FORTINET

ハイブリッドデータセンターで求められる新たな NGFW 機能

概要

最新のデータセンターの進化に伴い、アプリケーションとデータは、ハイブリッドインフラストラクチャ全体に分散しつつあります。その結果、ビジネスクリティカルなワークフローの俊敏性は向上しましたが、攻撃対象領域は拡大し、可視性とコントロールが損なわれています。ネットワークエンジニアリングとオペレーションの責任者がこのような状況に対応するには、ハイブリッド IT データセンター環境を保護できる高度な機能を備えた統合型セキュリティが必要です。

特に必要とされるのが、次世代ファイアウォール（NGFW）です。NGFW には、重要度の高いリスク管理機能、データセンター保護を組織全体に適用する拡張性、ビジネスを確実に継続する耐障害性、スタッフの負荷軽減と応答時間の短縮に役立つオートメーションとオーケストレーション機能が組み込まれています。

過去 2 年間で発生したダウンタイムの平均コスト（信用の失墜や風評被害を含む）は、企業 1 社あたり 6,720 万ドルにのぼります [1]。

データセンターの分散で拡大する攻撃対象領域

ビジネスユーザーは、ハイブリッド IT インフラストラクチャ全体に分散するデータセンターから、重要なアプリケーションにアクセスしています。オンプレミス、コロケーション、プライベートクラウドとパブリッククラウドにワークフローとデータが存在し、脆弱なコンテンツが広く分散しているため、攻撃対象領域は拡大し続けています。

高まるリスクを軽減しようと、多くのネットワークエンジニアリングとオペレーションの責任者がポイントセキュリティソリューションを次々と追加し、防御ギャップの解消や変化を続ける法規制コンプライアンスへの対応を試みてきました。ところが、このような断片的アプローチでは、現在直面している脆弱性はもちろん、今後登場する脆弱性に対抗することはできません。サイバー攻撃や自然災害でビジネスが中断する確率は高まっているだけでなく、セキュリティの総所有コスト（TCO）は増大し、複雑化しています。

ハイブリッドな IT 環境のセキュリティ保護

拡大するデータセンター攻撃対象領域に対処するには、まず、ハイブリッド IT 環境のあらゆる側面のセキュリティを統合しなければなりません。また、エンドツーエンドの可視性、ポリシー制御、侵入防止（IPS）、さらに次のような機能を備えた NGFW セキュリティも必要です。

- **パフォーマンス：**リスク管理には、高性能ネットワークに対応でき、攻撃対象領域を効果的に縮小する堅牢な機能を持つセキュリティソリューションが必要です。

ハイブリッドデータワークロードに関する懸案事項は、上位から、データセキュリティ / 法規制へのコンプライアンス（71%）、パフォーマンス（62%）、管理の容易さ（53%）となっています [2]。

- **耐障害性および拡張性：**拡張と多様化を続けるハイブリッド IT 環境に対応するには、拡張性、耐障害性、可用性を備えたデータセンターセキュリティにより、ビジネス継続性を確保しなければなりません。また、ネットワークおよびセキュリティアーキテクチャ全体に、ネットワーク障害や自然災害による中断に耐えられる機能も求められます。
- **オートメーションおよびオーケストレーション：**統合型セキュリティアーキテクチャは、インテリジェントなオートメーションの威力をハイブリッド IT インフラストラクチャ全体で発揮します。セキュリティレスポンスの自動化と管理の迅速化は、リスク軽減だけでなく、スタッフの作業負担、人為的なミス、運用コスト（OpEx）の軽減にも役立ちます。

リスク管理のパフォーマンス

一般的に、データセンターのファイアウォールは、ネットワークが最速となる場所に設置されます。したがって、このユースケースで NGFW ソリューションが効果を発揮するには、ネットワークパフォーマンスへの影響を最小限に抑えることができる高度な L7 セキュリティを使用しなければなりません。ネットワークボトルネックを発生させず、セキュリティ機能を安定した高パフォーマンスで実行するには、専用のセキュリティプロセッサが必要です。また、最新の分散型データセンターでは、さまざまな環境（オンプレミス、コロケーション、クラウドなど）に導入されているセキュリティ要素に加えて、ユーザー、アプリケーション、デバイスすべてを可視化する機能も要求されます。

現在発生しているセキュリティ侵害の 3 分の 1 以上が、信頼できる内部ソースに起因していることを考えれば [3]、内部ネットワークのアクセス制御は不可欠です。この課題の解決策としては、さまざまなユースケース（ユーザー、デバイス、アプリケーションの動的な信頼検証を含む）に対応できる拡張性と柔軟性を備えたネットワークセグメンテーションがあります。

現在、77% の組織が、非統合型のポイントセキュリティソリューションに、ある程度依存している状況にあります [4]。

ただし、スタンドアロンのセグメンテーションだけでは、コンテンツインスペクションといった高度な脅威に対抗できる重要度の高いセキュリティ機能の多くを提供できません。したがって、データセンター向けの NGFW は、さまざまなセグメンテーション手法、サードパーティセキュリティソリューションとの通信による脅威インテリジェンスの共有、コンテンツインスペクションと脅威保護の自動化に対応していなければなりません。

今日大量に発生している脅威とその速度に対抗するには、統合型セキュリティアーキテクチャ全体で、インテリジェンスをリアルタイムで共有する必要があります。また、未知の脅威を特定するには、人工知能（AI）も必要です。そして、AI による脅威の検知と防止を、あらゆる場所にあるデジタル資産に適用することが最も重要です。

耐障害性および拡張性

拡大を続けるデジタルイノベーションは、セキュリティに直接的な影響を与えます。データセンターワークロードがハイブリッド IT 環境全体に分散しつつある今、オンプレミスにある従来のアプリケーションの枠を超え、新たなアプリケーションとワークロードがクラウドや仮想マシン（VM）へと次々に拡大する状況に対応するには、柔軟な拡張性を備えたセキュリティが必要です。また、増加の一途をたどるトラフィックの処理も必須であり、非暗号化データフローと暗号化データフローの両方に対応しなければなりません。

現在、暗号化トラフィックは全体の 72% 以上を占めており、前年比で 20% 近く増加しました[5]。増加する暗号化トラフィックへの対策としては、HTTP および HTTPS トラフィックインスペクションツールによる高度な可視化が必要です。分散型データセンターは、暗号化されたデータフローを悪用して密かに移動する脅威に対して特に脆弱です。このリスクを軽減するには、SSL（Secure Sockets Layer）/ TLS（Transport Layer Security）の高度な暗号化トラフィックインスペクション（さらに、サンドボックスとデコイ / ハニーポットの統合）を活用し、アプリケーションパフォーマンスを低下させることなく、ユーザー / システム間や複数のシステム間を移動する大量のトラフィックを検査する必要があります。これには、最新の TLS 1.3 インスペクション機能が必要です[6]。

耐障害性と可用性という点では、コンポーネントの障害時にリアルタイムでフェイルオーバーできる機能が必須です。内蔵型の N+1 クラスタリングは、あらゆる単一障害点を排除できる完全に冗長なアーキテクチャを特徴とします。また、独立系業界エキスパートが提供するサードパーティ検証テストも、実環境においてソリューションの信頼性を高める上で役立ちます。

オートメーションとオーケストレーション

サイバーセキュリティスキルを持った人材は恒常的に不足しており、多くのセキュリティ組織は重い作業負担に悩んでいます。運用コストの抑制とセキュリティ技術リソースの解放によってビジネス成果に注力し、手作業をなくして最適化を実現するためには、運用上の複雑さの軽減が鍵となります。

これを実現するには、ワークフローの最適化など、導入と管理を合理化する機能を備えたデータセンターファイアウォールが効果的です。統合型セキュリティアーキテクチャは、インテリジェンスを共有し、レスポンスを自動化する基盤となり、ハイブリッドインフラストラクチャ全体でセキュリティを調整する役割を果たします。オープンなアプリケーションプログラミングインタフェース（API）をサポートする NGFW ソリューションは、パッチ未適用のアプリケーションや変化を続ける DevOps 環境において、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、セキュリティレスポンスの同期など、極めて重要な優位性を発揮します。

また、このようなソリューションがあれば、ユーザー、デバイス、アプリケーションの継続的な信頼を確立するビジネスロジックを適用し、セキュリティプロセス（プロビジョニングやアクセス制御など）の自動化を支援することもできます。これは、スタッフワークロードの軽減や運用コストの低減はもちろん、運用の効率化やセキュリティの有効性の向上にもつながります。さらに、コンプライアンスレポートと監査プロセスを自動化する NGFW 機能は、ワークフロー負荷の軽減だけでなく、変化を続ける政府機関や業界の法規制、およびアメリカ国立標準技術研究所（NIST: National Institute of Standards and Technology）や CIS（Center for Internet Security）のセキュリティ標準への対応にも役立ちます。

IT 意志決定者の半数以上（54%）が、ハイブリッドモデル採用を阻む課題の 1 つとして、人材の定着を指摘しています [7]。

トップクラスの NGFW を兼ね備えた統合型ソリューションを選択する

データセンターの分散化とハイブリッド IT アプローチの普及に伴い、組織の攻撃対象領域は拡大を続けています。データセンターにはさらなるパフォーマンス向上が求められているものの、ネットワークエンジニアリングとオペレーションの責任者は、セキュリティニーズとユーザーニーズの妥協点を見つけられずにいます。リスク、ネットワーク障害の発生率、コストが増大する中、最新データセンターのセキュリティを再検討することが求められています。セキュリティとパフォーマンスを両立するには、堅牢な NGFW ソリューションを基盤とする統合型セキュリティアーキテクチャが必須です。このようなソリューションは、パフォーマンス、耐障害性、拡張性、自動化機能を一元的に実現できます。

[1]「Downtime Can Cost a Company up to $67 Million Over Two Years, Threatening Brand Reputation」、Filip Truta 著、Security Boulevard、2019 年 2 月 21 日（英語）：
https://securityboulevard.com/2019/02/downtime-can-cost-a-company-up-to-67-million-over-two-years-threatening-brand-reputation/

[2]「91% of tech leaders say hybrid cloud is 'ideal' IT model」、Alison DeNisco Rayome 著、TechRepublic、2018 年 11 月 15 日（英語）：
https://www.techrepublic.com/article/91-of-tech-leaders-say-hybrid-cloud-is-ideal-it-model/

[3]「2019 Data Breach Investigations Report」、Verizon、2019 年 4 月（英語）：
https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf

[4]「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-cio-and-cybersecurity.pdf

[5]「Encrypted Traffic Reaches A New Threshold」、John Maddison 著、Network Computing、2018 年 11 月 28 日（英語）：
https://www.networkcomputing.com/network-security/encrypted-traffic-reaches-new-threshold

[6]「TLS 1.3: What This Means For You」、Alex Samonte 著、フォーティネット、2019 年 3 月 15 日（英語）：
https://www.fortinet.com/blog/business-and-technology/tls-is-here-what-this-means-for-you.html

[7]「91% of tech leaders say hybrid cloud is 'ideal' IT model」、Alison DeNisco Rayome 著、TechRepublic、2018 年 11 月 15 日（英語）：
https://www.techrepublic.com/article/91-of-tech-leaders-say-hybrid-cloud-is-ideal-it-model/

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

EB-distributed-hybrid-dc-ngfw-202102-R1