Comprendre le protocole IPsec IKEv1

Table des matières

Introduction

Ce document décrit le processus du protocole IKEv1 (Internet Key Exchange) pour un établissement de réseau privé virtuel (VPN).

Conditions préalables

Exigences

Cisco recommande que vous ayez une connaissance des concepts de sécurité de base :

- Authentification
- Confidentialité
- Intégrité
- IPsec

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Le processus de protocole IKEv1 (Internet Key Exchange) pour un établissement de réseau privé virtuel (VPN) est important pour comprendre l'échange de paquets afin de résoudre plus facilement tout problème de sécurité IP (IPsec) avec IKEv1.

IPsec

IPsec est une suite de protocoles qui assure la sécurité des communications Internet au niveau de la couche IP. L’utilisation actuelle la plus courante d’IPsec est de fournir un réseau privé virtuel (VPN), soit entre deux emplacements (passerelle à passerelle) ou entre un utilisateur distant et un réseau d’entreprise (hôte à passerelle).

Protocole IKE

IPsec utilise le protocole IKE pour négocier et établir des tunnels sécurisés de réseau privé virtuel (VPN) de site à site ou d’accès distant. Le protocole IKE est également appelé protocole ISAKMP (Internet Security Association and Key Management Protocol) (uniquement chez Cisco).

Il existe deux versions d’IKE :

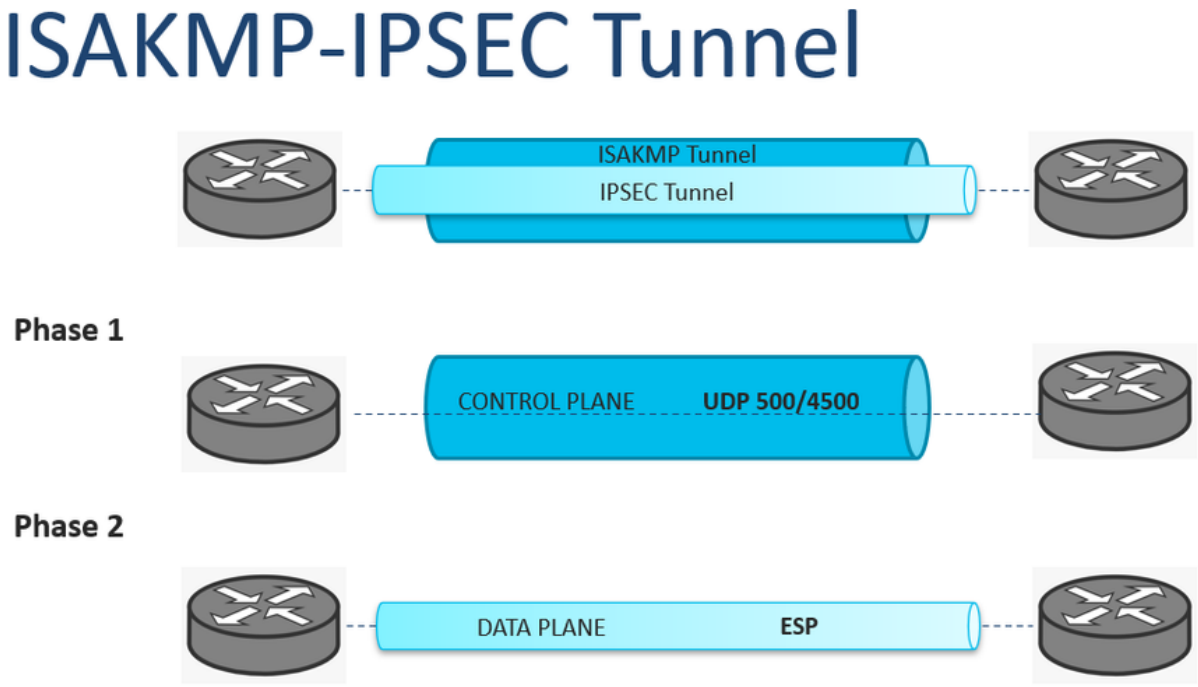
- IKEv1 : Défini dans la RFC 2409, The Internet Key Exchange
- IKE version 2 (IKEv2) : Défini dans la RFC 4306, Internet Key Exchange (IKEv2) Protocol

Phases IKE

ISAKMP sépare la négociation en deux phases :

- Phase 1 : les deux homologues ISAKMP établissent un tunnel sécurisé et authentifié qui protège les messages de négociation ISAKMP. Ce tunnel est connu sous le nom de ISAKMP SA. ISAKMP définit deux modes : le mode principal (MM) et le mode dynamique.
- Phase 2 : elle négocie les documents de clé et les algorithmes pour le chiffrement (SA) des données à transférer dans le tunnel IPsec. Cette phase s'appelle le mode rapide.

Pour matérialiser tous les concepts abstraits, le tunnel de phase 1 est le tunnel parent et la phase 2 est un sous-tunnel. Cette image illustre les deux phases sous forme de tunnels :



Remarque : le tunnel de phase 1 (ISAKMP) protège le trafic VPN du plan de commande entre les deux passerelles.L Le trafic du plan de contrôle peut être des paquets de négociation, des paquets d'informations, DPD, keepalives, rekey, etc. La négociation ISAKMP utilise les ports UDP 500 et 4500 pour établir un canal sécurisé.

Remarque : Le tunnel de phase 2 (IPsec) protège le trafic du plan de données qui traverse le VPN entre les deux passerelles. Les algorithmes utilisés pour protéger les données sont configurés dans la phase 2 et sont indépendants de ceux spécifiés dans la phase 1.
Le protocole utilisé pour encapsuler et chiffrer ces paquets est Encapsulation Security Payload (ESP).

Modes IKE (Phase 1)

Mode principal

Une session IKE commence lorsque l'initiateur envoie une proposition ou une proposition au

répondeur. Le premier échange entre les nœuds établit la politique de sécurité de base; l'initiateur propose les algorithmes de chiffrement et d'authentification à utiliser. Le répondant choisit la proposition appropriée (en supposant qu'une proposition est choisie) et l'envoie à l'initiateur. L'échange suivant transmet les clés publiques Diffie-Hellman et d'autres données. Toutes les négociations ultérieures sont chiffrées dans la SA IKE. Le troisième échange authentifie la session ISAKMP. Une fois que la SA IKE est établie, la négociation IPSec (mode rapide) commence.

Mode agressif

Le mode dynamique compresse la négociation de la SA IKE en trois paquets, toutes les données requises pour la SA étant transmises par l'initiateur. Le répondeur envoie la proposition, les éléments de clé et l'identifiant, et authentifie la session dans le paquet suivant. L'initiateur répond et authentifie la session. La négociation est plus rapide, et l'identifiant de l'initiateur et du répondeur est clair.

Mode IPsec (Phase 2)

Mode rapide

La négociation IPSec, ou le mode rapide, est similaire à une négociation IKE en mode agressif, sauf que la négociation doit être protégée dans une convention SA IKE. Le mode rapide négocie la SA pour le chiffrement des données et gère l'échange de clés pour cette SA IPSec.

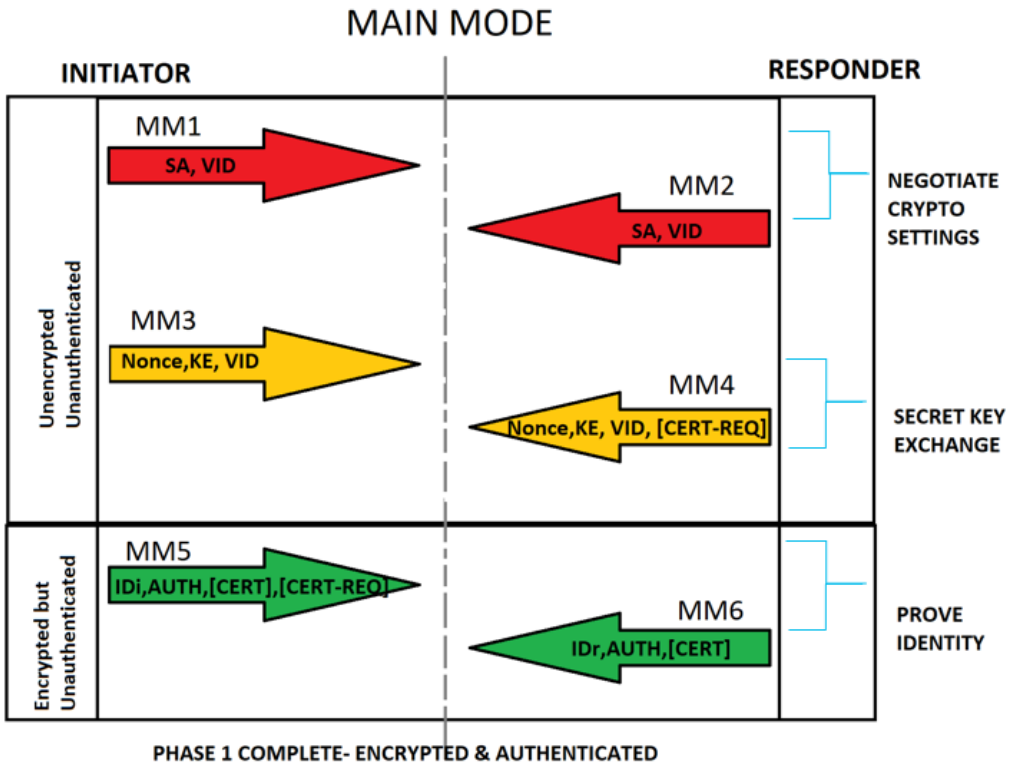
Glossaire IKE

- Une association de sécurité (SA) est l'établissement d'attributs de sécurité partagés entre deux entités réseau pour prendre en charge des communications sécurisées. Une SA comprend des attributs tels que l'algorithme et le mode cryptographiques; la clé de chiffrement du trafic et les paramètres des données de réseau à transmettre sur la connexion.
- Les ID de fournisseur (VID) sont traités pour déterminer si l'homologue prend en charge la fonction NAT-Traversal, la fonctionnalité Dead Peer Detection, la fragmentation, etc.
- Valeur Nonce : un nombre généré aléatoirement que l'initiateur envoie. Cette valeur Nonce est chiffrée avec les autres éléments à l'aide de la clé convenue, puis elle est renvoyée. L'initiateur vérifie le témoin et la valeur Nonce, et rejette tous les messages qui n'ont pas la bonne valeur Nonce. Cela permet d'éviter la relecture, car aucun tiers ne peut prédire la valeur Nonce générée aléatoirement.
- Informations Key-exchange (KE) pour le processus d'échange de clés sécurisé Diffie-Hellman (DH).
- L'identité de l'initiateur/répondeur (IDi/IDr) est utilisée pour envoyer des renseignements d'authentification à l'homologue. Ces informations sont transmises sous la protection du secret partagé commun.
- L'échange de clés Diffie–Hellman (DH) est une méthode d'échange sécurisé d'algorithmes cryptographiques sur un canal public.
- La clé IPSec partagée peut être dérivée et le DH est réutilisé pour assurer le secret de

transmission parfait (PFS) ou l'échange DH d'origine avec le secret partagé dérivé précédemment.

Échange de paquets en mode principal

Chaque paquet ISAKMP contient des informations sur la charge utile pour l'établissement du tunnel. Le glossaire IKE explique les abréviations IKE dans le cadre de la charge utile pour l'échange de paquets en mode principal, comme le montre cette image.

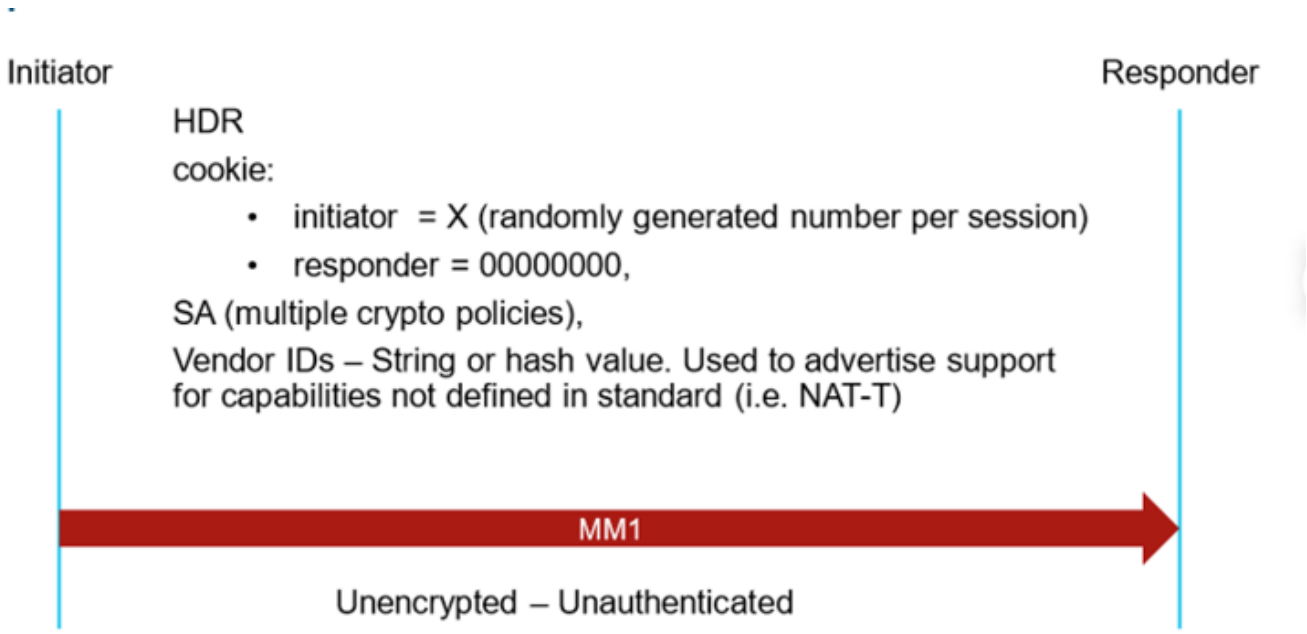


Mode principal 1 (MM1)

Pour définir les conditions des négociations ISAKMP, vous créez une politique ISAKMP qui comprend :

- Une méthode d'authentification pour garantir l'identité des homologues.
- Une méthode de chiffrement pour protéger les données et assurer la confidentialité.
- Une méthode de codes d'authentification de message hachés (HMAC) pour s'assurer de l'identité de l'expéditeur et pour s'assurer que le message n'a pas été modifié pendant le transfert.
- Un groupe Diffie-Hellman pour déterminer la force de l'algorithme de détermination de la clé de chiffrement. Les appareils de sécurité utilisent cet algorithme pour dériver les clés de chiffrement et de hachage.
- Une limite pendant laquelle l'appareil de sécurité utilise une clé de chiffrement avant de la remplacer.

Le premier paquet est envoyé par l'initiateur de la négociation IKE, comme le montre l'image:



Remarque : Le mode principal 1 est le premier paquet de la négociation IKE. Par conséquent, le SPI de l'initiateur est défini sur une valeur aléatoire tandis que le SPI du répondeur est défini sur 0. Dans le deuxième paquet (MM2), le SPI du répondeur doit recevoir une nouvelle valeur et l'ensemble de la négociation conserve les mêmes valeurs SPI.

Si MM1 est capturé et un analyseur de protocole réseau Wireshark est utilisé, la valeur SPI est dans le contenu du protocole ISAKMP (Internet Security Association and Key Management Protocol), comme le montre l'image:

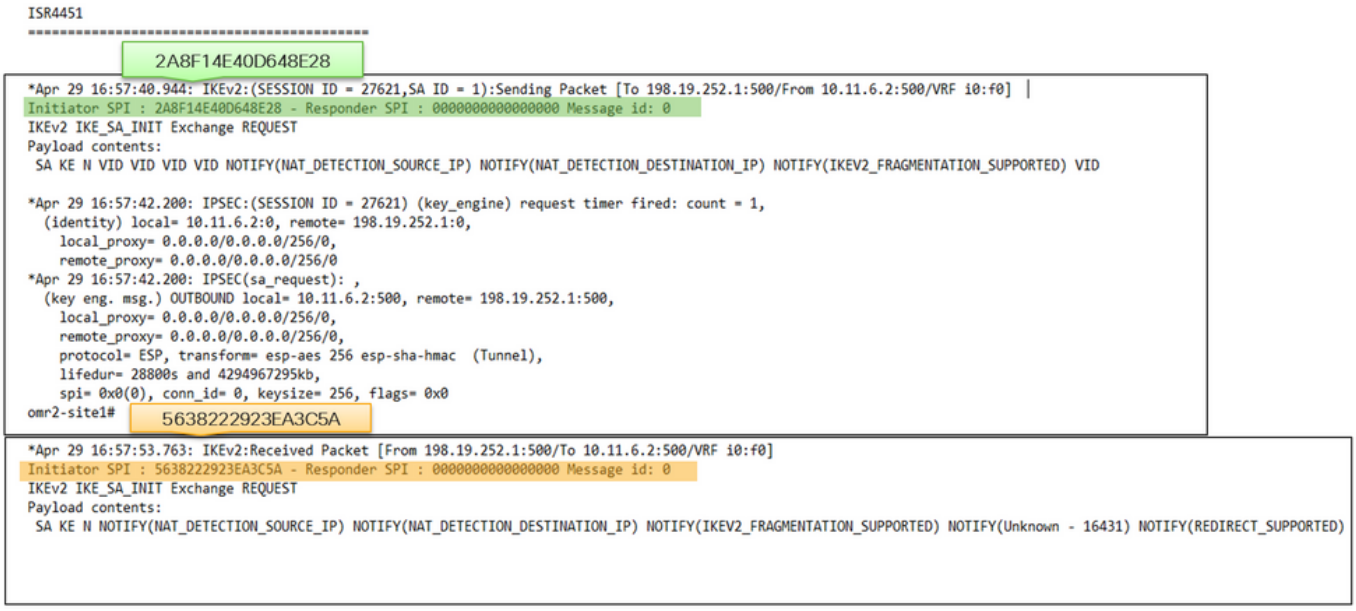
```
> Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
> Internet Protocol Version 4, Src: 170.49.116.200, Dst: 209.134.162.150
> User Datagram Protocol, Src Port: 500, Dst Port: 500
v Internet Security Association and Key Management Protocol
    Initiator SPI: 6f80c0380ef6bdfd
    Responder SPI: 0000000000000000
    Next payload: Security Association (33)
```

Remarque : Si le paquet MM1 se perd dans le chemin ou s'il n'y a pas de réponse MM2, la négociation IKE conserve les retransmissions MM1 jusqu'à ce que le nombre maximal de retransmissions soit atteint. À ce stade, l'initiateur conserve le même SPI jusqu'à ce que la négociation suivante soit redéclenchée.

Remarque : L'identification des SPI de l'initiateur et du répondeur est très utile pour identifier plusieurs négociations pour le même VPN ainsi que pour résoudre certains problèmes de négociation.

Identification de deux négociations simultanées

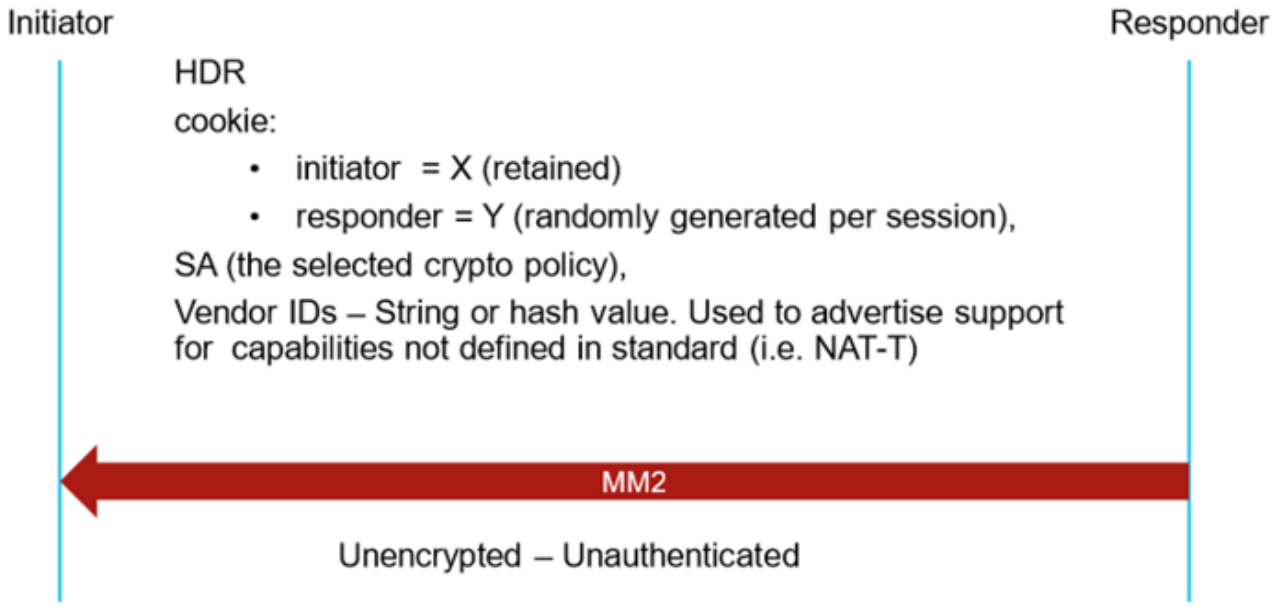
Sur les plates-formes Cisco IOS® XE, les débogages peuvent être filtrés par tunnel avec une condition pour l'adresse IP distante configurée. Cependant, les négociations simultanées sont affichées dans les journaux et il n'y a aucun moyen de les filtrer. Il est nécessaire de le faire manuellement. Comme mentionné précédemment, l'ensemble de la négociation conserve les mêmes valeurs SPI pour l'initiateur et le répondeur. Dans le cas où un paquet est reçu de la même adresse IP homologue, mais que le SPI ne correspond pas à la valeur précédente suivie avant que la négociation atteigne le nombre maximal de retransmissions, il s'agit d'une autre négociation pour le même homologue, comme le montre l'image:



Remarque : l'exemple illustre la négociation simultanée du premier paquet de la négociation (MM1). Cependant, cela peut se produire à n'importe quel point de négociation. Tous les paquets suivants doivent inclure une valeur différente de 0 sur la SPI du répondeur.

Mode principal 2 (MM2)

Dans le paquet du mode principal 2, le répondeur envoie la politique sélectionnée pour les propositions mises en correspondance et le SPI du répondeur est réglé sur une valeur aléatoire. L'ensemble de la négociation conserve les mêmes valeurs de SPI. Le MM2 répond à MM1 et le répondeur SPI est réglé à une valeur différente de 0, comme le montre l'image:



Si MM2 est capturé et qu'un analyseur de protocole réseau Wireshark est utilisé, les valeurs du SPI de l'initiateur et du SPI du répondeur se trouvent dans les limites du protocole ISAKMP (Internet Security Association and Key Management ou Association de sécurité Internet et protocole de gestion des clés), comme le montre l'image:

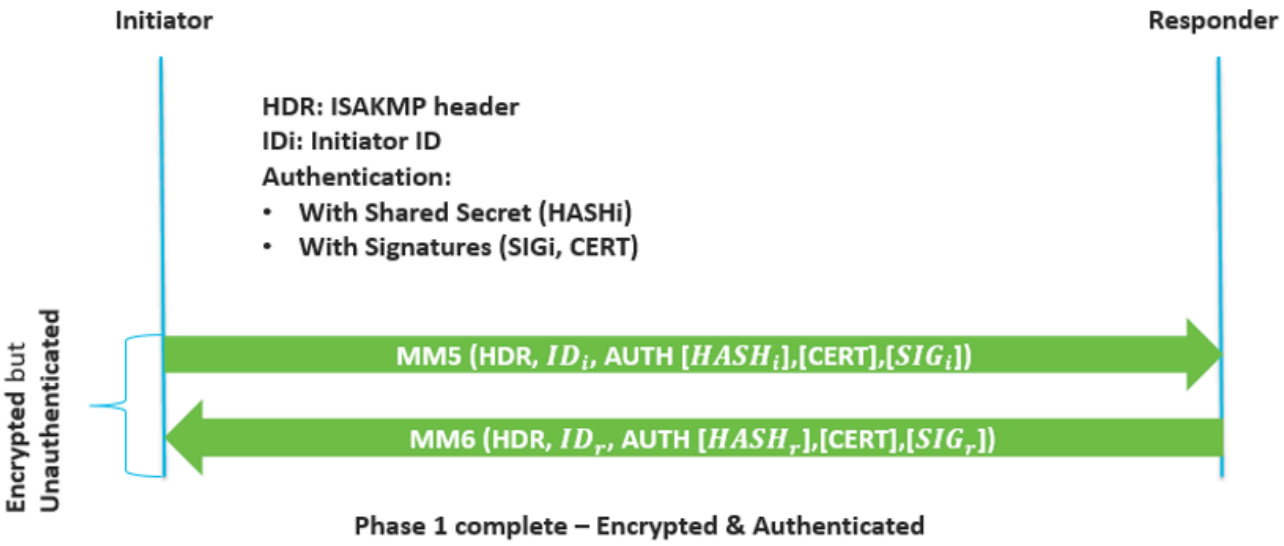
```
> Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
> Internet Protocol Version 4, Src: 209.134.162.150, Dst: 170.49.116.200
> User Datagram Protocol, Src Port: 500, Dst Port: 500
v Internet Security Association and Key Management Protocol
    Initiator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

Modes principaux 3 et 4 (MM3-MM4)

Les paquets MM3 et MM4 ne sont toujours pas chiffrés ni authentifiés, et l'échange de la clé secrète a lieu. Les modèles MM3 et MM4 sont montrés dans l'image:

Modes principaux 5 et 6 (MM5-MM6)

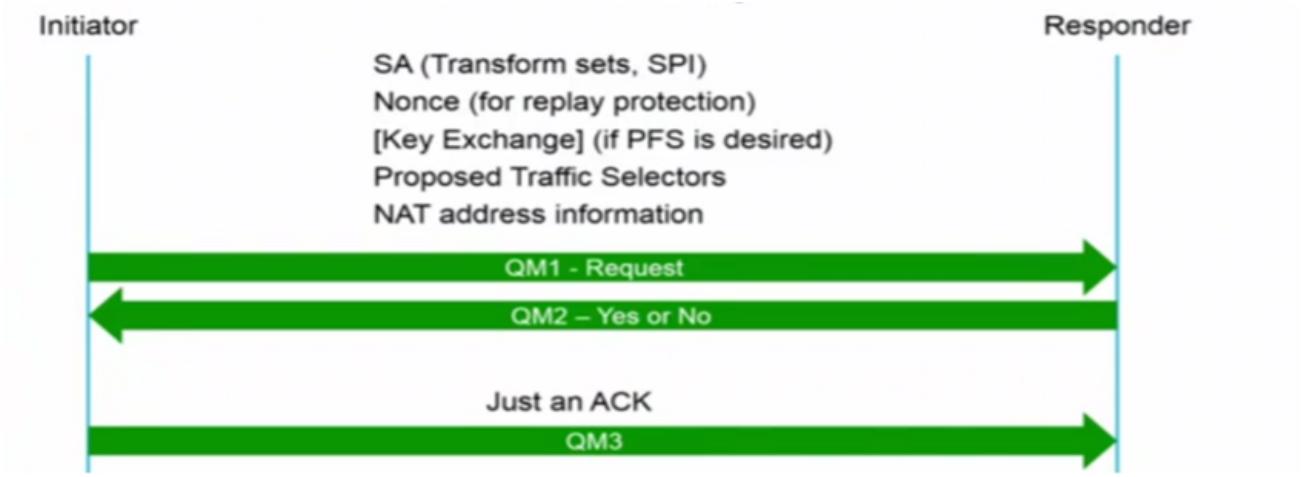
Les paquets MM5 et MM6 sont déjà chiffrés, mais toujours pas authentifiés. Sur ces paquets, l'authentification a lieu comme le montre l'image:



Mode rapide (QM1, QM2 et QM3)

Le mode rapide se produit après que le monde principal et IKE ont établi le tunnel sécurisé en phase 1. Le mode rapide négocie la politique IPSec partagée, pour les algorithmes de sécurité IPSec, et gère l'échange de clés pour l'établissement de la SA IPSec. Les valeurs Nonce sont utilisées pour générer de nouveaux éléments de clé secrète partagée et empêcher les attaques par relecture de fausses SA générées.

Trois paquets sont échangés au cours de cette phase, comme le montre l'image:



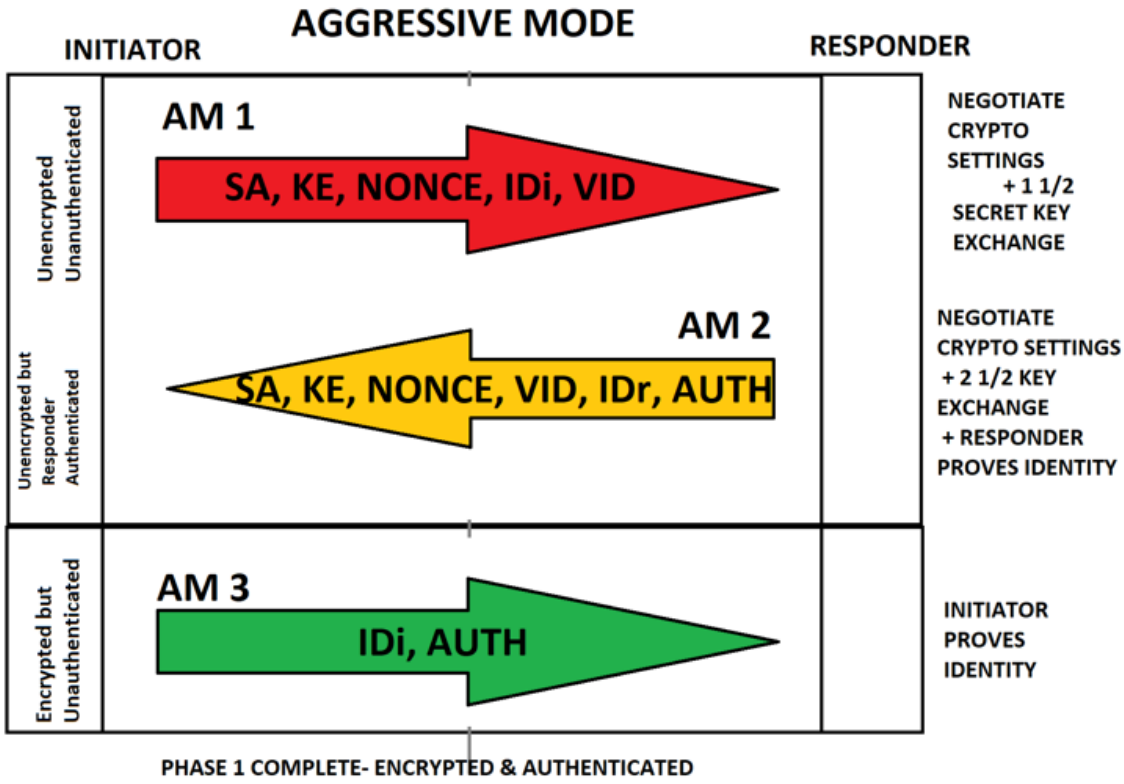
Échange de paquets en mode dynamique

Le mode dynamique compresse la négociation de la SA IKE en trois paquets, toutes les données requises pour la SA étant transmises par l'initiateur.

- Le répondeur envoie la proposition, les éléments de clé et l'identifiant, et authentifie la session dans le paquet suivant.
- L'initiateur répond et authentifie la session.

- La négociation est plus rapide, et l’identifiant de l’initiateur et du répondeur est clair.

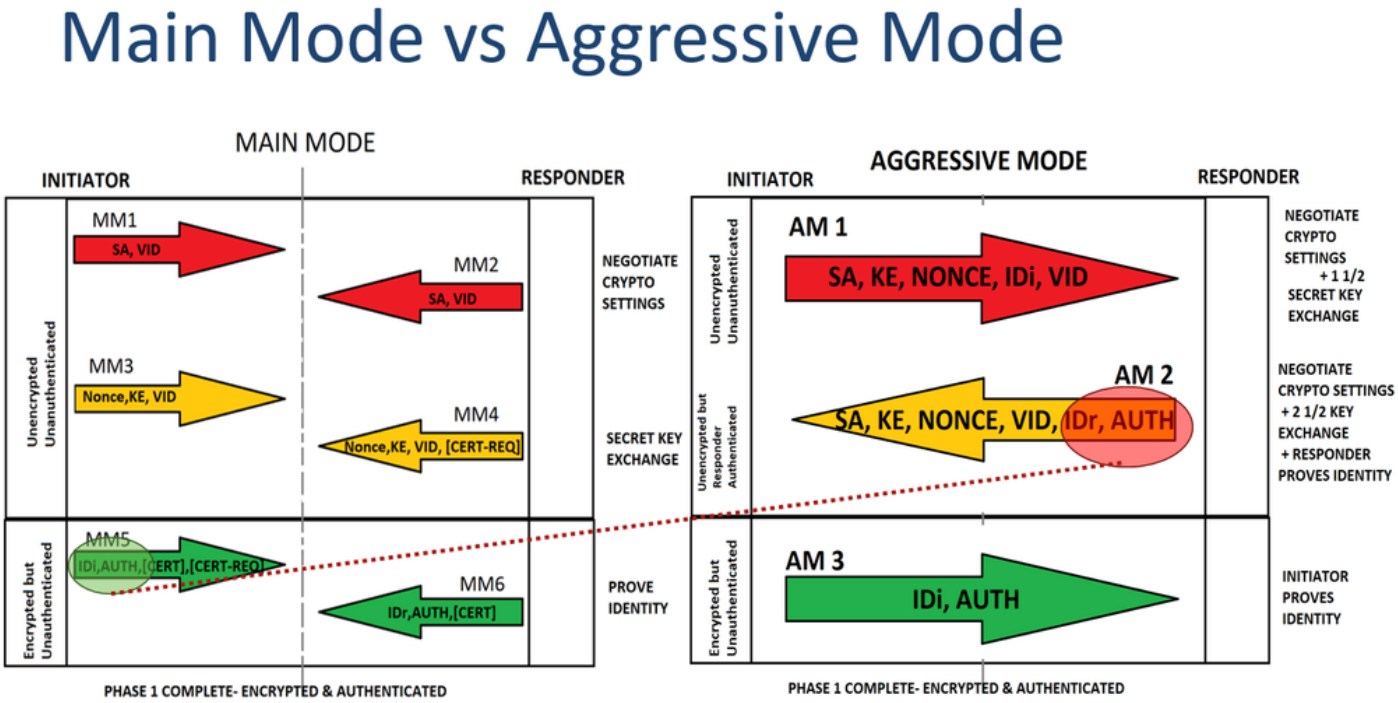
L’image montre le contenu de la charge utile pour les trois paquets échangés en mode dynamique:



Mode principal contre mode dynamique

Comparé au mode principal, le mode agressif se présente sous la forme de trois packages :

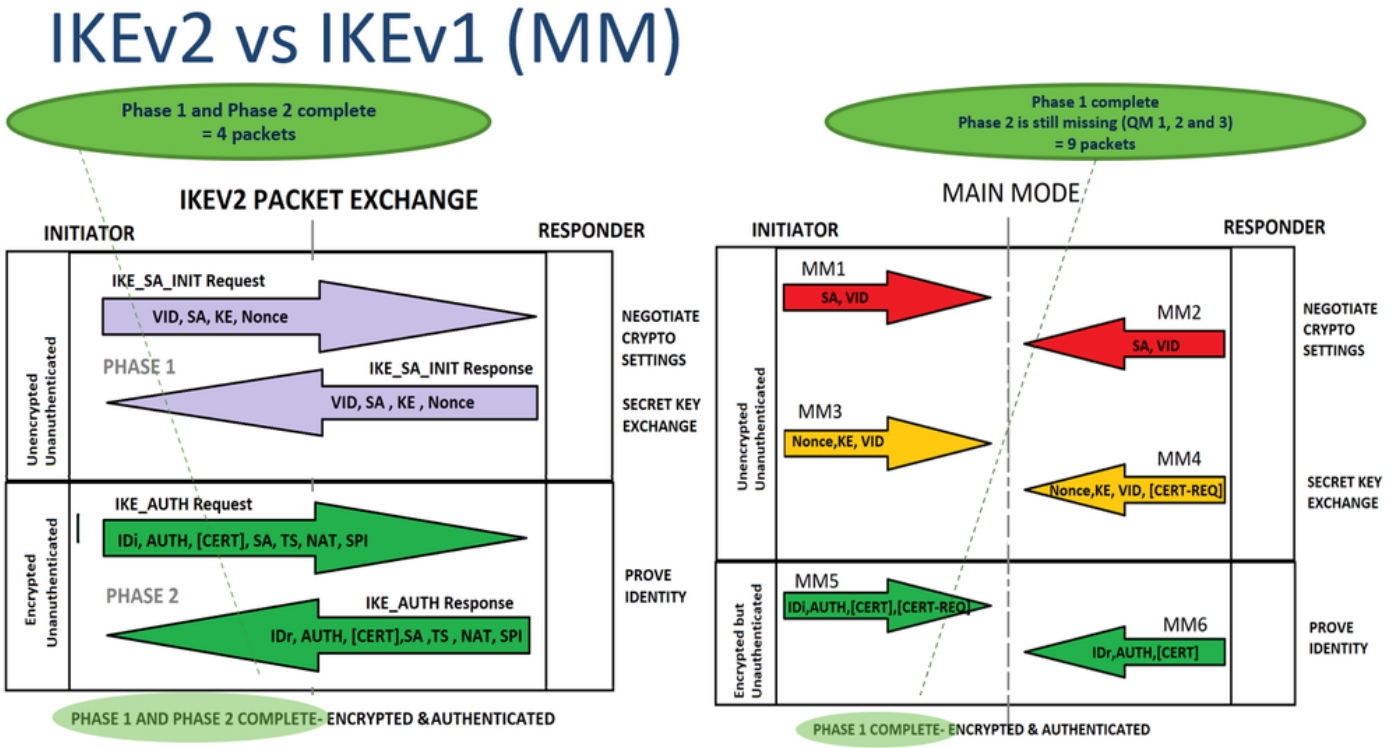
- AM1 absorbe MM1 et MM3.
- AM2 absorbe MM2, MM4 et une partie du MM6. C’est de là que vient la vulnérabilité du mode dynamique. L'AM 2 constitue l'IDr et l'authentification non chiffrées. Contrairement au mode principal, ces informations sont chiffrées.
- L'AM 3 fournit l'IDi et l'authentification. Ces valeurs sont chiffrées.



Échange de paquets IKEv2 vs IKEv1

Dans la négociation IKEv2, moins de messages sont échangés pour établir un tunnel. IKEv2 utilise quatre messages; IKEv1 utilise soit six messages (en mode principal), soit trois messages (en mode dynamique).

Les types de messages IKEv2 sont définis comme des paires de requête et de réponse. L'image montre la comparaison des paquets et le contenu de la charge utile d'IKEv2 par rapport à IKEv1:



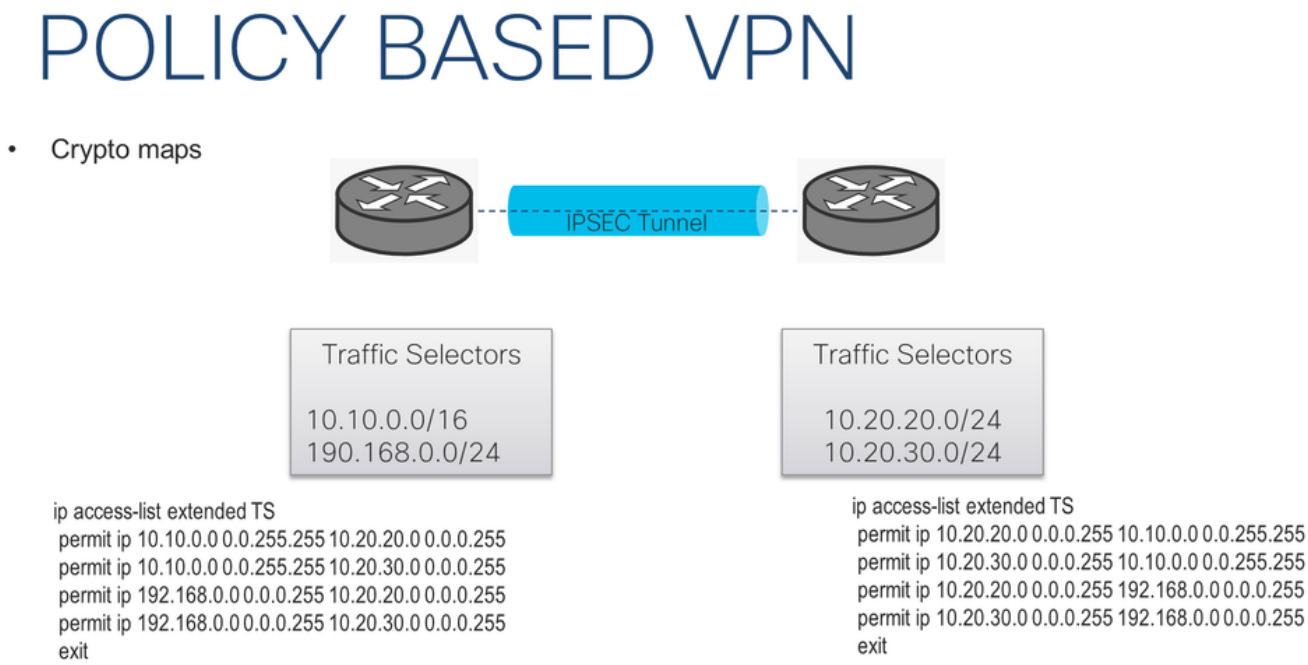
Remarque : ce document n'approfondit pas l'échange de paquets IKEv2. Pour obtenir plus de références, consultez IKEv2 Packet Exchange and Protocol Level Debugging (Échange de paquets IKEv2 et débogage au niveau du protocole).

Reposant sur des politiques comparativement à reposant sur des routes

VPN reposant sur des politiques

Comme son nom l'indique, un VPN reposant sur des politiques est un tunnel VPN IPsec avec une action de politique pour le trafic de transit qui répond aux critères de correspondance de la politique. Dans le cas des appareils Cisco, une liste de contrôle d'accès (ACL) est configurée et associée à une carte cryptographique pour préciser le trafic à rediriger vers le VPN et à chiffrer.

Les sélecteurs de trafic sont les sous-réseaux ou hôtes précisés dans la politique, comme le montre l'image:

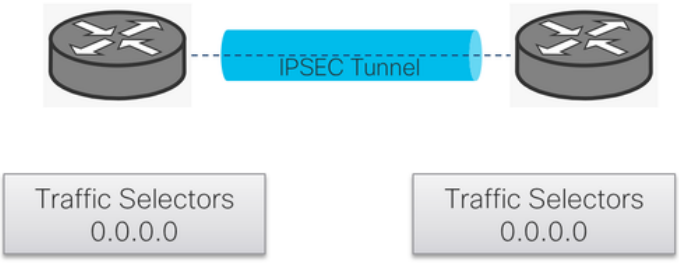


VPN reposant sur des routes

Une politique n'est pas nécessaire. Le trafic est redirigé vers les tunnels avec des routes, et il prend en charge le routage dynamique sur l'interface du tunnel. Les sélecteurs de trafic (trafic chiffré via le VPN) sont de 0.0.0.0 à 0.0.0.0 par défaut, comme illustré dans l'image :

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)
```

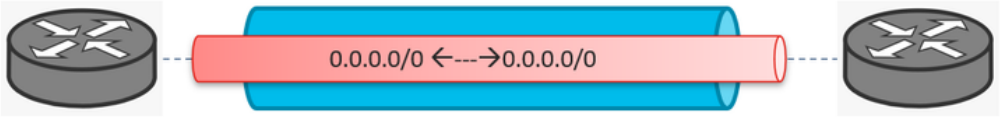
Remarque : en raison des sélecteurs de trafic 0.0.0.0, tout hôte ou sous-réseau est inclus dans. Par conséquent, une seule association de sécurité est créée. Il y a une exception pour le tunnel dynamique. Le présent document ne décrit pas les tunnels dynamiques.

Le VPN reposant sur des politiques et sur des routes peut être matérialisé comme le montre l'image:

ISAKMP-IPSEC Tunnel

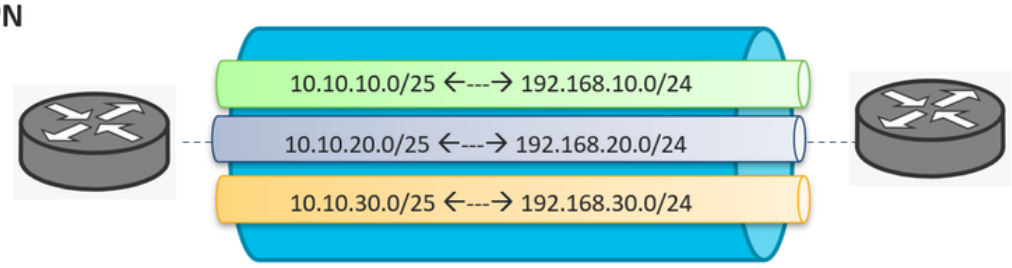
Route based VPN

*** Edges only support this.



Policy based VPN

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



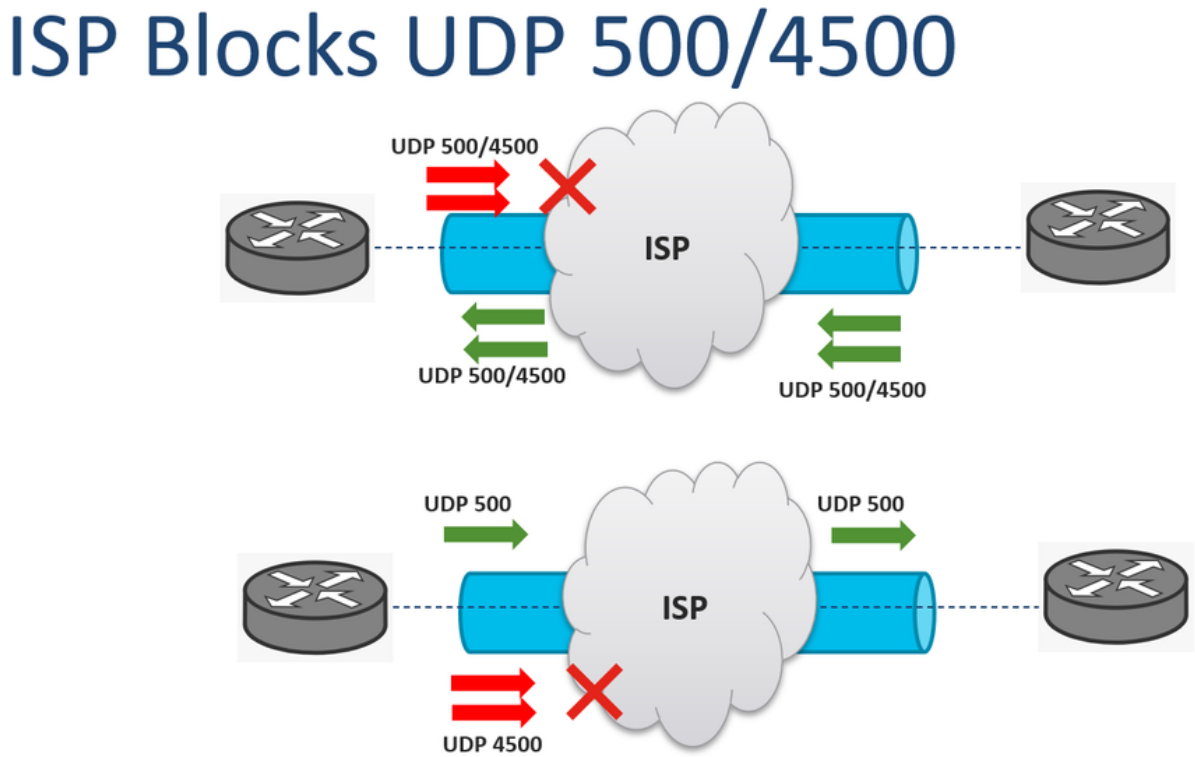
Remarque : Contrairement au VPN reposant sur des routes avec une seule SA, le VPN reposant sur les politiques peut créer plusieurs SA. Lors de la configuration d'une liste de contrôle d'accès (ACL), chaque instruction de la liste (si elles sont différentes) crée un sous-tunnel.

Problèmes courants liés au trafic non reçu par le VPN

Le fournisseur de services Internet bloque UDP 500/4500

Il est très courant que le fournisseur de services Internet (ISP) bloque les ports UDP 500/4500. Pour un établissement de tunnel IPsec, deux FAI différents peuvent être engagés. L'un d'eux peut bloquer les ports, et l'autre les autorise.

L'image montre les deux scénarios dans lesquels un fournisseur de services Internet ne peut bloquer les ports UDP 500/4500 que dans une direction:

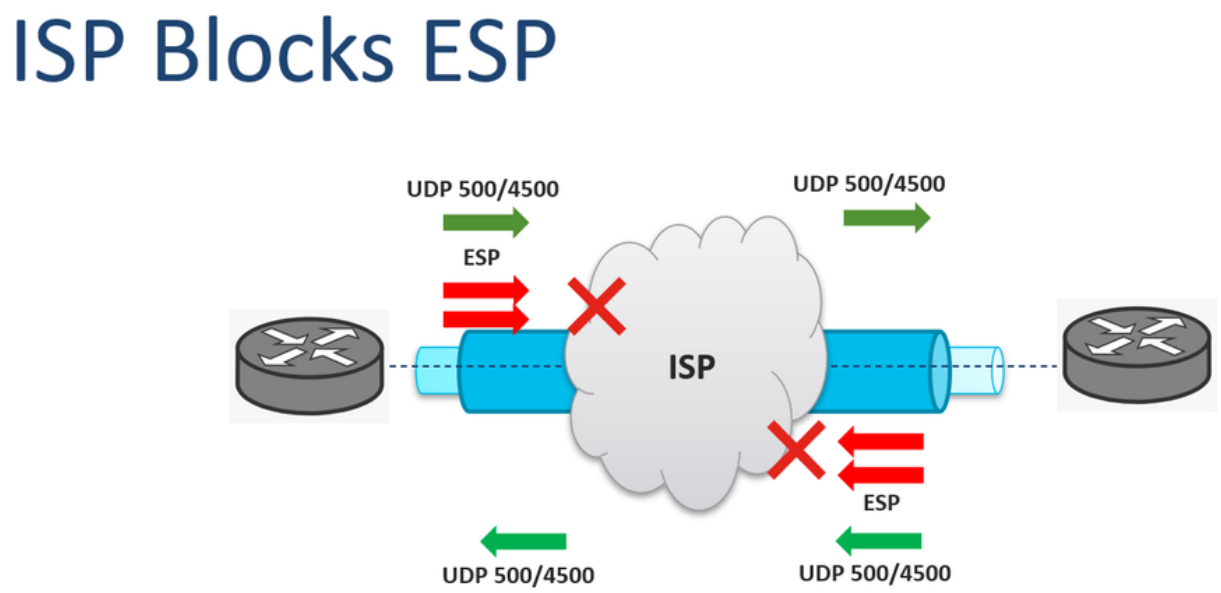


Remarque : Le port UDP 500 est utilisé par l'Internet Key Exchange (IKE) pour l'établissement de tunnels VPN sécurisés. L'UDP 4500 est utilisé lorsque la NAT est présente dans un point d'extrémité VPN.

Remarque : Lorsque le fournisseur de services Internet bloque UDP 500/4500, l'établissement du tunnel IPsec est touché, et il ne se déclenche pas.

Le fournisseur de services Internet bloque l’ESP

Un autre problème très courant sur les tunnels IPsec est que le FAI bloque le trafic ESP ; cependant, il autorise les ports UDP 500/4500. Par exemple, les ports UDP 500/4500 sont autorisés de manière bidirectionnelle. Par conséquent, le tunnel est correctement établi, mais les paquets ESP sont bloqués par le ou les FAI dans les deux directions. Cela entraîne l'échec du trafic chiffré via le VPN, comme indiqué dans l'image :



Remarque : lorsque le FAI bloque les paquets ESP, l'établissement du tunnel IPsec réussit, mais le trafic chiffré est affecté. Il peut être reflété avec le VPN activé, mais le trafic ne fonctionne pas sur lui.

Conseil : le scénario où le trafic ESP est bloqué dans une seule direction peut également être présent. Les symptômes sont les mêmes, mais il peut être facilement trouvé avec les informations statistiques du tunnel, l'encapsulation, les compteurs de décapsulation, ou les compteurs RX et TX.

Informations connexes

- Échange de paquets KEv2 et débogage au niveau du protocole
- Internet Key Exchange (IKE) – RFC 2409
- Protocole IKEv2 (Internet Key Exchange)
- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.