

Transitioning from Traditional VPN/MPLS to Secure Access Service Edge (SASE)

Table of Contents

Chapter 1:

- Abstract	3
- Introduction	3
- Background.....	4
- Problem Statement.....	5
- Research Objectives.....	5
- Research Scope.....	6

Chapter 2:

- Literature Review	7
• Evaluation of Traditional Architectures	7
• SASE and Zero Trust Convergence	7
• Critical Analysis of Migration Gaps	7

Chapter 3:

- Research Methodology	8
• Phase 1: Systematic Literature Review	8
• Phase 2: Qualitative Research.....	8
• Phase 3: Quantitative Performance Testing.....	8
• Phase 4: Framework Development & Validation.....	8
- Expected Outcomes.....	8
- Ethical Considerations and limitations	9
- Gantt Chart.....	10
- References	11

Abstract

The rapid integration of cloud-native technologies into enterprise sectors underscores an emergent need the establishment of efficient, secure connectivity that transcends traditional boundaries. This research examines the multifaceted nature of transitioning from perimeter centric networking specifically VPN and MPLS to Secure Access Service Edge (SASE). Drawing on a mixed methods approach that combines a systematic literature review, performance benchmarking, and threat modeling, this study aims to dissect the complex relationship between network performance and cloud-delivered security. The principal contribution of this work is the development of a novel migration framework designed to enhance organizational readiness and trust in SASE deployments. Additionally, the research provides a comprehensive assessment of SASE's potential impact on business continuity and user productivity.

Keywords: - Secure Access Service Edge (SASE), VPN, MPLS, Zero Trust, Cloud Security Framework, Migration Strategy.

Introduction

In an era where digital services seamlessly integrate into every facet of enterprise life from remote collaboration to cloud-hosted databases enterprise networks have reached a critical turning point. Traditionally, these networks relied on site-to-site VPN and MPLS/IP-VPN connections to provide secure access to corporate applications and data centers. These architectures were highly effective when applications resided within centralized data centers and users primarily operated from fixed office locations. However, the rise of cloud services, Software-as-a-Service (SaaS), remote work, and distributed applications has created new, rigorous requirements for network performance, security, and scalability that legacy systems were not designed to meet.

The promise of Secure Access Service Edge (SASE) to enhance efficiency and security in this new landscape is undeniable, yet the accelerated shift away from traditional hardware-bound perimeters brings forth critical challenges. Legacy VPN and IP-VPN infrastructures introduce significant performance degradation due to centralized traffic backhaul, limited scalability, and increased management complexity. Furthermore, perimeter-based security models are no longer sufficient in addressing identity-driven attacks, cloud-native threats, and modern security risks.

Despite the emergence of SASE as a converged framework integrating SD-WAN and cloud-delivered security services, trust in modern networking is often compromised by a deep-seated reliance on legacy "black-box" systems, issues of transparency, and fragmented security policies. There remains a significant lack of standardized migration frameworks to

guide this transition. Consequently, this research seeks to address the gap between current legacy capabilities and the organizational need for transparent, ethical, and trustworthy cloud-native systems by providing evidence-based guidance for the migration to SASE architectures.

Background

For decades, Multi-Protocol Label Switching (MPLS) and Virtual Private Networks (VPNs) served as the industry standard for secure enterprise connectivity. Traditional VPN and MPLS/IP-VPN networks were designed around a perimeter-based security model, where traffic is routed through centralized hubs for inspection and policy enforcement. While effective in earlier enterprise environments where applications resided within centralized data centers, this "castle-and-moat" model introduces significant inefficiencies for modern, cloud first enterprises.

As cloud applications and AI-driven services proliferate, they bring to light critical issues related to traffic "hairpinning" where cloud bound traffic is routed back to a central hub before reaching its destination causing increased latency and degraded performance. Furthermore, traditional routing often suffers from a "black-box" problem, where network behavior becomes difficult to predict, understand, or scale in a distributed context.

Secure Access Service Edge (SASE) represents a significant evolution in networking, fueled by breakthroughs in cloud-delivered security and software-defined WAN (SD-WAN). SASE addresses legacy limitations by integrating SD-WAN, Zero Trust Network Access (ZTNA), Cloud Access Security Broker (CASB), Secure Web Gateway (SWG), and Firewall as a Service (FWaaS) into a unified, scalable, and cloud-delivered framework. This convergence allows organizations to move away from hardware-bound perimeters toward a more transparent and agile architecture suited for the modern remote workforce.

Problem Statement

Traditional VPN and IP-VPN/MPLS architectures were designed for a perimeter-centric, site-to-site model. In the evolving landscape of cloud services, the black-box nature of these advanced legacy models poses significant challenges in ensuring accountability and efficient decision-making. Specifically:

- **Performance:** Traffic backhaul to central hubs causes increased latency and degraded application performance.
- **Operational Complexity:** Policy and route management scale poorly, leading to policy sprawl and manual management.
- **Security Gaps:** Perimeter-based models inadequately address identity-centric threats and allow for lateral movement by attackers.
- **Transition Risks:** Migrating creates significant transition costs and operational risks that often hinder widespread adoption.

These limitations negatively impact user experience, increase operational costs, and introduce security vulnerabilities. Although SASE aims to resolve these challenges, its effectiveness depends on provider infrastructure, organizational readiness, and implementation strategy. There remains a need for research into comparative performance, security posture, and migration frameworks.

Research Objectives

The main objective is to evaluate whether SASE can effectively address the performance, operational, and security challenges of traditional VPN and IP-VPN connectivity.

1. **Analyze Existing Challenges:** To comprehensively analyze and quantify the primary performance limitations (latency, throughput, jitter) of traditional VPN and IP-VPN/MPLS architectures.
2. **Analyze Operational Impacts:** To examine the impact of migration on policy complexity, transition costs (CapEx/OpEx), and required organizational processes.
3. **Evaluate SASE Solutions:** To critically assess the strengths and weaknesses of representative SASE implementations compared to legacy solutions across varied geographic PoP distributions.

4. **Propose a Robust Framework:** To develop a comprehensive framework for enhancing trust and efficiency in the SASE migration process.
5. **Validate Methodology:** To evaluate the security posture differences between architectures using red-team simulations and validate the framework in diverse application domains.
6. **Provide Implementation Guidance:** To offer actionable guidance for organizations, policymakers, and developers to integrate SASE effectively.

Research Scope

This research focuses on identifying and understanding key issues hindering trust and efficiency in enterprise networking, with emphasis on cloud-centric environments. It explores existing solutions, including SD-WAN, ZTNA, CASB, and FWaaS. The scope includes proposing a novel framework that integrates insights from these evaluations to offer practical migration guidelines.

- **Challenge Identification:** Concentrating on identifying issues that currently hinder trust and performance in enterprise networking, particularly in high-stakes domains.
- **Technical Evaluation:** Exploring existing SASE components including SD-WAN, ZTNA, CASB, SWG, and FWaaS.
- **Framework Development:** Proposing a novel framework that integrates technical performance data with ethical and operational guidelines.
- **Stakeholder Feedback:** Seeking validation from a range of stakeholders, including network developers, IT managers, and security experts.

Literature Review

Existing literature highlights the growing need to replace or augment traditional VPN architecture. Studies indicate that VPN backhauling causes increased latency and reduces cloud performance. Research shows that SASE offers benefits through distributed points of presence, integrated security, and identity-based access control.

Key findings c include:

1. Evaluation of Traditional Architectures

- Traditional VPN models suffer from performance bottlenecks.

2. SASE and Zero Trust Convergence

- Studies suggest that AI-driven networking can significantly contribute to resource management efficiency. The concept of "Trustworthy Networking" is proposed to be based on foundational principles: beneficence, non-maleficence, autonomy, fairness, and explicability.
- Literature underscores SASE's potential to enhance logical reasoning in traffic routing, possibly surpassing the capabilities of hardware-defined perimeters.
- Studies suggest that cloud-native networking significantly contributes to resource management efficiency and facilitates cross-sector collaborations.

3. Critical Analysis of Migration Gaps

Despite vendor claims of consolidated policies and improved threat inspection, significant gaps in knowledge remain:

1. A lack of long-term, multi-vendor comparative evaluations of performance and security.
2. The absence of standardized migration frameworks that quantify TCO and user experience across diverse topologies.
3. Insufficient comprehensive threat assessments regarding the centralization and supply-chain risks introduced by cloud-delivered SASE.

Research Methodology

The study adopts a structured mixed-method research approach integrating quantitative network performance testing, qualitative operational analysis, and controlled cybersecurity assessment. This ensures comprehensive evaluation aligned with enterprise deployment scenarios.

- **Phase 1: Systematic Literature Review**

Identifying and synthesizing existing research on trust, performance, and transparency in cloud-native networking.

- **Phase 2: Qualitative Research:**

Semi-structured interviews with a purposive sample of network architects and security ethicists to understand perceptions of trust and transparency.

- **Phase 3: Quantitative Performance Testing:**

Technical benchmarking of network performance (latency/jitter) and statistical analysis of survey data from IT professionals. And utilizing simulated environments and surveys to assess the prevalence of performance bottlenecks and evaluate the effectiveness of SASE solutions.

- **Phase 4: Framework Development & Validation:**

Integration of insights into a novel framework, followed by pilot testing in real-world enterprise environments, validated through expert reviews.

Expected Outcomes

The expected outcomes of this research aim to bridge the gap between technical performance and organizational trust during the transition to cloud-native architectures.

The research is expected to produce:

- **Comprehensive Analysis of Challenges:** A detailed examination of the multifaceted nature of trust and performance barriers in modern networking, specifically focusing on the limitations of current enterprise architectures.
- **Quantitative Benchmarking and Evaluation:** An assessment of current methodologies uncovering gaps in scalability and applicability through quantitative benchmarking results comparing VPN, IP-VPN, and SASE architectures. This

includes the identification of performance trade-offs under diverse cloud workloads.

- **Validated Security and Risk Assessment:** The development of a validated security risk assessment framework and threat model that addresses both legacy vulnerabilities and new centralization or supply-chain risks introduced by SASE.
- **Operational and Cost Analysis:** A comprehensive comparison of operational costs (CapEx/OpEx) and management complexity to support data-driven decision-making.
- **Innovative Migration Framework:** The formulation of a structured migration framework and decision model providing actionable guidelines for implementing trustworthy SASE practices. This approach balances technical advancement with ethical responsibility to ensure a reliable transition.
- **Industry and Academic Contribution:** Enrichment of academic and industry discourse by establishing best practices in enterprise network transformation and promoting collaborative efforts toward more transparent and ethical networking systems.

Ethical Considerations & Limitations

Ethical considerations include obtaining informed consent and ensuring confidentiality for all interview and survey participants. Limitations include the representativeness of qualitative samples and the rapid pace of technological development which may outstrip current regulations.

Gantt Chart

Activity	Start Date	Duration	Month 1	Month 2	Month 3	Month 4	Month 5	Month 6
Literature Review	01/09/2026	30 days						
Develop Methodology	16/10/2026	16 days						
Data Collection	01/11/2026	61 days						
Data Analysis	01/01/2027	31 days						
Framework Development	01/02/2027	28 days						
Final Submission	01/05/2027	15 days						

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](#)