技術概要

動的セグメンテーションのためのポリシー・エンフォースメント・ファイアウォール

企業ネットワークがデジタル変革の触媒となり、いたる所で接続できるようになるにつれて、従来のネットワークおよびセキュリティの担保に対する課題に対処するために、新しいポリシー実施とサイバーセキュリティ・ソリューションが必要になってきます。IoT デバイスが従業員、顧客、ゲストを、絶え間なく変化する境界内にある企業の無線および有線ネットワークに結び付けています。IP アドレスを利用した規則や物理的ネットワーク構成を使用するファイアウォールなどの標準的な防御は、もはや適切ではありません。

ポリシー・エンフォースメント・ファイアウォール (PEF)

内部への新しい攻撃は、従来のセキュリティ防御を回避してつけ込むように設計されています。多くの場合、ネットワークに数週間または数か月とどまり、データの抽出、致命的なデータ暗号化、またはまったく想定外の IT リソースの侵害を行います。同時に、IT はアプリケーション層の可視性がないため、ネットワーク・パフォーマンスとエンドユーザー・エクスペリエンスに直接影響します。

有線および無線のネットワーキングのリーダーとして、Aruba, a Hewlett Packard Enterprise company は、軍事レベルの暗号化とポリシー・エンフォースメント・ファイアウォール (PEF) と呼ばれる特殊な ID ベースのアクセスソリューションを含む包括的なエッジベースのサイバー保護の使用に初めて着手しました。PEF は ArubaOS および InstantOS で動作し、**世界中の 400 万を超えるインストールで実行される**実証済みテクノロジーです。アクセス・ポイントで「ゼロトラスト」境界を提供する、唯一のユーザーおよびデバイス中心のファイアウォールです。

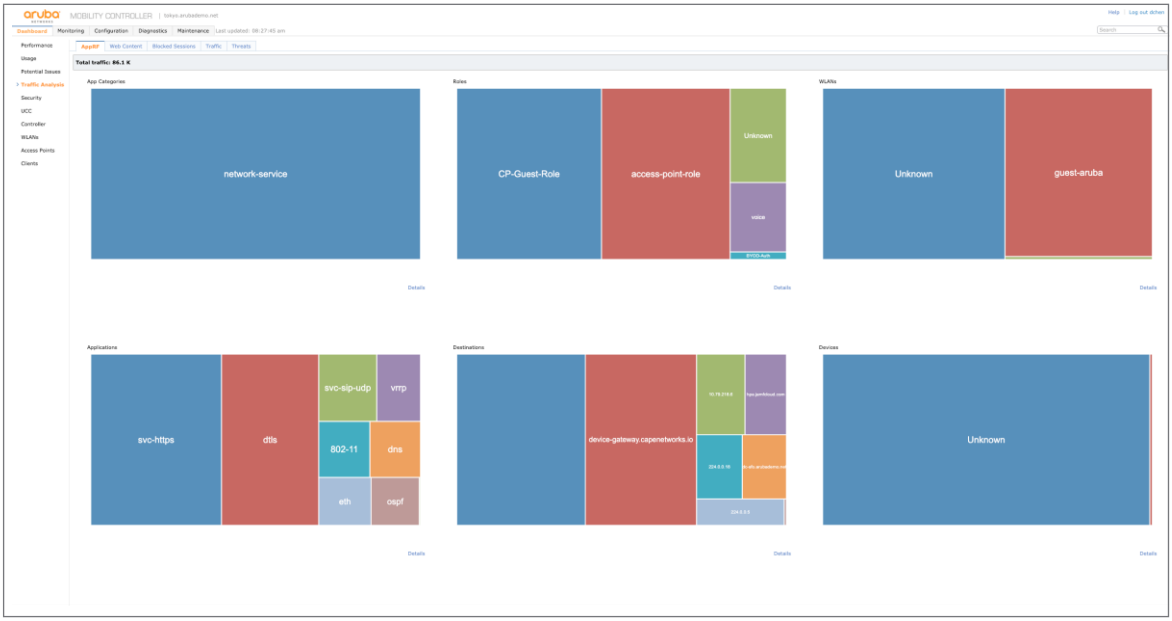
IP ベースの VLAN を制御に使用し、ユーザーやデバイスがネットワークに認証されないと有効にならない従来のファイアウォールは、高度な攻撃の格好の対象になってしまいます。代わりに、PEF を使用した Aruba のユーザーおよびアプリケーションファイアウォール方法は、ID、トラフィック属性、およびその他のセキュリティコンテキストを使用してこの脆弱性をカバーし、初期接続時にアクセス権限を集中制御します。1 秒ごとに攻撃者がネットワークに接続して何千ものマルウェアパケットを解き放つことを意味する場合、このギャップを埋めることは不可欠です。

主なメリット

- **一元的ゼロトラストアクセス:** 初期ネットワーク接続と従来のファイアウォールの実施の間のギャップを埋めます
- **Marsh による Cyber Catalyst℠:** PEF のリスク軽減機能により、選ばれた保険会社のより手厚いサイバー保険契約条件の認定を支援します
- **ユーザー/アプリケーションファイアウォール:** ロールベースのアクセス制御により構成エラーを最小限に抑えます
- **追加ハードウェア不要:** PEF は既存の Aruba ネットワークインフラストラクチャで実行されます
- **向上したパフォーマンス:** ハードウェアトラフィック加速処理機能搭載
- **自動自己学習:** 洞察に富んだネットワークおよびアプリケーション用途データを提供します
- **再利用可能なポリシー・ライブラリ：**便利で一貫的なポリシーを管理者が簡単に作成できるようにします
- **個別の接続:** ロールは、有線、無線、およびリモート接続全体でユーザーとデバイスに追随します
- **セキュリティ認定:** 行政機関がスポンサーを務める検証全範囲

CYBER CATALYST℠ 指定ソリューション

Aruba のポリシー・エンフォースメント・ファイアウォールテクノロジーを使用する組織は、ID やトラフィック属性、その他のコンテキストを使用して、初期接続時にアクセス権限を集中的に実施するゼロトラスト・アクセスモデルを実装できます。安全なロールベースのポリシーを動的に実施する技術と能力のため、Aruba ポリシー・エンフォースメント・ファイアウォールは、効果的にリスクを軽減する能力があるとして「Cyber Catalyst℠」に指定されました。



ArubaOS のダッシュボード・ビュー: 3000 を超えるアプリケーションへの高度な可視性

シンプルかつセキュアなネットワークアクセス

PEF は、有線および無線ネットワークを簡素化して保護する Aruba のエクスペリエンス・エッジの主要な技術ソリューションである動的セグメンテーションを可能にする基盤技術でもあります。ユーザーとアプリケーションの制御により、IT 部門は VLAN や SSID、ACL の追加を不要にし、複雑さを劇的に軽減できます。

PEF のアプリケーション可視化機能により、ネットワーク管理者は、ネットワークで実行されているアプリケーション、およびそれらを使用しているユーザーに関する豊富な洞察を得ることができます。WebCC は、URL フィルタリング、IP レピュテーション、ジオロケーション・フィルタリングを含む PEF を向上させるサブスクリプションベースのアドオン機能です。

ゼロトラスト保護のための認証強化とロールベースの制御

まず、ネットワーク上のサインオン処理中に、Active Directory (AD)、RADIUS、LDAP、SQL データベース、LDAP を利用している ID ストアやゲストデータベースとの統合により、各ユーザーまたはデバイスの ID が認証されます。ID が認証されると、ロールが割り当てられます。ロールとは、アプリケーションのアクセス権限とユーザー間やデバイス間の通信を含むアクセス許可の論理的グループです。

ユーザーをロールに関連付けることができるようにすると、ユーザーのセキュリティコンテキストが変更された場合 (たとえば、デバイスが侵害された場合)、ネットワークを再構成することなく、より制限の厳しい新しいロールを割り当てるだけでアクセス許可をすぐに変更できます。

ユーザーまたはデバイスのロールが割り当てられると、組織の保護優先度に基づいてポリシーが適用されます。これらのポリシーはネットワーク全体でユーザーに追随し、無線、有線、VPNのどの接続にも均等に適用されます。デバイスがディレクトリに登録されていない場合、指紋認証デバイスに基づいたデフォルトポリシーを適用できます (例: 「すべてのテレビ画面には、DNS、DHCP、およびインターネットを利用した HTTPS サービスへのアクセス権限が与えられますが、内部リソースへのアクセス権限は与えられません」)。

PEF で制御されたアクセスネットワークに接続している認識されたユーザーには、最初にロール (「病院の人事マネージャー」など) が割り当てられ、一連の IT 権限が付与されます。この場合管理者は、業務に必要なツールとネットワークサービス、つまり電子メール、Microsoft Office、従業員記録のみにはアクセスできますが、患者の医療情報にはアクセスできません。ユーザーが侵害された場合、新しいロール (「潜在的な侵害、隔離部に送信」)が自動的に適用され、実施されます。

その結果 PEF は、VLAN 構成を決定および変更するという、骨の折れる、手動で、エラーが発生しやすいやり方が排され、正確かつリアルタイムで実施できます。

また、PEF はディープ・パケット・インスペクションを利用しているため、**レイヤー 7 アプリケーションの認識と 3,000 のアプリケーション特定機能も併せ持ちます**。その結果、トラフィックの分離は、特定の単一アプリケーションの単一のユーザーまたはデバイスと同じくらい細かくできます。これは、VLAN ベースの方法ではできない手法です。

アプリケーションの優れた可視性

ディープ・パケット・インスペクション (DPI) によるアプリケーションの優れた可視性は、アプリケーション・パフォーマンスのリアルタイムでのトラブルシューティング、グローバルポリシーの設定、将来的な拡張の計画に利用できます。

内蔵ダッシュボードは、携帯アプリの使用状況とパフォーマンスに関するシンプルで強力なビューをロール別、アプリケーション別、ネットワーク別、その他の区分基準で IT 部門に提供します。

- **携帯アプリ:** Box などの企業向けアプリケーションと Apple FaceTime などの個人向けアプリケーションを同じ携帯デバイスで実行している場合でも、両者を区別します。
- **Apple AirPrint/AirPlayなどのネットワーク・サービス：**Arubaは、IPマルチキャスト動画トラフィックを最適化してサービスに自動的に優先度を設定し、ポリシー制御を適用します。
- **Webベース・アプリケーション：** Webベースのアプリケーションの多くは、クライアントとの通信に同じポートを使用しており、そのトラフィックはHTTPトラフィックのように見えます。Aruba のテクノロジーは、宛先アドレスを解決して、Facebook、Twitter、Box、WebEx や、数百の個別アプリケーションを特定します。
- **暗号化されたアプリケーション：** 暗号化されたトラフィックの場合、Aruba はヒューリスティックを使用してトラフィックパターンを探し、固有フィンガープリント認証でそれらのアプリケーションを識別します。

ポリシーベースのトラフィックの管理と制御

PEF 機能は、トラフィック使用率を最適化する制御機能を備えています。ロールベースのポリシーによって特定のユーザーまたはクラスに対して最大使用帯域幅を設定できるため、パワー・ユーザーによるネットワーク・リソースの独占を防ぐことができます。

同時に、トラフィック管理ポリシーによってデバイスに最小限の帯域幅を保証することで、ユーザーの生産性を維持できます。PEF は、パフォーマンスを奪うブロードキャストおよびマルチキャストトラフィックを最適化し、アプリケーションのパフォーマンスを向上させます。

mDNS、ARP、NetBIOSブロードキャストなど、帯域幅を多用する他のプロトコルについては完全にフィルタリングし、その使用をネットワークの特定の領域に限定することができます。

さらに、PEFは総合的なオンライン脅威インテリジェンスを提供し、ユーザーとネットワークを悪意のあるファイルとURLからリアルタイムに保護します。ポリシーは、URLフィルタリング、IPレピュテーション、ジオロケーション（WebCCサブスクリプション）のほか、ユーザー・ロールやデバイス・コンテキストに基づいて適用できます。

サービス制御機能の品質

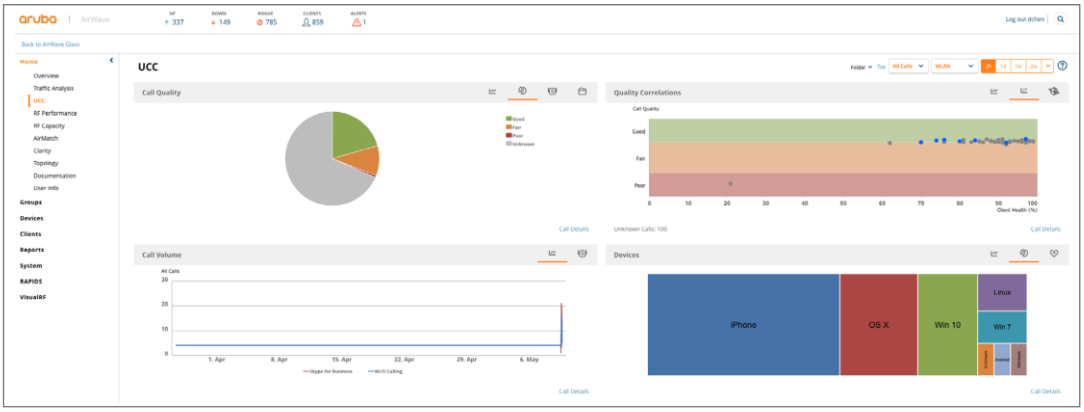
モバイル・アプリを特定して視覚化した後は、アクセス・コントロールとポリシーを適用することで、エンタープライズ・アプリケーションと個人用アプリケーションのパフォーマンスに優先順位を付けることができます。携帯デバイスが Wi-Fi 帯域幅をめぐって競合する中、PEF は本人にとって最も重要なアプリを保護します。

Apple AirPrint や AirPlay などのネットワークサービスが最適化され、IP マルチキャストビデオトラフィックが自動的に優先順位付けされ、Microsoft Teams や Skype for Business のような独自の Apple FaceTime トラフィックと暗号化された音声およびビデオセッションが自動的に識別され、優先順位付けされます。

さらに、Pandora、Netflix、Google Drive、Citrix GoToMeeting、Salesforce.com、Dropbox などの一般的な Web サービスは、ユーザー、デバイス、および場所に基づいてネットワーク上で優先順位付けができます。

PEFは、トラフィックに対して許可、ドロップ、ログ、拒否などの多数のファイアウォール・セキュリティ・アクションを適用できます。802.1pまたはDSCPマーキングによってパケットにタグを付けて優先度別に複数のキューに分類し、プロトコルに応じて異なる宛先にリダイレクトすることもできます。

さらに、音声プロトコルと動画プロトコルに対する高度な認識機能によって制御プロトコルとコール・セッションの両方に適切なQoSを自動的に適用できます。



Aruba UCC のダッシュボード・ビュー

PEFは、適切な優先度レベルと関連プロトコルが確実にマッピングされるようにします。たとえば、ユーザーから、またはユーザーへのトラフィックと、そのユーザーに関連付けられている音声QoSの設定の間に矛盾がある場合、そのトラフィックは適切な優先順位に再分類されます。

クリティカル・ユニファイド・コミュニケーション（UCC）サービスの場合、通話状態と品質に関する知識を活かしてより優れた VoIP 管理が可能になります。Aruba の AirMatch および ClientMatch RF 最適化テクノロジーを備えた AI を搭載したスマート機能は、稼動セッションの中断を軽減します。

UCC の最適化されたエクスペリエンス

統合された UCC ダッシュボードにより、Aruba は、Microsoft Teams、Microsoft Skype for Business、Apple FaceTime、Wi-Fi 通話、Jabber/Spark、SIP などさまざまな UCC アプリケーションの主要な通話品質メトリックをシンプルなビューで提供します。

ダッシュボードにマウスポインターを重ねてクリックすると、電話番号の関連付け、通話品質の追跡、通話詳細記録（CDR）、通話受付管理（CAC）などの詳細なレポートやトラブルシューティング情報が取得できます。

ダッシュボードには以下の機能があります。

- 通話品質と相関関係 – このグラフは、WLAN タブにおける AP 対クライアント通話品質、そしてエンドツーエンド・タブにおける有線・無線レッグを含むエンドツーエンドの品質を表します。
- 呼び出し量 - このグラフは、UCC アプリケーションの種類に基づいて行われた呼び出しの総数を表します。たとえば SIP、Lync、SCCP、H.323、NOE、SVP、VOCERA、FaceTime などです。
- デバイス – このグラフは、デバイスの種類ごとの音声セッションの内訳を表します。たとえば iPhone、OS X、Win 10 などです。

高性能なトラフィック処理

PEFを使用すれば、ポリシーの適用のためにパフォーマンスを犠牲にしたり、外付けのハードウェアを追加したりする必要はありません。

Arubaモビリティ・コントローラーは、制御処理、ネットワーク・トラフィックの処理、暗号化のための専用ハードウェアを備えた、ネットワーク・トラフィックの高速処理専用コントローラーです。

これにより、千単位のユーザーと万単位のアクティブ・セッションにまで拡張できる、高速、低レイテンシのポリシー適用が可能になりました。

認証と承認の外部インターフェイス

PEFは、ユーザーに対する細分性の高い制御を認証/承認サーバーによって拡張します。ネットワークからの自動切断、ロールの再割り当て、ファイアウォール・ポリシーの動的更新などの制御を有効化できます。

この機能は、IETF標準RFC 3576と、シンプルでありながら柔軟なXMLベースのAPI（アプリケーション・プログラミング・インターフェイス）という2種類のAPIによって実現されます。どちらのAPIも、ユーザーとポリシーの制御をモビリティ・コントローラーではなく外部のシステムに実行させることができます。

第3の統合インターフェイスであるsyslogプロセッサは、外部システムから受け取ったsyslogメッセージを正規表現で記述されたルールに基づいて処理することで、ユーザー・ロールの変更やブラックリストへのユーザーの追加といった構成可能な処理を行います。

攻撃対応のための平均時間の短縮

VLAN ベースのネットワーク構成を避けて制御を実施することにより、IT アクセスポリシーの適用に必要なリソースが大幅に削減され、攻撃対応を自動化できます。

PEF の細分性の高い制御により、正規の認証情報を選択してネットワーク全体に忍耐強く拡大する内部への攻撃が効果的に抑制されます。ユーザーまたはデバイスが限られたアクセス権限セットを持つロールを持っている場合、攻撃者も同様です。水平展開が含まれています。

データの流出やランサムウェアなどの攻撃が検出されると、PEF はロールを変更することにより、ユーザーまたはデバイスに関連付けられた権限を自動的に変更できます。攻撃対応には、帯域幅の削減、隔離、完全なブロックなど、さまざまなアクションが含まれます。攻撃警告は、単純な API 統合により、組織のセキュリティエコシステム内の特定のセキュリティ製品から発信できます。

CLEARPASS POLICY MANAGER との統合

ポリシー・エンフォースメント・ファイアウォールは、オプションで Aruba の ClearPass Policy Manager と統合される自己完結型のアクセス制御ソリューションです。ClearPass は、PEF に送られる認証情報およびポリシー規定サービスを整備し、大規模な一元的適用を実現する機能を提供します。ClearPass の主な利点は、個々のオフィスからグローバルな企業にいたるまで、認証情報とそのアクセス制御機能を統合することです。

ClearPass は、携帯機器管理から ServiceNow などのヘルプデスク・ソリューションにいたる 140 を超える Aruba テクノロジー・パートナーソリューションとのポリシー、ロールの実施、および攻撃対応の統合も支援します。

最高レベルのセキュリティ認証

Aruba のポリシー・エンフォースメント・ファイアウォール (PEF) は、Common Criteria および DoDIN-APL に基く NIAP 認定を受けています。PEF は NATO 承認製品リストにも載っています。

実装が簡単

IT 部門が環境を簡単に実装および保護できるように、PEF は、コントローラーベースのインフラストラクチャ用の Aruba オペレーティングシステム (AOS) で個別にライセンス供与されるソフトウェアオプションとして利用でき、コントローラーなしアクセス・ポイントのライセンス対象に含まれます。また、動的セグメンテーションを通じて Aruba ネットワークスイッチに提供されます。ハードウェアの追加は不要です。

まとめ

従来のファイアウォールは、アクセスが達成された後に VLAN 経由のポリシー適用を利用するため、IT チームは、ネットワーク接続時に開始される制圧攻撃への対応に苦労しています。PEF による Aruba のユーザーファイアウォール方法は、場所、接続方法、またはデバイスの種類に関係なく、ユーザーまたはデバイスの ID とロールに基づいて、ネットワーク接続の時点でゼロトラスト境界を提供するために構築された唯一のアクセス制御ソリューションです。

PEF が実施するきめ細かなアクセス許可により、組織は、攻撃が検出されたときにエンドポイントを自動的にブロックまたは隔離することにより、侵害されたユーザーとデバイスが攻撃に加担することを防ぎます。

PEF は既存の Aruba ネットワークインフラストラクチャのソフトウェアソリューションとして実装されるため、追加のハードウェアをインストールして識別・認証されたユーザーやデバイスのみがネットワークに接続されるようにする必要はありません。

機能概要	
機能	**メリット**
完全にステートフルなレイヤー 4 ～ 7 アプリケーションの可視性	データ・フローを双方向で制御することで、ネットワーク・エッジでユニークな可視性とセキュリティを提供します
影響を受けないパフォーマンス	コントローラーでのトラフィックの処理速度を低下させません
ユーザーファイアウォール	ユーザー、デバイスの種類、アプリケーション、または宛先に設定する AllAllows ロールベースのポリシー
UCC ダッシュボード	MOS、そして Teams や SIP などの UCC サービスの状況などのコール品質メトリックを表示
アプリケーション・アウェアなQoS	管理者がアプリケーション・トラフィックに優先順位を付け、RFレイヤーの動作を制御できるようにします
リアルタイム・アプリケーション・ダッシュボード	ネットワークの監視とトラブルシューティングのために、上位のアプリケーション、デバイス、宛先をリアルタイムに追跡します
再利用可能なポリシー・ライブラリ	便利で一貫的なポリシーを管理者が簡単に作成できるようにします
履歴データの収集	AirWaveを使用して、アプリケーションの使用とキャパシティ・プランニングに関する長期的な可視性を獲得します
ClearPass と外部 RADIUS 統合	ユーザーを認証し、詳細なデバイス識別と動的なポリシー更新をサードパーティ・デバイスまたはClearPassが実行できるようにします

Cyber Catalyst

Cyber Catalyst℠プログラムでは、大手サイバー保険会社は、自分たちがリスク軽減に際して効果的と考えるソリューションを評価および特定します。 参加保険会社はアリアンツ、AXIS、AXA の一部門である AXA XL、Beazley、CFC、ミュンヘン再保険、SOMPO インターナショナル、そしてチューリッヒ北アメリカです。 マイクロソフトは本プログラムの技術顧問を務めています。

aruba
a Hewlett Packard Enterprise company

TB_PEF_090419 a00073442enw