データシート

ARUBA POLICY ENFORCEMENT FIREWALL：モバイル・エンタープライズのためのアプリケーションの可視性とロールベースのセキュリティ

Aruba PEF（Policy Enforcement Firewall）は、コンテキストベースの制御によってアプリケーション・レイヤーのセキュリティと優先度設定を実現します。

PEFを導入することで、IT部門は、誰が、どのモバイル・デバイスで、ネットワークのどの領域にアクセスできるかを規定するネットワーク・アクセス・ポリシーを適用できます。

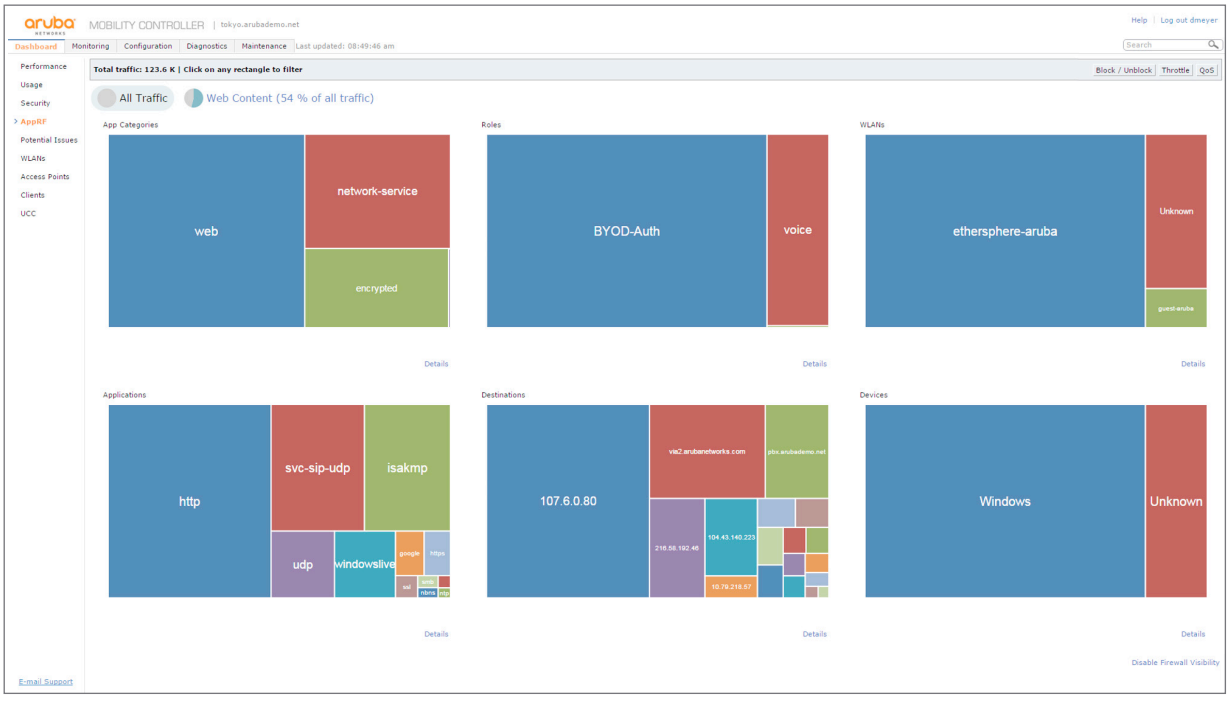
AppRFは、ネットワーク上で実行されているアプリケーションと、それを使用しているユーザーに関するインサイトをネットワーク管理者に提供するように設計されたPEF機能です。WebCCは、URLフィルタリング、IPレピュテーション、ジオロケーション・フィルタリングなどのオプションPEFサブスクリプション機能です。

Wi-Fiクライアントの動作を最適化し、RF干渉が生じないようにAPを維持するAruba ARM（Adaptive Radio Management）テクノロジーと連携することで、PEFはモバイル・アプリ、デバイス、悪意のあるURLに関する情報に基づいてインテリジェントなモバイル・セキュリティを提供します。

IDベースのポリシー制御

PEFとAppRFテクノロジーは、ネットワーク上の全トラフィックのユーザーレベルの認識を提供します。Arubaモビリティ・コントローラーは、有線、無線、VPNにまたがる単一ネットワーク上の複数のユーザー・カテゴリをサポートします。

ユーザーやデバイスがネットワークにサインオンする際に、それぞれのIDとロールが確認されます。従業員やその他の権限を持つ社内ユーザーを1つのクラスとして扱うことも、ディクショナリ・サーバー内の情報に基づいてさらに分割することもできます。



Arubaモビリティ・コントローラーのダッシュボード

ユーザー/デバイスのロールの確認後、管理者が定義した一連のテンプレート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。

アプリケーションのインテリジェントな特定

Aruba AppRFは、レイヤー4〜7トラフィックのDPI（ディープ・パケット・インスペクション）とインテリジェントな分析によって新たなタイプの多数のアプリケーションを識別します。

- **モバイル・アプリケーション：**Aruba AppRFテクノロジーは、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モバイル・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 AppRFテクノロジーは宛先アドレスに基づいて、Facebook、Twitter、Box、WebExなど、何百ものアプリケーションを一意に識別します。
- **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については、Aruba AppRFテクノロジーはヒューリスティックによってトラフィック・パターンを検出し、一意のフィンガープリントを確立することでこれらのアプリケーションを識別します。

アプリケーションの可視性

AppRFダッシュボードは、モバイル・アプリの使用状況とWLAN上でのパフォーマンスに関するシンプルで強力なビューをIT部門に提供します。Arubaモビリティまたは仮想コントローラーは、使用中のアプリケーションを表示、分類します。これは、ユーザー・ロール、アプリケーション、ネットワークなどの条件別に保存できます。

この情報は、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WLANポリシーの設定、将来的な拡張の計画に利用できます。長期的な履歴データについては、Aruba AirWaveネットワーク管理システムは、複数のArubaコントローラーからのデータを最長2年間に渡って集積できます。

ポリシーベースのトラフィックの管理と制御

PEF機能は、WLAN帯域幅の使用が最適化されるように制御します。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。WLANでは、パフォーマンスの低下を招くブロードキャスト・トラフィックやマルチキャスト・トラフィックをPEFが最適化することでアプリケーション・パフォーマンスを改善します。

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。

アプリケーションアウェアなサービス品質制御

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。モバイル・デバイスによってWi-Fi帯域幅の奪い合いとなった場合、AppRFテクノロジーは管理者の設定に基づいて優先すべきものを保護します。

Apple AirPrintやAirPlayなどのネットワーク・サービスは最適化され、IPマルチキャスト・ビデオ・トラフィックには自動的に優先順位が付けられます。また、Apple独自のFaceTimeトラフィックや、Microsoft Lyncのように暗号化された音声/ビデオ・セッションは、自動的に識別され、優先順位が付けられます。

さらに、Pandora、Netflix、Google Drive、Citrix GoToMeeting、Salesforce.com、Dropboxなどの一般的なWebサービスを、ユーザー、デバイス、場所に基いてWi-Fiに対して優先させることができます。

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。

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。

コール・ステータスの認識はそれ以上に強力です。これにより、空中のVoIP（Voice-over-IP）をよりスマートに管理できます。RF管理や負荷分散などの機能が通話中の音声品質に影響を生じることはありません。PEFは通話の終了まで待機し、その上でRFの最適化を実行します。

音声の包括的な管理と制御

PEFは、詳細なレポート機能やトラブルシューティング、表やグラフによる分かりやすいデータ表示など、SIP（Session Initiation Protocol）を利用したさまざまな音声管理機能を備えています。これ以外の主な機能は次のとおりです。

- 電話番号の対応付け – SIP対応端末を追跡し、その端末を電話番号で表示できます。
- 通話品質の追跡 – モビリティ・コントローラーで処理されるすべてのSIPコールのR値を自動的に計算、表示、追跡します。
- SIP認証の追跡 – IP PBXへのSIP端末の登録を追跡することで、端末が認証済みであるかどうかを確認します。
- コール詳細レコード（CDR） – 発信者、終了者、終了理由、拒否された、または失敗した通話、通話時間、通話品質など、Wi-Fiクライアント間で行われた通話の詳細情報を表示します。
- リアルタイムのCAC（コール・アドミッション制御）情報 – 負荷分散のために、コール密度、CAC状態、アクティブ・コールを迅速に特定します。

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。

すべてのユーザーに対するステートフルなファイアウォール

PEFは、ほぼすべてのユーザーに対して完全にステートフルなファイアウォール・インスタンスを実装します。ユーザーに許可される操作を厳密に制御し、ユーザー・クラス間を分離します。

モビリティ・コントローラーは、Wi-FiサービスとVPNトンネリングのいずれを提供する場合でも、クライアントとデータセンターの間の暗号化をサポートし、最高レベルのネットワーク・セキュリティを実現します。認証、暗号化、ポリシー適用は、PEFによって一元的に行われます。

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。

ネットワーク・セキュリティ導入の簡略化

外部サービス・インターフェイス（ESI）を使用することで、多様なネットワーク・サービス・アプライアンスをモビリティ・コントローラーと共に設置し、それらのサービスをネットワーク・クライアントに提供できます。

一元的に有効化されるこれらのアプライアンスは、ウイルス防御、コンテンツの検査とフィルタリング、侵入の防御と防止、コンテンツの変換、プロトコルベースの帯域幅シェーピングなどのサービスを提供します。

機能とメリット

機能	メリット
完全にステートフルなレイヤー4〜7ファイアウォール	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
完全にユーザー/アプリケーション・アウェア	組織内のロール、ユーザー、デバイス、アプリケーション、アプリケーションの宛先に基づくポリシーを設定できます
Unified Communications向けの高度なアプリケーション・レイヤー・ゲートウェイ	アプリケーションがファイアウォールの境界をまたいでシームレスに機能できるようにします
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AppRF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
外部RADIUSサーバーとの統合	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

注文情報

部品番号	説明
LIC-PEFNG-##	Policy Enforcement Firewallモジュール(##はAPのライセンス) – Aruba APまたはモビリティ・コントローラーの有線ポート経由でモビリティ・コントローラーに入るユーザー・トラフィックに適用されます。
LIC-PEFV-xx	Policy Enforcement Firewallモジュール(モビリティ・コントローラー・モデルxx用) – VPNトンネル経由でモビリティ・コントローラーに入るユーザー・トラフィックに適用されます。