

Cisco SAFE



セキュリティのための設計提案 【イントラネット／エクストラネット編】





営業所や支店に加えてパートナー企業を接続したE-ビジネスのためのインフラストラクチャ

企業内におけるネットワークでは、本社と支店あるいは営業所などの拠点間の接続に「専用線」と呼ばれる通信事業者のサービスを利用するのが一般的です。所属する従業員の数が少ない営業所については、ダイヤルアップで本社サーバに接続するということもありました。しかし、インターネットのブロードバンド化および低価格化によって、専用線の代わりにインターネットを利用して拠点間を接続するVPN（バーチャル プライベート ネットワーク）の利用が注目されています。専用線が距離や速度によって費用が大きく変わるのに対して、プロバイダを経由してインターネットを利用するVPNは、大幅なコストの削減を可能にします。

VPNとは、専用線（プライベートネットワーク）を仮想的（バーチャル）に公衆網で実現することを意味します。インターネットというパブリックなネットワークを利用しながら専用線を使った場合と同様の機能をもったネットワークの構築を可能にします。VPNを利用すれば、地理的あるいはコスト的に専用線接続が難しかった地域にイントラネットを拡張できるようになります。さらに複数拠点との接続が集中するヘッドエンドでは、トラフィックを1つの接続に集約できるので複数の回線を管理する必要がなくなり、ヘッドエンドの帯域幅とコストの節約に加えて、それを維持するリソースの削減にもなります。

VPNによるメリットは、企業内通信（イントラネット）の費用削減だけではありません。インターネットを効率的に利用することで、新しいアプリケーションやビジネス プロセスを実装できるようになります。たとえば、パートナー企業を接続するエクストラネットにVPNを利用すれば、新しい電子商取引やサプライチェーン マネジメントのビジネス モデルが実現されます。

ただしVPN導入には、信頼性の確保が鍵になります。企業内情報を流せるだけのそのためにセキュリティ対策はもちろんのこと、高い可用性も必要です。Cisco SAFE ブループリントには、VPNに必要な機能が設計のなかに組み込まれています。

リモートアクセスVPNとサイト間VPN

外出先あるいは自宅などの社外にいるユーザが企業ネットワークにアクセスするためのVPNは、「リモートアクセスVPN」といいます。一方、支社や支店などのネットワークからインターネットを経由して本社のネットワークに接続する場合に使用されるVPNは「サイト間VPN」と呼ばれます。リモートアクセス/VPNモジュールは、リモートアクセスVPNとサイト間VPNの両方をサポートしますが、ここではサイト間VPNを中心に説明します。リモートアクセスVPNについては『リモートアクセス編』を参照してください。



IPSec トンネルによるサイト間VPNの実現

サイト間VPNは、遠隔拠点からインターネット サービスプロバイダに接続し、そこから本社ネットワーク（ヘッドエンド）にアクセスできるようにするための技術です。リモートサイトとヘッドエンドとの間には安全な接続（トンネル）が形成され、トンネル内を流れるトラフィックが途中で改ざんされたり偽装されたりすることがないことを保証します。

トンネルを実現するためには、送信側と受信側との間でデータの完全性を確認し合う仕組みが必要です。その代表が「データの暗号化」です。

暗号化のためのプロトコルは、データリンク層で動作するレイヤ2VPNと、ネットワーク層で動作するレイヤ3VPNに分類されます。PPTP（Point-to-Point Tunneling Protocol）やL2TP（Layer 2 Tunneling Protocol）といったダイヤルアップ サービスで使われるプロトコルは、レイヤ2VPNプロトコルになります。サイト間VPNには、ネットワーク層で動作するレイヤ3VPNテクノロジーが利用されます。レイヤ3VPNプロトコルには、MPLS（Multi Protocol Label Switching）やIPSec（IP Security）があります。Cisco SAFEのサイト間VPN実装では、IPSecトンネルを使用します。

MPLSについて

MPLSは、一般的にサービスプロバイダが提供するサイト間VPNサービスに使われます。つまり、サービスプロバイダのIPネットワーク上で多数の顧客に対する専用IP接続を実現します。顧客からはATMやフレームリレーと同じような専用ネットワークとして捉えることができ、サービスプロバイダにとってはレイヤ3ネットワークという拡張性と管理性を活用できます。さらに特定のプロバイダが運営するIPネットワークで動作するため、運用範囲には制限はあるもののQoS（Quality of Service）やSLA（サービスレベル契約）を保証できるというメリットがあります。

IPSecのセキュリティサービス

IPSecは、IPネットワーク上でプライベート通信を安全に行うことを目的とした、オープン標準のフレームワークです。IPSecで定義されているサービスを利用して、パブリックIPネットワーク上でのデータ通信の機密性、完全性、および真正性を保証し、VPNを実現します。その安全な通信が保証される範囲は、2台のホスト間、ホストからセキュリティゲートウェイ、または2台のセキュリティゲートウェイ間ということになります。なお、セキュリティゲートウェイとは、IPSec接続を終端し、トンネルを通してトラフィックを遠端側に通過させるデバイスのことです。

IPSecが提供するセキュリティサービスには、次の2つがあります。

- ・ 認証ヘッダ (AH)

IPパケットのIPヘッダとパケットとの間に「認証ヘッダ」と呼ばれるデータを挿入します。認証ヘッダには、送信元によって暗号化チェックサムが書き込まれます。受信側では、同様にチェックサムを計算し、認証ヘッダの内容と比較することによって、メッセージが伝送中に変更されていないことを検証します。暗号化チェックサムの方式には、128ビットの強度を持つMD5 (メッセージダイジェスト5) -HMACと160ビットの強度を持つSHA (セキュア ハッシュ アルゴリズム) -HMACの2種類があります。

- ・ ESP (カプセル化セキュリティペイロード)

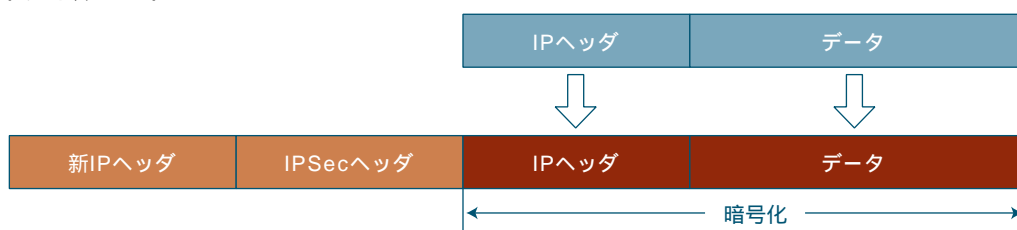
データを暗号化することによって、IPトラフィックの機密性だけでなく、認証およびリプレイ攻撃防止機能を提供します。暗号化に使用するキーには、対称暗号化 (共有キー暗号化) と非対称暗号化 (公開 / 秘密キー暗号化) がありますが、IPSecでは対称暗号化であるDES (データ暗号規格) および3DES (Triple DES) を採用しています。

VPN実装のためには、どちらかのサービスを選択して利用することも、両方のサービスを同時に使用することもできます。ただし、認証ヘッダはパケットの内容の機密性を守る機能がないため、ほとんどのIPSec VPNにはESPが使用されています。

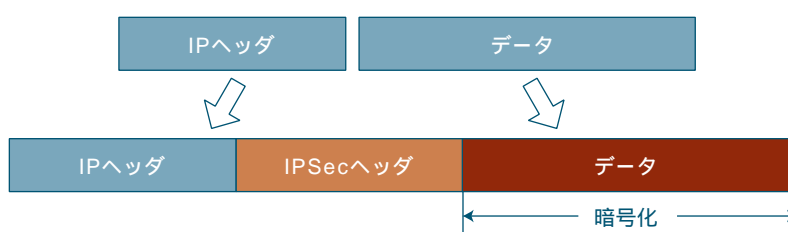
トンネルモードとトランスポートモード

IPSecは、接続の種類に応じて、トンネルモードとトランスポートモードという2つのモードのいずれかで動作します。トンネルモードでは、元のIPパケット全体が認証ヘッダあるいはESP内にカプセル化され、新しいIPヘッダがその周囲に置かれます。そのため、パケット全体が暗号化されるので、実際の送信元アドレスと宛先アドレスを隠すことができます。一方、トランスポートモードでは、認証ヘッダかESPが元のIPヘッダの後に置かれます。

トンネルモード



トランスポートモード



トンネルモードは、ルータやVPNコンセントレータなどのセキュリティゲートウェイがIPSec機能を提供する設計で使われます。トランスポートモードを利用するためには、通信を行うホストどうしがIPSecをサポートしている必要があります。

セキュリティアソシエーション

IPSecは、クライアント/サーバの関係ではなく、ピアツーピアの関係で動作します。2台のデバイスがセキュアなデータを交換するためには、使用する暗号化アルゴリズムについて合意を交わさなければなりません。ピア間のこの合意が、セキュリティアソシエーション（SA）です。

セキュリティアソシエーションでは、使用する認証および暗号化アルゴリズム、共有セッションキー、キーの有効時間、セキュリティアソシエーションの有効時間などの情報を定義します。セキュリティアソシエーションには、双方向で合意を行うIKE SAと、単方向で合意を行うIPSec SAの2種類があります。

認証

ネットワークのサービスや資源を利用するユーザを正確に識別することは、どんなネットワークのセキュリティにおいても重要な事項であり、VPNの配備を成功させるためには不可欠です。Cisco VPNソリューションは、ユーザの認証、アクセスレベルの判断、および必要な監査データやアカウントデータの保管などを行うための土台を提供するAAA（認証、権限付与、およびアカウントティング）の機能を中心に作られています。このような機能は、イントラネットおよびエクストラネットの両方のVPNアプリケーションにとって、もっとも重要な機能ということもできます。

キー管理

暗号化を使ってセキュアな通信を実現するため、キーの交換と管理がIPSecの重要な部分となります。IPSecでは、手作業とIKE（インターネットキー交換）の2つの方式でキーの交換と管理を行います。

IKEでは、キー情報を交換してSAを設定するまでには2つのフェーズがあります。IKEがメインモードおよびアグレッシブモードで動作するフェーズ1では、初期セキュアチャネルのIKE SAを設定します。フェーズ2ではIKEはクイックモードとなり、IPSec SAをネゴシエートします。





サイト間VPN設計の原則

VPNは、企業ネットワークの機能を各サイトおよびユーザに対して提供しなければなりません。しかも、インターネットというパブリックネットワークを経由しながら、従来の専用線によるWAN接続の特性をできるだけ維持することが求められます。

規模やセキュリティ要件によって異なる部分もありますが、実質的なVPN設計は共通しています。ここではネットワーク設計に関する原則について説明します。

セキュアな接続

アプリケーション、サービス、および資源へのアクセスを、ユーザの作業の邪魔にならないように制御することは、適切なネットワーク設計の要素です。アクセスコントロールリスト、ファイアウォール、コンテンツに基づいたフィルタリングツール、ウィルススキャンといったネットワークツールを使えば、ネットワークのなかを流れるデータのセキュリティを確保することができます。

またVPNサービスは共有ネットワークインフラストラクチャをまたがっているのですから、データの真正性とセキュリティの確保は大きな課題となります。そのために、トンネリングやカプセル化のテクニックを使った単純なトラフィックの分離から、暗号化による機密性の確保まで、セキュリティ要件のレベルに応じてさまざまな方法を実行しなければなりません。したがって、認証、キー管理、および暗号化などを備えたIPSecのような技術は、VPNの実現において重要な役割を果たします。

IPSecでは、データの完全性または暗号化によるセキュリティ機能を提供します。シスコでは、暗号化には3DES、データ完全性にはSHAの使用を推奨しています。3DESおよびSHAは他の方式よりもビット強度が大きいと、より安全であるといえます。ビット強度が増えてプロセッサの負担が増大したとしても、セキュリティの強化のほうが重要だと考えられます。

認証

VPNの実装では、セキュアな管理しやすい方法でデバイスを識別することが重要です。リモートデバイスを認証する際は、適切なトラフィックのみがトンネルの通過を許可されるように、ある程度のアクセス制御を配備する必要があります。デバイス認証には、事前共有キーかデジタル認証のいずれかを使用します。

事前共有キーには、ワイルドカード、グループ、およびユニークの3種類があります。ユニーク事前共有キーは特定のIPアドレスに結び付けられ、グループ事前共有キーはグループ名IDに結び付けられます。このうちグループ事前共有キーは、サイト間VPNには使用できません。またワイルドカード事前共有キーは固有の情報には関連付けられず、相手先を識別することができないため



ネットワークの全デバイスが同じキーを使用します。そのため1台のデバイスのセキュリティが侵害されてワイルドカード事前共有キーが判別されれば、すべてのデバイスが危険にさらされることになります。ユニーク事前共有キーの利用を検討することもできますが、大規模ネットワークには対応できず、キーの強度と変更頻度によっては、強固なデバイス認証が提供できなくなります。

デジタル認証では、どのデバイスも他のあらゆるデバイスに対して認証を行うことができるため、事前共有キーよりも優れた拡張性と柔軟性を提供します。デジタル証明書はIPアドレスではなく、デバイスに固有の署名付き情報に結び付けられ、全社的に適用される認証局によって検証されます。デジタル証明書を持つデバイスのセキュリティがハッカーに侵害されたりデバイスが盗まれた場合は、新しいCRL（証明書無効リスト）を全デバイスに通知して、そのデジタル証明書を無効にします。

デジタル認証は機能が複雑であるため、配備と管理に他より多くの管理リソースが必要とされます。しかし社内に認証局を置かずにサードパーティが管理する認証局を使用すれば、エクストラネットVPNの展開が容易になるという利点があります。VPNの規模が20台を超えるデバイスに成長した場合、またはデバイスが20台以下の場合でも堅牢なデバイス認証が必要とされる場合は、デジタル認証の使用を検討してください。

ネットワークアクセス制御

ネットワークへのアクセス制御は、ファイアウォールで行われるのが一般的です。VPNデバイスにも、その周辺にファイアウォールを設置すべきです。インターネットから受け取ったVPNトラフィックがキャンパスネットワークに到達する前に、アクセス制御によって適切なアドレス範囲とプロトコルのみを許可するようにします。ただしVPNアクセスポリシーの多くでは、社内ネットワークで利用可能な機能をリモートサイトに対しても許可する 경우가ほとんどです。したがって、リモートユーザに許可したいプロトコルを定義するのではなく、アクセスを禁止したいプロトコルを定義するほうが簡単でしょう。

大規模な展開では、各種VPNを別々のアクセス制御ポイントでセグメント化すると管理がしやすくなります。VPNの種類に応じて専用のファイアウォール インターフェイスを用意することになるので、異なるVPNアプリケーションに異なる信頼レベルを設定できるからです。たとえば、サイト間VPNに対しては、リモートアクセスVPNより少しだけ高い信頼レベルを設定しておきます。サイト間の場合はリモートピアのIPアドレスを知っており、デジタル認証を使用している可能性があります。リモートアクセスVPNの場合はリモートピアのアドレスを把握しておらず、グループ事前共有キーとセカンダリ認証を併用してユーザにネットワークへの入来を許可しているからです。

VPNデバイスからパブリックネットワークに向かって発信されるトラフィックのフィルタリングも重要です。このフィルタリングでは、VPNデバイスがパブリックインターフェイスに着信・発信するIPSecトラフィックのみを処理するようにします。この機能は、ファイアウォールではなく標準ACLを装備したルータで実行させることができます。

IP アドレッシング

どんな大規模IPネットワークにも共通していますが、適切なIPアドレッシングは非常に重要です。スケーラビリティ、パフォーマンス、そして管理性を維持するためには、メジャー ネットワークのサブネットをリモートサイトに割り当てます。こうすれば、暗号化ACLにはローカル ネットワークごとに1行を設定するだけで済み、ローカル ネットワーク自体が集約可能な場合は単一の設定を行うだけでよくなります。また、適切なサブネット構成によって、ヘッドエンドのルータ設定が簡素化されてスポーク ツー スポークの相互通信が可能になり、必要とされるトンネル数が減少します。

マルチプロトコル トンネリング

標準のIPSecは、IPユニキャスト トラフィックのみをサポートします。IPSecの場合、固有のIPSec SAを使って中央のネットワークから各リモート ネットワークへのトンネリング機能を提供します。マルチキャストで必要とされるリモート サイトどうしの接続を同じIPSec SAで提供することはできません。そこでマルチプロトコルやIPマルチキャスト トンネリングを利用するためには、別のトンネリング プロトコルが必要になります。

サイト間VPNの場合には、GRE（汎用ルーティング カプセル化）が最も適しているといえます。GREでは、その発信元や宛先にかかわらず、すべてのトラフィックをカプセル化します。ただしGREにはデータ暗号化やパケットの完全性保証機能がありません。単にユニキャスト以外のIPパケットをサポートするというだけです。

ネットワークアドレス変換

NAT（ネットワークアドレス変換）は、数少ないパブリックアドレスを多くのクライアントで共有する手段として使われます。このとき、プライベートアドレスを外部から隠すことができるため、セキュリティ機構の1つとして利用されることもあります。ただしVPNを利用している場合、NATがトンネル確立やトンネルを通じたトラフィックフローをブロックしてIPSec の妨げとなることがあるため、NATを適用する場所を把握しておくことが重要です。



IPSec暗号化の後でのNATの適用

IPSecトンネルのトラフィックは、IPアドレスが暗号化された状態になっています。そのため、IPSec暗号化の後にNATを適用した場合には、アドレス隠匿という意味では何の効果もありません。しかしIPアドレスを節約するためであれば、IPSecカプセル化の後にNATを適用してください。

この場合には、次のような注意点があります。

1対1のアドレス変換を利用する場合：

IPSecでパケットの完全性を提供するためにAHモードを使用している場合、1対1のアドレス変換が発生すると、シグニチャチェックサムが無効になってしまいます。シグニチャチェックサムは、IPヘッダの内容に基づいて計算されているため、IPヘッダが変更されると、パケットの伝送中に修正されたように見え、リモート側で廃棄されることとなります。ただしIPSecがESPを使用していれば、パケットの完全性を検証するためにIPヘッダが使用されないため、アドレス変換が実行されてもVPN上でパケットを問題なく送信できます。

多対1のアドレス変換を利用する場合：

多対1のアドレス変換（ポートアドレス変換）が実行される場合は、IPアドレスと送信元のIKEポート（通常はUDPポート500）が変更されます。VPNデバイスによってはUDP500以外のポートから発信されたIKE要求に対応できないため、ESPやAHを正しく扱えないことがあります。ESPやAHはIPよりも上位レイヤのプロトコルで、ポートを使用しないことに注意してください。

多くのリモートサイトで多対1のアドレス変換が使用されているため、こうしたNATの問題を克服するためにNAT透過という特殊なメカニズムが提供されています。NAT透過は、IKEおよびESPパケットを、UDPやTCPなどの別のトランスポート層プロトコルに再カプセル化します。これによって、暗号化されたトラフィックはブロックするように設定されているネットワークのアクセス制御をバイパスできます。

IPSec暗号化の前でのNATの適用

2つのサイトがIPSecを通して接続される場合、各サイトのネットワークアドレスに重複している部分があると、VPN終端デバイスがパケット転送先のサイトを判別できないためにトンネルが確立できません。IPSec暗号化の前にNATを使用すると、重複するネットワークの一方を固有のネットワークアドレス範囲に変換することで、この問題を解消できます。ただし、プロトコルのなかにはパケットのデータセグメントにIPアドレスを埋め込むものがあるため、パケットのIPヘッダだけでなくデータセグメントでもアドレス変換を実行するようしなければなりません。

フラグメンテーションとパス最大伝送ユニット検出

パケットがトンネルを通して送信される際に、カプセル化パケットが大き過ぎるためにリンクを通過できないと、フラグメンテーション（断片化）が発生します。しかしIPSecパケットについては、フラグメンテーションを避けるようにすべきです。断片化された状態のIPSecパケットは、その真正性を確認することができないからです。検証および復号化のためには、その前にパケットをリアセンブリしなければなりません。

フラグメンテーションを発生させることなくトンネルを通してパケットを送信するためのメカニズムにPMTUD（パス最大伝送ユニット検出）メカニズムがあります。これは、所定のパスに対してフラグメンテーションを起こすことなくパケットを送信するためのMTU（最大伝送ユニット）を判別します。

PMTUDをサポートするホストは、IPヘッダにDF（Don't Fragment）ビットを設定します。パケットがカプセル化される際には、元のIPヘッダから新しい外部IPヘッダにDFビットがコピーされます。パケットが宛先に向かってパスを伝送されるときに、暗号化パケットが次のリンクを通過するには大き過ぎる場合は、暗号化パケットの転送を試みているルータはICMPメッセージを送信元に送ってパケットを廃棄します。このとき送られるICMPメッセージがタイプ3であれば「宛先に到達不可能」、タイプ4であれば「DFビットが設定されているが途中でフラグメンテーションが必要」という意味になります。送信元ではICMPメッセージを受信すると、パケットが問題なくリンクを通過できるようにパケットサイズを小さくしてから再送します。

ICMPメッセージ タイプ3および4がネットワーク上で利用できなかったり、送信元のホストがPMTUDをサポートしていない場合には、IPSecカプセル化の前にフラグメンテーションが実行されるように、ローカルのVPN終端デバイスのMTU値を低く設定しておきます。このとき、カプセル化によってヘッダが追加されてパケットサイズが大きくなることに注意してください。たとえば、ESPをGREとともに使った場合で24バイト、3DESとSHAを使用した場合には56バイトが付加されます。

専用デバイスと多目的デバイス

ネットワーク設計プロセスの多くの場面で、ネットワーキングデバイスやセキュリティデバイスに統合された機能を使用するか、VPNアプライアンスの専門機能を使用するかを選択を迫られます。VPN機能をルータなどのデバイスで提供できれば、費用効果や相互運用性が高いという利点があります。しかし機能やパフォーマンス要件によっては、専用VPNアプライアンスが必要になる場合もあります。実際、IPSecは非常に要求の厳しい機能であるため、設計の規模が大きくなるほど、統合型ルータやファイアウォールではなくVPNアプライアンスが選択されます。

どちらを使用するかは、統合デバイスの機能上の利点と、アプライアンスで利用できるキャパシティや機能とを比較して決めてください。Cisco SAFEには、どちらのタイプのシステムも使用されています。

ネットワーク侵入検知システム

ネットワークIDS（侵入検知システム）テクノロジーを使用することで、セキュリティ境界を拡張することのリスクを低減できます。ネットワークIDSは、VPN設計のなかで次の2つの機能を実行します。

VPNデバイスから発信したまたはVPNデバイスに宛てられたトラフィックを分析して、リモートサイトやリモートユーザからVPNを通してやって来る攻撃を検出します。攻撃の発信元はわかっており、これがスプーフされている可能性は低いいため、ネットワークIDSはどの攻撃にも強力に対応できます。たとえば、不正なトラフィックを発見したときには、ネットワークIDSによってTCPリセットが実行されることもあります。

暗号化の後でネットワークIDSを適用することで、VPNデバイスが暗号化トラフィックのみを送受信していることを検証できます。

非VPNパケットを検出したらアラームを出すようにネットワークIDSを調整することで、暗号化パケットのみがネットワーク上を流れていることを確認できます。これによって、VPNデバイスの構成ミスを防ぎ、このデバイスを通して非暗号化トラフィックを不注意に許可してしまう可能性についても排除します。

セキュリティ監視システム

トラフィックの監視や侵入の探知は、ネットワーク侵入者に対するよい防御策となりますが、強力なセキュリティを実現するためには、できるだけ侵入しにくい状況を作ることが大切です。セキュリティ監査システムは、企業ネットワークをスキャンして、潜在的なセキュリティリスクを見つけ出します。また、包括的なネットワークセキュリティデータベースを利用することにより、セキュリティの弱点について詳しい情報を提供します。これによって、ネットワーク管理者は侵入者からネットワークをより堅固に守ることができます。

スプリットトンネリング

スプリットトンネリングは、リモートサイトのユーザが、最初にパブリックネットワーク（インターネット）へのトラフィックをトンネル内部に伝送しないように、プライベートVPNネットワークにアクセスすると同時にパブリックネットワークへのアクセスを許可することです。

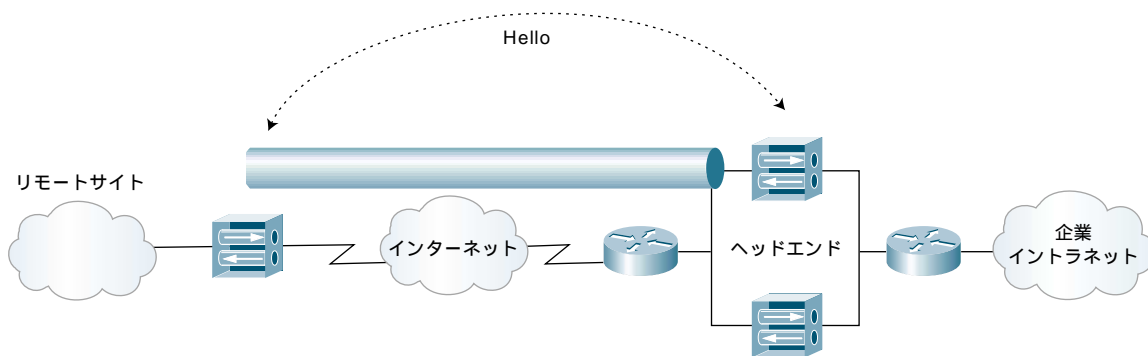
スプリットトンネリングを使用しないと、リモートサイトからインターネットへのトラフィックについても暗号化されてヘッドエンドを通過し、セキュリティゲートウェイによって復号化されてからインターネットに送出されることになります。

リモートサイトでスプリットトンネリングを利用する場合は、ステートフルファイアウォールを構内に設置して、リモートサイトへの着信と発信を許可されるトラフィックを制御するようにしてください。また各サイトのユーザのPCにはパーソナルファイアウォールを組み込んでおいてください。これは、特にモバイルパソコンに必要です。たとえば出張中にホテルの高速インターネットアクセスを使って、直接インターネットに接続することがあれば、そのPCは攻撃を受けやすくなります。

高可用性

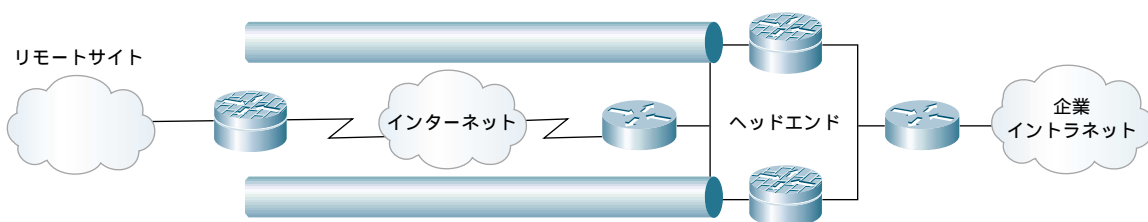
IPSecトンネルには、データを受信したというリモートサイトからの確認応答やフィードバックメカニズムがありません。そのため、リモートピアのステートを追跡する必要があります。この追跡を行わないと、デバイスがピアへの到達可能性を失ってもトンネルは確立されたままのように見えてしまいます。現在は、リモートピアの可用性とトンネル確立状態を判別するために、ルーティングプロトコルとIKEキープアライブという2つの方法を利用できます。ただしルーティングプロトコルはルータではサポートされますが、ファイアウォールやVPNコンセントレータでは利用できません。IKEキープアライブについては、どのデバイスでもサポートされています。

IKEキーブアライブは、リモートサイトのIKEピアへの到達可能性を判別するためにIKE SA上で送信されます。そして、障害が発生してピアが到達不可能になったことが分かると、接続がバックアップ デバイスに切り替わり、新しいトンネルが確立されます。ただし、その後で最初のデバイスがオンラインに復帰しても、バックアップ デバイスが使い続けられます。このメカニズムでは、それぞれのリモートサイトからヘッドエンドへのパスが1つだけであることに注意してください。



KEキーブアライブによる高可用性の実現

ルーティング プロトコルを利用する場合は、リモートサイトとヘッドエンドとの間には2つのパス（GREトンネル）が必要です。ルーティング アップデートが両方のトンネルを通過してリモートサイトに伝送され、リモートサイトは宛先ネットワークに到達可能なヘッドエンドにトラフィックを転送します。ルーティング コストを調整すれば、片方をプライマリ トンネルとして設定できるので、トンネルに障害が発生したときには、プライマリ パスが利用できないことをルーティング プロトコルが認識して、すぐにコンバージェンスが実行されます。ルーティング プロトコルを利用した場合には、障害から回復したときに元のプライマリ パスに復帰するように設定することもできます。



ルーティング プロトコルによる高可用性の実現

またコンセントレータやファイアウォールの多くでは、アクティブ/スタンバイ構成でフェールオーバー機能をサポートしています。2台のユニットを用意しておき、プライマリ デバイスが故障したときに、バックアップ デバイスがプライマリ デバイスのIPおよびMACアドレスを引継ぎ、トンネルを再確立します。ルータの場合は、アクティブ/アクティブ構成によって可用性と同時に負荷分散も提供できます。



リモートサイトの設計

リモートサイトの設計は、リモートアクセスVPNを終端する必要がないといった違いはありますが、基本的にCisco SAFEエンタープライズ モジュールと同じです。ただし、その規模や収容人数によって採用する設計オプションを変更する必要があります。また予想される負荷を考慮してVPNデバイスにはハードウェア アクセラレーションを装備したほうがよいでしょう。

またリモートサイトの場合は、VPNデバイスはたいていリモートサイトで管理されるため、暗号化ACLの設定が異なります。さらに、エッジ ルータなどのデバイスはVPN自体の外部にあるため、別の方法で管理する必要があります。この管理は、別個のトンネルやアプリケーションレベルのセキュリティ (SSH) を使って実行できます。

リモートサイトからヘッドエンドへの接続には、いくつかの方法があります。ここでは、次の4種類の方式を紹介します。

ソフトウェア アクセス方式

リモートユーザは、ソフトウェアVPNクライアントとパーソナル ファイアウォール ソフトウェアを搭載したPCを使用します。

リモートサイト ファイアウォール方式

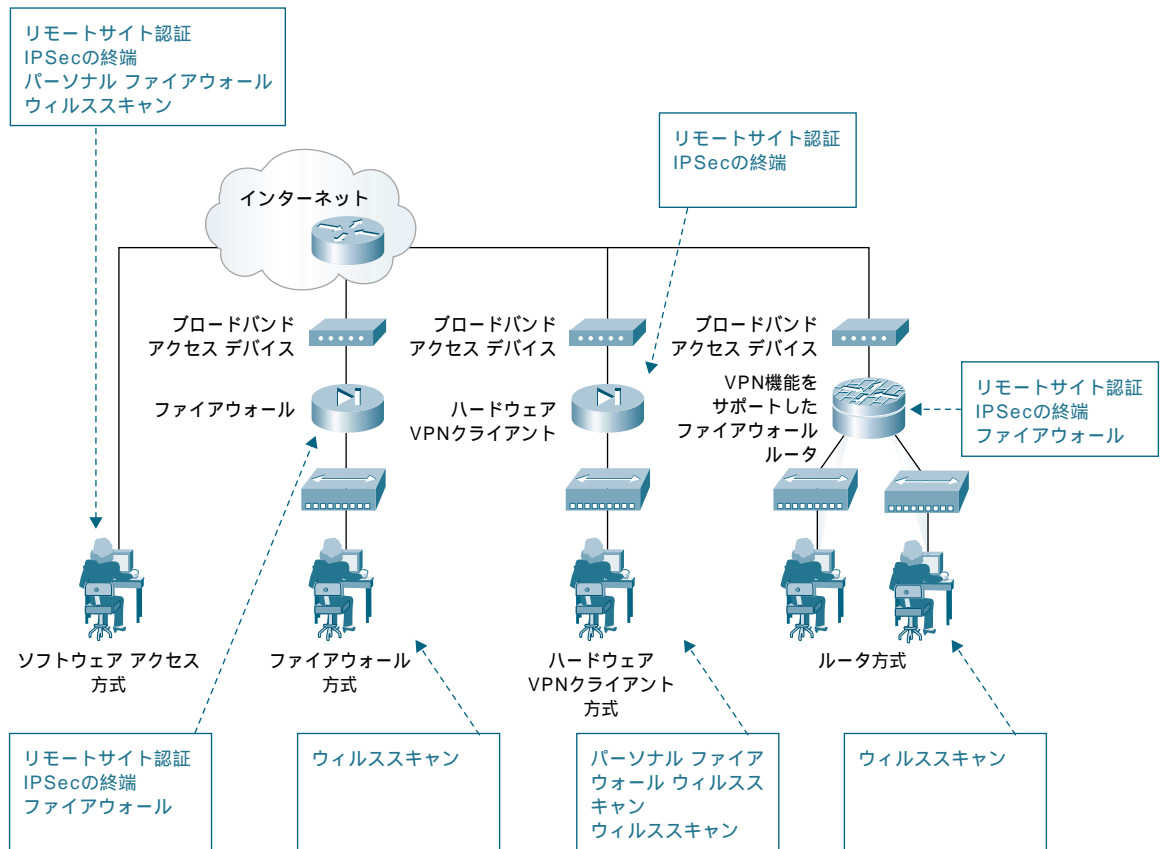
リモートサイトは、ファイアウォール機能とヘッドエンドへのIPSec VPN接続を提供する専用ファイアウォールによって保護されます。WAN接続には、サービスプロバイダが提供するブロードバンド アクセス デバイス (xDSLまたはケーブル モデム) が使われます。

ハードウェアVPNクライアント方式

リモートサイトは、ヘッドエンドへのIPSec VPN接続を提供するハードウェアVPNクライアント機能を使用します。WAN接続には、サービスプロバイダが提供するブロードバンド アクセス デバイスが使われます。

リモートサイト ルータ方式

リモートサイトは、ファイアウォール機能とヘッドエンドへのIPSec VPN接続を提供するルータを使用します。このルータが直接のブロードバンド アクセスを提供するか、サービスプロバイダが提供するブロードバンド アクセス デバイスを通してWAN接続が実現されます。



このうちソフトウェア アクセス方式は、おもにリモートアクセスVPNで使用されます。ここでは、それ以外の3種類の接続方式についての設計方針を説明します。ただし、どのサイトもCPE（顧客宅内機器）デバイスではNAT機能を実行しないと想定しています。またこれらの設計のパフォーマンスは、接続回線の種類やサービスプロバイダとの帯域幅契約によって異なります。

リモートサイト ファイアウォール方式

この接続方式は、1つのネットワークセグメントで構成されるSOHOや小規模なブランチオフィス向けです。VPNファイアウォールによってヘッドエンドへのVPN接続が確立され、NAT、ステータスフル検査、フィルタリングなどを実行します。

リモートサイト ネットワーク上の個々の PCは、出張のときなどにインターネット経由でイントラネットにアクセスしないのであれば、VPNクライアント ソフトウェアを使用する必要はありません。ただしエンタープライズクラスのファイアウォール機能が利用できると考えて、このリモートサイト構成ではスプリット トンネリングが有効化されています。したがって、スプリット トンネリングのリスクを軽減するためにウィルス スキャンング ソフトウェアを使用することが推奨されます。



管理の負担を軽減し、必要な場合はリモートサイトの相互通信を可能にするために、適切なアドレス集約を実装する必要があります。コーポレート ネットワークとインターネットへのアクセスと許可は、リモートサイト ファイアウォールとVPNヘッドエンド デバイスの両方の構成によって制御されます。リモートサイト ファイアウォールの構成とセキュリティ管理は、ファイアウォールのパブリック側から本社へのIPSecトンネルによって実行できます。この場合、リモートサイト ユーザが家庭内オフィス ファイアウォールの構成を変更する必要は一切ありません。このオプションでは、このリモートサイトの個々のユーザがコーポレート ネットワークにアクセスする場合にユーザ認証が実行されません。環境は制御されていると想定されています。環境が制御されていない場合は、ヘッドエンド ファイアウォールでユーザ認証を実行してください。

デバイス認証には事前共有キーを使用します。大規模な展開の場合は、デジタル認証が推奨されます。ヘッドエンドの可用性を判別するための高可用メカニズムとして、IKEキープアライブが使用されます。アドレスは他のどのネットワークとも重複しないと想定されているため、ローカル ネットワークを変換するためにVPN上でNATは使用されていません。

ハードウェアVPNクライアント方式

この接続方式もSOHOや小規模なブランチオフィスに使用されます。ハードウェアVPNクライアント方式には、2つの主要な利点があります。第一に、VPNソフトウェア クライアントの場合と同様に、社内ネットワークとインターネットへのアクセスと許可は、本社側から集中制御されます。VPNハードウェア クライアント デバイス自体の構成とセキュリティ管理は、中央サイトからSSL (Secure-Sockets-Layer) 接続を通して実行されます。第二の利点は、リモートサイト ネットワークの個々のPCにVPNクライアント ソフトウェアを使用する必要がないことです。ただし、企業ネットワークにアクセスするとき、個々のユーザについては認証が行われません。

動作モードには2つの種類があり、1つはNATを使用します。この場合、1つのリモートサイトの全ユーザがヘッドエンドからは1人のユーザとして見えます。もう1つのモードでは、すべてのデバイスがNATを使用しないでイントラネットにアクセスし、一度トンネルが確立された後で、イントラネット上のホストはハードウェア クライアント背後のホストへの接続を開始できるようになります。前者のほうが管理は簡単になりますが、SAFE VPNでは有用性の高い後者のモードが展開されています。

ハードウェア VPNクライアント方式の場合、デバイス認証には静的に構成されたグループ事前共有キーを使用します。大規模な展開の場合は、デジタル認証が推奨されます。ヘッドエンドの可用性を判別するための高可用メカニズムとして、IKEキープアライブまたはルーティング プロトコルを使用します。

リモートサイト ルータ方式

この接続方式は、ルータに完全な機能が装備されているため、複数セグメントで構成されるサイトにも対応可能で、QoSなどの拡張アプリケーションをサポートできます。また、VPNファイアウォールとブロードバンド アクセス デバイスの両方の機能を単一のデバイスに統合することも可能です。

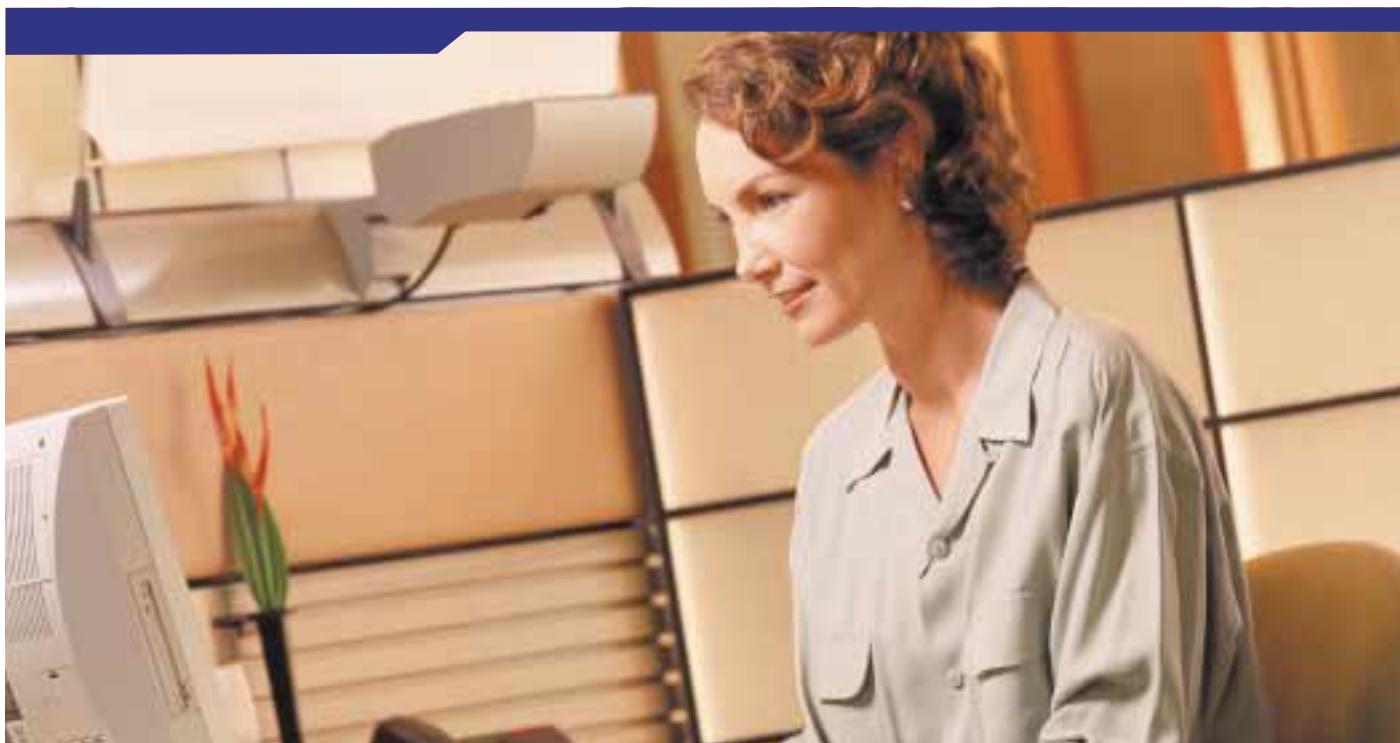
ヘッドエンドの可用性を判別するための高可用メカニズムとして、IKEキープアライブまたはルーティング プロトコルを使用します。

ネットワーク トポロジー

サイト間のネットワーク接続には、部分的メッシュ構造、フルメッシュ構造、分散型、ハブ アンド スポーク型といったネットワーク トポロジーがあります。どの場合にしても、多くの要素がネットワークのスケラビリティとパフォーマンスに影響を与えます。そのなかには、暗号化トラフィック処理を行うのか、IPSecをハードウェアとソフトウェアのどちらで実現するか、構成の複雑さ、高可用性、関連するセキュリティ機能、追跡するルーティング ピアとネットワークの数、QoSの維持などがあります。

フルメッシュ構造のネットワークでは、ネットワークの全デバイスが固有のIPSecトンネルを通してネットワークの他の全デバイスと通信しなければならないため、すぐにスケラビリティの限界に達してしまいます。部分的メッシュ構造のネットワークでは、必要な場合のみスポーク間接続が確立されるため、フルメッシュ構造のネットワークより優れた拡張性を備えています。ただしフルメッシュ構造ネットワークのデバイスと同様に、無理のないCPU使用率でデバイスがサポートできるトンネルの数に限界があります。どちらの場合も、動的トンネル エンドポイント検出メカニズムを利用することでスケラビリティを改善できます。

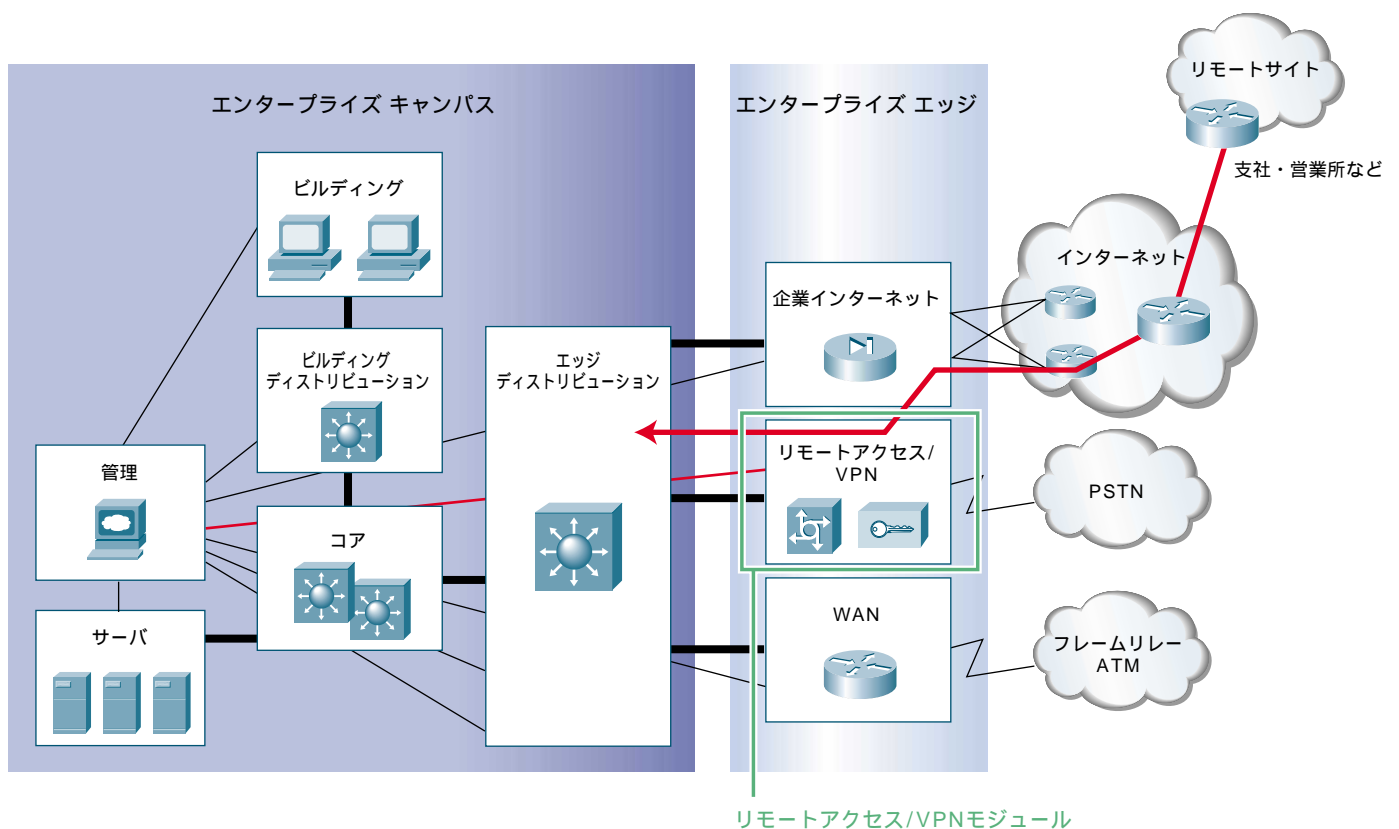
ハブ アンド スポーク型の場合は、接続するサイトが多くなったときにハブとして機能するヘッドエンドの増強が可能なため、より優れた拡張性を提供します。ただし、ヘッドエンドにはリモート サイト間の通信も含めてすべてのトラフィックが通過するため、かなりの帯域幅が必要となります。またヘッドエンドで 사용되는デバイスによっては、リモートサイトでスプリット トンネリングが必要とされる場合もあります。





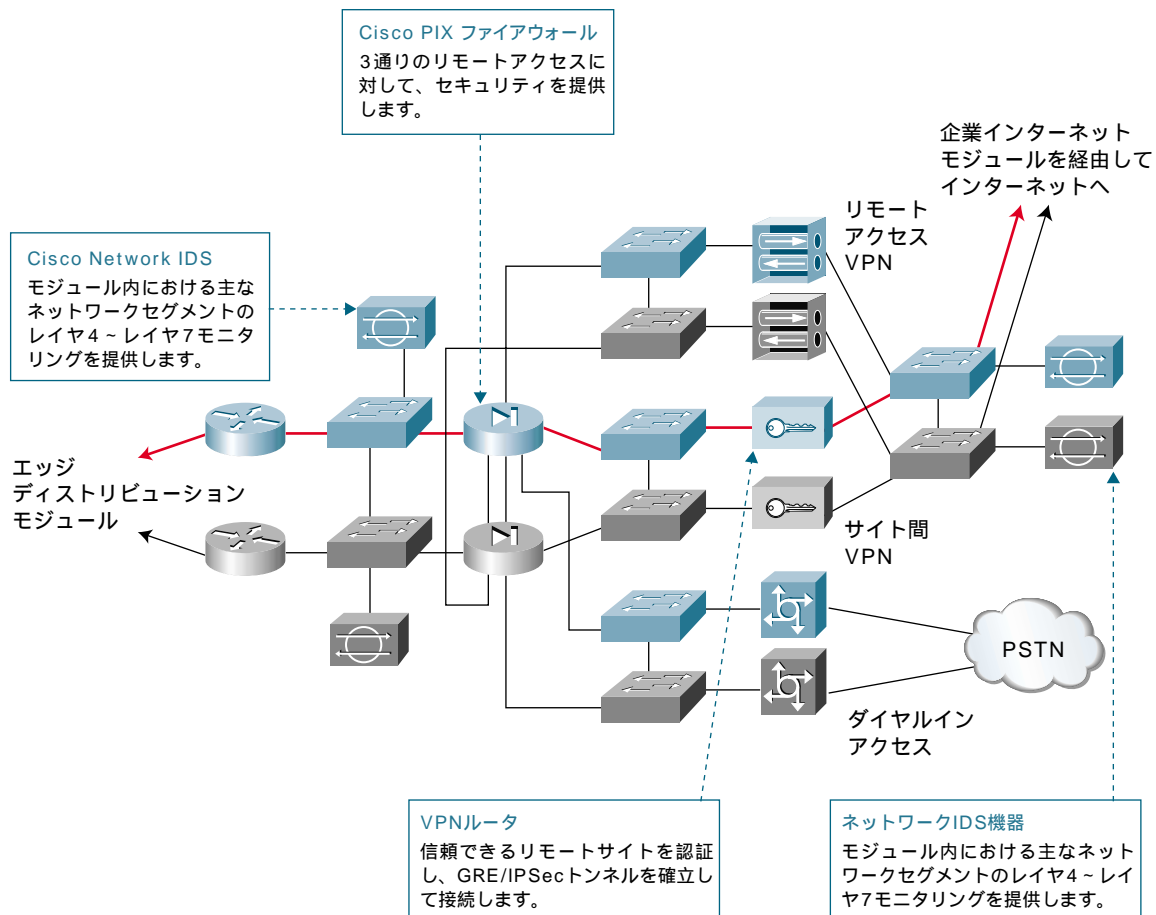
ヘッドエンドの設計

Cisco SAFEのエンタープライズネットワーク設計には、すでにVPNの機能が考慮されています。VPNに関する設計は、おもにリモートアクセス/VPNモジュールに組み込まれており、サイト間VPNとリモートアクセスVPNの両方をサポートします。ここでは、エンタープライズネットワークのリモートアクセス/VPNモジュールをさらに発展させて、高速で可用性の高いVPN終端を提供するように再設計しています。



リモートアクセス/VPNモジュールでは、リモートユーザからのVPNトラフィック、リモートサイトからのVPNトラフィック、および従来のダイヤルインユーザを終端します。リモートサイトからのVPNトラフィックは、VPNルータかVPNファイアウォールによって終端することになります。

VPNには高速性が必要とされるため、用途別の専用デバイスがモジュール全体を通して配備され、それぞれが異なる機能を提供します。



VPNにはハブ アンド スポーク トポロジーが使用されます。サイト間VPNトラフィックは企業インターネット モジュールのアクセス ルータから転送されますが、まず出力側ポイントでフィルタに掛けられ、リモートアクセスVPNセグメントに対応する特定のIPアドレスとプロトコルがフィルタを通過します。通過するプロトコルには、IKEとESPがあげられます。宛先IPアドレスはヘッドエンド端末デバイスのパブリック インターフェイスのIPアドレスに制限され、発信元アドレスはリモートサイトの既知の静的IPアドレスに制限されます。

発信元アドレスのフィルタリングによってセキュリティが強化されますが、サポートしているリモートサイトのアドレスが動的に割り当てられるようになっているとIPアドレスによるフィルタリングを実行できません。

VPNデバイスは、トンネリング終端用にIPSec、およびオプションでGREをサポートするように構成されています。このサイズ的设计では、リモートサイトはファイアウォール機能を装備する必要があります。ファイアウォール機能を装備しない場合、すべてのトラフィックがハブサイトにルーティングされることになり、ネットワークのパフォーマンスおよびスケーラビリティ要件を満たすことが難しくなります。

認証

サイト間VPN接続では、デジタル認証とIPSecピアのIPアドレスを使って強力でスケーラブルなデバイス認証を提供します。また小規模なVPNでサイト数が10未満であれば、事前共有キーを利用しても管理に大きな負担を与えません。

セキュリティ

イントラネットへのアクセスがかなり頻繁に実行されることを考えて、このモジュールではハイレベルのセキュリティが実現されています。VPNコンセントレータは、パブリックインターフェイスでESP、IKE、およびUDPポート10,000のみを許可します。

またトラフィックがリモートアクセス/VPNモジュールに伝送される前に実行されるフィルタリングにより、次の2種類のトラフィックのみが許可され、これ以外のフローがあると、IDSセンサーは重大度の高いアラームを起動します。

静的に既知のIPアドレスが指定されたりリモートサイトからVPNファイアウォールのパブリックIPアドレスに宛てられたESPとIKE

静的に既知のIPアドレスが指定されたりリモートサイトからVPNルータのパブリックIPアドレスに宛てられたESPとIKE

復号化の後で、VPNから発信された全トラフィックはただちに内部ファイアウォールに転送され、ここでフィルタにかけられてステートフルに検査されます。トラフィックが内部ルータに転送されている間、そのセグメントのIDSはレイヤ4~7の詳細なトラフィック分析を実行します。IDSが攻撃を検出した場合、ファイアウォールでこのフローを排除します。

スケーラビリティ

この設計では、VPNデバイス周囲のインフラストラクチャは高速要件に対応できるように設計されているため、WAN回線が制限要因になることはありません。あらゆる大規模VPN設計と同様に、使用されている高可用メカニズムを考えると、もっとも大きな制限要因は終端できるリモートサイトの数になります。リモートサイトが必要とする帯域幅にも依存しますが、この設計では100~250のリモートサイトトンネルをサポートできます。

セキュアな管理

すべてのデバイスの管理は、SSH、SNMP、TFTP、syslogなど、セキュアなプロトコルとセキュアでないプロトコルを併用して行われています。このモジュールでは、すべての管理はOOB(アウトオブバンド)管理ネットワークを通して実行されます。

NAT

サイト間VPN通信の場合はNATをバイパスします。この設計ではIPアドレスがイントラネット全体で重複しないようにしているので、信頼できるすべての参加者は実際のIPアドレスを使って通信できます。ただし、スプリットトンネリングが無効になっているため、インターネットにアクセスするときには企業インターネットモジュールでリモートアクセスクライアントのプライベートアドレスをアドレス変換しています。

ルーティング

エッジディストリビューションは、どのサブネットがリモートユーザによって使用されるかを認識しています。エッジディストリビューションルータは、デフォルトネットワークを使って、リモートアクセス/VPNモジュールにおけるこれらのサブネットへの到達可能性を判別します。使用されるデフォルトネットワークは、内部ファイアウォールとIDSセグメントです。エッジディストリビューションルータはその2つの内部ルータのアドバタイズメントを通して、VPNモジュールの可用性を追跡します。そして内部ルータは、動的なルーティングアップデートによってイントラネットの到達可能性を追跡し、リモートサイトに宛てられた全トラフィックをファイアウォールに静的にルーティングします。

ファイアウォールはリモートアクセストラフィックをVPNコンセントレータセグメントに静的にルーティングし、リモートサイトトラフィックをディストリビューションルータのHSRP仮想アドレスに静的にルーティングします。ディストリビューションルータはVPNルータと同じルーティングプロトコルを実行し、リモートサイトネットワークの可用性に関する更新情報を受信します。またリモートサイトがイントラネットに到達できるように、ヘッドエンドへの静的ルートを再配布するようにルーティングテーブルに登録します。これを行わないと、ルーティングプロトコルはファイアウォールを通過しないため、リモートサイトからイントラネットに到達できなくなってしまいます。

パフォーマンス

スプリット トンネリングを使用しない高速 xDSL/ケーブル ユーザが大量のデータを使用する可能性があります。VPNコンセントレータでは、デバイス上のユーザ数を制限することが可能ですが、各ユーザのスループットは制限できません。

多数のリモートサイトが存在するため、低遅延な高速ハードウェアアクセラレーションを導入する必要があります。ネットワークの帯域要件を考えると、OC-3 (155Mbps) 以上の高速 WAN リンクが必要です。ただしリモートサイトはスプリット トンネリングを有効にして、ヘッドエンドの帯域要件を軽減することができます。

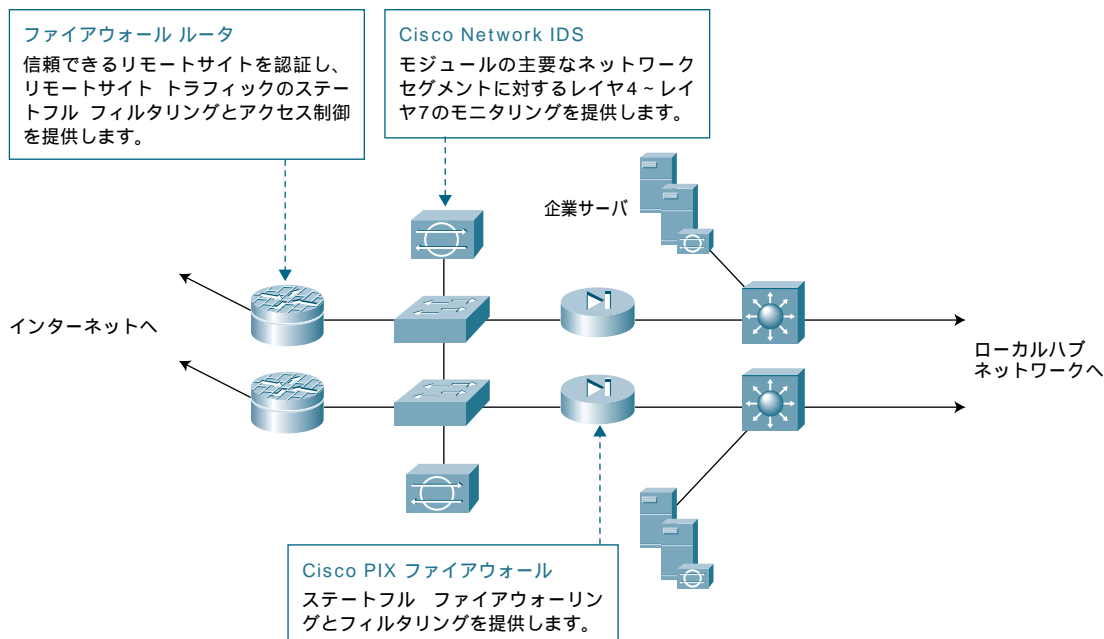
VPNファイアウォールソリューションを使用している場合は、VPNファイアウォールでアクセス制御を有効にし、ディストリビューションレイヤルータと内部ファイアウォール接続をすべて排除することを検討してください。パーソナルファイアウォールソフトウェアを配備していれば、リモートアクセスクライアントのスプリットトンネリングを有効にしてヘッドエンドのパフォーマンス要件を低減することができます。





分散ハブのための追加モジュール

分散ハブ モジュールはサイト間VPNをセキュアに終端し、VPN対応の小規模スポーク サイトと大規模エンタープライズのリモートアクセスおよびVPNモジュール ヘッドエンド間に中間レイヤを提供します。このレイヤにより、ローカルの小規模スポーク サイトはエンタープライズのハブサイトにトラフィックを送信しないで相互通信することが可能となります。



分散VPNモジュール

VPNルータは、リモートサイトとエンタープライズ ヘッドエンドからのトラフィックを終端します。ほとんどのトラフィックはスポーク ツー スポークのトラフィックです。ファイアウォールは、リモートサイトとローカル サービス間の全トラフィックに対してステートフル ファイアウォーリングとフィルタリングを提供します。リモートサイトとローカル サービスのセキュリティが侵害された場合には、ネットワーク IDSによって攻撃シグニチャが検出されるようになっています。

このモジュールには、次のような状況が発生することがあります。

- 分散ハブに対するスポークの高可用性が必要とされる
- ヘッドエンド ハブに対するディストリビューション レイヤの高可用性が必要とされる
- 複数の分散ハブが存在する可能性があり、ヘッドエンド経由での相互通信が必要とされる
- 分散ハブ経由でスポーク ツー スポーク相互通信が必要とされる

このような理由から、リモートサイト間でパケットをルーティングするために、ヘッドエンドおよび分散ハブ サイトでVPNルータが必要とされます。スポークには任意のVPNデバイスを使用できますが、VPNルータ スポークの場合はルーティング プロトコルを使って高可用性を提供している場合のみ高可用性を維持できます。また分散ルータは2つのHSRPグループを使ってリンクステータスを追跡します。

リモートVPNデバイスは、高可用性を保証されたVPNデバイスです。スポークと階層型ローカルネットワークには、イントラネット内で集約可能なサブネットを使用してください。階層型サイトではスプリット トンネリングは必要とされません。なぜなら、ヘッドエンドとスポーク サイトの両方がこの機能を備えていると想定されているからです。リモートにスプリット トンネリングの機能がないと、ヘッドエンドと階層型サイトで必要なパフォーマンスとスケーラビリティが増大することに注意してください。

このモジュールには、ディストリビューション レイヤに2台のVPNルータが装備されています。任意のレイヤでネットワーク負荷要件を満たすために3台以上のデバイスが必要とされる場合は、障害時の負荷分散機能を展開してください。

認証

サイト間VPN接続に対しては、デジタル認証を使って強力なスケラブルなデバイス認証が提供されます。

セキュリティ

スポークからスポークに、またはスポークからヘッドエンドにトラフィックが伝送される際、IDSやファイアウォール機能は実行されないことに注意してください。ファイアウォールおよびIDS機能はヘッドエンドに存在するため、この機能を2回実行する必要はありません。ステートフル ファイアウォール機能とフィルタリングは、いずれかのリモートサイトがローカル サービスにアクセスする際に実行されます。VPNルータのパブリック インターフェイスで着信したトラフィックをフィルタリングすることで、静的に既知のIPアドレスが指定されたりリモートサイトやヘッドエンドからのESPとIKEのみを許可します。

スケーラビリティ

このモジュールは、大規模エンタープライズのハブ アンド スポーク ネットワークのスケーラビリティを向上させるように設計されています。このディストリビューション レイヤは、最大200以上のリモートサイトに拡張できます。

セキュアな管理

すべてのデバイスのセキュアな管理は、SSH、SNMP、TFTP、syslog など、セキュアなプロトコルとセキュアでないプロトコルを併用して実行されます。このモジュールでは、すべての管理はヘッドエンドの管理モジュールへのインバンドVPNトンネルを通して実行されます。

NAT

処理されるアドレッシングはすべてVPN専用で、VPNトラフィック以外のインターネット アクセスは許可されていないため、このモジュールではNATは使用されていません。

ルーティング

VPNルータには、インターネットへのデフォルト ルートが設定されています。このルートには、すべてのパブリックIKEピアとリモートおよびヘッドエンドサイトの私設ネットワークが含まれます。ローカル ネットワークのみが、ファイアウォール ペアに静的にルーティングされます。ローカルの階層型ファイアウォールは、リモートサイト トラフィックの半分をそれぞれの仮想HSRP アドレスに転送します。ヘッドエンドに宛てられたトラフィックはHSRPグループに転送され、IPアドレスに基づいてロードバランスが実行されます。

パフォーマンス

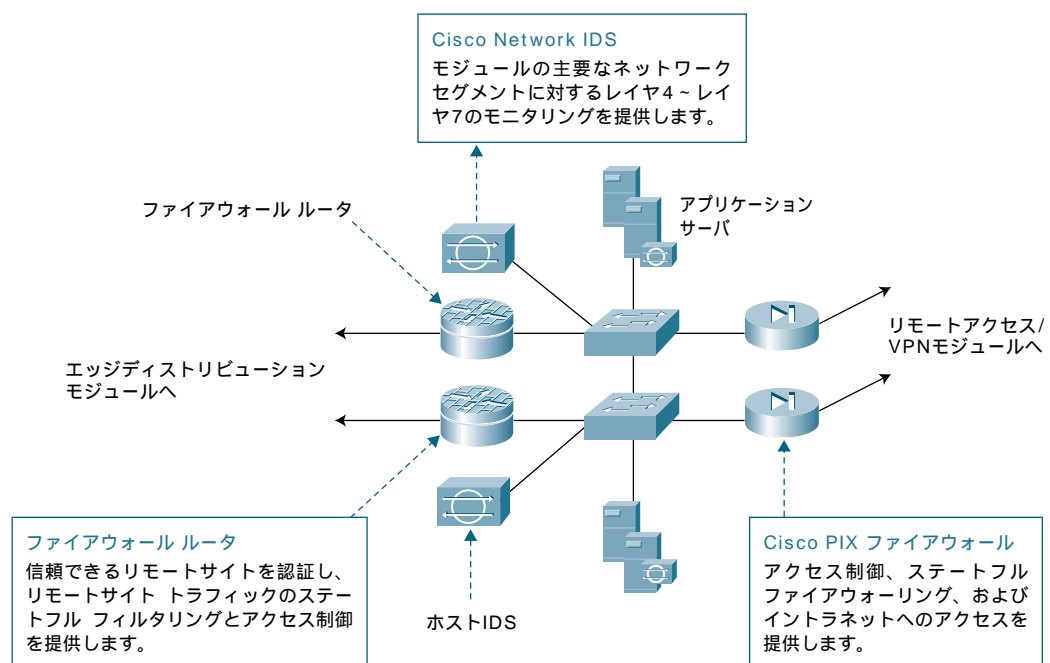
非常に多くのスポークがあり、スポーク ツー スポーク相互通信が必要とされることから、VPN デバイスには低遅延でハイレベルのパフォーマンスが必要とされます。これらのデバイスの帯域幅キャパシティとリモートサイトの数を考えると、DS3 (45 Mbps) 以上の高速WANリンクが必要です。





エクストラネットのための追加モジュール

エクストラネット モジュールは、ビジネス パートナーによるアプリケーション サーバへのアクセスを可能にし、サイト間およびリモートアクセスベースのエクストラネットをセキュアに終端するように設計されます。



この設計では、冗長VPNファイアウォールがVPN終端、フィルタリング、およびステートフルファイアウォール機能を提供します。データの機密度、そしてデータにアクセスするユーザが社外の人間だということを考慮して、ネットワークIDSとホストIDSの両方を配備しています。

このモジュールは、基幹アプリケーションのためにサイト間VPNとリモートアクセスVPNを非常に高可用性かつセキュアに終端させる必要があります。VPNファイアウォールで終端するリモートサイト デバイスはエンタープライズの管理下にはなく、時としてユーザ認証なしで、イントラネットからアプリケーション サーバへのアクセスが許可されるため、高度なセキュリティが必要です。



認証

ビジネス パートナーの接続に対して、ピア デバイスのIDを検証するためにデジタル認証が使用されます。サードパーティのデジタル認証が企業とビジネス パートナーの間の媒介者として機能して、より強力でスケーラブルなデバイス認証を提供します。サイト間VPNを通して接続するユーザに対しては、ユーザ認証は実行されません。したがって、アプリケーション サーバ上に堅牢なアプリケーションレベルのセキュリティを配備することが推奨されます。リモートアクセスVPN接続では、デバイスのグループ事前共有キーをワンタイム パスワードによるセカンダリ ユーザ認証と併用した、2つの部分から成る認証方式を使用します。ここではワンタイム パスワードが使用されていますが、リモートユーザの数によっては、関連コストが高くなってしまいます。静的ユーザ名とパスワードの組み合わせを展開するのは推奨されませんが、これらを使用する場合はパスワードに期限を設定してください。

セキュリティ

パートナーという外部ユーザからのアクセスが必要とされるため、このモジュールにはハイレベルのセキュリティを配備します。ただしリモートのIPアドレスが静的でない場合、発信元IPアドレスをベースとするフィルタリングは実行できません。

VPNファイアウォールでは、IKEおよびESPトラフィックのみがパブリック インターフェイスで終端されるようにします。VPNファイアウォールには厳しい着信ACLを実装して、VPNファイアウォールがローカルの内部サブネット宛てのVPNトラフィックのみを終端するようにしてください。

VPNファイアウォールでイントラネットへのルートを構成しないと、ローカルに接続されたネットワークかOOB管理ネットワーク以外のパケットは転送されないようになります。外部からのパケットは、アプリケーション サーバ経由でのみイントラネットに入ることができます。内部ファイアウォール ルータはアクセス制御を使って、アプリケーション サーバのIPアドレスとそれらが使用を許可されたサービスのみ、イントラネットへの通過を許可します。アプリケーションサーバはホストIDSを使ってローカルの攻撃を緩和し、セキュリティの侵害やハッカーによるイントラネット アクセスから保護します。



スケーラビリティとパフォーマンス

このモジュールは、エクストラネットの使用度が中程度から高い環境向けに設計されており、ハードウェア アクセラレーションによって低遅延な高速 VPN が提供されています。このエクストラネット モジュールは、200 以上のリモートサイトと 500 人以上のリモート同時接続ユーザをサポートします。より多くのサイトやユーザをサポートする必要がある場合は、VPN デバイスを追加してください。VPN デバイスを追加する場合は、ルーティング レイヤでアプリケーション サーバへのデフォルト ルートを提供する必要があります。デバイスはエクストラネット アプリケーションのみをサポートするため、ハイパフォーマンスが期待できます。

セキュアな管理

SSH、SNMP、TFTP、syslog など、セキュアなプロトコルとセキュアでないプロトコルを併用することで、すべてのデバイスに対するセキュアな管理が提供されます。このモジュールでは、すべての管理は OOB 管理ネットワークを通して実行されます。

NAT

接続するリモートサイトのアドレス スペースがアプリケーション サーバのアドレス スペースと重複している場合のみ、VPN ファイアウォールで NAT を使用してください。

ルーティング

ファイアウォール ルータはダイナミック ルーティング プロトコルを使って、アプリケーション ネットワークをエッジディストリビューションルータにアドバタイズします。VPN ファイアウォールには、内部ネットワークに対するルートを設定しないようにしてください。





設計目標

SAFE VPNはVPNの実装ガイドではありますが、VPNを提供するための包括的な設計ではありません。ネットワーク設計者がVPNのためのセキュリティと接続性の要件を満たすために企業ネットワークをどのように設計して実装していくかを検討できるようにするためのテンプレートです。

既存のネットワークをVPNに移行する際には、リモートサイトの数、使用するアプリケーション、パフォーマンス、信頼性要件を確認しておきます。次に、これらの要件をセキュアかつスケーラブルにサポートするネットワークを設計します。そのときの目標となる項目には、次のようなものがあります。

安全な接続

信頼性、パフォーマンス、スケーラビリティ

高可用性

ユーザおよびデバイスの認証

セキュリティ管理

攻撃の緩和

ネットワーク設計者は、VPN特有のセキュリティの考慮点とVPNの展開に関する基本的な推奨事項を理解したうえで、どのように既存のネットワークインフラストラクチャに適用していくかを検討してください。

© 2002 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、およびCiscoロゴは米国およびその他の国におけるCisco Systems, Inc.の商標または登録商標です。その他、記載されている会社名、製品名は各社の商標、登録商標または登録サービスマークです。この資料に記載された仕様は予告なく変更する場合があります。



シスコシステムズ株式会社

URL:<http://www.cisco.com/jp/>

問合せ URL:<http://www.cisco.com/jp/service/contactcenter/>

〒107-0052 東京都港区赤坂2-14-27 国際新赤坂ビル東館

TEL:03-6655-4433

電話でのお問合せは、以下の時間帯で受付けております。

平日 10:00 ~ 12:00 および 13:00 ~ 17:00

お問い合わせ先