Depuración de Nivel de Protocolo y Intercambio de Paquetes IKEv2

Contenido

Introducción

Este documento describe las ventajas de la última versión de Intercambio de claves de Internet (IKE) y las diferencias entre la versión 1 y la versión 2.

IKE es el protocolo utilizado para configurar una asociación de seguridad (SA) en el conjunto de protocolos IPsec. IKEv2 es la segunda y última versión del protocolo IKE. La adopción de este protocolo comenzó ya en 2006. La necesidad y la intención de una revisión del protocolo IKE se describieron en el Apéndice A del *Protocolo de intercambio de claves de Internet (IKEv2)* en RFC 4306.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

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

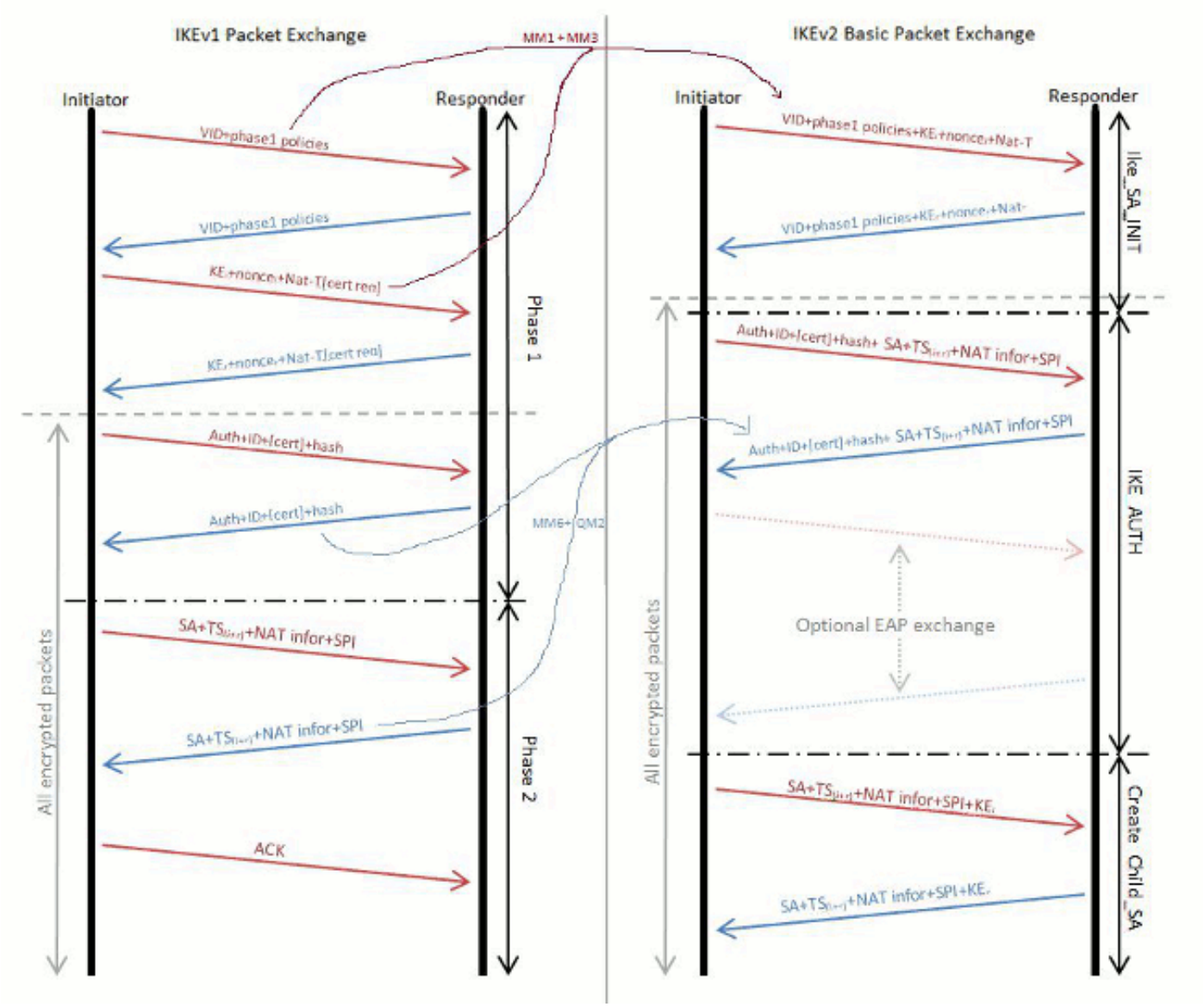
Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las

convenciones del documento.

Diferencias entre IKEv1 e IKEv2

Aunque el *protocolo de intercambio de claves de Internet (IKEv2)* en RFC 4306 describe con gran detalle las ventajas de IKEv2 sobre IKEv1, es importante tener en cuenta que se ha revisado todo el intercambio IKE. Este diagrama proporciona una comparación de los dos intercambios:



En IKEv1, hubo un intercambio de fase 1 claramente demarcado, que contiene seis paquetes seguidos de un intercambio de fase 2 compuesto por tres paquetes; el intercambio IKEv2 es variable. En el mejor de los casos, puede intercambiar hasta cuatro paquetes. En el peor de los casos, esto puede aumentar a hasta 30 paquetes (si no más), dependiendo de la complejidad de la autenticación, el número de atributos de protocolo de autenticación extensible (EAP) utilizados, así como el número de SA formadas. IKEv2 combina la información de Fase 2 en IKEv1 en el intercambio IKE_AUTH y garantiza que después de que el intercambio IKE_AUTH haya finalizado, ambos pares ya tienen una SA construida y lista para cifrar el tráfico. Esta SA sólo está construida para las identidades proxy que coinciden con el paquete de activación. Cualquier tráfico subsiguiente que coincida con otras identidades de proxy activa el intercambio CREATE_CHILD_SA, que es el equivalente del intercambio de Fase 2 en IKEv1. No hay modo agresivo ni modo principal.

Fases iniciales en el intercambio IKEv2

En efecto, IKEv2 solo tiene dos fases iniciales de negociación:

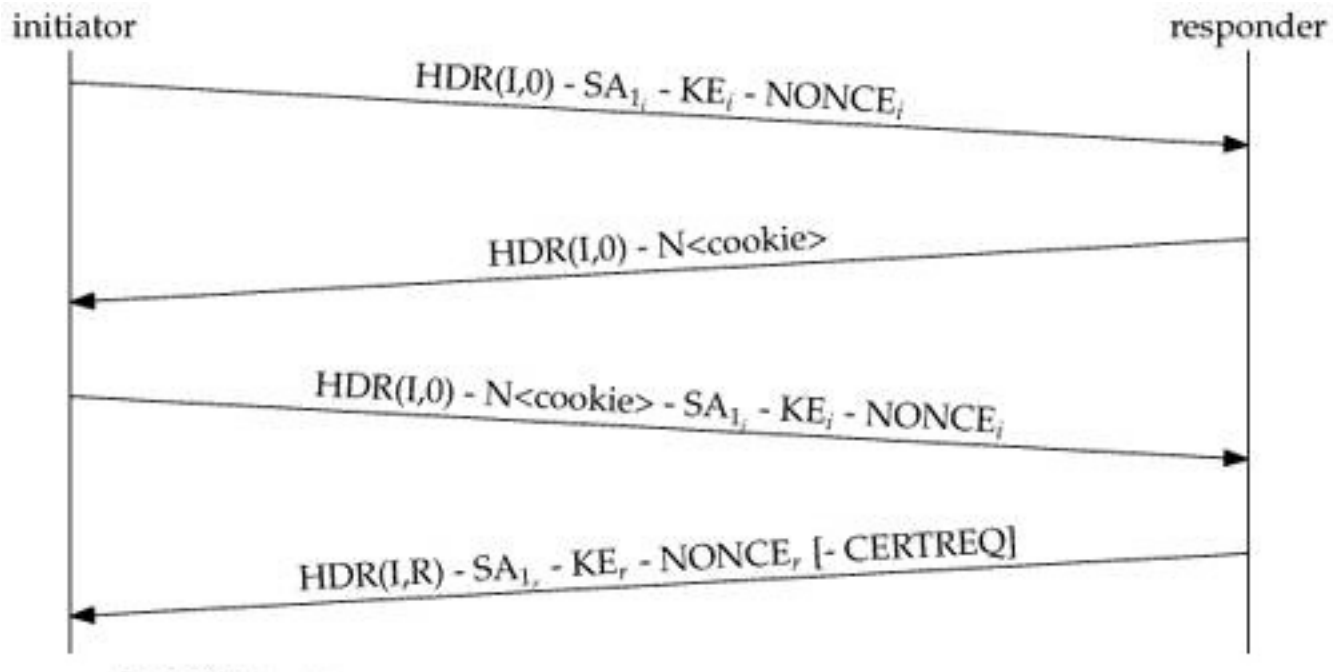
- Intercambio IKE_SA_INIT
- Intercambio IKE_AUTH

Intercambio IKE_SA_INIT

IKE_SA_INIT es el intercambio inicial en el que los pares establecen un canal seguro. Después de completar el intercambio inicial, todos los intercambios adicionales se cifran. Los intercambios contienen sólo dos paquetes porque combina toda la información usualmente intercambiada en MM1-4 en IKEv1. Como resultado, el respondedor tiene un costo computacional para procesar el paquete IKE_SA_INIT y puede salir para procesar el primer paquete; deja el protocolo abierto a un ataque DOS desde direcciones simuladas.

Para protegerse de este tipo de ataque, IKEv2 tiene un intercambio opcional dentro de IKE_SA_INIT para evitar ataques de suplantación. Si se alcanza un cierto umbral de sesiones incompletas, el respondedor no procesa el paquete más adelante, sino que envía una respuesta al Iniciador con una cookie. Para que la sesión continúe, el iniciador debe reenviar el paquete IKE_SA_INIT e incluir la cookie que recibió.

El Iniciador reenvía el paquete inicial junto con la carga útil Notify del respondedor que prueba que el intercambio original no fue suplantado. A continuación se muestra un diagrama del intercambio IKE_SA_INIT con el desafío de cookies:



Intercambio IKE_AUTH

Una vez que el intercambio IKE_SA_INIT ha finalizado, la SA IKEv2 se cifra; sin embargo, el peer remoto no se ha autenticado. El intercambio IKE_AUTH se utiliza para autenticar el par remoto y crear la primera SA IPsec.

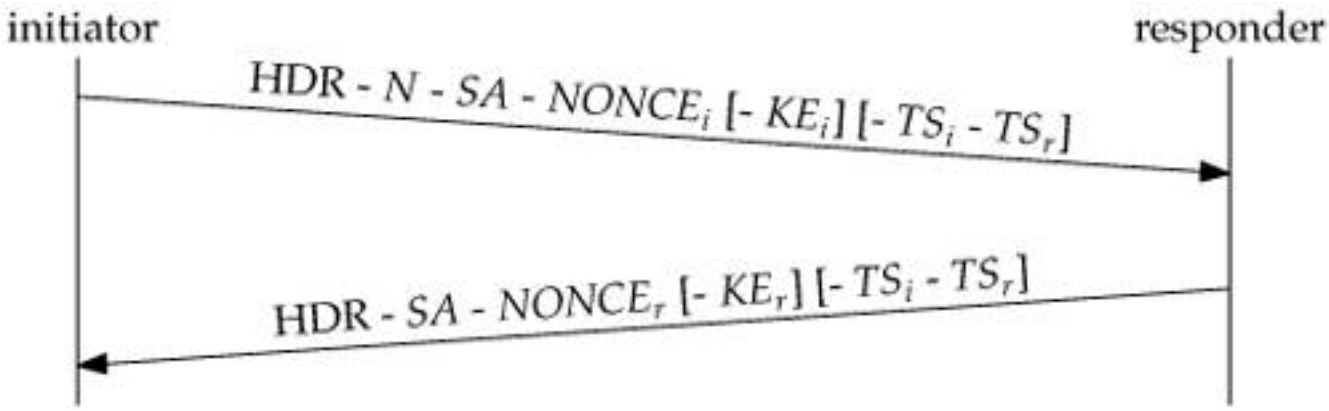
El intercambio contiene la ID de protocolo de administración de claves (ISAKMP) y la Asociación

de seguridad de Internet junto con una carga útil de autenticación. El contenido de la carga útil de autenticación depende del método de autenticación, que puede ser Pre-Shared Key (PSK), RSA certificates (RSA-SIG), Elliptic Curve Digital Signature Algorithm certificates (ECDSA-SIG) o EAP. Además de las cargas útiles de autenticación, el intercambio incluye las cargas útiles de SA y del Selector de tráfico que describen la SA IPSec que se creará.

Intercambios IKEv2 posteriores

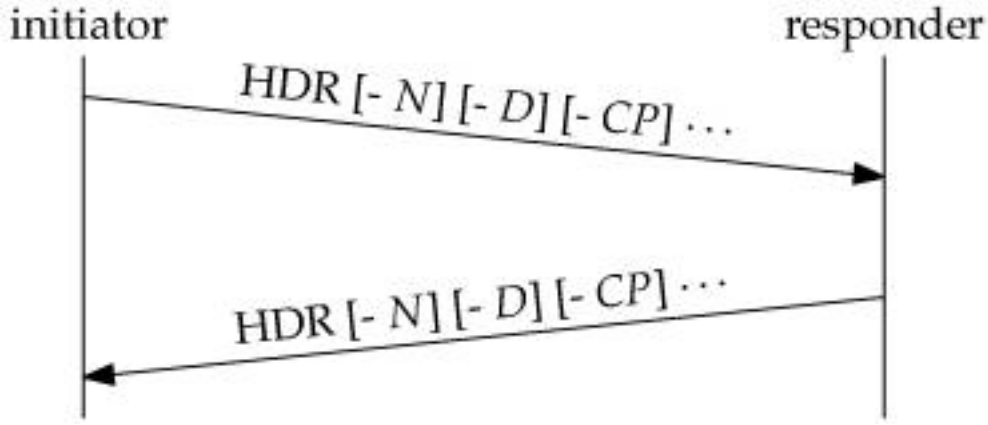
CREATE_CHILD_SA Exchange

Si se requieren SA secundarias adicionales, o si se debe volver a introducir la SA IKE o una de las SA secundarias, se utiliza la misma función que el intercambio de modo rápido en IKEv1. Como se muestra en este diagrama, sólo hay dos paquetes en este intercambio; sin embargo, el intercambio se repite para cada nueva clave o nueva SA:



Intercambio de información

Como ocurre en todos los intercambios de IKEv2, cada solicitud de intercambio de información espera una respuesta. Se pueden incluir tres tipos de cargas útiles en un intercambio INFORMATIONAL. Se puede incluir cualquier número de combinaciones de cargas útiles, como se muestra en este diagrama:



- La carga útil Notify (N) ya se ha visto junto con las cookies. También hay otros tipos. Llevan información de error y estado, como lo hacen en IKEv1.
- La carga útil Eliminar (D) informa al par de que el remitente ha eliminado una o más de sus SA entrantes. Se espera que el respondedor elimine esas SA y generalmente incluye Eliminar cargas útiles para las SA que corresponden en la otra dirección en su mensaje de respuesta.

- La carga útil de configuración (CP) se utiliza para negociar los datos de configuración entre los pares. Un uso importante del CP es solicitar (solicitar) y asignar (responder) una dirección en una red protegida por un gateway de seguridad. En el caso habitual, un host móvil establece una red privada virtual (VPN) con un gateway de seguridad en su red doméstica y solicita que se le asigne una dirección IP en la red doméstica.**Nota:** Esto elimina uno de los problemas que el uso combinado del protocolo de túnel de capa 2 (L2TP) e IPsec está destinado a resolver.

Información Relacionada

- Depuraciones ASA IKEv2 para VPN de sitio a sitio con PSK TechNote
- Diagnóstico de problemas de depuración de IPsec e IKE (modo principal IKEv1) de ASA
- Depuraciones de IOS IPSec e IKE - Nota técnica de resolución de problemas del modo principal IKEv1
- Depuraciones de ASA IPSec e IKE - IKEv1 Modo agresivo TechNote
- Cisco ASA 5500 Series Adaptive Security Appliances
- Descargas de software de dispositivos de seguridad adaptable Cisco ASA serie 5500
- Negociación IPSec/Protocolos IKE
- Cisco IOS Firewall
- Cisco IOS Software
- Secure Shell (SSH)
- Negociación IPSec/Protocolos IKE
- Soporte Técnico y Documentación - Cisco Systems