AT A GLANCE

DYNAMIC SEGMENTATION USE CASES

Built-in identity-based access control for Zero Trust and SASE security from edge-to-cloud

Businesses are accelerating their digital transformation initiatives to deliver new user experiences, support hybrid work, implement new business models and achieve greater IT efficiency. This gives rise to complex, globally distributed networks with unique visibility and security challenges.

Traditional security approaches that focus primarily on the perimeter of the network become ineffective as standalone security strategies. With Aruba's built-in foundation for Zero Trust and SASE, Aruba ESP (Edge Services Platform) offers edge-to-cloud security by applying rigorous security best practices and controls to previously trusted network resources.

WHAT IS DYNAMIC SEGMENTATION?

Aruba's market-leading Dynamic Segmentation solution is a critical element of the edge-to-cloud security built into Aruba ESP and establishes least privilege access to IT resources by segmenting traffic based on roles and associated access permissions (See Figure 1). This is a fundamental concept of both Zero Trust and SASE frameworks where trust is based on identity and policies , and not based on where and how a user or device connects.

Dynamic Segmentation unifies role-based access and policy enforcement across wired, wireless, and WAN networks, ensuring that users and devices can only communicate with destinations consistent with their role - keeping traffic secure and separate.

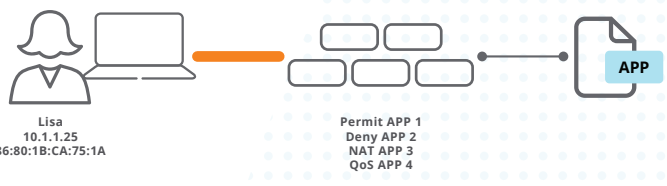

Figure 1: Role is a logical grouping of permissions. Permissions can include a list of applications and services that can be accessed, users and devices that can be reached, or even days of the week a particular user can connect to the network.

Aruba Central NetConductor

As organizations modernize their networks with overlays and widely adopted protocols such as EVPN/VXLAN, there is an opportunity to leverage the network architecture for increased protection and greater scale, but it often leads to significant configuration complexity and management overhead for the IT and security teams.

Aruba Central NetConductor aims to address the above problem with cloud-native security services and overlay-based enforcement, enabling organizations to automatically configure network infrastructure for optimal performance and consistently enforce granular access control security policies at global scale. With Central NetConductor, Dynamic Segmentation can be managed via the cloud with the ability to centrally define and enforce access policies either in a distributed or centralized fashion based on the choice of overlay.

The following use cases detail the principles of Dynamic Segmentation, the enforcement models, and the role of Central NetConductor with four scenarios that are increasingly common in modern networks :

USE CASE #1: IDENTIFYING AND SECURING NETWORK ENDPOINTS

Problem:

As the breadth and complexity of endpoint clients such as IoT devices continues to grow at a staggering rate, organizations are struggling to address an expanding cyber-attack surface. Traditional discovery and profiling techniques are no longer adequate to accurately find, fingerprint, and assign access privileges to these devices.

Solution:

For many purpose-built IoT devices, such as those found in a hospital or manufacturing plant, understanding the actual behavior of the device is the only way to accurately identify them. Aruba is the first to ingest device attributes, network flow data and system logs in a cloud-native platform to profile, classify and fingerprint clients based on their behavior in the network.

AI-powered Client Insights on Aruba Central leverages native infrastructure telemetry from access points, switches, and gateways, as well as clients without requiring installation of physical collectors or agents. ML-based classification models are used to identify and accurately profile a wide variety of clients, including a diverse set of IoT devices across the entire wired and wireless infrastructure. Client Insights allows for continuous monitoring of clients, which when paired with Central NetConductor or ClearPass provides closed loop, end-to-end access control.

Visibility and profiling are critical determinants of successful user and client traffic segmentation. For example, a global hospital network must have the capability to accurately identify and profile IoT devices based on their behavior, allowing only authorized users and devices access to patient medical records, and ensuring data privacy guidelines are adhered to.

USE CASE #2: AUTOMATING NETWORK CONFIGURATION AND MANAGEMENT

Problem:

As organizations seek to deliver new user experiences and drive business efficiency, the number of sites, network topologies and business requirements are overwhelming. Traditional approaches using manual and static VLAN-based configurations to secure networks are not only error-prone but also inadequate for these ever-changing, modern deployments (See Figure 2). Even the simplest configuration change or client onboarding can require long deployment cycles and extensive reconfigurations, severely impacting IT productivity.

Solution:

Central NetConductor comprises of cloud-native network and security services that automate configuration, policy definition and enforcement at global scale. Central NetConductor policy manager can be used to centrally define user groups and their associated enforcement rules. Central NetConductor fabric wizard simplifies the creation of overlays using an intuitive, graphical user interface and push-button automation, eliminating the need for CLI-based programming, routing table spreadsheets, or manual configuration of ACLs.

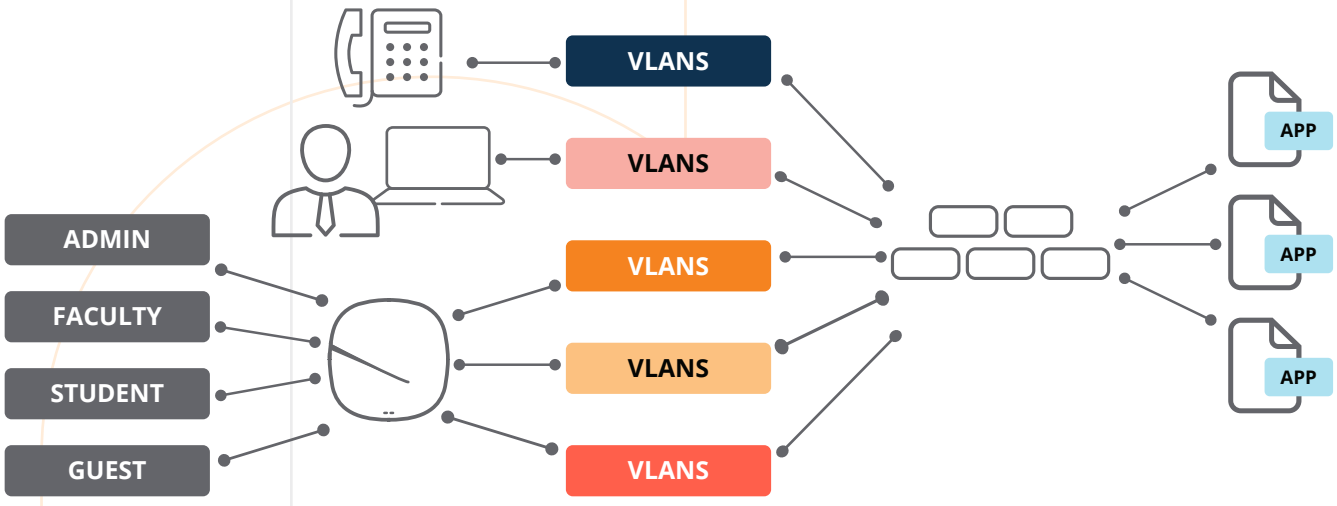

Figure 2: Static configurations lead to VLAN sprawl

By decoupling business intent from physical network construction, organizations can dramatically reduce the time and resources required to operate the network for enhanced IT productivity. Continuous monitoring of operational baselines along with health scores can help IT teams monitor overlay, sites, devices and troubleshoot network issues or potential security issues that are otherwise difficult to pinpoint. This high degree of automation means fewer resources are required to configure, maintain, and support the network, instead enabling IT to focus on driving strategic business priorities.

USE CASE #3: SECURITY AND POLICY ENFORCEMENT AT SCALE

Problem:

As networks become increasingly complex and geographically dispersed, there is an increasing need for segmentation strategies that can scale globally across physically disparate networks while ensuring performance, reliability, and efficiency. Most approaches that require routing of traffic outside its optimal path for security inspection result in latency, overheads, and sub-optimal user experience.

For example, in a manufacturing facility with a distributed network of hundreds of IoT devices, employees, vendors and contractors , delays in ensuring secure, authorized access to resources and systems could directly impact production outcomes.

Solution:

Central NetConductor uses widely adopted protocols such as EVPN/VXLAN to produce an intelligent network overlay that can be quickly deployed at massive scale, across heterogeneous networks from remote and branch locations to campuses and global enterprises. Overlay networks provide the agility to deploy flexible services at scale based on ever-changing connectivity and mobility demands of clients and applications.

The polices defined by Central NetConductor policy manager are expressed in group policy identifiers (GPIDs) that allows the network to carry access control information via the traffic itself, reflecting the role and access permission of the user or client (See Figure 3). Identifiers are embedded in the packet header and interpreted inline by Aruba CX switches and gateways for policy enforcement, eliminating the need to send traffic outside its optimal path for security inspection. If the security status of a client changes, its role is automatically modified to restrict access; that role change is then propagated to the network.

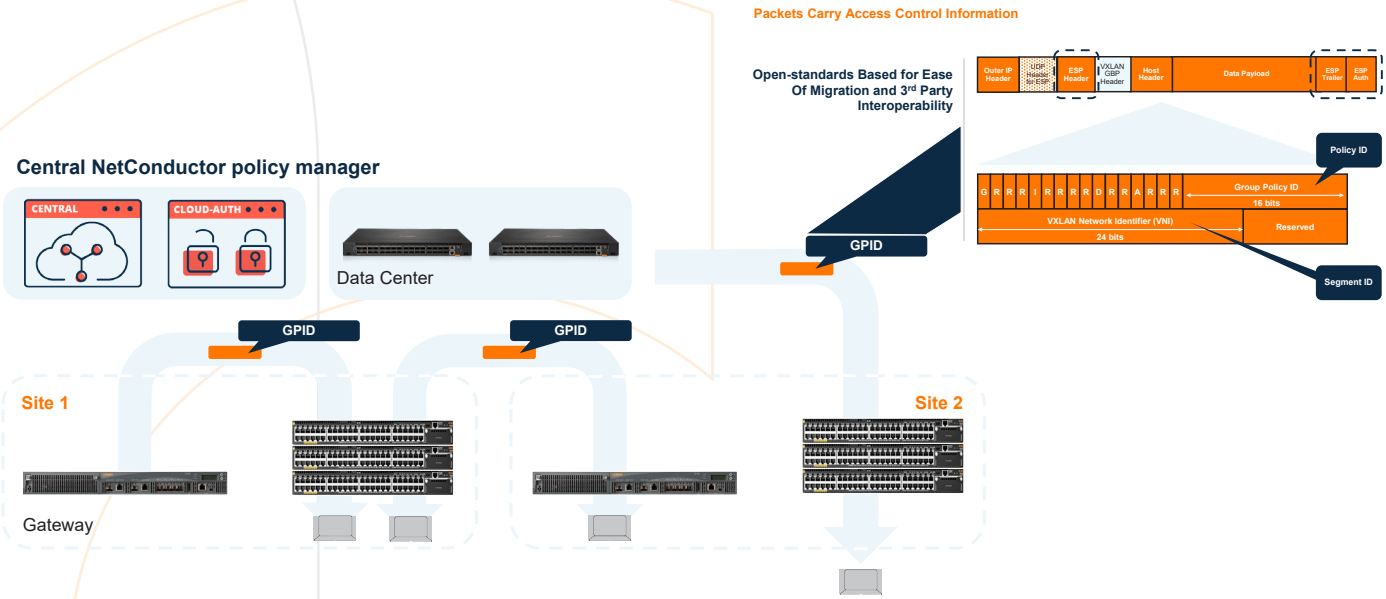

Figure 3: Group policy identifiers (GPIDs) enrich traffic with access control information. Identifiers are centrally defined within and applied from the policy manager and enforced across network locations via gateways and switches.

USE CASE #4: FLEXIBILITY OF ADOPTION

Problem:

Moving to new architectures and topologies like VXLAN for greater scale or adopting cloud-based network management often raises concerns about disrupting current operations and needing infrastructure upgrades. Organizations require a non-disruptive, interoperable solution that can be adopted at a pace defined by their business priorities.

Solution:

Aruba supports two ways to perform Dynamic Segmentation based on an organization's overall network architecture and choice of overlay : centralized and distributed.

With the centralized model, traffic is kept secure and separate with the use of GRE tunnels between access points and Aruba Gateways. Centralized policy definition is achieved either through ClearPass or Central NetConductor policy manager and gateways function as ingress policy enforcement points with Aruba's Layer 7 Policy Enforcement Firewall (PEF).

The distributed model uses an EVPN/VXLAN overlay and Central NetConductor cloud-native services such as policy manager and fabric wizard for policy definition and network configuration respectively. It supports inline policy enforcement through access control information carried in standards-based global policy identifiers (GPID).

Organizations currently using centralized policy enforcement approaches can continue with that approach and adopt over time a distributed approach in which enforcement is done by access devices, without rip and replace of existing infrastructure. Although Central NetConductor is optimized for Aruba networks, it is specifically designed for interoperability. Central NetConductor-capable infrastructure can coexist with current network management and security services, protecting investments and enabling organizations to modernize networks at their own pace.

KEY TAKEAWAYS

Aruba's market leading Dynamic Segmentation solution simplifies IT operations and enhances security by unifying role-based access and policy enforcement across wired, wireless, and WAN networks. Extending Dynamic Segmentation with a standards-based distributed overlay and cloud-native services ensures that identity-based policies can be automatically updated and continuously enforced across complex, globally distributed networks. Aruba Dynamic Segmentation is the one solution that simplifies the adoption of Zero Trust and SASE security regardless of the size and complexity of the network at a global scale.

AAG_DynamicSegmentation_SK_031722 a00074156enw

Contact us at www.arubanetworks.com/contact