HPE aruba networking

Business white paper

Architecting SASE with a secure business-driven SD-WAN

Hewlett Packard Enterprise | BlueAlly

Table of contents

Learn how the HPE Aruba Networking EdgeConnect Secure SD-WAN platform delivers unmatched protection and accelerate your journey to SASE

Executive summary

Software-driven wide area networks (SD-WAN) are enabling today's geographically distributed enterprises to realize the transformational promise of cloud computing, reduce capital and operating costs, provide the highest quality of experience for employees and customers, and adapt quickly to changing business requirements.

But digital transformation, cloud computing and hybrid working introduce new security challenges. These include:

- Users connecting from anywhere and from any device
- Increasing cybersecurity risks
- More sensitive data hosted in the cloud
- Proliferation of IoT devices increasing the attack surface
- Complying with regulations and industry standards

A key benefit delivered by an SD-WAN is the ability to actively utilize low-cost broadband services. However, because broadband services are "public" instead of "private", advanced security capabilities are required to ensure the confidentiality and integrity of application traffic traversing such connections. With a built-in firewall, secure SD-WANs provide advanced security at the branch including IDS/IPS and DDoS protection, it isolates IoT traffic from mission-critical applications by segmenting networks into zones and minimizes the attack surface to help compliance with industry standards.

Additionally, by moving most of their business applications to the cloud, organizations are facing new security challenges such as providing secure access to remote workers, safeguarding internet users from web-based threats, and ensuring sensitive corporate data hosted in cloud applications remains protected and exempt from data leaks.

By tightly integrating to SSE (Security Service Edge) solutions, advanced secure SD-WAN creates a robust SASE architecture allowing organizations to tackle the challenges of hybrid working and cloud computing.

This paper discusses why SD-WAN is critical to security, and how a comprehensive SD-WAN security deployment can better safeguard today's dynamic, cloud-first enterprises. It then goes on to reveal the extensive set of security capabilities incorporated in the HPE Aruba Networking EdgeConnect SD-WAN platform, including a next-generation firewall, and how the SD-WAN platform tightly integrates with Security Service Edge (SSE) capabilities, either with HPE Aruba Networking SSE to form a unified SASE (Secure Access Service Edge) solution, or with third-party cloud-security vendors.

Network security in the cloud era "Hybrid work and the relentless shift to cloud computing has accelerated SASE adoption"

– Gartner 2022[1]

As more applications and workloads migrate to the cloud, the role of the corporate data center has been significantly reduced. With hybrid working, the security perimeter is also dissolving as users connect from anywhere and from any device, accessing sensitive data hosted in the cloud.

Organizations that try to manage WANs using traditional routers are faced with continual compromises and trade-offs. Manual processes and complex architectures prevent organizations from establishing a secure architecture and effectively respond to malicious threats such as denial of service (DoS) attacks. Security concerns can hamper the use of low-cost broadband connections and slow the move toward the cloud in general, and SaaS applications in particular.

[1] Top Trends Impacting Infrastructure and Operations for 2023, Gartner, December 2022

The impact of these changes is that enterprise WAN architecture must change too. In August 2019, Gartner defined "Secure Access Service Edge" (SASE) as the combination of advanced WAN edge network capabilities with network security functions such as SWG, CASB, FWaaS, and ZTNA delivered in the cloud. A SASE architecture brings a more secure and flexible way to connect to cloud-hosted applications by not backhauling application traffic to a data center before forwarding it to the cloud.

With a SASE architecture, the SD-WAN can steer application traffic directly to a trusted SaaS provider or first to a cloud- hosted security service where more advanced security inspections can be performed before forwarding to the SaaS provider, all according to enterprise security policies.

Traditional, private line connectivity options (such as multi-protocol label switching, or MPLS) and routing practices—backhauling, in particular—are clearly a poor match for cloud-based apps. Key shortcomings include the negative impact they have on performance (especially for internet or cloud-destined traffic), the high cost of such network services and architectures, and the fact that they require to maintain a myriad of security equipment in branch locations.

The proliferation of Internet of Things (IoT) devices has become another major concern for organizations, significantly increasing the attack surface. Based on a simple design, these devices usually cannot host a security agent, and therefore they cannot be easily protected. Organizations require a different security solution for IoT devices to protect their networks from potential vulnerabilities that could breach the network. That's why SASE must be complemented with a Zero Trust, identity-based access control security framework, segmenting traffic so that users and IoT devices can only reach network destinations consistent with their role in the business.

Why SD-WAN is critical to security

Strong security is a prerequisite and integral element of many of the benefits of a business-driven SD-WAN. For instance, the use of broadband internet as a low-cost connectivity option is core to the SD-WAN value proposition. However, the fact that broadband is "public" instead of "private" introduces the need for capabilities to ensure the confidentiality and integrity of application traffic traversing such connections. And let's not forget, too, that inline deployment of SD-WAN devices places them "in the line of fire"—at least compared to the scenario where a traditional WAN optimizer is implemented in an out-of-path configuration.

Backhauling and local internet breakout

The practice of backhauling is where branch office application traffic destined for (or returning from) the internet is routed via a WAN connection between the branch and a corporate headquarters location. This allows application traffic to benefit from the security controls and countermeasures deployed at the headquarters site before being routed to the internet. However, backhauling application traffic results in poor performance due to added latency. The alternative, referred to as local internet breakout, is where selected branch office application traffic is routed directly to/from the internet (i.e., without the need to traverse the WAN and pass through a set of centrally deployed security tools before ultimately reaching the cloud-based application).

Although local internet breakout is essential for enhancing performance and reducing the bandwidth needed for backhauling, it also exposes branch users and their local networks directly to the internet and its myriad of threats. So now you need a way to limit outbound destinations, block unwanted/unsolicited inbound traffic and filter allowed/expected traffic for threats.

However, not all web applications are created equal, and some web traffic can expose the enterprise to viruses, trojans, DDoS attacks, and other vulnerabilities. Therefore, direct internet breakout must also be secure. For example, a web traffic security policy could be defined as follows:

- Send known, trusted business SaaS traffic such as voice and video traffic Unified Communications-as-a-Service (UCaaS) directly to the internet.
- Send all other web traffic to a Security Service Edge solution (SSE).
- Send enterprise data center-hosted application traffic directly to headquarters.

To implement such a policy, web traffic must be steered granularly to its intended destination. This requires identifying the application on the first packet because once an application session has been established, it cannot be redirected to an alternate destination without breaking the flow resulting in application disruption. And because IP address ranges utilized by SaaS applications change almost continuously, address table updates must be automated and implemented on a daily basis.

Intelligent, secure traffic steering

Although it's not a security capability per se, EdgeConnect First-packet iQ™ classification plays an important role in the overall effectiveness of the HPE Aruba Networking SD-WAN platform. By identifying applications on the first packet of a session, it enables application-driven traffic steering that not only ensures efficient use of WAN resources, but also helps automate security policy enforcement.

For example, with First-packet iQ, trusted SaaS and web traffic can be sent directly to the internet (avoiding the performance impact and cost of backhauling), while other traffic can be sent to an SSE (Security Service Edge) solution or to corporate security services. Automated SaaS IP address updates described previously ensure that application traffic is directed correctly according to defined security policies.

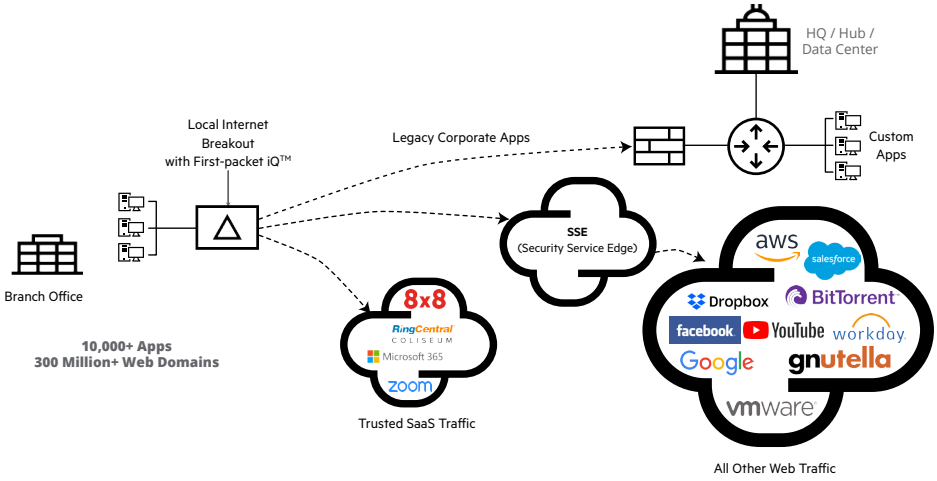


Figure 1. Application traffic is identified on the first packet to steer traffic to its correct destination to enable granular security policy enforcement.

Introducing HPE Aruba Networking EdgeConnect SD-WAN

The EdgeConnect SD-WAN platform provides enterprises with the flexibility to use any combination of transport technologies—including public broadband services—to connect users to applications without compromising application performance or security. The four main components of the platform include:

- **EdgeConnect SD-WAN** zero-touch physical or virtual appliances, which are deployed at an organization's branch offices, central sites, and cloud data centers
- **HPE Aruba Networking EdgeConnect SD-WAN Orchestrator**, a centralized management system that enables simplified configuration and orchestration of the entire WAN and provides complete observability into both legacy and cloud applications; QoS and security policies are defined centrally and automatically deployed globally to all appliances in the SD-WAN, increasing operational efficiency and minimizing human errors which can jeopardize branch security

- **WAN Optimization**, a performance pack that enables IT teams to engage market-leading WAN optimization capabilities, where needed, simply by checking a box in the Orchestrator interface
- **Advanced Security**, an optional security license that enables intrusion detection and prevention functions (IDS/IPS) in EdgeConnect SD-WAN appliances

EdgeConnect SD-WAN is designed with an extensive set of capabilities to address all of the branch WAN edge security challenges and requirements inherent in SD-WAN implementations.

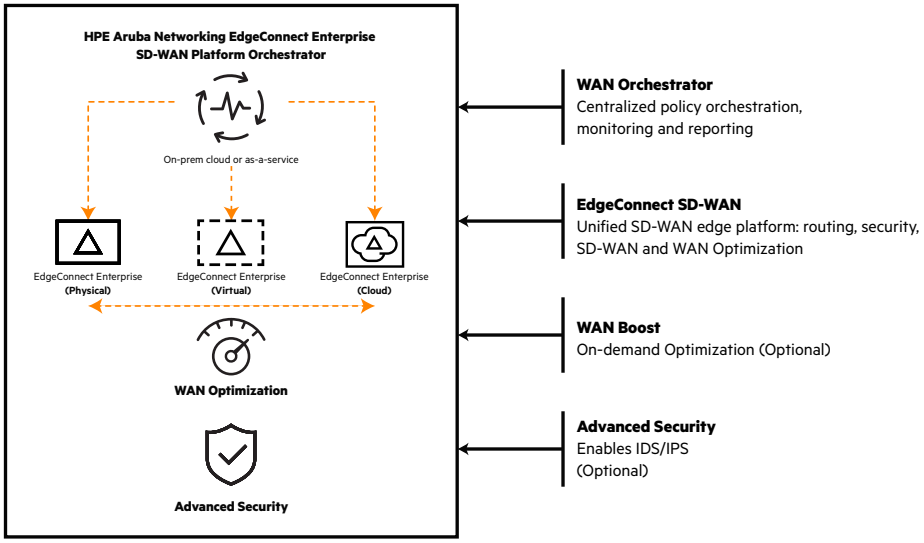


Figure 2. HPE Aruba Networking EdgeConnect SD-WAN platform

How EdgeConnect SD-WAN delivers a secure SD-WAN

HPE Aruba Networking EdgeConnect SD-WAN goes well beyond the basics of ensuring the confidentiality of application traffic traversing public networks. An extensive set of security capabilities provides coverage across four essential areas: the data plane, the management plane, integration with Security Service Edge (SSE), and compliance. The net result is the full-spectrum of protection needed for enterprises to fully realize the benefits of an advanced SD-WAN—enhanced application performance, lower overall WAN cost, and increased business agility—without being exposed to greater security risks.

Application-driven data plane security

Different applications deserve—or perhaps even require—different treatments when it comes to how they are handled from a security perspective (not to mention other "perspectives," such as QoS, performance optimization, and tunnel bonding policy). For example, a business application that is processing sensitive transactions might require encryption regardless of the type of transport being used to meet compliance requirements, while SaaS applications could be left to rely on their own native capabilities (e.g., TLS). This is why it's important to have an application-driven SD-WAN, where policies and configuration settings can be implemented on a per-application basis.

Relevant security capabilities available with HPE Aruba Networking EdgeConnect SD-WAN include:

Next-generation firewall: EdgeConnect SD-WAN includes a next-generation firewall that provides in a single entity, advanced security features such as deep packet inspection, intrusion prevention, as well as application and user identity awareness. It gives IT leaders the ability to block malware from entering the network based on application, identity, and context, regardless of the port/protocol used. Additionally, IT leaders benefit from an increased visibility into network activity and potential risks.

Intrusion Detection and Prevention (IDS/IPS): EdgeConnect SD-WAN integrates a rule-based Intrusion Detection and Prevention System (IDS/IPS). The signature-based system monitors network traffic to find patterns that match a particular attack signature. Integrated with the EdgeConnect next-generation firewall, the system allows application-level selection for inspection based on firewall zones and provides actions such as drop or allow traffic when an intrusion is detected.

The system can operate either in strict mode or performant mode. In strict 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. Using this mode, an intrusion is blocked after its detection. Depending on their security requirements, organizations can choose between the strict or performant mode.

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. The EdgeConnect Security App for Splunk provides a dashboard view of all security event notifications exported from EdgeConnect devices within an enterprise's SD-WAN. IT managers can easily configure EdgeConnect to forward all security event notifications to Splunk, centralizing logging, visualization, and analysis of security events alongside other telemetry or network events. From Splunk, users can filter, sort, navigate and view the collective security event notifications generated across the entire SD-WAN fabric, overall trends, and top talkers to help them pinpoint network events that require further investigation.

Figure 3. Splunk security dashboard

DDoS Defense: With the rising frequency of distributed denial-of-service (DDoS) attacks, it is imperative that organizations establish cost-effective defenses for any and all sites that might be affected. With EdgeConnect deployed at branch locations, that's precisely what you get. In the event of a DDoS attack, EdgeConnect limits the number of malicious requests with actions such as rapid aging, drop excess and block source.

Actions are based on preset or configurable DoS thresholds set for traffic parameters including flow rate, concurrent flows, and embryonic flows. Additionally, the solution can dynamically route the traffic over unaffected network links in case of a DDoS attack with no degradation to application performance or impact to SD-WAN manageability. EdgeConnect protects not only itself, but also protects all of the users and systems both on the local network and over the remaining, operational WAN connections.

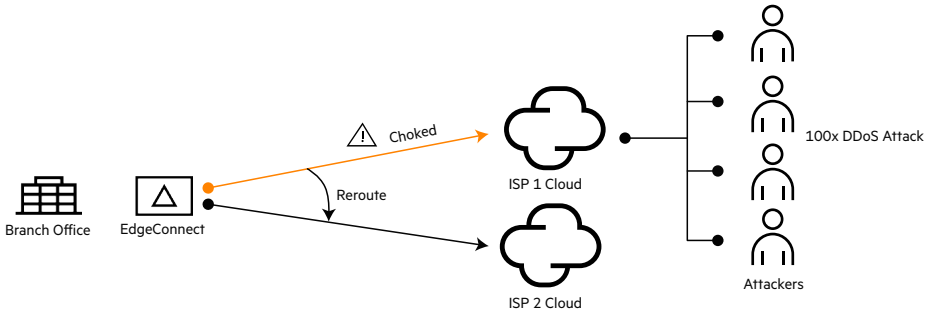


Figure 4. HPE Aruba Networking EdgeConnect SD-WAN protects the SD-WAN from DDoS attacks and routes traffic across an alternate transport service to keep applications running, enhancing business continuity.

Data in transit protection: Each HPE Aruba Networking EdgeConnect datapath is protected by IPSec tunnels that use AES 256-bit encryption to maintain application and data confidentiality. EdgeConnect uses an "IKE-less" IPSec UDP protocol; that is, it employs standards-based IPSec UDP encryption but doesn't require Internet Key Exchange pre-shared keys. Encryption keys are never repeated and are directionally unique. HPE Aruba Networking SD-WAN Orchestrator manages the encryption keys and rotations automatically, which reduces tunnel setup time without a loss of service. This protocol avoids problems encountered when deploying NAT (Network Address Translation) with IKE, such as failures when branch offices have multiple devices with different VPN requirements. Because IKE-less tunnels use different ports over IPSec, they are unlikely to be limited or blocked by upstream firewalls. These advanced features for protecting data in transit increase the flexibility, security, and robustness of secure communication between remote endpoints.

Data at rest protection: All blocks of data that persist within HPE Aruba Networking EdgeConnect appliances as a result of the optional WAN Optimization data de-duplication capability are protected with AES 128-bit encryption.

Zero Trust segmentation: EdgeConnect SD-WAN creates secure end-to-end zones across any combination of users, devices, application groups and virtual overlays, propagating configuration updates to sites in accordance with business intent. Paired with HPE Aruba Networking ClearPass Policy Manager, EdgeConnect SD-WAN enforces a Zero Trust architecture that dynamically segments the network and applies least privileged access principles. It ensures that users and IoT devices only communicate with destinations consistent with their role based on identity, access rights, and security posture.

Additionally, EdgeConnect SD-WAN allows organizations to create multiple application-specific virtual WAN overlays (also called business intent overlays). Each virtual overlay specifies priority and quality of service requirements for application groups based on business requirements. Using these specifications, EdgeConnect automates traffic steering end- to-end across all underlying WAN transport services.

Each virtual overlay is mapped to a LAN-side zone or zones. A zone may be comprised of VLANs, physical and logical interfaces, and sub-interfaces. Each zone can be assigned security policies that limit connectivity with other zones. For example, a policy could allow only outgoing traffic, or allow incoming traffic only from approved applications and services or block all traffic from less secure zones.

With Zero Trust segmentation:

- Users and IoT devices access resources based on role and context using least privilege access principles
- Traffic within each zone is isolated from traffic in other segments, reducing unauthorized access and limiting the scope of incidents
- Micro-segmentation is extended from the LAN, across the WAN, and to data centers and cloud platforms
- High-priority applications enjoy faster, more reliable performance across the WAN, increasing application availability and improving the experience and productivity of end users

Simple policy creation: IT administrators can create network segments in minutes using an intuitive graphical user interface. These segments can connect LANs with other LANs (LAN-WAN-LAN) and with data centers (LAN-WAN- data center). The virtual WAN overlays are defined based on business requirements and intent, not infrastructure details like IP addresses. Zone-based security policies are displayed in a configuration matrix that makes them easy to understand.

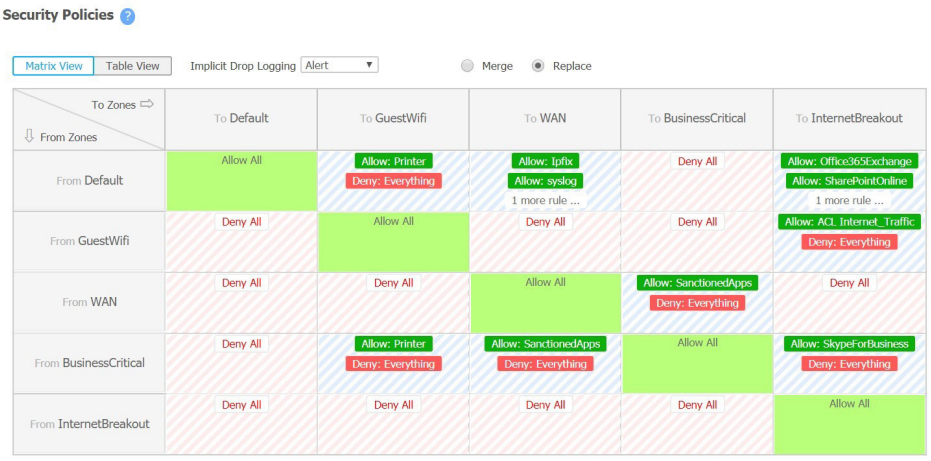
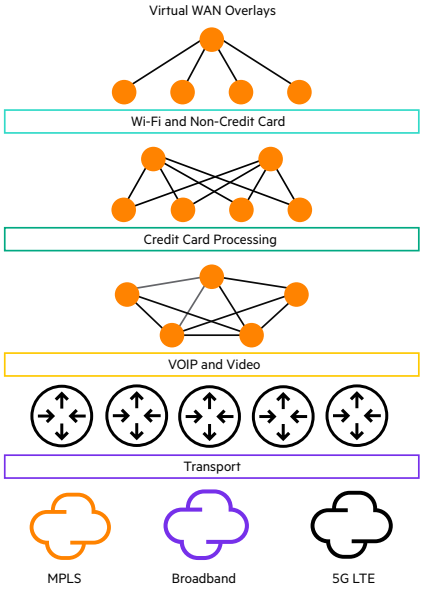


Figure 5. A security policy configuration matrix greatly simplifies the creation and management of segmentation rules.

Central orchestration and automated enforcement: Once virtual WAN overlays and zone-based firewall policies have been defined, HPE Aruba Networking SD-WAN Orchestrator deploys them to all EdgeConnect SD-WAN appliances, where they are automatically enforced. This replaces the time-consuming manual configuration of routers and firewalls every time a policy changes.

The benefits include:

- Consistent security policy enforcement across LANs and WANs
- Fewer configuration errors
- Improved compliance with regulations and industry standards
- Increased productivity for security and operations staffs



Access policy	Topology	Connection	QoS
Guest VLAN	Hub and Spoke	Internet	Min. Cost
Data VLAN	Dual Hub and Spoke	MPLS—Internet	Max. Availability
Voice VLAN	Full Mesh	MPLS—Internet—LTE	Max. Quality

Figure 6. HPE Aruba Networking EdgeConnect SD-WAN extends micro-segmentation across the WAN to help enterprises meet compliance standards.

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 HPE Aruba Networking EdgeConnect SD-WAN into a single solution to meet the increasing demand for integrated networking and security solutions. HPE Aruba Networking SSE is also tightly integrated with HPE Aruba Networking EdgeConnect SD-Branch and HPE Aruba Networking EdgeConnect Microbranch.

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.

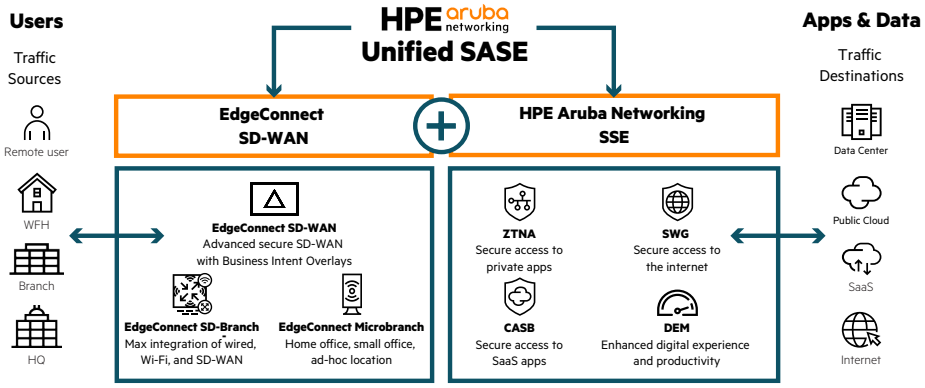


Figure 7. Deploy industry-leading HPE Aruba Networking EdgeConnect SD-WAN with the cloud-native HPE Aruba Networking SSE platform to build a unified SASE solution

SSE is a unified platform where ZTNA, SWG and 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 exfiltration with CASB. Additionally, the solution harmonizes access across the world via a cloud-backbone of Amazon Web Services (AWS), Microsoft Azure, Google™, and Oracle®.

HPE Aruba Networking SSE capabilities include:

- **ZTNA (Zero Trust Network Access)** is based on the principle to "never trust, always verify", so that a device connecting to the network is not trusted by default. Unlike a VPN that gives connected users broad access to the corporate network, ZTNA limits user access to only specific applications or microsegments that have been approved for the user, enforcing least-privilege access. With ZTNA, remote workers can connect from anywhere.

  Third-party users can also be easily onboarded in the network with agentless ZTNA. There's no need to install a ZTNA agent in laptops, third party users simply log in to a ZTNA web portal with their own credentials.

- **SWG (Secure Web Gateway)** sits between a user and a website to secure and protect against malicious threats.

  It performs several security inspections including URL filtering, malicious code detection and web access control, and provides policies that can limit access to adult sites, gambling, or dangerous sites for example.

- **CASB (Cloud Access Security Broker)** ensures sensitive data hosted in the cloud remains protected. It identifies and detects sensitive data in cloud applications and enforces security policies such as authentication and Single Sign On (SSO). It monitors user activities in cloud services, identifies potential security risks and policy violations to prevent data loss and control block uploads and downloads of SaaS applications such as Box, SharePoint, Facebook, and Salesforce. It prevents users from signing up for and using cloud applications that are not authorized by an organization's IT and security policies, allowing organizations to reduce shadow IT.
- **DEM (Digital Experience Monitoring)** ensures user productivity by measuring hop-by-hop metrics, and monitoring app, device, and network performance. IT can easily pinpoint connectivity issues and reduce mean time to resolution.

Integration with multiple SASE partners

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.

HPE Aruba Networking maintains technology partnerships with leading SSE (Security Service Edge) vendors covering solution areas such as Secure Web Gateways (SWG), Cloud Access Security Broker (CASB), Zero Trust Network Access (ZTNA) and remote browser isolation (RBI) from security companies like Zscaler, Netskope, Check Point, McAfee®, Palo Alto Networks and Symantec.

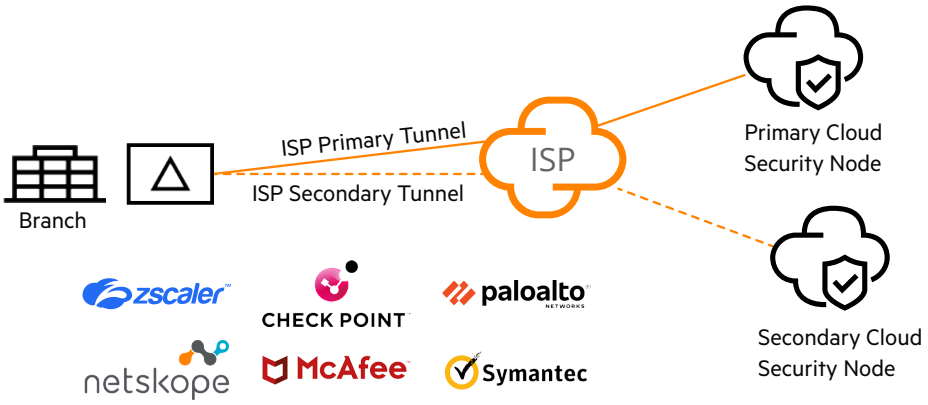


Figure 8. Automate service orchestration with multiple cloud-security vendors

Automated integration and orchestration: HPE Aruba Networking EdgeConnect automates the orchestration with third-party cloud security (SSE) vendors, and the configuration of IPSec tunnels between EdgeConnect and SSE vendors. With this capability, First-packet iQ™ application classification feature first identifies applications and web domains based on the first packet. The traffic is then intelligently steered to SSE services based on security policies defined by the organization. Administrators can also take advantage of a simple drag-and-drop interface that makes it easy to assign policies to traffic from specific applications and to route the traffic to specific security tools. For example, internet-bound traffic is automatically routed through cloud-based security services for Layer 7 access control, threat filtering, and analytics.

Management plane and system-level security

Despite being less top-of-mind than its data plane counterpart, system and management plane security is no less important. Relevant HPE Aruba Networking EdgeConnect capabilities in this area include:

Secure, Zero-Touch Provisioning: A key part of the HPE Aruba Networking EdgeConnect SD-WAN value proposition is a plug-and-play deployment model that enables rapid installation, without the need for a distributed IT presence. Security for this process takes the form of a two-step authentication and authorization procedure. Before receiving its settings and policies and becoming an active part of the SD-WAN, each newly connected EdgeConnect appliance first must be authenticated by the cloud portal from HPE Aruba Networking and then "approved" by an IT administrator using HPE Aruba Networking SD-WAN Orchestrator.

In addition, SD-WAN Orchestrator can also be used to subsequently revoke access for a given appliance (e.g., if it is stolen or otherwise compromised). This results in any in-flight traffic being dropped, and the specified appliance being unable to download configuration information or join the SD-WAN.

Encrypted Management Communications: All communication sessions between EdgeConnect appliances, SD-WAN Orchestrator, the HPE Aruba Networking cloud portal, and administrators' web browsers are protected with TLS 1.2. Furthermore, all weak protocols (e.g., SSLv2, SSLv3, TLS 1.0, TLS 1.1), weak hashes (e.g., MD5), and weak encryption algorithms (e.g., DES, RC4) are disabled by default.

System Hardening: EdgeConnect is a hardened appliance that ships with the factory default "harden" mode. This approach ensures out-of-the-box security for appliances plugged in for the first time.

Other management plane protections include:

Robust user authentication and authorization

- Support for local, RADIUS, TACACS+, and Oauth for authentication and authorization with identity management systems such as Active Directory and Okta.
- Granular role-based access control with read-only users and multiple administrator roles
- Whitelisting for Orchestrator that restricts administrative access to a specific set of IP addresses or subnets

Extensive logging for both SD-WAN Orchestrator and EdgeConnect

- Event logs/alarms—for system errors pertaining to memory, CPU, network interfaces, routing, and management plane connectivity
- Threshold crossing alerts—configurable, rising and falling thresholds to signal imminent/approaching conditions for concern, such as high-memory or bandwidth utilization
- Audit logs—for tracking all access to an activity conducted via any of the available management interfaces (CLI, WebUI, or REST APIs)
- Firewall logs—traffic flows inspected by the EdgeConnect next-generation firewall generate deny, accept, and drop events, as well as reasons for those events. Firewall logs can then be streamed to a third-party SIEM tool (e.g., Splunk).
- Netflow/traffic logs—for capturing full (non-sampled) flow data so that it can be streamed to a third-party tool (e.g., Netflow-collector)

In addition to being critical for network management and incident response, log data can be valuable for complying with standards such as HIPAA.

Security certification and compliance

As users connect from anywhere using connections that are inherently insecure such as broadband internet and 5G, and access sensitive data online, the need to certify an SD-WAN for security has become more pressing. HPE Aruba Networking EdgeConnect SD-WAN has earned the ICSA Labs Secure SD-WAN certification based on a comprehensive and robust set of SD-WAN functionality 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 ant-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**

With the assurance of using a secure SD-WAN, certified by a globally recognized independent, third-party organization, enterprises can simplify network architecture in branch locations by replacing branch firewalls with EdgeConnect SD-WAN.

Most of the security features covered so far are applicable to multiple requirements spanning multiple regulations. Authentication, authorization, and auditing capabilities, for instance, are a fundamental requirement of NIST Special Publication 800-53 (Security and Privacy Controls for Information Systems and Organizations)—and, therefore, of practically every regulation that invokes it.

Notable too, especially for its uniqueness among SD-WAN solutions, is EdgeConnect SD-WAN support for micro-segmentation. The ability to create encrypted, application-specific overlays can help IT teams control access to systems that store and process electronic private health information (ePHI) to support HIPAA compliance, segment off credit transactions and associated systems to substantially reduce the scope of their PCI DSS compliance efforts and reduce the risk of unauthorized access to information about customers to meet GDPR and other privacy rules.

Last, but not least, there are many ways EdgeConnect SD-WAN paired with HPE Aruba Networking SSE helps ease the burden of complying with relevant industry regulations, including: Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI DSS), Sarbanes-Oxley Act (SOX), the European Union GDPR, and others.

For example, to ensure compliance with regulations on data protection, CASB and DLP help enforce data protection. They monitor data at risk and prevent users from uploading sensitive data into cloud applications intentionally or unintentionally. CASB also helps reduce shadow IT and identify unsanctioned cloud applications in organizations, detect sensitive data in transit and enforce security policies such as authentication and Single Sign On (SSO).

ZTNA protects data from cyberthreats by masking private resources from the internet, keeping users off the network. SWG protects against malicious web traffic such as phishing or ransomware, reducing cybersecurity risks and improving compliance.

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

Conclusion

Fully realizing the many compelling benefits of a secure SD-WAN depends to no small extent on having a solution that accounts for the security issues, challenges, and opportunities that such an approach presents. In this regard, the extensive security capabilities of the HPE Aruba Networking EdgeConnect SD-WAN platform go well beyond the minimum-required level of protection afforded by transport-level encryption and message authentication.

With its built-in next-generation firewall, that provides advanced security features such as IDS/IPS and DDoS protection, HPE Aruba Networking EdgeConnect SD-WAN allows organizations to replace legacy firewalls, as well as routers, in branch offices, reducing hardware footprint, cost and complexity.

By combining EdgeConnect SD-WAN, featuring robust data and management plane security, with award-winning HPE Aruba Networking SSE, organizations can architect a unified SASE solution and accelerate their journey to SASE through seamless deployment and simplified management. For organizations preferring to adopt SASE with their choice of security services, EdgeConnect SD-WAN supports automated integration and orchestration with third-party cloud-delivered security solutions.

Finally, with the increasing use of IoT devices, EdgeConnect complements SASE with a zero-trust architecture to segment the network based on identity so that users and IoT devices can only reach network destinations consistent with their role in the business.

Make the right purchase decision.
Contact our presales specialists.

Contact us

Visit **ArubaNetworks.com**

BP_ArchitectingSASE_Cobranded_DT_080924 a00142252ENW

Hewlett Packard Enterprise