Verständnis des IPsec IKEv1-Protokolls

Inhalt

Einleitung

In diesem Dokument wird der IKEv1-Protokollprozess (Internet Key Exchange) für eine VPN-Einrichtung (Virtual Private Network) beschrieben, um den Paketaustausch zu verstehen und so die Fehlerbehebung für alle Arten von IPsec-Problemen mit IKEv1 zu vereinfachen.

Unterstützt von Amanda Nava, Cisco TAC Engineer.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse der grundlegenden Sicherheitskonzepte zu verfügen:

- Authentifizierung
- Vertraulichkeit
- Integrität
- IPsec

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

IPsec

IPsec ist eine Suite von Protokollen, die die Sicherheit der Internetkommunikation auf der IP-Ebene bietet. Die gängigste aktuelle Verwendung von IPsec besteht in der Bereitstellung eines Virtual Private Network (VPN), entweder zwischen zwei Standorten (Gateway-to-Gateway) oder zwischen einem Remote-Benutzer und einem Unternehmensnetzwerk (Host-zu-Gateway).

IKE-Protokoll

IPsec verwendet das IKE-Protokoll, um sichere Site-to-Site- oder Remote Access Virtual Private Network (VPN)-Tunnel auszuhandeln und einzurichten. Das IKE-Protokoll wird auch als Internet Security Association and Key Management Protocol (ISAKMP) bezeichnet (nur in Cisco).

Es gibt zwei Versionen von IKE:

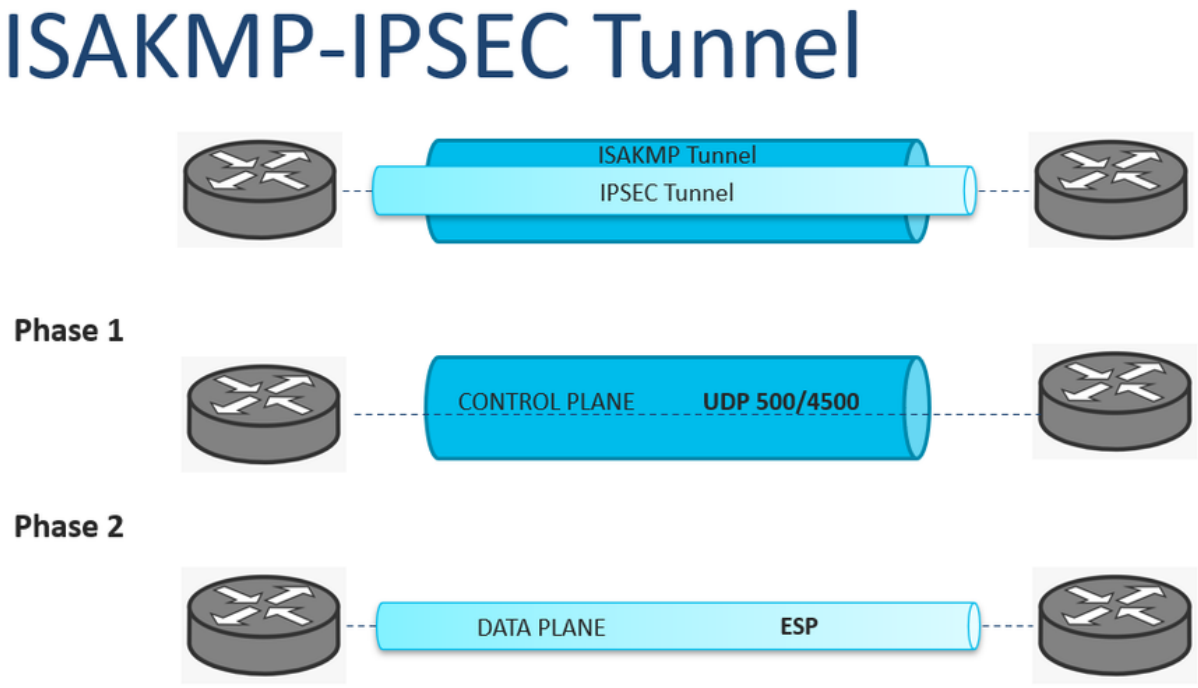
- IKEv1: Definiert in RFC 2409, The Internet Key Exchange
- IKE-Version 2 (IKEv2): Definiert in RFC 4306, Internet Key Exchange (IKEv2) Protocol

IKE-Phasen

ISAKMP trennt die Aushandlung in zwei Phasen:

- Phase 1: Die beiden ISAKMP-Peers stellen einen sicheren und authentifizierten Tunnel her, der ISAKMP-Verhandlungsnachrichten schützt. Dieser Tunnel wird als ISAKMP SA bezeichnet. ISAKMP definiert zwei Modi: Hauptmodus (MM) und aggressiver Modus.
- Phase 2: Es handelt wichtige Materialien und Algorithmen für die Verschlüsselung (SAs) der Daten aus, die über den IPsec-Tunnel übertragen werden sollen. Diese Phase wird als Quick Mode (Schnellmodus) bezeichnet.

Um alle abstrakten Konzepte zu verwirklichen, ist der Phase-1-Tunnel der Parent-Tunnel und Phase 2 ein Subtunnel. Dieses Bild veranschaulicht die beiden Phasen als Tunnel.



Anmerkung: Der ISAKMP-Tunnel (Phase 1) schützt den Control Plante VPN-Datenverkehr zwischen den beiden Gateways. Kontrollebenen-Datenverkehr kann Verhandlungspakete, Informationspakete, DPD, Keepalives, rekey usw. ISAKMP-Aushandlung verwendet die UDP 500- und 4500-Ports, um einen sicheren Kanal einzurichten.

Anmerkung: Phase-2-Tunnel (IPsec) schützt den Datenebenenverkehr, der das VPN zwischen den beiden Gateways durchläuft. TDie zum Schutz der Daten verwendeten Algorithmen werden in Phase 2 konfiguriert und sind unabhängig von den in Phase 1 angegebenen Algorithmen.
Das Protokoll zur Kapselung und Verschlüsselung dieser Pakete ist die Encapsulation Security Payload (ESP).

IKE-Modi (Phase 1)

Hauptmodus

Eine IKE-Sitzung beginnt, wenn der Initiator dem Teilnehmer ein Angebot oder einen Vorschlag sendet. Beim ersten Austausch zwischen Knoten werden die grundlegenden Sicherheitsrichtlinien festgelegt. Der Initiator schlägt die zu verwendenden Verschlüsselungs- und Authentifizierungsalgorithmen vor. Der Befragte wählt den geeigneten Vorschlag (wir gehen davon aus, dass ein Vorschlag ausgewählt ist) und sendet ihn an den Initiator. Beim nächsten Austausch werden öffentliche Diffie-Hellman-Schlüssel und andere Daten übergeben. Alle weiteren Verhandlungen werden innerhalb der IKE SA verschlüsselt. Der dritte Austausch authentifiziert die ISAKMP-Sitzung. Sobald die IKE SA eingerichtet ist, beginnt die IPSec-Aushandlung (Quick Mode).

Aggressive Mode

Der aggressive Modus zwingt die IKE SA-Aushandlung in drei Pakete, wobei alle für die SA erforderlichen Daten vom Initiator übergeben werden. Der Responder sendet das Angebot, das Schlüsselmaterial und die ID und authentifiziert die Sitzung im nächsten Paket. Der Initiator antwortet und authentifiziert die Sitzung. Die Verhandlung ist schneller, und die Initiator- und Responder-ID werden klar übertragen.

IPsec-Modus (Phase 2)

Quick-Mode

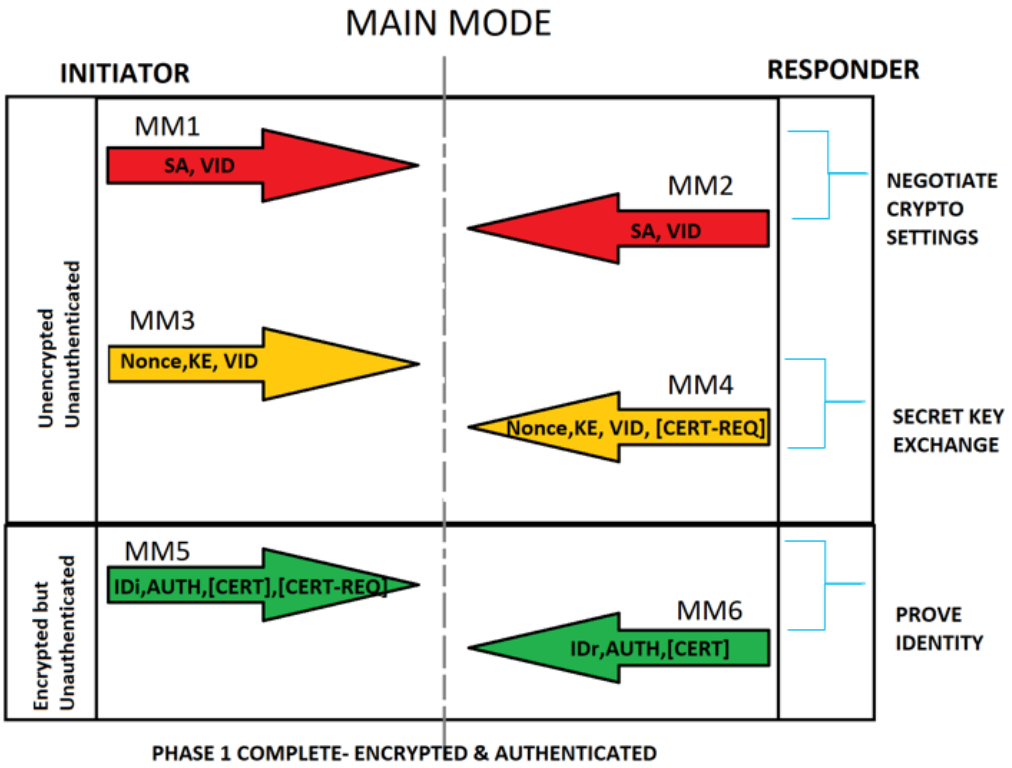
IPSec-Aushandlung oder Quick Mode ähnelt einer Aggressive Mode IKE-Aushandlung (mit Ausnahme der Aushandlung), muss innerhalb einer IKE SA geschützt werden. Im Schnellmodus wird die SA für die Datenverschlüsselung ausgehandelt und der Schlüsselaustausch für diese IPSec SA verwaltet.

IKE-Glossar

- Eine **Sicherheitszuordnung** (**SA**) ist die Einrichtung gemeinsamer Sicherheitsattribute zwischen zwei Netzwerkentitäten zur Unterstützung der sicheren Kommunikation. Ein SA umfasst Attribute wie Verschlüsselungsalgorithmus und -modus. Verschlüsselungsschlüssel für den Datenverkehr; und Parameter für die Netzwerkdaten, die über die Verbindung weitergegeben werden sollen.
- Die **Anbieter-IDs** (**VID**) werden verarbeitet, um festzustellen, ob der Peer die Funktion NAT-Traversal, Dead Peer Detection, Fragmentation usw. unterstützt.
- **Einmal**: eine zufällig generierte Nummer, die der Initiator sendet. Diese Nonce wird zusammen mit den anderen Artikeln mit dem vereinbarten Schlüssel gehasht und zurückgesendet. Der Initiator überprüft das Cookie und die Nonce und lehnt alle Nachrichten ab, die nicht einmal das Recht haben. Dies hilft, eine Wiederholung zu verhindern, da kein Dritter vorhersagen kann, was die Zufallsgenerierung ist.
- **Key-Exchange (KE)**-Informationen für den sicheren Schlüsselaustauschprozess Diffie-Hellman (DH).
- **Identitätsinitiator/-Responder (IDi/IDr.)** wird verwendet, um Authentifizierungsinformationen an den Peer zu senden. Diese Informationen werden unter dem Schutz des gemeinsamen geheimen Geheimnisses übermittelt.
- **Der Diffie-Hellman (DH)-Schlüsselaustausch ist eine Methode zum sicheren Austausch kryptografischer Algorithmen über einen öffentlichen Kanal.**
- Der gemeinsam genutzte IPSec-Schlüssel kann mit der DH abgeleitet werden, die erneut verwendet wird, um **Perfect Forward Secrecy (PFS)** oder den ursprünglichen DH-Austausch, der auf den zuvor abgeleiteten gemeinsamen geheimen Schlüssel aktualisiert wurde, zu gewährleisten.

Paketaustausch im Hauptmodus

Jedes ISAKMP-Paket enthält Payload-Informationen für die Tunneleinrichtung. Im IKE-Glossar werden die IKE-Abkürzungen als Teil des Payload-Inhalts für den Paketaustausch im Hauptmodus erläutert, wie in diesem Bild gezeigt.

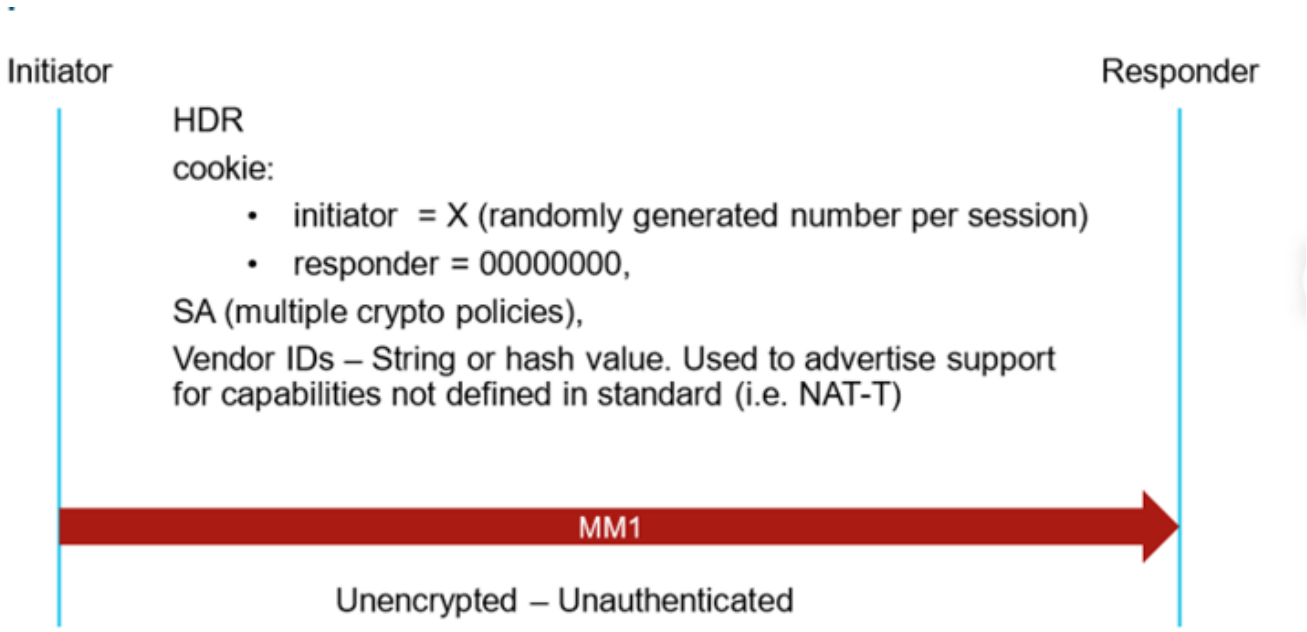


Hauptmodus 1 (MM1)

Um die Bedingungen für die ISAKMP-Verhandlungen festzulegen, erstellen Sie eine ISAKMP-Richtlinie, die Folgendes beinhaltet:

- Eine Authentifizierungsmethode, um die Identität der Peers sicherzustellen.
- Eine Verschlüsselungsmethode zum Schutz der Daten und zum Schutz der Privatsphäre.
- Eine Hashed Message Authentication Codes (HMAC)-Methode, um die Identität des Absenders sicherzustellen und sicherzustellen, dass die Nachricht bei der Übertragung nicht geändert wurde.
- Eine Diffie-Hellman-Gruppe, um die Stärke des Algorithmus zur Bestimmung des Verschlüsselungsschlüssels zu bestimmen. Die Sicherheits-Appliance verwendet diesen Algorithmus, um die Verschlüsselungs- und Hash-Schlüssel abzuleiten.
- Eine Beschränkung der Zeit, in der die Sicherheits-Appliance einen Verschlüsselungsschlüssel verwendet, bevor er ersetzt wird.

Das erste Paket wird vom Initiator der IKE-Aushandlung gesendet, wie im Bild gezeigt.



Anmerkung: Der Hauptmodus 1 ist das erste Paket der IKE-Aushandlung. Daher wird der Initiator-SPI auf einen Zufallswert gesetzt, während der Responder-SPI auf 0 festgelegt ist. Im zweiten Paket (MM2) muss der Responder-SPI mit einem neuen Wert beantwortet werden, und die gesamte Aushandlung behält die gleichen SPI-Werte bei.

Wenn das MM1 erfasst wird und ein Wireshark-Netzwerkprotokollanalyzer verwendet wird, befindet sich der SPI-Wert innerhalb der Internetsicherheitszuordnung und des Schlüsselverwaltungsprotokolls, wie im Bild gezeigt.

```
> 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)
```

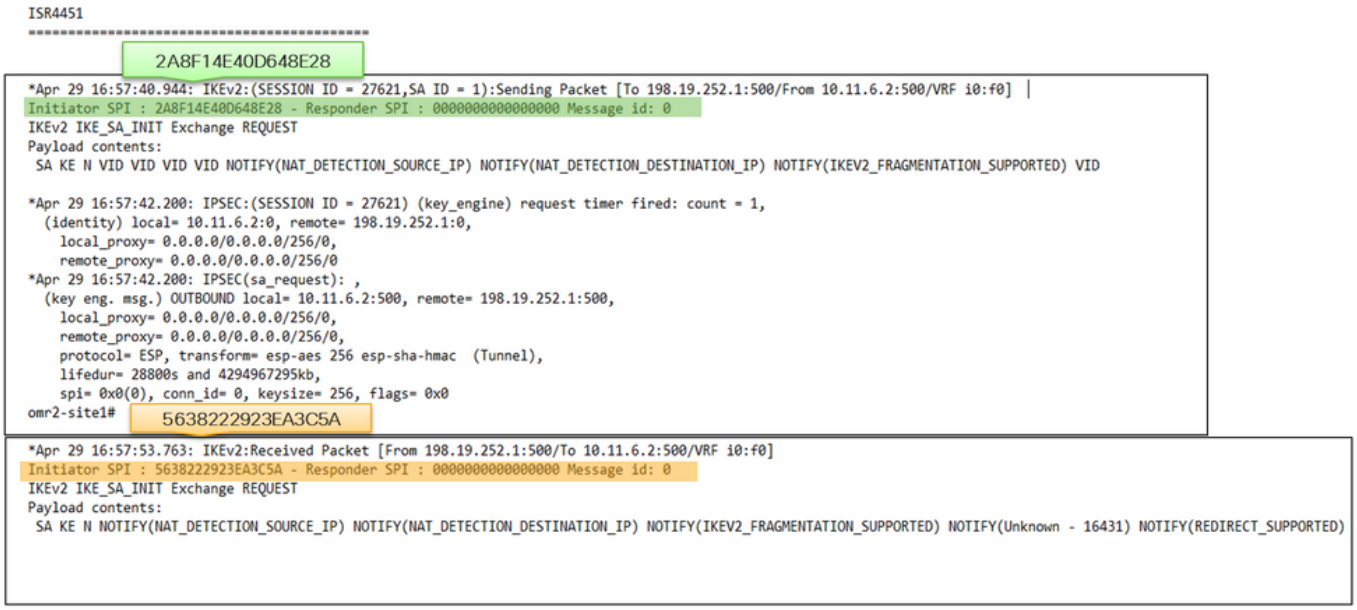
Anmerkung: Falls das MM1-Paket im Pfad verloren geht oder keine MM2-Antwort vorliegt, behält die IKE-Aushandlung die MM1-Neuübertragungen bei, bis die maximale Anzahl von Neuübertragungen erreicht ist. An diesem Punkt behält der Initiator den gleichen SPI bei, bis die nächste Aushandlung erneut ausgelöst wird.

Tipp: Die Identifizierung von Initiator- und Responder-SPIs ist sehr hilfreich, um mehrere Verhandlungen für dasselbe VPN zu identifizieren und einige Verhandlungsprobleme einzugrenzen.

Identifizieren von zwei gleichzeitigen Verhandlungen

Auf den Cisco IOS® XE-Plattformen können die Debug-Vorgänge pro Tunnel mit einer Bedingung für die konfigurierte Remote-IP-Adresse gefiltert werden. Die gleichzeitigen Aushandlungen werden jedoch in den Protokollen angezeigt, und es ist nicht möglich, sie zu filtern. Dies muss manuell durchgeführt werden. Wie bereits erwähnt, behält die gesamte Aushandlung dieselben SPI-Werte für Initiator und Responder bei. Falls ein Paket von derselben Peer-IP-Adresse

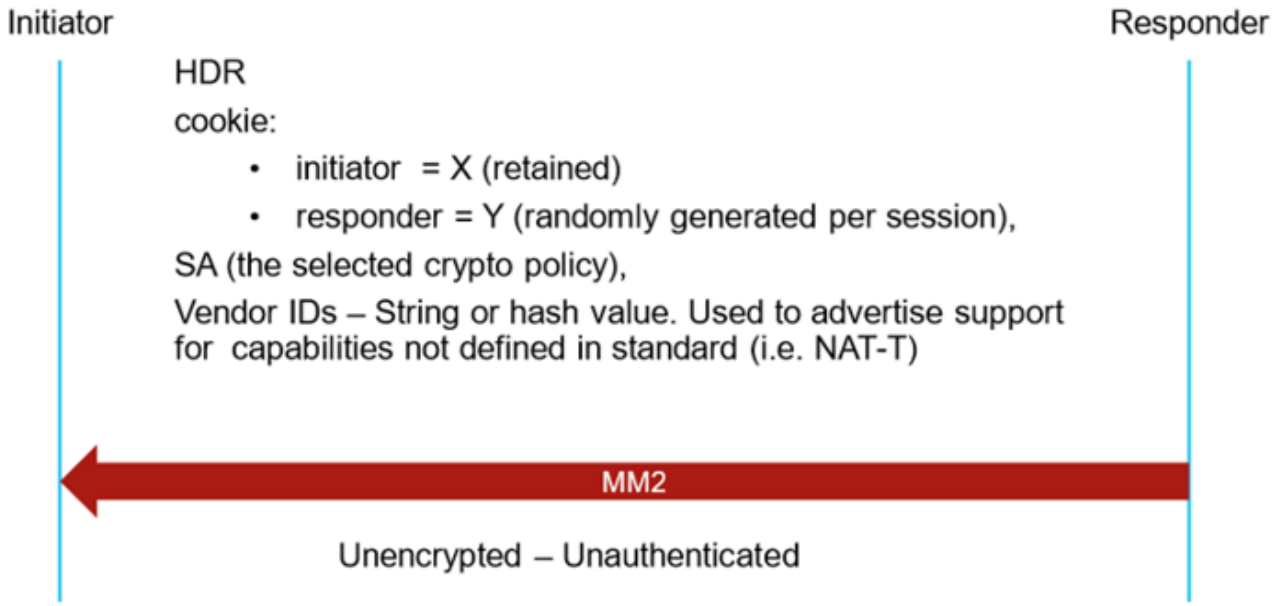
empfangen wird, das SPI jedoch nicht mit dem zuvor verfolgten Wert übereinstimmt, bevor die Aushandlung die maximale Anzahl an Weiterleitungen erreicht, ist dies eine weitere Aushandlung für denselben Peer wie im Bild dargestellt.



> **Anmerkung:** Das Beispiel zeigt die gleichzeitige Aushandlung für das erste Paket in der Aushandlung (MM1). Dies kann jedoch an jedem Aushandlungspunkt erfolgen. Alle nachfolgenden Pakete müssen einen Wert enthalten, der sich von 0 für den SPI des Responders unterscheidet.

Hauptmodus 2 (MM2)

Im Paket für den Hauptmodus 2 sendet der Responder die ausgewählte Richtlinie für die übereinstimmenden Vorschläge, und der SPI des Responders wird auf einen zufälligen Wert festgelegt. Die gesamte Aushandlung behält die gleichen SPIs-Werte bei. Der MM2 antwortet auf MM1, und der SPI-Responder wird auf einen anderen Wert als 0 gesetzt, wie im Bild gezeigt.



Wenn das MM2 erfasst wird und ein Wireshark-Netzwerkprotokollanalyzer verwendet wird, befinden sich die SPI-Werte für den Initiator und den Responder in der Internet Security Association und im Key Management Protocol, wie im Bild gezeigt.

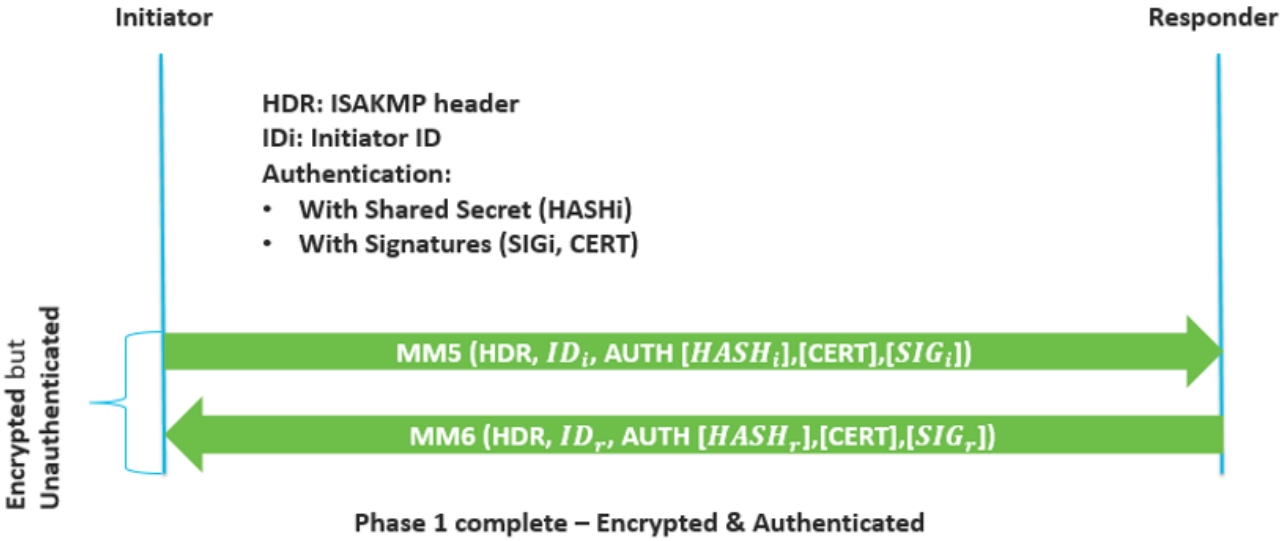
```
> Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
> Internet Protocol Version 4, Src: 209.134.162.150, Dst: 170.49.116.200
> User Datagram Protocol, Src Port: 500, Dst Port: 500
v Internet Security Association and Key Management Protocol
    Initiator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

Hauptmodus 3 und 4 (MM3-MM4)

Die MM3- und MM4-Pakete sind noch nicht verschlüsselt und nicht authentifiziert, und der geheime Schlüsselaustausch findet statt. MM3 und MM4 werden im Bild angezeigt.

Hauptmodus 5 und 6 (MM5-MM6)

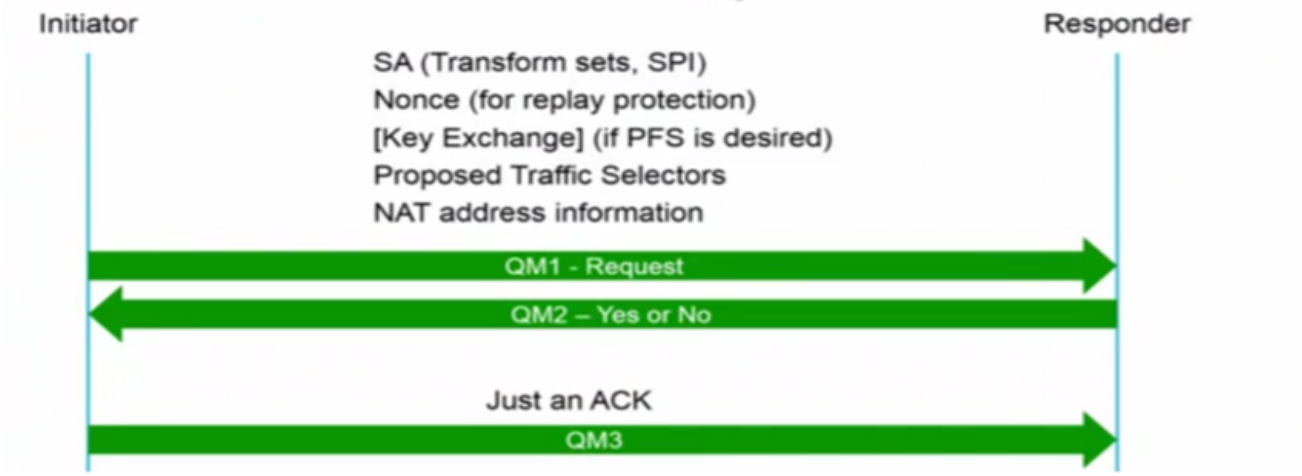
Die MM5- und MM6-Pakete sind bereits verschlüsselt, aber noch nicht authentifiziert. Bei diesen Paketen erfolgt die Authentifizierung, wie im Bild gezeigt.



Quick Mode (QM1, QM2 und QM3)

Der Quick-Modus tritt ein, nachdem der Hauptmonde und IKE den sicheren Tunnel in Phase 1 eingerichtet haben. Im Schnellmodus wird die gemeinsame IPSec-Richtlinie für die IPSec-Sicherheitsalgorithmen ausgehandelt und der Schlüsselaustausch für die IPSec SA-Einrichtung verwaltet. Die Nonces werden verwendet, um neues gemeinsam genutztes geheimes Schlüsselmaterial zu generieren und Replay-Angriffe durch falsche SAs zu verhindern.

In dieser Phase werden drei Pakete ausgetauscht, wie im Bild gezeigt.

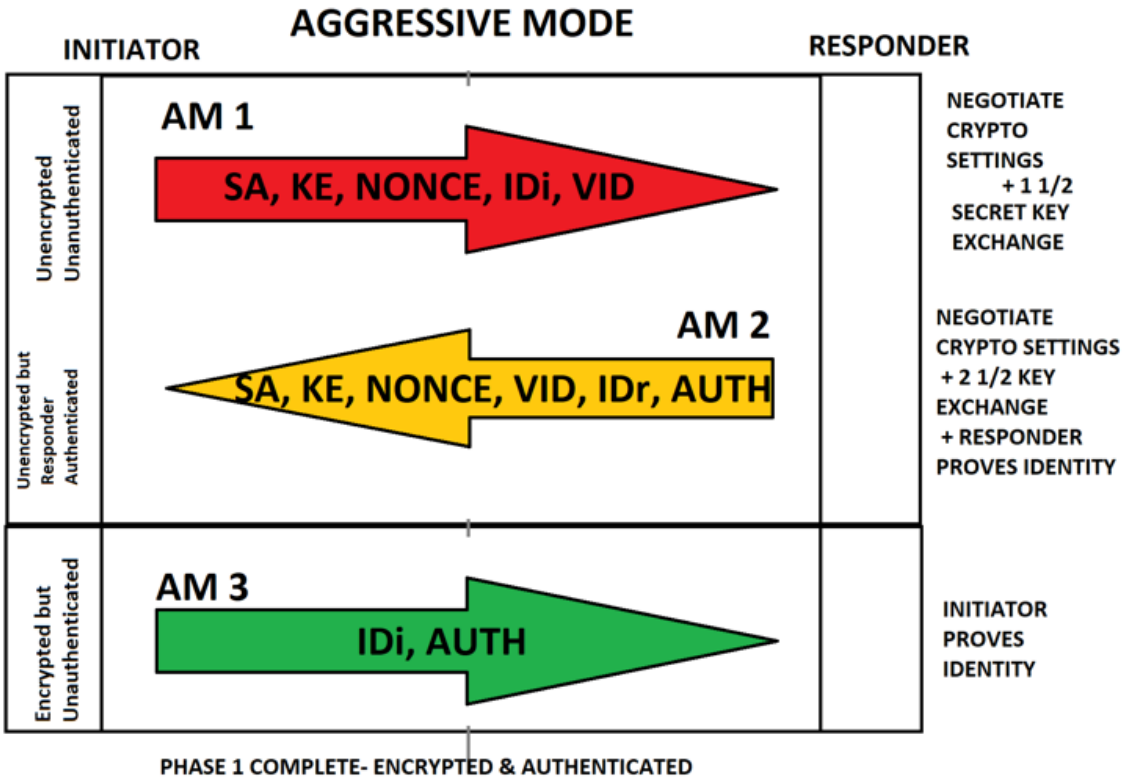


Aggressive Mode Packet Exchange

Im aggressiven Modus wird die IKE SA-Aushandlung in drei Pakete zusammengefasst, wobei alle für die SA erforderlichen Daten vom Initiator übergeben werden.

- Der Responder sendet das Angebot, das Schlüsselmaterial und die ID und authentifiziert die Sitzung im nächsten Paket.
- Der Initiator antwortet und authentifiziert die Sitzung.
- Die Verhandlung ist schneller, und die Initiator- und Responder-ID werden klar übertragen.

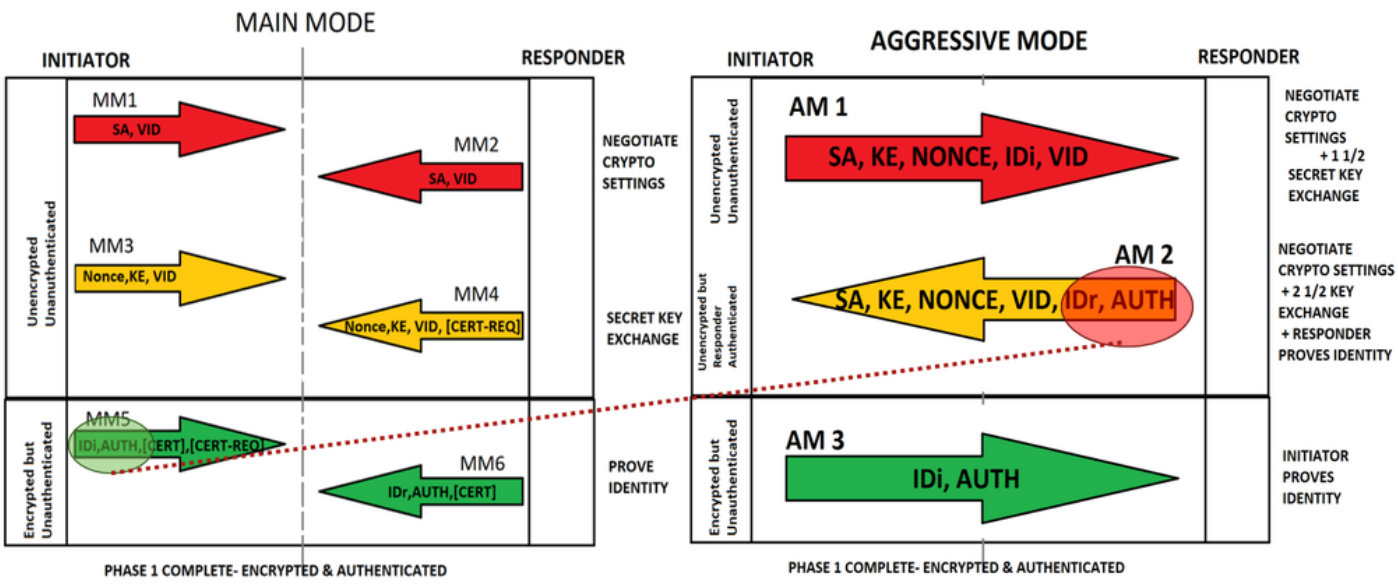
Das Bild zeigt den Payload-Inhalt für die drei im aggressiven Modus ausgetauschten Pakete.



Hauptmodus vs. aggressiver Modus

Im Vergleich zum Hauptmodus wird der aggressive Modus auf drei Pakete reduziert:

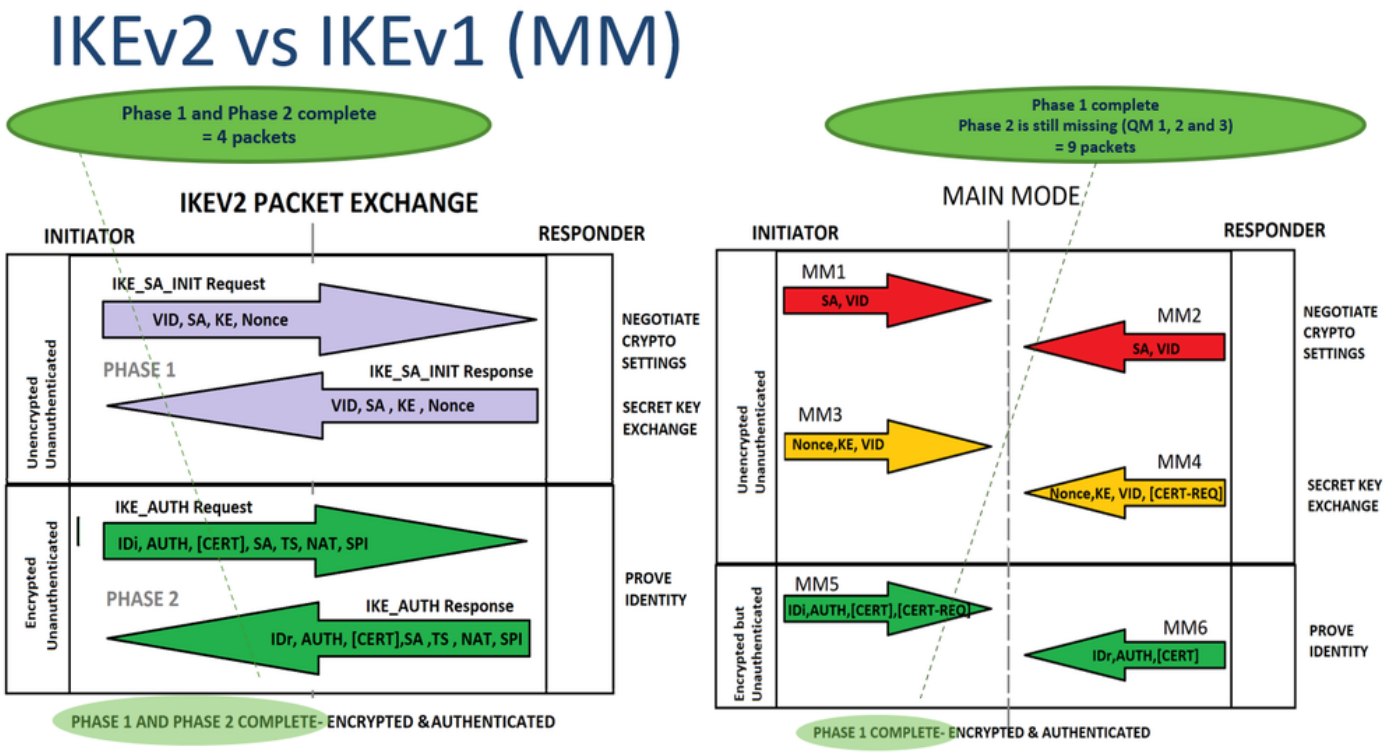
- AM 1 absorbiert MM1 und MM3
- AM 2 absorbiert MM2, MM4 und einen Teil des MM6. Hier kommt die Schwachstelle des aggressiven Modus hervor. Der AM 2 stellt die IDr. und die Authentifizierung unverschlüsselt dar, im Gegensatz zum Hauptmodus werden diese Informationen verschlüsselt.
- AM 3 stellt die IDi und die Authentifizierung bereit. Diese Werte werden verschlüsselt.



IKEv2 und IKEv1-Paketaustausch

Bei der IKEv2-Aushandlung werden weniger Nachrichten ausgetauscht, um einen Tunnel einzurichten. IKEv2 verwendet vier Nachrichten; IKEv1 verwendet entweder sechs Nachrichten (im Hauptmodus) oder drei Nachrichten (im aggressiven Modus).

Die IKEv2-Meldungstypen werden als Anforderungs- und Antwortpaare definiert. Das Bild zeigt den Paketvergleich und den Payload-Inhalt von IKEv2 und IKEv1.



Anmerkung: In diesem Dokument wird der IKEv2-Paketaustausch nicht genauer

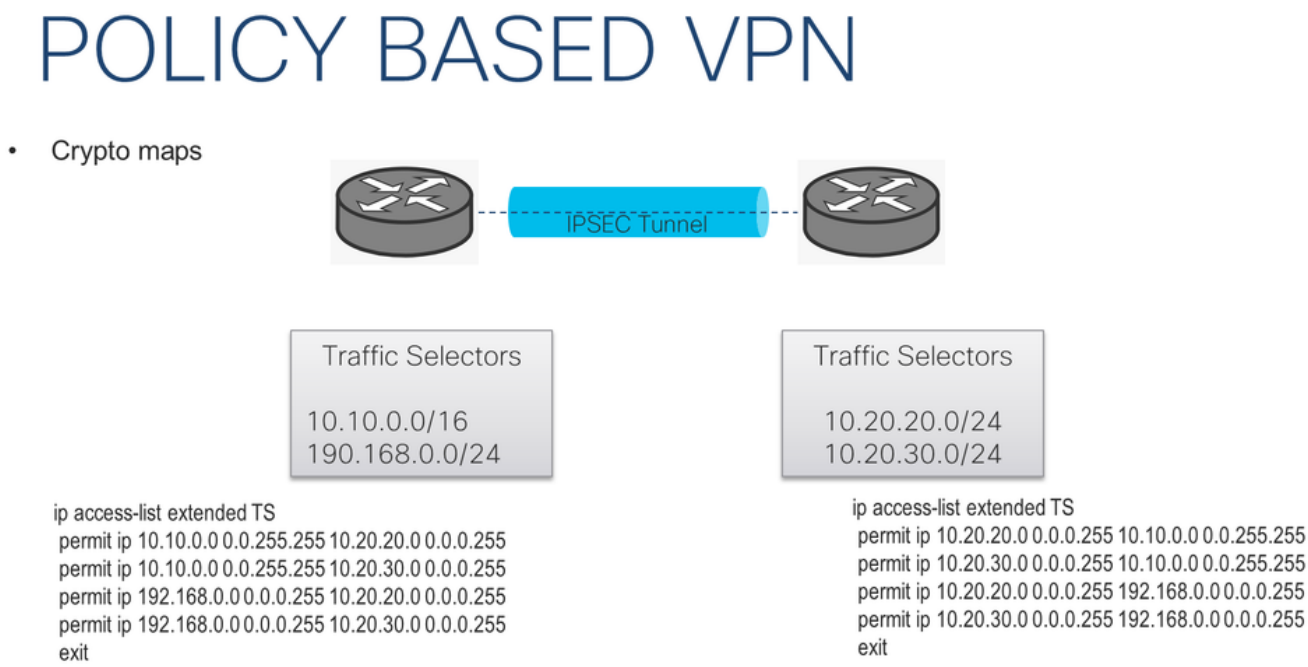
beschrieben. Weitere Referenzen finden Sie unter Debuggen auf IKEv2-Paketaustausch und Protokollebene.

Richtlinienbasiert und routen-basiert

Richtlinienbasiertes VPN

Wie der Name schon sagt, ist ein richtlinienbasiertes VPN **ein IPsec-VPN-Tunnel** mit einer Richtlinienaktion für den Transitverkehr, der die Anpassungskriterien der Richtlinie erfüllt. Bei Cisco Geräten wird eine Zugriffsliste (Access List, ACL) konfiguriert und mit einer Crypto Map (Crypto Map) verbunden, um den an das VPN umzuleitenden und verschlüsselten Datenverkehr anzugeben.

Bei den Datenverkehrsauswählern handelt es sich um die in der Richtlinie angegebenen Subnetze oder Hosts, wie im Bild gezeigt.

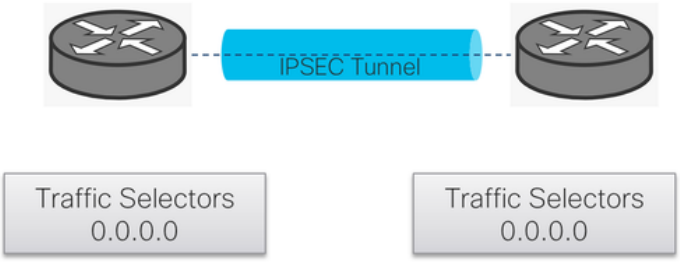


Routenbasiertes VPN

Eine Richtlinie ist nicht erforderlich, und der Datenverkehr wird an die Tunnel mit Routen umgeleitet. Sie unterstützt dynamisches Routing über die Tunnelschnittstelle. Die Datenverkehrsauswahl (über das VPN verschlüsselter Datenverkehr) ist bei 0.0.0.0. auf 0.0.0.0 setzen, wie im Bild gezeigt.

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)
```

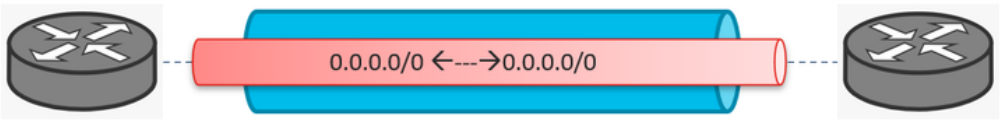
Anmerkung: Da die Traffic-Auswahloptoren 0.0.0.0 sind, ist jeder Host oder jedes Subnetz im Lieferumfang enthalten, daher wird nur eine SA erstellt. Es gibt eine Ausnahme für Dynamic Tunnel. In diesem Dokument werden dynamische Tunnel nicht beschrieben.

Das richtlinienbasierte und das routen VPN können wie im Bild gezeigt materialisiert werden.

ISAKMP-IPSEC Tunnel

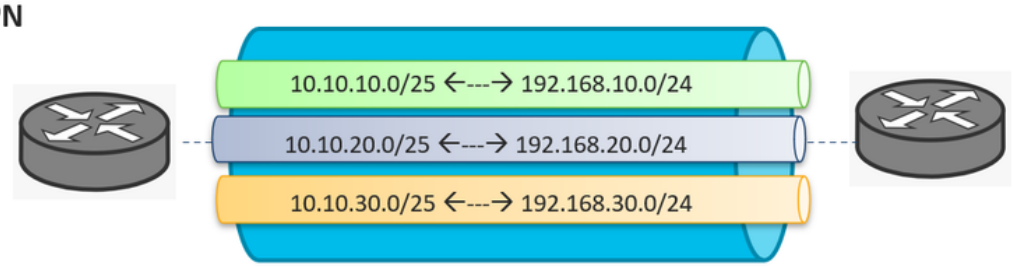
Route based VPN

*** Edges only support this.



Policy based VPN

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



.

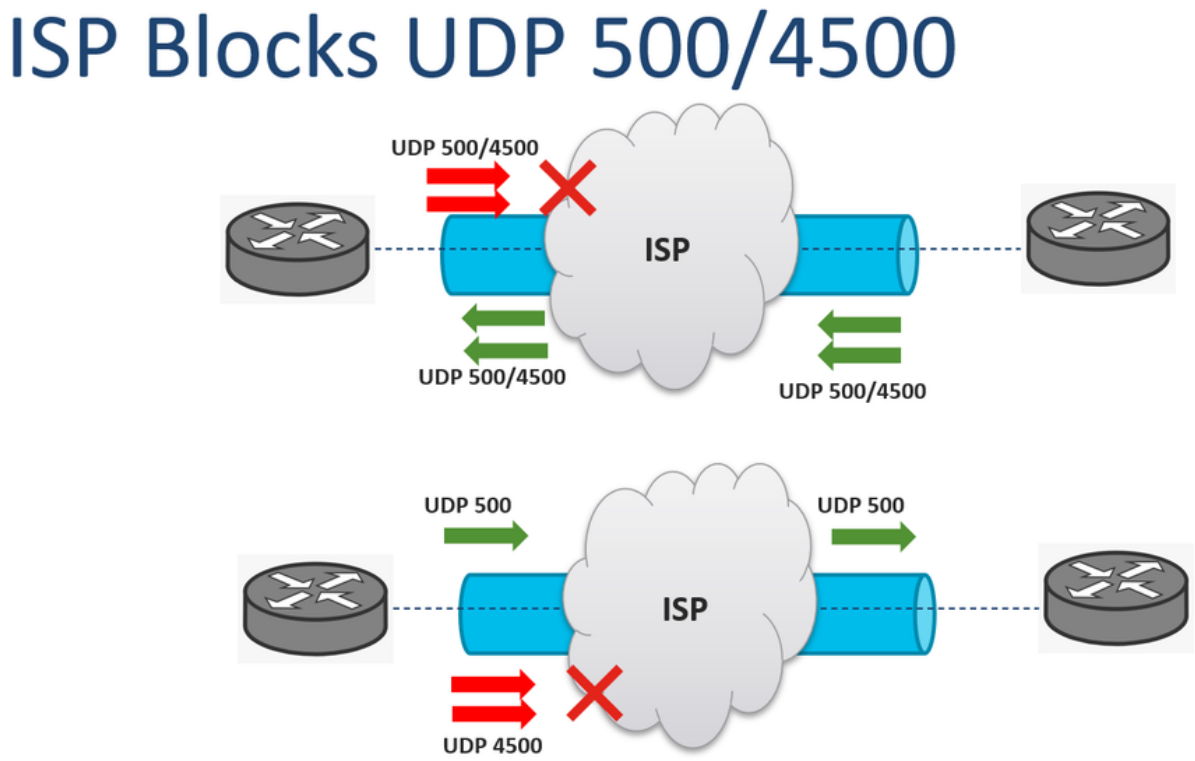
Anmerkung: Im Gegensatz zu einem routen-basierten VPN mit nur einem erstellten SA kann das richtlinienbasierte VPN mehrere SAs erstellen. Wenn eine ACL konfiguriert wird, erstellt jede Anweisung in der ACL (wenn sie sich von einer ACL unterscheidet) einen Sub-Tunnel.

Häufige Probleme beim Datenverkehr werden nicht über das VPN empfangen

ISP blockiert UDP 500/4500

Es ist ein sehr häufiges Problem, dass der Internet Services Provider (ISP) die UDP 500/4500-Ports blockiert. Bei einer IPsec-Tunneleinrichtung können zwei verschiedene ISPs aktiviert werden, von denen einer die Ports blockieren kann, der andere jedoch.

Das Bild zeigt die beiden Szenarien, in denen ein ISP die UDP 500/4500-Ports nur in eine Richtung blockieren kann.



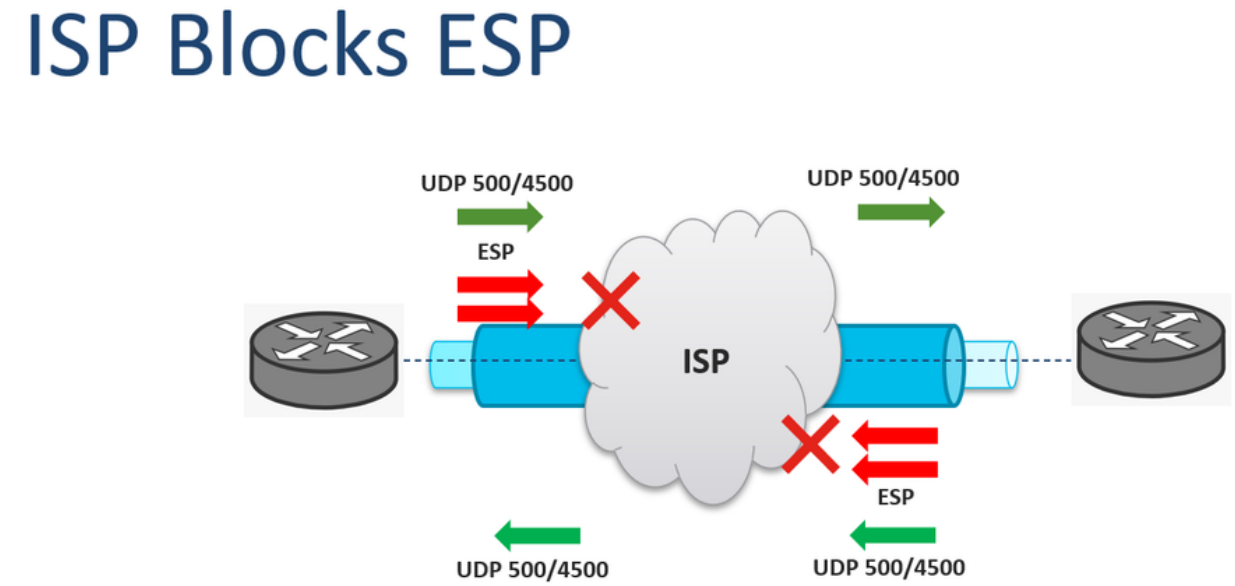
Anmerkung: Port UDP 500 wird vom Internet Key Exchange (IKE) für die Einrichtung sicherer VPN-Tunnel verwendet. UDP 4500 wird verwendet, wenn NAT auf einem VPN-Endpunkt vorhanden ist.

Anmerkung: Wenn der ISP das UDP 500/4500 blockiert, ist die IPsec-Tunneleinrichtung betroffen und nicht aktiv.

ISP blockiert ESP

Ein weiteres sehr häufiges Problem bei IPsec-Tunneln ist, dass der ISP den ESP-Datenverkehr

blockiert, jedoch die UDP 500/4500-Ports zulässt. Ein Beispiel: Die UDP 500/4500-Ports sind in bidirektionaler Weise zulässig. Der Tunnel ist also erfolgreich eingerichtet, aber die ESP-Pakete werden vom ISP oder ISP in beide Richtungen blockiert. Dies führt dazu, dass der verschlüsselte Datenverkehr durch das VPN fehlschlägt, wie im Bild gezeigt.



Anmerkung: Wenn der ISP ESP-Pakete blockiert, ist die IPsec-Tunneleinrichtung erfolgreich, der verschlüsselte Datenverkehr jedoch davon betroffen. Diese kann bei aktiviertem VPN wiedergegeben werden, der Datenverkehr funktioniert jedoch nicht.

Tipp: Das Szenario, in dem der ESP-Datenverkehr nur in eine Richtung blockiert wird, kann ebenfalls auftreten. Die Symptome sind dieselben, können jedoch leicht mit Informationen zu Tunnelstatistiken, Kapselungen, Entkapselungszählern oder RX- und TX-Zählern gefunden werden.

Zugehörige Informationen

- Debuggen von KEv2-Paket-Exchange und Protokollebene
- Internet Key Exchange (IKE) - RFC 2409
- Internet Key Exchange (IKEv2)-Protokoll
- Technischer Support und Dokumentation für Cisco Systeme