IKEv2 패킷 교환 및 프로토콜 레벨 디버깅

목차

[소개](#)
[사전 요구 사항](#)
[요구 사항](#)
[사용되는 구성 요소](#)
[표기 규칙](#)
[IKEv1과 IKEv2 간의 차이점](#)
[IKEv2 Exchange의 초기 단계](#)
[IKE_SA_INIT Exchange](#)
[IKE_AUTH Exchange](#)
[이후 IKEv2 교환](#)
[관련 정보](#)

소개

이 문서에서는 최신 버전의 IKE(Internet Key Exchange)의 장점과 버전 1과 버전 2의 차이점을 설명합니다.

IKE는 IPsec 프로토콜 제품군에서 SA(보안 연결)를 설정하는 데 사용되는 프로토콜입니다. IKEv2는 IKE 프로토콜의 두 번째 및 최신 버전입니다. 이 프로토콜의 채택은 2006년부터 시작되었습니다. IKE 프로토콜 개편의 필요성과 의도에 대해서는 RFC 4306의 부록 A *IKEv2(Internet Key Exchange) 프로토콜*에 설명되어 있습니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

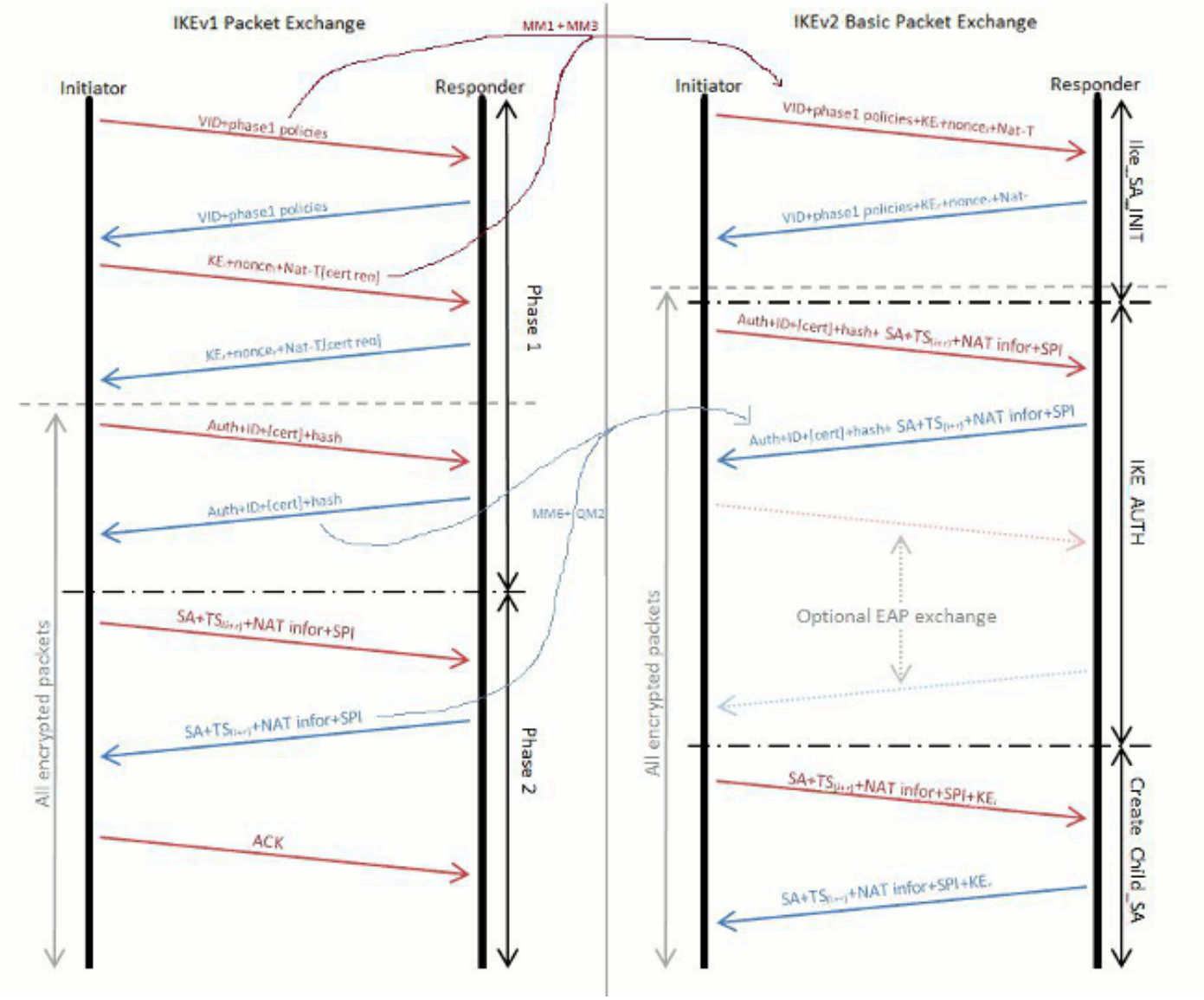
이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

표기 규칙

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

IKEv1과 IKEv2 간의 차이점

RFC 4306의 *IKEv2(Internet Key Exchange) 프로토콜은* IKEv1보다 IKEv2의 장점을 세부적으로 설명하지만 전체 IKE 교환이 재검토되었음을 유의해야 합니다. 이 다이어그램은 두 교환의 비교를 제공합니다.



IKEv1에서는 6개의 패킷이 포함된 1단계 교환이 명확하게 구분되었으며, 2단계 교환은 3개의 패킷으로 구성됩니다. IKEv2 교환은 변수입니다. 최대 4개의 패킷을 교환할 수 있습니다. 최악의 경우, 이는 인증의 복잡성, 사용된 EAP(Extensible Authentication Protocol) 특성 수 및 구성된 SA 수에 따라 최대 30개의 패킷(그 이상이 아닌 경우)으로 증가할 수 있습니다. IKEv2는 IKEv1의 2단계 정보를 IKE_AUTH 교환에 결합하며, IKE_AUTH 교환이 완료된 후 두 피어 모두 하나의 SA를 이미 빌드하여 트래픽을 암호화할 준비가 되었는지 확인합니다. 이 SA는 트리거 패킷과 일치하는 프록시 ID에 대해서만 구축됩니다. 다른 프록시 ID와 일치하는 후속 트래픽은 IKEv1의 2단계 교환에 해당하는 CREATE_CHILD_SA 교환을 트리거합니다. 적극적인 모드 또는 주 모드가 없습니다.

IKEv2 Exchange의 초기 단계

실제로 IKEv2에는 두 개의 초기 협상 단계만 있습니다.

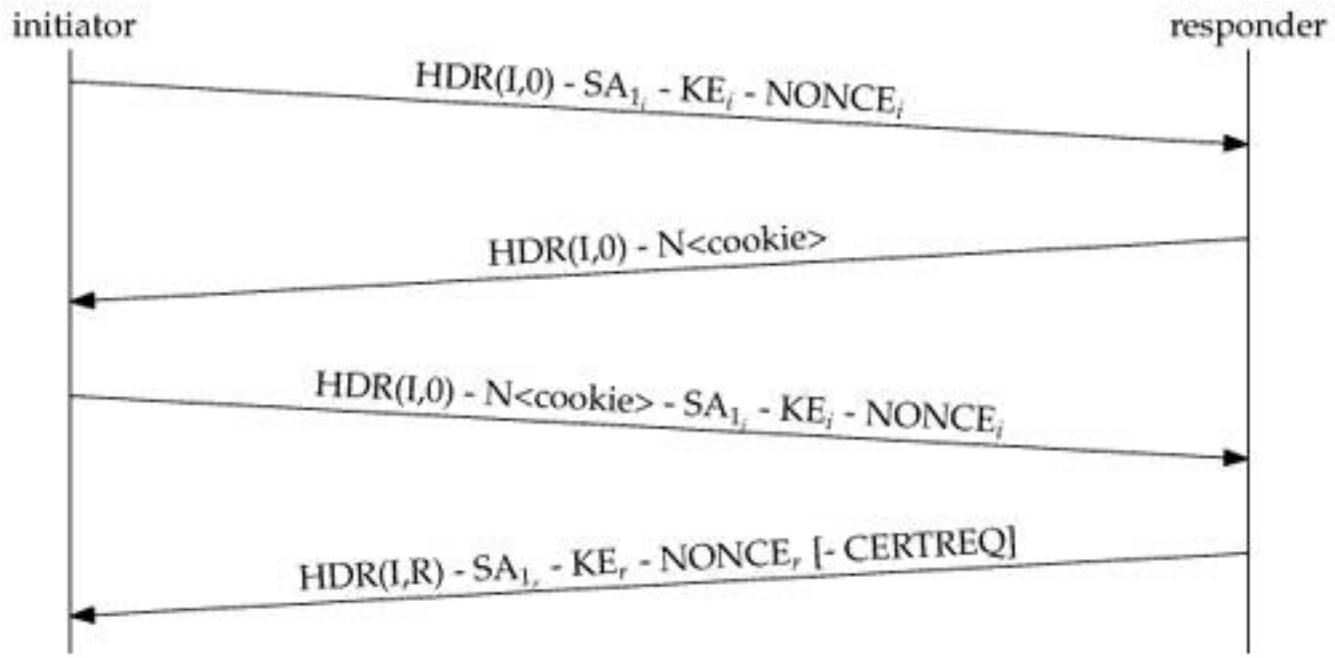
- IKE_SA_INIT Exchange
- IKE_AUTH Exchange

IKE_SA_INIT Exchange

IKE_SA_INIT는 피어가 보안 채널을 설정하는 초기 교환입니다. 초기 교환을 완료하면 모든 추가 교환이 암호화됩니다. 교환은 IKEv1의 MM1-4에서 일반적으로 교환되는 모든 정보를 결합하기 때문에 두 개의 패킷만 포함합니다. 따라서 응답자는 IKE_SA_INIT 패킷을 처리하는 데 컴퓨팅 비용이 많이 들며 첫 번째 패킷을 처리하도록 떠날 수 있습니다. 스푸핑된 주소에서 DOS 공격에 대한 프로토콜을 열어 둡니다.

이러한 공격으로부터 보호하기 위해 IKEv2에는 스푸핑 공격을 방지하기 위해 IKE_SA_INIT 내에서 선택적 교환이 있습니다. 불완전한 세션의 특정 임계값에 도달하면 응답자는 패킷을 더 이상 처리하지 않고 대신 쿠키를 사용하여 개시자에게 응답을 보냅니다. 세션을 계속하려면 초기자가 IKE_SA_INIT 패킷을 다시 전송하고 받은 쿠키를 포함해야 합니다.

초기자는 원래 교환이 스푸핑되지 않았음을 증명하는 응답자로부터 알림 페이로드와 함께 초기 패킷을 다시 전송합니다. 쿠키 챌린지와 함께 IKE_SA_INIT 교환의 다이어그램은 다음과 같습니다.



IKE_AUTH Exchange

IKE_SA_INIT 교환이 완료되면 IKEv2 SA가 암호화됩니다. 그러나 원격 피어가 인증되지 않았습니다. IKE_AUTH 교환은 원격 피어를 인증하고 첫 번째 IPsec SA를 생성하는 데 사용됩니다.

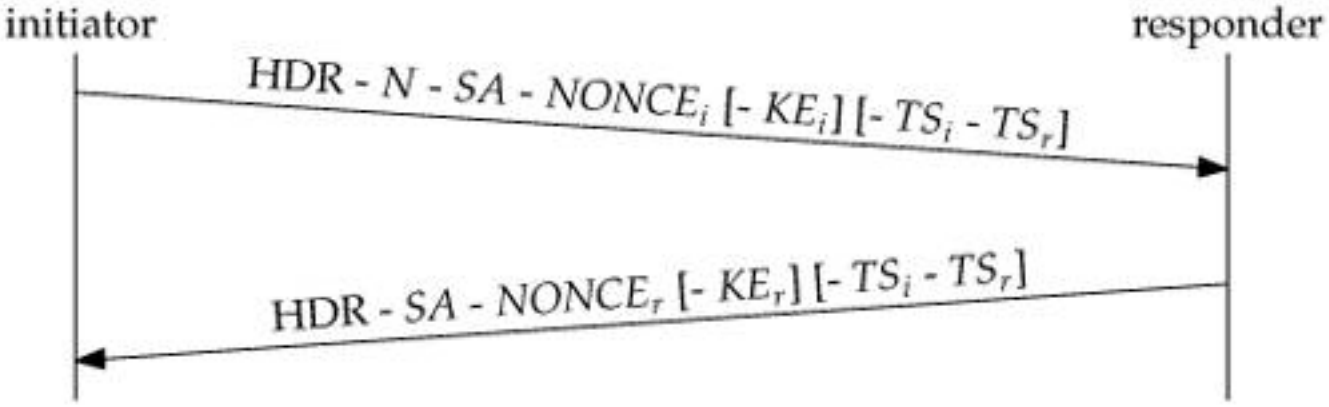
교환에는 인증 페이로드와 함께 ISAKMP(Internet Security Association and Key Management Protocol) ID가 포함되어 있습니다. 인증 페이로드의 내용은 PSK(Pre-Shared Key), RSA 인증서(RSA-SIG), ECDSA-SIG(Elliptic Curve Digital Signature Algorithm) 인증서 또는 EAP일 수 있는 인증 방법에 따라 달라집니다. 인증 페이로드 외에도, 교환에는 생성할 IPsec SA를 설명하는 SA 및 Traffic Selector 페이로드가 포함됩니다.

이후 IKEv2 교환

CREATE_CHILD_SA Exchange

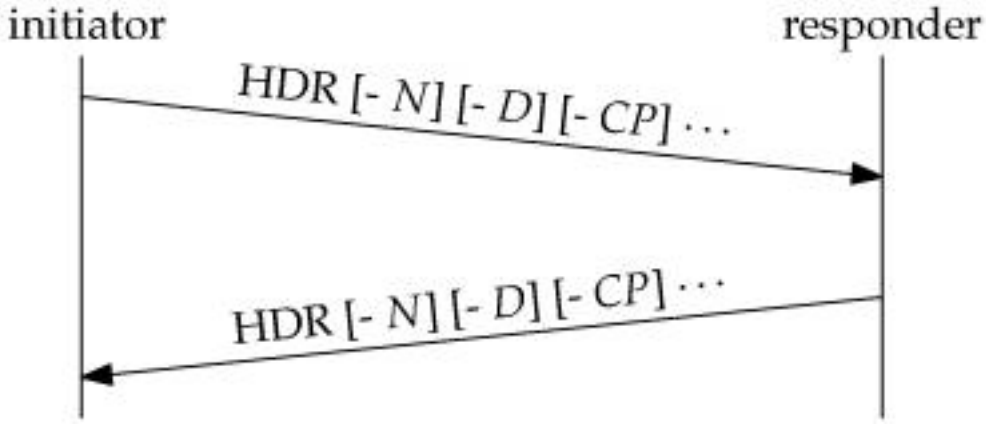
추가 하위 SA가 필요하거나 IKE SA 또는 하위 SA 중 하나를 키 재지정해야 하는 경우 빠른 모드 교환이 IKEv1에서 수행하는 것과 동일한 기능을 수행합니다. 이 다이어그램에 표시된 것처럼 이 교환

에는 두 개의 패킷만 있습니다. 그러나 교환은 모든 rekey 또는 new SA에 대해 반복됩니다.



정보 교환

모든 IKEv2 교환에 있는 것처럼 각 INFORMATIONAL Exchange 요청에는 응답이 필요합니다. 정보 교환에는 세 가지 유형의 페이로드를 포함할 수 있습니다. 이 다이어그램에 표시된 것처럼 페이로드의 조합을 원하는 수만큼 포함할 수 있습니다.



- Notify 페이로드(N)가 쿠키와 함께 이미 표시되었습니다. 여러 가지 다른 유형이 있습니다. IKEv1에서와 같이 오류 및 상태 정보를 전달합니다.
- Delete 페이로드(D)는 발신자가 하나 이상의 수신 SA를 삭제했음을 피어에 알립니다. 응답자는 해당 SA를 삭제해야 하며, 일반적으로 응답 메시지의 다른 방향에 해당하는 SA에 대한 Delete 페이로드를 포함합니다.
- CP(Configuration payload)는 피어 간의 컨피그레이션 데이터를 협상하는 데 사용됩니다. CP의 중요한 용도 중 하나는 보안 게이트웨이에 의해 보호되는 네트워크에 주소를 요청(요청)하고 할당(응답)하는 것입니다. 일반적으로 모바일 호스트는 홈 네트워크에 보안 게이트웨이가 있는 VPN(Virtual Private Network)을 설정하고 홈 네트워크에 IP 주소를 지정하도록 요청합니다.**참고:** 이렇게 하면 L2TP(Layer 2 Tunneling Protocol) 및 IPsec의 통합 사용이 해결할 수 있는 문제 중 하나가 해결됩니다.

관련 정보

- PSK가 포함된 Site-to-Site VPN용 ASA IKEv2 디버그 TechNote
- ASA IPsec 및 IKE 디버깅(IKEv1 기본 모드) 문제 해결 TechNote
- IOS IPSec 및 IKE 디버깅 - IKEv1 기본 모드 문제 해결 TechNote
- ASA IPSec 및 IKE 디버깅 - IKEv1 Aggressive Mode TechNote

- Cisco ASA 5500 Series Adaptive Security Appliance
- Cisco ASA 5500 Series Adaptive Security Appliances 소프트웨어 다운로드
- IPSec 협상/IKE 프로토콜
- Cisco IOS Firewall
- Cisco IOS 소프트웨어
- SSH(Secure Shell)
- IPSec 협상/IKE 프로토콜
- 기술 지원 및 문서 – Cisco Systems