IPsec IKEv1-protocol begrijpen

Inhoud

Inleiding

Dit document beschrijft het proces van het Internet Key Exchange (IKEv1)-protocol voor een VPN-instelling (Virtual Private Network) om de pakketuitwisseling te begrijpen voor een eenvoudiger probleemoplossing voor een IP-sec-probleem (Internet Protocol Security) met IKEv1.

Bijgedragen door Amanda Nava, Cisco TAC Engineer.

Voorwaarden

Vereisten

Cisco raadt aan dat u kennis hebt van basisbeveiligingsconcepten:

- Verificatie
- Vertrouwelijkheid
- Integriteit
- IPsec

Gebruikte componenten

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

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, zorg er dan voor dat u de mogelijke impact van elke opdracht begrijpt

IPsec

IPsec is een reeks protocollen die beveiliging van internetcommunicatie op de IP-laag bieden. Het meest gebruikelijke gebruik van IPsec is om een Virtual Private Network (VPN) te bieden, of tussen twee locaties (gateway-to-gateway) of tussen een externe gebruiker en een ondernemingsnetwerk (host-to-gateway).

IKE-protocol

IPsec gebruikt het IKE-protocol om te onderhandelen en beveiligde site-to-site of externe toegang Virtual Private Network (VPN)-tunnels in te stellen. IKE-protocol wordt ook de Internet Security Association en Key Management Protocol (ISAKMP) genoemd (alleen in Cisco).

Er zijn twee versies van IKE:

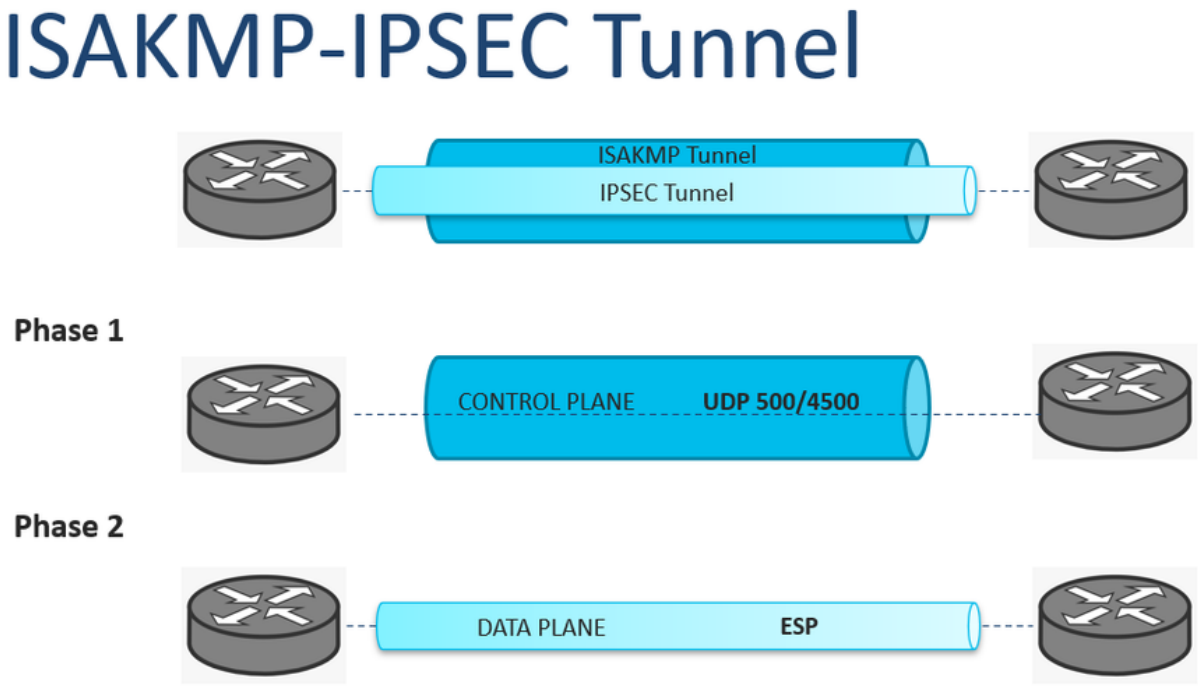
- IKEv1: Gedefinieerd in RFC 2409, The Internet Key Exchange
- IKE versie 2 (IKEv2): Gedefinieerd in RFC 4306, Internet Key Exchange (IKEv2)-protocol

IKE-fasen

ISAKMP scheidt de onderhandelingen in twee fasen:

- Fase 1: De twee ISAKMP-peers zorgen voor een beveiligde en geauthentiseerde tunnel, die de ISAKMP-onderhandelingsberichten beschermt. Deze tunnel staat bekend als de ISAKMP SA. Er zijn twee modi gedefinieerd door ISAKMP: Hoofdmodus (MM) en agressieve modus.
- Fase 2: Het onderhandelt over sleutelmaterialen en algoritmen voor de encryptie (SAs) van de gegevens die over de IPsec-tunnel moeten worden overgebracht. Deze fase wordt Quick Mode genoemd.

Om alle abstracte concepten te concretiseren, is de fase 1-tunnel de Parent-tunnel en fase 2 is een subtunnel. Dit beeld illustreert de twee fasen als tunnels.



Opmerking: Fase 1 (ISAKMP) Tunnel beschermt het VPN-verkeer van het besturingsplane tussen de twee gateways. Verkeer van besturingsplane kan zijn: onderhandelingspakketten, informatiepakketten, DPD, keepalives, rekey, enz. ISAKMP onderhandeling gebruikt de UDP 500- en 4500-poorten om een beveiligd kanaal te creëren.

Opmerking: Fase 2 (IPsec) Tunnel beschermt het verkeer van het Datacentervlak dat door VPN tussen de twee gateways passeert. ODe algoritmen die worden gebruikt om de gegevens te beschermen, worden in fase 2 geconfigureerd en zijn onafhankelijk van de in fase 1 gespecificeerde algoritmen.
Het protocol dat wordt gebruikt om deze pakketten in te sluiten en te versleutelen is de Encapsulation Security Payload (ESP).

IKE-modi (fase 1)

Hoofdmodus

Een IKE-sessie begint wanneer de initiatiefnemer een voorstel of voorstel naar de responder stuurt. De eerste uitwisseling tussen knooppunten stelt het basisveiligheidsbeleid vast; de initiator stelt voor gebruik te maken van versleutelings - en authenticatiealgoritmen . De responder kiest het juiste voorstel (we nemen aan dat er een voorstel geselecteerd is) en stuurt het naar de initiatiefnemer. De volgende uitwisseling geeft Diffie-Hellman openbare sleutels en andere gegevens door. Alle verdere onderhandelingen zijn versleuteld binnen IKE SA. De derde uitwisseling authenticeert de ISAKMP-sessie. Zodra het IKE SA wordt gevestigd, begint de onderhandeling van IPSec (Snelle modus).

Aggressief Mode

Aggressive Mode beperkt de IKE SA onderhandeling in drie pakketten, waarbij alle gegevens die

vereist zijn voor de SA door de initiatiefnemer worden doorgegeven. De responder verstuurt het voorstel, het belangrijkste materiaal en de ID en echt de sessie in het volgende pakket. De initiatiefnemer antwoordt en verklaart de sessie echt. De onderhandelingen verlopen sneller en de initiator- en responder-ID gaan in de openbaarheid.

IPsec-modus (fase 2)

Snelle modus

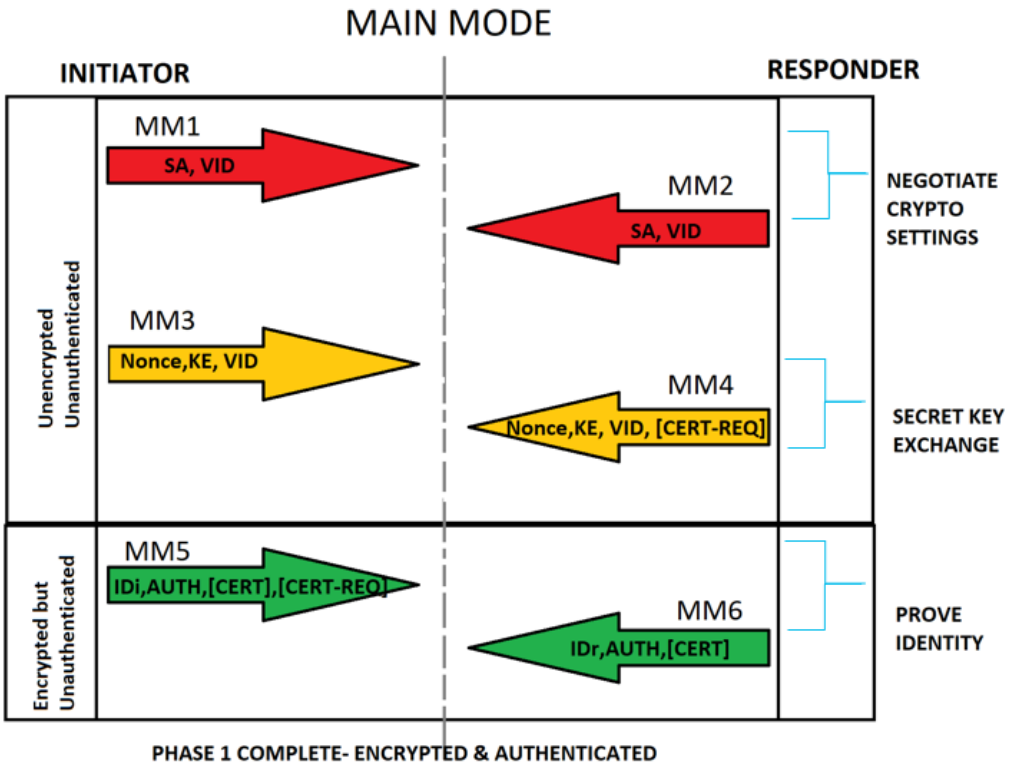
De onderhandeling van IPSec, of de Snelle modus, is vergelijkbaar met een agressieve mode IKE onderhandeling, behalve onderhandeling, moet binnen een IKE SA worden beschermd. De snelmodus bespreekt de SA voor de gegevensencryptie en beheert de belangrijkste uitwisseling voor die IPSec SA.

IKE-woordenlijst

- Een **Security Association** (**SA**) is de instelling van gedeelde beveiligingskenmerken tussen twee netwerkentiteiten ter ondersteuning van beveiligde communicatie. Een SA omvat eigenschappen zoals cryptografisch algoritme en -modus; Verkeersencryptiesleutel en parameters voor de netwerkgegevens die over de verbinding moeten worden doorgegeven.
- De **verkoper-ID's** (**VID**) worden verwerkt om te bepalen of de peer de NAT-traversal, de Dead Peer Detectie-functie, fragmentatie enz. ondersteunt.
- **Eenmaal**: een willekeurig gegenereerd nummer dat de initiator verstuurt. Deze regel wordt samen met de andere punten met de overeengekomen toets ingehakt en wordt teruggestuurd. De initiator controleert de koekjes en de éénmaal en wijst alle berichten af die niet de juiste één keer hebben. Dit helpt een herhaling te voorkomen, aangezien geen enkele derde kan voorspellen wat de willekeurig gegenereerde eenmalige is.
- **Key-exchange (KE)**-informatie voor het beveiligde sleuteluitwisselingsproces Diffie-Hellman (DH).
- **Identity Initiator/responder (IDi/IDr.)** wordt gebruikt om de authenticatie-informatie naar de peer te sturen. Deze informatie wordt doorgegeven onder bescherming van het gemeenschappelijk geheim.
- **Diffie-Hellman (DH) key exchange is een methode van beveiligde cryptografische algoritmen uitwisseling via een openbaar kanaal.**
- De gedeelde sleutel van IPSec kan met de DH worden afgeleid die opnieuw wordt gebruikt om **Perfect Forward Secundaire (PFS)** of de oorspronkelijke DH-uitwisseling te verzekeren die aan het eerder afgeleide gedeelde geheim is verfriest.

Hoofdmode Packet Exchange

Elk ISAKMP-pakket bevat payload-informatie voor de tunnelvestiging. De woordenlijst IKE verklaart de afkortingen IKE als deel van de lading inhoud voor de pakketuitwisseling op de hoofdmodus zoals in dit beeld weergegeven.

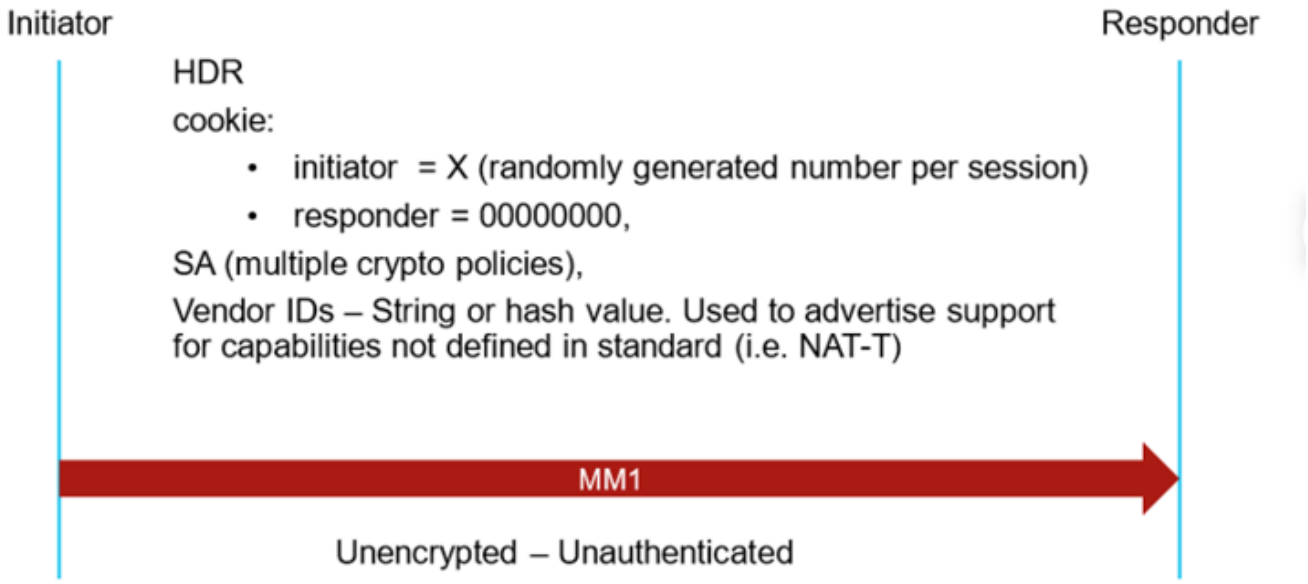


Hoofdmodus 1 (M1)

Om de voorwaarden van de ISAKMP-onderhandelingen te bepalen, creëert u een ISAKMP-beleid dat het volgende omvat:

- Een authenticatiemethode om de identiteit van de peers te waarborgen.
- Een coderingsmethode om de gegevens te beschermen en de privacy te garanderen.
- Een Hashed Message Authentication Codes (HMAC), methode om de identiteit van de afzender te waarborgen en ervoor te zorgen dat het bericht niet tijdens het transport wordt gewijzigd.
- Een Diffie-Hellman groep om de sterkte van het encryptie-sleutel-bepalingsalgoritme te bepalen. Het security apparaat gebruikt dit algoritme om de encryptie en de haktoetsen af te leiden.
- Een limiet voor de tijd dat het security apparaat met een coderingssleutel werkt, voordat deze wordt vervangen.

Het eerste pakket wordt door de Initiator van de IKE-onderhandeling verzonden zoals in de afbeelding.



Opmerking: De hoofdmodus 1 is het eerste pakket van de IKE-onderhandeling. Daarom is de SPI van de Initiator ingesteld op een willekeurige waarde terwijl SPI van de Responder op 0 is ingesteld. In het tweede pakket (MM2) moet de SPI van de Responder worden geantwoord met een nieuwe waarde en de gehele onderhandeling onderhoudt dezelfde SPIs waarden.

Als de M1 wordt opgenomen en een Wireless-shark netwerkprotocolanalyzer wordt gebruikt, is de SPI-waarde binnen de inhoud van de Internet Security Association en Key Management Protocol zoals in de afbeelding.

```
> 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)
```

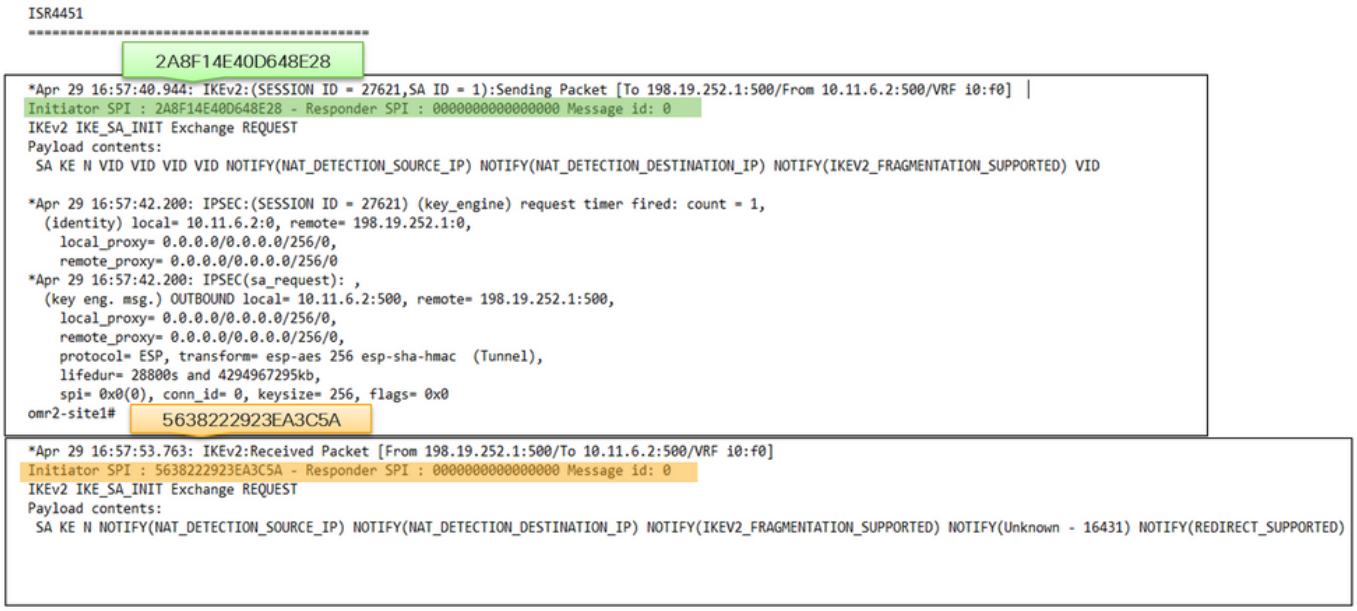
Opmerking: In het geval, het pakket MM1 gaat verloren in het pad of er is geen MM2-antwoord, de onderhandeling van IKE houdt de MM1-terugzending bij totdat het maximale aantal terugzendingen is bereikt. Op dit moment behoudt de Initiator dezelfde SPI totdat de volgende onderhandeling opnieuw wordt geactiveerd.

Tip: De identificatie van initiatiefnemers en Responder SPI's is zeer behulpzaam om meerdere onderhandelingen voor hetzelfde VPN te identificeren en sommige onderhandelingskwesties te beperken.

Twee gelijktijdige onderhandelingen identificeren

Op de Cisco IOS® XE-platforms kunnen de debugs per tunnel worden gefilterd met een voorwaardelijke voorwaarde voor het externe IP-adres dat is ingesteld, maar de gelijktijdige onderhandelingen worden weergegeven op de logs, en er is geen manier om ze te filteren. Dit moet u handmatig doen. Zoals eerder vermeld, behoudt de hele onderhandeling dezelfde SPI-

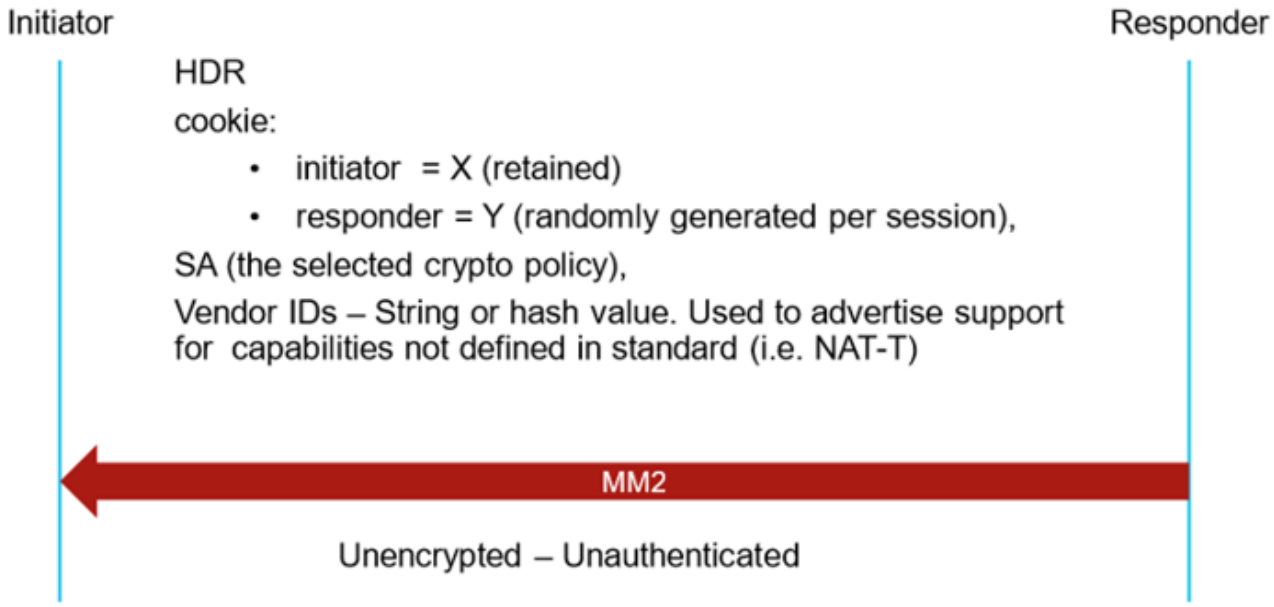
waarden voor Initiator en responder. Indien een pakket van hetzelfde peer IP-adres wordt ontvangen maar de SPI niet overeenkomt met de vorige waarde die is getraceerd voordat de onderhandeling het maximale aantal hertransmissie bereikt, is het een andere onderhandeling voor dezelfde peer als in de afbeelding.



> **Opmerking:** Het voorbeeld toont gelijktijdige onderhandeling voor het eerste pakket in de onderhandeling (MM1), echter, kan dit op elk onderhandelingspunt gebeuren. Alle volgende pakketten moeten een waarde bevatten die afwijkt van 0 op responder SPI.

Hoofdmodus 2 (M2)

In het pakket hoofdmodus 2 stuurt de responder het geselecteerde beleid voor de gematchte voorstellen en wordt de responder SPI op een willekeurige waarde ingesteld. De gehele onderhandeling handhaaft dezelfde SPI-waarden. De MM2-antwoorden op MM1 en de SPI-responder worden ingesteld op een andere waarde dan 0 zoals in de afbeelding.



Als de M2 wordt opgenomen en er een Wireless-shark netwerkprotocolanalyzer wordt gebruikt, zijn de SPI- en SPI-waarden van de initiator binnen de Internet Security Association en Key Management Protocol-inhoud zoals in de afbeelding weergegeven.

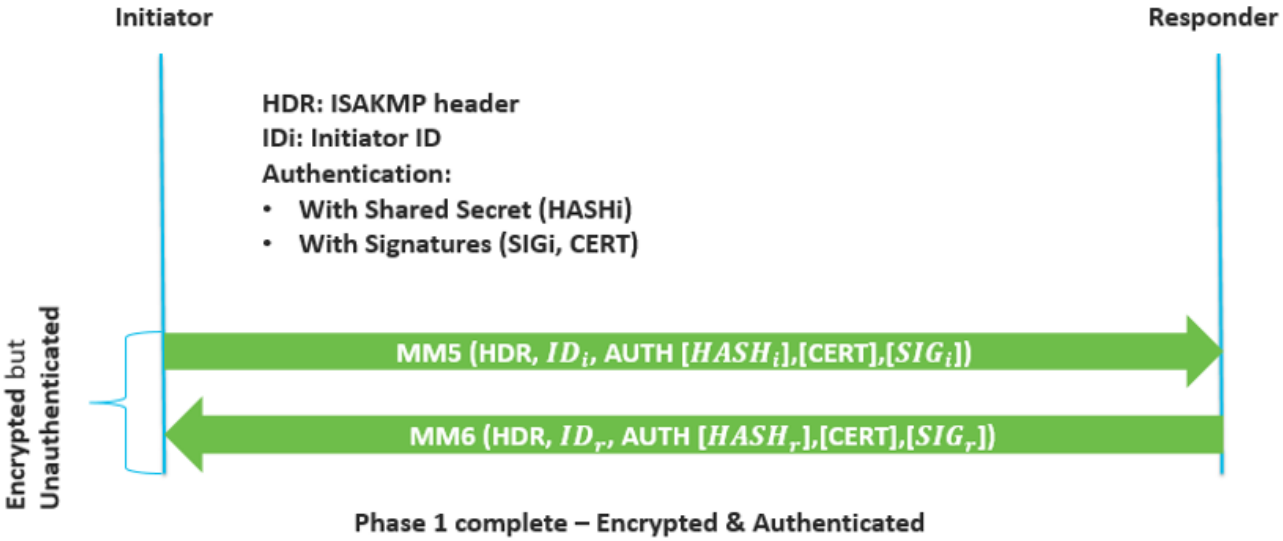
```
> Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
> Internet Protocol Version 4, Src: 209.134.162.150, Dst: 170.49.116.200
> User Datagram Protocol, Src Port: 500, Dst Port: 500
v Internet Security Association and Key Management Protocol
    Initiator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

Hoofdmodus 3 en 4 (MM3-M4)

De pakketten MM3 en M4 worden nog steeds niet versleuteld en niet echt bevonden en de geheime sleutel wordt uitgewisseld. MM3 en M4 worden in de afbeelding weergegeven.

Hoofdmodus 5 en 6 (MM5-MM6)

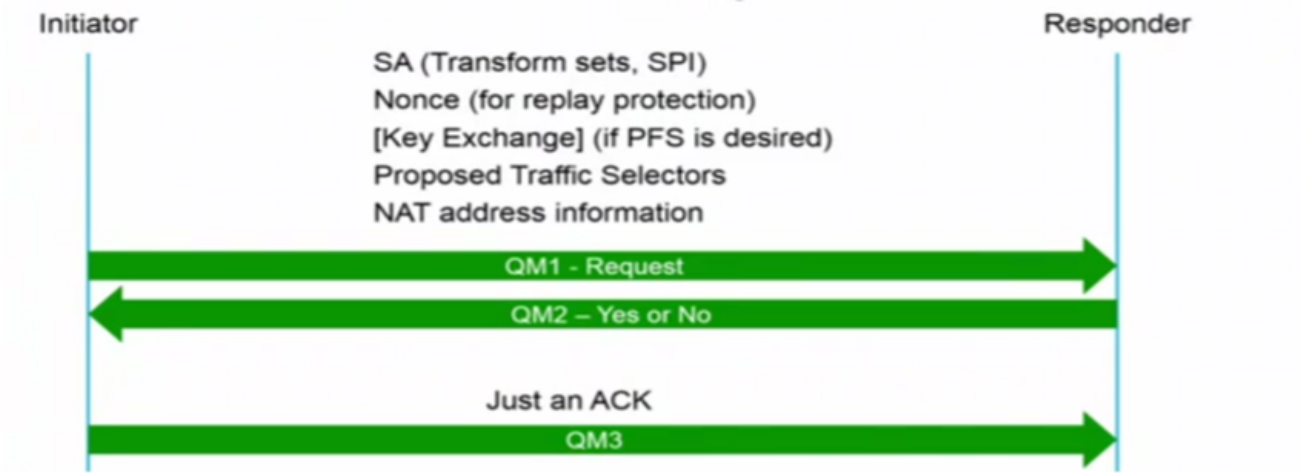
De pakketten MM5 en M6 zijn al versleuteld maar zijn nog niet echt bevonden. Op deze pakketten vindt de authenticatie plaats zoals in de afbeelding wordt getoond.



Snelle modus (QM1, QM2 en QM3)

De snelmodus treedt op nadat het hoofdmonde en het IKE de beveiligde tunnel in fase 1 heeft ingesteld. De snelle modus onderhandelt het gedeelde IPSec-beleid voor de IPSec-beveiligingsalgoritmen en beheert de belangrijke uitwisseling voor de IPSec SA-vestiging. De nonces worden gebruikt om nieuw gedeeld geheim belangrijk materiaal te genereren en te voorkomen dat aanvallen op boogschutters SA's worden gegenereerd.

Er worden drie pakketten uitgewisseld in deze fase, zoals in de afbeelding wordt getoond.

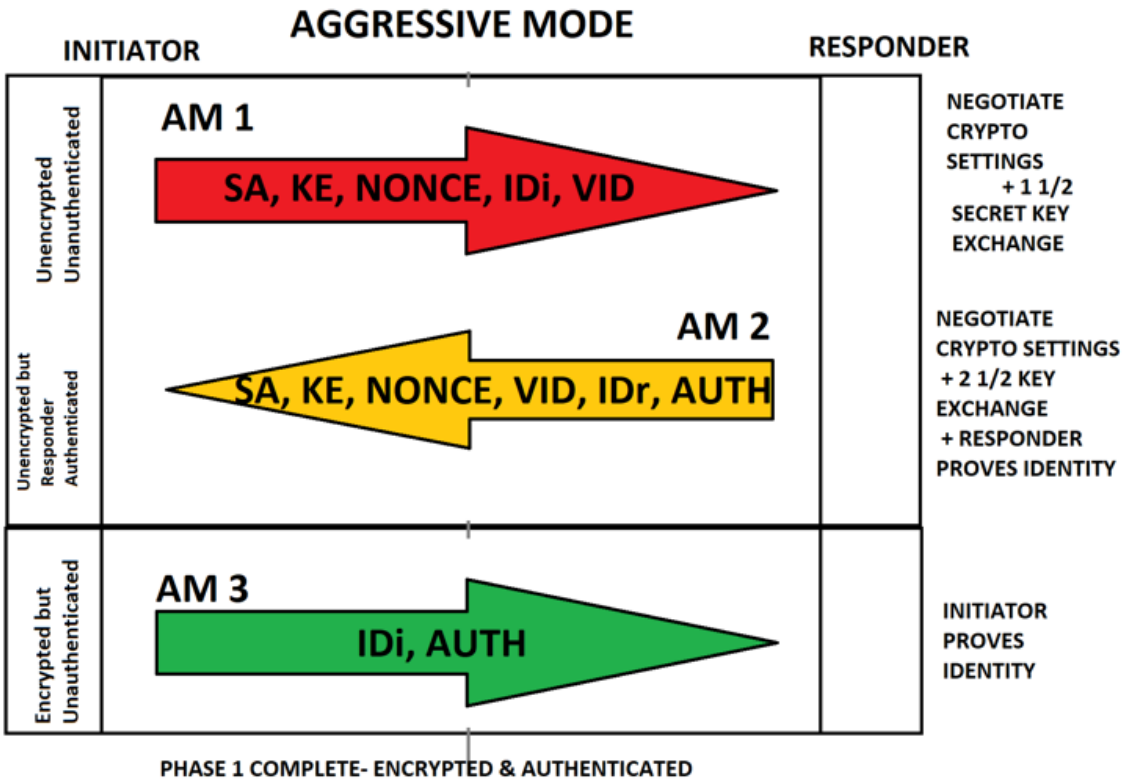


Aggressief Mode Packet Exchange

De agressieve modus beperkt de IKE SA onderhandeling in drie pakketten, waarbij alle gegevens vereist voor de SA door de initiator werden doorgegeven.

- De responder verstuurt het voorstel, het belangrijkste materiaal en de ID en echt de sessie in het volgende pakket.
- De initiatiefnemer antwoordt en verklaart de sessie echt.
- De onderhandelingen verlopen sneller en de initiator- en responder-ID gaan in de openbaarheid.

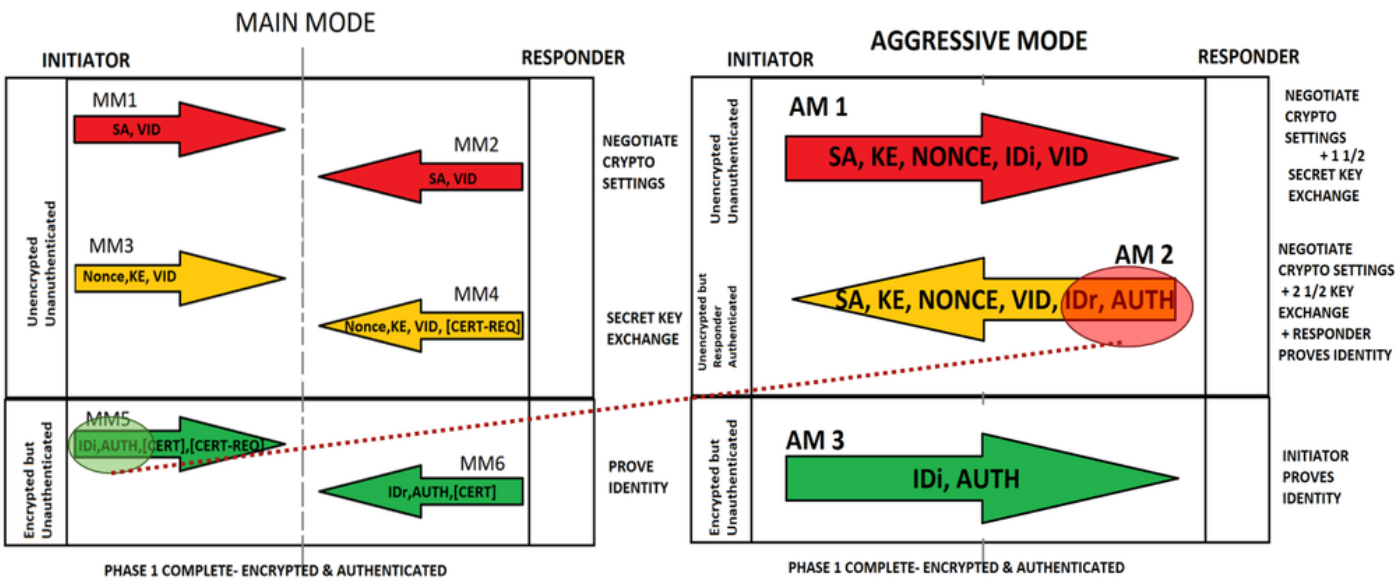
De afbeelding toont de lading-inhoud voor de drie pakketten die op Aggressieve modus worden uitgewisseld.



Belangrijkste modus vs. agressieve modus

Vergeleken met de hoofdmodus is de agressieve modus beperkt tot drie pakketten:

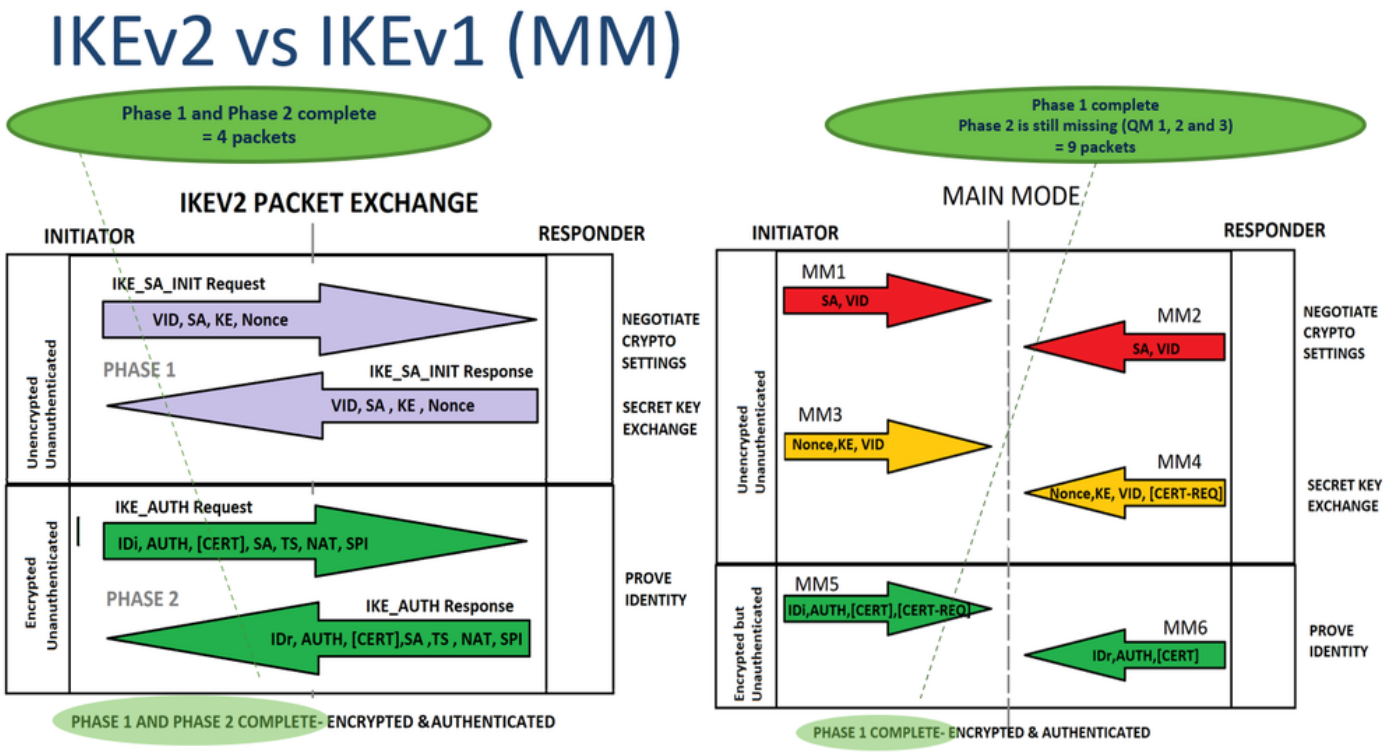
- AM 1 absorbeert M1 en M3
- AM 2 absorbeert M2, M4 en een deel van de MM6. Hier komt de kwetsbaarheid van de Aggressive Mode vandaan. AM 2 maakt het IDr en de niet-versleutelde verificatie op, in tegenstelling tot de hoofdmodus, is deze informatie versleuteld.
- AM 3 verstrekt de IDi en de verificatie, die waarden worden versleuteld.



IKEv2 vs IKEv1 Packet Exchange

In de IKEv2-onderhandeling worden minder berichten uitgewisseld om een tunnel op te zetten. IKEv2 gebruikt vier berichten; IKEv1 gebruikt zes berichten (in de hoofdmodus) of drie berichten (in agressieve modus).

De IKEv2-berichttypes worden gedefinieerd als "verzoek- en responspakketten". De afbeelding toont de pakketvergelijking en de payload-inhoud van IKEv2 versus IKEv1.



Opmerking: Dit document beschrijft niet dieper de IKEv2 Packet exchange. Voor meer

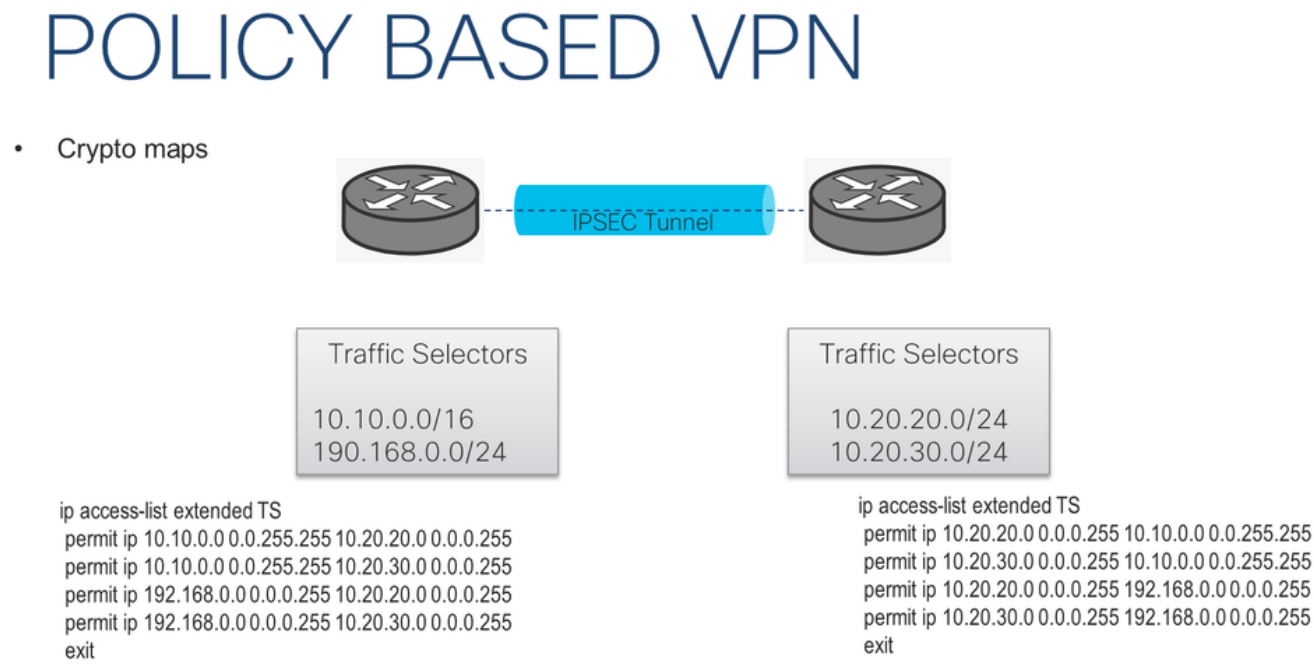
verwijzingen, navigeer naar IKEv2 Packet Exchange en Protocol Level Debugging.

Op beleid gebaseerde vs routegebaseerde

Op beleid gebaseerde VPN

Zoals de naam zegt, is een op beleid gebaseerd VPN **een IPsec VPN-tunnel** met een beleidsactie voor het transitverkeer dat voldoet aan de criteria om aan de criteria van het beleid te voldoen. In het geval van Cisco-apparaten wordt een toegangslijst (ACL) ingesteld en gekoppeld aan een crypto-kaart om het verkeer te specificeren dat opnieuw wordt gericht naar VPN en versleuteld.

De selectie van het verkeer zijn de subnetten of de gastheren die op het beleid zoals in het beeld worden getoond worden gespecificeerd.

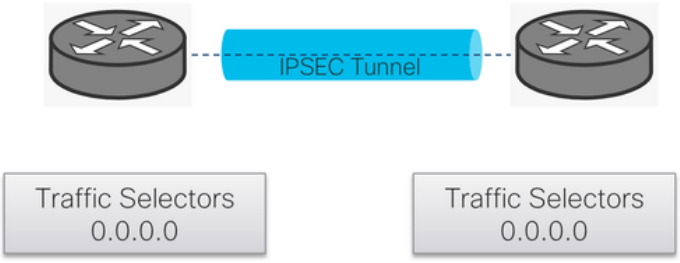


Routegebaseerde VPN

Een beleid is niet nodig en het verkeer wordt gericht naar de tunnels met routes en het ondersteunt dynamische routing via de tunnelinterface. De verkeerselectie (verkeer versleuteld via VPN) is standaard van 0.0.0.0 tot 0.0.0.0 zoals in de afbeelding.

ROUTE BASED VPN

- Supports dynamic routing over the tunnel interface.




```
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)
```

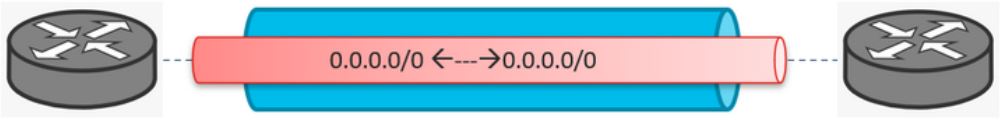
Opmerking: Wegens de selectie van het verkeer 0.0.0.0 is, om het even welke gastheer of Subnet binnen, daarom, slechts één SA gecreëerd. Er is een uitzondering voor Dynamische tunnel. Dit document beschrijft geen dynamische tunnels.

Het beleid en op route gebaseerde VPN kunnen worden verwezenlijkt zoals in de afbeelding.

ISAKMP-IPSEC Tunnel

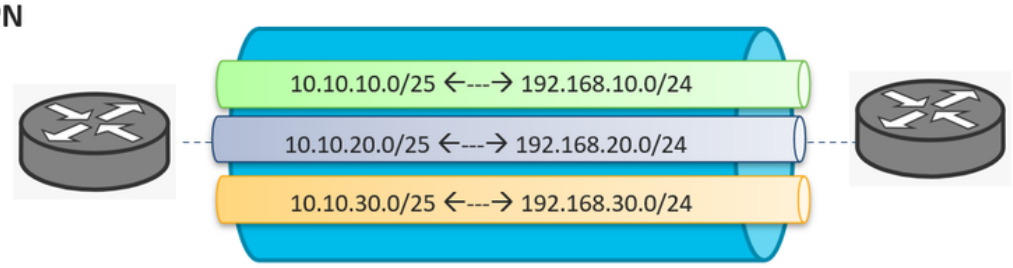
Route based VPN

*** Edges only support this.



Policy based VPN

- IOS - XE
- ASA
- FTD
- 3rd party devices



.

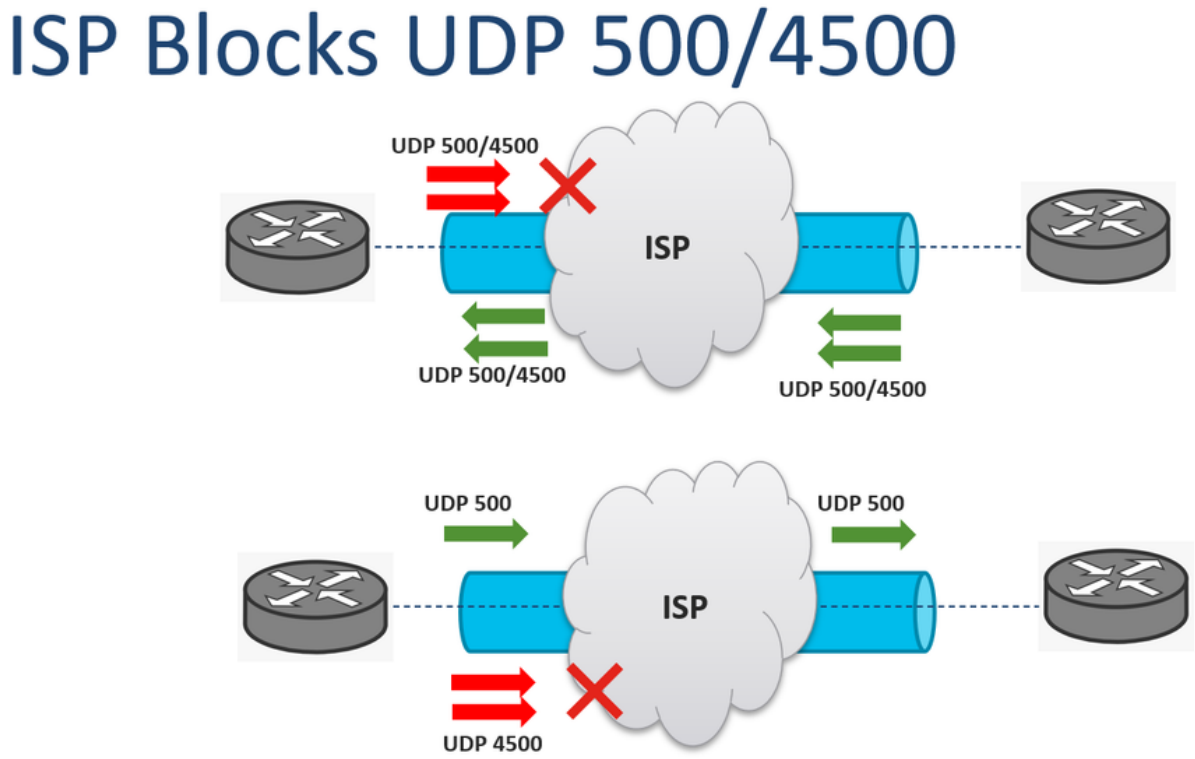
Opmerking: In tegenstelling tot op de route gebaseerde VPN met slechts één SA gecreëerd, kan op het beleid gebaseerde VPN multiples SA creëren. Als ACL wordt ingesteld, creëert elke verklaring op ACL (als deze verschillend is) een subtunnel.

Gemeenschappelijke problemen voor verkeer worden niet via VPN ontvangen

ISP-blokkeringen UDP 500/4500

Het is een veel voorkomend probleem dat de Internet Services Provider (ISP) de UDP 500/4500-poorten blokkeert. Voor een IPsec-tunnelvestiging kunnen twee verschillende ISP's worden ingeschakeld en één van hen kan de poorten blokkeren en de andere kan hen toestaan.

De afbeelding toont de twee scenario's waarin een ISP de UDP 500/4500-poorten in slechts één richting kan blokkeren.



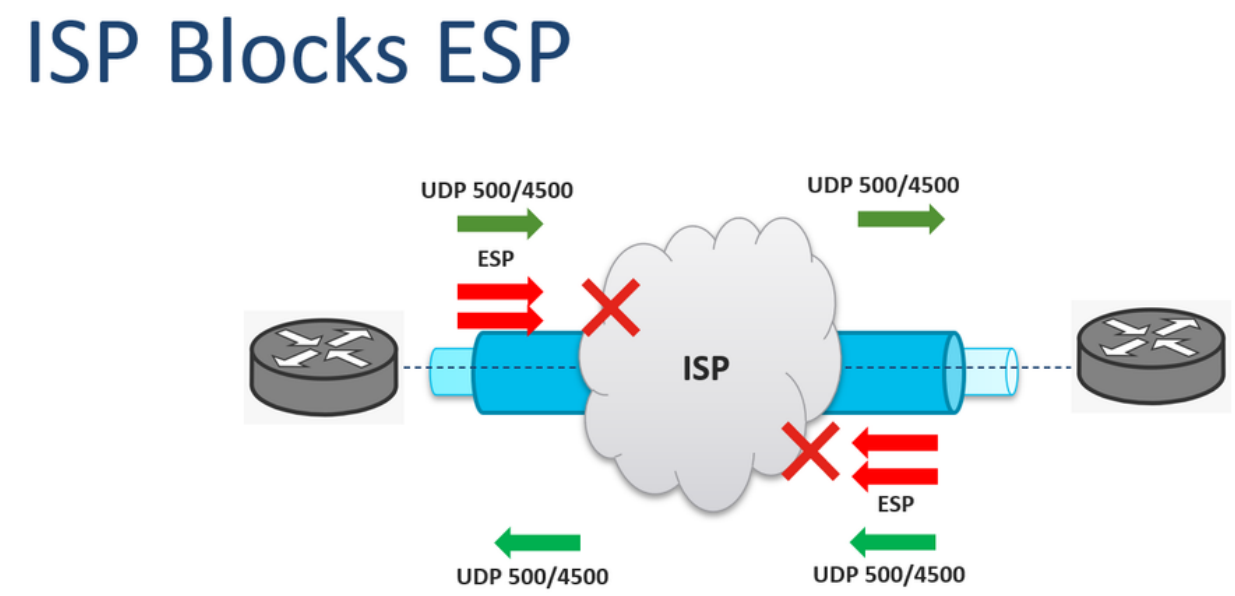
Opmerking: Port UDP 500 wordt door de Internet Key Exchange (IKE) gebruikt voor het opzetten van beveiligde VPN-tunnels. UDP 4500 wordt gebruikt wanneer NAT aanwezig is op één VPN-eindpunt.

Opmerking: Wanneer de ISP UDP 500/4500 blokkeert, wordt de IPsec-tunnelvestiging beïnvloed en staat het niet op.

ISP-blokkades ESP

Een ander veel voorkomend probleem in IPsec-tunnels is dat de ISP het ESP-verkeer blokkeert,

maar dat het UDP 500/4500-poorten toestaat. Een voorbeeld: de UDP 500/4500-poorten zijn toegestaan op bidirectionele manieren. Daarom wordt de tunnel geconstrueerd, maar de ESP-pakketten worden in beide richtingen geblokkeerd door de ISP of ISP's, waardoor het versleutelde verkeer via VPN niet verloopt zoals in de afbeelding.



Opmerking: Wanneer de ISP ESP-pakketten blokkeert, is de IPsec-tunnelvestiging geslaagd, maar het versleutelde verkeer wordt beïnvloed. Dat kun je met VPN doorgeven, maar het verkeer werkt er niet overheen.

Tip: Het scenario waarin het ESP-verkeer alleen in één richting wordt geblokkeerd, kan ook aanwezig zijn, de symptomen zijn hetzelfde maar kunnen gemakkelijk worden gevonden met de informatie over de tunnelstatistieken, de insluiting, de decapsultietellers of de TX-tellers.

Gerelateerde informatie

- KEv2 Packet Exchange en Protocol-niveau
- Internet Key Exchange (IKE) - RFC 2409
- Internet Key Exchange (IKEv2)-protocol
- Technische ondersteuning en documentatie – Cisco Systems