08.3 - Configuration d'un client Fedora

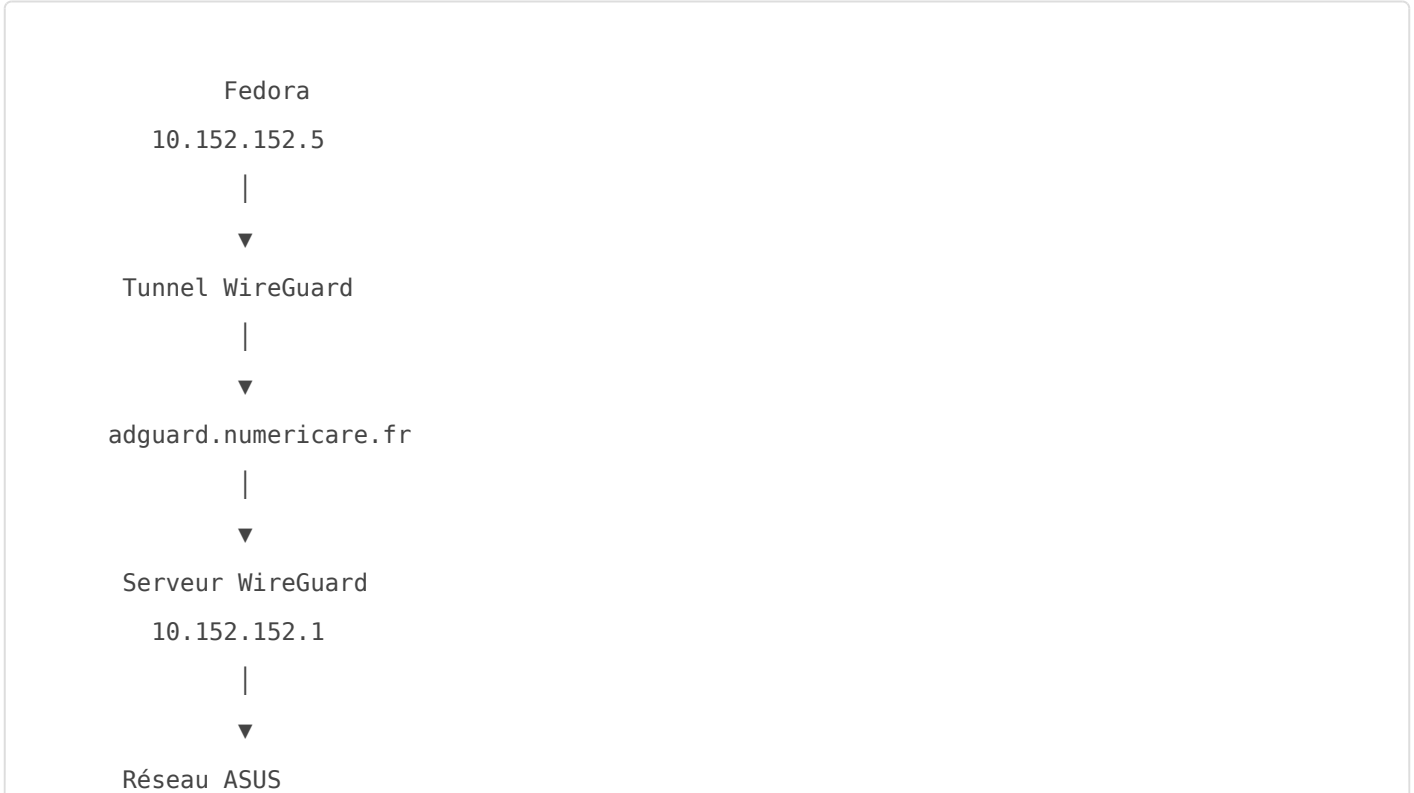
Cette page explique comment installer et configurer un client WireGuard sous Fedora afin d'accéder au réseau privé via le serveur VPN.

Le client utilisera la configuration générée lors du chapitre 07 (**fedora.conf**).

Prérequis

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

Architecture



```
    10.151.151.0/24
```

1. Installer WireGuard

```
sudo dnf install wireguard-tools -y
```

2. Vérifier l'installation

```
wg --version
```

Résultat attendu

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

3. Copier le fichier de configuration

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

4. Sécuriser le fichier

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

Vérifier :

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

Résultat attendu

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

5. Vérifier la configuration

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

Le fichier doit notamment contenir :

```
[Interface]

Address = 10.152.152.5/32

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'état du tunnel

```
sudo wg
```

La sortie doit afficher :

- le Peer du serveur ;
- un **Latest Handshake** récent ;
- les compteurs RX/TX.

---

8. Vérifier l'adresse IP

```
ip addr show wg0
```

Résultat attendu

```
inet 10.152.152.5/32
```

---

9. Tester la connectivité

```
ping 10.152.152.1
```

Puis :

```
ping 10.151.151.40
```

Les deux commandes doivent répondre.

---

10. Vérifier le DNS

```
nslookup google.fr
```

Le serveur DNS doit être :

```
10.152.152.1
```

Pour afficher la configuration DNS complète :

```
resolvectl status
```

11. Activer le démarrage automatique (optionnel)

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

Démarrer immédiatement :

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

Vérifier :

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

12. Arrêter le tunnel

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

Utilisation quotidienne

Commande	Description
`sudo wg-quick up wg0`	Démarrer le VPN.
`sudo wg-quick down wg0`	Arrêter le VPN.
`sudo wg`	Afficher l'état du tunnel.
`sudo wg show`	Afficher les statistiques détaillées.
`systemctl status wg-quick@wg0`	Afficher l'état du service.
`journalctl -u wg-quick@wg0`	Consulter les journaux.

Dépannage

Le tunnel ne démarre pas

```
journalctl -u wg-quick@wg0
```

Consulter les derniers messages d'erreur.

Aucun Handshake

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

Impossible d'accéder au réseau local

- Vérifier les **AllowedIPs**.
- Contrôler que le serveur WireGuard fonctionne.
- Vérifier le routage IPv4.

Le DNS n'utilise pas AdGuard Home

```
resolvectl status
```

Le serveur DNS actif doit être :

```
10.152.152.1
```

Bonnes pratiques

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

Résumé

Élément	Statut
WireGuard installé	
Configuration importée	
Tunnel établi	
Connexion au réseau domestique	
DNS AdGuard opérationnel	

> Le client Fedora est maintenant entièrement configuré et peut accéder au réseau domestique de manière sécurisée. Les chapitres suivants présentent la configuration des clients Android, iPhone/iPad et macOS.

Revision #1
Created 2026-07-30 08:05:15 UTC by Nico là
Updated 2026-07-30 08:05:42 UTC by Nico là