

08.4 - Configuration d'un client Android

Cette page explique comment installer et configurer WireGuard sur un smartphone ou une tablette Android afin d'accéder au réseau domestique de manière sécurisée.

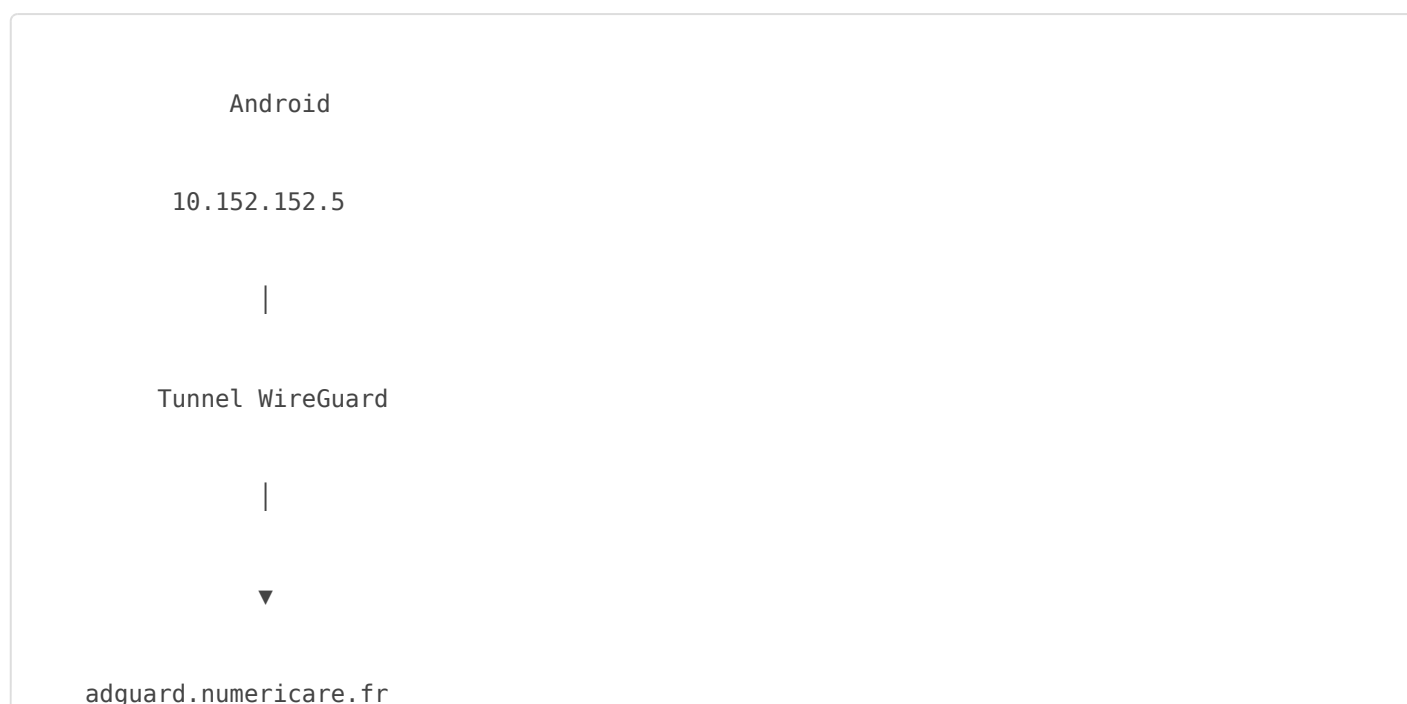
Deux méthodes d'import sont possibles :

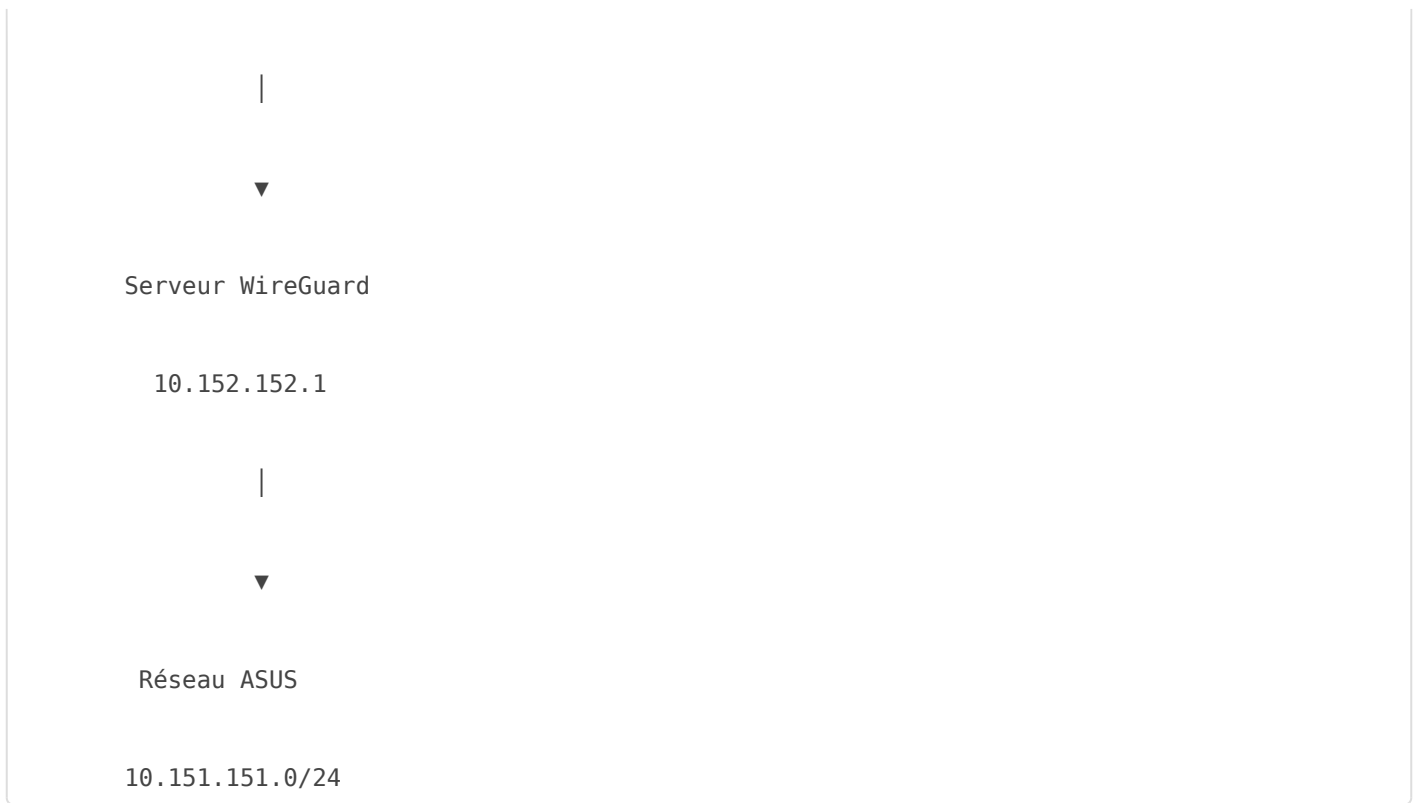
- Import via un QR Code (méthode recommandée).
- Import du fichier **android.conf**.

Prérequis

- Le serveur WireGuard est opérationnel.
- Le client Android a été créé (voir chapitre 07).
- Le QR Code ou le fichier **android.conf** est disponible.
- Une connexion Internet est disponible.

Architecture





1. Installer WireGuard

Installer l'application officielle **WireGuard** depuis le Google Play Store.

2. Ouvrir l'application

Au premier lancement, aucun tunnel n'est configuré.

3. Ajouter un tunnel

Appuyer sur le bouton :

+

Deux méthodes sont proposées :

- Scanner un QR Code.

- Importer depuis un fichier.

4. Import via QR Code (recommandé)

Sélectionner :

Scanner depuis un QR Code

Scanner le QR Code généré sur le serveur.

Le tunnel est automatiquement créé.

5. Import via un fichier

Si le QR Code n'est pas disponible :

Importer depuis un fichier

Sélectionner :

android.conf

6. Vérifier la configuration

Le tunnel doit contenir une configuration similaire à celle-ci :

```
[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
```

```
PersistentKeepalive = 25
```

7. Activer le tunnel

Appuyer sur l'interrupteur situé à droite du tunnel.

Android demande l'autorisation de créer un VPN.

Accepter la demande.

8. Vérifier la connexion

Une icône VPN apparaît dans la barre d'état Android.

Le tunnel est maintenant actif.

9. Vérifier le serveur

Depuis le serveur Debian :

```
sudo wg
```

Le client Android doit apparaître avec :

- Latest Handshake
 - Transfer RX
 - Transfer TX
-

10. Tester la connectivité

Depuis un navigateur Android, accéder à une application hébergée sur le réseau domestique.

Par exemple :

- Home Assistant
- BookStack
- Grafana
- NAS Synology

Si les applications sont accessibles, le tunnel fonctionne correctement.

11. Vérifier le DNS

Ouvrir un navigateur puis visiter un site de test DNS ou utiliser une application de diagnostic réseau.

Les requêtes DNS doivent être résolues par :

10.152.152.1

Le filtrage AdGuard Home est alors actif même en dehors du domicile.

12. Désactiver le VPN

Dans WireGuard, désactiver simplement l'interrupteur du tunnel.

Dépannage

Le tunnel ne se connecte pas

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

- Contrôler les clés du client.

Aucun Handshake

Sur le serveur :

```
sudo wg
```

Si aucun **Latest Handshake** n'apparaît, vérifier la configuration du client et la redirection du port UDP 51820.

Impossible d'accéder au réseau domestique

- Vérifier les **AllowedIPs**.
- Contrôler le routage IPv4 du serveur.
- Vérifier les règles NAT.

Les publicités ne sont pas bloquées

- Vérifier que le champ **DNS** est configuré avec **10.152.152.1**.
- Contrôler qu'aucun DNS privé Android n'est activé.

Bonnes pratiques

- Utiliser un tunnel différent pour chaque appareil Android.
- Ne jamais partager le QR Code avec une autre personne.
- Supprimer le tunnel si le téléphone est remplacé.
- Protéger le smartphone avec un code ou une authentification biométrique.
- Maintenir l'application WireGuard à jour.

Résumé

Élément	Statut
Application WireGuard installée	☑

Élément	Statut
Tunnel importé	☐
Connexion VPN établie	☐
Accès au réseau domestique	☐
DNS AdGuard opérationnel	☐

“ Le client Android est maintenant entièrement configuré. Le chapitre suivant présente la procédure équivalente pour un iPhone ou un iPad.

Revision #1
Created 2026-07-30 08:07:31 UTC by Nico là
Updated 2026-07-30 08:08:06 UTC by Nico là