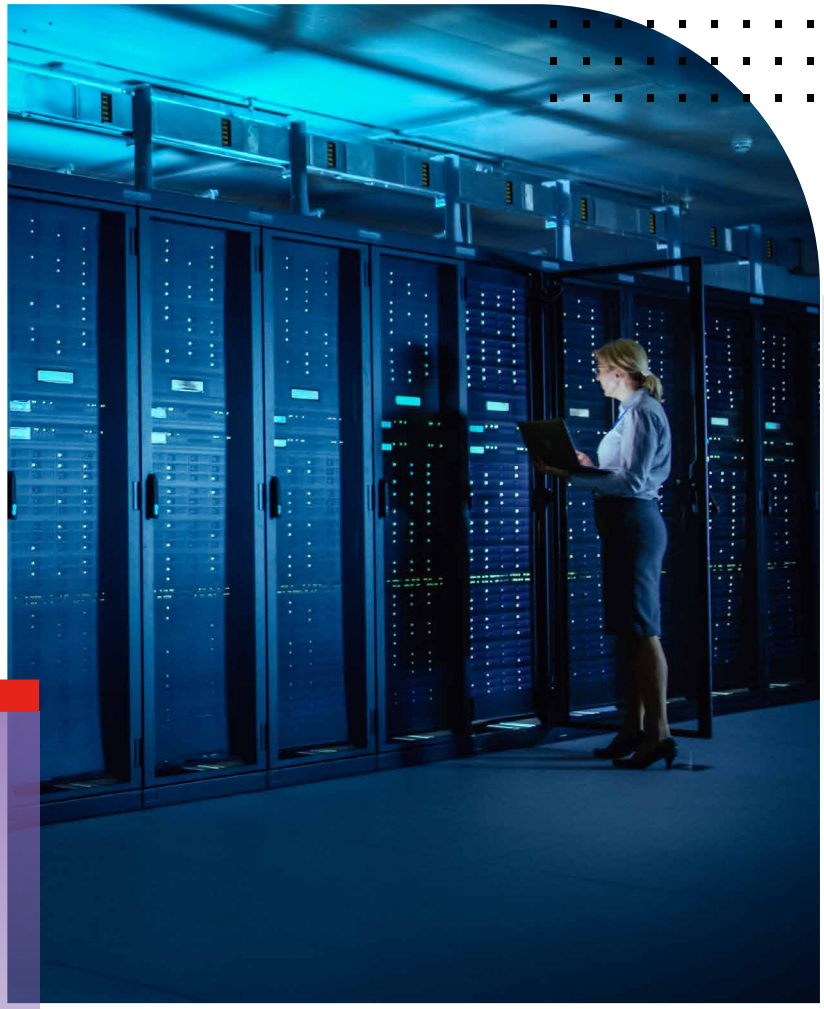
WHITE PAPER

ハイパースケール データセンターセキュリティ

ハイパースケールコンピューティングを阻害する、ネットワークとセキュリティの制約



概要

多くの業界において、多様なユースケースに対応するためにハイパースケールコンピューティングが採用されています。たとえば、大企業がハイブリッド IT アーキテクチャを構築してアプリケーションを迅速に立ち上げようとすると、物理ドメインと仮想ドメインに分散したアセット間の超高速通信が必要になります。ゲノム研究や航空宇宙研究などの高度な研究機関では、大規模なデータセットをネットワーク経由で転送する機能が必要です。e リテールなどの電子商取引企業は、ハイパースケールアーキテクチャを採用することで、サイバーマンデーなどのショッピングシーズンに爆発的に増加する接続を処理したり、COVID-19 のパンデミックによるアクティビティの急増に対処したりしています。

しかしながら、ハイパースケールデータセンターには、十分なセキュリティが確保されないという問題が存在します。その理由は、セキュリティソリューションが必要とされる速度に対応できなかったり、IT インフラが正しくセグメンテーションされていなかったりすると、多くの場合、セキュリティを有効にすることでネットワークのボトルネックが発生するためです。十分な機能を果たさないネットワークファイアウォールがボトルネックとなることから、ネットワークのエンジニアリングおよび運用管理者の多くは、ファイアウォールによるセキュリティを回避する道を選択しています。ところが、その選択によって、組織がさまざまな種類の攻撃の標的になり、基本的な機能の実行でさえも支障をきたすことになる恐れがあります。

ハイパースケールデータセンターの保護にあたっては、これまでの戦略を全面的に見直し、新しい戦略に最適なテクノロジーを選択する必要があります。

はじめに

デジタルイノベーション（DI）への取り組みとビジネスニーズによって、エンタープライズデータセンターの使用方法と、達成しなければならないパフォーマンス指標は変化しました。新しいネットワーク機能に対する需要に適応することが、ハイパースケールデータセンターの進化を促進しています。

ハイパースケールデータセンターは、効率的なスケーリングが可能で増大するビジネスニーズに合わせてダイナミックに稼働するデータセンターです。ハイパースケールアーキテクチャは、膨大な処理能力と天文学的なパフォーマンスが必要とされる、これまでにない要件に対応することを前提に設計されています。ビジネスニーズは業界によって異なります。ハイパースケールアーキテクチャは、次のような分野で必要とされています。

- **クラウドサービスプロバイダーを含む大規模エンタープライズ：**仮想化によって極めてスケーラブルな仮想ネットワークを作成しようとする組織では、VXLAN（Virtual eXtensible Local Area Network）に基づくネットワークセグメンテーションと同時に、物理 / 仮想両方のプラットフォームでホスティングされるサービス間の高速通信が必要です。
- **高速な e リテールを含むダイナミックな電子商取引サイト：**ショッピングシーズン、オンラインでの確定申告、給付金の申請などのイベントに伴って接続が急増すると、毎秒膨大な数のユーザー接続を処理する機能が必要です [1]。
- **医薬品、石油・ガス、航空宇宙業界における最先端の研究：**高度な研究にビッグデータや ML（機械学習）アルゴリズムを使用するには、40 Gbps と 100 Gbps の「エレファントフロー」を送信する機能が必要です [2]。
- **証券取引所：**電子取引インフラでは、できるだけ遅延を引き起こすことなく市場データを受信する必要があります [3]。
- **ハイパースケーラー（大規模でグローバルなテクノロジー企業）：**クラウドデータセンター間の高速なデータセンター相互接続によるディザスタリカバリ（DR）サイト間の複製には、データのプライバシーと機密性を実現するための高速インタフェースと高スループットの IPsec トンネル機能が必要です [4]。

多くの場合、これらの業界の企業は必要とするネットワークインフラに投資してきました。しかし、既存の次世代ファイアウォール（NGFW）ではハイパースケールアーキテクチャの大規模な拡張性とパフォーマンスのニーズを満たせないため、前述のようなニーズに対応できるセキュリティソリューションの調達は困難です。このような既存の NGFW は、企業が毎秒数千万のユーザー接続に対してアクセス制御を実行したり、DDoS 攻撃対策と必要不可欠なレイヤー 4 のファイアウォールの両方を実装したりしようとすると、対応が困難になります。結果として、パフォーマンスが低下するため、セキュリティ機能がビジネスの足手まといになること、あるいはネットワークインフラのスループットと待ち時間を最適化できなくなることを懸念する多くの組織は、セキュリティ機能を無効化することになります。しかし、これは危険なトレードオフであり、十分なセキュリティ制御が欠如した状態でエスカレートする要求に応えようとする選択は、攻撃されないことをひたすら天に祈るようなものです。

ハイパースケールアーキテクチャの課題

どの導入環境にも、ハイパースケールセキュリティの課題が存在します。

極めてスケーラブルで仮想化されたサービスを実行するための課題

企業は極めて俊敏にサービスを立ち上げ、生産性を高め収益を獲得できなければなりません。長期に投資利益率（ROI）のメリットを最大化するには、物理 / 仮想両方の資産の相互運用に対応する必要があります。

仮想化されたサービスを VXLAN などの極めてスケーラブルなテクノロジーを活用することによってすべてセグメント化し、VLAN では不可能な大規模スケーリングを実現できます。仮想化されたサービスは、多額の運用コストをかけることなく、スケールアップとスケールダウン、および移動が可能です。多くの場合、これらのサービスは既存の物理インフラ上の他のサービスとの通信に不可欠です。しかしながら、現在のほとんどのソリューションでは、パフォーマンスの低さと遅延の大きさに悩まされることになり、必要不可欠なレイヤー 4 のセキュリティでセッション状態を追跡することも、アクセス制御で許可するユーザーと許可しないユーザーを決定することもできません。また、高度なレイヤー 7 も提供していないため、脅威の検知を強化することも、コンプライアンスやリスク管理の目的でポリシーを適用することもできません。

イベントに伴う接続急増によって機能不全に陥る、順応性のないセキュリティ

前述の例と異なり、その他の業界では、個々の接続の量自体は、企業がごく短時間に処理する接続の総数に比べると、決して膨大ではありません。しかし、ブラックフライデーやサイバーマンデーなどの主要なショッピングシーズンの EC サイトでは、24 時間にわたって莫大なユーザートラフィックが発生します。そのトラフィック件数は、1 年で 2 番目に件数の多い日の 1.5 倍に及びます [5]。

また、確定申告のシーズン、大規模イベントのチケット販売開始日、春節などの休日、およびオンラインゲーム（特に数百人のプレーヤーが 30 分間同時に参加するオンラインゲーム）環境においても、同様にイベントベースの接続増加が発生します。

これに対し、ハイパースケールアーキテクチャであれば、オンライン納税申告者、小売業者、およびゲームホスティングサービスは毎秒数百万件の着信接続を受け入れ、効率的に処理できます。ハイパースケールの投資対効果は簡単に説明できます。接続の切断やレスポンスの遅れが発生すると、売上を失い、ブランドイメージが低下する可能性があります。たとえば、ページの読み込み時間が 1 ～ 3 秒間遅れると、サイトを離脱する顧客は平均で 32% 増加します [6]。

攻撃に対して脆弱な大規模ネットワークフロー

人工知能（AI）と ML アプリケーションでは、アルゴリズムのトレーニングとテストのために膨大なデータセット（多くの場合、数テラバイト [7]）が必要です。製薬、バイオテクノロジー、ゲノム、石油 / ガス業界の機関はすべて、このような大規模なデータセットを研究で使用します。これらの研究機関がデータを処理し分析するには、大規模なデータセットをネットワーク経由で効率的に送信できなければなりません。しかし、そのようなデータセットを効率的に送信するには、「エレファントフロー」と呼ばれる、最大 100 Gbps を処理できるネットワーク帯域幅が必要です。

研究機関は理論上、ルーターとスイッチをベースにして構築されたハイパースケールネットワークアーキテクチャを活用することで、必要な帯域幅を提供できます。ただし、これらのデバイスは、セッション状態を追跡することはなく、基本的なレイヤー 4 のセキュリティも提供していません。DDoS 攻撃が増加する中、これらのデバイスもまた攻撃に対して脆弱です。

さらに、これらの接続を介して送信されるデータは機密情報であることが多く、EU の GDPR（一般データ保護規則）や HIPAA（医療保険の携行性と責任に関する法律）などのデータ保護法の対象となっています。これらの法律はさまざまなアクセス制御を義務付けています。つまり、ファイアウォールなどのセキュリティテクノロジーを介してネットワークトラフィックをルーティングし、メッセージのフローを暗号化する必要があります。ただし、多くの NGFW は 10 Gbps を超える接続帯域幅を処理できません。結果として、研究の大幅な遅れにつながるだけでなく、既存 WAN の ROI のメリットを最大化することもできません。WAN リンクは 40 Gbps や 100 Gbps でデータが転送することが求められているのに、既存の NGFW がクラッシュせずにサポートできる単一フローが 10 Gbps であるからです。

数百万ドルの損失につながりかねないファイアウォールの遅延

株式市場の取引や競技ゲームをはじめとする業界では、ネットワーク遅延を最小限に抑えることが極めて重要です。ネットワークトラフィックのラウンドトリップタイム（RTT）にわずかでも遅延が発生すると、収益性やパフォーマンスに大きく影響する可能性があります。

このため、金融業界の組織は一般的にデータセンターへの遅延が極めて小さいネットワークインフラに投資します。電子取引インフラで許容される遅延は、わずか 5 μs 以下です [8]。遅延の影響を受けやすいコンテキストでは、多くの組織がネットワークスループットのためにセキュリティを犠牲にして NGFW を監視モードで構成しています。

高速のデータセンター相互接続には高スループットの IPsec 接続が必要

クラウドサービスプロバイダー、および CDN（コンテンツ配信ネットワーク）を運用する組織にとって、複数の地域サイト間でデータを複製する機能は不可欠です。組織が地域サイトを使用して保存データの完全なコピーをホストする主な理由には、耐障害性の向上、顧客の要求に対するレスポンスの遅延低減、そしてプライマリデータセンターの負荷軽減が挙げられます。

これを可能にするには、ネットワークの同期をサポートする地域サイト間の高帯域幅リンクである DCI（データセンター相互接続）が必要です [9]。クラウドサービスプロバイダーと CDN は機密データを送信することが多いため、これらのリンクは多くの場合 IPsec トンネルとして実装されます。ただし、それと同時に、レイヤー 4 のネットワークセキュリティではネットワークリンクと同じスループットで NGFW が IPsec トラフィックを処理する必要があります。ほとんどの既存の NGFW は 10 Gbps を超える IPsec スループットを実現できないため、これらのリンクを保護する NGFW によって、データセンター間での大量の転送の全体的な速度が低下する可能性があります。

終わりに

効率とカスタマーエクスペリエンスの向上を目的とした DI の取り組みにおいては、ネットワークインフラを進化させる必要があります。ハイパースケールデータセンターは、大規模なネットワークフロー、接続の急増、およびその他のユースケースをサポートするように設計されています。

ハイパースケールネットワークアーキテクチャの導入が進む中、多くの組織はハイパースケールセキュリティの実現というさらに困難な課題に直面しています。ネットワークのボトルネックを解消する目的で NGFW を無効にする、あるいは監視モードにすると、攻撃に対して無防備になるだけでなく、データ保護の法規制へのコンプライアンスに違反してしまう可能性があります。アプリケーションや IT インフラがセグメンテーションされていないと、エッジに侵入してネットワークのコアに到達する機会を侵入者に与えることになります。そして、攻撃の発生元が内部の信頼されたユーザーである場合、このような危険な結果はさらに深刻なものとなります。

ハイパースケールデータセンターには、極めて革新的なアプローチと拡大するビジネスニーズに合わせて拡張可能なセキュリティソリューションが必要です。ハイパースケールセキュリティソリューションによって、大量のユーザー接続をスケーラブルに処理し、毎秒数千万の接続に対応し、100 Gbps のエレファントフローをサポートし、大規模な仮想環境の効率的なセグメンテーションを可能にし、高パフォーマンスの必要不可欠なレイヤー 4 セキュリティでエンタープライズエッジを保護し、DDoS 攻撃を防ぐことができなければ、すべての賭けが失敗し、さまざまなサイバー攻撃を仕掛ける攻撃者にとって有利な方向に進み、ひいてはビジネスが混乱し、評判が低下し、最終的には廃業に追い込まれる恐れもあるのです。

[1] 「The Best Days for Holiday Sales: A Guide for Businesses」、Marisa Sanfilippo 著、Business News Daily、2019 年 12 月 2 日（英語）：
https://www.businessnewsdaily.com/10220-holiday-sale-days.html

[2] 「Digital innovation: A review and synthesis」、Rajiv Kohli、Nigel P. Melville 共著、Information Systems Journal、2018 年 1 月 29 日（英語）：
https://onlinelibrary.wiley.com/doi/abs/10.1111/isj.12193

[3] 「セキュアで高速なパフォーマンスを実現する FortiGate 次世代ファイアウォール」、フォーティネット、2019 年 9 月 23 日：
https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/ja_jp/SB-Secure-Communications.pdf

[4] 「What is DCI?」、Ciena、2019 年 5 月 16 日（英語）：https://www.ciena.com/insights/what-is/What-is-DCI.html

[5] 「The Best Days for Holiday Sales: A Guide for Businesses」、Marisa Sanfilippo 著、Business News Daily、2019 年 12 月 2 日（英語）：
https://www.businessnewsdaily.com/10220-holiday-sale-days.html

[6] 「Find Out How You Stack Up to New Industry Benchmarks for Mobile Page Speed」、Google、2017 年 3 月（英語）：
https://www.thinkwithgoogle.com/intl/en-aunz/advertising-channels/mobile/au-mobile-page-speed-new-industry-benchmarks/

[7] 「Machine Learning and HPC in Pharma Research and Development」、Mohammad Shaikh、Harsha Gurukar、Super Computing 2019、2019 年 11 月（英語）：
https://sc19.supercomputing.org/proceedings/bof/bof_pages/bof156.html

[8] 「セキュアで高速なパフォーマンスを実現する FortiGate 次世代ファイアウォール」、フォーティネット、2019 年 9 月 23 日：
https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/ja_jp/SB-Secure-Communications.pdf

[9] 「What is DCI?」、Ciena、2019 年 5 月 16 日（英語）：https://www.ciena.com/insights/what-is/What-is-DCI.html

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

WP-Demystifying-Security-Hyperscale-DC-202202-R1