**INTERVIEW QUESTIONS**

**1. What Is a VPN?**

A **Virtual Private Network (VPN)** is a secure tunnel between your device and the internet. It encrypts your data and routes it through a remote server, masking your IP address and location. This helps protect your online identity, bypass geo-restrictions, and secure data on public networks.

**2. How Does a VPN Protect Privacy?**

A VPN enhances privacy by:

* **Encrypting your internet traffic**, making it unreadable to ISPs, hackers, or surveillance systems.
* **Masking your IP address**, so websites and trackers can’t easily identify or locate you.
* **Preventing ISP tracking**, since they only see encrypted traffic going to the VPN server.

**3. VPN vs Proxy: What’s the Difference?**

| **Feature** | **VPN** | **Proxy** |
| --- | --- | --- |
| **Encryption** | Yes (end-to-end) | No or limited |
| **IP Masking** | Yes | Yes |
| **Traffic Coverage** | Entire device | Specific apps or browsers |
| **Security Level** | High | Low |
| **Use Case** | Privacy, security, streaming | Bypassing geo-blocks, scraping |

**4. What Is Encryption in VPN?**

VPN encryption transforms readable data (plaintext) into unreadable code (ciphertext) using algorithms like **AES-256**. This ensures:

* Confidentiality during transmission
* Protection against interception
* Secure tunneling between your device and VPN server

**5. Can VPN Guarantee Complete Anonymity?**

No. While VPNs **enhance anonymity**, they don’t guarantee it:

* VPN providers can still see your traffic unless they enforce strict no-log policies.
* Cookies, browser fingerprinting, and logged-in accounts (e.g., Google, Facebook) can still track you.
* Payment methods and account info may link back to your identity.

**6. What Protocols Do VPNs Use?**

Common VPN protocols include:

| **Protocol** | **Security** | **Speed** | **Best Use Case** |
| --- | --- | --- | --- |
| **OpenVPN** | High | Moderate | General use, strong encryption |
| **WireGuard** | High | Fast | Mobile, gaming, modern VPNs |
| **IKEv2/IPSec** | Good | Fast | Mobile switching, stability |
| **L2TP/IPSec** | Moderate | Moderate | Legacy systems |
| **PPTP** | Low | Fast | Obsolete, not recommended |

**7. What Are Some VPN Limitations?**

* **Slower speeds** due to encryption and rerouting
* **No protection against malware or phishing**
* **Trust issues** with some providers logging data
* **Limited compatibility** with certain apps or devices
* **Blocked by some websites or services**
* **Not fully anonymous** (especially if logged into accounts)

**8. How Does a VPN Affect Network Speed?**

VPNs can **reduce speed** due to:

* **Encryption overhead**: Strong encryption like AES-256 takes processing time
* **Server distance**: Farther servers increase latency
* **Server load**: Crowded servers slow down performance
* **Protocol choice**: OpenVPN is secure but slower; WireGuard is faster