



Check Point®

SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.



White Paper

Bridging the gap between connectivity and security

接続性とセキュリティの両立

IPSec VPNに対するチェック・ポイントの理念



Intelligent Security

チェック・ポイントは、境界、内部、WEBなど、ネットワークのあらゆる局面に対するセキュリティ・ソリューションを提供します。これにより、企業はネットワークや、ネットワーク・リソース等を安全に保護しながら、高い接続性を実現するリモート・アクセスを提供し、簡単に管理することができます。

Contents

本書の内容

概要	3
はじめに	3
VPNとネットワークの両方で高いセキュリティを実現する	3
シナリオ1: VPN機器をファイアウォールの手前に配置	4
シナリオ2: VPN機器をファイアウォールの背後に配置	5
シナリオ3: 統合ルータ	6
シナリオ4: VPN機器とファイアウォールを並列に配置	6
VPNのセキュリティを維持するチェック・ポイントのソリューション	7
SmartDefenseによる侵入防止	9
セキュリティのスプロール現象の防止	10
VPNの管理を容易にするためのさまざまな先進の技術を提供する	11
シンプルなVPN環境を実現するビルディング・ブロック	11
サイト間認証	11
VPNコミュニティ	11
サービス品質 (QoS)	12
ハイ・アベイラビリティとロード・シェアリング	12
VPNの構築を容易にするVPN-1	12
包括的な暗号化	12
統合された認証局	13
VPNコミュニティの実装	13
VPNに対するQoS	14
ハイ・アベイラビリティおよびロード・シェアリングを可能にするMEP(複数のエントリ・ポイント)	15
従来型のVPNの問題: 増加するリソースと動的化が進むネットワーク	16
ルート・ベースのVPN: シンプルなルーティングによる複雑なVPNの構築	16
しなやかなリスタート (Graceful Restart)	18
マルチキャスト・プロトコルのサポート	18
結論	19

概要

今日、企業のIT環境では、VPN (Virtual Private Network) に関して、接続性とセキュリティの両方のニーズを1つのソリューションで満たす統合型のアプローチが求められています。本社と支社・支店など遠隔地にあるオフィスをインターネット経由でVPN接続するにあたっては、VPNソリューションについて次の2点を考慮する必要があります。

- ソリューション自体の可用性とネットワークの安全性を保証するための十分な機能が備わっているか。
- 先進の技術と共に、ソリューションの運用管理の簡素化と負担軽減を可能にする管理機能が備わっているか。

Check Point VPN-1[®]は、これら2つの要件を両方とも満たすように設計されたセキュリティ・ゲートウェイ製品です。VPN-1は、シンプルさを犠牲にすることなく接続性とセキュリティの両立を実現します。

はじめに

IPsec VPN (Virtual Private Network) がごく一般的な技術となった現在では、多くの大規模企業がこの技術を利用して本社と支社・支店間を接続し、また自宅や出張先などから企業にインターネット経由で接続し機密情報をやり取りしています。しかし、IPsec VPNがこのように普及したことは、多くの組織のIT部門においてセキュリティ上の新たな問題をもたらす結果となっています。VPNは主に接続機能を提供する技術であるため、組織として何を重視するかについては、おのずとネットワーク・エンジニアの意見が尊重されることが多くあります。その結果、セキュリティを犠牲にしても、マルチキャストやダイナミック・ルーティングなどの高度なネットワーク機能が優先されることが多いのです。例えばルータ・ベースのVPNが登場したことは、ファイアウォールなどのセキュリティ機能を持たず、接続機能だけを提供するソリューションが普及するきっかけとなりました。一般的に境界ベースのファイアウォールは、VPNルータがネットワークの内側に置かれている場合は暗号化されたVPNトラフィックを検査することができず、VPNルータがネットワークの外側に置かれている場合はルータを保護することができません。そのため、セキュリティ・エンジニアはネットワークを保護するために複雑な問題回避策を講じるか、あるいは多くの場合、シンプルさを維持するためにセキュリティを犠牲にせざるを得なくなっています。接続性とセキュリティのトレードオフに関するこの問題は、その両立を実現することで解決する必要があります。

この技術白書では、接続性とセキュリティを両立させるための方策について説明すると共に、これを実現するための技術について概説します。その中で、VPNに対するこのアプローチにおける次の2つの原則を検討していきます。

- VPNとネットワークの両方で高いセキュリティを実現する
- VPNの管理を簡素化する先進の技術を提供する

VPNとネットワークの両方で高いセキュリティを実現する

VPNは元々、専用線やフレーム・リレーに代わる技術として考えられていたという歴史的背景を考えれば、接続性に重点が置かれる理由は容易に理解できます。しかしながら、現在のビジネスおよびIT環境において、接続性にばかり注目するのは、次の2つの理由から近視眼的であると言わざるを得ません。

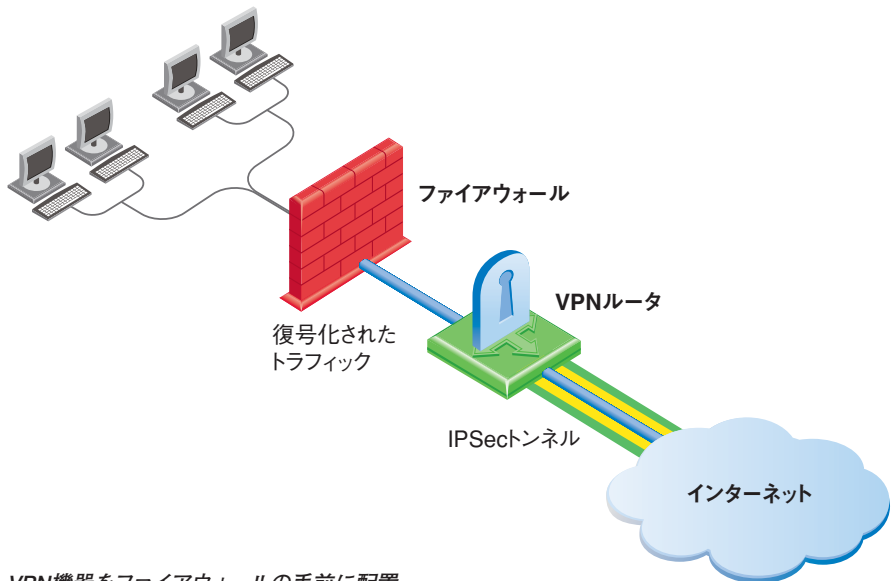
第1の理由は、VPNは信頼できないネットワークまたはある程度しか信頼できないネットワーク上に構築されるため、VPN機器を狙ったサービス妨害 (DoS) 攻撃などを受ける可能性があることです。しかしVPN機器自体には、これらの攻撃をブロックするために必要な防御機能が備わっていません。また、接続機能を提供するデバイスであるVPN機器は安定性を重視した設計になっており、次々と現れるセキュリティ上の問題に対応するために必要となる動的なアップデートを考慮した設計には当然なっていません。

第2の理由は、通常は信頼できるとされているネットワーク内部の利用者(社員など)が、ネットワーク・レベルの視点で見た場合、実際には100%完全に信頼できる存在ではないということです。組織において、ある人物が、本人が主張するとおりの人物であると見なすことはできても、セキュリティ担当者として、その人物が悪意ある行為をしないとまで断定することはできないのです。その人物のノートPCがワームに感染しているかもしれませんし、あるいはその人物が接続先のサーバにバッファ・オーバーフロー攻撃を仕掛けようとしているかもしれません。ワームなど、アプリケーション層で攻撃を行う脅威が出現したことで、VPNトラフィックを隔離してインテリジェントな検査を行うことはもはや必須となっています。このような検査を行わない場合、ネットワークは、支社・支店環境を踏み台にして侵入され、瞬く間にネットワーク全体に拡散するマルウェアの脅威にさらされることとなります。

セキュリティ担当者とネットワーク担当者の中でVPNに対する考え方が大きく異なるのは、VPNの技術とセキュリティの技術がそれぞれ異なるソリューションで提供されるという構造に主な原因があります。このためほとんどのネットワーク環境では、以下の4つの基本シナリオのいずれかを選択しなければならず、セキュリティが複雑化するか、あるいはセキュリティ面で妥協することを余儀なくされています。

シナリオ1：VPN機器をファイアウォールの手前に配置

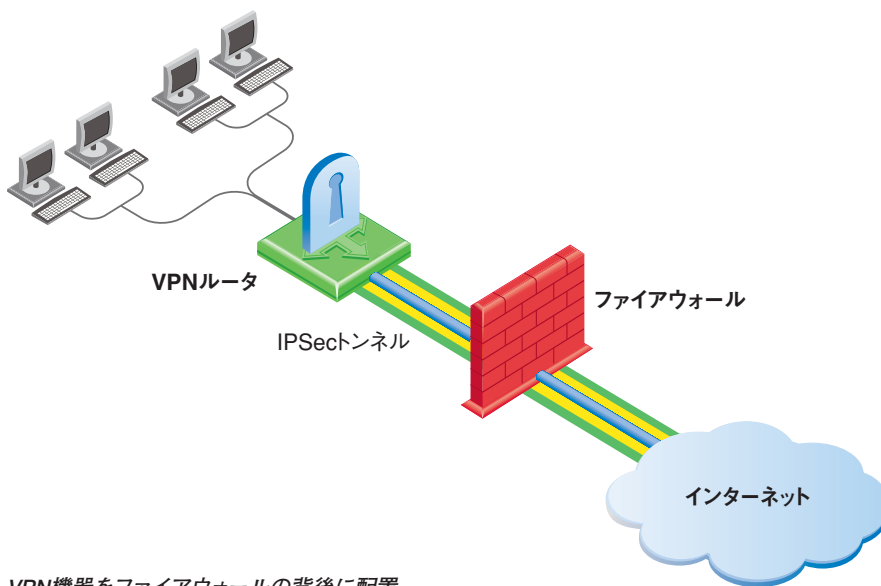
1つ目のシナリオは、VPN機器をファイアウォールとインターネットの間に配置するというものです。このシナリオでは、VPNコンセントレータかVPN対応ルータを使用するのが一般的で、どちらの機器も基本的なパケット・フィルタリング機能を備えている場合があります。この設定は、VPN対応ルータの普及に伴い、多くの組織(特に小規模なオフィス)で採用されています。この設定のメリットは、VPN機器がファイアウォールの手前でトラフィックを復号化できることです。ファイアウォールはトラフィックに基づいてインテリジェントな判断を下すことができるので、導入が簡単に行えます。



簡単に導入できる反面、この構成には1つ大きな問題点があります。VPN機器が境界の防御壁であるファイアウォールよりも外側に置かれているため、インターネット側から攻撃を受ける可能性があるのです。具体的には、脆弱性を突かれて乗っ取られたり、IPsec VPNにおける鍵管理のためのプロトコルであるIKE (Internet Key Exchange) に対するDoS攻撃によって使用不能にされるおそれがあります。VPN機器が提供するセキュリティ機能は、脆弱性がもたらす脅威やDoS攻撃などに対する有効な手立てにはなりません。

シナリオ2：VPN機器をファイアウォールの背後に配置

一般に、VPN機器をファイアウォールの背後に配置する場合は、VPNトンネルの向こう側にいるユーザを信頼できるユーザと見なすことになります。サイバー攻撃の大半は依然として信頼できるはずの内部関係者によって行われているという事実を考えると、これは極めてリスクの高い考え方であると言えます。このシナリオではVPNトラフィックの検査は行われません。境界ファイアウォールは、暗号化されたままのVPNトラフィックを理解することができないためです。

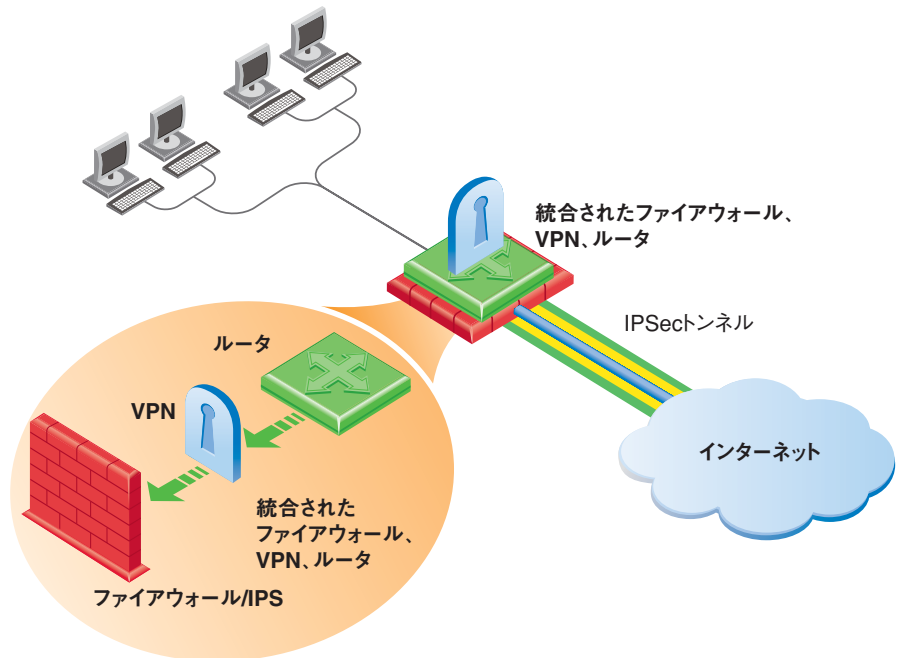


VPN機器をファイアウォールの背後に配置

このシナリオでは、ファイアウォール（およびそのセキュリティ・ポリシー）が完全に迂回されてしまうため、セキュリティ担当者の立場からすると複数の大きなリスクが生じることになります。1つは、ファイアウォールの手前に配置したときと同様、VPN機器がDoS攻撃や脆弱性がもたらす脅威にさらされることです。もう1つは、ファイアウォールが、トラフィックに含まれる悪意あるコンテンツを検査するという本来の役割を果たせないことです（攻撃トラフィックは検査されないままファイアウォールを通過してしまいます）。そして最後は、VPNトラフィックを通過させるために、ファイアウォールで複数のポートを開く必要があることです。これは、ポートはできるだけ開かないようにしてネットワークを「封鎖」という最も基本的なセキュリティ・ポリシーに違反することです。トラフィックがDMZ (Demilitarized Zone) 経由でファイアウォールを通過するように再ルーティングすることもできますが、この場合でもVPN機器自体のリスクはそのままであり、また管理者は設定が複雑になるという問題を抱えることになります。

シナリオ3：統合ルータ

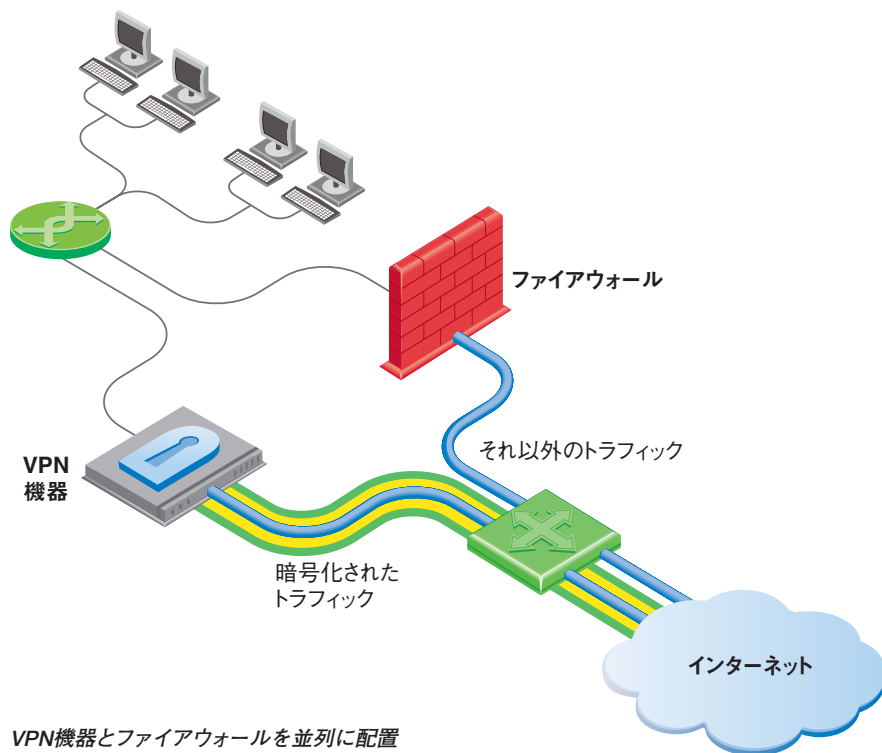
この問題を解決する手段としてネットワーク関連ベンダーが提供しているソリューションに、ルーティング、VPN、ファイアウォールなどの複数の機能を1つのプラットフォームにまとめた統合ルータがあります。このアプローチは理屈の上では正しいものですが、実際にはシナリオ1および2が抱える問題の多くはこのアプローチでも解決されません。その主な理由は、各モジュールが本当の意味で統合されているのではなく、それぞれ独立した機能として開発、実装されていることにあります。この種のソリューションでは、トラフィックを各モジュール間でリニアに渡すことによって、各種の処理を実行します。つまり、ルータ・モジュールが自身の処理を完了したら、トラフィックは必要に応じてVPNモジュールに渡され、最後にファイアウォール・モジュールに渡されるのです。処理の順序は製品によって異なる場合がありますが、モジュール間の連携が行われないという点は各製品に共通しています。この種のソリューションによって、ハードウェア・コストの削減と設置スペースの節約を実現できることは確かですが、ネットワークとVPNを各種の脅威から保護するという本来の目的を達成することはできません。統合されていない複数の機能を1つのプラットフォームで提供するというこのモデルは、多くのセキュリティ・アプライアンスに共通するものであり、それらはみな同じ問題を抱えています。



統合ルータ・アーキテクチャ

シナリオ4：VPN機器とファイアウォールを並列に配置

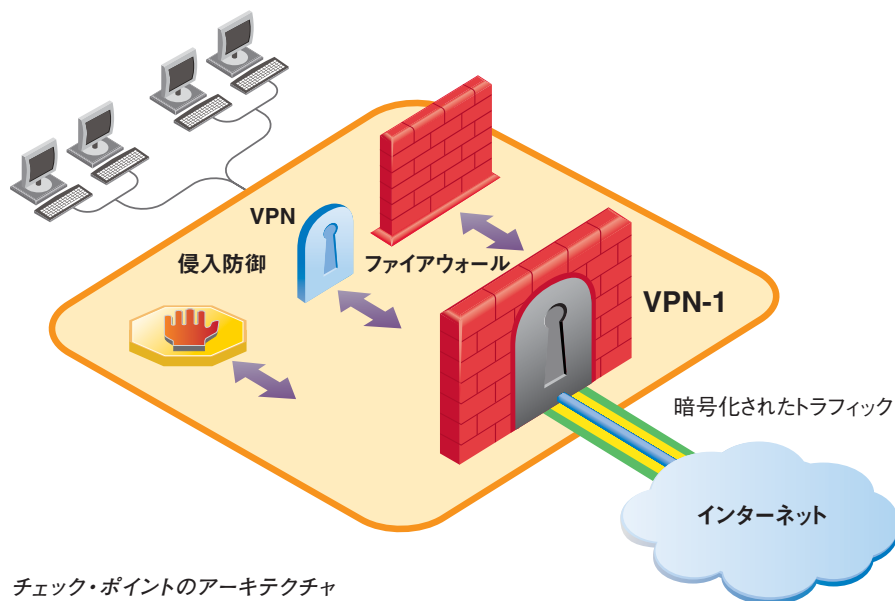
4つ目のシナリオは、VPN機器とファイアウォールを並列に配置するというものです。ゲートウェイ・ルータは、暗号化されたトラフィックをVPN機器に、それ以外のトラフィックをファイアウォールにルーティングします。このシナリオでは、シナリオ1~3のすべてのデメリットが引き継がれるうえに、設定と実装のシンプルさというメリットが失われます。VPN機器は依然として攻撃を受ける可能性があり、暗号化されたトラフィックはファイアウォールの検査を受けません。暗号化されたトラフィックを検査するには、ファイアウォールを通過するようにそのトラフィックを再ルーティングするか、あるいは別のファイアウォールをVPN機器の内側に設置する必要があります。



VPN機器とファイアウォールを並列に配置

VPNのセキュリティを維持するチェック・ポイントのソリューション

VPNを導入する場合のこれらの諸問題を解決するため、すなわち、接続性とセキュリティの両立を実現するため、チェック・ポイントのセキュリティ・ゲートウェイ製品ファミリVPN-1[®]では、完全な統合アーキテクチャが採用されています。VPN-1では、個々の機能がそれぞれ独立して動作するのではなく、ファイアウォール、VPN、および侵入防御の各機能が一体となって動作します。これらの機能は適切なタイミングで実行され、リスクを最小限に抑えます。これにより、設定を複雑にすることなく、VPNのDoS攻撃から保護し、ファイアウォールおよび侵入防御の機能によるVPNトラフィックの検査を両立することが可能になります。



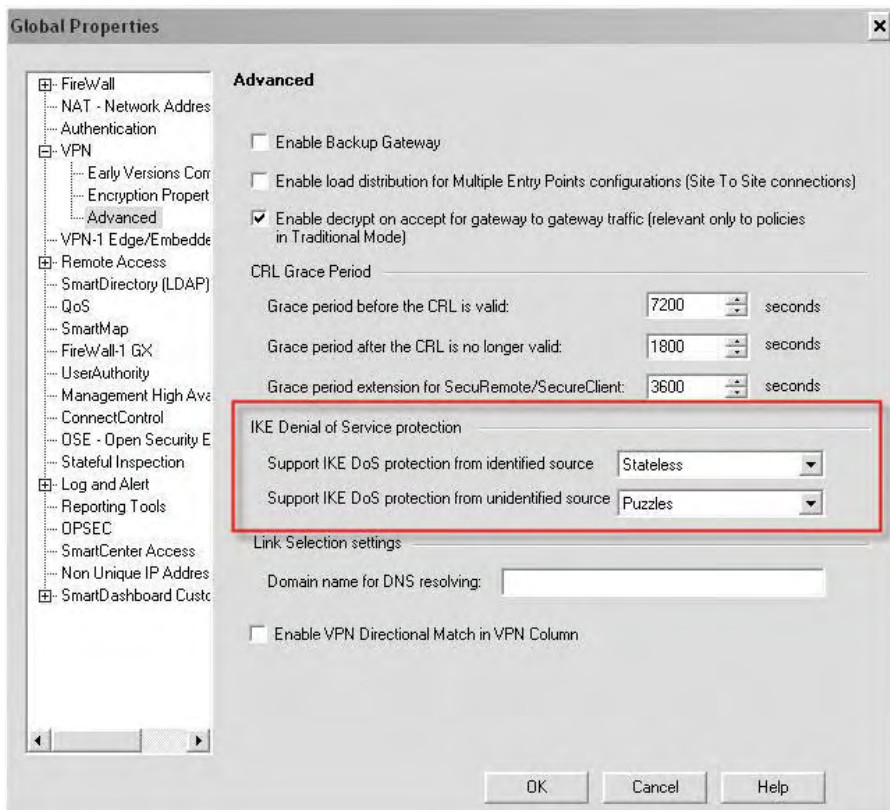
チェック・ポイントのアーキテクチャ

例えばVPN-1では、IKEに対するDoS攻撃からVPNを保護することができます。IKEに対する既知の攻撃は、VPNトンネルを作成するように要求する、特別な細工を施したパケットをVPNゲートウェイに送信してIKEプロトコル群の脆弱性を利用するというものです。ゲートウェイは機能上、このVPNトンネルの作成要求に応じてトンネル用のメモリを確保する義務があります。攻撃者は、このようなリクエストをランダムなIPアドレスから短い間に大量に送信することで、VPNゲートウェイのすべてのリソースを消費させ、ゲートウェイが正規のリクエストに対応できないようにすることができます。

このような攻撃を防ぐ手段としては、IKEの通信を既知のゲートウェイのIPアドレスに限定するという方法があります。しかしこの方法では、小規模なオフィスが数多く存在する環境で用いられることの多い動的IPアドレスが使用できなくなってしまいます。別の手段としては、秒あたりのIKEリクエストの数を監視して、リクエスト数がしきい値を超えた場合には攻撃の可能性があるとして新しいリクエストの受け付けを停止するという方法があります。

VPN-1には、サービスを停止せずにIKEへのDoS攻撃をブロックするための手段が、これら以外にも複数用意されています。その1つに、ステートレスな防御機能があります。VPN-1は、大きな負荷が生じているとき、またはある値が攻撃の可能性があることを示すしきい値に達したとき、リクエスト元のゲートウェイに対し、そのゲートウェイしか知り得ない数値を生成するよう求めるチャレンジを送信します。そして、リクエスト元のゲートウェイが正しい答えを返すまでの間、当該のリクエストを無視し、メモリやCPUリソースの割り当てを停止します。もし攻撃者が正規のゲートウェイのIPアドレスを詐称しているのであれば、このチャレンジを受信することができず、答えを返すことができません。この場合、当該リクエストは破棄されます。

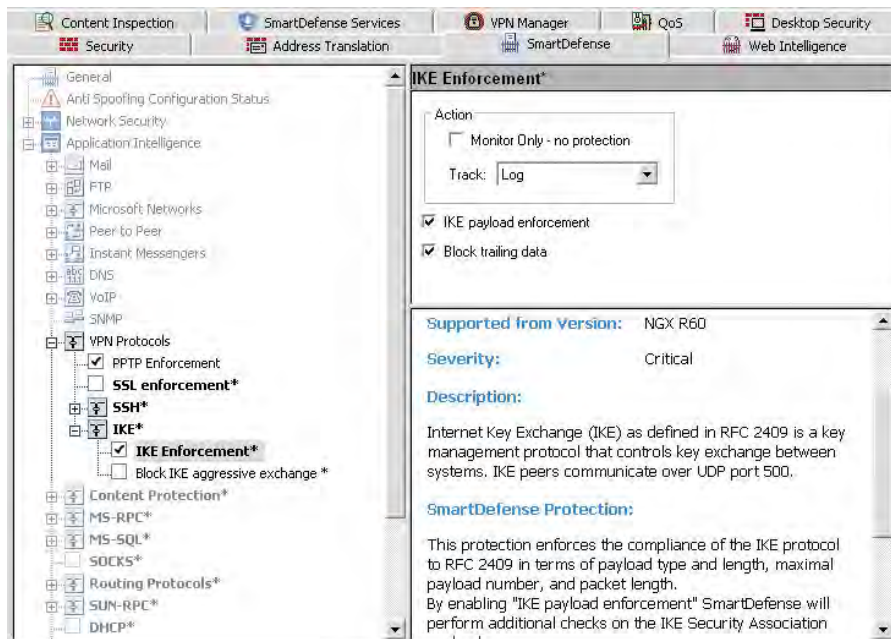
ただし攻撃者が、VPN-1が把握していない多数のIPアドレスを制御しており、それらに関連付けられたホストを乗っ取っているというケースも考えられます。これは、典型的な「ボット」のシナリオです。この場合、攻撃者はおそらくチャレンジに応答できてしまいます。VPN-1では、この問題に対処するためにパズル・チャレンジという手法を提供しています。パズル・チャレンジでは、リソースの割り当てを行う前に、リクエスト元のリモート・コンピュータに対して演算負荷の高いパズルを解くように要求します。このチャレンジは1秒あたり2~3個しか解くことができないため、リモート・コンピュータはリクエストを送信するのに時間がかかるようになり、その結果としてDoS攻撃の威力が弱められます。



VPN-1のIKE防御機能

SmartDefenseによる侵入防御

VPN-1では、専用の機能を使用する代わりに、侵入防御技術のSmartDefense™を利用してIKEを防御することもできます。SmartDefenseを利用した場合には、チェック・ポイントだけでなく競合他社のVPN技術も保護することが可能になります。IKEに対するDoS攻撃は、ベンダーを問わずあらゆるゲートウェイに対して行われる可能性があるため、然るべき対策を行うことは非常に重要なことです。米国CERT (Computer Emergency Readiness Team) は2002年8月、細工を施したパケットを1つ送信するだけでバッファ・オーバーフローを引き起こしたりDoS攻撃を引き起こすことのできる脆弱性が、複数のベンダーのソリューションに存在すると警告を発しています。チェック・ポイントのSmartDefenseは、正当なIKEトラフィックと悪意あるIKEトラフィックの振る舞いの違いを深いレベルで認識できるため、細工を施したパケットが例え1つだけであってもこれを検出することができます。VPN-1は、IKEプロトコルに準拠していないパケットを受信した場合には、そのパケットをネットワークの手前で破棄します。



SmartDefenseによるIKE防御機能

VPN-1ファミリでは、各種の防御機能が完全に統合されているため、VPNを狙った攻撃をブロックできるだけでなく、復号化後のトラフィックに悪意あるコンテンツが含まれていないかどうかを検査することもできます。すでに述べたように、ワームなどの悪意あるコードに感染している可能性のあるリモート・サイト(支社・支店など)やリモート・ユーザは、ある程度しか信頼できない存在として扱わなければなりません。VPN-1は、VPNトラフィックを検査なしで通過させるワイヤ・モードをサポートしていますが、ネットワークの安全性を維持するため、デフォルトではVPNトラフィックについても必要な検査を行います。

セキュリティのスプロール現象の防止

VPN-1の統合型のアプローチは、優れたセキュリティを提供するだけでなく、VPNの管理も簡素化します。ユーザ・データベースやポリシー、ログなどを個別に維持管理するための労力は、決して軽視できるものではありません。ファイアウォールやVPNソリューションごとに管理インターフェースやデータベースが必要となる環境は、設定ミスが生じる原因の1つであり、「セキュリティのスプロール現象」を引き起こします。セキュリティのスプロール現象とは、同じような設定作業を何度も繰り返す必要があったり、ポリシーの不統一によりセキュリティの実効性が低下したりすることで管理コストが増大するような、無秩序なセキュリティ環境のことをいいます。

VPN-1は、ファイアウォール、VPN、および侵入防御のすべての機能にわたって統一されたセキュリティ・アーキテクチャを採用しているため、セキュリティのスプロール現象の発生を防ぐことができます。このアーキテクチャにより、共通の作業に対しては共通のリソース(ユーザ・データベースなど)を使用できるようになるので、VPNの管理に伴うコストを大幅に削減すると共に、設定ミスが発生する可能性を最小限に抑えることが可能になります。

VPNの管理を容易にするためのさまざまな先進の技術を提供する

VPNは、以前は設定が複雑すぎて大規模な導入は難しいと考えられていましたが、近年では、ビジネス・コミュニケーションに欠かせない存在として急速に導入が進んでいます。ブロードバンド接続が広く普及したことによって、組織では、数年前と比べてより小規模なオフィスにもVPNを導入するようになっており、その結果としてより大規模なVPNが構築されるようになってきました。VPNの導入に対して確実に投資対効果を得るためには、VPN環境がよりシンプルになることが必要です。

シンプルなVPN環境を実現するビルディング・ブロック

VPNは元々、情報の機密性と完全性を保証する暗号化アルゴリズムを使用することによって、信頼できないネットワーク上で安全にデータをやり取りできるようにするためのソリューションでした。しかし現在のVPNは、より多くのサイトで設定されるようになったことで規模が拡大・複雑化しており、元々の役割に内包されていたシンプルさが失われてしまっています。今、VPNにはこのシンプルさを取り戻すことが求められています。また、構築自体を容易にすることに加えて、サイト間認証、VPNコミュニティ、サービス品質 (QoS)、ハイ・アベイラビリティ、およびロード・シェアリングといった機能についても考慮が必要になります。

サイト間認証

サイト間認証は、VPN環境が複雑化する最大の要因の1つです。通信を行う当事者のアイデンティティを保証するための仕組みには、主に次の2つの方法があります。1つは、秘密を共有する方法 (シェアード・シークレット)、すなわち手動で割り当てた暗号鍵のペアを2つのサイトで共有する方法です。フルメッシュ型のVPN (すべてのサイトが相互に直接通信するタイプのVPN) を構築しようとしている大規模組織の場合、この方法では $(n \times n - 1) / 2$ (n はサイト数) の鍵を管理することになります。例えば、75のサイトからなるフルメッシュ型のVPNを構築する場合は、手動で2775個の鍵を割り当てる必要があるということです。これに76番目のサイトを追加した場合には、さらに75個の鍵のペアが必要になります。またこれらの鍵は、セキュリティ上の理由から定期的に変更する必要があるため、問題はさらに複雑になります。そのため管理者の立場からすると、秘密鍵を共有する方法でVPNの規模を拡大することは、あまり現実的ではありません。

もう1つの方法は、公開鍵インフラストラクチャ (PKI) を利用した鍵交換のための認証局を用意することです。秘密鍵を共有する方法の場合、鍵を定期的に変更しないとブルート・フォース・アタックが成功する可能性が高くなりますが、2つ目の方法では、鍵を変更する必要がないためセキュリティはより高くなります。ただし、PKIシステムと集中ディレクトリが導入されていない企業の場合、これらの導入に相応のコストがかかるほか、VPN環境が複雑化することになります。

VPNコミュニティ

ネットワーク中のVPNゲートウェイにより構成されるVPNネットワークであるVPNコミュニティの設定は、ネットワーク管理者にとって長年の懸案事項です。通常、既存のVPNに新しいサイトとリソースを追加するには、既存のゲートウェイ群に新しいゲートウェイを認識させるなどの作業を手動で行う必要があります。手動で設定するサイトの数が多い場合には、ちょっとした設定ミスによって接続がうまくいかないなどの問題が起こりやすくなります。

サービス品質 (QoS)

VPN環境では、帯域管理とサービス品質 (QoS) の問題も考慮する必要があります。VPN通信では遅延が発生しがちであるため、VoIPなどのリアルタイム・アプリケーションが広く使われるようになっている現在の多くのネットワーク環境では、帯域管理とQoSの重要性が高まっています。そこで、VPNで暗号化を行いながら遅延の発生を最小限に抑えることのできる手段が必要になります。またQoSは、各アプリケーションに割り当てる帯域の割合を環境のニーズに合わせて定義できる柔軟性を備えたものでなければなりません。

ハイ・アベイラビリティとロード・シェアリング

VPNサービスの運用に際しては、ハイ・アベイラビリティとロード・シェアリングの機能が重要な役割を果たします。例えば、電子メールなどの内部リソースの可用性は、VPNが稼働しているかどうかによって依存します。従来のVPNは、例えハイ・アベイラビリティ機能を備えている場合でも、同期という点に問題を抱えています。1つのゲートウェイが使用不能になった場合、ユーザはセッションを最初からやり直す必要があるのです。これは、技術にあまり詳しくないユーザにとっての使いやすさを考えた場合、非常に大きな問題と言えます。また、ハイ・アベイラビリティ・クラスタにおいては、クラスタを構成する個々のゲートウェイが物理的に離れた場所にある場合でも、フェイルオーバーを確実にサポートできることが必要となります。

VPNの構築を容易にするVPN-1

VPN-1ソリューションは、各種の技術を提供することにより、VPNをVPN導入前の作業と変わらなく容易に構築することを可能にします。チェック・ポイントは、大規模なVPN環境をシンプルにすることに関して業界をリードする立場にありますが、それと同時に、先進の技術を通じて包括的な暗号化といった高度な機能も提供しています。

包括的な暗号化

VPN-1ファミリは、送受信するデータを保護するために、強固な暗号化アルゴリズムをサポートしています。VPN-1のVPN技術は、米国連邦政府の暗号モジュールに関する規格「Federal Information Processing Standards Publication 140-2」の認定を受けており、実績あるソリューションとしての確実性と、求められたセキュリティ・プロファイルに適切な暗号化アルゴリズムを適用する柔軟性を併せ持っています。

暗号化アルゴリズム	
IKE暗号化	AES-256
	3DES
	DES
	CAST
IPSec暗号化	AES-256
	AES-128
	3DES
	DES
	DES-40CP
	CAST
	CAST-40
	NULL
IKEおよびIPSecにおけるデータの完全性チェック	SHA1
	MD5

統合された認証局

サイト間認証に関する問題の解決策としてチェック・ポイントが提供しているのは、統合された認証局 (ICA) です。VPN-1には、サイト間VPN環境の複雑さを軽減させると共に、シンプルな認証メカニズムを通じて通信の機密性を向上させるICAが統合されています。このICAは、VPN-1や他のチェック・ポイント製品の統合管理を行うためのSmartCenter™サーバの一機能として提供され、X.509の証明書および証明書失効リスト (CRL) に完全対応しています。証明書は、VPNコンポーネントを有効にしたVPN-1 PowerまたはVPN-1 UTMを導入したときに自動的に作成および発行されます。鍵の有効期間や鍵長などの属性は、環境のニーズに合わせて柔軟にカスタマイズが行えます。このICAは、リモート・アクセスを行うVPNユーザ用に使用することもできます。

すでに別のPKIソリューションを導入している場合には、VPN-1でそのソリューションの証明書を使用することも可能です。サードパーティの証明書は、PKCS#10リクエストを使用して手動でインポートするか、または自動登録を使用して信頼できるCAから取得できます。VPN-1がサポートする自動登録プロトコルは次のとおりです。

- SCEP (Simple Certificate Enrollment Protocol)
- CMP v1 (Certificate Management Protocol)
- CMP v2

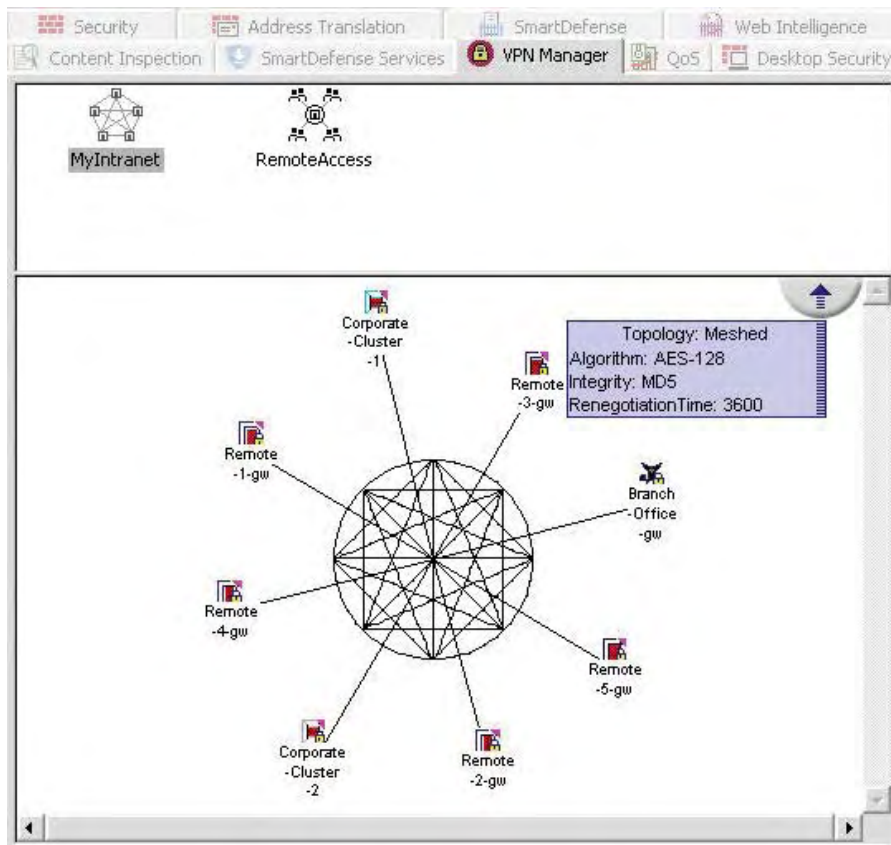
多くのサードパーティPKIベンダーは、Open Platform for Security (OPSEC™) を通じて、自社のソリューションとチェック・ポイントのソリューションとの相互運用性を認定しています。認定ソリューションの一覧は、<http://www.opsec.com>の「Security Enforcement」セクション→「Authentication」ページをご覧ください。VPN-1はX.509証明書に対応しているため、このページに記載されていないソリューションとも相互運用できる場合があります。

VPNコミュニティの実装

新しく導入するVPNゲートウェイの追加するための作業が簡単にかつシンプルに行えるようになれば、VPNコミュニティの設定も容易に行えるようになります。チェック・ポイントのVPNコミュニティによって、新しいVPN-1を既存のサイト間VPNを構成するVPNコミュニティに複雑な設定を行うことなく簡単に追加できます。これは、るようになることは、VPNをシンプルにするというチェック・ポイントの取り組みにおいて重要な概念です。新たに追加されたゲートウェイは必要なIPsec設定情報を自動的に引き継ぎ、既存のすべてのゲートウェイは新しいゲートウェイを直ちに認識します。設定可能な属性の一部を次に示します。

- IKEプロパティ (Diffie-Hellmanグループのタイプや、アグレッシブ・モードを使用するかどうかなど)
- 鍵交換およびデータの機密性維持のための、暗号化およびデータの完全性に関するアルゴリズム
- PFS (Perfect Forward Secrecy)
- 暗号化の対象としないアプリケーション、サービス、プロトコル

「ワン・クリックVPN」とも呼ばれるこの技術は、サイト間VPNの設定および新しいサイトの追加に要する時間を大幅に短縮します。この技術によって、大規模なVPN環境で設定ミスが発生する可能性も最小限に抑えられます。すべての設定は一箇所から引き継がれるため、VPNに関する問題が発生した場合でも、素早くトラブルシューティングを行うことができます。サードパーティのVPN機器もVPNコミュニティに参加できるので、レガシーなVPNソリューションからの移行も簡単です。この場合、サードパーティのVPN機器については手動で設定を行う必要がありますが、VPN-1はこれらの機器を自動的に認識し、適切な設定を受け入れます。これは、チェック・ポイントの技術によって実現されたVPN設定のシンプルさを示す一例です。



定義済みVPNコミュニティの表示

VPN-1では、コミュニティのVPNトポロジとしてメッシュ型とスター型の両方がサポートされています。メッシュ型のVPNでは、すべてのコミュニティ・メンバーは相互に直接通信することができます。スター型のVPNでは、サイト間のトラフィックの流れはハブ・アンド・スポーク型に似ており、すべてのトラフィックは一連の中央ゲートウェイを通じてルーティングされます。スター型VPNコミュニティの管理を簡素化するため、管理者は、VPNコミュニティを使用してトラフィックのルーティングを次のいずれかの形に設定することができます。

- 中央ゲートウェイ(セントラル・サイト)にのみルーティング
- 中央ゲートウェイにルーティングし、他のVPNコミュニティ・メンバーにルーティング
- 中央ゲートウェイにルーティングし、許可された場合に他のメンバーまたはインターネットにルーティング

VPNに対するQoS

VPN-1では、複数のセキュリティ機能が完全に統合されているため、ポリシー・ベースの帯域管理およびQoSも極めて有効に機能します。これらの機能により、暗号化処理による遅延の発生を最小限に抑えることができるため、VoIPなど遅延の影響を受けやすいアプリケーションも安心して利用できます。QoSポリシーは、次のような複数の手法を使用して定義できます。

- 他のトラフィックとの比較に基づく優先順位による重み付け
- 帯域の下限および上限の保証
- 低遅延キューイング(LLQ)
- DiffServグループ

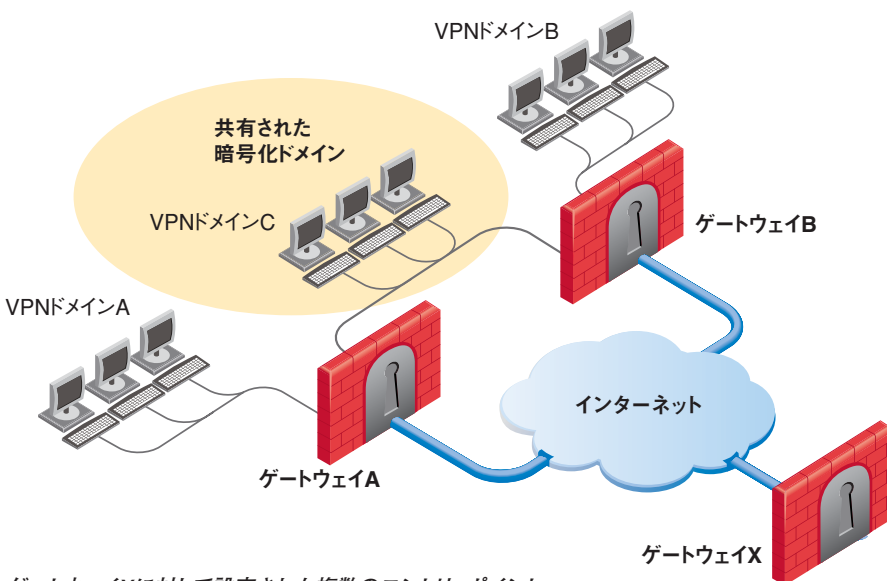
NAME	SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
VoIP								
VoIP Services	OWI-group	OWI-group	TCP SOCKS TCP SIP UDP SIP_UDP H323 H323_SIP H323_TMS H323_TMS_UDP	QoS Weight	- None	* All	* Any	
Site-to-Site VPN								
Site to Site VPN	OWI-group	OWI-group	GRE IPsec HTTP	QoS Weight	Log	* All	* Any	Prioritize VPN traffic between sites
Default	* Any	* Any	* Any	QoS Weight 10	- None	* All	* Any	

QoSポリシーの定義

ハイ・アベイラビリティおよびロード・シェアリングを可能にするMEP (複数のエン트리・ポイント)

MEP (Multiple Entry Point) は、VPNサービスに対しハイ・アベイラビリティおよびロード・シェアリングの機能を提供します。通常、VPNゲートウェイに障害が発生した場合、電子メールやVoIPなど、VPNゲートウェイの背後にある内部リソースはすべて使用できなくなります。MEPを使用するには、2台のVPN-1ゲートウェイがフレーム・リレーまたは専用線で内部的に接続され、どちらのVPN-1においても特定のリソースが暗号化ドメイン (VPNトンネルでトラフィックを暗号化する必要のある、ホストやサーバといった一連のリソース) に定義されている必要があります。MEPが有効になっている状態で一方のゲートウェイが使用不能になると、サイト間VPNのトラフィックは自動的にもう一方のゲートウェイに転送されます。ハイ・アベイラビリティ用に用いられる従来型のクラスタリング・ソリューションとは異なり、MEPでは、2台のゲートウェイは地理的に離れた場所 (例えば東京と大阪) に配置されていてもかまいません。

VPN-1では、従来型のハイ・アベイラビリティおよびクラスタリングもサポートされています。複数のVPN-1ゲートウェイを同じサイトに配置することで、VPNのパフォーマンスを向上させるアクティブ/アクティブのクラスタを設定できます。この場合、VPNセッションが1つのゲートウェイで開始されると、チェック・ポイントが特許を取得済みの技術ステートフル・インスペクション技術により、すべてのゲートウェイ間でそのセッションが同期されます。セッションを開始したゲートウェイが何らかの理由によって使用不能になった場合、そのセッションは自動的にクラスタの別のメンバーに引き継がれます。このとき、セッションを最初からやり直す必要はありません。



ゲートウェイXに対して設定された複数のエン트리・ポイント

従来型のVPNの問題：増加するリソースと動的化が進むネットワーク

従来型のVPNの構築方法は、暗号化ドメイン（VPNトンネルでトラフィックを暗号化する必要のある、各VPN機器の背後にあるリソース）を定義し、各ゲートウェイ間のルーティングを定義するというものです。規模が小さく静的なVPNである間は、この方法でも全く問題はありません。しかしながら、ネットワークの規模が拡大し、相互接続される動的なリソースが増えるにつれ、ドメイン・ベースのVPNはこれらに合わせて拡張することが困難になってきます。その理由は次のとおりです。

- リソース数の増加：VPNでアクセスするリソースが少ない数で安定している間は、ドメイン・ベースのVPNの運用に問題が生じることはありません。しかし、多数のオフィスからアクセスする必要のあるリソースが増え始めると、VPNドメインが徐々に大きくなり、適切に保守することが困難になってきます。
- ネットワークの規模拡大と動的リソースの増加：通常のネットワークでは、静的なルーティングに代わって動的なルーティングが主流になったことで、ルータ設定の簡素化とネットワークの信頼性向上が実現されました。しかしながら、従来型のVPNではリソース間のルーティングが静的に定義されているため、動的なルーティング環境に配置されているリソースにはうまく対応することができません。VPN接続されるオフィスの数が増えるにつれて、VPN機器間で必要となる静的ルートの数も大幅に増加してしまいます。

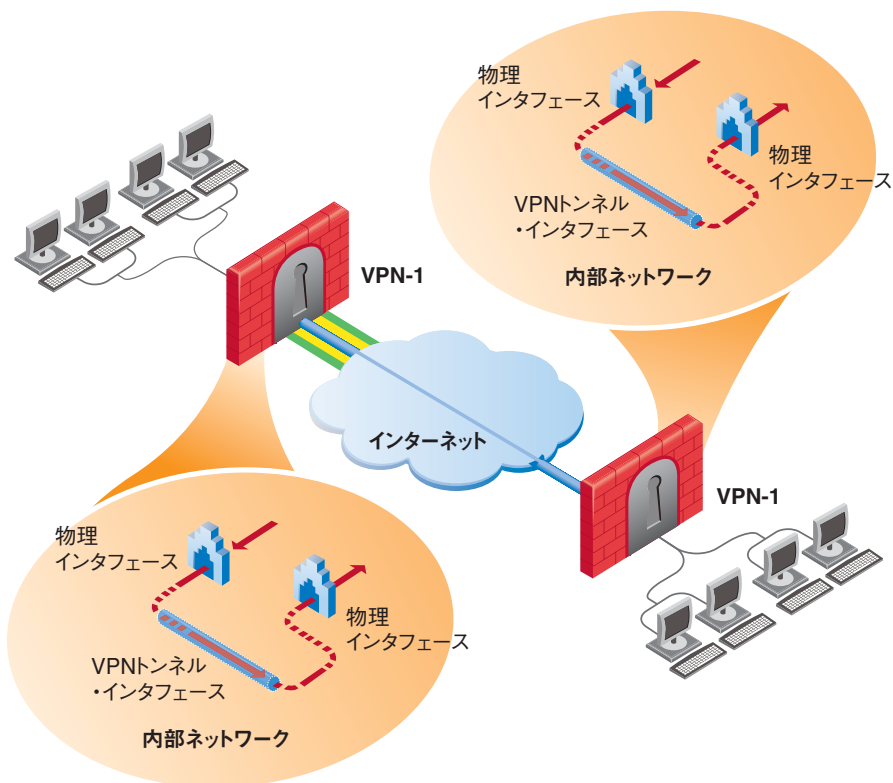
ルート・ベースのVPN：シンプルなルーティングによる複雑なVPNの構築

これらの問題を解決するのが、ルート・ベースのVPNです。ルート・ベースのVPNは、大規模なVPN環境の構築を容易にする、VPN-1の先進技術です。ルート・ベースのVPNがドメイン・ベースのVPNと最も異なっているのは、トラフィックを暗号化するかどうかの判断が、サブネットやホストなどの事前定義されたリソースではなく、IPルーティングに基づいて下されるという点です。

VPN-1では、VPNトンネル・インタフェース（VTI）を利用してVPN上の各サイト間の仮想ダイレクト・リンクを表すことで、これを実現します。各サイトは、VPNを通じた接続先となるVPN-1ゲートウェイに対応するVPNトンネル・インタフェースを保持しています。発信元のネットワークからVPNを介してリモート・オフィス宛てに送信されるパケットに対しては、次の処理が行われます。

1. アドレスX宛てのIPパケットについて、ルーティング・テーブルで照合が行われます。
2. ルーティング・テーブルにより、アドレスXは専用接続（VTI）を介してルーティングされることが示されます。
3. VPN-1がそのパケットを受信し、当該VPNで必要となるセキュリティ・パラメータを適用してから、宛先ゲートウェイのIPアドレスを挿入します。
4. パケットが物理インタフェースに再ルーティングされ、宛先のリモート・ゲートウェイに送信されます。

宛先のリモート・ゲートウェイでは、同じ処理が逆の順序で行われます。



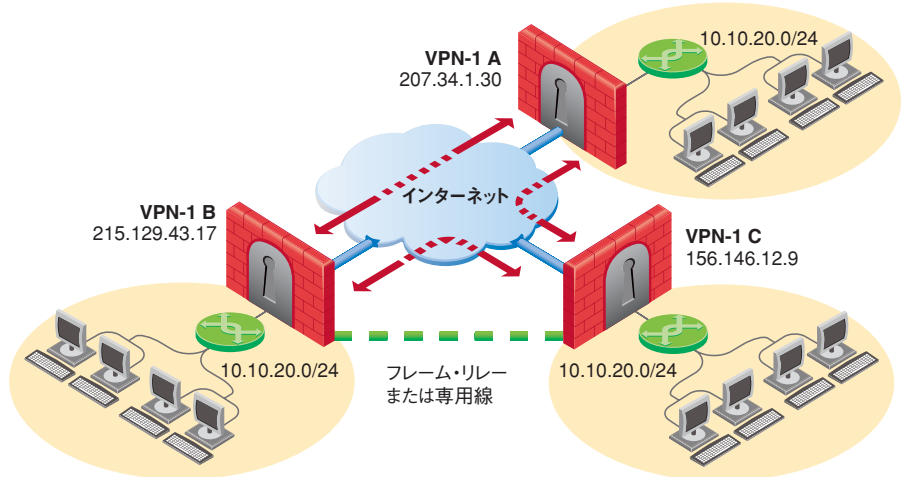
VPNトンネル・インタフェースを使用するルート・ベースのVPN

ルート・ベースのVPNでは、対応するVTI間で仮想接続を作成するのに、スタティック・ルーティングと動的・ルーティングの両方を使用できます。ただし、多数のサイトにまたがるVPNの安全性と信頼性を確保することに関しては、動的・ルーティングの方がスタティック・ルーティングよりもさまざまな点で優れています。

動的・ルーティングのサポート
OSPF
BGP
RIPv1
RIPv2

第1のメリットとしては、2台のVPN-1ゲートウェイが、保護対象となるネットワークのルーティング情報を交換し、それに基づいて動的にルートを変更できるという点が挙げられます。これにより、地理的に離れた場所にあるサイト同士が、フレーム・リレーや専用線などの論理的または物理的な専用接続がなくても、互いの動的・ルーティング・コミュニティに参加することが可能になります。さらに重要なのは、各VPN-1ゲートウェイが、暗号化されたトラフィックの最終的な宛先までの正しいルーティング方法を把握できることです。

次に、VPNの信頼性が向上するという点が挙げられます。例として、A、B、Cというサイトがそれぞれ、VTIを共有してルート・ベースのVPNを構築しているシナリオを考えてみます。この場合、サイトAとサイトBの間のリンクが使用不能になっても、サイトBは、サイトCがサイトAへのルートを持っていることを自動的に知ることができます。これは、MEPを使用したドメイン・ベースのVPNとは異なり、管理者による設定なしで自動的に行うことが可能です。



ルート・ベースのVPNとダイナミック・ルーティングを使用した、冗長性のあるVPN

しなやかなリスタート (Graceful Restart)

ダイナミック・ルーティングに関してVPN-1が提供する大きなメリットは、OSPFによるヒットレスなリスタート (Hitless Restart) / しなやかなリスタート (Graceful Restart) と、BGPによるしなやかなリスタートが可能であることです。これら2つのプロトコルは、通常はハイエンドのルータ製品にのみ搭載されている機能で、一時的なハードウェア障害 (再起動など) から素早く回復することを可能にします。例えば、ゲートウェイAがゲートウェイBと通信しようとしたときにゲートウェイBがダウンしていた場合、ゲートウェイAは通常、自身のルーティング・テーブルからそのルートを自動的に削除し、他のゲートウェイにもそのことを通知します。このため、ゲートウェイBが一時的にダウンしているだけの場合であっても、そのルートは他のゲートウェイでも連鎖反応的に削除されてしまいます。VPN-1では、ゲートウェイが一時的にダウンしている場合でも、そのルートは自動的に削除されず、しばらくの間は有効なルートとして扱われます。

マルチキャスト・プロトコルのサポート

ルート・ベースのVPNのダイナミック・ルーティングを使用するには、VPN上でのマルチキャスト・プロトコルの送信がサポートされるというメリットもあります。サイト間でビデオ会議アプリケーションなどが使用されることも多い現在、マルチキャスト・トラフィックを暗号化する機能はもはや必須とも言えます。VPN-1は、マルチキャスト・トラフィックの検査にも対応しているので、トラフィックの妥当性だけでなく、トラフィックに悪意あるコンテンツが含まれていないかどうか確認できます。

マルチキャスト・プロトコルのサポート
IGMP
PIM-SM
PIM-DM

多くの組織には、ドメイン・ベースのVPNとルート・ベースのVPNの両方を混在させて使用したいというニーズがあります。VPN-1ファミリは、ドメイン・ベースのVPNとルート・ベースのVPNの両方を使用できる高い柔軟性を備えています。これら2つのモードを同時に使用することもできるため、一方のモードから他方のモードへと段階的に移行することも可能です。

結論

チェック・ポイントのIPsec VPN技術は、「接続性を重視するネットワーク担当者とネットワークの保護を重視するセキュリティ担当者の両者のニーズを満たすものでなければならない」という理念に基づいています。IPsecベースのセキュリティ・ゲートウェイ製品であるVPN-1は、Fortune 100企業のすべてに導入されている実績あるセキュリティ機能と、複雑なVPNの構築および管理を容易にする先進の技術を組み合わせた、分散ネットワーク環境のための安全な接続機能を提供します。

Check Point Software Technologies Ltd.について

チェック・ポイント・ソフトウェア・テクノロジーズ・リミテッド (www.checkpoint.com) はインターネット・セキュリティにおけるトップ企業として、特に企業向けファイアウォール、コンシューマ向けインターネット・セキュリティ、およびVPNの世界市場においてマーケット・リーダーとして広く認められています。チェック・ポイントは、NGXプラットフォームを通じて、企業ネットワークおよびアプリケーション、遠隔勤務者、支店・支社環境、およびパートナー各社のエクストラネットのビジネス通信およびリソースを保護する、広範な境界、内部、Web、およびエンドポイント・セキュリティ・ソリューションのための統一されたセキュリティ・アーキテクチャを提供しています。チェック・ポイントのZoneAlarm Internet Security Suiteとその他のコンシューマ向けセキュリティ・ソリューションは、今日業界で最も高い評価を得ており、世界中で何百万人もユーザをハッカー、スパイウェア、ウイルス、および個人情報窃盗から未然に保護しています。またチェック・ポイントは、350社を超える各分野のトップベンダーが提供する“ベスト・オブ・ブリード”ソリューションとの統合および相互運用性を実現するフレームワークであるOPSEC (Open Platform for Security) により、自社ソリューションの能力をさらに拡大します。現在、チェック・ポイント・ソリューションは、世界88ヶ国、2200社を超えるパートナー・ネットワークを通じて販売、導入、サービス提供されています。チェック・ポイントの顧客には、Fortune 100社の全社と何万ものあらゆる規模の企業や組織が含まれています。

©2003-2006 Check Point Software Technologies Ltd. All rights reserved.

Check Point, Application Intelligence, Check Point Express, Check Point Express CI, Check Pointのロゴ, AlertAdvisor, ClusterXL, ConnectControl, Connectra, Cooperative Enforcement, Cooperative Security Alliance, CoSa, DefenseNet, Eventia, Eventia Analyzer, Eventia Reporter, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Hacker ID, IMsecure, INSPECT, INSPECT XL, Integrity, Integrity SecureClient, Integrity Clientless Security, InterSpect, IQ Engine, NG, NGX, Open Security Extension, OPSEC, OSFirewall, Policy Lifecycle Management, Provider-1, Safe@Office, SecureClient, SecureKnowledge, SecuRemote, SecurePlatform, SecurePlatform Pro, SecureServer, SecureUpdate, SecureXL, SecureXL Turbocard, SiteManager-1, SmartCenter, SmartCenter Express, SmartCenter Power, SmartCenter Pro, SmartCenter UTM, SmartConsole, SmartDashboard, SmartDefense, SmartDefense Advisor, Smarter Security, SmartL.S.M, SmartMap, SmartPortal, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, SofaWare, SSL Network Extender, Stateful Clustering, TrueVector, Turbocard, UAM, UserAuthority, User-to-Address Mapping, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Express, VPN-1 Express CI, VPN-1 Power, VPN-1 Power VSX, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 UTM, VPN-1 UTM Edge, VPN-1 VSX, Web Intelligence, ZoneAlarm, ZoneAlarm Anti-Spyware, ZoneAlarm Antivirus, ZoneAlarm Internet Security Suite, ZoneAlarm Pro, Zone Labs, Zone Labsのロゴは、Check Point Software Technologies Ltd. あるいはその関連会社の商標または登録商標です。その他の企業、製品名は各企業が所有する商標または登録商標です。本書で記載された製品は米国の特許No.5,606,668、5,835,726、6,496,935、6,873,988、および6,850,943により保護されています。その他の米国における特許や他の国における特許で保護されているか、出願中の可能性があります。

Bridging the gap between connectivity and security

P/N:502243-J 2006.9

※記載された製品仕様は予告無く変更される場合があります。



Check Point
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.

チェック・ポイント・ソフトウェア・テクノロジーズ株式会社
〒160-0022 東京都新宿区新宿5-5-3 建成新宿ビル6F
<http://www.checkpoint.co.jp/> E-mail: info_jp@checkpoint.com Tel: 03 (5367) 2500