Aruba SD-Branch and Zscaler automate security policy enforcement to deliver edge-to-cloud security for users and IoT connecting to SaaS and Cloud-hosted applications.

OVERVIEW

Security of the distributed enterprise network is a challenging, yet important task. As more organizations accelerate adoption of SaaS applications, many are implementing a Secure Access Service Edge (SASE) strategy to simplify their networks, strengthen their security, and improve end user quality of experience.

Critical to success when embracing to Zero Trust and SASE is the transformation of both WAN and security architectures with a cloud-first, secure and application-aware SD-WAN that makes it easy to protect users and IoT connecting to SaaS and public clouds. Aruba SD-Branch goes one step further to transform all aspects of branch LAN networking and security within the branch location and across the WAN.

SD-Branch, part of the Aruba Edge Services Platform (ESP), delivers edge-to-cloud security by addressing all layers of networking—wired, wireless, and WAN—and includes a comprehensive security portfolio across the unified network infrastructure. Connectivity spans from the access edge across the WAN and to the cloud with complete flexibility to deploy security services as required, both on-premises and integrated with best-of-breed cloud security solutions. This enables organizations to address the broadest range of security enforcement while moving to zero trust and SASE frameworks at their pace.

BETTER TOGETHER

Zscaler Internet Access (ZIA) is an industry-leading cloud-based security platform that provides a secure web gateway which can inspect every packet of network traffic coming from a branch for advanced threats – all done without additional hardware appliances. ZIA includes full inline content / SSL inspection, cloud-based sandboxing, DNS security and many more services. It is updated every day with more than 100,000 threat updates ensuring that users are protected from vulnerabilities using the latest techniques. These capabilities are delivered to Aruba SD-Branch customers from a global multi-tenant cloud-based management platform.

Aruba Branch gateways provide comprehensive threat protection with a user, device and application aware security policy enforcement firewall. It includes capabilities such as deep packet inspection, web content classification, IP reputation, and geo-location filtering as well as integrated IDS/IPS. These on premises security functions can be combined with the advanced Zscaler Internet Access security features to address a broad range of use cases with the branch gateway as the pivot point for centralized policy enforcement.

With the seamless integration of Aruba SD-Branch and Zscaler Internet Access, enterprises can easily deploy a complete edge-to-cloud security infrastructure, extending Zero Trust into a comprehensive Secure Access Service Edge (SASE) architecture.

WHY ARUBA SD-BRANCH AND ZSCALER

- Unified management of SD-LAN, SD-WAN with centrally managed security policy
- Policy-driven security segmentation augmented with AI/ML-driven device profiling
- Intelligent, policy-based traffic routing utilizing user and device roles and applications
- Orchestrated connectivity between SD-Branch Gateways and ZIA Public Service Edges
- Best of Breed cloud-delivered security with Advanced Threat Protection, SSL inspection, data protection, sandboxing, CASB and other security functions
ORCHESTRATED EDGE-TO-CLOUD SECURITY

Together, Aruba SD-Branch and Zscaler enable enterprises to implement edge-to-cloud security delivered from an automated, scalable, and cost-effective solution that protects users and IoT at the edge when connecting to SaaS and cloud-hosted applications.

This highly automated joint solution is designed to simplify IT operations while strengthening edge-to-cloud security by giving network and security administrators complete control to apply centralized security policy configuration that is enforced enterprise-wide. All tunnels, security policies and routing can be accessed and configured via Aruba Central, the centralized cloud-based platform for managing SD-Branch infrastructure. Aruba Central leverages Zscaler APIs to provision system attributes, query Zscaler for up-to-date node location information to ensure the SD-WAN overlay is always optimally distributed considering the dynamic nature of cloud points of presence and compliance constraints such as GDPR.

To get started, all that is required is a one-time setup on Zscaler to achieve following operational functions.

**Automatic onboarding into Zscaler Internet Access**

The Aruba Cloud Connect Framework reads “sites” defined in Aruba Central and automatically creates corresponding locations in ZIA (see Figure 1). It then uses Zscaler APIs to continuously monitor for any changes such as discovering new ZIA nodes. It also monitors the SD-Branch deployment. If a new gateway is added to a configuration group that is set to integrate with Zscaler, the whole discovery, site-creation, and tunnel-establishment process is performed automatically.

![Figure 1. Connecting Branch Groups to the Zscaler Public Service Edges](image)

**Tunnel Orchestration**

Once locations are defined and VPN credentials have been generated, the Aruba Cloud Connect Framework uses the SD-WAN Orchestrator to automatically build secure tunnels to Zscaler Internet Access enforcement nodes. It does so by obtaining public IP address and geo-location of each branch gateway and correlates that to the closest ZIA Public Service Edges. For example, a branch in Santa Clara, CA automatically establishes tunnels to ZIA Public Service Edges in San Francisco (primary) and Los Angeles (secondary). At the same time, a branch location in Bilbao, Spain would have its tunnels automatically established with ZIA Public Service Edges in Madrid (primary) and Paris (secondary).
**Policy Based Routing**

Once these tunnels have been established, SD-Branch Gateways can selectively redirect network traffic to these nodes based on identity (making use of Aruba user-roles) and application (leveraging Aruba DPI with first packet application classification). This rich user and application context, facilitates building policies to route traffic through the SD-WAN overlay, forward it directly to the internet, or send it via ZIA Public Service Edges for further security inspection and policy enforcement.

**ENTERPRISE-WIDE MANAGEMENT AND VISIBILITY**

Layers of security are implemented and managed with centrally managed security policies. Aruba Central provides unified management that includes wired, wireless, and SD-WAN edge configurations and security policies. It does so with interactive visibility dashboards, policy-based traffic optimization and AIOps features, built-in network and user-oriented troubleshooting tools. Network and security teams can centrally define and enforce network configurations and security policies across all branch sites. Changes are automatically pushed out across multiple branch locations resulting in a consistent user experience and consistent security enforcement at each branch.

Aruba Central gives NOC and SOC admins complete visibility from edge-to-cloud. See Figure 2 for the branch topology view with connectivity to Zscaler Internet Access nodes.

*Figure 2. Branch Network Topology View with Connectivity to Zscaler*
ZSCALER INTERNET ACCESS

Zscaler Internet Access delivers a security stack as a service from the cloud, eliminating the cost and complexity of traditional secure web gateway approaches (see Figure 3). By moving security to a globally distributed cloud, Zscaler brings the internet gateway closer to user for an optimal experience. It also simplifies security operations, as all capabilities are delivered from a global, multitenant cloud security platform and are operated from a single dashboard. Organizations can easily scale protection to users across all branch locations without the complexity of managing nextgen firewall equipment deployed at each location.

BUSINESS BENEFITS

With Aruba SD-Branch and the Zscaler Cloud Security Platform, any branch going direct to cloud can be provisioned and secured in minutes. Network and security teams are equipped with powerful LAN, WAN, and security tools providing control and visibility across their entire enterprise network. Delivering secure optimized experience for users at the edge as they access cloud and SaaS applications and services.

- **Eliminate the complexity of branch networks**
  Aruba SD-Branch encompasses each element within a branch – WLAN, wired, WAN, and security – to address all network connectivity needs

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

- **Enforce consistent business and zero trust security policies globally to all users**
  Automated branch security and cloud application updates ensure optimal network and security policy enforcement across all locations
SUMMARY
Aruba and Zscaler have taken the guess work out of protecting branch network operations and have partnered to provide an integrated SASE architecture that is automated, scalable, and cost-effective. Contact your local sales representative to see how Aruba and Zscaler deliver a comprehensive branch office infrastructure and security solution.

For more information on the Aruba SD-Branch solution, please visit: https://www.arubanetworks.com/solutions/SD-branch

For detailed technical information and installation instructions, please see this Tech Note located on the Aruba Support Portal: https://support.hpe.com/hpsc/doc/public/display?docId=a00087856en_us

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.