Summary

This guide will walk you through setting up a Wireguard VPN server on a Digital Ocean Droplet with a Windows laptop and an iPhone.

DigitalOcean Setup

1. Sign Up for a DigitalOcean Account

- New accounts on Digital Ocean are given $200 in credit for 60 days.

2. Create a Droplet

- Select the green "Create" button in the top right, then select "Droplets" from the dropdown menu

3. Choose an Image

- OS: Ubuntu
- Version: 24.04 (LTS) x64

4. Choose Size

- Droplet Type: Basic
- CPU options: Regular (SSD), $6/mo (the second option)

5. Choose Authentication Method

- I chose "Password" and generated and stored a password using Bitwarden

6. Finalize Details

- I customized the Hostname to be WireGuard so that it would look more appealing when working in the console
- Click "Create Droplet" in the bottom right

Install Docker Engine using the apt repository

These Instructions are based off of https://docs.docker.com/engine/install/ubuntu/

1. Set up Docker's apt repository.

```
# Add Docker's official GPG key:
sudo apt-get update
sudo apt-get install ca-certificates curl
sudo install -m 0755 -d /etc/apt/keyrings
sudo curl -fsSL https://download.docker.com/linux/ubuntu/gpg -o
/etc/apt/keyrings/docker.asc
sudo chmod a+r /etc/apt/keyrings/docker.asc
```

```
# Add the repository to Apt sources:
echo \
  "deb [arch=$(dpkg --print-architecture) signed-by=/etc/apt/keyrings/docker.asc] https://download.docker.com/linux/ubuntu \
  $(. /etc/os-release && echo "$VERSION_CODENAME") stable" | \
  sudo tee /etc/apt/sources.list.d/docker.list > /dev/null
sudo apt-get update
```

2. Install the Docker packages.

```
sudo apt-get install docker-ce docker-ce-cli containerd.io docker-buildx-plugin docker-compose-plugin
```

3. Verify that the Docker Engine installation is successful by running the hello-world image.

```
 sudo docker run hello-world
```

4. Add yourself to Docker Group (Optional but recommended)

```
sudo usermod -aG docker username
```

5. Check that Docker Installed Correctly

```
sudo docker run hello-world
```

6. Check that Compose Installed Correctly

```
sudo docker compose version
```

Setup WireGuard VPN Server with Docker

These Instructions are based off of https://thematrix.dev/setup-wireguard-vpn-server-with-docker/

1. Setup WireGuard

```
Run these on your server:

mkdir -p ~/wireguard/
mkdir -p ~/wireguard/config/
nano ~/wireguard/docker-compose.yml
```

Copy and paste the content below:

```
#version: '3.8'
services:
  wireguard:
    container_name: wireguard
    image: linuxserver/wireguard
    environment:
      - PUID=1000
      - PGID=1000
      - TZ=America/Chicago # Change this to your timezone
      - SERVERURL=1.2.3.4 # Change this to your server's IP address, note: this is located on your dashboard under ipv4
      - SERVERPORT=51820
      - PEERS=desktop,phone # Change these to the names you want to give your peers
      - PEERDNS=auto
      - INTERNAL_SUBNET=10.0.0.0
    ports:
      - 80:51820/udp # This was changed from 51820:51820/udp to avoid common blocks on residential internet connections.
    volumes:
      - ./config:/config
      - /lib/modules:/lib/modules
    restart: always
    cap_add:
      - NET_ADMIN
      - SYS_MODULE
    sysctls:
      - net.ipv4.conf.all.src_valid_mark=1
```

2. Start WireGuard

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

3. View The Logs

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

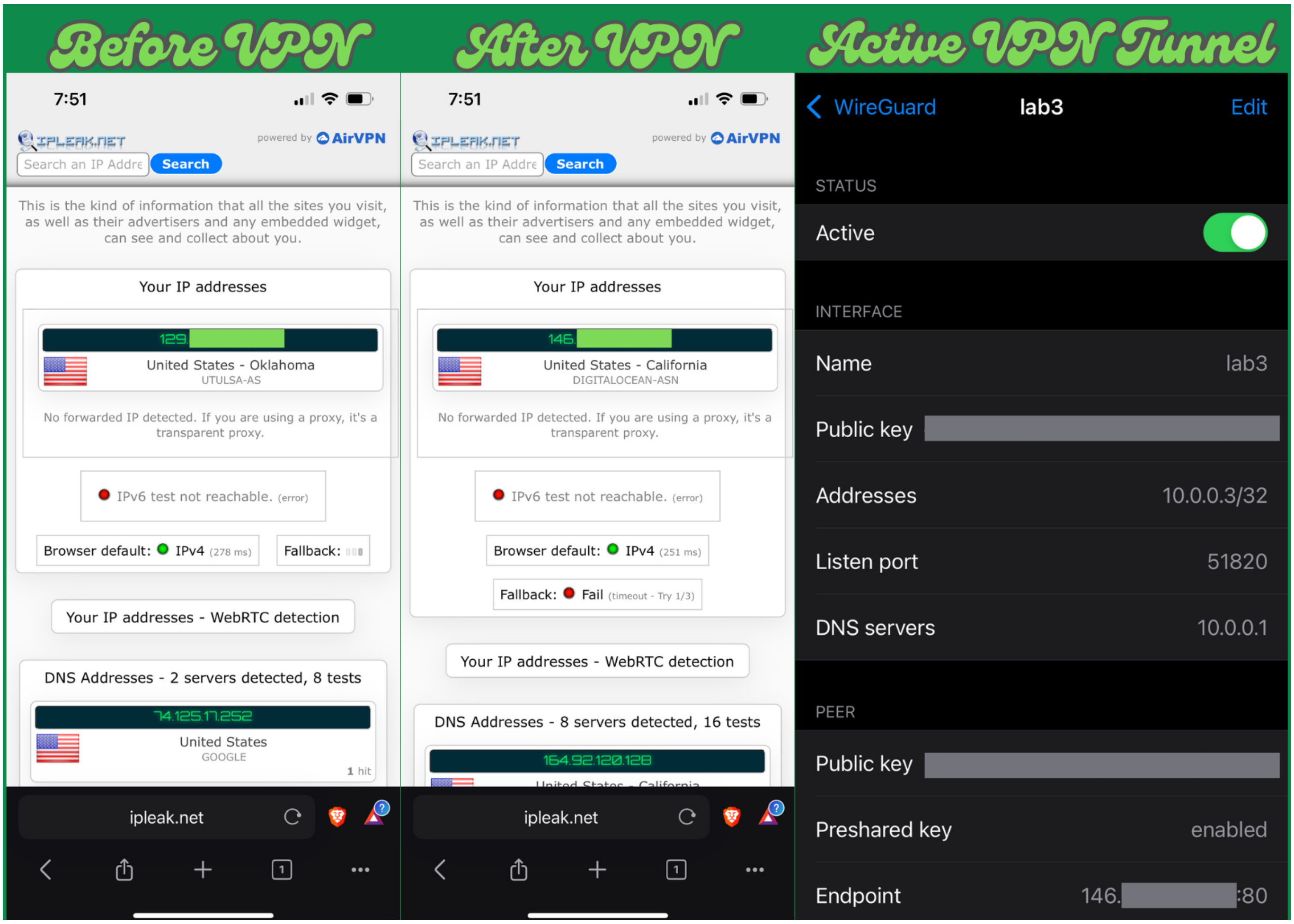
You will see the execution log, and QR codes of WireGuard VPN connection settings.

Connect your Phone to WireGuard

Open WireGuard VPN application on your phone, click +, Create from QR code

Since we changed the port to 80 instead of 51820, click on the vpn you just made, then click edit in the top right corner, then change the endpoint to the "your_ip:80"

To test that it is working check your localIP info in your WireGuard settings and visit IPLeak.net and compare them.



Before VPN

7:51

IPLEAK.NET powered by AirVPN

Search an IP Addre Search

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[redacted]

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 (278 ms) Fallback:

Your IP addresses - WebRTC detection

DNS Addresses - 2 servers detected, 8 tests

74.125.17.252
United States
GOOGLE
1 hit

ipleak.net

After VPN

7:51

IPLEAK.NET powered by AirVPN

Search an IP Addre Search

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

146[redacted]

United States - California
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 (251 ms)

Fallback: ● Fail (timeout - Try 1/3)

Your IP addresses - WebRTC detection

DNS Addresses - 8 servers detected, 16 tests

164.92.120.128
United States - California

ipleak.net

Active VPN Tunnel

< WireGuard lab3 Edit

STATUS

Active

INTERFACE

Name lab3

Public key [redacted]

Addresses 10.0.0.3/32

Listen port 51820

DNS servers 10.0.0.1

PEER

Public key [redacted]

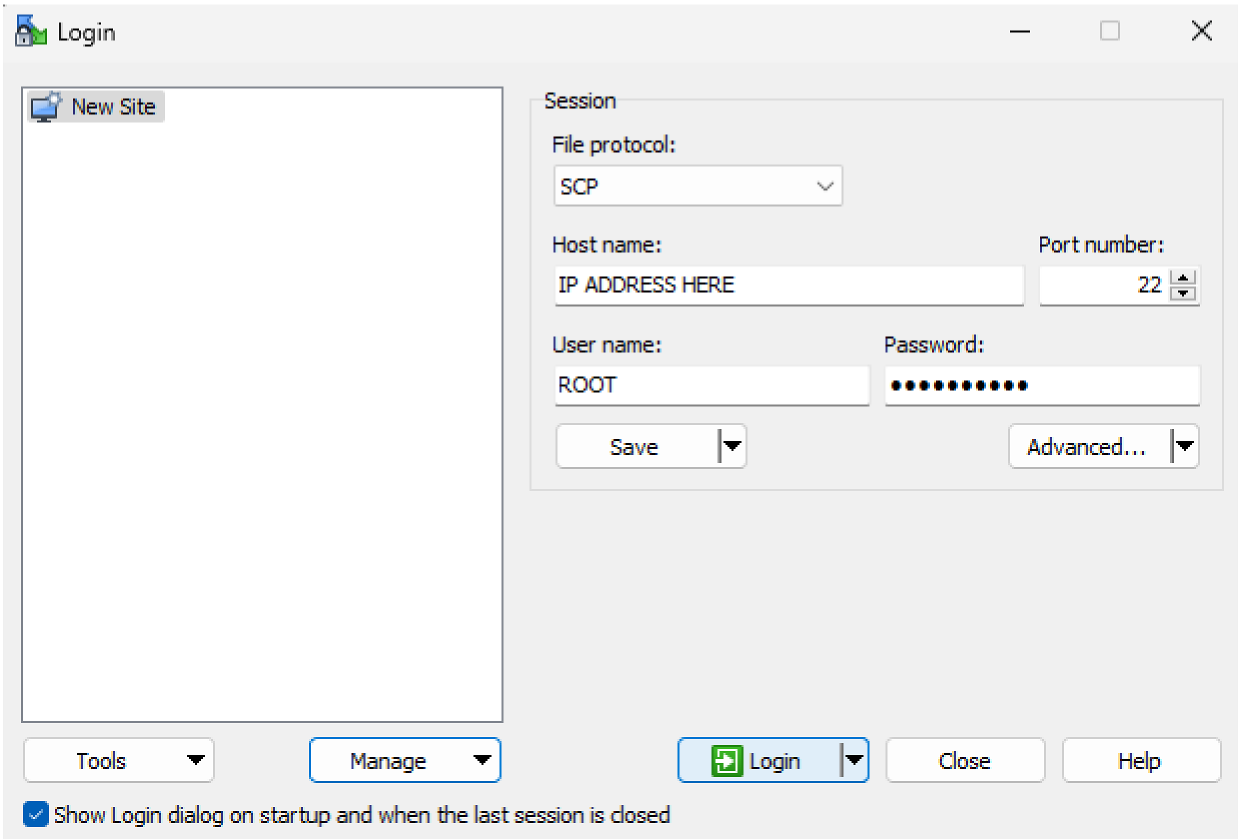
Preshared key enabled

Endpoint 146.[redacted]:80

Connect your laptop to WireGuard

Utilize WinSCP to copy over 'peer_desktop.conf'

Firstly, Set up your connection like so:



Session

File protocol: SCP

Host name: IP ADDRESS HERE

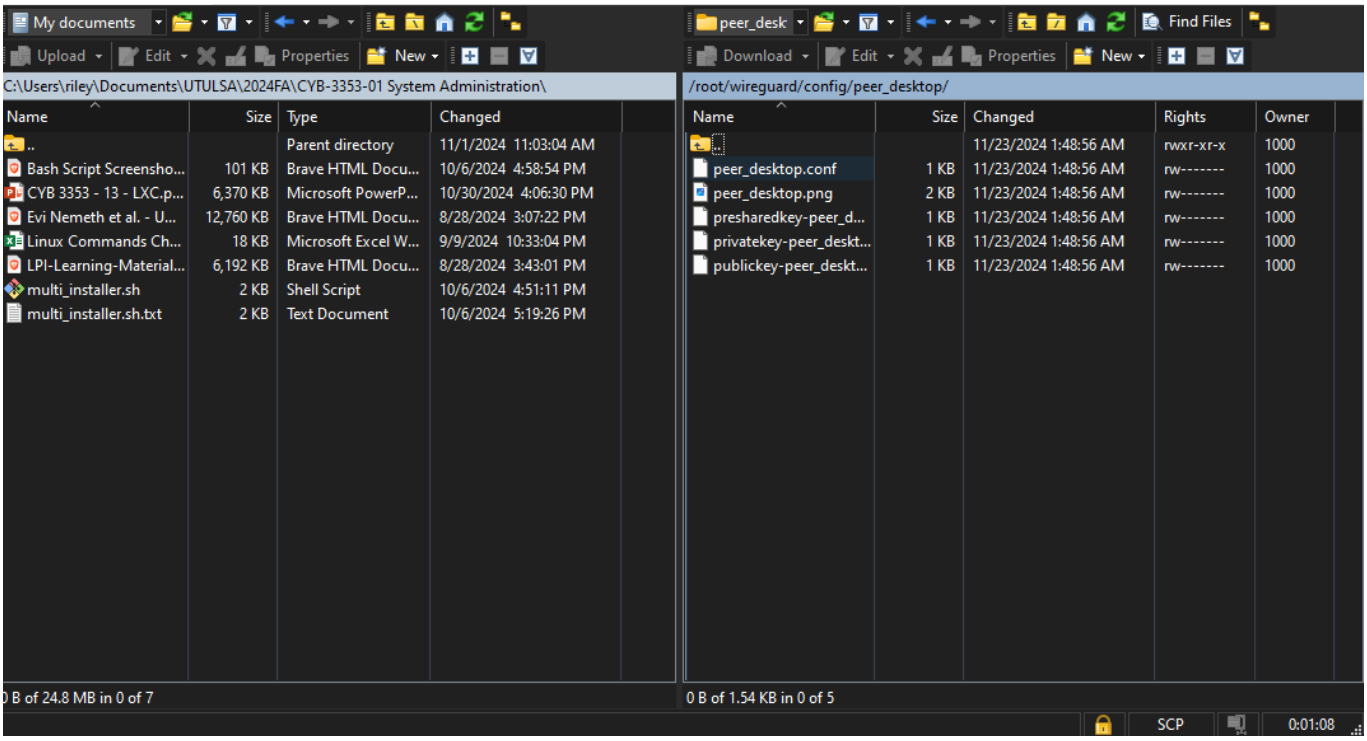
Port number: 22

User name: ROOT

Password: ●●●●●●●●●●

☑ Show Login dialog on startup and when the last session is closed

Then drag and drop 'peer_desktop.conf' from your droplet server to wherever you want to on your desktop.



C:\Users\riley\Documents\UTULSA\2024FA\CYB-3353-01 System Administration\

Name	Size	Type	Changed
..		Parent directory	11/1/2024 11:03:04 AM
Bash Script Screensho...	101 KB	Brave HTML Docu...	10/6/2024 4:58:54 PM
CYB 3353 - 13 - LXC.p...	6,370 KB	Microsoft PowerP...	10/30/2024 4:06:30 PM
Evi Nemeth et al. - U...	12,760 KB	Brave HTML Docu...	8/28/2024 3:07:22 PM
Linux Commands Ch...	18 KB	Microsoft Excel W...	9/9/2024 10:33:04 PM
LPI-Learning-Material...	6,192 KB	Brave HTML Docu...	8/28/2024 3:43:01 PM
multi_installer.sh	2 KB	Shell Script	10/6/2024 4:51:11 PM
multi_installer.sh.txt	2 KB	Text Document	10/6/2024 5:19:26 PM

0 B of 24.8 MB in 0 of 7

/root/wireguard/config/peer_desktop/

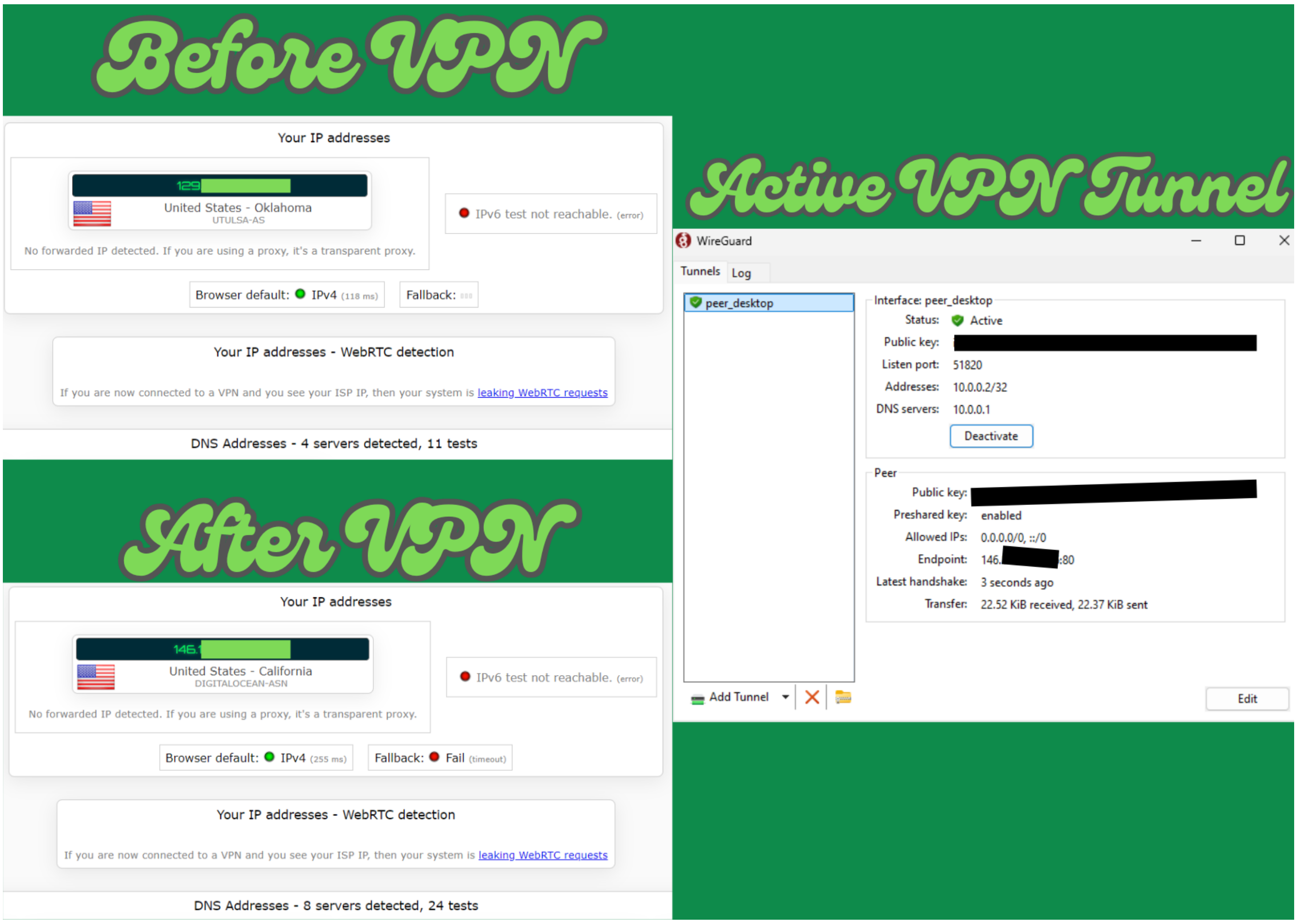
Name	Size	Changed	Rights	Owner
..		11/23/2024 1:48:56 AM	rwxr-xr-x	1000
peer_desktop.conf	1 KB	11/23/2024 1:48:56 AM	rw-------	1000
peer_desktop.png	2 KB	11/23/2024 1:48:56 AM	rw-------	1000
presharedkey-peer_d...	1 KB	11/23/2024 1:48:56 AM	rw-------	1000
privatekey-peer_deskt...	1 KB	11/23/2024 1:48:56 AM	rw-------	1000
publickey-peer_deskt...	1 KB	11/23/2024 1:48:56 AM	rw-------	1000

0 B of 1.54 KB in 0 of 5

Next, download WireGuard for Windows: https://www.wireguard.com/install/

Then, set up your VPN by clicking 'Add Tunnel' at the bottom left, navigating to 'peer_desktop.conf', then click 'Open'. If you forgot to change your Endpoint port, you can edit it in WireGuard by clicking 'Edit' at the bottom right and changing 'Endpoint = your_ip.195:51820' to 'Endpoint = your_ip.195:80'

To test that it is working check your localIP info in your WireGuard settings and visit IPLeak.net and compare them.



Before VPN

Your IP addresses

129[redacted]
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 (118 ms) Fallback:

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 - 4 servers detected, 11 tests

After VPN

Your IP addresses

146.1[redacted]
United States - California
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 (255 ms) Fallback: ● Fail (timeout)

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 - 8 servers detected, 24 tests

Active VPN Tunnel

WireGuard

Interface: peer_desktop
Status: Active
Public key: [redacted]
Listen port: 51820
Addresses: 10.0.0.2/32
DNS servers: 10.0.0.1

Peer
Public key: [redacted]
Preshared key: enabled
Allowed IPs: 0.0.0.0/0, ::/0
Endpoint: 146.[redacted]:80
Latest handshake: 3 seconds ago
Transfer: 22.52 KiB received, 22.37 KiB sent