Comprensión del protocolo IPsec IKEv1

Contenido

Introducción

En este documento se describe el proceso del protocolo de intercambio de claves de Internet (IKEv1) para un establecimiento de red privada virtual (VPN).

Prerequisites

Requirements

Cisco recomienda que conozca los conceptos básicos de seguridad:

- Autenticación
- Confidencialidad
- Integridad
- IPsec

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

El proceso del protocolo de intercambio de claves de Internet (IKEv1) para un establecimiento de red privada virtual (VPN) es importante para comprender el intercambio de paquetes con el fin de solucionar de forma más sencilla cualquier tipo de problema de seguridad de protocolo de Internet (IPsec) con IKEv1.

IPsec

IPSec es un conjunto de protocolos que proporciona seguridad a las comunicaciones de Internet en la capa IP. El uso actual más común de IPsec es el de proporcionar una red privada virtual (VPN), ya sea entre dos ubicaciones (puerta de enlace a puerta de enlace) o entre un usuario remoto y una red empresarial (de host a puerta de enlace).

Protocolo IKE

IPSec utiliza el protocolo IKE para negociar y establecer túneles seguros de red privada virtual (VPN) de sitio a sitio o de acceso remoto. El protocolo IKE también se denomina protocolo ISAKMP (del inglés Internet Security Association and Key Management Protocol, asociación de seguridad de Internet y administración de claves) (solo en Cisco).

Hay dos versiones de IKE:

- IKEv1: definido en RFC 2409, Intercambio de claves de Internet
- IKE versión 2 (IKEv2): definido en RFC 4306, protocolo de intercambio de claves de Internet

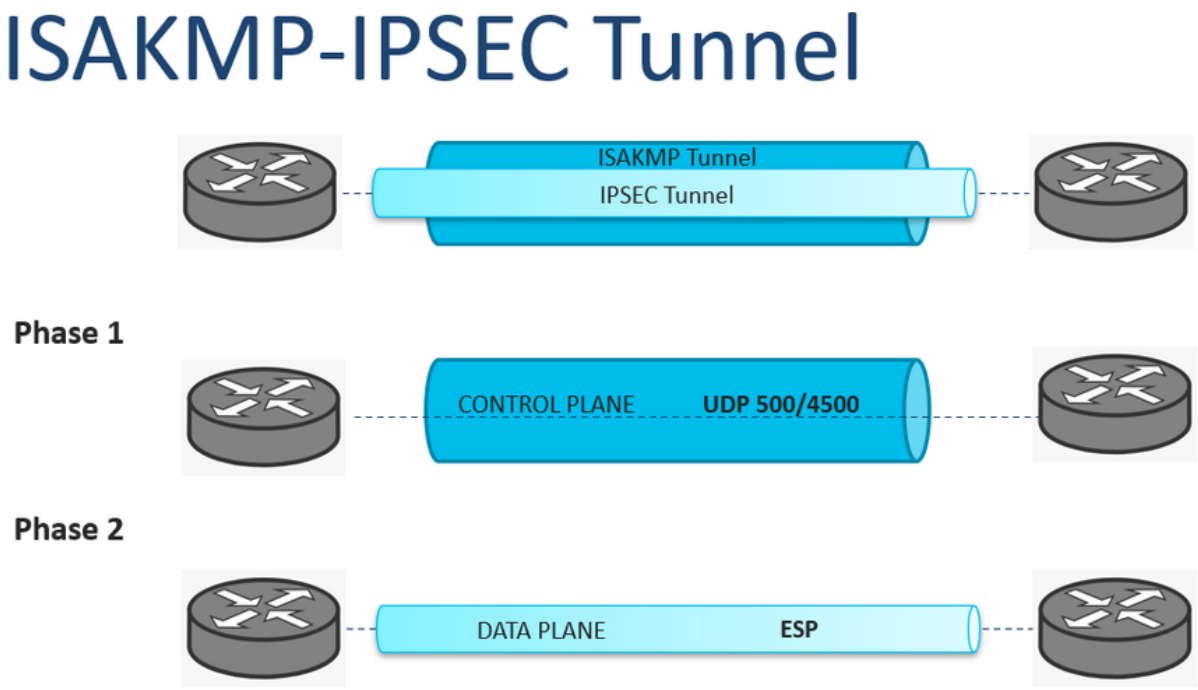
(IKEv2)

Fases IKE

ISAKMP separa la negociación en dos fases:

- Fase 1: Los dos pares ISAKMP establecen un túnel seguro y autenticado, que protege los mensajes de negociación ISAKMP. Este túnel se conoce como SA ISAKMP. ISAKMP define dos modos: modo principal (MM) y modo agresivo.
- Fase 2: negocia los materiales clave y los algoritmos para el cifrado (SA) de los datos que se van a transferir a través del túnel IPsec. Esta fase se denomina modo rápido.

Para materializar todos los conceptos abstractos, el túnel de fase 1 es el túnel principal y la fase 2 es un subtúnel. Esta imagen ilustra las dos fases como túneles:



Nota: El túnel de fase 1 (ISAKMP) protege el tráfico VPN del plano de control entre las dos puertas de enlace. El tráfico del plano de control puede ser paquetes de negociación, paquetes de información, DPD, señales de mantenimiento, regeneración de claves, etc. La negociación ISAKMP utiliza los puertos UDP 500 y 4500 para establecer un canal seguro.

Nota: El túnel de fase 2 (IPsec) protege el tráfico del plano de datos que pasa a través de la VPN entre las dos puertas de enlace. Los algoritmos utilizados para proteger los datos se configuran en la fase 2 y son independientes de los especificados en la fase 1.
El protocolo utilizado para encapsular y cifrar estos paquetes es la carga de seguridad de encapsulación (ESP).

Modos IKE (fase 1)

Modo principal

Una sesión IKE comienza cuando el iniciador envía una propuesta al respondedor. El primer intercambio entre nodos establece la política de seguridad básica; el iniciador propone los algoritmos de cifrado y autenticación que se van a utilizar. El respondedor elige la propuesta adecuada (supongamos que se elige una propuesta) y la envía al iniciador. El siguiente intercambio pasa las claves públicas Diffie-Hellman y otros datos. Todas las demás negociaciones se cifran dentro de la SA IKE. El tercer intercambio autentica la sesión ISAKMP. Una vez establecida la SA IKE, comienza la negociación IPSec (modo rápido).

Modo agresivo

El modo agresivo comprime la negociación IKE SA en tres paquetes, con todos los datos requeridos para la SA pasados por el iniciador. El respondedor envía la propuesta, el material clave y el ID, y autentica la sesión en el siguiente paquete. El iniciador responde y autentica la sesión. La negociación es más rápida y el ID de iniciador y de respondedor pasa a clear.

Modo IPsec (fase 2)

Modo rápido

La negociación IPSec, o modo rápido, es similar a una negociación IKE de modo agresivo, excepto la negociación, que se debe proteger dentro de una SA IKE. El modo rápido negocia la SA para el cifrado de datos y administra el intercambio de claves para esa SA IPSec.

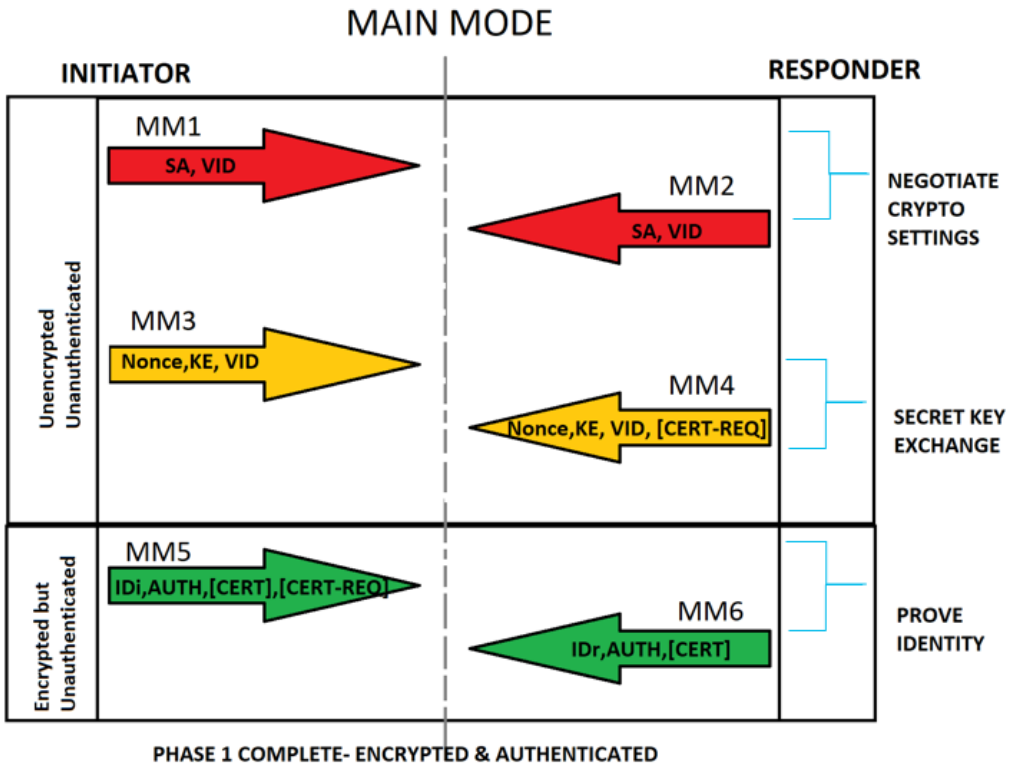
Glosario IKE

- Una asociación de seguridad (SA) es el establecimiento de atributos de seguridad compartidos entre dos entidades de red para permitir una comunicación segura. Una SA incluye atributos como el modo y el algoritmo criptográfico, la clave de cifrado del tráfico y los parámetros para que los datos de red se transmitan a través de la conexión.
- Los ID de proveedor (VID) se procesan para determinar si el par admite NAT-Traversal, la función de detección de par muerto, la fragmentación, etc.
- Nonce: un número generado aleatoriamente que el iniciador envía. Este nonce se trocea junto con los otros elementos con la clave acordada utilizada y se devuelve. El iniciador comprueba la cookie y el nonce y rechaza cualquier mensaje que no tenga el nonce correcto. Esto ayuda a evitar la repetición, ya que ningún tercero puede predecir qué es el nonce generado aleatoriamente.
- Información de intercambio de claves (KE) para el proceso de intercambio de claves seguro Diffie-Hellman (DH).
- El iniciador/respondedor de identidad (IDi/IDr.) se utiliza para enviar información de autenticación al par. Esta información se transmite bajo la protección del secreto compartido común.

- El intercambio de claves Diffie-Hellman (DH) es un método de intercambio seguro de algoritmos criptográficos a través de un canal público.
- La clave compartida IPSec se puede derivar con la DH utilizada de nuevo para garantizar Perfect Forward Secrecy (Confidencialidad directa perfecta, PFS) o el intercambio DH original actualizado con el secreto compartido derivado anteriormente.

Intercambio de paquetes de modo principal

Cada paquete ISAKMP contiene información de carga útil para el establecimiento del túnel. El glosario IKE explica las abreviaturas IKE como parte del contenido de carga útil para el intercambio de paquetes en el modo principal, como se muestra en esta imagen.



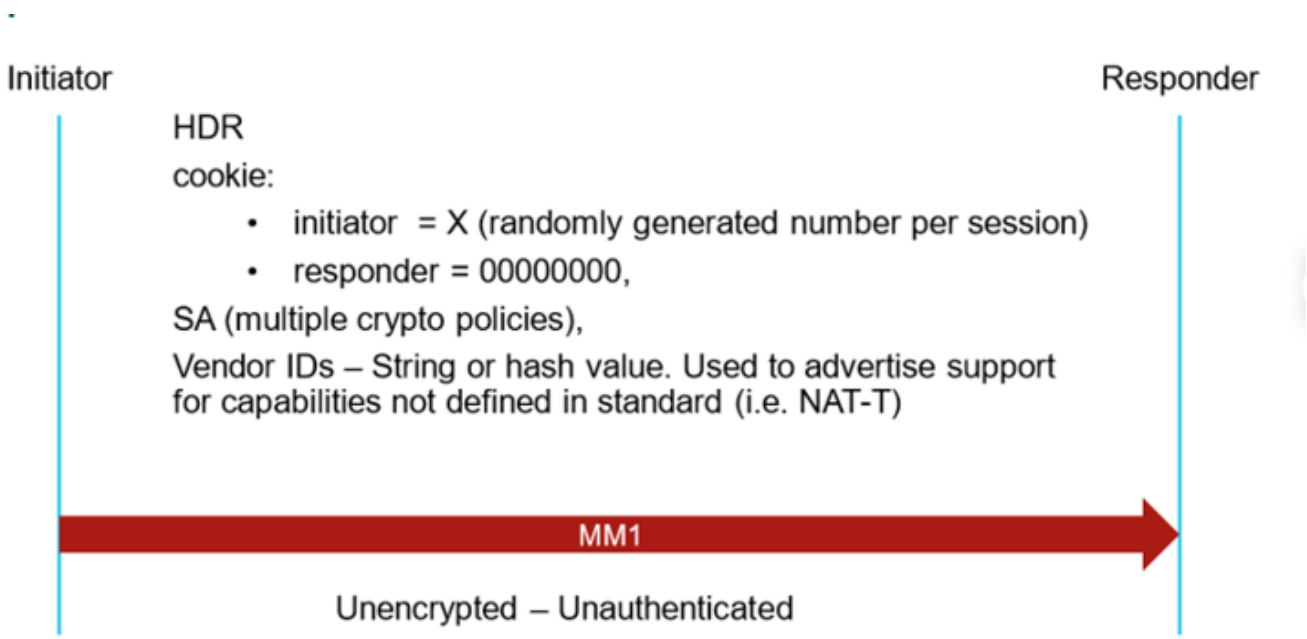
Modo principal 1 (MM1)

Para establecer los términos de las negociaciones ISAKMP, se crea una política ISAKMP, que incluye:

- Método de autenticación para garantizar la identidad de los pares.
- Un método de cifrado para proteger los datos y garantizar la privacidad.
- Un método de códigos de autenticación de mensajes codificados (HMAC) para garantizar la identidad del remitente y que el mensaje no se ha modificado durante el tránsito.
- Grupo Diffie-Hellman para determinar la seguridad del algoritmo de determinación de claves de cifrado. El dispositivo de seguridad utiliza este algoritmo para derivar el cifrado y las claves hash.

- Límite de tiempo durante el cual el dispositivo de seguridad utiliza una clave de cifrado antes de que se reemplace.

El iniciador de la negociación IKE envía el primer paquete como se muestra en la imagen:



Nota: El modo principal 1 es el primer paquete de la negociación IKE. Por lo tanto, el SPI del iniciador se establece en un valor aleatorio mientras que el SPI del respondedor se establece en 0. En el segundo paquete (MM2), se debe responder al SPI del respondedor con un nuevo valor y toda la negociación mantiene los mismos valores SPI.

Si se captura el MM1 y se utiliza un analizador de protocolo de red Wireshark, el valor SPI está dentro del contenido de Internet Security Association and Key Management Protocol como se muestra en la imagen:

```
> 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)
```

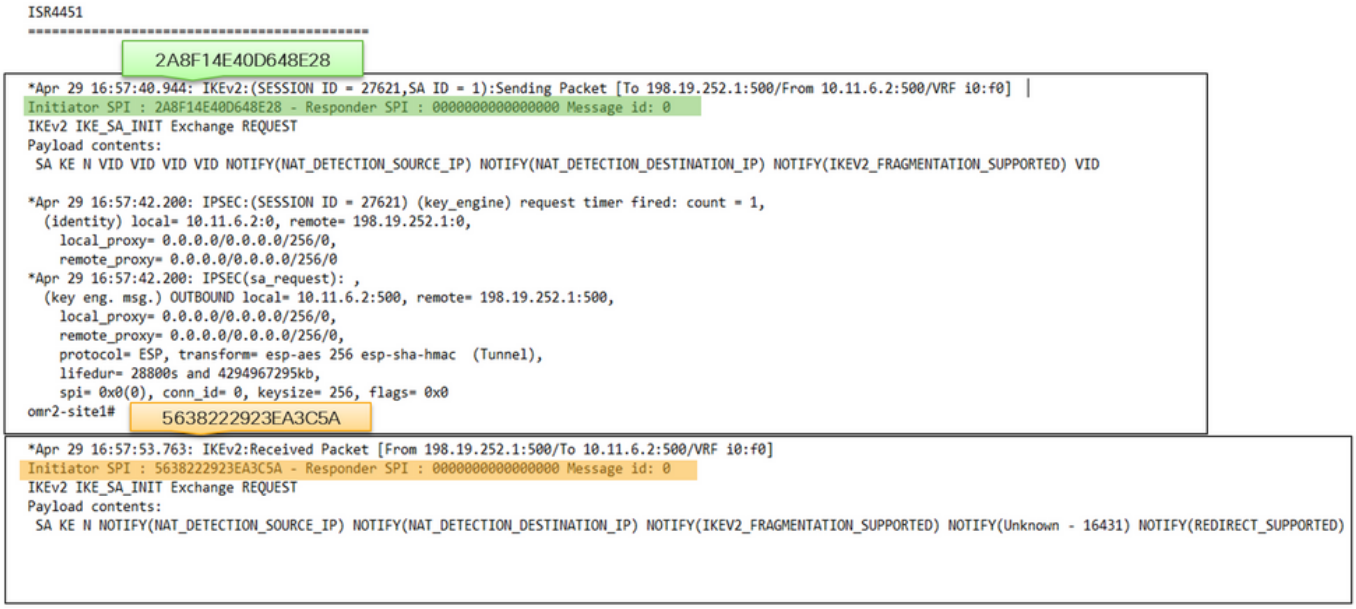
Nota: En el caso de que el paquete MM1 se pierda en la trayectoria o no haya respuesta MM2, la negociación IKE mantiene las retransmisiones MM1 hasta que se alcance el número máximo de retransmisiones. En este punto, el iniciador mantiene el mismo SPI hasta que se desencadena de nuevo la siguiente negociación.

Sugerencia: la identificación de SPI de iniciador y respondedor es muy útil para identificar

múltiples negociaciones para la misma VPN y reducir algunos problemas de negociación.

Identificar dos negociaciones simultáneas

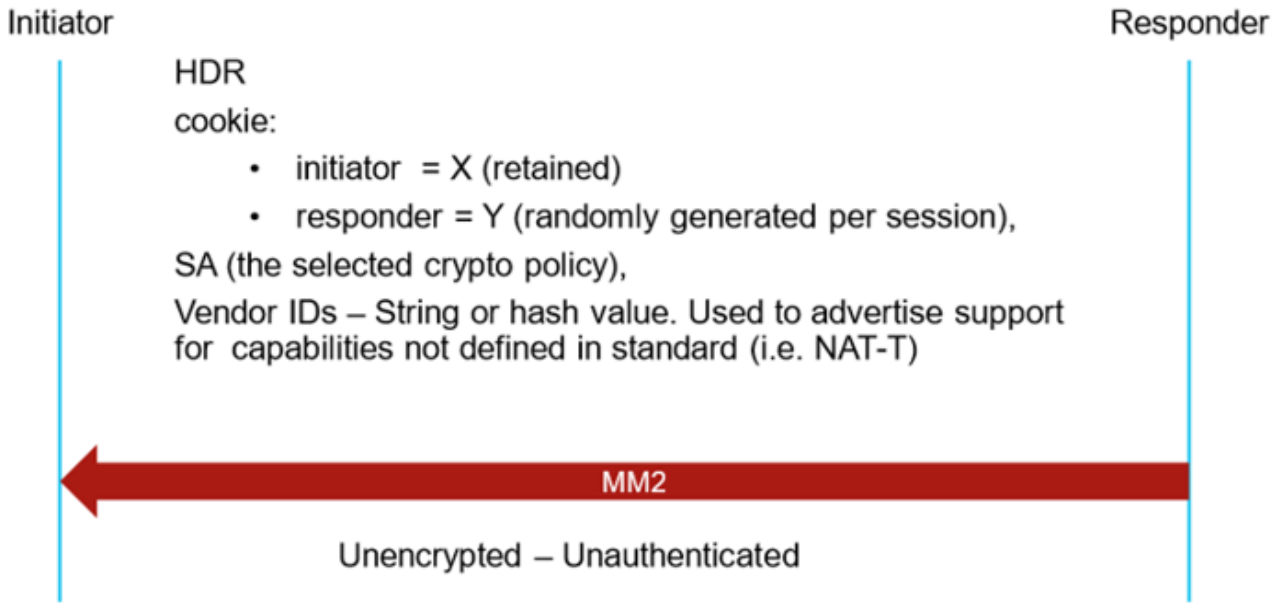
En las plataformas Cisco IOS® XE, las depuraciones se pueden filtrar por túnel con una condición para la dirección IP remota configurada. Sin embargo, las negociaciones simultáneas se muestran en los registros y no hay manera de filtrarlas. Es necesario hacerlo de forma manual. Como se mencionó anteriormente, toda la negociación mantiene los mismos valores SPI para el iniciador y el respondedor. En caso de que se reciba un paquete de la misma dirección IP par pero el SPI no coincida con el valor anterior seguido antes de que la negociación alcance el número máximo de retransmisión, se trata de otra negociación para el mismo peer como se muestra en la imagen:



Nota: El ejemplo muestra la negociación simultánea para el primer paquete en la negociación (MM1). Sin embargo, esto puede ocurrir en cualquier punto de negociación. Todos los paquetes subsiguientes deben incluir un valor diferente de 0 en el SPI del respondedor.

Modo principal 2 (MM2)

En el paquete del Modo principal 2, el respondedor envía la política seleccionada para las propuestas coincidentes, y el SPI del respondedor se establece en un valor aleatorio. Toda la negociación mantiene los mismos valores SPI. El MM2 responde al MM1 y el respondedor SPI está configurado en un valor diferente de 0 como se muestra en la imagen:



Si se captura el MM2 y se utiliza un analizador de protocolo de red Wireshark, los valores SPI del iniciador y SPI del respondedor se encuentran dentro del contenido de Internet Security Association and Key Management Protocol, como se muestra en la imagen:

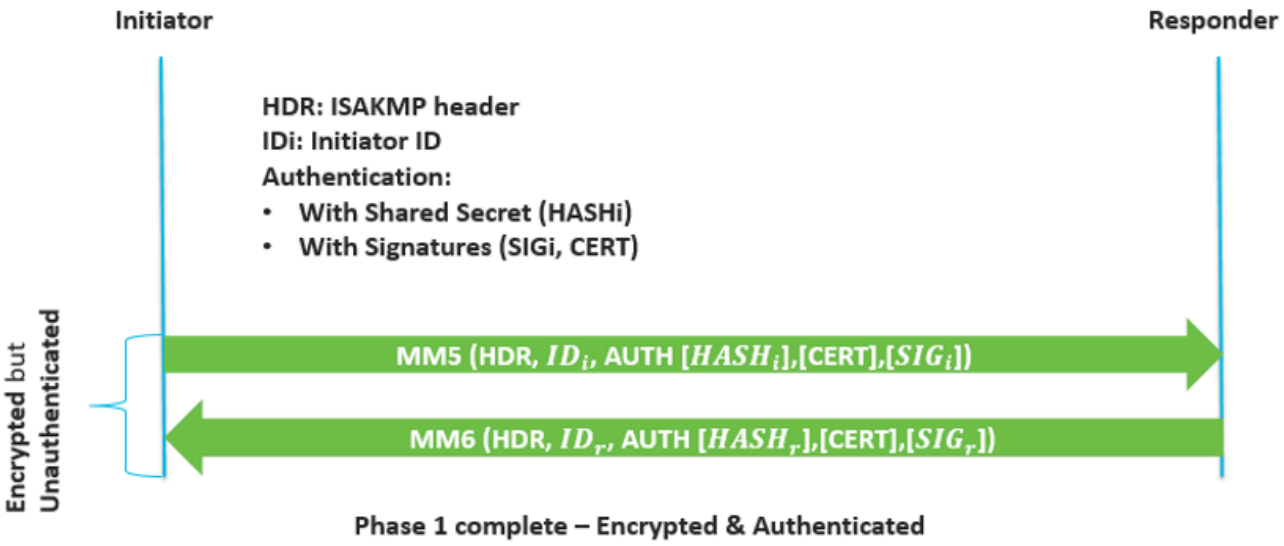
```
> Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
> Internet Protocol Version 4, Src: 209.134.162.150, Dst: 170.49.116.200
> User Datagram Protocol, Src Port: 500, Dst Port: 500
v Internet Security Association and Key Management Protocol
    Initiator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

Modo principal 3 y 4 (MM3-MM4)

Los paquetes MM3 y MM4 aún no están cifrados y no están autenticados, y se realiza el intercambio de claves secretas. En la imagen se muestran MM3 y MM4:

Modo principal 5 y 6 (MM5-MM6)

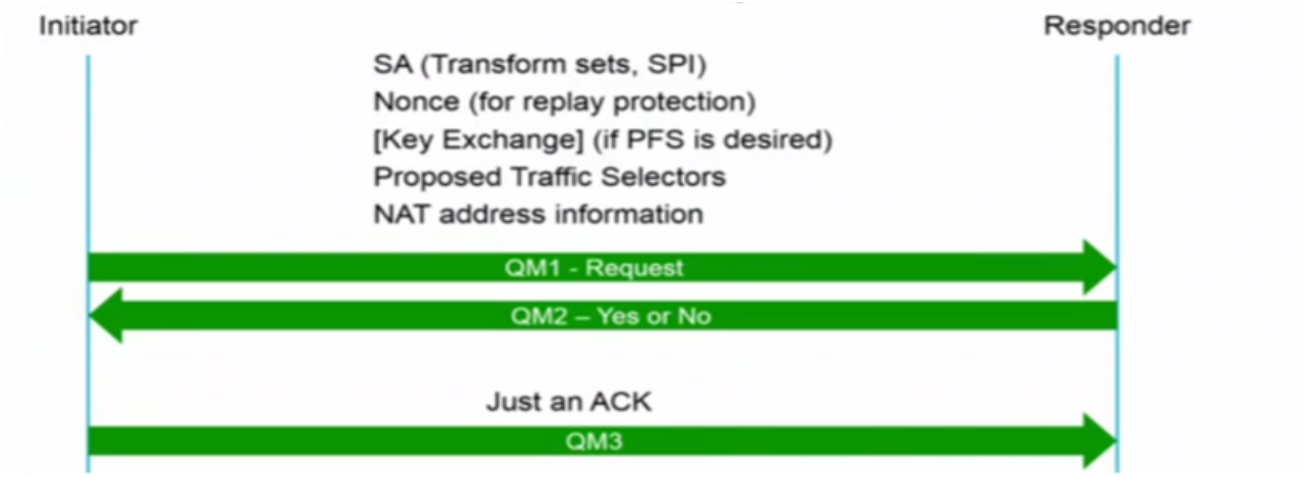
Los paquetes MM5 y MM6 ya están cifrados pero aún no están autenticados. En estos paquetes, la autenticación tiene lugar como se muestra en la imagen:



Modo rápido (QM1, QM2 y QM3)

El modo rápido se produce después de que el modo principal y la IKE hayan establecido el túnel seguro en la fase 1. El modo rápido negocia la política IPSec compartida para los algoritmos de seguridad IPSec y gestiona el intercambio de claves para el establecimiento de SA IPSec. Los nonces se utilizan para generar nuevo material de clave secreta compartida y evitar ataques de reproducción de SA falsas generadas.

En esta fase se intercambian tres paquetes, como se muestra en la imagen:



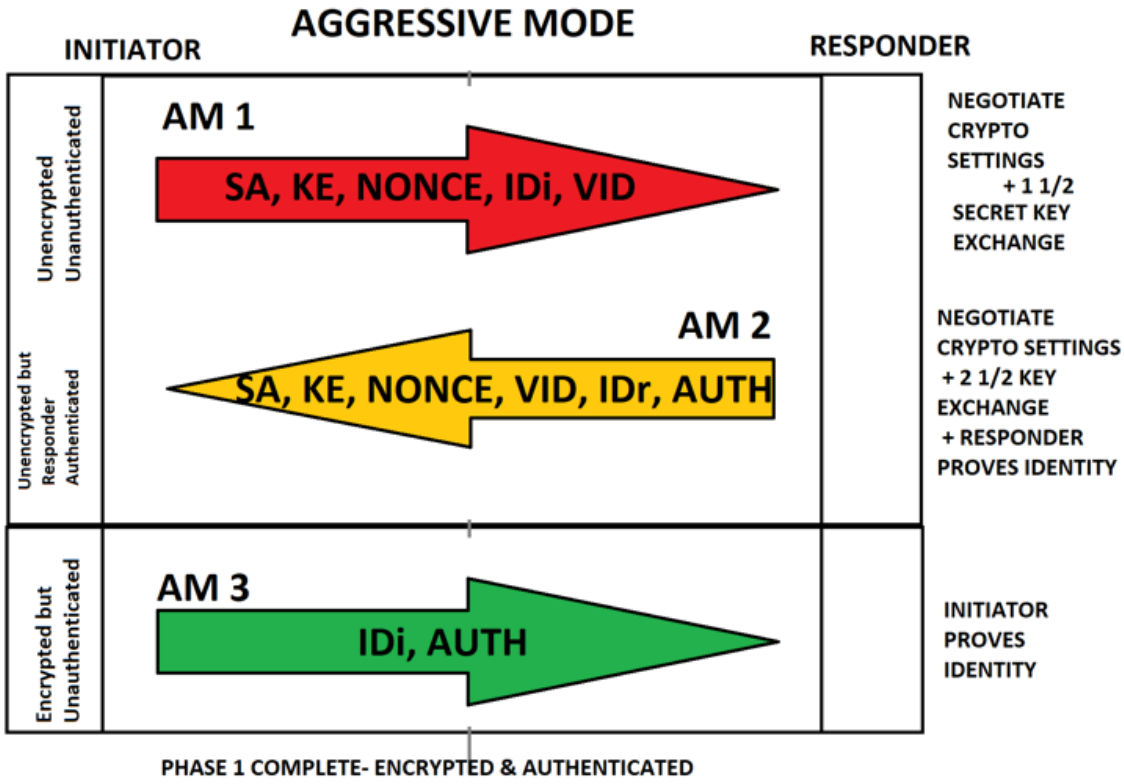
Intercambio de paquetes en modo agresivo

El modo agresivo comprime la negociación IKE SA en tres paquetes, con todos los datos requeridos para la SA pasados por el iniciador.

- El respondedor envía la propuesta, el material clave y el ID, y autentica la sesión en el siguiente paquete.
- El iniciador responde y autentica la sesión.

- La negociación es más rápida y el ID de iniciador y de respondedor pasa a clear.

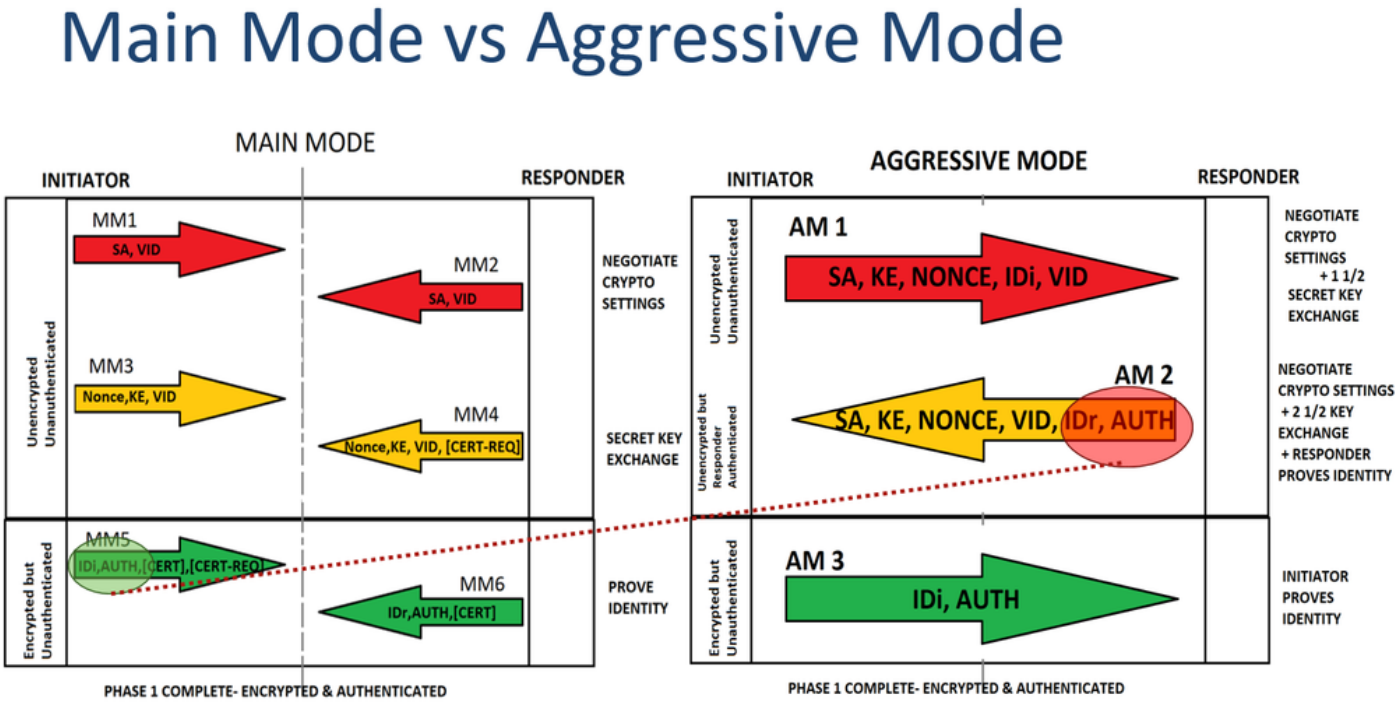
La imagen muestra el contenido de carga útil para los tres paquetes intercambiados en el modo agresivo:



Modo principal frente a modo agresivo

En comparación con el modo principal, el modo agresivo se reduce a tres paquetes:

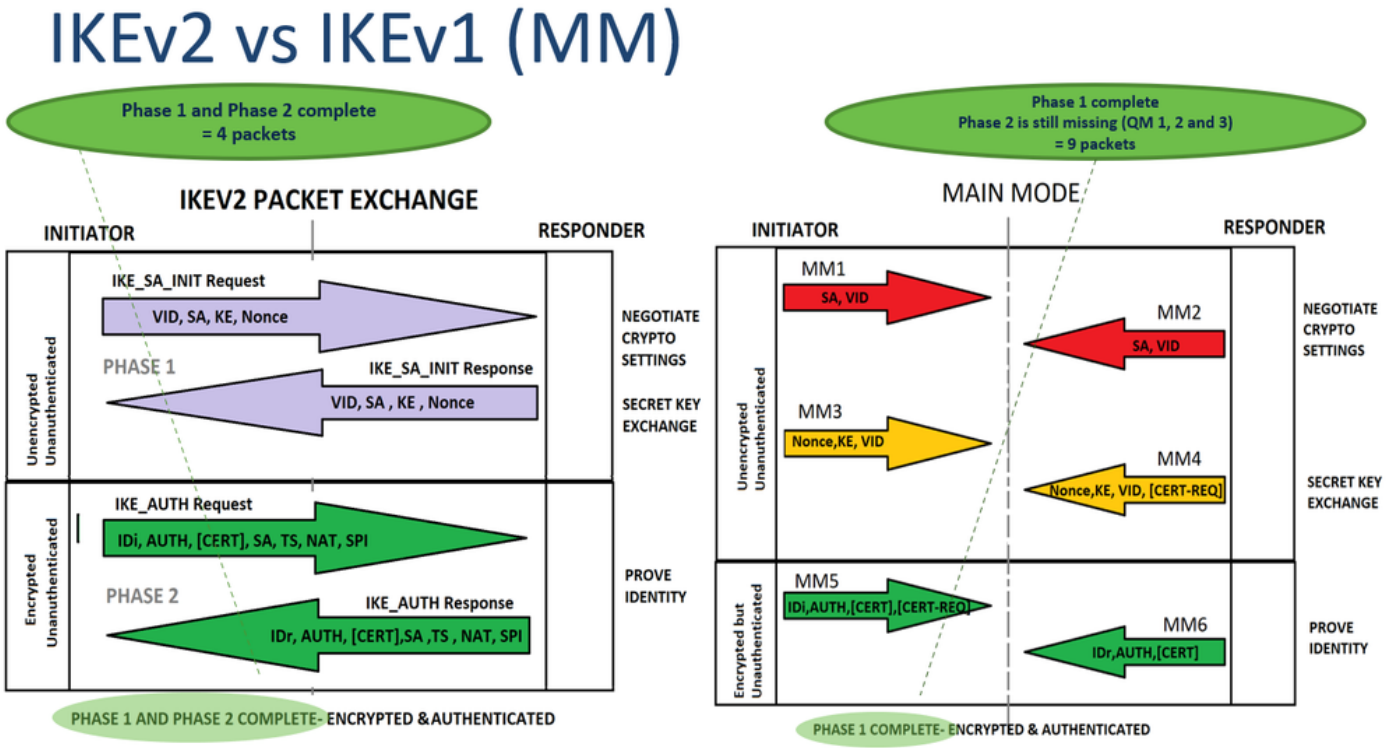
- AM 1 absorbe MM1 y MM3.
- AM 2 absorbe MM2, MM4, y parte del MM6. De aquí es de donde proviene la vulnerabilidad del modo agresivo. El AM 2 compone el IDr y la autenticación sin cifrar. A diferencia del modo principal, esta información está cifrada.
- AM 3 proporciona la IDi y la autenticación. Esos valores están cifrados.



Intercambio de paquetes IKEv2 frente a IKEv1

En la negociación IKEv2, se intercambian menos mensajes para establecer un túnel. IKEv2 utiliza cuatro mensajes; IKEv1 utiliza seis mensajes (en modo principal) o tres mensajes (en modo agresivo).

Los tipos de mensajes IKEv2 se definen como pares de solicitud y respuesta. La imagen muestra la comparación de paquetes y el contenido de carga útil de IKEv2 frente a IKEv1:



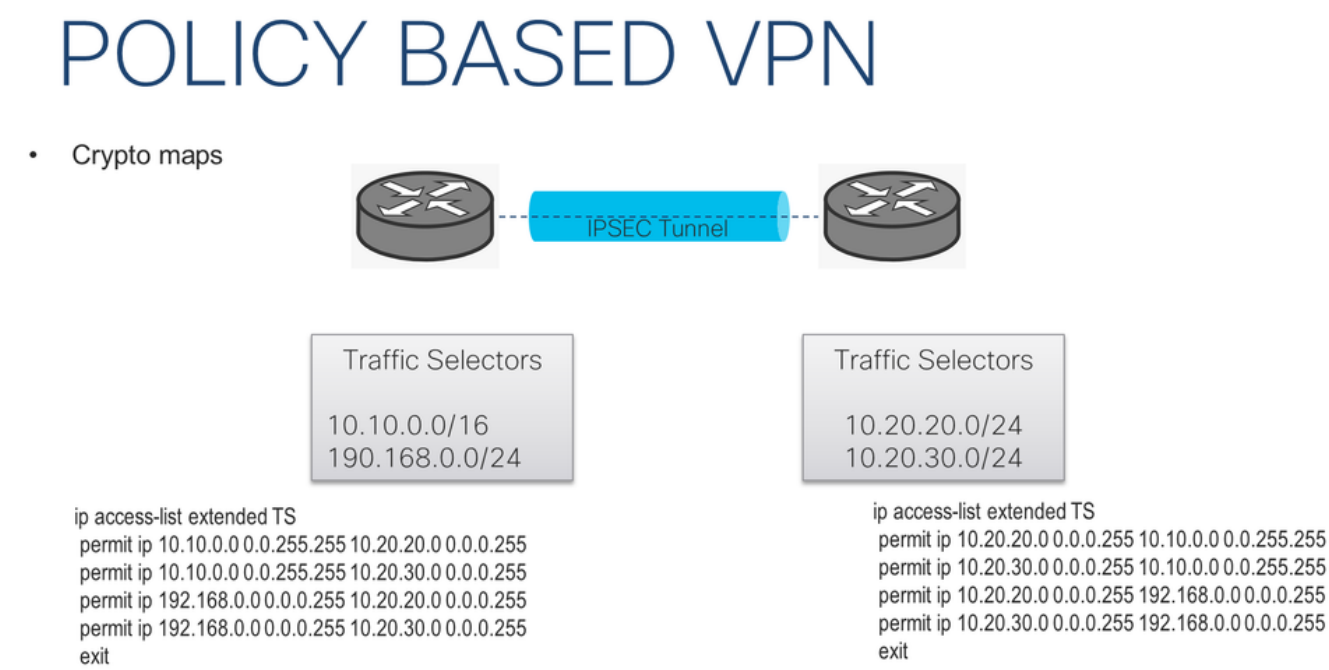
Nota: Este documento no profundiza en el intercambio de paquetes IKEv2. Para obtener más referencias, navegue hasta Intercambio de paquetes IKEv2 y Depuración a nivel de protocolo.

Basado en políticas frente a basado en rutas

VPN basada en políticas

Como indica el nombre, una VPN basada en políticas es un túnel VPN IPsec con una acción de política para el tráfico de tránsito que cumple los criterios de coincidencia de la política. En el caso de los dispositivos de Cisco, se configura una lista de acceso (ACL) y se asocia a un mapa criptográfico para especificar el tráfico que se redirigirá a la VPN y se cifrará.

Los selectores de tráfico son las subredes o los hosts especificados en la política como se muestra en la imagen:

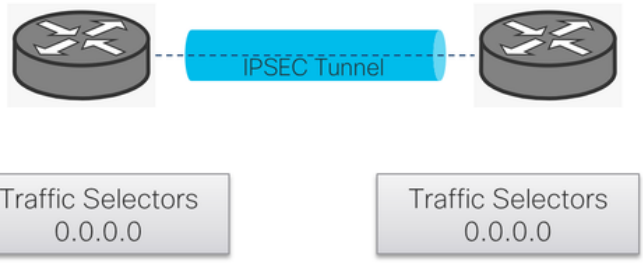


VPN basada en ruta

No se necesita una política. El tráfico se redirige hacia los túneles con rutas, y soporta el ruteo dinámico sobre la interfaz del túnel. Los selectores de tráfico (tráfico cifrado a través de la VPN) son de 0.0.0.0. a 0.0.0.0 de forma predeterminada, como se muestra en la imagen:

ROUTE BASED VPN

- Supports dynamic routing over the tunnel interface.

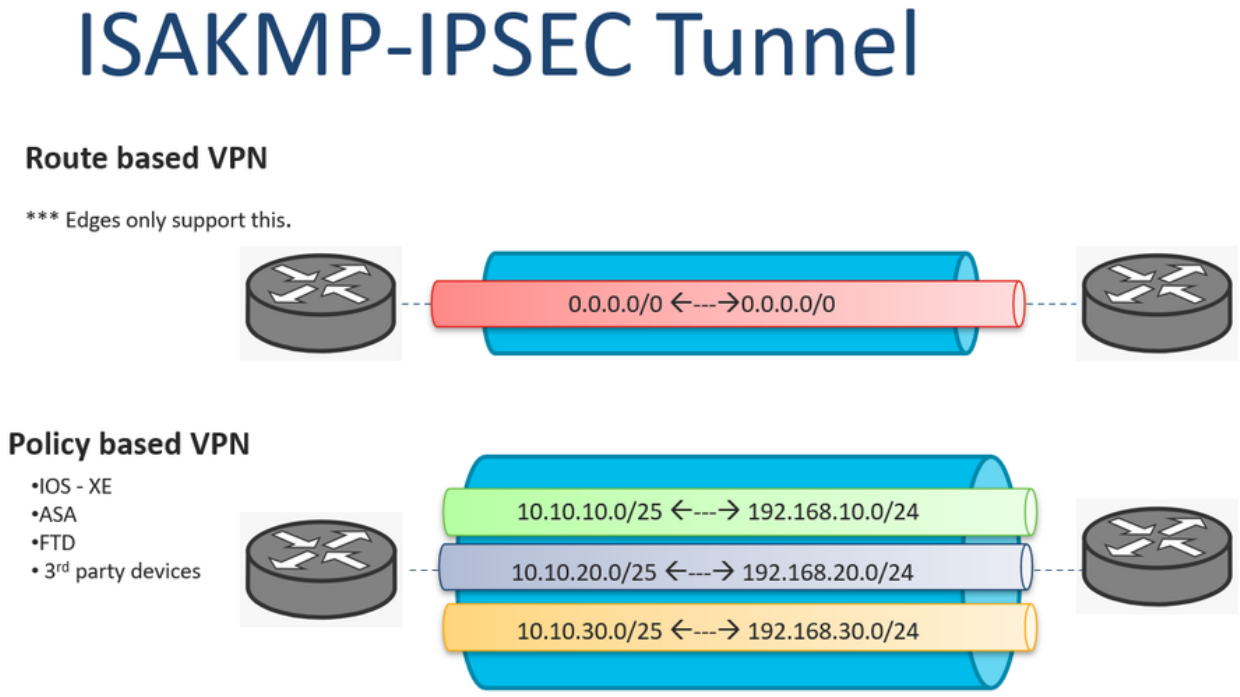



```
interface: Tunnel100001
   Crypto map tag: Tunnel100001-head-0, local addr 10.0.21.17

  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)
```

Nota: Debido a que los selectores de tráfico son 0.0.0.0, cualquier host o subred se incluye dentro de. Por lo tanto, sólo se crea una SA. Hay una excepción para el túnel dinámico. Este documento no describe los túneles dinámicos.

La política y la VPN basada en rutas se pueden materializar como se muestra en la imagen:



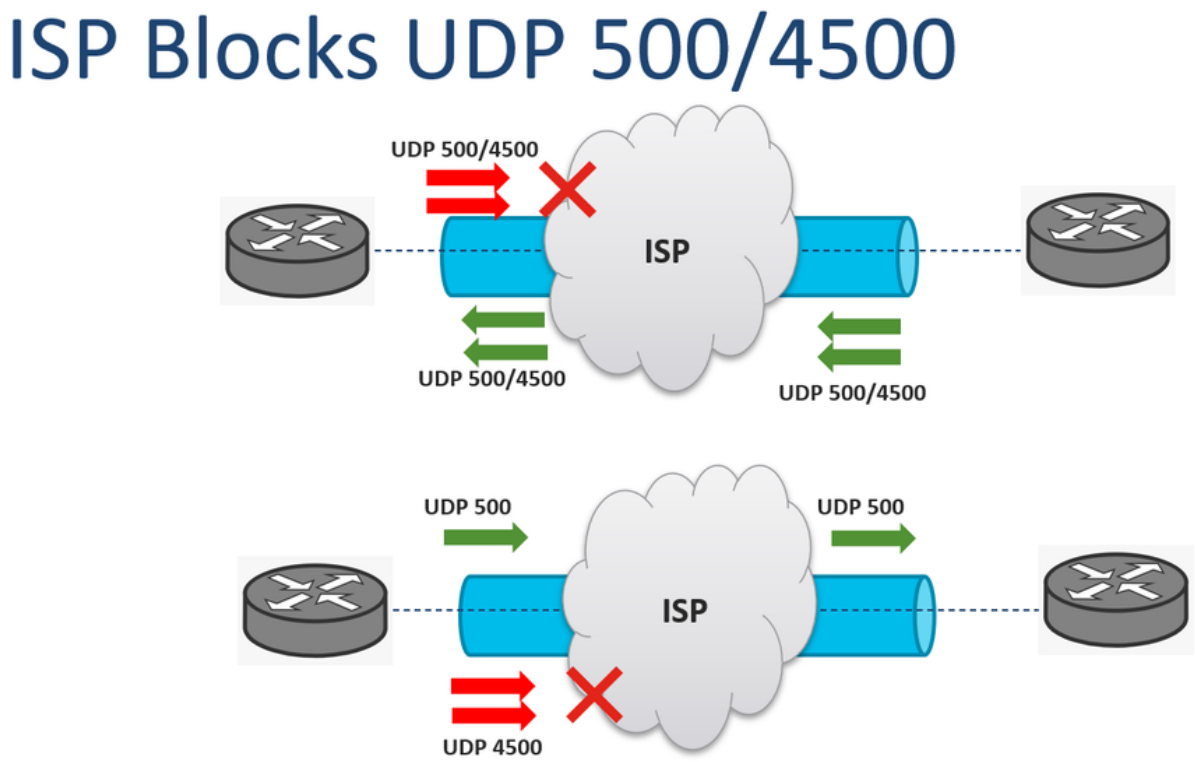
Nota: A diferencia de la VPN basada en rutas con una sola SA creada, la VPN basada en políticas puede crear múltiples SA. A medida que se configura una ACL, cada sentencia en la ACL (si son diferentes entre ellas) crea un subtúnel.

Problemas comunes para el tráfico que no recibe a través de la VPN

ISP bloquea UDP 500/4500

Es un problema muy común que el proveedor de servicios de Internet (ISP) bloquee los puertos UDP 500/4500. Para un establecimiento de túnel IPsec, se pueden conectar dos ISP diferentes. Uno de ellos puede bloquear los puertos y el otro los permite.

La imagen muestra los dos escenarios donde un ISP puede bloquear los puertos UDP 500/4500 en una sola dirección:

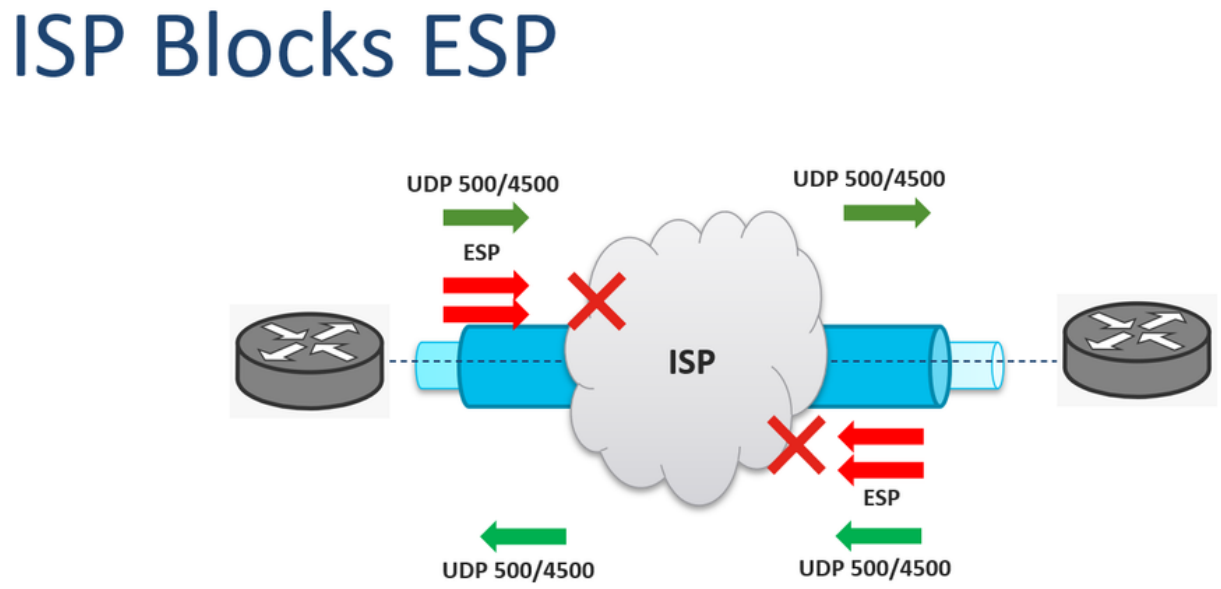


Nota: el puerto UDP 500 lo utiliza el intercambio de claves de Internet (IKE) para establecer túneles VPN seguros. UDP 4500 se utiliza cuando NAT está presente en un extremo VPN.

Nota: Cuando el ISP bloquea UDP 500/4500, el establecimiento del túnel IPsec se ve afectado y no se activa.

ISP bloquea ESP

Otro problema muy común en los túneles IPsec es que el ISP bloquea el tráfico ESP; sin embargo, permite los puertos UDP 500/4500. Por ejemplo, los puertos UDP 500/4500 se permiten de manera bidireccional. Por lo tanto, el túnel se establece correctamente, pero los paquetes ESP son bloqueados por el ISP o los ISP en ambas direcciones. Esto hace que el tráfico cifrado a través de la VPN falle como se muestra en la imagen:



Nota: Cuando el ISP bloquea paquetes ESP, el establecimiento del túnel IPsec se realiza correctamente, pero el tráfico cifrado se ve afectado. Se puede reflejar con la VPN activa, pero el tráfico no funciona sobre ella.

Sugerencia: también puede aparecer el escenario en el que el tráfico ESP se bloquea solo en una dirección. Los síntomas son los mismos, pero se puede encontrar fácilmente con la información de estadísticas de túnel, encapsulación, contadores de desencapsulación o contadores de RX y TX.

Información Relacionada

- Depuración a nivel de protocolo y de intercambio de paquetes KEv2
- Intercambio de claves de Internet (IKE): RFC 2409
- Protocolo de intercambio de claves de Internet (IKEv2)
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).