Redes privadas virtuales e Intercambio de claves de Internet para concentrador serie Cisco VPN 5000

Contenido

Introducción

Internet Key Exchange (IKE) es un método estándar utilizado para organizar comunicaciones seguras y autenticadas. El concentrador VPN 5000 de Cisco utiliza IKE para configurar túneles IPSec. Estos túneles IPSec son la columna vertebral de este producto.

Prerequisites

Requirements

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.

- Concentrador de la serie VPN 5000

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Convenciones

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

Tareas IKE

IKE se encarga de 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 realiza IKE, y es la más complicada. Siempre que negocia algo, es importante saber con quién negocia. La IKE puede utilizar uno de varios métodos para autenticar a las partes negociadoras entre sí.

- **Clave compartida**: IKE utiliza una técnica de hashing para garantizar que sólo alguien que posee la misma clave pueda enviar los paquetes IKE.
- **Firmas digitales estándar (DSS) o Rivest, Shamir, Adelman (RSA)** - IKE utiliza criptografía de firma digital de clave pública para verificar que cada persona es quien afirma ser.
- **Cifrado RSA**: IKE utiliza uno de dos métodos para cifrar suficiente negociación para asegurarse de que sólo una parte con la clave privada correcta pueda continuar la negociación.

Negociación de la sesión
Durante la negociación de sesión, IKE permite a las partes negociar cómo llevarán a cabo la autenticación y cómo protegerán cualquier negociación futura (es decir, la negociación de túnel IPSec). Estos elementos se negocian:

- **Método de autenticación**: este es uno de los métodos enumerados en la sección Autenticación de este documento.
- **Algoritmo de intercambio de claves** - Se trata de una técnica matemática para el intercambio seguro de claves criptográficas en un medio público (Diffie-Hellman). Las claves se utilizan en los algoritmos de cifrado y firma de paquetes.
- **Algoritmo de cifrado**: estándar de cifrado de datos (DES) o triple estándar de cifrado de datos (3DES).
- **Algoritmo de firma de paquetes**: Message Digest 5 (MD5) y Secure Hash Algorithm 1 (SHA-1).

'Intercambio de claves'

IKE utiliza el método de intercambio de claves negociado (consulte la sección Negociación de Sesión de este documento) para crear suficientes bits de material de claves criptográficas para proteger las transacciones futuras. Este método asegura que cada sesión IKE esté protegida con

un nuevo conjunto seguro de claves.

La autenticación, la negociación de sesión y el intercambio de claves constituyen la primera fase de una negociación IKE. Para un concentrador VPN 5000, estas propiedades se configuran en la sección **Política IKE** a través de la palabra clave Protection. Esta palabra clave es una etiqueta que tiene tres partes: algoritmo de autenticación, algoritmo de cifrado y algoritmo de intercambio de claves. Las piezas están separadas por un guión bajo. La etiqueta MD5_DES_G1 significa utilizar MD5 para la autenticación de paquetes IKE, utilizar DES para el cifrado de paquetes IKE y utilizar Diffie-Hellman group 1 para el intercambio de claves. Para obtener más información, consulte Configuración de la Política IKE para la Seguridad del Túnel IPSec.

Configuración y negociación del túnel IPSec

Después de que IKE haya terminado de negociar un método seguro para intercambiar información (fase uno), IKE se utiliza para negociar un túnel IPSec. Esto se logra utilizando la fase dos de IKE. En este intercambio, IKE crea nuevo material de codificación para el túnel IPSec que se va a utilizar (ya sea utilizando las claves de la fase uno IKE como base o realizando un nuevo intercambio de claves). También se negocian los algoritmos de cifrado y autenticación para este túnel.

Los túneles IPSec se configuran mediante la sección VPN Group (antes Secure Tunnel Establishment Protocol (STEP) Client) para los túneles de VPN Client y la sección Tunnel Partner para los túneles de LAN a LAN. La sección **Usuarios de VPN** es donde se almacena el método de autenticación para cada usuario. Estas secciones se documentan en Configuración de la Política IKE para la Seguridad del Túnel IPSec.

Extensiones IKE del concentrador VPN 5000

- **RADIUS**: IKE no admite la autenticación RADIUS. La autenticación RADIUS se realiza en un intercambio de información especial que se realiza después del primer paquete IKE del VPN Client. Si se requiere el protocolo de autenticación de contraseña (PAP), se requiere un secreto de autenticación RADIUS especial. Para obtener más información, consulte la documentación de NoCHAP y PAPAuthSecret en Configuración de la Política IKE para la Seguridad del Túnel IPSec. La autenticación RADIUS se autentica y se cifra. El intercambio PAP está protegido por PAPAuthSecret. Sin embargo, sólo hay uno de esos secretos para todo IntraPort, por lo que la protección es tan débil como cualquier contraseña compartida.
- **SecurID**: IKE no admite actualmente la autenticación de SecurID. La autenticación SecurID se realiza en un intercambio de información especial entre la fase uno y la fase dos. Este intercambio está totalmente protegido por la Asociación de Seguridad IKE (SA) negociada en la primera fase.
- **Protocolo de administración de acceso de túnel seguro (STAMP)**: las conexiones de VPN Client intercambian información con IntraPort durante el proceso IKE. La información, como si estuviera bien guardar secretos, qué redes IP se van a tunelizar o si se va a tunelizar el tráfico de Intercambio de paquetes entre redes (IPX), se envía en cargas privadas durante los dos últimos paquetes IKE. Estas cargas solo se envían a clientes VPN compatibles.

ISAKMP y Oakley

La Asociación de seguridad de Internet y el protocolo de gestión de claves (ISAKMP) es un

lenguaje utilizado para llevar a cabo negociaciones a través de Internet (por ejemplo, utilizando el protocolo IP). Oakley es un método para realizar un intercambio autenticado de material de clave criptográfica. IKE une ambos en un paquete, lo que permite configurar conexiones seguras a través de Internet inseguro.

STEP y STAMP

El protocolo de establecimiento de túnel seguro (STEP) es el nombre anterior del sistema VPN. En los días anteriores a IKE, se utilizó STAMP para negociar conexiones IPSec. Las versiones de VPN Client anteriores a 3.0 utilizan STAMP para establecer una conexión con 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 Cisco VPN 5000 Concentrator
- Página de soporte del producto Cisco VPN 5000 Client
- Soporte de la Tecnología IPSec Negotiation/IKE Protocols
- Soporte Técnico y Documentación - Cisco Systems