SOLUTION OVERVIEW

aruba
a Hewlett Packard Enterprise company

Dynamic Segmentation

Identity-based Access Control for Zero Trust and SASE security from edge-to-cloud at global scale

The proliferation of IoT devices and adoption of hybrid work initiatives have resulted in complex, geographically distributed networks with unique visibility and security challenges. Additionally, with organizations accelerating digital transformation to drive business efficiencies, IT teams are facing a growing challenge when it comes to implementing Zero Trust and SASE security frameworks from edge-to-cloud.

Aruba Dynamic Segmentation is a critical element of the Edge-to-Cloud Security built into Aruba ESP (Edge Services Platform) It is based on establishing least privilege access to IT resources by segmenting traffic based on identity and associated access permissions. This is a fundamental concept of both Zero Trust and SASE frameworks where trust is based on roles and policies, and not on where and how a user or endpoint clients such as IoT devices connect.

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

IDENTITY-BASED SEGMENTATION IS THE KEY FOR ZERO TRUST AND SASE

It has long been recognized that access control decisions based on how and where a user or device connects leads to highly manual and error-prone network configuration with significant security gaps. Zero Trust was introduced a decade ago to address this challenge by providing a security architecture that enables organizations to define and enforce IT access policies based on limited access to resources defined by a user's or clients identity and role. For instance, a printer should never be allowed to access a server with payroll information.

KEY BENEFITS

- **Simpler Network Operations –** Save time and eliminate VLAN sprawl by reducing the configuration needed for SSIDs, ACLs, subnets, and wired ports
- **Enhanced Security and Visibility –** Ensure users and devices only communicate with destinations consistent with their mission via centralized policy definition and role-based access
- **Cloud-based Management and Automation –** Leverage intent-based, easy-to-use workflows for policy definition and network configuration
- **Global scale and Interoperability –** Enable global scale while ensuring interoperability with third party infrastructure
- **Performance and Efficiency –** Eliminate IT overhead with automatically updated and continuously enforced policy

A Zero Trust network segments traffic based on access control policies—independent of the method of connection. Several years ago, SASE (Secure Access Service Edge) recognized the importance of cloud-based workloads and extended Zero Trust to include SD-WAN and cloud-delivered security services. Zero Trust and SASE frameworks provide the blueprint for a secure network foundation that uses identity-based segmentation that is built into the network to protect the organization.

THE PRINCIPLES OF DYNAMIC SEGMENTATION

Aruba is a market leader in delivering networks that support the access control mechanisms defined by Zero Trust and SASE. Aruba's Dynamic Segmentation utilizes identity, policy, and the network infrastructure to streamline and automate how IT protects critical assets and comprises the following functions:

Device Discovery and Profiling

As more and more IoT devices or clients are flooding on to the network, there is limited ability for IT to see and fingerprint everything that is connected. As a result, they have both operational and security blind spots that can lead to compromises across the organization. A key element of Aruba's Dynamic Segmentation is Aruba Central's AI-powered Client Insights. This solution uses telemetry from Aruba network infrastructure and machine learning to automatically profile any type of client that connects to the network with over 95% efficacy.

Aruba also offers an option for automated, AI-powered client profiling that works in third party network deployments. Learn more here.

Identity and Authentication

Once a user or device is identified through an authentication process involving 802.1x or other techniques , IT can then define appropriate role and access permissions which are automatically applied. This then ties access privileges to identity which is independent from the network connection or location of the user or device.

Role-based Policies

Role is a logical grouping of permissions that are assigned once the identity of a user or client is established. Permissions can include a list of applications that can be accessed, the services and other clients that can be reached, or even the days of the week a particular user can connect to the network. Roles and enforcement are determined by an organization's overall approach to Zero Trust and SASE along with compliance requirements such as GDPR.

Automated Enforcement

Once roles are defined, enforcement is done by the network infrastructure by using the access rights to appropriately route and segment traffic. As is described below, Aruba Dynamic Segmentation offers a choice of enforcement models that can be used individually or together.

DYNAMIC SEGMENTATION MODELS

Aruba supports two ways to perform Dynamic Segmentation based on an organization's overall network architecture.

DISTRIBUTED DYNAMIC SEGMENTATION

As organizations modernize their networks with the adoption of overlays and widely adopted protocols such as EVPN/VXLAN, there is an opportunity to leverage the overlay for increased protection and greater scale with Dynamic Segmentation. With the introduction of Aruba Central NetConductor, Dynamic Segmentation can be managed via the cloud with the ability to centrally define and propagate access policies and enforce them in a distributed fashion inline via Aruba switches and gateways (See Figure 1).

Business intent-based workflows

With Central NetConductor, IT can use a fabric wizard to abstract the complexity of the underlying network and simplify policy definition while automating network definition and configuration. Intuitive, graphical workflows coupled with push-button automation eliminate the need for CLI-based programming, routing table spreadsheets, or manual configuration of ACLs.

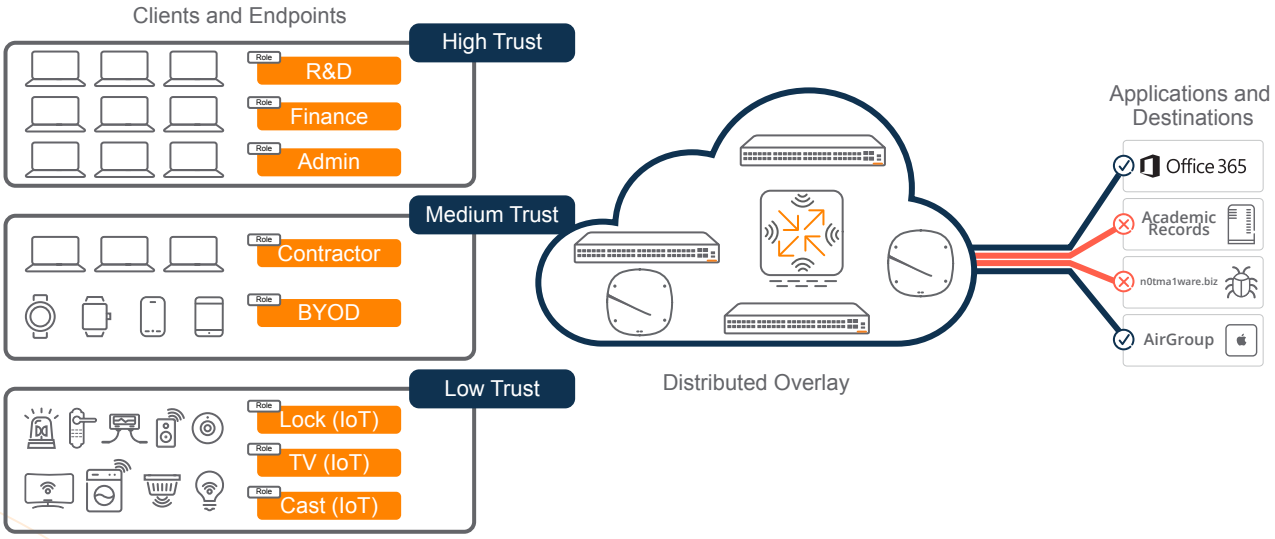

Figure 1: Dynamic Segmentation with a distributed overlay fabric

Group policy identifiers (GPIDs) for inline policy enforcement

The Central NetConductor policy manager defines roles and associated access policies. These polices are expressed in group policy identifiers and allows the network to carry access control information via the traffic itself, reflecting the role and access permission of the user or client. Identifiers are embedded in the packet header and interpreted inline by Aruba CX switches and gateways (See Figure 2). 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.

With group policy identifiers, distributed Dynamic Segmentation significantly enhances the scale in which policies are enforced while reducing latency and traffic overhead. The identifiers are based on industry standards and support bi-directional integration with third party networks.

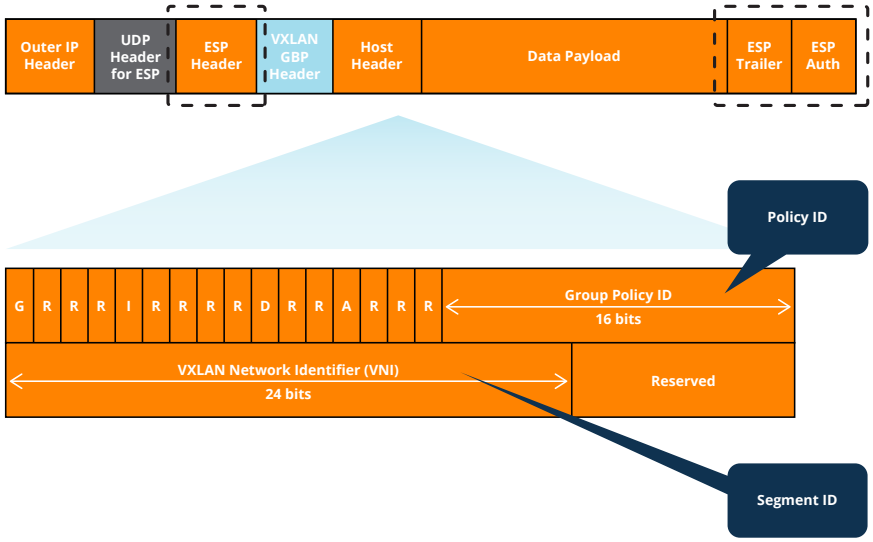

Figure 2: Group policy identifiers carry access control information through network traffic for inline policy enforcement

CENTRAL NETCONDUCTOR – SOLUTION INGREDIENTS

The components of Central NetConductor enable distributed Dynamic Segmentation for scale and performance as shown in Figure 3.

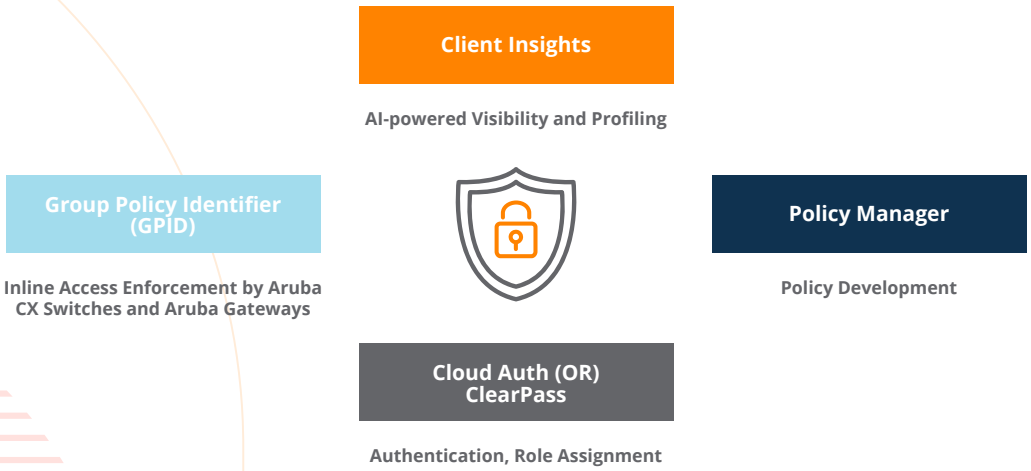

Figure 3: Solution ingredients for distributed Dynamic Segmentation with Central NetConductor

- **Client Insights –** The first and only agentless client visibility and fingerprinting capability built into a cloud-native management platform to eliminate network blind spots. AI-powered Client Insights leverages infrastructure telemetry and ML-based classification models to fingerprint, identify, and accurately profile a wide variety of clients across the entire wired and wireless infrastructure.
- **Cloud Auth –** Enables frictionless onboarding of end users and client devices either through MAC address-based authentication or through integrations with common cloud identity stores such as Google Workspace or Azure Active Directory to automatically assign the right level of network access.
- **Policy manager –** Defines user and device groups and creates the associated access enforcement rules for the physical network (See Figure 4)

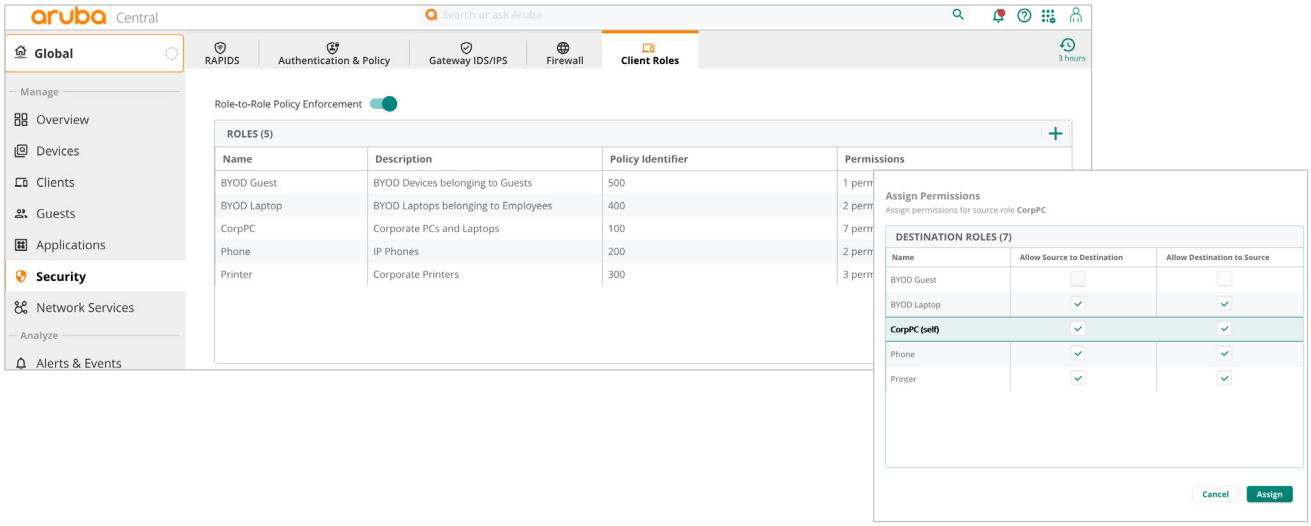

Figure 4: Intuitive, graphical interface for global policy definition

- **Fabric wizard –** Simplifies the creation of the overlays using an intuitive, graphical user interface, greatly easing the way virtual components are defined and configuration instructions are generated and pushed to switches and gateways (See Figure 5)

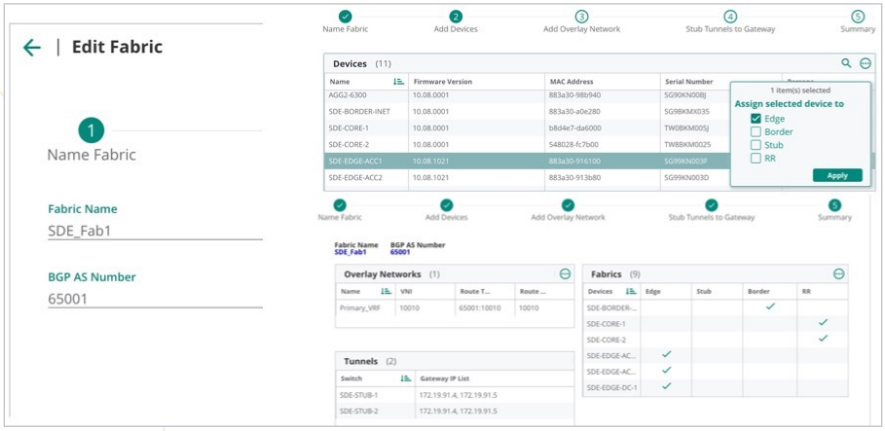

Figure 5: Easy-to-use, graphical workflow for simplified configuration and automated deployment of fabric overlay

- **Group policy identifier (GPID) –** Carries client policy information in traffic for in-line policy enforcement, which reduces configuration and security overheads and increases mobility and scalability.
- **Fabric-capable Aruba Switches and Gateways –** Supports configuration and enforcement based on the routing instructions and access privileges defined in the group policy identifier.

Note: Networks that use the Central NetConductor policy manager for policy orchestration can use either Cloud Auth or ClearPass for authentication and role assignment.

CENTRALIZED DYNAMIC SEGMENTATION

Centralized Dynamic Segmentation has been the mainstay approach for IT access control across multiple generations of network technology. With this model, traffic is kept secure and separate with the use of centralized overlay that comprises of GRE tunnels between access points and Aruba Gateways (or Mobility Controllers in controller-based environments). Gateways function as ingress policy enforcement points that possess knowledge about the roles of source and destination clients or applications (See Figure 6).

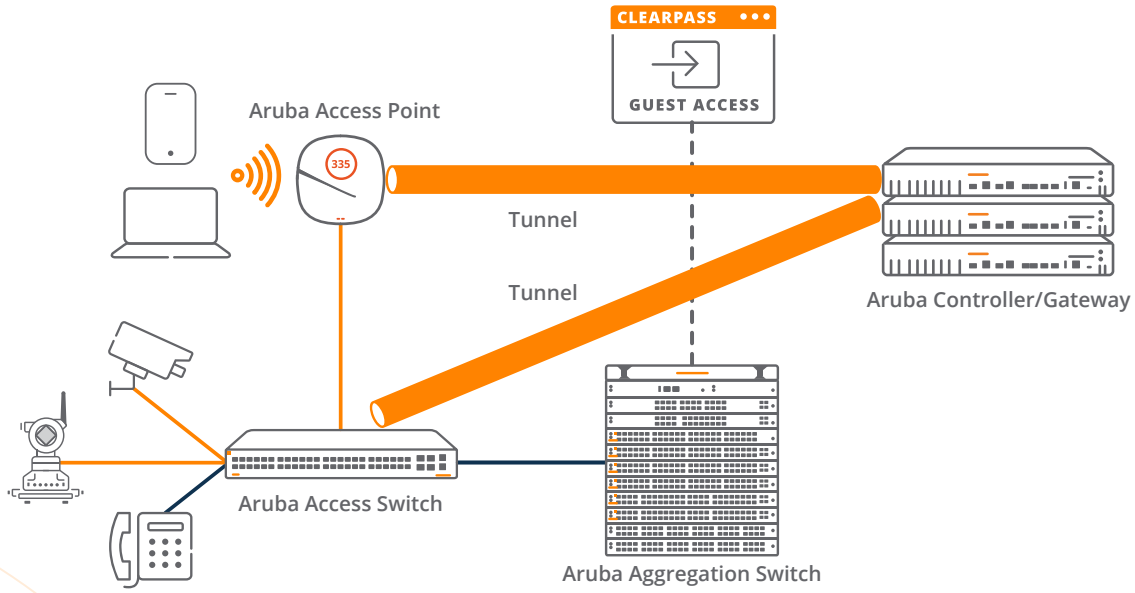

Figure 6: Centralized Dynamic Segmentation

Policy definition

Centralized policy definition can be achieved either through ClearPass or NetConductor policy manager for the centralized enforcement model.

ClearPass provides authentication, authorization and centralized policy definitions that follow the user throughout the network and are applied uniformly across wireless, wired and VPN connections. If the user changes to an unknown device, or is on an unsecured network, the policy will automatically change authorization privileges.

ClearPass supports standards-based 802.1X enforcement and other techniques for secure authentication. It 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.

ClearPass also supports the Aruba 360 Security Exchange Program with over 150 partner integrations for comprehensive integrated security coverage and response using firewalls, UEM and other existing solutions.

Learn more here.

Policy Enforcement Firewall (PEF)

Traditional firewalls that leverage IP-based VLANs for control only become active after a user or device is admitted to the network, leaving a potential opening for advanced attacks. Aruba's stateful, Layer 7 firewall PEF uses identity, traffic attributes and other context to centrally enforce access privileges at the time of initial connection. Inspection of traffic through PEF provides granular context about users, devices, applications, and locations. PEF serves as the underlying network technology supporting policy enforcement on Aruba Gateways (or Mobility Controllers in controller-based environments).

A CHOICE OF DYNAMIC SEGMENTATION MODELS

Extending VLAN-based architectures with an EVPN/VXLAN-based intelligent overlay fabric addresses siloed configuration and security issues, facilitating policy enforcement across complex, globally distributed networks (See Figure 7). The use of widely adopted protocols enables multi-vendor interoperability for integration with third party networks, without requiring a rip and replace of existing infrastructure.

Customers can use either a centralized or distributed overlay fabric or use both since the two enforcement models can coexist in an environment. Organizations currently using a centralized approach can flexibly adopt a distributed approach in which enforcement is done by access devices, at their own pace.

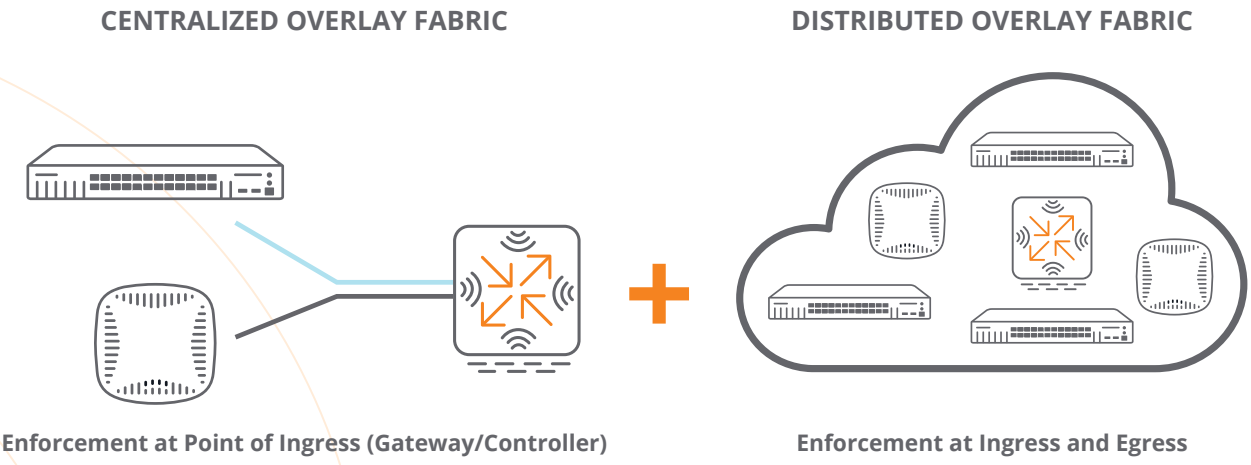

Figure 7: Distributed Dynamic Segmentation supports greater scale and performance by leveraging a distributed overlay fabric for policy enforcement at both points of ingress and egress

SUMMARY

As organizations move to better protect their networks, the segmentation of IoT, BYOD clients and user traffic is of utmost importance. Aruba's innovative Dynamic Segmentation solution allows IT to choose a model that best works for the environment to enhance their security by dynamically applying unified policies and enforcement capabilities from edge to cloud. With the granular role-based access permissions that Dynamic Segmentation enforces, compromised users and clients can easily be kept from participating in an attack by automatically blocking or quarantining the endpoint client when an attack is detected.

A choice of centralized or distributed models that can be consumed via cloud or on-premises ensures that appropriate access and security policies are automatically updated and continuously enforced across any network topology. 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.

SO_DynamicSegmentation_030322 a00058593enw