HPE aruba networking

Solution overview

Centrally orchestrated end-to-end segmentation

Enforce granular security policies with HPE Aruba Networking EdgeConnect SD-WAN

HPE

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 and the proliferation of IoT devices. Backhauling application traffic to the centralized data center or 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. Additionally, the explosion in the number of IoT devices is representing a significant security gap for organizations, as most IoT devices have a simple design and cannot run security agents.

To realize the full promise of digital transformation, 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 regulatory compliance while reducing complexity and cybersecurity risks.

Security transformation is a multi-layered approach. It starts with securing users, IoT 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, IoT 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 to the cloud. Secure access service edge (SASE) defines an architecture that combines advanced WAN edge network functions deployed at branch locations with comprehensive cloud security services, such as zero trust network access (ZTNA), secure web gateway (SWG), cloud access security broker (CASB), firewall-as-a-service (FWaaS), and many others.

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 HPE Aruba Networking EdgeConnect SD-WAN, 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, EdgeConnect SD-WAN 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 by combining multiple links.

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 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.

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.

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. HPE Aruba Networking ClearPass integration with EdgeConnect SD-WAN 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 SD-WAN Orchestrator (control plane for EdgeConnect SD-WAN) connects to the ClearPass API. The SD-WAN Orchestrator propagates security policy information and any updates related to the user, device type, role, and security posture to all EdgeConnect SD-WAN 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.

ClearPass augments SASE with a zero trust security framework. ClearPass identifies IoT devices and segments the network to isolate IoT traffic from other traffic based on identity and role. 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 requireme[nts such as PCI, HIPAA, and SOX.

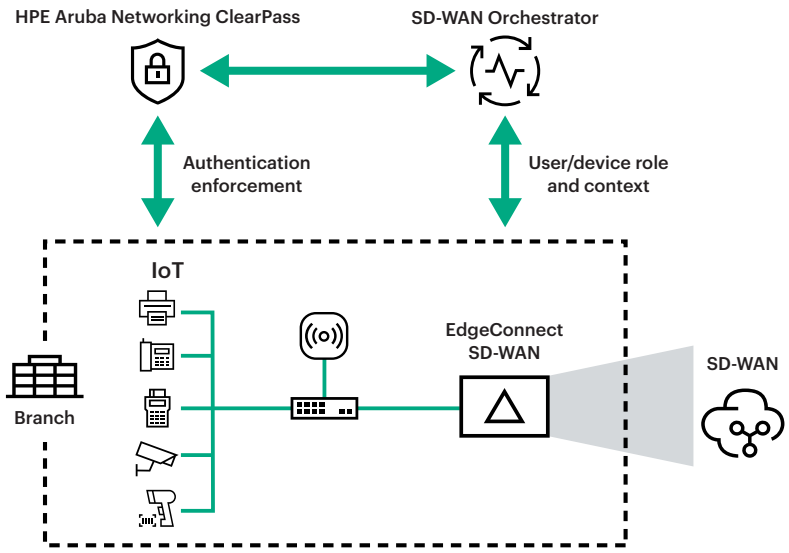

Figure 1. As the new device comes onto the network and registers with HPE Aruba Networking ClearPass, the SD-WAN Orchestrator (control plane for EdgeConnect SD-WAN) connects to the ClearPass API.

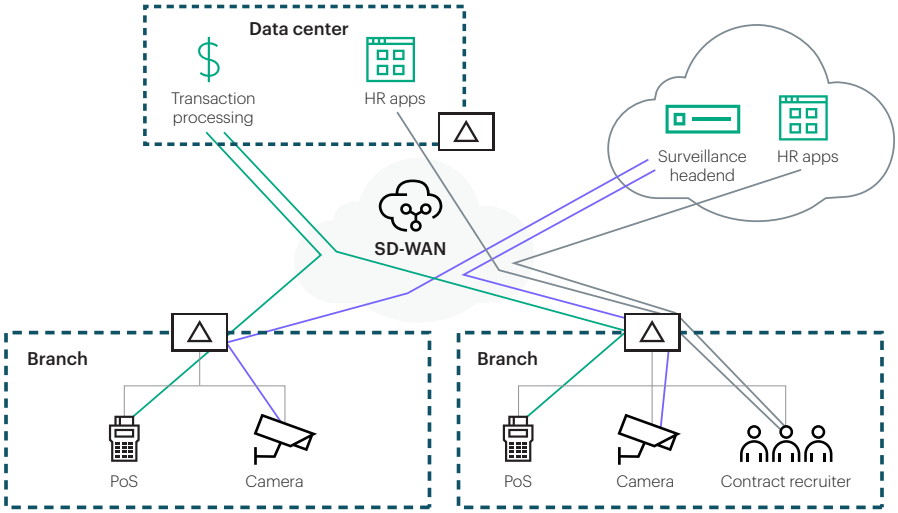

Figure 2. Zero trust segmentation ensures that users and devices can only communicate with destinations consistent with their role in the organization.

Additionally, advanced SD-WAN solutions like the EdgeConnect SD-WAN 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.

Comprehensive edge-to-cloud security

With applications moving to the cloud and hybrid working, EdgeConnect SD-WAN seamlessly integrates with HPE Aruba Networking Security Service Edge (SSE), to create a unified SASE platform, accelerating SASE deployment through a simplified management.

HPE Aruba Networking SSE is an integrated platform where ZTNA, SWG, and CASB share a single codebase. All policies are managed from a single user interface, making access control incredibly simple for IT admins. It enables users and authorized third parties to seamlessly connect from anywhere and access resources with agent and agentless ZTNA. Users are protected against cyber threats with SWG, and sensitive data hosted in SaaS applications are securely monitored to prevent data exfiltration with CASB. Additionally, the solution harmonizes access across the world via a cloud-backbone of Amazon Web Services (AWS), Microsoft Azure, Google™, and Oracle®.

For organizations preferring to adopt SASE with their choice of security services or to seamlessly integrate with an existing security ecosystem, EdgeConnect SD-WAN automates the orchestration to third-party SSE providers.

The EdgeConnect SD-WAN next-generation firewall with intrusion and detection and prevention (IDS/IPS) and DDoS defense capabilities protects branch sites from any incoming malicious threats. EdgeConnect SD-WAN IDS/IPS utilizes the common Unified Threat Management (UTM) framework from HPE Aruba Networking. The signature-based system monitors network traffic to find patterns that match a particular attack signature. Integrated with EdgeConnect next-generation firewall, the system allows application-level selection for inspection based on firewall zones, and provides actions such as drop, inspect and allow traffic. Threat logging relays network and security analytics back to HPE Aruba Networking Central or a third-party SIEM such as Splunk to deliver comprehensive edge-to-cloud security insight.

EdgeConnect SD-WAN detects and prevents DDoS attacks such as protocol attacks, ICMP floods, and SYN floods. Using firewall protection profiles, the solution ensures strict state handling and limits the number of malicious requests with actions such as rapid aging, drop excess and block source. With firewall protection profiles, administrators can enforce different levels of DDoS protection levels across the organization by binding firewall protection profiles to firewall zones.

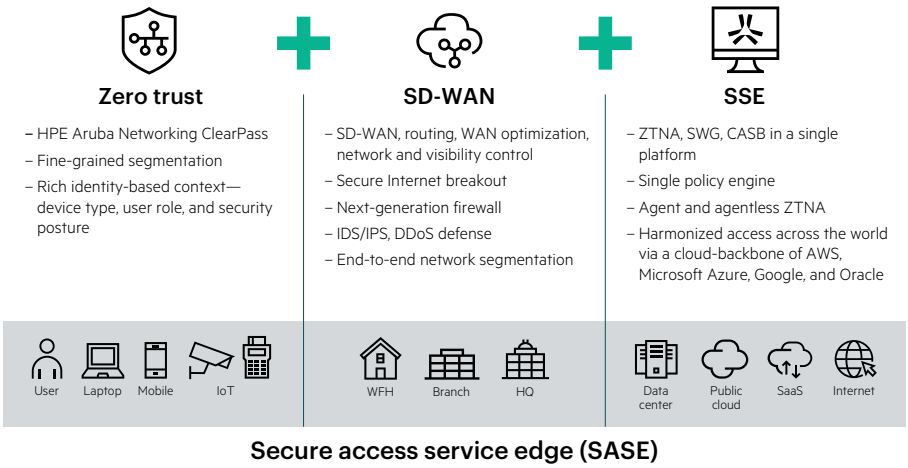

Figure 3. HPE Aruba Networking's edge-to-cloud security: A zero trust WAN and security edge

Consistent security policies with end-to-end segmentation

An enterprise network may utilize multiple types of WAN transport services or underlays. EdgeConnect SD-WAN 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) — EdgeConnect SD-WAN 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.

EdgeConnect SD-WAN centrally orchestrates end-to-end segmentation spanning the LAN-WAN-LAN, LAN-WAN-data center/HQ, and LAN-WAN-cloud. SD-WAN 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. SD-WAN Orchestrator centralized security administration pares down the task of defining multiple end-to-end zones to a matter of minutes.

Integrated with EdgeConnect SD-WAN, ClearPass augments rich identity-based context about the user, device type, role, and security posture into the EdgeConnect SD-WAN 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, security cameras, resource planning, and internet-bound traffic with separate policies for guest Wi-Fi, trusted SaaS and other web traffic. 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.

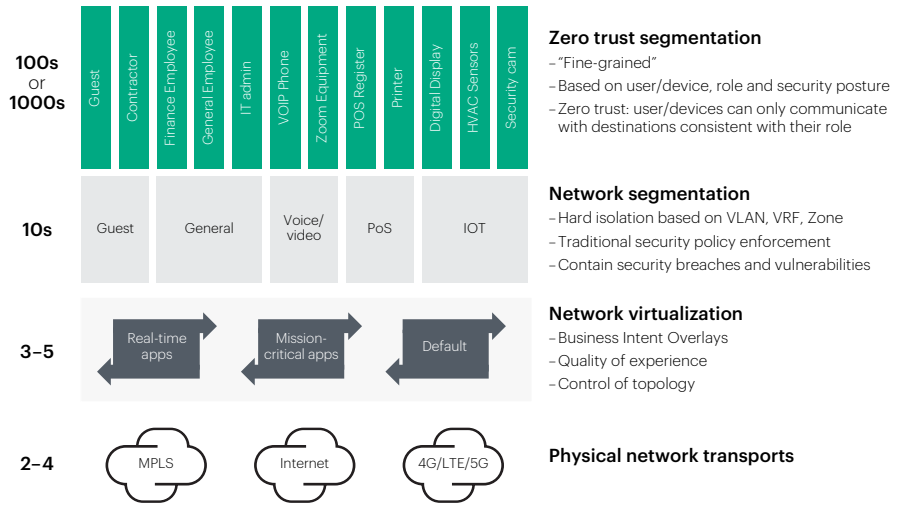

Figure 4. EdgeConnect SD-WAN multi-faceted end-to-end segmentation

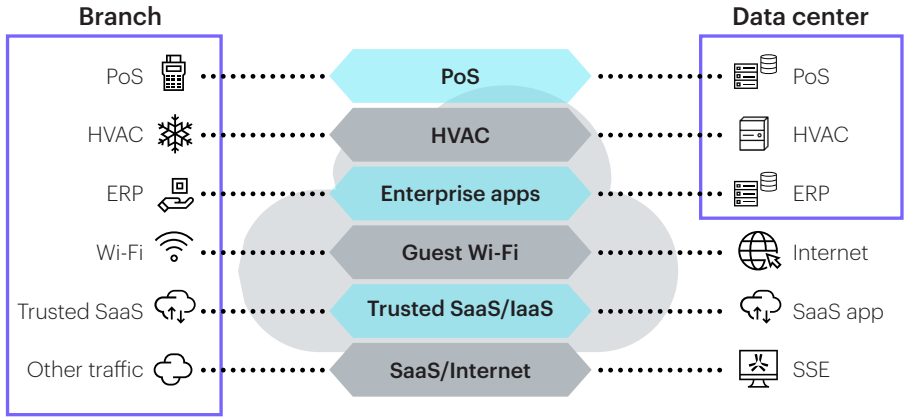

Figure 5. Simplify and automate end-to-end zones spanning the LAN-WAN-data center/cloud

Role-based segmentation in a multi-vendor environment

Additionally, EdgeConnect SD-WAN integrates HPE Aruba Networking Central NetConductor capabilities. This allows organizations to implement an enterprise-wide zero trust architecture, even in complex multi-vendor LAN environments, leveraging EVPN/VXLAN open standards.

EdgeConnect SD-WAN can transport role information across the entire fabric, whether the traffic is directed towards a VXLAN-based campus fabric managed via HPE Aruba Networking Central NetConductor or a third-party campus fabric solution supporting EVPN/VXLAN group-based policy. IT architects can easily create role-to-role micro-segmentation policies that can be applied to the entire enterprise. In case the network does not support VXLAN, radius snooping derives the role directly from RADIUS transactions for authentication and authorization or receives them as login and logout events from HPE Aruba Networking ClearPass via an API.

Through fine-grained segmentation, based on identity and roles, EdgeConnect SD-WAN isolates IoT traffic from mission-critical applications, ensuring that users and IoT devices reach destinations consistent with their role in the business while reducing cybersecurity risks.

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 remain within the branch LAN such as that for a printer shared between multiple zones. A matrix view from SD-WAN Orchestrator, shown in Figure 6, provides an easy-to-read, intuitive visualization of configured zones and defined allow-list exceptions. SD-WAN 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

After end-to-end segments, zone-based policies, and any exceptions have been defined, SD-WAN Orchestrator programs the policies automatically to every EdgeConnect SD-WAN appliance, eliminating time-consuming manual configuration of routers and firewalls. EdgeConnect SD-WAN 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)

HPE Aruba Networking has reimagined virtual routing and forwarding (VRF) for the modern cloud-first enterprise, thoughtfully unifying advanced segmentation capabilities into the EdgeConnect SD-WAN 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 EdgeConnect SD-WAN next-generation 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 SD-WAN Orchestrator management interface. Network managers can 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

ClearPass integration with EdgeConnect SD-WAN 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.

Advanced threat defense

IDS/IPS and DDoS defense capabilities integrated with the next-generation firewall of EdgeConnect SD-WAN provides built-in threat detection and prevention for north-south and east-west traffic within the branch.

Unified SASE

Overcome networking and security challenges with a single platform combining SD-WAN and SSE — for a simpler adoption and a faster deployment of SASE.

Automated orchestration with cloud security partners

EdgeConnect SD-WAN offers “one click” cloud security orchestration, drastically reducing deployment time because manual overrides are not 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.

Segmentation in multi-vendor environment

Enforce role-based segmentation in a multi-vendor environment leveraging EVPN/VXLAN open standards.

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 and isolate different traffic types more efficiently (for example, 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 DSS and HIPAA.

IoT security

Isolate IoT traffic from other traffic based on identity and role.

Agility and scalability

Easily configure multiple end-to-end segments.

Conclusion

With its next-generation firewall, the EdgeConnect SD-WAN platform is a crucial foundational pillar of a SASE architecture — providing the ability to support essential branch security functions such as Zero trust segmentation with ClearPass, IDS/IPS and DDoS defense, as well as consistent end-to-end security policy enforcement spanning the LAN, WAN, data center, and the cloud.

Through fine-grained segmentation, based on identity and roles, the solution isolates IoT traffic from critical applications, ensuring that users and IoT devices reach destinations consistent with their role in the business while reducing cybersecurity risks.

As users connect from anywhere to the cloud, accessing sensitive data in cloud applications and facing potential threats while browsing the internet, EdgeConnect SD-WAN seamlessly integrates to HPE Aruba Networking SSE — forming a unified SASE solution that offers simplicity and faster deployment. To tackle the security challenges of cloud-centric organizations, the SSE solution integrates advanced security capabilities including ZTNA, SWG, and CASB in a single platform, based on a single policy engine, facilitating policy management and operations.

Learn more at

HPE Aruba Networking EdgeConnect SD-WAN

HPE Aruba Networking SSE

HPE Aruba Networking SASE

Visit HPE.com

Chat now

a00109825ENW, Rev.1

HEWLETT PACKARD ENTERPRISE

hpe.com