

Secure MPLS-Based VPNs

MPLS VPN : MPLSベースのVPNの安全性

MPLSベースのVPNがフレームリレーやATMに劣らないセキュリティを提供する。

マイケル・ベリンジャー(Michael Behringer)とステファン・ワン(Stephen Wong)による報告

MPLS(Multiprotocol Label Switching)を基盤としたマネージドVPN(Virtual Private Network)によるさまざまなサービス面のメリットやコスト削減の可能性に魅力を感じている企業は多い。さらに、MPLSはフレームリレーやATM技術に劣らない高いレベルのセキュリティをもたらしてくれる。シスコの推奨のもとにCisco Powered Network契約を結んだサービスプロバイダが構築するMPLSネットワークにおいては、サービス拒否攻撃(DOS : Denial-Of-Service)やスプーフィングなどの対策を最適に設計することでネットワークへの主だった攻撃を困難、または不可能とする。

しかし、MPLSテクノロジーのセキュリティに関して一般的に間違った理解がされていることも少なくない。なかでも問題なのは「 IPベースのMPLSは本質的に安全ではない」というものだ。実際にはMPLSプロトコルはルートの分離、データの分離、パケットフィルタリング、およびネットワーク分離のメカニズムなどの多様な機能を実装しており、純粋なIPベースのネットワークのセキュリティ面を補完し強化している。

2番目の一般的な誤解は「 サービスプロバイダの顧客は、他者のVPNに侵入できる」というものだ。MPLS VPNは互いに完全に隔離されているので、そんなこと

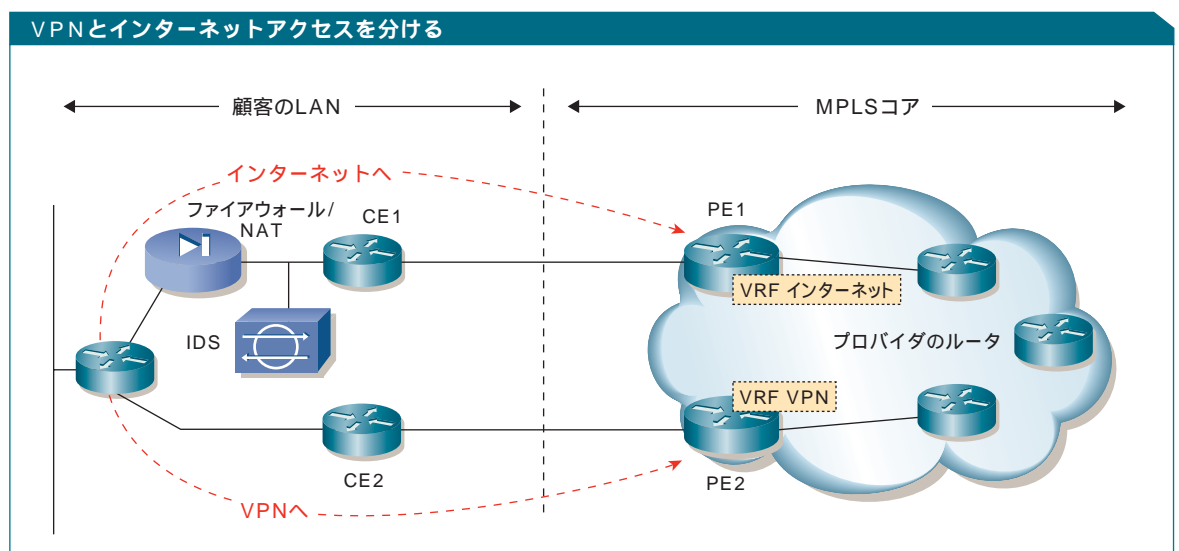


図1 : VPNでDoS攻撃を阻止するセキュリティを最大限に提供するためには、企業はフレームリレーやATMが個別のインフラアクセスを構築するように、プロバイダエッジへのVPNとインターネットアクセスを別々に割り当てることも可能である

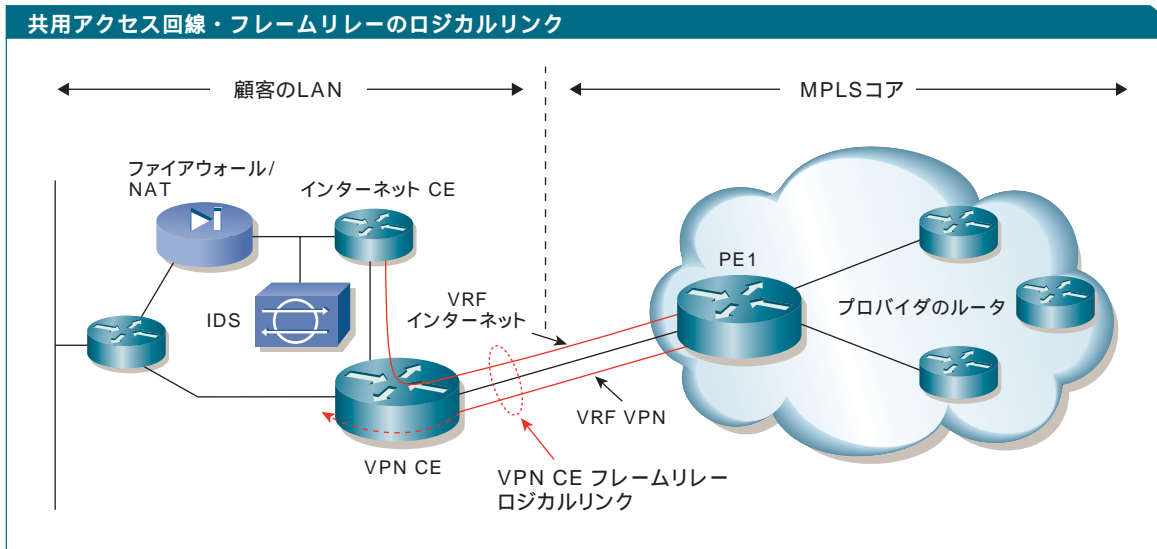


図2：企業は、カスタマエッジとプロバイダエッジの間に複数のフレームリレーのロジカルリンクを使うことにより、コストをコントロールしVPNとインターネットアクセスのサービスを分けることができる

は不可能である。そして、3番目の誤解は「MPLS VPNは外部のDoS攻撃に弱い」というものだ。だが、これも真実ではない。

純粹なMPLS VPNネットワークは全面的な安全が確保されている。MPLSのコアがインターネットアクセスも提供している場合でも、プロバイダエッジルータがVPNアクセスだけを提供していれば、DoS攻撃に対して完全な防御が図られるのである。

さらに一般的には「VPNサービス専用に使われているプロバイダエッジルータでさえもDoS攻撃に弱い」と懸念されている。確かにこれは理論的には正しいかも知れないが、誰であれ不要の侵入者を簡単に特定し切断することができるので、実際にはこのような事態が起こった例はない。

アドレス変更なし

マネージドVPNサービスは社内のネットワークやデスクトップ、サーバなどに特別な変更を加える必要がない。ほとんどの企業はプライベートIPアドレス配布プランを利用しており、コストとセキュリティ面での理由から、マネージドIP VPNサービスのネットワーク共有環境に移行する時もそのプランを残したいと望んでいるはずだ。MPLSは、別々のVPNが同じアドレス空間を使うことを可能にする(RFC 1918)。しかも、各

IPv4ルートに対して64ビットのルート識別子を使用してルーティングを分けるので、たとえ共有のアドレスを使ってもMPLSコアの内部ではそれぞれを明確に区別することができる。つまり、個々のVPN顧客とMPLSコアそのものは完全に独立しているためそれぞれがIPv4アドレス範囲全体を利用できるのである。

ルーティングとデータの分離

MPLSは2つの方法でルーティングの分離を達成している。1つは、各VPNをVirtual Routing and Forwarding(VRF)インスタンスに割り当てることである。プロバイダエッジルータ上にある各VRFは固有のVPNからのルートで形成される。それは静的に設定されたルート、あるいはプロバイダエッジと顧客エッジルータの間で動作するルーティングプロトコルを介したルートである。もう1つは、ルート識別など固有のVPN識別子をBGP(Border Gateway Protocol)に追加する方法である。マルチプロトコルBGPは関連するプロバイダエッジルータの間でVPNルートを交換するが、それはVPN固有のVRF内のルーティング情報として保持される。こうしてMPLSネットワーク全体のルーティングは各VPNに対して別々に保たれることになる。

MPLS VPNは、個別のIP VPNフォワーディングテーブルを持つことでレイヤ3のデータを分離している。サ

サービスプロバイダコア内のフォワーディングはラベルに基づいて実施される。MPLSはプロバイダエッジルータで開始し終了するLabel-Switched Path(LSP)を設定する。パケットは、特定VPNに関連づけられたプロバイダエッジルータインタフェース経由でのみそのVPNに入ることができ、ルータが使用するフォワーディングテーブルはこのインタフェースによって決定される。このようなアドレスプラン、ルートおよびデータの分離が実施されることでMPLS VPNにフレームリレーやATM VPNと同じレベルのセキュリティを提供する。

コアを隠す

MPLSコアネットワークを外界から隠すことによって攻撃は極めて難しくなる。MPLSはパケットのフィルタリングおよびネットワーク情報を自分の境界の外に通じないことでネットワークのコアを隠す。パケットフィルタリングは、VPNの顧客の内部ネットワークやMPLSコアに関するあらゆる情報が外部に漏れるのを防ぐ。プロバイダエッジルータだけがVPN固有の情報を持っているので、内部のネットワークのトポロジー情報を知らせる必要はないのである。

つまり、サービスプロバイダはプロバイダエッジとカスタマエッジの間のダイナミックルーティングプロトコルが必要とするプロバイダエッジルータのアドレスだけを知らせればよいのだ。

ダイナミックルートプロビジョニングの場合、顧客のVPNがルートをMPLSネットワークに配布しなければならない時にコアが学習するのは、特定のホストではなくネットワークルートだけである。したがって、ネットワークセキュリティが犠牲にされることはない。MPLS VPN環境では、プロバイダのネットワークが局外者やインターネットにアドレス配分情報を知らせることがないので攻撃者を寄せつけないのである。インターネッ

「Analysis of MPLS-Based IP VPN Security: Comparison to Traditional L2VPNS such as Frame Relay and ATM and Deployment Guidelines(MPLSベースのIP VPNのセキュリティ分析:フレームリレーやATMなどの従来のL2VPNとの比較と展開のガイドライン)」は cisco.com/packet/164_5b1 で読むことができる。

トアクセスと共用のVPNサービスでは、サービスプロバイダがNetwork Address Translation(NAT:ネットワークアドレス変換)を使ってルートをアナウンスすることができる。このアプローチは、典型的なインターネットアクセスサービスと同じ量の情報を開示するものである。

攻撃に対抗する

サービスプロバイダは、パケットのフィルタリングでアドレスを隠してルータへの到達を防いでいる。Access Control List(ACL:アクセス制御リスト)は、カスタマエッジルータのアクセスをルーティングプロトコルポートだけに限定する。外部からアタックを狙うハッカーは、MPLSコアに入り込んでプロバイダエッジルータ上に直接攻撃を加える、あるいはMPLSのシグナリングメカニズムを攻撃することによってレイヤ3のVPNを攻撃しようと企むケースがある。しかし、ルータが適切に設定されていれば、これらの襲撃を阻止することができる。

一方、エレメントのアドレスが外部から隠されていたとしても、今度は内部のハッカーがそれを推測的に突き止めてしまう可能性もある。しかし、MPLSアドレスの分離メカニズムは入ってくるパケットをVPNカスタマエッジのアドレス空間に属するものとして扱うので、そのアドレスは論理的に識別することができず、推測を基にコアルータへの到達を実現することは不可能である。

また、サービスプロバイダはルーティングの設定を通じてプロバイダエッジルータの既知のピアインタフェースに対する直接攻撃を避けることができる。静的ルーティングが最も安全なアプローチだが、この場合はプロバイダエッジルータは動的なルートリクエストが使用できないという弊害もある。静的ルートはプロバイダエッジルータのIPアドレス、またはカスタマエッジルータのインタフェースのどちらかへ向う。ルートがカスタマエッジルータのインタフェースへ向かう場合、このカスタマエッジルータはコアネットワークのIPアドレスはもちろん、プロバイダエッジルータのアドレスさえも全く知る必要がない。

一方、カスタマとプロバイダのエッジルータの間で動的にルーティングされるリンクは、個々のカスタマエッ

ジルータがプロバイダエッジルータのルータIDまたはピアIPアドレスを知る必要があることから、どうしても安全性では脆弱になる。

そこで、シスコはこのような接続も強化するためにいくつかの方法を推奨している。

可能であれば、カスタマエッジとプロバイダエッジのルータ間にBGPを使うことが望ましい。なぜならBGPはこのアプリケーションに対して最も進んだセキュリティ機能を持つからである。BGPは、プリフィックスフィルタリングやダンピングなど安定性を増すために複数の対抗手段が実装されている。

アクセスをルーティングプロトコルのポートへ向かうものと、エッジルータから来るものだけに制限するACLを使う。

スプーフィングを防ぐため、ルーティングプロトコルに対してMessage Digest Five (MD-5) 認証を設定する。

VFRごとに受容する最大ルート数を設定する。

スプーフィングの防止策、コミュニケーションの暗号化

スプーフィング攻撃はルーティング情報を変更しようとしたり、認証シーケンスにアクセスしようとするものであり、それがいったん成功すると次からはその情報を使って勝手にアクセスしてくる。しかし、たとえMPLS環境でIPソースアドレスのスプーフィングが可能だとしても、VPN間およびVPNとコアの間は完全に分離されているので、このメカニズムを使って他のVPNやコアを攻撃することは不可能である。同様に、ラベルのスプーフィングも全く無力だ。プロバイダエッジルータは、カスタマエッジのソースから受信したラベル付きの packets を自動的に廃棄するからである。

企業は適切に構築したMPLSコア上でさらにトラフィックを暗号化するというオプションもある。これにより規制順守とデータセキュリティの強化が可能となる。暗号化はカスタマエッジルータ間で運用する。MPLSにIPSec (IP Security) の暗号化を組み合わせることはセキュリティ強化に有効である。また、サービスプロバ

イダネットワークに対してパケットのペイロードが透過的であれば、専用あるいはアプリケーションレベルの暗号化スキームを組み合わせることも有用である。

プロビジョニングの選択肢

企業が自社のネットワークとプロバイダエッジ間の接続を割り当てる時には、セキュリティとコストのトレードオフを考慮する必要がある。どんな場合でも、プロバイダはVPN分離に関して全面的な管理をする。プロバイダエッジはカスタマエッジの信頼性の低いものとして扱い、カスタマエッジからは純粋なIPパケットだけを受け取る。多くの場合、サービスプロバイダは同じコアでVPNとインターネットアクセスという両方のサービスを提供しているが、シスコが推奨する適切なセキュリティ対策を講じさえすれば、常にセキュリティは安全圏内にある。ほとんどのMPLS VPNの展開では、VPNサービスは同じコアによってインターネットアクセスのためのオプションと併せて提供されている。フレームリレーやATMのコアの場合には、両サービスを提供するために2つの別々のインフラが必要となり、その分だけコスト高になってしまうのである。

最も安全ながら同時に最もコストがかかるプロビジョニングのシナリオは、ほとんどフレームリレーやATMのモデルと同じように、1つのサイトに対してVPNとインターネットアクセスの間を完全に分けることである(図1を参照)。つまり、2台のエッジルータと2系統のWANアクセス回線を導入し、各々のエッジルータからプロバイダのネットワークにつなぐのだ。この手法なら、インターネット接続を通じたいかなるDoS攻撃からもVPNネットワークを隔離する。

もう1つのシナリオは、プロバイダエッジでVPNとインターネットアクセスサービスを統合することだ。やはり2台のエッジルータと2本のアクセス回線を購入することになるが、同じプロバイダエッジルータにある別々のVRFインタフェースに送信するのである。この方法は、完全な分離を進める前者に比べてコストを抑えながら、VPNに対するDoS攻撃をかなり強力に防御することができる。

もう1つのプロビジョニングの選択肢として、WANの回線コストを削減するために両方のサービスに1本の

アクセス回線を使うことがあげられる。この方法は両方のサービスを支援するインフラを共有するので、DoS攻撃に対する防衛力は低くなる。しかし、カスタマエッジとプロバイダエッジルータの両面で適正な設定を施すことによって、アクセスをコントロールできる。したがって、このリスクは現実的というよりは理論上は考え得るというレベルのものとなる。典型的な単一回線のシナリオでは、2重のロジカルリンクおよびカスタマエッジとプロバイダエッジルータの双方に別個のサブインタフェースを備えた1本のフレームリレーのアクセス回線が使われる(図2を参照)。インターネットトラフィックはインターネットカスタマエッジルータに送られる。カスタマエッジのVPNルータは、VPNロジカルインタフェース経由でVPNトラフィックを常に分離するので、決してインターネットカスタマエッジルータへ送られるインターネットトラフィックと出会うことはない。

自分のサービスプロバイダに聞いてみよう

企業はサービスプロバイダに以下の質問をすることにより、提供されているMPLS VPNのセキュリティ水準を評価することができる。

インターネットとVPNアクセスは同じコアネットワークで提供されているか?

最も安全なのはVPNサービスだけを提供するケースだが、ほとんどの企業にとってはコアネットワークを共有しても十分な安全が確保される。

インターネットとVPNサービスに別々のプロバイダエッジルータを提供しているか?

統合型のプロバイダエッジルータはDoS攻撃に晒されるリスクが若干高い。プロバイダエッジルータが共有であろうが、あるいはインターネットアクセスサービスから分離されていようが、ハッカーはVPNの分離を侵害することはできない。

どうやってコアの安全を確保しているか?

Cisco Powered Networkプロバイダは、シスコのセキュリティのベストプラクティスにしたがってMPLSネットワークの安全を確保し、VPNサービスをフレームリレーやATMと同等に安全なものにしている。

ニースを拠点に活動するシスコのシニア・コンサルティング・エンジニアであるマイケル・ベリンジャーは、MPLSセキュリティやDoS攻撃の防御などサービスプロバイダのセキュリティの問題にフォーカスし、IETFを牽引するメンバーだ。連絡先はmbehring@cisco.com

ステファン・ワンはサービスプロバイダやネットワークに関するビジネスで20年以上の経験を持つ。シスコではMPLS、IPSec、レイヤ2、レイヤ3のVPNサービスを担当し、サービスプロバイダ・マーケティングで複数の役割を担っている。連絡先はstepwong@cisco.com

詳しい情報

TechTalk: "MPLS VPNセキュリティの理解"
(TechTalk: "Understanding MPLS VPN Security")

cisco.com/packet/164_5b2

MiercomからシスコへのMPLS VPNエンジニアリングレポート (Engineering Report MPLS VPN by Miercom for Cisco)

cisco.com/packet/164_5b3

IETF Internet-Draft 「BGP/MPLS IP VPNのセキュリティ分析 (IETF Internet-Draft "Analysis of the Security of BGP/MPLS IP VPNs")」

cisco.com/packet/164_5b4

「Cisco 20年間の歴史」をご覧ください

2004年12月、シスコシステムズは創業20周年を迎えました。創業20周年を記念し、ホームページにて「Cisco 20年間の歴史」をご紹介します。

スタンフォード大学のコンピュータ・サイエンティストであるレン・ボサックとサンディ・ラーナーが1984年12月に創業して以来、シスコシステムズは常にインターネットの発展に貢献するべく事業を展開してまいりました。シスコシステムズが刻んだ20年間の歴史をぜひ下記サイトをご覧ください。

<http://www.cisco.com/jp/news/timeline/>

