エグゼクティブブリーフ

エッジにおけるモバイルとIOTの特定、接続、および保護

はじめに

非常に多くの IoT デバイスがエンタープライズネットワークに接続される中、IT 部門はスマートビルディングのメリットを実現しつつ、多数の未知のデバイスの特定、プロファイリング、認証、およびポリシーの適用を自動的に行う適切なツールセットを持たないまま、自社の環境にそれらのデバイスを導入するリスクに対処しなければならないという課題に直面しています。

Aruba が発表した最新のソリューションは、エッジでの IoT の接続に対する 4 段階のアプローチ (ネットワーク上のデバイスの特定、インテリジェントスイッチによるモバイルおよび IoT デバイスの接続、業界をリードするポリシー管理機能によるネットワークの保護、パートナーエコシステムを活用したエンドツーエンドのセキュリティのイノベーション) でこうした課題に対応します。

多くの課題をもたらすIOT

モバイルデバイスが急増し、スマートビルディングへの移行が進む中、IT およびビジネス部門のリーダーには大きな課題がもたらされています。

可視性の欠如—ネットワーク上のデバイスを本当に把握できているか

セキュリティを確保するには、まず管理対象外のスマートフォン、不正なエンドポイント、IoT デバイスなどを含む、ネットワーク上のデバイスを把握する必要があります。こうしたデバイスは攻撃対象を増やし、エンタープライズセキュリティを脅かす原因になりますが、ネットワーク上のデバイスを確認する機能により、IT 部門はネットワークがどのような方法で、何によって使用されているのかをより詳細に把握できるようになります。IT 部門には、接続元にかかわらず、ネットワークに接続しているすべてのデバイスを特定してプロファイリングできることが求められますが、未知の有線 / 無線 IoT デバイスであふれる今日のネットワークでは、そうした処理が難しくなりつつあります。とは言え、すべてのデバイスは接続時にプロファイリングとアセスメントを行い、特定のカテゴリに割り当てるとともに、デバイスの種類、所有権のステータス、またはオペレーティングシステムに基づいて、自動的にアクセス権限を付与するか、アクセスを拒否する必要があります。

新たな課題をもたらす有線ネットワーク

各企業や業界の組織では、業種により動作感知装置、医療機器、工場内のプロセス制御装置など、必要とされている有線 IoT デバイスの数は、35% ～ 50% 超までと実にさまざまです。これまで、ネットワークアクセス制御 (NAC) に関する議論は主に、大部分のデバイスが接続される無線ネットワークのセキュリティを確保する方法を中心に展開されてきましたが、無線を傍受した未知のユーザーが、アクセスポイントの範囲内で非セキュアな SSID を使用して、あらゆる場所からアクセスを確立できるようになったことから、セキュアなセッション単位の接続が必須となりました。

このように、無線ネットワークのセキュリティの確保に重点が置かれると同時に、スイッチが安全な場所に設置されていることもあり、有線ネットワークは保護されてきませんでしたが、無線と同じような脆弱性の問題が発生することはないと考えられていました。しかし、有線ネットワークの増加に伴って多くのスイッチの一貫性が失われ、ポートが誰にでも使用できる開かれた状態になってしまいました。会議室やプリンターエリアのポートは、「ずさんな」セキュリティが存在する典型的な例であり、多くの IoT デバイスが有線接続される今日では、有線インフラストラクチャのセキュリティの確保にも同等の注意を払わなければなりません。

従来の有線インフラストラクチャはIoT向けに最適化されていない

従来のスイッチング環境では、従業員はモバイルを使用しておらず、IoT もまだ登場してはいませんでした。また、ファイアウォールや IT 環境の背後にあるアセットで境界のセキュリティを維持する必要がありました。しかし IoT の登場に伴って、今では有線インフラストラクチャにも無線インフラストラクチャと同様の高度な機能が求められるようになり、今日のスイッチには、すべてのデバイスを安全かつシームレスに接続できるよう、セキュリティと高度なネットワーク管理機能を組み込まなければなりません。

ネットワークを保護するにはワークフローの自動化が必要

毎日のようにエンタープライズネットワークに未知のモバイルおよび IoT デバイスが多数接続される今日では、各デバイスを管理するためのポリシーの割り当てと適用を手動で行うことはできないため、そうしたプロセス全体を自動化して現場での IT 部門の関与を最小限に抑え、リスクを軽減する必要があります。また、固定のデバイスとインフラストラクチャ自体についても、プロファイリングと自動チェックによって不審な変更を確認し、デバイスが不審な動きをしているのであれば、脅威を評価する前にそのデバイスを自動的に隔離しなければなりません。

ハッカーの一歩先を行くには膨大なコストが必要

私たちはほぼ毎日のように大規模なデータ漏洩があったことを耳にしますが、企業がセキュリティに投資するにあたっては、膨大なコストと時間がかかり、イノベーションだけでハッカーの一歩先を行くことはほとんど不可能です。Aruba のパートナーエコシステムは、最高のセキュリティパートナーが連携し、エンドツーエンドのセキュリティソリューションを提供することを目的に設計されています。

エッジでのセキュアなIOT接続に関するARUBAのブループリント

1. マルチベンダーの有線/無線ネットワークにおける未知のデバイスの特定とプロファイリング

ネットワークのセキュリティを確保するにはまず、ネットワーク上のデバイスを把握する必要があるため、組織にはすべてのデバイスを特定し、プロファイリングできる能力が不可欠です。Aruba の ClearPass ファミリは、スタンドアロンのアプライアンスとして、または包括的

なポリシー適用ソリューション内でエージェント不要のリアルタイムプロファイリング機能を使用できるという、競合製品にはない独自のメリットを備えています。

どちらのソリューションでも、動的または静的 IP アドレスを使用して、AAA 非対応もしくは AAA 対応の有線 / 無線ネットワークでエンドポイントやネットワークデバイスを継続的に特定することが可能で、包括的なダッシュボードにより、エンドポイントの総数とカテゴリ、ファミリ、およびデバイスの種類別の台数を簡単に確認できます。

新しい Aruba ClearPass Universal Profiler は、数分で配備して実行できるスタンドアロンの仮想アプライアンスで、NAC ソリューションを完備していない組織や NAC が配備されていないリモートエリア、または制限のあるエリアに合わせた設計となっています。Universal Profiler を使用すれば、ネットワーク上のデバイスをシンプルかつコスト効果の高い方法で特定およびプロファイリングできます。

Aruba ClearPass Policy Manager は、包括的なプロファイリング、AAA 非対応および AAA 対応の有線 / 無線ネットワークのポリシーの適用、ゲストアクセス、BYOD の導入、エンドポイントアセスメント機能、レポート、およびサードパーティのセキュリティとユーザーエクスペリエンスに重点を置いた組み込みのソリューション統合機能をサポートする、仮想 / 物理アプライアンスです。

2. 自動インテリジェンスによるIoTデバイスの接続

スマートビルディングへの移行が進む中、今日のビジネスではより高度な有線インフラストラクチャが必要とされています。ArubaOS およびスイッチの最新の機能強化は、インテリジェントエッジのパフォーマンスとセキュリティを強化し、モバイル /IoT デバイス向けに最適化する設計となっています。これらの機能強化を活用すれば、ビジネスクリティカルなアプリケーションの優先順位を決定してネットワークのセキュリティを確保するために、接続している IoT デバイスの特定と役割の割り当てを行い、無線 / 有線ネットワークにわたる役割ベースのアクセスを一元的に管理できます。

また、Aruba のレイヤー 3 スイッチは、ポリシーを適用して高度なサービスを拡張し、トラフィックの暗号化で LAN を保護できるよう、モビリティコントローラーへのユーザー / ポートベースの有線トラフィックのトンネリングにも対応しています。コスト効果の高い Aruba 2540 (およびその他の Aruba スイッチ) は、分散型企業で急増する IoT デバイスや接続デバイスのニーズに対応するため、ネットワークの配備と管理を簡素化し、それらに必要なコストを削減できる、Zero Touch Provisioning とオプションのクラウドベース管理機能をサポートしています。

3. 高度なポリシーによるネットワークの保護

デバイスを可視化したら、ポリシーの自動適用が可能になります。Aruba ClearPass Policy Manager を使用すれば、ネットワーク上のデバイスを確認してから、マルチベンダーの有線 / 無線ネットワークにわたってポリシーを適用し、それらのワークフローを自動化できます。ClearPass は、プロファイリング、ポリシーの適用、ゲストアクセス、BYOD の導入などをサポートし、IT 部門の負荷を軽減して強力な脅威保護機能を提供するとともに、シームレスなユーザーエクスペリエンスを実現します。また、新たに有線インフラストラクチャのセキュリティの確保に重点を置いた OnConnect 機能は、既存のスイッチプロトコルを使用して、会議室、IP 電話、プリンターエリアなどの攻撃を受けやすい場所にある有線ポートのロックダウンをサポートします。

4. イノベーションの促進によるエッジのセキュリティの強化

Aruba のテクノロジーエコシステムには、ClearPass Exchange との統合により、エッジとコアでエンドツーエンドのセキュリティを確保する、業界屈指のセキュリティソリューションが含まれています。Aruba のエコシステムには最近、IoT のセキュリティに重点を置く次のようなパートナーのソリューションが追加されました。

- Niara は、デバイスの種類と関連付けた既知のトラフィックパターンを使用して不審な挙動を特定し、ネットワークからのデバイスの排除を ClearPass に求めます。
- Attivo により、IT 部門は「偽の仮想」IoT デバイスを作成して、偽のデバイスからネットワークに攻撃を仕掛けようとするユーザーを特定できます。仮想デバイスで望ましくない挙動が検出されたら、Attivo は ClearPass にネットワークからのデバイスの排除を求めます。

結論

IoT を本格的に運用する組織が増える中、IoT デバイスの適切な導入と管理が成功の実現に不可欠となりつつあり、多くの企業がネットワークと自社のアセットを保護しながら、エッジでモバイルおよび IoT デバイスを安全に接続し、スマートビルディングから価値を引き出して効率化を図るための戦略を必要としています。IoT の接続に対する Aruba の 4 段階のアプローチは、ネットワーク上のデバイスの特定、高度な有線 / 無線インフラストラクチャによるデバイスの接続、ポリシー管理の自動化によるネットワークの保護、および潜在的なリスクに先手を打つための、パートナーエコシステムを活用したエンドツーエンドのセキュリティの強化におけるさまざまな課題に対応します。

a Hewlett Packard Enterprise company

1344 CROSSMAN AVE | SUNNYVALE, CA 94089
1.844.473.2782 | 電話: 1.408.227.4500 | ファクス: 1.408.227.4550 | INFO@ARUBANETWORKS.COM

www.arubanetworks.com