ソリューションの概要

ゼロトラスト・セキュリティ搭載 Aruba ESP

エッジのセキュリティ

ネットワーク・セキュリティにおける課題はここ数年著しく大きくなっています。多くのユーザーが広く分散している中で攻撃はより洗練され、持続的になっています。主にネットワーク境界に注力した従来のセキュリティ・アプローチは、スタンドアロンのセキュリティ戦略としての効果を失っています。モダンなネットワーク・セキュリティは、変化し続け、多様なユーザーやデバイスに対応し、ネットワーク・インフラストラクチャにおいて以前に「信頼された」エリアをターゲットにする流行の脅威にも対応する必要があります。

「ゼロトラスト」は、 モダンな企業の変わり続けるセキュリティ要件に応える効果的なモデルとして誕生しました。すべてのユーザー、デバイス、ネットワークセグメントを本質的に安全でなく、悪意のある可能性があるものとしてとらえるモデルです。ゼロトラスト・セキュリティ搭載 Aruba ESP は、過去に信頼されたネットワーク・リソースに厳格なセキュリティ・ベストプラクティスと制御を提供し、ネットワーク・セキュリティ・ポスチャ全体を改善します。

ARUBA ESP: ゼロトラストの主要原則

ゼロトラストは、考慮されるセキュリティ分野により大きく変わります。ゼロトラスト内ではアプリケーションレベルの制御が焦点となりますが、総合的な戦略は、在宅勤務の環境含めネットワーク・セキュリティや、増え続ける接続デバイスの数も考慮する必要があります。ゼロトラスト・セキュリティ搭載 Aruba ESP は、総合的な可視性、限られたアクセスのみを許可するマイクロセグメンテーションと制御、継続的な監視とポリシー適用を提供します。従来の VPN ソリューションも、同様の制御をキャンパスまたはブランチ・ネットワーク、さらには自宅またはリモート・ワーカーにまで広げて適用することにより強化されます。

IoT の時代では、適切なネットワーク・セキュリティの基本原則を導入するのはしばしば困難です。可能な場合、すべてのデバイスとユーザーは、ネットワークへのアクセスが提供される前に識別され、適切に認証される必要があります。認証に加え、ユーザーおよびデバイスはネットワーク接続時に、業務において必要とされる作業を行うために最低限必要なアクセスのみが提供されるよう設定されなければなりません。つまり、特定のユーザーまたはデバイスがアクセスできるネットワーク・リソース/アプリケーションを承認することです。最後に、エンドユーザーとアプリケーション間のすべての通信は暗号化される必要があります。

総合的な可視性へのニーズ

IoT の導入が進むにつれ、ネットワーク上のすべてのデバイスとユーザーの完全な可視性が重要な課題となってきます。可視性がなければゼロトラスト・モデルを支える重要なセキュリティ制御は適用するのが困難になります。自動化、AI ベースの機械学習、デバイスの種類の迅速な識別は重要です。

Aruba ClearPass デバイス・インサイトは、アクティブな検出方式とパッシブな検出方式の両方とプロファイリング技術を組み合わせ、ネットワークに接続している、または接続しようとしているデバイスをすべて検出できます。これにはノート PC やタブレットといった一般的なユーザーベースのデバイスが含まれますが、従来のツールと異なる点は、今日のネットワークで広く普及している実にさまざまな IoT デバイスを検出できることです。

「最小限のアクセス」とマイクロセグメンテーションの採用

可視性の次は、「最小限のアクセス」とマイクロセグメンテーションに関連したゼロトラスト ベストプラクティスが重要なステップです。ネットワーク上の各エンドポイントに最適な認証方法 (例: 完全な 802.1X、ユーザー・デバイス用多要素認証) を使用し、接続するデバイスまたはユーザーにとって本当に必要なリソースへのアクセスのみを承認するアクセス制御ポリシーを適用することです。

Aruba ClearPass Policy Manager により、IT やセキュリティ・チームが、有線または無線インフラストラクチャ、ブランチまたはキャンパスであれ、ネットワークのあらゆる場所に適用される単一のロールと関連付けられたアクセス権限を使用してこれらのベストプラクティスを実行できるようなロールベースのアクセス・ポリシーが作成できます。デバイスのプロファイリングが完了すると自動的に適切なアクセス制御ポリシーが割り当てられ、Aruba のダイナミック・セグメンテーション機能により他のデバイスと分離されます。ポリシー適用は、Aruba のポリシー・エンフォースメント・ファイアウォール (PEF) により提供されています。Aruba ネットワーク・インフラストラクチャに組み込まれた完全なアプリケーション・ファイアウォールです。また、Aruba インフラストラクチャは、無線ネットワーク接続上で WPA3 規格といった最もセキュアな暗号化プロトコル使用しています。

ClearPass Policy Manager は、多要素認証の使用と、ネットワーク上の主要ポイントで再認証を要求する機能を可能にする、さまざまな認証ソリューションとも統合しています。ClearPass エコシステムにより、お客様は、コンテキスト情報やその他のセキュリティ・テレメトリに関連したゼロトラスト要件に適合するためにその他のソリューションを簡単に組み込むことができます。

これにより ClearPass は、エンドポイント・セキュリティツールといったさまざまなソリューションと統合でき、デバイスのポスチャに基づいてよりインテリジェントなアクセス制御の判断を行うことができます。また、アクセス制御ポリシーも、使用されているデバイスの種類、ユーザーがどこから接続しているか、その他のコンテキストベースの条件に基づいて変更できます。

継続的な監視とポリシー適用

グラニュラー・セグメンテーションを実行するためのロールベースのアクセス制御と共に、ネットワーク上のユーザーやデバイスの継続的監視もゼロトラスト ベストプラクティスです。これは、インサイダー脅威、高度なマルウェア、従来の境界防御を回避するしつこい脅威に関連したリスクに対処するものです。

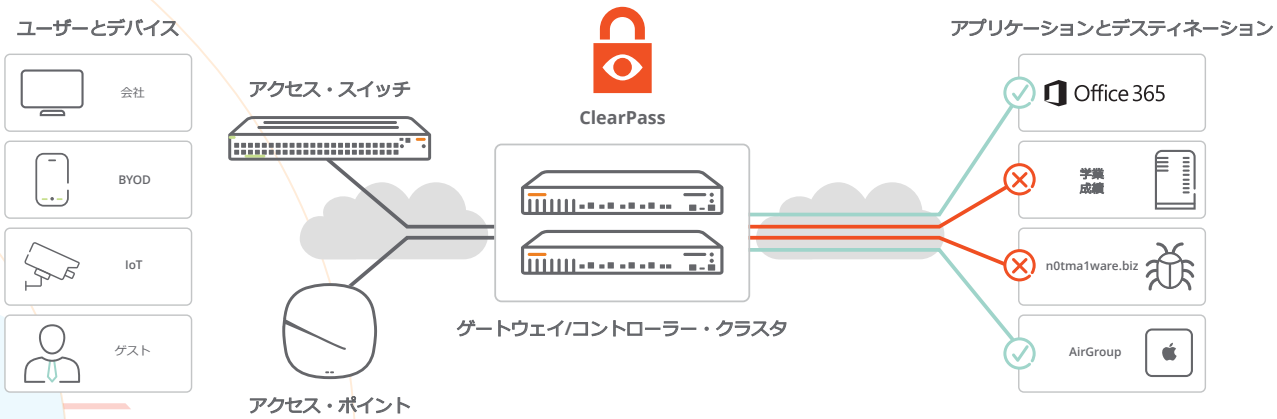

図1：Aruba ClearPass はダイナミック・セグメンテーションを使用して実行されるロールベースのアクセス制御ポリシーを自動的に割り当てます

図2：ゼロトラスト・セキュリティは Aruba ESP の主要な要素です

IDS/IPS による脅威の保護

Aruba の脅威防御機能は、フィッシング、サービス拒否 (DoS)、大きく広まっているランサムウェア攻撃など無数の脅威から守ります。Aruba 9000 SD-WAN ゲートウェイは、Aruba Central、ClearPass Policy Manager、ポリシー・エンフォースメント・ファイアウォールと共に、アイデンティティベースの侵入検出と防御 (IDS/IPS) を実行します。アイデンティティベースの IDS/IPS は、ゲートウェイを通過するブランチ・オフィス LAN (East-West) トラフィックや SD-WAN (North-South) トラフィックで署名/パターンベースのトラフィック検査を実行し、内蔵ブランチ・ネットワーク・セキュリティを提供します。Aruba Central 内の高度なセキュリティ・ダッシュボードは、IT チームにネットワーク可視性、マルチディメンションの脅威メトリクス、脅威インテリジェンス・データ、相関、インシデント管理を提供します。脅威イベントは SIEM システムと ClearPass に送信され、修復が行われます。

360 Security Exchange

クラス最高のセキュリティ・ソリューションで構成された 150 以上の統合機能と共に ClearPass Policy Manager は、複数のソースからのリアルタイムの脅威テレメトリに基づいてアクセスを動的に実行できます。ポリシーは、次世代ファイアウォール (NGFW)、セキュリティ情報およびイベント管理 (SIEM)、その他の多くのソースからのアラートに基づいてリアルタイムのアクセス制御を決定するために作成できます。ClearPass アクションはアクセスの制限 (例: インターネットのみ) から、修復目的でのネットワークからのデバイスの完全削除まで完全に構成可能です。

ARUBA ESP (エッジ・サービス・プラットフォーム)

お客様がエッジでのエクスペリエンス向上への投資を活用できるよう、Aruba は、エッジの統合、自動化、保護のために設計された、業界初の AI 応用プラットフォームである Aruba ESP を開発しました。ゼロトラスト・セキュリティは Aruba ESP の主要要素であり、AIOps や統合インフラストラクチャと組み合わせて、企業がコスト削減、オペレーションの簡素化、保護を実現できるようサポートします。

まとめ

今日のネットワーク環境と脅威ランドスケープには新しいアプローチが必要です。過去の境界中心のネットワーク・セキュリティは今日のモバイル・デバイスおよびそれらを使用するユーザー、または昨今広まりつつある IoT デバイスに適していません。ゼロトラスト・セキュリティ搭載 Aruba ESP は、分散された IoT 主導のネットワーク・インフラストラクチャの要件に応えるために可視性、制御、ポリシー適用を展開する総合的な機能コレクションを備えています。

a Hewlett Packard Enterprise company

SO_ZeroTrustSecurity_051120 a00097694enw