RED ISAKMP和Oakley資訊

目錄

簡介

本檔案提供有關網際網路安全性關聯和金鑰管理通訊協定(ISAKMP)和Oakley金鑰決定通訊協定的資訊。 這些協定是Internet工程任務組(IETF)的IPSec工作組正在考慮的Internet金鑰管理 的主要競爭者。

必要條件

需求

本文件沒有特定需求。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

技術問答

關於ISAKMP

ISAKMP提供網際網路金鑰管理框架，並為安全屬性的協商提供特定的協定支援。它本身不建立會話金鑰。但它可以與各種會話金鑰建立協定（如Oakley）一起使用，為網際網路金鑰管理提供完整的解決方案。ISAKMP規範也可用於postscript。

關於Oakley

Oakley協定使用混合Diffie-Hellman技術在Internet主機和路由器上建立會話金鑰。Oakley提供了完全向前保密(PFS)的重要安全屬性，並且基於經過大量公眾審查的加密技術。如果不需要屬性協商，Oakley可以單獨使用，或者可以與ISAKMP結合使用。當ISAKMP與Oakley一起使用時，金鑰託管不可行。

ISAKMP和Oakley協定已合併為混合協定。ISAKMP與Oakley的分辨使用ISAKMP框架來支援Oakley金鑰交換模式的一個子集。這種新的金鑰交換協定提供了可選的PFS、完全安全關聯屬性協商以及同時提供否認和不可否認的身份驗證方法。此協定的實施可用於建立VPN，並允許遠端站點（可能有動態分配的IP地址）使用者訪問安全網路。

關於IPSec

IETF的IPSec工作組 (IPSec Working Group)為IPv4和IPv6制定IP層安全機制的標準。該團隊還正在開發通用的金鑰管理協定，以用於Internet。如需詳細資訊，請參閱IP安全性與加密概觀。

ISAKMP軟體

Cisco Systems實作

Cisco Systems的ISAKMP守護程式軟體免費供任何商業或非商業用途使用，以幫助將ISAKMP作為網際網路金鑰管理的標準解決方案進行推廣。

Cisco ISAKMP軟體可通過麻省理工學院(MIT)的Web下載表單在美國和加拿大提供。 由於美國出口管製法律，思科無法在美國及加拿大以外分發此軟體。

Cisco ISAKMP守護程式使用PF_KEY金鑰管理應用程式介面(API)向作業系統核心（已實現此API）和周圍的金鑰管理基礎設施進行註冊。由ISAKMP守護進程協商的安全關聯將插入核心的金鑰引擎中。然後，它們可由系統的標準IPSec安全機制（身份驗證報頭[AH]和封裝安全負載[ESP]）使用。

可自由分發的美國海軍研究實驗室(NRL)IPv6+IPSec軟體分發用於4.4-BSD衍生系統（包括Berkeley Software Design， Inc. [BSDI]和NetBSD），包括IPv6、IPSec for IPv6、IPSec for IPv4和PF_KEY介面的實現。NRL軟體在美國和加拿大可通過麻省理工學院的網路下載表 提供。在美國和加拿大以外，可通過FTP從ftp://ftp.ripe.net/ipv6/nrl 獲取NRL軟體。

Cisco守護程式基於ISAKMP版本5，並使用Oakley金鑰確定協定版本1中的功能。

有關問題、錯誤修復、埠變更以及ISAKMP和Oakley的一般性討論的郵件清單已建立在isakmp-oakley@cisco.com。要加入此清單，請將包含訂閱isakmp-oakley的郵件正文**的電子郵件請求**傳送到：majordomo@cisco.com。

美國國防部(DoD)實施

美國國防部資訊保安研究辦公室已經將其ISAKMP原型實施 ，免費提供給美國境內分發。基於

Web的介面可用於下載軟體。此實施不包括任何會話金鑰交換功能，但包括完整的ISAKMP功能。

相關資訊

- IPSec支援頁面
- 技術支援 - Cisco Systems