Wireguard Setup with Docker-compose and Digital Ocean

Table of Contents

Installation Process

- Sign up for a **new** account using this URL https://m.do.co/c/d33d59113ab6
- Gets you $200 credit for 2 months of usage

Create an Ubuntu 22.04

1. 2nd Cheapest Droplet = $6/mont
   - Ubuntu 22.04
   - Basic
   - Regular Intel CPU
   - Normal SSD
2. Choose either SSH key or Password
3. Open the terminal and connect to the ubuntu-server using the following command

```
ssh root@[ip-address]
```

ip-address - should be shown on the droplet.

Update and Upgrade

After connecting use the following command

```
sudo apt update && sudo apt upgrade -y
```

Install Docker and Docker-Compose

```
sudo apt install docker.io docker-compose -y
```

Setup folders and create .yml

Create directories for WireGuard configuration:

```
mkdir -p ~/wireguard/
mkdir -p ~/wireguard/config/
```

Creates the necessary directory structure for the WireGuard service.

Setup Wireguard in Docker-compose.yml

Edit the Docker Compose file:

```
sudo nano ~/wireguard/docker-compose.yml
```

Copy the following content in docker-compose.yml file:

```
version: '3.8'
services:
  wireguard:
    container_name: wireguard
    image: linuxserver/wireguard
    environment:
      - PUID=1000
      - PGID=1000
      - TZ=Etc/UTC
      - SERVERURL=1.2.3.4
      - SERVERPORT=52820
      - PEERS=pc1,phone1
      - PEERDNS=auto
      - INTERNAL_SUBNET=10.0.0.0
    ports:
      - 52820:52820/udp
    volumes:
      - type: bind
        source: ./config/
        target: /config/
      - type: bind
        source: /lib/modules
        target: /lib/modules
    restart: always
    cap_add:
      - NET_ADMIN
      - SYS_MODULE
    sysctls:
      - net.ipv4.conf.all.src_valid_mark=1
```

Description of Docker Compose File Configuration

`container_name`

- Names the container `wireguard` for easier management.

`image`

- Uses the `linuxserver/wireguard` Docker image.

`environment`

- Sets environment variables for container customization:
  - **`PUID` and `PGID`:** Set to `1000` for the user's default UID and GID.
  - **`TZ`:** Specifies the timezone (set to `Etc/UTC`).
  - **`SERVERURL`:** Public IP or domain of the WireGuard server (replace `1.2.3.4`).
  - **`SERVERPORT`:** Port for the WireGuard service (`52820`).
  - **`PEERS`:** List of client peers (e.g., `pc1`, `phone1`).
  - **`PEERDNS`:** Sets DNS resolution for peers (use `auto`).
  - **`INTERNAL_SUBNET`:** Defines the internal VPN subnet (e.g., `10.0.0.0`).

Ports

- Maps port `52820` on the host to `52820/udp` in the container.

Volumes

- **`/config`:**
  - Binds the local `./config/` folder to the container's `/config/` for persistent data.
- **`/lib/modules`:**
  - Binds the host's `/lib/modules` for kernel module access.

Restart Policy

- Automatically restarts the container if it stops.

Capabilities and System Controls

- **`cap_add`:**
  - Grants the container network management (`NET_ADMIN`) and kernel module loading (`SYS_MODULE`) capabilities.

- `sysctls`:
    - Configures network settings (`net.ipv4.conf.all.src_valid_mark=1`).

Testing the VPN

Start the WireGuard container:

```
cd ~/wireguard/
docker-compose up -d
```

Brings up the container in detached mode (-d). Check logs to get the QR code:

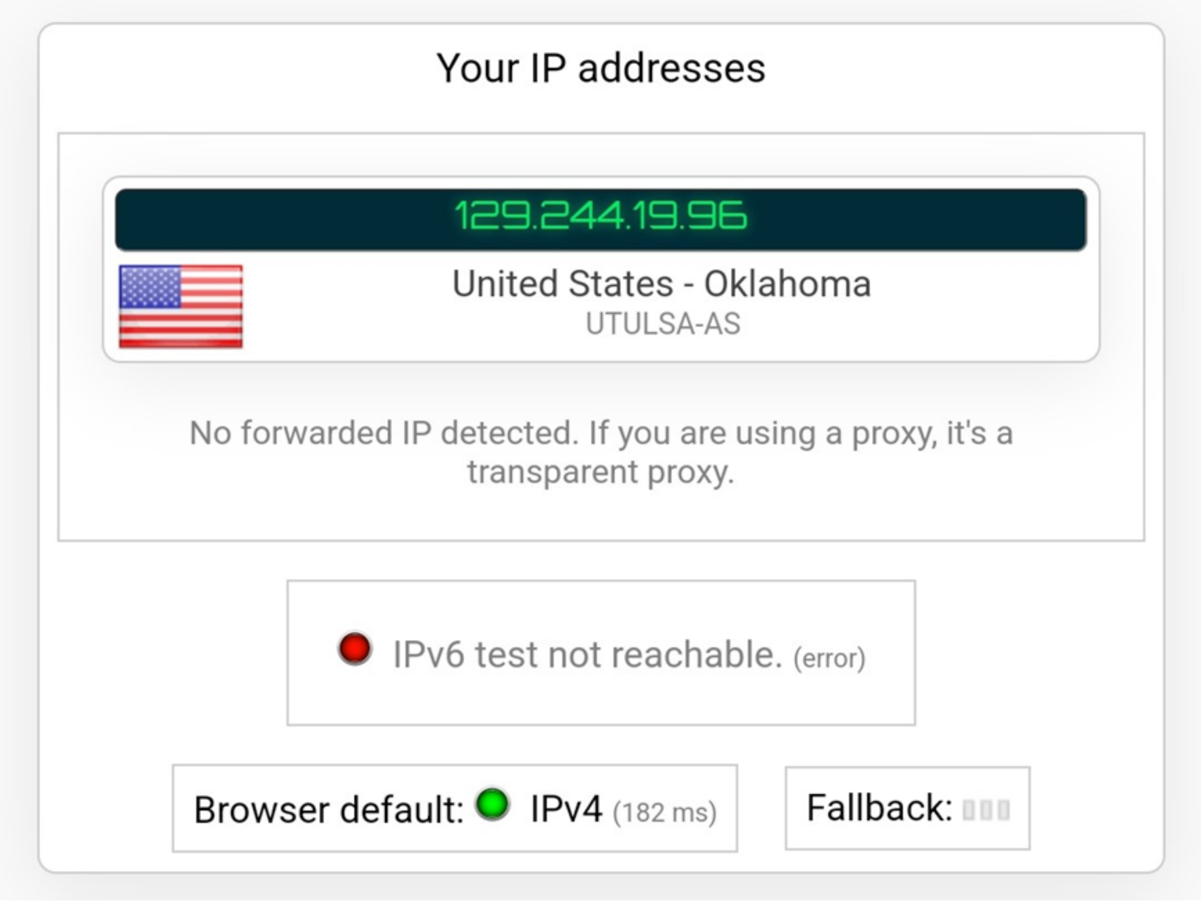
```
docker-compose logs -f wireguard
```

Configure and test VPN access on

- Mobile device: Import the peer configuration and test connectivity.
- Laptop: Set up the VPN connection and verify proper routing.

Mobile device

1. Open the Wireguard app and scan the QR code from the logs.
2. Before connecting:
    - Visit IPLeak.net and screenshot your local IP. The following screenshot shows the IP-Address:



Your IP addresses

129.244.19.96

United States - Oklahoma

UTULSA-AS

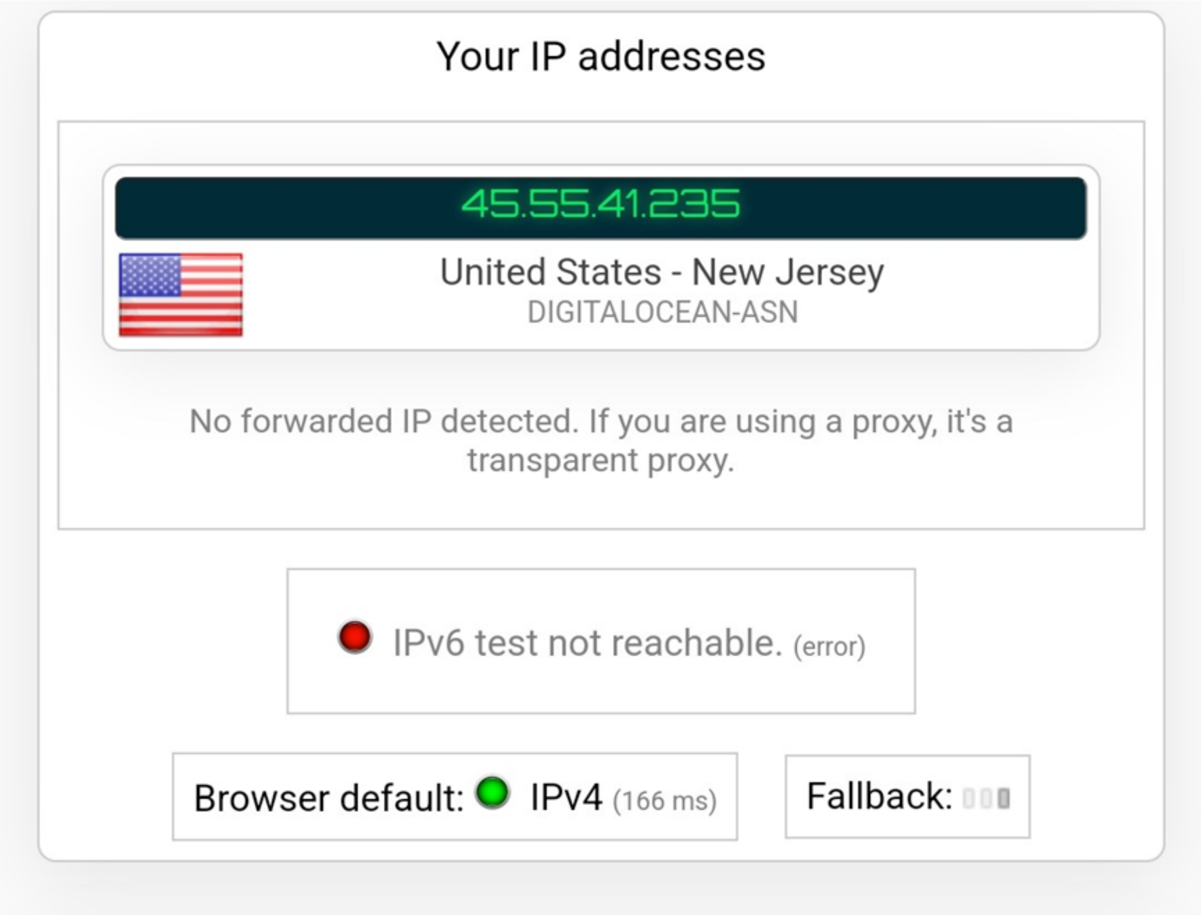
No forwarded IP detected. If you are using a proxy, it's a transparent proxy.

● IPv6 test not reachable. (error)

Browser default: ● IPv4 (182 ms)

Fallback:

3. After connecting:
   - Turn on the Wireguard VPN and revisit IPLeak.net
   - Screenshot of the VPN IP is shown below:



Your IP addresses

45.55.41.235

United States - New Jersey
DIGITALOCEAN-ASN

No forwarded IP detected. If you are using a proxy, it's a transparent proxy.

● IPv6 test not reachable. (error)

Browser default: ● IPv4 (166 ms)

Fallback:

Laptop

1. Setting Up the WireGuard Client for Ubuntu

```
sudo apt update
sudo apt install wireguard
```

2. Locate the WireGuard Configuration File

   To find the configuration file:

```
ls /opt/wireguard/config
```

3. Copy the Configuration File to Your Client

```
scp root@[ip-address]:/opt/wireguard/config/peer_pc1.conf ~/peer_pc1.conf
```

   or put the following content in `~/peer_pc1.conf`

```
[Interface]
PrivateKey = iLwC8xbCzwVd5j9s7Et/72d6keAAVTlkmxcY/wX6Ako=
ListenPort = 52820
Address = 10.0.0.2/32
DNS = 10.0.0.1

[Peer]
PublicKey = P5GnsQQZk4X0KilGkKNg5ND/XZjV0KP7QDNuShSCcG4=
PresharedKey = 5X6AWptfcPEHqhgi3nVlEb6vx833rLQic/ofI4TMy5s=
AllowedIPs = 0.0.0.0/0, ::/0
Endpoint = 45.55.41.235:52820
```

4. Import the Configuration File into WireGuard

   Use the WireGuard CLI:

   ```
   sudo wg-quick up ~/wireguard-client.conf
   ```

   To bring the interface down, use:

   ```
   sudo wg-quick down ~/wireguard-client.conf
   ```

5. Verify the VPN Connection Check WireGuard status- to verify that the VPN interface is up and running, use the following command:

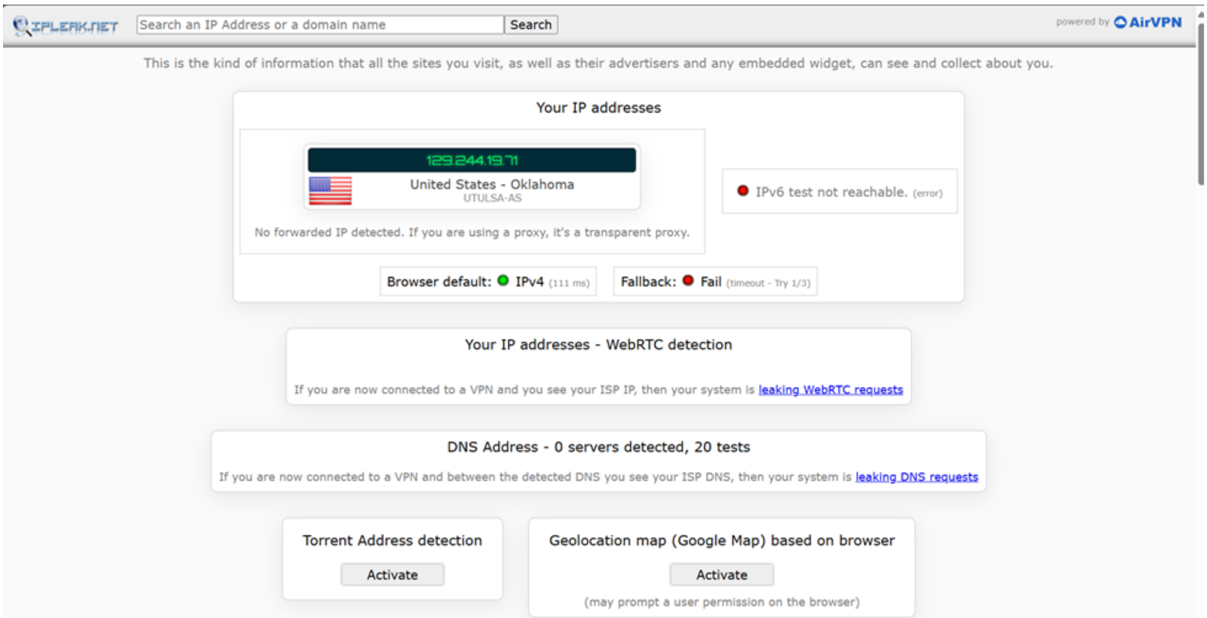
   ```
   sudo wg
   ```

6. Check IP address

   - Before connecting to the VPN - Go to IPLeak.net or run curl ifconfig.me in the terminal to see your current public IP.
   - After connecting to the VPN - Visit IPLeak.netagain or run curl ifconfig.me to confirm that your IP has changed to the VPN server's IP address.

References

- Setup Wireguard VPN server with Docker



This is the kind of information that all the sites you visit, as well as their advertisers and any embedded widget, can see and collect about you.

Your IP addresses

129.244.19.71
United States - Oklahoma
UTULSA-AS

No forwarded IP detected. If you are using a proxy, it's a transparent proxy.

● IPv6 test not reachable. (error)

Browser default: ● IPv4 (111 ms)

Fallback: ● Fail (timeout - Try 1/3)

Your IP addresses - WebRTC detection

If you are now connected to a VPN and you see your ISP IP, then your system is leaking WebRTC requests

DNS Address - 0 servers detected, 20 tests

If you are now connected to a VPN and between the detected DNS you see your ISP DNS, then your system is leaking DNS requests

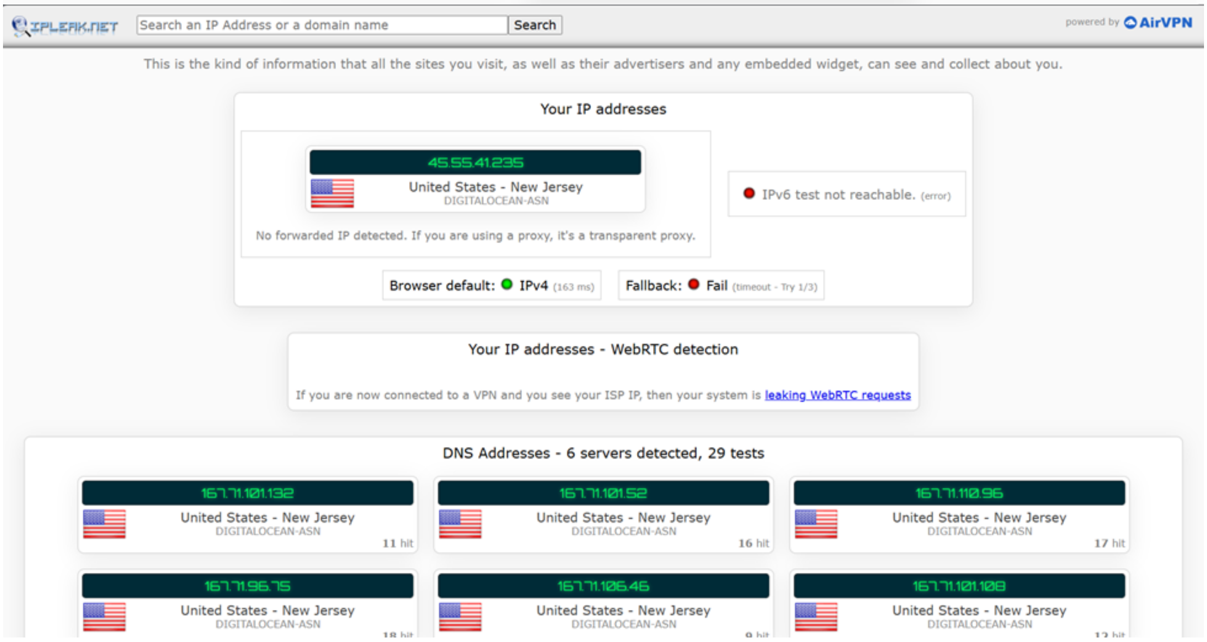
Torrent Address detection

Activate

Geolocation map (Google Map) based on browser

Activate

(may prompt a user permission on the browser)



This is the kind of information that all the sites you visit, as well as their advertisers and any embedded widget, can see and collect about you.

Your IP addresses

45.55.41.235
United States - New Jersey
DIGITALOCEAN-ASN

No forwarded IP detected. If you are using a proxy, it's a transparent proxy.

● IPv6 test not reachable. (error)

Browser default: ● IPv4 (163 ms)

Fallback: ● Fail (timeout - Try 1/3)

Your IP addresses - WebRTC detection

If you are now connected to a VPN and you see your ISP IP, then your system is leaking WebRTC requests

DNS Addresses - 6 servers detected, 29 tests

167.71.101.132
United States - New Jersey
DIGITALOCEAN-ASN
11 hit

167.71.101.52
United States - New Jersey
DIGITALOCEAN-ASN
16 hit

167.71.110.96
United States - New Jersey
DIGITALOCEAN-ASN
17 hit

167.71.96.75
United States - New Jersey
DIGITALOCEAN-ASN
18 hit

167.71.106.46
United States - New Jersey
DIGITALOCEAN-ASN
9 hit

167.71.101.108
United States - New Jersey
DIGITALOCEAN-ASN
12 hit