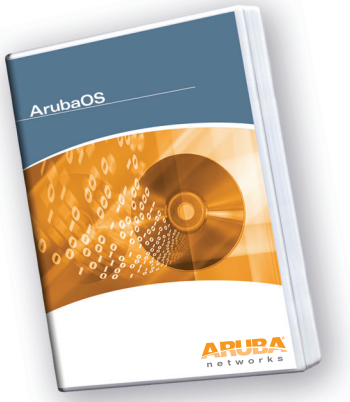
DATA SHEET

ArubaOS Policy Enforcement Firewall Module

ARUBAOS POLICY ENFORCEMENT FIREWALL MODULE



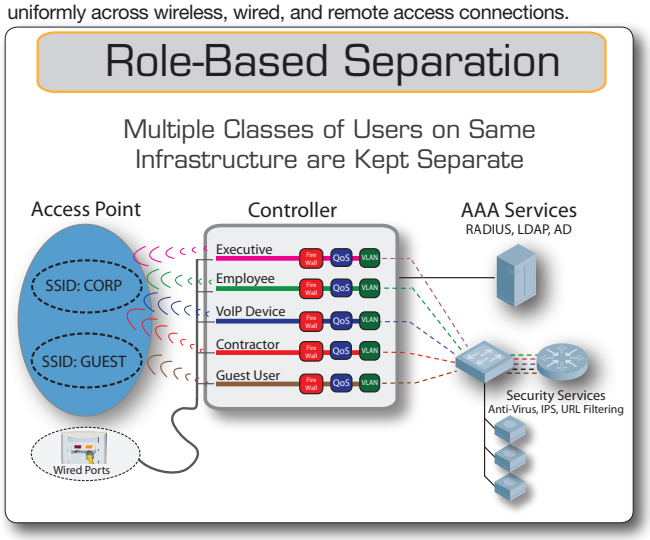
Aruba's Policy Enforcement Firewall (PEF) module for ArubaOS provides identity-based controls to enforce application-layer security, prioritization, traffic forwarding, and network performance policies for wired and wireless networks. Using PEF, organizations can enforce network access policies that specify who may access the network, which areas of the network they may access, and the performance thresholds of various applications. Administrators can build a unified, integrated system for network policy enforcement by leveraging PEF's open interfaces to external services such as content security appliances, NAC policy engines, performance monitors, and authentication/authorization servers.

For organizations adopting emerging applications such as Voice over Wi-Fi, the PEF module provides advanced voice management capabilities with enhanced visibility and control into voice sessions. Features such as SIP protocol decoding, phone number tracking, dial plan mapping, SIP-based authentication, and fine-grained queue management make large-scale enterprise voice deployments a reality.

IDENTITY-BASED POLICY CONTROLS

PEF provides user-level awareness of all traffic across the network. Enterprises today need to support a broad variety of users, devices, and applications – all of which want mobility. Traditional network architectures mandate that parallel networks be constructed to address the different needs of each constituent – for example, one network for employees and full-time contractors, another for guests, and a third for voice. Even when these networks can be constructed using the same physical hardware, there is an associated complexity and resulting high cost.

Aruba mobility controllers with PEF can support multiple user categories on a single network, spanning wired, wireless, and remote access. During the network sign-on process, the identity and role of each user or device is learned. Employees and other authorized internal users may be treated as a single class, or further subdivided according to information found in a directory server. Once the role of the user or device has been 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 remote access connections.



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. The VLAN-based security used in traditional network designs is both cumbersome to configure and deficient in security. External firewalls are limited because they understand only ports and IP subnets. To provide the highest level of security, a firewall requires knowledge of user identity when making access control decisions.

For the highest level of network security, Aruba Mobility Controllers support client-to-datacenter encryption, whether providing Wi-Fi services or VPN tunnel services. PEF provides a unified point of authentication, encryption, and policy enforcement. Policy control is tied to user identity rather than port, IP address, or MAC address; encryption/decryption provides a further check on user identity on a per-packet basis. This makes it impossible for a user to bypass security controls under any circumstances – for example, a guest user on the guest network who tries to configure a laptop with the MAC address and IP address of an employee will not be successful in accessing the employee network.

APPLICATION-AWARE QUALITY OF SERVICE CONTROLS

Once application flows have been identified, standard firewall security actions such as permit, drop, log, or reject can be applied. However, PEF is capable of more than just robust security. Rule actions can also tag packets with an 802.1p or DSCP marking, prioritize the traffic into multiple queues, or even redirect specific protocols to different destinations. Advanced awareness of voice and video protocols permits appropriate QoS to be applied to both the control protocol and the call sessions automatically. Knowledge of call status enables smarter wireless radio supervision; functions such as RF management and load balancing will not impact call quality while a voice call is active, instead waiting until voice handsets are on-hook to perform RF optimization.

For client devices using Wi-Fi Multimedia (WMM) for traffic priority management, a reality of the WMM system is that it will allow any client to request and use any priority level for any type of traffic. Because the

ARUBAOS POLICY ENFORCEMENT FIREWALL MODULE

standard lacks a method of enforcement, a badly-behaved client can break established QoS policies by sending lower priority traffic such as data file transfers at a higher priority level, such as that reserved for voice. Because PEF is application-aware, it will ensure that the appropriate priority level is mapped to the associated protocol – for instance, voice priority is always assigned to voice traffic. 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.

DYNAMIC TRAFFIC MANAGEMENT

PEF provides controls to optimize wireless network bandwidth usage, which can be a limited resource in many networks. Role-based policies can limit the maximum amount of bandwidth consumption for a particular user or class of users, preventing "power users" from monopolizing network resources. At the same time, traffic management policies also guarantee a minimum amount of bandwidth to ensure that devices are not starved. On Wi-Fi networks, 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 filtered completely and confined only to specific portions of the network.

HIGH-PERFORMANCE TRAFFIC PROCESSING

With PEF, policy enforcement does not come at the expense of performance. All Aruba 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 thousands of users and hundreds of thousands of active sessions.

EXTERNAL AUTHENTICATION & AUTHORIZATION INTERFACES

Extended authorization control allows fine-grained control of users from authorization and authentication servers. Controls such as automatic disconnection from the network, role re-assignment, 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. These APIs both allow external systems to exert user and policy control over an Aruba controller.

A third integration interface is available in the form of the Syslog Processor. This interface 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.

Authentication APIs can also be used to enable external captive portal authentication systems. Aruba controllers provide integrated captive portal authentication in the base system, with the ability to customize the captive portal look and feel on a per-SSID basis. Organizations wishing to develop more extensive captive portal systems with custom scripting, database operations, or other advanced behavior may do so using PEF's authentication API.

EASE NETWORK SECURITY DEPLOYMENTS

The External Services Interface (ESI) allows a wide array of network service appliances to be co-located with an Aruba controller to provide their services to clients on the network. Appliances providing services such as virus protection, content inspection and filtering, intrusion detection and prevention, content transformation, protocol-based bandwidth shaping and more are all enabled centrally. Until now, deploying such services in the interior of the network required placement of network service devices in every wiring closet, where they were placed in-line with all network traffic. ESI permits a centralized approach, enabling scalable and manageable deployments that minimize both capital and operational costs.

ESI is implemented through policy-based forwarding, permitting the selective redirection of traffic to any standard in-line device that supports transparent L2 or routed L3 mode. By using ESI to specify which traffic types are redirected to a network service device, network managers can deploy only the service capacity that is required for that specified subset of network traffic. ESI's load balancing algorithm distributes traffic between multiple service appliances to even out load while protecting against service failure.

ESI can also supplement network access control (NAC) by providing security services to client devices which cannot verify to the network that they are compliant. For example, IT policy may state that clients must run anti-virus software and have run a scan within the past week. If a client cannot run NAC agent software to perform host validation, ESI can direct traffic to and from that user through an anti-virus appliance in the network.

COMPREHENSIVE VOICE MANAGEMENT AND CONTROL

PEF adds extensive voice management functionality for networks using SIP, providing detailed reporting and troubleshooting capabilities. Information is available at a glance via extensive tables and graphs. Some of the capabilities include:

- Phone number association – SIP devices can be tracked and displayed by their associated phone number.
- Call quality tracking – Automatically calculates, displays and tracks the R-value for each SIP call being processed through the Aruba mobility controller.
- SIP authentication tracking – Tracks the registration of SIP devices to an IP PBX to determine if they are authenticated devices.
- Call detail records (CDRs) – Displays the calls made to or from Wi-Fi clients, including originator, terminator, termination reason, rejected and failed calls, duration, call quality, etc.
- CAC-based real-time information – Quickly determine call density, CAC state, and active calls.

To ensure sufficient voice capacity in the Wi-Fi network, Voice Call Admission Control (CAC) prevents any single AP from becoming congested with too many voice calls. This is accomplished by limiting the number of active voice calls allowed on a radio or by setting voice bandwidth thresholds. The system monitors the number of active voice calls and the bandwidth being used by voice devices, and automatically load-balances new calls to neighboring APs if the defined threshold is reached. Advanced voice clients using SIP and 802.11k allow the load balancing process to be transparent to the user.

ORDERING INFORMATION

PART NUMBER	DESCRIPTION
LIC-PEFNG-##	Policy Enforcement Firewall Module (## Access Point License) – Applies to user traffic entering the Mobility Controller through an Aruba access point or through a 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 networks

WWW.ARUBANETWORKS.COM

1344 Crossman Avenue. Sunnyvale, CA 94089 | Tel. +1 408.227.4500 | Fax. +1 408.227.4550

DS_PEF_US_100303