

# ArubaOS

## Policy Enforcement Firewall Module

### ArubaOS

Aruba's Policy Enforcement Firewall module provides identity-based security, Quality of Service (QoS) control, and traffic management capabilities to a usercentric network. Identity-based security is essential since mobile users can enter a network at any point, wired or wireless. Aruba's ICSA-certified stateful firewall enables user classification on the basis of user identity, device type, location, and time of day, and provides differentiated access for different classes of users.

Since the physical layer of security is missing in mobile networks, mobile users need to be treated with greater security than traditional fixed users. Firewalls are a mandatory part of an enterprise's layered security strategy for the mobile network, and Aruba's unique identity-based stateful firewall technology enables enterprises to define access controls for any user or group of users on the network.

### Identity-Based Stateful Firewalls

Aruba mobility controllers provide a single point of encryption/decryption, authentication, and firewall enforcement. Because they are identity-aware and also terminate encryption, they are immune from spoofing attacks that plague traditional network-based firewalls that filter on IP address rather than user identity.

### Complete Policy-Based Access Control

All organizations have written IT security policies. Policies can dictate the network access, protocols and applications that are permitted or denied, and levels of services that are provided. In most enterprises, policy compliance is monitored to varying degrees, but violations are discovered and dealt with after the fact. Aruba permits policies to be actively enforced, even in a mobile environment, with policies following the users as they roam across the edge of the network

### Quality of Service Control

Once application flows have been identified by the firewall, standard firewall actions such as permit, drop, log, or reject can be applied. However, Aruba's stateful firewall capability enables 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. Flow classification is stateful for many popular protocols, such as SIP, permitting appropriate QoS to be applied to both the control protocol and the call sessions.

### Role-Based Access Control

Aruba's stateful Policy Enforcement Firewall enables access to network resources based on the role of the user. This role is assigned or derived through a variety of different mechanisms such as external authentication databases, ESSID, or physical location. Once the role has been assigned to a user, differentiated policies can be applied

## Product Overview



## Benefits:

### Identity-Based Stateful Firewalls

- Firewall rules are aware of the user, not just IP addresses, leading to greater visibility and more complete control

### ICSA Certification

- Industry-standard verification of firewall quality and security, providing assurance that complete independent testing has been performed

### Policy-Based Access Control

- Permits translation of corporate security policy into action. Compliance with corporate security policy becomes mandatory and enforced rather than simply monitored

## Product Overview

### More Benefits:

#### Quality of Service Control

- Stateful flow classification enables identification of application flows for special treatment, such as providing enhanced QoS for voice

#### Role-Based Access Control

- Permits templates to be applied based on group membership, simplifying administration

#### High-Performance Security

- Hardware-accelerated encryption/decryption and firewall rule processing to eliminate bottlenecks
- Separation of control and data plane for scalability

#### High-Performance Wireless Security

Until now, enterprises have been forced to quarantine wireless users into a DMZ, where they were authenticated and firewalled as if they were coming in from the Internet. While this mechanism works from a security standpoint, the performance offered to the wireless user is severely impacted due to limitations with DMZ-based VPN gateways and firewalls. Aruba allows corporate users to be authenticated, encrypted and firewalled within the corporate intranet with the highest degree of security and performance, providing the connecting point between mobile users and the wired network.

#### Specifications:

##### Certification

- ICSA-certified, Corporate Firewall v4.1\* (\*Aruba 6000 only)

##### Role Determination Criteria

- Authentication-Default or RADIUS-derived
- Physical location

##### Stateful Application-level Gateway

- FTP
- SIP
- RTP/RTSP
- Cisco SCCP (Skinny)

##### Wired and Wireless QOS

- Flow classification
- Priority queues
- Bandwidth contracts
- 802.1p and DSCP tagging

##### Network Address Translation

- Source and destination

### LTI DataComm

23020 Eaglewood Ct. #100  
Sterling, VA 20166  
www.ltidata.com  
800-677-5050