netskope

aruba
a Hewlett Packard Enterprise company

SOLUTION BRIEF

Netskope with Aruba SD-WAN

Netskope and Aruba, a Hewlett Packard Enterprise company partner to provide scalable, secure branch, HQ and direct-to-net connectivity, with advanced data and threat protection for application users.

KEY USE CASES

- **Unencumbered safe connectivity to web and cloud applications:** Cloud-delivered SaaS solutions provide optimized application and data delivery for any user and location.
- **Security without compromising performance:** Global cloud infrastructure provides real-time, inline security defenses at scale, including Next-Generation Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), Data Loss Prevention (DLP), Zero Trust Network Access (ZTNA), and more.
- **Automated orchestration:** Centralized policy definitions and true zero-touch provisioning accelerate deployments of new branch locations and applications.
- **Secure Access Service Edge (SASE):** This framework enables a SASE architecture, based on integrated best-of-breed SD-WAN and cloud-delivered security services.

THE CHALLENGE

As applications migrate to the cloud, changing traffic patterns drive the need for a new approach to wide area network (WAN) and security architectures. When applications were hosted in enterprise data centers, branch traffic was backhauled with security primarily enforced at data center egress points. In today's modern enterprise, applications are everywhere: the data center, in public and private clouds, or delivered as Software-as-a-Service (SaaS). Users access applications from anywhere, from any device and across diverse transports, including broadband internet, further complicating the security model and creating IT challenges. The dissolving enterprise security perimeter expands the attack surface, significantly increasing the need for advanced data and threat protection services to mitigate exposure to threats.

NETSKOPE WITH ARUBA SD-WAN

While enterprises could deploy next-generation firewalls at every branch, that model is too costly to deploy and too complex to manage. To address the security and cost challenges, centrally orchestrated cloud-hosted security services, such as those available from Netskope, have emerged and continue to experience rapid adoption. The Netskope cloud-delivered security service, complemented by the application-aware Aruba EdgeConnect SD-WAN edge platform, recently acquired with Silver Peak, provides a powerful secure SASE solution. SASE protects the enterprise from threats and delivers the highest application performance and user experience while keeping costs in check.

CAPABILITIES

APPLICATION MIGRATION TO THE CLOUD COMPELS WAN AND SECURITY TRANSFORMATION

For many enterprises, migrating applications to the cloud presents a number of challenges. End-user application experience is influenced by latency, and thus, cloud-hosted applications perform better when the end user connects directly over the internet from the branch site. The traditional approach of backhauling all application traffic through an enterprise data center via an expensive MPLS connection only adds to the latency, degrading application performance and quality of experience. Adoption of local internet breakout to cloud-hosted (IaaS) and SaaS applications directly from branch locations not only optimizes available bandwidth but also reduces any latency that can negatively impact performance and user productivity.

The cloud-first paradigm calls for new methods to secure the access to hundreds or even thousands of cloud applications. Traditionally, when applications were hosted within the enterprise data center, guarding the enterprise against the unsafe internet was relatively straightforward with the deployment of expensive next-generation firewalls. But to deliver a high quality of experience for cloud-hosted applications, enterprises need a secure and high-performance network, built on a highly available foundation that can support local internet breakouts from the branch reliably while protecting the businesses from threats. Advanced SD-WAN solutions allow enterprises to intelligently break out cloud-destined traffic locally from branch sites over the internet. Additionally, the ability to support micro-segmentation capabilities and granular policy enforcement enables enterprises to secure their WAN, adhere to compliance mandates and defend against breaches. And with the comprehensive cloud-delivered security service from Netskope, the end user is protected when accessing cloud applications from remote branch locations. Together, Aruba and Netskope deliver a SASE architecture that uniquely addresses the evolving business needs faced by today's cloud-first enterprises.

Aruba EdgeConnect, integrated with cloud-hosted security services from Netskope, streamlines the WAN edge infrastructure at branch locations.

First-packet iQ enables application visibility and control

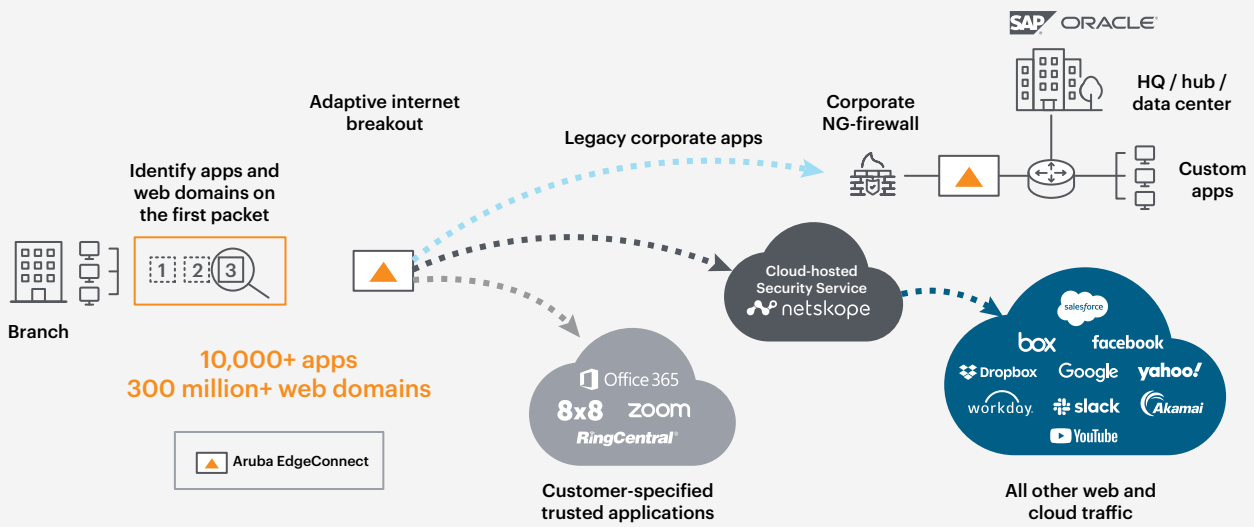

FIGURE 1: Netskope security cloud integration with the Aruba Aruba EdgeConnect SD-WAN

SECURE WAN ACCESS WITH ARUBA AND NETSKOPE

Cloud-hosted security services, such as Netskope, have emerged to provide a superior security alternative for cloud-first enterprises. Centrally managed cloud-delivered security services supply protection for all users, supported by consistent policies and policy enforcement across hundreds or even thousands of sites—without buying, deploying or managing any physical security appliances.

Aruba First-packet iQ application classification technology automatically identifies more than 10,000 SaaS applications and 300 million web domains on the first packet, enabling granular traffic steering and security policy enforcement. For instance, a business-driven security policy may:

- Send data center–hosted application traffic back to headquarters across MPLS
- Send trusted SaaS traffic, like unified communications as a service (UCaaS), directly to the SaaS provider across the internet
- Send all other internet-destined traffic, such as Box, Salesforce and web browsing, to the Netskope cloud-delivered security service for security inspection prior to handing off to the providers' cloud

Ensuring SaaS performance over the internet is far more complicated than conventional applications that run over your MPLS or private network. The challenge is that even if IT managers can identify the SaaS application, they may be unable to improve its performance since network performance is critical to SaaS, and the internet does not provide the same level of SLAs as MPLS services. Through the Silver Peak acquisition, Aruba provides a number of advanced features that optimize SaaS application performance over the internet including: cloud intelligence, efficient DNS query resolution, intelligent internet breakout, intelligent cloud breakout, O365 integration, and support for custom-defined applications.

SCALABLE, COMPREHENSIVE BUSINESS CONNECTIVITY AND SECURITY

The Aruba EdgeConnect SD-WAN edge platform streamlines the WAN edge infrastructure at branch locations. The Aruba EdgeConnect platform provides optimal networking services by delivering high-performance, reliable access to public cloud services, private data centers, and SaaS-based enterprise applications for branch offices, headquarters and users. Integration with the Netskope security cloud provides complementary security services, including a next-generation SWG, an advanced CASB, both with API-enabled and inline protections, as well as comprehensive data and threat protection for users, applications and data on any device and location. These security services are all managed from a single console with unified policy controls and intuitive reports and dashboards for SaaS, IaaS and web environments. The converged Aruba and Netskope solution delivers the promise of the SASE architecture: a thin branch WAN edge with comprehensive cloud-delivered security and management.

The Aruba EdgeConnect SD-WAN edge platform supports physical and virtual appliances that deliver consistent, highly available application performance, even for latency-sensitive applications such as voice and video. Aruba EdgeConnect appliances connect to build an SD-WAN fabric and communicate via secure IPSec tunnels to one another as well as the Netskope security cloud.

Branch offices connect to the enterprise data center to access on-premises data center–hosted applications and route to the Netskope NewEdge network infrastructure when accessing cloud applications and services. Similarly, headquarters-based application traffic traverses the SD-WAN fabric for branch access and is routed through the NewEdge network infrastructure when accessing cloud apps. Aruba EdgeConnect continuously monitors the entire SD-WAN fabric and underlying WAN transport services and automatically adapts to changing conditions to deliver optimal application performance, even when network changes, congestion or impairments occur.

SIMPLIFIED DEPLOYMENT FOR BRANCH SITES OR REMOTE WORKERS

From the Aruba Orchestrator, IT can configure tunnels from each branch site to the NewEdge network, where the Netskope cloud-delivered security service applies granular security controls and advanced data and threat protection. IT centrally defines the business-driven policies that dictate how applications are delivered across the SD-WAN fabric from Aruba Orchestrator. From a single pane of glass, IT can quickly define QoS policies, failover prioritization and service chaining to third-party network and security services, such as Netskope. Aruba Orchestrator also provides historical and real-time dashboards displaying a wealth of metrics for network health, application and network performance, WAN transport service performance and more.

Remote users outside of the Aruba SD-WAN fabric connect directly to the Netskope Security Cloud via encrypted SSL/TLS communications for the aforementioned security protections. Remote workers using corporate or managed devices are assigned the lightweight Netskope Client, which provides several key functions: it steers all traffic to the Netskope cloud, it delivers consistent notifications to end users for coaching and guidance purposes when users violate a policy, and it can provide the identity of the user with no additional setup needed by the customer. Remote workers in branch offices or those using their own personal or unmanaged devices such as in organizations supporting bring your own device (BYOD) would be directed to Netskope via its reverse proxy functionality where subsequent security controls would be applied. The reverse proxy is also used in situations where the client device is not using the Netskope client.

Together, Aruba and Netskope simplify and streamline the integration of cloud-native security functions with optimized SD-WAN capabilities. Aruba and Netskope fulfill and support the Gartner SASE design philosophy in which cloud-managed network services (e.g., WAN optimization, acceleration, QoS, dejitter, segmentation and basic stateful firewall) are combined with cloud-native, converged single-pass security controls (e.g., CASB, SWG, DLP, ZTNA) to offer organizations a highly scalable, fast and secure environment that protects users and data no matter where they are.

BEST-OF-BREED ECOSYSTEM PARTNERS

Aruba's Technology Partner Programs comprise an ecosystem of hundreds of technology vendors with which Aruba has worked to ensure interoperability across Aruba's networking, security, cloud, and location-based infrastructure. This means that our customers are able to use best-of-breed solutions and know that they integrate seamlessly with Aruba's portfolio to ensure secure connectivity in any environment.