バーチャル プライベート ネットワークの仕組み

内容

概要

このドキュメントでは、VPN の基本情報（VPN 基本コンポーネント、テクノロジー、トンネリング、VPN セキュリティなど）について説明します。

前提条件

要件

このドキュメントに特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。

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。

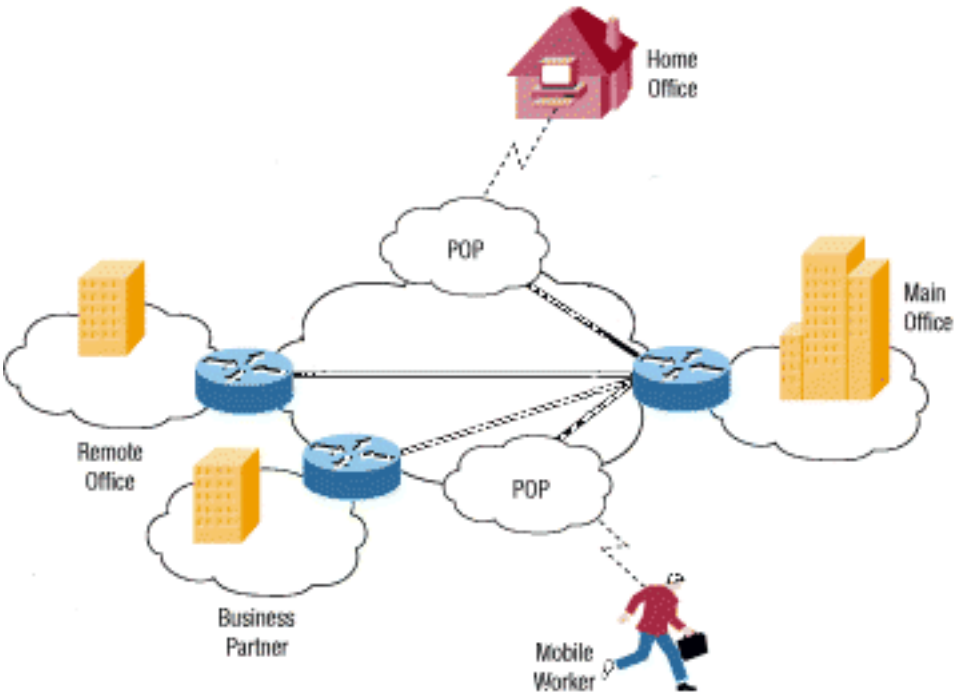
背景説明

過去 20 年間に世界は大きく変化しました。今日では、多くの企業が近隣や地域のニーズに対処するだけでなく、グローバルな市場や物流を考える必要に迫られています。多くの企業では、施設が全国に広がっており、世界中に広がっている場合もあります。しかし、すべての企業に共通して必要なことが 1 つあります。それは、オフィスがある場所がどこであれ、高速で安全で信頼

性の高い通信を維持する必要があることです。

最近まで、信頼性の高い通信とは、専用線を使用してワイドエリア ネットワーク (WAN) を維持することを意味していました。 144 Kbps の ISDN (Integrated Services Digital Network) から 155 Mbps の Optical Carrier-3 (OC3; オプティカル キャリア 3) ファイバまで、専用線が地理的に隣接する地域を越えて企業の専用線を拡張する役割を果たしてきました。WAN には、信頼性、パフォーマンス、およびセキュリティに関して、インターネットのようなパブリック ネットワークに優る明らかな利点があります。しかし、特に専用回線を使用している場合、WAN の維持にはかなりのコストがかかる可能性があります (多くの場合、オフィス間の距離が遠くなるとコストが上昇します)。 さらに、 (マーケティング スタッフの場合のように) スタッフの一部の移動が激しい組織の場合、専用線は適切なソリューションにはならず、企業ネットワークに頻繁にリモート接続して機密データにアクセスする必要が生じる可能性があります。

インターネットが普及するにつれて、企業は自社のネットワークを拡張する手段として、インターネットに注目するようになっています。まず、企業の従業員だけが使用するように設計されたサイトであるイントラネットが出現しました。今では、多くの企業が Virtual Private Network (VPN; バーチャル プライベート ネットワーク) を構築して、リモート スタッフや遠方のオフィスの必要に対応しています。



一般的な VPN の場合、会社の本社にメインのローカルエリア ネットワーク (LAN) があり、リモートのオフィスや施設に別の LAN があり、さらにフィールドから接続する個々のユーザが存在します。

VPN とは、パブリック ネットワーク (通常はインターネット) を使用してリモート サイトやユーザを一緒に接続するプライベート ネットワークのことです。専用線などの実際に回線を占有する接続を使用する代わりに、VPN では企業のプライベート ネットワークからリモートのサイトやスタッフにインターネット経由でルーティングされる「仮想」接続が使用されます。

VPN の構成要素

VPN には一般的に次の 2 つのタイプがあります。

- **リモート アクセス：Virtual Private Dial-up Network（VPDN）とも呼ばれ、社員がさまざまな遠隔地からプライベート ネットワークに接続する必要がある会社によって使用されるユーザ対 LAN の接続です。**一般に、大規模なリモートアクセス VPN を設定しようとする企業は、Internet Service Provider（ISP; インターネット サービス プロバイダー）を利用して、何らかの形態のインターネット ダイヤルアップ アカウントをユーザに提供しています。 在宅勤務者は、フリーダイヤルを使用してインターネットに接続し、VPN クライアント ソフトウェアを使用して企業ネットワークにアクセスできます。リモートアクセス VPN が必要な企業の例としては、フィールドに何百人もの営業担当者がいる大企業が考えられます。リモートアクセス VPN では、サードパーティのサービス プロバイダー経由で、企業のプライベート ネットワークとリモート ユーザの間に暗号化された安全な接続が確保されます。
- **サイト間：専用機器と大規模な暗号化を使用することで、企業はインターネットなどのパブリック ネットワークを介して複数の固定サイトを接続できます。**各サイトに必要なのは同じパブリック ネットワークへのローカル接続だけなので、長距離の専用線の費用を節約できます。サイト間 VPN は、さらにイントラネットやエクストラネットに分類できます。同じ企業のオフィス間に作成されたサイト間 VPN がイントラネット VPN と呼ばれるのに対し、企業とそのパートナーや顧客を接続するために作成された VPN はエクストラネット VPN と呼ばれます。

VPN を適切に設計すれば、企業に大きな利点があります。たとえば、次のことを実現できます。

- 接続地域の地理的な拡大
- 従来型 WAN に対する運用コストの削減
- リモートユーザの移動時間や旅費の削減
- 生産性の向上
- ネットワーク トポロジの簡素化
- グローバル ネットワーキングの実現
- 在宅勤務者サポートの実現
- 従来型 WAN よりも高い投資収益率（ROI）の実現

VPN を適切に設計するにはどのような機能が必要でしょうか。次の項目を取り入れる必要があります。

- セキュリティ
- 信頼性
- 拡張性
- ネットワーク管理
- ポリシー マネジメント

比喩：各 LAN はアイランド（IsLANd）です

大海原の 1 つの島に住んでいるところを想像してみてください。まわりには何千もの島々がありますが、近いものもあれば、遠いものもあります。通常はフェリーに乗って、自分の島から訪問先の島に渡ります。フェリーでの移動中は、ほとんどプライバシはありません。何をしていても他の人が見ている可能性があります。

それぞれの島はプライベート LAN を表しており、海はインターネットを表していると思ってください。フェリーで移動するのは、インターネット経由で Web サーバや別のデバイスに接続するのと似ています。インターネットを構成する配線やルータを制御することはできません。それは、フェリーに乗っている他の人々を制御できないのと同じです。2 つのプライベート ネットワーキングをパブリック リソースを使用して接続しようとする場合には、このことがセキュリティ上

の問題になります。

自分の島から別の島に橋を架けて、2 つの島の人々がさらに簡単で安全に直接行き来できるようにすることが決まります。その島が近くても、橋を架けて維持することには多額の費用がかかります。しかし、信頼性の高い安全な経路の必要性が非常に高いので、建設することにします。自分の島からずっと遠い 2 つ目の島にも橋を架けたいと思うのですが、費用がかかりすぎると判断します。

この状況は、専用線を使用することによく似ています。橋（専用線）は海（インターネット）とは別のものですが、島（LAN）をつなぐことができます。 リモート オフィスの接続にはセキュリティと信頼性が必要なので、多くの企業ではこのルートが選択されてきました。しかし、オフィスが非常に離れている場合は、非常に離れた距離に橋を架ける場合と同じように、実現不可能なほど費用がかかる場合があります。

では、このたとえ話の中で VPN はどこに当てはまるのでしょうか。自分の島の各住民に、次のような特性を備えた専用の小型潜水艇を支給するとします。

- 速い。
- どこへ行っても持ち運びが簡単。
- 他のボートや潜水艇から完全に隠すことができる。
- 信頼性が高い。
- 最初の 1 隻を購入したら、潜水艇を追加するための費用はほとんどかからない。

海には他の船も一緒に航海していますが、2 つの島の住民はいつでも好きなときにプライバシとセキュリティを確保して行き来できるようになります。基本的には、これが VPN の動作のしくみです。ネットワークの各リモート メンバーは、プライベート LAN に接続する媒体としてインターネットを使用しながら、安全で信頼性の高い方法で通信できます。専用線に比べて VPN では、ユーザ数と接続する場所をずっと簡単に拡張できます。実際のところ、一般的な専用線に対する VPN の主な利点はスケーラビリティです。距離に比例して費用が増加する専用線とは異なり、VPN を構築する場合には、各オフィスの地理的な場所はほとんど問題になりません。

VPN テクノロジー

適切に設計された VPN では、接続とデータのセキュリティを確保するためにいくつかの方法が利用されています。

- **データの機密性：これはおそらく VPN の実装によって提供される最も重要なサービスです。** プライベート データが転送されるので、データの機密保持は非常に重要です。データの機密保持はデータの暗号化によって実現できます。データの暗号化とは、1 台のコンピュータから別のコンピュータに送信されるすべてのデータを取得して、もう一方のコンピュータだけが復号化できる形式にデータを暗号化する処理のことです。ほとんどの VPN では、次のいずれかのプロトコルで暗号化を実現しています。**IPsec：インターネット プロトコル セキュリティ プロトコル（IPsec）は、強力な暗号化アルゴリズムやより包括的な認証などの強化されたセキュリティ機能を提供します。**IPsec には 2 つの暗号化モードがあります。トンネル モードとトランスポート モードです。トンネル モードでは各パケットのヘッダーとペイロードが暗号化されるのに対し、トランスポート モードではペイロードだけが暗号化されます。IPsec 準拠のシステムだけです。また、すべてのデバイスで共通キーか証明書を使用する必要があり、非常によく似たセキュリティ ポリシーを設定する必要があります。リモートアクセス VPN のユーザ用には、ユーザの PC 上で接続と暗号化を実現するサードパーティ ソフトウェア パッケージもあります。IPsec では、56 ビット（シングル DES）か 168 ビット（トリプル DES）のどちらかの暗号化がサポートされています。**PPTP/MPPE**:PPTPは、US

Robotics、Microsoft、3COM、Ascend、およびECI Telematicsを含むコンソーシアムである PPTP Forumによって作成されました。PPTP では、Microsoft Point-to-Point Encryption (MPPE) というプロトコルを使用する 40 ビットと 128 ビットの暗号化を装備したマルチプロトコル VPN がサポートされています。 PPTP 自身がデータの暗号化を実現しているのではないことに注意してください。**L2TP/IPsec**：一般にL2TP over IPsecと呼ばれ、レイヤ2トンネリングプロトコル(L2TP)のトンネリング上でのIPsecプロトコルのセキュリティを提供します。L2TP は、PPTP フォーラム、Cisco、Internet Engineering Task Force (IETF; インターネット技術特別調査委員会) のパートナーシップの結果として生み出された成果です。 Windows 2000 ではネイティブの IPsec と L2TP クライアントが提供されているので、主に Windows 2000 オペレーティング システムを使用したリモート アクセス VPN 用に使用されます。インターネット サービス プロバイダーがダイヤルイン ユーザに L2TP 接続を提供して、自分のアクセス ポイントとリモート オフィスのネットワーク サーバの間のトラフィックを IPsec で暗号化することもできます。

- **データの整合性：データがパブリック ネットワーク上で暗号化されていることも重要ですが、同様に、送信中に変更されなかったことを検証することも重要です。**たとえば、IPsec には、パケットの暗号化された部分またはパケットのヘッダー全体とデータ部分が改ざんされていないことを確認するメカニズムがあります。改ざんが検知されると、そのパケットは廃棄されます。データ整合性には、リモート ピアの認証が含まれる場合もあります。
- **データの発信元の認証：送信されるデータの送信元の ID を検証することは非常に重要です。**送信者 ID のスプーフィングに依存する多くの攻撃を防御するためには、必要です。
- **アンチ リプレイ：これは再生されたパケットを検出して拒否し、スプーフィングを防止する機能です。**
- **データ トンネリング/トラフィック フローの機密：トンネリングは、パケット全体を別のパケット内にカプセル化し、ネットワーク経由で送信するプロセスです。**トラフィックの発信元のデバイス ID を隠蔽することが望ましい場合には、データ トンネリングが便利です。たとえば、IPsec を使用する 1 台のデバイスがその背後にある多数のホストに属するトラフィックをカプセル化して、既存のパケットに自分独自のヘッダーを追加します。元のパケットとヘッダーを暗号化することにより (さらに、そのうえに追加されたレイヤ 3 ヘッダーに基づいてパケットをルーティングすることにより)、トンネリング デバイスはパケットの実際の送信元を事実上隠蔽します。信頼されたピアだけが、追加のヘッダーを削除して元のヘッダーを復号化した後に、本当の発信元を判別できます。RFC 2401に記さ れているとおり、コミュニケーションの外部特性の開示も、状況によっては懸念事項になる可能性があります。トラフィック フロー コンフィデンシャリティとは、発信元と宛先のアドレス、メッセージ長、または通信の頻度を隠蔽することにより、この後者の懸念に対処するサービスのことです。IPsec を使用する場合、特にセキュリティ ゲートウェイにおいてトンネル モードで ESP を使用すると、一定のレベルのトラフィック フロー コンフィデンシャリティを実現できます。」ここに一覧で示したすべての暗号化プロトコルでは、パブリック ネットワーク上に暗号化されたデータを送信する方法としてトンネリングも使用されています。トンネリング自身がデータ セキュリティを実現しているのではないことを理解しておくことは重要です。元のパケットが別のプロトコルの内部に単にカプセル化されているだけで暗号化されていなければ、パケット キャプチャ デバイスで引き続き表示可能な場合があります。ここでトンネリングについて言及されているのは、VPN が機能するために欠かせない部分であるためです。トンネリングには、3 つの異なるプロトコルが必要です。**パッセンジャー プロトコル：伝送される元のデータ (IPX、NetBeui、IP) 。カプセル化プロトコル**：元のデータにラップされるプロトコル(GRE、IPsec、L2F、PPTP、L2TP)。**キャリア プロトコル：情報が移動するネットワークによって使用されるプロトコル。**元のパケット (パッセンジャ プロトコル) はカプセル化プロトコルの中にカプセル化され、次にパブリック ネットワーク上を伝送されるためにキャリア プロトコルのヘッダー (通常は IP) 内に配置されます。カプセル化プロトコルで

もデータの暗号化が実行されることが多いことに注意してください。通常インターネット上では転送されない IPX や NetBeui などのプロトコルを、安全にセキュリティを確保して転送できます。サイト間 VPN の場合は、IPsec か Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）がカプセル化プロトコルとして使用されるのが普通です。GRE には、カプセル化されているパケットのタイプに関する情報やクライアントとサーバの間の接続に関する情報が含まれています。リモート アクセス VPN の場合は、Point-to-Point Protocol（PPP; ポイントツーポイント プロトコル）を使用してトンネリングが行われるのが普通です。 TCP/IP スタックの一部として PPP は、ホスト コンピュータとリモート システムの間のネットワークを介して通信する際には、他の IP プロトコルのキャリアとしても機能します。PPP トンネリングでは、PPTP、L2TP、Cisco の Layer 2 Forwarding（L2F; レイヤ 2 転送）のいずれかが使用されます。

- **AAA**：リモートアクセスVPN環境でより安全なアクセスを実現するために、認証、許可、アカウンティング(AAA)が使用されます。ユーザ認証を行わないと、VPN クライアント ソフトウェアが事前に設定されているラップトップや PC を操作すれば、だれでもリモート ネットワークにセキュアな接続を確立できてしまいます。ところが、ユーザ認証を行うと、接続を確立するには、有効なユーザ名とパスワードを入力する必要があります。ユーザ名とパスワードは VPN 終端デバイス自身に保存することも、Windows NT、Novell、LDAP などの他の多数のデータベースへの認証も行える外部の AAA サーバに保存することもできます。ダイヤルアップ クライアントからトンネルの確立を要求すると、VPN デバイスにユーザ名とパスワードの入力を求めるメッセージが表示されます。この情報はローカルで認証することも、外部の AAA サーバに送信することもできます。外部の AAA サーバでは、次のことが確認されます。どのユーザか（認証）何を行うことが許可されているか（許可）実際に何を行うか（アカウンティング）セキュリティ監査、課金、レポート作成に使用するためにクライアントをトラッキングする場合には、アカウンティング情報が特に役立ちます。
- **否認防止：特定のデータ転送、特に金融取引に関連するデータ転送では、否認防止が非常に望ましい機能です。**この機能は、一方の側がトランザクションへのかかわりを否認するような状況を防止するのに役立ちます。小切手を引き受ける前に銀行がサインを求めるのと同様に、否認防止機能は、送信メッセージにデジタル署名を添付することによって機能しています。これにより、送信者がトランザクションへのかかわりを否認する可能性を排除しています。

VPN ソリューションを構築するために使用できるプロトコルは多数あります。これらすべてのプロトコルでは、このドキュメントにリストしたサービスのサブセットが提供されています。どのプロトコルを選択するかは、どのサービス セットが必要かによって異なります。たとえば、ある組織では、クリア テキストでデータを送信することには何の問題も感じなくても、データの完全性を維持することは非常に重要視している場合があります。また、別の組織では、データの機密保持が絶対に欠かせないと考えている場合もあります。プロトコルの選択は、これらの組織により異なる可能性があります。使用可能なプロトコルとそれらの相対的な利点の詳細については、『適切な VPN ソリューションの選択』を参照してください。

VPN 製品

VPN のタイプ（リモートアクセスまたはサイト間）に基づいて、VPN に構築に特定のコンポーネントを配置する必要があります。必要なコンポーネントには次のようなものがあります。

- 各リモート ユーザ用のデスクトップ ソフトウェア クライアント
- Cisco VPN コンセントレータや Cisco Secure PIX Firewall などの専用ハードウェア
- ダイヤルアップ サービス用の専用 VPN サーバ
- リモート ユーザの VPN アクセス用にサービス プロバイダーが使用する Network Access

Server（NAS; ネットワーク アクセス サーバ）
- プライベート ネットワークとポリシー マネジメント センター

VPN の実装には広く受け入れられている標準が存在しないので、多くの会社が独自のターンキー ソリューションを開発してきました。たとえば、Cisco では次のようないくつかの VPN ソリューションを提供しています。

- **VPN コンセントレータ：Cisco VPN コンセントレータは、高度な暗号化と認証技術を採用し、リモートアクセスまたはサイト間 VPN を作成するために特別に構築されており、単一のデバイスが非常に多数の VPN トンネルを処理する必要がある環境に導入するのが理想です。** VPN コンセントレータは、専用設計によるリモートアクセス VPN デバイスの要件に対処できるように特別に開発されました。ハイ アベイラビリティ、ハイ パフォーマンス、スケーラビリティを実現するこのコンセントレータには、Scalable Encryption Processing（SEP）モジュールと呼ばれるコンポーネントが採用されているので、ユーザはキャパシティとスループットを簡単に増強できます。ユーザ数が 100 以下の小規模なビジネス環境から最大 10,000 もの同時リモート ユーザのサポートが必要な大規模なビジネス環境にまで適合できる、さまざまなモデルのコンセントレータが提供されています。

- **VPN 対応ルータ/VPN 最適化ルータ：Cisco IOS® ソフトウェアを実行するすべてのシスコ ルータは、IPsec VPN をサポートしています。**唯一の要件は、適切な機能セットの Cisco IOS イメージがルータで動作していることです。Cisco IOS VPN ソリューションでは、リモート アクセス、イントラネットとエクストラネットの VPN の要件が十分にサポートされています。つまり、VPN クライアント ソフトウェアが稼働するリモート ホストへの接続時にも、ルータ、PIX ファイアウォール、VPN コンセントレータなどの別の VPN デバイスへの接続時にも、Cisco ルータは同様に良好に機能します。VPN 対応ルータは、中程度の暗号化とトンネリングの要件を満たす必要がある VPN に適しており、すべての VPN サービスが Cisco IOS ソフトウェアの機能を利用して実現されています。VPN 対応ルータには、Cisco 1000、Cisco 1600、Cisco 2500、Cisco 4000、Cisco 4500、Cisco 4700 シリーズがあります。Cisco の VPN 最適化ルータでは、スケーラビリティ、ルーティング、セキュリティ、Quality of Service（QoS）が実現されています。 これらのルータは Cisco IOS ソフトウェアを基盤とするもので、中央サイトの VPN 集約経由の Small-Office/Home-Office（SOHO）のアクセスから大規模な企業ニーズまで、すべての状況に適したデバイスが提供されています。VPN 最適化ルータは、高度な暗号化とトンネリングの要件を満たす設計になっており、多くの場合、暗号化カードなどの追加ハードウェアを使用して高性能を実現しています。VPN 最適化ルータには、Cisco 800、Cisco 1700、Cisco 2600、Cisco 3600、Cisco7200、

Cisco7500 シリーズなどがあります。

- **Cisco Secure PIX Firewall**:Private Internet eXchange(PIX)ファイアウォールは、ダイナミックネットワークアドレス変換、プロキシサーバ、パケットフィルタリング、ファイアウォール、およびVPN機能を1つのハードウェアに統合します。このデバイスでは、Cisco IOS ソフトウェアを使用する代わりに、さまざまなプロトコルを処理する機能を削って IP に特化することによりオペレーティング システムを簡素化して、非常に高度なロバストネスとパフォーマンスを実現しています。Cisco ルータの場合と同様に、PIX ファイアウォールのすべてのモデルで IPsec VPN がサポートされています。VPN 機能を有効にするために必要なのは、ライセンス要件を満たしていることだけです。

- **Cisco VPN Client：シスコはハードウェアとソフトウェア両方の VPN クライアントを提供しています。**Cisco VPN Client（ソフトウェア）は、Cisco VPN 3000 シリーズ コンセントレータにバンドル提供されています。追加の費用は必要ありません。このソフトウェア クライアントは、ホスト コンピュータにインストールして、中央サイトのコンセントレータ（またはルータやファイアウォールなどの他の VPN デバイス）に安全に接続するために使用できます。 すべてのコンピュータに VPN Client ソフトウェアを導入する代わりに VPN 3002 Hardware Client を使用しても、多数のデバイスに VPN 接続機能を実現できます。

VPN ソリューションを構築するために使用するデバイスの選択は、最終的には望ましいスループットやユーザ数など多くの要因に依存する設計上の問題です。たとえば、数ユーザが使用する 1 つのリモート サイトが PIX 501 の背後にある場合は、501 の 3DES のスループット（約 3 Mbps）と VPN ピアの 5 個という最大数の制限が許容できるのであれば、既存の PIX を IPsec VPN エンドポイントとして設定できます。他方、多数の VPN トンネルの VPN エンドポイントとして機能する中央サイトでは、VPN 最適化ルータや VPN コンセントレータを採用するのが妥当と考えられます。この時点での選択は、設定しようとする VPN トンネルのタイプ（LAN 間またはリモート アクセス）と数によって異なってきます。ネットワーク設計者のすべての設計ニーズに応える高い柔軟性と ロバストなソリューションを実現するために、Cisco は VPN をサポートする広範なデバイスを提供しています。

関連情報

- VPDN について
- バーチャル プライベート ネットワーク（VPN）
- Cisco VPN 3000 シリーズ コンセントレータに関するサポート ページ
- Cisco VPN 3000 クライアントに関するサポート ページ

- IPSec ネゴシエーション/IKE プロトコルに関するサポート ページ
- PIX 500 シリーズ ファイアウォールに関するサポート ページ
- RFC 1661:The Point-to-Point Protocol (PPP)
- RFC 2661:Layer Two Tunneling Protocol "L2TP"
- How Stuff Works:バーチャル プライベート ネットワークの仕組み
- Overview of VPNs
- Tom Dunigan's VPN Page
- Virtual Private Network Consortium
- Requests for Comments (RFCs)
- テクニカルサポート - Cisco Systems