

# Mise en place de mon VPN

## Sommaire

Installation de Dockge.....	2
Installation de docker.....	2
Stack Dockge.....	2
Comment utiliser Dockge.....	2
Installation de Wireguard VPN.....	3
Prérequis.....	3
Stack Wireguard VPN.....	3
.....	4
Création du tunnel et configuration.....	4
Sur l'interface Web.....	4

## Installation de Dockge

### Installation de docker

Suivre la [documentation d'installation Docker](#) pour l'OS installé sur votre machine

### Stack Dockge

Le compose de dockge est le suivant :

version: "3.8"

services:

  dockge:

    image: louislam/dockge:1

    restart: unless-stopped

    ports:

      - 5001:5001

    volumes:

      - /var/run/docker.sock:/var/run/docker.sock

      - ./data:/app/data

    # Stacks Directory

    # ⚠ READ IT CAREFULLY. If you did it wrong, your data could end up writing into a WRONG PATH.

    # ⚠ 1. FULL path only. No relative path (MUST)

    # ⚠ 2. Left Stacks Path === Right Stacks Path (MUST)

      - /opt/stacks:/opt/stacks

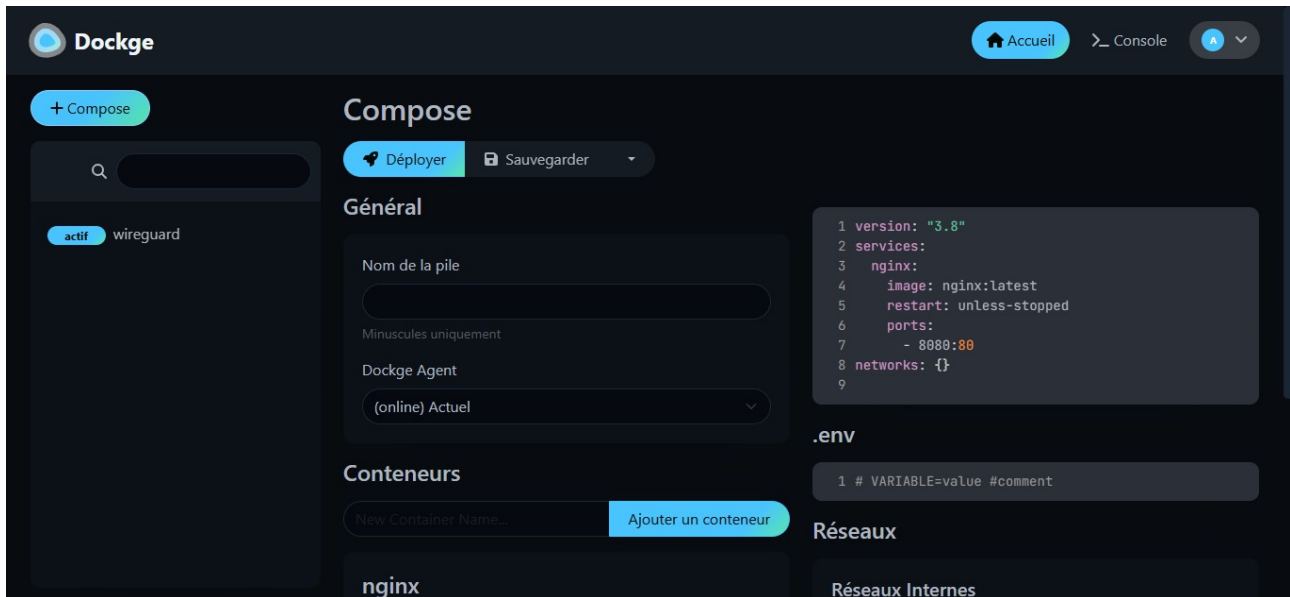
  environment:

    # Tell Dockge where to find the stacks

    - DOCKGE\_STACKS\_DIR=/opt/stacks

### Comment utiliser Dockge

Pour l'utilisation de votre compose Wireguard, cliquez sur la bulle bleue en haut à gauche « + COMPOSE », une fois sur la page (cf. image en dessous) copiez, collez le compose avec les modifications nécessaires, ajoutez un nom a votre pile puis cliquez sur la bulle fusée « Déployer ».



## Installation de Wireguard VPN

### Prérequis

Vous devez, en amont de la procédure d'installation, ouvrir sur votre interface de configuration FAI, le port 51820 en UDP.

### Stack Wireguard VPN

Le stack pour Wireguard est le suivant :

version: "3.9"

services:

wg-easy:

image: ghcr.io/wg-easy/wg-easy

restart: unless-stopped

sysctls:

- net.ipv4.ip\_forward=1

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

cap\_add:

- SYS\_MODULE

- NET\_ADMIN

## Mise en place VPN Wireguard

ports:

- 51821:51821/tcp
- 51820:51820/udp

volumes:

- ./wg-easy:/etc/wireguard

environment:

- PASSWORD\_HASH=your\_password
- WG\_HOST=Votre\_ip\_publique
- LANG=fr

container\_name: wg-easy

## Création du tunnel et configuration

Dans le stack Wireguard, il va falloir générer votre mot de passe avec un script qui génère des hachages de mot de passe bcrypt.

Dans la console de votre container/VM qui héberge dockge, tapez la commande suivante en remplaçant votre\_mot\_de\_passe par celui souhaité :

```
docker run -it ghcr.io/wg-easy/wg-easy wgpw votre_mot_de_passe
```

Ce qui va donner une combinaison similaire a celle-ci :

```
PASSWORD_HASH='$2a$12$KI4yuJ8g2c002pEYErJQWe9hV.PbKyxiE5ad3cS9jwtCS7nY0WP16'
```

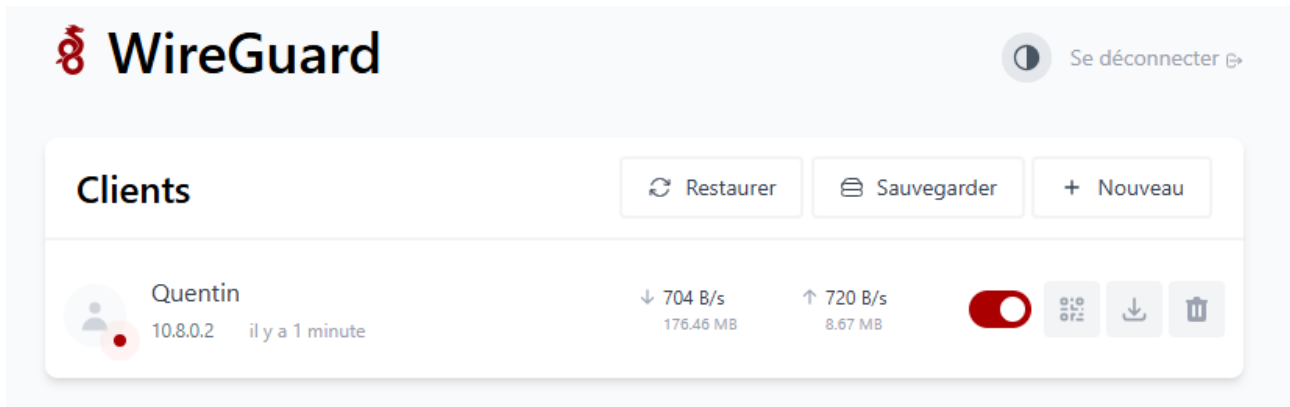
Il va falloir doubler tous les \$ ainsi qu'enlever les apostrophes du début et fin de mots de passe, puis copiez le a l'endroit du mot de passe dans le stack

Une fois déployez, rendez vous sur l'interface Web wireguard en tapant <http://ip:51821>

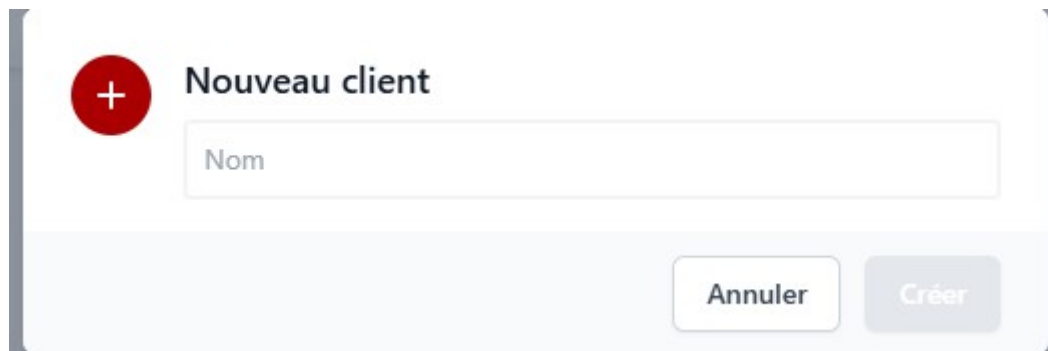
## Sur l'interface Web

Connectez vous en tapant le mot de passe choisi précédemment.

Vous pouvez maintenant créer un nouveau client en cliquant sur « Nouveau »



Nommez votre client.



Vous pouvez maintenant Activer/désactiver des clients sur l'interface Web.

Vous connecter en téléchargeant Wireguard sur votre PC, en téléchargeant la configuration du client et en l'exportant sur votre client Wireguard.

Pour accéder a votre VPN depuis un autre appareil, vous pouvez exporter la configuration sur l'autre appareil, ou scanner un QR code pour accéder directement au vpn sur votre mobile par exemple (à condition d'avoir préalablement téléchargé l'application)

Félicitation, vous pouvez maintenant accéder à votre réseau local à distance grâce a un canal virtuel sécurisé !