HPE aruba networking

Brochure

Four reasons to replace branch firewalls with a secure SD-WAN

Hewlett Packard Enterprise | BlueAlly

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

There was a time when SD-WAN solutions only focused on WAN virtualization with few considerations for security. Advanced secure SD-WAN solutions have emerged to fill this security gap to include the highest threat protection capabilities. In fact, the advanced security functions now supported on the most advanced SD-WAN platforms enable customers to completely retire dedicated branch firewalls and further simplify branch WAN infrastructure.

With a network architecture shifting to the cloud, branch offices must now tackle new security challenges as the network grows more complex, and more users connect outside the security perimeter. At the same time, enterprises are asking for more flexibility to cope with the growing number of cloud applications or the challenges of opening new branches or introducing new applications more quickly. Traditional network infrastructure based on MPLS, routers, and firewalls are unable to keep up with this trend due to their rigidity, cost, complexity, and because they were never designed for the cloud.

That's why secure SD-WAN solutions incorporate next-generation firewall capabilities — allowing organizations to perform simple and quick deployments without compromising security. These solutions leverage the flexibility offered by SD-WAN virtual overlays combined with firewall capabilities, providing security across the LAN, WAN, and cloud. With these advanced solutions, network administrators can:

- Create zones and restrict access between zones to segment the network based on identity and role
- Detect and prevent intrusions and DDoS attacks
- Perform deep packet inspection and filter packets based on applications
- Monitor the full state of active network connections
- Secure connections through data encryption
- Tightly integrate with security functions best performed in the cloud such as SWG, CASB, and ZTNA
- Log security events, and much more

The following sections describe the four reasons organizations replace their branch firewalls with an advanced secure SD-WAN to fully embrace the cloud-first era and modernize both network and security architectures.

Reason #1: A secure SD-WAN delivers comprehensive security services

Secure SD-WAN solutions incorporate next-generation firewall capabilities such as deep packet inspection, IDS/IPS, DDoS protection, and application and access control through identity-based policies and events logging.

IDS/IPS typically monitors network traffic to find patterns that match a particular attack signature. When an intrusion is detected, the system performs actions such as inspect, drop, and allow traffic. In the event of a DDoS attack, a secure SD-WAN limits the number of malicious requests with actions such as rapid aging, drop excess, and block source. Event logging can be filtered and viewed across the entire SD-WAN fabric to analyze events that require further investigation.

To provide flexibility to connect remote branches, SD-WAN combines heterogeneous links such as MPLS, internet, and 5G. However, unlike MPLS, internet and 5G links are not secure. To secure these links, a secure SD-WAN solution builds IPsec tunnels using AES 256-bit encryption across the entire SD-WAN fabric, protecting branch offices from potential data breaches. When SD-WAN virtual appliances are deployed in public clouds, IPsec tunnels are also created, extending corporate security policies to the cloud.

Finally, an advanced SD-WAN enforces security policies across the entire fabric by automatically propagating policy changes to branch offices through central orchestration.

Unlike branch firewalls, a secure SD-WAN provides advanced threat protection and also secures untrusted links and seamlessly enforces security policies across branch offices.

Reason #2: A secure SD-WAN simplifies local operations

In traditional router-based environments, local branches must deal with a sprawl of network and security equipment accumulated over the years. Additionally, local branches often lack experienced IT staff to install and maintain this equipment.

Not only does a secure SD-WAN integrate a next-generation firewall, but it also includes WAN capabilities such as routing and WAN optimization so that organizations can consolidate their equipment into one single appliance. It increases IT efficiency by consolidating network and security management in a single console instead of supporting multiple disparate management tools.

A secure SD-WAN is easy to deploy with zero-touch provisioning. No experienced IT staff is required locally because configuration and security policies are automatically pushed to branches. It's quick and easy to set up new branch offices, and security policy changes can be automatically distributed to hundreds or thousands of branches in minutes while minimizing errors.

Unlike branch firewalls, a secure SD-WAN relies on a thin branch model that is easy to deploy, flexible, and secure.

Reason #3: A secure SD-WAN fully supports cloud-first organizations

Traditionally, organizations routed the traffic to a data center for security inspection. As organizations have moved most of their applications to the cloud and increasingly use cloud applications like Microsoft 365, Salesforce, or RingCentral, sending the traffic back to the data center negatively impacts application performance.

A secure SD-WAN can break out cloud application traffic locally, eliminating inefficient backhaul to the data center. It automatically steers traffic to the internet based on business policies by identifying applications on the first packet, which greatly improves performance, and hence user experience. For example, trusted cloud applications, as defined by an organization's security policies, can be sent directly to the cloud while untrusted applications can be directed first to a cloud-delivered security service before forwarding to the SaaS provider. This approach allows organizations to build a SASE architecture by automatically steering traffic to a Security Service Edge (SSE) solution.

Unlike branch firewalls, a secure SD-WAN solution supports cloud-first organizations, improving performance and security, while streamlining the journey to SASE.

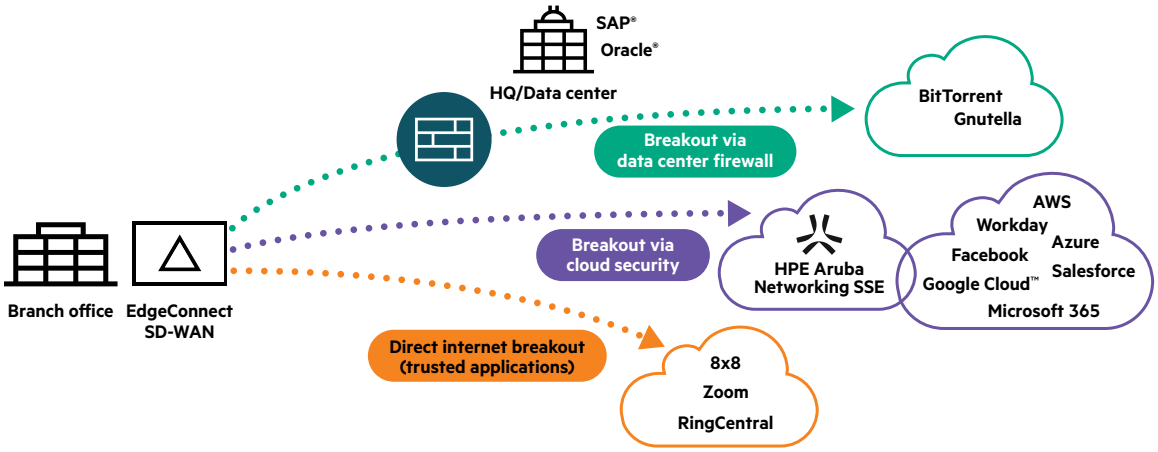

Figure 1. Intelligently steer traffic to the cloud with a secure SD-WAN

Reason #4: A secure SD-WAN helps secure IoT devices

In recent years, organizations have witnessed an explosion in the number of IoT devices, dramatically increasing the attack surface and posing major cybersecurity risks. IoT devices, based on a simple architecture, cannot run security agents. Therefore, organizations require a different security approach for IoT devices to protect their networks from potential vulnerabilities.

A secure SD-WAN solution goes beyond what is defined by SASE with its next-generation firewall capabilities. It can implement zero trust network segmentation, with identity and role-based access control, ensuring that users and IoT devices can only reach network destinations consistent with their role in the business.

IoT devices are also prone to web-based threats as they generate web traffic when they communicate with cloud services for updates, telemetry, or other purposes. The integration of Secure Web Gateway (SWG) to a secure SD-WAN ensures consistent and comprehensive protection for all devices on the enterprise network. As devices connect to the enterprise network, secure SD-WAN automatically directs the traffic to an SWG through dedicated tunnels, without requiring an SSE agent.

Unlike branch firewalls, a secure SD-WAN solution creates micro-segmentation extended from the LAN, across the WAN, and to data centers and cloud platforms. It seamlessly connects to SWG to protect all network devices from web-based threats.

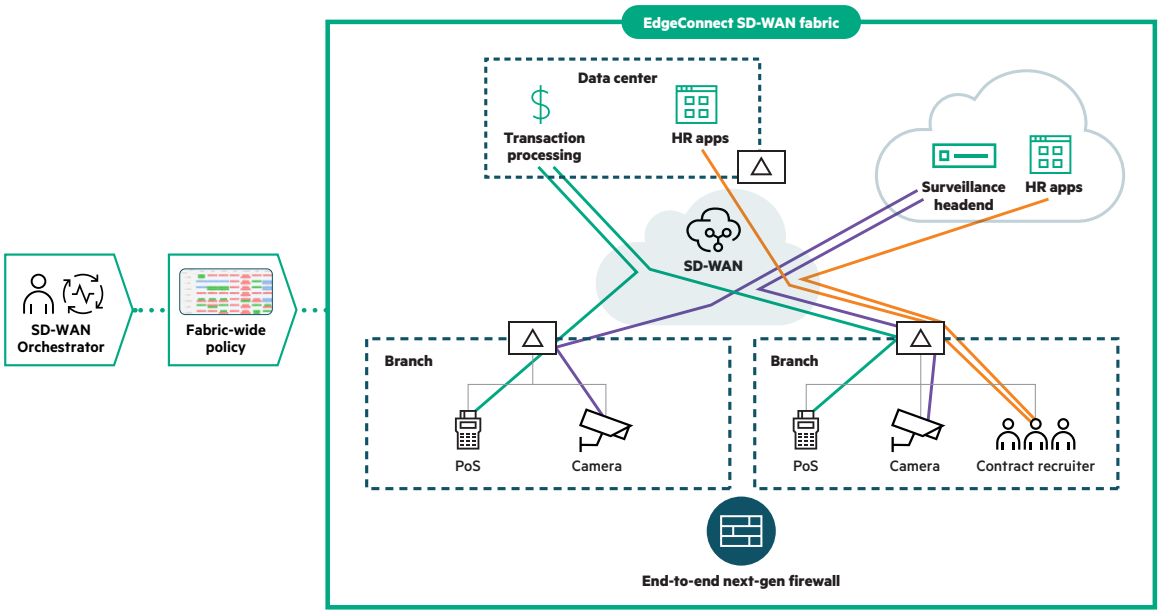

Figure 2. Secure IoT traffic with role-based segmentation with a secure SD-WAN

An advanced secure SD-WAN solution for the cloud-first era

A secure SD-WAN solution such as HPE Aruba Networking 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 offices from malicious activities. The solution tightly integrates with HPE Aruba Networking SSE as well as third-party SSE providers to form a robust SASE architecture.

Our solution partner

BlueAlly

BlueAlly is an authorized partner of HPE

(800) 886-5369
contact@blueally.com
www.blueally.com

For more information about HPE Aruba Networking, visit our partner website: www.securewirelessworks.com

HPE Aruba Networking EdgeConnect SD-WAN integrates SWG, part of HPE Aruba Networking SSE, through a single site license. The solution offers comprehensive protection to all users and things on the network. It is easy to deploy and doesn't require an agent installed on each device.

Recognized by an independent, global organization, EdgeConnect SD-WAN has earned the Secure SD-WAN certification from ICSA Labs thanks to its advanced SD-WAN and security features. The certification provides the assurance to securely replace firewalls in branches. It allows organizations to gain flexibility and reduce risk when implementing security controls at the branch and across the WAN. It increases IT efficiency, simplifies management by consolidating network and security equipment into one single platform, and helps enforce consistent security policy.

Learn more

arubanetworks.com/products/sd-wan

Visit **ArubaNetworks.com**

Make the right purchase decision. Contact our presales specialists.

Chat now (sales)

Call now

Get updates

Hewlett Packard Enterprise

BR_Replace-branch-firewalls-SD-WAN_Co-Brand_A4_RB_073024 a00141990ENW