DATA SHEET

ARUBA POLICY ENFORCEMENT FIREWALL: APP VISIBILITY AND ROLE-BASED SECURITY FOR MOBILE ENTERPRISES

The Aruba Policy Enforcement Firewall (PEF) provides context-based controls to enforce application-layer security and prioritization.

With PEF, IT can enforce network access policies that specify who may access the network, with which mobile devices and which areas of the network they may access.

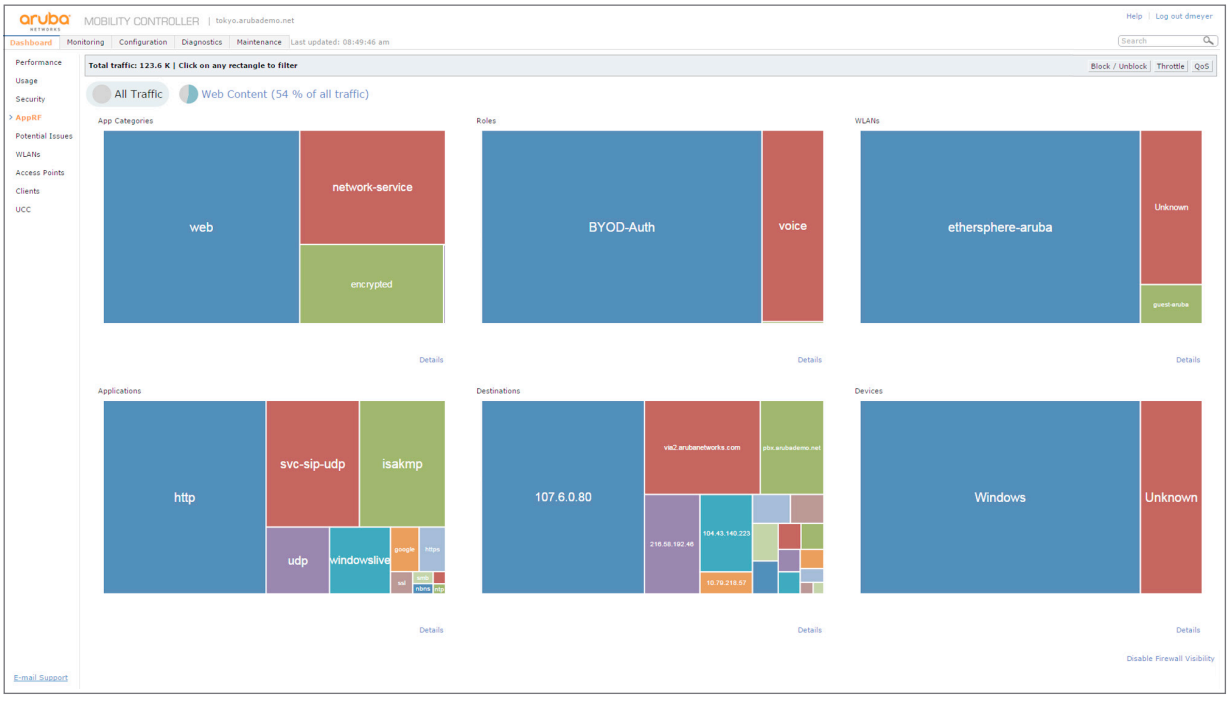
AppRF is a PEF feature that is designed to give network administrators insight into the applications that are running on their network, and who is using them. WebCC is an optional PEF subscription feature that includes URL filtering, IP reputation, and geolocation filtering.

Working with Aruba Adaptive Radio Management (ARM) technology, which optimizes Wi-Fi client behavior and makes sure that APs stay clear of RF interference, PEF delivers intelligent mobile security based on its knowledge of mobile apps, devices and malicious URLs.

IDENTITY-BASED POLICY CONTROLS

PEF with AppRF technology provides user-level awareness of all traffic across the network. Aruba Mobility Controllers support multiple user categories on a single network, spanning wired, wireless and VPNs.

During the network sign-on process, the identity and role of each user or device is learned. Employees and other authorized internal users can be treated as a single class or further subdivided according to information found in a directory server.



Dashboard view in the Aruba Mobility Controller

Once the role of the user or device is determined, policies are applied based on a series of administrator-defined templates. These policies follow the user throughout the network and are applied uniformly across wireless, wired and VPN connections.

INTELLIGENT APPLICATION IDENTIFICATION

Deep packet inspection (DPI) and of Layer 4-7 traffic and intelligent analysis allows Aruba AppRF technology to identify many new types of applications:

- **Mobile applications:** Aruba AppRF technology distinguishes corporate applications like Box from personal applications like Apple FaceTime, even when they are running on the same mobile device.
- **Network services like Apple AirPrint and AirPlay:** Aruba optimizes IP multicast video traffic and automatically prioritizes services, and adds policy controls.
- **Web-based applications:** Many web-based applications use the same port to communicate with clients and appear as HTTP traffic. Aruba AppRF technology resolves the destination address to identify unique applications like Facebook, Twitter, Box, WebEx and hundreds of others.
- **Encrypted applications:** For encrypted traffic, Aruba AppRF technology uses heuristics to look for traffic patterns and establishes a unique fingerprint to identify those applications.

APPLICATION VISIBILITY

The AppRF dashboard gives IT a simple, powerful view of mobile app usage and performance on the WLAN. Aruba mobility or virtual controllers display and categorize applications in use, which can be sorted by user role, application, network and other criteria.

This information can be used to troubleshoot application performance in real time, set global WLAN policies, and plan for future growth. For longer-term historical data, Aruba AirWave network management can aggregate up to two years of data from multiple Aruba controllers.

POLICY-BASED TRAFFIC MANAGEMENT AND CONTROL

PEF features controls that optimize WLAN bandwidth utilization. Role-based policies can limit the maximum amount of bandwidth consumption for a particular user or class of users, and prevents power users from monopolizing network resources.

At the same time, traffic management policies can guarantee minimum amounts of bandwidth for devices to ensure that users stay productive. On WLANs, PEF optimizes performance-robbing broadcast and multicast traffic to improve application performance.

Other bandwidth-hungry protocols such as mDNS, ARP and NetBIOS broadcasts can be completely filtered and confined only to specific portions of the network.

In addition, PEF provides comprehensive on-line threat intelligence to protect users and networks from malicious files and URLs in real-time. Policies can be enforced based on URL filtering, IP reputation, and geolocation (WebCC subscription), as well as user-role or device context.

APPLICATION-AWARE QUALITY OF SERVICE CONTROLS

After mobile apps are identified and visualized, access controls and policies can be applied to prioritize the performance of enterprise applications over personal ones. As mobile devices contend for Wi-Fi bandwidth, AppRF technology protects the apps you care most about.

Network services like Apple AirPrint and AirPlay are optimized, IP multicast video traffic is automatically prioritized, and proprietary Apple FaceTime traffic and encrypted voice and video sessions like Microsoft Lync are automatically identified and prioritized.

In addition, common web services like Pandora, Netflix, Google Drive, Citrix GoToMeeting, Salesforce.com and Dropbox can be prioritized over Wi-Fi based on user, device and location.

PEF can apply a number of firewall security actions to traffic, including permit, drop, log or reject. Packets can also be tagged with 802.1p or DSCP markings, prioritized into multiple queues and redirected to different destinations based on protocols.

Advanced awareness of voice and video protocols permits appropriate QoS to be applied to both the control protocol and the call sessions automatically.

PEF ensures that the appropriate priority level is mapped to the associated protocol. For instance, if traffic to or from a user is inconsistent with the associated QoS setting for voice, then that traffic is reclassified to the appropriate priority.

Most powerfully, knowledge of call status enables smarter voice-over-IP management across the air. Capabilities like RF management and load balancing do not affect voice quality during a call. Instead, PEF waits until voice handsets are on-hook to perform RF optimization.

COMPREHENSIVE VOICE MANAGEMENT AND CONTROL

PEF offers extensive voice management capabilities using the session initiation protocol (SIP), including detailed reporting and troubleshooting as well as at-a-glance data via tables and graphs. Other capabilities include:

- Phone number association – SIP-enabled devices can be tracked and displayed by their phone number.
- Call quality tracking – Automatically calculate, display and track the R-value for each SIP call being processed through a Mobility Controller.
- SIP authentication tracking – Track the registration of SIP devices to an IP PBX to determine if they are authenticated.
- Call detail records (CDRs) – Display calls made to and from Wi-Fi clients, including originator, terminator, termination reason, rejected and failed calls, duration, and call quality.
- Real-time call admission control (CAC) information – Quickly determine call density, CAC state and active calls for load balancing.

HIGH-PERFORMANCE TRAFFIC PROCESSING

With PEF, policy enforcement does not come at the expense of performance or require additional external hardware.

Aruba Mobility Controllers are purpose-built for high-speed processing of network traffic with dedicated hardware for control processing, network traffic processing and encryption.

The result is high-speed, low-latency policy enforcement that scales up to many thousands of users and hundreds of thousands of active sessions.

STATEFUL FIREWALLS FOR EVERY USER

PEF implements a full stateful firewall instance around every user, tightly controlling what the user is permitted to do and providing separation between user classes.

For the highest level of network security, Mobility Controllers support client-to-data center encryption, whether providing Wi-Fi services or VPN tunneling. PEF provides a unified point for authentication, encryption and policy enforcement.

EXTERNAL AUTHENTICATION AND AUTHORIZATION INTERFACES

PEF extends fine-grained control over of users from authorization and authentication servers. Controls such as automatic disconnection from the network, role reassignment, and dynamic updates of firewall policies can be enabled.

This functionality is enabled by two application programming interfaces (APIs) – IETF standard RFC 3576 and a simple yet flexible XML-based API. Both APIs allow external systems to exert user and policy control over Mobility Controllers.

A third integration interface, a syslog processor, accepts syslog messages from outside systems, processes them according to a regular-expression rule language, and then provides configurable actions such as changing a user role or placing a user on a blacklist.

EASE NETWORK SECURITY DEPLOYMENTS

The external services interface (ESI) allows a wide range of network service appliances to be co-located with Mobility Controllers to provide their services to clients on the network.

These centrally-enabled appliances provide services like virus protection, content inspection and filtering, intrusion detection and prevention, content transformation and protocol-based bandwidth shaping.

FEATURES & BENEFITS

Feature	Benefit
Fully Stateful Layer 4-7 Firewall	Provides unique visibility and security at the network edge by controlling the flow of data in a bidirectional way
Zero-impact performance	Doesn't slow down traffic processing on the controller
Fully user and application aware	Allows policy to be set by organizational role, user, device, application or app destination
Advanced Application Layer Gateways for Unified Communications	Allows applications to work seamlessly across firewall boundaries
Application Aware QoS	Enables administrators to prioritize application traffic and control RF layer behavior
Real-Time AppRF Dashboard	Track top applications, devices and destinations in realtime for network monitoring or troubleshooting
Reusable policy library	Makes it easy for administrators to create useful, consistent policies
Historical Data Collection	Use AirWave for long-term visibility into application use and capacity planning
Integration with external RADIUS servers	Authenticate users, allow third party devices or ClearPass to do detailed device identification and dynamic policy updates

ORDERING INFORMATION

Part Number	Description
LIC-PEFNG-##	Policy Enforcement Firewall module (## AP license) – Applies to user traffic entering the Mobility Controller through an Aruba AP or through a Mobility Controller wired port.
LIC-PEFV-xx	Policy Enforcement Firewall module for xx Mobility Controller model – Applies to user traffic entering the Mobility Controller through a VPN tunnel.

aruba
a Hewlett Packard Enterprise company

1344 CROSSMAN AVE | SUNNYVALE, CA 94089
1.844.473.2782 | T: 1.408.227.4500 | FAX: 1.408.227.4550 | INFO@ARUBANETWORKS.COM

www.arubanetworks.com