



IPSの統合における パフォーマンス上の課題と解決

チェック・ポイントの新技术により、パフォーマンスやセキュリティを犠牲にすることなくフル機能の侵入防御システムを統合

Contents

本書の内容

概要	3
IPSの統合によるパフォーマンスへの影響	4
IPSの統合においてパフォーマンスを最大化するチェック・ポイントの新技术	5
アクセラレーション技術 — SecureXL™	6
複数のCPUコアの効率的な使用 — CoreXL™	7
ネットワーク・トラフィックの効率的な分散 — ClusterXL®	8
スケーラビリティ	9
集中的な検査 — ステートフル・パケット・インスペクションによる高速化	10
パフォーマンス・ボトルネックの特定	10
IPSの統合によってネットワークを保護	11

概要

ITのパフォーマンス上の課題が解決されると、次は企業がそれまで解決できなかった課題を解決できることを認識し、ビジネスにとって重要性の高いサービスに適用できるかどうかを検討する段階に入ります。この技術白書では、ネットワーク・セキュリティの分野で新たに解決された課題について解説します。ネットワーク・ゲートウェイの新たな処理技術により、すべての機能が統合された侵入防御システム (IPS) と次世代ファイアウォールを、パフォーマンスを制限することなく組み合わせることが可能になりました。

予測不可能で急速に変化するセキュリティ上の脅威に対処するため、IPSとファイアウォール機能を統合してネットワークを保護する必要性が高まっています。そのような状況に合わせるかのように、パフォーマンスの向上を可能にする革新的なIPSが誕生しました。

IPSを統合する必要性を加速させたのは、アプリケーション層の脆弱性を突いた攻撃の急増です。2008年に公表された脆弱性の55%近くはWebアプリケーションの脆弱性でした¹。ほとんどの場合、これらの脆弱性に基づく攻撃は、ファイアウォールで確立した通常のポート/プロトコル経由の防御をすり抜けてしまうため、侵入防御機能によって深いレベルでパケットを検査しないと検出できず、さらに、深いレベルのパケット検査だけでも十分ではありません。IPSにおいて深いレベルのパケット検査とファイアウォール処理を自動的に統合し、防御をすり抜ける可能性のある攻撃をブロックするようファイアウォールに指示できる必要があります。ところが、IPS機能の統合は、一般的なファイアウォールのパフォーマンスを低下させるだけでなく、時としてダウンの原因になるというのがこれまでの常識でした。接続性を確保するためには、セキュリティが低下することを覚悟で、IPSとファイアウォールの統合をやめなければならなかったのです。

しかし、接続性をとるかセキュリティをとるかというジレンマは意味をなさなくなりました。チェック・ポイントのパフォーマンス向上を可能にする新技術によって、システムのパフォーマンスを低下させることなく、統合されたIPS機能を必要に応じて実装することが可能になりました。チェック・ポイントのR70セキュリティ・ゲートウェイを使用すると、チェック・ポイントの既存ファイアウォールにフル機能のIPSを統合できます。この技術白書では、それぞれのネットワークに適した統合型IPSを特定できるよう、パフォーマンスに関わるさまざまな問題について解説します。また、R70セキュリティ・ゲートウェイに採用されている新技術についても解説し、パフォーマンスやセキュリティを犠牲にすることなくフル機能のIPSを統合するうえでの課題と対処方法について説明します。

IPSの統合によるパフォーマンスへの影響

侵入検知/侵入防御システムは、企業ネットワークを保護し、既知および未知のワーム、自動化されたマルウェア、複合型の脅威など、特にアプリケーション層の脆弱性を突く攻撃からサーバや機密データを保護します。IPSの選定においては、堅牢なセキュリティを提供し、ますます巧妙化する攻撃および攻撃ベクトルから企業ネットワークを保護できるシステムを選ぶ必要があります。効率的な管理とポリシーの遵守も重要です。データの過負荷に対処でき、重要性の高い処理を優先し、ポリシーの遵守を追跡できるシステムでなければなりません。また、絶えず変化するセキュリティ・ニーズに柔軟に対応できるよう、柔軟に導入できるIPSが望ましいといえます。

これらを考慮した場合、高いパフォーマンスを実現できるIPSが必要になります。特に、インラインで統合されたIPS機能のすべての機能を実行し、企業向けファイアウォールによるアクセス制御の決定を行う場合はなおさらです。以下に、組織に適したIPSを選択するうえでパフォーマンスに関連して確認が必要な点をまとめます。

そのIPSはパフォーマンス要件を満たしているか？

企業ネットワークは、1G Ethernetから10G Ethernetに移行してきています。Voice-over-IPやIPベースのテレビ会議のようなマルチメディア・アプリケーションの利用が拡大したことで、ネットワークのキャパシティも急激に大きくなりました。しかし、パケットの量が増えて転送が高速化するにつれ、データセンターやネットワーク境界でのデータ・セキュリティの処理要件も劇的に高まります。スループットを高め、遅延を少なくすることが不可欠になります。パフォーマンス面で問題となりやすいもう1つの要素が、支社・支店環境や小規模環境を接続するゲートウェイです。リモート・サイトでマルチメディア・アプリケーションを速度の遅いWANで使用する場合、遅延などの影響を無くするため、ネットワークの保護に使用するゲートウェイ・セキュリティ・サービスとIPSに同等の高いパフォーマンスが求められます。

そのIPSは要求されるパフォーマンス・レベルでセキュリティを提供できるか？

従来型のファイアウォールによるポート/プロトコル経由のアクセス制御では、普通のアプリケーション処理に使用される一般的なポートを通過できる進化型の脅威にはもはや対抗できません。ハッカーやマルウェアは、攻撃経路としてアプリケーション層を使用するようになっています。正当なトラフィックに偽装されたこれらの攻撃を検出するには、より深いレベルでの検査を実施する必要があり、そのためにより多くの処理能力が必要になります。必要なすべての機能を、パフォーマンスを低下させることなく利用できるIPSを選定する必要があります。

そのIPSには冗長性と信頼性が組み込まれているか？

IPSの信頼性は非常に重要です。IPSに障害が発生し、ネットワーク上の他のコンポーネントやアプリケーションが停止すれば、ダウンタイム1秒ごとに次々と利益が失われることとなります。セキュリティ・ゲートウェイにも、誤って有効なトラフィックを除去することなく、本当の攻撃から継続的にネットワークを保護することが求められます。IPSの仕様には、冗長性に加え、業務やサービスをノンストップで提供するための信頼性が組み込まれていなければなりません。

そのIPSはインフラストラクチャの拡張ニーズに対応できるか？

大規模なネットワーク環境で使用するIPSソリューションは、ネットワーク環境だけでなく、ネットワーク中のPCやアプリケーションの利用方法の変更などにも柔軟に対応でき、他のプラットフォーム・ベンダーのハードウェアも問題なくサポートできなければなりません。IPSシステムには、企業レベルのあらゆるセキュリティ処理要件を満たすことのできる拡張性が求められます。

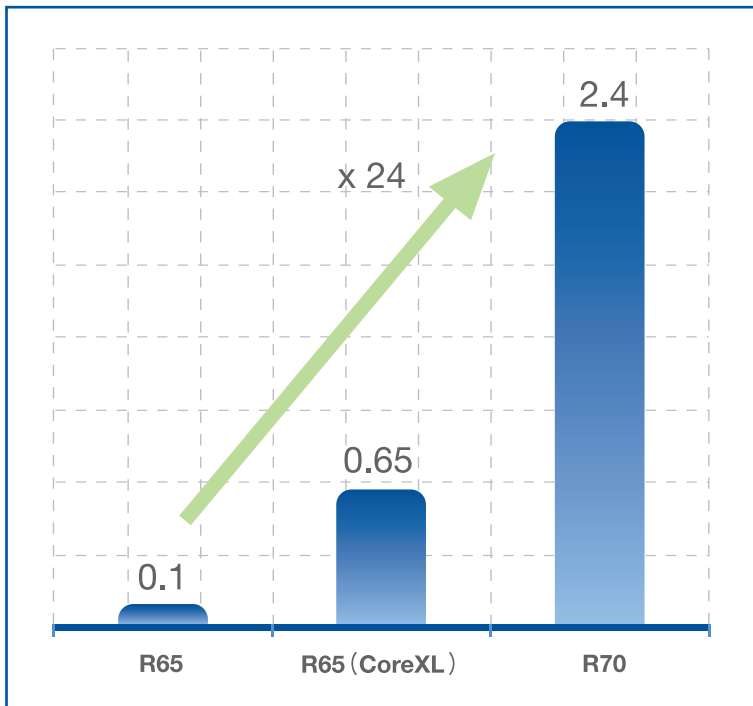
そのIPSは簡単に管理/更新できるか？

管理者は、どのIPS保護機能がどの程度パフォーマンスに影響するかを簡単に特定する必要があります。次々と進化する脅威や企業システムの変更に対応するためには、常に最新の脆弱性シグネチャで保護機能を更新できなければなりません。IPSは、TCOを削減しながらこのような管理を簡単に行える機能を備えている必要があります。

IPSの統合においてパフォーマンスを最大化する チェック・ポイントの新技术

前述の要件を満たすことができるかどうかは、IPSのコア・アーキテクチャによって決まります。チェック・ポイントのオープン・パフォーマンス・アーキテクチャは、最もパフォーマンスの高い侵入防御システムを実現するために設計されました。研究開発において最も重点を置いたのは、ユーザ環境においてセキュリティ・レベルを改善するための技術です。チェック・ポイントでは、Intelなどのマイクロプロセッサ・メーカーと密接な協力関係を築くことで、プロセッサ・プラットフォーム機能をチェック・ポイント・ソリューションに最大限活用できるようにしています。これらのパートナーシップを通じた技術の共有によって、IPSソリューションの統合のトータル・コストも大幅に低減できます。各パートナーがそれぞれの専門分野ごとに分業するこのパートナーシップは、オープン・セキュリティ・エコシステムと呼ぶべきものです。このオープン・セキュリティ・エコシステムにより、クローズドな独自システムよりも保護性能の高い統合ソリューションを、コスト・パフォーマンスに優れた価格で提供することが可能になっています。

チェック・ポイントのオープン・パフォーマンス・アーキテクチャは、IPSの統合を支える3つの技術、SecureXL、ClusterXL、CoreXLを基盤としています。これらの技術を相互に連携させることで、広範なオープン・サーバおよびアプライアンス上でのIPSのパフォーマンスを最大化します。



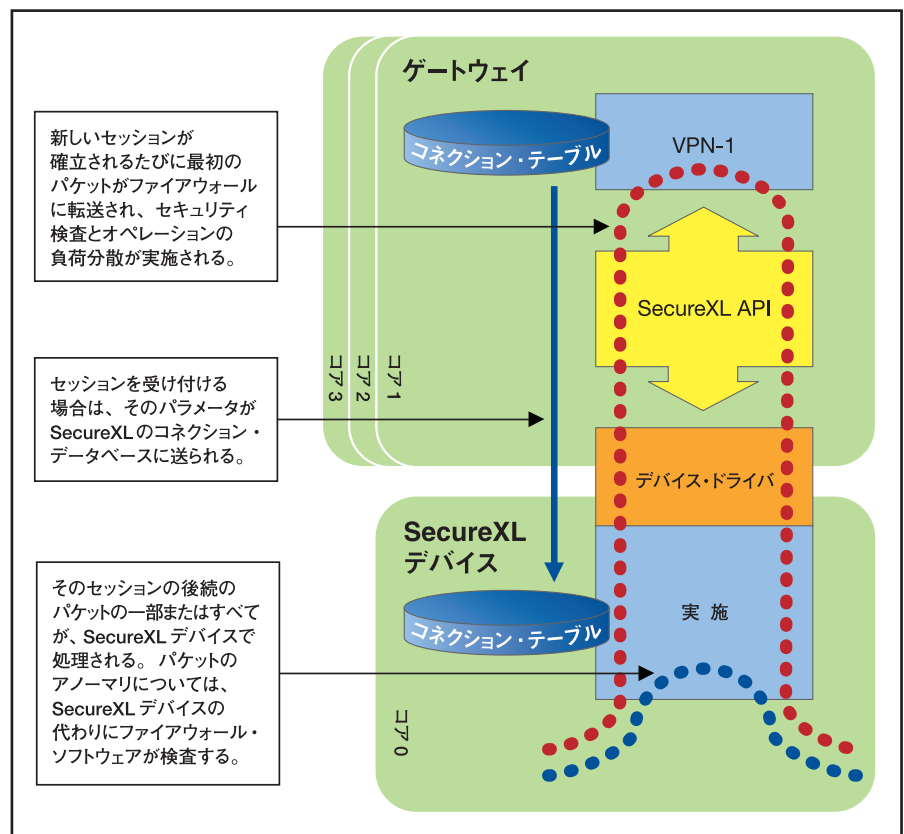
IPSにおいて推奨されるプロファイル、トラフィック構成、スループット (Gbps)
チェック・ポイントPower-1 9070アプライアンスを使用した場合

R70セキュリティ・ゲートウェイをマルチコア・プロセッサで稼働させる場合、コアを1つ追加したときの拡張性はほぼニア (70%以上) になります。IPSエンジンのスループット・パフォーマンスは、CoreXLを有効にすることで平均600%向上させることができます。使用されたテスト・パラメータは、8割の設定を有効にした厳格な保護プロファイルで、また、ゲートウェイを通過するトラフィックには、実際にインターネットを流れているものと同様のプロトコルおよびアプリケーションのトラフィックが使用されています。

アクセラレーション技術 — SecureXL

チェック・ポイントが特許を保有するアクセラレーション技術SecureXLは、負荷の高い複数のセキュリティ・オペレーションを高速化するためのAPIを備えたソフトウェア・パッケージから構成されます。SecureXLを使用すると、IPSだけでなく、チェック・ポイントのステートフル・インスペクション・ファイアウォールで実行するオペレーションも高速化できます。ステートフル・インスペクション・ファイアウォールでは、SecureXL APIを使用することで、こうしたオペレーションの処理を「SecureXLデバイス」と呼ばれる専用モジュール（パフォーマンスが最適化されたソフトウェア・モジュール）に負荷を分散することができます。

SecureXL対応ゲートウェイのファイアウォールはまず、SecureXL APIを使用してSecureXLデバイスにクエリを発行し、どのような機能が備わっているのかを確認します。次に、どのセッションのどの部分をファイアウォールで処理する必要があり、どの部分をSecureXLデバイスに負荷を分散できるのかを判別するポリシーを実装します。実際にそのゲートウェイを介して新しいセッションの確立が試行されると、ファイアウォールは、各セッションの最初のパケットを検査して、その接続がセキュリティ・ポリシーに基づいて許可されたものであるかどうかをチェックします。ファイアウォールは、このパケットを検査する際、セッションに対して実行する必要がある処理を判断し、ポリシーに基づいてそのうちの一部またはすべてをSecureXLデバイスに転送します。それ以降、そのセッションの該当するパケットは、直接SecureXLデバイスで検査されます。SecureXLデバイスは、対象トラフィックの詳細な分析および処理に必要なセキュリティ・ロジックを実装しています。パケットにアノマリ（異常な部分）を見つけた場合は、ファイアウォール・ソフトウェアとIPSエンジンでチェックします。またSecureXLには、接続の確立を完全にSecureXLデバイスで行うためのモードが用意されており、これを利用することで膨大な量のセッションを処理することが可能になります。



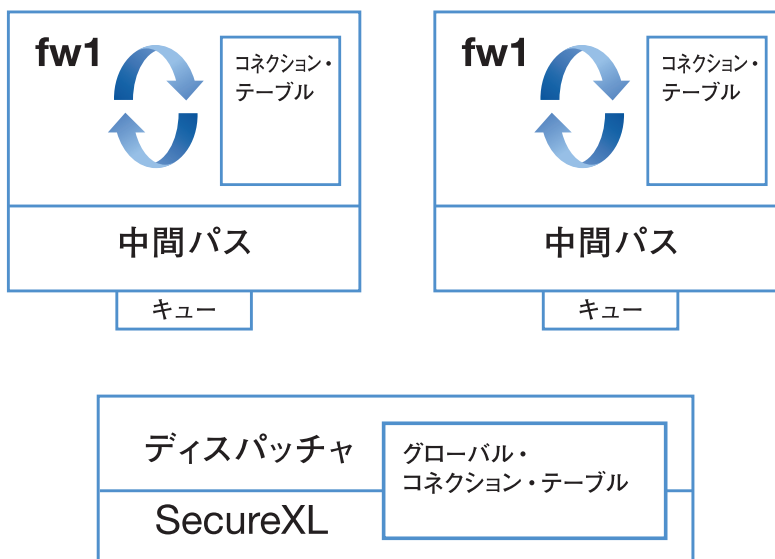
マルチコアCPUでのSecureXLによりIPSの統合によるパフォーマンス低下を最小限に抑える

パフォーマンスの向上は、SecureXL対応のソフトウェアおよびハードウェア・デバイス向けに最適化されたネットワーク・インタフェース・ドライバとマルチスレッド対応コードによって実現します。これらの機能を組み合わせることで、高速化されていないソリューションに比べ約3倍スループットが向上します。これらが、最終的には業界最高水準の価格性能比につながっています。マルチコア・システムでは、1つまたは複数のプロセッサをSecureXLの処理に割り当て、高速化されていないパケットは他のコアで実行しているIPSおよびファイアウォール・カーネルのインスタンスで処理できます。IPSとファイアウォールの統合にSecureXLを使用することで、セキュリティとパフォーマンスの要件の間で最適なバランスを実現できます。

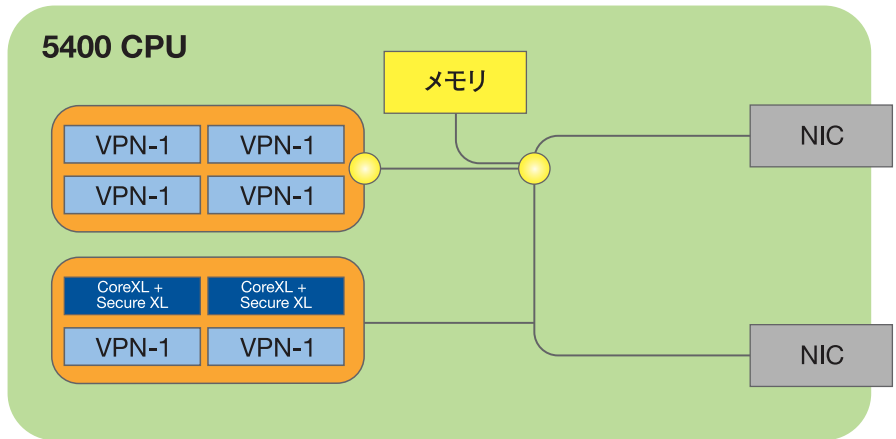
複数のCPUコアの効率的な使用 — CoreXL

CoreXLは、汎用マルチコア・プロセッサを最大限活用する業界初のセキュリティ技術です。先進のロード・バランシング機能を提供することにより、ファイアウォールにIPSを統合するうえで必要な深いレベルの検査のスループットを向上させます。マルチコアによって増強された処理性能により、ネットワークのセキュリティを高いレベルに維持しながら高いパフォーマンスを実現します。

CoreXL技術を有効にすると、SecureXLアクセラレーションを実行するために1つまたは複数のコアが割り当てられます。これらのコアは、トラフィックのディレクターとしても機能します。ディレクター以外のコアでは、IPSとVPN-1のインスタンスを実行します。例えば、アプライアンスが2個のクアッドコア・プロセッサを搭載している場合、2つのコアでSecureXLアクセラレーションを実行し、トラフィックはIPSとVPN-1のインスタンスを実行する他の6つのコアに処理させます。ディレクターとして動作するコアには、大きく2つの役割があります。1つはトラフィック受信時にそれをSecureXLで高速化できるかどうかを判断すること、もう1つはトラフィックに対して深いレベルのセキュリティ検査を実施するコアを割り当てることです。



マルチコアCPUにより統合化されたIPSを専用のコアで処理



マルチコアCPUにより統合化されたIPSを専用のコアで処理

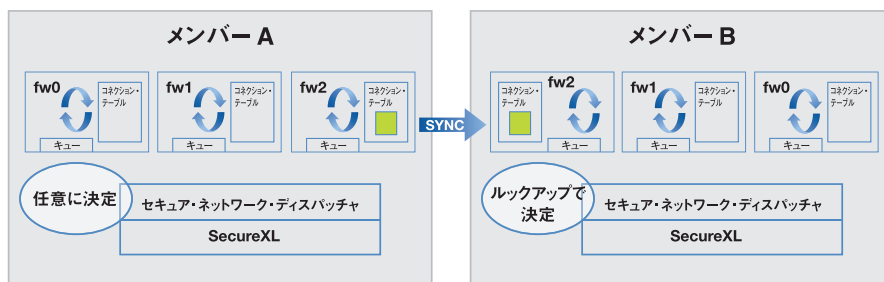
ネットワーク・トラフィックの効率的な分散 — ClusterXL

ClusterXLは、大量のトラフィックを知的に複数のゲートウェイに分散させる手段を提供することで、拡張性と信頼性を大幅に向上します。ゲートウェイ・クラスタは、物理的に同じ場所に配置することも、内部バックボーンを介してリモート配置することも可能です。後者の場合は、ビジネスの継続性を維持するために必要な冗長性がさらに向上します。

運用時には、クラスタを構成するR70セキュリティ・ゲートウェイは、それぞれ固有のIPアドレスと物理MACアドレスを保持することになります。ただし、クラスタに参加していないシステムからすると、いずれのクラスタ・メンバーも、クラスタを表す同一のバーチャルIPアドレスを持っているように見えます。各ゲートウェイは、内部ネットワークでも外部ネットワークでも相互に接続されます。

このような処理によって、クラスタ・メンバー間で素早く情報を共有できるようにしています。このやり取りは、複数のR70セキュリティ・ゲートウェイの間でセキュリティに関する情報および判断を確実に同期するために行われます。同期が必要なのは、ネットワークを行き来するトラフィックが、行きと帰りで同じクラスタ・メンバーを通過するとは限らないためです。ファイアウォール、VPN、NAT、およびIPSテーブルを共有することを「ステート同期」と呼びます。このステート同期により、1つのゲートウェイに障害が発生した場合に、残りのゲートウェイが中断なしでトラフィックを引き継ぐことが可能になります。フェイルオーバーが発生した場合も、同期済みのステート・テーブルを使用することで、アクティブな（障害のない）クラスタ・メンバーでのセキュリティ検査をそれまでどおり確実に実施できます。

実際のロード・シェアリングに関する判断は、ユニキャスト・モードとマルチキャスト・モードのいずれかの方法で行われます。ユニキャスト・モードでは、1台のR70セキュリティ・ゲートウェイが「ピボット」と呼ばれるクラスタ全体のコーディネータ役を担います。ピボットは、すべての内向きトラフィックを受信し、どのクラスタ・メンバーがその接続またはトラフィックを処理するかを決定します。一方のマルチキャスト・モードでは、複数の物理ネットワーク・インターフェース・カードをボンディング（1つに束ねること）して、単一のバーチャルMACアドレスを持つ単一のバーチャル・インターフェースを作ることができます。これにより、複数のネットワーク・セグメントが存在する複雑な導入シナリオにおける柔軟性を向上させることができます。このシナリオでは、1つのバーチャル・インターフェースを持つ各クラスタ・メンバーがすべてのパケットを受信します。パケットを処理するべきかどうかを各ゲートウェイが判断し、最終的に1つのゲートウェイがそのパケットを処理します。そして、その最初のパケットを処理したゲートウェイが、その接続の処理を担当することになります。



クラスタ・ロード・シェアリングによりIPS機能のパフォーマンスを向上

スケーラビリティ

チェック・ポイントは、コンピュータ処理アーキテクチャの変更を通じてセキュリティ業界をリードしており、さまざまなベンダー・プラットフォームに柔軟に対応しています。以下は、チェック・ポイントのIPSパフォーマンスの進化の歴史です。

- 2001年以前：カーネル・モード・セキュリティによってパフォーマンス要件に適合
- 2001年：SecureXL（米国特許番号6,496,935）セキュリティ・アクセラレーションAPIにより、ハードウェア・レベルでもソフトウェア内でも使用できる高度に最適化されたセキュリティ処理を実現（Performance Pack）
- 2002年：マルチノード・スケーラビリティを提供するClusterXLロード・シェアリングをリリース
- 2002年：マルチスレッド対応のSecureXL— Performance Packでカーネル・レベルのマルチスレッドを実現し、VPNパフォーマンスが格段に向上
- 2004年：SecureXL中間パス、SecureXLアーキテクチャの拡張により、最適化されたコードをPerformance Pack（マルチスレッド対応）とVPN-1コンテキストの両方から実行可能に
- 2006年：ClusterXL VSL（特許出願中1893/43、1893/46）— ClusterXLの拡張によってほぼリニアなマルチノード・スケーラビリティを実現したVSX NGX Scalability Packをリリース
- 2007年：CoreXLのウォーリー・フリー・セキュリティ（特許出願中1893/46）アーキテクチャによりカーネルを拡張し、コアの数に応じたグローバルなVPN-1セキュリティ処理を実現
- 2008年：SmartDefenseセキュリティ・エンジン— CoreXLとSecureXL中間パスの融合により、カーネル・レベルでのマルチスレッドを実現

IPS検出エンジンのパフォーマンス向上

チェック・ポイントのIPSパフォーマンス技術によって、検出エンジンの機能性が確実に向上します。

- 誤検出を抑制
- 安全性
- 信頼性
- 迅速なアップデート
- アプリケーションを正しく認識
- きめ細かい制御

R70セキュリティ・ゲートウェイ検出エンジンの詳細については、この技術白書の姉妹編「Proving Technical Confidence in Your IPS Detection Engine」をご覧ください。

集中的な検査—ステートフル・パケット・インスペクションによる高速化

2009年にチェック・ポイントが提供する最先端のオープン・パフォーマンス・アーキテクチャでは、CoreXLとSecureXLを使用したR70セキュリティ・ゲートウェイの融合によって高速化された高パフォーマンスのIPSエンジンに、インスタンスを複数のCPUコア間に分散してSecureXLコンテキスト内で最適化する最新のマルチティアIPSエンジンが加わりました。

接続が確立されてSecureXLコネクション・テーブルに登録されると、セキュア・ネットワーク・ディスパッチャによって追加の検査を実行するためのCPUコアが割り当てられます。各コアにはパッシブ・ストリーミング・ライブラリというインフラストラクチャ層があり、各種のセキュリティ・アプリケーションとネットワーク・パケットの間の仲介機能を果たすこの層でパケットの並べ替えや輻輳の処理を行います。

新しいマルチティアIPSエンジンは、1つのセキュリティ・アプリケーションとして提供されます。インターネット・プロトコル・スイートは、データのフォーマット、アドレス、ルート、適切な送信先への配信方法を決定するプロトコルとルールのセットで構成されています。IPS検出エンジンの1つの層で、これらの基準を満たしていない特異なパケットを素早く識別します。

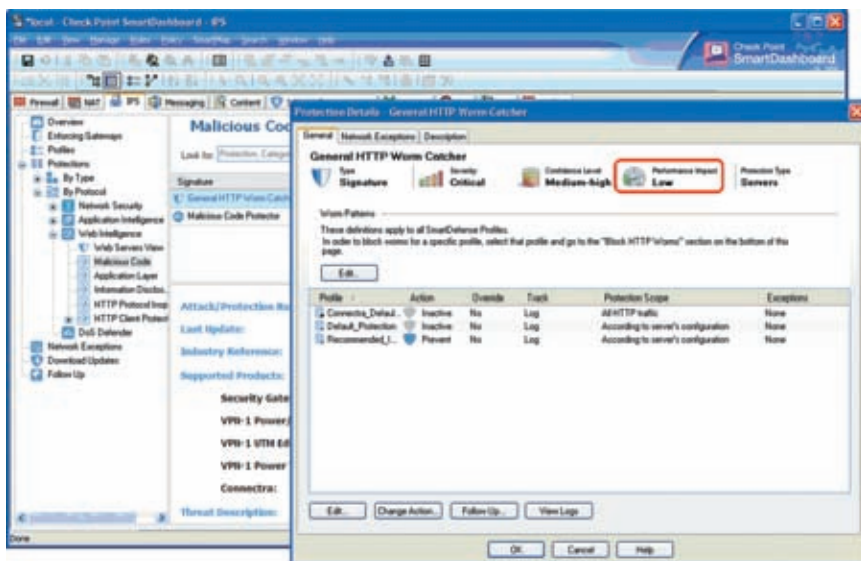
それ以外の攻撃は、基準を満たしたパケットや標的が絞られたアプリケーションまたはホストの脆弱性を突いた攻撃となります。これらの攻撃には、既知および未知の脆弱性を突くコマンドが挿入されたものもあります。これらの攻撃を識別する1つの方法は、使用されるコマンドを特定してそれをブロックすることです。それ以外の攻撃は、バッファ制限を指定すべきアプリケーションやオペレーティング・システムに適切な保護が施されていないことに付け込んだものです。この場合攻撃者は、同じオペレーティング・システム権限で、通常アプリケーション処理のコンテキストの外で実行できるコマンドを挿入したパケットを作成できます。

R70セキュリティ・ゲートウェイには、高速のパターン・マッチング・エンジンが採用されており、パケット・ストリーム内で攻撃が発生したときのコンテキストを調べることで既知および未知の攻撃を識別します。この識別では、2層の検査が行われます。1層目の検査では、悪意のあるトラフィックのおよそ90%が素早く除去されます。同じプロトコルにシグネチャを追加しても、パフォーマンスへの影響は最小限に抑えられます。

パフォーマンス・ボトルネックの特定

管理者は、どの保護機能がパフォーマンスに影響しているかを素早く把握する必要があります。そして、それらの保護機能を脅威の進化に合わせて常に最新の状態に更新し、脅威の進化に対応して脆弱性を修復するためのシステム変更も実施しなければなりません。それと同時に、保護機能の更新や追加が管理者にとって過大な負担にならないようにする必要があります。

R70セキュリティ・ゲートウェイなら、パフォーマンスへの影響を考慮しながらきめ細かい保護を適用できます。次のページの図に示すように、管理コンソールで保護機能ごとにパフォーマンスへの影響度（低、中、高、または重大）を設定できます。



セキュリティ設定ごとにパフォーマンスへの正確な影響を把握できるダッシュボード

IPSの統合によってネットワークを保護

チェック・ポイントのR70セキュリティ・ゲートウェイは、大規模な組織が高いセキュリティ・レベルを維持しながら高いパフォーマンスを実現するうえで必要となるIPSの統合を、スループット (Gbps) ベースの優れた価格性能比で実現します。R70セキュリティ・ゲートウェイのオープン・パフォーマンス・アーキテクチャは、パフォーマンスや接続性を犠牲にすることなく、ますます進化するアプリケーション層の脅威からネットワークを保護することを可能にします。ClusterXL、SecureXL、CoreXL、高速化したIPSエンジンなど、パフォーマンス向上を実現するさまざまな特許取得済み技術により、IPSの統合においてすべての要件を満たすパフォーマンスを提供します。R70セキュリティ・ゲートウェイに関する詳しい情報については、インターネット・セキュリティの分野で世界をリードするチェック・ポイントまでお問い合わせいただくか、<http://www.checkpoint.co.jp/products/softwareblades/architecture/index.html>をご覧ください。

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、世界の企業向けファイアウォール、パーソナル・ファイアウォール、データ・セキュリティ、およびVPN市場をリードしています。チェック・ポイントは、情報セキュリティの分野に注力するセキュリティの専門企業であり、ネットワーク・セキュリティからデータ・セキュリティ、セキュリティ管理ソリューションに至る広範な製品を提供しています。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、リモート・ユーザ、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幅広いセキュリティ・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。また、業界をリードするデータ・セキュリティ・ソリューションであるCheck Point Endpoint Security製品ラインナップを通じ、PCやモバイル端末に保存されている各種企業データや重要なデータの暗号化と保護を提供します。数々の受賞歴のあるチェック・ポイントのZoneAlarm Internet Security Suiteをはじめとするコンシューマ向けセキュリティ・ソリューションは、世界中で何百万にも及ぶお客様のPCをハッカー、スパイウェア、およびデータ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、何百社もの各分野のトップベンダーが提供する最高の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、世界中のパートナー・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。

©2003-2009 Check Point Software Technologies Ltd. All rights reserved.

Check Point, AlertAdvisor, Application Intelligence, Check Point Endpoint Security, Check Point Endpoint Security On Demand, Check Point Express, Check Point Express Cl, Check Pointのロゴ, ClusterXL, Confidence Indexing, ConnectControl, Connectra, Connectra Accelerator Card, Cooperative Enforcement, Cooperative Security Alliance, CoreXL, CoSa, DefenseNet, Dynamic Shielding Architecture, Eventia, Eventia Analyzer, Eventia Reporter, Eventia Suite, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Hacker ID, Hybrid Detection Engine, IMsecure, INSPECT, INSPECT XL, Integrity, Integrity Clientless Security, Integrity SecureClient, InterSpect, IPS-1, IQ Engine, MailSafe, NG, NGX, Open Security Extension, OPSEC, OSFirewall, Pointsec, Pointsec Mobile, Pointsec PC, Pointsec Protector, Policy Lifecycle Management, Provider-1, PureAdvantage, PURE Security, puresecurityの logo, Safe@Home, Safe@Office, SecureClient, SecureClient Mobile, SecureKnowledge, SecurePlatform, SecurePlatform Pro, SecuRemote, SecureServer, SecureUpdate, SecureXL, SecureXL Turbocard, Security Management Portal, Sentivist, SiteManager-1, SmartCenter, SmartCenter Express, SmartCenter Power, SmartCenter Pro, SmartCenter UTM, SmartConsole, SmartDashboard, SmartDefense, SmartDefense Advisor, Smarter Security, SmartLSM, SmartMap, SmartPortal, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, SMP, SMP On-Demand, SofaWare, SSL Network Extender, Stateful Clustering, TrueVector, Turbocard, UAM, UserAuthority, User-to-Address Mapping, UTM-1, UTM-1 Edge, UTM-1 Edge Industrial, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Express, VPN-1 Express Cl, VPN-1 Power, VPN-1 Power Multi-core, VPN-1 Power VSX, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 UTM, VPN-1 VSX, Web Intelligence, ZoneAlarm, ZoneAlarm Anti-Spyware, ZoneAlarm Antivirus, ZoneAlarm Internet Security Suite, ZoneAlarm Pro, ZoneAlarm Secure Wireless Router, 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。ZoneAlarm is a Check Point Software Technologies, Inc. Company. 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、5,987,611、6,496,935、6,873,988、6,850,943、および7,165,076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。

Solving the Performance Hurdle for Integrated IPS

P/N:502662-J 2009.03

※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。

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