# Security at Network Layer - IPSec and VPNs

Muhammad Shaheer
*Electrical and Computer Engineering*
*Habib University*
Karachi, Pakistan
Email: ms07552@st.habib.edu.pk

Hussain Mustansir
*Computer Science and Engineering*
*Habib University*
Karachi, Pakistan
Email: hm08436@st.habib.edu.pk

M. Arsalan Hussain
*Electrical and Computer Engineering*
*Habib University*
Karachi, Pakistan
Email: ms07607@st.habib.edu.pk

Ziaullah Shakeel
*Electrical and Computer Engineering*
*Habib University*
Karachi, Pakistan
Email: zs07752@st.habib.edu.pk

Sir Tariq Mumtaz
*Electrical and Computer Engineering*
*Habib University*
Karachi, Pakistan
Email: tariq.mumtaz@sse.habib.edu.pk

***Abstract*—Network security has grown significantly in recent years as cyber threats continue to evolve and target critical infrastructures, businesses, and individuals. Secure communication over public networks is no longer a luxury but a necessity in safeguarding sensitive information. VPNs, or Virtual Private Networks, have emerged as one of the fundamental solutions for ensuring data security over the internet by creating encrypted tunnels between endpoints. This study aims to explore the landscape of network security at the network layer, examine traditional solutions like IPSec, and evaluate modern alternatives like WireGuard.**

***Index Terms*—Virtual Private Networks, Cloud Networks, WireGuard, IPSec**

## I. Introduction

The Internet is one of the most important assets in the present times. With loads of data accessible through the internet in seconds, the connection enables us to perform our everyday office tasks, communicate, run businesses, or just scroll on social media. The most typical method for internet access is Wi-Fi. However, with Wi-Fi, the threat of data security and exploitation also resides. That is not the only setback of having a virtual connection. The internet can be very easily limited to a variety of content by authorities such as government and security organizations.

To protect from such troubles, VPNs can be established. VPN, abbreviated for Virtual Private Network, is a method of personal virtualization by creating a closed user group (CUG). It is a privacy-induced network, typically constructed from the public global internet. VPN enables users to access data by being essentially invisible to an external observer. Private organizations use VPNs to protect their data from intruders.

In Pakistan, the growing importance of network security encourages developments in this field. Bans posed by the governmental authorities on the usage of VPNs cause uninvited tension for accessibility and security for businesses and organizations that run on VPNs. The government's efforts are fundamental in controlling the use of VPNs in the promotion of cybercrime and terrorism. However, these restrictions pose significant challenges for individuals who rely on VPNs for secure and uninterrupted communication. Such measures demonstrate the critical need for robust and adaptive network security solutions in a country like Pakistan to succeed in a rapidly evolving digital landscape.

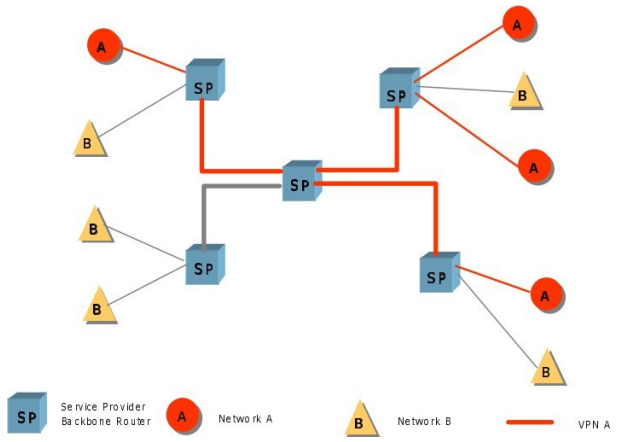


Fig. 1. VPN Projection Chart

## II. What are VPNs

A Virtual Private Network (VPN) is a secure and encrypted tunnel between a user and a server operated by a VPN service provider. By routing public internet traffic through this tunnel, a VPN ensures the protection of user data from potential trackers. The IP address of the VPN server acts as the user's virtual identity, effectively masking their actual location and identity.

VPNs typically employ the IPSec protocol suite to establish and maintain encrypted connections. However, other protocols, such as SSL/TLS, are also used, operating at different layers of the OSI model. In recent years, WireGuard has gained popularity as a modern and efficient alternative to IPSec, offering enhanced encryption performance.

Initially, VPNs were developed to address the growing need for faster and more flexible networking solutions for busi-

nesses. Enterprises required tools to improve communication efficiency, enhance security, scale operations, and increase profitability. VPNs rely on Internet Service Providers (ISPs) and Network Service Providers (NSPs) to create encrypted, dedicated communication channels, referred to as logical Virtual Private Networks.

### A. Applications of VPNs

VPNs play a pivotal role in ensuring data privacy and security across a wide range of applications:

- **Corporate Networks:** Organizations deploy VPNs to allow employees to securely access internal resources while working remotely.
- **Bypassing Geographical Restrictions:** VPNs enable users to access content that is geographically restricted, such as streaming services or censored websites.
- **Enhanced Privacy:** VPNs protect users' online activities from surveillance and tracking by masking their IP addresses.
- **Secure Communication:** VPNs provide a secure communication channel for transmitting sensitive data, ensuring confidentiality and integrity.

### B. Key Technologies Shaping Modern VPNs

- **Data Compression and Packet Technology:** This technology re-encrypts plaintext packets to reduce redundancy, thereby improving transmission performance. By compressing application-layer data, VPNs achieve faster and more efficient communication compared to plaintext transmission.These methods have become integral to many modern VPN solutions.
- **Multiline Multiplexing and Smart Routing Technology:** This technology enables VPN devices to support multiple Wide Area Network (WAN) lines simultaneously. By bundling these lines, users benefit from increased bandwidth and reliability. Multi-line backup ensures uninterrupted connectivity, as remaining lines maintain network availability even if one or more lines fail.

## III. Overview Of IPSec

Internet Protocol Security, abbreviated as IPSec, is a protocol or an extension that provides security to IP communications via the Public Internet at the Network Layer created by IETF. This can be accomplished in three different scenarios:

- Gateway-to-Gateway: Enterprise Level
- Host-to-Gateway: Remote Access Level
- Host-to-Host: End-to-End

IPSec's operations are based on the Internet Key Exchange (IKE) protocol. This facilitates the security associations between peers and ensures a secure exchange of cryptographic keys and negotiates.

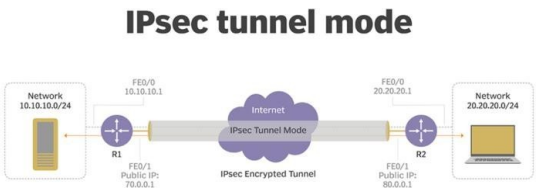


Fig. 2. IPSec Tunnel

## IV. WireGuard: The Modern VPN Standard

WireGuard is a modern VPN protocol that was started by Jason A. Donenfeld as an attempt to replace the existing IPSec-induced VPN protocols such as L2TP or OpenVPN. Over the years of rigorous analysis by multiple researchers, the other IPSec solutions were accused of being rather complex and weak. The protocols were not satisfying the security requirements for IP as they were supposed to.

To address the abovementioned issues, WireGuard was birthed holding a simple aim which was to provide simpler, quicker, and more secure protocol as an alternative to the existing ones.

WireGuard employs immaculate cryptographic techniques to ensure secure communication while maintaining the minimal codebase possible to ensure enhanced performance and reduced attack surface. The ease of configuration and support for both IPv4 and IPv6 networks make it an appealing choice for modern network security needs. WireGuard encapsulates data using the UDP protocol and leverages peer-based key exchange for establishing secure connections.

Unlike IPSec, WireGuard maintains a persistent connection between peers, making reconnections faster and more efficient. The simplicity of its configuration and its focus on ease of deployment make WireGuard a popular choice among enterprises and individual users alike.

### A. Core Features of WireGuard

WireGuard utilizes an architecture that prioritizes ease of use and performance. It is composed of the following mechanisms at its core:

**Noise Protocol Framework:** WireGuard relies on the Noise Protocol for its initial baseline. The Noise Protocol is a cryptographic framework that ensures key exchange with minimal latency. The algorithm used for this process is Curve25519, enabling the derivation of a shared symmetric key for encryption and decryption.

**Static Key Infrastructure:** WireGuard uses static public keys for identification and authentication of peers. These keys are not used for actual session encryption but are part of the initial handshake process to establish a secure connection.

**ChaCha20 Encryption:** Unlike IPSec, which uses AES, WireGuard encrypts data with the ChaCha20 cipher. This symmetric cipher is highly efficient, offering excellent performance even on devices with limited computational power.

**Poly1305 Authentication:** WireGuard employs the Poly1305 algorithm for message authentication, ensuring the confidentiality and integrity of the data.

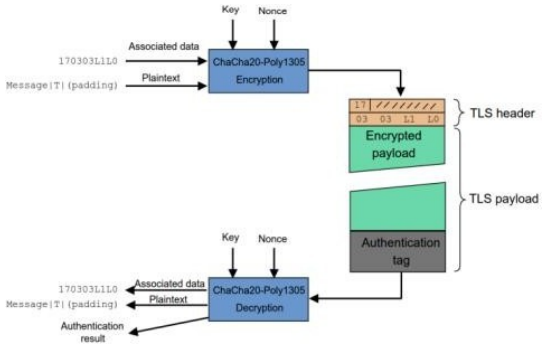


Fig. 3. Encryption in WireGuard

### B. Advantages of WireGuard over IPSec

WireGuard, as compared to IPSec, offers various advancements, making it more efficient and organized. Below are a few benefits of using WireGuard:

**Simplicity:** With approximately 4,000 lines of code, WireGuard's codebase is remarkably concise and compact compared to IPSec's complexity. This simplicity effectively reduces the likelihood of implementation errors.

**Performance:** The ChaCha20 algorithm and minimalistic handshake process significantly enhance the performance and speed of WireGuard by reducing latency compared to IPSec.

**Seamless Mobility:** WireGuard maintains active connections without interruption, unlike IPSec, which requires renegotiation when switching networks. This provides a smooth user experience.

**Cross-Platform Support:** WireGuard's compatibility with various platforms, including Linux, Windows, macOS, and mobile systems, makes it versatile and accessible. In contrast, IPSec primarily targets enterprise environments, such as organizational support.

### C. Challenges of WireGuard

Despite its benefits, WireGuard also presents certain challenges:

**Static Key Limitation:** WireGuard's reliance on static keys for configuration can complicate dynamic key management in large-scale deployments.

**Limited Flexibility:** While IPSec offers extensive configuration options, such as different encryption algorithms and tunnel modes suitable for highly customized setups, WireGuard's simplicity comes at the expense of such flexibility.

**No Built-in IP Address Assignment:** WireGuard cannot handle IP address assignments on its own. It requires external tools or scripts for managing IPs in multi-client environments.

### D. Why WireGuard is Becoming the New Standard

WireGuard's design philosophy aligns with the needs of modern network security. It is highly functional in scenarios requiring high performance. With its lightweight architecture, WireGuard becomes ideal for mobile devices and embedded systems. Additionally, its robust security framework effectively addresses contemporary threats.

WireGuard's popularity continues to grow due to its focus on simplicity and speed without sacrificing security, making it a preferred choice over traditional VPN protocols like IPSec.

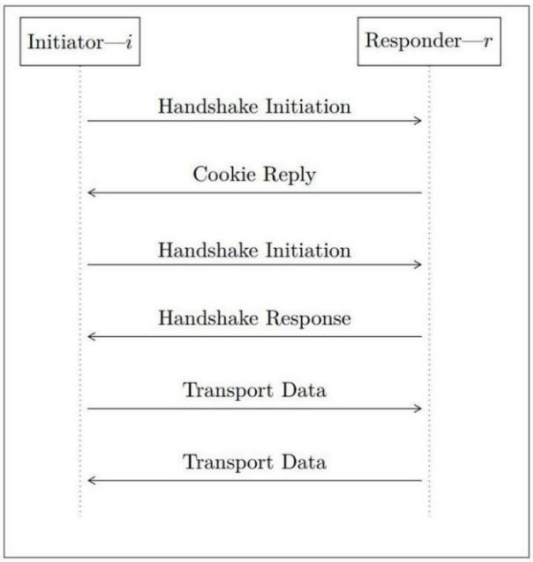


Fig. 4. Visualizing WireGuard's Mechanisms

## V. WireGuard Implementation

WireGuard's implementation on platforms like AWS EC2 involves configuring the server environment, setting up secure communication channels, and enabling client connectivity. The process includes the following steps:

### A. Server-Side Implementation

1) Begin by selecting a stable operating system, such as Ubuntu, and adding a security rule in its security group to allow all traffic from any IP address (0.0.0.0/0) on UDP port 51820. This is integral for internet access when creating the WireGuard tunnel.
2) Install the WireGuard package from trusted repositories and generate public and private key pairs for both the server and the clients. These keys facilitate secure peer-to-peer connections, with each peer identified by its public key.
3) Create a configuration file specifying the private key, the server's virtual address (usually `10.0.0.1/24`), and the Listen Port (`51820`) for the WireGuard tunnel. The tunnel is a virtual interface, typically named `wg0`, but it can be renamed (e.g., `wg7`).
4) Set up a `systemctl` service to ensure the WireGuard tunnel runs automatically upon system reboot. This is crucial since AWS EC2 instances may reboot as frequently as every eight hours.
5) Run the WireGuard server to verify that the protocol operates efficiently.

### B. Client-Side Implementation

The client-side implementation involves many similar steps:

1) Create configuration files specifying the server's endpoint, the client's private key, the client's virtual address (e.g., `10.0.0.2/24`), and the peer's public key (in this case, the server's public key).
2) Enable internet-bound traffic by applying routing configurations on the server, including IP forwarding and Network Address Translation (NAT).
3) Add the client to the server by specifying the client's public key and virtual address in the server configuration.
4) Run the tunnel command to activate the secure connection.
5) Test the connection by pinging `10.0.0.1`. The server should connect to the internet using the secure WireGuard tunnel.

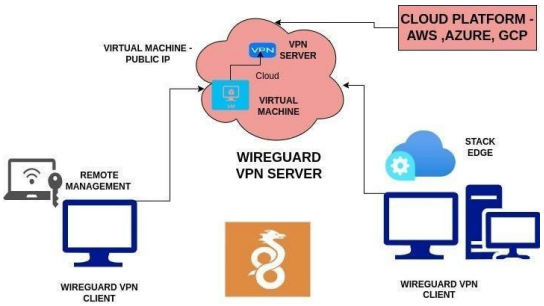


Fig. 5. Wireguard Design

## VI. Challenges and Future Directions

Despite the advancements in VPN technologies, several challenges remain. Government restrictions on VPN usage in some regions continue to limit their accessibility and effectiveness, making it harder for users to maintain privacy and security. In addition, legacy protocols like IPSec struggle to meet the scalability demands of modern, large-scale networks, which require more efficient and flexible solutions. As cyber threats continue to evolve rapidly, VPN protocols must constantly adapt and improve to counter emerging risks and maintain strong security.

Looking towards the future, there is a clear need for improved scalability in VPN technologies. Researchers should focus on developing new protocols capable of handling the increasing complexity of global networks without compromising performance. Another significant area of focus is the potential impact of quantum computing on cryptographic security. As quantum computers advance, existing encryption methods may no longer be secure, so VPN protocols will need to incorporate quantum-resistant encryption techniques.

## VII. Conclusion

This study examined traditional and modern VPN protocols, specifically IPSec and WireGuard, in the context of the evolving network security needs. While IPSec offers extensive flexibility and is wellsuited for complex, enterprise environments, its configuration complexity can be a drawback. In contrast, WireGuard's simplicity, efficiency, and modern cryptography make it a strong alternative, Figure 5: WireGuard Handshake Process Using the Noise Protocol Figure 4: VPN Topology particularly for latency-sensitive use cases. Each protocol serves distinct needs—IPSec for detailed, customizable security and WireGuard for speed and ease of use. The choice between them should be based on specific security requirements, performance needs, and ease of maintenance.

## References


[1] P. Wu, T. Lange, J. Appelbaum, and J. Donenfeld, "Analysis of the WireGuard protocol," Available online: https://www.lekensteyn.nl/files/pwu-wireguardthesis-final.pdf, 2019.

[2] J. A. Donenfeld, "WireGuard: Next Generation Kernel Network Tunnel," *Proceedings of the 2017 Network and Distributed System Security Symposium*, doi: https://doi.org/10.14722/ndss.2017.23160, 2017.

[3] P. Ferguson and G. Huston, "What is a VPN?," Available online: http://sol.te.net.ua/www/nanog/vpn.pdf, 1998.

[4] Z. Zhang, Y.-Q. Zhang, X. Chu, and B. Li, "An Overview of Virtual Private Network (VPN): IP VPN and Optical VPN," *Photonic Network Communications*, vol. 7, no. 3, pp. 213–225, 2004. doi: https://doi.org/10.1023/b:pnet.0000026887.35638.ce.

[5] Cloudflare, "What is IPsec?," Available online: https://www.cloudflare.com/learning/network-layer/what-is-ipsec/, n.d.

[6] P. Loshin, "What is IPsec (Internet Protocol Security)?," *SearchSecurity*, Available online: https://www.techtarget.com/searchsecurity/definition/IPsec-Internet-Protocol-Security, 2021.

[7] G. T. Menegueti, "Setting up a VPN with WireGuard Server on AWS EC2," *DEV Community*, Available online: https://dev.to/gabrieltetzner/setting-up-a-vpn-with-wireguard-server-on-aws-ec2-4a49, 2023.

[8] O. Adeyinka, "Analysis of problems associated with IPSec VPN Technology," *2008 Canadian Conference on Electrical and Computer Engineering*, doi: 10.1109/ccece.2008.4564875, 2008.

[9] H. Dhall, D. Dhall, S. Batra, and P. Rani, "Implementation of IPSec Protocol," *2012 Second International Conference on Advanced Computing & Communication Technologies*, doi: 10.1109/acct.2012.64, 2012.

[10] P. Eronen and C. Kaufman, "Internet Key Exchange Protocol Version 2 (IKEv2)," *RFC 7296*, Internet Engineering Task Force (IETF), 2014.