SOLUTION OVERVIEW

Software Defined Branch

Revolutionizing the branch for todays digital era

Distributed organizations such as retail, hospitality and healthcare are undergoing a digital transformation to better meet evolving business objectives and compete within their industries. This frequently means that IT must improve operations, deploy new services faster, and deliver an enhanced, and secure user experience.

Cloud-based services are driving rapid change across industries, especially as organizations transition to software-as-a-service applications in greater volume. The influx of mobile devices and Internet of Things (IoT), and the increasing demand for bandwidth also changes how the LAN and WAN must be managed moving forward.

By 2023, 70% of enterprises will rely on the Internet for branch and remote office connections[1] to the head office – just as 20 billion IoT devices enter the mainstream market.[2] These are daunting challenges for IT, whose budgets have been slashed in 2020. In addition, they now need to securely manage direct-to-Internet (DIA) traffic that is bypassing the corporate perimeter.

This potentially exposes the business to security risks, and increases the burden on IT to maintain consistent access layer policies. They must approach the branch network holistically, which will allow them to easily manage the onboarding of new devices, segmentation of traffic and the ability to assure SLAs are met within each branch and across all WAN links.

This is where IT requires an architecture flexible enough to scale with the pace of business demands today, as well as meet tomorrow's growth opportunities. All this while reducing costs and moving from a capital expense (CAPEX) to operating expense (OPEX) model.

KEY CAPABILITIES OF SD-BRANCH

- **Aruba Central** – single-pane-of-glass unified infrastructure management, AIOps, security and reporting.
- **Zero-Touch Provisioning** – with installer app reduces the time, cost and complexity of installing branch office networks.
- **Dynamic Segmentation** – context-aware policy enforcement for users and IoT – eliminates manual configuration of numerous VLANs with a single VLAN deployment.
- **SD-WAN Orchestration** – automatically sets up IPsec tunnels between gateways, building the SD-WAN overlay for very large networks.
- **End to End QoS** – application visibility and policy enforcement for over 3200 apps from LAN to WAN to the cloud.
- **SaaS and IaaS acceleration** – dynamic path optimization for high priority SaaS apps and selection of virtual gateways for AWS and Azure tunnels.
- **Zero Trust Security** – embraces a scalable security methodology from edge to cloud for consistent role-based enforcement and context-aware controls in a variety of branch networking requirements.

[1] Gartner, "SD-WAN: CSPs Must Seize the Internet Opportunity", Apr. 2018
[2] Ericsson Mobility Report, Nov. 2017

THE SOFTWARE DEFINED BRANCH

Aruba's answer is a software defined branch (SD-Branch) that combines best-in-class wireless, wired and WAN infrastructure with management capabilities that include assurance and orchestration features to help maximize performance and minimize operational costs. A Unified Infrastructure model gives organizations a way to simplify the deployment, configuration, and management of everything within a branch location and across the WAN using a single pane of glass management.

Aruba Central's Cloud solution provides this needed single of pane of glass that unifies management dashboards, and includes AIOps and security visibility for wired, wireless and SD-WAN networks. This enhances IT's ability to proactively see what is happening in each branch and troubleshoot issues more easily. In turn, leveraging Aruba's extensive portfolio of security and analytics solutions provide the needed context to customize access and bandwidth policies accordingly.

BEST IN CLASS UNIFIED INFRASTRUCTURE

Aruba's industry leading wireless, wired, and WAN solutions and software helps IT deliver the performance and reliability required for today's mobile-first environments. Unified management and end-to-end visibility keep mobile and IoT devices connected and performing at their best regardless of type, applications being used, or connection method.

Aruba Branch Gateways allow IT to deploy and manage WAN connections, without the cost and delays of the past. The Branch Gateways support multiple WAN connections that include the Internet, MPLS and cellular connections, software defined role-based policy enforcement and the ability to easily define best paths for data center, cloud, and SaaS destined traffic.

Zero Touch Provisioning (ZTP) offers IT the ability to quickly and accurately configure and deploy all access infrastructure within a branch. A simple to deploy mobile app allows any non-technical employee to barcode scan an Aruba access point, switch, or Branch Gateway and bring devices up, which reduces deployment timelines, and costly onsite visits.

ENTERPRISE SD-WAN

While the role of the traditional WAN routing has reliably served distributed enterprises for decades, many IT organizations are looking for a new solution that addresses the complexity of managing a WAN as applications and services shift to the Cloud, which often run over unsecure public broadband.

The Aruba Branch Gateway gives organizations a reliable, high performance secure VPN overlay network that supports broadband, MPLS, and LTE WAN uplink connections. From a routing standpoint, this provides IT with greater insight into the traffic flowing in and out of each branch, regardless of the uplink.

An Aruba headend gateway or virtual gateway is needed for VPN concentrator (VPNC) termination in hub-and-spoke topologies for IPsec VPN tunnels, and in data center routing scenarios. Aruba Virtual Gateways are deployed in public cloud infrastructures, such as an Amazon Web Services virtual private cloud (AWS VPC) or Microsoft Azure Virtual Network (VNet). These gateways serve as a virtual instance of a headend gateway to enable seamless and secure connectivity for all branch and data center locations connecting to public clouds.

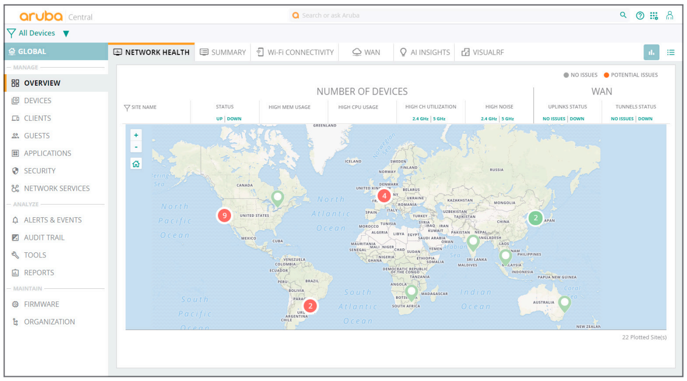
Aruba combines best-in-class wireless and wired infrastructure and management orchestration features with cost saving SD-WAN capabilities.

The standard branch office deployment consists of single or dual Aruba branch gateways, switches, and access points, which are sized based on the number of users and devices at the branch.

A smaller office or micro-branch can operate without a gateway by deploying a VPN terminated Aruba access point. Teleworkers at home or on the road can use the Aruba Virtual Intranet Access (VIA) soft client for secure access.

CLOUD-MANAGED SIMPLICITY AND SCALE

To simplify the remote management of various hardware within a branch, Aruba Central provides a single pane of glass that includes wireless, wired and WAN configuration and visibility dashboards, traffic optimization and AIOps features and built-in network and user-oriented troubleshooting tools.



Aruba Central dashboard for WLAN, LAN, and WAN management

Aruba Central IT can centrally define and enforce policies across all branch sites. Changes are automatically pushed out across multiple branch locations resulting in a consistent user experience and access privileges at each branch for users as they move from one branch location to another.

Aruba Central gives IT complete visibility from edge-to-cloud; it starts with a global view of company locations, data centers and cloud nodes, then moves to a particular location topology view, then drills down to an individual gateway, switch, or access point to display individual users, devices, and applications.

Multiple levels of IT administrator privileges help distribute the workload for environments that can span multiple time zones or responsibilities within IT. It's easy to set up who can see and make changes to the hardware in each branch, or assign read-only privileges to those with only help desk roles.

ZERO TRUST SECURITY

The lack of visibility and control by IT in branch environments is of utmost concern. IoT devices often get connected without ITs knowledge, as users find ways to bypass security controls. As distance between corporate and the branches is usually a factor, it's hard to easily unplug a device when its behavior has changed for the worse.

Aruba wireless and wired solutions support role-based access security that allows for dynamic segmentation of devices and traffic. The branch gateway provides an inspection/enforcement with app aware stateful firewall that protects the branch from internal threats using deep packet inspection (DPI), IDS/IPS, and content filtering rules.

Aruba ClearPass Policy Manager offers dynamic device profiling, real-time authentication and granular policy enforcement, with the ability to quarantine a device without physical interaction, Aruba ClearPass also scales for any size of type of environment.

Advanced threat defense capabilities are available to guard against a myriad of threats, including phishing, DoS and increasingly widespread ransomware attacks. Identity-based IDS/IPS performs signature- and pattern-based traffic inspection on both the branch office LAN traffic as well as the SD-WAN traffic flowing through the gateway. An advanced security dashboard provides IT teams with network-wide visibility, multi-dimensional threat metrics, threat intelligence data, correlation and incident management.

As more and more applications and solutions move to the cloud, a robust partner program offers customers the ability to leverage third-party defenses from vendors such as Zscaler, Palo Alto Networks, and Checkpoint. Instead of sending all traffic to the data center, real-time threat correlation, inline content inspection and other cloud firewall controls make it easy to protect today's mobile perimeter.

INDEPENDENT ASSESSMENT OF ARUBA SD-BRANCH

Miercom validated the performance and capabilities of the Aruba SD-Branch Solution including SD-WAN

Read the full report

AN OPTIMIZED BRANCH EXPERIENCE

Providing consistent experiences at each branch as well as at corporate are among many of IT's goals. This can be accomplished by leveraging context about each user, connected devices, and the types of applications that are being used. Allows IT to easily enforce access, bandwidth and security policies based on roles and known data.

This unique contextual-awareness enforces WAN policies within the Branch Gateway. For example, executives can be given a higher priority when using Zoom or Microsoft conferencing solutions over others. Policies can also be enforced within the gateway for inbound traffic and intra-branch traffic.

The gateway is also capable of monitoring the health of WAN links, which allows for seamless failover from one link to another. For links connecting to SaaS apps, the gateway measures bandwidth using active and passive probing to determine and use the optimal path dynamically.

AUTOMATED USER EXPERIENCE MONITORING

To continuously measure the experience of devices in the branch, Aruba's User Experience Insight offers a simple way to test the responsiveness of end-to-end connections within the branch, into the cloud, or to the data center.

SUMMARY

As organizations explore options for transforming their branch locations, Aruba's key differentiator is an open, software-based solution that is flexible, scalable and easy to deploy. Customers can choose from industry leading wireless, wired, and WAN technologies, cloud management and security solutions that ensure IT and users are receiving the best experience possible.

SD-BRANCH NETWORK SOLUTION COMPONENTS

Aruba Access Points

Secure business-class Wi-Fi connectivity managed from Aruba Central

Learn about Aruba Access Points

Aruba Ethernet Switches

Scalable high-performance wired access managed from Aruba Central

Learn about Aruba Switches

Aruba Branch Gateways

Secure gateways and virtual gateways for SD-WAN managed from Aruba Central

Learn about Aruba 9000 Series Gateways

aruba
a Hewlett Packard Enterprise company

SO_SDBranch_060220 a00060552enw

Contact Us **Share**