

# Ejemplo de Configuración de DMVPN Hub como Servidor CA para la Red DMVPN

## Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuración de hub + CA](#)

[Configuración de Spoke1](#)

[Verificación](#)

[Hub](#)

[Spoke](#)

[Troubleshoot](#)

[Problemas relacionados con IPSec](#)

[Problemas relacionados con PKI](#)

[Servidor CA](#)

[Radios DMVPN](#)

[Información Relacionada](#)

## Introducción

Este documento describe cómo configurar una red de VPN multipunto dinámica (DMVPN) con autenticación de certificados cuando el hub DMVPN se configura como autoridad certificadora (CA).

## Prerequisites

## Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Public Key Infrastructure (PKI)
- DMVPN con el uso de claves previamente compartidas
- Network Time Protocol (NTP)

## Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

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.

## Antecedentes

Una práctica bastante común y la forma recomendada de implementar una red DMVPN basada en PKI es configurar la DMVPN con certificados y un servidor CA explícito. Este documento describe cómo configurar una infraestructura PKI con un servidor Cisco IOS® CA:

### [Guía de Configuración de Public Key Infrastructure](#)

Complete estos pasos para trasladar esta infraestructura a una implementación de DMVPN:

1. Haga que los concentradores y los radios se registren y se autenticuen con el servidor de la CA como cualquier otro router, como se muestra en este ejemplo.

```
crypto pki trustpoint dmvpn
enrollment url http://192.168.1.1:80
revocation-check none
rsa-keypair dmvpn
```

2. Agregue este comando para cambiar la política de autenticación del método de autenticación para utilizar PKI en lugar de una clave previamente compartida.

```
crypto isakmp policy <number>
authentication rsa-sig
```

**Nota:** El método de autenticación no se muestra aquí porque PKI es el valor predeterminado. Ingrese el comando **show run all** en el router para ver la configuración.

```
crypto isakmp policy 2
encr aes 192
group 2
```

Sin embargo, ¿qué ocurre cuando el hub DMVPN (o cualquier otro router que forme parte de la infraestructura DMVPN) también es necesario para actuar como la CA? Para que la PKI funcione correctamente, ambos extremos del túnel necesitan tener un certificado firmado por la misma CA. Sin embargo, si uno de los routers DMVPN es en sí la CA, ¿cómo podemos conseguir que ese router en particular sea un miembro activo de la infraestructura PKI?

Complete estos pasos para registrar el router para sí mismo:

1. Configure el router como una CA.

```
crypto pki server dmvpn-ca
issuer-name CN=rtpvpnoutbound7.cisco.com
grant auto
lifetime certificate 25
lifetime ca-certificate 30
auto-rollover
database url nvram
```

2. Configure un punto de confianza en la CA con una URL de inscripción que apunte a la propia CA.

```
crypto pki trustpoint dmvpn
enrollment url http://192.168.1.1:80
revocation-check none
rsa-keypair dmvpn
!
```

```
interface GigabitEthernet0/1 // <-- interface on the same router.
description utfwbOrder01
ip address 192.168.1.1 255.255.255.252
duplex full
speed 1000
!
```

Inscriba y autentique la CA con los procedimientos estándar.

```
crypto pki authenticate <trustpoint>
crypto pki enroll <trustpoint>
```

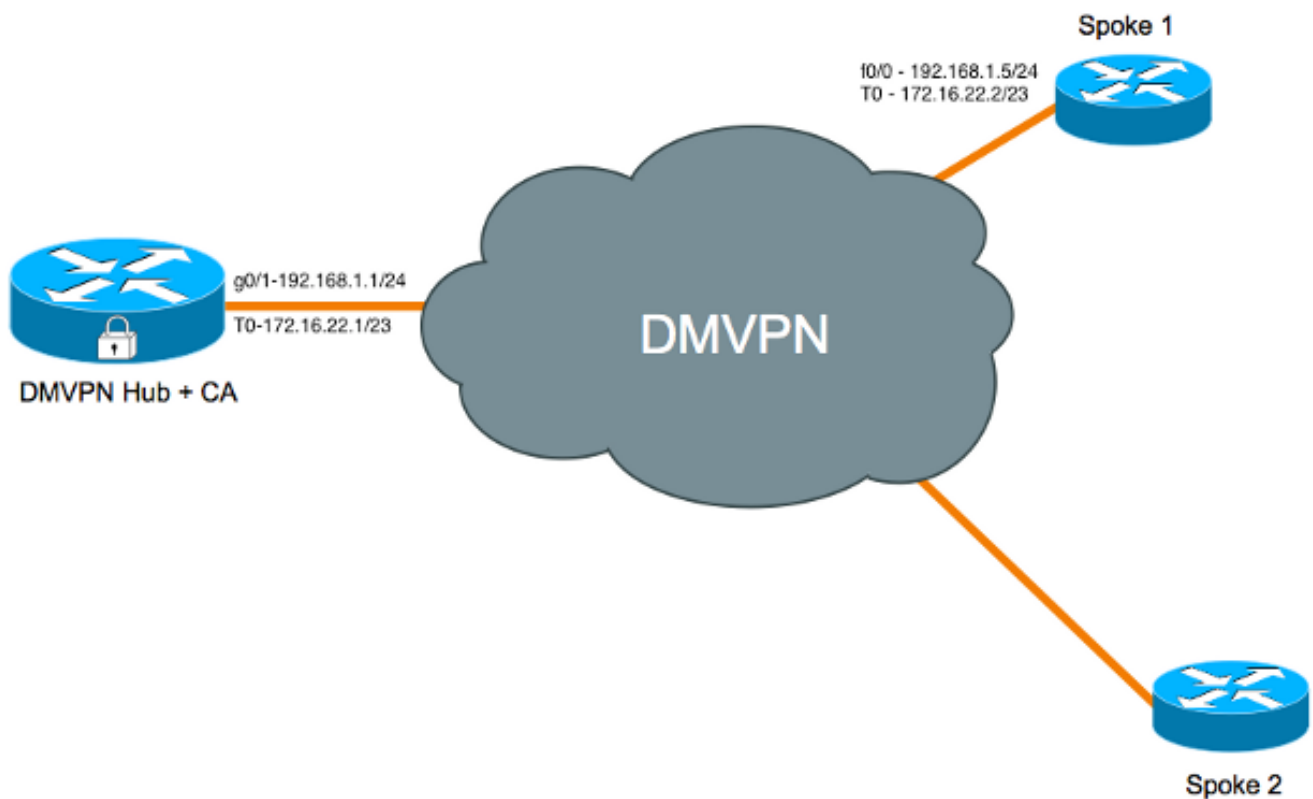
3. Configure los otros routers que forman parte de la infraestructura DMVPN para inscribirse y autenticarse en la CA.
4. Configure la política de protocolo de administración de claves (ISAKMP) y asociación de seguridad de Internet para utilizar PKI para la autenticación como se ha descrito anteriormente.

**Sugerencia:** Cisco recomienda utilizar NTP para mantener sincronizados los relojes en los routers DMVPN. Para obtener información sobre cómo configurar NTP, vea [Configuración de NTP](#).

## Configurar

**Nota:** Use la [Command Lookup Tool \(clientes registrados solamente\)](#) para obtener más información sobre los comandos usados en esta sección.

### Diagrama de la red



### Configuración de hub + CA

```
hostname Hub-CA
!
aaa new-model
!
!
aaa authentication attempts login 2
aaa authentication login default group tacacs+ enable
aaa authorization exec default group tacacs+ none
aaa accounting send stop-record authentication failure
!
aaa session-id common
clock timezone MST -7
clock summer-time MDT recurring
!
!
ip cef
!
ip domain name cisco.com
!
!
crypto pki server dmvpn-ca
issuer-name CN=Hub-CA.cisco.com
grant auto
lifetime certificate 25
lifetime ca-certificate 30
auto-rollover
database url nvram
!
! // trustpoint created for the CA server:
crypto pki trustpoint dmvpn-ca
revocation-check crl
rsa-keypair dmvpn-ca
!
! // trustpoint created for the hub to enroll with the CA which is itself
crypto pki trustpoint tp-dmvpn
enrollment url http://192.168.1.1:80
revocation-check none
rsa-keypair dmvpn
!
!
crypto pki certificate chain dmvpn-ca
certificate ca rollover 02
30820231 3082019A A0030201 02020102 300D0609 2A864886 F70D0101 04050030
2C312A30 28060355 04031321 72742D69 746F6362 72616E63 6876706E 2E63732E
7A696F6E 7362616E 6B2E636F 6D301E17 0D313430 34323931 35343932 385A170D
31343035 32393135 34393238 5A302C31 2A302806 03550403 13217274 2D69746F
63627261 6E636876 706E2E63 732E7A69 6F6E7362 616E6B2E 636F6D30 819F300D
06092A86 4886F70D 01010105 0003818D 00308189 02818100 B495D3A6 98C00CE4
DFE6661D 52104A06 50B893DB 2E1C95C1 2CFE8B36 370FA94D 82E3A217 6E0396A8
ED42D1C5 9F07AF7D 5692EE37 34F14319 F969E133 3F9F52A0 A14C47A0 426F9871
0D9DBFF8 E5372291 7374CC78 BB1433C4 3FE9B4A8 2D35B0A4 A0893308 BC9BC8CE
F5A00192 E88F9158 C8CFFCFA D3FB6F51 089E6069 D56B3B05 02030100 01A36330
61300F06 03551D13 0101FF04 05300301 01FF300E 0603551D 0F0101FF 04040302
0186301F 0603551D 23041830 168014EC 7FE1CBA4 FE94D7E8 906834C1 17FB4FDF
9B5B9530 1D060355 1D0E0416 0414EC7F E1CBA4FE 94D7E890 6834C117 FB4FDF9B
5B95300D 06092A86 4886F70D 01010405 00038181 000C7B6D 52B4615B EB79778F
19B3AA31 912E4151 B3D3F4E9 52D829A4 5FC4E14A 60AC5CC0 15148642 2A14B555
C46EDCE1 B14787D6 71A0C699 D630E12F 9C6A193D 1C3CE55C 9C5676ED F5DBBE4F
C975BC12 66C0371A 5E10821F 1CAD5428 EC73E2AC DFDE0C1A 18ADF552 6CFBF3BC
4BE7453B EB933A65 DFDA5ACB 449C7776 ED23D88D AB
quit
certificate ca 01
```

```
30820231 3082019A A0030201 02020101 300D0609 2A864886 F70D0101 04050030
2C312A30 28060355 04031321 72742D69 746F6362 72616E63 6876706E 2E63732E
7A696F6E 7362616E 6B2E636F 6D301E17 0D313430 33333031 35343932 385A170D
31343034 32393135 34393238 5A302C31 2A302806 03550403 13217274 2D69746F
63627261 6E636876 706E2E63 732E7A69 6F6E7362 616E6B2E 636F6D30 819F300D
06092A86 4886F70D 01010105 0003818D 00308189 02818100 B4925D9E 6E210AB3
700C3FC4 68B793DF 87CB7204 738A4442 3C040BD6 ACE7E031 176A255D AC196071
0BCDA0D4 05F229B0 F60A8E54 05CFD2CC F33DB23C 9E0FAA8C CDAF254E 181475A3
5C9C7C5E BE33673B 948DBB11 8EA72427 B4BCC2AA 3F4DEA42 294F8F17 4EDF7393
5E0C2950 4BA4CBB7 41118CDE 458CABEB EAF1A5F2 E9584813 02030100 01A36330
61300F06 03551D13 0101FF04 05300301 01FF300E 0603551D 0F0101FF 04040302
0186301F 0603551D 23041830 16801460 6F4399AE 5C350060 C2A99B11 9CCF2B6D
45239D30 1D060355 1D0E0416 0414606F 4399AE5C 350060C2 A99B119C CF2B6D45
239D300D 06092A86 4886F70D 01010405 00038181 000C546E A83E7A37 218C1148
C446FB66 6AFB1108 11B5B10F 182A33C0 F4F5F5C1 00A03BEA 67BCC87E 2C568EEA
A66B3D02 D41A9345 A69A9EBC 3E9BDEC1 3190EA72 721CD708 F2B45D1F 6B60F57D
BFC91B36 CFD7ABEE 4D9C6E86 7BAFBE37 11778E4D 58510B19 227E2E35 CB8D7CD9
022CD880 CEA1642B 789AAFBB 6D03251D 10549E3E 00
```

quit

crypto pki certificate chain tp-dmvpn

certificate 04

```
308201DF 30820148 A0030201 02020104 300D0609 2A864886 F70D0101 04050030
2C312A30 28060355 04031321 72742D69 746F6362 72616E63 6876706E 2E63732E
7A696F6E 7362616E 6B2E636F 6D301E17 0D313430 33333031 36323431 375A170D
31343034 32343136 32343137 5A303231 30302E06 092A8648 86F70D01 09021621
72742D69 746F6362 72616E63 6876706E 2E63732E 7A696F6E 7362616E 6B2E636F
6D305C30 0D06092A 864886F7 0D010101 0500034B 00304802 4100D06D 77D7511B
100FA533 43C82CED AE545AA1 15A6C247 306CFEC8 971497F9 1392B04B ECE4D8EB
5696BBB4 30A22F02 2D8C903D 414735D9 3C3A3472 22663D90 52F50203 010001A3
4F304D30 0B060355 1D0F0404 030205A0 301F0603 551D2304 18301680 14606F43
99AE5C35 0060C2A9 9B119CCF 2B6D4523 9D301D06 03551D0E 04160414 FCD1DF31
4BCFF453 046E764A 4FEB4531 A0498D5B 300D0609 2A864886 F70D0101 04050003
8181008C B386FA0E E2B1889F 7F96FF2C 3B0EF7A3 D64C3A3E 72E5E83A 6FB346A5
9E54DBC8 21EA0543 A68AB093 1E89F6B2 4D7F175D CE7FEA18 DDE23A55 A8AD5F15
594DC247 C5594E9E 9AD0B370 F0736907 1BE4EE4D 735DC116 CCEB238B ADFD5836
BD7B8E53 32E2B5B9 595DB0D6 D4EFCED1 98A74837 3CB2CB82 EFE5A6C3 52D081D5 840701
```

quit

certificate ca 01

```
30820231 3082019A A0030201 02020101 300D0609 2A864886 F70D0101 04050030
2C312A30 28060355 04031321 72742D69 746F6362 72616E63 6876706E 2E63732E
7A696F6E 7362616E 6B2E636F 6D301E17 0D313430 33333031 35343932 385A170D
31343034 32393135 34393238 5A302C31 2A302806 03550403 13217274 2D69746F
63627261 6E636876 706E2E63 732E7A69 6F6E7362 616E6B2E 636F6D30 819F300D
06092A86 4886F70D 01010105 0003818D 00308189 02818100 B4925D9E 6E210AB3
700C3FC4 68B793DF 87CB7204 738A4442 3C040BD6 ACE7E031 176A255D AC196071
0BCDA0D4 05F229B0 F60A8E54 05CFD2CC F33DB23C 9E0FAA8C CDAF254E 181475A3
5C9C7C5E BE33673B 948DBB11 8EA72427 B4BCC2AA 3F4DEA42 294F8F17 4EDF7393
5E0C2950 4BA4CBB7 41118CDE 458CABEB EAF1A5F2 E9584813 02030100 01A36330
61300F06 03551D13 0101FF04 05300301 01FF300E 0603551D 0F0101FF 04040302
0186301F 0603551D 23041830 16801460 6F4399AE 5C350060 C2A99B11 9CCF2B6D
45239D30 1D060355 1D0E0416 0414606F 4399AE5C 350060C2 A99B119C CF2B6D45
239D300D 06092A86 4886F70D 01010405 00038181 000C546E A83E7A37 218C1148
C446FB66 6AFB1108 11B5B10F 182A33C0 F4F5F5C1 00A03BEA 67BCC87E 2C568EEA
A66B3D02 D41A9345 A69A9EBC 3E9BDEC1 3190EA72 721CD708 F2B45D1F 6B60F57D
BFC91B36 CFD7ABEE 4D9C6E86 7BAFBE37 11778E4D 58510B19 227E2E35 CB8D7CD9
022CD880 CEA1642B 789AAFBB 6D03251D 10549E3E 00
```

quit

!

crypto isakmp policy 1

encr aes 192

group 2

!

!

crypto ipsec transform-set TRANSFORM\_SET esp-aes 192 esp-sha-hmac

```

mode transport
!
crypto ipsec profile DMVPN
set transform-set TRANSFORM_SET
!
!
interface Loopback0
ip address 172.16.20.63 255.255.255.255
no ip redirects
no ip unreachables
no ip proxy-arp
!
interface Tunnel0
bandwidth 100
ip address 172.16.22.1 255.255.254.0
no ip redirects
ip mtu 1400
ip flow ingress
ip nhrp authentication Cisco123
ip nhrp map multicast dynamic
ip nhrp network-id 99
ip tcp adjust-mss 1360
tunnel source GigabitEthernet0/1
tunnel mode gre multipoint
tunnel protection ipsec profile DMVPN
!
interface GigabitEthernet0/0
ip address 172.16.4.2
duplex full
speed 1000
!
interface GigabitEthernet0/1
ip address 192.168.1.1 255.255.255.0
no ip redirects
no ip unreachables
no ip proxy-arp
duplex full
speed 1000
!
router eigrp 1
passive-interface default
no passive-interface loopback0
no passive-interface Tunnel0
no auto-summary
!
ip route 0.0.0.0 0.0.0.0 192.168.1.2
! // required for the CA server to work
ip http server
!
!
ntp source GigabitEthernet0/1
ntp server 192.168.1.2
end

```

## Configuración de Spoke1

```

hostname Spoke1
!
ip source-route
!
!
ip cef

```

```
!  
!  
crypto pki trustpoint tp-dmvpn  
enrollment url http://192.168.1.1:80  
revocation-check none  
rsakeypair dmpvn-cert  
!  
!  
crypto pki certificate chain tp-dmvpn  
certificate 03  
308201E0 30820149 A0030201 02020103 300D0609 2A864886 F70D0101 04050030  
2C312A30 28060355 04031321 72742D69 746F6362 72616E63 6876706E 2E63732E  
7A696F6E 7362616E 6B2E636F 6D301E17 0D313430 33333031 35353834 385A170D  
31343034 32343135 35383438 5A303331 31302F06 092A8648 86F70D01 09021622  
4C41422D 72742D77 6573746A 6F726461 6E2E6373 2E7A696F 6E736261 6E6B2E63  
6F6D305C 300D0609 2A864886 F70D0101 01050003 4B003048 02410090 FD8FFD9F  
A6E78171 6563EAC6 61090A22 E51A87BC 7963E868 D47CA080 2637A4B8 9836DD1F  
F6C8DC5A EAB19653 EE1558AE 78D87BE5 11FC75B7 A9E3D2B2 48D15F02 03010001  
A34F304D 300B0603 551D0F04 04030205 A0301F06 03551D23 04183016 8014606F  
4399AE5C 350060C2 A99B119C CF2B6D45 239D301D 0603551D 0E041604 1474332C  
5904AA36 A85B4C6B A64C194E F6C8FC8B 9B300D06 092A8648 86F70D01 01040500  
03818100 7F5598C4 A568D54A 6993B692 DAF748F4 ADA65DF7 F11102AC D9C42D5B  
2A10BFB6 D1E952B8 2F7A6FFE 2646AAFE 6DB1BA60 192BC6BD C3070C97 EDB5C13A  
FD4984F4 52D808AB 851B3929 2208DC2A FE48D8E3 56AC4A38 8283BFC9 CBDB9F71  
A0106102 76DECEC2 35DCF37C A1B1CFE8 238808D7 21CA47F0 F2AB33BB B6884895 67412153  
quit  
certificate ca 01  
30820231 3082019A A0030201 02020101 300D0609 2A864886 F70D0101 04050030  
2C312A30 28060355 04031321 72742D69 746F6362 72616E63 6876706E 2E63732E  
7A696F6E 7362616E 6B2E636F 6D301E17 0D313430 33333031 35343932 385A170D  
31343034 32393135 34393238 5A302C31 2A302806 03550403 13217274 2D69746F  
63627261 6E636876 706E2E63 732E7A69 6F6E7362 616E6B2E 636F6D30 819F300D  
06092A86 4886F70D 01010105 0003818D 00308189 02818100 B4925D9E 6E210AB3  
700C3FC4 68B793DF 87CB7204 738A4442 3C040BD6 ACE7E031 176A255D AC196071  
0BCDA0D4 05F229B0 F60A8E54 05CFD2CC F33DB23C 9E0FAA8C CDAF254E 181475A3  
5C9C7C5E BE33673B 948DBB11 8EA72427 B4BBC2AA 3F4DEA42 294F8F17 4EDF7393  
5E0C2950 4BA4CBB7 41118CDE 458CABEB EAF1A5F2 E9584813 02030100 01A36330  
61300F06 03551D13 0101FF04 05300301 01FF300E 0603551D 0F0101FF 04040302  
0186301F 0603551D 23041830 16801460 6F4399AE 5C350060 C2A99B11 9CCF2B6D  
45239D30 1D060355 1D0E0416 0414606F 4399AE5C 350060C2 A99B119C CF2B6D45  
239D300D 06092A86 4886F70D 01010405 00038181 000C546E A83E7A37 218C1148  
C446FB66 6AFB1108 11B5B10F 182A33C0 F4F5F5C1 00A03BEA 67BCC87E 2C568EEA  
A66B3D02 D41A9345 A69A9EBC 3E9BDEC1 3190EA72 721CD708 F2B45D1F 6B60F57D  
BFC91B36 CFD7ABEE 4D9C6E86 7BAFBE37 11778E4D 58510B19 227E2E35 CB8D7CD9  
022CD880 CEA1642B 789AAFBB 6D03251D 10549E3E 00  
quit  
!  
!  
crypto isakmp policy 2  
encr aes 192  
group 2  
!  
crypto ipsec transform-set TRANSFORM_SET esp-aes 192 esp-sha-hmac  
mode transport  
!  
crypto ipsec profile DMVPN  
set transform-set TRANSFORM_SET  
!  
!  
interface Loopback0  
ip address 10.233.251.128 255.255.255.255  
!  
interface Tunnel0  
bandwidth 100
```

```

ip address 172.16.22.2 255.255.254.0
ip mtu 1400
ip nhrp authentication Cisco123
ip nhrp map 172.16.22.1 192.168.1.1
ip nhrp map multicast 192.168.1.1
ip nhrp network-id 99
ip nhrp nhs 172.16.22.1
ip tcp adjust-mss 1360
tunnel source FastEthernet0/0
tunnel destination 192.168.1.1
tunnel protection ipsec profile DMVPN
!
interface FastEthernet0/0
ip address 191.168.1.5 255.255.255.0
duplex full
speed 100
!
!
router eigrp 1
passive-interface default
no passive-interface FastEthernet0/0
no passive-interface Tunnel0
network 10.0.0.0
network 172.16.22.2 0.0.0.0
no auto-summary
!
ip route 0.0.0.0 0.0.0.0 192.168.1.2
!

```

## Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

El Analizador de Cisco CLI ([solo clientes registrados](#)) [admite determinados comandos show](#). Utilice el Analizador de Cisco CLI para ver un análisis de los resultados del comando show.

## Hub

```

Hub-CA#
Hub-CA#shpw crypto pki cert
Certificate
Status: Available
Certificate Serial Number (hex): 04
Certificate Usage: General Purpose
Issuer:
cn=Hub-CA.cisco.com
Subject:
Name: Hub-CA.cisco.com
hostname=Hub-CA.cisco.com
Validity Date:
start date: 10:24:17 MDT Mar 30 2014
end date: 10:24:17 MDT Apr 24 2014
Associated Trustpoints: tp-dmvpn

CA Certificate (Rollover)
Status: Available
Certificate Serial Number (hex): 02
Certificate Usage: Signature
Issuer:
cn=Hub-CA.cisco.com

```



Subject:  
Name: Hub-CA.cisco.com  
cn=Hub-CA.cisco.com  
Validity Date:  
start date: 09:49:28 MDT Apr 29 2014  
end date: 09:49:28 MDT May 29 2014  
Associated Trustpoints: dmvpn-ca

CA Certificate  
Status: Available  
Certificate Serial Number (hex): 01  
Certificate Usage: Signature  
Issuer:  
cn=Hub-CA.cisco.com  
Subject:  
cn=Hub-CA.cisco.com  
Validity Date:  
start date: 09:49:28 MDT Mar 30 2014  
end date: 09:49:28 MDT Apr 29 2014  
Associated Trustpoints: tp-dmvpn dmvpn-ca

**Hub-CA#show crypto isakmp sa detail**

Codes: C - IKE configuration mode, D - Dead Peer Detection  
K - Keepalives, N - NAT-traversal  
T - cTCP encapsulation, X - IKE Extended Authentication  
psk - Preshared key, rsig - RSA signature  
renc - RSA encryption  
IPv4 Crypto ISAKMP SA

C-id Local Remote I-VRF Status Encr Hash Auth DH Lifetime Cap.

1640 192.168.1.1 192.168.1.5 BRANCHVP ACTIVE aes sha rsig 2 23:55:26 N  
Engine-id:Conn-id = SW:640

IPv6 Crypto ISAKMP SA

**Hub-CA#show crypto ipsec sa**

interface: Tunnel0  
Crypto map tag: Tunnel0-head-0, local addr 192.168.1.1

protected vrf: BRANCHVPN  
local ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/47/0)  
remote ident (addr/mask/prot/port): (192.168.1.5/255.255.255.255/47/0)  
current\_peer 192.168.1.5 port 11431  
PERMIT, flags={origin\_is\_acl,}  
#pkts encaps: 75, #pkts encrypt: 75, #pkts digest: 75  
#pkts decaps: 72, #pkts decrypt: 72, #pkts verify: 72  
#pkts compressed: 0, #pkts decompressed: 0  
#pkts not compressed: 0, #pkts compr. failed: 0  
#pkts not decompressed: 0, #pkts decompress failed: 0  
#send errors 0, #recv errors 0

local crypto endpt.: 192.168.1.1, remote crypto endpt.: 192.168.1.5  
path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/1  
current outbound spi: 0x124040FF(306200831)  
PFS (Y/N): N, DH group: none

inbound esp sas:  
spi: 0x330534EB(855979243)  
transform: esp-192-aes esp-sha-hmac ,  
in use settings = {Transport UDP-Encaps, }  
conn id: 2065, flow\_id: Onboard VPN:65, sibling\_flags 80000006, crypto map: Tunnel0-head-0  
sa timing: remaining key lifetime (k/sec): (4466981/3324)

IV size: 16 bytes

replay detection support: Y

Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:

spi: 0x124040FF(306200831)

transform: esp-192-aes esp-sha-hmac ,

in use settings ={Transport UDP-Encaps, }

conn id: 2066, flow\_id: Onboard VPN:66, sibling\_flags 80000006, crypto map: Tunnel0-head-0

sa timing: remaining key lifetime (k/sec): (4466992/3324)

IV size: 16 bytes

replay detection support: Y

Status: ACTIVE

outbound ah sas:

outbound pcp sas:

## Spoke

Spoke1# **show crypto isakmp sa detail**

Codes: C - IKE configuration mode, D - Dead Peer Detection

K - Keepalives, N - NAT-traversal

T - cTCP encapsulation, X - IKE Extended Authentication

psk - Preshared key, rsig - RSA signature

renc - RSA encryption

IPv4 Crypto ISAKMP SA

C-id Local Remote I-VRF Status Encr Hash Auth DH Lifetime Cap.

5227 192.168.1.5 192.168.1.1 ACTIVE aes sha rsig 2 23:57:33 N

Engine-id:Conn-id = SW:1227

IPv6 Crypto ISAKMP SA

Spoke1#**show crypto ipsec sa**

interface: Tunnel0

Crypto map tag: Tunnel0-head-0, local addr 192.168.1.5

protected vrf: (none)

local ident (addr/mask/prot/port): (192.168.1.5/255.255.255.255/47/0)

remote ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/47/0)

current\_peer 192.168.1.1 port 4500

PERMIT, flags={origin\_is\_acl,}

#pkts encaps: 44, #pkts encrypt: 44, #pkts digest: 44

#pkts decaps: 47, #pkts decrypt: 47, #pkts verify: 47

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 0, #recv errors 0

local crypto endpt.: 192.168.1.5, remote crypto endpt.: 192.168.1.1

path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/2/1

current outbound spi: 0x330534EB(855979243)

PFS (Y/N): N, DH group: none

inbound esp sas:

spi: 0x124040FF(306200831)

```
transform: esp-192-aes esp-sha-hmac ,
in use settings ={Transport UDP-Encaps, }
conn id: 2239, flow_id: NETGX:239, sibling_flags 80000006, crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4520665/3449)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE
```

inbound ah sas:

inbound pcp sas:

```
outbound esp sas:
spi: 0x330534EB(855979243)
transform: esp-192-aes esp-sha-hmac ,
in use settings ={Transport UDP-Encaps, }
conn id: 2240, flow_id: NETGX:240, sibling_flags 80000006, crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4520674/3449)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE
```

outbound ah sas:

outbound pcp sas

## Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

El Analizador de Cisco CLI (solo clientes registrados) admite determinados comandos show. Utilice el Analizador de Cisco CLI para ver un análisis de los resultados del comando show.

**Nota:** Consulte Información Importante sobre Comandos de Debug antes de usar un comando debug.

## Problemas relacionados con IPSec

Estos debugs deben estar habilitados en ambos extremos afectados del túnel.

**debug dmvpn all** - Este comando en particular habilita este conjunto de debugs:

```
Spoke1#debug dmvpn all all
DMVPN all level debugging is on
Spoke1#show debug
```

```
NHRP:
NHRP protocol debugging is on
NHRP activity debugging is on
NHRP extension processing debugging is on
NHRP cache operations debugging is on
NHRP routing debugging is on
NHRP rate limiting debugging is on
NHRP errors debugging is on
IKEV2:
```

```
IKEV2 error debugging is on
IKEV2 terse debugging is on
IKEV2 event debugging is on
IKEV2 packet debugging is on
IKEV2 detail debugging is on
```

#### Cryptographic Subsystem:

```
Crypto ISAKMP debugging is on
Crypto ISAKMP Error debugging is on
Crypto IPSEC debugging is on
Crypto IPSEC Error debugging is on
Crypto secure socket events debugging is on
```

#### Tunnel Protection Debugs:

```
Generic Tunnel Protection debugging is on
```

#### DMVPN:

```
DMVPN error debugging is on
DMVPN UP/DOWN event debugging is on
DMVPN detail debugging is on
DMVPN packet debugging is on
DMVPN all level debugging is on
```

Estas depuraciones detalladas no siempre son necesarias y no deben habilitarse arbitrariamente ya que podrían sobrecargar el dispositivo. Normalmente, es mejor crear un subconjunto de depuraciones más relevantes a partir de este superconjunto y habilitarlas.

## Problemas relacionados con PKI

### Servidor CA

Estos comandos están relacionados con el servidor PKI. Debe ingresar un comando terminal monitor si se conecta con Telnet o Secure Shell (SSH).

Comando	Descripción
debug crypto pki messages	Muestra los detalles de la interacción (vaciado de mensajes) entre la CA y el router
debug crypto pki server	Muestra la depuración de un servidor de certificados PKI criptográfico
debug crypto pki Transactions	Muestra la interacción (tipo de mensaje) entre la CA y el router

### Radios DMVPN

Estos comandos son para cabecera o bifurcación. Para ver el resultado de la depuración, ingrese un comando terminal monitor si se utilizó Telnet/SSH para conectarse al router.

Comando	Descripción
debug crypto pki messages	Muestra los detalles de la interacción (vaciado de mensajes) entre la CA y el router
debug crypto pki server	Mostrar depuración para un servidor de certificados PKI criptográfico
debug crypto pki Transactions	Muestra la interacción (tipo de mensaje) entre la CA y el router
debug crypto isakmp	Muestra mensajes sobre eventos ISAKMP e IKE
debug crypto ipsec	Muestra eventos IPsec
debug crypto engine	Muestra mensajes de depuración sobre los motores criptográficos, que realizan cifrado y el descifrado

## Información Relacionada

- [Configuración e inscripción de un router Cisco IOS en otro router Cisco IOS configurado como servidor CA](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)