

09 - Mise à jour de WireGuard

Cette page décrit la procédure recommandée pour mettre à jour WireGuard et ses composants sur le serveur Debian hébergeant le service VPN.

L'objectif est de bénéficier des dernières corrections de sécurité, des améliorations de stabilité et des nouvelles fonctionnalités tout en garantissant la continuité du service.

Prérequis

- Disposer d'un accès SSH au serveur.
 - Être connecté avec un compte disposant des privilèges **sudo**.
 - Vérifier qu'aucune opération de maintenance n'est en cours.
-

1. Vérifier la version installée

Afficher la version des outils WireGuard :

```
wg --version
```

Exemple :

```
wireguard-tools v1.0.20210914
```

2. Vérifier les mises à jour disponibles

```
sudo apt update
```

Puis afficher les paquets pouvant être mis à jour :

```
apt list --upgradable
```

Si une nouvelle version de **wireguard** ou **wireguard-tools** apparaît dans la liste, une mise à jour est disponible.

3. Mettre à jour le système

```
sudo apt upgrade -y
```

Cette commande met à jour l'ensemble des paquets installés, y compris WireGuard si une nouvelle version est disponible.

4. Vérifier que le service est toujours actif

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

Le résultat attendu est similaire à :

```
Active: active (exited)
```

5. Vérifier le fonctionnement du tunnel

```
sudo wg
```

Contrôler notamment les informations suivantes :

- Présence de l'interface **wg0**.
 - Liste des clients configurés.
 - Derniers **Handshake**.
 - Compteurs RX/TX.
-

6. Vérifier l'écoute du port UDP

```
sudo ss -ltnp | grep 51820
```

Le serveur doit toujours être à l'écoute sur le port UDP **51820**.

7. Tester la connectivité

Depuis un client WireGuard :

- Établir le tunnel VPN.
- Accéder au réseau **10.151.151.0/24**.
- Vérifier la résolution DNS via AdGuard Home.

8. Redémarrer le service (si nécessaire)

Dans la majorité des cas, aucun redémarrage n'est nécessaire. Si toutefois la mise à jour le requiert, exécuter :

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

Vérifier ensuite le statut du service :

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

9. Consulter les journaux

En cas d'anomalie après la mise à jour :

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

Ou uniquement les derniers événements :

```
journalctl -u wg-quick@wg0 -n 50
```

Bonnes pratiques

- Mettre régulièrement le système Debian à jour.
- Effectuer les mises à jour durant une période de faible utilisation.
- Vérifier le bon fonctionnement des clients après chaque mise à jour.

- Contrôler les journaux système en cas d'anomalie.
- Maintenir le système d'exploitation également à jour afin de bénéficier des derniers correctifs de sécurité.

Résumé

Étape	Validation
Version vérifiée	☐
Paquets mis à jour	☐
Service WireGuard opérationnel	☐
Port UDP 51820 à l'écoute	☐
Tests de connexion validés	☐

“ La mise à jour de WireGuard est terminée. Le serveur bénéficie des dernières corrections tout en conservant sa configuration existante. Il est recommandé de vérifier le bon fonctionnement des clients après chaque mise à jour afin de garantir la disponibilité du service VPN.

Revision #1

Created 2026-07-30 08:19:55 UTC by Nico là

Updated 2026-07-30 08:20:22 UTC by Nico là