ArubaOS Policy Enforcement Firewall Module

Aruba's Policy Enforcement Firewall module provides identity-based security to the mobile edge of the network. Where users are mobile, identity-based security is a requirement since users may enter the 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.

IDENTITY-BASED STATEFUL FIREWALLS
Firewall rules are aware of the user, not just IP addresses, l eading 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

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

WEB-BASED CAPTIVE PORTAL
Provides SSL browser-based authentication for secure guest and employee access

HIGH-PERFORMANCE SECURITY
Hardware-accelerated encryption/decryption and firewall rule processing to eliminate bottlenecks

Separation of control and data plane for scalability

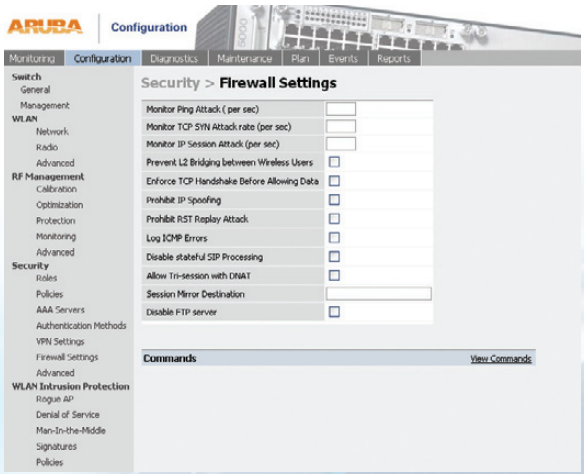
Because the physical layer of security is missing in mobile networks, mobile users should be treated with more caution than traditional fixed users. Firewalls are a mandatory part of an enterprise's layered security strategy for the mobile edge of the network. Aruba's unique identity-based stateful firewall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



Easy to use GUI for Firewall policy configuration

STATEFUL FLOW CLASSIFICATION

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.

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. The Aruba system allows corporate users to be authenticated, encrypted and firewalled within the corporate intranet with the highest degree of security and performance. Aruba provides the connecting point between wireless users and the wired network.

LAN-SPEED FIREWALLS FOR EACH USER

Even after strong authentication and encryption have been used, mobile users need to be treated with caution. With mobility comes the danger of stolen laptops and viruses picked up at public hotspots. Incorporating an identity-based firewall into the mobile edge of the network minimizes the risks and damage that can occur. By restricting what network resources are accessible by a mobile user, Aruba's Policy Enforcement Firewall helps eliminate the propagation of worms and viruses within the intranet.

CAPTIVE PORTAL FOR GUEST OR EMPLOYEE ACCESS

For clients without 802.1x, VPN, or other security software, Aruba supports a web-based captive portal that provides standard browser-based authentication. Captive portal authentication is encrypted using industry-standard SSL (Secure Sockets Layer), and can support both registered users with a login and password or guest users who supply only an email address. Through integration with back-end systems, captive portal can provide a secure guest access solution, permitting front-desk reception staff to issue and track authentication credentials for visitors.

SPECIFICATIONS

Certification
ICSA certified, Corporate Firewall v4.0

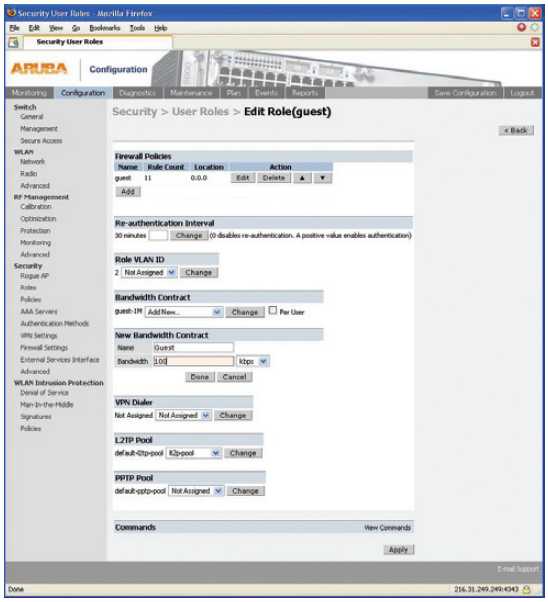
Role Determination Criteria
Authentication – Default or RADIUS-derived
Physical location

ESSID
MAC address

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



Create user roles with associated firewall policies.

FEATURE	BENEFIT
Identity-based stateful firewalls	• Keeps track of the state of sessions and traffic flows so that common attacks can be thwarted
Application-aware firewall	• Enables flow classifications based on application type
Hardware-accelerated processing	• All VPN and firewall processing is performed on an integrated encryption engine enabling high-speed wireless performance
Role-based policies	• Individual and group policies are derived and can be defined for fine-grained control
Captive portal	• Web-based captive portal provides standard browser-based authentication for guest access
Bandwidth contracts	• Limits bandwidth consumption for specific uses or applications so critical apps are not degraded

ARUBA™
The Mobile Edge Company
www.arubanetworks.com

1322 Crossman Avenue
Sunnyvale, California 94089
Tel: 408.227.4500 • Fax: 408.227.4550

10.5.SSPE.kh.10.1