

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

Problem statement:

Traditional VPN and IP-VPN/MPLS architectures were designed for a perimeter-centric, site-to-site enterprise model. As enterprises adopt cloud services and support a growing mobile and remote workforce, these legacy architectures exhibit critical shortcomings: traffic backhaul to central hubs causes increased latency and degraded application performance for cloud access; policy and route management scale poorly leading to operational complexity; and perimeter-based security models inadequately address identity-centric and cloud-native threats. Moreover, migrating from MPLS/IP-VPN to modern architectures creates transition costs and operational challenges for organizations.

These limitations have practical consequences: poor user experience for cloud and real-time applications, higher operational expenditure due to policy sprawl and manual management, and potential security gaps that can be exploited by attackers leveraging lateral movement and cloud misconfigurations. Given the increasing reliance on SaaS and remote work, resolving these connectivity and security gaps is critical to business continuity, user productivity, and regulatory compliance.

Although SASE promises to converge SD-WAN and cloud-delivered security to address these issues, its real-world effectiveness varies with provider PoP geography, vendor backbone quality, and organizational readiness.

continuing use or modernization of MPLS/IP-VPN with SD-WAN overlays to optimize routing; deploying client VPNs with enhanced endpoint security; and adopting SASE platforms that integrate SD-WAN, Zero Trust Network Access (ZTNA), Cloud Access Security Broker (CASB), Secure Web Gateway (SWG), and Firewall as a Service (FWaaS) in a cloud-delivered manner (Gartner, 2019; Zhang et al., 2021). Case studies show hybrid migration strategies (SD-WAN + SASE pilot) as common practice.

Justify the need for research

Despite vendor claims showing SASE benefits (reduced latency to cloud, consolidated policies, improved threat inspection, there remain gaps in knowledge

- 1- long-term, multi-vendor comparative evaluations of performance and security.
- 2- standardized migration frameworks that quantify TCO, operational risk, and user experience across diverse enterprise topologies
- 3- comprehensive threat assessments considering centralization and supply-chain risks introduced by SASE. Research is needed to produce evidence-based guidance for enterprises deciding whether, when, and how to migrate from traditional VPN/IP-VPN to SASE architectures

Research objectives

To evaluate whether SASE architectures can effectively and reliably address the performance, operational, and security challenges of traditional VPN and IP-VPN connectivity in cloud-centric enterprise environments, and to produce practical migration guidance for organizations.

1. To characterize and quantify the primary performance limitations (latency, throughput, jitter) of traditional VPN and IP-VPN/MPLS architectures for cloud and SaaS access under representative enterprise workloads.
2. To measure and compare the performance of representative SASE implementations against traditional VPN/IP-VPN solutions across varied geographic PoP distributions and workload types.
3. To analyze the operational impacts of migrating from MPLS/IP-VPN to SASE, including changes in policy management complexity, transition costs (CapEx/OpEx), and required organizational processes.
4. To evaluate the security posture differences between VPN/IP-VPN and SASE architectures using threat modeling and controlled red-team simulations, including an assessment of new centralization risks and mitigation strategies.
5. To develop a decision framework and step-wise migration roadmap (including pilot selection, hybrid operation strategies, and KPIs) that enterprises can use to assess readiness for SASE adoption and to plan optimal transitions.

Alignment of objectives with problem statement

- Objectives 1 and 2 directly target the documented performance problems (backhaul latency, cloud access degradation).
- Objective 3 addresses the operational and cost issues raised by migration challenges.
- Objective 4 responds to the security significance and the need to understand centralized risks.
- Objective 5 translates research findings into practical migration guidance to reduce organizational risk.

References

- Zero Trust VPN (ZT-VPN): A Systematic Literature Review and Cybersecurity Framework for Hybrid and Remote Work
https://www.researchgate.net/publication/385892360_Zero_Trust_VPN_ZT-VPN_A_Systematic_Literature_Review_and_Cybersecurity_Framework_for_Hybrid_and_Remote_Work
- SASE vs VPN: Scalability, Performance, and Security
<https://www.tufin.com/blog/sase-vs-vpn>
- SASE vs VPN – architecture and performance differences
<https://www.paloaltonetworks.sg/cyberpedia/sase-vs-vpn>
- Rajamohan(2014)- Performance Analysis and Special Issues of VPN Technologies in Communication: Trusted VPNs, Secure VPNs and Hybrid VPNs
(PDF) [Performance Analysis and Special Issues of VPN Technologies in Communication: Trusted VPNs, Secure VPNs and Hybrid VPNs](#)
- Mikhail Bragin(2021)- The challenges of traditional corporate VPNs – And how to overcome them
[The challenges of traditional corporate VPNs – And how to overcome them | Netbird](#)