RED ISAKMP と Oakley に関する情報

目次

概要

この資料は Internet Security Association and Key Management Protocol（ISAKMP）および Oakley キー判断プロトコルで情報を提供したものです。 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 ワーキンググループが考慮するインターネット鍵管理のための一流 競争相手です 。

前提条件

要件

このドキュメントに関する固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 はインターネット鍵管理に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特定のプロトコル サポートを提供します。 単独で、それはセッションキーを確立しません。 インターネット鍵管理に完全なソリューションを提供するのにそれがさまざまなセッションキー 確立プロトコルとどんなに、Oakley のような使用することができても。 ISAKMP 仕様はまたポストスクリプトで利用できます。

Oakley について

Oakley プロトコルはインターネットホストおよびルータのセッションキーを確立するハイブリッド デフィーヘルマン手法を使用します。 Oakley は完全転送秘密（PFS）の重要なセキュリティ特性を提供し、相当な国民の詮索を存続させた暗号手法に基づいています。 Oakley はアトリビュート ネゴシエーションが必要ではない、または Oakley は ISAKMP と共に使用することができます場合それ自体使用することができます。 ISAKMP が Oakley と使用されるとき、キー エスクローは実行不可能です。

ISAKMP および Oakley プロトコルはハイブリッド プロトコルに結合されました。 Oakley の ISAKMP の解決は Oakley 鍵交換モードのサブセットをサポートするのに ISAKMP のフレームワークを使用します。 この New 鍵 交換 プロトコルは否認および否認防止を両方提供するオプションの PFS、完全なセキュリティアソシエーション属性のネゴシエーションおよび認証方式を提供します。 このプロトコルの実装が VPN を確立するのに使用することができ、リモートサイト（だれが可能にするために動的に割り当てられた IP アドレスがあるかもしれないか）からのユーザをまたセキュア ネットワークにアクセスして下さい。

IPSec について

IETF の IPSec ワーキンググループは IPv4 および IPv6 両方の IP層 セキュリティ機構のための規格を開発します。 グループはまたインターネットの使用のための総称 キー 管理プロトコルを開発しています。 詳細については、IPセキュリティおよび暗号化 外観を参照して下さい。

ISAKMPソフトウェア

シスコシステムズ 実装

Cisco 社の ISAKMP デーモン ソフトウェアはインターネット鍵管理に標準 ソリューションとして先発 ISAKMP を助けてあらゆる商業か非営利的な無料で利用可能です。

Cisco ISAKMP ソフトウェアはマサチューセッツ工科大学（MIT）からの Web Download 形式を通して 米国およびカナダの内で利用できます。 米国エクスポート制御関連法規が原因で、Cisco は米国およびカナダ国外のこのソフトウェアを配布することができません。

Cisco ISAKMP デーモンは（PF_KEY キー管理 Application Program Interface （API）を登録するのにこの API を設定した）とオペレーティング システム カーネル周囲キー管理 インフラストラクチャ使用し。 ISAKMP デーモンによってネゴシエートされたセキュリティ結合はカーネルのキー エンジンに挿入されます。 彼らはシステム規格 IPsec セキュリティ メカニズム（認証ヘッダー[AH]によってそれから利用可能および Encapsulating Security Payload [ESP]）です。

4.4-BSD のための自由に配信できる米国 Naval Research Laboratory （NRL） IPv6+IPSec ソフトウェア配布はシステムを（を含む Berkeley Software Design、Inc. [BSDI]および NetBSD）含まれ

ています IPv6 の実装が、IPv6 のための IPSec、IPv4 および PF_KEY インターフェイスのための IPSec 得ました。 NRL ソフトウェアは MIT からの Web Download 形式を通して米国およびカナダの内で 利用できます。 米国およびカナダ国外で、NRL ソフトウェアは ftp://ftp.ripe.net/ipv6/nrl からの FTP を通して利用できます 。

Cisco デーモンは ISAKMP バージョン 5 に基づき、Oakley キー決定プロトコル バージョン 1.からの機能を使用します。

ISAKMP および Oakley の問題、バグ修正、移植変更および概論のためのメーリングリストは isakmp-oakley@cisco.com で確立されました。 このリストに加入するために、メッセージ ボディとの電子メールでの請求をの**定期講読します isakmp-oakley を**を送信 して下さい: majordomo@cisco.com。

米国米国国防総省（DoD）実装

情報 セキュリティ リサーチの米国 DoD オフィスは ISAKMP プロトタイプ実装を 米国内のディストリビューションに自由に利用できるようにしました。 Webベースのインターフェイスはソフトウェアをダウンロードするために利用できます。 この実装はセッションキー 交換機能が含まれませんが、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