



2005年2月

Check Point Software  
Technologies委託の  
ホワイトペーパー

文書番号205101

## 統合化されたアプリケーション・ セキュリティ・ソリューションによる セキュリティ投資収益率の向上

Check Pointは、CiscoやJuniperに比べ、単一のゲートウェイを使用して、境界部分でより多くのアプリケーションを先制的に保護し、高いセキュリティ投資収益率をもたらします。

## ライセンス使用許諾情報と適切な利用について

Entire contents ©2005 The Tolly Group, Inc. All rights reserved.



本文書( Tolly Group文書番号205101 )の適切な利用に関する詳細をご希望の方は、The Tolly Groupまで電話( 米国561-391-5610 )または電子メール( sales@tolly.com )にてお問い合わせください。

書面による事前の許可なしに、この出版物をいかなる形式によっても複製することを禁じます。本書に記載されている情報は、正確さと信頼性を期していますが、The Tolly Groupは、本書に記載されている情報の誤り、欠落、不備、またはその解釈に対して一切責任を負いません。

本報告書の抜粋を公開したり公共の資料に使用したりする場合は、必ず事前にThe Tolly Groupの承認を得る必要があります。



## Tolly Groupのサービス

最先端の情報技術( IT )製品とサービスの検証で15年以上の経験があるThe Tolly Groupは、正確かつ公平な評価や分析で世界的な評価を得ています。弊社は、実績あるテスト方法と公正なテスト方針を採用し、高い精度で製品・サービスのベンチマーク評価を行います。



2003年に始まったThe Tolly Groupの「Tolly Verified ( Tolly認定 )」は、WLANスイッチングからアンチスパムまで、広範な技術分野の数々の特性、機能、パフォーマンス特徴を、ベンダに偏らない中立的な立場から詳しく認証するサービスです。「Tolly Verified」ホームページをご覧ください。



弊社の「Up-to-Spec」サービスは、「Tolly Verified」で行われる「標準」の細分化されたテストを補足するカスタム・テストです。詳細は、「Up-to-Spec」ホームページをご覧ください。

The Tolly Groupは、特定の領域のみに特化した検証機関と異なり、保有する膨大な技術的知識を重点的マーケティング・サービスと組み合わせ、お客様が製品ベンチマークをより良く位置づけ、製品露出の機会を最大限に増やすことができるようお手伝いします。

## 本文書の作成者

ケビン・トリー( Kevin Tolly )  
The Tolly Group 社長兼CEO

チャールズ・ブルーノ( Charles Bruno )  
The Tolly Group 編集責任者

## 目次

- 4 エクスプロイトによって進む革新
- 5 統合化された侵入保護機能
- 9 アーキテクチャによる防御の深さ
- 12 セキュリティの総コスト
- 14 セキュリティへのインテリジェントなアプローチ

## 図のリスト

- 7 図1. テスト結果表 Check Pointの VPN-1 NGシリーズとCisco PIX515E、  
およびJuniper NetScreen-204との比較
- 12 図2. 単一サイト複合型ファイアウォール/IPSソリューションのTCO(総所有コスト)比較

# 統合化されたアプリケーション・セキュリティ・ソリューションによるセキュリティ投資収益率の向上

## エクスプロイトによって進む革新

エンタープライズ・クラスのネットワーク・セキュリティに関しては、ファイアウォールとVPNがネットワーク境界部のセキュリティの根本要素として確固たる地位を長年築いてきました。およそ65,000はあるであろうTCPのエントリ・ポイントで不要なポートをブロックすることにかけては、ファイアウォールは確かに優れています。しかし、すべてのポートを閉じてビジネスを行うことは不可能です。ハッカーはそのことをよく知っています。

アクセスをブロックするファイアウォールの有効性に気づいたハッカーは、巧みに戦略を変更し、まったく新しい革新的なエクスプロイトを採用しつつあります。

現在、ハッカーは、正規の企業通信プロトコルのトラフィック・ストリームの内部に巧妙に「エクスプロイト」(攻撃)を隠して、ネットワーク境界への侵入を試みています。今日、攻撃は、セキュアWebアクセス(SSL)や電子メール(SMTP)、データベース・アクセス(SQL)など、重要なアプリケーション全体に仕掛けられるようになっています。

ハッカーは、開いているポートを攻撃して以前のネットワーク・データにアクセスする方法に頼らずに、アプリケーションを輸送機関のように使用して重要なデータ・ストアにアクセスしています。ハッカーがアプリケーションを狙うようになったのは、従来のファイアウォールがアプリケーション・レベルの攻撃を検出して阻止できる設計になっていないためです。

ハッカーは、アプリケーションを介した攻撃によって、次のような目標を達成しようとしています。

- 正規ユーザへのサービス拒否(DoS サービス妨害)

- サーバやクライアントへの管理者アクセスの取得

- バックエンドの情報データベースへのアクセスの取得

- セキュリティを迂回してアプリケーションにアクセスできるようにする  
トロイの木馬ソフトウェアのインストール

- 「スニファ」モードで実行され、ユーザIDやパスワードを捕らえる  
ソフトウェアのサーバへのインストール

セキュリティ・ベンダは、このような巧みな攻撃に対して、侵入検知システムや侵入防止システム (IDS/IPS)を開発したり、アプリケーション動作を監視して理解し、その知識を活用するなどの方法で、攻撃や脅威を防ごうとしてきました。

Application Intelligenceは、アプリケーションによって使用されているプロトコルを把握し、プロトコルの実際また可能性のある制限を認識することで、セキュリティ攻略が示す特徴を見極めることのできるソフトウェア・ベースの技術です。そのため、脆弱だと思われる部分を狙う攻撃が、特定のファイアウォール・ポートをくぐり抜け、一定サイズを超えるペイロードを含む場合、そのような条件に合ったトラフィックを探すようにソフトウェアを調整することができます。該当するトラフィックが見つかった場合、そのトラフィックはドロップすることができます。

## 統合化された侵入防御

セキュリティ企業は、脅威が業務の効率を低下させたり、ひどい場合には業務に悪影響を及ぼして支障をきたすような事態を招く前に脅威を識別し、それに対処するためには、ファイアウォールとVPNの機能とともに、いわゆる「侵入防御」技術を組み合わせる必要があることを認識しています。

また、ビジネスの観点からも、複数の機能や管理の制御をシングル・ボックスに集中させることにより総所有コストの削減を図る技術統合は理にかなっています。これにより、先行投資となるセキュリティ導入コストや継続的な管理費用を抑制することができます。

スタンドアロン型のIDS/IPS製品が市場に到来し、ユーザは既にインストールされている信頼できるファイアウォール/VPNデバイスに加えて、境界セキュリティ・ボックスの追加採用の検討に迫られることが多くなりました。しかし、これは多額の追加コストを要し、ネットワークをより複雑にするものでした。管理者は、管理インタフェースの知識をまた新たに習得し、さらに新たなセキュリティ・デバイス層を物理的に管理しなければなりませんでした。

スタンドアロンのIDS/IPSに代わるものとして、シングル・ボックスでファイアウォール、VPN、侵入防御サービスが実行可能なマルチレイヤ・セキュリティ・デバイスがあります。さまざまなベンダが提供しているシングル・ボックスのソリューションが、すべて同じレベルの機能を提供すると考えているユーザは少なくありません。

しかしそれは事実ではありません。セキュリティ・デバイスとそのIDS/IPS機能は、ベンダによって大きな格差があります。

The Tolly Groupは、業界をリードするセキュリティ・ソリューション・サプライヤのひとつであるCheck Point Software Technologiesの依頼で、他社製品と比較した場合の、同社のCheck Point VPN-1 NGシリーズのファイアウォールに装備されたApplication Intelligenceの優れた有効性を証明し、脅威となるセキュリティ・エクスプロイトにそれぞれの製品がどう対処するかを示す一連のテストを実施しました。Check Pointは、Web環境向けに構築されたソフトウェア・アプリケーションで、多くの場合セキュリティが重要視されていないことを認識しています。大きな被害をもたらしたBlasterと呼ばれるセキュリティ・エクスプロイトは、このことを示す絶好の例です。Blasterは、RPC(遠隔手続き呼び出し)プロトコルを使用して送信されるメッセージを処理するDCOM(分散COM)インタフェースを攻撃することにより、MicrosoftのWindowsオペレーティング・システムに広範囲に存在した脆弱性を悪用しました。

## INSPECTエンジンが処理を促進

Check Point VPN-1 NGシリーズ・デバイスは、同社が特許を取得したStateful Inspection技術とINSPECTエンジンをベースとしたアーキテクチャに基づいています。INSPECTエンジンは、常駐するホスト・ゲートウェイ上でセキュリティ・ポリシーを実施し、処理するトラフィックのさまざまな通信層から必要な情報を抽出します。

INSPECTエンジンは、オペレーティングシステム・カーネルのデータリンク層とネットワーク層(第2層と第3層)の間に、動的にロードされます。データリンクは実際のネットワーク・インタフェース・カード(NIC)であり、ネットワークリンクはプロトコル・スタック(たとえばIP)の第1層であるため、Check PointのINSPECTエンジンは最下位のソフトウェア層に位置します。この層で検査を行うことで、INSPECTエンジンはすべてのインタフェース上の着信および発信パケットを確実に捕捉し検査します。パケットがどのような通信プロトコルやアプリケーション・プロトコルを使用するものであっても、INSPECTエンジンが最初にそのパケットがセキュリティ・ポリシーに適合するものであると判断しない限り、いかなるパケットも上位のプロトコル・スタック層で処理されることはありません。

INSPECTエンジンは「生のメッセージ」にアクセスするので、メッセージ内のすべての情報を検査できます。たとえば、上位のすべての通信層に関する情報や、メッセージ・データ自体(通信やアプリケーションより導き出された状態情報とコンテキスト)も検査できます。INSPECTエンジンは、定義されているセキュリティ・ポリシーに従って、パケットを受理するかどうかを決定するために、IPアドレス、ポート番号、およびその他必要な情報を検査します。

このようにINSPECTエンジンはパケットの内部を見ることができ、アプリケーション内の一部のコマンドだけを許可し、他のコマンドを拒否することができます。たとえば、INSPECTエンジンは、ICMP pingを許可する一方でリダイレクトは拒否したり、あるいはSNMPのgetを許可する一方でsetは拒否する、といったことが可能です。INSPECTエンジンは、値をテーブル形式で保管・検索でき(これにより動的なコンテキストが与えられる)パケットの任意部分のデータに対して論理演算や算術演算が実行できます。

Check PointのStateful Inspection アーキテクチャに関する詳細は、次のリンクを参照してください。

[http://www.checkpoint.co.jp/data/Stateful\\_Inspection.pdf](http://www.checkpoint.co.jp/data/Stateful_Inspection.pdf)

[http://www.checkpoint.com/products/downloads/Stateful\\_Inspection.pdf](http://www.checkpoint.com/products/downloads/Stateful_Inspection.pdf)

ソフトウェアの脆弱性は日々新しく発見され、ハッカーもWeb環境のさまざまな部分を攻略しようと、革新的な攻略方法を絶えず探しています。Check Pointは、スタンドアロン型「侵入防御」デバイスを追加で購入および導入することなく、境界環境全体を保護できる境界セキュリティ・ゲートウェイを提供できるのは、Application Intelligenceファイアウォールを搭載したCheck Point VPN-1 NGシリーズだけだとしています。(Check PointのApplication Intelligenceは、同社のINSPECTセキュリティ・アーキテクチャを基盤としています。詳細は補足記事をご覧ください。)

Check Pointによれば、他社のシングル・ボックス・ソリューションは、保護の点で不十分であったり、必要なセキュリティ機能の一部しか含まれていないシングル・ボックス・ソリューションでユーザを引き付けるものがほとんどです。ユーザは、導入が終わった後になって、必要範囲が保護されていないことに気づき、完全な境界セキュリティ・ソリューションを構築するために、そのベンダのスタンドアロン・ボックスを購入せざるを得なくなり得ます。

Check Pointは、2004年11月にThe Tolly Groupに委託して、3つのシングル・ボックス・ソリューションについて、提供されるセキュリティの度合いを検証しました。調査の対象になった製品は、Check Point VPN-1 NGシリーズのファイアウォール、Cisco Systems PIX 515Eファイアウォール、それにJuniper Networks, Inc.のNetScreen-204ファイアウォールです。

The Tolly Groupのテストでは、CiscoもJuniperも、ファイアウォール製品に本格的な侵入防御システムを実装していないため、テスト対象範囲のセキュリティ脆弱性に必要な幅広い対応能力をシングル・ボックス・ソリューションで実現できていないことを示しています。「Check Point クラス」の保護を実現するには、2番目の境界デバイスとして専用侵入防御ゲートウェイを導入しなければならないため、さらに資本と運用コストが余分にかかります。

The Tolly Groupは、テスト開始前、2004年11月に、The Tolly Groupの「Fair Testing Charter(公正テスト憲章)」に従い、CiscoとJuniper両社に連絡をとりました。The Tolly Groupは、両社にテスト参加を招請しましたが、11月末になってもCiscoからは招請に対する応答はありませんでしたが、Juniperはテスト参加と情報提供に同意しました。Juniperには完全なテスト方法が伝えられましたが、11月下旬時点でそれに対するJuniperからのコメントはありませんでした。The Tolly Groupは予備テスト結果をJuniper Networksに送り検討とコメントを促しましたが、年末時点でJuniperからのフィードバックはありませんでした。

3つの製品はすべて、あらゆる規模の企業に多く見られるさまざまなセキュリティ悪用エクスプロイトに接触させる25種類以上のテストを実施しました。

次に示す図1は、さまざまなセキュリティ・エクスプロイトに対する3つの製品の対応を示すものです。

テスト結果表 Check PointのVPN-1 NGシリーズとCisco PIX 515E、 およびJuniper NetScreen-204との比較					
テスト・ケース	SmartDefense アドバイザリ	テスト名称	Check Point VPN-1 NG シリーズ	Cisco PIX 515E セキュリティ・ アプライアンス	Juniper NetScreen -204
1	CPAI-2004-38	Netscape NSSライブラリにおけるレコード解析バッファ・オーバーフロー: SSLv2チャレンジ長さの強制	✔	✘	✘
2	CPAI-2004-37	Cisco IOSの不正OSPFによるサービス不能脆弱性: MD5認証OSPF接続の強制	✔	✘	✘
3	CPSA-2004-03	ダイナミック・ルーティング・プロトコルに対する攻撃: MD5認証RIPの強制	✔	✘	✘
4	CPSA-2004-03	Cisco IOSの不正OSPFによるサービス不能脆弱性: MD5認証OSPF接続の強制	✔	✔	✔
5	CPSA-2004-03	ダイナミック・ルーティング・プロトコルに対する攻撃: MD5認証BGPの強制	✔	✘	✘
6	CPAI-2004-25	SOCKSベースのトロイの木馬: SOCKSv4のブロック	✔	✘	✘
7	CPAI-2004-25	SOCKSベースのトロイの木馬: 非認証SOCKSv5のブロック	✔	✘	✘
8	CPAI-2004-21	IRCベースのワーム: 非標準IRCポートに対する強制	✔	✘	✘
9	CPSA-2003-09	SQLの複数の脆弱性: 拡張ストアド・プロシージャ(xp_cmdshell)の保護	✔	✘	✘
10	CPSA-2003-09	SQLの複数の脆弱性: パブリック・クエリ(sp_start_job)	✔	✘	✘
11	CPSA-2003-09	SQLの複数の脆弱性: パスワードなしの 管理者ログインのブロック	✔	✘	✘
12	CPAI-2004-19	Microsoft SSLライブラリにおけるリモート・セキュリティ侵害の脆弱性: 不正PCT (Protected Communications Transport)のブロック	✔	✘	✘
13	CPAI-2004-15	IKEアグレッシブ・モードに関する脆弱性: IKEアグレッシブ・モード鍵交換のブロック	✔	✘	✘
14	CPAI-2004-19	OpenSSL NULLポインタ処理による脆弱性: SSL長さの強制	✔	✘	✘
15	CPAI-2004-07	Microsoft ASN.1リモートによるコードの実行: NTLM(NT LAN Manager)に対する強制	✔	✘	✘
16	CPAI-2003-04	Microsoft SQLワーム(Slammer): Slammerテスト	✔	✘	✘
17	CPAI-2004-42	Microsoft JPEG 処理におけるバッファ・ オーバーフロー脆弱性: JPEGエクスプロイト	✔	✘	✘

テストの結果、Check Point VPN-1 NGシリーズのファイアウォールが、テスト対象製品では唯一、25以上のセキュリティ・エクスプロイトに対応し、ターゲット・システムへの侵入を確実に阻止するものであることがわかりました。

これにより、シングル・ボックスの製品ではCheck Point VPN-1 NGシリーズのファイアウォールが総合的な侵入防御を装備しているのに対し、Cisco PIX 515EやJuniper NetScreen-204は、テストに使用された脅威に対する防御に必要なIPS機能を一部しか備えていないことが実質的に示されました。

CiscoもJuniperも境界ゲートウェイ・ソリューションに何らかの侵入防御機能を付加していますが、Check Pointのソリューションが示すレベルの広範囲をサポートするためには、ユーザは侵入防御サービス専用のゲートウェイを追加導入する必要があり、その結果サービスが重複するだけでなく、Check Pointの製品と比較すると、ユーザは2ボックスのソリューションを使用するための所有コスト(購入、メンテナンス、運用の費用)により財務上の打撃を受けます。

問題はこれだけではありません。

Check Pointに匹敵する保護を実現するためには、CiscoまたはJuniperでは「2ボックス」ソリューションが必要になることがテストから明らかになりました。今回の調査ではCiscoやJuniperの「2ボックス」ソリューションを検証しませんでした。そのようなアプローチでは、ネットワークのセキュリティ面の管理もますます複雑化します。その点に関して、境界部のファイアウォール/VPNゲートウェイと内部侵入防止システム・ゲートウェイの両方を管理できる完全な統合管理システムは、CiscoからもJuniper Networksからも提供されていません。

これに対し、Check PointのSMART( Security Management Architecture セキュリティ管理アーキテクチャ)は、すべてのCheck Pointの境界ゲートウェイと内部ゲートウェイを管理でき、セキュリティ環境の管理を合理化させ、簡単にすることができます。

Check Pointは、今回テストしたCiscoとJuniper Networks製品と比べて、他にも優れた利点があります。同社はファイアウォール製品に、SmartDefenseサービスをバンドルしています。Check PointのSmartDefenseを使うと、ユーザはネットワーク層およびアプリケーション層への攻撃に対する防御を設定、実施、更新することができます。また、SmartDefenseサービスは、Check Pointがオンラインで提供するSmartDefenseアップデートとアドバイザリにより、攻撃の防御に関する情報や新しい攻撃に対する防御手段および関連情報を提供します。SmartDefenseコンソールは、VPN-1製品に含まれています。SmartDefenseはまた、Check PointのSMART管理およびレポート・インフラストラクチャを統合し、攻撃の検知、ブロック、ログ記録、監査、警告を行う単一の一元集中管理コンソールを提供します。

Juniperもセキュリティ更新サービスを提供していますが、同社のDeep Inspection™ファイアウォールとIDPソリューションは別のボックスであるため、更新サービスはそれぞれについて別個になっています。Juniperは現在自社のファイアウォールでサポートしているプロトコルのアップデートを提供していますが、新しい「Deep Inspection」プロトコルに対応するには、OSのアップグレードが必要です。IPSについては、Juniperは定期的な更新サービスを提供しています。Ciscoはファイアウォールの更新サービスを行っていませんが、IPSの更新サービスは提供しています。

対照的に、Check PointのSmartDefenseで利用できる防御は、SmartDefenseサービスへの加入により、更新して最新の状態を維持できます。CiscoはCisco IDSの更新サービスのみを提供しており、PIXファイアウォールについてはサービスを行っていません。Juniper NetworksはDeep InspectionファイアウォールとIDPの2つの異なる更新サービスを提供しています。

総所有コスト(TCO)の観点から見ると、Check Point VPN-1 NGシリーズのファイアウォールのコストがCiscoやJuniper Networksのシングル・ボックス・ソリューションよりも56パーセントも低いことが大まかな分析だけでもわかります。また、これらの競合製品はCheck Pointの侵入防御機能の一部しか備えていません。

まとめると、テストした中で、この評価に使用したエクスプロイトの全範囲を完全に防御できた製品は、Check Point VPN-1 NGシリーズのファイアウォールだけでした。同製品を使えば、今回テストしたCiscoやJuniper Networksの製品と比べ、ファイアウォール、VPNに加えて完全な防御機能を持つ、より堅牢でフル装備の多機能セキュリティ・ソリューションを手に入れることができます。

また、CiscoやJuniper Networksは、ユーザがシングル・ボックスで提供されている以上の広範な侵入防御機能を必要とした場合、2ボックスのゲートウェイ・ソリューションに解決を求めるようにユーザを先導する傾向があることもわかりました。

そうすると、Check Pointの提供製品よりもはるかに所有コストが増し、管理が複雑になります。Check Pointは、ユーザが1つのインタフェースを習得するだけで、ファイアウォール、VPN、侵入防御機能をすべて管理できる統合化された管理機能を提供しています。

## アーキテクチャによる防御の深さ

Check Point、Cisco、Juniper Networksのテスト対象製品のアーキテクチャについては、チェック・ポイントのApplication Intelligenceの設計と、Juniper Networksが採用しているディープ・パケット・インスペクションおよびCiscoのステートフル・パケット・インスペクション・エンジンを比較するとよくわかります。Juniperは、自社のDeep Inspection™ファイアウォール技術に基づくセキュリティ・アーキテクチャを使用しています。

Juniper Networksによれば、Deep Inspectionファイアウォールはステートフル・インスペクションを実現し、侵入防御技術をファイアウォールに統合して、ネットワーク境界でのアプリケーション・レベルの攻撃防御を可能にしています。Juniper NetworksのDeep Inspectionファイアウォールは、ネットワーク・セキュリティ機能を実行し、アプリケーション・メッセージを解析してトラフィックを許可するか拒否するか判断します。

Deep Inspection技術では、より深いレベルのアプリケーション認識をトラフィックに適用し、そのトラフィックの意図に基づいてアクセス・コントロールの判断が下されます。境界に配備されるDeep Inspectionファイアウォールは、Microsoft Windows、ピア・ツー・ピア(P2P)やインスタント・メッセージング(IM)などのインターネット・アプリケーションに対するアプリケーション・レベルの攻撃防御に焦点を合わせたものです。アプリケーション・レベルのあいまいさを排除し、デフラグメンテーション、再構成、スクラビング、正規化を行い、ネットワーク・パケットを、クライアント - サーバ間で転送されるアプリケーション・レベルのメッセージに変換します。次にプロトコルの一致を探し、攻撃が実行されるアプリケーション「サービス・フィールド」を確認し、そこからデータを抽出して、攻撃パターン・マッチを適用します。そして、アプリケーション・サービス・フィールドのいずれかにある影響の大きいプロトコル異常や攻撃パターンに基づき、トラフィックを許可するか拒否するかを判断します。Deep Inspectionファイアウォールはアプリケーション・レベルの攻撃をインターネット・ゲートウェイで遮断し、攻撃の目標到達を阻止できます。また、ユーザが独自に攻撃防御シグネチャを作成することもできます。

Ciscoは、ステートフル・パケット・インスペクションに依存していますが、同社のWebサイトによると、PIX 515Eは「プロトコル規格適合性試験、アプリケーションおよびプロトコル状態の追跡、ネットワーク・アドレス変換(NAT)サービスなど多様なセキュリティ施行技術と、プロトコル・フィールド長検査、URL長検査などの多岐にわたる攻撃検知・軽減技術」を採用しているとのこと。

CiscoとJuniperのセキュリティ・アーキテクチャは、主に「応答ベース」です。すなわち、両社のアーキテクチャ製品では、あらかじめベンダからの更新通知に応じてシグネチャ・データベースを更新しておかなければ、新種の脅威や既存の脅威の亜種を防ぐことはできないということです。これに対し、Check Pointは、シグネチャに依存せずに新種の脅威や既存の脅威の亜種を防ぎます。

Check Pointは、テスト・データに示されるとおり、アプリケーションに対してより深いレベルの防御を提供できるセキュリティ・アーキテクチャを備えています。Check Pointによると、同社はパターンやシグネチャー致だけに頼るのではなく、「クラス(部類)ベース」の検出方法を採用しています。

独自のINSPECTアーキテクチャおよびApplication Intelligenceアーキテクチャにより、Check Pointのファイアウォールは特定の攻撃だけでなく、攻撃のカテゴリ全体、すなわち攻撃の「クラス」を遮断します。チェック・ポイントは、シグネチャーに依存せず、RPCなどプロトコルの正規の使用を強制することにより、独自の防御レベルを提供しています。従来のシグネチャー・ベースの防御は、防御シグネチャー作成のために攻撃特性の完全な把握を必要とするため、後手に回ってしまいます。

Check PointのSmartDefenseは、同社のStateful Inspection、Application Intelligence、Web Intelligenceといった技術に基づくものです。SmartDefenseにより、ゲートウェイは特定の攻撃はもちろんのこと、攻撃のカテゴリ全体、すなわち「攻撃のクラス」を遮断することができます。Application Intelligenceの主要機能は次のとおりです。

標準規格に対する適合性の検証

プロトコルの正規使用状況の検証

悪質なデータのブロック

有害なアプリケーション操作の制御

SmartDefenseは、Check Pointの実施ポイントで攻撃をブロックします。SmartDefenseの一部の機能は、統合化されたファイアウォール・セキュリティ・ポリシーの一部として実施され、実施ポイントのセキュリティ・ポリシーとして配布されます。SmartDefenseの特定攻撃防御に加え、Check Point実施ポイントが実現するネットワーク・リソースへの厳格なアクセス・コントロールも有効な防御になっています。

SmartDefenseはさまざまなコンポーネントに統一セキュリティ・フレームワークを提供して、攻撃の特定と予防を行います。同社のSmartDashboard管理ディスプレイのSmartDefenseタブは、ツリー構造に分かれ、SmartDefenseの防御手段が分類して表示されます。

ツリーの各項目は、攻撃ファミリの防御策や、より一般的な攻撃防御・保護手段(システムのフィンガープリントのスクランブル処理など)などの機能カテゴリを表します。たとえば、SmartDefenseは、Blasterをブロックするだけでなく、Microsoft RPCプロトコルによって定義される適切な接続フローが妨害されるという特徴から、類似の変形ワームもブロックします。このようにSmartDefenseはクラス・ベースで攻撃をブロックするため、特定の攻撃シグネチャーに限定されることがありません。SmartDefenseコンソールでは、管理者はツリーの各カテゴリおよびサブカテゴリに対して攻撃防御・保護措置を設定し、攻撃や脆弱性についての情報を取得することができます。

テストを実施した時点では、CiscoからもJuniperからもCheck Pointが対応しているような完全装備のアプリケーション・プロトコルは提供されていませんでした。今回の調査と理解に基づく限り、Juniperのディープ・パケット・インスペクションでは、既存のプロトコル用のシグネチャをダウンロードまたはアップグレードすることはどのユーザでもできますが、新しいプロトコルを実装するにはOSのアップグレードが必要です。

Check Pointのファイアウォールは、テストを行った他のライバル製品と比べてコスト面で3つの利点があります。

ゲートウェイおよび管理ソフトウェアの初期資本コストが低い

運用コストと管理コストを削減できる

セキュリティ更新コストを低く抑えられる

同様に、今回テストしたCisco PIX OS 6.3.4には、アプリケーション・レベルのインスペクション方法が最低限含まれているだけでした。Ciscoのセキュリティ・アーキテクチャを基盤とするPIXファイアウォールは、OSをアップグレードしない限り、新しいアプリケーション(プロトコル)の検査方法を学習できません。Check Pointの場合、OSのアップグレードを必要としません。同社のSmartDefenseアップデートは、ダウンタイムなしでゲートウェイに組み込まれます。たとえば、Check Pointの場合、ゲートウェイを停止させずに、新しいプロトコルの保護機能や防御メカニズムを追加することができます。

テストの結果、Check Pointが、HTTP、HTTPS、SQL、SOCKS、IPSec、BGP、OSPF、RIPプロトコルに対応したインテリジェントなアプリケーション・セキュリティを提供することが明らかになりました。今回テストした他製品は上記のプロトコルを使用してアプリケーションを調べるよう設計されていないため、プロトコル・トラフィックがエクスプロイトの犠牲になる可能性があります。

Check Pointのファイアウォールが保護するプロトコルは、今日の企業環境で使用されているプロトコルの中でも最も重要なプロトコルです。SQLは、多くのミッション・クリティカルなビジネス・アプリケーションの中核となっています。Secure Sockets Layer(SSL)は、eコマースや機密情報を扱うその他のビジネス・アプリケーションの安全性を確保するためのミッション・クリティカルなツールです。BGP、OSPF、RIPは、最適な冗長ルーティング条件を確保するための主要ルーティング・プロトコルです。

Check Pointは、Microsoft環境を対象とした多数のプロトコル/アプリケーション・ベースの攻撃に対して迅速な防御を提供しています。Check Pointのソリューションは、CIFSやMicrosoft SQL( MS SQL )、Microsoft リモート・プロシージャ・コール( RPC )などのプロトコルに対してインテリジェントな検査を行うことができるため、攻撃の発生に伴って瞬時に防御することが可能です。また、多くの変種に対しても即応することができます。

パケット分析を基にした他のテスト対象製品は、今日最も一般的な攻撃ルートの一つであるMicrosoft プロトコルに対応しておらず、シグネチャに依存しています。シグネチャ・ベースのJuniperのアプローチは、攻撃の根本原因を理解していないため、変種を認識することはできません。

Juniperの顧客は、すでに自社ネットワークに不具合を生じさせている攻撃に対してJuniperが新たな防御を提供するのを待っていなければならず、また、変種の攻撃に対する防御手段も一切与えられません。

## セキュリティの総コスト

企業クラスのセキュリティ製品を配備する際、処理対象となるエクスプロイトやセキュリティ製品のアーキテクチャの妥当性など、技術上の考慮事項は十分に比較検討しなければならない要素です。

しかし、技術導入決定はビジネス決定であり、どのようなビジネス決定を下すにしても、その中心となるのは、初期コストとその後継続的にかかる費用であり、それに基づいて総所有コスト、つまりセキュリティの総コストを算出する必要があります。

今回の総所有コスト(TCO)分析では、TCOの定義にゲートウェイ・コスト、シグネチャ更新のための継続的なサブスクリプション・サービス・コスト、およびサポート・コストを含めました。

以下の表にまとめた販売価格(米ドル単位の北米価格)は、すべて2004年11月時点の情報です。Cisco PIX 515E関連の価格は、一般的なWebサイト、CDW.comの提示価格を使用しました。Juniper NetScreen-204関連の価格は、2004年11月付のJuniper価格表を参照したもので、Check Pointによって提供されました。

図2

単一サイト複合型ファイアウォール/IPSソリューションのTCO(総所有コスト)比較			
	Check Point Express 100*	Juniper NetScreen-204/ Juniper IDP-10	Cisco PIX 515E/ Cisco IDS 4215
ゲートウェイ		アプライアンス	アプライアンス
境界FW/VPN	(ソフトウェア:\$6,500 [ハードウェア:\$1,595])	\$11,500	\$7,495
IPS	込み	\$9,195	\$8,000
加入サービス			
境界FW/VPN		Deep Inspection Signature Service : \$920	サービス提供なし
IPS	(SmartDefenseサービス:\$1,000)	IDPコストに別サービスを含む	IDSコストを含む
サポート			
境界FW/VPN		\$1,040	\$900
IPS	\$975	-	\$700
合計	\$10,070	\$22,655	\$17,095

\*Check Point Express 100は、The Tolly Groupがテストした、Application Intelligenceファイアウォールを含むCheck Pointインターネット・セキュリティ・ソリューションのテスト時に使用した中規模企業境界ソフトウェア・バンドルの名称です。

ハードウェア、ソフトウェア、サポート・コストを合わせたTCO分析によると、Check Pointのシングル・ボックスのファイアウォール/IPSソリューションは、Juniper NetScreen-204またはCisco PIX 515Eの2ボックス・ソリューションと比べて70～125%少ない費用で済むことがわかりました。

基本機能レベルでも、テストで使用したCheck Point Express 100ソフトウェア・バンドル(境界部のファイアウォール/VPNと統合化されたIPS機能)は、CiscoやJuniperのほかのシングル・ボックス・アプライアンスに比べ、13～43%低コストでした。Check Pointのソリューションはソフトウェアのみの製品であるため、ホストPCのコスト(1,595米ドル)を含めても総費用は約8,000ドル程度で、Juniper Networksオプションと比べて30%ほど低く、

Ciscoアプライアンスと比べると同等のコストになります。Check Pointのソリューションに匹敵する機能をJuniper IDP-10で実現するためには、さらに9,195ドルがかかることを考えると、ハードウェア費用の差は相当なものとなります。Ciscoの場合、PIX 515Eの7,495ドルに加えて、IDS 4215に8,000ドルがかかります。Check Pointがシングル・ボックス・ソリューションで提供しているのと同レベルの防御を実現し、テストしたすべてのエクスプロイトを阻止するためには、いずれのベンダにおいてもこのようなデバイスが必要となります。

さらに、加入サービス、すなわち新たな攻撃シグネチャに遅れをとらないようセキュリティ・サービスを維持するための更新の問題もあります。Check PointとJuniperのサービス費用は同等ですが、Ciscoの更新サービスはIDS製品のもののみです。

サポート費用については、Check Point Express 100で年間費用975ドルの追加、Juniper NetScreen-204は1,040ドル、Ciscoはデバイス2台で1,600ドルの追加となります。

全体を通して見ると、ユーザは、NetScreen-204( 22,655ドル )の2ボックス・ソリューションではCheck Point Express 100( 10,070ドル )の2倍、Ciscoの2ボックス・ソリューションでは約70パーセント多く費用を支払うこととなります( 12ページの総所有コストの表を参照してください )。この分析をさらに掘り下げるには、配備に要する先行投資コスト以上のものを考慮に入れなければなりません。

インターネット・セキュリティ導入のTCOを定量化する試みはこれまでも多く行われてきましたが、TCOで最も重要な要因の一部が見落とされています。

不十分なセキュリティ対策は、企業全体のシステムのダウンタイムを招いたり、公衆へのセキュリティ侵害で顧客を失う事態につながったりすることがあります。ファイアウォール/VPNソリューションの総コストを検討するときに、ソリューションの根本的なセキュリティが購入者に見落とされがちだという事実は何とも皮肉です。実際、ファイアウォールの本来の役割はセキュリティであり、VPNの本来の役割は安全な接続性の確立にあるはずで

アプリケーションやプロトコルの脆弱性を狙った新種の攻撃は日々出現しています。セキュリティ製品は、このような脅威に週単位ではなく分単位で適応し、対処できるだけの機敏性を備えていなければなりません。新たな脅威が確認されたら、即座に防御手段を作成し、世界中のデバイスやユーザに配布する必要があります。このような即応性が必要であるということは、Check Pointが提供しているようなソフトウェア・ベースの方法が必要であることを示唆しています。セキュリティの必要条件には、セキュリティ・システムの柔軟性が含まれます。Check Pointの場合、ファイアウォールと完全なIPS機能が1つの製品に緊密に統合化されているため、そのような柔軟性が実現します。

JuniperやCiscoのソリューションではそうはいきません。シグネチャはASICでハードコード化されているため、セキュリティ更新をシステムにロードしなければならず、即座に動的に適用することができません。

一方、Check Pointのソリューションは、SMART( セキュリティ管理アーキテクチャ )という単一のコア管理インフラストラクチャを使用して、ファイアウォール、VPN、IPS関連の機能を制御しています。JuniperとCiscoの製品では状況が異なります。今日の環境を見る限り、動的に脅威に対応できることは不可欠ですが、CiscoのPIXアーキテクチャには、新しい検出機能を動的に追加する機能がありません。

さらに、CiscoもJuniperも、ファイアウォール/VPNと侵入検出機能で異なる管理制御が必要です。このため管理者は、複数のユーザ・インタフェースと設定プロセスに対処しなければならないため、TCOが増加することになります。

デバイスごとにコマンドライン操作を必要としない集中管理で操作が行える機能があれば、初期導入を行う場合も既存の配備に設定変更を加える場合も、管理時間を大幅に減少させることができます。

要約すると、今回テストした3つの製品のTCO分析では、Check Pointが大きく勝ることが裏付けられました。

Check PointがApplication Intelligenceで実現しているのと同じだけのアプリケーション保護をCiscoとJuniperで実現するには、境界部ゲートウェイ・ソリューションに専用IPSを補完しなければなりません。ユーザがNetScreen-204やPIX 515Eに加えて別売りのIPSを追加すると、JuniperとCiscoのソリューションの総コストは増加します。Cisco IDSとJuniper IDPでは、両方とも個別の管理・オンライン更新システムが必要となり、ソリューションの総コストはさらに増えることとなります。

## セキュリティへのインテリジェントなアプローチ

今日のように急激に変化するセキュリティ環境では、ユーザは複数のサービスを1つのプラットフォームから実行できるようなエンタープライズ・クラスのセキュリティ・ソリューションを求めています。そのようなソリューションを利用することで、コストを大幅に削減でき、日常のネットワーク管理作業を簡易化できるだけでなく、ネットワーク境界での応答性が向上し、新たな攻撃に先んじて対処できます。

このテストで対象となった製品のベンダ3社はいずれも、ファイアウォール、VPN、侵入防御サービスを組み合わせた多機能セキュリティ・プラットフォームを提供しています。しかしこれは、統合シングル・ボックス製品がすべて同等の機能や性能を持っているということではありません。事実、テストではその差が顕著に表れる結果となりました。

前述したとおり、Check Point VPN-1 NGシリーズのファイアウォールは、多くの利点があり、テストしたJuniperやCiscoのソリューションよりはるかに魅力的なマルチサービス・プラットフォームに仕上がっています。

テスト結果によると、Check Pointはより多くのプロトコル数に対応するアプリケーション・レベルのセキュリティを提供します。SQL、HTTP、HTTPS、SQL、SOCKS、IPSec、BGP、OSPF、RIPなどのプロトコルは、主流アプリケーションをサポートするほか、企業ネットワーク全体のアプリケーション・データ転送を実現します。Check Pointは、最も一般的なプロトコルだけでなく、特殊なプロトコルに対するセキュリティも提供しています。

Check Point VPN-1 NGシリーズのファイアウォールは、このように広範なプロトコルをサポートしているため、SQL、CIFS、SOCKS、P2P、IM、また主なルーティング・プロトコルなど、戦略的なアプリケーションへのサポートも含め、包括的なアプリケーション・サポートおよび防御が実現します。

攻撃が頻発しているのは、HTTPのような一般的なプロトコルばかりでなく、SQLなどその他のミッション・クリティカルなプロトコルや、OSPF、BGP、RIPなどの動的なルーティング・プロトコルにも広がっています。その点、Check PointのApplication Intelligenceは、広範なアプリケーション・プロトコルを防御するのに適した立場にあります。

Check Pointがこれらすべてのプロトコルをサポートするのに対し、ネットワークを保護するために攻撃シグネチャのフレームワークに依存するCiscoやJuniperは対応していません。このため、Check Pointの場合と異なり、アプリケーション・データが攻撃されやすくなります。

また、Check Pointのセキュリティ・アーキテクチャは、より適切にアプリケーション・データのサポートに対応します。Check PointのApplication Intelligence技術は、プロトコル・レベルの異常動作に対する防御を提供しますが、他のテスト対象製品は攻撃シグネチャを探すのみです。攻撃シグネチャに対するディープ・パケット・インスペクション検査では、アプリケーション・レベルの攻撃の防御は得られません。さらに、今回The Tolly Groupが検討した競合製品は、新たなアプリケーション検査機能を追加するためにOSのアップグレードを必要とします。

Check PointのVPN-1 NGシリーズに設定されているSmartDefense機能は、OSアップグレードを必要とする従来のIPSシステムと比べて、導入時間を短縮できます。

最後にTCOの観点では、Check Pointの場合、ファイアウォール、VPN、侵入防御サービスが1つのデバイスに統合されており、加えて総合的なアプリケーション・プロトコルのサポートが備えられています。今回のテストによると、JuniperやCiscoのシングル・ボックス・ソリューションが提供する機能は、Check Pointの機能に比べ、大きく下回っています。実質上、両ベンダはユーザに追加の侵入検出専用ボックスの導入を推奨することになり、TCOのライフサイクル・コストはさらにCheck Pointが有利になります。

つまり、JuniperとCiscoはシングル・ボックス・ソリューションの導入をユーザに促しますが、Check Pointがシングル・ボックス・ソリューションで提供している機能に匹敵するエンタープライズ・クラスの保護を実現するには、2番目の侵入検出アプライアンスを追加しなければならないことに、購入者はすぐに気づきます。

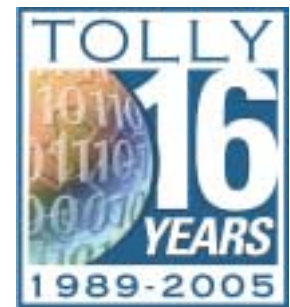
最終的に、ユーザはCheck Pointのシングル・ボックスを導入した場合の2倍以上の費用を2ボックス・ソリューションに払わなければなりません。

シングル・ボックスのマルチサービス・セキュリティ・プラットフォームを配備する前に、ファイアウォール、VPN、侵入防御のニーズを満たすかどうかを十分検討することは非常に有意義です。そうすれば、技術上の理由からもコスト面からも、Check Point VPN-1 NGシリーズファイアウォールを選択すべきだということがわかるでしょう。

要するに、CiscoやJuniper Networksの2ボックス・ソリューションは、コストと技術の両方の視点で問題があることがわかります。

Check Pointのインテリジェントなセキュリティ・ソリューションは、現時点で、さまざまな一般的なエクスプロイトからアプリケーション・トラフィックを最大限に保護する設計になっています。これは販売を促進するための誇大広告ではありません。3製品の根拠ある実地テスト結果に基づく厳然たる事実です。

情報技術( IT )は、急激な成長と絶え間ない変化を続けている分野です。The Tolly Groupは、エンジニアリング・レベルのテストを実施して、最新の商品や技術に関する貴重な情報をインターネット使用業界に提供しています。最大限の精度を確保するために細心の注意が払われていますが、誤りが生じる場合もあります。The Tolly Groupはいかなる場合も、本文書に掲載された情報の使用によって生じる直接的、間接的、特殊、付随的、二次的な損害を含め、いっさいの損害に対して責任を負うものではありません。本文書に掲載された商標はすべて該当する企業の所有物です。



The Tolly Group, Inc.  
 3701 FAU Blvd. Suite 100  
 Boca Raton, FL 33431  
 Phone: 561.391 5610  
 FAX: 561.391.5810  
<http://www.tolly.com>  
[info@tolly.com](mailto:info@tolly.com)

