08.2 - Configuration d'un client Ubuntu

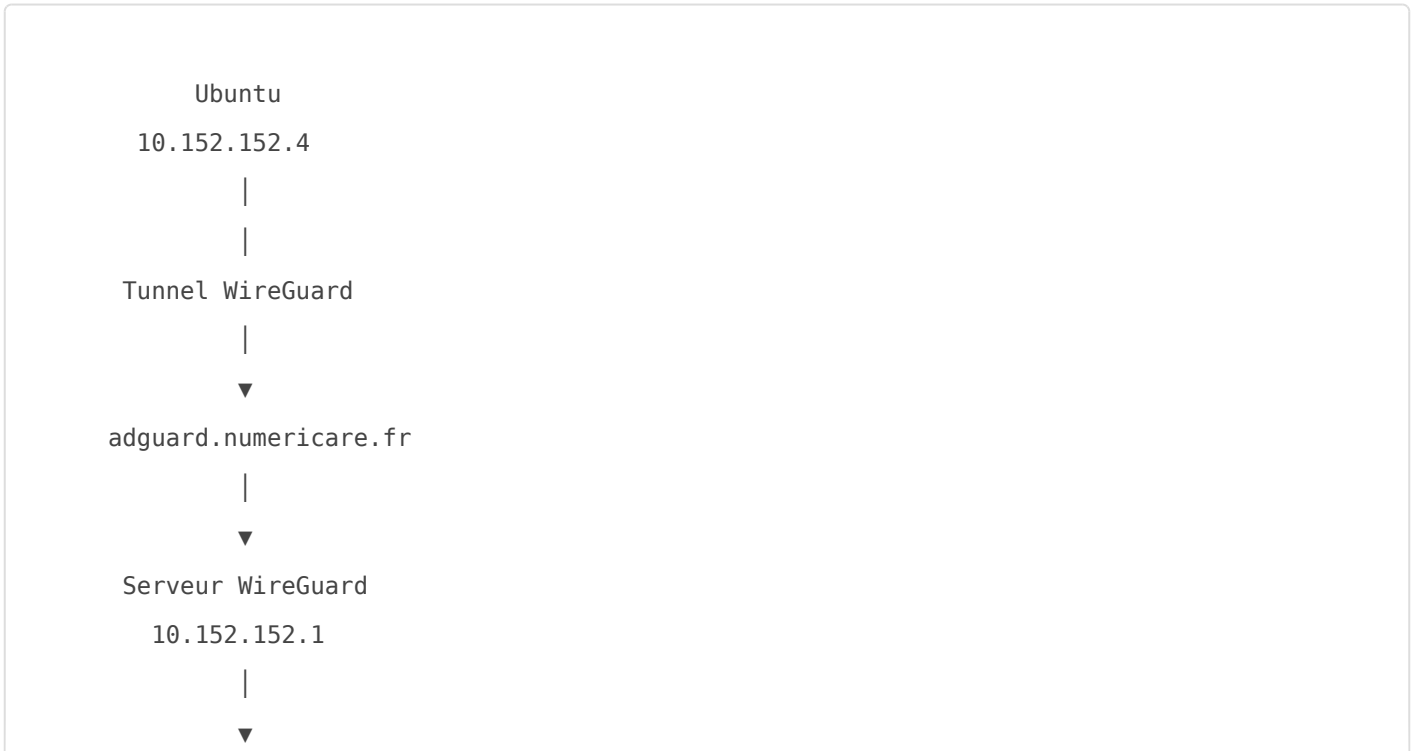
Cette page explique comment installer et configurer un client WireGuard sous Ubuntu afin d'accéder au réseau privé via le serveur VPN.

La configuration s'appuie sur le fichier **ubuntu.conf** généré lors de la création du client (voir chapitre 07).

Prérequis

- Le serveur WireGuard est opérationnel.
- Le client Ubuntu a été créé sur le serveur.
- Le fichier **ubuntu.conf** est disponible.
- Une connexion Internet est disponible.

Architecture



```
      Réseau ASUS
    10.151.151.0/24
```

---

1. Installer WireGuard

```
sudo apt update


sudo apt install wireguard -y
```

---

2. Vérifier l'installation

```
wg --version
```

Résultat attendu

```
wireguard-tools v1.x.x
```

---

3. Copier le fichier de configuration

Copier le fichier généré sur le serveur dans le répertoire système :

```
sudo cp ubuntu.conf /etc/wireguard/wg0.conf
```

---

4. Sécuriser les permissions

Le fichier contient la clé privée du client.

```
sudo chmod 600 /etc/wireguard/wg0.conf
```

Vérification :

```
ls -l /etc/wireguard/wg0.conf
```

Résultat attendu

```
-rw------- root root
```

---

5. Vérifier la configuration

```
sudo cat /etc/wireguard/wg0.conf
```

Le fichier doit contenir notamment :

```
[Interface]

Address = 10.152.152.4/32

DNS = 10.152.152.1



[Peer]

Endpoint = adguard.numericare.fr:51820

AllowedIPs = 10.151.151.0/24,10.152.152.0/24
```

---

6. Démarrer le tunnel

```
sudo wg-quick up wg0
```

Résultat attendu :

```


[#] ip link add wg0 type wireguard
[#] wg setconf wg0 ...
[#] ip address add ...
[#] ip link set up dev wg0
```

---

7. Vérifier l'interface VPN

```
ip addr show wg0
```

Résultat attendu

```
inet 10.152.152.4/32
```

---

8. Vérifier le tunnel

```
sudo wg
```

La sortie doit afficher :

- la clé publique du serveur ;
- un **Latest Handshake** récent ;
- les compteurs RX/TX.

---

9. Tester la connectivité

Tester le serveur VPN :

```
ping 10.152.152.1
```

Tester ensuite le réseau local :

```
ping 10.151.151.40
```

---

10. Vérifier le DNS

```
nslookup google.fr
```

Le serveur interrogé doit être :

```
10.152.152.1
```

11. Arrêter le tunnel

```
sudo wg-quick down wg0
```

12. Démarrage automatique (optionnel)

Pour établir automatiquement le VPN au démarrage :

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

Pour le désactiver :

```
sudo systemctl disable wg-quick@wg0
```

Commandes utiles

Commande	Description
`sudo wg`	Afficher l'état du tunnel.
`ip addr show wg0`	Afficher l'interface VPN.
`sudo wg-quick up wg0`	Démarrer le tunnel.
`sudo wg-quick down wg0`	Arrêter le tunnel.
`systemctl status wg-quick@wg0`	Afficher l'état du service.

Dépannage

L'interface wg0 n'existe pas

```
ip link show wg0
```

Vérifier que le fichier **/etc/wireguard/wg0.conf** est présent et correctement nommé.

Aucun Handshake

- Vérifier l'accès Internet.
- Contrôler le domaine **adguard.numericare.fr**.
- Vérifier le port UDP 51820.
- Contrôler les clés publiques.

Impossible d'accéder au LAN

- Contrôler les **AllowedIPs**.
- Vérifier que le serveur WireGuard est actif.
- Contrôler le routage IPv4 sur le serveur.

Le DNS ne fonctionne pas

```
resolvectl status
```

Le serveur DNS doit être :

```
10.152.152.1
```

Bonnes pratiques

- Conserver le fichier **ubuntu.conf** dans un emplacement sécurisé.
- Limiter les permissions du fichier de configuration.
- Utiliser une paire de clés unique par machine.
- Mettre régulièrement WireGuard à jour.
- Désactiver le tunnel lorsqu'il n'est plus utilisé.

Résumé

Élément	Statut
WireGuard installé	□
Configuration copiée	□

Élément	Statut
Tunnel opérationnel	
Connexion au réseau domestique	
DNS AdGuard fonctionnel	

> Le client Ubuntu est maintenant entièrement configuré et peut accéder de manière sécurisée au réseau domestique via WireGuard. La procédure pour Fedora est très proche, avec quelques différences liées au gestionnaire de paquets et aux outils d'administration.

Revision #1
Created 2026-07-30 08:03:51 UTC by Nico là
Updated 2026-07-30 08:04:19 UTC by Nico là