HPE aruba networking

セキュアなSD-WANとSWGによってブランチのセキュリティを強化し、SASEの基盤を構築

今日、多くの企業のオペレーションにおいて、ブランチオフィスは重要な役割を担うようになりましたが、それに伴ってブランチオフィスが抱えるサイバーセキュリティ課題も増え続けています。クラウドベースアプリケーション、IoTデバイス、リモートワークの急増により攻撃対象が拡大した結果、これらのブランチ拠点はサイバー攻撃の格好の標的となっています。

HPE GreenLake

25%

統合型セキュリティ (次世代ファイアウォール、SWG、DPI、UTM、URLフィルタリングなど) がSD-WANの最重要機能だと考える回答者の割合[1]

150億台以上

2029年までにエンタープライズインフラストラクチャに接続されるIoTデバイスの数[2]

中央の企業ネットワークに重点を置く従来のセキュリティモデルでは、多様化と分散化が進む現代のブランチオフィスを保護するには不十分です。従来型ファイアウォールは管理が難しく、各拠点で専門知識が必要となります。分散した多数のブランチ拠点全体にセキュリティポリシーを適用する作業は複雑で時間がかかるため、セキュリティ対策の一貫性がしばしば損なわれます。

さらに、多くの場合、スタンドアロン型SWG (セキュアWebゲートウェイ) ソリューションには、管理対象/非管理対象のデバイスに同時に対応できる包括的なセキュリティ機能が備わっていません。ユーザーやデバイスが感染サイトに誤ってアクセスした場合、ランサムウェアやフィッシング攻撃の被害に遭うおそれがあります。ゲスト、請負業者 (第三者)、BYODなどの非管理対象デバイスは、エンタープライズ ネットワークに接続する過程で悪意のあるWebサイトにアクセスしてしまい、組織に新たな脅威をもたらす可能性があります。さらに、IoTデバイスは、AIモデルのトレーニング、更新、テレメトリ、その他の目的でクラウドサービスと通信するときにWebトラフィックを生成するため、Webベースの脅威に見舞われやすい傾向があります。

したがって、企業は、近代的なネットワークが持つダイナミックな性質に対応し、さまざまなサイバー脅威から身を守るため、ブランチオフィスの各拠点に総合的なセキュリティフレームワークを導入しなければなりません。

EdgeConnect SD-WANに組み込まれた次世代ファイアウォール

EdgeConnect SD-WANは、次世代ファイアウォール (NGFW)、侵入検知/侵入防止システム (IDS/IPS)、分散型サービス拒否 (DDoS) 防御などの高度なセキュリティ機能を統合することによって、ブランチ拠点が直面するサイバーセキュリティの課題に対応します。

- **NGFW**は、ハイレベルなトラフィック検査、マルウェアのブロック、アプリケーション、ユーザーID、およびコンテキストに基づくセキュリティポリシーの適用により、包括的な脅威保護機能を提供します。
- **IDS/IPS**は、ネットワークトラフィックを継続的に監視して疑わしいパターンを検出し、潜在的な脅威をブロックするためのアクションを自動的に実行する、シグネチャーベースのシステムです。このシステムは、インラインモードまたはパフォーマンスモードで動作させることができます。インラインモードでは、トラフィックはセンサーを通過し、侵入が起きた時点で即時にブロックされます。一方、パフォーマンスモードでは、トラフィックのコピーが送信され、分析されるため効率がアップします。ネットワークのパフォーマンスに影響が及ぶことはありません。
- **DDoS防御**は、プロトコル攻撃、ICMPフラッド、SYNフラッドなどのDDoS攻撃から組織を保護します。EdgeConnect SD-WANは、迅速なエージング、過剰なトラフィックのドロップ、ソースブロックにより、悪意のある要求を減らします。アクションは、フローレートや、同時フロー数、初期フロー数などのトラフィックパラメーターに設定されたDoSしきい値 (事前設定済みまたは構成可能) に基づいて実行されます。
- **脅威ログ機能**は、リアルタイムで脅威を監視できるように、ネットワークやセキュリティの分析をHPE Aruba Networking Centralまたはサードパーティ のSIEM (Splunkなど) に提供します。EdgeConnect SD-WANのSplunk用セキュリティアプリケーションは、企業のSD-WAN内のEdgeConnect SD-WANデバイスからエクスポートされたセキュリティイベント通知がすべて表示されるダッシュボードを備えています。

[1] Worldwide SD-WAN Infrastructure 2023 Vendor Assessment、IDC

[2] Gartner、2021年2月

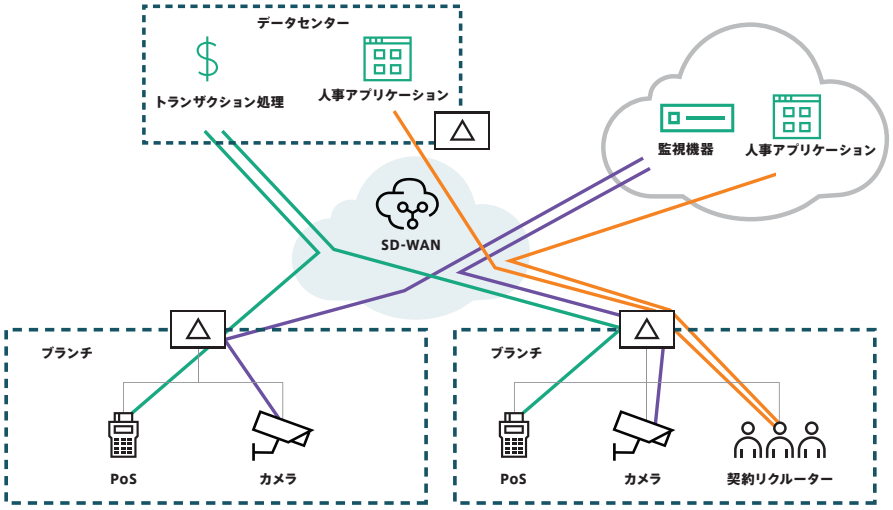
この統合により、お客様は従来のブランチファイアウォールを容易に置き換え、セキュリティポリシー管理を一元化し、各現場での技術的な専門知識を不要にすることができます。急速な拡張や堅牢なWANインフラストラクチャのようなケースでは、HPE Aruba Networking SSEのFWaaS機能がブランチ拠点に高度な保護を提供し、従来型のブランチファイアウォールを置き換えられるという点も重要なポイントです。

表1. HPE Aruba Networking EdgeConnect SD-WANの包括的なセキュリティ機能により、ブランチファイアウォールの容易な置き換えが可能に

機能	EdgeConnect SD-WAN
次世代ファイアウォール	✓
IDS/IPS	✓
DDoS防御	✓
ロールベースのセグメンテーション	✓
IoTのセキュリティ	✓
セキュリティイベントのログ作成	✓
SSEエージェントがインストールされていないSWG	✓
Unified SASE統合	✓

管理対象/非管理対象のすべてのデバイスを包括的に保護

HPE Aruba Networking ClearPassとEdgeConnect SD-WANの統合により、アイデンティティとロールベースのポリシーでアプリケーションインテリジェンスが強化され、ロールベースのセグメンテーションが可能になります。EdgeConnect SD-WANは、ロールベースのセグメンテーションにより、IoTなどの非管理対象デバイスのトラフィックをミッションクリティカルなアプリケーションから分離して、非管理対象デバイスを効果的に保護することができます。このようなセグメンテーションにより、攻撃に対して脆弱になりやすいIoTデバイスが、重要なビジネスオペレーションのセキュリティを損なうことがありません。さらに、EdgeConnect SD-WANは、EVPN/VXLANのオープンスタンダードを活用することで、複雑なマルチベンダーLAN環境においてもロール情報を伝送し、ファブリック全体にわたってロールベースのセグメンテーションを適用することができます。



ロールベースのセグメントテーションにより、ユーザーとデバイスは、確実に業務上の役割に一致する宛先のみにアクセスするようになります。

SWGによるWebベースの脅威からの保護

IoTを含むすべてのネットワークユーザーとデバイスをWebベースの脅威から全体的に保護するために、EdgeConnect　SD-WANをSWGで増強することができます。これにより、各デバイスにSSEエージェントをインストールする必要はなくなります。すべてのネットワークトラフィックが専用トンネル経由でHPE Aruba Networking SWGに転送されるようにすることによってこれを実現します。こうして、管理対象/非管理対象の両方のデバイスが同レベルで保護され、非管理対象デバイスも、管理対象デバイスと同様にWebベースの脅威から効果的に保護されるようになります。

HPE Aruba Networking SWGは、組織をWebベースの脅威から保護します。暗号化されたトラフィックを含むすべてのWebトラフィックを検査し、悪意のあるコンテンツを検出して有害なWebサイトへのアクセスをブロックします。このソリューションは、URL、DNS、コンテンツフィルター処理という3つのレイヤーによる保護と、暗号化されたHTTPSトラフィックのSSL復号化を組み合わせて使用します。ソリューションは、Webトラフィックをリアルタイムでスキャンし、マルウェアその他の悪意のあるコンテンツを検知、ブロックすると同時に、セキュリティポリシーを使用してアダルトコンテンツ、ギャンブルプラットフォームといった特定カテゴリのWebサイトや、重大なリスクをもたらすことが知られているサイトへのアクセスを制限します。また、DLPと組み合わせることによって機密データの漏洩を防止し、ユーザーのアクティビティを監視することもできます。

概要

ZTNAとCASBとの統合によりUnified SASEへと拡張

EdgeConnect　SD-WANは、SWGを追加することによって強固なサイバーセキュリティフレームワークの基盤を形成します。また、Zero Trust Network Access (ZTNA) とCloud Access Security Broker (CASB) の機能を統合することによって、包括的なSecure Access Service Edge (SASE) アーキテクチャーへのシームレスな拡張が可能です。

- **HPE Aruba Networking ZTNA**は、ユーザーのアイデンティティとコンテキストに基づいてすべてのアクセス要求の認証と認可を行います。ネットワークへの幅広いアクセスを提供する従来のVPNとは異なり、ZTNAは特定のアプリケーションやリソースへのアクセスを制限し、最小権限のアクセスを適用します。
- **HPE Aruba Networking CASB**は、SaaSアプリケーションでホストされている機密データの可視性と制御を提供し、セキュリティポリシーを執行するとともに、データ損失を防ぐことによって、SaaSアプリケーションのセキュリティを強化します。

メリット

- **包括的なゼロトラストセキュリティ**
- SD-WANとSWGの統合により、ネットワーク上のすべてのユーザーとIoTを含むデバイスをWebベースの脅威から保護する統合型セキュリティアプローチが実現します。内蔵型次世代ファイアウォールは、IDS/IPS、DDoS保護、ロールベースのセグメントテーションなどの機能でセキュリティレイヤーを追加し、全体的な保護フレームワークを強化します。

- **ハードウェアの設置面積を縮小し、運用を簡素化**
- 従来のブランチファイアウォールをEdgeConnect　SD-WANに置き換えることにより、ポリシー制御を一元化し、管理を簡素化することができます。このようなアプローチを取ることにより、ローカルレベルで技術的専門知識を持つ必要性は薄れ、ハードウェアとメンテナンスのコストが削減されるだけでなく、すべてのブランチ拠点で一貫したセキュリティポリシーが適用されるようになります。

- **Unified SASEへの移行を加速**
- お客様は、Unified　SASEアーキテクチャーへの移行を簡単に行うことができます。この統合的アプローチにより、セキュリティフレームワークが合理化され、シームレスな展開、統一されたセキュリティポリシー、一元管理、進化する脅威への適切な対処が実現します。

従来型ブランチファイアウォールを今すぐ置き換える

SWGが追加されたEdgeConnect　SD-WANは、IDS/IPS、DDoS保護、ロールベースのセグメンテーションなどの高度なセキュリティ機能を統合した包括的な次世代ファイアウォール機能を提供します。これらの機能を単一のソリューションに統合することによって、ネットワークセキュリティ管理が簡素化され、IoTを含むすべてのデバイスに対する保護が強化されます。このような統合的アプローチとゼロトラストセグメンテーションを組み合わせることにより、ネットワーク全体の強固なセキュリティが確保され、Unified　SASEアーキテクチャーへのシームレスな移行が促進されます。

最適な導入検討を。
HPEのプリセールススペシャリストに
お問い合わせください。

お問い合わせ

詳細はこちら

HPE Aruba Networking EdgeConnect SD-WAN

HPE Aruba Networking Unified SASE

セキュアなビジネス主導型SD-WANでSASEを構築

SWGを統合したセキュアSD-WAN: Unified SASEの基盤を構築

ArubaNetworks.com
にアクセス

Hewlett Packard Enterprise

AAG_Secure_SD-WAN_A4_SG_073024 a00141673JPN