適切な VPN ソリューションの選択

内容

概要

バーチャル プライベート ネットワーク (VPN) は、そのコストの低さと広範囲に及ぶネットワークを柔軟に展開できることから、人気が高まっています。テクノロジーの発展に伴い、VPN ソリューションを導入するためのオプションも増加しています。このテクニカル ノートでは、これらのオプションの一部を紹介し、各オプションを最も適切に利用できる状況を説明します。

はじめに

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。

前提条件

このドキュメントに関しては個別の前提条件はありません。

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。

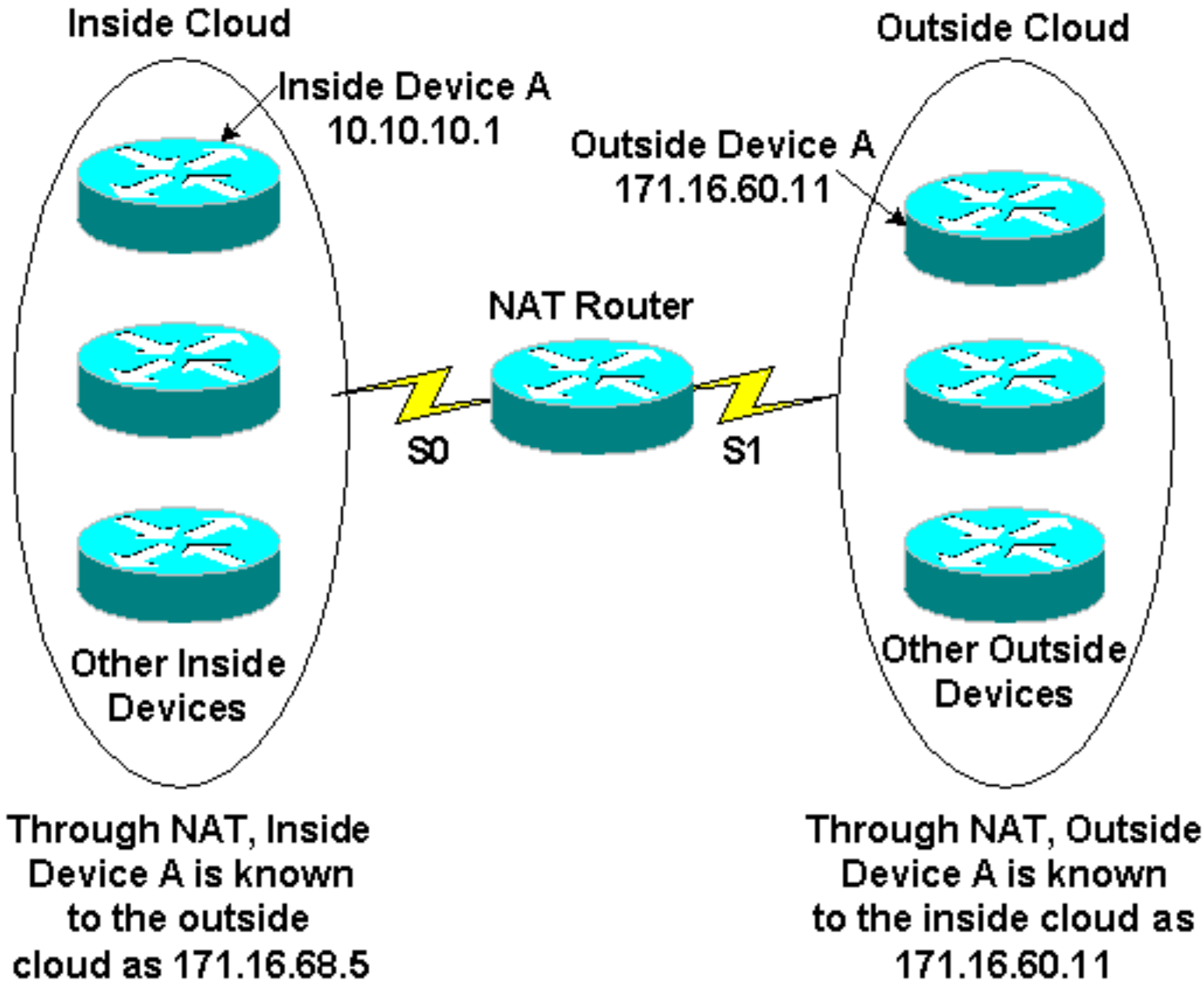
注：シスコでは、Cisco Secure PIX Firewall、Cisco VPN 3000 Concentrator、およびCisco VPN 5000コンセントレータを含む非IOSプラットフォームでも暗号化をサポートしています。

NAT

インターネットは短期間で、当初の設計者が予想していたよりも非常に大きな発展を遂げています。IP バージョン 4.0 で使用可能なアドレスの数に限りがでてきていることからも、このことが伺えます。また、それによって使用可能なアドレス スペースも少なくなってきています。この問題への 1 つの解決法が、Network Address Translation（NAT; ネットワーク アドレス変換）です。

NAT を使用することによって、ルータを内部と外部の境界で分けて設定することができます。つまり、外部（通常はインターネット）には 1 つまたは少数の登録済みのアドレスがあり、内部にはプライベート アドレッシング方式を使用することでいくつでもホストを持つことができます。アドレス変換方式の完全性を維持するために、NAT は、内部（プライベート）ネットワークと外部（パブリック）ネットワーク間の各境界ルータで設定する必要があります。セキュリティの観点から見た NAT の長所の 1 つは、プライベート ネットワーク上のシステムでは外部のネットワークから着信 IP 接続を受信しても、NAT ゲートウェイにその接続を許可する設定がされていないと受信することができないということです。さらに、NATは送信元デバイスと宛先デバイスに対して完全に透過的です。NATの推奨操作にはRFC 1918が含まれ 、これは適切なプライベートネットワークアドレッシング方式の概要です。NATの規格はRFC1631に記述されています 。

次の図は、内部変換ネットワークアドレスプールを使用したNATルータの境界定義を示しています。

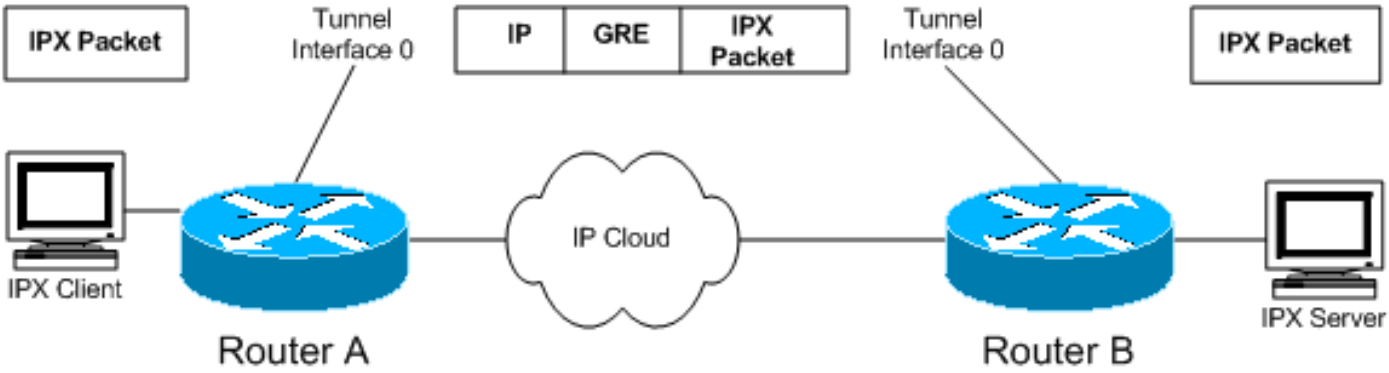


NATは一般に、インターネット上でルーティング可能なIPアドレスを節約するために使用されます。これは高価で数が限られています。NATは、インターネットから内部ネットワークを隠すことでセキュリティも提供します。

NATの動作については、「NATの動作の仕組み」を参照してください。

GREカプセル化トンネリング

Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）トンネルは共有されている WAN の全域に及ぶ特定のパスウェイを提供し、新しいパケット ヘッダーを持つトラフィックをカプセル化して指定された宛先に確実に配信します。トラフィックはエンドポイントでのみトンネルに入ることができ、もう一方のエンドポイントでのみ残すことができるため、ネットワークはプライベートです。トンネルは真の機密性（暗号化と同様）を提供しませんが、暗号化されたトラフィックを伝送できます。トンネルは、トラフィックが伝送される物理インターフェイスに設定された論理エンドポイントです。



図に示すように、GREトンネリングを使用して、非IPトラフィックをIPにカプセル化し、インターネットまたはIPネットワーク経由で送信することもできます。Internet Packet Exchange(IPX)およびAppleTalkプロトコルは、非IPトラフィックの例です。GREの設定については、「GREの設定」の「GREトンネルインターフェイスの設定」を参照してください。

IPXやAppleTalkなどのマルチプロトコルネットワークを使用し、インターネットまたはIPネットワーク経由でトラフィックを送信する必要がある場合は、GREが適切なVPNソリューションになります。また、GREカプセル化は、IPSecなどのトラフィックを保護する他の手段と組み合わせて使用されます。

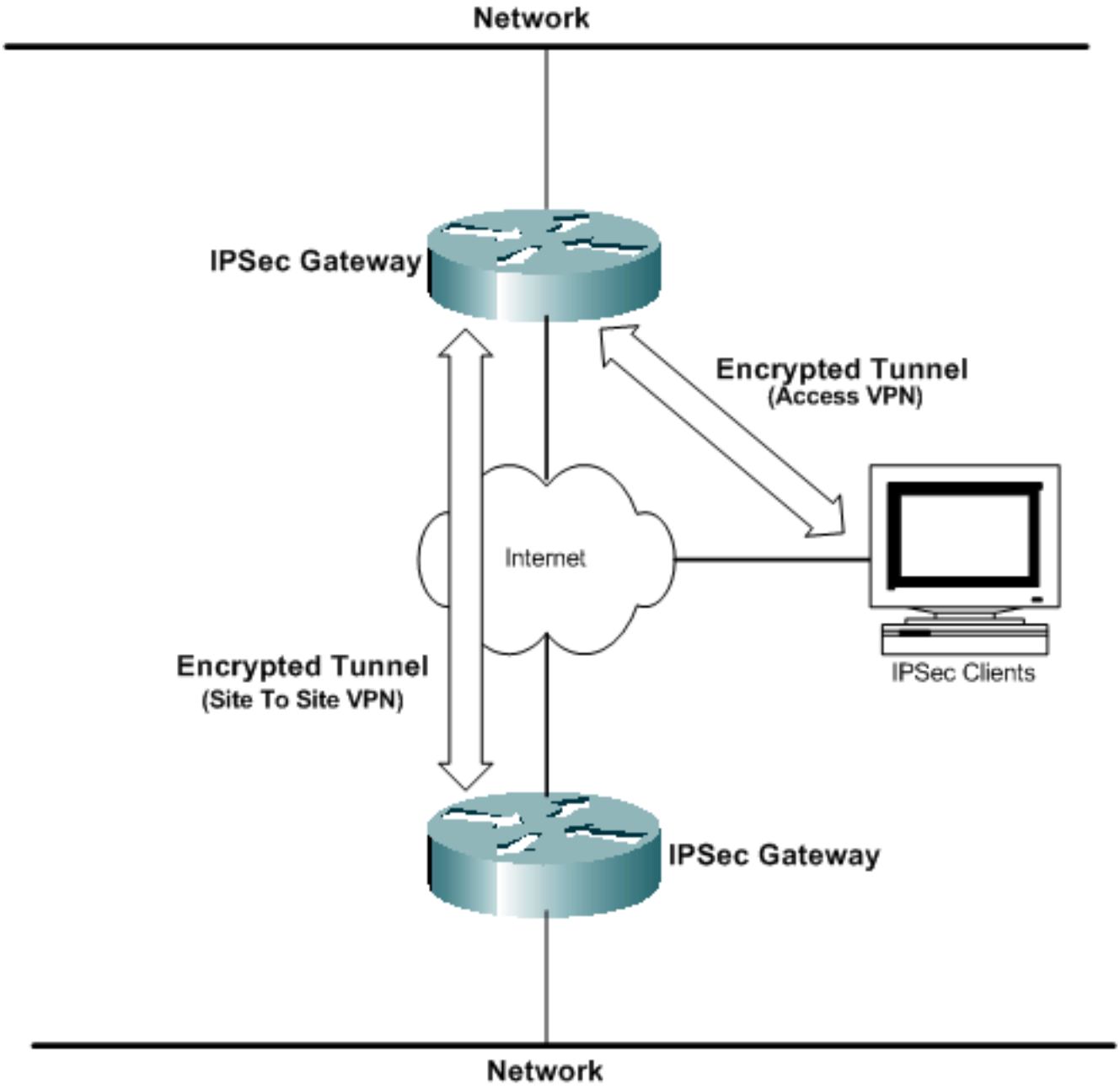
GREに関する技術的な詳細については、RFC 1701 とRFC 2784を参照してください 。

IPSec 暗号化

共有ネットワークを介して送信されるデータの暗号化は、VPNに最もよく関連するVPNテクノロジーです。シスコは UP Security (IPSec; インターネット プロトコル セキュリティ) データ暗号化方式に対応しています。IPSecは、ネットワーク層の参加ピア間でデータの機密性、データの整合性、およびデータ認証を提供するオープンスタンダードのフレームワークです。

IPSec暗号化は、Internet Engineering Task Force (IETF ; インターネット技術特別調査委員会) 標準で、IPSecクライアントソフトウェアの56ビットおよびトリプルDES(3DES)168ビット対称鍵暗号化アルゴリズムをサポートします。GRE 設定は IPSec のオプションです。IPSec は認証権限と Internet Key Exchange (IKE; インターネット キー交換) ネゴシエーションに対応しています。IPSec の暗号化は、クライアント、ルータ、ファオアウォール間のスタンドアロン環境で展開されるか、または VPN にアクセスする L2TP トンネリングとともに使用されます。IPSec は各種のオペレーティング システムのプラットフォームでサポートされています。

ネットワークに真のデータ機密性を求める場合は、IPSec暗号化が適切なVPNソリューションです。IPSecもオープンスタンダードであるため、異なるデバイス間の相互運用性を簡単に実装できます。



PPTP と MPPE

Point-to-Point Tunneling Protocol(PPTP)はMicrosoftによって開発されました。これはRFC2637で説明されています 。PPTP は Windows 9x/ME、Windows NT、Windows 2000 および WindowsXP のクライアント ソフトウェアで広く採用され、VPN を使用可能にしています。

Microsoft Point-to-Point Encryption (MPPE) は、RC4 ベースの 40-bit または 128-bit 暗号化を使用します。Microsoft からの IETF ドラフトに関する情報です。MPPE は Microsoft の PPTP クライアント ソフトウェア ソリューションの 1 つで、任意モード アクセスの VPN アーキテクチャで使用されます。PPTP および MPPE は、ほとんどのシスコのプラットフォームに対応しています。

PPTP は Cisco 7100 および 7200 プラットフォームの Cisco IOS ソフトウェア リリース 12.0.5.XE5 から対応しています。その他のプラットフォームでは Cisco IOS 12.1.5.T から対応しています。Cisco Secure PIX Firewall と Cisco VPN 3000 Concentrator も PPTP クラインアント接続に対応しています。

PPTPは非IPネットワークをサポートしているため、リモートユーザが企業ネットワークにダイヤ

ルインして異種企業ネットワークにアクセスする必要がある場合に便利です。

PPTPの設定については、「PPTPの設定」を参照してください。

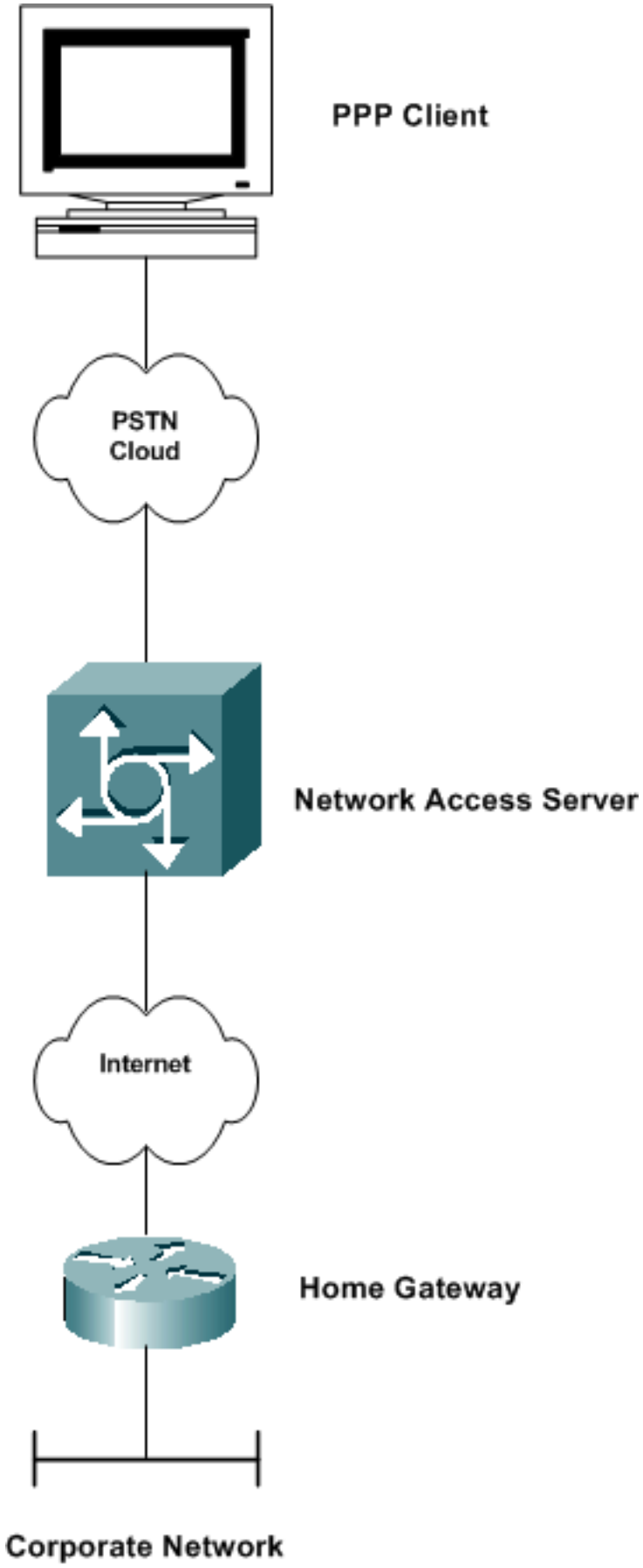
VPDN と L2TP

VPDN

シスコ標準の Virtual Private Dialup Network (VPDN; 仮想プライベート ダイヤルアップ ネットワーク) では、プライベート ネットワーク ダイヤルイン サービスでリモート アクセス サーバ全域をカバーできます。VPDN では、ダイヤルされるアクセス サーバ (AS5300 など) のことを、通常 Network Access Server (NAS; ネットワーク アクセス サーバ) と言います。 ダイヤルインユーザの宛先は、ホームゲートウェイ(HGW)と呼ばれます。

基本シナリオでは、 Point-to-Point Protocol (PPP; ポイントツーポイント プロトコル) のクライアントがローカル NAS に接続します。NAS は PPP セッションが、そのクライアントのホーム ゲートウェイ ルータに送信されると判断します。次に HGW はユーザを認証し、PPP ネゴシエーションを開始します。PPP 設定が完了すると、すべてのフレームが NAS を経由してクライアントとホーム ゲートウェイに送信されます。この方法は複数のプロトコルとコンセプトを一体化したものです。

VPDNの設定の詳細は、『セキュリティ*機能の設定』の「仮想プライベートダイヤルアップネットワー*クの設定」を参照してください。



L2TP

Layer 2 Tunneling Protocol（L2TP; レイヤ 2 トンネリング プロトコル）は IETF の規格で、PPTP と L2F の最良の特性を取り入れています。L2TP トンネルは、最初に IP と 非 IP トラフィックの強制モード（NAS から HGW へのダイヤルアップ）アクセス VPN に使用されます。

Windows 2000 と Windows XP は、VPN クライアント接続の方法としてこのプロトコルのネイティブ サポートを追加しています。

L2TPは、IPを使用して、インターネットなどのパブリックネットワーク上でPPPをトンネルするために使用されます。トンネルはレイヤ2で発生するため、上位層プロトコルはトンネルを認識しません。GREと同様に、L2TPでもレイヤ3プロトコルをカプセル化できます。UDPポート1701は、トンネルのイニシエータによってL2TPトラフィックを送信するために使用されます。

注：1996年に、シスコはVPDN接続を可能にするレイヤ2転送(L2F)プロトコルを作成しました。L2F は他の機能への対応もしていますが、L2TP に代わりつつあります。Point-to-Point Tunneling Protocol（PPTP; ポイントツーポイント トンネリング プロトコル）もまた 1996 年にインターネットのドラフトとして IETF によって作成されました。PPTP には、GRE のような PPP 接続のトンネリング プロトコル機能があります。

L2TPの詳細については、 Layer 2 Tunnel Protocolを参照してください。

PPPoE

PPP over Ethernet(PPPoE)は、主にデジタル加入者線(DSL)環境に導入される情報RFCです。PPPoE は既存のイーサネット インフラストラクチャを利用して、ユーザが同一 LAN 内で複数の PPP セッションを開始することを可能にします。この技術は、レイヤ 3 サービス セレクションを可能にします。これは、ユーザが 1 つのリモート アクセス接続を介して複数の宛先に同時に接続できるという新しいアプリケーションです。Password Authentication Protocol（PAP；パスワード認証プロトコル）またはChallenge Handshake Authentication Protocol（CHAP；チャレンジハンドシェイク認証プロトコル）を使用したPPPoEは、どのリモートルータが接続されているかを中央サイトに通知するためによく使用されます。

PPPoEは、主にサービスプロバイダーのDSL導入およびブリッジドイーサネットトポロジで使用されます。

PPPoEの設定の詳細については、「イーサネット上のPPPoEとIEEE 802.1Q VLANの設定」を参照してください。

MPLS VPN

Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）は新しい IETF 規格で Cisco Tag Switching をベースにしています。プロバイダーが費用効率良くアクセスでき、イントラネット、エクストラネット VPN サービスを提供する場合の自動プロビジョニング、迅速なロールアウト、そしてスケーラビリティ機能を可能にします。シスコはサービス プロバイダーとともに作業し、MPLS 対応の VPN サービスへのスムーズな移行を確実にします。MPLS は、ラベル ベースのパラダイムで動作し、パケットがプロバイダーのネットワークに入るときにタグ付けすることで、コネクションレス IP コアを介しての転送の効率を上げます。MPLS はルート区分を使用して VPN メンバーシップを識別し、VPN コミュニティ内にトラフィックを抑えます。

また、MPLSは、トラフィックフローではなくトポロジ情報に基づいて作成されるラベルスイッチドパスを確立することによって、IPルーティングパラダイムにコネクション型アプローチの利点を追加します。MPLS VPNは、サービスプロバイダー環境に広く導入されています。

MPLS VPNの設定の詳細は、「基本MPLS VPNの設定」を参照してください。

関連情報

- IPSec に関するサポート ページ
- バーチャル プライベート ネットワークの仕組み
- NAT に関するサポート ページ
- GREに関するサポートページ
- VPDNに関するサポートページ
- PPTP に関するサポート ページ
- PPPoEに関するサポートページ
- テクニカルサポート - Cisco Systems