PARTNER BRIEF

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

Zscaler and Aruba automate optimal security policy enforcement for any user, application, or device across any location with true zero-touch provisioning.

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 the branch 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 enterprise, applications are hosted everywhere: the data center, in public and private clouds, or delivered by myriad Software-as-a-Service (SaaS) providers. Users access applications from anywhere, from any device and across diverse WAN transports, including broadband internet, further complicating the security model and the IT challenge. The proliferation of IoT devices adds additional security challenges for IT, and the dissolving enterprise security perimeter increases the attack surface, significantly increasing the need for advanced security services to protect enterprises from threats.

While enterprises could deploy next-generation firewalls at every branch, that model is untenable. The hardware is too expensive and deploying and managing dedicated security appliances at hundreds or thousands of branch locations requires extensive IT resources. In addition, application traffic originating from branch locations requires advanced security controls, like sandboxing, intrusion prevention (IPS) and Data Loss Prevention, as well as SSL inspection to defend against threats and vulnerabilities.

To address these security and cost challenges, centrally orchestrated cloud-hosted security services, such as those available from Zscaler™, have emerged and are experiencing hyper-growth. The Zscaler Cloud Security Platform complemented by the application-aware, business-driven Aruba Edge Services Platform (ESP) provides a powerful secure access services edge (SASE) solution that protects the enterprise from threats, delivers the highest application performance and user experience, and keeps costs in check.

CLOUD-FIRST ENTERPRISE SECURITY CHALLENGES

Unpredictable application performance
Inability to prioritize traffic and enforce business-driven security policies can rob performance from business-critical applications

Time-consuming, error-prone policy configurations delay deployments
Ever-changing cloud applications require constant manual reconfiguration of routers and firewalls at every location

Inconsistent policy enforcement
Maintaining consistent security policy definitions across hundreds or thousands of sites is arduous

SOLUTION BENEFITS

Ensure fast, secure access to business-critical applications
Prioritization of business-critical applications delivers the highest quality of experience to users

Accelerate deployments of new branch locations and applications
Centralized policy definitions and true zero-touch provisioning accelerate deployments of new branch locations and applications, and enable faster onboarding of mergers and acquisitions

Deliver consistent business and security policies globally to all users
Automated security and cloud application updates ensure optimal network and security policy enforcement across all locations

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 directly over the internet. However, this 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. Alternatively, an enterprise can deploy next-generation firewalls at every branch location, but that adds tremendous IT complexity and is cost-prohibitive.

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 the branch office. 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 agentless devices which interact with internet-based services.

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. Those 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 based on applications, users, locations and devices, all according to 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. Nearly a million new threats that compromise enterprise security are discovered daily.[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 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 typically takes 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.

Remediating WAN performance and security issues: The emergence of the cloud, coupled with increasing use of 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.

[1]https://www.webarxsecurity.com/website-hacking-statistics-2018-february/

Addressing these challenges requires a re-architecting of the WAN and WAN 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. By integrating comprehensive WAN capabilities with comprehensive network security 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 of digital enterprises. 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 Zscaler and Aruba, leaders in security and WAN edge infrastructure solutions, deliver a SASE architecture that uniquely addresses the evolving business needs faced by cloud-first enterprises today.

Secure WAN access with Zscaler and Aruba

Cloud-hosted security services, such as Zscaler Internet Access™, have emerged to provide a superior security alternative for cloud-first enterprises. Centrally managed and supporting a full security stack, including next-generation firewall, access control, IPS, sandboxing, UTM, URL filtering, DLP, CASB, remote browser isolation, and more, Zscaler delivers identical protection for all users and consistent policies and policy enforcement across hundreds or even thousands of sites — without any security appliances to buy, deploy or manage.

Cloud-hosted security services coupled with the application-aware, business-driven Aruba EdgeConnect SD-WAN platform streamline WAN edge infrastructure at the branch. Enterprises no longer need to deploy expensive, complex-to-manage next-generation firewalls at every branch location.

Granular security policy enforcement: Aruba 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 be as follows:

1. Send enterprise data center-hosted application traffic directly to headquarters
2. Send only UCaaS traffic directly to providers' cloud services
3. Send all other internet-bound traffic, including Salesforce, Facebook, YouTube, Box, and web browsing traffic to a ZIA Public Service Edge for security inspection prior to handing off to providers' cloud or web services

Application, user and device level control: With the Aruba and Zscaler API integration, organizations can specify a set of Zscaler security policies to be applied for branch locations. Occasionally, different security policy enforcement is required for specific applications, users, and devices within a branch location. The Gateway Options feature enables organizations to define exceptions for sub-locations (See Figure 1).

An enterprise might define the following policies:

1. Enterprise traffic requires SSL inspection
2. IoT devices accessing the network require SSL inspection but not user authentication
3. Guest Wi-Fi access should not have SSL inspection enabled due to privacy concerns

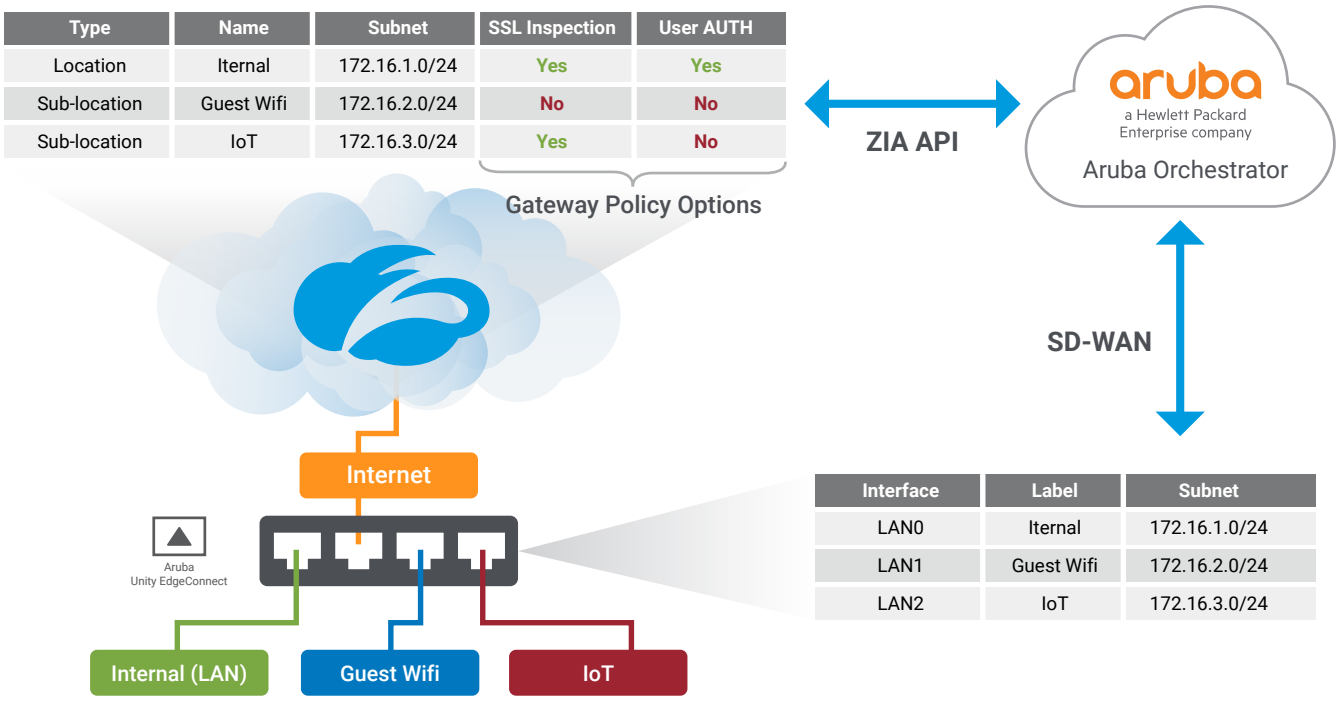

Figure 1: *Sub-location addresses and subnets mapped automatically to Zscaler Internet Access cloud-delivered security services, enabling IT to define unique security policies per sub-location.*

Centralized management: Not only does the Zscaler and Aruba integrated solution to 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: Zscaler and Aruba have partnered to greatly simplify cloud-security service onboarding. Fully automating IPsec tunnel configuration between Aruba EdgeConnect SD-WAN appliances and proximity-based ZIA Public Service Edge PoP eliminates the time-consuming task of manually defining IPsec 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 Edge PoPs (See Figure 2).

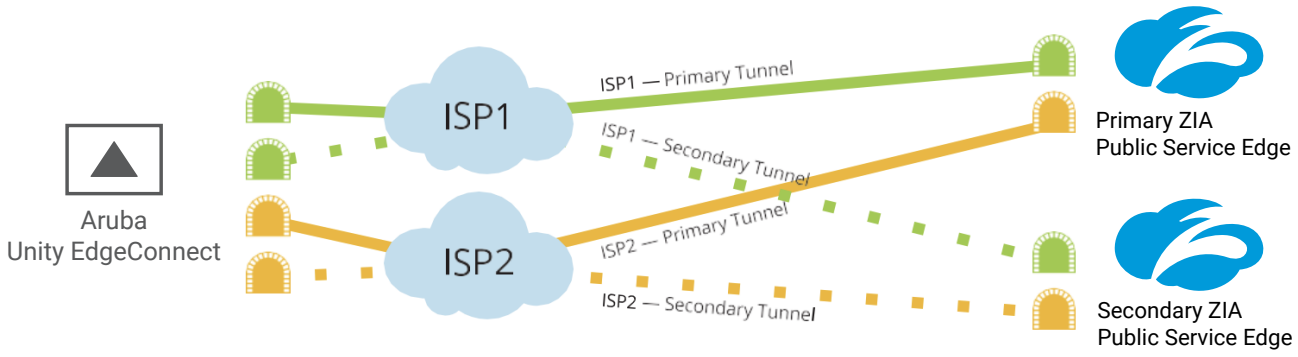

Figure 2: *Continuous best path selection delivers highest SaaS quality of experience and 99.999% availability*

From the Aruba Orchestrator console, IT simply validates a company's Zscaler subscription credentials (See Figure 3) and selects branch locations to connect to ZIA Public Service Edge PoPs. Orchestrator then automatically configures primary and optional secondary IPsec tunnels to the nearest primary and secondary ZIA Public Service Edge PoP to each branch location, delivering the highest quality of cloud application performance. The IP SLA engine within each EdgeConnect appliance continuously monitors the health of every IPsec tunnel. This health check measures liveliness to specific test points within each ZIA Public Service Edge PoP, automatically re-directing traffic to the backup node when necessary. If a new ZIA Public Service Edge PoP closer to a branch site becomes available, the configured tunnels are updated automatically, ensuring that the Zscaler/Aruba solution continuously adapts to deliver the peak application performance for users.

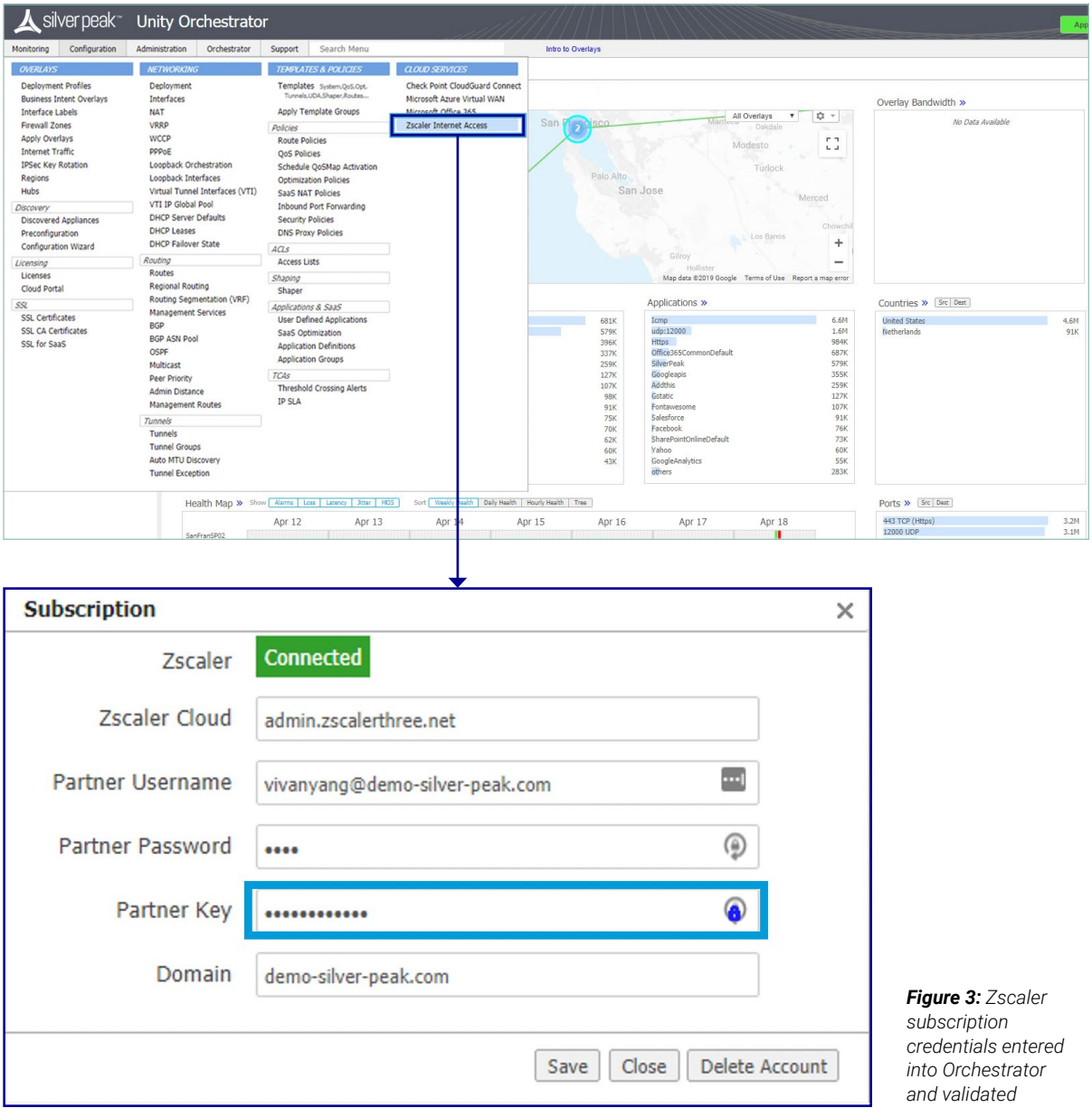

Figure 3: *Zscaler subscription credentials entered into Orchestrator and validated*

IT then selects the application traffic to forward to Zscaler ZIA Public Service Edge PoPs and simply "drags-and-drops" the preferred primary and secondary traffic handling policies into the configuration screen (See Figure 4); 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 Orchestrator.

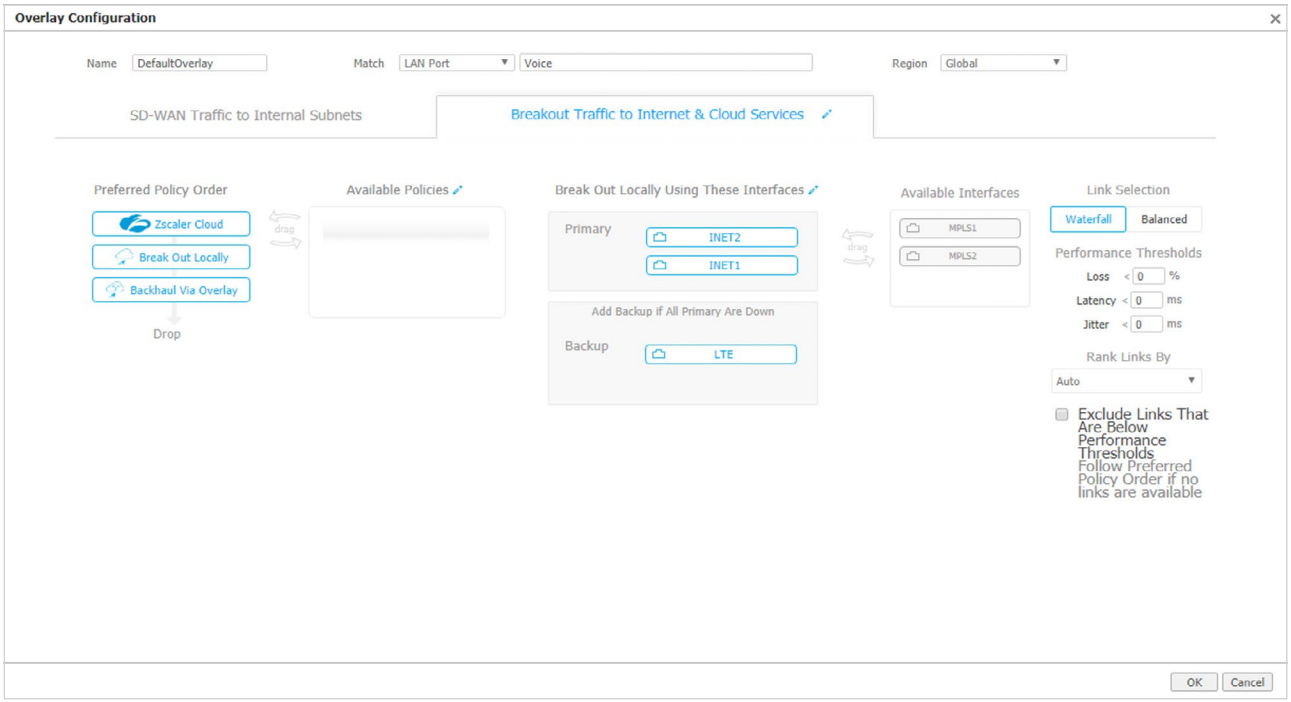

Figure 4: *Preferred traffic handling policy order configured per traffic class*

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 Edge PoPs. With this integration, hundreds of sites can be automatically connected within minutes, generating significant IT OPEX savings (See Figure 5). The integration delivers the added benefit of consistent policy enforcement across the SD-WAN, defending the enterprise from threats and vulnerabilities.

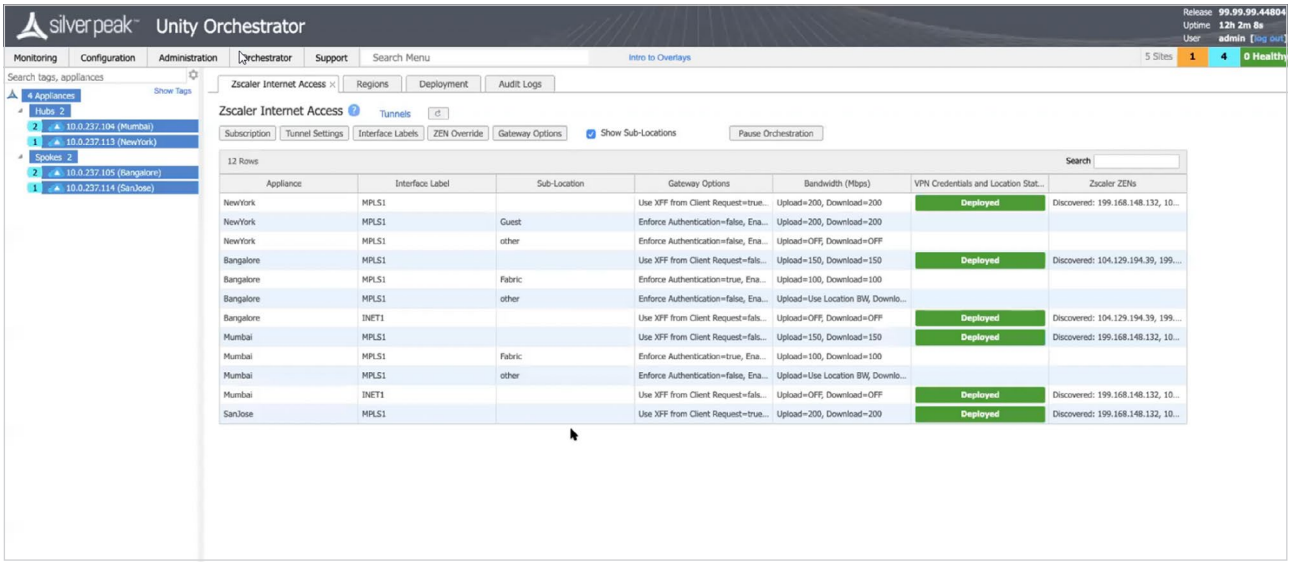

Figure 5: *Within minutes, every SD-WAN branch location is automatically connected to the closest Zscaler ZIA Public Service Edge PoPs*

In addition to enabling full automation for establishing IPsec tunnels to secure branch locations, the Aruba/Zscaler solution provides the flexibility to support major branch locations that require Gigabit speed bandwidth for internet-bound traffic. IT uses Aruba Orchestrator to centrally configure and monitor GRE tunnels between these locations and the closest primary and secondary ZIA Public Service Edge PoPs.

Zscaler + Aruba = better business outcomes

With the Zscaler Cloud Security Platform and Aruba self driving wide area network™, 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 services 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
- 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 devices at every location
- Minimize risk by delivering customized, granular network and security policies based on business requirements
- Reduce the time required for troubleshooting network and application bottlenecks and for fielding support/help desk 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 (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at zscaler.com or follow us on Twitter @zscaler.

About Aruba

Aruba, the global SD-WAN leader, delivers the transformational promise of the cloud with a business-first networking model. The Aruba EdgeConnect SD-WAN self-driving wide area network platform liberates enterprises from conventional WAN approaches to transform the network into a business accelerant. EdgeConnect replaces routers, unifying SD-WAN, firewall, segmentation, routing, WAN optimization and application visibility and control in a single platform. EdgeConnect continuously learns and adapts to meet the requirements of the business, delivering the highest quality of experience to enterprise users and IT organizations. Thousands of globally distributed enterprises have deployed Aruba WAN solutions across 100 countries. Learn more at arubanetworks.com.

zscaler™ / aruba a Hewlett Packard Enterprise company

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.com