

IPsec高速処理エンジン

当社では、VPNにおけるIPsec処理を、双方向フルワイヤスピードで実行するLSIの開発を進めています。本稿では、その基本的なコンセプトと特長について解説します。

* VPN : Virtual Private Network
* IPsec : Internet Protocol Security

はじめに

当社では、VPNにおけるIPsec処理を、双方向100Mbpsフルワイヤスピードで実行するLSIの開発を進めています。本製品を使用することにより、現在主流のルックアサイド*1型のIPsec処理LSIと比べて飛躍的な処理性能の向上が期待できます。本製品は、高速・低遅延・低揺らぎが求められる、これからのブロードバンドVPNルータに最適なLSIを目指しています。

IPsecとは

IPsecは、IPパケット単位でのセキュリティを実現する技術です。IPパケットを暗号化し、通信相手が本物であることや通信データが改ざんされていないことを保証し、アクセス制御を行います。

これまで、多くのセキュリティ機能はアプリケーション別に提供されてきましたが、IPsecの登場によって、アプリケーションごとにセキュリティ機能を用意する必要がなくなります。

近年、インターネットにおいて、拠点間を仮想的な専用線で相互接続し、安全な通信を可能にするVPNが注目を集めています。IPsecはVPNを実現するためのキーテクノロジーの一つとして利用されています。

開発コンセプト

ブロードバンドネットワークの普及に伴い、VPN業界標準であるIPsecに対応したブロードバンドルータが利用される機会が増えています。IPsecの機能であるパケットの暗号化/認証を実行するには、高速かつ大量の計算処理が必要です。このため、通常はIPsec専用のLSIを使って計算処理を行います。現状のIPsec対応VPNルータでは、ルックアサイド型のIPsec処理用LSIが使用されており、PCIバス経由でCPUとデータのやり取りを行います。しかし、このアーキテクチャではPCIバスにおけるボトルネックが存在し、IPsec処

理のスループットに大きな影響を与えています。

図1に、現状のIPsec対応VPNルータの内部構成を示します。

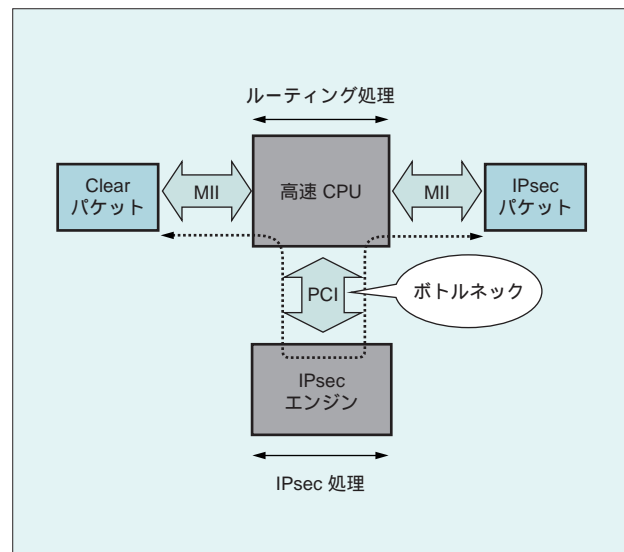
本製品は、ホストCPUからSRAMインタフェース経由で必要なコンフィギュレーションを設定したあと、双方向100Mbpsフルワイヤスピードで暗号化/復号化の処理を実行します。IPsecパケットは、MII*2インタフェース経由で、ルーティング処理を行うCPUとやり取りされますので、システムバス・ボトルネックの影響は受けません。

図2に、本製品を使用した場合のVPNルータの内部構成を示します。

図3に、現状のIPsec処理LSIと本製品の、パケットサイズに対するIPsec処理性能(3DES*3使用時)の比較を示します。このように、現状のルックアサイド型のIPsec処理LSIでは、十分な処理性能が得られていません。例えば企業の拠点間をつなぐVPNなど、広帯域が必要とされる市場へのニーズに応えるのは困難です。

一方、本製品は、パケットサイズに関係なくフルワイヤスピードでIPsec処理が可能です。当社では、本製品が高速ブロードバンド

図1 現状のIPsec対応VPNルータの内部構成



時代のVPN通信に欠かせないLSIソリューションとなることを目指しています。

特 長

● MII/RMIIインタフェース搭載

- ・ WAN側 1ポート, LAN側 1ポート(計 2ポート)
- ・ MII/RMIIモードの設定可能
- ・ PHYデバイス制御用SMIインタフェース搭載

● IKE^{*4}エンジン搭載

IKEの計算処理を高速化するために演算サポート用エンジンを搭載しています。

● IPsec処理エンジン搭載

フルワイヤスピードでIPsec処理を実行するために次の機能を搭載しています。

● フルワイヤ暗号エンジン

- DES/3DES(CBCモード)
- AES^{*5}(CBCモード, 鍵長 128/192/256ビット)

● フルワイヤ認証エンジン

- HMAC-SHA-1^{*6}
- HMAC-MD5^{*6}

● SA^{*7}データベース

- 64件のSAを設定可能(暗号方向: 64件, 復号方向: 64件)
- セレクタとして次のパラメータを指定可能
- IPアドレス/ポート番号/セキュリティパラメータ・インデックス(SPI)
- /トランスポート層プロトコル/IPsecプロトコル

● 対応パケット

- ・ PPPoE/パケット
- ・ VLAN^{*8}/パケット
- ・ IPv4/IPv6 両対応
- ・ NAT-Traversal^{*9}対応

● 対応モード

- ・ トランスポートモード(ESP^{*10}, AH^{*11}, ESP and AH)
- ・ トンネルモード(ESP, AH)
- ・ トランスポート over トンネルモード

● ホストインタフェース

- ・ SRAMインタフェース(16/32ビット)
- ・ BigEndian/LittleEndian切替え対応

● 拡張SAチップ

開発中の拡張SAチップ(仮名)を外部接続することで、本製品のSAデータベースの拡張が可能です。64件以上のSAが必要な、大規模ネットワークにも対応できます。

図2 本製品を使用した場合のVPNルータの内部構成

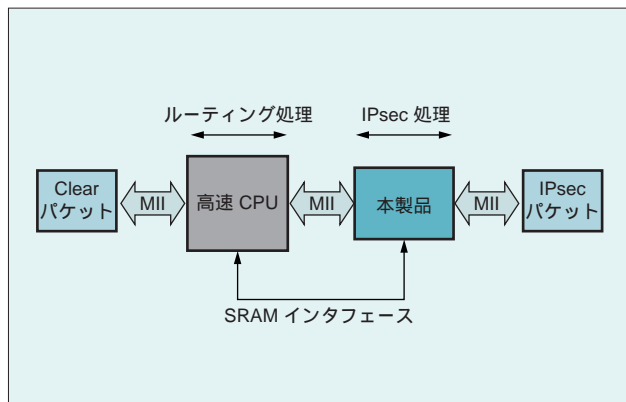
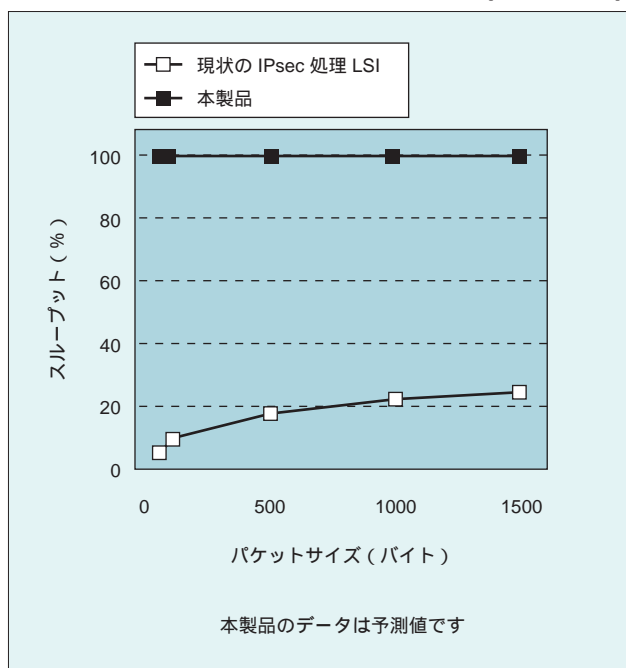


図3 パケットサイズに対するIPsec処理性能比較(3DES使用時)



開発環境

当社では、お客様のスピーディな製品開発をサポートするため、評価用プラットフォームの開発も進めています。OSにはLinuxを採用する予定です。

- * 1 : ルックアサイド : システムバス経由でCPUと接続する方式。
- * 2 : MII/RMII : PHY(物理層)とのインタフェース規格。
- * 3 : DES : 秘密鍵暗号化アルゴリズム。3DESは、DESを三重に適用したものの。
- * 4 : IKE(Internet Key Exchange) : 通信相手の認証を行い、IPsecで使う秘密鍵の交換を行うプロトコル。
- * 5 : AES : DESに代わる次世代の秘密鍵暗号化アルゴリズム。
- * 6 : HMAC-SHA-1, HMAC-MD5 : 通信データの改ざんチェックを行う認証方式。
- * 7 : SA(Security Association) : 送信元, 送信先, セキュリティプロトコルなどを定義した論理的な通信路。
- * 8 : VLAN(Virtual LAN) : LANにおいて、物理的な接続形態に依存することなく、端末の仮想的なグループを構築する技術。
- * 9 : NAT-Traversal : NAT越しにIPsecを行うための技術。
- * 10 : ESP(Encapsulating Security Payload) : 暗号化に用いられるセキュリティプロトコル。
- * 11 : AH(Authentication Header) : 認証に用いられるセキュリティプロトコル。