HPE aruba networking

Solution Overview

Implementing Zero Trust best practices

With HPE Aruba Networking network access control, SSE and SASE

IT security challenges have evolved significantly over the years as users have become increasingly decentralized and attacks have become more sophisticated and persistent. Traditional security approaches focused primarily on the perimeter of the network have become ineffective as stand-alone security strategies. Modern network security must accommodate an ever-changing, diverse set of users, applications, and devices, as well as much more prevalent threats targeting previously "trusted" parts of the network infrastructure.

Zero Trust has emerged as an effective model to better address changing security and regulatory compliance requirements of the modern enterprise by assuming that all users, devices, servers, and network segments are inherently insecure and potentially hostile.

Building on the foundations of Zero Trust, the SASE (Secure Access Service Edge) security architecture emerged, reflecting the importance of cloud-based workloads and augmenting advanced SD-WAN capabilities with cloud-delivered security services. Zero Trust and SASE frameworks provide the blueprint for a secure network foundation that uses identity-based network segmentation and application access controls to protect the organization.

With a built-in foundation for Zero Trust and SASE, HPE Aruba Networking Edge Services Platform (ESP) offers organizations security from edge to cloud, improving overall security posture by applying a rigorous set of security best practices and controls to previously trusted network and cloud resources.

HPE Aruba Networking ESP: core Zero Trust principles

Zero Trust varies significantly depending on which domain of security is being considered. Although application-level controls are a focal point within Zero Trust, a comprehensive strategy must also encompass network security, the growing number of connected devices, and the hybrid work environment. HPE Aruba Networking ESP with edge-to-cloud security incorporates comprehensive visibility, authentication and authorization, and least-privilege access controls, as well as continuous monitoring and policy enforcement, both on and off the corporate network. Zero Trust Network Access (ZTNA), the next generation of VPN-like access, enables organizations to extend Zero Trust Security to remote locations and mobile workers.

Figure 1. HPE Aruba Networking Zero Trust Security foundation

Basic principles of good networking dictate that, when possible, all devices and users should be identified and properly authenticated before granting them network access. In addition to authentication, users and devices should be given the least amount of access necessary to perform their business-critical activities once they're on the network. This means authorizing which network resources and applications any given user or device can access. Finally, all communications between end users and applications should be encrypted.

Yet many organizations struggle to implement these practices due to architectural complexity and lack of integration between disparate security components.

An approach with built-in support for each critical Zero Trust and SASE security capability can significantly improve protection while simplifying operations.

Achieving comprehensive visibility

With the increased adoption of IoT, full-spectrum visibility of all devices and users on the network has become an increasingly important—and challenging—task. Without visibility, critical security controls that support a Zero Trust model are difficult to apply. Automation, AI-based machine learning, and the ability to quickly identify device types are critical.

Cloud-based network management solution HPE Aruba Networking Central includes AI-powered visibility and profiling with Client Insights. Client Insights leverages native infrastructure telemetry from access points, switches, and gateways, as well as clients, without requiring installation of physical collectors or agents. ML-based classification models are used to automatically fingerprint and identify with up to 99% accuracy a wide variety of endpoints connecting to the network, including a diverse set of IoT devices across the entire wired and wireless infrastructure. For environments not managed by cloud-based HPE Aruba Networking Central or with third-party network devices, ClearPass Device Insight (CPDI) can be leveraged for ML-based identification and profiling of clients.

Easing authentication & authorization

Once a user or device is known and profiled, the next step is to authenticate its identity each time it connects to the network. With ClearPass, organizations can deploy wired or wirelessly using standards-based 802.1X enforcement for secure authentication. ClearPass also supports MAC address authentication for IoT and headless devices that may lack support for 802.1X. For wired environments where RADIUS-based authentication cannot be deployed, ClearPass offers an alternative using SNMP-based enforcement. Multiple authentication methods can be used to concurrently support a variety of use cases including support for multifactor authentication based on log-in times, posture checks, and other context such as new user, new device, and more.

For networks managed by HPE Aruba Networking Central, cloud-native NAC solution Cloud Auth enables frictionless on-boarding 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 to automatically assign the right level of network access.

Adopting identity-based access control for least-privilege access

Least-privilege access based on identity allows users and devices to access just the resources needed to perform their functions—and only for as long as they behave consistently with their role. This means applying an access control policy that limits access to resources and dynamically adjusts access when anomalous behavior is observed or breach is suspected.

Dynamic Segmentation establishes least-privilege access to applications and data by segmenting traffic based on identity and associated access permissions. Dynamic Segmentation supports two enforcement models—centralized and distributed—allowing IT to use one or both models based on the needs of the environment. With centralized Dynamic Segmentation, traffic is kept secure and separate with the use of GRE tunnels between access points and HPE Aruba Networking gateways (or mobility controllers). ClearPass Policy Manager enables the creation of role-based access policies that follow the user throughout the network and are applied uniformly across wireless, wired, and remote connections. Enforcement is provided by Policy Enforcement Firewall (PEF), a full application firewall embedded in HPE Aruba Networking network infrastructure.

HPE Aruba Networking Central NetConductor enables distributed Dynamic Segmentation using widely adopted technology, such as EVPN/VXLAN, to produce a distributed network overlay. The HPE Aruba Networking Central NetConductor full-stack solution includes cloud-native security services for global policy management and network configuration with a simple business-logic interface and intuitive workflows. Global policy identifiers reflecting the role and access permission of the user or device are embedded in the packet header and interpreted inline by CX switches and gateways for policy enforcement.

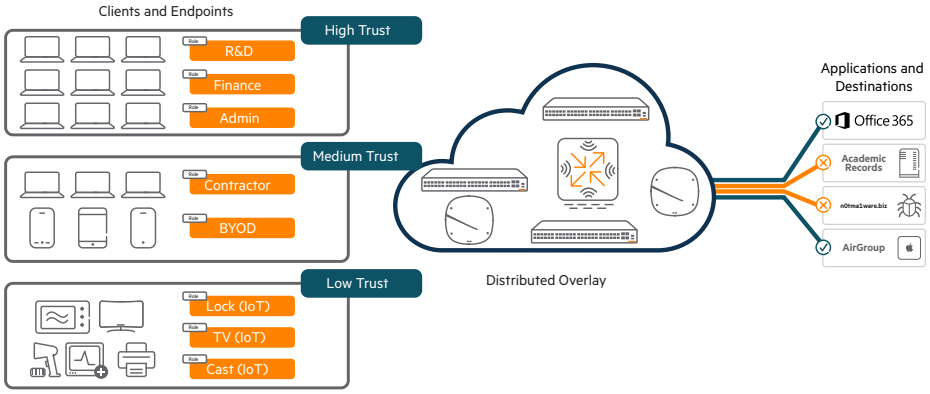


Figure 2. Dynamic Segmentation with a distributed overlay fabric

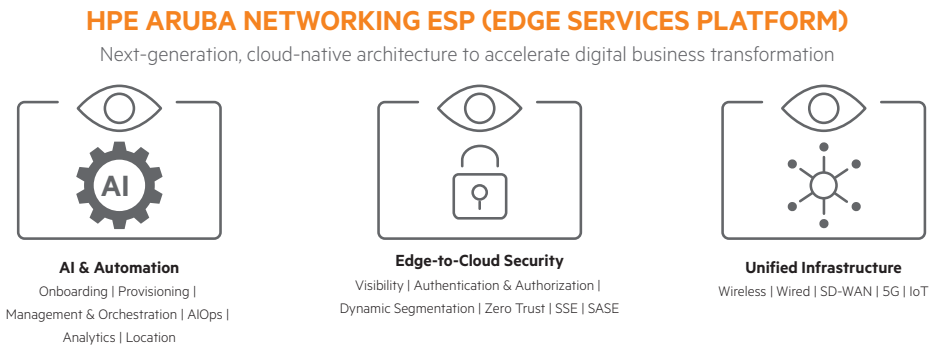


Figure 3. Edge-to-Cloud Security increases protection while simplifying network and security operations

Ensuring continuous monitoring and enforcement

With role-based access in place to enforce granular segmentation, ongoing monitoring of users and devices on the network make up another Zero Trust Security best practice. This addresses risks related to insider threats, advanced malware, or persistent threats that have circumvented traditional perimeter defenses.

360 Security Exchange

With over 150 integrations made up of best-of-breed security solutions that include security operations and response (SOAR) tool sets, ClearPass is able to dynamically enforce access based on real-time threat telemetry coming from multiple sources. Policies can be created to make real-time access control decisions based on alerts coming from security information and event management (SIEM) tools and many other sources. ClearPass actions are fully configurable, from limiting access (e.g., Internet access only) to fully removing a device from the network for remediation.

Threat protection

Prevent and contain threats from edge-to-cloud. An advanced security dashboard within HPE Aruba Networking Central provides IT teams with network-wide visibility, multi-dimensional threat metrics, and threat intelligence data, as well as correlation and incident management. Also within HPE Aruba Networking Central, an enhanced application identity engine allows IT organizations to see apps in use, assign risk scores based on app reputation and identity, and define risk-based alerts and policies. Risk-oriented traffic inspection enables organizations to supplement IDS/IPS by designating traffic to inspect at the gateway, reducing risk from threats that propagate beyond the firewall while improving performance and throughput. Threat events can be sent to SIEM systems and ClearPass for remediation.

Delivering access at the edge (SSE/SASE)

Increased hybrid work and continued migration of applications to the cloud are changing network planning and related security requirements, since approaches that rely on network control were not designed to accommodate a cloud-first world. Organizations require a comprehensive, edge-to-cloud approach to ensuring security and compliance that is independent of the method of connection and types of network while optimizing performance and availability.

Protecting against myriad threats, such as phishing, ransomware, and denial of service (DoS) attacks, is critical within the distributed enterprise. The market's first complete solution to receive Secure SD-WAN Certification from ICSA Labs, EdgeConnect SD-WAN with next-generation firewall and DDoS detection and remediation capabilities can replace outdated and difficult-to-manage physical firewalls at branch locations while delivering consistent security for all users, from any network location, from any device, and wherever applications are hosted.

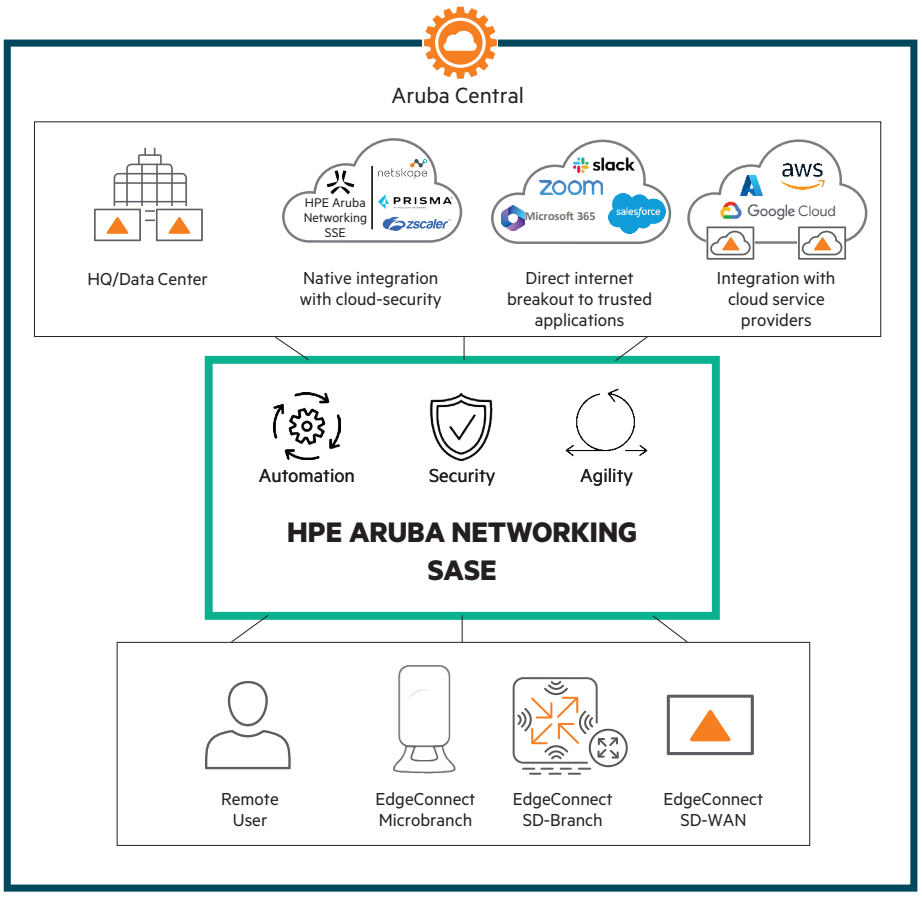


Figure 4. The HPE Aruba Networking SASE solution delivers enhanced, secure connectivity experiences without compromise to networking or security.

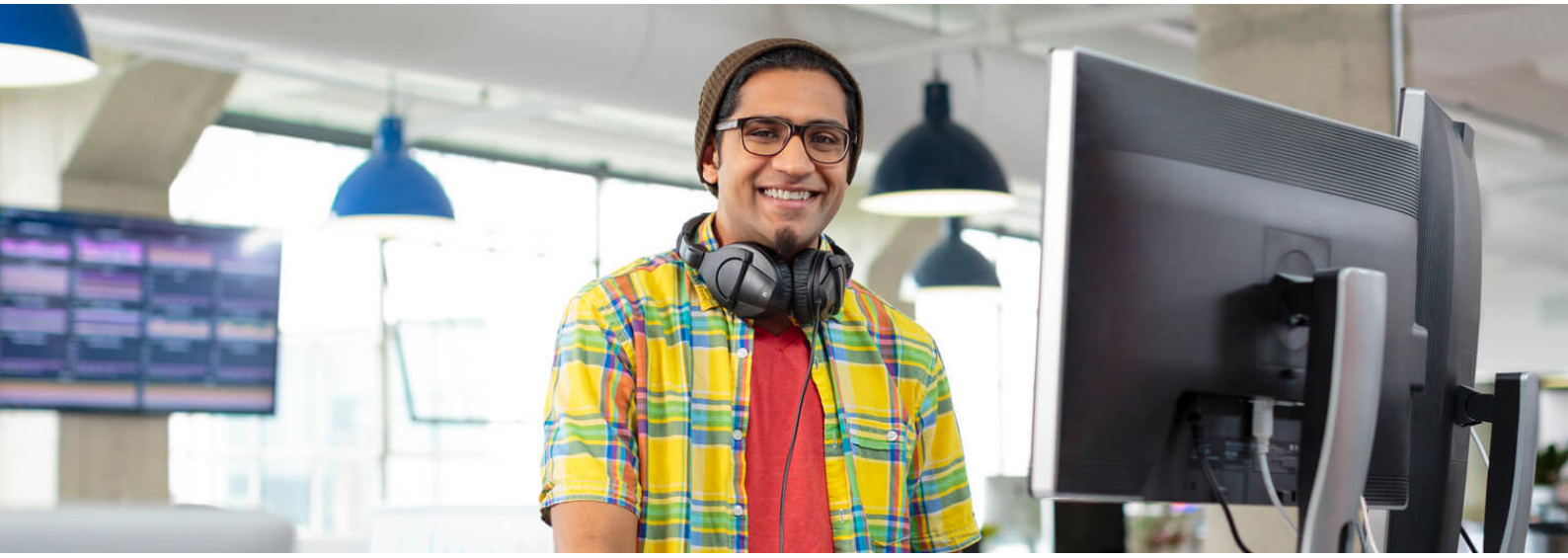
EdgeConnect solutions can also secure branch and microbranch locations using built-in firewall, Dynamic Segmentation, and Aruba Threat Defense capabilities, including IDS/IPS. App security services including DPI, Web classification and URL filtering, and IP and geo reputation data help organizations protect against threats wherever they originate.

By combining the advanced capabilities of EdgeConnect SD-WAN, SD-Branch, and microbranch solutions with the cloud-delivered, Zero Trust security services of an SSE (Security Service Edge), distributed organizations can build a flexible SASE architecture to ensure stable, secure access to business applications while converging network and security functions.

HPE Aruba Networking SSE empowers organizations to unify secure access across campus, branch, home, and remote locations. Access is harmonized across the world via a cloud backbone of Amazon Web Services (AWS), Microsoft Azure, Google™, and Oracle®.

The platform delivers authenticated user access to private applications at the network edge (Zero Trust Network Access—ZTNA), a secure web gateway (SWG) to safeguard user access to the Internet, and a cloud access security broker (CASB) that enforces policies to protect sensitive data, as well as data loss prevention (DLP) capabilities. When deployed with the EdgeConnect portfolio, organizations gain the operational benefits of a unified, single-vendor SASE solution.

For organizations seeking architectural flexibility without adding complexity, the EdgeConnect portfolio offers tight integrations with a wide variety of cloud security vendors. Automated orchestration and configuration significantly reduces the time and effort it takes to incorporate cloud-based security services into existing network infrastructure while preserving freedom of choice.



Building on a secure foundation

Zero Trust Security begins with supply chain and infrastructure confidence. HPE Aruba Networking solutions are developed according to software development lifecycle (SDLC) and secure software development framework (SSDF) best practices. Solutions can be used in compliance with mandates and programs such as Common Criteria, FIPS-140, DoDIN-APL, USGv6, and FedRAMP.

Device assurance

To safeguard against malicious boot code and device impersonation attacks, HPE Aruba Networking wired and wireless networking solutions use Trusted Platform Module (TPM) technology, an international standard for a secure, tamper-resistant crypto-processor designed to secure hardware by integrating cryptographic keys into devices. Installed during manufacturing, TPM technology can provide a secure root of trust upon which to build additional layers of Zero Trust and SASE security.

Wireless intrusion protection

Within HPE Aruba Networking Central, the Rogue AP Intrusion Detection System (RAPIDS) enables organizations to set custom rules for rogue AP detection according to their own risk thresholds. This capability can help protect against unauthorized rogue APs gaining backdoor access to the network and intercepting user data.

Summary

Today's business environment and threat landscape require a modern approach to network and application security. HPE Aruba Networking ESP with edge-to-cloud security provides built-in support for Zero Trust and SASE security frameworks, spanning visibility, identity-based control, and enforcement to address the requirements of a decentralized, IoT-driven and agile network infrastructure.

Learn more at

arubanetworks.com/zerotrust

Make the right purchase decision.
Contact our presales specialists.

Contact us

© Copyright 2023 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Google and Google Workspace are registered trademarks of Google LLC. Active Directory, Azure, and Microsoft are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Oracle is a registered trademark of Oracle and/or its affiliates. All third-party marks are property of their respective owners.

a00097694enw SK 061423