aruba
a Hewlett Packard Enterprise company

PARTNER SOLUTION OVERVIEW

Aruba and Netskope

Partnering to deliver an automated Secure Access Service Edge (SASE)

Aruba and Netskope partner to provide scalable, secure branch, HQ and direct-to-net connectivity, with advanced data and threat protection for application users

As enterprises accelerate the migration of applications to the cloud, changing traffic patterns are driving the need to transform wide area network (WAN) and security architectures. When applications were hosted in enterprise data centers, 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 cloud-first 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 dissolving enterprise security perimeter expands the attack surface, significantly increasing the need for advanced data and threat protection services to mitigate exposure to threats.

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 and context-aware, business-driven Aruba EdgeConnect SD-WAN edge platform provides a robust, secure access services edge (SASE) architecture. This best-of-breed SASE architecture protects the enterprise from threats while providing the ability to apply granular-level, identity-based security policy from edge-to-cloud to safely connect and protect users, devices, and applications.

KEY BENEFITS OF ARUBA AND NETSKOPE SOLUTION

- **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, 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 and enable faster assimilation of mergers and acquisitions.
- **Simplified management:** Netskope console enables security operations while Aruba Orchestrator enables network operations for branch connectivity
- **Secure Access Service Edge (SASE):** Enables a SASE architecture, based on integrated best-of-breed SD-WAN and cloud-delivered security services.
- **Granular identity-based security policies:** Integrating ClearPass Policy Manager with the Aruba EdgeConnect SD-WAN edge platform augments application intelligence by adding identity knowledge of users, devices, roles, and security posture providing a comprehensive zero trust security architecture.
- **Advanced intrusion detection and prevention (IDS/IPS):** Aruba EdgeConnect leverages the Aruba threat infrastructure to deliver complete visibility across the enterprise network. Advanced unified threat management (UTM) capabilities enable enterprises to provide east-west lateral security as well as secure local internet breakout from branch locations.

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 impacted 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 end user 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 high-performance, secure network, built on a highly available foundation that can support local internet breakout from the branch reliably while protecting the business from threats. An advanced SD-WAN solution enables enterprises to intelligently break out cloud-destined traffic locally from branch sites over the internet. Additionally, the ability to support micro-segmentation and granular policy enforcement provides enterprises with the ability 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.

EDGE-TO-CLOUD SECURITY 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 deliver 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

First-packet iQ enables application visibility and control

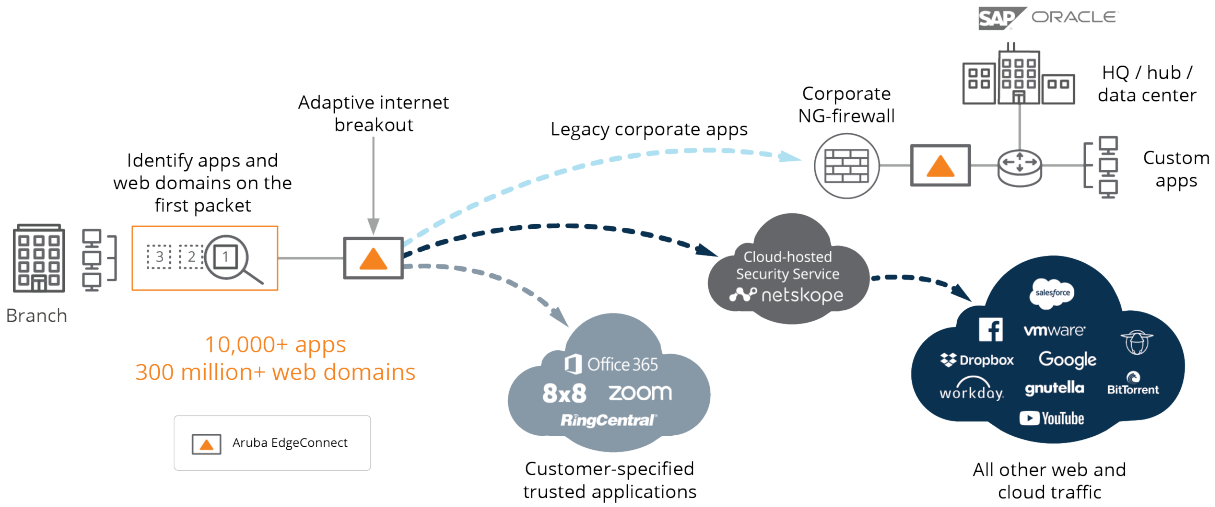

Figure 1: First-packet iQ application identification and classification enables granular traffic steering to enforce application- specific QoS and security policies.

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 include:

- Send data center-hosted application traffic back to headquarters across MPLS
- Send trusted SaaS traffic, like 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 it is for conventional applications that run over MPLS or a 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. 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
- Support for custom-defined applications

SCALABLE, COMPREHENSIVE BUSINESS CONNECTIVITY AND SECURITY

The Aruba EdgeConnect SD-WAN edge platform streamlines 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

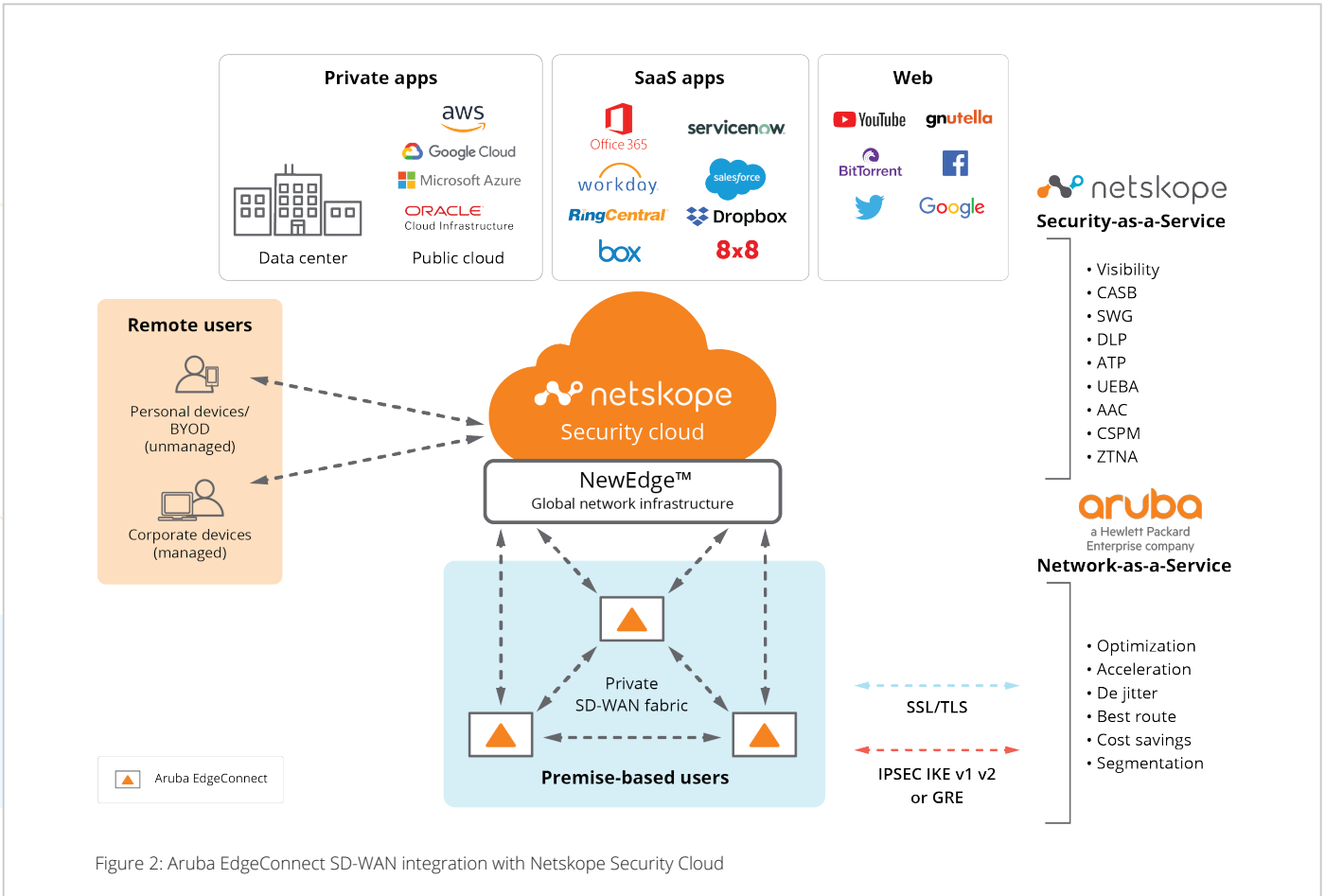

Figure 2: Aruba EdgeConnect SD-WAN integration with Netskope Security Cloud

managed from a single console with unified policy controls and intuitive reports and dashboards for SaaS, IaaS, and web environments. The integrated 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 to the Netskope Security Cloud.

Branch offices connect to the enterprise data center to access on-prem data center hosted applications and route to the Netskope NewEdge network infrastructure (a global network infrastructure that enables Netskope Security Cloud to deliver real-time security without the traditional security and performance trade-off) 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.

From the Aruba Orchestrator, IT can configure tunnels from each enterprise branch site location to the NewEdge network infrastructure, 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 quality of service (QoS) policies, failover prioritization and service chaining to third-party network and security services, such as the Netskope Security Cloud. Aruba Orchestrator also provides historical and real-time dashboards displaying a wealth of metrics for network health, application performance, 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 whereby the aforementioned security controls are applied. 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 Security 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 the Netskope Security Cloud via its reverse proxy functionality where subsequent security controls would be applied. The reverse proxy also is used in situations where the client device is not using the Netskope Client.

Together, Aruba and Netskope provide comprehensive edge-to-cloud security that fulfills and supports the Gartner Secure Access Service Edge (SASE) design philosophy in which cloud-managed network services (e.g. SD-WAN, routing, segmentation, IDS/IPS, zone-based stateful firewall and WAN optimization) are combined with cloud-native, converged single-pass security controls (e.g. CASB, SWG, DLP, ZTNA) to offer organizations with a highly-scalable, fast and secure environment that protects users and data no matter where they are.

ABOUT NETSKOPE

The Netskope Security Cloud provides unrivaled visibility and real-time data and threat protection when accessing cloud services, websites, and private apps from anywhere, on any device. Only Netskope understands the cloud and takes a data-centric approach that empowers security teams with the right balance of protection and speed they need to secure their digital transformation journey. Reimagine your perimeter with Netskope. For more information, visit www.netskope.com.

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.

DEPEND ON NETSKOPE

netskope

The Netskope Security Cloud provides unrivaled visibility and real-time data and threat protection when accessing cloud services, websites, and private apps from anywhere, on any device.

CONTACT US TODAY, SO WE CAN START BUILDING YOUR CUSTOMIZED CLOUD NETWORKING SOLUTION.

www.netskope.com Phone Number: +1(800) 979-6988 2445 Augustine Dr, 3rd Floor Santa Clara, CA 95054

aruba
a Hewlett Packard Enterprise company

© Copyright 2021 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

PSO_ArubaandNetskope_RVK_051421 a00112330enw

Contact us at www.arubanetworks.com/contact