DMVPN 1단계 디버깅 문제 해결 가이드

목차

소개

이 문서에서는 허브에서 발생하는 디버그 메시지와 DMVPN(Dynamic Multipoint Virtual Private Network) 1단계 구축의 스포크에 대해 설명합니다.

사전 요구 사항

이 문서의 컨피그레이션 및 debug 명령에 대해서는 Cisco IOS® Release 12.4(9)T 이상을 실행하는 두 개의 Cisco 라우터가 필요합니다.일반적으로 기본 DMVPN 1단계에서는 ASR(Aggregation Services Router)용 Cisco IOS Release 12.2(13)T 이상 또는 Release 12.2(33)XNC가 필요합니다. 단, 이 문서에 표시된 기능과 디버그는 지원되지 않을 수 있습니다.

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- GRE(Generic Routing Encapsulation)

- NHRP(Next Hop Resolution Protocol)
- ISAKMP(Internet Security Association and Key Management Protocol)
- IKE(Internet Key Exchange)
- IPSec(Internet Protocol Security)
- 다음 라우팅 프로토콜 중 하나 이상:EIGRP(Enhanced Interior Gateway Routing Protocol), OSPF(Open Shortest Path First), RIP(Routing Information Protocol) 및 BGP(Border Gateway Protocol)

사용되는 구성 요소

이 문서의 정보는 Cisco IOS Release 15.1(4)M4를 실행하는 Cisco 2911 ISR(Integrated Services Router)을 기반으로 합니다.

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

대폭 향상된 기능

이러한 Cisco IOS 버전은 DMVPN 1단계에 중요한 기능 또는 수정 사항을 도입했습니다.

- 릴리스 12.2(18)SXF5 - PKI(Public Key Infrastructure) 사용 시 ISAKMP 지원 향상
- 릴리스 12.2(33)XNE - ASR, IPSec 프로파일, 터널 보호, IPSec NAT(Network Address Translation) 통과
- 릴리스 12.3(7)T - iVRF(Inside Virtual Routing and Forwarding) 지원
- 릴리스 12.3(11)T - 전면 도어 Virtual Routing and Forwarding(fVRF) 지원
- 릴리스 12.4(9)T - 다양한 DMVPN 관련 디버그 및 명령 지원
- 릴리스 12.4(15)T - 공유 터널 보호
- 릴리스 12.4(20)T - DMVPN을 통한 IPv6
- 릴리스 15.0(1)M - NHRP 터널 상태 모니터링

표기 규칙

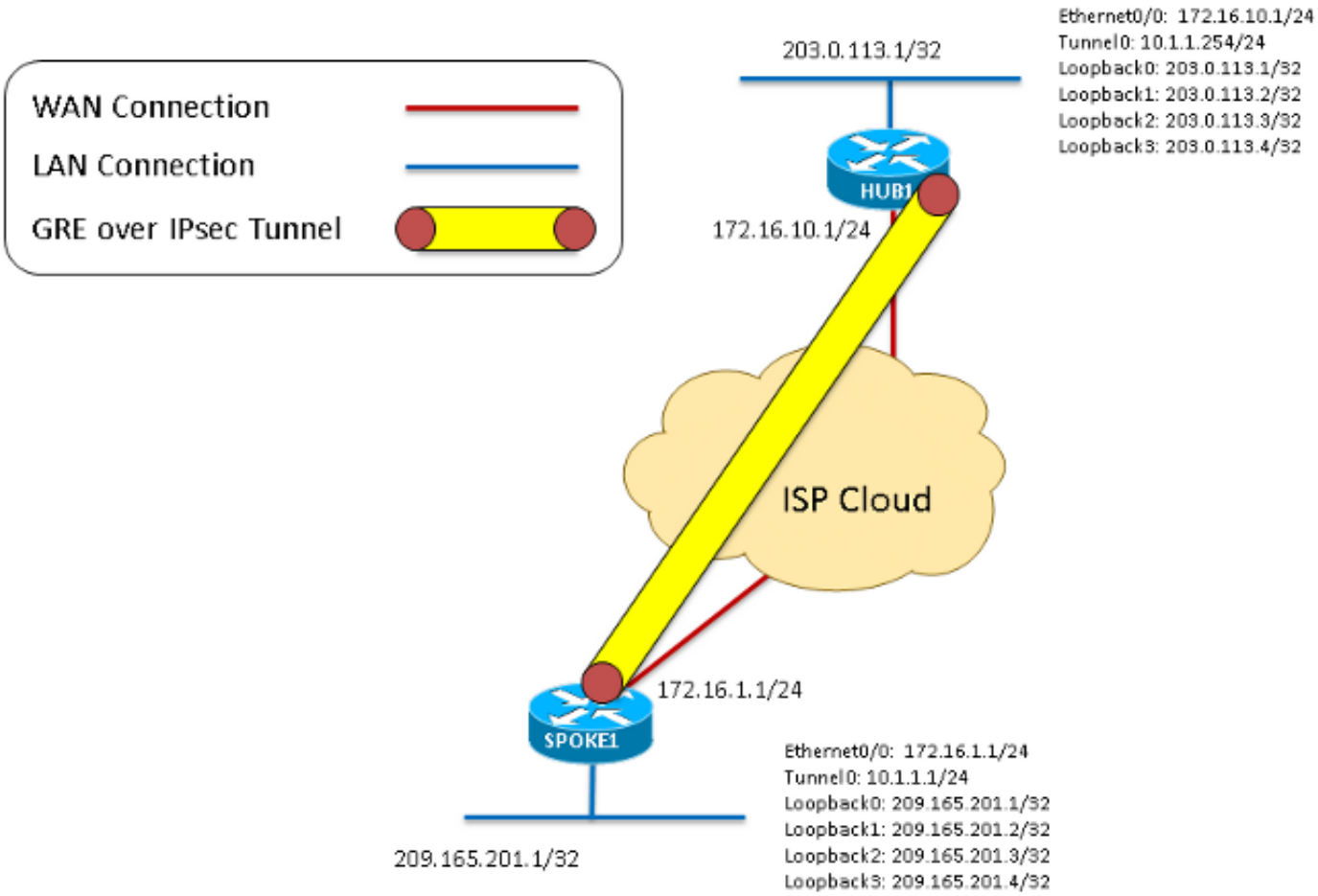
문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

관련 구성

토폴로지 개요

이 토폴로지에서는 릴리스 15.1(4)M4를 실행하는 2911 ISR 2개가 DMVPN 1단계에 대해 구성되었습니다.하나는 허브로, 다른 하나는 스포크로로.Ethernet0/0은 각 라우터에서 "인터넷" 인터페이스로 사용되었습니다.4개의 루프백 인터페이스는 허브 또는 스포크 사이트에 상주하는 로컬 영역 네트워크를 시뮬레이션하도록 구성됩니다.스포크가 하나만 있는 DMVPN 1단계 토폴로지이므로 스포크는 멀티포인트 GRE 터널이 아닌 포인트-투-포인트 GRE 터널로 구성됩니다.각 라우터에서 동일한 암호화 구성(ISAKMP 및 IPSec)을 사용하여 정확히 일치하는지 확인했습니다.

다이어그램 1



암호화

이는 허브와 스포크에서 동일합니다.

```
crypto isakmp policy 1
encr 3des
hash sha
authentication pre-share
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
crypto ipsec transform-set DMVPN-TSET esp-3des esp-sha-hmac
mode transport
crypto ipsec profile DMVPN-IPSEC
set transform-set DMVPN-TSET
```

허브

```
interface Tunnel0
ip address 10.1.1.254 255.255.255.0
no ip redirects
ip mtu 1400
ip nhrp authentication NHRPAUTH
ip nhrp map multicast dynamic
ip nhrp network-id 1
ip tcp adjust-mss 1360
no ip split-horizon eigrp 1
tunnel source Ethernet0/0
tunnel mode gre multipoint
tunnel key 1
tunnel protection ipsec profile DMVPN-IPSEC
```

```
end

interface Ethernet0/0
ip address 172.16.10.1 255.255.255.0
end

interface Loopback0
ip address 203.0.113.1 255.255.255.255
interface Loopback1
ip address 203.0.113.2 255.255.255.255
interface Loopback2
ip address 203.0.113.3 255.255.255.255
interface Loopback3
ip address 203.0.113.4 255.255.255.255

router eigrp 1
network 10.1.1.0 0.0.0.255
network 203.0.113.1 0.0.0.0
network 203.0.113.2 0.0.0.0
network 203.0.113.3 0.0.0.0
network 203.0.113.4 0.0.0.0
```

스포크

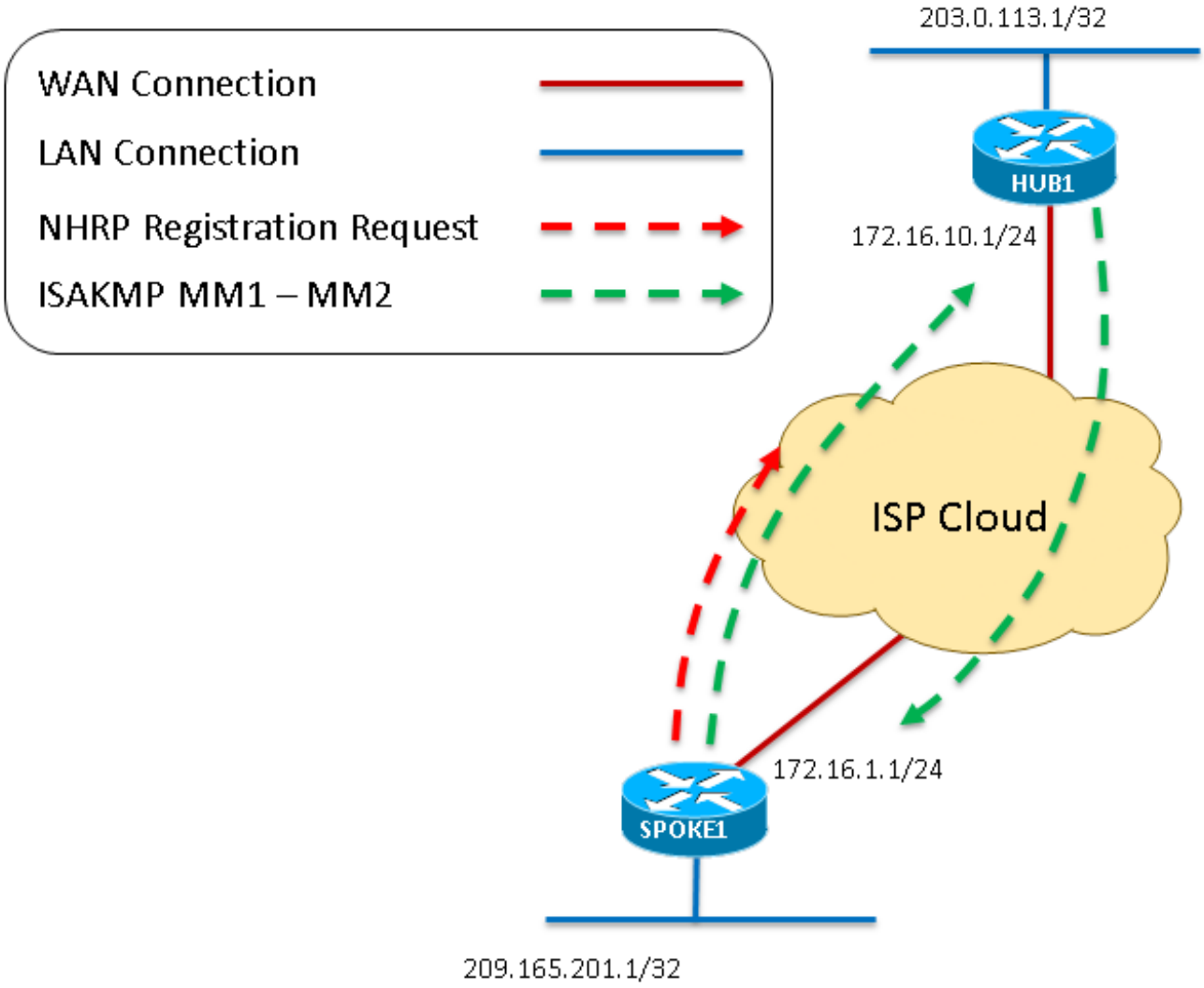
```
interface Tunnel0
ip address 10.1.1.1 255.255.255.0
ip mtu 1400
ip nhrp authentication NHRPAUTH
ip nhrp map 10.1.1.254 172.16.10.1
ip nhrp network-id 1
ip nhrp nhs 10.1.1.254
ip tcp adjust-mss 1360
tunnel source Ethernet0/0
tunnel destination 172.16.10.1
tunnel key 1
tunnel protection ipsec profile DMVPN-IPSEC
end

interface Ethernet0/0
ip address 172.16.1.1 255.255.255.0
end

interface Loopback0
ip address 209.165.201.1 255.255.255.255
interface Loopback1
ip address 209.165.201.2 255.255.255.255
interface Loopback2
ip address 209.165.201.3 255.255.255.255
interface Loopback3
ip address 209.165.201.4 255.255.255.255

router eigrp 1
network 209.165.201.1 0.0.0.0
network 209.165.201.2 0.0.0.0
network 209.165.201.3 0.0.0.0
network 209.165.201.4 0.0.0.0
network 10.1.1.0 0.0.0.255
```

디버깅

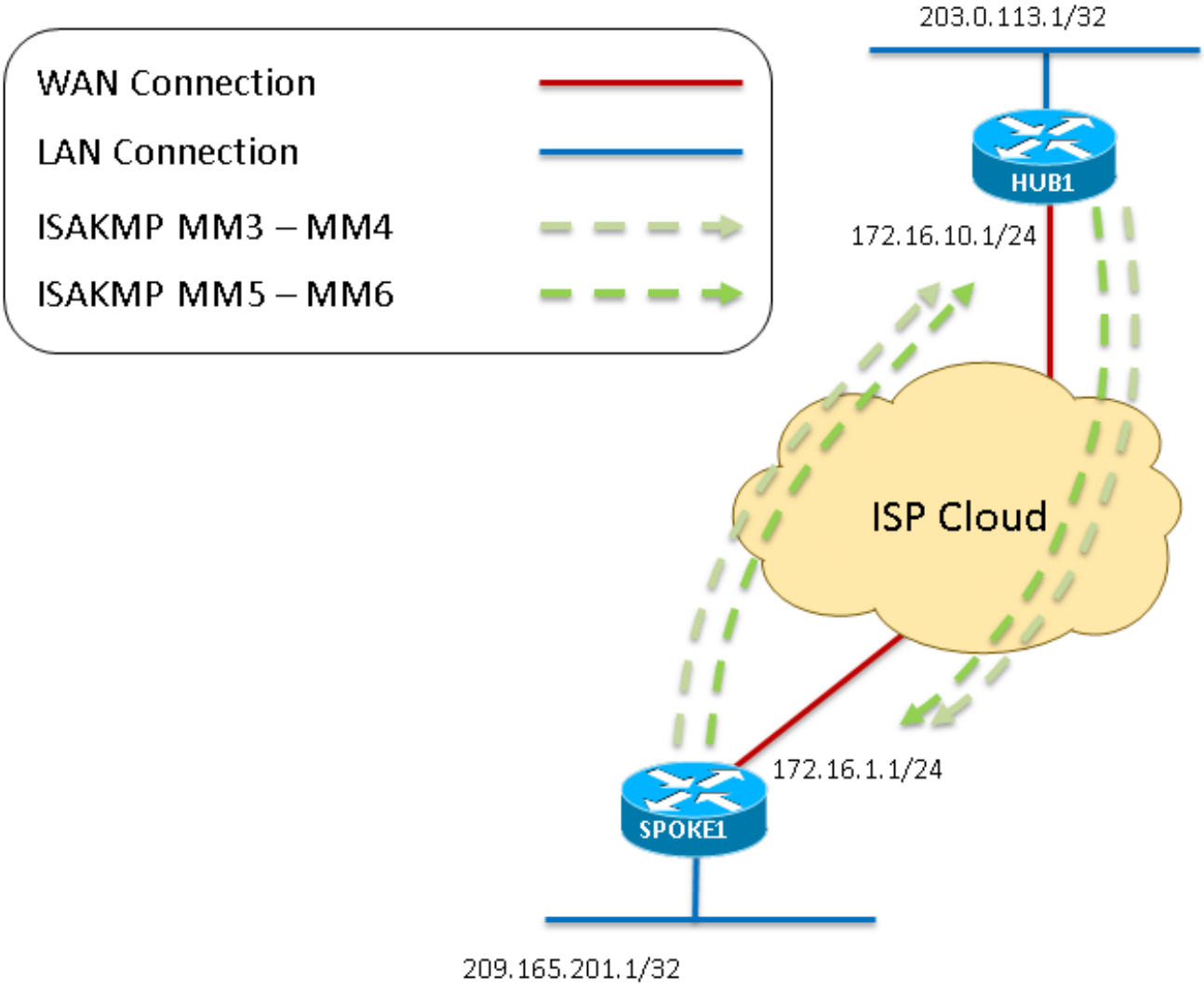
패킷 흐름 시각화

이 문서에서 볼 수 있는 전체 DMVPN 패킷 흐름을 시각화한 것입니다.각 단계를 설명하는 자세한 디버그도 포함되어 있습니다.

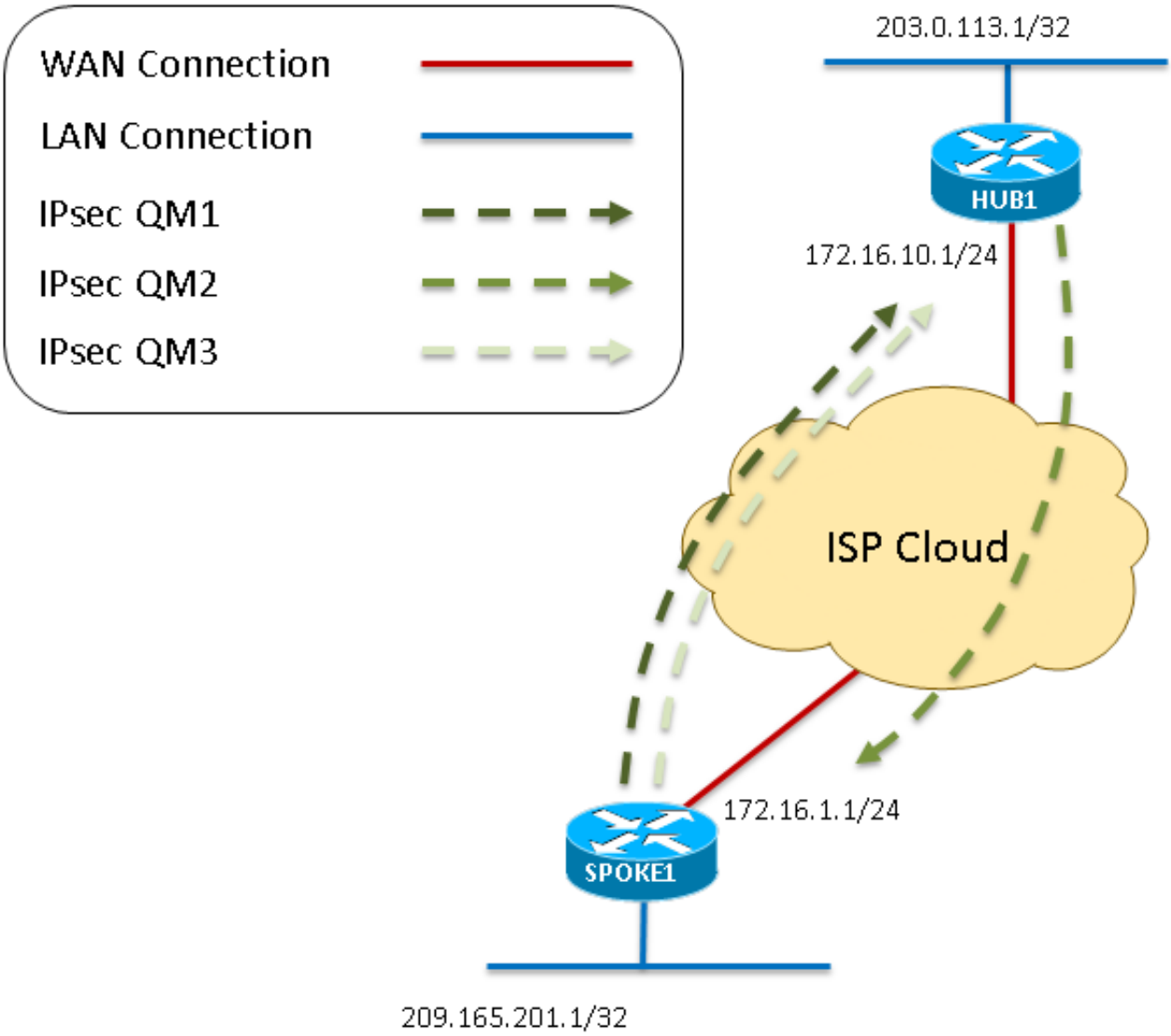
1. 스포크의 터널이 "no shutdown"이면 DMVPN 프로세스를 시작하는 NHRP 등록 요청이 생성됩니다.허브의 컨피그레이션이 완전히 동적이므로 스포크는 연결을 시작하는 엔드포인트여야 합니다.
2. 그런 다음 NHRP 등록 요청은 GRE에 캡슐화되어 암호화 프로세스가 시작됩니다.
3. 이때 첫 번째 ISAKMP 주 모드 메시지(ISAKMP MM1)가 스포크에서 포트 UDP500의 허브로 전송됩니다.
4. 허브는 MM1을 수신하고 처리하며 ISAKMP MM2와 응답합니다. 일치하는 ISAKMP 정책이 있습니다.
   다이어그램 2 - 1~4단계를 나타냅니다
   .



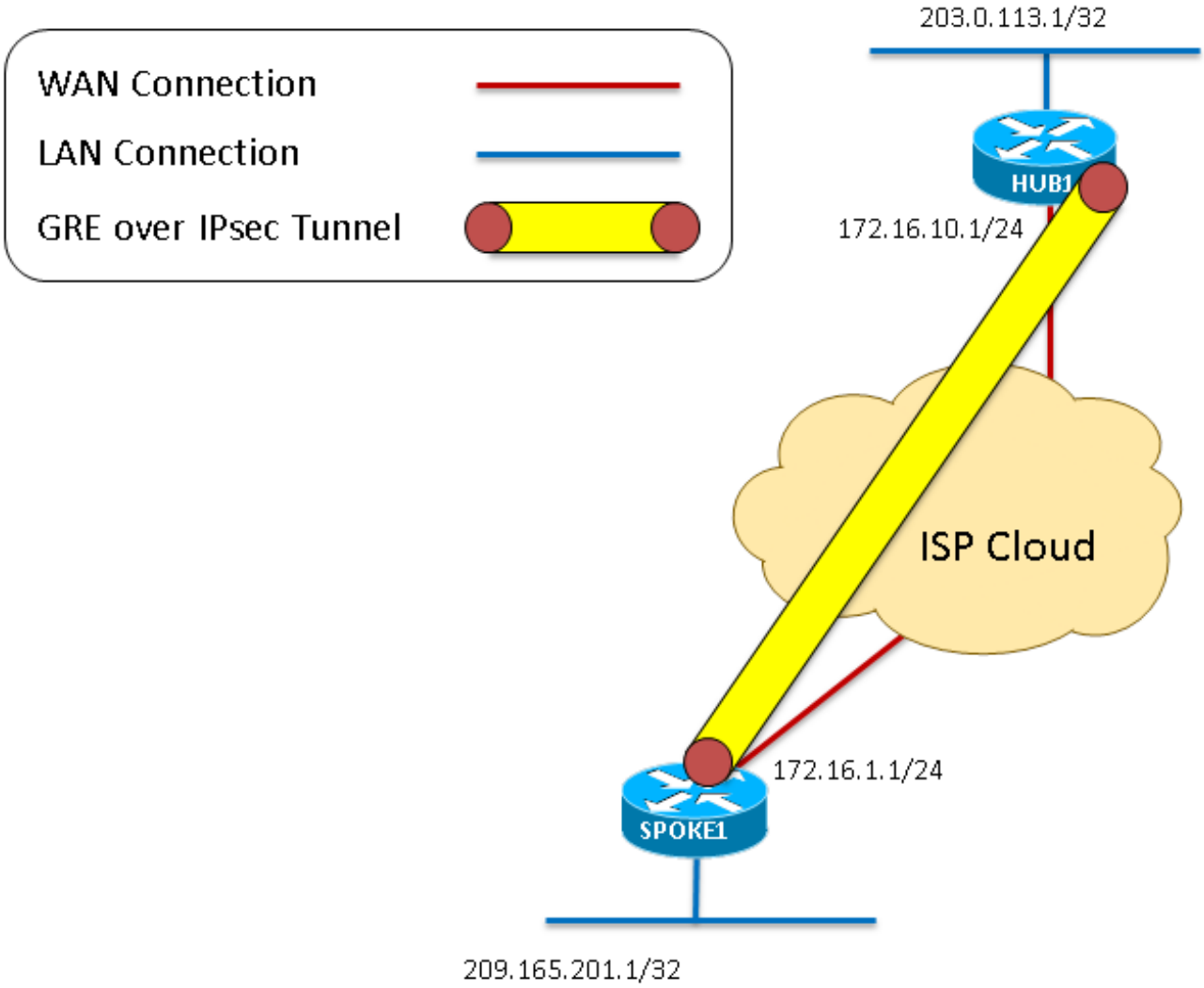
5. 스포크가 MM2를 수신하면 MM3으로 응답합니다. MM1과 마찬가지로 스포크는 수신된 ISAKMP 정책이 유효함을 확인합니다.
6. 허브는 MM3을 수신하고 MM4로 응답합니다.
7. ISAKMP 협상의 이 시점에서 NAT가 전송 경로에서 탐지되면 스포크는 포트 UDP4500에서 응답할 수 있습니다.그러나 NAT가 탐지되지 않은 경우 스포크는 계속 진행되며 UDP500에서 MM5를 전송합니다. 마지막으로, 허브는 주 모드 교환을 완료하기 위해 MM6로 응답합니다.
   다이어그램 3 - 5~7단계를 나타냅니다
   .



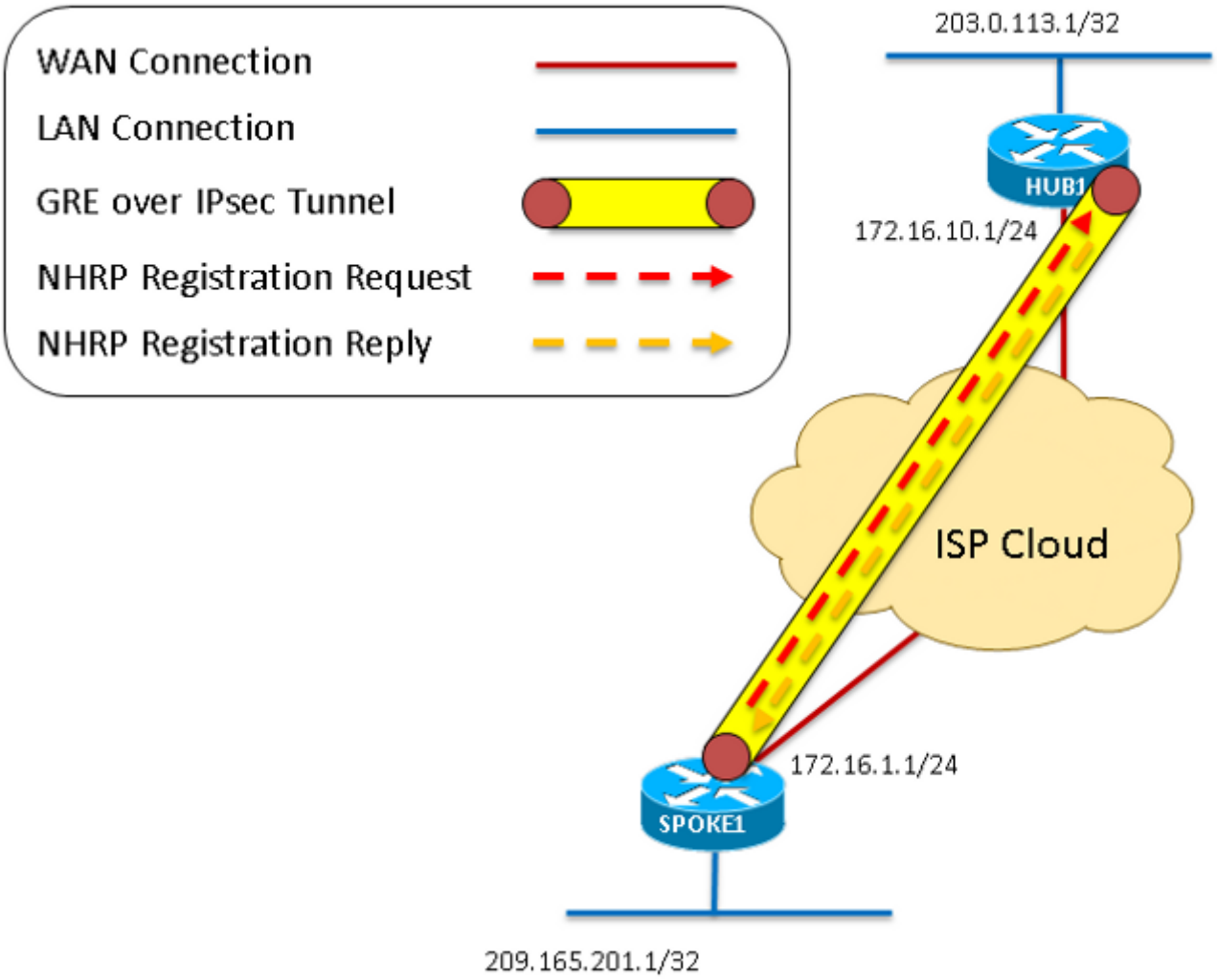
8. 스포크는 허브에서 MM6을 수신하면 빠른 모드를 시작하기 위해 UDP500의 허브로 QM1을 보냅니다.
9. 허브는 QM1을 수신하고 QM2로 응답합니다. 수신된 모든 특성이 수락됩니다.이때 허브는 이 세션에 대한 2단계 SA를 생성합니다.
10. 빠른 모드 협상의 마지막 단계로 QM2는 스포크에 의해 수신됩니다.그런 다음 Spoke는 2단계 SA를 만들고 응답하여 QM3을 전송합니다.ISAKMP 및 IPSec 협상을 완료합니다.이제 이러한 두 피어 간의 GRE 트래픽을 암호화하는 IPSec 세션이 있습니다.
    다이어그램 4 - 8~10단계를 나타냅니다
    .



11. 이제 암호화 세션이 작동 중이고 트래픽을 전달할 수 있으므로 이러한 패킷은 GRE over IPSec 터널 내에서 캡슐화됩니다.
    다이어그램 5 - 11단계 참조



12. 첫 번째 단계에서와 같이 스포크는 IPSec 터널을 통해 GRE를 통해 전송되는 NHRP 등록 요청을 생성합니다.
13. 허브는 스포크에 유효한 터널 및 NBMA(Nonbroadcast Multiaccess) 주소가 있음을 확인한 후 NHRP 등록 요청을 수신하고 NHRP 등록 응답을 전송합니다.Spoke는 등록 프로세스를 완료하는 이 NHRP 등록 응답을 받습니다.
    다이어그램 6 - 12~13단계를 나타냅니다
    .



이러한 디버그는 debug dmvpn all 명령을 hub 및 spoke 라우터에 입력할 때 발생합니다.이 특정 명령은 다음 디버깅 집합을 활성화합니다.

```
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
```

설명이 있는 디버깅

IPSec이 구현되는 컨피그레이션이므로 디버그에는 모든 ISAKMP 및 IPSec 디버그가 표시됩니다 .암호화 구성이 없으면 "IPsec" 또는 "ISAKMP"로 시작하는 디버그를 무시합니다.

허브 디버그 설명	시퀀스의 디버깅
이러한 처음 몇 개의 디버그 메시지는 터널 인터페이스에 입력된 **no shutdown** 명령으로 생성됩니다.메시지는 시작 중인 crypto, GRE 및 NHRP 서비스에 의해 생성됩니다. 허브에 NHRP 등록 오류가 나타납니다. 허브에 NHS(Next Hop Server)가 구성되지 않았기 때문입니다(허브는 DMVPN 클라우드의 NHS임). 예상된 일입니다.	IPSEC-IFC MGRE/Tu0:터널 상태를 확인하는 중입니다. **NHRP:if_up:Tunnel0 proto 0** IPSEC-IFC MGRE/Tu0:터널 시작 IPSEC-IFC MGRE/Tu0:crypto_ss_listen_start가 이미 수신 대기 중입 **%CRYPTO-6-ISAKMP_ON_OFF:ISAKMP가 켜져 있습니다.** **NHRP:등록을 보낼 수 없음 - 구성된 NHS가 없음** %LINK-3-업다운:Interface Tunnel0, 상태가 up으로 변경됨 NHRP:if_up:Tunnel0 proto 0 NHRP:등록을 보낼 수 없음 - 구성된 NHS가 없음 IPSEC-IFC MGRE/Tu0:터널 시작 IPSEC-IFC MGRE/Tu0:crypto_ss_listen_start가 이미 수신 대기 중입 **%LINEPROTO-5-업다운:Interface Tunnel0의 회선 프로토콜, 상태가로 변경됨** IPSEC-IFC GRE/Tu0:터널 상태를 확인하는 중입니다. IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1):연결 조회에서 0을 반니다. **IPSEC-IFC GRE/Tu0:crypto_ss_listen_start가 이미 수신 대기 중입니** **IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1):프로파일 DMVPN-IPS사용하여 소켓 열기** IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1):연결 조회에서 0을 반니다. IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1):즉시 터널을 트리거합 IPSEC-IFC GRE/Tu0:공유 목록에 Tunnel0 터널 인터페이스 추가 **NHRP:if_up:Tunnel0 proto 0** **NHRP:터널0:대상 10.1.1.254/32 next-hop 10.1.1.254 캐시 추가 172.16.10.1** IPSEC-IFC GRE/Tu0:터널 시작 IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1):연결 조회가 961D220환했습니다. IPSEC-IFC GRE/Tu0:crypto_ss_listen_start가 이미 수신 대기 중입니 IPSEC-IFC GRE/Tu0:crypto_ss_listen_start가 이미 수신 대기 중입니 IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1):프로파일 DMVPN-IPS사용하여 소켓 열기 IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1):연결 조회가 961D220환했습니다. IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1):소켓이 이미 열려 있습.무시합니다. CRYPTO_SS(터널 초):응용 프로그램 수신 대기 시작

mapdb AVL에 맵을 삽입하지 못했습니다. map + ace 쌍이 mapdb에
있습니다.
%CRYPTO-6-ISAKMP_ON_OFF:ISAKMP가 켜져 있습니다.
CRYPTO_SS(터널 초):활성 열린 소켓 정보:로컬 172.16.1.1
172.16.1.1/255.255.255.255/0, 원격 172.16.10.1
172.16.10.1/255.255.255.255/0, 포트 47, ifc Tu0
ISAKMP(1단계) 협상 시작
IPSEC(recalculate_mtu):sadb_root 94EFDC0 mtu를 1500으로 재설
IPSEC(sa_request):,
(key eng.메시지) OUTBOUND local= 172.16.1.1:500, remote=
172.16.10.1:500,
local_proxy= 172.16.1.1/255.255.255.255/47/0(type=1),
remote_proxy= 172.16.10.1/255.255.255.255/47/0(type=1),
protocol= ESP, transform= esp-3des esp-sha-hmac(전송),
lifedur= 3600s 및 4608000kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x0
ISAKMP:(0):SA 요청 프로필이 (NULL)
ISAKMP:172.16.10.1, 피어 포트 500에 대한 피어 구조를 만들었습니
ISAKMP:새 피어 생성 피어 = 0x95F6858 peer_handle = 0x8000004
ISAKMP:피어 구조체 0x95F6858 잠금, isakmp_initiator에 대한 refco
ISAKMP:로컬 포트 500, 원격 포트 500
ISAKMP:새 노드 0을 QM_IDLE로 설정
ISAKMP:(0):sa를 성공적으로 삽입합니다. sa = 8A26FB0
ISAKMP:(0):Aggressive 모드를 시작할 수 없습니다. 주 모드를 시도
ISAKMP:(0):172.16.10.1과 일치하는 피어 사전 공유 키를 찾았습니다
ISAKMP:(0):NAT-T vendor-rfc3947 ID 생성
ISAKMP:(0):NAT-T vendor-07 ID 생성
ISAKMP:(0):NAT-T vendor-03 ID 생성
ISAKMP:(0):NAT-T vendor-02 ID 생성
ISAKMP:(0):입력 = IKE_MESG_FROM_IPSEC, IKE_SA_REQ_MM
ISAKMP:(0):이전 상태 = IKE_READY 새 상태 = IKE_I_MM1

ISAKMP:(0):기본 모드 교환 시작
ISAKMP:(0):172.16.10.1 my_port 500 peer_port 500(I) MM_NO_STA
패킷 전송
ISAKMP:(0):IKE IPv4 패킷 전송
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1):연결 조회가 961D220
환했습니다.
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1):소켓 준비 메시지

스포크의 터널이 "no shutdown"이면 허브는 포트 500에서 IKE NEW SA(Main Mode 1) 메시지를 수신합니다. Responder로 허브는 ISAKMP SA(Security Association)를 생성합니다.
ISAKMP 상태가 IKE_READY에서 IKE_R_MM1로 변경됩니다.

수신된 IKE Main Mode 1 메시지가 처리됩니다.허브는 피어에 일치하는 ISAKMP 특성이 있으며 방금 생성한 ISAKMP SA에 채워집니다.이 메시

ISAKMP(0):172.16.1.1 dport 500 sport 500 global(N) NEW SA에서 수
신
ISAKMP:172.16.1.1, 피어 포트 500에 대한 피어 구조를 만들었습니다
ISAKMP:새 피어 생성 피어 = 0x8CACD00 peer_handle = 0x800000
ISAKMP:피어 구조체 0x8CACD00 잠금, crypto_isakmp_process_blo
대한 refcount 1
ISAKMP:로컬 포트 500, 원격 포트 500
ISAKMP:(0):sa를 성공적으로 삽입합니다. sa = 6A5BDE8
ISAKMP:(0):입력 = IKE_MESG_FROM_PEER, IKE_MM_EXCH
ISAKMP:(0):이전 상태 = IKE_READY 새 상태 = IKE_R_MM1
ISAKMP:(0):SA 페이로드를 처리하는 중입니다.메시지 ID = 0
ISAKMP:(0):공급업체 id 페이로드 처리
ISAKMP:(0):공급업체 ID가 Unity/DPD인 것 같지만 주요 69개 불일치
ISAKMP(0):공급업체 ID는 NAT-T RFC 3947입니다.

지는 피어가 암호화, SHA 해싱, DH(Diffie Hellman) 그룹 1, 사전 공유 키, 인증에 대한 기본 SA 수명(0x0 0x1 0x51 0x80 = 0x15180 = 86400초)에 3DES-CBC를 사용한다는 것을 보여줍니다.
ISAKMP 상태는 여전히 IKE_R_MM1입니다. 회신을 스포크에 보내지 않았기 때문입니다.
NAT-T 벤더 ID 메시지는 NAT의 탐지 및 통과에 사용됩니다.이러한 메시지는 NAT의 구현 여부에 관계없이 ISAKMP의 협상 중에 필요합니다 .DPD(Dead Peer Detection)에도 비슷한 메시지가 표시됩니다.

MM_SA_SETUP(주 모드 2)이 스포크로 전송되며, 이 경우 MM1이 유효한 ISAKMP 패킷으로 수신되고 수락되었음을 확인합니다.
ISAKMP 상태가 IKE_R_MM1에서 IKE_R_MM2로 변경됩니다.

ISAKMP:(0):공급업체 id 페이로드 처리
ISAKMP:(0):공급업체 ID가 Unity/DPD인 것 같지만 주요 245개 불일
ISAKMP(0):공급업체 ID는 NAT-T v7입니다.
ISAKMP:(0):공급업체 id 페이로드 처리
ISAKMP:(0):공급업체 ID가 Unity/DPD인 것 같지만 주요 157개 불일
ISAKMP:(0):공급업체 ID는 NAT-T v3입니다.
ISAKMP:(0):공급업체 id 페이로드 처리
ISAKMP:(0):공급업체 ID가 Unity/DPD인 것 같지만 주요 123개 불일
ISAKMP:(0):공급업체 ID는 NAT-T v2입니다.
ISAKMP:(0):172.16.1.1과 일치하는 피어 사전 공유 키를 찾았습니다
ISAKMP:(0):로컬 사전 공유 키 발견
ISAKMP:xauth에 대한 프로필을 검색하는 중...
ISAKMP:(0):우선순위 1 정책에 대해 ISAKMP 변형 1을 확인하는 중
ISAKMP: 암호화 3DES-CBC
ISAKMP: 해시 SHA
ISAKMP: 기본 그룹 1
ISAKMP: 인증 사전 공유
ISAKMP: 수명 유형(초)
ISAKMP: 0x0 0x1 0x51 0x80의 수명(VPI)
ISAKMP:(0):att를 사용할 수 있습니다.다음 페이로드는 0입니다.
ISAKMP:(0):허용 가능한 atts:실제 수명:0
ISAKMP:(0):허용 가능한 atts:life:0
ISAKMP:(0):sa vpi_length:4의 채우기
ISAKMP:(0):sa life_in_seconds:86400에 기록
ISAKMP:(0):실제 수명 반환:86400
ISAKMP:(0)::시작 수명 타이머:86400 .

ISAKMP:(0):공급업체 id 페이로드 처리
ISAKMP:(0):공급업체 ID가 Unity/DPD인 것 같지만 주요 69개 불일치
ISAKMP(0):공급업체 ID는 NAT-T RFC 3947입니다.
ISAKMP:(0):공급업체 id 페이로드 처리
ISAKMP:(0):공급업체 ID가 Unity/DPD인 것 같지만 주요 245개 불일
ISAKMP(0):공급업체 ID는 NAT-T v7입니다.
ISAKMP:(0):공급업체 id 페이로드 처리
ISAKMP:(0):공급업체 ID가 Unity/DPD인 것 같지만 주요 157개 불일
ISAKMP:(0):공급업체 ID는 NAT-T v3입니다.
ISAKMP:(0):공급업체 id 페이로드 처리
ISAKMP:(0):공급업체 ID가 Unity/DPD인 것 같지만 주요 123개 불일
ISAKMP:(0):공급업체 ID는 NAT-T v2입니다.
ISAKMP:(0):입력 = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
ISAKMP:(0):이전 상태 = IKE_R_MM1 새 상태 = IKE_R_MM1
ISAKMP:(0):NAT-T vendor-rfc3947 ID 생성
ISAKMP:(0):172.16.1.1 my_port 500 peer_port 500(R) MM_SA_SET
패킷 전송
ISAKMP:(0):IKE IPv4 패킷 전송
ISAKMP:(0):입력 = IKE_MESG_INTERNAL, IKE_PROCESS_COMP
ISAKMP:(0):이전 상태 = IKE_R_MM1 새 상태 = IKE_R_MM2
ISAKMP(0):172.16.10.1 dport 500 sport 500 global (I) MM_NO_STA
서 수신된 패킷
ISAKMP:(0):입력 = IKE_MESG_FROM_PEER, IKE_MM_EXCH
ISAKMP:(0):이전 상태 = IKE_I_MM1 새 상태 = IKE_I_MM2

ISAKMP:(0):SA 페이로드를 처리하는 중입니다.메시지 ID = 0
ISAKMP:(0):공급업체 id 페이로드 처리
ISAKMP:(0):공급업체 ID가 Unity/DPD인 것 같지만 주요 69개 불일치
ISAKMP(0):공급업체 ID는 NAT-T RFC 3947입니다.
ISAKMP:(0):172.16.10.1과 일치하는 피어 사전 공유 키를 찾았습니다
ISAKMP:(0):로컬 사전 공유 키 발견
ISAKMP:xauth에 대한 프로필을 검색하는 중...
ISAKMP:(0):우선순위 1 정책에 대해 ISAKMP 변형 1을 확인하는 중
ISAKMP: 암호화 3DES-CBC
ISAKMP: 해시 SHA
ISAKMP: 기본 그룹 1
ISAKMP: 인증 사전 공유
ISAKMP: 수명 유형(초)
ISAKMP: 0x0 0x1 0x51 0x80의 수명(VPI)
ISAKMP:(0):att를 사용할 수 있습니다.다음 페이로드는 0입니다.
ISAKMP:(0):허용 가능한 atts:실제 수명:0
ISAKMP:(0):허용 가능한 atts:life:0
ISAKMP:(0):sa vpi_length:4의 채우기
ISAKMP:(0):sa life_in_seconds:86400에 기록
ISAKMP:(0):실제 수명 반환:86400
ISAKMP:(0)::시작 수명 타이머:86400 .

ISAKMP:(0):공급업체 id 페이로드 처리
ISAKMP:(0):공급업체 ID가 Unity/DPD인 것 같지만 주요 69개 불일치
ISAKMP(0):공급업체 ID는 NAT-T RFC 3947입니다.
ISAKMP:(0):입력 = IKE_MESG_INTERNAL,
IKE_PROCESS_MAIN_MODE
ISAKMP:(0):이전 상태 = IKE_I_MM2 새 상태 = IKE_I_MM2
**ISAKMP:(0):172.16.10.1 my_port 500 peer_port 500(I) MM_SA_SET
패킷 전송**
ISAKMP:(0):IKE IPv4 패킷 전송
ISAKMP:(0):입력 = IKE_MESG_INTERNAL, IKE_PROCESS_COMP
ISAKMP:(0):이전 상태 = IKE_I_MM2 새 상태 = IKE_I_MM3

MM_SA_SETUP(주 모드 3)이 허브에 의해 수신됩니다.허브는 피어가 또 다른 Cisco IOS 디바이스이고 Cisco 또는 Cisco 피어에 대해 탐지된 NAT가 없다는 결론을 내렸습니다.
ISAKMP 상태가 IKE_R_MM2에서 IKE_R_MM3로 변경됩니다.

**ISAKMP(0):172.16.1.1 dport 500 sport 500 global (R) MM_SA_SETU
서 패킷을 받았습니다.**
ISAKMP:(0):입력 = IKE_MESG_FROM_PEER, IKE_MM_EXCH
ISAKMP:(0):이전 상태 = IKE_R_MM2 새 상태 = IKE_R_MM3

ISAKMP:(0):KE 페이로드를 처리하는 중입니다.메시지 ID = 0
ISAKMP:(0):NONCE 페이로드를 처리하는 중입니다.메시지 ID = 0
ISAKMP:(0):172.16.1.1과 일치하는 피어 사전 공유 키를 찾았습니다
ISAKMP:(1002):공급업체 id 페이로드 처리
ISAKMP:(1002):공급업체 ID가 DPD입니다.
ISAKMP:(1002):공급업체 id 페이로드 처리
ISAKMP:(1002):다른 IOS Box와 대화했습니다!
ISAKMP:(1002):공급업체 id 페이로드 처리
ISAKMP:(1002):공급업체 ID가 Unity/DPD인 것 같지만 주요 225개 불
ISAKMP:(1002):공급업체 ID가 XAUTH입니다.
ISAKMP:수신된 페이로드 유형 20
**ISAKMP(1002):이 해시가 일치하지 않습니다. 이 노드는 NAT 외부에
니다.**
ISAKMP:수신된 페이로드 유형 20

ISAKMP(1002):자체 또는 피어에 대한 NAT를 찾을 수 없음
ISAKMP:(1002):입력 = IKE_MESG_INTERNAL,
IKE_PROCESS_MAIN_MODE
ISAKMP:(1002):이전 상태 = IKE_R_MM3 새 상태 = IKE_R_MM3

MM_KEY_EXCH(주 모드 4)는 허브에서 전송됩니다.
ISAKMP 상태가 IKE_R_MM3에서 IKE_R_MM4로 변경됩니다.

ISAKMP:(1002):172.16.1.1 my_port 500 peer_port 500(R) MM_KEY_EXCH에 패킷 전송
ISAKMP:(1002):IKE IPv4 패킷 전송
ISAKMP:(1002):입력 = IKE_MESG_INTERNAL,
IKE_PROCESS_COMPLETE
ISAKMP:(1002):이전 상태 = IKE_R_MM3 새 상태 = IKE_R_MM4
ISAKMP(0):172.16.10.1 dport 500 sport 500 global (I) MM_SA_SET
서 패킷을 받았습니다.
ISAKMP:(0):입력 = IKE_MESG_FROM_PEER, IKE_MM_EXCH
ISAKMP:(0):이전 상태 = IKE_I_MM3 새 상태 = IKE_I_MM4

ISAKMP:(0):KE 페이로드를 처리하는 중입니다.메시지 ID = 0
ISAKMP:(0):NONCE 페이로드를 처리하는 중입니다.메시지 ID = 0
ISAKMP:(0):172.16.10.1과 일치하는 피어 사전 공유 키를 찾았습니다
ISAKMP:(1002):공급업체 id 페이로드 처리
ISAKMP:(1002):공급업체 ID는 Unity입니다.
ISAKMP:(1002):공급업체 id 페이로드 처리
ISAKMP:(1002):공급업체 ID가 DPD입니다.
ISAKMP:(1002):공급업체 id 페이로드 처리
ISAKMP:(1002):다른 IOS Box와 대화했습니다!
ISAKMP:수신된 페이로드 유형 20
ISAKMP(1002):이 해시가 일치하지 않습니다. 이 노드는 NAT 외부어
니다.
ISAKMP:수신된 페이로드 유형 20
ISAKMP(1002):자체 또는 피어에 대한 NAT를 찾을 수 없음
ISAKMP:(1002):입력 = IKE_MESG_INTERNAL,
IKE_PROCESS_MAIN_MODE
ISAKMP:(1002):이전 상태 = IKE_I_MM4 새 상태 = IKE_I_MM4
ISAKMP:(1002):초기 연락처 보내기
ISAKMP:(1002):SA에서 ID 유형 ID_IPV4_ADDR을 사용하여 사전 공
인증을 수행하고 있습니다.
ISAKMP(1002):ID 페이로드
    다음 페이로드:8
    유형:1
    주소:172.16.1.1
    프로토콜:17
    포트:500
    길이:12
ISAKMP:(1002):총 페이로드 길이:12

ISAKMP:(1002):172.16.10.1 my_port 500 peer_port 500(I) MM_KEY_EXCH에 패킷 전송
ISAKMP:(1002):IKE IPv4 패킷 전송
ISAKMP:(1002):입력 = IKE_MESG_INTERNAL,
IKE_PROCESS_COMPLETE
ISAKMP:(1002):이전 상태 = IKE_I_MM4 새 상태 = IKE_I_MM5

MM_KEY_EXCH(주 모드 5)가 허브에서 수신됩니다.
ISAKMP 상태가 IKE_R_MM4에서 IKE_R_MM5로 변경됩니다.

ISAKMP(1002):172.16.1.1 dport 500 sport 500 global (R) MM_KEY_EXCH에서 패킷을 받았습니다.
ISAKMP:(1002):입력 = IKE_MESG_FROM_PEER, IKE_MM_EXCH
ISAKMP:(1002):이전 상태 = IKE_R_MM4 새 상태 = IKE_R_MM5

또한 ISAKMP 프로파일이 없어 "peer matches *none* of the profiles"이 표시됩니다.이 경우 ISAKMP는 프로필을 사용하지 않습니다.

ISAKMP:(1002):처리 ID 페이로드입니다.메시지 ID = 0
ISAKMP(1002):ID 페이로드
다음 페이로드:8
유형:1
주소:172.16.1.1
프로토콜:17
포트:500
길이:12
ISAKMP:(0)::피어가 프로파일 중 *없음*과 일치
ISAKMP:(1002):HASH 페이로드를 처리하는 중입니다.메시지 ID = 0
ISAKMP:(1002):NOTIFY INITIAL_CONTACT 프로토콜 1 처리
spi 0, 메시지 ID = 0, sa = 0x6A5BDE8
ISAKMP:(1002):SA 인증 상태:
인증
ISAKMP:(1002):SA가 172.16.1.1으로 인증되었습니다.
ISAKMP:(1002):SA 인증 상태:
인증
ISAKMP:(1002):초기 연락처 처리,
로컬 172.16.10.1 원격 172.16.1.1 원격 포트 500을 사용하여 기존 1단
2단계 SA를 축소합니다.
**ISAKMP:피어 172.16.10.1/172.16.1.1/500/, 을 삽입하고 성공적으로
8CACD00을 삽입했습니다.**
ISAKMP:(1002):입력 = IKE_MESG_INTERNAL,
IKE_PROCESS_MAIN_MODE
ISAKMP:(1002):이전 상태 = IKE_R_MM5 새 상태 = IKE_R_MM5

IPSEC(key_engine):1개의 KMI 메시지가 있는 큐 이벤트를 받았습니
ISAKMP:(1002):SA에서 ID 유형 ID_IPV4_ADDR을 사용하여 사전 공
인증을 수행하고 있습니다.
ISAKMP(1002):ID 페이로드
다음 페이로드:8
유형:1
주소:172.16.10.1
프로토콜:17
포트:500
길이:12
ISAKMP:(1002):총 페이로드 길이:12
**ISAKMP:(1002):172.16.1.1 my_port 500 peer_port 500(R)
MM_KEY_EXCH에 패킷 전송**
ISAKMP:(1002):IKE IPv4 패킷 전송
ISAKMP:(1002):입력 = IKE_MESG_INTERNAL,
IKE_PROCESS_COMPLETE
ISAKMP:(1002):이전 상태 = IKE_R_MM5 새 상태 = IKE_P1_COMPL

ISAKMP:(1002):입력 = IKE_MESG_INTERNAL,
IKE_PHASE1_COMPLETE
ISAKMP:(1002):이전 상태 = IKE_P1_COMPLETE 새 상태 =
IKE_P1_COMPLETE
**ISAKMP(1002):172.16.10.1 dport 500 sport 500 global (I)
MM_KEY_EXCH에서 패킷을 받았습니다.**
ISAKMP:(1002):처리 ID 페이로드입니다.메시지 ID = 0
ISAKMP(1002):ID 페이로드

최종 MM_KEY_EXCH 패킷(기본 모드 6)은 허브에서 전송됩니다.그러면 이 디바이스가 2단계(IPSec 빠른 모드)에 준비되었음을 나타내는 1단계 협상이 완료됩니다.
ISAKMP 상태가 IKE_R_MM5에서 IKE_P1_COMPLETE로 변경됩니다.

다음 페이로드:8
유형:1
주소:172.16.10.1
프로토콜:17
포트:500
길이:12
ISAKMP:(0)::피어가 프로파일 중 *없음*과 일치
ISAKMP:(1002):HASH 페이로드를 처리하는 중입니다.메시지 ID = 0
ISAKMP:(1002):SA 인증 상태:
인증
ISAKMP:(1002):SA가 172.16.10.1으로 인증되었습니다.
**ISAKMP:피어 172.16.1.1/172.16.10.1/500/, 을 삽입하려고 시도했지
공적으로 95F6858을 삽입했습니다.**
ISAKMP:(1002):입력 = IKE_MESG_FROM_PEER, IKE_MM_EXCH
ISAKMP:(1002):이전 상태 = IKE_I_MM5 새 상태 = IKE_I_MM6

ISAKMP:(1002):입력 = IKE_MESG_INTERNAL,
IKE_PROCESS_MAIN_MODE
ISAKMP:(1002):이전 상태 = IKE_I_MM6 새 상태 = IKE_I_MM6

ISAKMP:(1002):입력 = IKE_MESG_INTERNAL,
IKE_PROCESS_COMPLETE
**ISAKMP:(1002):이전 상태 = IKE_I_MM6 새 상태 = IKE_P1_COMPL
ISAKMP(1단계) 협상 끝, IPSEC(2단계) 협상 시작**
ISAKMP:(1002):빠른 모드 교환 시작, M-ID: 3464373979
ISAKMP:(1002):QM 개시자가 spi를 가져옵니다.
**ISAKMP:(1002):172.16.10.1 my_port 500 peer_port 500(I) QM_IDLE
킷 전송**
ISAKMP:(1002):IKE IPv4 패킷 전송
ISAKMP:(1002):Node 3464373979, Input = IKE_MESG_INTERNAL,
IKE_INIT_QM
ISAKMP:(1002):이전 상태 = IKE_QM_READY 새 상태 = IKE_QM_I_
ISAKMP:(1002):입력 = IKE_MESG_INTERNAL,
IKE_PHASE1_COMPLETE
ISAKMP:(1002):이전 상태 = IKE_P1_COMPLETE 새 상태 =
IKE_P1_COMPLETE
**ISAKMP(1002):172.16.1.1 dport 500 sport 500 global(R) QM_IDLE에
킷을 받았습니다.**
ISAKMP:새 노드 -830593317을 QM_IDLE로 설정
ISAKMP:(1002):HASH 페이로드를 처리하는 중입니다.메시지 ID =
3464373979
ISAKMP:(1002):SA 페이로드를 처리하는 중입니다.메시지 ID =
3464373979
ISAKMP:(1002):IPSec 제안 확인 1
ISAKMP:변형 1, ESP_3DES
ISAKMP: 변환의 속성:
ISAKMP: encaps는 2입니다(전송).
ISAKMP: SA 수명 유형(초)
ISAKMP: SA 수명(기본) 3600
ISAKMP: SA 수명 유형(킬로바이트)
ISAKMP: 0x0 0x46 0x50 0x0의 SA 수명(VPI)
ISAKMP: 인증자는 HMAC-SHA입니다.
ISAKMP:(1002):att는 허용됩니다.

허브는 IPSec 제안이 있는 첫 번째 QM(빠른 모드) 패킷을 수신합니다 .수신된 속성은 다음을 지정합니다 .encaps 플래그는 2(전송 모드, 1의 플래그는 터널 모드), 기본 SA 수명 3600초 및 4608000킬로바이트(16진수 0x465000), 인증을 위한 HMAC-SHA, 암호화를 위한 3DES로 설정됩니다.로컬 컨피그레이션에서 설정된 특성이 동일하므로 제안서가 수락되고 IPSec SA의 셸이 생성됩니다.아직 SPI(Security Parameter Index) 값이 연결되어 있지 않으므로 이는 아직 트래픽을 전달하는 데 사용할 수 없는 SA의 셸에 불과합니다.

IPSEC(validate_proposal_request):제안부 #1
IPSEC(validate_proposal_request):제안 부분 #1
(key eng.메시지) INBOUND local= 172.16.10.1:0, remote= 172.16.
local_proxy= 172.16.10.1/255.255.255.255/47/0(type=1),
remote_proxy= 172.16.1.1/255.255.255.255/47/0(type=1),
protocol= ESP, transform= NONE(전송),
lighdur= 0s 및 0kb
spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x0

이는 정상적으로 작동한다고 말하는 일반적인 IPSec 서비스 메시지입니다.

IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1):연결 조회에서 0을
습니다.
IPSEC-IFC MGRE/Tu0:crypto_ss_listen_start가 이미 수신 대기 중입
IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1):프로파일 DMVPN-
IPSEC을 사용하여 소켓 열기
IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1):연결 조회에서 0을
습니다.
IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1):즉시 터널을 트리거
.
IPSEC-IFC MGRE/Tu0:공유 목록에 Tunnel0 터널 인터페이스 추가
IPSEC-IFC
MGRE/Tu0(172.16.10.1/172.16.1.1):tunnel_protection_start_pending
8C93888
IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1):수신 대기 요청

IP 프로토콜 47(GRE)에 대해 172.16.10.1(허브 공용 주소)에서 172.16.1.1(스포크 공용 주소)까지 의사 암호화 맵 엔트리가 생성됩니다. IPSec SA/SPI는 승인된 제안의 값을 사용하여 인바운드 및 아웃바운드 트래픽 모두에 대해 생성됩니다.

mapdb AVL에 맵을 삽입하지 못했습니다. map + ace 쌍이 mapdb에
있습니다.
CRYPTO_SS(터널 초):수동 열기, 소켓 정보:로컬 172.16.10.1
172.16.10.1/255.255.255.255/0, 원격 172.16.1.1
172.16.1.1/255.255.255.255/0, 포트 47, ifc Tu0
Crypto mapdb:프록시_일치
소스 주소:172.16.10.1
dst 주소:172.16.1.1
프로토콜:47
소스 포트:0
dst 포트:0
ISAKMP:(1002):NONCE 페이로드를 처리하는 중입니다.메시지 ID =
3464373979
ISAKMP:(1002):처리 ID 페이로드입니다.메시지 ID = 3464373979
ISAKMP:(1002):처리 ID 페이로드입니다.메시지 ID = 3464373979
ISAKMP:(1002):QM 응답자가 spi를 가져옵니다.
ISAKMP:(1002):Node 3464373979, Input = IKE_MESG_FROM_PEE
IKE_QM_EXCH
ISAKMP:(1002):이전 상태 = IKE_QM_READY 새 상태 =
IKE_QM_SPI_STARVE
ISAKMP:(1002):IPSec SA 생성
172.16.1.1에서 172.16.10.1(f/i) 0/0으로 인바운드 SA
(프록시 172.16.1.1~172.16.10.1)
spi 0xDD2AC2B3 및 conn_id 0이 있습니다.
3600초 수명
수명 4608000킬로바이트
아웃바운드 SA(172.16.10.1~172.16.1.1(f/i) 0/0
(프록시 172.16.10.1~172.16.1.1)
spi 0x82C3E0C4 및 conn_id 0이 있습니다.
3600초 수명
수명 4608000킬로바이트

허브에서 보낸 두 번째 QM 메시지입니다.터널 보호가 Tunnel0에서 가동 중임을 확인하는 IPSec 서비스에 의해 생성된 메시지입니다.
대상 IP, SPI, 변형 집합 특성, 수명(킬로바이트 및 초 단위)이 남은 또 다른 SA 생성 메시지가 표시됩니다.

ISAKMP:(1002):172.16.1.1 my_port 500 peer_port 500(R) QM_IDLE
킷 전송
ISAKMP:(1002):IKE IPv4 패킷 전송
ISAKMP:(1002):Node 3464373979, Input = IKE_MESG_INTERNAL,
IKE_GOT_SPI
ISAKMP:(1002):이전 상태 = IKE_QM_SPI_STARVE 새 상태 =
IKE_QM_R_QM2
CRYPTO_SS(터널 초):응용 프로그램을 소켓에 바인딩했습니다.
IPSEC(key_engine):1개의 KMI 메시지가 있는 큐 이벤트를 받았습니
Crypto mapdb:프록시_일치
소스 주소:172.16.10.1
dst 주소:172.16.1.1
프로토콜:47
소스 포트:0
dst 포트:0
IPSEC(crypto_ipsec_sa_find_ident_head):동일한 프록시 및 피어
172.16.1.1과 다시 연결
IPSEC(policy_db_add_ident):src 172.16.10.1, dest 172.16.1.1, dest_

IPSEC(create_sa):생성됨
(sa) sa_dest= 172.16.10.1, sa_proto= 50,
sa_spi= 0xDD2AC2B3(3710567091),
sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 3
sa_lifetime(k/sec)= (4536779/3600)
IPSEC(create_sa):생성됨
(sa) sa_dest= 172.16.1.1, sa_proto= 50,
sa_spi= 0x82C3E0C4(2193875140),
sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 4
sa_lifetime(k/sec)= (4536779/3600)
IPSEC(crypto_ipsec_update_ident_tunnel_decap_oce):tunnel0 ident
8B6A0E8 with tun_decap_oce 6A648F0 업데이트
IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1):연결 조회가 8C938
반환했습니다.
IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1):소켓 준비 메시지
IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1):연결 조회가 8C938
반환했습니다.
IPSEC-IFC
MGRE/Tu0(172.16.10.1/172.16.1.1):tunnel_protection_socket_up
IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1):신호 NHRP
IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1):MTU 메시지 mtu 14
받았습니다.
IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1):연결 조회가 8C938
반환했습니다.
ISAKMP(1002):172.16.10.1 dport 500 sport 500 global(I) QM_IDLE
킷을 받았습니다.
ISAKMP:(1002):HASH 페이로드를 처리하는 중입니다.메시지 ID =
3464373979
ISAKMP:(1002):SA 페이로드를 처리하는 중입니다.메시지 ID =
3464373979
ISAKMP:(1002):IPSec 제안 확인 1
ISAKMP:변형 1, ESP_3DES
ISAKMP: 변환의 속성:
ISAKMP: encaps는 2입니다(전송).

ISAKMP: SA 수명 유형(초)
ISAKMP: SA 수명(기본) 3600
ISAKMP: SA 수명 유형(킬로바이트)
ISAKMP: 0x0 0x46 0x50 0x0의 SA 수명(VPI)
ISAKMP: 인증자는 HMAC-SHA입니다.
ISAKMP:(1002):att는 허용됩니다.
IPSEC(validate_proposal_request):제안부 #1
IPSEC(validate_proposal_request):제안 부분 #1
(key eng.메시지) INBOUND local= 172.16.1.1:0, remote= 172.16.1
local_proxy= 172.16.1.1/255.255.255.255/47/0(type=1),
remote_proxy= 172.16.10.1/255.255.255.255/47/0(type=1),
protocol= ESP, transform= NONE(전송),
lighdur= 0s 및 0kb
spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x0
Crypto mapdb:프록시_일치
소스 주소:172.16.1.1
dst 주소:172.16.10.1
프로토콜:47
소스 포트:0
dst 포트:0
ISAKMP:(1002):NONCE 페이로드를 처리하는 중입니다.메시지 ID =
3464373979
ISAKMP:(1002):처리 ID 페이로드입니다.메시지 ID = 3464373979
ISAKMP:(1002):처리 ID 페이로드입니다.메시지 ID = 3464373979
ISAKMP:(1002):IPSec SA 생성
172.16.10.1에서 172.16.1.1(f/i) 0/0으로 인바운드 SA
(프록시 172.16.10.1~172.16.1.1)
spi 0x82C3E0C4 및 conn_id 0이 있습니다.
3600초 수명
수명 4608000킬로바이트
아웃바운드 SA(172.16.1.1~172.16.10.1(f/i) 0/0
(프록시 172.16.1.1~172.16.10.1)
spi 0xDD2AC2B3 및 conn_id 0이 있습니다.
3600초 수명
수명 4608000킬로바이트
ISAKMP:(1002):172.16.10.1 my_port 500 peer_port 500(I) QM_IDLE
킷 전송
ISAKMP:(1002):IKE IPv4 패킷 전송
ISAKMP:(1002):노드 삭제 -830593317 오류 "오류 없음" 오류
ISAKMP:(1002):Node 3464373979, Input = IKE_MESG_FROM_PEE
IKE_QM_EXCH
ISAKMP:(1002):이전 상태 = IKE_QM_I_QM1 새 상태 =
IKE_QM_PHASE2_COMPLETE
IPSEC(key_engine):1개의 KMI 메시지가 있는 큐 이벤트를 받았습니
Crypto mapdb:프록시_일치
소스 주소:172.16.1.1
dst 주소:172.16.10.1
프로토콜:47
소스 포트:0
dst 포트:0
IPSEC(crypto_ipsec_sa_find_ident_head):동일한 프록시 및 피어
172.16.10.1과 다시 연결
IPSEC(policy_db_add_ident):src 172.16.1.1, dest 172.16.10.1, dest_

IPSEC(create_sa):생성됨
(sa) sa_dest= 172.16.1.1, sa_proto= 50,
sa_spi= 0x82C3E0C4(2193875140),
sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 3
sa_lifetime(k/sec)= (4499172/3600)
IPSEC(create_sa):생성됨
(sa) sa_dest= 172.16.10.1, sa_proto= 50,
sa_spi= 0xDD2AC2B3(3710567091),
sa_trans= esp-3des esp-sha-hmac , sa_conn_id= 4
sa_lifetime(k/sec)= (4499172/3600)
IPSEC(update_current_outbound_sa):SPI DD2AC2B3에 대한 SA 피
172.16.10.1 현재 아웃바운드 sa 활성화
IPSEC(update_current_outbound_sa):피어 172.16.10.1 현재 아웃바
sa를 SPI DD2AC2B3에 업데이트
IPSEC(crypto_ipsec_update_ident_tunnel_decap_oce):tunnel0 ident
94F2740 updating with tun_decap_oce 794ED30
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1):연결 조회가 961D220
환했습니다.
IPSEC-IFC
GRE/Tu0(172.16.1.1/172.16.10.1):tunnel_protection_socket_up
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1):신호 NHRP
NHRP:NHS 10.1.1.254 Tunnel0 vrf 0 Cluster 0 Priority 0 ' '에서 'E'로
됨

IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1):연결 조회가 961D220
환했습니다.
NHRP:DEST 10.1.1.254을 통해 패킷을 전송하려고 시도하는 중
ISAKMP(1002):172.16.1.1 dport 500 sport 500 global(R) QM_IDLE에
킷을 받았습니다.
ISAKMP:(1002):노드 삭제 -830593317 오류 "QM 완료(대기)" 오류
ISAKMP:(1002):Node 3464373979, Input = IKE_MESG_FROM_PEE
IKE_QM_EXCH
ISAKMP:(1002):이전 상태 = IKE_QM_R_QM2 새 상태 =
IKE_QM_PHASE2_COMPLETE
IPSEC(key_engine):1개의 KMI 메시지가 있는 큐 이벤트를 받았습니
IPSEC(key_engine_enable_outbound):ISAKMP에서 알림을 사용하도
rec
IPSEC(key_engine_enable_outbound):spi 2193875140/50과 함께 SA
화
IPSEC(update_current_outbound_sa):SPI 82C3E0C4에 대한 현재 아
운드 sa172.16.1.1 SA 피어 활성화
IPSEC(update_current_outbound_sa):피어 172.16.1.1 현재 아웃바운
sa를 SPI 82C3E0C4로 업데이트함

NHRP:Tunnel0 vrf 0을 통해 등록 요청 전송, 패킷 크기:108
소스:10.1.1.1, dst:10.1.1.254
(F) 후:IPv4(1), 유형:IP(800), hop:255, 버전:1
shtl:4(NSAP), sstl:0(NSAP)
pktsz:108파운드:52
(M) 플래그:"unique nat", reqid:65540
src NBMA:172.16.1.1
소스 프로토콜:10.1.1.1, dst 프로토콜:10.1.1.254

이 최종 QM 메시지는 빠른 모드가 완료되었으며 IPSec이 터널의 양쪽에서 작동함을 확인합니다.
각 피어가 모든 상태(MM1~MM6/P1_COMPLETE)를 통과하는 ISAKMP와 달리 IPSec은 6개가 아닌 3개의 메시지만 있기 때문에 약간 다릅니다.Responder(이 경우 IKE_QM_R_QM1 메시지의 "R"에 표시되는 허브)는 QM_READY, QM_SPI_STARVE, QM_R_QM2, QM_PHASE2_COMPLETE로 이동합니다.개시자(스포크)는 QM_READY에서 QM_I_QM1로 직접 이동하여 QM_PHASE2_COMPLETE로 이동합니다.

(C-1) 코드:오류 없음(0)
접두사:32, mtu:17912, hd_time:7200
addr_len:0(NSAP), 하위 addr_len:0(NSAP), proto_len:0, 이전:0
응답자 주소 확장(3):
전송 NHS 레코드 내선 번호(4):
역방향 전송 NHS 레코드 확장(5):
인증 확장(7):
유형:일반 텍스트(1), 데이터&콜론;NHRPAUTH
NAT 주소 확장(9):
(C-1) 코드:오류 없음(0)
접두사:32, mtu:17912, hd_time:0
addr_len:4(NSAP), 하위 addr_len:0(NSAP), proto_len:4, 이전:0
클라이언트 NBMA:172.16.10.1
클라이언트 프로토콜:10.1.1.254
NHRP-속도:10.1.1.254에 대한 초기 등록 요청 전송, 요청 65540
%LINK-3-업다운:Interface Tunnel0, 상태가 up으로 변경됨
NHRP:if_up:Tunnel0 proto 0
NHRP:터널0:대상 10.1.1.254/32 next-hop 10.1.1.254의 캐시 업데이
172.16.10.1
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1):연결 조회가 961D220
환했습니다.
NHRP:DEST 10.1.1.254을 통해 패킷을 전송하려고 시도하는 중
IPSEC-IFC GRE/Tu0:터널 시작
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1):연결 조회가 961D220
환했습니다.
IPSEC-IFC GRE/Tu0:crypto_ss_listen_start가 이미 수신 대기 중입니
IPSEC-IFC GRE/Tu0:crypto_ss_listen_start가 이미 수신 대기 중입니
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1):프로파일 DMVPN-IPS
사용하여 소켓 열기
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1):연결 조회가 961D220
환했습니다.
IPSEC-IFC GRE/Tu0(172.16.1.1/172.16.10.1):소켓이 이미 열려 있습
.무시합니다.
%LINEPROTO-5-업다운:Interface Tunnel0의 회선 프로토콜, 상태가
로 변경됨
NHRP:Tunnel0 vrf 0을 통한 등록 요청 수신, 패킷 크기:108
(F) 후:IPv4(1), 유형:IP(800), hop:255, 버전:1
shtl:4(NSAP), sstl:0(NSAP)
pktsz:108파운드:52
(M) 플래그:"unique nat", reqid:65540
src NBMA:172.16.1.1
소스 프로토콜:10.1.1.1, dst 프로토콜:10.1.1.254
(C-1) 코드:오류 없음(0)
접두사:32, mtu:17912, hd_time:7200
addr_len:0(NSAP), 하위 addr_len:0(NSAP), proto_len:0, 이전:0
응답자 주소 확장(3):
전송 NHS 레코드 내선 번호(4):
역방향 전송 NHS 레코드 확장(5):
인증 확장(7):
유형:일반 텍스트(1), 데이터&콜론;NHRPAUTH
NAT 주소 확장(9):
(C-1) 코드:오류 없음(0)
접두사:32, mtu:17912, hd_time:0

NHS(허브)에 등록하기 위해 스포크에서 받은 NHRP 등록 요청입니다. 스포크가 "등록 응답"을 수신할 때까지 NHS에 등록을 계속 시도하므로 이러한 결과의 배수를 보는 것은 정상입니다.

src NBMA:이 패킷을 전송하고 NHS에 등록하려고 시도하는 스포크의 NBMA(인터넷) 주소

src 프로토콜:등록을 시도하는 스포크의 터널 주소

dst 프로토콜:NHS/허브의 터널 주소

인증 확장, 데이터 및 콜론;NHRP 인증 문자열

클라이언트 NBMA:NHS/허브의 NBMA 주소

클라이언트 프로토콜:NHS/허브의 터널 주소

addr_len:4(NSAP), 하위 addr_len:0(NSAP), proto_len:4, 이전:0
클라이언트 NBMA:172.16.10.1
클라이언트 프로토콜:10.1.1.254

NHRP 디버그 패킷 추가 대상 네트워크 10.1.1.1/32은 172.16.1.1의 NHRP에서 10.1.1.1의 next hop을 통해 사용 가능합니다. 172.16.1.1은 허브가 멀티캐스트 트래픽을 포워딩하는 주소 목록에도 추가됩니다.

NHRP:netid_in = 1, to_us = 1
NHRP:터널0:대상 10.1.1.1/32 next-hop 10.1.1.1 캐시 추가 172.16.1.1
NHRP:터널 엔드포인트 추가(VPN:10.1.1.1, NBMA:172.16.1.1)
NHRP:터널 엔드포인트에 대한 NHRP 하위 블록을 연결했습니다 (VPN:10.1.1.1, NBMA:172.16.1.1)

이러한 메시지는 스포크 터널 주소에 대한 해결과 마찬가지로 등록이 성공했음을 확인합니다.

NHRP:캐시에 대한 하위 블록 노드를 삽입했습니다.캐시에 대한 대상
된 하위 블록 노드:대상 10.1.1.1/32nhop 10.1.1.1
NHRP:10.1.1.1/32 인터페이스 Tunnel0의 내부 동적 캐시 항목을 외부
환
NHRP:Tu0:동적 멀티캐스트 매핑 NBMA 생성:172.16.1.1
NHRP:NBMA에 대한 동적 멀티캐스트 매핑 추가:172.16.1.1
NHRP:NBMA로 캐시 업데이트:172.16.10.1, NBMA_ALT:172.16.10.
NHRP:새 필수 길이:32
NHRP:DEST 10.1.1.1을 통해 패킷을 전송하려고 시도하는 중
NHRP:NHRP가 NBMA 172.16.1.1으로 10.1.1.1으로 성공적으로 확인
NHRP:캡슐화에 성공했습니다. 터널 IP 주소 172.16.1.1

앞서 받은 "NHRP 등록 요청"에 대한 응답으로 허브가 스포크로 보낸 NHRP 등록 회신입니다.다른 등록 패킷과 마찬가지로 허브는 여러 요청에 대한 응답으로 이러한 패킷의 배수를 전송합니다.

src,dst:터널 소스(허브) 및 대상(스포크) IP 주소.라우터에서 전송하는 GRE 패킷의 소스 및 목적지입니다.

src NBMA:스포크의 NBMA(인터넷) 주소

src 프로토콜:등록을 시도하는 스포크의 터널 주소

dst 프로토콜:NHS/허브의 터널 주소

클라이언트 NBMA:NHS/허브의 NBMA 주소

클라이언트 프로토콜:NHS/허브의 터널 주소

인증 확장, 데이터 및 콜론;NHRP 인증 문자열

NHRP:Tunnel0 vrf 0을 통해 등록 응답 전송, 패킷 크기:128
소스:10.1.1.254, dst:10.1.1.1
(F) 후:IPv4(1), 유형:IP(800), hop:255, 버전:1
shtl:4(NSAP), sstl:0(NSAP)
pktsz:128파운드:52
(M) 플래그:"unique nat", reqid:65540
src NBMA:172.16.1.1
소스 프로토콜:10.1.1.1, dst 프로토콜:10.1.1.254
(C-1) 코드:오류 없음(0)
접두사:32, mtu:17912, hd_time:7200
addr_len:0(NSAP), 하위 addr_len:0(NSAP), proto_len:0, 이전:0
응답자 주소 확장(3):
(C) 코드:오류 없음(0)
접두사:32, mtu:17912, hd_time:7200
addr_len:4(NSAP), 하위 addr_len:0(NSAP), proto_len:4, 이전:0
클라이언트 NBMA:172.16.10.1
클라이언트 프로토콜:10.1.1.254
전송 NHS 레코드 내선 번호(4):
역방향 전송 NHS 레코드 확장(5):
인증 확장(7):
유형:일반 텍스트(1), 데이터&콜론;NHRPAUTH
NAT 주소 확장(9):
(C-1) 코드:오류 없음(0)
접두사:32, mtu:17912, hd_time:0
addr_len:4(NSAP), 하위 addr_len:0(NSAP), proto_len:4, 이전:0
클라이언트 NBMA:172.16.10.1
클라이언트 프로토콜:10.1.1.254
NHRP:Tunnel0 vrf 0을 통한 등록 응답 수신, 패킷 크기:128
(F) 후:IPv4(1), 유형:IP(800), hop:255, 버전:1
shtl:4(NSAP), sstl:0(NSAP)
pktsz:128파운드:52
(M) 플래그:"unique nat", reqid:65541
src NBMA:172.16.1.1

	소스 프로토콜:10.1.1.1, dst 프로토콜:10.1.1.254 (C-1) 코드:오류 없음(0) 접두사:32, mtu:17912, hd_time:7200 addr_len:0(NSAP), 하위 addr_len:0(NSAP), proto_len:0, 이전:0 응답자 주소 확장(3): (C) 코드:오류 없음(0) 접두사:32, mtu:17912, hd_time:7200 addr_len:4(NSAP), 하위 addr_len:0(NSAP), proto_len:4, 이전:0 **클라이언트 NBMA:172.16.10.1** **클라이언트 프로토콜:10.1.1.254** 전송 NHS 레코드 내선 번호(4): 역방향 전송 NHS 레코드 확장(5): **인증 확장(7):** **유형:일반 텍스트(1), 데이터&콜론;NHRPAUTH** NAT 주소 확장(9): (C-1) 코드:오류 없음(0) 접두사:32, mtu:17912, hd_time:0 addr_len:4(NSAP), 하위 addr_len:0(NSAP), proto_len:4, 이전:0 **클라이언트 NBMA:172.16.10.1** **클라이언트 프로토콜:10.1.1.254** NHRP:netid_in = 0, to_us = 1
더 일반적인 IPSec 서비스 메시지는 제대로 작동한다고 말합니다.	IPSEC-IFC MGRE/Tu0:crypto_ss_listen_start가 이미 수신 대기 중입 IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1):프로파일 DMVPN- IPSEC을 사용하여 소켓 열기 IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1):연결 조회가 8C938 반환했습니다. IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1):소켓이 이미 열려 있 다.무시합니다. IPSEC-IFC MGRE/Tu0(172.16.10.1/172.16.1.1):tunnel_protection_stop_pending 8C93888 NHRP:NHS-UP:10.1.1.254
EIGRP 인접성이 10.1.1.1에서 인접 디바이스 스포크와 함께 작동함을 나타내는 시스템 메시지입니다.	%DUAL-5-NBRCHANGE:EIGRP-IPv4 1:인접 디바이스 10.1.1.1(Tunnel0)이 작동 중입니다.새로운 인접성 %DUAL-5-NBRCHANGE:EIGRP-IPv4 1:인접 디바이스 10.1.1.254(Tunnel0)이 작동 중입니다.새로운 인접성
성공적인 NHRP 확인을 확인하는 시스템 메시지입니다.	NHRP:NHRP가 NBMA 172.16.1.1으로 10.1.1.1으로 성공적으로 확인

기능 확인 및 문제 해결

이 섹션에는 허브 및 스포크의 문제를 해결하는 데 사용되는 가장 유용한 **show** 명령 중 몇 가지가 있습니다.특정 디버그를 활성화하려면 다음 디버그 조건을 사용합니다.

- 디버그 dmvpn 조건 피어 nbma *NBMA_ADDRESS*
- 디버그 dmvpn 조건 피어 터널 *TUNNEL_ADDRESS*
- 디버그 암호화 조건 피어 ipv4 NBMA_*ADDRESS*

암호화 소켓 표시

```
Spoke1#show crypto sockets

Number of Crypto Socket connections 1

Tu0 Peers (local/remote): 172.16.1.1/172.16.10.1
Local Ident (addr/mask/port/prot): (172.16.1.1/255.255.255.255/0/47)
Remote Ident (addr/mask/port/prot): (172.16.10.1/255.255.255.255/0/47)
IPSec Profile: "DMVPN-IPSEC"
Socket State: Open
Client: "TUNNEL SEC" (Client State: Active)

Crypto Sockets in Listen state:
Client: "TUNNEL SEC" Profile: "DMVPN-IPSEC" Map-name: "Tunnel0-head-0"

Hub#show crypto sockets

Number of Crypto Socket connections 1

Tu0 Peers (local/remote): 172.16.10.1/172.16.1.1
Local Ident (addr/mask/port/prot): (172.16.10.1/255.255.255.255/0/47)
Remote Ident (addr/mask/port/prot): (172.16.1.1/255.255.255.255/0/47)
IPSec Profile: "DMVPN-IPSEC"
Socket State: Open
Client: "TUNNEL SEC" (Client State: Active)

Crypto Sockets in Listen state:
Client: "TUNNEL SEC" Profile: "DMVPN-IPSEC" Map-name: "Tunnel0-head-0"
```

암호화 세션 세부 정보 표시

```
Spoke1#show crypto session detail
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

Interface: Tunnel0
Uptime: 00:01:01
Session status: UP-ACTIVE
Peer: 172.16.10.1 port 500 fvrf: (none) ivrf: (none)
Phase1_id: 172.16.10.1
Desc: (none)
IKEv1 SA: local 172.16.1.1/500 remote 172.16.10.1/500 Active
Capabilities:(none) connid:1001 lifetime:23:58:58
IPSEC FLOW: permit 47 host 172.16.1.1 host 172.16.10.1
Active SAs: 2, origin: crypto map
Inbound: #pkts dec'ed 25 drop 0 life (KB/Sec) 4596087/3538
Outbound: #pkts enc'ed 25 drop 3 life (KB/Sec) 4596087/3538

Hub#show crypto session detail
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

Interface: Tunnel0
```

```
Uptime: 00:01:47
Session status: UP-ACTIVE
Peer: 172.16.1.1 port 500 fvrf: (none)
ivrf: (none)
Phase1_id: 172.16.1.1
Desc: (none)
IKEv1 SA: local 172.16.10.1/500 remote 172.16.1.1/500 Active
Capabilities:(none) connid:1001 lifetime:23:58:12
IPSEC FLOW: permit 47 host 172.16.10.1 host 172.16.1.1
Active SAs: 2, origin: crypto map
Inbound: #pkts dec'ed 35 drop 0 life (KB/Sec) 4576682/3492
Outbound: #pkts enc'ed 35 drop 0 life (KB/Sec) 4576682/3492
```

crypto isakmp sa detail 표시

```
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.

1001 172.16.1.1 172.16.10.1 ACTIVE 3des sha psk 1 23:59:10
Engine-id:Conn-id = SW:1

IPv6 Crypto ISAKMP SA

Hub#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.

1001 172.16.10.1 172.16.1.1 ACTIVE 3des sha psk 1 23:58:20
Engine-id:Conn-id = SW:1

IPv6 Crypto ISAKMP SA
```

crypto ipsec sa detail 표시

```
Spoke1#show crypto ipsec sa detail
interface: Tunnel0
Crypto map tag: Tunnel0-head-0, local addr 172.16.1.1
protected vrf: (none)
local ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (172.16.10.1/255.255.255.255/47/0)
current_peer 172.16.10.1 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 24, #pkts encrypt: 24, #pkts digest: 24
#pkts decaps: 24, #pkts decrypt: 24, #pkts verify: 24
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#pkts no sa (send) 3, #pkts invalid sa (rcv) 0
#pkts encaps failed (send) 0, #pkts decaps failed (rcv) 0
#pkts invalid prot (recv) 0, #pkts verify failed: 0
#pkts invalid identity (recv) 0, #pkts invalid len (rcv) 0
```

```
#pkts replay rollover (send): 0, #pkts replay rollover (rcv) 0
##pkts replay failed (rcv): 0
#pkts internal err (send): 0, #pkts internal err (recv) 0

local crypto endpt.: 172.16.1.1, remote crypto endpt.: 172.16.10.1
path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
current outbound spi: 0xA259D71(170237297)
PFS (Y/N): N, DH group: none

inbound esp sas:
spi: 0x8D538D11(2371063057)
transform: esp-3des esp-sha-hmac ,
in use settings ={Transport,}
conn id: 1, flow_id: SW:1, sibling_flags 80000006,
crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4596087/3543)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE

inbound ah sas:
inbound pcp sas:
outbound esp sas:
spi: 0xA259D71(170237297)
transform: esp-3des esp-sha-hmac ,
in use settings ={Transport, }
conn id: 2, flow_id: SW:2, sibling_flags 80000006,
crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4596087/3543)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE
outbound ah sas:
outbound pcp sas:

Hub#show crypto ipsec sa detail
interface: Tunnel0
Crypto map tag: Tunnel0-head-0, local addr 172.16.10.1

protected vrf: (none)
local ident (addr/mask/prot/port): (172.16.10.1/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)
current_peer 172.16.1.1 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 34, #pkts encrypt: 34, #pkts digest: 34
#pkts decaps: 34, #pkts decrypt: 34, #pkts verify: 34
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#pkts no sa (send) 0, #pkts invalid sa (rcv) 0
#pkts encaps failed (send) 0, #pkts decaps failed (rcv) 0
#pkts invalid prot (recv) 0, #pkts verify failed: 0
#pkts invalid identity (recv) 0, #pkts invalid len (rcv) 0
#pkts replay rollover (send): 0, #pkts replay rollover (rcv) 0
##pkts replay failed (rcv): 0
#pkts internal err (send): 0, #pkts internal err (recv) 0

local crypto endpt.: 172.16.10.1, remote crypto endpt.: 172.16.1.1
path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
current outbound spi: 0x8D538D11(2371063057)
PFS (Y/N): N, DH group: none

inbound esp sas:
```

```
spi: 0xA259D71(170237297)
transform: esp-3des esp-sha-hmac ,
in use settings ={Transport, }
conn id: 1, flow_id: SW:1, sibling_flags 80000006,
crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4576682/3497)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas: spi: 0x8D538D11(2371063057)
transform: esp-3des esp-sha-hmac ,
in use settings ={Transport, }
conn id: 2, flow_id: SW:2, sibling_flags 80000006,
crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4576682/3497)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE

outbound ah sas:
outbound pcp sas:
```

ip nhrp 표시

```
Spoke1#show ip nhrp
10.1.1.254/32 via 10.1.1.254
Tunnel0 created 00:00:55, never expire
Type: static, Flags:
NBMA address: 172.16.10.1

Hub#show ip nhrp
10.1.1.1/32 via 10.1.1.1
Tunnel0 created 00:01:26, expire 01:58:33
Type: dynamic, Flags: unique registered
NBMA address: 172.16.1.1
```

ip nhs 표시

```
Spoke1#show ip nhrp nhs
Legend: E=Expecting replies, R=Responding, W=Waiting
Tunnel0:
10.1.1.254 RE priority = 0 cluster = 0

Hub#show ip nhrp nhs (As the hub is the only NHS for this DMVPN cloud,
it does not have any servers configured)
```

show dmvpn [detail]

```
"show dmvpn detail" returns the output of show ip nhrp nhs, show dmvpn,
and show crypto session detail

Spoke1#show dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
N - NATed, L - Local, X - No Socket
# Ent --> Number of NHRP entries with same NBMA peer
```

```
NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface: Tunnel0, IPv4 NHRP Details
Type:Spoke, NHRP Peers:1,

# Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb
----- --------------- --------------- ----- -------- -----
1 172.16.10.1 10.1.1.254 UP 00:00:39 S

Spoke1#show dmvpn detail
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
N - NATed, L - Local, X - No Socket
# Ent --> Number of NHRP entries with same NBMA peer
NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface Tunnel0 is up/up, Addr. is 10.1.1.1, VRF ""
Tunnel Src./Dest. addr: 172.16.1.1/172.16.10.1, Tunnel VRF ""
Protocol/Transport: "GRE/IP", Protect "DMVPN-IPSEC"
Interface State Control: Disabled

IPv4 NHS:
10.1.1.254 RE priority = 0 cluster = 0
Type:Spoke, Total NBMA Peers (v4/v6): 1

# Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb Target Network
----- --------------- --------------- ----- -------- ----- -----------------
1 172.16.10.1 10.1.1.254 UP 00:00:41 S 10.1.1.254/32


Crypto Session Details:
--------------------------------------------------------------------------------
Interface: Tunnel0
Session: [0x08D513D0]
IKEv1 SA: local 172.16.1.1/500 remote 172.16.10.1/500 Active
Capabilities:(none) connid:1001 lifetime:23:59:18
Crypto Session Status: UP-ACTIVE
fvrf: (none), Phase1_id: 172.16.10.1
IPSEC FLOW: permit 47 host 172.16.1.1 host 172.16.10.1
Active SAs: 2, origin: crypto map
Inbound: #pkts dec'ed 21 drop 0 life (KB/Sec) 4596088/3558
Outbound: #pkts enc'ed 21 drop 3 life (KB/Sec) 4596088/3558
Outbound SPI : 0x A259D71, transform : esp-3des esp-sha-hmac
Socket State: Open

Pending DMVPN Sessions:

Hub#show dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
N - NATed, L - Local, X - No Socket
# Ent --> Number of NHRP entries with same NBMA peer
NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface: Tunnel0, IPv4 NHRP Details Type:Hub, NHRP Peers:1,
# Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb
----- --------------- --------------- ----- -------- -----
1 172.16.1.1 10.1.1.1 UP 00:01:30 D
```

```
Hub#show dmvpn detail
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
N - NATed, L - Local, X - No Socket # Ent --> Number of NHRP entries with same NBMA peer NHS
Status: E --> Expecting Replies, R --> Responding, W --> Waiting UpDn Time --> Up or Down Time
for a Tunnel ==========================================================================
Interface Tunnel0 is up/up, Addr. is 10.1.1.254, VRF "" Tunnel Src./Dest. addr:
172.16.10.1/MGRE, Tunnel VRF "" Protocol/Transport: "multi-GRE/IP", Protect "DMVPN-IPSEC"
Interface State Control: Disabled Type:Hub, Total NBMA Peers (v4/v6): 1
# Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb Target Network ----- --------------- --
------------- ----- -------- ----- ----------------- 1 172.16.1.1 10.1.1.1 UP 00:01:32 D
10.1.1.1/32

Crypto Session Details:
-------------------------------------------------------------------------------- Interface:
Tunnel0
Session: [0x08A27858]
IKEv1 SA: local 172.16.10.1/500 remote 172.16.1.1/500 Active
Capabilities:(none) connid:1001 lifetime:23:58:26
Crypto Session Status: UP-ACTIVE
fvrf: (none), Phase1_id: 172.16.1.1
IPSEC FLOW: permit 47 host 172.16.10.1 host 172.16.1.1
Active SAs: 2, origin: crypto map
Inbound: #pkts dec'ed 32 drop 0 life (KB/Sec) 4576682/3507
Outbound: #pkts enc'ed 32 drop 0 life (KB/Sec) 4576682/3507
Outbound SPI : 0x8D538D11, transform : esp-3des esp-sha-hmac
Socket State: Open

Pending DMVPN Sessions:
```

관련 정보

- IPsec 문제 해결:디버그 명령 이해 및 사용
- 차세대 암호화
- RFC3706:IKE 데드 피어 탐지
- RFC3947:IKE NAT 통과
- 기술 지원 및 문서 – Cisco Systems