Configuring DN-Based Crypto Maps for VPN Device Access Control

Document ID: 18303

Contents

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.
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.

![Network Diagram](image)

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 SJKPI 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.

<table>
<thead>
<tr>
<th>SJhub (7200) Router configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>SJhub#write terminal</td>
</tr>
<tr>
<td>Building configuration...</td>
</tr>
<tr>
<td>Current configuration : 19802 bytes</td>
</tr>
</tbody>
</table>
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 DD06092A 864886F7 0D010105
  0500302D 310B3009 06035504 06130275 73310E30 0C060355 040A1305 63697363
  6F310E30 0C060355 040B1305 766A7670 6E301E17 DD030310 36313393 32303234
  305A170D 32313036 31393232 33323430 5A302D31 DB300906 03550406 13027573
  310E300C 06035504 QA130536 6973636F 310E300C 06035504 0B130573 6A76706E
  30819F30 0D06092A 864886F7 0D010101 05000381 BD003081 89028181 0E8C25B
  EDF4A6EE A352B142 C1657BF4 FBDA45E 4F2F7733 BD2B8879 96138C63 1DB713BF
  753BF845 2D7E600F AAF4D75B 9E959513 BB13FF13 36696F48 86C46F42 CF854A66
  4FBE81F8 025F216B A44D4BB2 39ADD1A5 1BCCF812 09A19BDC 468EEAE1 B6C2A378

69C81348 1A9CD61C 551216F2 BB168FBB 94CBEF37 E1D9A8F7 80BBC17F D1020301
0001A382 010F3082 010B3011 06096086 480186F8 42010104 04030200 07304F06
03551D1F 04483046 304A0A42 A04A043E 303C310B 03090603 55040613 02757331
0E300C06 355040A 13056369 73636F31 0E300C06 0355040B 1305736A 76706E31
0D300B06 35504053 13044352 4C31302B 0603551D 10042430 22800F32 30303130
36313932 32303234 305A810F 32303231 30363139 32323332 34035A03 0B603555
1D0F0404 03202106 301F0603 551D2304 18301680 1446C160 9CDBEA53 EE80A480
601A9658 3BBDF80D 2F301D06 03551D0E 04160414 46C1609C DBE5AE3EE 80A480E6
1A96585B 0DF8D2DF 300C0603 551D1304 05300301 01FF301D 06029A86 4886F67D
07410004 10300E1B 0856352E 30A342E 30032020 90300D06 092A8648 86FD07D1
01050500 03811800 7E3DBAC4 8CA7D5A B19C0625 8780D222 F965A1A2 C0C2B584
CBC5A203 F550FAC4 9656699A 52D8CB46 40776237 87163118 8F3C04F7 D2CAABA3
6AB34F99 AB71269E 7B9A0C10 DA098EC5 AE44BB46 701254CF 3BEC64C1 5DB2EE5
5EC0140B B0CC83497 D79F1B48 80018F51 3A4B6174 59R085AA 9CE3B939 629406AA
7CE9CC0D 01593E6B
quit
certificate ra-encrypt 3B2FD318
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
!
crypto identity FromSJVPN
  dn OU=sjvpn
  dn O=cisco
!
crypto identity FromSJPKI
  fqdn SJPKI.sjpki.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 mrout-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: 132BD14C0000000000B
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: 091B47AE8C8E2A94D3E8B38F292F5A6
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:
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 3B2FD307308202E4 3082024D A0030201 0202043B 2FD30730 0D06092A 864886F7 0D010105 0500030D 310B3009 06035504 06130275 73310E30 0D060535 040A1305 63697366 6F310E30 0C060355 040B1305 736A7670 6E301E17 0D030310 36313932 32303234 305A170D 32313036 31393232 33323430 5A302D31 0B300906 03550406 12037537 301E300C 06035504 0A130563 69736666 310E300C 06035504 0B130573 6A76706E 30819F30 0D06092A 864886F7 0D010101 0500030D 0D060308 80920181 0082C25B EDF4A6EE A352B142 C16578F4 FBDAF45E 4F2F7733 8D2B8879 9613BC63 1DB713BF 753BF845 2D7E600F 8A44D765 9E989513 B13FF13 36696F48 86C464F2 CF85A466 4F8E83F8 025F216B A44D4BB2 39ADD1A5 1BCCF812 09A19BDC 468EEAE1 B6C3A378 69C81348 1A9CD61C 551216F2 8B168FBB 94CBEB37 E1D9A8F7 80BBC17F D1020301 0001A382 0B1F03B8 010B3011 06096086 480186F8 42D1D104 04030200 07304F06 03551D1F 04483046 3044A404 A040A43E 303C310B 30090603 55040613 02757331 0E300C06 0355040A 13056369 73666631 0E300C06 0355040B 1305736A 76706E31 0D300B06 03550403 13044352 4C31302B 0603551D 10042430 22800F32 03030130 36313932 32032324 305A810F 32303231 30363139 32323332 34305A30 0B060355 1D0F0404 03020106 301F0603 551D2304 13016080 1446C160 9CD8EA53 EE80A480 601A9658 3B2D8F8D 3F302D06 03551D0E 04160414 46C1609C DBEA53EE 80A48060 1A96583B 0DF802DF 300C0603 551D2304 05030001 0FF301D 06092A86 488F67D7 07410004 10300E1B 0856352E 303A342E 30030204 90300D06 02A9684F 8670D0D1 01050500 03818100 7E3DBAC4 8CAE7D5A B19C0625 8780D222 F965A1A2 C0C25B84
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
!
no snmp-server community public RO
!
call rsvp-sync
!
mgcp profile default
!
dial-peer cor custom
!
!
!
tagkeeper
  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 tcp-small-servers
service udp-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 091B47AE8E8C2E9A4D3E8B38F292F5AF
3082032C 308202D6 A0030201 02020109 1B47AE8E CFE2A94D 3EBB38F2 92F5AF30
0D06092A 864886F7 0D010105 0500305F 310B3009 06035504 06130255 53310B30
09060355 04081302 34310311 303F0603 55040713 0835414E 204A4F53 45310E30
0C060355 040A1305 544A5441 43310E30 0C060355 040B1305 534A504B 49311030
0E060355 04031307 544A504B 49434130 16170030 32303311 31033135 3133395A
170D3037 30313131 30323030 30345A30 5F310B30 09060355 04061302 5553310B
30090603 55040813 02430111 11300F06 03550407 13085341 42042A4F 5345310E
300C0603 55040A13 05534A54 4143310E 300C0603 55040B13 05534A50 4B493110
300E0603 55040313 07534A50 4B494341 3053C300D 06092A86 488F670D 01010105
00034B00 30480241 00AEC268 0C6388F1 404A2E97 3C94742D 37070BEC 368069BF
C98A7A63 EB1131A5 DDC3E41F B9D9EB66 AF504D65 2B2D864C 87260696 8AFAF871
88AB0301 150F11D 63020301 0001A382 016C3082 01683013 06092A86 488F670D 01010105
37140204 061E0400 43004130 0B060355 1D0F0404 03020146 300F0603 551D1301
01FF0405 30030101 FF301D06 01135510E 04160414 2315574F 05405281 E113C7E8
6D83CBF2 33B71CB1 30820100 0603551D 1F0481F8 3081F530 81B8A0B1 5B49A1B2
8681AF6C 6461703A 2F2F2F24 43ED354A 504B4943 412C434E 3D7336A7 7066ED73
7066692C 443E2D43 44502C43 43ED5075 626C6963 2532304B 65792532 30536572
76696365 732C434E 3D536572 76696365 732C434E 3D436FE6 66966775 72617469
6F6E2C44 433D736A 706B692C 44433D63 6F6D3F63 65727469 66966761 75655265
7666F631 74696F6E 4C697374 3F626173 653F6F62 6A656374 636C6173 733D6352
4C446973 74726962 7574696F 6E506F69 6E743038 A036A034 86326874 74073A2F
2F736A76 7066ED73 706B692E 736A7076 692E636F 6D2F4365 7247456E 726F66C6
2F534A50 4B494341 2663726C 30100609 2B060104 01823715 01040302 0100300D
60092A86 488F670D 01010505 00340100 735977DF 7822B944 96A50106 722108F0
1A60E6F8 EFED9A9ED 2C7C9174 5EF48909 B4A66A08 226FBD11 3F20BA61 C556182A
8E914788 AE6C5363 A769805F 9E2F6458
quit
certificate ra-encrypt 054E63CE000000000000
3082048E 30820438 A0030201 02020A05 4E63CE00 00000000 03300D06 092A8648
86F70D01 01050500 5F3510B 30090603 55040613 02555331 0B300906 03550408
13024341 31131300F 06035504 07130853 414E204A 4F533531 0E300C06 0355040A
1305534A 54414331 0E300C06 0355040B 1305534A 504B4931 10300E06 0355040A
1307534A 504B4943 413011E7 0D033230 31313130 31353932 385A170D 3D343031
31313130 35393238 5A305F31 0B300906 03550406 13025553 310B3009 06035504
08130243 41311110 0F060355 04071308 53414E20 4A4F5345 310E300C 06035504
DA031553 4A544143 310E300C 06035504 0B130553 4A504B49 3110300E 06035504
03110753 4A56504E 52413081 9F300D06 092A8648 86F70D01 01010500 3818BD00
30818902 818100C6 E17A9C97 9CD883ED CCE68AAD DA4AF518 1D1B0056 EAE19CF7
controller ISA 2/1
!

quit

! crypto isakmp policy 1
hash md5

!--- Defines the hostname as the ISAKMP identity.
!--- SJPKI 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
!
!
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: 091B47AEE8CFE2A94D3E88B38F292F5AF
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: MicrosoftPKI

RA KeyEncipher Certificate
Status: Available
Certificate Serial Number: 054E63CE0000000000003
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: MicrosoftPKI

RA Signature Certificate
Status: Available
Certificate Serial Number: 054E60AD0000000000002
Key Usage: Signature
Issuer:
  CN = SJPKICA
  OU = SJPKI
  O = SJTAC
  L = SAN JOSE
  ST = CA
  C = US
Subject:
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

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 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 public key 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 public key 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 public key 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 public key 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 public key 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_MESG_INTERNAL, IKE_PROCESS_S_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_MESG_INTERNAL, IKE_PROCESS_S_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 0x50 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 50.1.1.0/255.255.255.0 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 20.1.1.0/255.255.255.0 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_MESG_FROM_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) QM_IDLE
00:01:53: ISAKMP (0:1): Node 1024386741, Input = IKE_MESG_FROM_PEER, 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_MESG_FROM_PEER, IKE_QM_EXCH
Old State = IKE_QM_R_QM2 New State = IKE_QM_PHASE2_COMPLETE
This output is an IKE negotiation between SJPKI and SJhub. The working debugs were collected on SJhub.
00:21:36: ISAKMP (0:4): Input = IKE_MESG_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 = SJPKICA, OU = SJPKI, 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_MESG_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_MESG_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_MESG_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 = SJPKI.sjpki.com
00:21:36: ISAKMP: received payload type 14
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_MESG_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_MESG_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): 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= 172.16.172.10, sa_prot= 50,
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.
This output is an IKE negotiation failure between SJPKI 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 to 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): 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: ISAKMP (0:2): CERT payload accepted
00:17:02: ISAKMP: 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 (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_P1_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
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
© 2014 - 2015 Cisco Systems, Inc. All rights reserved. Terms & Conditions | Privacy Statement | Cookie Policy | Trademarks of Cisco Systems, Inc.

Updated: Jan 19, 2006   Document ID: 18303