🔐 Technical Writeup: VPN Protocols (IPSec, OpenVPN, WireGuard)

📘 Introduction

A **Virtual Private Network (VPN)** extends a private network across a public one, allowing users to securely send and receive data as if their devices were directly connected to the private network. VPN protocols define the standards and rules used to establish secure connections and protect data in transit.

Three of the most widely used VPN protocols are:

- **IPSec** – an older but highly secure standard protocol suite.
- **OpenVPN** – an open-source, SSL/TLS-based VPN protocol.
- **WireGuard** – a modern, minimal, and high-performance VPN protocol.

2️⃣ OpenVPN

🔧 Overview:

- **Type**: Application-layer protocol
- **Encryption**: AES-256, ChaCha20, etc.
- **Use case**: Remote-access VPNs, cross-platform VPN clients

📡 Transport:

- Uses **SSL/TLS** for key exchange
- Runs over **UDP** (preferred) or **TCP**
- Can use **port 443** to bypass firewalls

🔐 Security:

- Authenticated with X.509 certificates or pre-shared keys
- Supports Perfect Forward Secrecy (PFS)
- Optional **TLS Auth (HMAC)** for additional security

🔄 Tunnel Types:

- **TUN** (layer 3 IP tunneling)
- **TAP** (layer 2 Ethernet bridging)

✅ Pros:

- Highly configurable and robust
- Open-source with large community support
- Works well in restrictive network environments

❌ Cons:

- Slightly slower than WireGuard
- More overhead and configuration complexity

📊 Comparison Table

Feature	IPSec	OpenVPN	WireGuard
OSI Layer	Network (L3)	Application (L5)	Network (L3)
Encryption	AES, 3DES	AES, ChaCha20	ChaCha20-Poly1305
Protocol	IP	TCP/UDP	UDP only
Performance	Moderate	Moderate	High
Configuration	Complex	Moderate	Simple
NAT Traversal	Needs NAT-T	Native Support	Native Support

Feature	IPSec	OpenVPN	WireGuard
Mobile Roaming	Poor	Moderate	Excellent
Codebase Size	Large	Large	Small (\~4K LOC)

🏁 Conclusion

Each VPN protocol has its strengths and best-use scenarios:

- **IPSec** is best for **site-to-site** corporate VPNs where security and compatibility are crucial.
- **OpenVPN** is a versatile, widely supported option for both site-to-site and client VPNs, particularly in **cross-platform** environments.
- **WireGuard** is emerging as the preferred choice for **speed, simplicity, and modern cryptography**, especially on **mobile and embedded devices**.

For most modern applications, **WireGuard** is a compelling choice unless compatibility or fine-grained control requires OpenVPN or IPSec.