

Challenges of Traditional VPN and IP-VPN Connectivity and Their Replacement Using Secure Access Service Edge (SASE)

Abstract

This research analyzes the challenges associated with traditional Virtual Private Network (VPN) and IP-VPN architectures and examines the transition toward Secure Access Service Edge (SASE). A literature review of six academic and industry research papers is conducted. Each paper is analyzed in terms of research objectives, methodologies, and findings. The study also provides a critical evaluation of each work and identifies connections and differences between the research results. The findings indicate that traditional VPN and IP-VPN solutions face limitations related to scalability, performance, and security in cloud-centric environments. SASE architectures address these challenges by integrating networking and security services into a cloud-native platform using Zero Trust principles.

Keywords

VPN, IP-VPN, MPLS, SASE, Zero Trust Architecture, Network Security, SD-WAN

Introduction

Organizations have traditionally relied on Virtual Private Network (VPN) and IP-VPN technologies to enable secure communication between remote users, branch offices, and enterprise data centers. These technologies provide encrypted communication tunnels across public networks and service provider infrastructures. However, the rapid adoption of cloud computing, Software-as-a-Service applications, and remote work has exposed several limitations in these traditional network architectures.

Secure Access Service Edge (SASE) has emerged as a modern architecture designed to address these limitations by combining networking and security capabilities into a

cloud-based service model. This research reviews several relevant academic papers to evaluate how modern network architectures are evolving from traditional VPN models toward SASE-based solutions.

What Is VPN?

A virtual private network (VPN) establishes an encrypted connection between a user's device and a remote server. This connection enables secure data transmission over public networks, such as the internet, masking the user's IP address and safeguarding sensitive information from interception. Traditionally, VPNs have been used by businesses to allow remote employees to access internal resources as if they were on the corporate network, and by individuals to evade online censorship or secure their web browsing activities.

VPN protocols like OpenVPN, IPSec, and L2TP encapsulate user traffic and transmit it through an encrypted tunnel, providing confidentiality and integrity for data in transit. However, while VPNs offer a layer of protection against eavesdropping, they originate from a time when perimeter-based security was the norm and internal resources were tightly controlled. As organizations migrate to cloud-based infrastructure and users connect from diverse, distributed locations, the efficacy and suitability of traditional VPNs have come increasingly into question.

The difference between SASE and VPNs is that SASE provides a cloud-native platform combining networking and security services, while VPNs primarily focus on creating secure data transmission tunnels.

SASE extends the traditional network perimeter by merging SD-WAN with SWG, CASB, FWaaS, and ZTNA, ensuring secure access regardless of user location. VPNs secure the connection between the user and the network, typically without the additional, integrated security features that SASE offers.

Why Traditional VPNs Fall Short

1. Security Vulnerabilities and Exploits

VPNs create a wide network tunnel that, once accessed, can provide entry into the broader corporate network. This “castle-and-moat” approach assumes everyone inside the VPN is trustworthy, granting lateral movement to authenticated users. Attackers who compromise VPN credentials can exploit unrestricted access to internal systems, escalate privileges, and exfiltrate data without easily being detected.

Moreover, VPN servers themselves are popular targets for attackers. Vulnerabilities in VPN software or weak authentication mechanisms are routinely exploited in ransomware and advanced persistent threat campaigns. Despite security patches, managing distributed VPN endpoints and keeping them up to date is a logistical challenge, leaving many organizations exposed to known exploits or zero-day vulnerabilities.

2. Performance and Scalability Bottlenecks

Traditional VPNs route all traffic through centralized gateways, often causing congestion as more users connect remotely. This architecture introduces latency, degrading the user experience for cloud applications and real-time communications. Bandwidth constraints at the VPN concentrator can lead to slow file transfers and laggy video calls. Scalability is another challenge as organizations grow or shift to hybrid work models.

Adding capacity to handle more users or higher throughput typically requires costly hardware upgrades or complex reconfiguration. This increases operational overhead and poses challenges during peak usage, such as sudden increases in remote work or disaster recovery scenarios. The rigid, centralized nature of VPN infrastructure does not align well with modern, agile enterprise IT needs.

3. Privacy Shortcomings and Trust Issues

Although VPNs encrypt traffic from endpoint to gateway, they do not offer true end-to-end encryption. Once data reaches the VPN server, it is decrypted before being forwarded to its final destination, meaning sensitive information can be exposed if the server infrastructure is compromised. Additionally, the VPN provider itself (whether internal or third-party) can view traffic metadata and, depending on policies, even inspect unencrypted content.

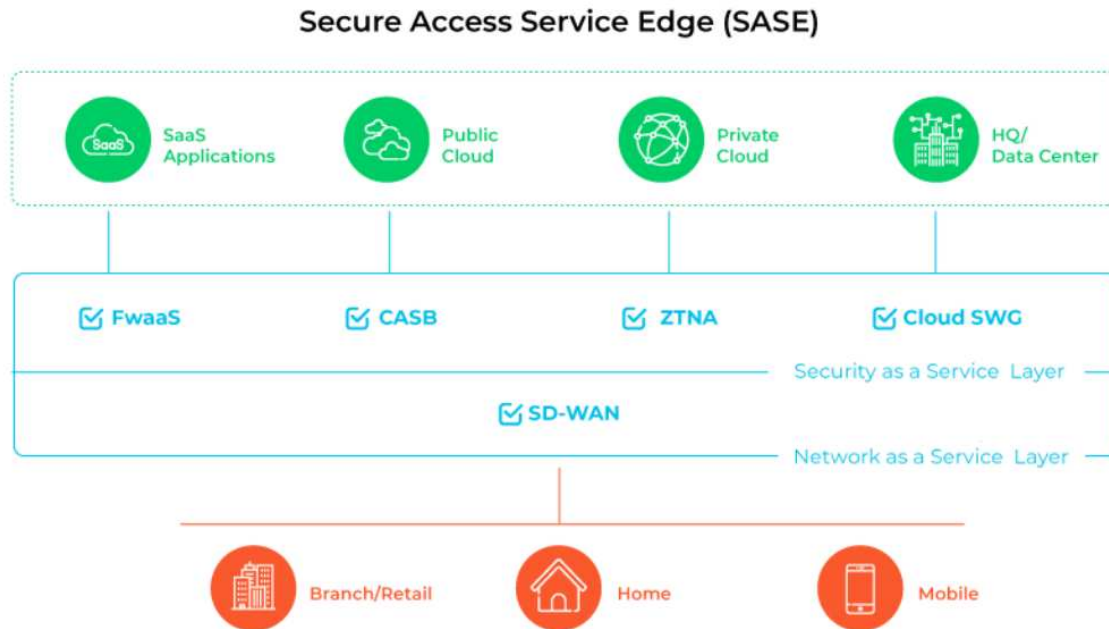
Trust is increasingly a concern as users and clients question who controls VPN servers and how privacy is maintained. Some consumer VPN services have faced scrutiny for logging activities or sharing user data with third parties. Within enterprises, reliance on a single point of trust can undermine compliance with data protection regulations, presenting legal and reputational risks in the event of a breach or misuse.

4. Limited Visibility and Endpoint Control

VPNs do not natively provide granular visibility into user activity or device posture. Administrators may see that a device is connected, but typically lack insight into its security health or what resources are being accessed. This blind spot makes it difficult to spot anomalous behavior, enforce least privilege policies, or respond quickly to compromised credentials.

Many VPN solutions are also platform-dependent, struggle with integration into modern device management frameworks, or lack the controls necessary to enforce security policies on mobile or unmanaged endpoints. As more devices connect from unmanaged home networks or public spaces, the inability to verify endpoint compliance creates new attack surfaces, further weakening security posture.

What Is SASE?



Secure access service edge (SASE) combines software-defined wide area networking (SD-WAN) and multiple security solutions like secure web gateway (SWG), cloud access security broker (CASB), firewall as a service (FWaaS), and zero trust network access (ZTNA) within a single cloud-delivered platform. Orchestrating various security and networking elements, SASE secures connections, streamlines security management, and supports a business's evolving network demands.

Addressing modern secure connectivity needs, SASE broadens the network perimeter to all points of entry, facilitating safe, effective cloud engagement for users everywhere.

SASE channels traffic via a cloud-centric service platform, integrating security and networking functions. Positioned at the edge, these services reduce latency, enhance performance, and centralize the enforcement of security policies. This streamlines operations throughout the organization.

By consolidating networking and security functions into a single, cloud-delivered service, SASE simplifies network management and enhances security.

The architecture supports the dynamic needs of modern organizations by providing scalable, unified access and protection for distributed environments.

Why do businesses today need SASE?

Businesses today are navigating a very different landscape from the traditional, centralized IT environments of the past.

That's why the secure access service edge (SASE) framework has emerged: to solve for modern security and connectivity demands.

Here's why businesses need SASE now more than ever:

Secure access service edge responds to the decentralization brought on by increased cloud adoption, mobile access, and remote working.

This shift means that both data and users are no longer confined to the office. Which has rendered traditional perimeter-based security models less effective.

How SASE resolves modern security and connectivity challenges



References

- [SASE vs. VPN: What Is the Difference? - Palo Alto Networks](#)
- <https://seraphicsecurity.com/learn/sase/vpn-replacement-why-vpn-falls-short-and-7-vpn-alternatives/>
- [Why Traditional VPNs Are Being Replaced by SASE | Fortinet](#)

Mohammed Aljaaidi,,