aruba
a Hewlett Packard Enterprise company

SOLUTION OVERVIEW

Implementing Zero Trust Best Practices

With Aruba ESP and Edge-to-Cloud Security

Network security challenges have evolved significantly over the years as users have become increasingly decentralized and attacks have become more sophisticated and persistent. Traditional security approaches that focused primarily on the perimeter of the network have become ineffective as stand-alone security strategies. Modern network security must accommodate an ever-changing, diverse set of users and devices, as well as much more prevalent threats targeting previously "trusted" parts of the network infrastructure.

Zero Trust has emerged as an effective model to better address the changing security requirements for the modern enterprise by assuming that all users, devices, servers, and network segments are inherently insecure and potentially hostile. Aruba ESP with Edge-to-Cloud Security improves the overall network security posture by applying a more rigorous set of security best practices and controls to previously trusted network resources.

ARUBA ESP: CORE ZERO TRUST PRINCIPLES

Zero Trust varies significantly depending on which domain of security is being considered. Although application-level controls have been a focal point within Zero Trust, a comprehensive strategy must also encompass network security and the growing number of connected devices, including the work from home environment. Aruba ESP with Edge-to-Cloud Security incorporates comprehensive visibility, least access micro segmentation and control, as well as continuous monitoring and enforcement. Even traditional VPN solutions are enhanced by ensuring that the same controls applied to campus or branch networks, also extend to the home or remote worker.

In the age of IoT, basic principles of good network security are often difficult to implement. When possible, all devices and users should be identified and properly authenticated before granting them network access. In addition to authentication, users and devices should be given the least amount of access necessary to perform their business-critical activities once they're on the network. This means authorizing which network resources and applications any given user or device can access. Finally, all communications between end users and applications should be encrypted.

THE NEED FOR COMPREHENSIVE VISIBILITY

With the increased adoption of IoT, full spectrum visibility of all devices and users on the network has become an increasingly challenging task. Without visibility, critical security controls that support a Zero Trust model are difficult to apply. Automation, AI-based machine learning, and the ability to quickly identify device types is critical.

Aruba ClearPass Device Insight uses a combination of active and passive discovery and profiling techniques to detect the full spectrum of devices connected or attempting to connect to the network. This includes common user-based devices such as a laptops and tablets. Where it differs from traditional tools is its ability to see the increasingly diverse set of IoT devices that have become increasingly pervasive on today's networks.

ADOPTING "LEAST ACCESS" AND MICRO SEGMENTATION

Once visibility is in place, applying Zero Trust best practices related to "Least Access" and micro segmentation are critical next steps. This means using the best authentication method possible for each endpoint on the network (i.e. full 802.1X and multi-factor authentication for user devices) and applying an access control policy that only authorizes access to resources that are absolutely necessary for that device or user.

Aruba ClearPass Policy Manager enables the creation of role-based access policies that enable IT and security teams to operationalize these best practices using a single role and associated access privileges that are applied anywhere on the network – wired or wireless infrastructure, in branch or on campus. Once profiled, devices are automatically assigned the proper access control policy and segmented from other devices via Aruba's Dynamic Segmentation capabilities. Enforcement is provided by Aruba's Policy Enforcement Firewall (PEF), a full application firewall that is embedded in Aruba network infrastructure. Aruba infrastructure also utilizes the most secure encryption protocols such as the WPA3 standard over wireless network connections.

ClearPass Policy Manager also integrates with a wide variety of authentication solutions enabling the use of multi-factor authentication and the ability to force re-authentication at key points throughout the network. Through the ClearPass ecosystem, customers can also easily incorporate other solutions to meet Zero Trust requirements related to contextual information and other security telemetry.

This means ClearPass can integrate with a wide variety of solutions such as Endpoint Security tools to make more intelligent access control decisions based on a device's posture. Access control policies can also be changed based on which type of device is being used, where the user is connecting from, and other context-based criteria.

CONTINUOUS MONITORING AND ENFORCEMENT

With role-based access control in place to enforce granular segmentation, ongoing monitoring of users and devices on the network make up another Zero Trust best practice. This addresses risks related to insider threats, advanced malware, or persistent threats that have circumvented traditional perimeter defenses.

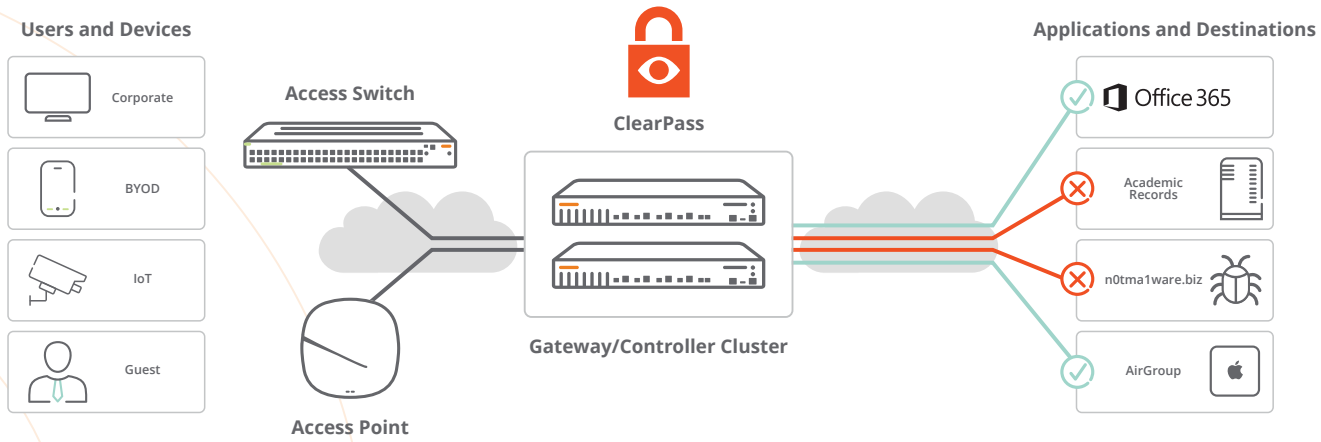

Figure 1: Aruba ClearPass automatically assigns role-based access control policies that are enforced using Dynamic Segmentation

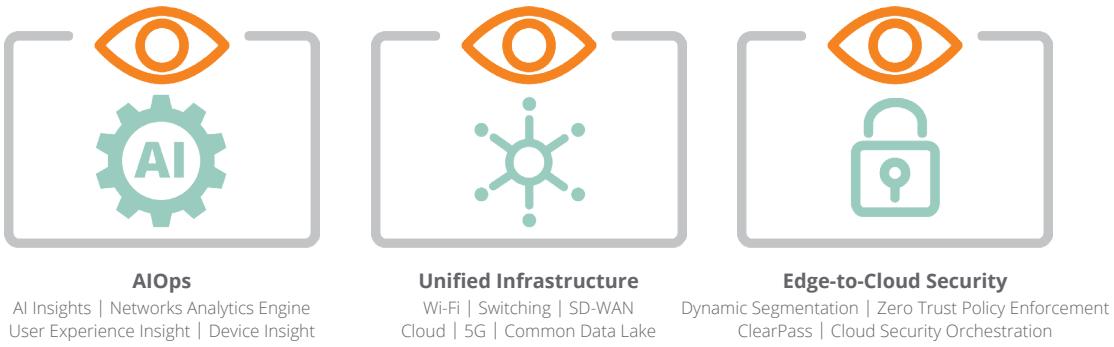

Figure 2: Edge-to-Cloud Security is a key pillar of Aruba ESP

Threat Defense with IDS/IPS

Aruba threat defense capabilities defend against a myriad of threats, including phishing, denial of service (DoS), and increasingly widespread ransomware attacks. Supported SD-WAN gateways perform identity-based intrusion detection and prevention (IDS/IPS), working together with Aruba Central, ClearPass Policy Manager, and the Policy Enforcement Firewall. Identity-based IDS/IPS performs signature- and pattern-based traffic inspection on both the branch office LAN (east-west) traffic as well as the SD-WAN (north-south) traffic flowing through the gateway to deliver embedded branch network security. An advanced security dashboard within Aruba Central provides IT teams with network-wide visibility, multi-dimensional threat metrics, threat intelligence data, as well as correlation and incident management. Threat events are sent to SIEM systems and ClearPass for remediation.

360 Security Exchange

With over 150 integrations made up of best-of-breed security solutions that include Security Operations and Response (SOAR) tool sets, ClearPass Policy Manager is able to dynamically enforce access based on real-time threat telemetry coming from multiple sources. Policies can be created to make real-time access control decisions based on alerts coming from Next-Gen Firewalls (NGFWs), Security Information and Event Management (SIEM) tools, and many other sources. ClearPass actions are fully configurable from limiting access (i.e. Internet only) to fully removing a device from the network for remediation.

ARUBA ESP (EDGE SERVICES PLATFORM)

To help our customers capitalize on opportunities at the Edge, we have developed Aruba ESP, the industry's first AI-powered platform designed to unify, automate, and secure the Edge. Edge-to-Cloud Security is a key component of Aruba ESP, and when combined with AIOps and a Unified Infrastructure, enables organizations to reduce costs, simplify operations, and stay secure.

SUMMARY

Today's network environment and threat landscape require a different approach. The perimeter-centric network security of the past was not designed for today's mobile workforce or emerging IoT devices. Aruba ESP with Zero Trust Security provides a comprehensive set of capabilities that span visibility, control, and enforcement to address the requirements of a decentralized, IoT-driven network infrastructure.

SO_ZeroTrustSecurity_SK_052721 a00097694enw

Contact us at www.arubanetworks.com/contact