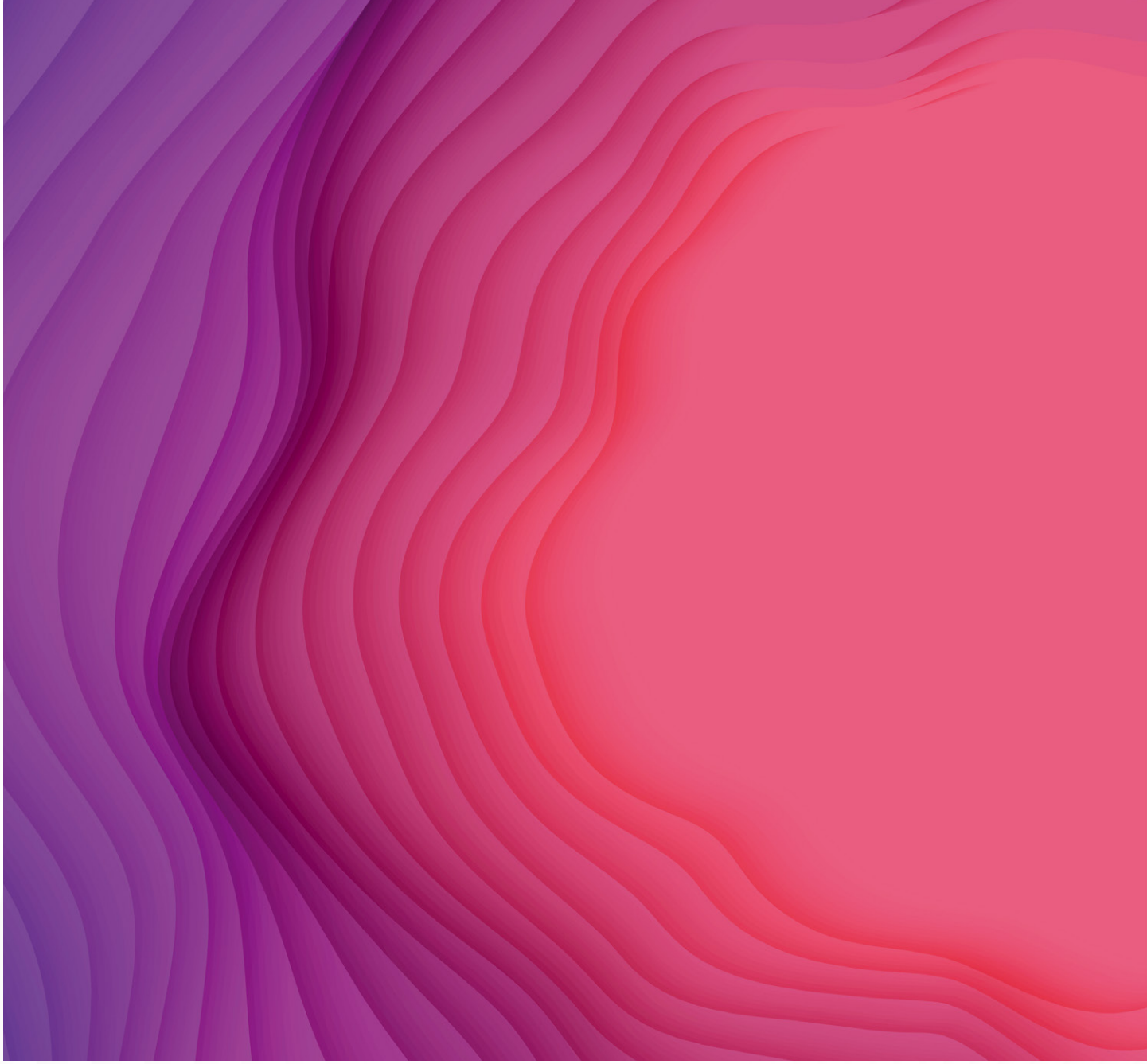


データセンターネットワークセキュリティの新常識

脱・高機能ファイアウォール専用機のススメ

HPE aruba networking

Contents

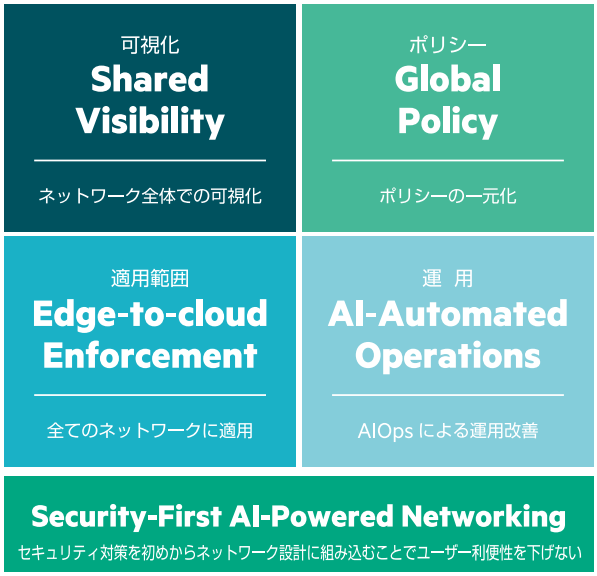
データセンターネットワーク編

セキュリティがビルトインされた Security-First AI-Powered Networking

SaaSをはじめとした各種クラウドアプリケーションを業務利用する機会が一般化した今、快適な業務環境を提供するためには、利便性や体感、快適さといったユーザエクスペリエンス（UX）を向上させるネットワークの最適化は重要な役割を果たします。一方で、ランサムウェアをはじめとする高度な脅威によるビジネス被害の拡大は後を絶ちません。特に、企業規模を問わずマルウェア被害が相次いでいることからも、どんな企業であってもセキュアな環境づくりがこれまで以上に求められています。

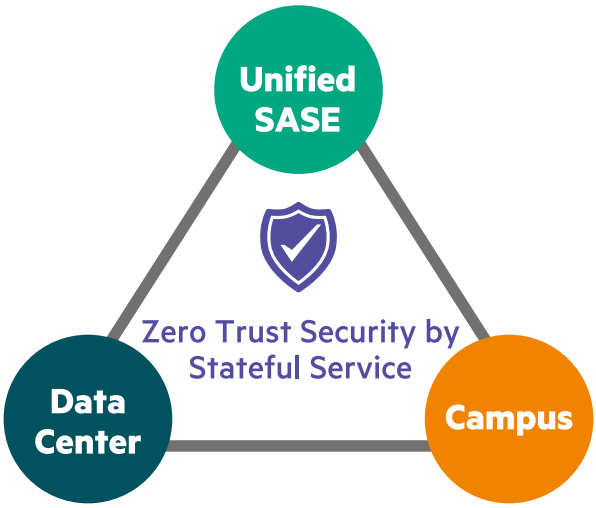
ただし、ネットワークの利便性と強固なセキュリティに求められる要件は、相反するものになりがちです。快適にアプリケーションを利用するためにネットワークへのアクセスを容易にすれば利便性は高まりますが、コンプライアンスの遵守を含めたセキュリティの観点からは、トラフィックや振る舞いの可視化、接続時の認証・認可、権限に応じたアクセス制御などが必要になり、要求レベルを高めるほど、ネットワークの性能や使い勝手に影響を与えてしまい、結果としてUXの低下を招くことになってしまいます。

そこでHPE Aruba Networkingが掲げているのが、最適なUXを維持しながらセキュアなネットワークを実現するためのアーキテクチャである「Security-First AI-Powered Networking」です。Security-First AI-Powered Networkingには、「ネットワーク全体での可視化」「ポリシーの一元化」「Edge-to-Cloud の全てのネットワークに適用」「AIOpsを活用したセキュリティの向上と運用の改善」という4つの特長が備わっています。



セキュリティの機能を標準でネットワーク製品にビルトインさせるSecurity-First AI-Powered Networkingによって、ハイパフォーマンスで快適なネットワークと高度な脅威に対応できるセキュアなネットワークを同時に提供することが可能となるのです。

セキュリティがビルトインされたネットワークは、多くの企業が検討を進めるゼロトラストのコンセプトにつながります。なかでも重要な要素となるのが、ステートフルサービスです。具体的には、内部からの必要な通信のみ許可し、外部からの不明な通信を全てブロックするステートフルファイアウォール機能です。キャンパスやWAN(≒Unified SASE)、そしてデータセンターなど企業を取り巻くネットワーク全ての領域でステートフルサービスを実装し、セキュリティと利便性を兼ね備えたネットワークを実現します。



データセンターにおける課題

このような企業を取り巻くネットワークの1つであるデータセンターを運用するIT部門においては、現在どんな課題が顕在

化しているのでしょうか。主に「運用性」「拡張性」「セキュリティ」の観点でまとめることができます。

運用性の課題

昨今では業務アプリケーションのクラウドシフトが進み、幅広いクラウドアプリケーションが利用されていますが、サーバやネットワーク運用が欠かせないデータセンター領域については、長い間アーキテクチャやデザインが大きく変更されておらず、モダナイゼーションが進んでいない企業も少なくありません。スイッチやルーターなどのネットワーク機器が個別最適化した状態で運用されているものの、複数ベンダーのソリューションが乱立しており、運用性や拡張性に大きな課題が残されています。

拡張性の課題

仮想環境が広がったことでサーバ運用やネットワーク、そしてセキュリティなどが複雑に絡み合い、物理環境と仮想環境の双方を柔軟に連携させていくことが求められています。仮想マシンがひと昔前に比べて増大したことでデータセンター内のトラフィックも大幅に増えているはずです。ユーザー体験を損なわないようパフォーマンスを維持・向上させていくためにも、ITインフラが柔軟に拡張していけるかどうかが、ビジネスを阻害しないITインフラづくりには欠かせません。個別最適化されたITインフラでは、柔軟に拡張していくことが難しいことは自明の理といえます。

セキュリティの課題

IT部門が対策に苦慮しているのが、攻撃の高度化による新たな脅威への対応です。最近では端末のロックやデータの暗号化によってシステムの業務利用を妨害し、復旧と引き換えに金銭を要求するランサムウェアによる被害が拡大していることはご存知の通りでしょう。マルウェアの侵入を前提としたゼロトラストと呼ばれる考え方をベースに、企業ごとに最適なセキュリティ対策を模索する必要がありますが、特に貴重な情報資産が保管されているデータセンター内では、サーバやラック間の通信となるEast-West通信におけるセキュリティ対策に注力する必要があります。セキュリティは後回しにできない喫緊の課題だけに、時間とコストをいかに軽減しながら自社に適したセキュリティ対策が実装できるかどうかにかかってきます。

データセンター運用における課題解決のアプローチ

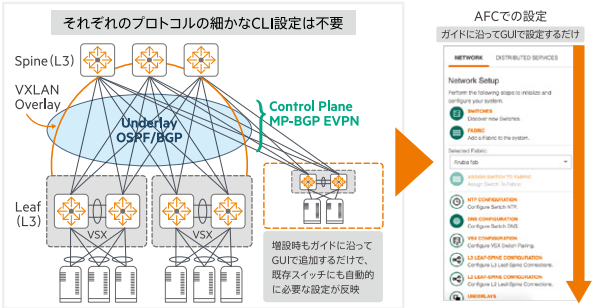
データセンターを中心としたITインフラの運用管理に対する多くの課題が顕在化している今、どのようなアプローチを活用するべきなのでしょうか。

運用性への解決アプローチ

できる限り運用管理の負担を減らすためにも、全体最適化を目指してITインフラが統合管理できる環境づくりを目指すべきです。そのためには、データセンターのみならず、支店や営業所などキャンパスネットワークからデータセンター内のコアネットワークまで含めて一元管理できる環境整備を進めていきたいところです。またサーバ環境との柔軟な連携による自動化を進めるためにも、豊富なAPIにて仮想環境との連携が可能な仕組みづくりを進めていきたいところです。

Aruba Fabric Composer（AFC）と呼ばれる管理ツールは、AOS-CXをネットワークOSに持つ各種スイッチを一元管理できるだけでなく、APIを通じてVMwareが提供する仮想マシンや仮想スイッチ、NICなどの自動検知および設定が可能となっており、運用管理における省力化、自動化、可視化に大きく貢献します。しかも、多様なプロトコルを理解したうえで複雑な設定が求められるSpine&Leafアーキテクチャであっても、ガイドに沿ってGUIから設定できるため、構築や運用の簡素化に貢献します。またAFCはネットワーク、仮想環境だけではなく後述のHPE Aruba Networking CX10000に組み込まれたセキュリティポリシーの一元管理する機能を有しています。

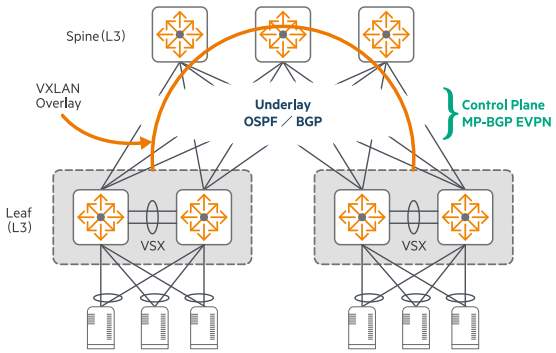
もちろん、全ての環境を一気に切り替えることは難しいため、既存ネットワーク上に新たな仮想ネットワークを形成し、物理的な環境に依存せずとも仮想スイッチを含めたEnd to Endの可視化と管理が可能な環境がつくり出せると理想的です。



拡張性への解決アプローチ

トラフィック量が増加するデータセンターにおいて、負担をかけることなく柔軟に拡張していける基盤整備が求められます。特にアプリケーション領域での柔軟な拡張が可能なクラウドアプリケーションのように、ITインフラ領域であってもクラウドネイティブな環境づくりを進めていきたいところです。とりわけ課題になる物理環境の拡張においては、サーバ領域におけるHCIのようなプライベートクラウド環境が理想的ですが、同じようにネットワーク領域においても、クラウド環境で管理しながら柔軟にスケールアウトしていけるようなものが理想的です。

従来のデータセンターネットワークは、コア・アグリゲーション・アクセスという3つの階層でネットワークが構成されてきましたが、最近ではダウンタイムなく柔軟にスケールアウトが可能なSpine&Leafアーキテクチャによる2層型のネットワークが大きな潮流となっています。可用性を高めながら、膨大なトラフィック量となっているEast-West通信を快適に処理できるネットワーク構成へ切り替えることで、柔軟に拡張していけるITインフラが整備できるようになります。

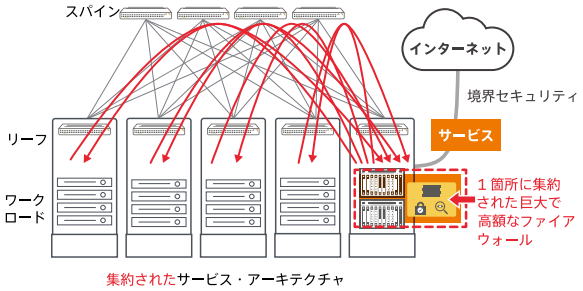


メリット	課題
スケーラビリティ 1,000、10,000、100,000 以上のエンドポイント（サーバー、ストレージ）を最適に相互接続 オーバーサブスクリプションの削減が容易	**多様なテクノロジ（プロトコル）の理解が必要** Underlay OSPF/BGP、Overlay VXLAN、Control Plane EVPN
高可用性 ノードやリンクに障害が発生した場合の冗長性を確保	**スイッチの設定が複雑**
低遅延 他のピアに到達するためのホップ数を最小にする	
E/Wトラフィック vs N/Sトラフィック 両方必要だが E/W への対応が Campus より重要に	

セキュリティへの解決アプローチ

データセンターにおけるセキュリティ対策は、従来はインターネットとの接続部分に設置された境界防御を前提としたファイアウォールが重要な役割を果たしてきましたが、マルウェアなどの攻撃が侵入することを前提にしたセキュリティ対策では、それだけでは不十分です。イントラネット内に侵入したマルウェアによって引き起こされる、他の端末へ感染を拡大させていく横の動きとしてのラテラルムーブを最小限に防ぐためにも、イントラネット内部にファイアウォールポリシーを細かく設ける必要があります。

データセンター内部にファイアウォールを設置し集中的に処理する場合、パフォーマンスを低下させないよう高性能なステートフルファイアウォールを導入する方法がありますが、大規模な投資が必要になるうえ、輻輳・レイテンシの増加への考慮が必要です。また新たな機器が展開されることで、運用管理の負担も増えてしまう可能性があります。できれば、コストを抑えながら各所にファイアウォールが設置できるような分散型の仕組みを検討してみることも有効です。



現在のアーキテクチャの課題

- ✕ 帯域幅が効率的に利用できない
- ✕ 輻輳と高レイテンシ
- ✕ 設計やトラブルシューティングが複雑
- ✕ 単一機能に限定
- ✕ Firewall の投資が非常に高価

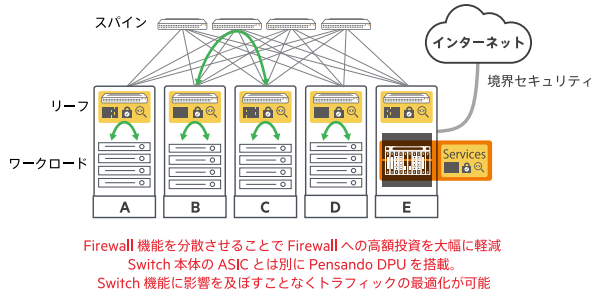
HPE Aruba Networkingからの新提案「HPE Aruba Networking CX 10000」とは？

データセンター運用に関連した多くの課題に応えることができるソリューションが、HPE Aruba Networkingが提供する分散サービススイッチ（DSS）である「HPE Aruba Networking CX10000」です。

HPE Aruba Networking CX10000は、ToR（Top of Rack）に設置するスイッチとして開発されたもので、HPE Aruba NetworkingとAMD Pensandoがコラボレーションしたことで生まれた分散型データ処理ユニットであるDPUを2つ搭載しています。ステートフルファイアウォールの機能をハードウェアにオフロードできる分散サービススイッチで、800Gbpsという高いスループット性能を兼ね備えています。

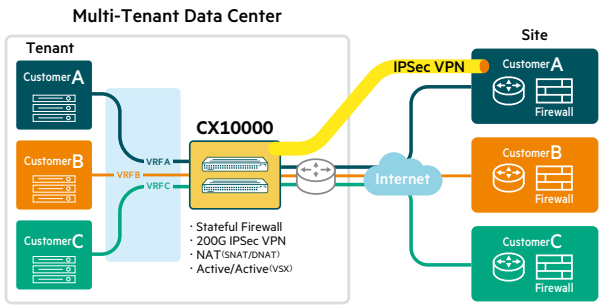
一般的なスイッチング処理はスイッチングASICにて処理し、ファイアウォール処理は2つのDPUが担うことで、ハイパフォーマンスな処理を実現します。

また、複数テナントが収容可能な200Gbpsのスループットを誇るハイスペックなIPsec終端装置として機能するため、HPE Aruba Networking CX 10000がハイブリッドクラウドとの接続を一手に担うことで、シンプルなネットワーク構成が実現できます。



Firewall 機能を分散させることで Firewall への高額投資を大幅に軽減
Switch 本体の ASIC とは別に Pensando DPU を搭載。
Switch 機能に影響を及ぼすことなくトラフィックの最適化が可能

- ✓ソフトウェア定義のサービス
- ✓ステートフルなセキュリティ・サービス
- ✓セキュリティポスチャの向上、アプライアンス・スプロールの制限、コスト削減
- ✓ネットワーク帯域幅とパフォーマンスの最適化
- ✓ネットワークやセキュリティのプロビジョニング及び運用の簡素化



分散サービススイッチであるHPE Aruba Networking CX 10000は、ステートフルファイアウォール機能だけでなく、ロードバランシング機能やNAT機能などへの対応も予定しており、それぞれ個別のソリューションが必要だった環境を集約することが可能になり、運用管理の負担をこれまで以上に軽減することができるソリューションとなっています。

ビルトインされたセキュリティ機能

セキュリティについては、East-West通信におけるラテラルムーブを防ぐことが可能なステートフルファイアウォール機能を備えた分散サービススイッチであるHPE Aruba Networking CX 10000であれば、万一のマルウェア侵入時にも最小限の範囲で被害を留めることが可能なMicro Perimeterとして役立ちます。また、800Gbpsのスループット性能を持っており、ラテラルムーブの抑制などセキュアな環境づくりに貢献しながら、仮想マシンの増加によって増え続けるEast-West通信のトラフィックでも快適に処理できます。

また分散配置されたHPE Aruba Networking CX10000に実装されるファイアウォールポリシーはAFCにより一元管理が可能で、データセンター内の高いセキュリティとシンプルな運用管理に貢献できます。

HPE Aruba Networking CX10000をはじめとしたHPE Aruba Networkingソリューションによって、データセンター運用における課題を解決しながら、セキュリティ機能がビルトインされたHPE Aruba Security-First AI-Powered Networkingとして、強固なセキュリティデータセンターネットワークが整備できます。ぜひ一度、ご検討いただければ幸いです。

お問い合わせ : 日本ヒューレット・パッカード合同会社　www.arubanetworks.com/contact