IPsec IKEv1 프로토콜 이해

목차

[소개](#)
[사전 요구 사항](#)
[요구 사항](#)
[사용되는 구성 요소](#)
[IPsec](#)
[IKE 프로토콜](#)
[IKE 단계](#)
[IKE 모드(1단계)](#)
[주 모드](#)
[적극적인 모드](#)
[IPsec 모드(2단계)](#)
[빠른 모드](#)
[IKE 용어집](#)
[기본 모드 패킷 교환](#)
[주 모드 1(MM1)](#)
[두 개의 동시 협상 식별](#)
[주 모드 2(MM2)](#)
[기본 모드 3 및 4(MM3-MM4)](#)
[기본 모드 5 및 6(MM5-MM6)](#)
[빠른 모드(QM1, QM2 및 QM3)](#)
[적극적인 모드 패킷 교환](#)
[주 모드와 적극적인 모드 비교](#)
[IKEv2와 IKEv1 패킷 교환](#)
[정책 기반 대 경로 기반](#)
[정책 기반 VPN](#)
[경로 기반 VPN](#)
[VPN을 통해 수신되지 않는 트래픽의 일반적인 문제](#)
[ISP가 UDP 500/4500을 차단함](#)
[ISP에서 ESP 차단](#)
[관련 정보](#)

소개

이 문서에서는 IKEv1 관련 IPsec(Internet Protocol Security) 문제에 대한 더 간단한 트러블슈팅을 위한 패킷 교환을 이해하기 위해 VPN(Virtual Private Network) 설정에 대한 IKEv1(Internet Key Exchange) 프로토콜 프로세스에 대해 설명합니다.

기고자: Amanda Nava, Cisco TAC 엔지니어

사전 요구 사항

요구 사항

Cisco에서는 다음과 같은 기본적인 보안 개념을 숙지하는 것이 좋습니다.

- 인증
- 기밀 유지
- 무결성
- IPsec

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 네트워크가 작동 중인 경우, 모든 명령의 잠재적인 영향을 이해해야 합니다.

IPsec

IPsec는 IP 레이어에서 인터넷 통신에 보안을 제공하는 프로토콜 모음입니다. IPsec의 가장 일반적인 사용 방법은 두 위치(게이트웨이 간) 간 또는 원격 사용자와 엔터프라이즈 네트워크(호스트 대 게이트웨이) 간에 VPN(Virtual Private Network)을 제공하는 것입니다.

IKE 프로토콜

IPsec은 IKE 프로토콜을 사용하여 보안 사이트 간 또는 원격 액세스 VPN(virtual private network) 터널을 협상하고 설정합니다. IKE 프로토콜은 ISAKMP(Internet Security Association and Key Management Protocol)라고도 합니다(Cisco에서만 해당).

IKE에는 두 가지 버전이 있습니다.

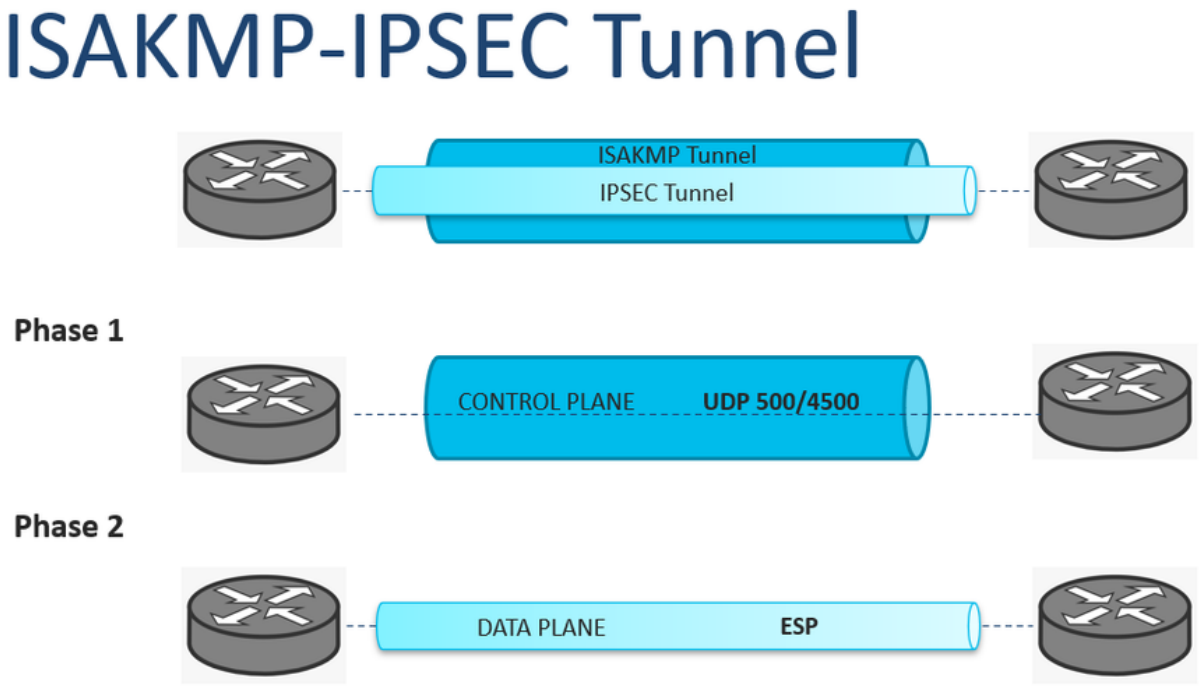
- IKEv1: RFC 2409에 정의, 인터넷 키 교환
- IKE 버전 2(IKEv2): RFC 4306, IKEv2(Internet Key Exchange) 프로토콜에 정의

IKE 단계

ISAKMP는 협상을 두 단계로 구분합니다.

- 1단계: 두 ISAKMP 피어는 ISAKMP 협상 메시지를 보호하는 보안 및 인증된 터널을 설정합니다. 이 터널을 ISAKMP SA라고 합니다. ISAKMP는 두 가지 모드를 정의합니다. 주 모드(MM) 및 적극적인 모드.
- 2단계: IPsec 터널을 통해 전송할 데이터의 암호화(SA)에 대한 키 자료와 알고리즘을 협상합니다. 이 단계를 빠른 모드라고 합니다.

모든 추상 개념을 구체화하기 위해 1단계 터널은 상위 터널이고 2단계는 하위 터널입니다. 이 그림에서는 두 단계를 터널로 보여 줍니다.



참고: ISAKMP(1단계) 터널은 두 게이트웨이 간의 제어 플레인 VPN 트래픽을 보호합니다. 컨트롤 플레인 트래픽은 협상 패킷, 정보 패키지, DPD, keepalive, rekey 등이 될 수 있습니다. ISAKMP 협상은 UDP 500 및 4500 포트를 사용하여 보안 채널을 설정합니다.

참고: IPsec(2단계) 터널은 두 게이트웨이 간에 VPN을 통과하는 데이터 플레인 트래픽을 보호합니다. T데이터를 보호하는 데 사용되는 알고리즘은 2단계에서 구성되며 1단계에서 지정한 알고리즘과 독립적입니다.
이러한 패킷을 캡슐화하고 암호화하는 데 사용되는 프로토콜은 ESP(Encapsulation Security Payload)입니다.

IKE 모드(1단계)

주 모드

IKE 세션은 개시자가 제안서 또는 제안을 응답자에게 보낼 때 시작됩니다. 노드 간 첫 번째 교환은 기본 보안 정책을 설정합니다. 이니시에이터는 사용할 암호화 및 인증 알고리즘을 제안합니다. 응답자는 적절한 제안을 선택하고(제안서를 선택한 것으로 가정) 개시자에게 전송합니다. 다음 교환은 Diffie-Hellman 공개 키와 기타 데이터를 전달합니다. 모든 추가 협상은 IKE SA 내에서 암호화됩니다. 세 번째 교환은 ISAKMP 세션을 인증합니다. IKE SA가 설정되면 IPSec 협상(빠른 모드)이 시작됩니다.

적극적인 모드

Aggressive Mode(적극적인 모드)는 IKE SA 협상을 3개의 패킷으로 압축하며, 개시자가 전달한 SA에 필요한 모든 데이터를 포함합니다. 응답자는 제안, 주요 자료 및 ID를 전송하고 다음 패킷에서 세션을 인증합니다. 개시자가 응답하고 세션을 인증합니다. 협상이 더 빨라지고 개시자 및 응답자 ID가 암호화되지 않습니다.

IPsec 모드(2단계)

빠른 모드

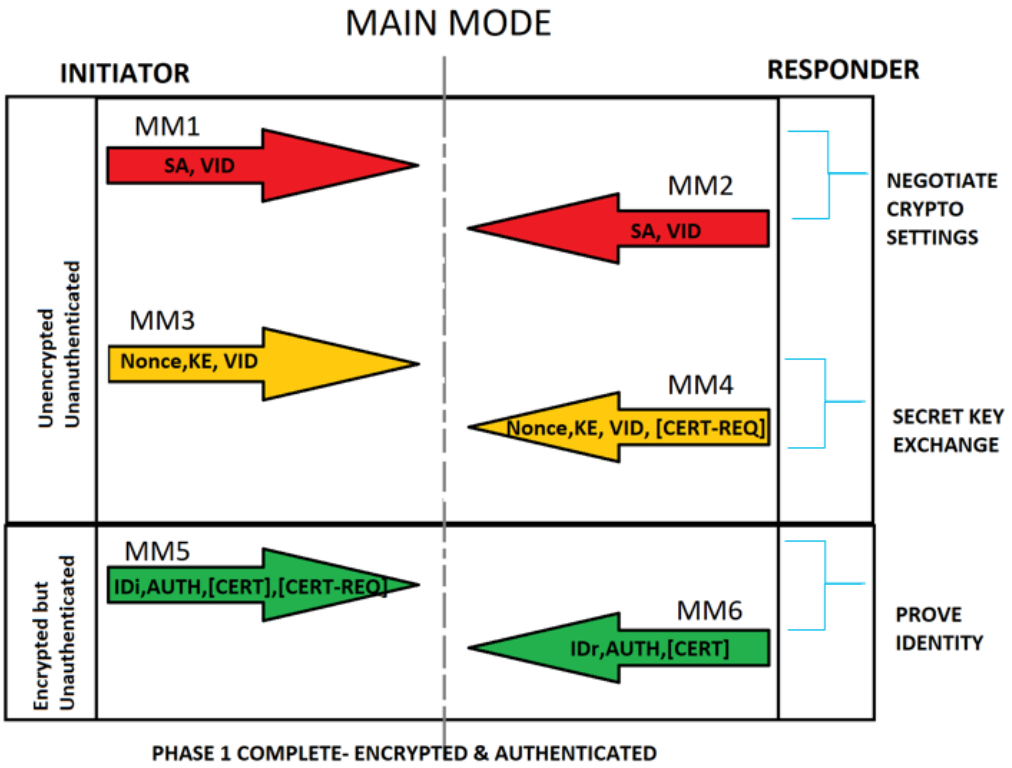
IPSec 협상 또는 빠른 모드는 협상을 제외하고 IKE SA 내에서 보호해야 하는 적극적인 모드 IKE 협상과 유사합니다. Quick Mode(빠른 모드)는 데이터 암호화를 위해 SA를 협상하고 해당 IPSec SA에 대한 키 교환을 관리합니다.

IKE 용어집

- SA(**Security Association**)는 보안 통신을 지원하기 위해 두 네트워크 엔터티 간의 공유 보안 특성을 설정하는 것입니다. SA에는 암호화 알고리즘 및 모드와 같은 특성이 포함됩니다. 트래픽 암호화 키 연결을 통해 전달되는 네트워크 데이터의 매개 변수입니다.
- **공급업체 ID**(**VID**)는 피어가 NAT-Traversal, Dead Peer Detection 기능, 프래그먼트화 등을 지원하는지 확인하기 위해 처리됩니다.
- **Nonce**: 임의 생성 번호. 이 nonce는 다른 항목과 함께 해시되고 합의된 키가 사용되며 다시 전송됩니다. 개시자는 쿠키와 nonce를 확인하고 올바른 nonce가 없는 메시지를 거부합니다. 이렇게 하면 임의로 생성된 nonce를 예측할 수 있는 제3자가 없으므로 재생이 방지됩니다.
- **DH**(**Diffie**-Hellman) 보안 키 교환 프로세스에 대한 **KE(Key-Exchange)** 정보
- **ID Initiator/responder(IDi/IDr)**는 피어로 인증 정보를 보내는 데 사용됩니다. 이 정보는 공통 공유 비밀을 보호하여 전송됩니다.
- **DH(Diffie-Hellman) 키 교환은 공용 채널을 통해 안전하게 암호화 알고리즘을 교환하는 방법입니다.**
- IPSec 공유 키는 PFS(**Perfect Forward Secrecy**) 또는 원래 DH 교환**을** 이전에 파생된 공유 암호로 새로 고침하는 데 다시 사용되는 DH로 파생될 수 있습니다.

기본 모드 패킷 교환

각 ISAKMP 패킷에는 터널 설정에 대한 페이로드 정보가 포함되어 있습니다. IKE 용어집에서는 이 이미지에 표시된 대로 기본 모드에서 패킷 교환에 대한 페이로드 콘텐츠의 일부로 IKE 약어를 설명합니다.

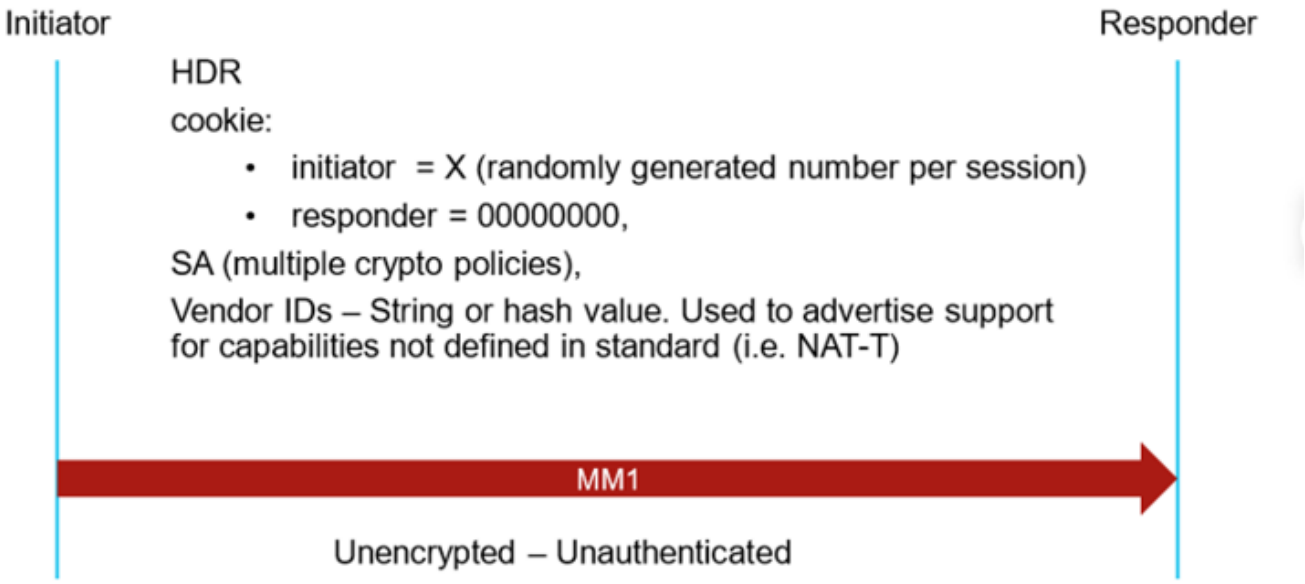


주 모드 1(MM1)

ISAKMP 협상 조건을 설정하려면 다음을 포함하는 ISAKMP 정책을 생성합니다.

- 피어의 ID를 확인하기 위한 인증 방법입니다.
- 데이터를 보호하고 개인 정보를 보호하기 위한 암호화 방법
- 발신자의 ID를 확인하고 메시지가 전송 중에 수정되지 않았는지 확인하는 HMAC(Hashed Message Authentication Codes) 방법.
- 암호화 키 결정 알고리즘의 강도를 결정하는 Diffie-Hellman 그룹입니다. 보안 어플라이언스는 이 알고리즘을 사용하여 암호화 및 해시 키를 파생합니다.
- 보안 어플라이언스가 대체되기 전에 암호화 키를 사용하는 시간 제한.

첫 번째 패킷은 이미지에 표시된 대로 IKE 협상의 개시자가 전송합니다.



참고: 기본 모드 1은 IKE 협상의 첫 번째 패킷입니다. 따라서 Responder SPI가 0으로 설정된 동안 Initiator SPI는 임의의 값으로 설정됩니다. 두 번째 패킷(MM2)에서 Responder SPI는 새 값으로 응답해야 하며 전체 협상이 동일한 SPI 값을 유지합니다.

MM1을 캡처하고 Wireshark 네트워크 프로토콜 분석기를 사용하는 경우 SPI 값은 이미지에 표시된 대로 Internet Security Association and Key Management Protocol(인터넷 보안 연결 및 키 관리 프로토콜) 콘텐츠 내에 있습니다.

```
> Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
> Internet Protocol Version 4, Src: 170.49.116.200, Dst: 209.134.162.150
> User Datagram Protocol, Src Port: 500, Dst Port: 500
v Internet Security Association and Key Management Protocol
    Initiator SPI: 6f80c0380ef6bdfd
    Responder SPI: 0000000000000000
    Next payload: Security Association (33)
```

참고: 이 경우 MM1 패킷이 경로에서 손실되거나 MM2 응답이 없는 경우 IKE 협상은 최대 재전송 수에 도달할 때까지 MM1 재전송을 유지합니다. 이 시점에서 개시자는 다음 협상이 다시 트리거될 때까지 동일한 SPI를 유지합니다.

팁: Initiator 및 Responder SPI를 식별하면 동일한 VPN에 대해 여러 협상을 식별하고 일부 협상 문제를 줄이는 데 매우 유용합니다.

두 개의 동시 협상 식별

Cisco IOS® XE 플랫폼에서는 구성된 원격 IP 주소에 대해 조건부로 디버그를 터널당 필터링할 수 있지만, 동시 협상이 로그에 표시되므로 이를 필터링할 방법이 없습니다. 수동으로 수행해야 합니다. 앞서 언급한 것처럼 전체 협상은 개시자와 응답자에 대해 동일한 SPI 값을 유지합니다. 동일한 피어 IP 주소에서 패킷을 수신하지만 협상이 최대 재전송 수에 도달하기 전에 추적된 이전 값과 SPI가 일치하지 않는 경우 이미지에 표시된 것과 동일한 피어에 대한 또 다른 협상입니다.

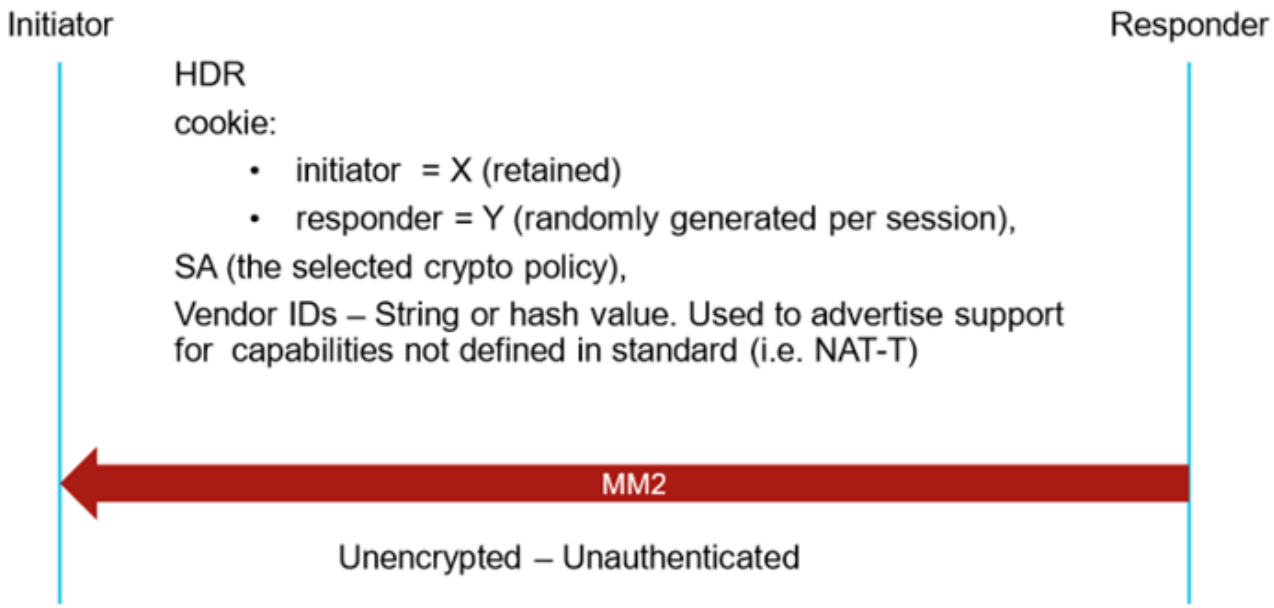
```
ISR4451
**********************************************
                2A8F14E40D648E28
*Apr 29 16:57:40.944: IKEv2:(SESSION ID = 27621,SA ID = 1):Sending Packet [To 198.19.252.1:500/From 10.11.6.2:500/VRF i0:f0]
Initiator SPI : 2A8F14E40D648E28 - Responder SPI : 0000000000000000 Message id: 0
IKEv2 IKE_SA_INIT Exchange REQUEST
Payload contents:
 SA KE N VID VID VID VID NOTIFY(NAT_DETECTION_SOURCE_IP) NOTIFY(NAT_DETECTION_DESTINATION_IP) NOTIFY(IKEV2_FRAGMENTATION_SUPPORTED) VID

*Apr 29 16:57:42.200: IPSEC:(SESSION ID = 27621) (key_engine) request timer fired: count = 1,
  (identity) local= 10.11.6.2:0, remote= 198.19.252.1:0,
    local_proxy= 0.0.0.0/0.0.0.0/256/0,
    remote_proxy= 0.0.0.0/0.0.0.0/256/0
*Apr 29 16:57:42.200: IPSEC(sa_request): ,
  (key eng. msg.) OUTBOUND local= 10.11.6.2:500, remote= 198.19.252.1:500,
    local_proxy= 0.0.0.0/0.0.0.0/256/0,
    remote_proxy= 0.0.0.0/0.0.0.0/256/0,
    protocol= ESP, transform= esp-aes 256 esp-sha-hmac  (Tunnel),
    lifedur= 28800s and 4294967295kb,
    spi= 0x0(0), conn_id= 0, keysize= 256, flags= 0x0
omr2-site1#
                5638222923EA3C5A
*Apr 29 16:57:53.763: IKEv2:Received Packet [From 198.19.252.1:500/To 10.11.6.2:500/VRF i0:f0]
Initiator SPI : 5638222923EA3C5A - Responder SPI : 0000000000000000 Message id: 0
IKEv2 IKE_SA_INIT Exchange REQUEST
Payload contents:
 SA KE N NOTIFY(NAT_DETECTION_SOURCE_IP) NOTIFY(NAT_DETECTION_DESTINATION_IP) NOTIFY(IKEV2_FRAGMENTATION_SUPPORTED) NOTIFY(Unknown - 16431) NOTIFY(REDIRECT_SUPPORTED)
```

참고: 이 예에서는 협상의 첫 번째 패킷(MM1)에 대한 동시 협상을 보여 주지만 이 협상은 어떤 협상 지점에서도 발생할 수 있습니다. 후속 패킷은 모두 responder SPI에서 0과 다른 값을 포함해야 합니다.

주 모드 2(MM2)

주 모드 2 패킷에서 응답자는 일치하는 제안서에 대해 선택한 정책을 전송하고 responder SPI는 임의의 값으로 설정됩니다. 전체 협상은 동일한 SPI 값을 유지합니다. MM2가 MM1에 응답하고 SPI 응답자는 이미지에 표시된 대로 0과 다른 값으로 설정됩니다.



MM2를 캡처하고 Wireshark 네트워크 프로토콜 분석기를 사용하는 경우 Initiator SPI 및 Responder SPI 값은 이미지에 표시된 대로 Internet Security Association 및 Key Management Protocol 콘텐츠 내에 있습니다.

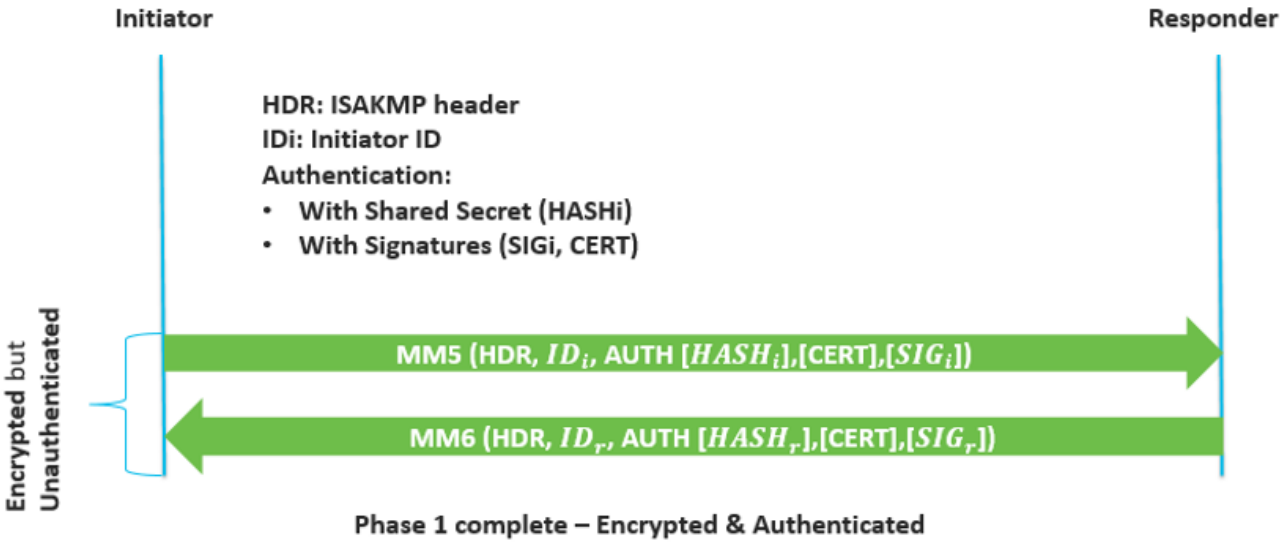
```
> Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
> Internet Protocol Version 4, Src: 209.134.162.150, Dst: 170.49.116.200
> User Datagram Protocol, Src Port: 500, Dst Port: 500
v Internet Security Association and Key Management Protocol
    Initiator SPI: 6f80c0380ef6bdfd
    Responder SPI: 2bc06438c94e88dc
    Next payload: Security Association (33)
```

기본 모드 3 및 4(MM3-MM4)

MM3 및 MM4 패킷은 여전히 암호화되지 않고 인증되지 않으며 비밀 키 교환이 이루어집니다. 이미지에 MM3 및 MM4가 표시됩니다.

기본 모드 5 및 6(MM5-MM6)

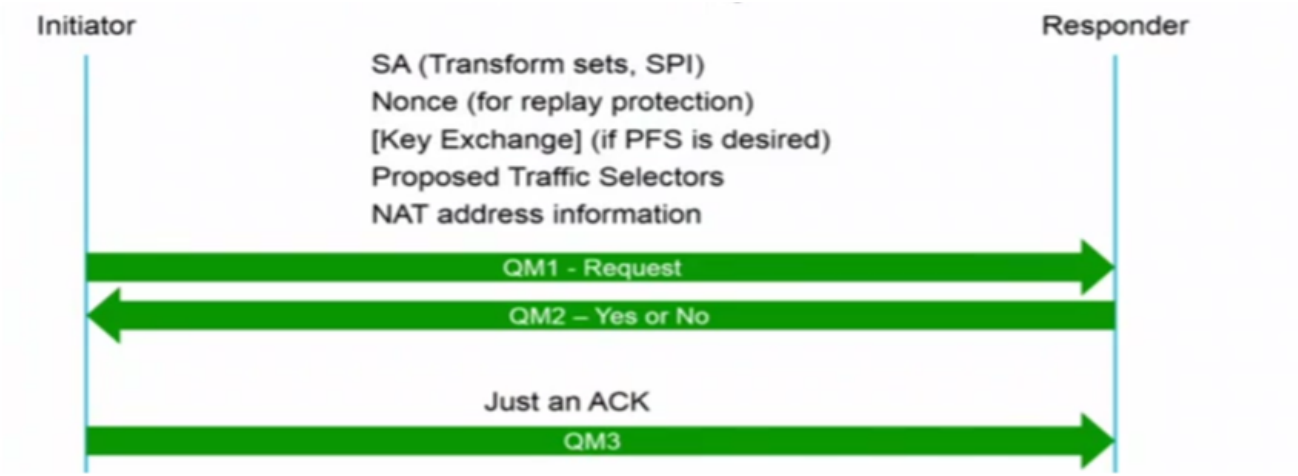
MM5 및 MM6 패킷은 이미 암호화되었지만 아직 인증되지 않았습니다. 이러한 패킷에서 인증은 이미지에 표시된 대로 수행됩니다.



빠른 모드(QM1, QM2 및 QM3)

빠른 모드는 기본 몽드와 IKE가 1단계에서 보안 터널을 설정한 후 발생합니다. 빠른 모드는 IPSec 보안 알고리즘에 대해 공유 IPSec 정책을 협상하고 IPSec SA 설정에 대한 키 교환을 관리합니다. 이 비전은 새 공유 비밀 키 자료를 생성하고 가짜 SA에서 생성된 재생 공격을 방지하는 데 사용됩니다.

이 단계에서는 이미지에 표시된 대로 3개의 패킷이 교환됩니다.

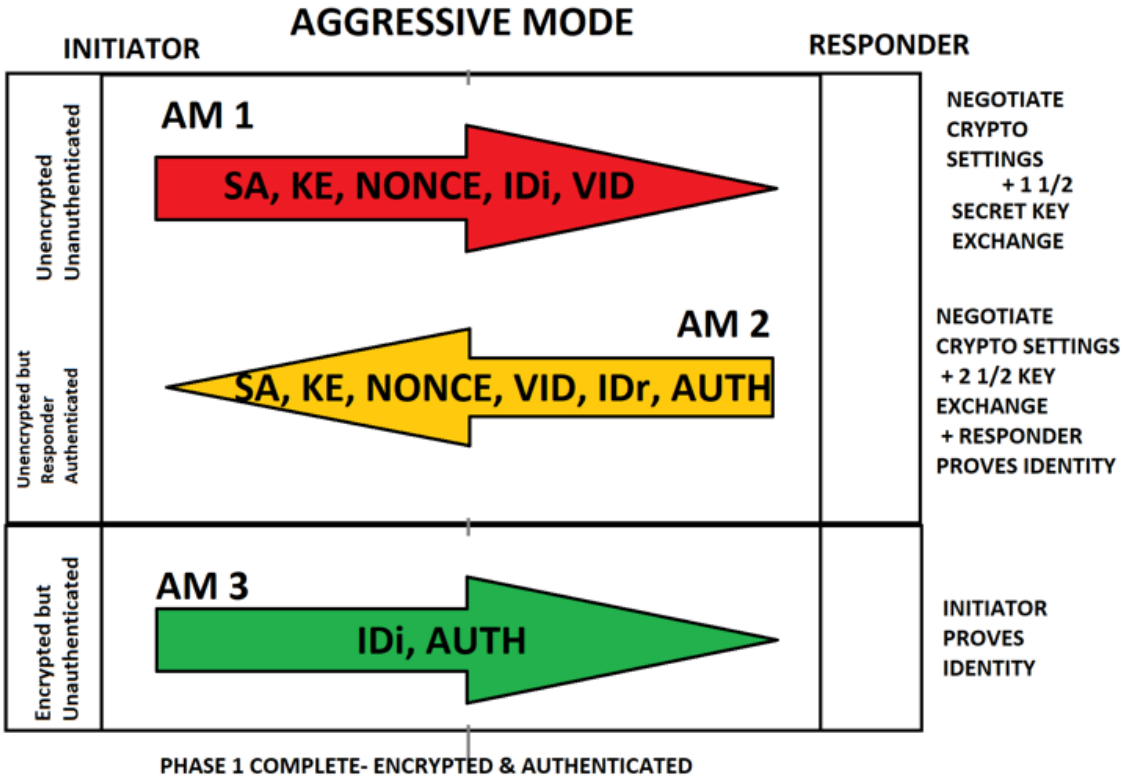


적극적인 모드 패킷 교환

Aggressive Mode(적극적인 모드)는 IKE SA 협상을 3개의 패킷으로 축소하며, 개시자가 전달한 SA에 필요한 모든 데이터를 포함합니다.

- 응답자는 제안, 주요 자료 및 ID를 전송하고 다음 패킷에서 세션을 인증합니다.
- 개시자가 응답하고 세션을 인증합니다.
- 협상이 더 빨라지고 개시자 및 응답자 ID가 암호화되지 않습니다.

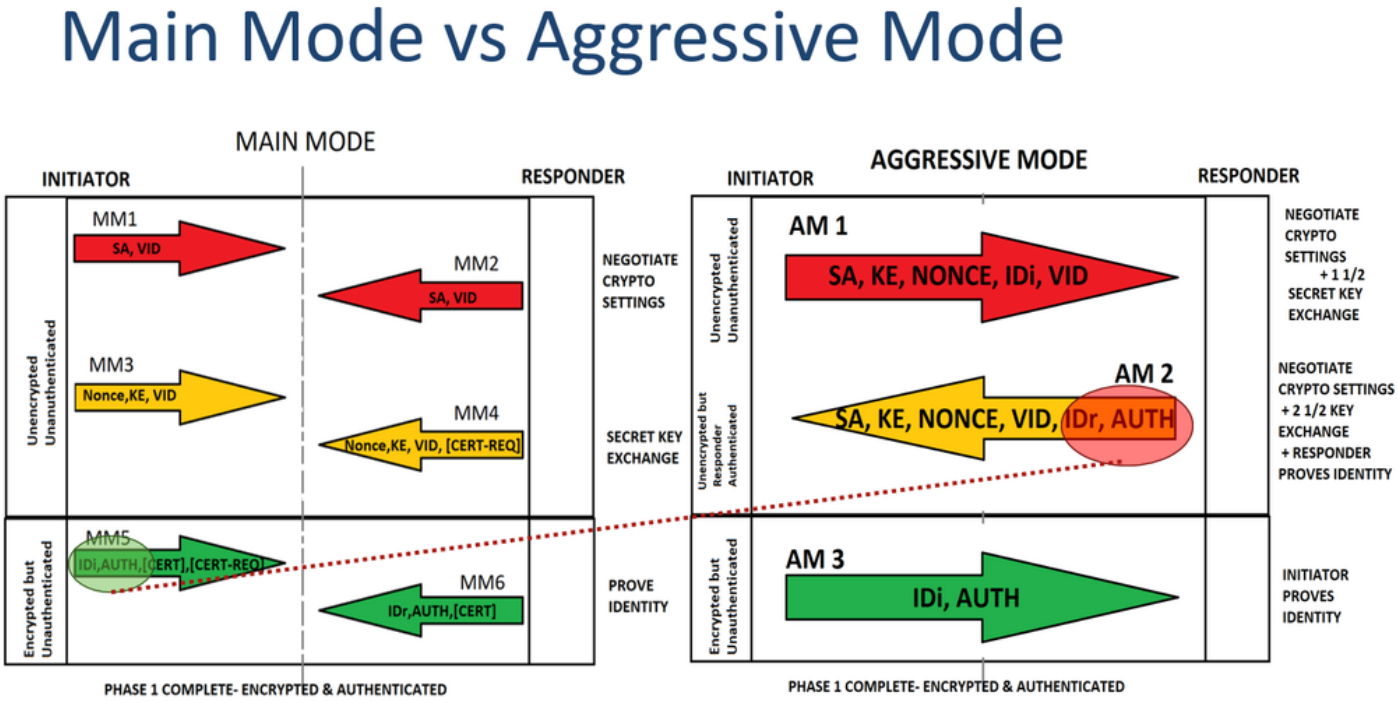
이 그림에서는 Aggressive 모드에서 교환된 세 패킷의 페이로드 내용을 보여줍니다.



주 모드와 적극적인 모드 비교

Aggressive Mode는 Main Mode와 비교하여 세 개의 패키지로 제공됩니다.

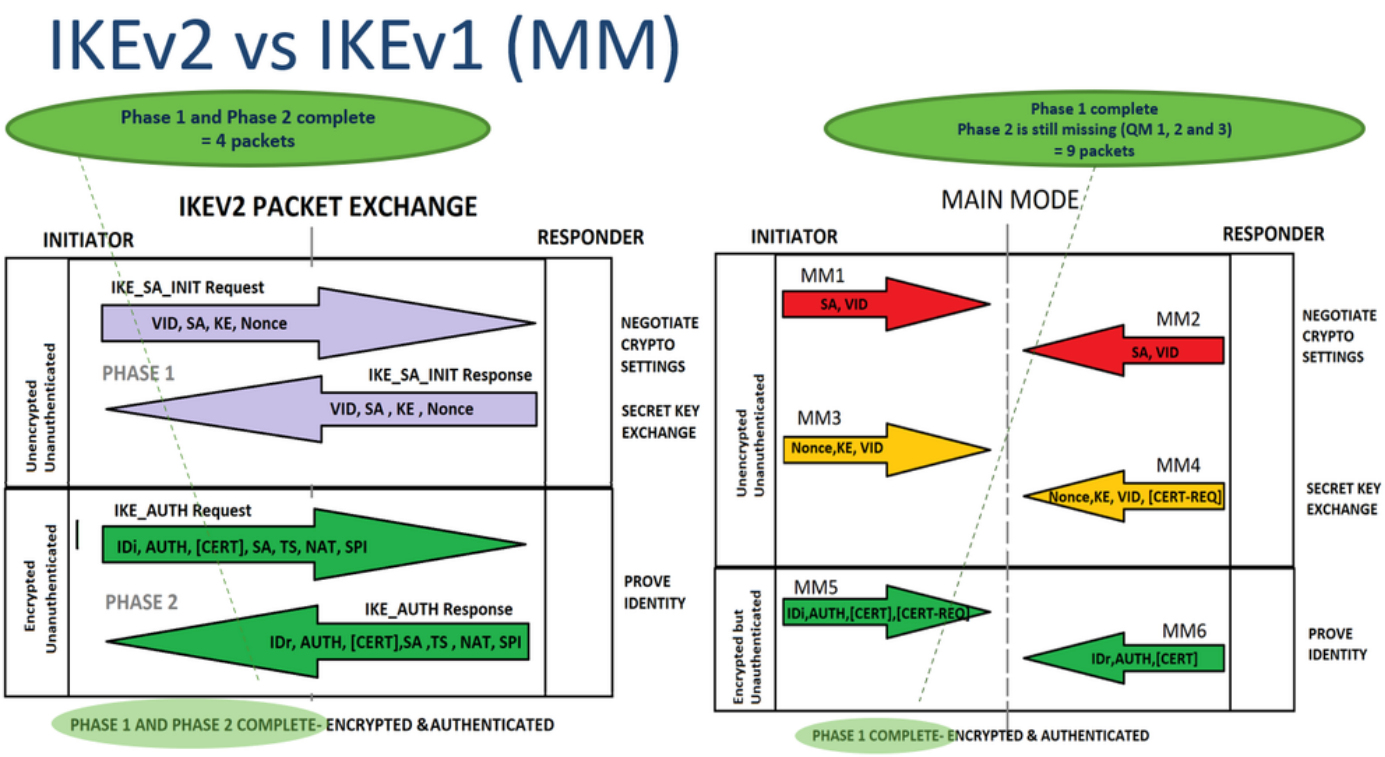
- AM 1은 MM1 및 MM3을 흡수합니다.
- AM 2는 MM2, MM4 및 MM6의 일부를 흡수합니다. 공격적 모드의 취약성은 여기에서 비롯됩니다. AM 2는 이 정보가 암호화되는 주 모드와 달리 암호화되지 않은 IDr 및 인증을 구성합니다.
- AM 3은 IDi 및 인증을 제공하며, 이러한 값은 암호화됩니다.



IKEv2와 IKEv1 패킷 교환

IKEv2 협상에서 터널을 설정하기 위해 교환되는 메시지 수가 줄어듭니다. IKEv2는 4개의 메시지를 사용합니다. IKEv1은 6개의 메시지(기본 모드) 또는 3개의 메시지(적극적인 모드)를 사용합니다.

IKEv2 메시지 유형은 요청 및 응답 쌍으로 정의됩니다. 이 그림에서는 IKEv2와 IKEv1의 패킷 비교 및 페이로드 내용을 보여 줍니다.



참고: 이 문서에서는 IKEv2 패킷 교환에 대해 자세히 설명하지 않습니다. 추가 참조를 보려면 IKEv2 Packet Exchange 및 Protocol Level Debugging으로 이동합니다.

정책 기반 대 경로 기반

정책 기반 VPN

이름 상태에 따라 정책 기반 VPN은 정책의 일치 기준을 충족하는 트랜짓 트래픽에 대한 정책 작업이 포함된 IPsec VPN 터널입니다. Cisco 디바이스의 경우 ACL(Access List)이 구성되고 암호화 맵에 연결되어 VPN으로 리디렉션되고 암호화되는 트래픽을 지정합니다.

트래픽 선택기는 이미지에 표시된 대로 정책에 지정된 서브넷 또는 호스트입니다.

POLICY BASED VPN

- Crypto maps

Traffic Selectors

10.10.0.0/16
190.168.0.0/24

```
ip access-list extended TS
 permit ip 10.10.0.0 0.0.255.255 10.20.20.0 0.0.0.255
 permit ip 10.10.0.0 0.0.255.255 10.20.30.0 0.0.0.255
 permit ip 192.168.0.0 0.0.0.255 10.20.20.0 0.0.0.255
 permit ip 192.168.0.0 0.0.0.255 10.20.30.0 0.0.0.255
 exit
```

Traffic Selectors

10.20.20.0/24
10.20.30.0/24

```
ip access-list extended TS
 permit ip 10.20.20.0 0.0.0.255 10.10.0.0 0.0.255.255
 permit ip 10.20.30.0 0.0.0.255 10.10.0.0 0.0.255.255
 permit ip 10.20.20.0 0.0.0.255 192.168.0.0 0.0.0.255
 permit ip 10.20.30.0 0.0.0.255 192.168.0.0 0.0.0.255
 exit
```

경로 기반 VPN

정책은 필요하지 않으며 트래픽이 경로가 있는 터널로 리디렉션되며 터널 인터페이스를 통한 동적 라우팅을 지원합니다. 트래픽 선택기(VPN을 통해 암호화된 트래픽)는 이미지에 표시된 대로 기본적으로 0.0.0.0.에서 0.0.0.0까지입니다.

ROUTE BASED VPN

- Supports dynamic routing over the tunnel interface.

Traffic Selectors
0.0.0.0

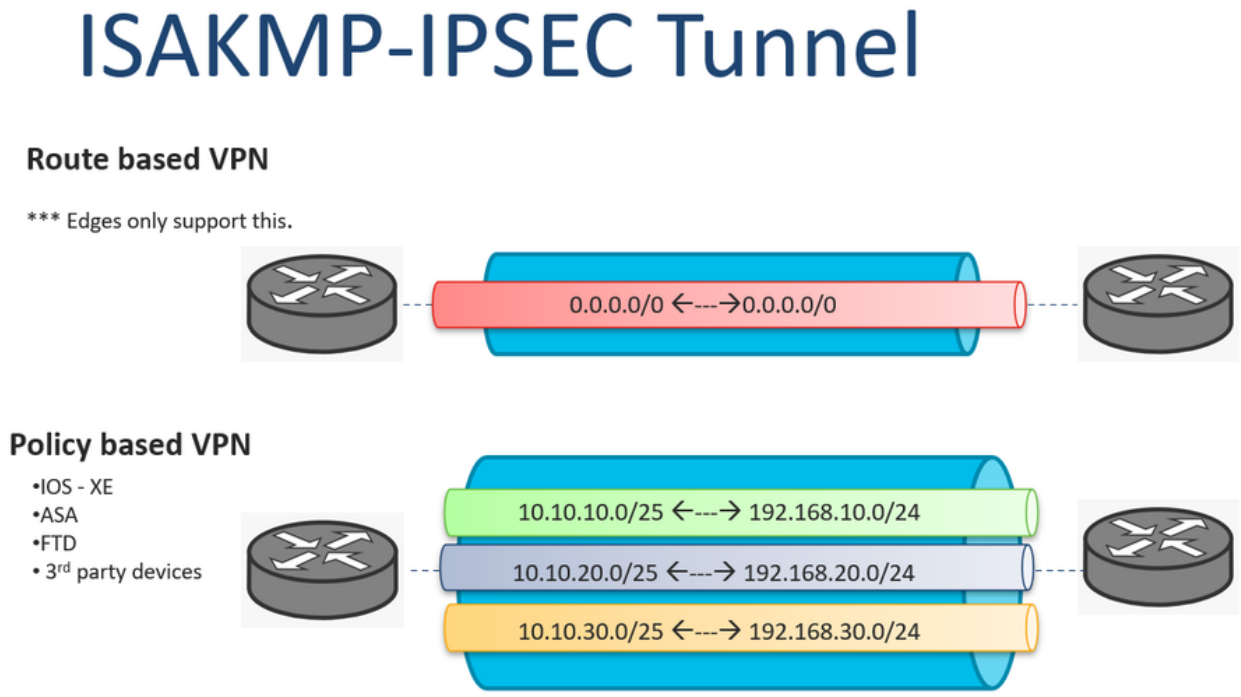
Traffic Selectors
0.0.0.0

```
interface: Tunnel100001
   Crypto map tag: Tunnel100001-head-0, local addr 10.0.21.17

  protected vrf: 1
  local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
```

참고: 트래픽 선택기가 0.0.0.0 때문에 모든 호스트 또는 서브넷이 포함되므로 하나의 SA만 생성됩니다. 동적 터널에 대한 예외가 있습니다. 이 문서에서는 동적 터널에 대해 설명하지 않습니다.

이미지에 표시된 대로 정책 및 경로 기반 VPN을 구체화할 수 있습니다.



.

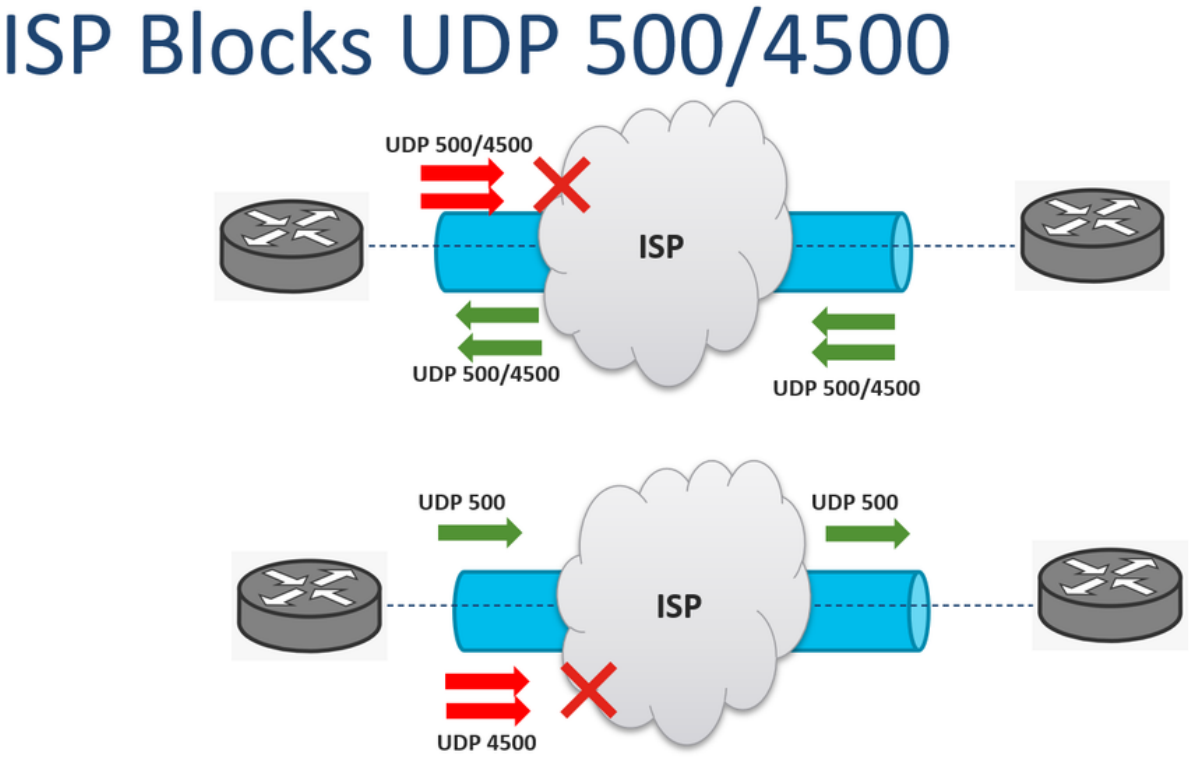
> **참고:** SA가 하나만 생성된 경로 기반 VPN과 달리 정책 기반 VPN은 다중 SA를 생성할 수 있습니다. ACL이 구성되면 ACL의 각 명령문(서로 다른 경우)은 하위 터널을 생성합니다.

VPN을 통해 수신되지 않는 트래픽의 일반적인 문제

ISP가 UDP 500/4500을 차단함

ISP(Internet Services Provider)가 UDP 500/4500 포트를 차단하는 것은 매우 일반적인 문제입니다. IPsec 터널 설정의 경우 두 개의 서로 다른 ISP를 연결할 수 있으며, 이 중 하나는 포트를 차단할 수 있으며 다른 하나는 포트를 허용합니다.

이 그림에서는 ISP가 UDP 500/4500 포트를 한 방향으로만 차단할 수 있는 두 가지 시나리오를 보여 줍니다.

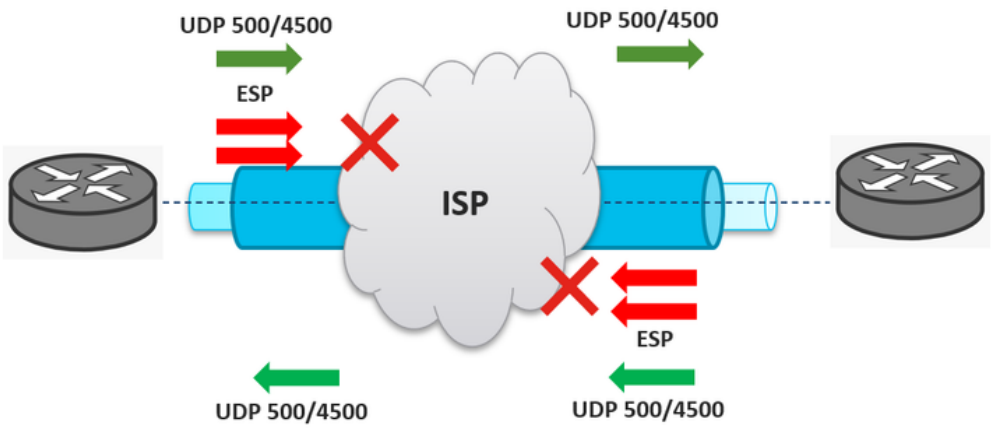


참고: 포트 UDP 500은 IKE(Internet Key Exchange)에서 보안 VPN 터널을 설정하는 데 사용됩니다. UDP 4500은 NAT가 하나의 VPN 엔드포인트에 있을 때 사용됩니다.

참고: ISP가 UDP 500/4500을 차단하면 IPsec 터널 설정이 영향을 받으며 작동하지 않습니다.

ISP에서 ESP 차단

IPsec 터널의 또 다른 매우 일반적인 문제는 ISP가 ESP 트래픽을 차단하지만 UDP 500/4500 포트를 허용한다는 것입니다. 예를 들어, UDP 500/4500 포트는 양방향으로 허용되므로 터널이 성공적으로 설정되지만 ISP 또는 ISP에 의해 양방향으로 ESP 패킷이 차단되므로 이미지에 표시된 것처럼 VPN을 통한 암호화된 트래픽이 실패합니다.



참고: ISP에서 ESP 패킷을 차단하면 IPsec 터널 설정이 성공하지만 암호화된 트래픽은 영향을 받습니다. 즉, VPN을 가동할 때 반사될 수 있지만 트래픽은 이를 통해 작동하지 않습니다.

팁: ESP 트래픽이 한 방향으로만 차단되는 시나리오도 나타날 수 있으며, 증상은 동일하지만 터널 통계 정보, 캡슐화, 역캡슐화 카운터 또는 RX 및 TX 카운터에서 쉽게 찾을 수 있습니다.

관련 정보

- KEv2 패킷 교환 및 프로토콜 수준 디버깅
- IKE(Internet Key Exchange) - RFC 2409
- IKEv2(Internet Key Exchange) 프로토콜
- 기술 지원 및 문서 – Cisco Systems