OKU Fen Bilimleri Enstitüsü Dergisi
8(3): 1353-1369, 2025

OKU Journal of The Institute of Science and Technology, 8(3): 1353-1369, 2025

Osmaniye Korkut Ata Üniversitesi
Fen Bilimleri Enstitüsü
Dergisi

Osmaniye Korkut Ata University
Journal of The Institute of
Science and Technology

Performance Evaluation of WireGuard and IPSec Protocols in Various Network Configurations

Tuğçe DEMİRDELEN[1*], Sefa KIRMIZI[2]

[1]Adana Alparslan Türkeş Science and Technology University, Faculty of Engineering, Department of Electrical and Electronics Engineering, Adana, Türkiye
[2]ULAK Haberleşme A.Ş. System Engineering, Ankara, Türkiye
[2]Adana Alparslan Türkeş Science and Technology University, Faculty of Engineering, Department of Electrical and Electronics Engineering, Adana, Türkiye

[1]https://orcid.org/0000-0002-1602-7262
[2]https://orcid.org/0009-0009-4510-507X
*Corresponding author: tdemirdelen@atu.edu.tr

Research Article

Article History:
Received: 18.03.2025
Accepted: 20.05.2025
Published online: 16.06.2025

Keywords:
VPN
WireGuard
IPSec
Throughput
CPU utilization
SD-WAN
Network performance
Information systems

ABSTRACT

This study aims to evaluate the performance of WireGuard and IPSec Virtual Private Network (VPN) protocols under various network configurations to determine their efficiency, reliability, and resource utilization in different scenarios. The configurations examined include Round Robin, IEEE 802.3ad bonding, single interface/single tunnel, dual interfaces/dual tunnels, and single interface/dual tunnels. Key performance metrics such as throughput and Central Processing Unit (CPU) utilization were analyzed to understand the impact of these protocols on network performance. The experimental results demonstrate that WireGuard outperforms IPSec in terms of throughput and CPU efficiency, showcasing lower overhead and improved speed, making it a more suitable option for high-performance and resource-constrained environments.Results indicate that WireGuard consistently delivers higher throughput and lower CPU utilization across these configurations, particularly excelling in multi-interface and load-balanced setups, thus making it a preferable choice for performance-critical environments..

WireGuard ve IPSec Protokollerinin Çeşitli Ağ Konfigürasyonlarında Performans Değerlendirmesi

Araştırma Makalesi

Makale Tarihçesi:
Geliş tarihi: 18.03.2025
Kabul tarihi:20.05.2025
Online Yayınlanma: 16.06.2025

***Anahtar** Kelimeler:*
VPN
WireGuard
IPSec
Veri aktarım hızı
CPU kullanımı
SD-WAN
Ağ performansı
Bilgi sistemleri

ÖZ

Bu çalışma, farklı ağ konfigürasyonları altında WireGuard ve IPSec Sanal Özel Ağ (VPN) protokollerinin performansını değerlendirerek, verimliliklerini, güvenilirliklerini ve kaynak kullanımını belirlemeyi amaçlamaktadır. İncelenen konfigürasyonlar arasında Round Robin, IEEE 802.3ad bağlantı birleştirme, tek arayüz/tek tünel, çift arayüz/çift tünel ve tek arayüz/çift tünel bulunmaktadır. Bu protokollerin ağ performansı üzerindeki etkisini anlamak için veri aktarım hızı (throughput), CPU kullanımı gibi temel performans metrikleri analiz edilmiştir. Deneysel sonuçlar, WireGuard'ın veri aktarım hızı ve CPU verimliliği açısından IPSec'ten daha iyi performans gösterdiğini, daha düşük ek yük ve daha yüksek hız sunduğunu ortaya koymaktadır. Bu da onu yüksek performans gerektiren ve kaynakların sınırlı olduğu ortamlar için daha uygun bir seçenek haline getirmektedir. Sonuçlar ayrıca, incelenen farklı ağ konfigürasyonlarının performansa olan etkisini özetlemekte olup, WireGuard’ın özellikle çoklu arayüz ve yük dengeleme yöntemlerinde IPSec’e göre tutarlı şekilde daha yüksek veri aktarım hızına ve daha düşük CPU kullanımına sahip olduğunu göstermektedir.

To Cite: Demirdelen T., Kırmızı S. Performance Evaluation of WireGuard and IPSec Protocols in Various Network Configurations. Osmaniye Korkut Ata Üniversitesi Fen Bilimleri Enstitüsü Dergisi 2025; 8(3): 1353-1369.

1. Introduction

The growing demand for high-performance and secure communication in modern networking environments has made Virtual Private Network (VPN) solutions essential components of network security architectures. VPN tunnels play a fundamental role in information systems, providing secure data transmission and ensuring network reliability. Among various VPN protocols, WireGuard and IPSec have emerged as prominent solutions, each offering distinct advantages in terms of performance, security, and resource utilization. WireGuard is a relatively new and lightweight VPN protocol recognized for its streamlined design, robust cryptography, and superior performance compared to traditional solutions such as IPSec and OpenVPN. Conversely, IPSec continues to be widely adopted due to its robustness and compatibility with enterprise environments.

This paper provides a comprehensive evaluation of WireGuard and IPSec performance under different network bonding and tunneling configurations, particularly focusing on Software-Defined Wide Area Network (SD-WAN) deployments. VPN performance is critical to SD-WAN effectiveness, making protocol evaluation essential.

Previous comparative studies have highlighted the performance characteristics of WireGuard and IPSec. Donenfeld (2017) and Mackey et al. (2020) have emphasized WireGuard’s ability to deliver lower latency and reduced CPU consumption, especially under high-load scenarios. Dowling and Paterson (2018) and Yang et al. (2019) have demonstrated that WireGuard’s kernel-level integration significantly reduces overhead and improves packet processing compared to user-space implementations such as those examined by Narayan et al. (2009).

Although WireGuard is increasingly popular, IPSec remains a dominant protocol in enterprise environments due to its mature security framework, compatibility with existing infrastructure, and extensive support for diverse encryption and authentication methods. However, IPSec’s complexity, stemming from multiple encapsulation layers and complex key exchanges, increases computational overhead and can negatively affect performance, as indicated by studies including Abbas et al. (2023) and Shen et al. (2023).

Network bonding techniques significantly impact VPN efficiency. Different bonding methods, such as Round Robin, IEEE 802.3ad (Link Aggregation Control Protocol - LACP), and adaptive load balancing, can affect bandwidth distribution, latency, and failover efficiency (Gentile et al., 2024; Sharma et al., 2024). Additionally, the Maximum Transmission Unit (MTU) configuration notably influences VPN throughput. Incorrect MTU settings can cause fragmentation, increased latency, and reduced efficiency (Vilanova, 2021; Balachandran et al., 2024).

Moreover, WireGuard’s stateless architecture and use of ChaCha20 encryption contribute to its superior performance in cloud environments compared to IPSec, which typically uses AES encryption (Gentile et al., 2022). Nonetheless, IPSec’s robustness against cyber threats makes it suitable for mission-critical applications, despite performance drawbacks (Gordeychik and Kolegov, 2018).

Further research into VPN optimization indicates that protocol overhead significantly affects efficiency. Pries et al. (2008) concluded that WireGuard’s minimalistic design reduces handshake latency and session establishment times compared to IPSec. Mansouri et al. (2020) also explored hybrid VPN deployments, showing that combining WireGuard and IPSec can enhance security while maintaining high performance.

Real-world case studies highlight that VPN protocol choice significantly influences network stability and efficiency. Organizations using WireGuard in SD-WAN environments experienced reduced operational costs and better scalability compared to traditional IPSec deployments (Shen et al., 2023). Similarly, Ostroukh et al. (2024) identified performance bottlenecks in encrypted traffic, providing recommendations on MTU optimization and bonding strategies.

This paper makes a unique contribution by comparing WireGuard and IPSec under various bonding and tunneling configurations and provides practical deployment guidance for SD-WAN scenarios**.** By analyzing throughput and CPU utilization, this research offers practical insights into optimal VPN deployment strategies. The results assist network engineers, system administrators, and IT decision-makers in selecting the most efficient VPN protocol for specific use cases, balancing security, performance, and resource efficiency.

2. Material and Methods

2.1. Mathematical Model

A mathematical model for this study can be formulated to describe the relationships between throughput (T), CPU utilization (C), packet-per-second (PPS), and MTU (M) under different VPN protocols and bonding configurations. Below is a structured approach to modeling these interactions.

2.1.1. Throughput Model

The throughput T (Mbps) depends on MTU, packets per second (PPS), bonding factor, and protocol efficiency, as expressed in Equation (1):

$$T = \frac{\eta \cdot P \cdot M \cdot B}{E} \tag{1}$$

Equation 1 shows the relationship where P represents the Packets Per Second (PPS), M is the MTU in bytes, B is the bonding configuration factor, and E is the encryption overhead factor, which varies based on the protocol used (WireGuard or IPSec). The bonding factor B changes depending on the strategy, with a single interface having B=1, round-robin bonding B=1.5, IEEE 802.3ad (LACP) B=1.8 due to load balancing improvements, and a dual interface/dual tunnel setup B=2. The overhead introduced by encryption and packet handling, denoted as O, is given by:

$$O = E \cdot (1 - \eta) \cdot P \tag{2}$$

where E is the encryption overhead factor, which is higher for IPSec due to additional encapsulation layers like ESP and IKE negotiations, making EIPSec>EWireGuard.

2.1.2. CPU Utilization Model

CPU utilization (%) C is primarily affected by encryption overhead O, the number of active interfaces N, and the protocol efficiency η:

$$C = \frac{P \times E \times N}{\eta} \tag{3}$$

As shown in Equation 2, Since WireGuard operates in kernel space while IPSec partially operates in user space, their efficiency factors differ. WireGuard has an efficiency range of η=0.85−0.95, while IPSec, due to its more complex encryption and multiple encapsulation layers, has a lower efficiency of η=0.65−0.80. Consequently, IPSec requires more CPU resources to achieve the same throughput compared to WireGuard.

2.1.3. Packet Processing Model (PPS)

The packet-per-second rate is defined by:

$$P = \frac{T.\gamma}{M} \tag{4}$$

Equation 3 indicates that Since VPN protocols process packets at different rates due to encapsulation overhead, an encapsulation efficiency factor γ is introduced, where:

where VPN protocols handle packets at different rates due to encapsulation overhead. The encapsulation efficiency factor γ\gammaγ varies between protocols, with WireGuard achieving γ=0.9 due to its lightweight design, while IPSec, burdened by additional ESP headers and rekeying processes, has a lower efficiency of γ=0.75.

2.2. Performance Analysis

Each test utilized iPerf3, a widely recognized network performance measurement tool, to assess throughput and CPU utilization. Tests were conducted with both single-session and 20 parallel TCP sessions using iPerf3. Each run lasted 30 seconds to ensure stability and reproducibility. CPU utilization was monitored in real time using htop throughout each test session. All VPN tunnels were created with default encryption and authentication settings, without manual tuning.

Table 1. Assumed protocol parameters for WireGuard and IPSec

Variable	Description	Units / Values
T	Throughput	Mbps
P	Packets per second	PPS
M	Maximum Transmission Unit	Bytes
B	Bonding configuration factor	1 (Single), 1.5 (RR), 1.8 (802.3ad), dual interface/dual tunnel B=2
E	Encryption overhead factor	High (IPSec), Low (WireGuard)
O	Overhead introduced by encryption	—
C	CPU utilization	Percentage (%)
η (eta)	Protocol efficiency	0.65–0.80 (IPSec), 0.85–0.95 (WireGuard)
γ (gamma)	Encapsulation efficiency (only in PPS model)	0.75 (IPSec), 0.90 (WireGuard)
N	Number of active interfaces	1 or 2

2.2.1. Test Setup and Environment

All experiments were conducted using standardized hardware platforms to eliminate variability in results due to hardware differences. The testbed consisted of:

Table 2. System requirements

Component	Specification
Processor	Multi-core high-performance server-grade CPUs
Memory	16 GB RAM or higher
Network Interfaces	Gigabit Ethernet
Operating System	Debian-based Linux distribution, optimized for VPN performance
VPN Implementations	WireGuard (kernel-based) and IPSec (Libreswan/StrongSwan implementations)

All VPN configurations were implemented with default encryption and authentication settings, ensuring that results reflect real-world deployments with minimal tuning.

2.2.2. Test Methodology

Each test scenario was executed under the following MTU value:

- 1500 bytes (default Ethernet frame size)

MTU values was adjusted 1500 bytes, and their effects on throughput, CPU load, and packet-per-second (PPS) rates were recorded. The VPN tunnels were established between two endpoints configured under various bonding and tunnel setups, including:

- Single Interface / Single Tunnel
- Dual Interfaces / Dual Tunnels

- Single Interface / Dual Tunnels
- IEEE 802.3ad Bonding (LACP)
- Round Robin Bonding

For each scenario, the following performance metrics were recorded:

Throughput (Mbps) – Measured using iPerf3 in TCP mode with multiple parallel streams

CPU Utilization (%) – Captured using system monitoring tools to evaluate processing overhead

Packets Per Second (PPS) – Analyzed to understand packet transmission efficiency

Transmission Rates – Evaluated in terms of sustained vs. peak throughput

Each test was repeated multiple times to ensure statistical validity, with results averaged to mitigate outliers.

2.2.3. Data Collection and Analysis

Performance data was logged in real-time and exported for further analysis using statistical tools. Comparative evaluations were performed to determine:

- The impact of CPU load on throughput and encryption overhead
- How different bonding strategies affect VPN traffic distribution and latency
- The optimal configurations for maximizing VPN performance in SD-WAN environments

By employing a structured and repeatable testing methodology, this study ensures that the results provide a reliable basis for understanding the trade-offs between WireGuard and IPSec in various network conditions. The findings contribute to best practices for VPN deployment optimization, particularly in performance-sensitive applications.

Figure 1 illustrates the experimental setup used in this study, which consists of two VPN endpoints connected via different bonding and tunneling configurations. The network infrastructure was carefully designed to minimize external factors that could impact performance measurements. The test environment was configured to allow a comprehensive evaluation of various scenarios, including single interface, dual tunnel, and multiple bonding modes, ensuring that the results reflect real-world deployment conditions.

To systematically evaluate the performance of WireGuard and IPSec VPN protocols under different network configurations, a series of controlled tests were conducted. Each test utilized iPerf3, a widely recognized network performance measurement tool, to assess throughput, CPU utilization. The tests were performed over 30-second intervals to ensure consistency and reliability of the recorded data.

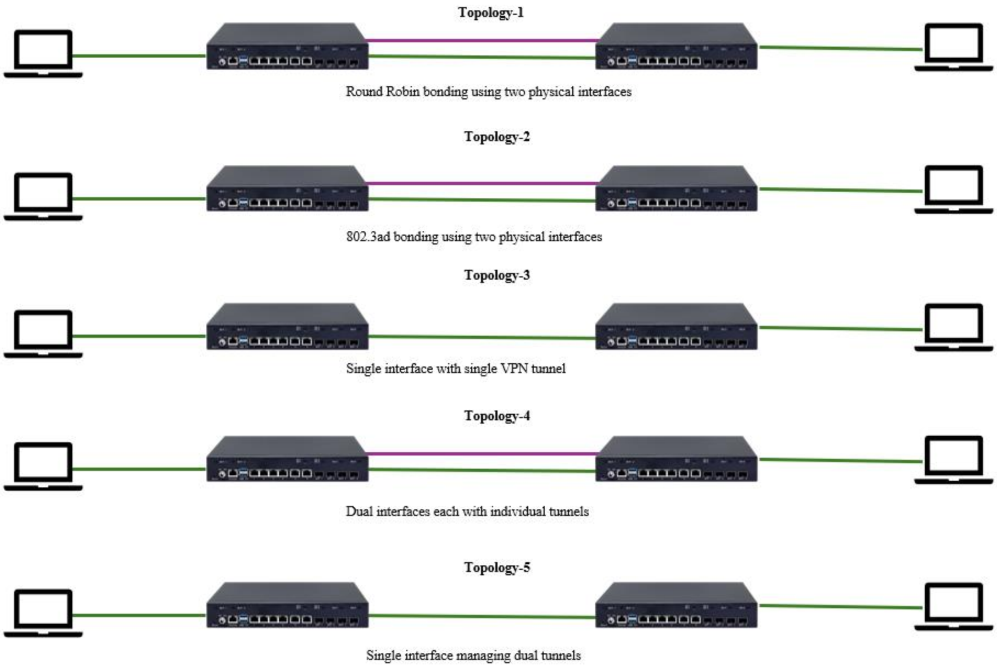
Topology-1
Round Robin bonding using two physical interfaces
Topology-2
802.3ad bonding using two physical interfaces
Topology-3
Single interface with single VPN tunnel
Topology-4
Dual interfaces each with individual tunnels
Topology-5
Single interface managing dual tunnels

Figure 1. Experimental setup for performance testing of wireguard and ipsec VPN protocols

3. Results and Discussion

This section presents the performance evaluation of WireGuard and IPSec under various network configurations. The experiments were conducted to analyze throughput, CPU utilization, and packet processing efficiency across different setups, including Round Robin bonding, IEEE 802.3ad bonding, single interface, dual interface with dual tunnels, and single interface with dual tunnels. The following subsections provide a detailed analysis of each configuration.

3.1. Round-robin

In the Round Robin bonding configuration, network traffic is evenly distributed across multiple links in a sequential manner, allowing for load balancing. This setup aims to improve throughput by utilizing multiple interfaces efficiently. The following figures illustrate the CPU utilization and throughput performance of WireGuard and IPSec under this mode.

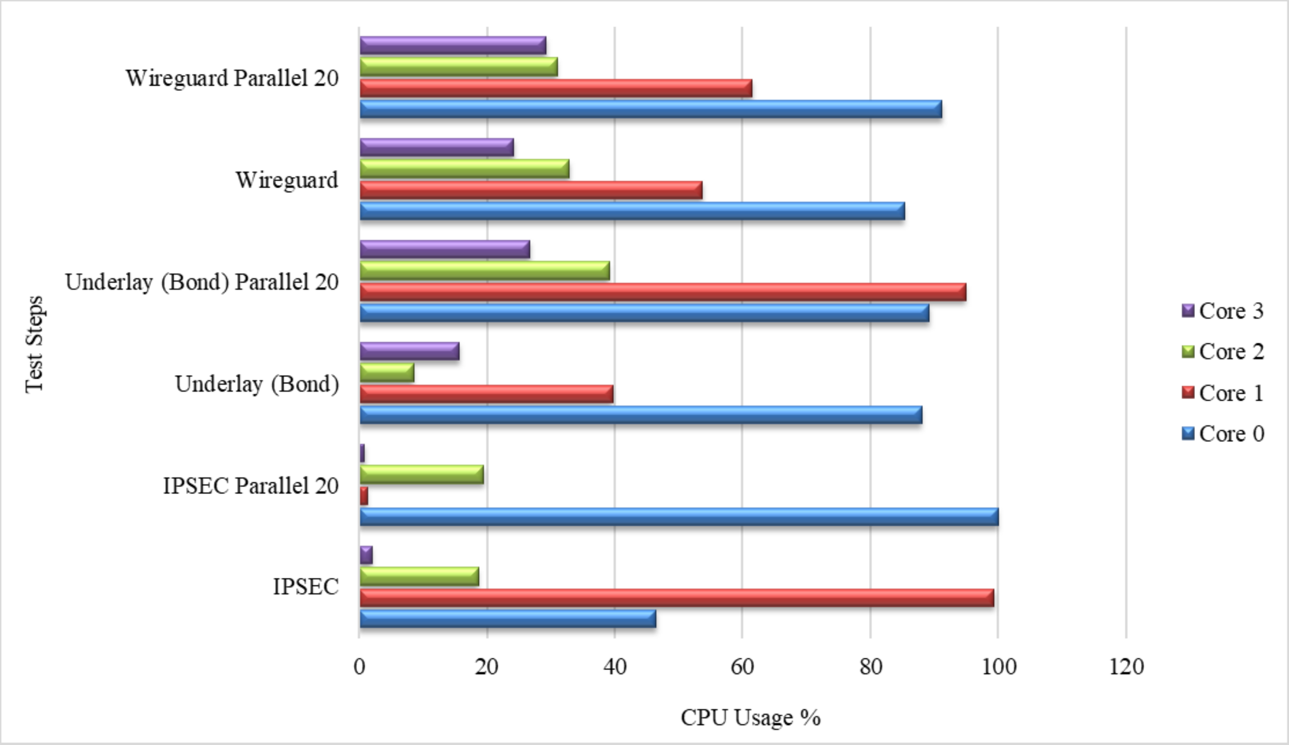

Figure 2. CPU utilization comparison of wireguard and ipsec using round robin bonding mode

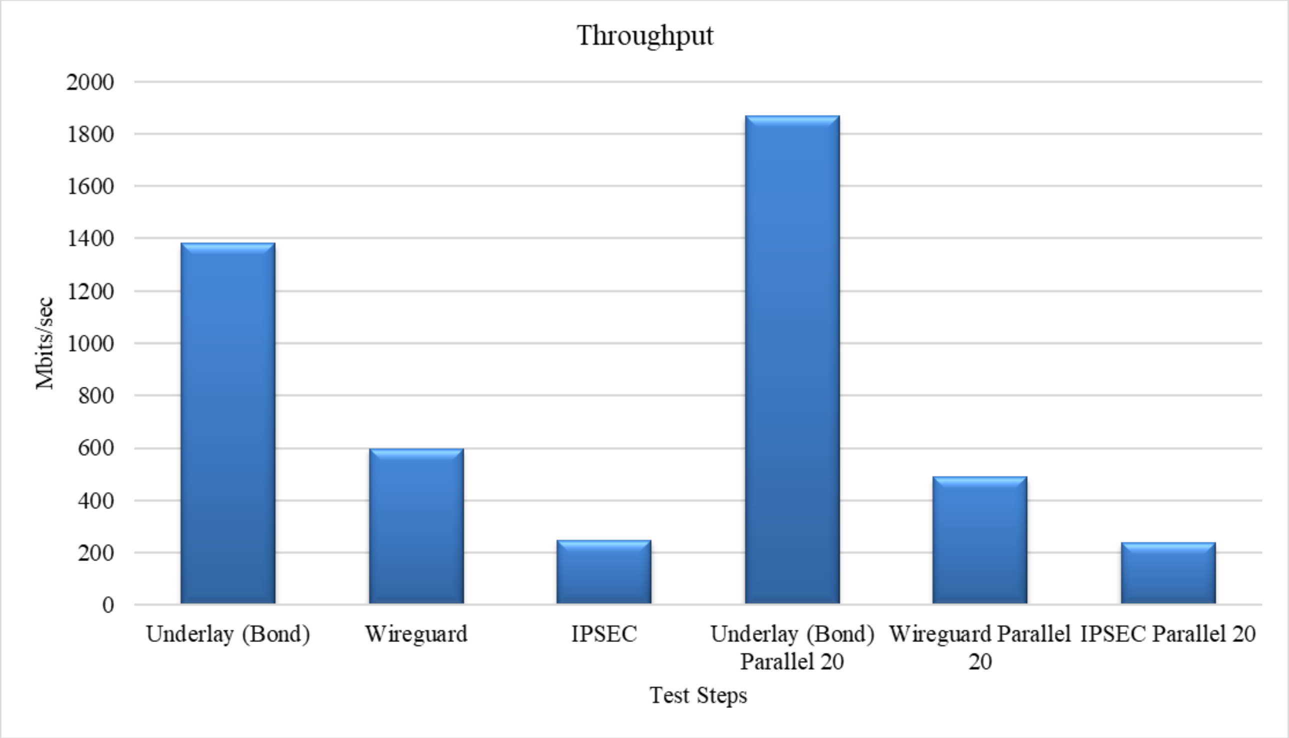

Figure 3. Throughput performance of wireguard and ipsec using round robin bonding mode

Figure 2 provides a detailed analysis of the CPU utilization of WireGuard and IPSec in Round Robin mode. Figure 3 presents the corresponding throughput measurements, showing that WireGuard achieves higher data transfer rates compared to IPSec. This performance disparity highlights the advantage of WireGuard's streamlined design, especially in high-bandwidth environments.

WireGuard achieved higher throughput than in Round Robin mode, with only a modest increase in CPU usage.

3.2. 802.3.ad

IEEE 802.3ad, also known as Link Aggregation Control Protocol (LACP), dynamically balances network traffic based on link conditions and negotiated parameters. This method improves bandwidth utilization while maintaining redundancy. The performance comparison of WireGuard and IPSec in this configuration is presented in the following graphs.

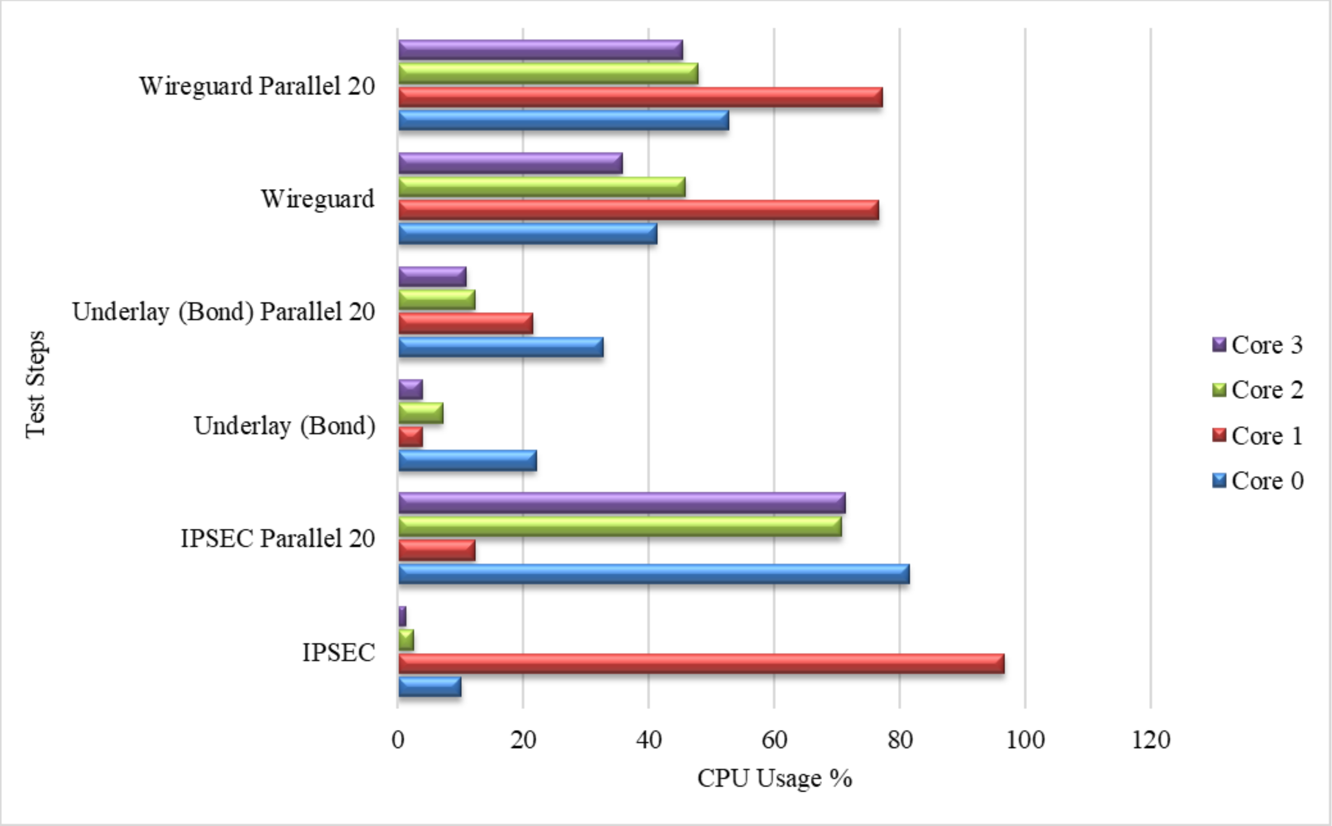

Figure 4. CPU utilization comparison of wireguard and ipsec using ıeee 802.3ad (lacp) bonding mode

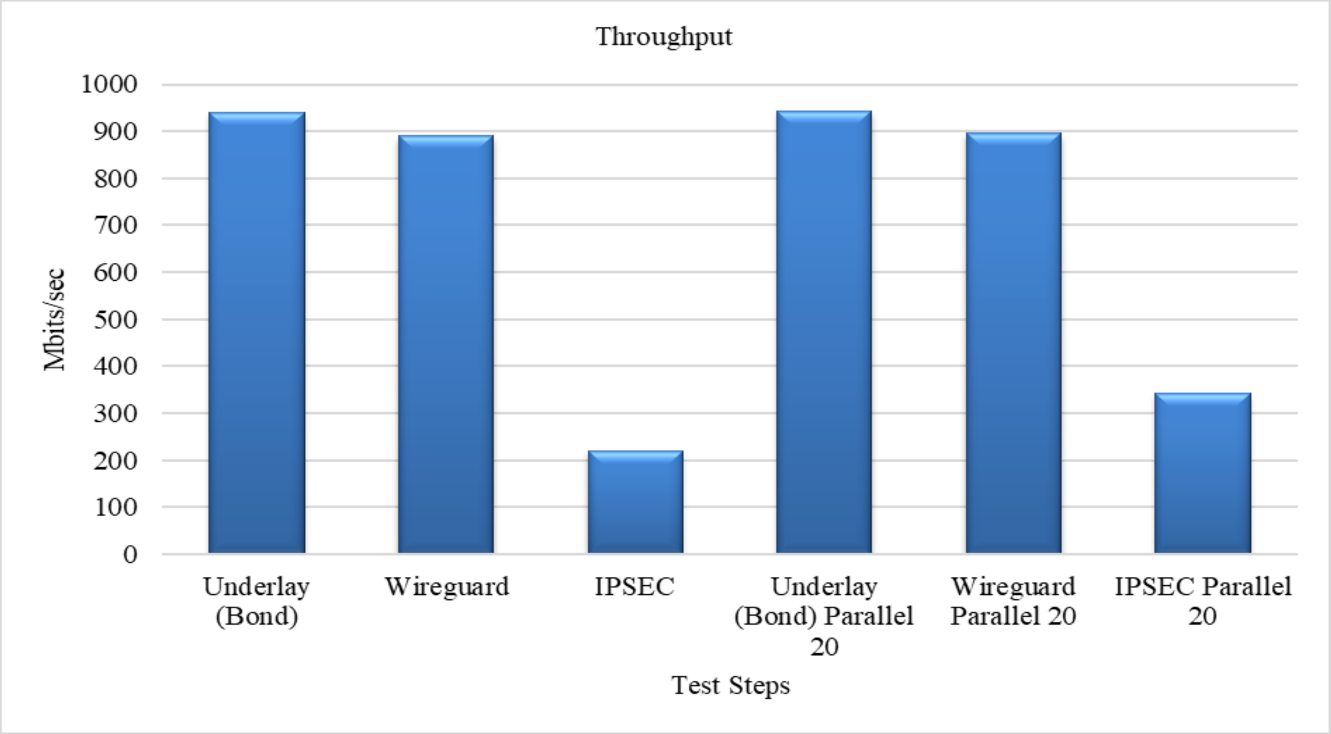

Figure 5. Throughput performance of wireguard and ıpsec using ieee 802.3ad (lacp) bonding mode

Figure 4 examines CPU utilization under IEEE 802.3ad bonding mode, revealing that while both VPN protocols benefit from load balancing, IPSec incurs a higher processing cost due to its more complex encryption mechanisms. WireGuard demonstrates better efficiency in this mode, maintaining stable CPU usage even as network load increases. Figure 5 displays the throughput performance in IEEE 802.3ad mode, where WireGuard outperforms IPSec in terms of sustained data transfer rates. These results suggest that IEEE 802.3ad bonding mode enhances overall network performance, but WireGuard is better suited for handling the associated workload without significantly increasing CPU consumption. WireGuard demonstrated improved throughput compared to Round Robin, while CPU usage slightly increased. IPSec showed higher throughput but suffered a substantial increase in CPU load, negatively affecting efficiency.

3.3. Single Interface

A single interface configuration represents a baseline scenario where all VPN traffic is transmitted through a single physical network interface. This setup helps assess the raw performance of WireGuard and IPSec without the influence of bonding or load-balancing mechanisms. The test results provide insights into how efficiently each protocol handles network traffic in a standard deployment.

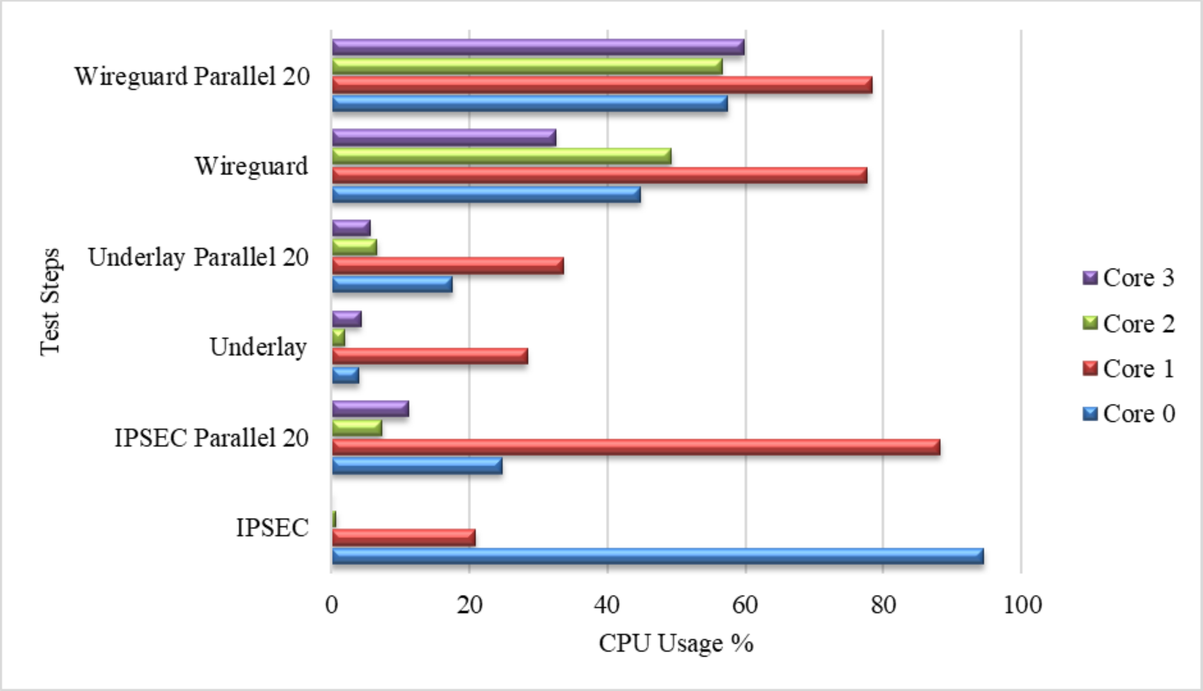

Figure 6. CPU utilization comparison of wireguard and ipsec with single interface configuration

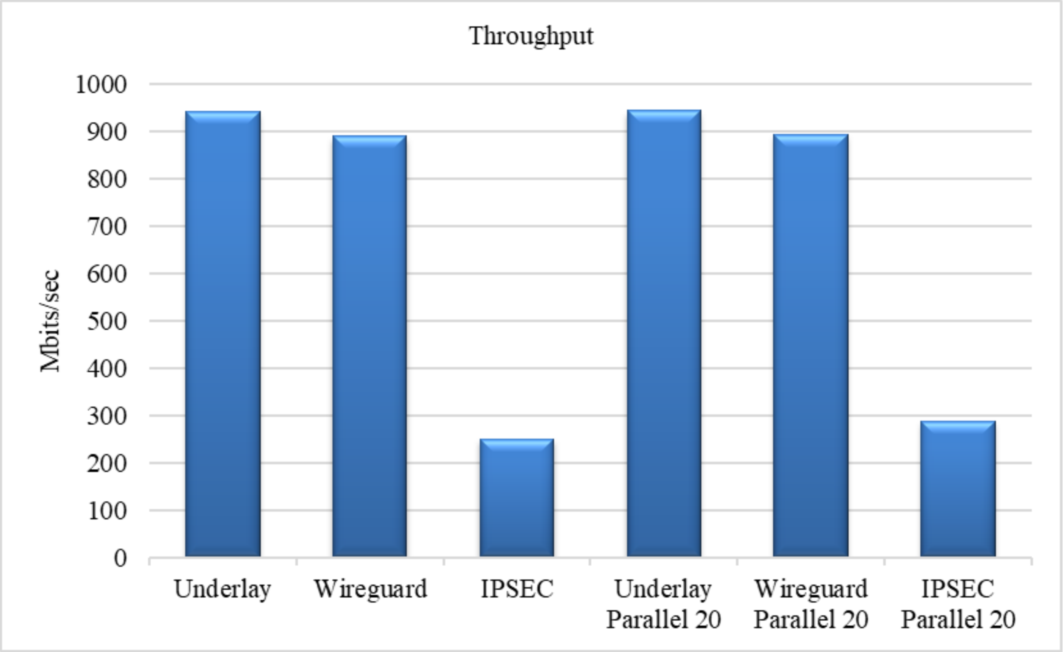

Figure 7. Throughput performance of wireguard and ipsec with single interface configuration

Figure 6 illustrates the CPU utilization of WireGuard and IPSec when operating with a single network interface. WireGuard uses significantly less CPU than IPSec, confirming its processing efficiency. This is especially important in systems where minimizing CPU load is critical. Figure 7 shows that WireGuard also delivers higher throughput in the same setup. Its lightweight design reduces encryption overhead, allowing it to maintain strong performance even with limited resources. Overall, WireGuard clearly outperforms IPSec in both CPU usage and data throughput in single-interface deployments.

3.4. Dual Interfaces Dual Tunnels

In this configuration, two physical interfaces are utilized, each establishing a separate VPN tunnel. This setup is expected to enhance throughput by distributing the traffic across independent paths. The results compare how WireGuard and IPSec manage multiple tunnels, evaluating their efficiency in leveraging additional network interfaces.

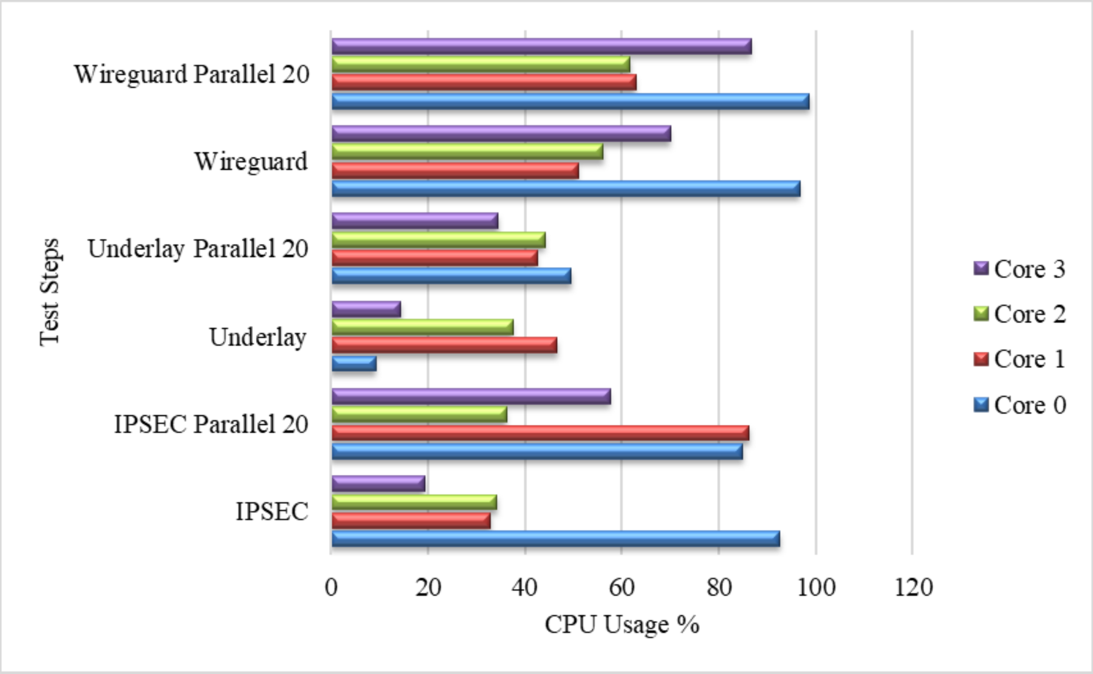

Figure 8. CPU utilization comparison of wireguard and ipsec in dual interface/dual tunnel configuration

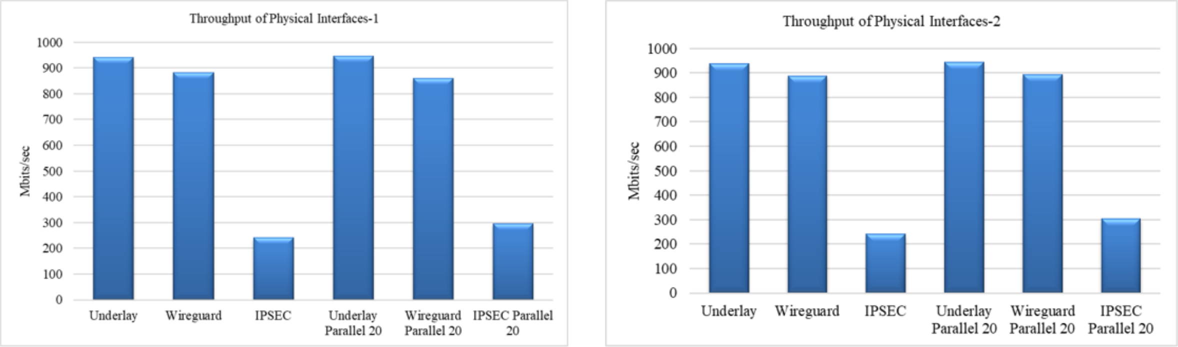

Figure 9. Throughput performance of wireguard and ipsec in dual interface/dual tunnel configuration

Figure 8 explores the impact of using dual interfaces and dual tunnels on CPU utilization. The results reveal that WireGuard effectively distributes processing loads across multiple tunnels, reducing the impact on any single core or network interface. In contrast, IPSec exhibits less efficient resource distribution, leading to higher CPU usage. Figure 9 presents the corresponding throughput results, showing that WireGuard achieves superior performance in dual interface/dual tunnel configurations. This suggests that WireGuard is more scalable in multi-tunnel deployments, making it a better choice for high-performance networking applications.

WireGuard provided higher throughput and lower CPU usage compared to IPSec. IPSec performance was hampered by high CPU usage.

3.5. Single Interface Dual Tunnel

Unlike the dual interface configuration, this setup utilizes a single physical interface while maintaining two separate VPN tunnels. The objective is to analyze the performance trade-offs between tunnel redundancy and the limitations of a single network interface. The following results highlight the impact of this approach on CPU utilization and throughput performance.

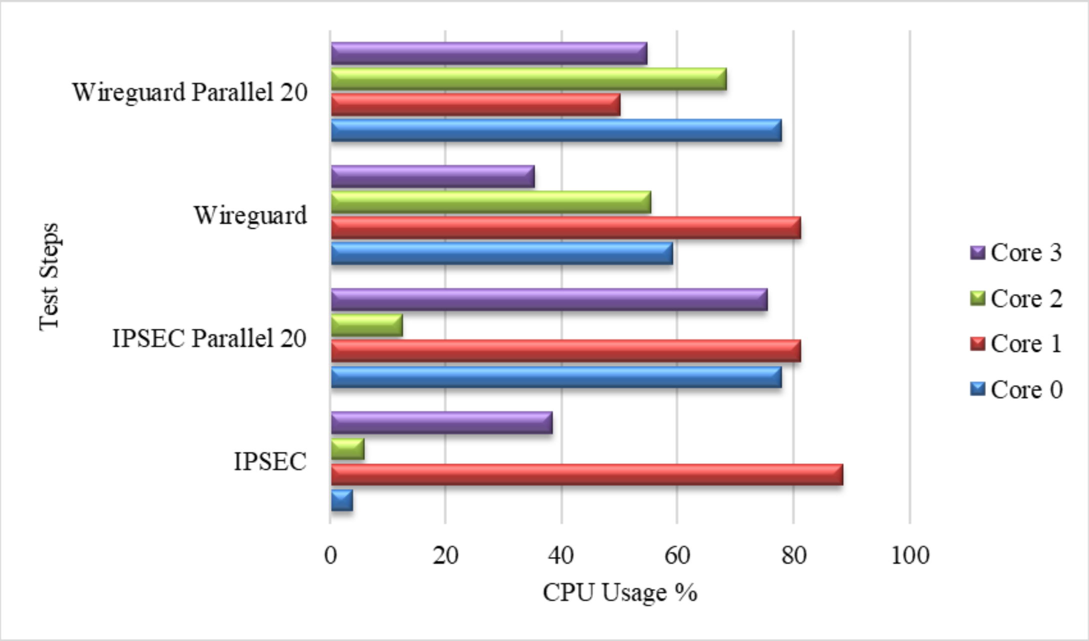

Figure 10. CPU utilization comparison of wireguard and ipsec in single interface/dual tunnel configuration

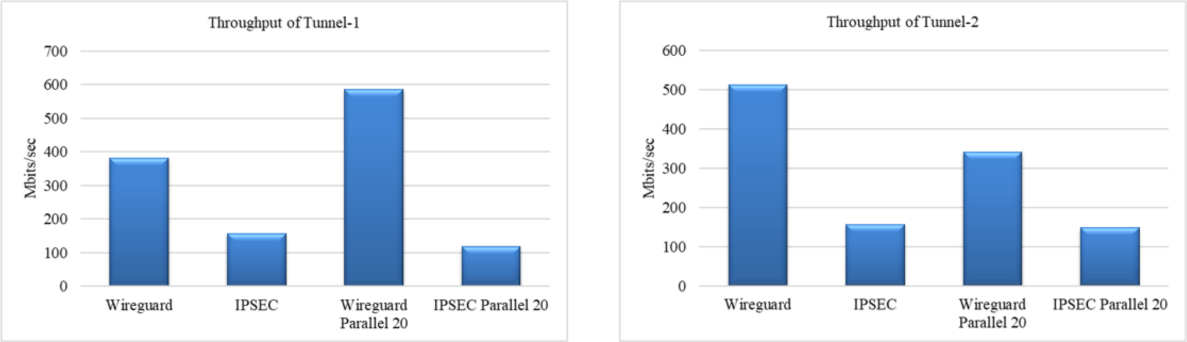

Figure 11. Throughput performance of wireguard and ipsec in single interface/dual tunnel configuration

Figure 10 evaluates the CPU utilization of WireGuard and IPSec in a single interface/dual tunnel configuration. The findings indicate that WireGuard maintains lower CPU consumption while effectively handling multiple tunnels. This efficiency translates into improved overall network performance. Figure 11 presents the throughput performance for this configuration, demonstrating that WireGuard consistently achieves higher data transfer rates despite bandwidth sharing between tunnels. IPSec, on the other hand, struggles with increased CPU consumption, which negatively impacts its throughput capabilities.

3.6. Detailed Comparative Analysis

- Round Robin vs. 802.3ad: Round Robin provided more stable throughput and lower CPU usage at an MTU of 1500 bytes.
- WireGuard vs. IPSec: WireGuard consistently outperformed IPSec across all configurations in both throughput and CPU efficiency.
- Single Interface, Multi-Tunnel Configurations: Sharing a single interface among multiple tunnels reduced overall throughput. However, WireGuard managed this constraint better than IPSec, achieving higher performance despite interface limitations.

These results are consistent with the findings of Dowling and Paterson (2018), who demonstrated that WireGuard's kernel-space implementation contributes to reduced overhead and improved encryption performance under heavy load. Similarly, Abbas et al. (2023) reported IPSec's high CPU consumption due to multi-layer encryption, supporting the overhead measurements observed in our test scenarios.

4. Conclusion

The results of this study clearly demonstrate that WireGuard consistently outperforms IPSec across various network configurations, particularly in high-load. WireGuard's lightweight architecture, streamlined cryptographic implementation, and kernel-space integration contribute to its superior performance in terms of throughput, CPU efficiency, and packet processing speed.

One of the key findings of this study is that WireGuard achieves significantly higher throughput compared to IPSec while maintaining lower CPU utilization, making it an ideal solution for environments where performance and resource efficiency are critical WireGuard's efficiency further enhances its suitability for high-bandwidth applications, increasing overall transmission efficiency.

Although IPSec is a mature and widely accepted VPN protocol, it introduces notable performance limitations. Its higher computational overhead stems from complex key exchange mechanisms (e.g., IKE), multi-layer encapsulation (e.g., ESP, AH), and partial user-space processing. These characteristics make IPSec less favorable for scenarios that demand high-speed, low-latency connectivity. However, IPSec remains a valid choice in specific contexts—particularly in legacy enterprise environments requiring robust security integration, regulatory compliance, or maximum interoperability with existing infrastructure. Acknowledging these trade-offs helps provide a more balanced perspective on protocol selection, enabling decision-makers to align protocol choices with operational priorities.

The analysis of different network bonding strategies also reveals that WireGuard benefits more from multi-interface and load-balancing configurations due to its ability to establish lightweight, stateless encrypted tunnels without introducing excessive protocol overhead. IPSec, on the other hand, struggles with multi-tunnel configurations, often requiring additional tuning to achieve optimal performance.

From a practical standpoint, these findings suggest that organizations seeking to deploy VPN solutions in SD-WAN architectures should prioritize WireGuard, particularly for cloud environments, remote workforce security, and bandwidth-intensive applications. Its ease of configuration, rapid handshake process, and minimal performance overhead make it a future-proof VPN solution, aligning well with the demands of scalable, low-latency, and high-performance network infrastructures.

In conclusion, WireGuard emerges as the superior choice for optimized SD-WAN deployments, where performance, efficiency, and scalability are key requirements. While IPSec remains a viable option for legacy systems and compatibility-driven scenarios, its higher CPU consumption and lower throughput present challenges in high-performance networking applications. The results of this study reaffirm the growing adoption of WireGuard as the preferred VPN protocol in modern network architectures.

Acknowledgment

The authors would like to express their gratitude to ULAK Haberleşme A.Ş. for providing the necessary support and resources that contributed to the successful completion of this study. Their valuable contributions and expertise in the field of communication technologies have been instrumental in facilitating this research.

References

Abbas H., Emmanuel N., Amjad MF., Yaqoob T., Atiquzzaman M., Iqbal Z., Shafqat N., Shahid WB., Tanveer A., Ashfaq U. Security assessment and evaluation of VPNs: a comprehensive survey. ACM Computing Surveys 2023; 55(13): 1-47.

Balachandran S., Dominic J., Sivankalai S. A comparative analysis of VPN and proxy protocols in library network management. Library of Progress-Library Science, Information Technology & Computer 2024; 44(3).

Donenfeld JA. WireGuard:next generation kernel network tunnel. NDSS, 2017.

Dowling B., Paterson KG. A cryptographic analysis of the WireGuard protocol. International Conference on Applied Cryptography and Network Security, 2018.

Gentile AF., Macrì D., Greco E., Fazio P. IoT IP overlay network security performance analysis with open source infrastructure deployment. Journal of Cybersecurity and Privacy 2024; 4(3): 629-649.

Gentile AF., Macrì D., De Rango F., Tropea M., Greco EJFI. A VPN performances analysis of constrained hardware open source infrastructure deploy in IoT environment. Future Internet 2022; 14(9): 264.

Gordeychik S., Kolegov D. SD-WAN Threat Landscape. arXiv preprint 2018.

Mackey S., Mihov I., Nosenko A., Vega F., Cheng Y. A performance comparison of WireGuard and OpenVPN. Proceedings of the Tenth ACM Conference on Data and Application Security and Privacy, 2020, 162-164.

Mansouri Y., Prokhorenko V., Babar MA. An automated implementation of hybrid cloud for performance evaluation of distributed databases. Journal of Network and Computer Applications 2020; 167: 102740.

Narayan S., Brooking K., De Vere S. Network performance analysis of vpn protocols: an empirical comparison on different operating systems. International Conference on Networks Security, Wireless Communications and Trusted Computing 2009; 645-668.

Oluyede MS., Mart J., Olusola A., Olatuja G. Security challenges and solutions in SD-WAN deployments. ScienceOpen Preprints 2024.

Ostroukh A., Pronin C., Podberezkin A., Podberezkina J., Volkov A. Enhancing corporate network security and performance: a comprehensive evaluation of wireGuard as a next-generation VPN solution. 2024 Systems of Signal Synchronization, Generating and Processing in Telecommunications 2024; 1-5.

Pries R., Yu W., Graham S., Fu X. On performance bottleneck of anonymous communication networks. 2008 IEEE International Symposium on Parallel and Distributed Processing, 2008, page number:1-11.

Sharma K., Tahiliani MP., Rathod VJ. Design and development of an emulation model for VPN and VPN bonding. 2024 IEEE International Conference on Electronics, Computing and Communication 2024; 1-6.

Shen Y., Wu Y., Shen J., Zhang H. WirePlanner: fast, secure and cost-efficient route configuration for SD-WAN. arXiv preprint 2023.

Shue CA., Gupta M., Myers SA. Ipsec: Performance analysis and enhancements. 2007 IEEE International Conference on Communications 2007; 1527-1532.

Ullah S., Choi J., Oh H. IPsec for high speed network links: performance analysis and enhancements. Future Generation Computer Systems 2020; 107: 112-125.

Vilanova JP. Next generation overlay networks: security, trust, and deployment challenges. Universitat Politècnica de Catalunya (UPC), 2021.

Yang Z., Cui Y., Li B., Liu Y., Xu Y. Software-defined wide area network (SD-WAN): architecture, advances and opportunities. 28th International Conference on Computer Communication and Networks, 2019, 1-9.