SOLUTION BRIEF

ランサムウェア攻撃や ボリューム型 DDoS 攻撃から ハイパースケールデータセンターを保護

概要

企業ではハイブリッド IT、IIoT（産業用 IoT）、5G が導入され、運用のアジリティが向上しています。これらのツールを用いて、展開や拡張が可能なアーキテクチャを構築することで、分散している拠点、キャンパス、オンプレミスのデータセンター、マルチクラウドを一体型のネットワークに相互接続することができるようになります。こうした変化の中でも、企業のオンプレミスデータセンターが、ほとんどのネットワークで重要な要素の 1 つであることは変わりません。従業員、顧客、パートナーが利用する、クラウドには移行できないようなアプリケーション、データ、ワークロードを保護するという面で、データセンターの役割は非常に重要となります。

しかし、データセンターのインフラストラクチャも分散化が進み、攻撃対象領域が大幅に拡大しています。分散した環境でシームレスに対応できる包括的なセキュリティ戦略がなければ、盲点が発生します。ネットワークのさまざまな箇所に展開されるポイントセキュリティ製品では可視性が低下し、侵害や攻撃の可能性が高まるといったセキュリティの欠陥が生じてしまいます。セキュリティが統一されていないため、攻撃対象の全体像を把握するのが困難になり、ランサムウェアや分散型サービス拒否（DDoS）など、ますます高度化する攻撃を効果的に阻止したり抑止したりすることができなくなります。

さらに状況を複雑にしているのが、ほとんどのデータセンターのセキュリティポリシーが、垂直方向のデータフローに重点を置いていることであり、エッジに不可欠なレイヤー 4 の保護を適用し、境界を完全に保護することを目指しています。しかし、特に分散型のデータセンター環境では、ほとんどのデータセントラフィックがセンター内で水平方向に流れています。つまり、脅威攻撃者が高度なランサムウェアやボリューム型 DDoS 攻撃（実際には、これらの攻撃が組み合わさっている傾向があります）を実行してセキュリティ基盤が圧迫されることがあれば、境界中心のセキュリティ対策は役に立たなくなるのです。

フォーティネットの先進的なイノベーションが昨今のハイブリッド環境を大規模に保護

フォーティネットのソリューションでは、20 年以上にわたるイノベーションを活用して、一貫したエンタープライズクラスの保護と最適なユーザーエクスペリエンスがすべてのネットワークエッジで提供されるようになっています。また、SD ブランチや SASE（セキュアアクセスサービスエッジ）といったフォーティネットのソリューションでは、ネットワーキングやセキュリティを集約して、保護や可視性を有効化し、複雑なハイブリッド環境での相互運用や拡張を実現します。

こうしたイノベーションにより、フォーティネットは、2022 年 Gartner® 社のネットワーク・ファイアウォールについてのクリティカル・ケイパビリティのエンタープライズデータセンターのユースケース [1] で 3 回連続で最も高いスコアと評価されました。またフォーティネットはネットワーク・ファイアウォールについての Magic Quadrant™ [2] でも 5 年連続でリーダーの 1 社に位置づけられています。

最新のネットワークプロセッサである NP7 では、アプリケーションやホステッドサービスのエッジを保護しながらビジネスを拡張し、高まるユーザーの要求に対応できるようにしており、最大 1.9 Tbps という驚異的なファイアウォールパフォーマンスを実現します。また、ハードウェアアクセラレーションによる DDoS 防御機能も搭載されているため、ボリューム型攻撃も防止できます。これらはすべて単一の FortiGate プラットフォームに搭載され、単一のコンソールによる管理で優れた操作性を実現しています。

次のように、NP7 は他に例を見ない独自の機能を備えています。

- 革新的なファストパスアクセラレーションを使用して、CPU からユーザー接続をオフロードすることで超高速スピードを実現しています。FortiGate NGFW は、1 秒あたり最大 1,000 万回の接続を可能にし、ネットワークパフォーマンスの向上をもたらします。
- NP7 は、アノマリベースでの侵入防止、チェックサムオフロード、パケットのデフラグも提供します。このマルチレイヤー保護では、まずパケットレベルでアノマリチェックを行い、各パケットが侵害されていないことを確認します。次に、インタフェースベースでのアノマリ防御、DDoS 防御、ポリシーベースでの侵入防御、ファイアウォールのファストパス、ビヘイビア（振る舞い）ベースでのメソッドといった高機能セットにより、DDoS 攻撃がシステムの他の部分に拡散するのを防ぎます。
- NP7 のハードウェアにも DDoS 防御機能が組み込まれているため、DDoS 攻撃の場合でも事業継続性とサービスの可用性を確保しています。DDoS 防御のハードウェアアクセラレーションポリシーでは、IPv4 / IPv6、インタフェース、アクセス制御リスト（ACL）ポリシーの処理が CPU からオフロードされるため、効率やパフォーマンスが向上し、非常に効果的に NP7 でのボリューム型攻撃を検知し、防止します。

- NP7 は、高パフォーマンスのデータセンター相互接続（DCI）のセキュリティを確保し、ディザスタリカバリ（DR）サイトやレプリケーションを構築するためにも使用できます。NP7 は、セッションおよびインターネットプロトコルセキュリティ（IPsec）のセキュリティアソシエーションキーを保存し、必要な暗号化 / 復号化を実行し、すべてのセッションを高速化します。コンパクトなフォームファクターにおいて、最大 310 Gbps の IPsec スループット（Suite B 規格）を実現します。

エッジを超えたセキュリティ

現在の NGFW では、動的な内部セグメンテーションファイアウォール（ISFW）機能を搭載した、動的なセキュアセグメンテーションのサポートも求められます。ISFW は脅威が水平方向に広がるのを防ぎ、完全統合型のソリューションが有する幅広い多層防御のポートフォリオと統合され、強力なコンプライアンスやアプリケーションアクセスコントロールを確立し、悪意のあるアクティビティをルートアウトして終了します。

しかし、昨今のネットワークは非常に動的でもあり、変動的な帯域幅やアプリケーションの要件にも対応しています。このような環境で求められる拡張性のあるセグメンテーションは、NP7 搭載の FortiGate プラットフォームが、不可欠となるレイヤー 4 ファイアウォールルールに統合されている VXLAN（Virtual Extensible LAN）のターミネーションや再発信をサポートするからこそ可能になります。これにより、企業は従来の物理データベースのドメインを仮想アプリケーションや Web サーバーのドメインに接続したハイブリッド IT アーキテクチャを構築でき、アジリティやオンデマンドの拡張性が実現します。

完全な脅威保護

必須とされる最善のセキュリティ機能をすべて単一の FortiGate NGFW 内に統合することで、完全な脅威保護が実現します。NP7 搭載の FortiGate ソリューションは、最大 500 Gbps を超えるスループットを実現し、組織が最適な総所有コスト（TCO）を実現できるようにサポートします。

データセンター向けに設計されている FortiGate NGFW は、FortiGate 製品ポートフォリオにおける業界トップのパフォーマンスを、FortiGuard Labs の FortiGuard セキュリティサービスが提供する組織的で実用的な脅威インテリジェンスと統合することで、次のようなメリットを提供します：

- フォーティネット NGFW は、業界唯一の SPU 採用により、シームレスなユーザーエクスペリエンスを実現
- ハイパースケーラビリティと超高速パフォーマンスにより、顧客の膨大なトラフィック負荷に対応
- ハードウェアによる IPv4 または IPv6 DDoS 計測制御により、データセンターのエッジでホストされるアプリケーションやインフラストラクチャを保護し、ボリュームベースのフラッディング攻撃を防止
- 厳重な制御を適用し、物理ネットワークインタフェースと内蔵のホスト保護エンジンの両方でアクセス制御リストを実行し、さまざまなパケットタイプにおける 1 秒あたりのパケット数を制限し、NGFW の堅牢性や復元性が向上するようにサポート
- ハイブリッド IT アーキテクチャのネットワーキングにセキュリティを組み込むハイパースケールのセキュリティ ドリブン ネットワーキングを構築することで、いつでもどこでもあらゆるワークロードを保護
- 業界をリードする複数の FortiGuard サービスを単一のプラットフォーム上で実行することで、ポイント製品を統合または排除して最適な TCO を実現
- 実用的で調整され、かつ完全に自動化された脅威保護により、攻撃対象領域全体にセキュリティを拡張
- 400 社以上のエコシステムパートナーをサポートするなど、分散型セキュリティ ファブリック全体で対応可能な使いやすい一元管理システムにより、運用の簡素化、ワークフローの自動化、時間の節約を実現

昨今の俊敏なネットワークやハイブリッドデータセンターの環境により、今日のデジタル市場では組織が効果的に競争できるようになっています。しかし、そのためには、動的な変化を捉え、拡張し、適応し、ランサムウェアや DDoS 攻撃などの高度な脅威を防御するように設計されたセキュリティソリューションが必要になります。フォーティネットの FortiGate ソリューションは統合型のプラットフォーム上に構築され、さらに業界唯一のカスタムセキュリティプロセッサを搭載しているため、環境に必要なセキュリティを損なうことなく、必要なネットワークを構築することができます。

[1]「フォーティネットブログ：フォーティネット、2022 年ガートナー社「ネットワークファイアウォールについてのクリティカル・ケイパビリティ」レポートの 3 つのユースケースで最も高いスコアに」、フォーティネット、2022 年 2 月 18 日：https://www.fortinet.com/jp/blog/business-and-technology/fortinet-2022-gartner-critical-capabilities-for-network-firewalls-report

[2]「フォーティネット、2021 年のガートナー社ネットワークファイアウォールについてのマジック・クアドラントでリーダーの 1 社に位置づけられる」、フォーティネット、2021 年 11 月：https://www.fortinet.com/jp/solutions/gartner-network-firewalls

フォーティネットジャパン合同会社

〒106-0032
東京都港区六本木 7-7-7　Tri-Seven Roppongi 9 階
www.fortinet.com/jp/contact

お問い合わせ

SB-Protecting-Hyperscale-Datacenters-202204-R1