IKEv2 Packet Exchange en Protocol-niveau afluisteren

Inhoud

Inleiding

Dit document beschrijft de voordelen van de nieuwste versie van Internet Key Exchange (IKE) en de verschillen tussen versie 1 en versie 2.

IKE is het protocol dat wordt gebruikt om een beveiligingsassociatie (SA) op te zetten in de IPsec-protocolreeks. IKEv2 is de tweede en laatste versie van het IKE-protocol. De aanneming van dit protocol is al in 2006 begonnen. De noodzaak en bedoeling van een herziening van het IKE-protocol werd beschreven in Bijlage A van het *Internet Key Exchange-protocol (IKEv2)* in RFC 4306.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

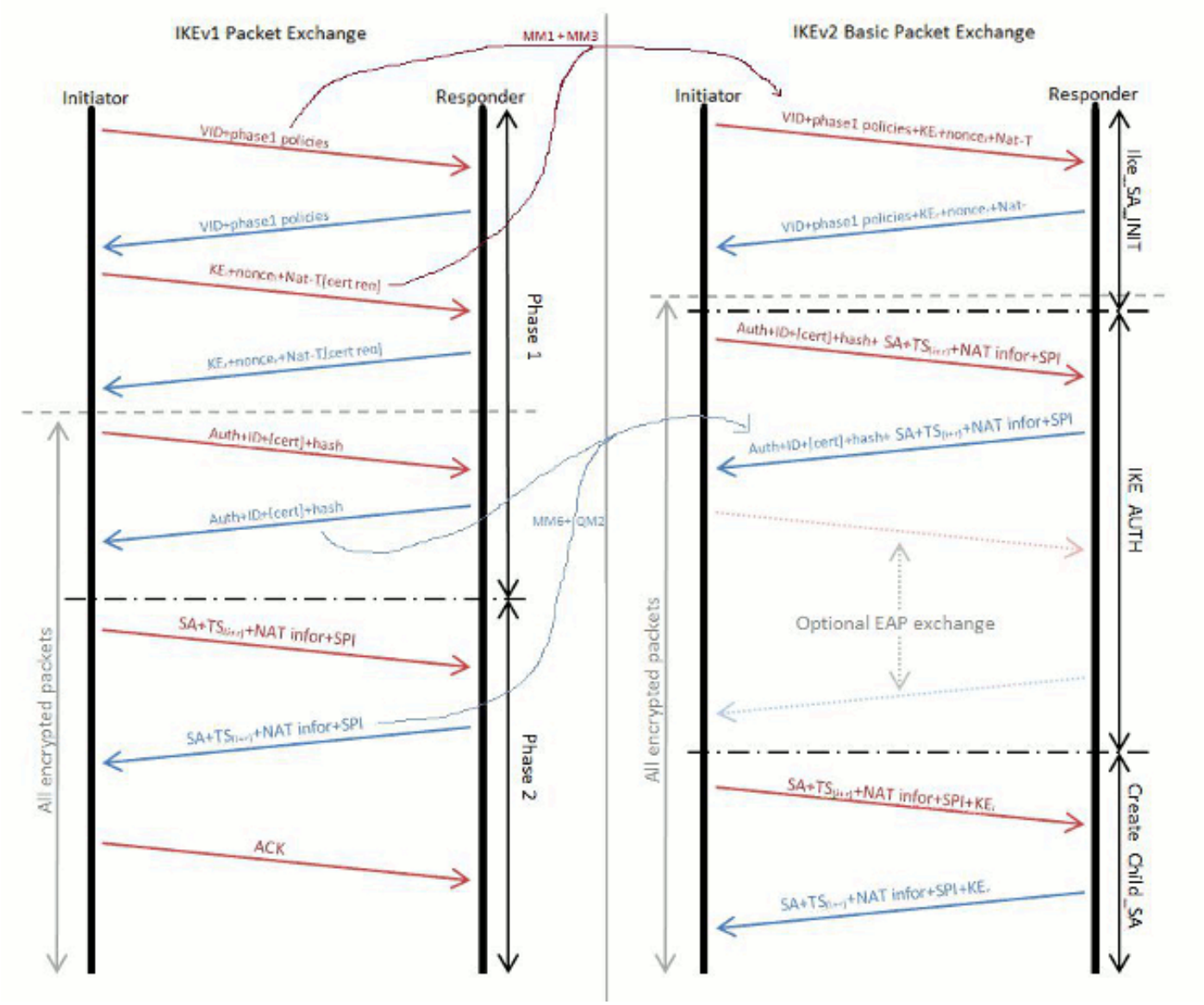
Dit document is niet beperkt tot specifieke software- en hardware-versies.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Verschillen tussen IKEv1 en IKEv2

Terwijl *het Protocol van Internet Key Exchange (IKEv2)* in RFC 4306 de voordelen van IKEv2 ten opzichte van IKEv1 in detail beschrijft, is het belangrijk op te merken dat de gehele IKE-uitwisseling is herzien. In dit schema worden de twee beurzen vergeleken:



In IKEv1 was er een duidelijk afgebakend fase 1-uitwisseling, dat zes pakketten bevat, gevolgd door een fase 2-uitwisseling bestaat uit drie pakketten; de IKEv2-uitwisseling is variabel. Op zijn best, kan het slechts vier pakketten uitwisselen. In het ergste geval kan dit toenemen tot wel 30 pakketten (zo niet meer), afhankelijk van de complexiteit van de authenticatie, het aantal Extensible Authentication Protocol (EAP) eigenschappen, evenals het aantal gevormde SA's. IKEv2 combineert de fase 2-informatie in IKEv1 in de IKE_AUTH-uitwisseling en garandeert dat, nadat de IKE_AUTH-uitwisseling is voltooid, beide peers al een SA hebben gebouwd en klaar zijn om verkeer te versleutelen. Deze SA is enkel gebouwd voor de volmachtidentiteiten die het trekker pakje passen. Elk vervolg verkeer dat overeenkomt met andere proxy-identiteiten zet vervolgens de CREATE_CHILD_SA-uitwisseling in gang, wat gelijk is aan de fase 2-uitwisseling in IKEv1. Er is geen agressieve modus of hoofdmodus.

Initiële fasen in IKEv2 exchange

IKEv2 heeft in feite slechts twee eerste onderhandelingsfasen:

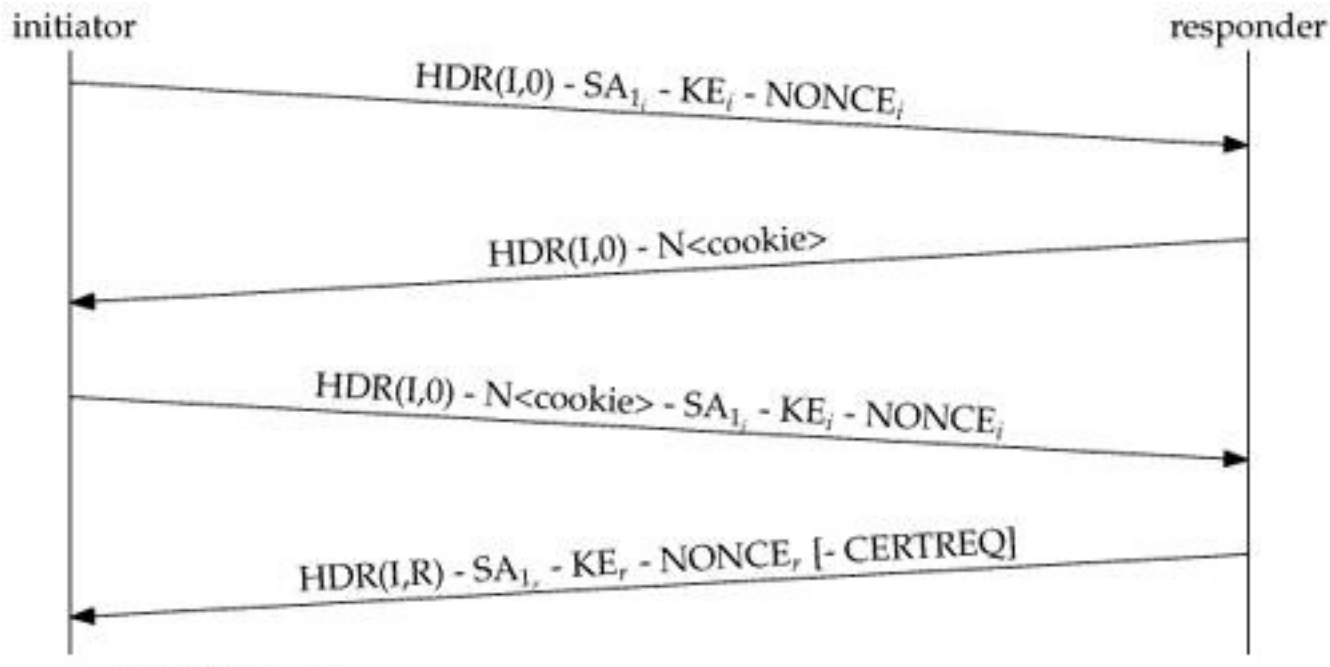
- IKE_SA_INIT exchange
- IKE_AUTH-exchange

IKE_SA_INIT exchange

IKE_SA_INIT is de eerste uitwisseling waarin de peers een veilig kanaal inrichten. Nadat de eerste uitwisseling is voltooid, worden alle verdere uitwisselingen versleuteld. De uitwisselingen bevatten slechts twee pakketten omdat zij alle informatie die gewoonlijk in MM1-4 in IKEv1 wordt uitgewisseld combineren. Als resultaat hiervan is de responder computationeel duur om het IKE_SA_INIT pakket te verwerken en kan het de eerste pakket laten verwerken; het protocol wordt opengelaten voor een DOS-aanval van spoofed-adressen.

Om te beschermen tegen dit soort aanvallen heeft IKEv2 een optionele uitwisseling binnen IKE_SA_INIT om te voorkomen dat er aanvallen met spoofing plaatsvinden. Als een bepaalde drempel van onvolledige sessies wordt bereikt, verwerkt de responder het pakket niet verder, maar stuurt hij een antwoord op de Initiator met een koekje. Om door te kunnen gaan, moet de Initiator het IKE_SA_INIT pakket opnieuw versturen en het ontvangen koekje toevoegen.

De Initiator herstelt het eerste pakket samen met de lading van de responder op de hoogte die bewijst dat de oorspronkelijke uitwisseling niet gespoofd was. Hier is een diagram van IKE_SA_INIT uitwisseling met koekje uitdaging:



IKE_AUTH-exchange

Nadat de IKE_SA_INIT uitwisseling is voltooid, wordt IKEv2 SA versleuteld; de peer op afstand is echter niet echt bevonden . De IKE_AUTH uitwisseling wordt gebruikt om de externe peer voor authentiek te verklaren en om de eerste IPsec SA te creëren.

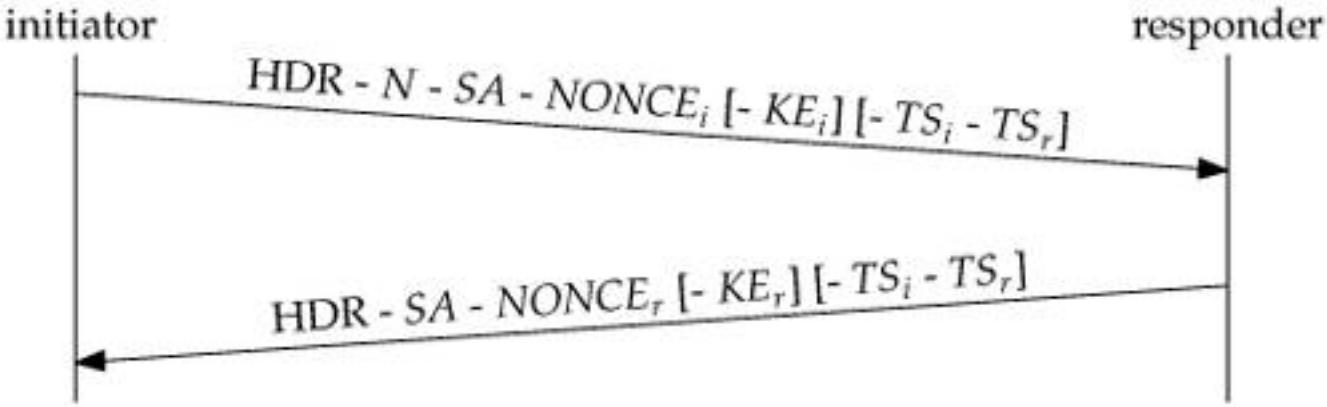
De uitwisseling bevat de ID van Internet Security Association en Key Management Protocol (ISAKMP) samen met een authenticatie-lading. De inhoud van de authenticatie-lading is afhankelijk van de methode van authenticatie, die kan worden voorafgegaan door gedeelde sleutel

(PSK), RSA-certificaten (RSA-SIG), Elliptic Curve Digital Signature Algorithm-certificaten (ECDSA-SIG) of EAP. Naast de verificatiebetalingen omvat de uitwisseling de SA- en Traffic Selector-nuttige ladingen die de te creëren IPsec SA beschrijven.

Later IKEv2-uitwisselingen

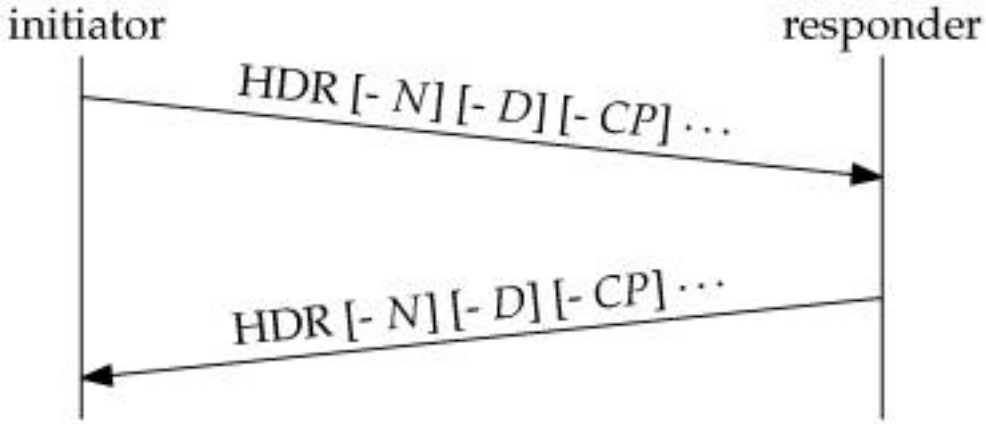
CREATE_CHILD_SA exchange

Als extra kind SA's nodig zijn of als de IKE SA of een van de kind SA's opnieuw moet worden gecontroleerd, heeft deze dezelfde functie als de snelle-modemuitwisseling in IKEv1. Zoals in dit schema wordt getoond, zijn er slechts twee pakketten in deze ruil; voor iedere rekey of new SA herhaalt de ruil echter:



INFORMELE WISSELING

Aangezien het in alle IKEv2-beurzen is, verwacht elk verzoek om informatie-uitwisseling een antwoord. Drie soorten betalingen kunnen worden opgenomen in een informatie - uitwisseling. Een eventueel aantal combinaties van nuttige lading kan worden opgenomen, zoals aangegeven in dit schema:



- De aangegeven lading (N) is al gezien in combinatie met koekjes. Er zijn ook verschillende andere typen. Ze dragen informatie over fouten en status, zoals ze in IKEv1 doen.
- De Delete payload (D) meldt de peer dat de afzender één of meer van zijn inkomende SA's heeft verwijderd. Verwacht wordt dat de responder deze SA's zal verwijderen en gewoonlijk loonbelasting voor de SA's zal verwijderen die in de andere richting in haar antwoordbericht overeenkomt.
- De Configuration payload (CP) wordt gebruikt om te onderhandelen over

configuratiegegevens tussen de peers. Een belangrijk gebruik van de CP is om te vragen (verzoek) en (antwoord) een adres op een netwerk toe te wijzen dat door een veiligheidstoegang beschermd wordt. In het typische geval, vestigt een mobiele host een Virtual Private Network (VPN) met een beveiligingsgateway op het thuisnetwerk en verzoekt hij het IP-adres op het thuisnetwerk aan te geven.**Opmerking:** dit heft een van de problemen op die het gecombineerde gebruik van Layer 2 Tunneling Protocol (L2TP) en IPsec wil oplossen.

Gerelateerde informatie

- ASA IKEv2-debugs voor Site-to-Site VPN met PSKs TechNotes
- ASA IPsec- en IKE-debugs (IKEv1 hoofdmodus) voor probleemoplossing bij technische opmerking
- IOS IPSec- en IKE-implementaties - IKEv1 hoofdmodus voor probleemoplossing
- ASA IPSec and IKE-implementaties - IKEv1 aggregation mode TechNotes
- Adaptieve security applicaties van Cisco ASA 5500 Series
- Cisco ASA 5500 Series softwaredownloads voor adaptieve security applicaties
- IPsec-onderhandeling/IKE-protocollen
- Cisco IOS Firewall
- Cisco IOS-software
- Secure Shell (SSH)
- IPsec-onderhandeling/IKE-protocollen
- Technische ondersteuning en documentatie – Cisco Systems