HPE Aruba Networking EdgeConnect SD-WAN

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

With enterprise applications migrating 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 internet services into the WAN transport mix.

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

EdgeConnect SD-WAN provides a secure network foundation for Zero Trust and SASE frameworks to tackle the networking and security challenges of hybrid working and cloud computing. The solution tightly integrates with HPE Aruba Networking SSE to form a unified SASE platform, for simpler adoption and faster deployment of SASE.

Additionally, EdgeConnect SD-WAN includes a built-in next-generation firewall providing fine-grained segmentation and identity-based access control capabilities, as well as IDS/IPS and DDoS defense to protect branch offices from malicious activities.

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

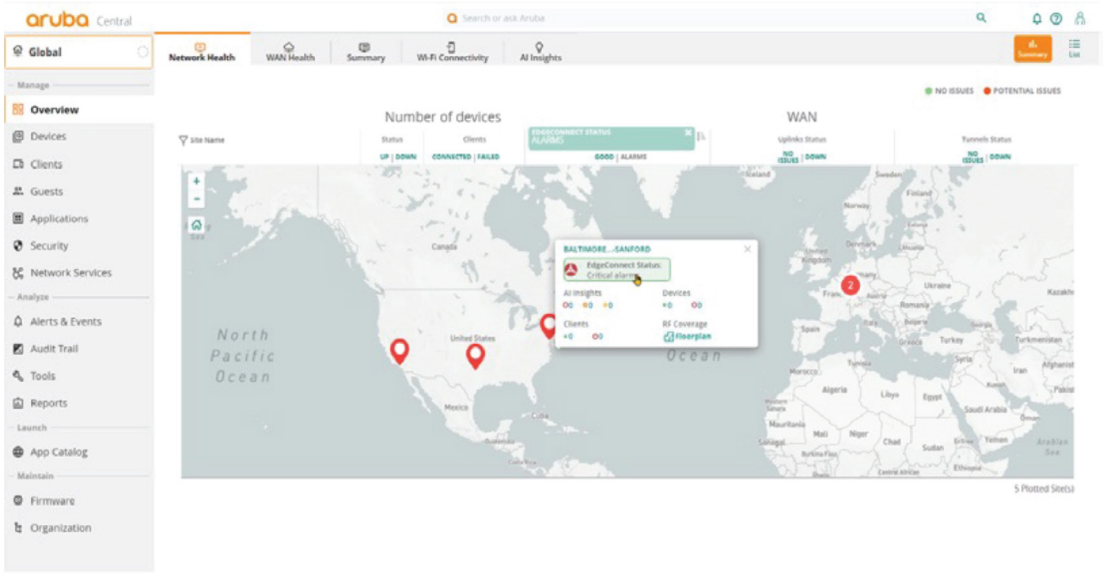

Figure 1. HPE Aruba Networking Central can directly launch HPE Aruba Networking EdgeConnect SD-WAN Orchestrator to view the enterprise-wide SD-WAN topology, health status, and alarms of all EdgeConnect SD-WAN appliances in the network

HPE Aruba Networking EdgeConnect SD-WAN platform

Three components comprise the HPE Aruba Networking EdgeConnect SD-WAN platform:

- **HPE Aruba Networking EdgeConnect SD-WAN** physical or virtual SD-WAN appliances (supporting any common hypervisors and public clouds) are 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.
- **HPE Aruba Networking EdgeConnect SD-WAN Orchestrator,** included with the EdgeConnect SD-WAN platform, provides unprecedented levels of visibility into both legacy and cloud applications, and centrally assigns policies based on business intent to secure and control all WAN traffic. Policy automation speeds and simplifies deployment of multiple branch offices and enables consistent policies across applications. Moreover, customers can launch the SD-WAN Orchestrator software directly from HPE Aruba Networking Central to view the enterprise-wide SD-WAN topology, health status, and alarms of all EdgeConnect SD-WAN appliances in the SD-WAN and other HPE Aruba Networking wired and wireless network devices.
- **HPE Aruba Networking EdgeConnect WAN Optimization** is an optional performance pack that combines WAN optimization technologies with EdgeConnect SD-WAN to create a single, unified WAN edge platform. WAN Optimization accelerates performance of latency-sensitive applications and minimizes transmission of repetitive data across the WAN in a single, unified SD-WAN edge platform.

EdgeConnect SD-WAN unified fabric

EdgeConnect SD-WAN provides a comprehensive portfolio of access deployment options to connect enterprise organizations to a single SD-WAN fabric, orchestrated by HPE Aruba Networking Central. This integration provides a consistent, scalable, and easy-to-manage solution that reduces complexity and enhances performance across all locations. It includes three types of right-sized deployment models, or "onramps," to the SD-WAN fabric including:

- **HPE Aruba Networking EdgeConnect SD-WAN** provides maximum network performance and security through an advanced secure SD-WAN using Business Intent Overlays
- **HPE Aruba Networking EdgeConnect SD-Branch** allows IT Admins to consolidate branch networking components for maximum integration across wireless, LAN, and SD-WAN with integrated security and centralized cloud management.
- **HPE Aruba Networking EdgeConnect Microbranch** is ideally suited for small office or work-from-home sites. It uses a range of HPE Aruba Networking remote access points (RAPs) paired with SD-WAN capabilities enabling secure connectivity to the corporate enterprise network.

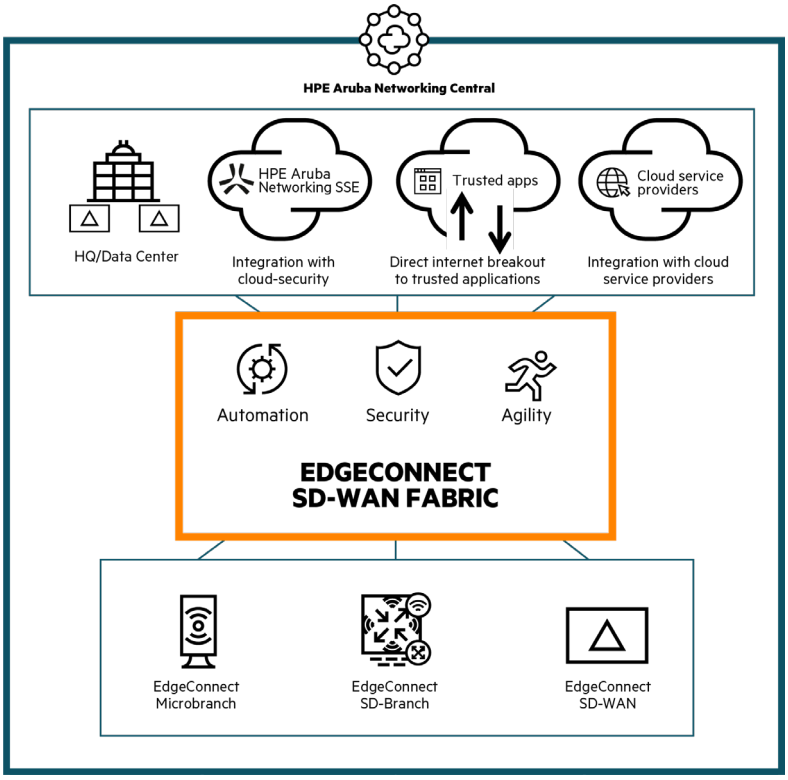

Figure 2. HPE Aruba Networking EdgeConnect SD-WAN fabric

HPE Aruba Networking Central orchestrates the EdgeConnect SD-WAN fabric between EdgeConnect SD-WAN, EdgeConnect SD-Branch and EdgeConnect Microbranch devices. This integration allows EdgeConnect SD-WAN physical appliances to act as VPN concentrators (VPNC) in the SD-WAN fabric, connecting EdgeConnect SD-Branch gateways and EdgeConnect Microbranch APs to either EdgeConnect SD-Branch VPNC or EdgeConnect SD-WAN VPNC in hub locations. Additionally, tunnels and routes are visible on both HPE Aruba Networking Central and SD-WAN Orchestrator. Organizations with an existing EdgeConnect SD-WAN deployment can leverage this feature to build a consistent networking and security strategy, seamlessly integrating with other HPE Aruba Networking products such as EdgeConnect SD-Branch, EdgeConnect Microbranch, switches and access points.

EdgeConnect SD-WAN key features

- **Business Intent Overlays:** 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. It includes techniques to overcome the adverse effects of dropped and out-of-order packets that are common with broadband internet and MPLS connections, thus improving application performance.

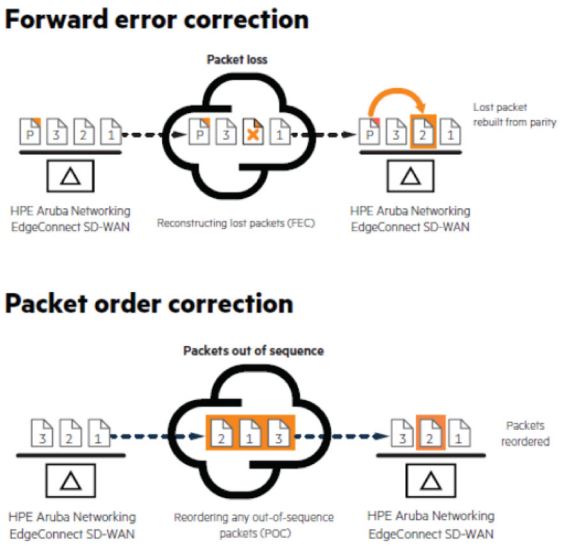

Figure 3. Path conditioning — advanced network and application performance capabilities

- **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 broadband, MPLS, or any combination of links based upon company-defined policies that hinge on business intent. In the event of an outage or brownout, EdgeConnect SD-WAN automatically continues to carry traffic on remaining links or switches over to a secondary connection.

  Network traffic traversing an EdgeConnect SD-WAN can be tuned for availability, quality, throughput, and efficiency. This is accomplished on a per-application basis via 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 can customize link prioritization and traffic steering policies based on multiple criteria, including physical performance characteristics, link economics, link resiliency characteristics, and customer-definable attributes.

AppExpress

AppExpress optimizes user experience for up to 50 business-critical private and SaaS applications such as Zoom, Workday, SAP®, Microsoft 365, and other applications. AppExpress exploits SD-WAN path diversity by automatically selecting the best path for each application. The feature leverages synthetic polling and real-time user traffic observations to intelligently steer traffic regardless of how the application traffic is broken out. This includes:

- **Local breakout:** It efficiently routes traffic over MPLS, internet, 4G/5G, or satellite links, automatically choosing the best link for optimal performance.
- **Optimized steering to IaaS:** the system automatically steers traffic to a virtual instance of EdgeConnect SD-WAN hosted in IaaS platforms such as Amazon Web Services, Microsoft Azure, and Google Cloud™, ensuring efficient data flow.
- **SSE PoP:** AppExpress selects the best SSE Point of Presence (PoP) that offers the highest performance, further enhancing user experience.

To determine how to steer the traffic and to report performance, AppExpress relies on the Application Performance Index or Apdex. Apdex is an industry standard that measures user experience based on a sample set of latency measurements to produce a normalized score ranging from 0 to 100. Each measurement is put into three levels of responsiveness including “Satisfied”, “Tolerating” and “Frustrated” to calculate the Apdex score.

The Apdex score is continuously monitored so that the best path is dynamically selected depending on network conditions. This ensures that users consistently enjoy an unparalleled experience when accessing critical business applications.

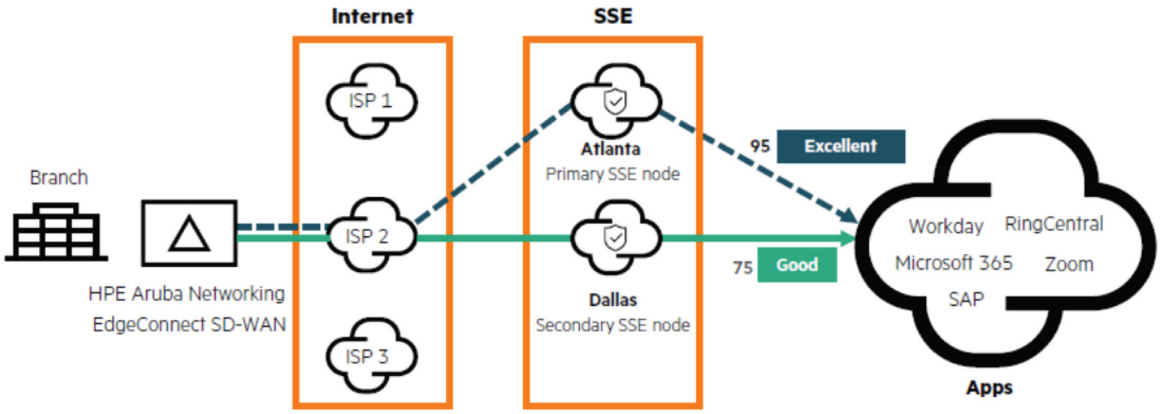

Figure 4. Optimize app performance, including SSE on ramp, with AppExpress

- **First-packet iQ application classification:** HPE Aruba Networking 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.

- **Unified SASE (Secure Access Service Edge):** To address the growing demand for integrated networking and security in the era of hybrid working and cloud computing, HPE Aruba Networking EdgeConnect SD-WAN solution seamlessly combines with HPE Aruba Networking SSE to establish a unified SASE platform. This cohesive approach streamlines adoption and expedites deployment of SASE.

  The unified SASE solution not only encompasses the functionalities of SD-WAN but also extends its capabilities to meet the security needs of remote users and hybrid workers through Zero Trust Network Access (ZTNA). ZTNA ensures that access is granted with the principle of least privilege, strengthening overall security posture. Moreover, ZTNA enables users and authorized third parties to access resources with or without an agent. The unified SASE platform safeguards against malicious web traffic, including ransomware, malware, and phishing attacks, with Secure Web Gateway (SWG), provides robust protection for sensitive data and prevents data loss through Cloud Access Security Broker (CASB) and includes Digital Experience Monitoring (DEM) to optimize user experience and operations.

  ZTNA, SWG, CASB, and DEM are seamlessly integrated into a single codebase for simplified policy management through a single interface and a single policy engine. Additionally, the solution harmonizes access across the world via an Amazon Web Services, Microsoft Azure, and Google Cloud backbone.

- **Automated orchestration to third-party SSE vendors:** HPE Aruba Networking EdgeConnect SD-WAN automates integration with leading SSE partner solutions from Zscaler, Netskope, Palo Alto Networks, Skyhigh Security, Broadcom, 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:** EdgeConnect SD-WAN includes a next-generation firewall that provides, in a single entity, advanced security features such as intrusion detection and prevention (IDS/IPS), DDoS defense and role-based segmentation, as well as application and user identity awareness. It blocks malware from entering the network based on application, identity and context, regardless of the port/protocol used and provides increased visibility into network activity and potential risks.

- **Role-based 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. HPE Aruba Networking ClearPass integration with EdgeConnect SD-WAN augments application intelligence with 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-cloud, while also accelerating troubleshooting and problem resolution.

  Additionally, EdgeConnect SD-WAN integrates Central NetConductor capabilities. This combined solution allows organizations to implement an enterprise wide Zero Trust architecture, even in complex multi-vendor LAN environments, leveraging EVPN/VXLAN open standards. EdgeConnect SD-WAN can transport role information across the entire fabric, whether the traffic is directed towards a VXLAN-based campus fabric managed via NetConductor or a third-party campus fabric solution supporting EVPN VXLAN group-based policy. IT architects can easily create role-to-role micro-segmentation policies that can be applied to the entire enterprise. In case the network does not support VXLAN, radius snooping derives the role directly from RADIUS transactions for authentication and authorization or receives them as login and logout events from ClearPass via API.

- **NAC Security:** The integration of HPE Aruba Networking ClearPass with EdgeConnect SD-WAN enables administrators to secure EdgeConnect SD-WAN ports using 802.1X and MAC authentication. This is ideal for small locations, home offices, or any place where SD-WAN ports may be vulnerable to unauthorized access. With Network Access Control (NAC) enabled, the EdgeConnect SD-WAN appliance authenticates traffic using 802.1X, supporting EAP-TLS, EAP-TTLS, and EAP-PEAP authentication methods. MAC authentication is also available for devices such as IoT, that don't support the 802.1X protocol.

- **Intrusion Detection and Prevention (IDS/IPS):** HPE Aruba Networking EdgeConnect SD-WAN optionally integrates a rule-based Intrusion Detection and Prevention System (IDS/IPS) that utilizes the common HPE Aruba Networking 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 or allow traffic. The system can operate either in inline mode or performant mode. In inline mode, the traffic passes through the sensor it is immediately blocked when an intrusion occurs. In performant

mode, traffic is analyzed out of path, providing more efficiency without impacting network performance.

Threat events can be sent to an external SIEM such as Splunk for security analytics to monitor real-time threats, enabling IT to quickly act on them.

The integration with Splunk is performed through a custom application, called HPE Aruba Networking EdgeConnect Security App, easily downloadable from Splunk base. Compatible with both Splunk Enterprise and Splunk Cloud, the EdgeConnect Security App provides a dashboard view of IDS/IPS events stemming from EdgeConnect SD-WAN. Using Splunk, administrators can filter, sort, navigate, and view the collective security event notifications generated across the entire SD-WAN fabric, overall trends, and top talkers.

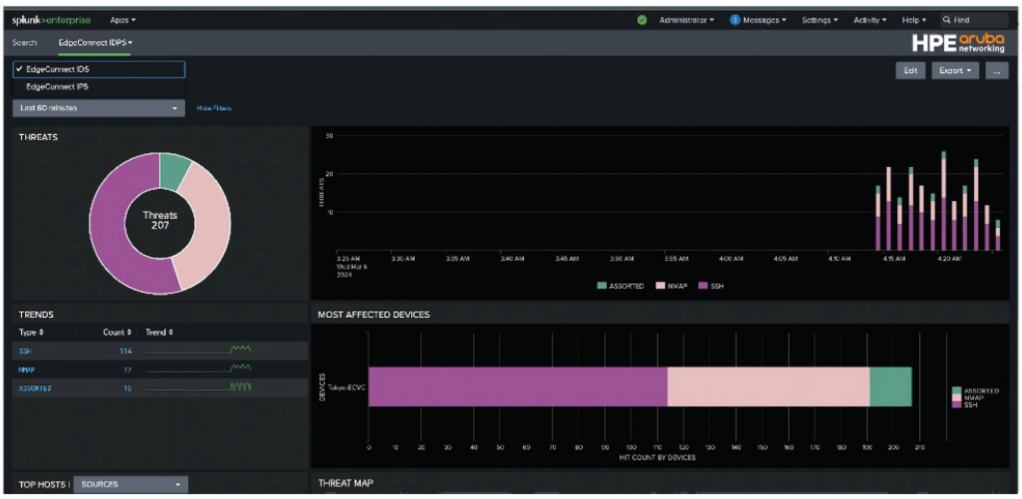

Figure 5. View IDS/IPS events in Splunk stemming from HPE Aruba Networking EdgeConnect SD-WAN

- **DDoS defense and Firewall Protection Profile:** EdgeConnect SD-WAN detects and prevents protocol attacks such as 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 triggered based on preset or configurable DoS thresholds applied to traffic parameters including flow rate, concurrent flows, and embryonic flows. To help manage the network during a DoS attack, administrators can set minimum and maximum thresholds. The minimum threshold helps spot problems early on, while the maximum threshold makes sure traffic doesn't drop prematurely. This gives administrators better control, making sure that they only drop traffic when necessary. 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 also blocks a list of IP addresses of known attackers and dynamically routes the traffic over unaffected network links in case of a DDoS attack, ensuring business continuity.
- **Adaptive DDoS** is an optional feature that uses machine learning to automatically adjust DoS thresholds, simplifying DoS threshold configuration and eliminating the need for frequent updates due to changing network conditions. Traditionally, administrators set DoS thresholds manually, often based on estimates, requiring frequent adjustments. Adaptive DDoS automates this process with two key functionalities: Auto Rate-Limiting and Smart Burst. Auto Rate-Limiting uses machine learning to regularly calculate a new baseline based on network statistics and patterns. This baseline sets the minimum DoS threshold. Smart Burst is applied to the maximum threshold, automatically allocating unused flow capacity across configured firewall zones. Smart Burst manages "good traffic bursts" (e.g., login spikes in the morning or backups at night) while preventing bad traffic from consuming bandwidth. It offers four modes: Baseline Plus (adds a buffer to the baseline), Committed Burst (proportionally allocates extra flow capacity to firewall zones), Excess Burst (unused Committed Burst capacity is pooled and shared as an additional layer of support), and a custom setting.
- **DDoS Analytics:** EdgeConnect SD-WAN includes a comprehensive set of reports for DoS defense such as threshold violations, flow drops, denied hosts and packets counts, top talkers, and alarms such as exceeded DoS thresholds.

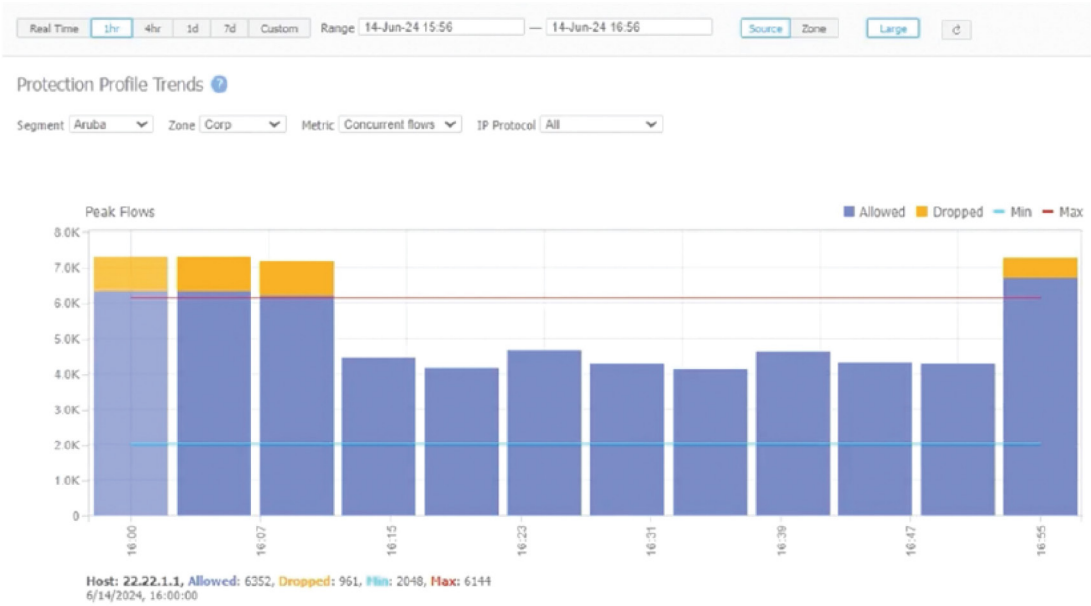

Figure 6. View the number of flows allowed and dropped for each five-minute time interval per firewall zones in EdgeConnect SD-WAN

- **Routing:** 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.
- **Bridge group:** For small locations, EdgeConnect SD-WAN can act as a switch by providing layer 2 connectivity (bridging) between two to four ports of an EdgeConnect SD-WAN appliance, creating a bridge group. Interfaces in the bridge group can be configured with the same parameters available on physical or sub-interfaces, such as segmentation, firewall zones, labels, DHCP server and relay, VRRP, BGP, OSPF, multicast, and branch NAT.
- **High availability:** The 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 EdgeConnect SD-WAN appliances are interconnected with a HA link that allows tunnels over each underlay to connect to both appliances.
- **Zero-touch provisioning:** Plug-and-play deployment enables branch office deployment of HPE Aruba Networking EdgeConnect SD-WAN in seconds, automatically connecting with other 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, meaning no unauthorized outside traffic can enter the branch. With the option to deploy 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.
- **5G Cellular Bridge/LTE links:** HPE Aruba Networking provides flexibility to support high-speed WAN connectivity for enterprise branch offices, pop-up locations, and small office/home offices with either a 5G cellular bridge or USB LTE modem. By using the HPE Aruba Networking 100 Series Cellular Bridge or a plug-and-play HPE Aruba Networking USB LTE modem with EdgeConnect SD-WAN, enterprises can fully manage their equipment through SD-WAN Orchestrator, while ensuring optimal connectivity to critical applications and resources, even when primary connectivity experience a failure. The 5G Cellular Bridge and the USB LTE modem features global support for nearly all major carriers and works with many EdgeConnect SD-WAN gateway models. The 5G Cellular Bridge can be mounted anywhere and powered via power over ethernet (PoE). This provides the option for optimal mounting for enhanced coverage and signal quality.

HPE Aruba Networking EdgeConnect SD-WAN Orchestrator key features:

- **Single screen administration:** Enables quick and easy implementation of network-wide business intent policies to 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.

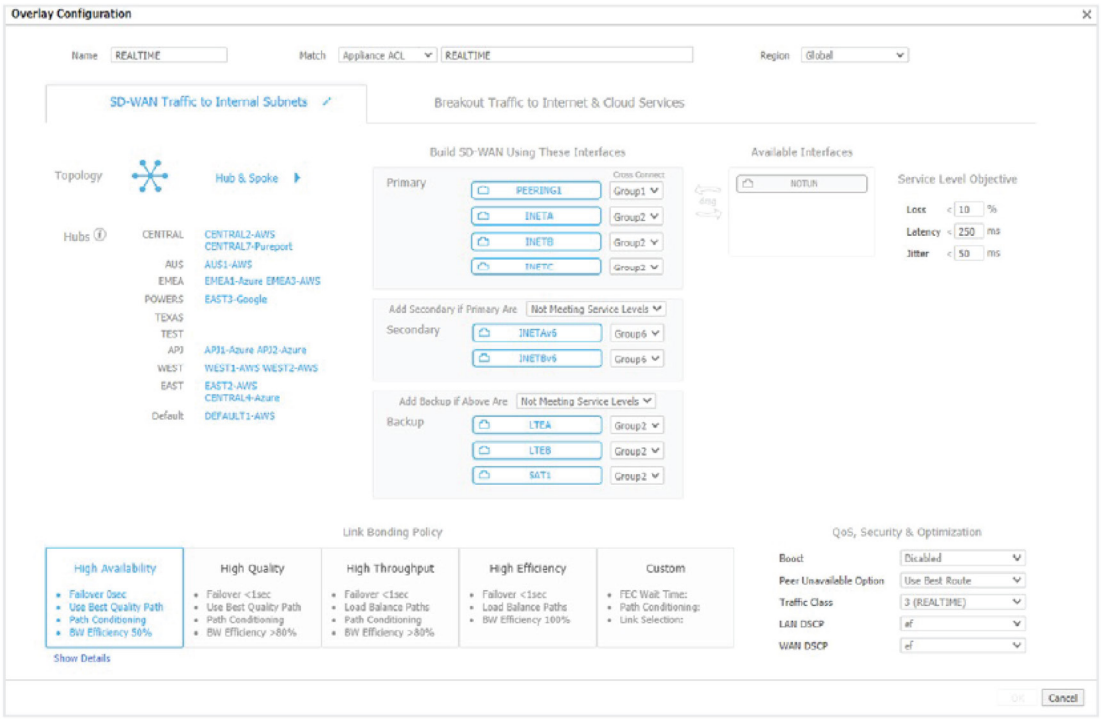

Figure 7. HPE Aruba Networking EdgeConnect SD-WAN Orchestrator enables centralized definition and automated distribution of network-wide business intent policies to multiple branch offices

Embrace multi-cloud networking

Deploy virtual HPE Aruba Networking EdgeConnect SD-WAN appliances in a public cloud such as Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform, Oracle Cloud, or Alibaba Cloud, as well as other network connectivity providers such as Equinix and Megaport. A virtual EdgeConnect SD-WAN appliance can also be deployed in AWS GovCloud, AWS China, AWS Outposts, AWS Local Zones, or Azure Government Cloud.

By deploying an EdgeConnect SD-WAN appliance in a cloud environment, organizations can optimize or "ruggedize" the first mile between the branch and the public cloud to deliver better network performance, reliability, and quality. This provides a cloud on-ramp to connect on-premises networks or other cloud environments to cloud workloads, removing the manual complexity of connecting branch offices to the cloud.

The virtual EdgeConnect SD-WAN appliances support establishing tunnels over the internet as well as other private connections such as AWS Direct Connect, Microsoft Azure ExpressRoute, Google Cloud Interconnect, Oracle Cloud FastConnect, or Alibaba Cloud Express Connect. If a brownout or blackout occurs when establishing SD-WAN tunnels over multiple WAN transports, 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.

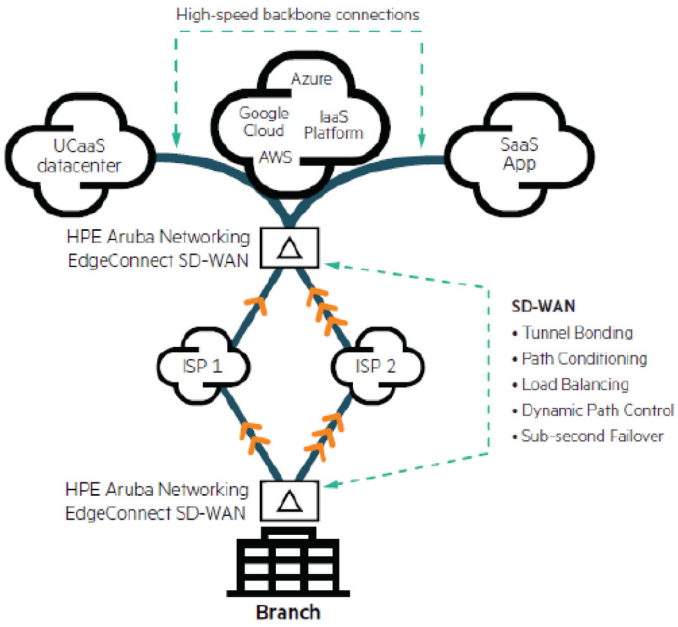

Figure 8. High speed backbone connections

The EdgeConnect SD-WAN AWS Cloud WAN and AWS Transit Gateway integration is designed to provide seamless, scalable, and secure connectivity between enterprise branch locations, data centers, and AWS cloud infrastructure. This integration simplifies multi-region and global networking by leveraging the capabilities of AWS Transit Gateway and AWS Cloud WAN, in conjunction with the advanced features of EdgeConnect SD-WAN. EdgeConnect SD-WAN with AWS Cloud WAN preserves and extends on-premises network segments into AWS, thereby increasing overall data security, access control, and performance.

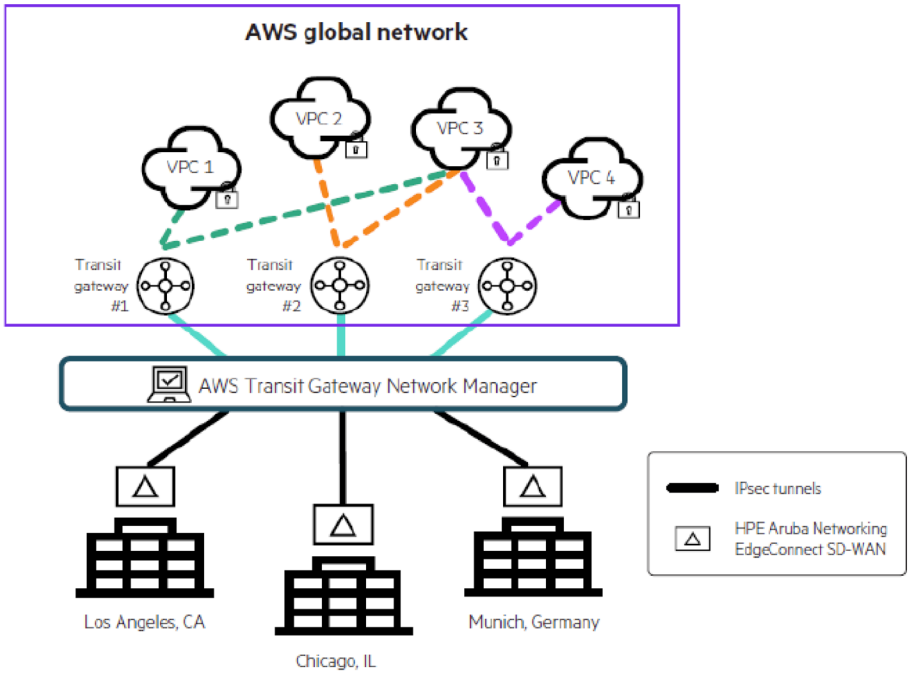

Figure 9. HPE Aruba Networking EdgeConnect SD-WAN branch-to-cloud and branch-to-branch connectivity using AWS TGNM

The Microsoft Azure integration allows an EdgeConnect SD-WAN appliance deployed in Azure to seamlessly establish connectivity with an Azure Virtual WAN Hub, an Azure Route Server, or an Azure Internal Load Balancer depending on your use case. This enables organizations to extend their SD-WAN capabilities into Azure, ensuring optimized performance and security for Azure-hosted workloads and services.

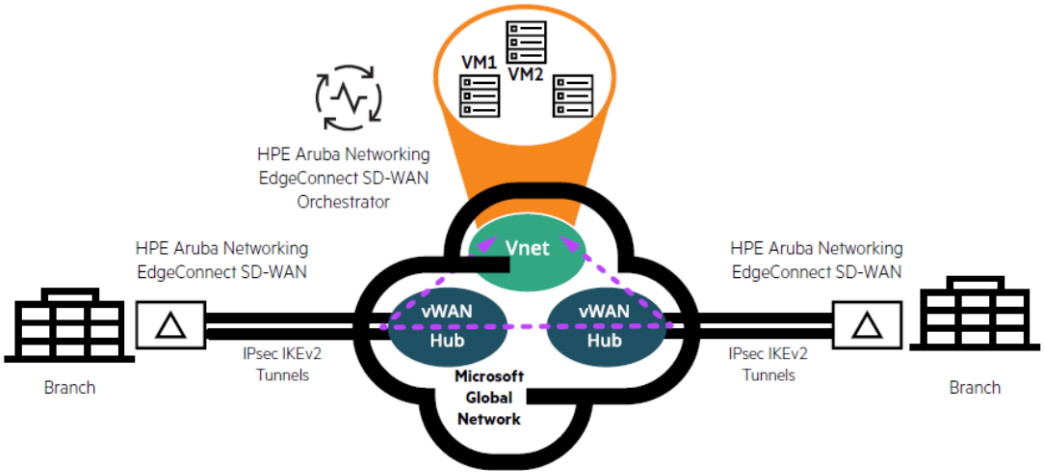

Figure 10. HPE Aruba Networking EdgeConnect SD-WAN branch-to-cloud and branch-to-branch connectivity using Azure Virtual WAN (vWAN)

Tunnel-in-tunnel

The tunnel-in-tunnel feature allows network administrators to create IPSec UDP SD-WAN tunnels inside third-party, standard IPSec tunnels, enabling direct traffic to the backbones of cloud service providers like AWS, Microsoft Azure, Google Cloud, Megaport, and Equinix. With a Virtual Tunnel Interface (VTI) connection between two locations, this protocol supports static routing, improving traffic flow. This setup leverages the fast, reliable backbones of cloud providers to enhance network performance and reduce latency.

Delivering the highest quality of experience for Microsoft 365

With the Microsoft 365 REST API integration, HPE Aruba Networking EdgeConnect SD-WAN continuously learns and discovers new Microsoft 365 end points and/or IP addresses and automatically re-configures EdgeConnect SD-WAN if a new, closer Microsoft 365 end point becomes available. By doing so, users can achieve optimal Microsoft 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 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.

SASE and built-in security

As cloud-based security becomes increasingly crucial, HPE Aruba Networking EdgeConnect SD-WAN seamlessly integrates with HPE Aruba Networking SSE, resulting in a unified SASE platform that streamlines SASE deployment while simplifying management. This integrated platform offers advanced security features such as ZTNA (Zero Trust Network Access), SWG (Secure Web Gateway), and CASB (Cloud Access Security Broker), addressing the networking and security challenges faced by cloud-centric organizations and hybrid working scenarios. Notably, it provides robust web-based threat defense and data protection for SaaS applications and ensures secure access for remote workers.

Additionally, the EdgeConnect SD-WAN solution streamlines the orchestration process to third-party SSE providers, offering organizations the flexibility to adopt SASE with their preferred security services or smoothly integrate with an existing security ecosystem.

The orchestration is automated with Secure Internet Breakout that intelligently routes traffic based on first packet iQ application classification. The feature directs traffic to SSE services, data centers, or the cloud in compliance with predefined security policies, regulatory mandates, and business intent.

Additionally, the SD-WAN solution incorporates a built-in next-generation firewall, with IDS/IPS and DDoS defense capabilities, allowing organizations to replace legacy firewalls in branch offices. IT teams benefit from centralized and automated security policy governance through zero-touch provisioning, streamlining management processes and minimizing configuration errors.

To deliver Zero Trust networking, the SD-WAN solution enables role-based segmentation of users, applications, and WAN services into secure zones based on identity, access rights, and security posture. Applying the principle of least privilege access, it ensures that users and devices only communicate with destinations that align with their respective roles.

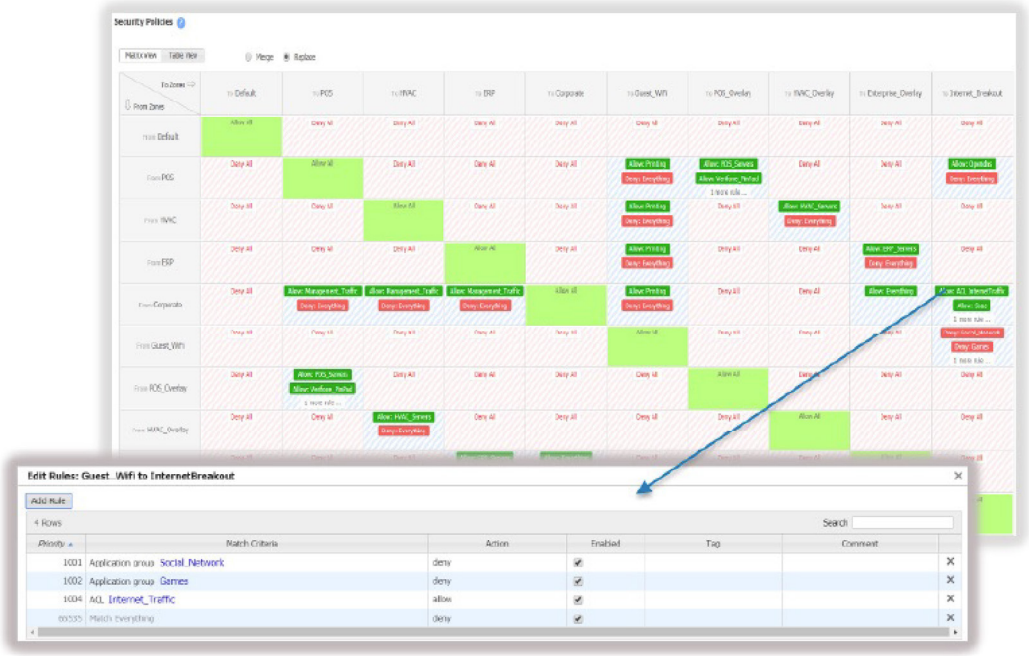

Figure 11. A matrix view from HPE Aruba Networking EdgeConnect SD-WAN Orchestrator provides an easy-to-read, intuitive visualization of configured zones and defined Allow list exceptions

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. HPE Aruba Networking ClearPass integration with HPE Aruba Networking EdgeConnect SD-WAN augments application intelligence with user and device identity and role-based policy, enabling fine-grained segmentation. This additional identity-based context provides 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 SD-WAN Orchestrator (control plane for EdgeConnect SD-WAN) connects via the ClearPass API. The SD-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 HPE Aruba Networking 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 transaction 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.

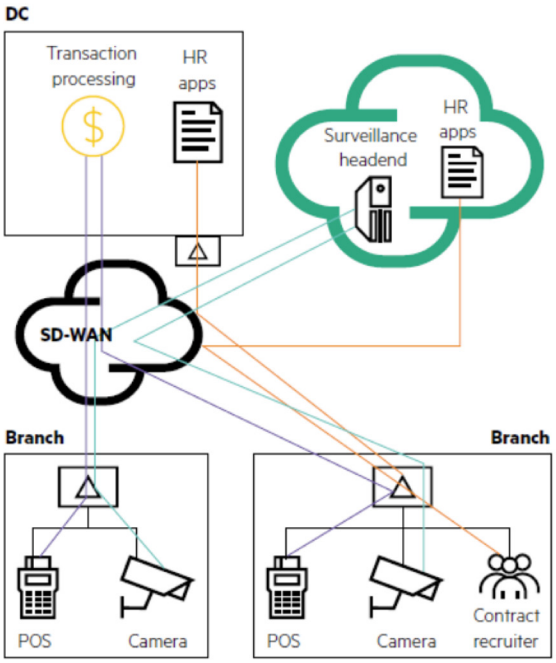

Figure 12. Zero Trust segmentation allows for users and devices to only communicate with destinations consistent with their role in the organization

Virtual routing and forwarding (VRF) segmentation

Network managers can configure and manage separate addressing, routing, and security policies consistently with the HPE Aruba Networking EdgeConnect SD-WAN across end-to-end segments and microsegments 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.

Secure SD-WAN certification by ICSA Labs

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

SD-WAN Orchestrator enables faster SD-WAN deployments

HPE Aruba Networking SD-WAN Orchestrator, included with EdgeConnect SD-WAN for on-premises installations and available as an optional cloud-hosted service subscription, enables zero-touch provisioning of EdgeConnect SD-WAN appliances in the branch. SD-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. SD-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 EdgeConnect SD-WAN profiles that describe the virtual and physical configuration of the location

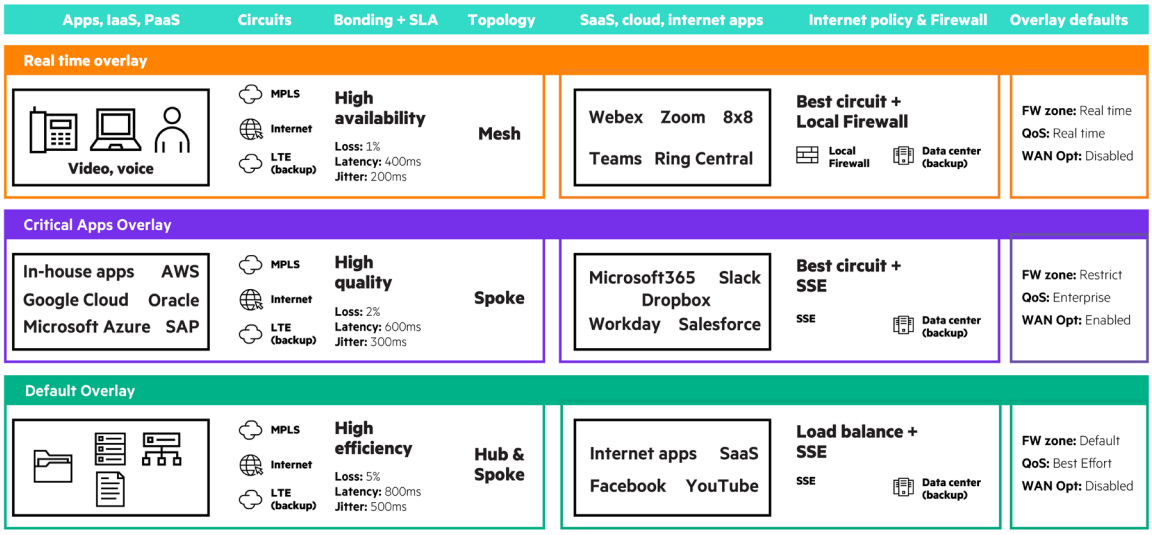

Figure 13. Business intent overlays configured with HPE Aruba Networking EdgeConnect SD WAN Orchestrator

In addition to centralized and automated control of the entire SD-WAN topology, SD-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

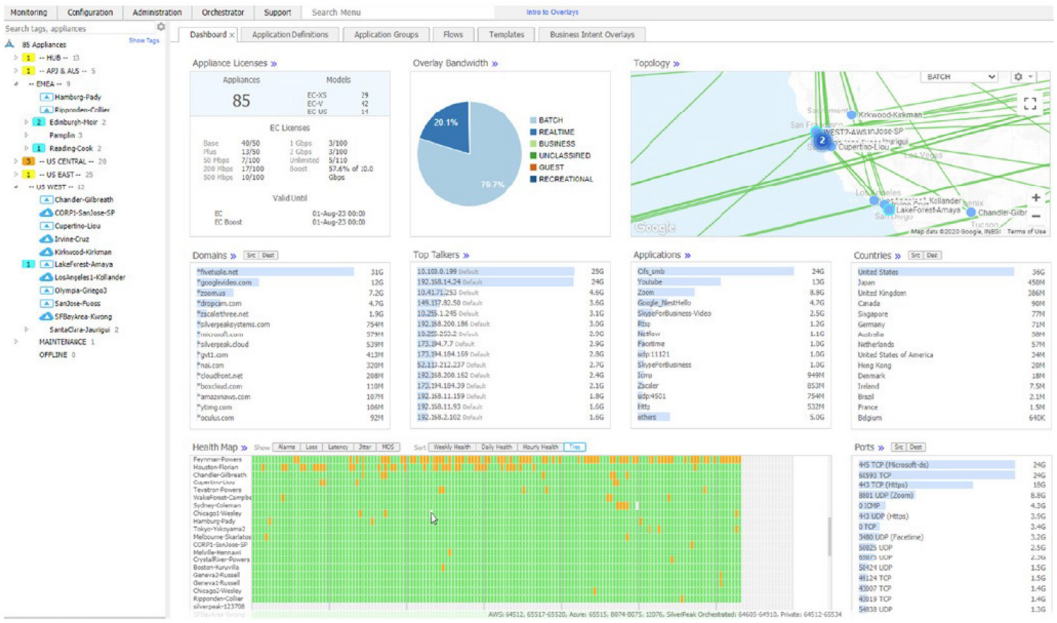

Figure 14. HPE Aruba Networking EdgeConnect SD-WAN Orchestrator enables centralized and automated overlay management

Boost application performance as needed

HPE Aruba Networking EdgeConnect WAN Optimization is an optional feature 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. WAN Optimization inspects WAN traffic at the byte level and stores content in local data stores. Advanced fingerprinting techniques recognize repetitive patterns for local delivery. Data reduction can be applied to all IP-based protocols, including TCP and UDP.

Why add WAN optimization?

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.

WAN Optimization use case examples

- Customers replicating to a disaster recovery (DR) site thousands of miles away might want to add WAN Optimization 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 WAN Optimization to overcome the effects of high latency. With WAN Optimization, customers gain the flexibility to enable enhanced WAN optimization capabilities where and when it is needed in a fully integrated solution. WAN Optimization is licensed per Mbps, 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. HPE Aruba Networking offers a variety of TCP acceleration techniques to mitigate WAN latency, including Window Scaling, Selective Acknowledgement, Round-Trip Measurement, and High Speed TCP.

Microsoft 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. WAN Optimization 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 EdgeConnect SD-WAN appliances, WAN Optimization inspects WAN traffic at the byte level and stores content in local data stores. As new packets arrive, HPE Aruba Networking 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.

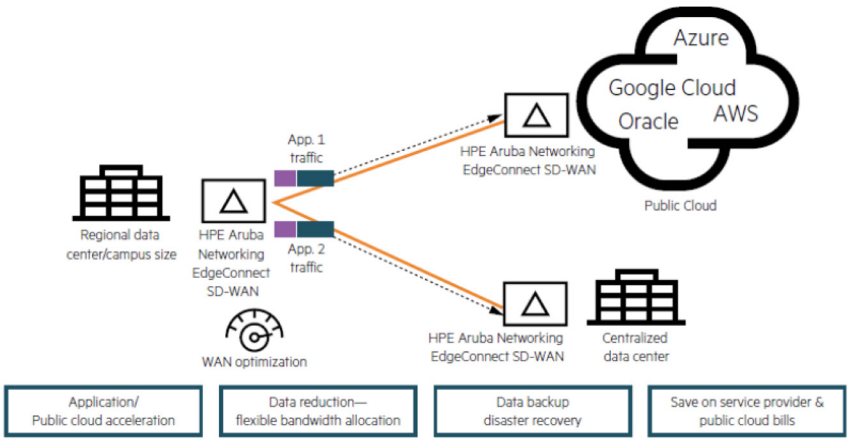

Figure 15. HPE Aruba Networking EdgeConnect WAN Optimization reduces latency effects and increases throughput

HPE Aruba Networking EdgeConnect SD-WAN hardware portfolio

	EdgeConnect SD-WAN 10104	EdgeConnect SD-WAN XS	EdgeConnect SD-WAN 10106	EdgeConnect SD-WAN 10108	EdgeConnect SD-WAN S-P	EdgeConnect SD-WAN M-H	EdgeConnect SD-WAN L-H	EdgeConnect SD-WAN XL-H
Model	EC-10104	EC-XS	EC-10106	EC-10108	EC-S-P	EC-M-H[1]	EC-L-H[1]	EC-XL-H[1]
Typical Deployment[2]	Small branch/ home office	Small branch	Small branch	Medium branch	Large branch	Head office/DC large hub	Data Center large hub	Data center large hub
Typical WAN Bandwidth[3]	2-500 Mbps	2-1000 Mbps	2-1000 Mbps	2-2000 Mbps	10-3000 Mbps	50-5000 Mbps	2-10 Gbps	2-10 Gbps
Simultaneous Connections	256,000	256,000	256,000	256,000	256,000	2,000,000	2,000,000	2,000,000
Recommended WAN Optimization up to	200 Mbps	250 Mbps	250 Mbps	500 Mbps	500 Mbps	1 Gbps	1 Gbps	5 Gbps
IDS/IPS	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Redundancy/FRUs[4]	No	No	No	No	SSD and Power (AC or DC)	SSD and Power	SSD and Power	SSD, NVMe, Power
Datapath Interfaces[5]	4 x RJ45 10/100/1000	4 x RJ45 10/100/1000	2x 10G SFP+ 2x Combo (SFP/1GbE) 2xGbE (PoE)	2x 10G SFP+ 2x Combo (SFP/1GbE) 2xGbE (PoE)	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 1/10G/25G EC-XL-H 10G: 6 x 1/10G

[1] EC XL H and EC XL H 10G comes pre equipped with NVMe for maximum WAN optimization.
[2] For best performance, EdgeConnect SD WAN Operating System Release 9.1 or higher is recommended.
[3] WAN Bandwidth assumes bidirectional traffic (symmetric up link and down link). For total WAN throughput (Rx+Tx), multiply these numbers by 2.
[4] FRU Power Supplies are an additional SKU.
[5] EC 10106, EC 10108, EC S P, EC M H, EC L H and EC XL H all support pluggable optics.

HPE Aruba Networking EdgeConnect SD-WAN gateway specification sheets

EC-US | EC-10104 | EC-XS | EC-10106 | EC-10108
EC-S-P | EC-M-H | EC-L-H | EC-XL-H

HPE Aruba Networking EdgeConnect SD-WAN technical support

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

Flexible deployment models

- **HPE Aruba Networking EdgeConnect SD-WAN Virtual (EC-V) —** Download and install 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. HPE Aruba Networking customers who have an IaaS presence in AWS, Microsoft Azure, Oracle Cloud Infrastructure or Google Cloud Platform can deploy EdgeConnect SD-WAN within their hosted cloud environment.
- **EdgeConnect SD-WAN Physical (EC) —** For enterprises that are not virtualized in the branch, choose one of the EdgeConnect SD-WAN hardware appliance models for plug-and-play deployment.

HPE EdgeConnect SD-WAN tiered subscription licensing

HPE Aruba Networking 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, 3, 5, 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 unlimited bandwidth tiers. Moreover, the Foundation license supports Hub-and-Spoke topology (4 Hubs/ region), a limited number of VRFs, and includes a cloud-hosted SD-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 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 SD-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 SD-WAN Orchestrator can purchase a separate SKU set with the 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 SD-WAN Orchestrator. It is well suited for customers that require a private installation of their SD-WAN management software.

Optional HPE Aruba Networking EdgeConnect SD-WAN licenses

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

WAN Optimization: HPE Aruba Networking EdgeConnect WAN Optimization is an optional WAN optimization performance pack that may be ordered and deployed flexibly to sites that require application acceleration. WAN Optimization is offered in 100 Mbps or 10 Gbps 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 HPE Aruba Networking EdgeConnect SD-WAN Orchestrator Global Enterprise (not applicable for Advanced on-prem license).

Visit **HPE.com**

Chat now (sales)

a00109847ENW, Rev. 1

Hewlett Packard Enterprise