AT A GLANCE

GATEWAY USE CASES

Today's networks are reshaping operations to adapt to a post-Covid environment. Digital transformation has accelerated by five years or more.[1] Public cloud spending is up nearly 20% year over year.[2] And, nearly half of all employees will continue to work remotely at least some of the time.[3]

IT organizations are recognizing that to build an effective network, it requires an edge-to-cloud architecture that meets Zero Trust and SASE framework demands and the quality of service that users require. While cloud-managed networks can provide many of the control functions that have been traditionally provided by a wireless controller or gateway, some functions are best delivered locally. For this reason, many large campus environments and branch deployments are opting to use gateways to take advantage of SD-WAN features to optimize routing at the branch or to provide additional Wi-Fi capabilities.

This guide focuses on five common challenges where Aruba edge gateways can be deployed to better meet today's connectivity requirements.

WHAT ARE GATEWAYS?

Gateways are high-performance appliances that have evolved to support a wide range of use cases and can act as (1) SD-WAN device with intelligent routing and tunnel orchestration software or (2) the wireless control plane for greater security and scalability. Gateways are not a refresh of wireless controllers; they are expressly designed to be both cloud and IoT ready. It's important to note that gateways are not required for enterprise network connectivity but as seen in the use cases below, enhance performance, manageability, and scale.

Figure 1: Aruba's next-generation 9000 Series Gateways, like the 9012 shown above, are dual-purpose devices offering Wi-Fi controller capabilities or SD-Branch optimizations.

THE NEXT GENERATION ARUBAOS

ArubaOS 10 (AOS10) is the distributed network operating system working with Aruba Central[4] that controls Aruba Access Points (APs) and optional gateways. With AOS10, the same operating system supports AP-only mode, APs with gateways, and SD-Branch capabilities to provide a unified architecture for remote workers, mid-sized branches and large campuses. Benefits include greater scale, AIOps for faster problem resolution, enhanced security, and unified management.

USE CASE 1: LOWER COST/GREATER EFFICIENCY WITH SD-BRANCH

Challenge:

Managing hybrid WAN branches with MPLS and direct internet access is time consuming and error prone, yet enterprise SD-WAN solutions may be overkill for branch needs.

Solution:

Gateways have historically been valued for their campus Wi-Fi control functions, but they have a second, equally important use: SD-WAN gateways to support SD-branch. SD-branch technology provides a centrally-managed unified platform for SD-WAN, routing, security, LAN and Wi-Fi to deliver the ease of deployment, operations, and cost savings needed when managing large, distributed branch locations.

The SD-Branch orchestrator seamlessly updates the overlay network across multiple branch locations, data centers, public clouds, and SaaS – delivering a consistent user experience and policy enforcement. It provides:

- Greater visibility into performance across every uplink in a branch to improve the reliability, re-routing traffic over a secondary link as necessary
- Dynamic traffic steering based on roles, applications, and even IoT devices to prioritize traffic and improve user experience

- VPNC headend gateway to securely connect branches
- Enhanced branch security with stateful application-aware firewall, dynamic segmentation, intrusion detection, web content filtering/classification and integration with third-party cloud security providers
- Unified management across wired, wireless, and SD-branch
- Reduced footprint to a single WAN edge device

USE CASE 2: INCREASED SCALE

Problem:

IT operators struggle to manage wireless networks as they scale to thousands or tens of thousands of APs.

Solution:

In large campus environments, gateways can increase the scalability to tens of thousands of APs at a single site. The optimal gateway design is dependent several factors including the traffic patterns expected and site specifics.

Cloud-native software such as ArubaOS 10 – together with Aruba Central for centralized management and orchestration – means that there is less processing need on the gateways to manage clients and access points. Enterprises can use fewer gateways to manage very large environments with thousands of APs and devices.

USE CASE 3: ENHANCED SECURITY

Challenge:

Increase in security breaches. Nearly 80% of senior IT and IT security leaders believe their organizations lack sufficient protection against cyberattacks despite increased IT security investments to deal with distributed IT and work-from-home challenges.[5]

Solution:

Zero Trust Security embraces a scalable security methodology from edge to cloud for consistent role-based enforcement and context-aware controls. Gateways provide enhanced security capabilities needed to strengthen security posture.

Key elements include:

- **IDS/IPS intrusion detection system (IDS)** performs deep packet inspection in monitoring network traffic for malware and suspicious activity. When either is detected, the IDS alerts network managers, while the intrusion prevention system (IPS) takes immediate action to block threats from spreading to networked devices based on policies set in Aruba's ClearPass access control system.
- **Dynamic Segmentation** automatically enforces consistent policies across wired and wireless networks to keep traffic for any user or device separate and secure, regardless of the application or service. It establishes the gateway as a unified policy enforcement engine for traffic from AP or switch, and allows you to enforce deep packet inspection, policy firewalls, and bandwidth control on a user or device basis.
- **Guest WLANs** are created for guests, visitors, contractors, and any non-employee users who use the enterprise Wi-Fi network and are typically unencrypted. The gateway assigns the IP address for the guest clients. Captive portal or passphrase-based authentication methods can be set for this wireless network.
- **Centralized encryption** is performed by the gateway since access points do not perform encryption or decryption in the default tunnel mode. The APs receive encrypted wireless frame and package them into an IP tunnel to the gateway. At the gateway, the IP tunnel packet header is removed and decrypted. Because APs never have access to encryption keys, the attacker will not be able to break into Wi-Fi sessions that pass through the AP; only gateways require physical protection.

USE CASE 4: IMPROVED USER EXPERIENCE WHEN ROAMING

Challenge:

Poor experience when users move from one subnet to another, for example on a large campus.

Solution:

Consider the scenario: A company uses a single subnet per building on their campus. This means that the roaming domains are restricted to that building and application persistence when roaming across buildings is lost. Wireless devices are impacted with calls dropped during roaming and new sign-ons required when moving from building to building. To provide session persistence, you need to allow a station to maintain the same Layer 3 address when roaming throughout a multi-VLAN network. Gateways support tunneling so that two disparate networks can connect directly to one another, bypassing normal routing rules. This capability provides seamless roaming between Layer 2 and Layer 3 and improves the mobile user experience.

USE CASE 5: SIMPLIFIED MANAGEMENT

Challenge:

Managing hundreds or even thousands of APs at a single site can be a cumbersome and time-consuming manual process.

Solution:

With increased pressure on IT teams, simplified management is a key reason to deploy gateways. Gateways offer several advantages including dynamic segmentation (discussed under security), which eliminates manual configuration of multiple VLANs with a single VLAN deployment and provides context-aware policy enforcement for users and IoT. In addition, gateways include:

- **Dynamic RADIUS proxy** provides an alternative to adding all APs as NAS clients. When it is enabled, the gateway becomes a single anchor for RADIUS requests for all users regardless of the AP to which a user connects. All RADIUS packets are sourced with the gateway. The advantage with this model, is you only need to add the gateway IP address to the RADIUS client list on the authentication server.
- **Zero touch provisioning** supports plug-and-play deployments. Traditionally, the deployment of gateways and controllers was a multiple step process where the master controller information and local configurations were first pre-provisioned. After the managed device connected to the network, it established a secure tunnel to the master and downloaded the global configuration. Zero touch provisioning automates deployment of managed devices by accessing the location and global configuration and licenses and automatically provisioning itself. This is ideal for branch deployments with little or no onsite IT resources.
- **MultiZone** capability allows different gateways to work with the same AP infrastructure in a secure, segmented manner. Examples of this kind of separation are federal unclassified versus classified networks, separate operating networks, and employee/contractor/guest access. All APs authenticate against a primary zone defined and configured on the gateway and can be directed to authenticate with up to three other zones. Individual role-based access and policy enforcement rules can be implemented on a per zone basis, tailored to the requirements of that zone.

KEY TAKEAWAYS

With gateways, enterprises can deliver even greater power and enhanced flexibility to the Edge. The hardware can act as SD-Branch gateway for scalability, security, and WAN management or as a Wi-Fi gateway. Aruba offers small format and larger gateways as well as virtual gateways so enterprises can leverage their existing virtualization infrastructure if desired.

For more information, please refer to the Aruba Gateways and Controllers webpage or contact your Aruba sales representative.

[1] Gartner, July 2021
[2] Gartner, November 2020
[3] Gartner, July 2021
[4] Aruba Central is required because AOS10 is delivered as services hosted within Central.
[5] IDG Research Services survey commissioned by Insight Enterprises, February 2021

aruba
a Hewlett Packard Enterprise company

AAG_GatewayUseCases_100821 a00118174enw

Contact us at www.arubanetworks.com/contact