SASE構築・運用に忙殺されることがあなたの仕事なの?

手間暇かけずに最強SASEを作るために必要なたった1つのこと

HPE aruba networking

Contents

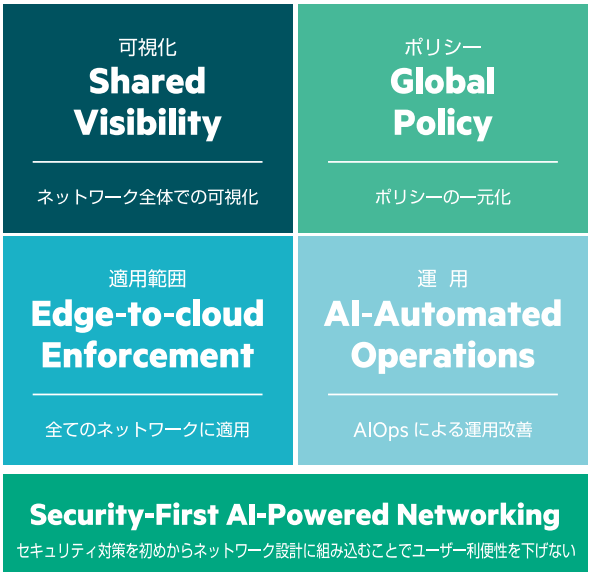
Unified SASE 編

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。

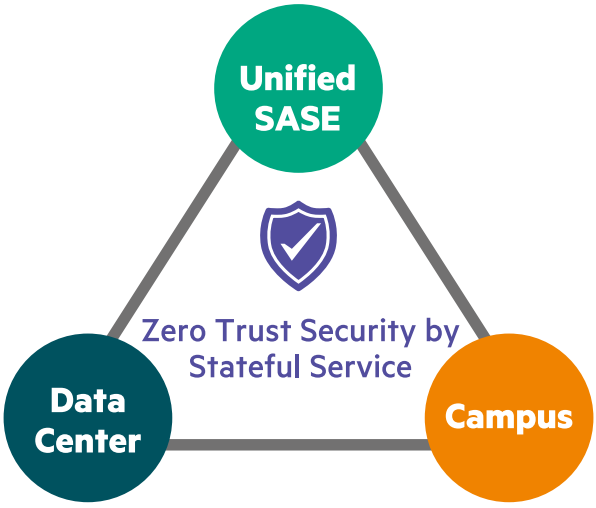
ただし、ネットワークの利便性と強固なセキュリティに求められる要件は、相反するものになりがちです。快適にアプリケーションを利用するためにネットワークへのアクセスを容易にすれば利便性は高まりますが、コンプライアンスの遵守を含めたセキュリティの観点からは、トラフィックや振る舞いの可視化、接続時の認証・認可、権限に応じたアクセス制御などが必要になり、要求レベルを高めるほど、ネットワークの性能や使い勝手に影響を与えてしまい、結果としてUXの低下を招くことになってしまいます。

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。



ゼロトラストを実現するSASE

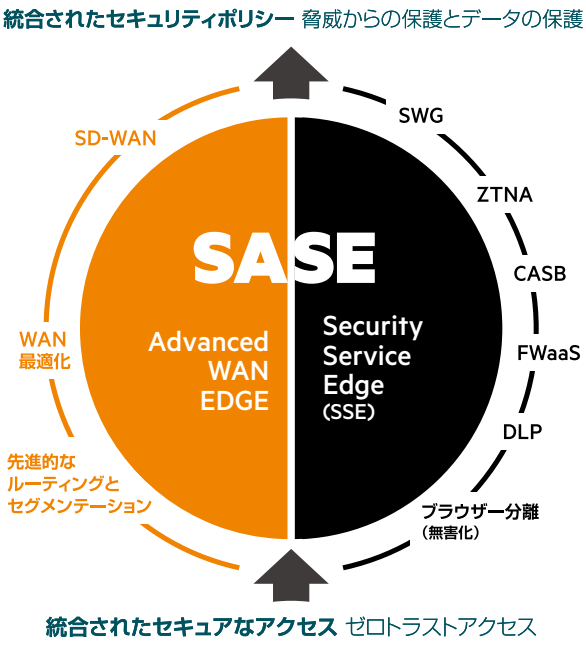
そんな企業を取り巻くネットワークの1つであるWAN領域においては、ゼロトラストにおいて求められる複数コンポーネントを組み合わせたSASE（Secure Access Service Edge）による環境づくりが重要になってきます。

そもそもゼロトラストとは、ネットワークやセキュリティにおいて「何も信頼しない」ことを前提とした考え方です。この信頼しないという考え方に立つゼロトラストでは、ネットワークに接続してくるデバイスやユーザーが、常に信頼に足るかどうかをその都度判断していくことが必要で、何か問題があれば動的に対処できる仕組みづくりが重要です。また、昨今では

標的型攻撃も含めた高度化された脅威の広がりとともに、従業員が機密情報を持ち出す内部不正といったインシデントも発生するなど、外部からの脅威だけでなく、境界内部にも脅威が存在してしまっています。その意味では、侵入されることを前提とした多層防御セキュリティの考え方にシフトせざるを得なくなっていることも、ゼロトラストの重要性が高まる大きな要因の1つといえるのです。

このゼロトラストを実現するための環境として注目されているのが、統合ネットワークとセキュリティ機能の各種コンポーネントを組み合わせたSASEです。SASEは、大きく分けて統合セキュリティ機能を備えたSSE（Security Service Edge）と、SD-WANを中心としたWANエッジサービスの2つが備わっています。

SSEには、クラウドセキュリティとしてプロキシ機能やフィルタリング機能を提供するクラウドSWG（Secure Web Gateway）やプライベートゾーンへのアクセスを制御することが可能なZTNA（Zero Trust Network Access）、クラウドサービスにおける利用状況の可視化や制御を行うCASB（Cloud Access Security Broker）、アクセス制御をはじめとした高度な次世代ファイアウォール機能がサービス実装できるFWaaS（Firewall as a Service）、重要データの漏洩などを防ぐDLP（Data Loss Prevention）などを組み合わせて、単一のセキュリティサービスとして提供するものです。



またSD-WANは、トラフィックの内容を判断し、データセンターとの接続に利用するセキュアな拠点間接続とデータセンターを経由せず各拠点から直接クラウドアプリケーションにアクセスさせるローカルブレイクアウトが可能になるソリューションで、SWGをはじめとしたクラウドセキュリティ上に通信を振り分けることで、ネットワーク領域からセキュアな環境づくりに貢献します。

さらに、エンドポイントそのものを防御するための仕組みとして注目されているのが、デバイスの挙動を監視して保護することが可能なEDR（Endpoint Detection and Response）や、PCやスマートフォン、タブレットなどあらゆるデバイスを管理することが可能なUEM（Unified Endpoint Management）などです。多くの企業が従来型のアンチウイルスソフトに代わってEDRを検討・導入する傾向にあり、自社で管理できるエンドポイント保護には有効な策となるはずです。

SASE環境に求められるたった1つの真実 “シングルベンダー”

WAN環境においてセキュリティと利便性を兼ね備えた環境を整備することに貢献するSASEですが、前述した通り実装に必要なコンポーネントが数多く存在しており、これらをうまく組み合わせてつくり上げていくことが求められます。統一したポリシーでの運用はもちろん、SSEのコンポーネント同士の連携やローカルブレイクアウトを可能にするネットワーク領域に必要なSD-WANとの柔軟な連携など、ソリューション検討から環境整備、稼働後の運用まで考えると、異なるベンダーのコンポーネントを組み合わせていくことによる弊害が出てくる可能性は否定できません。

そこで重要になってくるのが、SSEおよびSD-WANを単一のベンダーで提供できるかどうかです。確かに、それぞれのコンポーネントを組み合わせて利用するベストオブブリードなアプローチも可能ですが、当然ながら運用していくためのノウハウが必要で、インテグレータによる支援や手作業による運用管理も少なくありません。そもそもSASEを構築・運用することが、システム部門が本来果たすべき役割ではないことからも、できる限り構築や運用がシンプルに実施できるシングルベンダーのソリューションを選択したいところです。

SD-WAN実装の理想

SASEにおけるネットワーク領域で重要な役割を果たすSD-WANですが、PCなどの端末にインストールするエージェントを利用してトラフィックを制御する方法が挙げられます。た

だし、既存のネットワーク構成を変更せずとも導入できるものの、エージェントが展開できないIoTデバイスやプリンタ、カメラなどがクラウドアプリケーションと通信するような運用がある場合は個別に対応する必要があります。当然、個別対応によって管理が煩雑になってしまう可能性があり、最適なアプローチとはいえません。エージェントのインストールも含めて展開や運用保守に課題が出てくることも考慮すると、拠点の出入口に設置したSD-WAN対応のアプライアンスにてWANへのトラフィックを制御するべきでしょう。

選択肢となりうるUTMが最適でないわけ

実際にSSEを提供するソリューションの多くは、SD-WAN対応のアプライアンスを持ち合わせていません。本来であればシングルベンダーSASEが理想的ですが、一部安価なUTMと組み合わせて実装するケースも見受けられます。このUTMには、多くの課題が顕在化しています。本来インターネットトラフィックのパフォーマンス向上のために検討するSD-WANのはずが、その目的が果たせないケースも出てきているのです。

【課題1】ローカルブレイクアウトしたが、パフォーマンスが改善されない

通常のSD-WANでは、通信の宛先を見て特定のクラウドアプリケーションにトラフィックを振り分ける機能を持っていますが、UTMのようなシンプルなトラフィック制御では、実際にパフォーマンスが改善されないケースも出ています。

一般的にローカルブレイクアウト環境を整備する場合、バックアップや回線増強を考慮してISPの異なる複数の回線を導入するケースが一般的です。複数回線のなかでクラウドアプリケーションのパフォーマンスを考慮してトラフィックが振り分けられるソリューションを選択するべきです。

【課題2】データセンターと閉域接続しているIaaSへの対応など柔軟性に乏しい

インターネットトラフィックのパフォーマンス改善に役立つローカルブレイクアウトですが、ケースによってはデータセンターを経由したこれまでの経路や、広帯域な環境を持つパブリッククラウドのクラウドハブを経由してアクセスするほうがパフォーマンス向上につながる場合も少なくありません。

UTMをはじめとしたソリューションの場合、宛先は考慮するものの、ルートごとにパフォーマンスを詳細に計測して最適な経路を選択するような仕組みは備わっていません。宛先だけでローカルブレイクアウトしてしまうようなものではなく、データセンター経由のアクセスも含めて柔軟に経路選択できる仕組みが望まれます。

【課題3】ローカルセキュリティでの限界、SASEと柔軟に連携できない

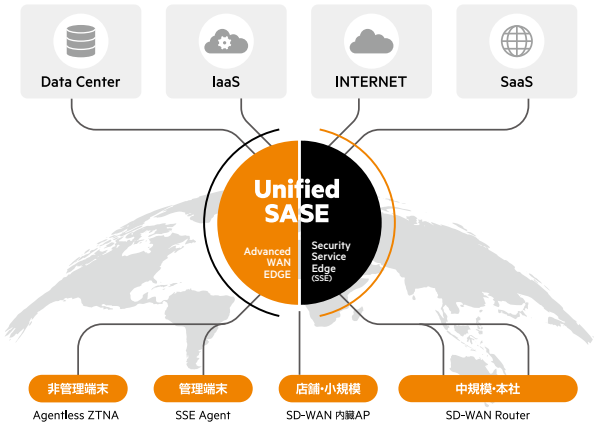
複数コンポーネントで構成されるSASEは、クラウド側でセキュリティ対策を実装していくことになるため、拠点に設置されたローカルセキュリティとしてのUTMに頼った構成とはアプローチが異なります。また、クラウドセキュリティとの連携が十分に考慮されていないため、将来的なSASEへの移行も視野に入れると、UTMは最適な選択肢とはいえません。SSEとのAPI連携が可能なUTMも存在しますが、統一したポリシーがどこまで適用できるかしっかりと見ておく必要があります。

【課題4】グローバルでガバナンスが発揮できない

グローバルに拠点を持つ企業の場合、日本と海外でのITインフラが統合されておらず、現地ローカルで最適なものを選択したうえで、個別最適化された形で運用管理しているケースは意外と多いものです。しかし、ランサムウェアやサプライチェーン攻撃など高度な攻撃手法を用いたインシデントが増えた今、グローバル全体でのガバナンスは強化していかなければならない状況にあります。統合管理が難しいUTMなどのローカルセキュリティに頼る環境から脱却し、SASEをはじめとしたクラウドセキュリティへの移行を視野に、グローバルでのガバナンスを強化するためのきっかけづくりにするべきです。

HPE Aruba Networkingが提供するHPE Aruba Networking Unified SASE

HPE Aruba Networkingでは、従来から展開していたSD-WANとともに、買収したAxis Security社が持つSSEを合わせたソリューションであるHPE Aruba Networking Unified SASEを提供しており、シングルベンダーで高度なSASE環境が実装できるソリューションを提供しています。



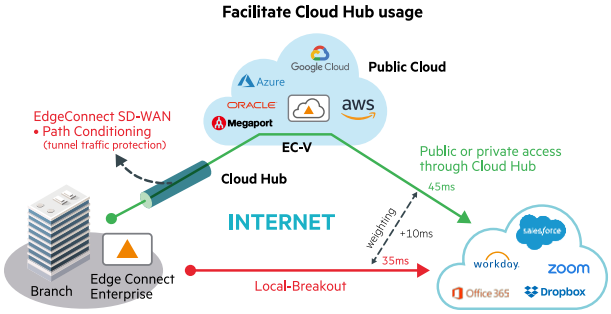
HPE Aruba Networking Unified SASEでは、アクセスコントロールポリシーに基づいて企業内のプライベートリソースへのセキュアなアクセスを実現するZTNAとともに、あらゆるWebトラフィックの監視・検査によってマルウェアからの保護およびURLフィルタリング機能を提供するSWG、SaaSアプリケーションに対する管理・制御・監視を実現するクラウドベースのセキュリティを提供するCASB、そしてエンドツーエンドでユーザーエクスペリエンスを可視化し生産性向上に寄与するDEM（Digital Experience Monitoring）をHPE Aruba Networking SSEとして提供します。

他社にあるような寄せ集めのコンポーネントではなく、統合SSEプラットフォームとして開発されており、シンプルな管理コンソールとAWSやAzure、GCP、Oracleなどのクラウドバックボーンを介して最適なアクセスを実現できるところが特徴です。また、ZTNAはクライアントからの通信だけではなく、サーバ発通信のアプリケーションにも対応し、VPNの完全撤廃が実現できます。またエージェントを必要としないエージェントレスZTNAもサポートしており、取引先を含めたサプライチェーン全体でのセキュアなアクセス環境への柔軟な対応も可能です。

そしてSD-WAN領域においては、HPE Aruba Networking SD-WANソリューション「Aruba EdgeConnect SD-WAN」を提供しています。拠点側に物理・仮想構成に対応できるEdgeConnect SD-WANアプライアンスを設置し、クラウド側に置かれたAruba Orchestratorによって統合的な管理が可能なソリューションです。HPE Aruba Networkingが保有する膨大なSaaSデータベースを活用し、的確なアプリケーション識別でWANトラフィックの最適な制御を実現します。

これまでグローバルでのガバナンスが十分でなかったとしても、クラウド上にあるAruba Orchestratorを活用することで、EdgeConnect SD-WANアプライアンス経由の通信が全て可視化、制御しやすくなり、日本主導のガバナンス強化を図ることができます。サプライチェーン攻撃など高まる脅威に対しても、グローバルガバナンスの強化によってリスクを最小限にとどめることに役立つはずです。

またEdgeConnect SD-WANでは、Microsoft 365やZoom、Salesforceといった各種クラウドアプリケーションとの接続において、パケットロスやレイテンシーなどパフォーマンスに影響する指標を詳細に計測し、最適な経路選択を行うApp Expressと呼ばれる機能が備わっています。単なる宛先だけのローカルブレイクアウトだけでなく、パフォーマンスに配慮した経路を自動的に選び出すことが可能になり、オフィスよりも自宅のほうがアクセスしやすいといった、ユーザー体験を損なうような事態を回避することができます。



App Expressが最適なパスを決定

10ミリ秒の遅延が追加されたパブリッククラウドを経由するパスは、直接のSaaSトラフィックブレイクアウトよりも優先される場合があり

クラウドオンランプとのトンネル保護の利点により、アプリケーションパフォーマンスの遅延の違いを上回る可能性

セキュリティ機能がバンドルされた快適なネットワーク環境を提供するSecurity-First AI-Powered Networkingにおいて、WAN領域のソリューションとしてゼロトラスト実現に貢献するHPE Aruba Networking Unified SASE。SD-WANも含めて真のシングルベンダーSASEとなるHPE Aruba Networking Unified SASEについて、ぜひ検討してみてはいかがでしょうか。

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