HPE aruba networking

Elevate branch security with secure SD-WAN and SWG, establishing the foundation for SASE

In today's world, branch offices play a crucial role in the operations of many organizations, but they face increasing cybersecurity challenges. The proliferation of cloud-based applications, IoT devices, and remote work has expanded the attack surface, making these branch locations prime targets for cyberattacks.

HPE GreenLake

25%

of respondents consider integrated security such as next-generation firewall, SWG, DPI, UTM, and URL filtering, as the most important feature for SD-WAN[1]

15b+

IoT devices will connect to enterprise infrastructure by 2029[2]

Traditional security models, focused on central corporate networks, are insufficient for protecting the diverse and dispersed nature of modern branch offices. Legacy firewalls are difficult to manage and require local expertise. Applying security policies across many distributed branch sites is time-consuming and complex, often resulting in inconsistent security measures.

Additionally, standalone SWG (Secure Web Gateway) solutions often fall short in providing comprehensive security for both managed and unmanaged devices. Users and devices can inadvertently access infected sites, leading to potential ransomware and phishing attacks. Unmanaged devices such as guests, third-party contractors, or BYODs can reach malicious websites as they connect to the enterprise network, introducing new threats into the organization. IoT devices are also prone to web-based threats as they generate web traffic when they communicate with cloud services for AI model training, updates, telemetry, or other purposes.

Therefore, organizations must adopt a holistic security framework to cope with the dynamic nature of modern networks and offer comprehensive protection against a wide array of cyber threats to branch locations.

EdgeConnect SD-WAN built-in next-generation firewall

EdgeConnect SD-WAN addresses the cybersecurity challenges faced by branch locations by integrating advanced security features such as a next-generation firewall (NGFW), Intrusion Detection and Prevention System (IDS/IPS), and Distributed Denial-of-Service (DDoS) protection.

- **NGFW** provides comprehensive threat prevention by inspecting traffic at a deeper level, blocking malware and enforcing security policies based on application, user identity, and context.
- **IDS/IPS** is a signature-based system that continuously monitors network traffic for suspicious patterns and automatically takes action to block potential threats. The system can operate either in inline mode or performant mode. In inline mode, the traffic passes through the sensor so that the traffic is immediately blocked when an intrusion occurs. In performant mode, a copy of the traffic is sent for analysis, providing more efficiency without impacting network performance.
- **DDoS defense** protects organizations against DDoS attacks such as protocol attacks, ICMP floods, and SYN floods. EdgeConnect SD-WAN mitigates malicious requests through rapid aging, dropping excess traffic, and blocking sources. Actions are based on preset or configurable DoS thresholds set for traffic parameters including flow rate, concurrent flows, and embryonic flows.
- **Threat logging** provides network and security analytics to HPE Aruba Networking Central, or a third-party SIEM such as Splunk, to monitor threats in real time. The EdgeConnect SD-WAN Security App for Splunk provides a dashboard view of all security event notifications exported from EdgeConnect SD-WAN devices within an enterprise's SD-WAN.

[1] Worldwide SD-WAN Infrastructure 2023 Vendor Assessment, IDC

[2] Gartner, February 2021

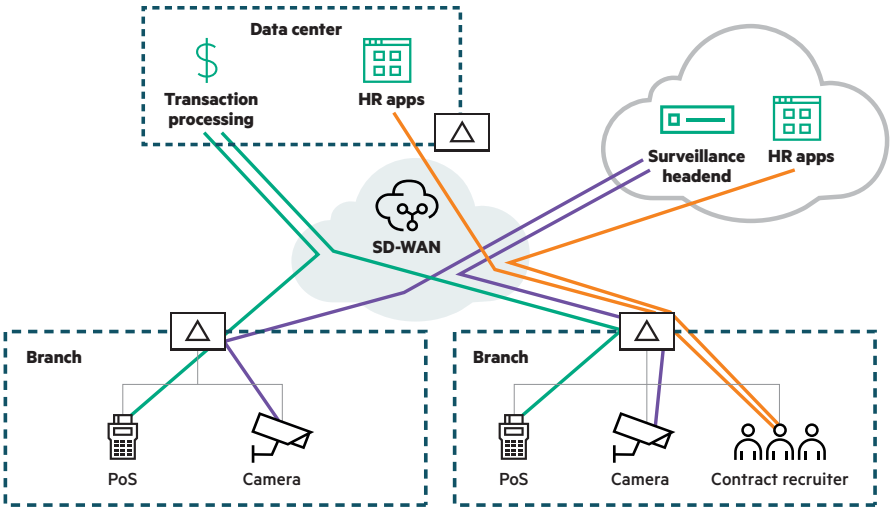
This integration enables organizations to easily replace traditional branch firewalls, centralizing security policy management and eliminating the need for local technical expertise. It is worth mentioning that in some cases, like rapid scaling or a robust WAN infrastructure, FWaaS capabilities within HPE Aruba Networking SSE can provide advanced branch protection and replace legacy branch firewalls.

Table 1. HPE Aruba Networking EdgeConnect SD-WAN offers comprehensive security to easily replace branch firewalls.

Feature	EdgeConnect SD-WAN
Next-generation firewall	✓
IDS/IPS	✓
DDoS Defense	✓
Role-based segmentation	✓
IoT security	✓
Security events logging	✓
SWG with no SSE agent installed	✓
Unified SASE integration	✓

Comprehensive protection for all devices, managed and unmanaged

HPE Aruba Networking ClearPass integration with EdgeConnect SD-WAN augments application intelligence with identity and role-based policy, enabling role-based segmentation. With role-based segmentation, EdgeConnect SD-WAN can effectively secure unmanaged devices, such as IoT, by isolating their traffic from mission-critical applications. This segmentation ensures that IoT devices, which might be more vulnerable to attacks, do not compromise the security of essential business operations. Additionally, EdgeConnect SD-WAN can transport role information, even in complex multi-vendor LAN environments, leveraging EVPN/VXLAN open standards, to enforce role-based segmentation across the entire fabric.



Role-based segmentation ensures that users and devices only reach destinations consistent with their role in the business

Defending against web-based threats with SWG

To comprehensively protect all network users and devices, including IoT, against web-based threats, EdgeConnect SD-WAN can be augmented with SWG, eliminating the need to install an SSE agent on each device. This is achieved by directing all network traffic through a dedicated tunnel to HPE Aruba Networking SWG, ensuring that both managed and unmanaged devices receive the same level of protection. Unmanaged devices are shielded from web-based threats as effectively as managed devices.

HPE Aruba Networking SWG protects organizations against web-based threats. It inspects all web traffic for malicious content, including encrypted traffic, and blocks access to harmful websites. The solution uses a 3-layer protection including URL, DNS and content filtering, paired with SSL decryption for encrypted HTTPS traffic. It performs real-time scanning of web traffic to detect and block malware and other malicious content, while using security policies to restrict access to specific categories of websites, including adult content, gambling platforms, and sites known to pose significant risks. It can also be combined with DLP to prevent the leakage of sensitive data and monitor user activity.

Extending to unified SASE with ZTNA and CASB

EdgeConnect SD-WAN, augmented with SWG, forms the foundation for a robust cybersecurity framework and can be seamlessly extended to a comprehensive Secure Access Service Edge (SASE) architecture by integrating Zero Trust Network Access (ZTNA) and Cloud Access Security Broker (CASB) capabilities.

- **HPE Aruba Networking ZTNA** ensures that every access request is authenticated and authorized based on the user's identity and context. Unlike traditional VPNs that provide broad access to the network, ZTNA limits access to specific applications and resources, enforcing least-privilege access.
- **HPE Aruba Networking CASB** enhances security for SaaS applications by providing visibility and control over sensitive data hosted in SaaS applications, enforcing security policies, and preventing data loss.

Benefits

- **Comprehensive zero trust security**
  The integration of SD-WAN with SWG provides a cohesive security approach, protecting all users and devices, including IoT, on the network from web-based threats. The built-in, next-generation firewall adds an extra layer of security, enhancing the overall protection framework with features like IDS/IPS, DDoS protection, and role-based segmentation.

- **Reduced hardware footprint and simplified operations**
  Replacing traditional branch firewalls with EdgeConnect SD-WAN simplifies management through centralized policy control. This approach reduces the need for local technical expertise, lowers hardware and maintenance costs, and ensures consistent security policies across all branch locations.

- **Accelerated journey to unified SASE**
  Organizations can easily transition to a unified SASE architecture. This integrated approach streamlines the security framework, ensuring seamless deployment, unified security policies, centralized management, and adaptation to evolving threats.

Replace legacy branch firewalls now

EdgeConnect SD-WAN, augmented with SWG, delivers a comprehensive, next-generation firewall capability that integrates advanced security features like IDS/IPS, DDoS protection, and role-based segmentation. By consolidating these functionalities into a single solution, it simplifies network security management and enhances protection for all devices, including IoT. This unified approach, combined with zero trust segmentation, ensures robust security across the network, facilitating a seamless transition to a unified SASE architecture.

Learn more at

HPE Aruba Networking EdgeConnect SD-WAN

HPE Aruba Networking unified SASE

Architecting SASE with a Secure Business-Driven SD-WAN

Secure SD-WAN with integrated SWG: Building the foundation to unified SASE

Visit **ArubaNetworks.com**

Make the right purchase decision.
Contact our presales specialists.

Contact us

Hewlett Packard Enterprise

AAG_Secure_SD-WAN_A4_SG_073024 a00141673ENW