Intercambio de paquetes IKEv2 y debugging del nivel del protocolo

Contenido

Introducción

Este documento describe las ventajas de la última versión del Internet Key Exchange (IKE) y las diferencias entre la versión 1 y la versión 2.

El IKE es el protocolo usado para configurar una asociación de seguridad (SA) en la habitación de Protocolo IPSec. IKEv2 es la segunda y última versión del IKE Protocol. Adopción para este protocolo comenzado ya desde 2006. La necesidad y el intento de una revisión del IKE Protocol fueron descritos en el Apéndice A del *protocolo del intercambio de claves de Internet (IKEv2)* en el RFC 4306.

prerrequisitos

Requisitos

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

Mientras que el *protocolo del intercambio de claves de Internet (IKEv2)* en el RFC 4306 describe con gran detalle las ventajas de IKEv2 sobre IKEv1, es importante observar que el intercambio entero IKE fue revisado. Este diagrama proporciona una comparación de los dos intercambios:

En IKEv1, había un intercambio claramente demarcado de la fase 1, que contiene seis paquetes seguidos por un intercambio de la fase 2 se compone de tres paquetes; el intercambio IKEv2 es variable. En el mejor de los casos, puede intercambiar únicamente cuatro paquetes. En peor de los casos, esto puede aumentar a tanto mientras que 30 paquetes (si no más), dependiendo de la complejidad de la autenticación, el número de atributos del Protocolo de Autenticación Extensible (EAP) usados, así como el número de SA formaron. IKEv2 combina la información de la fase 2 en IKEv1 en el intercambio IKE_AUTH, y se asegura de que después de que el intercambio IKE_AUTH sea completo, ambos pares hagan ya un SA construir y lo alista para cifrar el tráfico. Este SA se construye solamente para las identidades de representación que hacen juego el paquete del activador. Cualquier tráfico subsiguiente que haga juego otras identidades de representación entonces acciona el intercambio CREATE_CHILD_SA, que es el equivalente del intercambio de la fase 2 en IKEv1. No hay modo agresivo o modo principal.

Fases iniciales en el intercambio IKEv2

En efecto, IKEv2 tiene solamente 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 cual los pares establecen un canal seguro. Después de que complete el intercambio inicial, se cifra todo intercambia más lejos. Los intercambios contienen solamente dos paquetes porque combina toda la información intercambiada generalmente en MM1-4 en IKEv1. Como consecuencia, el respondedor es de cómputo costoso procesar el paquete IKE_SA_INIT y puede irse para procesar el primer paquete; sale del protocolo abierto a un ataque DOS de los direccionamientos del spoofed.

Para proteger contra esta clase de ataque, IKEv2 tiene un intercambio opcional dentro de IKE_SA_INIT a prevenir contra los ataques de simulación. Si cierto umbral de las sesiones incompletas se alcanza, el respondedor no procesa el paquete más lejos, sino que por el contrario envía una respuesta al iniciador con un Cookie. Para que la sesión continúe, el iniciador debe volver a enviar el paquete IKE_SA_INIT e incluir el Cookie que recibió.

El iniciador vuelve a enviar el paquete inicial junto con el payload de la notificación del respondedor que prueba que el intercambio original no era spoofed. Aquí está un diagrama del intercambio IKE_SA_INIT con el desafío del Cookie:

Intercambio IKE_AUTH

Después de que el intercambio IKE_SA_INIT sea completo, se cifra IKEv2 SA; sin embargo, no

han autenticado al peer remoto. El intercambio IKE_AUTH se utiliza para autenticar al peer remoto y para crear primer IPSec SA.

El intercambio contiene el Internet Security Association and Key Management Protocol (ISAKMP) ID junto con un payload de la autenticación. El contenido del payload de la autenticación es dependiente en el método de autenticación, que puede ser clave previamente compartida (PSK), los Certificados RSA (RSA-SIG), los Certificados elípticos del Digital Signature Algorithm de la curva (ECDSA-SIG), o EAP. Además de las cargas útiles de la autenticación, el intercambio incluye las cargas útiles del selector SA y del tráfico que describen IPSec SA que se creará.

Intercambios posteriores IKEv2

Intercambio CREATE_CHILD_SA

Si requieren al niño adicional SA, o si IKE SA o uno del niño SA necesita ser reintroducido, sirve la misma función que el intercambio del Quick Mode hace en IKEv1. Tal y como se muestra en del este diagrama, hay solamente dos paquetes en este intercambio; sin embargo, las repeticiones del intercambio para cada reintroducen o nuevo SA:

Intercambio INFORMATIVO

Mientras que está en todos los intercambios IKEv2, cada petición INFORMATIVA del intercambio cuenta con una respuesta. Tres tipos de cargas útiles pueden ser incluidos en un intercambio INFORMATIVO. Cualquier número de cualquier combinación de cargas útiles puede ser incluido, tal y como se muestra en del este diagrama:

- El payload de la notificación (n) se ha visto ya conjuntamente con los Cookie. Hay varios otros tipos también. Llevan el error y la información de estatus, como hacen en IKEv1.
- El payload de la cancelación (d) informa al par que el remitente ha borrado uno o más de sus SA entrantes. Se espera que borre esos SA e incluye generalmente al respondedor las cargas útiles de la cancelación para los SA que corresponden en la otra dirección en su mensaje de respuesta.
- El payload de la configuración (CP) se utiliza para negociar los datos de configuración entre los pares. Un uso importante del CP es pedir (petición) y asignar (respuesta) un direccionamiento en una red protegida por un gateway de seguridad. En el caso típico, un host móvil establece un Red privada virtual (VPN) con un gateway de seguridad en su red doméstica y pide que esté dado una dirección IP en la red doméstica.**Nota:** Esto elimina uno de los problemas que el uso combinado del protocolo Layer 2 Tunneling Protocol (L2TP) y el IPSec se piensa para solucionar.

Información Relacionada

- Debugs ASA IKEv2 para el VPN de sitio a sitio con la Nota Técnica de PSKs
- IPSec ASA y debugs IKE (modo principal IKEv1) que resuelven problemas la Nota Técnica
- IPSec IOS y debugs IKE - Modo principal IKEv1 que resuelve problemas la Nota Técnica
- IPSec ASA y debugs IKE - Nota Técnica del modo agresivo IKEv1
- Cisco ASA 5500 Series Adaptive Security Appliances
- Descargas del software del Dispositivos de seguridad adaptable Cisco ASA de la serie 5500

- IPSec Negotiation/IKE Protocols
- Cisco IOS Firewall
- Cisco IOS Software
- Secure Shell (SSH)
- IPSec Negotiation/IKE Protocols
- Soporte Técnico y Documentación - Cisco Systems