISAKMP (0:2): peer keepalives capabilities: 0x1 **00:02:21: ISAKMP (0:2): SA has been authenticated with 172.16.172.52** 00:02:21: ISAKMP (0:2): Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE Old State = IKE_R_MM5 New State = IKE_R_MM5 00:02:21: ISAKMP (2): ID payload next-payload : 6 type : 2 protocol : 17 port : 500 length : 19 00:02:21: ISAKMP (2): Total payload length: 23 00:02:21: ISAKMP (0:2): sending packet to 172.16.172.52 (R) QM_IDLE 00:02:21: ISAKMP (0:2): Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE Old State = IKE_R_MM5 New State = IKE_P1_COMPLETE 00:02:23: ISAKMP (0:2): received packet from 172.16.172.52 (R) QM_IDLE 00:02:23: ISAKMP (0:2): processing HASH payload. message ID = -304515331 00:02:23: ISAKMP (0:2): processing SA payload. message ID = -304515331 00:02:23: ISAKMP (0:2): Checking IPSec proposal 1 00:02:23: ISAKMP: transform 1, ESP_DES 00:02:23: ISAKMP: attributes in transform: 00:02:23: ISAKMP: encaps is 1 00:02:23: ISAKMP: SA life type in seconds 00:02:23: ISAKMP: SA life duration (basic) of 3600 00:02:23: ISAKMP: SA life type in kilobytes 00:02:23: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0 00:02:23: ISAKMP: authenticator is HMAC-MD5 00:02:23: ISAKMP (0:2): atts are acceptable. 00:02:23: IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) dest= 172.16.172.69, src= 172.16.172.52, dest_proxy= 20.1.1.0/255.255.255.0/0/0 (type=4), src_proxy= 50.1.1.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform= esp-des esp-md5-hmac , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4 00:02:23: ISAKMP (0:2): processing NONCE payload. message ID = -304515331 00:02:23: ISAKMP (0:2): processing ID payload. message ID = -304515331 00:02:23: ISAKMP (2): ID_IPV4_ADDR_SUBNET src 50.1.1.0/255.255.255.0 prot 0 port 0 00:02:23: ISAKMP (0:2): processing ID payload. message ID = -304515331 00:02:23: ISAKMP (2): ID_IPV4_ADDR_SUBNET dst 20.1.1.0/255.255.255.0 prot 0 port 0 00:02:23: ISAKMP (0:2): asking for 1 spis from ipsec 00:02:23: ISAKMP (0:2): Node -304515331, Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH Old State = IKE_QM_READY New State = IKE_QM_SPI_STARVE 00:02:23: IPSEC(key_engine): got a queue event... 00:02:23: IPSEC(spi_response): getting spi 206728450 for SA from 172.16.172.52 to 172.16.172.69 for prot 3 00:02:23: ISAKMP: received ke message (2/1) 00:02:23: ISAKMP (0:2): sending packet to 172.16.172.52 (R) QM_IDLE 00:02:23: ISAKMP (0:2): Node -

```
304515331, Input = IKE_MESG_FROM_IPSEC, IKE_SPI_REPLY Old State = IKE_QM_SPI_STARVE New State =
IKE_QM_R_QM2 00:02:23: ISAKMP (0:2): received packet from 172.16.172.52 (R) QM_IDLE 00:02:23:
ISAKMP (0:2): Creating IPSec SAs 00:02:23: inbound SA from 172.16.172.52 to 172.16.172.69 (proxy
50.1.1.0 to 20.1.1.0) 00:02:23: has spi 0xC526D02 and conn_id 2000 and flags 4 00:02:23:
lifetime of 3600 seconds 00:02:23: lifetime of 4608000 kilobytes 00:02:23: outbound SA from
172.16.172.69 to 172.16.172.52 (proxy 20.1.1.0 to 50.1.1.0 ) 00:02:23: has spi -92118549 and
conn_id 2001 and flags 4 00:02:23: lifetime of 3600 seconds 00:02:23: lifetime of 4608000
kilobytes 00:02:23: ISAKMP (0:2): deleting node -304515331 error FALSE reason "quick mode done
(await()" 00:02:23: ISAKMP (0:2): Node -304515331, Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH Old
State = IKE_QM_R_QM2 New State = IKE_QM_PHASE2_COMPLETE 00:02:23: IPSEC(key_engine): got a queue
event... 00:02:23: IPSEC(initialize_sas): , (key eng. msg.) dest= 172.16.172.69, src=
172.16.172.52, dest_proxy= 20.1.1.0/255.255.255.0/0/0 (type=4), src_proxy=
50.1.1.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform= esp-des esp-md5-hmac , lifedur=
3600s and 4608000kb, spi= 0xC526D02(206728450), conn_id= 2000, keysize= 0, flags= 0x4 00:02:23:
IPSEC(initialize_sas): , (key eng. msg.) src= 172.16.172.69, dest= 172.16.172.52, src_proxy=
20.1.1.0/255.255.255.0/0/0 (type=4), dest_proxy= 50.1.1.0/255.255.255.0/0/0 (type=4), protocol=
ESP, transform= esp-des esp-md5-hmac , lifedur= 3600s and 4608000kb, spi=
0xFA8261EB(4202848747), conn_id= 2001, keysize= 0, flags= 0x4 00:02:23: IPSEC(create_sa): sa
created, (sa) sa_dest= 172.16.172.69, sa_prot= 50, sa_spi= 0xC526D02(206728450), sa_trans= esp-
des esp-md5-hmac , sa_conn_id= 2000 00:02:23: IPSEC(create_sa): sa created, (sa) sa_dest=
172.16.172.52, sa_prot= 50, sa_spi= 0xFA8261EB(4202848747), sa_trans= esp-des esp-md5-hmac ,
sa_conn_id= 2001 00:02:31: ISAKMP (0:2): sending packet to 172.16.172.52 (R) QM_IDLE 00:02:31:
ISAKMP (0:2): purging node -2051070354 00:02:31: ISAKMP (0:2): Input = IKE_MESG_FROM_TIMER,
IKE_TIMER_IM_ALIVE Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE 00:02:31: ISAKMP
(0:2): received packet from 172.16.172.52 (R) QM_IDLE 00:02:31: ISAKMP (0:2): processing HASH
payload. message ID = -739583249 00:02:31: ISAKMP (0:2): processing NOTIFY ITS_ALIVE_ACK
protocol 1 spi 0, message ID = -739583249, sa = 62DF5324 00:02:31: ISAKMP (0:2): peer
172.16.172.52 is alive! 00:02:31: ISAKMP (0:2): deleting node -739583249 error FALSE reason
"informational (in) state 1" 00:02:31: ISAKMP (0:2): Input = IKE_MESG_FROM_PEER, IKE_INFO_NOTIFY
Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE
```

Liste des révocations de certificat (CRL) cachant sur les Routeurs

```
SJVPN#show crypto ca crls CRL Issuer Name: OU = sjvpn, O = cisco, C = us LastUpdate: 00:57:38
UTC Jan 14 2002 NextUpdate: 01:57:38 UTC Jan 15 2002 Retrieved from CRL Distribution Point:
LDAP: CN = CRL1, OU = sjvpn, O = cisco, C = us SJhub#show crypto ca crls CRL Issuer Name: OU =
sjvpn, O = cisco, C = us LastUpdate: 00:57:38 UTC Jan 14 2002 NextUpdate: 01:57:38 UTC Jan 15
2002 Retrieved from CRL Distribution Point: LDAP: CN = CRL1, OU = sjvpn, O = cisco, C = us
```

Certificats d'un serveur de Microsoft CA

Ce qui suit met au point a été collecté sur SJPKI et SJhub pendant la négociation d'IKE. Après que SJPKI vérifie la première charge utile CERT_REQ, il trouve déjà les Certificats assortis dans sa base de données, ainsi il ne continue pas à regarder dans la deuxième charge utile CERT_REQ. Dans ce cas, des Certificats du serveur de Microsoft CA sont utilisés pour l'authentification d'IKE.

- Debugs collectés sur SJPKI
- Debugs collectés sur SJhub

Debugs collectés sur SJPKI

```
2d21h: IPSEC(sa_request): ,
(key eng. msg.) src= 172.16.172.10, dest= 172.16.172.69,
src_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),
dest_proxy= 20.1.1.0/255.255.255.0/0/0 (type=4),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 3600s and 4608000kb,
spi= 0xE8559075(3897921653), conn_id= 0, keysize= 0, flags= 0x4004
2d21h: ISAKMP: received ke message (1/1)
```

2d21h: ISAKMP: local port 500, remote port 500
2d21h: ISAKMP (0:1): Input = IKE_MESG_FROM_IPSEC, IKE_SA_REQ_MM
Old State = IKE_READY New State = IKE_I_MM1
2d21h: ISAKMP (0:1): beginning Main Mode exchange
2d21h: ISAKMP (0:1): sending packet to 172.16.172.69 (I) MM_NO_STATE
2d21h: ISAKMP (0:1): received packet from 172.16.172.69 (I) MM_NO_STATE
2d21h: ISAKMP (0:1): Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
Old State = IKE_I_MM1 New State = IKE_I_MM2

2d21h: ISAKMP (0:1): processing SA payload. message ID = 0
2d21h: ISAKMP (0:1): Checking ISAKMP transform 1 against priority 1 policy
2d21h: ISAKMP: encryption DES-CBC
2d21h: ISAKMP: hash MD5
2d21h: ISAKMP: default group 1
2d21h: ISAKMP: auth RSA sig
2d21h: ISAKMP: life type in seconds
2d21h: ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80
2d21h: ISAKMP (0:1): atts are acceptable. Next payload is 0
2d21h: ISAKMP (0:1): SA is doing RSA signature authentication
   using id type ID_FQDN
2d21h: ISAKMP (0:1): Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
Old State = IKE_I_MM2 New State = IKE_I_MM2

2d21h: ISAKMP (0:1): sending packet to 172.16.172.69 (I) MM_SA_SETUP
2d21h: ISAKMP (0:1): Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
Old State = IKE_I_MM2 New State = IKE_I_MM3

2d21h: ISAKMP (0:1): received packet from 172.16.172.69 (I) MM_SA_SETUP
2d21h: ISAKMP (0:1): Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
Old State = IKE_I_MM3 New State = IKE_I_MM4

2d21h: ISAKMP (0:1): processing KE payload. message ID = 0
2d21h:.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/3/4 ms
SJPKI# ISAKMP (0:1): processing NONCE payload. message ID = 0
2d21h: ISAKMP (0:1): SKEYID state generated
2d21h: ISAKMP (0:1): processing CERT_REQ payload. message ID = 0 2d21h: ISAKMP (0:1): peer wants a CT_X509_SIGNATURE cert 2d21h: ISAKMP (0:1): peer want cert issued by CN = SJPKICA, OU = SJPKI, O = SJTAC, L = SAN JOSE, ST = CA, C = US 2d21h: ISAKMP (0:1): already have a matching cert for this peer. Finish processing cert req. 2d21h: ISAKMP (0:1): processing vendor id payload 2d21h: ISAKMP (0:1): speaking to another IOS box! 2d21h: ISAKMP (0:1): Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE Old State = IKE_I_MM4 New State = IKE_I_MM4 2d21h: ISAKMP (1): ID payload next-payload : 6 type : 2 protocol : 17 port : 500 length : 15 2d21h: ISAKMP (1): Total payload length: 19 2d21h: ISKAMP: growing send buffer from 1024 to 3072 2d21h: ISAKMP (0:1): sending packet to 172.16.172.69 (I) MM_KEY_EXCH 2d21h: ISAKMP (0:1): Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE Old State = IKE_I_MM4 New State = IKE_I_MM5 2d21h: ISAKMP (0:1): received packet from 172.16.172.69 (I) MM_KEY_EXCH 2d21h: ISAKMP (0:1): Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH Old State = IKE_I_MM5 New State = UNKNOWN 2d21h: ISAKMP (0:1): processing ID payload. message ID = 0 **2d21h: ISAKMP (0:1): processing CERT payload. message ID = 0 2d21h: ISAKMP (0:1): processing a CT_X509_SIGNATURE cert 2d21h: CRYPTO_PKI: status = 0: crl check ignored 2d21h: CRYPTO_PKI: WARNING: Certificate, private key or CRL was not found while selecting CRL 2d21h: CRYPTO_PKI: cert revocation status unknown. 2d21h: ISAKMP (0:1): cert approved with warning 2d21h: ISAKMP (0:1): processing SIG payload. message ID = 0 2d21h: ISAKMP (1): sa->peer.name = , sa->peer_id.id.id_fqdn.fqdn = SJhub.sjtac.com** 2d21h: ISAKMP:received payload type 14 2d21h: ISAKMP (0:1): processing keep alive: proposal=10/2 sec., actual=10/2 sec. 2d21h: ISAKMP (0:1): peer knows about the keepalive extension mechanism. 2d21h: ISAKMP (0:1): read keepalive extended attribute VPI: /0x2/0x4 2d21h: ISAKMP (0:1): peer keepalives capabilities: 0x1 2d21h: ISAKMP (0:1): SA has been authenticated with 172.16.172.69 2d21h: ISAKMP (0:1): Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE Old State = UNKNOWN New State = UNKNOWN 2d21h: ISAKMP (0:1): Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE Old State = UNKNOWN New State = IKE_P1_COMPLETE 2d21h: ISAKMP (0:1): beginning Quick Mode exchange, M-ID of -1644677681 2d21h: ISAKMP (0:1): sending packet to 172.16.172.69 (I) QM_IDLE 2d21h: ISAKMP (0:1): Node -1644677681, Input = IKE_MESG_INTERNAL, IKE_INIT_QM Old State = IKE_QM_READY New State = IKE_QM_I_QM1 2d21h: ISAKMP (0:1): Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE Old State =

```
IKE_P1_COMPLETE New State = IKE_P1_COMPLETE 2d21h: ISAKMP (0:1): received packet from
172.16.172.69 (I) QM_IDLE 2d21h: ISAKMP (0:1): processing HASH payload. message ID = -1644677681
2d21h: ISAKMP (0:1): processing SA payload. message ID = -1644677681 2d21h: ISAKMP (0:1):
Checking IPSec proposal 1 2d21h: ISAKMP: transform 1, ESP_DES 2d21h: ISAKMP: attributes in
transform: 2d21h: ISAKMP: encaps is 1 2d21h: ISAKMP: SA life type in seconds 2d21h: ISAKMP: SA
life duration (basic) of 3600 2d21h: ISAKMP: SA life type in kilobytes 2d21h: ISAKMP: SA life
duration (VPI) of 0x0 0x46 0x50 0x0 2d21h: ISAKMP: authenticator is HMAC-MD5 2d21h: ISAKMP
(0:1): atts are acceptable. 2d21h: IPSEC(validate_proposal_request): proposal part #1, (key eng.
msg.) dest= 172.16.172.69, src= 172.16.172.10, dest_proxy= 20.1.1.0/255.255.255.0/0/0 (type=4),
src_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4 2d21h: ISAKMP (0:1):
processing NONCE payload. message ID = -1644677681 2d21h: ISAKMP (0:1): processing ID payload.
message ID = -1644677681 2d21h: ISAKMP (0:1): processing ID payload. message ID = -1644677681
2d21h: ISAKMP (0:1): Creating IPSec SAs 2d21h: inbound SA from 172.16.172.69 to 172.16.172.10
(proxy 20.1.1.0 to 10.1.1.0) 2d21h: has spi 0xE8559075 and conn_id 2029 and flags 4 2d21h:
lifetime of 3600 seconds 2d21h: lifetime of 4608000 kilobytes 2d21h: outbound SA from
172.16.172.10 to 172.16.172.69 (proxy 10.1.1.0 to 20.1.1.0 ) 2d21h: has spi -889328648 and
conn_id 2030 and flags 4 2d21h: lifetime of 3600 seconds 2d21h: lifetime of 4608000 kilobytes
2d21h: IPSEC(key_engine): got a queue event... 2d21h: IPSEC(initialize_sas): , (key eng. msg.)
dest= 172.16.172.10, src= 172.16.172.69, dest_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),
src_proxy= 20.1.1.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 3600s and 4608000kb, spi= 0xE8559075(3897921653), conn_id= 2029, keysize= 0, flags= 0x4
2d21h: IPSEC(initialize_sas): , (key eng. msg.) src= 172.16.172.10, dest= 172.16.172.69,
src_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4), dest_proxy= 20.1.1.0/255.255.255.0/0/0 (type=4),
protocol= ESP, transform= esp-des esp-md5-hmac , lifedur= 3600s and 4608000kb, spi=
0xCAFDEBF8(3405638648), conn_id= 2030, keysize= 0, flags= 0x4 2d21h: IPSEC(create_sa): sa
created, (sa) sa_dest= 172.16.172.10, sa_prot= 50, sa_spi= 0xE8559075(3897921653), sa_trans=
esp-des esp-md5-hmac , sa_conn_id= 2029 2d21h: IPSEC(create_sa): sa created, (sa) sa_dest=
172.16.172.69, sa_prot= 50, sa_spi= 0xCAFDEBF8(3405638648), sa_trans= esp-des esp-md5-hmac ,
sa_conn_id= 2030 2d21h: ISAKMP (0:1): sending packet to 172.16.172.69 (I) QM_IDLE 2d21h: ISAKMP
(0:1): deleting node -1644677681 error FALSE reason "" 2d21h: ISAKMP (0:1): Node -1644677681,
Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH Old State = IKE_QM_I_QM1 New State =
IKE_QM_PHASE2_COMPLETE SJPKI# 2d22h: ISAKMP (0:1): received packet from 172.16.172.69 (I)
QM_IDLE 2d22h: ISAKMP (0:1): processing HASH payload. message ID = -2115263482 2d22h: ISAKMP
(0:1): processing NOTIFY ITS_ALIVE protocol 1 spi 0, message ID = -2115263482, sa = 6335D814
2d22h: ISAKMP (0:1): deleting node -2115263482 error FALSE reason "informational (in) state 1"
2d22h: ISAKMP (0:1): Input = IKE_MESG_FROM_PEER, IKE_INFO_NOTIFY Old State = IKE_P1_COMPLETE New
State = IKE_P1_COMPLETE 2d22h: ISAKMP (0:1): sending packet to 172.16.172.69 (I) QM_IDLE 2d22h:
ISAKMP (0:1): purging node -1850875331 2d22h: ISAKMP (0:1): Input = IKE_MESG_FROM_PEER,
IKE_MESG_KEEP_ALIVE SJPKI#Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE
```

Debugs collectés sur SJhub

```
SJhub#
00:07:26: ISAKMP (0:0): received packet from 172.16.172.10 (N) NEW SA
00:07:26: ISAKMP: local port 500, remote port 500
00:07:26: ISAKMP (0:3): Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
Old State = IKE_READY New State = IKE_R_MM1
00:07:26: ISAKMP (0:3): processing SA payload. message ID = 0
00:07:26: ISAKMP (0:3): Checking ISAKMP transform 1 against priority 1 policy
00:07:26: ISAKMP: encryption DES-CBC
00:07:26: ISAKMP: hash MD5
00:07:26: ISAKMP: default group 1
00:07:26: ISAKMP: auth RSA sig
00:07:26: ISAKMP: life type in seconds
00:07:26: ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80
00:07:26: ISAKMP (0:3): atts are acceptable. Next payload is 3
00:07:26: ISAKMP (0:3): Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
Old State = IKE_R_MM1 New State = IKE_R_MM1

00:07:26: ISAKMP (0:3): SA is doing RSA signature authentication
   using id type ID_FQDN
00:07:26: ISAKMP (0:3): sending packet to 172.16.172.10 (R) MM_SA_SETUP
```

00:07:26: ISAKMP (0:3): Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
Old State = IKE_R_MM1 New State = IKE_R_MM2

00:07:26: ISAKMP (0:3): received packet from 172.16.172.10 (R) MM_SA_SETUP
00:07:26: ISAKMP (0:3): Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
Old State = IKE_R_MM2 New State = IKE_R_MM3

00:07:26: ISAKMP (0:3): processing KE payload. message ID = 0
00:07:26: ISAKMP (0:3): processing NONCE payload. message ID = 0
00:07:26: ISAKMP (0:3): SKEYID state generated
00:07:26: ISAKMP (0:3): processing CERT_REQ payload. message ID = 0 00:07:26: ISAKMP (0:3): peer wants a CT_X509_SIGNATURE cert 00:07:26: ISAKMP (0:3): peer want cert issued by CN = SJPKICA, OU = SJPKI, O = SJTAC, L = SAN JOSE, ST = CA, C = US 00:07:26: ISAKMP (0:3): processing vendor id payload 00:07:26: ISAKMP (0:3): speaking to another IOS box! 00:07:26: ISAKMP (0:3): Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE Old State = IKE_R_MM3 New State = IKE_R_MM3 00:07:26: ISAKMP (0:3): sending packet to 172.16.172.10 (R) MM_KEY_EXCH 00:07:26: ISAKMP (0:3): Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE Old State = IKE_R_MM3 New State = IKE_R_MM4 00:07:26: ISAKMP (0:3): received packet from 172.16.172.10 (R) MM_KEY_EXCH 00:07:26: ISAKMP (0:3): Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH Old State = IKE_R_MM4 New State = IKE_R_MM5 00:07:26: ISAKMP (0:3): processing ID payload. message ID = 0 **00:07:26: ISAKMP (0:3): processing CERT payload. message ID = 0 00:07:26: ISAKMP (0:3): processing a CT_X509_SIGNATURE cert 00:07:26: CRYPTO_PKI: status = 0: crl check ignored 00:07:26: CRYPTO_PKI: WARNING: Certificate, private key or CRL was not found while selecting CRL 00:07:26: CRYPTO_PKI: cert revocation status unknown. 00:07:26: ISAKMP (0:3): cert approved with warning 00:07:26: ISAKMP (0:3): processing SIG payload. message ID = 0 00:07:26: ISAKMP (3): sa->peer.name = , sa->peer_id.id.id_fqdn.fqdn = SJPKI.sjtac** 00:07:26: ISAKMP:received payload type 14 00:07:26: ISAKMP (0:3): processing keep alive: proposal=10/2 sec., actual=10/2 sec. 00:07:26: ISAKMP (0:3): peer knows about the keepalive extension mechanism. 00:07:26: ISAKMP (0:3): read keepalive extended attribute VPI: /0x2/0x4 00:07:26: ISAKMP (0:3): peer keepalives capabilities: 0x1 00:07:26: ISAKMP (0:3): SA has been authenticated with 172.16.172.10 00:07:26: ISAKMP (0:3): Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE Old State = IKE_R_MM5 New State = IKE_R_MM5 00:07:26: ISAKMP (3): ID payload next-payload : 6 type : 2 protocol : 17 port : 500 length : 19 00:07:26: ISAKMP (3): Total payload length: 23 00:07:26: ISKAMP: growing send buffer from 1024 to 3072 00:07:26: ISAKMP (0:3): sending packet to 172.16.172.10 (R) QM_IDLE 00:07:26: ISAKMP (0:3): Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE Old State = IKE_R_MM5 New State = IKE_P1_COMPLETE 00:07:26: ISAKMP (0:3): received packet from 172.16.172.10 (R) QM_IDLE 00:07:26: ISAKMP (0:3): processing HASH payload. message ID = -1644677681 00:07:26: ISAKMP (0:3): processing SA payload. message ID = -1644677681 00:07:26: ISAKMP (0:3): Checking IPSec proposal 1 00:07:26: ISAKMP: transform 1, ESP_DES 00:07:26: ISAKMP: attributes in transform: 00:07:26: ISAKMP: encaps is 1 00:07:26: ISAKMP: SA life type in seconds 00:07:26: ISAKMP: SA life duration (basic) of 3600 00:07:26: ISAKMP: SA life type in kilobytes 00:07:26: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0 00:07:26: ISAKMP: authenticator is HMAC-MD5 00:07:26: ISAKMP (0:3): atts are acceptable. 00:07:26: IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) dest= 172.16.172.69, src= 172.16.172.10, dest_proxy= 20.1.1.0/255.255.255.0/0/0 (type=4), src_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform= esp-des esp-md5-hmac , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4 00:07:26: ISAKMP (0:3): processing NONCE payload. message ID = -1644677681 00:07:26: ISAKMP (0:3): processing ID payload. message ID = -1644677681 00:07:26: ISAKMP (3): ID_IPV4_ADDR_SUBNET src 10.1.1.0/255.255.255.0 prot 0 port 0 00:07:26: ISAKMP (0:3): processing ID payload. message ID = -1644677681 00:07:26: ISAKMP (3): ID_IPV4_ADDR_SUBNET dst 20.1.1.0/255.255.255.0 prot 0 port 0 00:07:26: ISAKMP (0:3): asking for 1 spis from ipsec 00:07:26: ISAKMP (0:3): Node -1644677681, Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH Old State = IKE_QM_READY New State = IKE_QM_SPI_STARVE 00:07:26: IPSEC(key_engine): got a queue event... 00:07:26: IPSEC(spi_response): getting spi 3405638648 for SA from 172.16.172.10 to 172.16.172.69 for prot 3 00:07:26: ISAKMP: received ke message (2/1) 00:07:27: ISAKMP (0:3): sending packet to 172.16.172.10 (R) QM_IDLE 00:07:27: ISAKMP (0:3): Node -1644677681, Input = IKE_MESG_FROM_IPSEC, IKE_SPI_REPLY Old State = IKE_QM_SPI_STARVE New State = IKE_QM_R_QM2 00:07:27: ISAKMP (0:3): received packet from 172.16.172.10 (R) QM_IDLE 00:07:27: ISAKMP (0:3): Creating IPSec SAs 00:07:27: inbound SA from 172.16.172.10 to 172.16.172.69 (proxy 10.1.1.0 to 20.1.1.0) 00:07:27: has spi 0xCAFDEBF8 and conn_id 2002 and flags 4 00:07:27: lifetime of 3600 seconds 00:07:27: lifetime of 4608000 kilobytes 00:07:27: outbound SA from 172.16.172.69 to 172.16.172.10 (proxy 20.1.1.0 to 10.1.1.0) 00:07:27: has spi -397045643 and conn_id 2003 and flags 4 00:07:27: lifetime of 3600 seconds 00:07:27: lifetime of 4608000 kilobytes 00:07:27: ISAKMP (0:3): deleting node -1644677681 error FALSE reason "quick mode done (await()" 00:07:27: ISAKMP (0:3): Node -1644677681, Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH Old

```
State = IKE_QM_R_QM2 New State = IKE_QM_PHASE2_COMPLETE 00:07:27: IPSEC(key_engine): got a queue
event... 00:07:27: IPSEC(initialize_sas): , (key eng. msg.) dest= 172.16.172.69, src=
172.16.172.10, dest_proxy= 20.1.1.0/255.255.255.0/0/0 (type=4), src_proxy=
10.1.1.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform= esp-des esp-md5-hmac , lifedur=
3600s and 4608000kb, spi= 0xCAFDEBF8(3405638648), conn_id= 2002, keysize= 0, flags= 0x4
00:07:27: IPSEC(initialize_sas): , (key eng. msg.) src= 172.16.172.69, dest= 172.16.172.10,
src_proxy= 20.1.1.0/255.255.255.0/0/0 (type=4), dest_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),
protocol= ESP, transform= esp-des esp-md5-hmac , lifedur= 3600s and 4608000kb, spi=
0xE8559075(3897921653), conn_id= 2003, keysize= 0, flags= 0x4 00:07:27: IPSEC(create_sa): sa
created, (sa) sa_dest= 172.16.172.69, sa_prot= 50, sa_spi= 0xCAFDEBF8(3405638648), sa_trans=
esp-des esp-md5-hmac , sa_conn_id= 2002 00:07:27: IPSEC(create_sa): sa created, (sa) sa_dest=
172.16.172.10, sa_prot= 50, sa_spi= 0xE8559075(3897921653), sa_trans= esp-des esp-md5-hmac ,
sa_conn_id= 2003 00:07:30: ISAKMP (0:2): sending packet to 172.16.172.52 (R) QM_IDLE 00:07:30:
ISAKMP (0:2): purging node -652282805 00:07:30: ISAKMP (0:2): Input = IKE_MESG_FROM_TIMER,
IKE_TIMER_IM_ALIVE Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE 00:07:30: ISAKMP
(0:2): received packet from 172.16.172.52 (R) QM_IDLE 00:07:30: ISAKMP (0:2): processing HASH
payload. message ID = 564680579 00:07:30: ISAKMP (0:2): processing NOTIFY ITS_ALIVE_ACK protocol
1 spi 0, message ID = 564680579, sa = 62DF5324 00:07:30: ISAKMP (0:2): peer 172.16.172.52 is
alive! 00:07:30: ISAKMP (0:2): deleting node 564680579 error FALSE reason "informational (in)
state 1" 00:07:30: ISAKMP (0:2): Input = IKE_MESG_FROM_PEER, IKE_INFO_NOTIFY Old State =
IKE_P1_COMPLETE New State = IKE_P1_COMPLETE 00:07:32: ISAKMP (0:2): purging node 1414513005
00:07:36: ISAKMP (0:3): sending packet to 172.16.172.10 (R) QM_IDLE 00:07:36: ISAKMP (0:3):
purging node -2115263482 00:07:36: ISAKMP (0:3): Input = IKE_MESG_FROM_TIMER, IKE_TIMER_IM_ALIVE
Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE 00:07:36: ISAKMP (0:3): received packet
from 172.16.172.10 (R) QM_IDLE 00:07:36: ISAKMP (0:3): processing HASH payload. message ID = -
1850875331 00:07:36: ISAKMP (0:3): processing NOTIFY ITS_ALIVE_ACK protocol 1 spi 0, message ID
= -1850875331, sa = 63338630 00:07:36: ISAKMP (0:3): peer 172.16.172.10 is alive! 00:07:36:
ISAKMP (0:3): deleting node -1850875331 error FALSE reason "informational (in) state 1"
00:07:36: ISAKMP (0:3): Input = IKE_MESG_FROM_PEER, IKE_INFO_NOTIFY Old State = IKE_P1_COMPLETE
New State = IKE_P1_COMPLETE 00:07:40: ISAKMP (0:2): received packet from 172.16.172.52 (R)
QM_IDLE 00:07:40: ISAKMP (0:2): processing HASH payload. message ID = 2075099983 00:07:40:
ISAKMP (0:2): processing NOTIFY ITS_ALIVE protocol 1 spi 0, message ID = 2075099983, sa =
62DF5324 00:07:40: ISAKMP (0:2): deleting node 2075099983 error FALSE reason "informational (in)
state 1" 00:07:40: ISAKMP (0:2): Input = IKE_MESG_FROM_PEER, IKE_INFO_NOTIFY Old State =
IKE_P1_COMPLETE New State = IKE_P1_COMPLETE 00:07:40: ISAKMP (0:2): sending packet to
172.16.172.52 (R) QM_IDLE 00:07:40: ISAKMP (0:2): purging node 1356214450 00:07:40: ISAKMP
(0:2): Input = IKE_MESG_FROM_PEER, IKE_MESG_KEEP_ALIVE Old State = IKE_P1_COMPLETE New State =
IKE_P1_COMPLETE
```

Sortie de la commande show

Vous pouvez utiliser la commande de **show crypto ipsec sa** de vérifier l'ISAKMP et les associations de sécurité d'IPSec sur les Routeurs après que les tunnels soient avec succès négociés. La sortie témoin est affichée ci-dessous.

```
SJhub#show crypto isakmp sa dst src state conn-id slot 172.16.172.69 172.16.172.10 QM_IDLE 3 0
172.16.172.69 172.16.172.52 QM_IDLE 2 0 SJhub#show crypto ipsec sa interface: Ethernet4/0 Crypto
map tag: vpn, local addr. 172.16.172.69 local ident (addr/mask/prot/port):
(20.1.1.0/255.255.255.0/0/0) remote ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
current_peer: 172.16.172.10 PERMIT, flags={origin_is_acl,} #pkts encaps: 4, #pkts encrypt: 4,
#pkts digest 4 #pkts decaps: 4, #pkts decrypt: 4, #pkts verify 4 #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.: 172.16.172.69, remote crypto endpt.:
172.16.172.10 path mtu 1500, media mtu 1500 current outbound spi: E8559075 inbound esp sas: spi:
0xCAFDEBF8(3405638648) 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):
(4607998/3434) IV size: 8 bytes replay detection support: Y inbound ah sas: inbound pcp sas:
outbound esp sas: spi: 0xE8559075(3897921653) 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): (4607999/3434) IV size: 8 bytes replay detection support: Y outbound ah sas:
outbound pcp sas: local ident (addr/mask/prot/port): (20.1.1.0/255.255.255.0/0/0) remote ident
(addr/mask/prot/port): (50.1.1.0/255.255.255.0/0/0) current_peer: 172.16.172.52 PERMIT,
flags={origin_is_acl,} #pkts encaps: 2, #pkts encrypt: 2, #pkts digest 2 #pkts decaps: 2, #pkts
```

decrypt: 2, #pkts verify 2 #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.: 172.16.172.69, remote crypto endpt.: 172.16.172.52 path mtu 1500, media mtu 1500 current outbound spi: FA8261EB inbound esp sas: spi: 0xC526D02(206728450) 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): (4607999/3108) IV size: 8 bytes replay detection support: Y inbound ah sas: inbound pcp sas: outbound esp sas: spi: 0xFA8261EB(4202848747) 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): (4607999/3108) IV size: 8 bytes replay detection support: Y outbound ah sas: outbound pcp sas: SJVPN#**show crypto isakmp sa** dst src state conn-id slot 172.16.172.69 172.16.172.52 QM_IDLE 2 0 SJVPN#**show crypto ipsec sa** interface: Ethernet1/0 **Crypto map tag: vpn, local addr. 172.16.172.52 local ident (addr/mask/prot/port): (50.1.1.0/255.255.255.0/0/0) remote ident (addr/mask/prot/port): (20.1.1.0/255.255.255.0/0/0) current_peer: 172.16.172.69 PERMIT, flags={origin_is_acl,} #pkts encaps: 2, #pkts encrypt: 2, #pkts digest 2 #pkts decaps: 2, #pkts decrypt: 2, #pkts verify 2 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0 #send errors 3, #recv errors 0** local crypto endpt.: 172.16.172.52, remote crypto endpt.: 172.16.172.69 path mtu 1500, media mtu 1500 current outbound spi: C526D02 inbound esp sas: spi: 0xFA8261EB(4202848747) transform: esp-des esp-md5-hmac , in use settings ={Tunnel, } slot: 0, conn id: 2029, flow_id: 1, crypto map: vpn sa timing: remaining key lifetime (k/sec): (4607999/3398) IV size: 8 bytes replay detection support: Y inbound ah sas: inbound pcp sas: outbound esp sas: spi: 0xC526D02(206728450) transform: esp-des esp-md5-hmac , in use settings ={Tunnel, } slot: 0, conn id: 2030, flow_id: 2, crypto map: vpn sa timing: remaining key lifetime (k/sec): (4607999/3389) IV size: 8 bytes replay detection support: Y outbound ah sas: outbound pcp sas: SJPKI#**show crypto isa sa** dst src state conn-id slot 172.16.172.69 172.16.172.10 QM_IDLE 1 0 SJPKI#**show crypto ipsec sa** interface: Ethernet1/0 **Crypto map tag: vpn, local addr. 172.16.172.10 local ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0) remote ident (addr/mask/prot/port): (20.1.1.0/255.255.255.0/0/0) current_peer: 172.16.172.69 PERMIT, flags={origin_is_acl,} #pkts encaps: 7, #pkts encrypt: 7, #pkts digest 7 #pkts decaps: 7, #pkts decrypt: 7, #pkts verify 7 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0 #send errors 3, #recv errors 0** local crypto endpt.: 172.16.172.10, remote crypto endpt.: 172.16.172.69 path mtu 1500, media mtu 1500 current outbound spi: CAFDEBF8 inbound esp sas: spi: 0xE8559075(3897921653) transform: esp-des esp-md5-hmac , in use settings ={Tunnel, } slot: 0, conn id: 2029, flow_id: 1, crypto map: vpn sa timing: remaining key lifetime (k/sec): (4607998/3308) IV size: 8 bytes replay detection support: Y inbound ah sas: inbound pcp sas: outbound esp sas: spi: 0xCAFDEBF8(3405638648) transform: esp-des esp-md5-hmac , in use settings ={Tunnel, } slot: 0, conn id: 2030, flow_id: 2, crypto map: vpn sa timing: remaining key lifetime (k/sec): (4607999/3308) IV size: 8 bytes replay detection support: Y outbound ah sas: outbound pcp sas:

Informations connexes

- Pages de support produit de sécurité IP (IPSec)
- Support technique - Cisco Systems