08.1 - Configuration d'un client Windows 11

Cette page explique comment installer et configurer le client WireGuard sous Windows 11 afin d'accéder au réseau privé via le serveur VPN.

À l'issue de cette procédure, l'ordinateur pourra se connecter au réseau domestique en toute sécurité et utiliser AdGuard Home comme serveur DNS.

Prérequis

- Le serveur WireGuard est opérationnel.
- Le client Windows a été créé sur le serveur (voir chapitre 07).
- Le fichier **windows.conf** est disponible.
- Une connexion Internet est disponible.

Architecture

```
      Internet
          |
          ▼
adguard.numericare.fr
          |
 UDP 51820
          |
          ▼
 Serveur WireGuard
   10.152.152.1
          |
 ─────────────────
          |
Réseau ASUS
```

```
    10.151.151.0/24
```

1. Installer WireGuard

Télécharger puis installer le client officiel WireGuard pour Windows.

Conserver les options d'installation par défaut.

2. Lancer WireGuard

Au premier lancement, la liste des tunnels est vide.

```
No tunnels configured.
```

3. Importer la configuration

Cliquer sur :

```
Import tunnel(s) from file...
```

Sélectionner le fichier :

```
windows.conf
```

Le tunnel apparaît immédiatement dans la liste.

4. Vérifier la configuration

Le contenu doit être similaire à celui-ci :

```
[Interface]

PrivateKey = xxxxxxxxxxxxxxxxxxxxxxxxx

Address = 10.152.152.2/32

DNS = 10.152.152.1


[Peer]

PublicKey = xxxxxxxxxxxxxxxxxxxxxxxxx

Endpoint = adguard.numericare.fr:51820

AllowedIPs = 10.151.151.0/24,10.152.152.0/24

PersistentKeepalive = 25
```

Comprendre les paramètres

Paramètre	Description
Address	Adresse VPN attribuée au poste Windows.
DNS	Utilisation d'AdGuard Home via le VPN.
Endpoint	Adresse publique du serveur WireGuard.
AllowedIPs	Réseaux accessibles via le VPN (Split Tunnel).
PersistentKeepalive	Maintient la connexion ouverte derrière un NAT.

---

5. Établir la connexion

Cliquer sur :

```
Activate
```

L'état du tunnel devient :

```
Active
```

---

6. Vérifier l'adresse IP VPN

Ouvrir PowerShell :

```
ipconfig
```

Une nouvelle interface WireGuard doit apparaître.

Résultat attendu

```
Adresse IPv4 : 10.152.152.2
```

---

7. Tester la connectivité

Tester le serveur WireGuard :

```
ping 10.152.152.1
```

Tester ensuite le serveur Docker / AdGuard :

```
ping 10.151.151.40
```

Les deux réponses doivent être positives.

---

8. Vérifier le DNS

Exécuter :

```
nslookup google.fr
```

Le serveur DNS utilisé doit être :

```
10.152.152.1
```

Cela confirme que toutes les requêtes DNS transitent par AdGuard Home.

---

9. Vérifier le serveur

Depuis le serveur Debian :

```
sudo wg
```

Le client Windows doit apparaître.

Exemple

```
peer: xxxxxxxxxxxxxxxx

latest handshake: 25 seconds ago

transfer: 48 KiB received

transfer: 120 KiB sent
```

---

10. Déconnecter le VPN

Dans WireGuard, cliquer sur :

```
Deactivate
```

La connexion VPN est immédiatement interrompue.

Dépannage

Le tunnel reste inactif

- Vérifier la connexion Internet.
- Vérifier le port UDP 51820 sur le routeur.
- Contrôler l'adresse Endpoint.
- Vérifier la clé publique du serveur.

Aucun Handshake

Sur le serveur :

```
sudo wg
```

Si aucun **Latest Handshake** n'apparaît :

- vérifier la redirection UDP 51820 ;
- contrôler le pare-feu Windows ;
- vérifier que le domaine DNS pointe vers l'adresse IP publique correcte ;
- contrôler les clés publiques et privées.

Impossible d'accéder au réseau domestique

- Vérifier les **AllowedIPs**.
- Vérifier que le routage IPv4 est activé sur le serveur.
- Contrôler les règles NAT (iptables).

Les publicités ne sont pas bloquées

- Contrôler que le DNS est bien **10.152.152.1**.
- Tester avec :

```
nslookup google.fr
```

Le serveur interrogé doit être WireGuard / AdGuard Home.

Bonnes pratiques

- Conserver le fichier **windows.conf** dans un emplacement sécurisé.
- Ne jamais partager la clé privée.
- Installer les mises à jour du client WireGuard.
- Désactiver le tunnel lorsqu'il n'est plus nécessaire.
- Contrôler régulièrement le nombre de Peers autorisés sur le serveur.

Résumé

Élément	Statut
Client WireGuard installé	□
Configuration importée	□
Tunnel établi	□
Connexion au réseau domestique	□
DNS AdGuard fonctionnel	□

> Le client Windows est désormais entièrement configuré. Les chapitres suivants présentent la configuration des autres plateformes (Ubuntu, Fedora, Android, iPhone/iPad et macOS), dont la logique est similaire mais avec des méthodes d'installation propres à chaque système.

Revision #1
Created 2026-07-30 07:58:05 UTC by Nico là
Updated 2026-07-30 08:00:23 UTC by Nico là