aruba
a Hewlett Packard Enterprise company

TECH BRIEF

EXTEND THE WAN TO THE HOME OFFICE/SMALL OFFICE WITH EDGECONNECT MICROBRANCH

SHIFT TO REMOTE WORK

Approximately 50% of employees will work remotely, at least part of the time once the pandemic subsides.[1] The new normal is a highly distributed workforce yet it represents new challenges for IT. Fully 70% of organizations report that they experience issues with mission-critical applications daily or several times a week.[2]

IT teams are now tasked with ensuring a secure and reliable experience for a highly distributed workforce that is accessing data center and cloud-based applications over consumer broadband and cellular connections that are outside IT's control and visibility. What is needed is an easier way for IT to provide enterprise-grade connectivity to employees who are working remotely by extending the WAN from the campus to the home office and small office or ad-hoc locations.

INTRODUCING EDGECONNECT MICROBRANCH

Building upon Aruba's remote access point technology, the EdgeConnect Microbranch solution adds advanced SD-WAN and SASE capabilities to deliver a cloud-managed, enterprise-grade solution for the home office or small office as part of a hybrid work environment. IT can remotely deploy and centrally manage secure network connectivity for hundreds or even thousands of remote workers or small office employees to deliver an in-office experience using Aruba Central and any Aruba access point – without need for a gateway.

Remote workers can connect wireless clients (laptops, smartphones, tablets) as well as wired clients, such as VoIP phones, and access mission-critical applications reliably and securely. As backup, the AP can be used with an LTE dongle inserted into the USB port for uplink redundancy and business continuity. IT benefits from a unified approach that enables staff to configure, troubleshoot, and optimize network performance across campus, branch, and remote work environments. Intelligent route and tunnel orchestration and policy-based routing drives operational efficiencies and optimizes network performance.

KEY FEATURES

- **Cloud-managed Wi-Fi:** any Aruba AP can be used to provide reliable, high-performing connectivity to deliver the same user experience and security whether an employee is at home or in the office.
- **Intelligent policy-based routing:** Automates how traffic should be routed to endpoints based on rules for specific applications, websites, or types of users to improve performance and security.
- **Automated route and tunnel orchestration:** APs can orchestrate VPN tunnels on demand and reroute traffic as needed to optimize network performance.
- **SASE and Zero Trust:** Applies policy-based routing to orchestrate tunnels and direct certain remote user traffic for cloud security inspection to extend SASE and Zero Trust architecture to the home office.
- **WAN health troubleshooting:** Dashboard views provide near real-time updates on WAN availability, utilization, and throughput with drill downs into ISP and VPN performance to accelerate problem resolution.
- **Access to in-office resources:** Employees can plug in VoIP phones or wired printers directly into the AP and can securely access on-campus resources using corporate SSIDs.

REMOTE WORK ARCHITECTURE

Aruba APs are fully capable of providing secure wireless (and wired) connectivity between remote branch offices or teleworkers and corporate resources using IPsec VPN tunnels. The tunnels and routes between the AP and data center are automatically created without user intervention through Aruba Central with the help of tunnel orchestration and route orchestration. There is no need for manual tunnel configuration or route calculation to optimize performance.

[1, 2] IDC, February 2021

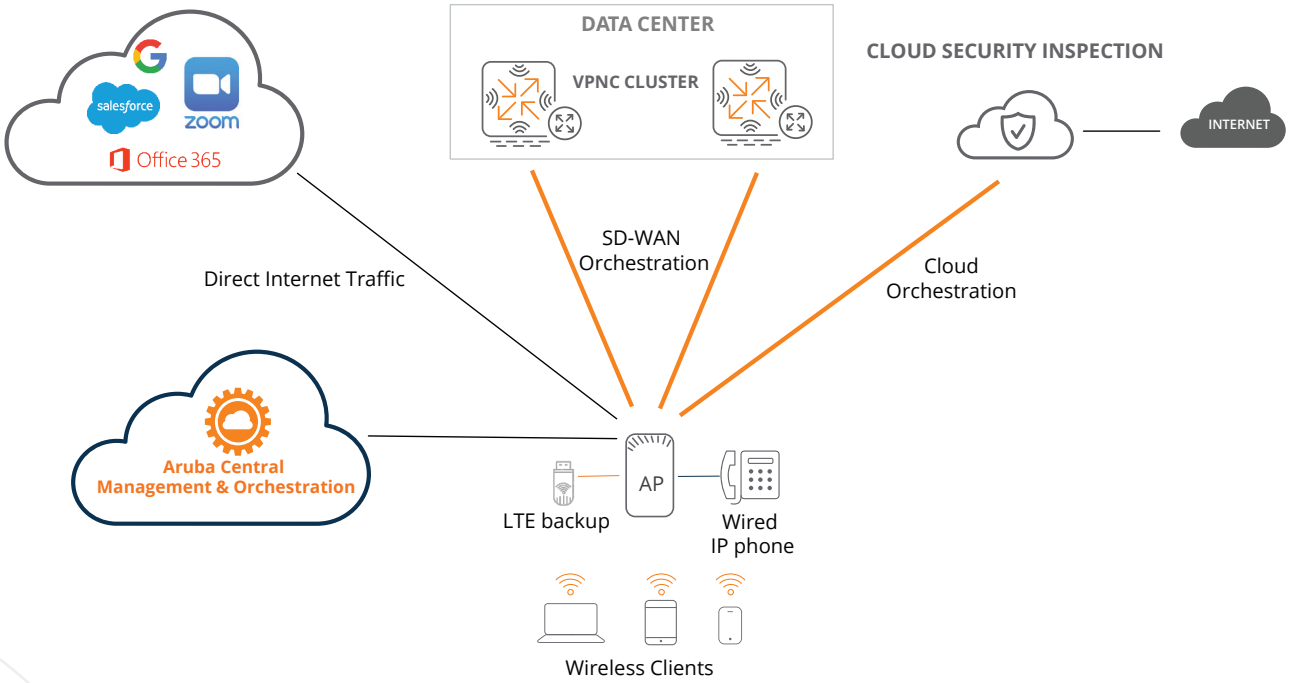

Figure 1: The EdgeConnect Microbranch solution includes Aruba Central for management and control and an AP located in the small office/home office to support VPN capabilities, SD-WAN orchestration, and SASE. LTE backup can be added via an AP dongle.

In the microbranch architecture, the AP can create a VPN tunnel over the internet to a VPN Concentrator (VPNC) cluster deployed in an on-premises or cloud-based data center or public cloud – or use direct internet access to route directly to a SaaS application. The AP also provides advanced SD-WAN functionality, which was previously available on the gateways, to offer high reliability to remote workers. Implementation is streamlined since Wi-Fi connectivity and SD-WAN capabilities are combined in one operating system and run on the cloud-managed AP without need for a additional hardware or appliances on premises.

EdgeConnect Microbranch offers flexibility with support for Layer 2, Layer 3, and mixed modes of deployment. For Layer 2 deployments, the DHCP server runs in the data center where the VPN Concentrator (VPNC) is located. In Layer 3 deployments, the AP itself acts as the DHCP server for the clients. No gateway or associated overhead is required thereby accelerating deployment and streamlining operations in Layer 2, Layer 3, or mixed mode.

Aruba Central provides the management and orchestration for the EdgeConnect Microbranch solution. As the management and orchestration console for Aruba ESP (Edge Services Platform), Aruba Central provides a single point of control to oversee every aspect of wired and wireless LANs, WANs, and VPNs across campus, branch, and remote office locations. AI-powered analytics, end-to-end orchestration and automation, and advanced security features are built natively into the solution. Live upgrades, robust reporting, and live chat support are also included, bringing more efficiency to day-to-day maintenance activities. Built on a cloud-native, microservices architecture, Aruba Central delivers on enterprise requirements for scale and resiliency.

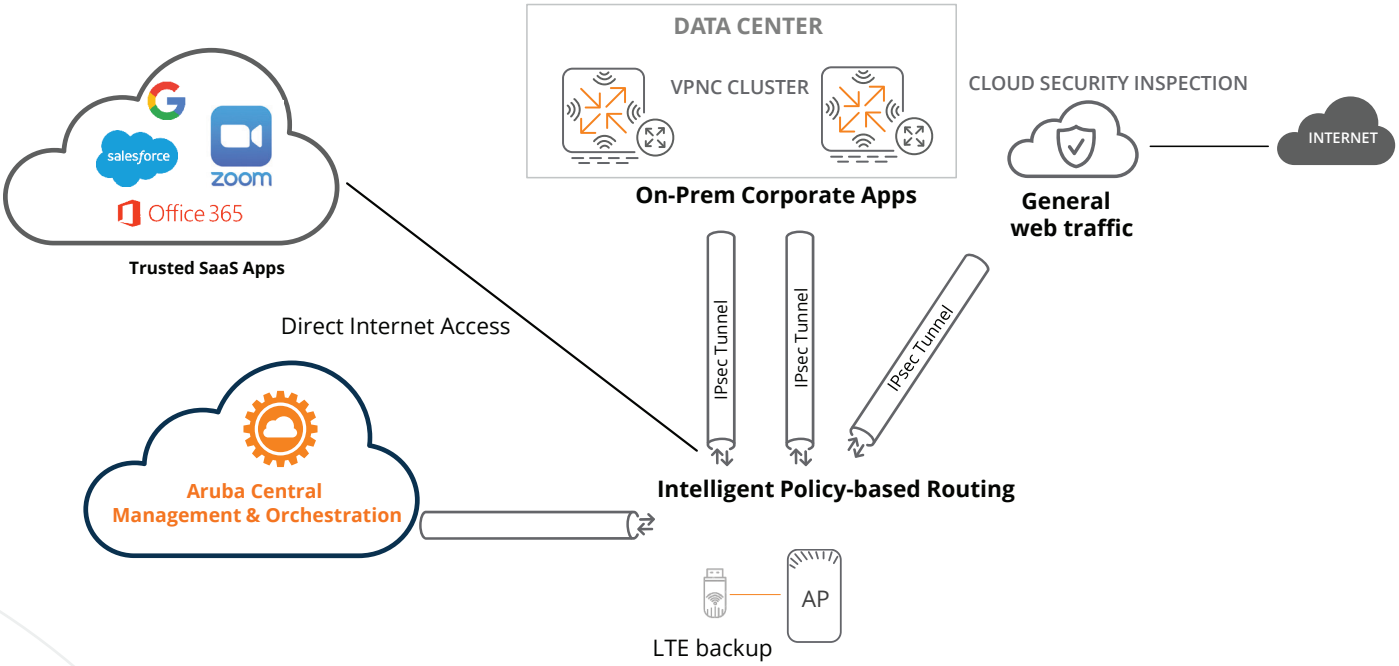

Figure 2: The EdgeConnect Microbranch solution supports split tunnel mode and SD-WAN policy-based routing for greater security and improved user experience.

SD-WAN POLICY-BASED ROUTING

Traditionally, all user traffic is forwarded to the data center for policy checks. This process causes tremendous traffic backhauls and with ever-increasing employees working remotely, impacts user experience and workforce productivity.

Policy-based orchestration applies consistent rules to remote user traffic to enhance security and improve user experience. In a microbranch deployment, traffic is forwarded through the overlay network or to the Internet using destination-based routing or can be forwarded using intelligent policy-based routing to create rules that make use of all available links. With policy-based routing, APs can consistently implement automated policies such as those listed below to ensure:

- Remote user traffic to corporate goes to data center through a secure IPsec VPN tunnel.
- Remote user traffic such as general web traffic goes directly to cloud security inspection through an orchestrated tunnel.
- Remote user traffic to corporate's trusted SaaS applications can go directly to the SaaS provider via the Internet to minimize latency for video conferencing and other mission-critical applications.

Enterprises can also specify fine-grained rules based on the specific applications and destination websites (or web-categories) to determine how the traffic should be treated. Because policies are defined centrally with Aruba Central, they can be applied consistently. Users benefit from improved performance since policies can be implemented to optimize routing and to avoid unnecessary delays or backhauling of traffic.

Tunnel Orchestration removes the complexity and scalability issues associated with configuring IPsec tunnels between APs of a remote site and the headend gateway and can operate in centralized, distributed or local mode for greater flexibility.

ZERO TRUST AND SASE EDGE-TO-CLOUD SECURITY

The EdgeConnect Microbranch solution expands the Zero Trust and SASE framework to the home/small office in hybrid work environments by using policy-based routing to orchestrate tunnels and direct certain remote user traffic for cloud security inspection.

Cloud security inspection policies can be configured directly through Aruba Central to streamline operations. Once configured, EdgeConnect Microbranch automatically tunnels traffic to the cloud security provider over IPsec to the best available POP enabling IT to support large numbers of remote work locations without deploying additional appliances or endpoint agents.

In addition, for traffic destined for the data center, Aruba ClearPass applies consistent policies and granular security controls at the application, user, device, or location level across wireless, wired and VPN networks. IT benefits from detailed visibly of all devices connecting to the enterprise, increased control through simplified and automated authentication or authorization of devices, and faster, better incident analysis and response.

COMPREHENSIVE WAN HEALTH VISIBILITY

To better troubleshoot and optimize performance, the EdgeConnect Microbranch solution provides visibility into the AP's WAN and VPN health including packet loss, latency, and jitter metrics (Figure 3). Armed with this information, IT can quickly assess overall health and determine if the issue is with the ISP or elsewhere. Moreover, IT can also monitor traffic usage and throughput at different time intervals. With other solutions, IT visibility into the WAN is often limited to the health of the VPN Concentrator so when remote workers report issues, operators are unable to assess the situation fully.

CENTRALIZED DEPLOYMENT AND MANAGEMENT

Because APs are managed by cloud-native Aruba Central, IT can centrally configure, monitor, and troubleshoot using a single pane of glass across campus, branch, and remote worker environments and unify network management across wired, wireless, and SD-WAN. Central provides rich features including Zero Touch Provisioning, auto clustering, and centralized IP address pools. Orchestration services for tunnels and routes automate tunnel creation and route optimization and eliminate manual configuration processes.

PRODUCT REQUIREMENTS

Aruba Central for cloud-based management and orchestration

3xx, 5xx or 6xx Series Aruba APs running ArubaOS 10.x

7xxx/9xxx Series Gateways or Virtual Gateway in the data center to act as VPN Concentrators

KEY TAKEAWAYS

The EdgeConnect Microbranch solution helps IT ensure secure, reliable access for remote workforces. It extends the WAN to remote workers, providing them with an in-office experience and unlocking new application use cases for remote work. With cloud-based network management and Zero Touch Provisioning, IT can manage highly distributed environments more easily, troubleshoot issues impacting remote workers, and extend the SASE framework to enforce consistent policies across campus, branch, and remote work environments.

LEARN MORE

Explore the Aruba ESP work from home solution that leverages Aruba Central and Aruba Access Points.

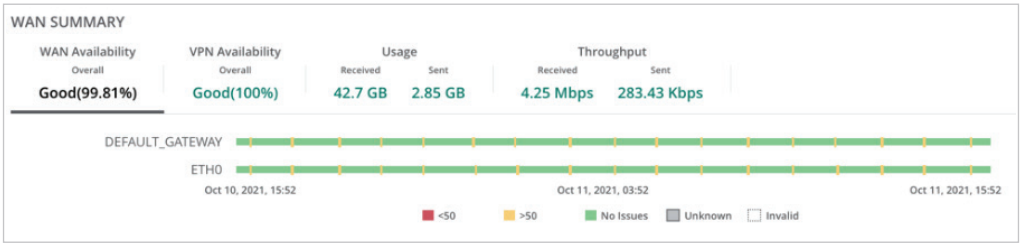

Figure 3. IT gains deep visibility and drilldowns into WAN health.

TB_WANtoSO-HOEdgeConnectMicrobranch_SK_112421 a00119570enw

Contact us at www.arubanetworks.com/contact