aruba
a Hewlett Packard Enterprise company

SOLUTION OVERVIEW

Centrally orchestrated end-to-end segmentation

The Aruba EdgeConnect SD-WAN edge platform enforces consistent and granular end-to-end security policies across the LAN, WAN, Data Center, and the Cloud.

A NEW WAN AND SECURITY EDGE

Today's enterprise networks fall short of delivering the agility and security required to address the needs of the cloud-first world. Backhauling application traffic to the centralized data center or a headquarters worked well when all the enterprise applications lived there. With increasing traffic from users in branch offices and applications moving to the cloud, backhauling traffic across a hub-and-spoke legacy network provides a poor user experience, increases security risk, and is expensive.

Enterprises must secure applications in the cloud and protect users connecting to these applications across the wide-area network (WAN). To realize the full promise of the cloud, enterprises will need to transform both their WAN and security architectures — not just one or the other. With transformed network and security architectures, enterprises can embrace timely innovations to accelerate productivity, revenue growth, and profitability while containing costs. Realistically speaking, this is a journey for most customers and starts by understanding where they are today and the necessary steps they must take to accelerate their digital transformation initiatives.

Security transformation is a multi-layered approach. It starts with securing users, devices, and applications. Many legacy networks do not fully embrace the Zero Trust model, a framework that works under the assumption that no user or application is trusted until authenticated. Zero trust demands that all users, devices, and applications prove "who" they are and "what" applications and data they are authorized to access, regardless of whether they are sitting within or outside the network perimeter. Having a Zero Trust model in place ensures that only verified users, devices, and applications access the business resources that are consistent with their roles.

At the next layer, we must think about the different security measures and how they apply to the application traffic moving across the WAN. Over the last few years, there has been increased adoption of cloud-based security services primarily since they don't slow down the network performance as much. The Secure Access Service Edge (SASE), a new term coined by Gartner, defines an architecture that combines advanced WAN edge network functions deployed at branch locations with comprehensive cloud security services, such as secure web gateway (SWG), cloud access security broker (CASB), firewall-as-a-service(FWaaS), ZTNA, and many others. At this stage, customers have an option to deploy a single vendor SASE solution or embrace the freedom and flexibility that comes with a best-of-breed SASE multi-vendor solution.

Finally, customers must look at their existing network security and determine how to roll out changes consistently. Predominantly, network security has been a manual, device-centric approach. Software-defined Wide Area Networks (SD-WAN) have transformed the way users connect to enterprise applications. In contrast to the traditional device-centric approach that uses TCP/IP addresses and access control lists (ACLs), an SD-WAN employs a more intelligent and more automated business-driven model to control how traffic traverses the WAN.

With the Aruba EdgeConnect SD-WAN edge platform, enterprises create multiple application-specific virtual WAN overlays. Each virtual overlay — or business intent overlay — specifies priority and quality of service requirements for application groups based on business requirements or intent. With these definitions in place, Aruba EdgeConnect automates traffic steering on an end-to-end basis across all underlying WAN transport services, including MPLS, broadband, and 4G/5G/LTE, providing the ability to

deliver the highest quality of experience that is better than what can be provided by any of the underlying transport services individually.

However, security policy definition and enforcement across the traditional WAN remains a manual, fragmented, device-centric approach. Multiple disparate policies must be defined for the LAN, WAN, Data Center, and the Cloud. Current zone-based firewalls and other security devices must be individually programmed, device-by-device, and then stitched together with separate policies defined across the WAN. Not only is this time-consuming and expensive, but it also leads to inconsistent security policies that expose the enterprise to unnecessary risks due to inconsistent configurations and errors.

ZERO TRUST: SECURING THE EDGE BY ROLE, CONTEXT, AND APPLICATION

With the increase in the numbers and types of IoT connected devices, mobile devices, remote workers, and adoption of cloud applications, enterprises must align their security policies based on business intent while also striving for consistency. Aruba ClearPass integration with EdgeConnect augments application intelligence with user and device identity and role-based context, enabling fine-grained segmentation. This additional identity-based context enables consistent security policy enforcement network-wide, from the edge to the cloud, while also streamlining troubleshooting and problem resolution.

As a new user or device connects to the network and registers with ClearPass, the Aruba Orchestrator (control plane for Aruba EdgeConnect) connects to the ClearPass API. The Orchestrator propagates security policy information and any updates related to the user, device type, role and security posture to all EdgeConnect appliances in the network.

Because IoT devices are agentless, it is not possible to run a third-party VPN or ZTNA client on them. Thus, a SASE architecture doesn't fully address the security challenges posed by IoT devices that are connected to the enterprise network.

Aruba ClearPass augments SASE with a zero trust security framework. With ClearPass, the network can identify and segment IoT devices and traffic at the network edge and isolate it from other traffic in the network. This new layer of context enables fine-grained segmentation without the complexity of managing multiple VLANs. For example, a fine-grained segmentation policy can prevent IoT security cameras from accessing credit card transactions or HVAC systems. Zero trust dynamic segmentation helps enterprises isolate any potential security threats by device type, role, and application while helping them meet industry compliance requirements such as PCI, HIPAA, and SOX.

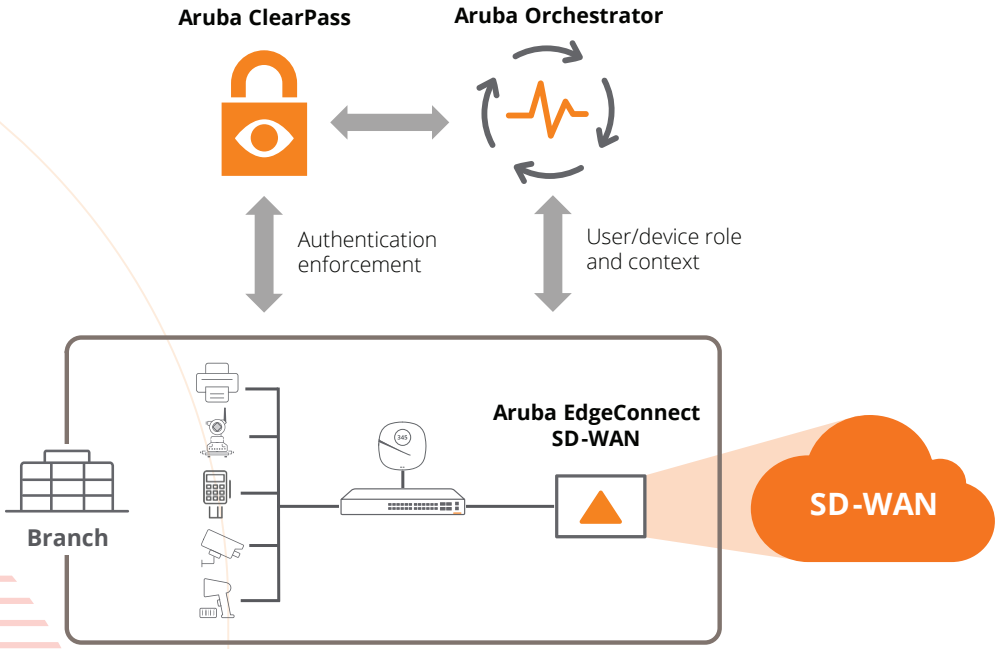

Figure 1: As the new device comes onto the network and registers with Aruba ClearPass, the Aruba Orchestrator (control plane for Aruba EdgeConnect) connects to the ClearPass API.

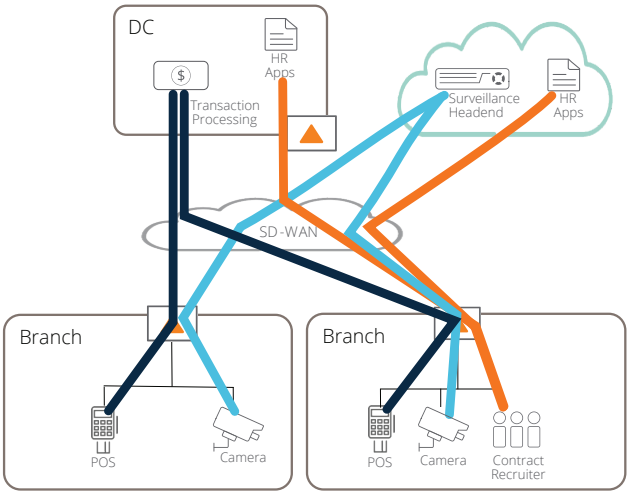

Figure 2: Zero trust segmentation ensures that users and devices can only communicate with destinations consistent with their role in the organization.

COMPREHENSIVE EDGE-TO-CLOUD SECURITY

Advanced SD-WAN solutions like the Aruba EdgeConnect SD-WAN edge platform enable enterprises to intelligently and securely break out cloud-destined traffic locally from branch sites over the internet. Plus, they support micro-segmentation capabilities and granular policy enforcement, enabling enterprises to secure their WAN, adhere to compliance mandates, and defend against breaches.

Automated orchestration of an industry-leading, cloud-delivered security service with the application and identity-aware Aruba EdgeConnect provides a powerful SASE solution without compromising network functionality or security capabilities. Implementing a SASE architecture that combines cloud security with an advanced SD-WAN eliminates both the cost and complexity of managing multiple on-prem next-generation firewalls. The EdgeConnect zone-based stateful firewall with unified threat management (IDPS) protects branch sites from any incoming malicious threats.

The integration of Aruba Threat Defense with the Aruba EdgeConnect SD-WAN edge platform extends advanced intrusion detection and prevention capabilities to the SD-WAN fabric. Both physical and virtual instances of EdgeConnect leverage threat infrastructure and threat feeds from Aruba Central, enabling enterprises to deliver east-west lateral security and secure internet breakout from branch office locations. Threat logging relays network and security analytics back to Aruba Central or a third-party SIEM such as Splunk to deliver comprehensive edge-to-cloud UTM insight. Furthermore, Aruba UTM capabilities integrated with EdgeConnect's zone-based stateful firewall enable granular selection for inspection where users can allow, deny or inspect specific application traffic.

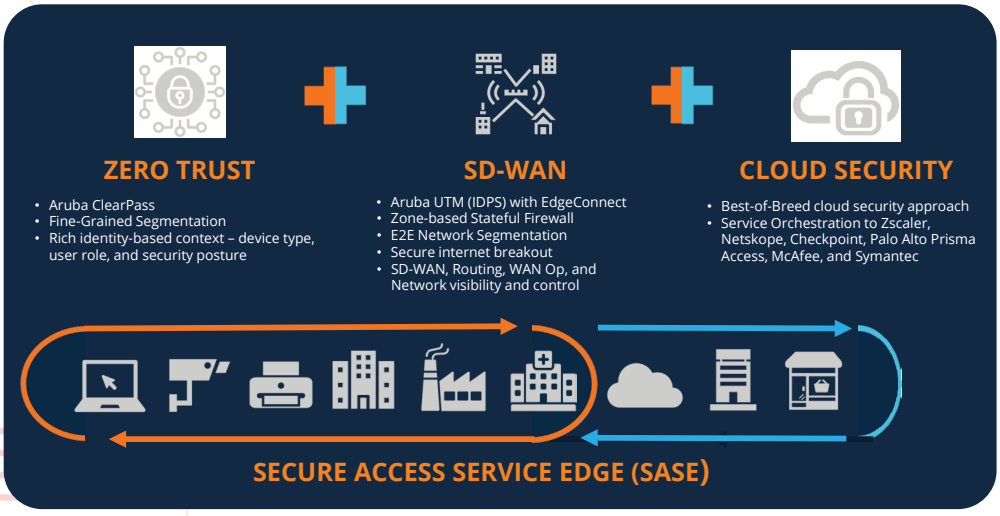

Figure 3: Aruba's Edge to Cloud Security: A new WAN and security edge

CONSISTENT SECURITY POLICIES WITH END-TO-END SEGMENTATION

An enterprise network may utilize multiple types of WAN transport services or underlays. EdgeConnect can bond two or more transport services to form a single logical connection, aggregating the performance of all underlying links. Built upon an application-specific virtual WAN overlay model - business intent overlays (BIO) - Aruba EdgeConnect abstracts the underlying physical transport services from the virtual overlays, each supporting unique QoS, transport, failover, and security policies per application group. Business intent overlays deliver applications aligned with business requirements to users.

Aruba EdgeConnect centrally orchestrates end-to-end segmentation spanning the LAN-WAN-LAN, LAN-WAN-Data Center/HQ, and LAN-WAN-Cloud. Aruba Orchestrator, enables distributed enterprises to segment users, applications, and WAN services into secure end-to-end zones in compliance with predefined security policies, regulatory mandates, and business intent. This results in consistent security policies and automates enforcement across the enterprise. Aruba Orchestrator centralized security administration pares down the task of defining multiple end-to-end zones to a matter of minutes.

Integrated with EdgeConnect, Aruba ClearPass augments rich identity-based context about the user, device type, role, and security posture into the EdgeConnect policy engine. For example, if we take a typical retail chain customer, independent end-to-end segments can be defined for point of sale (POS) traffic, IoT-connected devices such as digital display, HVAC sensors, and security cameras, resource planning, and internet-bound traffic with separate policies for guest Wi-Fi trusted SaaS and recreational web applications. Segments extend from the LAN, across the WAN, and to the cloud service provider's data center. Traffic within a segment is isolated from traffic in other segments, preventing unauthorized access. If a threat were to surface, its impact is contained to the compromised segment. Zone-based security policy definitions also define the transport topology and failover policies for each segment.

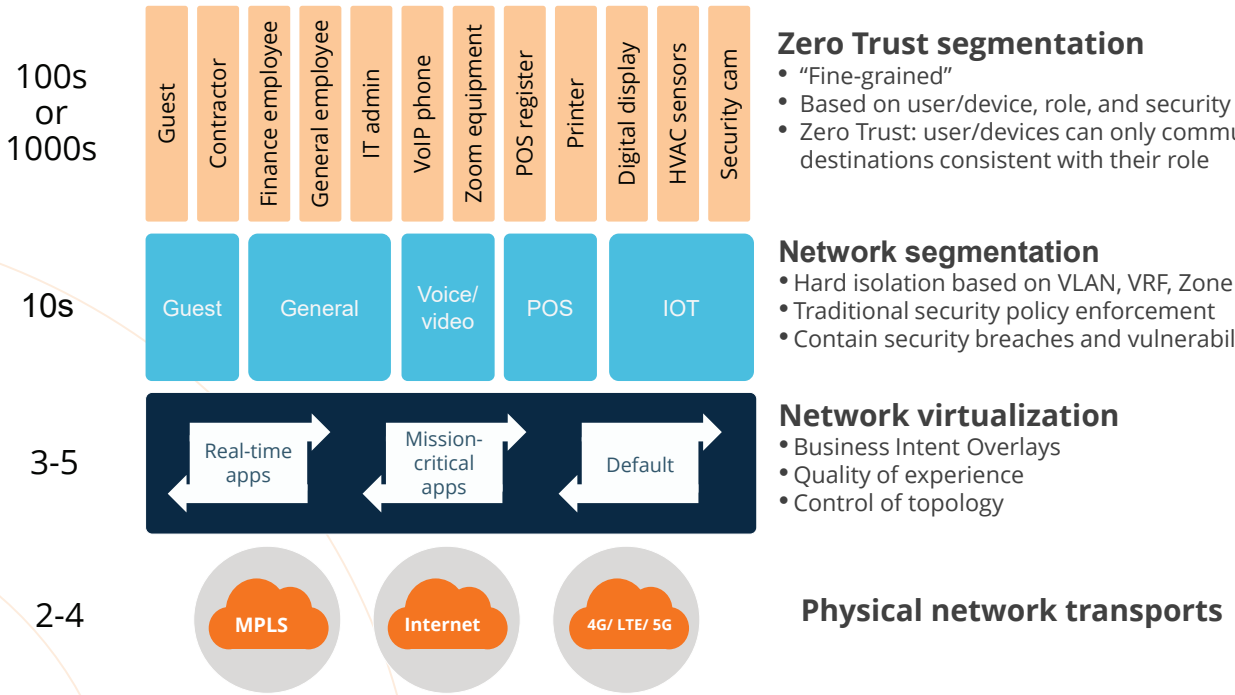

Figure 4: Aruba EdgeConnect multi-faceted end-to-end segmentation

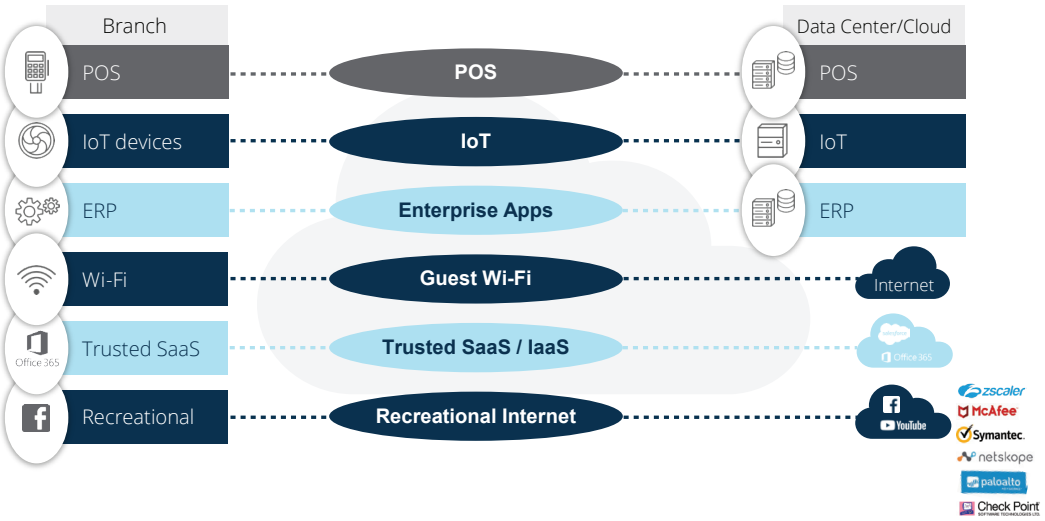

Figure 5: Simplify and automate end-to-end zones spanning the LAN-WAN-Data Center/Cloud

CENTRALIZED ORCHESTRATION IMPROVES OPERATIONAL EFFICIENCY

Using an intuitive graphical user interface, an IT administrator can define segments spanning the LAN and the WAN. Each LAN-side zone may be mapped to a business intent overlay, extending segmentation across the WAN. Multiple LAN-side zones may be mapped to a single business intent overlay. However, the traffic from a single LAN-side zone can be mapped only to a single business intent overlay.

Application traffic within a zone is enabled across the LAN and mapped to the corresponding WAN segment, but all other traffic is denied by default. IT can allow trusted applications or allow specific applications to access users or devices in a different zone. This may include policies for traffic that remains within the branch LAN such as that for a printer shared between multiple zones. A matrix view from Aruba Orchestrator, shown in Figure 6, provides an easy-to-read, intuitive visualization of configured zones and defined allowlist exceptions. Aruba Orchestrator also supports a standard table view, similar to that provided by firewall management applications, making the transition to the end-to-end segmentation model seamless for security professionals.

AUTOMATED ENFORCEMENT AND THREAT CONTAINMENT REDUCES RISK

Once end-to-end segments, zone-based policies and any exceptions have been defined, Aruba Orchestrator programs the policies automatically to every Aruba EdgeConnect SD-WAN appliance, eliminating time-consuming manual configuration of routers and firewalls. Aruba EdgeConnect automates consistent security policy enforcement across the LAN and WAN and to the data center to help enterprises meet compliance requirements, reduce threat risks and ensure continuous business operations.

	Camera	Surveillance Headend	POS Terminal	Transaction Processing	Contract Recruiter	HR Apps
Camera	✗	✓	✗	✗	✗	✗
Surveillance Headend	✓	✓	✗	✗	✗	✗
POS Terminal	✗	✗	✗	✓	✗	✗
Transaction Processing	✗	✗	✓	✓	✗	✗
Contract Recruiter	✗	✗	✗	✗	✗	✓
HR Apps	✗	✗	✗	✗	✓	✓

Figure 6: Security policies enable LAN to WAN traffic within a zone (segment) but deny traffic between zones until IT explicitly allows specific communication between zones.

WAN SEGMENTATION WITH VIRTUAL ROUTING AND FORWARDING (VRF)

Aruba has reimagined virtual routing and forwarding (VRF) for the modern cloud-first enterprise, thoughtfully unifying advanced segmentation capabilities into the Aruba EdgeConnect SD-WAN edge platform.

VRFs allow multiple instances of a routing table to co-exist within the same router/switch, operating at the same time. One or more logical or physical interfaces may have a VRF, and these VRFs do not share routes. Hence packets are only forwarded between interfaces on the same VRF. Because the routing instances are independent, the same or overlapping IP addresses can be used without conflicting with each other. Network functionality is improved because network paths can be segmented without requiring multiple routers.

By combining new VRF capabilities with the existing Aruba EdgeConnect zone-based stateful firewall and network address translation (NAT) capabilities, network managers can apply advanced segmentation definitions to routes and application traffic with just a few mouse clicks within the Aruba Orchestrator management interface. Network managers can now configure and manage separate addressing, routing and security policies consistently across end-to-end segments and micro-segments for traffic traversing the networks of large-scale multinational enterprises and federations of independent companies. Advanced segmentation eliminates the arduous task of manually stitching together VRF, firewall and NAT policies in a consistent manner, dramatically simplifying the management of diverse scenarios and providing unprecedented flexibility when contending with overlapping IP address spaces.

SOLUTION BENEFITS

Zero trust segmentation

Aruba ClearPass integration with EdgeConnect augments application intelligence with user and device identity and role-based context, enabling fine-grained segmentation to assist enterprises in reducing risk and meeting compliance requirements.

Unified Threat Management

The integration of Aruba UTM (IDPS) capabilities with EdgeConnect provides built-in threat detection and prevention for North-South and East-West traffic within the branch.

Best of breed SASE

The advanced, open EdgeConnect SD-WAN platform avoids vendor lock-in and enables a best of breed SASE architecture without compromising either network or security functions.

Automated orchestration with cloud security partners

Aruba EdgeConnect offers “one click” cloud security orchestration, drastically reducing deployment time since no manual overrides are needed. Automated Orchestration finds the nearest cloud security point of presence (POP), thereby optimizing traffic flow.

Consistent policies

Enforce end-to-end zone-based security policies spanning LAN-WAN-LAN, LAN-WAN-Data center and LAN-WAN-Cloud.

Separate lines of business (LoB)

Provide selective access to relevant data and applications to business units or departments based on access privileges; restrict access to specific segments of the network for subsidiary and business partner companies.

Simplified management and visibility

Separate authenticated users from guest users, isolate different traffic types more efficiently, e.g., video surveillance traffic from transactional traffic.

Improved operational efficiency

Centrally orchestrate consistent security policies with fewer human programming errors.

Reduced risk

Contain threats with end-to-end segmentation of users, applications and WAN services.

Better compliance

Segment applications and data to help maintain compliance with regulatory mandates like PCI and HIPAA.

Greater IP address usability

Support overlapping IP address ranges in different segments.

Agility and scalability

Easily configure multiple end-to-end segments.

CONCLUSION

As the threat landscape continues to evolve, the enterprise SD-WAN must enable the agility to adopt new security innovations quickly and cost-effectively. Enterprises should evaluate platforms that offer the freedom of choice to integrate best-of-breed cloud security services now and in the future, and avoid being locked into proprietary single-vendor solutions.

The Aruba EdgeConnect SD-WAN edge platform is a crucial foundational pillar of a best-of-breed SASE architecture, providing the ability to support essential branch security functions such as Zero Trust segmentation with ClearPass, unified threat management with built-in IDPS, and consistent end-to-end security policy enforcement spanning the LAN, WAN, Data Center and the Cloud.

SO_Centrally-Orchestrated-End-to-End-Segmetation_SK_091321 a00109825enw

Contact us at www.arubanetworks.com/contact