Software Defined Branch

Solution Overview

Providing consistent experiences at each branch as well as at corporate level 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. This allows IT to easily enforce access, bandwidth and security policies based on roles and other contextual data.

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 organisations 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 to the head office – just as 20 billion IoT devices enter mainstream market. These are daunting challenges for IT, whose budgets are only expected to grow 3.2% in 2019. 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.

THE SOFTWARE DEFINED BRANCH

Software defined branch (SD- Branch) combines best-in-class wireless, wired and WAN infrastructure with management capabilities that include assurance and orchestration features to help maximise performance and minimise operational costs. IT organisations can now utilize a common model, implemented with cloud-based management in mind to simplify the deployment, configuration, and management of everything within a branch location.

The Cloud based platform provides a single of pane of glass for wireless, wired and WAN management, enhancing ITs ability to proactively see what is happening in each branch and troubleshoot issues more easily. In turn, leveraging an extensive portfolio of security and analytics solutions provide the needed context to customise access and bandwidth policies accordingly.

BEST IN CLASS LAN INFRASTRUCTURE

Industry leading wireless and wired LAN solutions and software helps IT deliver the performance and reliability required for today's mobile-first environments. Built-in features keep mobile and IoT devices connected and performing at their best regardless of type, applications being used, or connection method.

Branch Gateways allow IT to deploy and manage WAN connections, which in addition to wired and wireless management is a third and critical IT responsibility. The Branch Gateways support multiple WAN connections, software defined role-based policy enforcement and the ability to easily define best paths for Internet and data center 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 access point, switch, or SD-Branch Gateway and bring devices up, for reduced deployment timelines.

Software Defined Branch

SD-WAN GATEWAYS

While the role of the traditional router has reliably served distributed enterprises for decades, many IT organisations are looking for a new solution that takes advantage of today's broadband connection alternatives.

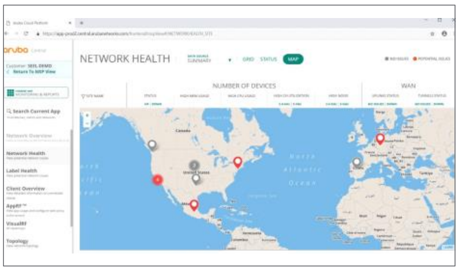
The Branch Gateway offers organisations a reliable, high performance option that supports broadband, MPLS, and LTE WAN connections. From a routing standpoint, this provides IT with greater insight into the traffic flowing in and out of each branch, regardless of the uplink.

A headend gateway is needed for VPN concentrator (VPNC) termination in hub-and-spoke topologies for IPsec VPN tunnels, and in data center and campus routing scenarios. Virtual gateways are deployed in public cloud infrastructures, such as an Amazon Web Services virtual private cloud (AWS VPC) or Microsoft Azure Virtual Network (V-Net).

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.

CLOUD-MANAGED SIMPLICITY AND SCALE

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



CENTRAL dashboard for network management

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.

INTEGRATED BEST-IN-CLASS SECURITY

The lack of visibility by IT in branch environments is of utmost concern. IoT devices get connected without ITs knowledge. Users find ways to bypass security controls where distance between corporate and the branches is usually a factor. It's hard to easily unplug a device with behavior that has changed for the worse.

Wireless and wired solutions support role-based access security that allows for dynamic segmentation of devices and traffic. The branch gateway then includes a built-in stateful firewall that protects the branch from internal threats using deep packet inspection (DPI), and 'Central' can be used to enforce web and content filtering rules.

For dynamic device profiling, granting real-time access privileges and granular policy enforcement, with the ability to quarantine a device without physical interaction, the 'ClearPass' solution offers enterprise scalability for any type of environment.

CLOUD-BASED SECURITY PARTNERS

As more and more applications and solutions move to the cloud, a robust partner program offers customers the ability to leverage third-party defenses. 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.

SUMMARY

As organisations explore options for transforming their branch locations, the key 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.

GET IN TOUCH WITH US TO DISCUSS YOUR REQUIREMENTS