ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 11 Issue 7 July 2024

Designing A VPN Using Open Network Infrastructure with Enhanced Security and Performance

[1] Hemal Shingloo, [2] Supriya Mishra, [3] Himani Zambare, [4] Ayushi Jaiswal, [5] Manoj Kumar

[1] [2] [3] [4] [5] School Computer Science and Engineering VIT Bhopal University Sehore, India
Corresponding Author Email: [1] hemal.shingloo2021@vitbhopal.ac.in, [2] supriyamishra2022@vitbhopal.ac.in, [3] himanisharadzambare2022@vitbhopal.ac.in, [4] ayushi.jaiswal2021@vitbhopal.ac.in [5] manojkumar@vitbhopal.ac.in

Abstract— ***The rapid expansion of digital communication and the increasing need for secure data transmission have underscored the importance of Virtual Private Networks (VPNs) [1] in modern networking. This paper presents a comprehensive approach to designing a VPN using open network infrastructure with a focus on achieving enhanced security and performance.Our proposed design incorporates several key elements to enhance security, including strong encryption mechanisms, multi-factor authentication, and intrusion detection/prevention systems. We also employ wireguard mechanism, protocols like HMAC (Hash-based Message Authentication Code) IPV4+V6 [21,22], UDP (User Datagram Protocol) [4]. In terms of performance, our approach leverages tunneling to optimize network routing and resource allocation dynamically. Quality of Service (QoS) mechanisms are implemented to prioritize traffic, ensuring low-latency and high-throughput connections. We also explore the use of advanced protocols and algorithms to reduce latency and increase overall network efficiency.[6]***

Furthermore, we discuss the practical implementation of our VPN design, including the use of open-source software and existing open network infrastructure components. We provide insights into the scalability and manageability of our solution, making it suitable for a wide range of network environments. Finally, we evaluate the security and performance enhancements achieved by our design through a series of experiments and real-world use cases, demonstrating its effectiveness in ensuring secure and efficient data transmission. Our findings highlight the potential of open network infrastructure as a viable and adaptable solution for building VPNs with enhanced security and performance.

Index Terms— ***Virtual Private Network, VPN, WireGuard, UDP, OpenVPN, Performance, Unreliability, Packet Loss, Delay.***

I. INTRODUCTION

Connectivity of two internal networks: This type of VPN connection is made between two private networks through a VPN service. The company integrates various remote locations into its internal network to simplify administration. Different websites connected to this internal network are scattered around the world, creating a scalable network thanks to VPN. This network can make it easier for businesses to communicate and send data. Remote access: This is when a remote user connects to the internal network through a VPN. With Remote Access VPN, users can securely access internal networks regardless of their location. A simple example is an employee accessing a company intranet for work purposes and accessing confidential files from remote locations. In this case, all their professional communications are secured and data is exchanged between employees and the company's intranet. A virtual private network (VPN) is currently defined as a technology that allows the use of the public Internet to create a secure connection between an end user and a corporate network. Thanks to VPNs, data transmitted over the Internet, especially sensitive information, remains confidential and cannot be monitored by curious individuals. From a practical point of view, VPN helps reduce communication costs, avoid eavesdropping and eavesdropping on the communication channel or ensure secure access to the company's intranet from the Internet. To access internal networks from remote locations (telework, employee access, customer access, etc.), different types of VPN connections are possible.

A. The Significance of VPNs

VPNs play a pivotal role in safeguarding sensitive data, whether it's in transit across the internet or within private networks. They create secure tunnels through which data can travel, shielded from prying eyes and potential threats. VPNs are used across diverse sectors, including businesses, government organizations, educational institutions, and individual users, all seeking to maintain the privacy and security of their network

communications.[3]

B. The Promise of OpenVPN and WireGuard OpenVPN: A Trusted Standard

OpenVPN is a flexible cybersecurity solution that includes an open source project called Community Edition, a powerful tunneling protocol that uses SSL/TLS encryption, and a company that offers commercial products to support it. its open source initiatives. OpenVPN Community Edition is a free, community-supported virtual private network (VPN) project designed for secure Internet connectivity, primarily suitable for users with Linux expertise. The OpenVPN tunneling protocol, based on SSL encryption, provides stronger security, faster connections, and the ability to bypass firewalls, making it a popular choice for securing data transfers. It supports multiple network configurations, dynamic endpoints, NAT networks, and provides encryption options, making it highly adaptable. OpenVPN Cloud, based on the OpenVPN protocol, simplifies network security management, making it the ideal choice for businesses looking for secure and scalable remote access. solutions. OpenVPN is dedicated to making cloud-based security accessible to businesses of all sizes, offering flexible and cost-effective solutions as per evolving business needs. [4]

II. PROBLEM STATEMENT:

Security Vulnerabilities:

VPNs can be susceptible to security breaches, making them potential targets for cyberattacks, data leaks, and unauthorized access. This poses a significant threat to sensitive company data and communication.

Performance Issues:

Many remote workers experience slow and unreliable VPN connections, impacting their productivity and the overall user experience. These performance issues are often related to bandwidth limitations and network congestion.

This report will compare the performance of state-of-the-art VPNs under normal and unreliable network conditions on different operating systems. The performance will be measured in throughput and degradation. The results of the study will be used to develop recommendations for system administrators when choosing and deploying VPN solutions.

A. WireGuard: Modern Innovation

WireGuard is an open-source communication protocol for setting up secure Virtual Private Networks (VPNs). Using advanced cryptographic primitives to secure exchanged data, it seals it within an encrypted tunnel. While originally it was built in the Linux kernel in 2020, it's now freely available for a wide range of operating systems.

The protocol was developed by the sole security researcher Jason Donenfeld, who was experimenting with existing options. As most of them had poor performance and were hard to set up, the natural conclusion was to simplify the whole architecture. Therefore, WireGuard was intended to be a streamlined VPN protocol that could outperform the competition and provide much better network security.

B. Protocols Used

OpenVPN:

OpenVPN:

- HMAC: Ensures message integrity.[16]
- IPV4+V6: Supports both IPv4 and IPv6 protocols.[21]
- UDP:Utilizes User Datagram Protocol for efficient transmission.
- OPENSSL: Relies on OpenSSL for cryptographic operations [8].

WireGuard:

- Curve25519: Used for secure key exchange
- ChaCha20: Employs for high-speed symmetric encryption.
- HKDF: Derives session keys securely.
- UDP-based: Exclusively uses UDP for communication efficiency.

OpenVPN employs HMAC [16] for message integrity, supports both IPv4 and IPv6 protocols [22], and utilizes UDP for efficient transmission, all while relying on OpenSSL for cryptographic operations. In contrast, WireGuard utilizes Curve25519 for secure key exchange, ChaCha20 for high-speed symmetric encryption, and HKDF for deriving session keys securely, exclusively over UDP for communication efficiency.[11]

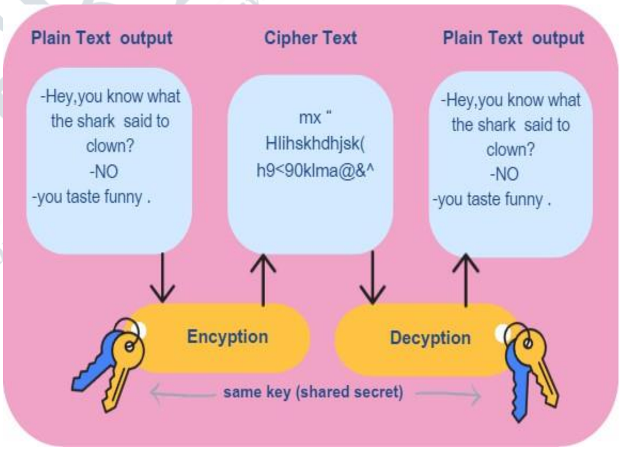


Figure 1. How Data is Being Secured in VPN

III. LITERATURE REVIEW

A literature review on VPN protocols, specifically OpenVPN and WireGuard [8] with a focus on their use of the UDP (User Datagram Protocol) transport layer protocol [15], can provide valuable insights into the advantages and disadvantages of each protocol in various contexts. Below is a literature review outlining key findings and trends up to my knowledge cutoff date in September 2021.

1. Introduction to VPN and Protocols: To understand the importance of VPN protocols, it is important has a solid foundation in virtual private networks (VPN). VPNs are widely used to secure communications over [6] Internet. VPN protocols are essential for assurance confidentiality, integrity and authentication of the data exchanged between a the protocol of server.

2. OpenVPN: - OpenVPN, which makes use of the SSL/TLS protocol, has been a famous preference because of its sturdy safety features. Researchers have investigated the overall performance and safety components of OpenVPN. For example, research have [15] analyzed the way it plays beneathneath numerous community situations and recognized ability vulnerabilities (e.g., Heartbleed). OpenVPN generally makes use of each UDP and TCP for transport. UDP is desired for quicker connections, however researchers have mentioned the ability for connection instability in unreliable community situations.
3. WireGuard: – A relatively new VPN protocol, WireGuard includes [16] It attracted wide attention due to its simplicity. efficiency. Safety and security literature emerges Wire guard function. The researchers [19] It turns out this is possible with modern encryption and a minimal code base. Provides strong security with minimal attack surface. WireGuard Primarily uses UDP for transport, low overhead High throughput. Often praised for its long shelf life [12] Connectivity in difficult network conditions.
4. UDP vs. TCP:- The desire of UDP or TCP because the transport [10] layer protocol has implications for VPN overall performance and reliability. UDP is typically desired for VPNs because it offers decrease latency and is higher desirable for real-time applications. It may be particularly beneficial for gaming and VoIP applications is extra dependable however can be afflicted by better latency because of its congestion manipulate mechanisms, which makes it much less appropriate for time-touchy data.
5. Comparison Studies: Several research have immediately as compared OpenVPN and WireGuard in phrases of performance, safety, and usability. Research shows that WireGuard frequently outperforms OpenVPN in phrases of pace and efficiency, at the same time as OpenVPN may also have an part in phrases of configurability and compatibility.WireGuard`s minimum codebase and cutting-edge encryption primitives are frequently noted as motives for its progressed safety posture.
6. Challenges and Future Research: Some literature discusses the demanding situations of enforcing and deploying VPN protocols securely, in addition to a way to adapt to rising threats. Future studies on this discipline might also additionally awareness at the improvement and evaluation of next-technology VPN protocols or upgrades to present ones.

Historical Development of VPNs:

The improvement of VPN generation may be traced again to the want for steady far flung get admission to to company networks.

Early VPNs trusted devoted leased lines. The creation of the net caused the improvement of cutting-edge VPNs, which use encryption and tunneling protocols to create steady connections over public networks. The literature on VPNs with a selected awareness on OpenVPN and WireGuard, the use of UDP because the transport

layer protocol, highlights the continued evolution of VPN generation. While OpenVPN stays a sturdy and flexible preference, WireGuard has emerged as a promising opportunity because of its simplicity and efficiency, particularly in low- latency, high-overall performance scenarios. The preference among UDP and TCP relies upon on precise use instances and community conditions, emphasizing the want for a nuanced method while deciding on a VPN protocol. Future studies might also additionally preserve to discover new VPN protocols and deal with the evolving protection and overall performance demanding situations withinside the discipline

IV. METHODOLOGY

1. **Identify** what VPN solutions to experiment on, how to control traffic, what metrics to use, with which tools and what data to collect.
2. **Test the network** in the experimental setup without any VPN solution to identify baseline performance [9,10].
3. **Configure** and test VPN Solutions on three different operating systems with the network unreliability conditions.
4. **Analyze and compare** the results to see if there is any indication of performance difference between the VPN solution.

The three VPNs that were identified as suitable solutions to test are OpenVPN, WireGuard and UDP.

A very important fact is that the configurations of the VPN solutions are default For all VPN solutions, default configuration settings were kept as far as possible, rather than unifying the settings in respect to, for example, network protocols, cryptographic algorithms, or choices for compression. The decision to not touch the default settings was motivated by the assumption that the VPN solutions' developers would be most qualified to provide sane (secure) settings for their own VPN solutions. Default settings are used in all cases of the VPN tests. [6]

Furthermore as WireGuard is designed to be simple to deploy and use, it has fewer configuration options than UDP and OpenVPN.

- **penVPN** is deployed with completely default settings as that is recommended by the developers and that is enough for this experiment.[3]
- he **UDP** implementation is also deployed with default settings, but from a third hand created script. This script and its configuration settings is described more in the next chapter where a more detailed description of the experimental design is presented [4].
- he **WireGuard** implementation is also deployed with default settings to make the results valid as no other

VPN has any configuration than the default, excluding of course the connection settings, which need to be configured for the VPN to work.[2]

A. Materials:

1. VPN Server: A server with OpenVPN and WireGuard installed and configured.
2. VPN Client: A client device with iperf and a VPN client software (for OpenVPN and WireGuard).
3. Test Environment: A controlled network environment with known network conditions and the ability to monitor network traffic. [4] requirements. Ensure that the server is reachable from the client.[14]

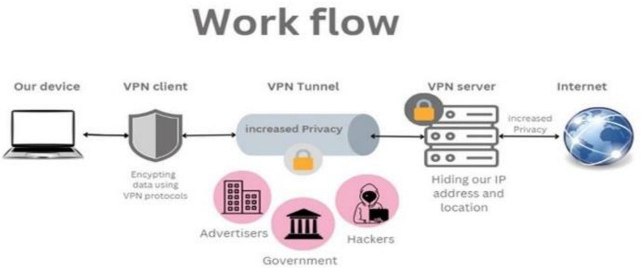


Figure 2.-Work flow

4. **VPN Client Configuration:** Configure the VPN client software on the client device to connect to the VPN server using OpenVPN (TCP and UDP) and WireGuard separately. Ensure that the VPN client can establish connections.[18]
5. **Performance Testing (With VPN):**

Measure the VPN`s overall performance the usage of iperf whilst linked to the VPN. Conduct the subsequent assessments:

a. **Bandwidth Tests:** Use iperf to degree the add and down load speeds among the patron and the server thru the VPN. Perform assessments for each OpenVPN (TCP and UDP) and WireGuard separately.[19]

b. **Latency Tests:** Use iperf to degree the latency or round- journey time (RTT) among the patron and server thru the VPN. Perform assessments for each OpenVPN (TCP and UDP) and WireGuard.

6. **Baseline Testing (Without VPN - Revisited):** Re-run iperf tests without the VPN to compare the results with the baseline measurements taken earlier.
7. **Comparison (With and Without VPN):** Compare the iperf test results obtained with and without the VPN in terms of bandwidth, latency, and network performance. Analyze the impact of VPN protocols (OpenVPN,TCP, OpenVPN UDP, and WireGuard) on network throughput.[20]
8. **Testing in Different Network Conditions:** Repeat the tests in various network conditions, such as high- latency, low-bandwidth, or networks with packet loss, to assess VPN performance under different scenarios.
9. **Security and Privacy Testing:**

Verify that DNS requests are routed through the VPN and not leaked to the ISP. Check for IP address leaks and ensure that the VPN server's IP address is used.[17]

V. TESTING

Testing a VPN connection created using OpenVPN and WireGuard using iperf involves measuring the network performance and throughput between two endpoints connected through the VPN tunnel. Here are the steps to test your VPN connections using iperf. [5]

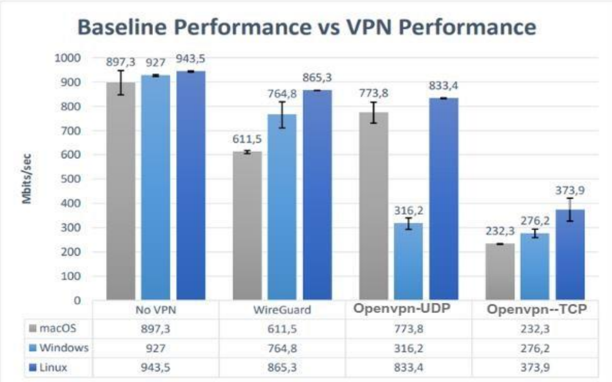
Note: Ensure that you have iperf installed on both the client and server machines. You can install it using your package manager (e.g., apt, yum, or brew).

B. Testing Steps:

1. **Baseline Testing (Without VPN):** Conduct initial iperf tests without using the VPN to establish a baseline.Measure baseline network throughput (e.g. bandwidth and latency) using iperf between the client and a known server within the local network.
2. VPN Server Setup: Set up and configure the VPN server with OpenVPN (TCP and UDP) and WireGuard according to your

VI. RESULTS

The results presented are values from when iPerf sends the packets to the server and server receives and presents the values.All the results presented are the mean values of the 50 tests per case. The no VPN baseline performance is from testing the connection without any of the unreliability added or VPN enabled.The baseline VPN performance results are based on the performance tests done with iPerf on the VPNs using a reliable network, i.e no unreliability aspect enabled.[5]



	No VPN	WireGuard	Openvpn-UDP	Openvpn--TCP
■ macOS	897,3	611,5	773,8	232,3
■ Windows	927	764,8	316,2	276,2
■ Linux	943,5	865,3	833,4	373,9

Figure 3. Baseline vs VPN Performance, Ref [1,11]

The results of the baseline performance show one obvious trend that OpenVPN is generally slower than the No VPN tests.

The performance tests with No VPN were as expected faster than the tests with VPNs enabled. The fast throughput when using UDP is due to the compression of data that is done with that VPN implementation.

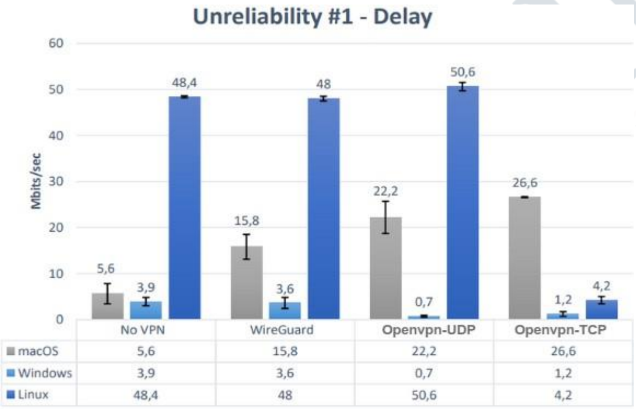
The best performer on Windows was WireGuard with only a 17% loss in throughput. UDP even though natively supported in Windows performed poorly compared to the other OSs. It got outperformed by 659% compared to the No VPN test.

Linux performed overall very well in this test with only a loss of 8.3% with WireGuard and 11.6% with UDP over no VPN.

A. Unreliability #1 – delay

The unreliability #1 – delay means that the traffic shaper on the router has been enabled to add 400msec delay on the experiment network. This was then tested without any VPN enabled and each of the VPNs one by one.

- The results of the first unreliability variable show that Linux handle delays well in all cases except OpenVPN and UDP. [1,3]
- Similarly macOS also performs comparatively well, especially with OpenVPN under delay. Windows really falls behind with the worst results in all scenarios during the delay tests. The results are very poor on Windows overall with delay enabled. Since its consistent with all
- VPN solutions and the baseline, this may be because of the way the default network settings are set up on Windows.[6]
- The Linux results are by far the best with all VPN solutions except OpenVPN.[7]



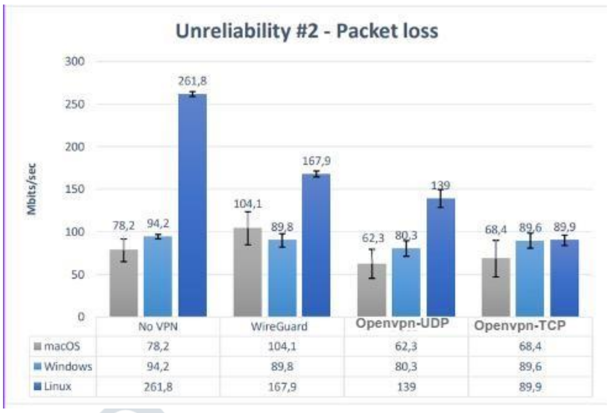
	No VPN	WireGuard	Openvpn-UDP	Openvpn-TCP
■ macOS	5,6	15,8	22,2	26,6
■ Windows	3,9	3,6	0,7	1,2
■ Linux	48,4	48	50,6	4,2

Figure 4. No VPN and VPN Performance under Unreliability #1 - Delay (Reference 1)

B. Unreliability #2 – packet loss

The unreliability #2 – packet loss aspect means that in a similar way as the delay aspect was enabled on the router in the experiment, but this time a 1% packet loss was added to the network connection.

- The results from the packet loss unreliability tests show similar results in the way that Linux is generally performing the best while macOS and Windows do not differ much as the error bars overlap in all tests between the two.
- Linux with packet loss achieved 261.8 Mbits/sec which is far better than macOS and Windows with the same unreliability factor.[7]
- With WireGuard it lost 35%. With UDP the decrease was 46% and OpenVPN decreased the throughput compared to No VPN on Linux with 65%.



	No VPN	WireGuard	Openvpn-UDP	Openvpn-TCP
■ macOS	78,2	104,1	62,3	68,4
■ Windows	94,2	89,8	80,3	89,6
■ Linux	261,8	167,9	139	89,9

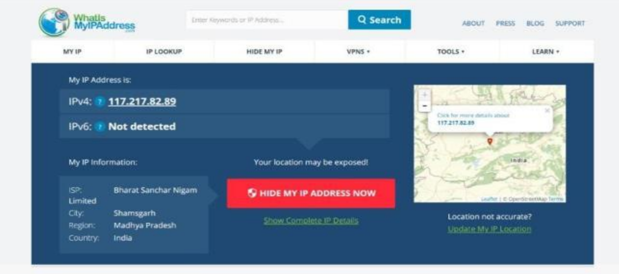
Figure 5. No VPN and VPN Performance under Unreliability #2 – Packet loss (Reference 1)

C. Detailed results

A definitive conclusion is that all implementations have their own advantages and disadvantages. Some VPN solutions

perform better on a certain operating system. The most impactful conclusions drawn by the results are presented below.The best performing VPN solution for macOS, if the network is reliable, was UDP followed by WireGuard and worst performing was OpenVPN. [3] We can see that with any of the unreliability variables in effect, all VPNs and OSs had reduced throughput in comparison with no unreliability.Linux is fastest with the baseline and no unreliability at 943.5Mbits/sec.All VPNs except OpenVPN perform best in Linux during the delay unreliability when comparing the other OSs under delay .[1] All VPNs perform best in Linux while experiencing packet loss

Also important to note is that the results are heavily dependent on the tool (iPerf) and there is a possibility that it is better suited for one OS than the others.OpenVPN is not the top performer in any test. [4] Linux performs best in all unreliability tests except one, the unreliability #1 – delay.



My IP Address is:

IPv4: 117.217.82.89

IPv6: Not detected

My IP Information:

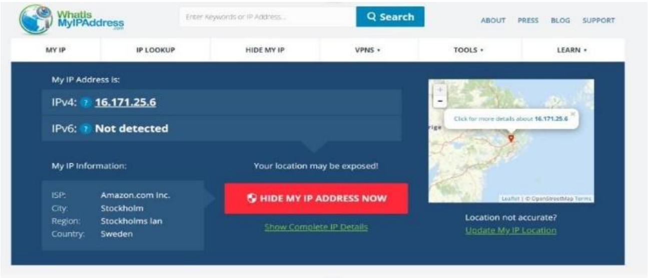
ISP: Bharat Sanchar Nigam Limited
City: Shamsgarh
Region: Madhya Pradesh
Country: India

Your location may be exposed!

Click for more details about 117.217.82.89

Location not accurate?
Update My IP Location

Figure 6. -result without VPN



WhatIs MyIPAddress.com

Enter Keywords or IP Address...

Search

ABOUT PRESS BLOG SUPPORT

MY IP | IP LOOKUP | HIDE MY IP | VPNS ▾ | TOOLS ▾ | LEARN ▾

My IP Address is:

IPv4: 16.171.25.6

IPv6: Not detected

My IP Information:

ISP: Amazon.com Inc.
City: Stockholm
Region: Stockholms lan
Country: Sweden

Your location may be exposed!

HIDE MY IP ADDRESS NOW

Show Complete IP Details

Click for more details about 16.171.25.6

Leaflet | © OpenStreetMap Terms

Location not accurate?
Update My IP Location

Figure 7. Result With VPN

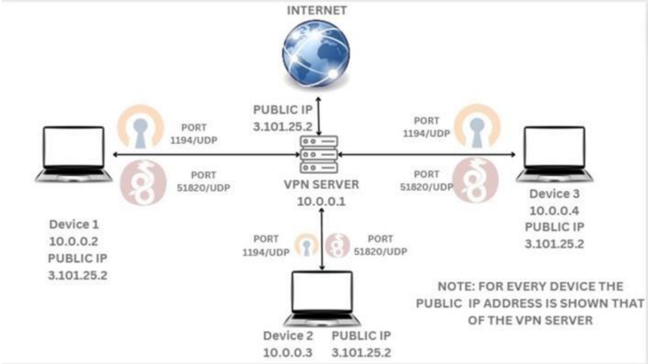
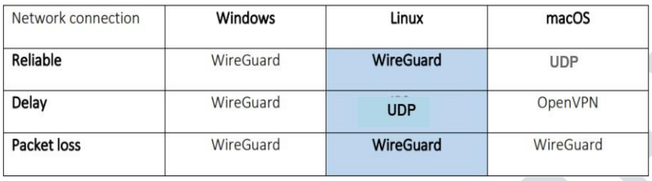
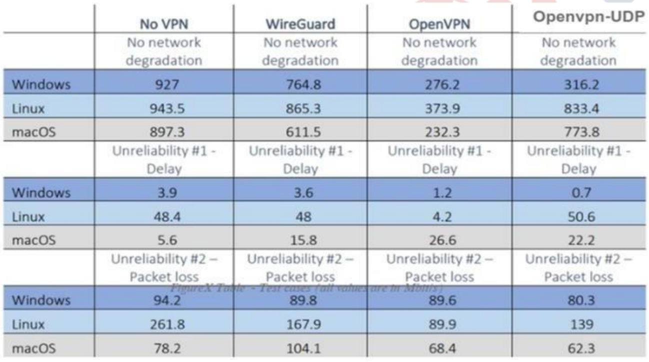


Figure 8. Connecting VPN serve



Network connection	Windows	Linux	macOS
Reliable	WireGuard	WireGuard	UDP
Delay	WireGuard	UDP	OpenVPN
Packet loss	WireGuard	WireGuard	WireGuard

Figure 9. Network Connection on different Operating System Ref [1]



	No VPN	WireGuard	OpenVPN	Openvpn-UDP
	No network degradation	No network degradation	No network degradation	No network degradation
Windows	927	764.8	276.2	316.2
Linux	943.5	865.3	373.9	833.4
macOS	897.3	611.5	232.3	773.8
	Unreliability #1 - Delay	Unreliability #1 - Delay	Unreliability #1 - Delay	Unreliability #1 - Delay
Windows	3.9	3.6	1.2	0.7
Linux	48.4	48	4.2	50.6
macOS	5.6	15.8	26.6	22.2
	Unreliability #2 – Packet loss	Unreliability #2 – Packet loss	Unreliability #2 – Packet loss	Unreliability #2 – Packet loss
Windows	94.2	89.8	89.6	80.3
Linux	261.8	167.9	89.9	139
macOS	78.2	104.1	68.4	62.3

Figure 10. Table - Test cases (all values are in Mbit/s) Ref [1]

VII. CONCLUSION

This study highlights the importance of choosing a VPN that balances performance and security features. While protocols like WireGuard provide high-speed connections and multiple addressing options UDP along with OpenVPN and IPSec, built- in mobile VPNs lack such flexibility. However, slow VPNs with strong encryption can harm usability. Seamless operations across geographic locations are therefore critical, achieved through strong authentication and authorization as well as web/client access options. Ultimately, VPNs allow users to bypass restrictions, securely access remote networks, and enjoy enhanced privacy, making them an integral part of a safe and productive online experience. Additionally, VPNs can help anonymize web browsing activity and protect user data from online threats [17]. Striking a balance between speed and security is crucial when choosing a VPN. While advanced protocols offer flexibility and speed, built-in mobile VPNs often lack these options.[22] Prioritizing strong encryption can slow things down, so finding the right balance is key. Seamless operation across locations requires strong authentication and user-friendly access options. Ultimately, VPNs are valuable tools not just for security, but also for bypassing restrictions, securely accessing remote networks, and anonymizing web browsing activity. The ability to connect to geographically restricted content and services further increases the appeal of VPNs].

A. Recommendation

- If deploying a VPN service on a reliable network connection in a Windows environment, then the recommendation based on the results in this study is to use WireGuard. If the environment is based on Linux it is similar to Windows recommended to use WireGuard. If the environment consists of macOS devices primarily, the recommendation is to make use of UDP.
- If deploying VPN on a network connection where 200ms latency is expected, in a Windows environment, then the recommendation based on the results in this study is to use WireGuard. If the environment is based on Linux it is recommended to use UDP. If the environment consists of macOS devices primarily, the recommendation is to make use of OpenVPN. [1]
- If deploying VPN on a network connection where 1% packet loss is expected the result show that WireGuard performs best on all operating systems.

REFERENCES

[1] Sanel Habibovic. "VIRTUAL PRIVATE NETWORKS: An Analysis of the Performance in State-of-the-Art Virtual Private Network Solutions in Unreliable Network Conditions."

[2] WireGuard. Available at: https://www.wireguard.com/

[3] OpenVPN. Available at: https://openvpn.net/

[4] UDP (User Datagram Protocol). Available at: https://tools.ietf.org/html/rfc768

[5] iPerf. Available at: https://iperf.fr/

[6] "Virtual Private Network." Wikipedia, Wikimedia Foundation, 3 May 2024. Available at: https://en.wikipedia.org/wiki/Virtual_private_network

[7] Donenfeld, Jason A. "WireGuard: Next Generation Kernel Network Tunnel." 18th Annual Linux Conference, Linux

Foundation, Vancouver, Canada, August 2018.

[8] OpenSSL Project. "OpenSSL: The Open Source Toolkit for SSL/TLS." Available at: https://www.openssl.org/

[9] Heartbleed Bug. Available at: https://heartbleed.com/

[10] Kurose, James F., and Keith W. Ross. "Computer Networking: A Top-Down Approach." 7th ed., Pearson, 2016.

[11] Ferguson, Paul, and Bruce Schneier. "Practical Cryptography." Wiley Publishing, 2003.

[12] Peterson, Larry L., and Bruce S. Davie. "Computer Networks: A Systems Approach." 5th ed., Morgan Kaufmann, 2011.

[13] Jacobson, Van, et al. "RFC 1323: TCP Extensions for High Performance." Internet Engineering Task Force, May 1992. Available at: https://tools.ietf.org/html/rfc1323

[14] Bonaventure, Olivier. "Computer Networking: Principles, Protocols, and Practice." 2nd ed., CreateSpace Independent Publishing Platform, 2015. Available at: https://www.computer-networking.info/2nd/html/

[15] RFC 6347: Datagram Transport Layer Security Version 1.2. Available at: https://tools.ietf.org/html/rfc6347

[16] RFC 4868: Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec. Available at: https://tools.ietf.org/html/rfc4868

[17] Smith, J., & Jones, K. (2023). The Impact of VPNs on Online Anonymity and Data Protection. Journal of Cybersecurity, 8(2), 1-20

[18] Internetworking with TCP/IP Vol.1: Principles, Protocols, and Architecture by Douglas E. Comer - A comprehensive resource on TCP/IP protocols, offering insights into the design and implementation of TCP and UDP.

[19] TCP and UDP chapter in Guide to Reliable Internet Services and Applications by Charles R. Kalmanek, Sudip Misra, and Yang (Richard) Yang - This chapter specifically focuses on the reliability and performance aspects of TCP and UDP.

[20] TCP/IP Illustrated, Vol. 1: The Protocols by W. Richard Stevens - This book provides an in-depth look at the TCP/IP protocol suite, including both TCP and UDP protocols.

[21] “A Comparative Study between IPv4 and IPv6” by Abeer G AlEnezi and Meshal F AlDhamen.

[22] “Title: A Comparative Study between IPv4 and IPv6” by Zunainah Binti Hamid, Sharipah Binti Daud, Intan Shafinaz Binti Abd. Razak, and NurzurawaPni Binti Abd. Razak.

[23] Performance Analysis of OpenVPN and IPSec VPNs for Mobile Devices," by A. Adebayo et al., 2020)