ISAKMP ROJO y Información de Oakley

Contenido

Introducción

Este documento proporciona la información sobre el Internet Security Association and Key Management Protocol (ISAKMP) y el protocolo de la determinación de clave Oakley. Estos protocolos son competidores principales para la administración de claves de Internet que es considerada por el Grupo de trabajo del IPSec de la Fuerza de tareas de ingeniería en Internet (IETF) (IETF).

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

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

Información técnica

Sobre el ISAKMP

El ISAKMP proporciona un marco para la administración de claves de Internet y proporciona el soporte a protocolo específico para la negociación de los atributos de seguridad. Solamente, no establece las claves de la sesión. No obstante puede ser utilizado con los diversos protocolos de establecimiento de la clave de la sesión, tales como Oakley, para proporcionar una solución completa a la administración de claves de Internet. La especificación ISAKMP también está disponible en la posdata.

Sobre el Oakley

El protocolo Oakley utiliza una técnica híbrida de Diffie Hellman para establecer las claves de la sesión en los host de Internet y el Routers. El Oakley proporciona la propiedad de seguridad importante del Confidencialidad directa perfecta (PFS) y se basa en las técnicas de cifrado que han sobrevivido el escrutinio público sustancial. El Oakley se puede utilizar en sí mismo, si no hay negociación del atributo necesaria, o el Oakley se puede utilizar conjuntamente con el ISAKMP. Cuando el ISAKMP se utiliza con el Oakley, la custodia clave no es posible.

El ISAKMP y los protocolos Oakley se han combinado en un protocolo híbrido. La resolución del ISAKMP con el Oakley utiliza el marco del ISAKMP para soportar un subconjunto de modos del intercambio de claves del Oakley. Este nuevo Key Exchange Protocol proporciona los PF opcionales, negociación del atributo de asociación de seguridad total, y los métodos de autentificación que proporcionan la renegación y la no renegación. Las aplicaciones de este protocolo se pueden utilizar para establecer los VPN y también para tener en cuenta los usuarios del acceso de los sitios remotos (quién pueden tener una dirección IP dinámicamente afectada un aparato) a una red segura.

Sobre el IPSec

El Grupo de trabajo del IPSec IETF desarrolla los estándares para los mecanismos de seguridad de la capa IP para el IPv4 y el IPv6. El grupo también está desarrollando los protocolos de la Administración de clave genérica para el uso en el Internet. Para más información, refiera a la seguridad IP y a la descripción general de encripción.

Software ISAKMP

Implementación de Cisco Systems

Cisco Systems software daemon ISAKMP está disponible gratuitamente para que cualquier uso comercial o no comercial ayude al ISAKMP anticipado como solución estándar a la administración de claves de Internet.

El software ISAKMP de Cisco está disponible dentro de los Estados Unidos y del Canadá a través de una forma de la descarga de la red de Massachusetts Institute of Technology (MIT). Debido a las leyes de control de la exportación de Estados Unidos, Cisco no puede distribuir este software fuera de los Estados Unidos y del Canadá.

El ISAKMP daemon de Cisco utiliza PF_KEY el Application Program Interface de la administración de claves (API) para registrarse con un corazón del sistema operativo (que ha implementado este API) y la infraestructura de administración de claves circundante. Insertan a las asociaciones de seguridad que han sido negociadas por el ISAKMP daemon en el motor dominante del corazón. Están entonces disponible para uso de los mecanismos de seguridad del IPSec estándar del sistema (encabezado de autenticación [AH] y Encapsulating Security Payload [ESP]).

La distribución de software libre-distribuible E.E.U.U. Naval Research Laboratory (NRL) IPv6+IPSec para los sistemas derivados 4.4-BSD ([BSDI] incluyendo y NetBSD de Berkeley Software Design, Inc.) incluye la implementación del IPv6, el IPSec para el IPv6, el IPSec para el IPv4, y PF_KEY la interfaz. El software NRL está disponible dentro de los Estados Unidos y del Canadá a través de una forma de la descarga de la red del MIT. Fuera de los Estados Unidos y del Canadá, el software NRL está disponible con el FTP de ftp://ftp.ripe.net/ipv6/nrl .

La daemon de Cisco se basa en el ISAKMP versión 5 y utiliza las características de la Versión del protocolo 1. de la determinación de clave Oakley.

Una lista de correo para los problemas, los arreglos del bug, los cambios que viraban hacia el lado de babor, y la discusión general del ISAKMP y del Oakley se ha establecido en isakmp-oakley@cisco.com. Para unirse a esta lista, envíe un pedido por correo electrónico con un cuerpo del mensaje de **inscriben ISAKMP-Oakley** a: majordomo@cisco.com.

Implementación del Departamento de defensa de Estados Unidos (DoD)

La oficina DoD E.E.U.U. de investigación de seguridad de información ha hecho su implementación del prototipo ISAKMP libremente disponible para la distribución dentro de los Estados Unidos. Un interfaz basada en la Web está disponible para descargar el software. Esta implementación no incluye ninguna capacidades de intercambio de la clave de la sesión, sino incluye las características completas ISAKMP.

Información Relacionada

- Página de soporte de IPSec
- Soporte Técnico - Cisco Systems