PALO ALTO NETWORKS AND ARUBA

Technology Segment: Network Security Configuration Management

BENEFITS

- Applies enhanced user and device context, including role, health and more, to NGFW rules and policies for protection against unsanctioned traffic.
- Protects network users 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 NGFW and policy-based response with ClearPass.
- Leverages existing NGFWs to provide a new dimension of machine learning-based attack detection for insider attacks.
- Enables comprehensive, cloud-based logging.

The Challenge

As the trend toward more flexible, productive network topology grows, the challenge is how to incorporate the security and control a mobile-first architecture needs to cover both wired and wireless connectivity. How do 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, or IoT, devices connecting to the general IT infrastructure. Many of these devices are plugged into the network and introduce new vectors for vulnerabilities.

Overview

Aruba® ClearPass™ is a proven network access control and policy management product that can discover, profile, authenticate and authorize any network access on wired or wireless networks, including for BYOD and IoT devices. Its position as network gatekeeper enables secure network access and accelerated attack response. It integrates with Aruba IntroSpect™ User and Entity Behavior Analytics and can be deployed on any vendor's network infrastructure.

Aruba IntroSpect UEBA is a network-agnostic family of continuous monitoring and advanced attack detection software. It uses machine learning to detect changes in user and device behavior indicative of attacks that have evaded traditional security defenses. Machine learning algorithms generate risk scores based on the severity of attacks, along with the associated forensic information, to speed up incident investigations for security teams.

Together, Aruba and Palo Alto Networks® deliver a powerful approach that integrates with the Palo Alto Networks Security Operating Platform. Aruba ClearPass Secure NAC provides real-time, user-to-device mapping and device health checks. Aruba IntroSpect UEBA makes use of Palo Alto Networks next-generation firewall, or NGFW, logs to detect changes in user or device behavior, large or small, that often indicate insider attacks. Both products generate logs and alerts that can be sent to the cloud-based Palo Alto Networks Logging Service. This combined offering brings you superior visibility into corporate, IoT and devices on the network, allowing you to enforce firewall policies and application access based on user identity and device security posture.

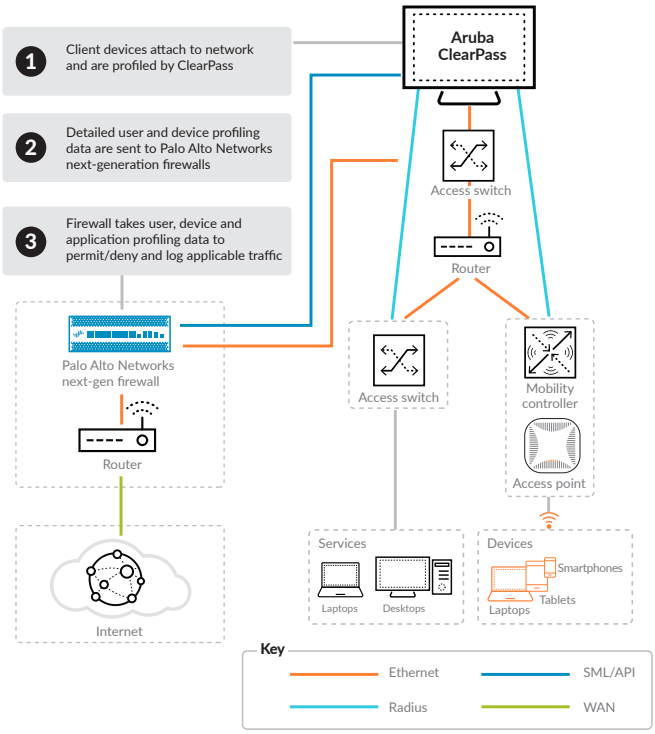

Figure 1: ClearPass integration with Palo Alto Networks NGFW

Integration

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

ClearPass delivers user identity to User-ID™ technology and device information to the Host Information Profile, enabling Palo Alto Networks NGFWs to enforce real-time rules based on user, device and application at every point of control. Conversely, when an NGFW generates an alert, it can be sent to ClearPass to trigger a range of predetermined, policy-based actions, from quarantine to blocking.

IntroSpect collects and aggregates logs from Palo Alto Networks NGFWs, either directly from the device or from aggregation points, such as security information and event management, or SIEM, products.

IntroSpect UEBA builds baselines of normal user and device behavior with machine learning to find previously unknown insider attacks. When deviations occur, IntroSpect can update a user or device risk score and generate an alert for the security team. IntroSpect is designed to use your existing security infrastructure, and it is especially well-suited to use NGFWs as key sources of network activity to help build and monitor baselines. NGFWs and IntroSpect seamlessly integrate via tightly coupled log collection and parsing.

IntroSpect and ClearPass generate a variety of logs and alerts, all of which can be sent to the Palo Alto Networks Logging Service for storage and subsequent analysis.

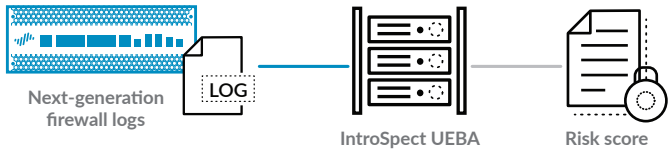

Figure 2: Risk score processing

About Aruba, a Hewlett Packard Enterprise Company

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. To learn more, visit Aruba at http://www.arubanetworks.com.

About Palo Alto Networks

We are the global cybersecurity leader, known for always challenging the security status quo. Our mission is to protect our way of life in the digital age by preventing successful cyberattacks. This has given us the privilege of safely enabling tens of thousands of organizations and their customers. Our pioneering Security Operating Platform emboldens their digital transformation with continuous innovation that seizes the latest breakthroughs in security, automation, and analytics. By delivering a true platform and empowering a growing ecosystem of change-makers like us, we provide highly effective and innovative cybersecurity across clouds, networks, and mobile devices.

Find out more at www.paloaltonetworks.com.

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com