Aruba and Zscaler automate 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 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. 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 the security and cost challenges, centrally orchestrated cloud-hosted security services, such as those available from Zscaler™, have emerged and continue to experience hyper-growth. The Zscaler Cloud Security Platform complemented by the application-aware, business-driven Aruba EdgeConnect SD-WAN edge platform, provides...
formerly Silver Peak, provides a powerful secure access services edge (SASE) solution that protects the enterprise from threats, delivers the highest application performance and user experience while keeping costs in check.

**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. 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 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. Nearly a million new threats that could 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 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.

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 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 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 WAN edge and security infrastructure solutions, enable customers to implement zero trust and SASE frameworks that uniquely addresses the evolving business needs faced by cloud-first enterprises today.

SECURE WAN ACCESS WITH ARUBA AND ZSCALER
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 buying, deploying or managing any physical security appliances.

Cloud-hosted security services coupled with the application-aware, business-driven Aruba EdgeConnect platform streamlines 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 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 only UCaaS traffic directly to providers’ cloud services
- Send all 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 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.
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 1). 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. Fully automating IPsec tunnel configuration between EdgeConnect SD-WAN appliances and proximity-based Zscaler Enforcement Node (ZEN) 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 ZEN PoPs (See Figure 2).

![Figure 2. Continuous best path selection delivers highest SaaS quality of experience and 99.999% availability](image2)

![Figure 3. Zscaler subscription credentials entered into Orchestrator and validated](image3)
From the Aruba Orchestrator console, IT simply validates a company’s Zscaler subscription credentials (See Figure 3) and selects branch locations to connect to ZEN PoPs. The Aruba Orchestrator then automatically configures primary and optional secondary IPsec tunnels to the nearest primary and secondary ZEN PoP 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 IPsec tunnel. This health check measures liveliness to specific test points within each ZEN PoP, automatically re-directing traffic to the backup node when necessary. If a new ZEN PoP 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.

The IT administrator then selects the application traffic to forward to Zscaler ZEN 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 Aruba Orchestrator.

In addition to enabling full automation for establishing IPsec tunnels to secure branch locations, the Aruba EdgeConnect/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 ZEN PoPs.
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 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

Figure 5. Within minutes, every SD-WAN branch location is automatically connected to the closest Zscaler ZEN POPs

- 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/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 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 gateway appliances.

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