Información de RED ISAKMP y Oakley

Contenido

Introducción

Este documento proporciona información sobre la Asociación de Seguridad de Internet y el Protocolo de administración de claves (ISAKMP) y el Protocolo de determinación de claves Oakley. Estos protocolos son los principales contendientes para la gestión de claves de Internet que está examinando el Grupo de Trabajo IPSec del Grupo de Trabajo de Ingeniería de Internet (IETF).

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

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Información técnica

Acerca de ISAKMP

El ISAKMP proporciona un marco para la administración de claves de Internet y proporciona el soporte de protocolo específico para la negociación de atributos de seguridad. Solo, no establece claves de sesión. Sin embargo, se puede utilizar con varios protocolos de establecimiento de claves de sesión, como Oakley, para proporcionar una solución completa a la administración de claves de Internet. La especificación ISAKMP también está disponible en postscript.

Acerca de Oakley

El protocolo Oakley utiliza una técnica Diffie-Hellman híbrida para establecer las claves de sesión en los hosts y routers de Internet. Oakley proporciona la importante propiedad de seguridad de Perfect Forward Secrecy (PFS) y se basa en técnicas criptográficas que han sobrevivido a un escrutinio público sustancial. Oakley se puede utilizar por sí solo, si no se necesita ninguna negociación de atributos, o Oakley se puede utilizar junto con ISAKMP. Cuando ISAKMP se utiliza con Oakley, la garantía bloqueada de claves no es factible.

Los protocolos ISAKMP y Oakley se han combinado en un protocolo híbrido. La resolución de ISAKMP con Oakley utiliza el marco de ISAKMP para soportar un subconjunto de modos de intercambio de claves Oakley. Este nuevo protocolo de intercambio de claves proporciona PFS opcional, negociación de atributos de asociación de seguridad completa y métodos de autenticación que proporcionan tanto rechazo como no rechazo. Las implementaciones de este protocolo se pueden utilizar para establecer VPN y también para permitir el acceso de usuarios de sitios remotos (que pueden tener una dirección IP asignada dinámicamente) a una red segura.

Acerca de IPSec

El Grupo de Trabajo IPSec de IETF desarrolla estándares para mecanismos de seguridad de capa IP tanto para IPv4 como para IPv6. El grupo también está desarrollando protocolos genéricos de gestión de claves para su uso en Internet. Para obtener más información, refiérase a Descripción General de Seguridad IP y Cifrado.

Software ISAKMP

Implementación de Cisco Systems

El software daemon ISAKMP de Cisco Systems está disponible gratuitamente para cualquier uso comercial o no comercial para ayudar a avanzar ISAKMP como solución estándar para la administración de claves de Internet.

El software ISAKMP de Cisco está disponible en los Estados Unidos y Canadá a través de un formulario de descarga web del Massachusetts Institute of Technology (MIT). Debido a las leyes de control de exportaciones de Estados Unidos, Cisco no puede distribuir este software fuera de Estados Unidos y Canadá.

El daemon de Cisco ISAKMP utiliza la Interfaz de programa de gestión de claves (API) PF_KEY para registrarse en un kernel del sistema operativo (que ha implementado esta API) y la infraestructura de gestión de claves que lo rodea. Las asociaciones de seguridad que han sido negociadas por el daemon ISAKMP se insertan en el motor clave del núcleo. A continuación, están disponibles para su uso por los mecanismos de seguridad IPSec estándar del sistema

(encabezado de autenticación [AH] y carga útil de seguridad de encapsulación [ESP]).

La distribución de software IPv6+IPSec para sistemas derivados de 4,4 BSD (incluidos Berkeley Software Design, Inc. [BSDI] y NetBSD), de libre distribución, incluye la implementación de IPv6, IPSec para IPv6, IPSec para IPv4 y la interfaz PF_KEY. El software NRL está disponible en los Estados Unidos y Canadá a través de un formulario de descarga del MIT. Fuera de los Estados Unidos y Canadá, el software NRL está disponible a través de FTP en ftp://ftp.ripe.net/ipv6/nrl .

El daemon de Cisco se basa en la versión 5 de ISAKMP y utiliza las funciones del Protocolo de determinación de claves Oakley versión 1.

Se ha establecido una lista de correo para los problemas, las correcciones de errores, los cambios de la portada y el debate general sobre ISAKMP y Oakley en isakmp-oakley@cisco.com. Para unirse a esta lista, envíe una solicitud de correo electrónico con un cuerpo de mensaje de **suscripción isakmp-oakley** a: majordomo@cisco.com.

Implementación del Departamento de Defensa de Estados Unidos

La Oficina de Investigación de la Seguridad de la Información de DoD de los Estados Unidos ha hecho que su Implementación del Protocolo ISAKMP esté disponible libremente para su distribución dentro de los Estados Unidos. Hay disponible una interfaz basada en web para descargar el software. Esta implementación no incluye ninguna capacidad de intercambio de claves de sesión, pero sí incluye funciones ISAKMP completas.

Información Relacionada

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