aruba
a Hewlett Packard Enterprise company

TECHNOLOGY BRIEF

POLICY ENFORCEMENT FIREWALL FOR DYNAMIC SEGMENTATION

As enterprise networks become the catalyst for digital transformation and connectivity becomes ubiquitous, new policy enforcement and cyber security solutions are required to deal with challenges to traditional network and security approaches. IoT devices are joining employees, customers and guests on corporate wireless and wired networks in an ever-changing perimeter. Standard defenses such as firewalls that use rules and physical network configuration based on IP addresses are no longer adequate.

POLICY ENFORCEMENT FIREWALL (PEF)

New attacks on the inside are being designed to evade and exploit traditional security defenses. They often dwell in the network for weeks or months only to extract, fatally encrypt data, or otherwise compromise IT resources when least expected. At the same time, IT lacks visibility into the application layer – directly impacting network performance and end-user experiences.

As a leader in wireless and wired networking, Aruba, a Hewlett Packard Enterprise Company, has pioneered the use of comprehensive edge-based cyber protection that includes military-grade encryption and a specialized identity-based access solution called the Policy Enforcement Firewall (PEF). PEF runs on ArubaOS and InstantOS, and is a proven technology that runs on **over 4 million installations worldwide**. It is the only user- and device-facing firewall that provides a "zero trust" boundary at the point of access.

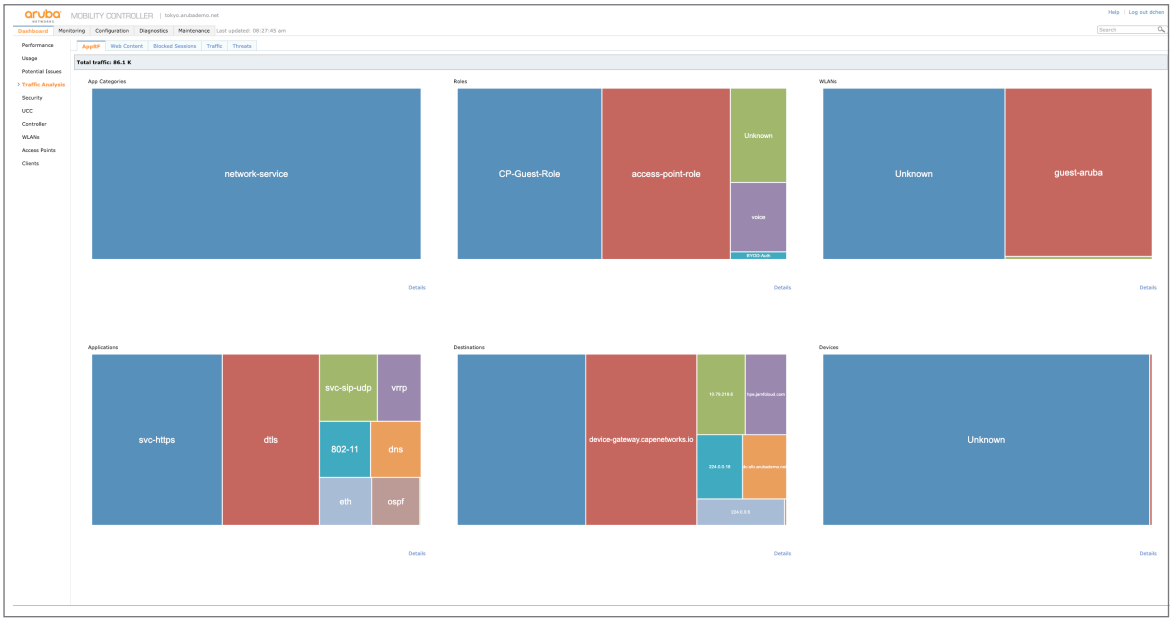
Traditional firewalls that leverage IP-based VLANs for control and only become active after a user or device is admitted to the network leave a tempting opening for advanced attacks. Instead, Aruba's user and application firewall approach with PEF covers this vulnerability by using identity, traffic attributes and other security context to centrally control access privileges at time of initial connection. Filling this gap is essential when each second an attacker is connected to the network can mean unleashing thousands of malware packets.

KEY BENEFITS

- **Centralized, Zero Trust Access:** Reduces the gap between initial network connection and traditional firewall enforcement
- **Cyber Catalyst℠ by Marsh:** Helps qualify for enhanced cyber insurance policy terms from select insurers based on PEF's ability to reduce risk
- **User and application firewalls:** Role-based access control minimizes configuration error
- **No additional hardware required:** PEF runs on existing Aruba network infrastructure
- **Streamlined performance:** Includes hardware-accelerated traffic processing
- **Automated self-learning:** Provides insightful network and application usage data
- **Reusable policy library:** Makes it easy for administrators to create useful, consistent policies
- **Connection Independent:** Roles follow users and devices across wried, wireless and remote connections
- **Security certifications:** Full range of government sponsored validation

A CYBER CATALYST℠ DESIGNATED SOLUTION

Organizations using Aruba's Policy Enforcement Firewall technology can implement a zero trust access model that uses identity, traffic attributes and other context to centrally enforce access privileges at the time of an initial connection. Because of technology and ability to dynamically enforce secure role-based policies, Aruba Policy Enforcement Firewall has been designated "Cyber Catalyst℠" based on its ability to effectively reduce risk.



ArubaOS dashboard view: Visibility into 3000+ applications

SIMPLE AND SECURE NETWORK ACCESS

PEF is also the underlying technology that enables Dynamic Segmentation, a key technical solution within Aruba's Experience Edge that simplifies and secures wired and wireless networks. Through user and application controls, IT can eliminate the need to add VLANs, SSIDs, or ACLs – dramatically reducing complexity.

PEF's application visibility feature enables network administrators to gain rich insight into the applications that are running on the network – and who is using them. WebCC is a subscription-based add-on feature that enhances PEF by including URL filtering, IP reputation and geo-location filtering.

STRONG AUTHENTICATION AND ROLE-BASED CONTROL FOR ZERO TRUST PROTECTION

To start, during the network sign-on process the identity of each user or device is verified via integration with Active Directory (AD), RADIUS, LDAP, SQL databases, LDAP-based identity stores or guest database. Once identity is established, a role is assigned. A role is a logical grouping of permissions that include application access rights and inter-user or device communication.

The value of associating a user with a role is that if a user's security context changes (e.g. the device is compromised) the access permissions can be immediately changed by simply assigning a new, more restrictive role without requiring network re-configuration.

Once the role of the user or device is assigned, policies are applied based on an organization's protection priorities. These policies follow the user throughout the network and are applied uniformly across wireless, wired and VPN connections. If devices are not registered in a directory, default policies based on the fingerprinted device type can be applied (e.g. "All television screens are given access to DNS, DHCP, and Internet-based HTTPS services but not to internal resources").

A recognized user connecting to a PEF-controlled access network will initially be assigned a role (e.g. "hospital HR manager") and it will come with a set of IT permissions. In this case, the administrator will be allowed access to only those tools and network services required for their job: email, Microsoft Office, and employee records—but not patient health care information. If the user is compromised, a new role ("potential compromise, send to quarantine") will automatically be applied and enforced.

As a result, PEF eliminates the arduous, manual and error-prone task of determining and changing a VLAN configuration while providing precise and real time enforcement.

And, because PEF utilizes deep packet inspection, it has **Layer 7 application awareness and recognizes over 3,000 applications**. As a result, traffic separation can be as granular as a single user or device for one specific application—a technique that is impractical with VLAN-based approaches.

RICH APPLICATION VISIBILITY

Rich application visibility with Deep Packet Inspection (DPI) can be used to troubleshoot application performance in real-time, set global policies, and plan for future growth.

The built-in dashboard gives IT a simple, powerful view of mobile application usage and performance that can be sorted by user role, application, network and other criteria:

- **Mobile applications:** Distinguish 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's technology resolves the destination address to identify unique applications like Facebook, Twitter, Box, WebEx and hundreds of others.
- **Encrypted applications:** For encrypted traffic, Aruba uses heuristics to look for traffic patterns and establishes a unique fingerprint to identify those applications.

POLICY-BASED TRAFFIC MANAGEMENT AND CONTROL

PEF features controls that optimize traffic 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. 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.

QUALITY OF SERVICE CONTROLS

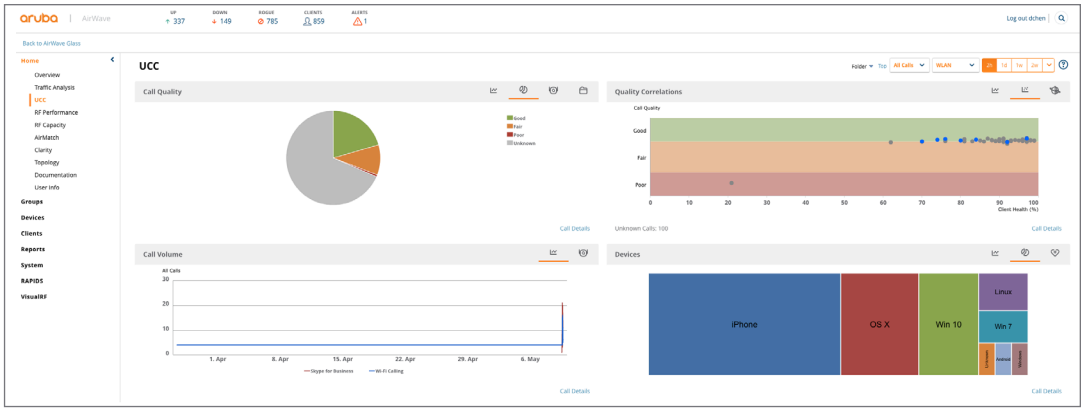
After mobile apps are identified and visualized, access controls and policies can be applied to prioritize the performance of enterprise applications over personal ones. As mobile devices contend for Wi-Fi bandwidth, PEF protects the apps you care most about.

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 Teams or Skype for Business 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 the network 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.



Aruba UCC dashboard view

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.

For critical unified communications (UCC) services, knowledge of call status and quality enables smarter VoIP management. AI-powered smarts with Aruba's AirMatch and ClientMatch RF optimization technologies mitigate any disruption to active sessions.

OPTIMIZED EXPERIENCE FOR UCC

With an integrated UCC dashboard, Aruba provides a simple visualization of key call quality metrics for a variety of UCC applications including Microsoft Teams, Microsoft Skype for Business, Apple FaceTime, Wi-Fi calling, Jabber/Spark and SIP.

By hovering and clicking directly on the dashboards, you can get detailed reporting and troubleshooting information, such as phone number association, call quality tracking, call detail records (CDRs) and call admission control (CAC).

The dashboard includes:

- Call Quality and Correlations – These graphs displays the AP-to-Client call quality under the WLAN tab and the end-to-end quality including wired and wireless legs of the call under the End-to-End tab.
- Call Volume – This graph displays the total number of calls made based on the UCC application type. For example, SIP, Lync, SCCP, H.323, NOE, SVP, VOCERA, and FaceTime.
- Devices – This graph displays the breakdown of voice sessions by device type. For example, iPhone, OS X, Win 10, etc

HIGH-PERFORMANCE TRAFFIC PROCESSING

With PEF, policy enforcement does not come at the expense of performance nor 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.

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 denylist.

REDUCE MEAN TIME TO ATTACK RESPONSE

By avoiding VLAN-based network configuration to enforce controls, the resources required to implement IT access policies are dramatically reduced and attack response can be automated.

With PEF's fine-grained control, attacks on the inside that co-opt legitimate credentials and patiently expand throughout the network are effectively throttled. If the user or device has a role with a narrow set of access permissions, so will the attacker. Lateral spread is contained.

Once an attack such as data exfiltration or ransomware is detected, PEF can automatically change the permissions associated with the user or device by changing the role. Attack responses can include a range of actions from bandwidth reduction, quarantining and outright block. Attack alerts can come from any of the security products that are in an organization's security ecosystem based on simple API integrations.

INTEGRATION WITH CLEARPASS POLICY MANAGER

The Policy Enforcement Firewall is a self-contained access control solution that optionally integrates with Aruba's ClearPass Policy Manager. ClearPass provides the ability to streamline the authentication and policy definition services that are delivered to PEF for centralized enforcement at scale. A key benefit of ClearPass is that it consolidates the authentication and authorization access control functions, from an individual office to a global enterprise.

ClearPass also supports the integration of policy, role enforcement and attack response with over 140 Aruba technology partner solutions from mobile device management to help desk solutions such as ServiceNow.

THE HIGHEST LEVEL OF SECURITY CERTIFICATION

Aruba's Policy Enforcement Firewall (PEF) is NIAP-accredited under the Common Criteria and DoDIN-APL. PEF is also on the NATO approved product list.

EASE OF IMPLEMENTATION

To ensure that IT can easily implement and secure their environment, PEF is available as a separately licensed software option in the Aruba Operating System (AOS) for controller-based infrastructure and is included in the licensing of controller-less access points. It is also delivered to Aruba network switches through Dynamic Segmentation. No additional hardware required.

SUMMARY

Because traditional firewalls utilize VLAN-based policy enforcement after access is achieved, IT teams are struggling to keep pace with neutralizing attacks that start at time of network connection. Aruba's User firewall approach through PEF is the only access control solution built to deliver a Zero Trust boundary at point of network connection, based on the identity and role of a user or device, regardless of location, method of connection or device type.

With the granular access permissions that PEF enforces, organizations can keep compromised users and devices from participating in an attack with precision isolation and by automatically blocking or quarantining the endpoint when an attack is detected.

Because PEF is implemented as a software solution on existing Aruba network infrastructure, no additional hardware installation is required to ensure that only identified and authorized users and devices are connected to the network.

FEATURE SUMMARY	
Feature	**Benefit**
Fully Stateful Layer 4-7 application visibility	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
User Firewall	AllAllows role-based policies to be set for the user, device type, application, or destination
UCC Dashboard	View call quality metrics such as MOS and health for UCC services like Teams and SIP
Application Aware QoS	Enables administrators to prioritize application traffic and control RF layer behavior
Real-Time Application 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
ClearPass and external RADIUS integration	Authenticate users, allow third party devices or ClearPass to do detailed device identification and dynamic policy updates

Cyber Catalyst

In the Cyber Catalyst℠ program, leading cyber insurers evaluate and identify solutions they consider effective in reducing cyber risk. Participating insurers include Allianz; AXIS; AXA XL, a division of AXA; Beazley; CFC; Munich Re; Sompo International; and Zurich North America. Microsoft is a technical advisor to the program.

aruba
a Hewlett Packard Enterprise company

TB_PEF_101420 a00073442enw