HPE aruba networking

Data sheet

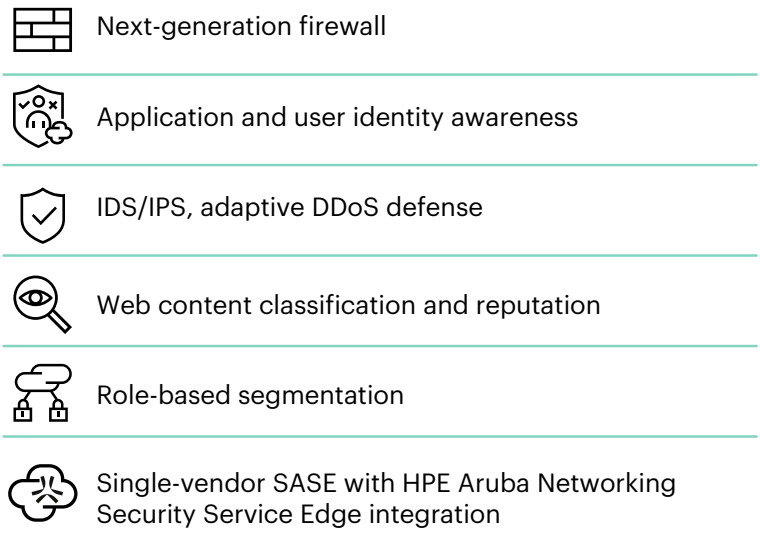
Zero trust and threat defense with HPE Aruba Networking EdgeConnect SD-WAN

HPE

In today's hyper-connected digital world, cybersecurity is no longer an optional safeguard — it's a business imperative. Enterprises operate in an environment where cyber threats are not just increasing in frequency but also in sophistication. These threats encompass a wide range of challenges, including malware, phishing attacks, ransomware, and data breaches.

To tackle growing security challenges, enterprises can enforce zero trust principles and simplify security architectures in branch locations with an advanced, secure SD-WAN solution such as HPE Aruba Networking EdgeConnect SD-WAN. The solution includes a built-in next-generation firewall with intrusion detection and prevention system (IDS/IPS), adaptive distributed denial of service (DDoS) capabilities, and role-based segmentation to protect branch offices from malicious activities. By adopting a secure SD-WAN solution with comprehensive integrated security functions, organizations can retire branch firewalls to simplify branch infrastructure and eliminate the cost and complexity associated with ongoing management of dedicated branch firewalls. Security policies can be applied once for the entire distributed enterprise, simplifying management and operations.

Additionally, HPE Aruba Networking EdgeConnect SD-WAN tightly integrates with HPE Aruba Networking SSE (Security Service Edge) to form a single-vendor SASE solution, providing secure, optimized access to SaaS, private applications, and the internet. It allows organizations to enforce least-privilege access for hybrid workers, protect users from web-based threats, and safeguard sensitive data in SaaS applications.



Simplify branch security

- Consolidate network and security equipment
- Replace firewall in branches
- Reduce appliance sprawl
- Reduce WAN complexity
- Reduce cost of managing dedicated branch firewall
- Less service, support, and maintenance costs

Figure 1. Integrated zero trust security in HPE Aruba Networking EdgeConnect SD-WAN

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 HPE Aruba Networking 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:** An optional WAN optimization performance pack that provides advanced WAN optimization technologies with HPE Aruba Networking EdgeConnect SD-WAN.

— **HPE Aruba Networking EdgeConnect dynamic threat defense (or advanced security license):** An optional security license that adds IDS/IPS, adaptive DDoS, smart SYN cookie, and secure web service (web classification and reputation, IP reputation) to the HPE Aruba Networking EdgeConnect SD-WAN to create a single, secure SD-WAN platform.

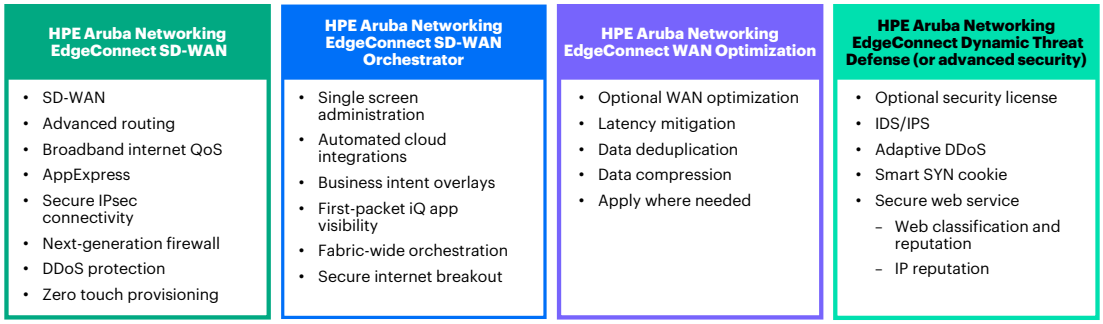


Figure 2. HPE Aruba Networking EdgeConnect SD-WAN platform components

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:

— End-to-end segmentation
— Role-based segmentation
— Network access control (NAC) security
— Web classification and reputation, IP reputation
— Adaptive DDoS protection
— Smart SYN cookie
— IDS/IPS
— Threat logging and security analytics
— Integration with security service edge (SSE)

End-to-end segmentation: HPE Aruba Networking 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.

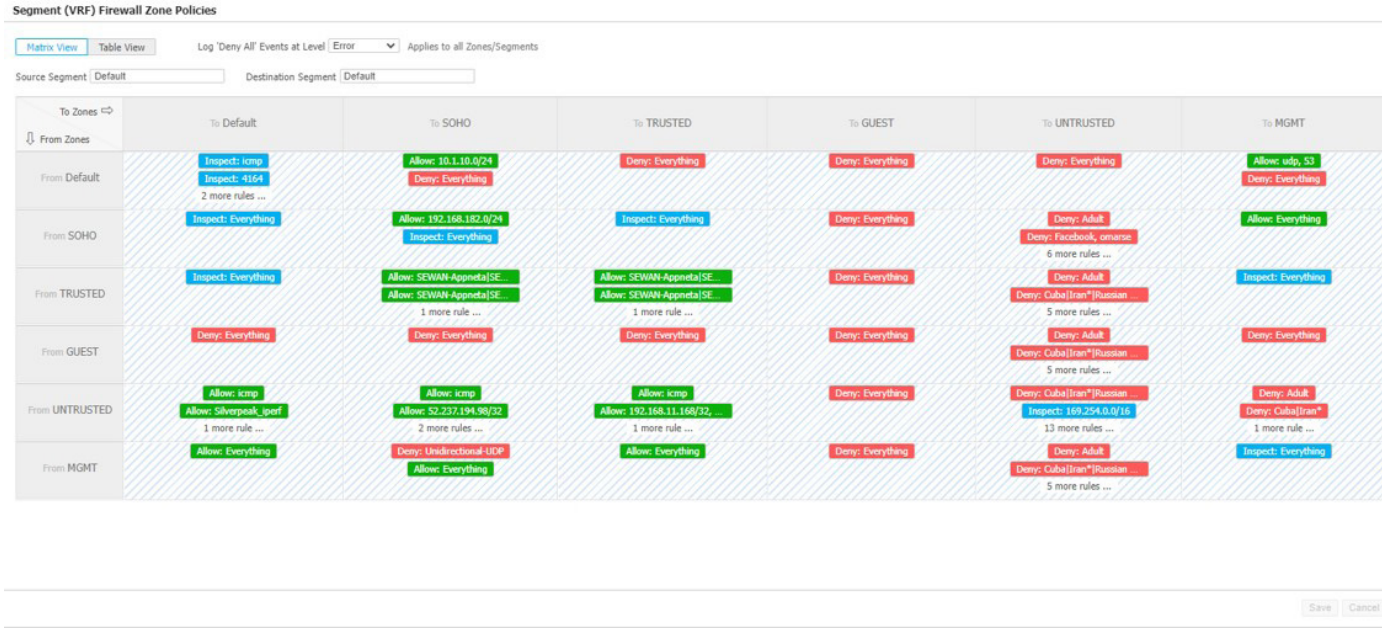


Figure 3. HPE Aruba Networking EdgeConnect SD-WAN enables centralized security policy configuration with an easy-to-use security matrix

Role-based segmentation: HPE Aruba Networking ClearPass integration with HPE Aruba Networking EdgeConnect SD-WAN augments application intelligence with the user and device identity and role-based policies, enabling fine-grained segmentation without the complexity of managing multiple VLANs. The additional identity-based context offers consistent security policy enforcement that can be deployed network-wide, from edge to cloud, simplifying operations and management. Additionally, with the proliferation of IoT devices, it helps identify IoT devices and segments the network to isolate IoT traffic from mission-critical applications.

NAC security: The integration of HPE Aruba Networking ClearPass enables administrators to secure HPE Aruba Networking 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 NAC enabled, the HPE Aruba Networking 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.

Threat intelligence with secure web service: With the optional secure web service, HPE Aruba Networking EdgeConnect SD-WAN enhances security with advanced web classification and reputation, as well as IP reputation analysis.

Web classification and reputation (also known as URL filtering) helps organizations block access to harmful, inappropriate, or illegal websites that propagate malware, spam, spyware, and phishing attacks, as well as websites with sensitive content such as adult or gambling content. The solution tracks more than 1 billion domains and 43 billion URLs and classifies them into more than 85 site categories, including high-risk categories, by leveraging machine learning to increase speed and accuracy. To determine web reputation, the service uses site history, age, rank, location, networks, links, real-time performance, and other contextual and behavioral trend data to determine a URL reputation score from 1 to 100, with tiers split into trustworthy, low risk, moderate risk, suspicious, and high risk.

In addition to web classification and reputation, the IP reputation service strengthens security by providing real-time threat intelligence and global visibility into millions of malicious IPs, with new threats detected daily. IPs are categorized by threat types, including Windows exploits, web attacks, phishing, botnets, scanners, reputation, spam sources, mobile threats, and proxies. Using data analysis and correlation, the service assigns a predictive risk score from 1 to 100 for each IP address. Based on this score, IPs are classified into five tiers similar to URL reputation scores. This enables administrators to quickly identify and block high-risk IPs, helping prevent cyber threats such as malware, ransomware, phishing, and command-and-control attacks.

DDoS defense: HPE Aruba Networking EdgeConnect SD-WAN detects and prevents DDoS attacks such as protocol attacks, ICMP floods, SYN floods, IP spoofing attacks and more. The solution enforces strict state handling and limits the number of malicious requests through actions such as rapid aging, drop excess and block source, defined for preset or configurable DoS thresholds. With firewall protection profiles, administrators can enforce different levels of DDoS protection levels across the organization by binding firewall protection profiles to firewall zones.

To configure DoS thresholds, the solution combines three categories including threshold classification (source-level and zone-level), metrics to monitor (flows per second, concurrent flows and embryonic flows) and IP protocol (TCP, UDP, ICMP, others, and all). Each threshold is associated with a minimum and maximum value. 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.

For each threshold, the solution provides the following actions: log, rapid aging, drop excess, block source, and enables SYN cookies for maximum action. The use of SYN cookies prevents legitimate connections from being dropped when the SYN queue fills up during SYN flood attacks. This is achieved by embedding a cookie in the SYN-ACK response, which verifies that the client IP address is real and not spoofed.

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 (for example, 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.

Additionally, the solution includes a comprehensive set of reports for DoS defense including threshold violations, flow drops, denied hosts and packets counts, top talkers, and alarms such as exceeded DoS thresholds.

Smart SYN cookie is an optional feature that adds intelligence to the traditional SYN cookie mechanism, optimizing performance where cookie generation can be resource intensive. A cap is automatically enforced on the number of SYN cookies generated to prevent resource exhaustion. SYN packets exceeding the limit are dropped to preserve system stability. The system also evaluates the reputation of the source IPs based on historical behavior. IP reputation applies to internal IPs (or LAN IPs) and external IPs when the secure web service option is enabled. Depending on the IP reputation score, the solution decides whether to respond with a SYN cookie, allow a normal flow, or denylist the source IP.

Intrusion detection and prevention (IDS/IPS): Included with the optional HPE Aruba Networking EdgeConnect dynamic threat defense license (or advanced security license), 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 HPE Aruba Networking 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 provides a dashboard view of IDS/IPS events stemming from HPE Aruba Networking EdgeConnect SD-WAN with Splunk's extensive investigation and visualization capabilities to deliver advanced security reporting and analysis.

SASE with HPE Aruba Networking SSE: To address the growing demand for integrated networking and security in the era of hybrid working and cloud computing, the HPE Aruba Networking EdgeConnect SD-WAN solution seamlessly combines with HPE Aruba Networking SSE to establish a single-vendor SASE platform. This cohesive approach streamlines adoption and accelerates deployment of SASE.

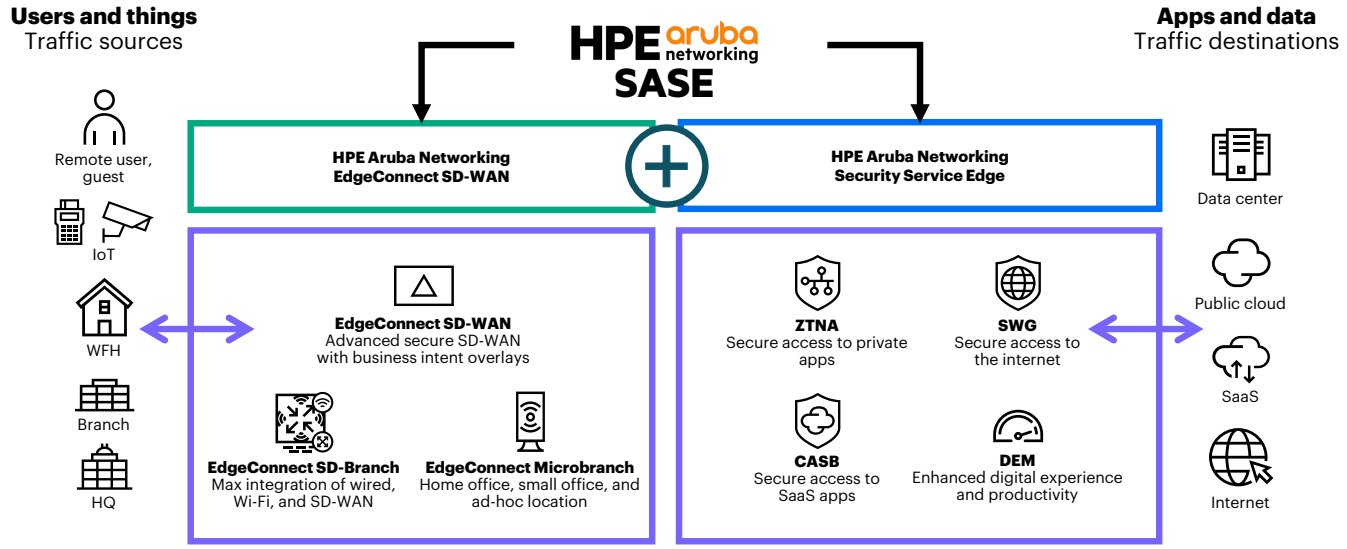


Figure 4. Deploy industry-leading HPE Aruba Networking EdgeConnect SD-WAN with the cloud-native HPE Aruba Networking SSE platform for a single-vendor SASE solution

HPE Aruba Networking SSE is a cloud-native solution where zero trust network access (ZTNA), secure web gateway (SWG), and cloud access security broker (CASB) 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 through a cloud-backbone of Amazon Web Services (AWS), Microsoft Azure, and Google™.

HPE Aruba Networking 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 EdgeConnect SD-WAN security features

Security features	Description
Secure edge	
Layer 7 firewall	Included with HPE Aruba Networking EdgeConnect SD-WAN
End-to-end zone-based enforcement	Included
Stateful firewall	Included
DDoS detection and mitigation	Included
IP fragmentation flood mitigation	Included
End-to-end segmentation and ACLs	Included
Application-based policy enforcement	Included
User and device identity awareness	Included
Anti spoofing	Included
Secure syslog	Included
Threat notification and logging	Included
Firewall logs	Included
NetFlow/traffic logs	Included
Policy enforcement at SD-WAN edge devices	Included
Routing segmentation (VRFs)	Included
Encryption of sensitive data IPSec, IPSec Suite B, IKEv1/v2 (multiple SHA & AES options)	Included
TACACS/RADIUS integration	Included
OAUTH/SAML SSO	Included
JSON Web Token SSO	Included
FIPS 140-2 Level 1	Included
Common criteria certification	Included
IDS/IPS	Requires an optional HPE Aruba Networking EdgeConnect dynamic threat defense license (or advanced security license)
Adaptive DDoS	Requires an optional HPE Aruba Networking EdgeConnect dynamic threat defense license (or advanced security license)
Smart SYN cookie	Requires an optional HPE Aruba Networking EdgeConnect dynamic threat defense license (or advanced security license)

Security features	Description
Web classification and reputation (URL filtering)	Requires an optional HPE Aruba Networking EdgeConnect dynamic threat defense license (or advanced security license)
IP reputation	Requires an optional HPE Aruba Networking EdgeConnect dynamic threat defense license (or advanced security license)
Role-based segmentation	Requires HPE Aruba Networking ClearPass integration
NAC security	Requires HPE Aruba Networking ClearPass integration
Secure cloud	
ZTNA	Delivered through HPE Aruba Networking SSE
SWG	Delivered through HPE Aruba Networking SSE
CASB	Delivered through HPE Aruba Networking SSE
Data loss prevention (DLP)	Delivered through HPE Aruba Networking SSE
Digital experience monitoring (DEM)	Delivered through HPE Aruba Networking SSE

For best performance, HPE Aruba Networking EdgeConnect SD-WAN Operating System (ECOS) 9.6 or higher is recommended. ECOS base license is included with EdgeConnect SD-WAN platform.

Conclusion

As cyber threats become more sophisticated and organizations are more distributed, enterprises require a secure SD-WAN solution such as HPE Aruba Networking EdgeConnect SD-WAN to enforce zero trust principles in branch locations. This solution features a built-in next-generation firewall with IDS/IPS, adaptive DDoS defense, URL filtering, role-based segmentation, and consistent end-to-end security policy enforcement across the LAN, WAN, data center, and cloud. By adopting HPE Aruba Networking EdgeConnect SD-WAN, organizations can replace branch firewalls to streamline their architecture and integrate with HPE Aruba Networking SSE, forming a single-vendor SASE solution to secure access to applications and the internet.

Learn more at

HPE.com/SD-WAN

Visit HPE.com

Chat now

a00126773ENW, Rev. 2

HEWLETT PACKARD ENTERPRISE

hpe.com