

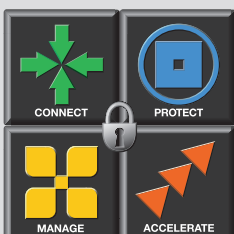
リモートVPNセッションのエンドツーエンド・セキュリティ

本書の内容

- 1 はじめに
- 2 リスクの認識
- 3 セキュリティ・ホールのパッチング
- 4 統合アプローチ
- 5 高い管理性能によるセキュリティの向上
- 6 まとめ

要点：

- リモート・アクセスにおけるセキュリティ・リスク
- パーソナル・ファイアウォールの必要性
- リモート・ユーザに対するエンドツーエンド・セキュリティの保証





はじめに



最近、ケーブル・モデムやDSLなどのインターネット・アクセスからVPNテクノロジーを使用し、社内ネットワーク・リソースにアクセスするリモート・ワーカーの数が増加しています。しかしながら、これらのブロードバンド・インターネット・サービスの「常時接続」環境において、各マシンは侵入の脅威に対し、門戸を開いたままの状態となり、その結果クライアントおよび企業ネットワークの両方が危険にさらされています。企業は、社内リソースへのアクセスに使用されているVPNセッションをハッカーの乗っ取りから防御するために、VPNクライアントにエンドツーエンド・セキュリティ・ソリューションを実装することとなります。

企業のセキュリティ管理者は、これらのリモート・ユーザのシステムを保護するために、一方的な「規定」から、高速接続の有益性を体験するユーザの可能性を阻害するポリシーの適用などさまざまな手法をとることができます。しかし、最良の方法は、必要なセキュリティを確保しながら、ユーザがブロードバンド・インターネット・サービスを十分活用できるような包括的なソリューションを周到に展開することです。

リスクの認識

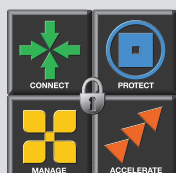
リモート・アクセスVPNは、幾つかの側面で企業にセキュリティ上のリスクをもたらす場合があります。まず、ビジネスに使用するマシンには、多くの場合、保護すべき企業データが保存されているため、ファイアウォールなどアクセス制御の手段を講じる必要があります。次に、社員のマシンとの間で交換されるデータを保護する必要があります。データの保護はVPN本来の目的ですが、常時接続のブロードバンド・サービスを使用することにより、長時間のVPNセッションが攻撃されやすくなるため、リスクがより深刻に広範囲に及びます。さらに、社員のPCを保護する最大の理由は、長期間潜伏して活動するトロイの木馬プログラムなどがPCに侵入することを防御するためです。たとえば、ハッカーがユーザの入力内容をすべて取得するプログラムを、インターネットに接続された無防備なPCに送り込んだとします。その結果、社内VPNで使用されるユーザ・パスワードがハッカーの手に渡った場合、VPNの目的は果たせなくなります。また、別の危険なタイプのトロイの木馬プログラムは、無防備なPCを密かに分散サービス拒否 (DDoS) 攻撃の攻撃者 (ゾンビ) として登録し利用します。

ネットワーク・セキュリティ管理者がこれらに関する認識を深めるにつれ、エンド・ツー・エンドの企業セキュリティ・ソリューションの必要性が明白となります。では、この問題に対処するのに最適なのはどのような方法でしょうか？

セキュリティ・ホールのパッチング

VPNクライアントを保護する方法の1つは、ユーザが個別に管理するパーソナル・ファイアウォールのインストールをユーザに義務づける企業方針を定めることです。この種のソリューションは、現在、市場で数多く販売されています。しかし、この方法では、エンド・ユーザにパーソナル・ファイアウォールのインストール、構成、管理などの重い負担を必要とします。また、必要なサポートやトレーニングの提供が困難であり、セキュリティの徹底において現実的ではありません。

別の解決方法として、中央で管理するパーソナル・ファイアウォールを導入し個々のマシンを保護することが考えられます。しかし、この方法には、VPNセッションを確立する前にユーザがパーソナル・ファイアウォールの設定を無効にするのを防ぐことや設定を変更できないようにする手段がありません。VPNクライアントとファイアウォール製品を統合しない限り、クライアント・マシンにおいてパーソナル・ファイアウォールを確実に動作させる方法がありません。セキュリティ管理やエンド・ユーザの知識不足が、VPNトンネルのセキュリティを損う恐れがあり、ネットワーク全体のセキュリティが脅かされる結果になります。





また、リモート・アクセスVPN接続とデスクトップ・セキュリティに2つの異なる製品を展開する場合、組織は関連する管理コストを検討しなければなりません。VPNクライアントまたはデスクトップ・ファイアウォールの新しいリリースすべてに関して、互換性を確認する必要があります。また、独立したクライアント・セキュリティ製品を複数使用する場合、ネットワーク・セキュリティ管理者は、新規ユーザの追加に必要なタスク、またはVPNユーザ全員に対して両ソリューションの企業セキュリティ・ポリシーを更新する際に必要なタスクなど、拡張性や管理などの問題を考慮する必要があります。

統合アプローチ

しかし、今日では、デスクトップ・セキュリティ機能とVPNクライアント・ソリューションを緊密に統合させたソリューションがあり、このアプローチにはさまざまな利点があります。たとえば、統合されたファイアウォールとVPNクライアントでは、すべてのエンド・ユーザ・マシンで自動的にセキュリティが実施されます。VPNはクライアント側の暗号化およびユーザ認証により一般的な接続性を提供しますが、これらのソリューションはさらにアクセス制御やクライアント・セキュリティを保証する制御などの強力なセキュリティ機能も提供します。これらの機能により、管理者は中央管理によりクライアント・セキュリティ・ポリシーを実施し、クライアントにルールベースのアクセス制御を課し、異なるユーザ・グループに異なるポリシーを指定することなどが可能です。営業担当者やITスタッフなど、さまざまなタイプのリモート・アクセスVPNユーザがいる組織は、多様なユーザのニーズに合わせてデスクトップ・セキュリティ・ポリシーを作成することができます。

このようなソリューションにおける他の利点は、クライアントに特定のアプリケーションがインストールされているかどうか、またはWindowsレジストリの値など、クライアント・マシンのさまざまな条件を確認可能なWindowsの“.dll”ファイルを使用したセキュリティ・チェックをカスタマイズし実施するようにネットワーク・セキュリティを拡張できることです。図1に示すように、セキュリティ・チェックにパスすることを、VPN接続の確立をクライアントに許可する条件として使用することができます。たとえば、クライアント・マシンとVPNセッションを確立する前に、そのマシンのアンチウイルス・ソリューションが最新の状態に更新されていることを確認するようにソリューションを構成し、クライアントと企業ネットワークを有害なウイルスから保護することができます。

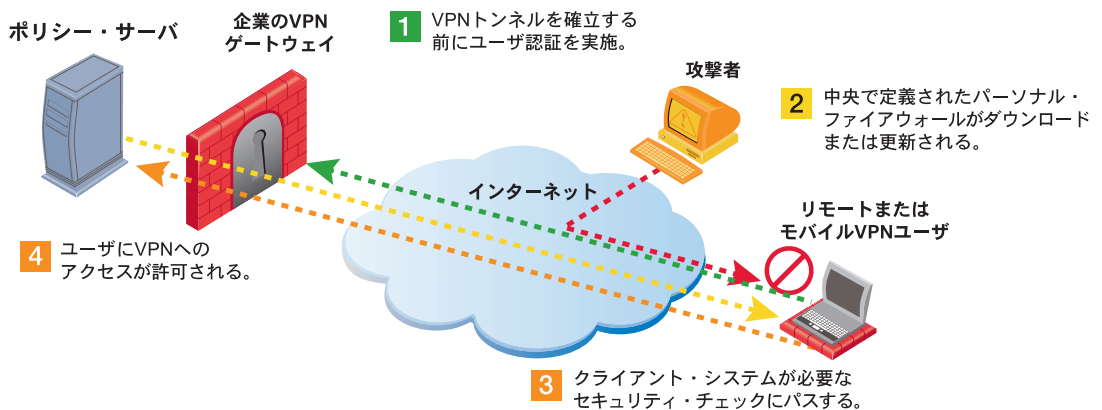
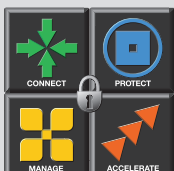


図1: VPNクライアントに対する包括的なセキュリティ

高い管理性能によるセキュリティの向上

管理が困難なクライアント・セキュリティ・ソリューションでは、必要なレベルのセキュリティが提供されていないため、多数のリモート・ユーザの展開および管理を支援する機能を備えた製品を探すことが重要です。たとえば、クライアント・ソフトウェアのセットアップが難しいと、多くのユーザがシステムを誤って構成し、期待するレベルのセキュリティが確保されません。VPNベンダの中には、自己解凍および自動実行





を行い、クライアント・システムに自動的にインストールされるツールを提供するベンダがあります。このようなツールを使用すると、エンド・ユーザは専門的な知識や作業も必要がないため、社内ヘルプデスクのサポート・コストが最小限にできるに加え、ソフトウェアは常に正しくセットアップされます。

同様に、組織はクライアント・ソフトウェアが最新の状態でない場合に自動的に更新する製品を探し、必要なすべてのソフトウェアを常に最新の状態に保ち、クライアント・セキュリティを大幅に向上させる必要があります。新しいソフトウェア・コンポーネントは、透過的にクライアントにプッシュダウンされて適用され、必要に応じてサービスやマシンが自動的に再起動されることが望まれます。

まとめ

組織は、リモート・アクセスVPNの真の利点を実現するために、選択したテクノロジーがVPNクライアントに包括的なセキュリティを提供することを確認する必要があります。暗号化や認証などの標準的なVPN機能は、VPNユーザとの間の通信を保護しますが、エンド・ユーザが使用するマシンの保護も企業の全体的なセキュリティにとって重要な要件です。クライアント・システムは、VPN自体と緊密に統合されるパーソナル・ファイアウォール技術で保護する必要があります。包括的なVPNソリューションは、VPN接続の条件として、VPNクライアントにセキュリティ要件を実施させる機能を備えていなければなりません。VPNクライアントが保護されて初めて、組織はネットワークのセキュリティが万全であると考えることができます。

チェック・ポイント・ソフトウェア・テクノロジーズについて

チェック・ポイント・ソフトウェア・テクノロジーズは、インターネット・セキュリティ分野において世界をリードする企業で、VPNおよびファイアウォールの世界市場でマーケット・リーダーとして認められています。同社のセキュア・バーチャル・ネットワーク (SVN) アーキテクチャは、独自の技術により、安全で信頼性の高いインターネット通信を可能にするVPNおよびセキュリティのインフラストラクチャを提供します。SVNソリューションは、同社の次世代製品ファミリに組み込まれて、企業ネットワーク、リモート接続する社員、ブランチ・オフィス、パートナーを結ぶエクストラネットにおけるビジネス通信とリソースを保護します。SVNの機能を拡張したものがチェック・ポイントのOPSEC (Open Platform for Security) で、業界をリードする300社以上の最高品質のソリューションを統合、相互運用するための業界のフレームワークを提供します。チェック・ポイントのソリューションは、203カ国で認定された2,500社のパートナーによって販売、統合、保守が行われています。詳細については、(800) 429-4391または(650) 628-2000にお問い合わせいただくか、チェック・ポイントのWebサイト (<http://www.checkpoint.com>または<http://www.opsec.com>) をご覧ください。

連絡先：

インターナショナル本社：
3A Jabotinsky Street, 24 th Floor
Ramat Gan 52520, Israel
Tel: 972-3-753 4555
Fax: 972-3-575 9256
e-mail: info@Checkpoint.com

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
東京都新宿区新宿5-5-3
建成新宿ビル6F
Tel: 03-5367-2500 (代表)
Fax: 03-5367-2501
e-mail: info@checkpoint.co.jp
URL: <http://www.checkpoint.co.jp>

© 2002 Check Point Software Technologies Ltd. All rights reserved. Check Point, Check Pointのロゴ、FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FireWall-1 SmallOffice, FireWall-1 VSX, FireWall-1 XL, FloodGate-1, INSPECT, INSPECT XL, IQ Engine, Open Security Extension, OPSEC, Provider-1, SecureKnowledge, SecurePlatform, SecureXL, SiteManager-1, SmartCenter, SmartCenter Pro, SmartDashboard, SmartDefense, SmartLSM, SmartMap, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartView Tracker, SVN, UAM, User-to-Address Mapping, UserAuthority, VPN-1, VPN-1 Accelerator Card, VPN-1 Net, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 SmallOffice, およびVPN-1 VSXは、Check Point Software Technologies Ltd.およびその関連会社の商標、サービス・マークまたは登録商標です。その他の製品名は、各企業が所有する商標または登録商標です。本文で記載された製品は、米国の特許No. 5,606,668および5,835,726によって保護されています。また、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、特許出願中の可能性があります。
* 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。
P/N 501145

