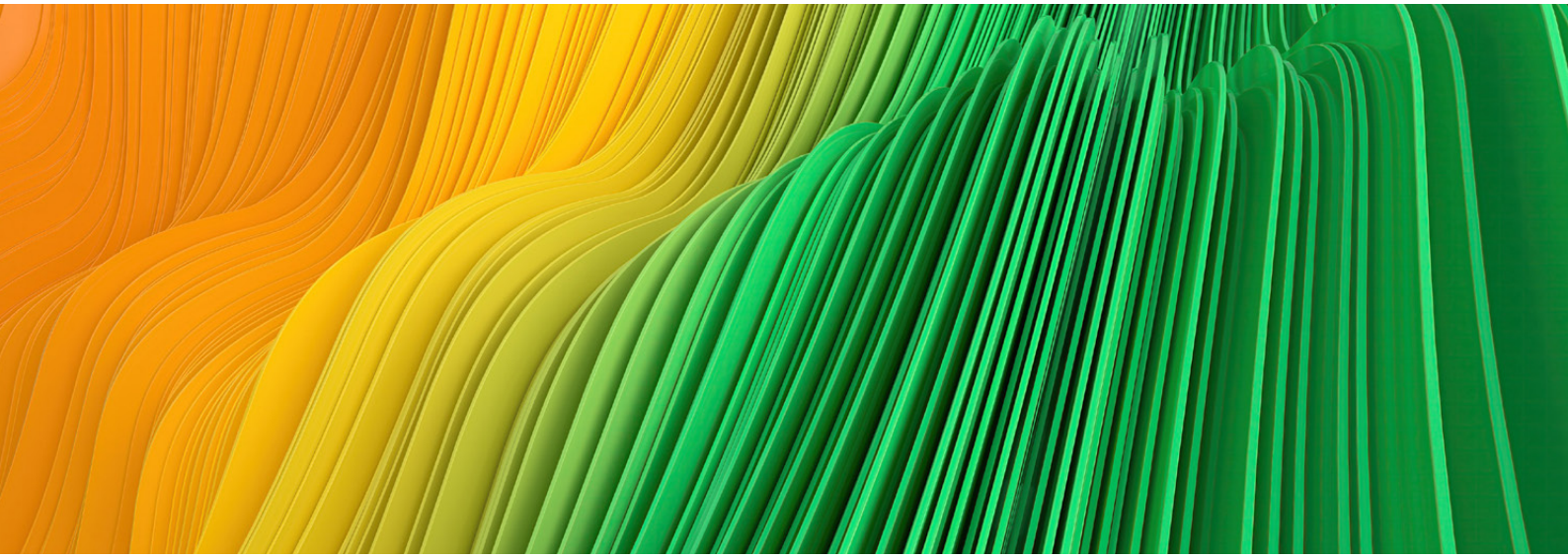
HPE aruba networking

HPE Aruba Networking EdgeConnect SD-branch and Zscaler

Scaling the branch: HPE Aruba Networking and Zscaler tackle branch security

HPE Aruba Networking EdgeConnect SD-Branch and Zscaler deploy a complete edge-to-cloud security infrastructure, extending Zero Trust into a comprehensive Secure Access Service Edge (SASE) architecture

Hewlett Packard Enterprise | zscaler



Why HPE Aruba Networking EdgeConnect SD-Branch and Zscaler

- Tightly integrated SASE architecture through API integration and automated orchestration between HPE Aruba Networking and Zscaler
- Advanced SD-WAN paired with best-in-class SSE capabilities such as SWG, CASB, RBI, sandboxing functions, and others
- Intelligent, policy-based traffic routing based on first packet application classification and user role
- Role-based segmentation using AI/ML-driven device profiling to augment SASE and secure IoT devices
- Unified management of SD-LAN, SD-WAN with centrally managed security policy in HPE Aruba Networking Central

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.

SASE combines advanced SD-WAN with Security Service Edge (SSE) capabilities. SSE includes cloud-security services such as SWG (Secure Web Gateway), CASB (Cloud Access Security Broker) and ZTNA (Zero Trust Network Access).

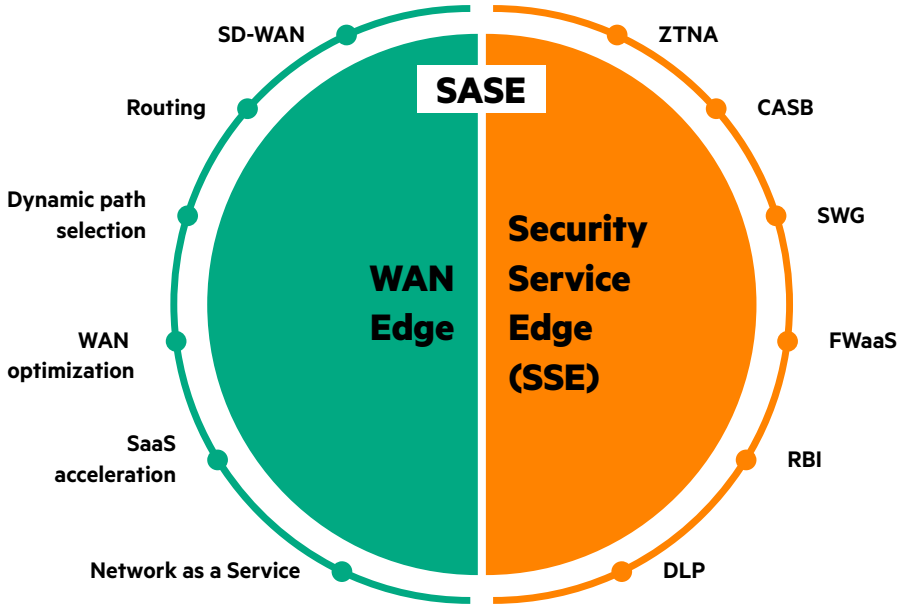


Figure 1. SASE is a network architecture that combines SD-WAN with Security Service Edge (SSE) capabilities

HPE Aruba Networking EdgeConnect SD-Branch, part of the HPE Aruba Networking 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.

Critical to success when embracing 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. HPE Aruba Networking EdgeConnect SD-Branch goes one step further to transform all aspects of branch LAN networking and security within the branch location and across the WAN.

Better together

Zscaler Internet Access (ZIA) is an industry-leading cloud-based security platform that provides SSE capabilities including Secure Web Gateway (SWG) which can inspect every packet of network traffic coming from a branch for advanced threats — all done without additional hardware appliances. ZIA also includes CASB (Cloud Access Security Broker), Data Loss Prevention (DLP), Remote Browser Isolation (RBI), cloud-based sandboxing, and more. 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 HPE Aruba Networking EdgeConnect SD-Branch customers from a global multi-tenant cloud-based management platform.

Additionally, EdgeConnect SD-Branch provides comprehensive threat protection using a role-based stateful firewall. It includes capabilities such as deep packet inspection, web content classification, IP reputation, and geolocation filtering as well as integrated IDS/IPS. Paired with HPE Aruba Networking ClearPass, it provides advanced Zero Trust role-based access control and dynamic segmentation, enabling organizations to isolate the network so that users and IoT devices can only reach destinations consistent with their role in the business.

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 SD-Branch as the pivot point for centralized policy enforcement.

With the seamless integration of HPE Aruba Networking EdgeConnect 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.

Orchestrated SASE architecture

Together, HPE Aruba Networking EdgeConnect SD-Branch and Zscaler enable enterprises to implement SASE 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 HPE Aruba Networking Central, the centralized cloud-based platform for managing SD-Branch infrastructure. HPE Aruba Networking 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.

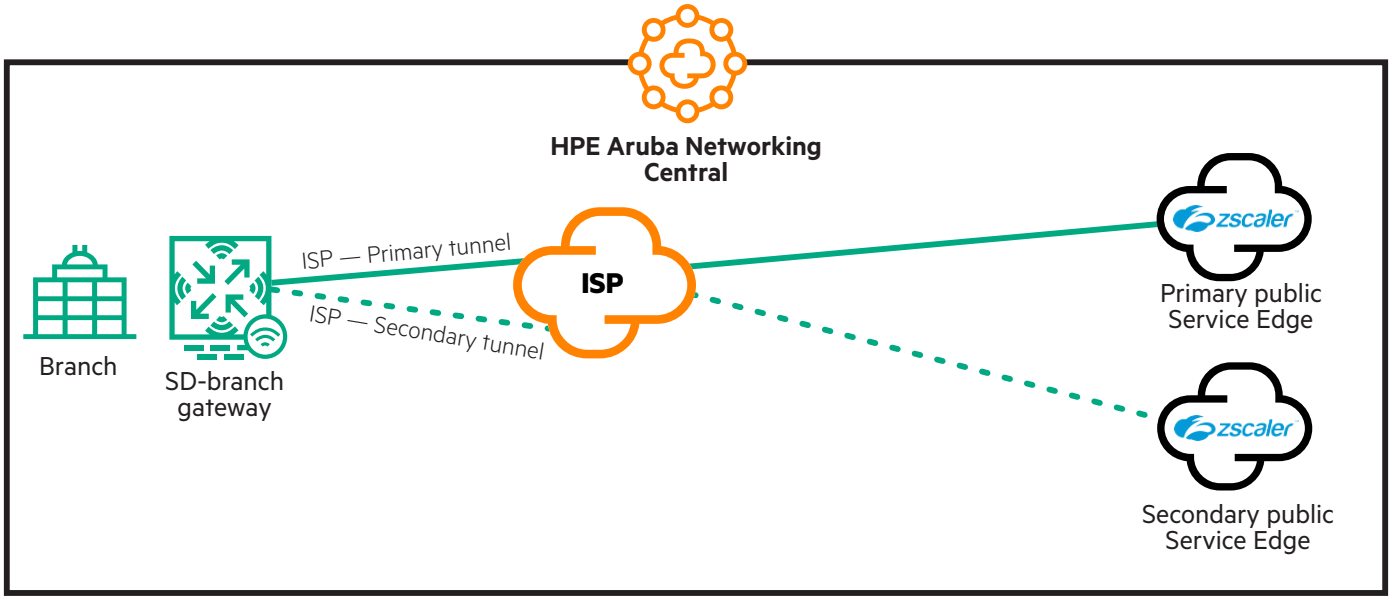


Figure 2. HPE Aruba Networking EdgeConnect SD-Branch automates orchestration to Zscaler

The Cloud Connect Service handles the tunnel establishment through automated orchestration between EdgeConnect SD-Branch Gateways and the nearest ZIA Public Service Edge. It does so by executing the following steps:

1. The SD-Branch Orchestrator queries the ZIA API for the nearest nodes (or ZIA Public Service Edges) for each EdgeConnect SD-Branch Gateway.

2. HPE Aruba Networking Central creates the "Locations" in ZIA for all gateways using the ZIA APIs. For organizations with a wide variety of users, HPE Aruba Networking Central can create sub-locations. For example, an organization can define a sub-location for its corporate network, and another sub-location for its guest network. By doing so, different policies can be implemented to different VLANs behind an SD-Branch Gateway.

3. Unique VPN credentials are also created for each Gateway.

4. HPE Aruba Networking Central instructs each Gateway to establish IPsec tunnels with the nearest two ZIA Public Service Edges using the VPN credentials that have been created.

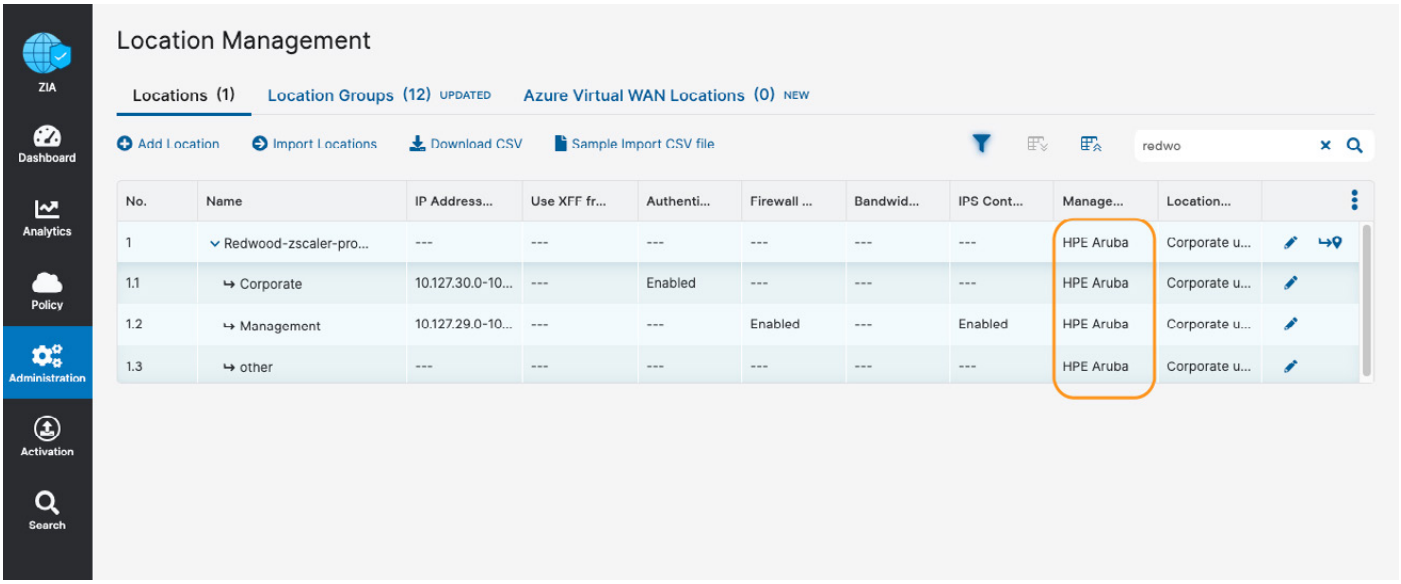


Figure 3. HPE Aruba Networking EdgeConnect SD-Branch gateway locations in Zscaler Internet Access

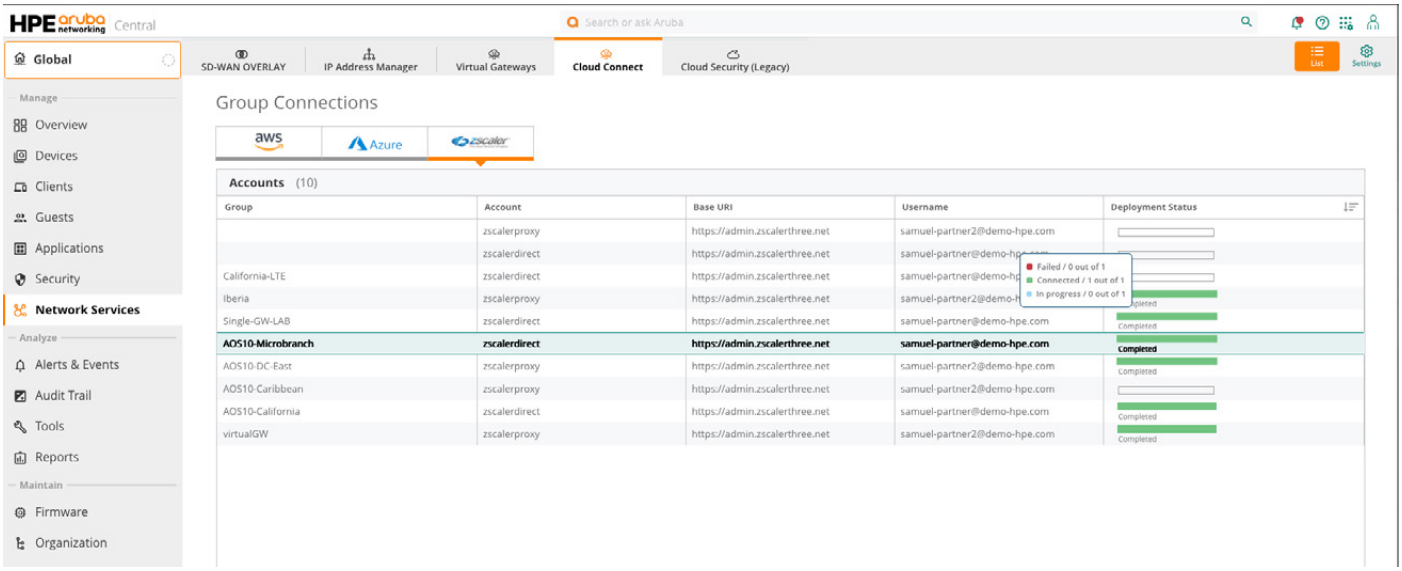


Figure 4. Connecting Branch Groups to the Zscaler Public Service Edges

Any changes are continuously monitored, such as new ZIA nodes by HPE Aruba Networking Central. The system 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.

In addition to enabling full automation for establishing IPsec tunnels to secure branch locations, network administrators can manually configure GRE tunnels to support major branch locations that require Gigabit speed bandwidth for internet-bound traffic.

Policy based routing

Once these tunnels have been established, SD-Branch Gateways can selectively redirect network traffic to Zscaler based on first packet application classification. Trusted applications such as Microsoft 365 or UcaaS can be directly sent to the cloud, while all other traffic is sent to Zscaler for security inspection.

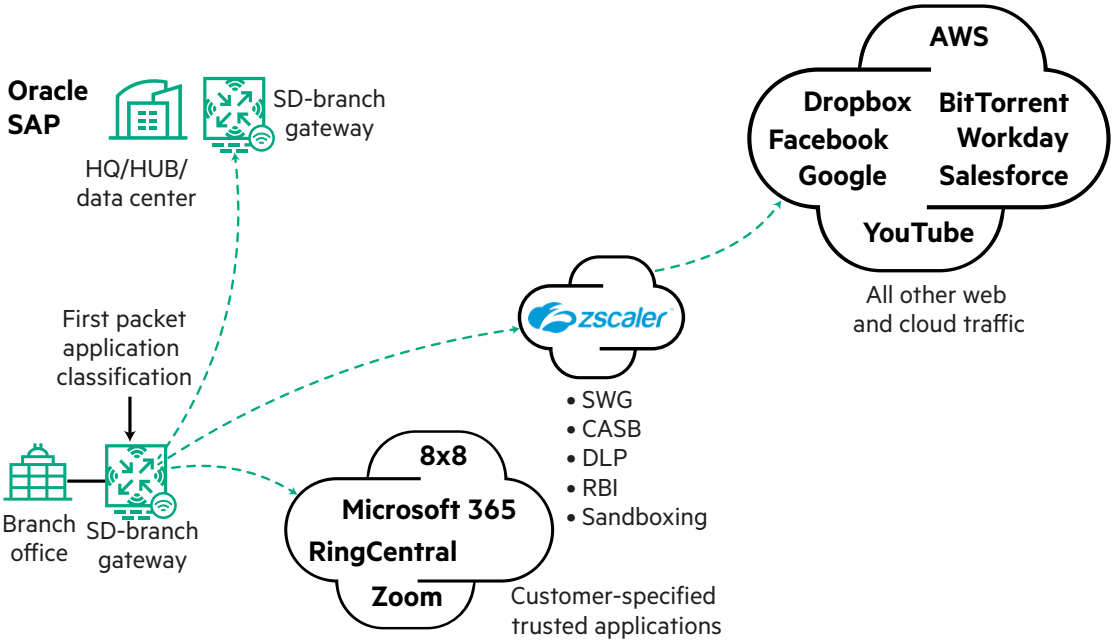


Figure 5. The cloud application traffic is automatically sent to Zscaler based on first packet application classification

Other policies can be used to route the traffic to Zscaler based on user role or firewall attributes (Protocol, source/destination address, source/destination port). An enterprise might define the following policies: cameras are full-tunneled to the data center, guest traffic is sent directly to the Internet, and Employees/IoT are sent to the Internet through the ZIA service with the exception of trusted SaaS applications.

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. HPE Aruba Networking 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 consistent user experience and consistent security enforcement at each branch.

HPE Aruba Networking Central gives NOC and SOC admins complete visibility from edge-to-cloud. See Figure 6 for the branch topology view with connectivity to Zscaler Internet Access nodes.

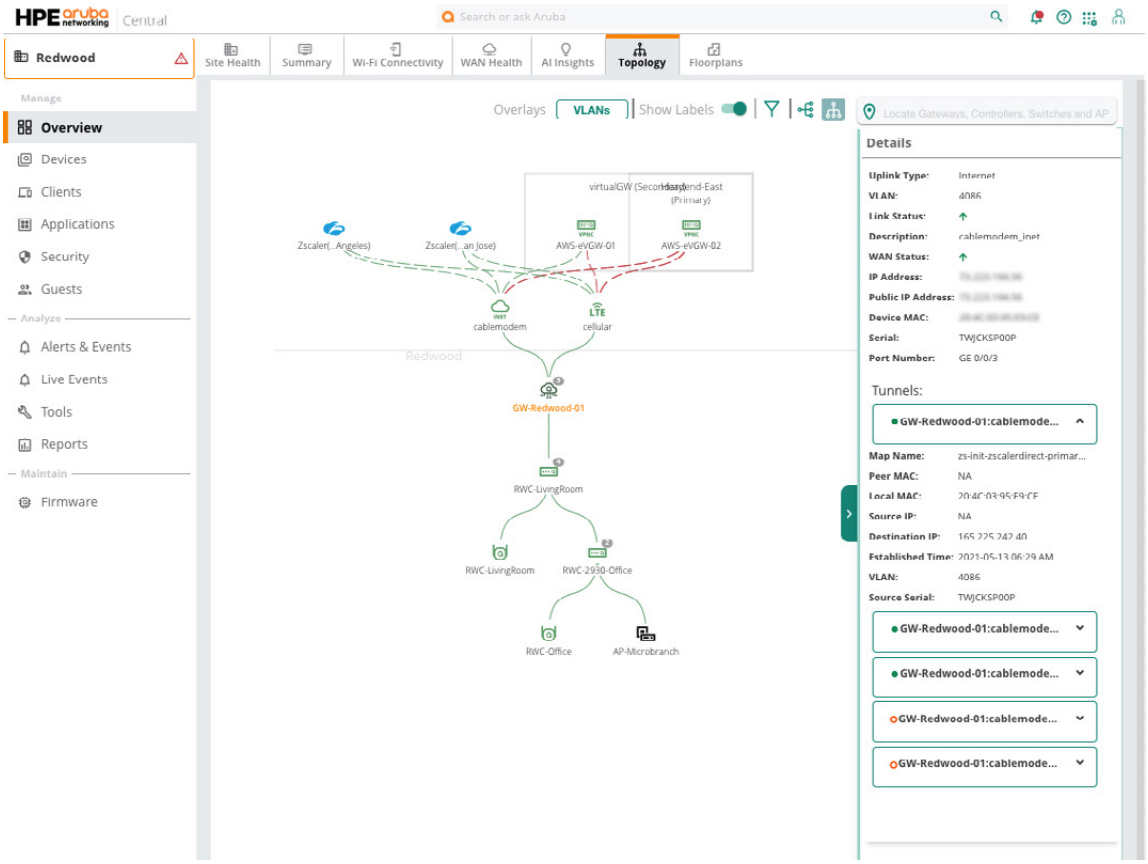


Figure 6. Branch Network Topology View with Connectivity to Zscaler

Business benefits

With HPE Aruba Networking EdgeConnect 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.

- **Implement end-to-end security**

  HPE Aruba Networking EdgeConnect SD-Branch and Zscaler Internet Access are tightly integrated, providing the full benefits of a SASE architecture. Additionally, SD-Branch is integrated with the HPE Aruba Networking wireless and wired infrastructure that are securely managed by the HPE Aruba Networking Central single platform.

- **Enforce consistent security policies globally to all users**

  Automated branch security updates ensure optimal policy enforcement across all locations.

- **Augment SASE with Zero Trust segmentation**

  SASE is complemented with a Zero Trust, identity-based access control security framework, segmenting traffic so that users and IoT devices can only reach network destinations consistent with their role in the business.

- **Eliminate the complexity of branch networks**

  HPE Aruba Networking EdgeConnect SD-Branch encompasses each element within a branch — WLAN, wired, WAN, and security — to address all network connectivity needs.

Our solution partners

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 X @zscaler.

- **Quickly deploy and secure new sites and applications**

  Centralized policy definitions and true zero-touch provisioning accelerate deployments and quickly secure new branch locations, enabling faster onboarding of mergers and acquisitions.

Summary

HPE Aruba Networking 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 HPE Aruba Networking and Zscaler deliver a comprehensive branch office infrastructure and security solution.

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

For detailed instructions on integrating Zscaler Internet Access (ZIA) with the HPE Aruba Networking EdgeConnect SD-Branch platform, please see this deployment guide.

Make the right purchase decision. Contact our presales specialists.

Contact us

Visit **ArubaNetworks.com**

Hewlett Packard Enterprise

PSO_SD-Branch-and-Zscaler_A4_RB_070224 a00114992ENW