Informations RED ISAKMP et Oakley

Contenu

Introduction

Ce document fournit l'association de sécurité de l'information sur Internet et le protocole de gestion de clés (ISAKMP) et la détermination Protocol de clé d'Oakley. Ces protocoles sont de principaux concurrents pour la gestion des clés d'Internet étant considérée par le groupe de travail d'IPSec de l'Internet Engineering Task Force (IETF).

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

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

Conventions

Pour plus d'informations sur les conventions de documents, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Les informations techniques

Au sujet de l'ISAKMP

L'ISAKMP fournit un cadre pour la gestion des clés d'Internet et fournit le support spécifique de protocole pour la négociation des attributs de Sécurité. Seulement, il n'établit pas des clés de session. Toutefois il peut être utilisé avec de divers protocoles d'établissement de clé de session, tels qu'Oakley, pour fournir une solution complète à la gestion des clés d'Internet. La spécification d'ISAKMP est également disponible dans le post-scriptum.

Au sujet d'Oakley

Le protocole d'Oakley emploie une technique hybride de Diffie-Hellman pour établir des clés de session sur des hôtes et des Routeurs d'Internet. Oakley fournit l'importante propriété de Sécurité du perfect forward secrecy (PFS) et est basé sur les techniques cryptographiques qui ont survécu au scrutin public substantiel. Oakley peut être utilisé par lui-même, si aucune négociation d'attribut n'est nécessaire, ou Oakley peut être utilisé en même temps que l'ISAKMP. Quand l'ISAKMP est utilisé avec Oakley, l'engagement principal n'est pas faisable.

L'ISAKMP et les protocoles d'Oakley ont été combinés dans un protocole hybride. La résolution de l'ISAKMP avec Oakley emploie le cadre de l'ISAKMP pour prendre en charge un sous-ensemble de modes d'échange de clé d'Oakley. Ce nouveau protocole d'échange de clés fournit le PFS facultatif, la pleine négociation d'attribut d'association de sécurité, et les méthodes d'authentification qui fournissent la répudiation et la non-répudiation. Des réalisations de ce protocole peuvent être utilisées pour établir des VPN et pour tenir compte également des utilisateurs de l'accès de sites distants (qui peuvent avoir une adresse IP dynamiquement allouée) à un réseau sécurisé.

Au sujet d'IPSec

Le groupe de travail d'IPSec De l'IETF développe des normes pour des mécanismes de sécurité d'IP-couche pour l'ipv4 et l'IPv6. Le groupe également développe des protocoles de gestion de clés génériques pour l'usage sur l'Internet. Le pour en savoir plus, se rapportent à la sécurité IP et à l'aperçu de cryptage.

Logiciel d'ISAKMP

Implémentation de Cisco Systems

Le logiciel de démon de l'ISAKMP de Cisco Systems est gratuit disponible pour n'importe quel usage commercial ou non commercial d'aider l'ISAKMP anticipé comme solution étalon à la gestion des clés d'Internet.

Le logiciel d'ISAKMP de Cisco est disponible dans les Etats-Unis et le Canada par une forme de téléchargement de Web à partir de Massachusetts Institute of Technology (MIT). En raison des lois de contrôle d'exportation des Etats-Unis, Cisco ne peut pas distribuer ce logiciel en dehors des Etats-Unis et du Canada.

Le démon d'ISAKMP de Cisco emploie l'interface de programmation de gestion des clés PF_KEY (API) pour s'inscrire à un noyau du système d'exploitation (qui a mis en application cet API) et l'infrastructure de gestion des clés environnante. Des associations de sécurité qui ont été négociées par le démon d'ISAKMP sont insérées dans l'engine principale du noyau. Ils sont alors

disponibles à l'usage des mécanismes de sécurité d'IPSec de la norme de système (en-tête d'authentification [OH] et encapsuler charge utile de Sécurité [ESP]).

Les États-Unis libre-distribuables la distribution logicielle que navale du laboratoire de recherche (NRL) IPv6+IPSec pour 4.4-BSD a dérivé des systèmes (Berkeley Software Design, Inc. y compris [BSDI] et NetBSD) inclut l'implémentation de l'IPv6, IPSec pour l'IPv6, IPSec pour l'ipv4, et l'interface PF_KEY. Le logiciel NRL est disponible dans les Etats-Unis et le Canada par une forme de téléchargement de Web à partir de MIT. En dehors des Etats-Unis et du Canada, le logiciel NRL est disponible par le FTP de ftp://ftp.ripe.net/ipv6/nrl .

Le démon de Cisco est basé sur la version 5 d'ISAKMP et utilise des caractéristiques de la version 1 de Protocol de détermination de clé d'Oakley.

Une liste de diffusion pour des problèmes, des correctifs de bogue, des modifications de mise en communication, et la discussion générale de l'ISAKMP et de l'Oakley a été établie chez isakmp-oakley@cisco.com. Pour joindre cette liste, envoyez une demande d'email avec un corps du message de **s'abonnent l'ISAKMP-oakley** à : majordomo@cisco.com.

Implémentation du Ministère américain de la Défense des Etats-Unis (DoD)

Le bureau des États-Unis DoD de la recherche de protection des données a rendu son implémentation de prototype d'ISAKMP librement disponible pour la distribution dans les Etats-Unis. Une interface basée sur le WEB est disponible pour télécharger le logiciel. Cette implémentation n'inclut aucune capacité d'échange de clé de session, mais inclut de pleines caractéristiques d'ISAKMP.

Informations connexes

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