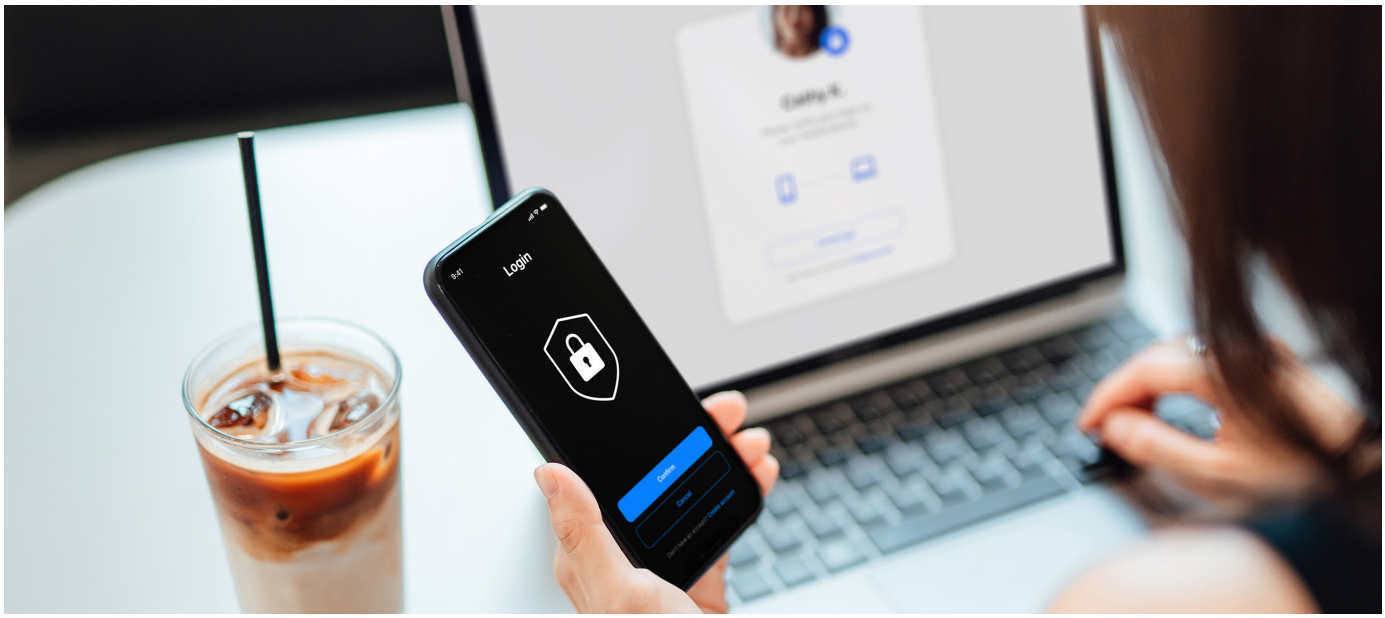
HPE aruba networking

Solution overview

Enable advanced security with HPE Aruba Networking EdgeConnect SD-Branch

Protecting the branch from today's evolving threats with an advanced secure SD-WAN

HPE



Key benefits

Advanced security capabilities in EdgeConnect SD-Branch provide key benefits including:

- Unified SASE through a tight integration with HPE Aruba Networking SSE
- Automated orchestration to third-party cloud security vendors
- Integrated security across wired and wireless networks
- End-to-end dynamic segmentation across distributed enterprises
- Granular firewall policies based on users and application roles
- Detection and blocking of intrusions with a daily updated threat library
- Increased visibility and real-time monitoring of external threats across all sites

Introduction

With applications moving to the cloud and hybrid working, remote users are accessing enterprise resources from anywhere through untrusted links. At the same time, cybersecurity risks have increased dramatically due to the explosion of devices connected to the network and sensitive data hosted in the cloud.

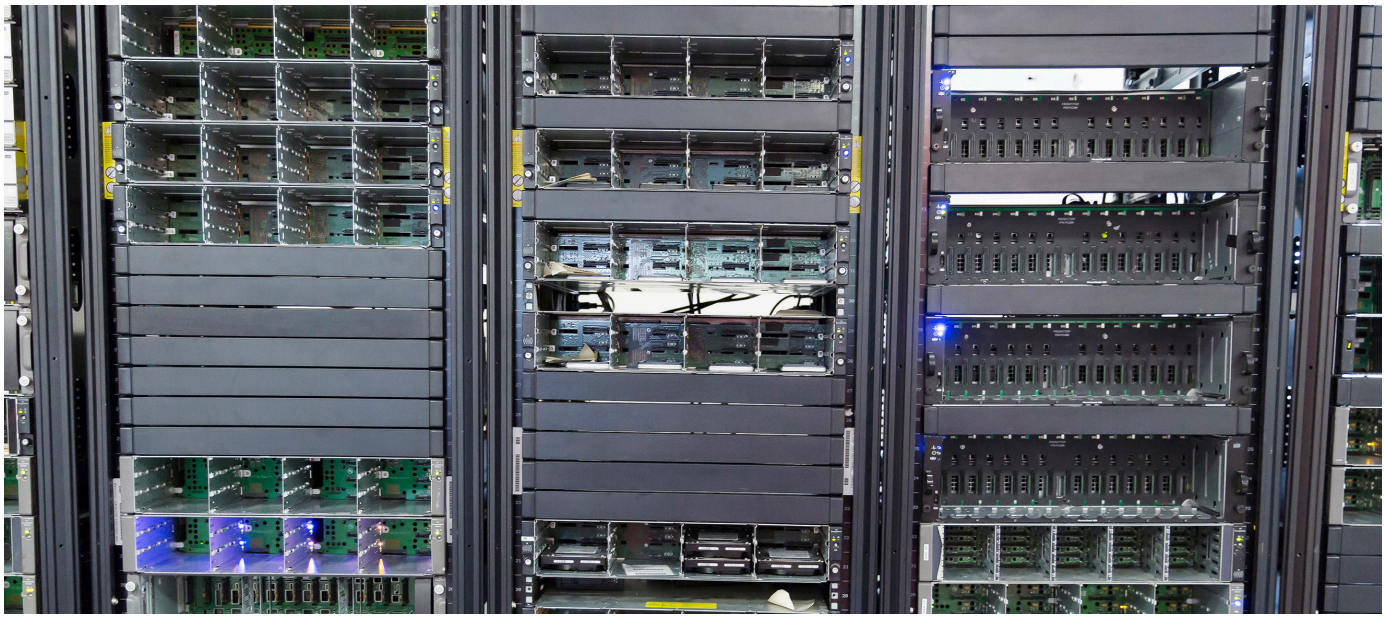
As the security perimeter is dissolving, Gartner defined in 2019 the concept of secure access service edge (SASE) that combines SD-WAN and cloud-delivered security services, security service edge (SSE), bringing a more secure and flexible way to connect by not backhauling application traffic to a data center and performing advanced security inspection in the cloud. Gartner indeed predicted[1] that "by 2025, more than 50% of organizations will have explicit strategies to adopt SASE, up from less than 5% in 2020."

Additionally, with the proliferation of IoT devices in enterprises, SASE must be augmented with a zero trust, identity-based access control framework to enforce security and protect local branches from breaches as IoT devices cannot run security agents and the attack surface is growing.

EdgeConnect SD-Branch provides fully integrated SD-WAN security by establishing and enforcing policies in branches with a stateful, application-aware firewall, including deep packet inspection (DPI) combined with application classification and web content filtering. A traffic inspection engine provides extensive intrusion detection and prevention functionality (IDS/IPS), blocking malicious attacks and ensuring continued operations.

The solution tightly integrates with HPE Aruba Networking SSE to form a unified SASE platform, for a simpler adoption and a faster deployment of SASE. The solution can also seamlessly integrate with third-party security vendors for specific needs or to integrate with an existing security ecosystem. HPE Aruba Networking then takes this a step further by providing role-based dynamic segmentation across the LAN and WAN so that users and IoT devices can only reach network destinations consistent with their role in the business, preventing outside threats to spread the network, which is a key objective of securing distributed enterprises.

[1] Gartner Says Cloud Will Be the Centerpiece of New Digital Experiences, November 2021



Security without compromise with EdgeConnect SD-Branch

While keeping the performance and cost benefits of SD-WAN, HPE Aruba Networking's security functions are handled at the edge rather than backhauled to the data center or campus. Security can be divided into assurances for the integrity of either the LAN or the WAN. The LAN requires assurances for East-West traffic and the WAN needs security for traffic across sites, also known as North-South traffic.

The state of the art in SD-WAN gateways should include routing, SD-WAN overlay creation, security, deep packet inspection, and other functions that had historically been handled in separate appliances.

The following table explains the tools for securing these networks.

This table highlights the many different security components of EdgeConnect SD-Branch. HPE Aruba Networking gateways support an application aware stateful firewall,[2] deep packet inspection (DPI), web content filtering, VPN overlays, IDS/IPS, dynamic segmentation, security dashboards, and unified SASE through integration with HPE Aruba Networking SSE (Security service edge).

Table 1. Functionality to secure LAN and LAN traffic

Security feature	Details
Stateful, Application-Aware with deep packet inspection	User and application awareness with full policy enforcement thanks to deep packet inspection (DPI)
Intrusion detection and prevention (IDS/IPS)	Integrated intrusion prevention with advanced security dashboards
Integration with SIEM tools	Threat events streamed to Security Information and Event Management (SIEM) systems such as Splunk
Web content filtering	Provides the ability to create policies based on categories of sites
IP reputation	Automatically restricts traffic from known malicious sources
Unified SASE	Tightly integrates with HPE Aruba Networking SSE to build a unified SASE platform
Dynamic segmentation	Provides role-based segmentation across the LAN and WAN for distributed enterprises
Management plane security and system hardening	Provides advanced features to secure the platform including secure boot, zero-touch provisioning and AES256 encryption

[2] For more information, see the Unified Policy for the Distributed Enterprise technical document and the Policy Enforcement Firewall Technical Brief

Stateful, application aware firewall with deep packet inspection

EdgeConnect SD-Branch includes a stateful, application-aware firewall, with deep packet inspection (DPI) capabilities. It provides organizations with an enhanced platform to deal with new and emerging threats, enabling more granular policy control.

EdgeConnect SD-Branch's DPI recognizes over 3,700 protocols and applications to offer visibility and control. The solution performs DPI of application traffic and reports it in a dashboard that monitors the bandwidth and quality of experience of applications traversing the network.

DPI also allows network administrators to create firewall policies based on application type and application category. For example, administrators can create policies to restrict user access to an application or application category. They can also define traffic-shaping policies such as bandwidth control and QoS per application for client roles, and block bandwidth-monopolizing applications on a guest role within an enterprise.

Intrusion detection and prevention (IDS/IPS)

Intrusion prevention detects malicious activities and performs actions when an intrusion is detected. EdgeConnect SD-Branch's detection engine inspects all traffic going through the network, using both signature-based and pattern-based inspection, leveraging a library of known threats.

If an intrusion matches a signature pattern, the system takes action. The solution sends alerts and notifications to the network administrator. If IPS is activated, the traffic is blocked to protect the organization against a malicious activity. Additionally, the solution enables network administrators to define a list of allowed threats even if their signature matches a known pattern.

Intrusion detection provides threat intelligence on malicious activities including command and control, ransomware, phishing, malware, spyware, trojans, and exploit kits. Updated daily, it ensures that organizations stay on top of the dynamic threat landscape that constantly evolves. The solution includes over thousands of rules broken down into 50 categories. Furthermore, the rule set is always growing: submissions are received from all over the world covering previously unseen threats. The signature pack ensures optimum performance and accurate detection. The most relevant signatures are automatically deployed to all gateways managed by HPE Aruba Networking Central. Intrusion prevention functionality is accessed and managed under Security Management in HPE Aruba Networking Central (Figure 1).

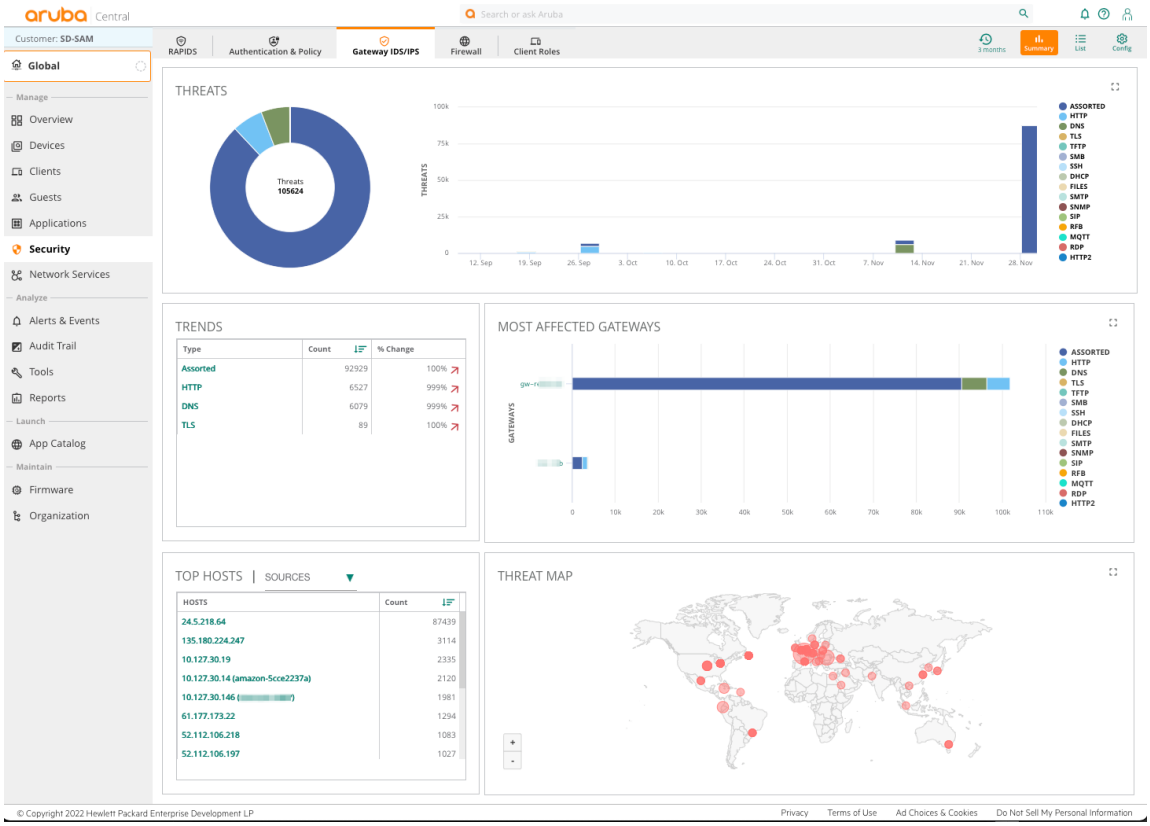


Figure 1. Intrusion prevention security dashboard under HPE Aruba Networking Central

Perceived threats, including alerts, are collated and presented in the top tile. The threats are categorized according to how they enter the branch (for instance, through an HTTP or DNS request). From this dashboard, you can see threats over time, mapping user and application traffic to threats. You can also see trends for different types of threats.

The metrics used are by threat category, the type and severity of the threats, along with threat prevalence. You can also drill down to impacted users and devices and the source and level of the impact. Figure 2 shows all the threats affecting one particular device.

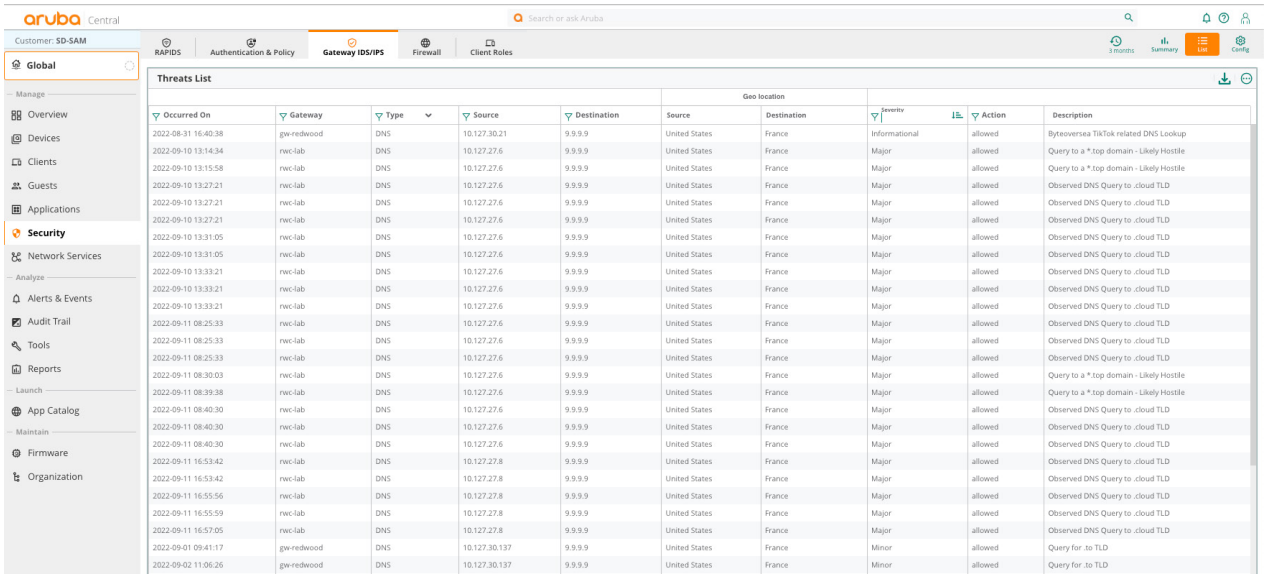


Figure 2. Threat list for single device obtained by drilling down from dashboard

In addition to the date, this table shows the gateway through which the threat entered the branch, along with the type of threat, its source, and a description. For any particular threat, you can drill down further to look at the details (Figure 3).

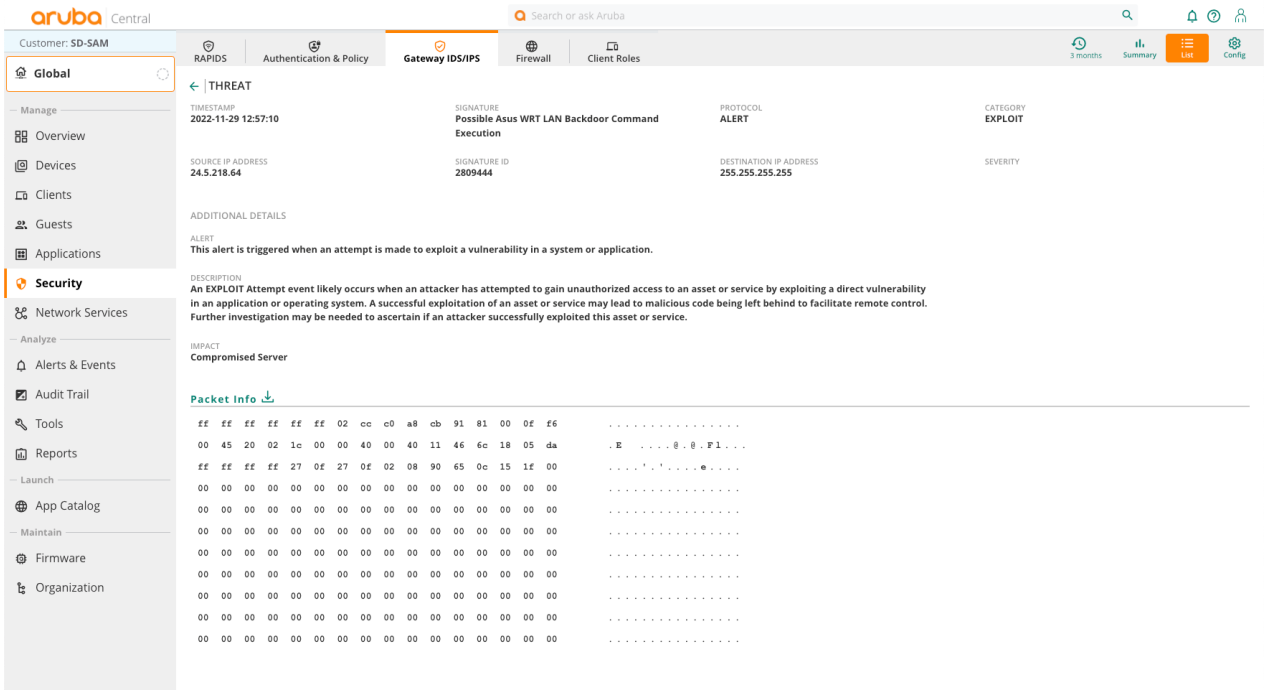


Figure 3. Threat details

This view tells you the type of threat (Category) and provides the threat signature. HPE Aruba Networking's threat intelligence includes an extensive signature pack and rule set with tens of thousands of rules and dozens of categories.

You can edit the policies based on the information you see on the Threat Details page (Figure 4).

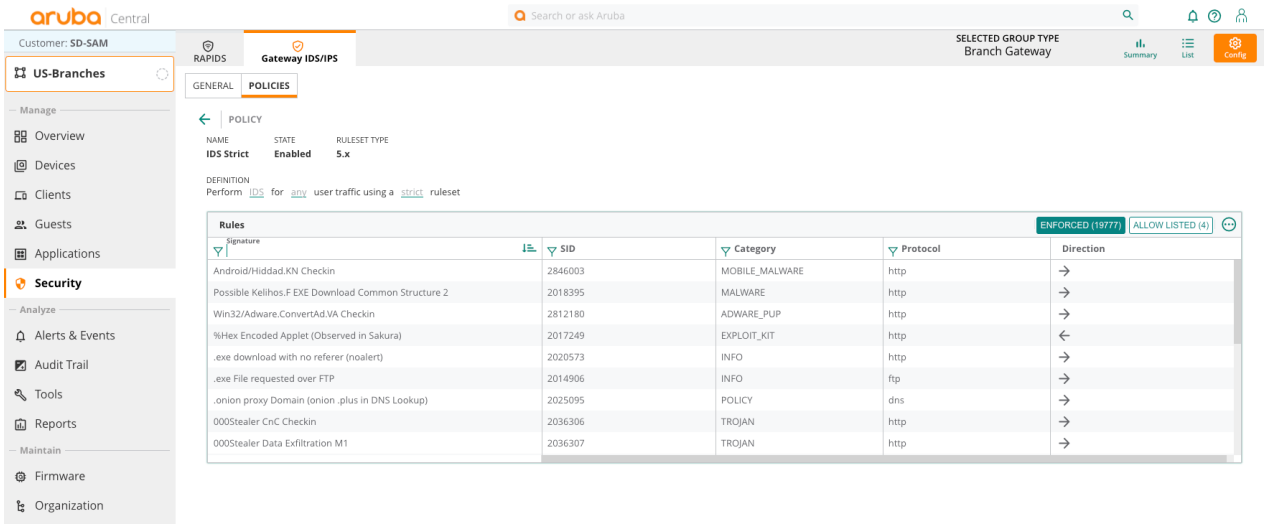


Figure 4. Edit policy rules for a set of threats

There are built-in policies that define rules to drop or allow packets that match a specified threat signature. These are shown in Figure 5.

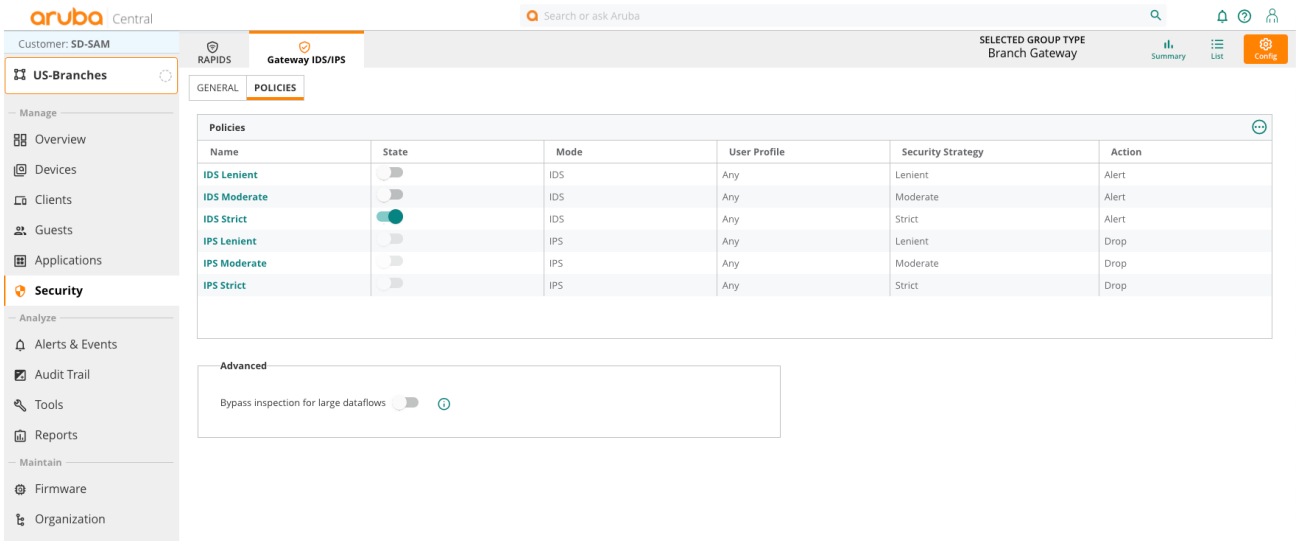


Figure 5. Built-in policies for threat management

For both IDS and IPS, the security strategies may be lenient, moderate, or strict. These settings will allow, issue alerts, or drop traffic.

Integration with SIEM tools

EdgeConnect SD-Branch captures events related to traffic sessions in syslog message format. Threat events are managed with Central Alert Framework for notification and integration with third-party logging tools and security analytics tools based on configured thresholds.

Events, such as intrusions, can be streamed to Security Information and Events Management (SIEM) systems such as Splunk to provide advanced visibility and monitoring. It allows IT departments to pinpoint events that require further investigation to manage and resolve incidents quickly.

Figure 6. Splunk security dashboard

Web content classification, IP reputation and geolocation filtering

Content filtering blocks specific websites that can be potentially harmful to organizations, objectionable and even criminal. Web content filtering helps organizations identify websites that propagate malware, spam, spyware and phishing attacks, as well as websites with sensitive content such as adult or gambling content.

HPE Aruba Networking EdgeConnect SD-Branch provides web content classification (or URL filtering) and classifies more than 80 site categories including high-risk categories, by leveraging machine learning to increase speed and accuracy.

It also provides IP reputation and Geolocation filtering that helps assess in real time the risk stemming from inbound traffic.

The IP Reputation service provides a real time feed of known malicious IP addresses broken down into 10 categories so IT security administrators can easily identify threats by type. These categories include Windows Exploits, Web Attacks, Phishing, Botnets, Denial of Service, Scanners, Proxies, Reputation, Spam Sources, and Mobile Threats.

The service uses site history, age, rank, location, networks, links, real time performance, as well as other contextual and behavioral trends to determine an IP Reputation Index and makes a classification into five reputation tiers including Trustworthy, Low Risk, Moderate Risk, Suspicious, and High Risk. In total, the solution classifies 842+ million domains and 37+ billion URLs.

The Geolocation filtering service associates source/destination IP addresses with location. It allows organizations to apply policies to permit or drop inbound or outbound communications with certain known malicious countries.

With web content filtering, organizations can protect their employees against malicious web content, improve productivity, set and enforce usage policies, and secure organizations against legal liabilities.

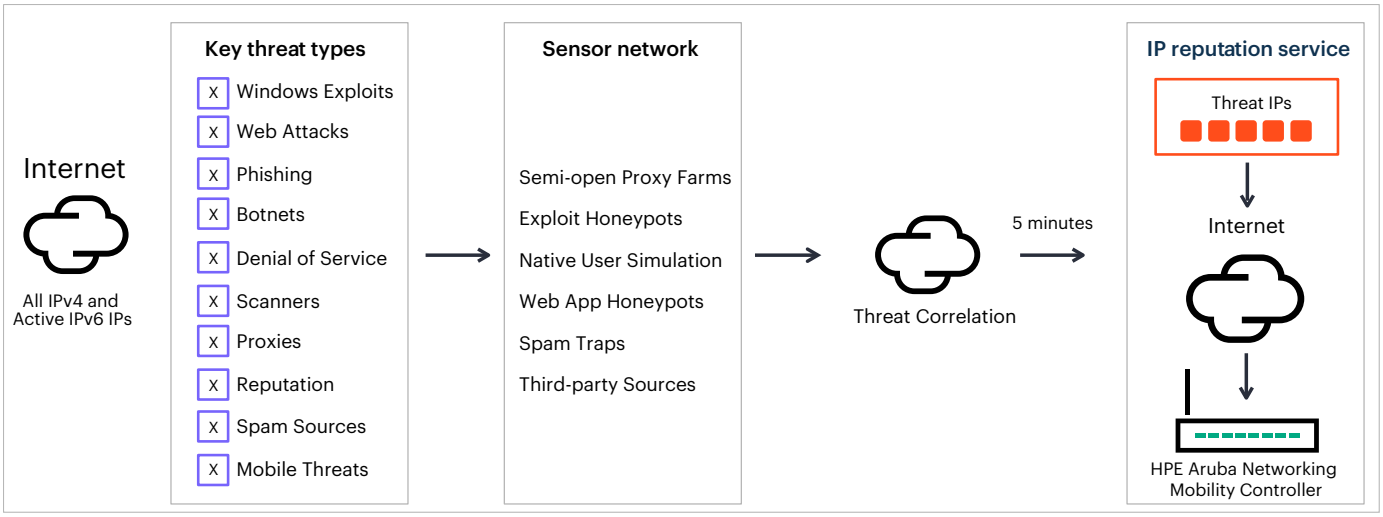


Figure 7. The IP reputation service tracks and filters in real time external threats

Unified SASE

Gartner defined secure access service edge (SASE) in 2019 to tackle the network and security challenges posed by users connecting from anywhere while accessing sensitive data in applications hosted in the cloud using untrusted links. Previously, employees connected to a local enterprise network and accessed applications hosted in a data center, so that it was easier to protect the network.

To enforce security in a now borderless enterprise and a hybrid workforce, SASE combines SD-WAN features with based HPE Aruba Networking SSE capabilities including zero trust network access (ZTNA), cloud access security broker (CASB), secure web gateway (SWG), and digital experience monitoring (DEM).

HPE Aruba Networking SSE offers a comprehensive solution where ZTNA, SWG, CASB and DEM work together seamlessly using a shared codebase. All policies can be managed from a single user interface, simplifying access control for IT administrators. It enables users 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®.

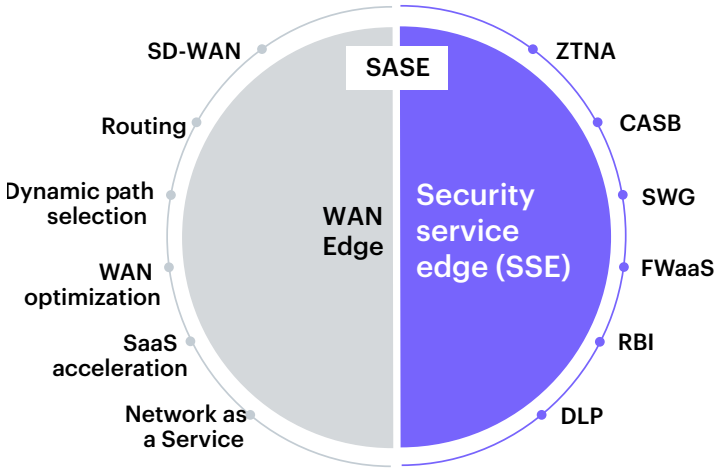


Figure 8. SASE architecture

Key capabilities of HPE Aruba Networking SSE include:

ZTNA (Zero trust network access): The solution follows the principle of "never trust, always verify." Unlike VPNs that grant broad access to the corporate network, ZTNA restricts user access to specific applications or microsegments that have been authorized for each user. This approach enforces the principle of least-privilege access. It allows remote workers to connect securely from anywhere, as well as third-party users with agentless ZTNA, so that they simply log in to a web portal using their own credentials, without installing a ZTNA agent.

SWG (Secure web gateway): SWG acts as an intermediary between users and websites, providing protection against malicious threats such as ransomware and phishing. It performs various security inspections, including URL filtering, content filtering, and web access control. Additionally, SWG provides policies to restrict access to specific categories of websites such as adult content, gambling, or dangerous sites.

CASB (Cloud access security broker): CASB ensures the security of sensitive data hosted in the cloud. It identifies and detects sensitive data within cloud applications and enforces security policies such as authentication and Single Sign-On (SSO). It monitors user activities within cloud services, identifies potential security risks and policy violations, and prevents data loss. CASB also controls the uploading and downloading of data in SaaS applications like Box, SharePoint, Facebook, and Salesforce. Moreover, CASB prevents users from using unauthorized cloud applications, reducing the risk of shadow IT.

DEM (Digital experience monitoring): DEM focuses on maintaining user productivity by measuring hop-by-hop metrics and monitoring the performance of applications, devices, and networks. With DEM, IT administrators can easily identify connectivity issues and reduce the mean time to resolution, ensuring a smooth digital experience for users.

EdgeConnect SD-Branch also integrates with multiple cloud-security vendors such as ZScaler. To do so, EdgeConnect SD-Branch builds secure tunnels between SD-Branch and SSE solutions and automates the orchestration to SSE services.

In addition, EdgeConnect SD-Branch can selectively redirect network traffic based on identity and application, by leveraging deep packet inspection (DPI) with first packet application classification. Trusted applications such as Microsoft 365 and Salesforce are directly routed to the internet while traffic from other cloud applications is sent to HPE Aruba Networking SSE or other cloud-delivered security solution for further security inspection. In some cases, the traffic can be routed to the data center, for example for legacy applications hosted in the data center, or for security reasons.

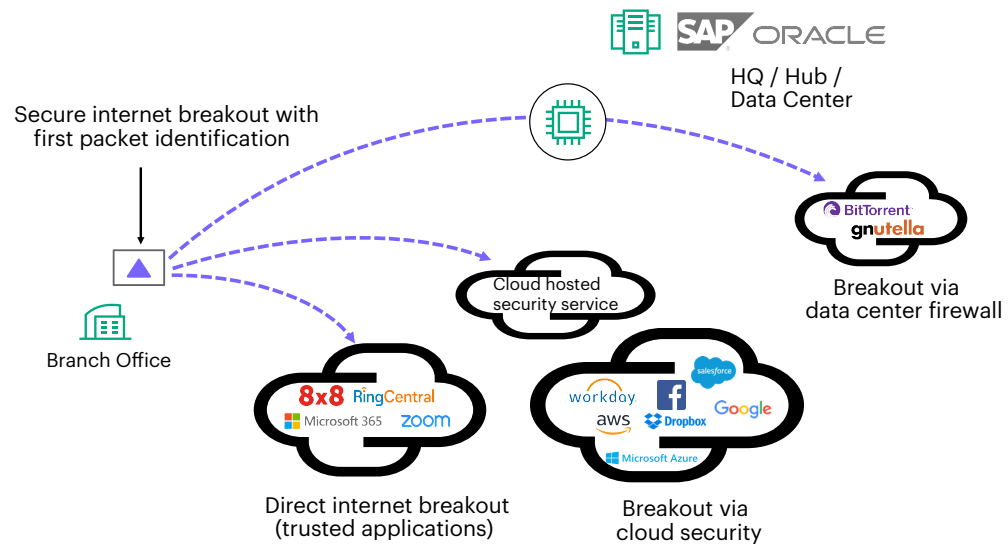


Figure 9. Build a unified SASE platform with HPE Aruba Networking and seamlessly break out traffic based on security policies

Dynamic segmentation

SASE is essential to protect remote users as the security perimeter is dissolving. However, with the proliferation of devices connected to the network, like IoT devices, it has become critical to reduce the attack surface by segmenting the network into multiple zones to limit the spread of potential attacks.

Therefore, 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.

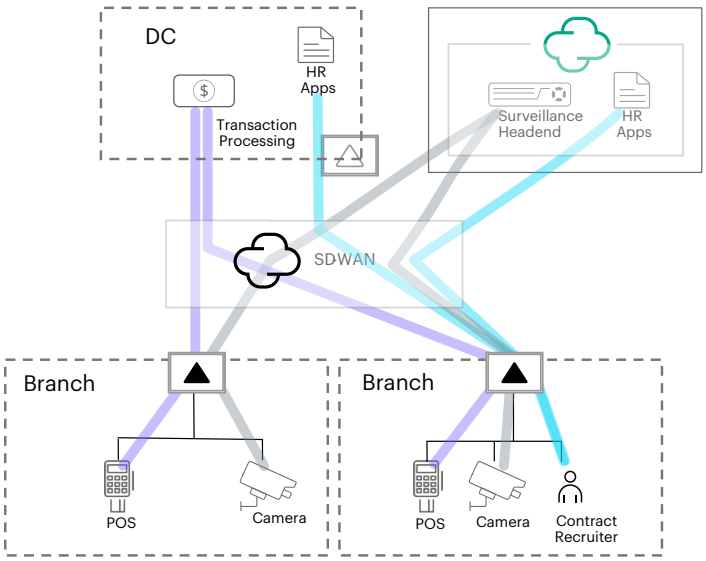
Not only does segmentation enable organizations to increase security and control, but also application performance. Indeed, network administrators can define specific zones for mission-critical applications and other zones for less critical applications such as HVAC systems, avoiding congestion and prioritizing traffic.

Traditionally, organizations defined VLANs to segment the network. VLAN configuration remains a complex and error-prone process, because network administrators needed to manually configure many individual network elements, as well as Access Control Lists (ACLs) that use hardwired IP address ranges tied to specific VLANs. With mobility, IoT explosion and increasingly distributed enterprises, this approach has become very complex, resulting in VLAN sprawl and unmanageable network. Even the simplest configuration change or client onboarding can require long deployment cycles and extensive reconfigurations, severely impacting IT productivity.

EdgeConnect SD-Branch uses role-based dynamic segmentation to enable organizations to segment the network across the LAN and WAN in a simple and scalable manner, while tackling the challenges of mobility and IoT. Paired with HPE Aruba Networking ClearPass Policy Manager, EdgeConnect SD-Branch enforces a zero trust architecture and applies least privilege access principles. It ensures that users and devices only communicate with destinations consistent with their role based on identity, access rights, and security posture.

The integration of HPE Aruba Networking ClearPass Policy Manager with HPE Aruba Networking EdgeConnect SD-Branch adds identity knowledge of users, devices and roles supporting authentication protocols such as RADIUS, TACACS+, and OAuth2 and multiple identity stores like Microsoft Active Directory. Policies are then created based on these roles and are configured and enforced at the gateways by HPE Aruba Networking Central. These policies allow authorization to access applications or destinations, and also to access each other (such as inter-user communication or access to devices).

To close visibility gaps often associated with mobile and IoT devices, HPE Aruba Networking Central offers ML-based classification of all clients with HPE Aruba Networking Client Insights. This feature uses dynamic comparisons against crowdsourced fingerprints of known clients and MAC range classification in the likely event that unknown devices are connected to the network.



	Camera	Surveillance Headend	POS Terminal	Transaction Processing	Contract Recruiter	HR Apps
Camera	✗	✓	✗	✗	✗	✗
Surveillance Headend	✓	✓	✗	✗	✗	✗
POS Terminal	✗	✗	✗	✓	✗	✗
Transaction Processing	✗	✗	✓	✓	✗	✗
Contract Recruiter	✗	✗	✗	✗	✗	✓
HR Apps	✗	✗	✗	✗	✓	✓

Figure 10. Dynamic segmentation extended to the WAN

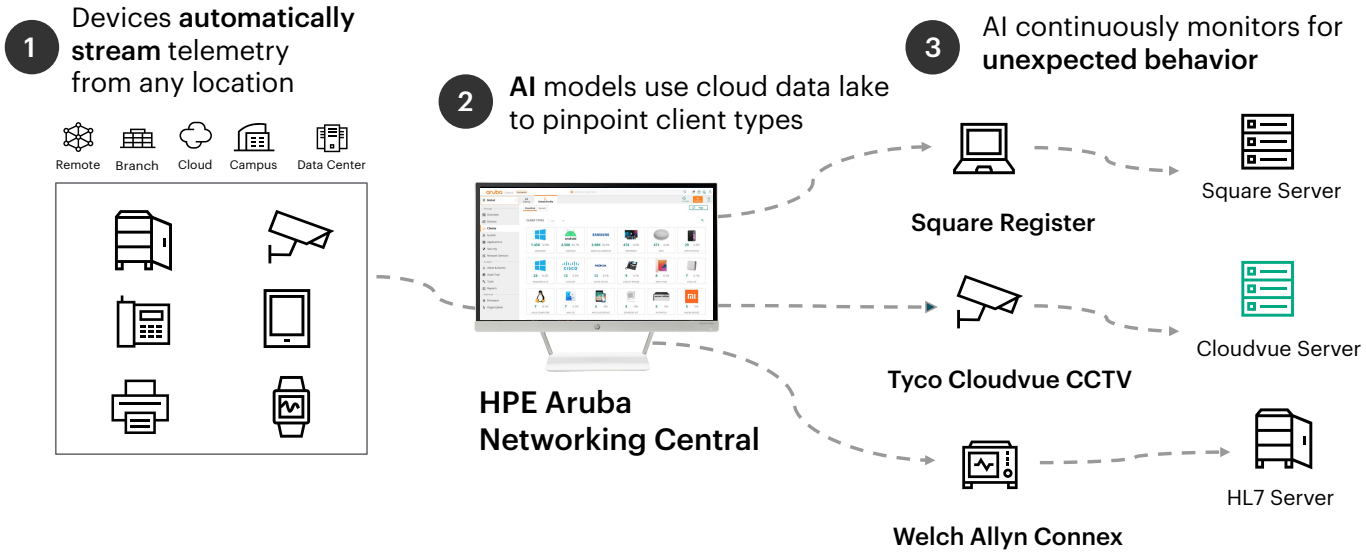


Figure 11. HPE Aruba Networking Client Insights uses network and client telemetry with machine learning to accurately fingerprint and classify all wired and Wi-Fi connected

To seamlessly enforce global policy security across complex, globally distributed networks, HPE Aruba Networking Central includes NetConductor that uses EVPN, VXLAN and BGP protocols to facilitate inline policy enforcement. It automatically builds and orchestrates intelligent overlays, tied to a full policy-based micro-segmentation model, based on global roles, across the entire network infrastructure of the organization. The HPE Aruba Networking gateways deployed in branches encapsulates the client traffic information with VXLAN-BGP and IPSec, which contains role information in the VXLAN header. The Gateway in the destination site will then enforce the role-based policies for client traffic.

In other words, the role attributed to any connected device on the network is defined globally with HPE Aruba Networking Central. Central then carries role information to HPE Aruba Networking gateways, via tunnel orchestrator, and instructs gateways to allow or deny traffic between devices globally, across the WAN.

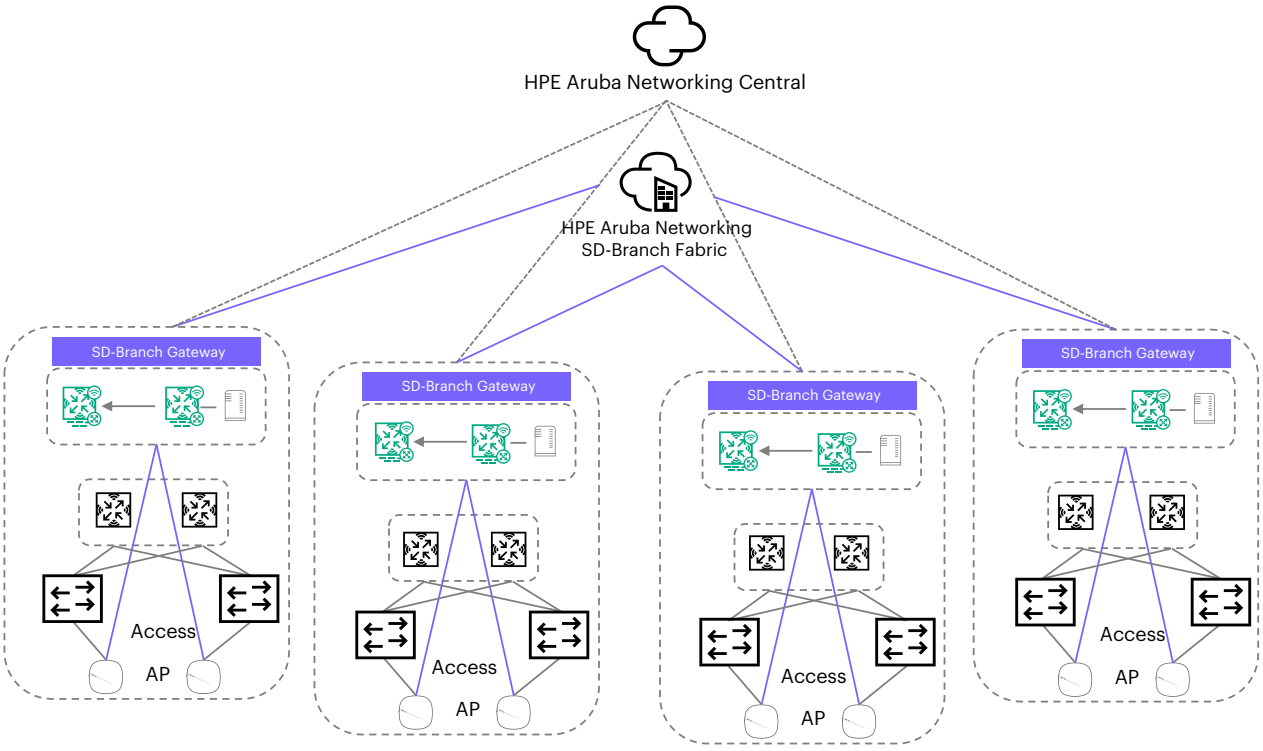


Figure 12. Enable dynamic segmentation in complex, distributed network architectures by deploying EdgeConnect SD-Branch with NetConductor

NetConductor also includes CloudAuth that enables frictionless onboarding of end users and client devices either through integrations with cloud identity stores such as Azure Active Directory and Google Workspace™, or through MAC-based authentications and AI-based Client Insights. This automates and simplifies policy definition for IoT devices with behavior-based profiling using AI or ML based classification, enabling a stronger security posture than by using MAC addresses alone.

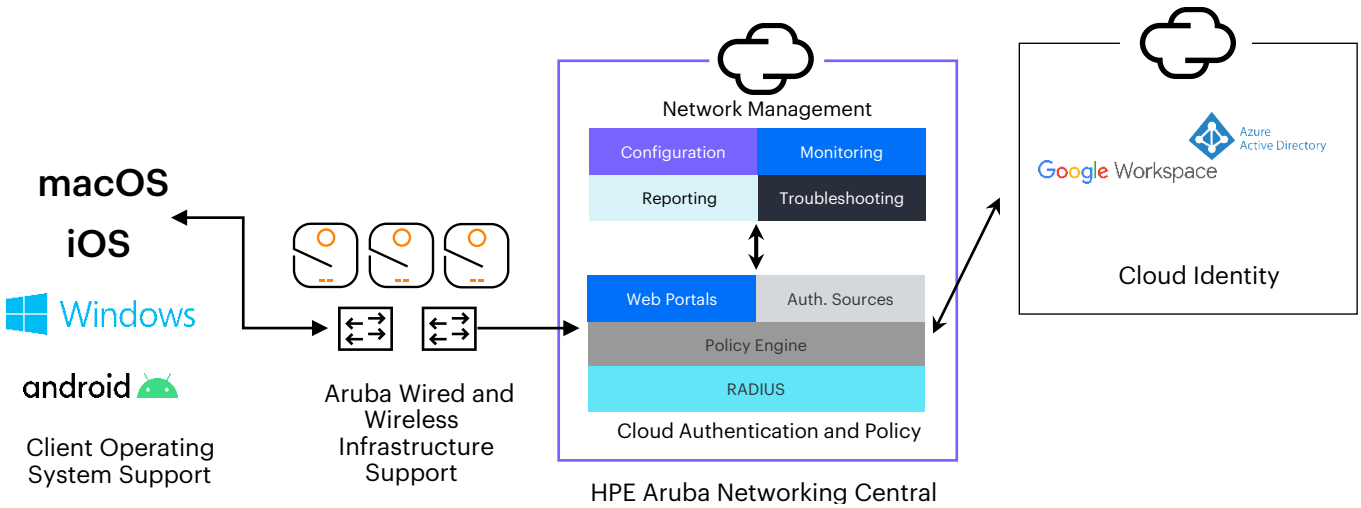
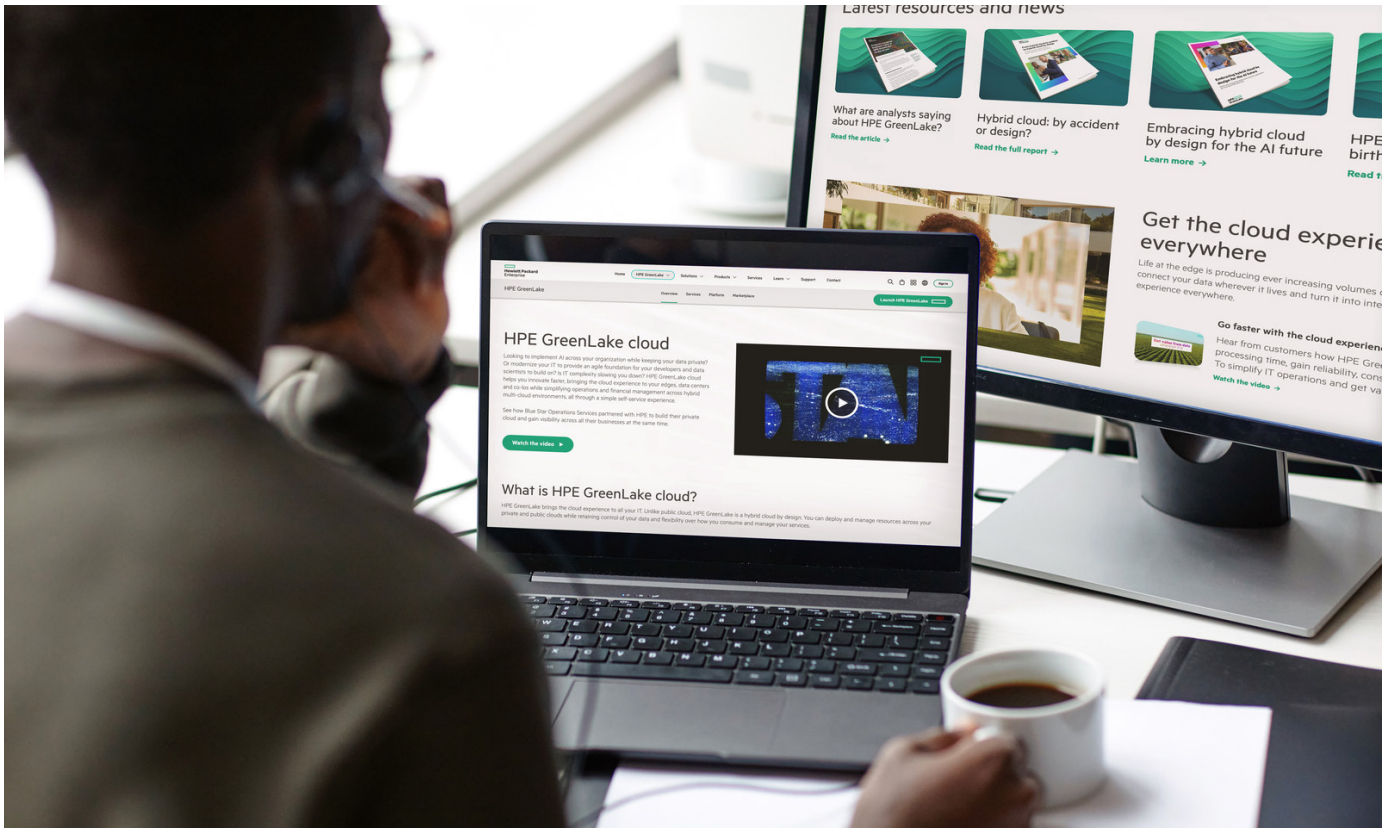


Figure 13. CloudAuth service in NetConductor provides a flexible, powerful framework for granting network access



Management plane security and system hardening

EdgeConnect SD-Branch[3] uses Trusted Platform Module (TPM) technology, an international standard for a secure tamper-resistant cryptoprocessor, which is a dedicated microcontroller designed to secure hardware by integrating cryptographic keys into devices. By using tamper-resistant keys, the device integrity and boot code can be validated as unchanged, ensuring a clean startup process. Attestation encryption keys are installed during manufacturing to enable the process.

Secure boot — EdgeConnect SD-Branch requires HPE Aruba Networking-issued TPM certificate (Trusted Platform Module) to load ArubaOS. TPM-signed software image heavily restricts communications until EdgeConnect SD-Branch gateway receives its initial configuration from HPE Aruba Networking Central.

Secure zero touch provisioning — To secure communications with HPE Aruba Networking Central, EdgeConnect SD-Branch leverages the TPM certificate loaded in the HPE Aruba Networking gateways. This connection uses the Transport Layer Security protocol (TLS 1.2).

WAN Protect ACL — A default ACL protects the WAN side of EdgeConnect SD-Branch from external threats. It is applied to all ports which are marked as WAN port.

AES 256 encryption — EdgeConnect SD-Branch builds IPSec encrypted tunnels using AES 256-bit encryption across the entire SD-WAN fabric. IPSec tunnels are based on Internet Key Exchange Protocol Version 2 (IKEv2). HPE Aruba Networking gateways leverage factory installed Trusted Platform Module (TPM) certificates for mutual authentication to simplify and automate overlay tunnel establishment. TPM factory certificates are installed on each gateway at the factory, however user uploaded certificates are supported if required. The only protocol and port that needs to be open for an overlay IPSec tunnel to be established is UDP destination port 4500.

HPE Aruba Networking framework to zero trust security and compliance

HPE Aruba Networking provides an integrated approach to ensure zero trust security that encompasses LAN, WLAN, and WAN networks. This approach consists of five steps including:

- **Visibility:** Discover devices on the network based on AI methods
- **Authentication and authorization:** authenticate and define access policies
- **Role-based access security:** dynamically provide access to some segments of the network
- **Continuous monitoring:** detect external threats based on alerts
- **Enforcement and response:** provide relevant response to identified threats.

Figure 14. HPE Aruba Networking integrated approach to security (wired and wireless security)

[3] To learn more, please refer to the HPE Aruba Networking EdgeConnect SD-Branch hardening guide.

— **Visibility:** With the increased adoption of IoT, HPE Aruba Networking Client Insights enables organizations to quickly identify device types based on ML-based classification models.

— **Authentication:** HPE Aruba Networking ClearPass Policy Manager and HPE Aruba Networking creates role-based access policies, and authenticates every device connected to the network. Multiple authentication methods can be used. For networks managed by HPE Aruba Networking Central, Cloud Auth provides onboarding of end users and client devices either through MAC or through integrations with cloud identity stores such as Google Workspace or Azure Active Directory.

— **Role-based access control:** EdgeConnect SD-Branch provides dynamic segmentation based on role and identity enabling a zero trust architecture with least privilege access. Additionally, NetConductor, part of HPE Aruba Networking Central enables dynamic segmentation over large, distributed networks using widely-adopted protocols such as EVPN/VXLAN.

— **Continuous monitoring and enforcement:** EdgeConnect SD-Branch performs intrusion detection and prevention (IDS/IPS), performing signature- and pattern-based traffic inspection on both the branch office LAN (east-west) traffic as well as the SD-WAN (north-south) traffic. An advanced security dashboard within HPE Aruba Networking Central provides IT teams with network-wide visibility, multi-dimensional threat metrics, threat intelligence data, as well as correlation and incident management. Threat events are sent to SIEM systems and ClearPass for remediation.

The table below shows the different security components available for HPE Aruba Networking EdgeConnect SD-Branch.

HPE Aruba Networking helps organizations achieve compliance to many standards and regulatory frameworks such as the NIST CSF framework, HIPAA and PCI DSS thanks to its advanced AI-based identity capabilities, zero trust dynamic segmentation, IDS/IPS, unified SASE, and its tight integration with multiple third-party cloud security vendors as well as its ability to monitor and stream network events to SIEM solutions such as Splunk.

Table 2. Security components available for HPE Aruba Networking EdgeConnect SD-Branch

Security component	Details
Client Insights	Uses network and client telemetry with machine learning to accurately fingerprint and classify all wired and Wi-Fi connected user and IoT endpoints for policy assignment and enforcement. Also monitors the behavior of traffic flows for added security.
CloudAuth	Enables onboarding of end users and client devices either through MAC address-based authentication or through integrations with common cloud identity stores such as Google Workspace or Azure Active Directory.
HPE Aruba Networking ClearPass Policy Manager	Provides role- and device-based secure network access control for IoT, BYOD, corporate devices, as well as employees, contractors and guests across any multivendor wired, wireless and VPN infrastructure.
Policy Enforcement Firewall	Next-generation role-based user, device, and application policy enforcement firewall provides automated dynamic segmentation for wireless and wired access security.
Central NetConductor	Automatically configures LAN, WLAN, and WAN infrastructure at scale to deliver optimal network performance while enforcing granular access control security policies.

HPE Aruba Networking security partners

To provide advanced security capabilities, EdgeConnect SD-Branch integrates the technology components from a variety of security partners including Qosmos, Webroot, and proofpoint.

ENEA Qosmos	Qosmos's embedded DPI-based traffic intelligence provides the capacity to identify close to 3500 applications.
WEBROOT®	Webroot's machine learning technology classifies content, reputation, and geolocation for billions of URLs.
proofpoint.	Proofpoint Threat Intelligence provides threat intelligence on malicious activities and ensures that organizations stay on top of the dynamic threat landscape. It includes over 65,000 rules broken down into 50 categories.

Conclusion

With the acceleration of digital transformation, organizations must now modernize their network architecture to support the move of applications to the cloud, hybrid working and the need for increasing bandwidth. As the security perimeter is dissolving and cybersecurity risks increase, organizations must overhaul their networking and security capabilities in branch offices.

EdgeConnect SD-Branch provides an integrated solution that combines SD-WAN, wireless and wired connectivity along with advanced cloud-delivered security capabilities. It provides a variety of mechanisms for securing the distributed enterprise including:

— Unified SASE by combining EdgeConnect SD-Branch with HPE Aruba Networking SSE
— Automated orchestration to third-party SSE vendors such as ZScaler
— Application-aware stateful firewall with deep packet inspection and intrusion detection and prevention (IDS/IPS)
— Threat event logging that can be streamed to third-party SIEM solutions to improve incident management
— Role-based dynamic segmentation ensuring users and IoT devices reach destinations consistent with their role, even in complex distributed environments
— Web content classification, IP reputation and geolocation filtering
— Data encryption over the entire SD-WAN fabric
— Hardened platform with Trusted Platform Module (TPM) protection

EdgeConnect SD-Branch is a key component of the Edge Services Platform (ESP) from HPE Aruba Networking, enabling organizations to accelerate digital business transformation through automated network management, edge-to-cloud security, and predictive AI-powered insights. It provides a unified approach to centrally manage all security and network aspects including wireless, LAN and WAN connectivity, as well as Network as a Service (NaaS), with common zero trust and SASE security frameworks spanning the entire portfolio. HPE Aruba Networking advanced AIOps capabilities automatically and continuously monitor network, and application performance as well as security policy enforcement, enabling automated remediation to impairments or potential threats.

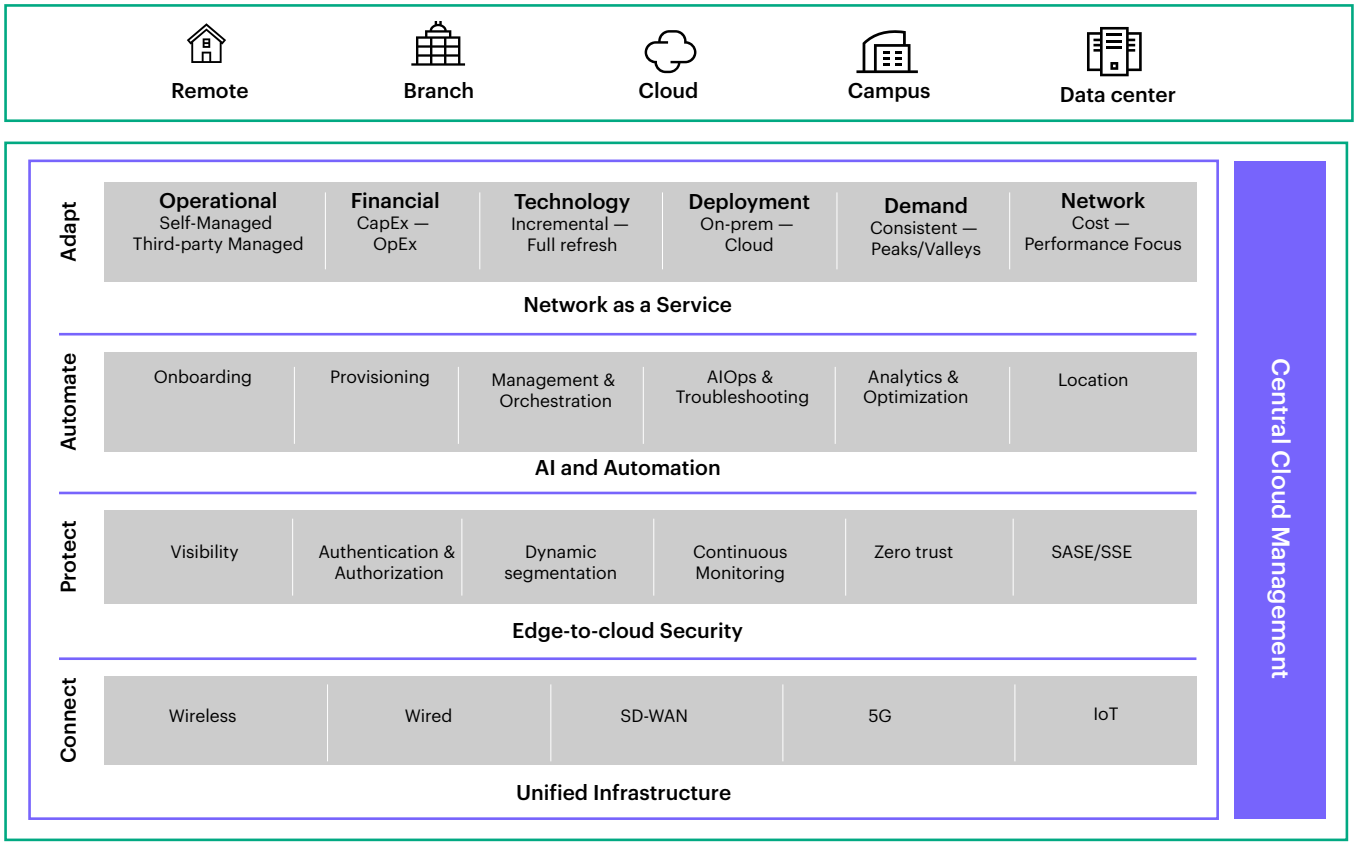


Figure 15. The four layers of the Edge Services Platform from HPE Aruba Networking

Resources

The following resources are available for more information:

— Unified Policy For the Distributed Enterprise: Role-based policy and security across LAN and WAN

— Policy Enforcement Firewall Technical Brief: Functionality of the gateway's stateful firewall

— Edge-to-Cloud Security Page: HPE Aruba Networking's integrated framework for visibility, control and AI-powered insights

— Zero Trust and SASE Page: HPE Aruba Networking built-in zero trust and SASE security to ensure that the same access controls are applied everywhere

— HPE Aruba Networking EdgeConnect SD-WAN Home Page: Functionality and benefits of HPE Aruba Networking's SD-WAN solution

— HPE Aruba Networking EdgeConnect SD-Branch: Functionality and benefits of EdgeConnect SD-Branch solution

— HPE Aruba Networking EdgeConnect SD-Branch Data sheet: Includes ordering information for HPE Aruba Networking Virtual Gateways

— Dynamic Segmentation Solution Overview: Identity-based access control at a global scale

— HPE Aruba Networking Central NetConductor Solution Overview: Automate configuration, policy definition and enforcement at global scale

Visit HPE.com

Chat now

a00093929ENW

HEWLETT PACKARD ENTERPRISE

hpe.com