對常見DMVPN問題進行故障排除

目錄

簡介

本文描述動態多點VPN (DMVPN)問題最常見的解決方案。

必要條件

需求

Cisco建議您瞭解Cisco IOS®路由器上的DMVPN配置。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco IOS

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。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

背景資訊

本文描述動態多點VPN (DMVPN)問題最常見的解決方案。其中許多解決方案可以在DMVPN連線的任何深入故障排除之前實施。本文檔提供了一份常用步驟清單，在您開始排除連線故障並致電思科技術支援之前，請務必先嘗試這些步驟。

有關詳細資訊，請參閱動態多點VPN配置指南Cisco IOS版本15M&T。

請參閱瞭解和使用調試命令對IPsec進行故障排除，瞭解用於對IPsec問題進行故障排除的常見調試命令。

DMVPN配置不起作用

問題

最近配置或修改的DMVPN解決方案不起作用。

當前的DMVPN配置不再有效。

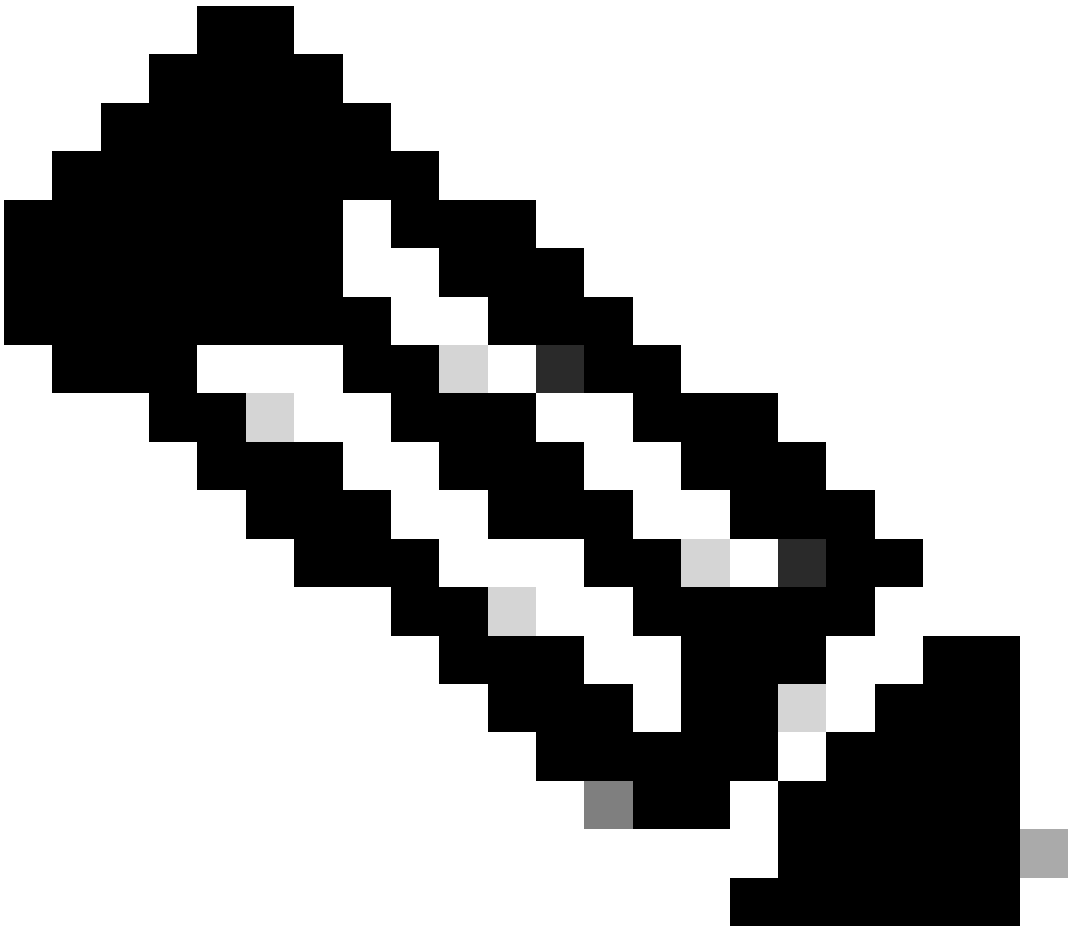
解決方案

本節包含最常見DMVPN問題的解決方案。

這些解決方案（無特定順序）可用作專案核對表，以便在進行深入故障排除之前進行驗證或嘗試：

- 常見問題

- 驗證網際網路安全性關聯和金鑰管理通訊協定(ISAKMP)封包是否已在網際網路服務提供者(ISP)遭到封鎖。
- 驗證移除通道保護時，通用路由封裝(GRE)是否有效。
- 下一跳解析協定(NHRP)註冊失敗。
- 驗證是否已正確配置生命週期。
- 驗證是否只在一個方向傳輸流量。
- 驗證已建立路由協定鄰居。



附註：開始之前，請檢查下列步驟：

---

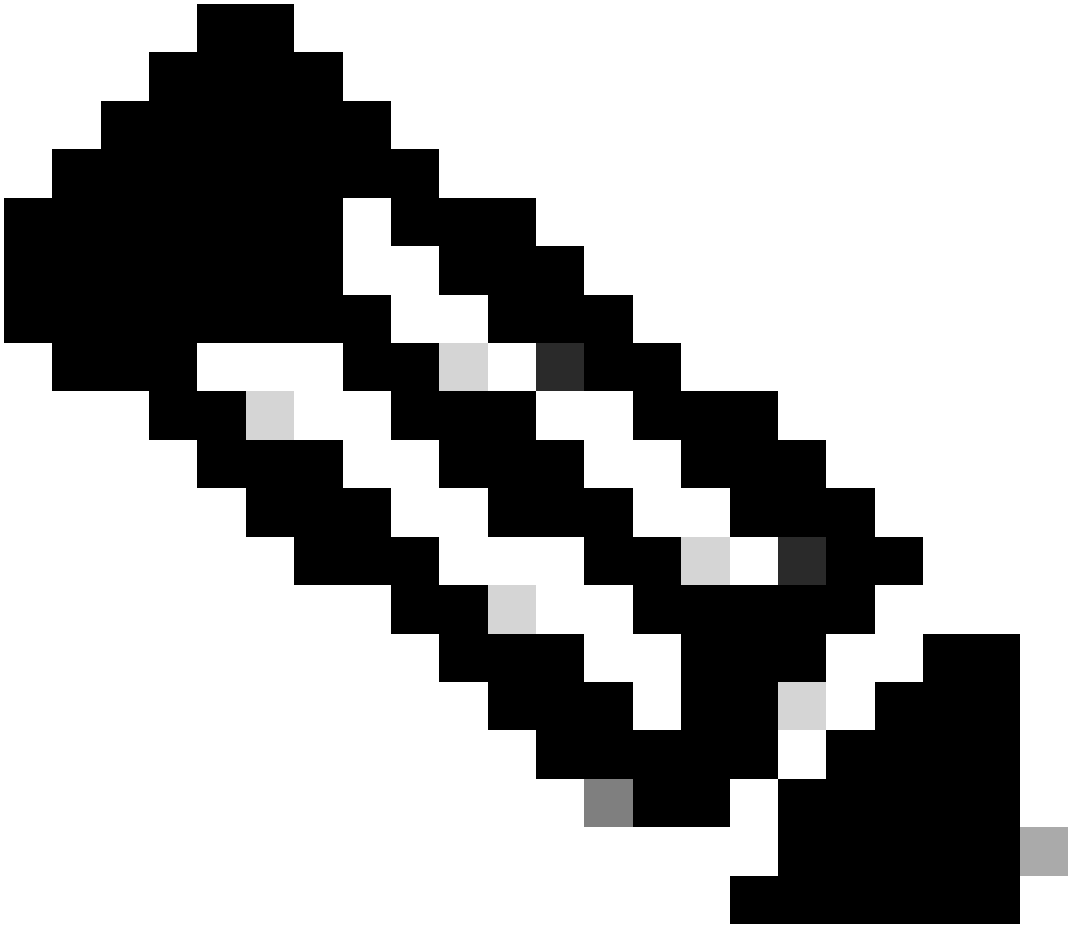
1. 同步中心和分支之間的時間戳
2. 啟用msec調試和記錄時間戳：

```
Router(config)#service timestamps debug datetime msec

Router(config)#service timestamps log datetime msec
```

3. 啟用調試會話的終端exec提示符時間戳：

```
Router#terminal exec提示符時間戳
```



注意：透過這種方式，您可以輕鬆地將調試輸出與show命令輸出關聯。

常見問題

檢驗基本連通性

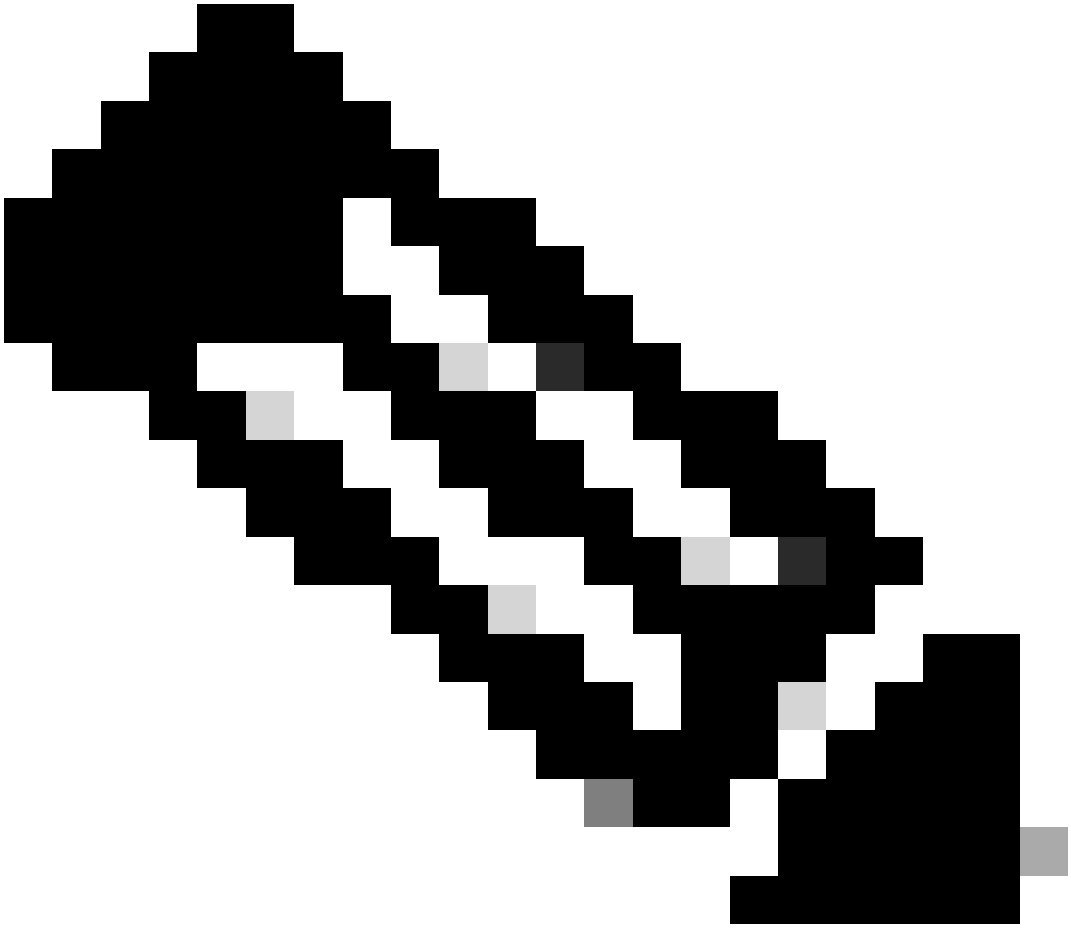
1. 從集線器ping具有NBMA地址的分支點，然後反向。

   這些ping必須直接從物理介面發出，而不是透過DMVPN隧道。但願沒有防火牆阻止ping資料包。如果此方法不起作用，請檢查路由以及中心路由器和分支路由器之間的任何防火牆。

2. 此外，請使用traceroute檢查已加密隧道資料包採用的路徑。

3. 使用debug和show命令驗證無連線的狀態：

   - debug ip icmp
   - debug ip packet



注意：debug ip packet命令會生成大量輸出，並消耗大量的系統資源。在生產網路中必須謹慎使用此命令。請始終使用access-list命令。 有關如何透過debug ip packet使用access-list命令，請參閱使用IP訪問清單進行故障排除。

驗證ISAKMP策略是否不相容

如果配置的ISAKMP策略與遠端對等體提議的策略不匹配，路由器將嘗試預設策略65535。如果兩者都不匹配，則會導致ISAKMP協商失敗。

show crypto isakmp sa命令顯示ISAKMP SA處於MM_NO_STATE中，這表示主模式失敗。

驗證預共用金鑰是否不正確

如果雙方的預共用金鑰不相同，協商將失敗。

路由器會返回「合理性檢查失敗」的消息。

驗證IPsec轉換集是否不相容

如果IPSec轉換集在兩個IPSec裝置上不相容或不匹配，則IPSec協商失敗。

路由器會針對IPSec提議返回「atts不被接受的消息。

驗證是否在ISP上阻止了ISAKMP資料包

<#root>

```
Router#
```

show crypto isakmp sa

```
IPv4 Crypto ISAKMP SA
Dst                src                state        conn-id      slot       status
172.17.0.1      172.16.1.1        MM_NO_STATE         0              0       ACTIVE
172.17.0.1      172.16.1.1        MM_NO_STATE         0              0       ACTIVE (deleted)
172.17.0.5        172.16.1.1        MM_NO_STATE      0             0       ACTIVE
172.17.0.5        172.16.1.1        MM_NO_STATE      0             0       ACTIVE (deleted)
```

上一個示例顯示了VPN隧道抖動。

此外，檢查debug crypto isakmp 來驗證輻射點路由器是否傳送了udp 500資料包：

<#root>

```
Router#
```

debug crypto isakmp

<#root>

```
04:14:44.450: ISAKMP:(0):Old State = IKE_READY
                        New State = IKE_I_MM1
```

04:14:44.450: ISAKMP:(0): beginning Main Mode exchange

```
04:14:44.450: ISAKMP:(0): sending packet to 172.17.0.1
              my_port 500 peer_port 500 (I) MM_NO_STATE
04:14:44.450: ISAKMP:(0):Sending an IKE IPv4 Packet.
```

04:14:54.450: ISAKMP:(0): retransmitting phase 1 MM_NO_STATE..

```
.
04:14:54.450: ISAKMP (0:0): incrementing error counter on sa,
              attempt 1 of 5: retransmit phase 1
04:14:54.450: ISAKMP:(0): retransmitting phase 1 MM_NO_STATE
04:14:54.450: ISAKMP:(0): sending packet to 172.17.0.1
              my_port 500 peer_port 500 (I) MM_NO_STATE
04:14:54.450: ISAKMP:(0):Sending an IKE IPv4 Packet.
```

04:15:04.450: ISAKMP:(0): retransmitting phase 1 MM_NO_STATE..

```
.
04:15:04.450: ISAKMP:(0): retransmitting phase 1 MM_NO_STATE...
04:15:04.450: ISAKMP (0:0): incrementing error counter on sa,
              attempt 2 of 5: retransmit phase 1
04:15:04.450: ISAKMP:(0): retransmitting phase 1 MM_NO_STATE
```

前面的debug 輸出顯示輻射點路由器每隔10秒傳送一次udp 500資料包。

檢查ISP，檢視輻射點路由器是否直接連線到ISP路由器，以確保它們允許udp 500流量。

在ISP允許udp 500之後，在出口介面中增加入站ACL，該介面是隧道源以允許udp 500確保udp 500流量進入路由器。使用show access-

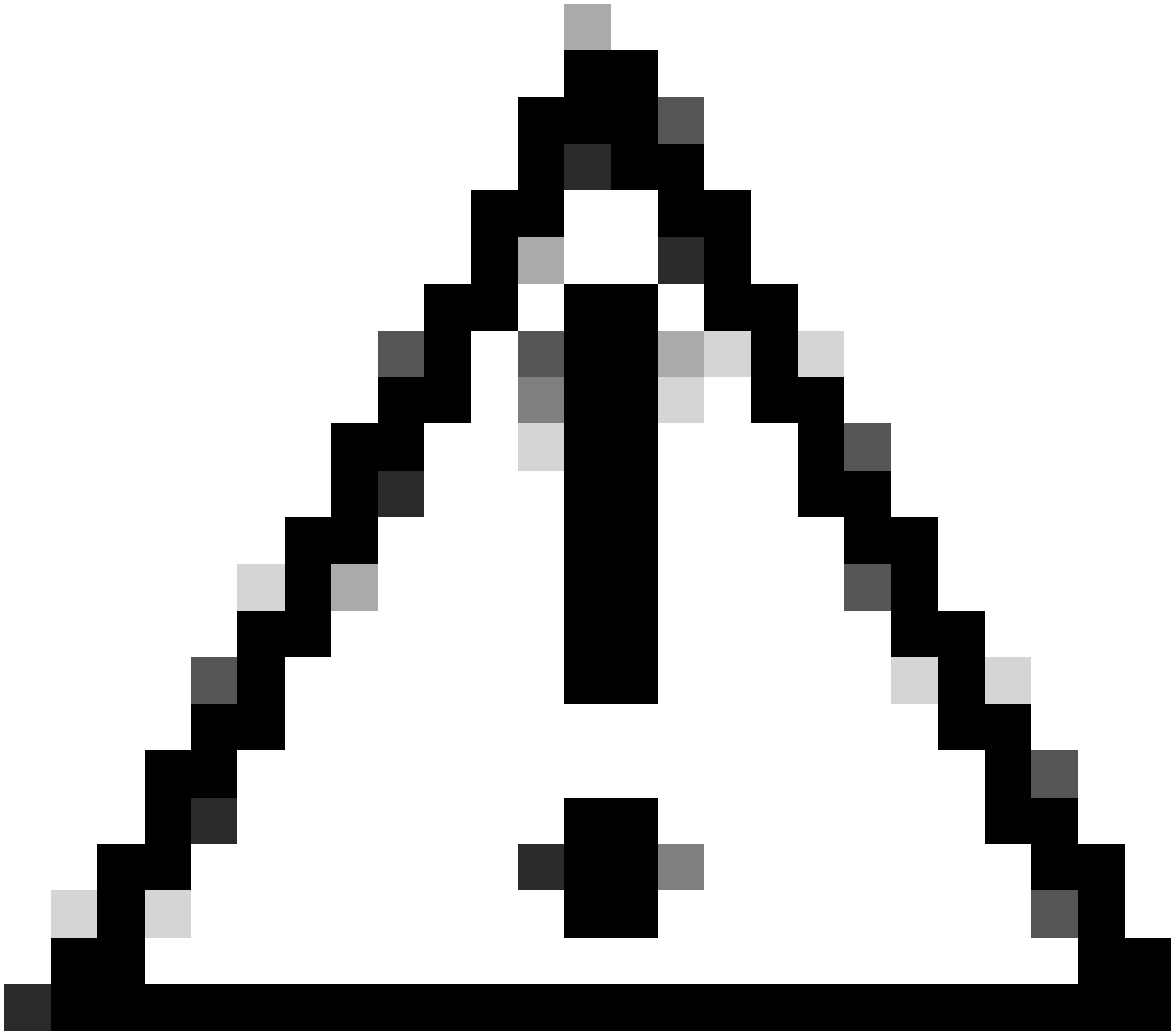
list命令驗證命中計數是否在遞增。

```
    <#root>

Router#


show access-lists 101


Extended IP access list 101
    10 permit udp host 172.17.0.1 host 172.16.1.1 eq isakmp log (4 matches)
    20 permit udp host 172.17.0.5 host 172.16.1.1 eq isakmp log (4 matches)
    30 permit ip any any (295 matches)
```



注意：請確保您的access-list中允許ip any any。否則，由於訪問清單應用在出口介面的入站方向，因此可以阻止所有其他流量。

驗證GRE在隧道保護刪除後是否正常工作

當DMVPN不起作用時，在使用IPsec進行故障排除之前，請驗證GRE隧道在沒有IPsec加密的情況下是否工作正常。

有關詳細資訊，請參閱如何配置GRE隧道。

NHRP註冊失敗

中心和分支之間的VPN隧道已啟動，但無法傳遞資料流量：

```
<#root>

Router#

show crypto isakmp sa

        dst             src             state          conn-id  slot   status
        172.17.0.1      172.16.1.1      QM_IDLE           1082    0    ACTIVE

<#root>

Router#

show crypto IPSEC sa

local  ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (172.17.0.1/255.255.255.255/47/0)

#pkts encaps: 154, #pkts encrypt: 154, #pkts digest: 154
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
```

```
inbound esp sas:
spi: 0xF830FC95(4163959957)
outbound esp sas:
spi: 0xD65A7865(3596253285)

!--- !--- Output is truncated !---
```

它顯示返回流量不會從隧道的另一端返回。

檢查分支路由器中的NHS條目：

<#root>

```
Router#
```

show ip nhrp nhs detail

```
Legend: E=Expecting replies, R=Responding
Tunnel0: 172.17.0.1  E  req-sent 0
```

req-failed 30

```
 repl-recv 0
Pending Registration Requests:
Registration Request: Reqid 4371, Ret 64  NHS 172.17.0.1
```

它顯示NHS請求失敗。要解決此問題，請確保分支路由器隧道介面上的配置正確。

組態範例:

<#root>

```
interface Tunnel0
 ip address 10.0.0.9 255.255.255.0
 ip nhrp map 10.0.0.1 172.17.0.1
 ip nhrp map multicast 172.17.0.1
```

ip nhrp nhs 172.17.0.1

!--- !--- Output is truncated !---

配置示例，其中包含NHS伺服器的正確條目：

<#root>

```
interface Tunnel0
 ip address 10.0.0.9 255.255.255.0
 ip nhrp map 10.0.0.1 172.17.0.1
 ip nhrp map multicast 172.17.0.1
```

ip nhrp nhs 10.0.0.1

!--- !--- Output is truncated !---

現在，驗證NHS條目和IPSec加密/解密計數器：

<#root>

```
Router#
```

show ip nhrp nhs detail

```
Legend: E=Expecting replies, R=Responding
Tunnel0:        10.0.0.1 RE  req-sent 4
```

req-failed 0

```
repl-recv 3 (00:01:04 ago)

Router#
```

show crypto IPSec sa

```
local  ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (172.17.0.1/255.255.255.255/47/0)
```

#pkts encaps: 121, #pkts encrypt: 121, #pkts digest: 121
#pkts decaps: 118, #pkts decrypt: 118, #pkts verify: 118

```
inbound esp sas:
spi: 0x1B7670FC(460747004)
outbound esp sas:
spi: 0x3B31AA86(993110662)

!--- !--- Output is truncated !---
```

驗證是否已正確配置生命週期

使用以下命令驗證當前SA生存時間和下次重新協商的時間：

- **show crypto isakmp sa detail**
- **show crypto ipsec sa peer<NBMA-address-peer>**

注意SA生存期值。如果它們接近配置的生命週期（對於ISAKMP預設為24小時，對於IPsec預設為1小時），則意味著這些SA最近進行了協商。如果您稍待片刻，然後再次協商這些協定，則ISAKMP和/或IPSec可能會上下反彈。

<#root>

Router#

show crypto ipsec security-assoc lifetime

Security association lifetime: 4608000 kilobytes/3600 seconds

Router#

show crypto isakmp policy

```
Global IKE policy
Protection suite of priority 1
Encryption algorithm: DES-Data Encryption Standard (65 bit keys)
Hash algorithm: Message Digest 5
Authentication method: Pre-Shared Key
Diffie-Hellman group: #1 (768 bit)
```

Lifetime: 86400 seconds, no volume limit

```
Default protection suite
 Encryption algorithm: DES- Data Encryption Standard (56 bit keys)
 Hash algorithm: Secure Hash Standard
 Authentication method: Rivest-Shamir-Adleman Signature
 Diffie-Hellman group: #1 (768 bit)
 Lifetime: 86400 seconds, no volume limit

Router#
```

show crypto ipsec sa

```
interface: Ethernet0/3
    Crypto map tag: vpn, local addr. 172.17.0.1
   local  ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (172.17.0.1/255.255.255.255/47/0)
   current_peer: 172.17.0.1:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 19, #pkts encrypt: 19, #pkts digest 19
    #pkts decaps: 19, #pkts decrypt: 19, #pkts verify 19
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
    #send errors 1, #recv errors 0
     local crypto endpt.: 172.16.1.1, remote crypto endpt.: 172.17.0.1
     path mtu 1500, media mtu 1500
     current outbound spi: 8E1CB77A

 inbound esp sas:
      spi: 0x4579753B(1165587771)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2000, flow_id: 1, crypto map: vpn
```

sa timing: remaining key lifetime (k/sec): (4456885/3531)

```
        IV size: 8 bytes
        replay detection support: Y
outbound esp sas:
      spi: 0x8E1CB77A(2384246650)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2001, flow_id: 2, crypto map: vpn
```

```
sa timing: remaining key lifetime (k/sec): (4456885/3531)
```

```
        IV size: 8 bytes
        replay detection support: Y
```

驗證是否只在一個方向傳輸流量

分支到分支路由器之間的VPN隧道已啟動，但無法傳遞資料流量。

```
   <#root>

Spoke1#
```

```
show crypto ipsec sa peer 172.16.2.11
```

```
   local  ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (172.16.2.11/255.255.255.255/47/0)
```

```
#pkts encaps: 110, #pkts encrypt: 110
    #pkts decaps: 0, #pkts decrypt: 0,
```

```
local crypto endpt.: 172.16.1.1,
remote crypto endpt.: 172.16.2.11
      inbound esp sas:
      spi: 0x4C36F4AF(1278669999)
      outbound esp sas:
      spi: 0x6AC801F4(1791492596)

!--- !--- Output is truncated !---


Spoke2#
```

```
sh crypto ipsec sa peer 172.16.1.1
```

```
   local  ident (addr/mask/prot/port): (172.16.2.11/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)
```

```
 #pkts encaps: 116, #pkts encrypt: 116,
   #pkts decaps: 110, #pkts decrypt: 110,
```

```
local crypto endpt.: 172.16.2.11,
remote crypto endpt.: 172.16.1.1
     inbound esp sas:
     spi: 0x6AC801F4(1791492596)
     outbound esp sas:
     spi: 0x4C36F4AF(1278669999

!--- !--- Output is truncated !---
```

spoke1中沒有解封封包，這表示esp封包會在從spoke2傳回spoke1的路徑中某個地方捨棄。

spoke2路由器同時顯示encap和decap，這表示ESP流量在到達spoke2之前被過濾。它可能發生在spoke2的ISP端，或者發生在spoke2路由器和spoke1路由器之間路徑中的任何防火牆上。在允許ESP（IP通訊協定50）之後，spoke1和spoke2都會顯示封裝和解除封裝計數器增加。

<#root>

```
spoke1#
```

```
show crypto ipsec sa peer 172.16.2.11
```

```
   local  ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (172.16.2.11/255.255.255.255/47/0)
```

```
 #pkts encaps: 300, #pkts encrypt: 300
    #pkts decaps: 200, #pkts decrypt: 200
```

```
!--- !--- Output is truncated !---
```

```
spoke2#
```

```
sh crypto ipsec sa peer 172.16.1.1
```

```
   local  ident (addr/mask/prot/port): (172.16.2.11/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)
```

```
#pkts encaps: 316, #pkts encrypt: 316,
   #pkts decaps: 300, #pkts decrypt: 310
```

```
!--- !--- Output is truncated !---
```

驗證已建立路由協定鄰居

分支無法建立路由協定鄰居關係：

<#root>

Hub#

show ip eigrp neighbors

```
H   Address     Interface   Hold Uptime     SRTT    RTO       Q      Seq
                                (sec)             (ms)  Cnt     Num
2   10.0.0.9     Tu0         13  00:00:37     1    5000       1      0
0   10.0.0.5     Tu0         11     00:00:47   1587   5000       0     1483
1   10.0.0.11    Tu0         13     00:00:56     1    5000       1      0
```

Syslog message:
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 10:
Neighbor 10.0.0.9 (Tunnel0) is down: retry limit exceeded

Hub#

show ip route eigrp

```
    172.17.0.0/24 is subnetted, 1 subnets
C       172.17.0.0 is directly connected, FastEthernet0/0
     10.0.0.0/24 is subnetted, 1 subnets
C       10.0.0.0 is directly connected, Tunnel0
C    192.168.0.0/24 is directly connected, FastEthernet0/1
S*   0.0.0.0/0 [1/0] via 172.17.0.100
```

驗證是否在集線器中正確配置了NHRP組播對映。

在集線器中，需要在集線器隧道介面中配置動態nhrp組播對映。

組態範例:

```
interface Tunnel0
 ip address 10.0.0.1 255.255.255.0
 ip mtu 1400
 no ip next-hop-self eigrp 10
 ip nhrp authentication test
 ip nhrp network-id 10
 no ip split-horizon eigrp 10
 tunnel mode gre multipoint

!--- !--- Output is truncated !---
```

包含用於動態nhrp組播對映的正確條目的配置示例：

```
    <#root>

interface Tunnel0
 ip address 10.0.0.1 255.255.255.0
 ip mtu 1400
 no ip next-hop-self eigrp 10
 ip nhrp authentication test


ip nhrp map multicast dynamic


 ip nhrp network-id 10
 no ip split-horizon eigrp 10
 tunnel mode gre multipoint

!--- !--- Output is truncated !---
```

這允許NHRP自動將分支路由器增加到組播NHRP對映。

有關詳細資訊，請參閱Cisco IOS IP編址服務命令參考中的ip nhrp map multicast dynamic 命令。

<#root>

Hub#

show ip eigrp neighbors

```
IP-EIGRP neighbors for process 10
H   Address     Interface   Hold   Uptime   SRTT    RTO     Q     Seq
                                            (sec)    (ms)   Cnt    Num
2   10.0.0.9     Tu0         12   00:16:48   13     200     0     334
1   10.0.0.11    Tu0         13   00:17:10   11     200     0     258
0   10.0.0.5     Tu0         12   00:48:44  1017    5000    0     1495
```

Hub#

show ip route

```
     172.17.0.0/24 is subnetted, 1 subnets
C       172.17.0.0 is directly connected, FastEthernet0/0
```

D   192.168.11.0/24 [90/2944000] via 10.0.0.11, 00:16:12, Tunnel0

```
     10.0.0.0/24 is subnetted, 1 subnets
C       10.0.0.0 is directly connected, Tunnel0
C    192.168.0.0/24 is directly connected, FastEthernet0/1
```

```
D    192.168.2.0/24 [90/2818560] via 10.0.0.9, 00:15:45, Tunnel0
```

```
S*   0.0.0.0/0 [1/0] via 172.17.0.100
```

透過eigrp協定獲知分支的路由。

遠端訪問VPN與DMVPN整合的問題

問題

DMVPN工作正常，但無法建立RAVPN。

解決方案

使用ISAKMP配置檔案和IPSec配置檔案來實現此目的。 為DMVPN和RAVPN建立單獨的配置檔案。

有關詳細資訊，請參閱DMVPN和帶ISAKMP配置檔案的簡易VPN伺服器配置示例。

Dual-hub-dual-dmvpn問題

問題

dual-hub-dual-dmvpn問題。具體而言，隧道會關閉，無法重新協商。

解決方案

在中心點和分支點上的隧道介面使用隧道IPsec保護中的shared關鍵字。

組態範例：

```
interface Tunnel43
 description <<tunnel to primary cloud>>
 tunnel source interface vlan10
 tunnel protection IPSec profile myprofile shared

!--- !--- Output is truncated !---

interface Tunnel44
 description <<tunnel to secondary cloud>>
 tunnel source interface vlan10
 tunnel protection IPSec profile myprofile shared

!--- !--- Output is truncated !---
```

有關詳細資訊，請參閱思科IOS安全命令參考(A-C)中的**tunnel protection** 命令。

透過DMVPN登入到伺服器時出現問題

問題

無法訪問透過DMVPN網路伺服器的流量。

解決方案

問題可能與使用GRE和IPsec的封包的MTU和MSS大小有關。

現在，封包大小可能是分段的問題。若要消除此問題，請使用以下命令：

<#root>

```
ip mtu 1400
ip tcp adjust-mss 1360
crypto IPSec fragmentation after-encryption (global)
```

您還可以配置**tunnel path-mtu-discovery**命令來動態發現MTU大小。

有關詳細說明，請參閱解決GRE和IPSEC中的IP分段、MTU、MSS和PMTUD問題.

無法通過特定埠訪問DMVPN上的伺服器

問題

無法通過特定埠訪問DMVPN上的伺服器。

解決方案

驗證是否停用Cisco IOS防火牆功能集並檢視其是否有效。

如果運行正常，則問題與Cisco IOS防火牆配置有關，與DMVPN無關。

相關資訊

- **動態多點VPN (DMVPN)**
- **IPSec 協商/IKE 通訊協定**
- **思科技術支援與下載**

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。