Intercâmbio de pacote IKEv2 e depuração de nível de protocolo

Contents

Introduction

Este documento descreve as vantagens da versão mais recente do Internet Key Exchange (IKE) e as diferenças entre a versão 1 e a versão 2.

IKE é o protocolo usado para configurar uma associação de segurança (SA) no conjunto de protocolos IPsec. IKEv2 é a segunda e mais recente versão do protocolo IKE. A adoção deste protocolo começou já em 2006. A necessidade e a intenção de uma revisão do protocolo IKE foram descritas no Apêndice A do *Protocolo IKEv2* no RFC 4306.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

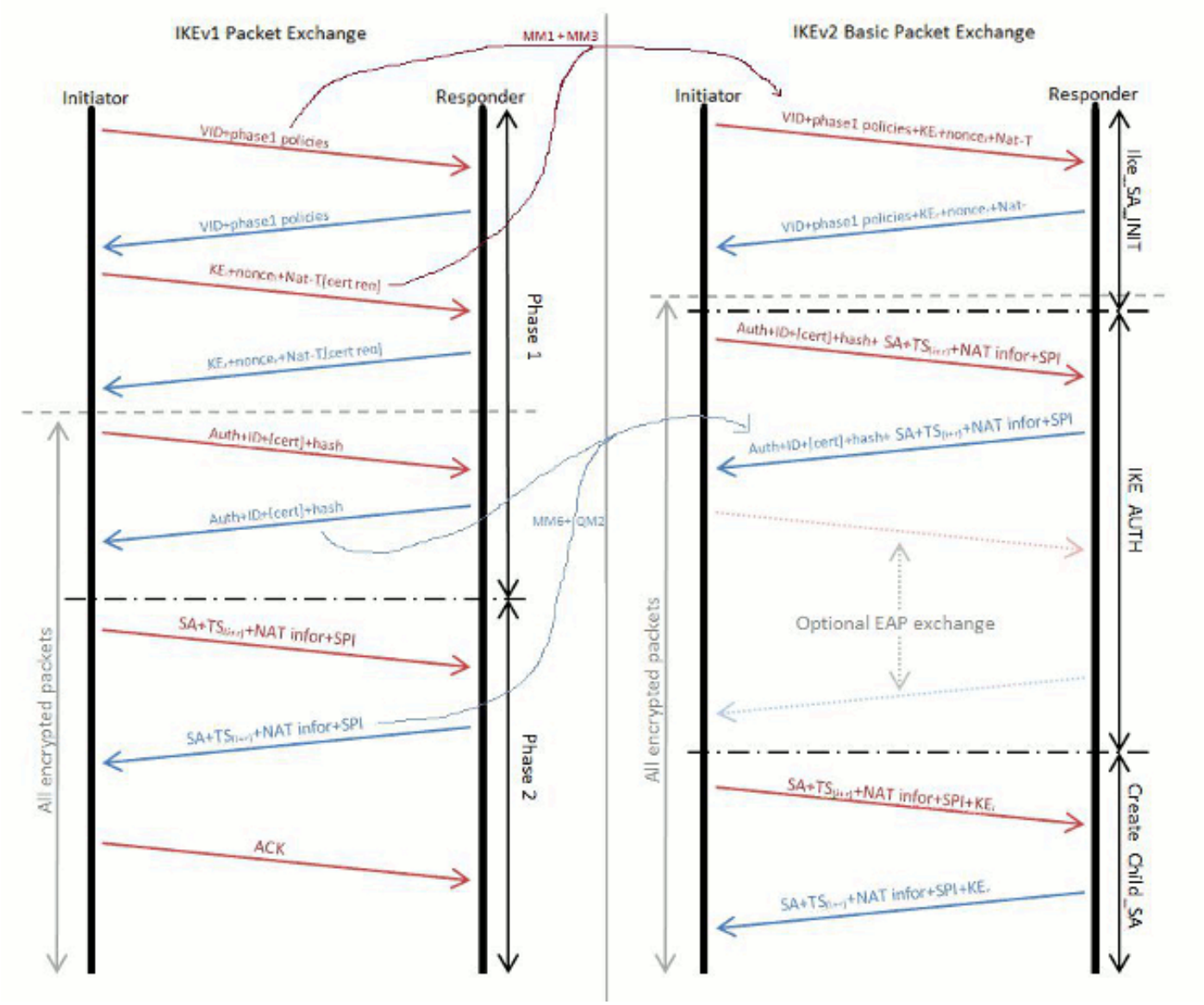
Este documento não se restringe a versões de software e hardware específicas.

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Diferenças entre IKEv1 e IKEv2

Embora o *protocolo IKEv2 (Internet Key Exchange)* no RFC 4306 descreva com grande detalhe as vantagens do IKEv2 sobre IKEv1, é importante observar que todo o intercâmbio IKE foi revisado. Este diagrama fornece uma comparação das duas trocas:



No IKEv1, houve uma troca de fase 1 claramente demarcada, que contém seis pacotes seguidos de uma troca de fase 2 composta por três pacotes; a troca de IKEv2 é variável. Na melhor das hipóteses, pode trocar até quatro pacotes. Na pior das hipóteses, isso pode aumentar para até 30 pacotes (se não mais), dependendo da complexidade da autenticação, do número de atributos do Extensible Authentication Protocol (EAP) usados, bem como do número de SAs formados. O IKEv2 combina as informações da Fase 2 em IKEv1 na troca IKE_AUTH e garante que após a conclusão da troca IKE_AUTH, ambos os pares já têm um SA criado e pronto para criptografar o tráfego. Essa SA é criada somente para as identidades de proxy que correspondem ao pacote de disparo. Qualquer tráfego subsequente que corresponda a outras identidades de proxy dispara a troca CREATE_CHILD_SA, que é o equivalente da troca da Fase 2 em IKEv1. Não há modo agressivo ou modo principal.

Fases Iniciais no Intercâmbio IKEv2

Na verdade, o IKEv2 tem apenas duas fases iniciais de negociação:

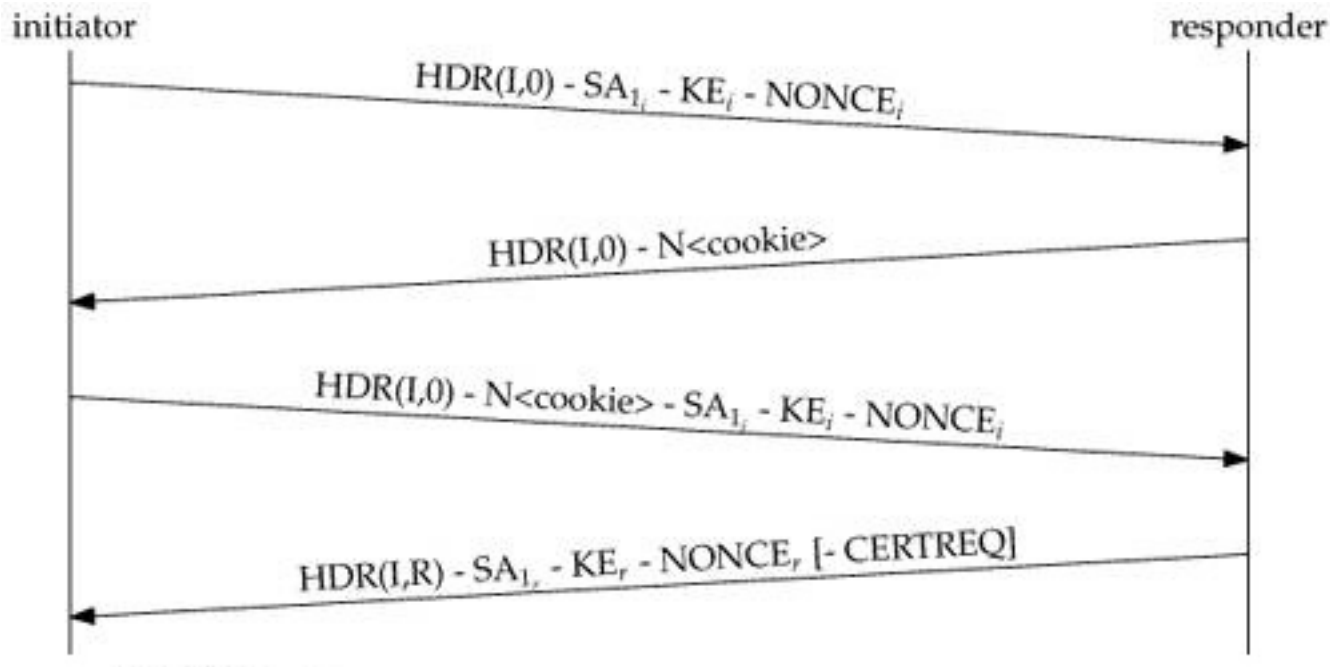
- IKE_SA_INIT Exchange
- Troca IKE_AUTH

IKE_SA_INIT Exchange

IKE_SA_INIT é a troca inicial na qual os colegas estabelecem um canal seguro. Depois de concluir a troca inicial, todas as outras trocas serão criptografadas. As trocas contêm apenas dois pacotes porque combinam todas as informações normalmente trocadas em MM1-4 em IKEv1. Como resultado, o respondente é computacionalmente caro para processar o pacote IKE_SA_INIT e pode sair para processar o primeiro pacote; ele deixa o protocolo aberto a um ataque DOS de endereços falsificados.

Para proteger contra esse tipo de ataque, o IKEv2 tem uma troca opcional dentro do IKE_SA_INIT para evitar ataques fraudulentos. Se um determinado limite de sessões incompletas for atingido, o respondente não processará o pacote mais além, mas enviará uma resposta ao iniciador com um cookie. Para que a sessão continue, o iniciador deve reenviar o pacote IKE_SA_INIT e incluir o cookie recebido.

O iniciador reenvia o pacote inicial junto com a carga de notificação do respondente que prova que a troca original não foi falsificada. Aqui está um diagrama da troca IKE_SA_INIT com desafio de cookie:



Troca IKE_AUTH

Após a conclusão da troca IKE_SA_INIT, o SA IKEv2 é criptografado; no entanto, o peer remoto não foi autenticado. A troca IKE_AUTH é usada para autenticar o peer remoto e criar a primeira SA IPsec.

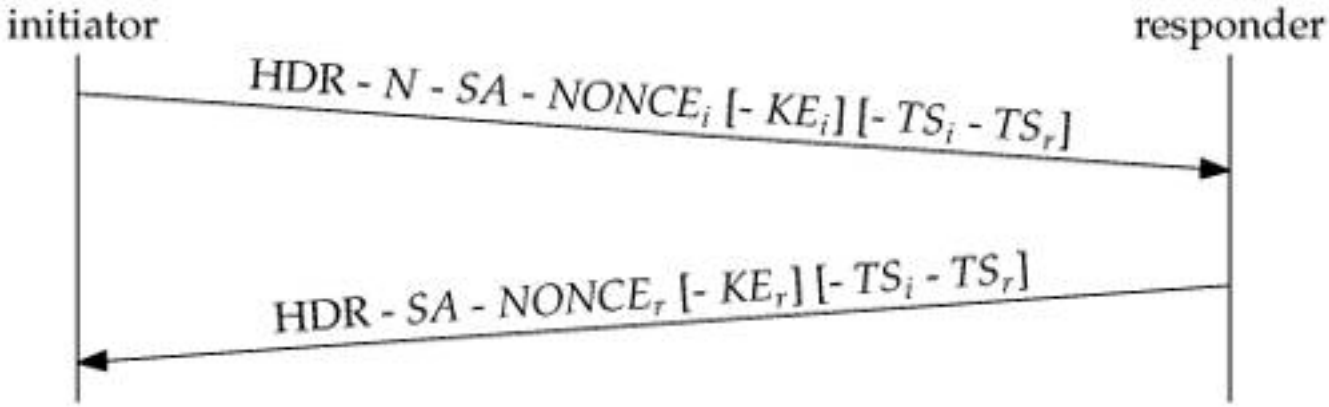
O intercâmbio contém a ID da Internet Security Association and Key Management Protocol (ISAKMP) junto com um payload de autenticação. O conteúdo do payload de autenticação depende do método de autenticação, que pode ser Pre-Shared Key (PSK), certificados RSA

(RSA-SIG), certificados Elliptic Curve Digital Signature Algorithm (ECDSA-SIG) ou EAP. Além dos payloads de autenticação, a troca inclui os payloads SA e do Seletor de Tráfego que descrevem a SA IPsec a ser criada.

Trocas de IKEv2 posteriores

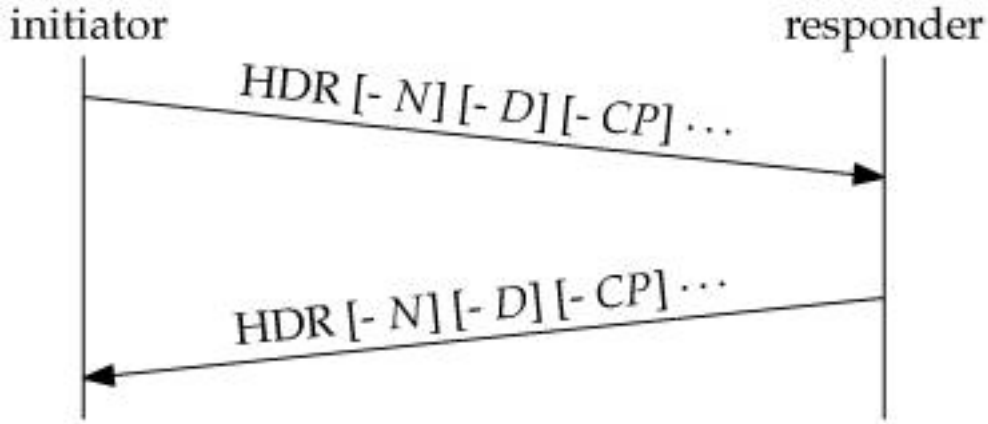
CREATE_CHILD_SA Exchange

Se houver necessidade de SAs filho adicionais ou se o SA IKE ou um dos SAs filho precisar ser rechaveado, ele terá a mesma função que a troca de modo rápido tem no IKEv1. Como mostrado neste diagrama, há apenas dois pacotes nesta troca; no entanto, a troca se repete para cada chave ou SA novo:



Troca INFORMATIVA

Como está em todas as trocas de IKEv2, cada solicitação de Troca de INFORMAÇÕES espera uma resposta. Três tipos de cargas úteis podem ser incluídos em uma troca INFORMATIVA. Qualquer número de qualquer combinação de cargas úteis pode ser incluído, como mostrado neste diagrama:



- A carga útil Notify (N) já foi vista em conjunto com cookies. Há vários outros tipos também. Eles carregam informações de erro e status, como fazem no IKEv1.
- O payload Delete (D) informa ao peer que o remetente excluiu uma ou mais de suas SAs de entrada. Espera-se que o respondente exclua essas SAs e geralmente inclui Delete payloads para as SAs que correspondem na outra direção em sua mensagem de resposta.
- O payload de configuração (CP) é usado para negociar dados de configuração entre os peers. Um uso importante do CP é solicitar (solicitar) e atribuir (responder) um endereço em

uma rede protegida por um gateway de segurança. Em um caso típico, um host móvel estabelece uma VPN (Virtual Private Network) com um gateway de segurança em sua rede residencial e solicita que lhe seja dado um endereço IP na rede residencial.**Observação:** isso elimina um dos problemas que o uso combinado do L2TP (Layer 2 Tunneling Protocol) e do IPsec deve resolver.

Informações Relacionadas

- Depurações do ASA IKEv2 para VPN site a site com PSKs TechNote
- ASA IPsec e IKE debugs (modo principal IKEv1) - Nota técnica de solução de problemas
- IOS IPSec e depurações IKE - IKEv1 Main Mode Troubleshooting TechNote
- IPSec ASA e depurações de IKE - modo agressivo IKEv1 TechNote
- Dispositivos de segurança adaptáveis Cisco ASA 5500 Series
- Downloads de software dos dispositivos de segurança adaptável Cisco ASA 5500 Series
- Negociação IPsec/Protocolos IKE
- Cisco IOS Firewall
- Cisco IOS Software
- Secure Shell (SSH)
- Negociação IPsec/Protocolos IKE
- Suporte Técnico e Documentação - Cisco Systems