aruba
a Hewlett Packard Enterprise company

AT A GLANCE

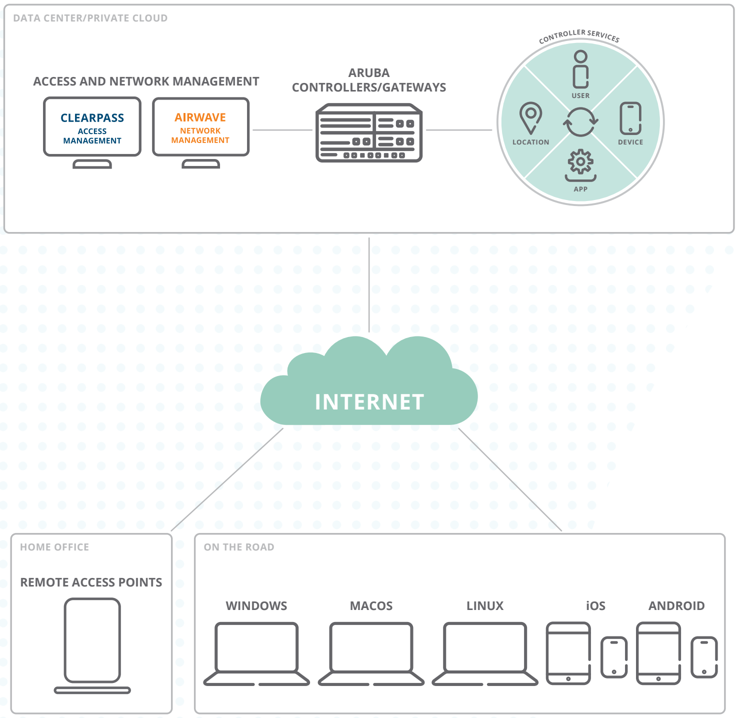
SECURING THE DISTRIBUTED WORKFORCE

Ensuring Connectivity and Availability through Security Best Practices

The way we work has changed dramatically over the last decade with teams now distributed remotely around the world. The ability for these teams to remotely connect, collaborate with other team members, and access the tools and data required to do their jobs has become mission-critical for every organization. Ensuring this connectivity and collaboration are done in a secure and compliant manner is a key concern as many IT organizations support an increasingly de-centralized and global workforce.

KEY CONSIDERATIONS

- **Secure Remote Connectivity** – Speed, simplicity and security are paramount to support an ever-growing remote workforce. Security and compliance considerations must offer maximum protection and risk reduction without hindering service level and availability expectations. Best practices such as network access control and segmentation must be based on the role of the user, vs where they are connecting from. Aruba solutions deliver transparent, yet secure experiences to users regardless of their location.
- **Speed and Ease of Deployment** – With a growing, decentralized workforce, enabling connectivity can be challenging. To deal with constantly changing external factors, as well as business drivers, large numbers of users must be brought online with little disruption to the network infrastructure or the business. Features like Aruba Zero-Touch Provisioning provide simple, on-site network setup, configuration and management without onsite IT support to make onboarding new remote users easy. VPN connectivity can be extended to users using VIA clients or RAPs which then connect back to an Aruba Gateway or Virtual Gateway for VPN termination.
- **Seamless User Experience** – Remote users need access to all of the applications, data and resources they have become accustomed to having at their fingertips. This means their experience remotely should be identical to their experience when they are physically in the office. Aruba solutions create this environment through solutions such as the Aruba Remote Access Point (RAP).



SPECIFIC SOLUTIONS THAT CAN HELP

Aruba Remote Access Points (RAPs)

Remote Access Points (RAPs) create a secure SSL/IPSec VPN connection back to an Aruba Mobility Controller over any wide-area transport, including 4G cellular, residential DSL, and cable networks with plug-and-play simplicity. Each RAP is secure by design, utilizing a factory certificate and TPM chip to connect, providing certificate-based authentication tied to each individual RAP. Additionally, all traffic is then encrypted via IPSec for securing data in transit.

Aruba VIA

VIA is a hybrid IPsec/SSL VPN client that automatically scans and selects the best, secure connection to terminate corporate-bound traffic. Unlike traditional VPNs which require dedicated hardware, Aruba integrates VPN services directly on existing Aruba secure infrastructure to simplify architecture and management. For military-grade security, VIA supports Suite B cryptography when used with the ArubaOS Advanced Cryptography (ACR) module. In this deployment model, mobile devices or desktop workstations can securely access networks that handle controlled unclassified, confidential and classified information.

Aruba Controllers and Gateways

Aruba Controllers and Gateways provide connectivity and security capabilities including VPN termination for remote workers. Aruba Controllers are high-performance appliances for the enterprise that provide optimized layer 3 roaming, scalability and redundancy for campus networks of any size. ArubaOS includes Policy Enforcement Firewall (PEF), AI-based RF optimization and Dynamic Segmentation that extends to Aruba's family of access switches. Aruba Gateways are cloud-managed appliances for the branch optimized for SD-WAN MPLS, Internet and cellular connectivity. Each gateway includes PEF, SD-WAN Orchestrator and branch level Dynamic Segmentation.

ClearPass Policy Manager

Aruba's ClearPass provides complete visibility and role-based access control for IoT, BYOD, corporate devices, as well as employees, contractors and guests across any multivendor wired, wireless and VPN infrastructure. Aruba ClearPass policies are enforced by the Aruba Policy Enforcement Firewall (PEF) – even for remote users connecting using Aruba VIA or an Aruba Remote Access Points (RAPs).

Policy Enforcement Firewall

PEF is also the underlying technology that enables Dynamic Segmentation, a key technical solution within Aruba's Experience Edge that simplifies and secures wired and wireless networks. This capability extends to remote users giving administrators critical security visibility, control and enforcement capabilities.

aruba
a Hewlett Packard
Enterprise company

AAG_SecuringDistributedWorkforce_051920 a00099832enw

Contact Us Share