aruba
a Hewlett Packard Enterprise company

SOLUTION OVERVIEW

NEXT-GENERATION SECURITY FOR MOBILE ENTERPRISE

EXTENDING ADAPTIVE TRUST ACROSS DISTRIBUTED ORGANIZATIONS

Today's mobile users have rendered the traditional enterprise network perimeter obsolete. Armed with three or more devices, these users continuously test network boundaries and force IT to accommodate anywhere, anytime access for everything from email to corporate resources.

Mobility is a double-edge sword. It drives innovation and productivity. But it also creates serious challenges by breaking traditional security architectures and protective mechanisms that weren't designed to accommodate the worker that's always on the move.

The trust models established for corporate-owned devices don't apply in a BYOD world. Smart devices bypass traditional security controls and are walked right through the front door onto the network – often without IT's knowledge.

Trust can no longer be assumed just because a user authenticates through Active Directory. In a mobile world filled with smartphones, tablets and laptops, trust must be earned, validated and constantly assessed to ensure that access rights, threat levels and risks are properly accounted for.

These challenges are made worse when data protection, mobility and other resources are extended to branches, satellite offices, remote campuses, and teleworkers. Cost and complexity can limit the ability to fully replicate services across all locations, resulting in inconsistencies and compromises that threaten security.

To overcome these challenges, Palo Alto Networks and Aruba have teamed-up to deliver the industry's first security framework designed for today's anywhere, anytime workforce – Adaptive Trust™. The solution combines market-leading Wi-Fi mobility and access controls with next-generation cybersecurity and advanced threat protection.

PROTECTING MOBILE HEADQUARTERS AND CAMPUSES

Adaptive Trust security requires identification, authentication, and validation of every user, device, and application based on contextual policies defined by IT. These policies are rigorously enforced by Aruba Mobility-Defined Networks™ and the Palo Alto Networks next-generation firewall.

ARUBA AND PALO ALTO NETWORKS PARTNER TO PROVIDE ADAPTIVE TRUST SECURITY

- **Uniform protection** – Easy, cost-effective and consistent threat prevention from the data center to all branches and remote locations.
- **Enforcement built for mobility** – Leverage roles, applications, traffic types, and other contextual data to provide appropriate network access from anywhere while blocking the most sophisticated threats and zero-day exploits.
- **Context-based policies** – User roles, device types/status, device ownership, and location are shared with Palo Alto Networks to dynamically respond to mobile risks and threats.
- **Enhanced Visibility** – Dynamic profiling of devices provides valuable context for accurate device-level policy enforcement.
- **User self-service** – Offload device provisioning and guest access helps reduce IT helpdesk tickets while increasing productivity.

Mapping user and device information to network security policies enables IT to govern what a user can access with a particular device and authorized applications. Policies can be very fine-grained, including Wi-Fi bandwidth, quality of service, and location awareness.

As new users and devices connect, Aruba shares contextual data – IP address, device type, and user role – with the Palo Alto Networks firewall. When applications are launched, the firewall classifies traffic and enforces policies according to whom and what is connected.

Users and devices can be quarantined, dropped from the network or surveyed, and applications can be controlled based on whom and what is connected to the infrastructure, or blocked if there's no legitimate use.

Enhanced cybersecurity against known and unknown malware, zero-day exploits, and advanced persistent threats is provided by WildFire™ from Palo Alto Networks. WildFire automatically identifies new, previously unknown malware and immediately delivers intelligences to break the attack kill chain.

Aruba fortifies posture by defining specific resources that users and their devices can access. Combined with the Palo Alto Networks enterprise security platform, access layer changes are now shared with the network firewall for strong inspection and enforcement of security policies for traffic, both coming and going.

Aruba and Palo Alto Networks integration benefits:

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

CONSISTENT PROTECTION FOR REMOTE LOCATIONS

Organizations that use Aruba and Palo Alto Networks GlobalProtect™ and WildFire in the data center and headquarters can easily and cost-effectively extend these security platforms to branches and remote sites via Aruba's Cloud Services Controllers.

The integration uses true zero-touch provisioning. Simply plug in an Aruba Cloud Services Controller and connect it to Aruba 802.11ac or 802.11n APs at the branch. The controller automatically establishes a secure connection and downloads the appropriate configuration and security settings from a centralized Aruba Mobility Controller.

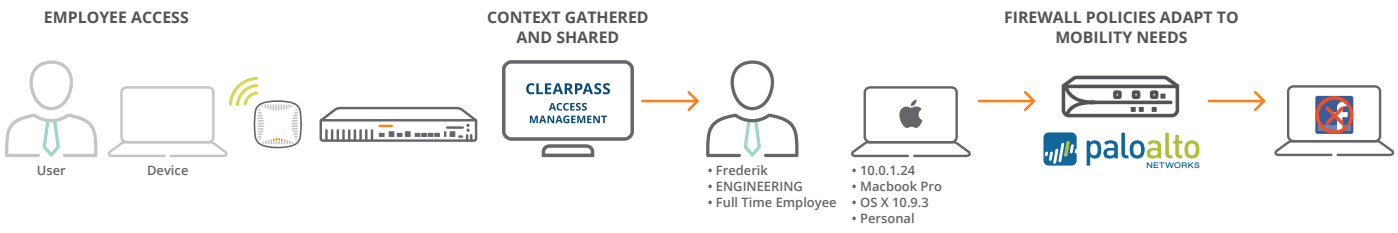
With an automatic connection to the Palo Alto Networks GlobalProtect Gateway, traffic receives the same enforcement of security policy and threat prevention throughout the enterprise and across all branch offices.

Palo Alto Networks GlobalProtect Gateways terminate the VPN connection on a next-generation firewall, and thus provide threat prevention and policy enforcement based on application, user, content, location and device state.

The Aruba Cloud Services Controller automatically establishes a VPN connection to the optimal GlobalProtect Gateway to extend the logical perimeter. Security is enhanced by Palo Alto Networks WildFire advanced threat detection and prevention which provides protection against new mobile threats and malware.

Aruba's Cloud Services Controller integration with Palo Alto Networks GlobalProtect delivers the best mobility and threat protection for every distributed location. Now all distributed enterprises can enjoy the same zero-day protection, uniform policy-enforcement, endpoint protection and enterprise-class mobility across all branch locations.

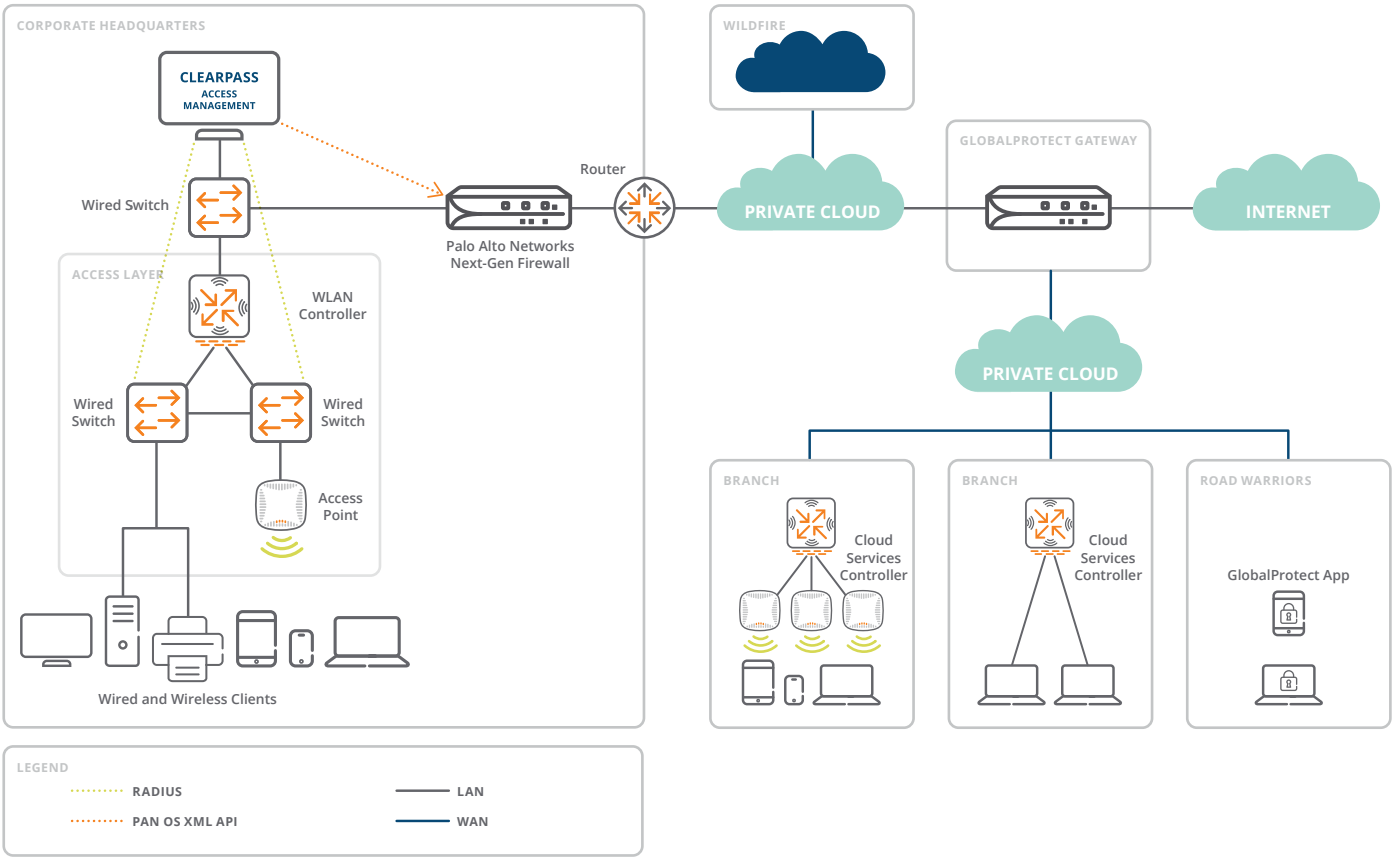
CONTEXTUAL DATA EXCHANGED WITH PALO ALTO NETWORKS FIREWALL



SOLUTION COMPONENTS

- **Palo Alto Networks firewalls** – Single-pass software engine and function-specific processing for networking, security, threat prevention, and management with predictable performance.
- **Palo Alto Networks GlobalProtect** – Blending technology and intelligence to provide a comprehensive solution for mobile security to stop mobile threats, enforce security policies, and protect networks from compromised and non-compliant mobile devices.
- **Palo Alto Networks WildFire** – Continuously analyze files and documents to look for new malicious content, and take immediate action to disseminate intelligence on emerging threats to Palo Alto Networks customers around the globe.
- **Controllerless Aruba Instant™ and controller-managed Aruba Wi-Fi access points (APs)** – 802.11ac and 802.11n access points deliver superb Wi-Fi performance to a wide range or indoor and outdoor environments and remote locations.
- **Aruba 7000 series Cloud Services Controllers and 7200 series Mobility Controllers** – Offering centralized network engineering, IP services and policy controls, while simplifying the integration of security and enterprise app platforms.
- **Aruba ClearPass policy management platform** – Features ultra-scalable AAA with RADIUS and TACACS+ and a policy engine that leverages contextual data based on user roles, device types, app usage and location.

EXTENDING ADAPTIVE TRUST ACROSS DISTRIBUTED NETWORKS



PALO ALTO NETWORKS

Palo Alto Networks is leading a new era in cybersecurity by protecting thousands of enterprise, government, and service provider networks from cyber threats. Unlike fragmented legacy products, our security platform safely enables business operations and delivers protection based on what matters most in today's dynamic computing environments: applications, users, and content. Find out more at http://www.paloaltonetworks.com.

ARUBA NETWORKS

Aruba Networks is a leading provider of next-generation network access solutions for the mobile enterprise. The company designs and delivers Mobility-Defined Networks that empower IT departments and #GenMobile, a new generation of tech-savvy users who rely on their mobile devices for every aspect of work and personal communication.

To create a mobility experience that #GenMobile and IT can rely upon, Aruba Mobility-Defined Networks™ automate infrastructure-wide performance optimization and trigger security actions that used to require manual IT intervention. The results are dramatically improved productivity and lower operational costs.

Listed on the NASDAQ and Russell 2000® Index, Aruba is based in Sunnyvale, California, and has operations throughout the Americas, Europe, Middle East, Africa and Asia-Pacific regions. For more information please visit www.arubanetworks.com.

aruba
a Hewlett Packard Enterprise company

SO_PAN_SK_020519