Eliminação de erros do intercâmbio de pacotes IKEv2 e do nível de protocolo

Índice

Introdução

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

O IKE é o protocolo usado para estabelecer uma associação de segurança (SA) na série de protocolo IPSec. IKEv2 é a segunda e versão a mais atrasada do protocolo IKE. Adoção para este protocolo começado a partir de 2006. A necessidade e a intenção de uma revisão do protocolo IKE foram descritas no apêndice A do *protocolo do intercâmbio de chave de Internet (IKEv2) no* RFC 4306.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

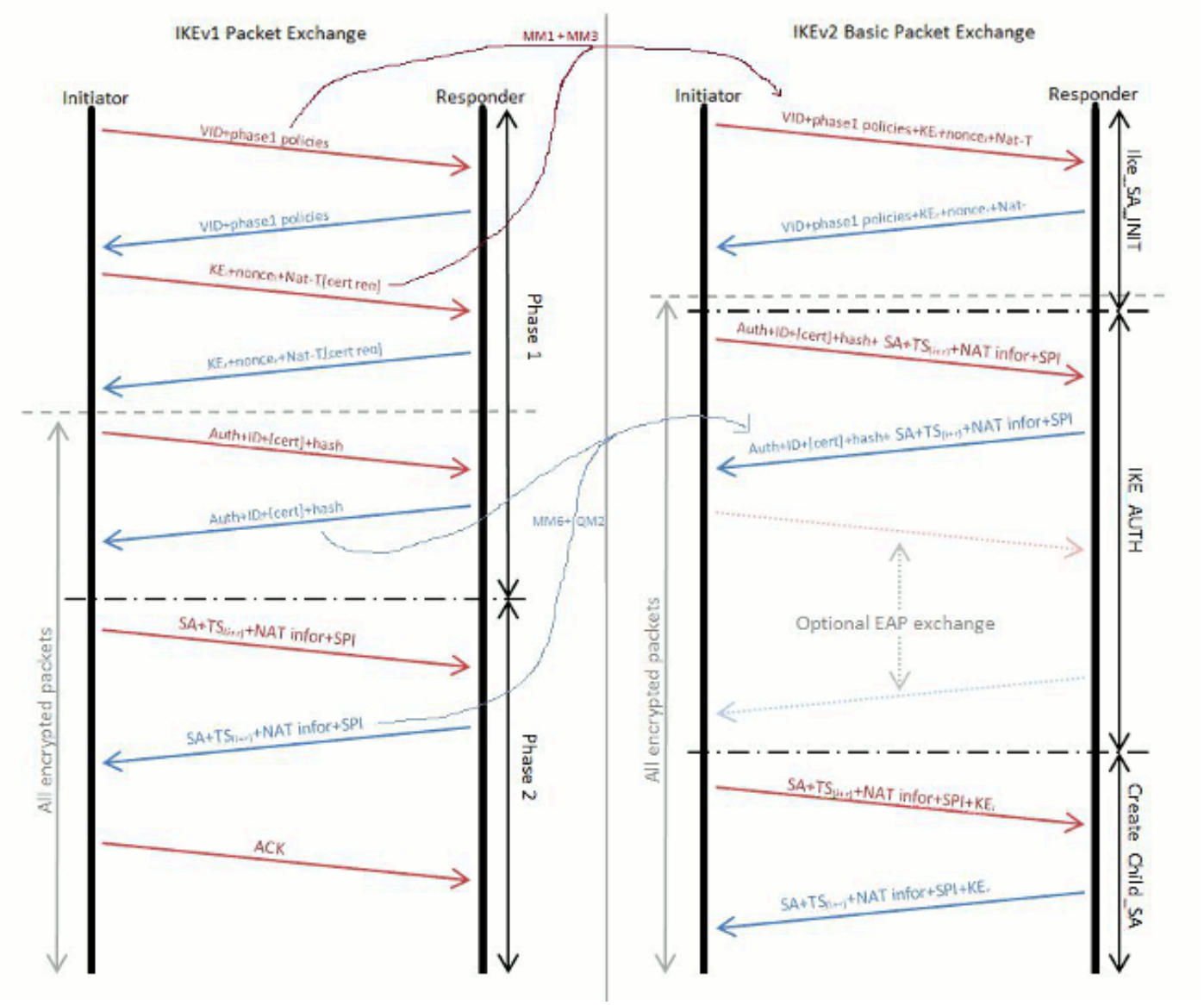
Este documento não se restringe a versões de software e hardware específicas.

Convenções

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

Diferenças entre IKEv1 e IKEv2

Quando o *protocolo do intercâmbio de chave de Internet (IKEv2) no* RFC 4306 descrever em grande detalhe as vantagens de IKEv2 sobre IKEv1, é importante notar que a troca inteira IKE esteve revisada. Este diagrama fornece uma comparação das duas trocas:



Em IKEv1, havia uma troca claramente delimitada da fase 1, que contivesse seis pacotes seguidos por uma troca da fase 2 fosse composta de três pacotes; a troca IKEv2 é variável. O melhor possível, pode trocar somente quatro pacotes. No pior dos casos, isto pode aumentar ao tanto como enquanto 30 pacotes (se não mais), segundo a complexidade da autenticação, o número de atributos do Extensible Authentication Protocol (EAP) usados, assim como o número de SA formaram. IKEv2 combina a informação da fase 2 em IKEv1 na troca IKE_AUTH, e assegura-se de que depois que a troca IKE_AUTH está completa, ambos os pares já tenham um SA construído e apronta-se para cifrar o tráfego. Este SA é construído somente para as identidades de proxy que combinam o pacote do disparador. Todo o tráfego subsequente que combinar outras identidades de proxy então provoca a troca CREATE_CHILD_SA, que é o equivalente da troca da fase 2 em IKEv1. Não há nenhum modo assertivo ou modo principal.

Fases inicial na troca IKEv2

De fato, IKEv2 tem somente duas fases inicial de negociação:

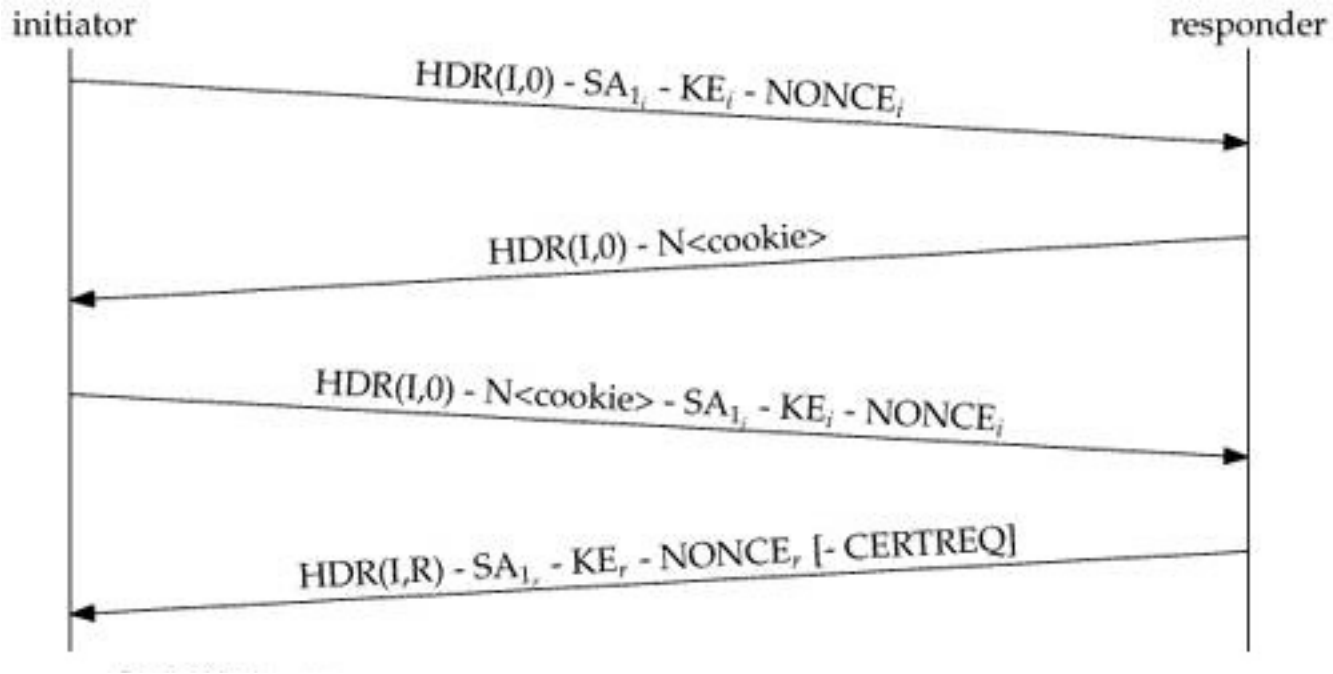
- Troca IKE_SA_INIT
- Troca IKE_AUTH

Troca IKE_SA_INIT

IKE_SA_INIT é a troca inicial em que os pares estabelecem um canal seguro. Depois que termina a troca inicial, tudo troca mais está cifrado. As trocas contêm somente dois pacotes porque combina toda a informação trocada geralmente em MM1-4 em IKEv1. Em consequência, o que responde é computacionalmente caro processar o pacote IKE_SA_INIT e pode sair para processar o primeiro pacote; sae do protocolo aberto a um ataque DOS dos endereços falsificado.

A fim proteger deste tipo do ataque, IKEv2 tem uma troca opcional dentro de IKE_SA_INIT a impedir contra ataques de falsificação. Se um determinado ponto inicial de sessões incompletas é alcançado, o que responde não processa o pacote mais, mas envia pelo contrário uma resposta ao iniciador com um Cookie. Para que a sessão continue, o iniciador deve enviar novamente o pacote IKE_SA_INIT e incluir o Cookie que recebeu.

O iniciador envia novamente o pacote inicial junto com o payload da notificação do que responde que prova que a troca original não era falsificado. Está aqui um diagrama da troca IKE_SA_INIT com desafio do Cookie:



Troca IKE_AUTH

Depois que a troca IKE_SA_INIT está completa, IKEv2 SA está cifrado; contudo, o peer remoto não foi autenticado. A troca IKE_AUTH é usada para autenticar o peer remoto e para criar primeiro IPsec SA.

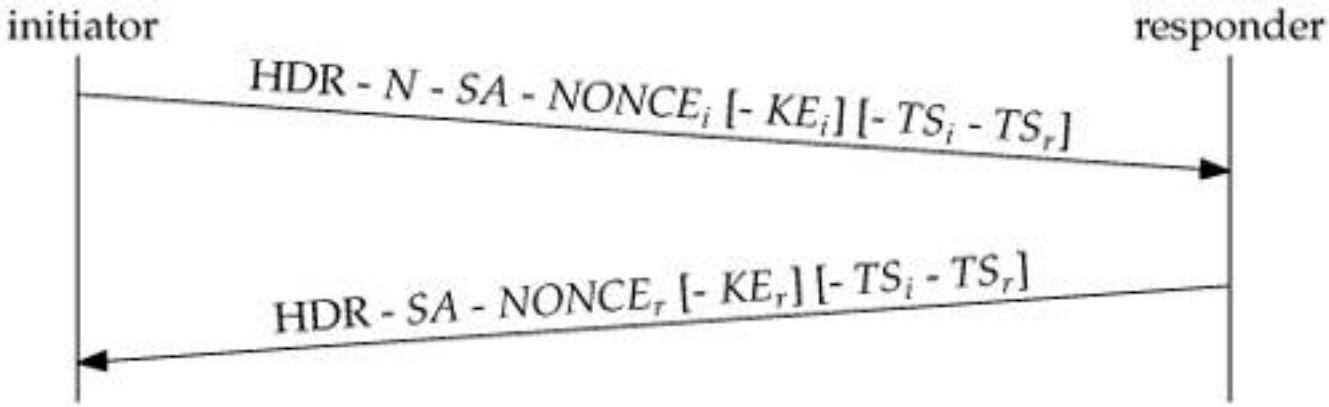
A troca contém o Internet Security Association and Key Management Protocol (ISAKMP) ID junto com um payload da autenticação. Os índices do payload da autenticação são dependentes do método de autenticação, que pode ser a chave pré-compartilhada (PSK), os Certificados RSA (RSA-SIG), os Certificados elípticos do Digital Signature Algorithm da curva (ECDSA-SIG), ou o

EAP. Além do que as cargas úteis da autenticação, a troca inclui as cargas úteis do seletor SA e de tráfego que descrevem IPsec SA a ser criado.

Trocas IKEv2 mais atrasadas

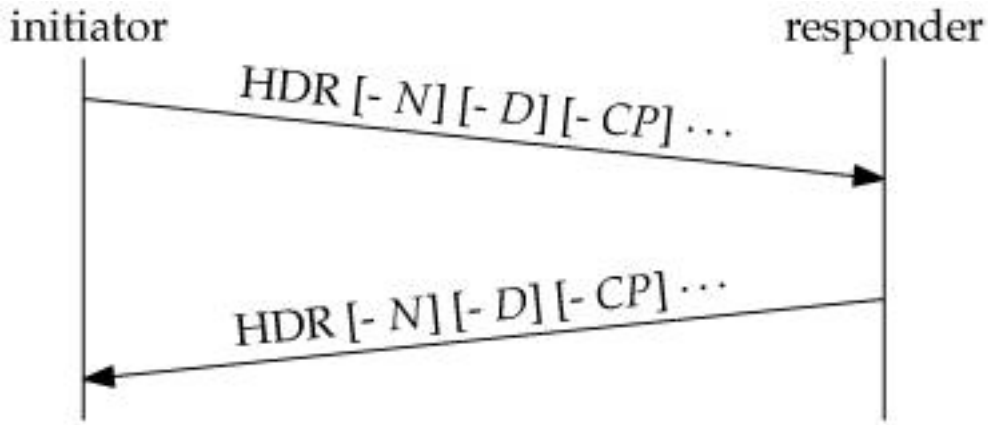
Troca CREATE_CHILD_SA

Se a criança adicional SA está exigida, ou se IKE SA ou um da criança SA precisa re-de ser fechado, serve a mesma função que a troca do Quick Mode faz em IKEv1. Segundo as indicações deste diagrama, há somente dois pacotes nesta troca; contudo, as repetições da troca para o cada rekey ou SA novo:



Troca INFORMATIVA

Enquanto está em todas as trocas IKEv2, cada pedido INFORMATIVO da troca espera uma resposta. Três tipos de cargas úteis podem ser incluídos em uma troca INFORMATIVA. Todo o número de qualquer combinação de cargas úteis pode ser incluído, segundo as indicações deste diagrama:



- O payload da notificação (N) tem sido visto já conjuntamente com Cookie. Há diversos outros tipos também. Levam o erro e a informação de status, como fazem em IKEv1.
- O payload da supressão (d) informa o par que o remetente suprimiu de uns ou vários de seus SA entrantes. O que responde é esperado suprimir daqueles SA e inclui geralmente cargas úteis da supressão para os SA que correspondem no outro sentido em seu mensagem de resposta.
- O payload da configuração (CP) é usado para negociar dados de configuração entre os pares. Um uso importante do CP é pedir (pedido) e atribuir (resposta) um endereço em uma

rede protegida por um gateway de segurança. No caso típico, um host móvel estabelece um Virtual Private Network (VPN) com um gateway de segurança em sua rede home e pede que esteja dado um endereço IP de Um ou Mais Servidores Cisco ICM NT na rede home.**Nota:** Isto elimina um dos problemas que o uso combinado do protocolo Layer 2 Tunneling Protocol (L2TP) e o IPsec é pretendido resolver.

Informações Relacionadas

- O ASA IKEv2 debuga para o VPN de Site-para-Site com PSK TechNote
- O IPsec ASA e o IKE debugam (modo principal IKEv1) pesquisar defeitos TechNote
- O IPsec IO e o IKE debugam - Modo principal IKEv1 que pesquisa defeitos TechNote
- O IPsec ASA e o IKE debugam - IKEv1 modo assertivo TechNote
- Cisco ASA 5500 Series Adaptive Security Appliances
- Downloads do software do Dispositivos de segurança adaptáveis Cisco ASA série 5500
- Negociação IPsec/Protocolos IKE
- Cisco IOS Firewall
- Cisco IOS Software
- Secure Shell (SSH)
- Negociação IPsec/Protocolos IKE
- Suporte Técnico e Documentação - Cisco Systems