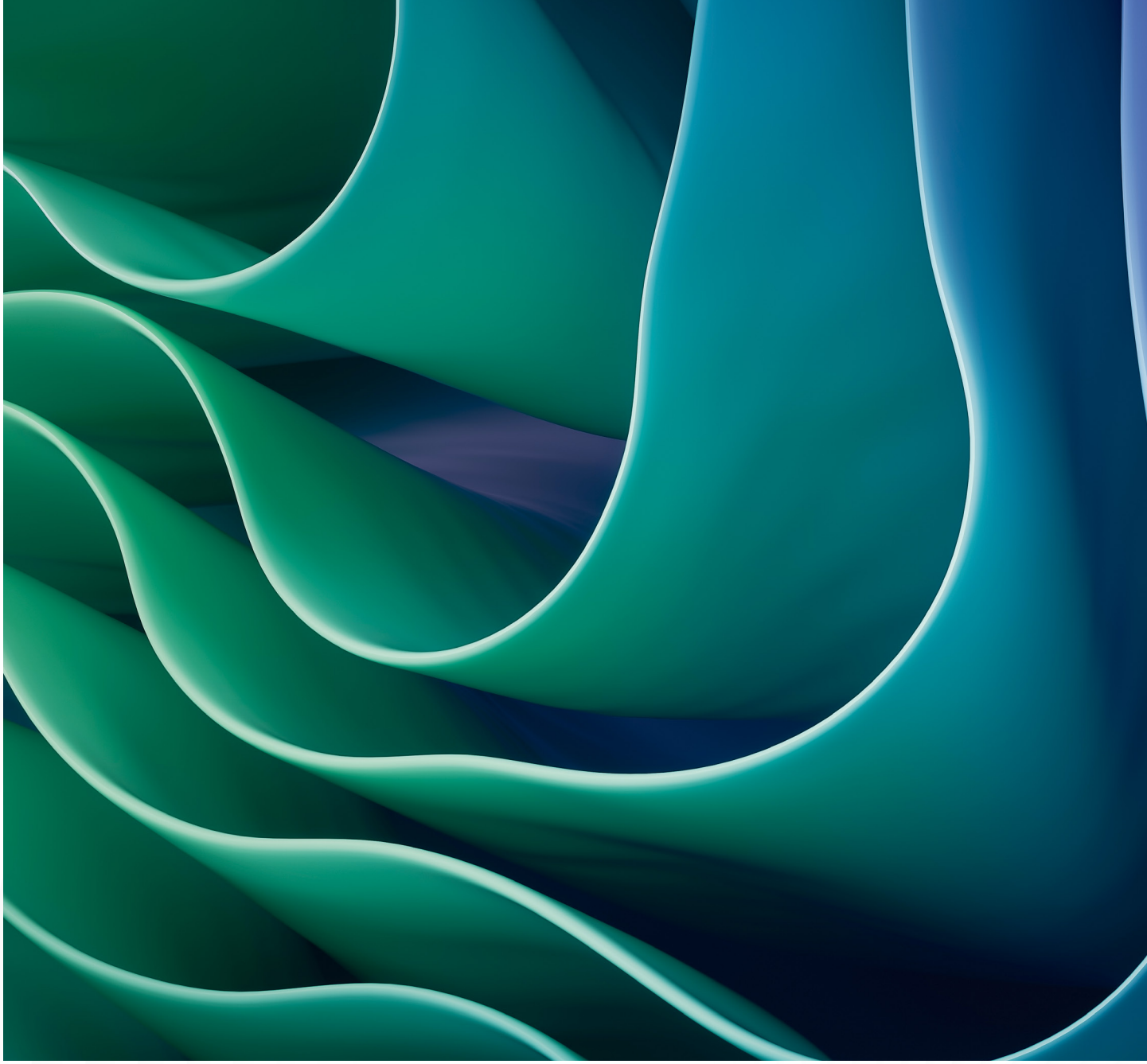


ランサムウェア発生源から見る“誤った投資”へ警鐘を鳴らす！

HPE Aruba Networking だから実現可能な「全方位ゼロトラスト」の方程式

HPE aruba networking

企業規模問わず対象となる マルウェアの存在

新たなビジネス変革を達成するために多くの企業がDXに取り組むなど、かつてないほどデジタル化が進んでいる状況にあるなか、悪意のある攻撃者が企業を狙って情報搾取を図ろうという動きが加速しています。世界的でセキュリティインシデントが数多く報告されるなど、多くの企業が悪意のある高度な攻撃に手を焼いている状況にあります。そんな脅威のなかでも、企業規模問わず被害を被っているのが、企業ネットワークに侵入して情報を搾取し、そのデータを不正に暗号化したうえで、復元と引き換えに身代金を要求する悪質なマルウェアであるランサムウェアです。

ランサムウェアは、メールやWebサイトからの感染とともに、脆弱性を狙ったネットワーク経由での攻撃や公開サーバへの不正ログインなど、その感染経路や方法は多岐にわたっており、これまで実施してきた境界防御で不正なアクセスを防ぐことが困難な状況です。業務アプリケーションの多くがクラウド上に展開されていることからも、境界防御に変わる新たな考え方が、現代のセキュリティ対策に求められてきています。同時に、ネットワーク侵入後に特定の端末を踏み台にして秘匿性の高い情報を搾取するといった攻撃の高度化によって、もはや社内環境であれば安全という方程式が成り立たなくなってきていることも、境界防御が限界を迎えている背景にあります。

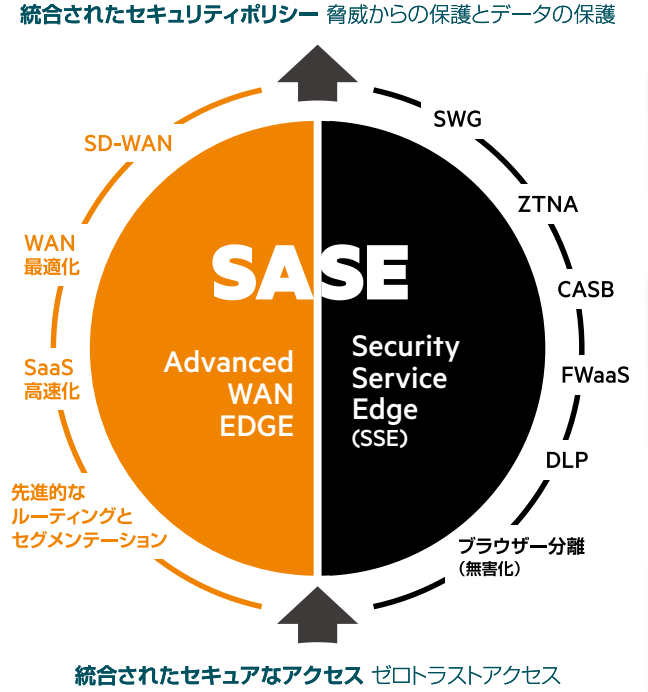
ゼロトラストを実現する SASEの有効性

そこで境界防御に変わる新たな考え方の中心となるのが、"何も信頼しない"というゼロトラストという考え方です。このゼロトラストは、NIST（National Institute of Standards and Technology：米国国立標準技術研究所）でも「SP 800-207: Zero Trust Architecture (A) ZT2nd DRAFT」としてゼロトラストがクラウド化・テレワーク型社会におけるセキュリティモデルとして紹介されています。このなかでは、大きく指定されたリソースへアクセス許可を決定するポリシーエンジン（PE）と通信経路の確立・遮断などを行うポリシーアドミニストレータ（PA）が備わったポリシー決定ポイント（PDP）と、そのポリシーを実行するポリシー実施ポイント（PEP）が主な論理コンポーネントとして定義されています。

そして、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(Secure Access Service Edge)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を中心としたセキュアネットワークの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。

SASEによりネットワークとセキュリティの変革を実現



また、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。

ランサムウェア被害、その発生源はどこにある？

SASEが大きなトレンドになっていますが、実はそれだけではマルウェア対策として有効とはいえません。特にランサムウェア

の場合、企業内部に侵入した後に脆弱性のあるエンドポイントを踏み台にして被害を拡大させるラテラルムーブが発生しますが、エンドポイントに対してEDRやSSEに関連したエージェントを導入していれば、常にSWGをはじめとしたクラウド上に展開されるSSEにアクセスさせる環境を整えることが必要です。

ただし、エージェントが展開できるのは、自社が管理できるエンドポイントがその中心で、自社で管理していない端末にエージェントを導入することは難しいところです。つまり、BYOD端末をはじめとした非管理端末を業務に利用している場合、管理端末とは別の対策を施す必要があります。この非管理端末の対象となるのは、何も自社に限った話ではありません。グループ会社や海外拠点といった自社で管理対象外の端末も含まれており、自社主導でエージェントが導入できない場合への対処が求められるのです。なお、自社で管理対象のデバイスだとしても、IoT機器やネットワークカメラといったエージェントが導入できない端末の場合には、個別の管理が必要になってしまいます。

実は、この非管理端末が昨今のランサムウェア被害の拡大を招いている大きな原因の一つになっています。Microsoftが公表している「Digital Defense Report 2023」によれば、過去1年間のランサムウェア攻撃の80～90%は、管理されていないデバイスから発生していることが明らかになっています。このことからも、EDRなどが導入できる管理対象のデバイスに大きな投資をするのではなく、非管理対処のデバイスへの対策にこそ投資を行う必要があるのです。ランサムウェアの発生源から考えれば、注目すべきは非管理端末への対策なのです。管理対象のエンドポイントにさらなる投資を進めようとしている企業は、ぜひ認識を改めるべきだといわざるを得ません。

非管理端末も含めた全方位ゼロトラストのススメ

自社で管理できる端末に対しては、ゼロトラスト実現に向けたSASEが有効な手立てとなりますが、一方で、ランサムウェアの発生源となっている非管理端末に対する有効な対策とは、具体的にどんな方法が考えられるのでしょうか。ここで重要になってくるのが、エンドポイントとなるデバイスを起点としたアプローチではなく、ネットワーク領域でのゼロトラストです。非管理端末にエージェントが導入できない以上、マルウェアが侵入してしまうことを前提に、ネットワーク側でマルウェアによるラテラルムーブを最小限に留める方策を検討する必要があります。ここで重要なのか、Micro Perimeter及びMicro Segmentation、そしてSSEが持つZTNAをはじめとしたSASEによるアプローチです。

• 境界をネットワーク内に多数設置する Micro Perimeter

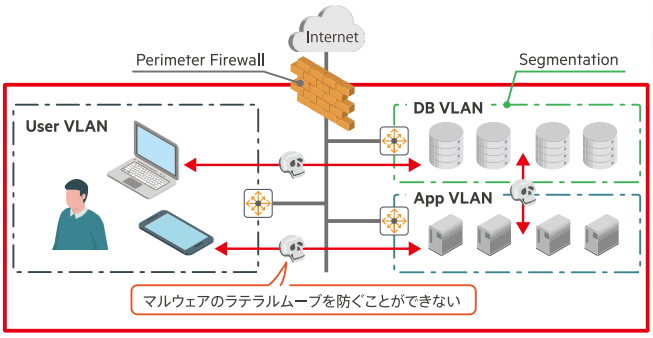
Micro Perimeterは、インターネットとの境界にこれまで設置していたファイアウォールの機能を、部門や部署といった細かな単位に分散して設置するものです。エンドポイントに近い範囲に設置された、パケットの振る舞いを検証して動的にフィルタリングが可能なステートフルファイアウォール機能でマルウェアの通信を制御することで、ラテラルムーブなどを最小限の範囲に留めることが可能です。エージェントが導入できずにSSE側でセキュリティチェックができない非管理端末が万一マルウェアに感染している場合でも、Micro Perimeterによって被害拡大を防ぐことができます。

• 最小限のアクセスに限定する Micro Segmentation

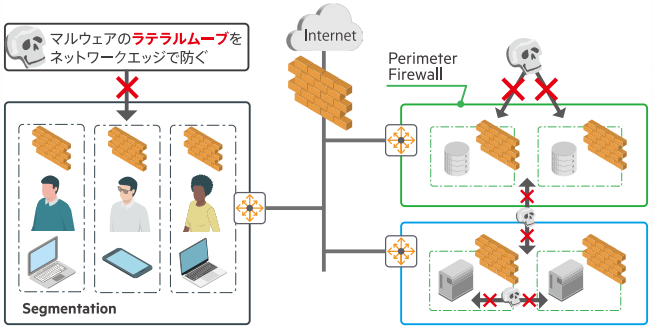
Micro Segmentationは、部門や部署、職制など利用者ごとにアクセスできるシステムをロールとして割り当て、最小限のアクセスだけを許可するものです。万一マルウェアに感染したエンドポイントが接続された場合でも、最小限のアクセスしか許可されていないことでラテラルムーブをおさえることができます。そもそも非管理端末がアクセスされた場合にも、限定されたアクセスだけを許可しておくことで対処できます。

マルウェアのラテラルムーブを防ぐ
Micro Perimeter & Micro Segmentationが必須要件に

■ Legacy Perimeter & Segmentation



■ Micro Perimeter & Micro Segmentation



・SD-WANとZTNAを中心としたSASE

SASEに関しては、SD-WANルーターやWi-Fiアクセスポイントなどゲートウェイとなるネットワーク機器がSSEとのセッションを確立させる機能を持っていれば、例えば拠点内にエージェントレスの非管理端末が接続された場合でも、その通信をオーバーレイによるトンネルを経由して強制的にSSEへ振り分けていくことでセキュアな環境が維持できます。万一エンドポイントがマルウェアに感染していた場合でも、ステートフルファイアウォール機能が実装されたMicro Perimeterの役割を果たすSD-WANルーターをはじめとしたゲートウェイによって、ラテラルムーブを最小限におさえられます。また、Micro Segmentationによって最小限のアクセスだけを許可しておけば、そもそもマルウェアの横展開自体をおさえることができることでしょう。

さらに、グループ会社などが保有する非管理端末への対策には、SSEが持つZTNAの機能を活用することで、自社へアクセスした場合でも限られたシステムにのみアクセスを許可することで、セキュアな環境づくりが実現します。

これら3つのアプローチによって全方位的なゼロトラストの環境が整備でき、部分的なゼロトラストでは実現できない非管理端末への対処が可能になるわけです。

データセンター及び キャンパス・ブランチネットワーク領域への 具体的なアプローチ

全方位ゼロトラストを実現するためには、企業のイントラネット全体に対して、ラテラルムーブを防ぐための環境づくりが求められます。そのため、基幹システムをはじめとした環境が設置・管理されているデータセンターネットワークの領域とともに、本社や支店などの主要な拠点となるキャンパスネットワーク、そして営業所をはじめとした小さな拠点となるブランチネットワークにおける全方位ゼロトラストのアプローチを考える必要があります。

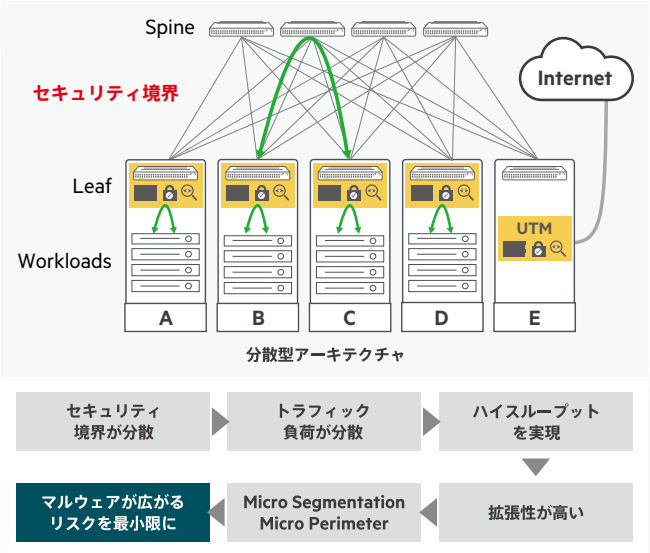
イントラネットとは別にクラウド環境に各種業務アプリケーションが設置されている場合は、管理可能なエンドポイントに対してエージェントを導入し、全ての通信をSSEに振り分けていくことでインターネットセキュリティを実現することが可能です。クラウドへの通信を振り分けるSD-WANとともに、クラウドセキュリティを実現するSSEを組み合わせたSASEが有効なソリューションになってきます。

・データセンターネットワーク

データセンターネットワークにおいては、サーバ間を含めた全ての通信をステートフルファイアウォール経由にすることで、Micro Perimeterの環境を実装することになります。この場合、全ての通信が集約できる高性能でハイパフォーマンスなステートフルファイアウォール機器を導入している企業が多くみられますが、1台だけでも非常に高額なうえに、単一障害点になってしまうことから冗長化構成を採用するとかなりの投資を覚悟する必要があります。最近ではスマートNICにファイアウォール機能を実装することでハードウェアに処理をオフロードさせるソリューションも出てきていますが、サーバの大掛かりな入れ替えが発生し、導入が困難になる場合があります。

データセンターネットワークは、コア・アグリゲーション・エッジの3階層デザインから、今は大量に発生するサーバ間の通信、いわゆるEast-Westの通信を効率的に処理するための、リーフ(葉)とスパイン(幹)で構成されたスパイン/リーフ型の2階層構成が大きなトレンドになっています。また、単一障害点を作らないよう機能を分散させた分散サービススイッチ(DSS:Distributed Services Switch)への移行が進んでいることからも、集約された環境からラック単位に分散したサービススイッチをトップオブラックに配置して、ラックごとにステートフルファイアウォールによるMicro Perimeterを実装し、ラテラルムーブを最小限におさえるアプローチが有効です。

Dss(分散サービススイッチ)によるゼロトラストデータセンター



・キャンパス及びブランチネットワーク

本社や支店などのキャンパスネットワークや営業所などのブランチネットワークにおいては、通常ネットワークへの接続は無線LANなどを経由するパターンが一般的になっていますが、利用者によってロールを詳細に割り当てておき、必要最小限のアクセスのみを許可するMicro Segmentationの環境は整備したいところです。また万一マルウェアに感染したエンドポイントが接続された場合は、そのエンドポイントを動的に隔離できるダイナミックセグメンテーションの環境づくりも意識すべきです。

部門や部署などネットワークの単位を狭めたうえでステートフルファイアウォールを細かく設置し、マルウェアのラテラルムーブを防ぐMicro Perimeterとしての環境整備も意識したいところですが、いずれの方策であっても、既存業務を継続しているタイミングにおいては、全てのネットワーク環境を刷新しないと導入できない仕組みは現実的に選択できません。できる限り既存のネットワークを維持したまま、うまくMicro SegmentationやMicro Perimeterの環境を整えていきましょう。

なお、エンドポイントにEDRを導入している場合は、そのものがファイアウォールの役割を果たしますが、あくまで管理端末の範囲のみ。ネットワークカメラやIoT機器などEDRを含めたエージェントが導入できない非管理端末への対策として、ネットワーク接続の基点となるWi-Fiアクセスポイントや外部に抜けるSD-WANルーターといったゲートウェイ部分にファイアウォール機能を用意しておくことも検討すべきです。

全方位ゼロトラストを可能にする HPE Aruba Networkingのソリューション

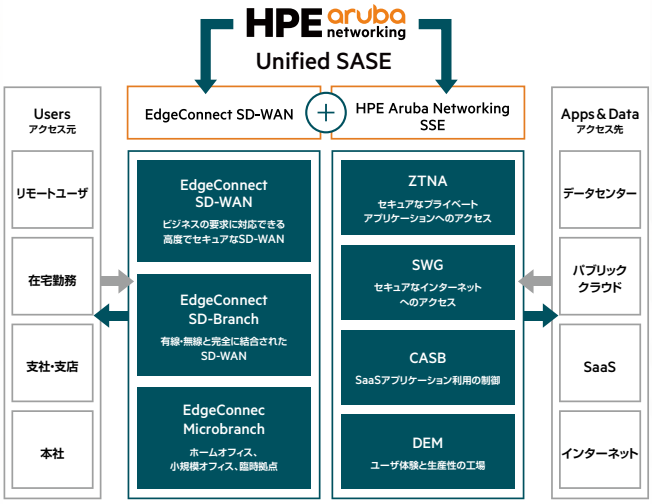
HPE Aruba Networkingでは、非管理端末も含めた全方位ゼロトラスを実現するためのソリューションを提供しています。具体的には、SASEソリューションとなるHPE Aruba Networking Unified SASEとともに、データセンターネットワークに対してMicro PerimeterおよびMicro Segmentationを実現する分散サービススイッチのAruba CX 10000、そしてキャンパスやブランチにおいてラテラルムーブを防ぐ環境づくりにHPE Aruba Networkingコントローラー／ゲートウェイ、アクススイッチ、Wi-Fiアクセスポイントなどが役立ちます。合わせて、ユーザーやデバイス認証を実施しながら、ネットワークの状況に応じて動的にアクセス制御するダイナミックセグメンテーションを実現するための認証サーバとなるClearPassも有効な策として提供可能です。

• HPE Aruba Networking Unified SASE

HPE Aruba Networkingでは、非管理端末も含めた全方位ゼロトラスを実現するためのソリューションを提供しています。その一つが、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です。

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及び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SSEとして提供します。

HPE Aruba Networking Unified SASE
業界をリードするEdgeConnect SD-WANと次世代SSEをSASEとしてご提供

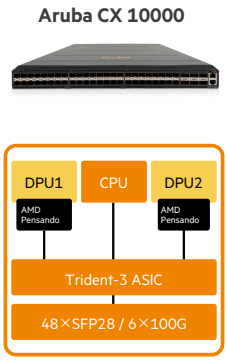


他社にあるような寄せ集めのコンポーネントではなく、統合SSEプラットフォームとして開発されており、シンプルな管理コンソールとAWSやAzure、GCP、Oracleなどのクラウドバックボーンを介して最適なアクセスを実現できるところが特徴です。また、ZTNAはSSHやRDP、サーバ発通信などさまざまなプロトコルに対応、エージェントレスZTNAもサポートしており、取引先含めたサプライチェーン全体でのセキュアなアクセス環境への柔軟な対応も可能です。

• データセンターネットワークへ適用する Aruba CX 10000

分散サービススイッチとして展開しているAruba CX 10000は、AMD Pensandoとのコラボレーションで生まれた分散型データ処理ユニットであるDPUを2つ搭載しており、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ます。しかも、一般的なスイッチング処理はArubaが持つASICが、ステートフルサービスは2つのDPUが担うことで、スループット性能が800Gbpsというハイパフォーマンスな処理を可能にするソリューションとなっています。

Aruba CX 10000 Distributed Services Switch - Powered by AMD Pensando



システム構成
- T3 Switching ASIC-3.2 Tbps、32MB Buffer (shared)
- フォワーディング、ルーティング、その他基本機能に利用
- 2×AMD Pensando DPU
- ステートフルサービスに利用
- 2×Redundant Power Supplies (N+1)
- AOS-CX OS、Spine & Leaf に対応

ポート構成
- 48×1／10G／25G SFP28、6×100G QSFP
- 1×1G RI45 management、1×RJ45 console port、1×USB

ステートフルサービス、利用シーン
- East-West セグメンテーション
- ステートフルファイアウォール、DDos フィルタリング
- マイクロセグメンテーション
- Flow Logging／Statistics

管理オプション
- Aruba AFC & Pensando PSM
- PSM & DevOps Tools (Terraform／Ansible)、REST API
- Aruba Central

ステートフルサービスにより、ラテラルムーブによるマルウェアの侵入・拡散を防ぐ

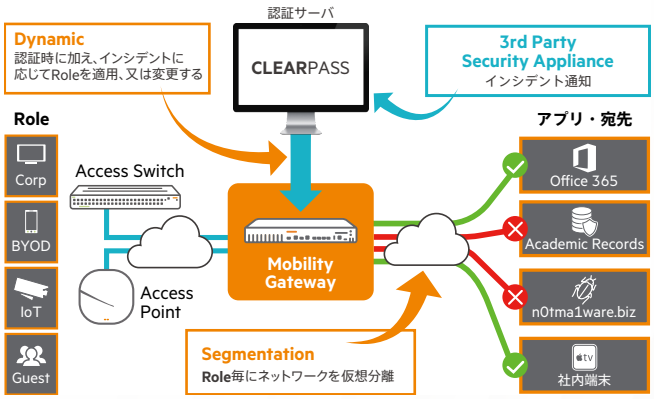
大型のステートフルファイアウォール機器に比べてコストパフォーマンスに優れ、ラックごとに設置することで単一障害点のリスクを解消、高スループットを実現するMicro Perimeterとして、データセンター内のラテラルムーブを最小限の範囲にとどめます。

・キャンパスおよびブランチへのゼロトラストに役立つソリューション群

既存環境を大きく変更せずにゼロトラスを実現するため、HPE Aruba Networkingではコアスイッチの横にHPE Aruba Networkingゲートウェイを設置し、エッジに展開しているAruba CXスイッチ・シリーズをはじめとしたアクススイッチや各種Wi-Fiアクセスポイントとの間でオーバーレイによるトンネルを確立することで新たな仮想ネットワークを構築、既存のVLANとは異なる新たなセグメントをシンプルに用意できます。そして、コントローラーやゲートウェイが持つステートフルファイアウォール機能によって、オーバーレイネットワークに接続されたエンドポイントごとにMicro Perimeterが用意されます。

また認証サーバのClearPassと連携し、アクセスする人の属性に応じてロールを割り当てて最小限のアクセスに範囲を絞るロールベースのアクセス制御を実現します。また、UTMやEDRといった3rd Partyのセキュリティ製品とClearPassが連携することで、セッションを維持しているClearPassが感染した端末を検疫用など別のセグメントに動的に移動させるダイナミックセグメンテーションを実現します。

Aruba Dynamic Segmentation で脅威を動的に隔離



HPE Aruba Networking Unified SASEで実現するVPN撤廃シナリオ

ランサムウェア対策として重要な非管理端末への対応ですが、もう一つ攻撃者が狙ってくる起点となってくるのが、ネットワーク上に設置されているVPN機器の脆弱性です。

・VPNのリスク

VPNは、テレワークを前提とした働き方に大きく舵を切った企業や関係会社を含めたグループ企業が自社のリソースへ安全にアクセスさせるために利用しているケースが多いのが実情です。設置されているVPN装置にアクセスさせ、社内にある各種セキュリティコンポーネントを経由させることで、安全なインターネットアクセスや社内リソース活用が可能になります。

しかし、VPNの脆弱性を悪用して内部に侵入され、ランサムウェアの攻撃を受けるケースが後を断ちません。つまりVPNは攻撃者の侵入経路となっているのです。また、全ての通信がVPNを経由させることで回線が逼迫し、生産性低下を招いてしまっているケースも少なくありません。そんな状況を改善するためには、アプライアンスであるVPN装置や回線の増強が必要で、大掛かりな投資が必要になるケースも。しかも、VPNを経由するとあらゆる社内リソースにアクセスできてしまうことでラテラムムーブのリスクを高めてしまう可能性もあるなど、理想的な環境とはいえません。

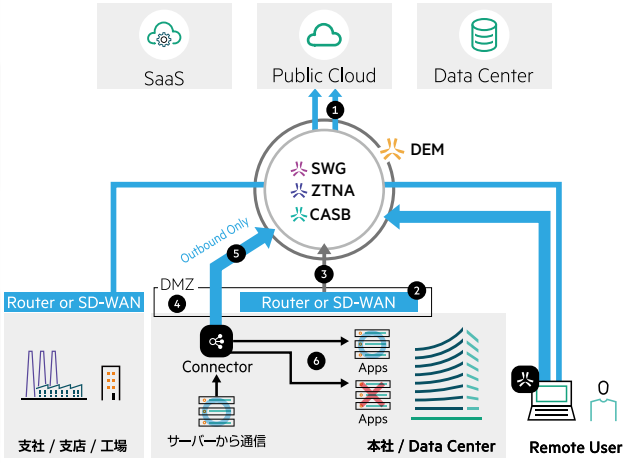
・VPN撤廃に効くZTNA

全方位ゼロトラストを実現するためには、このVPNによる課題に応える環境づくりも必要です。HPE Aruba Networkingでは、HPE Aruba Networking Unified SASEが備えているZTNAの機能で、既存VPNの課題を解決するソリューションを提供しています。

HPE Aruba Networking Unified SASEのZTNAでは、社内から

アウトバウンド通信だけを行うConnectorと呼ばれる小さなプログラムを立ち上げ、このConnectorとSASEのコンポーネントが通信を行うことで、リモートユーザーがデータセンター内のアプリケーションに安全にアクセス可能となります。VPN装置自体を撤廃させることができるため、ラテラルムーブのリスク回避につながるだけでなく、回線費用や機器増強のコストもかかりません。しかも、アプリケーション単位でのアクセス制御が可能なため、アクセスするユーザー属性に応じたMicro Segmentationへの展開も可能になります。

HPE Aruba Networking SSEのZTNAによる課題の解決

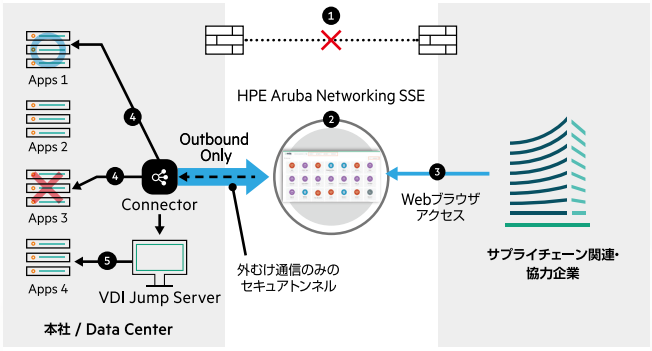


1. DCを経由しないセキュアで快適なアクセス（生産性向上）
2. VPN撤廃によるコスト削減
3. 回線縮小によるコストの最適化
4. アプライアンスのライセンスと管理コストの削減
5. 攻撃対象領域削減によるセキュリティレベル向上
6. アプリケーション単位でアクセス制御（ZTNA）

• サプライチェーンの協力会社や買収企業などからのアクセスには エージェントレス ZTNA が有効

このZTNAは、自社で管理しきれないグループ会社はもちろん、新たに買収してシステム統合ができてない買収先企業やサプライチェーン関連の協力企業が自社のリソースにアクセスする際にも有効です。HPE Aruba Networking Unified SASEのZTNAが提供するWeb上のポータル画面にアクセスし、アウトバウンド通信だけを行うConnectorとやり取りすることで、外部企業が必要なリソースだけにアクセスさせることができます。最小限のアクセスだけが許可されているため、VPNの脆弱性を狙った攻撃のリスクが回避できるだけでなく、ラテラルムーブ対策としても役立ちます。そして、エージェントレスで利用できることから、サプライチェーン全体にある非管理端末からのアクセスに対してもゼロトラスト環境が提供できるなど、全方位ゼロトラストへの大きな一歩が踏み出せます。

買収先企業、協力会社、関係会社からの安全なアクセス
エージェントがインストールできない環境にエージェントレスZTNA



1. 拠点間のネットワーク接続はなし
2. ポータルを提供
3. ブラウザベースのセキュアアクセスでポリシーを制御
4. アプリケーション単位でアクセス制御（ZTNA）
5. webだけでなくRDP、SSH、DB等のプロトコルをサポート

ネットワーク領域に強みを持ちながら、新たにSSE環境の提供も可能になったHPE Aruba Networkingだからこそ実現可能な全方位ゼロトラスト。非管理端末に対する備えも含めて、ぜひ一度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