

# Wireguard + Pihole = Kết nối VPN và lướt web không ads

Install wireguard + pihole with this portainer stack

WireGuard được sử dụng để thiết lập các kết nối VPN an toàn và hiệu quả. Nó bảo vệ dữ liệu khi truyền qua mạng, đảm bảo quyền riêng tư và an toàn cho người dùng. Với cấu hình đơn giản và hiệu suất cao, WireGuard phù hợp cho cả cá nhân và doanh nghiệp.

Pi-hole được sử dụng để chặn quảng cáo và theo dõi trực tuyến ở cấp độ mạng. Hoạt động như một DNS sinkhole, Pi-hole ngăn chặn các yêu cầu đến các máy chủ quảng cáo và theo dõi, cải thiện tốc độ duyệt web và bảo vệ quyền riêng tư cho tất cả các thiết bị kết nối vào mạng.

Khi kết hợp WireGuard và Pi-hole, bạn có thể thiết lập một mạng VPN an toàn, đồng thời chặn quảng cáo và theo dõi trực tuyến. WireGuard bảo vệ kết nối internet của bạn bằng cách mã hóa dữ liệu, trong khi Pi-hole chặn các quảng cáo và trình theo dõi ở cấp độ DNS, đảm bảo quyền riêng tư và trải nghiệm duyệt web sạch hơn cho tất cả các thiết bị kết nối vào mạng VPN.

Lưu ý: cài đặt này trên Ubuntu OS và docker + portainer stack

services:

wireguard:

image: lscr.io/linuxserver/wireguard:latest

container\_name: wireguard

cap\_add:

- NET\_ADMIN # Work good on Ubuntu System
- SYS\_MODULE #optional

environment:

- PUID=0 # just type "id" on your OS (Ubuntu/Centos) terminal to see puid and pgid
- PGID=0
- TZ=Asia/Ho\_Chi\_Minh
- SERVERURL=ABC.DOMAIN.COM #public domain
- SERVERPORT=51820 #optional

- PEERS=20 #optional
- PEERDNS=172.21.0.3 #optional
- INTERNAL\_SUBNET=10.13.13.0 #optional
- ALLOWEDIPS=0.0.0.0/0 #optional
- PERSISTENTKEEPALIVE\_PEERS= #optional
- LOG\_CONFS=true #optional

volumes:

- /home/USERNAME/docker/wireguard/config:/config # Change USERNAME to your Ubuntu/Centos Username
- /home/USERNAME/docker/wireguard/lib/modules:/lib/modules #Change USERNAME to your Ubuntu/Centos

Username

ports:

- 51820:51820/udp

sysctls:

- net.ipv4.conf.all.src\_valid\_mark=1
- net.ipv4.ip\_forward=1

networks:

private\_network:

ipv4\_address: 172.21.0.4

restart: unless-stopped

pihole:

container\_name: pihole

image: pihole/pihole:latest

restart: unless-stopped

hostname: pi.hole

ports:

- "88:80/tcp" # Expose port 88 to the public, you can visit with IP:88 or ABC.DOMAIN.COM:88 to pihole and

configure it later

dns:

- 127.0.0.1

volumes:

- ./etc-pihole:/etc/pihole/
- ./etc-dnsmasq.d:/etc/dnsmasq.d/

cap\_add:

- NET\_ADMIN

networks:

private\_network:

ipv4\_address: 172.21.0.3

networks:

private\_network:

```
ipam:
  driver: default
  config:
    - subnet: 172.21.0.0/24
```

<input type="checkbox"/>	Name↓↑	State↓↑ Filter ▾	Quick Actions	Stack↓↑	Image↓↑	Created↓↑	IP Address↓↑	Published Ports↓↑	Ownership↓↑
<input type="checkbox"/>	pihole	healthy		wireshark	pihole/pihole:latest	2024-07-01 05:02:16	172.21.0.3	<a href="#">88:80</a>	administrators
<input type="checkbox"/>	wireguard	running		wireshark	lscr.io/linuxserver/wireguard:latest	2024-07-01 05:12:41	172.21.0.4	<a href="#">51820:51820</a>	administrators

Bạn có thể vào pihole và config lại với port 88.

Còn wireguard bạn vào đường dẫn để /home/USERNAME/docker/wireguard/config, sau đó copy toàn bộ folder peer1, peer2, peer3.... về máy, mỗi folder sẽ có conf và hình qr để đăng nhập. Đối với window thì cứ import cái file conf của peer vào là hoạt động. đối với đt thì cài wireguard và scan qr