aruba
a Hewlett Packard Enterprise company

EBOOK

Edge to Cloud Security: A New WAN and Security Edge

A practical guide to adopting a secure access service edge (SASE) architecture

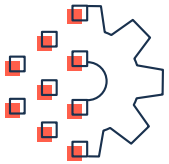
Digital transformation and work from anywhere (WFA) impacts on WAN and security in a cloud-first World

As organizations contend with challenges from the ongoing COVID-19 pandemic and a new "work from anywhere" (WFA) normal, the adoption of cloud-hosted services continues to accelerate. This shift is intensifying the urgency to transform conventional data center and MPLS-centric and VPN-based networks to a cloud-native secure access service edge (SASE), which features more dynamic provisioning of secure network services while protecting data from end-to-end across the WAN.

The 3 most important questions IT executives must address when it comes to securing the WAN are:

- How can I make sure that I select the right SD-WAN architecture to securely support business applications in a cloud-first environment?
- How will the permanent, hybrid WFA environment impact IT decisions on adapting a security architecture in a SASE framework?
- How can IT manage the security challenges associated with the proliferation of largely agentless IoT devices?

Let's examine how networking and security requirements are changing in a cloud-first world.



50%

of respondents in 2021 In process, currently implementing and executing various digital transformation initiatives compared to 38% in 2020[1]

45%

of enterprises have a cloud-first policy[2]

1, 2. ESG IT Technology Intentions Spending Survey, December 2020

Zero Trust, ZTNA, and SASE in a cloud-first world

Traditional security solutions were not designed with the cloud in mind. The concept of backhauling traffic to a centralized data center worked when all applications resided there. With increasing traffic from users in branch offices, and applications moving to the cloud, however, backhauling traffic across a hub-and-spoke legacy network provides a poor user experience, increases security risk, and is expensive.

Legacy network security solutions may not yet incorporate the concept of Zero Trust, an IT security model for identity and access management. It works under the assumption that no user or software action is trusted until authenticated. In other words, authenticate everything, and then restrict access to only those applications and data consistent with the user's or device's role. Zero trust demands that all users, devices, and application instances must prove they are who or what they purport to be, and that they are authorized to access only the resources they seek regardless of whether they are sitting within or outside the network perimeter.

Zero Trust Network Access (ZTNA) is a set of technologies that operates on a Zero Trust framework, where access is granted on a "need-to-know," least-privileged basis defined by granular policies. ZTNA gives users seamless and secure connectivity to private applications without ever placing them on the network or exposing apps to the internet.

Finally, there is SASE, a new term coined by Gartner. SASE defines an edge architecture that combines comprehensive WAN capabilities with comprehensive cloud-delivered network security functions, such as secure web gateway (SWG), cloud access security broker (CASB), firewall-as-a-service (FWaaS), ZTNA, and more.

Challenges with WAN and network security

In today's cloud-first world, WAN and network security needs are more inter-dependent than ever before. To realize the full promise of digital transformation, enterprises will need to transform both their WAN and security architectures to support business applications hosted and accessed from anywhere and any transport network.

Let's examine the most important security and WAN challenges facing enterprise IT and networking teams:

- How can I embrace the business and operational advantages of the cloud while maintaining high levels of security and reducing overall risk?
- How do I ensure a consistent and high-quality user experience for all cloud-hosted business applications across the WAN?
- How do I deploy and enforce consistent network access policies for employees working in a hybrid (partly in the office/branch) or work from anywhere (WFA) environment?
- How do I keep up with the security and WAN connectivity of so many different devices, users, and applications?
- Can choosing the right SD-WAN platform improve WAN and network security integration?
- Can I get all of the security services I need from a single vendor?

Addressing SD-WAN application and security policy integration

In today's fast-paced, global economy, enterprises need the agility to spin up new branch sites quickly and adjust policy and security rules dynamically. Propagating policy context is also critical for branch automation and a key capability that only an advanced SD-WAN solution, like the Aruba EdgeConnect SD-WAN edge platform, can deliver.

An advanced SD-WAN solution can also help enterprises eliminate the need for multiple appliances by unifying key branch WAN edge functions, such as:

- SD-WAN
- Routing
- Zone-based firewall and segmentation
- Unified threat management (UTM)
- Network and application visibility and control
- WAN optimization

Consolidating these functions will simplify or "thin" the branch WAN edge. It will also create significant IT efficiencies and more consistent Quality of Service (QoS) and security policy enforcement by centralizing management.

Aruba EdgeConnect centralized SD-WAN orchestration unifies the configuration and ongoing management. It also ensures that QoS and security are consistently applied and enforced to applications — or classes of applications — regardless of how or where they are being accessed. Application performance and security can be dictated by top-down business policies, not bottoms-up technology constraints.

How SD-WAN enables more consistent security

Implementing a SASE architecture that combines cloud-delivered security with an advanced SD-WAN solution eliminates the cost and complexity associated with managing multiple on-premises next-generation firewalls; the model still requires stateful zone-based firewall functionality at branch office sites to block incoming threats.

The EdgeConnect platform includes:

- Intelligence and application awareness to recognize and permit allow-listed applications to access cloud-hosted resources directly
- Automated integration and orchestration with cloud-security vendors from the branch office to the nearest security enforcement point of presence (PoP)

Key benefits include:

- Reduced latency
- Optimized application performance
- Support for the highest quality of experience for trusted SaaS applications

The integration of Aruba Threat Defense with the Aruba EdgeConnect SD-WAN edge platform extends advanced intrusion detection and prevention (IDS/IPS) capabilities to the SD-WAN. EdgeConnect's physical and virtual appliances leverage Aruba threat infrastructure and threat feeds from Aruba Central, enabling enterprises to deliver east-west lateral security and secure local internet breakout from branch locations. They can be deployed centrally, on-premise or in the cloud. Threat logging provides network and security analytics back to Aruba Central and delivers comprehensive edge-to-cloud UTM capabilities.

Zero Trust: Securing the Edge by role, context & application

With the increase in mobile devices, remote work forces, cloud-hosted applications, and Internet of Things (IoT)-connected devices, enterprises must align business intent-based networking policies and security policies.

The integration of the Aruba ClearPass Policy Manager identity-based access control with the Aruba EdgeConnect SD-WAN platform increases application intelligence by adding identity knowledge of users, devices, roles, and security posture to form the basis of a secure WAN edge.

This new layer of context enables fine-grained segmentation of device types based on their role in the organization, without the complexity of managing thousands of VLANs. For example, a fine-grained segmentation policy can be defined to prevent security cameras from accessing credit card transaction processing or HVAC management systems. It can also restrict security cameras so they can communicate to the surveillance headend or recording device but not to other cameras. This helps IT manage application security compliance and security audits. It also generates threat logs that can be exported to a third-party Security Information and Event Management (SIEM) application.

57%

of respondents say their organizations have either deployed or will deploy Zero Trust[3]

49%

of respondents say their organizations have either deployed or will deploy SASE architectures[4]

71%

of respondents would select a best-in-breed vendor when deploying both SD-WAN and cloud-delivered security for a SASE architecture[5]

3, 4, 5. Ponemon Institute, The State of SD-WAN, SASE and Zero Trust Security Architectures, April 2021

ClearPass: Securing IoT with advanced SD-WAN

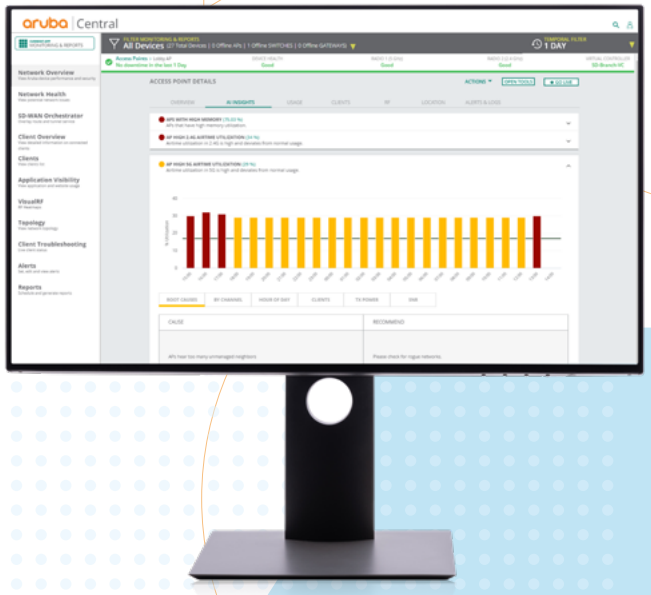
Mobile phones, laptops, or tablets can be secured with ZTNA software agents; however, security software agents cannot be installed on IoT devices since they are agentless. This presents a security challenge that SASE does not directly address.

An Aruba EdgeConnect SD-WAN platform can reduce the risk associated with breaches when deploying IoT devices. The EdgeConnect platform identifies and classifies application traffic on the first packet, intercepts it at the network edge, and can assign it to an appropriate segment. This coarse-grained segmentation secures it from other traffic on the network.

ClearPass integration with EdgeConnect augments application intelligence with user and device identity and role-based policy, enabling even finer-grained segmentation. The additional identity-based context enables consistent security policy enforcement that can be enforced network-wide, from the edge to the cloud.

Aruba Zero Trust Dynamic Segmentation helps enterprises identify security threats by device, role, and application while adhering to industry compliance standards such as PCI, HIPAA, and SOX.

Combining advanced SD-WAN and cloud-delivered security using a policy-based ZTNA ensures the enterprise WAN, users, devices, and applications are always secure.



Best of breed WAN and security - without compromise!

Addressing security and cost challenges, centrally-orchestrated best-of-breed cloud-hosted security services have emerged and continue to enjoy rapid adoption. Centrally-managed cloud-delivered security services supply protection for all users, supported by consistent policies and policy enforcement across hundreds or even thousands of sites — without the complexity of deploying or managing any physical security appliances.

Advanced SD-WAN solutions like the Aruba Edgeconnect SD-WAN edge platform let enterprises intelligently 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-aware Aruba EdgeConnect SD-WAN edge platform provides a powerful SASE solution without compromising either network functionality or security capabilities.

SASE protects the enterprise from threats and delivers the highest application performance and user experience while keeping costs in check.

Benefits of this marriage of SD-WAN and cloud-delivered security include:

- Greater business agility and simplified IT policies with a SASE architecture that delivers the full benefits of the cloud
- Simplified and streamlined integration of cloud-native security functions with optimized SD-WAN capabilities
- Freedom to choose best-of-breed network security and best-of-breed SD-WAN capabilities
- Avoiding single vendor lock-in
- Eliminating the need to deploy expensive and complex next-generation firewalls at every branch location
- Flexibility to adopt new security innovations in the future

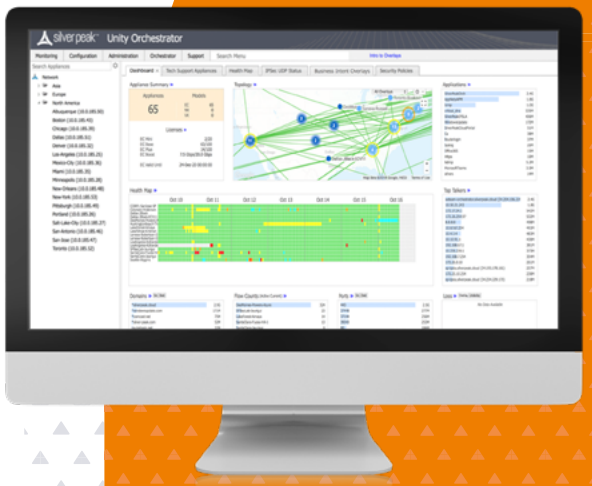
Cloud-based security automation with SD-WAN

Enterprises are seeking easier ways to integrate and manage their applications across their WAN and security infrastructure. One of the best ways to simplify the orchestration of cloud-based security services at branch sites is to leverage automation with Aruba EdgeConnect SD-WAN.

EdgeConnect uses application programmable interfaces (APIs) and third-party service orchestration to integrate with the leading cloud-security providers, including ZScaler, Check Point, NetSkope, and Palo Alto Prisma Access.

The Aruba Orchestrator validates the cloud security credentials to connect and then automates or orchestrates the process of connecting branch locations in the SD-WAN fabric to the closest primary and optional secondary cloud security enforcement PoPs.

Security policy configuration is a simple drag-and-drop action from the intuitive Aruba Orchestrator user interface, enabling organizations to specify a set of security policies to be applied to all branch locations in a single action.



Flexibility & freedom of choice

As the threat landscape continues to evolve, enterprises must retain the agility to be agile when adopting new security solutions quickly and cost-effectively. They should evaluate platforms that offer the freedom of choice to integrate best-of-breed network and security solutions. They can then avoid being locked in to proprietary single vendor solutions or having to settle for basic features and capabilities.

The Aruba EdgeConnect business-driven SD-WAN platform is a key pillar of a best-of-breed SASE architecture, providing the ability to integrate a best-in-class SD-WAN platform with a variety of best-in-class cloud-delivered security services. Aruba EdgeConnect supports the foundational security functions required at the branch and complements cloud-delivered security to deliver a seamless secure access service edge across the entire enterprise.

For more information, please go to www.arubanetworks.com/sdwan

eBook_Aruba-Edge-to-Cloud-Security_DC_062321 a00114994enw

aruba
a Hewlett Packard Enterprise company