SOLUTION BRIEF

FortiGate NGFW を活用したプロアクティブで革新的なデータセンターセキュリティでビジネスの継続性を実現

概要

今日のビジネスでは、データセンターの圧倒的な可用性と耐障害性が求められます。しかし、攻撃対象領域は急速に拡大しており、脅威が巧妙化し進化しているため、それは決して容易なことではありません。FortiGate 次世代ファイアウォール（NGFW）を利用すれば、暗号化 / 非暗号化両方のトラフィックをすべて検査すると共に、99.999% の高可用性と優れた MTBF（平均故障間隔）を実現することができます。FortiGate NGFW は、単機能セキュリティ製品の点在が原因で複雑化しているセキュリティプロセスを簡素化します。また、動的なオブジェクトを使用してあらゆるセグメンテーションに対応することで L7 の高度なセキュリティを提供すると同時に、一元的な可視化と集中制御を実現します。

FortiGate NGFW

- 第三者機関に認められた最高レベルのセキュリティ効果
- 暗号化トラフィックのインスペクションと脅威保護に関する最適な価格性能比
- 最小限の TCO で最大限のビジネス価値を実現
- オープン API によるサードパーティ製オーケストレーション / オートメーションシステムとの統合
- 99.999% の高信頼性とキャリアグレードの OS（全モデル共通）

データセンターの進化に合わせたセキュリティ強化が必要

デジタルトランスフォーメーション（DX）は、データセンターを防御型のオンプレミスインフラストラクチャから、仮想、オンプレミス、クラウドの各要素を組み合わせた分散型のハイブリッド IT 環境へと進化させました。それらの新しい分散型データセンターでは優れたアジリティと新しい機能が提供され、ビジネスユーザーとパブリックユーザーが同様にアプリケーションを利用します（たとえば、医療分野では、スタッフと患者の両方がサービスにアクセスする必要があります）。

しかし、機能の拡張に伴ってサイバー攻撃のリスクも増加します。クラウド対応の分散型データセンターを古いセキュリティツール（元来はオンプレミス環境専用に設計されているもの）と組み合わせると、ネットワークの攻撃対象領域が拡大し、アプリケーションや基幹インフラストラクチャが機能停止状態になる可能性が高くなります。その結果、ビジネスへの甚大な損害が発生することが考えられます。IDC によると、平均的なインフラストラクチャ障害の場合、時間あたりの損害額は 10 万ドル、基幹アプリケーションの障害では 50 ～ 100 万ドルに上るとされています [1]。

セキュリティ侵害が増加していることから、1 社あたりのサイバー犯罪の損害額は 2018 年には 1,300 万ドル（2017 年から 12% 増）に達しています [2]。

統合セキュリティエコシステムの導入

継続的に確実な事業運用を実行するため、ネットワークエンジニアリングとネットワークオペレーションのリーダーは、まず第一に基幹ビジネスアプリケーションとサービスをその実行場所に関係なく保護することによって、リスクを効果的に管理する必要があります。分散型のハイブリッド IT インフラストラクチャにおいて、望ましくないネットワークセキュリティの条件に耐える、拡張性と耐障害性を備えたネットワークセキュリティアーキテクチャを構築しなければなりません。

さらには、設備投資（CapEx）と運用コスト（OpEx）の両方を減らすために業務を合理化するアーキテクチャ戦略を選択し、攻撃対象領域として拡散している単機能セキュリティ製品への依存状態から脱却する必要があります。実際に、全体の 4 分の 3 以上となる 77% の組織が、非統合型の単機能セキュリティソリューションにある程度依存する状況にあります。そのような状況では、サイバー攻撃に対してネットワークが脆弱な状態が続くだけでなく、コストと複雑性も増加します [3]。この対応策となるセキュリティの統合では、業務の簡素化とワークフローのオートメーションが実現します。これにより、より重要なビジネスにセキュリティの技術リソースを注力させて、成果の達成とオペレーションの最適化が可能になります。

効果的なデータセンターセグメンテーションの実現

リスクを管理するには、攻撃対象領域を減らす必要があります。これは、ネットワークセグメンテーションによってある程度実現することができます。ネットワークセグメンテーションは、ワークロードを個別に分割しながら、ネットワークへの不正侵入のラテラルムーブメント（水平移動）を抑制します。分散型データセンターのセグメンテーションでは、多様なユースケースに対応する十分な柔軟性が要求されます。そのようなソリューションは、ビジネスの継続性を維持するためのハイブリッド IT アーキテクチャ全体にわたる拡張性、耐障害性、可用性を備えている必要があります。

しかしながら、セグメンテーション自体にはコンテンツを検査して脅威を見つけ出すためのメカニズムはありません。したがって、脅威インテリジェンスの共有と脅威保護の自動化を実現するために、さまざまなセグメンテーション方式を採用することができ、サードパーティのセキュリティソリューションとの連携が可能な NGFW ソリューションが必要になります。

拡大するリスクに対するプロアクティブなセキュリティ機能

FortiGate NGFW は、フォーティネット セキュリティ ファブリックの構成要素であり、進化するデータセンターにおける前述のセキュリティ要件に対応します。特に、FortiGate NGFW には FortiGuard Labs による統合脅威インテリジェンスが提供されており、既知の攻撃だけでなく、人工知能（AI）を活用する FortiSandbox によって未知の攻撃も検知することができます。この総合的な脅威インテリジェンスは、セキュリティインフラストラクチャのすべての部分でリアルタイムに共有されるので、リスク状況の改善に役立ちます。

FortiGate NGFW のコア機能は、ネットワークエンジニアリングとネットワークオペレーションのリーダー向けに、様々な理由で理想的となる以下の選択肢を提供します。

リスク管理

FortiGate NGFW は、複数ベンダーのインフラストラクチャにおいて、サードパーティのテクノロジーやプラットフォームと緊密に統合されるように設計されています。ファブリックコネクタ、およびファブリック・レディ パートナーが提供する互換性により、双方向通信および脅威インテリジェンスの共有を可能にします。FortiGate NGFW は、あらゆるセグメンテーション戦略に適応し（動的オブジェクトを使用してネットワークの変化に対応）、信頼性に優れた L7 の高度なセキュリティを提供します。実際に、FortiGate NGFW は第三者機関によるテストで業界トップクラスのセキュリティ効果を提供することが実証されています [4]。

FortiGate NGFW は、NSS Labs が毎年実施している NGFW 業界テストにおいて、5 年連続で「推奨」評価を獲得しています [5]。

耐障害性および拡張性

データセンターでは、最大限の可用性と耐障害性が要求されます。FortiGate NGFW は、キャリアグレードのハードウェアとソフトウェアを備えているだけでなく、N+1 の冗長クラスタリング（コンポーネント障害の発生に備えたシステムバックアップ用）を適用することによって、99.999% の可用性と優れた MTBF を実現します。

また、ネットワークセキュリティにおいては、暗号化 / 非暗号化両方のトラフィックすべてを保護する拡張性も重要です。今日では、ネットワークトラフィックの 72% は SSL（Secure Sockets Layer）/ TLS（Transport Layer Security）によって暗号化されているため、暗号化トラフィックのインスペクション機能が必要とされています [6]。SSL / TLS 暗号を使用してネットワークへの侵入とデータ流出を実行するサイバー攻撃が 50% 以上にのぼることから、SSL / TLS インスペクションは不可欠な機能となっています [7]。しかしながら、多くの NGFW では SSL / TLS インスペクションを有効にするとパフォーマンスが著しく低下し、CapEx と OpEx の大幅な増加を招きます。

FortiGate NGFW は、非暗号化 / 暗号化（TLS バージョン 1.3 を含む）両方のワークフローに対する高性能のインスペクションを実行します。特に、SSL インスペクションの価格性能比は業界トップクラスで、SSL / TLS インスペクションが有効な場合でも、保護された Mbps（メガビット / 秒）あたりの TCO（総所有コスト）は最高レベルを達成しています [8]。

オートメーションおよびオーケストレーション

FortiGate NGFW は、フォーティネット セキュリティ ファブリック アーキテクチャの根幹として、単機能製品の統合を通じてビジネス価値を最大化します。既存のセキュリティソリューションはオープン API によって FortiGate NGFW と統合され、ワークフローのオートメーション、オーケストレーション、およびパッチが適用されていないアプリケーションや絶えず変化する DevOps 環境を保護するセキュリティの同期を可能にします。この包括的な統合は、一元的な監視と管理による脅威検知を可能にする、最新および過去のログに対する IOC（Indicators of Compromise：侵害指標）の可視化によって、さらに機能強化されます。

また FortiGate NGFW は、コンプライアンスレポート、監査、オーケストレーションの自動化が可能で、NIST（米国国立標準技術研究所）や CIS（Center for Internet Security）などのセキュリティ標準へのコンプライアンスを実現します。さらに、厳格化の進む新たな法律や業界の規制に対して、ネットワークエンジニアリングおよびネットワークオペレーションの部門が対応できるようにします。また、360 Protection および Enterprise Protection の両バンドルに含まれているフォーティネットのセキュリティレーティングサービス [9] を利用することで、ネットワークエンジニアリングおよびネットワークオペレーションのリーダーは、セキュリティ態勢をプロアクティブに管理して経時的に改善すると同時に、問題の発生前にリスクを検知できるようになります。

拡大する攻撃対象領域を保護する

ハイブリッド IT 環境においてデータセンターの分散化が進むに伴い、ネットワークエンジニアリングおよびネットワークオペレーションのリーダーに対して、ビジネスの継続に不可欠な可用性の確保が要求されています。まず、脅威インテリジェンスの共有、高度なセグメンテーション、アクセス制御などを実現する、統合型のセキュリティアーキテクチャを採用する必要があります。次に、トラフィックの需要増加に対応する拡張性と共に、リスクを管理可能な耐障害性を備えたセキュリティが不可欠です。そして最後に、コストを削減するセキュリティワークフローのオートメーションとオーケストレーションの展開が求められます。

FortiGate NGFW は、これら 3 つの要件をすべて満たし、あらゆるセキュリティアプローチの基盤、つまりデータセンターにおける形態と性質の変化に対応可能な統合セキュリティソリューションを提供します。その結果、セキュリティ運用の簡素化と TCO の削減を両立させると共に、業界トップレベルの確実な保護を実現します。

[1]「Is Your Disaster Recovery Plan Up to Date?」、CIO、Kevin O’ Connor 著、2016 年 4 月 18 日（英語）：https://www.cio.com/article/3058074/is-your-disaster-recovery-plan-up-to-date.html
[2]「Ninth Annual Cost of Cybercrime Study」、Accenture および Ponemon Institute、2019 年 3 月 6 日（英語）：https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf
[3]「The CIO and Cybersecurity: A Report on Current Priorities and Challenges」、フォーティネット、2019年5月23日(英語)：https://www.fortinet.com/content/dam/maindam/PUBLIC/02_MARKETING/08_Report/report-ciso-and-cybersecurity.pdf
[4]「認定」、フォーティネット、2019 年 7 月 12 日時点の情報：https://www.fortinet.com/jp/corporate/about-us/product-certifications.html
[5] 同上
[6]「フォーティネット脅威レポート 2018 年第 3 四半期版」、フォーティネット、2018 年 11 月：https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/ja_jp/TR-18Q3.pdf
[7]「Study Reveals Hackers Increasingly Use Encryption to Hide Criminal Activity.」、Lifeline Data Centers、2019 年 3 月 21 日時点の情報（英語）：https://lifelinedatacenters.com/data-center/hackers-use-encryption/
[8]「フォーティネット、NSS Labs の最新 NGFW レポートで「Recommended（推奨）」評価を獲得 ...」、フォーティネット、2018 年 7 月 25 日：https://www.fortinet.com/jp/corporate/about-us/newsroom/press-releases/2018/nss-labs-ngfw-report.html
[9]「Proactive, Actionable Risk Management with the Fortinet Security Rating Service」、フォーティネット、2019年2月14日(英語)：https://www.fortinet.com/content/dam/fortinet/assets/white-papers/wp-security-rating-service.pdf

フォーティネットジャパン株式会社

〒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-FortiGate-Series-SS-202001-R1