Informations RED ISAKMP et Oakley

Contenu

Introduction

Ce document fournit des informations sur l'Internet Security Association and Key Management Protocol (ISAKMP) et le protocole Oakley Key Determination Protocol. Ces protocoles sont les principaux candidats à la gestion des clés Internet examinés par le Groupe de travail IPSec de l'Internet Engineering Task Force (IETF).

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Conventions

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

Informations techniques

À propos d'ISAKMP

L'ISAKMP fournit un cadre pour la gestion des clés Internet et fournit le support de protocole spécifique pour la négociation des attributs de sécurité. Seul, il n'établit pas de clés de session. Cependant, il peut être utilisé avec divers protocoles d'établissement de clé de session, comme Oakley, pour fournir une solution complète à la gestion des clés Internet. La spécification ISAKMP est également disponible en post-script.

À propos d'Oakley

Le protocole Oakley utilise une technique Diffie-Hellman hybride pour établir des clés de session sur les hôtes et les routeurs Internet. Oakley fournit l'importante propriété de sécurité de Perfect Forward Secrecy (PFS) et est basée sur des techniques cryptographiques qui ont survécu à un examen public approfondi. Oakley peut être utilisé seul, si aucune négociation d'attribut n'est nécessaire, ou Oakley peut être utilisé conjointement avec ISAKMP. Lorsque ISAKMP est utilisé avec Oakley, le blocage de clé n'est pas possible.

Les protocoles ISAKMP et Oakley ont été combinés en un protocole hybride. La résolution d'ISAKMP avec Oakley utilise le cadre d'ISAKMP pour prendre en charge un sous-ensemble des modes d'échange de clés d'Oakley. Ce nouveau protocole d'échange de clés fournit des PFS en option, une négociation d'attribut d'association de sécurité complète et des méthodes d'authentification qui fournissent à la fois la répudiation et la non-répudiation. Les mises en oeuvre de ce protocole peuvent être utilisées pour établir des VPN et permettre aux utilisateurs de sites distants (qui peuvent disposer d'une adresse IP allouée dynamiquement) d'accéder à un réseau sécurisé.

À propos d'IPSec

Le groupe de travail IPSec de l'IETF élabore des normes pour les mécanismes de sécurité de couche IP pour IPv4 et IPv6. Le groupe développe également des protocoles génériques de gestion des clés à utiliser sur Internet. Pour plus d'informations, reportez-vous à la Vue d'ensemble de la sécurité et du chiffrement IP.

Logiciel ISAKMP

Implémentation de Cisco Systems

Le logiciel de démon ISAKMP de Cisco Systems est disponible gratuitement pour toute utilisation commerciale ou non commerciale afin de faire progresser ISAKMP en tant que solution standard de gestion des clés Internet.

Le logiciel Cisco ISAKMP est disponible aux États-Unis et au Canada via un formulaire de téléchargement Web du Massachusetts Institute of Technology (MIT). En raison des lois américaines sur le contrôle des exportations, Cisco ne peut pas distribuer ce logiciel en dehors des États-Unis et du Canada.

Le démon Cisco ISAKMP utilise l'API (Key Management Application Program Interface) de PF_KEY pour s'enregistrer auprès d'un noyau de système d'exploitation (qui a mis en oeuvre cette API) et de l'infrastructure de gestion des clés environnante. Les associations de sécurité qui ont été négociées par le démon ISAKMP sont insérées dans le moteur clé du noyau. Ils sont ensuite

disponibles pour utilisation par les mécanismes de sécurité IPSec standard du système (en-tête d'authentification [AH] et Encapsulating Security Payload [ESP]).

La distribution de logiciels IPv6+IPSec du Naval Research Laboratory (NRL) des systèmes dérivés de 4.4-BSD (y compris Berkeley Software Design, Inc. [BSDI] et NetBSD) est distribuable librement. Elle inclut la mise en oeuvre d'IPv6, d'IPSec pour IPv6, d'IPSec pour IPv4 et de l'interface PF_KEY. Le logiciel NRL est disponible aux États-Unis et au Canada par l'intermédiaire d'un formulaire de téléchargement Web du MIT. En dehors des États-Unis et du Canada, le logiciel NRL est disponible par FTP à partir de ftp://ftp.ripe.net/ipv6/nrl .

Le démon Cisco est basé sur la version 5 d'ISAKMP et utilise les fonctionnalités du protocole de détermination de clé Oakley version 1.

Une liste de diffusion pour les problèmes, les corrections de bogues, les changements de portage et les discussions générales sur ISAKMP et Oakley a été établie à l'adresse isakmp-oakley@cisco.com. Pour vous joindre à cette liste, envoyez une demande par e-mail avec un corps de message **subscribe isakmp-oakley** à : majordomo@cisco.com.

Mise en oeuvre du Département de la défense des États-Unis

Le département de la Défense des États-Unis a rendu ISAKMP Prototype Implementation disponible gratuitement pour distribution aux États-Unis. Une interface Web permet de télécharger le logiciel. Cette implémentation n'inclut aucune fonctionnalité d'échange de clé de session, mais inclut toutes les fonctionnalités ISAKMP.

Informations connexes

- Page d'assistance IPsec
- Support technique - Cisco Systems