ソリューション ショーケース

シスコによる拡張次世代ファイアウォール プラットフォームの導入

日付:2016 年 2 月 **著者**:Jon Oltsik、シニア主任アナリスト

摘要:次世代ファイアウォール(NGFW)は当初、アプリケーションとネットワーク保護を専用のネットワーク アプライアンス上で統合する万能薬として市場に投入されました。確かに NGFW は進歩の象徴でした。しかしその製品の多くは、ソフトウェア統合、脅威管理機能、高パフォーマンス、および全体的なシステム管理が不十分でした。ESG では、このような短所は次世代ファイアウォール プラットフォームの導入によって解決されるだろうと考えています。次世代ファイアウォール プラットフォームは、拡張性、高スループット、包括的な脅威管理、一元的なコマンドや制御を意図して設計されています。シスコによる Firepower NGFW の発表は、この種のプラットフォームに相当します。リスクの低減、脅威管理の改善、セキュリティ運用の合理化を求める企業 CISO からの関心を集めることが期待されます。

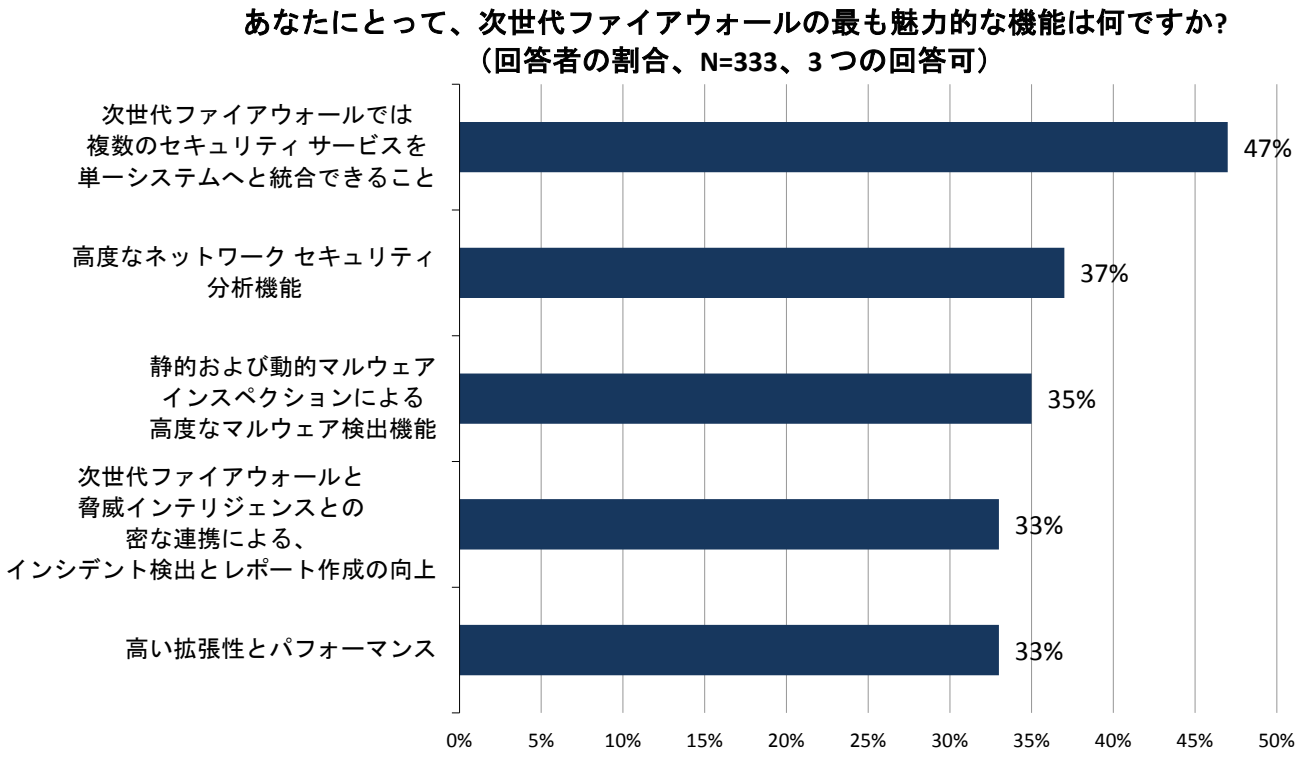
概要

ESG の調査によると、2014 年、次世代ファイアウォールを導入済みの企業組織は 30%、NGFW の実装段階にある企業組織は 33% でした。[1]NGFW がこれほど注目されているのはなぜでしょうか?ESG の調査では、セキュリティ プロフェッショナルが特に魅力を感じている NGFW の機能は、セキュリティ サービスの統合、高度なネットワーク セキュリティ分析機能、高度なマルウェア検出機能であることが明らかになりました(図 1 参照)。[2]

[1] 出典:ESG Research Report、*Network Security Trends in the Era of Cloud and Mobile Computing (クラウドとモバイル コンピューティングの時代におけるネットワーク セキュリティの動向)* [英語]、2014 年 8 月。

[2] 出典:同上。

図 1. 次世代ファイアウォールの魅力的な機能 トップ 5



出典:Enterprise Strategy Group、2016

NGFW の現実

次世代ファイアウォールは、アプリケーション制御、ネットワーク制御、脅威管理などの機能を単一の統合システム上で実現することを約束していました。しかし、この謳い文句は多くの場合実状とはかけ離れています。サイバーセキュリティの専門家は、NGFW について次のような欠点に不満を訴えています。

- **パフォーマンス上の問題。**次世代ファイアウォールの中には、さまざまなサービスが付属しているものがあり、「1 つの製品で数多くのことが可能になる」というような幻想を生み出しています。現実には、単一の製品で使用されるサービスが多くなりすぎると、NGFW のパフォーマンスは低下します。よって、ネットワークの圧迫や重要な業務アプリケーション/サービスが中断される可能性があることが概念実証テストによって明らかになると、統合計画が打ち切られることがあります。

- **アプリケーション層統合の欠如。**ディープ パケット インスペクション、IDS/IPS、マルウェア対策機能などのファイアウォール サービスは、緩い連携に留まっていることがあります。このため、NGFW は革新的なサイバーセキュリティ技術というよりは Unified Threat Management（UTM 統合脅威管理）アプライアンスの漸進的な改善になってしまっています。

- **基本レベルの脅威管理。**当初の次世代ファイアウォールにおける脅威管理は、ネットワークベースのウイルス対策や署名のみに基づく侵入検知、気休め程度の Web 脅威保護といった安全サービスにとても近いものでした。マルウェアのサンドボックス対策機能が追加されている NGFW もありますが、そのようなシステムは、ネットワーク周辺、内部ネットワーク、クラウドベースのワークロードにわたる包括的な脅威管理をカバーするものではなく、脅威対策を戦術的に統合するものとなる傾向があります。

- **クローズド アーキテクチャ。**これまでと同様、一部の NGFW には、独自のハードウェア アプライアンスに数々の機能を組み込んでいるものがあります。そのようなシステムでは、API を利用したり、ごく一部のセキュリティ ツールと連携することはできますが、DevOps プロセスやセルフサービスのオートメーション/オーケストレーション ツールを扱う現在のソフトウェア定義型 IT インフラストラクチャにおいては十分とは言えません。

- **管理の課題。**緩く連携したセキュリティ サービスに基づく NGFW には、緩く連携した管理システムが付属する傾向があります。そのような管理システムでは、構成管理、ポリシー管理、変更管理、およびレポート機能をサービス単位で扱っています。このため、セキュリティ運用が複雑になったりオーバーヘッドが生じたりする可能性があります。

次世代ファイアウォールの新モデル

前途有望だと謳われていた次世代ファイアウォールでしたが、これまでに説明した課題を残し、セキュリティ チームの現状は、NGFW の導入前と比べてごくわずかに改善された程度に留まっています。では何が必要なのでしょうか。ESG では、セキュリティ チームの要件を満たすため、企業組織が求める次世代ファイアウォール プラットフォームでは、次のことを可能にする必要があると考えています（表 1 参照）。

- **拡張性、パフォーマンス、柔軟性。**次世代ファイアウォールには、企業の統合ニーズを満たすために多数のネットワークおよびセキュリティ サービスを単一システム上で実行するだけの実力が必要です。それにはハイエンド プロセッサ、専用ハードウェア コンポーネント、および最新のマルチスレッド オペレーティング システムが適切に組み合わされている必要があります。さらに、必要に応じて複数のハードウェア アプライアンス、VM、およびクラウドベース環境の間でワークロードやセキュリティ サービスを調整できるような柔軟な設計も求められます。

- **統合。**NGFW は、ドキュメント化された API の提供、エコシステム パートナーによる技術との相互運用、および一般的な標準規格のサポートを通じて、各種のセキュリティ ツールと密に統合できる必要があります。この種の統合オプションが、従来の次世代ファイアウォール アプライアンスと真の拡張可能プラットフォームとの違いです。

- **エンドツーエンドの脅威管理。**次世代エンドポイント プラットフォームは、追加の基本的な保護手段というよりはむしろ、サンドボックス対策、脅威インテリジェンス、侵害のエンドポイント インジケータやネットワーク インジケータ、IDS/IPS アラートといった広範なサイバーセキュリティ機能と密に連携するものでなければなりません。それにより、ネットワークとエンドポイントにおける脅威の共有、データの質的向上、イベントの相関付け、自動修復の中枢として NGFW プラットフォームが位置付けられるようになります。

- **包括的な管理機能。**ファイアウォール管理は、防御、検出、応答において企業の要件に沿ったものである必要があります。このため、セキュリティ サービス間での直感的なエンドツーエンドのポリシー管理や一元的なレポート作成が要求されます。また、脅威や脆弱性、社内のガバナンス ニーズに関連したリアルタイムの変化に基づいて、ポリシーを自動化、変更、適用する能力も必要になります。

表 1. 次世代ファイアウォール プラットフォームの側面

要件	説明	根拠
拡張性、パフォーマンス、柔軟性	高性能なハードウェアおよびソフトウェア。セキュリティ サービスをアプライアンス間で実行したり、VM として導入したりできる機能。	企業は、アプリケーションおよびサービスを中断させることなくセキュリティ機能を統合するために、高いシステム パフォーマンスやスループットを必要としています。また、IT インフラストラクチャ、ソフトウェア定義ネットワーク、クラウド コンピューティングにおける変更に対応できるよう、セキュリティ サービスを分散できる必要もあります。
統合	ドキュメント化されたオープンな API、パートナー エコシステム、および標準規格の採用。	企業は、既存のツールを最大限に活かすと同時に、それに新しいツールを簡単に統合できる機能を必要としています。また、リスク管理やインシデント対応のワークフローにおいてセキュリティ機能をサービス チェーンとして相互運用できることも必要です。
エンドツーエンドの脅威管理	密に連携する脅威管理サービス。マルウェア サンドボックス対策、IDS/IPS、脅威インテリジェンス、エンドポイント フォレンジックやネットワーク フォレンジックなど。	企業は、脅威管理ツール間を密に調整して、攻撃面を減らし、進行中のサイバー攻撃を検出し、インシデント対応作業を加速する必要があります。

出典：Enterprise Strategy Group、2016

シスコの NGFW プラットフォーム

シスコにはネットワーク セキュリティ分野における長い歴史があり、ファイアウォール技術は幾度となく変化を遂げてきました。パケット フィルタリング、ステートフル インスペクション、ディープ パケット インスペクション（DPI）、そして次世代ファイアウォールです。シスコは今、新しい Firepower NGFW により大きく前進しています。Firepower NGFW は、シスコと Sourcefire による数多くのセキュリティ サービスを組み合わせることで、インシデントの防御、検出、対応すべてを行う共通プラットフォームを構築します。シスコの製品発表に含まれている具体的な内容は以下のとおりです。

- **Firepower NGFW の導入。**Cisco ASA ファイアウォール、Sourcefire 次世代 IPS、Advanced Malware Protection（AMP）、およびその他のシスコのセキュリティ アセットを真にソフトウェアレベルで統合しています。シスコは、このプラットフォームを「業界初の完全に統合された、脅威に重点を置いた次世代ファイアウォール」であるとし、優れた防御や管理を提供しながらセキュリティ運用を合理化できると考えています。

- **一連の新しいアプライアンス。**シスコは、低遅延/高スループット アプライアンス ファミリに、FirePower 4100 シリーズを導入しました。これは、ファイアウォール、次世代 IPS、URL フィルタリング、高度なマルウェア防御/検出の統合インスペクション エンジンを 1 RU 密度に最適化して設計されています。

- **Firepower Management Center 6.0。**新しい NGFW プラットフォームを補完するために、シスコは新しいセキュリティ管理システムも発表しています。このシステムを利用する IT 担当者や SOC チームは、きめ細かなポリシー管理、サービス チェーン化、セキュリティ分析を実現できます。シスコは、Firepower Management Center 6.0 によってセキュリティ運用を単純化しながら、サイバーセキュリティ チームがさらに強力で効率的なツールセットを使用できるようにしたいと考えています。

Firepower NGFW プラットフォームは、インターネット エッジ環境など特定のユース ケースをターゲットにしています。そのため、すべてのユース ケースに最適というわけではありません。たとえば、Firepower NGFW ソフトウェアは、VPN、クラスタリング、マルチテナント サポートなどの要素を初期リリースでは提供しない予定です。ただし、対象となる顧客に対してシスコは FirePOWER サービスとともに ASA ファイアウォール（新しいアプライアンス上でソフトウェアとして実行可能）などのその他のソフトウェアや製品を利用して引き続きサービスを提供します。このような既存システムを引き続きサポートしながら、シスコは Firepower NGFW に拡張機能を追加していく予定です。

シスコは、Firepower NGFW を導入することで、ファイアウォール アプライアンスから、最新の NGFW プラットフォームへと移行を進めています。このようなシフトは、リスクの低減、保護の向上、インシデント対応作業の加速、セキュリティ運用の合理化を求める企業 CISO にとって注目すべき点であると言えます。

結論

サイバーセキュリティの専門家は、ある種の「特効薬」となるソリューションを探し求めてきました。それは、ネットワークに迅速に導入でき、防御、検出、対応における大幅な改善を実現できるソリューションです。しかし残念ながら、そのような「特効薬」となるソリューションは存在しません。有能な CISO であれば、強力なサイバーセキュリティが正式なプロセス、適切なポリシー、一元的なコマンドや制御、分散化したポリシーの適用、そしてリアルタイムの包括的な可視性に依存していることを知っています。ファイアウォールの技術は、サイバーセキュリティ マシンにおいて不可欠な歯車として進化してきました。しかし、いまだ多数ある必要なパズル ピースのうちの 1 つにすぎません。

次世代ファイアウォール プラットフォームは、このような状況を考慮して設計されています。ファイアウォール機能を拡張して統合することにより、脅威の防御、検出、および修復を改善します。NGFW プラットフォームはその他のセキュリティ ツールと相互運用しており、これは古い格言「全体は部分の総和に勝る」に合致します。最後に、次世代ファイアウォール プラットフォームは、管理を念頭に置いて設計され、負担が多く、人員不足のサイバーセキュリティ チームの生産性を向上します。

シスコは、ネットワーク セキュリティの進化に積極的に関与してきました。シスコによる最近の発表は、彼らが積極的な関与を続けていくことのさらなる証拠と言えます。新しいプラットフォーム、新しい NGFW アプライアンス、そしてより一層包括的なセキュリティ管理ソリューションの導入は、シスコのネットワーク セキュリティの系図におけるまさに最新章なのです。