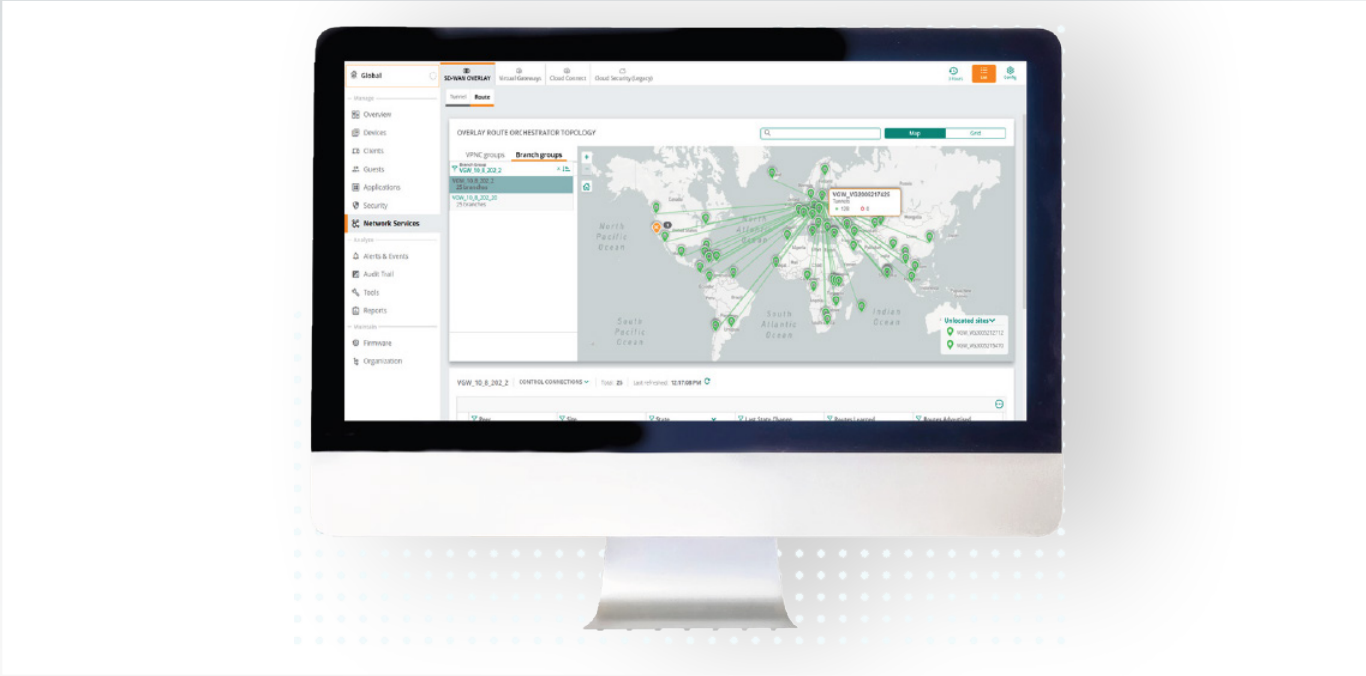
HPE aruba networking

Data sheet



HPE Aruba Networking 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

HPE

Key features

— Unified SASE with HPE Aruba Networking SSE or 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 zero touch provisioning (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 Amazon Web Services (AWS), Microsoft Azure, and Google Cloud

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 hybrid working, 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.

HPE Aruba Networking 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 HPE Aruba Networking (security service edge) SSE to form a unified SASE platform while offering advanced built-in security features such as IDS/IPS and web content filtering. It also integrates with other technology components from HPE Aruba Networking such as wireless networking and switching, managed through a single console, HPE Aruba Networking Central, providing a consolidated, secure network infrastructure. Thanks to its advanced SD-WAN capabilities, 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 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. EdgeConnect SD-Branch gateways are cloud-managed and enable organizations to deploy a full software-defined branch (SD-Branch) solution.

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. HPE Aruba Networking 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 branch gateways, headend gateways, and virtual gateways from HPE Aruba Networking. There is no on-premises management equipment to update or maintain.

Additionally, HPE Aruba Networking Central includes a full-service AIOps solution that automates common troubleshooting activities. AIOps include AI 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. HPE Aruba Networking Central also offers third-party integrations with other IT platforms through APIs and webhooks.

Cloud-based orchestration

Based on a cloud-native, multitenant architecture, HPE Aruba Networking 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, the HPE Aruba Networking EdgeConnect SD-Branch solution offers unrestricted bandwidth per every gateway license[1]. This means organizations have access to full hardware performance capabilities right out of the box—no upgrade purchases required.

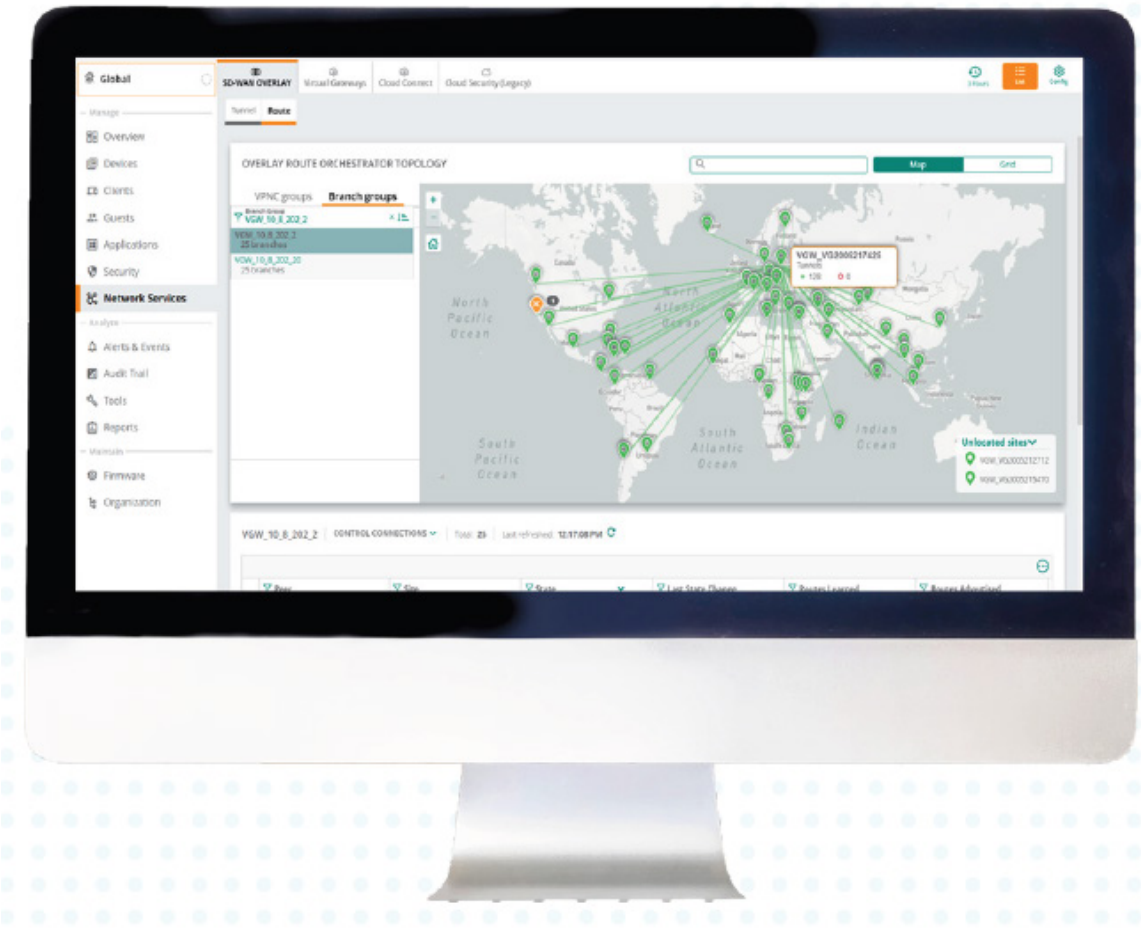


Figure 1. HPE Aruba Networking EdgeConnect SD-Branch

[1] Except for virtual gateways in the cloud.

SD-Branch gateways

Gateways for branch

HPE Aruba Networking SD-Branch Gateways are designed to support multiple WAN connections across broadband, MPLS, and cellular links. The HPE Aruba Networking 9004-LTE Gateway includes integrated hardware-based LTE. Additionally, by using the HPE Aruba Networking 100 Series 5G Cellular Bridge or a plug and play HPE Aruba Networking USB LTE modem, enterprises can fully leverage 5G or LTE connections on any branch gateways. The 5G Cellular Bridge can also be mounted anywhere and powered through power over ethernet (PoE), for enhanced coverage and signal quality.

The use of HPE Aruba Networking Central ensures optimal connectivity to critical applications and resources, even when primary connectivity experience a failure. It enables organizations 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 (for example, active/active and active/standby) making it ideal for sites that need full redundancy.

Gateways for headend

HPE Aruba Networking 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

HPE Aruba Networking 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 HPE Aruba Networking 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 multicloud network

HPE Aruba Networking EdgeConnect 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. Cloud Connect, a service within HPE Aruba Networking 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

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

Microsoft preferred solution

HPE Aruba Networking 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.

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, 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 HPE Aruba Networking Central SD-WAN Advanced License. For more information, refer to the latest HPE Aruba Networking Central subscriptions order guide.

Key WAN features

Overlay and hybrid WAN management

HPE Aruba Networking EdgeConnect SD-Branch managed by HPE Aruba Networking 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

HPE Aruba Networking 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.

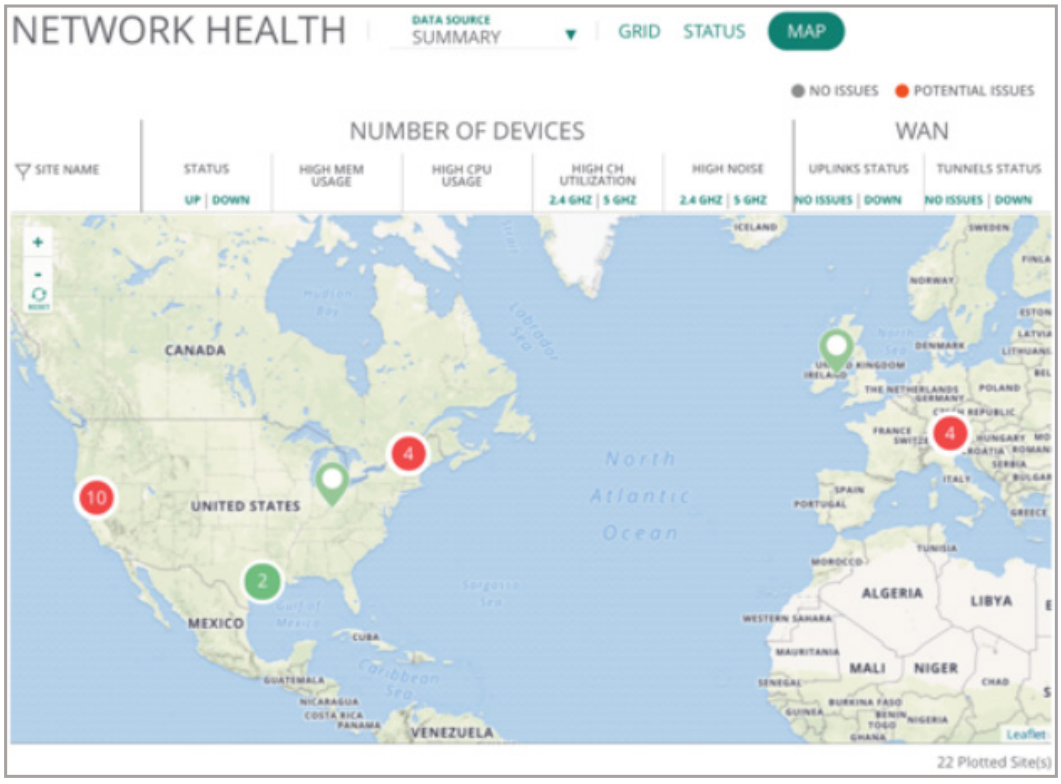


Figure 2. HPE Aruba Networking Central WAN Health dashboard

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, HPE Aruba Networking 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 time frame.

Unrestricted bandwidth

HPE Aruba Networking 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, HPE Aruba Networking Central provides users with a step-by-step navigation that simplifies provisioning of the network.

Configuration hierarchy

Network settings can be preconfigured and customized in HPE Aruba Networking 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 using HPE Aruba Networking Central. Settings can be applied based on configuration and other network-specific requirements.

Simple, mobile provisioning

The HPE Aruba Networking 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™.

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 HPE Aruba Networking 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.

HPE Aruba Networking 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. HPE Aruba Networking Central NetConductor automatically builds and orchestrates intelligent overlays using EVPN, VXLAN and BGP protocols, enabling role-based microsegmentation and policy enforcement across complex, distributed networks. For more information on HPE Aruba Networking dynamic segmentation, refer to the solution overview.

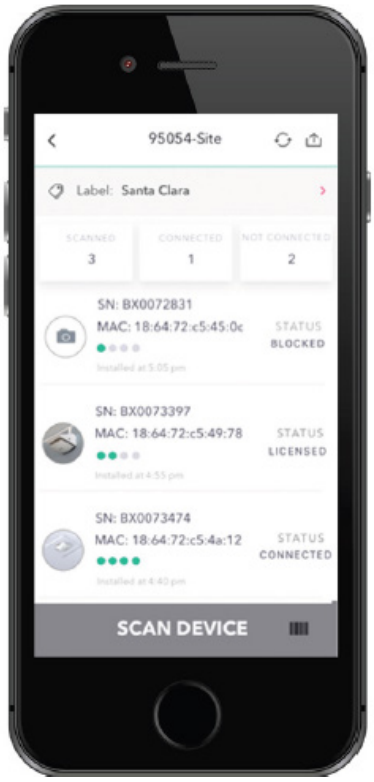


Figure 3. Example of the HPE Aruba Networking mobile installer app for device onboarding

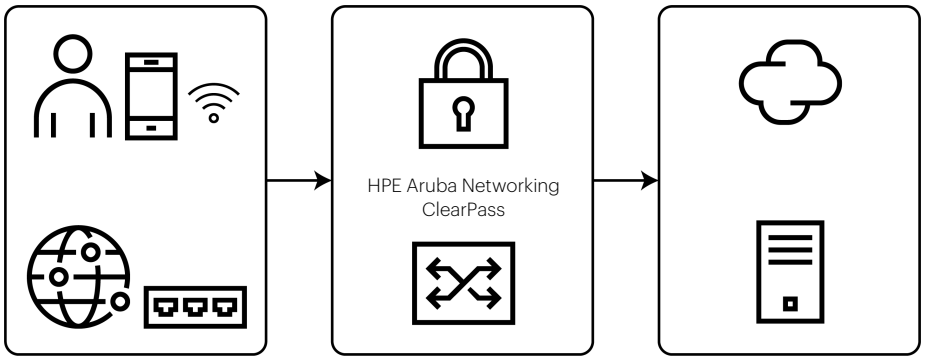


Figure 4. Isolate mobile from IoT traffic with dynamic segmentation

Policy Enforcement Firewall (PEF)

Included within the Foundational 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 dynamic segmentation.

Application visibility and control

Also included in the Foundational 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 Foundational 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 HPE Aruba Networking 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 Foundational 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 systems capabilities (IDS/IPS) on top of existing security features.

An advanced security dashboard provides IT teams with network-wide visibility, multidimensional threat metrics, threat intelligence data, correlation and incident management. This feature requires the appropriate HPE Aruba Networking 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.

Unified SASE

To enable hybrid working and tackle the security challenges of cloud computing, HPE Aruba Networking EdgeConnect SD-Branch integrates with HPE Aruba Networking SSE to build a unified SASE platform, meeting the increasing demand for integrated networking and security. As a unified SASE solution, it is easy to deploy thanks to a single, tightly integrated solution, including a simplified management.

HPE Aruba Networking SSE provides least-privilege access to users and authorized third-party users thanks to agent and agentless zero trust network access (ZTNA). It protects internet users against cyber threats with secure web gateway (SWG), and ensures sensitive data remains protected in SaaS applications while preventing data from being lost with cloud access security broker (CASB). It offers an enhanced digital experience and productivity with digital experience monitoring (DEM).

ZTNA, SWG, CASB, and DEM share a single codebase where all policies are managed from a single user interface, making access control incredibly simple for IT admins. Additionally, the solution harmonizes access across the world through a cloud-backbone of Amazon Web Services (AWS), Microsoft Azure, Google Cloud, and Oracle® Cloud.

EdgeConnect SD-Branch also seamlessly integrates with third-party security vendors. The orchestration is fully automated using the Cloud Connect service from HPE Aruba Networking. HPE Aruba Networking 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*

HPE Aruba Networking Branch Gateways (small and medium)						
Features	**9004**	**9012[2]**	**7005**	**7008**	**7010**	**7024**
Deployment mode	Small/Medium	Small/Medium	Small	Small	Medium	Medium
Maximum clients	Up to 2048[3]	Up to 2048[3]	Up to 1024[3]	Up to 1024[3]	2048	2048
Maximum VLANs	128	128	127	127	127	127
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	128K[4]	128K[4]	64K	64K	32K	32K
IDS/IPS throughput	Up to 1.1 Gbps[5]	Up to 1.1 Gbps[5]	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 (1); 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[6]	Desktop/1RU	Desktop/1RU	Desktop/1RU	1RU	1RU

[2] 9012 can be deployed as branch gateway or Headend Gateway with IDS/IPS (with appropriate license)

[3] The 9004 and 7005/7008 offers a base capacity license for up to 75 clients

[4] 64K when IDS/IPS is enabled with AOS lower than 10.5

[5] IDS/IPS throughput results based upon iMix traffic with zero loss input for AOS SD-WAN image 2.3 or AOS 10.2

[6] RU can support two 9004 gateways side-by-side using an optional mount kit

HPE Aruba Networking Branch Gateways (large)							
Features	**7030**	**7210**	**7220**	**7240XM**	**9106**	**9114**	**9240**
Deployment mode	Large	Large	Large	Large	Large	Large	Large
Maximum clients	4096	16K	24K	32K	8K	10K	32K
Maximum VLANs	255	4096	4096	4096	4096	4096	4096
Firewall throughput	8 Gbps	20 Gbps	40 Gbps	40 Gbps	15 Gbps	20 Gbps	20 Gbps
Encrypted throughput (AES-CBC)	2.6 Gbps	6 Gbps	20 Gbps	30 Gbps	10 Gbps	20 Gbps	20 Gbps
IDS/IPS	N/A	N/A	N/A	N/A	2.5 Gbps	4 Gbps	6 Gbps
Active firewall sessions	64K	2M	2M	2M	2M	2M	4M
WAN/LAN Interfaces	8 (combo)	2 (combo)	2 (combo)	2 (combo)	2 (combo); 2 x 10G SFP+; 2 x 1G (PoE 60W)	4 (combo); 4 x 10G SFP+	4 x 25G SFP28
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	Yes (2); USB 3.0	Yes (2); USB 3.0
Form factor/ footprint	1 RU	1 RU	1 RU	1 RU	1 RU	1 RU	1 RU

* For complete hardware specifications, see the related datasheets.

HPE Aruba Networking Headend Gateways										
Features	**7010/7024**	**7030**	**7210**	**7220**	**7240XM**	**7280**	**9012**	**9106**	**9114**	**9240**
Deployment mode	VPN Concentrator (VPNC)	VPNC	VPNC	VPNC	VPNC	VPNC	VPNC	VPNC	VPNC	VPNC
Encrypted throughput (AES-CBC)	2.6 Gbps	2.6 Gbps	7 Gbps	22 Gbps	30 Gbps	45 Gbps	3.5 Gbps	10 Gbps	20 Gbps	20 Gbps
Maximum tunnels	256	512	1024	4096	6144	8192	512	8000	16,000	32,000
Route scale	4K	4K	8K	16K	32K	32K	12K	12K	12K	32K
Form factor/ footprint	1RU	1RU	1RU	1RU	1RU	1RU	1RU	1 RU	1RU	1RU

HPE Aruba Networking 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 VMware 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)	4 (including a management interface)	4 (including a management interface)	4 (including a management interface)
Maximum tunnels (per model)	512, 4096, and 8192	512, 4096, and 8192	512, 4096, and 8192	512, 4096, and 8192
Infrastructure costs	BYOL + hosted service costs including compute, storage and egress data	BYOL + hosted service costs including compute, storage and egress data	BYOL + hosted service costs including compute, storage and egress data	N/A

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

— HPE Aruba Networking Central subscriptions ordering guide
— HPE Aruba Networking 7000 Series Mobility Controller data sheet
— HPE Aruba Networking 7200 Series Mobility Controller data sheet
— HPE Aruba Networking 9000 Series Gateways data sheet
— HPE Aruba Networking Virtual Gateway deployment guide

Visit HPE.com

Chat now

© Copyright 2025 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Google Cloud, Google, and Android are registered trademarks of Google LLC. Linux is the registered trademark of Linus Torvalds in the U.S. and other countries. VMware ESXi and VMware vSphere are registered trademarks or trademarks of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. Azure, Microsoft, and Skype are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Oracle is a registered trademark of Oracle and/or its affiliates. All third-party marks are property of their respective owners.

a00047570ENW, Rev. 3

HEWLETT PACKARD ENTERPRISE

hpe.com