Entender o protocolo IKEv1 IPsec

Contents

Introdução

Este documento descreve o processo do protocolo Internet Key Exchange (IKEv1) para o estabelecimento de uma Virtual Private Network (VPN).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento de conceitos básicos de segurança:

- Autenticação
- Confidencialidade
- Integridade
- IPsec

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O processo de protocolo de Internet Key Exchange (IKEv1) para o estabelecimento de uma Rede Virtual Privada (VPN) é importante para entender a troca de pacotes para solucionar mais simples qualquer tipo de problema de Internet Protocol Security (IPsec) com IKEv1.

IPsec

O IPsec é um conjunto de protocolos que fornece segurança às comunicações da Internet na camada IP. O uso atual mais comum do IPsec é fornecer uma Rede Virtual Privada (VPN), entre dois locais (gateway a gateway) ou entre um usuário remoto e uma rede corporativa (host a gateway).

Protocolo IKE

O IPsec usa o protocolo IKE para negociar e estabelecer túneis de rede virtual privada (VPN - Virtual Private Network) de acesso remoto ou site a site. O protocolo IKE também é chamado de Internet Security Association and Key Management Protocol (ISAKMP) (Somente na Cisco).

Há duas versões do IKE:

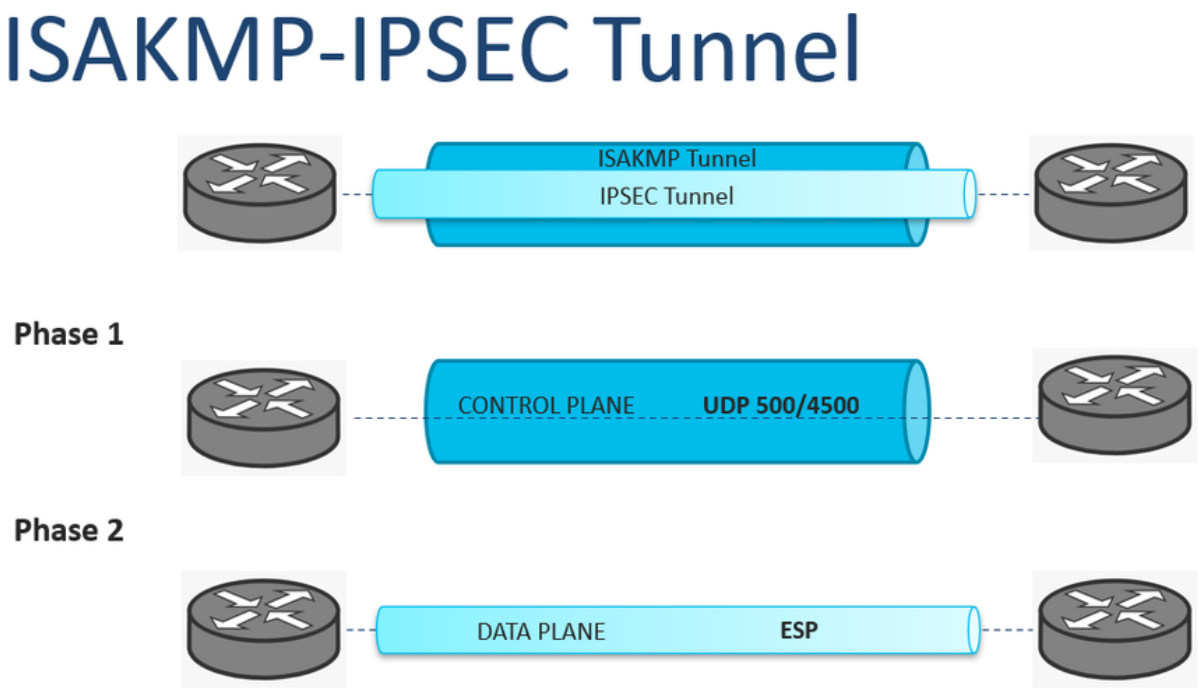
- IKEv1: definido no RFC 2409, o Internet Key Exchange
- IKE versão 2 (IKEv2): definido no RFC 4306, protocolo de intercâmbio de chave de Internet (IKEv2)

Fases IKE

O ISAKMP separa a negociação em duas fases:

- Fase 1: Os dois pares ISAKMP estabelecem um túnel seguro e autenticado, que protege as mensagens de negociação ISAKMP. Esse túnel é conhecido como ISAKMP SA. Há dois modos definidos pelo ISAKMP: Modo principal (MM) e Modo agressivo.
- Fase 2: Ele negocia os principais materiais e algoritmos para a criptografia (SAs) dos dados a serem transferidos pelo túnel IPsec. Essa fase é chamada de Modo Rápido.

Para materializar todos os conceitos abstratos, o túnel da Fase 1 é o túnel Pai e a fase 2 é um subtúnel. Esta imagem ilustra as duas fases como túneis:



Observação: o túnel da fase 1 (ISAKMP) protege o tráfego de VPN da placa de controle entre os dois gateways. O tráfego do plano de controle pode ser pacotes de negociação, pacotes de informações, DPD, keepalives, rechaveamento e assim por diante. A negociação de ISAKMP usa as portas UDP 500 e 4500 para estabelecer um canal seguro.

Observação: o túnel da fase 2 (IPsec) protege o tráfego do plano de dados que passa pela VPN entre os dois gateways. Os algoritmos usados para proteger os dados são configurados na Fase 2 e são independentes dos especificados na Fase 1.
O protocolo usado para encapsular e criptografar esses pacotes é o Encapsulation Security Payload (ESP).

Modos IKE (Fase 1)

Modo principal

Uma sessão IKE começa quando o iniciador envia uma proposta ou proposta ao respondente. A primeira troca entre nós estabelece a política de segurança básica; o iniciador propõe os algoritmos de criptografia e autenticação a serem usados. O respondente escolhe a proposta apropriada (suponha que uma proposta seja escolhida) e a envia ao iniciador. A próxima troca passa chaves públicas Diffie-Hellman e outros dados. Todas as outras negociações são criptografadas dentro do SA IKE. A terceira troca autentica a sessão ISAKMP. Uma vez que o SA de IKE é estabelecido, a negociação de IPSec (Modo Rápido) é iniciada.

Modo agressivo

O Modo Agressivo compacta a negociação IKE SA em três pacotes, com todos os dados necessários para a SA passados pelo iniciador. O respondente envia a proposta, o material-chave e a ID e autentica a sessão no próximo pacote. O iniciador responde e autentica a sessão. A negociação é mais rápida, e a ID do iniciador e do respondente é liberada.

Modo IPsec (Fase 2)

Modo Rápido

A negociação IPSec, ou Modo Rápido, é semelhante a uma negociação IKE de Modo Agressivo, exceto a negociação, deve ser protegida dentro de uma SA IKE. O Modo Rápido negocia o SA para a criptografia de dados e gerencia a troca de chaves para esse SA IPSec.

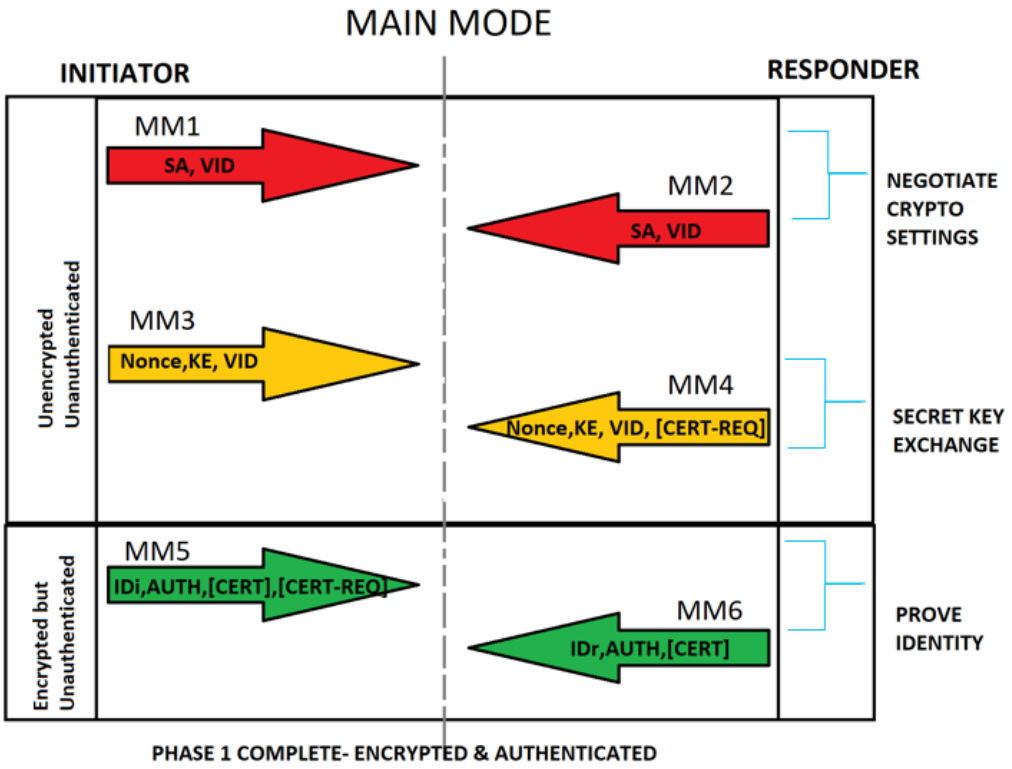
Glossário IKE

- Uma associação de segurança (SA) é o estabelecimento de atributos de segurança compartilhados entre duas entidades de rede para oferecer suporte à comunicação segura. Uma SA inclui atributos como algoritmo e modo criptográfico, chave de criptografia de tráfego e parâmetros para que os dados da rede sejam passados pela conexão.
- As IDs de fornecedor (VIDs) são processadas para determinar se o peer oferece suporte ao recurso NAT-Traversal, Dead Peer Detection, Fragmentation e assim por diante.
- Nonce: um número gerado aleatoriamente enviado pelo iniciador. Este nonce é misturado com outros itens com a chave acordada usada e é enviado de volta. O iniciador verifica o cookie e o nonce e rejeita qualquer mensagem que não tenha o nonce correto. Isso ajuda a evitar a repetição, já que nenhum terceiro pode prever o que é o nonce gerado aleatoriamente.
- Informações de troca de chaves (KE) para o processo de troca segura de chaves Diffie-Hellman (DH).
- O iniciador/respondente de identidade (IDi/IDr.) é usado para enviar informações de autenticação ao par. Estas informações são transmitidas sob a proteção do segredo comum partilhado.
- A troca de chaves Diffie-Hellman (DH) é um método de troca segura de algoritmos criptográficos através de um canal público.
- A chave compartilhada de IPSec pode ser derivada com o DH usado novamente para garantir Perfect Forward Secrecy (PFS) ou a troca DH original atualizada para o segredo

compartilhado derivado anteriormente.

Troca de pacotes do modo principal

Cada pacote ISAKMP contém informações de payload para o estabelecimento de túnel. O glossário IKE explica as abreviações IKE como parte do conteúdo de payload para a troca de pacotes no modo principal, como mostrado nesta imagem.

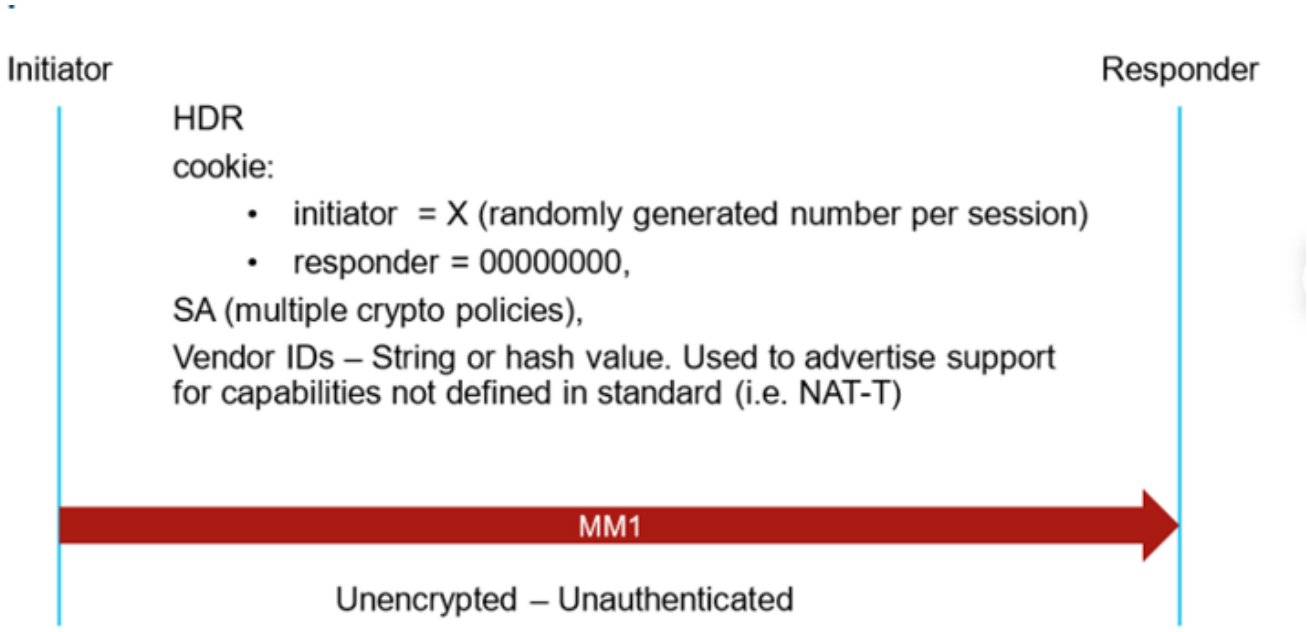


Modo principal 1 (MM1)

Para definir os termos das negociações de ISAKMP, crie uma política de ISAKMP, que inclui:

- Um método de autenticação, para garantir a identidade dos pares.
- Um método de criptografia, para proteger os dados e garantir a privacidade.
- Um método de Códigos de Autenticação de Mensagem com Hash (HMAC) para garantir a identidade do remetente e para garantir que a mensagem não tenha sido modificada em trânsito.
- Um grupo Diffie-Hellman para determinar a força do algoritmo de determinação da chave de criptografia. O Security Appliance usa esse algoritmo para derivar as chaves de criptografia e hash.
- Um limite de tempo para o Security Appliance usar uma chave de criptografia antes de ser substituído.

O primeiro pacote é enviado pelo iniciador da negociação IKE, como mostrado na imagem:



Observação: o Main Mode 1 é o primeiro pacote da negociação IKE. Portanto, o SPI do iniciador é definido como um valor aleatório, enquanto o SPI do respondente é definido como 0. No segundo pacote (MM2), o SPI do Respondente deve ser respondido com um novo valor e a negociação inteira mantém os mesmos valores de SPIs.

Se o MM1 for capturado e um analisador de protocolo de rede Wireshark for usado, o valor SPI estará dentro do conteúdo do Internet Security Association and Key Management Protocol, como mostrado na imagem:

```
> 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)
```

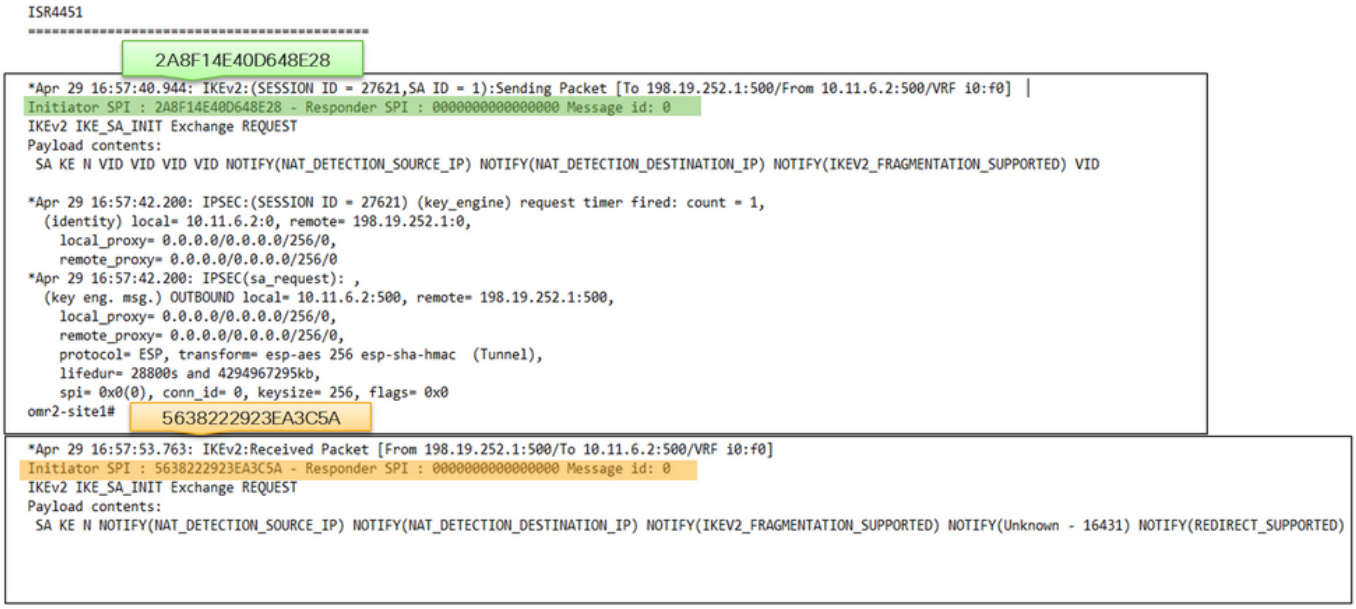
Observação: caso o pacote MM1 se perca no caminho ou não haja resposta MM2, a negociação IKE mantém as retransmissões MM1 até que o número máximo de retransmissões seja atingido. Neste ponto, o Iniciador mantém o mesmo SPI até que a próxima negociação seja acionada novamente.

Dica: a identificação de SPIs do iniciador e do respondente é muito útil para identificar várias negociações para a mesma VPN e restringir alguns problemas de negociação.

Identificar duas negociações simultâneas

Nas plataformas Cisco IOS® XE, as depurações podem ser filtradas por túnel com um condicional

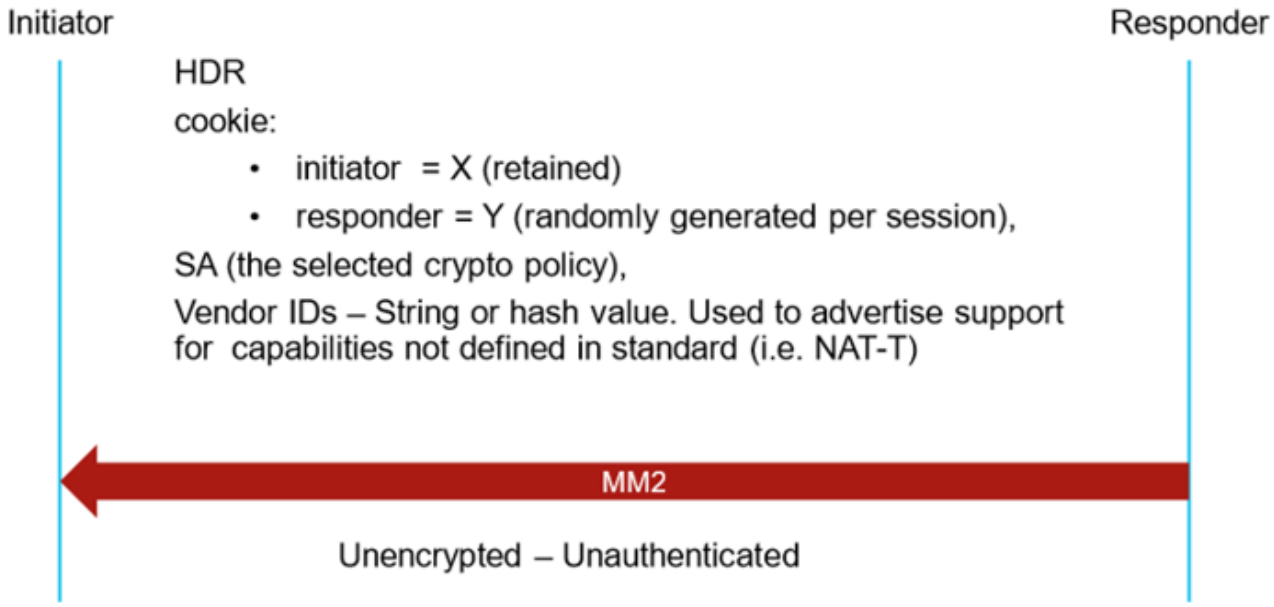
para o endereço IP remoto configurado. No entanto, as negociações simultâneas são exibidas nos logs e não há como filtrá-las. É necessário fazê-lo manualmente. Como mencionado anteriormente, a negociação inteira mantém os mesmos valores SPI para o iniciador e o respondente. Caso um pacote seja recebido do mesmo endereço IP de peer, mas o SPI não corresponda ao valor anterior rastreado antes que a negociação atinja o número máximo de retransmissão, trata-se de outra negociação para o mesmo peer, como mostrado na imagem:



Observação: o exemplo mostra a negociação simultânea para o primeiro pacote na negociação (MM1). No entanto, isso pode ocorrer em qualquer ponto de negociação. Todos os pacotes subsequentes devem incluir um valor diferente de 0 no SPI do respondente.

Modo principal 2 (MM2)

No pacote Main Mode 2 (Modo principal 2), o respondente envia a política selecionada para as propostas correspondentes e o SPI do respondente é definido como um valor aleatório. A negociação inteira mantém os mesmos valores de SPIs. O MM2 responde ao MM1 e o respondedor SPI é definido com um valor diferente de 0, como mostrado na imagem:



Se o MM2 for capturado e um analisador de protocolo de rede Wireshark for usado, os valores SPI do iniciador e SPI do respondente estarão dentro do conteúdo do Internet Security Association and Key Management Protocol, como mostrado na imagem:

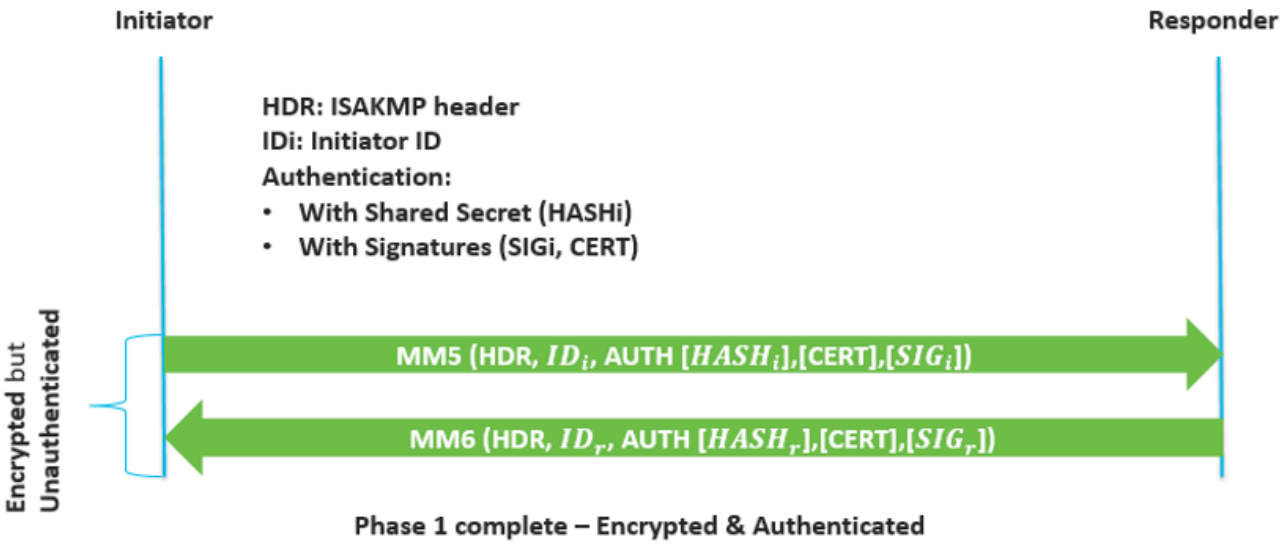
```
> Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
> Internet Protocol Version 4, Src: 209.134.162.150, Dst: 170.49.116.200
> User Datagram Protocol, Src Port: 500, Dst Port: 500
v Internet Security Association and Key Management Protocol
    Initiator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

Modo principal 3 e 4 (MM3-MM4)

Os pacotes MM3 e MM4 ainda não são criptografados e não são autenticados, e ocorre a troca de chave secreta. MM3 e MM4 são mostrados na imagem:

Modo principal 5 e 6 (MM5-MM6)

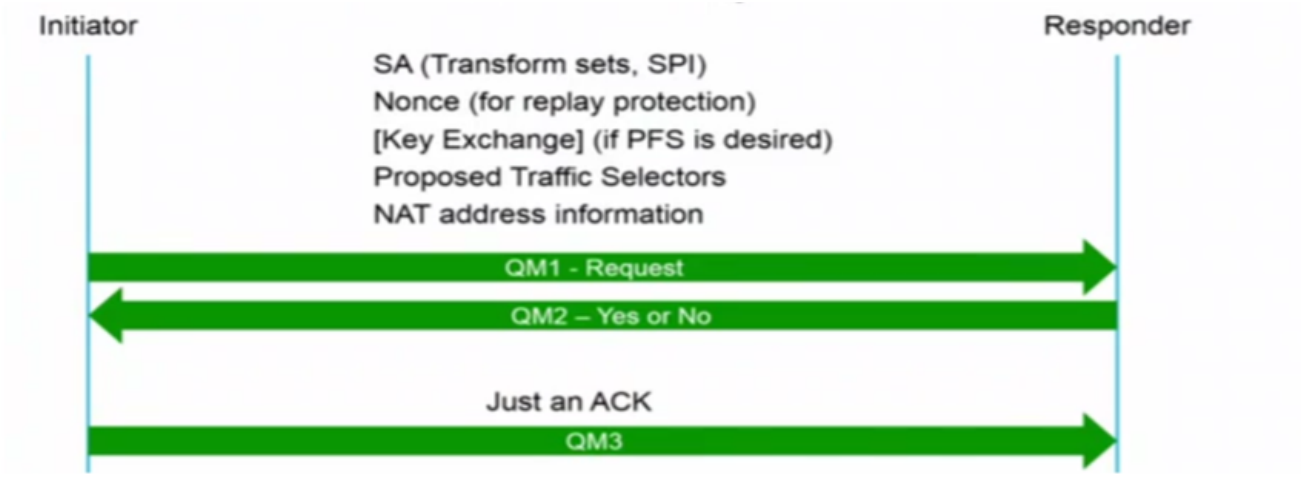
Os pacotes MM5 e MM6 já estão criptografados, mas ainda não foram autenticados. Nesses pacotes, a autenticação ocorre conforme mostrado na imagem:



Modo Rápido (QM1, QM2 e QM3)

O modo rápido ocorre depois que o modo principal e o IKE estabelecem o túnel seguro na fase 1. O Modo Rápido negocia a política IPSec compartilhada para os algoritmos de segurança IPSec e gerencia a troca de chaves para o estabelecimento de IPSec SA. Os momentos são usados para gerar novo material de chave secreta compartilhada e evitar ataques de repetição de SAs falsas geradas.

Três pacotes são trocados nesta fase, como mostrado na imagem:



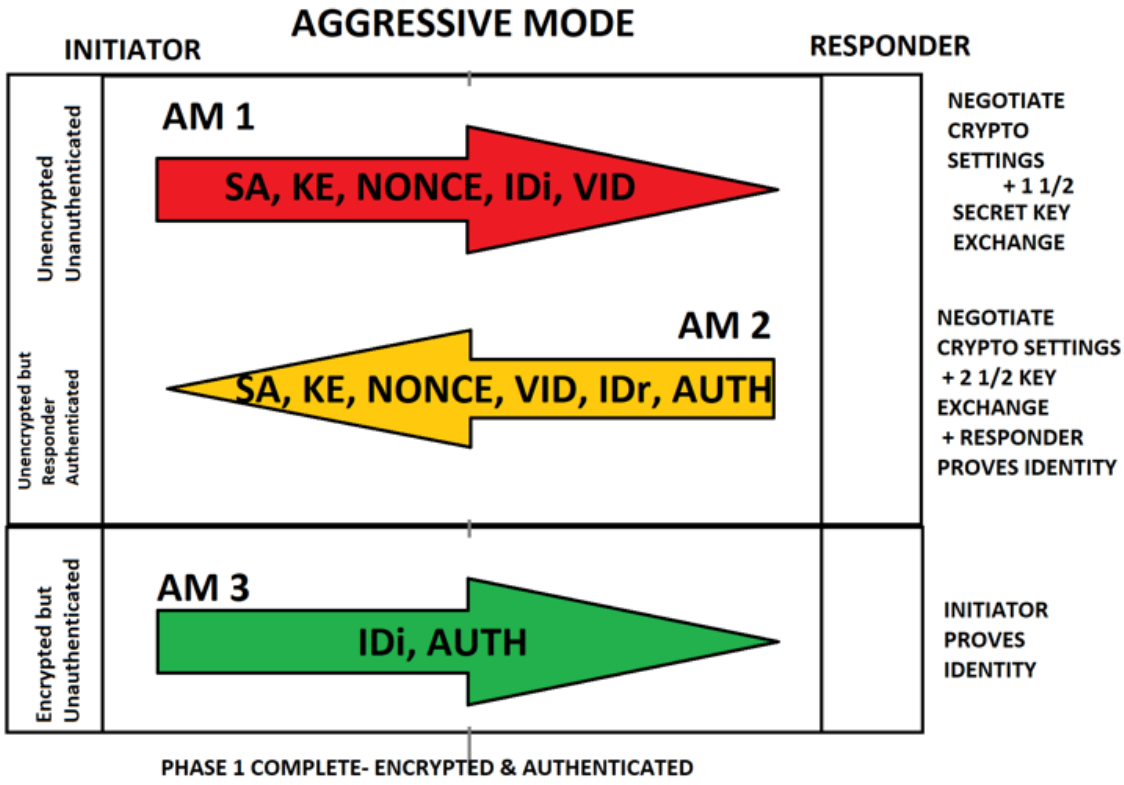
Troca de pacotes de modo agressivo

O Modo Agressivo compacta a negociação IKE SA em três pacotes, com todos os dados necessários para a SA passados pelo iniciador.

- O respondente envia a proposta, o material-chave e a ID e autentica a sessão no próximo pacote.
- O iniciador responde e autentica a sessão.

- A negociação é mais rápida, e a ID do iniciador e do respondente é liberada.

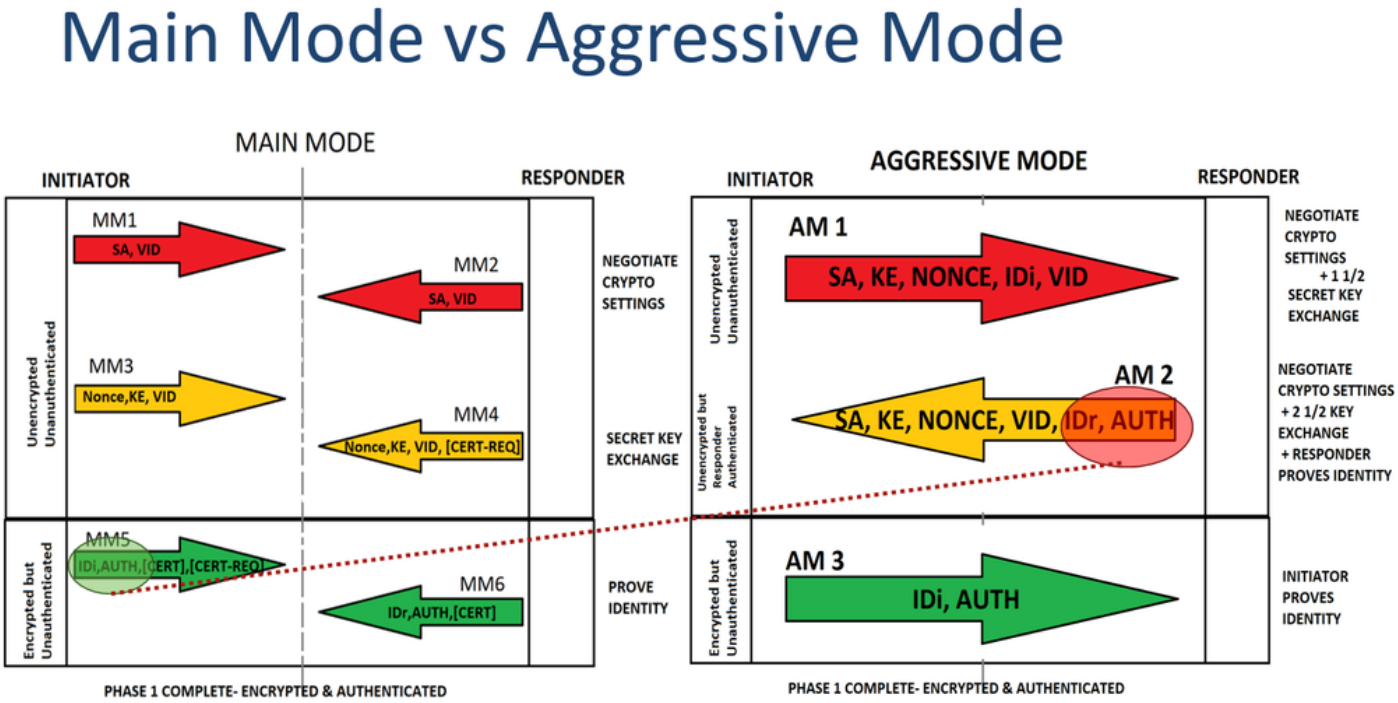
A imagem mostra o conteúdo de payload dos três pacotes trocados no modo Agressivo:



Modo principal vs Modo agressivo

Em comparação com o modo principal, o modo agressivo se reduz a três pacotes:

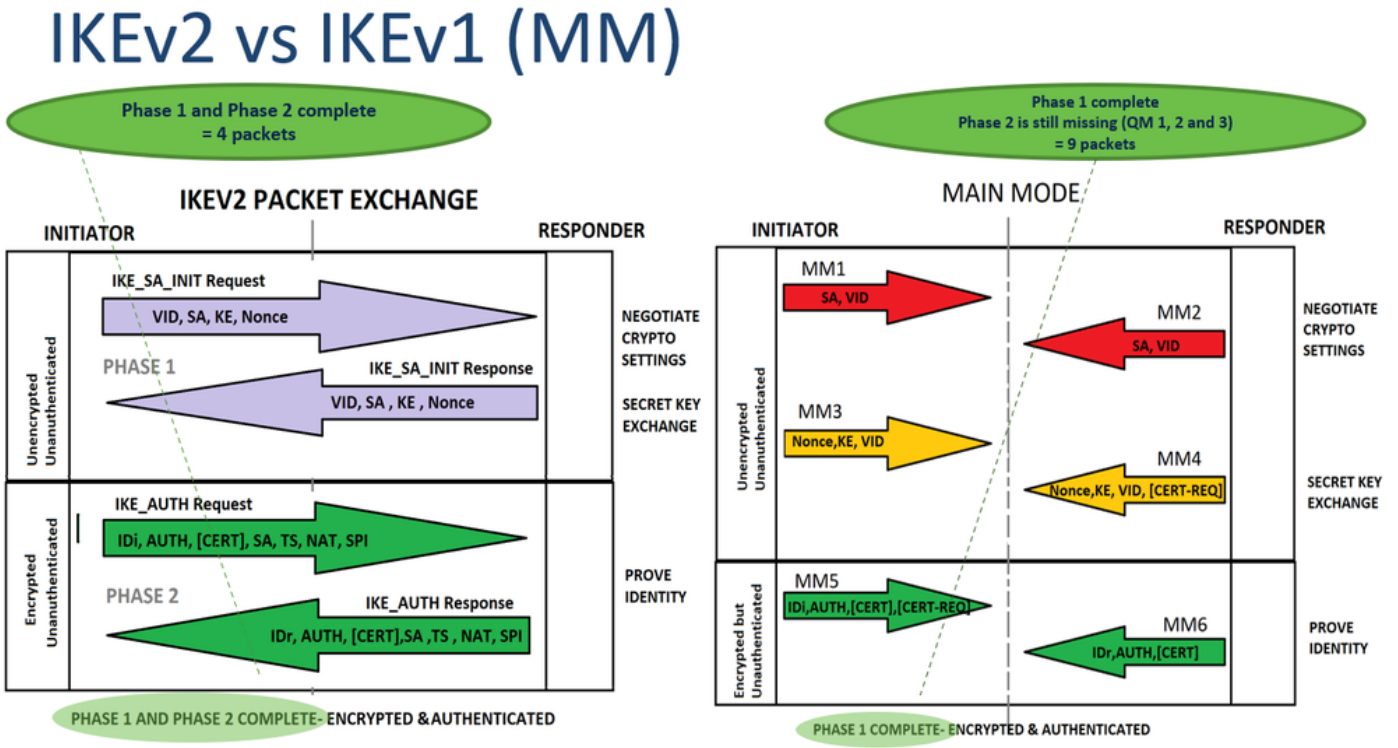
- A AM 1 absorve MM1 e MM3.
- AM 2 absorve MM2, MM4 e parte do MM6. É daí que vem a vulnerabilidade do Modo agressivo. O AM 2 compõe o IDr e a Autenticação não criptografados. Ao contrário do modo principal, essas informações são criptografadas.
- AM 3 fornece o IDi e a Autenticação. Esses valores são criptografados.



Intercâmbio de pacotes IKEv2 vs IKEv1

Na negociação de IKEv2, menos mensagens são trocadas para estabelecer um túnel. IKEv2 usa quatro mensagens; IKEv1 usa seis mensagens (no modo principal) ou três mensagens (no modo agressivo).

Os tipos de mensagem IKEv2 são definidos como pares de Solicitação e Resposta. A imagem mostra a comparação de pacotes e conteúdo de payload de IKEv2 versus IKEv1:



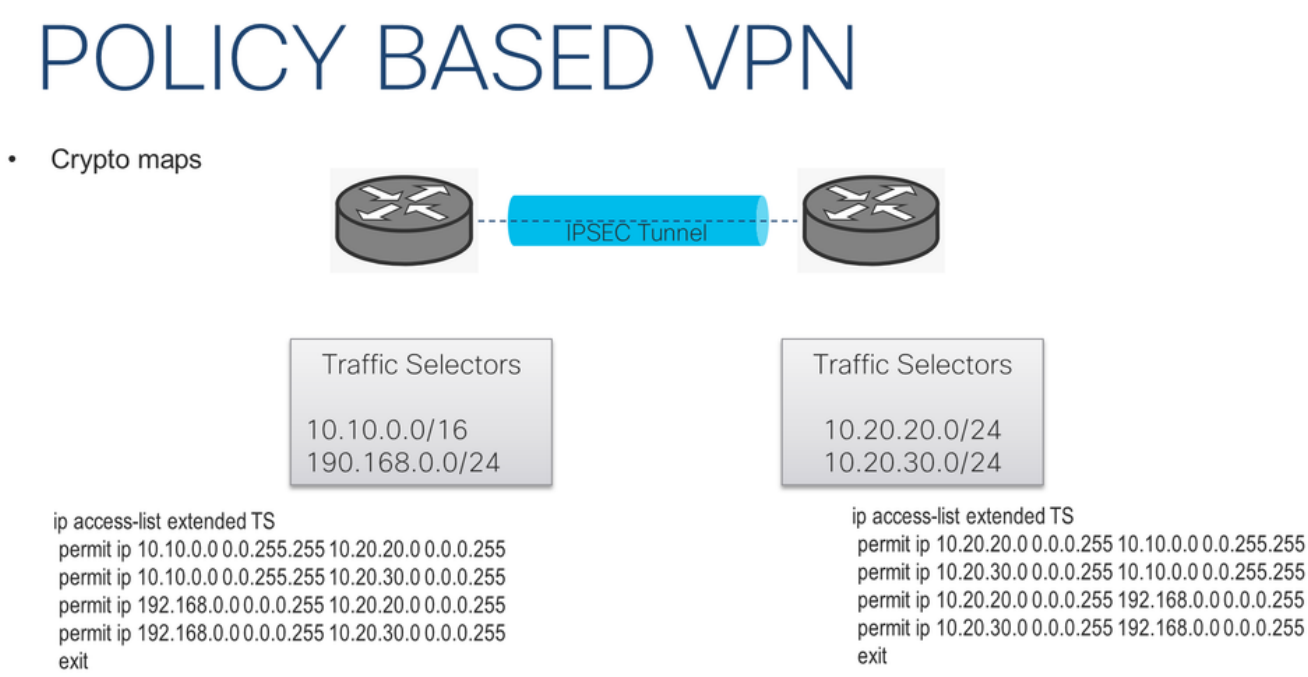
Observação: este documento não se aprofunda na troca de pacotes IKEv2. Para obter mais referências, navegue para Intercâmbio de pacotes IKEv2 e Depuração de nível de protocolo.

Com base em políticas versus com base em rotas

VPN baseada em políticas

Como o nome diz, uma VPN baseada em política é um túnel VPN IPsec com uma ação de política para o tráfego de trânsito que atende aos critérios de correspondência da política. No caso de dispositivos Cisco, uma lista de acesso (ACL) é configurada e anexada a um mapa de criptografia para especificar o tráfego a ser redirecionado para a VPN e criptografado.

Os seletores de tráfego são as sub-redes ou os hosts especificados na política, conforme mostrado na imagem:

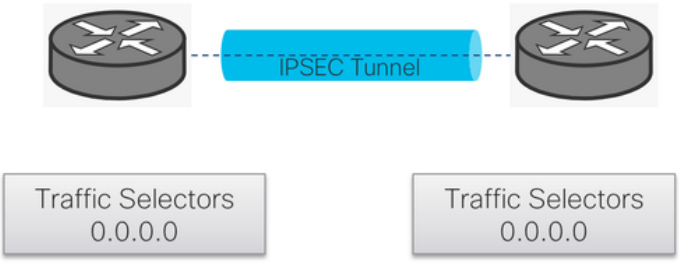


VPN baseada em rota

Uma política não é necessária. O tráfego é redirecionado para os túneis com rotas e suporta o roteamento dinâmico na interface do túnel. Os seletores de tráfego (tráfego criptografado através da VPN) são de 0.0.0.0. a 0.0.0.0 por padrão, como mostrado na imagem:

ROUTE BASED VPN

- Supports dynamic routing over the tunnel interface.

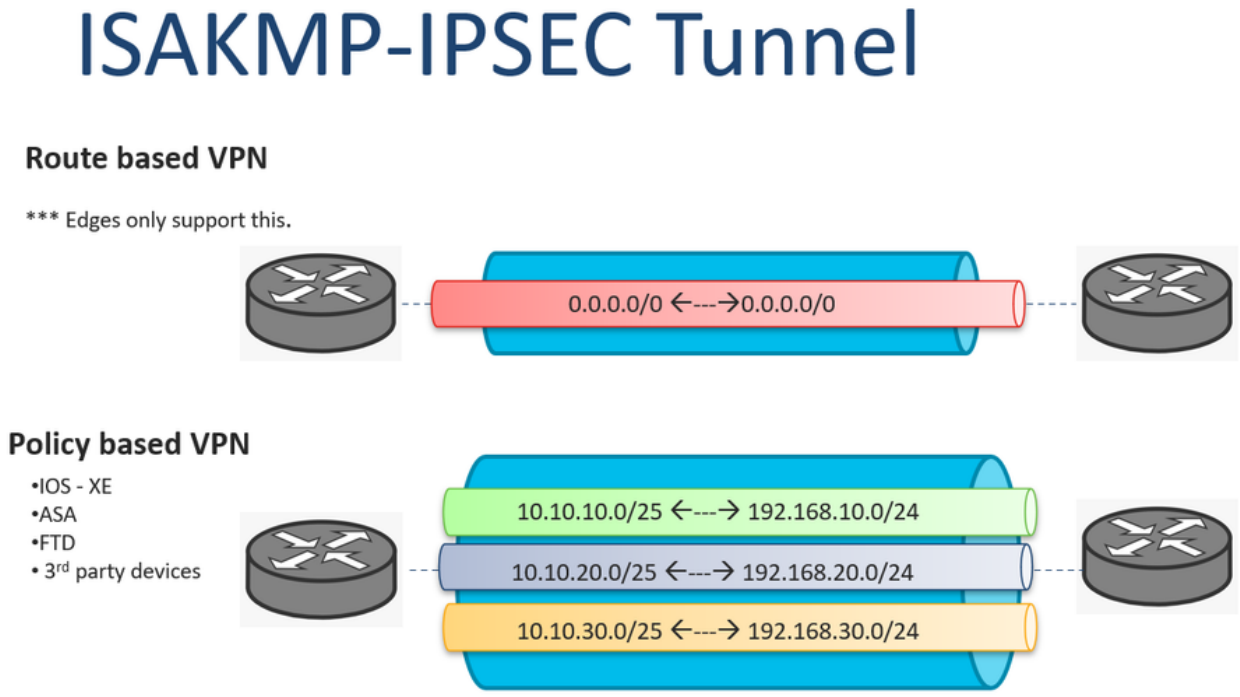



```
interface: Tunnel100001
   Crypto map tag: Tunnel100001-head-0, local addr 10.0.21.17

  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)
```

Observação: devido aos seletores de Tráfego serem 0.0.0.0, qualquer host ou sub-rede é incluído dentro do. Portanto, somente uma SA é criada. Há uma exceção para túnel dinâmico. Este documento não descreve os túneis dinâmicos.

A política e a VPN baseada em rota podem ser materializadas conforme mostrado na imagem:



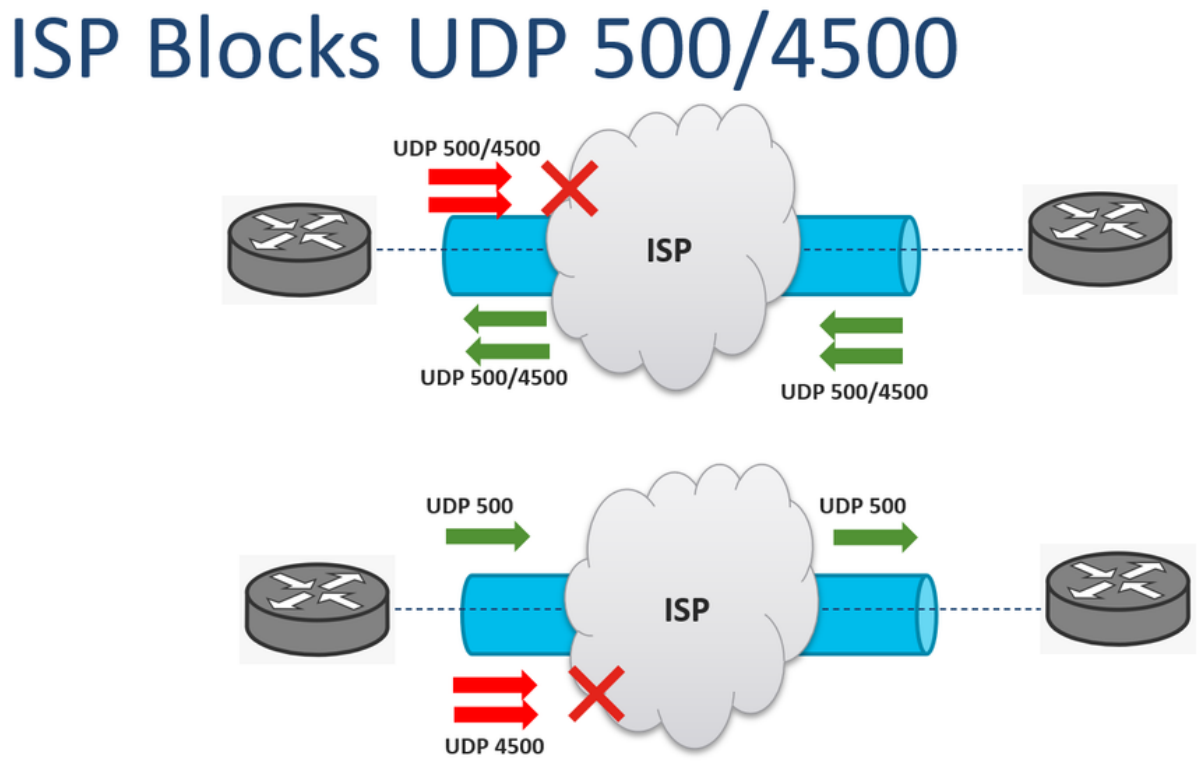
Observação: ao contrário da VPN baseada em rota com apenas um SA criado, a VPN baseada em política pode criar vários SAs. À medida que uma ACL é configurada, cada instrução na ACL (se forem diferentes entre elas) cria um subtúnel.

Problemas comuns de tráfego não recebido através da VPN

ISP bloqueia UDP 500/4500

É muito comum que o Provedor de Serviços de Internet (ISP) bloqueie as portas UDP 500/4500. Para o estabelecimento de um túnel IPsec, dois ISPs diferentes podem ser ativados. Um deles pode bloquear as portas e o outro permite.

A imagem mostra os dois cenários em que um ISP pode bloquear as portas UDP 500/4500 em apenas uma direção:

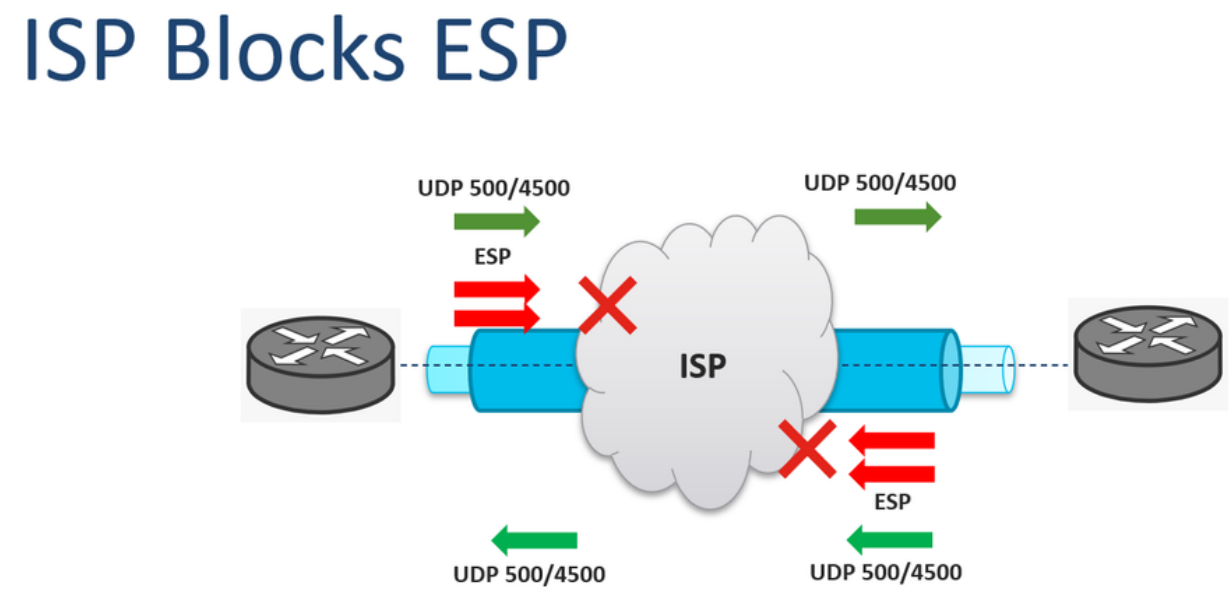


Observação: a porta UDP 500 é usada pelo Internet Key Exchange (IKE) para o estabelecimento de túneis VPN seguros. O UDP 4500 é usado quando o NAT está presente em um endpoint de VPN.

Observação: quando o ISP bloqueia o UDP 500/4500, o estabelecimento de túnel IPsec é afetado e não é ativado.

Blocos ISP ESP

Outro problema muito comum nos túneis IPsec é que o ISP bloqueia o tráfego ESP; no entanto, ele permite as portas UDP 500/4500. Por exemplo, as portas UDP 500/4500 são permitidas de maneira bidirecional. Portanto, o túnel é estabelecido com êxito, mas os pacotes ESP são bloqueados pelo ISP ou pelos ISPs em ambas as direções. Isso faz com que o tráfego criptografado através da VPN falhe, como mostrado na imagem:



Observação: quando o ISP bloqueia pacotes ESP, o estabelecimento de túnel IPsec é bem-sucedido, mas o tráfego criptografado é afetado. Ele pode ser refletido com a VPN ativada, mas o tráfego não funciona sobre ela.

Dica: o cenário em que o tráfego ESP é bloqueado apenas em uma direção também pode estar presente. Os sintomas são os mesmos, mas podem ser facilmente encontrados com as informações de estatísticas de túnel, encapsulamento, contadores de desencapsulamento ou contadores RX e TX.

Informações Relacionadas

- Intercâmbio de pacotes KEv2 e depuração no nível de protocolo
- O Internet Key Exchange (IKE) - RFC 2409
- Protocolo Internet Key Exchange (IKEv2)
- Suporte Técnico e Documentação - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.