aruba
a Hewlett Packard Enterprise company

Validated Solution Guide

Aruba Solution TME

May 28, 2025

Table of Contents

Central

The Aruba Central cloud platform hosts applications for managing policy across the ESP architecture. Central provides a user interface that facilitates policy creation and consistent implementation on all devices in an Aruba ESP network.

Central manages on-premise gateways, APs, and switches to ensure consistent policy implementation.

Gateway

ArubaOS 10 is a cloud-ready, AI-integrated wireless network operating system. Gateways running AOS 10 are configured through Central. They excel at processing large ACLs, using DPI and IDP/IPS functions to perform deeper levels of inspection to further secure the network. Available gateway features and capabilities make it easier to adapt Aruba ESP Policy to different security requirements that vary from company to company.

When designing a gateway cluster for high-availability purposes, ensure that cluster capacity is below 50% to allow for hitless failover and uninterrupted connectivity in case of a cluster member failure.

Gateway clustering also can be used to increase scale without replacing existing gateways. A new gateway can be clustered with an existing one. An 80% capacity figure is the recommended maximum target to avoid performance issues. However, APs build a single GRE tunnel back to a single controller. When a cluster is at or below 50% utilization, APs establish redundant GRE tunnels to two cluster members.

The maximum cluster size for 7000 and 9000 series gateways is four devices. The maximum cluster size for 7200 series gateways is 12 devices. When possible, use larger capacity gateways, rather than more gateways, to meet requirements and increase flexibility for growth.

Homogeneous clusters are required. Mixing different gateway models within the same cluster is not supported.

Authentication servers, AAA profiles, roles, and policies are all configured through the Central configuration page for gateways.

On the **Devices > Gateways** tab > **Security** page, create user roles and associate them with AAA profiles using the subcategories in the same section. The AAA profile in the **Role Assignment** tab enables the gateway (in this example) to recognize the role returned by a RADIUS server during a client authentication event and map it to the appropriate endpoint.

The **Security > Policies** section enables creation of firewall rule sets based on application session properties. ArubaOS has six policy types, including standard and extended ACLs for compatibility with router software from popular vendors. However, firewall session policies provide equivalent and greater functions than standard and extended ACLs and should be used instead.

Policies are associated with a role in the **Roles** configuration tab on the page illustrated above. When a role is created and associated with a policy, a AAA profile can be configured to enable user authentication and role assignment. A secure per-user session can be managed from Central to secure the network access layer through the gateway cluster.

Switching

Aruba switches support a set of features called User-Based Tunneling (UBT). The switch tunnels client traffic back to a gateway cluster within a GRE tunnel, similar to how an AP tunnels client traffic. The gateway serves as a centralized policy enforcement point for wired, wireless, as well as WAN or Internet traffic.

UBT provides a centralized policy that supports Aruba Colorless Ports. A switch can dynamically tunnel traffic to a gateway cluster for policy enforcement so that any client device can connect to a properly configured switchport and dynamically receive the appropriate level of network access. This level of dynamic port assignment eliminates the need to manually configure and maintain multiple switch-port ranges for different devices.

To a network engineer, UBT eliminates the frustrating emergency Monday morning escalations to reconfigure ports for last-minute employee moves because someone forgot to submit a change request the week before. Also eliminated is the need to manage large port mapping plans that call for switch ports 1-8 configured as trunk ports for IAPs, 9-16 as access ports for security cameras, 17-20 as access ports for printers, and any other devices supported by the business.

All switches configured by NetConductor must be in the same Central group. Wireless gateways may remain in an existing wireless group or be included in the switching group.

Solution Components

Aruba Central NetConductor components include the following:

Group Policy Identifier (GPID)

GPID carries client policy information in traffic for inline policy enforcement, which reduces configuration and security overhead and increases mobility and scalability.

Fabric Wizard

Fabric Wizard simplifies the creation of overlays using an intuitive, graphic user interface, greatly simplifying how virtual components are defined and how configuration instructions are generated and pushed to switches and gateways.

Network Insights

Network Insights combines network expertise, artificial intelligence, and machine learning to detect, triage, root cause, and resolve Wi-Fi, wired, and WAN issues. The tool uses class-based site comparisons and best practices to identify opportunities for user experience optimization.

Client Insights

Client Insights uses network and client telemetry with machine learning to accurately fingerprint and classify all wired and Wi-Fi connected user and IoT endpoints for policy assignment and enforcement. It also monitors the behavior of traffic flows for added security.

Flexible Network Access Control

Flexible network access control ensures that entities are correctly identified and assigned a role that defines their access privileges using Cloud Auth cloud-native NAC, ClearPass, or third-party solutions.

Fabric-Capable Aruba Switches and Gateways

Aruba switches and gateways support configuration and enforcement based on the routing instructions and access privileges defined in relation to the GPID.

Aruba ClearPass Policy Manager and Aruba Central's Cloud Auth service are key components for applying effective role-based policy.

ClearPass can be deployed on-premises as a physical or virtual appliance to authenticate and assign client devices the appropriate level of network access. It interfaces with internal or external repositories such as LDAP, Device Insight, and partner firewall databases to quickly establish the identity of a device or user to make an informed decision about the level of access before establishing IP connectivity.

Cloud Auth is a cloud-native security service and an integral part of Aruba Centra's NetConductor. It integrates with a company's existing cloud identity store, such as Google Workspace or Azure Active Directory, to authenticate and assign the appropriate level of network access, similar to ClearPass.

Aruba ESP Policy design may contain one or more of the following elements:

- Aruba Central
- Aruba ClearPass Policy Manager
- Aruba CX Switches
- ArubaOS 10 Gateways and Access Points
- Aruba Central NetConductor.

The following diagrams are high-level examples of centralized and distributed policy enforcement models.

The first diagram, the *centralized model*, uses user-based tunneling (UBT) to encapsulate and forward wired client traffic to the ArubaOS 10 Gateway cluster via a GRE tunnel. The Gateways decapsulate and analyze the traffic, enforce user roles and other related attributes, then forward the traffic to their corresponding destinations.

In the second diagram, the *distributed model*, Aruba CX switches form an EVPN-VXLAN overlay fabric. Data traffic is encapsulated and forwarded in a VXLAN tunnel that enables policy enforcement on any VXLAN-GBP-aware device configured with a corresponding role and policy.

Centralized and Distributed Models

Gateway

Gateways are configured using Aruba Central and the NetConductor workflow. Existing Aruba wireless LANs are easily integrated into a NetConductor fabric. The recommended approach is to connect the gateway cluster to two Aruba CX 8360 switches configured as a VSX pair. The pair takes on the Stub persona during fabric configuration.

The wireless LAN and the overlay fabric are connected over a static VXLAN tunnel configured between the controller cluster and the Stub switch to which it is connected. This tunnel ensures that the role ID is communicated between the WLAN and the EVPN fabric by preserving the VXLAN header.

NetConductor requires adding personas to switches within the fabric. The gateways should be connected to a VSX aggregation switch pair, and the switches should be assigned the Stub persona from NetConductor. This causes NetConductor to configure a static VXLAN tunnel between the gateways and switches and enables the communication of a VXLAN header containing GPID between the EVPN fabric and the WLAN overlay.

gateway_vxlan_tunnels

Switching

Switches are configured using Aruba Central NetConductor. Aruba Central NetConductor provides an intuitive user experience resulting in the deployment of an EVPN-VXLAN overlay fabric.

The Aruba CX switch operating system provides a sophisticated suite of L3 capabilities necessary for building highly resilient overlay networks based on EVPN-VXLAN, using the proposed Group Based Policy field to carry a Group Policy ID value that enables evaluation of any packet anywhere in the network against a policy. Each user or device session carried through the fabric is assigned a role ID enabling each switch in the network to enforce role-based policy.

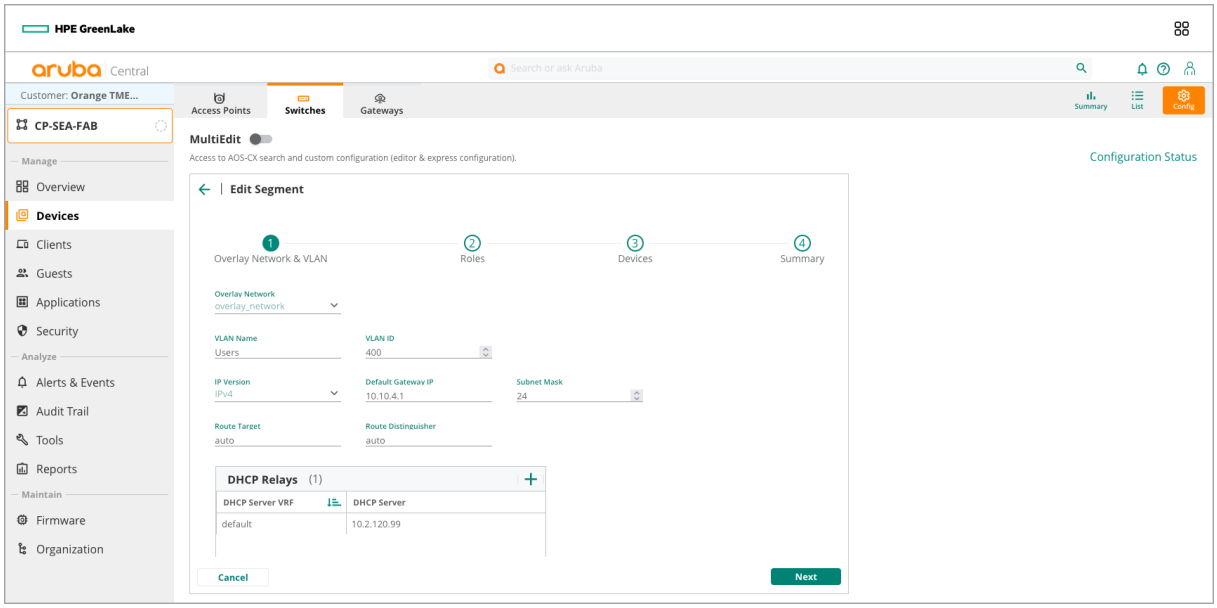

Figure 1: Fabric_segment_config

Authentication and Profiling

The identity of a connected device is established though an authentication event or a profiling result. The identity is associated with a role used for traffic generated by a user or device as long as the network connection is active and/or authentication policy allows connection.

TIPS Role

Within Aruba ClearPass, role mapping tags devices and users within a service with as much information as possible for use in a policy decision. Within a Role Mapping Policy, a user and/or device can be mapped to a TIPS role which is significant only within a ClearPass cluster deployment. This TIPS role can be used by the Enforcement Policy (along with attributes such as time of day, profiled information, or Microsoft Active Directory security group membership) to make a decision about the level of access a network client is granted. That Enforcement Policy then returns the user role attribute to be applied for the authenticating client to the AP, gateway, or switch .

Network Devices and Device Groups

Configure the list of Network Devices (e.g., RADIUS and TACACS clients) for which ClearPass must accept authentication requests. As an option, build device groups that the ClearPass service can use to classify, accept, and process requests, such as a group of switches from specific vendors, that may require different attributes in a response.

Policy Design

This guide is intended to help IT professionals understand considerations for policy design in a campus environment.

Introduction

The Aruba Edge Services Platform (ESP) architecture provides components necessary to design and implement a comprehensive, zero-trust network across a modern enterprise. Aruba ESP ensures consistent policy administration in the campus, across the WAN, within branches, and in the data center.

Policy configured on Aruba's cloud management platform, Aruba Central, is propagated across the network infrastructure to ensure consistent policy enforcement wherever and whenever the organization provides network connectivity.

This "single pane of glass" configuration approach ensures consistent policy application across different device types in both large and small network environments. Use of a conditionally assigned, access-based role associates a device or user with a set of privileges for each network interaction. The roles are configured consistently throughout the enterprise, facilitated by automation delivered by Aruba Central.

Fundamentals of Policy Design

When designing a security policy, first review the following activities and concepts:

- Complete network requirements for users and devices.
- Required authentication types or mechanisms.
- Device-to-device traffic requirements
- Device-to-cloud or Internet requirements.
- Traffic inspection capabilities within the network.
- Device attributes and available profiling capabilities.
- Network hardware capabilities.
- Compute resources.

Aruba ESP is designed to provide a flexible network system that increases accessibility while addressing the important need to enforce a consistent end-to-end, zero-trust security policy.

This guide delves into three key facets of policy management:

Step 1 Policy Definition: Establish roles and specify their access levels.

Step 2 Authentication and Role Assignment: Onboard users and devices to the network and allocate roles that align with their designated policies.

Step 3 Enforcement: Implement the defined policy for authenticated users throughout the network infrastructure.

Purpose of This Guide

This guide provides an overview of the design decisions involved in developing an effective ESP policy layer implementation, with best practice guidance for designing effective security policies while interoperating with a commonly available user database such as Microsoft Active Directory.

Design Goals

The desired result is a highly reliable and scalable design that is easy to maintain and adapt to changing organizational needs. Key features addressed by the Aruba ESP policy design guide include:

- End-to-end zero trust.
- Manageable design for any deployment type or size.
- Selection criteria to determine the most effective policy and implementation method.
- Information on each component and the role it plays in policy enforcement.
- Design options to provide flexible segmentation.
- Information on third-party integration.

The guide is not intended to provide an exhaustive discussion of all options, but it presents the most commonly recommended designs, features, and hardware.

Audience

This guide is written for IT professionals responsible for designing an Aruba ESP campus network. These IT professionals perform a variety of roles:

- Systems engineers who require a standard set of procedures for implementing solutions
- Project managers who create statements of work for Aruba implementations
- Aruba partners who sell technology or create implementation documentation.

Customer Use Cases

This version of the guide focuses on the policy needs of a typical campus network.

Zero Trust Overview

Zero Trust is a security model in which no device, user, or network segment is inherently trustworthy and must be treated as a potential threat.

To enhance security in modern enterprises where users and devices are remote and threats are bypassing traditional perimeter defenses, it is critical to adopt a rigorous security model that performs checks on a continuous basis. Before accessing the network, all devices and users should be identified and authenticated and given the least amount of access required, and then be continuously monitored

Benefits of Zero Trust

Zero Trust helps ensure network security for today's era of mobility, IoT, and work from home environments. Key benefits of Zero Trust include:

- Limits exposure to security risks related to vulnerable IoT devices.
- Helps reduce the risk of advanced threats that bypass traditional perimeter security controls.
- Limits damage related to lateral movement by attackers and infected devices.
- Takes a more holistic approach to security regardless of who or what is connecting and from where.
- Applies best practice such as micro-segmentation for a "Least Access" approach.

Requirements of Zero Trust

Aruba views the following three items as requirements for achieving Zero Trust in the network. These items will be discussed in more detail throughout this policy guide:

- **Authentication and Authorization:** Active and passive discovery of all users and devices on the network.
- **Least access micro-segmentation and control:** Access control policies grant access only to resources that are absolutely necessary for a device or user and segment them from other resources that are not required.
- **Continuous monitoring and enforcement:** Ongoing monitoring of users and devices on the network greatly reduces risks related to threats and malware.

Aruba Zero Trust Architecture

The Aruba Edge Services Platform (ESP) architecture provides flexible and highly reliable designs to ensure efficient access to applications and data for all authorized users, while simplifying operations and accelerating service delivery. Innovations in high availability combined with enhanced simplicity and programmability provide a best-in-class industry network solution for modern organizations.

Aruba ESP is an evolution of Aruba's end-to-end architecture, providing a Unified Infrastructure with centralized management that leverages Artificial Intelligence Operations (AIOps) for an improved operational experience with a Zero Trust Security policy. Aruba ESP is the industry's first platform that is built specifically for the new requirements of the Intelligent Edge.

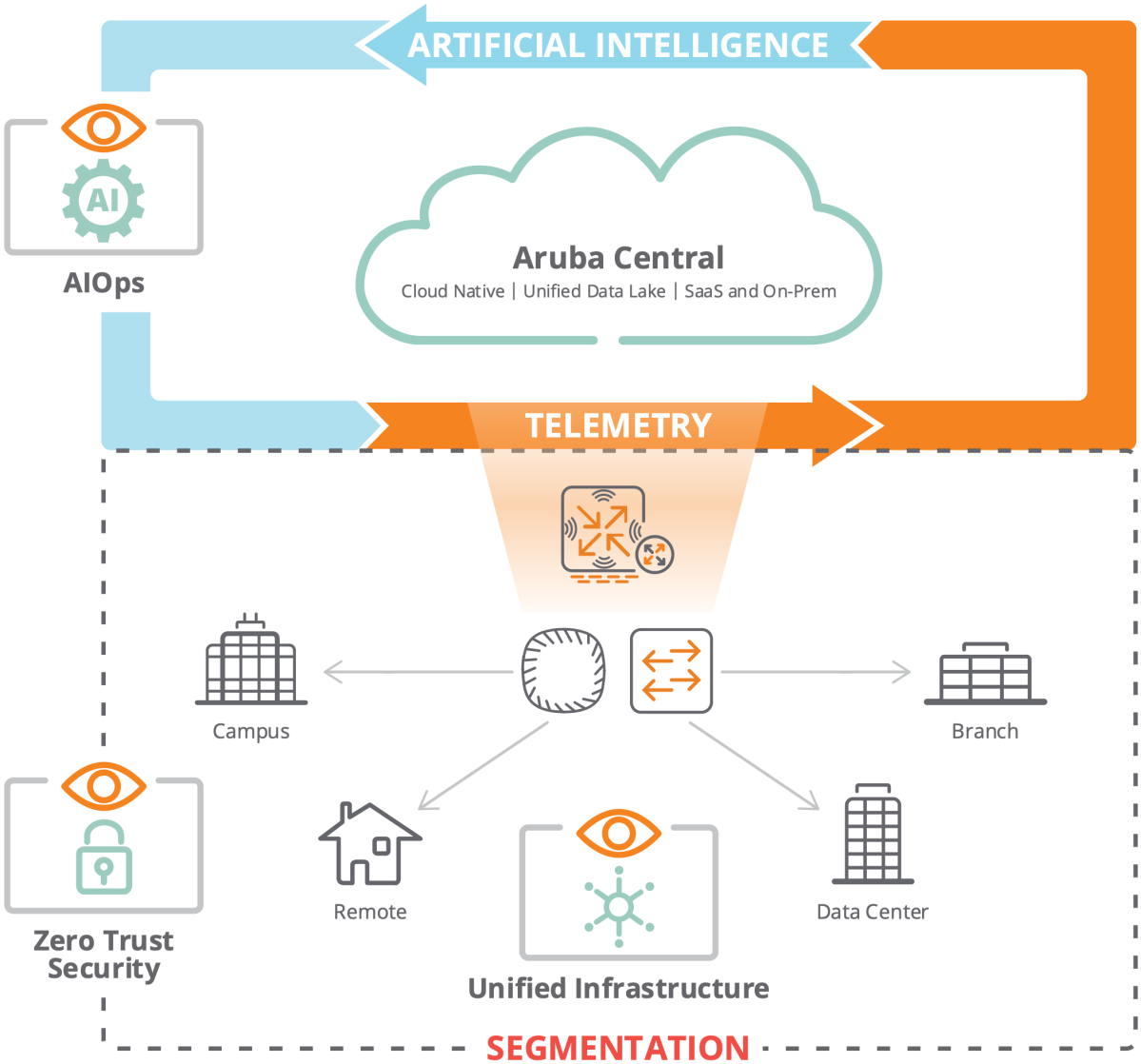

Figure 2: ESP Architecture

Aruba ESP offers a breadth of services, including onboarding, provisioning, orchestration, security, analytics, location tracking, and management. AI Insights reveal issues before they impact users. Intuitive, workflow-centric navigation enables the organization to accomplish tasks quickly and easily using views that present multiple dimensions of correlated data. Policies are created centrally, and features such as Dynamic Segmentation enable the network administrator to implement them over an existing infrastructure. The Aruba ESP architecture is built in distinct layers, as shown in the figure below.

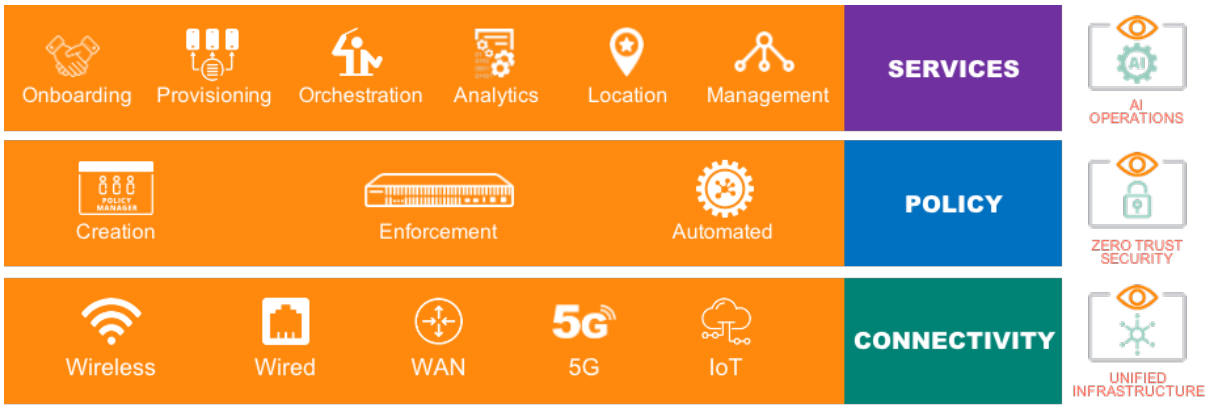

Figure 3: ESP Layers

Aruba ESP Policy Layer

The policy layer for the Aruba ESP campus is implemented using overlay technologies and traffic filtering mechanisms to isolate user and application traffic. Data traffic can be tunneled back to a gateway cluster for centralized enforcement or handled within a switch fabric that provides policy enforcement at every node in the network.

ClearPass Policy Manager is typically used to provide network authentication (i.e., RADIUS) to a user database (i.e., LDAP) and to define user roles with associated policies enforced within the network. Device Insights ensure that the endpoint security posture is determined from information gathered from the network.

Aruba ESP's powerful policy management is derived by separating policy from the network's IP design. Traffic tunneled to a gateway cluster is tagged at ingress with a user role that determines how the gateway treats the traffic during forwarding. Traffic in a distributed fabric is tagged using the VXLAN-Group Based Policy (GBP) feature to assign a role ID to every frame in the fabric, ensuring consistent policy enforcement across LAN, WLAN, and WAN.

Figure 4: ESP Policy Layer

Aruba Central NetConductor

Aruba Central NetConductor is a collection of edge-to-cloud networking and security services designed to achieve a consistent Zero Trust network. Central NetConductor reduces the complexity of addressing connectivity and security challenges by automating deployment, operations, and security policy of the network in a cloud-native service.

The sections below describe the creation of roles and policy, applying roles to users, and the enforcement of policies based on roles within the NetConductor Framework

Policy Definition

Roles

A role is simply a way to represent a grouping of users or devices. A role is assigned when a new user or device is brought onto the network. Aruba uses various methods to assign roles, and there are multiple ways a role can impact policies.

Historically, roles and their accompanying policies were defined separately for each platform in the network in various places. Going forward, roles are defined in Aruba Central Global Policy Manager or Aruba Central, and this centralized configuration is applied consistently across all network infrastructure.

Roles are assigned to users and devices using a network access control (NAC) solution such as ClearPass or Cloud Auth.

Global Policy Manager

Aruba Central Global Policy Manager configures roles and role-to-role policies. To make these roles more powerful and consistent with the ESP architecture, they can be managed globally from Aruba Central. For example, if you have five roles in your network, a role-to-role policy is created by defining permissions from one role to another. By configuring this only once in Central, it is applied to all relevant network devices: from a Microbranch or Bridge Mode AP, to a Mobility Gateway, to a switch. There is no need to build three different formats of security policy.

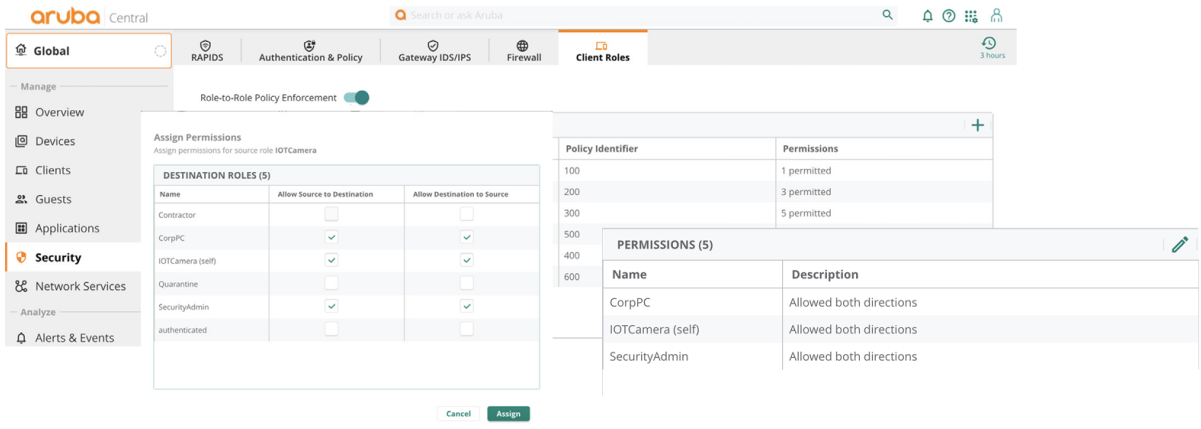

Figure 5: GPM

Authentication and Authorization

ClearPass

ClearPass Policy Manager is a full-featured RADIUS, TACACS, guest lifecycle management, and captive portal platform. In a Zero Trust architecture, ClearPass can be responsible for **Authentication and Authorization**, providing initial onboarding for the network and assigning the **Role** or other attributes that are used in enforcement. ClearPass also provides **continuous monitoring and enforcement**, changing the access level of any device on the network based on monitored changes or events.

ClearPass can access user and device authentication information stored within a local database, a user database connected to the local network, or a cloud-hosted user database. ClearPass has the ability to query most sources for user information using a variety of authentication methods.

ClearPass Policy Manager provides secure role- and device-based network access control for Internet of Things (IoT), bring your own device (BYOD), and corporate devices as well as for employees, contractors, and visitors across wired, wireless, and VPN infrastructure. With a built-in, context-based policy engine, RADIUS, TACACS+, non-RADIUS enforcement using OnConnect, device profiling, posture assessment, onboarding, and visitor access options, ClearPass is unrivaled as a foundation for network security for organizations of any size.

ClearPass also supports secure self-service capabilities, making it easier to access the network. Users can securely configure their own devices for enterprise use or Internet access based on administrative policy controls. Aruba wireless customers get unique integration capabilities, such as AirGroup, as well as ClearPass Auto Sign-On (ASO). ASO passes users' network authentication automatically to their enterprise mobile apps, so they can get right to work.

ClearPass Policy Manager Key Features

- Role-based, unified network access enforcement across multi-vendor networks
- Intuitive policy configuration templates and visibility troubleshooting tools
- Support for multiple authentication/authorization sources (AD, LDAP, SQL)
- Self-service device onboarding with built-in certificate authority (CA) for BYOD
- Visitor access with extensive customization, branding, and sponsor-based approvals
- Integration with key UEM solutions for in-depth device assessments
- Comprehensive integration with the Aruba 360 Security Exchange Program.

ClearPass is the only policy platform that centrally enforces all aspects of enterprise-grade NAC for any industry. Granular policy enforcement is based on a user's role, device type and role, authentication method, unified endpoint management (UEM) attributes, device health, traffic patterns, location, and time of day. The scalable deployment supports tens of thousands of devices and authentications, surpassing the capabilities of legacy AAA solutions. Options are available for small to large organizations with centralized or distributed environments.

Cloud Auth

Cloud Auth on Aruba Central provides a seamless, cloud-based onboarding and NAC solution. Small and medium-sized organizations with limited IT personnel benefit from simplified workflows and secure role-based policies administered through Aruba Central to ensure that users and devices have appropriate network access.

In a Zero Trust architecture, Cloud Auth can be responsible for **Authentication and Authorization**, providing initial onboarding for the network, and assigning the **Role** or other attributes that are used in enforcement. Cloud Auth also provides **continuous monitoring and enforcement**, changing the access level of any device on the network based on monitored changes or events.

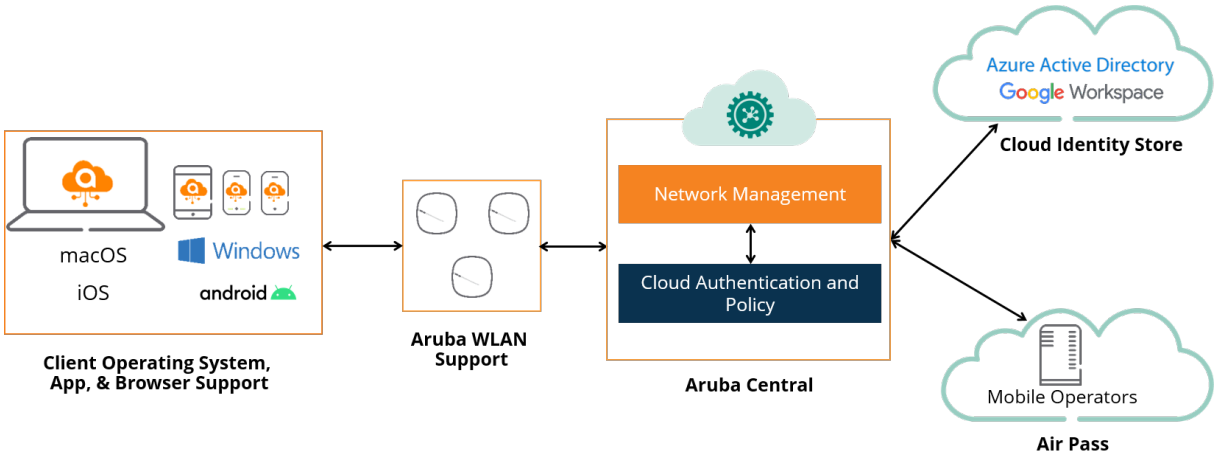

Figure 6: Clouth Auth Overview

Enforcement

Central NetConductor gives network and security teams a shared toolbox to ensure optimal connectivity and the appropriate level of protection. It extends the capabilities of Aruba's market-leading Dynamic Segmentation across multiple network overlays, making it easy to adopt comprehensive Zero Trust and SASE security.

NetConductor supports two deployment models, Centralized and Distributed.

Centralized

In a centralized policy model, wireless and/or wired data traffic is tunneled back to a gateway cluster for security enforcement and traffic-shaping.

In the example below, a user from the finance department authenticates to the campus network. Another user is logged into a guest kiosk computer directly connected to a UBT-enabled switch. Both the AP and the switch forward traffic via GRE tunnels to the Gateway. The Gateways decapsulate and analyze the traffic, apply security policy based on user roles and other attributes, then forward the traffic to their authorized destinations. In this case, all enforcement is performed at the Gateways.

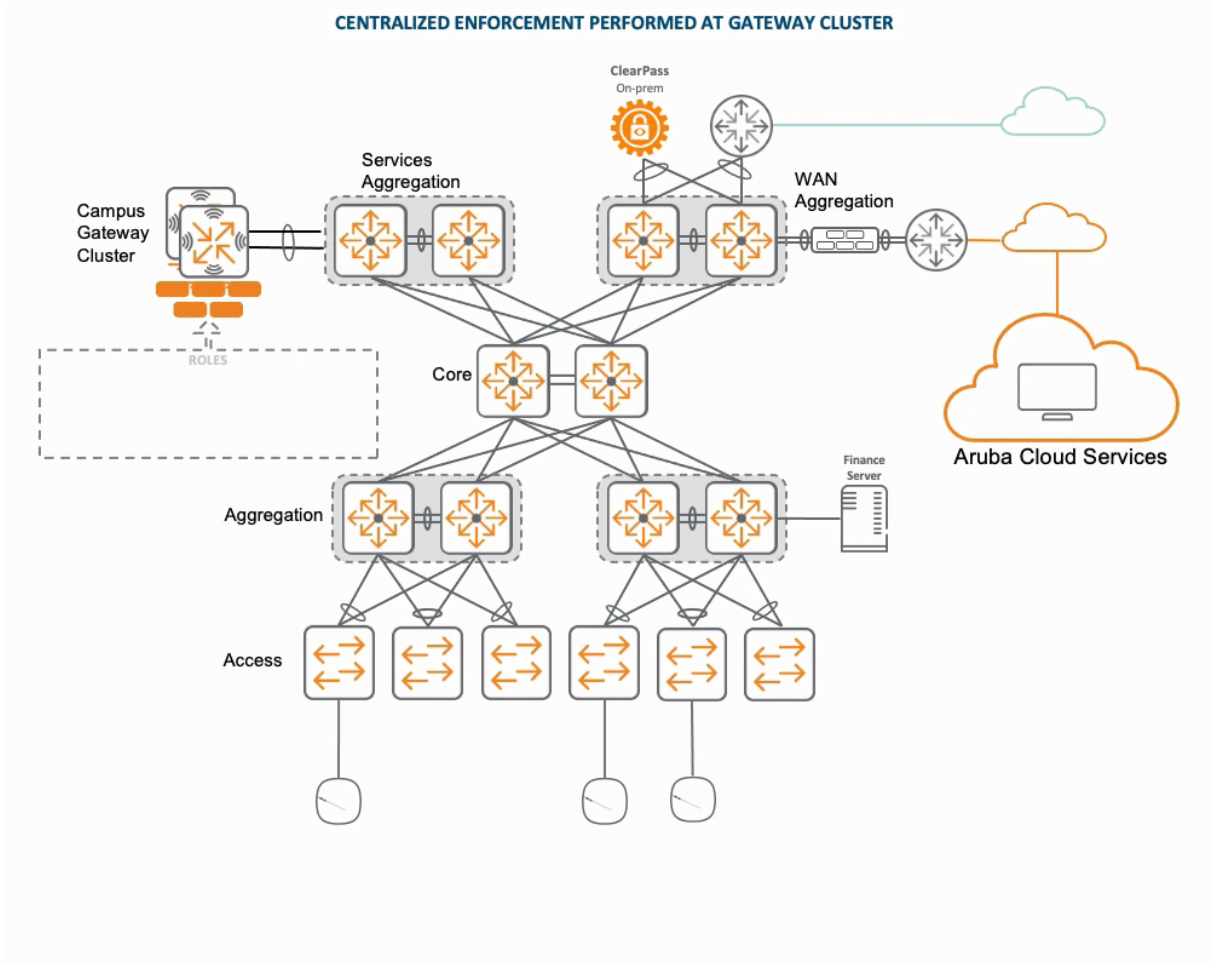

Figure 7: Centralized Enforcement

Distributed

Distributed policy enforcement uses VXLAN tunnels to create virtual networks between switches. Aruba CX switches are able to enforce policy locally with many of the same capabilities found on gateways. This is particularly powerful when securing east-west traffic within a campus. These capabilities are described as the Aruba ESP NetConductor solution.

NetConductor pairs VXLAN with an MP-BGP EVPN control plane to ensure endpoint reachability across geographically diverse subnets and broadcast domains.

In the example below, a wired user from the finance department authenticates to the campus network. A different user is logged into a guest kiosk computer. The switches analyze the traffic locally, apply security policy based on user roles and other attributes, then forward the traffic to their authorized destinations. Using the native firewall capabilities of the switches, policy enforcement can be performed at the edge, allowing the traffic to take a more direct path to its destination. This strategy results in greater flexibility and scalability than the centralized model.

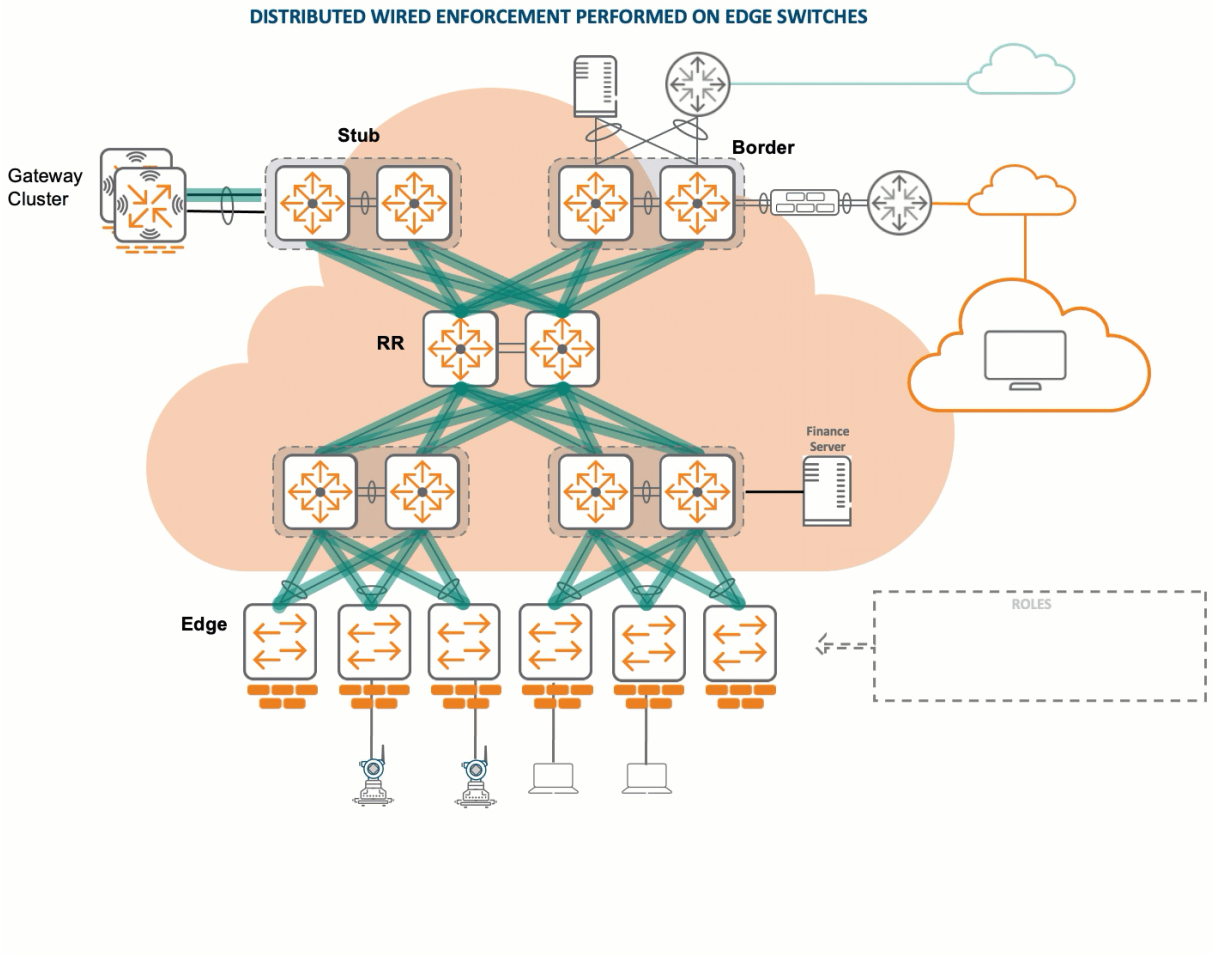

Figure 8: Distributed Enforcement

WAN Propagation

For a role based Zero-Trust model to be effective, the role must travel with data-packets across the WAN environment. Both of Aruba's SD-WAN solutions, EdgeConnect SD-Branch and EdgeConnect SD-WAN, support this capability.

Summary

The table below summarizes the Aruba product that helps achieve various facets of Zero Trust.

Requirement	Zero Trust Architecture	Aruba ESP Solution
Know what is on the network	An organization protects resources by defining what resources it has	Aruba Central Client InsightsClearPass Policy ManagerCloud Auth
Authenticate all users and devices	Create, store, and manage enterprise user accounts and identity records	ClearPass Policy ManagerCloud Auth

Requirement	Zero Trust Architecture	Aruba ESP Solution
Ensure that asset configuration and compliance guidelines are followed	Gather information about the enterprise asset's current state and apply updates to configuration and software components	ClearPass Onguard
Assign and enforce access policies in the network	All resource authentication and authorization are dynamic and strictly enforced before access is allowed by coordinating a policy engine and a policy enforcement point	See the Policy Enforcement page that discusses how Zero Trust policies are enforced throughout the network.Aruba Roles
Communicate bi-directionally with the security ecosystem and respond to attacks	Provide real-time (or near real-time) feedback on the security posture of enterprise information systems; integrate with security information and event management systems	ClearPass Policy Manager/Aruba 360 Security Exchange

Roadmap to Zero Trust

Transitioning from a traditional network with minimal segmentation, authentication, or policy enforcement to a full Zero Trust environment requires deliberate planning, collaboration, and iterative implementation. This chapter provides a roadmap to help organizations move step-by-step toward achieving a secure Zero Trust model using HPE Aruba Networking solutions.

Start with the End in Mind: The NetConductor Vision

Creating a Zero Trust network starts with three core principles:

- Identify and authenticate every device on the network,
- Enforce business intent policy,
- Continuously monitor traffic on the network, reacting in real time.

HPE Aruba Networking NetConductor provides the tools to onboard diverse devices, enforce consistent policies, and dynamically adjust access levels based on user and device activity.

First, devices must be onboarded and authenticated to the network. HPE Aruba Networking NAC services simplify the onboarding process for Guest, IoT, BYOD, and corporate devices. This ensure that every device on the network is identified, authenticated, and categorized according to its role and purpose.

Next, policy enforcement ensures consistent and secure access to network resources. Centralized or distributed network fabrics apply access policies across the network, while SD-WAN capabilities extend these controls to geographically dispersed locations. This approach guarantees uniform security standards regardless of where devices connect.

Finally, continuous verification enhances security by monitoring user and device behavior in real time. Access levels are modified dynamically based on activity, ensuring that the network enforcement adapts to evolving conditions and potential threats. This ongoing evaluation helps maintain a secure environment without compromising operational efficiency.

The ultimate goal is to replace the traditional “allow-all” model with a dynamic Zero Trust framework. In this model, every user and device interaction is verified, and access is granted only to authorized resources. By following the steps outlined below, organizations can achieve a fully realized Zero Trust environment, underpinned by granular control, compliance, and continuous monitoring.

Step 1: Develop a Policy Matrix

The first step in building a Zero Trust network is developing a comprehensive policy matrix. This document maps roles, devices, and access levels across the organization, acting as the foundation for network security. This document is built by engaging key stakeholders—including IT, operations, and business leaders—to align network policies with organizational goals. This collaboration ensures that the policy matrix reflects both security requirements and business priorities.

After a policy based on business policies is created, it must be enacted into the network. The numerous ways to accomplish this are outlined in this chapter.

Understand the Network's Composition

Before defining policies, its critical to understand which devices connect to the network, how they connect, their traffic flows, and the kind of traffic they generate. A full inventory of endpoints helps inform the development of the policy matrix.

Data can be gathered using tools such as HPE Aruba Networking Central Client Insights, MDM solutions, and endpoint management systems, and by collaborating with endpoint management teams.

The example table below documents the devices connecting to the network.

Endpoints	Connectivity Type	Authentication Type	Traffic Type	Traffic Pattern	Notes
Android Tablets	wireless	Dot1x	User traffic	N-S, E-W	enterprise communication
Zebra Scanner	wireless	MAC	User traffic	N-S, E-W	PoS scanners
Windows	wired, wireless	Dot1x	User traffic	N-S, E-W	PoS system
Apple tablets	wireless	Dot1x	User traffic	N-S, E-W	enterprise communication
Camera (PoE)	wired	MAC	Video	N-S	physical security
Badge Reader (PoE)	wired	MAC	Data	N-S	physical-access security
Printer	wired	no-auth	Data	E-W	Printers for PoS systems
Media player	wired, wireless	no-auth	Video	N-S	multicast stream

This image provides an example of client discovery using Client Insights within HPE Aruba Networking Central.

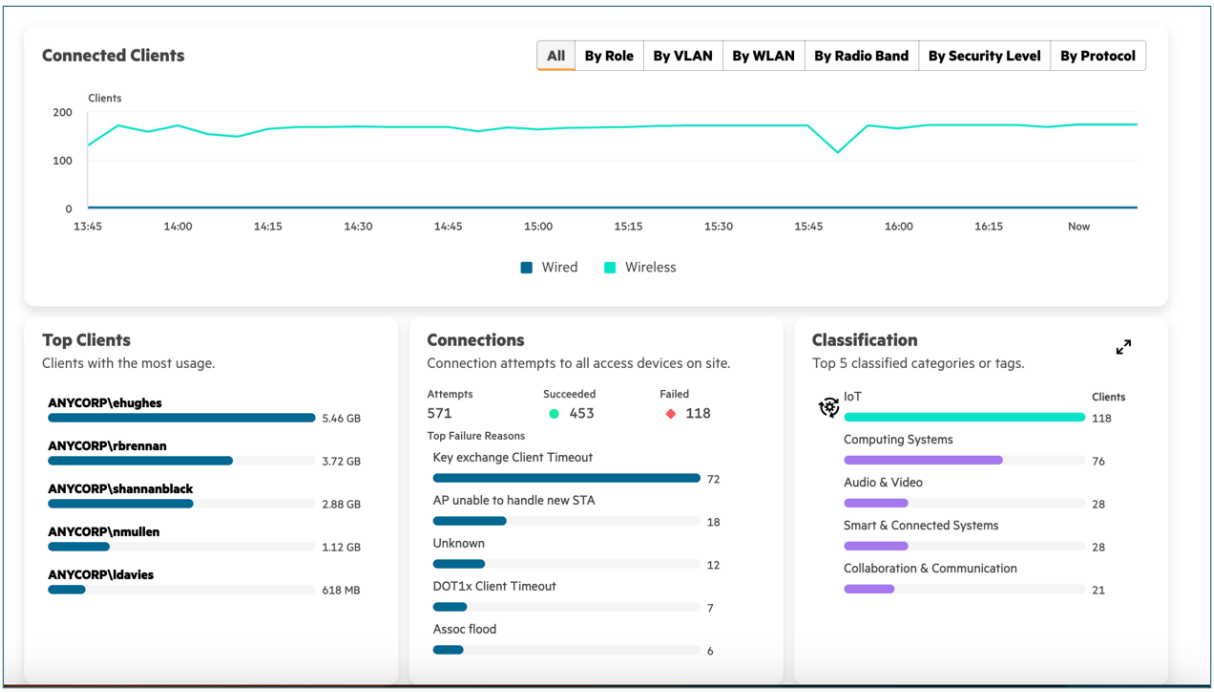

Figure 9: Client Insights

Start Small

When creating the initial policy matrix, it is essential to start small and expand as the network administrators grow more comfortable with Zero Trust policies. This approach minimizes disruption to business operations and allows for iterative refinement of policies. Begin by defining a limited set of high-level roles, such as “Guest,” “IoT,” and “Employee”. These roles should capture the broadest categories of access needs initially without delving into excessive granularity.

For each role, define basic access permissions and denials. For example:

- **Guest Role:** Allow access to internet services (HTTP/HTTPS) but block all internal network resources.
- **IOT Role:** Permit communication with cloud control services while restricting access to internal applications and peer-to-peer device communication.
- **Employee Role:** Provide access to corporate resources based on departmental needs while blocking access to sensitive administrative systems.

Gather Data for Policy Design

To build these roles effectively, use existing network monitoring tools to analyze traffic patterns. Tools such as NetFlow or AppRF provide insights into typical device behavior, helping to identify which resources are accessed most frequently by different groups. Additionally, HPE Aruba Networking Central Client Insights can provide valuable information by identifying what is running on the network

and by analyzing communication patterns. This visibility is critical for refining role definitions and understanding traffic flows. For example, these tools can detect specific application dependencies and peer-to-peer communications, aiding in the development of precise access policies. Use this data to validate initial role definitions and ensure that they align with real-world usage.

Iterative Expansion

After successfully implementing basic roles and policies, gradually expand the policy matrix to include additional roles and finer-grained access controls. For example, split the Employee role into sub-roles such as “Finance”, “Engineering”, and “Sales”, each with tailored permissions. Introduce conditional policies that adjust roles based on device posture or network location. For example, restrict access to financial applications unless the device is connected via a secure, corporate-managed endpoint.

By starting small and expanding iteratively, organizations can develop a robust policy framework without overwhelming IT teams or disrupting business operations. This incremental approach ensures that policies remain manageable and effective as the network evolves.

The image below shows an example of grouping of devices into “roles” and an associated policy created using Central Policy Manager.

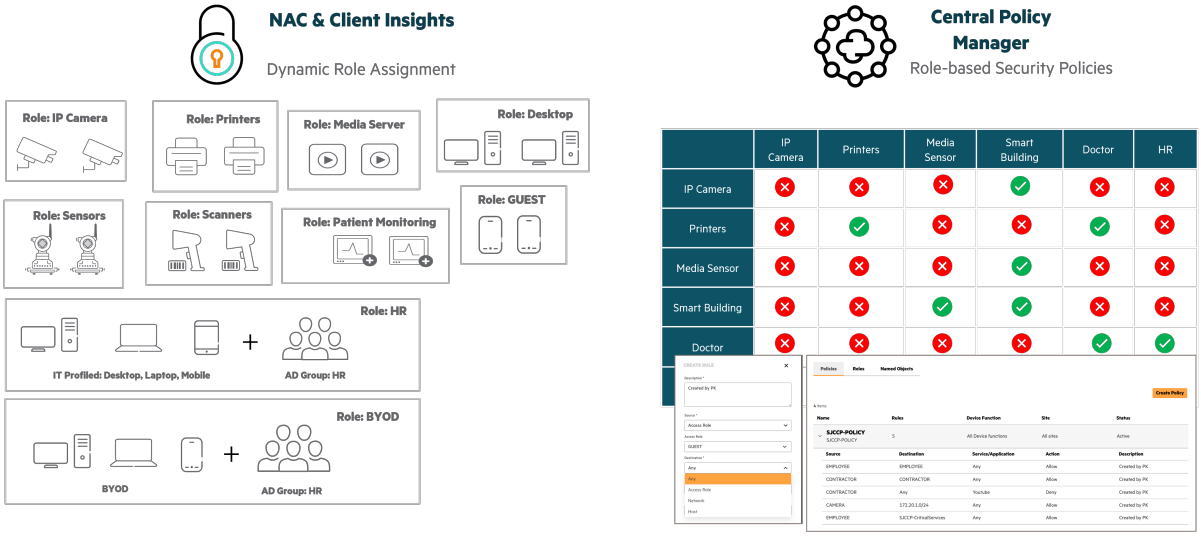

Figure 10: NAC and Policy

Step 2: Address Networks Without Network Access Control

Organizations without existing NAC capabilities can still make significant strides toward Zero Trust with other methods of role assignment. Shift from IP-based controls to role-based policies to establish a more adaptive security model while gaining familiarity with policy enforcement based on user identity instead of IP subnets. Examples of how to get started with role based policies, without a NAC solution, are provided below.

Role Derivation on AOS-10 Gateways

Enable role derivation to dynamically assign roles during the connection process when a NAC server is not used. Configure the derivation rules to evaluate attributes such as the SSID, MAC address, or device OS. For example, corporate devices connecting to the “Corp-WiFi” SSID could be assigned an “Employee” role, while IoT devices connecting to the “Corp-WiFi” SSID could be assigned the IoT role by matching a vendor OUI.

VLAN Role Mapping on SD-WAN Gateways

Both EdgeConnect SD-WAN and EdgeConnect SD-Branch gateways provide the capability to map a physical interface or VLAN interface to a role. This feature is particularly useful as a fallback or default-role mechanism, assigning a role to traffic when a NAC solution is not yet in place or before individual user roles are dynamically assigned.

Using VLAN-to-role mapping is an excellent starting point for organizations beginning their journey into role-based policies. By mapping existing VLANs to roles, you can implement role-based segmentation without requiring the immediate deployment of a NAC solution. For example, a VLAN designated for guest traffic can be assigned a “Guest” role, while an IoT VLAN can be assigned an “IoT” role.

This approach offers a dual benefit: it enables role-based control of network traffic and provides a low-risk environment to familiarize IT teams with managing roles. As your organization gains experience with this framework, it can be better prepared to adopt more advanced NAC capabilities and dynamically assign roles to individual users and devices.

By starting with VLAN-to-role mapping, organizations can establish a strong foundation for Zero Trust principles while minimizing complexity and disruption.

Step 3: Adopt a NAC Solution

Introducing a NAC solution is a pivotal step in implementing Zero Trust. HPE Aruba Networking NAC solutions provide robust capabilities for device authentication and role assignment. Most NAC solutions, even free ones, can integrate with Aruba’s Vendor-Specific Attribute (VSA) “Role,” enabling seamless role-based controls across the network.

Profiling IoT Devices with Client Insights

One of the most significant security challenges is managing IoT devices, which often lack traditional authentication capabilities. HPE Aruba Networking Central Client Insights, integrated with HPE Aruba Networking NAC solutions, enables deep device profiling based on observed behavior and attributes. For example, a surveillance camera can be identified by its MAC address, traffic patterns, and manufacturer information. After profiling, assign an IoT-specific role that restricts access only to the required cloud control services, while blocking all internal resources.

Managing BYOD with ClearPass BYOD Certificates

BYOD devices present another layer of complexity due to their diverse ownership and configurations. Use HPE Aruba Networking ClearPass's BYOD onboarding feature to issue unique device certificates during the enrollment process. These certificates ensure that only authorized personal devices can connect to the network. Define a BYOD role that limits access to internet resources and specific corporate applications, while blocking sensitive internal systems.

Guest Access with AUP Pages

For Guest devices, simplicity is key. Implement a captive portal with an Acceptable Use Policy (AUP) page to ensure compliance before granting access. Configure HPE Aruba Networking ClearPass to assign the Guest role upon successful authentication or AUP acceptance. This role should permit basic Internet access while denying all internal resource connections. Aruba's flexible captive portal options support branding and customization to align with organizational needs.

Corporate Devices with 802.1X Authentication

Corporate-owned devices typically demand the highest level of trust and access. Use 802.1X authentication to verify users and devices. An enterprise PKI (Public Key Infrastructure) should be used to issue machine and user certificates. Assign these devices to an "Employee" role, with access tailored to departmental requirements. For additional security, incorporate endpoint posture checks with MDM (mobile device management) to validate compliance with corporate standards before granting full access.

Consider these common strategies to ensure comprehensive coverage and maintain consistent policy enforcement across diverse device types and user groups.

Step 4: Start Small with Enforcement

Zero Trust benefits become tangible when it comes to policy enforcement. Begin small with limited enforcement to minimize migration challenges while validating the effectiveness of new policies. Focus on restricting access to sensitive resources for low-trust roles. For example, establish preliminary policies to deny IoT devices from accessing internal file servers or to block guest devices from communicating with production networks.

Start with VLAN-Based Enforcement

The simplest way to begin is to enforce VLANs. Assign roles to specific VLANs and apply ACLs at the VLAN level to restrict traffic. For example, a Guest VLAN might only permit HTTP/HTTPS traffic to external destinations, while an IoT VLAN allows communication only with specific cloud endpoints. This approach provides immediate segmentation and can be implemented without major changes to network configuration or operation.

Expand to Role-Based Enforcement

Consider incorporating Aruba's role-based policies for more granular control where roles are derived dynamically through a NAC, enabling enforcement based on real-time user and device attributes.

Centralized Fabrics

Centralized fabrics are straightforward and highly effective. These fabrics enable centralized role-based policy enforcement, allowing for scalable and consistent policy application. In certain cases, centralized fabrics can be layered onto an existing network without disruption. For example, organizations can enforce Zero Trust policies specifically for contractors accessing the network while leaving the rest of the infrastructure unchanged. To learn more about Centralized Fabrics, refer to the NetConductor Enforcement Models chapter of the Policy Design guide..

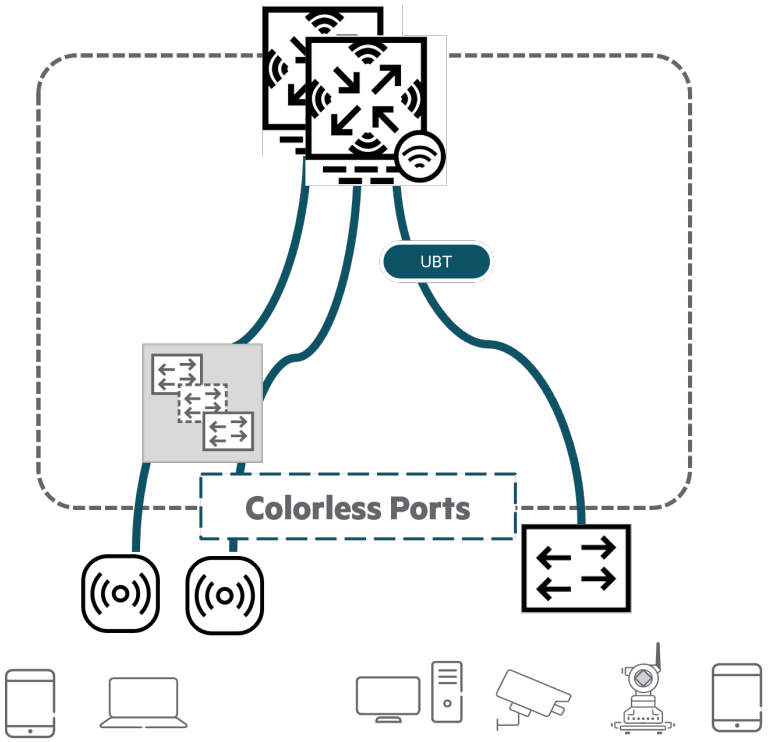

Figure 11: Centralized Fabrics

Distributed Fabrics

Distributed fabrics work well in environments with significant east-west traffic requirements where distributed policy enforcement at the edge is required. Unlike centralized fabrics, which route traffic through a core enforcement point, distributed fabrics enable policy enforcement closer to the edge, reducing latency and optimizing bandwidth usage. To learn more about Distributed Fabrics, refer to the policy enforcement page.

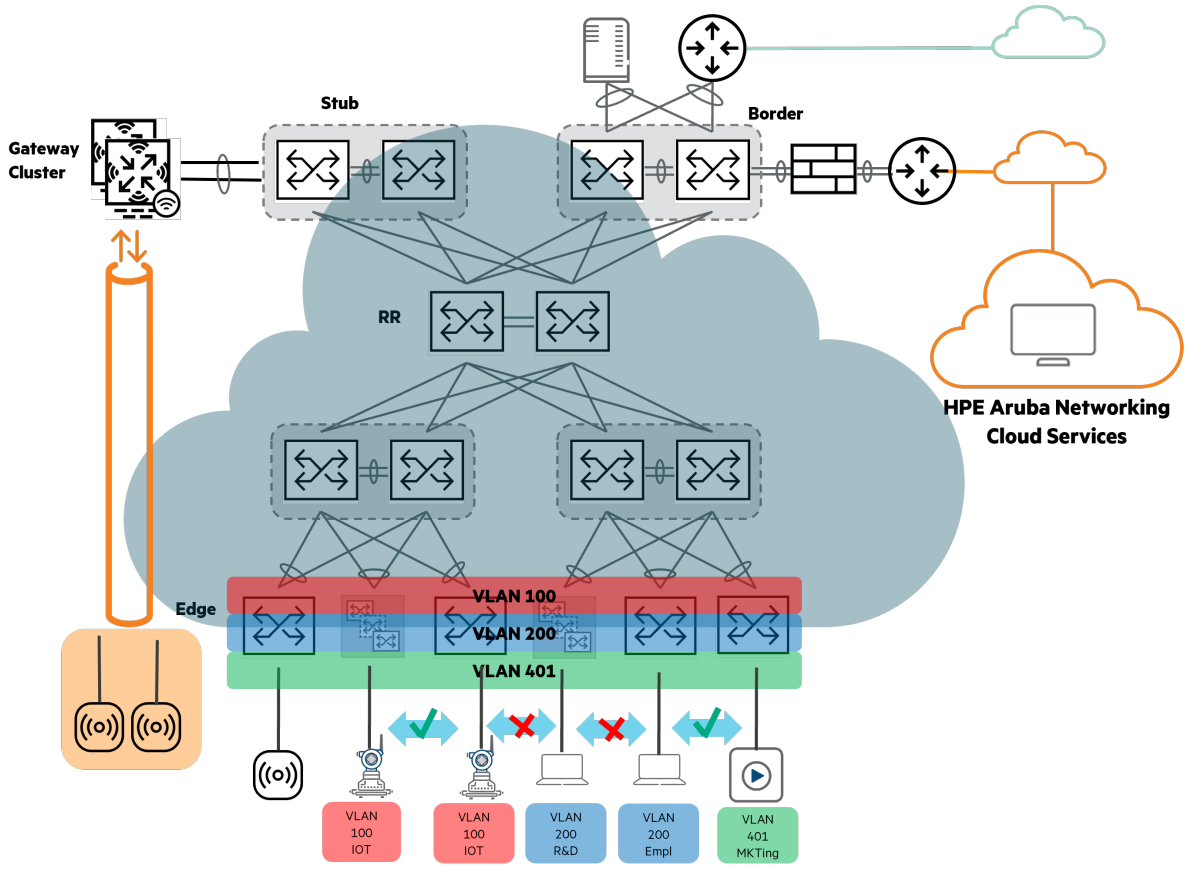

Figure 12: Distributed Fabrics

SD-WAN Gateways

EdgeConnect SD-WAN gateways can use roles to enhance and extend security and policy enforcement directly at the network edge. This integration provides a highly scalable, on-premise enforcement point that supports a broad range of advanced security capabilities, including zone-based firewall policies, intrusion prevention and detection systems (IPS/IDS), and application-aware policy enforcement.

Role-Based Zone Firewall Policies

Roles can be integrated seamlessly into EdgeConnect's zone-based firewall policies, offering fine-grained control over traffic flow between zones. For example, using "Guest," "IoT," and "Corporate" roles can determine the access rules applied between zones, such as restricting guest traffic to Internet-only zones or limiting IoT devices to communicate only with designated cloud services. Incorporate roles into zone policies to ensure that access control decisions are both context-aware and consistently enforced across the network.

Role Integration with Business Intent Overlays

Business Intent Overlays (BIOs) are a key feature of EdgeConnect SD-WAN gateways, providing the ability to define traffic handling and prioritization based on business requirements. Roles enhance BIO policies dynamically by influencing how traffic is routed and prioritized. For example, traffic from devices assigned an “Executive” role might be routed over the highest-performing, lowest-latency path, while “Guest” role traffic could be relegated to a secondary path with lower priority. This ensures that critical applications and users receive the performance they need without compromising network efficiency.

On-Premises Security Enhancement with Roles

EdgeConnect SD-WAN gateways offer powerful on-premise security options, and roles further enhance these capabilities.

- **IPS/IDS Integration**: Roles can influence how IPS/IDS policies are applied. For example, traffic from devices in the “Corporate” role might be subject to stricter intrusion detection policies than “Guest” traffic, reflecting the higher security requirements for sensitive corporate data.
- **Application-Aware Policies**: EdgeConnect’s application visibility allows organizations to create granular, role-specific policies. For example, users in the “Sales” role can have prioritized access to CRM applications, while “IoT” role devices can be restricted to communicating only with approved application endpoints.
- **Web Filtering and URL Categorization**: Role-based policies can be extended to web filtering, where “Guest” roles might be restricted from accessing certain categories of websites, while “Employee” roles can have more lenient access based on business needs.

By combining roles with EdgeConnect’s advanced security features, organizations can implement a Zero Trust approach that is not only robust but also highly adaptable. Roles add a layer of contextual intelligence to firewall rules, IPS/IDS, application prioritization, and more, ensuring that every enforcement decision aligns with the organization’s security and business objectives. This powerful integration allows EdgeConnect SD-WAN gateways to act as a critical enabler of Zero Trust security, all while optimizing traffic and enhancing user experiences.

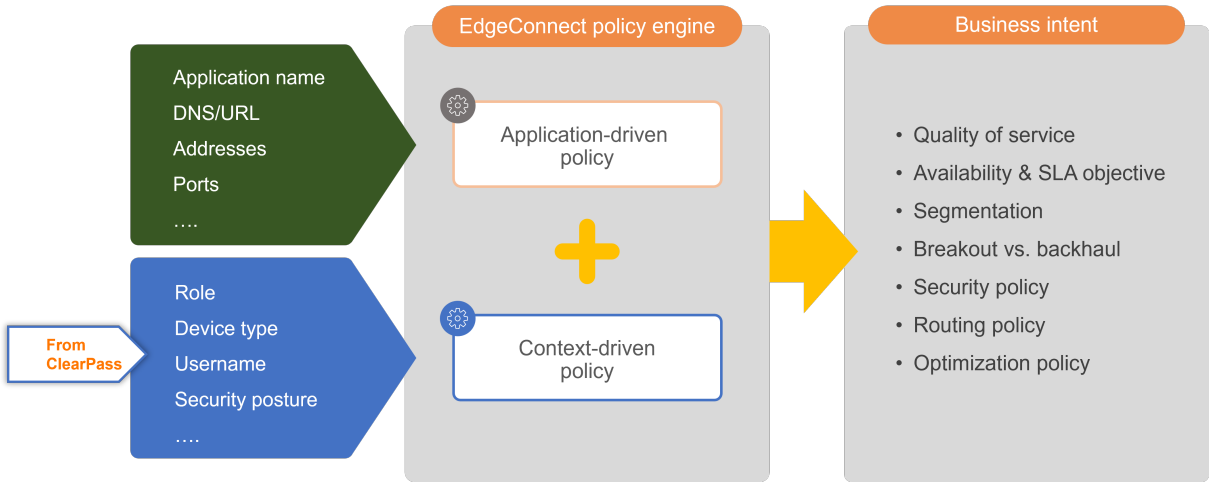

Figure 13: EdgeConnect Role Usage

Step 5: Expand as the Network Modernizes

As network infrastructure evolves, expand Zero Trust implementation to encompass more sophisticated controls. Adoption of Roles, a cornerstone of Aruba's Zero Trust capabilities, enables real-time policy assignments based on evolving contextual factors. Replace static VLAN configurations with Roles to streamline operations and reduce complexity.

Extend Zero Trust across a WAN environment by integrating Aruba's SD-WAN solutions into a Zero Trust architecture. This ensures consistent policy enforcement across a distributed enterprise.

Enhance visibility with Aruba Central, which provides detailed dashboards and analytics for tracking device behavior, user activity, and application performance. Use these insights proactively to address anomalies and refine the policy matrix. For example, if a previously trusted device begins accessing resources outside its assigned role, trigger an automatic quarantine response.

Deploy advanced threat detection capabilities, such as Aruba's Intrusion Detection and Prevention (IDP) systems, to complement the Zero Trust strategy. These systems can identify and mitigate threats that bypass traditional defenses, ensuring comprehensive protection.

Plan your policy design strategy using the steps above to implement an efficient, effective comprehensive strategy with minimal disruption to existing network operation. Address policy design in phases, starting with restricting access at the highest level and layering policy based on usage levels and risk zones. Often, careful planning based on these steps can eliminate redundant policies and enforcement practices and reduce implementation and maintenance time when upgrading existing infrastructure.

Finally, adopt a continuous improvement mindset. Schedule periodic reviews of Zero Trust implementations, incorporating lessons learned from incident reports, audits, and industry trends. Regularly update policies, roles, and enforcement mechanisms to address emerging threats and adapt to organizational changes.

Policy Definition

Definition of policy involves business-oriented discussion more than a technical one. It requires categorizing users and devices based on their connectivity needs and specifying the access permissions for each group. This is accomplished by defining Aruba Roles and then associating those roles to a policy in Global Policy Manager.

Roles

An Aruba role is simply a way to represent a grouping of users or devices, which is assigned when connecting to the network. Aruba ESP provides the ability to assign a role to any connected client in the network and enforce the policy based on the role.

IT administrators define a role for every type of user or device attempting to gain access. All traffic for an assigned role is subject to its associated policy throughout network.

During the authentication and authorization process, organizations can apply a long list of built-in and customizable attributes that Aruba devices support based on the role assigned. These attributes provide administrators with additional classifications to allow or deny network access.

Available attributes include:

- Hostname
- IP address
- Location of a gateway
- MDM membership status
- Firewall traffic classification
- Client OS version
- Time of day
- Profiled device type.

Precise assignment of a role is an important foundation for enforcing Zero Trust policy in an organization.

Roles defined for users and devices should be grouped with a common set of security requirements. Keep the number of roles as small as possible, while still obtaining the desired security policy. The fewer roles in use, the easier it is to understand and maintain policy.

Policies

A policy and its assigned roles must be defined carefully to serve as a comprehensive solution that provides appropriate, uninterrupted access to all trusted network devices, while securing the network from threats.

A policy is a set of rules governing client behavior on the network. A policy rule defines the traffic permitted or denied traffic between roles. Roles are often dynamically assigned during authentication, and all traffic from the associated user or device is marked with a role ID for that access instance.

After traffic is marked with a unique role ID, the policy can be enforced on any Aruba device, which ensures a consistent security posture across all areas of the network.

Global Policy Manager

The Aruba Central cloud platform hosts applications to manage policy across the ESP architecture. Central provides an interface identified as Global Policy Manager (GPM). Within GPM, an operator defines the roles and role-to-role policies. These elements are then pushed to relevant networking infrastructure for enforcement.

An example of GPM in use today is a NetConductor fabric. The switches and gateways in a NetConductor fabric use a policy ID (Aruba Role) marked in the VXLAN header of every packet in the overlay to enable policy enforcement anywhere in the network. Policies are configured through the **Client Roles** interface in the gateway **Security** configuration section on Central.

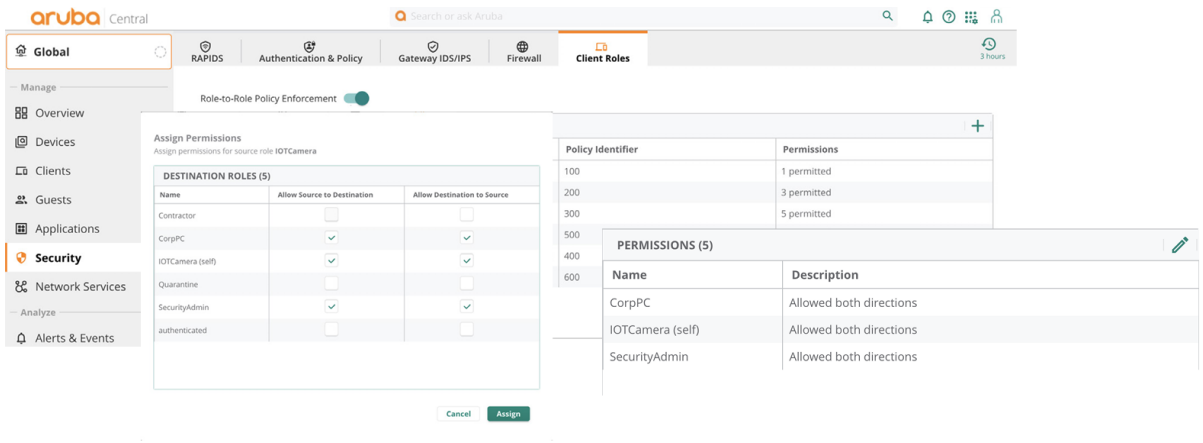

Figure 14: GPM

Additional Policy Managers

Global Policy Manager is the future for unified policy definition at Aruba. Policy definition within GPM will continue to be enhanced and support more Aruba products in the future. Today, policy also is managed in the following additional products:

- Campus policy on AOS-10 Gateways
- Data center policy with Pensando Policy Manager
- SD-WAN policy on AOS-10 Gateways
- SD-WAN policy on EdgeConnect SD-WAN gateways

Authentication Design

Authentication is the process of validating that a user or device is who they claim to be, and authorization is the process of determining the type of access given to that user or device. This chapter discusses how these tasks are performed in an enterprise network, as well as how to design the systems responsible for authentication and authorization.

Campus & Branch Networks

ClearPass

ClearPass is the on-premise network access control solution for campus and branch networks. It is a flexible and powerful solution that can be implemented as a physical or virtual appliance in multiple virtual environments. While it can be deployed as a stand-alone AAA server, it is best practice to deploy a cluster of multiple ClearPass instances for high availability (HA) and load balancing. Refer to the Installation Guide for details.

The implementation and operation of ClearPass are managed directly within the web UI of the Publisher node. The ClearPass Deployment Guide provides detailed procedures for installing the solution. Refer to the ClearPass User Guide for more complete coverage of features and commands.

When using ClearPass, take time to plan the desired client experience when joining the network. Create a flow chart to outline the authentication and authorization process for sharing with both technical and business teams. This sets proper expectations and illustrates the benefits of the new solution. It also ensures that stakeholders understand the benefits of additional security steps.

Defining user experience and business requirements determines which ClearPass functions are required for implementation. This guide lists ClearPass services and features used in most implementations.

The sections below outline key considerations when deploying ClearPass.

Cluster Design

ClearPass uses a Publisher/Subscriber model to provide multi-instance clustering. Another term for this model is *hub and spoke*, where the hub corresponds to the Publisher, and the spokes correspond to the Subscribers. This section provides guidance on how to design ClearPass clusters.

ClearPass can be deployed either as a dedicated hardware appliance, virtual machine running on top of VMware vSphere Hypervisor or Microsoft Hyper-V, or in the public cloud.

The **Publisher node** functions as the controller in a cluster. The Publisher is the central point of configuration, monitoring, reporting, and database replication. The Publisher manages all databases. There can be only one active Publisher in this model, with a potentially unlimited number of Subscribers. The Publisher node has full read/write access to the configuration database. All configuration changes must be made on the Publisher. The Publisher node sends configuration changes to each Subscriber node.

The **Subscriber nodes** are worker nodes. AAA load, RADIUS requests, and policy decisions are made on Subscriber nodes. Subscriber nodes maintain a read-only local copy of the configuration database.

NOTE:

Refer to the **Policy Manager Ordering and Sizing Guide** on the Aruba Support Portal for additional ClearPass cluster guidance, or contact your Aruba account team.

The following factors determine the size of a Policy Manager cluster.

- Determine how many endpoints must be authenticated.
    1. The number of authenticating endpoints can be determined by taking the number of users times the number of devices per user.
    2. To this total, add other endpoints that perform MAC-based authentication, such as printers and other non-authenticating endpoints.
- Take into account the following factors:
    1. Number and type of authentications and authorizations:
        - MAC authentication/authorizations vs. PAP vs. EAP-MSCHAPv2 vs. PEAP-MSCHAPv2 vs. PEAP-GTC vs. EAP-TLS
        - Active Directory vs. local database vs. external SQL datastore
        - No posture assessment vs. in-band posture assessment in a PEAP tunnel vs. HTTPS-based posture assessment by OnGuard.
    2. RADIUS accounting load
    3. Operational tasks taking place during authentications, such as configuration activities, administrative tasks, replication load, periodic report generation, etc.
    4. Disk space consumed
        - Note that Policy Manager writes copious amounts of data for each transaction. (this data is displayed in the Access Tracker).

Publisher Design

The Publisher server must be sized appropriately because it handles database write operations from all Subscribers simultaneously. The Publisher also must be capable of handling the total-number of endpoints within the cluster and be capable of processing remote work directed to it when guest-account creation and onboarding occur.

To optimize Publisher performance in a large-scale environment, the Publisher should not receive direct authentication or Guest/Onboard requests, so that its resources can be dedicated to replication traffic and API requests from Subscribers.

If the worker traffic sent from the Subscriber servers is expected to fully saturate the capacity of the Publisher server, ClearPass Insight should not be enabled on the Publisher server. If the Publisher server has spare capacity, it can be used to support the Policy Manager Insight database. However, take care to monitor the Publisher server's capacity and performance.

Subscriber Design

Network devices should use the nearest Subscriber to redirect Guest and Onboard clients. From the client's point of view, the internal API call to the Publisher is handled transparently. The best response times for static resources are obtained if the server is nearby.

Subscriber should be used as workers to process the following:

- Authentication requests (RADIUS, TACACS+, Web-Auth)
- Online Certificate Status Protocol (OCSP) requests
- Static content delivery (images, CSS, JavaScript)

Avoid sending *worker traffic* to the Publisher, since the Publisher services API requests from Subscribers, handles the resulting database changes, and sends replication changes back to the Subscribers.

Verify that Online Certificate Status Protocol (OCSP) checks are enabled for EAP-TLS, if Onboard is configured. When using Onboard, ensure that the EAP-TLS authentication method in Policy Manager is configured to perform *localhost* OCSP checks.

Bandwidth and Latency Requirements

In a large-scale deployment, bandwidth congestion and high latency (greater than 200 ms) between network devices and a Subscriber may result in a low-quality user experience for users of that Subscriber.

For reliable operation of each Subscriber, ensure that there is sufficient bandwidth available for communications with the Publisher.

For basic authentication operations, there is no specific requirement for high bandwidth. However, the number of round-trips to complete an EAP authentication could cause delay for the end user.

It is important consider the delay between a Policy Manager server and a NAD/NAS (a controller or switch) when building geographically distributed clusters. In a large, geographically dispersed cluster, estimate the worst case round-trip time (RTT) between a NAS/NAD and all potential servers in the cluster that might handle authentication.

- Aruba recommends that the round-trip time between a NAD/NAS and a Policy Manager server should not exceed 600 ms.
- The acceptable delay between cluster servers is less than 100 ms. RTT should be less than 200 ms.
- The link bandwidth should be greater than 10 Mbps.
- Configure each NAD/NAS to reference multiple RADIUS servers that adhere to RTT guidance for load balancing and failover purposes.

Authentication Methods and Sources

Define the authentication methods used to allow or deny clients onto the network. The list of methods available includes, but is not limited to, PEAP, EAP-TLS, EAP-TTLS, and MAC-auth.

Identify all authentication sources needed to support the authentication methods defined in the previous step. Sources such as Active Directory, MDM solutions, and internal user or guest device repositories also can be included.

Consider which users and devices are onboarded to the network, and design an authentication flow to support it. Common methods include:

- 802.1x with EAP-TLS or PEAP for corporate-owned devices and users
- 802.1x with EAP-TLS for contractors, relying on OnBoard to provision the certificate
- MPSK + Device profiling for devices without a supplicant, such as IoT devices and printers
- Lobby registration or Enhanced Open with an acceptable use policy for guest users.

Enforcement Considerations

The following common enforcement methods are considered in depth in the Policy Enforcement design guide:

- Assign an Aruba Role, which is used by infrastructure to enforce policy
  - Centralized role enforcement
  - Distributed role enforcement
- Assign dynamic VLAN for segmentation
- Assign dynamic ACL for segmentation

Infrastructure Considerations

Use a standardized naming convention for VLANs across the campus so they can be referenced easily by ClearPass. For example, if the enterprise user VLAN ID and name vary by IDF, building, or floor, a complex Enforcement Policy is required to identify the appropriate VLAN ID to return based on the IDF name, subnet, etc. Service configuration is simplified by standardizing VLAN names, even if the IDs are different. Using this method, ClearPass needs to send only one standard response.

Enforcement Models

Policy enforcement involves allowing or denying traffic for a connected user or device using a set of rules based on role assignment, additional user or device attributes, and traffic type.

While ClearPass or Central Global Policy Manager define policy and perform authentication services, policy enforcement occurs on network devices such as switches, gateways, and APs (Bridge Mode or Microbranch).

NetConductor Enforcement Models

This section discusses the two primary NetConductor enforcement models within a campus, and how policy is propagated and enforced across a WAN network.

Centralized Enforcement

When building networks using a centralized policy architecture, APs and switches form GRE tunnels to a gateway cluster to which all user traffic is tunneled. Centralized design is effective and efficient for client-initiated, north-south-bound traffic such as that destined for a data center or the Internet. All policy enforcement is performed on the gateways incorporating role and VLAN assignments.

An authentication server in an 802.1X authentication exchange responds with an assigned role and RADIUS attributes, and gateways apply the policy associated with the role for all sessions initiated by the client.

Centralized fabrics are commonly deployed in branch or campus environments. Find more information in the campus design guide.

Wireless

Aruba gateway clusters provide a high-performance, scalable solution for centralized policy enforcement using Aruba's high-throughput Policy Enforcement Firewall and Deep Packet Inspection features.

The illustration below demonstrates a high-level example of centralized wireless policy enforcement performed by an AOS 10 Gateway cluster.

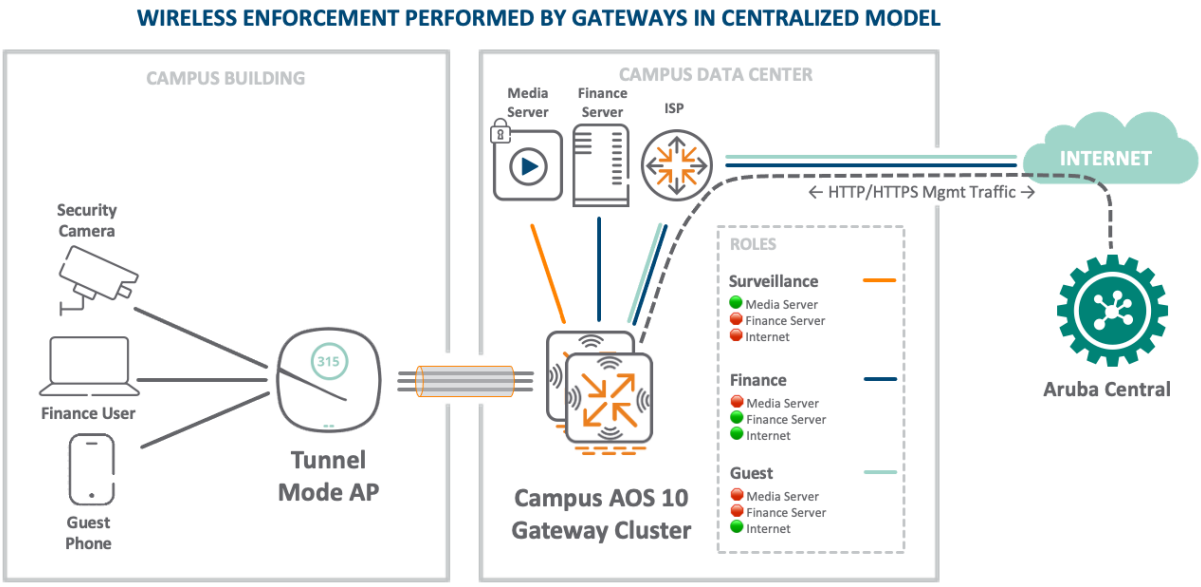

Figure 15: Centralized Wireless Enforcement

Wi-Fi clients associate to a tunnel mode AP that forwards traffic to the Gateway cluster via a GRE tunnel. The Gateways decapsulate and analyze the traffic, enforce user role policy, then forward the traffic to its destination:

- Security cameras are assigned the Surveillance role that allows communication only with the media server.
- The laptop associated with a login belonging to a user in the finance department is assigned the Finance role that allows communication with the finance server and the Internet.
- The Guest role is assigned to the guest phone traffic and is sent to the Internet only.

All the roles are assigned dynamically at the Gateways by Aruba ClearPass or Cloud Auth.

Wired

Much like the centralized wireless enforcement diagram, the diagram below demonstrates a high-level example of centralized wired policy enforcement performed by an AOS 10 Gateway cluster.

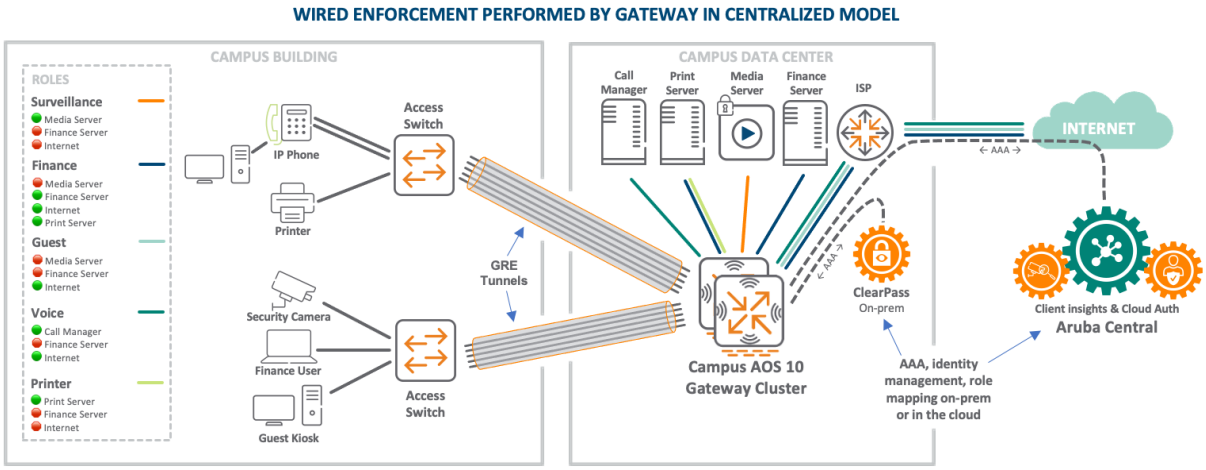

Figure 16: Centralized Wired Enforcement

With centralized wired enforcement, user-based tunneling (UBT) provides a tunnel between Aruba switches and an AOS 10 Gateway cluster. A granular, role-based policy is applied to prioritize application traffic and dictate the network resources that can be accessed as part of Aruba's Dynamic Segmentation. The roles can be assigned by ClearPass or Cloud Auth.

Distributed Enforcement

In a distributed policy architecture, Aruba CX switches form an EVPN-VXLAN overlay fabric. Data traffic is encapsulated in a VXLAN packet that includes a group policy ID (GPID) in the header. This enables policy enforcement on any VXLAN-GBP-aware device configured with a corresponding role and policy.

Distributed policy enforcement implemented in Aruba Central NetConductor provides consistent and efficient policy enforcement in all directions of traffic flow.

The policy enforced on a switch is configured within Aruba Central and downloaded to the switch when it is added to the overlay fabric. The same is done for gateways connected into a NetConductor fabric.

Distributed fabrics are commonly deployed in branch or campus environments as well as data centers. In data centers, EVPN-VXLAN fabrics are deployed using Aruba Fabric Composer (AFC), and Aruba roles are not currently used for policy enforcement. More information on distributed fabric designs can be found in the campus design guide and datacenter design guide.

Wired

The Aruba CX switch operating system provides a sophisticated suite of Layer 3 capabilities necessary for building highly resilient overlay networks based on EVPN-VXLAN, using the Group Based Policy field of the VXLAN header to carry a Group Policy ID. Each user or device session carried through the fabric is assigned a role ID enabling each switch in the network to enforce role-based policy.

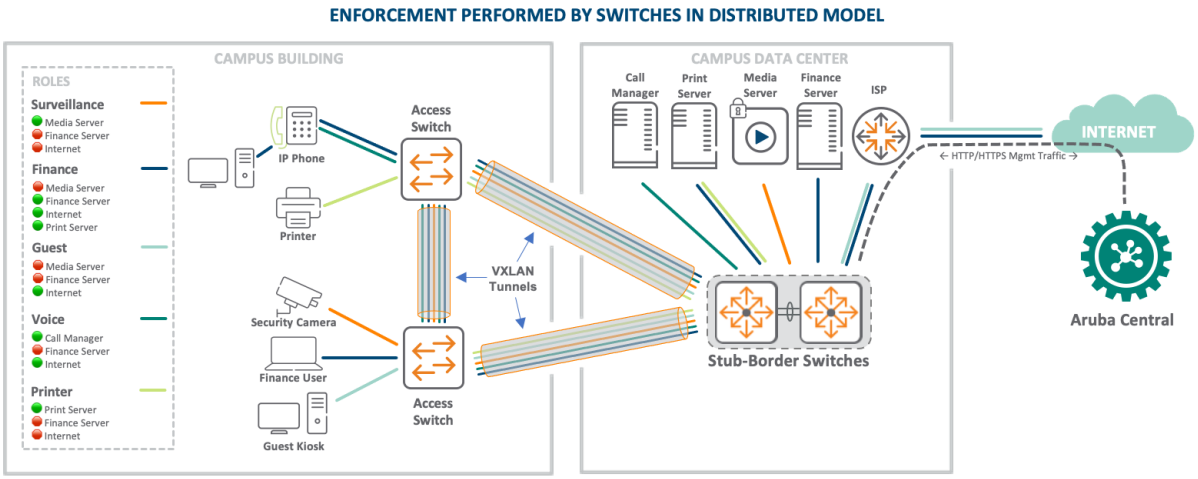

Figure 17: Distributed Enforcement

In the example above, traffic is inspected and policy is enforced locally at each switch or switch stack, for a more efficient data path between source and destination.

- User roles are applied to each session, permitting traffic for each device as defined by the organization's IT security policy.
- Surveillance traffic is permitted only between cameras and media servers.
- Finance users are permitted to communicate with their Finance servers, print servers, and the Internet.
- Guests are restricted to only Internet access.

The model is configured and supported from Aruba Central's comprehensive interface.

Wireless

For the wireless LAN, Gateways and the overlay fabric are connected through a static VXLAN tunnel configured between a Gateway cluster and the aggregation switch to which they are connected. This static tunnel ensures that the role ID is communicated between the WLAN and the EVPN fabric by preserving the VXLAN header.

Based on the role ID, gateways enforce policy on traffic using the integrated policy enforcement firewall (PEF).

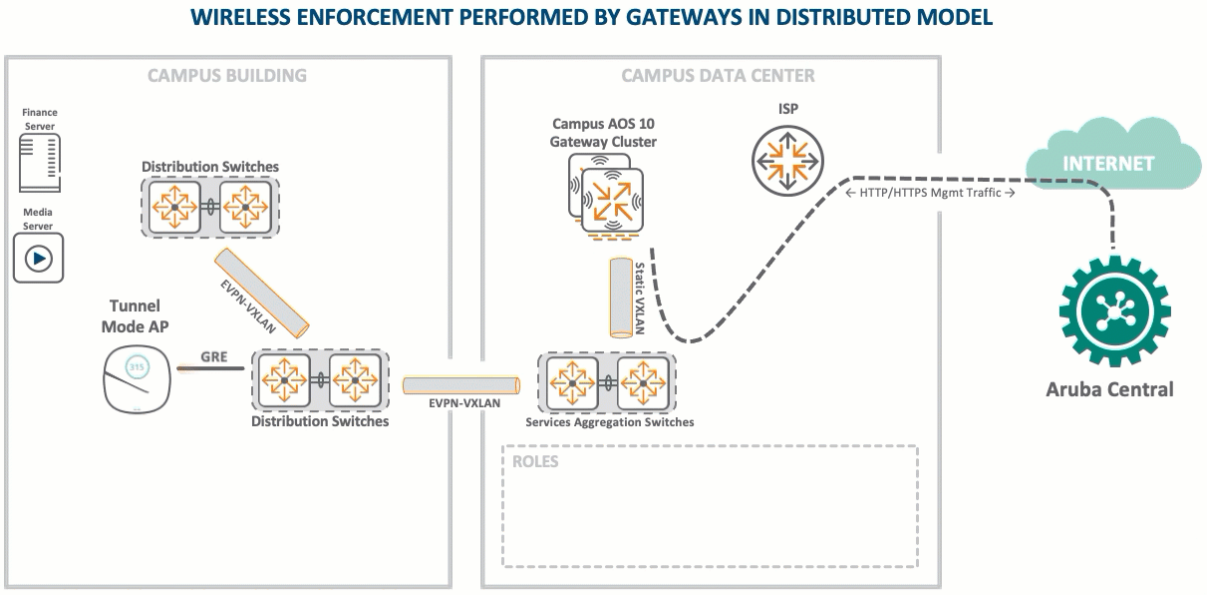

Figure 18: WLAN in Distributed Enforcement

The animated diagram above demonstrates how client traffic is handled in a distributed enforcement deployment. First, note that EVPN-VXLAN tunnels are set up between switch stacks, and static VXLAN tunnels are set up between the Gateways and switches in the overlay fabric. GRE tunnels are formed between the AP and Gateways. Client traffic is GRE-encapsulated at the AP and forwarded through the underlay to the Gateway cluster, not the overlay fabric.

When the surveillance camera associates to the AP, its traffic is sent to the Gateway via the GRE tunnel, where it is decapsulated and inspected. It is then VXLAN-encapsulated and assigned the GPID associated with the Surveillance role. The Gateway then forwards the traffic to the local LAN using the static VXLAN tunnel, after which it is forwarded to the Media Server.

The Finance user is processed in the same manner, but traffic is forwarded based on the security policy assigned to the Finance role, which permits three possible destinations.

The guest phone is handled similarly, but only permitted to access the Internet based on the Guest role policy.

Currently, only Tunnel Mode is supported in a distributed model.

WAN Enforcement: EdgeConnect SD-Branch

In the Centralized Multi-site Fabric with Aruba SD-Branch deployment, the ArubaOS 10 Aruba Gateways act as WLAN and user-based tunnel gateways, and enable connectivity and role propagation over the SD-Branch WAN network. The following example explains the Centralized Multi-Site Fabric deployment using ArubaOS 10 Aruba Gateways.

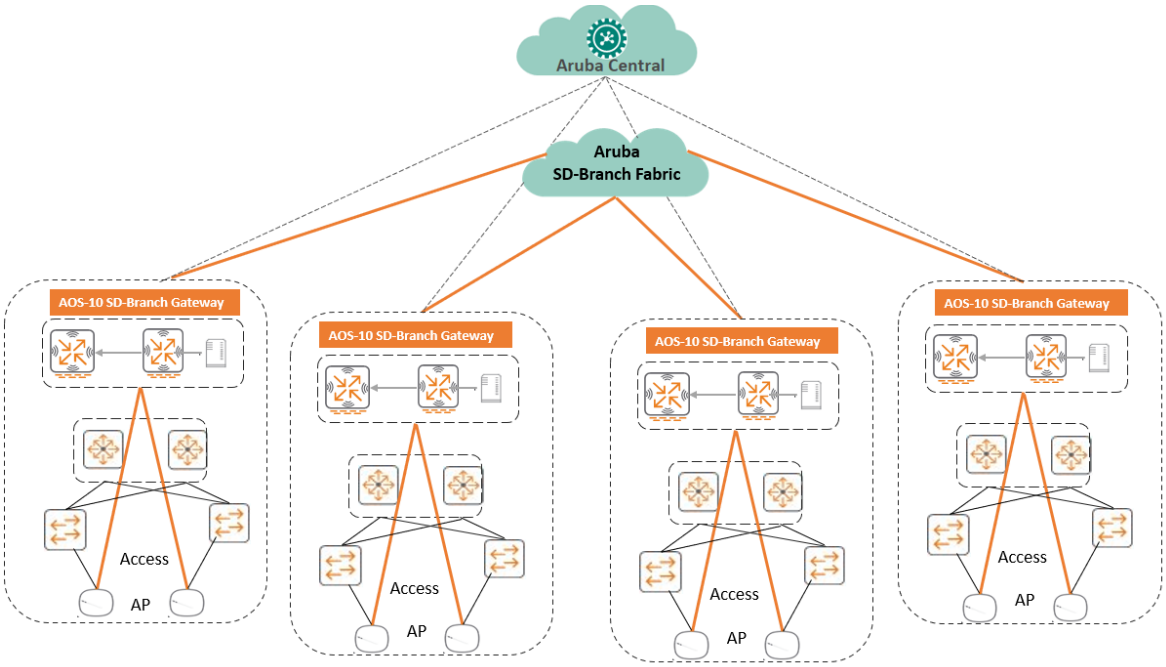

Figure 19: SD-Branch WAN Policy

In the Centralized Multi-Site Fabric deployment, customers can propagate role information and enforce role-based policies for client traffic across multiple sites connected by an Aruba SD-Branch fabric. The ArubaOS 10 Gateways act as the WLAN and user-based tunnel Gateways for wired and wireless clients within each site, and act as the policy enforcement point for the clients within the site. To enforce role-based policies destined to clients across the fabric, the ArubaOS 10 Gateways encapsulate the client traffic using both VXLAN and IPsec, which contain role information in the GPID field in the VXLAN header. The ArubaOS 10 Gateway in the destination site then enforces the role-based policies for client traffic. Role propagation also can be selectively enabled on a per-group basis for SD-Branch deployments.

More information on SD-Branch WAN policy enforcement is found in the branch design guide.

CX 10000 and Pensando Policy Services Manager

Implementation of the Aruba ESP data center policy layer is dependent on the chosen network architecture. An EVPN-VXLAN design offers a rich combination of overlay technologies and traffic filtering mechanisms to isolate user and application traffic, configured primarily on leaf switches. A Two-Tier design offers many of the same filtering options, requiring configuration at both the core and access layers.

The Aruba CX 10000 Distributed Services Switch (DSS) enforces east-west traffic policy using an inline stateful firewall in hardware within the switch. A DSS optimizes performance and traffic flow characteristics over a centralized firewall strategy and can replace hypervisor-based firewalls, increasing hypervisor CPU and memory resources for hosted workloads. The CX 10000 can be placed in both EVPN and Two-Tier architectures, but with greater policy flexibility in an EVPN design.

Aruba Fabric Composer (AFC) integration with both vCenter and AMD Pensando Policy Services Manager (PSM) provides a powerful combination for managing east-west data center policy using CX 10000 switches and VM guest policy assignment. Network and security administrators can manage all policy elements centrally, while empowering VM administrators to assign VM guests to a policy block in their own independent workflow through the assignment of VM tags. AFC also supports centralized configuration of access control lists (ACLs).

More detailed information on policy enforcement in the data center is found in the Datacenter Design Guide.

www.arubanetworks.com

3333 Scott Blvd. Santa Clara, CA 95054
1.844.472.2782 | T: 1.408.227.4500 | FAX: 1.408.227.4550