aruba
a Hewlett Packard Enterprise company

SOLUTION OVERVIEW

ARUBA CENTRAL NETCONDUCTOR

Cloud-native Network and Security Services that Automate Configuration, Policy Definition and Enforcement at Global Scale for the Streamlined Operations and Enhanced Protection Required by Modern Networks.

Digital acceleration driven by hybrid work, new customer and user experiences, and the need for improved IT efficiencies makes it more important than ever for the network to provide the flexibility and security needed to keep up with constantly changing business requirements. Yet advancing critical business initiatives while managing a growing volume of network sites and topologies can quickly become overwhelming.

The antidote to growing network complexity is a network fabric. A fabric is a logical overlay that "stitches" together disparate, dispersed network infrastructure (underlays).

Unlike VLAN-based approaches that rely on extensive manual monitoring and configuration, an overlay provides holistic control of the network, eliminating the need for labor-intensive management of physical and virtual infrastructure, and helping organizations save time and money. Network overlays allow greater scalability than traditional VLAN-based approaches, making them an ideal choice for managing and securing complex, highly-distributed networks.

ARUBA CENTRAL NETCONDUCTOR: OVERLAY-BASED AUTOMATION FOR MODERN NETWORKS

Digital acceleration calls for an automated, agile, always-protected network. That's why Aruba introduced Aruba Central NetConductor: cloud-native network connectivity and security services designed to relieve IT teams from tedious and error-prone manual network operations. Central NetConductor is the next-generation solution for increasingly complex networks, enabling organizations of all types and sizes to automatically configure LAN, WLAN, and WAN infrastructure to deliver optimal network performance while enforcing granular access control security policies that are the foundation of Zero Trust and SASE architectures.

Central NetConductor comprises services delivered by Aruba Central, the platform that is the foundation of the Aruba Edge Services Platform (ESP)—the industry's original AI-powered, cloud-native architecture designed to automate, unify, and protect the edge.

ARUBA CENTRAL NETCONDUCTOR COMPONENTS

- **Policy manager:** Defines user and device groups and creates the associated access enforcement rules for the physical network.
- **Group policy identifier (GPID):** Carries client policy information in traffic for in-line policy enforcement, which reduces configuration and security overhead and increases mobility and scalability.
- **Fabric wizard:** Simplifies the creation of overlays using an intuitive, graphical user interface, greatly easing how virtual components are defined and configuration instructions are generated and pushed to switches and gateways.
- **Network Insights:** Brings together network expertise, artificial intelligence, and machine learning to detect, triage, root cause, and resolve Wi-Fi, wired and WAN issues. Employs class-based site comparisons and best practices to identify user experience optimization opportunities.
- **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. Also monitors the behavior of traffic flows for added security.
- **Flexible Network Access Control:** Ensure entities are properly 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:** Supports configuration and enforcement based on the routing instructions and access privileges defined in the GPID.

KEY BENEFITS

- Automates and accelerates the deployment, management, and protection of distributed enterprise networks, from edge to cloud
- Enhances security by extending Aruba's market-leading Dynamic Segmentation with role-based segmentation and continuous in-line monitoring of client behavior using AI/ML techniques
- Reduces IT burden by automating ongoing network configuration and management based on business intent workflows
- Allows ongoing network modernization by supporting heterogeneous networking environments with widely adopted protocols like EVPN/VXLAN—no need for rip-and-replace
- Accelerates digital transformation through Aruba ESP, the industry's original AI-powered, cloud-native architecture designed to automate, unify, and protect the edge

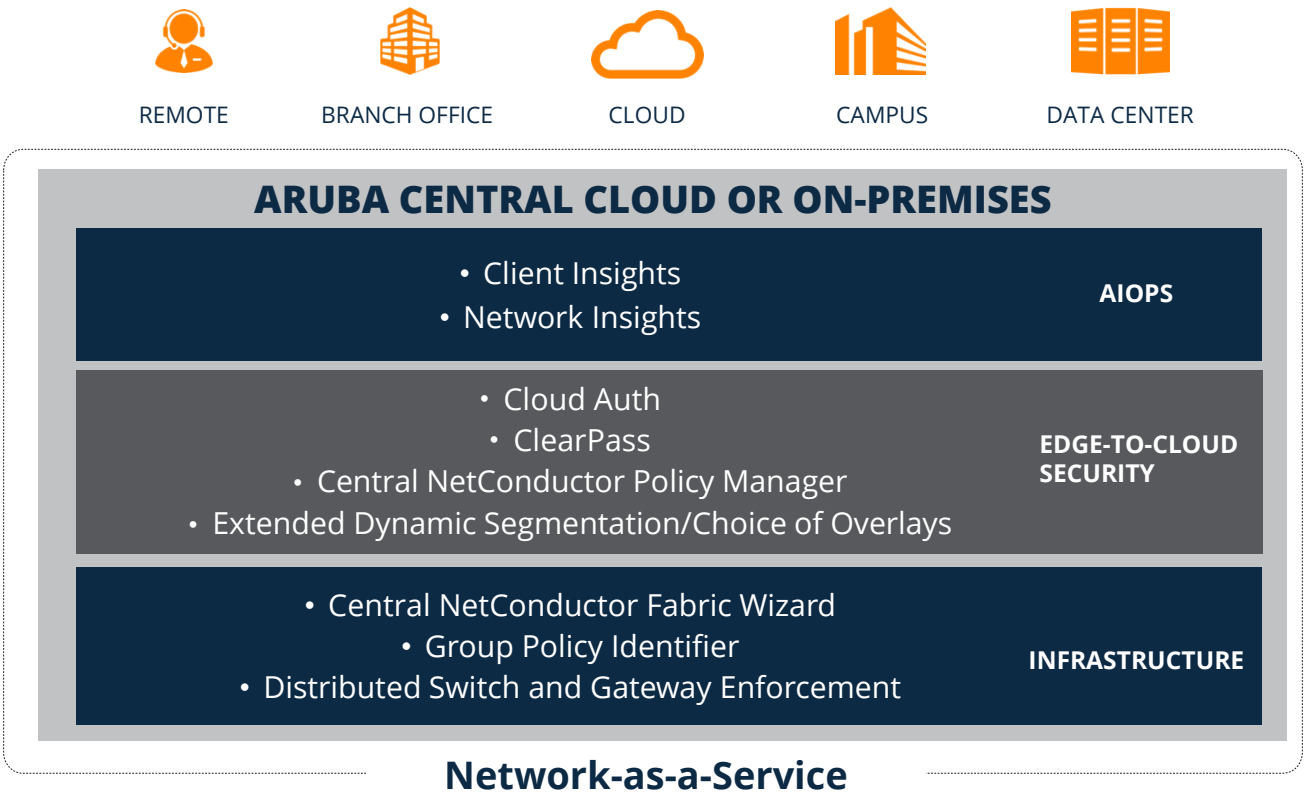

Figure 1: Aruba Central NetConductor services provide the benefits of Aruba ESP throughout the enterprise network.

COMPREHENSIVE NETWORK AUTOMATION

With Central NetConductor, client traffic and security policies are decoupled from the underlying network construction—no more VLAN and routing table spreadsheets, or manual configuration of ACLs.

At deployment, the Central NetConductor fabric wizard automates the creation of the logical overlay with UI-driven workflows that use connection topology to define VXLAN components. The resultant CLI configuration instructions are automatically pushed to Central NetConductor-capable switches and gateways.

Post-deployment, Central NetConductor relies on client policy to control access for users and devices. Once a policy is defined, it is automatically propagated throughout the network within minutes, so the network continually reflects the intended business workflows and associated role-based access without any manual intervention or updating.

Central NetConductor leverages Network Insights, automated troubleshooting, and proactive recommendations for improved network performance and IT efficiency. For example, overlay health is constantly monitored, giving IT teams insights into service level at a glance. Health scores can help IT teams monitor overlays, sites, and devices and troubleshoot network issues that may otherwise be difficult to pinpoint, such as route, tunnel, and segment status.

This high degree of automation and optimization means less IT resources are required to configure, maintain, and support the network. In addition, continuous monitoring of operational baselines ensures optimal performance.

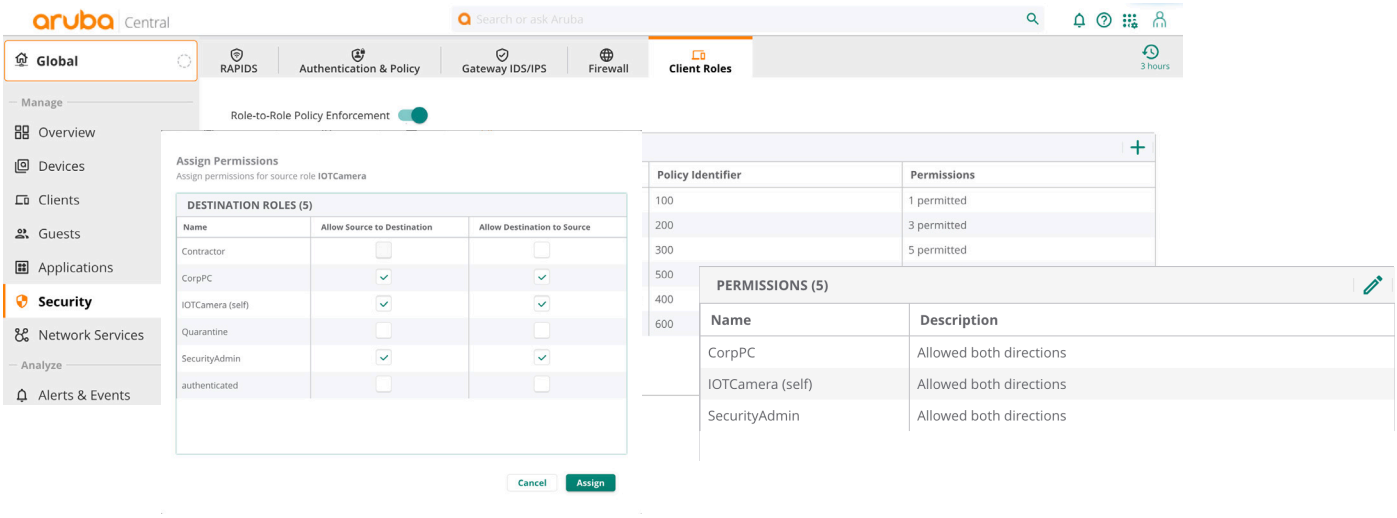

Figure 2: Simple, intuitive user interfaces enable IT teams to quickly easily translate business intent to network configuration.

EXTENDED DYNAMIC SEGMENTATION FOR ZERO TRUST AND SASE

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

Discovery and Profiling

Central NetConductor utilizes Aruba Central Client Insights to discover, profile, and continuously monitor devices. Client Insights provides AI-powered user and device discovery to ensure all users and devices on the network—even rogue IoT devices—are seen and controlled.

ARUBA CENTRAL CLIENT INSIGHTS: AI-POWERED USER AND DEVICE DISCOVERY AND AUTHENTICATION

Aruba is the first to ingest device fingerprinting, network flow data, and system logs via a cloud-native platform to profile, classify and tag clients based on their behavior in the network. This AI-powered approach provides an agentless solution that uses native infrastructure telemetry to develop ML-based classifications, which go beyond basic profiling to support always-on monitoring and granular policy enforcement.

Authentication

Through the Central Cloud Auth service (or an on-premises solution such as ClearPass or compatible third-party solution), identified users and devices are assigned a role that contains both connectivity requirements and access policies associated with that entity. Roles can be matched to an inventory of business outcomes, supporting least-privilege access control.

Authorization

The Central NetConductor policy manager translates assigned roles into the appropriate network routing and associated access policies. This is accomplished without requiring knowledge of the underlying physical infrastructure via GPID.

Enforcement

GPIDs enable a distributed policy enforcement model that provides Zero Trust security without compromising performance. GPIDs encode client role information in the packet header, eliminating the need to send traffic outside its optimal path for security inspection. GPIDs are interpreted in-line by Aruba CX switches and gateways, with traffic segmentation enforced based on the assigned role and its real-time destination and access privileges.

Central NetConductor provides flexibility in enforcement model. Organizations currently using centralized policy enforcement approaches, such as Policy Enforcement Firewalls in Aruba gateways, can continue with that approach and adopt over time a distributed approach in which enforcement is done by access devices.

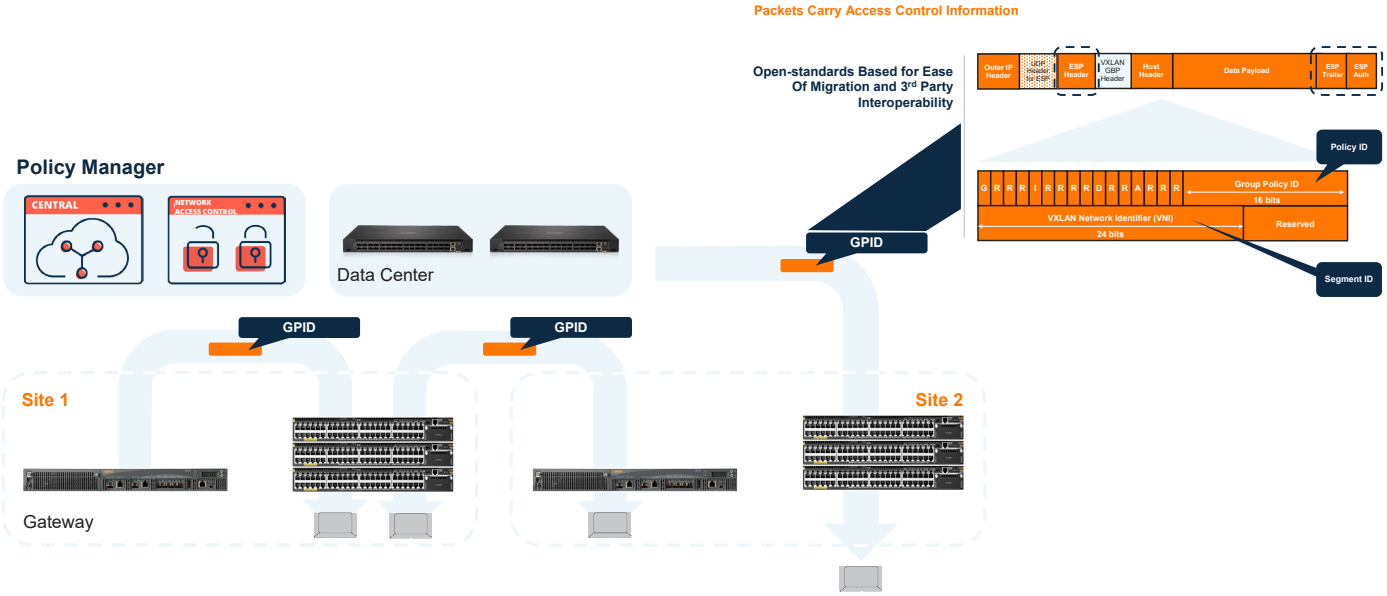

Figure 3: Group policy identifiers (GPIDs) enrich traffic with access control information. Identifiers are centrally defined within and applied from the policy manager and enforced across network locations via gateways and switches.

OPEN STANDARDS-BASED INTEROPERABILITY

Network modernization is a journey, not a destination. With Central NetConductor, organizations can benefit from the visibility, authentication, and security services delivered by Aruba Central without a rip-and-replace of their current network infrastructure. Central NetConductor uses widely adopted protocols such as EVPN/VXLAN to produce the intelligent network overlays. As a result, these intelligent overlays can be quickly deployed, at massive scale, across heterogeneous networks across all domains, from remote and branch locations to campuses and global enterprises.

Although Central NetConductor is optimized for Aruba networks, it is specifically designed for interoperability. Central NetConductor-capable infrastructure can coexist alongside current network management and security services, protecting investments and enabling organizations to modernize networks at their own pace.

EVPN/VXLAN AND GROUP POLICY IDENTIFIERS: CONSISTENT ENFORCEMENT, REDUCED OVERHEAD

EVPN/VXLAN is an overlay network framework used to manage disparate, globally dispersed networks and address the limitations of traditional VLANs. EVPN/VXLAN enables fine-grained segmentation so organizations can separate traffic on a global basis based on user, device, and type—an increasingly important capability due to the proliferation of IoT and BYOD endpoints. Using EVPN/VXLAN, organizations can connect geographically dispersed locations using layer 2 virtual bridging, which allows the extension of Dynamic Segmentation across physical locations. This approach not only ensures consistent security throughout the network, it also enhances scalability and significantly reduces network provisioning overhead.

SUMMARY

Aruba Central NetConductor is a cloud-native network orchestration solution designed to help IT teams deal with network complexity and security gaps by automatically configuring the LAN, WLAN, and WAN infrastructure to deliver optimal connectivity that scales across a global network while enforcing granular access control security policies that are the foundation of Zero Trust and SASE architectures. By decoupling business intent from physical network construction, organizations can dramatically reduce the time and resources required to operate the network while significantly increasing network reliability, performance, and security.

For more information, visit www.arubanetworks.com/CentralNetConductor.

SO_ArubaCentralNetconductor_SK_090522 a00121121enw