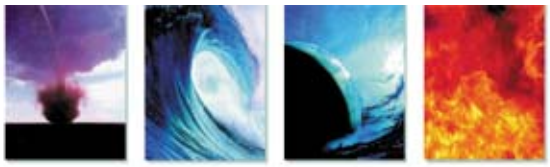
NETWORKING STACKS



IPSec プロトコルスタック

Overview

インターネットプロトコルセキュリティ（IPSec）は、ネットワーク層で、インターネット上の確保された通信を提供するためのプロトコルスイートです。IPSecのゴールは、高価なホストとアプリケーション部分修正を必要とせずに、既存のネットワークインフラストラクチャーの脅威を最小化することです。IPSecは、IPv6でサポートされています。

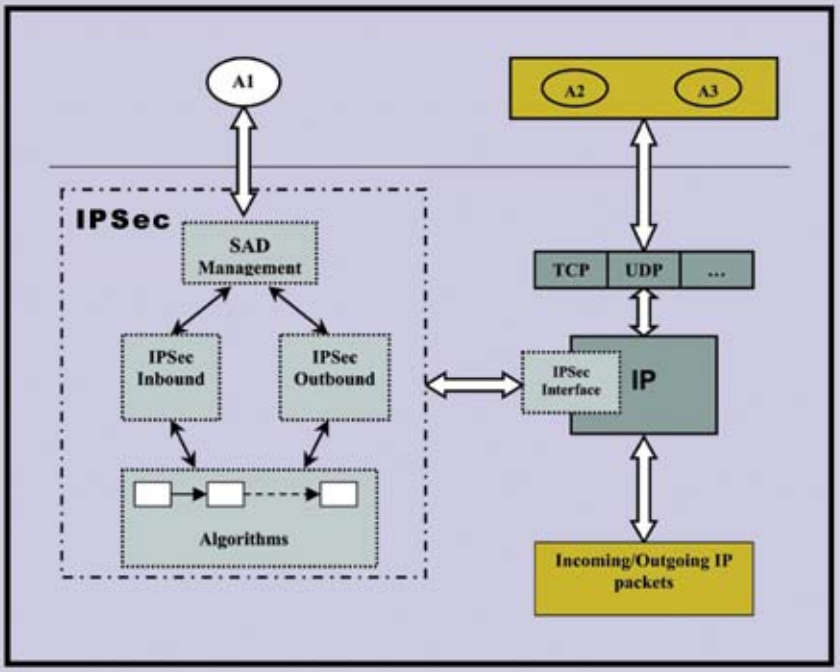
IPSecの提供するサービス：
- データソース認証
- データの完全性
- 機密性
- リプレイ攻撃からの保護
- IPベースのアプリケーションとの運用性

e3Global

イースリーグローバル株式会社

〒106-0032
東京都港区六本木 3-4-24 六本木足立ビル 302
TEL 03-6229-4525　FAX 03-6229-4526
http://www.e3global.com/

e3-IPSec Architecture



スタック概要

e3-IPSecのコンポーネント：
- 暗号ペイロード（ESP）
- 認証ヘッダー（AH）
- 鍵交換（IKE）プロトコルを実装するために使用される、インターネットセキュリティアソシエーション＆インターネット鍵管理プロトコル（ISAKMP）

機能と特長

- **認証ヘッダー（AH）**
  IP認証ヘッダー（AH）は、コネクションレス完全性とデータソース認証をIPデータグラムに提供するために使用されます。また、リプレイからの保護も提供します。
- **暗号ペイロード（ESP）**
  機密性、データソース認証、コネクションレス完全性、反リプレイサービス、制限されたトラフィックフローの機密性を提供します。
- **トランスポートモード**
  介在セキュリティゲートウェイなしで、クライアント－クライアント、またはクライアント－サーバー通信をサポートします。
- **セキュリティアソシエーション（SA）**
  セキュリティアソシエーション（SA）は、安全に通信するためにエンティティがどのようにセキュリティサービスを用いるかを記述する2つ以上のエンティティ間の関係です。
- **インターネット鍵管理プロトコル（IKMP）**
  IKEは、セキュリティアソシエーションを作成するメカニズムを提供します。IPSecはパケットレベル処理を提供する一方、インターネットキー管理プロトコル（IKMP）はセキュリティアソシエーションのネゴシエーションを行います。IKEは、IPSecのセキュリティアソシエーションを設定するために使われます。MainとQuickモードのオペレーションをサポートしています。

サポートRFC

- RFC 2401: Security Architecture for the Internet Protocol
- RFC 2402: IP Authentication Header
- RFC 2403: The Use of HMAC-MD5 within ESP and AH
- RFC 2404: The Use of HMAC-SHA-1 within ESP and AH
- RFC 2406: IP Encapsulating Security Payload (ESP)
- RFC 2410: The NULL Encryption Algorithm and Its Use With IPSec
- RFC 2451: The ESP CBC-Mode Cipher Algorithms

お問合せ: info@e3global.com イースリーグローバル株式会社　ネットワーク事業部