**1. Prerequisites**

* **Your Computer:** This will host the VPN server (e.g., running Windows, Linux, or macOS).
* **Public IP Address:** You need a static public IP address or a dynamic DNS service to reach your VPN server from outside.
* **Firewall/Router Access:** Ensure you can configure your router to forward ports.
* **OpenVPN Software:** Install OpenVPN server software on your computer.

**2. Install OpenVPN Server**

**On Linux (e.g., Ubuntu)**

1. Update the system:

bash

Copier le code

sudo apt update && sudo apt upgrade

1. Install OpenVPN and Easy-RSA (for certificate management):

bash

Copier le code

sudo apt install openvpn easy-rsa

1. Set up Easy-RSA:

bash

Copier le code

make-cadir ~/openvpn-ca

cd ~/openvpn-ca

1. Configure and generate certificates for the server and clients.

**On Windows**

1. Download OpenVPN from the official website.
2. Install the software and the OpenVPN service component.
3. Use the Easy-RSA scripts (bundled with OpenVPN) to generate certificates.

**On macOS**

* Use Homebrew to install OpenVPN:

bash

Copier le code

brew install openvpn

* Follow the same certificate setup as Linux.

**3. Configure the OpenVPN Server**

1. **Create a Server Configuration File**:
   * Example: /etc/openvpn/server.conf (Linux/macOS) or place in C:\Program Files\OpenVPN\config (Windows).
   * Sample configuration:

conf

Copier le code

port 1194

proto udp

dev tun

ca ca.crt

cert server.crt

key server.key

dh dh.pem

server 10.8.0.0 255.255.255.0

push "redirect-gateway def1 bypass-dhcp"

push "dhcp-option DNS 8.8.8.8"

keepalive 10 120

cipher AES-256-CBC

user nobody

group nogroup

persist-key

persist-tun

verb 3

1. **Enable IP Forwarding**:
   * Linux: Edit /etc/sysctl.conf and set net.ipv4.ip\_forward=1.
   * Windows/macOS: Configure the system to allow packet forwarding.
2. **Set up NAT Rules**:
   * Linux: Use iptables for NAT forwarding.

bash

Copier le code

sudo iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -o eth0 -j MASQUERADE

* + Ensure the rule persists on reboot (use iptables-persistent or similar).

**4. Generate Client Profiles**

1. Create client certificates using Easy-RSA.
2. Bundle the keys into .ovpn files.
   * Example of a client .ovpn file:

conf

Copier le code

client

dev tun

proto udp

remote YOUR\_PUBLIC\_IP 1194

resolv-retry infinite

nobind

persist-key

persist-tun

remote-cert-tls server

cipher AES-256-CBC

verb 3

<ca>

# Insert contents of ca.crt here

</ca>

<cert>

# Insert contents of client.crt here

</cert>

<key>

# Insert contents of client.key here

</key>

**5. Configure Your Router for Port Forwarding**

1. Log in to your router's admin panel.
2. Forward port 1194 (UDP) to your VPN server's local IP address.
3. Save and apply the changes.

**6. Install OpenVPN Client**

* Install OpenVPN Connect (or any OpenVPN-compatible client) on your phone or computer.
* Import the .ovpn configuration file and connect.

**7. Test the Connection**

1. Ensure the VPN server is running:
   * On Linux: sudo systemctl start openvpn@server
   * On Windows: Start the OpenVPN service.
2. Use the client to connect.
3. Verify the connection by checking your public IP address (e.g., on [whatismyip.com](https://whatismyip.com)).