
WIREGUARD®
FAST, MODERN, SECURE VPN TUNNEL

Contents

Installation et configuration de WireGuard VPN sur Ubuntu 2

Prérequis 2

Étape 1 : Installer WireGuard 3

Étape 2 : Générer les clés du serveur 3

Étape 3 : Activer le transfert IP (IP Forwarding) 4

Étape 4 : Configurer le serveur (wg0.conf) 4

Étape 4 : Suite 5

Étape 5 : Configurer le pare-feu (UFW) 6

Étape 6 : Configurer un client (ex: votre téléphone ou portable) 6

Étape 7 : Démarrer le serveur 8

Étape 8 : Redirection de port sur le routeur 8

Comment se connecter 8

Configuration et utilisation d'un domaine avec DDNS (No-IP) 9

Étape 1 : Créer votre compte et nom d'hôte (Sur le web) 9

Étape 2 : Préparer Ubuntu 10

Étape 3 : Télécharger et installer No-IP 10

Étape 4 : Configuration (Pendant l'installation) 11

Étape 5 : Automatiser le démarrage (Très important) 11

Étape 6 : Vérifier que ça fonctionne 12

Résumé pour votre VPN 12

Installation et configuration de WireGuard VPN sur Ubuntu

WireGuard est un logiciel de VPN (réseau privé virtuel) moderne. Il permet de créer un "tunnel" chiffré entre deux appareils (par exemple : ton PC à la maison ↔ ton serveur ou ton réseau du travail) pour que la connexion soit sécurisée et privée, même si tu passes par Internet.

Voici le guide étape par étape pour transformer votre machine Ubuntu en serveur VPN WireGuard.

Prérequis

- Machine Ubuntu : Connectée à votre réseau local (LAN).
- Redirection de port (Port Forwarding) : Vous devez pouvoir vous connecter à votre routeur Internet et rediriger un port UDP (par défaut 51820) vers l'adresse IP locale de votre machine Ubuntu.
- IP Publique ou DDNS : Vous devez connaître l'adresse IP publique de votre domicile. Si elle change souvent (IP dynamique), configurez un nom d'hôte DDNS (comme DuckDNS ou No-IP).

Étape 1 : Installer WireGuard

Mettez à jour votre liste de paquets et installez les outils nécessaires.

```
sudo apt update
sudo apt install wireguard
```

Étape 2 : Générer les clés du serveur

WireGuard utilise une paire de clés publique/privée. Vous devez les générer pour le serveur.

1. Passez en utilisateur root pour faciliter la gestion des fichiers :

```
sudo -i
cd /etc/wireguard/
```

2. Définissez les permissions pour que seul root puisse lire les clés privées :

```
umask 077
```

3. Générez les clés :

```
wg genkey | tee server_private.key | wg pubkey > server_public.key
```

- Vous avez maintenant deux fichiers : server_private.key et server_public.key. Vous aurez besoin de leur contenu sous peu. Ouvrez les fichiers avec sudo nano et copiez leur contenu dans un document texte.

Étape 3 : Activer le transfert IP (IP Forwarding)

Pour que le VPN puisse acheminer le trafic de l'extérieur vers vos appareils locaux, Ubuntu doit être autorisé à transférer les paquets.

1. Ouvrez le fichier de configuration sysctl :

```
nano /etc/sysctl.conf
```

2. Trouvez la ligne #net.ipv4.ip_forward=1 et décommentez-la (supprimez le # au début).
3. Sauvegardez et quittez (Ctrl+O, Entrée, Ctrl+X).
4. Appliquez les changements :

```
sysctl -p
```

Étape 4 : Configurer le serveur (wg0.conf)

C'est l'étape principale de la configuration.

1. Trouvez le nom de votre interface réseau : Exécutez : `ip route list default`. Cherchez le mot dev. Le texte qui suit est le nom de votre interface (souvent eth0, enp3s0, etc.). Supposons que c'est eth0 pour ce guide, mais remplacez-le par le vôtre ci-dessous.
2. Créez le fichier de configuration :

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

Étape 4 : Suite…

3. Copiez la configuration suivante dans le fichier :

```
[Interface]
# L'adresse IP interne du VPN (pas votre IP locale)
Address = 10.66.66.1/24
# Le port UDP sur lequel WireGuard écoute
ListenPort = 51820
# La clé privée de votre serveur (copiez le contenu de server_private.key)
PrivateKey = <INSÉREZ_CLÉ_PRIVÉE_SERVEUR_ICI>
# Règles de masquage IP (NAT)
# Ces règles permettent aux clients VPN d'accéder à Internet et à votre LAN.
# REMPLACEZ 'eth0' par le nom réel de votre interface réseau !
PostUp = iptables -A FORWARD -i wg0 -j ACCEPT; iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
PostDown = iptables -D FORWARD -i wg0 -j ACCEPT; iptables -t nat -D POSTROUTING -o eth0 -j MASQUERADE
# Configuration du Client 1 (ex: votre téléphone)
[Peer]
# Vous générerez ces clés à l'étape 6
PublicKey = <INSÉREZ_CLÉ_PUBLIQUE_CLIENT_ICI>
# L'IP interne que vous assignez à ce client
AllowedIPs = 10.66.66.2/32
```

Étape 5 : Configurer le pare-feu (UFW)

Si vous utilisez UFW (Uncomplicated Firewall), vous devez autoriser le trafic VPN et SSH (pour ne pas vous bloquer l'accès).

```
sudo ufw allow 51820/udp
sudo ufw allow OpenSSH
sudo ufw enable
```

Étape 6 : Configurer un client (ex: votre téléphone ou portable)

Vous ne pouvez pas vous connecter sans une paire de clés client.

1. Générer les clés du client (faites-le sur le serveur pour l'instant) :

```
wg genkey | tee client_private.key | wg pubkey > client_public.key
```

2. Ajouter la clé publique du client à la config du serveur :

- Copiez le contenu de client_public.key.
- Éditez à nouveau /etc/wireguard/wg0.conf.
- Collez la clé dans le champ PublicKey sous la section [Peer] créée à l'étape 4.

Étape 6 : Suite…

3. Créer le fichier de configuration du client : Vous devrez transférer ce fichier sur votre appareil client (ou utiliser un code QR). Créez un fichier texte (ex: client.conf) sur votre ordinateur avec ce contenu :

```
[Interface]
# L'adresse IP interne du client
Address = 10.66.66.1/24
# La clé privée du client
PrivateKey = <INSÉREZ_CLÉ_PRIVÉE_CLIENT_ICI>
# Serveur DNS (utilisez l'IP de votre routeur, ex: 192.168.1.1, ou Google 8.8.8.8)
DNS = 1.1.1.1

[Peer]
# La clé publique du SERVEUR (contenu de server_public.key)
PublicKey = <INSÉREZ_CLÉ_PUBLIQUE_SERVEUR_ICI>
# L'IP Publique de votre internet résidentiel : Port
Endpoint = votre.ip.publique.adresse:51820
# IPs à router via le VPN.
# 0.0.0.0/0 route TOUT (Internet + LAN) via le VPN.
# Si vous voulez SEULEMENT l'accès LAN, utilisez : 192.168.1.0/24 (selon votre sous-réseau)
AllowedIPs = 0.0.0.0/0
PersistentKeepalive = 25
```

Étape 7 : Démarrer le serveur

De retour sur votre serveur Ubuntu, démarrez l'interface WireGuard :

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

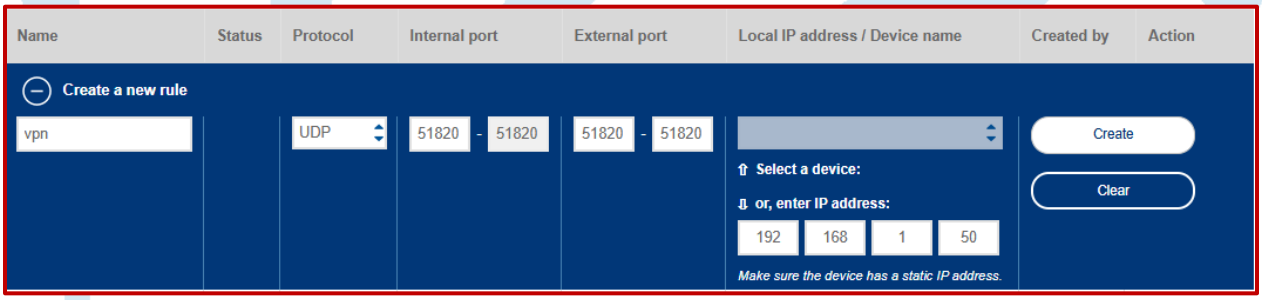
Vérifiez le statut pour vous assurer que tout fonctionne :

```
systemctl status wg-quick@wg0
```

Étape 8 : Redirection de port sur le routeur

C'est l'étape où la plupart des erreurs surviennent.

1. Connectez-vous à votre routeur (généralement 192.168.1.1 ou 192.168.0.1).
2. Trouvez les paramètres de Port Forwarding (Redirection de port).
3. Redirigez le port UDP 51820 vers l'IP Locale de votre serveur Ubuntu (ex: 192.168.1.50).



Comment se connecter

1. Installez l'application WireGuard sur votre téléphone ou portable.
2. Importez le fichier client.conf créé à l'étape 6.
3. Activez le tunnel.
4. Essayez de faire un "ping" sur un appareil de votre réseau local pour vérifier la connexion.

Configuration et utilisation d'un domaine avec DDNS (No-IP)

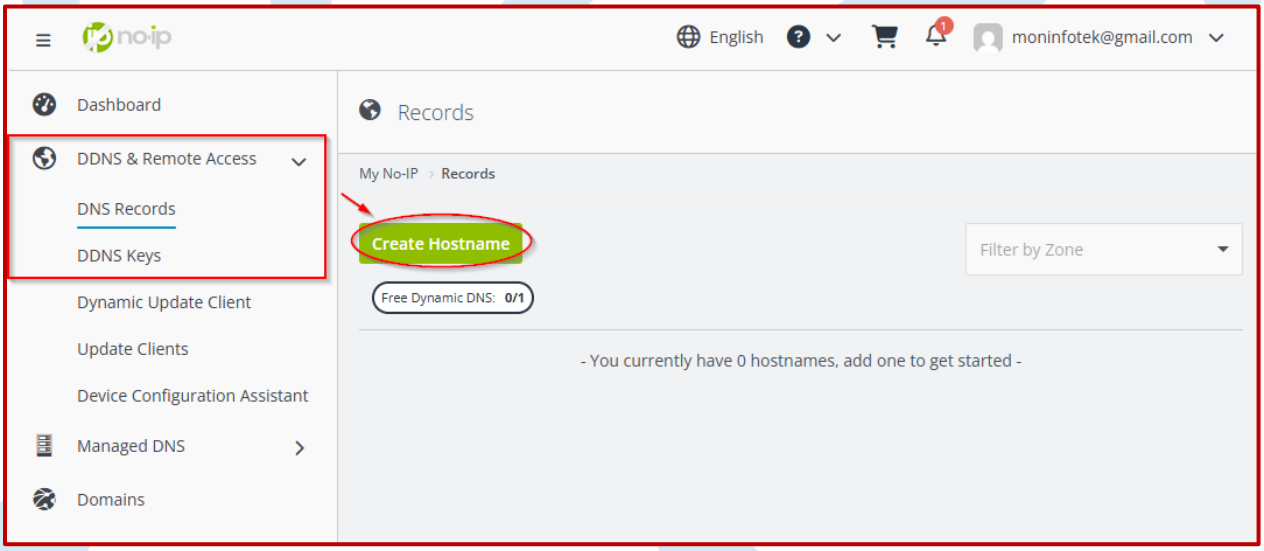
Comme le client No-IP ne s'installe pas directement via apt install comme les autres logiciels, il faut le télécharger et l'installer manuellement. Ne vous inquiétez pas, c'est une procédure standard. Voici les étapes détaillées pour installer et configurer le client de mise à jour (DUC) de No-IP sur votre serveur Ubuntu.

Étape 1 : Créer votre compte et nom d'hôte (Sur le web)

Allez sur le site de No-IP (https://www.noip.com/sign-up)

Créez un compte gratuit.

Créez un nom d'hôte (Hostname). Par exemple : mon-vpn-maison.ddns.net.



Important! Gardez votre identifiant (courriel) et mot de passe à portée de main.

Étape 2 : Préparer Ubuntu

Nous aurons besoin d'outils pour installer le logiciel (car nous allons le "compiler").

Ouvrez votre terminal et tapez :

```
sudo apt update
sudo apt install build-essential wget tar
```

Étape 3 : Télécharger et installer No-IP

Nous allons télécharger le logiciel officiel, le décompresser et l'installer.

1. Allez dans le dossier des sources (un dossier temporaire standard) :

```
cd /usr/local/src/
```

2. Téléchargez le fichier :

```
sudo wget http://www.no-ip.com/client/linux/noip-duc-linux.tar.gz
```

3. Décompressez l'archive :

```
sudo tar xf noip-duc-linux.tar.gz
```

4. Entrez dans le dossier créé (le numéro de version peut varier, donc on utilise *) :

```
cd noip-2.1.9-1/
```

Note : Si cette commande échoue, faites ls pour voir le nom exact du dossier et tapez cd noip- suivi de la touche TAB.

5. Installez le logiciel :

```
sudo make install
```

Étape 4 : Configuration (Pendant l'installation)

Dès que vous tapez sudo make install, le programme va vous poser des questions dans le terminal. Voici comment répondre :

1. Login/Email : Entrez le courriel utilisé pour votre compte No-IP.
2. Password : Entrez votre mot de passe No-IP.
3. Update frequency : Il demandera à quelle fréquence vérifier l'IP (en minutes). La valeur par défaut est 30. Tapez 30 et faites Entrée.
4. Selection : Si vous avez plusieurs noms de domaine, il vous demandera lequel mettre à jour. Choisissez celui pour votre VPN.

Étape 5 : Automatiser le démarrage (Très important)

Par défaut, si vous redémarrez votre serveur, No-IP ne redémarrera pas tout seul. Nous devons créer un "service".

1. Créez le fichier de service :

```
sudo nano /etc/systemd/system/noip2.service
```

2. Copiez et collez le contenu suivant dans le fichier :

```
[Unit]
Description=No-IP Dynamic Update Client
After=network.target
[Service]
Type=forking
ExecStart=/usr/local/bin/noip2
[Install]
WantedBy=multi-user.target
```

3. Sauvegardez et quittez (Ctrl+O, Entrée, Ctrl+X).
4. Activez et démarrez le service :

```
sudo systemctl enable noip2
sudo systemctl start noip2
```

Étape 6 : Vérifier que ça fonctionne

Pour voir si le logiciel tourne bien et quelle IP il a détectée, utilisez cette commande :

```
sudo noip2 -S
```

(Le S doit être majuscule).

Vous devriez voir une ligne indiquant votre IP publique actuelle et le statut "Updated successfully".

Résumé pour votre VPN

Maintenant que No-IP est configuré :

1. Dans le fichier de configuration de votre téléphone/laptop (client.conf de la page 7 Étape 6), mettez :

```
Endpoint = mon-vpn-maison.ddns.net:51820
```

2. C'est tout ! Votre serveur Ubuntu informera automatiquement No-IP si votre adresse résidentielle change.

Note importante concernant la version gratuite de No-IP : La version gratuite vous enverra un courriel tous les 30 jours vous demandant de confirmer que vous utilisez toujours le nom de domaine. Vous devez cliquer sur le lien dans ce courriel, sinon ils supprimeront le nom de domaine.