aruba
a Hewlett Packard Enterprise company

AT A GLANCE

KEY SD-WAN USE CASES

Simplifying management of wide area networks

The transition to cloud-based services is fundamentally changing the way branch wide area networks (WANs) are being architected. As end-users, IoT and BYOD devices at distributed sites are accessing Internet-based applications, organizations are seeking better ways to improve end-user experiences and IT operations.

For engineers responsible for the WAN, the interim solution has been to supplement existing WAN connections (or uplinks) with affordable Internet connections such as high-speed broadband or DSL. However, the lack of a unified management solution means that additional moves, adds, and changes are required for each new uplink added to the network.

To better support today's digital transformation along with evolving performance and quality of service traffic demands, Aruba's SD-WAN solution offers enhanced traffic visibility, automated route orchestration and consistent security policies. This guide focuses on three common use cases where Aruba's SD-WAN solution can help.

WHAT IS SD-WAN?

Software-defined WAN (SD-WAN) technology is primarily a cloud-based management solution to increase an organization's ability to simply and better manage routing traffic over MPLS, broadband and cellular connections, while also reducing costs. A unified view into the performance and health of each WAN uplink and advanced features such as Dynamic Path Steering and Policy-based Routing to optimize and direct traffic are also included.

USE CASE #1: ENABLING THE TRANSITION TO THE CLOUD

Problem: Corporate Resources Are Hosted Outside the Network Perimeter

Cloud services, such as unified communications (UCC) and Internet-based software-as-a-service (SaaS) applications are delivering many benefits that are recognized by IT and end users. The IT organization is no longer responsible for ongoing software updates, upgrades and maintenance tasks. Users gain the ability to choose between web and mobile apps that are easy to use, from anywhere.

But this migration has introduced security and risk implications as corporate traffic now bypasses the corporate data center and goes directly to the cloud. This potentially exposes sensitive data to malicious users, as well as exposing employees to an increased number of cyber-attacks.

Solution: Design the Network to Extend to the Public Cloud

By deploying Aruba's SD-WAN gateways at each branch, IT can gain new levels of insight into multiple points of egress – from inside the branch, from public cloud infrastructure, and from the Internet.

In the branch, a built-in user and application-aware firewall allows IT to dynamically steer traffic over the appropriate WAN connection based on the roles of employees, guests or even IoT devices. This makes it easy to prioritize applications such as Office365 to travel over preferred links, while traffic generated by guests are routed down a best effort-designated link.

The use of an Aruba Virtual Headend Gateway allows IT to securely connect branch networks directly to applications hosted public cloud infrastructure (e.g. Azure or AWS). Unlike traditional SD-WAN vendors, Aruba provides full orchestration – which includes: deployment, configuration, routing, WAN health-checks, and troubleshooting. This means that IT can reduce the amount of configuration they need to perform in their VPC or VNET environments.

And finally, to secure traffic destined for the public Internet, Aruba SD-WAN includes web content filtering/classification that allows IT to create policies based on a site's reputation and risk score. For added protection there is also the ability to easily integrate with third-party web security gateways such as Palo Alto Networks, ZScaler, and Check Point.

USE CASE #2: OPTIMIZING BRANCH WAN PERFORMANCE

Problem: Perceived Reliability of Internet Connections

Private WAN connections such as MPLS provide enterprises with unparalleled performance through guaranteed SLAs, and adherence to corporate security policies. However, in part due to the rise in public cloud services, the market for MPLS is declining because organizations are capitalizing on the benefits of widely available and more affordable public broadband connections.

But even as enterprises are supplementing their MPLS connections with broadband/DSL (e.g. hybrid WAN), they still consider the public Internet too risky from a performance standpoint – despite potential cost savings of up to 100 times the cost of MPLS.

Solution: WAN Health-Based Monitoring and Steering

By adding the ability to measure and see WAN health across every uplink in a branch, IT can now better control traffic behavior and improve the reliability of broadband connections. The ability to leverage context such as user role, Layer 7 application visibility and dynamic path steering can be used for granular routing policies that improve network performance and utilization. Factors such as real-time health insight also minimize disruption to the network. For example, if the minimum threshold for latency, jitter, or packet loss is reached, traffic can be re-routed over a secondary uplink – ensuring minimal impact to end-users.

USE CASE #3: SIMPLIFYING WAN MANAGEMENT

Problem: The Traditional Way to Configure Networks Doesn't Scale

Traditional WAN infrastructure is made up of multiple pieces of on-premises hardware (e.g. a router, WAN optimizer, firewall) and a varying number of WAN connections that are all managed separately. What this means is that every new or ongoing move, add, or configuration change will require a truck roll in every branch network. As more mobile and IoT devices, cloud applications, and social media are being used, the ability for IT to maintain visibility, make changes and quickly resolve issues is untenable.

Solution: Centralize Visibility And Control

By introducing a single pane of glass to manage a WAN environment, as well as Wi-Fi and wired infrastructure, organizations can reduce their reliance on setting up changes through their MPLS service provider. Aruba's SD-WAN solution is managed via Aruba Central, a unified network operations and assurance platform that consolidates visibility, setting up routing policies and directly applying configuration changes to the WAN gateways. Central is used to manage Aruba Wi-Fi and switches as well.

Our SD-WAN gateways include unique branch and security capabilities that can be used with third party firewall services – meaning that organizations can reduce their WAN footprint to as few as a single WAN edge device. This also means that IT now has the foundation in place to migrate away from legacy routers and WAN optimizers entirely to consolidate what is being managed in each branch. This is also easily managed via a single pane of glass.

KEY TAKEAWAYS

Aruba's SD-WAN solution provides distributed enterprises with the full set of tools and features needed to prepare branch networks for the transition towards the greater use of cloud services. This includes key capabilities that optimize WAN routing, connectivity to applications hosted in the data center, public cloud, and directly to the Internet, and security features and integrations that protect corporate data.

Aruba SD-WAN is also designed to provide extra value for utilizing Aruba's leading Wi-Fi and switching infrastructure by leveraging user roles and Layer 7 application context for branch to campus to cloud policy enforcement. A unified cloud-managed platform then simplifies deployment and configuration tasks, while helping to reduce IT workloads and WAN management expenditures.

For more information, please refer to the following resources:

- Aruba SD-WAN webpage
- Aruba SD-WAN solution datasheet
- Contact your Aruba sales representative

a Hewlett Packard Enterprise company

AAG_KeySDWANUseCases_061219 a00075217enw