RED ISAKMP和Oakley信息

目录

简介

本文档提供有关互联网安全关联和密钥管理协议(ISAKMP)和Oakley密钥确定协议的信息。这些协议是Internet密钥管理的主要竞争者，Internet工程任务组(IETF) 的IPSec工作组正在 考虑这些协议。

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

有关文件规则的更多信息请参见“ Cisco技术提示规则”。

技术信息

关于ISAKMP

ISAKMP为Internet密钥管理提供框架，并为安全属性协商提供特定协议支持。仅此一项，它不建立会话密钥。但是，它可与各种会话密钥建立协议（如Oakley）配合使用，为Internet密钥管理提供完整的解决方案。ISAKMP规范也可在postscript中使用。

关于奥克利

Oakley协议使用混合Diffie-Hellman技术在Internet主机和路由器上建立会话密钥。Oakley提供完美向前保密(PFS)的重要安全属性，并基于经过大量公众监督的加密技术。如果不需要属性协商，Oakley可自行使用，或者Oakley可与ISAKMP一起使用。当ISAKMP与Oakley配合使用时，密钥托管不可行。

ISAKMP和Oakley协议已合并为混合协议。ISAKMP与Oakley的解析使用ISAKMP框架支持Oakley密钥交换模式的子集。此新密钥交换协议提供可选的PFS、完全安全关联属性协商和身份验证方法，可同时提供可抵赖性和不可抵赖性。此协议的实施可用于建立VPN，并允许来自远程站点（可能具有动态分配的IP地址）的用户访问安全网络。

关于IPSec

IETF的IPSec工作组 为IPv4和IPv6开发IP层安全机制的标准。该工作组还在开发用于Internet的通用密钥管理协议。有关详细信息，请参阅IP安全和加密概述。

ISAKMP软件

思科系统实施

思科系统公司的ISAKMP守护程序软件可免费用于任何商业或非商业用途，以帮助将ISAKMP作为互联网密钥管理的标准解决方案加以推广。

Cisco ISAKMP软件可通过麻省理工学院(MIT)的Web下 载表在美国和加拿大境内提供。 由于美国出口控制法，思科无法在美国和加拿大之外分发此软件。

Cisco ISAKMP守护程序使用PF_KEY密钥管理应用程序接口(API)向操作系统内核（已实施此API）和周围的密钥管理基础设施注册。由ISAKMP守护程序协商的安全关联将插入到内核的密钥引擎中。然后，系统的标准IPSec安全机制（身份验证报头[AH]和封装安全负载[ESP]）可以使用它们。

4.4-BSD衍生系统（包括Berkeley Software Design， Inc. [BSDI]和NetBSD）的可自由分发的美国海军研究实验室(NRL)IPv6+IPSec软件分发包括IPv6、IPSec for IPv6、IPSec forIPv4和PF_KEY接口。NRL软件在美国和加拿大通过MIT的Web下载表格 提供。在美国和加拿大以外，NRL软件可通过FTP从ftp://ftp.ripe.net/ipv6/nrl获取 。

思科守护程序基于ISAKMP第5版，使用Oakley密钥确定协议第1版中的功能。

有关问题、漏洞修复、移植更改以及ISAKMP和Oakley的一般讨论的邮件列表已在isakmp-oakley@cisco.com上建立。要加入此列表，请向以下用户发送邮件请求：majordomo@cisco.com。

美国国防部(DoD)实施

美国国防部信息安全研究办公室已经免费提供其ISAKMP原型 ，供在美国境内分发。基于Web的界

面可用于下载软件。此实施不包括任何会话密钥交换功能，但包括完整的ISAKMP功能。

相关信息

- IPSec 支持页面
- 技术支持 - Cisco Systems