aruba
a Hewlett Packard Enterprise company

AT A GLANCE

KEY DYNAMIC SEGMENTATION USE CASES

Simplifying and Securing Wired and Wireless Networks

The impact of digital transformation today is paving the way for new technology that integrates users into the design, as well as the ability to leverage emerging Internet of Things (IoT) devices. This new focus has empowered IT to establish a larger role in how the business performs, yet has also wreaked havoc on traditional methods used to manage wired and wireless network infrastructure.

To ensure the increasing use and density of IoT devices does not impact the business nor IT policies, Dynamic Segmentation, a key component of Aruba's Architecture, identifies and enforces rules for devices and their traffic.

WHAT IS DYNAMIC SEGMENTATION?

As the name implies, Dynamic Segmentation helps simplify and secure the network by unifying policy enforcement across wired and wireless networks. Enforcement is based on Aruba's unique ability to apply role-based access control using a built-in Policy Enforcement Firewall (PEF). This firewall is designed to apply rules per user and device, as well as Layer 4-7 application types.

With Dynamic Segmentation, IT can satisfy a range of use cases by centralizing configuration that has traditionally been done at multiple hops in the network (Figure 1).

This At-A-Glance focuses on four common use cases where Dynamic Segmentation can help.

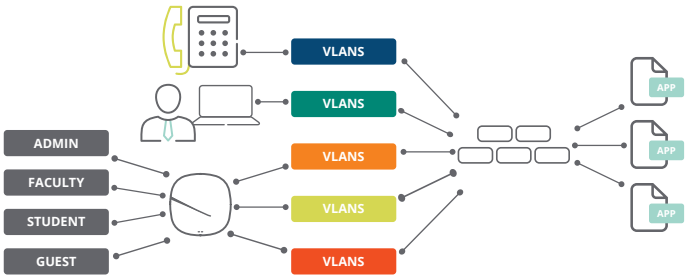
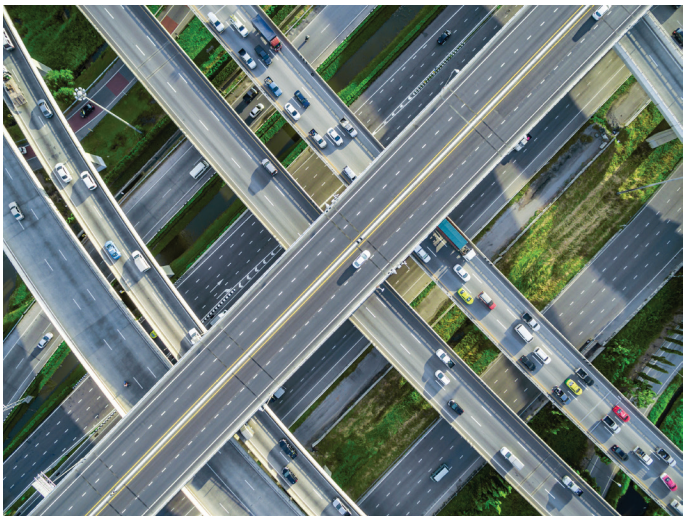


Figure 1: Each new user adds to VLAN or SSID sprawl



USE CASE #1: SIMPLIFYING NETWORK MANAGEMENT

Problem: Managing Policy is Spiraling Out of Control

BYOD and mobility caused IT to add VLANs everywhere and create new SSIDs because unknown devices now needed access, and users were connecting from anywhere. And now IoT is forcing IT to expand these efforts to ensure that these devices do not impact traditional business processes.

The first use case focuses on reducing the amount of configuration needed for the campus network to support ongoing moves, adds, and changes – in fact, just a single change in policy could potentially mandate changes for SSIDs, ACLs and subnets at every hop in the network (Figure 3).

This problem becomes larger as network requirements grow while resources remain stagnant.

Solution: Role-Based Access Control

By deploying Dynamic Segmentation, IT can now leverage the concept of user and device roles to dynamically assign rules or privileges to a given user or device – regardless of the SSID, port or location.

In Figure 2, a contractor named Lisa is given access to App 1 (e.g. WhatsApp) which is a cloud-based service, but denied access to App 2 (e.g. SharePoint) which is an on-prem hosted service. Using information gathered from a RADIUS server and identity store, the system applies appropriate network access whenever Lisa connects on-campus. Likewise, a full-time employee on the same network will receive a different set of privileges, while a headless device such as a security camera is assigned different privileges based on its policy rules.

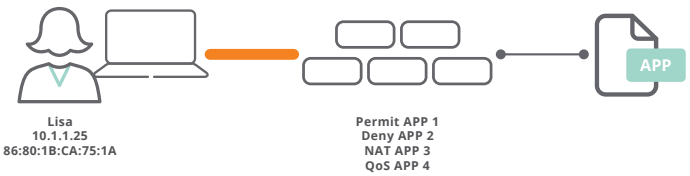


Figure 2: Now, a role can be used to simplify configuration

The concept of "roles" is applied across the infrastructure to provide advanced context for a simpler, smarter and more scalable network architecture. As a user goes from a corporate office to a remote office, the network-assigned role, access privileges, and policy follow.

USE CASE #2: SIMPLER WAY TO SEPARATE TRAFFIC

Problem: The Priority of Applications is Difficult to Enforce

As the business invests in new applications and services, the campus network is becoming more mission-critical and bandwidth-sensitive – which makes the ability to meet user expectations and SLAs more difficult to maintain. This is especially true for organizations that must meet strict compliance requirements (e.g. PCI, HIPAA, CIPA).

For example, how does IT ensure that the contractor from the previous use case has a seamless experience when on a Microsoft Teams call as she moves from a wired conference room phone to a video-enabled laptop at her desk? The same applies to WhatsApp, Zoom, or Wi-Fi calling. In typical fashion, a maze of configurations will be needed for the wired and wireless networks, which includes QoS policies for voice and video to optimize for roaming.

This problem proves exponentially more difficult to scale as different groups within the business invest in a variety of new cloud applications – all competing for priority.

Solution: A Single Point of Enforcement

With Dynamic Segmentation, IT can use Aruba's Policy Enforcement Firewall (PEF) technology to establish consistent segmentation of user traffic as it flows through the network. This means that policies and configurations that were typically performed at different nodes on campus can be consolidated – reducing manual touchpoints, while noticeably simplifying the network architecture.

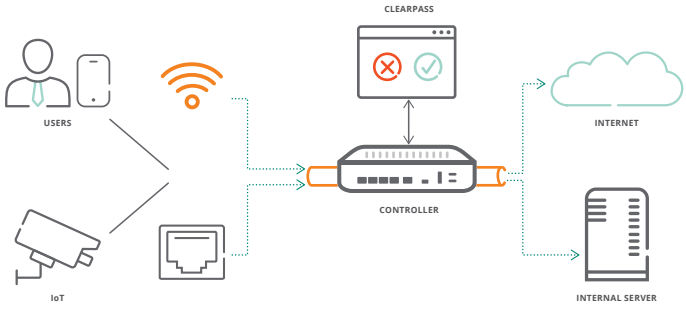


Figure 3: Dynamic Segmentation provides consistent enforcement for wired and wireless traffic

With PEF enabled, based on a user or device role all traffic is encapsulated in GRE tunnels, inspected, and assigned appropriate priority. In addition, PEF understands Layer 7 application awareness for over 3,000 applications, using Deep Packet Inspection (DPI). This allows IT to prioritize traffic by application and user and device role – for instance corporate video, voice, or UCC traffic is given high priority – while rate-limiting or throttling less important services like social media or entertainment streams being generated by guests.

IT can also improve QoS and security using Aruba's WebCC feature, which is a subscription-based web content filtering option that provides visibility into Internet destinations and utilizes metrics such as reputation – to limit or throttle access.

USE CASE #3: BETTER DEVICE VISIBILITY

Problem: Digital Workplace IoT is Converging With Traditional User Devices

It's not just users, applications and BYOD on the network any longer. Legacy systems such as telecom equipment, surveillance infrastructure, and HVAC systems are now being designed with Internet access in mind, and include wireless or wired network connectivity. All of this IoT means that IT has a lot of new devices to account for.

Unfortunately, aside from updating their wired and wireless configurations to support these new devices, there's a problem with visibility. IT doesn't always know what, where, and when these new devices are connecting to the network – which poses a big risk.

Solution: Enhanced Fingerprinting of Devices

While PEF includes the ability to recognize device types (e.g. Windows 7, MacOS X, Android, and iPhone) it can also utilize rich device profiles from Aruba's ClearPass Policy Manager or ClearPass Device Insight for more granular detail about devices. This greater visibility ensures that there are fewer devices classified as "unknown" on the network, which helps apply appropriate policies.

The ability for IT to easily see if a sensor is related to their HVAC system or to a manufacturing process not only helps the business from a workflow process, but from a security perspective as well. Internet access is granted for any known device that is to receive cloud-only access, and unknown devices can be given limited access or kept off of the network.

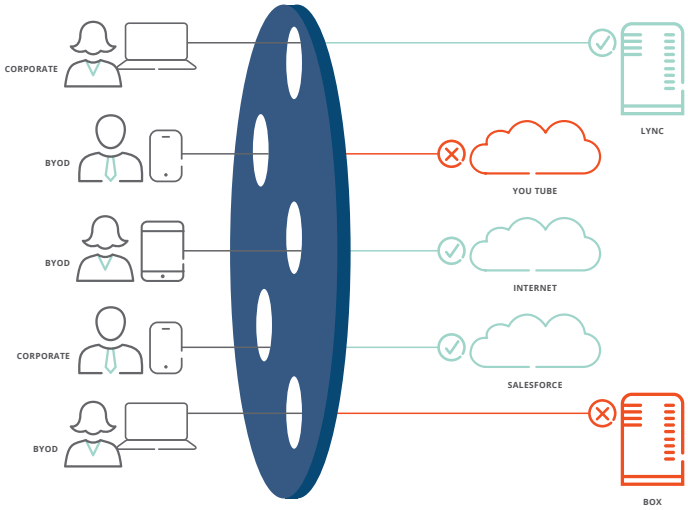
USE CASE #4: CONSISTENT POLICIES EVERYWHERE

Problem: Changes Become Riskier and More Complex in Distributed Networks

For environments with a large number of wireless APs and network switches, as well as distributed enterprises with many remote branch sites, even the simplest configuration change can require long deployment cycles and multiple truck rolls. Networks will also be more prone to misconfiguration and more inconsistent in what policies are enforced and how they were implemented.

Solution: Centralized Management of Policies

By deploying Dynamic Segmentation, IT can ensure policies are consistently enforced for each user, device type, and application in the campus – but also in every branch site through Aruba SD-Branch. While PEF provides unique role-based access control and ClearPass offers enhanced visibility, IT can also use ClearPass to centrally manage policies for all geographic locations – another valuable component of Aruba's Experience Edge Architecture.



THE SOLUTION INGREDIENTS

Aruba Gateways and Mobility Controllers

The Mobiilty Controller allows IT to perform policy enforcement, mandate bandwidth contracts and other traffic segmentation capabilities. PEF serves as the underlying netowrk technology in support of these two environments.

Aruba ClearPass Policy Manager

The primary functions of ClearPass include device profiling, authentication, authorization and centralized policy management. Once roles and policies are defined, they follow the user or device across the wired and wireless networks.

Aruba Wireless Access Points

Wi-Fi 5 (802.11ac) and Wi-Fi 6 (802.11ax) APs forward all wireless traffic through GRE tunnels to the controller. They also provide built-in AI intelligence, IoT and location services.

Aruba Network Access Switches

Aruba 2930F/M, 3810M and 5400R series switches forward all wired traffic through GRE tunnels to the controller. Just like APs, they utilize roles to perform User-Based Tunneling (UBT), and also per-port segmentation with Port-Based Tunneling (PBT).

KEY TAKEAWAYS

Aruba Dynamic Segmentation provides a new response to implementing today's mission-critical use cases, whether in the campus or the branch. Automation simplifies the typical complexity involved with introducing new devices into a working production environment, while adding security. And IT gains visibility, a unified policy enforcement framework for wired and wireless networks, and a simple model that allows them to spend time delivering new services, and not on performing repetitive management tasks. For more information, please refer to the Dynamic Segmentation Solution Overview, or contact your Aruba sales representative for more information.

a Hewlett Packard Enterprise company

AAG_DynamicSegmentation_SK_080519 a00074156enw