Secure SD-WAN Fabric with HPE Aruba Networking EdgeConnect SD-WAN

Enterprise applications and workloads are distributed in branch offices, headquarters, data center sites, and public and private clouds. In addition, most businesses use SaaS and applications hosted in IaaS that reside outside the enterprise network perimeter. The explosion of mobile and IoT devices in the enterprise has dramatically increased the attack surface, exposing enterprises to security breaches that can compromise data and result in network downtime.

To tackle growing security challenges emerging due to cloud migration and a dissolving security perimeter, enterprises need an advanced, secure SD-WAN solution like the HPE Aruba Networking EdgeConnect SD-WAN platform that includes a built-in next-generation firewall and fine-grained segmentation with identity- and role-based access control, anti-spoofing, attack detection and protection as well as DDoS defense and IDS/IPS to protect branch office sites from malicious activities.

By adopting a secure SD-WAN solution with comprehensive integrated security functions, organizations can retire branch firewalls to simplify WAN architecture and eliminate the cost and complexity associated with ongoing management of dedicated branch firewalls.

To provide a comprehensive edge to cloud security, EdgeConnect SD-WAN tightly integrates with HPE Aruba Networking SSE (Security Service Edge) to enable a unified SASE architecture. The unified SASE solution allows organizations to perform advanced security inspection directly in the cloud instead of backhauling application traffic to a data center before forwarding it to the cloud. Eliminating backhaul improves application performance and response times, enhancing overall end user Quality of Experience.

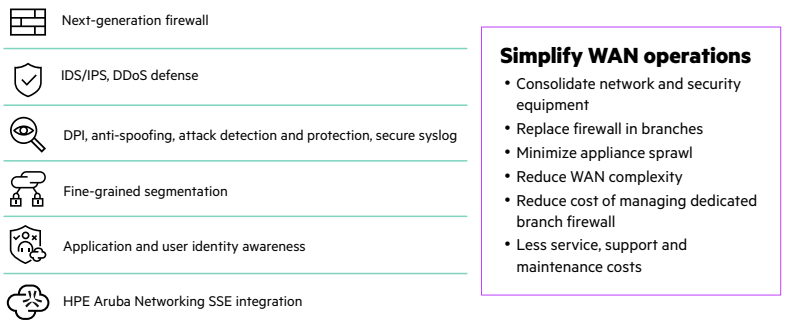

Figure 1. HPE Aruba Networking EdgeConnect SD-WAN platform offers comprehensive integrated security that allows enterprises to retire branch firewalls.

Moreover, applying security policies across many distributed branch sites is often time-consuming and complex, requiring tedious site-by-site configuration. However, with HPE Aruba Networking EdgeConnect SD-WAN, security policies can be easily applied by configuring only once for the entire distributed enterprise, enabling an end-to-end secure SD-WAN fabric. EdgeConnect SD-WAN centrally orchestrates enterprise-wide segmentation spanning the LAN-WAN-LAN, LAN-WAN-Data Center, and LAN-WAN-Cloud. Centralized security policy configuration enables enterprises to quickly segment users, applications, and WAN services into secure end-to-end zones in compliance with predefined security policies, regulatory mandates, and business intent. This results in consistent security policies and automated enforcement across the distributed enterprise. IT can quickly define security policies, control application traffic between zones, and apply policies to groups of applications or individual applications. Once security policies are defined, they are automatically pushed to 1000s of sites without the need to manually program individual devices or send IT experts out into the field.

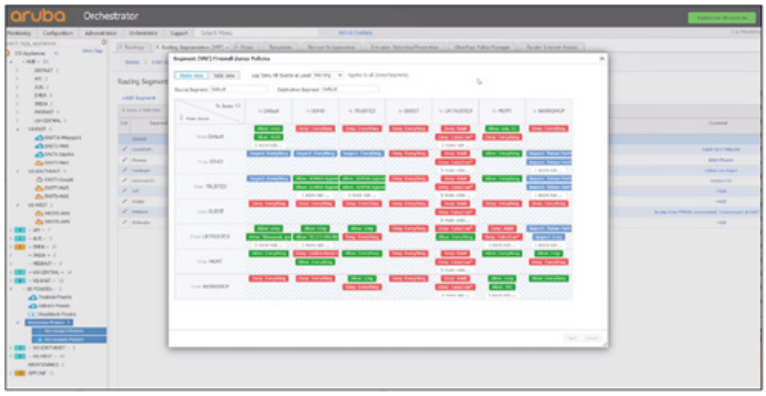

Figure 2. HPE Aruba Networking EdgeConnect SD-WAN enables centralized security policy configuration with an easy-to-use security matrix. Policies are configured only once for the entire SD-WAN fabric and distributed globally to all branch sites.

The HPE Aruba Networking EdgeConnect SD-WAN platform includes:

- **HPE Aruba Networking EdgeConnect SD-WAN:** the physical or virtual SD-WAN appliance deployed in branch offices, data centers, and instantiated in public clouds to create a secure virtual network overlay.
- **HPE Aruba Networking EdgeConnect SD-WAN Orchestrator:** included with EdgeConnect SD-WAN, it is an SD-WAN control plane software that 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.
- **HPE Aruba Networking EdgeConnect WAN Optimization:** is an optional WAN optimization performance pack that provides advanced WAN optimization technologies with EdgeConnect SD-WAN.
- **HPE Aruba Networking EdgeConnect Dynamic Threat Defense (or Advanced Security license):** is an optional security license that adds IDS/IPS support to the EdgeConnect SD-WAN to create a single, secure SD-WAN edge platform.

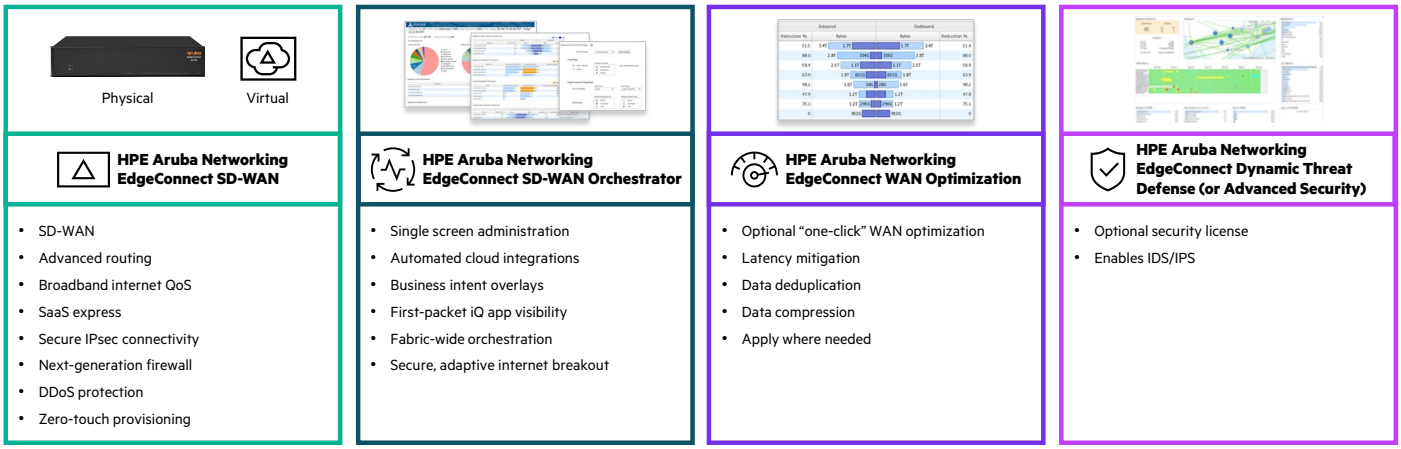

Figure 3. HPE Aruba Networking EdgeConnect SD-WAN platform components

In August 2022, the HPE Aruba Networking EdgeConnect SD-WAN earned the ICSA labs Secure SD-WAN certification, passing rigorous testing based on a comprehensive set of SD-WAN features and robust platform security requirements. In addition to SD-WAN capabilities such as tunnel bonding, dynamic path selection, and zero-touch provisioning, ICSA Labs security requirements for a secure SD-WAN include:

- Support for advanced security functions including DDoS (Distributed Denial of Service) detection and mitigation, anti-malware, and IDS/IPS
- Encryption of sensitive data, as well as administrative and operational communications
- Policy enforcement at SD-WAN edge devices
- Security events logging

The certification assures using a secure SD-WAN solution certified by a globally recognized independent, third-party organization.

Advanced security features of HPE Aruba Networking EdgeConnect SD-WAN

Next-generation Firewall: HPE Aruba Networking EdgeConnect SD-WAN includes a built-in next-generation firewall that provides, advanced security features such as

- Deep-packet inspection
- Intrusion detection and prevention system (IDS/IPS)
- DDoS detection and mitigation
- Application and user identity awareness
- Anti-spoofing
- Attack detection and protection
- Threat logging and security analytics

Fine-grained segmentation: Create secure end-to-end zones across any combination of users, devices, application groups and virtual overlays, pushing configuration updates to sites in accordance with business intent. HPE Aruba Networking ClearPass integration with HPE Aruba Networking 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.

DDoS defense: HPE Aruba Networking 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 DDoS 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. EdgeConnect SD-WAN can also block a list of IP addresses from known attackers and dynamically route the traffic over unaffected network links in case of a DDoS attack ensuring business continuity.

Attack detection and protection: HPE Aruba Networking EdgeConnect SD-WAN detects and prevents attacks such as feature-reset replay attack, ICMP error replay attack, FTP fake clients and FTP bounce attack.

Intrusion Detection and Prevention (IDS/IPS): Included with the optional HPE Aruba Networking EdgeConnect Dynamic Threat Defense license (or Advanced Security License), the intrusion detection/ prevention system (IDS/IPS) can monitor traffic for potential threats and malicious activities and generates threat events based on preconfigured rules. 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 HPE Aruba Networking Central or a third-party SIEM such as Splunk to monitor threats in real time, enabling IT to quickly act.

Splunk integration: HPE Aruba Networking has introduced a custom application for Splunk, called HPE Aruba Networking EdgeConnect Security App. Easily downloadable from Splunkbase, this app leverages the network data provided by the HPE Aruba Networking EdgeConnect SD-WAN platform with Splunk's extensive investigation and visualization capabilities to deliver advanced security reporting and analysis.

Unified SASE with HPE Aruba Networking: The unified SASE solution from HPE Aruba Networking provides a connectivity fabric that comprises award-winning HPE Aruba Networking SSE and industry-leading EdgeConnect SD-WAN into a single solution to meet the increasing demand for integrated networking and security solutions. The solution helps accelerate organizations' journey to SASE. As a unified SASE solution, it is easy to deploy thanks to a single, tightly integrated platform, including simplified management.

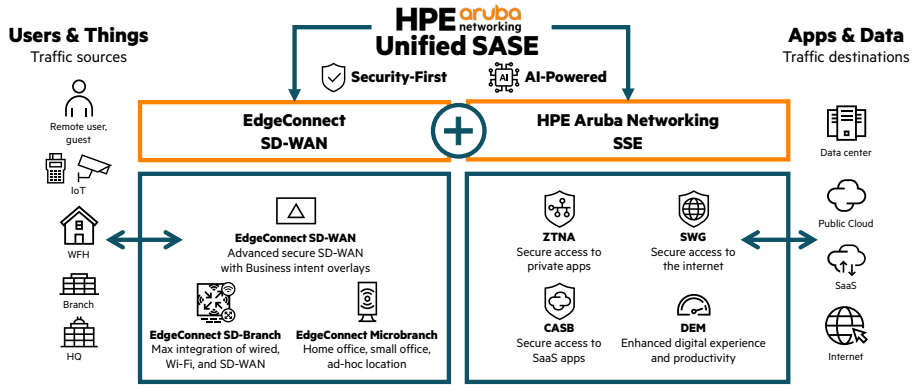

Figure 4. Deploy industry-leading HPE Aruba Networking EdgeConnect SD-WAN with the cloud-native HPE Aruba Networking platform for a unified SASE solution

HPE Aruba Networking SSE is an integrated platform where ZTNA (Zero Trust Network Access), SWG (Secure Web Gateway) and CASB (Cloud Access Security Broker) share a single codebase. All policies are managed from a single user interface, making access control incredibly simple for IT admins. It enables users and authorized third parties to access resources with agent and agentless ZTNA. Users are protected against web-based threats with SWG, and sensitive data hosted in SaaS applications are securely monitored to prevent data loss with CASB. Additionally, the solution harmonizes access across the world via a cloud-backbone of Amazon Web Services (AWS), Microsoft Azure, Google, and Oracle.

EdgeConnect SD-WAN can also seamlessly connect to a variety of cloud security services from third-party vendors, for organizations preferring to adopt SASE with their choice of security services or to seamlessly integrate with an existing security ecosystem. Automated orchestration, using a drag-and-drop interface, enables IT to configure consistent enterprise-wide security policies based on business requirements.

HPE Aruba Networking SD-WAN security features

Security features	Platform
Secure Edge	
Layer 7 firewall	Included with HPE Aruba Networking EdgeConnect SD-WAN Operating System (ECOS)
E2E zone-based enforcement	Included with ECOS
Stateful firewall	Included with ECOS
Deep-packet inspection (DPI)	Included with ECOS
DDoS detection and mitigation	Included with ECOS
Attack detection and protection	Included with ECOS
IP fragmentation flood mitigation	Included with ECOS
Role-based segmentation and ACLs	Included with ECOS
Application-based policy enforcement	Included with ECOS
User and device identity awareness	Included with ECOS
ICSA Labs Secure SD-WAN certification	Included with ECOS
Anti-spoofing	Included with ECOS
Secure syslog	Included with ECOS
Threat notification and logging	Included with ECOS
Firewall logs	Included with ECOS
NetFlow/traffic logs	Included with ECOS
Policy enforcement at SD-WAN edge devices	Included with ECOS
Routing segmentation (VRFs)	Included with ECOS
Encryption of sensitive data **IPsec, IPsec Suite B, IKEv1/v2 (multiple SHA and AES options)**	Included with ECOS
RBAC	Included with ECOS
TACACS/Radius integration	Included with ECOS
OAUTH/SAML SSO	Included with ECOS
JSON web token SSO	Included with ECOS

HPE Aruba Networking SD-WAN security features

Security features	Platform
Secure Edge	
FIPS 140-2 level 1	Included with ECOS
NAC integration	Included with ECOS
IDS/IPS	Requires an optional HPE Aruba Networking EdgeConnect Dynamic Threat Defense license (or Advanced Security license)
Secure Cloud	
ZTNA (Zero Trust Network Access)	Delivered via HPE Aruba Networking SSE
SWG (Secure Web Gateway)	Delivered via HPE Aruba Networking SSE
CASB (Cloud Access Security Broker)	Delivered via HPE Aruba Networking SSE
DLP (Data Loss Prevention)	Delivered via HPE Aruba Networking SSE
DEM (Digital Experience Monitoring)	Delivered via HPE Aruba Networking SSE

* For best performance, HPE Aruba Networking EdgeConnect SD-WAN Operating System (ECOS) 9.2 or higher is recommended. ECOS base license is included with EdgeConnect SD-WAN platform.

Conclusion

As the threat landscape continues to evolve, enterprises need a secure SD-WAN solution like HPE Aruba Networking EdgeConnect SD-WAN that supports all necessary branch WAN edge security functions including a built-in next-generation firewall, fine-grained segmentation with identity- and role-based access control, anti-spoofing, DDoS defense, attack detection and protection, IDS/IPS, and consistent end-to-end security policy enforcement spanning the LAN, WAN, Data Center, and the Cloud. With EdgeConnect SD-WAN, organizations can retire branch firewalls to simplify WAN architecture and integrate with HPE Aruba Networking SSE to gain the freedom and flexibility that comes with a unified SASE platform.

Make the right purchase decision.
Contact our presales specialists.

Contact us

Visit **ArubaNetworks.com**

Hewlett Packard Enterprise

DS_Secure-SD-WAN-Fabric_RVK_032824 a00126773ENW