DATA SHEET

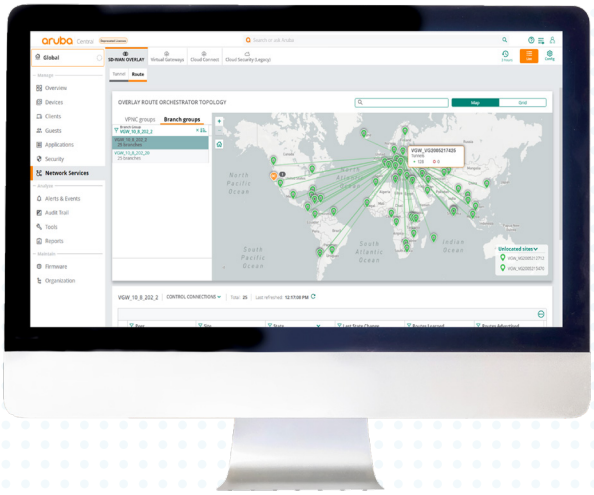
ARUBA EDGECONNECT SD-BRANCH

Address the entire remote branch user experience from edge-to-cloud with unified management, AIOps and security for wired, wireless and WAN networking

As enterprises shift to cloud-based services and users connect from anywhere, Software-Defined WAN (SD-WAN), a key component of Security Access Service Edge (SASE), is the answer to support cloud-based architectures and protect organizations from increasing cybersecurity risks.

Aruba EdgeConnect SD-Branch is an all-in-one solution that enables organizations to seamlessly deploy networking and security capabilities in branches and simplify local operations. The solution benefits from a tight integration with other Aruba technology components such as wireless networking and switching, managed via a single console, Aruba Central. It offers advanced security features such as IDS/IPS and web content filtering and integrates with multiple leading SSE (Security Service Edge) vendors to form a best-of-breed SASE architecture. Thanks to its advanced SD-WAN capabilities, Aruba EdgeConnect SD-Branch optimizes routing decisions and improves visibility across the LAN and WAN edge. Security features based on end-user roles, device type, and location context combined with intelligent LAN and WAN management make Aruba EdgeConnect SD-Branch solution ideal for branches in distributed enterprises.

Any organization with lean and centralized network teams can improve the time to deploy, manage and maintain branch networks, while enhancing the user experience and business operations. Aruba EdgeConnect SD-Branch Gateways are cloud-managed and enable organizations to deploy a full software defined branch (SD-Branch) solution.



KEY FEATURES

- Best-of-breed SASE with orchestrated SSE integrations
- Policy enforcement firewall, Deep Packet Inspection, and IDS/IPS
- Web content classification, URL filtering, IP reputation, and geolocation filtering
- Scalable, cloud-native, multitenant orchestration with support of hub and spoke, hub mesh and branch mesh topologies
- High performance branch gateways with ZTP
- Licenses with unrestricted bandwidth for every SD-WAN gateway
- Policy-based routing for 3700+ applications and protocols
- Dynamic path optimization for high priority SaaS apps
- Optimized for Microsoft 365
- Virtual gateways and hub routing available for AWS, Azure and Google Cloud

INTELLIGENT LAN AND WAN MANAGEMENT

Through simplified workflows, managing a WAN can be completely orchestrated to improve the speed of deployment, network performance, and ongoing configuration changes. Aruba Central, an AI-powered network operations, assurance, and security platform, provides a single point of control to oversee every aspect of wired and wireless LAN, SD-WAN, and cloud across campus, branch, remote, and data center locations. Cloud advantages make it easy to configure and deploy and see data from Aruba branch gateways, headend gateways, and virtual gateways from anywhere. There is no on-premises management equipment to update or maintain.

Additionally, Aruba Central includes a full-service AIOps solution that automates common troubleshooting activities. AIOps include Network Insights to automatically diagnose common network issues, AI Search to search troubleshooting

tips and solution guides using natural language, and AI Assist to automatically collect log files and troubleshooting data. Aruba Central also offers third-party integrations with other IT platforms through APIs and webhooks.

CLOUD-BASED ORCHESTRATION

Based on a cloud-native, multi-tenant architecture, Aruba Central provides end-to-end orchestration to easily distribute routes and build scalable and secure tunnels. WAN links are automatically discovered, and tunnels are orchestrated based on business and topological needs. The orchestrator only sets up tunnels between sites that need them. Similarly, routes are only advertised between gateways that have reachability between each other. The orchestrator also simplifies the deployment of virtual gateways within Amazon AWS, Google Cloud and Microsoft Azure public cloud infrastructure by automating cloud discovery, onboarding, and management.

UNRESTRICTED BANDWIDTH

Unlike other SD-WAN vendors, Aruba's EdgeConnect SD-Branch solution offers unrestricted bandwidth per every gateway license.[1] This means you have access to full hardware performance capabilities right out of the box – no upgrade purchases required.

SD-BRANCH GATEWAYS

Gateways for Branch

Aruba Branch Gateways are designed to support multiple WAN connections across broadband, MPLS, and LTE cellular links. The 9004-LTE gateway includes integrated hardware-based LTE. All other Branch Gateways support USB port-based LTE. Software features include the ability to route and prioritize traffic being sent to the data center, public cloud infrastructure or the Internet. Each gateway also supports High Availability (HA) requirements (e.g., active/active and active/standby), making it ideal for sites that need full redundancy.

Gateways for Headend

Aruba Gateways deployed in headend/data center environments act as VPN concentrators (VPNCs) to terminate traffic from branch sites, microbranch (access points only) sites and VPN end points. These gateways offer support for thousands of branch sites. For example, one or more headend gateways can be used to terminate IPsec tunnels established from branch gateways in a hub-and-spoke topology.

Gateways for Public Cloud

Aruba virtual gateways are deployed in public cloud infrastructures, such as a Microsoft Azure Virtual Network (VNET), Amazon Web Services virtual private cloud (AWS VPC) or Google Cloud Virtual Private Cloud (Google VPC). These gateways serve as a virtual instance of a headend gateway, and enable seamless and secure connectivity for all branch and data center locations connecting to public clouds. Virtual gateways support public Internet and private connections such as Direct Connect.

Virtual gateways are managed by Aruba Central and include full orchestration that completely automates VNET/VPC discovery, subnet management, gateway onboarding, HA configuration and status monitoring.

Virtual gateways support up to 4 Gbps of throughput, with 1, 3, and 5 year subscription options.

SD-WAN Integration with Public Multi-Cloud Network

Aruba SD-Branch gateway provides orchestrated secure branch connectivity directly to public cloud provider global backbone networks. This greatly simplifies the SD-WAN overlay by connecting branch locations directly to regional points of presence (POPs) providing access to cloud resources within a region and across regions. The overlay also supports branch-to-branch communication without virtual gateways at each VPC. Aruba Cloud Connect, a service within Aruba Central, provides a single dashboard to streamline the management and operation of SD-WAN integrations with AWS Transit Gateway Network Manager and Microsoft Azure Virtual WAN.

MICROSOFT FEATURES

Office 365, Teams and Skype for Business Aruba's integration with Microsoft enables unique application insight that detects Office 365, Teams and Skype for Business traffic and then prioritizes them over less critical applications. Aruba Central also includes specific call quality heuristics for additional visibility.

Microsoft preferred solution

Aruba Virtual Gateways are a Microsoft preferred solution on the Azure Marketplace. This means the gateway application has been validated by Microsoft experts as having proven competencies and capabilities that meet customer needs.

[1] Except for virtual gateways in the cloud

POLICY-BASED ROUTING AND SUPPORTED PROTOCOLS

With Policy-based Routing (PBR), traffic can be routed across multiple private or public WAN uplinks based on application type and link health, device profile, user role, and destination. Supported protocols include BGP, OSPF and static routes.

SaaS OPTIMIZATION

SaaS Express ensures high-priority SaaS applications such as Microsoft 365 (Office 365), Dropbox, and Slack are operating at the highest level of performance when transiting over multiple Internet provider links. The solution uses the DPI engine to classify applications on the first packet. SaaS Express connects users from a branch site to SaaS applications in a seamless and secure way, and constantly monitors the SaaS Quality of Experience (QoE). The interface includes a drill-down dashboard so the user can identify and perform root-cause analysis on SaaS performance-related issues.

This feature requires the Aruba Central SD-WAN Advanced License. For more information, please refer to the latest Aruba Central Order Guide.

KEY WAN FEATURES

Overlay and Hybrid WAN Management

EdgeConnect SD-Branch managed by Aruba Central introduces a new architecture that provides a network overlay for WAN connections to improve visibility and control across private and public connections (hybrid WAN).

Orchestrated SD-WAN Topologies

Aruba Central provides route and tunnel orchestration to build different topologies (Hub and Spoke, Hub Mesh, Branch Mesh) that simplify the connectivity between all locations while providing resiliency and maximum flexibility. Hub and Spoke topologies easily allow branches to take the shortest path to the right resources, Hub Mesh allows building a fully transitive backbone network, and Branch Mesh seamlessly enables direct communications between network spokes (or branches).

Site-to-Site VPNs

Secure connections can also be established from one branch site to another over a public Internet connection. This allows users from different locations to access network resources hosted within the corporate network without going through the data center.

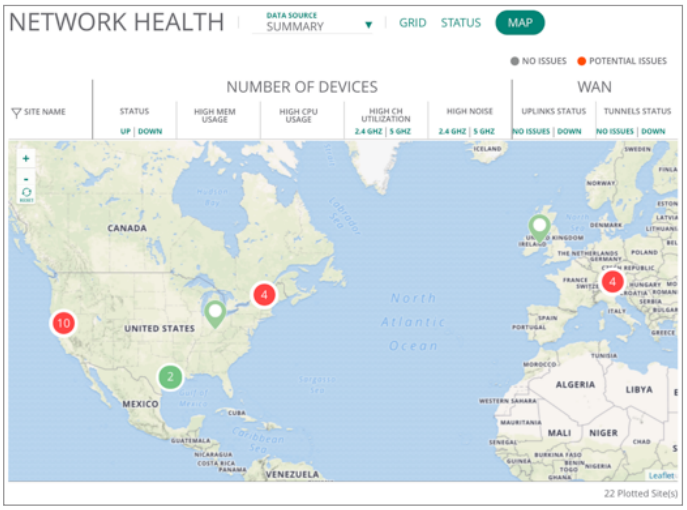


Figure 1: Aruba Central WAN Health Dashboard

Dynamic Path Steering (DPS)

WAN traffic can be automatically routed over the best available uplink based on characteristics, such as WAN throughput, latency, jitter and packet loss. The solution also supports Forward Error Correction (FEC), to compensate any packet loss during traffic flow, improving application performance.

WAN Visibility

With deep packet inspection technology, Aruba Central provides monitoring for application traffic that enters and exits a branch network – regardless of the uplink type. This makes it easy for IT to manage WAN environments that increasingly utilize public WAN connections.

WAN Compression

Ideal for use during periods of network congestion, this WAN compression feature allows IT to send more traffic through the same WAN circuit at any given moment or timeframe.

Unrestricted Bandwidth

Aruba Central licenses provide access to the full bandwidth specification for each gateway. No additional license upgrades required.

KEY CONFIGURATION FEATURES

Simplified Installation Wizard

For easy configuration of branch gateways, Aruba Central provides users with a step-by-step navigation that simplifies provisioning of the network.

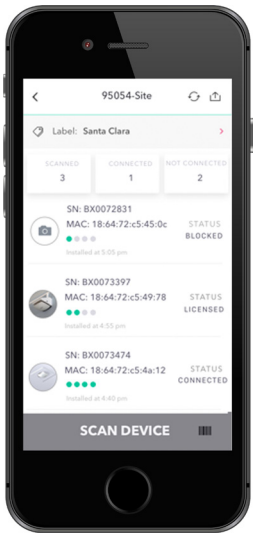


Figure 2: Example of Aruba's mobile installer app for device onboarding.

Configuration Hierarchy

Network settings can be pre-configured and customized in Aruba Central based on branch-specific requirements. Zero Touch Provisioning (ZTP) provides an easy and error-free deployment model.

Zero Touch Provisioning (ZTP)

Using Zero Touch Provisioning, the hardware gateways can be factory-shipped and deployed onsite using Aruba Activate™, a cloud-based activation service that seamlessly works with Aruba Central. Settings can be applied based on configuration and other network-specific requirements.

Simple, mobile provisioning

Aruba's mobile installer app allows on-site personnel to easily onboard gateways. A central IT team can verify device location, licenses, and status with no additional steps required. This is available for iOS and Android.

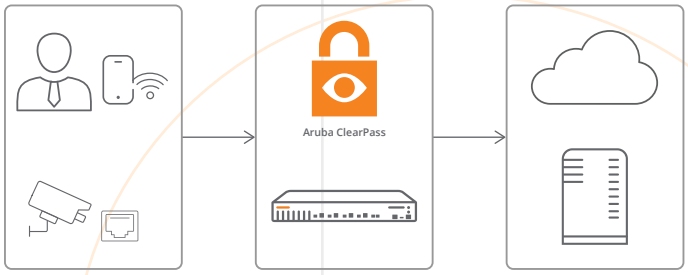


Figure 3: Segment mobile and IoT traffic using Aruba

KEY SECURITY FEATURES

Dynamic Segmentation

To simplify and better secure wired and wireless network access, the branch gateway can automatically enforce per-user and per-device roles on wired and wireless networks. Integration with ClearPass Policy Manager allows for centralized role and policy management. This ensures consistent policy regardless of user role and device type, and eliminates the need to configure unnecessary SSIDs, ACLs, VLANs and subnets at every node in the network. Aruba Client Insights accurately identifies and classifies all wired and Wi-Fi connected user and IoT endpoints with AI-based insights for policy enforcement.

Large organizations often operate across complex, globally distributed networks. Aruba Central NetConductor automatically builds and orchestrates intelligent overlays using EVPN, VXLAN and BGP protocols, enabling role-based micro-segmentation and policy enforcement across complex, distributed networks. For more information on Dynamic Segmentation, please refer to the solution overview.

Policy Enforcement Firewall

Included within the Foundation license, PEF allows for wired and wireless user and application traffic to be sent to a branch gateway through GRE tunnels for inspection.

Enforcement of policies based on user role, device type, application and location is accomplished through Aruba Dynamic Segmentation.

Application visibility and control

Also included in the Foundation license is an application visibility feature that uses Deep Packet Inspection (DPI) technology to evaluate and optimize performance and QoS policies for over 3700 applications and protocols, including encrypted and hidden traffic.

Web content filtering

The Web Content Classification (WebCC) bundle is part of the Foundation license and includes URL filtering, IP reputation, and geolocation filtering. URL filtering classifies more than 80 site categories by leveraging machine learning for speed and accuracy. The IP reputation service uses contextual and behavioral trends to determine an IP Reputation Index and makes a classification into five reputation tiers including

Trustworthy, Low Risk, Moderate Risk, Suspicious, and High Risk. The geolocation filtering service associates source/destination IP addresses with location to allow or drop communications with certain known malicious countries.

Firewall Logging

The Aruba Central firewall logging dashboard provides graphical and tabular displays of the effectiveness of gateway-enforced firewall rules across the corporate network. It starts with a global view of gateways with most blocked sessions. From there, drill-down for detailed blocked session information by source and destination IP address, and policy rule being enforced. Firewall Logging is also included in the Foundation license.

Threat Defense with IDS/IPS

To improve security against a growing attack surface, gateways deployed in SD-WAN mode add role and identity-based intrusion detection and prevention capabilities (IDS/IPS) on top of existing security features.

An advanced security dashboard provides IT Teams with network-wide visibility, multi-dimensional threat metrics, threat intelligence data, correlation and incident management. This feature requires the appropriate Aruba Central security subscription license. Threat events can also be streamed to Security Information and Events Management (SIEM) systems such as Splunk to provide advanced visibility and monitoring.

Best-of-breed SASE

Aruba EdgeConnect SD-Branch integrates with leading SSE vendors to enable organizations to build a best-of-breed SASE architecture and provide freedom of choice. The orchestration is fully automated using the Aruba Cloud Connect service, enabling organizations to quickly deploy multiple cloud-security partners. Aruba gateways assume the role of an on-premises agent of centrally-hosted firewalls such as those provided by Palo Alto Networks and Check Point Software, or web security gateways such as Zscaler and Symantec.

TECHNICAL SPECIFICATIONS*

BRANCH GATEWAYS (SMALL AND MEDIUM)

Features	9004	9012[3]	7005	7008	7010	7024
Deployment mode	Small/Medium	Small/Medium	Small	Small	Medium	Medium
Maximum clients	Up to 2,048[4]	Up to 2,048[4]	Up to 1,024[4]	Up to 1,024[4]	2,048	2,048
Maximum VLANs	4096	4096	4096	4096	4096	4096
Firewall throughput	4 Gbps	6 Gbps	2 Gbps	2 Gbps	8 Gbps	8 Gbps
Encrypted throughput (AES-CBC)	4 Gbps	4 Gbps	1.2 Gbps	1.2 Gbps	2.6 Gbps	2.6 Gbps
Active firewall sessions	64K/128K[5]	64K/128K[5]	64K	64K	32K	32K
IDS/IPS throughput	Up to 1.1 Gbps[2]	Up to 1.1 Gbps[2]	N/A	N/A	N/A	N/A
WAN/LAN Interfaces	4	12	4	8	16	24
PoE in/out	–	Out; 120W	In; E0	Out; 100W	Out; 150W	Out; 400W
USB (WAN)	Yes (1); USB 3.0	Yes (2); USB 3.0	Yes (1); USB 2.0	Yes (2); USB 2.0	Yes (2); USB 2.0	Yes (1); USB 2.0
Form factor/ footprint	Desktop/1RU[1]	Desktop/1RU	Desktop/1RU	Desktop/1RU	1RU	1RU

[1] RU can support two 9004 gateways side-by-side using an optional mount kit
[2] IDS/IPS throughput results based upon iMix traffic with zero loss input for AOS SD-WAN image 2.3 or AOS 10.2
[3] 9012 can be deployed as branch gateway or Headed Gateway with IDS/IPS (with appropriate license)
[4] The 9004 and 7005/7008 offers a base capacity license for up to 75 clients.
[5] 64K sessions with IDS/IPS and 128K without IDS/IPS.

BRANCH GATEWAYS (LARGE)

Features	7030	7210	7220	7240XM	9240
Deployment mode	Large	Large	Large	Large	Large
Maximum clients	4096	16K	24K	32K	64K
Maximum VLANs	4096	4096	4096	4096	4096
Firewall throughput	8 Gbps	20 Gbps	40 Gbps	40 Gbps	20 Gbps
Encrypted throughput (AES-CBC)	2.6 Gbps	6 Gbps	20 Gbps	30 Gbps	15 Gbps
Active firewall sessions	64K	2M	2M	2M	4M
WAN/LAN Interfaces	8 (combo)	2 (combo)	2 (combo)	2 (combo)	4 (25G SFP)
USB (WAN)	Yes (1); USB 2.0	Yes (1); USB 2.0	Yes (1); USB 2.0	Yes (1); USB 2.0	Yes (1); USB 3.0
Form factor/footprint	1 RU	1 RU	1 RU	1 RU	1 RU

HEADEND GATEWAYS								
Features	**7010/7024**	**7030**	**7210**	**7220**	**7240XM**	**7280**	**9012**	**9240**
Deployment mode	VPN Concentrator (VPNC)	VPNC	VPNC	VPNC	VPNC	VPNC	VPNC	VPNC
Encrypted through-put (AES-CBC)	2.6 Gbps	2.6 Gbps	7 Gbps	22 Gbps	30 Gbps	45 Gbps	3.5 Gbps	19.4 Gbps
WAN compression performance	2.5 Gbps	2.5 Gbps	10 Gbps	10 Gbps	10 Gbps	10 Gbps	1.7 Gbps	-
Maximum tunnels	512	512	1,024	4,096	6,144	8,192	1,024	8,192
Route scale	3,000	6,000	6,000	20,000	30,000	30,000	12,000	32,000
Form factor/footprint	1RU	1RU	1RU	1RU	1RU	1RU	1RU	1RU

*For complete hardware specifications, please see the related datasheets.

VIRTUAL GATEWAYS	PUBLIC CLOUD INFRASTRUCTURE			
Features	**Amazon Web Services (AWS)**	**Microsoft Azure**	**Google Cloud**	**VMware ESXi**
Deployment mode	EC2 instance in VPC	Linux VM instance in VNET	VM instance in VPC	VM instance using vSphere
Virtual Gateway models	500 Mbps, 2 Gbps, 4 Gbps	500 Mbps, 2 Gbps, 4 Gbps	500 Mbps, 2 Gbps, 4 Gbps	500 Mbps, 2 Gbps, 4 Gbps
Firewall throughput	500 Mbps, 2 Gbps, 4 Gbps	500 Mbps, 2 Gbps, 4 Gbps	500 Mbps, 2 Gbps, 4 Gbps	500 Mbps, 2 Gbps, 4 Gbps
Virtual CPUs	4, 8 and 16 vCPU	4, 8 and 16 vCPU	4, 8 and 16 vCPU	4, 8 and 16 vCPU
Memory	7.5 GB, 15 GB and 30 GB	14 GB, 16 GB and 32 GB	16 GB, 32 GB and 64 GB	7 GB, 15 GB and 30 GB
Storage	15 GB, 30 GB and 60 GB	15 GB, 30 GB and 60 GB	15 GB, 30 GB and 60 GB	15 GB, 30 GB and 60 GB
Number of interfaces	4 (including a management interface)			
Maximum tunnels (per model)	1600, 4096 and 8192	1600, 4096 and 8192	1600, 4096 and 8192	1600, 4096 and 8192
Infrastructure costs	BYOL + hosted service costs including compute, storage and egress data.			N/A

For additional information on ordering and full gateway hardware specifications, please refer to:

- Aruba Central Ordering Guide
- 7000 Series Mobility Controller Data sheet
- 7200 Series Mobility Controller Data sheet
- 9004 Series Gateways Data sheet
- Aruba Central Virtual Gateway Deployment Guide

DS_ArubaSD-WAN_RVK_060623 a00047570enw

Contact us at www.arubanetworks.com/contact