

Configuring DN–Based Crypto Maps for VPN Device Access Control

Document ID: 18303

Introduction

Prerequisites

Requirements

Components Used

Conventions

Background Information

Configure

Network Diagram

Configurations

Verify

Troubleshoot

Related Information

Introduction

This document describes how to configure Distinguished Name (DN)–based crypto maps to provide access control so that a VPN device can establish VPN tunnels with a Cisco IOS® router. In this document's example, Rivest, Shamir, and Adelman (RSA) signature is the method for the IKE authentication. In addition to standard certificate validation, DN–based crypto maps try to match the peer's ISAKMP identity with certain fields in its certificates, such as the X.500 distinguished name or the fully qualified domain name (FQDN).

Prerequisites

Requirements

This feature was first introduced in Cisco IOS Software Release 12.2(4)T. You must this release or later for this configuration.

The Cisco IOS Software Release 12.3(5) was also tested. However, the DN based crypto maps failed due to Cisco bug ID CSCed45783 (registered customers only) .

Components Used

The information in this document is based on these software and hardware versions:

- Cisco 7200 routers
- Cisco IOS Software Release 12.2(4)T1 c7200–ik8o3s–mz.122–4.T1

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

For more information on document conventions, refer to Cisco Technical Tips Conventions.

Background Information

Previously, during IKE authentication using the RSA signature method, and after certification validation and optional certificate revocation list (CRL) checking, Cisco IOS continued the IKE Quick Mode negotiation. It did not provide a method to prevent the remote VPN devices from communicating with any encrypted interfaces, other than restrictions on the encrypting peer's IP address.

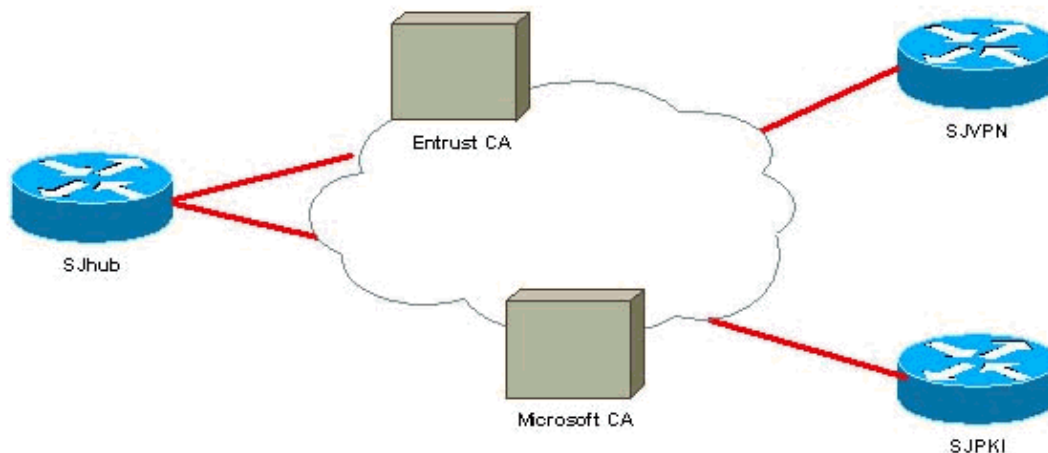
Now with DN-based crypto map, Cisco IOS can restrict remote VPN peers to only access selected interfaces with specific certificates. In particular, certificates with certain DNs or FQDNs.

Configure

In this section, you are presented with the information to configure the features described in this document.

Network Diagram

This document uses the network setup shown in this diagram.



Configurations

This document uses the configurations shown here.

In this example, a simple network setup is used to demonstrate the feature. SJhub router has two identity certificates, one from Entrust certificate authority (CA) and the other one from Microsoft CA. See the Related Information section to find out how to configure multiple-identity CAs on Cisco routers. SJhub has two interfaces, each of which has a DN-based crypto map applied. SJVPN and SJPKI are two routers configured as IPsec peers to SJhub. They are used as test routers to verify how the DN-based crypto map applied on SJhub can be used to restrict access of VPN peers.

SJhub (7200) Router configuration

```
SJhub#write terminal
Building configuration...

Current configuration : 19802 bytes
```

```

!
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

!--- Defines the crypto ca identity.
!--- This router has multiple identity certificates:
!--- one from Entrust CA, the other one from Microsoft CA.

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	BC95EAF7	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
7A163447 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 F2A3907F F236F508 43742D4A E89A76EF 3CB98722 D0A7DC1F 432F386C
721A3379 D50B7EA7 43C07AD0 AA6C087D FDA7BDBF 0BA92FA3 711A7F54 FBCAFBF6
633FCEFA AA9D9A8D 2C79550F 99314B3E FCA97F64 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 054E63CE00000000000003

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
```

```
!--- Defines ISAKMP policy.
```

```
!--- "rsa-sig" is the default IKE authentication method.
```

```
crypto isakmp policy 1
  hash md5
```

```
!--- Defines using router's hostname as the ISAKMP identity.
```

```
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
!
```

```
!--- Defines crypto map vpn.
```

```
!--- Also "set identity FromSJVPN" corresponds to "crypto identity FromSJVPN,"
```

```
!--- so only VPN devices with the certificate the DN defined in crypto
```

```
!--- identity FromSJVPN can access the interface to which
```

```
!--- the crypto map vpn is applied.
```

```
crypto map vpn 10 ipsec-isakmp
  set peer 172.16.172.52
  set transform-set myset
  set identity FromSJVPN
  match address 101
!
```

```
!--- Defines crypto map pki.
```

```
!--- Also "set identity FromSJPKI" corresponds to "crypto identity FromSJPKI,"
```

```
!--- so only VPN devices with the certificate the FQDN defined in crypto
```

```
!--- identity FromSJPKI can access the interface to which
```

```
!--- the crypto map pki is applied.
```

```
!
crypto map pki 10 ipsec-isakmp
  set peer 172.16.172.10
  set transform-set myset
  set identity FromSJPKI
  match address 102
!
```

```
!--- Defines the crypto identity which is linked
!--- to a specific crypto map.
!--- With FromSJVPN applied to crypto map vpn,
!--- only VPN devices that use their DN (with OU=sjvpn,O=cisco)
!--- as an ISAKMP identity are able to connect to the interface
!--- to which crypto map vpn is applied.
!--- With FromSJKPI applied to crypto map pki,
!--- only VPN devices that use their FQDN (matching SJKPI.sjpk.com)
!--- as an ISKAMP identity are able to connect to the interface
!--- to which crypto map pki is applied.
```

```
crypto identity FromSJVPN
```

```
dn OU=sjvpn
```

```
dn O=cisco
```

```
!
```

```
crypto identity FromSJKPI
```

```
fqdn SJKPI.sjpk.com
```

```
!
```

```
!
```

```
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 172.16.172.54 255.255.255.240
```

```
ip route-cache same-interface
```

```
no ip mroute-cache
```

```
duplex half
```

```
crypto map vpn
```

```
!
```

```
interface Ethernet4/1
```

```
ip address 172.16.172.13 255.255.255.240
```

```
duplex half
```

```
crypto map pki
```

```
!
```

```
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 10.1.1.0 255.255.255.0 172.16.172.1
```

```
ip route 50.1.1.0 255.255.255.0 172.16.172.48
```

```
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
```

SJhub#**show crypto ca cert**

Certificate

```
Status: Available  
Certificate Serial Number: 132BD14C00000000000B  
Key Usage: General Purpose  
Issuer:  
  CN = SJKICA  
  OU = SJKI  
  O = SJTAC  
  L = SAN JOSE  
  ST = CA  
  C = US  
Subject Name Contains:  
  Name: SJhub.sjtac.com  
CRL Distribution Point:  
  ldap:///CN=SJKICA,CN=sjvpnmspi,CN=CDP,CN=Public%20Key%20Services,  
CN=Services,CN=Configuration,DC=sjki,  
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: 054E60AD0000000000002  
Key Usage: Signature  
Issuer:  
  CN = SJKICA  
  OU = SJKI  
  O = SJTAC  
  L = SAN JOSE  
  ST = CA  
  C = US  
Subject:  
  CN = SJVPNRA  
  OU = SJKI  
  O = SJTAC  
  L = SAN JOSE  
  ST = CA
```

C = US
CRL Distribution Point:
ldap:///CN=SJKICA,CN=sjvpnmspi,CN=CDP,CN=Public%20Key%20Services,
CN=Services,CN=Configuration,DC=sjpk,
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 = SJKICA
OU = SJKI
O = SJTAC
L = SAN JOSE
ST = CA
C = US
Subject:
CN = SJVPNRA
OU = SJKI
O = SJTAC
L = SAN JOSE
ST = CA
C = US

CRL Distribution Point:
ldap:///CN=SJKICA,CN=sjvpnmspi,CN=CDP,CN=Public%20Key%20Services,
CN=Services,CN=Configuration,DC=sjpk,
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 = SJKICA
OU = SJKI
O = SJTAC
L = SAN JOSE
ST = CA
C = US
Subject:
CN = SJKICA
OU = SJKI
O = SJTAC
L = SAN JOSE
ST = CA
C = US

CRL Distribution Point:
ldap:///CN=SJKICA,CN=sjvpnmspi,CN=CDP,CN=Public%20Key%20Services,
CN=Services,CN=Configuration,DC=sjpk,
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
```

SJVPN (7200) Router Configuration

```
SJVPN#write terminal
Building configuration...

Current configuration : 8796 bytes
!
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 8B168FBF 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 433D46B6 B2D1DDC5 385C5135 DB2075F1 4D252ACF AC80DA4C 2111946F
26F7193B 8EA1CA66 8332D2A1 5310B2D7 07C985A8 0B44CE37 BC95EAF7 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

!---- Defines DN as the ISAKMP identity.
!---- SJVPN is configured to connect to the e4/0
!---- interface of the SJhub router.
!---- Since the crypto map applied on that interface
!---- checks for the DN, you need to make sure
!---- this router uses DN as the ISAKMP identity in the ID payload
!---- during the IKE negotiation with SJhub.

crypto isakmp identity dn
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 172.16.172.54
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 cert**

```
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 (7200) Router Configuration

```
SJPKI#write terminal
Building configuration...

Current configuration : 12338 bytes
!
! Last configuration change at 18:05:19 UTC Tue Jan 15 2002
! NVRAM config last updated at 18:00:50 UTC Tue Jan 15 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 sjpki.com
!
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 054E63CE00000000000003
  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 70028681 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 2CEFFFC7E B2C42AED 167FA630 AB3F9460 5E12B77F 07BC860A 48A5DBDB
E942F9B8 1B053148 05A70A17 B2EF37D4 F4234622 DD59571B F8D8AF09 2B54D40C 9145302Dquit

```
certificate 02A67C73000000000000E
3082044C 308203F6 A0030201 02020A02 A67C7300 00000000 0E300D06 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 31313531 37353232 315A170D 30343031
31353137 35323231 5A302031 1E301C06 092A8648 86F70D01 0902130F 534A504B
492E736A 706B692E 636F6D30 5C300D06 092A8648 86F70D01 01010500 034B0030
48024100 B11200E8 F624D6AF 829D5C7E F7E3B0BE BDF673B OCBDE855 3CBB6380
4924DD74 B94263D2 DFD84B99 30394E52 0C275781 5E7B6DAD AF18215C 8B89239A
2EA27CC5 02030100 01A38202 D1308202 CD300B06 03551D0F 04040302 05A0301D
0603551D 0E041604 1436E3C5 E21DAD36 C5B3CAC9 39EB6DA3 9FE3304A 38308198
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 534A504B 492E736A 706B692E 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 4D6EDD81 DC9F6F7A 9BFD64DA CF3D356F
96981088 953D446F 53702BF5 A5AA04FB CE7B2F37 24169894 A2395CF9 CFA00242
2AC51B0F EF1B5BDD 80F470E8 629F4F28
quit
!
crypto isakmp policy 1
hash md5

!--- Defines the hostname as the ISAKMP identity.
!--- SJKPI is configured to connect to the e4/1 interface of SJhub router.
!--- Since the crypto map applied on that interface checks for the FQDN,
!--- you need to make sure this router uses FQDN as the ISAKMP
!--- identity in the ID payload
!--- during the IKE negotiation with SJhub.

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 172.16.172.13
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 = SJKICA
OU = SJKPI
O = SJTAC
L = SAN JOSE
ST = CA
C = US

Subject:

CN = SJKICA
OU = SJKPI
O = SJTAC
L = SAN JOSE
ST = CA
C = US

CRL Distribution Point:

ldap:///CN=SJKICA,CN=sjvpnmspki,CN=CDP,CN=Public%20Key%20Services,
CN=Services,CN=Configuration,DC=sjpi,
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: MicrosoftPKI

RA KeyEncipher Certificate

Status: Available

Certificate Serial Number: 054E63CE000000000003

Key Usage: Encryption

Issuer:

CN = SJKICA
OU = SJKPI
O = SJTAC
L = SAN JOSE
ST = CA
C = US

Subject:

CN = SJVPNRA
OU = SJKPI
O = SJTAC
L = SAN JOSE
ST = CA
C = US

CRL Distribution Point:

ldap:///CN=SJKICA,CN=sjvpnmspki,CN=CDP,CN=Public%20Key%20Services,
CN=Services,CN=Configuration,DC=sjpi,
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: MicrosoftPKI

RA Signature Certificate

Status: Available

Certificate Serial Number: 054E60AD0000000000002

Key Usage: Signature

Issuer:

CN = SJKICA
OU = SJKPI
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=SJKICA,CN=sjvpnmspi,CN=CDP,CN=Public%20Key%20Services,
CN=Services,CN=Configuration,DC=sjpk,
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: MicrosoftPKI

Certificate
Status: Available
Certificate Serial Number: 02A67C7300000000000E
Key Usage: General Purpose
Issuer:
  CN = SJKICA
  OU = SJPKI
  O = SJTAC
  L = SAN JOSE
  ST = CA
  C = US
Subject Name Contains:
  Name: SJPKI.sjpk.com
  CRL Distribution Point:
    ldap:///CN=SJKICA,CN=sjvpnmspi,CN=CDP,CN=Public%20Key%20Services,
CN=Services,CN=Configuration,DC=sjpk,
DC=com?certificateRevocationList?base?objectclass=cRLDistributionPoint
  Validity Date:
    start date: 17:52:21 UTC Jan 15 2002
    end date: 17:52:21 UTC Jan 15 2004
  Associated Identity: MicrosoftPKI

```

Verify

This section provides information you can use to confirm your configuration is working properly.

Certain **show** commands are supported by the Output Interpreter tool, which allows you to view an analysis of **show** command output.

Note: Before issuing **debug** commands, please see Important Information on Debug Commands.

In this example, these IOS debug commands are used to verify how the feature works:

- **debug crypto isakmp** Displays debug information about IPSec connections and shows the first set of attributes that are denied due to incompatibilities on both ends.
- **debug crypto ipsec** Displays the source (SRC) and destination (Dest) IPSec tunnel endpoints.
- **debug crypto pki transactions** Displays debug messages for the trace of interaction (message type) between the certification authority (CA) and the router.
- **debug crypto pki messages** Displays debug messages for the details of the interaction (message dump) between the certification authority (CA) and the router.

This output is an IKE negotiation between SJVPN and SJhub. The working debugs were collected on SJhub.

```

00:01:45: ISAKMP (0:0): received packet from 172.16.172.52 (N
) NEW SA

```

00:01:45: ISAKMP: local port 500, remote port 500
00:01:45: ISAKMP (0:1): Input = IKE_MESG_FROM_PEER, IKE_MM_EX
CH
Old State = IKE_READY New State = IKE_R_MM1
00:01:45: ISAKMP (0:1): processing SA payload. message ID = 0
00:01:45: ISAKMP (0:1): Checking ISAKMP transform 1 against p
riority 1 policy
00:01:45: ISAKMP: encryption DES-CBC
00:01:45: ISAKMP: hash MD5
00:01:45: ISAKMP: default group 1
00:01:45: ISAKMP: auth RSA sig
00:01:45: ISAKMP: life type in seconds
00:01:45: ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0
x80
00:01:45: ISAKMP (0:1): atts are acceptable. Next payload is
3
00:01:45: ISAKMP (0:1): Input = IKE_MESG_INTERNAL, IKE_PROCES
S_MAIN_MODE
Old State = IKE_R_MM1 New State = IKE_R_MM1

00:01:45: ISAKMP (0:1): SA is doing RSA signature authenticat
ion using id type ID_FQDN
00:01:45: ISAKMP (0:1): sending packet to 172.16.172.52 (R) M
M_SA_SETUP
00:01:45: ISAKMP (0:1): Input = IKE_MESG_INTERNAL, IKE_PROCES
S_COMPLETE
Old State = IKE_R_MM1 New State = IKE_R_MM2

00:01:45: ISAKMP (0:1): received packet from 172.16.172.52 (R
) MM_SA_SETUP
00:01:45: ISAKMP (0:1): Input = IKE_MESG_FROM_PEER, IKE_MM_EX
CH
Old State = IKE_R_MM2 New State = IKE_R_MM3

00:01:45: ISAKMP (0:1): processing KE payload. message ID = 0
00:01:45: ISAKMP (0:1): processing NONCE payload. message ID
= 0
00:01:45: ISAKMP (0:1): SKEYID state generated
00:01:45: ISAKMP (0:1): processing CERT_REQ payload. message
ID = 0
00:01:45: ISAKMP (0:1): peer wants a CT_X509_SIGNATURE cert
00:01:45: ISAKMP (0:1): peer want cert issued by OU = sjvpn,
O = cisco, C = us
00:01:45: ISAKMP (0:1): processing vendor id payload
00:01:45: ISAKMP (0:1): speaking to another IOS box!
00:01:45: ISAKMP (0:1): Input = IKE_MESG_INTERNAL, IKE_PROCES
S_MAIN_MODE
Old State = IKE_R_MM3 New State = IKE_R_MM3

00:01:45: ISAKMP (0:1): sending packet to 172.16.172.52 (R) M
M_KEY_EXCH
00:01:45: ISAKMP (0:1): Input = IKE_MESG_INTERNAL, IKE_PROCES
S_COMPLETE
Old State = IKE_R_MM3 New State = IKE_R_MM4

00:01:45: ISAKMP (0:1): received packet from 172.16.172.52 (R
) MM_KEY_EXCH
00:01:45: ISAKMP (0:1): Input = IKE_MESG_FROM_PEER, IKE_MM_EX
CH
Old State = IKE_R_MM4 New State = IKE_R_MM5

00:01:45: ISAKMP (0:1): processing ID payload. message ID = 0
00:01:45: ISAKMP (0:1): processing CERT payload. message ID =
0
00:01:45: ISAKMP (0:1): processing a CT_X509_SIGNATURE cert
00:01:45: CRYPTO_PKI: status = 0: poll CRL

00:01:47: CRYPTO_PKI: ldap_bind() succeeded.
00:01:48: CRYPTO_PKI: set CRL update timer with delay: 46524
00:01:48: CRYPTO_PKI: the current router time: 13:15:25 UTC Jan 15 2002

00:01:48: CRYPTO_PKI: the last CRL update time: 01:10:49 UTC Jan 15 2002
00:01:48: CRYPTO_PKI: the next CRL update time: 02:10:49 UTC Jan 16 2002
00:01:48: CRYPTO_PKI: status = 0: failed to get public key from the storage
00:01:48: CRYPTO_PKI: status = 65535: failed to get issuer pubkey in cert
00:01:48: CRYPTO_PKI: status = 0: failed to get public key from the storage
00:01:48: CRYPTO_PKI: status = 65535: failed to get issuer pubkey in cert
00:01:48: CRYPTO_PKI: status = 0: failed to get public key from the storage
00:01:48: CRYPTO_PKI: status = 65535: failed to get issuer pubkey in cert
00:01:48: CRYPTO_PKI: status = 0: failed to get public key from the storage
00:01:48: CRYPTO_PKI: status = 65535: failed to get issuer pubkey in cert
00:01:48: CRYPTO_PKI: status = 0: failed to get public key from the storage
00:01:48: CRYPTO_PKI: status = 65535: failed to get issuer pubkey in cert
00:01:48: CRYPTO_PKI: status = 0: failed to get public key from the storage
00:01:48: CRYPTO_PKI: status = 65535: failed to get issuer pubkey in cert
00:01:49: CRYPTO_PKI: transaction GetCRL completed
00:01:49: CRYPTO_PKI: blocking callback received status: 105
00:01:49: CRYPTO_PKI: Certificate verified, chain status= 1
00:01:49: ISAKMP (0:1): processing SIG payload. message ID = 0
00:01:49: ISAKMP:received payload type 14
00:01:49: ISAKMP (0:1): processing keep alive: proposal=10/2 sec., actual=10/2 sec.
00:01:49: ISAKMP (0:1): peer knows about the keepalive extension mechanism.
00:01:49: ISAKMP (0:1): read keepalive extended attribute VPI : /0x2/0x4
00:01:49: ISAKMP (0:1): peer keepalives capabilities: 0x1
00:01:49: ISAKMP (0:1): SA has been authenticated with 172.16.172.52
00:01:49: ISAKMP (0:1): Input = IKE_MSG_INTERNAL, IKE_PROCESS_MAIN_MODE
Old State = IKE_R_MM5 New State = IKE_R_MM5

00:01:49: ISAKMP (1): ID payload
next-payload : 6
type : 2
protocol : 17
port : 500
length : 19
00:01:49: ISAKMP (1): Total payload length: 23
00:01:49: ISAKMP (0:1): sending packet to 172.16.172.52 (R) QM_IDLE
00:01:49: ISAKMP (0:1): Input = IKE_MSG_INTERNAL, IKE_PROCESS_COMPLETE
Old State = IKE_R_MM5 New State = IKE_P1_COMPLETE

00:01:53: ISAKMP (0:1): received packet from 172.16.172.52 (R

```
) QM_IDLE
00:01:53: ISAKMP (0:1): processing HASH payload. message ID =
1024386741
00:01:53: ISAKMP (0:1): processing SA payload. message ID = 1
024386741
00:01:53: ISAKMP (0:1): Checking IPsec proposal 1
00:01:53: ISAKMP: transform 1, ESP_DES
00:01:53: ISAKMP: attributes in transform:
00:01:53: ISAKMP: encaps is 1
00:01:53: ISAKMP: SA life type in seconds
00:01:53: ISAKMP: SA life duration (basic) of 3600
00:01:53: ISAKMP: SA life type in kilobytes
00:01:53: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x
50 0x0
00:01:53: ISAKMP: authenticator is HMAC-MD5
00:01:53: ISAKMP (0:1): atts are acceptable.
00:01:53: IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) dest= 172.16.172.54, 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
00:01:53: ISAKMP (0:1): processing NONCE payload. message ID
= 1024386741
00:01:53: ISAKMP (0:1): processing ID payload. message ID = 1
024386741
00:01:53: ISAKMP (1): ID_IPV4_ADDR_SUBNET src 50.1.1.0/255.25
5.255.0 prot 0 port 0
00:01:53: ISAKMP (0:1): processing ID payload. message ID = 1
024386741
00:01:53: ISAKMP (1): ID_IPV4_ADDR_SUBNET dst 20.1.1.0/255.25
5.255.0 prot 0 port 0
00:01:53: ISAKMP (0:1): asking for 1 spis from ipsec
00:01:53: ISAKMP (0:1): Node 1024386741, Input = IKE_MSG_FRO
M_PEER, IKE_QM_EXCH
Old State = IKE_QM_READY New State = IKE_QM_SPI_STARVE

00:01:53: IPSEC(key_engine): got a queue event...
00:01:53: IPSEC(spi_response): getting spi 1528686631 for SA
from 172.16.172.52 to 172.16.172.54 for prot 3
00:01:53: ISAKMP: received ke message (2/1)
00:01:53: ISAKMP (0:1): sending packet to 172.16.172.52 (R) Q
M_IDLE
00:01:53: ISAKMP (0:1): Node 1024386741, Input = IKE_MSG_FRO
M_IPSEC, IKE_SPI_REPLY
Old State = IKE_QM_SPI_STARVE New State = IKE_QM_R_QM2

00:01:53: ISAKMP (0:1): received packet from 172.16.172.52 (R) QM_
IDLE
00:01:53: ISAKMP (0:1): Creating IPsec SAs
00:01:53: inbound SA from 172.16.172.52 to 172.16.172.54
(proxy 50.1.1.0 to 20.1.1.0)
00:01:53: has spi 0x5B1DE827 and conn_id 2000 and flags 4
00:01:53: lifetime of 3600 seconds
00:01:53: lifetime of 4608000 kilobytes
00:01:53: outbound SA from 172.16.172.54 to 172.16.172.52
(proxy 20.1.1.0 to 50.1.1.0 )
00:01:53: has spi 2031705275 and conn_id 2001 and flags 4
00:01:53: lifetime of 3600 seconds
00:01:53: lifetime of 4608000 kilobytes
00:01:53: ISAKMP (0:1): deleting node 1024386741 error FALSE reason "
quick mode done (await())"
00:01:53: ISAKMP (0:1): Node 1024386741, Input = IKE_MSG_FROM_PEER,
IKE_QM_EXCH
Old State = IKE_QM_R_QM2 New State = IKE_QM_PHASE2_COMPLETE
```

```

00:01:53: IPSEC(key_engine): got a queue event...
00:01:53: IPSEC(initialize_sas): ,
(key eng. msg.) dest= 172.16.172.54, 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= 0x5B1DE827(1528686631), conn_id= 2000, keysize= 0, flags= 0x
4
00:01:53: IPSEC(initialize_sas): ,
(key eng. msg.) src= 172.16.172.54, 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= 0x79195CBB(2031705275), conn_id= 2001, keysize= 0, flags= 0x
4
00:01:53: IPSEC(create_sa): sa created,
(sa) sa_dest= 172.16.172.54, sa_prot= 50,
sa_spi= 0x5B1DE827(1528686631),
sa_trans= esp-des esp-md5-hmac , sa_conn_id= 2000
00:01:53: IPSEC(create_sa): sa created,
(sa) sa_dest= 172.16.172.52, sa_prot= 50,
sa_spi= 0x79195CBB(2031705275),
sa_trans= esp-des esp-md5-hmac , sa_conn_id= 2001
00:01:59: ISAKMP (0:1): sending packet to 172.16.172.52 (R) QM_IDLE

00:01:59: ISAKMP (0:1): purging node -1588679962
00:01:59: ISAKMP (0:1): Input = IKE_MESG_FROM_TIMER, IKE_TIMER_IM_ALI
VE
Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE

00:01:59: ISAKMP (0:1): received packet from 172.16.172.52 (R) QM_IDL
E
00:01:59: ISAKMP (0:1): processing HASH payload. message ID = 1510798
388
00:01:59: ISAKMP (0:1): processing NOTIFY ITS_ALIVE_ACK protocol 1
spi 0, message ID = 1510798388, sa = 632F165C
00:01:59: ISAKMP (0:1): peer 172.16.172.52 is alive!

```

This output is an IKE negotiation between SJPKI and SJhub. The working debugs were collected on SJhub.

```

SJhub#
00:21:36: ISAKMP (0:0): received packet from 172.16.172.10 (N) NEW SA
00:21:36: ISAKMP: local port 500, remote port 500
00:21:36: ISAKMP (0:4): Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
Old State = IKE_READY New State = IKE_R_MM1
00:21:36: ISAKMP (0:4): processing SA payload. message ID = 0
00:21:36: ISAKMP (0:4): Checking ISAKMP transform 1 against priority 1 policy
00:21:36: ISAKMP: encryption DES-CBC
00:21:36: ISAKMP: hash MD5
00:21:36: ISAKMP: default group 1
00:21:36: ISAKMP: auth RSA sig
00:21:36: ISAKMP: life type in seconds
00:21:36: ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80
00:21:36: ISAKMP (0:4): atts are acceptable. Next payload is 3
00:21:36: ISAKMP (0:4): Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
Old State = IKE_R_MM1 New State = IKE_R_MM1

00:21:36: ISAKMP (0:4): SA is doing RSA signature authentication using id type ID_FQDN
00:21:36: ISAKMP (0:4): sending packet to 172.16.172.10 (R) MM_SA_SETUP
00:21:36: ISAKMP (0:4): Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
Old State = IKE_R_MM1 New State = IKE_R_MM2

00:21:36: ISAKMP (0:4): received packet from 172.16.172.10 (R) MM_SA_SETUP

```

```
00:21:36: ISAKMP (0:4): Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH
Old State = IKE_R_MM2 New State = IKE_R_MM3

00:21:36: ISAKMP (0:4): processing KE payload. message ID = 0
00:21:36: ISAKMP (0:4): processing NONCE payload. message ID = 0
00:21:36: ISAKMP (0:4): SKEYID state generated
00:21:36: ISAKMP (0:4): processing CERT_REQ payload. message ID = 0
00:21:36: ISAKMP (0:4): peer wants a CT_X509_SIGNATURE cert
00:21:36: ISAKMP (0:4): peer want cert issued by CN = SJKICA, OU = SJKI,
O = SJTAC, L = SAN JOSE, ST = CA, C = US
00:21:36: ISAKMP (0:4): processing vendor id payload
00:21:36: ISAKMP (0:4): speaking to another IOS box!
00:21:36: ISAKMP (0:4): Input = IKE_MSG_INTERNAL, IKE_PROCESS_MAIN_MODE
Old State = IKE_R_MM3 New State = IKE_R_MM3

00:21:36: ISAKMP (0:4): sending packet to 172.16.172.10 (R) MM_KEY_EXCH
00:21:36: ISAKMP (0:4): Input = IKE_MSG_INTERNAL, IKE_PROCESS_COMPLETE
Old State = IKE_R_MM3 New State = IKE_R_MM4

00:21:36: ISAKMP (0:4): received packet from 172.16.172.10 (R) MM_KEY_EXCH
00:21:36: ISAKMP (0:4): Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH
Old State = IKE_R_MM4 New State = IKE_R_MM5

00:21:36: ISAKMP (0:4): processing ID payload. message ID = 0
00:21:36: ISAKMP (0:4): processing CERT payload. message ID = 0
00:21:36: ISAKMP (0:4): processing a CT_X509_SIGNATURE cert
00:21:36: CRYPTO_PKI: status = 0: crl check ignored
00:21:36: CRYPTO_PKI: WARNING: Certificate,
private key or CRL was not found while selecting CRL

00:21:36: CRYPTO_PKI: cert revocation status unknown.
00:21:36: ISAKMP (0:4): cert approved with warning
00:21:36: ISAKMP (0:4): processing SIG payload. message ID = 0
00:21:36: ISAKMP (4): sa->peer.name = , sa->peer_id.id.id_fqdn.fqdn =
SJKI.sjki.com
00:21:36: ISAKMP:received payload type 14
00:21:36: ISAKMP (0:4): processing keep alive: proposal=10/2 sec., actual=10/2 sec.
00:21:36: ISAKMP (0:4): peer knows about the keepalive extension mechanism.
00:21:36: ISAKMP (0:4): read keepalive extended attribute VPI: /0x2/0x4
00:21:36: ISAKMP (0:4): peer keepalives capabilities: 0x1
00:21:36: ISAKMP (0:4): SA has been authenticated with 172.16.172.10
00:21:36: ISAKMP (0:4): Input = IKE_MSG_INTERNAL, IKE_PROCESS_MAIN_MODE
Old State = IKE_R_MM5 New State = IKE_R_MM5

00:21:36: ISAKMP (4): ID payload
next-payload : 6
type : 2
protocol : 17
port : 500
length : 19
00:21:36: ISAKMP (4): Total payload length: 23
00:21:36: ISAKMP: growing send buffer from 1024 to 3072
00:21:36: ISAKMP (0:4): sending packet to 172.16.172.10 (R) QM_IDLE
00:21:36: ISAKMP (0:4): Input = IKE_MSG_INTERNAL, IKE_PROCESS_COMPLETE
Old State = IKE_R_MM5 New State = IKE_P1_COMPLETE

00:21:37: ISAKMP (0:4): received packet from 172.16.172.10 (R) QM_IDLE
00:21:37: ISAKMP (0:4): processing HASH payload. message ID = 1725643858
00:21:37: ISAKMP (0:4): processing SA payload. message ID = 1725643858
00:21:37: ISAKMP (0:4): Checking IPsec proposal 1
00:21:37: ISAKMP: transform 1, ESP_DES
00:21:37: ISAKMP: attributes in transform:
00:21:37: ISAKMP: encaps is 1
00:21:37: ISAKMP: SA life type in seconds
00:21:37: ISAKMP: SA life duration (basic) of 3600
00:21:37: ISAKMP: SA life type in kilobytes
```

```
00:21:37: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0
00:21:37: ISAKMP: authenticator is HMAC-MD5
00:21:37: ISAKMP (0:4): atts are acceptable.
00:21:37: IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) dest= 172.16.172.13, 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
00:21:37: ISAKMP (0:4): processing NONCE payload. message ID = 1725643858
00:21:37: ISAKMP (0:4): processing ID payload. message ID = 1725643858
00:21:37: ISAKMP (4): ID_IPV4_ADDR_SUBNET src 10.1.1.0/255.255.255.0 prot 0 port 0
00:21:37: ISAKMP (0:4): processing ID payload. message ID = 1725643858
00:21:37: ISAKMP (4): ID_IPV4_ADDR_SUBNET dst 20.1.1.0/255.255.255.0 prot 0 port 0
00:21:37: ISAKMP (0:4): asking for 1 spis from ipsec
00:21:37: ISAKMP (0:4): Node 1725643858, Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH
Old State = IKE_QM_READY New State = IKE_QM_SPI_STARVE

00:21:37: IPSEC(key_engine): got a queue event...
00:21:37: IPSEC(spi_response): getting spi 1791759000 for SA
from 172.16.172.10 to 172.16.172.13 for prot 3
00:21:37: ISAKMP: received ke message (2/1)
00:21:37: ISAKMP (0:4): sending packet to 172.16.172.10 (R) QM_IDLE
00:21:37: ISAKMP (0:4): Node 1725643858, Input = IKE_MESG_FROM_IPSEC, IKE_SPI_REPLY
Old State = IKE_QM_SPI_STARVE New State = IKE_QM_R_QM2

00:21:37: ISAKMP (0:4): received packet from 172.16.172.10 (R) QM_IDLE
00:21:37: ISAKMP (0:4): Creating IPsec SAs
00:21:37: inbound SA from 172.16.172.10 to 172.16.172.13
(proxy 10.1.1.0 to 20.1.1.0)
00:21:37: has spi 0x6ACC1298 and conn_id 2002 and flags 4
00:21:37: lifetime of 3600 seconds
00:21:37: lifetime of 4608000 kilobytes
00:21:37: outbound SA from 172.16.172.13 to 172.16.172.10
(proxy 20.1.1.0 to 10.1.1.0 )
00:21:37: has spi 1523784602 and conn_id 2003 and flags 4
00:21:37: lifetime of 3600 seconds
00:21:37: lifetime of 4608000 kilobytes
00:21:37: ISAKMP (0:4): deleting node 1725643858 error FALSE reason
"quick mode done (await())"
00:21:37: ISAKMP (0:4): Node 1725643858, Input = IKE_MESG_FROM_PEER,
IKE_QM_EXCH
Old State = IKE_QM_R_QM2 New State = IKE_QM_PHASE2_COMPLETE

00:21:37: IPSEC(key_engine): got a queue event...
00:21:37: IPSEC(initialize_sas): ,
(key eng. msg.) dest= 172.16.172.13, 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= 0x6ACC1298(1791759000), conn_id= 2002, keysize= 0, flags= 0x4
00:21:37: IPSEC(initialize_sas): ,
(key eng. msg.) src= 172.16.172.13, 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= 0x5AD31B9A(1523784602), conn_id= 2003, keysize= 0, flags= 0x4
00:21:37: IPSEC(create_sa): sa created,
(sa) sa_dest= 172.16.172.13, sa_prot= 50,
sa_spi= 0x6ACC1298(1791759000),
sa_trans= esp-des esp-md5-hmac , sa_conn_id= 2002
00:21:37: IPSEC(create_sa): sa created,
(sa) sa_dest= 172.16.172.10, sa_prot= 50,
```

```
sa_spi= 0x5AD31B9A(1523784602),
sa_trans= esp-des esp-md5-hmac , sa_conn_id= 2003
```

This output is an IKE negotiation failure between SJVPN and SJhub when the OU fields do not match. From the debugs collected on SJhub, IKE authentication in the phase I negotiation is still successful after certificate validation and CRL checking. However, during QM negotiation, when the settings in the crypto map are checked, QM negotiation fails. This is due to the DN mismatch between the crypto identity set on the SJhub and the ISAKMP identity sent by the SJVPN.

```
SJhub#
00:01:42: ISAKMP (0:0): received packet from 172.16.172.52 (N) NEW SA
00:01:42: ISAKMP: local port 500, remote port 500
00:01:42: ISAKMP (0:1): Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
Old State = IKE_READY New State = IKE_R_MM1
00:01:42: ISAKMP (0:1): processing SA payload. message ID = 0
00:01:42: ISAKMP (0:1): Checking ISAKMP transform 1 against priority 1 policy
00:01:42: ISAKMP: encryption DES-CBC
00:01:42: ISAKMP: hash MD5
00:01:42: ISAKMP: default group 1
00:01:42: ISAKMP: auth RSA sig
00:01:42: ISAKMP: life type in seconds
00:01:42: ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80
00:01:42: ISAKMP (0:1): atts are acceptable. Next payload is 3
00:01:42: ISAKMP (0:1): Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
Old State = IKE_R_MM1 New State = IKE_R_MM1

00:01:42: ISAKMP (0:1): SA is doing RSA signature authentication
using id type ID_FQDN
00:01:42: ISAKMP (0:1): sending packet to 172.16.172.52 (R) MM_SA_SETUP
00:01:42: ISAKMP (0:1): Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
Old State = IKE_R_MM1 New State = IKE_R_MM2

00:01:42: ISAKMP (0:1): received packet from 172.16.172.52 (R) MM_SA_SETUP
00:01:42: ISAKMP (0:1): Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
Old State = IKE_R_MM2 New State = IKE_R_MM3

00:01:42: ISAKMP (0:1): processing KE payload. message ID = 0
00:01:42: ISAKMP (0:1): processing NONCE payload. message ID = 0
00:01:42: ISAKMP (0:1): SKEYID state generated
00:01:42: ISAKMP (0:1): processing CERT_REQ payload. message ID = 0
00:01:42: ISAKMP (0:1): peer wants a CT_X509_SIGNATURE cert
00:01:42: ISAKMP (0:1): peer want cert issued by OU = sjvpn, O = cisco, C = us
00:01:42: ISAKMP (0:1): processing vendor id payload
00:01:42: ISAKMP (0:1): speaking to another IOS box!
00:01:42: ISAKMP (0:1): Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
Old State = IKE_R_MM3 New State = IKE_R_MM3

00:01:42: ISAKMP (0:1): sending packet to 172.16.172.52 (R) MM_KEY_EXCH
00:01:42: ISAKMP (0:1): Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
Old State = IKE_R_MM3 New State = IKE_R_MM4

00:01:42: ISAKMP (0:1): received packet from 172.16.172.52 (R) MM_KEY_EXCH
00:01:42: ISAKMP (0:1): Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
Old State = IKE_R_MM4 New State = IKE_R_MM5

00:01:42: ISAKMP (0:1): processing ID payload. message ID = 0
00:01:42: ISAKMP (0:1): processing CERT payload. message ID = 0
00:01:42: ISAKMP (0:1): processing a CT_X509_SIGNATURE cert
00:01:42: CRYPTO_PKI: status = 0: poll CRL
00:01:45: CRYPTO_PKI: ldap_bind() succeeded.
00:01:45: CRYPTO_PKI: set CRL update timer with delay: 44535
00:01:45: CRYPTO_PKI: the current router time: 13:48:34 UTC Jan 15 2002

00:01:45: CRYPTO_PKI: the last CRL update time: 01:10:49 UTC Jan 15 2002
00:01:45: CRYPTO_PKI: the next CRL update time: 02:10:49 UTC Jan 16 2002
```

```

00:01:45: CRYPTO_PKI: status = 0: failed to get public key from the storage
00:01:45: CRYPTO_PKI: status = 65535: failed to get issuer pubkey in cert
00:01:45: CRYPTO_PKI: status = 0: failed to get public key from the storage
00:01:45: CRYPTO_PKI: status = 65535: failed to get issuer pubkey in cert
00:01:45: CRYPTO_PKI: status = 0: failed to get public key from the storage
00:01:45: CRYPTO_PKI: status = 65535: failed to get issuer pubkey in cert
00:01:45: CRYPTO_PKI: status = 0: failed to get public key from the storage
00:01:45: CRYPTO_PKI: status = 65535: failed to get issuer pubkey in cert
00:01:45: CRYPTO_PKI: status = 0: failed to get public key from the storage
00:01:45: CRYPTO_PKI: status = 65535: failed to get issuer pubkey in cert
00:01:46: CRYPTO_PKI: transaction GetCRL completed
00:01:46: CRYPTO_PKI: blocking callback received status: 105
00:01:46: CRYPTO_PKI: Certificate verified, chain status= 1
00:01:46: ISAKMP (0:1): processing SIG payload. message ID = 0
00:01:46: ISAKMP:received payload type 14
00:01:46: ISAKMP (0:1): processing keep alive: proposal=10/2 sec., actual=10/2 sec.
00:01:46: ISAKMP (0:1): peer knows about the keepalive extension mechanism.
00:01:46: ISAKMP (0:1): read keepalive extended attribute VPI: /0x2/0x4
00:01:46: ISAKMP (0:1): peer keepalives capabilities: 0x1
00:01:46: ISAKMP (0:1): SA has been authenticated with 172.16.172.52
00:01:46: ISAKMP (0:1): Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
Old State = IKE_R_MM5 New State = IKE_R_MM5

00:01:46: ISAKMP (1): ID payload
next-payload : 6
type : 2
protocol : 17
port : 500
length : 19
00:01:46: ISAKMP (1): Total payload length: 23
00:01:46: ISAKMP (0:1): sending packet to 172.16.172.52 (R) QM_IDLE
00:01:46: ISAKMP (0:1): Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
Old State = IKE_R_MM5 New State = IKE_P1_COMPLETE

00:01:50: ISAKMP (0:1): received packet from 172.16.172.52 (R) QM_IDLE
00:01:50: ISAKMP (0:1): processing HASH payload. message ID = 804465872
00:01:50: ISAKMP (0:1): processing SA payload. message ID = 804465872
00:01:50: ISAKMP (0:1): Checking IPsec proposal 1
00:01:50: ISAKMP: transform 1, ESP_DES
00:01:50: ISAKMP: attributes in transform:
00:01:50: ISAKMP: encaps is 1
00:01:50: ISAKMP: SA life type in seconds
00:01:50: ISAKMP: SA life duration (basic) of 3600
00:01:50: ISAKMP: SA life type in kilobytes
00:01:50: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0
00:01:50: ISAKMP: authenticator is HMAC-MD5
00:01:50: %CRYPTO-4-IKE_QUICKMODE_BAD_CERT:
encrypted connection attempted with a peer without the
configured certificate attributes
00:01:50: IPSEC(validate_proposal): peer failed identity check
00:01:50: ISAKMP (0:1): atts not acceptable. Next payload is 0
00:01:50: ISAKMP (0:1): phase 2 SA not acceptable!
00:01:50: ISAKMP (0:1): sending packet to 172.16.172.52 (R) QM_IDLE
00:01:50: ISAKMP (0:1): purging node -1542959357
00:01:50: ISAKMP (0:1): Unknown Input for node 804465872:
state = IKE_QM_READY, major = 0x00000001, minor = 0x0000000C

00:01:50: %CRYPTO-6-IKMP_MODE_FAILURE: Processing of Quick mode failed
with peer at 172.16.172.52

```

This output is an IKE negotiation failure between SJKPI and SJhub when the FQDN fields do not match. As seen from the debugs collected on SJhub router, IKE authentication in the phase I negotiation is still successful after certificate validation (there was no CRL checking in this case due the "crl optional" in the

configuration). However, during QM negotiation, when the settings in the crypto map are checked, QM negotiation fails. This is due to the FQDN mismatch between the crypto identity set on the SJhub and ISAKMP identity sent by the SJPKI.

```
SJhub#
00:17:02: ISAKMP (0:0): received packet from 172.16.172.10 (N) NEW SA
00:17:02: ISAKMP: local port 500, remote port 500
00:17:02: ISAKMP (0:2): Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
Old State = IKE_READY New State = IKE_R_MM1
00:17:02: ISAKMP (0:2): processing SA payload. message ID = 0
00:17:02: ISAKMP (0:2): Checking ISAKMP transform 1 against priority 1 policy
00:17:02: ISAKMP: encryption DES-CBC
00:17:02: ISAKMP: hash MD5
00:17:02: ISAKMP: default group 1
00:17:02: ISAKMP: auth RSA sig
00:17:02: ISAKMP: life type in seconds
00:17:02: ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80
00:17:02: ISAKMP (0:2): atts are acceptable. Next payload is 3
00:17:02: ISAKMP (0:2): Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
Old State = IKE_R_MM1 New State = IKE_R_MM1

00:17:02: ISAKMP (0:2): SA is doing RSA signature authentication
using id type ID_FQDN
00:17:02: ISAKMP (0:2): sending packet to 172.16.172.10 (R) MM_SA_SETUP
00:17:02: ISAKMP (0:2): Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
Old State = IKE_R_MM1 New State = IKE_R_MM2

00:17:02: ISAKMP (0:2): received packet from 172.16.172.10 (R) MM_SA_SETUP
00:17:02: ISAKMP (0:2): Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
Old State = IKE_R_MM2 New State = IKE_R_MM3

00:17:02: ISAKMP (0:2): processing KE payload. message ID = 0
00:17:02: ISAKMP (0:2): processing NONCE payload. message ID = 0
00:17:02: ISAKMP (0:2): SKEYID state generated
00:17:02: ISAKMP (0:2): processing CERT_REQ payload. message ID = 0
00:17:02: ISAKMP (0:2): peer wants a CT_X509_SIGNATURE cert
00:17:02: ISAKMP (0:2): peer want cert issued by CN = SJPKICA,
OU = SJPKI, O = SJTAC, L = SAN JOSE, ST = CA, C = US
00:17:02: ISAKMP (0:2): processing vendor id payload
00:17:02: ISAKMP (0:2): speaking to another IOS box!
00:17:02: ISAKMP (0:2): Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
Old State = IKE_R_MM3 New State = IKE_R_MM3

00:17:02: ISAKMP (0:2): sending packet to 172.16.172.10 (R) MM_KEY_EXCH
00:17:02: ISAKMP (0:2): Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
Old State = IKE_R_MM3 New State = IKE_R_MM4

00:17:02: ISAKMP (0:2): received packet from 172.16.172.10 (R) MM_KEY_EXCH
00:17:02: ISAKMP (0:2): Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
Old State = IKE_R_MM4 New State = IKE_R_MM5
00:17:02: ISAKMP (0:2): processing ID payload. message ID = 0
00:17:02: ISAKMP (0:2): processing CERT payload. message ID = 0
00:17:02: ISAKMP (0:2): processing a CT_X509_SIGNATURE cert
00:17:02: CRYPTO_PKI: status = 0: crl check ignored
00:17:02: CRYPTO_PKI: WARNING: Certificate, private key or
CRL was not found while selecting CRL

00:17:02: CRYPTO_PKI: cert revocation status unknown.
00:17:02: ISAKMP (0:2): cert approved with warning
00:17:02: ISAKMP (0:2): processing SIG payload. message ID = 0
00:17:02: ISAKMP (2): sa->peer.name = ,
sa->peer_id.id.id_fqdn.fqdn = SJPKI.sjtest.com
00:17:02: ISAKMP:received payload type 14
00:17:02: ISAKMP (0:2): processing keep alive: proposal=10/2 sec.,
```

```

actual=10/2 sec.
00:17:02: ISAKMP (0:2): peer knows about the keepalive extension mechanism.
00:17:02: ISAKMP (0:2): read keepalive extended attribute VPI: /0x2/0x4
00:17:02: ISAKMP (0:2): peer keepalives capabilities: 0x1
00:17:02: ISAKMP (0:2): SA has been authenticated with 172.16.172.10
00:17:02: ISAKMP (0:2): Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
Old State = IKE_R_MM5 New State = IKE_R_MM5

00:17:02: ISAKMP (2): ID payload
next-payload : 6
type : 2
protocol : 17
port : 500
length : 19
00:17:02: ISAKMP (2): Total payload length: 23
00:17:02: ISAKMP: growing send buffer from 1024 to 3072
00:17:02: ISAKMP (0:2): sending packet to 172.16.172.10 (R) QM_IDLE
00:17:02: ISAKMP (0:2): Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
Old State = IKE_R_MM5 New State = IKE_PI_COMPLETE

00:17:02: ISAKMP (0:2): received packet from 172.16.172.10 (R) QM_IDLE
00:17:02: ISAKMP (0:2): processing HASH payload. message ID = 1014150051
00:17:02: ISAKMP (0:2): processing SA payload. message ID = 1014150051
00:17:02: ISAKMP (0:2): Checking IPsec proposal 1
00:17:02: ISAKMP: transform 1, ESP_DES
00:17:02: ISAKMP: attributes in transform:
00:17:02: ISAKMP: encaps is 1
00:17:02: ISAKMP: SA life type in seconds
00:17:02: ISAKMP: SA life duration (basic) of 3600
00:17:02: ISAKMP: SA life type in kilobytes
00:17:02: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0
00:17:02: ISAKMP: authenticator is HMAC-MD5
00:17:02: %CRYPTO-4-IKE_QUICKMODE_BAD_CERT:
encrypted connection attempted with a peer without the
configured certificate attributes
00:17:02: IPSEC(validate_proposal): peer failed identity check
00:17:02: ISAKMP (0:2): atts not acceptable. Next payload is 0
00:17:02: ISAKMP (0:2): phase 2 SA not acceptable!
00:17:02: ISAKMP (0:2): sending packet to 172.16.172.10 (R) QM_IDLE
00:17:02: ISAKMP (0:2): purging node 1366519308
00:17:02: ISAKMP (0:2): Unknown Input for node 1014150051:
state = IKE_QM_READY, major = 0x00000001, minor = 0x0000000C

00:17:02: %CRYPTO-6-IKMP_MODE_FAILURE: Processing of Quick mode
failed with peer at 172.16.172.10

```

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

DN-based crypto map matches the remote VPN peer's ISAKMP identity with the DN or FQDN names defined under crypto identity configuration. Make sure that your remote VPN devices have the right fields selected as the ISAKMP identity. On the Cisco IOS router, the **crypto isakmp identity** `<address/hostname/dn>` command can be used to choose certain fields for ISAKMP identity.

These debugs from SJhub show an example where the crypto map is set to check the DN, while the VPN peer uses the hostname as an ISAKMP identity:

```

00:28:36: ISAKMP (0:1): processing ID payload. message ID = 0
00:28:36: ISAKMP (0:1): processing CERT payload. message ID = 0
00:28:36: ISAKMP (0:1): processing a CT_X509_SIGNATURE cert
00:28:36: CRYPTO_PKI: Certificate verified, chain status= 1
00:28:36: ISAKMP (0:1): processing SIG payload. message ID = 0

```

```
00:28:36: ISAKMP (1): sa->peer.name = , sa->peer_id.id.id_fqdn.fqdn =
SJVPN.sjvpn.com
00:28:36: ISAKMP:received payload type 14
00:28:36: ISAKMP (0:1): processing keep alive: proposal=10/2 sec., actual=10/2 sec.
00:28:36: ISAKMP (0:1): peer knows about the keepalive extension mechanism.
00:28:36: ISAKMP (0:1): read keepalive extended attribute VPI: /0x2/0x4
00:28:36: ISAKMP (0:1): peer keepalives capabilities: 0x1
00:28:36: ISAKMP (0:1): SA has been authenticated with 172.16.172.52
00:28:36: ISAKMP (0:1): Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
Old State = IKE_R_MM5 New State = IKE_R_MM5

00:28:36: ISAKMP (1): ID payload
next-payload : 6
type : 2
protocol : 17
port : 500
length : 19
00:28:36: ISAKMP (1): Total payload length: 23
00:28:36: ISAKMP (0:1): sending packet to 172.16.172.52 (R) QM_IDLE
00:28:36: ISAKMP (0:1): Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
Old State = IKE_R_MM5 New State = IKE_P1_COMPLETE

00:28:36: ISAKMP (0:1): received packet from 172.16.172.52 (R) QM_IDLE
00:28:36: ISAKMP (0:1): processing HASH payload. message ID = 1940367247
00:28:36: ISAKMP (0:1): processing SA payload. message ID = 1940367247
00:28:36: ISAKMP (0:1): Checking IPsec proposal 1
00:28:36: ISAKMP: transform 1, ESP_DES
00:28:36: ISAKMP: attributes in transform:
00:28:36: ISAKMP: encaps is 1
00:28:36: ISAKMP: SA life type in seconds
00:28:36: ISAKMP: SA life duration (basic) of 3600
00:28:36: ISAKMP: SA life type in kilobytes
00:28:36: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0
00:28:36: ISAKMP: authenticator is HMAC-MD5
00:28:36: %CRYPTO-4-IKE_QUICKMODE_BAD_CERT: encrypted
connection attempted with a peer without the
configured certificate attributes
```

Related Information

- [Configuring Multiple-Identity Certificate Authorities on Cisco IOS® Routers](#)
- [IPsec Product Support Pages](#)
- [Technical Support – Cisco Systems](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Jan 19, 2006

Document ID: 18303
