SOLUTION BRIEF

IBM SECURITY ACCESS MANAGER AND ARUBA CLEARPASS

Redefining authentication and authorization for web applications from any device

IBM Security and Aruba Networks unify network access policy, mobile device management (MDM) and application accessibility for security and convenience.

OVERVIEW

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

IBM's Security Access Manager and Aruba ClearPass provide a uniquely powerful way to extend risk-based access control across multiple application types for consistent security policies.

Customers can now use real-time network authentication attributes to securely provide access to protected applications across wireless, wired and VPN environments.

OVERCOMING APPLICATION ACCESSIBILITY CHALLENGES

The popularity of bring-your-own-device (BYOD) initiatives has challenged IT to provide granular policies for securing access to cloud and mobile applications.

Users today may carry up to three endpoints, which limit the use of generic policies based on static attributes. IT now needs the ability to create context-aware policies that include the status of a user's network authentication as well as risk-based device assessments leveraged from MDM solutions like IBM's Fiberlink MaaS360.

The ideal scenario also ensures a correlation between a user, each device they connect to the network and per session network authentication credentials.

CUSTOMER BENEFITS

- Extends IBM capabilities to include network authentication and device status
- Supports any existing multivendor network and endpoint environment
- Network authentication for Auto Sign-On to protected web applications
- Simplifies traditional user single sign-on limitations

Subsequent access to protected web applications is then granted and differentiated based on device type, risk score and location. Logins to defined web applications will result in no additional username/password challenges.

THE IBM SECURITY AND ARUBA SOLUTION

The ability to provide users with the convenience of an Auto Sign-on to protected web resources using a seamless network logon requires the following components:

- IBM Security Access Manager for Web with ClearPass ISAM plugin (v7.0 or later)
- Aruba ClearPass Access Management System™ (v6.3 or later)
- Aruba Mobility Controller (ArubaOS v6.4 or later)

Optional components can include:

- IBM Security Access Manager for Mobile (v8.0 or later)
- Mobile Device Management – IBM/FiberLink Maas360, MobileIron, AirWatch, Citrix Xenprise or others

IBM® Security Access Manager (ISAM) for Web – safeguards access to web applications using contextaware access controls with added protection against advanced web threats.

IBM® Security Access Manager for Mobile – mobile access security protection enforces contextaware authorization through mobile device finger printing, geographic location awareness, and IP reputation for adaptive, risk-based access.

Aruba ClearPass Access Management System – a single multivendor platform for managing and enforcing role-based access policies for wireless, wired and VPN networks. Provides an external authentication interface for the ISAM suite that grants access based on network authentication and authorization data for Auto Sign-On to web applications.

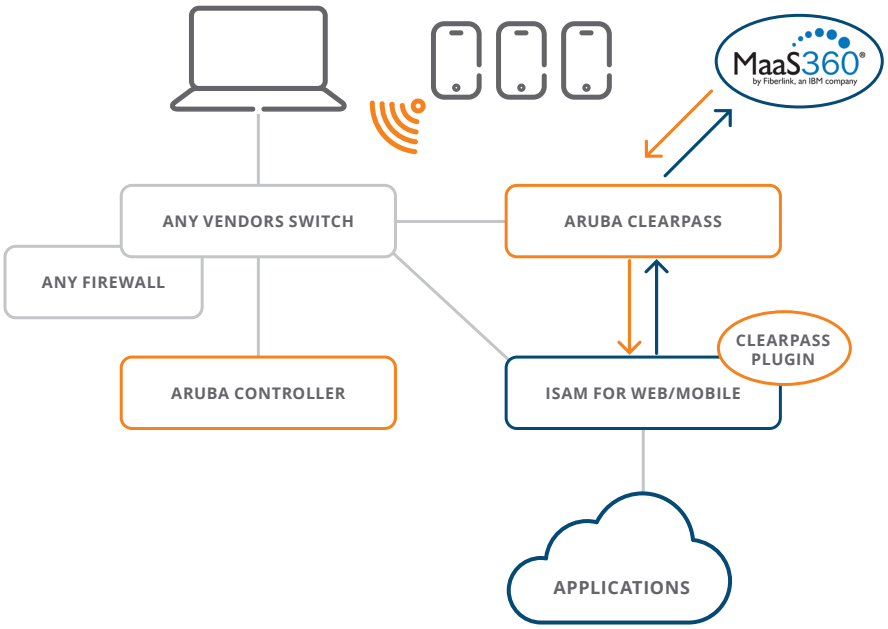
Aruba Mobility Controller – hardened wireless controller that manages system operation functions using an embedded real-time operating system with dedicated packet-processing hardware for all routing, switching and firewall functions. Maintains network authorization state for access to web applications for Auto Sign-On functionality.

SUMMARY

Together, IBM® Security Access Manager for Web and Mobile and Aruba's ClearPass platform provide a risk based access control system for protected web resources and a powerful multivendor policy engine and authentication platform.

Customer value extends beyond network infrastructure interoperability and enhanced security to a new level of user convenience.

Secure authentication and authorization workflow



1. User accesses the network and is redirected to ClearPass for authentication.
2. Policy is enforced based on user role and device and data is shared with the ClearPass ISAM plugin and Aruba Mobility Controller.
3. User requests access to protected ISAM web/mobile resources.
4. ISAM uses the data within the ClearPass ISAM plugin to assess the users request – valid as long as network authentication is current.
5. A successful authentication ensures the identity of the user and provides Auto Sign-On for targeted applications – for each subsequent login attempt.

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