



Unified Threat Management (UTM)

次世代の統合脅威管理デバイスによるネットワークの保護



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

はじめに	3
今日のUTMデバイス	3
今日のUTMデバイスの課題	4
次世代のUTMデバイス	4
セキュリティ機能の拡張	4
さまざまなデバイスの管理	4
データの機密性	5
チェック・ポイントが提供する次世代のUTMデバイス	5
結論	6

はじめに

インターネットはもはや、どのような規模の企業にとっても、安全にビジネスを行える空間ではなくなっています。ウイルスやスパイウェアが溢れ、分散サービス妨害 (DDoS) 攻撃などの卑劣な手段によってネットワークをダウンさせようと企むハッカーたちが至るところに潜んでいます。つまり、企業ネットワークにとっての脅威は増える一方の状況となっているのです。実際、IT業界を対象とする市場調査会社における最近の調査でも、ネットワーク・セキュリティを巡る状況は悪化する一方であることが明らかになっています。

IDCの「Enterprise Security Survey 2005」では、調査対象となった473社のうちの40パーセント近くが実際の被害を伴う攻撃を受けたことがあると回答し、従業員数が1,000人を超える企業160社のうちの半分以上が被害を伴う攻撃を11回以上受けたことがあると回答しています。またInformationWeekの「U.S. Information Security 2005」でも、調査対象となったIT担当者2,540人のうちの67パーセントが、2004年8月から2005年8月の間に自社を対象とするウイルスの攻撃を受けたことがあると回答しています。こうした結果は、この2つの調査に限りません。これらのデータを見れば、状況が悪化していることは一目瞭然です。

常に変化し続ける脅威と、次々に出現する新たなセキュリティ上の課題に直面している今日の企業は、ネットワークを常に安全な状態に維持することのできるセキュリティ・ソリューションを必要としています。しかしながら、これらのソリューションの導入は容易ではなく、また多くの企業には、高いレベルのセキュリティを実現するために必要とされる複数のポイント・ソリューションを購入するだけの財政的な余裕がありません。そのうえ、ポイント・ソリューションの多くは運用管理に手間がかかるため、購入することができたとしても、その管理に人員を割かなければならず、さらなる負担増を強いられることとなります。

そのため現在では、あらゆる規模の企業において、低価格で管理が容易ながらも最高レベルのセキュリティを提供するシンプルなオールインワン・ソリューションが求められるようになってきました。こうしたニーズに応えるために最近登場したのが、統合脅威管理 (UTM) と呼ばれる新しいタイプのセキュリティ・ソリューションです。UTMは、企業のネットワーク環境を保護するために必要なコストを削減し、その複雑さを軽減するための各種のセキュリティ機能が統合されたシンプルなオールインワン型のソリューションです。

今日のUTMデバイス

現在、各ベンダーから提供されているUTMデバイスの多くは、基本的なファイアウォール、侵入防御、およびアンチウイルスの各機能を1つのデバイスに統合するオールインワン型のアプローチを採用しています。価格はターゲットとする規模により数万円から数十万円までさまざまですが、いずれもプラグ・アンド・プレイで、つまりIT担当者やサポート・スタッフがなくても(あるいはわずかなサポートで)簡単に導入できるような設計になっています。また製品によっては、アンチスパイウェアやWebセキュリティなどの機能が搭載されている場合もあります。

これらのオールインワン・アプライアンスにはさまざまなメリットがあります。まず、セキュリティが必要になったとき、セキュリティが必要な場所にすぐに導入できるという点が挙げられます。次に、幅広いセキュリティ機能が統合されているため、複数のポイント・ソリューションを導入・管理せずに済むことがあります。さらには、使いやすさを重視した設計になっていることから、多くの場合、設置後わずかな設定作業でセキュリティ機能を有効にできるというメリットもあります。またほとんどのUTMデバイスでは、幅広い管理オプションを提供することで、セキュリティに関する作業をできる限り少なくしたいと考えている企業のニーズに応えています。

今日のUTMデバイスの課題

とは言え、現在のUTMデバイスに欠点がないというわけではありません。UTMデバイスが登場し、実際の環境で運用され始めてから3年ほどになるところで、顧客や専門家から現在のUTMデバイスが抱える問題点や課題が指摘され始めています。最も大きな課題の1つは、保守に関するものです。セキュリティ上の脅威は極めて速いペースで進化を遂げているため、新たな脅威へ常に対応するために、定期的なアップデートが必要となりますが、多くのベンダーのデバイスではこのプロセスの自動化や集中化が行われていません。アップデートを手動で行うということは、そのぶん人間の介在が必要になるということです。これは、そもそもUTMデバイスが極力排除しようとしていたことの1つであり、これによって効率性と生産性が低下することになります。

管理に関する課題もあります。UTMデバイスを導入することによって、企業で必要となるポイント・ソリューションを減らすことができるのは確かですが、UTMデバイスの数が数百台から数千台ともなれば、その管理に大変な労力が必要とされます。またWebアプリケーション・ファイアウォール、SSL VPNゲートウェイ、エンドポイント・セキュリティのクライアントおよび他のセキュリティ・デバイスなどについても管理が必要になります。これらを管理するための機能は、従来型のUTMデバイスでは全く考慮されていません。このような異機種のセキュリティ・デバイスやソフトウェアを管理することは、特に脅威の監視やレポートと言った面で困難な場合があります。さらに問題となるのは、今後出現する脅威に対処するために、さらなるセキュリティ機能をUTMデバイスに統合していく必要があることです。これらの問題や課題を解決するためには、セキュリティ機能をシームレスに組み込み、統合することのできるフレームワークが必要になります。

次世代のUTMデバイス

第1世代のUTMデバイスの主な目的は、複数のポイント・ソリューションを1つのフレームワークに統合することにあります。次世代のUTMデバイスには、セキュリティ機能を拡張すると同時に、管理作業に伴う負担とコストをコントロールすることが求められます。

セキュリティ機能の拡張

従来のUTMデバイスが提供する機能は、ファイアウォール、侵入防御、およびアンチウイルスに限定されることがほとんどでした。次世代のUTMデバイスでは、これらに加えて、Webアプリケーション・ファイアウォール、アンチスパイウェア、IPSec VPN/SSL VPNなどの機能を統合することが必要になります。これらを取り組むことにより、機能面においては、企業ネットワークを保護するために必要な機能が拡充されます。また次世代のUTMデバイスでは、さらに次のような機能も必要になります。

- VoIP (Voice over IP) 用のセキュリティ機能
- インスタント・メッセージングおよびP2Pアプリケーションの管理機能
- ワーム対策機能

さまざまなデバイスの管理

次世代のUTMデバイスには、従来のポイント・ソリューションや既存のUTMデバイスと連携して、包括的で一貫性のあるセキュリティ環境を構築できることも求められます。第1世代のUTMデバイスは、複数のセキュリティ機能を1つのデバイスに統合することだけを目的としていましたが、次世代のUTMデバイスでは、さまざまな異なるセキュリティ・デバイスも1つの管理コンソールの下に統合することで、管理環境全体の簡素化を実現できなければなりません。これにより、管理者の負担を大幅に軽減し、設定ミスが発生する可能性を低く抑えると同時に、ネットワーク全体にわたって一貫したセキュリティ・ポリシーを適用することが可能になります。

従来のUTMデバイスはネットワークのコアのみを保護の対象としていますが、次世代のUTMデバイスではネットワークの隅々にわたり — コアと境界、およびその間にあるあらゆるポイント — が保護の対象となります。ネットワークの強度は、セキュリティが最も弱いポイントの強度に依存するため、ネットワーク管理者は、ネットワーク全体で同じレベルのセキュリティが保たれるようにしなければなりません。そのためUTMデバイスでは、エンドポイントを常に最新の状態に維持できるように、セキュリティに不備のあるエンドポイントを隔離して強制的に最新のアップデートをインストールさせるといった機能が備わっていることも重要になります。

データの機密性

次世代のUTMデバイスには、最新のVPN技術（転送中のデータに強度の高い暗号化アルゴリズムを適用するといった、データの機密性を維持するための機能など）も統合されることになります。これらのデバイスでは、128~256ビットのAES (Advanced Encryption Standard)、56~168ビット・トリプルDES、およびSSLプロトコルに対応している必要があります。これらの機能と、セキュリティ・ポリシーの複数の要素を定義および管理する機能とを組み合わせることにより、かつてないほど柔軟にデータを制御することが可能になります（ただしこれは、セキュリティという意味ではオプション的な機能です）。

チェック・ポイントが提供する次世代のUTMデバイス

チェック・ポイントは、このような次世代のUTMデバイスをすでに提供しています。チェック・ポイントのフラッグシップUTM製品であるVPN-1® UTM™には、ファイアウォール、侵入防御、アンチウイルス、アンチスパイウェア、Webアプリケーション・ファイアウォール、およびIPSec VPN/SSL VPNの各機能が統合されています。VPN-1 UTMは、あらゆる規模の企業に対応できる拡張性を備え、Fortune 100企業で採用されている実績あるチェック・ポイントの技術を搭載しています。

また、支社・支店などの比較的小規模なリモート・サイト向けUTMアプライアンスとして、VPN-1 UTM Edge™シリーズも用意されています。VPN-1 UTM Edgeにより、支社・支店環境においても本社と同じレベルのセキュリティを維持できるようになるため、これらの環境が企業ネットワークへの踏み台として利用されることを防ぐことができます。

チェック・ポイントは、先進の管理ソリューションであるSmartCenter™を通じて、チェック・ポイントのUTM製品群およびその他のチェック・ポイント製品を一元的に管理、アップデート、および監視できるようにしています。このため、VPN-1 UTMゲートウェイとVPN-1 UTM Edgeアプライアンスを、他のチェック・ポイント製品と共に単一のコンソールから管理することが可能です。管理作業を単一のコンソールから行えるということは、サイト全体にわたって確実に、迅速に、そして頻繁にセキュリティ・アップデートを実施できるということです。そして、頻繁にアップデートを行えるということは、ネットワークがより安全になるということを示します。

チェック・ポイントの集中管理機能は、ネットワーク全体へのセキュリティ・ポリシーの配布を集中化することにより、管理に関する最大の問題を解決します。つまり管理者は、複数の製品および複数のサイトのセキュリティ・ポリシーを一元的に管理できるようになるのです。これにより、組織全体のセキュリティの一貫性が向上するほか、組織のセキュリティ状況の全体像を把握することが可能になります。ネットワークのセキュリティをより広い視野で把握できるので、管理者は、リアルタイムで効率的にセキュリティ上の問題に対処できるようになります。

またチェック・ポイントのUTMデバイスは、ハイ・アベイラビリティ機能を内蔵することにより、大規模企業で求められるレベルの可用性を実現しています。ゲートウェイの冗長構成とバックアップ用ISPリンクの追加に対応するほか、すべてのゲートウェイの状態を監視して稼働状況をチェックできる管理機能も備えています。

結論

増加する一方のセキュリティ上の脅威に悩まされながらもその対策に十分なリソースを割くことのできない企業は、その規模を問わず、機能の統合と管理の簡素化を実現したUTMソリューションを導入することによって、大きなメリットを得ることができます。現在、さまざまなUTMソリューションが続々と登場していますが、チェック・ポイントが提供するソリューションは、実績ある各種のセキュリティ機能を統合し、複数のサイトに配置されたセキュリティ機器の管理、アップデート、およびレポートを一元化することによって、セキュリティ環境の簡素化を実現します。チェック・ポイントのソリューションは、セキュリティ管理に要する時間とコストを削減します。そして、セキュリティ・ソリューションとして最も重要なことですが、ネットワークを確実に保護します。チェック・ポイントのソリューションは、企業を取り巻く環境が激しく変化する中、ネットワークが確実に保護されるという安心感をCIOやITマネージャにもたらしめます。

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のロゴ, AlertAdvisor, ClusterXL, Cooperative Enforcement, ConnectControl, Connectra, CoSa, Cooperative Security Alliance, DefenseNet, Eventia, Eventia Analyzer, Eventia Reporter, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Hacker ID, IMsecure, INSPECT, INSPECT XL, Integrity, InterSpect, IQ Engine, NGX, Open Security Extension, OPSEC, OSFirewall, Policy Lifecycle Management, Provider-1, Safe@Office, SecureClient, SecureKnowledge, SecurePlatform, SecuRemote, SecureXL Turbocard, SecureServer, SecureUpdate, SecureXL, SiteManager-1, SmartCenter, SmartCenter Power, SmartCenter Pro, SmartCenter UTM, Smarter Security, SmartDashboard, SmartDefense, SmartDefense Advisor, SmartLSM, SmartMap, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, SofaWare, SSL Network Extender, Stateful Clustering, TrueVector, Turbocard, UAM, User-to-Address Mapping, UserAuthority, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 UTM Edge, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 UTM, VPN-1 Power, VPN-1 SecureServer, VPN-1 VSX, VPN-1 Power VSX, Web Intelligence, ZoneAlarm, ZoneAlarm Pro, ZoneAlarm Antivirus, ZoneAlarm Anti-Spyware, ZoneAlarm Internet Security Suite, 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。本書に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。

Unified Threat Management

P/N:502165-J 2006.8

※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