RED ISAKMP和Oakley信息

目录

简介

本文在互联网安全协会和密钥管理协议(ISAKMP)和Oakley密钥确定协议提供信息。这些协议是考虑的互联网密钥管理的主导的竞争者由互联网工程任务组(IETF)的 IPSec工作组 。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

技术信息

关于ISAKMP

ISAKMP为互联网密钥管理提供一个框架并且为安全属性的协商提供特定协议支持。单独，它不设立会话密钥。然而它可以与多种会话密钥建立协议一起使用，例如Oakley，提供完整的解决方案给互联网密钥管理。ISAKMP规格也是可用的在附言。

关于Oakley

Oakley协议使用一个混合的Diffie-Hellman技术设立在互联网主机和路由器的会话密钥。Oakley提供完整转发安全性(PFS)重要安全属性和根据生存了大量的公众监督的密码技术。可以单独使用Oakley，如果属性协商不是需要的，或者Oakley可以与ISAKMP一道使用。当ISAKMP与Oakley一起使用时，密钥代管法不可行。

ISAKMP和Oakley协议被结合了到混合协议。ISAKMP的解决方法与Oakley的使用ISAKMP框架支持Oakley密钥交换模式的一子集。此新密钥交换协议提供可选PFS、提供拒绝和不可否认性的完整的安全关联属性协商和认证方法。此协议的实施可以用于设立VPN并且允许从远程站点(谁可以有一个动态地已分配IP地址)访问的用户到安全网络。

关于IPSec

IETF的IPSec工作组 发展IP层安全机制的标准IPv4和IPv6的。组也开发一般键管理协议为在互联网的使用。欲知更多信息，参考IP安全和加密概述。

ISAKMP软件

Cisco系统实施

Cisco系统的ISAKMP守护软件免费是可用的为所有商业或非商业使用帮助预先的ISAKMP作为标准解决方案到互联网密钥管理。

Cisco ISAKMP软件是可用的在美国和加拿大通过从麻省理工学院(MIT)的一Web下载表。由于美国出口控制控制定律，思科无法分配此软件在美国和加拿大境外。

Cisco ISAKMP守护程序使用PF_KEY密钥管理Application Program Interface (API)向登记实现此API)的一个操作系统的内核(和周围的密钥管理基础设施。由ISAKMP守护协商的安全关联插入到内核的关键引擎。他们是然后可用的供系统标准IPSec安全安全机制使用(认证报头[AH]和封装安全有效载荷[ESP])。

4.4-BSD派生的系统的可自由分配的美国Naval Research Laboratory (NRL) IPv6+IPSec软件分配(包括Berkeley Software Design， Inc. [BSDI]和NetBSD)包括IPv6的实施， IPv6的IPSec， IPv4和PF_KEY接口的IPSec。NRL软件是可用的在美国和加拿大通过从MIT的一Web 下载表。在美国和加拿大境外， NRL软件通过从ftp://ftp.ripe.net/ipv6/nrl的FTP是可用的 。

Cisco守护程序根据ISAKMP版本5并且使用从Oakley密钥确定协议版本1.的功能。

问题、bug修复、移植的ISAKMP和Oakley更改和一般讨论的一邮件列表设立了在isakmp-oakley@cisco.com。要加入此列表，请发送与消息主题的一个电子邮件请求**订阅isakmp-oakley**对：majordomo@cisco.com。

美国国防部(DoD)实施

信息安全研究美国DoD办公室使其ISAKMP原型实施 免费可得对在美国内的分配。基于Web的接口

为下载是可用的软件。此实施不包括任何会话密钥Exchange功能，然而包括全双工ISAKMP功能。

相关信息

- IPSec 支持页面
- 技术支持 - Cisco Systems