08.6 - Configuration d'un client macOS

Cette page explique comment installer et configurer WireGuard sur macOS afin d'accéder au réseau domestique via le serveur VPN.

La méthode recommandée consiste à utiliser l'application officielle WireGuard disponible sur l'App Store.

Prérequis

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

Architecture

```
macOS

10.152.152.6

|

Tunnel WireGuard

|

▼

adguard.numericare.fr
```

```
            |
            ▼
     Serveur WireGuard
       10.152.152.1
            |
            ▼
      Réseau ASUS
     10.151.151.0/24
```

---

1. Installer WireGuard

Installer l'application officielle **WireGuard** depuis l'App Store.

---

2. Ouvrir l'application

Au premier lancement, aucune configuration VPN n'est présente.

---

3. Importer un tunnel

Cliquer sur :

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

Puis sélectionner le fichier :

```
macos.conf
```

Le tunnel est automatiquement ajouté.

---

4. Vérifier la configuration

La configuration doit être similaire à :

```
[Interface]

PrivateKey = xxxxxxxxxxxxxxxxxxxxxxxx

Address = 10.152.152.6/32

DNS = 10.152.152.1


[Peer]

PublicKey = xxxxxxxxxxxxxxxxxxxxxxxx

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 Mac.
DNS	Utilisation d'AdGuard Home via le tunnel VPN.
Endpoint	Nom DNS public du serveur WireGuard.
AllowedIPs	Réseaux accessibles via le VPN (Split Tunnel).
PersistentKeepalive	Maintient la connexion active derrière un routeur NAT.

---

5. Activer le tunnel

Cliquer sur :

```
Activate
```

Lors de la première connexion, macOS demande l'autorisation d'ajouter une configuration VPN.

Valider la demande puis s'authentifier avec Touch ID ou le mot de passe de la session.

---

6. Vérifier la connexion

Une icône VPN apparaît dans la barre de menus de macOS.

Le tunnel est maintenant actif.

---

7. Vérifier le serveur

Depuis le serveur Debian :

```
sudo wg
```

Le client macOS doit apparaître avec :

- Latest Handshake
- Transfer RX
- Transfer TX

---

8. Tester la connectivité

Ouvrir le Terminal puis exécuter :

```
ping 10.152.152.1
```

Puis :

```
ping 10.151.151.40
```

Les deux commandes doivent répondre.

---

9. Vérifier le DNS

Afficher la configuration DNS active :

```
scutil --dns
```

Le serveur DNS utilisé par le tunnel doit être :

```
10.152.152.1
```

Le filtrage AdGuard Home est alors appliqué aux requêtes DNS transitant par le VPN.

---

10. Désactiver le VPN

Dans WireGuard, cliquer sur :

```

Deactivate
```

Le tunnel est immédiatement fermé.

Utilisation avancée (Terminal)

Les utilisateurs avancés peuvent également gérer le tunnel en ligne de commande à l'aide de **wg-quick** (si les outils WireGuard sont installés).

```
sudo wg-quick up wg0

sudo wg

sudo wg-quick down wg0
```

Dépannage

Le tunnel ne se connecte pas

- Vérifier la connexion Internet.
- Contrôler que **adguard.numericare.fr** est résolu correctement.
- Vérifier l'ouverture du port UDP 51820.
- Contrôler les clés publiques et privées.

Aucun Handshake

Depuis 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 sur le serveur.
- Vérifier les règles NAT.

Les publicités ne sont pas bloquées

- Vérifier que le DNS du tunnel est bien **10.152.152.1**.
- Contrôler qu'aucun autre logiciel VPN ou DNS n'est actif.

Bonnes pratiques

- Conserver le fichier **macos.conf** dans un emplacement sécurisé.
- Ne jamais partager la clé privée.
- Mettre régulièrement macOS et WireGuard à jour.

- Utiliser un tunnel distinct pour chaque Mac.
- Désactiver le VPN lorsqu'il n'est plus nécessaire.

Résumé

Élément	Statut
Application WireGuard installée	□
Configuration importée	□
Tunnel établi	□
Accès au réseau domestique	□
DNS AdGuard opérationnel	□

> Le client macOS est désormais entièrement configuré et peut accéder au réseau domestique de manière sécurisée via WireGuard. Vous disposez maintenant d'une procédure complète pour les principales plateformes : Windows, Ubuntu, Fedora, Android, iPhone/iPad et macOS.

Revision #1
Created 2026-07-30 08:10:47 UTC by Nico là
Updated 2026-07-30 08:11:02 UTC by Nico là