SOLUTION OVERVIEW

CLEARPASS EXCHANGE: SHARE RICH, CONTEXTUAL DATA TO BUILD A COORDINATED AND ADAPTIVE MOBILITY DEFENSE

While billions of Wi-Fi enabled smartphones and tablets connect to enterprise networks, IT is struggling to gain visibility and maintain security. It's a major challenge to ensure security while also delivering an exceptional user experience without creating a provisioning nightmare.

That challenge is complicated by the fact that IT still relies on multiple, disparate systems like network access control (NAC), enterprise mobility management (EMM), policy management, firewalls, guest management, single sign-on solutions, helpdesk and trouble-ticketing systems.

Stringing together numerous point-products has led to complexity, higher costs and compromised security controls. This siloed approach also leads to more time-consuming configuration and manual helpdesk tasks.

IT needs a better, more adaptive way to secure the mobile enterprise. The flexible work habits of today's mobile workforce require dynamic policy enforcement based on contextual data that includes user roles, device types, ownership, location, and app usage.

More importantly, the security products and management systems that have been deployed must be able to exchange this contextual data and work together to provide increased visibility from top to bottom.

Aruba Networks® developed ClearPass Exchange, a baseline feature of the ClearPass Access Management System, to address the need for comprehensive, adaptive security.

ClearPass Exchange is the central decision point for sharing contextual data with a wide range of third-party IT systems, giving you the benefit of a coordinated defense where all components operate as one fully-integrated system.

KEY INTEGRATION ECOSYSTEM: NETWORK SECURITY

figure 1.0a_011515_clearpassexchange-soa

MAKE BETTER-INFORMED DECISIONS

As the gatekeeper for incoming access-layer traffic, ClearPass performs profiling, authentication and authorization of users and devices. In this role, the ClearPass server collects a wealth of valuable and authoritative contextual data such as:

- The identity of users
- The current status and posture of a device.
- The location of the connected user and device.

This contextual data is gathered from numerous internal and third-party systems through one-way and bidirectional communication. To simplify the sharing of context, ClearPass supports a wide array of APIs and protocols, including: SQL, syslog, XML, SOAP, SAML, OAuth2, and HTTP.

For example, using XML APIs, ClearPass Exchange can poll EMM systems for a variety of device information, including manufacturer and model, encryption status, blacklisted and whitelisted applications, and jailbroken status. When EMM systems detect policy violations, they are incorporated into ClearPass' policy decision making.

KEY INTEGRATION ECOSYSTEM: TRANSACTIONS

figure 1.0b_012015_clearpassexchange-soa

ClearPass uses an adaptive-trust approach to define access policies on any multivendor network. All users and devices are assessed before and after they connect to the network to access enterprise resources. Access policies are then adjusted dynamically based on the perceived risk of the connection, which is determined through context.

KEY INTEGRATION ECOSYSTEM: AUTHENTICATION

figure 1.0c_011515_clearpassexchange-soa

Why share context?

After the access decision is made, the rich session context constructed by ClearPass is saved so it can be shared with other systems to help protect your network.

ClearPass Exchange provides context-sharing and seamless integration of ClearPass services with many third-party devices and management systems. Customers benefit from the ability to integrate their own systems, as well as from a spectrum of pre-integrated solutions from Aruba.

For example, Aruba has prepackaged an exchange of information with the Palo Alto Networks next-generation firewall, which strengthens network edge security by enforcing app-level policies at a more accurate user and device level. Likewise, SIEM solutions like Splunk and HP ArcSight can leverage the user, device and location visibility gathered in ClearPass.

ClearPass can also interact with non-network IT systems and helpdesk tools to automatically create and populate tickets with information about a specific user, device and location in the event of an authentication failure.

It's even possible to add mobility context to other IT workflows by extending network, device and user intelligence to cloud-based services such as Twilio, ServiceNow, and Nearbuy/RetailNext.

The result is improved automation, user satisfaction and less time spent on manual IT tasks. Just imagine what else you can do now that the mobility infrastructure is communicating with your security and business systems.

Build-your-own integrated system

Have an innovative idea that requires integration with a customized, non-mainstream system? Aruba makes it easy to build-your-own and share contextual data with non-traditional helpdesk/incident notifications, customer relationship management (CRM), room automation and LED lighting, and many other systems.

KEY INTEGRATION ECOSYSTEM: NOTIFICATIONS

figure 1.0d_011515_clearpassexchange-soa

ClearPass Exchange provides a real-time event framework, customizable outbound APIs and user-friendly forms that make context-sharing integrations between ClearPass and third-party systems a snap.

Outbound HTTP-based RESTful APIs allow ClearPass Exchange to interact with any API-enabled web service using standard HTTP commands. This gives ClearPass tremendous flexibility and extensibility so you can integrate network-triggered workflows with any server you choose.

Aruba has even created a ClearPass Exchange Recipe Site for its social networking Airheads Community (http://community.arubanetworks.com), where members share their build-your-own integration experiences with other ClearPass users.

THE POWER OF PARTNERS

In addition to custom integration, Aruba works with industry-leading partners to natively integrate ClearPass with EMM, firewalls, single sign-on, and many other systems, right out of the box.

ENTERPRISE MOBILITY MANAGEMENT

Featured Integration: ClearPass and MobileIron

Integrating EMM with a NAC system is critical as BYOD and the Internet-of-things endpoints proliferate in the workplace. It lets EMM systems share contextual data about devices and makes it easier to enforce network policies using attributes gathered by an EMM agent.

Fortunately, ClearPass offers rich bidirectional integration with multiple Tier 1 EMM vendors, including MobileIron, AirWatch by VMware, Citrix XenMobile, JAMF Software, IBM, SOTI, and SAP Afaria.

For example, MobileIron's EMM can tell the ClearPass server about a device's posture, its OS version, the apps running, who owns the device, whether the device is personal or corporate-owned, and other information.

This detailed contextual information enables ClearPass to determine whether to allow the device to connect to the network, what resources it is allowed to access once it connects, and actions that the device can perform while connected.

If a user fails to authentication with the network multiple times, ClearPass can trigger a MobileIron notification message directly to the device and trigger the network to automatically quarantine the device or take other corrective action.

Conversely, device posture assessments performed by MobileIron for missing EMM agents as well as blacklisted applications can trigger ClearPass access enforcement, remediation and notifications.

This built-in EMM integration ensures that ClearPass has the necessary device posture information to make the best adaptive trust decisions. Additional notifications and value-added policy events can also be triggered.

JAILBREAK DETECTION WORKFLOW WITH MOBILEIRON

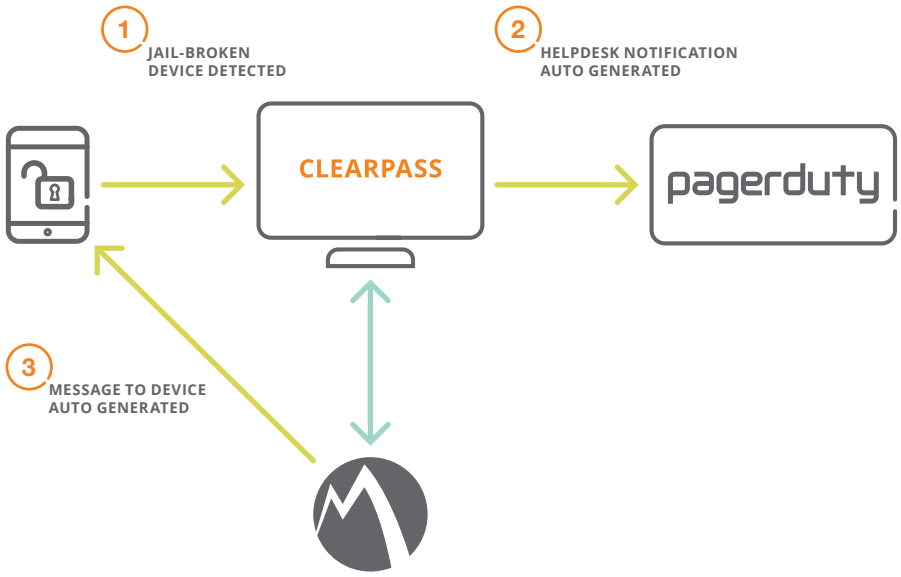

figure 2.0_011515_clearpassexchange-soa

NEXT-GENERATION FIREWALLS

Featured Integration: ClearPass and Palo Alto Networks

Palo Alto Networks next-generation firewalls feature traffic classification that natively inspects all apps, threats and content. ClearPass integration extends the policy enforcement capabilities of these firewalls beyond simple IP address and directory-based user identity information.

Now you can enforce policies based on user and device, guest network, and non-directory identity information. This is crucial to handle the volume and diversity of devices that connect to enterprise networks, and ensures that enforcement rules are applied correctly.

ClearPass integration with Palo Alto Networks firewalls lets you give an iPad user external web browsing privileges to access webmail and social sites, while restricting that same user on a company-issued laptop to external web browsing with no access to webmail and social sites.

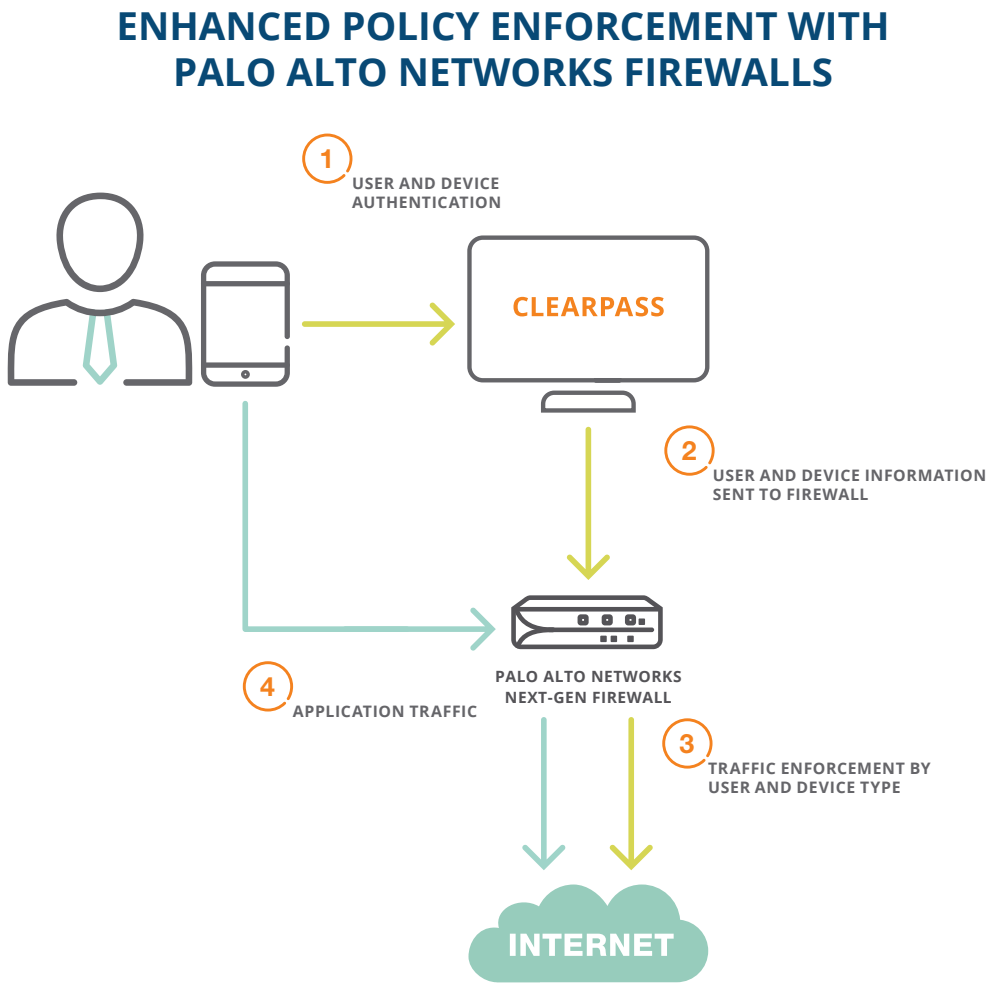

figure 3.0_011515_clearpassexchange-soa

SECURITY INCIDENT EVENT MANAGEMENT (SIEM)

Featured Integration: ClearPass and Splunk

SIEM systems let you aggregate all security events for data correlation and possible coordinated enforcement actions with other systems. Sharing NAC/AAA data with these solutions is essential to any access layer security strategy.

ClearPass integrates with SIEM systems like LogRhythm, HP ArcSight and Splunk to share session logs, audit events, event records and other syslog data. Contextual data shared by ClearPass enables SIEM systems to rapidly pinpoint security threats and policy violations.

The ClearPass App for Splunk lets you visualize ClearPass Policy Manager syslog feeds about employees, contractors, guests and others who connect to your enterprise via wireless, wired and VPNs.

Additionally, ClearPass integration with Splunk makes it easy to track authentication requests, failures and alerts, policy enforcement trends – such as the Top 10 most frequent enforcement profiles applied – endpoint profiles, session details, and other useful information.

SECURITY ANALYTICS AND INCIDENT MANAGEMENT WITH SPLUNK

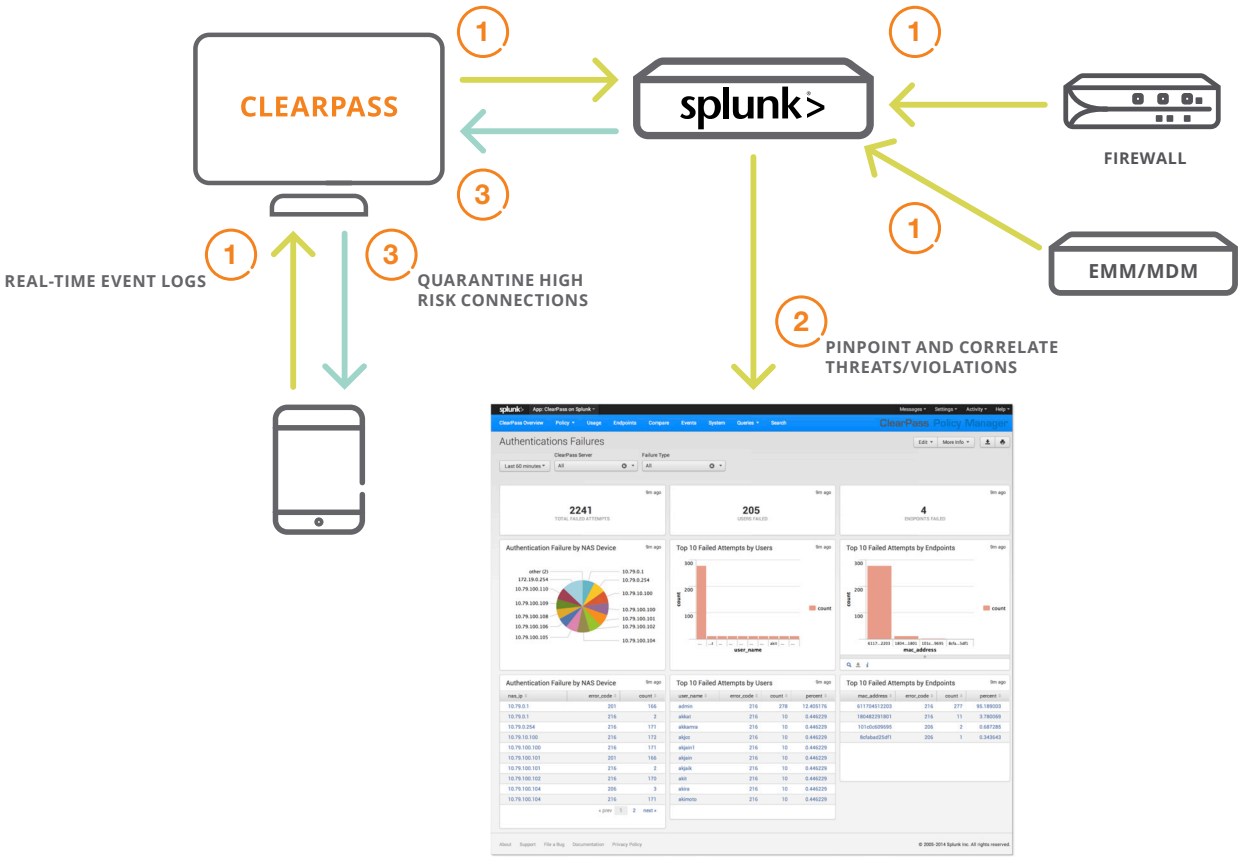

figure 4.0_012015_clearpassexchange-soa

INCIDENT NOTIFICATION SYSTEMS

Featured Integration: ClearPass and PagerDuty

ClearPass integrates with virtually any notification system, including management systems, SMS, traditional email, and call-back voice systems. By integrating with PagerDuty's operations performance platform, for example, ClearPass can notify your operations team about a security event and ensure that they get the message.

Timely event notification and escalation is crucial to reducing response times to incidents that impact employees, customer satisfaction and revenue. ClearPass integration with PagerDuty cuts the volume of unnecessary notifications and lets you rapidly identify and resolve network security issues.

This integration also serves-up performance metrics that can be used to streamline processes and improve the customer experience. Your customer relations staff can be proactively notified when VIP guests arrive or quickly identify hotel guests who need assistance with network access.

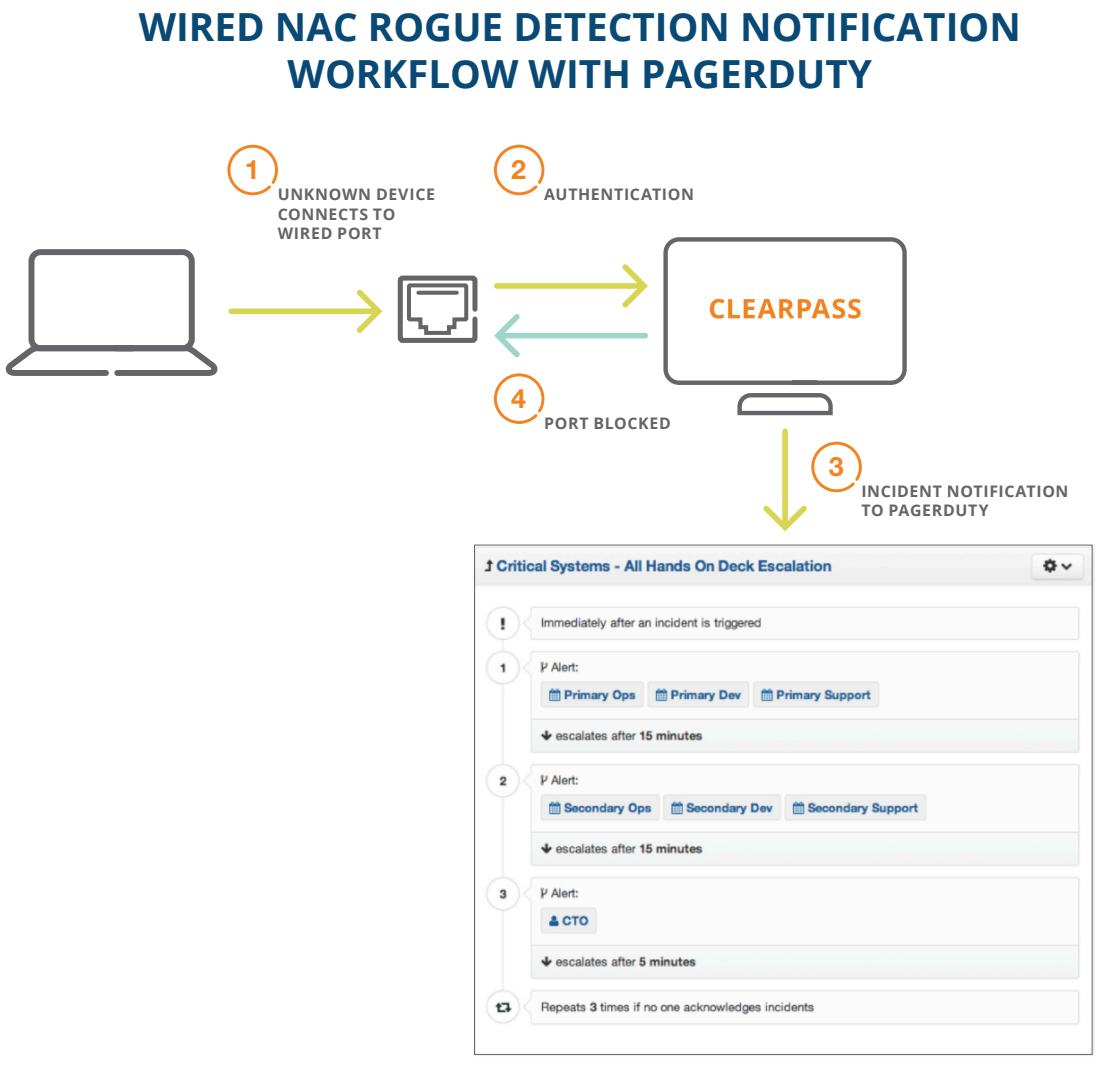

figure 5.0_011915_clearpassexchange-soa

AUTO SIGN-ON FOR APPS

Featured Integration: ClearPass and the IBM Security Access Manager (iSAM)

Managing user authentication and single sign-on for web applications can be challenging as endpoints such as smartphones are increasingly used to access enterprise applications.

With the ClearPass Auto Sign-On capability, once users authenticate to the network, they don't need to repeatedly login again to use their mobile apps. ClearPass validates a user's network login and automatically authenticates the user to their mobile apps.

ClearPass Exchange uses the security assertion markup language (SAML) to extend auto sign-on to third-party systems, including iSAM. ClearPass integration extends iSAM capabilities to include network authentication and device status.

This lets you use real-time authentication attributes to ensure secure access to protected apps across wireless, wired and VPNs. For example, iSAM-for-Web safeguards access to web apps using context-aware access controls with added protection against advanced threats.

By extending auto sign-on to protected web applications, ClearPass Exchange eliminates the need for users to log into iSAM separately. Users enjoy a simpler, more secure connectivity experience while you maintain control of web access.

AUTO SIGN-ON WITH IBM SECURITY ACCESS MANAGER (iSAM)

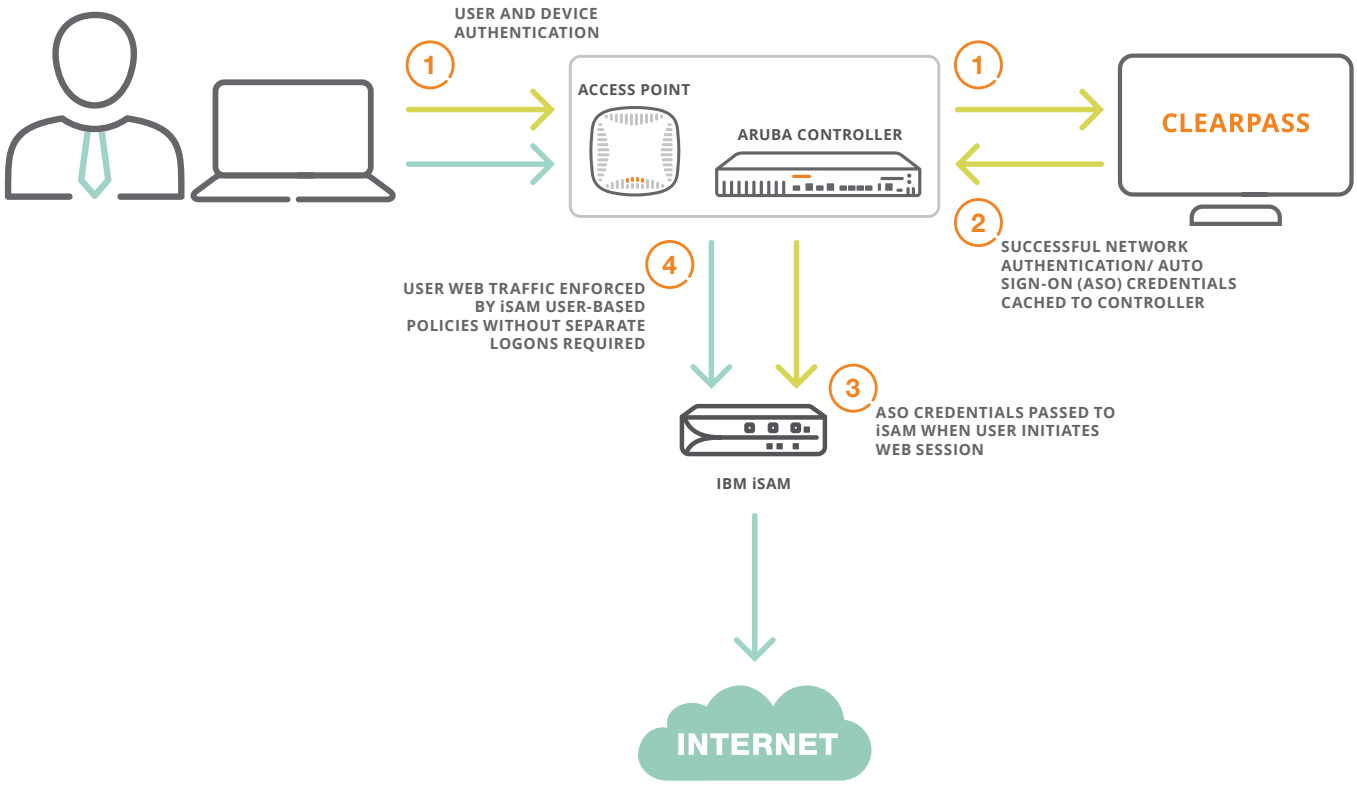

figure 6.0_011915_clearpassexchange-soa

BUILDING AN ADAPTIVE DEFENSE

Integration between best-of-breed IT systems, including the sharing of contextual information, is the key to a coordinated, adaptive security defense. It's the type of security that is needed in today's mobile enterprise, where more and more Wi-Fi-enabled mobile devices are connecting inside and outside of your enterprise security perimeter.

Instead of taking a siloed approach where your security systems are blind to each other's actions, Aruba ClearPass Exchange provides bidirectional visibility through the power of integration.

With ClearPass, it's easy to integrate a variety of systems – from access layer, EMM and network security products to hospitality, payment and messaging systems – and trigger http-based workflow actions with the open platform of your choosing.

IT benefits from greatly enhanced workflow automation. End users benefit from self-service and a vastly improved user experience. And above all, your enterprise benefits from coordinated, adaptive security that's purpose-built for today's dynamic and highly mobile environment.

aruba NETWORKS

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