Interview Questions

1. What is a VPN?

A **Virtual Private Network (VPN)** is a security tool that creates an **encrypted tunnel** between your device and the internet. It routes your data through a secure server, masking your real IP address and location. This helps protect your online identity, prevent tracking, and ensure private communication across public or untrusted networks.

---

2. How does a VPN protect privacy?

A VPN protects privacy by **encrypting all the data** that travels between your device and the VPN server. This means internet service providers (ISPs), hackers, or third parties cannot view your browsing activity or intercept sensitive information. Additionally, since VPNs **hide your real IP address**, websites and trackers cannot accurately determine your identity or location.

---

3. Difference between VPN and Proxy

While both VPNs and proxies reroute your internet traffic, they differ in **security and scope**:

- A **Proxy** only masks your IP address for specific applications or browsers, but it **does not encrypt** the data.
- A **VPN**, on the other hand, encrypts **all network traffic** from your device and offers stronger privacy and security.
  In short, a proxy hides you, while a VPN **protects and hides** you.

---

4. What is encryption in VPN?

Encryption in VPN refers to the process of converting readable data (plaintext) into an unreadable form (ciphertext) so that only authorized parties can access it. VPNs commonly use **AES-256-bit encryption**, which is considered military-grade and virtually impossible to crack. This ensures that even if your data is intercepted, it remains meaningless to unauthorized users.

---

5. Can VPN guarantee complete anonymity?

No, a VPN cannot guarantee **complete anonymity**. While it significantly enhances privacy by masking your IP and encrypting data, certain activities like logging into social media accounts or

sharing personal information can still reveal your identity. Additionally, your VPN provider may retain connection logs depending on its policy. A **no-logs VPN** and good user habits together provide strong but not absolute anonymity.

---

6. What protocols do VPNs use?

VPNs use **tunneling protocols** to securely transmit data. Some common ones include:

- **OpenVPN:** Highly secure and widely supported.
- **WireGuard:** Modern, lightweight, and fast.
- **IKEv2/IPSec:** Offers stability and quick reconnections.
- **L2TP/IPSec:** Older but still used for compatibility.
  Each protocol balances **speed, security, and reliability** differently.

---

7. What are some VPN limitations?

While VPNs are powerful privacy tools, they have certain limitations:

- May cause a **drop in internet speed** due to encryption overhead.
- **Free VPNs** often have limited servers and questionable data policies.
- VPNs **cannot protect** against phishing or malware on their own.
- Some countries **block or restrict** VPN usage.
- Trust must be placed in the **VPN provider's integrity** and privacy policy.

---

8. How does a VPN affect network speed?

A VPN can **slightly reduce network speed** because data must first travel to the VPN server before reaching the destination, and the encryption process adds processing overhead. However, modern protocols like **WireGuard** minimize this impact. The actual speed difference depends on factors like server distance, server load, and encryption strength.