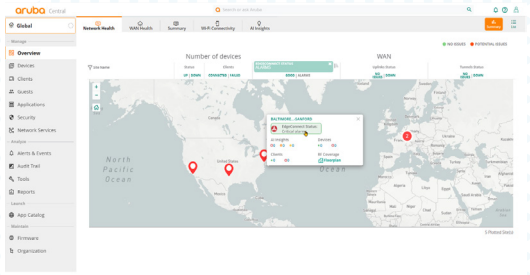
DATA SHEET

ARUBA EDGECONNECT SD-WAN PLATFORM

As cloud-based application adoption continues to accelerate, geographically distributed enterprises increasingly view SD-WAN as critical to connecting users to applications.

Aruba EdgeConnect SD-WAN physical appliances shown here are also available as virtual appliances.



Aruba Central provides the ability directly launch Aruba WAN Orchestrator and view the enterprise-wide SD-WAN topology, health status, and alarms of all Edge-Connect SD-WAN appliances in the network

As enterprise applications migrate from the corporate data center to the cloud, private line connections such as multi-protocol label switching (MPLS) have proven to be overly rigid and expensive. With greater reliance on the internet, the opportunity to achieve "cloud speed" is better served by integrating broadband services into the WAN transport mix.

The Aruba EdgeConnect SD-WAN platform enables enterprises to improve application performance and dramatically reduce the cost and complexity of building a WAN by leveraging broadband to connect users to applications.

Additionally, Aruba EdgeConnect SD-WAN provides a secure network foundation for Zero-Trust and SASE frameworks. The solution includes a next-generation firewall with fine-grained segmentation and identity-based access control capabilities, as well as IDS/IPS and DDoS defense to protect branch locations from malicious activities. The solution also tightly integrates with leading cloud security providers to build a best-of-breed SASE architecture.

Recognized by an independent, third-party organization, Aruba EdgeConnect SD-WAN has earned the **Secure SD-WAN certification from ICSA Labs** thanks to its advanced SD-WAN and security features.

ICSA Labs provides third-party testing and certification of security and health IT products, as well as network-connected devices, to measure product compliance, reliability, and performance.

ARUBA EDGECONNECT SD-WAN PLATFORM

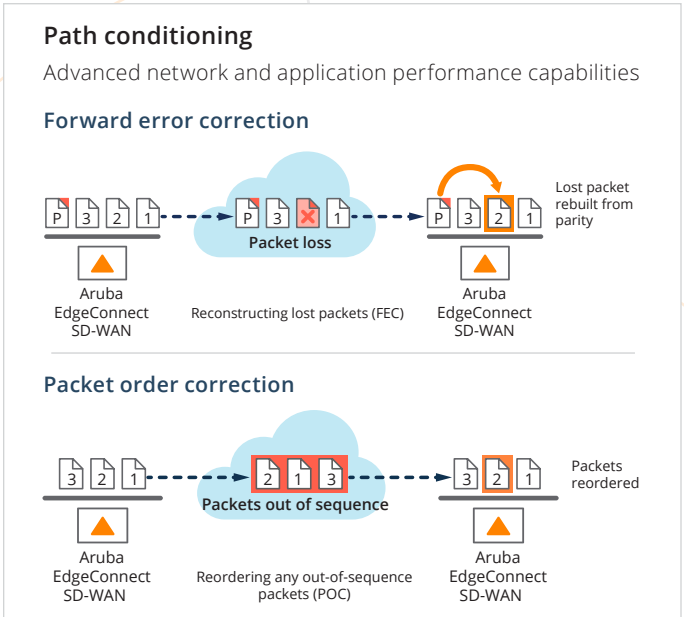
Three components comprise the Aruba EdgeConnect SD-WAN platform:

- **Aruba EdgeConnect SD-WAN** physical or virtual SD-WAN appliances (supporting any common hypervisors and public clouds) deployed in branch offices to create a secure, virtual network overlay. This enables customers to move to a broadband WAN at their own pace, whether site-by-site, or via a hybrid WAN approach that leverages MPLS and broadband internet connectivity.
- **Aruba WAN Orchestrator**, included with the Aruba EdgeConnect SD-WAN platform, provides unprecedented levels of visibility into both legacy and cloud applications with the unique ability to centrally assign policies based on business intent to secure and control all WAN traffic. Policy automation speeds and simplifies the deployment of multiple branch offices and enables consistent policies across applications. Moreover, customers can launch the Aruba WAN Orchestrator software directly from Aruba Central. Aruba Central provides the ability to view the enterprise-wide SD-WAN topology, health status, and alarms of all EdgeConnect SD-WAN appliances in the SD-WAN in addition to other Aruba wired and wireless network devices.

- **Aruba WAN Boost** WAN Optimization is an optional WAN optimization performance pack that combines Aruba WAN optimization technologies with Aruba EdgeConnect SD-WAN to create a single, unified WAN edge platform. Aruba WAN Boost allows companies to accelerate performance of latency-sensitive applications and minimize transmission of repetitive data across the WAN in a single, unified SD-WAN edge platform.

ARUBA EDGECONNECT SD-WAN KEY FEATURES

- **Business Intent Overlays:** Aruba EdgeConnect SD-WAN is built upon an application-specific virtual WAN overlay model. Multiple overlays may be defined to abstract the underlying physical transport services from the virtual overlays, each supporting different QoS, transport, failover and security policies. Groups of applications are mapped to different business intent overlays to deliver applications to users in alignment with business requirements. Business intent overlays may also be deployed to extend micro-segmentation of specific application traffic from the data center across the WAN to help maintain security compliance mandates.
- **Path Conditioning**: This feature provides private-line-like performance over the public internet. Includes techniques to overcome the adverse effects of dropped and out-of-order packets that are common with broadband internet and MPLS connections to improve application performance.



- **Tunnel Bonding:** Configured from two or more physical WAN transport services, bonded tunnels form a single logical overlay connection, aggregating the performance of all underlying links. Real-time traffic steering is applied over any broadband or MPLS link, or any combination of links based on company-defined policies based upon business intent. In the event of an outage or brownout, Aruba EdgeConnect SD-WAN automatically continues to carry traffic on the remaining links or switches over to a secondary connection.

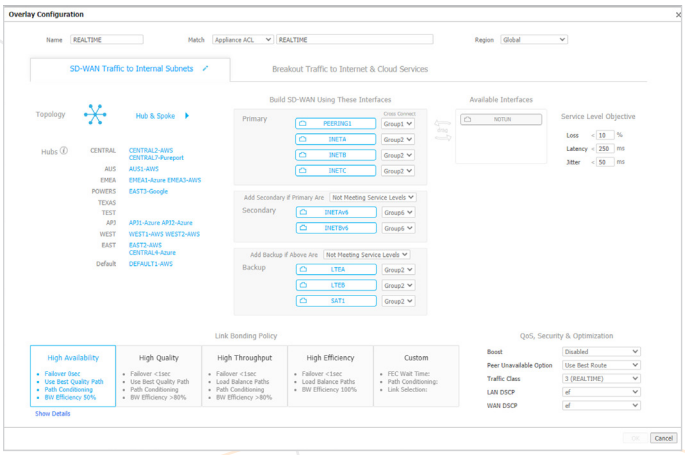
  Network traffic traversing an Aruba EdgeConnect SD-WAN can be tuned for availability, quality, throughput and efficiency. This is accomplished on a per-application basis through the use of Business Intent Overlays. Multiple business intent policies can be created, each with its own specific bonding policy. As part of this policy definition, the customers have the ability to customize the link prioritization and traffic steering policies based on multiple criteria, including physical performance characteristics, link economics, link resiliency characteristics and customer-definable attributes.
- **First-packet iQ Application Classification:** EdgeConnect SD-WAN First-packet iQ application classification identifies applications on the first packet to deliver trusted SaaS and web traffic directly to the Internet while directing unknown or suspicious traffic to the data center firewall or IDS/IPS. Identifying applications on the first packet is especially important when branches are deployed behind Network Address Translation (NAT); the correct path must be selected based on the first packet to avoid session interruption.
- **Secure Internet Breakout:** Granular, intelligent traffic steering enabled by First-packet iQ eliminates the inefficiency of backhauling all HTTP/HTTPS traffic to the data center. The solution eliminates the potential for wasted bandwidth and performance bottlenecks for trusted SaaS and web traffic. Trusted traffic is sent directly across the Internet while unknown or suspicious traffic may be sent automatically to more robust security services in accordance with corporate security policies.
- **Best-of-Breed Secure Access Service Edge (SASE):** Aruba EdgeConnect SD-WAN automates the integration with leading cloud security partner solutions from Zscaler, Netskope, Check Point, Palo Alto Networks, McAfee, Symantec and others to create a seamless secure access service edge architecture. Automated orchestration, using a drag-and-drop interface, enables IT to configure

consistent enterprise-wide security policies based on business requirements.

- **Next-generation Firewall:** Aruba EdgeConnect SD-WAN includes a next-generation firewall that provides in a single entity, advanced security features such as deep packet inspection, intrusion prevention, DDoS defense, as well as application and user identity awareness. It gives IT leaders the ability to block malware from entering the network based on application, identity and context, regardless of the port/protocol used. Additionally, IT leaders benefit from an increased visibility into network activity and potential risks.
- **Fine-grained Segmentation:** Create secure end-to-end zones across any combination of users, application groups and virtual overlays, pushing configuration updates to sites in accordance with business intent. Aruba ClearPass integration with EdgeConnect SD-WAN augments application intelligence with the user and device identity and role-based policy, enabling fine-grained segmentation. The additional identity-based context offers consistent security policy enforcement that can be enforced network-wide, from edge to the cloud, while also accelerating troubleshooting and problem resolution.
- **Intrusion Detection and Prevention:** Aruba EdgeConnect SD-WAN integrates a rule-based Intrusion Detection and Prevention System IDS/IPS and utilizes the common Aruba Unified Threat Management (UTM) framework. The signature-based system monitors network traffic to find patterns that match a particular attack signature. Integrated with EdgeConnect SD-WAN next-generation firewall, the system allows application-level selection for inspection based on firewall zones, and provides actions such as drop, inspect and allow traffic when an intrusion is detected. Threat logging provides network and security analytics back to Aruba Central or a third-party SIEM such as Splunk to monitor threats in real time, enabling IT to quickly take action.
- **DDoS Defense:** Aruba EdgeConnect SD-WAN detects and prevents attacks such as protocol attacks, ICMP floods, SYN floods, IP spoofing attacks and more. Using firewall protection profiles, the solution ensures strict state handling and limits the number of malicious requests with actions such as rapid aging, drop excess and block source. Actions are based on preset or configurable DoS thresholds set for traffic parameters including flow rate, concurrent flows, and embryonic flows. With firewall protection profiles, administrators can enforce different levels of DDoS protection levels across the organization by binding firewall protection profiles to firewall zones. The solution can also block a list of IP addresses from known attackers and dynamically routes the traffic over unaffected network links in case of a DDoS attack ensuring business continuity.
- **Routing:** Aruba EdgeConnect SD-WAN supports standard Layer 2 and Layer 3 open networking protocols such as VLAN (802.1Q), LAG (802.3ad), IPv4 and IPv6 forwarding, GRE, IPsec, VRRP, WCCP, PBR, BGP (version 4), OSPF.
- **High Availability:** The Aruba EdgeConnect SD-WAN HA cluster protects from hardware, software and transport failures. High Availability is achieved by providing fault tolerance on both the network side (WAN) and on the equipment side. The Aruba EdgeConnect SD-WAN appliances are inter-connected with a HA link that allows tunnels over each underlay to connect to both appliances.
- **Zero-Touch Provisioning:** A plug-and-play deployment model enables Aruba EdgeConnect SD-WAN to be deployed at a branch office in seconds, automatically connecting with other Aruba EdgeConnect SD-WAN instances in the data center, other branches, or in cloud Infrastructure as a Service (IaaS) such as Amazon Web Services, Microsoft Azure, Oracle Cloud Infrastructure and Google Cloud Platform.
- **WAN Hardening:** Each WAN overlay is secured edge-to-edge via 256-bit AES encrypted tunnels. No unauthorized outside traffic can enter the branch. With the option to deploy Aruba EdgeConnect SD-WAN directly onto the internet, WAN hardening secures branch offices without the appliance sprawl and operating costs of deploying and managing dedicated firewalls.
- **LTE Links:** The Aruba USB LTE modem provides a convenient solution for enterprises looking for high-speed WAN connectivity to support small office/home office, branches, and pop-up locations by making it easy to add primary or backup LTE WAN links. By using a plug-and-play Aruba USB LTE modem with EdgeConnect SD-WAN, enterprises can fully manage their LTE equipment through Aruba WAN Orchestrator, while ensuring optimal connections to critical applications and resources, even when primary connections experience failures or become unreliable. Aruba USB LTE modem features global support for nearly all major carriers and works with many EdgeConnect SD-WAN gateway models.

ARUBA WAN ORCHESTRATOR KEY FEATURES

- **Single Screen Administration:** Enables quick and easy implementation of network-wide business intent policies, which eliminates complex and error-prone policy changes at every branch
- **Real-Time Monitoring and Historical Reporting:** Provides specific details into application, location, and network statistics, including continuous performance monitoring of loss, latency, and packet ordering for each enterprise customers' network path. All HTTP and native application traffic are identified by name and location, and alarms and alerts allow for faster resolution of network issues
- **Bandwidth Cost Savings Reports:** Documents the cost savings for moving to broadband connectivity



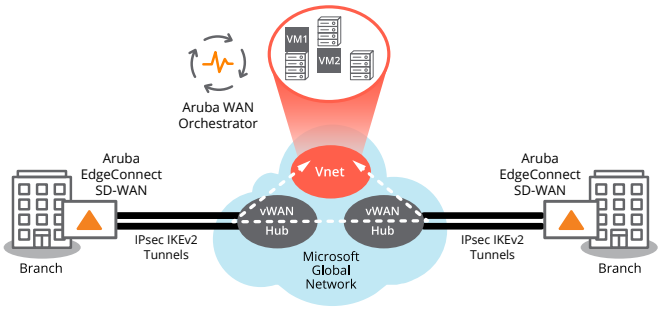
Aruba WAN Orchestrator enables centralized definition and automated distribution of network-wide business intent policies to multiple branch offices.

INTEGRATION WITH MICROSOFT AZURE VIRTUAL WAN (VWAN) AND AWS TRANSIT GATEWAY NETWORK MANAGER (TGNM)

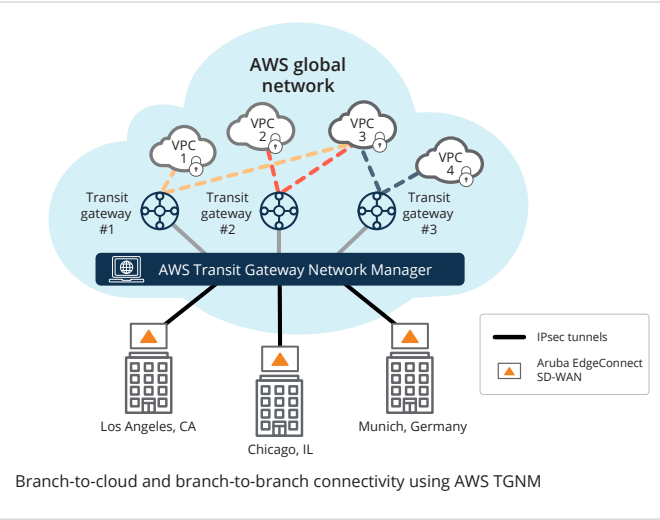
By integrating the Microsoft Azure vWAN and AWS Transit Gateway Network Manager (TGNM) REST APIs, the EdgeConnect SD-WAN enables customers to quickly build a cloud on-ramp and automate network deployments, removing the manual complexity of connecting branch offices to local Azure or AWS Points of Presence (PoPs). The API integration enables Aruba EdgeConnect SD-WAN to identify the locations of branches in the network and determine the closest VPN Gateway (vWAN hub or head-end gateway in AWS) to connect to. Aruba EdgeConnect SD-WAN automatically establishes standards-based IPsec tunnels, and configuring both of the tunnel endpoints for each branch to a VPN Gateway.

Key Features:

- Automate branch connectivity to Azure and AWS Points of Presence (PoPs)
- Simplify network expansion and troubleshooting
- Faster onboarding to applications and workloads — both to and from Azure and AWS
- Optimized routing within Azure or AWS network
- Centralized Network Monitoring
- Global Network Visibility
- Cohesive policy configuration



Branch-to-cloud and branch-to-branch connectivity using Azure vWAN



Branch-to-cloud and branch-to-branch connectivity using AWS TGNM

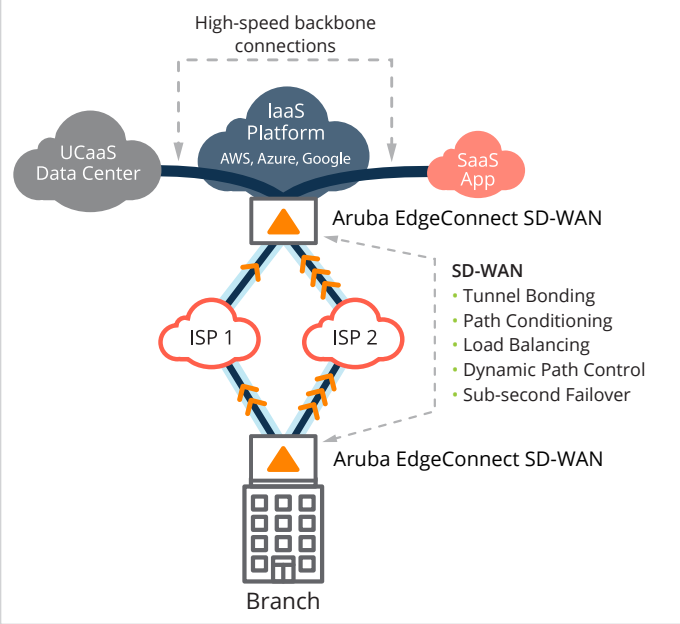
DELIVERING THE HIGHEST QUALITY OF EXPERIENCE FOR MICROSOFT 365

With the Microsoft 365 REST API integration, Aruba continuously learns and discovers new Microsoft 365 end points and/or IP addresses and automatically re-configures Aruba EdgeConnect SD-WAN if a new, closer Microsoft 365 end point becomes available. By doing so, users always achieve optimal Office 365 connectivity and performance by reducing the round-trip time (RTT). The EdgeConnect SD-WAN has been

independently tested and certified to support the Microsoft 365 Connectivity Principles. As a result of the independent testing, the Aruba EdgeConnect SD-WAN platform has been inducted into the Microsoft 365 Networking Partner Program and has been given the official "Works with Microsoft 365" designation.

EXTEND WAN FABRIC TO THE CLOUD

Deploy virtual Aruba EdgeConnect SD-WAN appliances in a public cloud such as AWS, Azure, Google Cloud Platform, or Oracle Cloud to optimize connections between branch locations and the cloud using all the SD-WAN benefits. If a brownout or blackout occurs, the remaining link(s) continue to carry traffic so that users don't notice any disruption to voice calls, audio and video conferences, or any other application. Ruggedized first mile between the branch and the public cloud delivers better network performance, reliability, and quality.



ZERO TRUST: SECURING THE EDGE BY ROLE, CONTEXT, AND APPLICATION

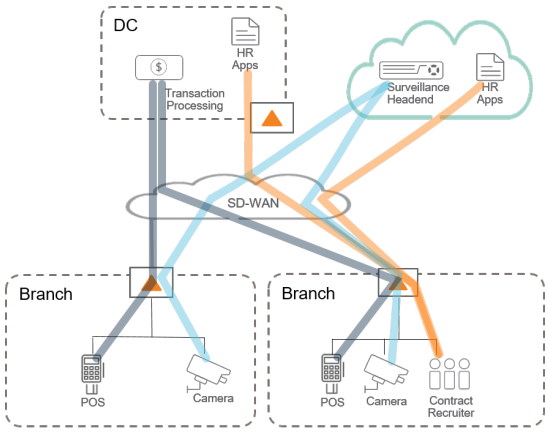
With the increase in mobile devices, remote workers, cloud-hosted applications, and IoT connected devices, enterprises must align their security policies based on business intent while also striving for consistency. Aruba ClearPass integration with EdgeConnect SD-WAN augments application intelligence with user and device identity and role-based policy, enabling fine-grained segmentation. This additional identity-based context enables consistent security policies that can be enforced network-wide, from edge to cloud, while also accelerating troubleshooting and problem resolution.

As a new user or device connects to the network and registers with ClearPass, the Aruba WAN Orchestrator (control plane for Aruba EdgeConnect SD-WAN connects via the ClearPass API. Aruba WAN Orchestrator propagates security policy information related to user, device type, role, and security posture to all EdgeConnect SD-WAN appliances in the network.

Because IoT devices are agentless, it is not possible to run a third-party VPN or ZTNA client on them. Thus, a SASE architecture doesn't fully address the security challenges posed by the IoT devices in the enterprise network.

With the Aruba ClearPass zero trust security framework, the network can identify and segment IoT devices and traffic at the network edge and isolate it from other traffic in the network. This layer of context enables fine-grained segmentation without the complexity of managing multiple VLANs.

For example, a fine-grained segmentation policy can prevent IoT security cameras from accessing credit card transactions or HVAC systems. Zero trust dynamic segmentation helps enterprises isolate any potential security threats by device type, role, and application while helping them meet industry compliance requirements such as PCI, HIPAA, and SOX.



Zero Trust Segmentation allows for users and devices to only communicate with destinations consistent with their role in the organization.

VIRTUAL ROUTING AND FORWARDING (VRF) SEGMENTATION

Network managers can configure and manage separate addressing, routing and security policies consistently with the EdgeConnect SD-WAN across end-to-end segments and micro-segments for traffic traversing large-scale multinational enterprises and federations of independent companies. Advanced segmentation eliminates the arduous task of manually stitching together VRF, firewall and NAT policies in a consistent manner, dramatically simplifying the management of diverse scenarios and providing unprecedented flexibility when contending with overlapping IP address spaces.

SPLUNK INTEGRATION

Security information and event management (SIEM) tools help to proactively identify potential security threats and vulnerabilities before they have a chance to disrupt business operations and affect revenue. Aruba has introduced a custom application for Splunk, called Aruba EdgeConnect Security App. Easily downloadable from Splunkbase, this app leverages the network data provided by the Aruba EdgeConnect SD-WAN platform with Splunk's extensive investigation and visualization capabilities to deliver advanced security reporting and analysis. Compatible with both Splunk Enterprise and Splunk Cloud, the Aruba EdgeConnect Security App provides a dashboard view of all security event notifications stemming from EdgeConnect SD-WAN devices. Using Splunk, IT can filter, sort, navigate, and view the collective security event notifications generated across the entire SD-WAN fabric, overall trends, and top talkers to help organizations pinpoint network events that warrant further investigation.

SUPPORT FOR CUSTOM USER-DEFINED APPLICATIONS

Many organizations continue to support applications customized for or internal to the company that are hosted in the corporate data center. Such custom applications are critical for the enterprise and with the EdgeConnect SD-WAN, customers can ensure optimal performance of these applications. From Aruba WAN Orchestrator, IT can easily configure a custom application definition that enables Aruba EdgeConnect SD-WAN to identify such applications on the first packet.

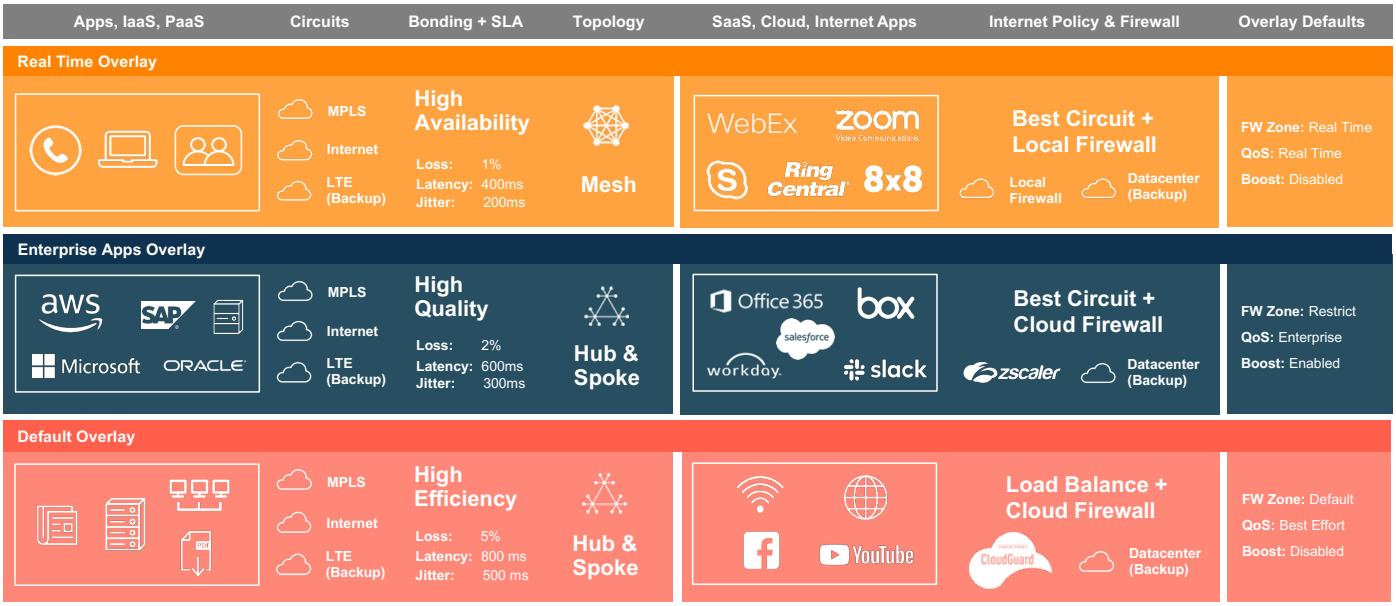
EFFICIENT DNS QUERY RESOLUTION

A critical step in the DNS proxy is to resolve the DNS query quickly. With Aruba EdgeConnect SD-WAN, customers can reach DNS servers in close proximity to branch sites eliminating backhaul of the DNS request to the remote data centers where enterprise DNS servers are hosted. From the branch location itself, DNS requests can be made directly to Global DNS servers, which reduces the impact of latency in establishing a SaaS application session, thereby improving SaaS application performance.

ARUBA WAN ORCHESTRATOR ENABLES FASTER SD-WAN DEPLOYMENTS

Aruba WAN Orchestrator, included with Aruba EdgeConnect SD-WAN for on-premise installations and available as an optional Aruba cloud-hosted service subscription, enables zero-touch provisioning of Aruba EdgeConnect SD-WAN appliances in the branch. Aruba WAN Orchestrator automates the assignment of business intent policies to ensure faster and easier connectivity across multiple branches, eliminating the configuration drift that can come from manually updating rules and access control lists (ACLs) on a site-by-site basis. Aruba WAN Orchestrator enables customers to:

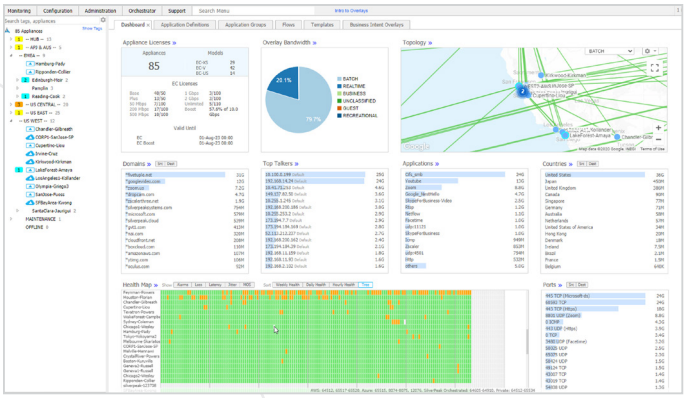
- Avoid WAN reconfigurations by delivering applications to
- users in customized virtual overlays
- Align application delivery to business goals through virtual WAN overlays based on business intent
- Simplify branch deployments with Aruba EdgeConnect SD-WAN profiles that describe the virtual and physical configuration of the location



Business intent overlays configured with Aruba WAN Orchestrator

In addition to centralized and automated control of the entire SD-WAN topology, Aruba WAN Orchestrator provides specific detail into WAN performance, including:

- Detailed reporting on application, location, and network statistics
- Continuous performance monitoring of throughput, loss, latency, jitter and packet ordering for all network paths
- Identification of all application traffic by name and location
- Alarms and alerts to visualize and prioritize software and hardware issues within the WAN allow for faster problem resolution
- Bandwidth cost savings report for documenting the cost savings of moving to broadband



Aruba WAN Orchestrator enables centralized and automated overlay management.

GAIN CONTROL OVER THE CLOUD

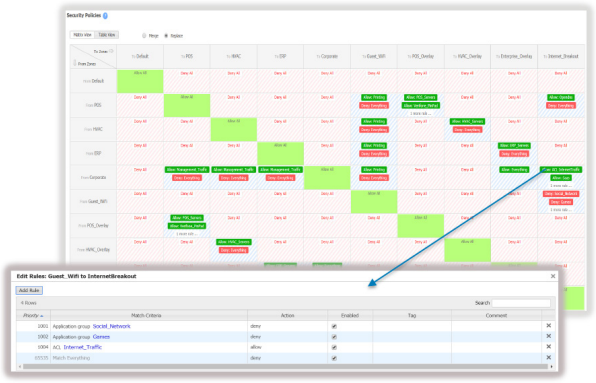
Gain an accurate picture of how Infrastructure-as-a-Service (IaaS) and Software-as-a-Service (SaaS) are being used within your organization.

- Name-based identification and reporting of all cloud applications
- Tracking of SaaS provider network traffic
- Cloud Intelligence provides Internet mapping of optimal egress to SaaS services

EDGE TO CLOUD SECURITY

Advanced capabilities provide cloud-first enterprises with the control to centralize and automate security policy governance and safely connect users directly to applications. They automate application traffic steering across the LAN and WAN in compliance with predefined security policies, regulatory mandates and business intent. With the solution, distributed enterprises can dynamically segment users, applications, and WAN services into secure zones based on identity, access rights, and security posture. Least privileged access principles are applied, ensuring that users and devices only communicate with destinations consistent with their role. Aruba EdgeConnect SD-WAN also offers advanced threat defense capabilities including intrusion detection and prevention as well as DDoS protection.

Additionally, the solution is tightly integrated with leading SSE (Security Service Edge) vendors, providing advanced security features such as ZTNA (Zero-Trust Network Access), CASB (Cloud Access Security Broker) and SWG (Secure Web Gateway) to build a best-of-breed SASE architecture.



A matrix view from Aruba WAN Orchestrator, provides an easy-to-read, intuitive visualization of configured zones and defined whitelist exceptions.

SECURE SD-WAN CERTIFICATION BY ICSA LABS

The Aruba EdgeConnect SD-WAN platform has earned the ICSA Labs Secure SD-WAN certification, passing rigorous testing based on a comprehensive and robust set of SD-WAN features and platform security requirements.

ICSA Labs Secure SD-WAN certification requirements include:

- **Advanced SD-WAN features** such as tunnel bonding, dynamic path selection and zero-touch provisioning
- **Native support (or via service chaining) for advanced security** functions such as anti-malware, intrusion prevention and DoS protection
- **Encryption** of sensitive data, as well as administrative and operational communications
- **Policy enforcements** for both WAN-specific functions and security policies
- **Security events logging**

The globally recognized certification provides the assurance of using a secure SD-WAN solution certified by a recognized independent, third-party organization. It also enables enterprises to simplify network architecture by securely replacing traditional branch firewalls with Aruba EdgeConnect SD-WAN.

BOOST APPLICATION PERFORMANCE AS NEEDED

Aruba WAN Boost is an optional WAN Optimization performance that includes:

- Latency Mitigation: TCP and other protocol acceleration techniques are applied to all traffic, minimizing the effects of latency on application performance and significantly improving application response times across the WAN.
- Data Reduction: Data compression and deduplication eliminates the repetitive transmission of duplicate data. Aruba Boost inspects WAN traffic at the byte-level and stores content in local data stores. Advanced finger-printing techniques recognize repetitive patterns for local delivery. Data Reduction can be applied to all IP-based protocols, including TCP and UDP.

WHY ADD ARUBA WAN BOOST?

Aruba EdgeConnect SD-WAN appliances alone provide enhanced application performance for broadband or hybrid WAN deployments, utilizing the included packet-based tunnel bonding, dynamic path control (DPC), and path conditioning for overcoming the adverse effects of dropped and out-of-order packets that are common with Internet connections.

However, sometimes additional performance is needed for specific applications or locations. As distance between locations increases over the WAN, application performance degrades. This has less to do with the available bandwidth, and is more about the time it takes to send and receive data packets over distance, and the number of times data must be re-sent.

ARUBA WAN BOOST USE CASE EXAMPLES

- Customers replicating to a disaster recovery (DR) site thousands-of-miles away might want to add Aruba WAN Boost to ensure recovery point objectives (RPOs) are not compromised.
- Enterprises with remote sites located in rural areas, or with sites that are exceptionally farther away from the company's data center, might want to add Aruba Boost to overcome the effects of high latency. With Aruba WAN Boost, customers gain the flexibility to enable enhanced WAN optimization capabilities where and when it is needed in a fully integrated solution. Aruba WAN Boost is licensed per-megabit-per-second, per-month, so customers do not have to pay for WAN optimization across the entire network.

OVERCOME EFFECTS OF LATENCY

The time it takes for information to go from sender to receiver and back is referred to as network latency. Since the speed of light is constant, WAN latency is directly proportional to the distance traveled between the two network endpoints. Aruba offers a variety of TCP acceleration techniques to mitigate WAN latency, including Window Scaling, Selective Acknowledgement, Round-Trip Measurement, and High Speed TCP.

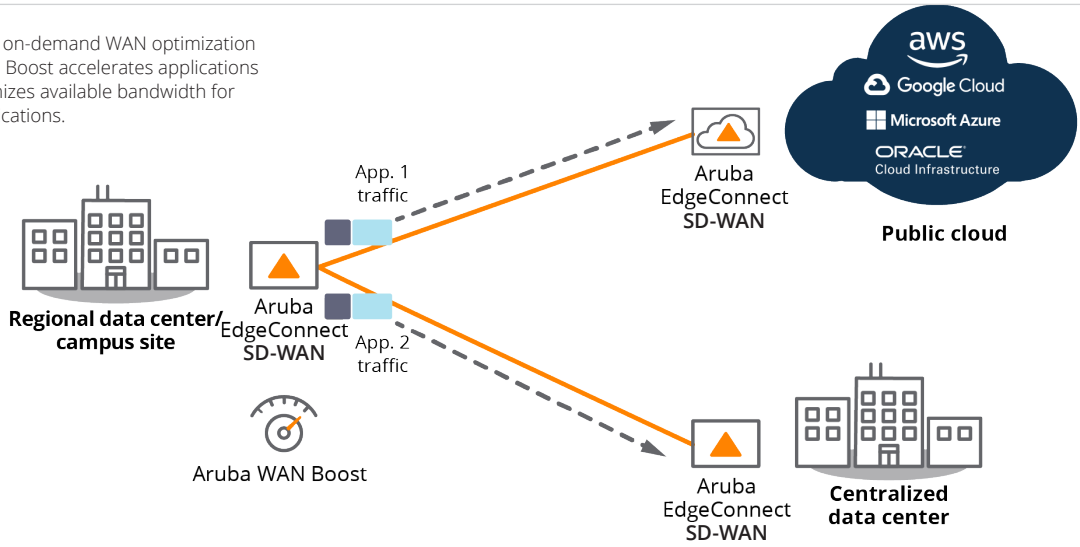
Windows and other applications that rely on the Common Internet File System (CIFS) often take longer to perform common file operations over distance, such as retrieving and sharing files. Aruba WAN Boost helps these applications not only by improving the underlying TCP transport, but also by accelerating CIFS through CIFS read-ahead, CIFS write-behind, and CIFS metadata optimizations.

INCREASE THROUGHPUT

As packets flow through Aruba EdgeConnect SD-WAN appliances, Aruba WAN Boost inspects WAN traffic at the byte-level and stores content in local data stores. As new packets arrive, Aruba computes fingerprints of the data contained within the packets, and checks to see whether these fingerprints match data that is stored locally.

If the remote appliance contains the information, there is no need to resend it over the WAN. Instead, specific start-stop instructions are sent to deliver the data locally.

"One-click" on-demand WAN optimization with Aruba Boost accelerates applications and maximizes available bandwidth for other applications.



Application/ Public cloud acceleration	Data reduction — flexible bandwidth allocation	Data backup, disaster recovery	Save on service provider & public cloud bills

ARUBA EDGECONNECT SD-WAN HARDWARE PORTFOLIO

	EdgeConnect SD-WAN US	EdgeConnect SD-WAN 10104	EdgeConnect SD-WAN XS	EdgeConnect SD-WAN S-P	EdgeConnect SD-WAN M-H	EdgeConnect SD-WAN L-H	EdgeConnect SD-WAN XL-H
							
Model	EC-US	EC-10104	EC-XS	EC-S-P	EC-M-H*	EC-L-H*	EC-XL-H*
Typical Deployment	Small Branch/ Home Office	Small Branch/ Home Office	Small Branch	Large Branch	Head Office/DC Large Hub	Data Center Large Hub	Data Center Large Hub
Typical WAN Bandwidth**	1–200 Mbps	2-500 Mbps	2–1000 Mbps	10–3000 Mbps	50–5000 Mbps	2–10 Gbps	2–10 Gbps
Simultaneous Connections	256,000	256,000	256,000	256,000	2,000,000	2,000,000	2,000,000
Recommend-ed Boost up to	25 Mbps	200 Mbps	250 Mbps	500 Mbps	1 Gbps	1 Gbps	5 Gbps
IDS/IPS	Not supported	Yes	Yes	Yes	Yes	Yes	Yes
Redundancy/ FRUs*	No	No	No	SSD and Power (AC or DC)	SSD and Power	SSD and Power	SSD, NVMe, Power
Data Path Interfaces	3 x RJ45 10/100/1000	4 x RJ45 10/100/1000	4 x RJ45 10/100/1000	8 x RJ45 4 x 1/10G Optical	8 x RJ45 4 x 1/10G Optical	6 x 1/10G Optical	6 x optical interfaces EC-XL-H: 6 x 1/10/25G EC-XL-H-10G: 6 x 1/10G

* EC-XL-H and EC-XL-H-10G comes pre-equipped with NVMe for maximum WAN optimization (Boost)
** EC-S-P, EC-M-H, EC-L-H, and EC-XL-H all support pluggable optics
*** See software compatibility table for minimum software releases required to support the new EC –H models
**** WAN Bandwidth assumes bidirectional traffic (symmetric up-link and down-link). For total WAN throughput (Rx+Tx), multiply these numbers by 2.
***** For best performance, EdgeConnect SD-WAN Operating System Release 9.1 or higher is recommended****** FRU Power Supplies are an additional SKU

ARUBA EDGECONNECT SD-WAN PLATFORM SPECIFICATION SHEETS

ULTRA-SMALL | 10104 | EXTRA-SMALL | SMALL

MEDIUM | LARGE | EXTRA-LARGE

ARUBA EDGECONNECT SD-WAN TECHNICAL SUPPORT

Term	Support is included as part of the Aruba EdgeConnect SD-WAN subscription license
Web-based support portal	Unlimited access 24 / 7 / 365 includes software downloads, technical documentation, and online knowledge base
Software updates	Major and minor features releases; maintenance releases
Technical support	24 / 7 / 365 phone / e-mail / web (Global Technical Assistance Centers — TAC)
Response time	30 minutes for high priority (P1) — critical
HW warranty and maintenance	Refer to the Aruba EdgeConnect SD-WAN warranty and maintenance policies data sheet for further information

FLEXIBLE DEPLOYMENT MODELS

- Aruba EdgeConnect SD-WAN Virtual (EC-V) — Download and install Aruba EdgeConnect SD-WAN from anywhere in the world. The software runs on all common hypervisors, including VMware ESXi, Microsoft Hyper-V, Citrix XenServer, and KVM. Aruba customers who have an IaaS presence in AWS, Microsoft Azure, Oracle Cloud Infrastructure or Google Cloud Platform can deploy Aruba EdgeConnect SD-WAN within their hosted cloud environment.
- Aruba EdgeConnect SD-WAN Physical (EC) — For enterprises that are not virtualized in the branch, choose one of the Aruba EdgeConnect SD-WAN hardware appliance models for plug-and-play deployment.

ARUBA EDGECONNECT SD-WAN TIERED SUBSCRIPTION LICENSING

Aruba EdgeConnect SD-WAN platform is available as a software subscription. Two subscription tiers are available, Foundation and Advanced, in either single or multi-year increments (1,2,3,4,5,6, and 7 years) and at multiple bandwidth tiers. Subscription tier mixing is not supported, i.e., every EdgeConnect SD-WAN appliance in an SD-WAN fabric must run either Foundation or Advanced licenses.

Foundation License Tier: The Foundation license tier includes essential SD-WAN features and all of the advanced NGFW features. The Foundation license is available in 100 Mbps, 1 Gbps, and 10 Gbps bandwidth tiers. Moreover, the Foundation license supports Hub-and-Spoke topology (4 Hubs/ region), a limited number of VRFs, and includes a cloud-hosted Aruba WAN Orchestrator subscription (Foundation OaaS). The Foundation license supports three BIOs, all essential QoS parameters and fundamental data retention capabilities, making it ideal for customers who require a simple, easy-to-manage SD-WAN with comprehensive NGFW features.

Advanced License Tier: Advanced license tier includes all Aruba EdgeConnect SD-WAN advanced SD-WAN features and all of the advanced NGFW features. The Advanced license is available in 20 Mbps, 50 Mbps, 100 Mbps, 200 Mbps, 500 Mbps, 1 Gbps, 2 Gbps, and Unlimited bandwidth tiers. Moreover, the Advanced license supports unlimited topology, 64 VRFs and includes a cloud-hosted Aruba WAN Orchestrator subscription (Advanced OaaS). The Advanced OaaS appeals to enterprises that prefer a zero-CAPEX SD-WAN management solution without the capital investment and the associated complexity of managing on-premises infrastructure. The Advanced license supports up to seven BIOs, advanced QoS parameters, and enhanced data retention capabilities making it ideal for customers who do not want to compromise on the SD-WAN features and want comprehensive NGFW features.

Enterprises that require on-premises deployment of Aruba WAN Orchestrator can purchase a separate SKU set with Advanced on-prem license tier. The on-prem edition of the Advanced license offers the same rich capabilities as the Advanced license but enables enterprises to manage their own instance of Aruba WAN Orchestrator. It is well-suited for customers that require a private installation of their SD-WAN management software.

OPTIONAL EDGECONNECT SD-WAN LICENSES

Dynamic Threat Defense: Enterprises that that require comprehensive IDS/IPS capabilities integrated with the SD-WAN can optionally deploy the Dynamic Threat Defense license.

WAN Boost: Aruba WAN Boost is an optional WAN optimization performance pack that may be ordered and deployed flexibly to sites that require application acceleration. Aruba WAN Boost is offered in 100Mbps or 10Gbps blocks

Moreover, large global enterprises with multiple business units (BU) or subsidiaries that have a requirement to support different regional QoS or security policies can optionally deploy Aruba WAN Orchestrator Global Enterprise (not applicable for Advanced on-prem license).

DS_Aruba-EdgeConnect-Solution_SK_070623 a00109847enw

Contact us at www.arubanetworks.com/contact