Contenido

Introducción

El Internet Key Exchange (IKE) es un método estándar usado para arreglar las comunicaciones seguras, autenticadas. El concentrador del Cisco VPN 5000 utiliza el IKE para configurar los túneles IPsec. Estos túneles IPsec son la estructura básica de este producto.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- VPN de la serie 5000 concentrador

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Para obtener más información sobre las convenciones del documento, consulte Convenciones de Consejos Técnicos de Cisco.

Tareas IKE

El IKE maneja estas tareas:

- Autenticación
- Negociación de la sesión
- 'Intercambio de claves'
- Configuración y negociación del túnel IPSec

Autenticación

La autenticación es la tarea más importante que el IKE logra, y es el más complicado. Siempre que usted negocie algo, es importante saber con quién usted negocia. El IKE puede utilizar uno de varios métodos para autenticar los partidos de negociación el uno al otro.

- **Clave compartida** - El IKE utiliza una técnica del picado para asegurarse de que solamente alguien que posee la misma clave puede enviar los paquetes IKE.
- **Digital Signature Standard (DSS) o Rivest, Shamir, firmas digitales del Adelman (RSA)** - el IKE utiliza la criptografía de la firma digital de la clave pública para verificar que cada partido es quién demandan ser.
- **Encripción RSA** - El IKE utiliza uno de dos métodos para cifrar bastante de la negociación para asegurarse de que solamente un partido con la clave privada correcta puede continuar la negociación.

Negociación de la sesión

Durante la negociación de la sesión, el IKE permite que los partidos negocien cómo conducirán la autenticación y cómo protegerán cualquier negociación futura (es decir, Negociación de túnel IPSec). Se negocian estos elementos:

- **Método de autentificación** - Éste es uno de los métodos enumerados en la sección de la autenticación de este documento.
- **Key Exchange Algorithm** - Esto es una técnica matemática para con seguridad intercambiar las claves cifradas sobre un medio público (Diffie Hellman). Las claves se utilizan en el cifrado y los algoritmos de firma del paquete.
- **Algoritmo de encripción** - Data Encryption Standard (DES) o Estándar de triple cifrado de datos (3DES).
- **Algoritmo de firma del paquete** - Publicación de mensaje 5 (MD5) y algoritmo de troceo seguro 1 (SHA-1).

'Intercambio de claves'

El IKE utiliza el método negociado del intercambio de claves (véase la sección de la negociación de la sesión de este documento) para crear bastantes bits del material de clave criptográfica para asegurar las transacciones futuras. Este método se asegura de que protejan a cada sesión IKE con un nuevo, seguro conjunto de las claves.

La autenticación, la negociación de la sesión, y el intercambio de claves constituyen el fase uno

de una negociación IKE. Para un VPN 5000 concentrator, estas propiedades se configuran en la sección de la **política IKE** con la contraseña de protección. Esta palabra clave es una escritura de la etiqueta que tiene tres pedazos: algoritmo de autenticación, algoritmo de encripción, y Key Exchange Algorithm. Los pedazos son separados por un caracter de subrayado. La escritura de la etiqueta MD5_DES_G1 significa el uso MD5 para la autenticación del Paquete IKE, el uso DES para el cifrado del Paquete IKE, y el grupo Diffie-Hellman 1 del uso para el intercambio de claves. Para más información, refiera a configurar la política IKE para la Seguridad del túnel IPsec.

Configuración y negociación del túnel IPSec

Después de que el IKE haya acabado de negociar un método de intercambio de información seguro (fase uno), el IKE se utiliza para negociar un túnel IPsec. Esto es realizado usando la fase dos IKE. En este intercambio, el IKE crea el material de codificación reciente para que el túnel IPsec utilice (con las claves del fase uno IKE como base o realizando un nuevo intercambio de claves). El cifrado y los algoritmos de autenticación para este túnel también se negocian.

Los túneles IPsec se configuran usando la sección del grupo VPN (antes el cliente del protocolo secure tunnel establishment (PASO)) para los túneles del cliente VPN y la sección del partner de túnel para los túneles de LAN a LAN. La sección de los **usuarios de VPN** es donde el método de autentificación para cada usuario se salva. Estas secciones se documentan en configurar la política IKE para la Seguridad del túnel IPsec.

Extensiones IKE del VPN 5000 concentrator

- **RADIUS** - El IKE no tiene ningún soporte para la autenticación de RADIUS. La autenticación de RADIUS se realiza en un intercambio de la información especial que ocurra después del primer paquete IKE del cliente VPN. Si se requiere el protocolo password authentication (PAP), se requiere un secreto especial de la autenticación de RADIUS. Para más información, refiera a la documentación de NoCHAP y de PAPAuthSecret en configurar la política IKE para la Seguridad del túnel IPsec. Se autentica y se cifra la autenticación de RADIUS. El intercambio PAP es protegido por el PAPAuthSecret. Sin embargo, hay solamente un tal secreto para el Intraport entero, así que la protección es tan débil como cualquier contraseña compartida.
- **SecurID** - El IKE no tiene actualmente ningún soporte para la autenticación de SecurID. La autenticación de SecurID se realiza en un fase uno y una fase medios dos del intercambio informativo especial. Este intercambio es protegido completamente por la asociación de seguridad IKE (SA) negociada en el fase uno.
- **Protocolo secure tunnel access management (SELLO)** - Información del intercambio de las conexiones de cliente VPN con el Intraport durante el proceso IKE. La información por ejemplo si todo correcto salvar los secretos, que las redes del IP a hacer un túnel, o si hacer un túnel el tráfico del Intercambio de paquetes entre redes (IPX), se envía en privado las cargas útiles durante los dos paquetes IKE más recientes. Estas cargas útiles se envían solamente a los clientes VPN compatibles.

ISAKMP y Oakley

El Internet Security Association and Key Management Protocol (ISAKMP) es un lenguaje usado para conducir las negociaciones a través de Internet (por ejemplo, usando protocolo IP). El

Oakley es un método para conducir un intercambio autenticado del material de clave cifrada. El IKE pone los dos juntos en un paquete, que permite que las conexiones seguras sean configuradas a través del Internet no segura.

STEP y STAMP

El protocolo secure tunnel establishment (PASO) es el nombre anterior del sistema VPN. En los días PRE-IKE, el SELLO fue utilizado para negociar las conexiones del IPSec. Las versiones del cliente VPN anterior que el SELLO del uso del 3.0 para establecer una conexión con un Intraport.

Información Relacionada

- Anuncio de fin de venta de los concentradores Serie VPN 5000 de Cisco
- Configuración del túnel LAN a LAN del router al concentrador VPN de la serie 5000
- Página de soporte del producto concentrador del Cisco VPN 5000
- Página de soprte del producto del Cliente Cisco VPN 5000
- Soporte de tecnología de la Negociación IPSec/Protocolos IKE
- Soporte Técnico y Documentación - Cisco Systems