Infoblox
CONTROL YOUR NETWORK

Expand visibility and control while reducing time to attack response – Infoblox DDI Integrates with Aruba ClearPass

SOLUTION NOTE

Introduction

aruba
a Hewlett Packard Enterprise company

Today's enterprise network consists of a large number of network and security devices. All these devices generate their own incidents but these network and security devices don't always share information. This lack of interoperability and inability to share event data results in network and security tools working in silos with no context. If a customer can see all the devices in a single place, he can eliminate silos and respond quickly to security and network changes. According to ESG research report on Security Operations Challenges, Priorities and Strategies in 2017 [1], keeping up with the volume of security alerts and lack of integration between different security tools are biggest challenges related to security operations. According to the same survey, investing in technologies to automate security operations, threat detection technologies and creating security operations technology by integrating multiple tools are the top security operations priorities. Organizations are investing heavily in automation/orchestration of incident response to improve collaboration between cyber security and IT operations team, keep up with volume of security alerts, make decision on prioritizing of alerts and shorten response time for incident response.

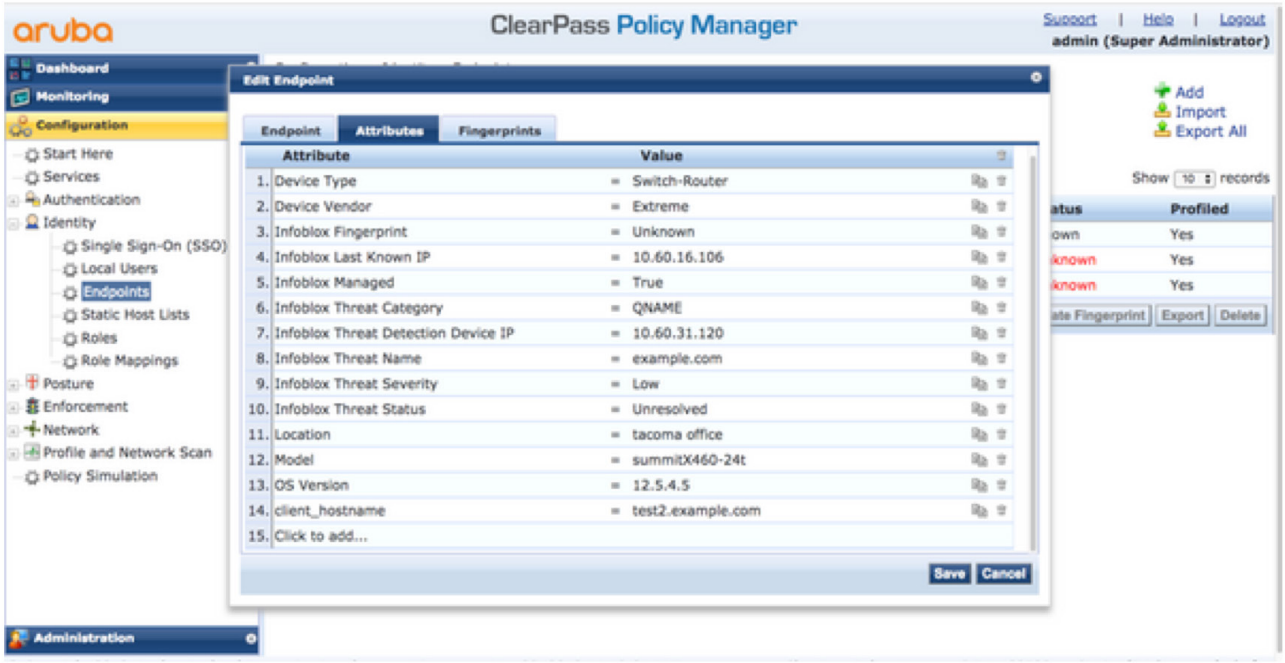
Infoblox and Aruba ClearPass have decided to join forces to help organizations improve their security operations and to reduce time to containment. To allow network and security admins to automatically share information about assets and DNS security events, Infoblox, the market leader in DNS, DHCP and IPAM (DDI), has integrated with Aruba ClearPass Policy Manager. Infoblox sends information on new devices along with IP address as well as Indicators of compromise (IoCs). Aruba ClearPass can then use this information to block or monitor infected endoints using policy-driven actions. As shown in the figure below, customers are able to see information on devices discovered by Infoblox in Aruba ClearPass Policy Manager.

Users can click on the device to get additional information about the device, such as IP address, hostname, device type, device model, and location as shown below. The ClearPass Policy Manager can then optionally fingerprint the device and assign a specific role and access permissions that correspond to IT control policies.

Infoblox
CONTROL YOUR NETWORK

Expand visibility and control while reducing time to attack response – Infoblox DDI Integrates with Aruba ClearPass

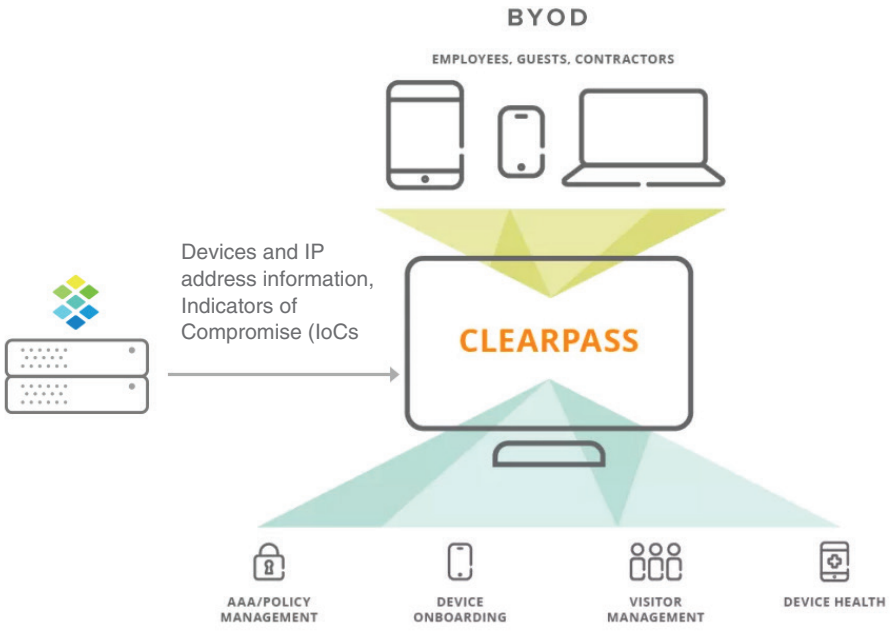
SOLUTION NOTE



Benefits of Infoblox and how is it different?

Infoblox delivers actionable network intelligence to enterprises, government agencies, and service providers around the world. As the industry leader in DNS, DHCP, and IPAM (DDI), Infoblox provides control and security from the core — empowering thousands of organizations to increase efficiency and visibility, reduce risk, and improve customer experience.

The combined solution



Infoblox
CONTROL YOUR NETWORK

Expand visibility and control while reducing time to attack response – Infoblox DDI Integrates with Aruba ClearPass

SOLUTION NOTE

As shown in the figure above, Infoblox sends new end hosts and information about compromised devices to Aruba ClearPass using Outbound Notifications. Aruba ClearPass can use that information and Indicators of Compromise (IoCs) to get context to prioritize threats and take action, thus reducing time to containment.

Thus, benefits of the integration include visibility into new devices and infected hosts in single place, context for prioritization of threats, elimination of silos, faster response to network and security events.

This integration is supported on Aruba ClearPass - minimum code version 6.6.0. However, recommended versions are 6.7.x and higher. For this integration, Infoblox supports Outbound API. Additionally, integration is also supported via Infoblox community web-site.

Summary

From IoT to an always-on mobile workforce, organizations face increasingly complex IT infrastructures that are more exposed to attacks than ever before. By combining Infoblox's DNS security and network visibility with ClearPass' control of access to the network, users can automate their network discovery, profiling and attack response.

Visibility, Control, Response:

Malicious insiders and IoT-based attacks continue to grow, bypassing your perimeter security defenses. With Infoblox and Aruba ClearPass integration you are able to automate the a wide range of adaptive attack responses including re-authentication, bandwidth throttling, quarantine and block.

Certified secure. The best defense for wired and wireless connections:

Malware have become increasingly intelligent, using the DNS in over 90% of its campaigns. With Infoblox and Aruba ClearPass integration you are more protected than ever from DNS attacks and DNS based data exfiltration and DNS Tunnelling with inline protection on Infoblox DNS and policy driven-actions on Aruba ClearPass.

Identify what's on your multi-vendor wired and wireless network:

Automatic population of your Aruba ClearPass endpoints list with Mac addresses that are found by Infoblox so that you can see every network asset with unmatched clarity, context, and insight. In addition to Mac address authentication, ClearPass can authenticate users and devices through a wide variety mechanisms to ensure that the highest level of visibility and control is maintained.

About Aruba, a Hewlett Packard Enterprise company

Aruba, a Hewlett Packard Enterprise company, is a leading provider of next-generation networking solutions for enterprises of all sizes worldwide. The company delivers IT and cybersecurity solutions that empower organizations to serve the latest generation of mobile-savvy users who rely on cloud-based business apps for every aspect of their work and personal lives.

Infoblox
CONTROL YOUR NETWORK

Expand visibility and control while reducing time to attack response – Infoblox DDI Integrates with Aruba ClearPass

SOLUTION NOTE

References

https://www.siemplify.co/resources/2017-esg-research-report-security-operations-challenges/

Other Aruba – Infoblox integrations:

1. Integrating ClearPass with Infoblox typically tags the username context, as well as the external device being authenticated, along with its respective MAC address, which further simplifies IP address management on the Infoblox side. http://www.arubanetworks.com/techdocs/ClearPass/6.7/PolicyManager/Content/CPPM_UserGuide/Admin/EndpointContextServersAdd_Infoblox.htm

2. This integration allows ClearPass to send Username and Mac Address mapping information to Infoblox's Mac Address Filters. https://community.arubanetworks.com/aruba/attachments/aruba/ForoenEspanol/1861/1/ClearPass

3. his integration authenticates a device on Aruba ClearPass and then based on data received from Infoblox through an enforcement profile puts the device onto a chosen network.https://github.com/aruba/clearpass-exchange-snippets/tree/master/ipam/infoblox-authz

About Infoblox

Infoblox delivers Actionable Network Intelligence to enterprises, government agencies, and service providers around the world. As the industry leader in DNS, DHCP, and IP address management (DDI), Infoblox provides control and security from the core—empowering thousands of organizations to increase efficiency and visibility, reduce risk, and improve customer experience.

Corporate Headquarters: +1.408.986.4000 1.866.463.6256 (toll-free, U.S. and Canada) info@infoblox.com www.infoblox.com