

第 7 章

VPN

7.1 VPN の設定手法

SEIL は VPN (仮想プライベートネットワーク) を構築する手段として、IPsec をサポートしています。ここでは、SEIL で VPN を構築するための設定手法について説明します。

7.1.1 Tunnel インターフェイス (IP over IP)

Tunnel インターフェイス機能を使用し、拠点間で IP over IP(RFC2003) によるトンネリングが可能です。

非常に簡単な設定で任意の 2 点間結び、静的・動的なルーティングが可能です。

トンネルインターフェイスでは暗号化処理を行わないため SEIL の転送能力をほとんど損ないませんが、通信内容は保護されません。VPN として保護された通信を行うためには、IPsec を併用して Tunnel インターフェイスでの通信を暗号化するように設定します

広域 LAN やフレッツ・グループアクセスのような閉域網中の任意の 2 点間を、隣接するネットワークセグメントのように見せたり、IPv4 over IPv6 トンネル等として、IPv4(または IPv6) ネットワーク上でルーティングされないプロトコルをトンネリングする場合等にも有効です。

7.1.2 ポリシーベース IPsec(トンネルモード IPsec/トランスポートモード IPsec)

一般的な IPsec 対応機器で用いられる、トンネルモードまたはトランスポートモードの IPsec を使用して拠点間で暗号化トンネルを構成し、通信内容を盗聴などから保護します。

ネットワーク対ネットワーク間またはネットワーク対ホスト間の VPN にはトンネルモードを使用し、ホスト対ホスト間の VPN にはトランスポートモードを使用します。

暗号化対象とする通信は、送信元や宛先のアドレスやポート番号などに基づくセキュリティポリシーの設定により判別して暗号化トンネルへ通されます。

ブロードキャストやマルチキャストのパケットはセキュリティポリシーにマッチさせることができないため、拠点間で RIP や OSPF によるルーティングが必要な構成には向きませんが、ルーティング設定では扱えない、送信元情報による経路制御が可能です。(ルーティング設定では宛先情報により経路

制御を行います)

7.1.3 ルーティングベース IPsec(IPsec インターフェイス)

ルーティングベース IPsec では IPsec インターフェイスを使用して 2 点間を結びます。IPsec インターフェイスは Tunnel インターフェイスと同様に扱うことができ、通過する通信は暗号化により保護されます。

ルーティングベース IPsec で構築された IPsec トンネルでは、暗号化対象とする通信を、ルーティング設定により制御することができ、RIP や OSPF による動的経路制御も可能です。

※ SEIL/neu T1,128,2FE ver.1 系ファームウェアでは対応していません。

7.1.4 Tunnel インターフェイス + トランスポートモード IPsec

Tunnel インターフェイスによるトンネリングでは、ホスト間の通信はトンネルの始点-終点間でカプセル化され (暗号化はされず)、トンネル始点-終点間の通信としてパブリックネットワークを中継されます。このトンネル始点-終点間の通信にポリシーベース IPsec(トランスポートモード) を適用することにより、通常は保護されない Tunnel インターフェイスでの通信を IPsec により保護することができます。

また、SEIL/neu T1,128,2FE ver.1 系ファームウェアではルーティングベース IPsec(IPsec インターフェイス) に対応していないため、これらの SEIL が含まれる構成の IPsec-VPN で RIP や OSPF(マルチキャスト) を使用する場合には、Tunnel インターフェイスとトランスポートモード IPsec を組み合わせる必要があります。

7.1.5 自動鍵交換 (IKE)

SEIL は、IPsec の鍵交換を自動化する IKE 機能に対応しています。安全性の向上と保守管理を容易にするため、IPsec 使用時は IKE による鍵交換を推奨します。

SEIL は、IKE の認証は事前共有鍵 (preshared key) にも対応しています。また、鍵交換モードは Main mode 及び Aggressive mode を選択可能です。

7.1.6 暗号化トンネルのアドレスが固定割り当てでない場合

SEIL は、暗号化トンネルの始点となる自己 IP アドレスが、接続サービスの仕様により動的割当てである場合にも IPsec-VPN を構築することができます。

この場合、暗号化トンネルの始点をアドレスではなくインターフェイス名で指定し、再接続などによる IP アドレス変更に自動追従します。

また、Turbo 及び Plus ではこれに加え、暗号化トンネルの終点となる対向機器 (peer) のアドレスが動的に変わる場合にも IPsec-VPN を構築することができ、クライアントホストのローカルネットワーク情報を元にセキュリティポリシーを自動生成することも可能です。

※ 対向機器が、SEIL シリーズのように自己アドレスの動的変化に対応している必要があります。