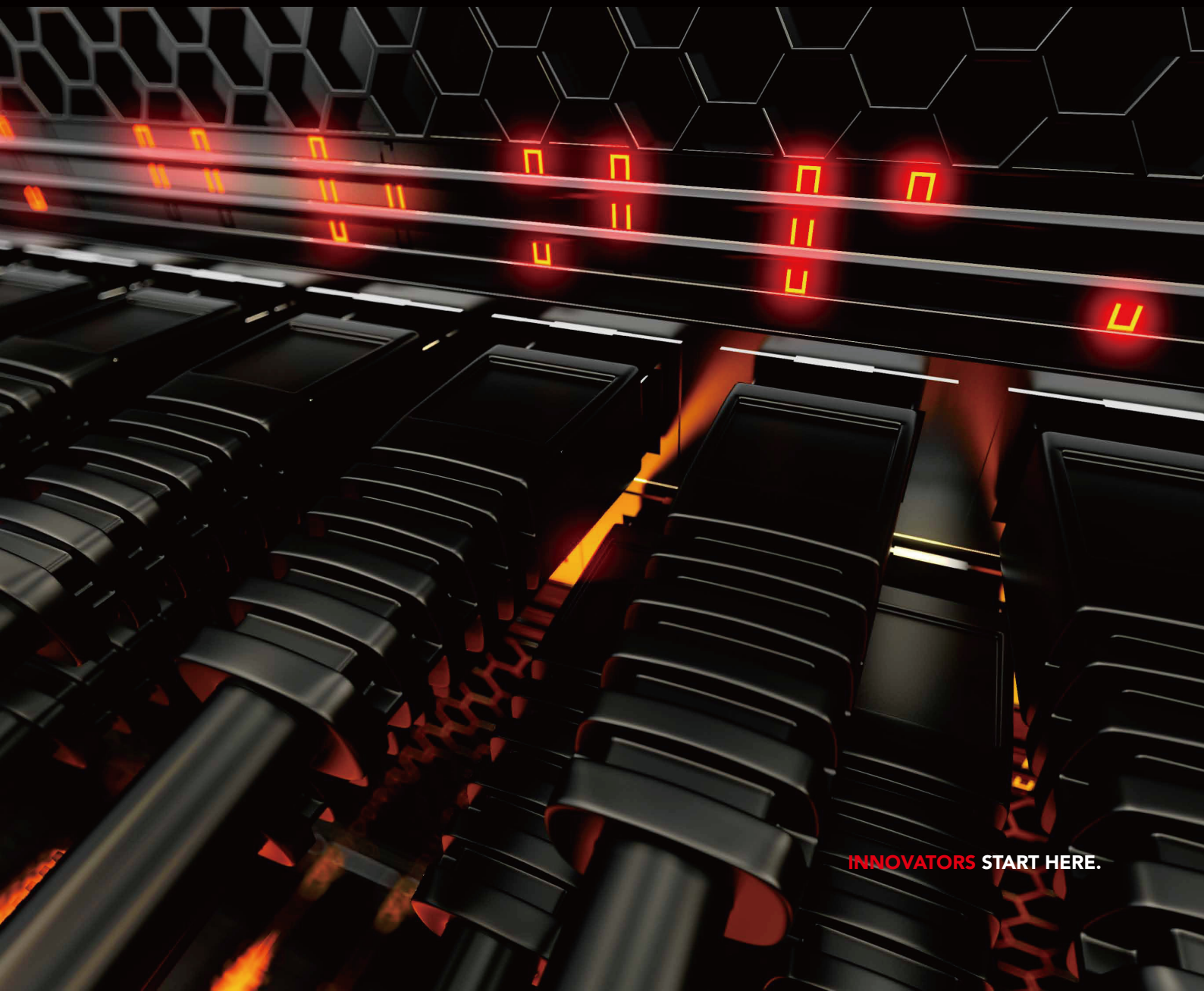
WIND RIVER

ネットワークセキュリティアプリケーション向けの アクセラレーテド ディープ パケット インスペクション

インテルXeonプロセッサにWind River Content Inspection Engineを搭載して
ハイパフォーマンスDPIを提供



WIND RIVER

概要

悪意のあるコンテンツのデータストリームをラインレートでスキャンするための、高度なセキュリティ機器の要件は、ネットワークセキュリティベンダにとって大きな課題となっています。今日のネットワークのデータレートに対処しきれないセキュリティ機器は、攻撃を見逃しやすく、セキュリティ違反のリスクが増加します。現在、DPI（ディープパケットインスペクション）としても知られる高速コンテンツスキャンが存在しますが、このテクノロジは通常、高速で動作するための専用ハードウェアが必要で、開発および製造コストが高くつくソリューションです。

マルチコア インテル® アーキテクチャを使用するソフトウェアベースのアプローチは、システムのニーズの変化に応じて進化できる柔軟性、高いコスト効果が、スケーラビリティのあるソリューションを提供できます。

Wind River® Content Inspection Engine は、シングルコアおよびマルチコア両方のプロセッサ向けのソフトウェアパターンマッチングソリューションです。ソフトウェアベースのDPIソリューションを提供し、使用コア数に応じて、1Gbps未満から160Gbpsのスケーラビリティがあります。マルチコアプロセッサ向けに最適化されたDPIテクノロジを提供することにより、小規模ネットワークアプライアンスから大規模ネットワーク要素まで、セキュリティ機器においてデータコンテンツをラインレートでスキャンするコスト効果の高いソフトウェアソリューションを提供します。

目次

INNOVATORS START HERE.

ディープ パケット インスペクション

高いクロックレート、大容量キャッシュなど高度な機能を備えた新しいプロセッサアーキテクチャにより、今までエンドシステムにしかなかった機能をネットワークセキュリティ機器に組み込むことができるようになりました。ネットワーク要素は、ブリッジングや転送を行うだけに限らず、パケット通過時にパケットをスキャンします。この技術を利用し、ネットワーク管理者は、従来型ファイアウォールに加え、不正侵入検知/防御システム(IDS/IPS)、ネットワークアンチウィルスおよびマルウェアスキャナを配備しています。また、複数のセキュリティ機能をUTM(Universal Threat Management)アプライアンスに組み込んでいる場合もあります。

パケットのヘッダのみを見る従来型ファイアウォールと異なり、より高度なこのタイプの機器では、DPIテクノロジを使用して各パケットのコンテンツを調べ、脅威を検出します。DPIテクノロジでは、パケットヘッダのフィールドのみに基づいてセキュリティの決定を行うのではなく、セキュリティアプリケーションがデータストリームのコンテンツの中を徹底的に調べ、悪意のあるコンテンツを識別できます。しかし、データストリームを詳細に調べるためコストとして、データストリームのコンテンツをスキャンするためにCPUを集中的に使用するので、トラフィック負荷が増大すると実現不能となる可能性があります。

つまり、DPIのツールとしての有効性は、負荷の下でどれほどパフォーマンスを上げられるかにかかってきます。机上の論理的条件の下で問題なく動作しても、大量のトラフィックの下では失敗してしまうシステムでは、重大なセキュリティ問題が生じます。例えとして、国境監視員がすべての自動車を停止させ、中を詳細に調査するという新しい指令を受けたとします。交通量が少ない辺鄙な国境ではセキュリティの強化になるかもしれませんが、主要な国境ではひどい渋滞が生じてしまいます。渋滞を解消しようと国境監視員が勝手に自動車を返せば混乱が生じますし、ひどくなると、制御なしでの入国を認めることになります。この状態は、まさに着信データレートに追いつけないセキュリティ機器が引き起こす恐れのある事態と同じです。パケットがキューをドロップするため、エンドシステムは再転送しなければならず、事態はさらに悪化します。または、パケットは盲目的にフェイルオープン状態で許可される可能性があります。

こういう事態を防ぎ、パフォーマンスを向上させるために、ネットワークセキュリティベンダは通常、ハードウェア支援DPIテクノロジを利用し、ネットワークの速度で詳細スキャンを実行します。この専用シリコンは高価で使い方が難しく、ソフトウェアは異なるプログラミングパラダイムを使用しなければならなくなります。そのため、維持するのが困難で、また製品ライン全体に配備するにはコストが高くつきます。
しかし、マルチコアプロセッサが登場したことにより、優れた設計のDPIソフトウェアを使ったアプローチでの対応が可能になりました。また、この方法は、従来のハードウェアベースのソリューションより優れたパフォーマンスを発揮します。

パターンマッチング

多くのDPI実装の中心には、パターンマッチングの概念があります。これは、着信バイトストリームを、シグネチャと呼ばれる既知の攻撃パターンのデータベースに照らし合わせる機能です。これらのシグネチャは、悪意のある可能性のあるコンテンツを表し、シンプルなリテラル文字列の形式にしたり、他の不適切な可変量データにより分割した特定のバイト配列など、より複雑なパターンにしたりすることができます。後者のタイプのシグネチャは、正規表現のシンタクスを使用し、独自の文法と組み合わせて記述されることがあります。

リテラル検索は非常に集中的となりますが、正規表現検索は大量のCPUリソースを使用する必要があり、特に高速での実行時に何千ものシグネチャを検索する場合に問題が生じます。図1では代表的なシステムのパフォーマンスの明らかな相違を示しています。シンプルなパケットフィルタリングを行う基本ファイアウォールを実行している場合と、同一システムで、ルールとパターンのセットに対してDPIを実行している場合を比較したものです。

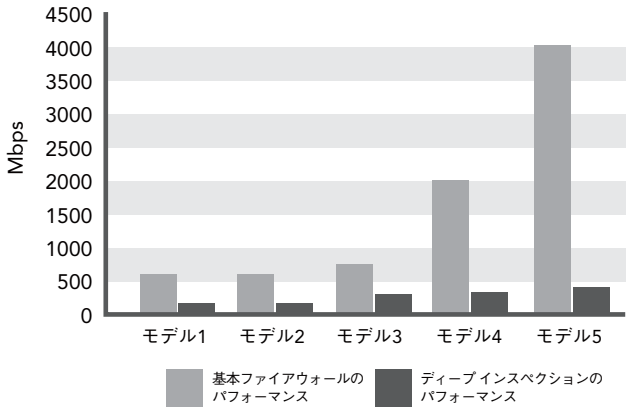


図1：ファイアウォールのパフォーマンス－基本対DPI

インテルアーキテクチャプラットフォーム上でのパケット処理

インテルアーキテクチャプラットフォームで実行されるソフトウェアが優れたパケット処理パフォーマンスを達成する理由は多くあります。新しいマイクロアーキテクチャの迅速な導入とプロセステクノロジの改善を組み合わせたインテルの「チック・タック」戦略により、IAマルチコアプロセッサは、コントロールプレーンとデータプレーン処理の両方において群を抜いたパフォーマンスを実現しています。

最近のイノベーションには、フロントサイドバス（FSB）のポイントツーポイントのインテルQuickPathインターコネクトへの交換、対称型マルチスレッディング、NUMA（non-uniform memory access）のサポート、埋め込み型広域メモリコントローラ、より高速なCRC（cyclic redundancy check）計算の新しいストリーミング命令などがあります。この緊密なインテグレーションにより、今まで以上に効率よくパケットがNICから運ばれ、ローカルメモリに入れられます。

パケットがメモリに入ると、アプリケーションソフトウェアはインテルDPDK（データプレーン開発キット）とインテルQuickAssistテクノロジを使用して、割り込みなしパケット受送信、プリフェッチおよびキャッシュ警告、NUMA認識、リアルタイムバッファマネジメントおよびゼロコピーバッファ、ロックなしリング、IA最適化最長接頭語一致、フロー分類などの機能を使用してパケット処理をスピードアップします。
これらの機能に併せ、IAプロセッサの高クロックレートや大容量キャッシュなどにより、IAマルチコアプラットフォームは低負荷処理向けおよび高負荷処理向けアプリケーションの両方に適したプラットフォームとなりました。また、市場最先端のパケット処理機能や、暗号処理、圧縮、DPIなど集中的なデータパスワークロードの加速化が可能になっています。

アーキテクチャの高度な機能と、インテルDPDKおよびインテルQuickAssistテクノロジは、強力なサポートツールセットに支えられて、最もスケーラビリティのある最高のパフォーマンスのソリューションを市場にすばやく効率よく投入するための新世代製品を生み出しています。

優れたパターンマッチャーは、シグネチャ数に関係なく、ディターミニスティック（決定論的：応答性に対する時間保証）に優れたパフォーマンスで、着信バイトストリームをシグネチャデータベースに照らし合わせることができます。つまり、パターンマッチャーは、総当たり方式（着信バイトストリームを順次各シグネチャと比較する）よりはるかに優れたパフォーマンスを発揮します。データストリーム内を繰り返し行ったり来たりするのは、キャッシュ効率が非常に悪く、パターン数に応じた拡張ができません。

一部のソフトウェアベースのパターンマッチャーでは、トライベースのアルゴリズムを使用してこの総当たり方式の欠点を克服しているものもあります。この場合、検索するパターンセットを、パターン間の関係をマッピングするデータ構造に整理しています。着信パケットが到着すると、ソフトウェアはマップのみを見てマッチがあるかどうか調べます。これは、IPアドレスルックアップの実行方法と類似しています。

この方法は、パターン数が増加するのにつれ、総当たり方式よりパフォーマンスが良くなりますが、シグネチャ数とプロセッサのキャッシュサイズによっては、欠点もあります。このようにトライ検索すると、1パケット当たりかなりのメモリアクセスが生じ、最悪の場合、受信1バイト当たり1メモリのアクセスが生じます。そうすると、総当たり方式に比べてパフォーマンスが改善されることにはなりません。

このように、DPIテクノロジはますます高度になってきていますが、効果的なパフォーマンスの拡張という課題も生じています。検査がより徹底的に細粒化されると、より多くの処理が必要となります。また、それに伴い、現在公開されている最新のスキャン方式の代わりを見つけることが、より重要になってきます。

ウインドリバーのソリューション

業界の多くのパターンマッチャーは、キャッシュフレンドリではないアルゴリズムによる簡単な順次型手法として実装されるか、待ち時間およびスケーラビリティが問題となりがちな専用ハードウェアの機能として実装されています。ウインドリバーのソフトウェアパターンマッチングソリューションを活用することで、機器ベンダはコスト効果よくDPIパフォーマンスを促進し拡張することが可能です。

Wind River Content Inspection Engine はポータブルで、OS に依存しない、マルチスレッド型ソフトウェアパターンマッチングライブラリです。簡単にインテグレーションおよび設置ができる、libPCRE の代わりとなる製品です。PCRE（Perl 互換正規表現）シンタクスの大規模サブセットをサポートするだけでなく、libPCRE よりはるかに優れたパフォーマンスを提供します。Content Inspection Engine をインテルアーキテクチャプラットフォームに配備すると、ハイパースレッディング、レシーブサイドスケーリング、SIMD 命令などの機能を利用して、最大 160Gbp のスキャンパフォーマンスを実現できます。また、従来型の正規表現だけでなく、アンカー、文字クラス、バウンドの繰り返しなどを含め、大部分のセキュリティとデータネットワーキングアプリケーションに必要なさまざまな他のシグネチャもサポートします。

データベース内の各パターンに照らし合わせてデータストリームを繰り返し行ったり来たりする順次型手法と異なり、Content Inspection Engine のパフォーマンスは検索するパターン数に直接依存しません。データストリームは、シグネチャセット内のすべての正規表現について同時にスキャンされ、マッチが検出されるとアプリケーションに返されます。Content Inspection Engine のパフォーマンスはディターミニスティックで、従来型のスキャンシステムに通常見られるような大きなパフォーマンスの揺れはありません。

各着信パケットを独立してスキャンしたり、再結合したデータストリームとしてスキャンすることで、パケット内における攻撃の検出を実現します。たとえば、セキュリティアプリケーションは、TCP（伝送制御プロトコル）ストリームを再アセンブルし、Content Inspection Engine ライブラリを呼び出してスキャンできます。部分マッチを記録するので、そのストリームにさらに多くのデータが到着すると、中止した場所からスキャンの再開が可能です。

スモールシグネチャフットプリント

通常の表現検索ソリューションの主要コンポーネントはコンパイラです。コンパイラは、シグネチャセットをバイトコードに変換し、パターンマッチングエンジンが理解できるようにします。コンパイラによっては、シグネチャフットプリントが小さいものがありますが、これらは順次型検索をサポートするエンジン向けのことが多いため、小規模データベースの利点はスケーラビリティのなさに相殺されてしまいます。

また、大規模で複雑なデータベースを構築するコンパイラもあります。ここにはパターンの関係情報があり、何千ものシグネチャの検索が平行処理されますが、メモリフットプリントは大きくなります。平行スキャンが可能なデータベースは、本質的に大規模です。すべてのパターンと共にその関係も保存する必要があるので、シグネチャの性質によっては指数的に増大する可能性があります。大規模データベースにより、プロセッサキャッシュのオーバーフローや、過度のメモリアクセスが生じる可能性があるという欠点があります。多い時は、1 アクセスが処理するのに 1 バイトが必要になります。

いずれの手法も、机上のシナリオではよい結果がでるかもしれませんが、何千ものシグネチャとデータストリームがある実世界の環境で実行すると最適なパフォーマンスには届かない可能性があります。Content Inspection Engine は、従来のデータベースの平行スキャンにつきもののメモリフットプリントの増大なしで、何千ものシグネチャを平行スキャンします。Content Inspection Engine コンパイラは、独自の技術を使用して、シグネチャセットの主要部分を取り出すデータベースを構築しており、大部分の使用事例の場合、全データをプロセッサキャッシュに保存できるほど小さなフットプリントのデータベースとなっています。データベースをコンパクトにしておくことで、外部メモリへのアクセスは、通常の操作ではほとんど必要なくなります。構成によっては、マッチが生じた場合のみ外部メモリアクセスが生じることがありますが、これは、パターンマッチングエンジンでは理想的な動作です。

パフォーマンスの直線的拡張

Content Inspection Engine は対称型マルチスレッディングを利用することで、使用するハードウェアスレッド数に対して、直線的にパフォーマンスを拡張します。各スキャンは他のスキャンと独立して実行されるので、パフォーマンスに悪影響を及ぼすことなく、異なるデータストリームを同時処理できます。

マルチスレッディング自体は、優れたスキャンパフォーマンスを保証するには十分ではありません。他のソフトウェアパターンマッチャーも実際、マルチスレッド・アーキテクチャである場合もありますが、共有パターンデータベースに対する各スレッドのコンテンションにより、スケーラビリティが制限されます。

Content Inspection Engine内のデータベースは、メモリフットプリントが小さく、IAプロセッサのキャッシュが大きいので、各スレッドはローカルキャッシュに存在するデータベースに照らし合わせてデータをスキャンできます。これにより、マルチコアシステム内の共有メモリコンテンションが劇的に削減され、スレッド数が増加するにつれ、従来のようにパフォーマンス曲線が平らになることなく、直線的に向上します。

インテルXeonプロセッサ E5-2600シリーズのベンチマーク

パターンマッチングパフォーマンスの測定値は、多くの要因に影響されます。シグネチャのタイプと数、着信トラフィックの内容、データで検出されたマッチまたは一部マッチの数などがすべてベンチマークの結果に影響します。結果を意義あるものにするためには、テストで実際のシグネチャおよび実際のネットラークトラフィックを使用する必要があります。

パフォーマンスベンチマークは、新規デュアルソケット、クワッドコア（合計8コア）インテルXeon®プロセッサ E5-2600シリーズベースのプラットフォーム上でContent Inspection Engineライブラリを実行し、主要なセキュリティ機器ベンダから調達した現在のIPSシグネチャ全セットを使用して行いました。

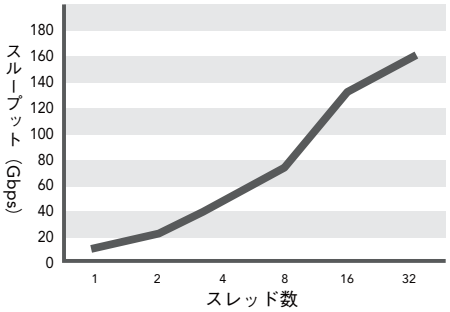
入力は、PCAPファイルで取得して再生した実際のHTTPトラフィックから得ました。簡単なアプリケーションを書いて、PCAPファイルをメモリに読み込み、Content Inspection Engine APIをパケット毎に呼び出し、IPSやWebプロキシなど実際のネットワークアプリケーションの動作をシミュレーションしました。脅威が複数のパケットに渡っていると思われる場合には、ストリーミングモードでデータをマッチし、脅威が単一パケットのデータに含まれていると思われる場合には、非ストリーミングモードでデータをマッチしました。

使用したシグネチャセットには、クライアント宛/サーバー宛両方の複数の変数およびURI（uniform resource identifier）セットが含まれます。すべてのシグネチャは3秒以内にランタイムデータベースにコンパイルされました。

ベンチマークアプリケーションでは特に、PCAPファイルの読み取りおよびスキャンの前処理および後処理の時間を除いた、生のパターンマッチングパフォーマンスを測定しました。パターンマッチングに使用したすべてのデータは、このベンチマーク用にメモリに保存したデータです。

図2の結果では、8スレッドまではほぼ直線的なスケーラビリティが見られ、32スレッドに近づくとやや緩やかになります。32スレッドで、生のDPIスキャンパフォーマンスは最高の160Gbpsとなります。

インテルXeonプロセッサ E5-2600シリーズに搭載したWindRiver Content Inspection Engineのパフォーマンス



Tier-1 ベンダ IPS シグネチャとHTTPテストトラフィック	Wind RiverContent Inspection Engine のスループット（Gbps）					
Signature Set Type	1 Thread	2 Threads	4 Threads	8 Threads	16 Threads	18 Threads
Streaming, 69 Complex Signatures	11.9	23.3	46.3	74	132.4	159.5
Streaming, 142 Complex Signatures	6.2	12.4	24.5	43.1	81.8	95.2
Streaming, 43 Complex Signatures	3.8	7.5	14.9	25.7	48.5	56.7
Streaming, 235 Complex Signatures	1.4	2.8	5.5	10	19.1	20.8
Non-streaming, 13K Medium-Complexity Signatures	1.2	2.3	4.7	8.6	16.5	19.9
Non-streaming, 8K Medium-Complexity Signatures	2.2	4.4	8.7	16	30.6	34.4

図2：現在のIPSシグネチャと実際のHTTPトラフィックを使用した場合の、Wind River Content Inspection Engineのパフォーマンス

図3では、共通のシグネチャセットとデータストリームを使用しつつ、実際のプロセッサ自体を変えて、Content Inspection Engine ライブラリを実行した場合のパフォーマンスの向上を示しています。すべてのプラットフォームはデュアルソケット、クワッドコアシステム（8コア）です。同一のAPIを使用し、同一のContent Inspection Engineソフトウェアライブラリを、IAファミリ内の異なるプロセッサで使用した場合、生のスキャンパフォーマンスは、希望の機器のパフォーマンスと価格ポイントに比較的一致して上下します。

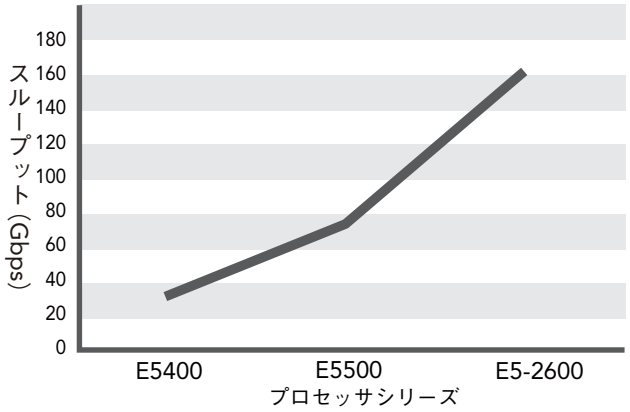


図3：マルチコアインテルプロセッサを使用した、
Wind River Content Inspection Engineのパフォーマンスの拡張

結論

ネットワークセキュリティ機器ベンダは、製品を単一プラットフォームに統合する場合に、妥協しなければならないことがよくあります。低負荷処理およびシンプルなパケットフィルタリング向けに設計されているハードウェアおよびソフトウェアは、大企業の高度セキュリティアプリケーション向けに設計されているハードウェアおよびソフトウェアと大きく異なることがあります。しかし、初期開発コストの削減と継続的なソフトウェア管理を考えると、統合は価値ある目標となります。コストを削減しながらも新製品をすばやく提供し続ける、という市場からの圧力を考えると、平行開発を行う組織が、異なるプラットフォーム上で類似製品を作成するのは、もはや不可能です。

そのため、ベンダは、製品ファミリ内のすべての製品上で同一ソフトウェアを使用できるように、予測可能なパフォーマンス、および、高レベルのスケーラビリティとフレキシビリティを提供する機動力のあるプラットフォームを求めています。これは、マルチコアプロセッシングを利用して、1Gbps未満の小規模アプライアンスから数Gbpsの大規模ネットワーク機器に至るまで、広範な製品ラインに使用できるソフトウェア専用ソリューションを採用することによってのみ実現可能です。

Wind River Content Inspection Engineのパターンマッチングソリューションを使用すると、高度なセキュリティアプリケーションでDPIパフォーマンスを160Gbpsまで直線的に拡張できます。同じライブラリを、使用するハードウェアプロセッサのスレッド数を調整するだけで、大企業規模のネットワーク機器と同じようにコスト効率よく、小規模アプライアンスで使用することができます。

インテルのアーキテクチャプロセッサとWind River Content Inspection Engineを組み合わせれば、セキュリティソリューションベンダは、ネットワークのスループットを簡単に拡張できる単一プラットフォームを作成して、複数プラットフォームを作成する追加コストなしで、異なる市場セグメントのニーズを満たすことができます。

intel Intelligent Systems Alliance

ウインドリバーは組み込みソフトウェアとモバイルソフトウェアのリーディングカンパニーです。
企業がデバイスソフトウェアを、より早く高品質かつ低コスト、かつ高信頼性で開発、運用、管理することを可能にします。

WIND RIVER ウインドリバー株式会社

東京本社
〒150-0012 東京都渋谷区広尾1-1-39 恵比寿プライムスクェアタワー
TEL.03-5778-6001（代表）

大阪営業所
〒532-0011 大阪市淀川区西中島7-5-25 新大阪ドイビル
TEL.06-6100-5760（代表）

www.windriver.co.jp

© 2012 Wind River Systems, Inc. Wind River、およびVxWorks は、Wind River Systems, Inc. の登録商標です。記載されているその他の商標は、各所有者に帰属します。
詳細：www.windriver.com/company/terms/trademark.html Rev.06/2011

■販売代理店

121221WRKK（0050_CIE_WP_1012）