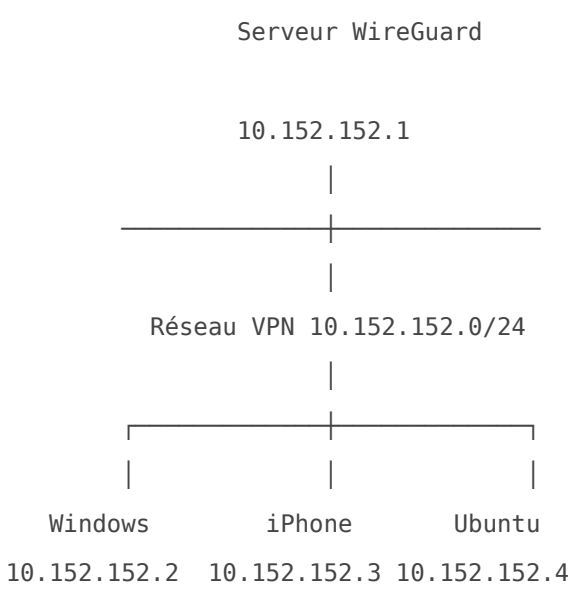
07 - Création d'un client WireGuard

Cette page décrit la procédure permettant d'ajouter un nouveau client au serveur WireGuard.

Chaque client possède sa propre paire de clés cryptographiques ainsi qu'une adresse IP dédiée sur le réseau VPN.

Architecture



---

1. Créer le dossier du client

Chaque client possède son propre répertoire contenant ses clés, sa configuration et, si nécessaire, son QR Code.

```
cd /opt/network/wireguard/clients


mkdir -p windows
```

```
cd windows
```

2. Générer les clés cryptographiques

Limiter les permissions des fichiers générés.

```
umask 077
```

Créer ensuite la paire de clés.

```
wg genkey | tee windows.key | wg pubkey > windows.pub
```

3. Vérifier les fichiers générés

```
ls -l
```

Résultat attendu

```
windows.key
windows.pub
```

4. Afficher les clés

```
cat windows.key


cat windows.pub
```

> **Important**
>
> - La clé privée reste exclusivement sur le client.
> - La clé publique sera ajoutée au serveur WireGuard.

5. Déclarer le client sur le serveur

Éditer le fichier de configuration du serveur.

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

Ajouter à la fin du fichier :

```
[Peer]

PublicKey = <CONTENU_DE_WINDOWS.PUB>

AllowedIPs = 10.152.152.2/32
```

Chaque client doit disposer d'une adresse IP unique.

Client	Adresse VPN
Windows	10.152.152.2
iPhone	10.152.152.3
Ubuntu	10.152.152.4
Android	10.152.152.5

---

6. Créer le fichier de configuration du client

```
nano windows.conf
```

Configuration du client

```
[Interface]

PrivateKey = <CONTENU_DE_WINDOWS.KEY>

Address = 10.152.152.2/32
```

```
DNS = 10.152.152.1


[Peer]

PublicKey = bdo5MJaEb+NSEk9x5I2yStIDUjvgvgAoZkeQDksSMT4=

Endpoint = adguard.numericare.fr:51820

AllowedIPs = 10.151.151.0/24,10.152.152.0/24

PersistentKeepalive = 25
```

Comprendre les paramètres

Paramètre	Description
PrivateKey	Clé privée du client.
Address	Adresse IP du client sur le VPN.
DNS	Serveur AdGuard Home accessible via le VPN.
Endpoint	Nom DNS public du serveur WireGuard.
AllowedIPs	Détermine les réseaux qui transitent dans le VPN.
PersistentKeepalive	Maintient la connexion active derrière un NAT.

Pourquoi utiliser ces AllowedIPs ?

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

Cette configuration met en œuvre un **Split Tunnel**.

- Le réseau domestique (10.151.151.0/24) passe dans le VPN.
- Le réseau VPN (10.152.152.0/24) passe également dans le tunnel.
- La navigation Internet continue d'utiliser la connexion locale du client.

Pourquoi utiliser DNS = 10.152.152.1 ?

Le serveur WireGuard héberge également AdGuard Home.

Les requêtes DNS transitent donc dans le VPN vers l'adresse du serveur WireGuard.

```
DNS = 10.152.152.1
```

Cette configuration permet de bénéficier du filtrage AdGuard même lorsque le client est connecté depuis Internet.

---

7. Recharger WireGuard

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

---

8. Vérifier que le client est enregistré

```
sudo wg
```

Le nouveau **Peer** doit apparaître.

---

9. Générer un QR Code (Android / iPhone)

```
qrencode -o /opt/network/wireguard/qr/windows.png < windows.conf
```

Ou directement dans le terminal :

```
qrencode -t ansiutf8 < windows.conf
```

---

10. Importer la configuration

Plateforme	Méthode
Windows	Importer le fichier **windows.conf** dans le client WireGuard.
Linux	Copier le fichier dans **/etc/wireguard/wg0.conf** puis démarrer **wg-quick**.
Android	Scanner le QR Code.
iPhone / iPad	Scanner le QR Code.

---

11. Vérifications

Une fois connecté :

```
ping 10.151.151.40
```

Puis :

```
nslookup google.fr
```

Le serveur DNS utilisé doit être :

```
10.152.152.1
```

Enfin, sur le serveur :

```
sudo wg
```

Le client doit apparaître avec :

- Latest Handshake
- Transfer RX
- Transfer TX

Bonnes pratiques

- Une paire de clés par client.
- Ne jamais réutiliser une clé privée.
- Attribuer une adresse VPN unique à chaque client.
- Conserver le fichier **.conf** avec les clés dans le dossier du client.

- Redémarrer WireGuard après l'ajout d'un nouveau Peer.
- Supprimer un Peer inutilisé afin de limiter la surface d'exposition.

Résumé

Élément	Statut
Clés générées	□
Peer ajouté au serveur	□
Configuration client créée	□
QR Code généré	□
Connexion prête	□

> Le client WireGuard est maintenant prêt à être utilisé. Les chapitres suivants détaillent la configuration spécifique de chaque plateforme (Windows, Ubuntu, Fedora, Android, iPhone et macOS).

Revision #3
Created 2026-07-30 07:55:54 UTC by Nico là
Updated 2026-08-06 11:49:36 UTC by Nico là