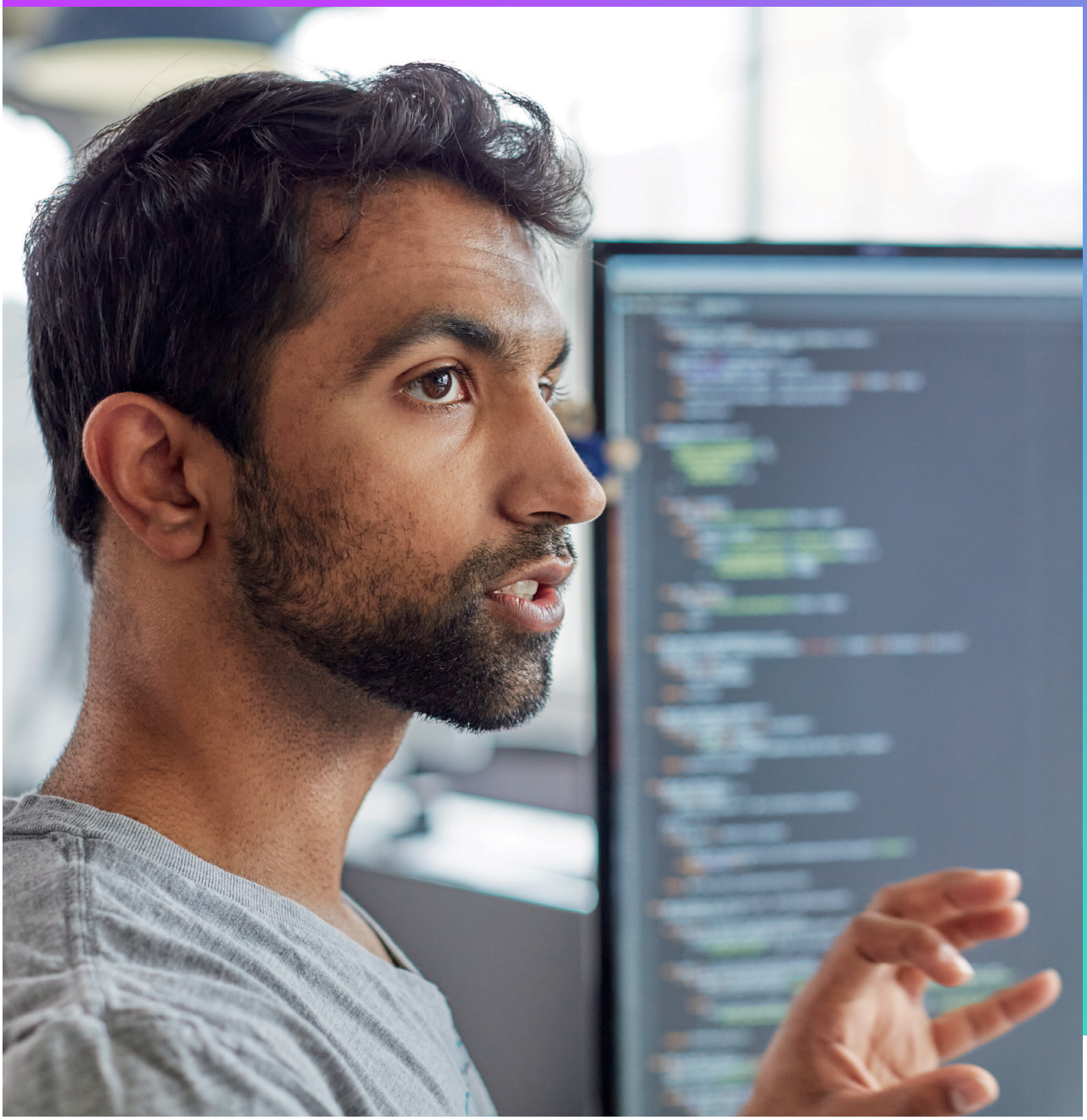


HPE aruba networking

The architect's guide to adopting Secure Access Service Edge (SASE)

HPE GreenLake

Introduction

Architects are uniquely positioned to witness the dynamic evolution of technology. Amid this rapid transformation, they occupy a privileged standpoint, particularly when it comes to the innovative frontiers of network and security technologies. Today's architects bear the critical responsibility of discerning the optimal solutions and technologies from a plethora of choices, addressing pressing concerns like secure application access and seamless business connectivity.

In hybrid work environments, where applications straddle both on-premises and cloud realms, architects need to adopt Zero Trust principles to modernize legacy network connectivity safeguards and redefine the very methods of dispensing secure application access.

This guide empowers architects with a holistic grasp of the strategic significance behind incorporating a SASE framework. It covers the key challenges in networking and security and unravels the intricacies of SASE—delivering pivotal platform prerequisites, use cases, and pragmatic recommendations. These provisions guide architects through implementation and the successive stages of their transformative SASE journey.

Security and network challenges for architects

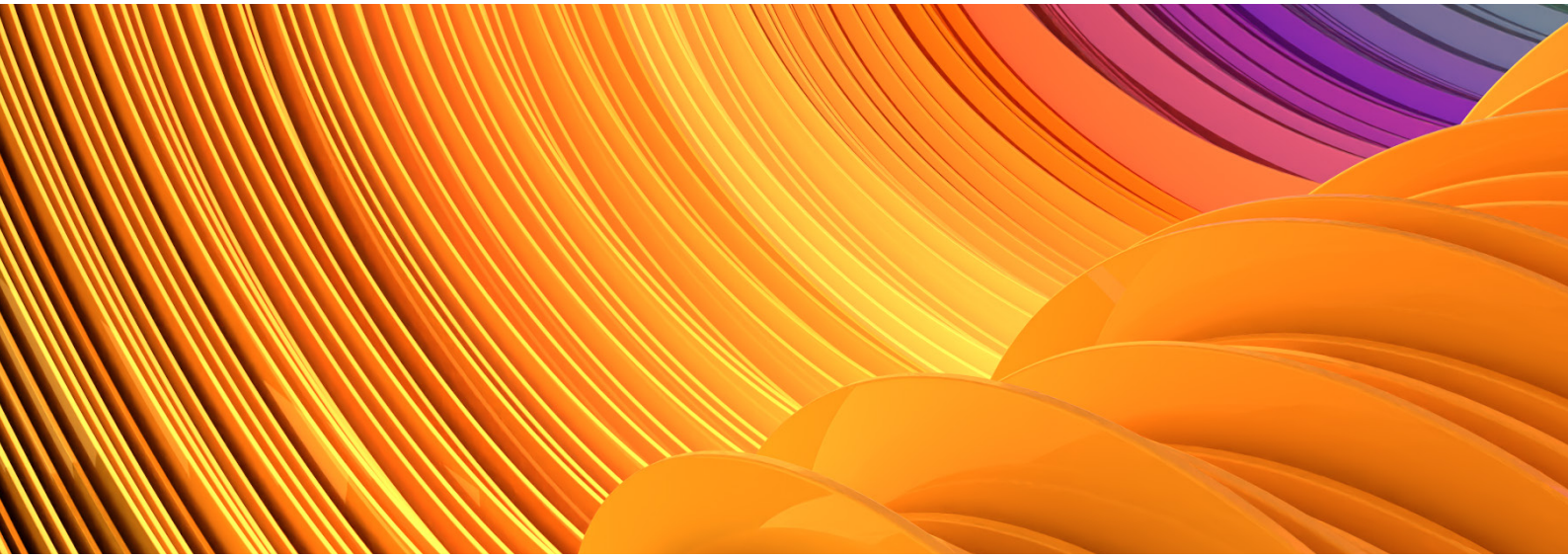
While digital transformation has empowered architects in numerous areas, it has also created a variety of security and networking challenges and complexities that architects must strategically navigate.

Security challenges and needs

- Enable comprehensive security for all users, devices, and applications
- Eliminate attack surface and attack vectors
- Minimize the impact of ransomware or malware attacks by reducing lateral movement
- Implement least-privilege access with Zero Trust policies
- Protect against data exfiltration with enhanced control of data
- Reduce security blind spots by gaining visibility and control of shadow IT
- Enable SSL encryption at scale with cloud
- Enhance visibility with an extensive view into all user, device, and application activity

Networking challenges and needs

- Support all applications—legacy or cloud—with a single-access solution
- Minimize vendor sprawl and simplify network services
- Ensure a consistent and high-quality user experience for all cloud-hosted business applications across the WAN
- Maintain up-to-date network connectivity policy enforcement with changes to new users, IoT devices, and applications
- Reduce over-extension of network privileges to users
- Segment access on a granular one-to-one basis, without network access or network segmentation
- Optimize connectivity paths and reduce latency with intelligent routing
- Reduce outages and downtime with precise digital experience troubleshooting
- Speed deployment and provide effortless scale with a cloud-native architecture



63%

of organizations have a 3+ security solutions

A SASE solution can help overcome the mix of both security and networking challenges faced today. In addition, the ideal SASE solution should unify your security and networking teams rather than create further tension.

SASE overview and components

What is SASE?

Secure Access Service Edge, or SASE, is a cybersecurity concept that was first introduced in 2019 by Gartner®. SASE is an IT framework that combines networking and security functions into a single platform that securely connects all users, devices, and applications across the globally distributed workforce.

The main components of SASE are advanced SD-WAN (WAN edge) and comprehensive cloud-delivered security (Security Service Edge, or SSE).

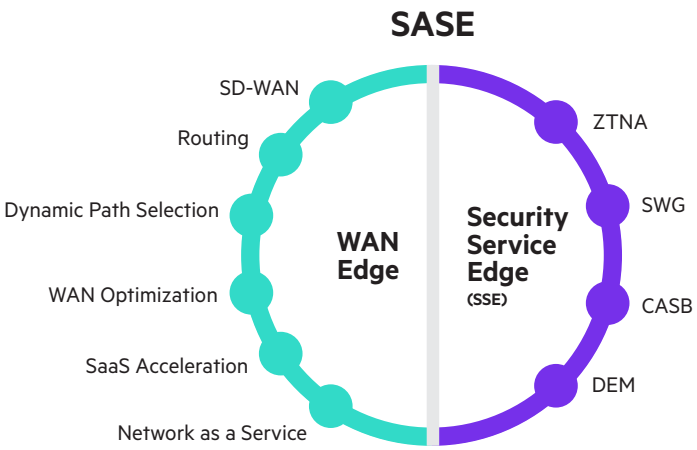


Figure 1. Secure Access Service Edge

The elements of SASE

Let's break each SASE element down further:

WAN edge services (Secure SD-WAN)

Security: Includes secure SD-WAN next-generation firewall capabilities, including IDS/IPS and granular segmentation—enabling organizations to replace branch firewalls and secure IoT devices. Additionally, all connections are encrypted over the SD-WAN fabric.

QoS and SaaS optimization: Identifies application traffic on the first packet and dynamically steers it to enforce both QoS and security policies as defined by business intent to avoid backhauling of traffic to the data center.

Routing: Replaces branch router functions including BGP routing with SD-WAN with continuous self-learning and automatic daily updates to cloud application definitions and TCP/IP address ranges.

Multicloud networking: Allows you to deploy virtual instances of SD-WAN solutions in cloud service providers such as AWS, Microsoft Azure, and Google Cloud—establishing a resilient connection from the branch office to the cloud.

Dynamic path control: Combines multiple transport links including MPLS, broadband internet, 4G/5G, or satellite links. It dynamically selects the best links based on network conditions and business intent.

Intelligent network operations: Enables intelligent monitoring and management of all underlay transport services, using tunnel bonding and path conditioning to actively use multiple forms of WAN transport to provide a private-line-like performance over internet links, enabling organizations to reduce MPLS dependency and quickly spin up new branches.

WAN optimization: Accelerates the transmission of data over the WAN by applying TCP protocol acceleration as well as data deduplication and compression algorithms.

Centralized orchestration: Allows business and security policies to be centrally managed from a single interface to simplify network operations and troubleshooting, as administrators can make changes and apply policies from a central location.

Security Service Edge (SSE)

Zero Trust Network Access (ZTNA): Ensures secure access to private applications. ZTNA technology provides granular, identity based Zero Trust access to private applications and resources, regardless of where they are hosted or where users are located. Modern ZTNA solutions allow teams to eliminate remote access VPNs for employees and third-party users, significantly reducing the attack surface by allowing access to specific authorized private applications without extending access to the underlying network.

Secure Web Gateway (SWG): Provides secure access to the Internet. SWG protects the distributed business against advanced attacks with capabilities like web filtering, SSL inspection, and malware detection and prevention. SWG ensures that authorized users get fast, secure access to Internet resources while protecting the business from harm.

Cloud Access Security Broker (CASB): Ensures secure access to SaaS applications. CASB allows IT to identify, manage, and control the use of cloud services. A CASB service mediates connections between users and cloud-based SaaS applications and helps regulate data flow, prevents data loss, and uncovers shadow IT to ensure sensitive data remains protected.

Digital Experience Monitoring (DEM): Delivers enhanced digital experience and productivity. DEM provides enhanced, in-line visibility and analysis into the interactions, experience, and performance of devices, applications, and networks. DEM helps IT teams better utilize their time by accelerating troubleshooting and allowing for pinpoint diagnostics of experience issues.

SASE platform requirements

When evaluating a robust and effective Secure Access Service Edge (SASE) platform, certain key solution requirements must be met. These requirements encompass comprehensive architecture, features, and capabilities, all aimed at ensuring a secure, agile, and streamlined network and security infrastructure. SASE platform requirements include:

- **Unified security and networking:** A core tenet of SASE is the convergence of security and networking functionalities. The platform should seamlessly integrate, or in some cases overlay, with security services such as VPN, firewalling, intrusion prevention, secure web gateways, and more with networking capabilities like SD-WAN to enable consistent and efficient traffic management.
- **Cloud-native architecture:** SASE platforms should be inherently cloud-native, designed to leverage the scalability, elasticity, and agility of cloud environments. This ensures the seamless integration of on-premises resources, cloud applications, and remote users into a cohesive security and networking fabric.
- **Global edges:** An essential aspect of SASE is its distributed architecture, which entails having on ramps close to the users across various geographical locations. These edges facilitate optimized traffic routing, reduced latency, and enhanced user experiences by directing traffic through the most optimal paths.
- **Zero Trust Security model:** SASE platforms must adhere to a Zero Trust security model, wherein trust is never assumed based on location alone. Identity, device posture, and contextual factors play pivotal roles in determining access to resources, thereby bolstering overall security.
- **Granular segmentation:** To enhance security, SASE platforms should support fine-grained segmentation, enabling the segmentation of network traffic into smaller, isolated segments. This helps contain potential breaches and limit lateral movement within the network.
- **Application-aware security:** The ability to provide granular security policies based on application-level insights is crucial. SASE platforms should be capable of identifying and classifying applications to apply tailored security measures based on their specific requirements.

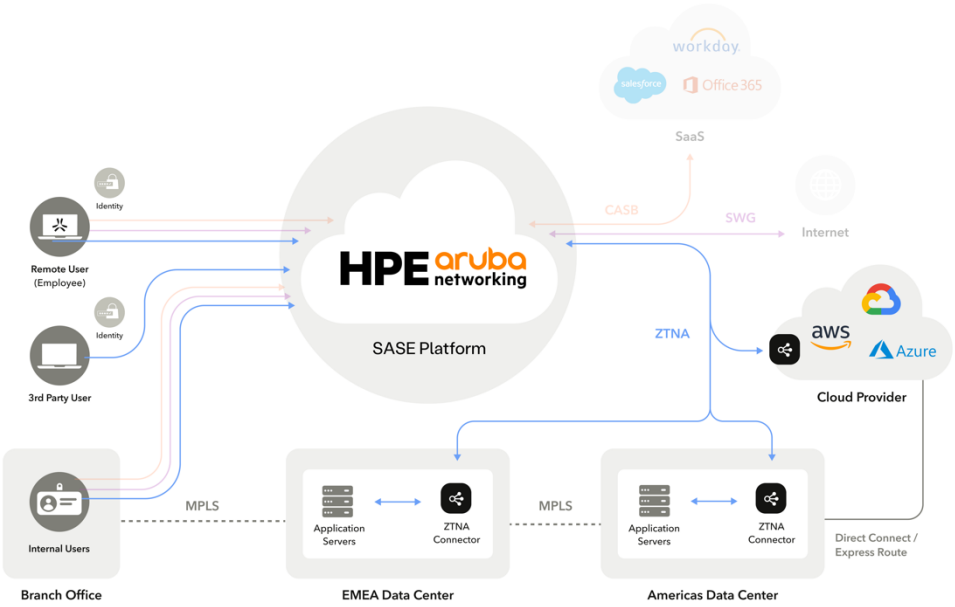


Figure 2. Secure remote access to private applications

- **User-centric policies:** SASE frameworks should allow the creation of policies that are user-centric, accommodating the dynamic nature of modern work environments. Policies should adapt based on user roles, device types, and locations to ensure a balance between security and user experience.
- **Comprehensive analytics and visibility:** Robust analytics and visibility tools are essential for monitoring network and security performance. SASE platforms should offer real-time insights into traffic patterns, user behavior, and threat detection, facilitating proactive responses.
- **Integrated threat intelligence:** An effective SASE platform should integrate threat intelligence feeds and advanced threat detection mechanisms to identify and thwart emerging security threats in real-time.

Five SASE use cases

Let's cover some common SASE use cases architects might consider to provide quick wins that positively impact the business. You can implement SASE in a planned, phased approach by understanding its benefits and impact on typical use cases—no need to change everything at once.

1. Secure remote access to private applications

Many enterprises still use legacy VPNs to provide network access to remote employees and extended business ecosystem users who only need access to a limited number of private applications. However, 65% of businesses are considering the switch away from legacy VPN in favor of another remote access alternative (2022 VPN Risk Report, Cybersecurity Insiders). Many of these organizations may find themselves turning to Zero Trust Network Access (ZTNA) technologies as a result. By prioritizing ZTNA adoption for business-critical applications, IT and security teams can significantly reduce risk while also providing a better user experience for the business.

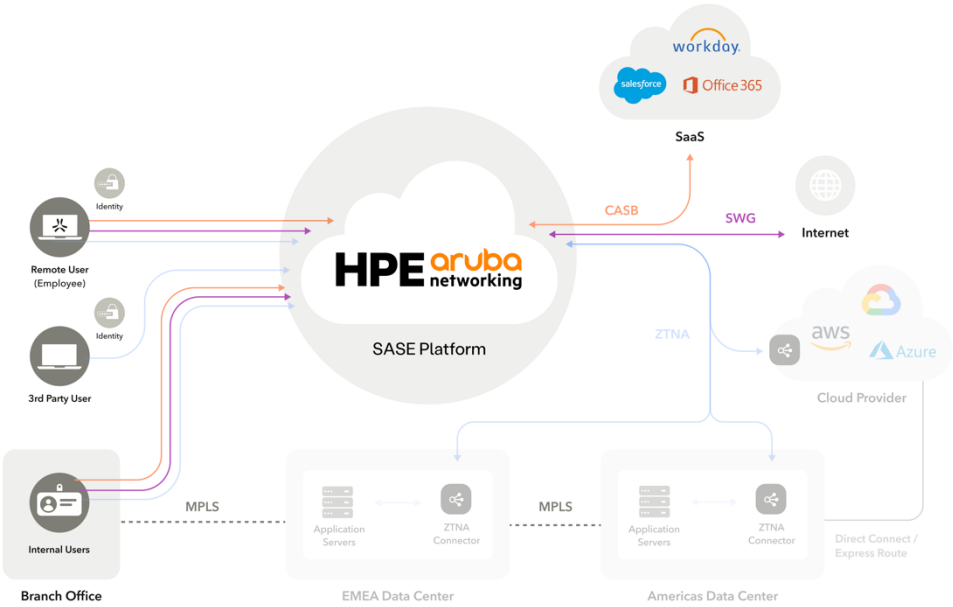


Figure 3. Secure access to the Internet and SaaS applications

2. Secure access to the Internet and SaaS applications

The imperative lies in simplifying complexities in a landscape teeming with countless websites and SaaS applications at users' disposal. This can be achieved by intelligently categorizing applications into distinct segments, guided by the imperatives of business necessity, the potential for data leakage, and the potential impact on user performance.

To embark on this journey, start by pinpointing the core business application services in use across your enterprise. Familiar applications like Microsoft 365, Salesforce, and Workday, among others, fall under this category. These services invariably demand controlled entry, a watchful eye for detecting threats, threat prevention, and safeguards against data loss. It's here that the significance of Secure Web Gateway (SWG) and Cloud Access Security Broker (CASB) solutions comes to the forefront and should be deployed.

As businesses pivot towards a landscape dominated by web-based resources and SaaS offerings, an extensive repository of customer and user data, intellectual property, and other mission-critical data transcends geographical boundaries, becoming accessible to a global audience. Safeguarding the pathways to these services takes precedence like never before.

As you advance your SASE deployment, the integration of SWG and CASB functionalities can provide secure access for your workforce to the Internet and SaaS applications. Not all SASE solutions are created equal, so when evaluating a potential provider, be sure to look for these critical capabilities and features:

- Comprehensive SSL/TLS inspection across all traffic flows
- Vigilant malware scanning with real-time sandboxing
- Precise URL and content filtering guided by dynamic risk scores
- Robust data loss protection fortified by inline enforcement, enabling you to control downloads, uploads, copy/paste actions, and more

With a cloud-delivered SASE offering, IT and security teams can extend an optimal access experience to Internet and SaaS applications without compromising security. This is one of the many benefits of a unified SASE platform. (See Figure 3.)

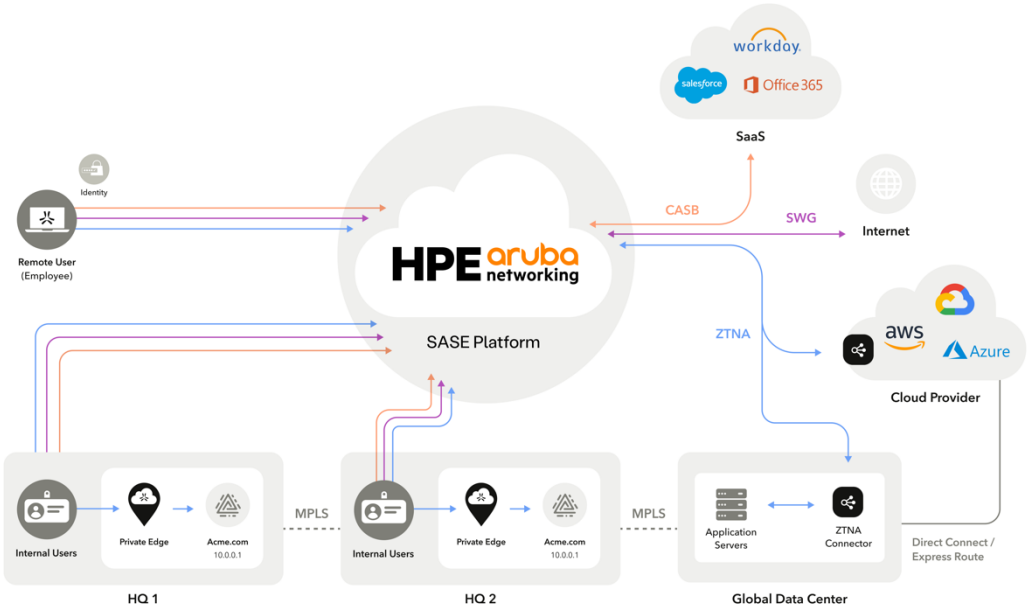


Figure 4. Zero Trust security for hybrid access

3. Secure hybrid work

As employees return to the office or work in a hybrid context, it is important that users receive the same Zero Trust standard and consistent access experience across all environments. As the workforce becomes more fluent across on and off-prem environments, certain access policies may need to be re-evaluated, such as traditionally blocked access to streaming audio, streaming video, and social media sites. Because employees may need to use these sites from their work devices to access resources while offsite, the challenge is enabling access in a secure manner regardless of their location.

To ensure secure access, provide all office locations with (guest) networks that only have Internet connectivity. This removes the risk of lateral movement of threats or the attack "blast radius" if the offices have network connectivity to data centers and other office locations, while still providing employees with the same experience. Plan to start reducing branch connectivity (discussed in the following sections) to make this a more permanent strategy. (See Figure 4.)

4. Mergers & acquisitions: Accelerate IT integration

In the rapidly evolving landscape of today's business environment, mergers and acquisitions (M&As) have garnered increasing traction as a means to expand a company's horizons, gaining entry into new markets and technologies. Despite the benefits that M&A deals offer, they often entail intricate processes that consume time and involve multiple stakeholders, all while navigating a landscape brimming with sensitive data.

Zero Trust Network Access (ZTNA), an integral component of the broader SASE architecture, emerges as a pivotal solution to streamline these complexities, rendering the process more efficient, less fraught with risk, and more cost-effective. ZTNA presents an elegant avenue to furnish Day 1 access to vital applications for users spanning both sides of the merger, all without necessitating the integration of networks or infrastructures. The cornerstone of this approach hinges on a prioritized list of Day 1 applications, encompassing critical functions such as HR, ERP, and various web-based tools that demand immediate accessibility.

A second critical facet involves establishing an identity strategy. This strategy is pivotal in ensuring that users can access these applications through robust authentication—even prior to the consolidation of directories, users, and groups stemming from the amalgamated organizations in the M&A scenario. To fulfill these imperatives, the chosen platform should offer seamless integration with multiple identity providers, thereby fulfilling the application access requirements for all user entities involved.

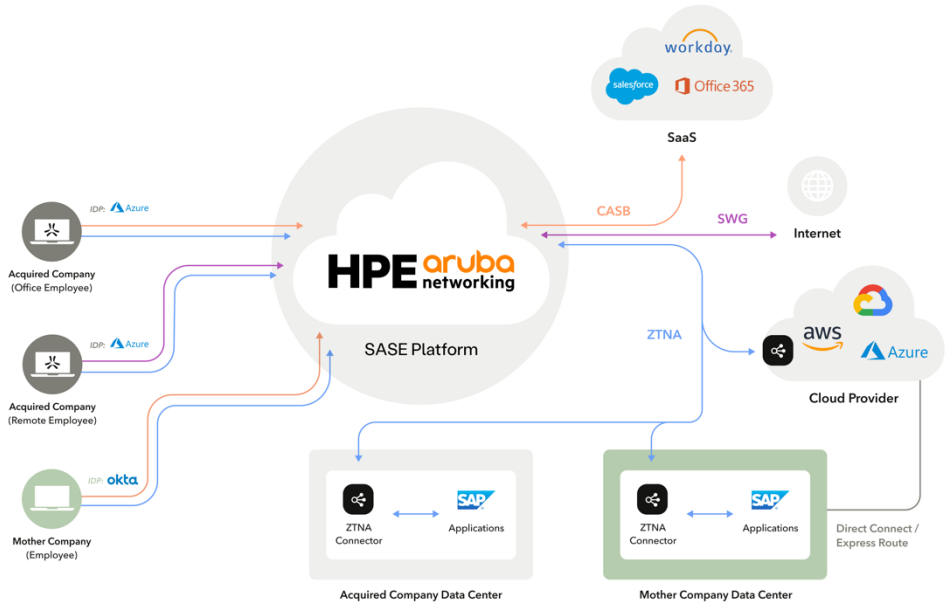


Figure 5. Streamline M&A integrations through ZTNA and SD-WAN

Additionally, company expansion (planned or unplanned) such as new branch locations, hybrid working, and mergers and acquisitions require IT to scale the enterprise WAN quickly and efficiently. A multi-fabric SD-WAN architecture allows organizations to simplify network management by enabling a single logical network to span multiple physical fabrics, including WAN, data center, and cloud environments. This enables companies to centralize network management, automate workflows, and streamline operations while delivering consistent and secure application performance and simplify the M&A IT implementation. (See Figure 5.)

5. Branch connectivity and improved security

Many branch offices rely on MPLS to connect their network to the headquarters. This architecture has become increasingly rigid as most business applications moved to the cloud. Directing all traffic to the data center for security inspection is no longer relevant because it negatively impacts application performance and increases security risks.

SD-WAN intelligently steers traffic to the cloud based on business and security policies—and with the flexibility to enable enterprises to continue to augment MPLS for mission-critical private data center-hosted applications with broadband. For example, trusted applications such as real-time video applications that require high bandwidth connectivity are directly routed to the cloud without further inspection. On the other hand, traffic from untrusted applications or applications with sensitive data are automatically routed to an SSE service to perform the necessary security controls.

SD-WAN also establishes end-to-end connectivity to the cloud by seamlessly integrating with cloud service providers such as AWS, Microsoft Azure, and Google Cloud—enabling multi-cloud and significantly improving application performance and security.

Secure SD-WAN integrates a next-generation firewall so that branch offices can reduce their hardware footprint by removing legacy firewalls as well as traditional routers and WAN optimization devices. Next-gen firewall capabilities also include fine-grained segmentation capabilities, enabling organizations to isolate IoT traffic from mission-critical applications while reducing the attack surface.

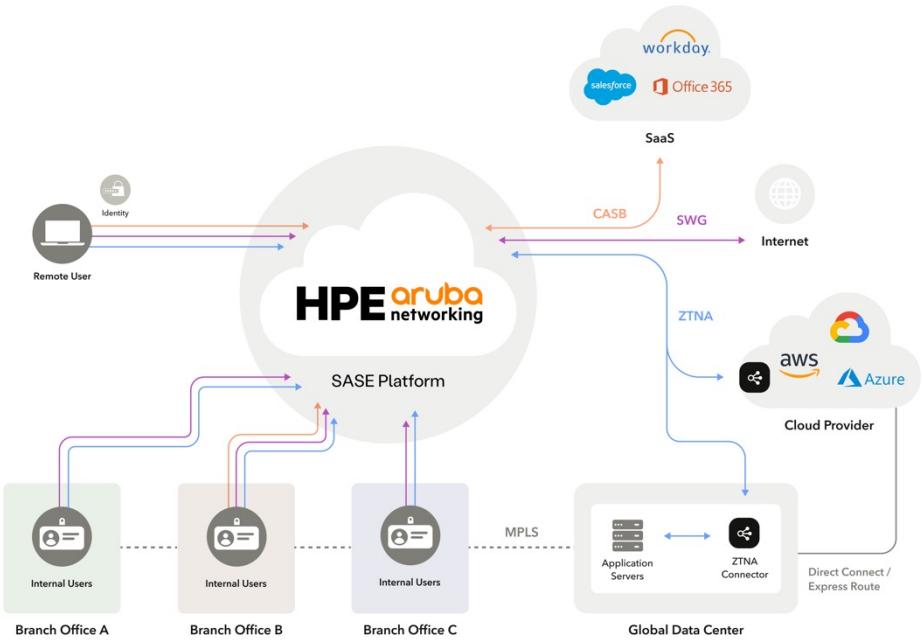


Figure 6. Secure branch and multi-cloud connectivity

Additionally, the proliferation of IoT devices connected to the network represents another security breach risk in offices because IoT devices have a simple design and cannot run a security agent. You need to find a way to isolate IoT traffic from mission-critical applications to safeguard your business. (See Figure 6.)

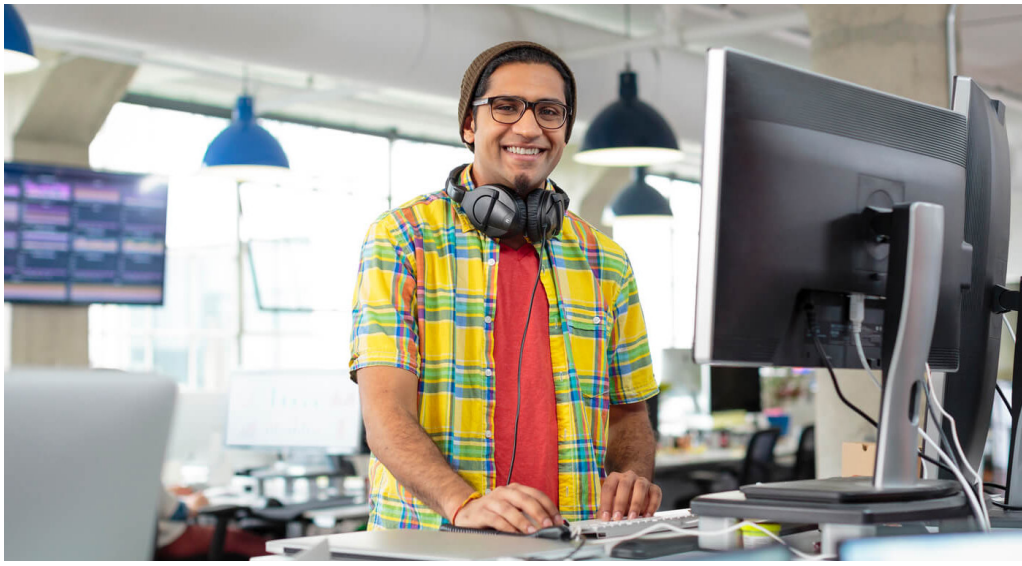
Recommendations for architects

Embarking on the SASE journey requires architects to think strategically. You can begin by conducting a comprehensive assessment of your existing architecture and identifying your critical applications, user behavior patterns, and high-risk security vulnerabilities. This groundwork not only serves as a compass, but it also illuminates the areas where SASE can have the most impact.

With this foundation established, the next step involves tailoring a SASE implementation that aligns with your specific organization's unique needs and objectives. It's important to look at the business risks, prioritize the applications and user groups that demand immediate attention, and craft a phased approach that balances security enhancements with operational continuity.

Moreover, crafting a clear roadmap that outlines key milestones and timelines is pivotal to the success of your SASE initiative. Engaging key stakeholders early in the process, including IT teams, security personnel, and business leaders, ensures that everyone is aligned with the overarching goals and benefits of integrating SASE principles into your network and security strategies.

This collaborative approach not only fosters a smooth transition, but it also enhances the likelihood of garnering support and resources as you navigate the dynamic landscape of modern security and networking challenges.



Summary

In the digitally transformed world, architects are the key to many network and security innovations realized by businesses today. Change is brought about by the architects who evolve with the business and explore new models, much like the SASE framework.

Through the architect's choice of solutions, a business can thrive with complementary security and networking functions, uncompromised security, simplified networking, enhanced user experience, and much more.

Consider what a unified SASE platform can do for your business. The HPE Aruba Networking team has experts who can help you on your SASE journey and show you where to start.

Start today

Try out our unified SASE solution with a 24-hour test drive at https://www.arubanetworks.com/sase-test-drive/.

Visit **ArubaNetworks.com**

Contact us, and we can build a plan together.

Contact us

Hewlett Packard Enterprise

a00134385ENW CT 091823