aruba
a Hewlett Packard Enterprise company

SOLUTION OVERVIEW

UNIFIED ACCESS SECURITY WITH ARUBA CLEARPASS AND PALO ALTO NETWORKS

PROTECT YOUR NETWORK, COMING AND GOING

Over 30,000 companies in 140 countries, and over half the Global 2000 rely on Palo Alto Networks next-generation security platform to combat today's advanced threats that come through their front door. But it's easy to forget that some of the most damaging attacks also come from behind the lines.

The volume and diversity of mobile devices that connect at work are challenging the effectiveness of physical network security and endpoint health. And IT can lose control without the right tools. More than ever, an inside-out security model that addresses the inherent insecurity of devices and users must become a priority.

Aruba ClearPass fortifies your posture by defining specific resources users and their devices can access. Combined with Palo Alto Networks next-generation security platform, access layer changes are now shared with the network firewall for strong gateway protection of all traffic that's coming and going.

Palo Alto Networks and ClearPass benefits

- Holistic threat protection from inside and outside sources.
- Block unauthorized users and devices before they access your internal network.
- User and device context shared from the point of entry with Palo Alto Networks next-generation firewalls for better security and protection against unsanctioned traffic from within the enterprise.

CAPABILITIES CHECKLIST

ClearPass provides Palo Alto Networks next-generation firewalls with enhanced user and device information for use by Palo Alto Networks Panorama central management system.

Palo Alto Networks Policy Enforcement Capabilities Using:	Palo Alto Networks next-generation firewalls	ClearPass + Palo Alto Networks next-generation firewalls
IP address only	✓	✓
User identity (AD/LDAP user) + IP address	✓*	✓
User identity (non-AD/non-LDAP) + IP address		✓
User identity (guest network) + IP address		✓
User and device type identity + IP address		✓

* Requires PAN in-line profiler agent

FREQUENTLY ASKED QUESTIONS

Q: Do Palo Alto Networks next-generation firewalls have native user identity profiling capabilities in its policy framework? When do I use ClearPass?

Palo Alto Networks next-generation firewalls support user and device identity profiling but require integration with data sources like AD and LDAP for the information. ClearPass provides a broader view as the authoritative firewall profiling source for users and devices (enterprise and guest) along with headless office automation devices.

Q: Does Palo Alto Networks/ClearPass integration require additional Aruba hardware?

No. ClearPass excels in any wired/wireless multivendor environment, including Cisco, HP, Dell, Juniper, and Aruba. ClearPass also integrates with a variety of identity stores to bring user visibility to Palo Alto Networks beyond Active Directory / LDAP.

Q: Where else can ClearPass help?

Through powerful inbound/outbound APIs, ClearPass can publish and subscribe to contextual data from other multivendor enterprise systems. ClearPass also supports native capabilities like policy management, personal device configuration, certificate authority and distribution, device health, and best-in-class guest management.

CLEARPASS INTEGRATION WITH PALO ALTO NETWORKS NEXT-GENERATION FIREWALL

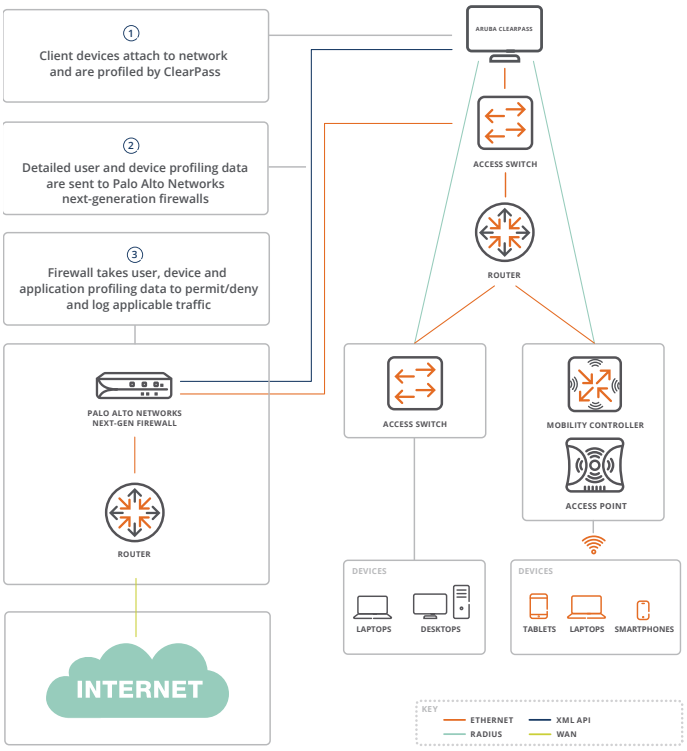

figure 2.0_032416

a Hewlett Packard Enterprise company

1344 CROSSMAN AVE | SUNNYVALE, CA 94089
1.866.55.ARUBA | T: 1.408.227.4500 | FAX: 1.408.227.4550 | INFO@ARUBANETWORKS.COM

www.arubanetworks.com