# **VPN Setup & Management**

We are going to use WireGuard as our VPN service for now, but it will change in the future.

## ****1. Setting Up the Script****

1. **Create the script file**:

vi vpn-setup.sh

1. **Copy and paste the script** into vpn-setup.sh.
2. **Make it executable**:

chmod +x vpn-setup.sh

1. **Move to a system path for easy access**:

sudo mv vpn-setup.sh /usr/local/bin/vpn-setup

## ****2. Commands and Usage****

### ****Install & Setup the VPN****

To install and configure WireGuard:

sudo vpn-setup install

* Installs WireGuard and required dependencies.
* Generates server keys.
* Configures the WireGuard server.
* Enables firewall rules and starts the VPN.

### ****Add a VPN Client****

To create a new client:

sudo vpn-setup add client\_name

* Generates keys for the client.
* Configures the WireGuard server to accept the client.
* Creates a client configuration file.
* Displays a QR code for mobile device setup.
* Logs the creation time.

### ****Remove a VPN Client****

To remove a client:

sudo vpn-setup remove client\_name

* Deletes the client’s configuration.
* Removes the client from the WireGuard server.
* Logs the removal time.

### ****Monitor Client Connections****

To log client connections:

sudo vpn-setup log

* Checks for active connections every **10 seconds**.
* Logs each successful handshake.

### ****Enable Auto-Logging on Boot****

This ensures the VPN is always running:

sudo vpn-setup service

* Creates a systemd service to run the logging script at boot.

## ****3. Configuration Details****

### ****Server Configuration (****/etc/wireguard/wg0.conf****)****

* **Server IP:** 10.0.0.1/24
* **Port:** 51820
* **Encryption:** Uses private/public key pairs
* **Public IP Detection:** Automatically detected via default network route.

### ****Client Configuration Example****

A generated client file (client\_name.conf) will look like this:

[Interface]

PrivateKey = CLIENT\_PRIVATE\_KEY

Address = 10.0.0.X/32

DNS = 1.1.1.1

[Peer]

PublicKey = SERVER\_PUBLIC\_KEY

Endpoint = SERVER\_IP:51820

AllowedIPs = 0.0.0.0/0, ::/0

PersistentKeepalive = 25

## ****4. Logging & Security Features****

✅ Logs when a client is added or removed.

✅ Logs client connection activity.

✅ Prevents duplicate script execution to avoid conflicts.

✅ Uses iptables for enhanced firewall security.

## ****5. Troubleshooting****

### ****Check the VPN Status****

sudo systemctl status wg-quick@wg0

### ****Restart the VPN****

sudo systemctl restart wg-quick@wg0

### ****Check VPN Logs****

sudo cat /var/log/wireguard\_client.log

## ****7. Connecting to the VPN****

### ****Get Your Client Configuration File****

Run the following command on your **WireGuard server** to generate a client configuration:

sudo vpn-setup add client\_name

This will create a client file at:

/etc/wireguard/clients/client\_name.conf

You need to transfer this file to your **client device**.

### ****Transfer the Configuration to Your Client****

#### ****Windows/Mac/Linux (via SCP or SFTP)****

If you're using a desktop computer, copy the config file using **SCP**:

scp username@your-server-ip:/etc/wireguard/clients/client\_name.conf ./

Replace username with your server username and your-server-ip with your VPS public IP.

#### ****Mobile (via QR Code)****

The script generates a **QR code**.

* Open the **WireGuard app** on your phone.
* Tap **Add Tunnel** > **Scan QR Code** and scan the generated QR code.

### ****Install WireGuard on Your Client****

#### ****Linux (Debian/Ubuntu)****

sudo apt install wireguard -y

#### ****Windows & Mac****

1. Download **WireGuard**
2. Install and open the WireGuard application.
3. Click **Add Tunnel** > **Import Configuration File** and select client\_name.conf.

#### ****Android & iOS****

1. Download **WireGuard** from the App Store/Google Play.
2. Open the app and **import the** .conf **file** or **scan the QR code**.

### ****Connect to the VPN****

Once the client configuration is added:

#### ****On Linux:****

sudo wg-quick up client\_name

To disconnect:

sudo wg-quick down client\_name

#### ****On Windows/Mac/Android/iOS:****

1. Open the WireGuard application.
2. Select the imported VPN profile.
3. Click **Activate / Connect**.

### ****Verify Your VPN Connection****

Check your **public IP address** before and after connecting:

curl -s ifconfig.me

If the IP changes to your **VPN’s IP**, your connection is successful.

#### **Updated on:** 7th February 2025