Task 4: VPN Connectivity Setup on Linux

Objective:

To demonstrate the setup and connection of a Linux machine to a VPN using an .ovpn configuration file, simulating encrypted communication over a public or insecure network.

Overview:

Virtual Private Networks (VPNs) provide secure, encrypted tunnels for network traffic. There are multiple types of VPN solutions available:

- **Free VPNs** (e.g., VPNGate)
- **Paid VPNs** (e.g., NordVPN, ExpressVPN)
- **CLI-based VPNs** (OpenVPN)
- **GUI-based clients** (e.g., ProtonVPN GUI, NetworkManager integration)

Chosen Approach:

For task demonstration purposes, we chose **VPNGate**, a free VPN service offering publicly available .ovpn configuration files.

Implementation Steps:

1. **Downloaded an .ovpn file** from the VPNGate public server list.
    - Example used: vpngate_public-vpn-210.opengw.net_tcp_443.ovpn
2. **Tested the OpenVPN connection:**
3. sudo openvpn --config vpngate_public-vpn-210.opengw.net_tcp_443.ovpn
4. **Resolved Cipher Negotiation Error:**
    - Added required cipher to the OpenVPN config:
    - data-ciphers AES-256-GCM:AES-128-GCM:CHACHA20-POLY1305:AES-128-CBC
5. **Successfully connected to the VPN:**
    - Verified by checking new IP address and ensuring internet connectivity worked over the VPN tunnel.

Outcome:

- VPN tunnel successfully established between the Linux machine and the VPNGate server.
- Traffic was routed through the encrypted connection.
- This confirmed a secure remote connection setup over an untrusted network, meeting the task's objectives.