DOCUMENTATION

- **Setting up a VPN server using a Raspberry Pi 4 can be a great way to secure your internet connection and access your home network remotely. Here's a step-by-step guide to help you create a VPN server using Raspberry Pi 4**

  Note: Before you start, make sure you have a Raspberry Pi 4 (with Raspbian or Raspberry Pi OS installed), a stable internet connection

1) Update and Upgrade

- Connect to your Raspberry Pi via SSH or directly using a monitor and keyboard.
- Update the package list and upgrade the installed packages to the latest versions by running these commands.

```
sudo apt update
sudo apt upgrade
```

2) Install OpenVPN

- Install the OpenVPN server software.

```
sudo apt install openvpn
```

3) Generate Certificates and Keys

- Create a directory to store the OpenVPN configuration files and keys

```
mkdir ~/vpn-config
cd ~/vpn-config
```

- Generate the Diffie-Hellman key exchange file (this may take some time)

```
openssl dhparam -out dh.pem 2048
```

- Generate the root certificate authority (CA) certificate and key:

```
openssl genpkey -algorithm RSA -out ca-key.pem
openssl req -new -key ca-key.pem -x509 -out ca.pem -days 365
```

- Generate the server certificate and key:

```
openssl genpkey -algorithm RSA -out server-key.pem
openssl req -new -key server-key.pem -out server.csr
openssl x509 -req -in server.csr -CA ca.pem -CAkey ca-key.pem -out server-cert.pem -days 365
```

- Generate the HMAC signature.

```
openvpn --genkey --secret ta.key
```

4) Configure OpenVPN

- Copy the necessary files to the OpenVPN configuration directory.

```
sudo cp ~/vpn-config/{server-key.pem,server-cert.pem,ca.pem,dh.pem,ta.key} /etc/openvpn
```

- Copy the sample server configuration file and edit it.

```
sudo cp /usr/share/doc/openvpn/examples/sample-config-files/server.conf.gz /etc/openvpn/
sudo gzip -d /etc/openvpn/server.conf.gz
sudo nano /etc/openvpn/server.conf
```

- Uncomment the following lines in the config file.

```
push "redirect-gateway def1 bypass-dhcp"
push "dhcp-option DNS 208.67.222.222"
push "dhcp-option DNS 208.67.220.220"
```

- Enable IP forwarding to allow the VPN traffic to be routed.
- Edit the sysctl.conf file.

```
sudo nano /etc/sysctl.conf
```

- Uncomment the line: **net.ipv4.ip_forward=1,** Save and exit.
- Enable the change.

```
sudo sysctl -p
```

- Modify the IPTables to allow VPN traffic.

```
sudo iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -o eth0 -j MASQUERADE
sudo iptables-save | sudo tee /etc/iptables/rules.v4
```

- Enable OpenVPN to start on boot.

```
sudo systemctl enable openvpn
```

5) Start and Test the VPN Server

```
sudo systemctl start openvpn
```

- Check the status to ensure there are no errors.

  ```
  sudo systemctl status openvpn
  ```

- Test the VPN connection from a client device using an OpenVPN client. Import the client configuration file (you can use the .ovpn file created from the server configuration).

6) Configure Port Forwarding

- Log in to your router and set up port forwarding for UDP port 1194 (the default OpenVPN port) to the internal IP address of your Raspberry Pi.

7) Securing Your VPN

- Consider adding additional security measures such as using a strong passphrase for the server key, setting up a firewall, and regularly updating your system.