PARTNER SOLUTION OVERVIEW

Aruba & Palo Alto Networks
Next-Generation Firewall and Network Access Control

As the trend toward a more flexible, productive network topology grows, the challenge is to incorporate the security and control a mobile-first architecture needs to cover both wired and wireless connectivity. How can an organization’s networking and security teams centrally define policies and controls that apply whenever and wherever users and devices connect? What happens when a legitimate user or device is compromised after connecting?

In addition, organizations face an onslaught of headless and internet of things (IoT) devices connecting to the general IT infrastructure. Many of these devices are plugged into the network and introduce new vectors.

Aruba ClearPass is a proven network access control and policy management solution that can discover, profile, authenticate, and authorize any network access on wired or wireless networks, including for bring-your-own-device (BYOD) practices and headless IoT/OT devices. Its position as network gatekeeper enables secure network access and accelerated attack response. The Palo Alto Networks Security Operating Platform prevents successful cyberattacks through intelligent automation. Together, Aruba and Palo Alto Networks deliver powerful integrated capabilities. Aruba ClearPass Secure NAC provides real-time user-to-device mapping and device health checks, using Next-Generation Firewall policies and rules to detect changes in user or device behavior—large or small—that often indicate insider attacks. This combined offering provides superior visibility into IoT and corporate devices on the network, allowing you to enforce firewall policies and application access based on user identity and device security posture.

HOW IT WORKS

Aruba ClearPass provides total visibility of connected and connecting users as well as devices in wired and wireless multi-vendor environments.

WHY ARUBA AND PALO ALTO NETWORKS

- Applies enhanced user and device context, including role, device health, and more, to Next-Generation Firewall rules and policies for protection against unsanctioned traffic.
- Protects users on the network from threats such as phishing, malware, and exploits.
- Stops unauthorized users and devices by implementing a single policy of authorization and enforcement across wired and wireless networks, up to the application level, for users and IoT devices.
- Enables closed-loop attack detection via Next-Generation Firewall and policy-based response with ClearPass.

ClearPass delivers user identity to User-ID technology and device information to the Host Information Profile (HIP), enabling Palo Alto Networks Next-Generation Firewalls to enforce real-time rules based on user, device, and application at every point of control. Conversely, when a Next-Generation Firewall generates an alert, it can be sent to ClearPass to trigger a range of predetermined, policy-based actions, from quarantine to blocking. This seamless, automated enforcement can help prevent one compromised machine from becoming a thousand.

ClearPass collects and aggregates user and device data from Palo Alto Networks Next-Generation Firewalls, either directly from the device or from aggregation points, such as security information and event management (SIEM) products.
1. Client devices attach to network and are profiled by ClearPass Policy Manager.

2. Detailed user and device profiling data are sent to Palo Alto Networks Next-Generation Firewall.

3. Firewall takes user, device and application profile data to permit/deny and log applicable traffic.

Figure 1: Aruba and Palo Alto Networks Joint Solution Diagram
**USE CASE NO. 1: SECURE USE OF EMPLOYEE-OWNED DEVICES AND STOP UNAUTHORIZED NETWORK ACCESS**

**Challenge**
Modern enterprises incorporate a distributed workforce (HQ, branch, remote, and on-the-go) and must unify the operations of an exponentially growing number of users and devices as well as stop unauthorized use on the corporate network.

**Solution**
Integration between the Next-Generation Firewall and ClearPass Policy Manager stops unauthorized access. ClearPass initially profiles client devices detected on the corporate network, providing total visibility of connected and connecting users in both wired and wireless environments. The Next-Generation Firewall examines user and device profiling data to determine the right of access.

**Benefit**
Granular user and device access control, combined with visibility into the corporate network, strengthens overall security posture. The integrated solution stops unauthorized users and devices by implementing a single policy of authorization and enforcement across wired and wireless networks, up to the application level, for users and IoT devices.

**USE CASE NO. 2: MAINTAIN FULL VISIBILITY AND GRANULAR CONTROL OF USER ACCESS TO CORPORATE APPLICATIONS AND DATA**

**Challenge**
Prevent users from accessing inappropriate content on the corporate network (wired or wireless) as well as ensure the privacy of the organization’s intellectual property and application data.

**Solution**
Palo Alto Networks Next-Generation Firewall integrates with ClearPass Policy Manager to provide granular access control and visibility into corporate users and their profiles for application access. HIP attributes are passed from ClearPass to the Next-Generation Firewall via HIP Objects. A Next-Generation Firewall that has a GlobalProtect license scrutinizes the received HIP data and thus enforces policy rules. Any anomalies of inappropriate content access will generate alerts from the Next-Generation Firewall, which will be sent to ClearPass, triggering a range of predetermined policy-based actions, from quarantine to blocking.

**Benefit**
This integration enables you to map and enforce security on network devices as well as monitor traffic by users and applications. Granular access control and visibility into the corporate network let you ensure users are acting within the bounds of your organization’s policies. You’re also protected against unsanctioned application access based on user and device context, organization role, access rights, health, and Next-Generation Firewall policy rules. This type of policy-based, real-time enforcement can help prevent the lateral movement of malicious users, whether they are internal employees, contractors, or other third parties.
SUMMARY
Aruba, a Hewlett Packard Enterprise company, is a leading provider of next-generation networking solutions for enterprises of all sizes worldwide. The company delivers IT and cybersecurity solutions that empower organizations to serve the latest generation of mobile-savvy users who rely on cloud-based business apps for every aspect of their work and personal lives.

DEPEND ON PALO ALTO NETWORKS
Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. They are headquartered in Santa Clara, California.

www.paloaltonetworks.com Phone: 408-753-4000
3000 Tannery Way, Santa Clara, CA 95054