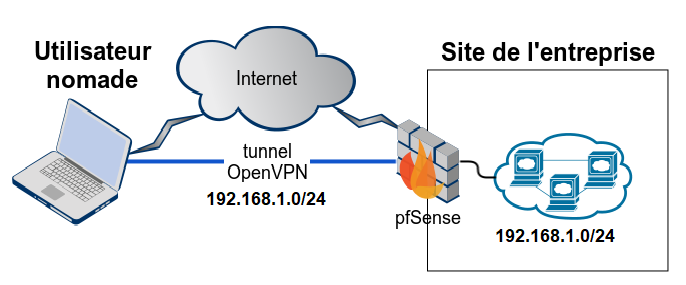
**VPN (Virtual Private Network)**

Une fois le VPN activé, un tunnel sécurisé est créé entre vous et le serveur VPN.

Les informations qui transitent dans un tunnel VPN seront chiffrées.

Votre ordinateur va recevoir une adresse IP compatible avec le réseau de l'entreprise.



Les utilisateurs du Cégep du Vieux Montréal utilisent le logiciel "FortiClient VPN" de la compagnie Fortinet pour se connecter au serveur VPN du cégep.



Le masque de sous-réseau de l'adresse IP 10.205.0.9 est 255.255.255.255.

Ce qui fait qu'un utilisateur VPN ne peut pas communiquer avec un autre utilisateur VPN.



Il existe au moins cinq protocoles pour le VPN.

Le protocole VPN qui sera utilisé pour ce laboratoire sera OpenVPN.

OpenVPN est rapide et très fiable.

OpenVPN est un protocole open source.

OpenVPN

* OpenVPN utilise le cryptage AES et le niveau de chiffrement est de 256 bits
* OpenVPN est plus rapide que PPTP et L2TP/IPSec
* OpenVPN est compatible avec Windows, Linux et macOS
* OpenVPN nécessite une application tierce
* OpenVPN permet d'utiliser un port TCP ou UDP
* OpenVPN utilise le port 1194 par défaut mais il est possible de le modifier pour 443

Si OpenVPN utilise le port 443 alors le trafic VPN est presque indiscernable du trafic standard HTTPS.

PPTP (Point-to-point Tunneling Protocol) est un ancien protocole VPN qui existe depuis Windows 95

* PPTP est facile à configurer
* PPTP a un très faible niveau de sécurité

SSTP (Secure Socket Tunneling Protocole) un protocole qui appartient à Microsoft<

* Il existe depuis Windows Vista Service Pack 1
* SSTP utilise le cryptage AES et le niveau de chiffrement est de 256 bits

L2TP/IPsec

WireGuard est un nouveau protocole VPN.

* WireGuard est compatible avec Windows, macOS, BSD, iOS, Android, Linux (Debian, Ubuntu, Fedora, …)

Tailscale

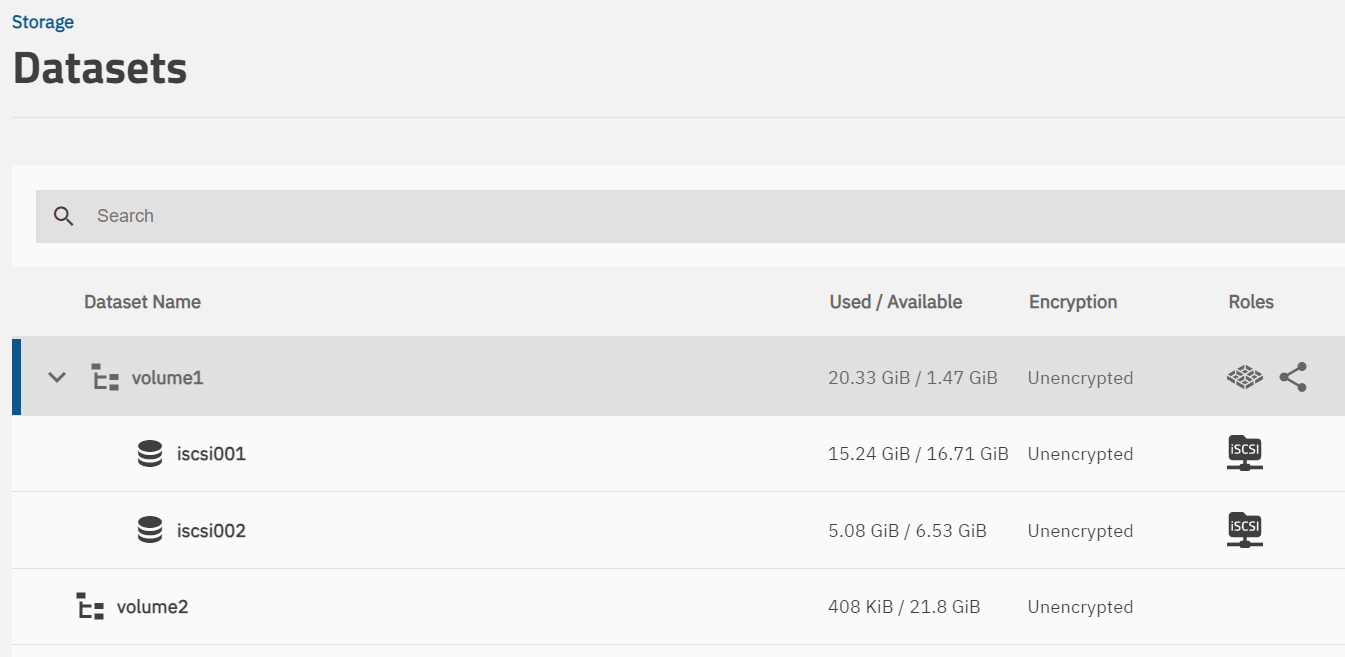
https://tailscale.com

**Mise en place**

Le but de ce laboratoire est d'installer, configurer et tester un serveur WireGuard sur TrueNAS.



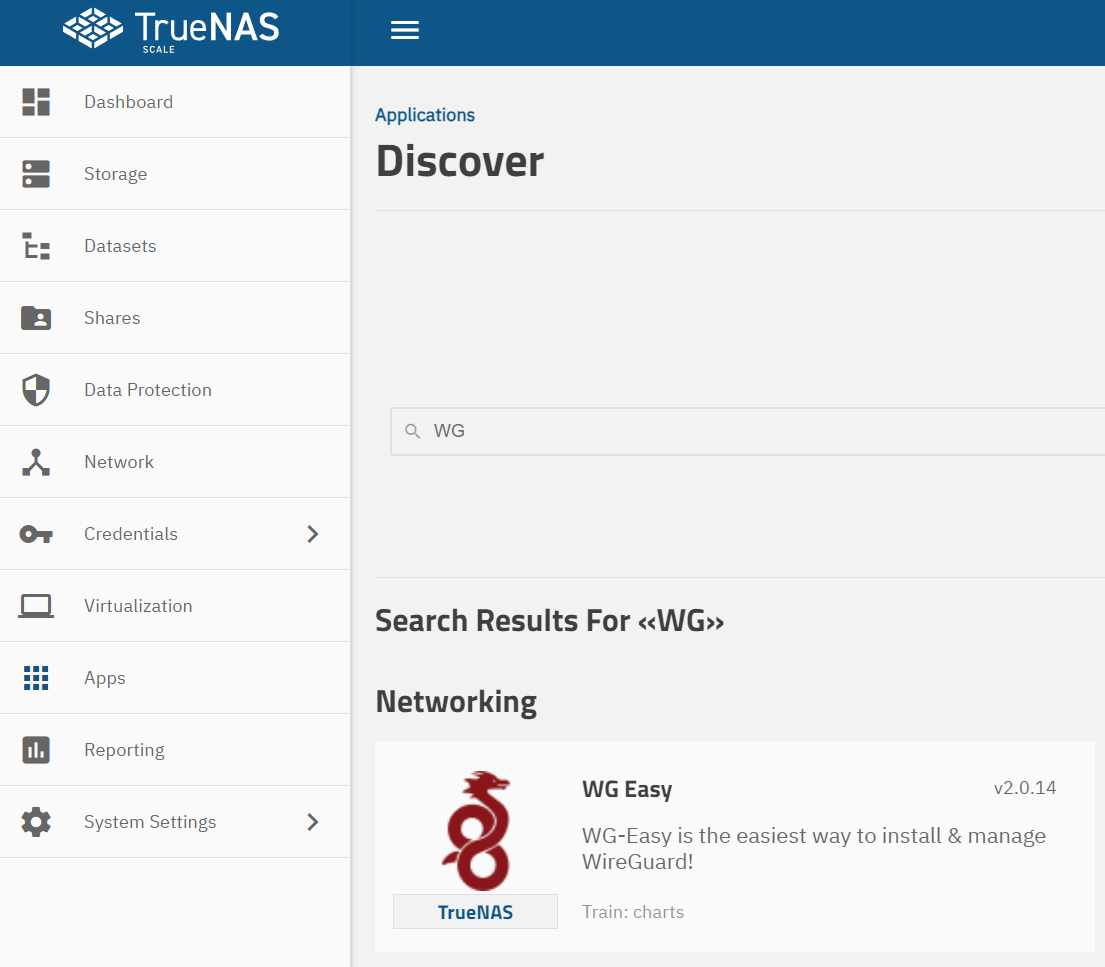
WireGuard sera installé sur le pool "**volume2**".



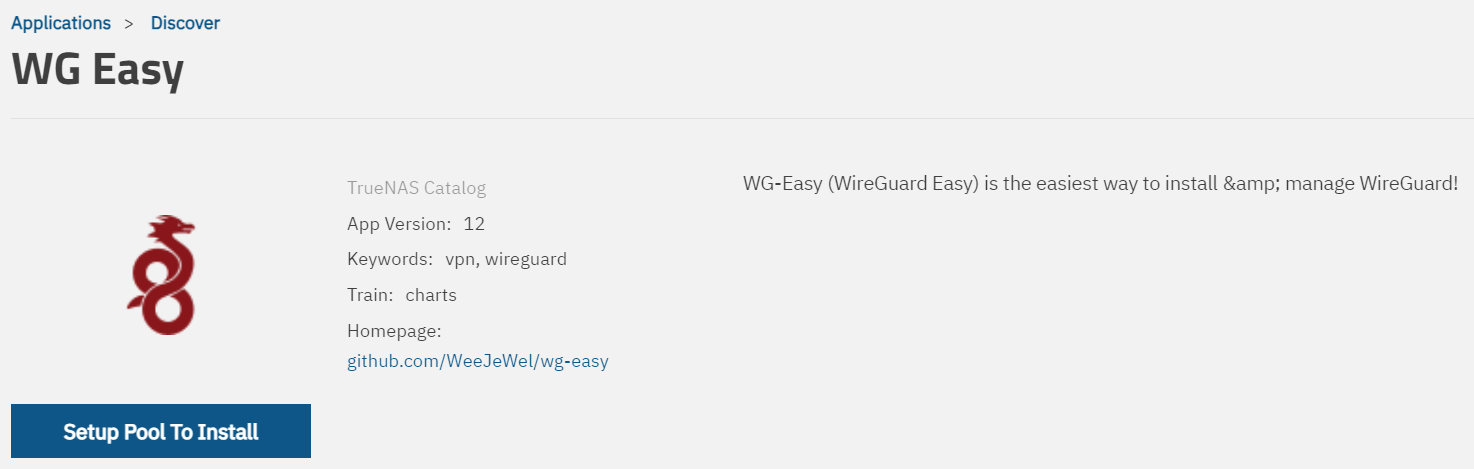
**Installation de WireGuard**

L'installation et la configuration se font en utilisant l'adresse IP **192.168.1.80** ou l'adresse IP **192.168.1.81**.

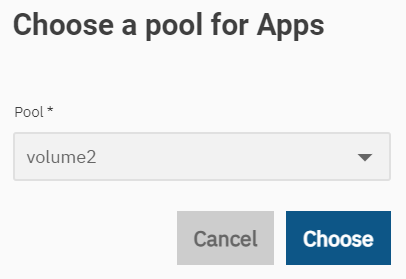
Dans le menu "**Apps**"



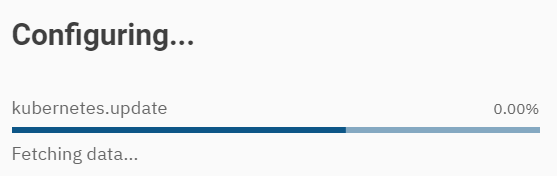
Vous devez cliquer sur l'application.

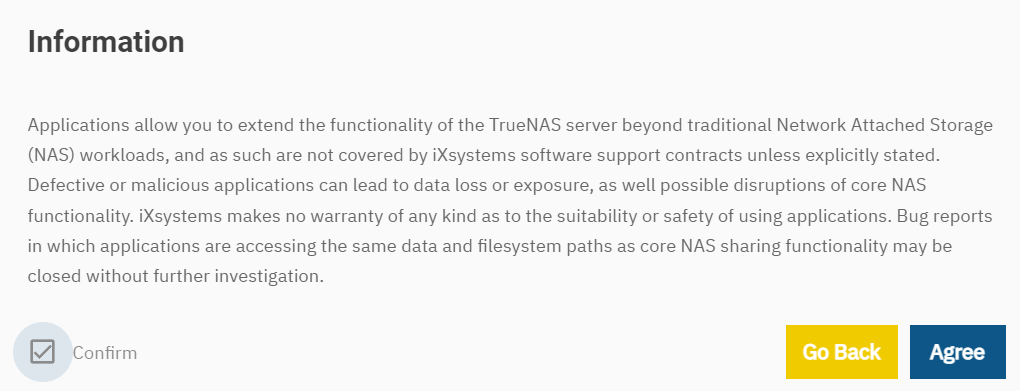


Vous devez cliquer sur le bouton "**Setup Pool To Install**".



L'installation de WireGuard se fait dans un "**conteneur**".

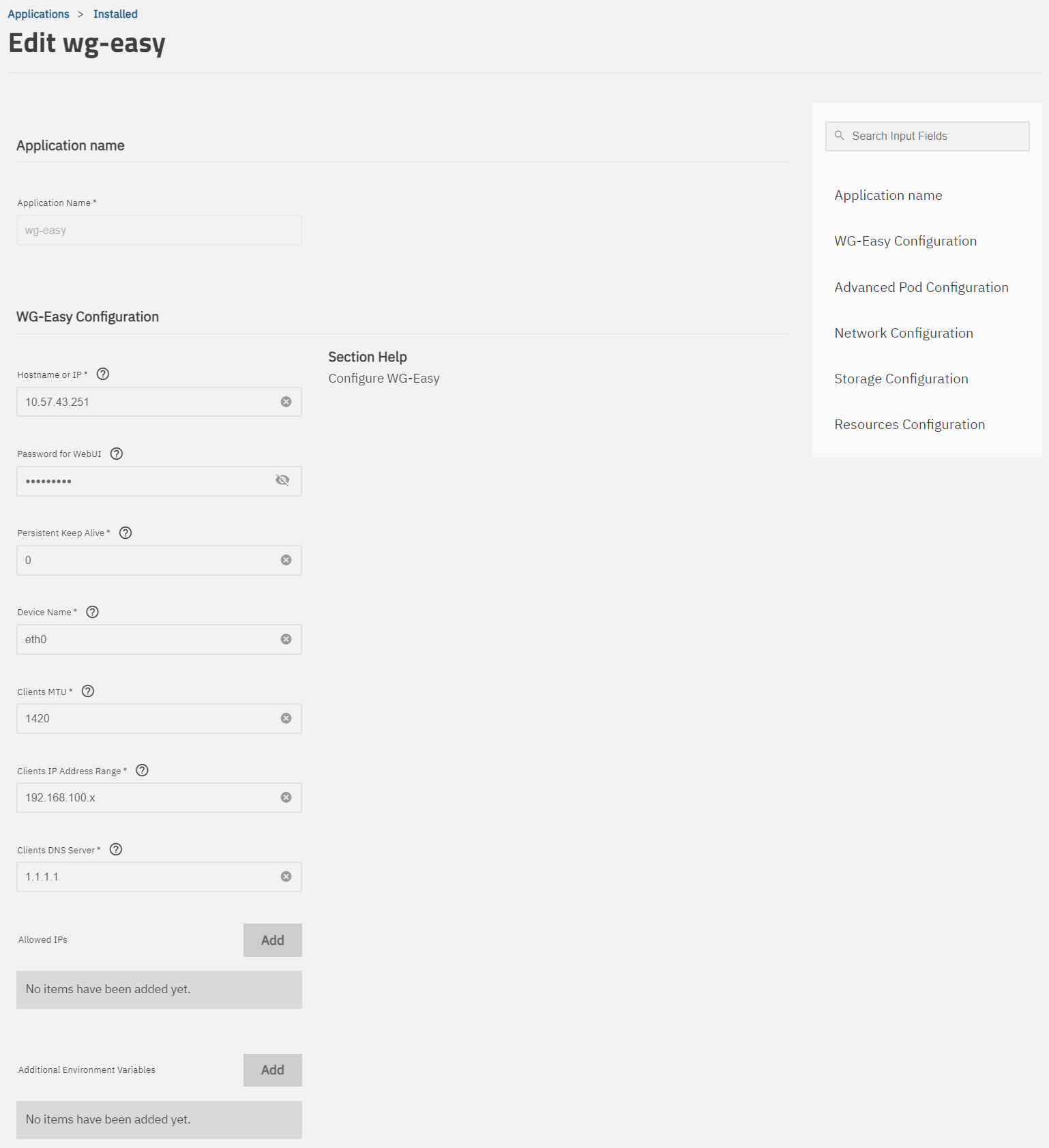




**L'installation de WireGuard est terminée.**

**Configuration de WireGuard**

La première partie de la page de configuration.

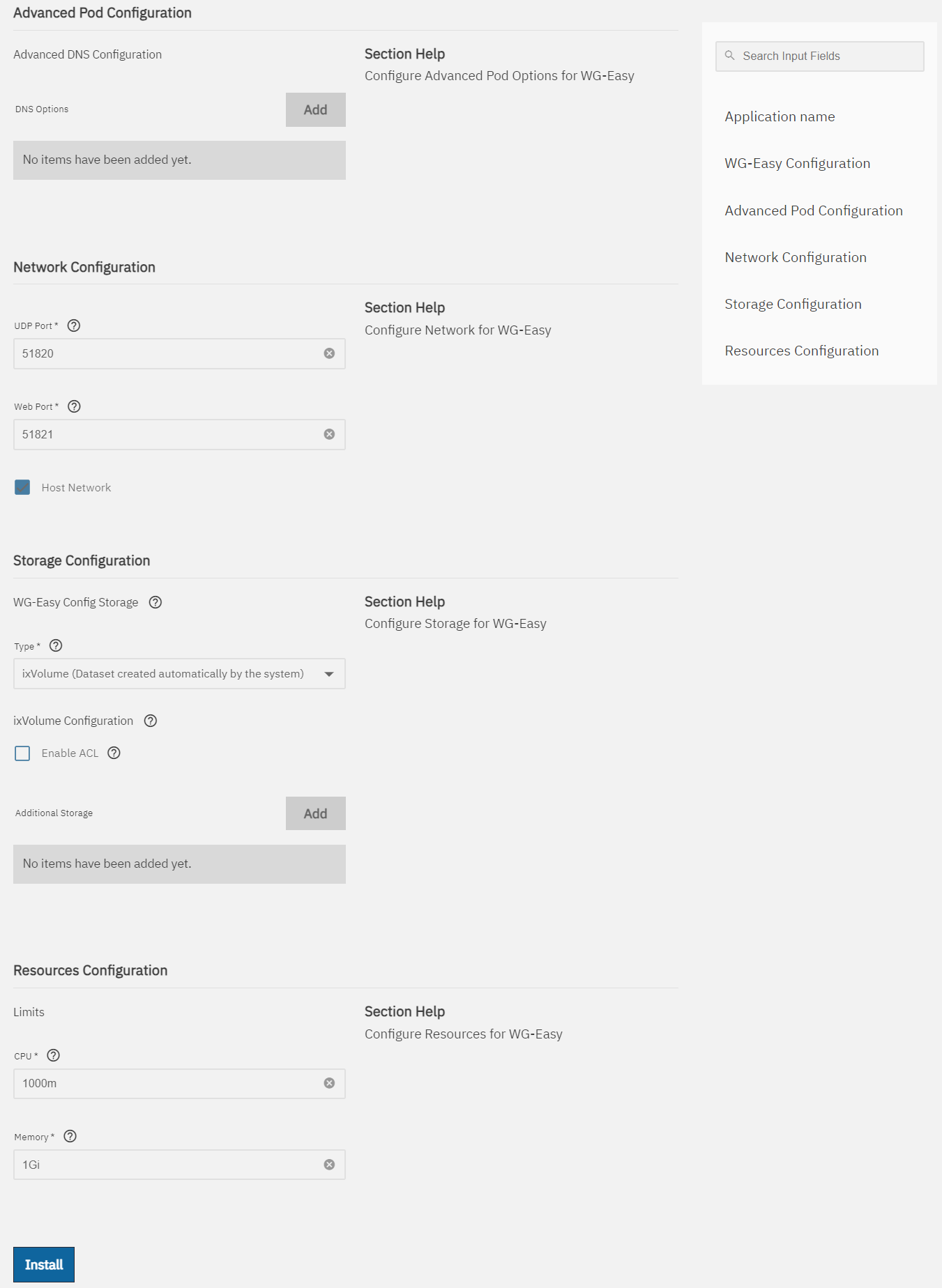


**Hostname or IP =** **10.57.yy**.**xx** (External Host) **C'est l'adresse IP du côté WAN pour accéder à TrueNAS.**

**Password for WebUI =** **AAAaaa111** **C'est le mot de passe de la page web pour WireGuard.**

**Client IP Address Range =** **192.168.100.x** **Le réseau pour les clients qui vont se connecter à WireGuard.**

La deuxième partie de la page de configuration.



**Voir la page suivante.**

**UDP Port =** **51820** (External Port)

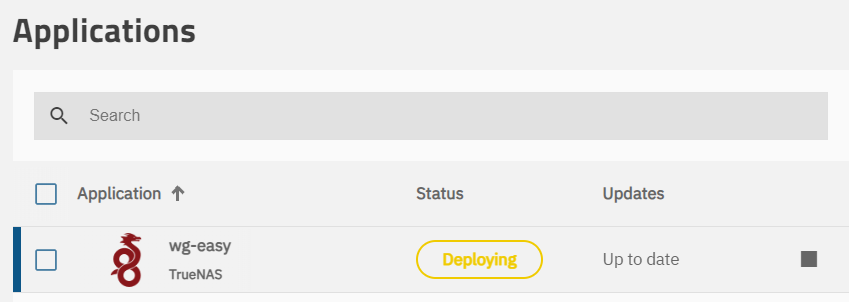
**Web Port =** **51821** (WebUI Port)

**CPU =** **1000m 1000m signifie que WireGuard peut utiliser jusqu'à 1 cœur pour le CPU**

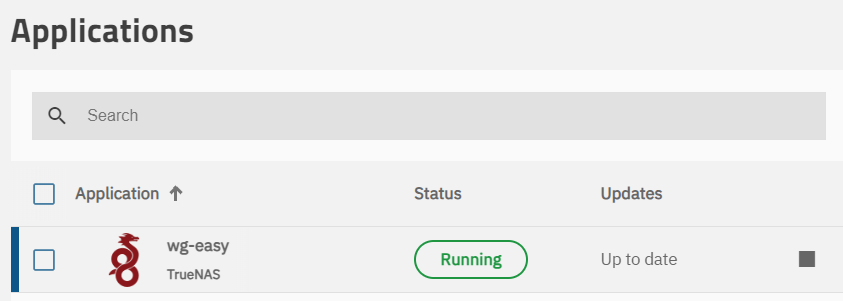
**Memory =** **1Gi 1Gi signifie que WireGuard peut utiliser jusqu'à 1 GO de mémoire (1024MB)**

Vous devez cliquer sur le bouton "**Install**".

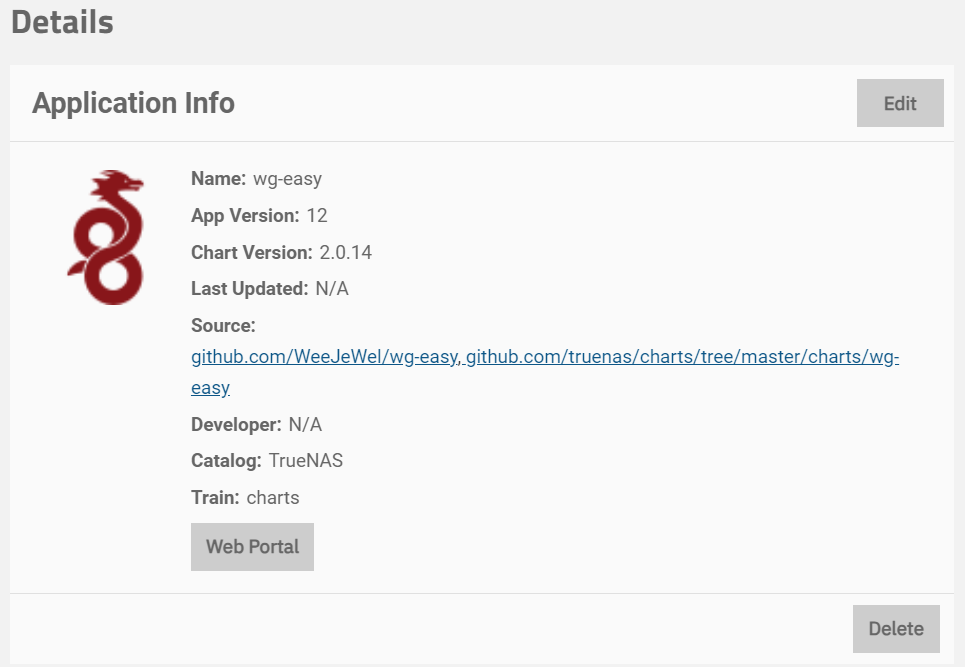
L'état de WireGuard est "**Deploying**".

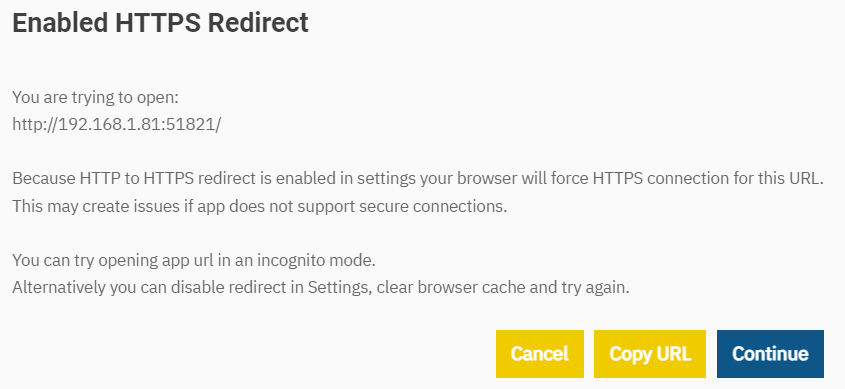


L'état de WireGuard est "**Running**".



Pour configurer WireGuard, vous devez cliquer sur "**Web Portal**". (Web UI)

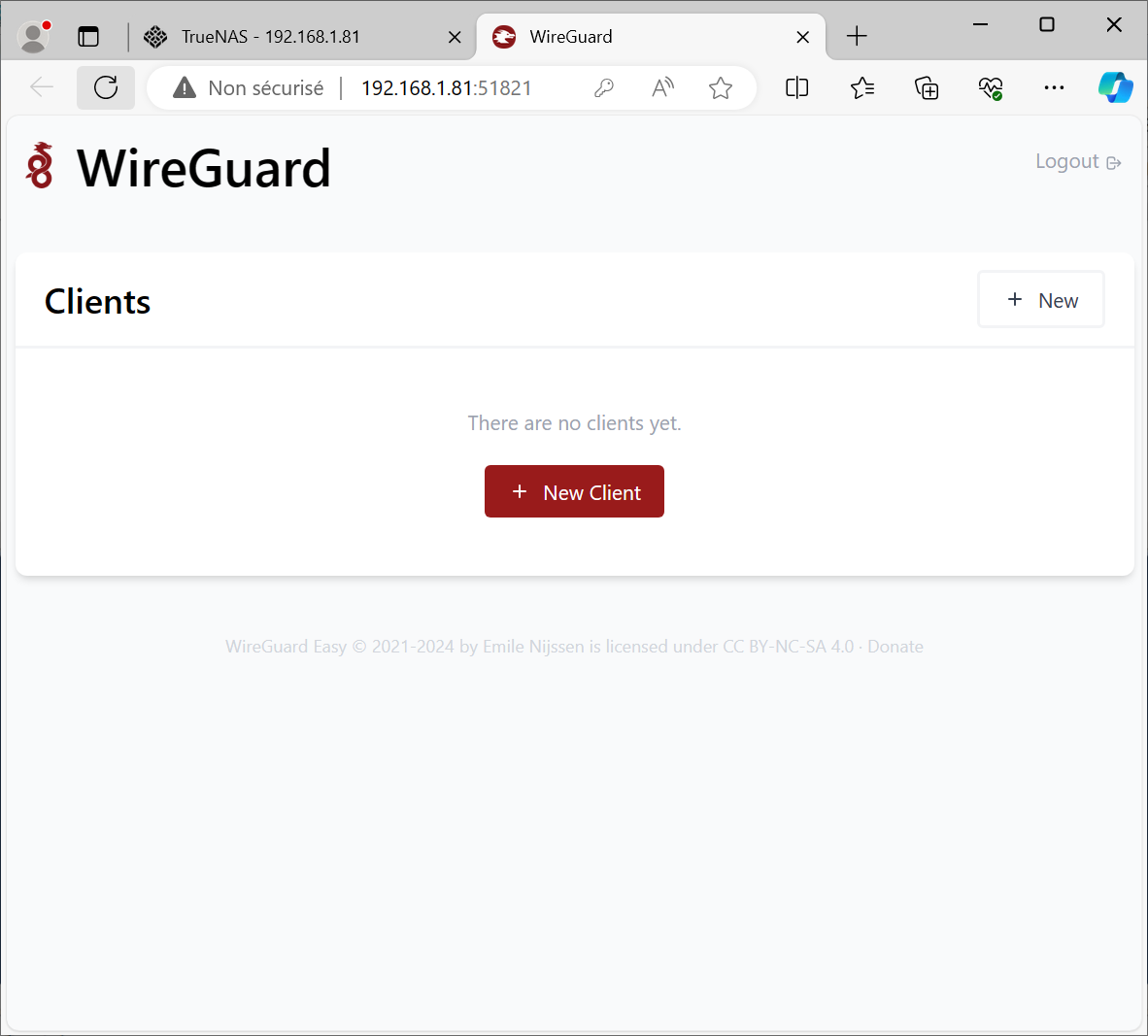




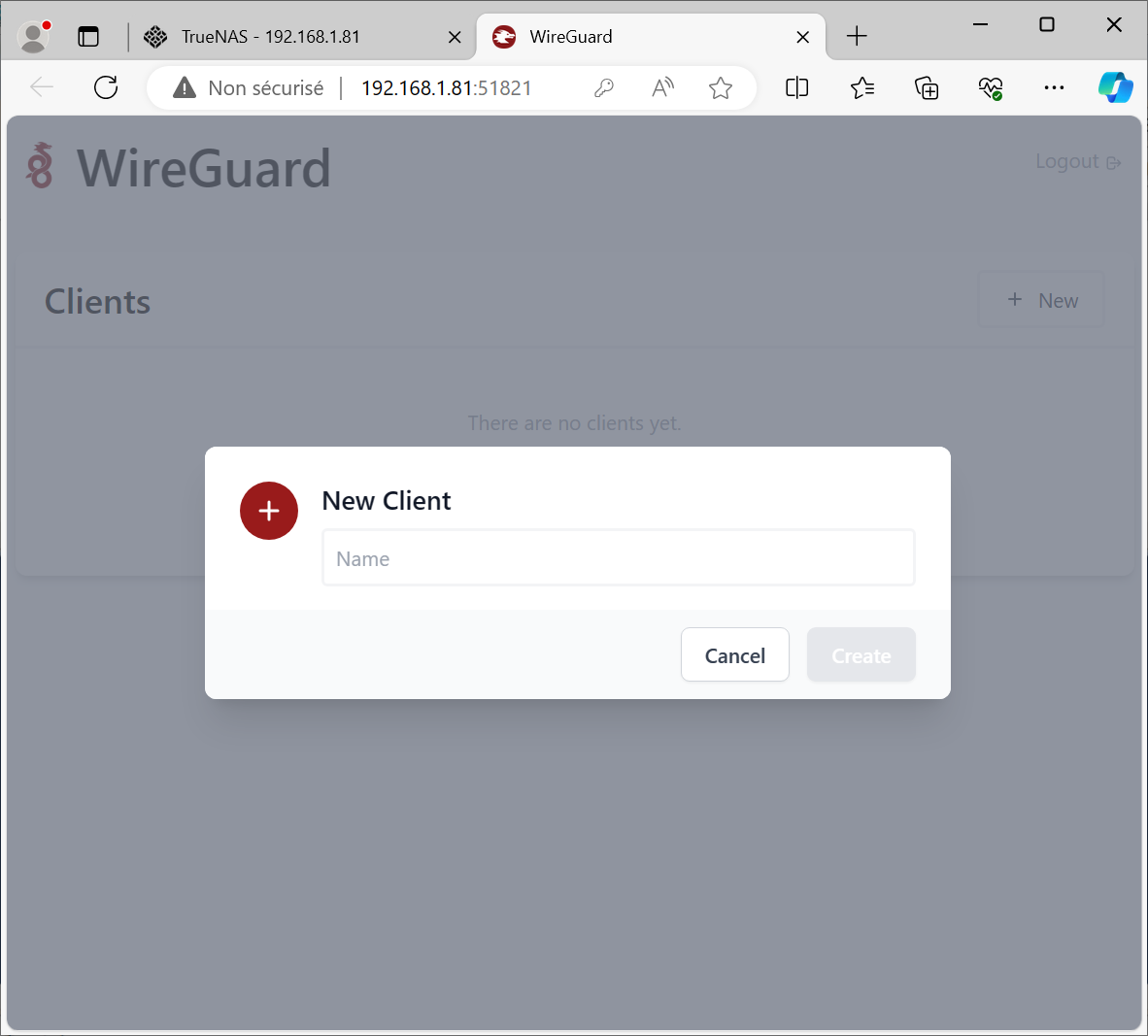
Vous devez cliquer sur le bouton "**Continue**".

Le mot de passe de la page web est **AAAaaa111**.





Vous devez cliquer sur le bouton "**New Client**".



Vous devez créer un utilisateur pour WireGuard.



Vous devez cliquer sur la flèche qui pointe vers le bas pour télécharger le fichier de configuration.

Le nom du fichier est "**wg01.conf**" et contient les informations pour se connecter à WireGuard.

**Configurations du pare-feu dans pfSense**

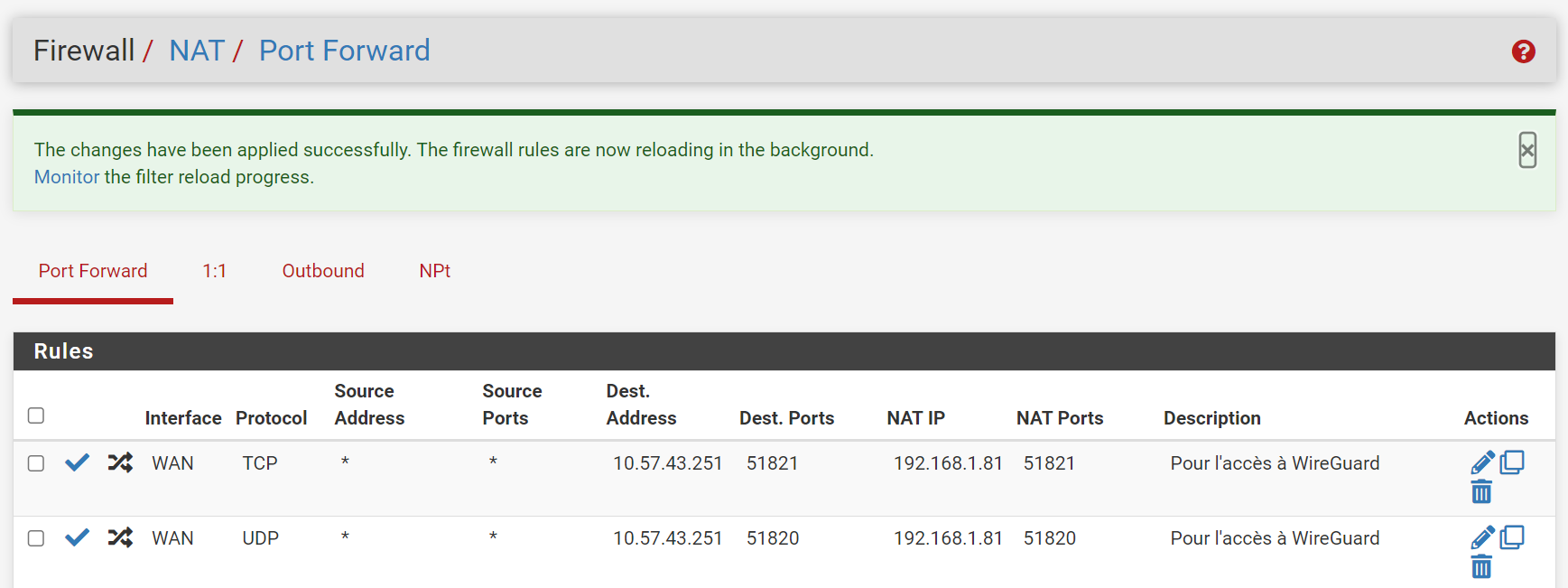
Avant de continuer, il est important de configurer deux redirections de port sur le routeur pfSense.

La première redirection de port

* Adresse IP externe = **10.57.yy.xx**
* Adresse IP interne = **192.168.1.81**
* Numéro de port = **51821**
* Protocole = **TCP**

La deuxième redirection de port

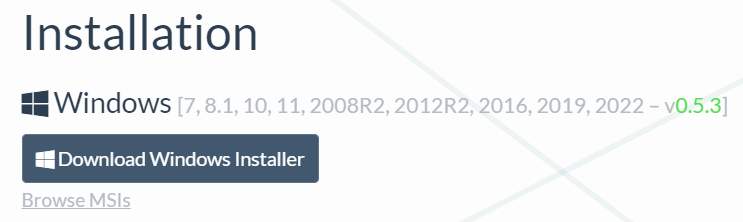
* Adresse IP externe = **10.57.yy.xx**
* Adresse IP interne = **192.168.1.81**
* Numéro de port = **51820**
* Protocole = **UDP**



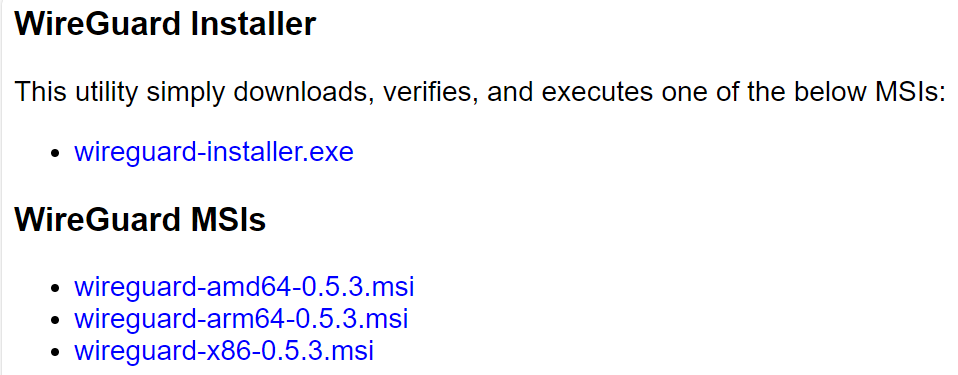
**Configurations sur le serveur réel**

Il faut télécharger le client Windows pour WireGuard.

https://www.wireguard.com/install

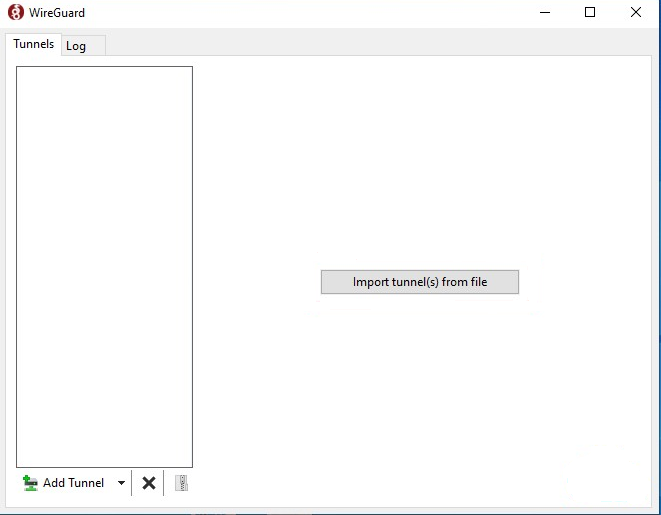


Vous devez cliquer sur "**Browse MSIs**" pour télécharger un fichier avec l'extension .MSI.



Il faut télécharger le fichier "**wireguard-amd64-0.5.3.msi**".

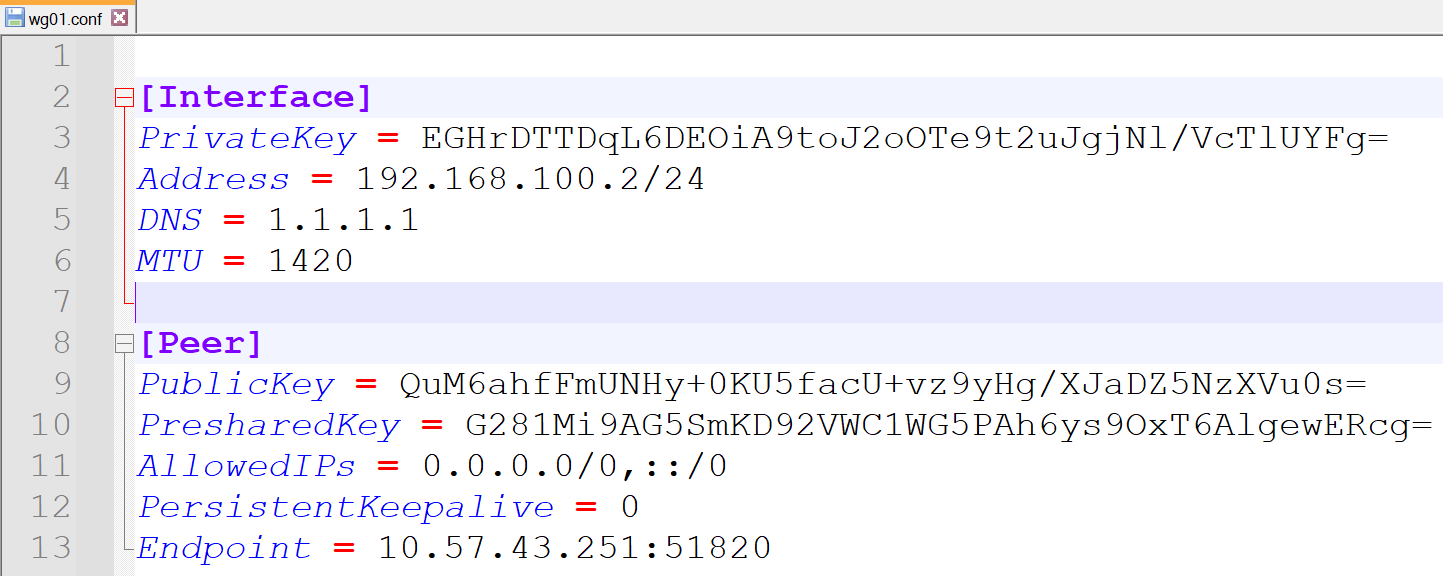
Vous devez installer le client WireGuard sur le serveur réel.



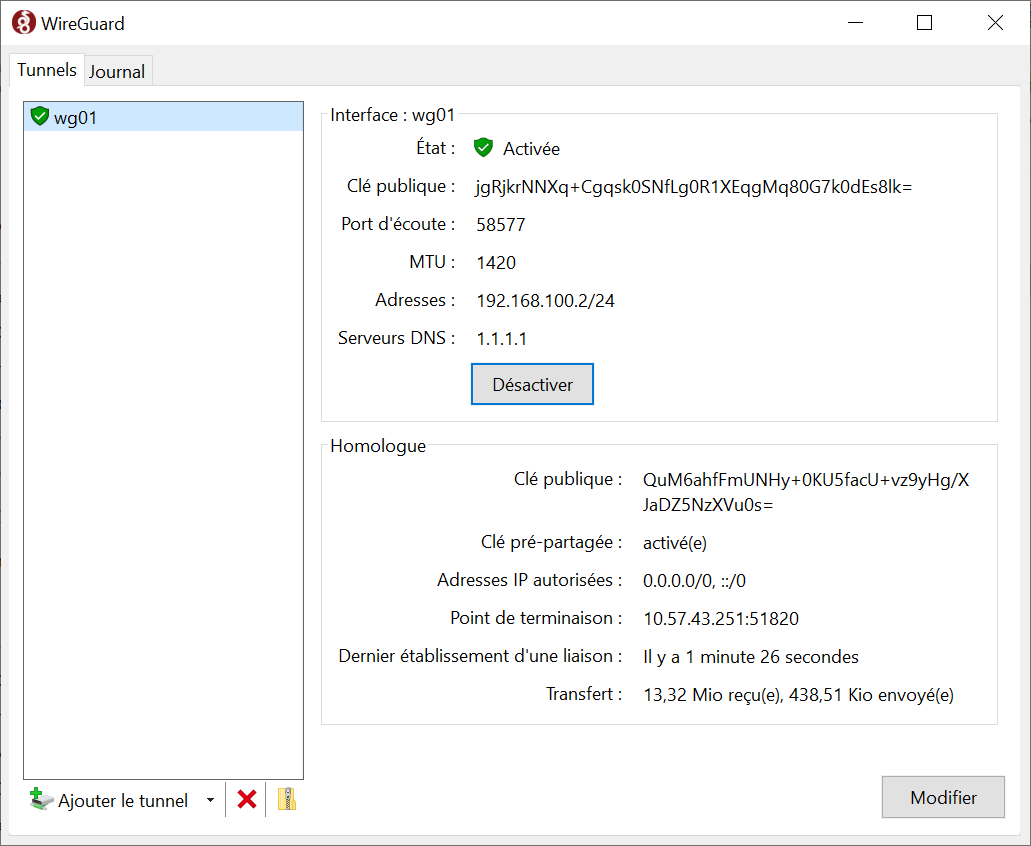
Vous devez cliquer sur le bouton "**Import tunnel(s) from file**".

Vous avec besoin du fichier "**wg01.conf**".

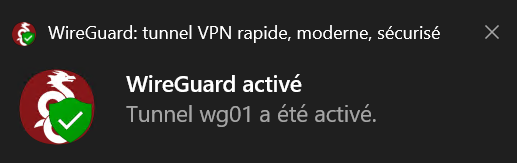
Le contenu du fichier "**wg01.conf**".



La configuration du ficher est valide.



Vous devez cliquer sur le bouton "**Activer**".

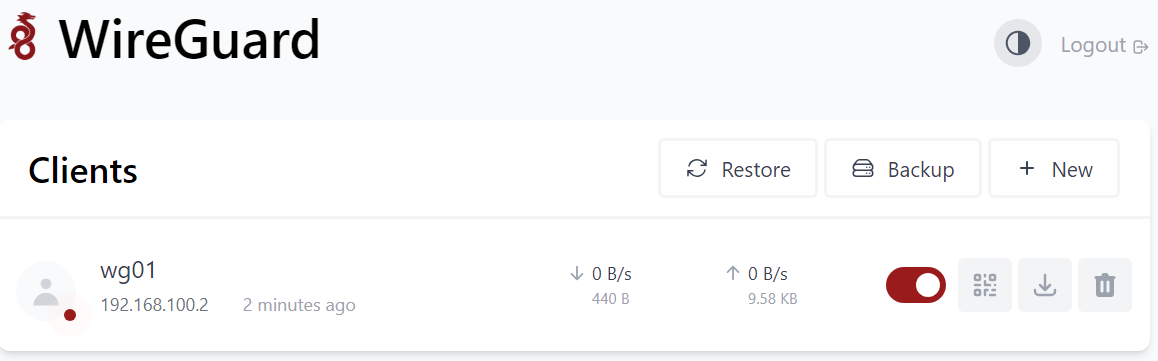


Le client WireGuard ajoute une nouvelle carte réseau.



Il est possible d'accéder à toutes les ressources qui sont du côté LAN du routeur.

Dans la configuration de l'application WireGuard dans la section "**Clients**", le point rouge clignote pour indiquer que le client **wg01** utilise la connexion VPN de WireGuard.



**Tests**

Lorsque la connexion VPN est établie le "client externe" a une adresse IP qui fait partie du réseau privé.

Ce qui fait que le "client externe" peut accéder à toutes les ressources qui sont dans le réseau privé.

1. Tests de PING de l'ordinateur réel vers le réseau PRIVÉ.

**ping 192.168.1.1** pfSense fonctionne correctement

**ping 192.168.1.10** SERVEUR1 fonctionne correctement

**ping 192.168.1.20** SERVEUR2 fonctionne correctement

**ping 192.168.1.80** TrueNAS fonctionne correctement

**ping 192.168.1.81** TrueNAS fonctionne correctement

1. Vous devez avoir accès au "Bureau à distance" en utilisant les adresses du réseau 192.168.1.0/24.
2. Vous devez avoir accès au site web

**http://192.168.1.101**

**http://192.168.1.102**

**http://192.168.1.10:1080**

**http://192.168.1.10:1180**

Pour accéder aux sites web avec des noms, vous devez modifier le DNS dans le fichier "**wg01.conf**".

Le nouveau DNS sera 192.168.1.20.



http://adr1.formation.local

http://adr2.formation.local

http://ent1.formation.local

http://ent2.formation.local