TECHNICAL PAPER

aruba
a Hewlett Packard Enterprise company

Architecting an Application-Driven WAN Edge

Aruba EdgeConnect SD-WAN edge platform liberates enterprises from the cost, complexity and headaches associated with traditional router-centric WAN infrastructure.

CLOUD DEMAND AND THE INTERNET ARE REDEFINING THE WIDE AREA NETWORK

As organizations continue to adopt Software-as-a-Service (SaaS) applications and cloud infrastructure (IaaS), exploding traffic levels and changing traffic patterns are prompting enterprises to reevaluate their Wide Area Networks (WANs). In virtually every market segment, applications are moving to the cloud and a decreasing number are hosted on-premise in the data center. To compound the networking challenge, application bandwidth requirements continue to increase to deliver a superior user experience.

The traditional model of backhauling traffic from branch offices to the data center for robust security inspection is no longer optimal as it wastes bandwidth and adds latency, ultimately impairing application performance. There is a real need for a better way to send traffic directly over the internet from branch locations to trusted SaaS and cloud-based applications, while maintaining compliance with enterprise security mandates.

Over the past two years, Software-Defined WAN (SD-WAN) solutions have emerged to address these challenges, creating a new paradigm for connecting users to applications, while dramatically reducing WAN costs. Rather than relying on traditional routing protocols such as BGP or OSPF, an SD-WAN provides a new, application-driven way to intelligently steer traffic across the WAN by leveraging the most direct paths to SaaS and web applications.

A complete SD-WAN solution also must assure consistent application performance and resiliency, automate traffic steering in an application-driven manner based on business intent, improve network security and dramatically simplify the WAN architecture. Ideally, this simplification would extend to the physical implementation of the solution in the branch. As depicted in Figure 1, traditional router-centric architectures typically comprise multiple physical devices including a router, WAN optimization appliance, firewall, and the addition of SD-WAN introduces yet another function to the branch WAN architecture— each with a distinct management system. Contrast this with the advanced, application-driven architecture shown in Figure 2, where foundational network functions such as routing, stateful firewall, WAN optimization and SD-WAN are delivered as a single, integrated solution managed thru a central orchestration platform.

ROUTER-CENTRIC WAN ARCHITECTURE

1. **Complex**
   Requires specialized IT expertise across multiple disparate management tools to configure, deploy and maintain
2. **Inefficient**
   Unable to fully utilize and optimize all the appliances for cloud-first environment
3. **Expensive**
   Costly and hard to manage and maintain

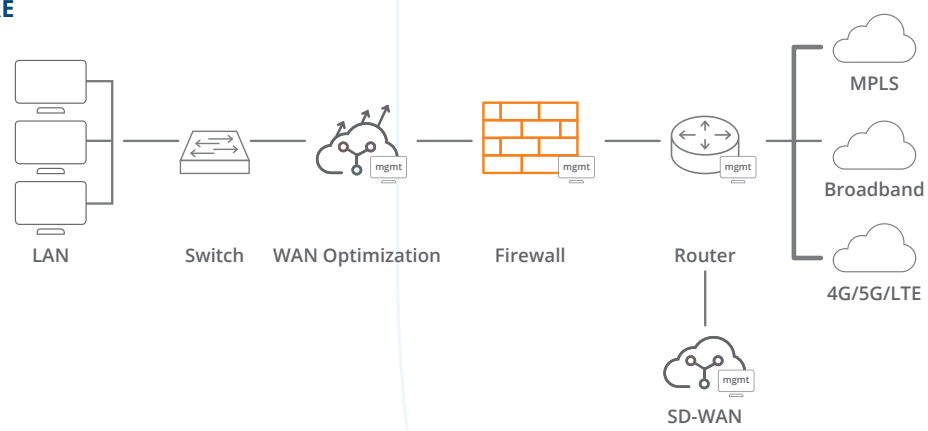

Figure 1. A rigid WAN architecture based on legacy branch routers is expensive and complex to manage.

APPLICATION-DRIVEN WAN ARCHITECTURE

1. **Simple**
   Business intent architecture responds quickly to business needs
2. **Agile**
   Application-driven architecture and management drastically reduces IT resources to operate a site
3. **Cost Effective**
   Orchestrated, consolidated network functions results in tremendous savings. Enables use of cost-effective broadband connectivity to access critical apps

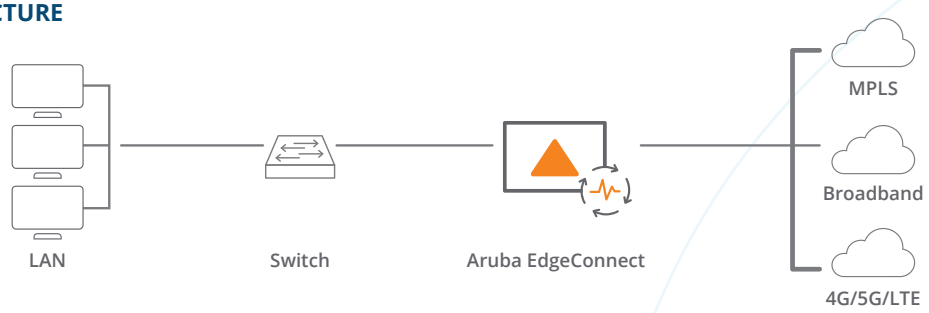

Figure 2. An Aruba EdgeConnect thin branch architecture integrates SD-WAN, WAN optimization, routing and stateful firewall functionality into a single, fully integrated solution, simplifying and consolidating the WAN edge and increasing operational efficiency.

SIMPLIFYING WAN ARCHITECTURE WITH AN APPLICATION-DRIVEN WAN EDGE

The Aruba EdgeConnect SD-WAN edge platform enables a thin branch that dramatically simplifies the branch WAN edge architecture and is purposefully engineered to power today's cloud-first, distributed enterprises. It simplifies branch office infrastructure by consolidating network functions like SD-WAN, WAN optimization routing and security into a single software instance that runs on a single physical or virtual appliance. Management of the thin branch is streamlined through the centralized orchestration of application driven policies based in alignment with business requirements. By deploying a thin branch SD-WAN solution, enterprises can dramatically improve business agility and lower costs, while simultaneously improving network and application performance, availability and security.

Deploying a thin branch architecture requires more than simply consolidating multiple network functions into a single physical or virtual device. Also required is support for flexible, orchestrated service chaining to additional network functions, particularly for application layer security processing. An application-driven model supports granular application QoS and security policies, improves application resilience and performance and automatically enforces business intent across the WAN. This is all managed centrally from a single pane-of-glass, Aruba Orchestrator, streamlining configuration, deployment and administration of the WAN (Figure 3). Zero-touch provisioning allows network managers to easily add new sites to the SD-WAN without specialized IT resources require at branch office locations.

Orchestrator provides an intuitive graphical user interface, enabling IT to centrally assign policies to secure and control application traffic across the SD-WAN. Different virtual WAN overlays – business intent overlays – may be defined, each with unique logical topologies and QoS and security policies based on application characteristics and business priorities. IT defines business intent overlay configurations, security service chaining as well as any subsequent changes centrally, and Orchestrator automatically distributes them to every site across the SD-WAN.

In contrast to the repetitive, CLI-intensive management model employed by traditional router-based WAN architectures, the Aruba EdgeConnect centralized SD-WAN management model, powered by Aruba Orchestrator, streamlines the operational aspects of managing the WAN, improving operational efficiency and minimizing the potential for human errors that can impact application availability

SECURE APPLICATIONS AND ADAPTIVE INTERNET BREAKOUT

Traditional router-centric WAN architectures with limited capabilities offer an all-or-nothing approach to steering internet traffic and cloud applications. Traffic is either sent directly to the internet or backhauled to headquarters. Enterprise security policies often mandate different levels of processing based on the nature of applications, resulting in the requirement for granular steering on an application-by-application basis.

The inability to identify HTTP/HTTPs applications traffic immediately and steer it across its optimal path wastes bandwidth and impairs cloud and web application performance.

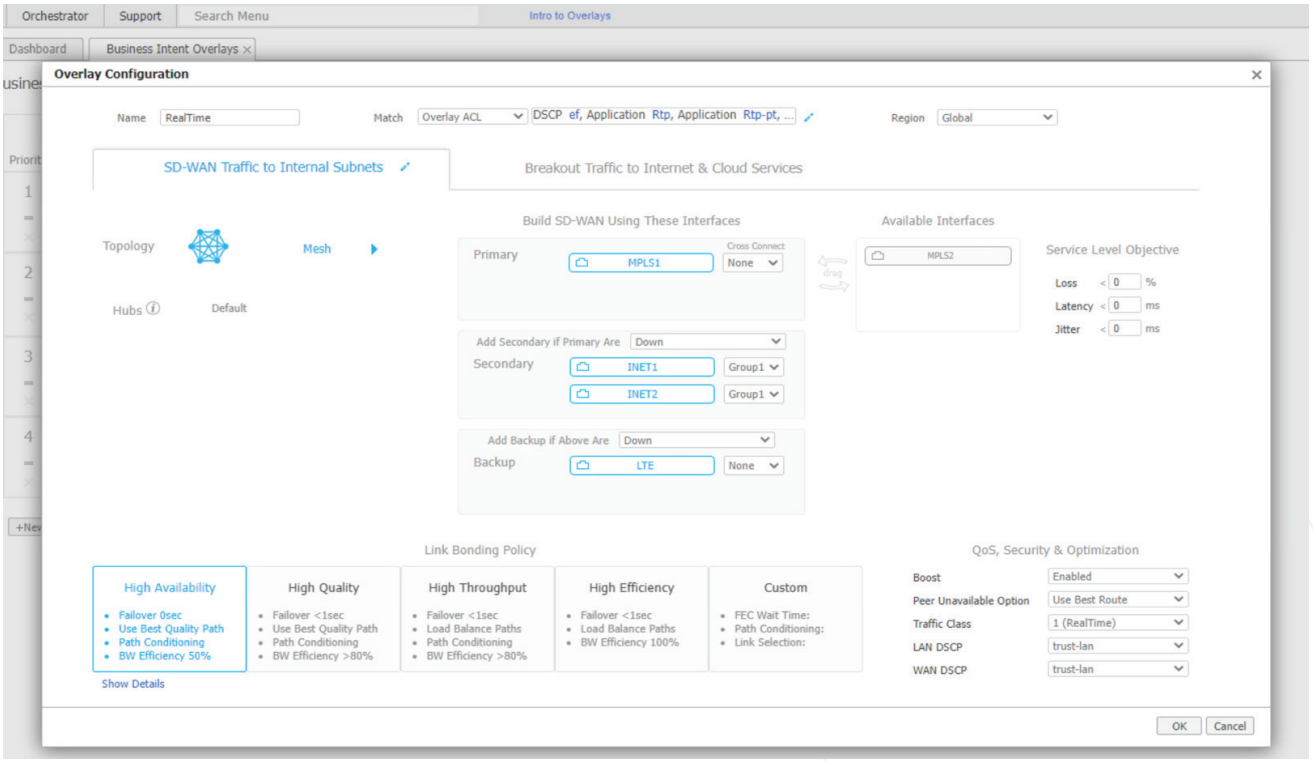

Figure 3. From the Aruba Orchestrator business intent overlay template, network managers can easily assign policies and enable WAN optimization with simple clicks and a drag-and-drop interface.

Many enterprises want to leverage the favorable economics of broadband to connect users directly to cloud applications from branch locations, but face a two-fold challenge. They must first have the ability to identify and classify application traffic based on first packet of each flow so that traffic can be automatically steered to the correct destination. Without this advanced capability, all web-bound traffic is either sent directly to the internet or backhauled to a regional hub or corporate data center firewall. Second, when steering applications traffic directly to the internet, security becomes a key requirement.

Aruba First-packet iQ, an intelligent application identification technology, goes beyond traditional Deep Packet Inspection (DPI) and port-level techniques by adding a cloud-hosted internet map and geolocation database with DNS response cache and HTTP get request cache. First-packet iQ incorporates real-time machine learning to provide the highest levels of application intelligence available today. The combination of these advanced techniques with machine learning has already enabled EdgeConnect to accurately identify more than 10,000 applications and more than 300 million web domains on the first-packet, providing customers with granular visibility and control of their HTTP/HTTPs applications traffic.

Furthermore, the security of granular internet breakout is assured through the combination of an integrated stateful firewall and simple service chaining to next generation firewalls should application traffic require further security inspection. Traffic is easily and automatically service chained to next-generation firewalls or alternatively traffic can be steered to a cloud-delivered security service from Zscaler, Netskope, Checkpoint,Palo Alto Prisma Access, McAfee or Symantec.

As shown in Figure 4, with Aruba EdgeConnect, enterprises can connect directly to the cloud via adaptive internet breakout using broadband internet connections.

For instance, a security policy can be:

- Steer trusted cloud-hosted apps directly to the cloud provider, e.g., UCaaS and O365
- Steer less-trusted apps first to a cloud-delivered security service
- And, steer suspicious apps back to the data center where traffic can receive an advanced inspection from a next-gen firewall, e.g., BitTorrent

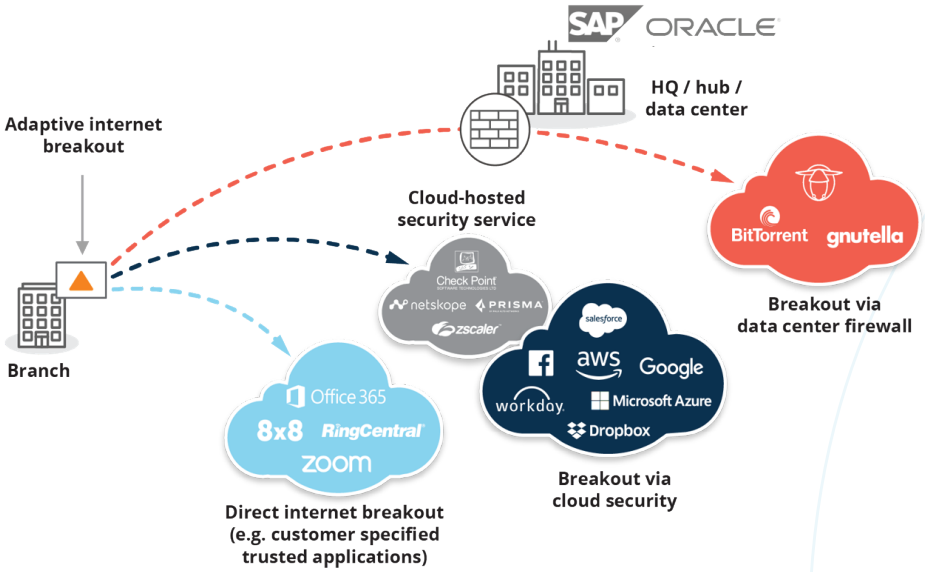

Figure 4. First-packet iQ application classification enables Aruba EdgeConnect to granulary steer traffic on an application basis to meet QoS and security policies based on business intent.

ENSURING NO SINGLE POINT OF FAILURE: A RESILIENT BRANCH

Look at any distributed enterprise and you are sure to find a variety of mission-critical applications that are critical to business functions supported across branch locations. Therefore, "always-on" access to applications no matter where they reside becomes a "foundational requirement" to keep business running. The Aruba EdgeConnect HA cluster architecture enables deployment of EdgeConnect devices in pairs, delivering device, LAN and WAN resiliency while ensuring connectivity over any combination of transport including consumer broadband.

To address the SD-WAN migration and interoperability challenges, Aruba EdgeConnect integrates BGP and OSPF routing interoperability into the SD-WAN solution, resulting in several key benefits. First, it enables seamless interoperability with sites not yet part of the SD-WAN, eliminating the need to manually program local subnets. Second, it automates deployments in the data center through Layer 3 BGP advertisement without using PBR or WCCP.

ACCELERATING LATENCY-SENSITIVE APPLICATIONS TO IMPROVE PRODUCTIVITY

In addition to the ability to breakout traffic locally at the branch, WAN optimization can be enabled and assigned on a per-site and per-application basis to overcome latency challenges when connecting to IaaS or data centers. Geographically distributed branch sites often require a WAN optimization solution to ensure acceptable application performance. No matter how much WAN bandwidth is provisioned at the branch, latency caused by distance can ultimately degrade application performance. For applications that create large file transfers, such as backup and recovery operations, data deduplication and compression algorithms assure Recovery Time and Recovery Point Objectives are achieved.

The optional Aruba Boost WAN optimization software license may be applied on an application-by-application or site-by-site basis, only when and where it's required. Boost is fully integrated with EdgeConnect, delivered and managed as a single solution. Supporting WAN optimization with traditional router-centric WAN edge architectures requires yet another appliance along with its companion management application.

The result? Users are connected securely and experience a consistent application experience whether the applications are hosted in the data center or the cloud.

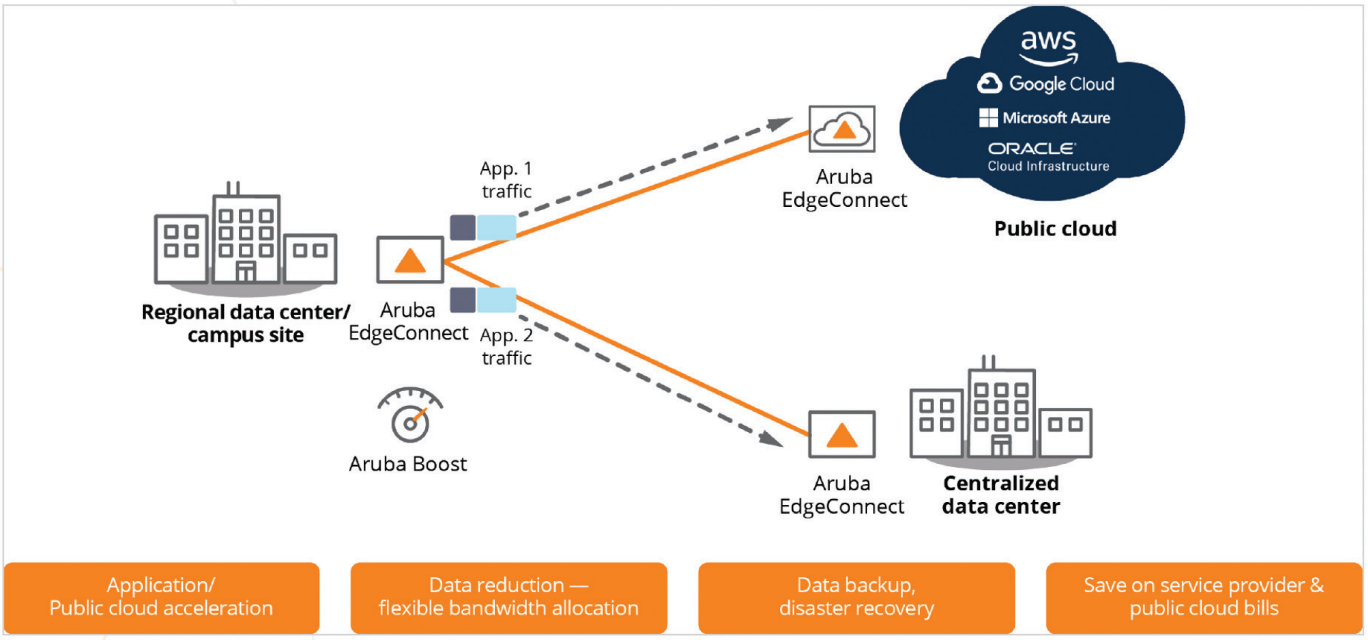

Figure 5. EdgeConnect HA cluster architecture for LAN, WAN and device survivability

CONCLUSION

Geographically distributed enterprises embracing cloudfirst initiatives require a different model to build the branch office WAN edge. The traditional router-centric approach has worked supporting WAN architectures where all applications resided in the corporate data center. However, with distributed applications, a new solution is required to handle the shift in traffic patterns and the increased use of internet services to connect directly to web-based applications.

The Aruba EdgeConnect SD-WAN edge platform empowers distributed enterprises to build a thin branch that combines a single platform for SD-WAN, WAN optimization, routing, IDPS and a stateful firewall to deliver operational efficiencies and enhance user productivity. The solution delivers predictable performance for cloud and web-based applications with bandwidth optimization and consistent application security policies no matter where the application resides. Aruba EdgeConnect integrates BGP and OSPF routing for interoperability with existing WAN architectures, enabling organizations to move beyond traditional router-centric architectures to an advanced application-driven SD-WAN. Centralized management with Aruba Orchestrator automates and accelerates branch office WAN provisioning, increasing IT resource efficiency while lowering operational costs.

TP_ApplicationDrivenWAN Edge_SK_113021 a00119354enw