TECHNICAL PAPER

aruba
a Hewlett Packard Enterprise company

Automate and Accelerate Networking and Policy Orchestration from the Cloud with Aruba Central NetConductor

STREAMLINE OPERATIONS AND ENHANCE PROTECTION AT GLOBAL NETWORK SCALE WITH SIMPLIFIED NETWORK CONFIGURATION AND SECURITY SERVICES

TABLE OF CONTENTS

INTRODUCTION

Every decade or so, we see a major development in technology that changes the demands of the modern enterprise network. Today we are amid the next big shift: the era of data—not data that is generated in the cloud or the data center, but rather data that is generated where the action takes place—the edge—where users, devices, and applications all come together. The network at the edge becomes even more mission-critical and thus its requirements go far beyond standard connectivity and access technologies of the past.

At the cusp of this shift, many IT organizations are feeling pressure from the initial waves. These waves are coming in the form of an onslaught of IoT (or unintelligent) devices and an increasing number of connected personal devices. Increased clients on the network brings a larger cyber security attack surface to manage. While network engineers have had the tools to protect the assets on the network through segmentation for a very long time, traditional approaches are running out of steam both functionally and operationally. Modern network protocols and designs like overlays can overcome these limitations but can lead to configuration management complexity and overhead. Network teams are not only stretched in the areas of knowledge they need to understand, but also in the cycles they have to get things done. Finally, digital acceleration and globalization have forced organizations to bring consistency to their operating model, which is hindered by tools built without cloud scale in mind. This leaves IT organizations asking:

- How do we continue to allow the business partners that rely on the stability of the network to do their jobs while also increasing the pace at which new use cases can be implemented?
- How do we remove my talented IT staff from the daily grind of network provisioning tasks so that they can focus on higher order functions?
- How do we make a transformational design shift in my network with the need to maintain uptime and not impact existing use cases?

ARUBA CENTRAL NETCONDUCTOR—A NETWORKING AND SECURITY SERVICES FOR THE EDGE-TO-CLOUD NETWORK

Aruba Central NetConductor is a collection of edge-to-cloud networking and security services designed to tackle these problems for the modern enterprise network. Central NetConductor delivers an innovative approach to tackle the connectivity and security challenges of network modernization by providing cloud-native services that automate and accelerate the deployment, operations, and security of the network. It ties directly to the Aruba Edge Services Platform (ESP) vision of an edge-to-cloud network. The main components of Central NetConductor help address issues faced by the modern network:

- **Cloud-Native Single Pane of Glass** for intent-driven network and policy orchestration and AI/ML-based assurance across the wired, wireless, and wide area network
- **Global Role-Based Policy Orchestration** for automated policy management, including IoT clients based on AI/ML-driven client profiling
- **Choice of Intelligent Overlays** for dynamic, flexible, and scalable networks with standards-based technology stacks for multi-vendor interoperability and phased migration strategies

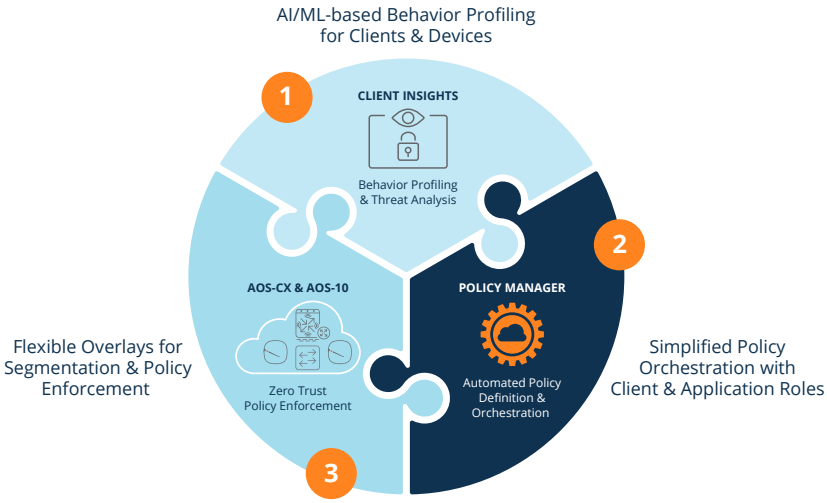

Figure 1. Components of Aruba Central NetConductor

SIMPLE AND SECURE NETWORKS WITH GLOBAL ROLE-BASED POLICIES

With new business models such as hybrid work driving the need for efficiency and increased vulnerability due to the explosion of IoT (or unintelligent) devices in the enterprise network, Aruba role-based policies simplify policy definition across both wired and wireless networks irrespective of geographic location and point of connectivity to the network. A role is a logical grouping of clients with common permissions that include application access rights and inter-user or device communication. It is built on the Zero Trust Enforcement Model, where users and devices are denied access to other devices and applications by default unless explicitly given permissions. It enables businesses to translate security intent to network designs, abstracting the underlying complexities of the network.

Role-Based Policy Simplifies Network Design and Operations

Traditionally, location-/network-specific constructs such as IP addresses or subnets were used to define security policies, leading to complexity and inflexibility in the network due to the lack of client mobility brought about by these segmentation requirements. IT teams also lose the opportunity for automation as they have to pre-provision the network based on these VLANs and subnet constructs. Role-based policies allow policy to be abstracted from the underlying network by assigning identity-based Roles to endpoints and users. These identities are derived either by authentication via Identity stores such as Active Directory, or by profiling how these endpoints behave with Client Insights. This naturally leads to the simplified design, deployment, and operations of these less complex networks, as the network no longer needs to be segmented using traditional network constructs such as VLANs and the administrator no longer needs to pre-provision the network to accommodate user onboarding.

Central NetConductor Enables Global Role-Based Policy Orchestration

Central NetConductor allows the network administrator, working in conjunction with the security team, to implement role-based security policies across the global network using intent-based workflows. The Central NetConductor policy manager simplifies the task of administrators when defining policy for clients using Aruba User Roles, which allows clients to be grouped based on their identity. This condenses what typically would be thousands of complex IP or VLAN-based security rules in a firewall, to a few dozen role-based security rules. This enables administrators to focus on defining policies based on their desired business intent and eliminates constant updating of policies because of client and application VLAN/IP changes.

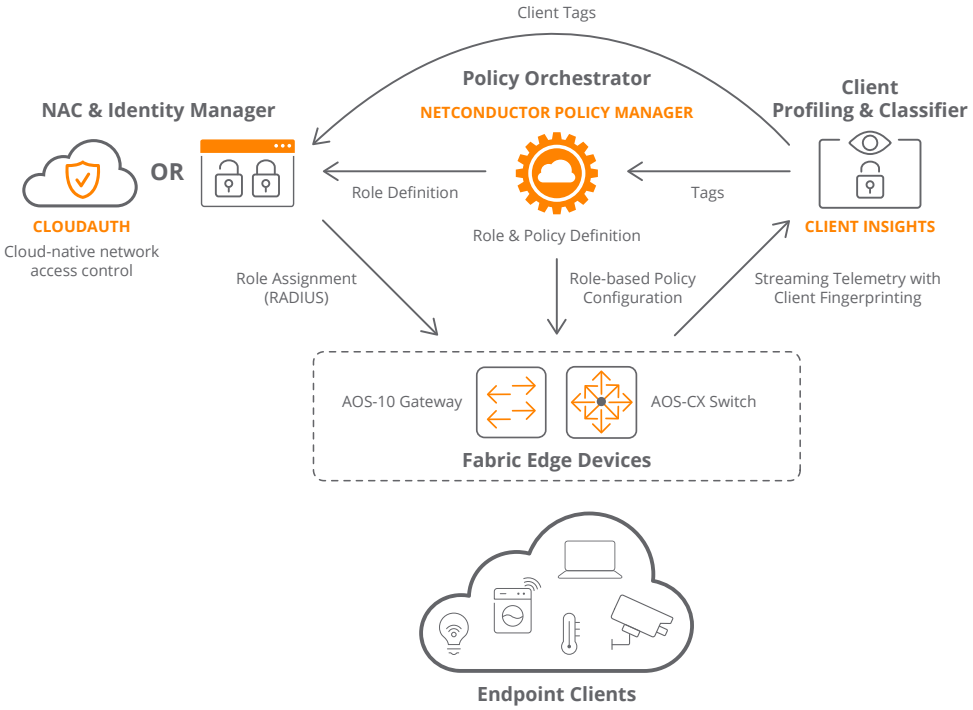

Figure 2. Global Role-Based Policy Orchestration from Aruba Central NetConductor

Central NetConductor orchestrates policies with these easy steps:

1. **Global Policy Orchestration** — The Central NetConductor policy manager is a new service that acts as the single interface for management of network and security policies in the network. Network administrators can define roles in Central and assign role-based permissions for these roles in a common policy language. For example, an organization that wants to implement a business-driven policy can do so from Aruba Central in a few simple clicks:

   "Allow all the video cameras in the network to access DVR recorders, but not the printers. Oh, and by the way, make sure that interns and contractors cannot access these cameras."

2. **NAC (Network Access Control) and Identity Management** — Central NetConductor provides customers the flexibility to pick their NAC solution of choice, whether that is ClearPass, our market-leading on-premises Network Access Control (NAC) solution, or Cloud Auth, the first integrated and cloud-native NAC and identity management solution, which builds on ClearPass NAC market leadership and streamlines the protection of distributed enterprise networks by working seamlessly across wired, wireless, and WAN connections. The roles defined in Central are automatically synchronized to either Cloud Auth or ClearPass, where customers can then map their users and devices to these roles. Aruba also supports third-party NAC solutions using standards-based mechanisms (VSAs) to assign roles to clients, giving customers the flexibility of choice and the opportunity to migrate in a phased manner.

3. **Policy Enforcement on Network Edge Devices** — Central NetConductor enables Aruba's AOS-10 gateways and AOS-CX switches to enforce role-based policies in line. Role-based policies defined in Central are pushed to the edge infrastructure devices. As clients and devices authenticate onto the network, these clients are assigned a role based on authentication from the NAC. The infrastructure edge devices enforce role-based policies either in a distributed manner at the edge via AOS-CX switches or at the centralized AOS-10 gateway, depending on the organization's choice of overlays. This enhances security from internal threats within the network that would have otherwise gone undetected by traditional perimeter firewalls.

4. **Client Profiler and Threat Analysis** — Client Insights is a service that discovers, profiles, and continuously monitors devices. It provides AI-powered user and device discovery to ensure all users and devices on the network—even rogue IoT devices—are seen and controlled. In the era of IoT and BYOD devices, the need to eliminate blind spots related to these devices on the network has become very relevant. Central NetConductor provides the ability to automate and simplify policy definition for IoT devices with behavior-based profiling using AI- or ML-based classification. This simplifies policy definition and ensures consistent policy enforcement across the entire network.

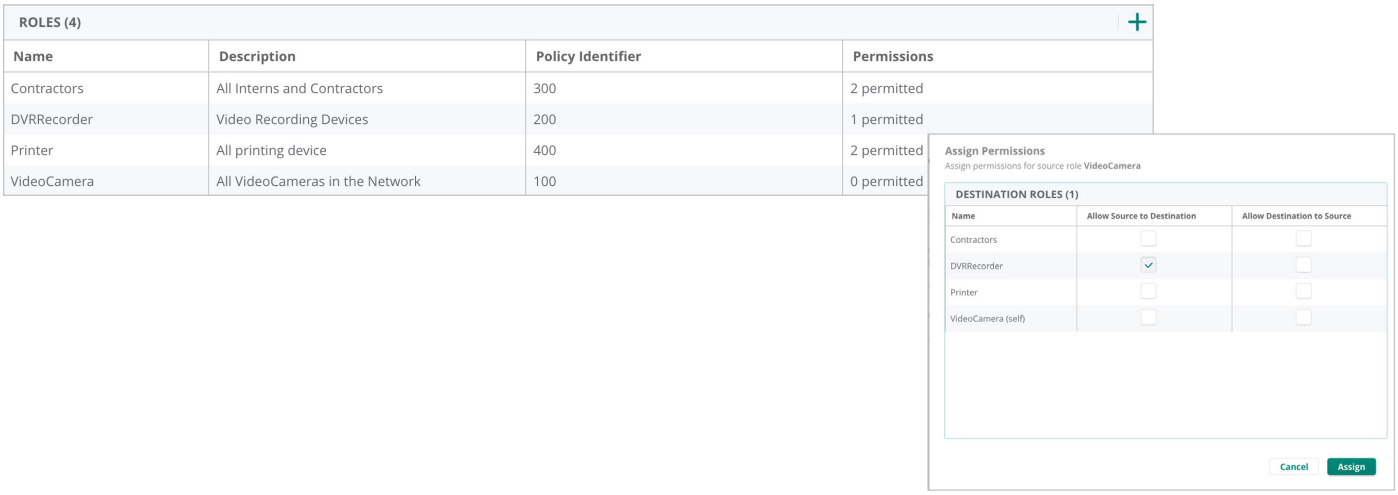

Figure 3. Role-Based Policy Definition in Aruba Central

FLEXIBLE AND SCALABLE NETWORKS WITH INTELLIGENT OVERLAYS

Another key pillar of Central NetConductor is the ability to operate flexible and scalable networks using intelligent overlays. Unlike other competitive architectures, Central NetConductor provides enterprises the choice between two different overlay models, giving organizations flexibility to decide which model to deploy based on their use cases, scale, and multi-vendor interoperability requirements. These overlays are agnostic of the underlying network, giving organizations flexibility of network design (2-tier vs. 3-tier topology, L2 at the access vs. L3 routed access, etc.) and choice of protocols used (OSPF vs. BGP, etc.) Furthermore, these overlays can be adopted and rolled out using phased migration workflows from Aruba Central.

Overlay Networks Allows On-Demand Orchestration of Services

An overlay is a method of defining layers of network abstraction using software to run multiple separate, virtualized networks on the top of a physical layer. Overlay networks provide the ability to deploy flexible services based on ever-changing connectivity and mobility demands of the endpoints and applications. Decoupling the overlay network from the physical topology enables on-demand deployment of layer 2 and layer 3 services irrespective of underlay physical topology. This eliminates the cost of manually modifying the network to cater to the movement of these clients and applications. Overlay networks also enable the ability to carry endpoint or user role information across the network without requiring all devices in the path to understand or manage the roles.

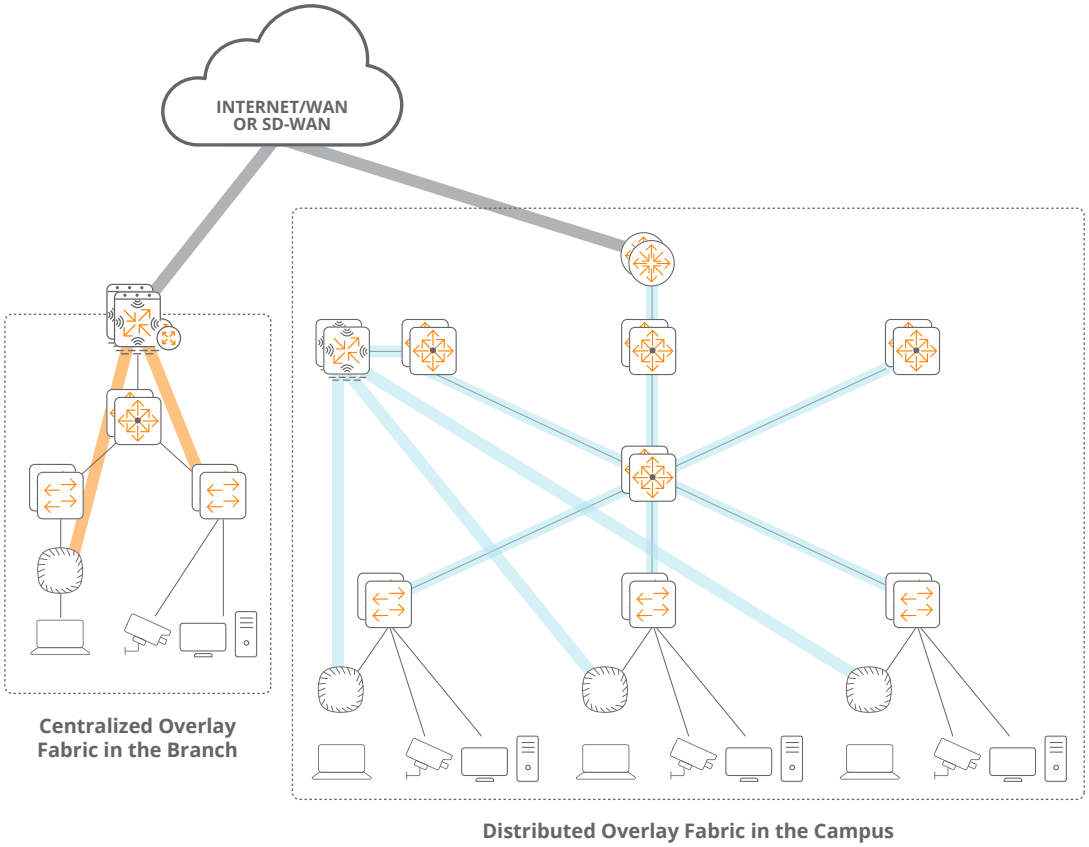

Figure 4. Choice of Overlay Fabrics with Central NetConductor

Centralized Overlay Fabric: Simple, Enhanced Security; Consistent Across Wired & Wireless

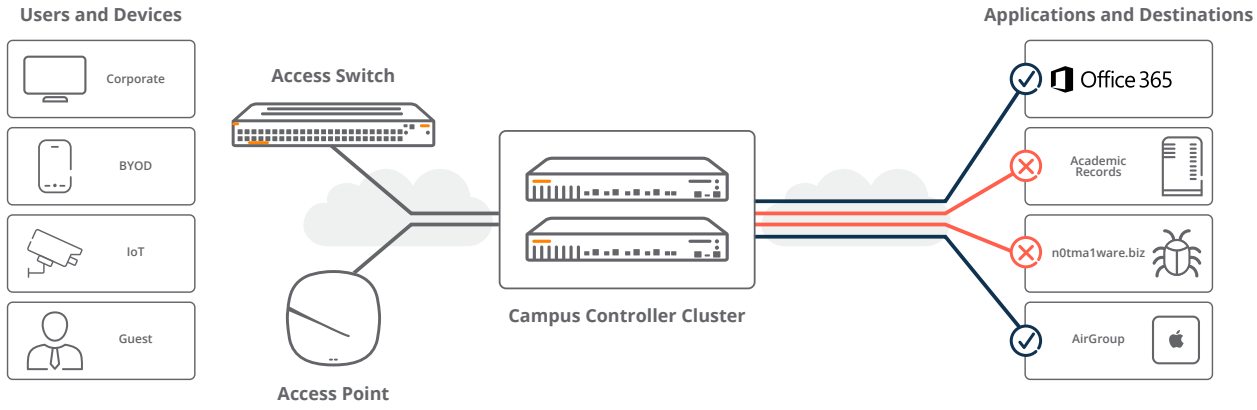

Figure 5. Centralized Overlay Fabric

The centralized overlay fabric enables role-based segmentation (or micro-segmentation) and enhanced security features for all wired and wireless clients in the network by tunneling client traffic from Aruba access points and switches to a centralized Aruba gateway for deep packet inspection and enhanced stateful firewall features such as IDS/IPS, Web Filtering, and role-based session rules. This provides a consistent operator experience across both wired and wireless networks. Centralized overlays work best for smaller campuses and distributed enterprises, providing them a scalable, secure, and high-performance network, while simplifying the deployment and operations of the network.

Distributed Overlay Fabric: Scalable, Multi-Vendor Ready Fabric for the Enterprise Campus

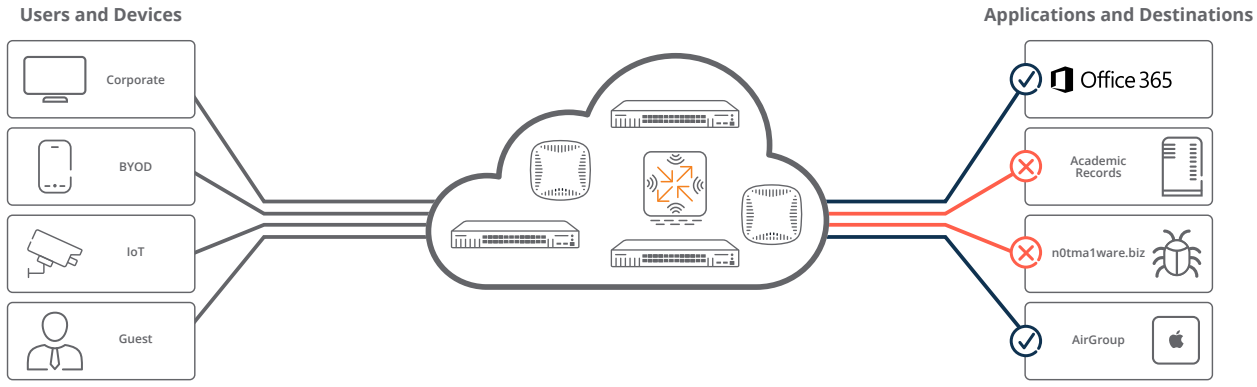

Figure 6. Distributed Overlay Fabric

The distributed overlay fabric enables large enterprises to deploy a multi-vendor and scalable overlay across the wired, wireless, and wide area network and enables role-based policy enforcement at all of the edges of the fabric. It simplifies network operations by leveraging intelligent client-based automation capabilities that stitch up and tear down VXLAN tunnels based on client onboarding. Based on standard protocols such as BGP-EVPN and VXLAN, the distributed overlay fabric provides a consistent architecture across the campus and data center.

Automated Fabric Provisioning on AOS-CX and AOS-10 with Aruba Central

Central NetConductor introduces the ability to deploy a distributed overlay fabric on a campus network with AOS 10 gateways and AOS-CX switches. This capability is a standards-based implementation leveraging EVPN on the control plane and VXLAN-GBP on the data plane, enabling multi-vendor interoperability and phased migration strategies. The CX portfolio is further differentiated by optimized TCAMs for role-based policies, dynamic tunnel creation based on client authentication, and optimized host-route learning mechanisms that provide greater scale and enhanced usability compared to competitive products.

The Central NetConductor fabric wizard simplifies the deployment of a fabric over an existing traditional network. The wizard uses simple workflows to translate customer's business intent into fabric-wide configurations, eliminating the need for users to have detailed knowledge of concepts such as EVPN, VNIs, VTEPs, and VRFs. For example, manually provisioning a BGP-EVPN fabric across 200 switches within a campus—which entails creating switch-specific configurations, provisioning these switches individually, and then checking and validating the configurations—can take a week; the fabric wizard accomplishes provisioning in less than 10 minutes, without introducing human error.

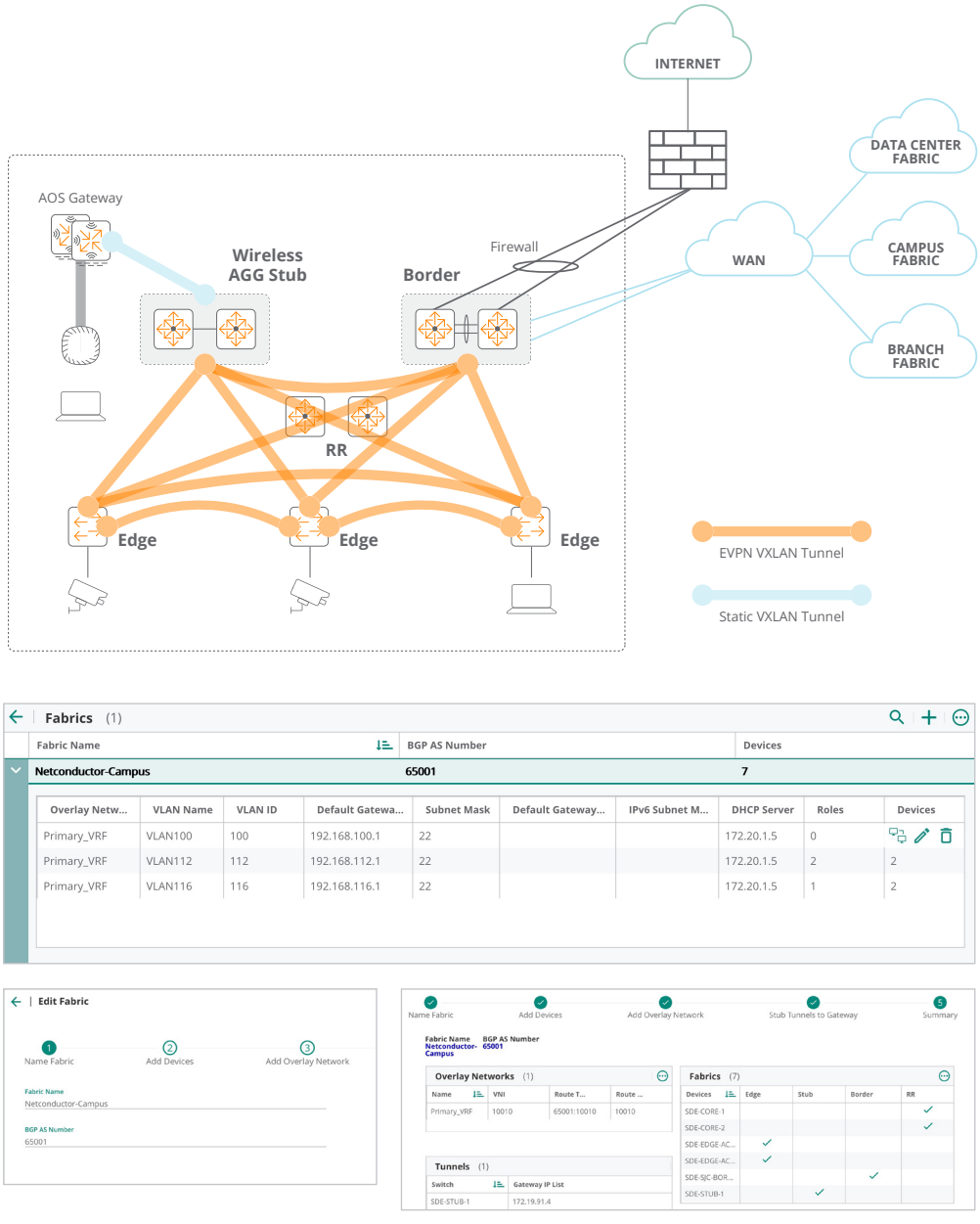

Figure 7. Automated Deployment of Distributed Overlay with Central NetConductor Fabric Wizard

CONCLUSION

Aruba Central NetConductor tackles the problems brought about by digital transformation by unifying workflows with a single pane of glass for network and policy management, simplifying policy and network design and operations with role-based policies, and reducing complexity with intent-driven automated workflows, all without the need to rearchitect or redesign anything in the existing networks. It aims to be the most scalable, secure, and flexible edge-to-cloud security framework on the market.

For more information, visit arubanetworks.com/centralnetconductor.

TP_ArubaCentralNetConductor_030322 a00121122enw

Contact us at www.arubanetworks.com/contact