RED ISAKMP と Oakley に関する情報

内容

概要

このドキュメントでは、Internet Security Association and Key Management Protocol(ISAKMP)およびOakley Key Determination Protocol(OAKLEY)について説明します。これらのプロトコルは、インターネット技術特別調査委員会(IETF)のIPSec Working Group (IPSec Working Group)によって検討されているインターネットキー管理の主要なコンテンダーです 。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

表記法

ドキュメント表記の詳細は、「シスコ テクニカル ティップスの表記法」を参照してください。

技術情報

ISAKMPについて

ISAKMPは、インターネットキー管理のフレームワークを提供し、セキュリティ属性のネゴシエーションに対する特定のプロトコルサポートを提供します。単独では、セッションキーは確立されません。ただし、Oakleyなどのさまざまなセッションキー確立プロトコルで使用して、インターネットキー管理の完全なソリューションを提供できます。ISAKMP仕様は、Postscriptでも使用できます。

Oakleyについて

Oakleyプロトコルは、ハイブリッドDiffie-Hellman(DH)技術を使用して、インターネットホストおよびルータにセッションキーを確立します。Oakleyは、Perfect Forward Secrecy（PFS；完全転送秘密）の重要なセキュリティ特性を提供し、暗号技術に基づいており、公開されている人々の調査から生き残っています。Oakleyは、属性ネゴシエーションが不要な場合は単独で使用でき、OakleyはISAKMPと組み合わせて使用できます。ISAKMPがOakleyで使用されている場合、キーエスクローは実行できません。

ISAKMPプロトコルとOakleyプロトコルは、ハイブリッドプロトコルに統合されています。OakleyによるISAKMPの解決では、ISAKMPのフレームワークを使用して、Oakleyキー交換モードのサブセットをサポートします。この新しいキー交換プロトコルは、オプションのPFS、完全なセキュリティアソシエーション(SA)属性ネゴシエーション、およびレピュテーションと非レピュテーションの両方を提供する認証方式を提供します。このプロトコルの実装は、VPNを確立するために使用でき、また、リモートサイト（動的に割り当てられたIPアドレスを持つ可能性がある）のユーザがセキュアネットワークにアクセスできるようにします。

IPSecについて

IETFのIPSec Working Groupは 、IPv4とIPv6の両方のIP層セキュリティメカニズムの標準を開発し、インターネットで使用するための一般的なキー管理プロトコルも開発しています。詳細については、『IP Security and Encryptionの概要』を参照してください。

ISAKMPソフトウェア

シスコの導入

Cisco SystemsのISAKMPデーモンソフトウェアは、ISAKMPをインターネットキー管理の標準ソリューションとして拡張するために、商用または非商用の用途で無料で利用できます。

Cisco ISAKMPソフトウェアは、米国およびカナダでMassachusetts Institute of Technology(MIT)からWebダウンロードフォームを使用して入手できます。 米国の輸出規制法により、シスコはこのソフトウェアを米国およびカナダ以外に配布できません。

Cisco ISAKMPデーモンは、PF_KEY Key Management Application Program Interface(API)を使用して、オペレーティングシステムカーネル（このAPIを実装した）およびその周辺のキー管理インフラストラクチャに登録します。ISAKMPデーモンによってネゴシエートされたセキュリティアソシエーションは、カーネルのキーエンジンに挿入されます。この機能は、システムの標準IPSecセキュリティメカニズム(認証ヘッダー(AH)およびカプセル化セキュリティペイロード(ESP))で使用できます。

4.4-BSD派生システム（Berkeley Software Design, Inc. [BSDI]およびNetBSDを含む）用の無料配

布可能なU.S. Naval Research Laboratory(NRL)IPv6+IPSecソフトウェア配布IPv4用のEC、およびPF_KEYインターフェイス。NRLソフトウェアは、MITのWebダウンロードフォームを通じて米国とカナダで入手できます 。米国およびカナダ以外では、NRLソフトウェアはftp://ftp.ripe.net/ipv6/nrlからFTPで入手できます 。

CiscoデーモンはISAKMPバージョン5に基づいており、Oakley Key Determination Protocolバージョン1の機能を使用します。

ISAKMPおよびOakleyに関する問題、バグ修正、移植の変更、および一般的なディスカッションのメーリングリストがisakmp-oakley@cisco.comで確立されました。このリストに参加するには、**subscribe isakmp-oakley**のメッセージ本文を含む電子メール要求**を次の宛先に送信**します。majordomo@cisco.com にアクセスしてください。

米国国防総省(DoD)の実装

米国のDoD Office of Information Security Researchは、ISAKMPプロトタイプの実装を米国内で自由に配布できるようにした 。ソフトウェアのダウンロードには、Webベースのインターフェイスを使用できます。この実装には、セッションキー交換機能は含まれませんが、完全なISAKMP機能が含まれています。

関連情報

- IPSec に関するサポート ページ
- テクニカルサポート - Cisco Systems