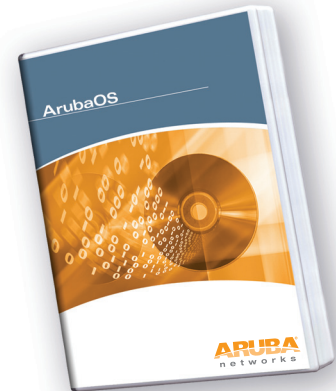




ARUBAOS POLICY ENFORCEMENT FIREWALL MODULE

Aruba's Policy Enforcement Firewall (PEF) module for ArubaOS provides identity-based controls to enforce security, prioritization, traffic forwarding, and performance policies for Aruba's networking solutions. Most organizations have network access policies that specify who may access the network, which parts of the network they may access, and what quantity of network resources they may consume. While many organizations monitor for policy compliance, Aruba's PEF module provides the critical capability of turning IT policy into mandatory, enforceable actions. Administrators can build a unified, integrated system for network policy enforcement by leveraging PEF's open interfaces to external services such as security appliances, NAC policy engines, performance monitors, and authentication/authorization servers.



IDENTITY-BASED POLICY CONTROLS

- Enable translation of corporate network policies into mandatory, enforceable actions
- Policies are tied to user identity rather than device, port, wireless SSID, IP subnet, or VLAN
- Role-based system permits policy templates to be applied based on group membership, simplifying administration

STATEFUL FIREWALLS LOCK DOWN NETWORK SECURITY

- Firewall rules are aware of the user, not just IP addresses, leading to greater visibility and more complete control
- Puts critical security separation between different classes of users (e.g. students and faculty) or different classes of devices (e.g. barcode scanners and laptops)
- ICSA certified: Industry-standard verification of firewall quality and security, providing assurance that complete independent testing has been performed

APPLICATION-AWARE QUALITY OF SERVICE CONTROLS

- Stateful flow classification enables identification of application flows for special treatment, such as providing enhanced QoS for video streams
- Voice application awareness tracks on-hook/off-hook status of voice devices to better optimize wireless RF management

TRAFFIC MANAGEMENT CONTROLS OPTIMIZE PERFORMANCE

- Advanced bandwidth management controls guarantee minimum available bandwidth while capping maximum bandwidth consumption
- Performance-robbing broadcast/multicast traffic can be filtered, suppressed, or proxied without impacting applications
- Selectively block specific bandwidth-hungry protocols such as mDNS, ARP, and NetBIOS broadcasts
- Prevent "power users" from monopolizing limited network resources at the expense of other clients

HIGH-PERFORMANCE TRAFFIC PROCESSING

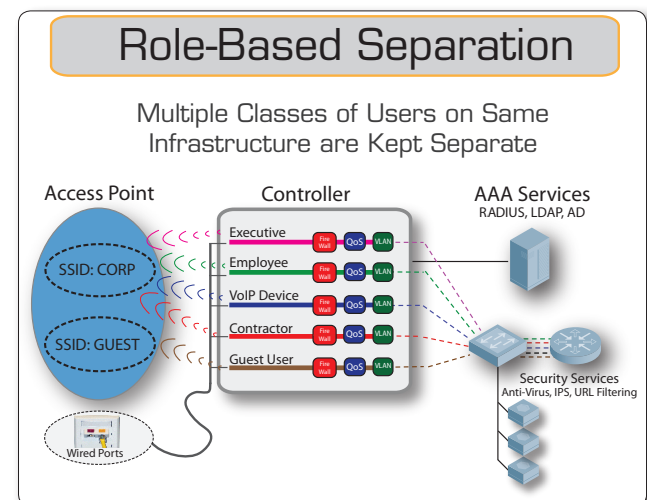
- Hardware-accelerated encryption and firewall rule processing eliminates bottlenecks
- Separation of control and data plane improves scalability

EXTERNAL AUTHENTICATION & AUTHORIZATION INTERFACES

- Seamlessly integrate external web-based authentication portals, allowing unique customization of the user experience
- Link controllers with NAC policy engines to dynamically modify user privileges based on metrics such as client behavior
- Automatically disconnect users from the network when security systems, such as an IPS, match pre-defined conditions
- Programmatic interfaces to external systems provided through RADIUS (RFC 3576), a flexible XML-based API, and the Syslog Processor

NETWORK SERVICE DELIVERY

- Centralize network service appliances (e.g. anti-virus, IPS, URL filtering) in the datacenter for clients that do not or cannot implement these services themselves
- Fault-tolerance is achieved through load balancing and continuous health checking of external services
- Process only specific traffic from specific users, based on client device health, trust state, or behavior detection
- Open interfaces preserves investment in existing security and service vendors and prevents vendor lock-in



ARUBA OS POLICY ENFORCEMENT FIREWALL MODULE

IDENTITY-BASED POLICY CONTROLS

All organizations have written IT policies. Policies can dictate the network access, protocols and applications that are permitted or denied, levels of services that are provided, and allowable resource usage. 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. Policies are applied and access rights are controlled based on the role of the user. This role is assigned or derived through a variety of different mechanisms such as external authentication databases, wireless SSID, or physical location.

STATEFUL FIREWALLS LOCK DOWN NETWORK SECURITY

Converged networks support multiple classes of users and devices on the same physical infrastructure. For this to be effective and secure, identity-aware firewalls are required to provide separation between user classes. Aruba controllers provide a single point of encryption, authentication, and policy enforcement. Because controllers are identity-aware and also manage encrypted sessions, they are immune from spoofing attacks that plague traditional network-based firewalls that filter on IP address rather than user identity.

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, 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. Advanced application-layer 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 prevents wireless-level processes, such as RF management and load balancing, from impacting call quality.

TRAFFIC MANAGEMENT CONTROLS OPTIMIZE PERFORMANCE

Wireless bandwidth is a limited resource, and Aruba's Policy Enforcement Firewall provides controls to optimize usage of that resource. Bandwidth-management policies, based on user role, limit the maximum amount of bandwidth that a particular user or class of users may consume. At the same time, traffic management policies also guarantee a minimum floor on bandwidth consumption to ensure that devices are not starved. PEF optimizes broadcast and multicast traffic to improve application performance while not wasting bandwidth.

HIGH-PERFORMANCE TRAFFIC PROCESSING

With Aruba, policy enforcement does not come at the expense of performance. All Aruba controllers are purpose-built for high-speed processing of network traffic. Each controller implements dedicated hardware for control processing, for network traffic processing, and for 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 the role of a user or placing a user on a blacklist.

Authentication APIs can also be used to enable external captive portal Web-based authentication systems. ArubaOS provides 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.

NETWORK SERVICE DELIVERY

A PEF feature known as the External Services Interface (ESI) permits a wide array of network service appliances to be co-located with an Aruba controller to provide their services to clients on the network. Typically deployed in a DMZ or at an organization's Internet gateway, these appliances provide services such as virus protection, content inspection and filtering, intrusion detection and prevention, content transformation, protocol-based bandwidth shaping and more. 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. This allows network managers to use equipment they already own and know, protecting and leveraging their existing investments. Although all "at risk" traffic should be screened, passing all network traffic through network service devices could lead to performance bottlenecks. ESI makes this process more efficient by only forwarding traffic that meets established criteria to service appliances.

For example, some traffic types, such as Enterprise Resource Planning (ERP) traffic or SQL database transactions, do not carry viruses and do not need to be filtered for virus protection. Alternatively, web, email and file-transfer traffic does require virus filtering. By using ESI to specify which traffic types are redirected to a network service device, network managers need deploy only enough service capacity for that specified subset of network traffic and will not need to deploy as many, if any, additional appliances.

ESI also supplements NAC implementations by providing security services to client devices which do not provide the service themselves, or which cannot verify to the network that they run such services. IT policy may state, for example, that clients must run anti-virus software and must have run an anti-virus scan within the past week. If a client cannot run NAC agent software to perform validation of this policy, ESI can direct traffic to and from that user through an anti-virus appliance in the network.

To enable high availability, ESI supports health checking and load-balancing of traffic to external devices. Flexible health checking techniques permit Aruba controllers to determine the operational state of external devices without custom software development or vendor lock-in. By health checking a pool of devices, the system ensures that traffic is not redirected to a device that is down.



WWW.ARUBANETWORKS.COM

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