

Challenges of Interconnecting Multiple Networks: A Comparative Study Between VPN and SD-WAN Solutions and Their Impact on Performance and Security

Fatimatulzahraa Ihsan Mohsen
University of Babylon

Article Info	ABSTRACT
<p>Article history: Received Sept. 01, 2025 Revised Nov., 20, 2025 Accepted Dec., 10, 2025</p> <p>Keywords: SD-WAN, VPN, Network Interconnection, Security, MPLS.</p>	<p>With the arrival of technological time, connection on the Internet has become inevitable.</p> <p>Many networks can be a challenging question when it comes to protests as well as security issues. Virtual private networks (VPN) have been used to provide safe channels for connection, but are surrounded by delay and scalability. On the other hand, software-defined wide area networks (SD-WAN) have been an alternative with customized routing, dynamic bandwidth distribution and underlying safety facilities. We analyze VPN and SD-WAN solutions when it comes to safety and performance in this article. Our findings indicate that although VPN is heavily encrypted, it will not avoid heavy load tests. The SD-WAN solution is still better in terms of performance and uses a new security mechanism, and that's why an appropriate replacement.</p>
<p>Corresponding Author: Fatimatulzahraa Ihsan Mohsen University of Babylon Baghdad, Iraq Email: fatimaalzahraa9313@gmail.com</p>	

1 Introduction

With the increasing dynamic digital age of today, most businesses depend upon the connectivity of more than one distributed network for communication, resource sharing, and efficient management of more than one place. Therefore, such requirements made it necessary to interconnect networks with greater efficiency and security [1]. Secure data transport in public networks that the Internet has existed in the form of the virtual private network (VPN) for decades. A positive aspect of VPN is that they are quite easy to install in external offices and the cloud computing environment when building safe tunnels that ensure data security and accuracy [2]. But VPN is slow and cumbersome to search large companies because of the stable timetables that end to encrypt and decrypt information. This introduces additional delays and wastage of bandwidth. In addition, working with multiple VPN connections can be hard and resource-intensive [3]. To face these limitations, a networking technology called Software-Defined Wide Area Network (SD-WAN) was created to link several branch offices and data centers across wide regions. SD-WAN uses overlay network to provide central management and control, and can enhance network performance by using multiple connection types (LTE, MPLS, broadband), and dynamic routing along the best path [3]. There is still ongoing research on performance and security of SD-WAN technology. Although a lot of research has looked at VPN scalability and security or SD-WAN optimization separately, there isn't a thorough analysis that looks at how well they link several networks at once. In this paper, we compare VPN and SD-WAN solutions in terms of performance and security in complex, multi-network environments. We will analyze bandwidth, latency, packet loss, and measure security metrics, including encryption and threat mitigation capabilities. Our paper is organized as follows: In Section 1 we gave an introduction of the topic. Section 2 contains background knowledge about VPN

and SD-WAN. In section 3 we define our method for comparing the two solutions. Section 4 provides experimental details in terms of performance and security. In section 5 and 6 we discuss the differences and highlight the major features of each method. Finally, we conclude our research in Section 7.

2 Literature Review

Virtual Private Networks (VPNs)

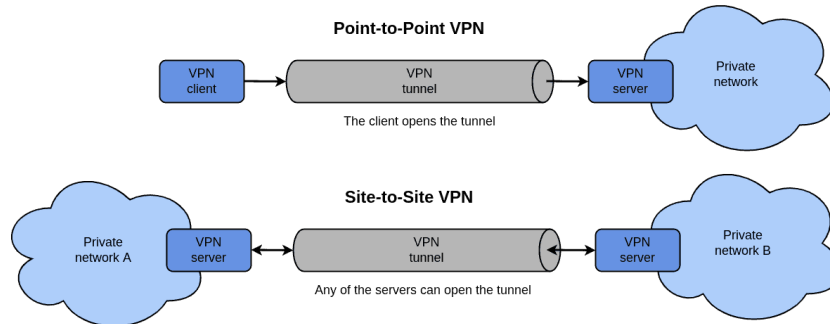


Figure 1: Virtual Private Networks Architecture.

Existing research on Virtual Private Network (VPN) solutions extensively highlights both performance and security challenges. If a host wishes to connect to a private LAN network remotely over the internet, a virtual private network (VPN) is a network solution. VPNs employ a method that typically entails building a tunnel with two exits: one at the host station and one at the private company network (alternative configurations are also possible). A VPN protocol, such as IPsec or WireGuard, is used to build the tunnel. To ensure security and integrity of data, all communication passing through the tunnel is encrypted and hashed. In addition, VPNs use login credentials as an authentication system. This process can make the network slow, and lossy, and not scalable. Moreover, management of VPN networks requires manual configuration of multiple point-to-point connections. In terms of security, VPNs use strong encryption standards such as (AES-256, IPsec) protocols. However, these protocols also have security flaws and they cannot adapt to traffic patterns. For example, if appropriate endpoint controls are not in place, VPNs may let harmful software to spread from user devices into corporate networks [2].

Software-Defined Wide Area Networks (SD-WANs)

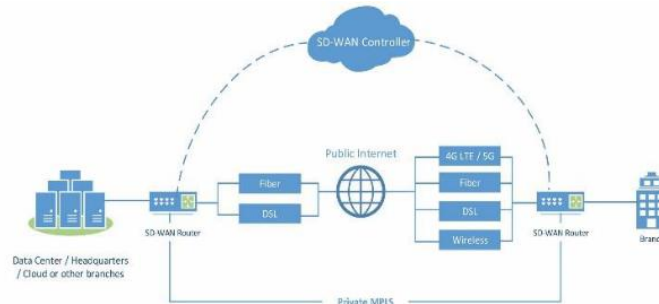


Figure 2: SD-WAN Architecture.

Software defined wide area Network (SD-WAN) is a network method that organizations can network and manage branch offices in large geographical areas along with many data centers. Together with SD-WAN, a virtual overlay network is created to offer centralized control and control, as well as equipped with support for the underlying physical infrastructure. SD-WAN improved the performance and safety of more than one connection types, including broadband, long-term development (LTE) and MPLS, and dynamic routing of traffic with the best path. By simplifying network operations, it can automate network policies and settings and provide visibility and control over all connected devices and applications [3]. SD-WAN research has delayed the benefits of companies with more networks, such as better performance, centralized management and flexibility.

SD-WAN balances the bandwidth and decreases the latency through a double-level design, which is based on an overlay (software-defined virtual network) and a substrate (private lines and physical lines). Using this approach, the Dynamic network has the ability to select the path of routing that ensures user experience and provides more management options. Furthermore, SD-WAN applies mechanisms like division, politics enforcement and firewalls in order to enhance security services [4].

In contrast, SD-Wan has to satisfy requirements such as:

- 1- Reliance on public internet access that is insecure for bandwidth variation and latency increases.
- 2- Intervals of deployment possibility.
- 3- Additional difficulties in managing security policy properly on dispersed websites [5].

Comparative research on SD-WAN and VPN discusses how SD-WAN offers better performance through offering centralized control that enhances monitoring and troubleshooting processes and dynamics. While observing the current literature, we noticed a research gap in thorough, integrated analysis between VPN and SD-WAN in terms of performance and security. Few studies compare their performance and security, with the majority of studies focusing on one type of networks.

3 Methodology

This section explains the research approach to compare between the two networks. It involves security and performance evaluation measures and shows the data sources used while in comparative studies.

Research Approach

To simulate the actual business settings, research design included a broad field -tested experiments in the false network environment with geographically scattered places associated with the network (WAN). Serious results were supplemented and the existing academic works and learning from the industry WhitePaper were cross -checked along with learning from Whitepaper.

Evaluation Criteria

The solutions were assessed based on the following key criteria:

- **Performance Metrics:** To compare the performance of our two networks, we measured latency reduction, jitter, cost efficiency, scalability, traffic isolation, and policy enforcement. Jitter can be calculated as follows:

$$Jitter_{Delay var} = \frac{\sum variation delay}{\sum packets recieved} \dots \dots \dots (1)$$

- **Security Metrics:** On measurement of safety, we computed breach of security policy, hazards, match points, vulnerable repair time and unauthorized access attempts.

Data Sources

- **Experimental testing:** Installation of VPN and SD-Van was mimicked with the network simulator and traffic generators to allow real-time measurement of throws, delay, package loss and wrong activity, such as a decrease or audience under stressful conditions.
- **Safety analysis:** Each network category was tested through encryption performance, firewall integration and partition options through vulnerable scanning and simulation of scanning and penetration.

- **Secondary data:** To provide even more generality, industry reports, publications of colleague assessment and additional performance and security information provided by supplier White Papers.

4 Performance Analysis

Table 1: Comparative Numerical Analysis of VPN and SD-WAN Performance Metrics [6].

Metric	VPN	SD-WAN
Latency	70 – 90 ms (office hours, due to encryption & fixed routing)	40 – 60 ms (off-peak); up to 80 – 100 ms during congestion
Jitter (Delay Variation)	2 – 4 ms (moderate, encryption adds micro-delays)	1 – 3 ms (off-peak); spikes to 5 – 8 ms at peak hours
Packet Loss	0.5 – 1%	0% off-peak; up to 3% during peak hours
Cost Efficiency	30 – 40% more expensive per Mbps (VPN/MPLS)	20 – 40% cost savings compared to VPN/MPLS
Scalability	Limited: $O(n^2)$ tunnel growth; high management overhead	High: centralized orchestration; 50 – 60% faster branch deployment
Traffic Isolation	Strong encryption (AES/IPsec protocols), but with no segmentation	Application-aware segmentation
Policy Enforcement	Static error-prone management	Centralized management

VPN uses the same method to anchor traffic between websites and building tunnels on public internet connections. Due to the overload and long -term data routes on the Internet, VPN usually suffers from delay, nervousness and package loss, which adversely affects performance. In addition, Overhead can associate with VPN encryption and decrypting procedures also reduce performance and introduce multiple delays, especially when working with large versions of data or long -distance connections [6]. On the other hand, SD-WAN has a better performance as it uses a double-list architecture, which includes an overlay software and a multi-connecting support network (MPLS, broadband, LTE) that helps choose the best way in real time. In addition, the quality of service (QOS) priority increases, dynamic road selection improves reliability and improves the user experience by optimizing bandwidth and reducing delay and package loss. Unlike VPNs, SD-WAN balances traffic at multiple links and can switch to backup ducts when they occur with package loss.

5 Security Analysis

Table 2: Comparative Analysis of VPN and SD-WAN Security Metrics.

Metric	VPNs	SD-WANs
Security Policy Violations	Higher due to decentralized policies	Lower with centralized policy enforcement
MTTD	Longer detection times	Shorter detection times with advanced analytics
Compliance Score	More challenging to maintain	Easier to maintain with built-in compliance features
Vulnerability Remediation Time	Longer without automation	Shorter with integrated vulnerability management
Unauthorized Access Attempts	Higher risk if not properly configured	Lower risk with advanced security features

Although VPN and SD-WAN use encrypted communication to protect both data, there are significant differences in their safety structures. To create a safe connection tunnel between endpoints, VPN uses strong encryption techniques such as IPSEC or SSL/TLS, which guarantees data integrity, but they do not describe network traffic patterns or application behavior. In addition, the VPN division is missing with tunnel channels; This closing point results in weaknesses, such as possible harmful software from distant users. These are considered the most important security threat to VPN. In addition, VPN -is dependent on external safety layers for safety and does not use the integrated danger or firewall functions [7]. In SD-Wan, these limits are fixed using integrated safety functions. To provide centralized policy enforcement and real-time traffic management, framework, SD-WAN segmentation, SACTE Access Service Edge (SASE), and uses the next generation firewall (NGFW). SD-WAN checks and the data separate the panels, which show better monitoring and deviations. However, this requires frequent upgrades to fix the new weaknesses initiated by new features and technologies.

6 Discussion

Companies have to be taken into account while planning interfacing multiple networks, which are subjected to VPN and SD-WAN solutions. Since SD-WAN uses more than one network roads and intelligent routing methods, SD-Wan performs much better than traditional VPN configurations. This allows SD-wise to adapt to the needs of fast, bandwidth consumption, which is currently safer to maintain with global companies. On the other hand, VPN is challenging with stable routing, and its one-trill encrypted tunnels introduced encryption overhead. They build over time and create poor user experiences. Our safety assessment indicates that VPN does not have the facilities found in centralized security administration and SD-W. Second, vulnerability and harmful software that can be promoted via VPN, the risk learning point for companies because they are unable to find partitions or exposure to the entire network. In contrast, SD-WAN, infiltration detection, next generation firewall and URL filtration provide more depth and dynamic network protection with new safety technologies such as firewall and URL filtering. However, SD-WAN presents additional operational problems and potential attack surfaces that require continuous policy control and safety monitoring due to its complexity and dependence on different types of connections. Companies must balance security and performance factors against costs and complexity. VPN is easy to install and they work well for small to medium -sized businesses. SD-WAN scalability provides flexibility and automation capacity, but they require a great investment and operational expertise.

7 Conclusion

This research compared the performance and security of SD-WAN and VPN. SD-WAN has advantages that reduce latency and increase reliability. VPN employs single-path, static tunnels, which may provide less performance. VPN provides encryption but does not leverage centralized control and threat detection. Although it does involve continued maintenance, SD-WAN features robust security functionalities, offering a more flexible and overall protection. While SD-WAN is preferable for large, sophisticated networks that require improved performance and security, VPNs are also appropriate for smaller or simpler installations. Future studies may examine AI-enhanced security frameworks and hybrid VPN-SD-WAN solutions. All things considered, SD-WAN is a major advancement in network connectivity and works better than standard VPNs to enable business digital transformation.


References

- [1] M. A. Ouamri, T. Alharbi, D. Singh, and Z. Sylia, *A comprehensive survey on software-defined wide area network (SD-WAN): principles, opportunities and future challenges*, vol. 81, no. 1. Springer US, 2025. doi: 10.1007/s11227-024-06718-1.
- [2] Sudipti Banerjee. and Dr. Rajni Ranjan Singh Makwana, “Virtual Private Network: Survey and Research Challenges,” *International Journal of Latest Technology in Engineering Management & Applied Science*, vol. 14, no. 6, pp. 211–226, 2025, doi: 10.51583/ijltemas.2025.140600028.
- [3] R. R. H. Amin and D. H. Ahmed, “Comparative Analysis of Flexiwan, OPNSense, and pfSense Cybersecurity Mechanisms in MPLS / SD-WAN Architectures,” *Passer Journal of Basic and Applied Sciences*, vol. 6, no. 1, pp. 27–32, 2024, doi: 10.24271/PSR.2023.390989.1295.
- [4] M. Shamshul and H. Omar, “Software Defined-Wide Area Network (SD- WAN) Security Solutions : A Comparative Study,” vol. 5, no. 8, pp. 463–480, 2023, doi: 10.35629/5252-0508463480.
- [5] E. Briefing, “Enterprise Networking Challenges : How Can Sd- Wan Help ?,” no. May, pp. 1–11, 2019.
- [6] O. Timilehin, “Performance Analysis of Voice Transmission Over IPsec-Enabled Communication Links,” no. November 2024, 2024, [Online]. Available: <https://www.researchgate.net/publication/388673601>
- [7] S. Yadav, “Master of Science in Internetworking Capstone Project Report SD-WAN service analysis, solution, and its applications,” 2021, [Online]. Available: <https://era.library.ualberta.ca/items/2613b784-8aa6-498c-accb-b8bb86462b58/view/3864f381-2d43-484b-9756-8b2a267cb2e2/Yadav.pdf>

BIOGRAPHIES OF AUTHORS

The recommended number of authors is at least 2. One of them as a corresponding author.

Please attach clear photo (3x4 cm) and vita. Example of biographies of authors:

	<p>and a Bachelor's degree in Computer Science from the University of Babylon. Gained professional experience working at Al-Zahraa University and Warith Al-Anbiyaa University in Karbala.</p> <p>Fluent in Arabic (native), with proficiency in English and Persian.</p> <p>Possesses strong technical skills in:</p> <ul style="list-style-type: none"> • Text processing, spreadsheets, and slide presentations. • Web design. • Programming languages: Python, C++, Matlab. <p>A responsible and organized individual, eager to enhance work experience and contribute effectively in the field of computer engineering.</p>
2 Author 2 picture	Mini cv
Author 3picture	Mini cv
Author 4 picture	Mini cv
Author 5picture	Mini cv