ソリューションの概要

ダイナミック・セグメンテーション

有線 / 無線ネットワークを統一するシンプルでセキュアなアクセス

IoT デバイスの数が増え、ビジネスに不可欠なモビリティとクラウドサービスの使用がデジタル・ワークプレイスの革新を促進し、あらゆる種類のデバイスとユーザーをセキュアに接続できるほどスマートなネットワーク・エッジですか？従来の有線 / 無線ネットワークは、ビジネスに不可欠なモビリティ、IoT アクセス、またはセキュリティを念頭に置かずに開発されました。キャンパスおよびブランチ・ネットワーク全体に位置する、変化し続けるモバイル・デバイスや IoT デバイスに手動構成と静的構成を使用する今日のアプローチは、新しいセキュリティリスクを生み出し、IT チームが日常的に直面する面倒な作業となっています。

ネットワークをシンプルかつ保護するために、Aruba ダイナミック・セグメンテーションは、有線 / 無線ネットワーク間でポリシーの適用を統一し、トラフィックを安全かつ分離した状態に保ちます。IoT と IT で管理されるクライアント・デバイスを使用したビジネス向けの運用と企業管理ネットワークの共存が容易になり、ネットワーク・エクスペリエンスと IT 運用をエンド・ツー・エンドで最適化できるようになりました。

ダイナミック・セグメンテーションは、Aruba の基本的なロールベースのポリシー機能、ユーザー・ファイアウォールから収集されたインテリジェンスを、豊富なレイヤー 7 アプリケーションの可視性と統合された Web コンテンツ・フィルタリングと共に活用します。

主なビジネスおよび技術の推進要因

よりシンプルなポリシー管理

IoT およびクライアント・デバイスのオンボーディングには通常、複数のタッチポイントが必要でした。多くの場合、ネットワーク内のすべてのホップで新しい VLAN、ACL、またはサブネットを手動で構成する必要がありました。大規模な分散型ネットワークの継続的な移動、追加、および変更も、時間がかかり、エラーが発生しやすくなります。複雑さを軽減しながら、強力なセキュリティを備えたネットワークを設計することは、通常、相互に排他的です。

ユーザー・エクスペリエンスの向上

ユーザーは、どのデスクからでも、どの現場からでも、どこに接続するのでも、有線か無線かに関係なく、同じネットワーク・エクスペリエンスを期待します。仮想プライベート・ネットワーク (VPN) を使ってもらうとなると一苦労です。IT サポートを必要とするあらゆるネットワーク・エクスペリエンスは、マイナスと見なされます。従業員、ゲスト、買い物客、学生のいずれであっても、ユーザー・エクスペリエンスは組織の成功に影響します。スマートフォン、プリンター、ビデオ会議機器などの新しい種類のデバイスの接続は、多くの場合、IT の知識やサポートなしで行われます。IT は、セキュアなネットワーク上のすべての機能の可視性と管理を維持しながら、完璧なエクスペリエンスを提供することが期待されます。

スマート照明から監視カメラやバッジリーダーまで、あらゆる規模のネットワークに IoT デバイスが急速に導入されています。この新たに見出されたネットワーク接続は、多くの魅力的なメリットをもたらしますが、これらのデバイスが機密性の高い金融、医療、およびビジネスの重要なデータと同じ経路に便乗すると、ネットワークがセキュリティリスクにさらされます。これらのデバイスには、強力なセキュリティが内蔵されていることはほとんどなく、堅牢な認証もありません。パスワードはクリアテキストで保存され、安全なサプリカントがなく、多くの場合、誰でも立ち入れるエリアに放置されているため、ネットワーク侵害を誘発します。

主なメリット

- **より優れた一貫性のあるユーザー エクスペリエンス** - 無線ネットワークから有線ネットワークへのユーザーロール、ディープ・パケット・インスペクションの適用、デバイス・プロファイリング機能の拡張
- **よりシンプルなネットワーク運用** - SSID、ACL、サブネット、および有線ポートに必要な構成を削減することで、時間を節約し、VLAN のスプロールを排除
- **セキュリティとデバイスの可視性の向上** - ClearPass および Policy Enforcement Firewalls (PEF) により可視性とポリシーの適用を強化

ネットワークの脆弱性は、2020 年までに 200 億台を超える企業ネットワークに接続されている IoT/ ヘッドレス・デバイスの数によって明らかにされています。

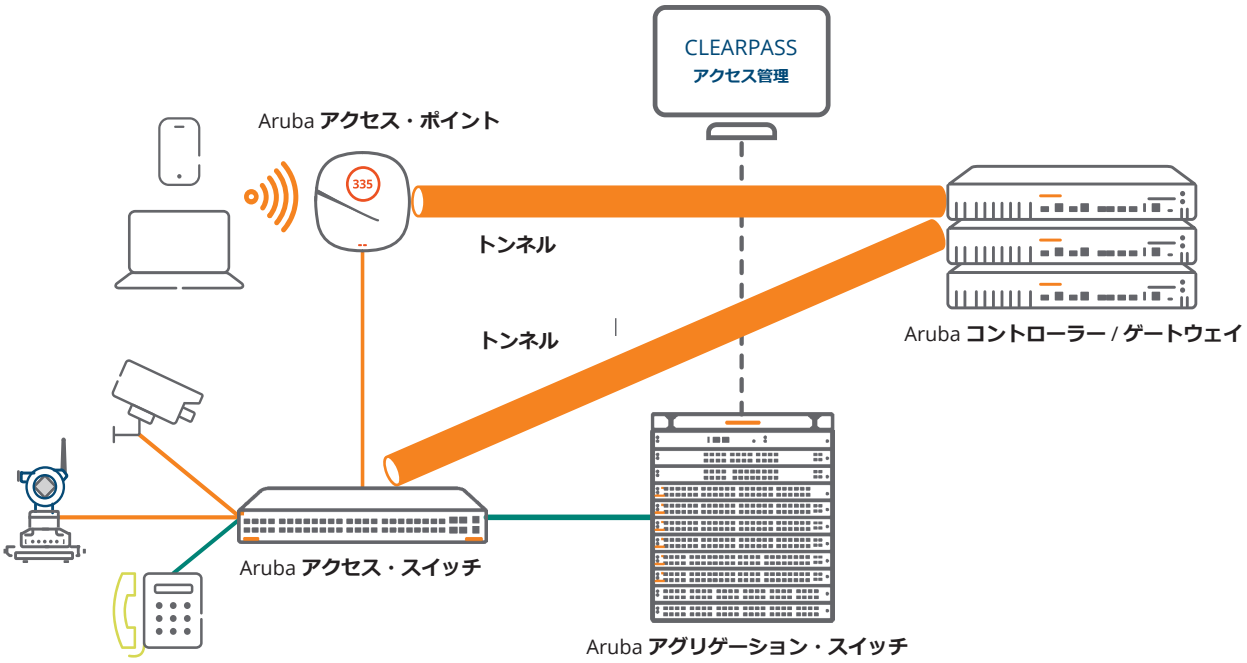
出典 : Gartner (2017 年 1 月)

スイッチングへの WLAN イノベーションの拡張

ダイナミック・セグメンテーションは、Aruba のセキュアなポリシー管理および WLAN ポリシー適用機能を拡張し、有線ネットワーク・アクセスをシンプルかつ安全にします。これにより、ポートまたはユーザーロールに基づいて有線クライアント・デバイスにポリシーを動的に割り当てることができます。IoT デバイスの数は 2020 年までに 200 億に達すると予測されていますので、これは非常に重要な機能です。Aruba ネットワーク・スイッチは、ポリシー管理用の ClearPass と、適用のためのモビリティ・コントローラーによってサポートされ、ネットワーク・アクセスの統合において重要な役割を果たします。

ロールベースのポリシー

ダイナミック・セグメンテーションを実施することにより、ロールベースのポリシーの決定とアクセス権は、デバイスの種類、使用されるアプリケーション、さらにはユーザーまたはデバイスの場所に基づいて行われます。もともと無線セキュリティに対応するために使用されていたロールベースのポリシーは、従業員、ゲスト、請負業者などのユーザーの種類別にネットワーク・トラフィックをセグメント化し、複雑で静的なネットワーク構成を排除することでネットワーク管理を大幅に簡素化しました。この強力な機能により、アクセスポリシーや BYOD ポリシーの管理などの IT ワークフローが合理化され、アプリケーションのパフォーマンスが向上しました。



ダイナミック・セグメンテーション、エクスペリエンス・エッジの一部

動的なロールベースのポリシー管理を無線 AP と有線スイッチに拡張することにより、モビリティ、IoT、クラウドのポリシーを管理および適用する根本的にシンプルで、セキュアでありながら別の方法が提供されます。ClearPass ポリシー定義を適用する Aruba のモビリティ・コントローラー / ゲートウェイは、ロールを動的に理解して利用できるようになりました。この機能により、ポリシーを動的に割り当てることで、複雑で静的な VLAN、ACL、およびサブネットを管理する時間がかかり、エラーが発生しやすいタスクがなくなります。

レイヤー 4 ～ 7 セグメンテーション

Aruba スイッチが活用する 2 番目の基本機能はセグメンテーションです。Aruba WLAN アーキテクチャは、アクセス・ポイントとコントローラーまたはゲートウェイ間のトンネルを使用して、トラフィックを安全に保ち、分離します。このトンネルベースのセグメンテーションは、Aruba の内蔵の Policy Enforcement Firewall (PEF) を使用して、リスクの高いトラフィックのファイアウォール・インスペクションなどのセキュリティを提供します。PEF は詳細なコンテキスト (ユーザー、デバイス、アプリ、場所) を提供し、最先端の検知と防御に対する高価なファイアウォールの必要性を軽減します。ID、デバイスの種類、および場所に基づくコンテキスト・ポリシーを使用すると、トラフィック・フローが割り当てられたロールに適応するだけで、単一のネットワーク構成を持つさまざまなユーザー・グループのニーズを満たすことができます。

この WLAN トンネリング・アーキテクチャを使用することで、Aruba スイッチは、従来、ローカル VLAN を手動で使用する必要があるのに対して、ロールベースのセグメンテーションアプローチを提供できるようになりました。これは、信頼性の低い IoT デバイスやアプリケーションの可視性を提供するのに最適です。Aruba スイッチは、選択したトラフィックを動的にトンネリングし、アクセス・ポイントと同様にディープ・パケット・インスペクションとデバイスの認証を行えるようになりました。例えば、監視カメラには、指定したサーバーのみにトラフィックを制限する権限を持つロールを動的に割り当てることができ、ネットワークの他の部分に悪意のあるアクセスの機会を排除できます。

この新しいセグメンテーション機能により、コントローラーで行われるすべての認証を使用して Port-Based Tunnelling (PBT) またはスイッチで認証を行う User-Based-Tunnelling (UBT) に設定できるトンネリングを使用して、セキュリティ・ポスチャが向上します。このセグメンテーションはオーバーレイとして動作するため、スイッチング・インフラストラクチャ全体のリッピングおよび交換が不要で、選択したエリアでセキュアなトンネルを使用することで、VLAN の実装と共存できます。

ダイナミック・セグメンテーションは、モビリティ・コントローラーを統一されたポリシー適用エンジンとして確立することで、有線 / 無線ネットワークをシンプルおよびセキュアにします。AP またはスイッチからのトラフィックは、ポリシー適用 FIrewall (PEF) による検査のために GRE トンネルにカプセル化されます。

ソリューションの構成要素

Aruba 無線アクセス・ポイント

802.11ac および 802.11ax Wi-Fi パフォーマンスは、あらゆる環境のニーズを満たします。内蔵の AI インテリジェンスと、ロケーション・サービスは、ユーザーと IoT デバイスに最適なエクスペリエンスを提供するために必要な自動化と可視性を IT に提供します。

Aruba ネットワーク・スイッチ

キャンパスおよびブランチ・ネットワークのスケーラビリティ、セキュリティ、高パフォーマンスを実現する、統合された有線 / 無線の統合基盤を開発します。ダイナミック・セグメンテーションにより、IT チームはポリシーを適用し、最先端のサービスを利用し、トンネルを介してネットワーク内の任意の場所で有線ユーザーと IoT トラフィックを安全にセグメント化する簡単な方法を IT チームに独自に提供します。そのトンネルは、コントローラー上で行われた認証で Port-Based Tunnel (PBT) を使用するか、Aruba スイッチで行われた認証で User-Based Tunnel (UBT) を介して使用します。

Aruba ゲートウェイとモビリティ・コントローラー

ソリューションの重要な部分として、コントローラーまたはゲートウェイは、有線トラフィックと無線トラフィックの両方のポリシー・エンフォーサーとして機能します。Aruba モビリティ・コントローラー (AOS 8.1 以降を実行) により、IT はポリシーの適用、帯域幅契約、その他のトラフィック制限を活用できます。ブランチ環境では、Aruba 一元管理 ブランチ・ゲートウェイがこの役割を実行します。ポリシー適用ファイアウォールは、これら 2 つの環境をサポートする基盤となるネットワーク技術として機能します。

プロファイリングを使用した Aruba ClearPass Policy Manager

無線および有線アクセス制御のネットワーク・アクセス・ポリシーを一元的に管理および適用します。その主な機能は、デバイスのプロファイリング、認証、承認とポリシーの適用です。ClearPass を使用して、役割と権限が定義されると、有線および無線アクセスを介してユーザーまたはデバイスに従います。そのため、ユーザーが不明なデバイスに変更され

た場合、またはセキュリティで保護されていないネットワーク上にある場合、ポリシーは自動的に承認権限を変更します。Downloadable User Roles (DUR) は ClearPass で構成されるため、スイッチで役割またはポリシーを定義する必要がなくなります。

まとめ

ビジネスに重要なモビリティと新たな IoT 接続要件をより適切に処理するために、Aruba の革新的なダイナミック・セグメンテーション・ソリューションは、IT 運用を簡素化し、統合ポリシーを動的に適用してセキュリティを向上させ、ネットワーク内の任意の場所に最先端のサービスを提供します。これにより、適切なアクセス・ポリシーとセキュリティ・ポリシーがシームレスに分散され、自動的に適用し、すべての無線および有線ユーザーおよびデバイスに対して個別の適用が実現します。

SO_DynamicSegmentation_SK_092419 a00058593enw