Wireguard

Setup Script

```
#!/bin/bash

# Checks to see if script is being run as root
if [ "$EUID" -ne 0 ]; then
  echo "Please run as root"
  exit
fi

sudo apt install wireguard

# Deletes keys in case this script is being run again
rm -f /etc/wireguard/*

# Create necessary directories, including parents
mkdir -p /etc/wireguard/client



# Create and store server private and public key
wg genkey | tee /etc/wireguard/server_priv.key | wg pubkey | tee /etc/wireguard/server_pub.key

# Get the server public and private key as well as the network interface
server_priv_key=$(cat /etc/wireguard/server_priv.key)
server_pub_key=$(cat /etc/wireguard/server_pub.key)
network_interface=$(ip -o -4 route show to default | awk '{print $5}')



# Client
# Create client public and private key and store it in vars for later
wg genkey | tee /etc/wireguard/client/client_priv.key | wg pubkey | tee /etc/wireguard/client/client_pub.key
client_priv_key=$(cat /etc/wireguard/client/client_priv.key)
client_pub_key=$(cat /etc/wireguard/client/client_pub.key)
```

```
# Create initial client config
echo "[Interface]
PrivateKey = $client_priv_key
Address = 10.0.0.2/24

[Peer]
PublicKey = $server_pub_key
Endpoint = servername_or_ip:51820
AllowedIPs = 0.0.0.0/0
" > /etc/wireguard/client/wg0.conf


# Create the config file for wireguard
echo "[Interface]
Address = 10.0.0.1/24
SaveConfig = true
ListenPort = 51820
PrivateKey = $server_priv_key
PostUp = iptables -A FORWARD -i %i -j ACCEPT; iptables -t nat -A POSTROUTING -o $network_interface -j
MASQUERADE
PostDown = iptables -D FORWARD -i %i -j ACCEPT; iptables -t nat -D POSTROUTING -o $network_interface -j
MASQUERADE

[Peer]
PublicKey = $client_pub_key
AllowedIPs = 10.0.0.2/24
" > /etc/wireguard/wg0.conf

# Change permissions so only root can access the files
chmod 600 /etc/wireguard/server_priv.key
chmod 600 /etc/wireguard/wg0.conf

# Allow 51820 through ufw
ufw allow 51820/udp

# Start wireguard and set it to auto start on boot
wg-quick up wg0
systemctl enable wg-quick@wg0
```

Setup - Manual

1 - Update system and install wireguard

```
apt update && apt upgrade && apt install wireguard
```

2 - Make the necessary folders

```
mkdir -p /etc/wireguard/client
```

3 - Create the server's public and private keys

```
wg genkey | tee /etc/wireguard/server_priv.key | wg pubkey | tee /etc/wireguard/server_pub.key
```

4 - Find the servers network interface

```
ip -o -4 route show to default | awk '{print $5}
```

5 - Nano into

```
/etc/wireguard/wg0.conf
```

(Make sure to add network interface and server private key)

```
[Interface] Address = 10.0.0.1/24
SaveConfig = true
ListenPort = 51820
PrivateKey = SERVER_PRIVATE_KEY
PostUp = iptables -A FORWARD -i %i -j ACCEPT; iptables -t nat -A POSTROUTING -o NETWORK_INTERFACE_HERE -j MASQUERADE
PostDown = iptables -D FORWARD -i %i -j ACCEPT; iptables -t nat -D POSTROUTING -o NETWORK_INTERFACE_HERE -j MASQUERADE
```

6 - Update file permissions so only root can read the config file and private key

```
chmod 600 /etc/wireguard/server_priv.key chmod 600 /etc/wireguard/wg0.conf
```

7 - Allow the vpn port through UFW

```
ufw allow 51820/udp
```

8 - Start wireguard and set it to auto start at boot

```
wg-quick up wg0 systemctl enable wg-quick@wg0
```

9 - Create the client keys

```
wg genkey | tee /etc/wireguard/client/priv.key | wg pubkey | tee /etc/wireguard/client/pub.key
```

10 - Create the client config file (copy to client device)

```
[Interface] PrivateKey = CLIENT_PRIVATE_KEY
Address = 10.0.0.2/24 [Peer]
PublicKey = SERVER_PUBLIC_KEY
Endpoint = SERVER_IP_OR_DOMAIN:51820
AllowedIPs = 0.0.0.0/0
```

11 - Add peer info to the server config

```
[Interface] Address = 10.0.0.1/24
SaveConfig = true
ListenPort = 51820
PrivateKey = SERVER_PRIVATE_KEY
PostUp = iptables -A FORWARD -i %i -j ACCEPT; iptables -t nat -A POSTROUTING -o NETWORK_INTERFACE_HERE -j MASQUERADE
PostDown = iptables -D FORWARD -i %i -j ACCEPT; iptables -t nat -D POSTROUTING -o NETWORK_INTERFACE_HERE -j MASQUERADE

# ================
[Peer]
PublicKey = PUBLIC_KEY
AllowedIPs = 10.0.0.2/24
```

Setup with SeaBee's setup script

```
wget https://raw.githubusercontent.com/seabee33/wireguard_helper/refs/heads/main/wg_helper.py && chmod +x wg_helper.py && sudo python3 wg_helper.py
```

Auto start at boot

1 - ensure the client config is at `/etc/wireguard/wg0.conf`
2 - enable it to start at boot with `sudo systemctl enable wg-quick@wg0`

Revision #3
Created 22 March 2025 10:56:46 by Conor
Updated 16 June 2025 23:42:02 by Conor