作為CA伺服器的DMVPN網路配置示例

目錄

簡介

本檔案介紹將DMVPN中心設定為憑證授權單位(CA)時，如何使用憑證驗證來設定動態多點VPN(DMVPN)網路。

必要條件

需求

思科建議您瞭解以下主題：

- 公開金鑰基礎架構 (PKI)
- 使用預共用金鑰的DMVPN
- 網路時間協定(NTP)

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

背景資訊

部署基於PKI的DMVPN網路的一種相當常見的做法和推薦的方法是使用證書和顯式CA伺服器配置DMVPN。本文檔介紹如何使用Cisco IOS® CA伺服器設定PKI基礎設施：

Public Key Infrastructure組態設定指南

完成以下步驟，以便將此基礎設施連線到DMVPN部署：

1. 讓中心和分支像任何其他路由器一樣向CA伺服器註冊和驗證其自身，如本例所示。

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

2. 新增此命令可將身份驗證方法身份驗證策略更改為使用PKI而不是預共用金鑰。

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

附註：此處未顯示驗證方法，因為PKI是預設設定。在路由器上輸入**show run all**命令以檢視配置。

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

但是，當還需要DMVPN中心（或作為DMVPN基礎設施一部分的任何其它路由器）充當CA時，會發生什麼情況？為了使PKI成功工作，隧道的兩端都需要具有由同一CA簽名的證書。但是，如果其中一個DMVPN路由器本身是CA，那麼如何使該特定路由器成為PKI基礎設施的活動成員？

完成以下步驟，以便向自身註冊路由器：

1. 將路由器配置為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. 使用指向CA本身的註冊URL在CA上配置信任點。

```
crypto pki trustpoint dmvpn
enrollment url http://192.168.1.1:80
revocation-check none
rsakeypair dmvpn
!
interface GigabitEthernet0/1 // <-- inerface on the same router.
description utfwb0rder01
ip address 192.168.1.1 255.255.255.252
duplex full
speed 1000
!
```

使用標準步驟註冊並向自身驗證CA。

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

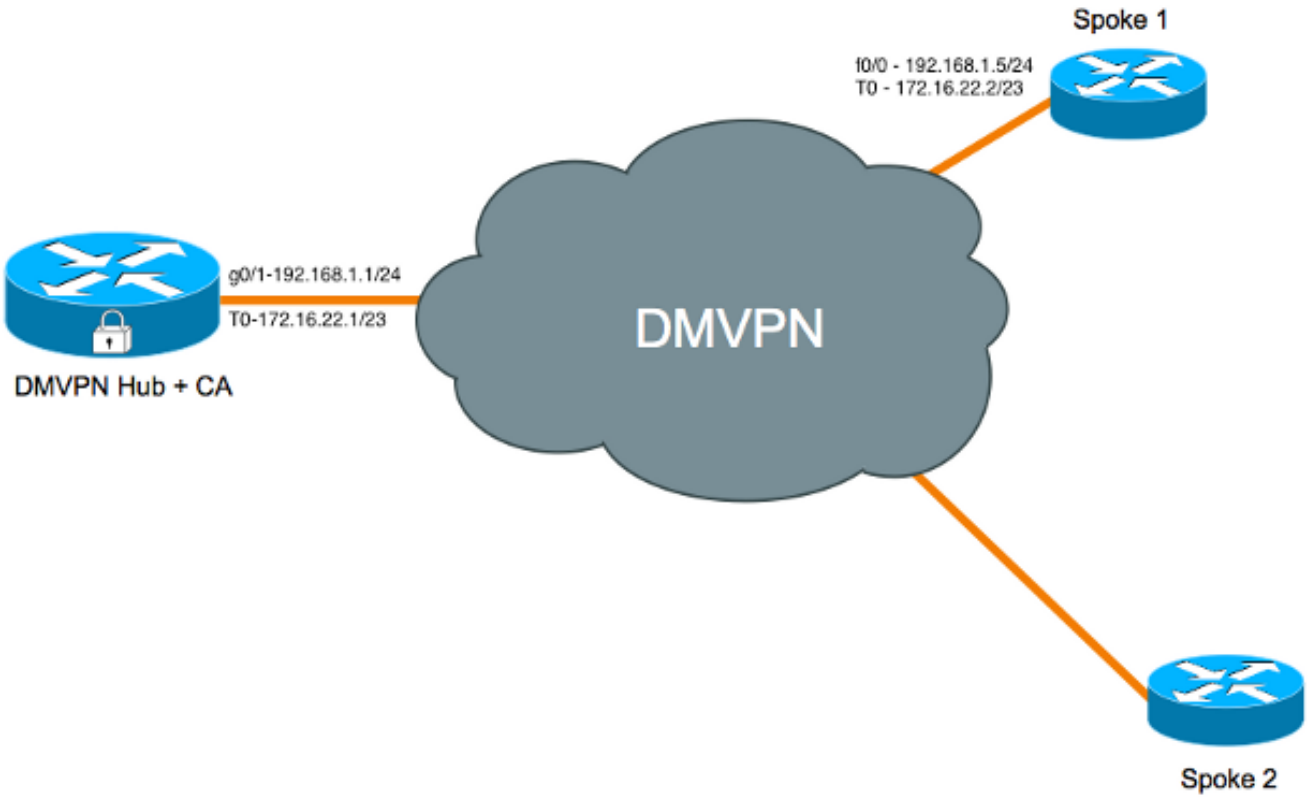
3. 將作為DMVPN基礎設施一部分的其它路由器配置為向CA註冊和身份驗證。
4. 如前所述，配置網際網路安全關聯和金鑰管理協定(ISAKMP)策略以使用PKI進行身份驗證。

提示:思科建議您使用NTP來保持DMVPN路由器上的時鐘同步。有關如何配置NTP的資訊，請參閱配置NTP。

設定

附註：使用命令查詢工具(僅供已註冊客戶使用)可獲取本節中使用的命令的更多資訊。

網路圖表



集線器+ CA配置

```
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
rsakeypair 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
rsakeypair 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 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 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 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 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
```

Spoke1配置

```
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
!
```

驗證

使用本節內容，確認您的組態是否正常運作。

Cisco CLI Analyzer（僅供已註冊客戶使用）支援某些 show 指令。使用 Cisco CLI Analyzer 檢視 show 指令輸出的分析。

中心

```
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:

輻條

```
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
```

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

Cisco CLI Analyzer（僅供已註冊客戶使用）支援某些 **show 指令。**使用 Cisco CLI Analyzer 檢視 show 指令輸出的分析。

> **附註**：使用 **debug 指令之前，請先參閱**有關 Debug 指令的重要資訊。

IPSec相關問題

應在隧道的兩個受影響端點上啟用這些調試。

debug dmvpn all - 此特定命令啟用此組調試：

```
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
```

此類詳細調試並非總是必需的，不應該隨意啟用，因為它可能會使裝置過載。通常最好從這個超級集合中建立一個更相關的調試子集並啟用它們。

PKI相關問題

CA伺服器

這些命令與PKI伺服器相關。如果使用Telnet或安全殼層(SSH)進行連線，則需要輸入terminal monitor命令。

指令	說明
debug crypto pki messages	顯示CA和路由器之間互動（消息轉儲）的詳細資訊
debug crypto pki server	顯示加密PKI證書伺服器的調試
debug crypto pki transactions	顯示CA和路由器之間的互動（消息型別）

DMVPN輻條

這些命令適用於頭端或分支。若要檢視偵錯輸出，請輸入terminal monitor命令（如果使用Telnet/SSH連線到路由器）。

指令	說明
debug crypto pki messages	顯示CA和路由器之間互動（消息轉儲）的詳細資訊
debug crypto pki server	顯示加密PKI證書伺服器的調試
debug crypto pki transactions	顯示CA和路由器之間的互動（消息型別）
debug crypto isakmp	顯示有關ISAKMP和IKE事件的消息
debug crypto ipsec	顯示IPSec事件
debug crypto engine	顯示有關執行加密和解密的加密引擎的調試消息

相關資訊

- 配置一台Cisco IOS路由器並將其註冊到另一台配置為CA伺服器的Cisco IOS路由器
- 技術支援與文件 - Cisco Systems