防御とパフォーマンスが重要な理由とは

ダニエル・アユーブ（CISSP、CISM、CISA）

次世代ファイアウォールは、マルチコアアーキテクチャとリアルタイムのディープパケットインスペクション機能を組み合わせることで、今日のエンタープライズネットワークで求められる防御とパフォーマンスの要件を満たします。

概要

次世代ファイアウォール（NGFW：Next-Generation Firewall）では、防御とパフォーマンスを切り離して考えることはできません。セキュリティのために性能と生産性を犠牲にすることは避けるべきです。旧式のファイアウォールはネットワークパケットのデータペイロードの検査に対応しておらず、深刻なセキュリティリスクを伴います。多くのベンダーはステートフルパケットインスペクション（SPI：Stateful Packet Inspection）のスピードのみをアピールしていますが、セキュリティとパフォーマンスの真の判断基準となるのはディープパケットインスペクション（DPI：Deep Packet Inspection）の性能と有効性です。これを補うために、ファイアウォールベンダーの多くは、従来のデスクトップアンチウイルス技術で用いられているマルウェアインスペクションのアプローチを採用しています。ダウンロードされたファイルをバッファリングした上でマルウェアの検査を行うというこの方法の場合、一時メモリストレージの最大ファイルサイズが制限される可能性があるため、大幅な遅延が生じるだけでなく、深刻なセキュリティリスクを伴います。NSS Labs が実施した独立テストによって、マルチコアアーキテクチャと Reassembly-Free Deep Packet Inspection®（RFDPI）を統合した Dell™ SonicWALL™ SuperMassive™ E10800 次世代ファイアウォールがこれらの制限を解消し、企業で求められる極めて高度な防御機能とパフォーマンスの両方を提供できることが実証されました。

[1] "Defining the Next-Generation Firewall," Gartner RAS Core Research Note G00171540, John Pescatore, Greg Young, 12 October 2009, R3210

次世代ファイアウォールの定義

分かりやすく説明すると、NGFW とは、侵入防止システム（IPS：Intrusion Prevention System）にアプリケーションのインテリジェンスと制御を統合することで、DPI ファイアウォール技術を活用するというものです。

業界の定義

Gartner では、NGFW を「徹底的なトラフィック検査を行い、攻撃をブロックする、ワイヤ速度の統合ネットワークプラットフォーム」と定義しています。[1] Gartner によると、NGFW は最低限以下の要件を満たしている必要があります。

- 中断を伴わないインラインの bump-in-the-wire 構成
- 標準的な第 1 世代ファイアウォール機能（ネットワークアドレス変換（NAT：Network-Address Translation）、ステートフルプロトコルインスペクション（SPI：Stateful Protocol Inspection）、仮想プライベートネットワーキング（VPN：Virtual Private Networking）など）
- 統合シグネチャベースの IPS エンジン
- アプリケーション認識、フルスタックの可視性、きめ細かな制御
- ファイアウォールの外からの情報（ディレクトリベースのポリシー、ブラックリスト、ホワイトリストなど）を取り込むための機能
- 将来の情報フィードやセキュリティ脅威を取得するためのアップグレードパス
- 有害な暗号化されたアプリケーションの識別を可能にする SSL 復号化

次世代ファイアウォールの進化

これまでのファイアウォール

1980 年代に利用されていた第 1 世代のファイアウォールは、ポート、プロトコル、MAC/IP アドレスなどの基準に基づきパケットフィルタリングを提供し、OSI モデルの第 2、第 3 層で動作するというものでした。1990 年代には、SPI 機能が統合された第 2 世代のファイアウォールが登場しました。これらは、状態テーブルを基準に受信/発信トラフィックの状態を検証し、OSI モデルの第 2、第 3、第 4 層で動作します。2000 年代に入って登場した第 3 世代のファイアウォールは、処理能力がさらに向上し、パケットペイロード全体の DPI、侵入防止、マルウェア検出、ゲートウェイアンチウイルス、トラフィック解析、アプリケーション制御、IPSec、SSL VPN など多様な機能を備えています。コンテンツフィルタリングや、データ漏えい防止、侵入検知、アンチマルウェアといった機能は、複数のシステムを使って提供するのがこれまで一般的とされてきました。ファイアウォールは、単に侵入を防止するだけでなく、このような機能もあわせて実行する製品へと変わりつつあります。その進化における次なるトレンドを象徴する機能が、統合脅威管理（UTM：Unified Threat Management）です。

次世代ファイアウォール

現在、Web 2.0 アプリケーション（Salesforce.com、SharePoint、Farmville など）の運用には TCP ポート 80 および暗号化された SSL（TCP ポート 443）が使用されています。今日の NGFW はパケットのペイロードを検査し、既知の脆弱性や、エクスプロイト攻撃、ウイルス、マルウェアなどの不正なアクティビティのシグネチャの照合をオンザフライで実行します。DPI ではまた、管理者が詳細な許可/拒否ルールを設定し、特定のアプリケーションや Web サイトを制御できるようになっています（Yahoo インスタントメッセンジャーのチャットは許可するが、ファイル転送は許可しないなど）。パケットのコンテンツが検査されることから、あらゆる統計情報をエクスポートすることが可能です。つまり管理者は、トラフィックの解析情報を容易にチェックでき、キャパシティプランニングやトラブルシューティングのほか、社員の 1 日の行動の監視も行えます。今日のファイアウォールは OSI モデルの 2、3、4、5、6、7 層で動作するようになっています。

NGFW の機能要件

次世代ファイアウォールの機能要件は以下のようになっています。

レガシー機能

NGFW には、パケットフィルタリングや、ステートフルパケットインスペクション、ネットワークアドレス変換（NAT：Network Address Translation）、ハイアベイラビリティ（HA：High Availability）など、第 1 世代のファイアウォールに含まれる標準機能がすべて備わっています。

統合 IPS

効果的な侵入防止システムには、検知回避技術に対抗し、受信/発信通信のスキャニングや検査により、悪質な、または疑わしい通信とプロトコルを特定するための高度な機能が求められます。侵入防止ならびに脅威防御を効果的に行うには、アプライアンス、GUI、導入を個別に管理する手間のかからない、ベストインクラスのファイアウォールと侵入防止機能が必要です。IPS 機能を実装した NGFW は、エンタープライズクラスの evasion 攻撃耐性、強力なコンテキスト/コンテンツ保護機能、ならびに包括的な脅威防御とアプリケーション制御を 1 台の統合デバイスで提供します。

アプリケーションのインテリジェンスと制御

アプリケーションの認識と制御は、プロトコルレベルでの実行、アプリケーションのきめ細かな制御によるフルスタックの可視性、使用されているポートやプロトコルに関係なくアプリケーションを識別できる能力で構成されます。

ファイアウォール外の情報

ユーザ ID を認識することで、管理者は（IP アドレスをたどってユーザ ID を調べな

くても）AD ユーザ/グループに基づきアプリケーションポリシーを実行し、使用状況とトラフィックを把握することができます。

適応性

脅威の変化に動的に適応することも、NGFW の重要な機能の 1 つです。Dell SonicWALL は、デバイスを新しいシグネチャにより定期的に更新することで脅威を遮断し、絶え間なく変化するマルウェアを巡る状況を常に把握できるようにします。

ペイロードスキャニングとパフォーマンス

上記のすべての要件において、パフォーマンスのためにセキュリティを犠牲にしなくてもすむように、最適なスループットレートでのフルペイロードのスキャンを行うことが求められます。

パフォーマンス

帯域幅サービスで最高の投資収益率（ROI）を達成し、組織の生産性レベルの最適化を図りつつ、最上級のセキュリティを維持するには、遅延を最小限に抑えることで最適なスループットを確保し、トラフィックのスキャンを円滑に行えるようにする必要があります。これらの要件を満たすために、マルチギガビットのスループットレートが NGFW の標準性能として定められています。Dell SonicWALL NGFW ソリューションは、特許取得済みの Dell SonicWALL RFDPI[2] テクノロジーを適用することで、バッファリングとパケットの再構築を行うことなく DPI を有効化できることから、パフォーマンスの大幅な向上につながります。ハードウェア面から見ると、Dell SonicWALL NGFW は最新のマルチコアアーキテクチャとパラレルプロセッシング技術を組み合わせることで、スループットの最大化にも対応します。

次世代ファイアウォールが必要な理由とは

SPI 世代のファイアウォールが対応していたのは、マルウェアが深刻な問題ではなく、Web ページがただの読み物だった時代のセキュリティです。当時の主な管理対象は、ポート、IP アドレス、プロトコルでした。しかし、インターネットが進化し、サーバやクライアントブラウザから動的なコンテンツを配信できるようになるのと同時に、現在 Web 2.0 と呼ばれている多様なアプリケーションが登場してきました。

SPI はパケットのデータ部の検査を行わず、ハッカー達はそこをうまくついて攻撃を仕掛けてきます。このような新しい脅威に対応するために、SPI ファイアウォールベンダーは、従来のマルウェア防御技術にファイルサーバや PC で利用されていた手法を組み合わせることにしました。しかし、この方法は遅延と複雑さという 2 つの深刻な欠点を抱えており、SPI ファイアウォールにマルウェア防御を追加するための応急処置でしかありませんでした。

1 つ目の欠点はファイルのバッファリング時に遅延が生じるというものであり、ファイルのサイズにも制限がありました。ファイアウォールベンダーは keep-alive パケットを送信して遅延を防止することでこの問題に対処しようとしているものの、総体的に見て遅延が生じる結果となっています。検査時のファイルのバッファリングにメモリーを利用することで、さらなる遅延が生じるだけでなく、容量の問題も発生することから、ファイルサイズを事前に設定した値（通常は 100MB）に制限することで、これに対処しています。インターネットの利用が拡大し、大型ファイルの共有が増加する一方で、SPI/マルウェア検出のハイブリッドテクノロジーは拡張に対応していないのが現状です。

2 つ目の欠点は、従来のポイントソリューションは導入、管理、更新が困難で、運用の複雑化とオーバヘッドコストの増大を招いてしまうことでした。巧妙化した攻撃は従来のステートフルパケット検査製品を突破してしまいます。これらのソリューションでは、複雑化する脅威に対抗するための、高性能でタイムリーな統合型の防御を提供することはできません。

[2] U.S. Patents 7,310,815; 7,600,257; 7,738,380; 7,835,361

これらの欠点を克服するために、Dell SonicWALL は現在入手可能なものの中でもっとも効果的で高性能な NGFW ソリューションを提供します。先頃、テキサス州オースチンにある NSS Labs の研究施設で、 Dell SonicWALL の次世代ファイアウォールの独立テストが実施され、SonicOS 6.0 搭載の SuperMassive E10800 が最高評価の「Recommend（推奨）」ステータスを 2 年連続で獲得しました。この実証済みの SonicOS アーキテクチャは、すべての Dell SonicWALL ファイアウォール製品のコアとなる技術です。NSS Labs のテスト結果については、本稿の最後で詳しく説明します。

企業に必要なものとは

多くの組織はアプリケーションカオスという問題に直面しています。今や、ネットワーク通信は E メールのような蓄積交換型のアプリケーションだけに依存しているわけではありません。利用されるツールは、リアルタイムコラボレーションツール、Web 2.0 アプリケーション、インスタントメッセンジャー（IM：Instant Messenger）やピアツーピアアプリケーション、Voice over IP（VoIP）、ストリーミングメディア、テレカンファレンシングにまで広がってきており、それぞれが攻撃の経路となる危険性をはらんでいます。ネットワークや事業目的で使用しているアプリケーションと、無駄で危険性の高いアプリケーションとを区別できずにいる組織は少なくありません。

今日の組織は、クリティカルアプリケーションを提供すると同時に、社員が無駄で危険性の高い Web ベースのアプリケーションを利用しないように制止する必要があります。クリティカルアプリケーションに対して帯域幅の優先順位を設定する一方で、ソーシャルメディアやゲーム用のアプリケーションについては制限を設けるか、もしくは完全にブロックする必要があります。またセキュリティに関する指令や規制に従わなければ、罰金やペナルティを課されたり、損失を被ることにもなりかねません。

防御とパフォーマンス

今日の企業にとって、防御とパフォーマンスは切り離して考えることのできない課題です。従来の SPI ファイアウォールが提供する低レベルのセキュリティや、一部の NGFW に起因するネットワークボトルネックをこれ以上看過することは許されません。ファイアウォールやネットワークのパフォーマンスが低下すれば、遅延の影響を受けやすいコラボレーティブアプリケーションの品質が低下し、ひいてはサービスレベルや生産性にも悪影響が及ぶ可能性があります。さらに悪いことには、ネットワークパフォーマンスの低下を避けるために、ネットワークセキュリティソリューションの機能を犠牲にする IT 組織も出てきています。

すべてのコンテンツのスキャニングと制御

規模の大小、さらには公共か民間かを問わず、あらゆるタイプの組織が、汎用アプリケーションの持つ脆弱性に起因する新たな脅威に直面しています。ソーシャルネットワークはマルウェアの温床となっており、その一方で、人々は職場やホームオフィスのコンピュータを利用して、ブログや、ソーシャライジング、メッセージ交換、ビデオ、音楽、ゲーム、ショッピング、E メールをオンラインで楽しんでいます。

アプリケーションのインテリジェンスと制御

ストリームビデオや、ピアツーピア（P2P：Peer-to-Peer）、ホステッドまたはクラウドベースのアプリケーションなど、さまざまなアプリケーションによって、組織は侵入、データ漏えい、ダウンタイムの危機にさらされています。これらのアプリケーションはセキュリティの脅威を発生させるだけでなく、帯域幅や生産性を低下させ、貴重な帯域幅をめぐってミッションクリティカルなアプリケーションと競合します。組織にとって何より必要なのは、生産的な業務環境を可能にするスピードとセキュリティを維持しつつ、重要なビジネスアプリケーションの帯域幅を保証するツールを導入し、受信/発信のトラフィックフローを防御するためのアプリケーションのインテリジェンスと制御性を確保することです。

DPI で必要とされる高性能 NGFW

アンチマルウェアエンジンに接続されたソケットを利用してコンテンツを再構築するという旧式のプロキシ設計には、効率の悪さという欠点があります。メモリースラッシングによるオーバーヘッドによって、遅延の増加、パフォー

マンスの低下、ファイルサイズの制限といった問題が引き起こされます。旧来の DPI 方式では、メモリーでトラフィックを収集・格納し、それらをスキャンします。このようなプロキシもしくはアセンブリによるアプローチを利用する場合、容量がなくなるまでメモリーが消費され、その結果、ファイアウォールはトラフィックをスキャンすることなく通過させるか（決してあってはならないことです）、メモリーが利用できるようになるまですべてのトラフィックをブロックします。さらには、許容できない遅延が生じた場合、リアルタイムアプリケーションに悪影響が及ぶことになります。

Dell SonicWALL のアプローチ

高性能なマルチコアアーキテクチャと再構築不要の DPI テクノロジーを組み合わせることで、Dell SonicWALL 次世代ファイアウォールは業界をリードするアプリケーションインテリジェンスと制御、侵入防止、マルウェア防御、SSL 検査を、マルチギガビットのスピードで提供します。

Dell SonicWALL の特許取得済みの RFDPI[3] テクノロジーを実装した Dell SonicWALL 次世代ファイアウォールは、侵入防止、マルウェア防御、およびアプリケーションのインテリジェンス、制御、リアルタイムビジュアライゼーションを緊密に統合することで、あらゆる規模の組織にセキュリティと制御を提供します。Dell SonicWALL NGFW ソリューションはすべてのトラフィックをスキャンし、最高性能のネットワークのニーズに合わせて大規模な拡張に対応します。Dell SonicWALL のアプリケーションのインテリジェンス、制御、ビジュアライゼーションにより、管理者はビジネスおよび非ビジネスの両方のアプリケーションを制御・管理し、ネットワークとユーザの生産性を高めることが可能です。

Dell SonicWALL 次世代ファイアウォールでは、セキュリティやパフォーマンスを低下させることなく、あらゆるポートでサイズ制限なしにファイルをスキャンすることができます。同時に処理できるファイルやネットワークストリームの数に制限はなく、ファイアウォールに負荷が集中している場合でも、感染ファイルが未検知のまま防御を擦り抜けるということはありません。加えて、同ファイアウォールでは SSL 暗号化されたトラフィックに対してあらゆるセキュリティ技術やアプリケーション制御技術を適用することができ、トラフィックがマルウェアを媒介する事態を防げます。Dell SonicWALL 次世代ファイアウォールは FIPS 140-2 および Common Criteria（拡張認定）の認定を取得しています。Dell SonicWALL の製品は、GSA Schedule や NASA SEWP IV をはじめとする連邦政府契約機関で購入することができます。

RFDPI かバッファリングか

ディープパケットインスペクションファイアウォールを選択する際に、IT 管理者が念頭に置いておくべきことがあります。それは、デバイスによっては処理能力、メモリ、ストレージに制限があり、ほとんどのベンダーの製品でペイロードのバッファリングなしでは大容量ファイルの脅威検査を行えないため、遅延の発生や、検査の迂回によるセキュリティの低下といった問題が生じる結果になるということです。

Dell SonicWALL のアプローチが優れている理由

Dell SonicWALL RFDPI はこれらの課題を解消し、パフォーマンスやセキュリティを犠牲にすることなく、リアルタイムのフルパケット DPI 機能を提供します。RFDPI エンジンは、複雑なパターンマッチング、ヒューリスティック、コリレーション、リアルタイムの高度な決定方法論、正規化（X、Y、Z、その他）を組み合わせて利用します。その一方で、ファイルのサイズに関係なく、極めて高いパフォーマンス、低遅延、高効率が維持されます。

Dell SonicWALL のマルチコアアーキテクチャ

Dell SonicWALL のマルチコアハードウェアアーキテクチャには、ネットワークトラフィック処理の高速化に向けた 2 つの重要な優位性が備わっています。1 つ目は、Cavium の CPU がネットワーク通信をハードウェアレベルで「理

[3] * U.S. Patents 7,310,815; 7,600,257; 7,738,380; 7,835,361; 7,991,723

解」できるようにカスタマイズされている点です。そして 2 つ目の優位性は、複数のコアでデータストリームを並行処理できる点です。Dell SonicWALL のマルチコアアーキテクチャでは、各 CPU がネットワークパケットの一部を他の CPU と同時進行で処理できるため、有効なプロセッササイクルの最適な利用が可能になります。このような最適な組み合わせにより、パケット、コンテンツ、セキュリティの処理のための高性能で効率的なソリューションが実現します。

マルチコアアーキテクチャは、高性能マルチコアプロセッサアーキテクチャ技術にハードウェア高速化を組み合わせることで、パフォーマンスと拡張性を最大化し、消費電力を最小化します。Dell SonicWALL SuperMassive™ E10000 ファイアウォールシリーズは、電力、設置面積、冷却（PSC：Power, Space and Cooling）を考慮した設計になっており、アプリケーション制御および脅威防御において業界最高レベルの Gbps/ワット値を提供します。

他のベンダーは汎用プロセッサとセキュリティ用のコプロセッサを利用するという構成を採用していますが、このようなソリューションは拡張に対応することができません。今だに ASIC（Application-Specific Integrated Circuit）プラットフォームの設計・構築を続けているベンダーも存在します。攻撃は複雑化する一方であり、それに伴いより細かな検査要件を満たす必要があることから、従来のシングルプロセッサおよび ASIC によるソリューションでは、ネットワーク境界の内外でそれらの攻撃にリアルタイムで対応することは不可能です。

汎用プロセッサはシングルプロセッシング CPU ですべての機能をまかなっています。これらのプロセッサはセキュリティアクセラレーションに対応していません。よって高速化が必要な場合は、通常、サードパーティのセキュリティコプロセッサを追加しなければならず、開発の複雑化を招いてしまいます。汎用プロセッサは高速のクロック速度で動作し、コプロセッサを追加する必要があることから、エネルギー効率が悪く、通常の処理でもより多くの電力を消費します。加えて、汎用プロセッサとセキュリティコプロセッサをつなぐバスの速度による制約もあります。またメモリー帯域幅が制限される場合もあり、結果、パケット処理の速度の低下につながります。全体的に見て、汎用のシングルプロセッサ設計が提供する NGFW の高性能 DPI 用のハードウェアプラットフォームは理想的とは言えないものとなっています。

ASIC プラットフォームは高速パケット転送には適していますが、ネットワークセキュリティアプライアンスで使用する場合、設計上の問題があり、制約を伴います。特に深刻な問題として、ベンダーが ASIC のマイクロコードをフィールドアップグレードして、セキュリティをめぐる状況の変化に対応することが難しい点があげられます。ASIC ソリューションでは、マイクロコードスペースの不足により、パフォーマンスの大幅な低下を伴うことなく、プロトコルの変更や、標準の更新、バグに対応するための新機能を追加することができない可能性があります。よって、顧客がアプライアンスをアップグレードして将来のネットワークのニーズに対応できるという保証がなく、ASIC ベースのセキュリティアプライアンスの利用が制限されてしまいます。さらには、ASIC は極めて低速でしか DPI を実行できないため、主に SPI 用として利用されています。

Dell SonicWALL Reassembly-Free Deep Packet Inspection（RFDPI）エンジン

Dell SonicWALL RFDPI は、ファイルサイズに関係なく、ファイル、添付ファイル、および特定の圧縮アーカイブ内で照合を行うことができ、正規化されたパターンマッチングを実行するために、必要に応じて変換を行います。Dell SonicWALL RFDPI の基本アルゴリズムは、決定性有限オートマトン（DFA：Deterministic Finite Automata）を適用することで、決定論的な低遅延のマッチングを提供します。

RFDPI によって、Dell SonicWALL 次世代ファイアウォールでは防御範囲をマルウェアのブロックにまで広げることが可能です。現在入手可能な有力ソリューションのほとんどは、6 つの

プロトコル（HTTP、SMTP、IMAP、POP3、FTP、SMB）しかスキャンできず、他のプロトコルで転送される悪質なトラフィックは検査対象となりません。そのため、セキュリティに関する誤った考えが定着しています。Dell SonicWALL RFDPI は、包括的なアンチ x テクノロジーにより、毎回すべてのポートのパケットとプロトコルを残さずスキャンする唯一のソリューションであり、転送プロトコルに関係なく、既知のウイルスとマルウェアを検出しブロックすることが可能です。

その一方で、 Dell SonicWALL の RFDPI エンジンは単純なパターンマッチングよりもはるかに高度な処理に対応します。シグネチャ作成時にはパケット型などのデータも考慮に入れ、悪質なソフトウェアでのみ使われる特定のパケット型（暗号化された ICMP など）があると RFDPI が判断した場合、それだけでそのファイルは悪質と見なされます。Dell SonicWALL のインテリジェントなマルウェア検出技術は、フロー内の有害なコードを含む要素を見つけ出し、重要でないビットからなる無害なエンベロープを通して解析を行ないます。さらには、ファイルスキャニングの一環として脆弱性を特定する際に、魔法数（ファイル形式を見極めるのに使われる整数値）を解析し、それを事前に定義されたリストと照らし合わせてファイルコンテンツの実際の値と期待値とを比較することも可能です。これらの技術を使うことで、一見無害のファイルのように見える、これまで確認されていない新種のマルウェアを特定することができます。

Dell SonicWALL のファイアウォールで採用されているシグネチャの多くはカスタム記述されており、個々のマルウェア種ではなくファミリに共通して見られる特定のコードフラグメントを検出できるようになっています。つまり、ファイルや実行ファイル全体を見なくても、フローが悪質かどうか見極めることができるというわけです。RFDPI では新しい変異種に含まれるマルウェアの悪質な部分の特定が可能なことから、地下経済の一部として利用されている「商用」マルウェアの大多数に対抗する、さらなる防御が実現することになります。

事故が発生すれば、システムログの数千のエントリをくまなく探すという労働集約型の調査が必要になります。Dell SonicWALL の RFDI エンジンは、（膨大な経験値に基づく）ヒューリスティック技術を利用してこれらの事故の数を削減することで、不正行為に対するさらなる防御を提供します。インテリジェントなポリシーの作成により、パスワードで保護された圧縮ファイルのブロックや、Visual BASIC マクロが含まれる MS-Office ファイルのブロックといったヒューリスティック機能の利用が可能になります。

加えて、Dell SonicWALL Application Intelligence and Control は RFDPI を利用してすべてのパケットをスキャンし、使用中のアプリケーションとそれらを利用しているユーザを特定します。Dell SonicWALL は、ネットワークを自動的かつシームレスに防御するためのシグネチャデータベースを保持しています。すべてのネットワークトラフィックを余すことなくスキャンし、ポートやプロトコルの種類に関係なく、アプリケーショントラフィックとユーザを特定することで、完全なアプリケーションインテリジェンスと制御を提供します。

特定のモデルに対するオプションのアドオンライセンスとして提供される Deep Packet Inspection for SSL（DPI SSL）は、SSL 暗号化されたトラフィックの防御を拡張し、コンプライアンスの徹底、コンテンツフィルタリング、データ漏えいの防止を可能にすると同時に、マルウェアの新たな媒介手段を排除します。暗号化されたトラフィックはユーザに対して透過的に復号化し、検査した上で、再度暗号化し、受信と発信の両方の接続用に設定することが可能です。

また、管理者がアプリケーショントラフィックをビジュアル化して、批判的所見に基づきネットワークの利用を制御し、ネットワークポリシーを調整できることも欠かせない要件です。Dell SonicWALL Application Flow Monitor で

はアプリケーションのアクティビティに関するリアルタイムのグラフが提供されることから、管理者はポリシーを変更して、ネットワークの生産性を向上させることができます。加えて、拡張ポートを備えた NetFlow/IPFIX により、独自のトラフィック解析やビジュアライゼーションを行うことも可能です。

サードパーティによる検証

インフラストラクチャのテストが必要な理由

「2013 NSS Labs Security Value Map™（2013 年版 NSS Labs セキュリティ価値マップ）」を見ると、多くの次世代ファイアウォール製品でテスト結果が一律ではないことが分かります。NSS Labs グループの最新のテストでは、多数の製品であふれかえる次世代ファイアウォール市場の広範なデバイスのパフォーマンスとセキュリティ効果に関する詳細なデータを提供しており、潜在的購入者が十分な情報に基づき決定を下せるようになっています。

NSS Labs による検証

NSS Labs は、セキュリティ製品のテスト/認証を行う世界的な独立テスト機関です。同社の分析は、業界でもっとも包括的で現実的なテストの 1 つとして知られています。「NSS Labs Next-Generation Firewall Security Value Map™」には極めて重要なテスト結果が示されており、ブロック率（総合的防御、検知回避、検出漏れ、セキュリティの安定性を含む）と保護性能（Mbps）あたりの価格がグラフにまとめられています。Gartner は NSS Labs の認定の価値を認め、「Gartner Gartner Magic Quadrant for Network IPS」のランキングを決める際の基準の候補リストにこれらを加えています。

1991 年より、NSS Labs は情報セキュリティ調査 & テストのコミュニティを先導し、独自の価値ある情報を IT の意思決定者達に提供しています。

NSS Labs のテスト結果

最近実施された「NSS Labs 2013 Next-Generation Firewall Security Value Map™」テストで、Dell SonicWALL SuperMassive™ E10800（SonicOS 6.0 搭載）が最高評価の「Recommend（推奨）」ステータスを 2 年連続で獲得しました。

SuperMassive は最高度のセキュリティ効果を有する製品として認められ、安定性と信頼性、ファイアウォール、アプリケーション制御、アイデンティティ認識のテストにおいて 100% の評点を取得しました。検知回避、難読化、フラグメンテーションの既知の技術に対する耐性も完璧であり、Dell SonicWALL 次世代ファイアウォールはすべての関連テストで 100% を獲得しています。NSS Labs によるテストと評価では、次世代ファイアウォール性能である 16.6 Gbps での SuperMassive E10800 の動作が審査され、演算負荷の高い SSL 復号化テストにおいて、同製品は競争力のある TCO を維持しつつ、マルチギガビットへの性能拡張を行うことに成功しました。

NSS Labs の分析結果にはこうあります。「次世代ファイアウォールは、ポートだけでなく、アプリケーション単位でのきめ細かな制御を提供できるものでなければならない。不要なアプリケーションが HTTP/S 経由で侵入してくることのない安全な境界を再構築するには、このような機能が必要である。また、きめ細かなアプリケーション制御によって、管理者はポートだけでなくアプリケーションごとにセキュリティポリシーを定義することができる。このことからも、同機能は次世代ファイアウォールにとって欠かせない要件と言える」。SuperMassive E10800 は、「不要なアプリケーションのブロック」と「特定のアクションのブロック」において 100% の評点を獲得しました。NSS Labs のテストにより、Dell SonicWALL SuperMassive E10800 が複数のルール、オブジェクト、アプリケーションで構成される複雑な発信と受信のポリシーを正しく実行することが確認されました。SuperMassive では、特定のアプリケーションのための標準外のポートを含むすべてのポートに対して、アプリケーション制御を実行することが可能です。

さらには、「2012 NSS Labs Security Value Map（SVM）for IPS」にもあるように、IPS を統

合した SuperMassive E10800 Next-Generation Firewall は NSS Labs の「Recommend（推奨）」ステータスを獲得しただけでなく、多くの IPS ベンダーの製品を凌駕する性能を発揮しました。NSS Labs のレポートにはこうあります。「Dell SonicWALL SuperMassive SonicOS 6.0 は既知の検知回避技術に対する完全な耐性を備えており、すべての関連テストにおいて 100% の評点を獲得。同製品は、IP フラグメンテーション、TCP ストリームセグメンテーション、RPC フラグメンテーション、URL 難読化、HTML Evasion、FTP Evasion のすべての攻撃を、惑わされることなく、正しく検知した。フラグメント化や難読化を使った攻撃のブロックに成功しただけでなく、それらすべてを正確に復号化した」

まとめ

独立テストによって実証されたとおり、Reassembly-Free Deep Packet Inspection テクノロジーをサポートする Dell SonicWALL のマルチコアアーキテクチャは、徹底的な防御とエンタープライズ級のパフォーマンスを提供します。TZ シリーズから SuperMassive E10800 まで、すべての Dell SonicWALL ファイアウォール製品のコアに SonicOS アーキテクチャが採用されていることから、組織は実証済みの製品ラインの中から 1 つを選択し、最高性能のネットワークのニーズに合わせて大規模な拡張を行うことが可能です。

Dell SonicWALL SuperMassive E10000 シリーズは、大企業、公共機関、大学、マルチテナント/サービスプロバイダーのニーズを満たす設計となっており、拡張性、信頼性、および徹底的なセキュリティをマルチギガビットのスピードで提供します。この統合ソリューションは、Dell SonicWALL RFDPI エンジンを利用してすべてのパケットを余すことなくスキャンすることにより、高性能と低遅延を確保しつつ、ストリーム全体のコンテンツの全検査と高度な侵入防止機能、マルウェア防御、アプリケーションインテリジェンス、制御とリアルタイムのビジュアライゼーション、SSL 暗号化されたセッションの検査を提供します。

SuperMassive 9000 シリーズ次世代ファイアウォールプラットフォームは、効率性とパワフルさを兼ね備えたソリューションにより、E10000 シリーズと同じ高度な防御機能とパフォーマンスを企業にもたらします。SuperMassive 9000 は拡張性、信頼性、および徹底的なセキュリティをマルチギガビットのスピードで提供する設計となっており、パフォーマンスを犠牲にすることなく、究極のセキュリティを提供します。

Dell SonicWALL TZ 215、Network Security Appliance（NSA）シリーズ、E-Class NSA シリーズ、SuperMassive 9000 および E10000 シリーズからなる Dell SonicWALL 次世代ファイアウォール製品は、従来のファイアウォールソリューションの制約を解消し、企業が重要な事業目標を達成するためのネットワークパフォーマンスを確保しつつ、新たな脅威に対応するためにネットワークセキュリティを拡張することを可能にします。