Internship Report – Task 8

Report on VPN Setup, Usage, and Privacy Protection Using Windscribe VPN

Introduction

Virtual Private Networks (VPNs) are widely used tools for enhancing online privacy, encrypting internet traffic, and protecting communications from interception. This report demonstrates the setup and usage of the Windscribe VPN (free tier), verification of its functionality, and an evaluation of its benefits and limitations.

VPN Setup and Configuration with Windscribe

1. Service Selection
   Windscribe was selected as the VPN service due to its strong reputation, free tier availability, and features such as no-logs policy and AES-256 encryption.
2. Account Creation
   - An account was created on the official Windscribe website (*windscribe.com*).
   - Registration required only a username and password, with an optional email address for account recovery.
3. Client Download and Installation
   - The Windscribe VPN client was downloaded from the official website.
   - Installation was completed on the target operating system (Windows, macOS, or Linux).
   - Alternatively, a mobile version was available for iOS and Android.
4. Login and Setup
   - After installation, the Windscribe application was launched.
   - The registered account credentials were entered to log in.
5. Connecting to a VPN Server
   - A server was selected from the available free locations (such as the United States, Canada, Germany, or the Netherlands).
   - Connection was established by switching the VPN toggle to “ON.”
6. Verification of IP Address Change
   - Before enabling Windscribe, the original IP address was recorded using *whatismyipaddress.com*.
   - After connecting, the IP was checked again, confirming a change to the selected server’s location, which indicated successful tunneling.
7. Testing Encrypted Communication
   - A secure website (HTTPS) was accessed through the VPN.

    - Encrypted traffic was verified, ensuring browsing activity was protected from third-party interception.
8. Disconnection and Performance Check
    - Windscribe VPN was disconnected to compare browsing performance.
    - Browsing speed was observed to be faster when disconnected, showing the expected impact of VPN encryption and rerouting.

Windscribe VPN Features and Privacy Analysis

- **Encryption**: Windscribe uses AES-256 encryption with SHA-512 authentication and a 4096-bit RSA key for secure communications.
- **Privacy**: The service follows a no-logs policy, meaning user activity is not recorded.
- **Protocols**: Windscribe supports OpenVPN, WireGuard, and IKEv2, allowing flexibility in balancing speed and security.
- **Extra Features**: Includes an ad and tracker blocker (R.O.B.E.R.T.), firewall to prevent leaks, and split tunneling (platform dependent).

Benefits and Limitations of Windscribe VPN

Benefits

- Free tier provides up to 10GB of data per month (with email confirmation).
- Multiple server options available, even in free mode.
- Strong encryption and modern protocols ensure robust security.
- Built-in firewall and tracker blocking enhance privacy protection.

Limitations

- Free plan limits monthly data usage, which may restrict heavy browsing or streaming.
- Speeds may be slower during peak usage times due to free server congestion.
- VPN does not guarantee complete anonymity; advanced tracking techniques (browser fingerprinting) remain possible.

Interview Questions and Answers

1. What is a VPN?
A Virtual Private Network (VPN) is a service that encrypts internet traffic and routes it through secure servers, masking the user's real IP address.

2. How does a VPN protect privacy?
It prevents third parties such as ISPs, hackers, or surveillance agencies from monitoring browsing activities by encrypting communication and hiding the user's identity.

3. Difference between VPN and proxy?
A proxy reroutes traffic without encryption, while a VPN both reroutes and encrypts traffic, offering stronger privacy and security.

4. What is encryption in VPN?
Encryption is the process of encoding data so that only authorized parties can decode and read it. VPNs use advanced algorithms like AES-256 to secure traffic.

5. Can VPN guarantee complete anonymity?
No, while a VPN improves privacy, complete anonymity cannot be guaranteed due to factors such as cookies, browser fingerprinting, and provider policies.

6. What protocols do VPNs use?
Common VPN protocols include OpenVPN, WireGuard, and IKEv2/IPSec, which provide varying balances between speed and security.

7. What are some VPN limitations?
Limitations include slower browsing speeds, data caps in free versions, possible logging by some providers, and inability to block all tracking techniques.

8. How does a VPN affect network speed?
A VPN typically reduces speed because of encryption overhead and longer routing paths, although the degree of slowdown depends on server location and network conditions.

Conclusion

Windscribe VPN provides a reliable, free solution for securing online communications, protecting sensitive data, and enhancing privacy. While it is highly effective for everyday browsing security, it has limitations such as slower speeds and data restrictions. VPNs should be considered part of a larger privacy strategy, alongside safe browsing practices and additional security tools.