アプリケーションの可視化と管理を越えて：NGFW のあるべき姿

概要

現代のネットワークとその構成要素は絶えず進化しており、必要とされる保護を提供するには従来の次世代ファイアウォールでは不十分です。

このドキュメントでは、以下のトピックについて説明します。

- 一般的な次世代ファイアウォールは主にアプリケーションの可視化と制御を重視しているため、脅威防御の面では不十分
- リソースが限られた環境で高度な脅威に対抗するために必要となるもの
- 業界初のフル統合型、脅威重視型の次世代ファイアウォール（NGFW）、Cisco FirePOWER™ Next-Generation Firewall（NGFW）の利点

はじめに

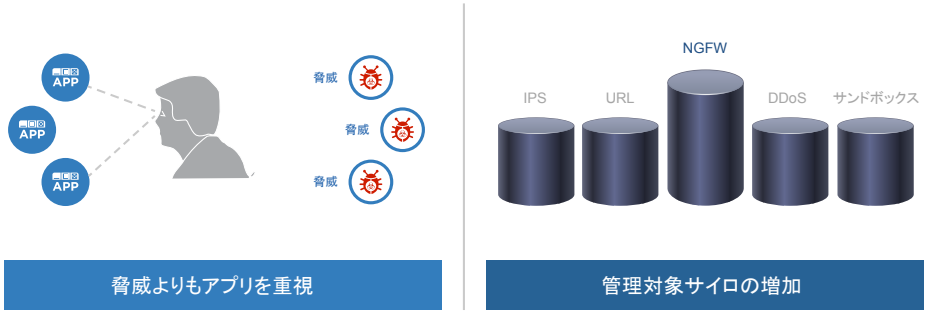
デジタル変革の規模は巨大であり、多くのビジネス チャンスを生み出しています。150 億を超えるデバイスが現在インターネットに接続されており、2030 年にはその数は 5,000 億に達すると予測されています。[1] また、今後 10 年間で、デジタル変革が世界中のビジネスで生み出す機会の価値はおよそ 19 兆ドルに及ぶと推定されています。[2] その一方で、この変革はサイバー犯罪者にとっても大きな機会を生み出すことが予想されます。サイバー犯罪の世界市場の規模は、およそ 4,500 億ドルから 1 兆ドルと推定されています。[3]

現代のネットワークとそのコンポーネントは常に進化しており、そのため攻撃可能な領域も拡大しています。攻撃者は金銭的な報酬を目当てに、ネットワークに侵入し、増え続けるデジタル資産を盗み出すため、さらに高度な方法を編み出しています。一旦ネットワークに侵入してしまった侵入者は、検出が困難です。実際に、高度な脅威の検出にはおよそ 100 日かかっています（業界中央値）。[4]

今日のネットワーク セキュリティの課題

セキュリティは、デジタル経済や新たなビジネス モデルが生み出すビジネス チャンスをつかむための基礎となるものです。次世代ファイアウォール（NGFW）の登場は重要な一歩ではありました。しかし、一般的な NGFW ではアプリケーションへのアクセス制御を重視するあまり、脅威防御機能がおろそかになっていました。このような不完全なアプローチでは、巧妙な攻撃者や高度なマルウェアが及ぼすリスクから十分に保護することはできません。その上、こうした NGFW の場合、感染後の対応は限定されます。感染対象を把握して封じ込め、迅速に修復することができないからです。

従来の NGFW は、視野が狭く、管理も困難です。



組織には製品を追加するためのリソースもなければ、このような断片的なアプローチから生じる複雑性を管理できるセキュリティ人員もいません。実際、セキュリティ向上の障壁として最もよく挙げられるのが、限られたリソースです。[5] さらに、こうした連携のないセキュリティ サービスは運用する上でも柔軟性に欠き、ビジネス成長の妨げとなります。

1. シスコの Internet of Things：http://www.cisco.com/web/solutions/trends/iot/indepth.html [英語]
2. http://ioeassessment.cisco.com/learn [英語]
3. RSA/CNBC：http://www.cisco.com/web/offer/emear/38586/images/Presentations/P16.pdf [英語]
4. 2016 年シスコ年次セキュリティ レポート
5. 2016 年シスコ年次セキュリティ レポート

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

アプリケーションの可視化と管理を越えて：NGFW のあるべき姿

NGFW のあるべき姿

NGFW プラットフォームはより大きな役割を果たす必要があります。求められているのは、以下を実現できる次世代ファイアウォールです。

- 脅威への対応に重点を置き、攻撃前、攻撃中、攻撃後といった一連の攻撃のすべての段階にわたって脅威からの保護を提供
- すべてのセキュリティ サービスおよびイベント情報を単一のビューと管理プラットフォームにフル統合
- 既存のセキュリティ投資と連携し相乗効果を発揮

こうした条件を満たす次世代ファイアウォールは、的確なアプリケーション制御という価値のみならず、高度な回避型マルウェア攻撃による脅威に対する、現実に即したセキュリティ効果も提供します。組織は業務を合理化し、ネットワークを有効に活用できるようになります。

Cisco FirePOWER NGFW のご紹介

Cisco FirePOWER Next-Generation Firewall（NGFW）は、業界初のフル統合型、脅威重視型の次世代ファイアウォール（NGFW）です。従来の NGFW を越えて、一連の攻撃全体に対する総合的な保護を提供します。

Cisco FirePOWER NGFW では、アプリケーションの制御にとどまらない、はるかに優れたセキュリティ プラットフォームが利用できます。マルチベクター情報を照合することで回避動作や疑わしい挙動を速やかに検出し、侵害の兆候を示すホストをすばやく特定できます。また、より多くの脅威の阻止、ネットワークの可視性の向上、ゼロデイ脅威や標的型脅威の速やかな緩和が可能です。さらに、重要なタスクを自動化することで、組織が業務に集中し、既存のリソースを最大限に活用できるようになります。

保護機能を完備

Cisco FirePOWER NGFW は、世界で最も広く導入されているステートフル ファイアウォール技術を搭載しています。また次世代 IPS や高度なマルウェア保護、アプリケーションの可視化と制御、レピュテーションベース URL フィルタリングも提供します。これらの機能はすべて、1 つのアプライアンスで提供され、多機能かつ統合的な管理コンソールで管理されます。

Cisco FirePOWER NGFW：一連の攻撃全体に対する防御を完備

より多くの脅威を阻止

既知および新出の脅威に、業界で最も効果的な脅威保護で対抗しましょう。シスコの NGFW は統合的なサンドボックス ソリューションと、ファイルの普及率や性質を調査する機能を備えることで、回避型、標的型脅威を特定し、害を及ぼす前に阻止することができます。

© 2016 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

より多くの情報を把握

常に変化し続けるネットワーク内に存在するユーザ、ホスト、アプリケーション、モバイル デバイス、仮想環境、脅威、そして脆弱性について把握しましょう。こうした情報はネットワークの保護に役立ちます。NGFW は脅威とネットワークの脆弱性を自動的に照合できるため、セキュリティ チームは脅威に優先順位をつけ、順位の高いものに注力できます。

すばやい検出と対応

高度な脅威をすばやく緩和することにより、数ヵ月かかっていた検出および修復までの時間を、数時間まで短縮できます。シスコの場合、その時間は 17.5 時間です。[6] マルウェアの感染範囲やファイルへのパスと挙動を瞬時に把握し、シグネチャが入手可能となる前に封じ込めを行います。

複雑さを緩和し、運用を簡素化

すべてのセキュリティ機能を、単一の管理インターフェイスを持つ 1 つの高性能プラットフォームに統合できます。Cisco FirePOWER Management Center はポリシーを統一、一元化し、シンプルにすることで、多層的な防御セキュリティ アーキテクチャの管理に要する負荷を軽減します。ネットワークの脆弱性を自動的に分析して保護を推奨することで、変化が激しく人員も不足しがちな今日の環境にふさわしい保護を提供します。

ネットワークを有効に活用

Cisco FirePOWER NGFW は、Cisco Identity Services Engine（ISE）など、シスコ® の他のセキュリティ ソリューションと連携することで、識別データの共有やネットワークのセグメント化を実現し、OpenDNS でインターネット中のドメインを可視化します。インテリジェンス、コンテキスト、ポリシー制御が共有されるため、このアプローチは効果的で俊敏なものとなります。また、管理も簡単になり、管理コストの削減も図れます。ネットワークのセグメント化を自動化することで、脅威を迅速に封じ込めることができます。Cisco Talos が提供する DNS や脅威に関するグローバルなインテリジェンスにより、レピュテーションに基づいた脅威指標が得られます。これによって早期に警告が発せられるため、ネットワーク セキュリティ デバイスは攻撃が起こる前に防御の準備が可能です。

Cisco FirePOWER NGFW はお客様のセキュリティを高め、高度な脅威を迅速に軽減し、業務を合理化します。セキュリティを成長の原動力とし、ぜひ新しいビジネス チャンスをつかみ取ってください。

詳細

Cisco FirePOWER Next-Generation Firewall の詳細については、www.cisco.com/go/ngfw [英語] を参照してください。

6.2016 年シスコ年次セキュリティ レポート

シスコ、およびシスコ ロゴは、シスコまたはその関連会社の米国およびその他の国における登録商標または商標です。シスコの商標の一覧については、www.cisco.com/go/trademarks をご覧ください。掲載されている第三者の商標はそれぞれの権利者の財産です。「パートナー」または「partner」という用語の使用は、シスコと他社との間のパートナーシップ関係を意味するものではありません。(1110R)

C11-736644-00 02/16