# Role of VPNs in Privacy and Secure Communication Report

**Task Objective:** To understand the role of VPNs in privacy and secure communication using online VPN clients such as ProtonVPN or Windscribe, and provide a detailed summary of VPN encryption and privacy features,

## 1. Introduction

This report serves as a technical and practical analysis of Virtual Private Network (VPN) technology. The primary objectives are to:

1. Demonstrate the core functionality of a VPN (IP address masking and encryption).
2. Analyze critical security features and protocols (No-Log Policy, Kill Switch, OpenVPN vs. WireGuard).
3. Summarize the essential benefits and limitations of using a VPN for personal and professional use.

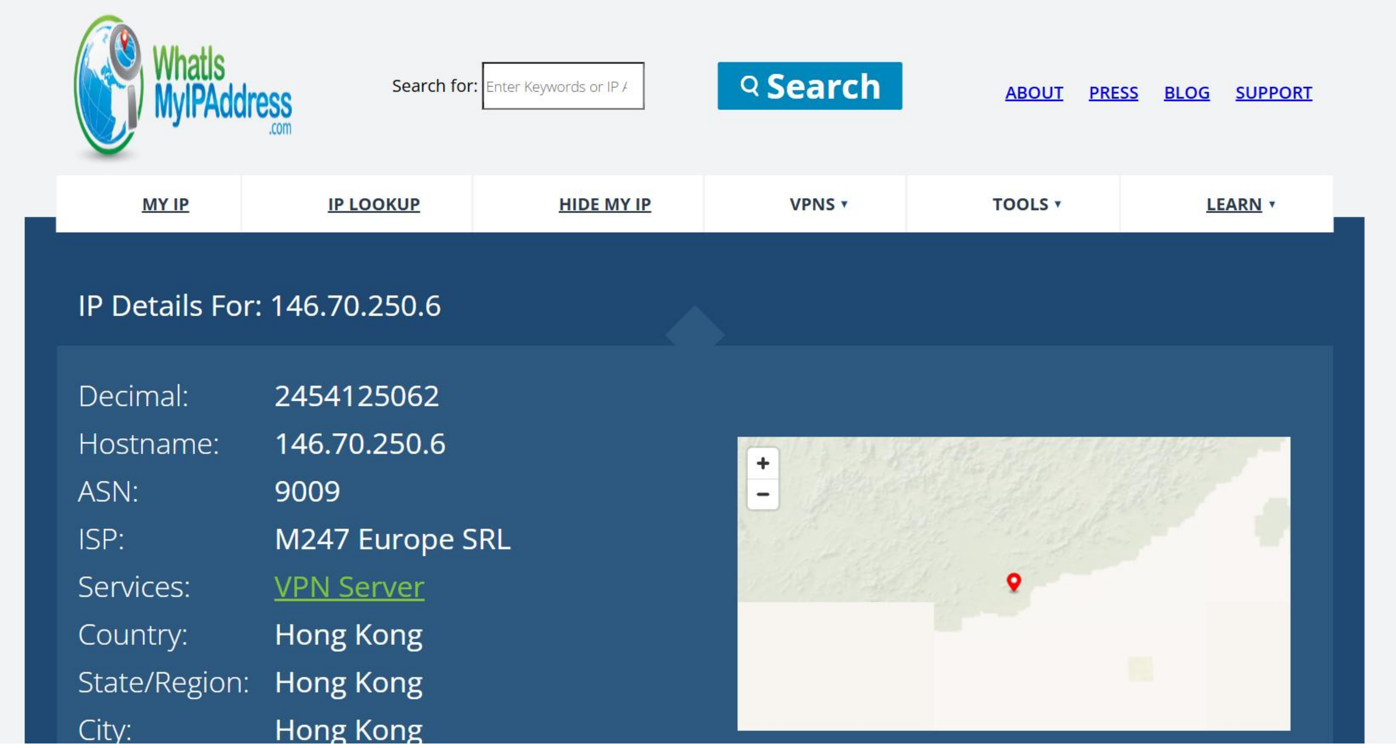
## 2. Practical Demonstration and Observation

### 2.1. VPN Setup and IP Address Verification

**VPN Service Used:** Windscribe (for demonstration purposes) **Server Location Used:** Hong Kong

A VPN connection was established from the user's local network to a remote server in Hong Kong. The primary function of a VPN—masking the user's real geographical location and IP address—was immediately verified using an external IP checker tool.

- **Evidence of Masking:** The IP checker website displayed an IP address originating from **Hong Kong**, successfully concealing the user's true location.



IP Details For: 146.70.250.6

| | |
|---|---|
| Decimal: | 2454125062 |
| Hostname: | 146.70.250.6 |
| ASN: | 9009 |
| ISP: | M247 Europe SRL |
| Services: | VPN Server |
| Country: | Hong Kong |
| State/Region: | Hong Kong |
| City: | Hong Kong |

### 2.2. Network Performance and Disconnection Test

After establishing the secure connection, observations were made regarding network performance and security integrity:

1. **Network Speed:** Due to the overhead of encryption and the significant distance to the Hong Kong server, a **noticeable, slight reduction in network speed** was observed. This confirms that increased latency and processing load are expected trade-offs for enhanced security.
2. **IP Integrity on Disconnect:** Upon manually disabling the VPN, the IP verification site instantly confirmed that the **original, local IP address had returned**. This successfully verified that the VPN client managed the tunnel effectively and did not leak the original IP address during the connection, returning to the default network state only upon explicit disconnection.

## 3. Technical Analysis and Key Privacy Features

A VPN's security effectiveness hinges on its underlying protocols and client-side features.

### 3.1. VPN Protocols: OpenVPN vs. WireGuard

Two primary protocols govern a VPN's tunnel establishment and encryption: **OpenVPN** and **WireGuard**. OpenVPN is a mature, highly flexible, open-source protocol that typically utilizes the AES-256 cipher. It is trusted for its **battle-tested security** but is generally **slower** due to its extensive codebase and high encryption overhead. In contrast, **WireGuard** is a newer, minimalist, open-source protocol, boasting a compact codebase of roughly 4,000 lines. It employs modern cryptography like ChaCha20, resulting in superior **speed and efficiency** and easier security auditing, which drives its rapid industry adoption.

### 3.2. Critical Privacy Safeguards

Critical client-side features ensure operational security, most notably the **No-Log Policy** and the **Kill Switch**. The **No-Log Policy** is a provider's contractual guarantee not to record user data, connection timestamps, or browsing history. This feature is vital for **ultimate privacy**, ensuring activity remains untraceable even under legal scrutiny. The **Kill Switch** provides an essential automatic safety net: if the encrypted VPN connection fails unexpectedly, the feature instantly blocks all internet traffic. This action is crucial because it **prevents leaks** by stopping the device from falling back to the unprotected, default network, which would expose the user's real IP and data.

## 4. Summary of VPN Benefits and Limitations (Task 8)

### 4.1. Key Benefits

VPNs are indispensable tools in modern digital life, providing benefits across security, privacy, and access:

- **Enhanced Security:** By encrypting all data, a VPN protects users from interception and cyber threats, particularly when using unsecured public Wi-Fi networks in cafes, airports, or hotels.
- **True Privacy:** VPNs mask the user’s real IP address and location, preventing surveillance and tracking by Internet Service Providers (ISPs), advertisers, and malicious third parties.

- **Bypassing Geo-Restrictions:** Users can connect to servers in different countries to access region-locked content, streaming services, or bypass internet censorship imposed by local networks or governments.
- **ISP Throttling Prevention:** By hiding the nature of the user's traffic (e.g., streaming or downloading), a VPN can prevent ISPs from selectively slowing down a user's connection based on activity.

### 4.2. Key Limitations

Despite the advantages, VPNs have inherent limitations that users must understand:

- **Performance Trade-off:** As observed in the demonstration, VPNs often introduce latency and a reduction in network speed due to the distance to the server and the computational cost of data encryption/decryption.
- **Not Total Security:** A VPN is not a replacement for comprehensive security software. It cannot protect against malware, viruses, phishing attempts, or data voluntarily shared by the user (e.g., on social media).
- **Blocking:** Certain high-security services, especially streaming platforms and financial institutions, employ sophisticated detection methods and may block known VPN IP addresses.
- **Trust in Provider:** The user must inherently trust that their VPN provider genuinely adheres to its No-Log Policy, as the provider sits in a privileged position to view the traffic if they choose to log it.

## 5. Conclusion

The practical demonstration confirmed the core functionality of IP masking and illustrated the common trade-off of speed for security. The technical analysis highlights that features like the Kill Switch and No-Log Policy are critical components defining a VPN's true value proposition. In summary, a VPN is an essential tool for bolstering online security and privacy, provided the user selects a reputable service and understands its performance limitations.