Solution Brief

Reducing Costs and Complexity While Increasing Performance and Security with Secure Access Service Edge Architecture from Aruba and Netskope

Introduction

Enterprise network traffic patterns have changed dramatically over the past few years. The shift to cloud-based applications is increasing the amount of data that leaves the corporate network. The increase in telework and video conferencing as a result of the pandemic has dramatically altered data traffic patterns and exposed inefficiencies in existing network infrastructures.

Traditional enterprise network design directed all traffic to a central data center, with the data center firewall handling all traffic in and out of the corporate network. This architecture allowed IT to easily control the data entering and exiting the corporate network, while keeping the attack surface small. As use of SaaS applications and external web and cloud traffic increased, this central firewall quickly became a bottleneck that limited performance and impacted user experience.

Software Defined WAN (SD-WAN) enables branch offices to break out traffic intelligently: sending internal traffic to the corporate headquarters or data center while data destined for the cloud can bypass the headquarters or data center and go from the branch office directly to the cloud. The combination of an advanced SD-WAN and cloud-delivered security is commonly known as secure access service edge or SASE. The ideal model for delivering a SASE architecture requires the following functions at the edge and in the cloud.

At the Edge:

- SD-WAN
- Routing
- Zone-based Firewal
- Advanced Segmentation
- UTM
- WAN Optimization

In the Cloud:

- Firewall as a Service (FWaaS) to consistently apply and enforce security policies across all locations and users
- Secure Web Gateway (SWG) to filter and protect web traffic and enforce corporate policies
- Cloud Access Security Broker (CASB) to enforce corporate policies with cloud-based applications to help protect corporate data
- Zero Trust Network Access (ZTNA) to allow targeted access to specific applications and resources, replacing VPNs which gives complete access to the LAN

SASE combines the flexibility and performance of SD-WAN infrastructure with the robust protection provided by cloud-hosted security services. Each office is equipped with an SD-WAN appliance that connects to the cloud security service provider.

Due to its software-defined nature, SD-WAN can be rapidly reconfigured to adapt to changing network patterns, such as when employees in one region are suddenly required to work remotely while employees in another region are allowed to return

Table of Contents

Introduction 1

Advanced SD-WAN with Aruba Edge-Connect SD-WAN Edge Platform . 2

Cloud-delivered Security with Netskope Security Cloud. 2

Intel's Ongoing Investment in SASE 3

Conclusion 4

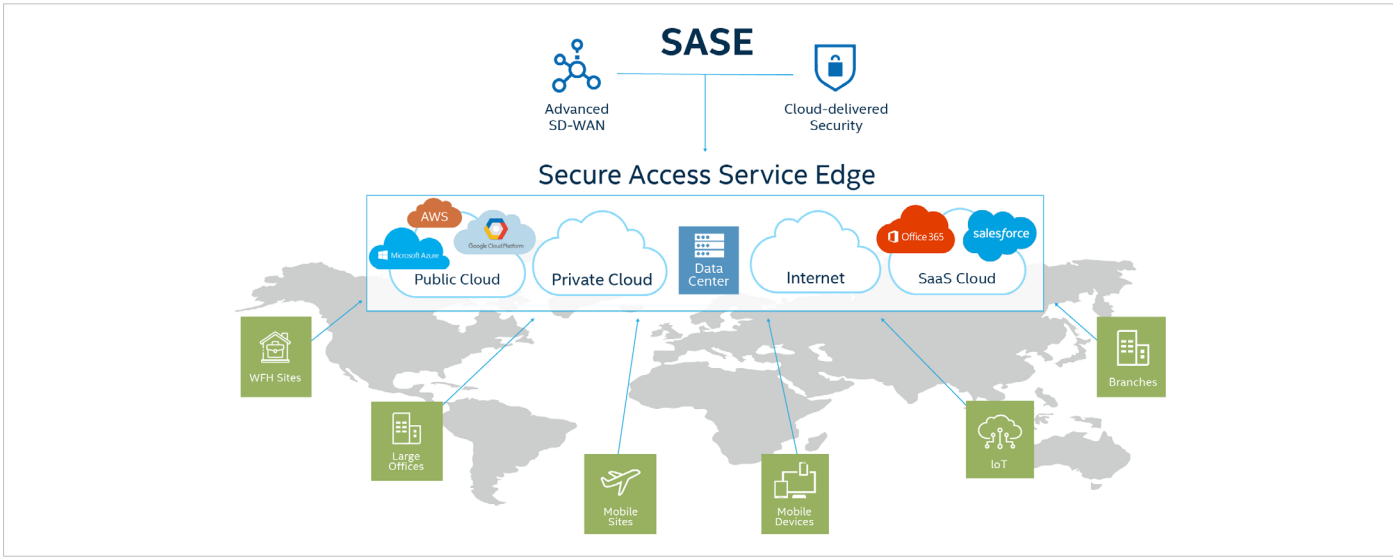

Figure 1. Secure Access Service Edge (SASE) Network

to the office. It also gives customers granular control over which traffic gets steered to the cloud security vendor's network. Similarly, cloud-delivered security solutions can address rapidly evolving security needs as new applications, security and compliance requirements, and threats emerge. Plus, cloud security extends protection to the users even when they are off the corporate network. The combination of these two services results in a solution that delivers seamless security services and speeds application performance without hindering business productivity or negatively impacting the end-user experience.

Advanced SD-WAN with Aruba EdgeConnect SD-WAN Edge Platform

Aruba EdgeConnect has been designed to help customers reduce cost and complexity compared to legacy, function specific appliances, as they deploy SD-WAN infrastructure. EdgeConnect enables companies to create a virtual WAN for every class of traffic, with application performance, security, and routing policies automatically programmed to all sites to ensure consistency across the network. With EdgeConnect, end users experience consistent application performance including high quality voice and video over broadband connections. IT benefits with real-time monitoring, continuous adaptation, and automated response to ensure the highest performance and availability, whether applications reside in the data center or the cloud.

Aruba EdgeConnect SD-WAN edge platform identifies more than 10,000 SaaS applications and 300 million web domains, enabling intelligent traffic steering and security policy enforcement. As new SaaS applications are released, EdgeConnect filters can be automatically updated to ensure the SD-WAN adapts and evolves to keep up with the dynamic environment.

With the SD-WAN appliance needing to scan every packet and compare against these huge lists of applications and web sites, Aruba engineers knew performance would be a critical element in the design of the EdgeConnect platform. Aruba chose to base EdgeConnect on Intel® architecture to deliver a solution that could easily scale to meet the performance needs of each location. With Intel Atom® processors powering appliances for small branch offices to the family of Intel® Xeon® processors for larger campuses, Intel architecture allows Aruba to deploy a common code base across a wide range of hardware platforms to deliver performance tailored for specific office sizes. These processors also include instructions that accelerate AES cryptographic functions, allowing EdgeConnect to use encryption extensively with minimal impact to overall system performance.

EdgeConnect is also able to leverage other Intel technologies to enhance performance. Data Plane Development Kit (DPDK) is an open-source library that accelerates packet processing workloads, allowing for higher bandwidth while reducing CPU overhead and allowing more CPU resources to be allocated to other functions. Specific optimizations in DPDK for Intel® products have been shown to improve packet processing performance by up to ten times.

Cloud-delivered Security with Netskope Security Cloud

Netskope Security Cloud delivers high-performance real-time, inline and data-centric security while also simplifying the orchestration and management of ever-changing security requirements and policies across an organization. Netskope Security Cloud combines SWG, CASB, ZTNA, along with cloud firewall, data loss prevention, remote browser isolation, and other security solutions. This cloud-native architecture uses big-data analytics to analyze security risks, eliminate blind spots, and simplify policy enforcement. Web classification and filtering algorithms, combined with machine learning content analysis, allows organizations to apply security policies regardless of whether traffic is going to a known or unknown website or cloud application, and regardless of whether it is directed to a business or personal account of the application, such as with Microsoft Office365 or Google G-suite.

The resulting need to scan large amounts of traffic at high speed, while introducing as little latency as possible, while also inspecting deeper into the packets, drove Netskope to also base their solution on Intel® Xeon® Scalable processors.

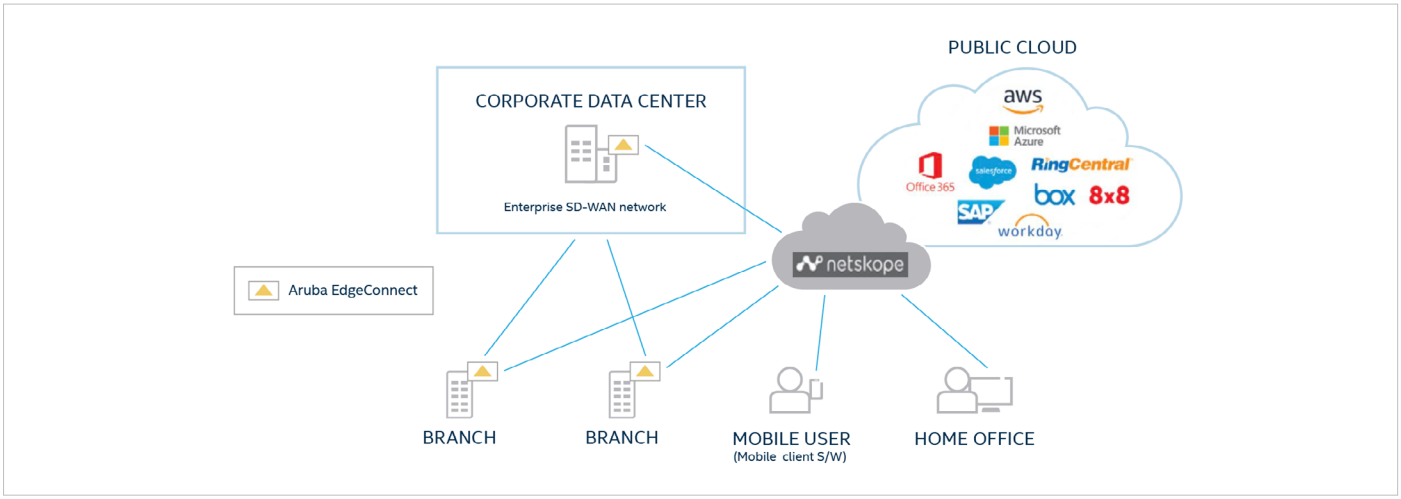

Figure 2. With Aruba EdgeConnect, enterprises can connect directly to cloud using broadband internet.

In addition to DPDK to increase packet processing performance, Netskope was also able to utilize HyperScan, a library of pattern matching algorithms that leverage optimizations found in Intel Xeon processors to accelerate matching performance. This allows Netskope to increase the breadth and depth of its security algorithms, including watching for signatures of new Zero Day exploits along with more robust IDS and IPS functions while maintaining throughput levels.

Intel technology is a key component in the Netskope NewEdge security private cloud. Comprised of data centers in more than 50 regions globally, each data center has full compute, with all services integrated in a single-pass architecture to provide customers real-time, inline security traffic processing. Netskope built NewEdge from the ground-up to optimize for performance and low latency, and Netskope maintains complete control over routing, peering, and data center locations to avoid the unpredictable performance of the public cloud. Similarly, NewEdge does not use virtual POPs, which require backhauling traffic inside the cloud security vendor's network and merely moves the traffic bottlenecks of legacy WAN architectures to the cloud.

Intel's Ongoing Investment in SASE

By basing their solutions on Intel architecture, Aruba and Netskope are able to take advantage of several key advantages that helped them achieve their goals, including:

- **Flexible workload capacity** – With processors ranging from Intel Atom processor to Intel® Xeon® D processor and Intel Xeon Scalable processor product family, Netskope and Aruba can design solutions to accommodate the full range of work locations, from small branch offices to large campuses.
- **Hardware-based security** – Secure boot, platform attestation, and virtualization technologies included in Intel architecture helps ensure that software is trusted, isolated, and more difficult for attackers to compromise.
- **Accelerated cryptographic operations** – Support for high-speed cryptographic functions delivers optimal protection for data with minimal impact to CPU resources.

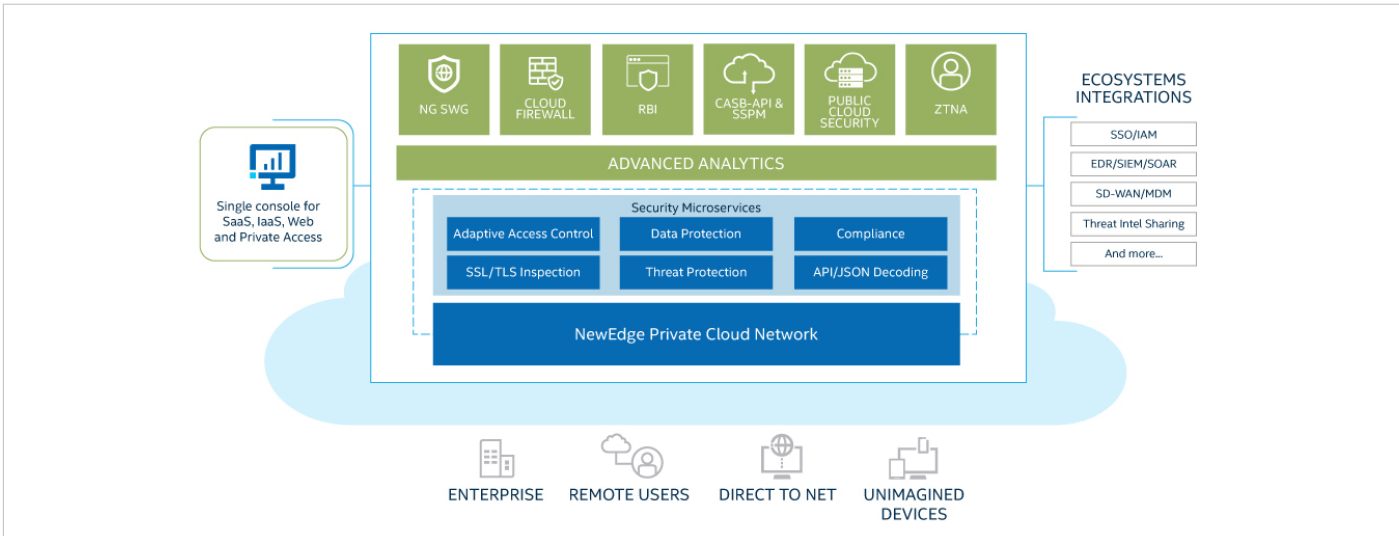

Figure 3. The Netskope SASE-ready architecture and cloud-native, secure edge services.

- **Accelerated packet processing operations** – Support for the latest high-speed Ethernet controllers along with packet processing optimizations ensures solutions can keep up with the latest bandwidth requirements.

In addition to the capabilities that are already being leveraged by Aruba and Netskope, Intel continues to develop new technologies and collaborate with industry partners to deliver solutions that that will augment and improve SASE implementations in the future. Examples include:

- Artificial Intelligence and Deep Learning accelerators built into the CPU that allow expanded use of AI to detect security anomalies and help keep customers safe.
- Collaboration with software developers to integrate support for new capabilities into tools such as OpenVINO, PyTorch, and TensorFlow, which will allow SASE developers to add sophisticated machine learning capabilities to deliver cutting-edge security solutions that respond to the increasing threats to business networks while maintaining high through-put and low latency to ensure day-to-day operations run smoothly.

Conclusion

The move to the cloud is diminishing the value and effectiveness of legacy network infrastructures. Plus the rapid shift to remote and hybrid work is further accelerating this transformation. The increased use of web and cloud-based applications requires the flexibility and efficiency of SD-WAN at the branch, headquarters and data center. Similarly, the security requirements of this new architecture require the universal coverage and high efficacy of cloud-delivered security services. These dual requirements underpin the unique benefits of a SASE implementation and are driving the convergence of networking and security architectures.

With Aruba Edge Connect SD-WAN platform working in unison with Netskope Security Cloud, organizations can transform their infrastructure at their own pace. The flexibility of this combined solution allows business to start with select cloud-based apps, and then expand at their own pace until all traffic has been routed to the cloud for security. Because both Aruba and Netskope solutions are based on Intel architecture, organizations can have the confidence that their SASE investment will have the scalability, performance, and innovation to continue to adapt and respond to evolving network and security needs in the future.

Printed in USA 349100-001 EN ♻ Please Recycle 1221/DL/ICKK/PDF