aruba
a Hewlett Packard Enterprise company

PARTNER SOLUTION OVERVIEW

Aruba EdgeConnect SD-WAN and Zscaler

Cloud-delivered Secure Access for Any User, Any Application and Any Location Anywhere

Aruba EdgeConnect SD-WAN and Zscaler create a tightly integrated SASE architecture that automates security policy enforcement for any user, application or device across any location.

EXECUTIVE SUMMARY

As applications continue to migrate to the cloud, changing traffic patterns drive the need for a new Wide Area Network (WAN) approach and security model. When all applications were hosted in enterprise data centers, all traffic from branch locations was backhauled to the data center over MPLS circuits, with the entire stack of security services enforced at data center egress points, requiring only rudimentary security services at the branch.

In today's modern enterprise, applications are hosted everywhere: the data center, in public and private clouds, or delivered by myriad Software-as-a-Service (SaaS) providers. With a hybrid workforce, remote workers access applications from anywhere, from any device and across diverse WAN transports, including broadband internet, further complicating the security model and the IT challenge. They need consistent security and always-on threat protection that traditional networks no longer support. As cyberattacks continue to evolve, organizations require advanced security controls, like intrusion prevention (IPS), Data Loss Prevention and sandboxing, as well as SSL inspection to defend against threats and vulnerabilities.

The proliferation of IoT devices adds other security challenges for IT, as these devices cannot run a security agent and significantly increase the attack surface, which requires additional protection measures to isolate IoT devices.

To address these security challenges, the secure Aruba EdgeConnect SD-WAN platform supports cloud-first organizations by intelligently and securely steering application traffic to the cloud. It includes advanced next-generation firewall and routing capabilities, allowing organizations to replace legacy branch firewalls and routers, and reduce hardware footprint at the branch. For further protection in the cloud, the solution tightly integrates with

CLOUD-FIRST SECURITY CHALLENGES

Dissolving security perimeter

Users connect from anywhere and from any device using untrusted links, while accessing sensitive data in the cloud.

Unpredictable application performance

In traditional network architectures, the traffic is backhauled to the data center for security inspection, impacting application performance.

Equipment sprawl

Organizations have accumulated many networking and security devices that are difficult to configure and maintain, leading to inconsistent security policies.

SOLUTION BENEFITS

Support cloud-first organizations

Build a tightly integrated SASE architecture with best-in-class SD-WAN and SSE through automated orchestration, API integration and intelligent steering to the cloud.

Enable hybrid work

Provide secure access from everywhere while delivering the highest quality of experience to users.

Reduce hardware footprint and enforce consistent security policies to all users

Replace legacy branch firewalls and routers and automate security updates to enforce consistent security policy across all locations.

zscaler

the Zscaler Cloud Security Platform that adds Security Service Edge (SSE) capabilities such as ZTNA, CASB and SWG. This enables organizations to build a powerful secure access service edge (SASE) architecture that combines SD-WAN and SSE, to protect them against growing cyberthreats, while delivering the highest application performance in multi-cloud environments.

APPLICATION MIGRATION TO THE CLOUD COMPELS WAN AND SECURITY TRANSFORMATION

Enterprises face several challenges when migrating applications to the cloud. To deliver the highest performance, users should connect directly to cloud-hosted and SaaS applications over the internet. However, that increases the attack surface at branch locations and, without the deployment of strong security measures, can expose the enterprise to threats and vulnerabilities.

In the device-centric model based on routers and discrete firewalls, this has meant a hub-and-spoke architecture and backhauling all internet-bound traffic to a headquarters site for inspection by next-generation firewalls. This backhaul consumes expensive MPLS bandwidth, adds latency and negatively impairs application performance.

CLOUD-FIRST IT SECURITY CHALLENGES

A "work-from-anywhere WAN" — any device, anywhere: IT faces another security challenge in executing cloud-first strategies. Users access cloud and SaaS applications from everywhere — home, hotels, the local coffee shop — not just from branch offices. The rapid growth of IoT devices adds to the security task. To address this challenge, enterprises must arm workers with a security service solution that follows them wherever they go, providing a fast and secure experience for all users wherever they connect. And in today's enterprise, that security must extend to the broad range of headless IoT devices that reside in the network. Unlike laptops, tablets and smart phones, ZTNA software agents cannot be installed on headless IoT devices. Therefore, additional security measures not addressed by SASE must be taken. Enterprises can address this risk by implementing comprehensive role-based access control solutions that enable centralized definition of security policies that isolate and segment IoT devices by zones of related devices, applications, and services. These zones — or segments — enable devices to communicate only with destinations consistent with their role.

Not all apps are created equal: Some SaaS offerings, such as VoIP services, are jitter-sensitive, support robust security measures and therefore don't expose risk to the enterprise. Connecting users directly to these applications provides the best user experience. However, other cloud or web-based applications may not be as secure or may expose the enterprise to threats or intellectual property (IP) leakage and require more advanced security inspection. For example, an employee could inadvertently — or maliciously — transfer company IP in a Facebook message. In another example, corporate policy may dictate excluding Guest Wi-Fi traffic from SSL inspection or user authentication while applying those requirements to all other traffic.

Work-from-anywhere, any device and any application exceptions must be implemented automatically and consistently across the enterprise to ensure the security of the corporate network is not compromised. IT must be able to support granular security policies with end-to-end segmentation based on applications, users, locations and devices, all in accordance with business requirements or "intent."

Applications and vulnerabilities change constantly: SaaS application definitions and the range of IP addresses used to access them change continuously, especially for popular SaaS applications, such as Microsoft Office 365, UCaaS applications like RingCentral and recreational apps, such as Facebook, Instagram and others. A research study shows that hundreds of millions of attempted cyberattacks occurs every day[1]. The WAN and security must continuously adapt — automatically — so that IT can keep pace with constant changes in order to provide secure, uninterrupted access to business-critical applications.

Rapidly deploying new branch locations and applications: To maintain a competitive edge in today's global markets, IT must respond quickly to deploy new applications as well as bring new sites online. Bringing up new sites under the traditional WAN model based on routers, discrete firewalls and MPLS connections can typically take three months or longer. To address business growth, whether organic or through acquisitions, and to meet application demands, enterprises now require the ability to automate deployment of new WAN and security services with true zero-touch provisioning.

[1] Help Net Security. 2021. https://www.helpnetsecurity.com/2021/02/17/malware-2020/

Remediating WAN performance and security issues: The emergence of the cloud, coupled with increasing use of broadband internet and 4G/LTE services as active WAN transports, makes it more difficult for IT to resolve security, network and application performance issues. However, end-user expectations for always-on, high-performing applications is higher than ever. Enterprises need tools that enable faster troubleshooting so that IT can be more responsive to the business.

Addressing these challenges requires a re-architecting of the WAN and security infrastructure models.

SASE FOR A CLOUD-FIRST WORLD

Digital transformation has rendered traditional network and security architectures obsolete, as applications migrate from the data center to the cloud. Gartner coined the term secure access service edge (SASE) to describe offerings designed to address this new paradigm. SASE is an architecture that combines SD-WAN with cloud-delivered security services (SSE or Security Service Edge).

By integrating comprehensive SD-WAN capabilities with SSE functions, such as secure web gateway (SWG), cloud access security broker (CASB), firewall-as-a-service (FWaaS), and zero trust network access (ZTNA), enterprises can support the dynamic secure access needs for digital transformation. The key design principal of SASE is the transformation from heavy hardware-laden branches to thin branches with cloud-native services, including WAN management and a comprehensive stack of security services. This architecture allows enterprises to balance performance, availability, agility and costs.

Together Aruba and Zscaler, leaders in SD-WAN and cloud security, enable customers to implement zero trust and SASE frameworks that uniquely addresses the evolving business needs faced by cloud-first enterprises today.

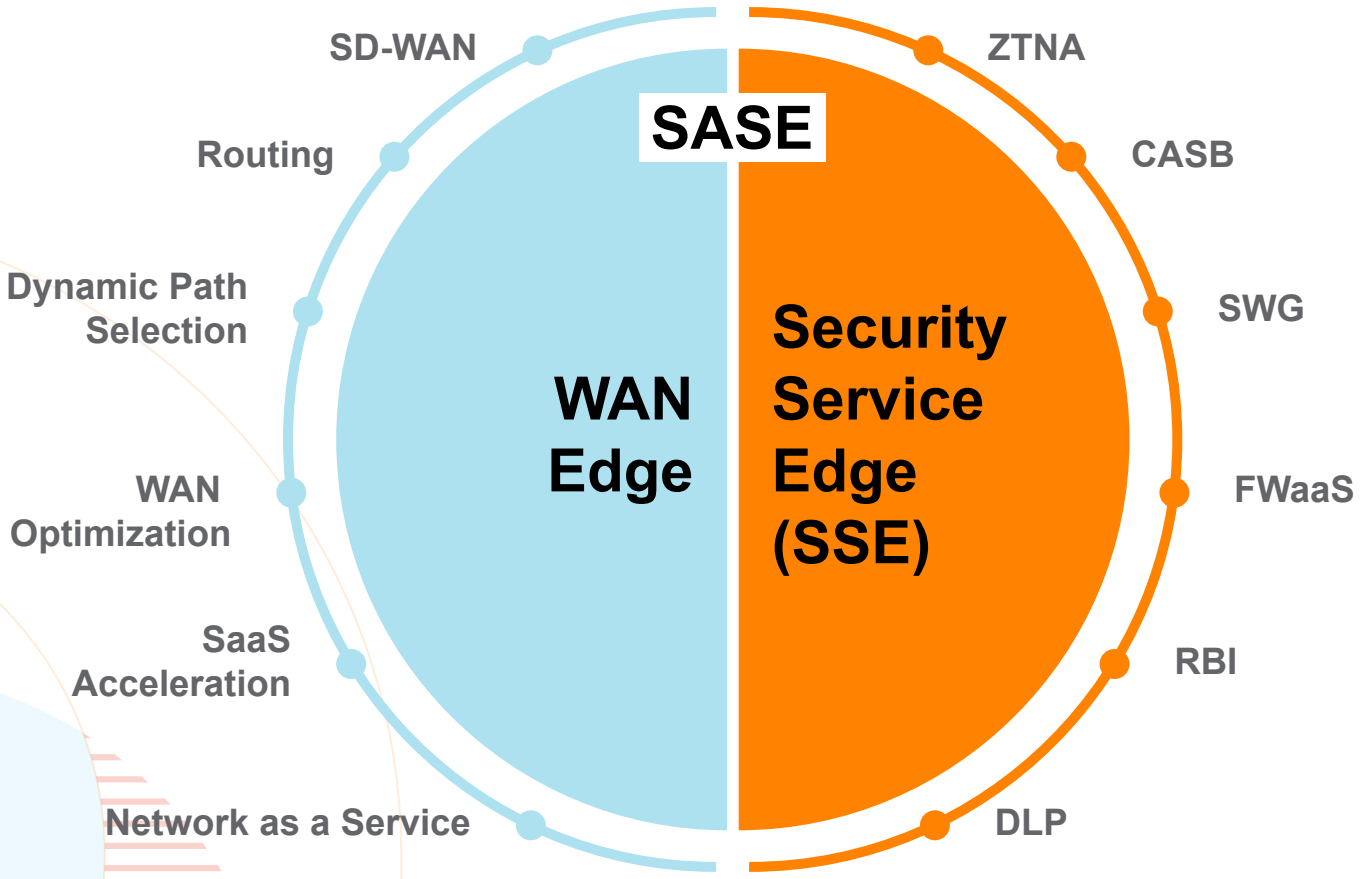

Figure 1. SASE is a network architecture that combines SD-WAN with Security Service Edge (SSE) capabilities

SECURE WAN ACCESS WITH ARUBA AND ZSCALER

Cloud-hosted security services, such as Zscaler Internet Access™ (ZIA), is an SSE solution that provides a superior security alternative for cloud-first enterprises. Centrally managed and supporting a full security stack, including SWG (Secure Web Gateway), CASB (Cloud Access Security Broker), DLP (Data Loss Prevention), RBI (Remote Browser Isolation), sandboxing, and more, Zscaler delivers identical protection for all users and consistent policies and policy enforcement across hundreds or even thousands of sites — without buying, deploying or managing any physical security appliances.

Zscaler Internet Access coupled with the secure, business-driven Aruba EdgeConnect SD-WAN platform streamlines WAN edge infrastructure at the branch. EdgeConnect fully automates the orchestration with Zscaler and allows organizations to define security policies that are enforced either at the branch or in the Zscaler cloud.

Built-in next-generation firewall in EdgeConnect SD-WAN: Not only does Aruba EdgeConnect SD-WAN improve application performance, enable more efficient connectivity, and reduce network complexity, it also includes a next-generation firewall and routing capabilities, allowing organizations to replace legacy firewalls and routers at the branch, and consolidate network and security equipment.

Enterprises no longer need to deploy expensive, complex-to-manage next-generation firewalls at every branch location. Aruba EdgeConnect next-generation firewall capabilities include advanced security features such as DPI (Deep Packet Inspection), IDS/IPS and DDoS protection. Additionally, it provides fine-grained segmentation based on identity and role. This enables organizations to secure IoT devices that cannot run ZTNA agents, by ensuring that users and IoT devices only reach destinations consistent with their role in the business.

Granular security policy enforcement: Aruba EdgeConnect First-packet iQ™ application identification enables intelligent, granular traffic steering. This facilitates granular security policy enforcement based on business intent, securing the organization while delivering the highest performance for all applications.

For example, a set of business-driven security policies might include:

- Send enterprise data center-hosted application traffic directly to headquarters
- Send trusted SaaS traffic such as UCaaS, directly to providers' cloud services
- Send other internet-bound traffic, including Salesforce, Facebook, YouTube, Box and web browsing traffic to a Zscaler cloud point of presence (PoP) for security inspection prior to handing off to providers' cloud or web services

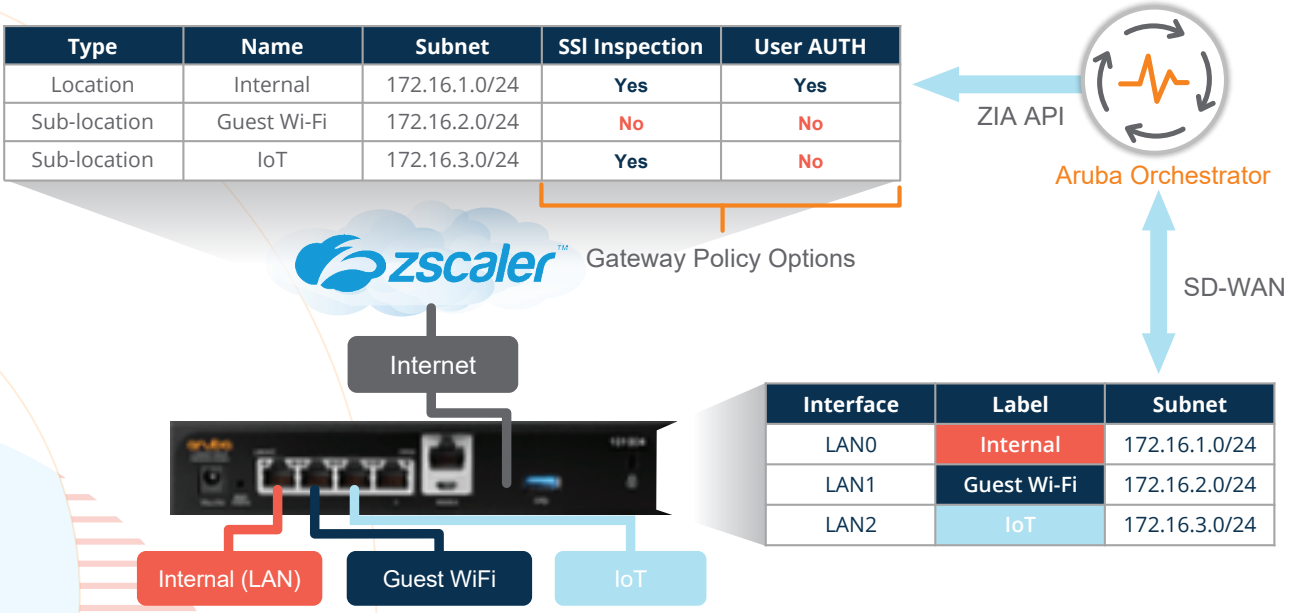

Figure 2. Sub-location addresses and subnets mapped automatically to Zscaler Internet Access cloud-delivered security services, enabling IT to define unique security policies per sub-location.

Application, user and device level control: With the Aruba EdgeConnect and Zscaler API integration, IT organizations can specify a set of Zscaler security policies to be applied across branch locations. Occasionally, different security policy enforcement is required for specific applications, users, and devices within a branch location. The Zscaler Gateway Options feature enables organizations to define exceptions for sub-locations (See Figure 2). An enterprise might define the following policies:

- Enterprise traffic requires SSL inspection
- IoT devices accessing the network require SSL inspection but not User authentication, and
- Guest Wi-Fi access should not have SSL inspection enabled due to privacy concerns

Centralized Management: Not only does the Aruba EdgeConnect and Zscaler integrated solution simplify WAN infrastructure at the branch, it is also centrally managed. With true zero-touch provisioning, all policies, including Gateway Options and location/sub-location rules, are defined once and pushed automatically to all sites. This provides the ability to deploy new policies quickly across hundreds or even thousands of sites in a matter of minutes.

Bringing new sites online or making policy changes or updates is equally easy. Centrally managed policy configuration and administration eliminates device-by-device configuration inherent to the discrete firewall model and minimizes the potential for human errors. The result is consistent, granular, end-to-end security policy enforcement.

Fully Automated Onboarding: Aruba and Zscaler have partnered to greatly simplify cloud- security service onboarding to automatically provision both IPsec and GRE tunnels using API automation Integrations. Fully automating tunnel configuration between EdgeConnect SD-WAN appliances and proximity-based ZIA Public Service Edge (formerly Zscaler Enforcement Node – ZEN) eliminates the time-consuming task of manually defining tunnels at every branch site. Location information from the Zscaler portal is "learned" by Aruba Orchestrator and used to connect branch sites to the closest primary and backup ZIA Public Service Edges (See Figure 3).

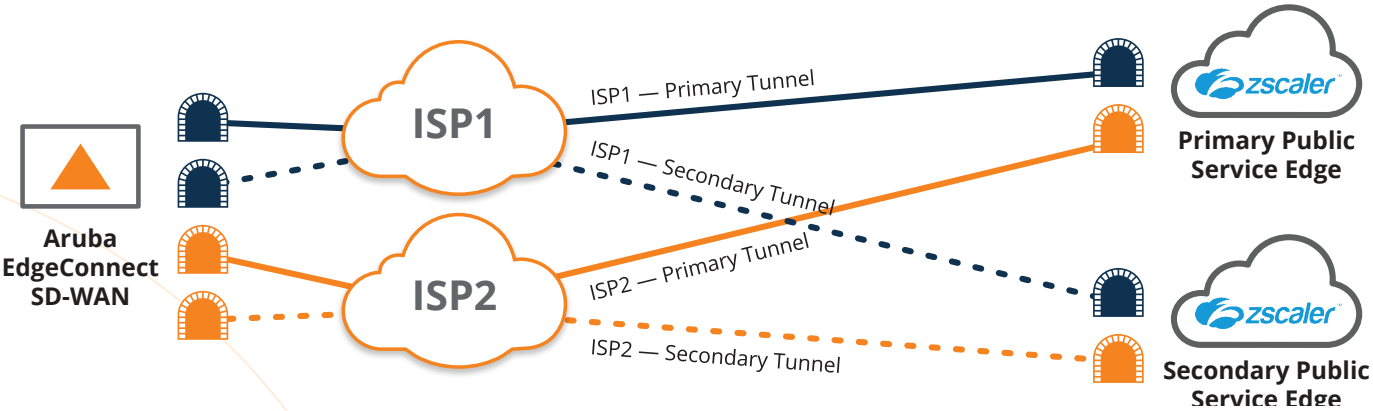

Figure 3. Continuous best path selection delivers highest SaaS quality of experience and 99.999% availability

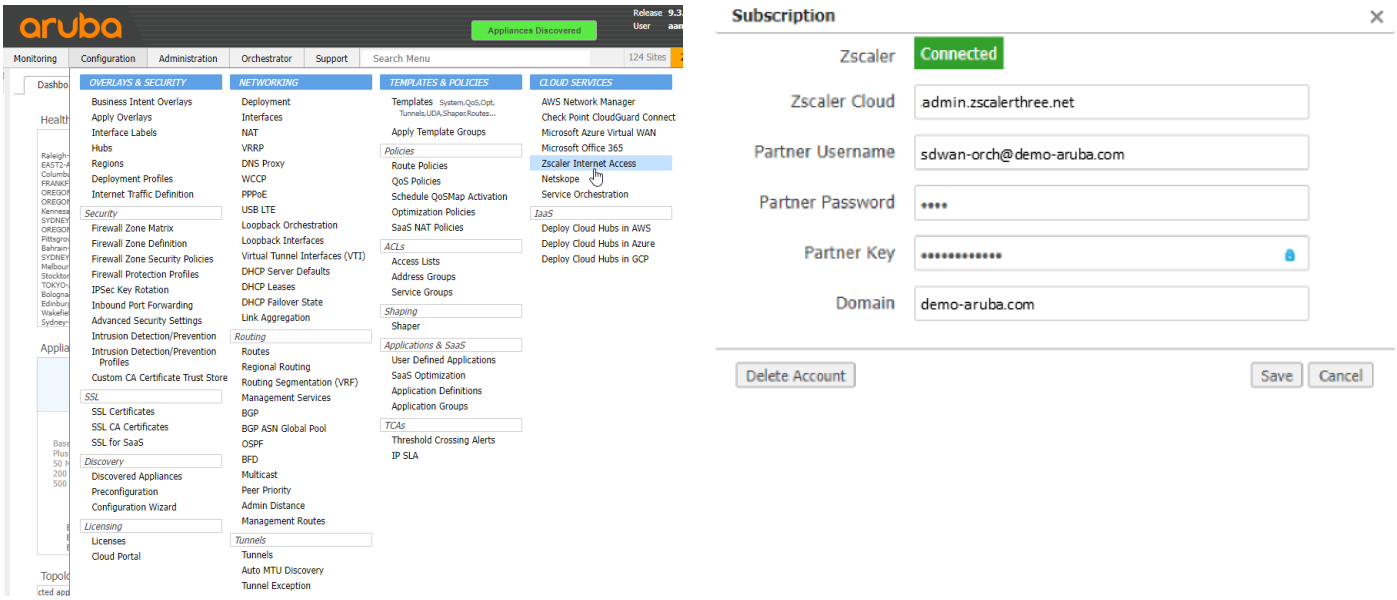

Figure 4. Zscaler subscription credentials entered into Orchestrator and validated

From the Aruba Orchestrator console, IT simply validates a company's Zscaler subscription credentials (See Figure 4) and selects branch locations to connect to ZIA Public Service Edges. The Aruba Orchestrator then automatically configures primary and optional secondary tunnels to the nearest primary and secondary ZIA Public Service Edge to each branch location, delivering the highest quality of cloud application performance. The IP SLA engine within each Aruba EdgeConnect appliance continuously monitors the health of every tunnel. This health check measures liveliness to specific test points within each ZIA Public Service Edge, automatically re-directing traffic to the backup node when necessary. If a new ZIA Public Service Edge closer to a branch site becomes available, the configured tunnels are updated automatically, ensuring that the Aruba/Zscaler solution continuously adapts to deliver the peak application performance for users. For specific needs, Zscaler subclouds can be set up to forward web traffic to a specific region instead of the nearest service edge. Organizations located near a border or for geopolitical reasons can use this service to redirect the traffic to another region.

The IT administrator then selects the application traffic to forward to ZIA Public Service Edges and simply "drags-and-drops" the preferred primary and secondary traffic handling policies into the configuration screen (See Figure 5); this is typically, all internet-bound traffic except whitelisted traffic, such as UCaaS. Future policy changes may be updated easily and pushed to all locations with a single mouse click in Aruba Orchestrator.

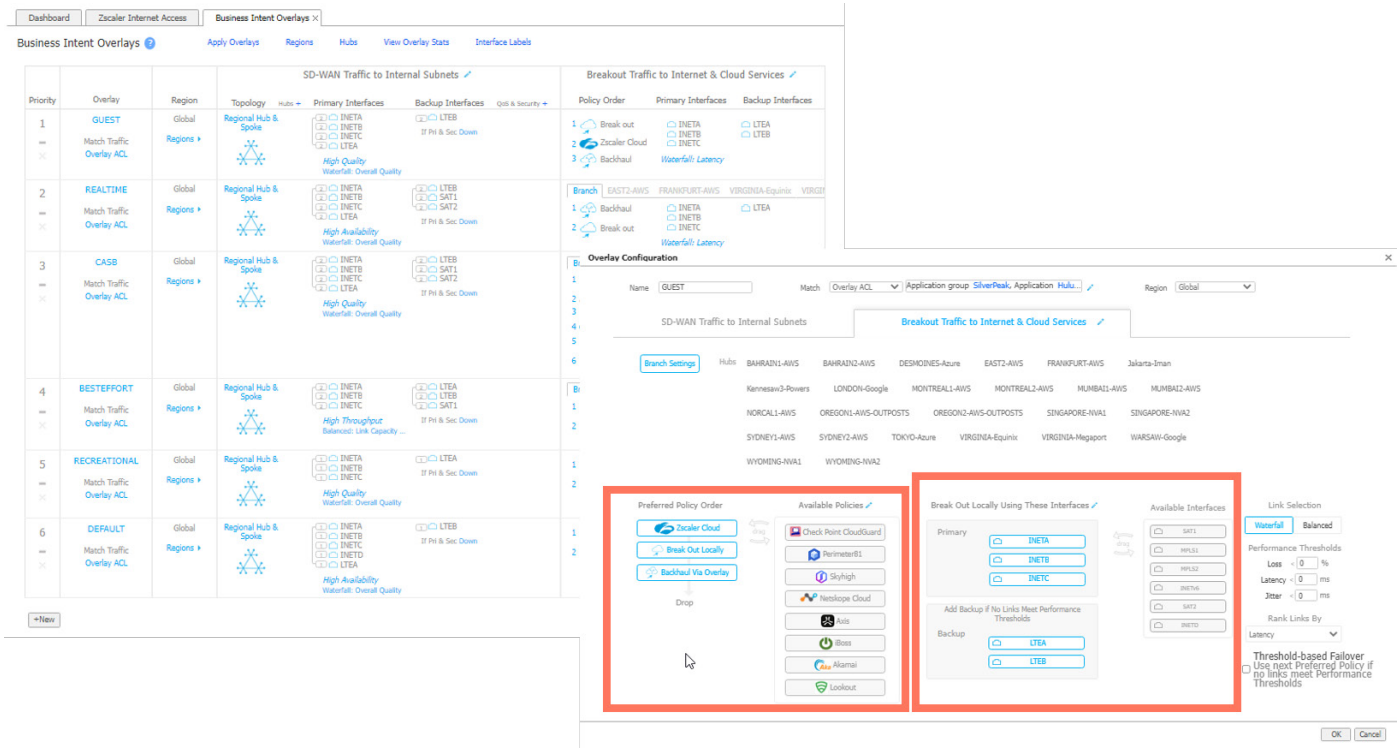

Figure 5. Preferred traffic handling policy order configured per traffic class

Aruba leveraged the Zscaler API to integrate and automate the process of connecting branch locations in the SD-WAN fabric to the closest primary and optional secondary ZIA Public Service Edges. With this integration, hundreds of sites can be automatically connected within minutes, generating significant IT OPEX savings (See Figure 6). The integration delivers the added benefit of consistent policy enforcement across the SD-WAN, defending the enterprise from threats and vulnerabilities.

ARUBA + ZSCALER = BETTER BUSINESS OUTCOMES

With the Aruba self-driving wide area network™ platform and Zscaler Cloud Security Platform, branches going direct to cloud can be provisioned and secured in minutes. Ultimately, enterprises can realize a multiplier effect from their existing and future cloud investments by delivering faster deployments, optimal performance and end user quality of experience from cloud applications, and secure SD-WAN connectivity that continuously adapts to changing business requirements.

For IT, that means lower costs and simplified operations. End users enjoy fast, secure and uninterrupted access to the business-critical applications they need.

- Provide a secure access service edge (SASE) architecture that delivers the full benefits of the cloud — greater business agility and simplified IT
- Streamline branch WAN and security infrastructure, eliminating the need for discrete routers and next-generation firewalls, and myriad on-premises devices, while enhancing security in a work-from-anywhere world
- Deliver fast, secure access to business-critical applications with 99.999% availability, increasing overall business productivity and user experience

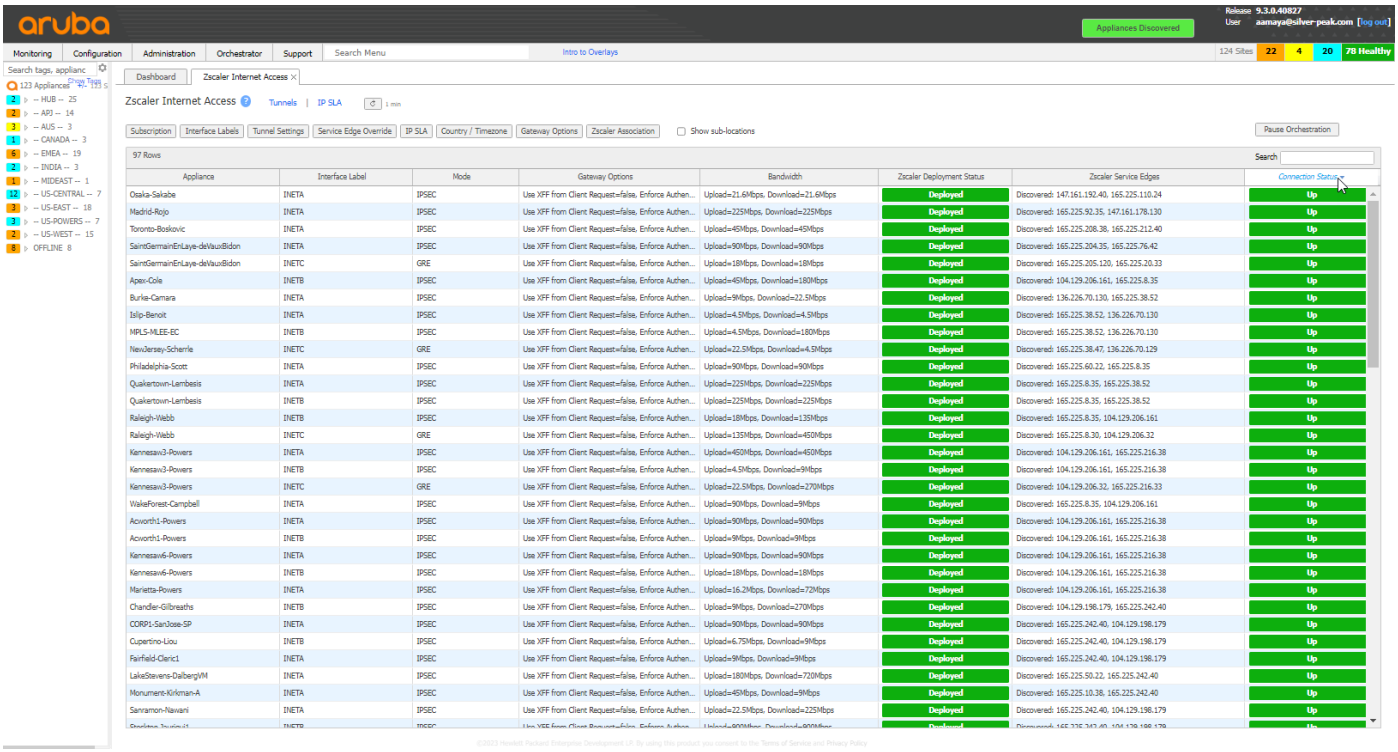

Figure 6. Within minutes, every SD-WAN branch location is automatically connected to the closest ZIA Public Service Edges

- Quickly add and secure new branches with automated deployments and true zero-touch provisioning, increasing business agility and accelerating time-to-revenue
- Make changes easier, minimize human errors and enable faster troubleshooting so that IT is more responsive to the business
- Centrally define security requirements once, and automatically deliver optimal security for employees, guests and IoT devices at every location
- Minimize risk by delivering customized, granular network segmentation and security policies based on business requirements
- Reduce the time required for troubleshooting network and application bottlenecks and for fielding support/helpdesk calls day and night
- Minimize dependence on high-cost MPLS services and eliminate costly security appliances
- Realize a multiplier effect on cloud investments by modernizing the WAN and security while delivering better performance reliability, control, and economics

ABOUT ZSCALER

Zscaler enables organizations to securely transform their networks and applications for a mobile and cloud-first world. Zscaler cloud-delivered services securely connect users to their applications and cloud services, regardless of device, location, or network, while providing comprehensive threat prevention and a fast user experience. All without costly, complex gateway appliances. Learn more at zscaler.com or follow us on Twitter @zscaler.

DEPEND ON ZSCALER

Zscaler enables organizations to securely transform their networks and applications for a mobile and cloud-first world. Zscaler cloud-delivered services securely connect users to their applications and cloud services, regardless of device, location, or network, while providing comprehensive threat prevention and a fast user experience. All without costly, complex security appliances.

Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

PSO_ArubaECandZscaler_RVK_030123 a00112611enw

Contact us at www.arubanetworks.com/contact