

THE ARUBA DIFFERENCE

The ClearPass Access Management System provides the foundation for the Aruba Adaptive Trust defense model. It provides central control and mobile security enforcement based on roles, and real-time contextual information on any multivendor network.

This unique approach, based on the ClearPass Exchange common-language integration, enables enterprise organizations to leverage contextual information across security systems for granular and accurate policy enforcement.

ClearPass delivers secure enterprise mobility by integrating policy management with AAA, guest network access, secure onboarding, device health checks, and other self-service capabilities – all from one platform.

ClearPass also enables two-factor authentication by leveraging multiple identity stores within one service, including Microsoft Active Directory, LDAP-compliant directories, ODBC-compliant SQL databases, token servers and internal databases.

Providing an invaluable source of additional context, identity stores can also be utilized to authenticate users and authorize the use of specific enterprise resources.

ClearPass Exchange support for REST APIs and data feeds allows crucial enterprise mobility intelligence to be shared between ClearPass and other security solutions and business workflow systems.

Consequently, Palo Alto® Networks Next-Generation Firewalls can automatically leverage user and device context for granular app-level policies. And EMM applications like MobileIron are now able to share user, device and location visibility for security Wi-Fi enforcement.

CLEARPASS OFFERS A WIDE RANGE OF FEATURES THAT ENABLE SECURE ENTERPRISE MOBILITY

- **Enhanced visibility** – dynamic profiling of devices as they connect provides valuable information that can be used within policies and for troubleshooting.
- **Enterprise-ready policies** – built-in policy service templates deliver where legacy AAA solutions fail. BYOD initiatives and guest access services are created and usable with minutes.
- **Centralized context** – all collected data like location, device type and status, and device ownership is usable and shared with existing security solutions from a central repository.
- **Self-service** – users are allowed to self-configure personal devices, revoke certificates for lost devices and sponsor guest access, which reduces IT helpdesk tickets while increasing productivity for all.
- **Enforcement built for mobility** – managing separate VLANs to enforce network privileges based on traffic types is complex and burdensome. Policies for mobile devices requires leveraging roles, traffic types and other contextual data to automatically direct users to appropriate network segments. VLAN and ACL enforcement is only used when required.

Interaction with helpdesk tools like ServiceNow® automatically initiates a helpdesk ticket with vital information about the user, device and access problem in the event of a network authentication failure.

DATA EXCHANGED WITH OTHER NETWORK TOOLS



figure 2.0_011915_adaptivetrust-wpa

USING ARUBA ADAPTIVE TRUST FOR SECURE ENTERPRISE MOBILITY

ClearPass addresses the needs of the ever-changing policy landscape and replaces point solutions and management headaches with one comprehensive, secure, robust policy management system. This lowers capex and opex while opening a path to create finely-tuned security policies with an emphasis on simplicity and a better user experience for #GenMobile.

By leveraging context from multiple identity stores and authentication methods, ClearPass allows IT to create more granular enforcement policies. This means that corporate-managed and personal devices are treated differently on the same infrastructure.

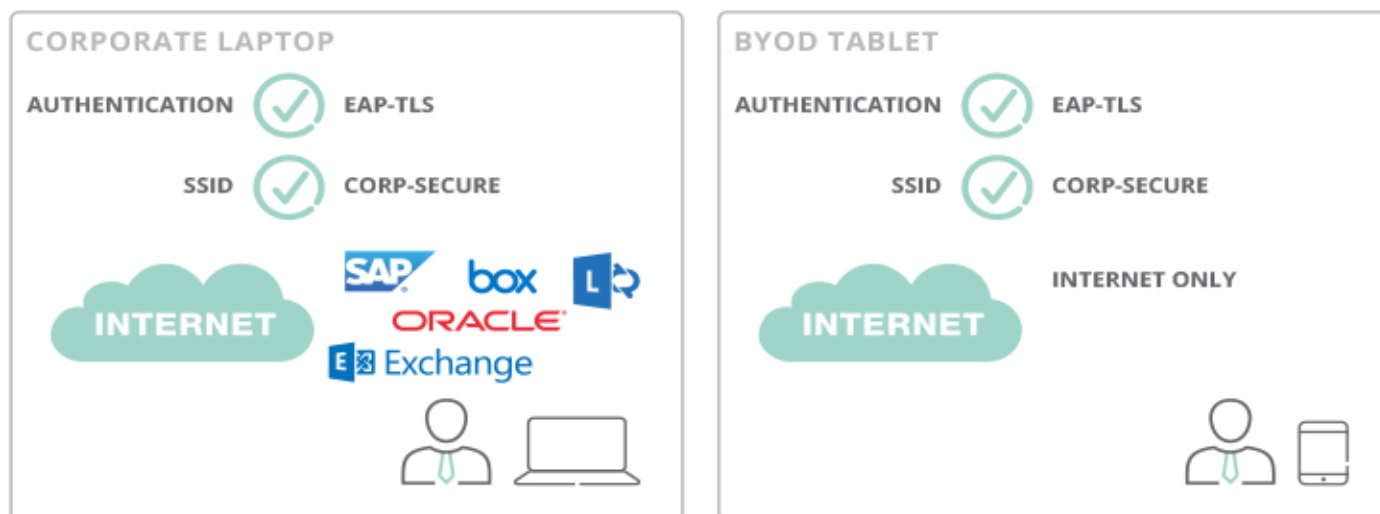
The result is a dynamic, integrated and robust solution that easily adapts network and security functions to the mobile needs of employees, allowing enterprise organizations to quickly tackle a wide range of common challenges.

BYOD AND IT-ISSUED DEVICES ON THE SAME SSID

Instead of broadcasting multiple SSIDs or creating complex VLAN mappings to accommodate BYOD, role-based enforcement and contextual policies let ClearPass easily differentiate access for personally-owned devices.

ClearPass also distributes and provisions device-specific credentials on each BYOD endpoint to limit or revoke access privileges. This dramatically simplifies the access infrastructure while improving security and lowering the provisioning burden on IT.

BYO AND CORPORATE DEVICES ON SAME SSID



ClearPass allows differentiated access on the same SSID based user, device and location information.

figure 3.0_011915_adaptivetrust-wpa

EXTEND IT CONTROLS TO DEVICES AT HOME

Ensuring that personal mobile devices conform to policies is no easy task, especially when they aren't physically connected to the network. ClearPass easily extends policy controls and enforcement to devices that connect from remote locations like home offices.

Persistent and dissolvable agents that are used with computers can likewise be utilized to ensure that all devices are thoroughly assessed and pass health checks before they access the enterprise network.

ClearPass also works with EMM systems, pulling contextual data from smartphones and tablets to trigger enforcement actions for any device requesting enterprise wired, wireless or VPN access. Context can include jailbroken status, white and black-listed apps, device type and more.

PREVENT BYOD ON GUEST NETWORKS

Guest networks allow guests and other VIPs to enjoy Wi-Fi connectivity during their visit, but are often misused by employees who attempt to bypass corporate BYOD policies for a network connection.

ClearPass can quickly determine if a BYOD or IT-managed device belongs on the guest network by leveraging context gathered during device registration and onboarding. This limits the amount of enterprise data that is exposed on open guest networks.

AUTHORIZATION AND ENCRYPTION ON OPEN NETWORKS

Wi-Fi hotspots are a convenient means for remote employees and professionals who travel to stay connected to enterprise resources. Unfortunately, many of these hotspots are vulnerable to a variety of cyber threats and man-in-the-middle attacks.

To eliminate liabilities and safeguard customers, ClearPass offers an easy way to add enterprise-grade security on any public Wi-Fi network. Augmenting the protected extensible authentication protocol (PEAP) framework, ClearPass ensures that each guest sessions is encrypted and thus invisible to anyone trying to sniff Wi-Fi packets.

SUMMARY

Evolving user habits, threats, and mobile devices require a new approach to secure enterprise networks. The #GenMobile way of working has completely diluted the notion of a fixed perimeter – it doesn't exist in a mobile world where users connect and work from anywhere.

To that end, best-of-breed policy management, NAC, network firewall, and EMM systems must find a common way to share and protect enterprise resources. It's time for centrally-managed policies, secure BYOD and guest access workflows that enable IT to deliver secure enterprise-class mobility that minimizes risks.

ClearPass is the heart of the Aruba Adaptive Trust model. It acts as a centralized gatekeeper and contextual store for all user authentication and device data. ClearPass identifies and authenticates users and devices, trust-based rules grant appropriate access privileges based on specific needs.

By employing the Aruba Adaptive Trust model, enterprise IT organizations can ensure that the growing risks associated with mobility are addressed at the point of authentication and beyond, with a higher degree of user and IT satisfaction.

ABOUT ARUBA NETWORKS, AN HP COMPANY

Aruba Networks, an HP company, 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.

To learn more, visit Aruba at <http://www.arubanetworks.com>. For real-time news updates follow Aruba on [Twitter](#) and [Facebook](#), and for the latest technical discussions on mobility and Aruba products visit Airheads Social at <http://community.arubanetworks.com>.



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

©2015 Aruba Networks, Inc. Aruba Networks®, Aruba The Mobile Edge Company® (stylized), Aruba Mobility Management System®, People Move. Networks Must Follow®, Mobile Edge Architecture®, RFPProtect®, Green Island®, ETIPS®, ClientMatch®, Bluescanner™ and The All Wireless Workspace Is Open For Business™ are all Marks of Aruba Networks, Inc. in the United States and certain other countries. The preceding list may not necessarily be complete and the absence of any mark from this list does not mean that it is not an Aruba Networks, Inc. mark. All rights reserved. Aruba Networks, Inc. reserves the right to change, modify, transfer, or otherwise revise this publication and the product specifications without notice. While Aruba Networks, Inc. uses commercially reasonable efforts to ensure the accuracy of the specifications contained in this document, Aruba Networks, Inc. will assume no responsibility for any errors or omissions. WP_AdaptiveTrust_052815