일반적인 DMVPN 문제 해결

목차

소개

이 문서에서는 DMVPN(Dynamic Multipoint VPN) 문제에 대한 가장 일반적인 솔루션을 설명합니다.

사전 요구 사항

요구 사항

Cisco IOS® 라우터의 DMVPN 컨피그레이션에 대한 지식이 있는 것이 좋습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco IOS란

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

배경 정보

이 문서에서는 DMVPN(Dynamic Multipoint VPN) 문제에 대한 가장 일반적인 솔루션을 설명합니다. 이러한 솔루션 중 다수는 DMVPN 연결의 심층적인 트러블슈팅에 앞서 구현할 수 있습니다. 이 문서는 연결 트러블슈팅을 시작하기 전에 시도해야 할 일반적인 절차의 체크리스트로 표시되며 Cisco 기술 지원 서비스에 문의하십시오.

자세한 내용은 Dynamic Multipoint VPN Configuration Guide, Cisco IOS Release 15M&T를 참조하십시오.

IPsec 문제를 해결하는 데 사용되는 일반적인 디버그 명령에 대한 설명은 Understand and Use Debug Commands to Troubleshoot IPsec을 참조하십시오.

DMVPN 컨피그레이션이 작동하지 않음

문제

최근에 구성되거나 수정된 DMVPN 솔루션이 작동하지 않습니다.

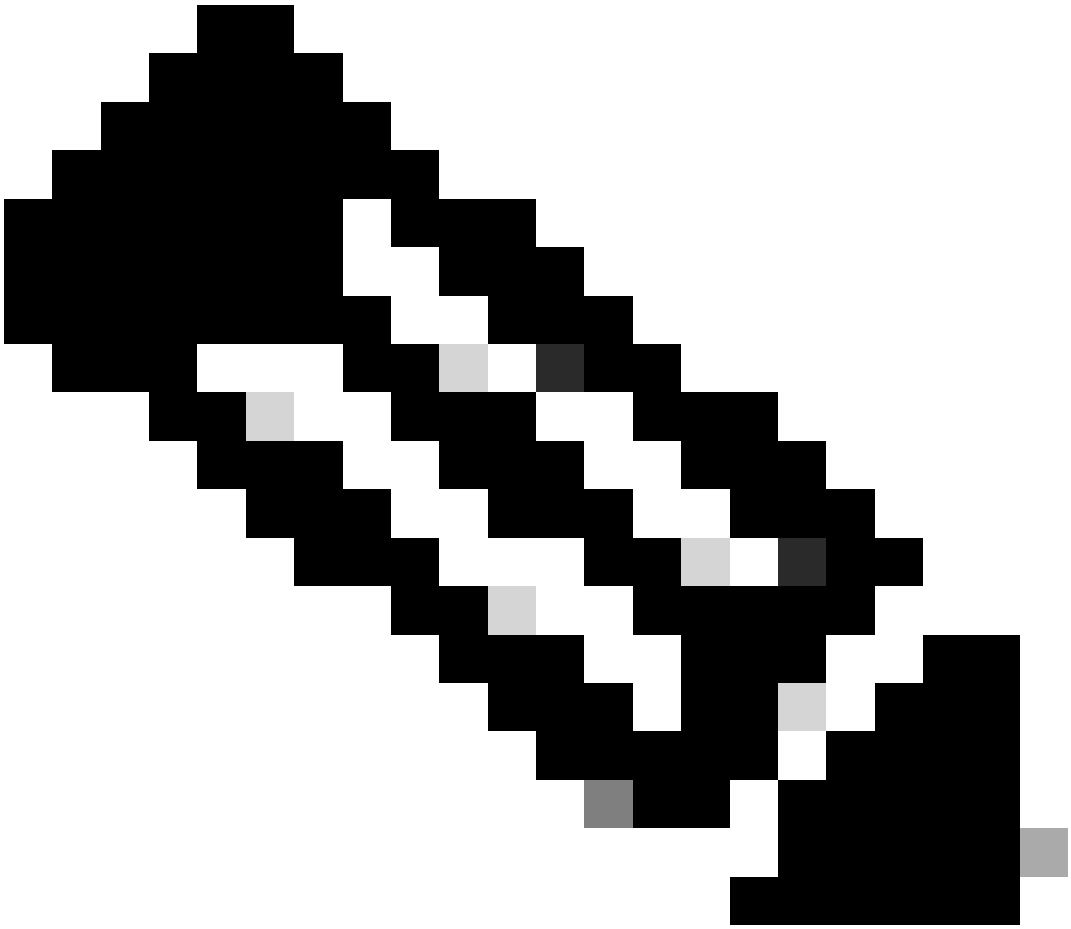
현재 DMVPN 컨피그레이션이 더 이상 작동하지 않습니다.

솔루션

이 섹션에는 가장 일반적인 DMVPN 문제에 대한 솔루션이 포함되어 있습니다.

이러한 솔루션(특정 순서 없음)은 심층적인 트러블슈팅을 수행하기 전에 확인하거나 시도할 항목의 체크리스트로 사용할 수 있습니다.

- 일반적인 문제
- ISP(인터넷 서비스 공급자)에서 ISAKMP(인터넷 보안 연결 및 키 관리 프로토콜) 패킷이 차단되었는지 확인합니다.
- 터널 보호가 제거될 때 GRE(Generic Routing Encapsulation)가 작동하는지 확인합니다.
- NHRP(Next-Hop Resolution Protocol) 등록이 실패합니다.
- 수명이 올바르게 구성되었는지 확인합니다.
- 트래픽이 한 방향으로만 흐르는지 확인합니다.
- 라우팅 프로토콜 네이버가 설정되었는지 확인합니다.



참고: 시작하기 전에 다음 단계를 확인하십시오.

---

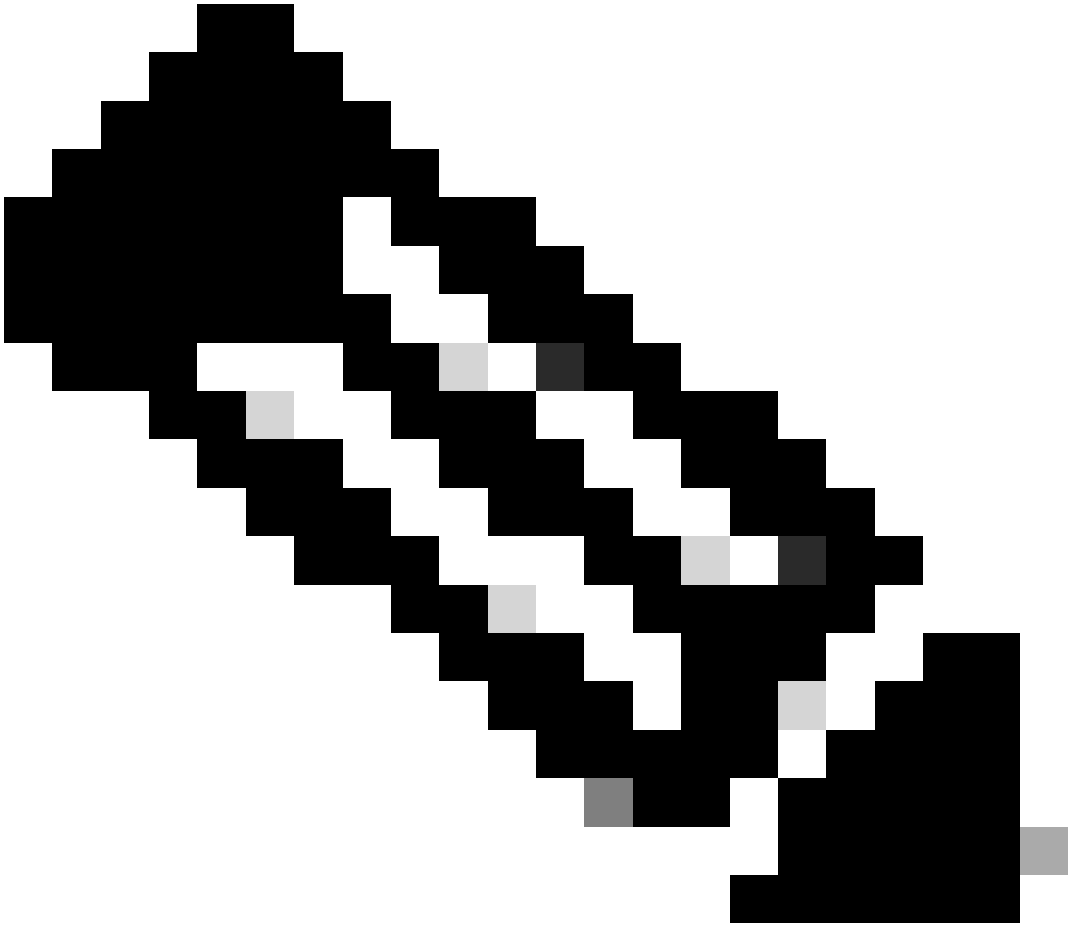
1. 허브와 스포크 간의 타임스탬프 동기화
2. msec 디버그 및 로그 타임스탬프 활성화:

   라우터(config)#service 타임스탬프 디버그 datetime msec

   라우터(config)#service 타임스탬프 로그 datetime msec

3. 디버깅 세션에 대한 터미널 EXEC 프롬프트 타임스탬프를 활성화합니다.

   Router#terminal exec 프롬프트 타임스탬프



참고: 이렇게 하면 디버그 출력을 show 명령 출력과 쉽게 상호 연결할 수 있습니다.

일반적인 문제

기본 연결 확인

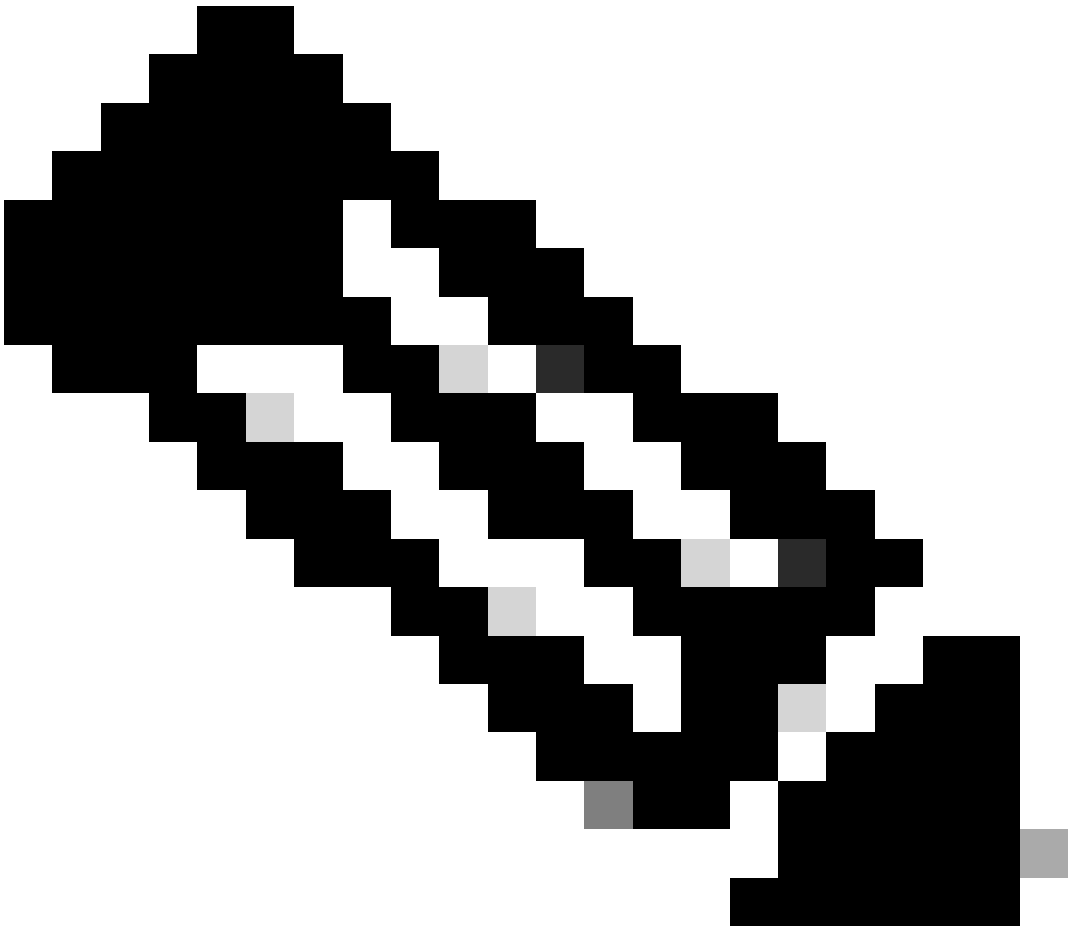
1. NBMA 주소를 사용하여 허브에서 스포크로 Ping을 수행하고 반대 방향으로 전환합니다.

   이러한 ping은 DMVPN 터널을 통해서가 아니라 물리적 인터페이스를 통해 직접 이동해야 합니다. ping 패킷을 차단하는 방화벽이 없기를 바랍니다. 이 방법이 작동하지 않으면 허브 라우터와 스포크 라우터 간의 라우팅 및 방화벽을 확인합니다.

2. 또한 traceroute를 사용하여 암호화된 터널 패킷이 사용하는 경로를 확인합니다.

3. debug 및 show 명령을 사용하여 연결이 없음을 확인합니다.

   - 디버그 ip icmp
   - debug ip packet



참고: debug ip packet 명령은 상당한 양의 출력을 생성하고 상당한 양의 시스템 리소스를 사용합니다. 프로덕션 네트워크에서는 이 명령을 신중하게 사용해야 합니다. 항상 access-list 명령과 함께 사용합니다. debug ip 패킷과 함께 access-list를 사용하는 방법에 대한 자세한 내용은 Troubleshoot with IP Access Lists를 참조하십시오.

호환되지 않는 ISAKMP 정책 확인

구성된 ISAKMP 정책이 원격 피어에서 제안한 정책과 일치하지 않으면 라우터는 기본 정책인 65535을 시도합니다. 둘 중 하나라도 일치하지 않으면 ISAKMP 협상에 실패합니다.

show crypto isakmp sa 명령은 ISAKMP SA가 MM_NO_STATE에 있음을 보여주는데, 이는 기본 모드가 실패했음을 의미합니다.

잘못된 사전 공유 키 암호 확인

사전 공유 비밀이 양쪽에서 동일하지 않으면 협상은 실패합니다.

라우터가 온전성 검사 실패 메시지를 반환합니다.

호환되지 않는 IPsec 변형 집합 확인

두 IPsec 디바이스에서 IPsec transform-set이 호환되지 않거나 일치하지 않으면 IPsec 협상이 실패합니다.

라우터가 IPsec 제안에 대해 허용되지 않는 atts 메시지를 반환합니다.

ISAKMP 패킷이 ISP에서 차단되는지 확인

<#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)
```

앞의 예에서는 VPN 터널 플래핑을 보여 줍니다.

또한 스포크 라우터debug crypto isakmp 가 udp 500 패킷을 전송하는지 확인합니다.

<#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
```

이전 출력에서는 debug 스포크 라우터가 10초마다 udp 500 패킷을 전송하는 것을 보여줍니다.

ISP에 문의하여 Spoke 라우터가 ISP 라우터에 직접 연결되어 있고 UDP 500 트래픽을 허용하는지 확인합니다.

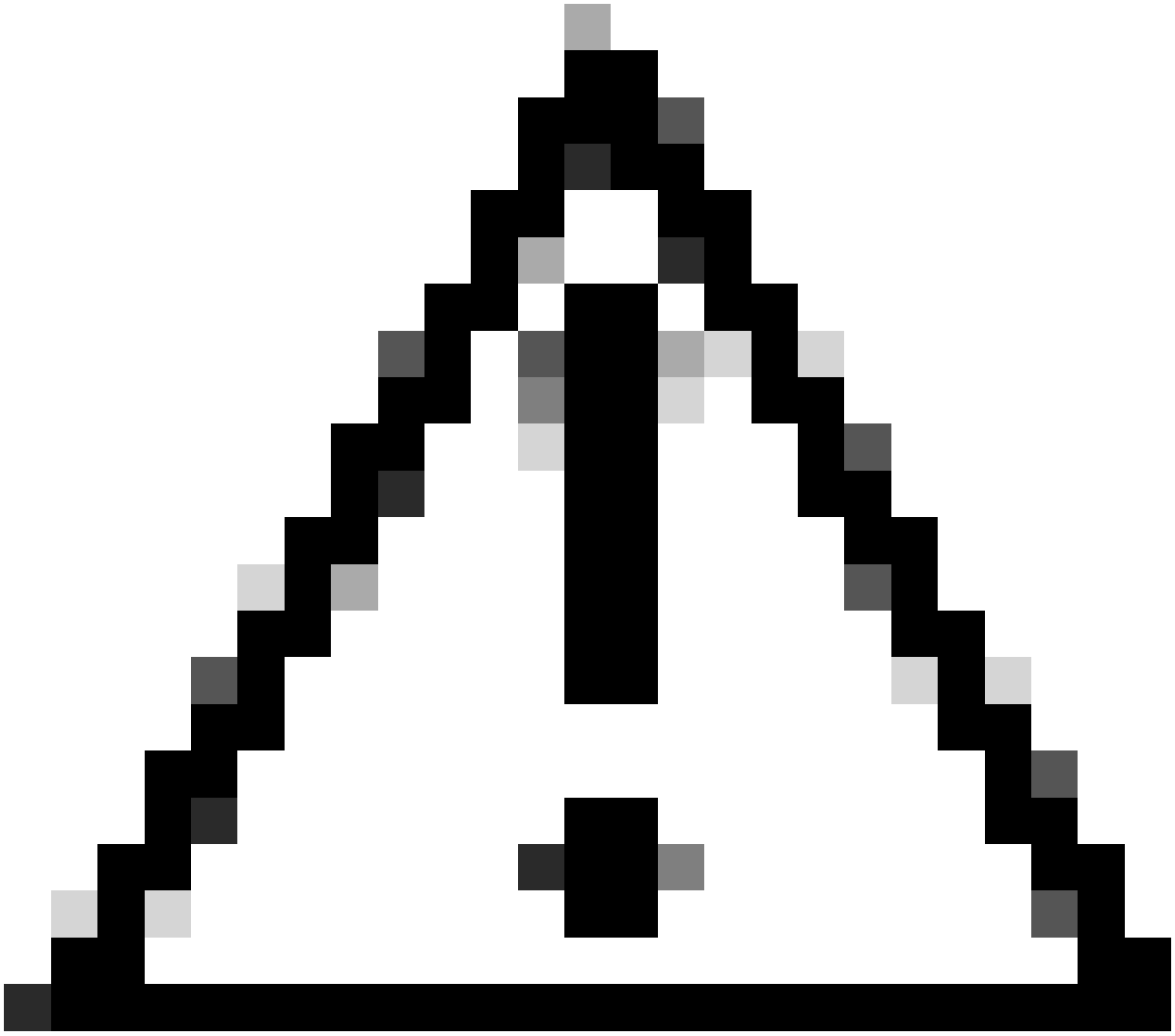
ISP에서 udp 500을 허용한 후 이그레스 인터페이스에 인바운드 ACL을 추가합니다. 이그레스 인터페이스는 udp 500이 udp 500 트래픽이 라우터로 들어오도록 허용하는 터널 소스입니다. 이 명령을 show access-list사용하여 적중 횟수가 증가하는지 확인합니다.

<**#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)



주의: 액세스 목록에서 ip any가 허용되는지 확인하십시오. 그렇지 않으면 다른 모든 트래픽은 이그레스 인터페이스의 인바운드에 적용된 액세스 목록으로 차단될 수 있습니다.

터널 보호가 제거될 때 GRE가 작동하는지 확인

DMVPN이 작동하지 않을 경우 IPsec 문제를 해결하기 전에 IPsec 암호화 없이 GRE 터널이 제대로 작동하는지 확인하십시오.

자세한 내용은 GRE 터널 구성 방법을 참조하십시오.

NHRP 등록 실패

허브와 스포크 간의 VPN 터널이 작동하지만 데이터 트래픽을 전달할 수 없습니다.

<#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 !---
```

이는 반환 트래픽이 터널의 다른 끝에서 반환되지 않음을 보여줍니다.

스포크 라우터에서 NHS 항목을 확인합니다.

<#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
```

NHS 요청이 실패한 것으로 표시됩니다. 이 문제를 해결하려면 스포크 라우터 터널 인터페이스의 컨피그레이션이 올바른지 확인하십시오.

컨피그레이션 예시:

```
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 !---

NHS 서버에 대한 올바른 항목이 포함된 컨피그레이션 예:


```
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 !---

이제 NHS 항목 및 IPsec 암호화/암호 해독 카운터를 확인합니다.

<#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 !---

수명이 올바르게 구성되었는지 확인

다음 명령을 사용하여 현재 SA 수명 및 다음 재협상 시간을 확인합니다.

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

SA 수명 값을 확인합니다. 구성된 수명에 근접한 경우(기본값은 ISAKMP의 경우 24시간, IPsec의 경우 1시간), 이는 이러한 SA가 최근에 협상되었음을 의미합니다. 잠시 후에 다시 협상한 경우 ISAKMP 및/또는 IPsec이 상하로 바운스될 수 있습니다.

<#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
```

트래픽이 한 방향으로만 흐르는지 확인

스포크 투 스포크 라우터 간의 VPN 터널이 작동하지만 데이터 트래픽을 전달할 수 없습니다.

<#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 !---
```

spoke1에는 decapp 패킷이 없습니다. 이는 esp 패킷이 spoke2에서 spoke1으로 돌아오는 경로 어딘가에서 삭제됨을 의미합니다.

spoke2 라우터에는 encap 및 decap이 모두 표시됩니다. 즉, ESP 트래픽이 spoke2에 도달하기 전에 필터링됩니다. 스포크2의 ISP 쪽 또는 스포크2 라우터와 스포크1 라우터 간의 경로에 있는 모든 방화벽에서 발생할 수 있습니다. ESP(IP Protocol 50)를 허용하면 spoke1 및 spoke2 모두 encaps 및 decaps 카운터가 증가합니다.

<#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 !---

라우팅 프로토콜 네이버가 설정되었는지 확인합니다.

스포크가 라우팅 프로토콜 네이버 관계를 설정할 수 없습니다.

<#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
```

NHRP 멀티캐스트 매핑이 허브에 올바르게 구성되어 있는지 확인합니다.

허브에서는 허브 터널 인터페이스에 동적 nhrp 멀티캐스트 매핑이 구성되어 있어야 합니다.

컨피그레이션 예시:

```
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 !---
```

동적 nhrp 멀티캐스트 매핑에 대한 올바른 항목이 있는 컨피그레이션 예:

<#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 !---
```

이를 통해 NHRP는 멀티캐스트 NHRP 매핑에 스포크 라우터를 자동으로 추가할 수 있습니다.

자세한 내용은 Cisco IOS IP ip nhrp map multicast dynamic Addressing Services 명령 참조의 명령을 참조하십시오.

<#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
```

스포크에 대한 경로는 eigrp 프로토콜을 통해 학습됩니다.

DMVPN 통합을 사용하는 원격 액세스 VPN 문제

문제

DMVPN은 정상적으로 작동하지만 RAVPN을 설정할 수 없습니다.

솔루션

이를 위해 ISAKMP 프로파일 및 IPsec 프로파일을 사용합니다. DMVPN 및 RAVPN에 대해 별도의 프로필을 생성합니다.

자세한 내용은 DMVPN 및 ISAKMP 프로필을 사용하는 Easy VPN 서버 구성 예를 참조하십시오.

듀얼 허브 듀얼 dmvpn 문제

문제

듀얼 허브 듀얼 dmvpn 문제. 특히 터널이 다운되어 재협상할 수 없습니다.

솔루션

허브 및 스포크의 터널 인터페이스 모두에 대해 터널 IPsec 보호에서 shared 키워드를 사용합니다.

컨피그레이션 예:

```
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 !---
```

자세한 내용은 Cisco **tunnel protection** IOS Security Command Reference (A-C)의 명령을 참조하십시오.

DMVPN을 통한 서버 로그온 문제

문제

DMVPN 네트워크 서버를 통한 문제 트래픽에 액세스할 수 없습니다.

솔루션

이 문제는 GRE 및 IPsec을 사용하는 패킷의 MTU 및 MSS 크기와 관련이 있을 수 있습니다.

이제 패킷 크기는 프래그먼트화와 관련된 문제가 될 수 있습니다. 이 문제를 해결하려면 다음 명령을 사용하십시오.

<#root>

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

MTU 크기를 동적**tunnel path-mtu-discovery**으로 검색하도록 명령을 구성할 수도 있습니다.

자세한 설명은 GRE 및 IPSEC에서 IP 프래그먼트화, MTU, MSS 및 PMTUD 문제 해결을 참조하십시오.

특정 포트를 통해 DMVPN의 서버에 액세스할 수 없음

문제

특정 포트를 통해 DMVPN의 서버에 액세스할 수 없습니다.

솔루션

Cisco IOS 방화벽 기능 집합을 비활성화하고 작동하는지 확인합니다.

정상적으로 작동하면 DMVPN이 아닌 Cisco IOS 방화벽 컨피그레이션과 관련된 문제입니다.

관련 정보

- **DMVPN(Dynamic Multipoint VPN)**
- **IPSec 협상/IKE 프로토콜**
- **Cisco 기술 지원 및 다운로드**

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.