WHITE PAPER

aruba
a Hewlett Packard Enterprise company

ARUBA SD-BRANCH OVERVIEW

June 2018

Table of Contents

Overview of the Traditional Branch

Branch networks are changing rapidly. The most pressing challenges of today include an increasing number of mobile and IoT devices, growing bandwidth requirements of the business, and modern users who expect connectivity for work and personal use—all while the teams that run these distributed networks stay the same size or even shrink. New network roll-outs are expected to be completed in a short period of time and IT organizations are being asked to improve service levels, reduce costs, and shift spending from capital expense (CAPEX) to operating expense (OPEX). At the same time, there are broader industry shifts under way, described in this section.

ADOPTION OF CLOUD SERVICES

Widespread adoption of cloud services such as Office 365 and the shifting of enterprise workloads to public clouds have changed the traffic flows from the branch. Routing Internet-bound traffic via a central hub-site is no longer a cost-effective or performance-friendly option. More and more, traffic is destined for services running on public clouds reachable directly via the Internet, rather than to an organization's internal private data center. Consequently, IT organizations are looking at providing direct Internet access from the branch in order to enable direct user connectivity to cloud services and minimize latency.

SHIFT TO THE INTERNET AS A BUSINESS TRANSPORT MEDIUM

Traditional WAN connectivity is expensive. Installations involve long lead times and changes to networks are slow to implement. The architecture of the Internet has evolved considerably, with most large software-as-a-service (SaaS) and cloud providers peering at the edges of the Internet, enabling high-bandwidth, low-latency access to their services. In many places, the Internet is good enough to serve as the primary WAN transport, but traditional routing protocols are only able to make routing decisions based on the traffic destination rather than more intelligent factors like packet loss, latency, jitter, or application flow, making legacy solutions unable to take advantage of enhanced Internet services. Organizations need an intelligent way to take advantage of lower-cost links such as high-speed Internet and highly available, if expensive, cellular backup links.

INCREASING REQUIREMENTS FOR MOBILE AND IOT DEVICES

Mobile users and devices continue to consume applications such as video, voice, and storage that impact network performance and health. Growing numbers of Internet of Things (IoT) devices further expand mobile use cases and signify a shift of technology deployments away from traditional IT controls. This adds additional management and security pain points on top of visibility challenges.

BRANCH POLICY AND SECURITY COMPLEXITY

Branch local area networks (LANs) can be surprisingly complex. With a proliferation of virtual LANs and access control mechanisms scattered across multiple network devices, deploying consistent policies is difficult. The way different network devices name features and are configured can lead to unpredictable or inconsistent results. The need for a variety of services in the branch—routing, switching, wireless LANs, caching, URL filtering, firewalling, wide-area network (WAN) compression, etc.—has led to a proliferation of single purpose devices, each with its management platform and associated learning curve. Figure 1 shows the large number of devices needed to provide user services in a typical branch network.

SLOW AND COMPLEX ON-BOARDING

Branch locations often have no local technical resource to install hardware and perform troubleshooting. Today's branch deployment models almost always require a technical installer on the ground, driving up both cost and complexity. On-boarding large distributed networks with small teams requires a considered approach to the installation process factoring in third party installers, non-skilled installation personnel, and the need to create and leverage cookie-cutter configuration models. To do this without sending skilled personnel onsite means that installing and bringing up a branch network must be simple, must leverage cloud-based management with true, unattended provisioning, must be designed for non-technical personnel, and ideally uses a consumer-style user interface.

Aruba Software Defined Branch (SD-Branch)

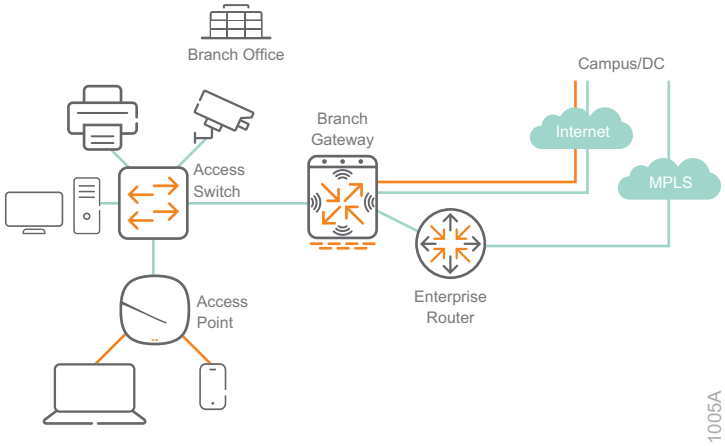
Using an architectural approach that simplifies the delivery of branch requirements, Aruba Software-Defined Branch (SD-Branch) helps unify networks and services that were traditionally managed and designed with distinct operational silos. This solution solves problems on several fronts, beginning with:

- The WAN—Enables the use of SD-WAN technology to support the use of the Internet to replace or augment MPLS services
- The LAN—Flattens the branch into one or two VLANs and eliminates dependence on static IP addressing schemes and hardwired ACLs across multiple devices
- Branch onboarding—Supports bringing up hundreds of locations per week by using non-technical local resources with easy-to-use mobile applications and centralized cloud services for the technical team

The SD-Branch extends the software-defined aspect to all elements of the branch, delivering a full-stack solution, including features such as:

- Zero touch provisioning (ZTP) for most network devices with a templated cookie-cutter approach for automating the roll out of new branch locations. Scale-out cloud management enables rapid growth in the number of branch sites.
- SD-WAN and WLAN/LAN visibility and control through cloud-managed SaaS.
- A zero-trust model for security that removes policy from a physical port based model to one with device authentication and firewalling on site. Advanced security services are delivered by leveraging industry-leading Security-as-a-Service (SECaaS) offerings.
- A consistent policy approach to wired, wireless, and WAN for traffic segmentation, isolation, and path selection.

Figure 1 *SD-Branch Integrated into existing WAN design*



The Aruba SD-Branch solution consists of five main components:

- Cloud management—Aruba Central, a cloud-based lifecycle management service,, offers a central point of management and control for all Aruba access points (APs), switches, branch gateways, and headend gateways. Aruba Central can automatically configure the SD-WAN overlay VPN and provide topology views of the network. Aruba Central also aggregates and correlates diverse sets of information in order to provide insights into network operations.
- Branch gateway—The branch gateway is the appliance at the branch that connects to WAN uplinks and participates as an end-point in the SD-WAN overlay fabric. The branch gateway is a policy enforcement point for wired, wireless, security, and WAN policies including routing. The gateway functions include stateful firewall, web content classification, hybrid WAN connectivity, IPsec VPN, QoS, and WAN path monitoring and selection. The branch gateway is a software function that runs on the Aruba 7000 series appliances.

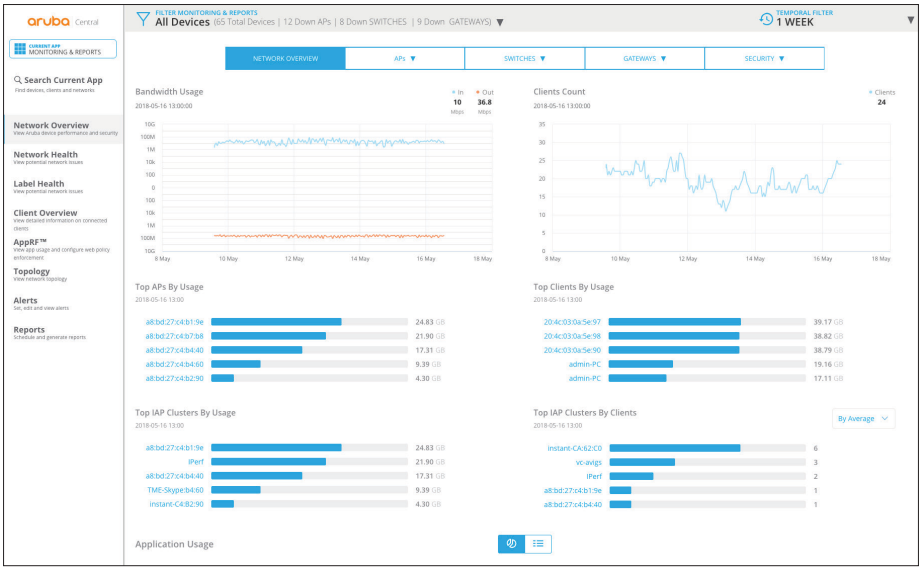
- Branch WLAN/LAN—Aruba switches and APs provide wired and wireless networking for users at branch sites. Access to the branch network is controlled by the Aruba network infrastructure, using role-based policies centralized in the headend or data center. This architecture allows any device to connect via wired or wireless and authenticate on to the network.
- Headend gateway—The headend gateway acts as a VPN concentrator and runs at the headend in hub-and-spoke and multi hub-and-spoke topologies, terminating IPsec VPN tunnels and participating in the data center and campus routing. The headend gateway also participates in the SD-WAN fabric overlay topology. The headend gateway is a software function that runs on the Aruba 7200 series appliances.

The Aruba SD-Branch Key Features

SIMPLICITY WITH AUTOMATION

- Cloud management—Aruba Central provides centralized management, monitoring, and troubleshooting of Aruba gateways, instant access points, and wired switches, and it enables seamless integration with third-party, cloud-based security providers. Extensive use of templates allows for simple branch provisioning, and a dedicated Install Manager enables simple mobile app-based onboarding for network devices. Extensive use of templates allows for simple branch on-boarding. Aruba Central replaces on-site network management.
- Real-time health monitoring—Cloud-managed sensors at each branch site monitor application performance from a centralized location, 24/7/365.
- Zero-touch provisioning—All of the Aruba branch devices support ZTP, including the gateway, APs, and switches. Aruba devices use DHCP and DNS to connect with Aruba Activate in order to discover Aruba Central and self-provision without operator intervention. The devices have TPM crypto-processors embedded in hardware in order to allow for secure, mutual authentication.
- Automatic VPN setup—The Aruba solution takes away the complexity of setting up secure VPN tunnels by automatically establishing the overlay topology and advertising routes available over the overlay.

Figure 2 *Cloud management of SD-Branch with Aruba Central*



SECURITY

- IPsec VPN—Aruba branch gateways and headend gateways support high-performance IPsec VPN for secure overlay networking across the Internet or other untrusted networks.
- Client VPN—Aruba branch gateways and headend gateways support VPN termination from client endpoints directly. In a branch, this enables employees or contractors to access internal systems, such as security cameras or IoT sensors, based on their allowed role.
- Dynamic segmentation—You can tunnel connections on Aruba wired switch ports to the branch gateway and apply consistent policy to the user or device the same way you apply policy to wireless users.
- Stateful firewall—The Aruba Policy Enforcement Firewall (PEF) is a full, stateful firewall able to tightly control what users and devices are permitted to do, enabling application-layer security and providing separation between user-roles. This gives network administrators insight into the applications running on the network and who is using them.
- Web content classification & reputation—The Aruba branch gateway uses Webroot cloud-based machine-learning classification technology. Web sites are classified for content-based filtering. The reputation of all public IP address space is monitored to detect and block threats such as spam, exploits, botnets, phishing, proxies, and mobile threats. Geolocation information allows you to block IP ranges based on country.
- Cloud security integration—You can route select traffic that is bound for the Internet to cloud security services such as Zscaler or Palo Alto Networks GlobalProtect. This allows organizations that use cloud-security services to have the same policy applied to user groups in the branch or at headquarters.

ROLE-BASED POLICY

- Common policy for wired, wireless and WAN—The Aruba solution provides a common policy framework based on user-role for wired and wireless LAN, WAN, and security policies. Aruba ClearPass can dynamically push role and security policies to the branch gateway to be applied to users or devices. Other NAC solutions can be used as well.
- Application fingerprinting—The Aruba branch gateway can identify approximately 2600 applications and apply policy to block, permit, rate limit, and apply QoS based on application, user, and role to make sure business traffic is routed using the best available path and that low priority applications are rate-limited or blocked.
- Policy-based routing—You can route traffic based on roles (application or user), application and FQDN, or IP destination. For example, you could route guest traffic directly to the Internet and employee traffic over the MPLS network.

SD-WAN

- Path quality monitoring—To reduce the load on WAN links and better gauge the performance of real applications, the branch gateway can actively and passively monitor connections for latency, jitter, packet loss, and throughput.
- Dynamic path selection (DPS)—Link conditions change over time. Using health monitoring information, DPS can intelligently route-traffic based on policy so that applications are routed over the best available path. For example, you can route real-time voice and video on the path with the lowest latency and jitter while you route bulk traffic on the path with the most bandwidth.
- Routing—Static and dynamic routing support allows the branch gateway to fully replace a traditional router for networks with MPLS by allowing the branch gateway to exchange IP routes with the service providers MPLS router.
- Compression—To improve throughput, the branch gateways can compress IP traffic on the VPN overlay.
- Bandwidth contracts—This allows you to control the amount of bandwidth an application or group of applications can use. The limits can be enforced based on user-role or interface in the upstream and downstream directions. For example, if you don't want to block access to an application for a user group but you don't want the application to negatively affect business related traffic, you can limit the applications network bandwidth.

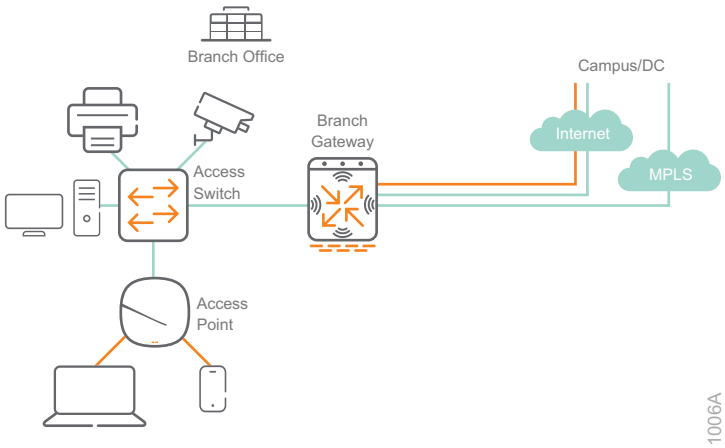
Solution Benefits

The Aruba SD-Branch solution enables organizations to address many of the problems they are facing today in the branch. The SD-WAN component of the solution includes a branch gateway that combines the functions of many discrete devices such as firewall, WAN router, deep packet Inspection engine, and WAN optimization into a single device, reducing the number of devices to deploy and maintain.

Enabling more cost-effective WAN connection types and a transport independence is the goal of SD-WAN. The Aruba SD-WAN feature allows you to use a combination of traditional WAN links and Internet links together with all links actively carrying traffic, rather than using some for backup purposes only. Combined with key components of SD-Branch, the solution delivers simple but powerful routing based on user-role, device type, application, and path quality across a variety of WAN topologies.

The move away from a physical security model based on where a device connects to the network to a role-based model enables many benefits for branch operations. A policy follows the user model, allowing an administrator to configure policies that are access- and location-agnostic, delivering a single policy framework for wired, wireless, and WAN. Wired switches can act as "wired APs" tunneling all user traffic to the branch gateway so a single consistent policy can be applied. Organizations get end-to-end segmentation of traffic enforced at the branch and maintained across the entire network.

Figure 3 *Fully integrated SD-Branch solution*



The solution provides simple onboarding for all branch network devices using ZTP. Aruba Central delivers a cloud-based, single-pane-of-glass management and monitoring solution and the move to cloud enables a subscription-based consumption model.

The Aruba 7000 series branch gateway is an enterprise-class product with a small form-factor and high performance—starting with the Aruba 7005, which provides 2 Gbps of firewall and 1.2 Gbps of IPsec VPN and going up to the Aruba 7030, with 8 Gbps of firewall and 2.4 Gbps of IPsec VPN in a 1U appliance. The Aruba 7200 series headend gateway delivers 12 Gbps of firewall and 4.5 Gbps of IPsec VPN with the 7205 going up to 40 Gbps of firewall and 30 Gbps of IPsec VPN on the high-end 7280.

The interest in SD-WAN is an inflection point to roll out the SD-Branch within the context of unified management across multiple operational silos in order to:

- Improve IT visibility.
- Expand SD-WAN capabilities with insight into the branch as far as user and device awareness.
- Provide consistent policy enforcement from a centralized point with ClearPass, which can dynamically apply rules across highly distributed enterprises such as retail and hospitality.

All of these and additional expansions help simplify IT management, enhance user experience consistently across multiple sites, and bring differentiated, context-aware security to improve wired, wireless, and WAN policies.

Over the longer term, SD-Branch extends the campus experience across the distributed enterprise with rich SD-WAN capabilities, security that extends from users and devices to applications and WAN state, and management and onboarding with cloud scale. These features extend to locations, large and small, to improve deployment flexibility. SD-Branch is a comprehensive vision that is unique to Aruba and serves as a platform for additional services that can be delivered to the enterprise.

.

© Copyright 2018 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. Aruba Networks and the Aruba logo are registered trademarks of Aruba Networks, Inc. Third-party trademarks mentioned are the property of their respective owners. To view the end-user software agreement, go to www.arubanetworks.com/assets/legal/EULA.pdf

You can use the feedback form to send suggestions and comments about this guide.

aruba
a Hewlett Packard Enterprise company

B-000180A-3 09/18