aruba
a Hewlett Packard Enterprise company

SOLUTION OVERVIEW

SECURE AND SIMPLIFIED ACCESS FOR USERS AND DEVICES

Aruba Dynamic Segmentation for the network edge

The growing number of IoT devices and the use of business-critical mobility and cloud services are driving digital workplace innovations, which leads us to the question — is the network edge smart enough to securely connect all types of devices and users? Legacy networks were created without business-critical mobility, IoT access or security in mind. Today's approach of using manual and static configurations for these ever changing mobile and IoT devices located throughout campus and branch networks presents new security risks and has become a cumbersome task that IT teams face every day.

Aruba's Dynamic Segmentation solution helps solve this complex challenge in a unique and intelligent way that both simplifies access layer management for IT teams and provides a more secure, consistent experience, regardless of user or device type or how and where they connect. By extending Aruba's foundational role-based wireless policy capability to wired switches, Dynamic Segmentation improves security, delivers consistent user experience and simplifies IT operations across the entire wired and wireless network.

DRIVERS FOR SIMPLE, UNIFIED ACCESS

Policy administration complexity

Managing and securing ever changing networks while delivering a flawless user experience is a challenge. On-boarding wired users and IoT devices requires multiple touch points and implementing unified policies for wired and wireless networks is time consuming and can result in complicated, difficult troubleshooting. Managing adds-moves-changes for large networks with many device types and users is also very time intensive and error prone. Designing a network with strong security and control for both wired and wireless access in a simple, unified way is imperative to preventing network breaches.

Enhancing the user experience

As users move from desk to conference area, from dorm to classroom, they expect the same network experience no matter where they connect or how – wired or wireless. And asking them to use a virtual private network (VPN) is a challenge. Any network experience that requires IT support is seen as negative. User experience – whether employee, guest, shopper, or student – affects an organization's success. Connecting new device types, such as smart phones, printers or video conferencing equipment is often done without IT's knowledge or support. The expectation is that IT provides a flawless experience while maintaining visibility and management of all things on a secure network.

The Growth of IoT devices and new security concerns

From smart lighting to security cameras and badge readers, IoT devices are rapidly being deployed throughout networks of all sizes. This newfound network connectivity brings many appealing benefits, but also exposes the network to security risks as these devices hop on the same pathways as sensitive financial, medical, and business critical data. These devices rarely have strong security built in and also lack robust authentication. Passwords are stored in clear text, they lack secure supplicants, and they are often physically located in un-secured public areas – which opens the door to network breaches.

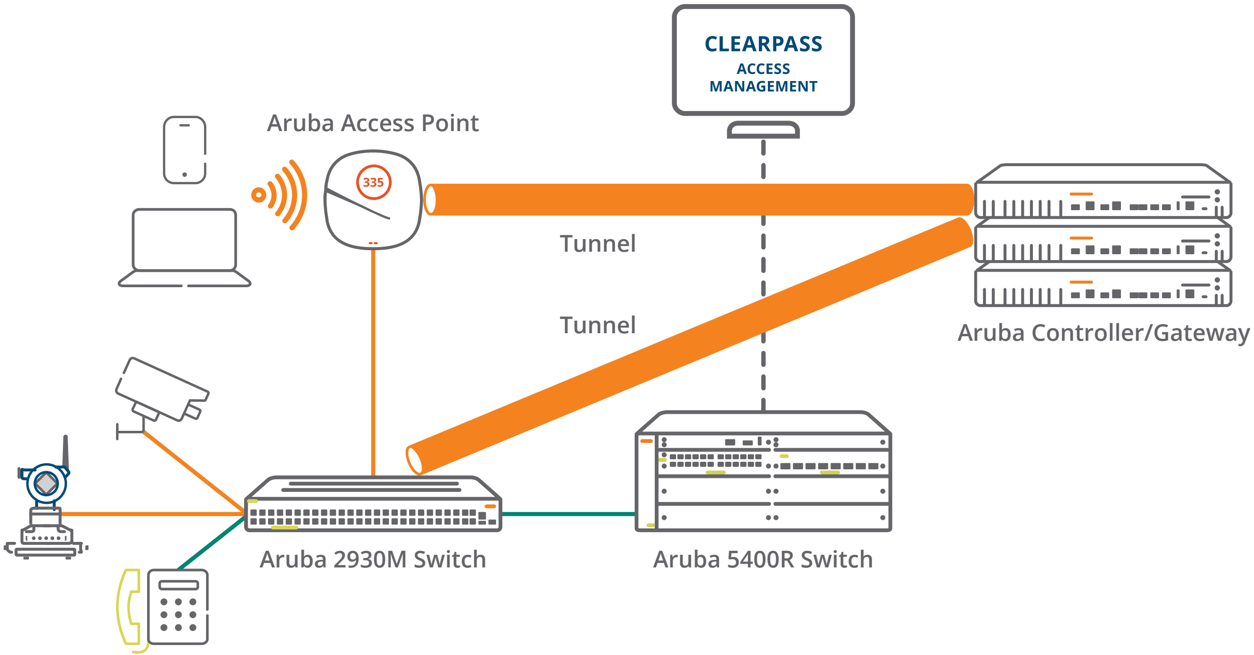
> Network vulnerability is exposed with the number of IoT/headless devices connected to enterprise networks projected to grow to over 20 billion by 2020.
>
> *Source: Gartner (January 2017)*

EXTENDING WLAN INNOVATIONS TO SWITCHING

Aruba's Dynamic Segmentation utilizes Aruba's inherently secure wireless and policy management solutions, to make wired network access simpler to secure. This capability is important because the switch no longer just provides wired access for legacy devices; it has become a wireless aggregator and provides connectivity for a growing number of emerging IoT devices. By implementing role-based (employee, guest, camera, etc.) policies that leverage intelligence within Aruba controllers and Aruba ClearPass for policy management, Aruba access switches can now help secure the edge.

Role-based policies

By implementing Dynamic Segmentation, role-based policy decisions and access rights are made based on the device type, application used, and even the location of the user or device. Originally used to address wireless security, role-based policies segmented network traffic by user type such as employee, guest or contractor, while dramatically simplifying network management by eliminating complex and static network configurations. This powerful capability streamlined IT workflows such as managing access and BYOD policies and ensured better application performance.



Dynamic Segmentation for the Network Edge

Extending dynamic role-based policy management to the wired edge provides a fundamentally simple, secure, yet different way to manage and enforce policies for mobility, IoT, and cloud. Aruba's intelligent access switch software, which leverages Aruba ClearPass for centralized policy definitions and enforcement, is now able to dynamically understand and utilize roles. This ability eliminates the time consuming and error prone task of managing complex and static VLANs, ACLs, and subnets as this is dynamically assigned to wired ports as a device establishes a connection.

Segmentation

The second foundational capability that the Aruba switches leverage is segmentation. The Aruba WLAN architecture keeps traffic secure and separated with the use of tunnels between access points and a controller or gateway. This tunnel-based segmentation provides security such as firewall inspection of high-risk traffic, through the use of Aruba's built-in Policy Enforcement Firewall (PEF). PEF delivers deep packet inspection which provides granular context (user, device, app, location), mitigating the need for expensive firewalls for first line of interrogation and defense. With contextual policies based on identities, device type and location, you can satisfy the needs of different groups of users with a single network configuration as traffic flows simply adapt to the assigned roles.

By using this WLAN tunnelling architecture, Aruba switches can now provide a role-based segmentation approach versus the traditional, more manual use of local VLANs. This is ideal for untrusted IoT devices or for providing application visibility, as Aruba switches can now dynamically tunnel selected traffic to the controller for deep packet inspection and device authentication just as an access point does. For example, a security camera can dynamically be assigned a role with rights that restricts its traffic to a specified server only, eliminating the opportunity for malicious entrance to other parts of the network.

This new segmentation capability improves security posture with tunnelling that can be set-up for either Port-Based Tunnelling (PBT) with all authentication done on the controller or User-Based-Tunnelling (UBT) with authentication done on the switch. Because this segmentation operates as an overlay, it can co-exist with VLAN implementations by utilizing secure tunnels in selected areas with no ripping and replacing of the entire switching infrastructure.

Devices tunnelled to an Aruba Mobility Controller can have firewall and access policies implemented to restrict access. Rather than installing expensive firewalls within the network infrastructure, network administrators can use the controller's built-in PEF capabilities to control both wired, wireless, and VPN access while satisfying the needs of different groups of users with a single network configuration.

BENEFITS OF ARUBA'S DYNAMIC SEGMENTATION SOLUTION

In addition to a higher level of wired access security, control and efficiency, Dynamic Segmentation also provides:

- **A better, consistent user experience** – Centralized, unified role-based policy control of wireless and wired traffic delivers the same policy and consistent user experience wherever a user or IoT device is, however they connect, wired or wirelessly.
- **Simplified operations** – IT saves time and reduces configuration errors by eliminating manual, static configurations of VLANs and ACLs. Co-existence with traditional VLAN segmentation means network designs do not need to be disrupted and does not require ripping and replacing switching infrastructure.
- **Improved security posture** – Enhanced context aware information such as device profiling with built-in controller security services lets you take advantage of additional security features such as firewalling, packet inspection and finger printing for both wireless and wired traffic. The dynamic firewall inspection of "at risk" wired traffic such as IoT devices greatly strengthens the posture at the edge.

THE SOLUTION INGREDIENTS

Aruba Wireless Access Points

802.11ac and 802.11ax Wi-Fi performance that meets the needs of any environment. Built-in AI intelligence, and location services offer IT the automation and visibility needed to deliver an optimal experience, for users and IoT devices.

Aruba Access Switches

Create an integrated wireless-wired foundation that delivers scalability, security and high performance for campus and branch networks. Dynamic Segmentation uniquely gives IT teams a simple way to apply policies, utilize advanced services and securely segment wired user and IoT traffic anywhere in the network via tunnels – using Port-Based Tunnel (PBT) with authentication done on controller or via a User-Based Tunnel (UBT) with authentication done at the Aruba switch (running ArubaOS-Switch 16.04 or above).

Aruba Controllers and Gateways

As a crucial part of the solution, controllers or gateways act as a policy enforcer for both wired and wireless traffic. The Aruba Mobility Controller (running AOS 8.1 or later) allows IT to leverage policy enforcement, bandwidth contracts and other traffic restrictions. In a branch environment, the Aruba Central-managed Branch Gateway (running AOS 8.4) performs this role. The Aruba Policy Enforcement Firewall enforces application-layer security, prioritization and enforces network access policies that specify who may connect to the network, with which mobile devices and which segments of the network are accessible.

Aruba ClearPass

Offers the ability to centrally manage and enforce network access policies for wireless and wired access control. Its primary functions are device profiling, authentication, and authorization and policy enforcement. Using ClearPass, once the role and the privileges are defined, they follow the user or device across wired and wireless access. So, if the user changes to an unknown device, or is on an unsecured network, the policy will automatically change authorization privileges. Downloadable User Roles (DUR) are configured on ClearPass, which eliminates the need to define roles or policies on a switch.

SUMMARY

To better handle business critical mobility and emerging IoT connectivity requirements, Aruba's innovative Dynamic Segmentation solution simplifies IT operations and improves security by dynamically applying unified policies and enforcing advanced services anywhere in the network. This ensures that appropriate access and security policies are seamlessly distributed, automatically applied, and independently enforced for all wireless and wired users and devices.

TO LEARN MORE

http://www.arubanetworks.com/products/networking/

aruba
a Hewlett Packard
Enterprise company