GL·iNet



Manuel d’utilisation

GL-MG1300 / Mango 2

Mini-routeur de voyage double bande

Version du micrologiciel 4.10.0

À propos de ce manuel

Ce manuel vous accompagne dans la prise en main de votre appareil. Il présente le produit, les connexions matérielles, l'accès à l'interface d'administration Web, la configuration initiale et les instructions détaillées pour toutes les fonctions logicielles de l'interface d'administration Web.

Ce guide vous permettra de :

- Découvrir les principales caractéristiques du produit
- Choisir un emplacement adapté à l'appareil
- Effectuer les branchements en suivant les instructions étape par étape
- Vous connecter facilement à l'interface d'administration Web
- Configurer les paramètres initiaux et maîtriser toutes les fonctions logicielles de l'interface d'administration Web

Conventions utilisées

Ces symboles et couleurs vous aident à suivre les étapes plus facilement.

Convention	Signification
Texte turquoise souligné	Lien cliquable permettant d'ouvrir une page Web ou une section précise
Texte en gras	Met en évidence des informations importantes, notamment les titres, les liens et les noms exacts des menus et des éléments de l'interface Web de l'appareil
>	Chemin d'accès à la page correspondante (par exemple, Système > Micrologiciel)
Remarque	Informations essentielles pour la configuration, l'utilisation et la sécurité. Leur non-respect peut entraîner un échec de configuration, un dysfonctionnement ou des dommages matériels
Conseils	Conseils pour tirer le meilleur parti de votre appareil

Remarque :

- Les fonctions de l'appareil peuvent varier selon le modèle et la version du micrologiciel.
- La disponibilité des produits varie selon les régions ou les spécifications du fournisseur d'accès à Internet (FAI).
- Les images, procédures et descriptions de ce guide sont fournies à titre d'illustration et peuvent différer de votre situation réelle.

Besoin d’aide ou d’informations complémentaires ?

- Mise à jour du micrologiciel : Centre de téléchargement des micrologiciels GL.iNet | Routeurs
- Communauté : échangez sur nos produits et partagez vos expériences sur le forum de la communauté GL.iNet
- Assistance technique : contactez notre équipe d’assistance depuis la page de contact

Copyright © 2026 GL.iNet Technology (HK) Ltd. Tous droits réservés.

Aucune partie de ce manuel ne peut être reproduite, transcrite, traduite ou distribuée, sous quelque forme ou par quelque moyen que ce soit, sans l’autorisation écrite préalable de GL.iNet Technology (HK) Ltd. GL.iNet est une marque déposée de GL.iNet Technology (Hong Kong) Ltd. en Chine et/ou dans d’autres pays et régions. Tous les autres noms de marques et de produits mentionnés appartiennent à leurs propriétaires respectifs et sont des marques commerciales ou déposées.

Le contenu de ce document peut être modifié sans préavis, notamment à la suite de mises à jour du produit. Sauf accord contraire, ce document est fourni à titre informatif uniquement. Les déclarations, informations et recommandations qu’il contient ne constituent aucune forme de garantie.

GL Tech (HK) Ltd : #601, 5W, Hong Kong Science Park, N.T. Hong Kong
GL Intelligence, Inc. : 10400 Eaton Place, Suite 215, Fairfax, VA 22030

Table des matières

Chapitre 1 Présentation de votre routeur 9

1.1 Présentation du produit 10

1.1.1 Aspect extérieur 10

1.1.2 Ports et boutons 11

1.1.3 LED 12

1.2 Caractéristiques techniques 12

1.3 Contenu de l'emballage 14

Chapitre 2 Branchements 15

2.1 Choix de l'emplacement 16

2.2 Branchement du routeur 16

Chapitre 3 Connexion à l'interface du routeur 17

Chapitre 4 Configuration de la connexion Internet 19

4.1 Assistant de configuration rapide 20

4.2 Configuration manuelle de la connexion Internet 21

4.2.1 Connexion à Internet par câble Ethernet 22

4.2.2 Connexion à Internet via un réseau Wi-Fi existant 27

4.2.3 Connexion à Internet par partage de connexion USB 33

4.2.4 Connexion à Internet via un modem USB 38

Chapitre 5 Réseau sans fil 40

5.1 Affichage de l'état du Wi-Fi 41

5.2 Paramètres sans fil 42

5.2.1 Réseau principal 42

5.2.2 Réseau invité 43

5.2.3 Réseau IoT 45

Chapitre 6 Appareils clients 47

6.1 Informations sur les appareils 49

6.2 Actions 51

6.3 Suppression de clients 55

6.4 Tri 56

Chapitre 7 Services cloud 57

7.1 GL.iNet Account 58

7.1.1 Activer GL.iNet Account 58
7.1.2 Dissocier GL.iNet Account 61
7.2 GoodCloud 62
7.2.1 Activation de GoodCloud 62
7.2.2 Gestion de votre routeur 66
7.2.3 Dissociation de l'appareil 70
7.3 GoodPAS 71
7.3.1 Configuration rapide 71
7.3.2 Vérification de la connexion 75
7.3.3 Passer à l'offre supérieure 76
Chapitre 8 Comprendre les VPN 77
8.1 Introduction 78
8.2 Cas d'utilisation 79
Chapitre 9 Tableau de bord VPN 81
9.1 Importation d'un profil VPN 82
9.2 Ajout d'un tunnel VPN 86
9.2.1 Procédure générale 86
9.2.2 Exemples de configuration 89
9.3 Kill Switch 107
9.4 Tout autre trafic 108
9.5 Options du tunnel 109
9.6 Priorité des tunnels 111
Chapitre 10 Configuration d'un serveur VPN 114
10.1 Configuration d'un serveur OpenVPN 115
10.1.1 Préparation 115
10.1.2 Étapes de configuration 116
10.1.3 Dépannage 119
10.2 Configuration d'un serveur WireGuard 120
10.2.1 Préparation 120
10.2.2 Étapes de configuration 121
10.2.3 Dépannage 124
Chapitre 11 Configuration d'un client VPN 125
11.1 Configuration d'un client OpenVPN 126
11.1.1 Préparation 126

11.1.2 Configuration de NordVPN 126
11.1.3 Configuration manuelle d'un client OpenVPN pour un autre fournisseur 132
11.2 Configuration d'un client WireGuard 135
11.2.1 Préparation 135
11.2.2 Configuration d'AzireVPN 136
11.2.3 Configuration de Hide.me 141
11.2.4 Configuration d'IPVanish 144
11.2.5 Configuration de Mullvad 149
11.2.6 Configuration de NordVPN 154
11.2.7 Configuration de PIA (Private Internet Access) 159
11.2.8 Configuration de Surfshark 164
11.2.9 Configuration manuelle d'un client WireGuard pour un autre fournisseur 169
Chapitre 12 Réseau 175
12.1 Multi-WAN 176
12.1.1 Suivi de l'état des interfaces 176
12.1.2 Mode Multi-WAN 179
12.2 Sous-réseau 182
12.2.1 Réseau principal 182
12.2.2 Réseau invité 188
12.2.3 Réseau IoT 193
12.2.4 Réseaux VLAN 197
12.3 Ports Ethernet 201
12.3.1 WAN 202
12.3.2 LAN 203
12.3.3 Double connexion WAN Ethernet 205
12.4 DNS 207
12.4.1 Paramètres du serveur DNS 208
12.4.2 Modification du fichier hosts 210
12.5 IPv6 212
12.5.1 Mode IPv6 213
12.5.2 Méthode d'obtention du DNS 213
12.6 IGMP Snooping 214
12.7 Mode réseau 215
12.8 Accélération réseau 217

Chapitre 13 Contrôle des flux 219
13.1 Contrôle parental 220
Chapitre 14 Sécurité 227
14.1 Redirection de port 228
14.1.1 DMZ 228
14.1.2 Redirection de port 229
14.2 Accès administrateur 232
14.2.1 Contrôle d'accès 232
14.2.2 Contrôle d'accès distant 235
14.2.3 Ouverture de ports sur le routeur 236
14.3 Mode NAT 237
Chapitre 15 Applications 238
15.1 Extensions 239
15.2 DNS dynamique 240
15.2.1 Activation du DDNS 240
15.2.2 Vérification du fonctionnement du DDNS 243
15.2.3 Accès HTTPS à distance 245
15.2.4 Accès SSH à distance 248
15.3 Stockage réseau 250
15.3.1 Branchement du stockage 250
15.3.2 Configuration de Samba 251
15.4 Tailscale 254
15.4.1 Configuration de Tailscale 255
15.4.2 Annoncer les sous-réseaux WAN 258
15.4.3 Annoncer les sous-réseaux LAN 259
15.4.4 Nœuds de sortie personnalisés 260
15.4.5 Exécuter un nœud de sortie 261
Chapitre 16 Système 268
16.1 Vue d'ensemble 269
16.2 Mot de passe administrateur 270
16.3 Mise à jour 271
16.3.1 Mise à jour en ligne 271
16.3.2 Mise à jour locale 272
16.4 Tâches planifiées 274

16.4.1 Programmation du voyant LED 274
16.4.2 Redémarrage planifié 275
16.4.3 Programmation du Wi-Fi 5 GHz 275
16.4.4 Programmation du Wi-Fi 2,4 GHz 277
16.5 Fuseau horaire 281
16.6 Paramètres du commutateur 282
16.7 Réinitialisation du micrologiciel 283
16.8 Journaux 284
16.9 Paramètres avancés 286
Déclaration de conformité 288

Chapitre 1

Présentation de votre routeur

Ce chapitre présente le routeur, ses caractéristiques techniques et le contenu de l’emballage.

1.1 Présentation du produit

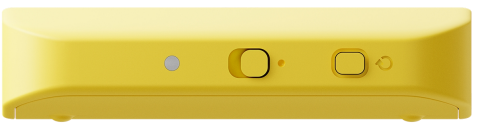
Mango 2 est le premier mini-routeur de voyage Wi-Fi 5 double bande de GL.iNet. Son boîtier ultrafin facilite le transport. Il offre des débits théoriques de 400 Mbit/s sur la bande 2,4 GHz et de 866 Mbit/s sur la bande 5 GHz, avec une configuration MIMO 2×2. OpenVPN et WireGuard sont préinstallés. Il prend en charge plus de 30 services VPN, chiffre automatiquement tout le trafic réseau et permet la gestion à distance via GoodCloud, pour allier performances, praticité et sécurité.

1.1.1 Aspect extérieur

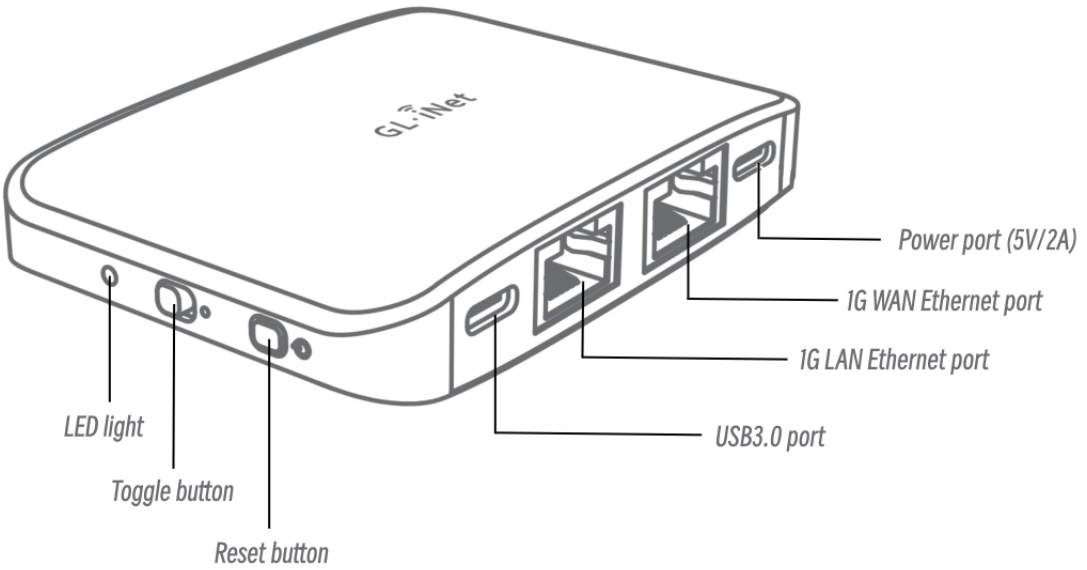








1.1.2 Ports et boutons



Élément	Description
Prise d'alimentation	Permet de brancher l'adaptateur secteur.
Port WAN 1G	Permet de relier le routeur à un modem ou à une prise Ethernet pour accéder à Internet.
Port LAN 1G	Permet de brancher des appareils filaires si nécessaire.
Port USB 3.0	Pour les supports de stockage USB, le partage de connexion USB d'un téléphone et les clés de connexion mobile compatibles.
Bouton de réinitialisation	Maintenez le bouton enfoncé pendant **3 secondes** puis relâchez-le pour réparer votre réseau.
	Maintenez le bouton enfoncé pendant **8 secondes** puis relâchez-le : le routeur retrouve ses paramètres d'usine.
Commutateur	Le commutateur physique permet de modifier certains paramètres d'un simple geste. Configurez-le dans l'interface d'administration Web pour activer ou désactiver les fonctions souhaitées.

1.1.3 LED

État	Signification
Bleu fixe	Démarrage en cours
Bleu à pulsation lente	Appareil démarré, sans connexion Internet
Blanc fixe	Connexion Internet établie
Bleu clignotant rapidement	Réinitialisation en cours

1.2 Caractéristiques techniques

Interfaces	1 port Ethernet WAN 1G 1 port Ethernet LAN 1G 1 port USB 3.0 1 port d'alimentation Type-C 1 bouton de réinitialisation 1 commutateur
CPU	MediaTek, double cœur à 880 MHz
Mémoire / Stockage	DDR3 128MB / NOR 2MB + NAND 128MB
Protocoles	IEEE 802.11a/b/g/n/ac
Débit Wi-Fi	400 Mbit/s (2,4 GHz), 866 Mbit/s (5 GHz)
Antennes	2 antennes Wi-Fi internes
Débit Ethernet	10/100/1 000 Mbit/s
Alimentation	Type-C, 5 V/2 A
Consommation électrique	< 5 W (sans charge USB)
Température de fonctionnement	0 à 40 °C (32 à 104 °F)

Température de stockage	−20 à 70 °C (−4 à 158 °F)
Dimensions / Poids	89 × 63 × 15 mm / 100 g
Autres ressources	Fiche technique / Micrologiciel / Application / Tutoriels

*Les débits Wi-Fi reposent sur les normes IEEE 802.11, par exemple 802.11ac pour le Wi-Fi 5. Le débit réel et la portée peuvent être inférieurs en raison d'obstacles (murs, métal), de la congestion du réseau ou des capacités des appareils clients.

*L'utilisation du Wi-Fi 5 (802.11ac) et de ses fonctions (DL MU-MIMO, 256-QAM) nécessite des appareils clients compatibles avec ces technologies.

1.3 Contenu de l’emballage

L’emballage contient :

- 1 Mango 2 (GL-MG1300)
- 1 câble d’alimentation USB-C vers USB-C
- 1 manuel d’utilisation
- 1 carte de remerciement



1 x User manual



1 x Mango 2 (GL-MG1300)



1 x Thank You Card



1 x Power cable

Chapitre 2

Branchements

Ce chapitre explique comment choisir l’emplacement du routeur et effectuer les branchements.

2.1 Choix de l’emplacement

Suivez ces conseils pour choisir un emplacement offrant les meilleures performances.

- **Évitez l’humidité et la chaleu**r : ne placez pas le routeur dans un endroit exposé à l’eau, à l’humidité ou à des températures élevées, par exemple près d’un évier ou d’un radiateur.
- **Ventilation et refroidissement** : placez le routeur dans un endroit frais et bien ventilé pour permettre une bonne dissipation de la chaleur.
- **Emplacement central** : placez le routeur à un endroit permettant de le brancher facilement à une prise de courant et de connecter plusieurs appareils, par exemple au centre du salon.
- **Disposition des câbles** : disposez les câbles et le cordon d’alimentation de manière à éviter tout risque de trébuchement.
- **Surface stable** : posez le routeur sur une surface plane et horizontale, comme une étagère ou un bureau, pour assurer sa stabilité.
- **Évitez les interférences électromagnétiques** : éloignez le routeur des sources d’interférences, comme les appareils Bluetooth ou les fours à micro-ondes, pour limiter les perturbations du signal.

2.2 Branchement du routeur

1. **Mise sous tension**

   Assemblez les deux parties de l’adaptateur secteur. Branchez-le au routeur, puis à une prise de courant. Le routeur démarre automatiquement.
2. **Connexion d’un appareil au routeur**

   Connectez un appareil, tel qu’un ordinateur portable ou un smartphone, au routeur par Wi-Fi ou à l’aide d’un câble Ethernet.
   - **Wi-Fi** : sur votre appareil, ouvrez Paramètres > WLAN, repérez le nom du réseau Wi-Fi du routeur dans la liste des réseaux disponibles et saisissez le mot de passe. Le nom du réseau et le mot de passe par défaut figurent sur l’étiquette du routeur.
   - **Ethernet** : reliez votre appareil à un port LAN du routeur à l’aide d’un câble Ethernet.
3. **Connexion à l’interface du routeur**

   Lors de la première connexion au routeur, Internet n’est pas encore disponible. Connectez-vous à l’interface du routeur comme indiqué au chapitre 3 et effectuez la configuration initiale pour accéder à Internet.

Chapitre 3

Connexion à l’interface du routeur

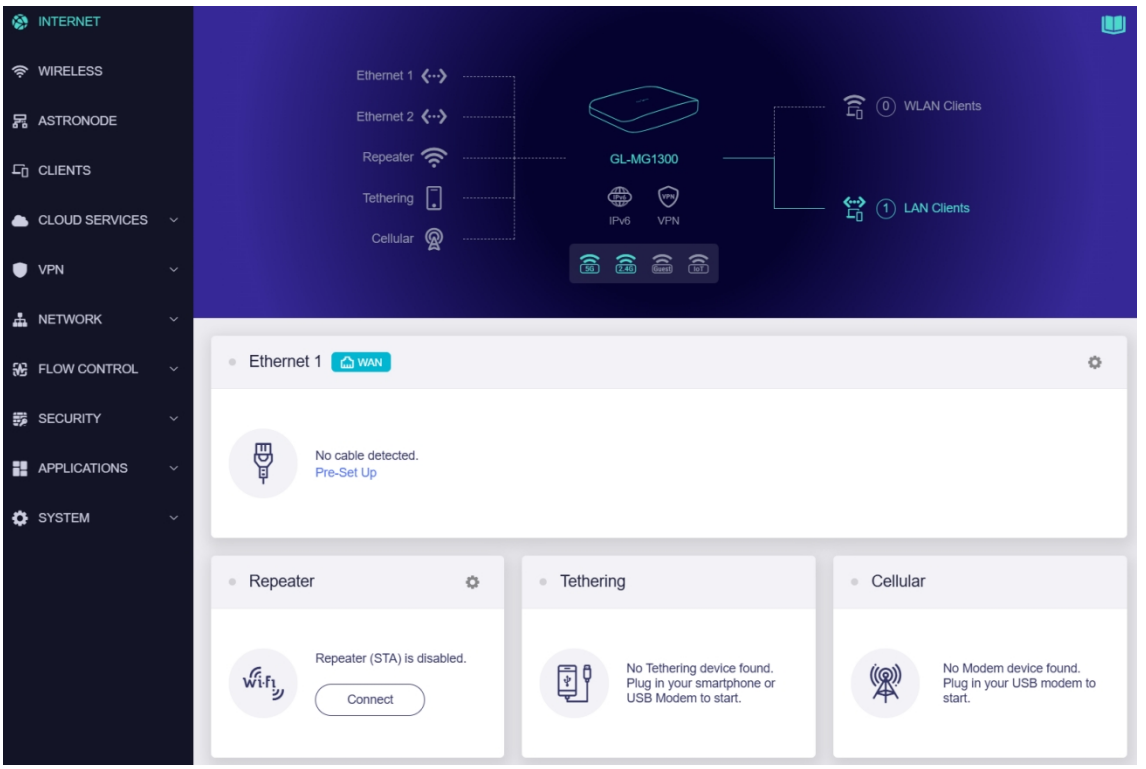
Ce chapitre explique comment accéder à l’interface d’administration Web de votre routeur.

Configurez et gérez votre routeur depuis une interface d'administration Web accessible sur Windows, macOS ou Linux avec un navigateur, comme Microsoft Edge, Google Chrome, Mozilla Firefox ou Apple Safari.

Remarque : si vous préférez utiliser l'application GL.iNet plutôt que l'interface d'administration Web, téléchargez l'application et suivez les instructions à l'écran.

Suivez les étapes ci-dessous pour accéder à l'interface d'administration Web du routeur.

1. Connectez un appareil (par exemple, un ordinateur de bureau ou portable) au routeur par Wi-Fi ou avec un câble Ethernet.
2. Ouvrez un navigateur Web (Chrome et Edge sont recommandés) et accédez à http://192.168.8.1. La page de connexion à l'interface d'administration Web s'affiche. Si vous ne parvenez pas à accéder à cette interface, consultez cette page pour résoudre le problème.
3. Définissez votre mot de passe administrateur. Pour renforcer la sécurité, choisissez un mot de passe robuste. Cliquez ensuite sur **Suivant (Next)** pour continuer.
4. Vous accédez ensuite à l'interface d'administration Web du routeur.



Chapitre 4

Configuration de la connexion Internet

Ce chapitre présente les différentes méthodes de connexion Internet permettant d’adapter le routeur à votre environnement réseau.

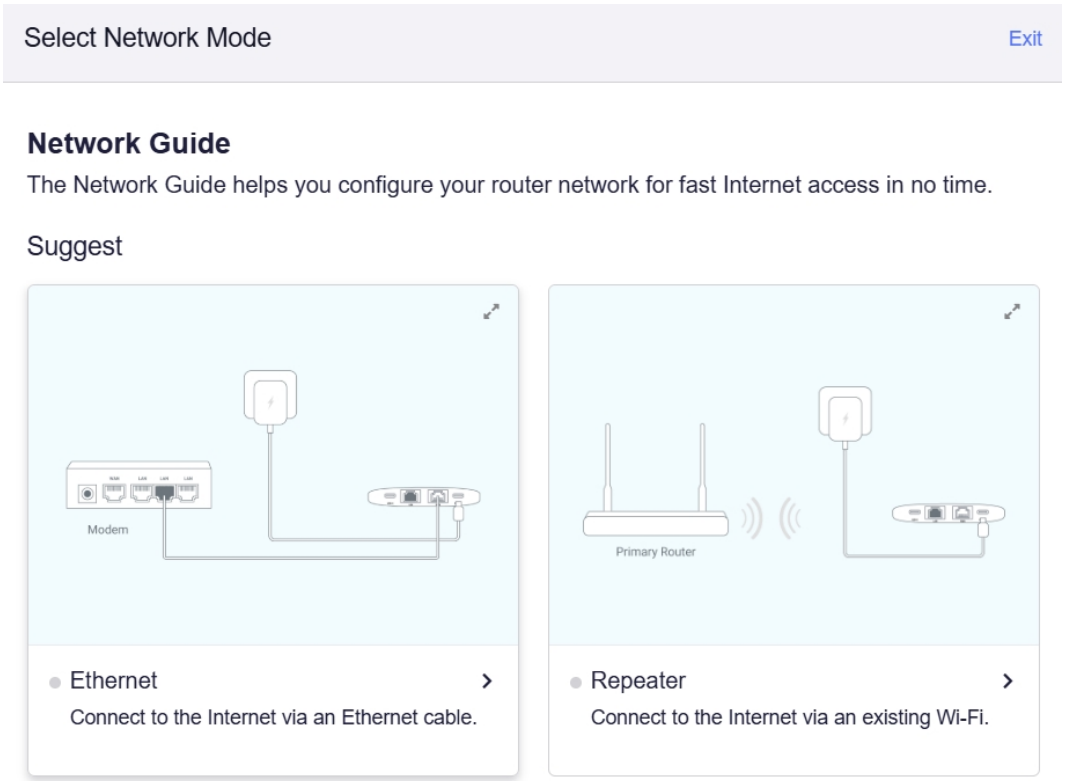
4.1 Assistant de configuration rapide

L’assistant de configuration Web vous guide dans la configuration réseau du routeur. Suivez les étapes ci-dessous pour lancer l’assistant.

1. Connectez-vous à l’interface d’administration Web du routeur en suivant les instructions du chapitre 3.
2. Sur la page d’accueil, cliquez sur l’icône en forme de livre dans l’angle supérieur droit.



3. Suivez l’assistant de configuration pour configurer le routeur et établir une connexion Internet.



Si vous utilisez l’application GL.iNet, suivez les instructions à l’écran pour configurer l’accès à Internet.

4.2 Configuration manuelle de la connexion Internet

L’assistant facilite la configuration rapide du réseau. La configuration manuelle permet d’adapter les paramètres réseau avancés à vos besoins et de vérifier ou de modifier les connexions existantes.

Mango 2 propose quatre modes de connexion à Internet : Ethernet, répéteur, partage de connexion USB et modem USB. Choisissez le mode adapté à vos besoins.

1. **Ethernet** : reliez le routeur au réseau haut débit en branchant un câble Ethernet sur le port WAN. Le routeur obtient généralement une adresse IP automatiquement via DHCP. Vous pouvez également définir une adresse IP statique ou configurer PPPoE manuellement. Cette méthode offre une connexion stable et rapide, adaptée au domicile et au bureau disposant d’un accès fixe à Internet.

2. **Répéteur (Repeater)** : ce mode permet au routeur de se connecter à un réseau Wi-Fi existant pour étendre sa couverture et créer un réseau local distinct et sécurisé. Il peut toutefois réduire le débit de transmission. Il convient aux zones mal couvertes nécessitant une extension du signal ou aux lieux publics où vous souhaitez renforcer la sécurité de votre connexion.

3. **Partage de connexion USB (USB Tethering)** : reliez un smartphone ou un autre appareil compatible au routeur à l’aide d’un câble USB pour partager sa connexion mobile, par exemple 4G ou 5G. Cette solution pratique convient à un accès Internet temporaire, notamment en déplacement ou dans les zones sans accès fixe à Internet.

4. **Modem USB** : branchez au routeur un modem USB cellulaire contenant une carte SIM. Le routeur se connecte alors à Internet via un réseau mobile 4G ou 5G, indépendamment d’un accès fixe. Cette méthode offre une grande mobilité et convient notamment à une utilisation en véhicule ou en extérieur.

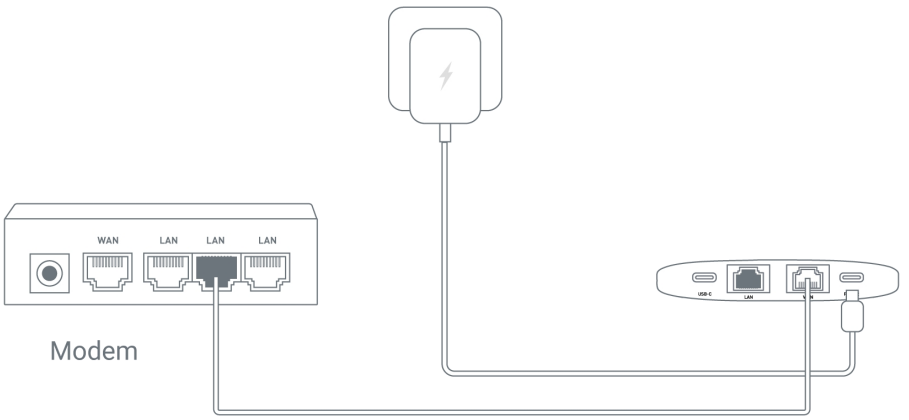
4.2.1 Connexion à Internet par câble Ethernet

Reliez le routeur au réseau haut débit en branchant un câble Ethernet sur le port WAN. Le routeur obtient généralement une adresse IP automatiquement via DHCP. Vous pouvez également définir une adresse IP statique ou configurer PPPoE manuellement. Cette méthode offre une connexion stable et rapide, adaptée au domicile et au bureau disposant d'un accès fixe à Internet.

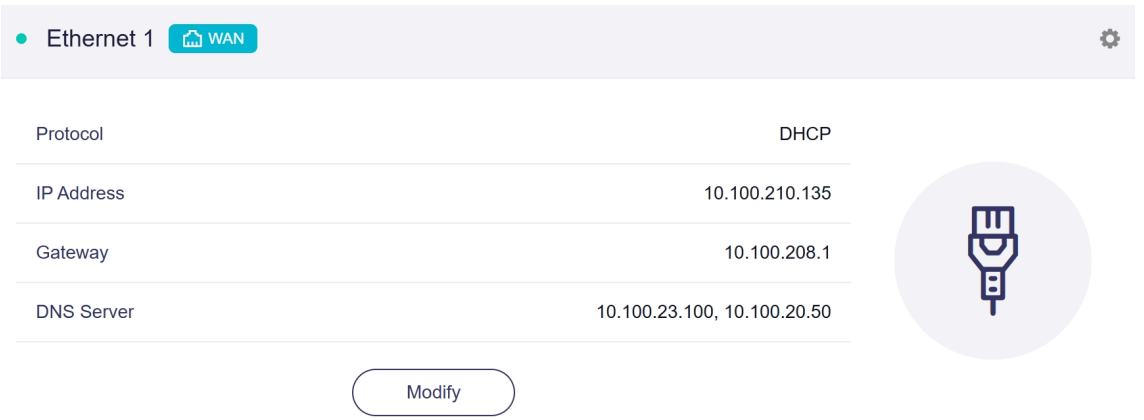
Configuration de base

Suivez les étapes ci-dessous pour connecter le routeur à Internet à l'aide d'un câble Ethernet.

1. Reliez le port **WAN** du routeur à l'appareil en amont (modem du FAI, routeur principal, commutateur réseau ou prise Ethernet) à l'aide d'un câble Ethernet.

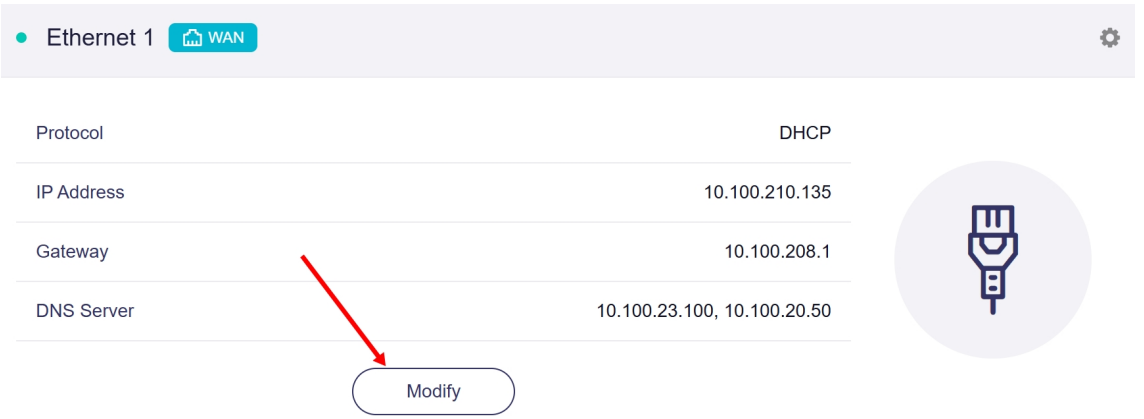


2. Connectez-vous à l'interface d'administration Web du routeur et ouvrez **INTERNET** > **Ethernet**. Si la connexion est établie, la section Ethernet affiche les informations du réseau, notamment le protocole, l'adresse IP, la passerelle et le serveur DNS.



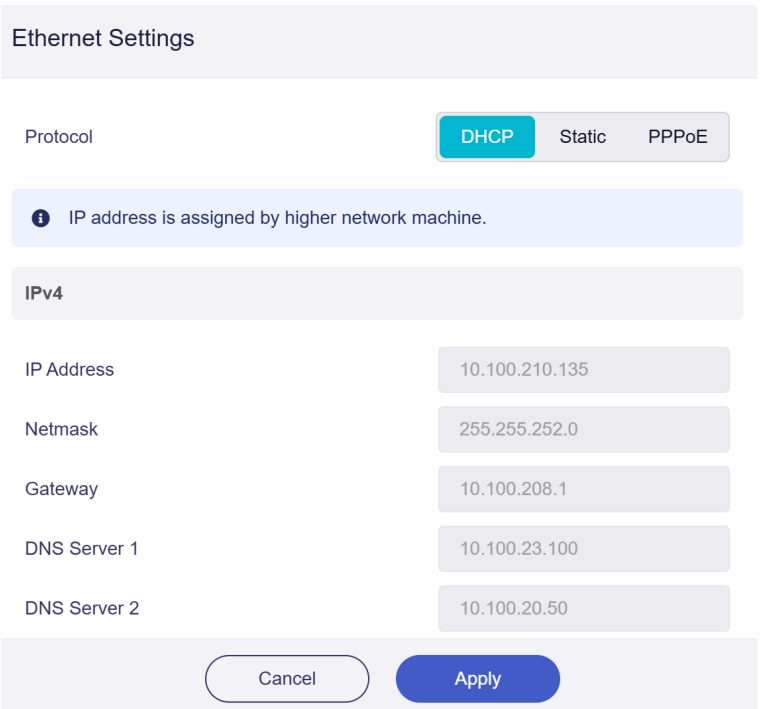
Protocoles

Trois protocoles sont disponibles : DHCP, statique et PPPoE. Cliquez sur **Modifier (Modify)** pour changer de protocole.



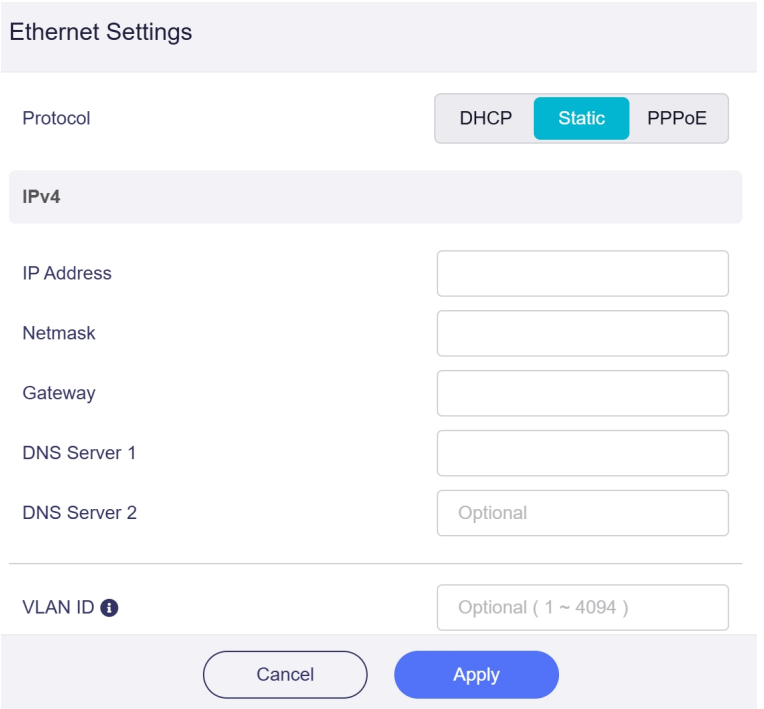
- **DHCP**

  DHCP est le protocole réseau par défaut et le plus courant. Selon un modèle client-serveur, il attribue automatiquement des adresses IP et d'autres paramètres de configuration aux appareils d'un réseau IP.



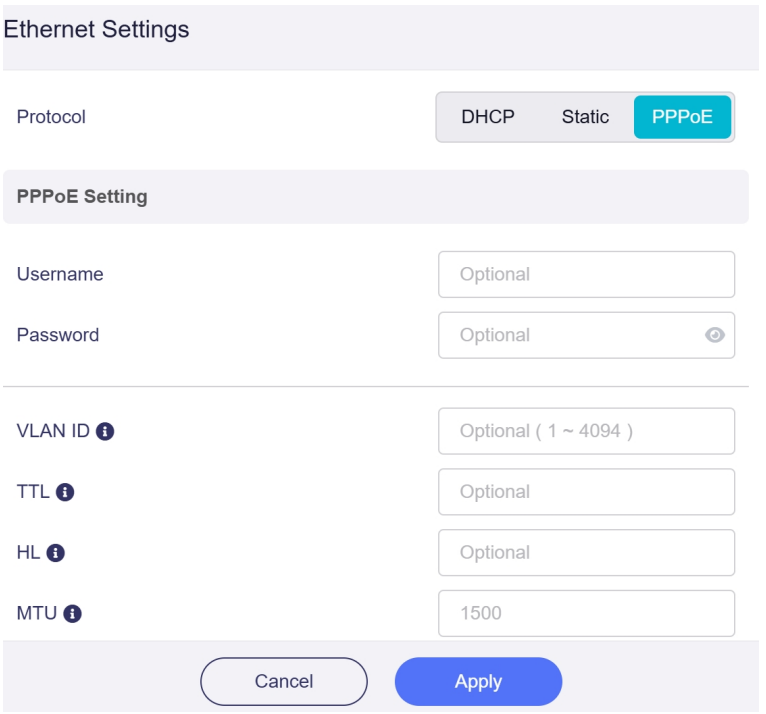
- **Statique (Static)**

  Une adresse IP statique est nécessaire si votre fournisseur d'accès à Internet (FAI) vous attribue une adresse IP publique fixe ou si vous devez définir manuellement les paramètres réseau, comme l'adresse IP, la passerelle et le masque de sous-réseau.



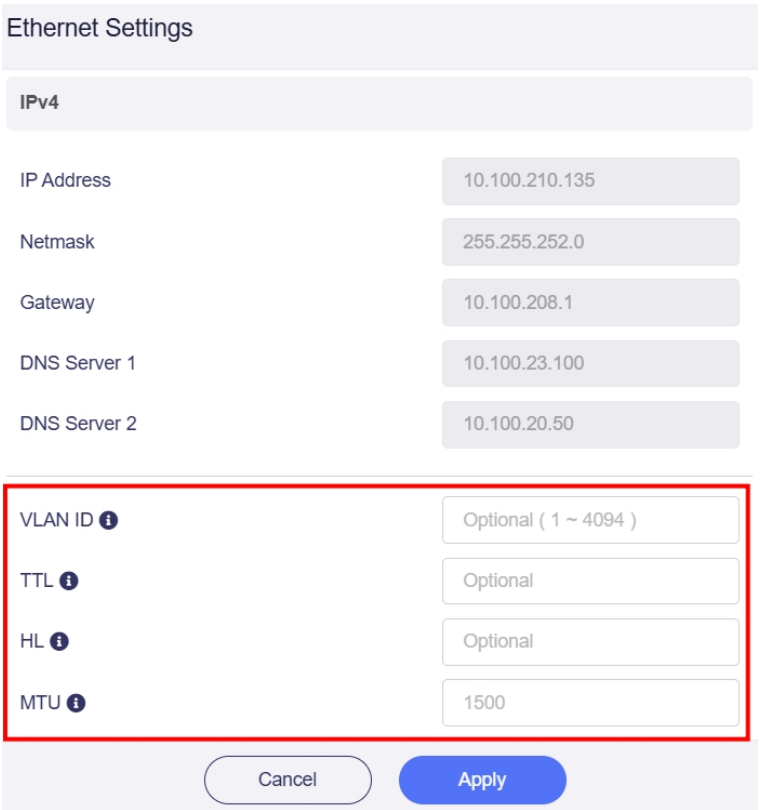
- **PPPoE**

  PPPoE (Point-to-Point Protocol over Ethernet) est un protocole réseau très utilisé par les FAI. Ceux-ci fournissent généralement un modem ainsi qu'un identifiant et un mot de passe propres à votre connexion, nécessaires pour configurer l'accès à Internet.


Ethernet Settings
Protocol
DHCP
Static
PPPoE
PPPoE Setting
Username
Optional
Password
Optional
VLAN ID
Optional (1 ~ 4094)
TTL
Optional
HL
Optional
MTU
1500
Cancel
Apply

Paramètres avancés

Outre les paramètres essentiels, ces trois protocoles proposent des paramètres avancés facultatifs.



- **VLAN ID**

  Ce paramètre n'est nécessaire que si le serveur du fournisseur exige un identifiant VLAN balisé précis pour cette interface.
- **TTL**

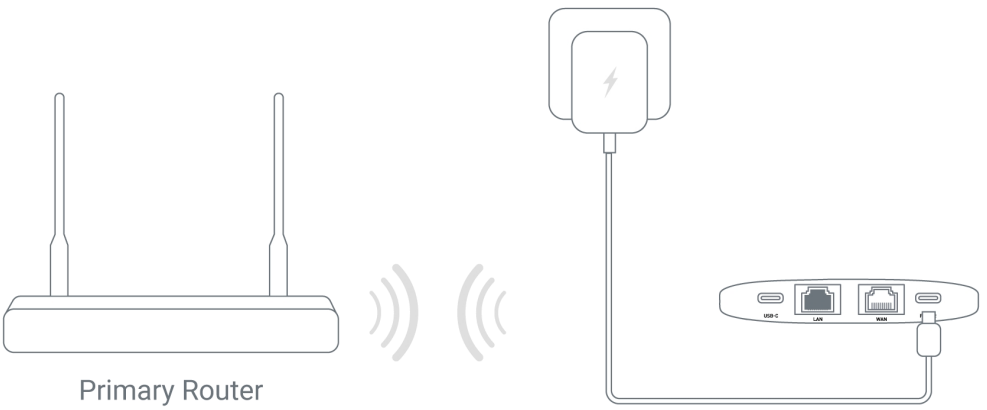
  Le TTL (Time To Live, durée de vie) définit la durée de vie maximale des paquets dans le réseau. Par défaut, le routeur diminue de 1 le TTL des paquets reçus des appareils clients avant de les transmettre. Pour modifier ce comportement, vous pouvez définir ici une valeur fixe. Le paramètre TTL ne s'applique qu'à IPv4.
- **HL**

  En IPv6, le champ HL (Hop Limit, limite de sauts) limite le nombre de sauts que peuvent effectuer les paquets dans le réseau. Il remplit le même rôle que le TTL en IPv4.
- **MTU**

  La valeur MTU par défaut est de 1 500 octets.

4.2.2 Connexion à Internet via un réseau Wi-Fi existant

Connectez le routeur en mode répéteur à un réseau Wi-Fi existant pour renforcer la couverture et créer un réseau local isolé du réseau principal. Dans un hôtel ou un café proposant un point d'accès public gratuit, le répéteur étend le signal Wi-Fi, permet à plusieurs appareils de se connecter par câble ou sans fil et protège votre réseau.

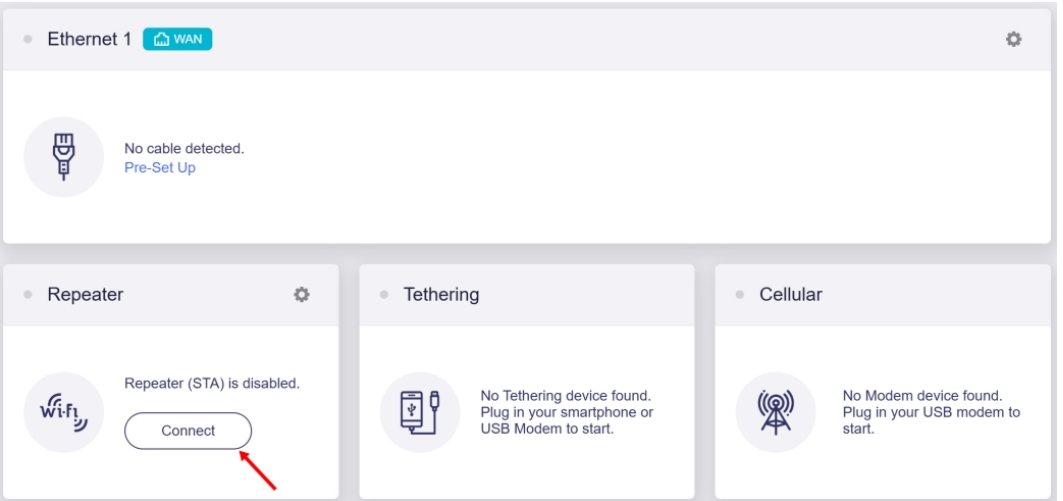


La fonction répéteur GL.iNet utilise par défaut le mode WISP (Wireless Internet Service Provider). Le routeur crée ainsi son propre sous-réseau et agit comme un pare-feu pour vous protéger du réseau public.

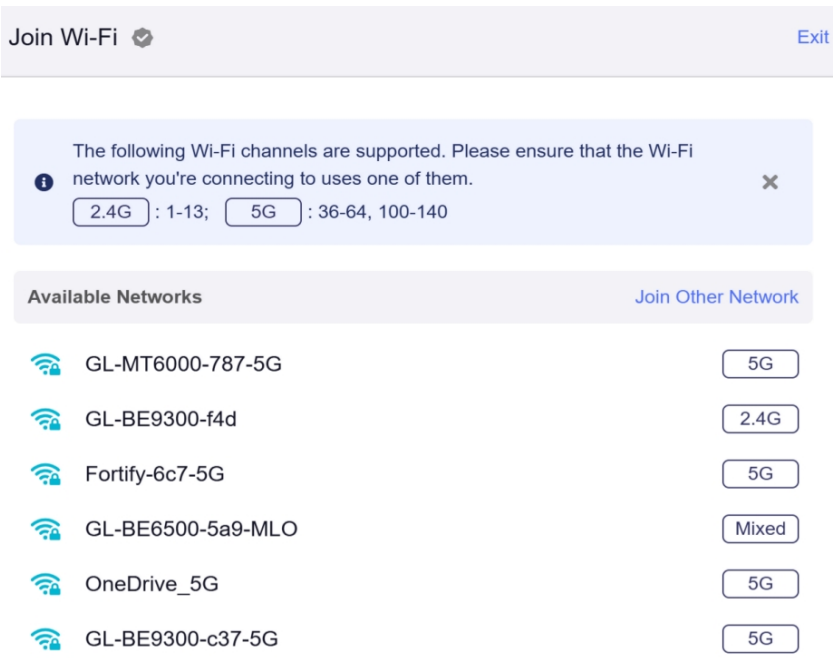
Configuration de base

Pour connecter le routeur à un réseau Wi-Fi existant en mode Répéteur, procédez comme suit.

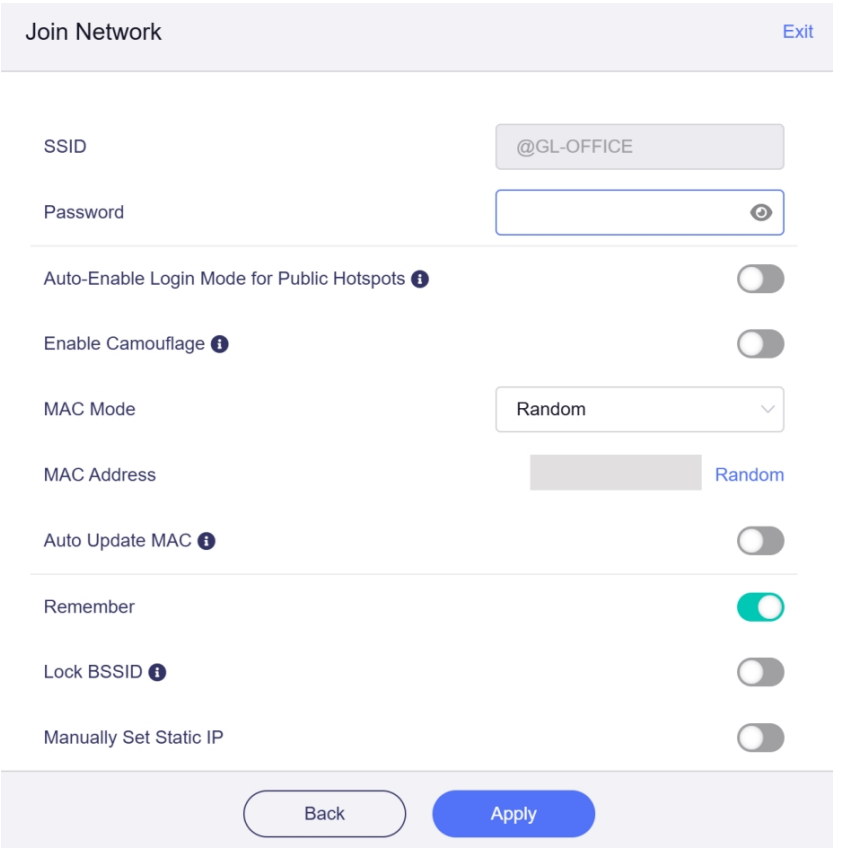
1. Connectez-vous à l'interface d'administration Web du routeur et ouvrez **INTERNET** > **Répéteur (Repeater)**. Cliquez sur **Connecter (Connect)**.



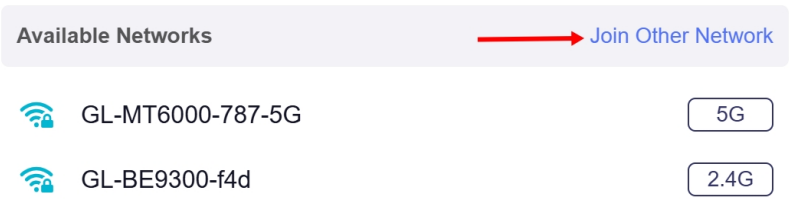
2. Dans la fenêtre qui s'affiche, choisissez le réseau Wi-Fi souhaité dans la liste des réseaux disponibles.



3. Saisissez le mot de passe Wi-Fi correct, puis cliquez sur **Appliquer (Apply)**.



Si le SSID du réseau souhaité n'apparaît pas dans la liste, cliquez sur **Rejoindre un autre réseau (Join Other Network)** dans l'angle supérieur droit. Saisissez le SSID et les autres informations demandées, puis cliquez sur **Appliquer (Apply)**.

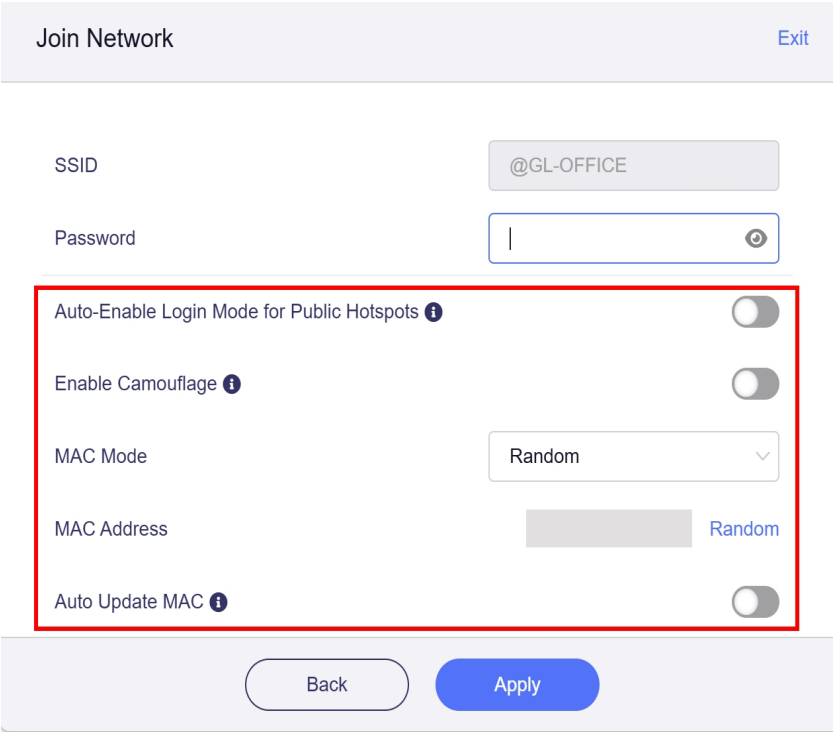


4. Patientez une minute pendant la connexion du routeur. Une fois la connexion établie, la page se présente comme ci-dessous.



Paramètres des points d’accès publics

Pour connecter le routeur à un point d’accès public doté d’un portail captif, il est recommandé d’activer les fonctions suivantes afin de faciliter la connexion.



- **Activation automatique du mode de connexion aux points d’accès publics**
  Si cette option est activée, le routeur passe automatiquement en mode de connexion aux points d’accès publics lorsqu’il est connecté à un point d’accès mais ne peut pas accéder à Internet. Certains services sont alors suspendus et le mode DNS passe en automatique, ce qui peut révéler votre activité réseau au fournisseur du réseau, par exemple l’hôtel ou le centre commercial. Même si cette option est désactivée, le routeur vous propose ce mode lorsqu’il détecte un portail captif ou ne parvient pas à s’y connecter.
- **Activer le camouflage**
  Si cette option est activée, le routeur prend l’identité de l’appareil client utilisé pour accéder à l’interface d’administration en reproduisant son adresse MAC.
- **Mode MAC**
  Choisissez l’adresse MAC utilisée par le routeur pour se connecter au point d’accès public.
  D’usine (Factory) : utilise l’adresse MAC attribuée à l’appareil en usine.
  Cloner (Clone) : utilise une copie de l’adresse MAC d’un appareil client pour la connexion.

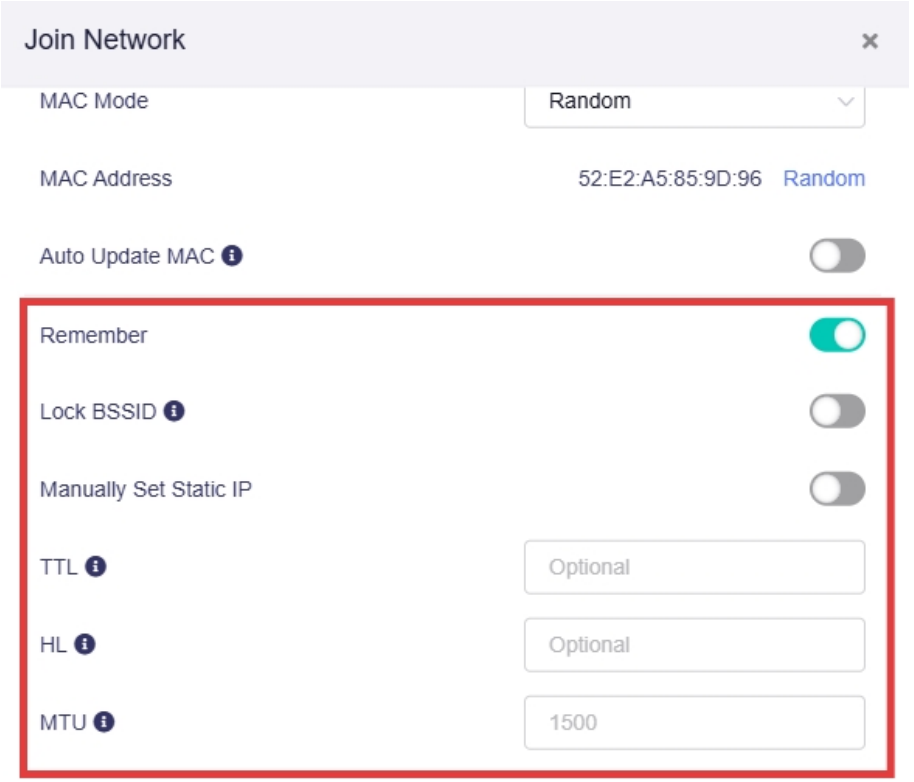
Si l’adresse souhaitée n’apparaît pas dans la liste, saisissez-la manuellement. Remarque : de nombreux appareils utilisent des adresses MAC aléatoires, souvent appelées « adresse Wi-Fi privée » ou « adresse matérielle aléatoire », lorsqu’ils se connectent au Wi-Fi. L’adresse affichée ici peut donc différer de l’adresse MAC physique de l’appareil.
Aléatoire (Random) : génère automatiquement une adresse MAC aléatoire pour la connexion.

- **Mise à jour automatique de l’adresse MAC**
  Si cette option est activée, l’adresse MAC est mise à jour automatiquement.

Lors de l’enregistrement de la configuration réseau, le mode MAC et toute adresse MAC clonée ou aléatoire sont associés au SSID enregistré. Vous pouvez modifier ces paramètres manuellement pour chaque SSID à tout moment.

Paramètres avancés

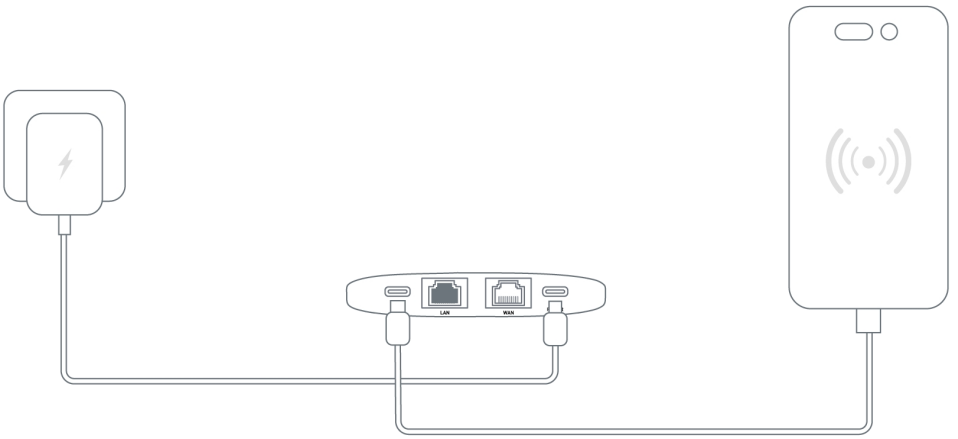
Des paramètres avancés facultatifs sont disponibles lors de la connexion au réseau.



- **Mémoriser (Remember)** : activez cette option pour mémoriser le réseau Wi-Fi auquel le routeur se connecte en mode répéteur. Elle est disponible à partir du micrologiciel v4.7.
- **Verrouiller le BSSID (Lock BSSID)** : si cette option est activée, lorsque le routeur sélectionne un réseau utilisant ce SSID, il ne se connecte qu'au point d'accès correspondant au BSSID choisi.
- **Définir manuellement une IP statique** : cette option est disponible à partir du micrologiciel v4.7.
- **TTL** : le TTL (Time To Live, durée de vie) définit la durée de vie maximale des paquets dans le réseau. Renseignez-le selon les exigences de l'opérateur. Par défaut, le routeur diminue de 1 le TTL des paquets reçus des appareils clients avant de les transmettre. Pour camoufler ce comportement, vous pouvez définir ici une valeur fixe. Le TTL ne s'applique qu'à IPv4.
- **HL** : en IPv6, le champ HL (Hop Limit, limite de sauts) limite le nombre de sauts des paquets dans le réseau. Il remplit le même rôle que le TTL en IPv4.
- **MTU** : la valeur par défaut est de 1 500.

4.2.3 Connexion à Internet par partage de connexion USB

Le partage de connexion USB, ou Tethering, consiste à relier un smartphone au routeur avec un câble USB pour partager sa connexion mobile, par exemple 4G ou 5G. Cette méthode convient à un accès Internet temporaire, notamment en déplacement ou dans les zones sans accès fixe à Internet.

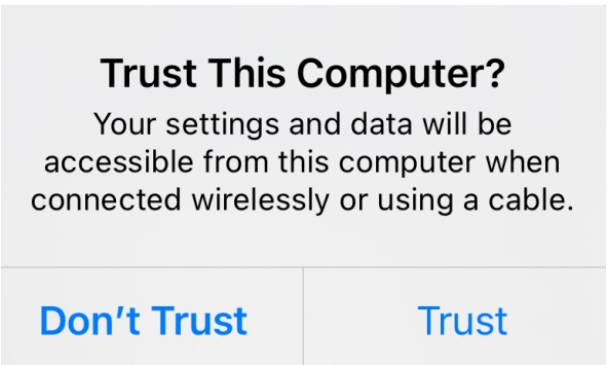


Les modems autonomes, dits « host-less », utilisent également le mode de partage de connexion USB lors de leur configuration.

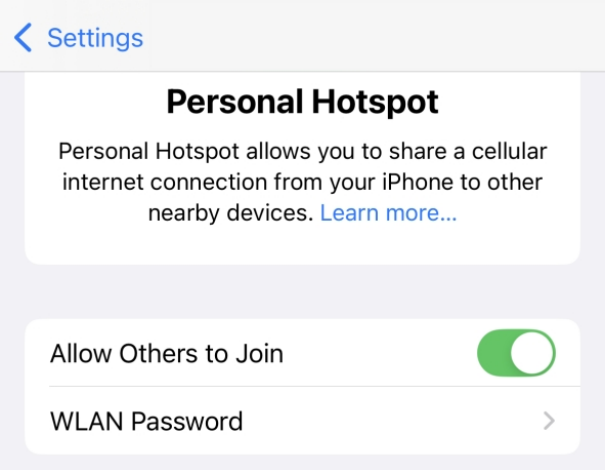
Remarque : certains opérateurs mobiles limitent le partage de connexion ou le facturent en supplément. Renseignez-vous auprès de votre opérateur.

Partage de connexion avec un iPhone

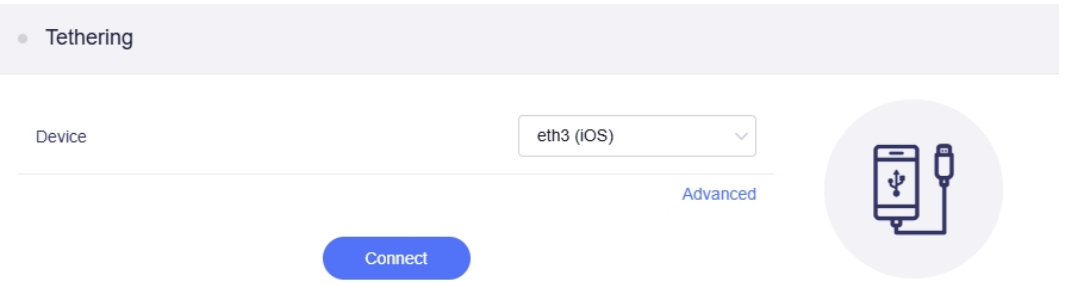
1. Reliez l'iPhone au port USB du routeur à l'aide d'un câble USB. Une boîte de dialogue vous demande si vous souhaitez faire confiance à cet appareil. Touchez **Se fier (Trust)** pour continuer.



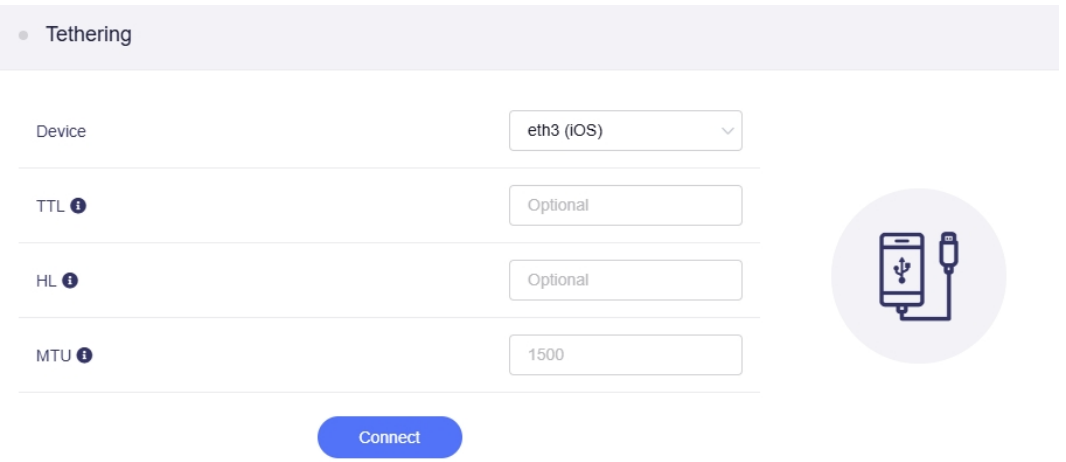
2. Sur l'iPhone, ouvrez **Réglages (Settings)** > **Partage de connexion (Personal Hotspot)**. Activez **Autoriser d'autres utilisateurs (Allow Others to Join)**.



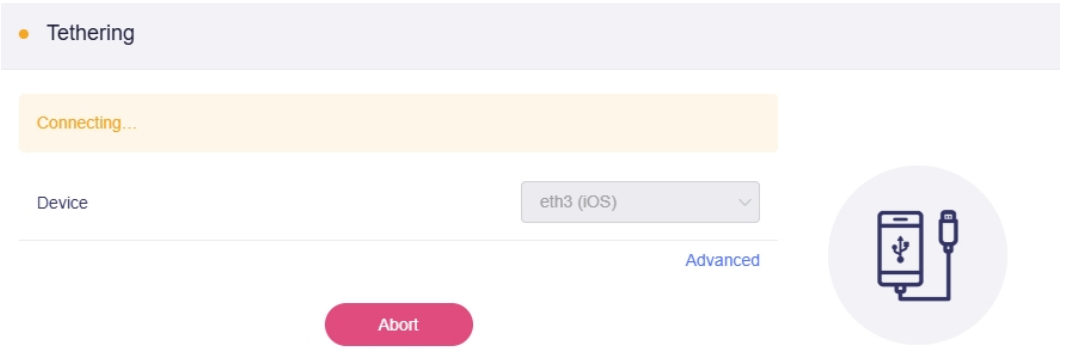
3. Connectez un ordinateur ou un autre téléphone au routeur. Connectez-vous à l'interface d'administration Web du routeur, ouvrez **INTERNET** > **Partage de connexion (Tethering)**, puis cliquez sur **Connecter (Connect)**.



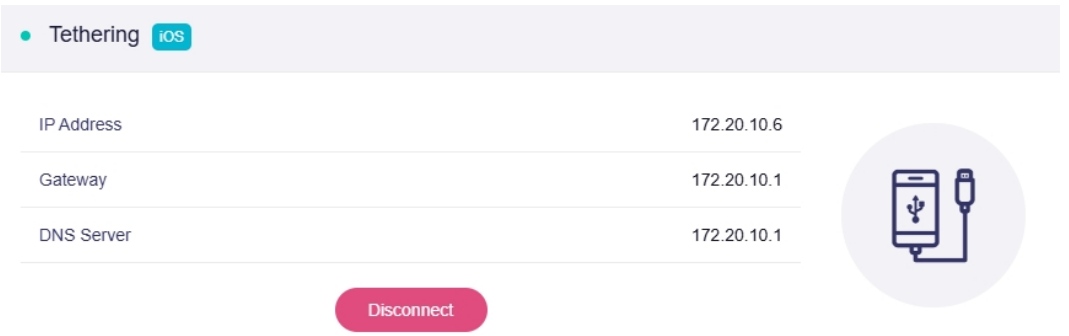
Pour régler les paramètres avancés, comme TTL, HL et MTU, cliquez sur **Avancé (Advanced)** et ajustez-les avant de cliquer sur **Connecter (Connect)**.



4. La connexion démarre.

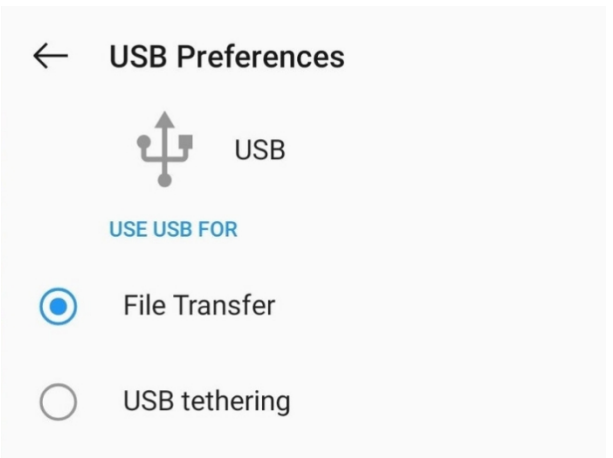


Une fois la connexion établie, cette page en affiche les détails.



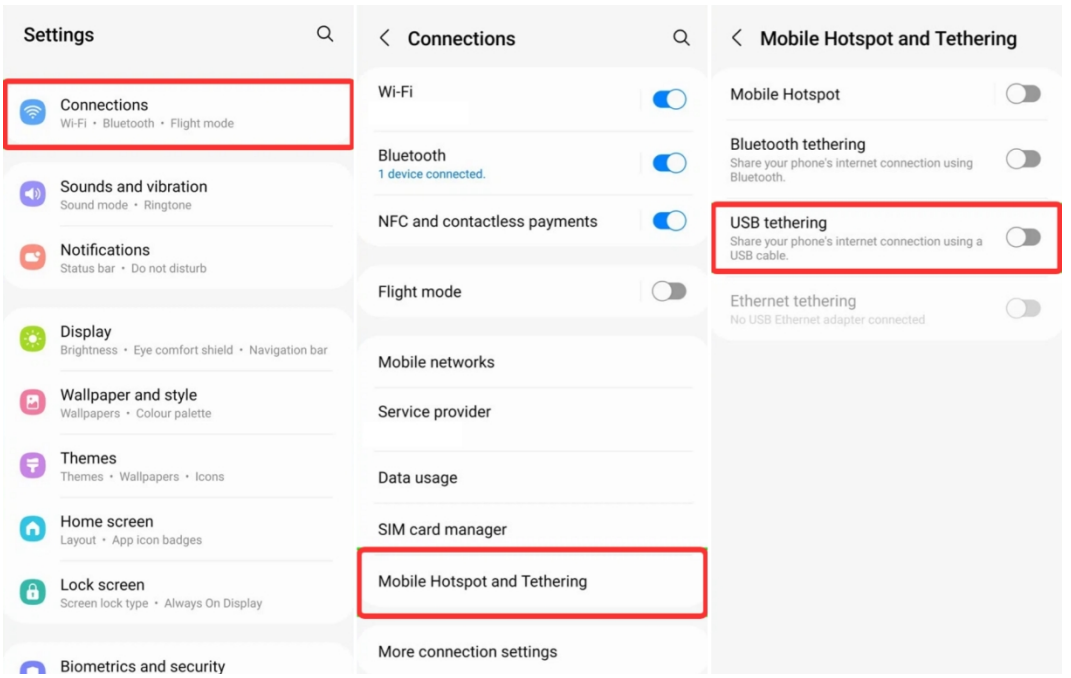
Partage de connexion avec un téléphone Android

1. Reliez le téléphone Android au port USB du routeur avec un câble USB. Une boîte de dialogue peut afficher les préférences USB (USB preferences). Si vous y êtes invité, sélectionnez **Partage de connexion USB (USB Tethering)** ou **Transfert de fichiers (File Transfer)**.



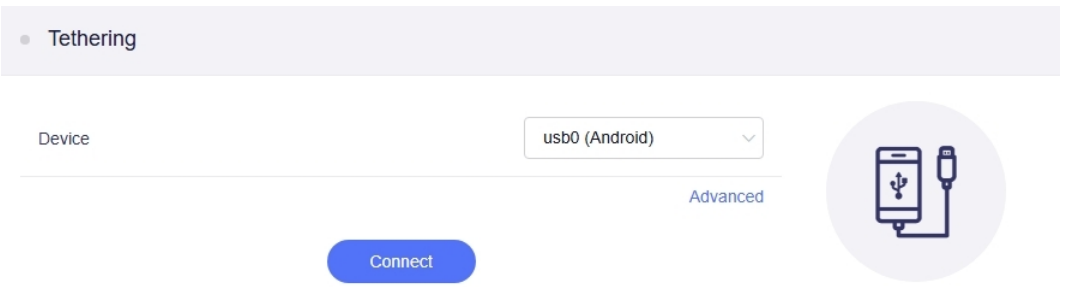
2. Sur votre téléphone, ouvrez **Paramètres (Settings)** > **Réseau et Internet (Network & Internet)** > **Point d'accès personnel (Personal Hotspot)**.

Activez **Point d’accès personnel (Personal Hotspot)** ou **Partage de connexion USB (USB Tethering)**.

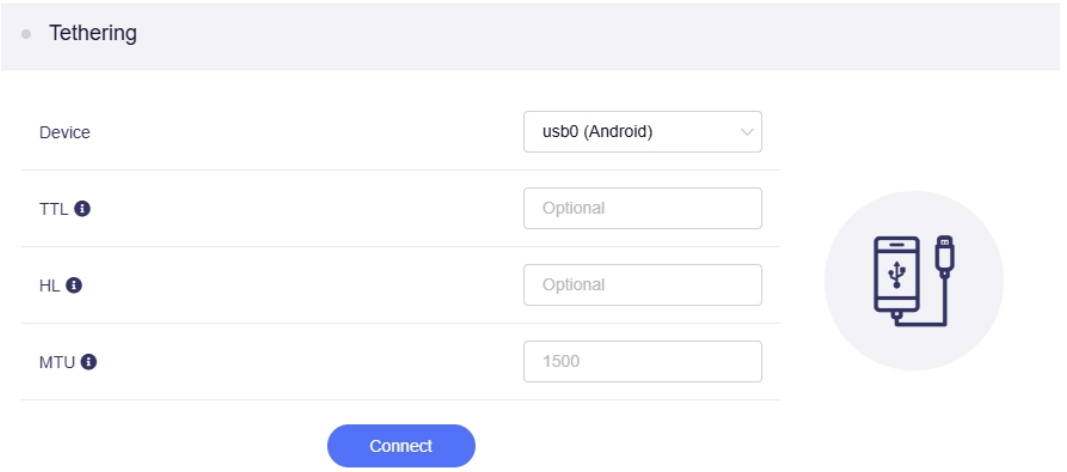


(La procédure d’activation du partage de connexion USB varie selon la marque. Consultez les paramètres de votre appareil pour trouver cette option et contactez l’assistance du fabricant si nécessaire.)

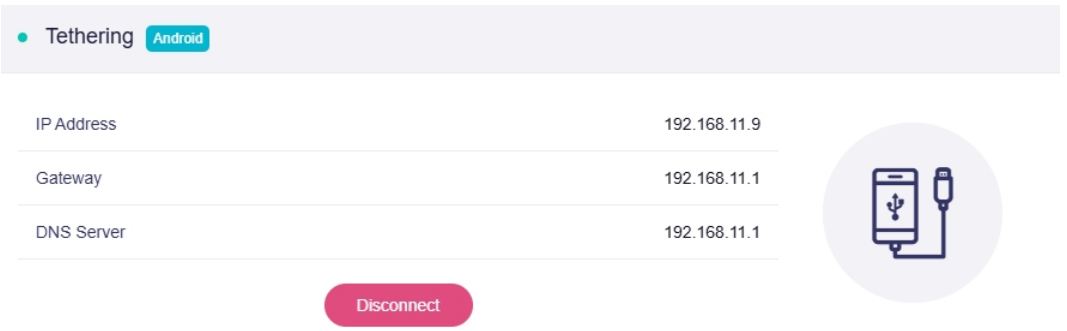
3. Connectez un ordinateur ou un autre téléphone au routeur, puis connectez-vous à l’interface d’administration Web et ouvrez **INTERNET** > **Partage de connexion (Tethering)**. Cliquez sur **Connecter (Connect)**.



Pour régler les paramètres avancés, comme TTL, HL et MTU, cliquez sur **Avancé (Advanced)** et ajustez-les avant de cliquer sur **Connecter (Connect)**.



4. La connexion démarre. Une fois établie, son état apparaît sur cette page.



Dépannage

Si le partage de connexion échoue, essayez les solutions suivantes :

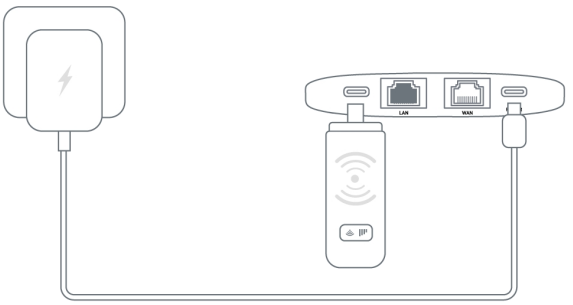
- Utilisez le bloc d'alimentation d'origine du routeur.
- Débranchez puis rebranchez le câble USB.
- Essayez un autre câble USB. Vérifiez qu'il permet le transfert de données, et pas seulement la recharge.
- Désactivez puis réactivez plusieurs fois le « partage de connexion USB » sur le téléphone Android.
- Désactivez puis réactivez plusieurs fois « Autoriser d'autres utilisateurs » sur l'iPhone.
- Redémarrez votre smartphone et réessayez.

Si le problème persiste, contactez notre assistance technique à l'adresse support@gl-inet.com.

4.2.4 Connexion à Internet via un modem USB

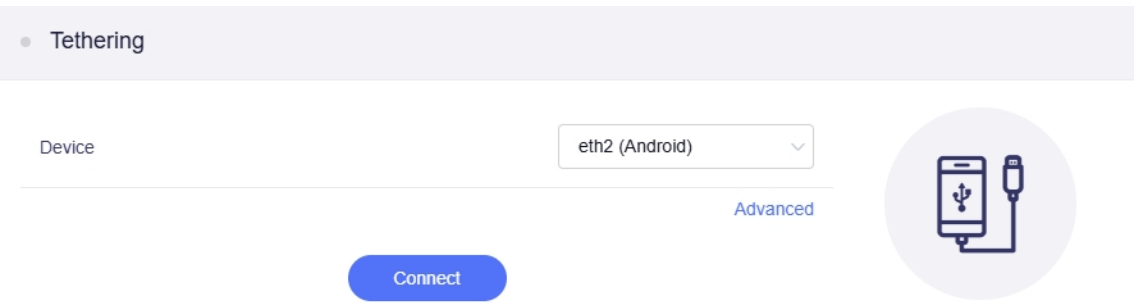
Branchez un modem USB cellulaire au port USB du routeur pour le connecter à Internet. Le routeur utilise alors les réseaux 4G ou 5G sans dépendre d'un accès fixe à Internet. Cette méthode convient à une utilisation en véhicule ou en extérieur. La connexion est gérée par l'interface Partage de connexion (Tethering) ou Cellulaire (Cellular) du routeur.

Sur Mango 2, vous pouvez brancher directement un modem USB-C, ou utiliser un adaptateur USB-C vers USB-A pour brancher un modem USB-A.

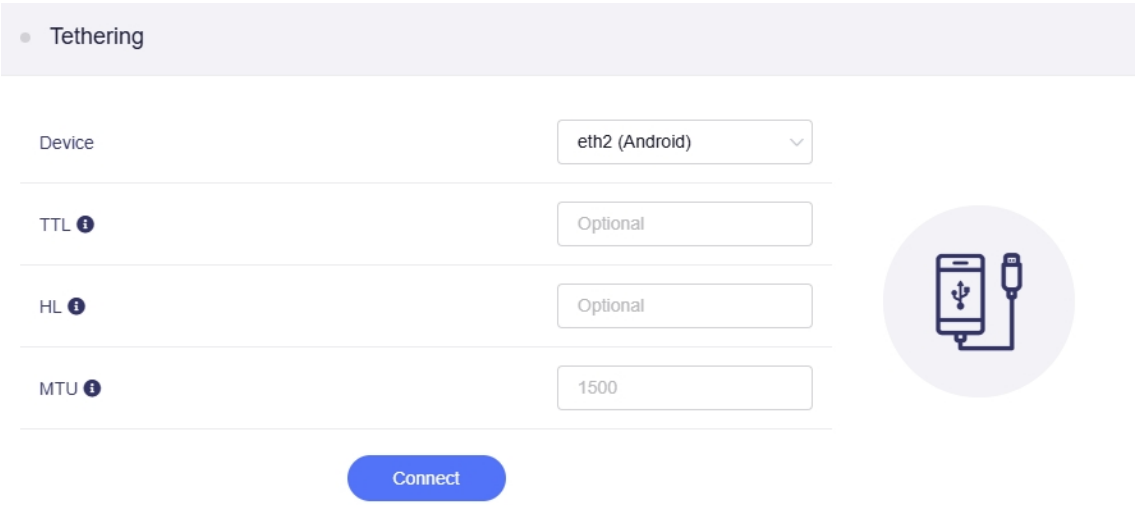


Suivez les étapes ci-dessous pour connecter le routeur à Internet via un modem USB.

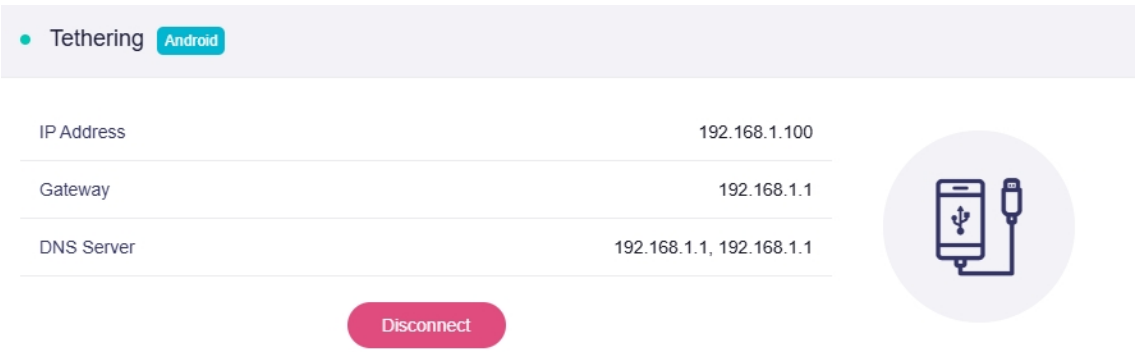
1. Avant d'allumer le routeur, branchez à son port USB un modem USB contenant une carte SIM.
2. Connectez-vous à l'interface d'administration Web du routeur, ouvrez **INTERNET** > **Partage de connexion (Tethering)**, puis cliquez sur **Connecter (Connect)**.



Pour régler les paramètres avancés, comme TTL, HL et MTU, cliquez sur **Avancé (Advanced)**. Ajustez les paramètres, puis cliquez sur **Connecter (Connect)**.

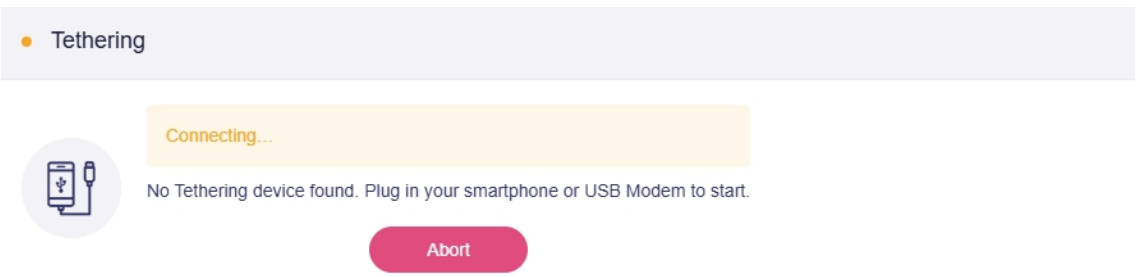


3. La connexion démarre. Une fois établie, cette page affiche les informations réseau.



Conseils :

1. Après la configuration initiale, si vous redémarrez le routeur en laissant le modem USB branché ou si vous rebranchez le modem, celui-ci est reconnu automatiquement. La connexion réseau s'établit sans avoir à cliquer de nouveau sur « Connecter ».
2. Si vous débranchez le modem USB, la page affiche « Aucun appareil de partage de connexion détecté » (No Tethering device found), comme ci-dessous. L'interface de partage de connexion reste à l'état « Connexion en cours » (Connecting).



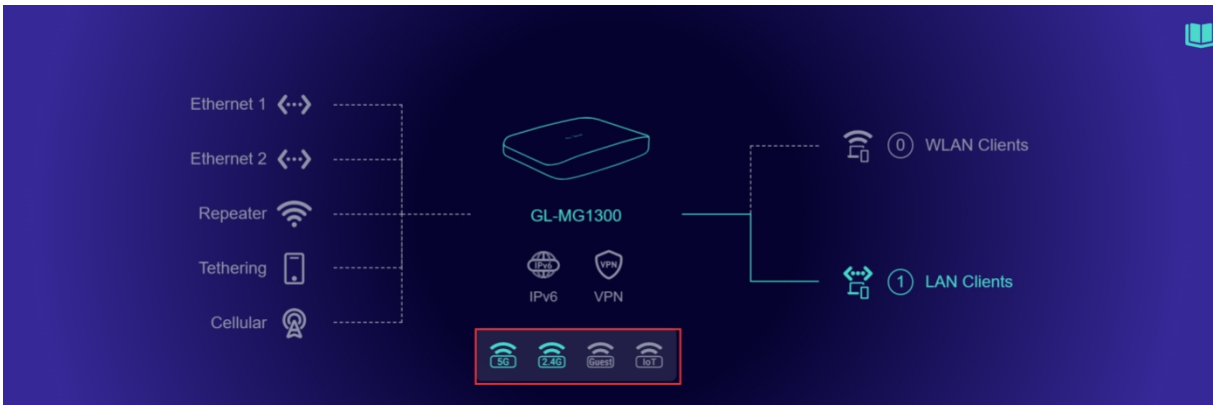
Chapitre 5

Réseau sans fil

Ce chapitre explique comment vérifier l’état du Wi-Fi et configurer les paramètres sans fil.

5.1 Affichage de l’état du Wi-Fi

Les réseaux Wi-Fi du routeur sont activés par défaut. L’icône Wi-Fi correspondante s’allume sous l’image du modèle sur la page INTERNET.



Lorsque vous placez le pointeur sur l’icône d’un réseau Wi-Fi activé, un code QR s’affiche comme ci-dessous. Scannez-le pour vous connecter rapidement au réseau correspondant.



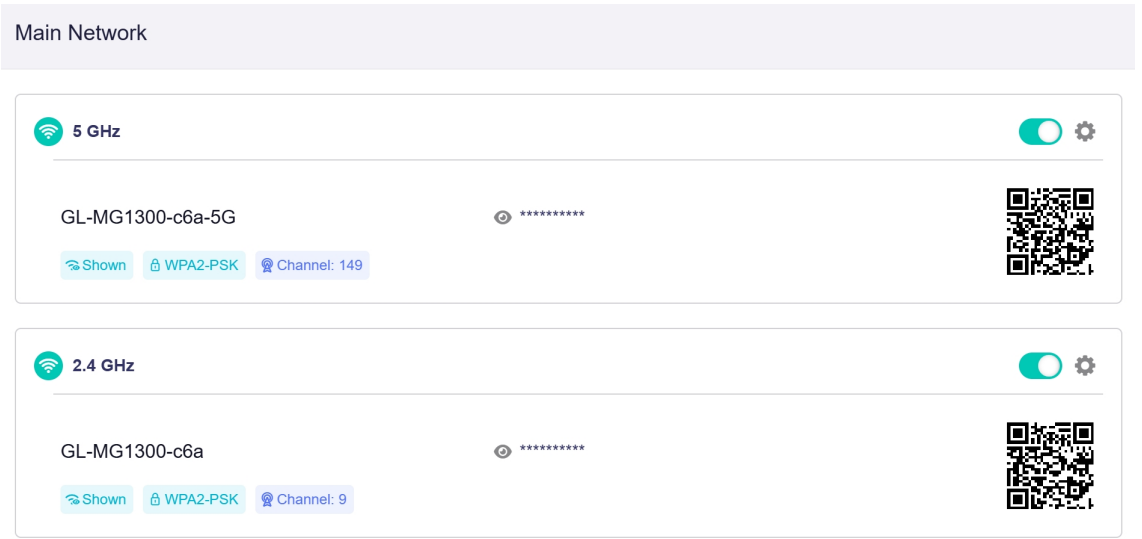
5.2 Paramètres sans fil

Connectez-vous à l'interface d'administration Web du routeur et ouvrez **SANS FIL (WIRELESS)**.
La page Sans fil permet de configurer les réseaux Wi-Fi principal, invité et IoT. Les bandes Wi-Fi prises en charge varient selon le modèle.

5.2.1 Réseau principal

Le réseau principal est votre réseau Wi-Fi habituel. Il peut émettre simultanément sur plusieurs bandes radio, toutes activées par défaut.

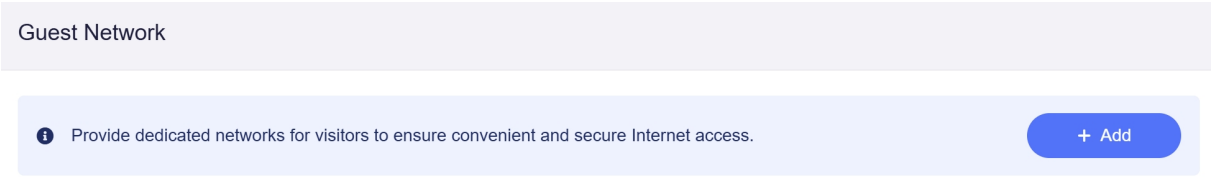
Cliquez sur l'engrenage à droite pour consulter ou modifier les paramètres Wi-Fi de chaque bande : SSID, sécurité, mot de passe, BSSID aléatoire, puissance d'émission, largeur de bande et canal Wi-Fi.
Remarque : les bandes Wi-Fi disponibles varient selon le modèle.



5.2.2 Réseau invité

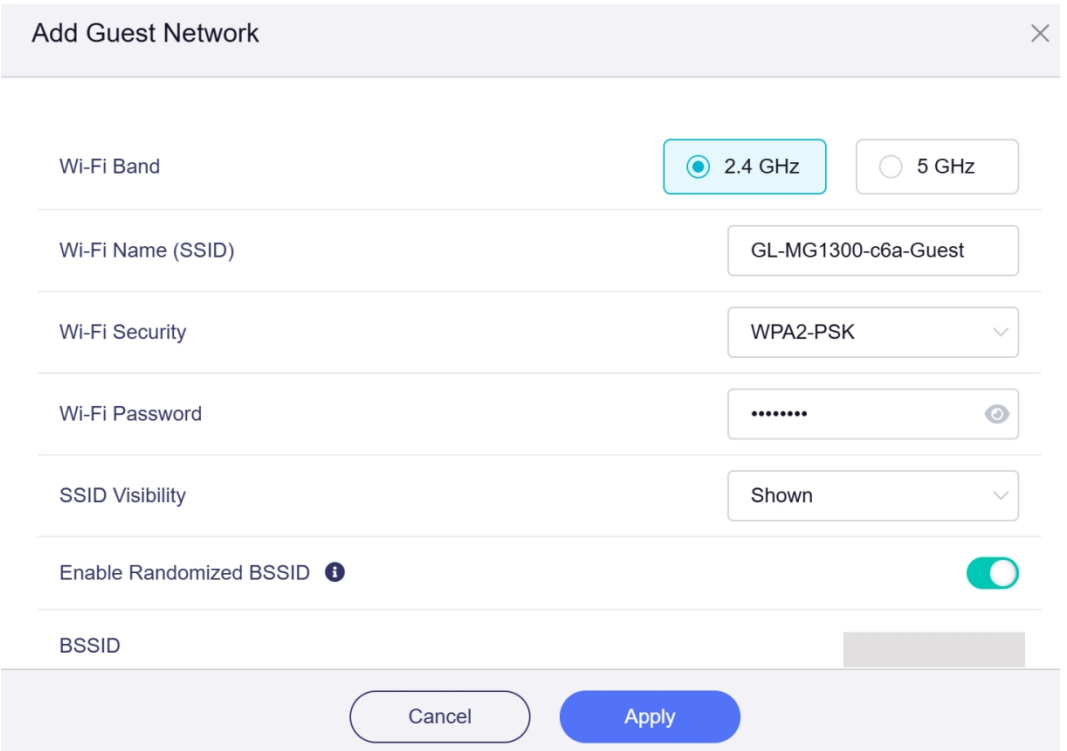
Le réseau invité est un réseau Wi-Fi dédié aux visiteurs. Toutes ses bandes sont désactivées par défaut. Vous pouvez activer et configurer les paramètres de base de chaque bande : SSID, mode de sécurité, mot de passe et activation du BSSID aléatoire.

Pour créer un réseau Wi-Fi invité, cliquez sur **Ajouter (Add)** à droite.

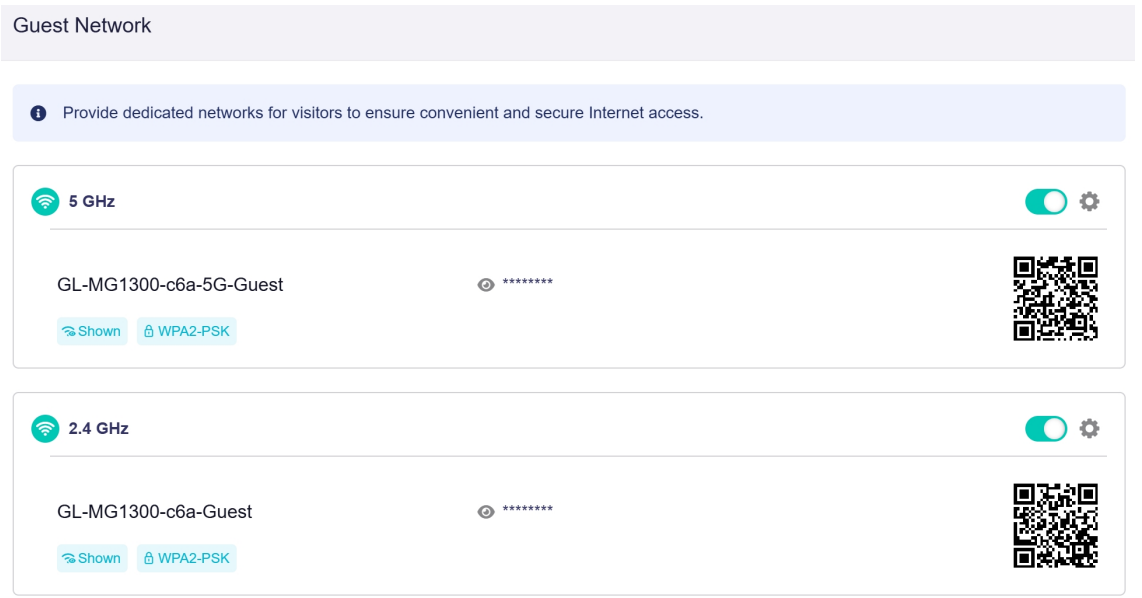


Sélectionnez une bande Wi-Fi, configurez les paramètres, puis cliquez sur **Appliquer (Apply)**.

Remarque : les bandes Wi-Fi disponibles varient selon le modèle.



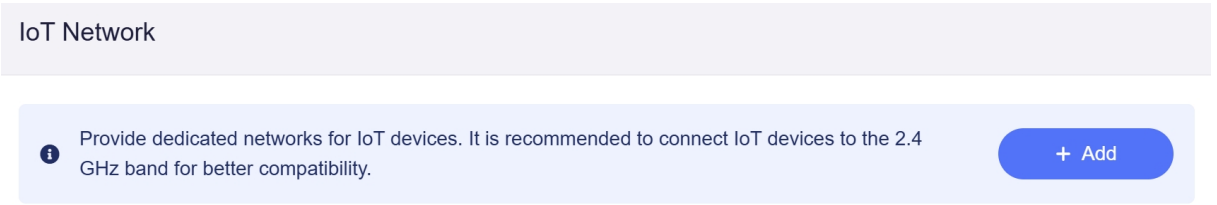
Une fois le réseau activé, la page se présente comme ci-dessous.


Guest Network
Provide dedicated networks for visitors to ensure convenient and secure Internet access.
5 GHz
GL-MG1300-c6a-5G-Guest
****
Shown
WPA2-PSK
2.4 GHz
GL-MG1300-c6a-Guest
****
Shown
WPA2-PSK

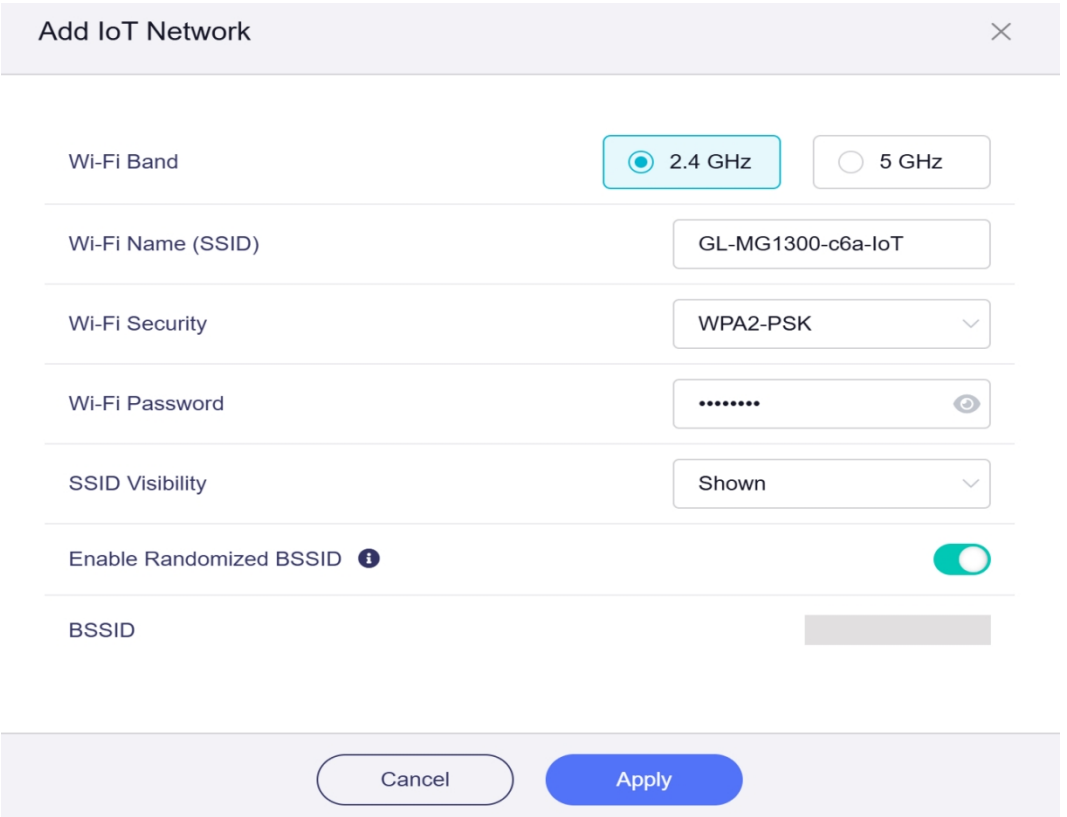
5.2.3 Réseau IoT

Le réseau IoT est un réseau Wi-Fi dédié aux appareils intelligents. Toutes ses bandes sont désactivées par défaut. Vous pouvez activer et configurer les paramètres de base de chaque bande : SSID, mode de sécurité, mot de passe et activation du BSSID aléatoire.

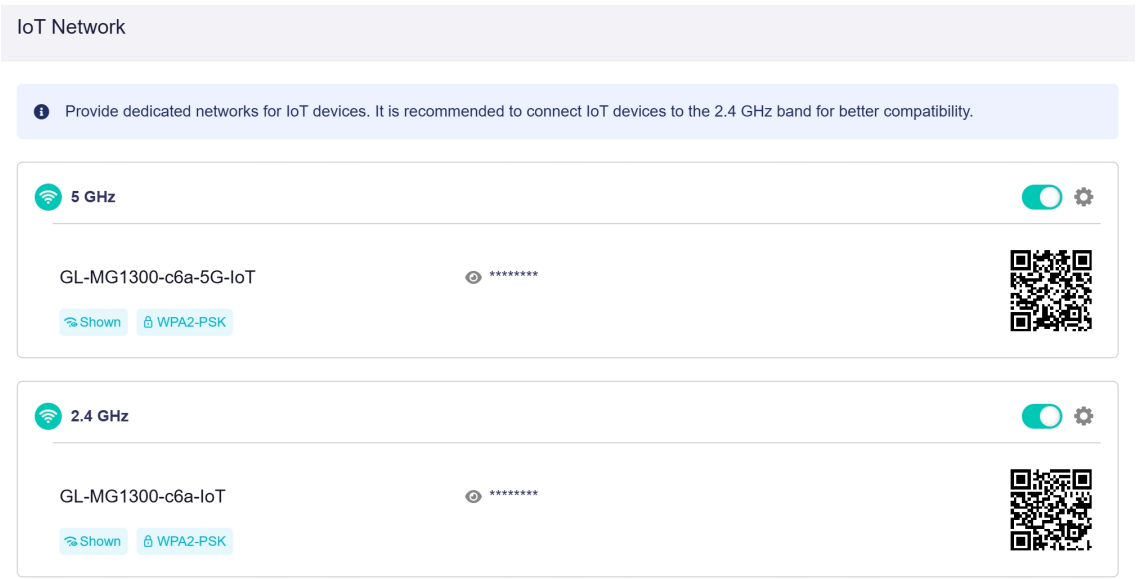
Pour créer un réseau Wi-Fi IoT, cliquez sur **Ajouter (Add)** à droite.



Sélectionnez une bande Wi-Fi, configurez les paramètres, puis cliquez sur **Appliquer (Apply)**.



Une fois le réseau activé, la page se présente comme ci-dessous.


IoT Network
Provide dedicated networks for IoT devices. It is recommended to connect IoT devices to the 2.4 GHz band for better compatibility.
5 GHz
GL-MG1300-c6a-5G-IoT
****
Shown
WPA2-PSK
2.4 GHz
GL-MG1300-c6a-IoT
****
Shown
WPA2-PSK

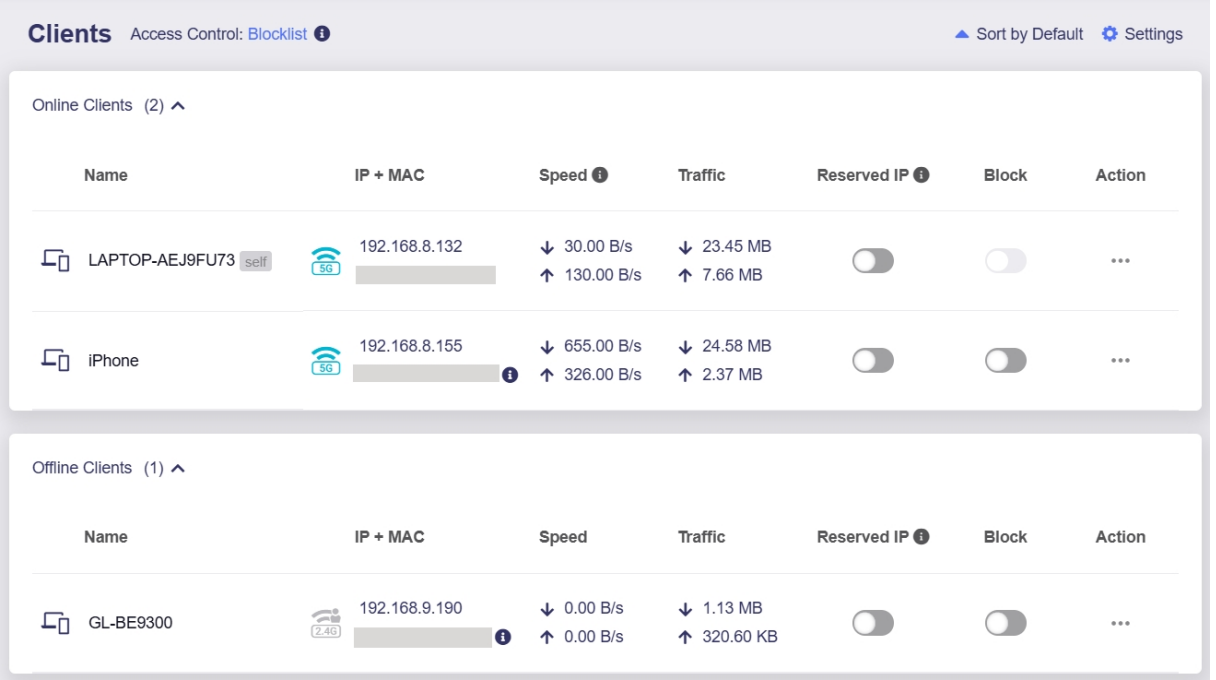
Chapitre 6

Appareils clients

Ce chapitre explique comment consulter les informations des appareils connectés et gérer leurs connexions.

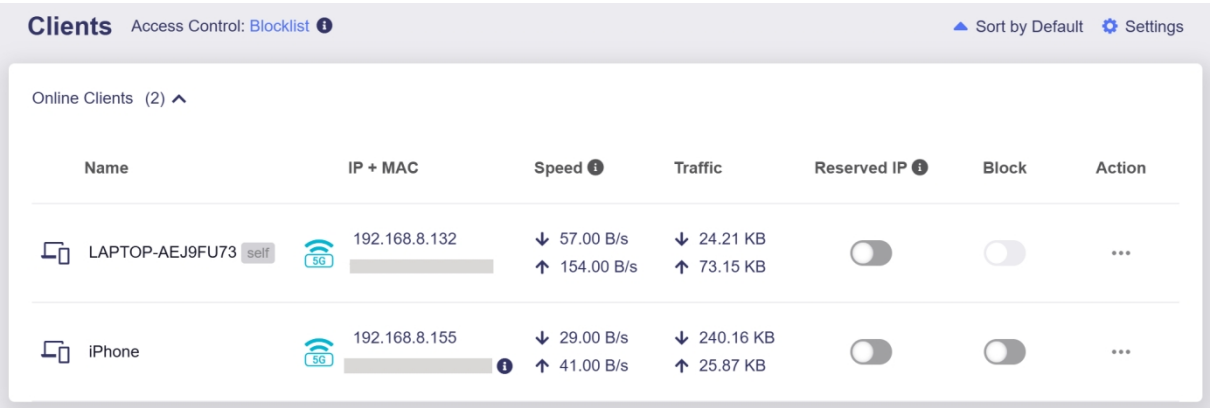
Connectez-vous à l'interface d'administration Web du routeur et ouvrez **CLIENTS**.

La page Clients affiche, de gauche à droite, le nom des appareils connectés, leur type de connexion, leurs adresses IP et MAC, leur débit et leur trafic. Elle permet également de réserver une adresse IP, de bloquer un client ou d'effectuer d'autres actions rapidement.



- **Clients en ligne (Online Clients)** : appareils actuellement connectés au réseau du routeur.
- **Clients hors ligne (Offline Clients)** : appareils déjà connectés au routeur auparavant, mais actuellement déconnectés.

6.1 Informations sur les appareils



1. **Nom de l'appareil**

   La première colonne affiche le nom et le type de l'appareil, selon le nom d'hôte fourni par celui-ci. L'icône bleue à côté du nom indique le mode de connexion : l'appareil est relié au routeur par un câble Ethernet.

2. **Adresses IP et MAC**

   La deuxième colonne affiche les adresses IP et MAC de l'appareil connecté. Si l'appareil utilise une adresse MAC aléatoire, un message le signale.



   Une adresse MAC dont le deuxième caractère est 2, 6, A ou E, sans distinction de casse, est considérée comme aléatoire. Certains appareils utilisent toutefois une autre règle de génération : cette méthode de détection peut donc manquer de précision.

3. **Débit**

   La troisième colonne affiche le débit Internet de l'appareil connecté. Il s'agit du débit moyen des trois dernières minutes. Le calcul commence à l'ouverture de cette page : si elle n'est ouverte que depuis 10 secondes, la moyenne porte uniquement sur ces 10 secondes.

4. **Trafic** : la quatrième colonne affiche le trafic Internet de l'appareil connecté.

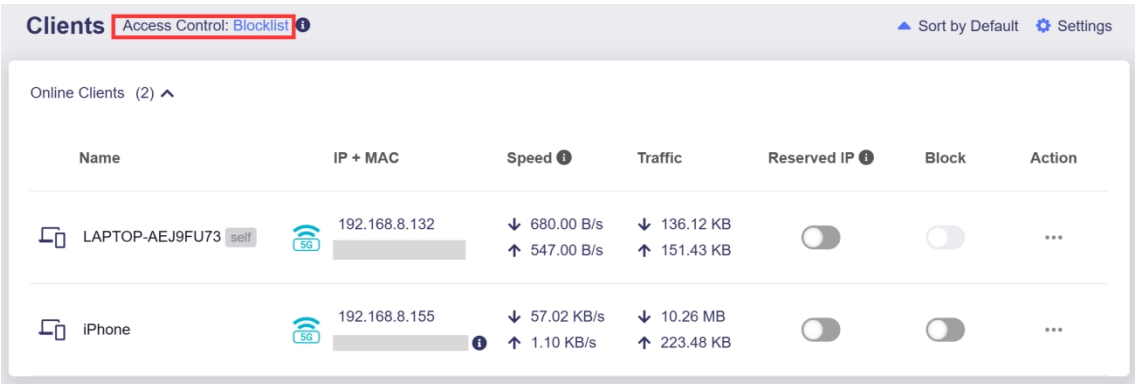
5. **Réserver une adresse IP**

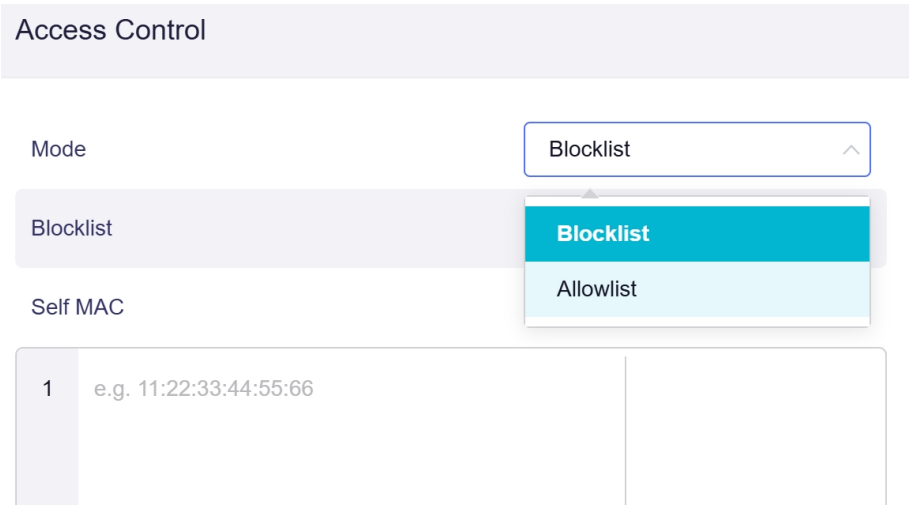
   La cinquième colonne permet de réserver en un clic une adresse IP pour l'appareil connecté. Lorsqu'une adresse est réservée pour un client du réseau local, celui-ci reçoit toujours la même adresse IP à chaque connexion au routeur.

6. **Liste de blocage**

La sixième colonne permet de bloquer certains appareils connectés en un clic.

Par défaut, la règle de contrôle d'accès utilise une liste de blocage. Vous pouvez choisir une liste d'autorisation en haut de la page.



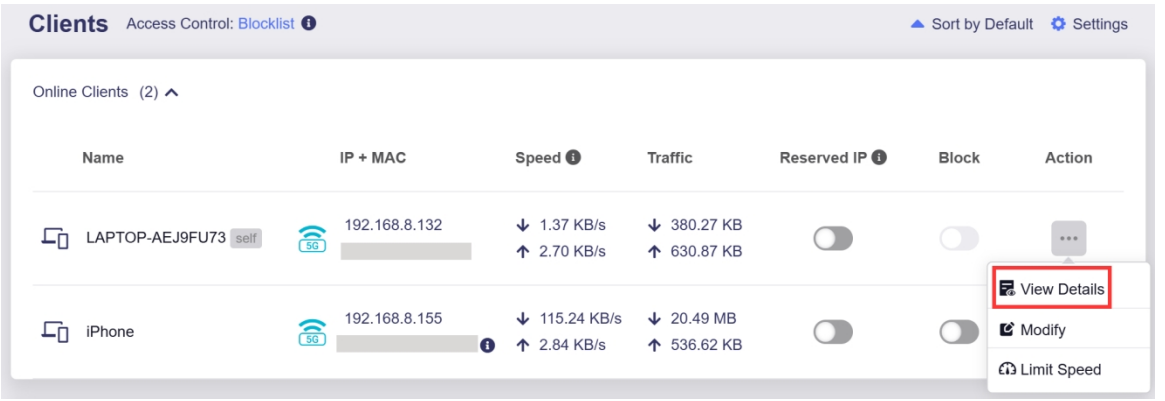


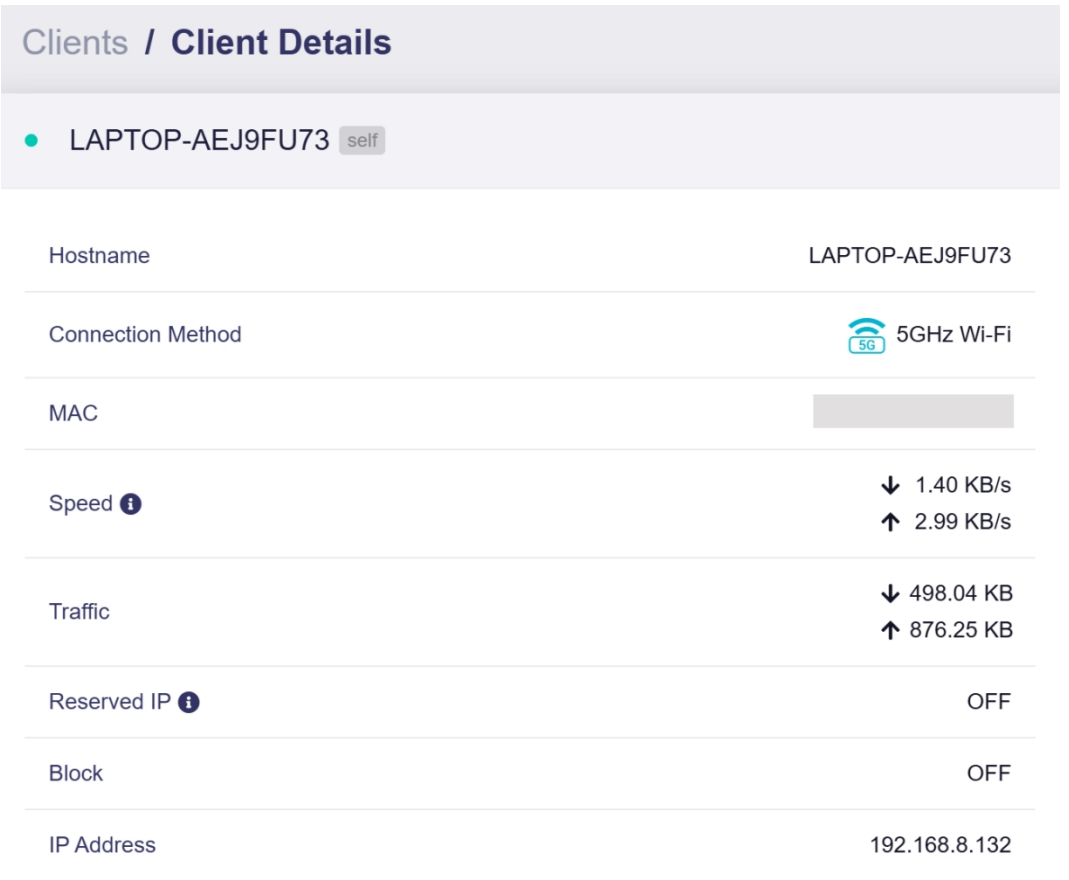
- **Liste de blocage (Blacklist)** : les appareils dont l'adresse MAC figure dans cette liste ne peuvent pas se connecter au routeur. Le blocage repose sur l'adresse MAC : un appareil bloqué peut donc se reconnecter s'il utilise une autre adresse MAC.
- **Liste d'autorisation (Allowlist)** : seuls les appareils possédant les adresses MAC indiquées peuvent se connecter au routeur. Ce mode convient aux appareils IoT et à la gestion des réseaux d'entreprise.

6.2 Actions

1. **Afficher les détails**

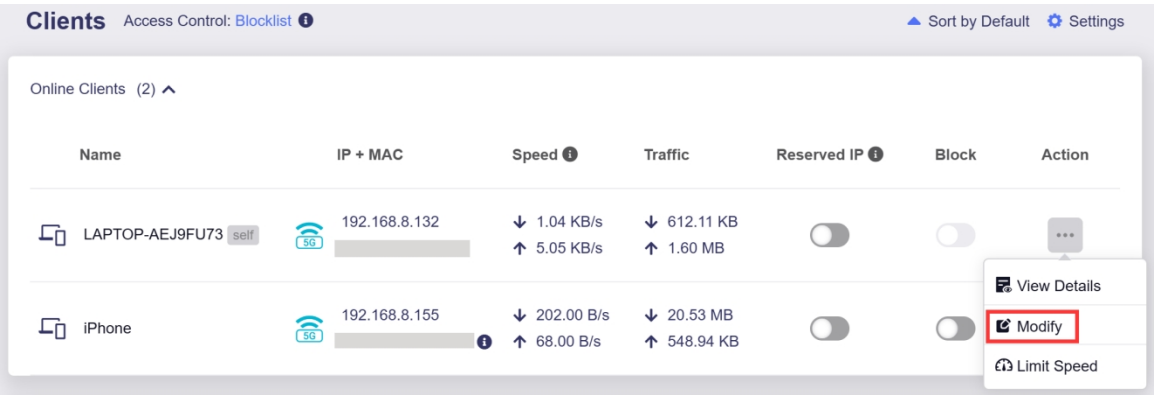
   Cliquez sur les trois points dans la colonne **Action**, puis sur **Afficher les détails (View Details)** dans le menu déroulant pour consulter les informations de l'appareil sur une seule page.

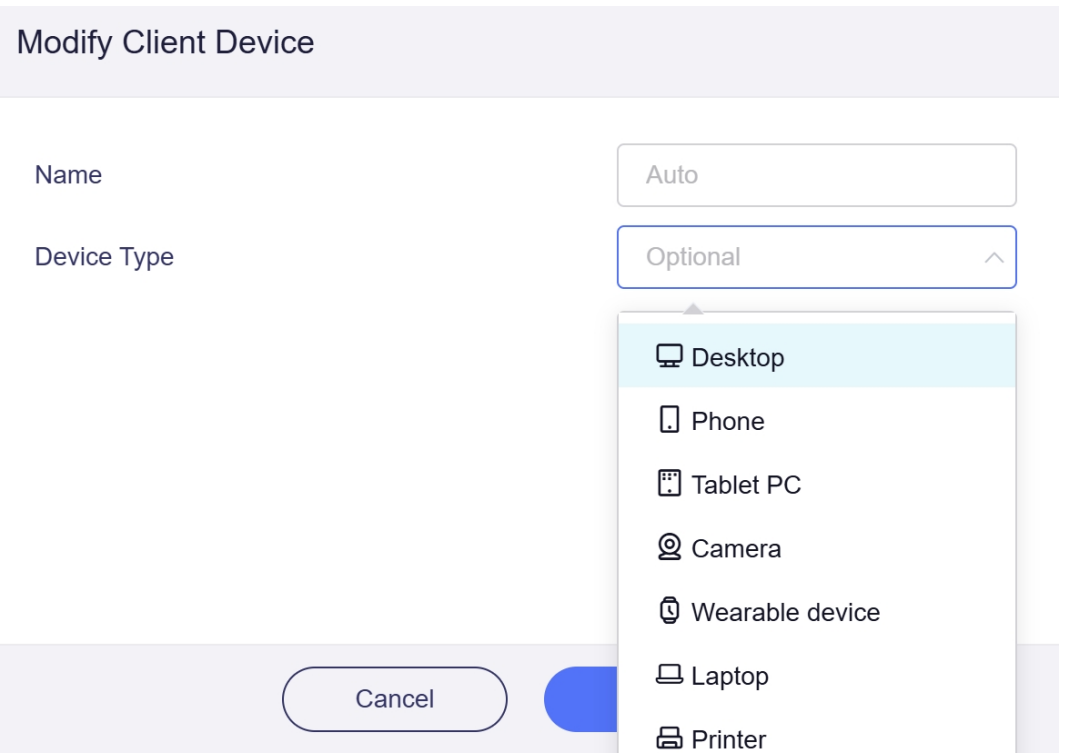




2. **Modifier**

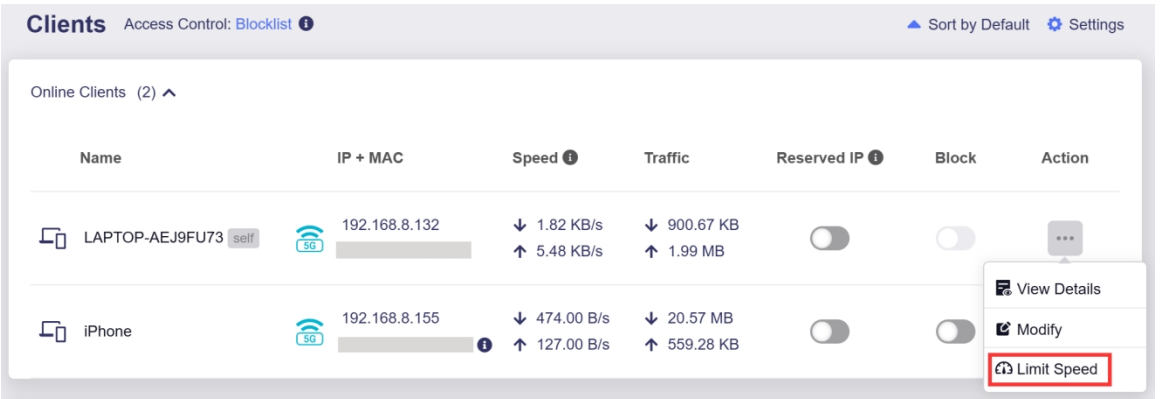
Cliquez sur les trois points dans la colonne **Action**, puis sur **Modifier (Modify)** dans le menu déroulant pour modifier le nom et le type de l'appareil.

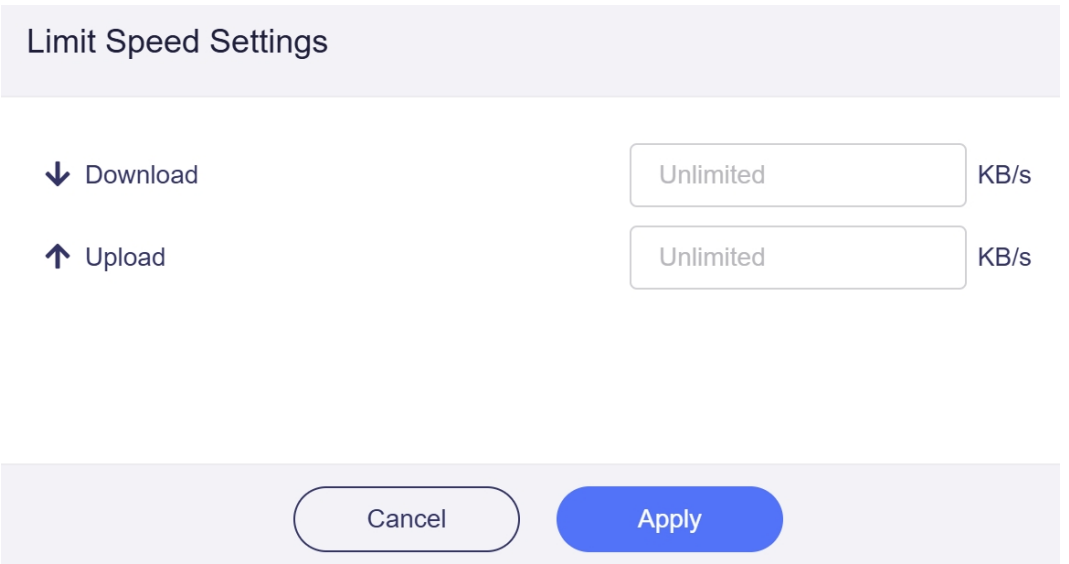




3. **Limiter le débit**

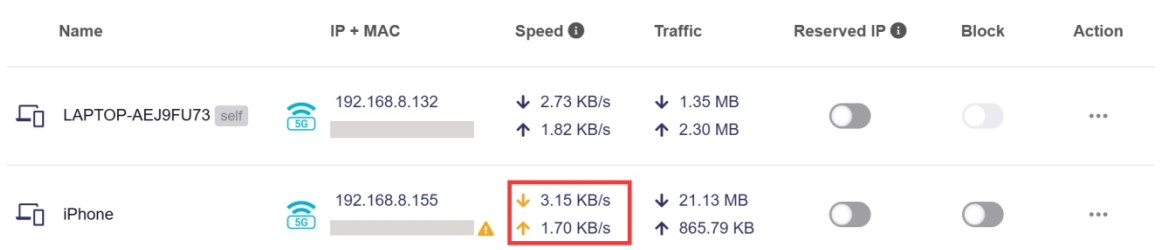
Cliquez sur les trois points dans la colonne **Action**, puis sur **Limiter le débit (Limit Speed)** dans le menu déroulant.





Vous pouvez limiter le débit d'un appareil connecté. L'unité utilisée est le Ko/s (KB/s).

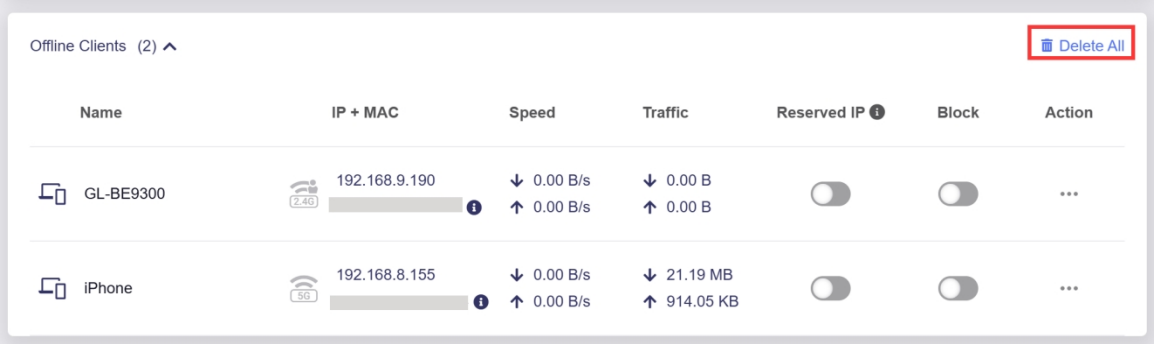
Lorsqu'une limite de débit est appliquée à un appareil, les flèches de débit montant et descendant deviennent jaunes.



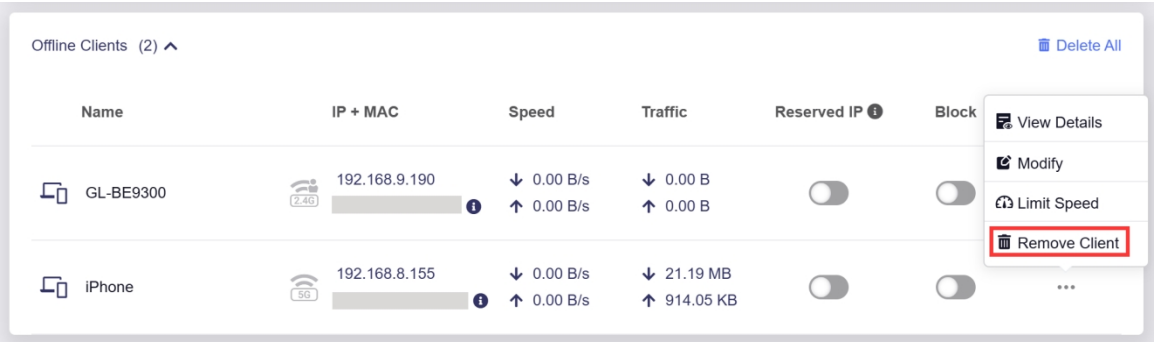
Conseil : si l’option Limiter le débit n’apparaît pas, ouvrez **RÉSEAU (NETWORK)** > **Accélération réseau (Network Acceleration)** et désactivez l’accélération. L’option Limiter le débit devient alors disponible.

6.3 Suppression de clients

Dans la section **Clients hors ligne (Offline Clients)**, cliquez sur **Tout supprimer (Delete All)** dans l'angle supérieur droit pour supprimer tous les clients hors ligne.

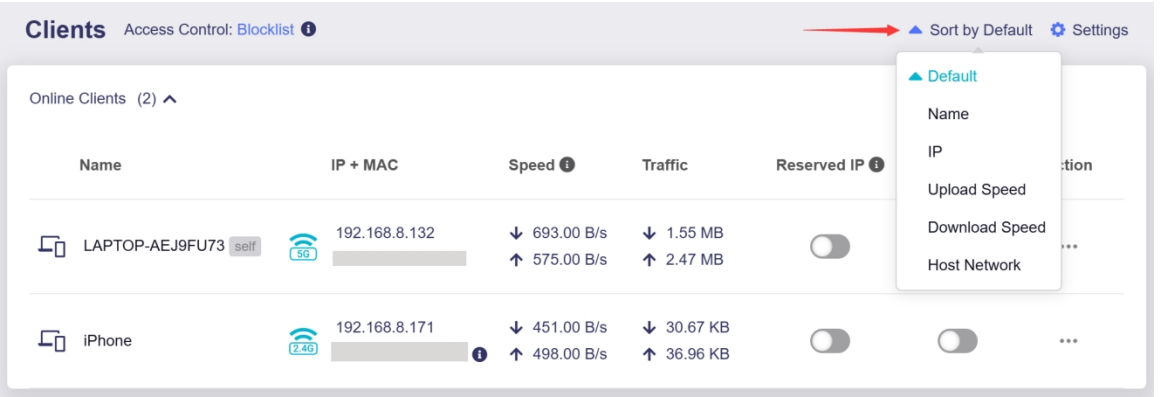


Pour supprimer un client précis, cliquez sur les trois points dans la colonne **Action**, puis sur **Supprimer le client (Remove Client)** dans le menu déroulant.



6.4 Tri

Vous pouvez définir la règle de tri des appareils en haut à droite de la page Clients.



Les règles de tri par défaut sont les suivantes.

- L'appareil utilisé pour accéder à l'interface d'administration Web du routeur figure toujours en première position.
- Dans la section **Clients en ligne (Online Clients)**, les appareils connectés depuis le plus longtemps apparaissent en premier.
- Dans la section **Clients hors ligne (Offline Clients)**, les appareils déconnectés depuis le plus longtemps apparaissent en premier.

Chapitre 7

Services cloud

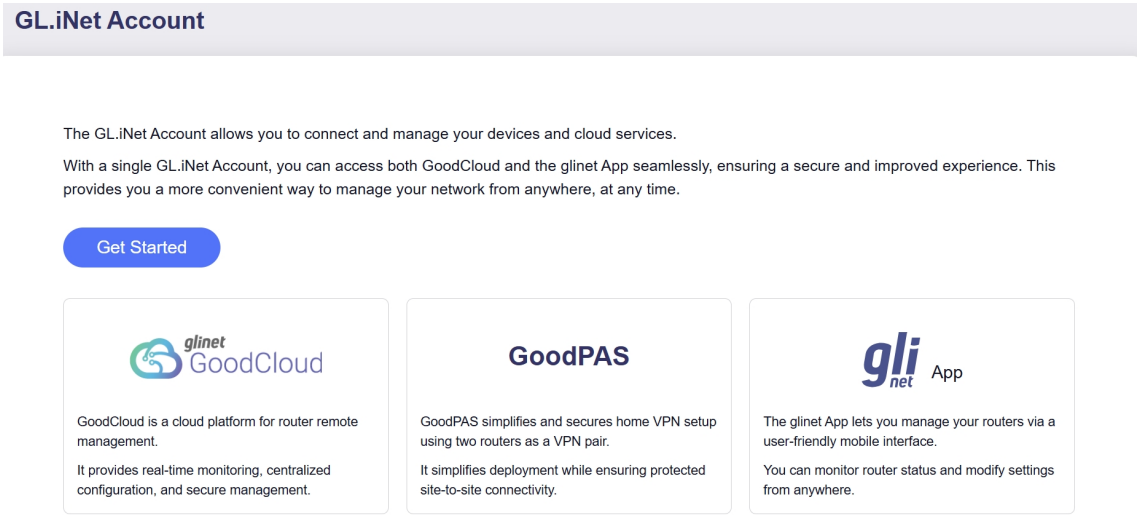
Ce chapitre présente trois services cloud : GL.iNet Account, GoodCloud et GoodPAS.

7.1 GL.iNet Account

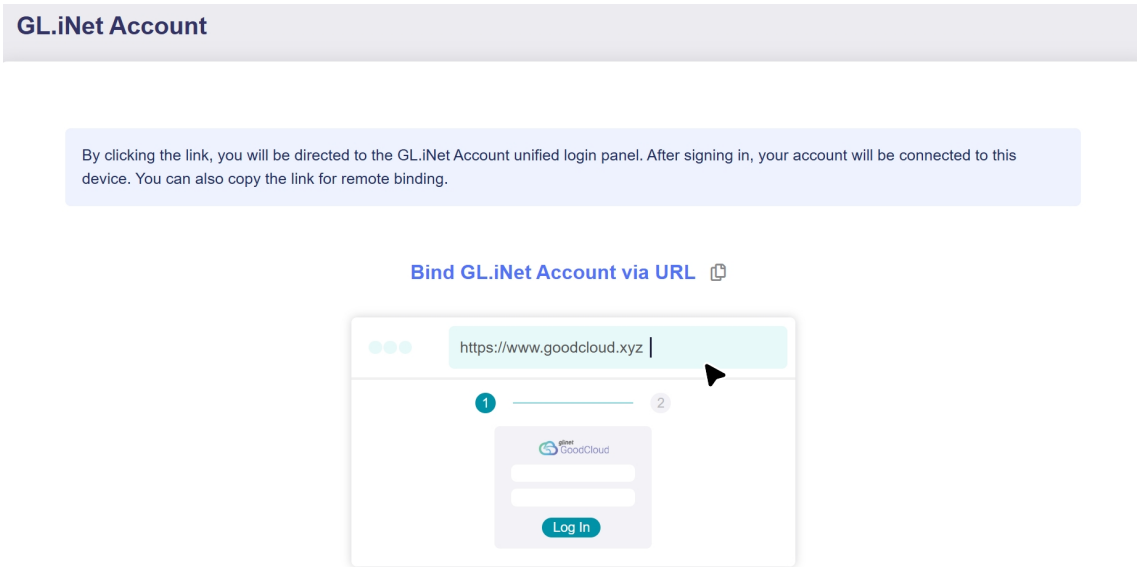
GL.iNet Account permet de connecter et de gérer vos appareils et vos services cloud. Vous pouvez accéder aux fonctions et services cloud, notamment GoodCloud, GoodPAS et l'application GL.iNet.

7.1.1 Activer GL.iNet Account

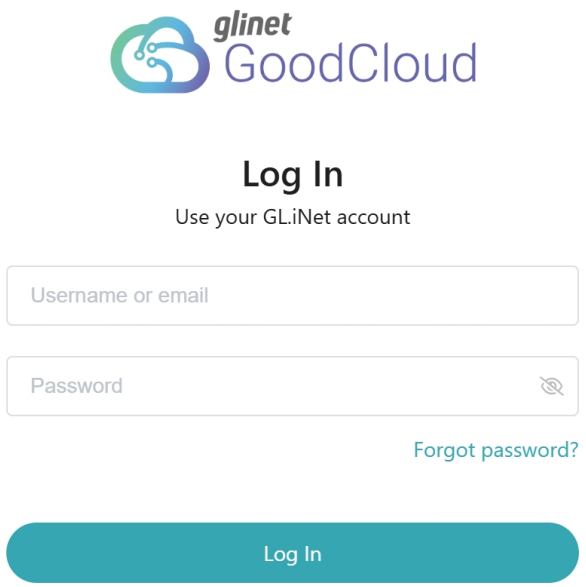
1. Connectez-vous à l'interface d'administration Web du routeur, ouvrez **SERVICE CLOUD (CLOUD SERVICE)** > **GL.iNet Account**, puis cliquez sur **Commencer (Get Started).**



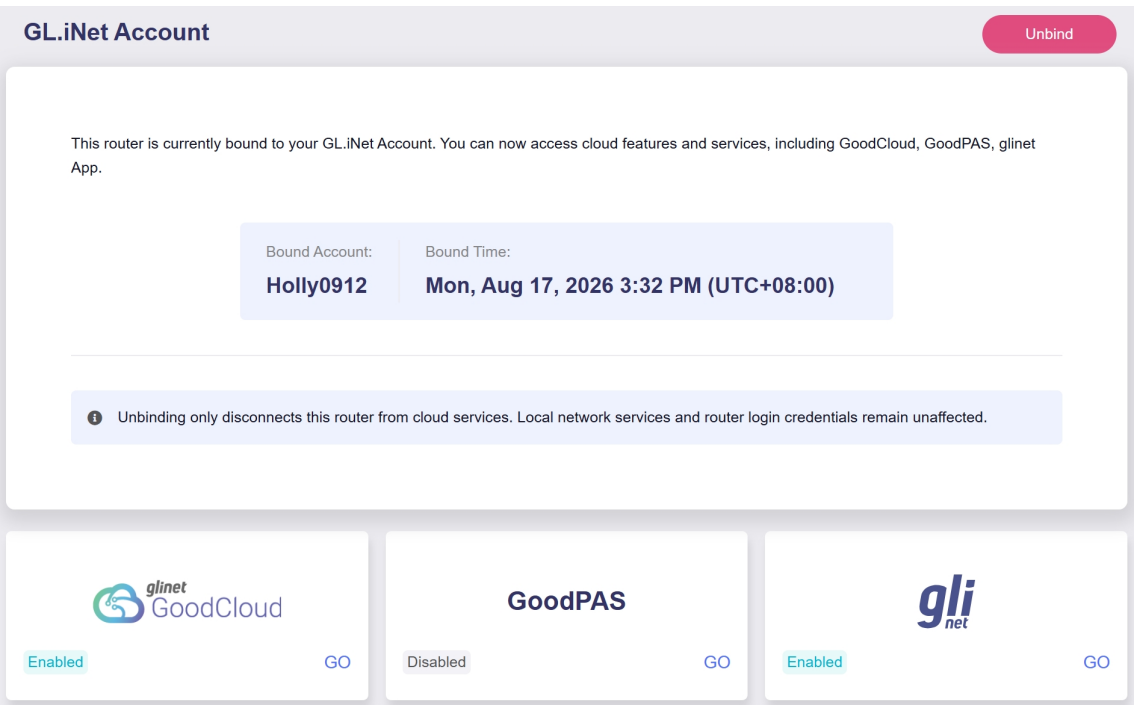
2. Une URL s'affiche alors sur la page. Cliquez sur le **lien** pour vous connecter via la page GL.iNet Account, ou copiez-le pour associer l'appareil à distance.



3. Connectez-vous avec votre compte GL.iNet. Si vous n’avez pas de compte, créez-en un, puis connectez-vous.



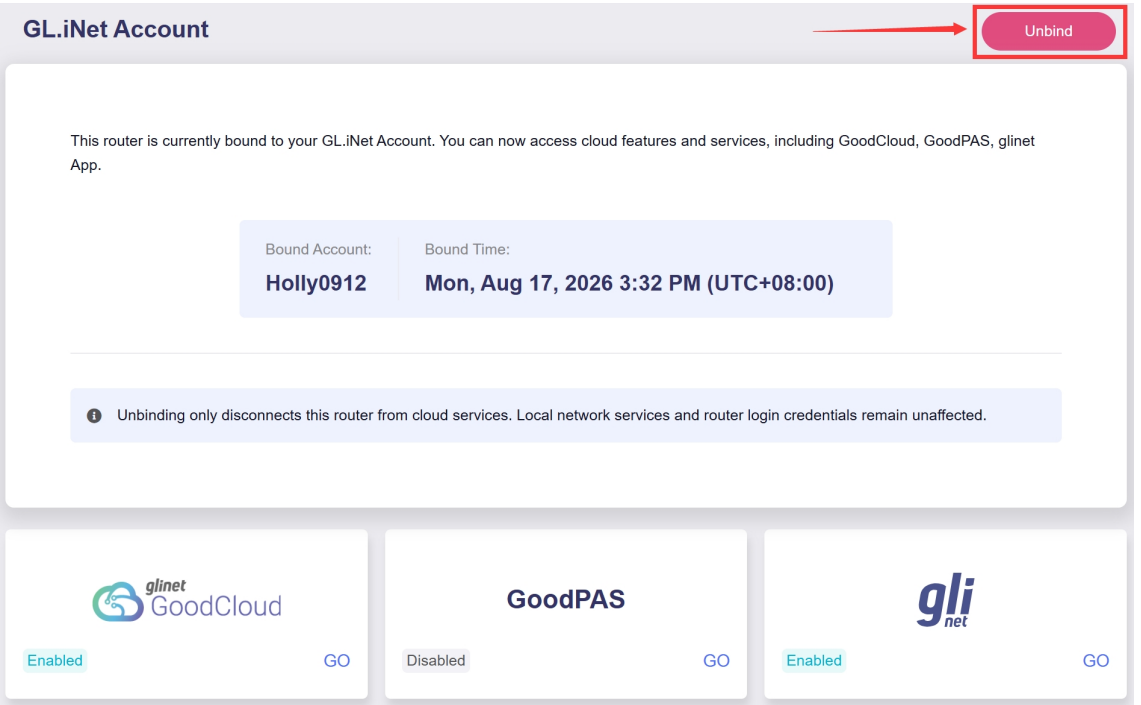
4. Après la connexion, la page affiche le compte associé et la date et l’heure de l’association. Vous pouvez gérer l’association entre le routeur et votre compte GL.iNet sur cette page. L’indication Activé/Désactivé dans l’angle inférieur gauche de chaque service cloud permet de vérifier son état. Cliquez sur **GO** à côté d’un service pour ouvrir la page correspondante.



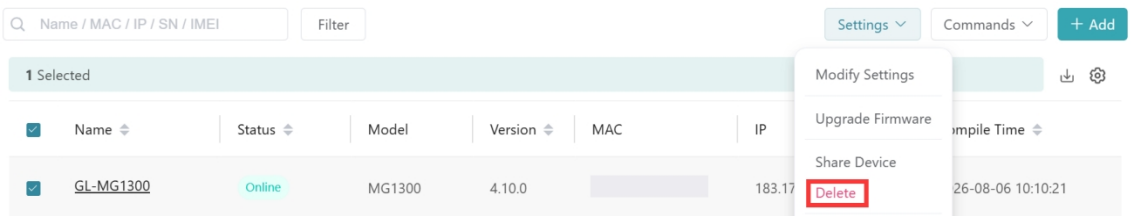
5. GoodPAS est désactivé par défaut. Pour l’activer, consultez la section 7.3 GoodPAS**.**

7.1.2 Dissocier GL.iNet Account

Dans l'interface d'administration Web du routeur, ouvrez **SERVICES CLOUD (CLOUD SERVICES)** > **GL.iNet Account**, puis cliquez sur **Dissocier (Unbind)**. Votre appareil est alors dissocié de votre compte GoodCloud.



Vous pouvez également vous connecter à la plateforme Cloud et ouvrir **Appareil (Device)** > **Appareils associés (Bound Devices)**. Sélectionnez l'appareil à dissocier, cliquez sur **Paramètres (Settings)** dans l'angle supérieur droit, puis sélectionnez **Supprimer (Delete)**. L'appareil est alors dissocié de votre compte GoodCloud.



7.2 GoodCloud

GL.iNet GoodCloud est une plateforme qui simplifie le déploiement et la gestion à distance des appareils connectés. Elle permet d'accéder facilement aux routeurs GL.iNet et de les gérer à distance. En centralisant les appareils réseau dans le cloud, les utilisateurs peuvent réaliser des opérations groupées, comme le déploiement de configurations réseau et les mises à jour logicielles. Ils peuvent aussi accéder à distance à l'interface d'administration Web du routeur ou à son terminal via SSH, pour gérer leurs appareils réseau de bout en bout, quelle que soit leur localisation.

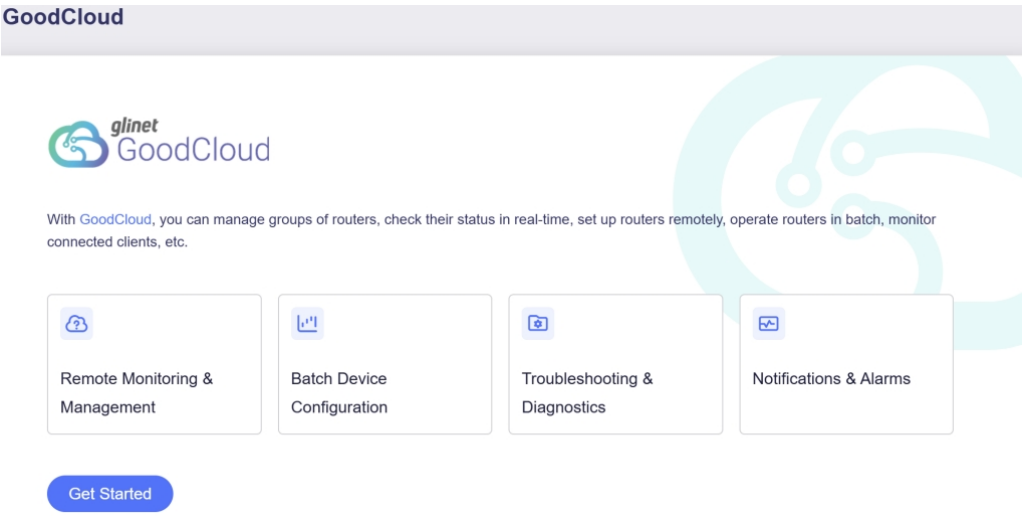
Avec GoodCloud, vous pouvez :

- Vérifier l'état du routeur en temps réel
- Gérer des groupes de routeurs
- Configurer les routeurs à distance
- Surveiller les clients connectés
- Effectuer des opérations groupées sur les routeurs
- Établir une connexion site à site

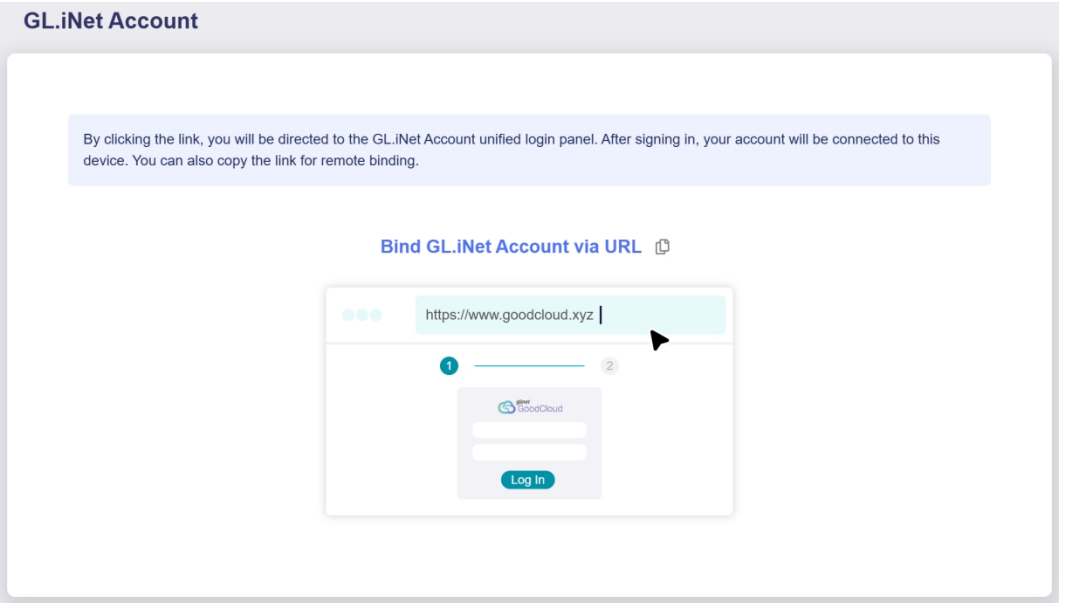
Certaines fonctions sont proposées dans les offres Enterprise et VAR (Value Added Reseller, revendeur à valeur ajoutée). Consultez cette page pour en savoir plus.

7.2.1 Activation de GoodCloud

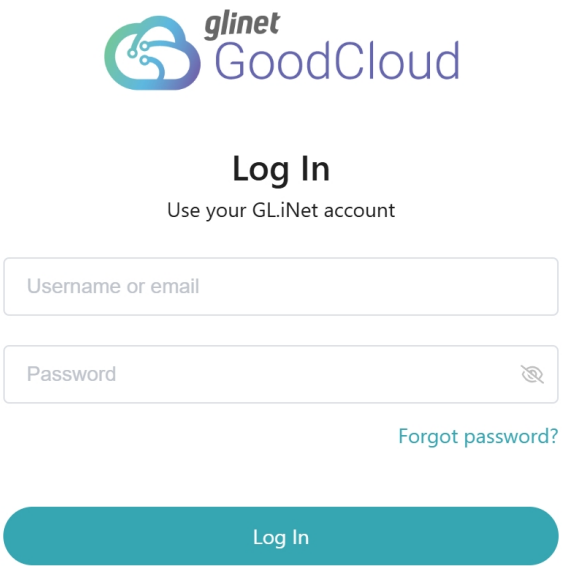
1. Connectez-vous à l'interface d'administration Web du routeur, ouvrez **SERVICE CLOUD (CLOUD SERVICE)** > **GoodCloud**, puis cliquez sur **Commencer (Get Started).**



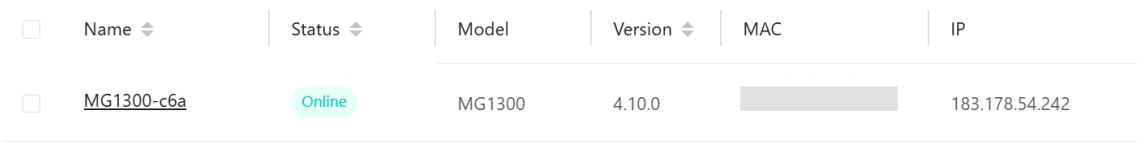
2. Une URL s’affiche alors sur la page. Cliquez sur le **lien** pour vous connecter via la page GL.iNet Account, ou copiez-le pour associer l’appareil à distance.



3. Connectez-vous avec votre compte GL.iNet. Si vous n’en possédez pas, créez-en un, puis connectez-vous.



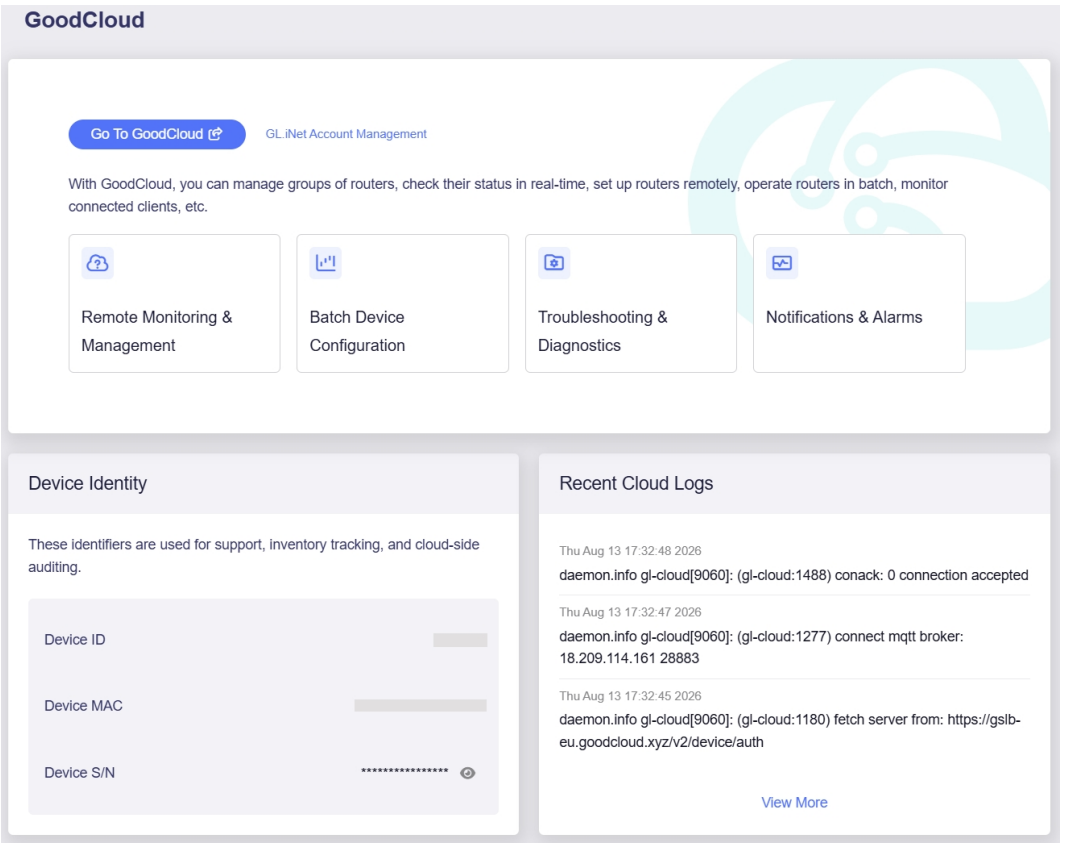
4. À l’étape suivante, confirmez les informations de votre compte et de l’appareil, puis cliquez sur **Associer (Bind)**. Vous accédez alors à la plateforme GoodCloud, où vous pouvez vérifier que le routeur est associé à votre compte.



Conseils :

- La procédure d'association à GoodCloud varie selon la version du micrologiciel.
- Si vous ne recevez pas l'e-mail de vérification lors de l'inscription, vérifiez votre dossier de courrier indésirable ou réessayez plus tard. Pour obtenir de l'aide, écrivez-nous à support@gl-inet.com.

5. Après l'association, revenez à la page des services cloud dans l'interface d'administration Web. Elle affiche l'identité de l'appareil associé et les journaux cloud récents, notamment l'identifiant, l'adresse MAC et le numéro de série de l'appareil.



6. Lorsque vous vous connectez à GoodCloud, l'accès Web distant et l'accès SSH distant sont également activés par défaut. Ces fonctions facilitent la gestion et le dépannage à distance.

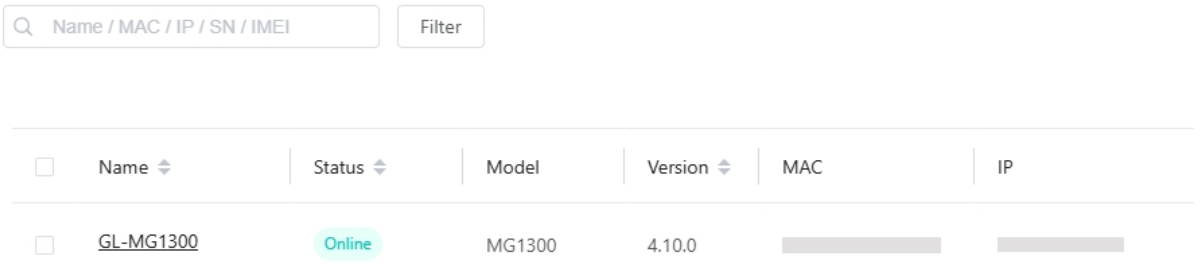
- **Accès Web distant (Remote Web Access)** : accédez à distance à l'interface d'administration Web du routeur depuis GoodCloud via HTTP/HTTPS.

- **SSH à distance (Remote SSH)** : accédez au terminal du routeur depuis GoodCloud via SSH.

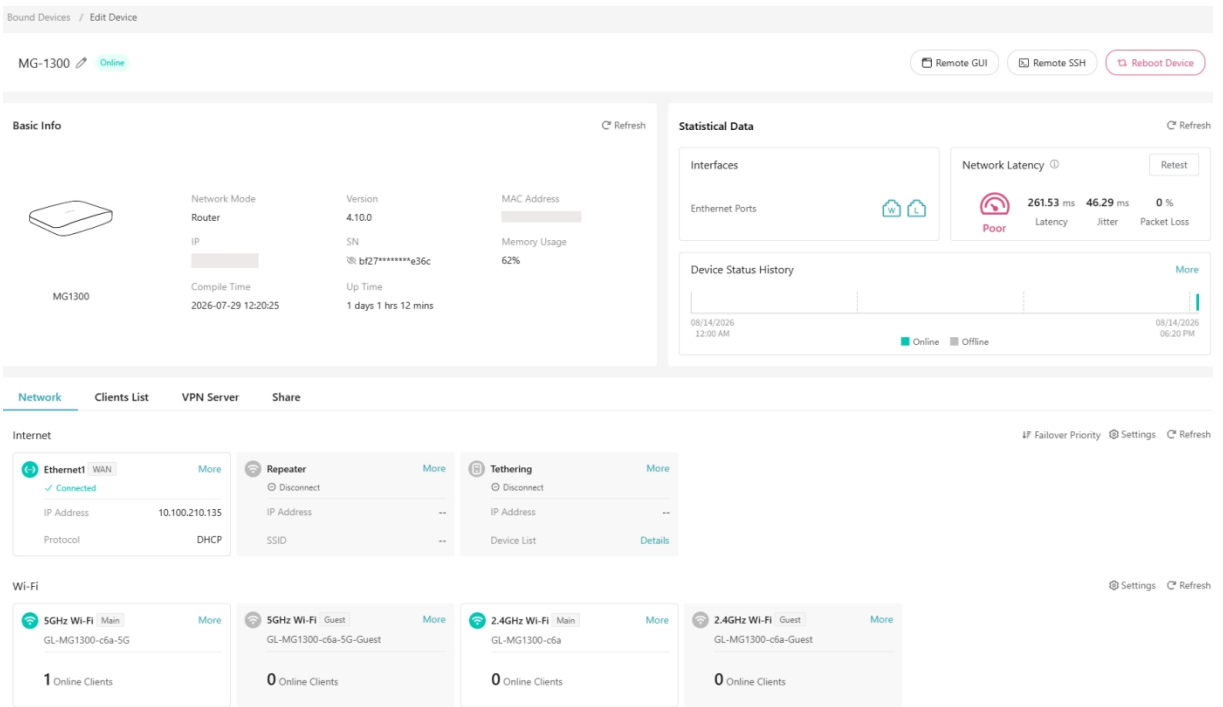
7.2.2 Gestion de votre routeur

Consultation des informations de l’appareil

Connectez-vous à GoodCloud et ouvrez **Appareils (Devices)** > **Appareils associés (Bound Devices)**. Vous pouvez consulter les informations de base : nom d’hôte, état en ligne ou hors ligne, modèle, version du micrologiciel et adresse MAC.

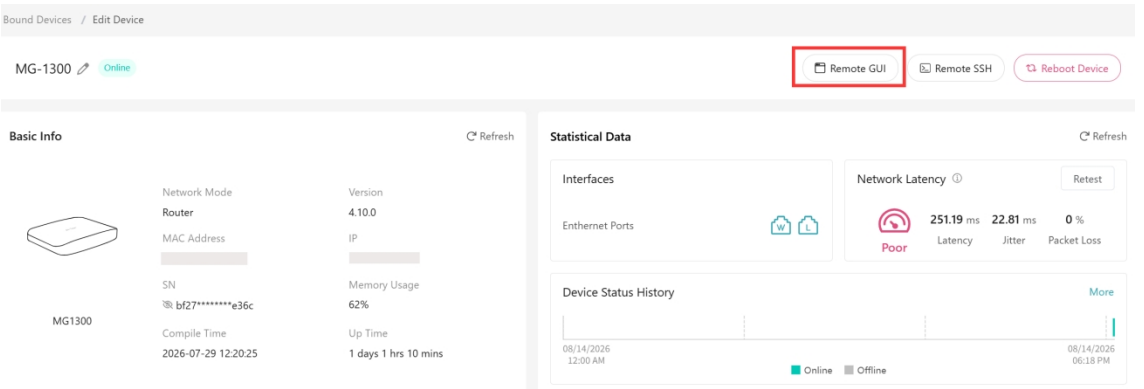


Cliquez sur le nom de l’appareil pour ouvrir sa page de détails. Elle présente les informations de base, les statistiques, la vue d’ensemble du réseau, la liste des clients et la chronologie. Vous pouvez également effectuer des opérations avancées, comme accéder au routeur à distance ou le redémarrer.

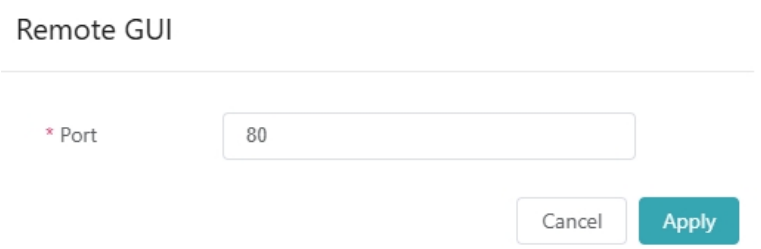


Accès distant à l’interface Web

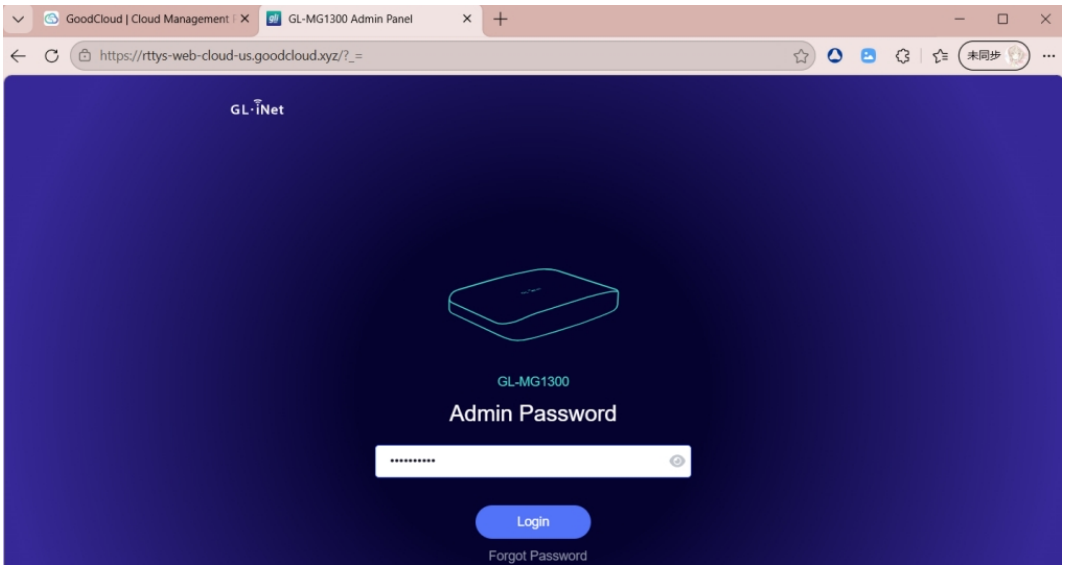
1. Connectez-vous à la plateforme GoodCloud et ouvrez **Appareils (Devices)** > **Appareils associés (Bound Devices)**. Cliquez sur l’appareil auquel vous souhaitez accéder pour ouvrir sa fiche. Sur cette fiche, cliquez sur le bouton **Interface distante (Remote GUI)** dans l’angle supérieur droit.



2. Sélectionnez le protocole de transfert et le port. Les valeurs par défaut sont **HTTP** et le port **80**. Si vous choisissez HTTPS, le port passe automatiquement à 443. Cliquez ensuite sur **Appliquer (Apply)**.

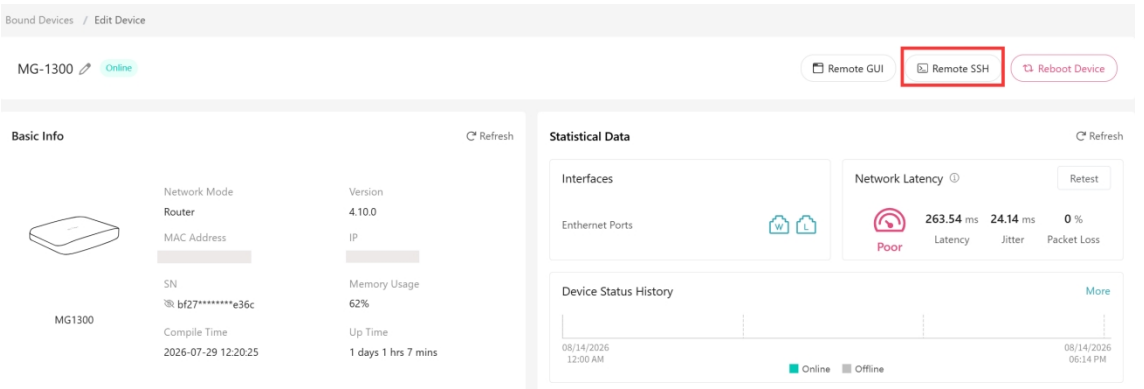


3. Vous êtes redirigé vers la page de connexion du routeur. Saisissez le mot de passe administrateur pour accéder à distance à son interface d’administration Web.



Accès distant au terminal

1. Connectez-vous à GoodCloud et ouvrez **Appareils (Devices)** > **Appareils associés (Bound Devices)**. Cliquez sur l'appareil auquel vous souhaitez accéder pour ouvrir sa page de détails.
2. Sur cette page, cliquez sur le bouton **SSH à distance (Remote SSH)** dans l'angle supérieur droit.

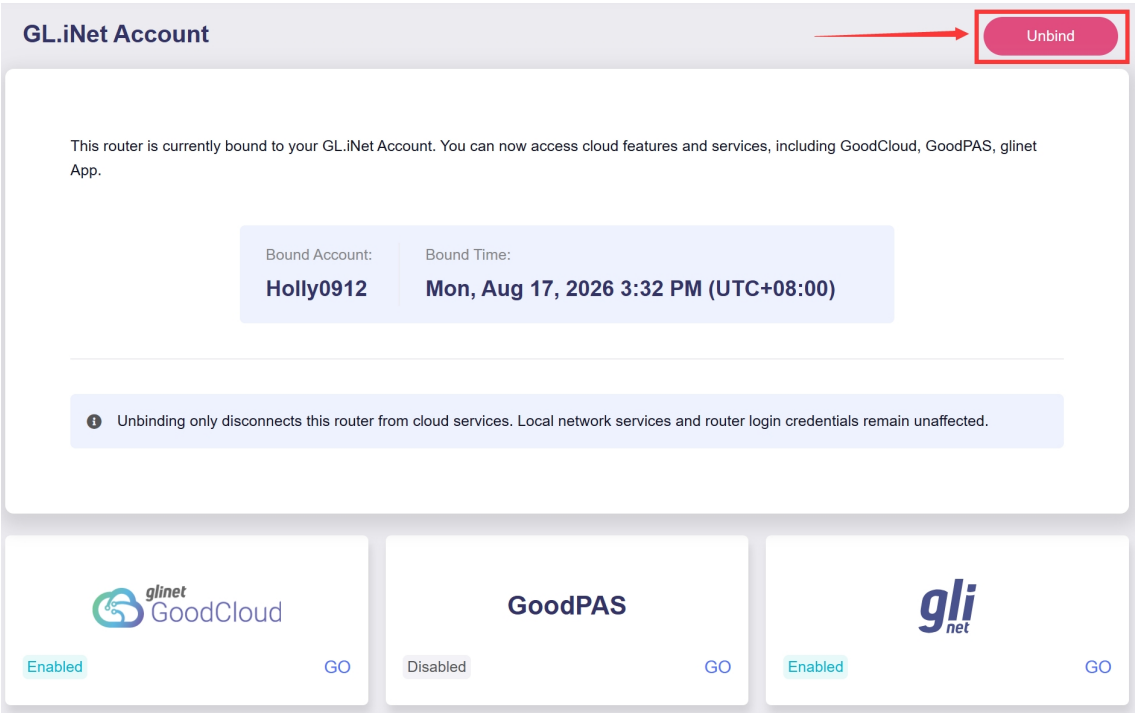


3. Connectez-vous avec l'identifiant **root** et saisissez le mot de passe pour accéder au terminal du routeur.

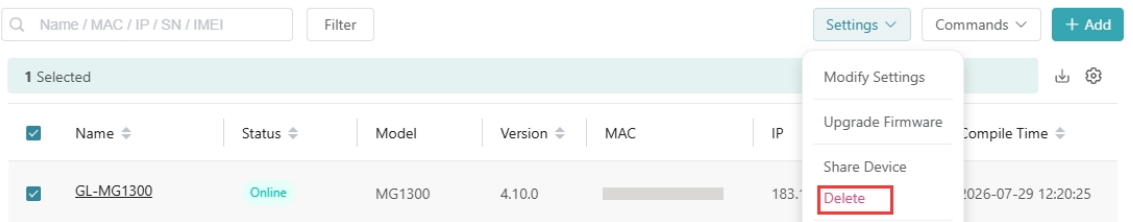

GL-MG1300 login: root
Password:
BusyBox v1.35.0 (2023-04-09 12:27:46 UTC) built-in shell (ash)
W I R E L E S S F R E E D O M
OpenWrt 22.03.4, r20123-38ccc47687
root@GL-MG1300:~#

7.2.3 Dissociation de l’appareil

Dans l’interface d’administration Web du routeur, ouvrez **SERVICES CLOUD (CLOUD SERVICES)** > **GL.iNet Account**, puis cliquez sur **Dissocier (Unbind)**. Votre appareil est alors dissocié de votre compte GoodCloud.



Vous pouvez également vous connecter à la plateforme Cloud et ouvrir **Appareils (Devices)** > **Appareils associés (Bound Devices)**. Sélectionnez l’appareil à dissocier, cliquez sur **Paramètres (Settings)** dans l’angle supérieur droit, puis choisissez **Supprimer (Delete)**. L’appareil est alors dissocié de votre compte GoodCloud.



7.3 GoodPAS

GoodPAS est une fonction réseau avancée pour les routeurs GL.iNet, qui facilite l'accès à distance et la gestion des appareils. Intégrée au SDK des routeurs GL.iNet, elle utilise le protocole AmneziaWG avec obfuscation du trafic intégrée pour fournir des connexions stables et sécurisées et un accès distant fiable, à tout moment et depuis n'importe où.

Cette fonction permet d'accéder facilement à votre réseau domestique à distance. Configurez et associez directement les appareils à l'aide d'un code d'accès dynamique dans l'interface d'administration Web : une connexion sécurisée entre votre routeur de voyage et votre réseau domestique s'établit en quelques secondes, sans inscription ni connexion à un compte.

Remarque :

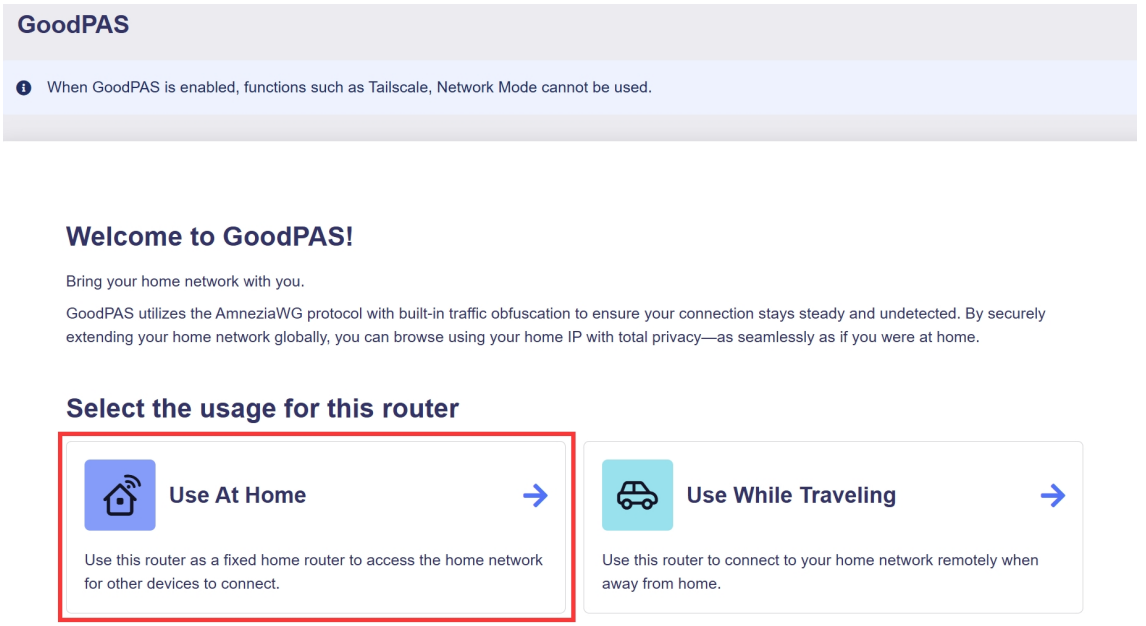
1. Il est déconseillé d'utiliser GoodPAS simultanément avec les fonctions suivantes, car cela peut provoquer des conflits de routage : GoodCloud Site to Site, ZeroTier, Tailscale et Tor.
2. Lorsque GoodPAS est activé, la fonction Mode réseau n'est pas disponible.

7.3.1 Configuration rapide

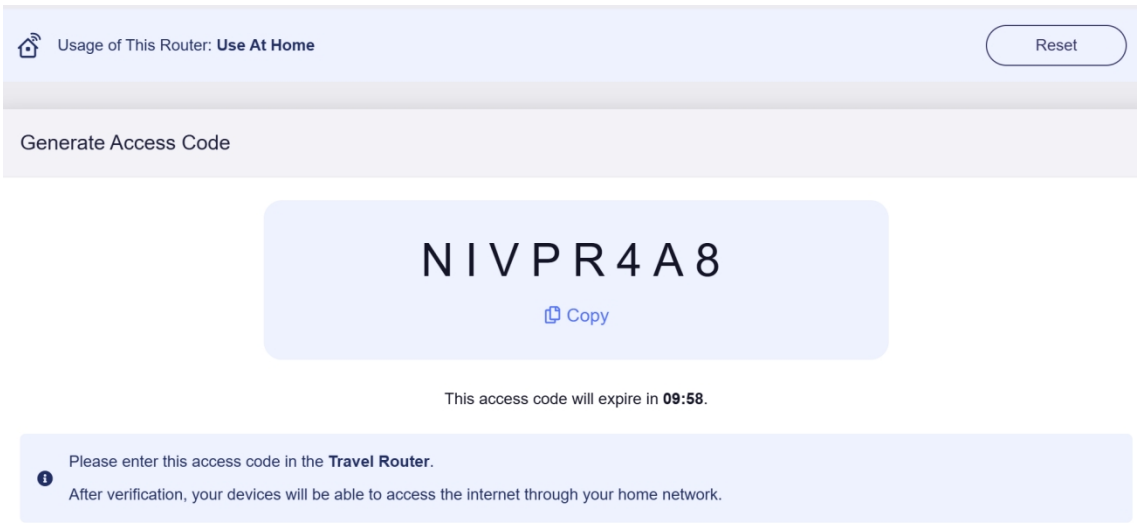
L'exemple ci-dessous utilise Mango 2 (GL-MG1300) et Flint 3 (GL-BE9300) pour créer un réseau GoodPAS. Flint 3 sert de routeur domestique, tandis que Mango 2 sert de routeur de voyage et achemine le trafic réseau vers Flint 3 pour accéder à Internet.

Conseil : chaque routeur GL.iNet bénéficie de **10 GB de données gratuites par mois** pour le réseau GoodPAS. Les appareils du réseau GoodPAS utilisent le forfait de données du routeur domestique pour accéder à Internet. Si nécessaire, vous pouvez souscrire l'offre GoodPAS+ pour disposer de données illimitées.

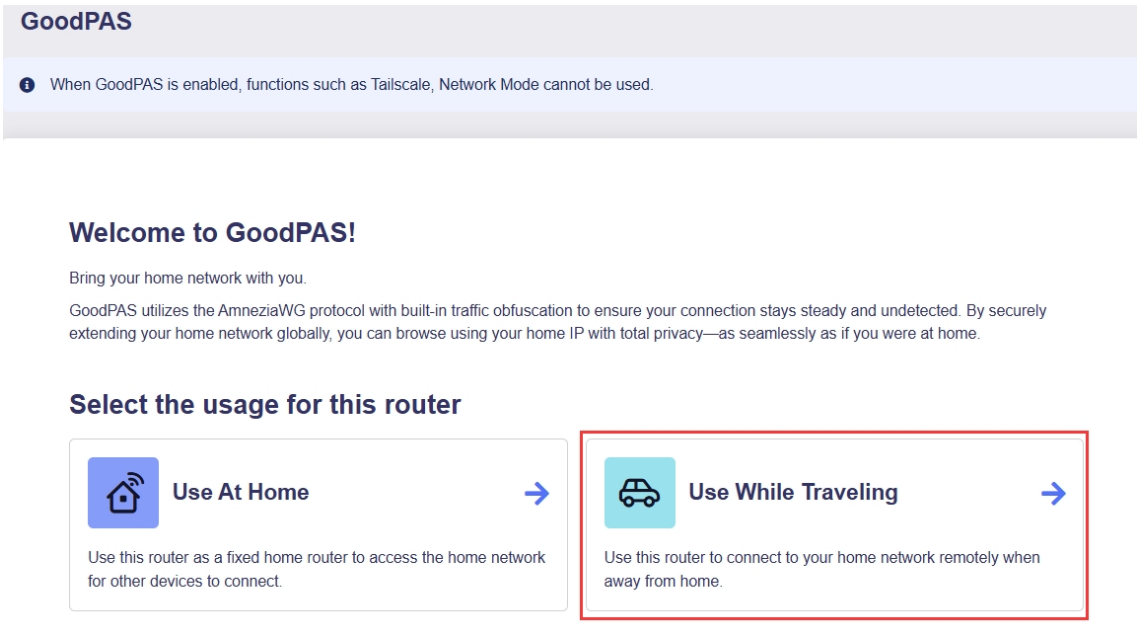
1. Configurez la connexion Internet de Flint 3.
   Connectez-vous à l'interface d'administration Web de Flint 3 et ouvrez la page INTERNET. Connectez-le à Internet avec l'un des modes pris en charge : Ethernet, répéteur, partage de connexion ou réseau mobile.
2. Dans l'interface d'administration Web de Flint 3, ouvrez **SERVICES CLOUD (CLOUD SERVICES)** > **GoodPAS**. Cliquez sur **Utiliser à domicile (Use At Home)**.



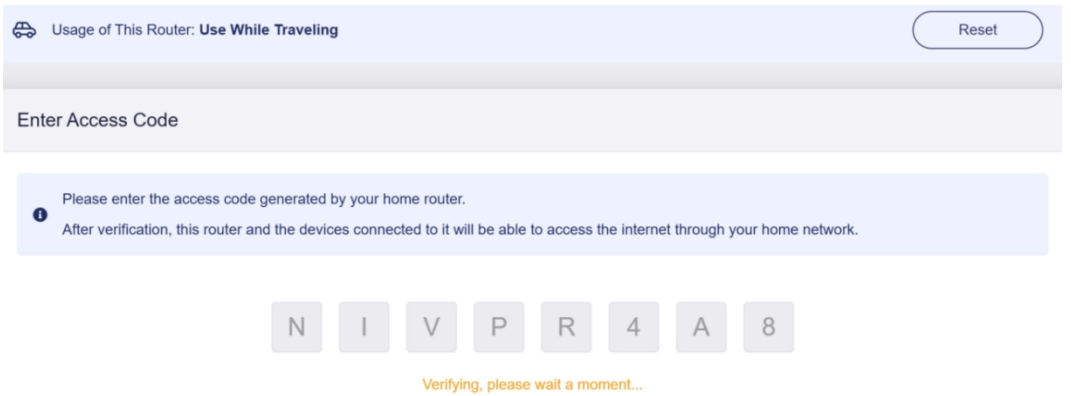
Un **code d'accès (Access Code)** est généré. Copiez-le pour l'utiliser ensuite.



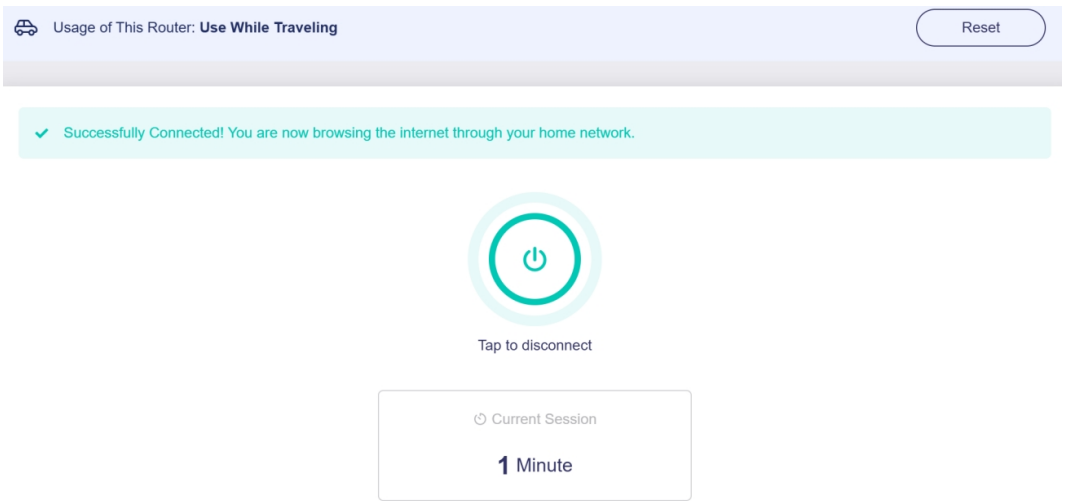
3. Configurez la connexion Internet de Mango 2.
   Connectez-vous à l'interface d'administration Web de Mango 2 et ouvrez la page INTERNET. Connectez-le à Internet avec l'un des modes pris en charge : Ethernet, répéteur, partage de connexion ou réseau mobile.
4. Saisissez le code d'accès.
   Dans l'interface d'administration Web de Mango 2, ouvrez **SERVICES CLOUD (CLOUD SERVICES)** > **GoodPAS**. Cliquez sur **Utiliser en voyage (Use While Traveling)**.



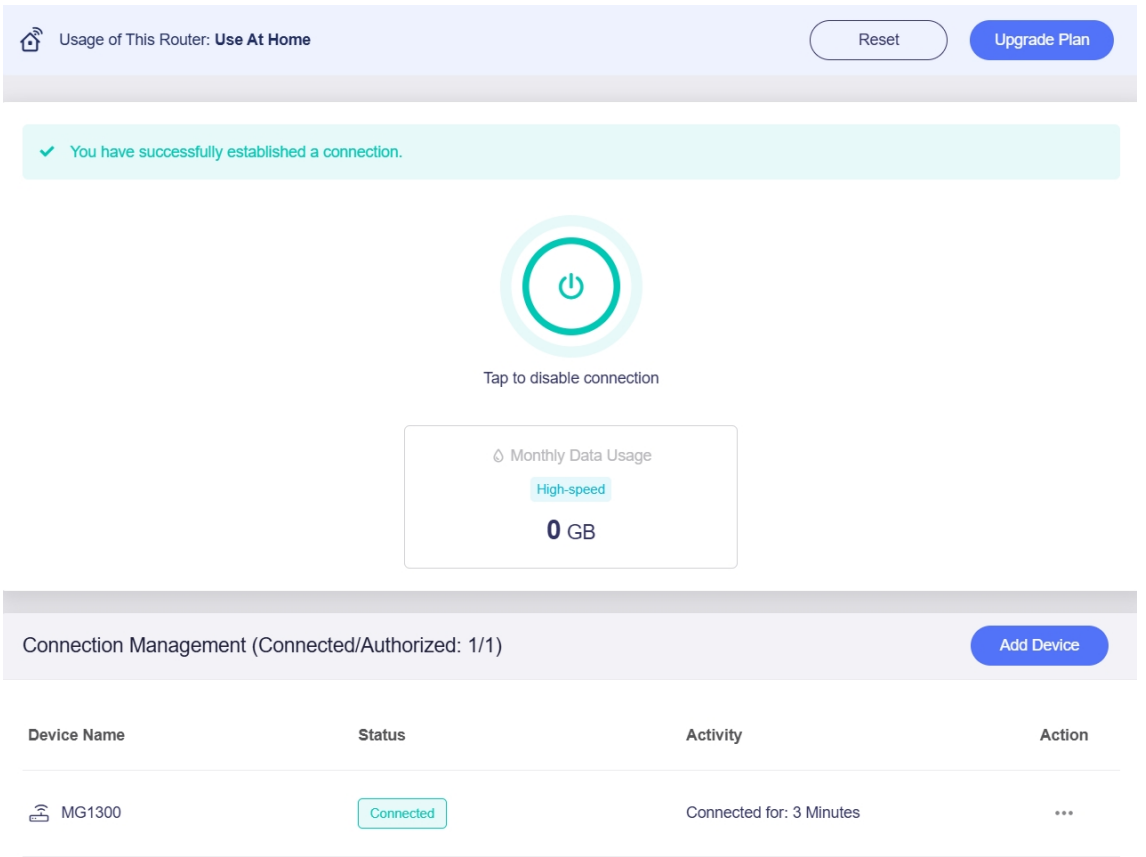
Saisissez le code d'accès obtenu à l'étape 2 et attendez la fin de la vérification.



La connexion au routeur domestique Flint 3 est alors établie. Vous pouvez désormais naviguer sur Internet en toute sécurité via votre réseau domestique.

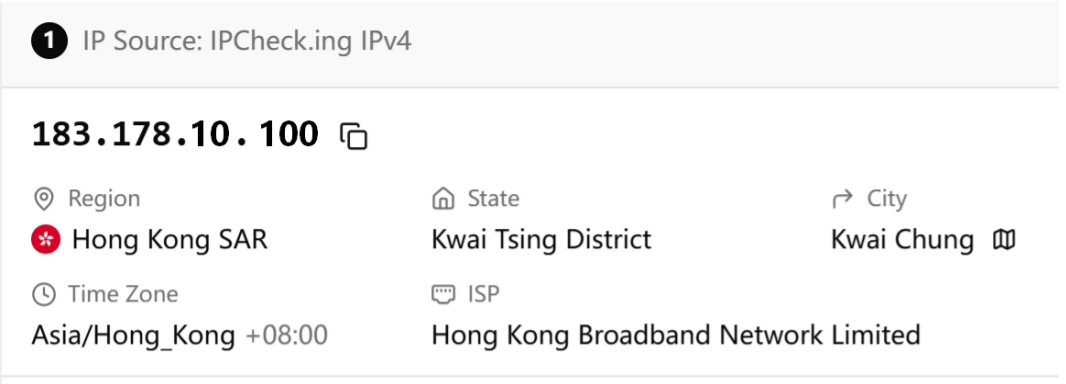


5. L’interface d’administration Web de Flint 3 affiche également l’état de la connexion, comme illustré ci-dessous.

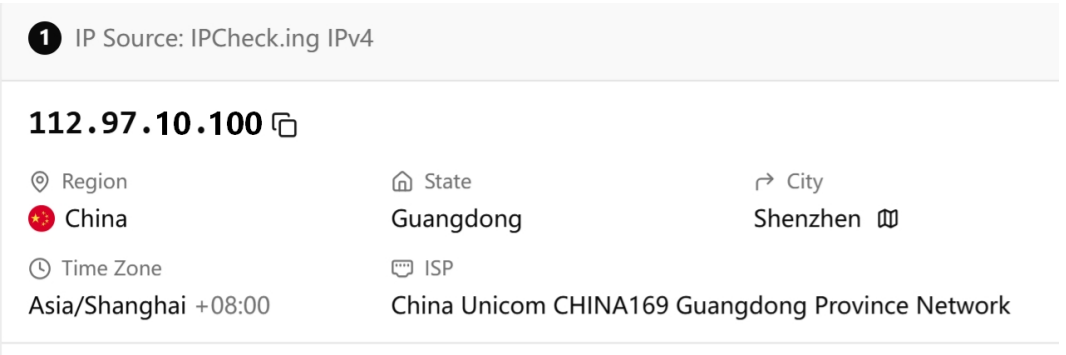


7.3.2 Vérification de la connexion

1. Connectez un ordinateur portable ou un smartphone au Wi-Fi du routeur de voyage Mango 2.
2. Ouvrez un navigateur et accédez à ipcheck.ing ou à un autre site de vérification d'adresse IP. Le site affiche l'adresse IP publique de Flint 3, ce qui indique que Mango 2 accède à Internet via votre routeur domestique Flint 3.

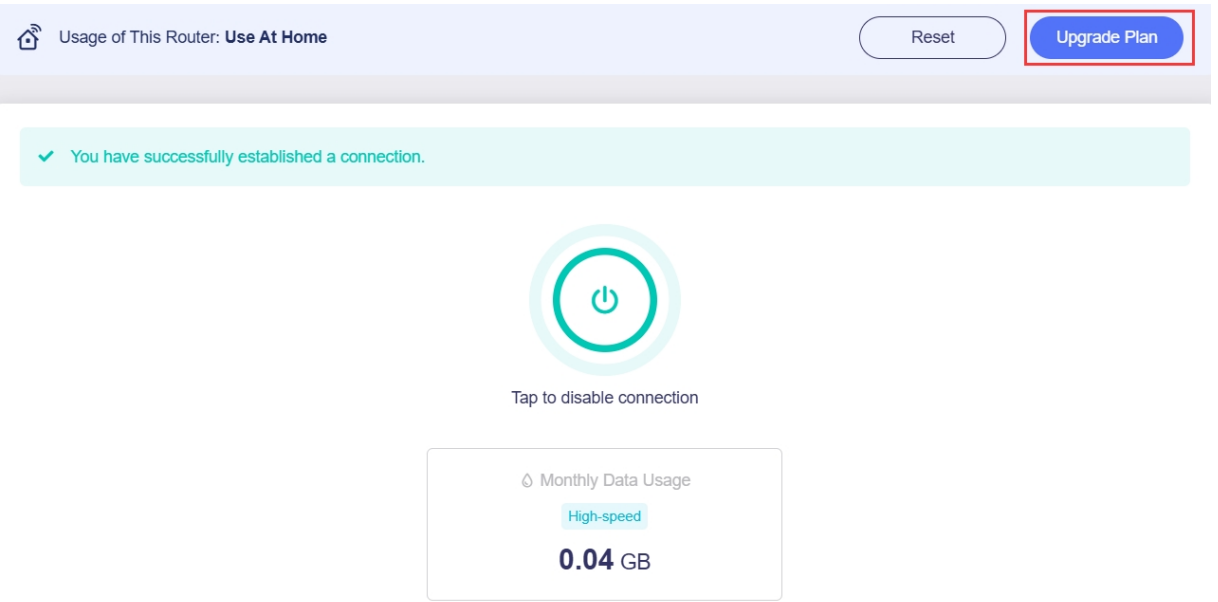


3. Déconnectez GoodPAS sur Mango 2, puis actualisez la page Web pour relancer la vérification de l'adresse IP. Le site affiche l'adresse IP publique de Mango 2, ce qui indique que Mango 2 accède à Internet via son réseau local.



7.3.3 Passer à l’offre supérieure

Chaque routeur GL.iNet bénéficie de **10 GB de données gratuites par mois** pour le réseau GoodPAS. Les appareils du réseau GoodPAS utilisent le forfait de données du routeur domestique pour accéder à Internet. Si nécessaire, vous pouvez souscrire l’offre **GoodPAS+** pour disposer de données illimitées.



Chapitre 8

Comprendre les VPN

Ce chapitre présente les principes des VPN et leurs principaux cas d’utilisation.

8.1 Introduction

VPN

Un VPN (Virtual Private Network, réseau privé virtuel) établit un tunnel privé et chiffré entre un appareil et un serveur distant. Il protège les données transmises et permet d'accéder de manière sécurisée à des réseaux privés ou à accès restreint.

Routeur VPN

Un routeur VPN intègre une fonction VPN qui protège tous les appareils connectés. Configuré comme client VPN, il achemine l'ensemble du trafic dans un tunnel chiffré, sans configuration individuelle de chaque appareil. Vous protégez ainsi plusieurs appareils à la fois, gagnez du temps et maintenez une configuration cohérente, en réduisant les risques liés à des réglages individuels incorrects.

Les routeurs GL.iNet prennent en charge plus de 30 services VPN commerciaux courants utilisant OpenVPN et WireGuard. Importez vos fichiers de configuration VPN pour activer une connexion sécurisée. Consultez cette page pour obtenir la liste complète des fournisseurs VPN tiers.

OpenVPN

OpenVPN est un protocole VPN open source utilisant la sécurité SSL/TLS pour établir des connexions d'un appareil à un site ou de site à site. Il prend en charge plusieurs méthodes de chiffrement, TCP et UDP, et facilite le passage à travers les pare-feu et le NAT.

WireGuard

WireGuard est un protocole VPN léger et rapide, plus simple et plus efficace qu'OpenVPN. Il utilise une cryptographie moderne et une base de code réduite, qui facilite l'audit et renforce la sécurité. Ses algorithmes ChaCha20 et Poly1305 assurent le chiffrement et l'intégrité des données.

8.2 Cas d’utilisation

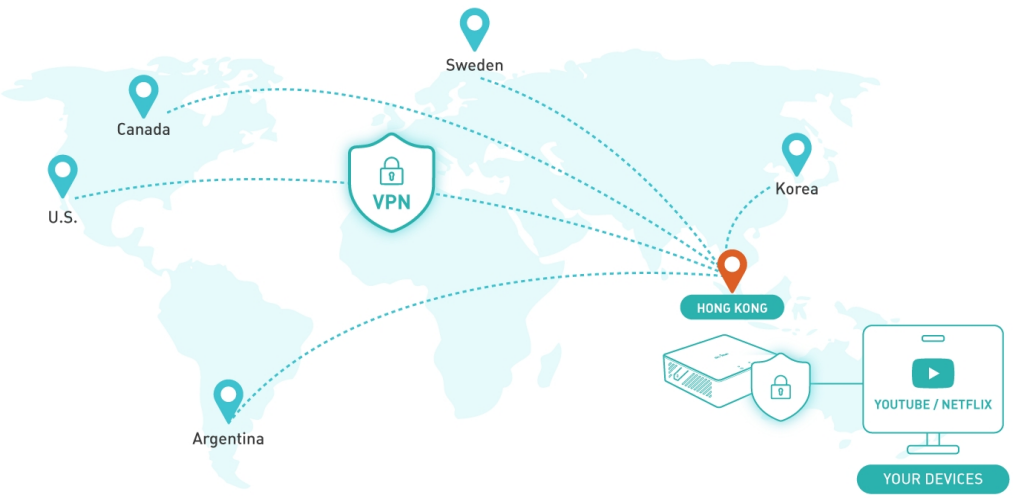
1. **Protection des données personnelles**

   Grâce au routeur, le service VPN protège de nombreux appareils : ordinateurs portables, téléphones, tablettes, mais aussi consoles de jeux, téléviseurs et appareils de streaming. Vos données sont protégées sur les connexions filaires comme sans fil. Vous pouvez également personnaliser les règles VPN pour adapter la protection de certains appareils.



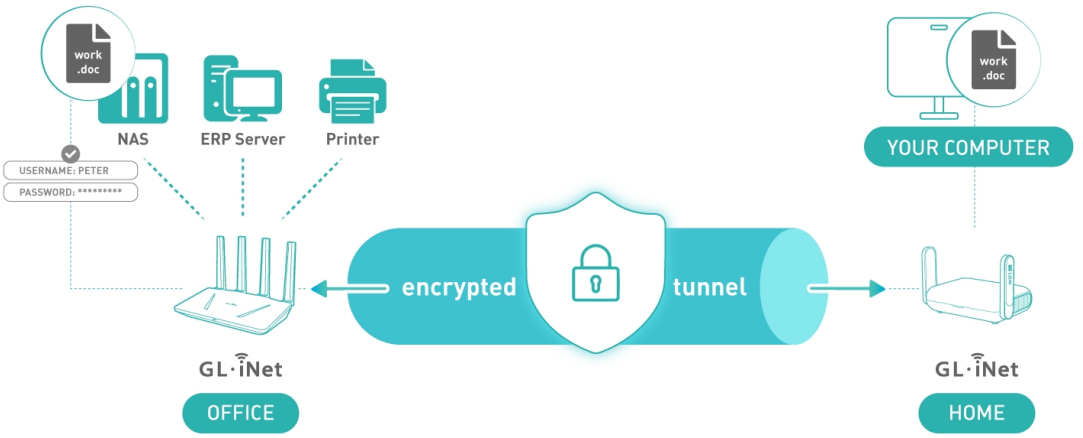
2. **Accès aux contenus depuis le monde entier**

   Certains sites limitent l’accès selon votre localisation. Un VPN peut permettre de lever ces restrictions lorsque cela est nécessaire. En vous connectant à différents serveurs tiers, vous obtenez des adresses IP différentes pour naviguer ou accéder aux sites soumis à des restrictions géographiques.



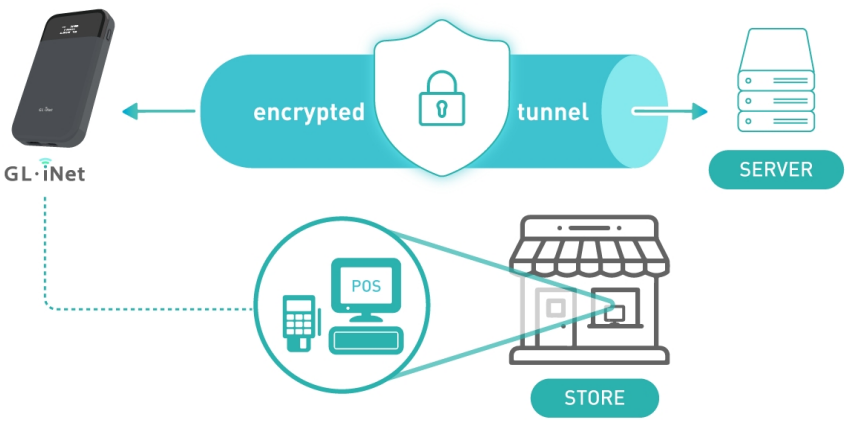
3. **Sécurité des données des petites entreprises**

   De nombreuses personnes travaillent dans des espaces de coworking ou des cafés et utilisent le Wi-Fi public gratuit. Ces réseaux sont exposés aux cyberattaques. En configurant votre routeur de voyage comme client VPN, vous disposez d'une connexion sécurisée pour travailler où que vous soyez.



4. **Sécurisation des paiements**

   Les petits commerçants traitent les données de paiement de leurs clients lors des transactions sur place. Avec un routeur VPN, leurs terminaux de paiement transmettent les informations de carte bancaire par un tunnel VPN chiffré pour sécuriser les paiements.



Chapitre 9

Tableau de bord VPN

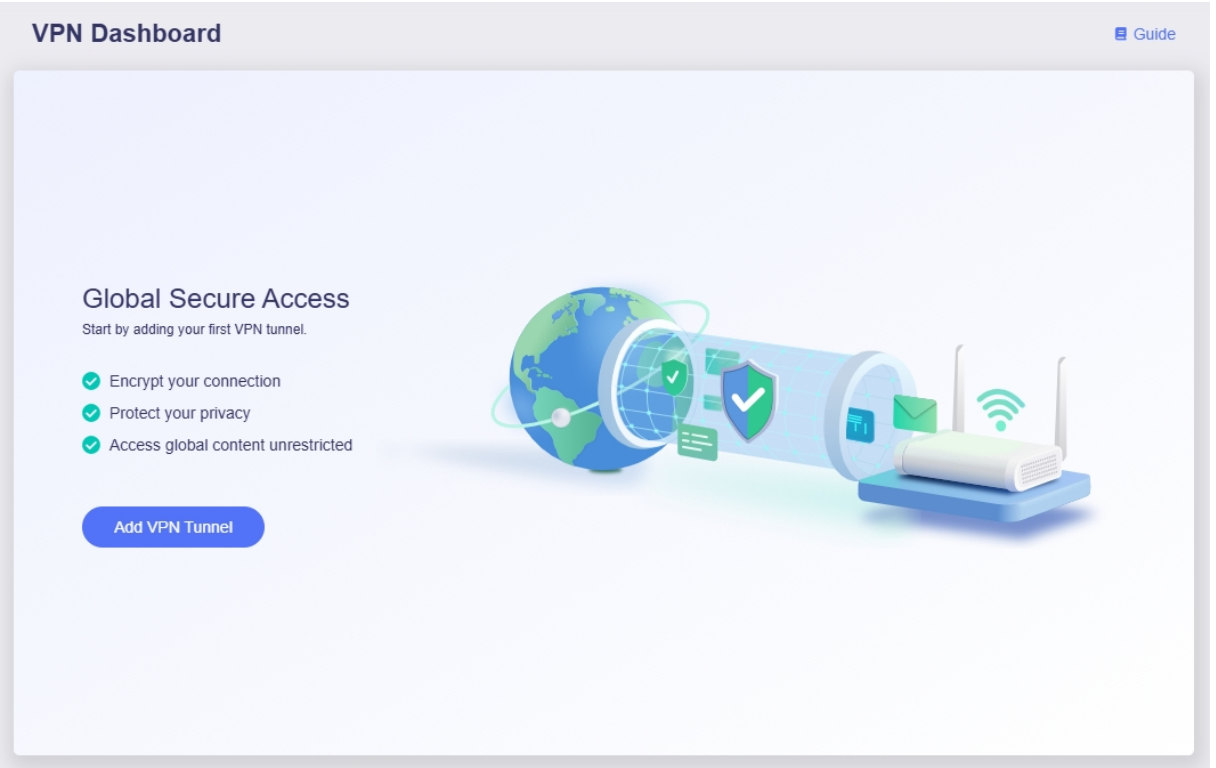
Ce chapitre explique comment gérer les connexions VPN depuis l’interface d’administration Web.

Connectez-vous à l'interface d'administration Web du routeur et ouvrez **VPN** > **Tableau de bord VPN (VPN Dashboard)**.

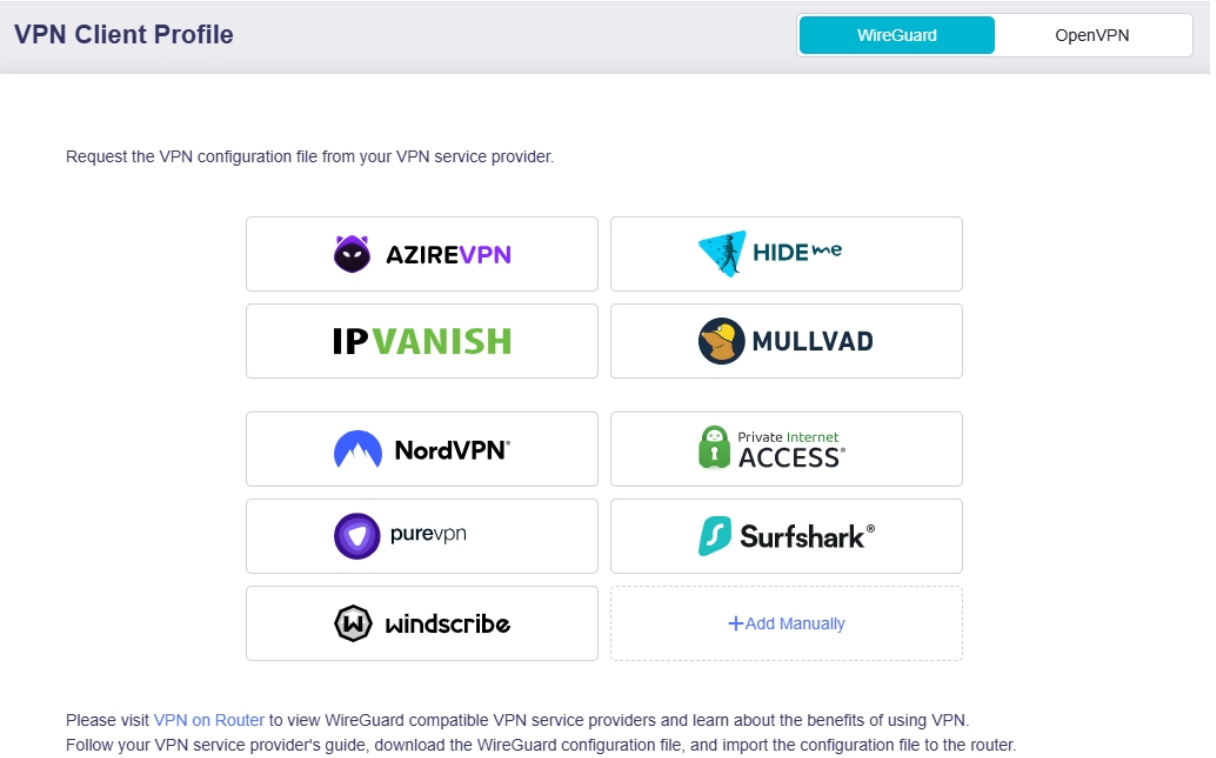
Le tableau de bord VPN affiche les détails de la connexion VPN : règles de routage, serveur connecté, statistiques de trafic, IP virtuelle du client et journal de connexion. Il permet aussi de configurer des paramètres avancés, comme le Kill Switch VPN, le masquage IP et la MTU.

9.1 Importation d'un profil VPN

À la première ouverture de cette page, si aucun tunnel n'a été créé, la page se présente comme ci-dessous. Cliquez sur **Ajouter un tunnel VPN (Add VPN Tunnel)** pour commencer.



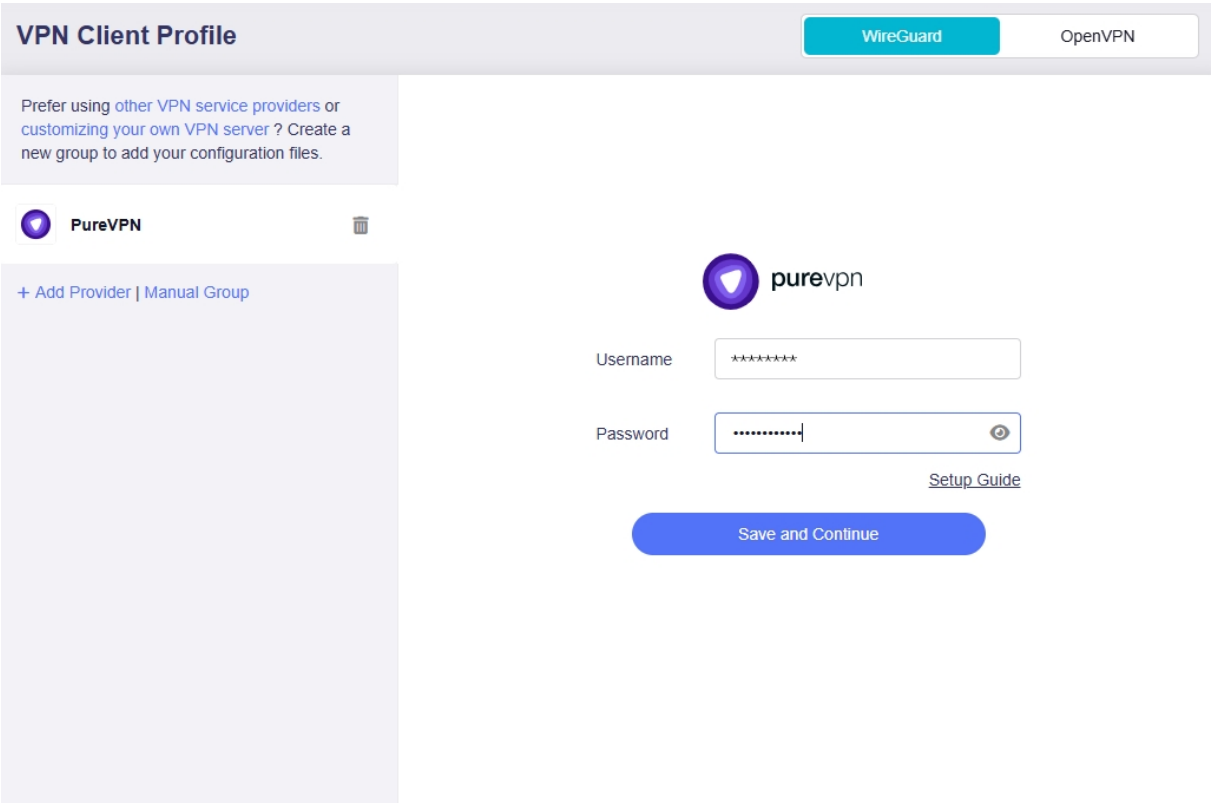
La page **Profil du client VPN (VPN Client Profile)** s'ouvre. Choisissez un fournisseur VPN et connectez-vous.



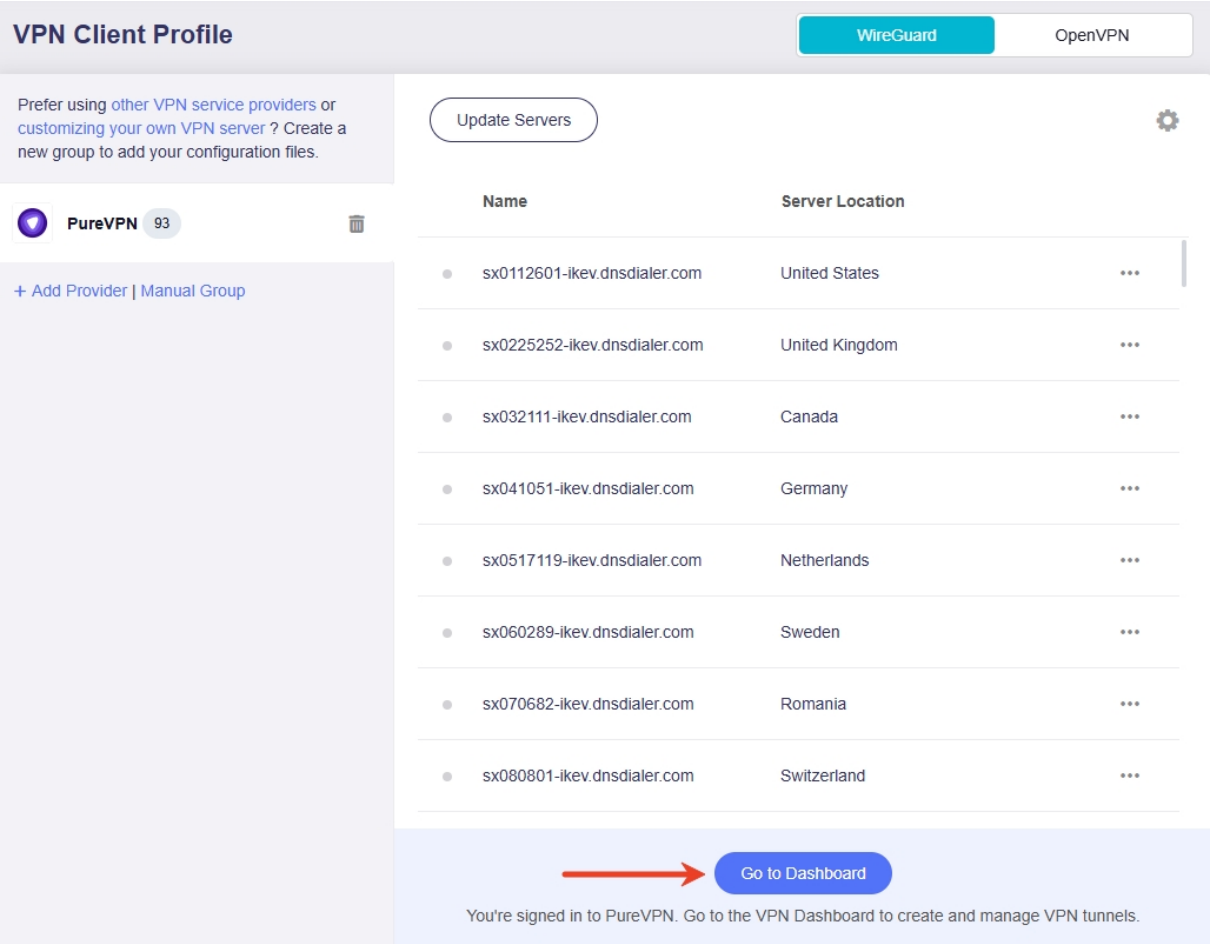
Conseils :

1. Les fournisseurs VPN affichés sont intégrés à l'interface Web des routeurs GL.iNet. Avec un abonnement actif, il suffit de saisir vos identifiants pour vous connecter et obtenir les fichiers de configuration VPN.
2. Si vous êtes abonné à un autre fournisseur VPN ou souhaitez importer vos propres configurations VPN, cliquez sur **Ajouter manuellement (Add Manually)** et importez-les.

L'exemple utilise PureVPN. Cliquez sur PureVPN et connectez-vous avec des identifiants valides.



Une liste de profils VPN s’affiche, comme ci-dessous. Cliquez sur **Accéder au tableau de bord (Go to Dashboard)** en bas pour ouvrir le tableau de bord VPN et configurer votre tunnel et votre politique VPN.



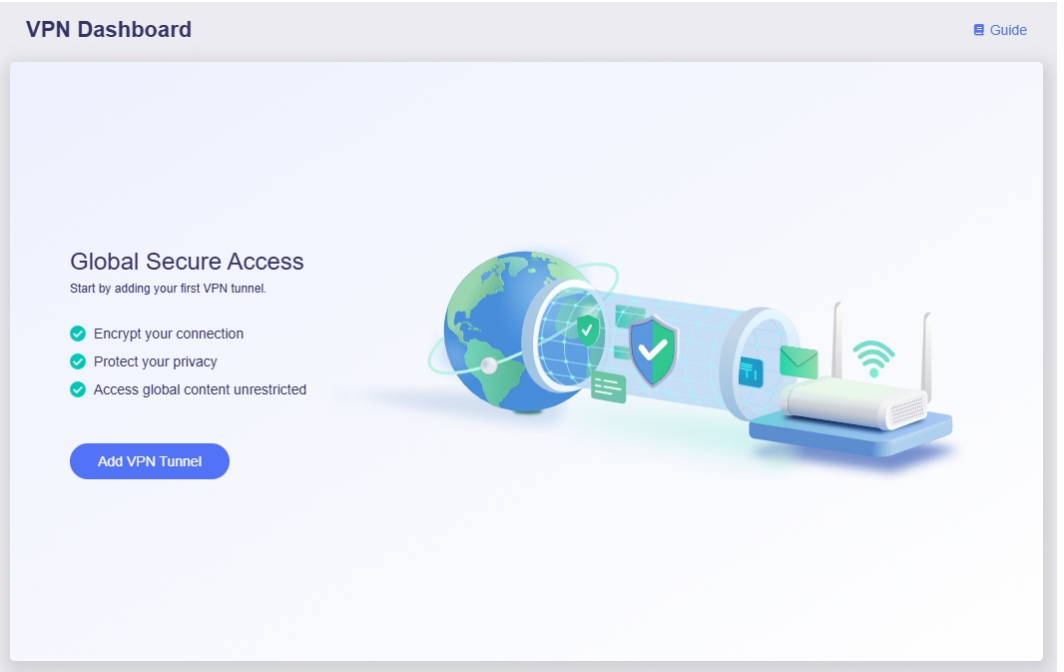
Conseil : certains fournisseurs VPN vous demandent de choisir un protocole VPN ou des serveurs/villes avant d'afficher la liste des profils.

9.2 Ajout d’un tunnel VPN

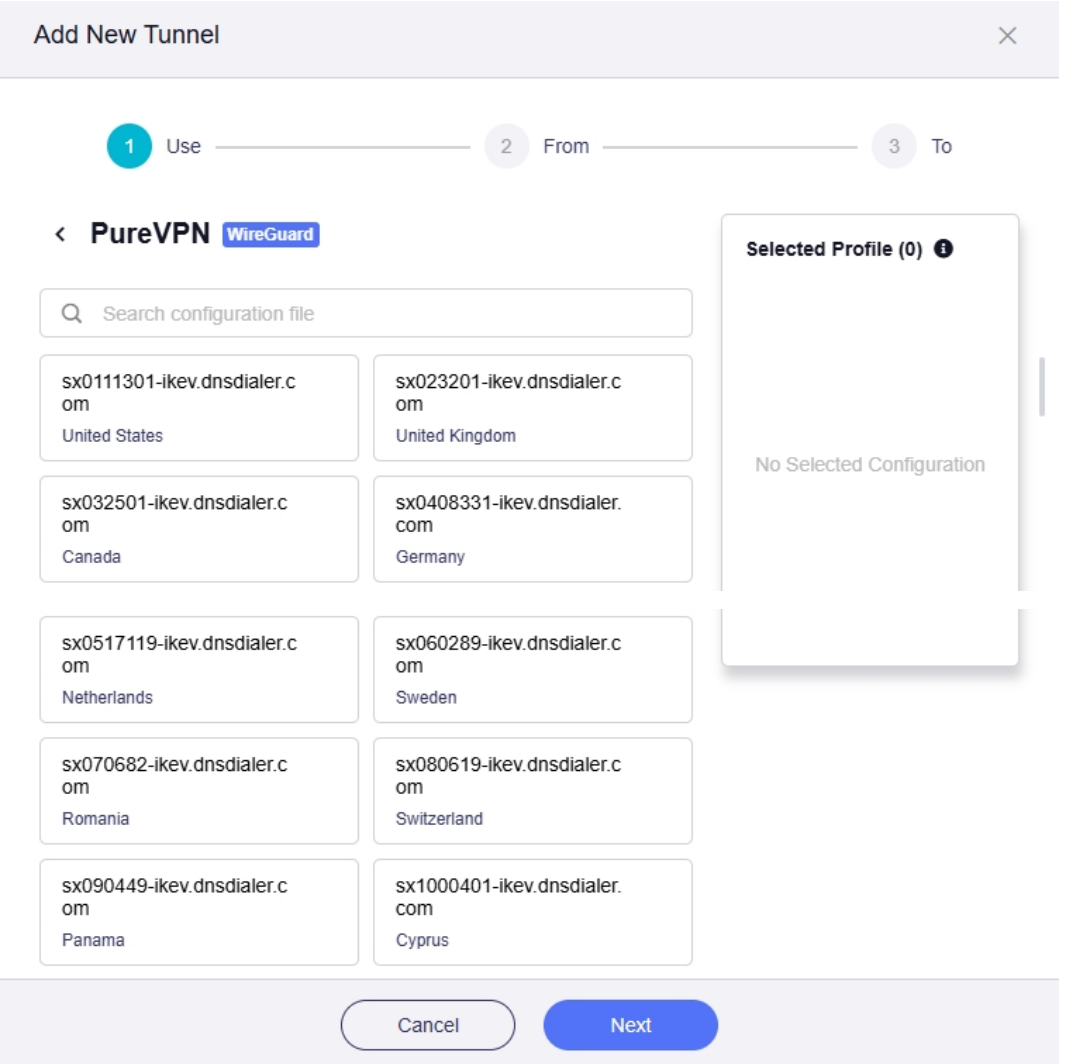
9.2.1 Procédure générale

Suivez les étapes ci-dessous pour ajouter un tunnel VPN et configurer les politiques VPN. Consultez les exemples de configuration si nécessaire.

1. Dans le tableau de bord VPN, cliquez sur **Ajouter un tunnel VPN (Add VPN Tunnel)**. Un assistant de configuration s’ouvre à droite.



2. Sélectionnez un ou plusieurs profils. Ajustez leur priorité à droite si nécessaire, puis cliquez sur **Suivant (Next)**.



Remarque : si plusieurs profils sont sélectionnés, le tunnel essaie chacun d'eux par ordre de priorité jusqu'à établir une connexion. Si tous les profils d'un tunnel échouent, le système décide s'il doit utiliser le réseau local du routeur (WAN) selon l'état du Kill Switch dans les paramètres Options du tunnel (Tunnel Options) et Tout autre trafic (All Other Traffic).

3. Sélectionnez la source des clients, puis cliquez sur **Suivant (Next)**. Quatre options sont proposées :
   - **Tous les clients (All Clients)** : le trafic de tous les appareils correspond à cette règle.
   - **Types de connexion spécifiés (Specified Connection Types)** : le trafic des types de connexion sélectionnés, par exemple sous-réseau LAN, Passerelle transparente ou Réseau invité, correspond à cette règle.

- **Appareils spécifiés (Specified Devices)** : le trafic des appareils sélectionnés, identifiés par leur adresse MAC, correspond à cette règle.
- **Exclure les appareils spécifiés (Exclude Specified Devices)** : le trafic des appareils sélectionnés, identifiés par leur adresse MAC, ne correspond pas à cette règle.

4. Sélectionnez la destination, puis cliquez sur **Appliquer (Apply)**. Trois options sont proposées :
   - **Toutes les destinations (All Targets)** : le trafic correspondant à cette règle est acheminé vers toutes les destinations.
   - **Liste de domaines/IP spécifiés (Specified Domain / IP List)** : le trafic correspondant à cette règle est acheminé vers les domaines ou adresses IP spécifiés. Saisissez-les manuellement.
   - **Exclure la liste de domaines/IP spécifiés (Exclude specified Domain / IP List)** : le trafic correspondant à cette règle n'est pas acheminé vers les domaines ou adresses IP spécifiés. Saisissez-les manuellement.
5. Le tunnel VPN est ajouté. Le **tableau de bord VPN (VPN Dashboard)** s'ouvre. Ajoutez d'autres tunnels si nécessaire. Pour votre sécurité, vérifiez l'état du Kill Switch dans Tout autre trafic (All Other Traffic) et **Options du tunnel (Tunnel Options)** avant d'activer le tunnel VPN.

9.2.2 Exemples de configuration

Voici deux exemples courants de configuration de politiques VPN, avec des instructions détaillées.

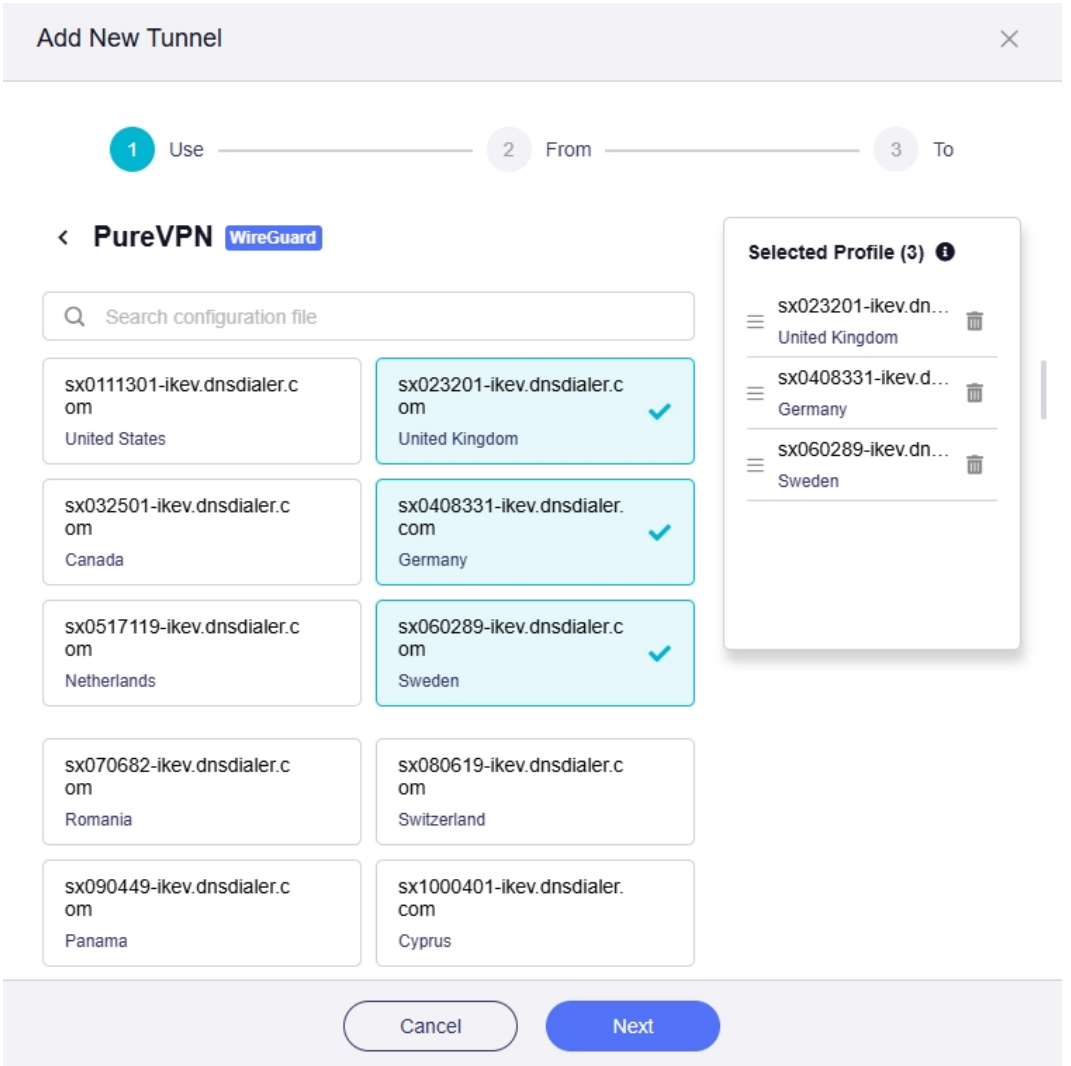
Exemple 1 : acheminer uniquement le trafic de certains appareils via le VPN

Besoins :

1. Seuls certains appareils connectés à ce routeur accèdent à Internet via le VPN. Tous les autres utilisent le WAN local.
2. Les appareils sélectionnés doivent utiliser exclusivement le VPN. Si celui-ci se déconnecte de manière inattendue, leur accès Internet est bloqué pour éviter les fuites DNS et le suivi de leur adresse IP.

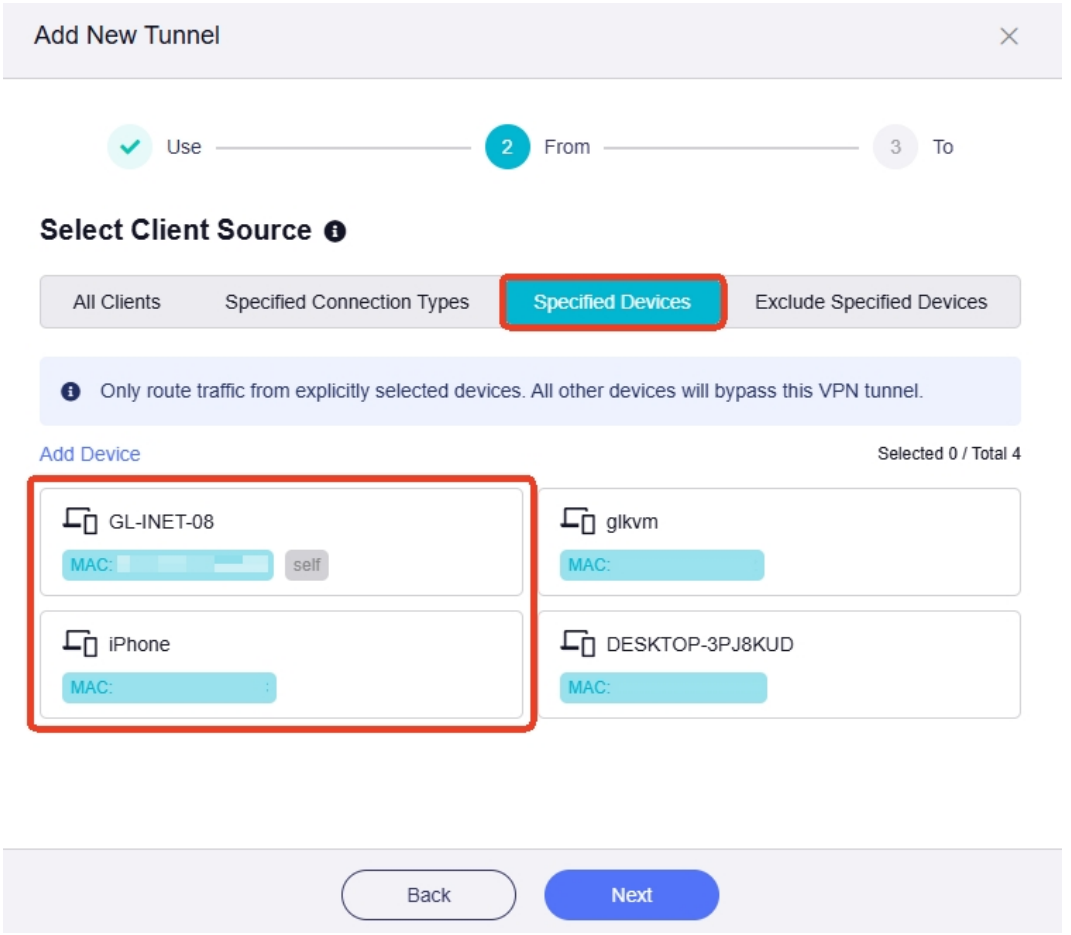
Étapes de configuration :

1. Sélectionnez le profil VPN.
   Si vous vous êtes connecté à un service VPN intégré ou avez importé un fichier de configuration, les profils disponibles apparaissent ici. Sinon, ouvrez **Profil du client VPN (VPN Client Profile)** pour vous connecter avec vos identifiants ou importer manuellement un fichier de configuration.
   L'exemple utilise PureVPN. Sélectionnez un ou plusieurs profils et ajustez leur priorité à droite si nécessaire.



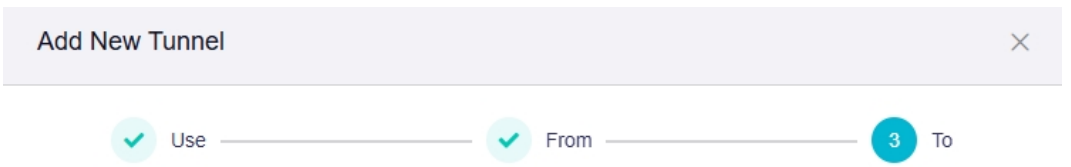
2. Sélectionnez la source des clients.

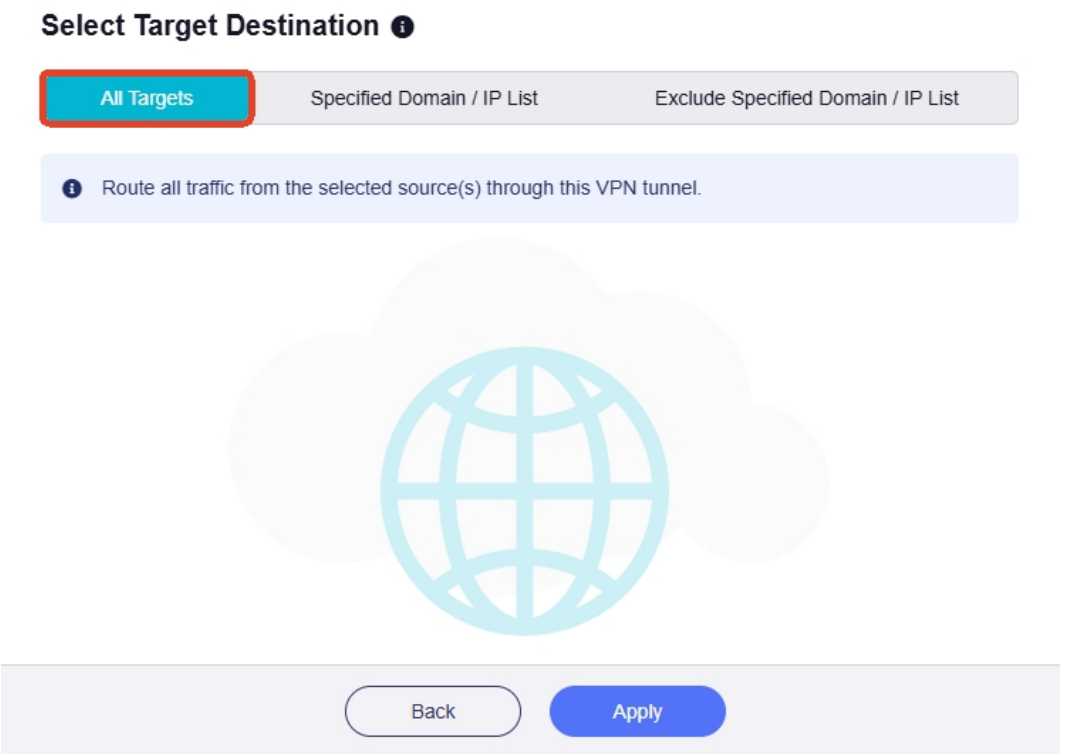
   Ouvrez l'onglet **Appareils spécifiés (Specified Devices)**, sélectionnez les appareils qui utiliseront le VPN, puis cliquez sur **Suivant (Next)**.



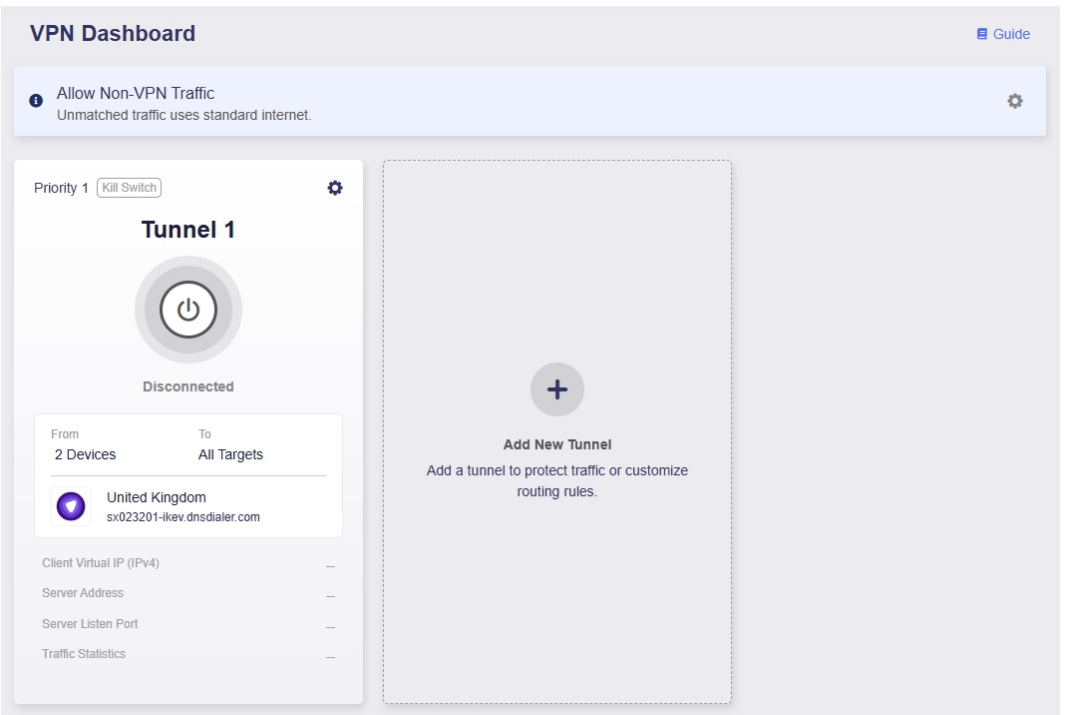
3. Sélectionnez la destination.

Ouvrez l'onglet **Toutes les destinations (All Targets)**, choisissez-le comme destination du trafic, puis cliquez sur **Appliquer (Apply)**.

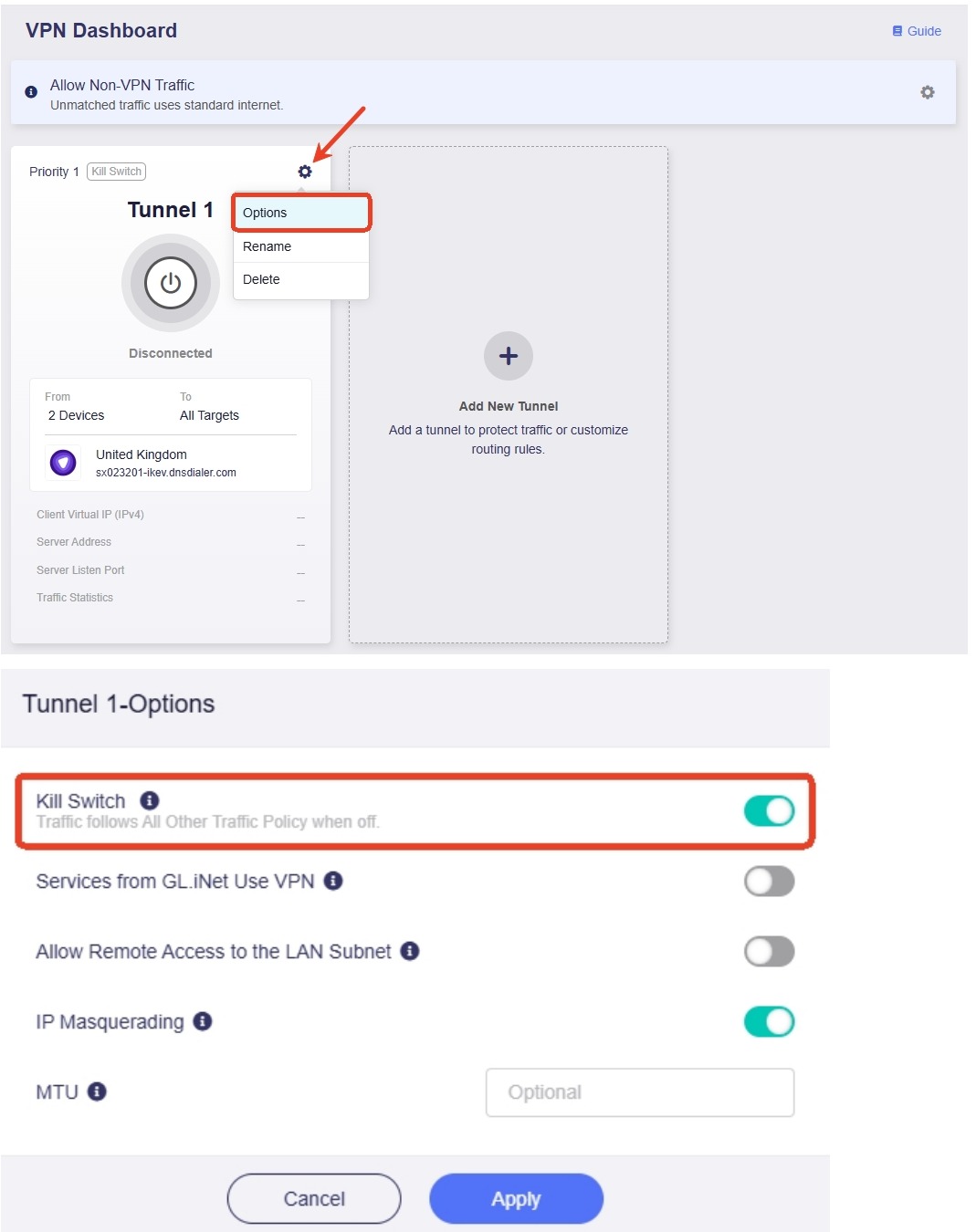




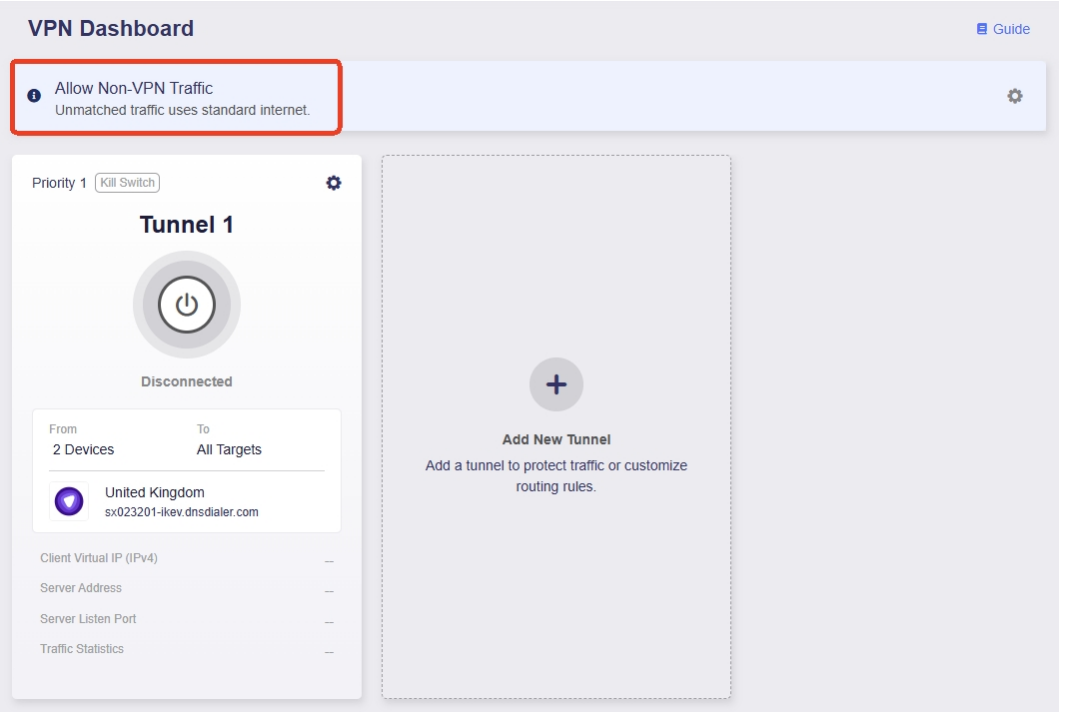
4. Le tableau de bord VPN s'ouvre. Le tunnel VPN a été ajouté, comme ci-dessous.



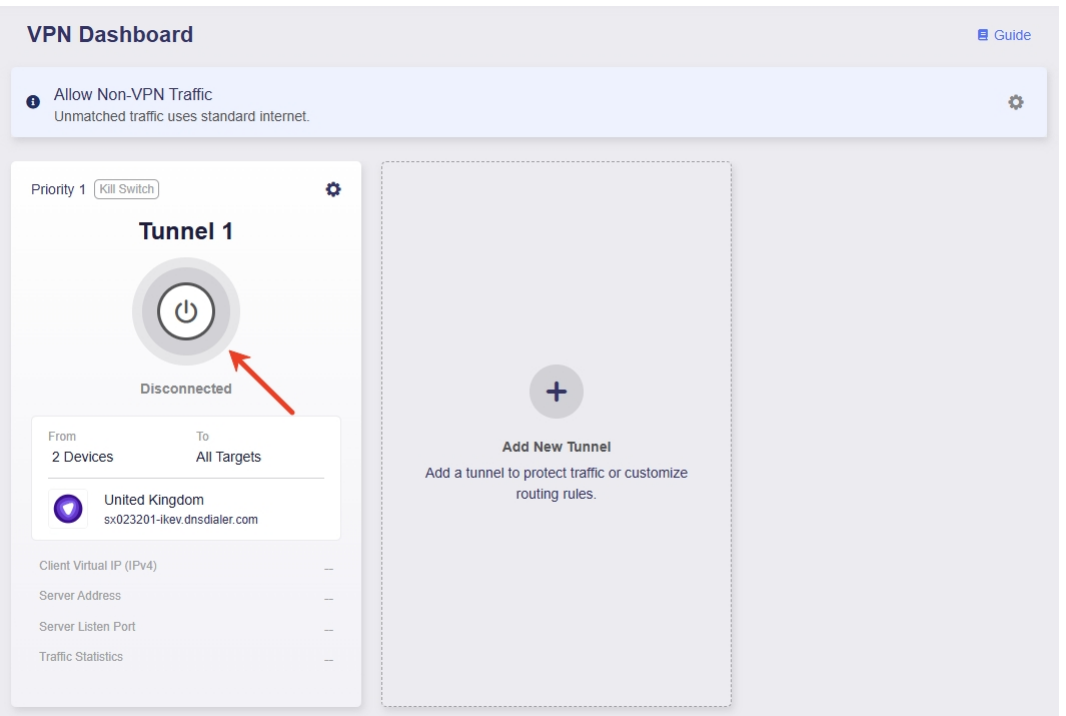
5. Vérifiez que le **Kill Switch** de ce tunnel est activé. Si le VPN se déconnecte de manière inattendue, l'accès Internet du trafic correspondant à ce tunnel est bloqué pour éviter les fuites DNS et le suivi des adresses IP.



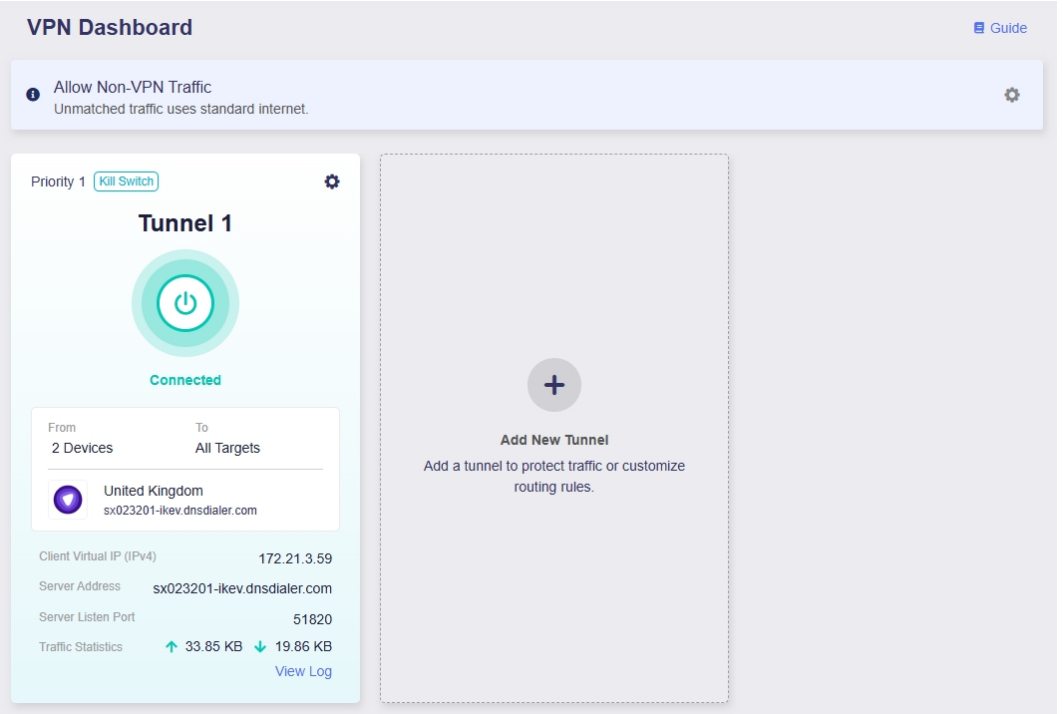
6. Vérifiez que **Autoriser le trafic hors VPN (Allow Non-VPN Traffic)** est activé. Cette option est activée par défaut pour que le trafic ne correspondant pas au tunnel VPN puisse accéder à Internet via le WAN local.



7. Cliquez sur le bouton central pour activer ce tunnel.



8. Une fois la connexion établie, la page affiche les détails de la connexion VPN : politique VPN, statistiques de trafic, adresse du serveur, port d’écoute et adresse IP virtuelle.



Désormais, seuls les deux appareils sélectionnés accèdent à Internet via le VPN. Si celui-ci se déconnecte de manière inattendue, leur accès Internet est bloqué pour éviter les fuites DNS et le suivi de leur adresse IP. Tous les autres appareils utilisent le WAN local.

Exemple 2 : utiliser le VPN 1 pour certains sites Web sur tous les appareils et acheminer tout le reste du trafic via le VPN 2

Besoins :

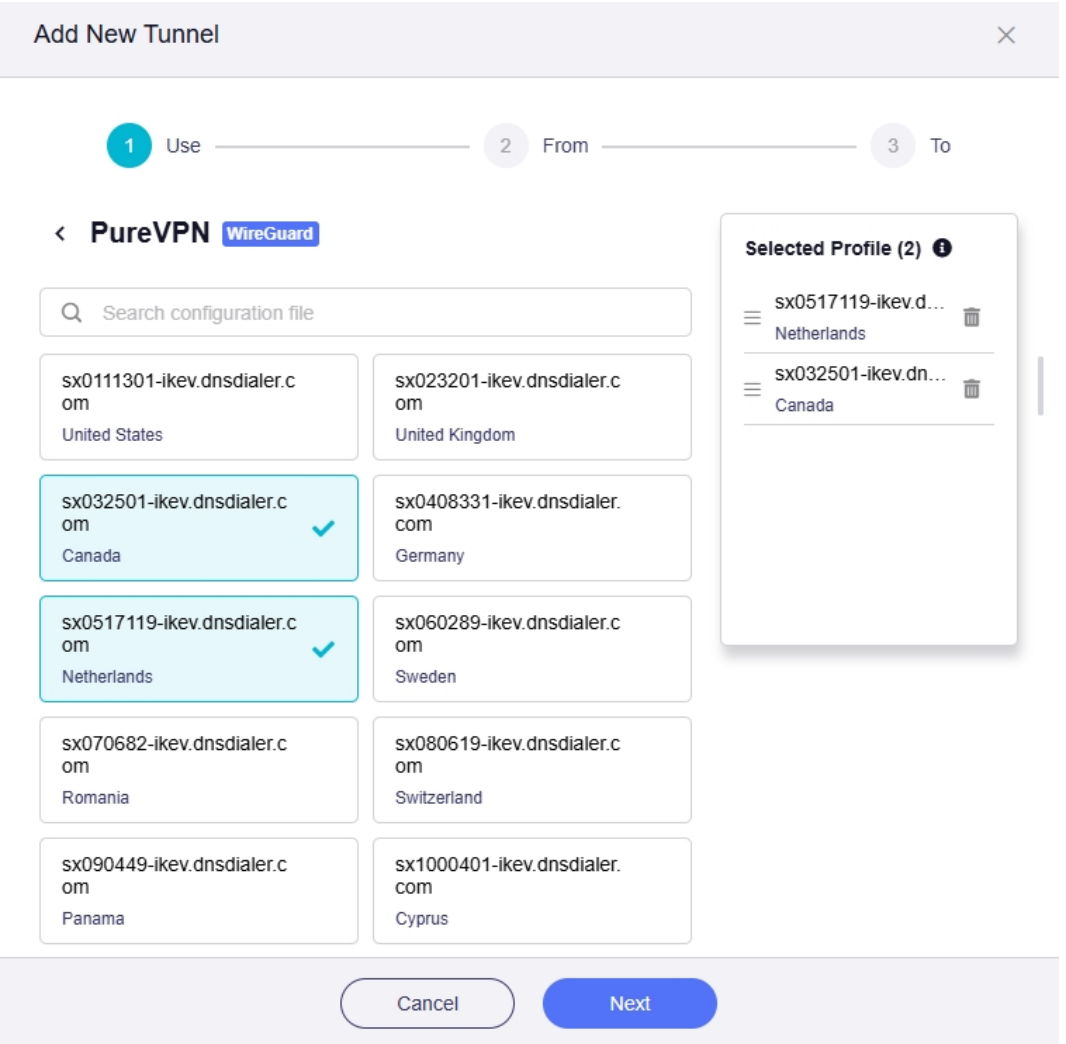
1. Tous les appareils utilisent le tunnel VPN 1 pour accéder aux domaines de certains réseaux sociaux et services de streaming, et le tunnel VPN 2 pour tous les autres accès à Internet.
2. Si les tunnels VPN se déconnectent de manière inattendue, l'accès Internet de tous les appareils est bloqué pour éviter les fuites DNS et le suivi de leur adresse IP.

Étapes de configuration :

1. Sélectionnez le profil VPN du tunnel 1.
   Si vous vous êtes connecté à un service VPN intégré ou avez importé un fichier de configuration, les profils disponibles apparaissent ici. Sinon, ouvrez **Profil du client VPN**

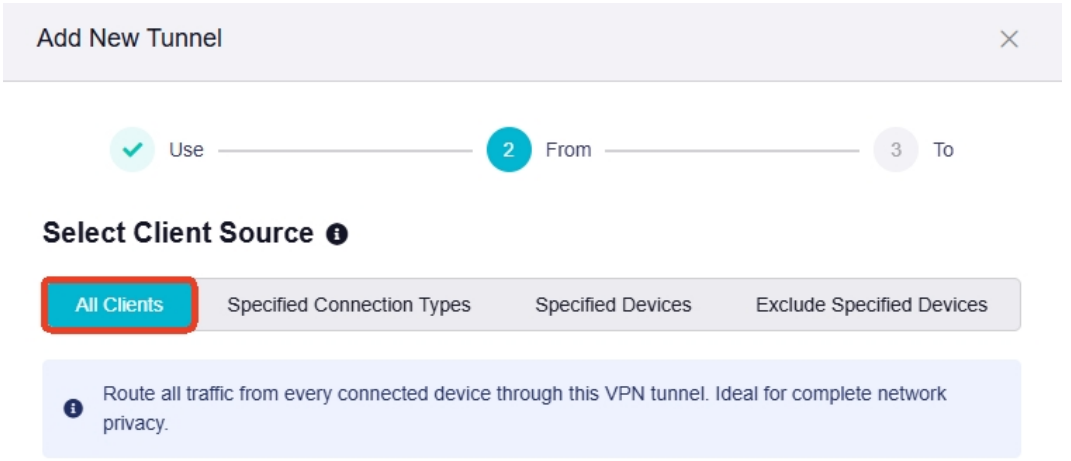
(VPN Client Profile) pour vous connecter avec vos identifiants ou importer manuellement un fichier de configuration.

L'exemple utilise PureVPN. Sélectionnez un ou plusieurs profils. Ajustez leur priorité à droite si nécessaire, puis cliquez sur **Suivant (Next)**.

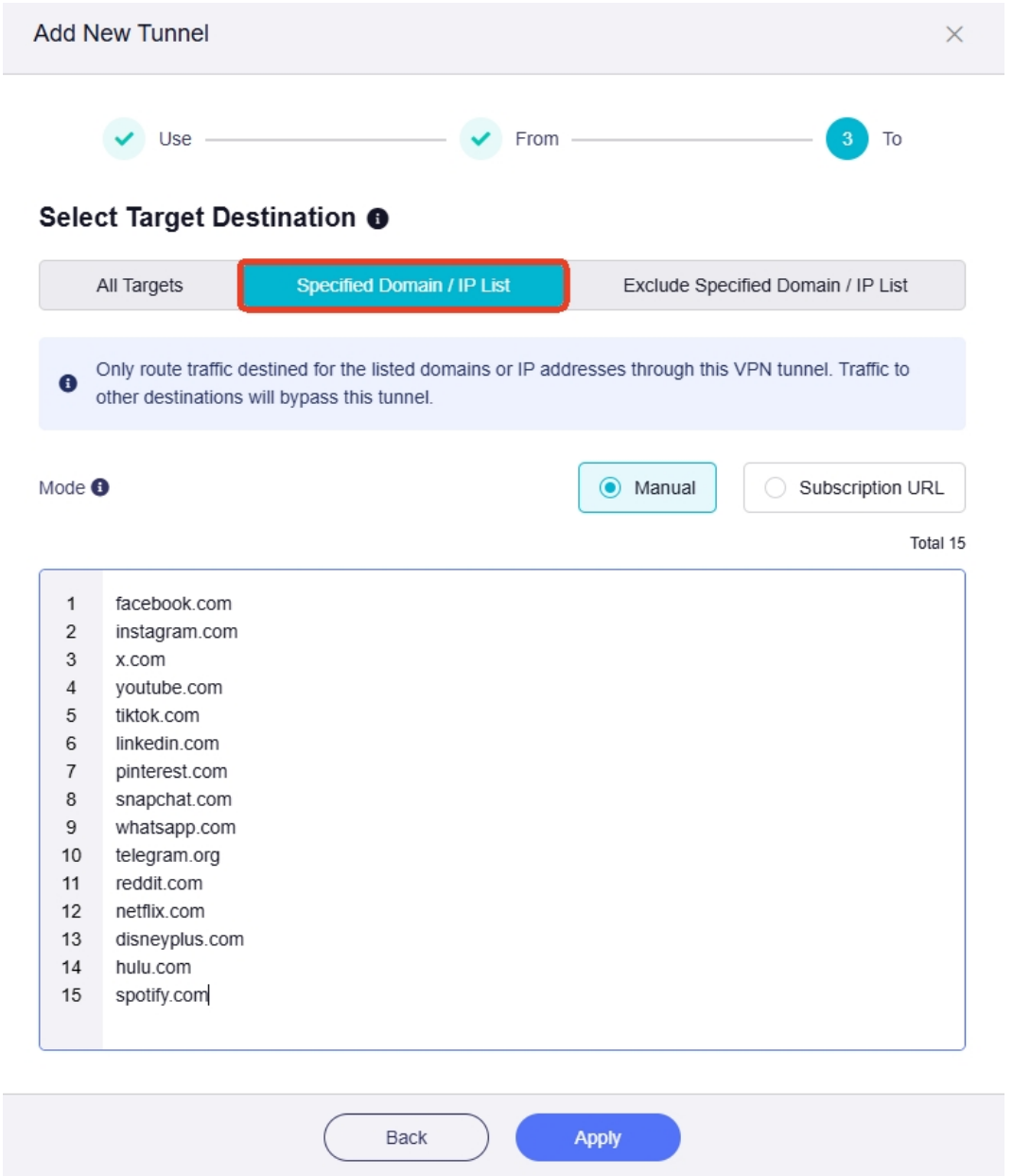


2. Sélectionnez la source des clients.

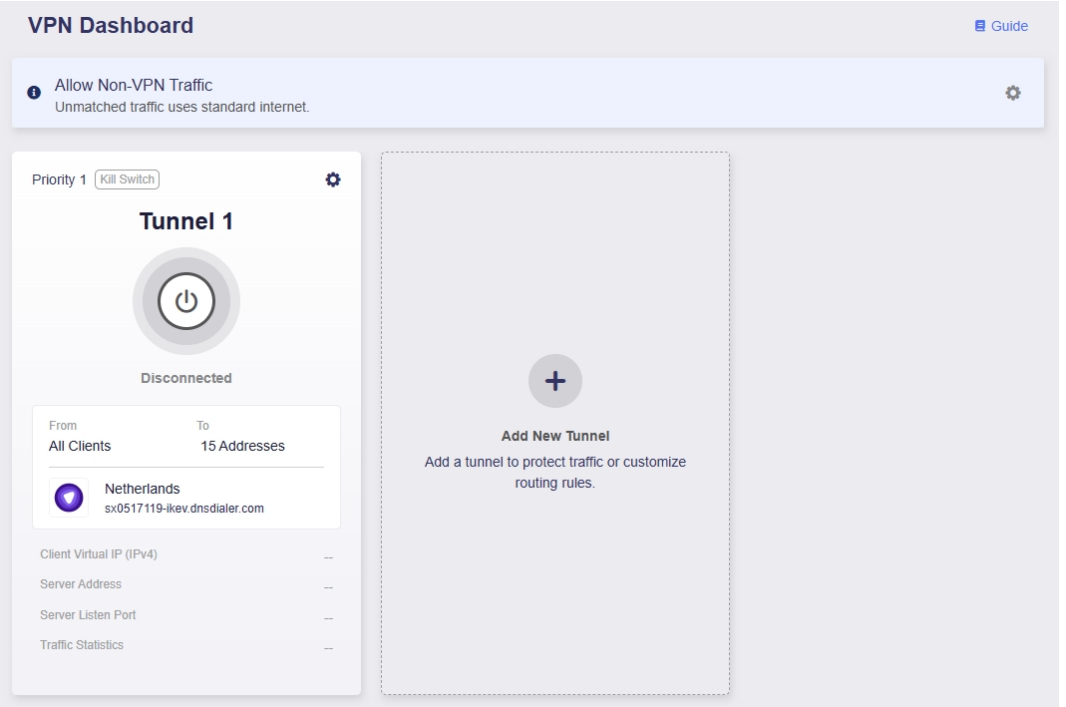
Ouvrez l'onglet **Tous les clients (All Clients)**, choisissez-le comme source des clients du tunnel 1, puis cliquez sur **Suivant (Next)**.



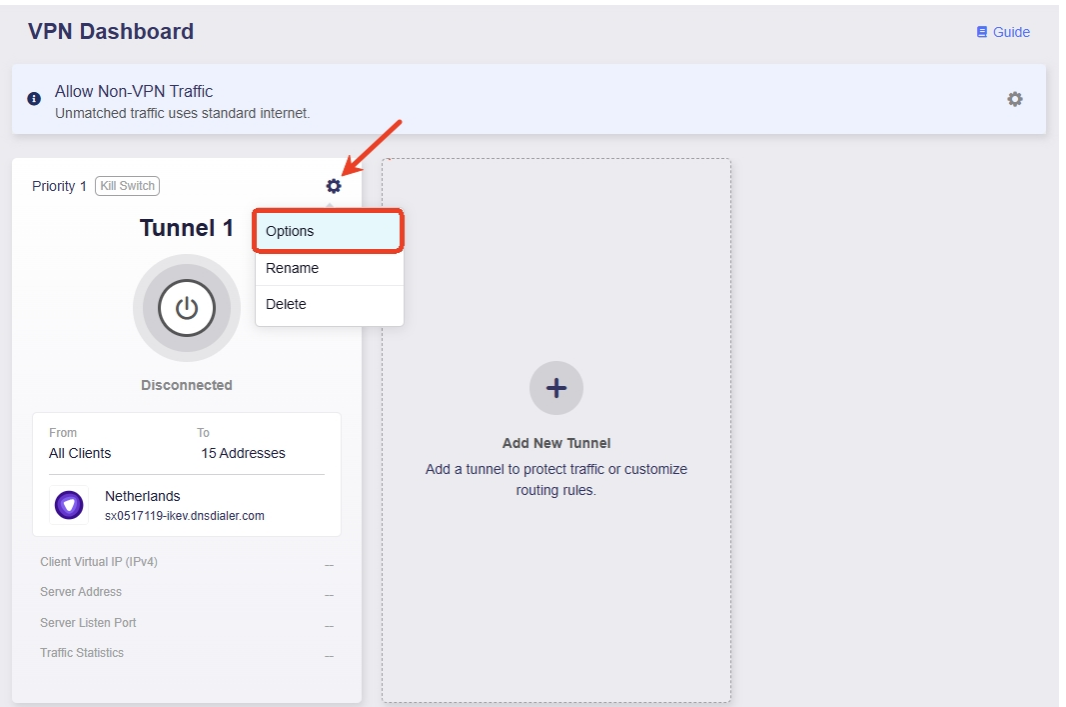
3. Sélectionnez la destination.
   Ouvrez l'onglet **Liste de domaines/IP spécifiés (Specified Domain / IP List)**, saisissez les domaines de quelques réseaux sociaux et services de streaming courants, comme ci-dessous, puis cliquez sur **Appliquer (Apply)**.

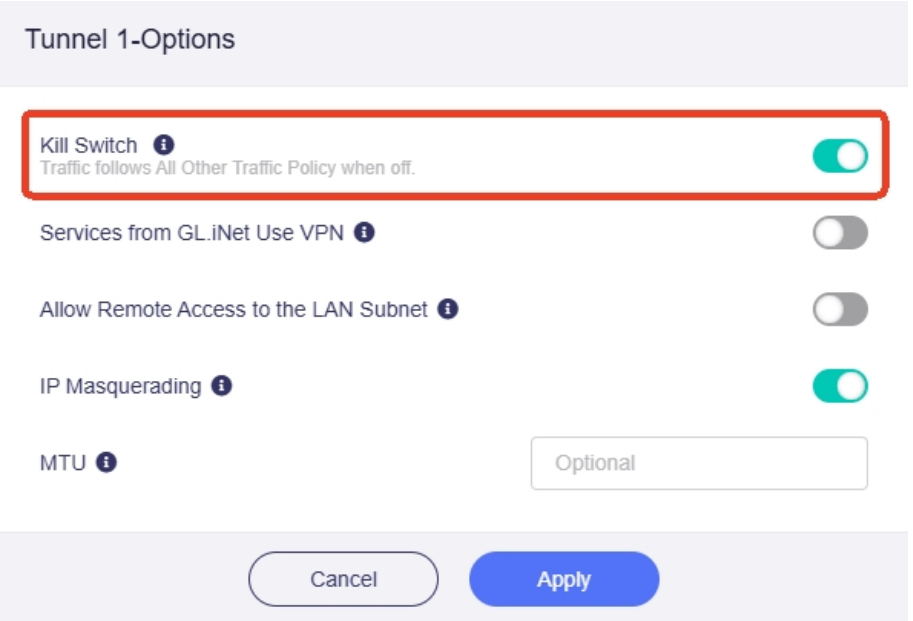


4. Le tableau de bord VPN s’ouvre. Le tunnel VPN 1 a été ajouté.

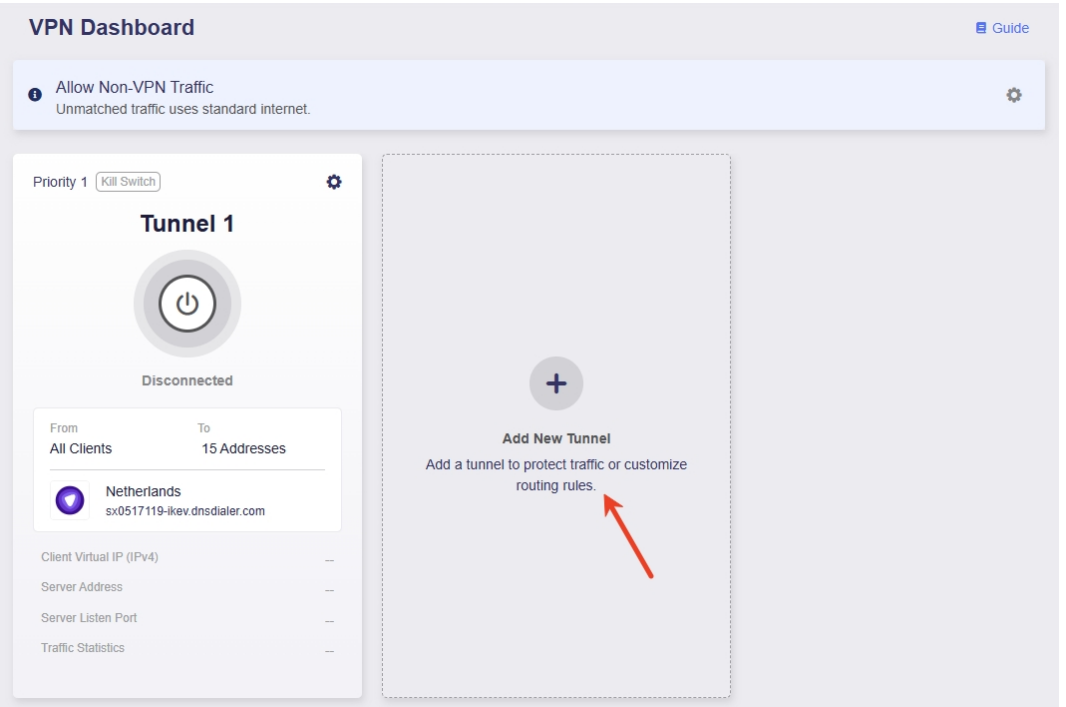


5. Vérifiez que le **Kill Switch** du tunnel 1 est activé. Si le VPN se déconnecte de manière inattendue, l'accès Internet du trafic correspondant à ce tunnel est bloqué pour éviter les fuites DNS et le suivi des adresses IP.



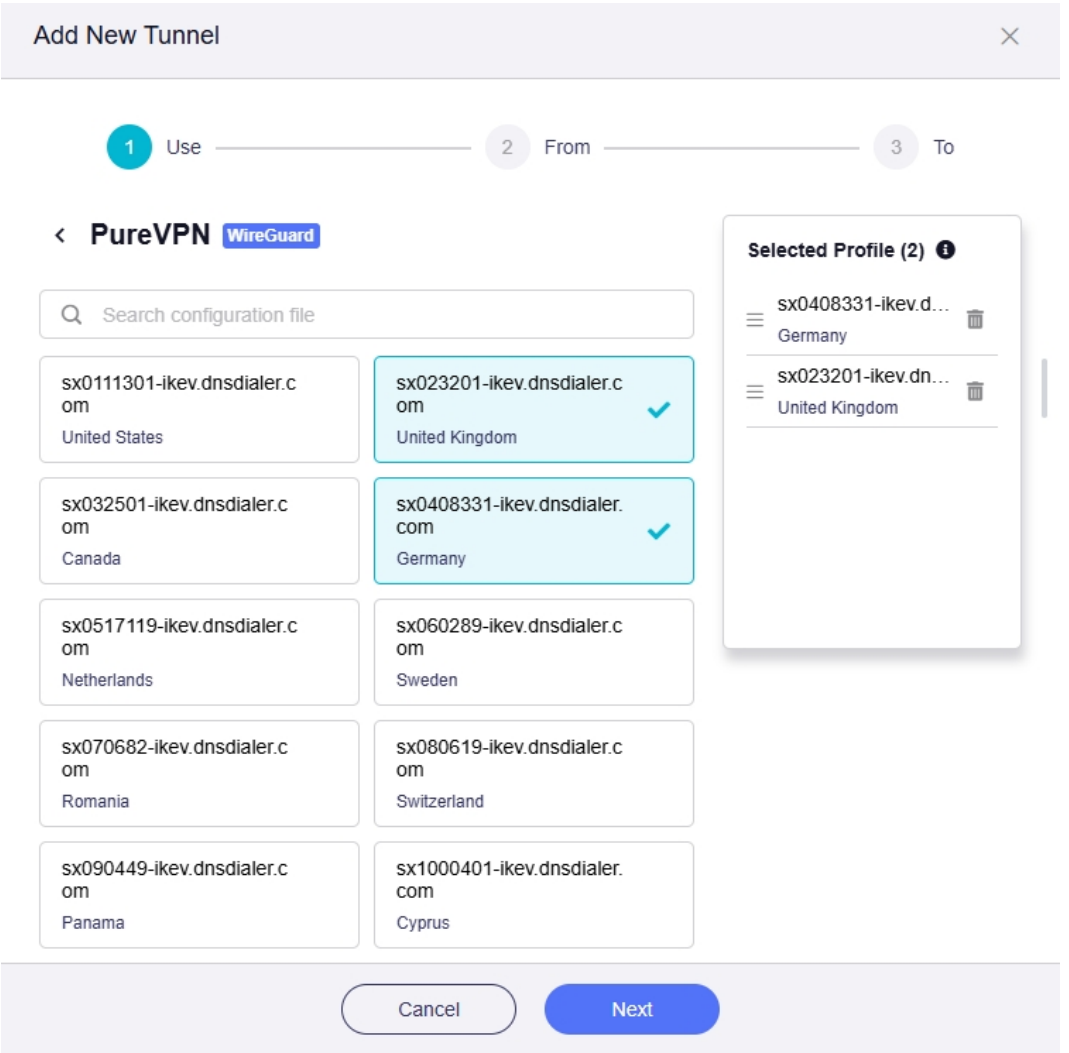


6. Cliquez sur **Ajouter un tunnel (Add New Tunnel)** pour ajouter le tunnel 2.



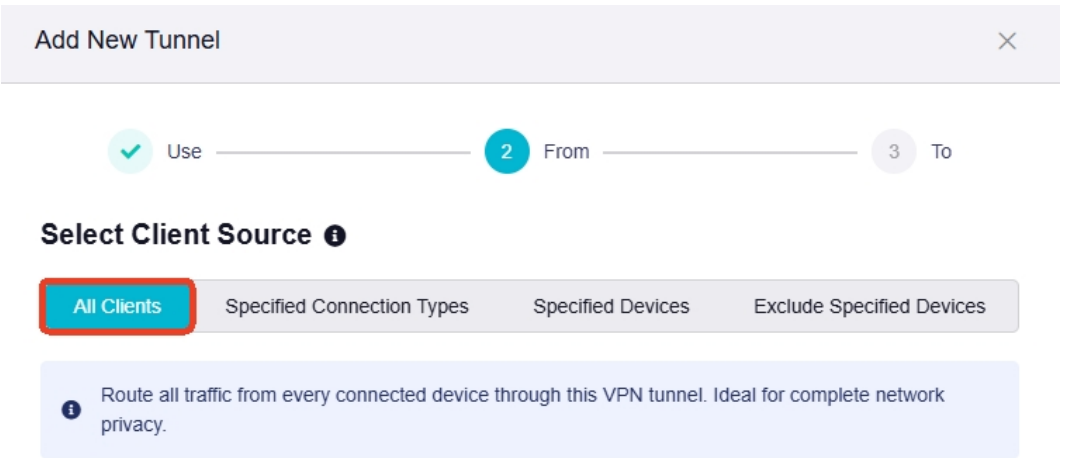
7. Sélectionnez le profil VPN du tunnel 2.

   Sélectionnez un ou plusieurs profils et ajustez leur priorité à droite si nécessaire. Cliquez ensuite sur **Suivant (Next)**.



8. Sélectionnez la source des clients.

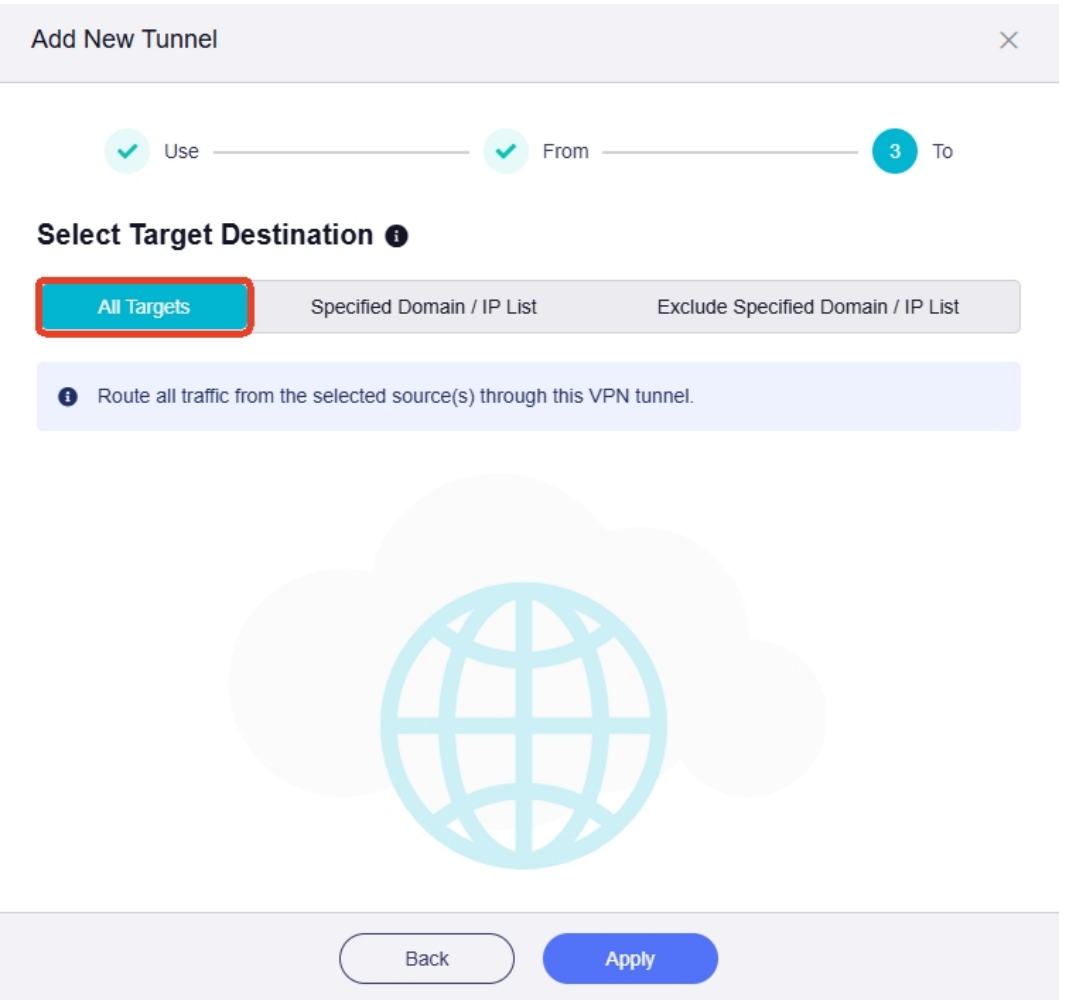
Ouvrez l'onglet **Tous les clients (All Clients)**, choisissez-le comme source des clients du tunnel 2, puis cliquez sur **Suivant (Next)**.



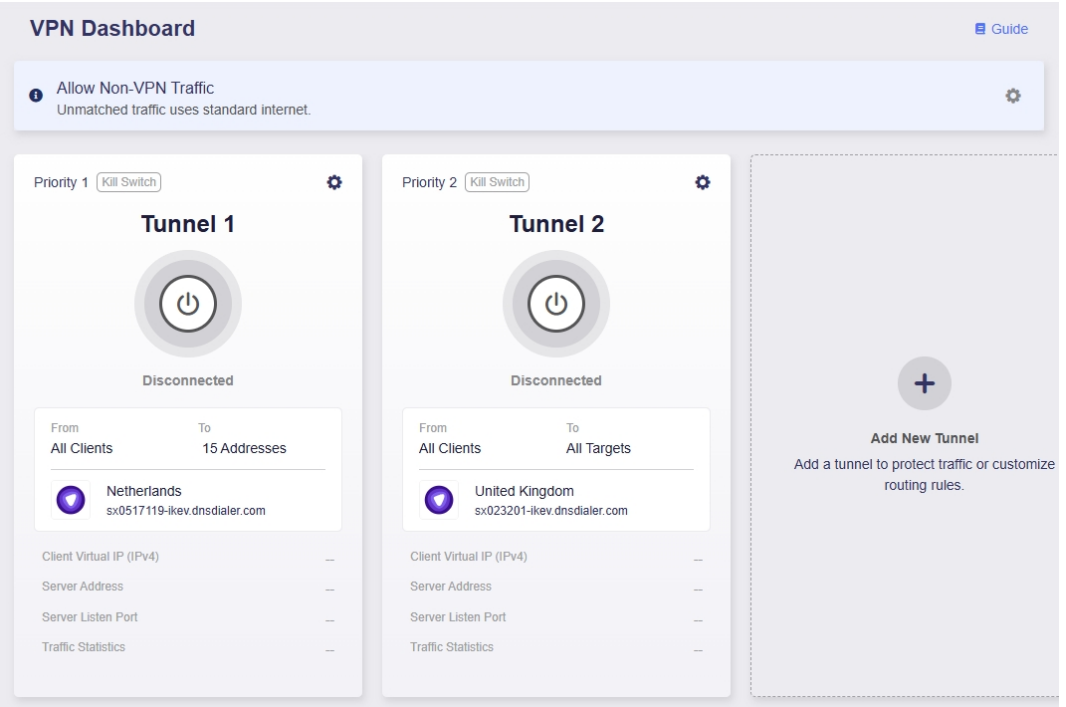


9. Sélectionnez la destination.

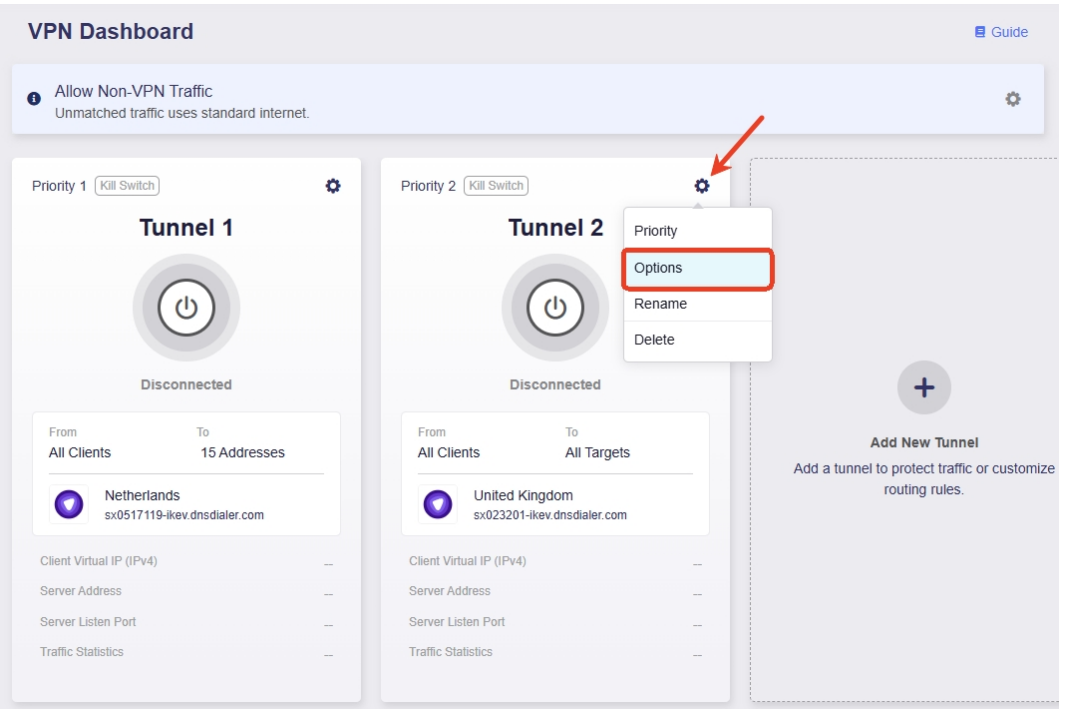
Ouvrez l'onglet **Toutes les destinations (All Targets)**, choisissez-le comme destination du trafic du tunnel 2, puis cliquez sur **Appliquer (Apply)**.

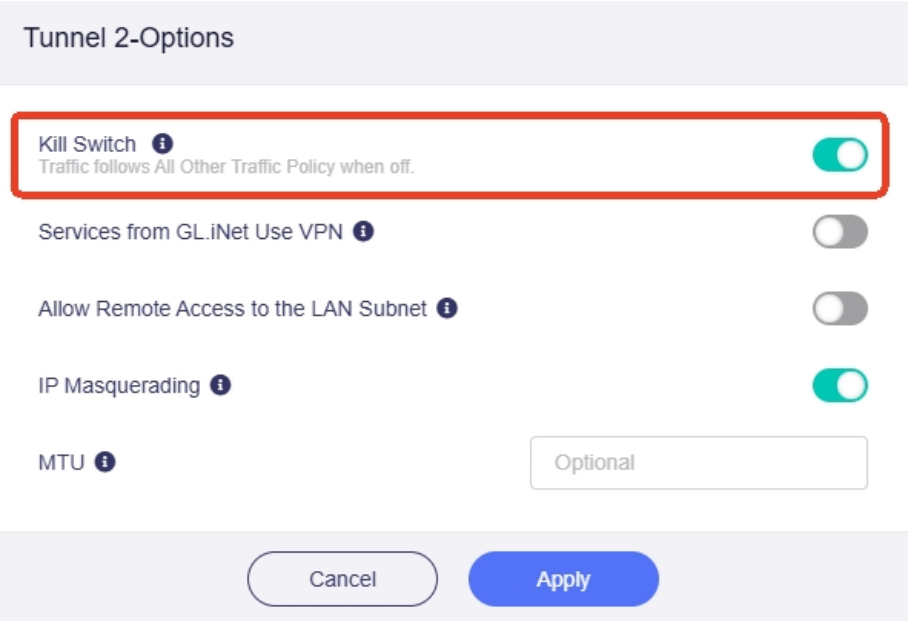


10. Le tableau de bord VPN s’ouvre. Le tunnel VPN 2 a été ajouté.

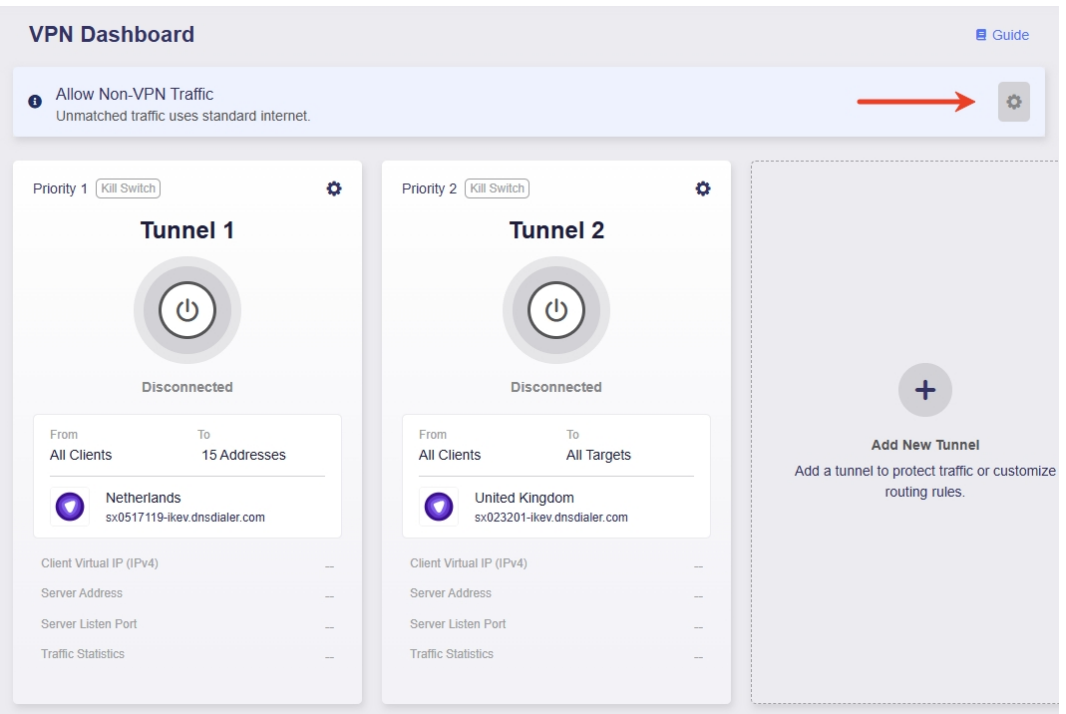


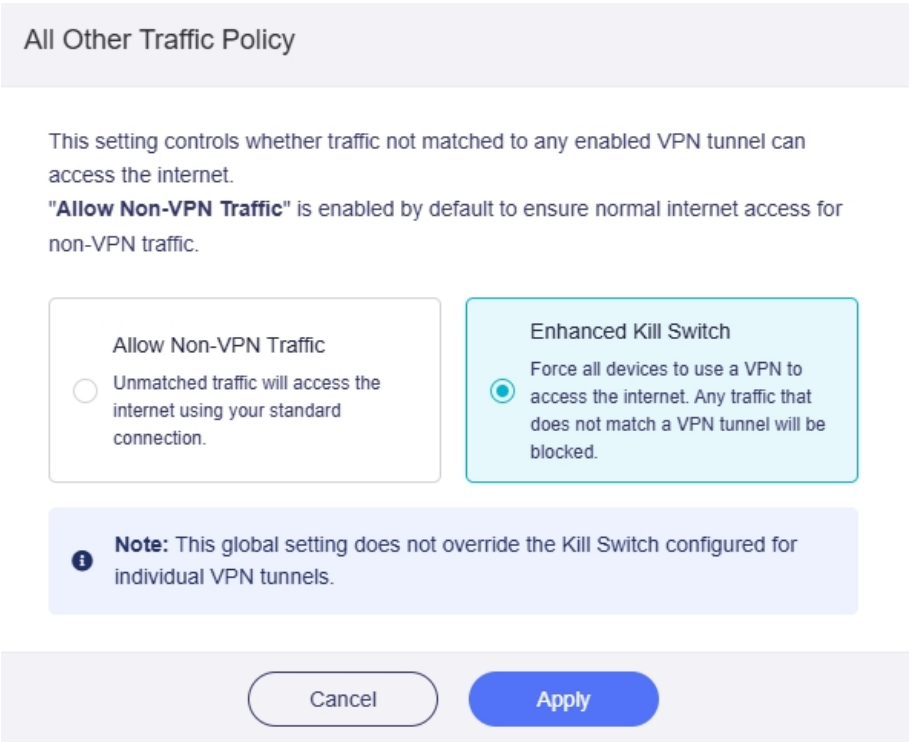
11. Vérifiez que le **Kill Switch** du tunnel 2 est activé. Si le VPN se déconnecte de manière inattendue, l’accès Internet du trafic correspondant à ce tunnel est bloqué pour éviter les fuites DNS et le suivi des adresses IP.



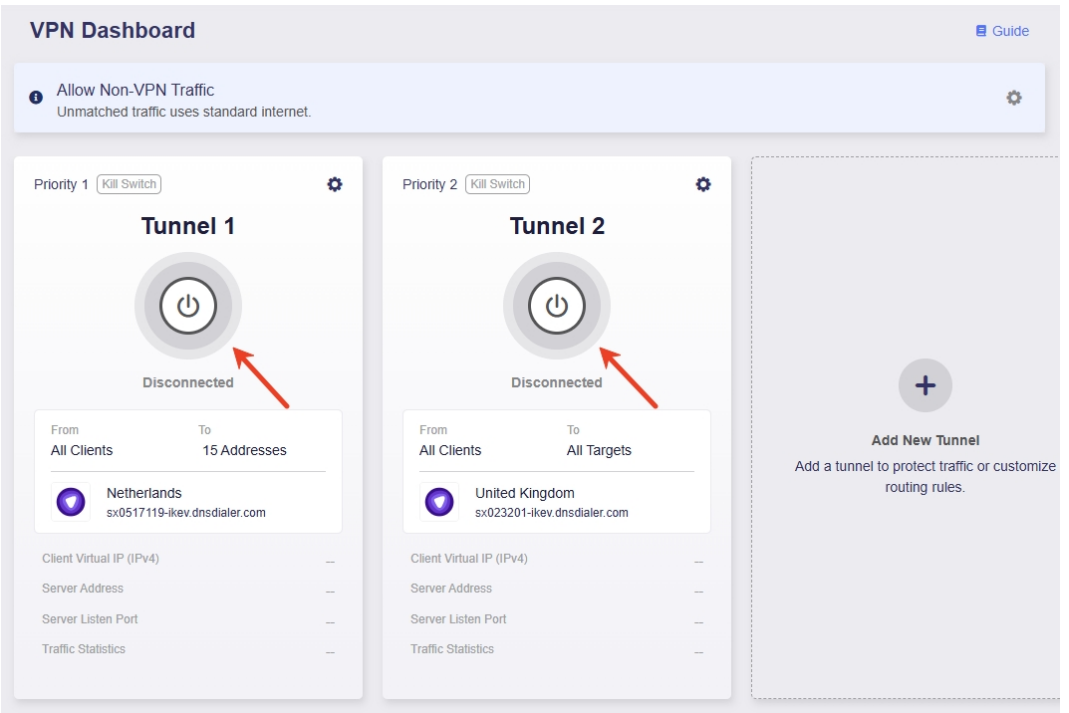


12. Cliquez sur l'engrenage dans l'angle supérieur droit pour activer le **Kill Switch renforcé (Enhanced Kill Switch)**. Ainsi, tout le trafic doit accéder à Internet via le VPN.

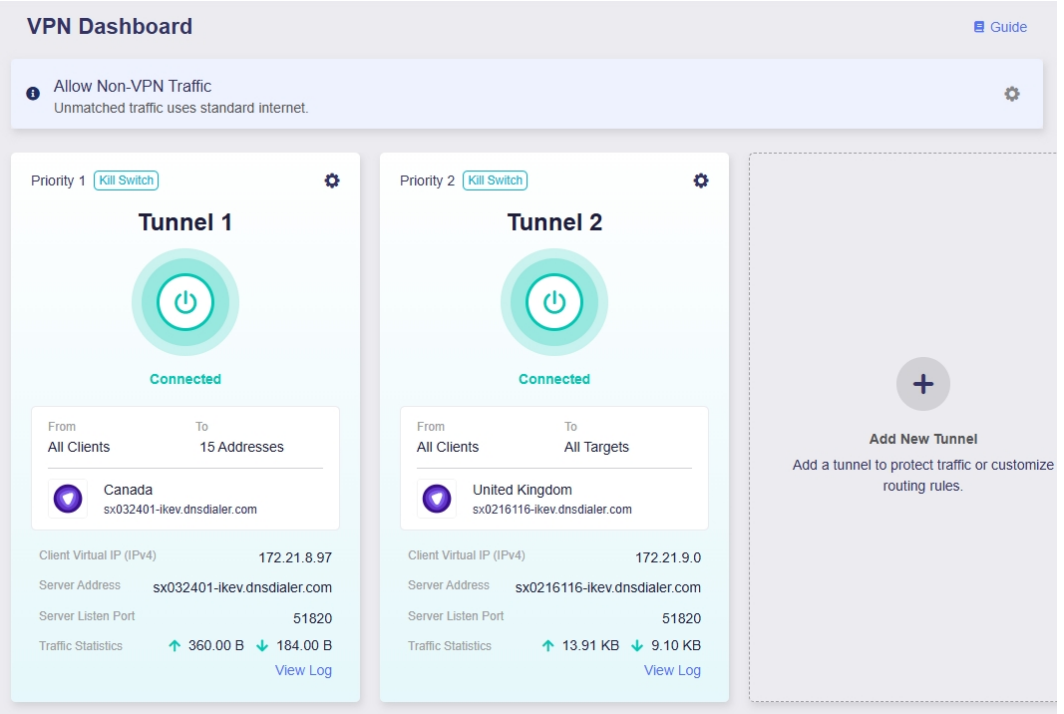




13. Cliquez sur le bouton central pour activer les tunnels 1 et 2.



14. Une fois la connexion établie, la page affiche les détails de la connexion VPN : politique VPN, statistiques de trafic, adresse du serveur, port d’écoute et adresse IP virtuelle.



Désormais, tous les appareils utilisent le tunnel VPN 1 pour accéder aux domaines spécifiés et le tunnel VPN 2 pour tous les autres accès à Internet. Si les tunnels VPN se déconnectent de manière inattendue, l’accès Internet de tous les appareils est bloqué pour éviter les fuites DNS et le suivi de leur adresse IP.

9.3 Kill Switch

Le Kill Switch est une fonction de sécurité des connexions VPN. Si le VPN se déconnecte de manière inattendue, il coupe automatiquement tout accès Internet de votre réseau local pour éviter d'exposer votre véritable adresse IP et vos données en ligne. Il maintient ainsi la confidentialité et la sécurité. Cette fonction est particulièrement utile pour préserver un accès Internet sécurisé et anonyme, par exemple sur un réseau public, lors du traitement de données sensibles ou pour masquer votre véritable adresse IP.

Une fois activé, il bloque tout trafic client qui tente de contourner le tunnel VPN. Il empêche ainsi les fuites VPN dues à des problèmes de configuration DNS, des déconnexions inattendues, des requêtes directes vers des adresses IP ou d'autres situations similaires.

Depuis le micrologiciel v4.8, les routeurs GL.iNet permettent de configurer le Kill Switch pour la connexion VPN globale et pour chaque tunnel VPN.

- Pour configurer le Kill Switch de la connexion VPN globale, consultez Tout autre trafic.
- Pour configurer le Kill Switch de chaque tunnel VPN, consultez Options du tunnel.

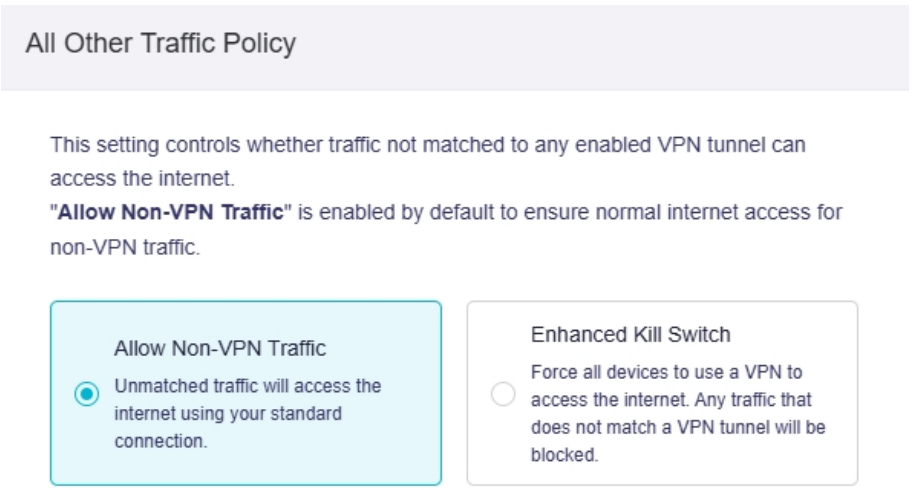
9.4 Tout autre trafic

Cliquez sur l’engrenage dans l’angle supérieur droit pour définir la politique du trafic ne correspondant à aucun tunnel VPN.

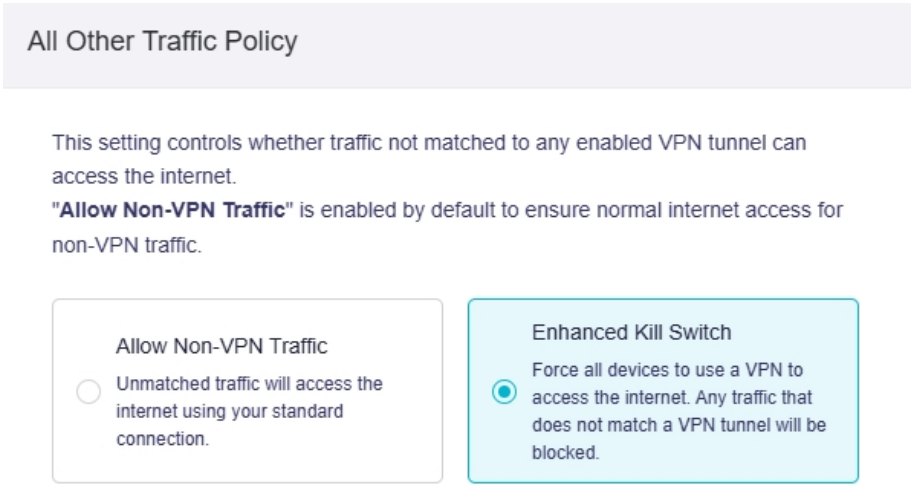


Cette politique détermine si le trafic ne correspondant à aucun de vos groupes de tunnels VPN peut accéder à Internet. Deux options sont proposées :

- **Autoriser le trafic hors VPN (Allow Non-VPN Traffic)** : activé par défaut pour maintenir l’accès Internet du trafic hors VPN.



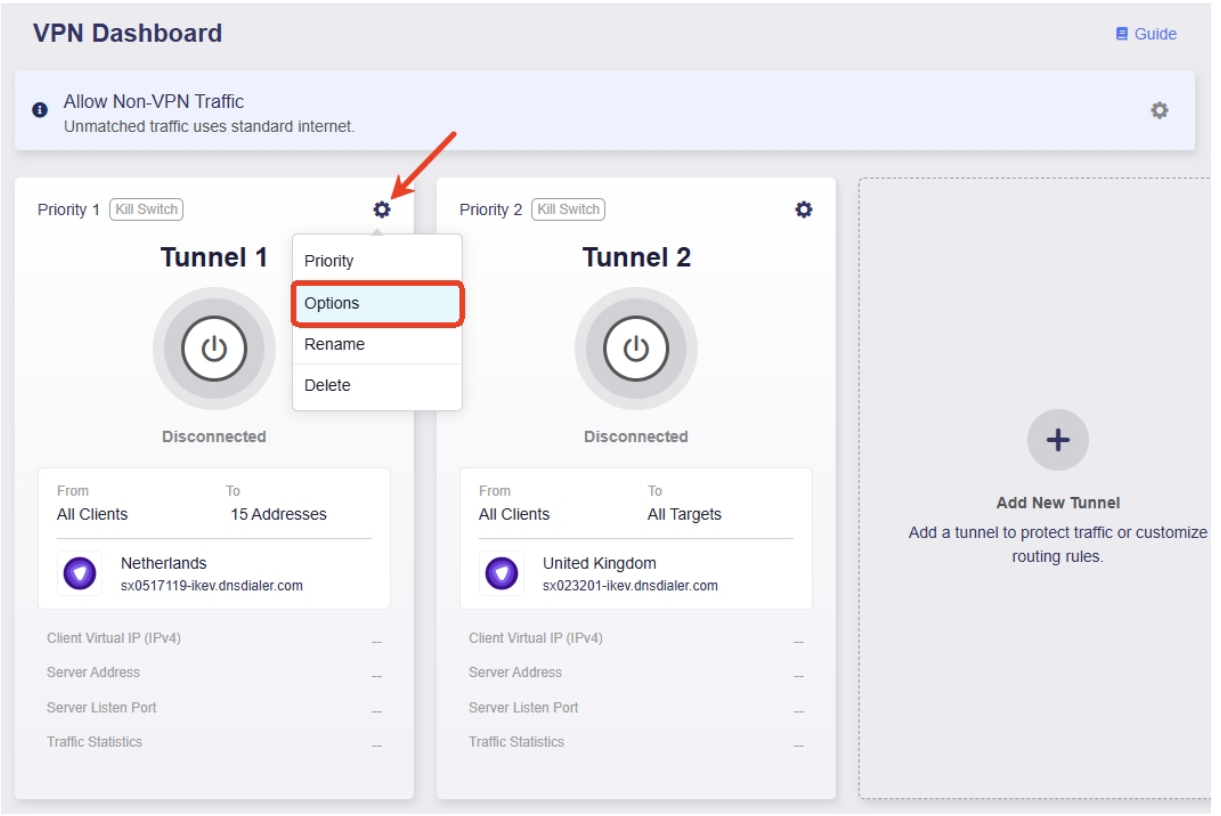
- **Kill Switch renforcé (Enhanced Kill Switch)** : oblige tous les appareils à accéder à Internet via un VPN. Tout trafic ne correspondant à aucun tunnel VPN est bloqué. Ce paramètre global ne remplace pas le Kill Switch configuré pour chaque tunnel VPN.

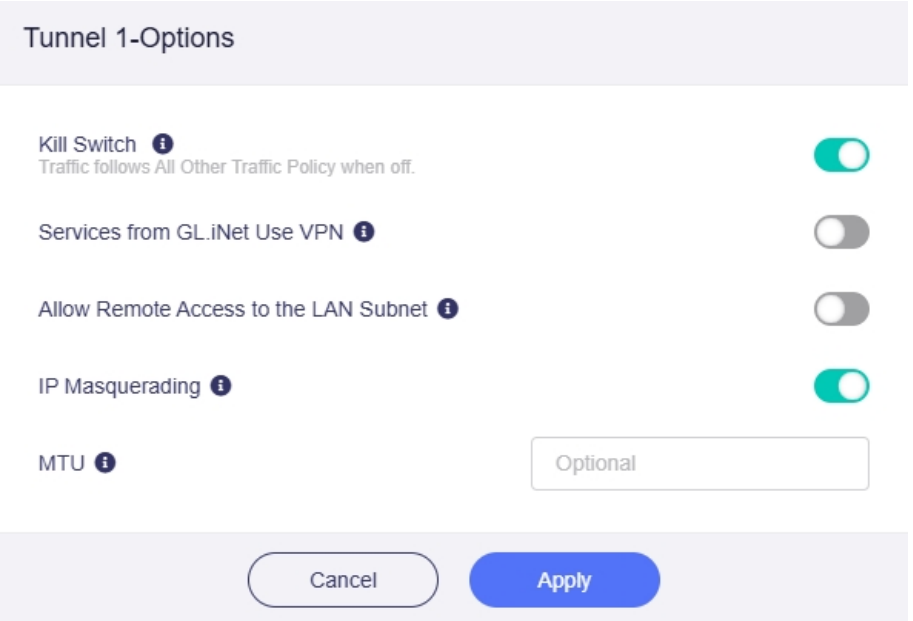


9.5 Options du tunnel

Vous pouvez configurer des paramètres avancés pour chaque tunnel VPN, comme le Kill Switch VPN, le masquage IP et la MTU.

Cliquez sur l'engrenage d'un groupe de tunnels, puis choisissez **Options**.

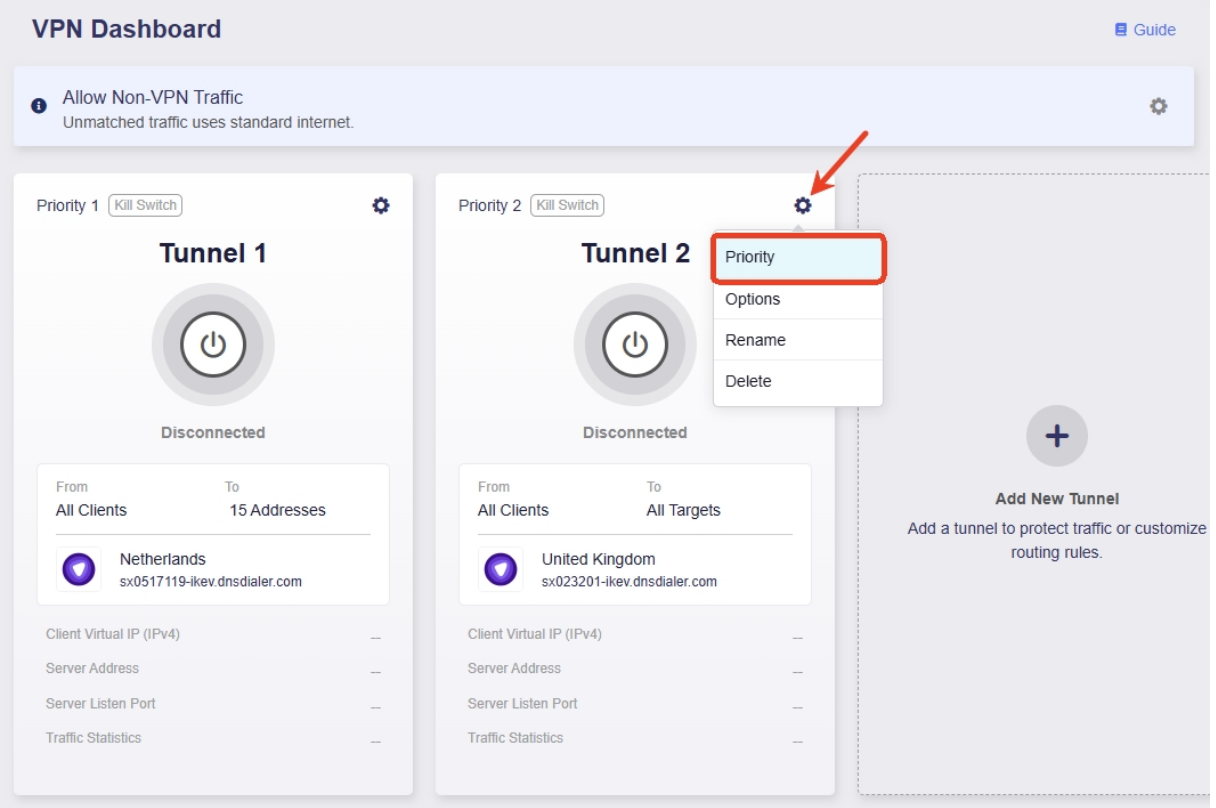




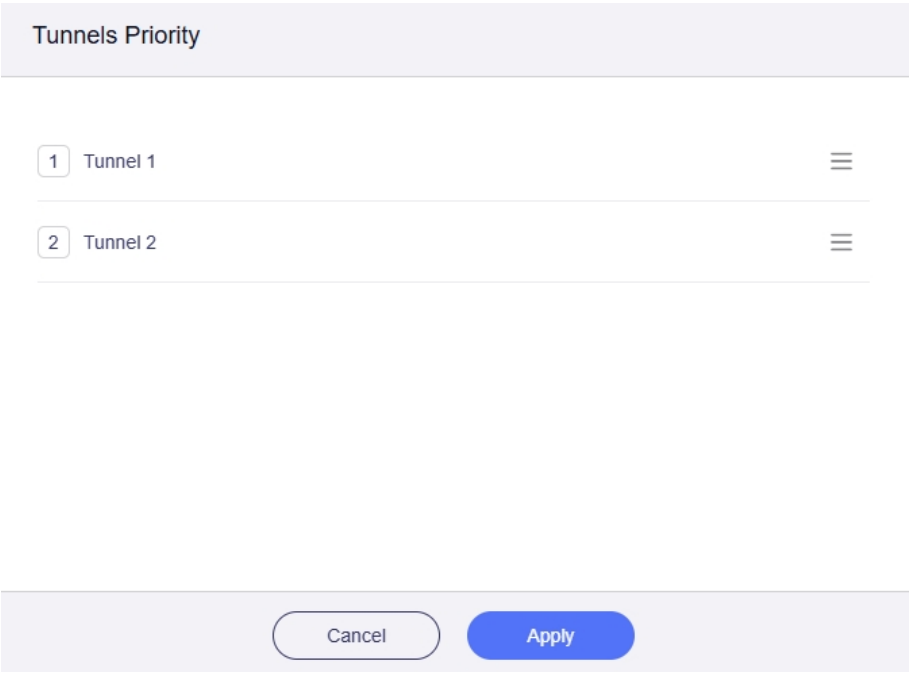
- **Kill Switch** : une fois activé, le trafic correspondant à ce tunnel VPN est bloqué si la connexion VPN échoue de manière inattendue. S'il est désactivé, ce trafic bascule vers le tunnel Tout autre trafic (All Other Traffic).
- **Services GL.iNet via le VPN (Services from GL.iNet Use VPN)** : si cette option est activée, GoodCloud, DDNS et rtty transmettent leurs paquets par les tunnels VPN. Elle est désactivée par défaut, car ces services ont généralement besoin de l'adresse IP réelle de l'appareil pour fonctionner correctement.
- **Autoriser l'accès distant au sous-réseau LAN (Allow Remote Access to the LAN Subnet)** : une fois activé, l'accès distant à ce routeur et à ses appareils LAN via le VPN est autorisé. Le serveur VPN doit annoncer une route de retour vers le sous-réseau LAN du routeur.
- **Masquage IP (IP Masquerading)** : une fois activé, les adresses IP source des clients LAN sont remplacées par l'IP du tunnel VPN du routeur. Ne désactivez cette option que pour une configuration site à site dans laquelle le correspondant distant connaît vos sous-réseaux LAN.
- **MTU** : la valeur définie pour le tunnel remplace celle du fichier de configuration.

9.6 Priorité des tunnels

Pour modifier la priorité des tunnels, cliquez sur l’engrenage d’un groupe de tunnels et choisissez **Priorité (Priority)**.



Maintenez le bouton de la souris enfoncé sur l’icône à trois lignes à droite et faites-la glisser pour réordonner les tunnels. Cliquez ensuite sur **Appliquer (Apply)**.



Lorsque plusieurs tunnels sont actifs, le routeur applique les règles suivantes :

1. Le trafic est d'abord comparé à la règle du tunnel le plus prioritaire. S'il correspond, il emprunte ce tunnel ; sinon, le routeur essaie le tunnel suivant par ordre de priorité, et ainsi de suite.
2. Chaque groupe de tunnels fonctionne indépendamment. Dès que le trafic correspond à la règle d'un tunnel, il est acheminé par celui-ci et ne bascule pas d'un groupe à un autre.
3. Vous pouvez sélectionner plusieurs profils dans chaque groupe pour permettre un basculement au sein du tunnel. Si le profil le plus prioritaire devient indisponible, le tunnel utilise automatiquement le profil suivant par ordre de priorité, et ainsi de suite.
4. Si un tunnel VPN se déconnecte de manière inattendue, le système décide s'il doit acheminer le trafic vers le tunnel Tout autre trafic selon l'état du **Kill Switch** de ce tunnel VPN.
    - Si le Kill Switch est activé, le trafic est bloqué et ne bascule pas vers le tunnel Tout autre trafic (All Other Traffic).
    - Si le Kill Switch est désactivé, le trafic bascule vers le tunnel Tout autre trafic.
5. Dans le tunnel **Tout autre trafic (All Other Traffic)**, le mode choisi détermine si le trafic ne correspondant à aucun tunnel VPN peut accéder à Internet.
    - **Autoriser le trafic hors VPN (Allow Non-VPN Traffic)** : activé par défaut pour que le trafic ne correspondant à aucun tunnel VPN puisse accéder à Internet via le WAN local.

- **Kill Switch renforcé (Enhanced Kill Switch)** : oblige tous les appareils à accéder à Internet via un VPN. Tout trafic ne correspondant à aucun tunnel VPN est bloqué. Ce paramètre global ne remplace pas le Kill Switch configuré pour chaque tunnel VPN. Il renforce la protection et bloque l’accès Internet ordinaire pour éviter les fuites d’adresse IP.

Chapitre 10

Configuration d’un serveur VPN

Ce chapitre explique comment configurer un routeur GL.iNet comme serveur OpenVPN ou WireGuard.

10.1 Configuration d’un serveur OpenVPN

OpenVPN est un protocole VPN open source qui utilise le chiffrement SSL/TLS pour sécuriser les connexions point à point et site à site. Pour configurer un serveur OpenVPN sur un routeur GL.iNet, regardez cette vidéo ou suivez les étapes ci-dessous.

10.1.1 Préparation

1. **Vérifiez que vous disposez d’une adresse IP publique**

   Cliquez ici pour vérifier si votre fournisseur d’accès à Internet (FAI) vous attribue une adresse IP publique.

   Sans adresse IP publique, votre routeur ne peut pas servir de serveur OpenVPN.

   Autres solutions :

   - Si un routeur principal se trouve en amont du routeur GL.iNet, connectez-vous à son interface et vérifiez qu’il possède une adresse IP publique attribuée par votre FAI.
   - Demandez une adresse IP publique à votre FAI. Ce service peut entraîner des frais supplémentaires.
   - Si ces deux méthodes ne fonctionnent pas, par exemple si votre réseau utilise un CGNAT, vous pouvez essayer notre solution SD-WAN GoodPAS.

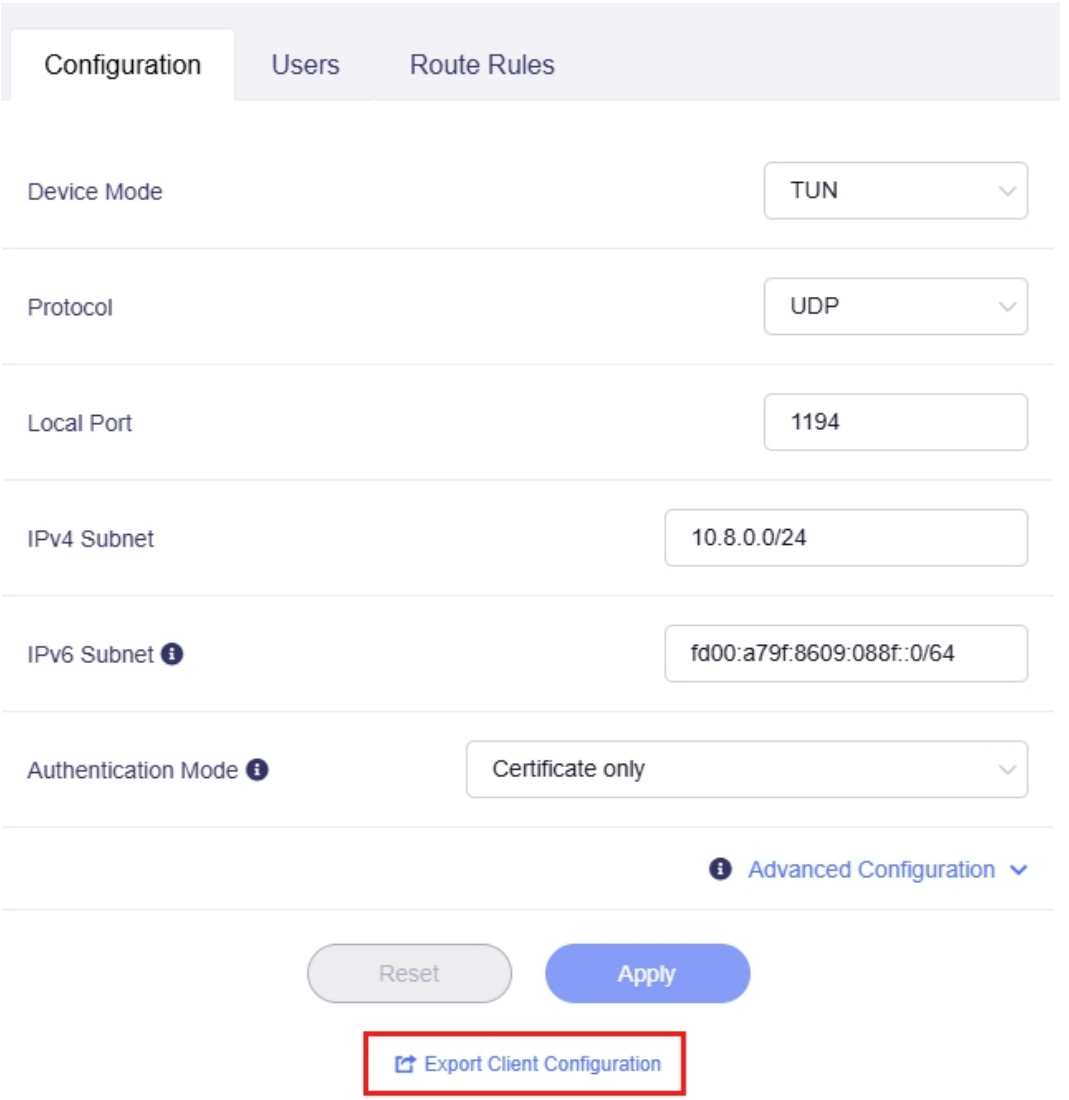
2. **Vérifiez si une redirection de port est nécessaire**

   - Si le routeur GL.iNet est le routeur principal de votre réseau, aucune redirection de port n’est nécessaire. Passez à l’étape suivante.
   - Si un routeur principal est déjà utilisé et que le routeur GL.iNet est secondaire, configurez une redirection de port sur le routeur principal.
   - Si plusieurs appareils intermédiaires séparent le routeur GL.iNet du routeur principal, configurez la redirection de port sur chacun d’eux.

10.1.2 Étapes de configuration

1. Connectez-vous à l'interface d'administration Web du routeur, ouvrez **VPN** > **Serveur OpenVPN (OpenVPN Server)**, puis cliquez sur **Générer la configuration (Generate Configuration)** (uniquement lors de la configuration initiale du serveur VPN).
2. Appliquez la configuration.

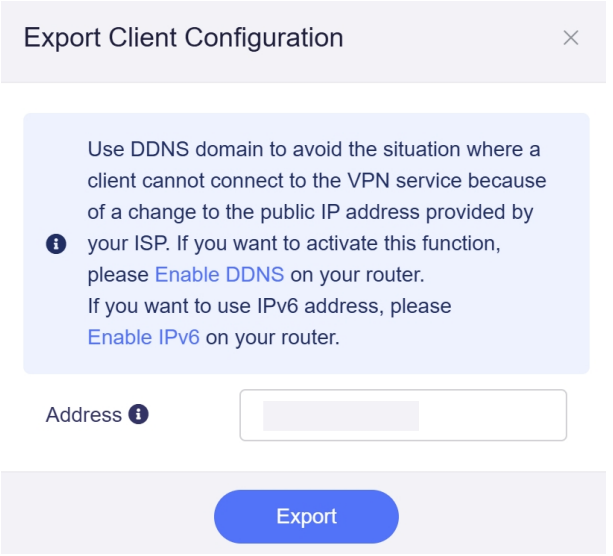
   La configuration par défaut convient à la plupart des situations. Cliquez sur **Exporter la configuration client (Export Client Configuration)** en bas de la page, puis passez à l'étape 3. Si vous avez modifié la configuration, cliquez sur **Appliquer (Apply)** avant de l'exporter.



- **Mode de l'appareil (Device Mode)** : TAP-S2S ou Tun. Consultez cette page pour connaître les différences.

- **Protocole (Protocol)** : UDP ou TCP. Consultez cette page pour connaître les différences.
- **Mode d'authentification (Authentication Mode)** : détermine la méthode utilisée lors de la connexion du client au serveur. Trois options sont proposées :
  - **Certificat uniquement (Certificate Only)** : le routeur génère automatiquement les certificats et les clés du serveur et du client, puis les intègre au fichier de configuration. Aucun identifiant supplémentaire n'est requis lors de l'importation sur le client.
  - **Identifiant/mot de passe uniquement (Username/Password Only)** : le routeur génère une configuration client sans certificats ni clés. Ajoutez d'abord un identifiant et un mot de passe dans l'onglet **Utilisateurs (Users)**, puis exportez la configuration client. Renseignez ces identifiants lors de l'importation sur le client.
  - **Identifiant/mot de passe et certificat (Username/Password and Certificate)** : ajoutez d'abord un identifiant et un mot de passe dans l'onglet **Utilisateurs (Users)** avant d'exporter la configuration client. Le routeur génère également les certificats et les clés du serveur et du client et les intègre au fichier. Lors de l'importation sur le client, le certificat et la clé sont vérifiés avant l'authentification par identifiant et mot de passe, pour une sécurité à deux facteurs.
- **Configuration avancée (Advanced Configuration)** : personnalisez d'autres paramètres du serveur si nécessaire.

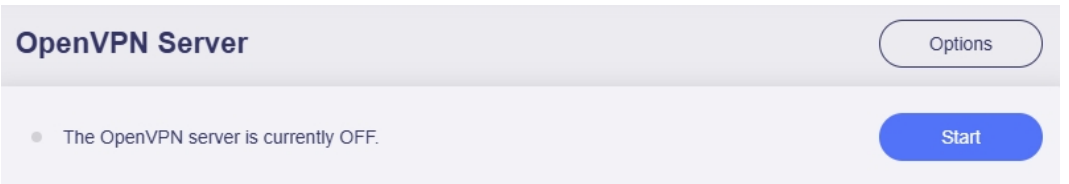
3. Exportez la configuration client.
   Cliquez sur **Exporter la configuration client (Export Client Configuration)** en bas de l'onglet Configuration, après avoir appliqué vos modifications éventuelles. Dans la fenêtre qui s'affiche, cliquez sur **Télécharger (Download)** pour exporter la configuration.



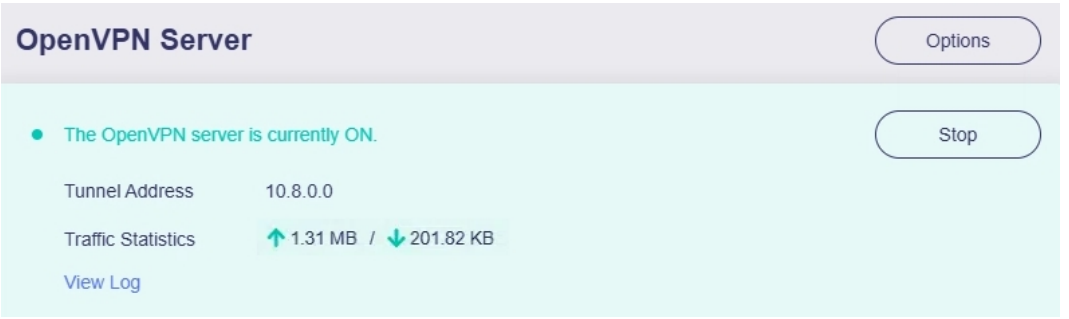
Conseils :

- Si votre adresse IP publique change fréquemment, ouvrez **APPLICATIONS** > **DNS dynamique (Dynamic DNS)** et activez DDNS. Vous pouvez alors utiliser le domaine DDNS comme adresse de serveur.
- Avant d'exporter le fichier de configuration, vous pouvez sélectionner l'adresse du serveur dans une liste : adresse IP publique, domaine DDNS ou adresse IP WAN actuelle. Une fois l'adresse sélectionnée, celle du fichier de configuration est mise à jour automatiquement. Téléchargez à nouveau le fichier de configuration si l'adresse du serveur change.

4. Démarrez le serveur OpenVPN.
   Sur la page **Serveur OpenVPN (OpenVPN Server)**, cliquez sur **Démarrer (Start)** dans l'angle supérieur droit.



L'état de connexion apparaît en haut de la page. Si les statistiques de trafic montant et descendant s'affichent, le serveur OpenVPN fonctionne.



10.1.3 Dépannage

Voici les causes courantes d’un échec de connexion :

- Le serveur VPN ne possède pas d’adresse IP publique. Consultez cette page pour obtenir de l’aide.
- Une redirection de port peut être nécessaire. Consultez cette page pour obtenir de l’aide.
- Votre FAI bloque le port utilisé par le serveur OpenVPN. Choisissez un autre port ou contactez votre FAI.
- La connexion VPN peut être bloquée dans certains pays ou certaines régions.

10.2 Configuration d’un serveur WireGuard

WireGuard® est un VPN simple, rapide et moderne, fondé sur une cryptographie de pointe. Il vise à être plus rapide, plus simple et plus pratique qu’IPSec, tout en limitant la complexité de configuration, et nettement plus performant qu’OpenVPN. Pour configurer un serveur WireGuard sur un routeur GL.iNet, regardez cette vidéo ou suivez les étapes ci-dessous.

10.2.1 Préparation

1. **Vérifiez que vous disposez d’une adresse IP publique**

   Cliquez ici pour vérifier si votre fournisseur d’accès à Internet vous attribue une adresse IP publique.

   Sans adresse IP publique, votre routeur ne peut pas servir de serveur WireGuard.

   Autres solutions :

   - Si un routeur principal se trouve en amont du routeur GL.iNet, connectez-vous à son interface et vérifiez qu’il possède une adresse IP publique attribuée par votre FAI.
   - Demandez une adresse IP publique à votre FAI. Ce service peut entraîner des frais supplémentaires.
   - Si ces deux méthodes ne fonctionnent pas, par exemple si votre réseau utilise un CGNAT, vous pouvez essayer notre solution SD-WAN GoodPAS.

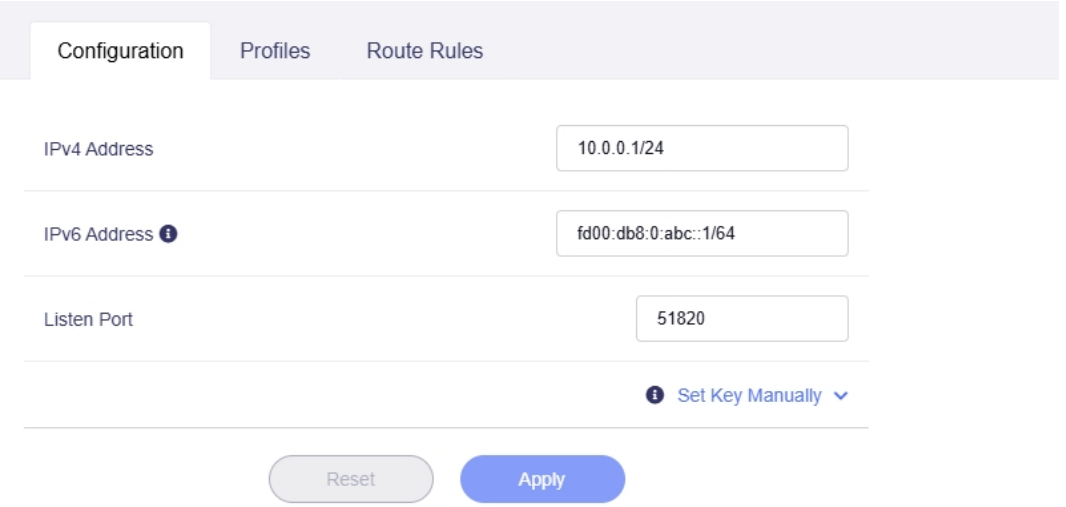
2. **Vérifiez si une redirection de port est nécessaire**

   - Si le routeur GL.iNet est le routeur principal de votre réseau, aucune redirection de port n’est nécessaire. Passez à l’étape suivante.
   - Si un routeur principal est déjà utilisé et que le routeur GL.iNet est secondaire, configurez une redirection de port sur le routeur principal.
   - Si plusieurs appareils intermédiaires séparent le routeur GL.iNet du routeur principal, configurez la redirection de port sur chacun d’eux.

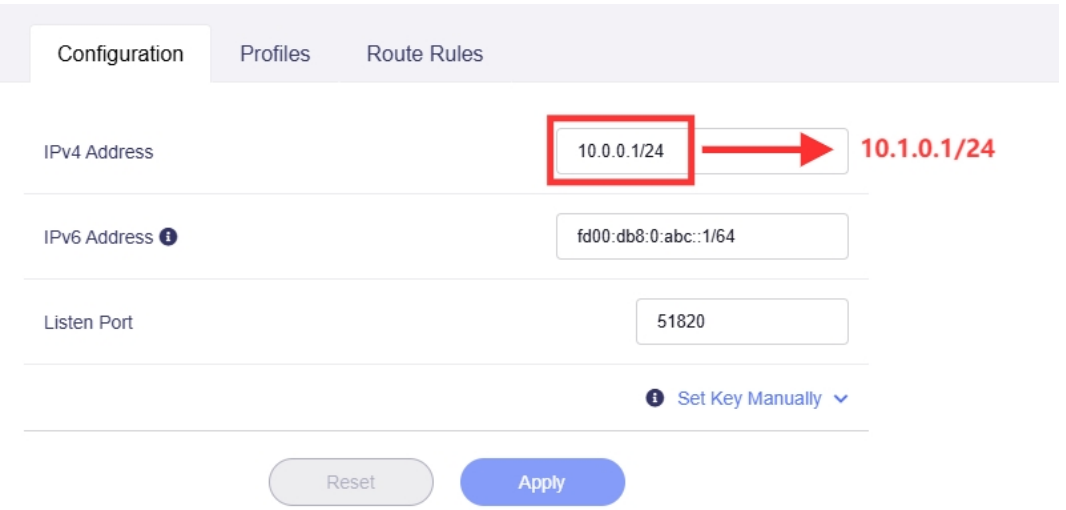
10.2.2 Étapes de configuration

1. Connectez-vous à l'interface d'administration Web du routeur, ouvrez **VPN** > **Serveur WireGuard (WireGuard Server)**, puis cliquez sur **Générer la configuration (Generate Configuration)** (uniquement lors de la configuration initiale du serveur VPN).
2. Appliquez la configuration.

   La configuration par défaut convient à la plupart des situations. Ne modifiez l'adresse IPv4 que si elle entre en conflit avec la passerelle du routeur en amont.

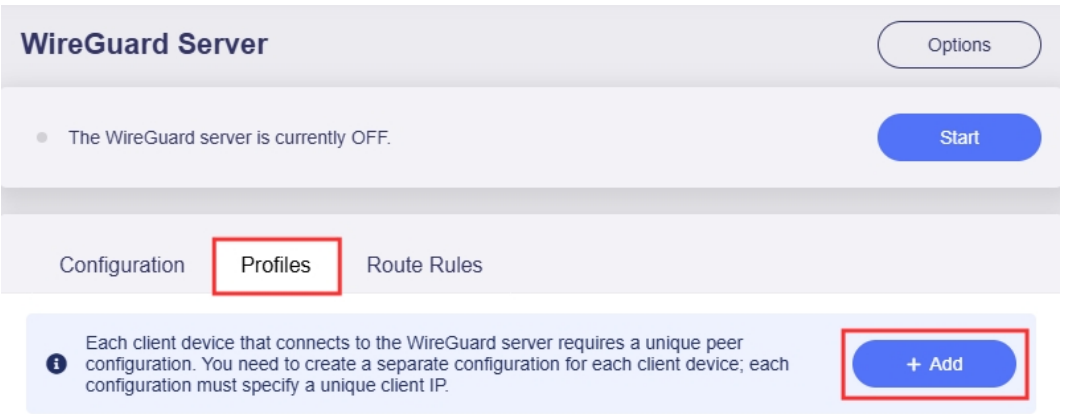


   En cas de conflit, choisissez une autre adresse IPv4, par exemple **10.1.0.1/24**, puis cliquez sur **Appliquer (Apply)**. Conservez la notation CIDR « /24 » pour éviter les problèmes de connexion.

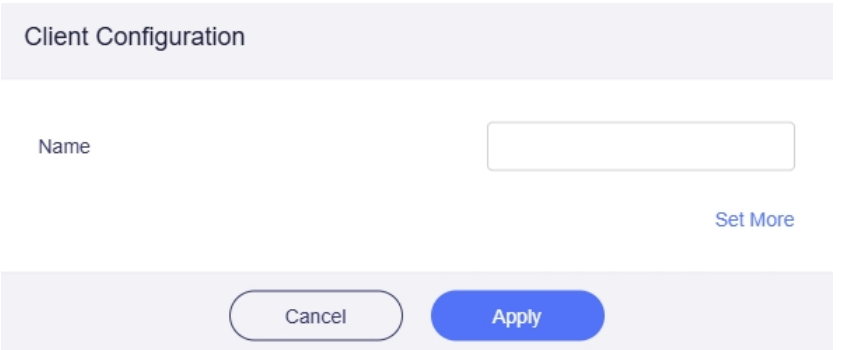


3. Ajoutez un profil.

Ouvrez l'onglet **Profils (Profiles)**, puis cliquez sur **Ajouter (Add)** pour générer un profil pour votre appareil.



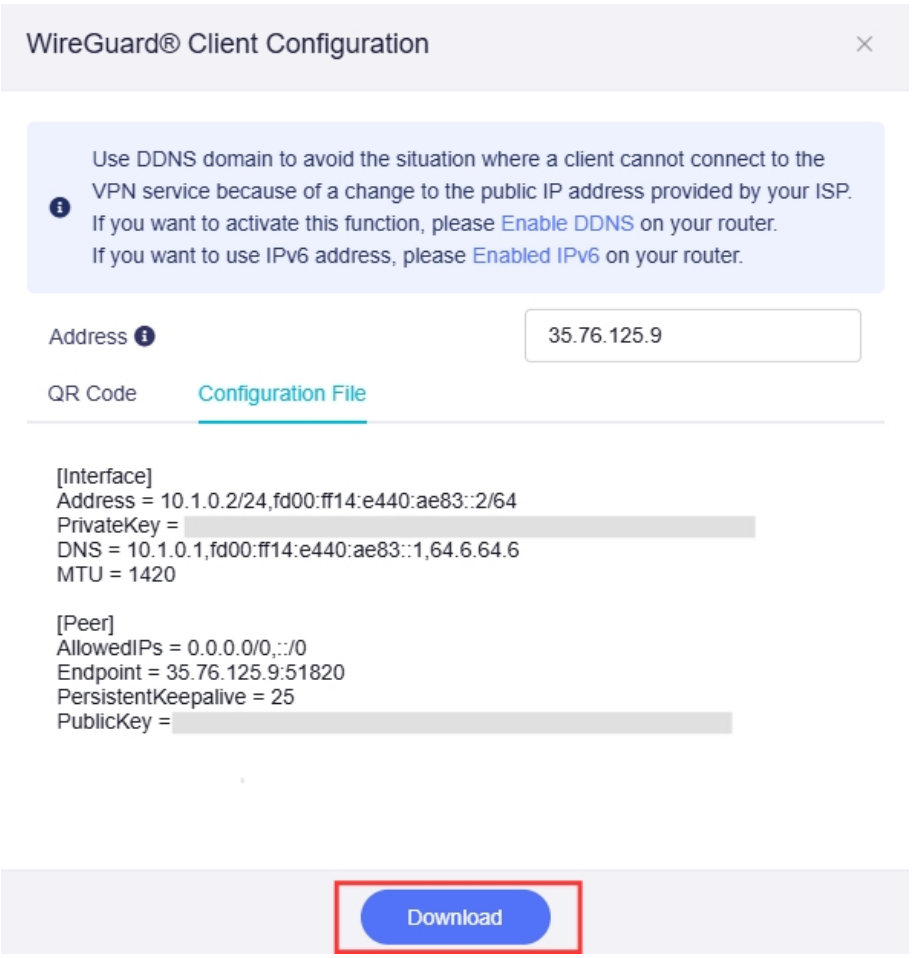
Saisissez un nom explicite et cliquez sur **Appliquer (Apply)** pour continuer.



Conseil : pour accéder aux appareils du LAN du client WireGuard depuis le serveur WireGuard, configurez les routes dans l'onglet **Règles de routage (Route Rules)**. Consultez cette page pour en savoir plus.

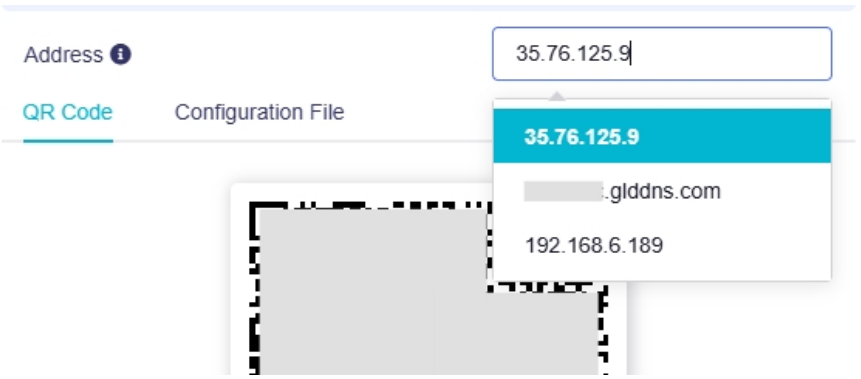
4. Téléchargez la configuration.
   Après l'ajout du profil, le routeur génère la configuration sous trois formes : code QR, texte brut et fichier .conf. Choisissez la méthode qui vous convient.
   - **Code QR** : adapté aux appareils disposant de l'application WireGuard, comme les smartphones, tablettes et ordinateurs portables. Ouvrez l'application WireGuard sur l'appareil à configurer comme client et scannez le code QR pour importer la configuration.
   - **Texte brut** : permet de consulter la configuration et de la copier-coller ailleurs pour une configuration manuelle, par exemple dans l'application WireGuard ou sur un routeur GL.iNet.

- **Fichier .conf** : cliquez sur **Télécharger (Download)** pour enregistrer le fichier .conf sur votre appareil. Vous pouvez ensuite l'importer directement dans l'application WireGuard ou sur un routeur GL.iNet.

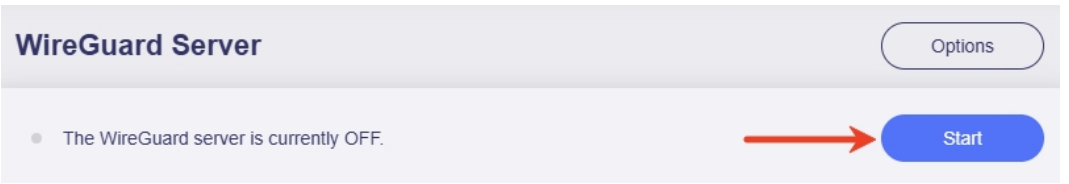


Conseils :

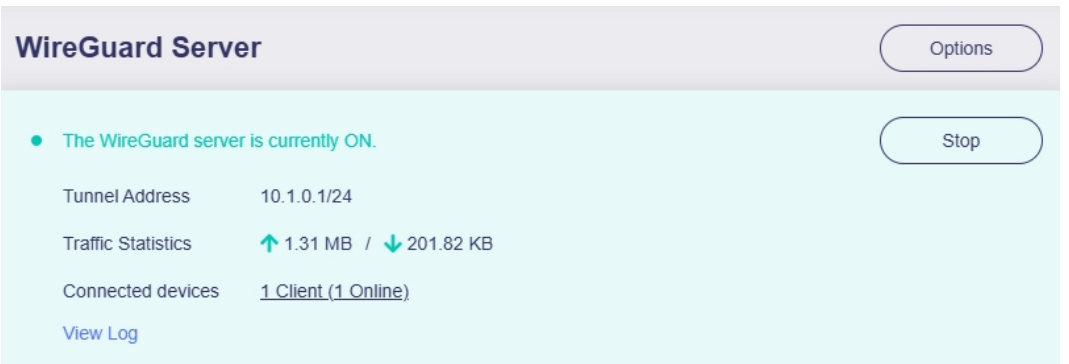
- Si votre adresse IP publique change fréquemment, ouvrez **APPLICATIONS** > **DNS dynamique (Dynamic DNS)** et activez DDNS. Vous pouvez alors utiliser le domaine DDNS comme adresse de serveur.
- Depuis le micrologiciel v4.8, vous pouvez choisir l'adresse du serveur dans une liste avant d'exporter le fichier : IP publique, domaine DDNS ou adresse IP WAN actuelle. L'adresse est mise à jour automatiquement dans le fichier. Téléchargez de nouveau le fichier si l'adresse du serveur change.



5. Démarrez le serveur WireGuard.
   Sur la page **Serveur WireGuard (WireGuard Server)**, cliquez sur **Démarrer (Start)** dans l'angle supérieur droit.



   L'état de connexion apparaît en haut de la page. Si les statistiques de trafic montant et descendant et les appareils connectés s'affichent, le serveur WireGuard fonctionne.



10.2.3 Dépannage

Voici les causes courantes d'un échec de connexion :

- Le serveur VPN ne possède pas d'adresse IP publique. Consultez cette page pour obtenir de l'aide.
- Une redirection de port peut être nécessaire. Consultez cette page pour obtenir de l'aide.
- Votre FAI bloque le port utilisé par le serveur WireGuard. Choisissez un autre port ou contactez votre FAI.
- La connexion VPN peut être bloquée dans certains pays ou certaines régions.

Chapitre 11

Configuration d’un client VPN

Ce chapitre explique comment configurer un routeur GL.iNet comme client OpenVPN ou WireGuard.

11.1 Configuration d’un client OpenVPN

11.1.1 Préparation

Vérifiez d’abord que vous disposez d’un abonnement actif auprès d’un fournisseur VPN prenant en charge la configuration manuelle d’OpenVPN. Consultez cette page pour connaître les fournisseurs OpenVPN compatibles avec GL.iNet.

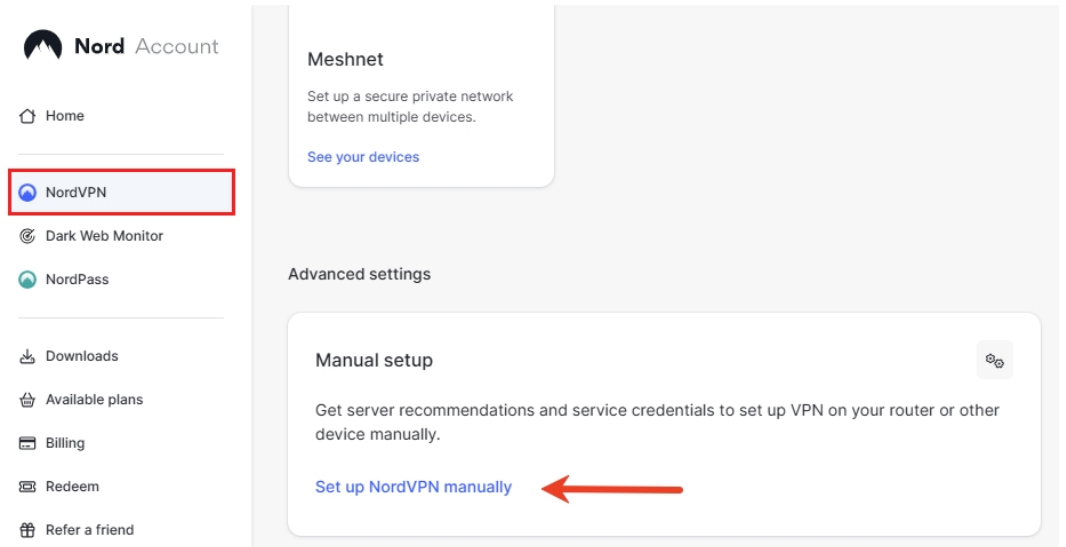
Rendez-vous ensuite sur le site officiel de votre fournisseur VPN pour obtenir les identifiants de service ou le fichier de configuration. Si vous ne savez pas comment obtenir ce fichier, consultez ce lien ou contactez l’assistance du fournisseur.

11.1.2 Configuration de NordVPN

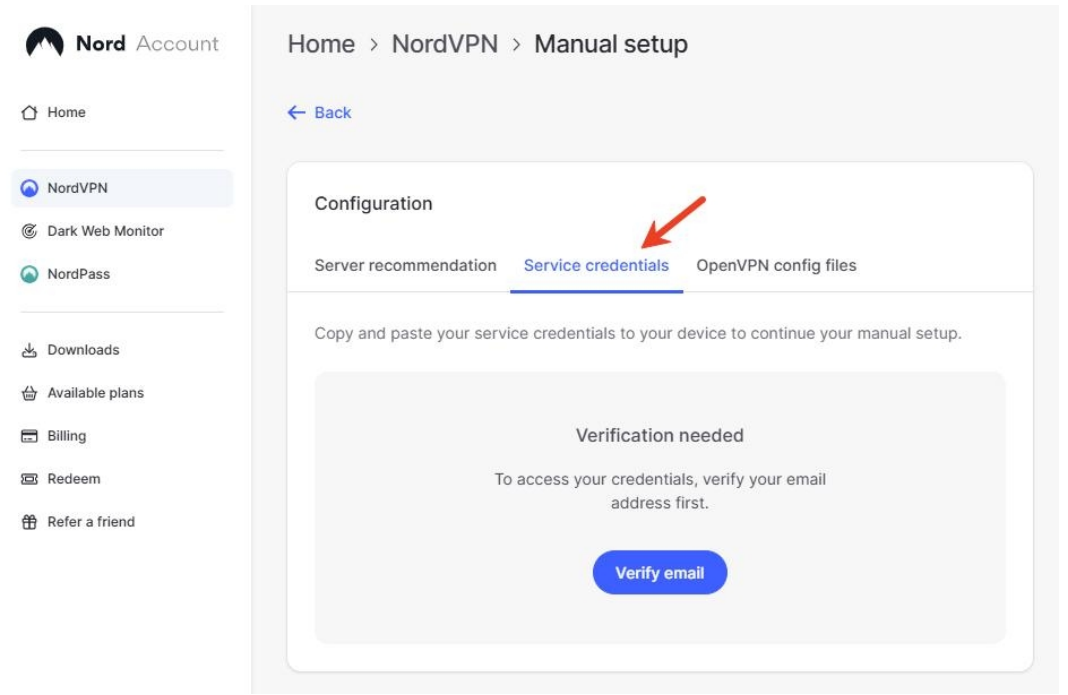
NordVPN est intégré à l’interface d’administration Web GL.iNet. Saisissez vos identifiants de service, obtenus depuis le tableau de bord NordVPN, dans l’interface d’administration Web du routeur ou l’application mobile GL.iNet pour récupérer les fichiers de configuration de tous les serveurs NordVPN, sans avoir à les téléverser manuellement.

Suivez les étapes ci-dessous pour configurer le routeur comme client NordVPN.

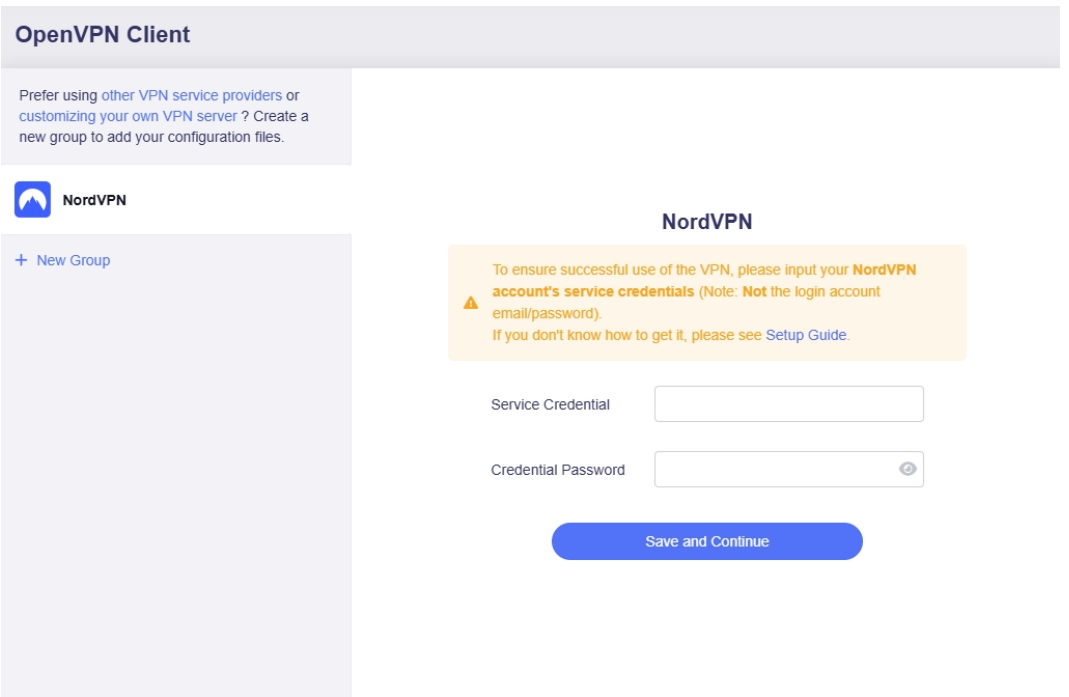
1. Connectez-vous à votre compte Web NordVPN ici.
2. Dans le tableau de bord Nord, cliquez sur **NordVPN**, puis sur **Configurer NordVPN manuellement (Set up NordVPN manually)**.



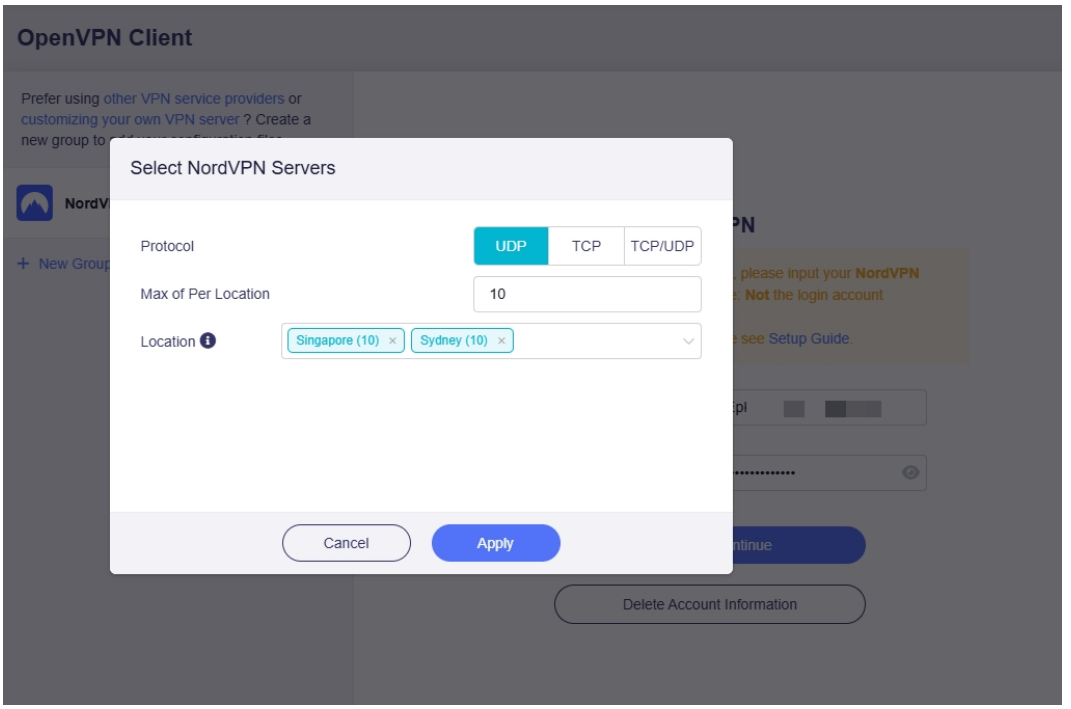
Repérez les **identifiants de service (service credentials)** et copiez-les pour les utiliser ensuite.



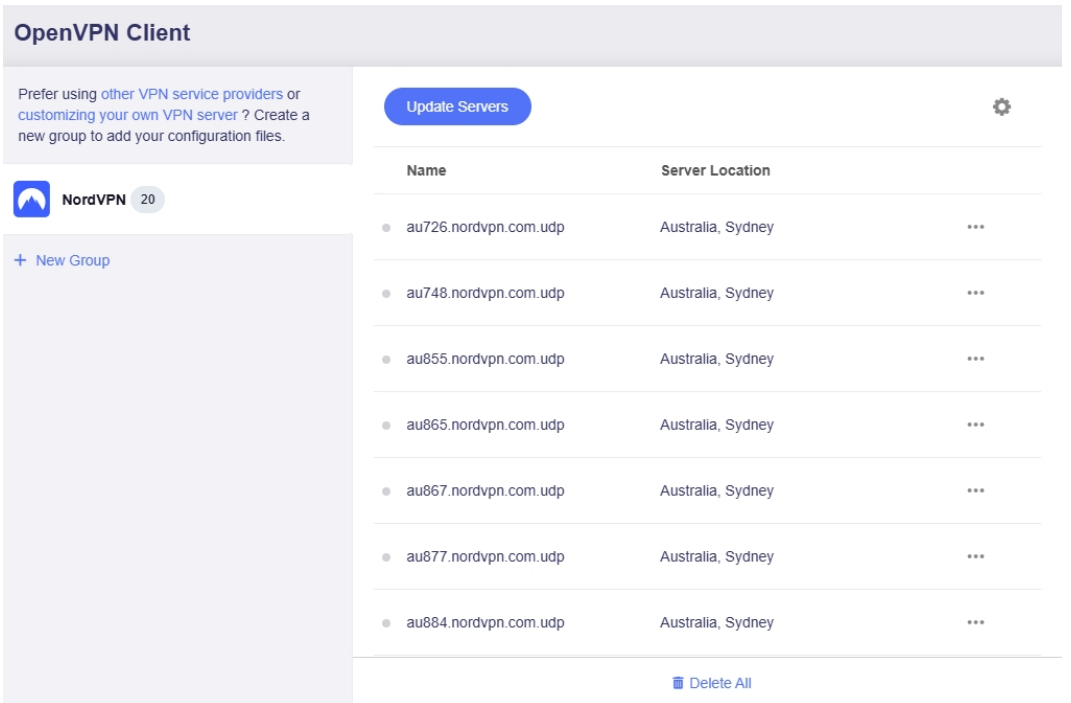
3. Connectez-vous à l'interface d'administration Web du routeur et ouvrez **VPN** > **Client OpenVPN (OpenVPN Client)** > **NordVPN**. Saisissez les identifiants de service (attention : il ne s'agit PAS de l'adresse e-mail et du mot de passe de connexion au compte), puis cliquez sur **Enregistrer et continuer (Save and Continue)**.



4. Choisissez le protocole, le nombre maximal de serveurs par emplacement et les emplacements, puis cliquez sur **Appliquer (Apply)**.

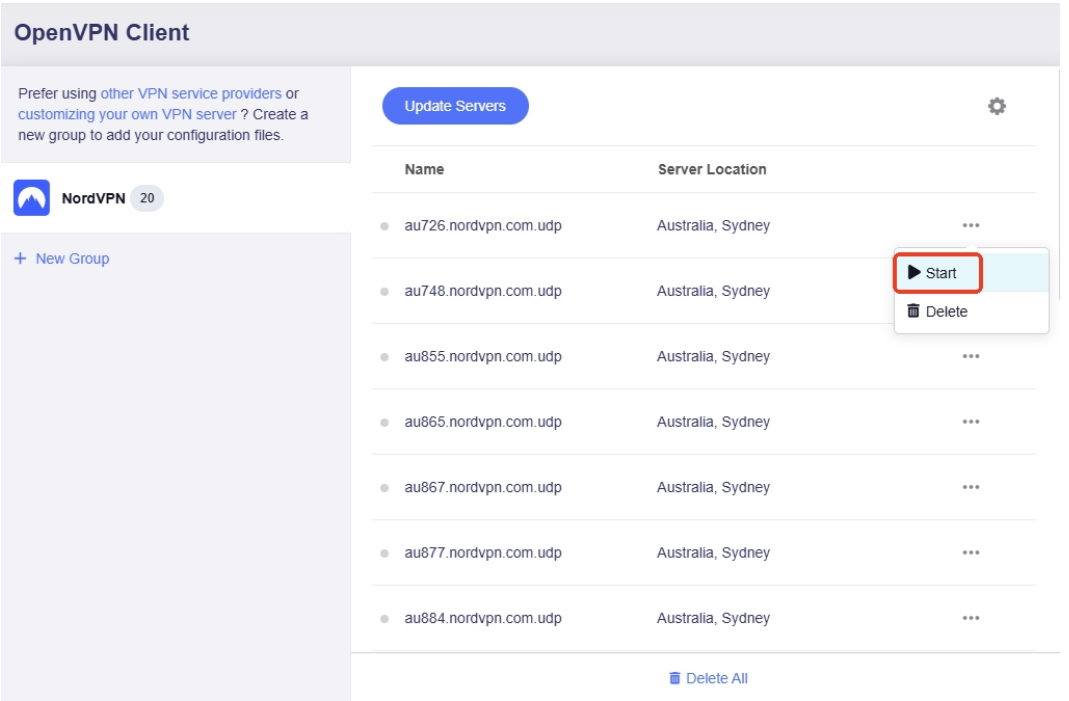


Les fichiers de configuration sont téléchargés.

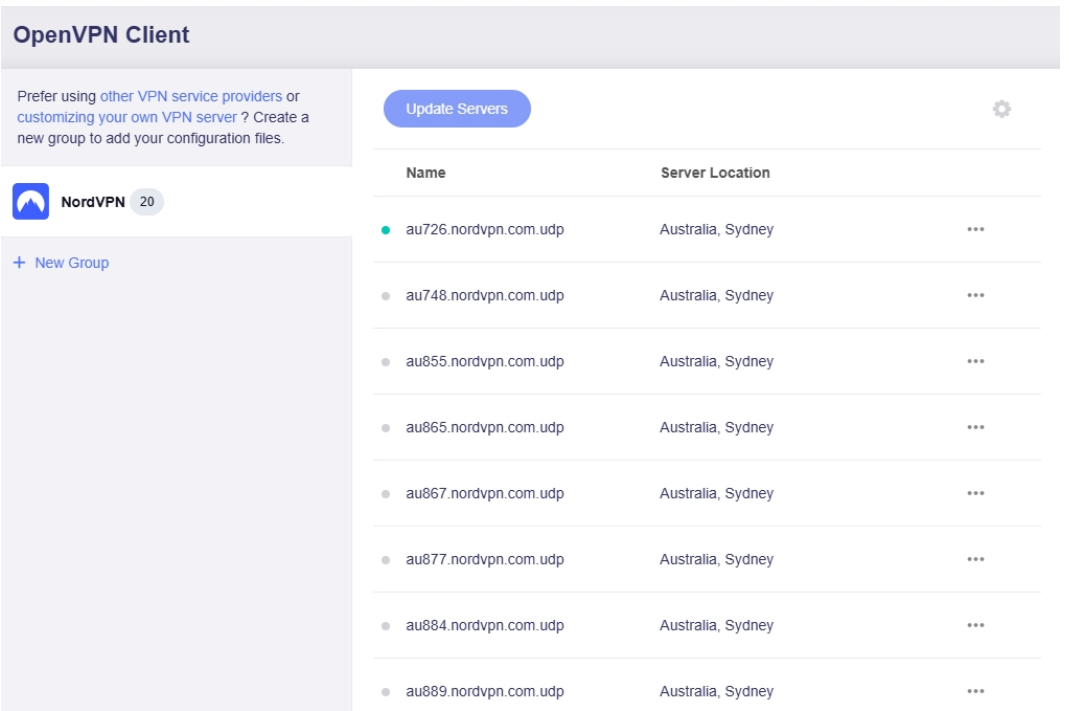


5. Établissez une connexion.

   Sélectionnez un serveur et cliquez sur les trois points à droite pour lancer la connexion.



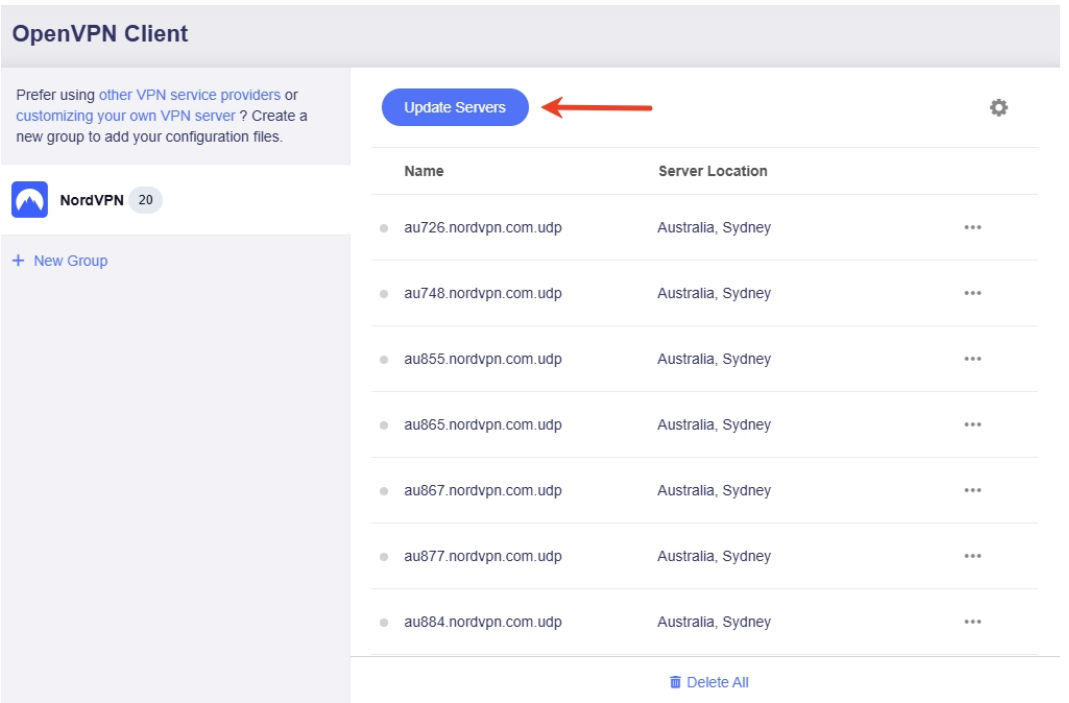
6. Une fois la connexion établie, un point vert apparaît à côté du fichier de configuration.



Vous pouvez également consulter les détails de la connexion dans le **Tableau de bord VPN (VPN Dashboard)**.

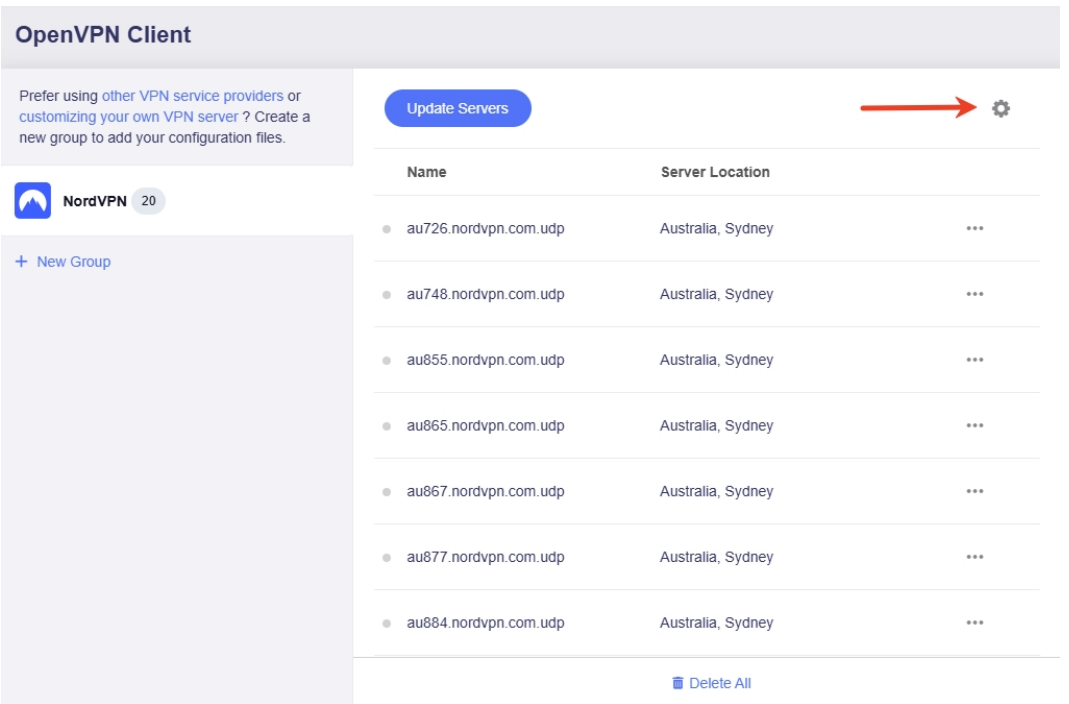
7. Mettez à jour les serveurs.

Cliquez sur **Mettre à jour les serveurs (Update Servers)** pour récupérer la liste à jour des serveurs disponibles et éviter les échecs liés à leur maintenance ou à leur arrêt.



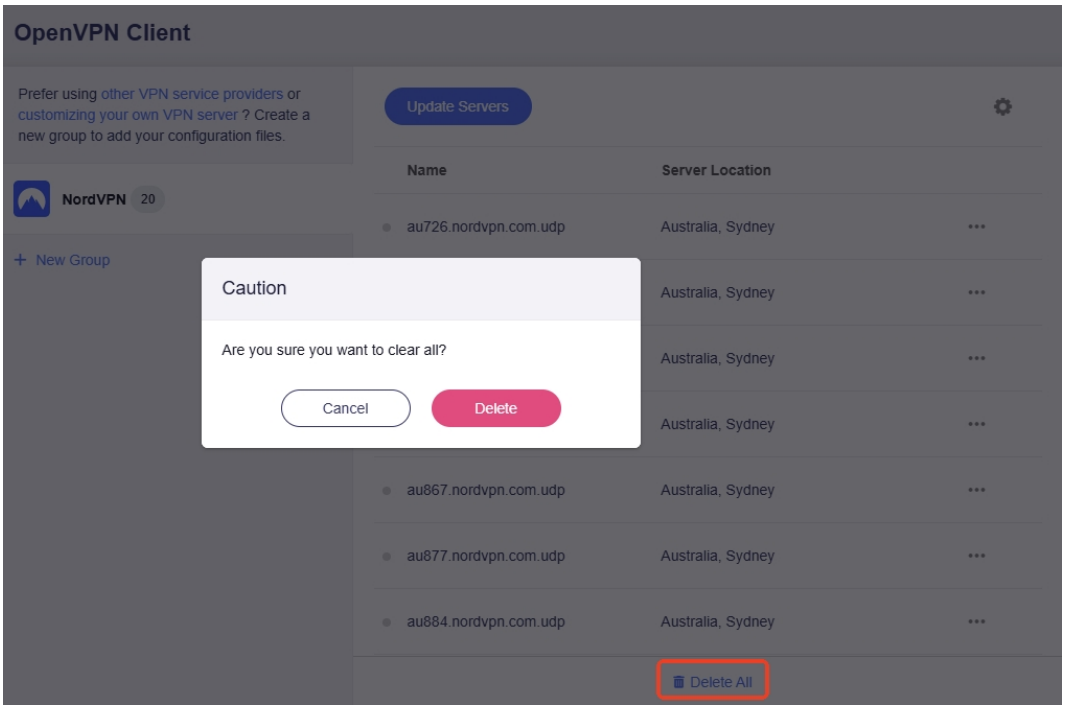
8. Modifiez les identifiants.

   Cliquez sur l'engrenage pour modifier vos identifiants de connexion.



9. Supprimez tous les fichiers.

Cliquez sur **Tout supprimer (Delete All)** pour supprimer tous les fichiers de configuration en un clic.

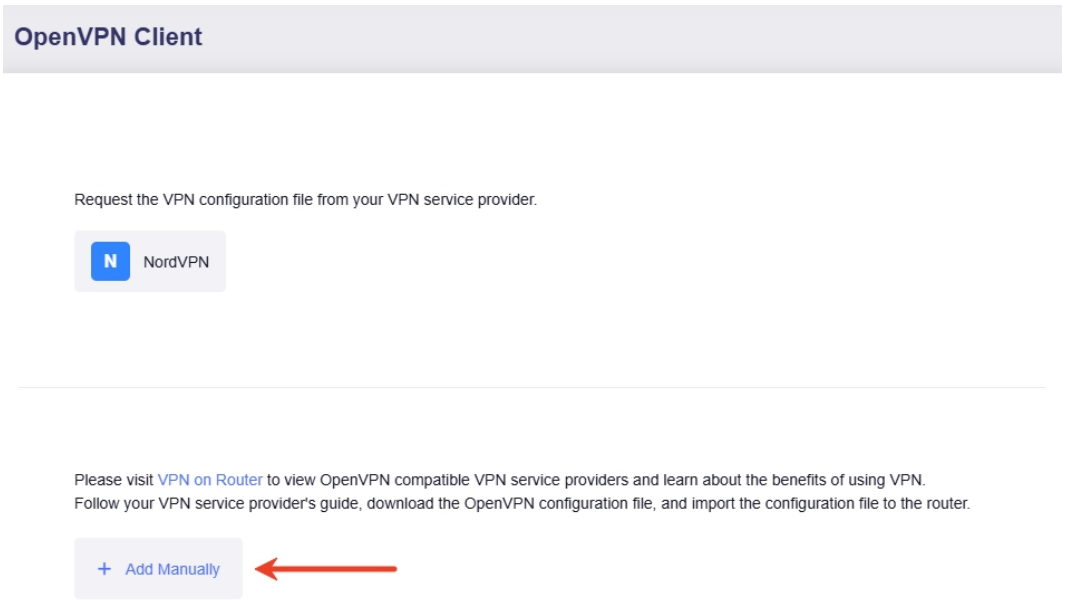


11.1.3 Configuration manuelle d’un client OpenVPN pour un autre fournisseur

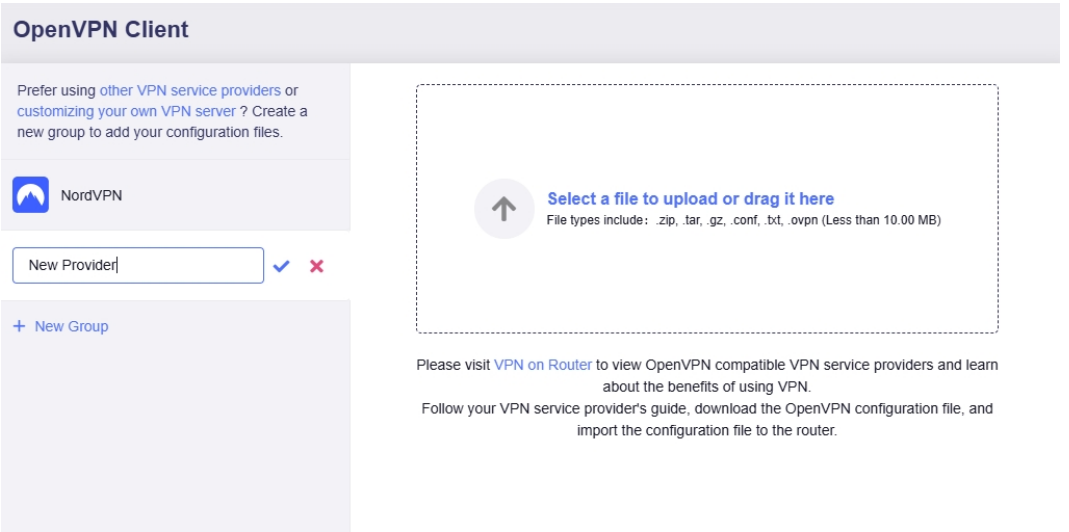
Si votre fournisseur OpenVPN n’est pas intégré à notre interface, récupérez d’abord le fichier de configuration sur son site officiel. Importez-le ensuite sur le routeur pour configurer le client OpenVPN.

Dans les étapes suivantes, nous prenons PIA (Private Internet Access) comme exemple.

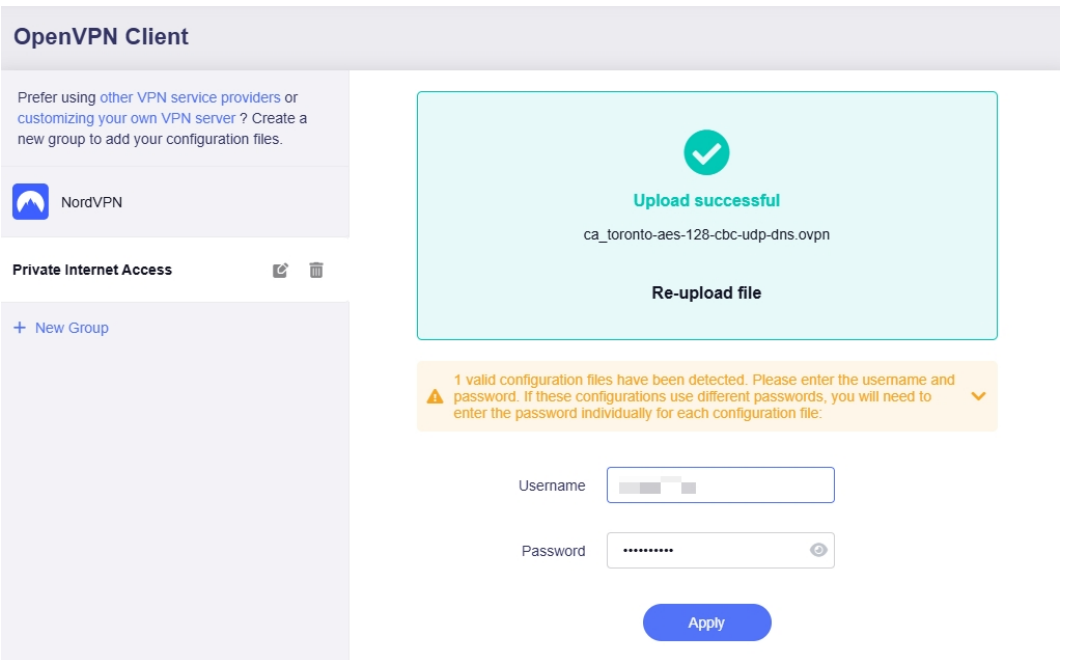
1. Téléchargez un fichier de configuration sur le site officiel de Private Internet Access.
2. Connectez-vous à l’interface d’administration Web du routeur, ouvrez **VPN** > **Client OpenVPN (OpenVPN Client)**, puis cliquez sur **Ajouter manuellement (Add Manually)**.



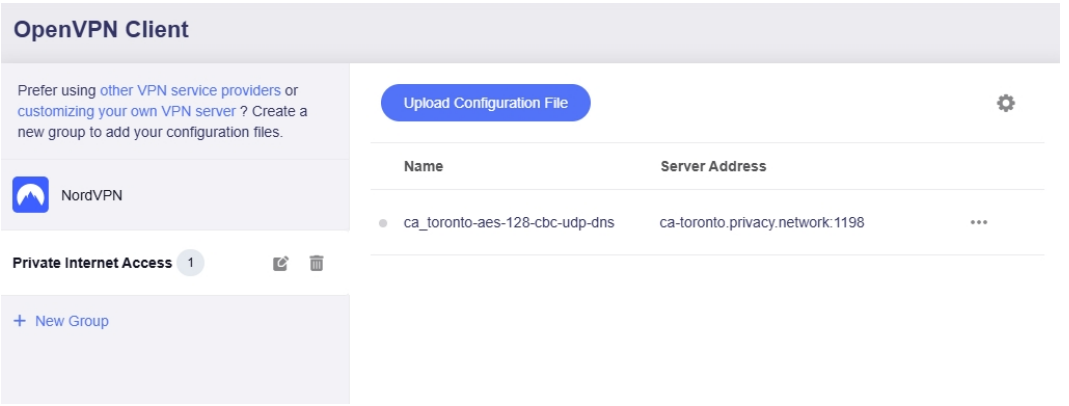
3. Un groupe est créé dans la barre latérale gauche. Donnez-lui un nom explicite.



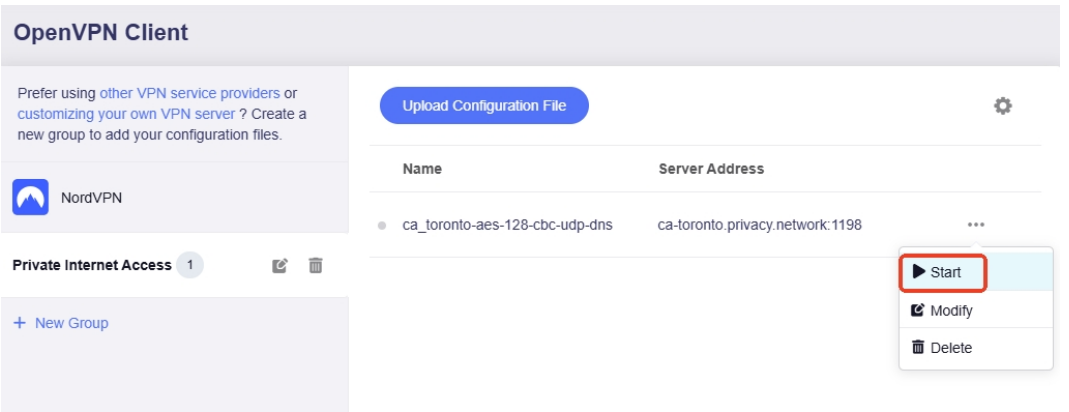
4. Importez votre fichier de configuration OpenVPN. Saisissez les identifiants si nécessaire, puis cliquez sur **Appliquer (Apply)**.



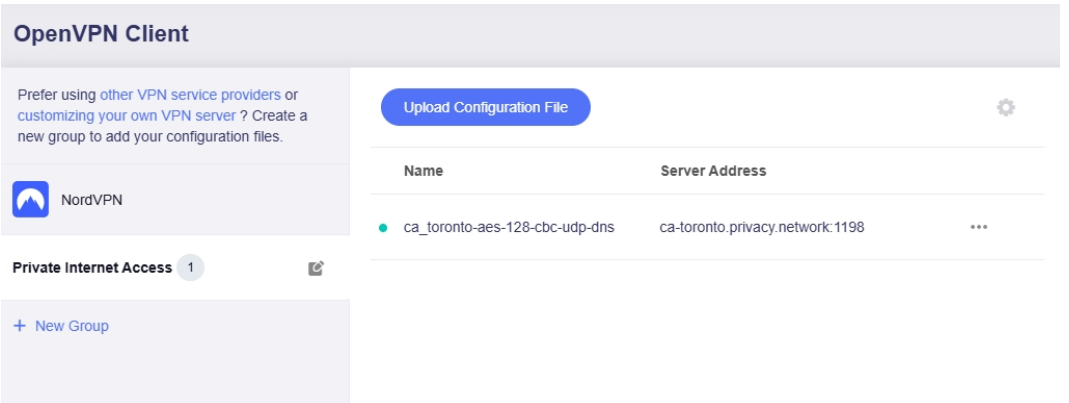
Le fichier importé apparaît dans la liste.



5. Cliquez sur les trois points à droite pour lancer la connexion.



6. Une fois la connexion établie, un point vert apparaît à côté du fichier de configuration.



Vous pouvez également consulter les détails de la connexion dans le **Tableau de bord VPN (VPN Dashboard)**.

11.2 Configuration d’un client WireGuard

Vous pouvez configurer le client WireGuard depuis l’application mobile GL.iNet ou l’interface d’administration Web.

- L’application mobile intègre plusieurs fournisseurs WireGuard, comme AzireVPN, Mullvad VPN, OVPN, StrongVPN et PIA VPN. Pour configurer le service, saisissez les identifiants de votre abonnement. Ouvrez l’application et suivez les instructions à l’écran.
- L’interface d’administration Web intègre certains fournisseurs de services WireGuard et permet aussi une configuration manuelle. Vous pouvez saisir les identifiants de votre service WireGuard pour une configuration rapide ou téléverser un fichier de configuration pour terminer la configuration.

11.2.1 Préparation

Vérifiez d’abord que vous disposez d’un abonnement actif auprès d’un fournisseur VPN prenant en charge la configuration manuelle de WireGuard. Consultez cette page pour connaître les fournisseurs WireGuard compatibles avec GL.iNet.

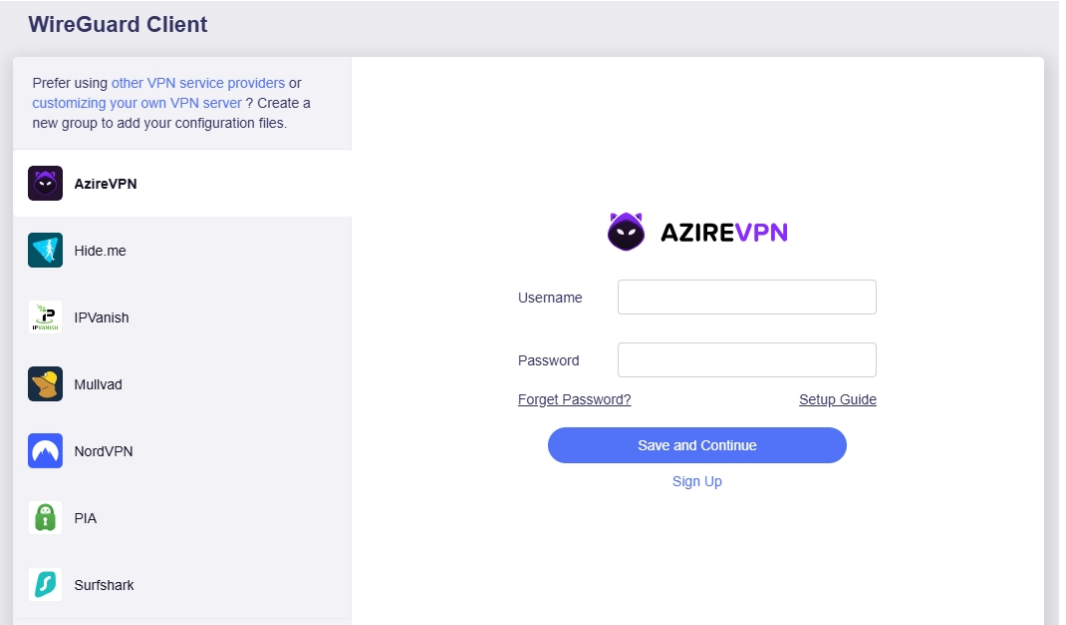
Sélectionnez ensuite votre fournisseur ci-dessous pour accéder directement aux instructions détaillées.

- Configuration d’AzireVPN
- Configuration de Hide.me
- Configuration d’IPVanish
- Configuration de Mullvad
- Configuration de NordVPN
- Configuration de PIA (Private Internet Access)
- Configuration de Surfshark
- Configuration manuelle d’un client WireGuard pour un autre fournisseur

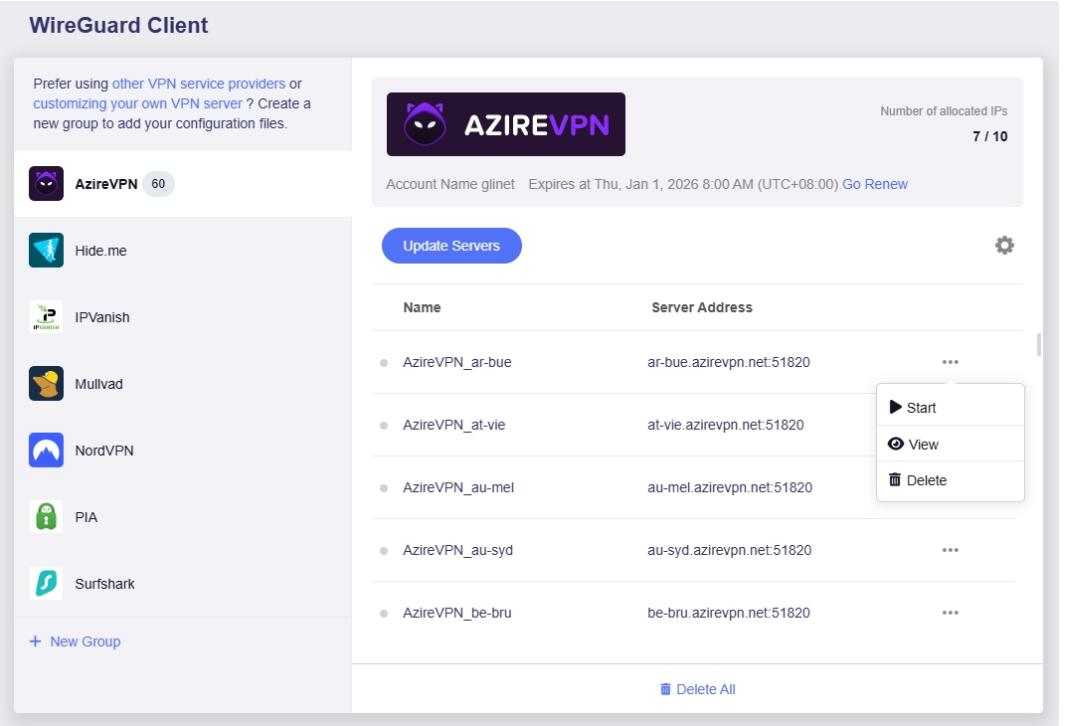
11.2.2 Configuration d’AzireVPN

Suivez les étapes ci-dessous pour configurer le routeur comme client AzireVPN.

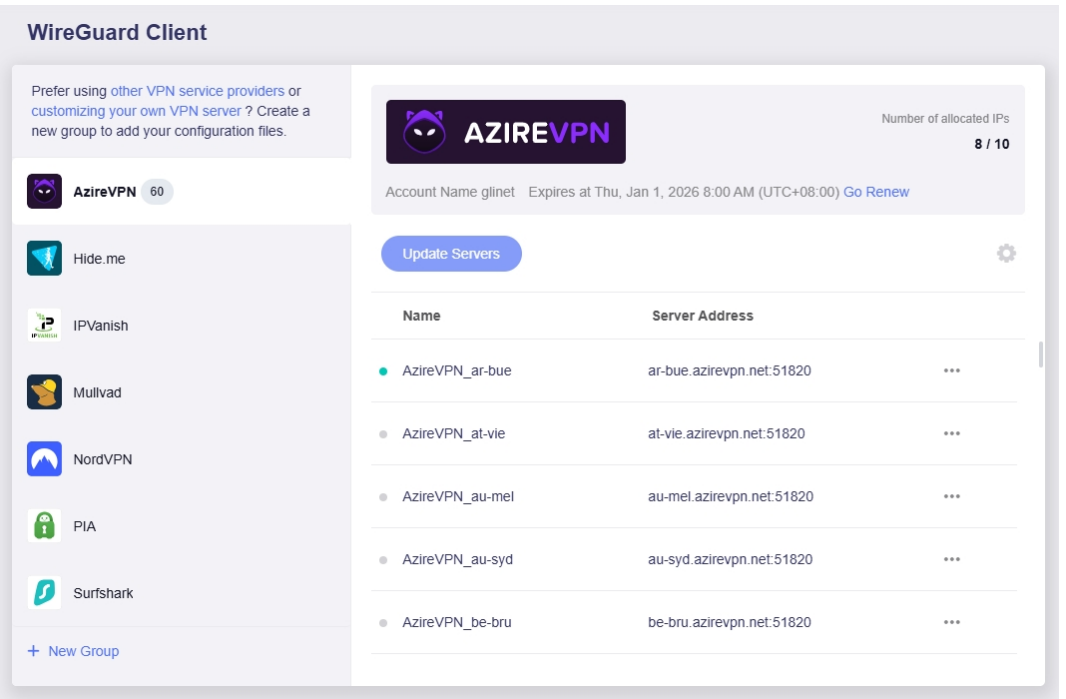
1. Connectez-vous à l’interface d’administration Web du routeur et ouvrez **VPN** > **Client WireGuard (WireGuard Client)** > **AzireVPN**.
2. Saisissez l’identifiant et le mot de passe, puis cliquez sur **Enregistrer et continuer (Save and Continue)**. Les fichiers de configuration de chaque serveur sont générés.



3. Choisissez un serveur et cliquez sur les trois points à droite pour lancer la connexion.



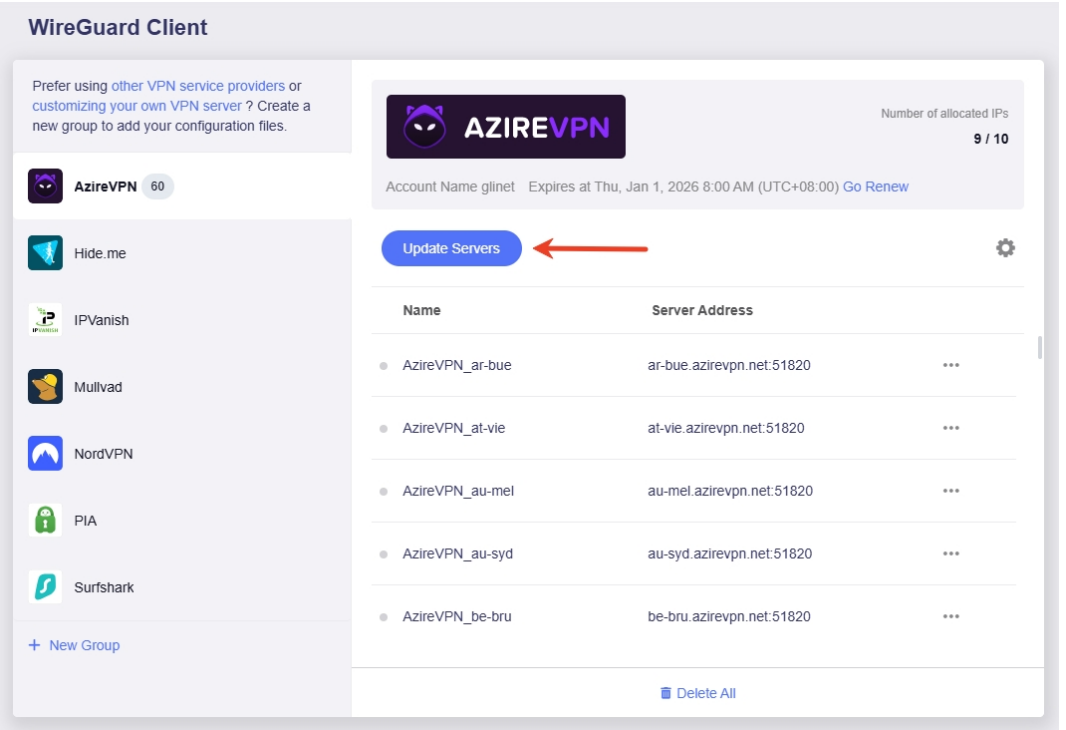
4. Une fois la connexion établie, un point vert apparaît à côté du fichier de configuration.



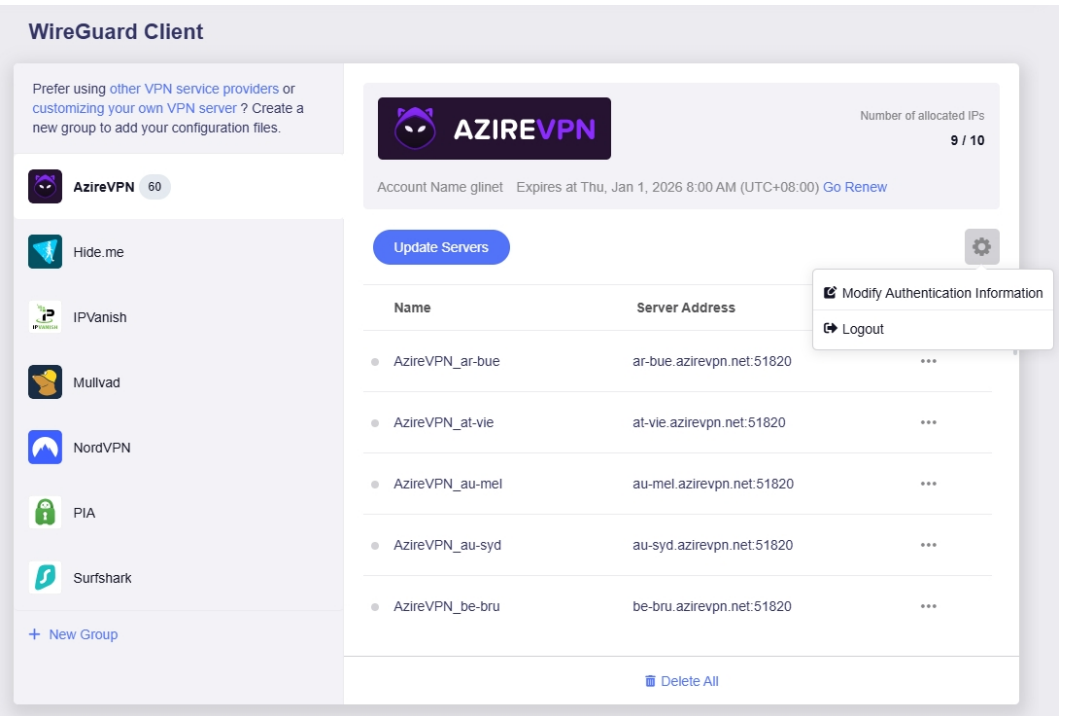
Vous pouvez également consulter les détails de la connexion dans le **Tableau de bord VPN (VPN Dashboard)**.

5. Mettez à jour les serveurs.

Cliquez sur **Mettre à jour les serveurs (Update Servers)** pour récupérer la liste à jour des serveurs disponibles et éviter les échecs liés à leur maintenance ou à leur arrêt.

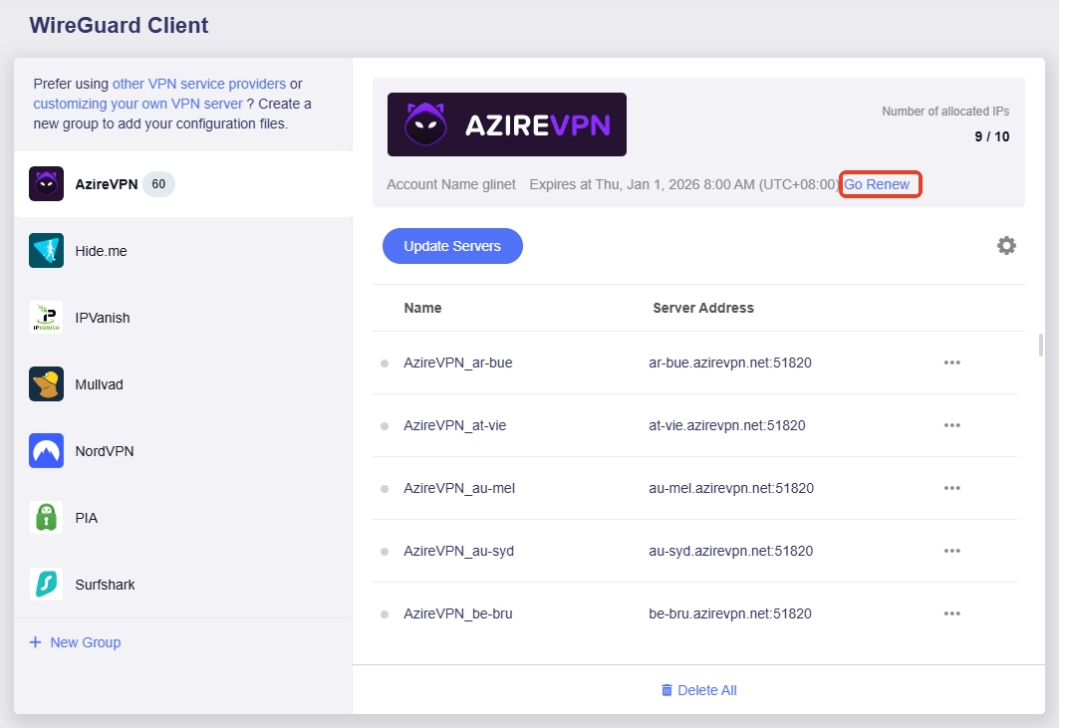


6. Modifiez les identifiants ou déconnectez-vous.
   Cliquez sur l'engrenage pour modifier vos identifiants ou vous déconnecter.

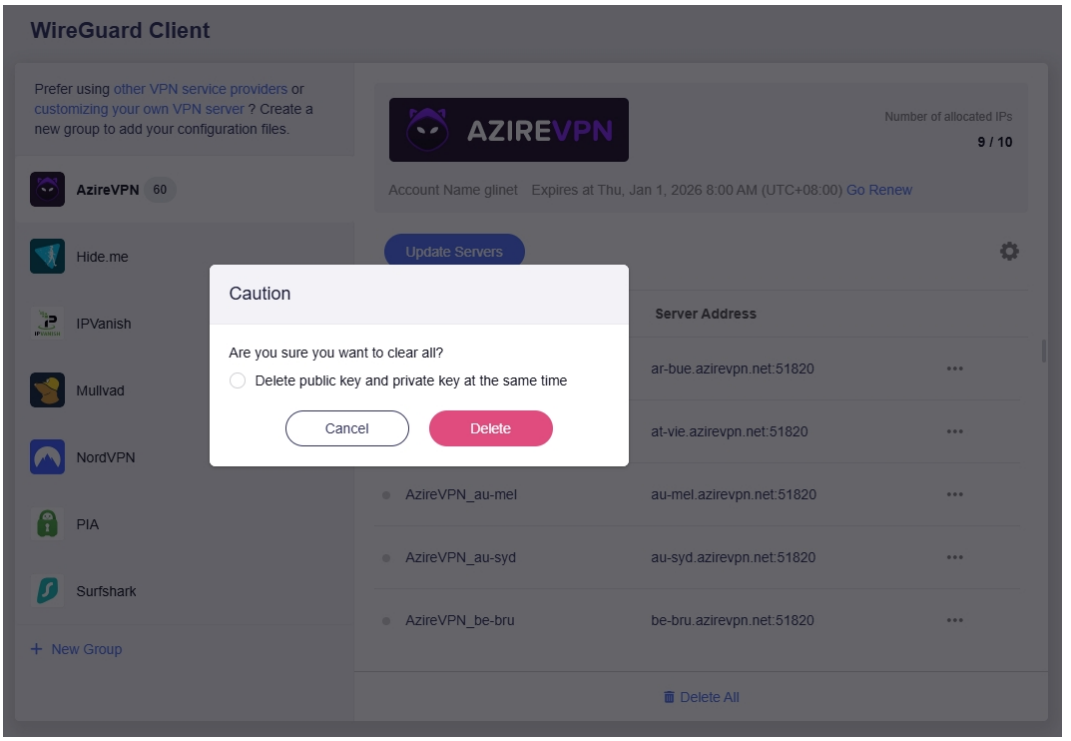


7. Renouvelez l'abonnement.

Cliquez sur **Renouveler (Go Renew)** pour ouvrir le site officiel et renouveler votre abonnement.



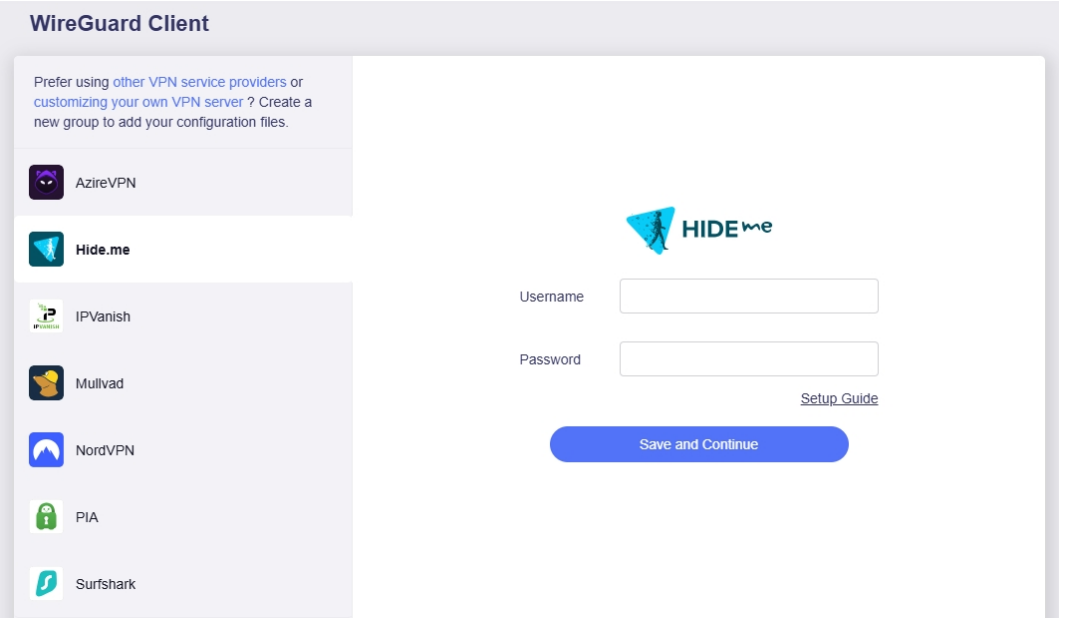
8. Supprimez tous les fichiers.
   Cliquez sur **Tout supprimer (Delete All)** pour supprimer tous les fichiers de configuration en un clic. Vous pouvez choisir de supprimer également les clés privée et publique.


WireGuard Client
Prefer using other VPN service providers or customizing your own VPN server ? Create a new group to add your configuration files.
AzireVPN 60
Hide.me
IPVanish
Mullvad
NordVPN
PIA
Surfshark
New Group
AZIREVPN
Number of allocated IPs
9 / 10
Account Name glinet Expires at Thu, Jan 1, 2026 8:00 AM (UTC+08:00) Go Renew
Update Servers
Caution
Are you sure you want to clear all?
Delete public key and private key at the same time
Cancel
Delete
Server Address
ar-bue.azirevpn.net:51820
at-vie.azirevpn.net:51820
AzireVPN_au-mel
au-mel.azirevpn.net:51820
AzireVPN_au-syd
au-syd.azirevpn.net:51820
AzireVPN_be-bru
be-bru.azirevpn.net:51820
Delete All

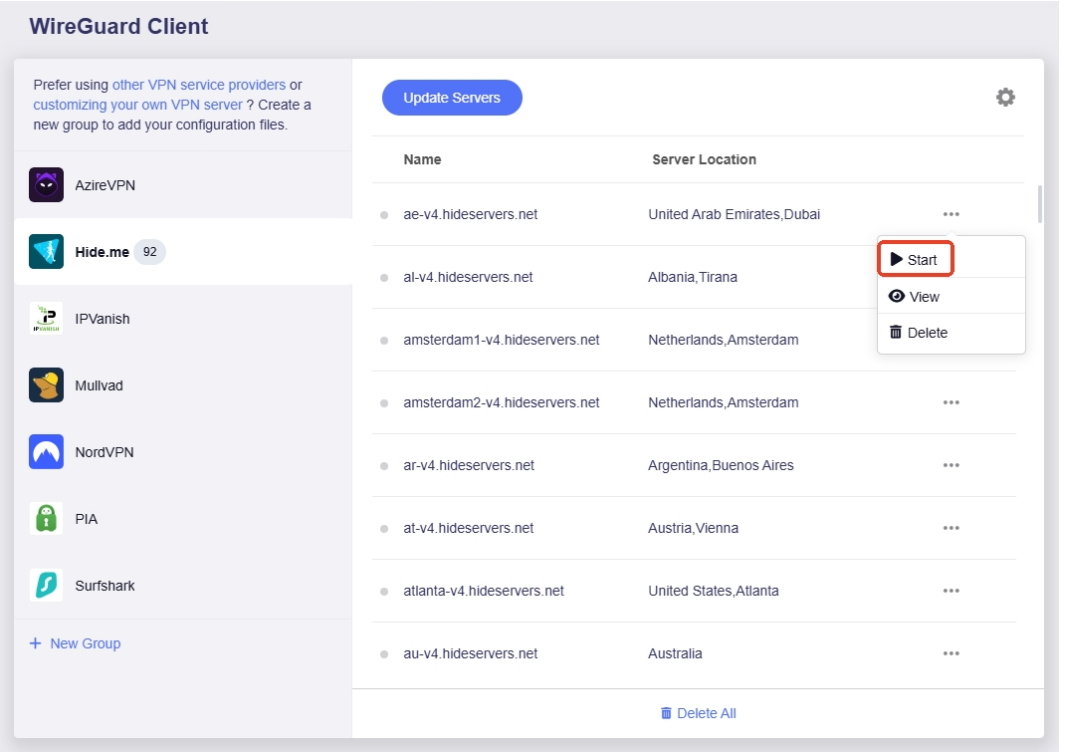
11.2.3 Configuration de Hide.me

Suivez les étapes ci-dessous pour configurer le routeur comme client Hide.me.

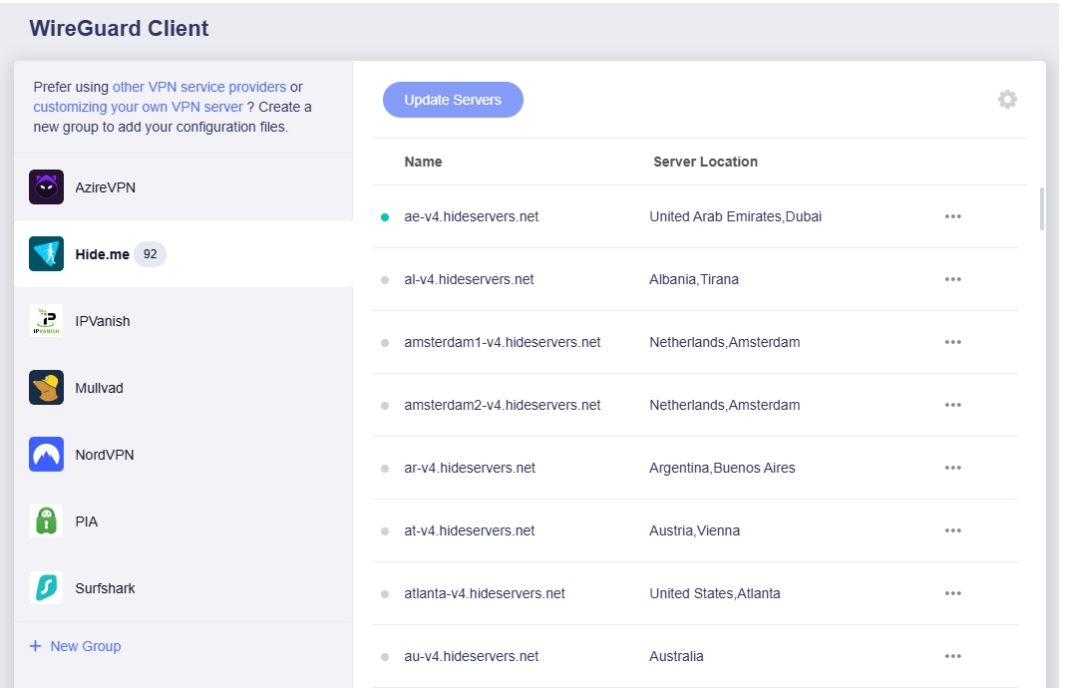
1. Connectez-vous à l'interface d'administration Web du routeur et ouvrez **VPN** > **Client WireGuard (WireGuard Client)** > **Hide.me**.
2. Saisissez l'identifiant et le mot de passe, puis cliquez sur **Enregistrer et continuer (Save and Continue)**. Les fichiers de configuration de chaque serveur sont générés.



3. Choisissez un serveur et cliquez sur les trois points à droite pour lancer la connexion.



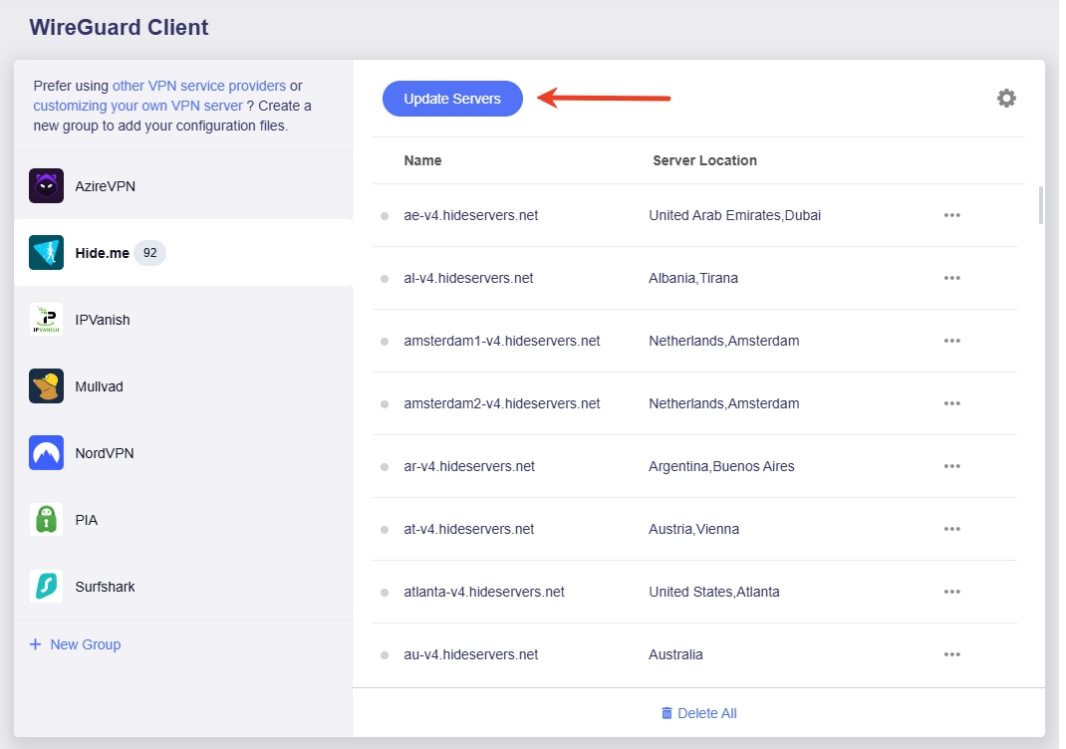
4. Une fois la connexion établie, un point vert apparaît à côté du fichier de configuration.



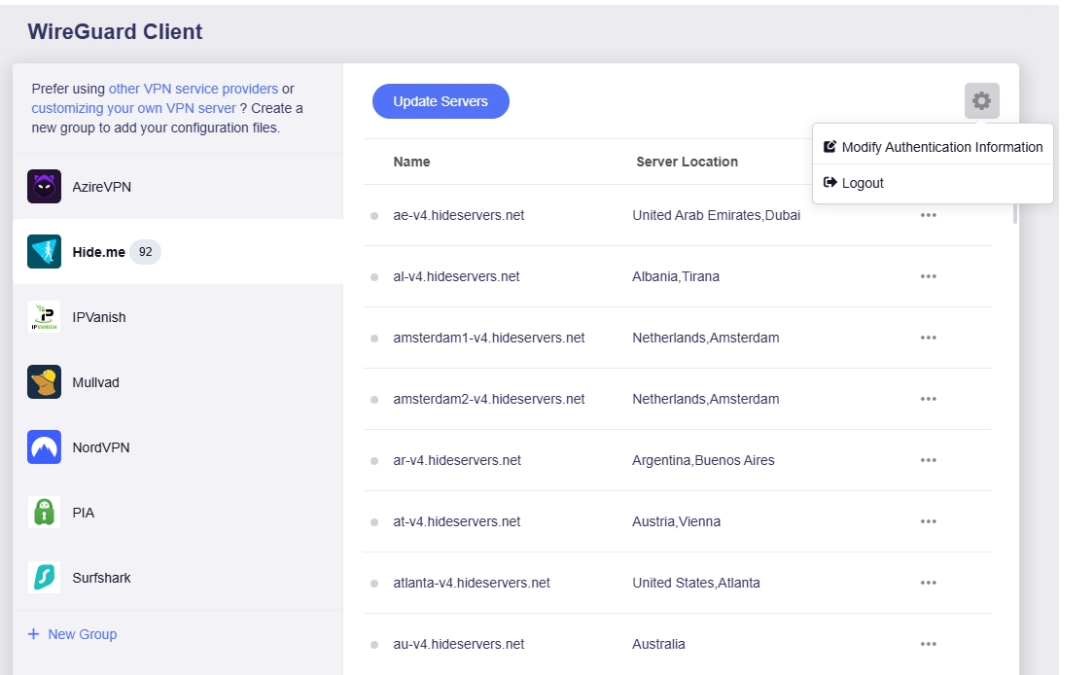
Vous pouvez également consulter les détails de la connexion dans le **Tableau de bord VPN (VPN Dashboard)**.

5. Mettez à jour les serveurs.

Cliquez sur **Mettre à jour les serveurs (Update Servers)** pour récupérer la liste à jour des serveurs disponibles et éviter les échecs liés à leur maintenance ou à leur arrêt.

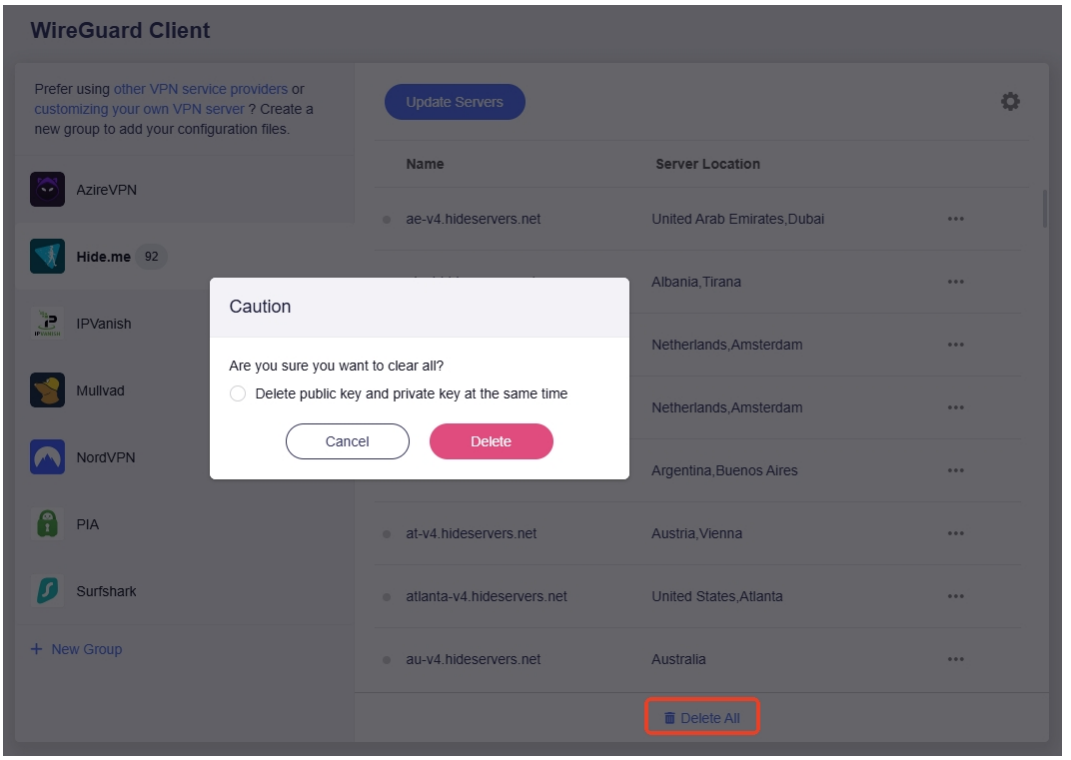


6. Modifiez les identifiants ou déconnectez-vous.
   Cliquez sur l'engrenage pour modifier vos identifiants ou vous déconnecter.



7. Supprimez tous les fichiers.

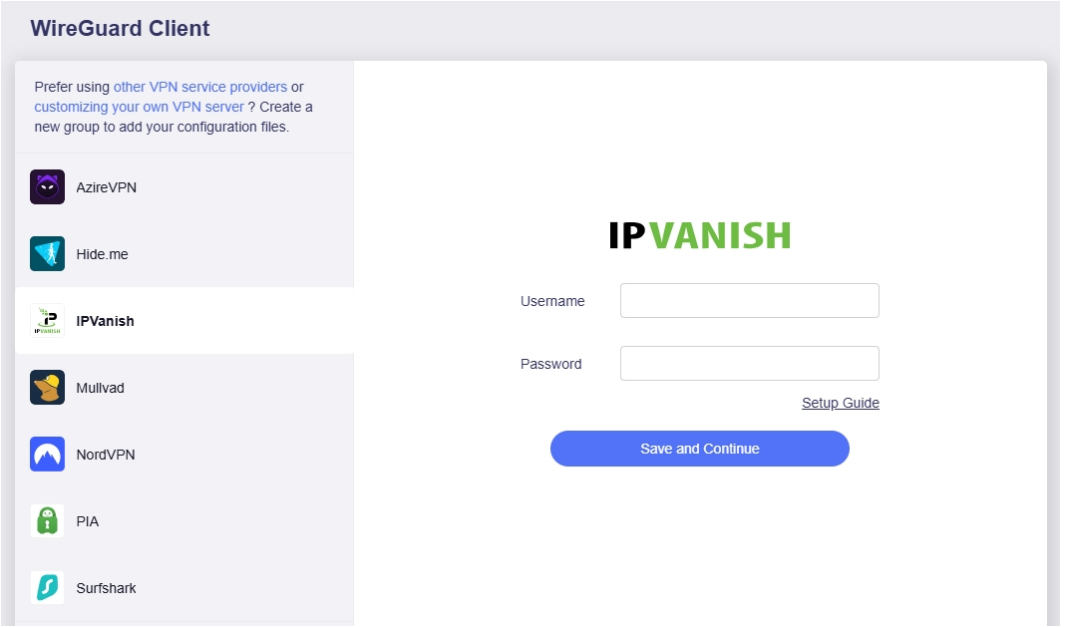
Cliquez sur **Tout supprimer (Delete All)** pour supprimer tous les fichiers de configuration en un clic. Vous pouvez choisir de supprimer également les clés privée et publique.



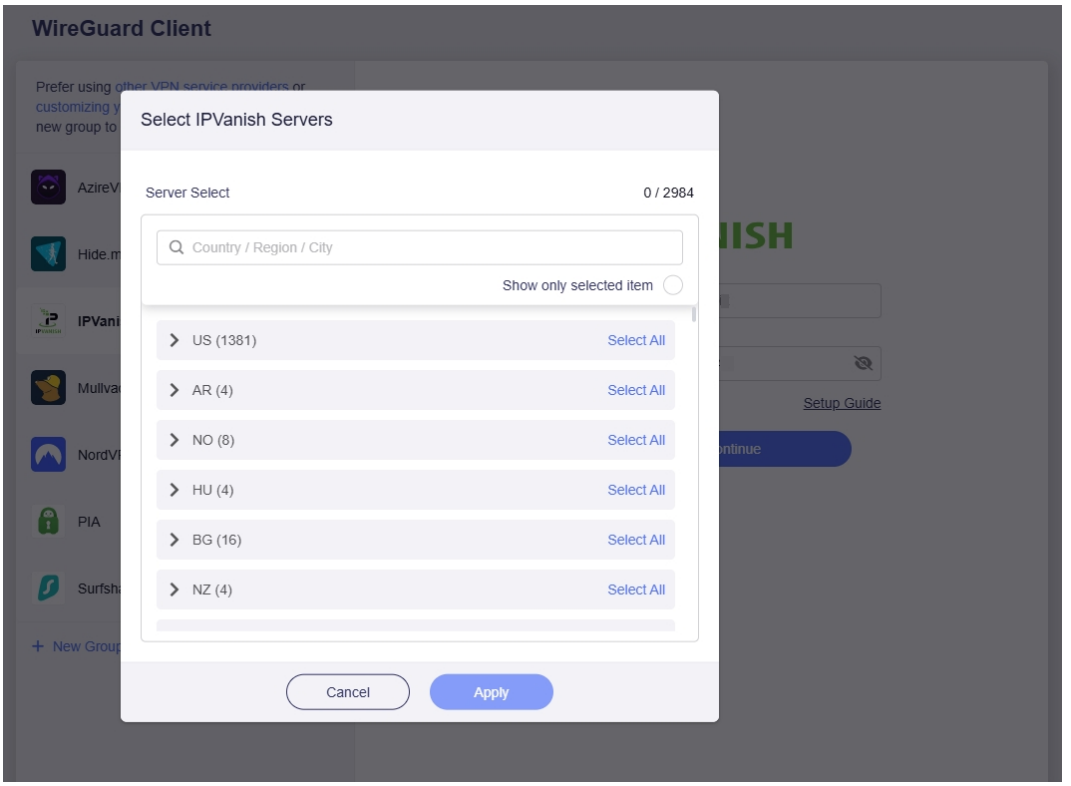
11.2.4 Configuration d'IPVanish

Suivez les étapes ci-dessous pour configurer le routeur comme client IPVanish.

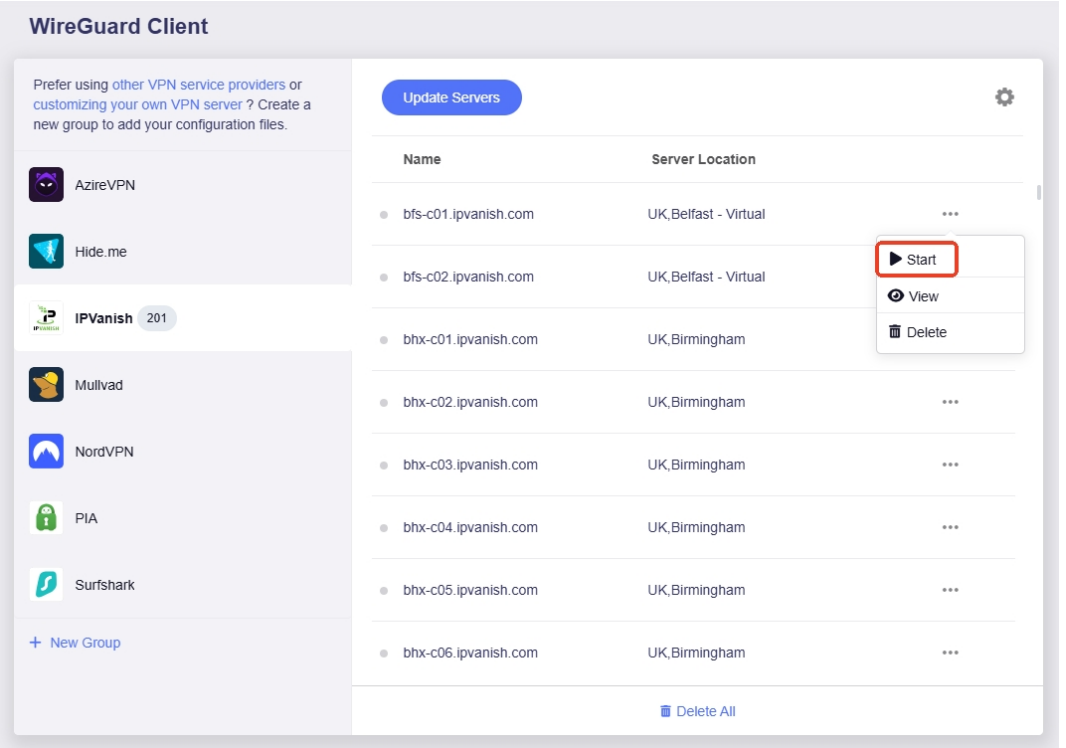
1. Connectez-vous à l'interface d'administration Web du routeur et ouvrez **VPN** > **Client WireGuard (WireGuard Client)** > **IPVanish**.
2. Saisissez l'identifiant et le mot de passe, puis cliquez sur **Enregistrer et continuer (Save and Continue)**.



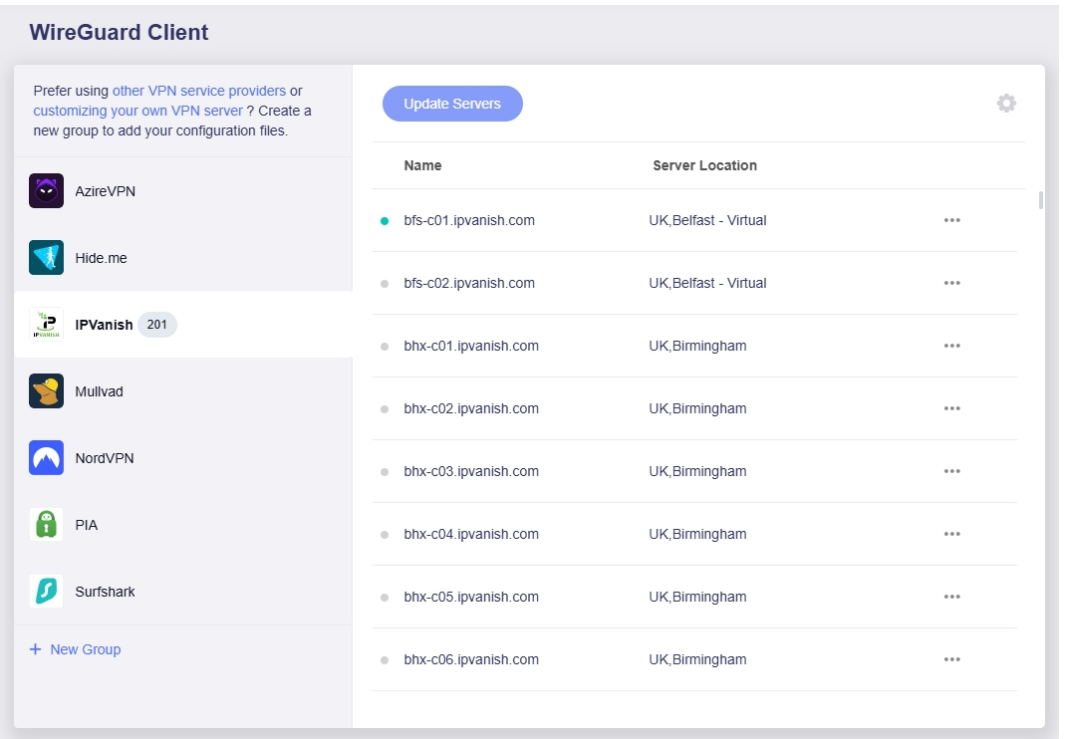
3. Sélectionnez les serveurs souhaités et cliquez sur **Appliquer (Apply)**.



4. Choisissez un serveur et cliquez sur les trois points à droite pour lancer la connexion.



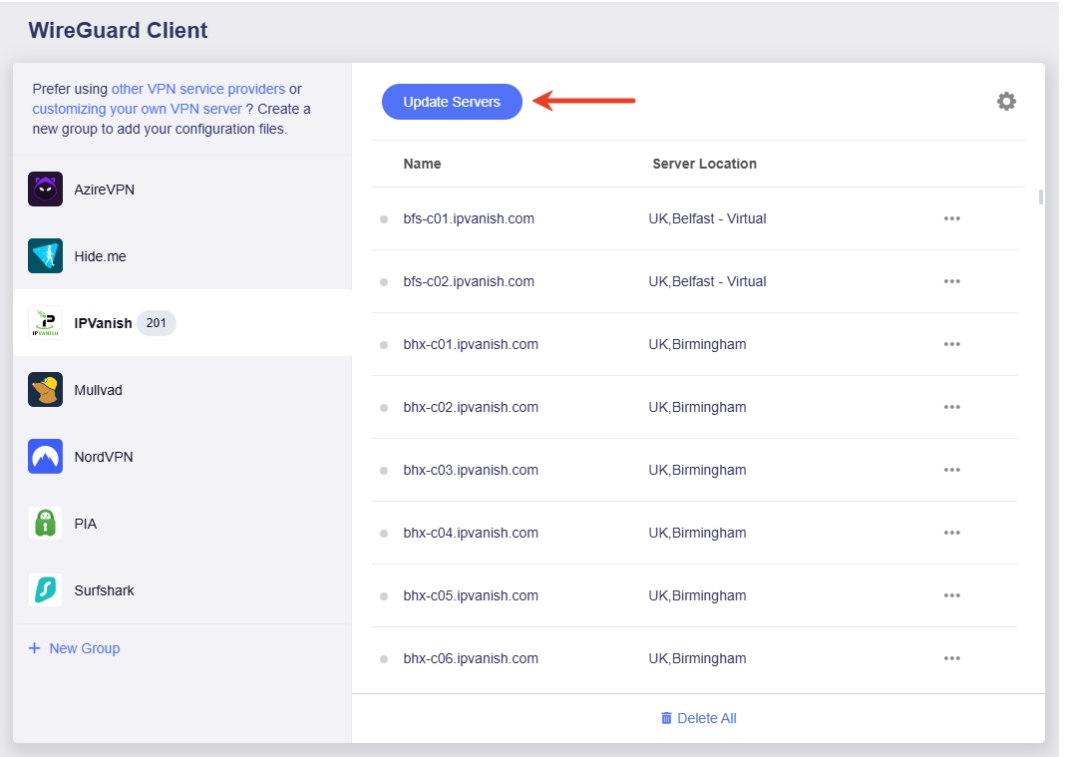
5. Une fois la connexion établie, un point vert apparaît à côté du fichier de configuration.



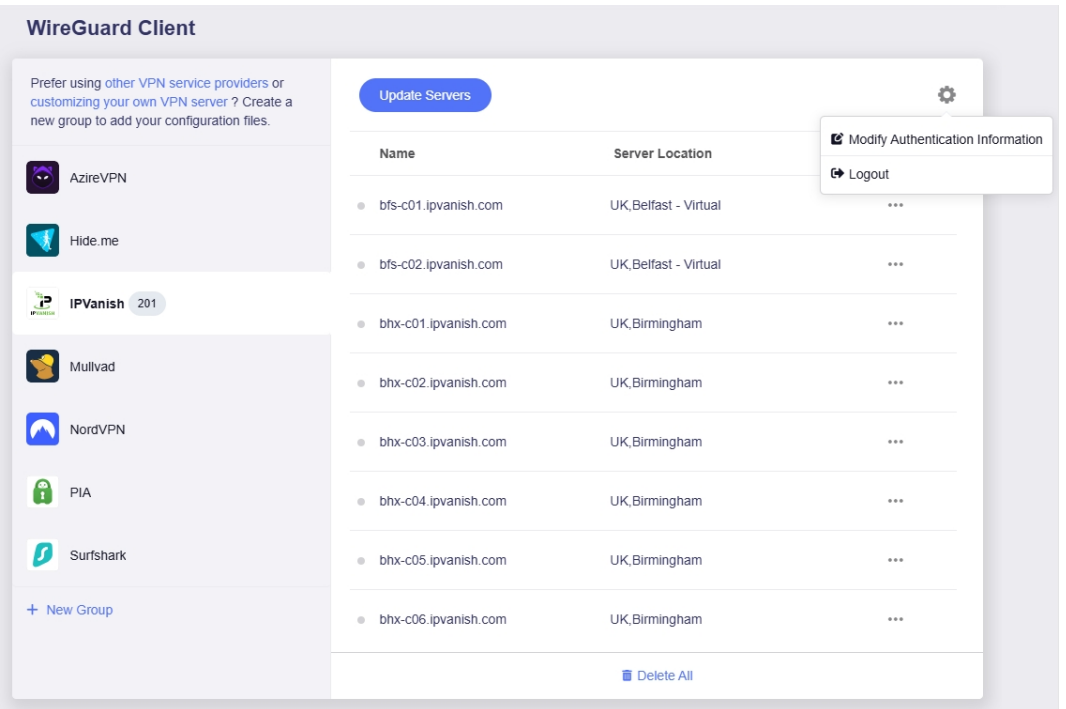
Vous pouvez également consulter les détails de la connexion dans le **Tableau de bord VPN (VPN Dashboard)**.

6. Mettez à jour les serveurs.

Cliquez sur **Mettre à jour les serveurs (Update Servers)** pour récupérer la liste à jour des serveurs disponibles et éviter les échecs liés à leur maintenance ou à leur arrêt.

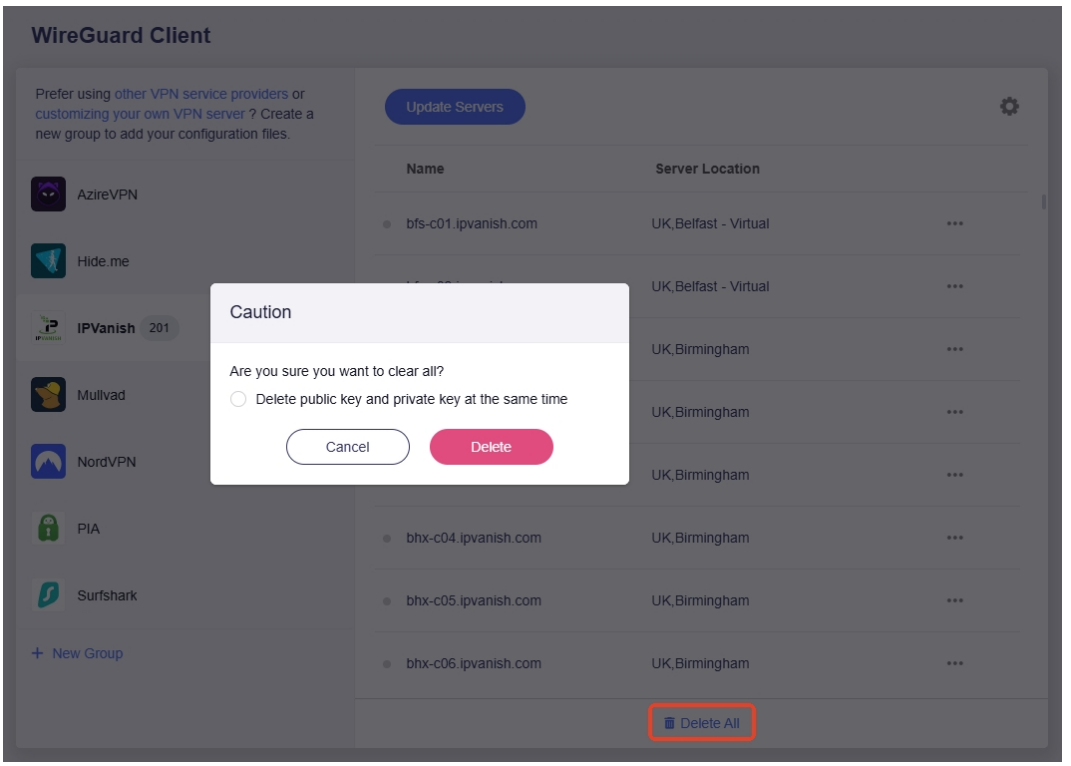


7. Modifiez les identifiants ou déconnectez-vous.
   Cliquez sur l'engrenage pour modifier vos identifiants ou vous déconnecter.



8. Supprimez tous les fichiers.

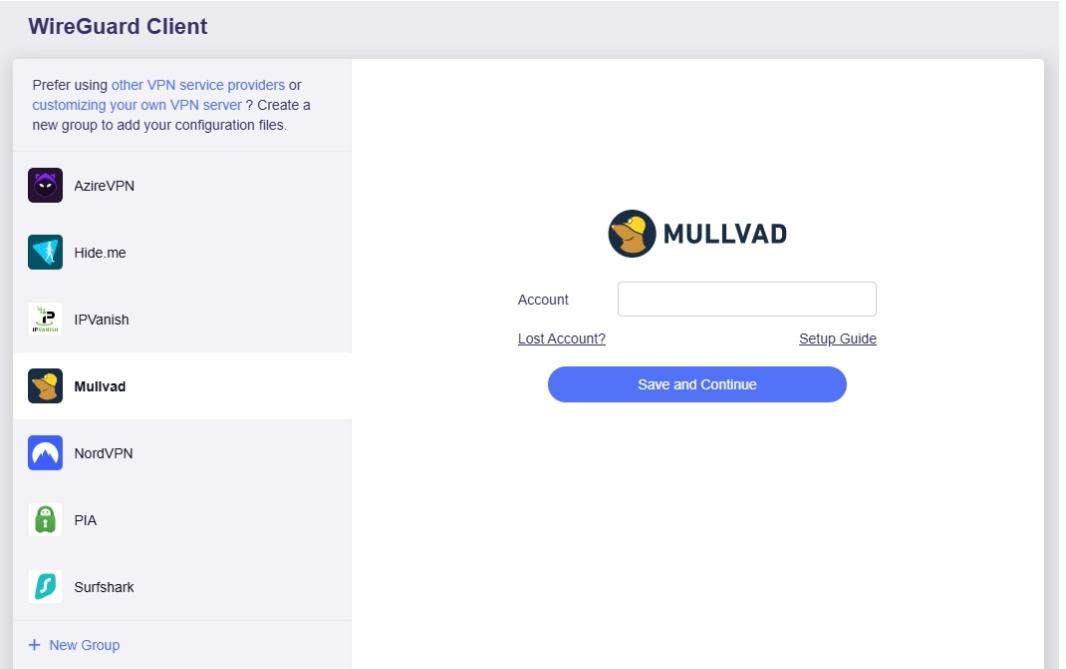
   Cliquez sur **Tout supprimer (Delete All)** pour supprimer tous les fichiers de configuration en un clic. Vous pouvez choisir de supprimer également les clés privée et publique.



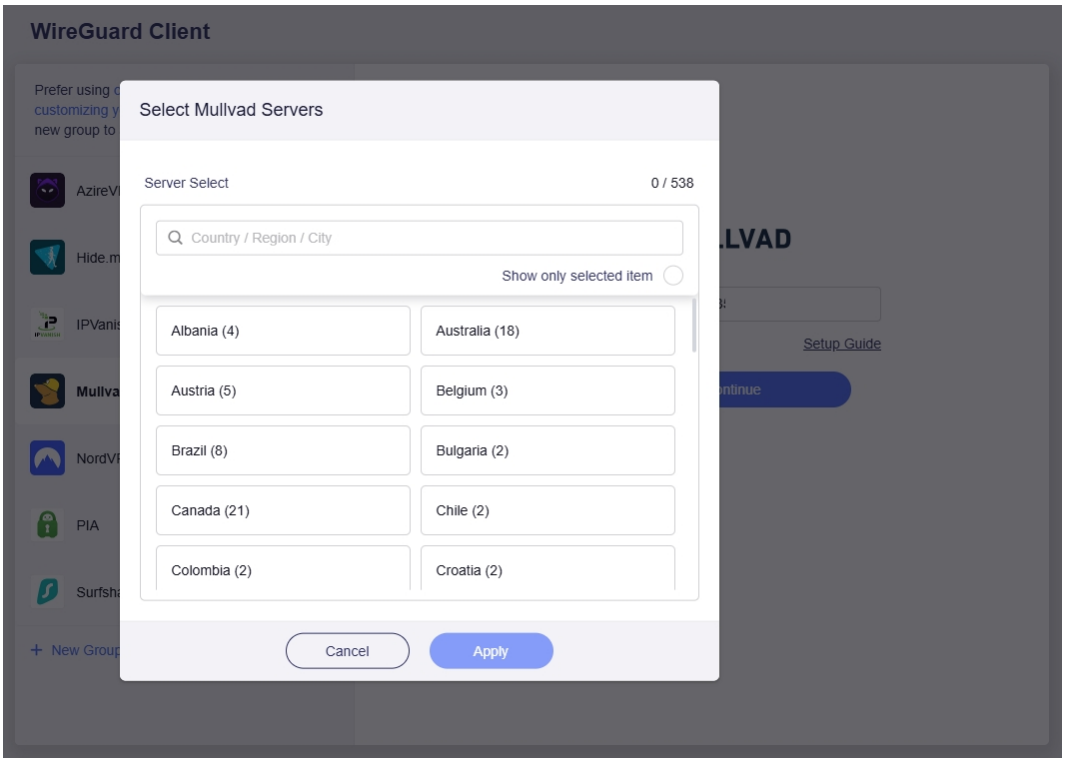
11.2.5 Configuration de Mullvad

Suivez les étapes ci-dessous pour configurer le routeur comme client Mullvad.

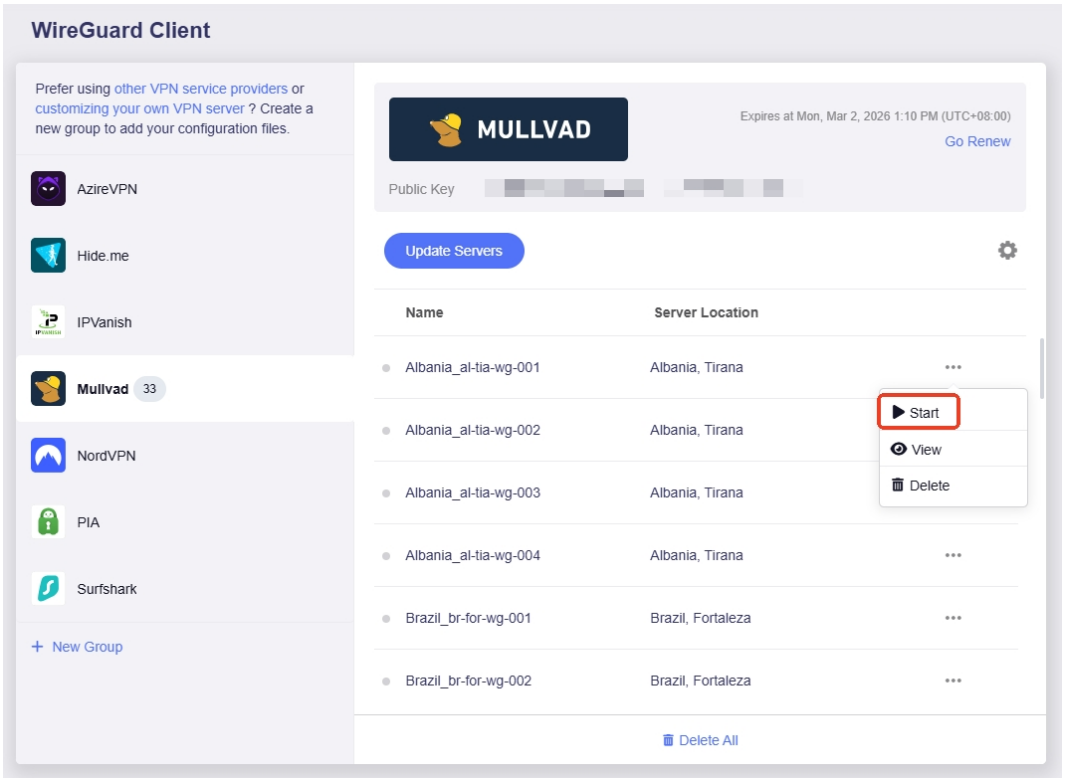
1. Connectez-vous à l'interface d'administration Web du routeur et ouvrez **VPN** > **Client WireGuard (WireGuard Client)** > **Mullvad**.
2. Saisissez l'identifiant et le mot de passe, puis cliquez sur **Enregistrer et continuer (Save and Continue)**.



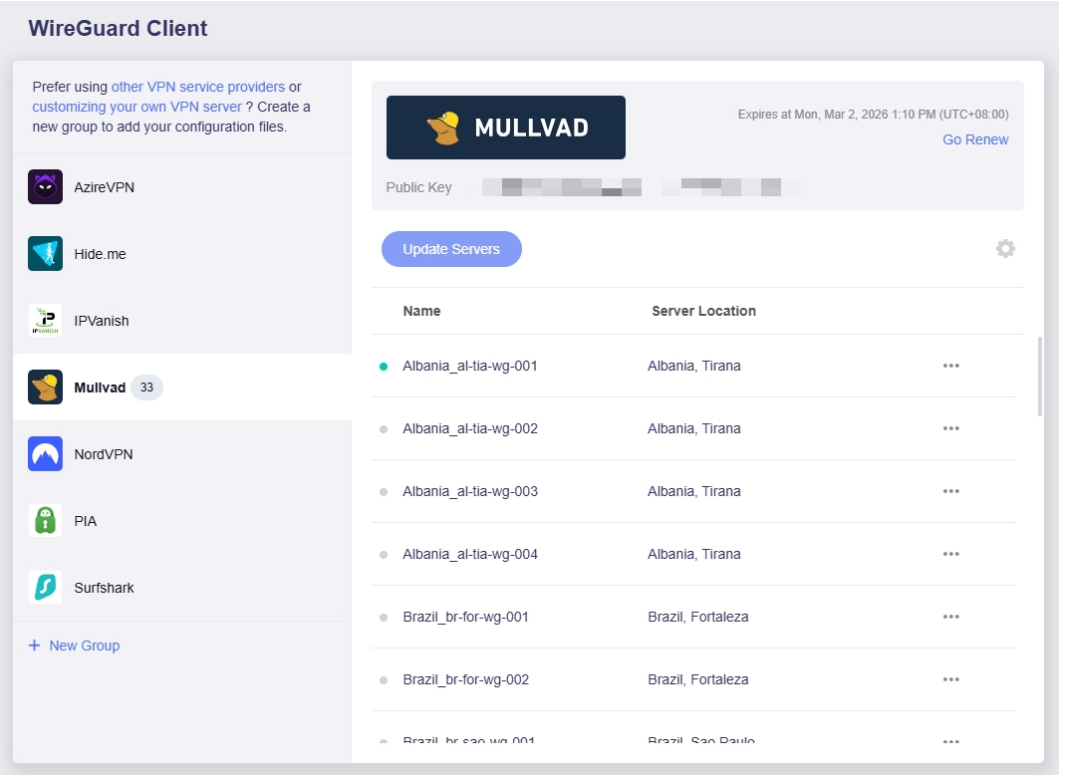
3. Sélectionnez les serveurs souhaités et cliquez sur **Appliquer (Apply)**.



4. Choisissez un serveur et cliquez sur les trois points à droite pour lancer la connexion.



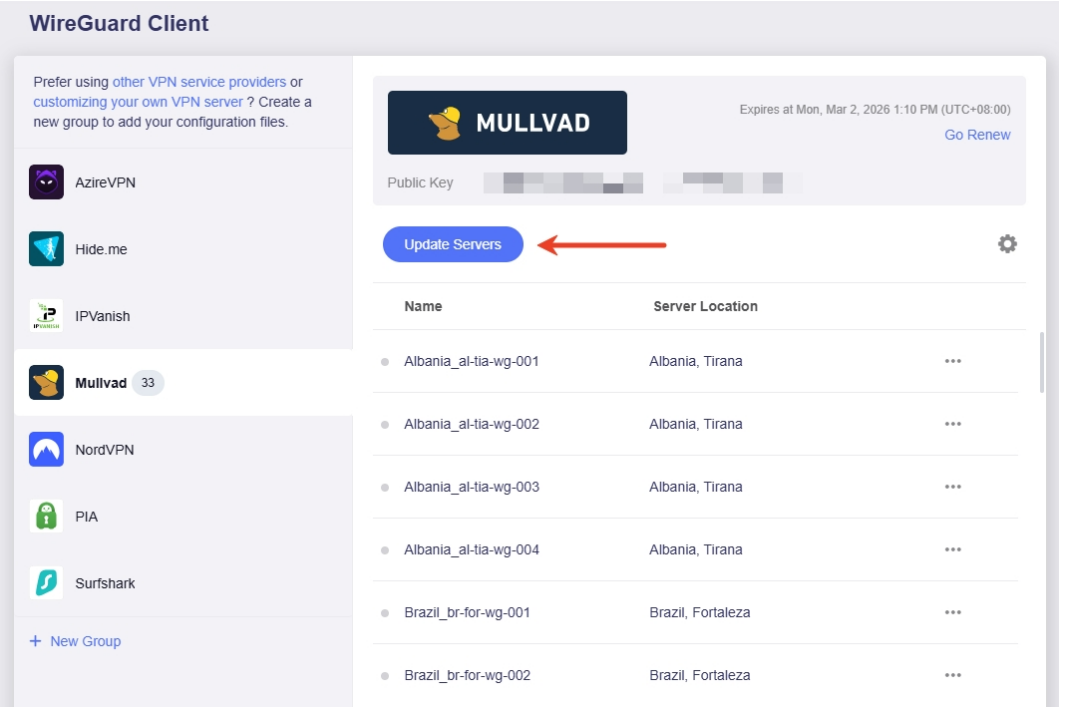
5. Une fois la connexion établie, un point vert apparaît à côté du fichier de configuration.



Vous pouvez également consulter les détails de la connexion dans le **Tableau de bord VPN (VPN Dashboard)**.

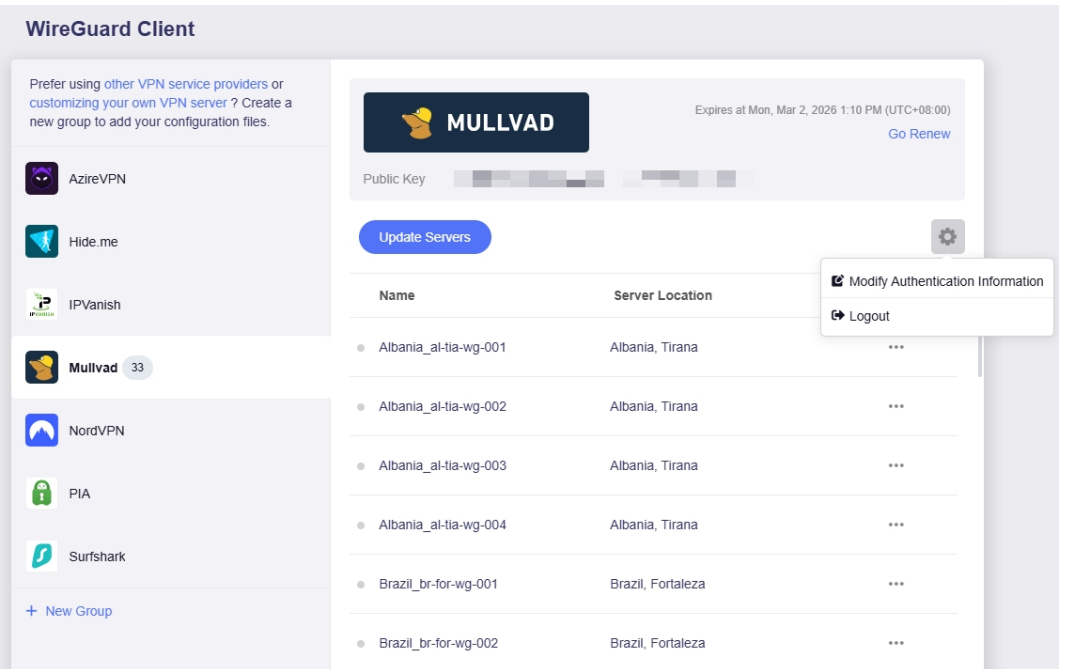
6. Mettez à jour les serveurs.

   Cliquez sur **Mettre à jour les serveurs (Update Servers)** pour récupérer la liste à jour des serveurs disponibles et éviter les échecs liés à leur maintenance ou à leur arrêt.



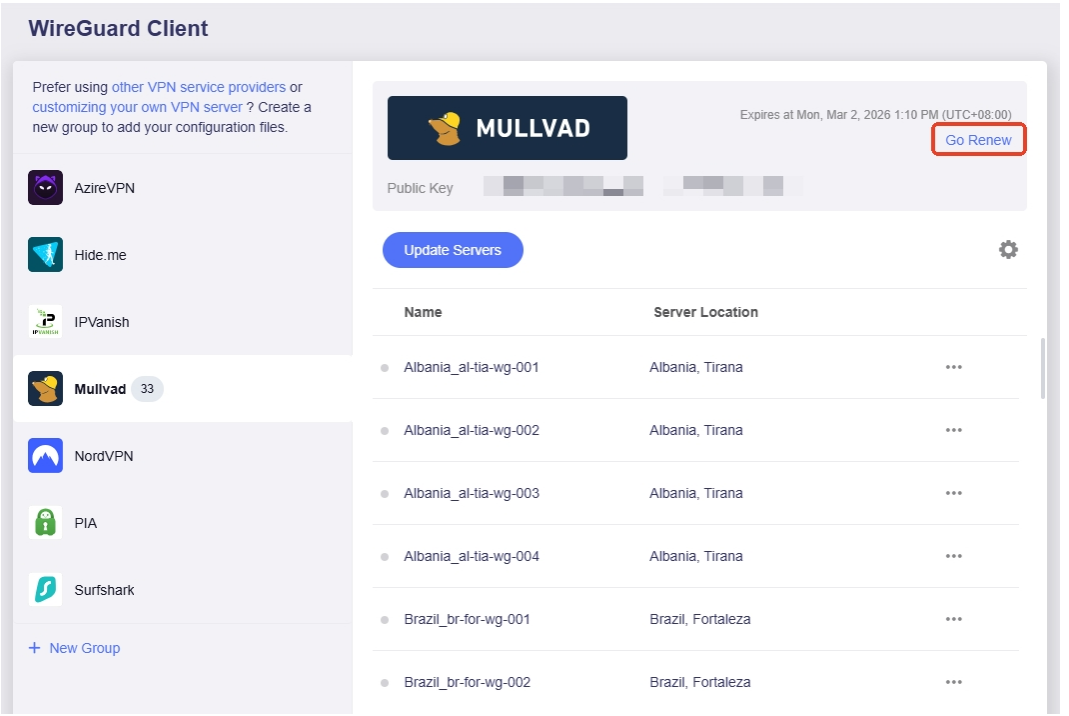
7. Modifiez les identifiants ou déconnectez-vous.

   Cliquez sur l’engrenage pour modifier vos identifiants ou vous déconnecter.



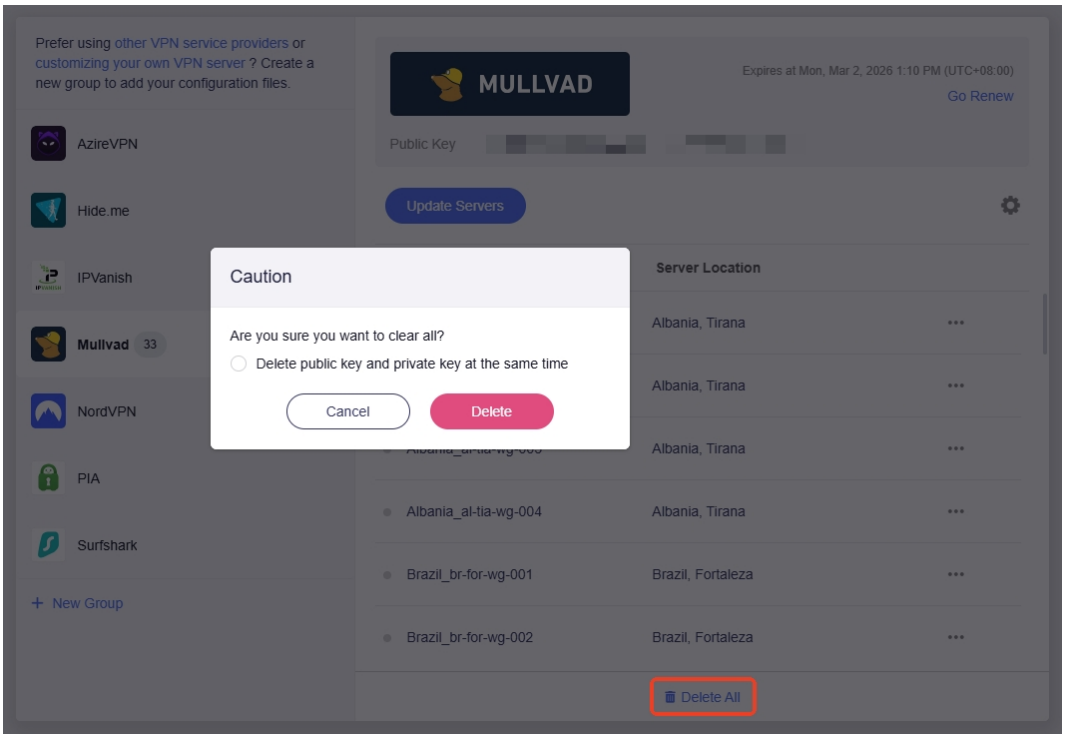
8. Renouvelez l’abonnement.

   Cliquez sur **Renouveler (Go Renew)** pour ouvrir le site officiel et renouveler votre abonnement.



9. Supprimez tous les fichiers.

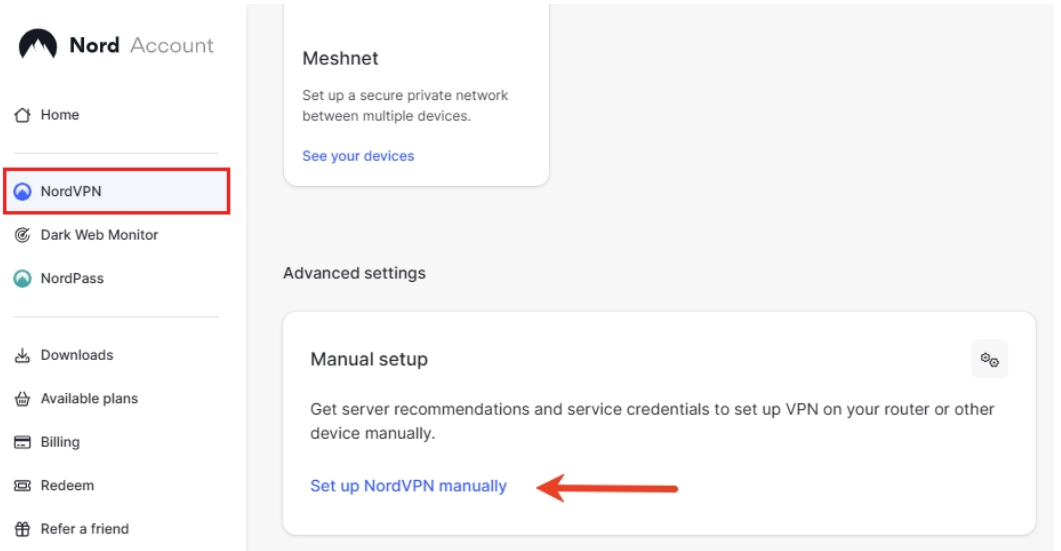
   Cliquez sur **Tout supprimer (Delete All)** pour supprimer tous les fichiers de configuration en un clic. Vous pouvez choisir de supprimer également les clés privée et publique.



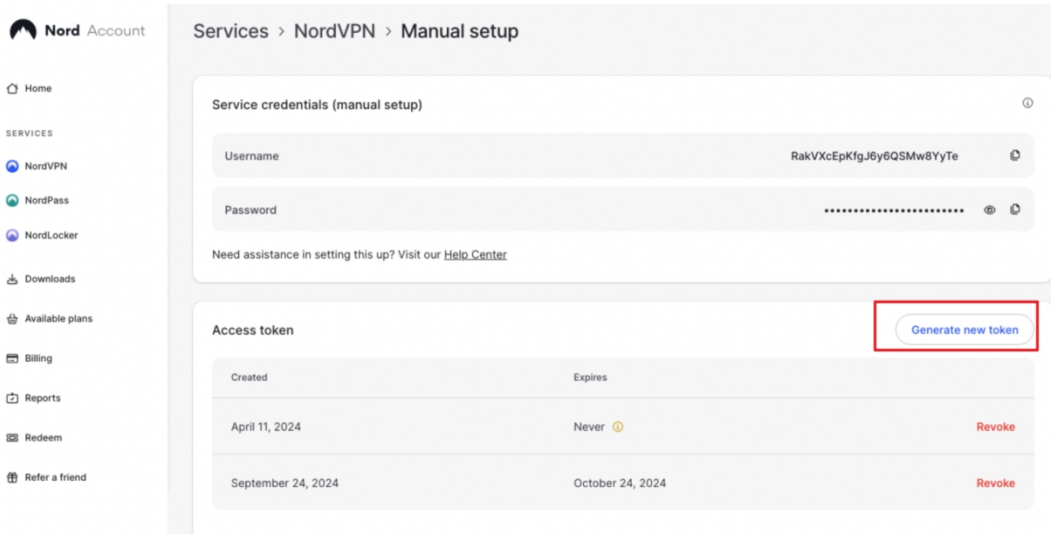
11.2.6 Configuration de NordVPN

Suivez les étapes ci-dessous pour configurer le routeur comme client NordVPN.

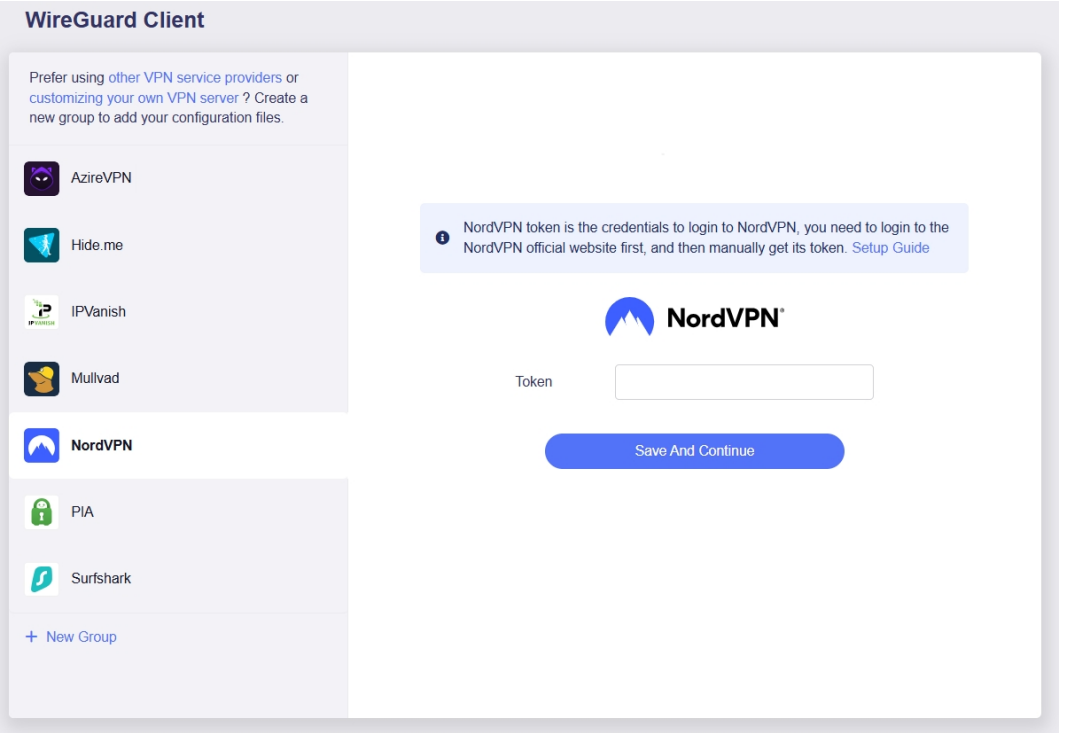
1. Connectez-vous à votre compte Web NordVPN ici.
2. Dans le tableau de bord Nord, cliquez sur **NordVPN**, puis sur **Configurer NordVPN manuellement (Set up NordVPN manually)**.



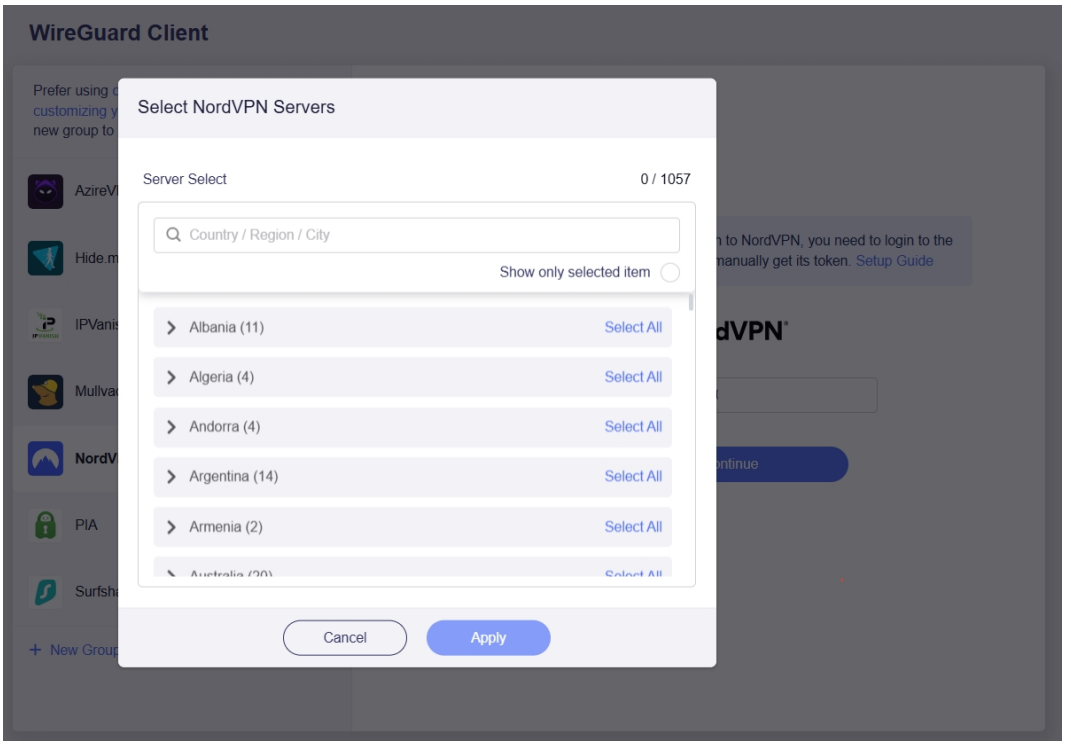
Repérez la section **Jeton d'accès (Access Token)**. Créez un jeton et copiez-le pour l'utiliser ensuite.



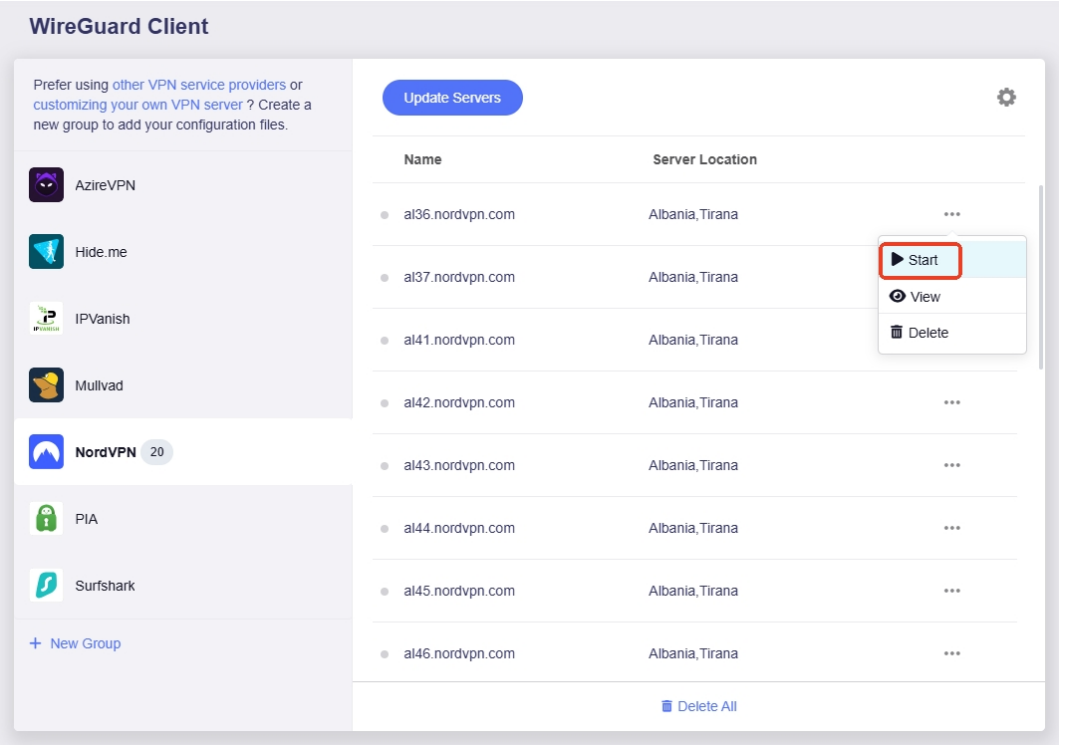
3. Connectez-vous à l'interface d'administration Web du routeur et ouvrez **VPN** > **Client WireGuard (WireGuard Client)** > **NordVPN**.
4. Saisissez le jeton et cliquez sur **Enregistrer et continuer (Save and Continue)**.



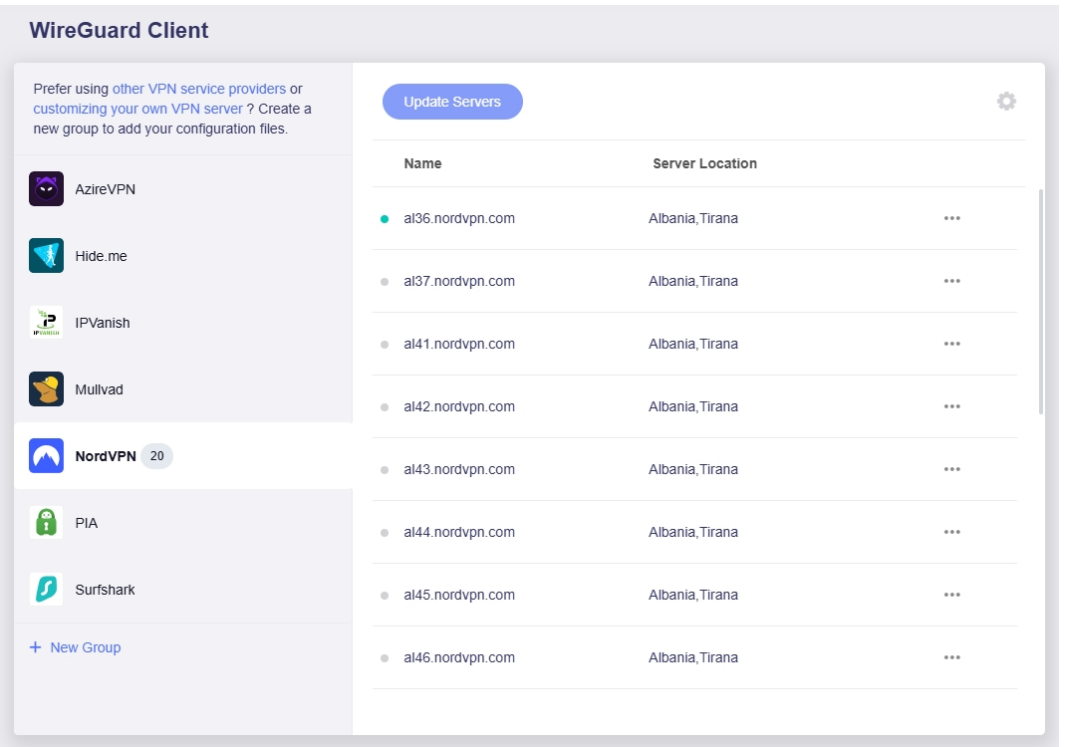
5. Sélectionnez les serveurs souhaités et cliquez sur **Appliquer (Apply)**.



6. Choisissez un serveur et cliquez sur les trois points à droite pour lancer la connexion.



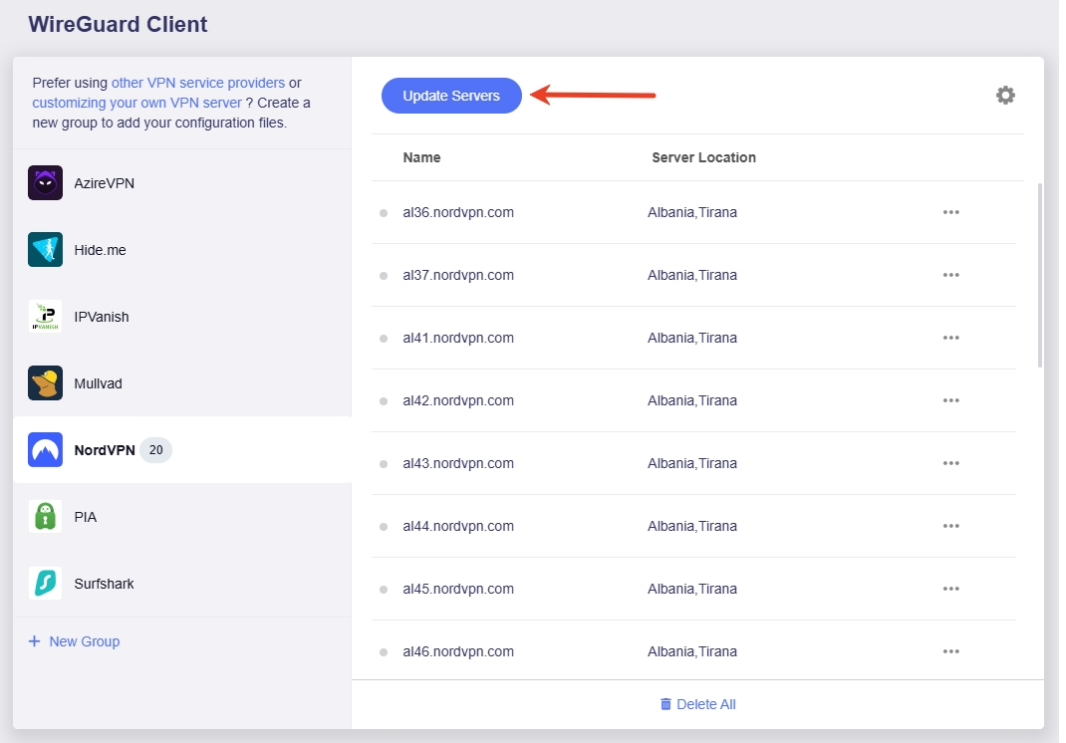
7. Une fois la connexion établie, un point vert apparaît à côté du fichier de configuration.



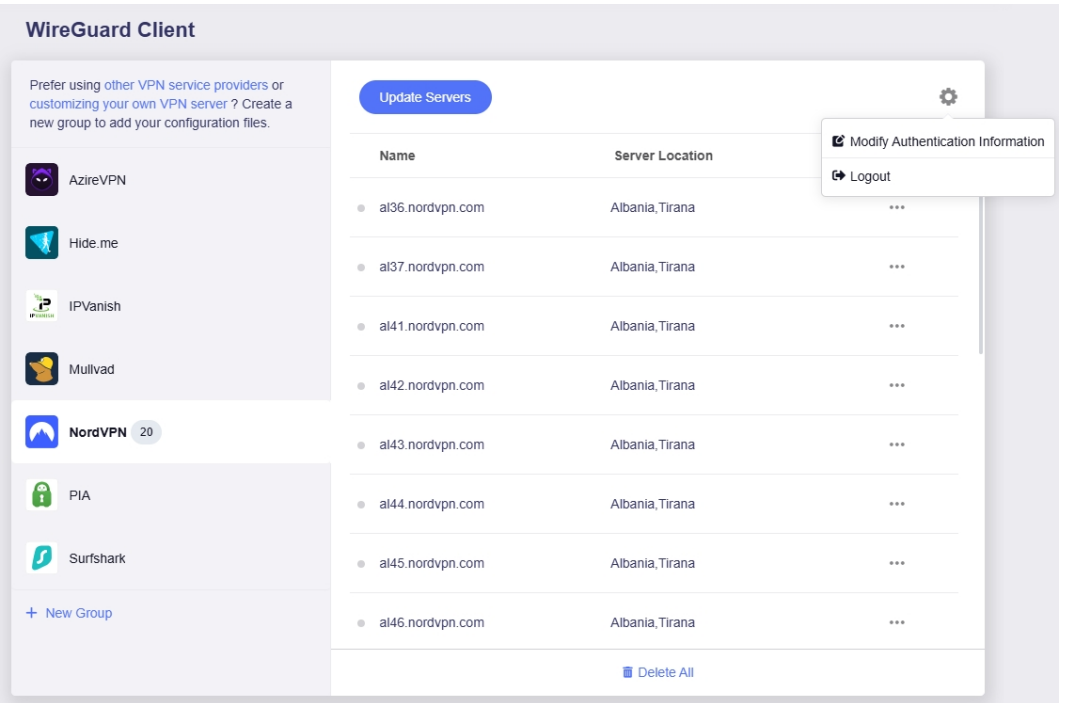
Vous pouvez également consulter les détails de la connexion dans le **Tableau de bord VPN (VPN Dashboard)**.

8. Mettez à jour les serveurs.

Cliquez sur **Mettre à jour les serveurs (Update Servers)** pour récupérer la liste à jour des serveurs disponibles et éviter les échecs liés à leur maintenance ou à leur arrêt.

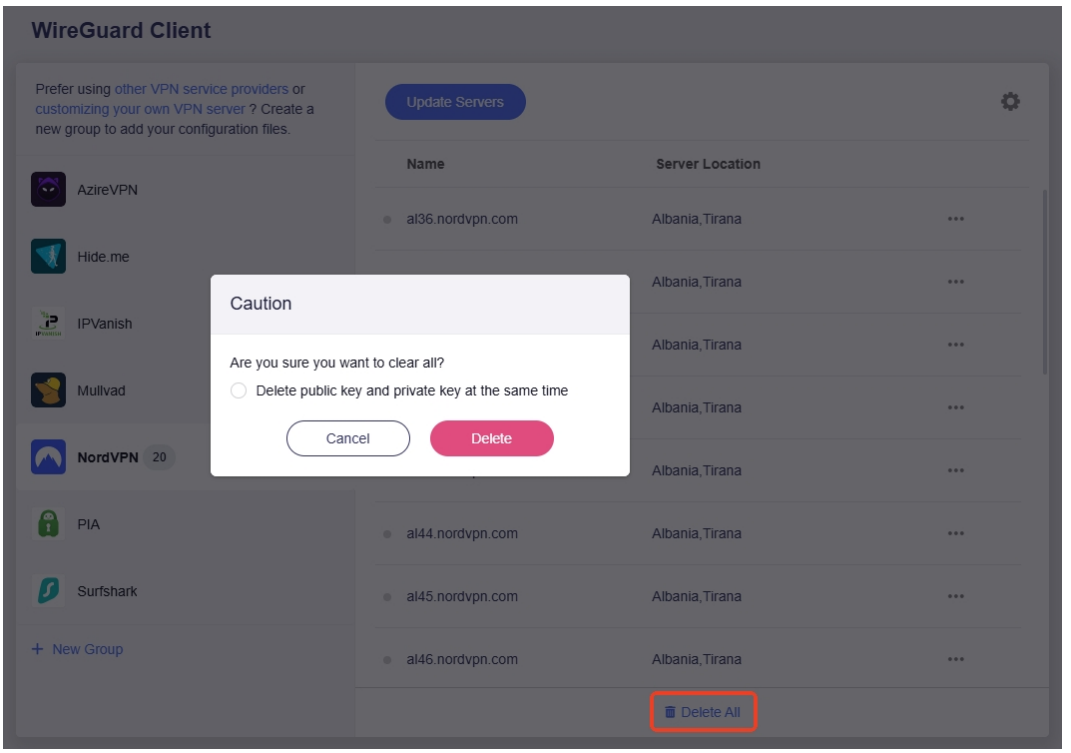


9. Modifiez les identifiants ou déconnectez-vous.
   Cliquez sur l'engrenage pour modifier vos identifiants ou vous déconnecter.



10. Supprimez tous les fichiers.

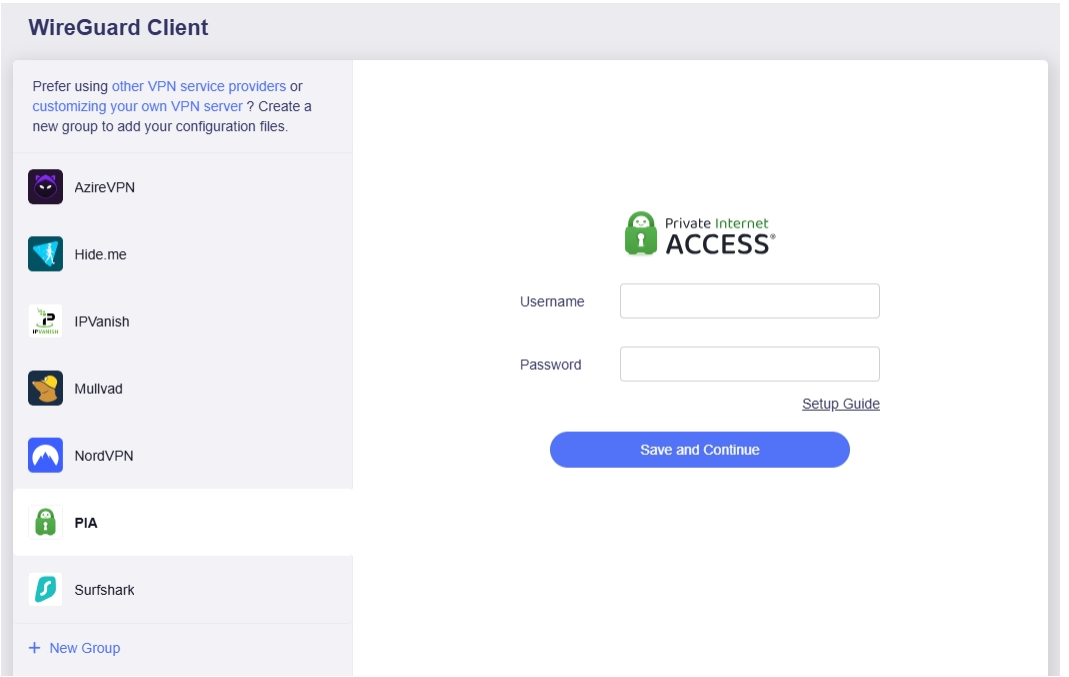
    Cliquez sur **Tout supprimer (Delete All)** pour supprimer tous les fichiers de configuration en un clic. Vous pouvez choisir de supprimer également les clés privée et publique.



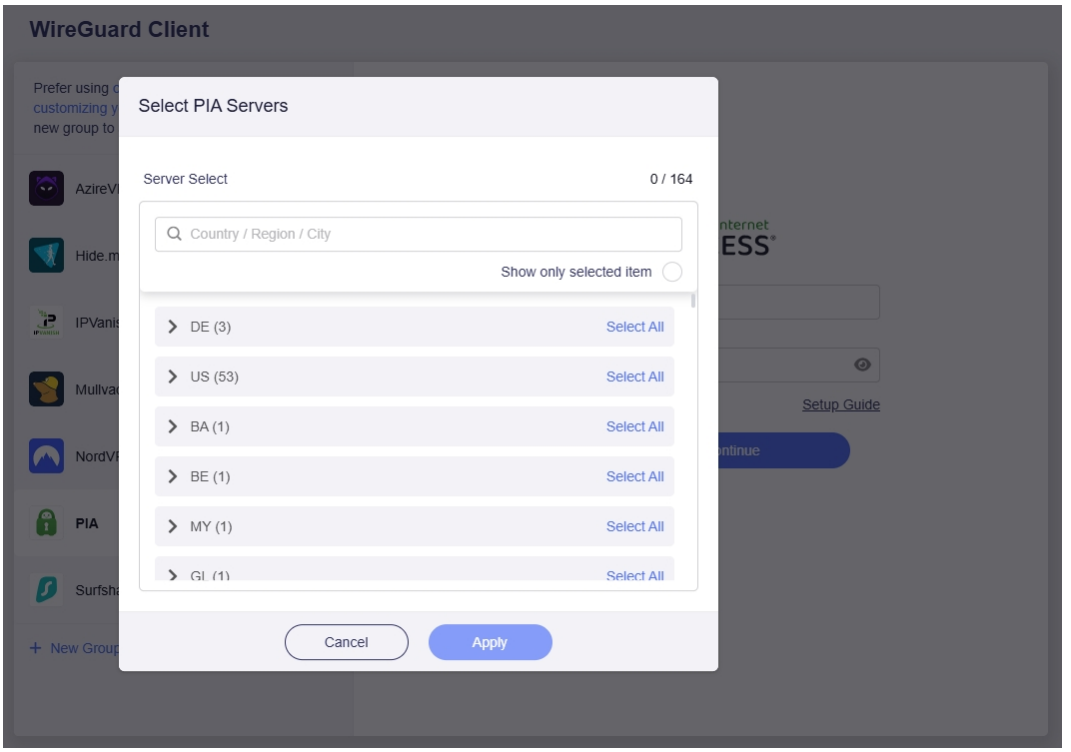
11.2.7 Configuration de PIA (Private Internet Access)

Suivez les étapes ci-dessous pour configurer le routeur comme client PIA.

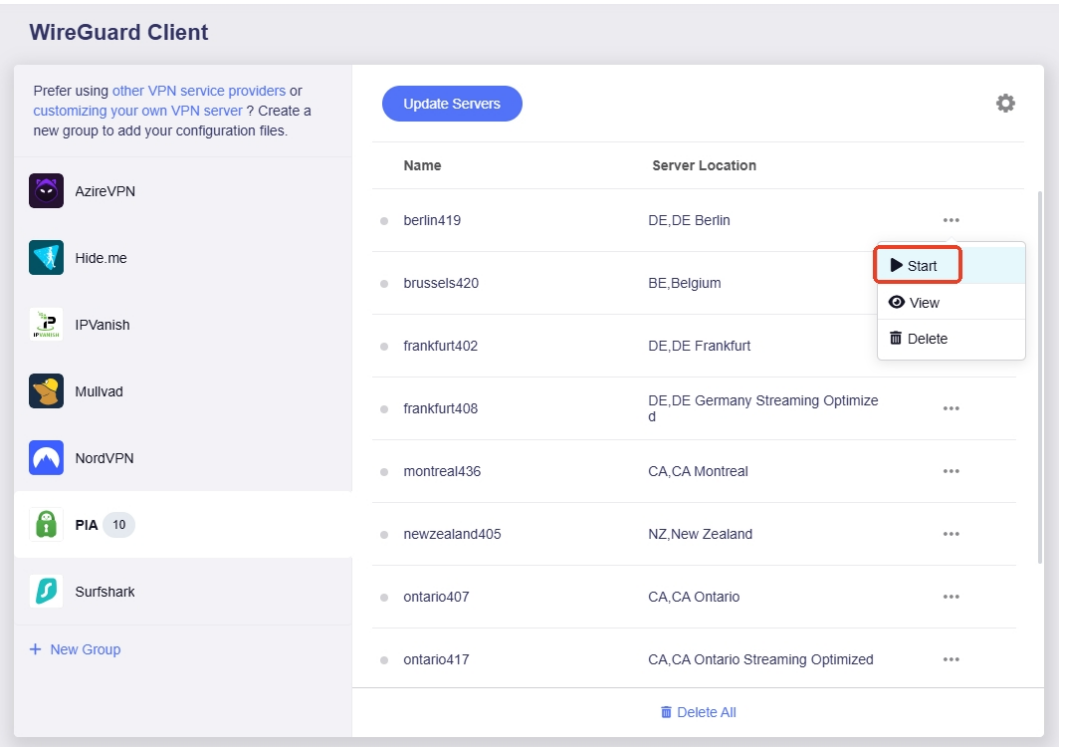
1. Connectez-vous à l'interface d'administration Web du routeur et ouvrez **VPN** > **Client WireGuard (WireGuard Client)** > **PIA**.
2. Saisissez l'identifiant et le mot de passe, puis cliquez sur **Enregistrer et continuer (Save and Continue)**.



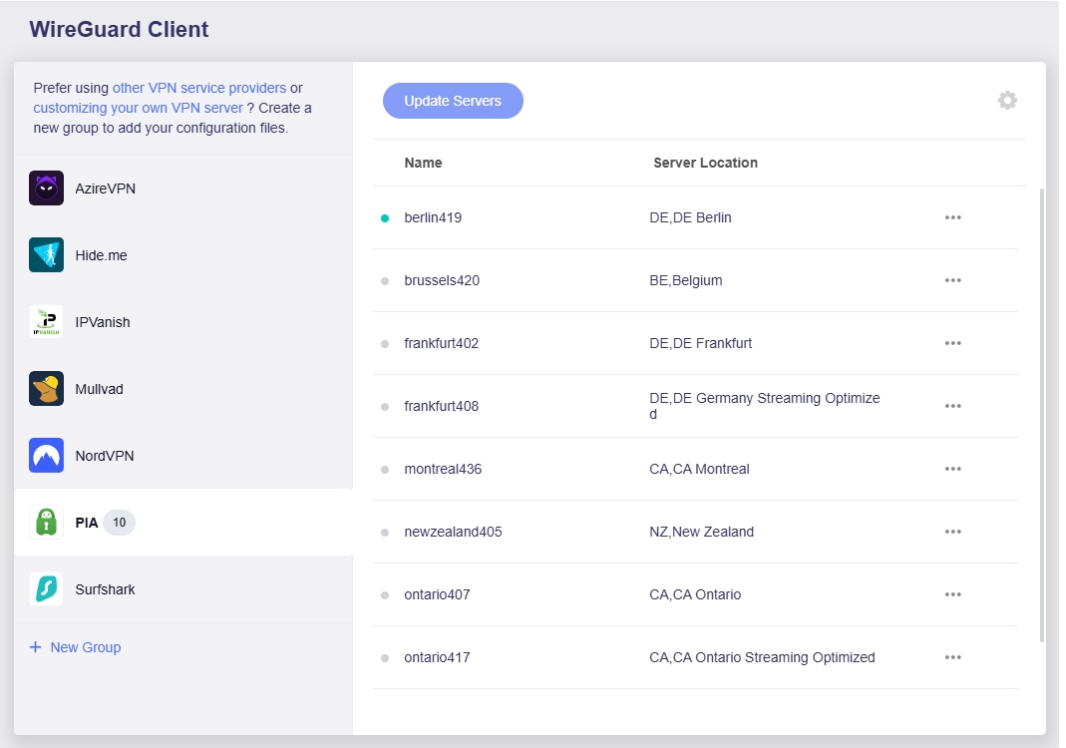
3. Sélectionnez les serveurs souhaités et cliquez sur **Appliquer (Apply)**.



4. Choisissez un serveur et cliquez sur les trois points à droite pour lancer la connexion.



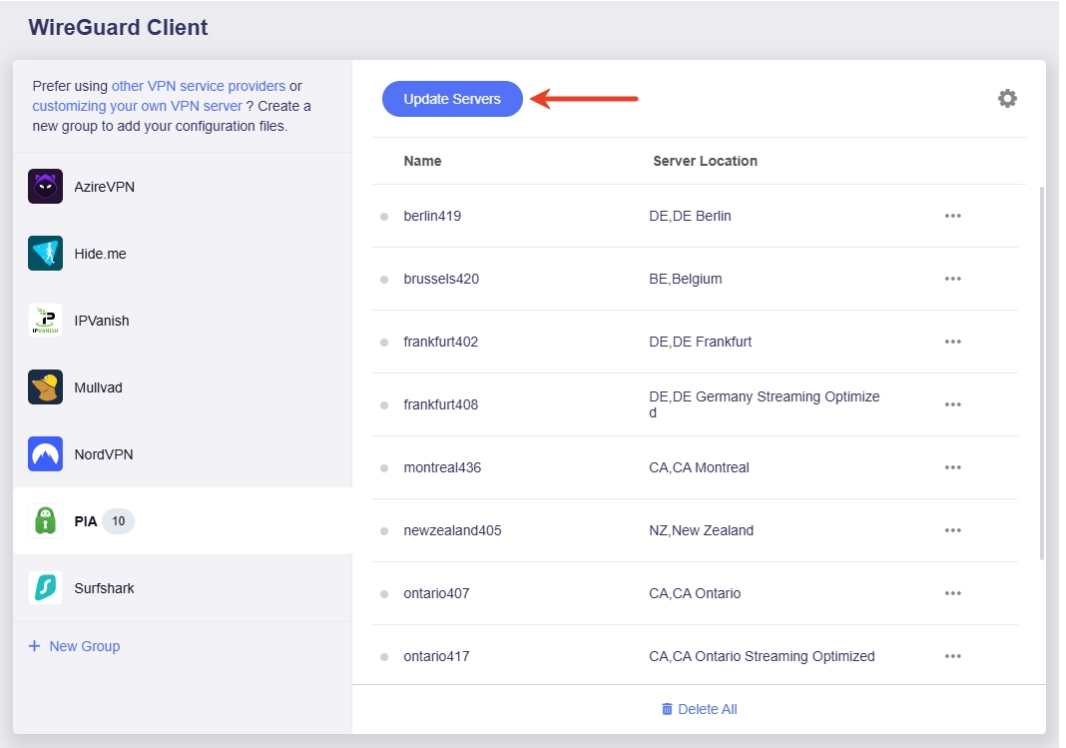
5. Une fois la connexion établie, un point vert apparaît à côté du fichier de configuration.



Vous pouvez également consulter les détails de la connexion dans le **Tableau de bord VPN (VPN Dashboard)**.

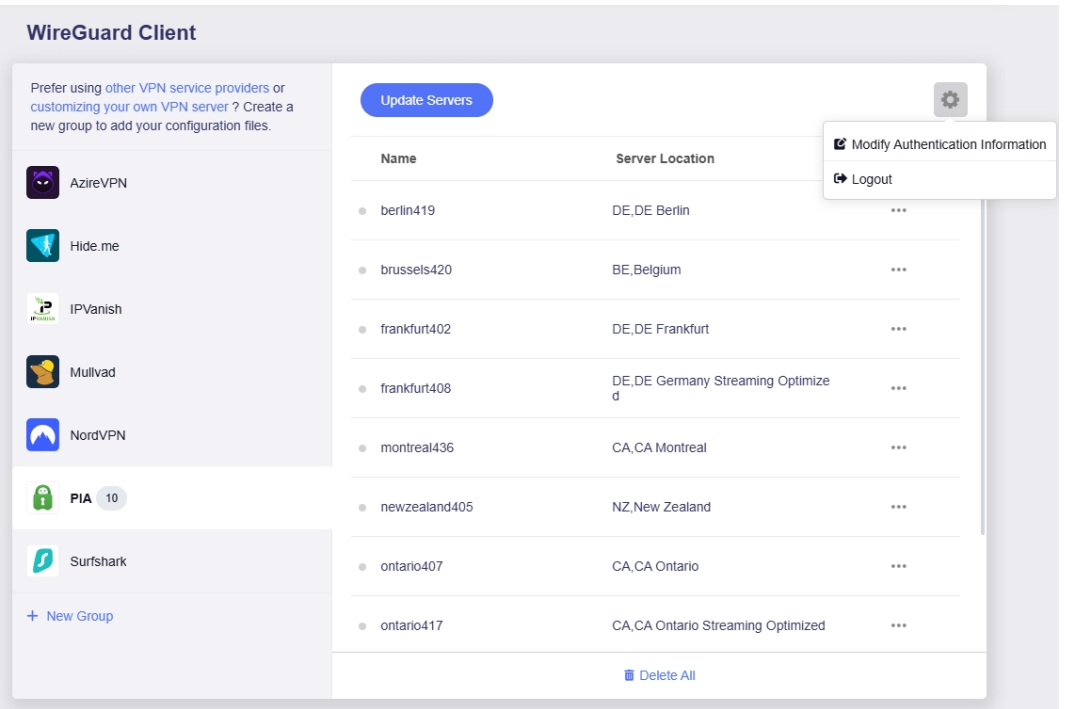
6. Mettez à jour les serveurs.

   Cliquez sur **Mettre à jour les serveurs (Update Servers)** pour récupérer la liste à jour des serveurs disponibles et éviter les échecs liés à leur maintenance ou à leur arrêt.



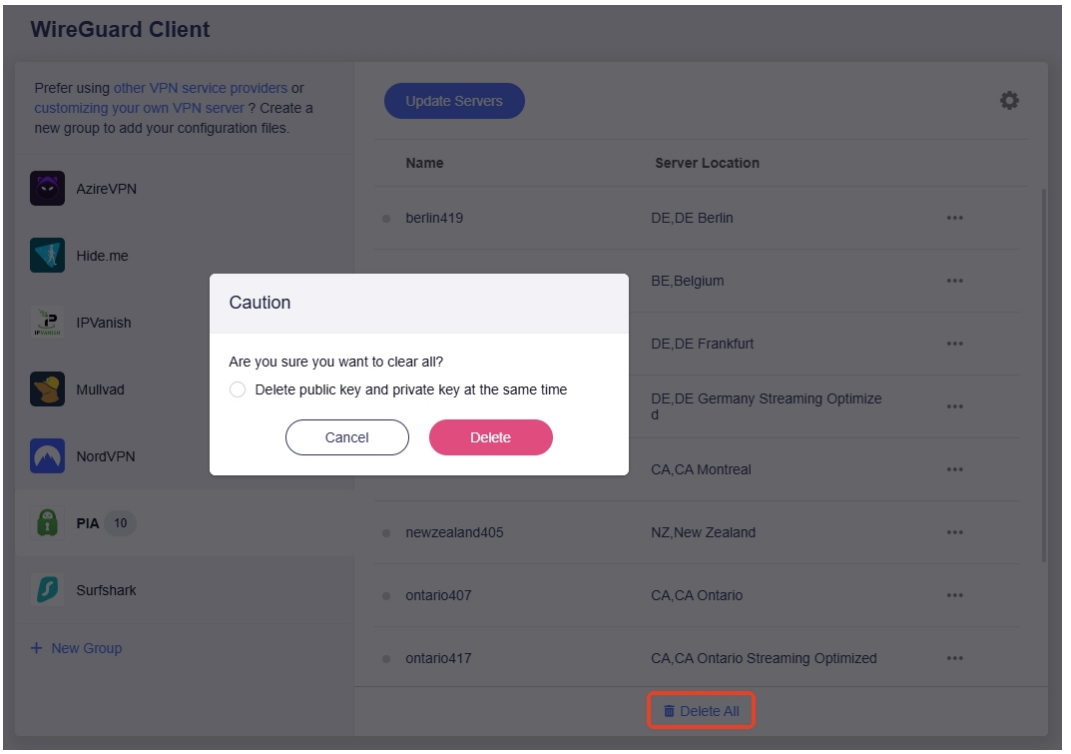
7. Modifiez les identifiants ou déconnectez-vous.

   Cliquez sur l'engrenage pour modifier vos identifiants ou vous déconnecter.



8. Supprimez tous les fichiers.

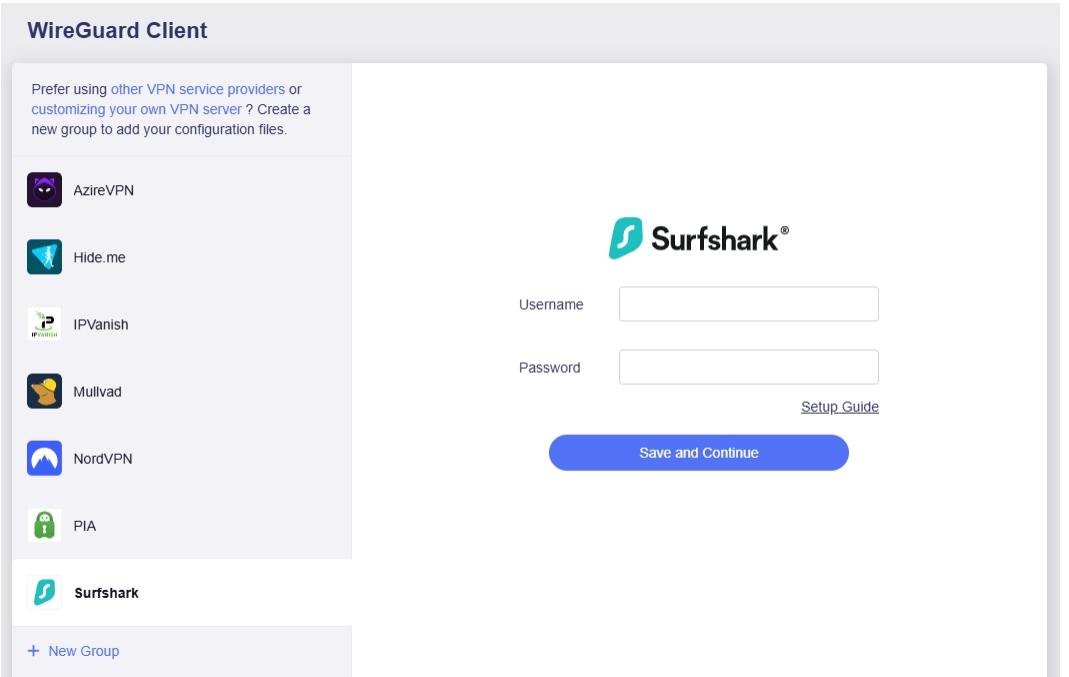
Cliquez sur **Tout supprimer (Delete All)** pour supprimer tous les fichiers de configuration en un clic. Vous pouvez choisir de supprimer également les clés privée et publique.



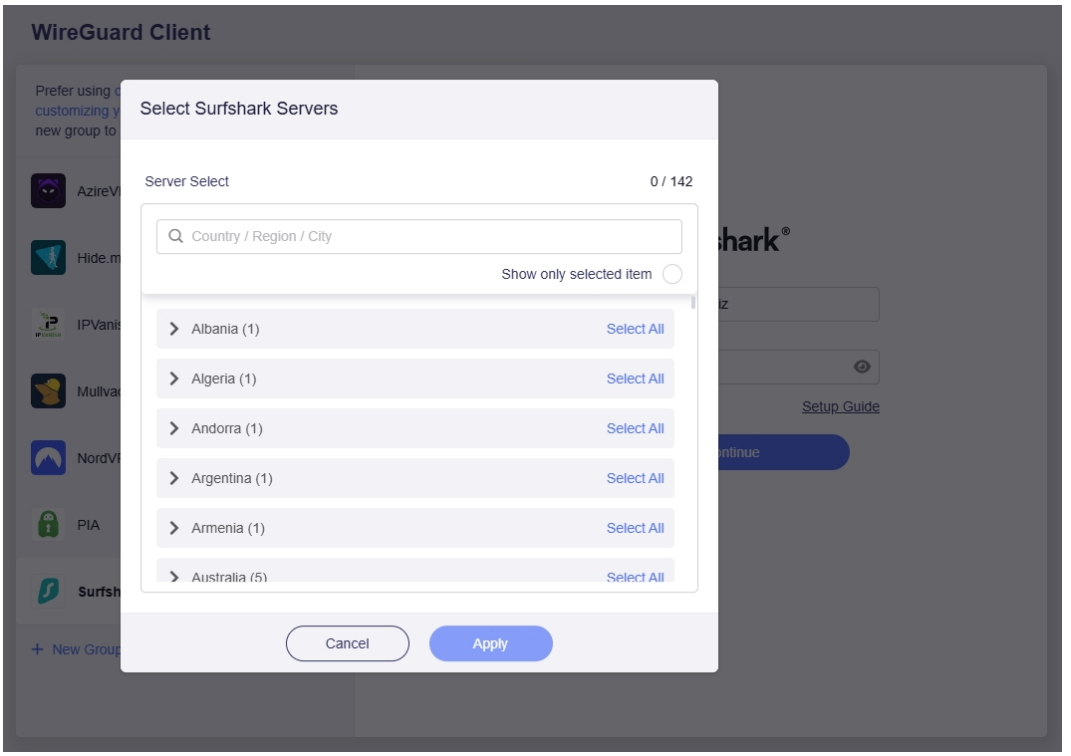
11.2.8 Configuration de Surfshark

Suivez les étapes ci-dessous pour configurer le routeur comme client Surfshark.

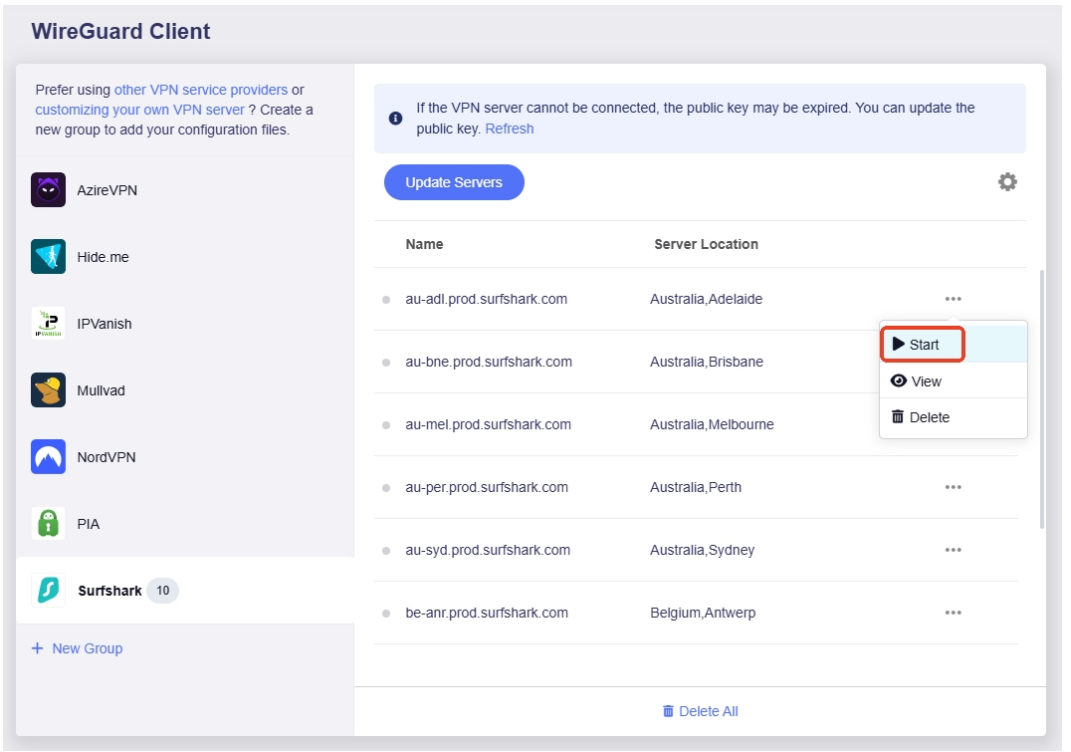
1. Connectez-vous à l'interface d'administration Web du routeur et ouvrez **VPN** > **Client WireGuard (WireGuard Client)** > **Surfshark**.
2. Saisissez l'identifiant et le mot de passe, puis cliquez sur **Enregistrer et continuer (Save and Continue)**.



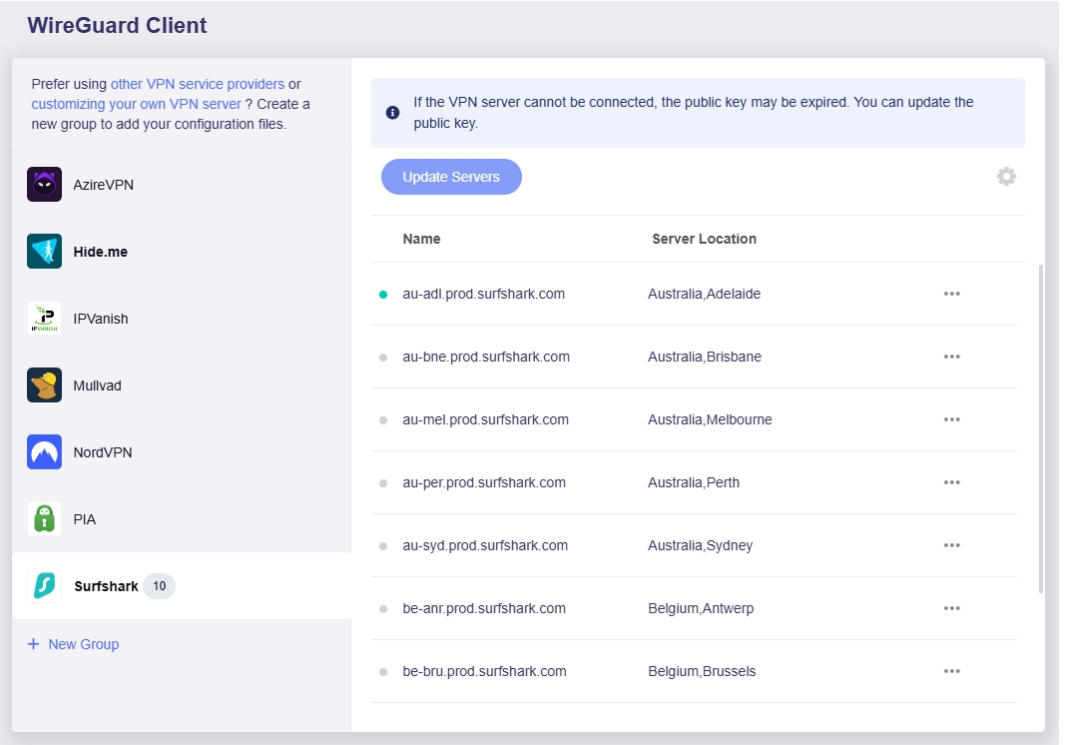
3. Sélectionnez les serveurs souhaités et cliquez sur **Appliquer (Apply)**.



4. Choisissez un serveur et cliquez sur les trois points à droite pour lancer la connexion.

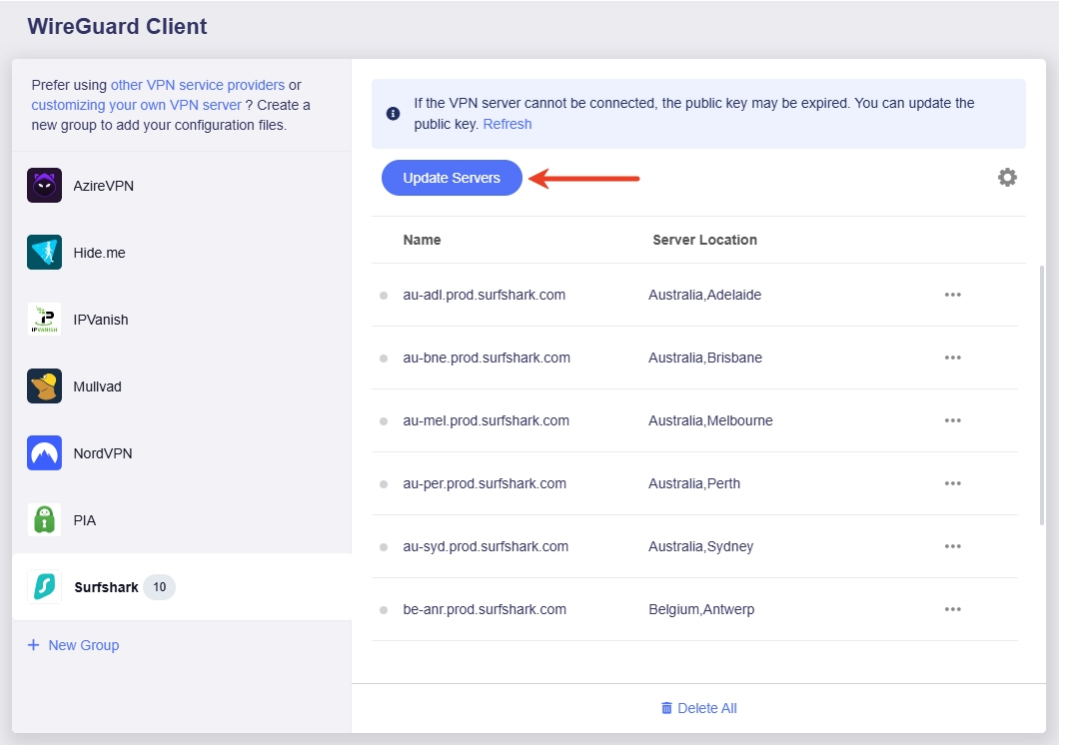


5. Une fois la connexion établie, un point vert apparaît à côté du fichier de configuration.



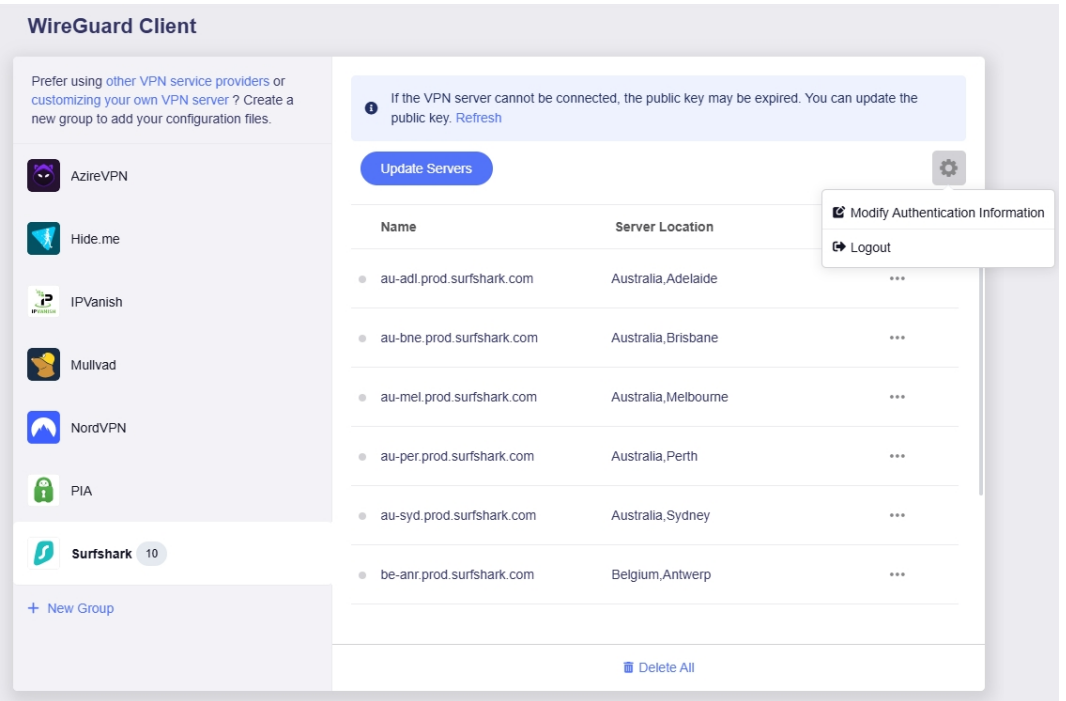
Vous pouvez également consulter les détails de la connexion dans le **Tableau de bord VPN (VPN Dashboard)**.

6. Mettez à jour les serveurs.
   Cliquez sur **Mettre à jour les serveurs (Update Servers)** pour récupérer la liste à jour des serveurs disponibles et éviter les échecs liés à leur maintenance ou à leur arrêt.



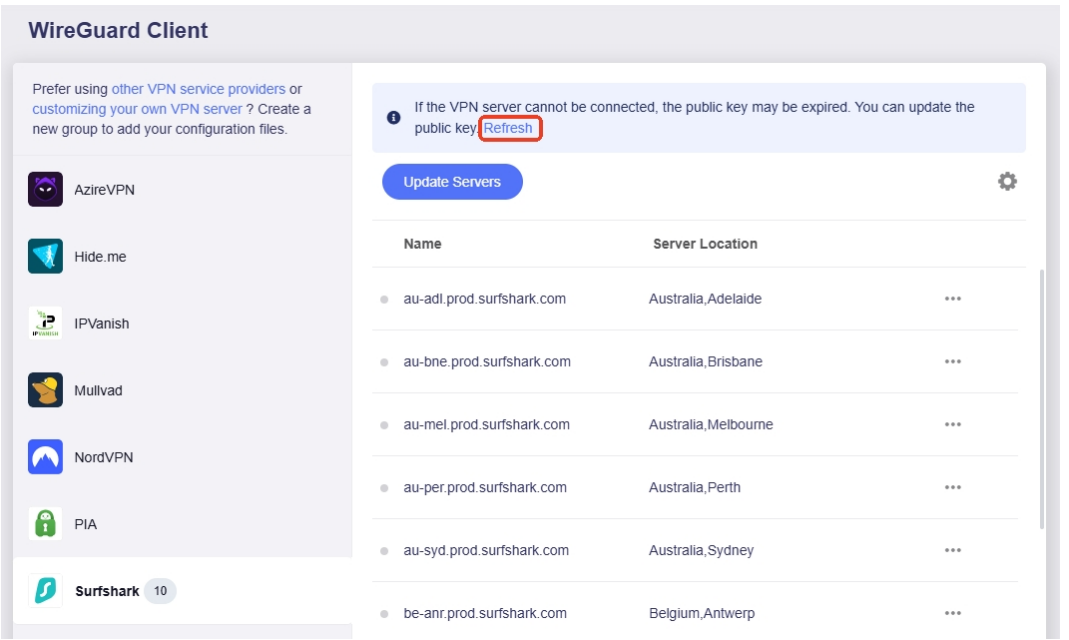
7. Modifiez les identifiants ou déconnectez-vous.

   Cliquez sur l’engrenage pour modifier vos identifiants ou vous déconnecter.



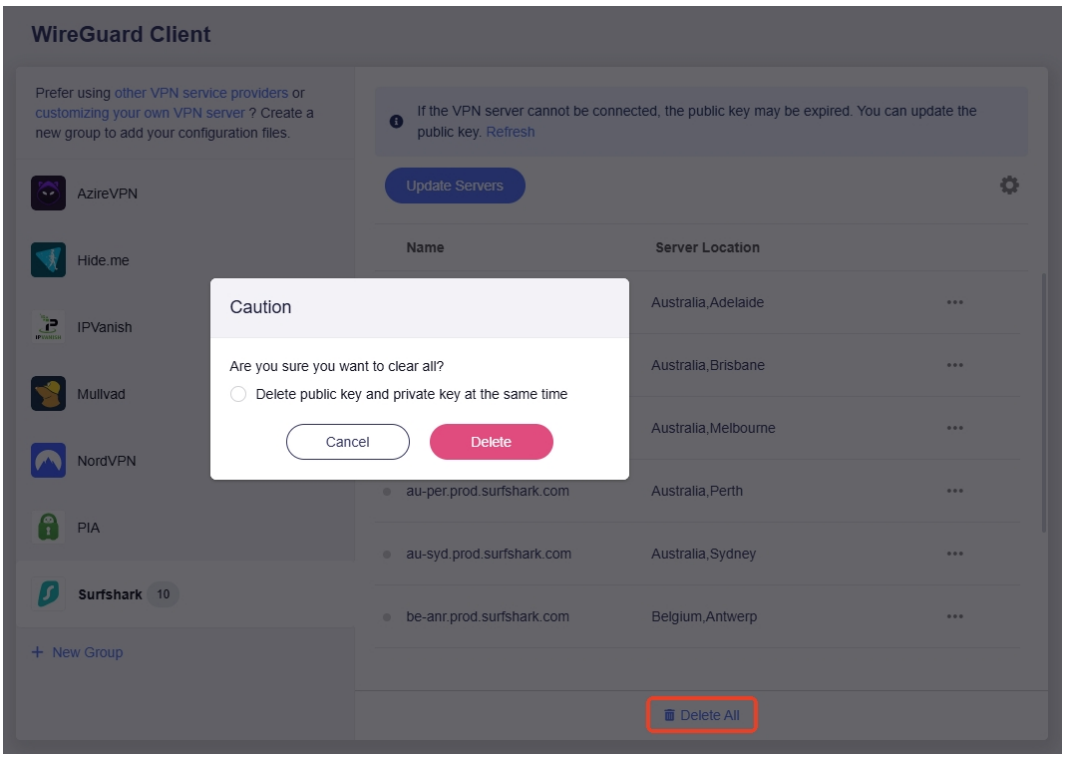
8. Actualisez les données.

Si la connexion au serveur VPN échoue, cliquez sur **Actualiser (Refresh)** pour mettre à jour la clé publique.



9. Supprimez tous les fichiers.

   Cliquez sur **Tout supprimer (Delete All)** pour supprimer tous les fichiers de configuration en un clic. Vous pouvez choisir de supprimer également les clés privée et publique.

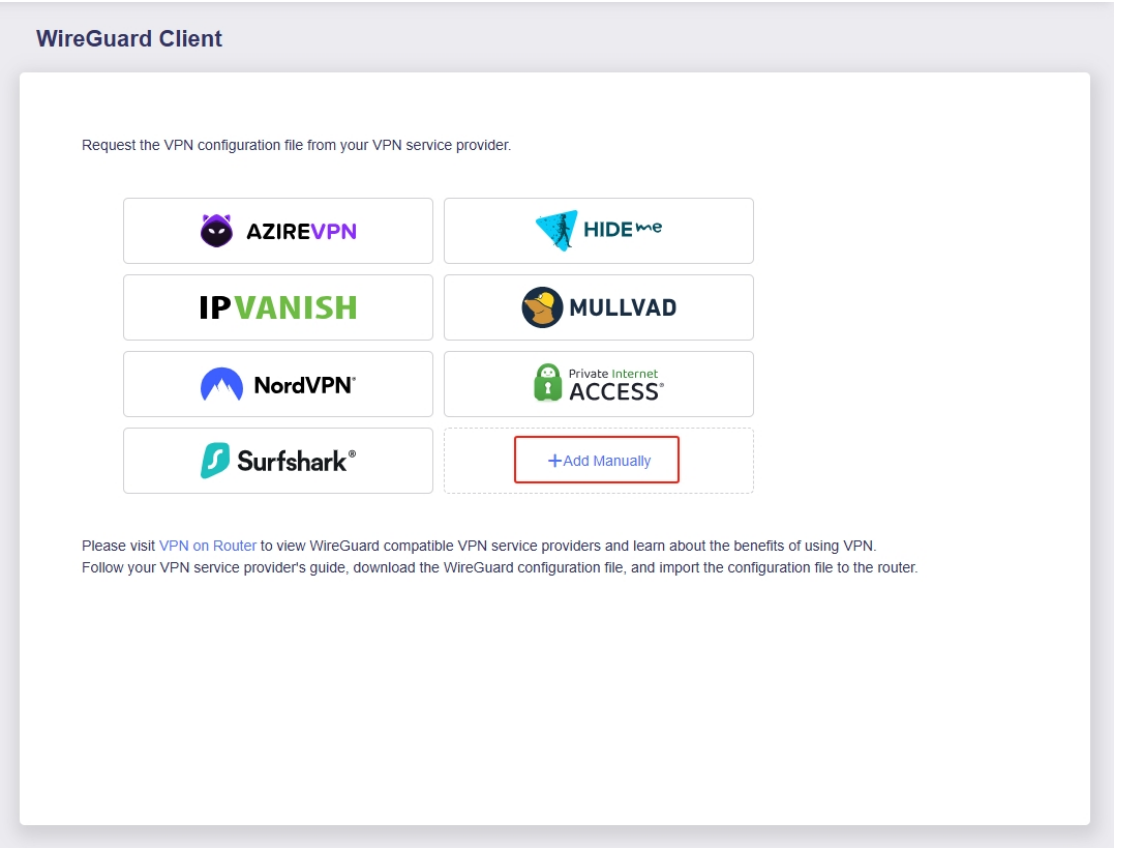


11.2.9 Configuration manuelle d’un client WireGuard pour un autre fournisseur

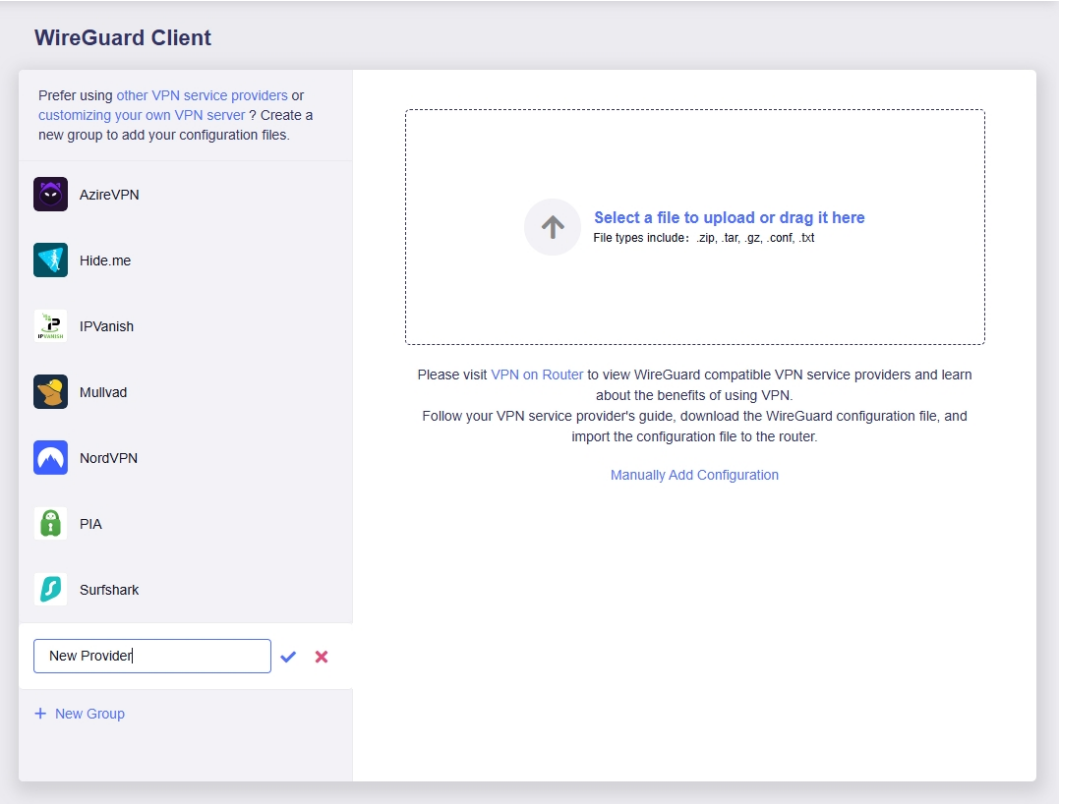
Si votre fournisseur WireGuard n’est pas intégré à l’interface d’administration Web, obtenez d’abord le fichier de configuration sur son site officiel. Téléversez ensuite ce fichier sur le routeur pour configurer un client WireGuard. Si vous ne savez pas comment télécharger les fichiers de configuration, consultez ce guide ou contactez le service d’assistance du fournisseur.

Suivez les étapes ci-dessous pour importer le fichier sur le routeur et configurer le client WireGuard.

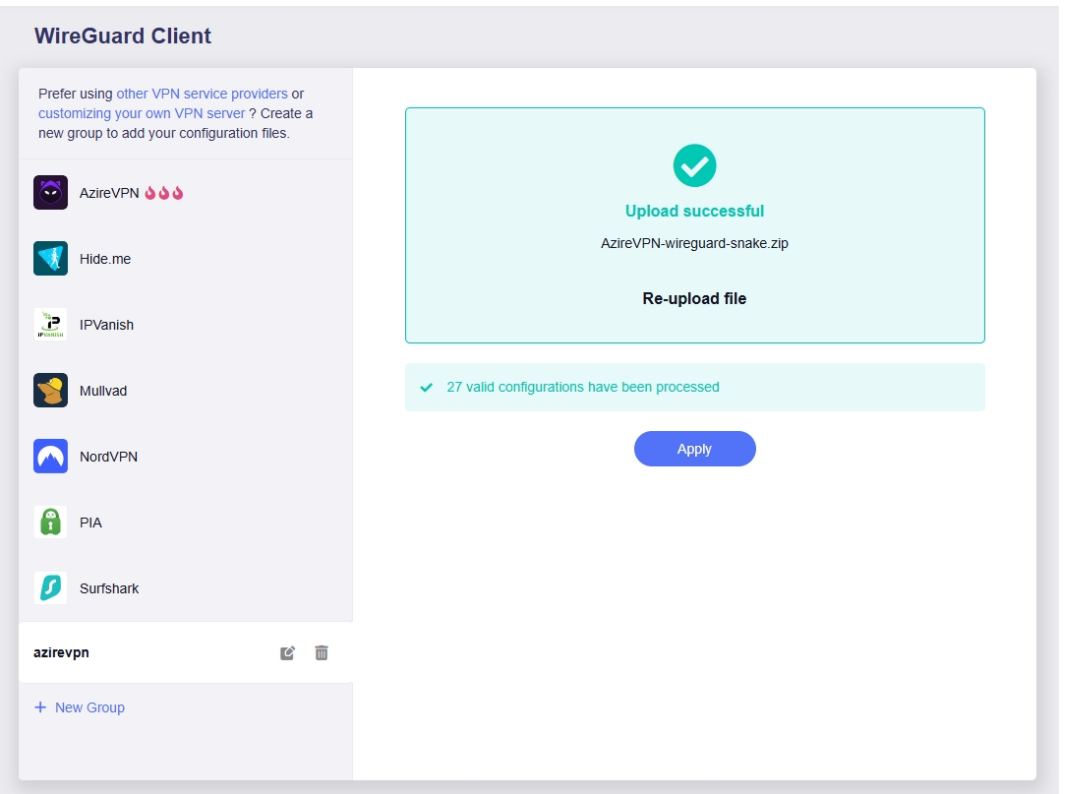
1. Connectez-vous à l’interface d’administration Web du routeur et ouvrez **VPN** > **Client WireGuard (WireGuard Client)** > **Ajouter manuellement (Add Manually)**.



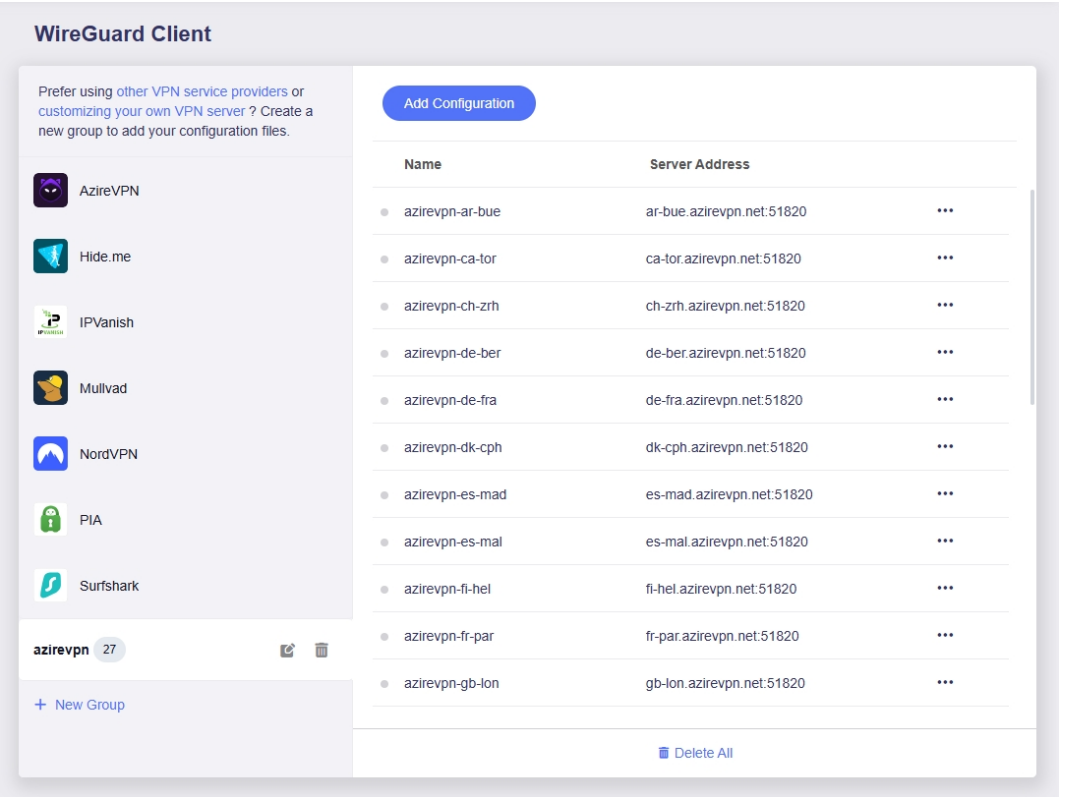
2. Un groupe est créé dans la barre latérale gauche. Donnez-lui un nom explicite.



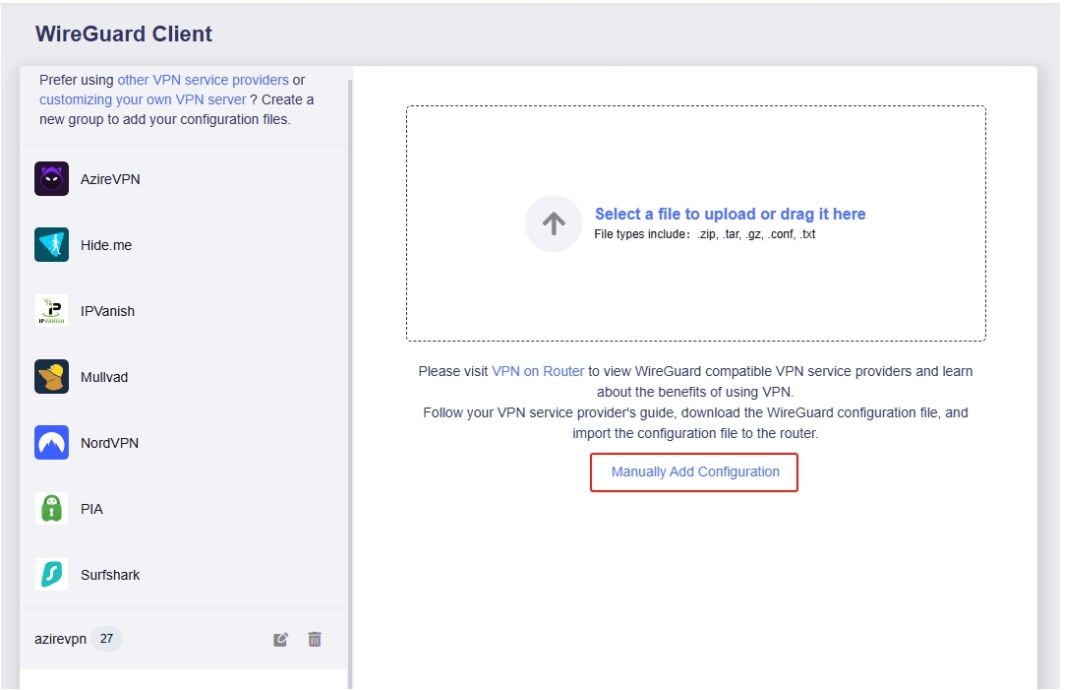
3. Cliquez sur la zone d'importation et sélectionnez votre fichier WireGuard. Les formats zip, tar, gz, conf et txt sont pris en charge. Cliquez sur **Appliquer (Apply)**.

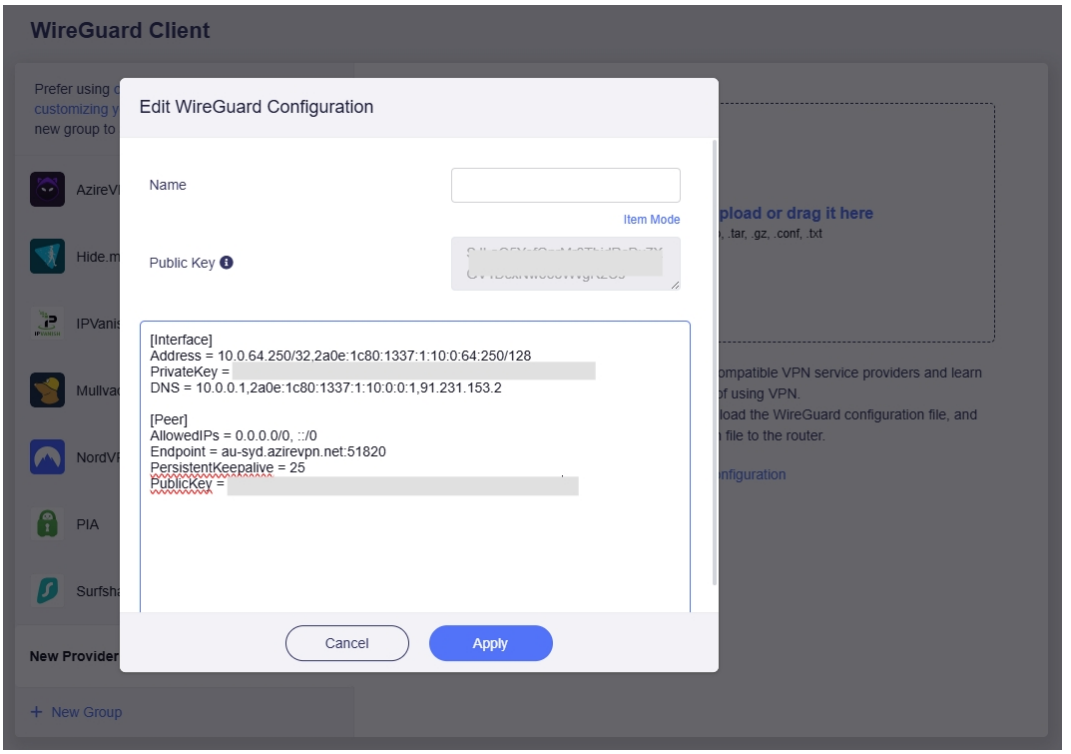


Si vous importez une archive contenant plusieurs fichiers de configuration, elle est décompressée automatiquement, comme ci-dessous.

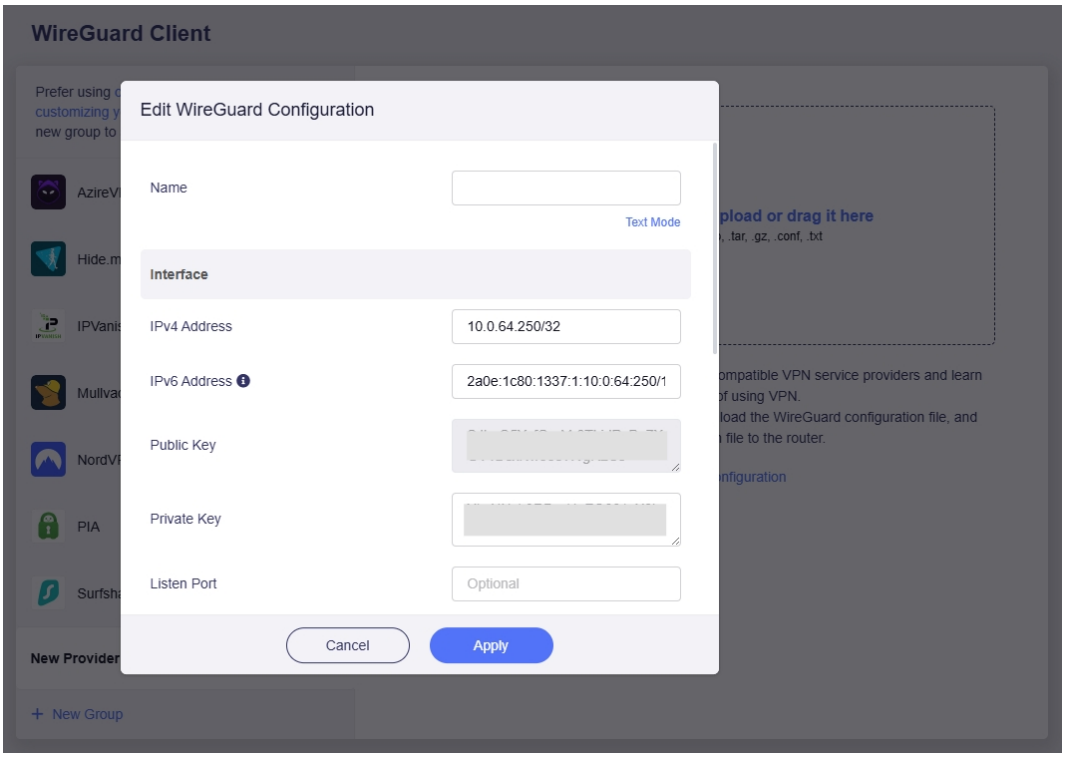


Vous pouvez aussi cliquer sur **Ajouter une configuration manuellement (Manually Add Configuration)** en bas de la zone d’importation, renseigner la configuration sous forme de texte, puis cliquer sur **Appliquer (Apply)**.

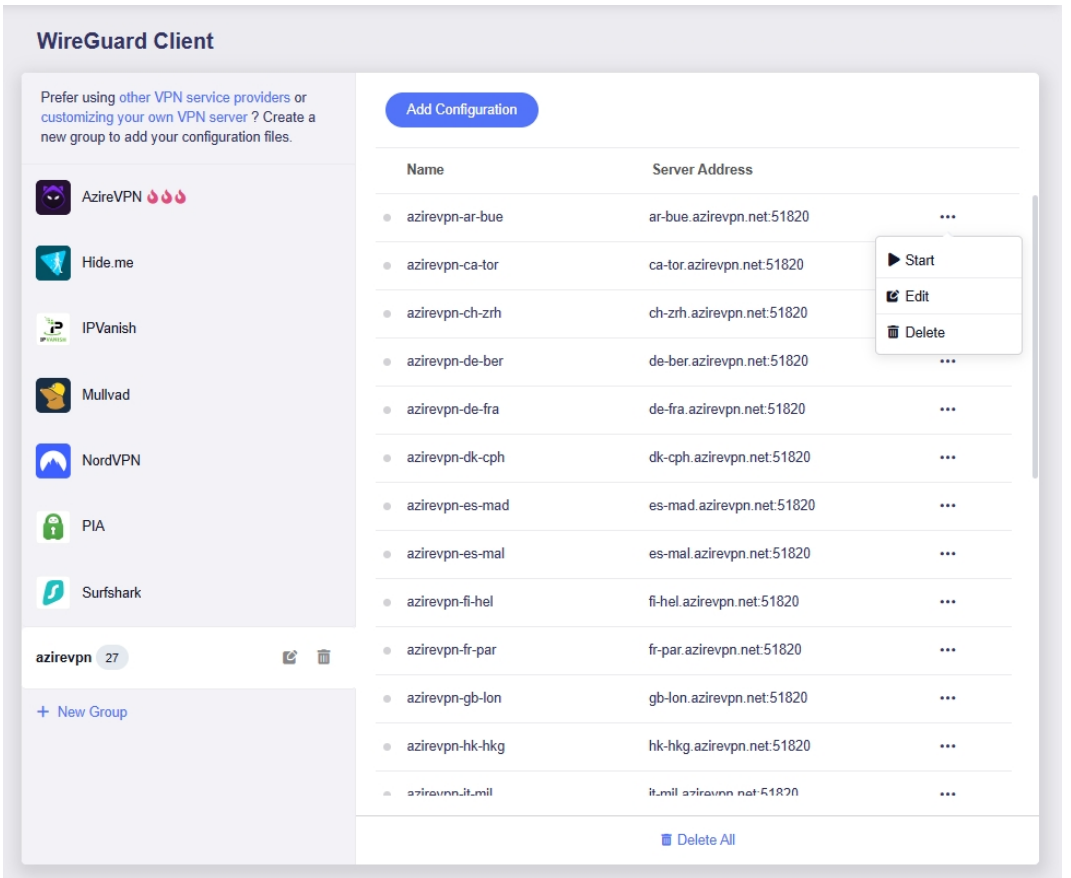




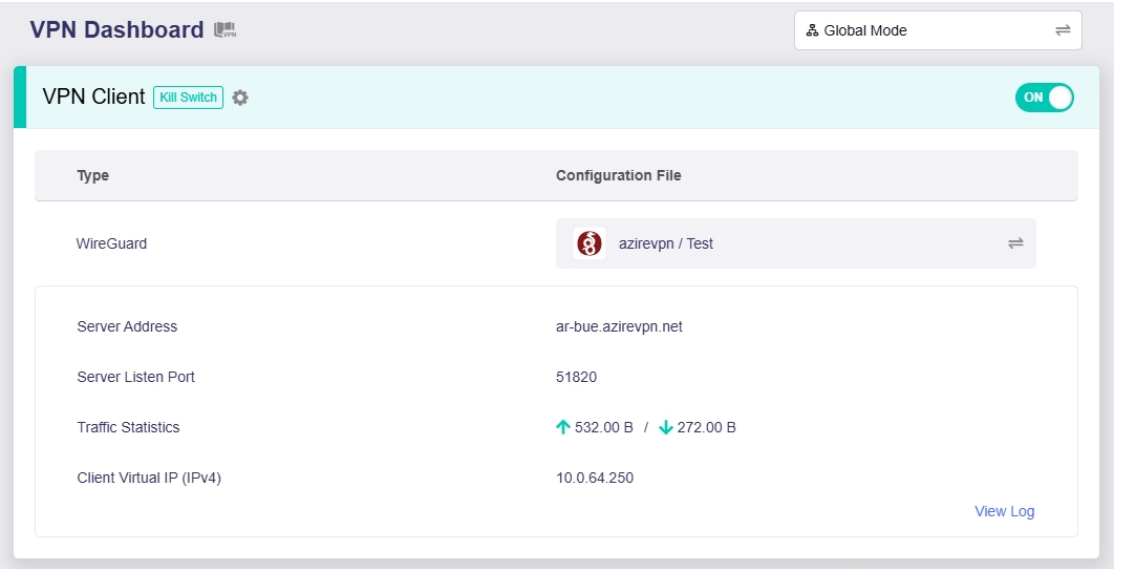
Pour vérifier chaque paramètre, passez en mode Élément (Item), contrôlez la configuration, puis cliquez sur **Appliquer (Apply)**.



4. Cliquez sur les trois points à droite pour lancer la connexion.



5. Une fois la connexion établie, un point vert apparaît à côté du fichier de configuration. Consultez les détails dans le **Tableau de bord VPN (VPN Dashboard)**.



Chapitre 12

Réseau

Ce chapitre présente les paramètres réseau et leur gestion, notamment les sous-réseaux, le DNS et IPv6.

12.1 Multi-WAN

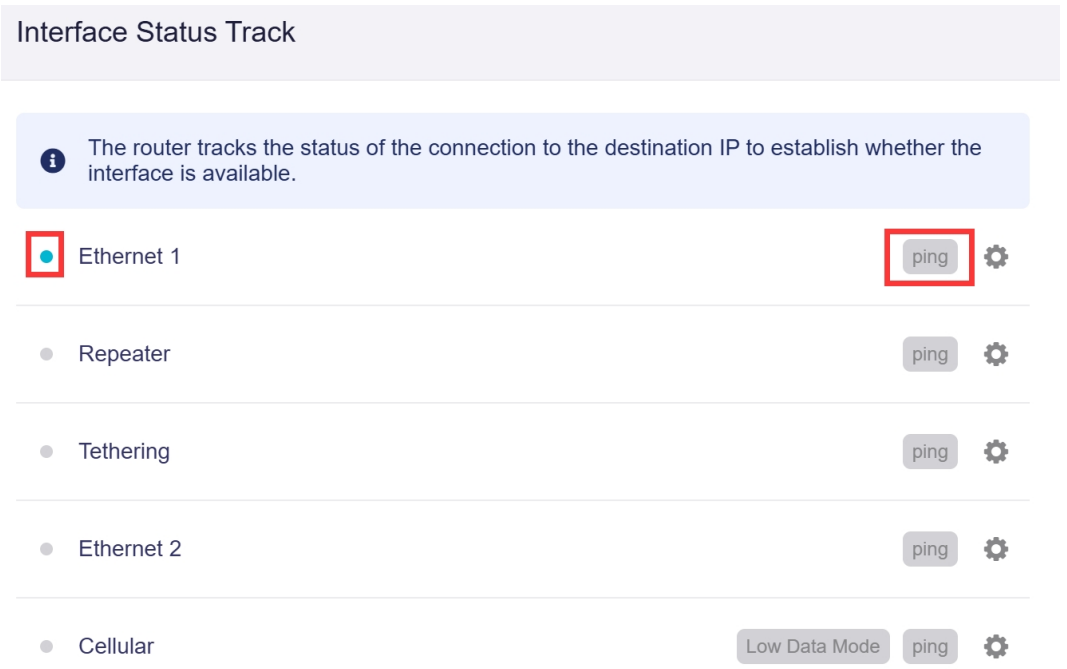
Multi-WAN permet d'utiliser simultanément plusieurs méthodes d'accès à Internet et de configurer différentes options de connexion sur le routeur. Deux modes sont proposés :

- **Basculement (Failover)** : passe automatiquement à une connexion de secours peu après la défaillance de la connexion principale pour maintenir l'accès réseau.
- **Équilibrage de charge (Load Balance)** : répartit le trafic entre les connexions disponibles selon un ratio défini, afin de les utiliser simultanément et d'optimiser la bande passante.

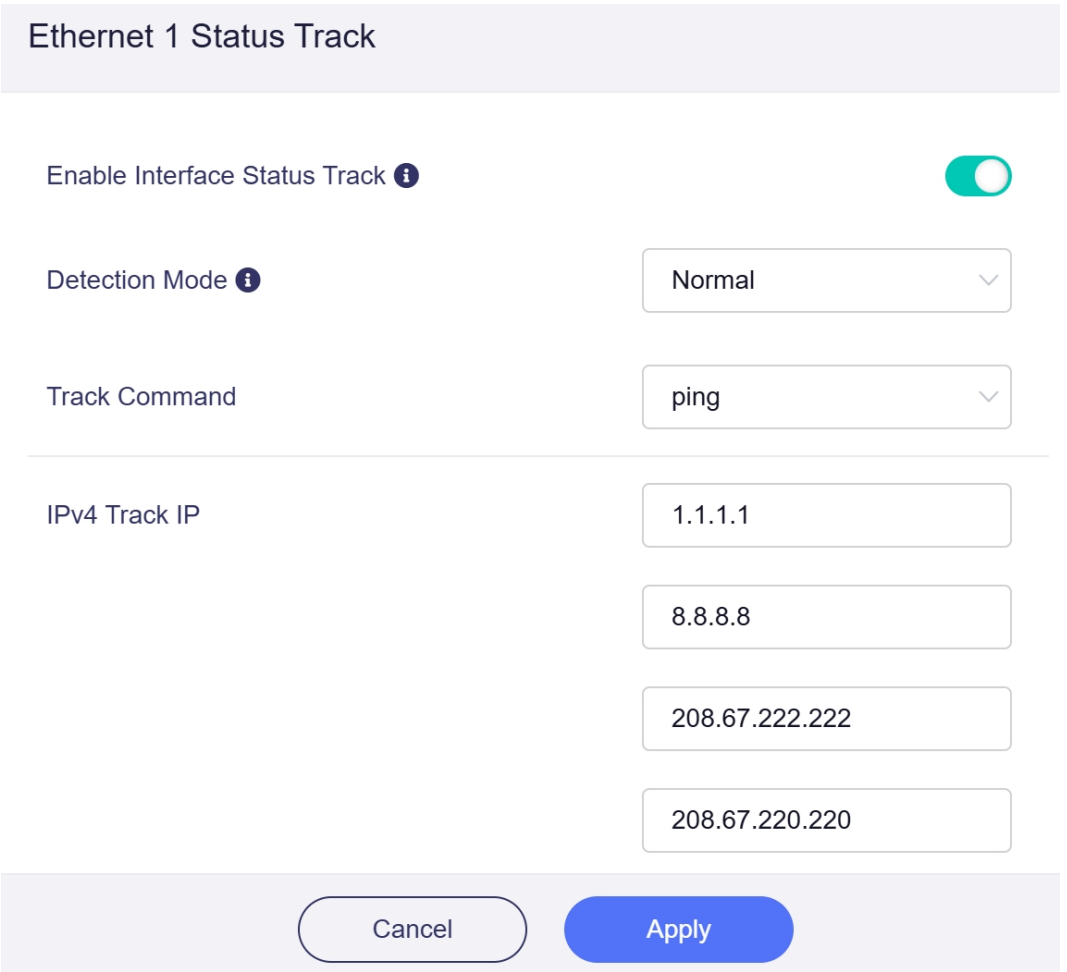
Connectez-vous à l'interface d'administration Web du routeur et ouvrez **RÉSEAU (NETWORK)** > **Multi-WAN**. Cette page comprend deux sections : suivi de l'état des interfaces et mode Multi-WAN.

12.1.1 Suivi de l'état des interfaces

Les routeurs GL.iNet utilisent la commande **ping** pour vérifier la connexion à une adresse IP cible et déterminer si l'interface est disponible. Un point vert apparaît à gauche si elle est disponible ; sinon, il est gris.



Dans la section **Suivi de l’état des interfaces (Interface Status Track)**, cliquez sur l’engrenage à droite pour régler le suivi de chaque interface. Les paramètres Ethernet sont présentés ci-dessous. La même logique s’applique aux autres interfaces.

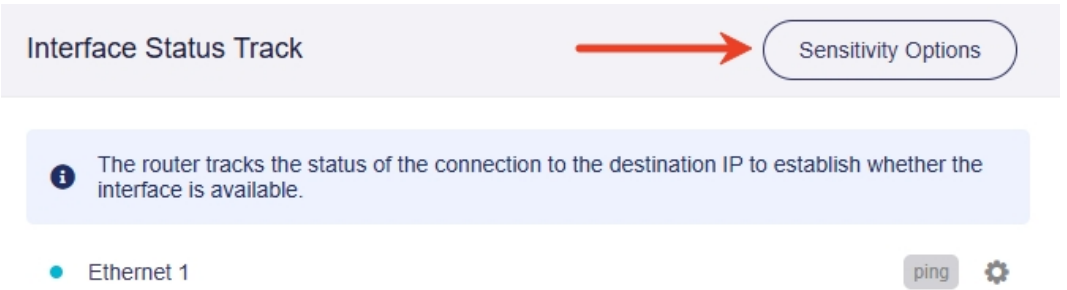


- **Activer le suivi de l’état de l’interface (Enable Interface Status Track)** : activé par défaut. Si vous le désactivez, le routeur détermine l’état de l’interface selon les conditions physiques, par exemple le branchement du câble Ethernet.
- **Mode de détection (Detection Mode)** : introduite sous le nom Mode données réduites dans le micrologiciel v4.5, cette fonction a été renommée Mode de détection en v4.7. Trois modes sont proposés : Normal, Données réduites et Strict.
  - **Mode normal (Normal Mode)** : utilisé par défaut.
  - **Mode données réduites (Low Data Mode)** : lance le suivi uniquement lorsqu’une erreur réseau survient sur l’interface. Utilisez-le avec un forfait de données limité. La

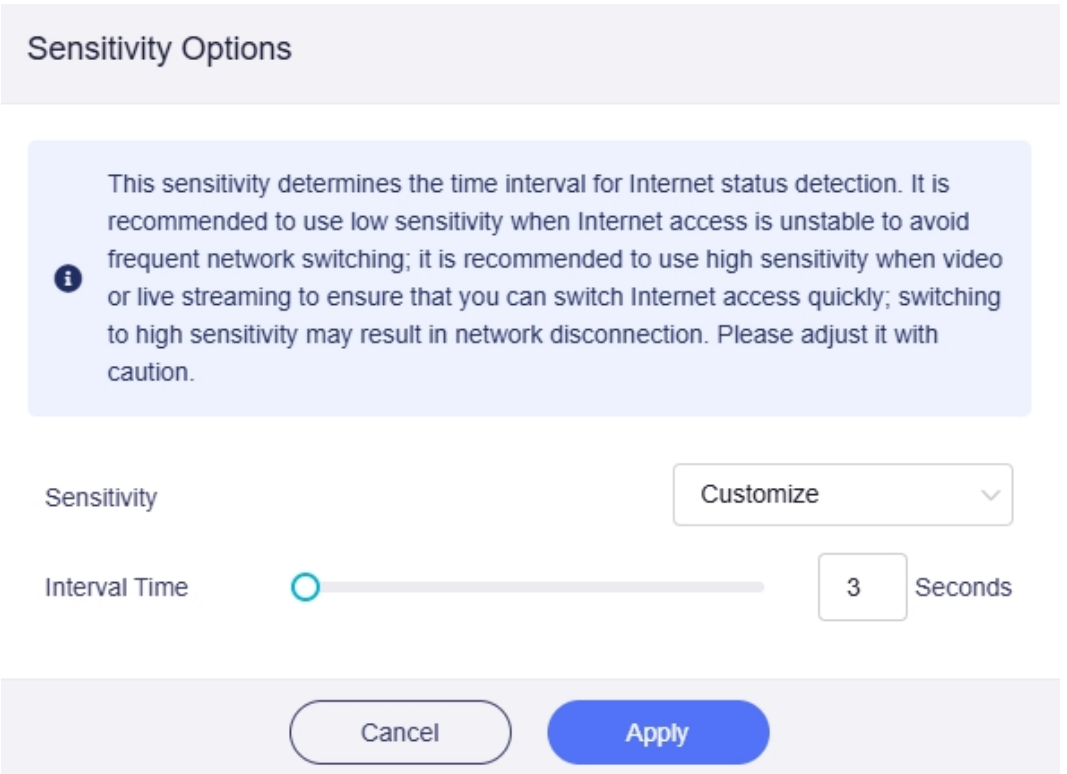
reconnexion peut être légèrement plus lente qu'en mode normal. Il est activé par défaut uniquement pour l'interface cellulaire.

  - **Mode strict (Strict Mode)** : détermine l'état de l'interface uniquement à partir du résultat de la commande de détection envoyée à une adresse IP publique.
- **Commande de suivi (Track Command)** : la commande ping vérifie la connexion à l'IP cible et la disponibilité de l'interface.
- **IP de suivi IPv4 (IPv4 Track IP)** : personnalisez les adresses IPv4 utilisées pour le suivi si nécessaire.

Cliquez sur **Options de sensibilité (Sensitivity Options)** dans l'angle supérieur droit.



Choisissez un intervalle de détection Faible, Moyen ou Élevé, ou personnalisez-le. L'intervalle peut être compris entre 0,5 et 90 secondes.



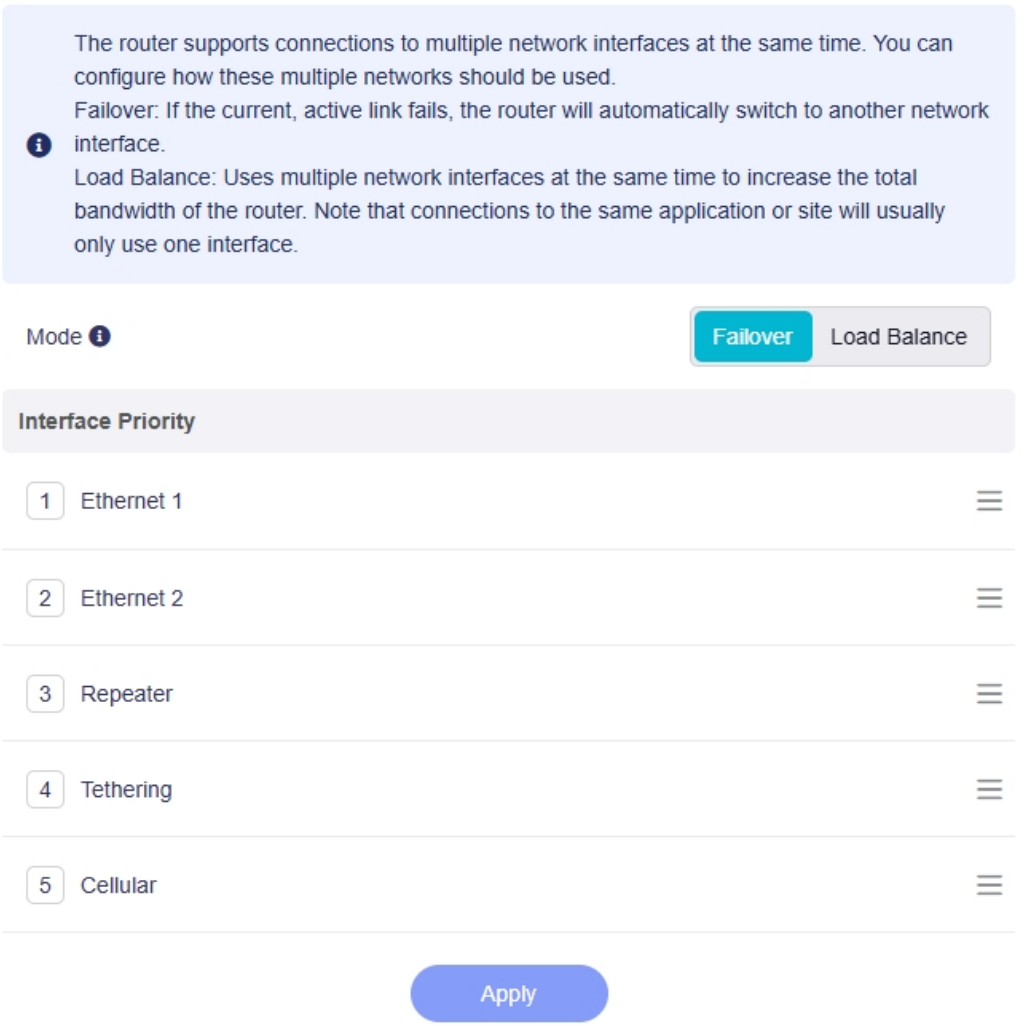
12.1.2 Mode Multi-WAN

Deux modes sont proposés : **Basculement (Failover)** et **Équilibrage de charge (Load Balance)**. Ils ne peuvent pas être utilisés simultanément.

Basculement

Le basculement est le mode par défaut lorsque plusieurs connexions sont configurées. Si la liaison active échoue, le routeur utilise automatiquement une autre interface pour accéder à Internet.

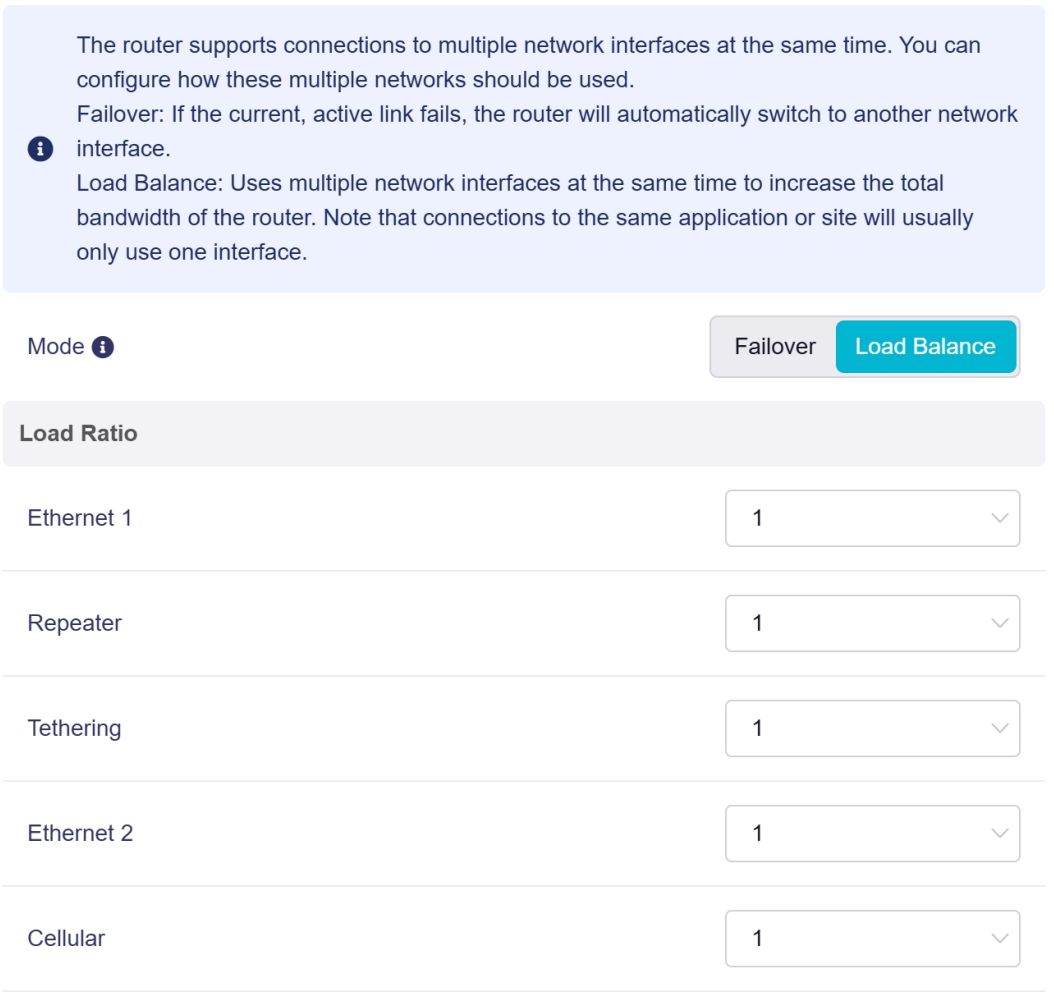
Vous pouvez définir une priorité pour chaque interface. En cas de défaillance, le routeur sélectionne l'interface disponible la plus prioritaire. Dès qu'une connexion plus prioritaire est rétablie, il l'utilise de nouveau automatiquement.



Équilibrage de charge

Ce mode utilise plusieurs interfaces simultanément pour augmenter la bande passante totale du routeur. Le système répartit les nouvelles connexions selon le ratio de charge configuré. Les connexions à une même application ou à un même site utilisent toutefois généralement une seule interface.

Le ratio de charge définit la proportion de nouvelles connexions attribuée à chaque interface. Par exemple, si cinq interfaces, Ethernet 1, Répéteur, Partage de connexion, Cellulaire et Ethernet 2, donnent accès à Internet, un ratio de 1:1:1:1:1 répartit la charge à parts égales. Le système distribue les nouvelles connexions entre ces interfaces selon ce ratio.



Vous pouvez personnaliser le rapport de répartition si nécessaire. Par exemple, si Ethernet 1 dispose de 100 Mbit/s, le répéteur de 200 Mbit/s et qu'aucune autre connexion n'est active, définissez les rapports sur 1 pour Ethernet 1, 2 pour le répéteur et 0 pour le partage de connexion, le réseau mobile et Ethernet 2. Le système répartit les nouvelles connexions entre

ces interfaces selon le rapport 1:2 : Ethernet 1 reçoit donc deux fois moins de connexions que le répéteur. Ce mode améliore l'efficacité du débit global en répartissant la charge entre toutes les interfaces disponibles, contrairement au mode Basculement.

Remarque : les connexions et le trafic existants ne suivent pas nécessairement le ratio de charge. La répartition réelle se rapproche progressivement du ratio configuré au fil de l'utilisation.

12.2 Sous-réseau

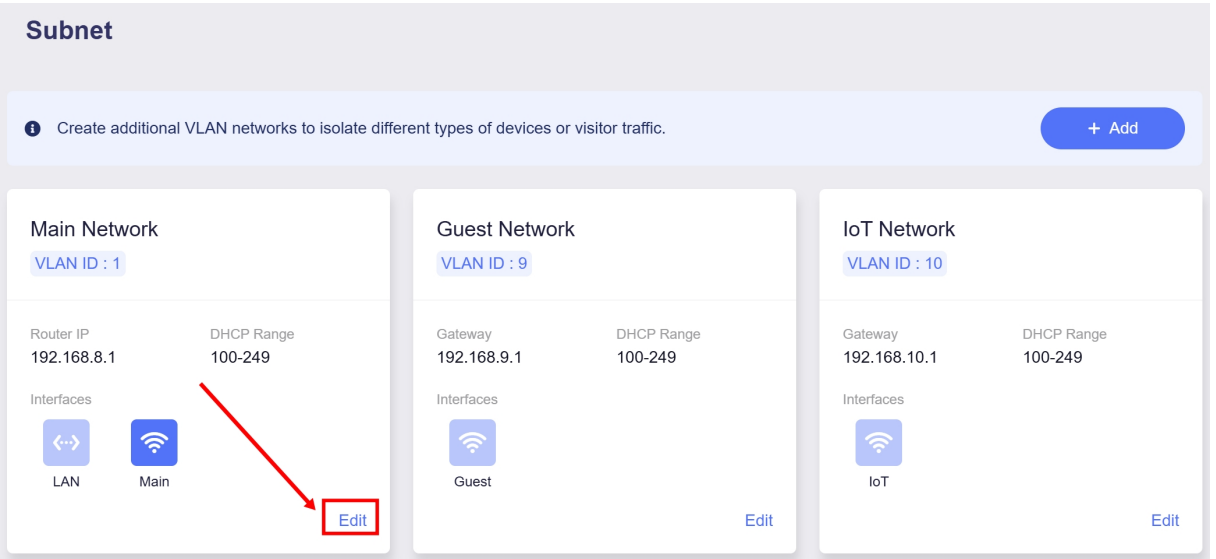
Un sous-réseau est une subdivision logique d'un réseau, qui permet d'organiser et d'isoler les appareils dans différents segments.

Connectez-vous à l'interface Web du routeur et ouvrez **RÉSEAU (NETWORK)** > **Sous-réseau (Subnet)**. Vous pouvez y configurer le réseau principal, le réseau invité, le réseau IoT et des réseaux VLAN personnalisés.

12.2.1 Réseau principal

Le réseau principal correspond à la connexion via votre Wi-Fi principal ou Ethernet. Il affiche l'état de toutes les interfaces, l'identifiant VLAN, l'adresse IP du routeur et la plage DHCP.

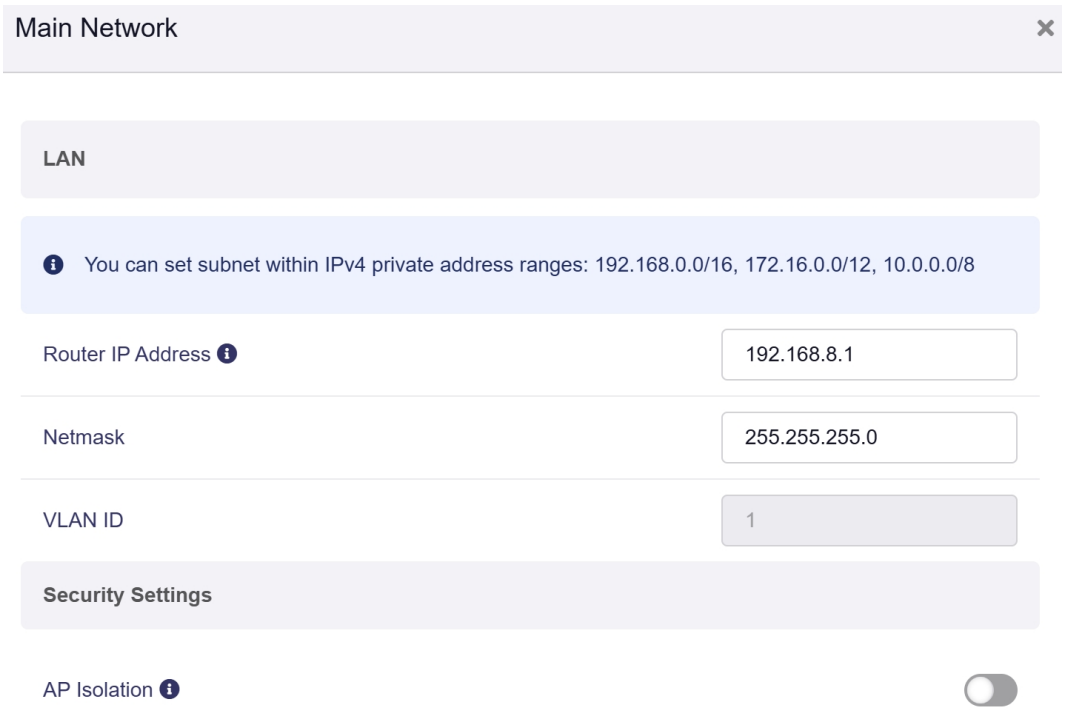
Cliquez sur **Modifier (Edit)** en bas à droite pour configurer le réseau principal.



La page de configuration comprend les paramètres de base, le serveur DHCP et la réservation d'adresses.

Paramètres de base

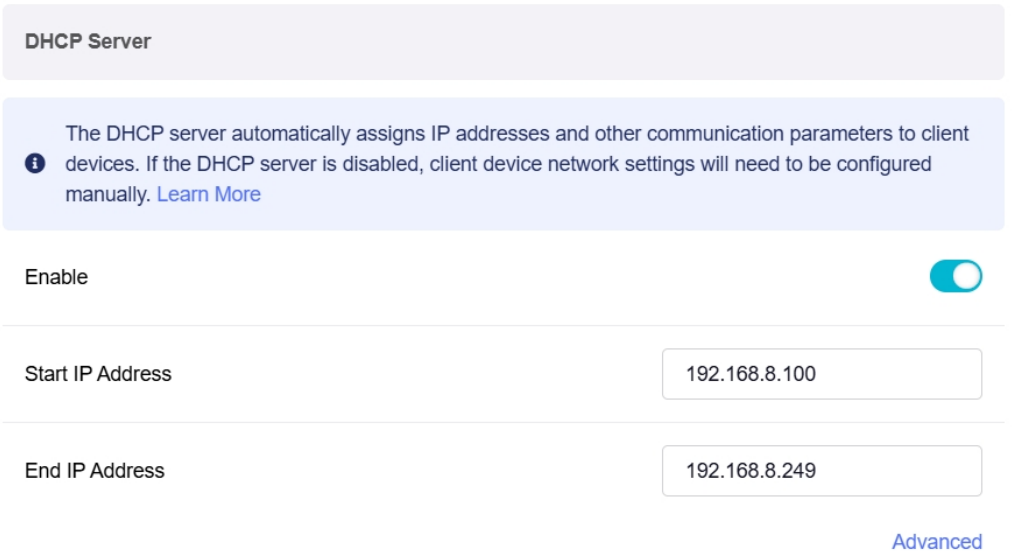
Les paramètres de base comprennent l'adresse IP du routeur, le masque de sous-réseau et l'identifiant VLAN. Vous pouvez définir un sous-réseau dans les plages IPv4 privées : 192.168.0.0/16, 172.16.0.0/12 et 10.0.0.0/8.



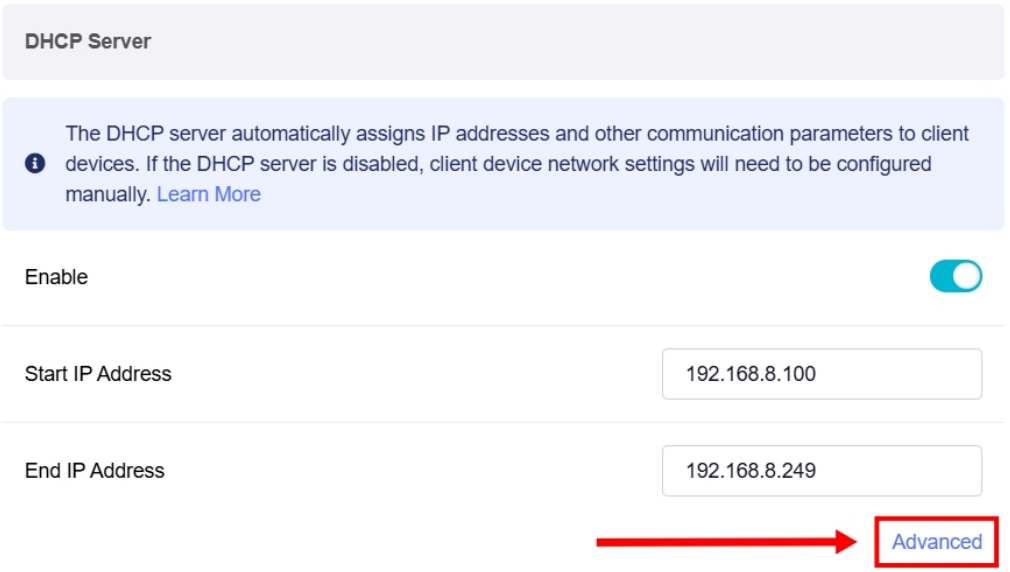
- **Adresse IP du routeur (Router IP Address)** : adresse à saisir dans le navigateur pour ouvrir l'interface d'administration. Par défaut, elle est 192.168.8.1. Modifiez-la si elle entre en conflit avec le réseau en amont.
- **Masque de sous-réseau (Netmask)** : deux valeurs sont proposées : 255.255.255.0 et 255.255.0.0.
- **Identifiant VLAN (VLAN ID)** : l'identifiant VLAN du réseau principal est 1 par défaut et ne peut pas être modifié.
- **Isolation des clients (AP Isolation)** : isole les appareils clients dans des segments distincts. Ils ne peuvent plus communiquer avec les autres appareils du même réseau.

Serveur DHCP

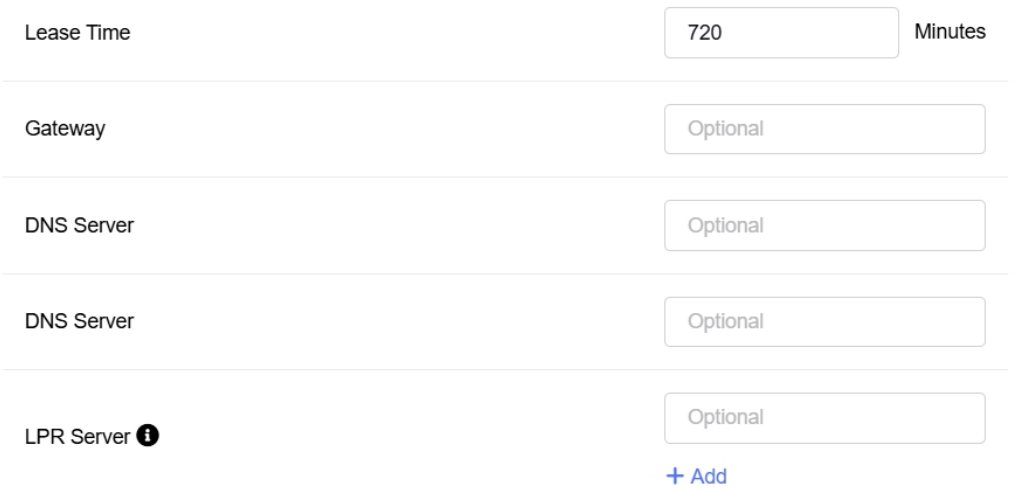
Le serveur DHCP attribue automatiquement une adresse IP et les autres paramètres de communication à chaque client connecté. Il est activé par défaut sur le routeur GL.iNet, avec une plage d'adresses de 192.168.8.100 à 192.168.8.249. Vous pouvez personnaliser cette plage.



Cliquez sur **Avancé (Advanced)** dans l'angle inférieur droit.



Vous pouvez définir la durée du bail, la passerelle, les serveurs DNS et le serveur LPR.



- **Durée du bail (Lease Time)** : durée pendant laquelle un appareil peut utiliser l'adresse IP attribuée par DHCP.
- **Passerelle (Gateway)** : composant du routeur qui achemine le trafic entre le réseau local et les réseaux externes, comme Internet.
- **Serveur DNS** : deux champs permettent de configurer les résolveurs principal et secondaire. Saisissez le serveur DNS principal dans le champ supérieur et le secondaire dans le champ inférieur. Si le serveur principal devient indisponible, les appareils clients basculent automatiquement vers le serveur secondaire pour maintenir la résolution des noms de domaine.
- **Serveur LPR (LPR Server)** : le service Line Printer Remote gère les travaux d'impression et permet aux appareils du réseau d'envoyer des demandes d'impression à des imprimantes distantes. Vous pouvez configurer plusieurs ports LPR pour les imprimantes.

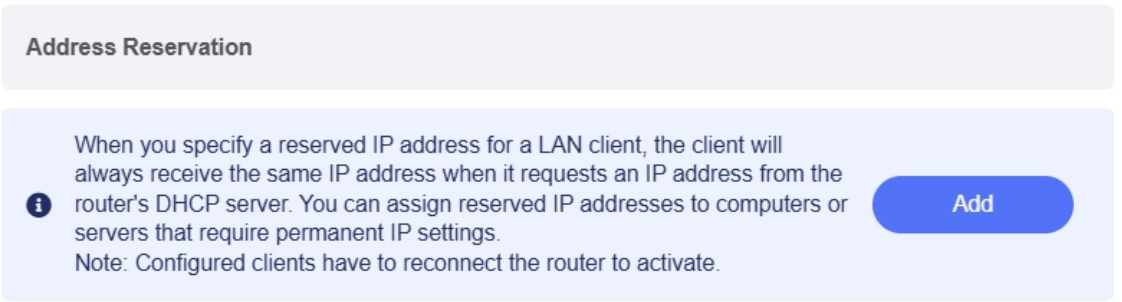
Remarque : si vous désactivez le serveur DHCP, définissez manuellement une IP statique et les autres paramètres de communication sur chaque client. Consultez cette page pour en savoir plus.

Réservation d’adresses

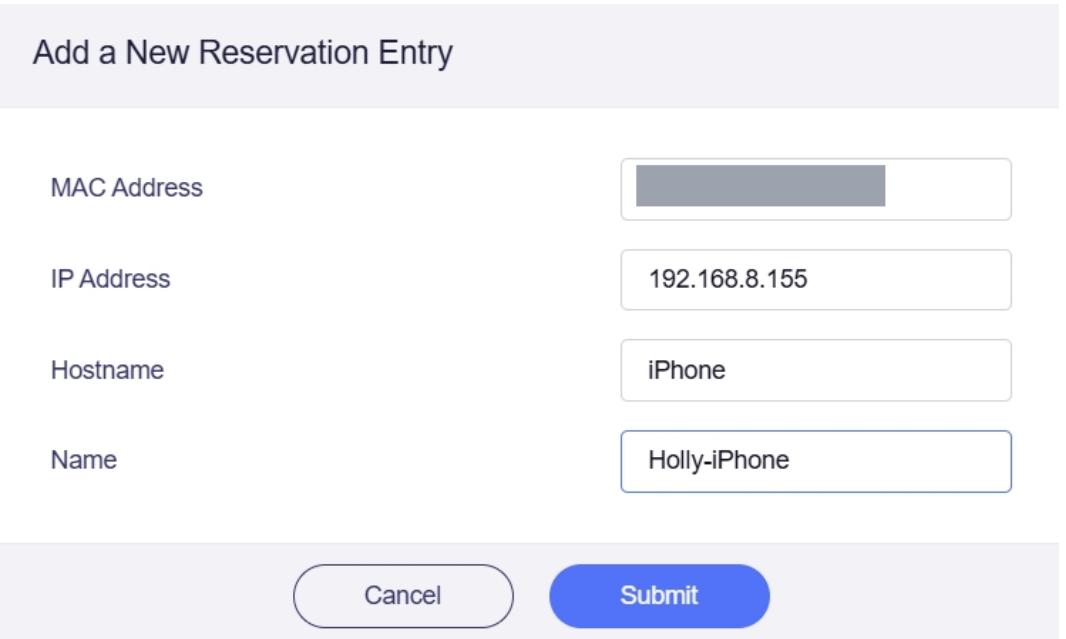
La réservation d’adresses permet d’attribuer une IP fixe à un client LAN. Celui-ci reçoit alors toujours la même adresse du serveur DHCP du routeur. Cette fonction convient aux ordinateurs et aux serveurs nécessitant une adresse permanente. Les clients concernés doivent se reconnecter au routeur pour que le réglage prenne effet.

Pour configurer une réservation d’adresse, procédez comme suit.

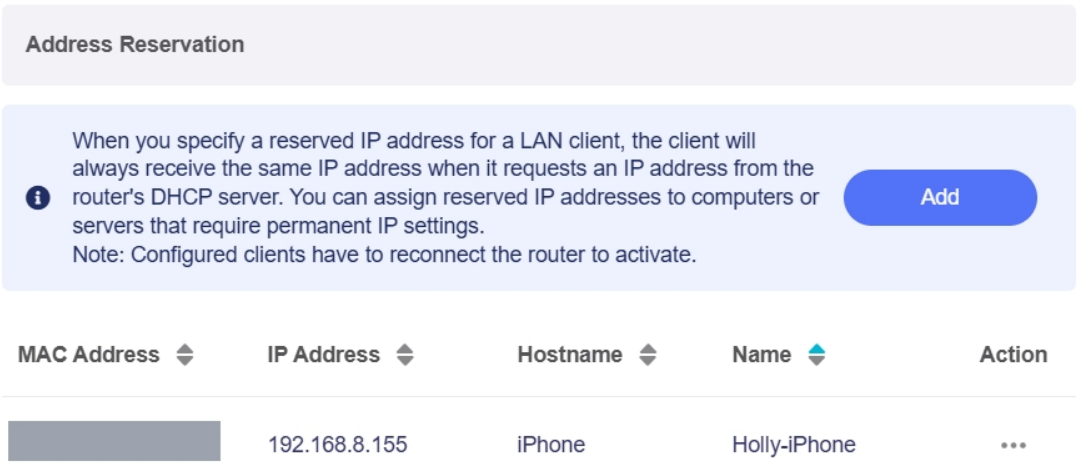
1. Dans l’interface Web du routeur, ouvrez **Sous-réseau (Subnet)** > **Réseau principal (Main Network)** > **Réservation d’adresses (Address Reservation)**, puis cliquez sur **Ajouter (Add)**.



2. Dans la fenêtre qui s’affiche, sélectionnez l’adresse MAC dans la liste. L’adresse IP correspondante est renseignée automatiquement. Saisissez un nom d’hôte et un nom personnalisé pour identifier facilement l’appareil, puis cliquez sur **Valider (Submit)**.



3. La nouvelle réservation apparaît dans la liste, comme ci-dessous.

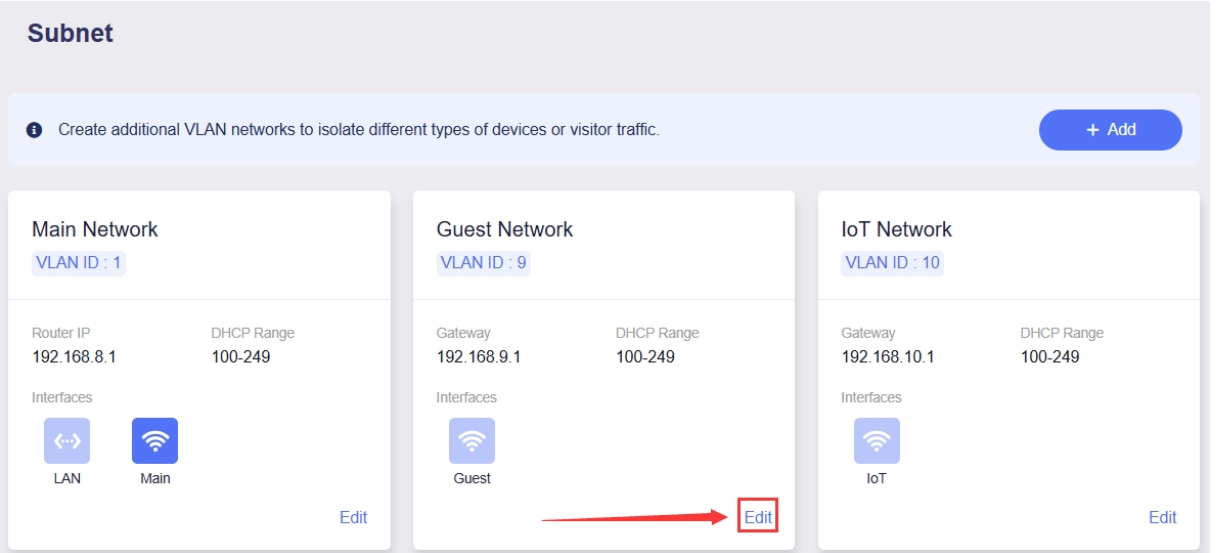


12.2.2 Réseau invité

Le réseau invité est un réseau dédié aux visiteurs, séparé de votre LAN principal pour protéger votre réseau privé.

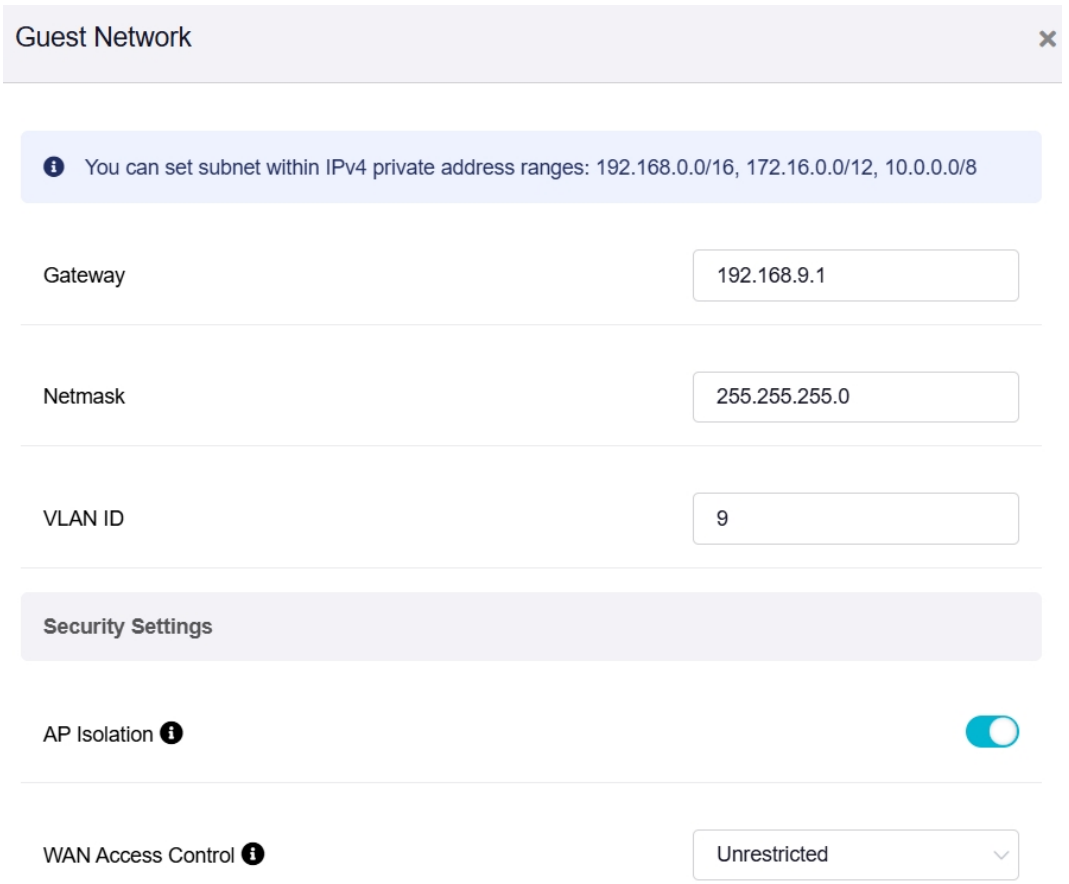
Dans l'interface Web du routeur, ouvrez **RÉSEAU (NETWORK)** > **Sous-réseau (Subnet)** > **Réseau invité (Guest Network)**. Cette page permet de configurer le réseau invité, notamment les paramètres de base et le serveur DHCP.

Cliquez sur **Modifier (Edit)** en bas à droite pour configurer le réseau invité.



Paramètres de base

Les paramètres de base comprennent la passerelle, le masque de sous-réseau, l'isolation des clients, l'identifiant VLAN et le contrôle d'accès au WAN.



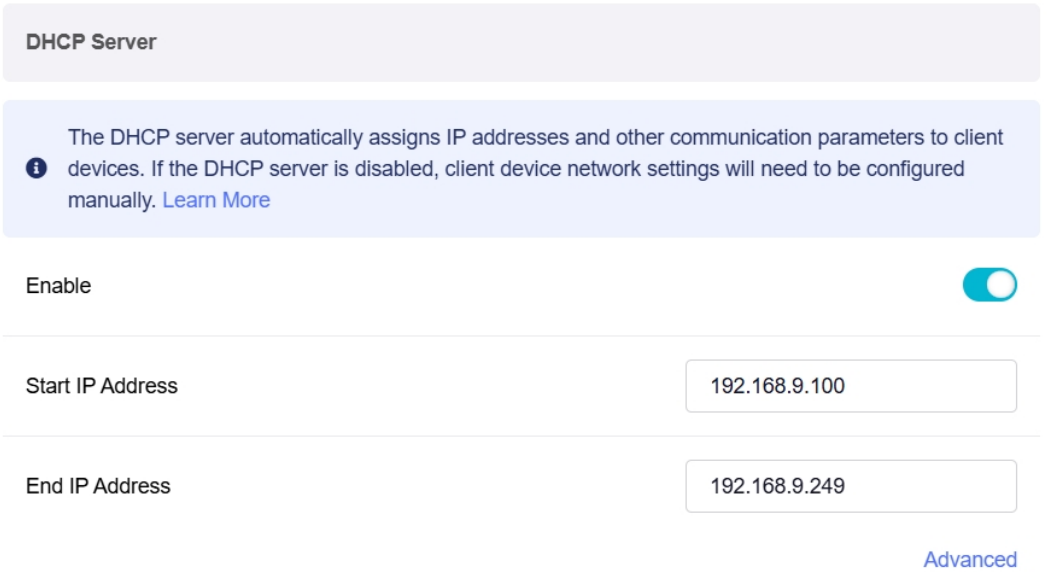
- **Passerelle (Gateway)** : l'adresse par défaut est 192.168.9.1. Vous pouvez la modifier, mais elle ne doit pas entrer en conflit avec la passerelle du réseau principal.
- **Masque de sous-réseau (Netmask)** : deux valeurs sont proposées : 255.255.255.0 et 255.255.0.0.
- **Identifiant VLAN (VAN ID)** : l'identifiant VLAN du réseau invité est 9 par défaut. Vous pouvez le modifier selon vos besoins.
- **Isolation des clients (AP Isolation)** : isole les clients invités dans des segments distincts pour empêcher leur communication avec les autres appareils du même réseau.
- **Contrôle d'accès au WAN (WAN Access Control)** : gère l'accès du sous-réseau local aux réseaux côté WAN, notamment Internet et les autres sous-réseaux WAN.
  Trois modes de contrôle d'accès au WAN sont proposés :
  - **Sans restriction (Unrestricted)** : autorise ce sous-réseau à accéder à Internet et aux autres sous-réseaux côté WAN sans restriction.
  - **Bloquer les sous-réseaux WAN (Block WAN Subnet)** : bloque l'accès aux autres sous-réseaux côté WAN. L'accès à Internet reste disponible.

- **Bloquer l’accès Internet (Block Internet Access)** : bloque tout accès sortant, y compris Internet et les sous-réseaux côté WAN.

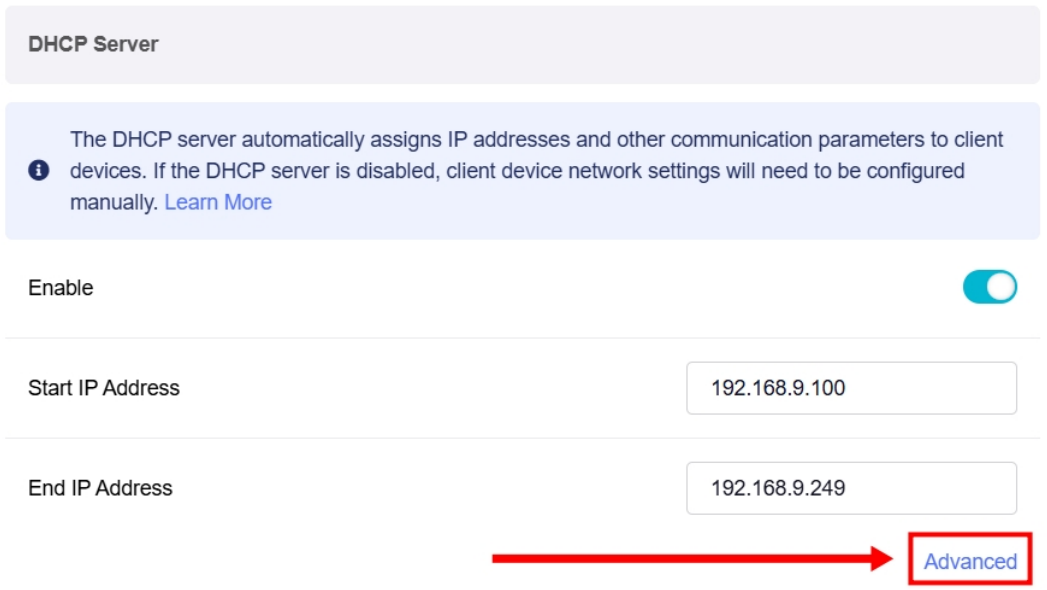
Serveur DHCP

Le réseau invité étant désactivé par défaut, son serveur DHCP reste désactivé et masqué jusqu'à son activation manuelle.

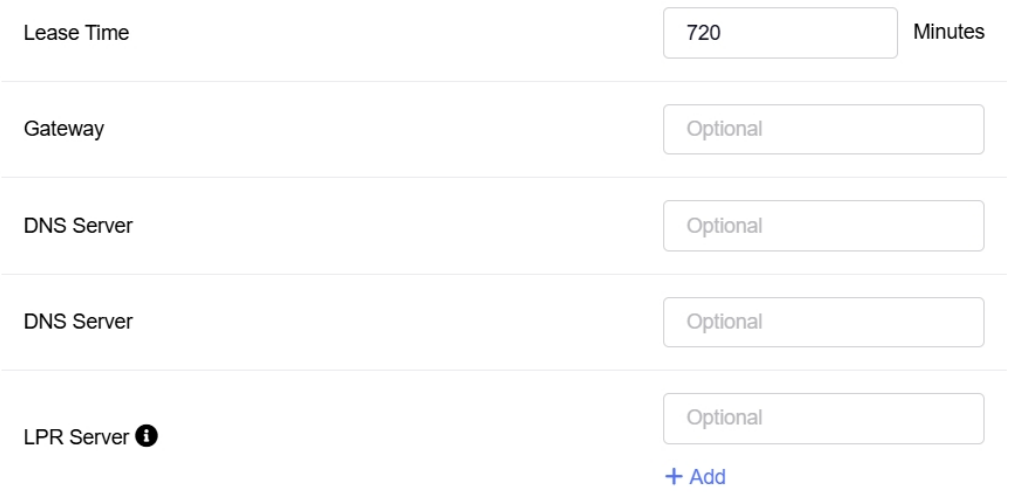
Une fois activé, le serveur DHCP attribue automatiquement une adresse IP et les autres paramètres de communication à chaque client. Sa plage d'adresses s'étend de 192.168.9.100 à 192.168.9.249. Vous pouvez la personnaliser.



Cliquez sur **Avancé (Advanced)** dans l'angle inférieur droit.



Vous pouvez définir la durée du bail, la passerelle, les serveurs DNS et le serveur LPR.



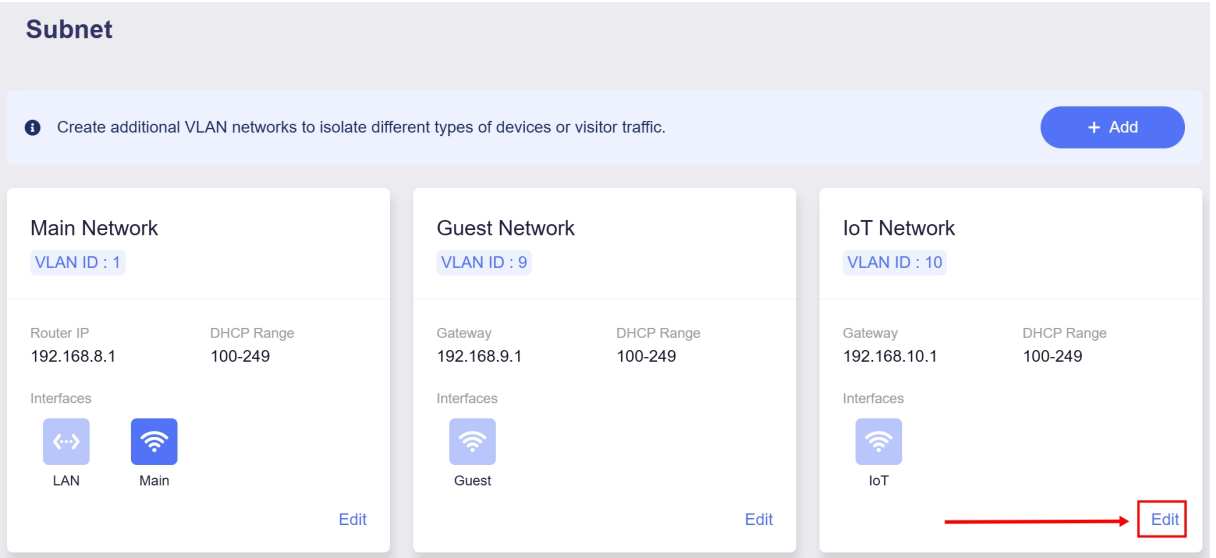
- **Durée du bail (Lease Time)** : durée pendant laquelle un appareil peut utiliser l'adresse IP attribuée par le DHCP du réseau invité.
- **Passerelle (Gateway)** : composant du routeur qui achemine le trafic entre le réseau invité et les réseaux externes, comme Internet.
- **Serveur DNS** : deux champs permettent de configurer les résolveurs principal et secondaire. Saisissez le serveur DNS principal dans le champ supérieur et le secondaire dans le champ inférieur. Si le serveur principal devient indisponible, les appareils clients basculent automatiquement vers le serveur secondaire pour maintenir la résolution des noms de domaine.
- **Serveur LPR (LPR Server)** : le service Line Printer Remote gère les travaux d'impression et permet aux appareils du réseau d'envoyer des demandes d'impression à des imprimantes distantes. Vous pouvez configurer plusieurs ports LPR pour les imprimantes.

12.2.3 Réseau IoT

Le réseau IoT crée un réseau Wi-Fi dédié aux objets connectés. Isolé du réseau principal, il offre une meilleure compatibilité et renforce la sécurité. Vous pouvez consulter directement l'état des interfaces, l'identifiant VLAN, la passerelle et la plage DHCP.

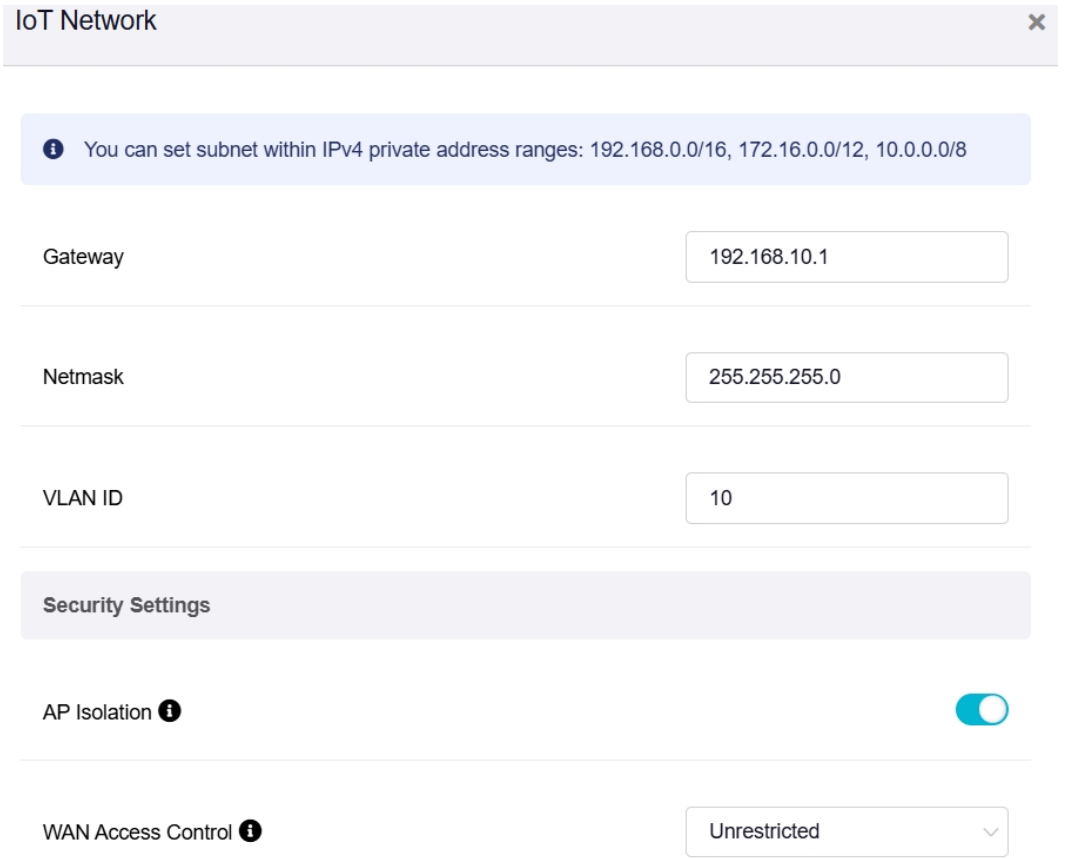
Dans l'interface Web du routeur, ouvrez **RÉSEAU (NETWORK)** > **Sous-réseau (Subnet)** > **Réseau IoT (IoT Network)**. Cette page permet de configurer le réseau IoT, notamment les paramètres de base et le serveur DHCP.

Cliquez sur **Modifier (Edit)** en bas à droite pour configurer le réseau invité.



Paramètres de base

Les paramètres de base comprennent la passerelle, le masque de sous-réseau, l'isolation des clients, l'identifiant VLAN et le contrôle d'accès au WAN.

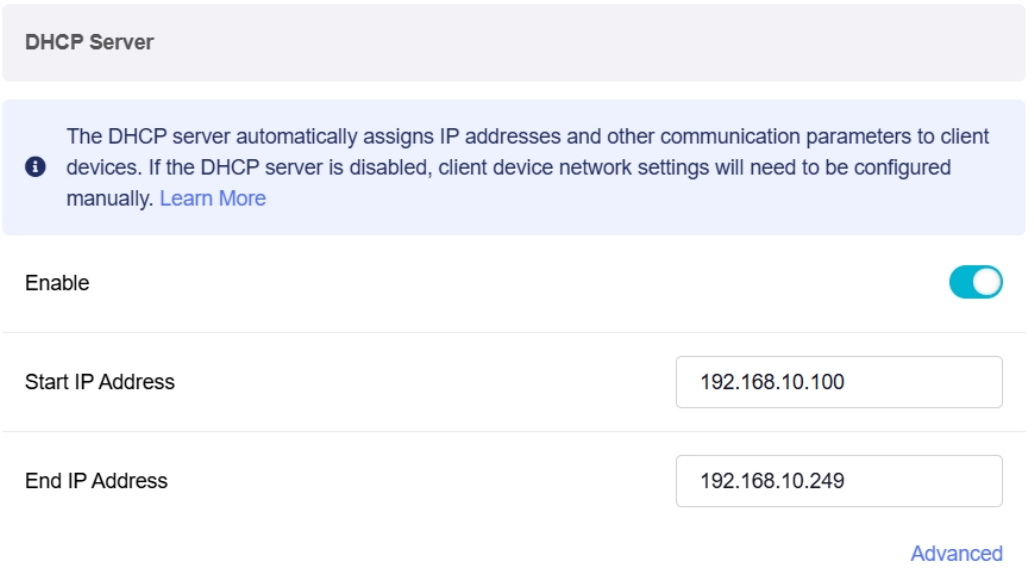


- **Passerelle (Gateway)** : l'adresse par défaut est 192.168.10.1. Vous pouvez la modifier, mais elle ne doit pas entrer en conflit avec la passerelle du réseau principal.
- **Masque de sous-réseau (Netmask)** : deux valeurs sont proposées : 255.255.255.0 et 255.255.0.0.
- **Identifiant VLAN (VAN ID)** : l'identifiant VLAN du réseau invité est 10 par défaut. Vous pouvez le modifier selon vos besoins.
- **Isolation des clients (AP Isolation)** : isole les clients invités dans des segments distincts pour empêcher leur communication avec les autres appareils du même réseau.
- **Contrôle d'accès au WAN (WAN Access Control)** : gère l'accès du sous-réseau local aux réseaux côté WAN, notamment Internet et les autres sous-réseaux WAN.
  Trois modes de contrôle d'accès au WAN sont proposés :
  - **Sans restriction (Unrestricted)** : autorise ce sous-réseau à accéder à Internet et aux autres sous-réseaux côté WAN sans restriction.
  - **Bloquer les sous-réseaux WAN (Block WAN Subnet)** : bloque l'accès aux autres sous-réseaux côté WAN. L'accès à Internet reste disponible.
  - **Bloquer l'accès Internet (Block Internet Access)** : bloque tout accès sortant, y compris Internet et les sous-réseaux côté WAN.

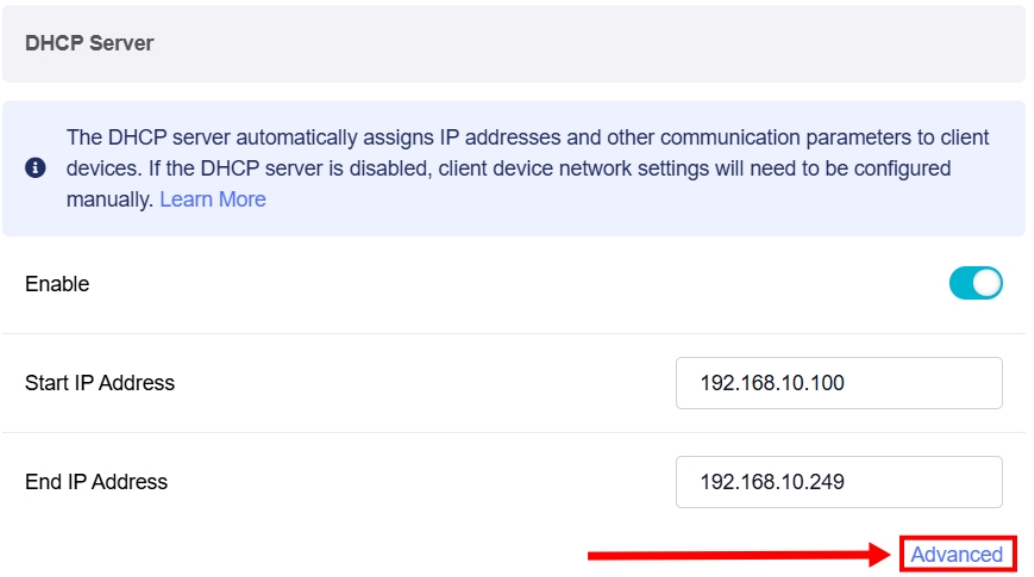
Serveur DHCP

Le réseau IoT étant désactivé par défaut, son serveur DHCP reste désactivé et masqué jusqu'à son activation manuelle.

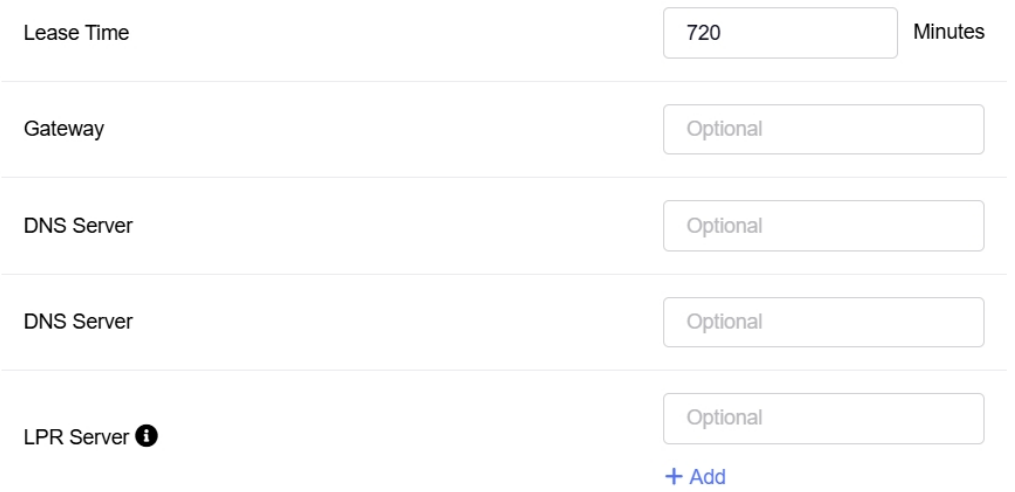
Une fois activé, le serveur DHCP attribue automatiquement une adresse IP et les autres paramètres de communication à chaque client connecté. La plage d'adresses du réseau IoT s'étend de 192.168.10.100 à 192.168.10.249. Vous pouvez la personnaliser.



Cliquez sur **Avancé (Advanced)** dans l'angle inférieur droit.



Vous pouvez définir la durée du bail, la passerelle, les serveurs DNS et le serveur LPR.

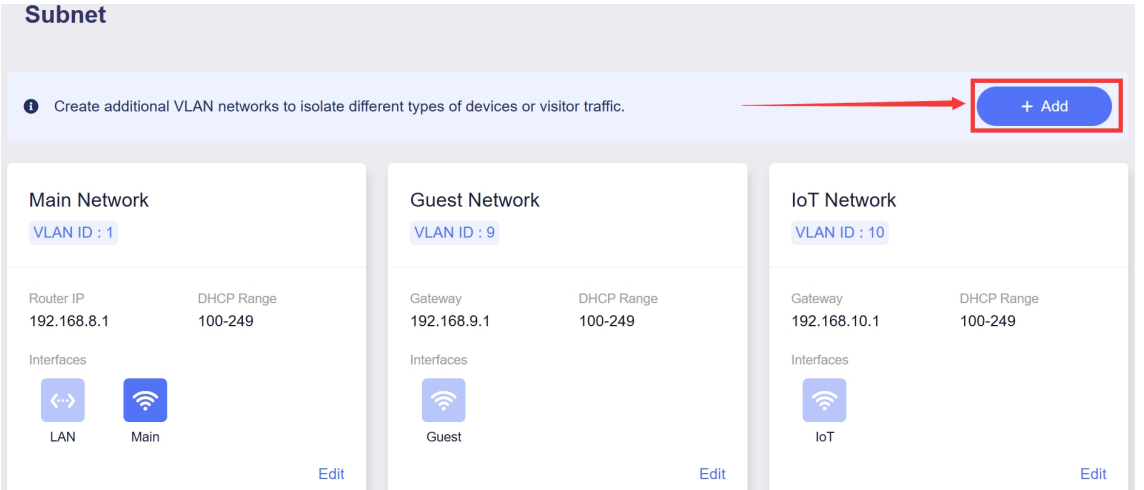


- **Durée du bail (Lease Time)** : durée pendant laquelle un appareil peut utiliser l'adresse IP attribuée par le DHCP du réseau invité.
- **Passerelle (Gateway)** : composant du routeur qui achemine le trafic entre le réseau invité et les réseaux externes, comme Internet.
- **Serveur DNS** : deux champs permettent de configurer les résolveurs principal et secondaire. Saisissez le serveur DNS principal dans le champ supérieur et le secondaire dans le champ inférieur. Si le serveur principal devient indisponible, les appareils clients basculent automatiquement vers le serveur secondaire pour maintenir la résolution des noms de domaine.
- **Serveur LPR (LPR Server)** : le service Line Printer Remote gère les travaux d'impression et permet aux appareils du réseau d'envoyer des demandes d'impression à des imprimantes distantes. Vous pouvez configurer plusieurs ports LPR pour les imprimantes.

12.2.4 Réseaux VLAN

La rubrique Réseaux VLAN permet de créer des réseaux VLAN supplémentaires pour isoler différents types d'appareils ou le trafic des visiteurs selon vos besoins.

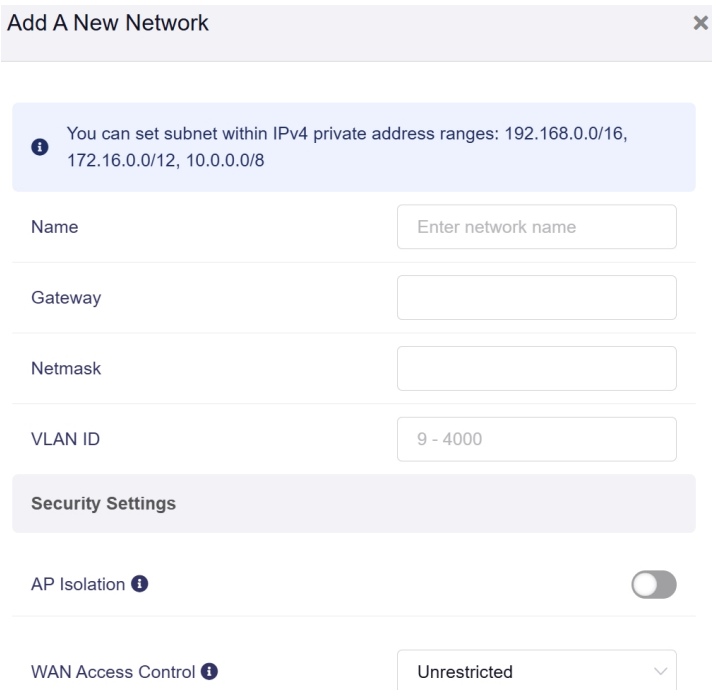
Cliquez sur **+ Ajouter (+ Add)** à droite de la page pour configurer un nouveau réseau.



Cette page permet de configurer les réseaux VLAN, notamment les paramètres de base et le serveur DHCP.

Paramètres de base

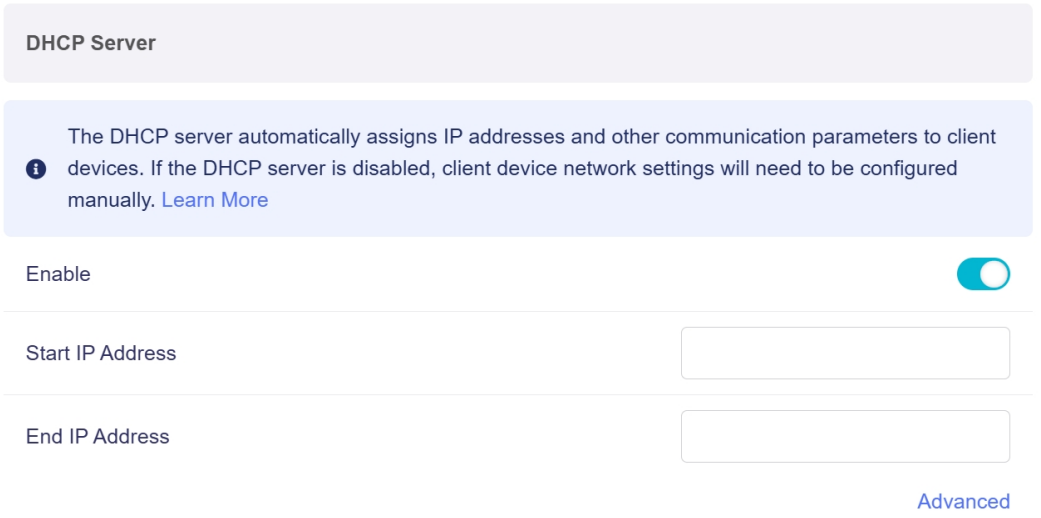
Cette page permet de configurer les informations de base des réseaux VLAN.



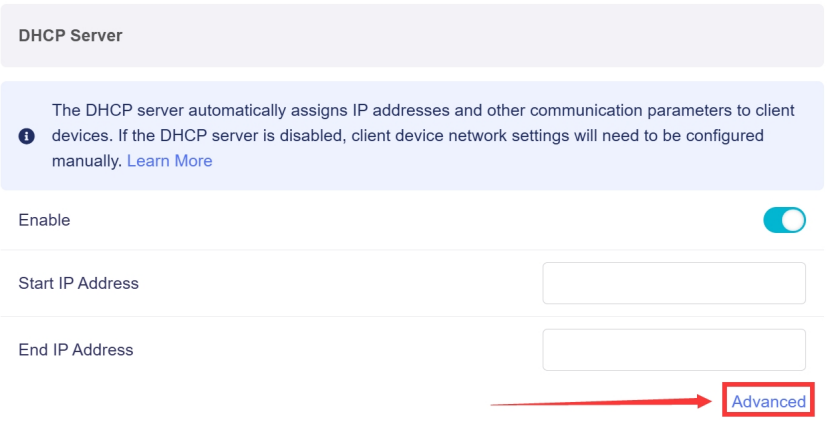
- **Nom (Name)** : donnez un nom au nouveau sous-réseau pour l'identifier.
- **Passerelle (Gateway)** : l'adresse par défaut est 192.168.10.1. Vous pouvez la modifier, mais elle ne doit pas entrer en conflit avec la passerelle du réseau principal.
- **Masque de sous-réseau (Netmask)** : deux valeurs sont proposées : 255.255.255.0 et 255.255.0.0.
- **Identifiant VLAN (VAN ID)** : lors de la création d'un sous-réseau, attribuez-lui un identifiant VLAN compris entre 9 et 4 000. N'utilisez pas un identifiant déjà occupé, pour éviter les conflits réseau.
- **Isolation des clients (AP Isolation)** : isole les clients invités dans des segments distincts pour empêcher leur communication avec les autres appareils du même réseau.
- **Contrôle d'accès au WAN (WAN Access Control)** : gère l'accès du sous-réseau local aux réseaux côté WAN, notamment Internet et les autres sous-réseaux WAN.
  Trois modes de contrôle d'accès au WAN sont proposés :
  - **Sans restriction (Unrestricted)** : autorise ce sous-réseau à accéder à Internet et aux autres sous-réseaux côté WAN sans restriction.
  - **Bloquer les sous-réseaux WAN (Block WAN Subnet)** : bloque l'accès aux autres sous-réseaux côté WAN. L'accès à Internet reste disponible.
  - **Bloquer l'accès Internet (Block Internet Access)** : bloque tout accès sortant, y compris Internet et les sous-réseaux côté WAN.

Serveur DHCP

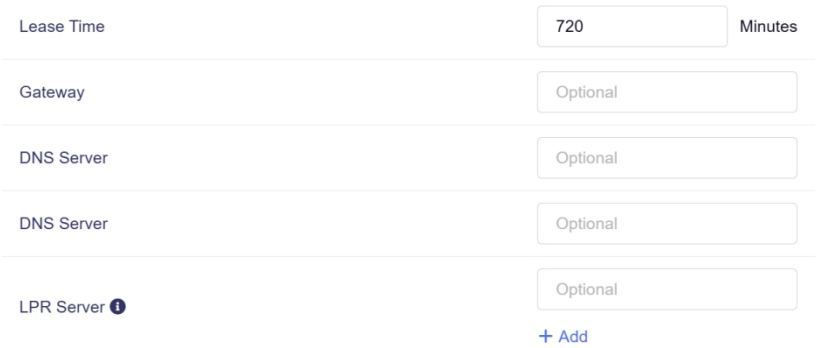
Une fois activé, le serveur DHCP attribue automatiquement une adresse IP et les autres paramètres de communication à chaque client connecté. Vous pouvez personnaliser la plage d'adresses.



Cliquez sur **Avancé (Advanced)** pour accéder à d'autres paramètres si nécessaire.



Vous pouvez définir la durée du bail, la passerelle, les serveurs DNS et le serveur LPR.



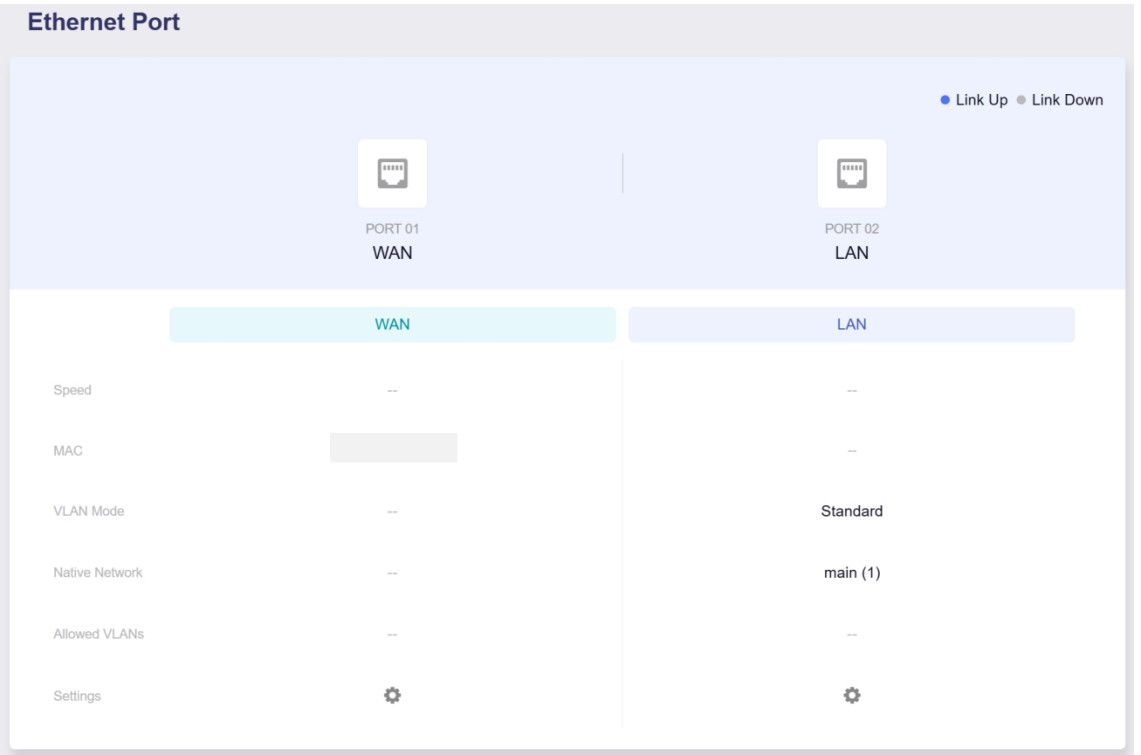
- **Durée du bail (Lease Time)** : durée pendant laquelle un appareil peut utiliser l'adresse IP attribuée par le DHCP du réseau invité.
- **Passerelle (Gateway)** : composant du routeur qui achemine le trafic entre le réseau invité et les réseaux externes, comme Internet.
- **Serveur DNS** : deux champs permettent de configurer les résolveurs principal et secondaire. Saisissez le serveur DNS principal dans le champ supérieur et le secondaire dans le champ inférieur. Si le serveur principal devient indisponible, les appareils clients basculent automatiquement vers le serveur secondaire pour maintenir la résolution des noms de domaine.
- **Serveur LPR (LPR Server)** : le service Line Printer Remote gère les travaux d'impression et permet aux appareils du réseau d'envoyer des demandes d'impression à des imprimantes distantes. Vous pouvez configurer plusieurs ports LPR pour les imprimantes.

Une fois configuré, le nouveau réseau VLAN apparaît sur la page avec les informations du sous-réseau.

12.3 Ports Ethernet

Dans l'interface Web du routeur, ouvrez **RÉSEAU (NETWORK)** > **Ports Ethernet (Ethernet Port)**. Cette page permet de gérer les ports Ethernet du routeur.

La page Ports Ethernet affiche toutes les interfaces du routeur. Vous pouvez consulter leur état de connexion, définir le rôle des ports Ethernet (WAN ou LAN) et voir leurs détails : adresse MAC, débit négocié et état actuel de la liaison. Vous pouvez aussi affecter les interfaces physiques aux sous-réseaux que vous avez créés.

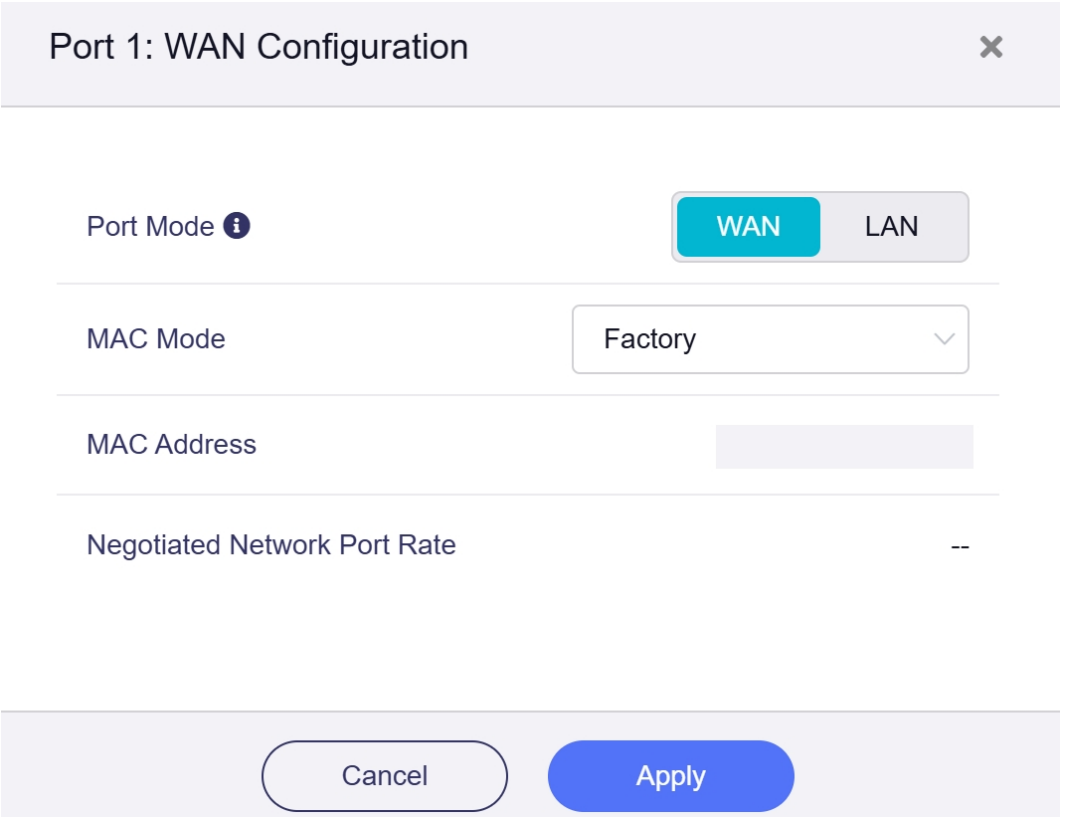


- **Liaison active (Link up)** : lorsque l'icône du port est bleue, la liaison physique est active.
- **Liaison inactive (Link Down)** : lorsque l'icône du port est grise, la liaison physique est inactive.
- **Débit (Speed)** : débit de transmission négocié du port Ethernet.
- **MAC** : adresse MAC du port.
- **Identifiant VLAN (VLAN ID)** : les ports LAN peuvent fonctionner en mode Standard ou VLAN multiples.
- **Réseau natif (Native Network)** : sous-réseau par défaut, non balisé, affecté au port LAN.

- **VLAN autorisés (Allowed VLANs)** : VLAN balisés autorisés à traverser ce port en mode VLAN multiples.
- **Paramètres (Settings)** : cliquez pour ouvrir la page de configuration du port concerné.

12.3.1 WAN

La section **WAN** affiche le rôle du port, WAN ou LAN, son adresse MAC et le débit négocié.



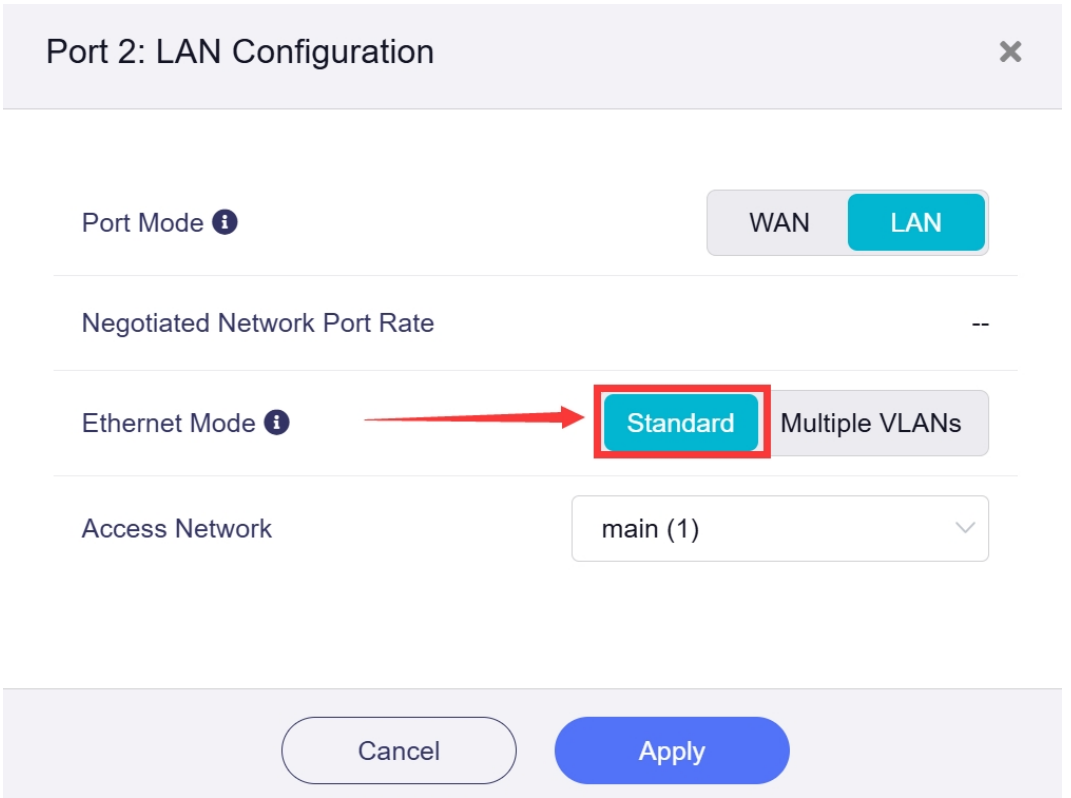
- **Mode du port (Port Mode)** : mode de fonctionnement actuel du port WAN physique. Vous pouvez le définir sur LAN selon vos besoins.
- **Mode MAC (MAC Mode) :** le mode d'usine est utilisé par défaut. Vous pouvez choisir le mode clonage ou le mode aléatoire.
- **Adresse MAC (MAC Address)** : adresse MAC de l'interface WAN.
- **Débit négocié du port réseau (Negotiated Network Port Rate) :** vitesse de liaison négociée de l'interface WAN, affichée uniquement lorsqu'une liaison valide est détectée.

12.3.2 LAN

La section **LAN** affiche la configuration du port LAN. Vous pouvez définir le rôle du port sur **LAN** ou **WAN**, choisir son mode Ethernet (Standard ou plusieurs VLAN) et consulter le débit de liaison négocié.

1. Mode standard

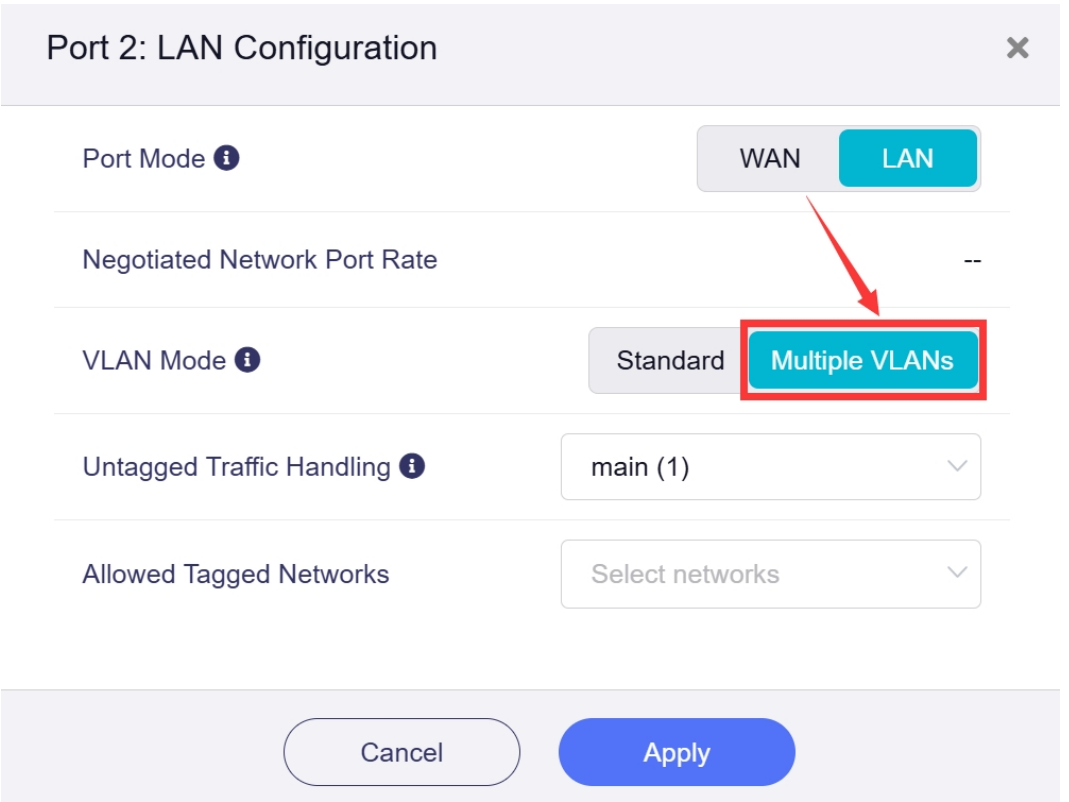
   Le mode standard autorise un seul VLAN non étiqueté (Untagged) et sert à connecter des appareils terminaux.



- **Débit négocié du port réseau (Negotiated Network Port Rate)** : vitesse de liaison négociée de l'interface WAN, affichée uniquement lorsqu'une liaison valide est détectée.
- **Mode Ethernet (Ethernet Mode)** : le mode standard est sélectionné par défaut.
- **Réseau d'accès (Access Network)** : permet d'isoler les réseaux en affectant les ports LAN à différents sous-réseaux.

2. Mode Plusieurs VLAN

Le mode Plusieurs VLAN permet de transporter plusieurs VLAN étiquetés (Tagged) sur un même port. Il sert généralement à connecter des points d'accès ou d'autres commutateurs.



- **Débit négocié du port réseau (Negotiated Network Port Rate)** : vitesse de liaison négociée de l'interface WAN, affichée uniquement lorsqu'une liaison valide est détectée.
- **Mode VLAN (VLAN Mode)** : pour passer au mode Plusieurs VLAN, cliquez sur l'onglet Multiple VLANs.
- **Traitement du trafic non étiqueté (Untagged Traffic Handling)** : configurez le traitement des paquets non étiquetés sur ce port. Vous pouvez les rejeter directement ou les transférer vers un autre sous-réseau, qui devient le réseau natif associé au PVID.
- **Réseaux étiquetés autorisés (Allowed Tagged Networks)** : définit les VLAN autorisés à traverser ce port en mode étiqueté. Sélectionnez les réseaux VLAN dans la liste ; seul le trafic correspondant sera transmis.

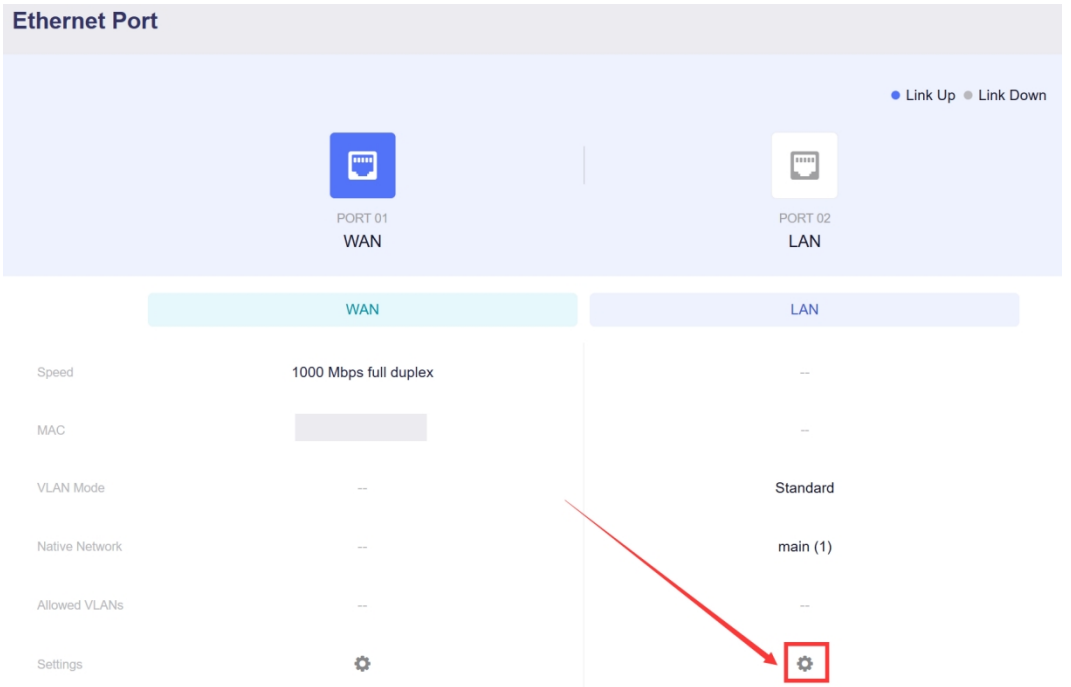
Remarque : le débit négocié d'un port WAN ou LAN s'affiche uniquement lorsqu'un câble Ethernet est branché.

Ce débit dépend des capacités du port et du câble Ethernet.

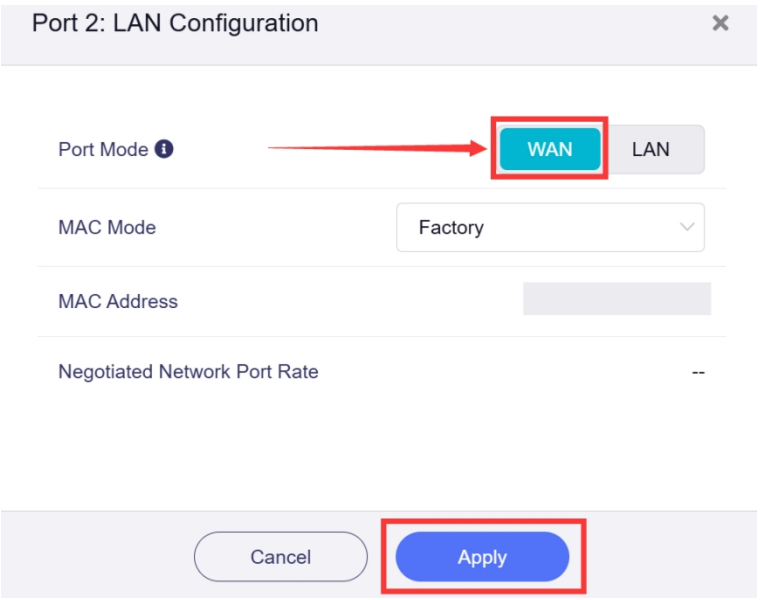
12.3.3 Double connexion WAN Ethernet

La fonction de double connexion WAN Ethernet permet de convertir un port Ethernet LAN en un second port WAN, afin de disposer de deux connexions Internet Ethernet. Elle permet également de se connecter simultanément à deux réseaux indépendants, par exemple professionnel et personnel, pour davantage de souplesse sans matériel supplémentaire.

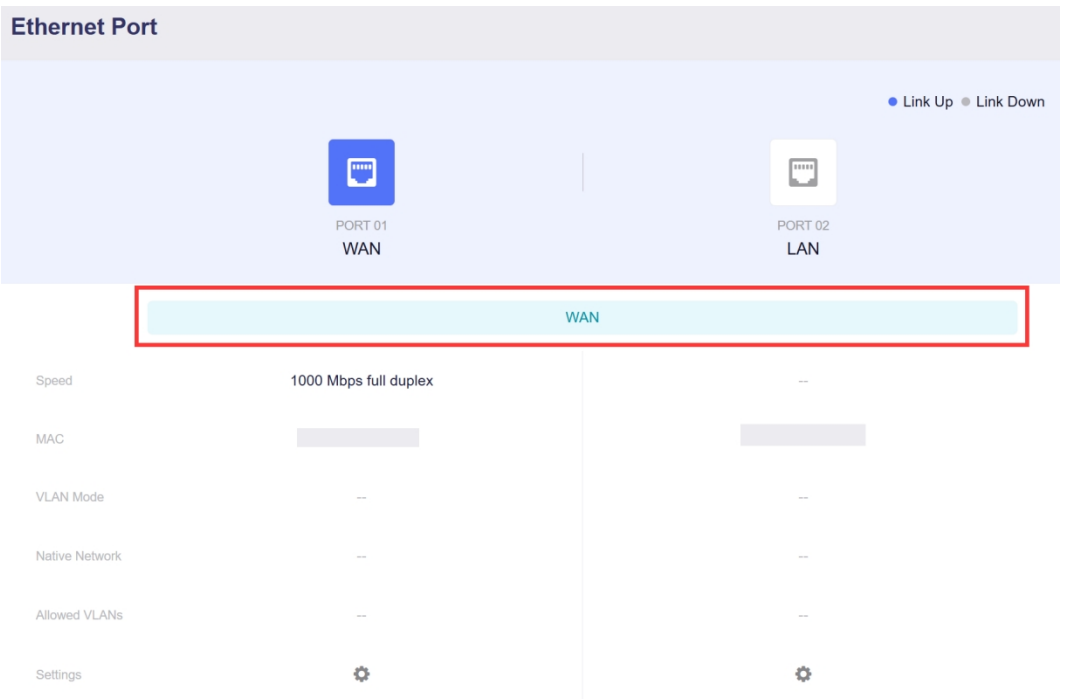
1. Sur la page Port Ethernet, cliquez sur le paramètre LAN pour ouvrir la page de configuration.



2. Sélectionnez WAN comme rôle du port, puis cliquez sur **Appliquer (Apply)**.



3. Revenez à la page Port Ethernet pour vérifier que le rôle du port est passé à WAN. Le port LAN fonctionne alors comme un port WAN.

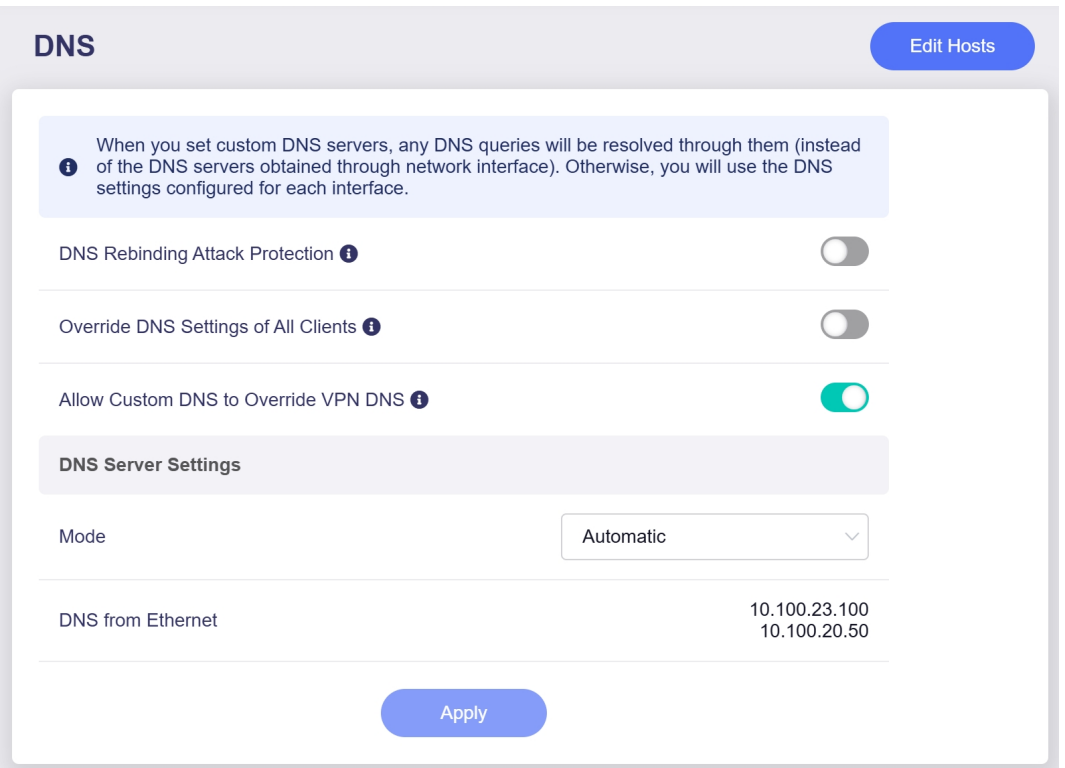


12.4 DNS

Le DNS (Domain Name System, système de noms de domaine) convertit les noms de domaine lisibles, comme www.google.com, en adresses IP utilisables par les appareils, comme 142.250.185.142, pour accéder aux sites et aux services.

Le serveur DNS du routeur est le service DNS intégré qui traduit les noms de domaine en adresses IP pour tous les appareils connectés. Il fonctionne généralement de deux façons : il récupère automatiquement les adresses DNS du réseau en amont pour assurer la résolution par défaut, ou utilise les adresses DNS publiques personnalisées (par exemple 8.8.8.8) que vous configurez dans l'interface d'administration Web pour optimiser l'accès au réseau ou renforcer la sécurité. Une fois la configuration effectuée, tous les appareils connectés utilisent ce même serveur DNS par défaut, sans configuration DNS individuelle.

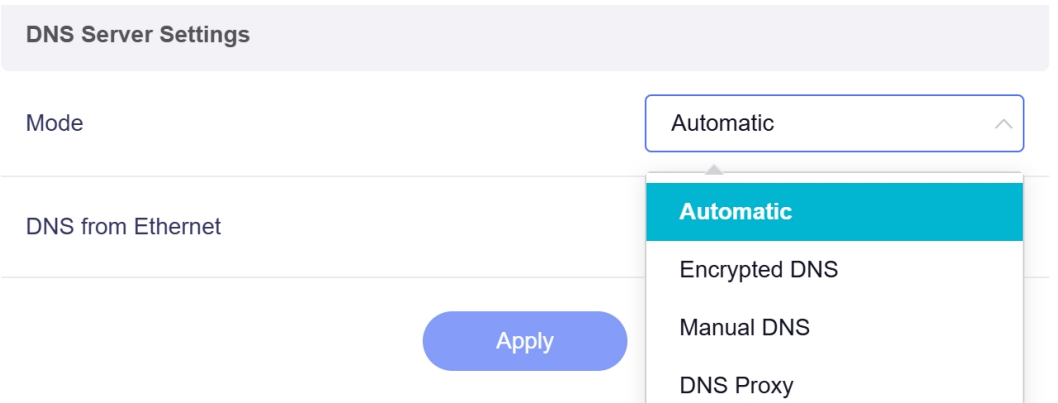
Connectez-vous à l'interface d'administration Web du routeur et ouvrez **RÉSEAU (NETWORK)** > **DNS**. Cette page permet de configurer les paramètres DNS, notamment les options de sécurité, les modes du serveur et les règles de priorité DNS selon les situations réseau.



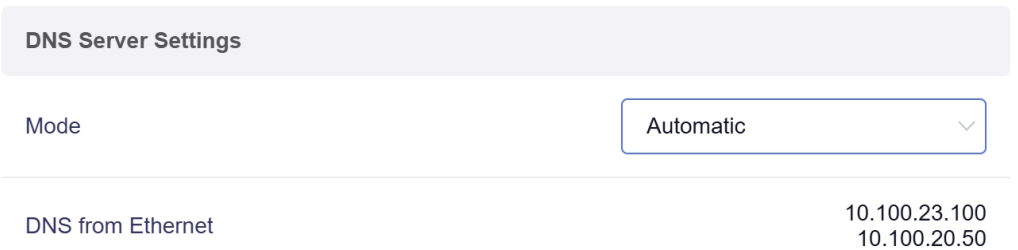
- **Protection contre le rebinding DNS (DNS Rebinding Attack Protection)** : bloque les tentatives malveillantes de résolution DNS. Elle peut toutefois empêcher certaines résolutions DNS privées. Désactivez-la si votre réseau utilise un portail captif, comme une page de connexion Wi-Fi publique.
- **Remplacer les paramètres DNS de tous les clients (Override DNS Settings of All Clients)** : impose les serveurs DNS du routeur à tous les appareils connectés, indépendamment de leurs propres réglages, pour une configuration DNS uniforme.
- **Autoriser le DNS personnalisé à remplacer le DNS VPN (Allow Custom DNS to Override VPN DNS)** : si un DNS personnalisé est défini, le trafic passant par le tunnel VPN l'utilise à la place du DNS de la connexion VPN. Vos règles DNS personnalisées restent ainsi applicables lorsque vous utilisez le VPN.

12.4.1 Paramètres du serveur DNS

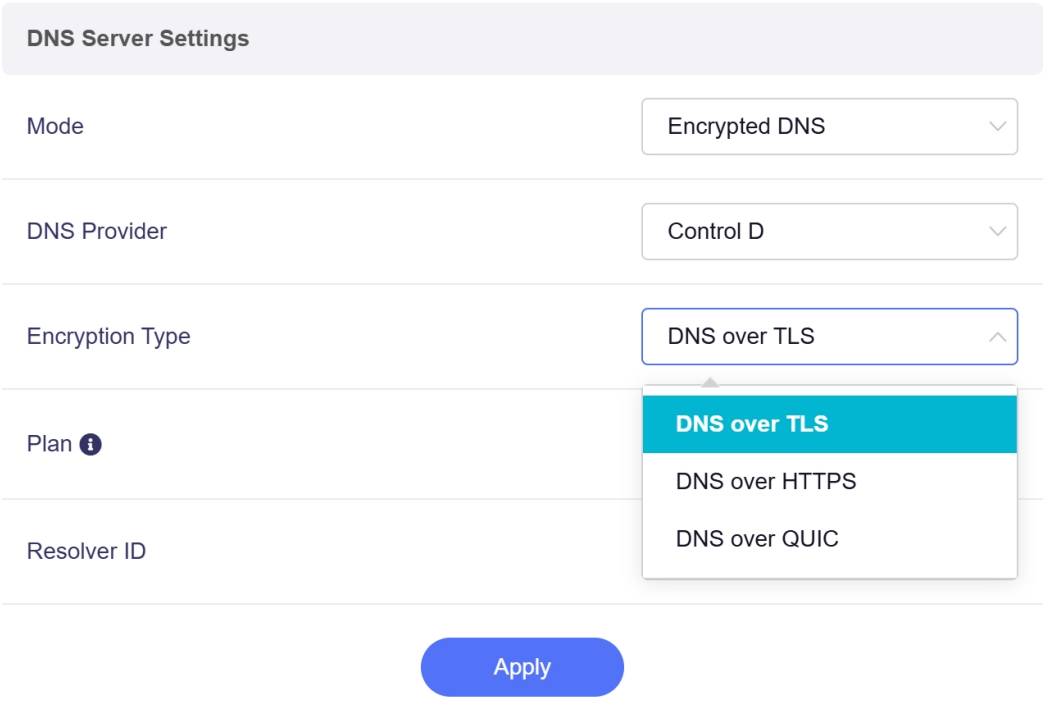
Quatre modes sont proposés : Automatique, DNS chiffré, DNS manuel et Proxy DNS.



1. **Automatique (Automatic)** : le routeur obtient les adresses des serveurs DNS du réseau en amont et les applique à tous les appareils connectés.

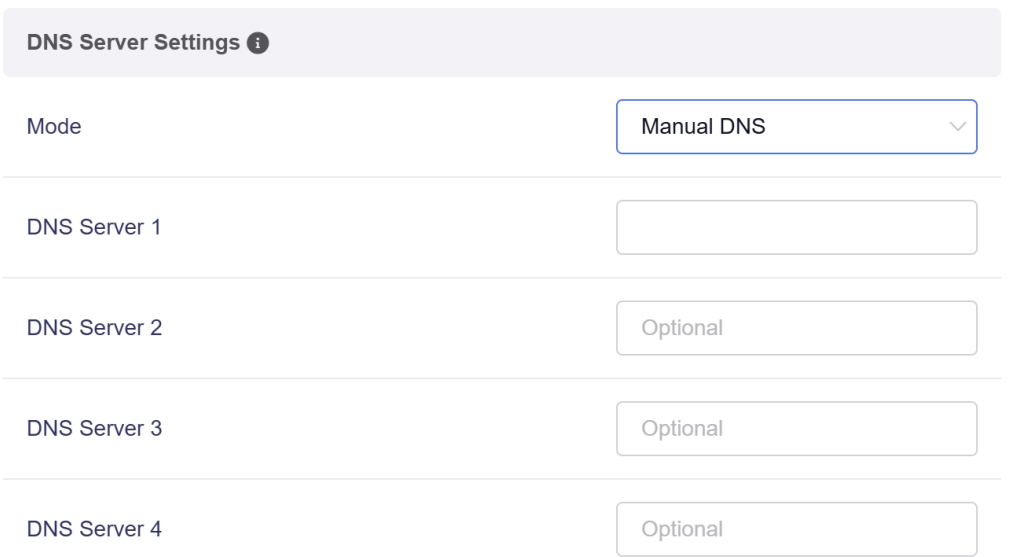


2. **DNS chiffré (Encrypted DNS)** : utilise des protocoles chiffrés pour traiter les requêtes DNS et protéger les données de résolution contre l'écoute et l'altération.
   Quatre types de chiffrement sont proposés : DNS over TLS, DNSCrypt-Proxy, DNS over HTTPS et Oblivious DNS over HTTPS.



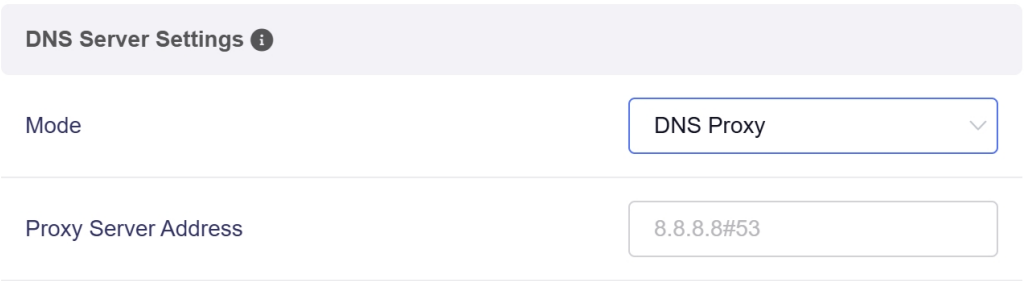
- Pour DNS over TLS, choisissez Control D, NextDNS ou Cloudflare comme fournisseur DNS.
- Pour les trois autres types, sélectionnez au moins un serveur DNS dans la liste, et jusqu'à huit serveurs. Si vous en sélectionnez plusieurs, le routeur utilise automatiquement le plus rapide.

3. **DNS manuel (Manual DNS)** : permet de personnaliser les serveurs DNS du routeur. Cliquez sur Serveur DNS 1 et choisissez un serveur dans la liste. Les autres champs DNS sont renseignés automatiquement.



Remarque : pour renseigner des adresses IPv6 dans le DNS manuel, activez d'abord IPv6 sur le routeur.

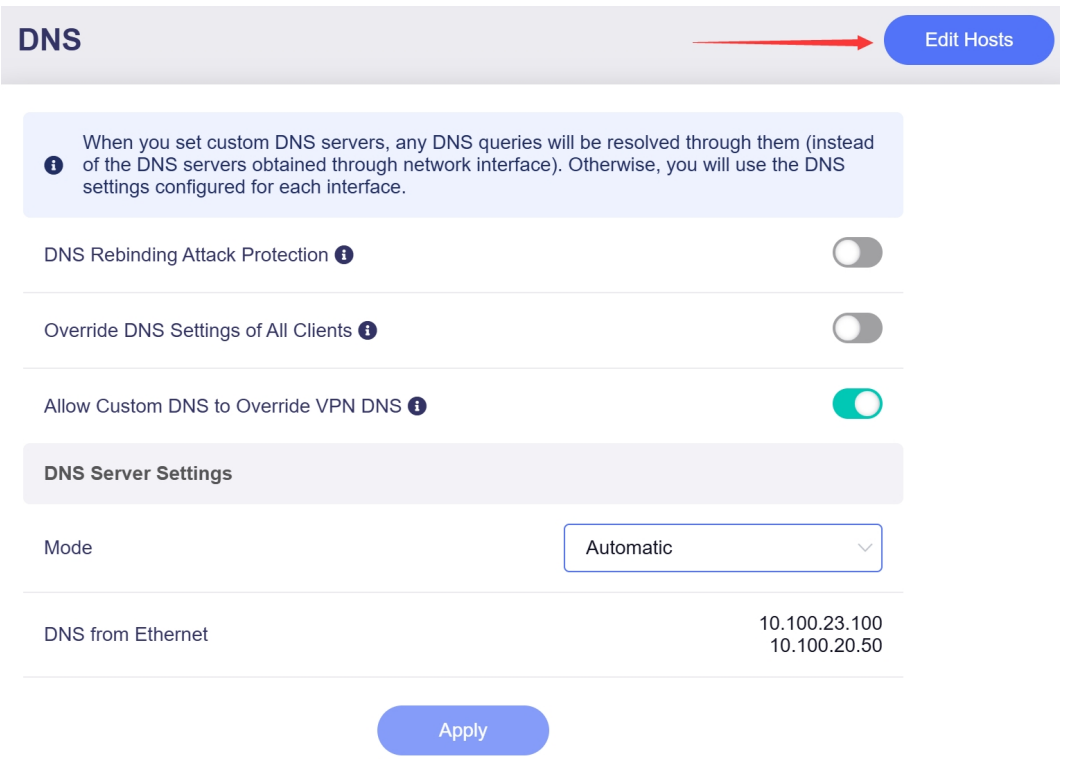
4. **Proxy DNS (DNS Proxy)** : transmet toutes les requêtes DNS par un serveur proxy et utilise son environnement réseau pour la résolution, selon vos besoins d'accès.



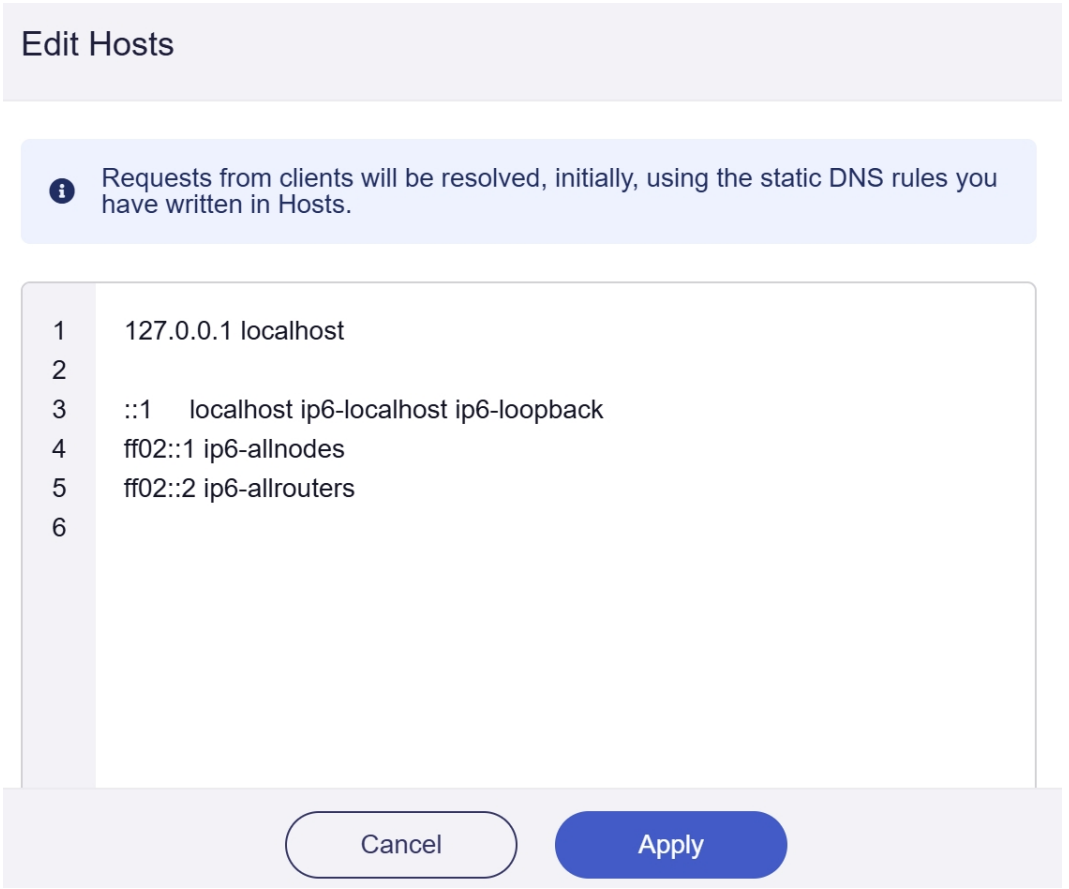
12.4.2 Modification du fichier hosts

Vous pouvez définir des règles statiques de résolution DNS.

Sur la page DNS, cliquez sur **Modifier hosts (Edit Hosts)** dans l'angle supérieur droit.



Les requêtes des clients sont résolues en priorité avec les règles statiques saisies ici. Vous pouvez associer manuellement des adresses IP à des noms d'hôtes, comme l'entrée de bouclage locale 127.0.0.1 localhost, pour personnaliser la résolution des noms.

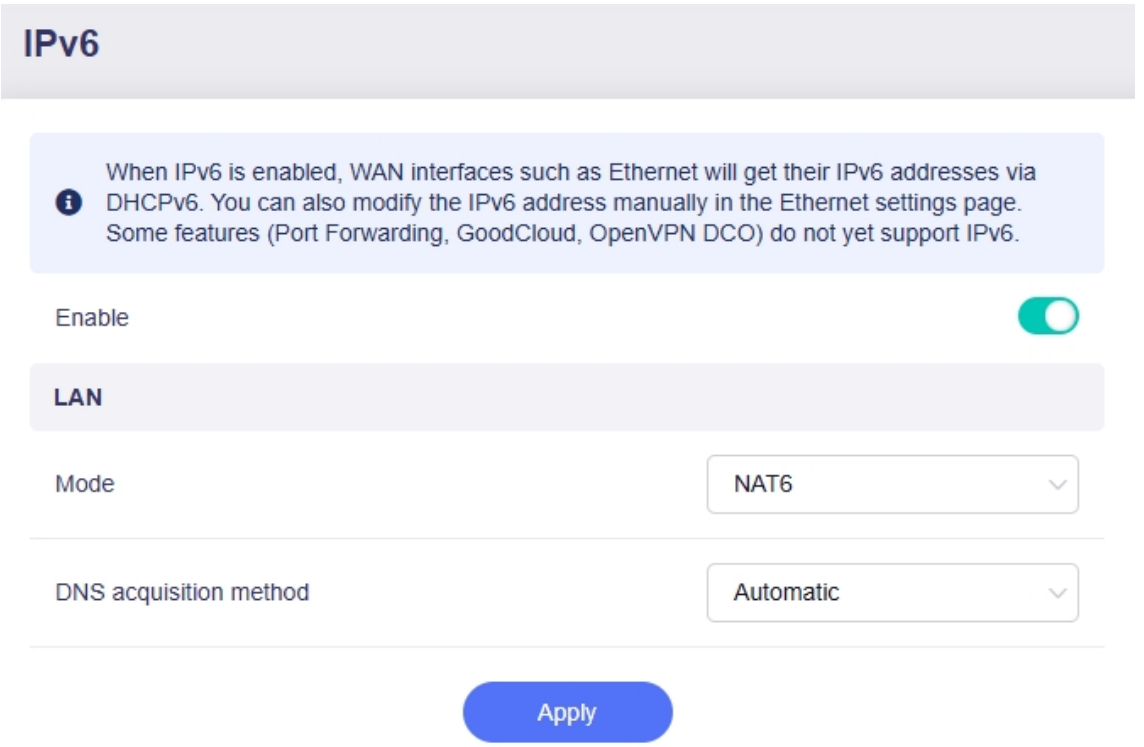

Edit Hosts
Requests from clients will be resolved, initially, using the static DNS rules you have written in Hosts.
1 127.0.0.1 localhost
2
3 ::1 localhost ip6-localhost ip6-loopback
4 ff02::1 ip6-allnodes
5 ff02::2 ip6-allrouters
6
Cancel
Apply

12.5 IPv6

IPv6 (Internet Protocol version 6) est la version la plus récente du protocole Internet, conçue pour remplacer IPv4. Son espace d'adressage beaucoup plus vaste répond à l'épuisement des adresses IPv4 et à la croissance mondiale du nombre d'appareils connectés.

Connectez-vous à l'interface d'administration Web du routeur et ouvrez **RÉSEAU (NETWORK)** > **IPv6**. Cette page permet d'activer et de configurer IPv6. Lorsque cette fonction est activée, les interfaces WAN, comme Ethernet, obtiennent leur adresse IPv6 via DHCPv6.

Activez l'option **Activer (Enable)**, choisissez le mode du réseau principal et la méthode d'obtention du DNS, puis cliquez sur **Appliquer (Apply).**



Remarque : certaines fonctions, comme le pare-feu, GoodCloud et OpenVPN DCO, ne prennent pas encore en charge IPv6. Leur activation simultanée avec IPv6 peut provoquer des problèmes de connexion.

12.5.1 Mode IPv6

Quatre modes sont disponibles : Natif, Passthrough, NAT6 et IPv6 statique.

- **Natif (Native)** : convient lorsque le routeur obtient directement une adresse IPv6 publique et attribue automatiquement des adresses IPv6 aux appareils connectés. Il répond aux besoins IPv6 de la plupart des utilisateurs.
- **Transmission directe (Passthrough)** : transmet les paquets IPv6 sans traitement ni conversion. Certaines applications ou certains services nécessitent de préserver intégralement les paquets pour les traiter ou les analyser. Ce mode est utilisé pour le dépannage réseau ou l'analyse de sécurité.
- **NAT6** : convient lorsque le routeur sert de passerelle et attribue des adresses IPv6 internes dynamiques aux appareils du réseau. Les terminaux se connectent par un terminal de réseau optique (ONT) et obtiennent une adresse IPv6 du réseau local.
- **IPv6 statique (Static IPv6)** : convient aux appareils ou services nécessitant une adresse IPv6 fixe, comme les serveurs ou les imprimantes réseau. L'adresse reste identique, ce qui facilite la gestion et l'accès.

12.5.2 Méthode d'obtention du DNS

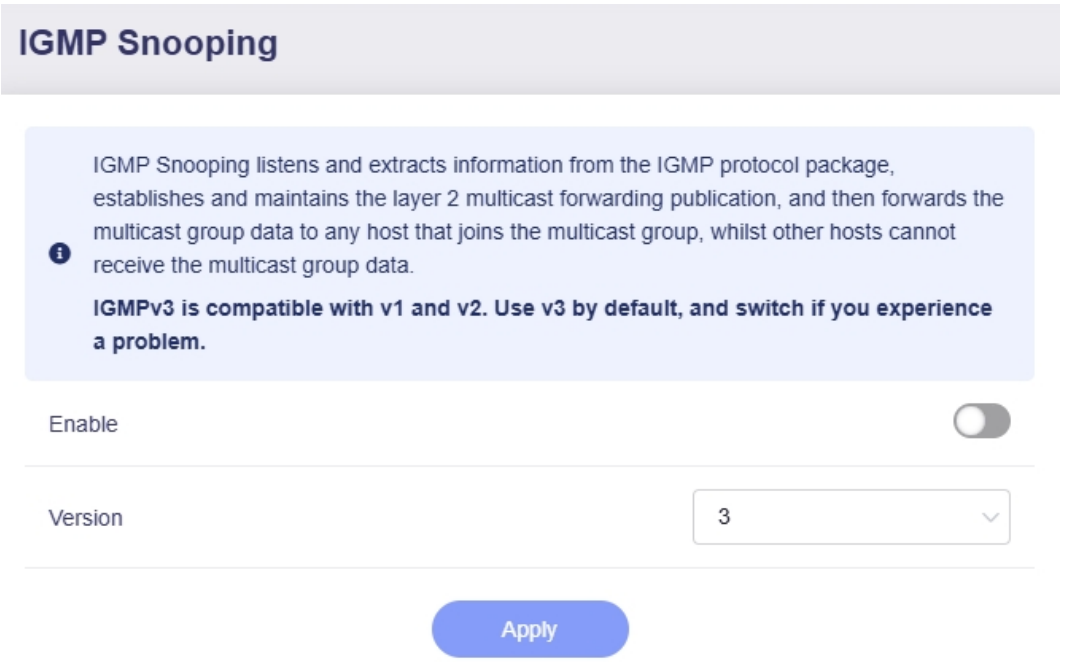
Ce paramètre détermine comment le routeur obtient les adresses des serveurs DNS IPv6. Deux options sont disponibles : Automatique et Manuelle.

- **Automatique (Automatic)** : le routeur obtient les adresses DNS IPv6 dynamiquement, par exemple via DHCPv6.
- **Manuelle (Manual)** : saisissez les adresses des serveurs DNS IPv6 souhaités. Une configuration manuelle incorrecte peut empêcher la résolution des noms de domaine en adresses IP. Utilisez-la avec prudence.

12.6 IGMP Snooping

IGMP Snooping analyse les paquets IGMP, en extrait les informations et crée puis maintient une table de transfert multicast de couche 2. Les données multicast sont ensuite transmises uniquement aux hôtes ayant rejoint le groupe correspondant.

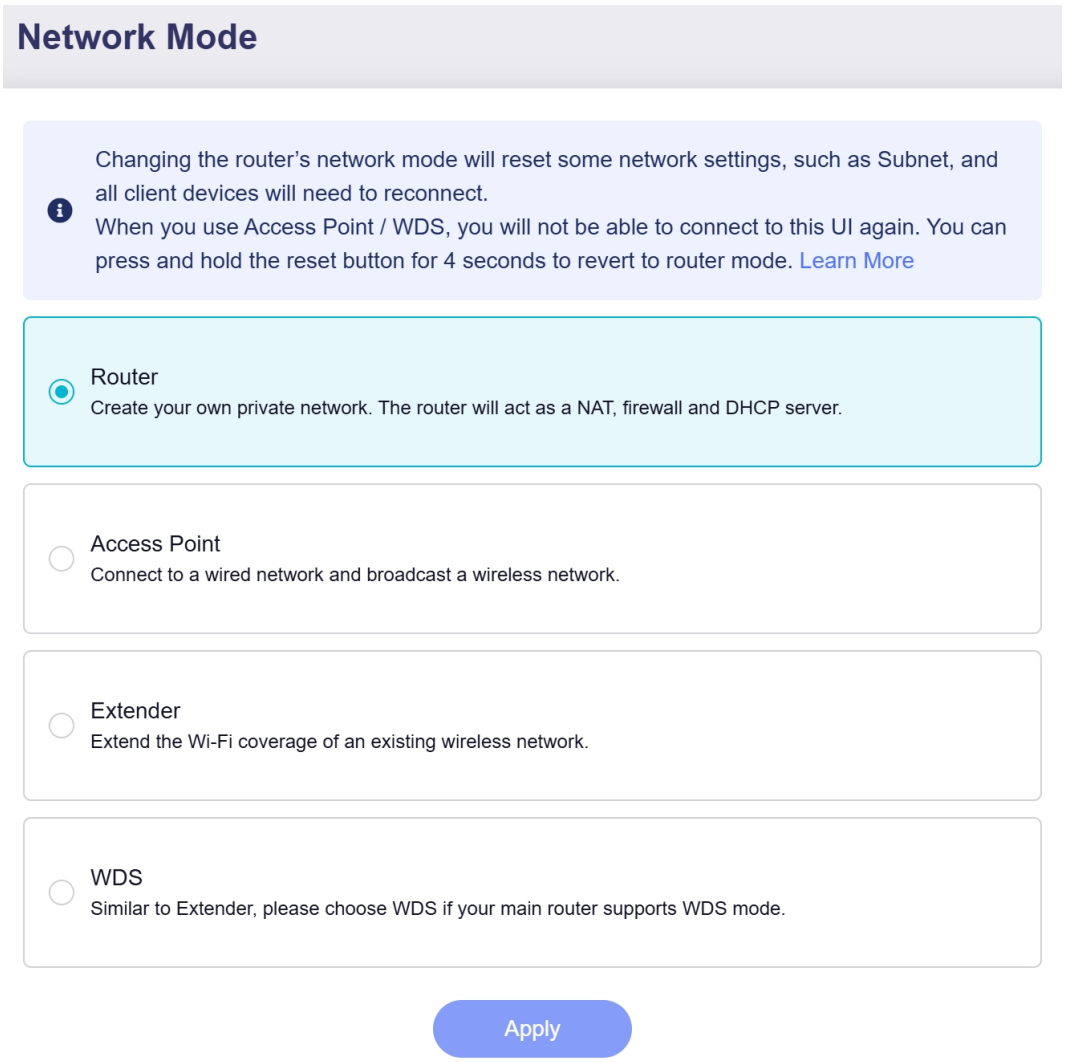
Connectez-vous à l'interface d'administration Web du routeur et ouvrez **RÉSEAU (NETWORK)** > **IGMP Snooping**. Vous pouvez activer cette option pour utiliser la multidiffusion sur le routeur, si nécessaire.



12.7 Mode réseau

Le mode réseau définit le rôle et les fonctions du routeur selon vos besoins de déploiement.

Connectez-vous à l'interface d'administration Web du routeur et ouvrez **RÉSEAU (NETWORK)** > **Mode réseau (Network Mode)**. Vous pouvez y modifier le mode réseau du routeur.



- **Routeur (Router)** : mode par défaut de la plupart des routeurs domestiques et de petite entreprise. Il crée un réseau local privé et sert de passerelle entre Internet et les appareils connectés. Il active le NAT, le DHCP et le pare-feu intégré. Relié à une connexion en amont, comme la fibre, il attribue automatiquement des IP privées aux appareils et protège l'ensemble du réseau privé.

- **Point d’accès (Access Point)** : relie le routeur à un réseau filaire par câble LAN et diffuse un signal Wi-Fi pour étendre la couverture et connecter davantage d’appareils. Le NAT et le DHCP sont désactivés : le routeur fonctionne comme un point d’accès sans fil et un commutateur, sans servir de passerelle autonome.
- **Extenseur (Extender)** : étend la couverture d’un réseau Wi-Fi existant et réduit les zones sans signal. Le routeur reçoit les signaux du routeur principal sans fil, puis les retransmet. Aucune liaison filaire n’est nécessaire, contrairement au mode Point d’accès. La bande passante peut toutefois être divisée par deux, car l’appareil doit recevoir et transmettre simultanément.
- **WDS** : le mode Wireless Distribution System étend la couverture Wi-Fi sans fil, comme le mode Extenseur, mais permet aussi de créer des ponts sans fil entre plusieurs routeurs compatibles. Il est recommandé lorsque le routeur en amont prend en charge WDS.
  Ce mode convient aux bâtiments à plusieurs étages ou aux petits sites de bureaux où plusieurs routeurs doivent former un réseau Wi-Fi commun. Contrairement au mode Extenseur, qui relie un routeur principal à un seul extenseur, WDS permet à plusieurs routeurs interconnectés d’émettre et de recevoir les signaux pour assurer une couverture continue sur une zone plus vaste.

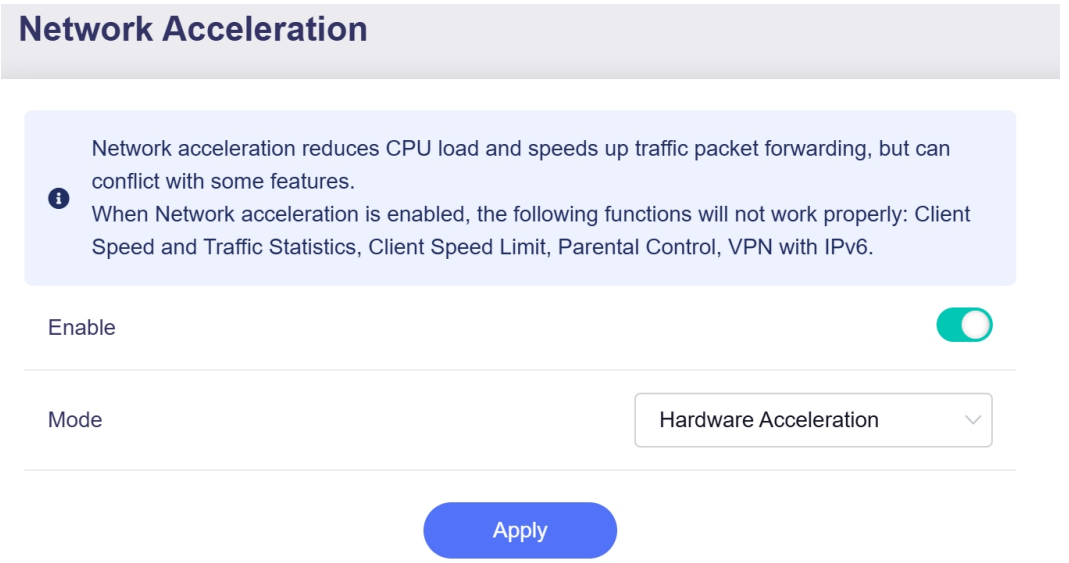
Remarque :

1. Après un changement de mode réseau, tous les appareils clients doivent se reconnecter au routeur pour assurer une connexion stable.
2. **En mode Point d’accès ou WDS, l’adresse IP d’origine ne permet plus d’accéder à l’interface d’administration Web**. Connectez-vous au routeur en amont pour trouver l’adresse IP qu’il a attribuée à ce routeur, puis utilisez cette adresse pour accéder à l’interface d’administration Web. Si vous n’avez pas accès au routeur en amont, maintenez le bouton de réinitialisation enfoncé pendant 4 secondes pour revenir au mode Routeur par défaut.
3. **En mode Point d’accès, Extendeur ou WDS, les fonctions suivantes ne sont pas disponibles** : contrôle d’accès (listes d’autorisation et de blocage), GoodPAS, VPN, AdGuard Home, contrôle parental, ZeroTier, Tailscale, redirection de ports, Multi-WAN, serveur DHCP, réservation d’adresses, réseau invité, DNS, port Ethernet, IPv6, passerelle transparente, IGMP Snooping, accélération réseau et paramètres NAT.

12.8 Accélération réseau

L'accélération réseau réduit la charge du processeur et accélère le transfert des paquets, mais peut entrer en conflit avec certaines fonctions.

Connectez-vous à l'interface d'administration Web du routeur et ouvrez **RÉSEAU (NETWORK)** > **Accélération réseau (Network Acceleration)**. Cette page permet d'activer l'accélération réseau et de choisir entre accélération matérielle et accélération logicielle.



- **Accélération matérielle (Hardware Acceleration)** : confie les tâches réseau fréquentes, comme le NAT, le transfert de paquets et la vérification des sommes de contrôle, à du matériel dédié, tel qu'un NPU ou une puce HWNAT. Elle fonctionne sur les connexions Ethernet et Répéteur. Avec leurs chemins fixes et leurs règles simples, elle assure un débit élevé, une faible latence et une charge minimale du processeur, pour transmettre les données au débit maximal de la liaison.
- **Accélération logicielle (Software Acceleration)** : utilise le processeur principal du routeur avec un noyau ou des pilotes optimisés, comme SWNAT. Elle fonctionne sur les connexions cellulaires 4G/5G, où l'accélération matérielle est généralement indisponible, et offre une bonne compatibilité avec les protocoles complexes. Malgré sa souplesse, elle peut atteindre les limites du processeur lorsque le débit est élevé, notamment avec des fonctions avancées.

Remarque : lorsque l’accélération réseau est activée, les fonctions suivantes ne fonctionnent pas correctement : statistiques de débit des clients, statistiques de trafic, limitation du débit, contrôle parental et VPN avec IPv6.

Chapitre 13

Contrôle des flux

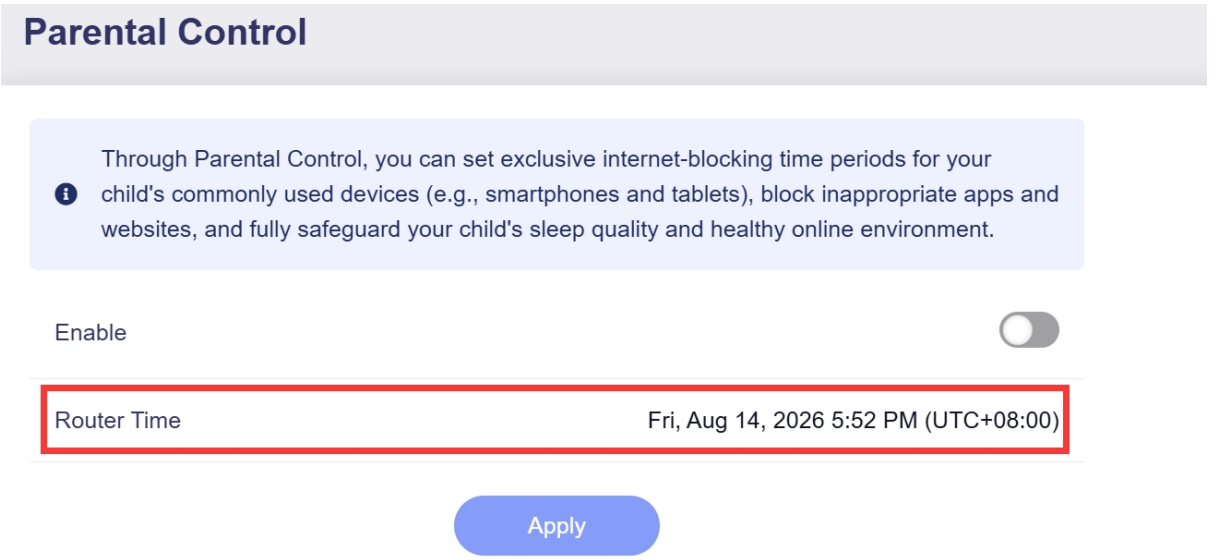
Ce chapitre présente le contrôle parental, qui permet de filtrer les sites Web et de limiter l’utilisation des appareils.

13.1 Contrôle parental

Le contrôle parental protège les enfants en bloquant les sites inadaptés et en limitant le temps d'utilisation des appareils. Il réduit l'accès aux contenus nuisibles, aide à gérer le temps d'écran et encourage un usage responsable d'Internet.

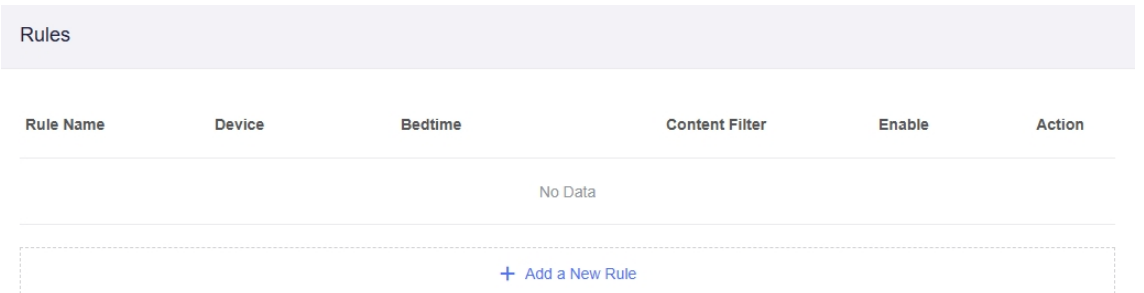
Suivez les étapes ci-dessous pour configurer le contrôle parental.

1. Connectez-vous à l'interface d'administration Web du routeur et ouvrez **CONTRÔLE DES FLUX (FLOW CONTROL)** > **Contrôle parental (Parental Control)**. Vérifiez que l'heure du routeur est correcte.

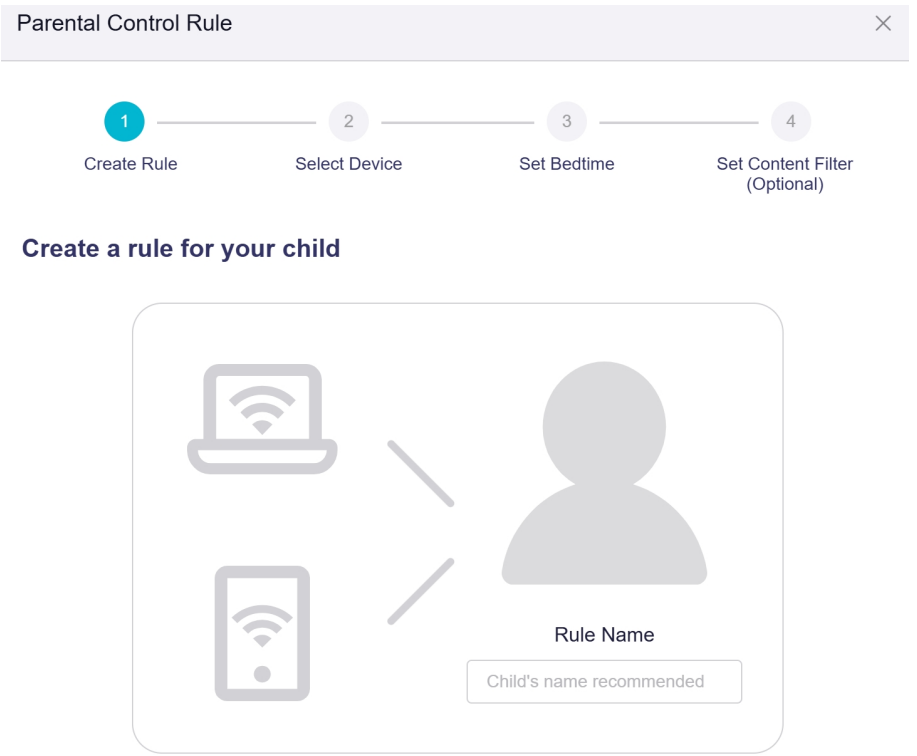


Sinon, ouvrez **SYSTÈME (SYSTEM)** > **Fuseau horaire (Time Zone)** pour la synchroniser.

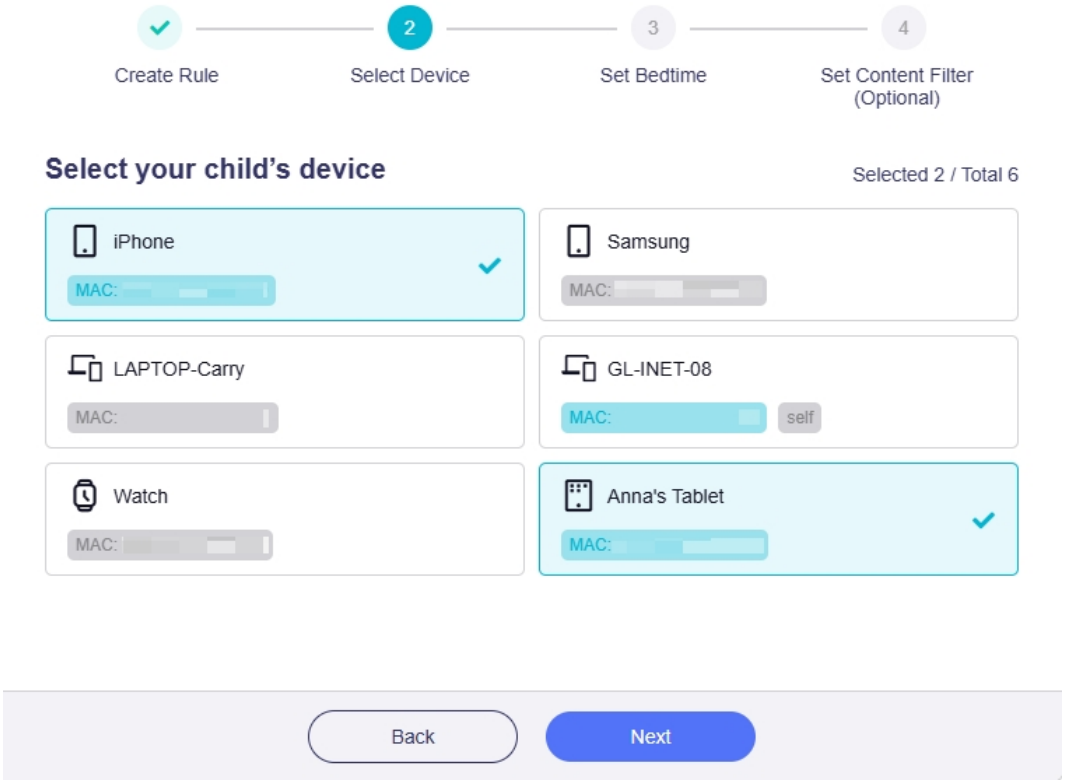
2. Activez le contrôle parental et cliquez sur **Appliquer (Apply)**.
3. La liste des règles s'affiche comme ci-dessous. Cliquez sur **Ajouter une règle (Add a New Rule)**.



4. Dans la fenêtre qui s’ouvre, créez une règle et donnez-lui un nom, puis cliquez sur **Suivant (Next)**.

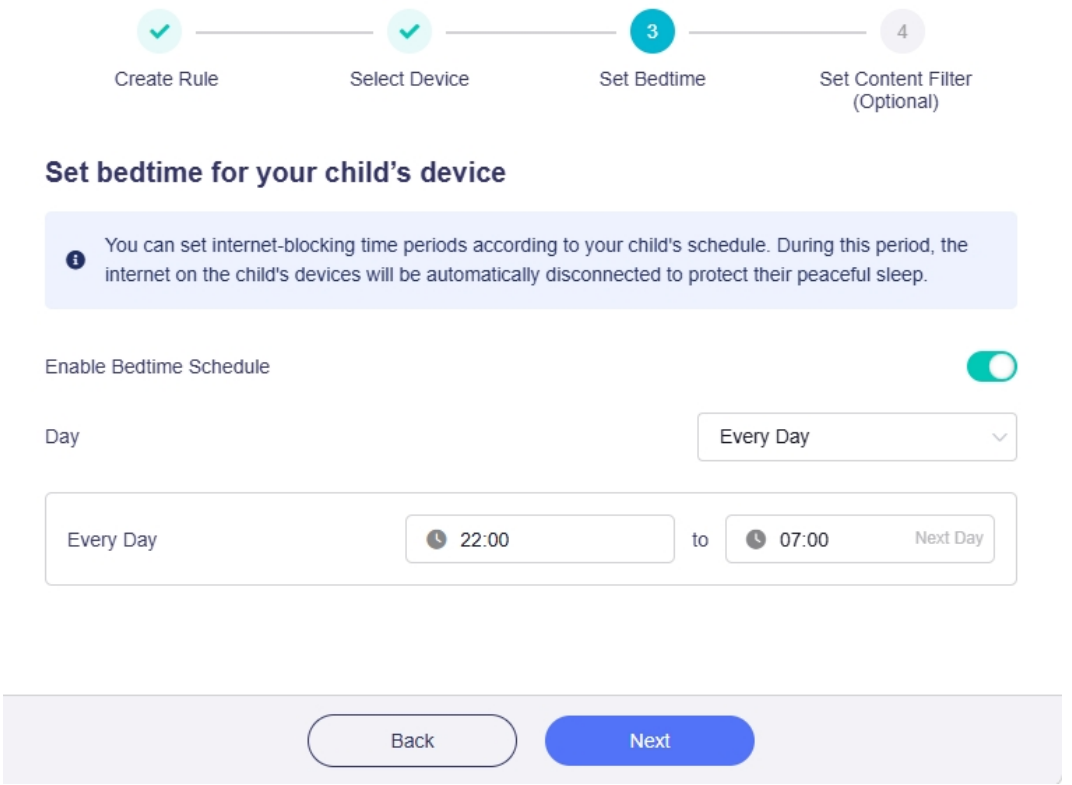


5. Sélectionnez l’appareil de votre enfant, puis cliquez sur **Suivant (Next)**.
   Seuls les appareils connectés au routeur par Wi-Fi ou Ethernet apparaissent sur cette page. Le cyan indique qu’un appareil est en ligne ; le gris indique qu’il est hors ligne.



Conseil : pour identifier plus facilement les appareils connectés, ouvrez la page **CLIENTS** et personnalisez leur nom.

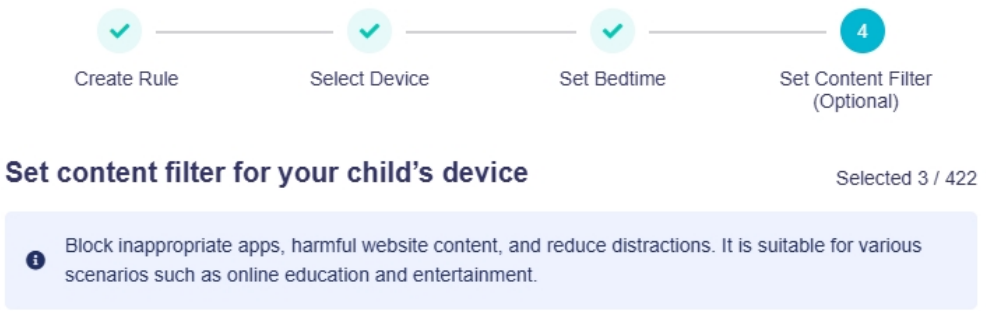
6. Définissez les horaires de coucher pour l'appareil de votre enfant, puis cliquez sur **Suivant (Next)**. Les appareils sélectionnés ne pourront pas accéder à Internet pendant cette période. Par défaut, les horaires sont identiques chaque jour.

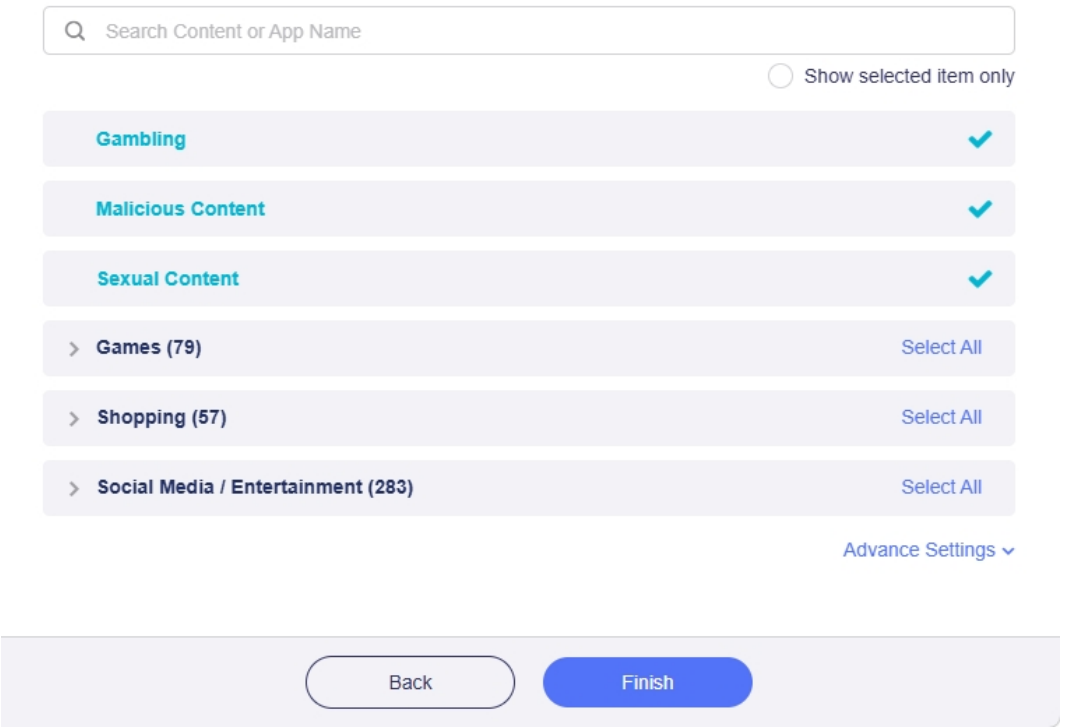


Pour définir des horaires différents selon le jour de la semaine, sélectionnez **Personnaliser les jours (Customize Days)**, configurez les horaires, puis cliquez sur **Suivant (Next)**.

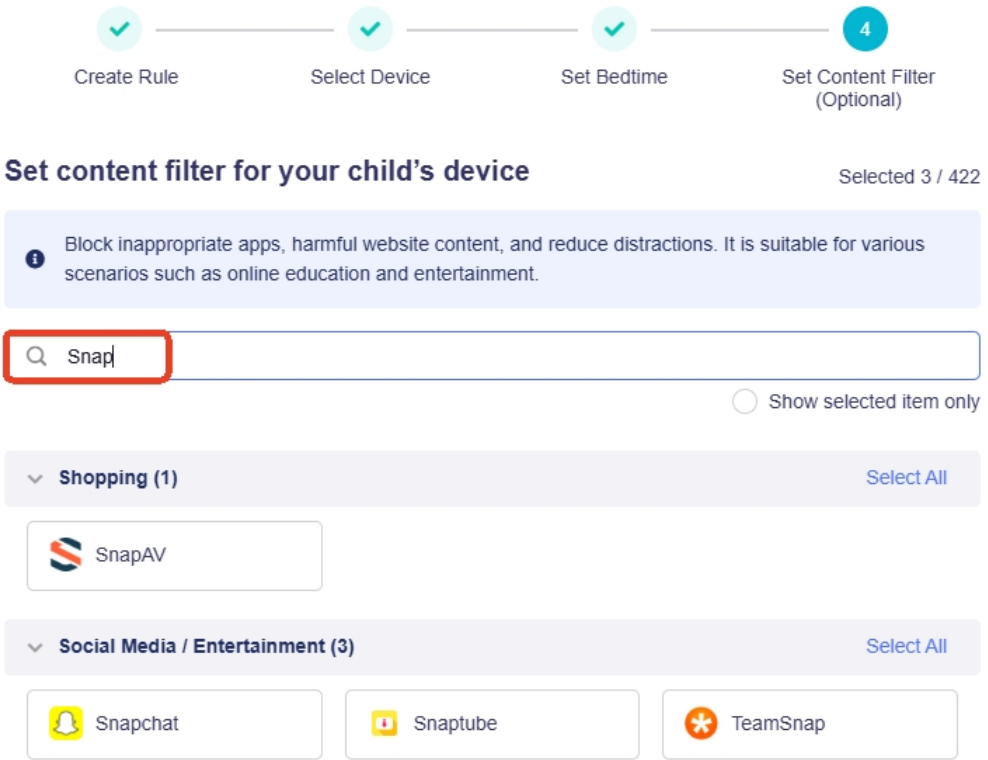
7. Sélectionnez les filtres de contenu.

   Trois catégories sont sélectionnées par défaut : **Jeux d'argent (Gambling)**, **Contenu malveillant (Malicious Content)** et **Contenu sexuel (Sexual Content)**. Vous pouvez sélectionner d'autres catégories selon vos besoins, comme **Jeux (Games)**, **Achats (Shopping)**, **Réseaux sociaux (Social Media)** ou **Divertissement (Entertainment)**.

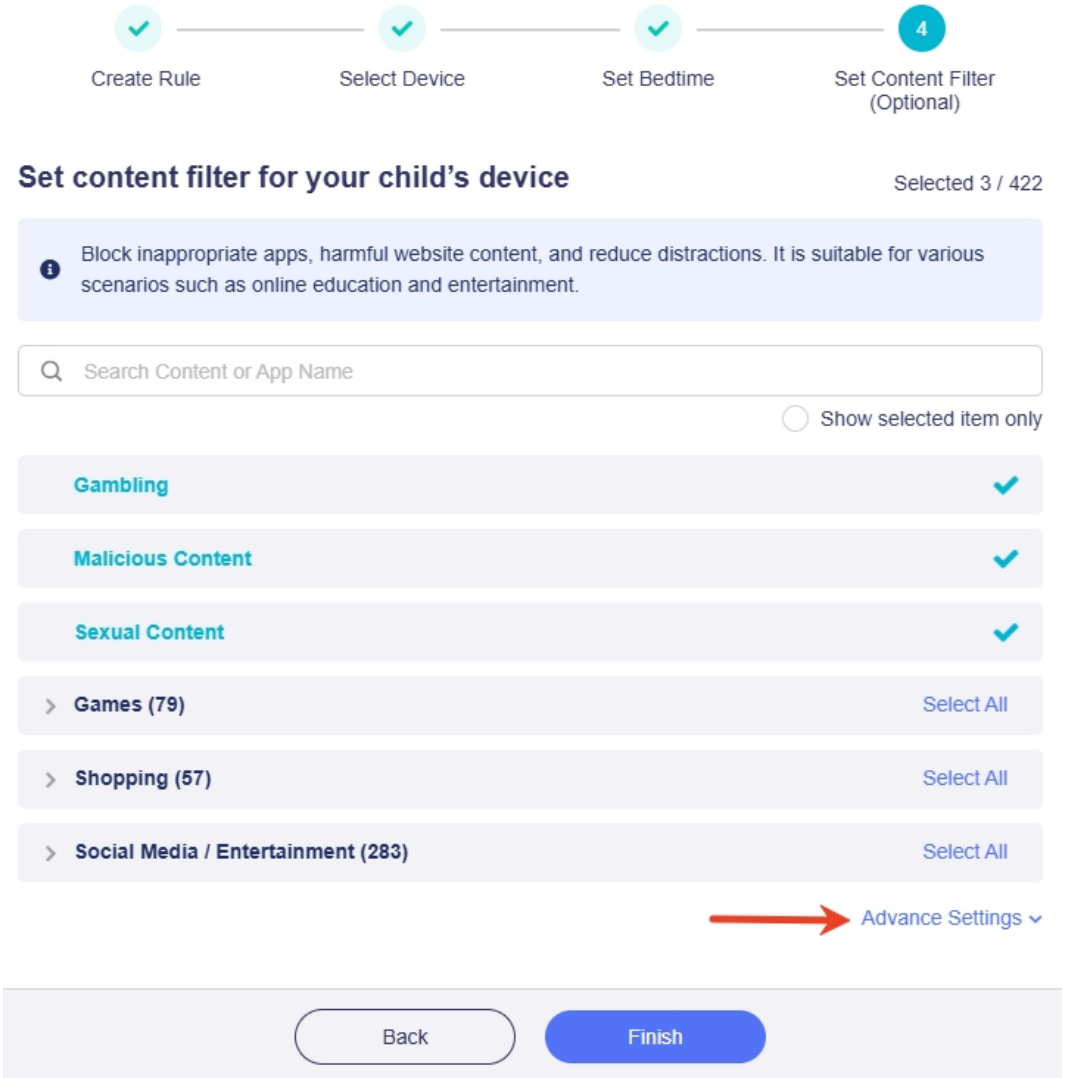




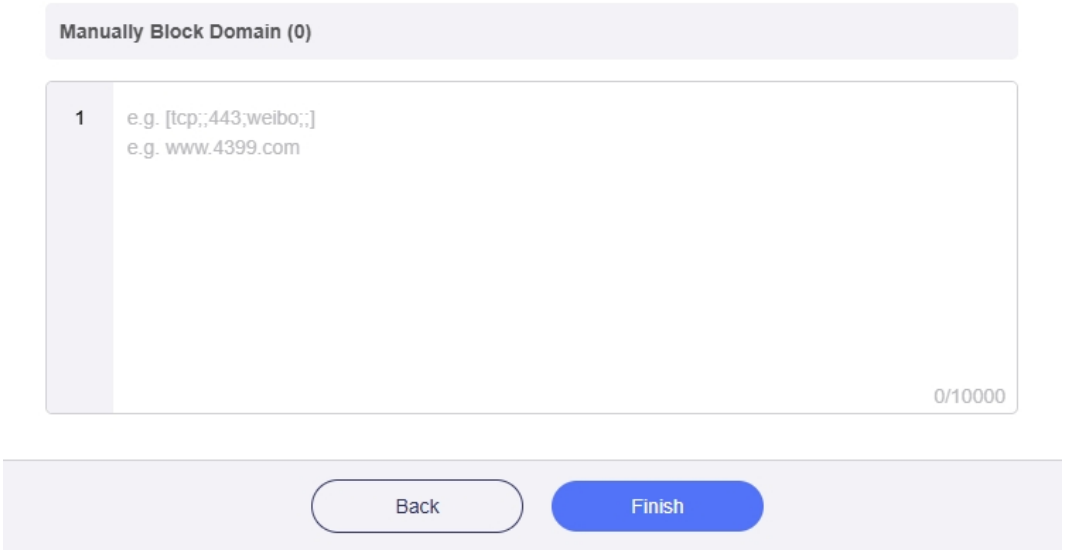
Si vous ne trouvez pas l'application à bloquer, utilisez le champ de recherche en haut de la page.



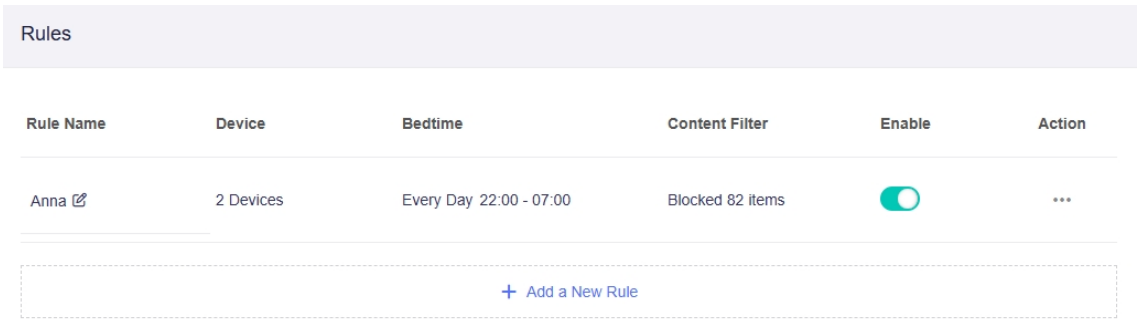
8. Pour bloquer certains domaines, cliquez sur **Paramètres avancés (Advanced Settings)** en bas à droite.



Saisissez les domaines manuellement, puis cliquez sur **Terminer (Finish)**.



9. La règle est ajoutée. La liste indique son nom, le nombre d’appareils associés, les horaires de coucher, les contenus filtrés et son état (activée ou désactivée).



Chapitre 14

Sécurité

Ce chapitre présente la gestion de la sécurité du réseau, notamment la redirection de port, les paramètres d’accès administrateur et le mode NAT.

14.1 Redirection de port

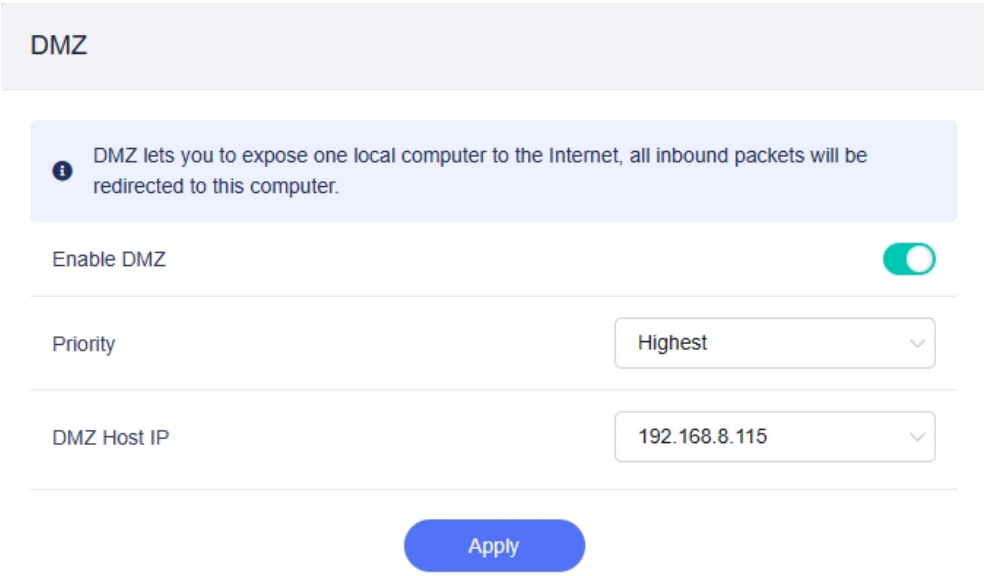
La redirection de port achemine les requêtes externes vers des appareils précis du réseau local. Cette page propose deux fonctions : **DMZ**, pour un accès direct complet à un appareil, et **Redirection de port (Port Forwarding)**, pour un accès ciblé à certains ports.

14.1.1 DMZ

La DMZ expose un ordinateur à Internet en lui redirigeant tous les paquets entrants.

Pour activer la DMZ, procédez comme suit.

1. Dans l'interface d'administration Web, ouvrez **SÉCURITÉ (SECURITY)** > **Redirection de port (Port Forwarding)** > section **DMZ**.
2. Activez **Activer la DMZ (Enable DMZ)**. Sélectionnez la priorité et l'IP de l'hôte DMZ dans les listes, puis cliquez sur **Appliquer (Apply)**.



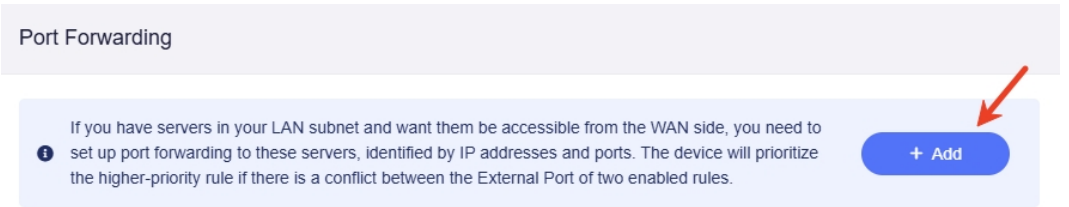
- **Priorité (Priority)** : choisissez La plus élevée ou La plus faible. Si la DMZ est prioritaire sur les règles de redirection de port, celles-ci deviennent inopérantes. Sinon, les requêtes ne sont transmises au client DMZ que si aucune règle ne correspond au port demandé.
- **IP de l'hôte DMZ (DMZ Host IP)** : sélectionnez l'adresse IP interne de l'appareil qui recevra tous les paquets entrants.

14.1.2 Redirection de port

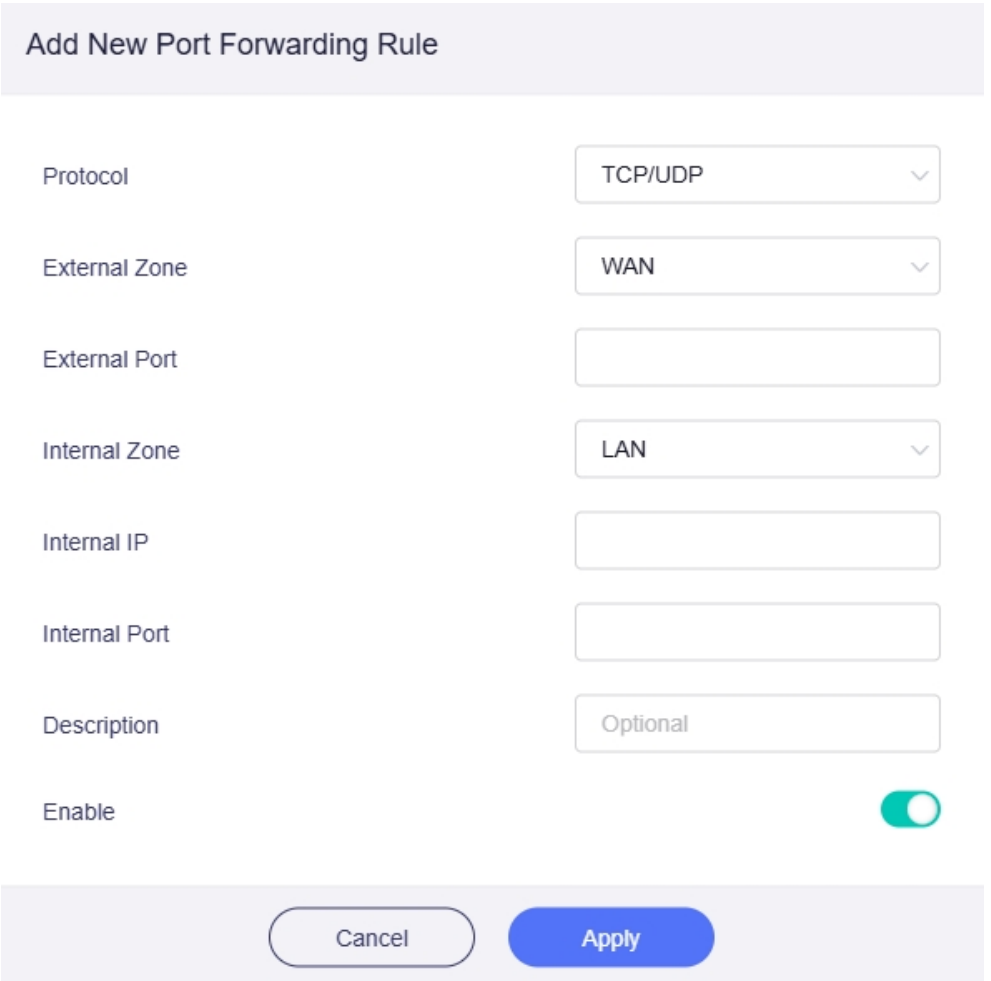
La redirection de port permet à des ordinateurs distants de se connecter à un ordinateur ou serveur local situé derrière le pare-feu LAN, comme un serveur Web ou FTP.

Pour configurer une redirection de port, procédez comme suit.

1. Dans l'interface d'administration Web, ouvrez **SÉCURITÉ (SECURITY)** > **Redirection de port (Port Forwarding)** > **section Redirection de port (Port Forwarding)**, puis cliquez sur **Ajouter (Add)**.



2. Dans la fenêtre qui s'affiche, saisissez ou sélectionnez les paramètres nécessaires, puis cliquez sur **Appliquer (Apply)** pour ajouter la règle.



- **Protocole (Protocol)** : choisissez TCP, UDP ou TCP et UDP.
- **Zone externe (External Zone)** : options disponibles : WAN, client WireGuard, serveur WireGuard, client OpenVPN, serveur OpenVPN et LAN.
- **Port externe (External Port)** : numéro de port externe compris entre 1 et 65535. Définissez un port ou une plage en séparant le premier et le dernier numéro par un tiret, par exemple 501-510.
- **Zone interne (Internal Zone)** : options disponibles : LAN, client WireGuard, serveur WireGuard, client OpenVPN, serveur OpenVPN et WAN.
- **IP interne (Internal IP)** : adresse IP attribuée par le routeur à l'appareil nécessitant un accès distant. Si vous avez défini un port unique dans Port externe, définissez-en un ici. Si vous avez défini une plage dans Port externe, renseignez la plage correspondante ici.
- **Port interne (Internal Port)** : numéro de port interne de l'appareil. Saisissez un port précis. Laissez ce champ vide s'il est identique au port externe.

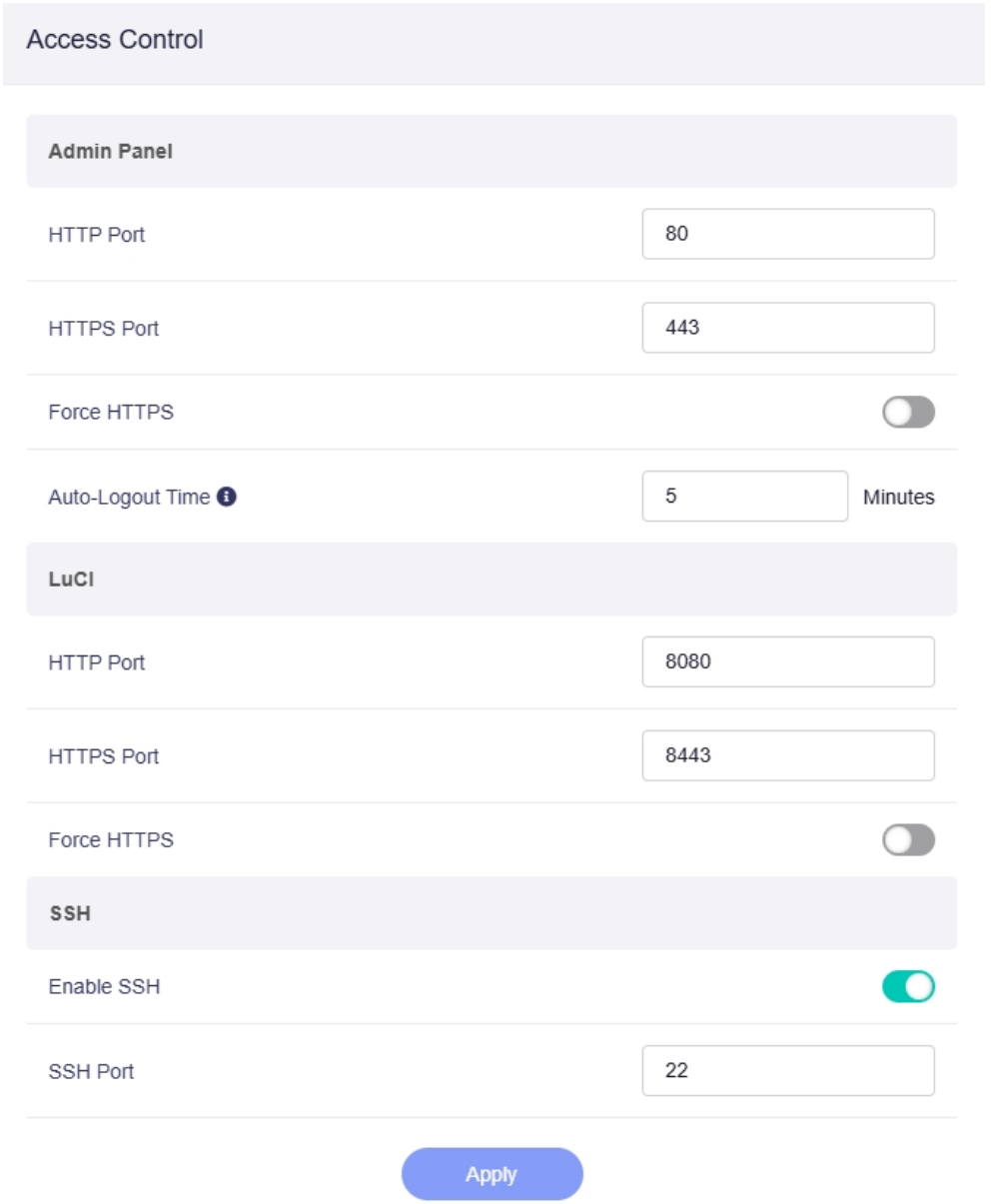
- **Description** : nom ou description de la règle, facultatif.
- **Activer (Enable)** : active ou désactive la règle.

14.2 Accès administrateur

Connectez-vous à l'interface d'administration Web du routeur et ouvrez **SÉCURITÉ (SECURITY)** > **Accès administrateur (Admin Access)**. Cette page permet de configurer l'accès local et l'accès distant HTTPS/SSH au routeur, et de gérer ses ports ouverts afin de protéger le routeur et le réseau contre les accès non autorisés.

14.2.1 Contrôle d'accès

Cette section gère l'accès à l'interface d'administration, à LuCI et à SSH. Elle permet de limiter les tentatives d'analyse et d'intrusion sur les ports par défaut et d'éviter les problèmes liés aux conflits de ports.



Interface d’administration

- **Port HTTP (HTTP Port)** : 80 par défaut, pour l’accès HTTP non chiffré à l’interface Web.
- **Port HTTPS (HTTPS Port)** : 443 par défaut, pour l’accès HTTPS sécurisé à l’interface Web.
- **Forcer HTTPS (Force HTTPS)** : impose une connexion HTTPS sécurisée pour accéder à l’interface Web.
- **Délai de déconnexion automatique (Auto-Logout Time)** : 5 minutes par défaut. Une session d’administration inactive est déconnectée après ce délai pour renforcer la sécurité. Vous pouvez le régler entre 1 minute et 3 heures.

LuCI

Installez d'abord LuCI dans les Paramètres avancés (Advanced Settings) avant de configurer son contrôle d'accès.

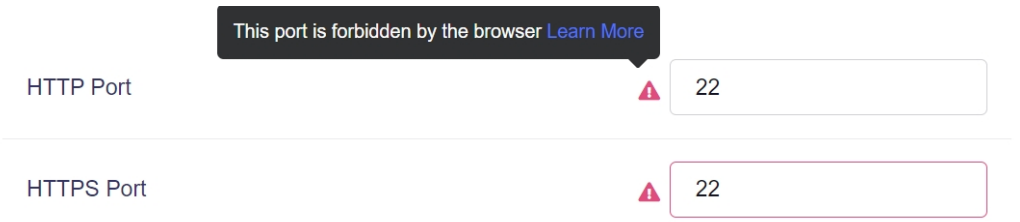
- **Port HTTP (HTTP Port)** : 8080 par défaut, pour l'accès HTTP non chiffré à LuCI.
- **Port HTTPS (HTTPS Port)** : 8443 par défaut, pour l'accès HTTPS sécurisé à LuCI.
- **Forcer HTTPS (Force HTTPS)** : impose une connexion HTTPS sécurisée pour accéder à LuCI.

SSH

- **Activer SSH (Enable SSH)** : activé par défaut, autorise ou interdit l'accès SSH au routeur.
- **Port SSH (SSH Port)** : 22 par défaut, utilisé pour l'accès SSH au routeur.

Remarque :

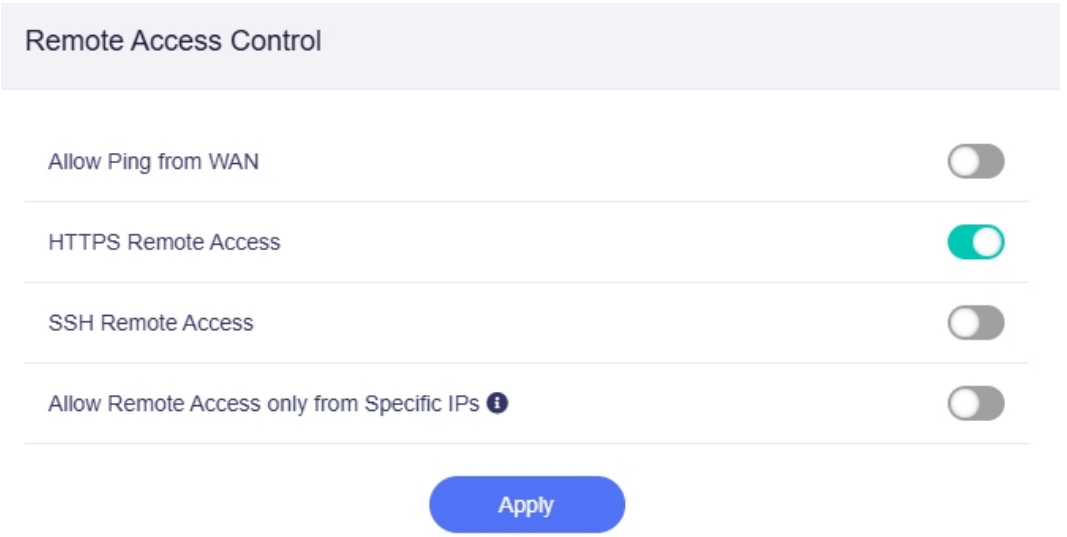
1. Si le port choisi entre en conflit avec un port réservé, notamment par les navigateurs ou les conventions réseau, le message « Ce port est interdit par le navigateur » (This port is forbidden by the browser) s'affiche.



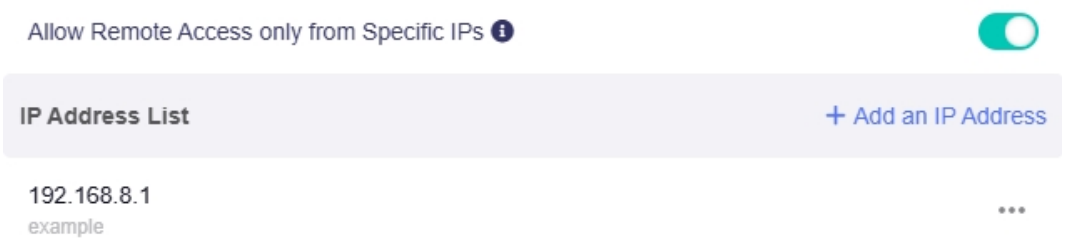
2. Si vous modifiez un port dans le micrologiciel, renseignez le nouveau numéro pour accéder à l'interface d'administration. Si vous l'avez oublié, réinitialisez le routeur pour rétablir le port par défaut.

14.2.2 Contrôle d’accès distant

Cette section gère les accès distants HTTPS et SSH et les requêtes ping depuis le WAN. Elle permet aussi de restreindre l’accès à certaines adresses IP pour concilier administration à distance et sécurité.

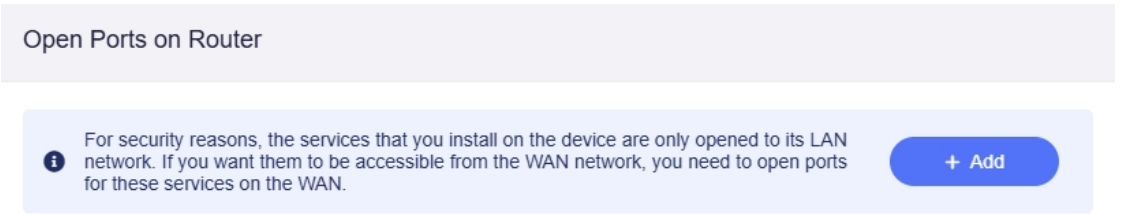


- **Autoriser le ping depuis le WAN (Allow Ping from WAN)** : permet de vérifier que le routeur est joignable depuis le WAN en cas de problème et de mesurer la latence et les pertes de paquets.
- **Accès HTTPS à distance (HTTPS Remote Access)** : permet d’accéder de manière sécurisée à l’interface Web du routeur via HTTPS. Les données échangées lors de l’administration à distance depuis un navigateur sont chiffrées.
- **Accès SSH à distance (SSH Remote Access)** : permet d’accéder au terminal et de gérer le routeur à distance par SSH, dans un tunnel chiffré.
- **Autoriser l’accès distant depuis certaines IP (Allow Remote Access from Specific IPs)** : disponible uniquement si l’une des trois fonctions précédentes est activée. Ajoutez les adresses IP autorisées pour limiter l’administration distante aux appareils qui les utilisent.

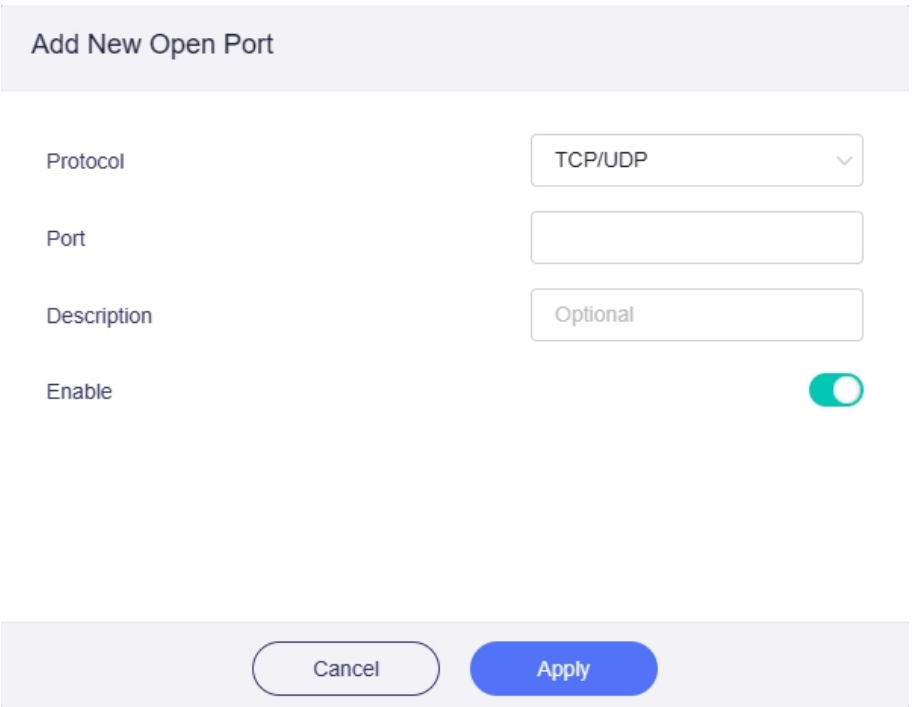


14.2.3 Ouverture de ports sur le routeur

Cette section gère l'accès aux services hébergés sur le routeur. Les services Web et FTP, par exemple, nécessitent l'ouverture de leurs ports pour être accessibles depuis le WAN. Par sécurité, les services installés ne sont accessibles que depuis le LAN par défaut. Ouvrez ici les ports nécessaires pour autoriser l'accès WAN.



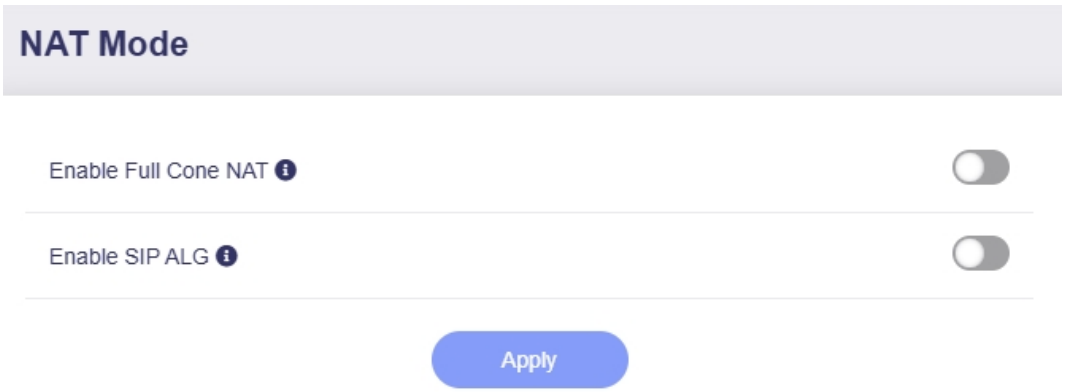
Pour ouvrir un port, cliquez sur **Ajouter (Add)**, puis renseignez les informations demandées dans la fenêtre.



- **Protocole (Protocol)** : choisissez TCP, UDP ou TCP/UDP. Ce choix détermine la transmission des données du service associé au port.
- **Port** : saisissez le numéro du port à ouvrir.
- **Description** (facultative) : ajoutez une brève description, comme « Serveur Web » ou « Service FTP », pour faciliter la gestion.
- **Activer (Enable)** : active ou désactive la règle de redirection.

14.3 Mode NAT

Dans l'interface d'administration Web, ouvrez **SÉCURITÉ (SECURITY)** > **Mode NAT (NAT Mode)**. Deux fonctions sont proposées : Full Cone NAT et SIP ALG.



- **Full Cone NAT** : peut réduire la latence et améliorer la réactivité des jeux en ligne. Son activation peut toutefois diminuer la sécurité, car elle autorise les connexions entrantes sans restriction.
- **SIP ALG** : vise à limiter les effets de plusieurs NAT sur le trafic SIP (Session Initiation Protocol). Dans la plupart des cas, cette fonction n'apporte pas d'amélioration et peut perturber les appels VoIP : son dans un seul sens, absence de sonnerie, coupures inattendues ou renvoi direct vers la messagerie vocale.

Chapitre 15

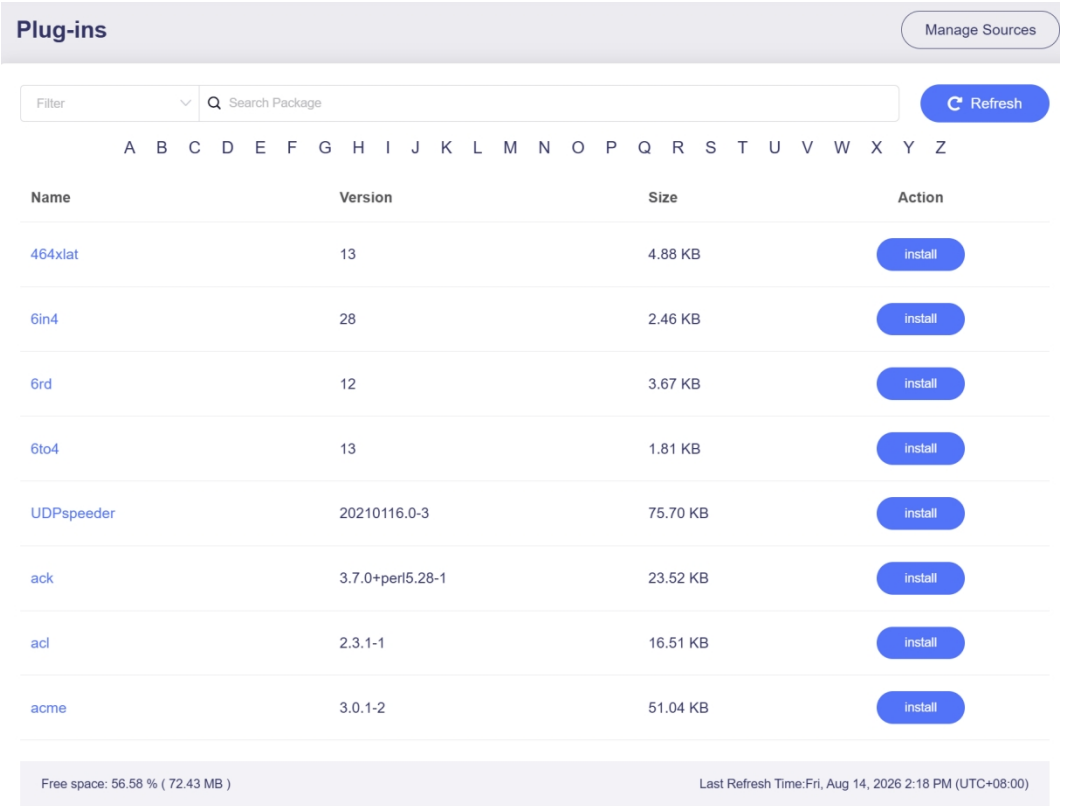
Applications

Ce chapitre présente certaines applications des routeurs GL.iNet, notamment les modules complémentaires, le DNS dynamique, le stockage réseau et Tailscale.

15.1 Extensions

La page Extensions permet de gérer les paquets OpenWrt.

Connectez-vous à l'interface d'administration Web du routeur et ouvrez **APPLICATIONS** > **Modules complémentaires (Plug-ins).** Vous pouvez installer ou supprimer tout paquet disponible dans le dépôt. Cliquez sur **Actualiser (Refresh)** pour mettre à jour la liste des paquets avant d'installer des modules complémentaires.



Remarque :

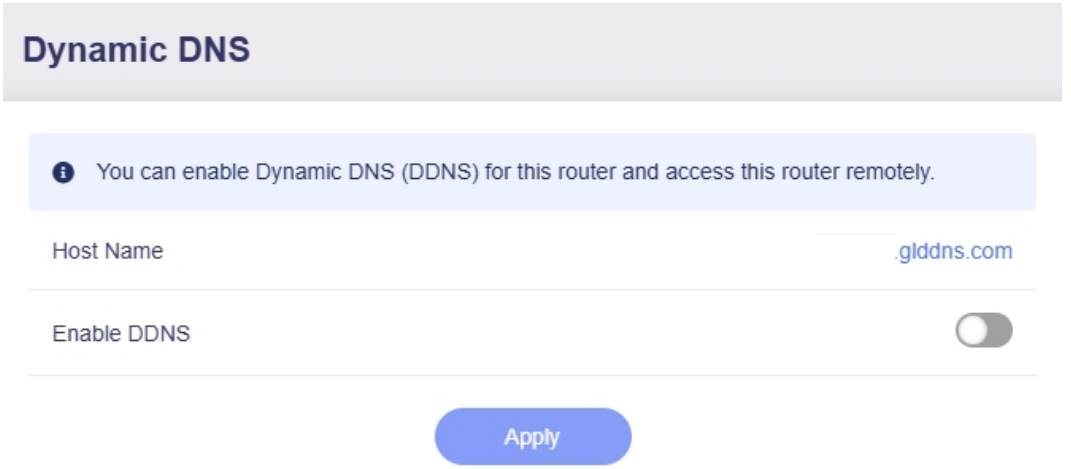
1. Il est déconseillé de mettre à jour les extensions préinstallées dans le micrologiciel officiel GL.iNet, comme nginx, AdGuard Home ou Tailscale.
2. Les extensions tierces installées manuellement peuvent être mises à jour. GL.iNet n'est toutefois pas responsable des problèmes de sécurité qu'elles peuvent entraîner. Pour toute question, contactez leurs auteurs.

15.2 DNS dynamique

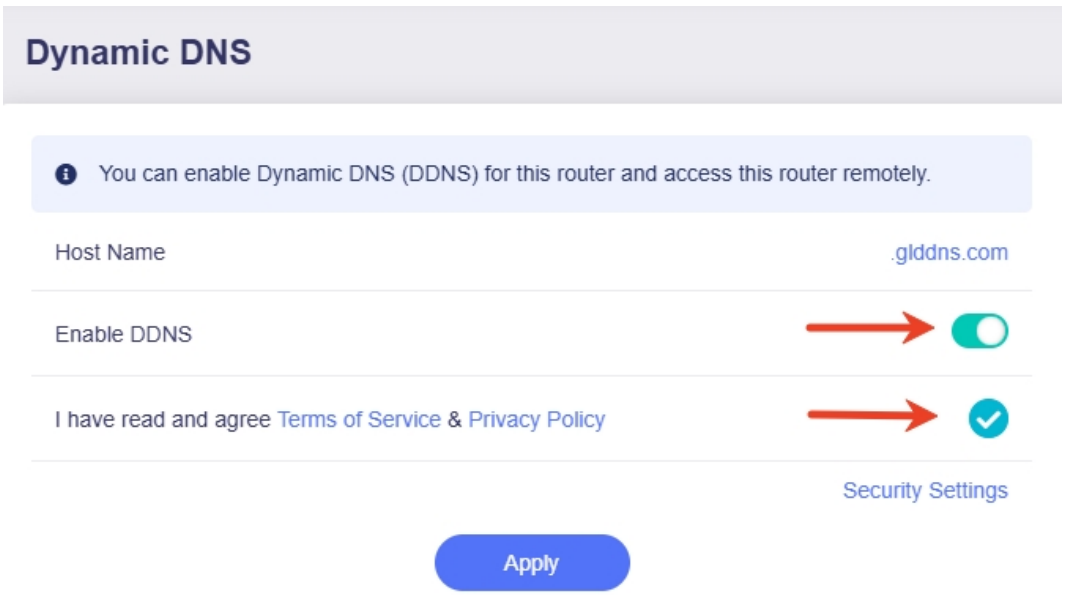
Le DNS dynamique (DDNS) associe un nom de domaine à l'adresse IP dynamique d'un appareil réseau. Il permet d'accéder au routeur à distance. Cette fonction nécessite une adresse IP publique.

15.2.1 Activation du DDNS

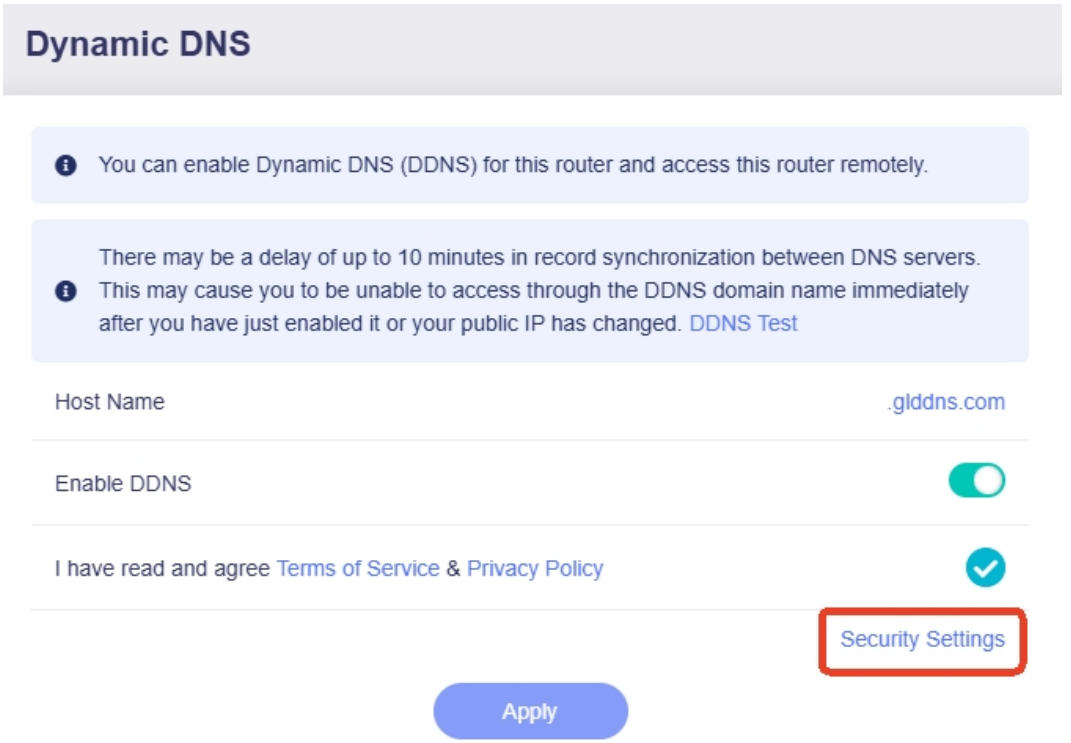
1. Connectez-vous à l'interface d'administration Web du routeur et ouvrez **APPLICATIONS** > **DNS dynamique (Dynamic DNS)**. La page ci-dessous s'affiche.



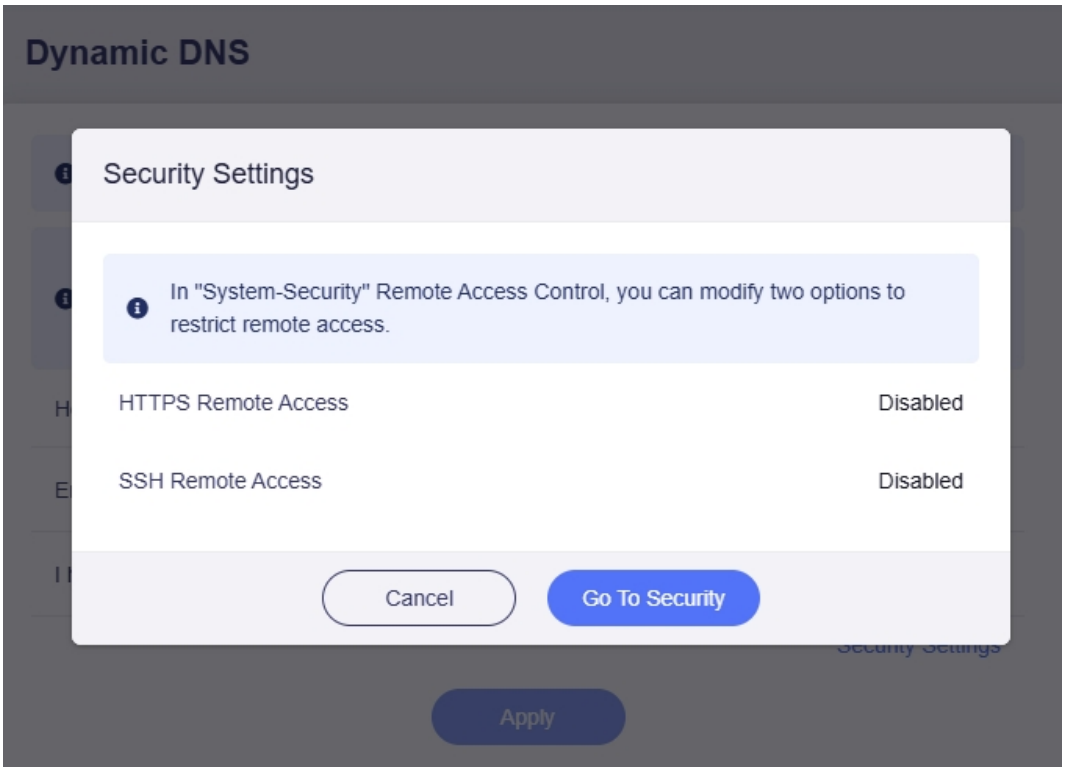
2. Activez **Activer le DDNS (Enable DDNS)**, lisez et acceptez les **Conditions d'utilisation et la Politique de confidentialité (Terms of Services & Privacy Policy)**, puis cliquez sur **Appliquer (Apply)**.



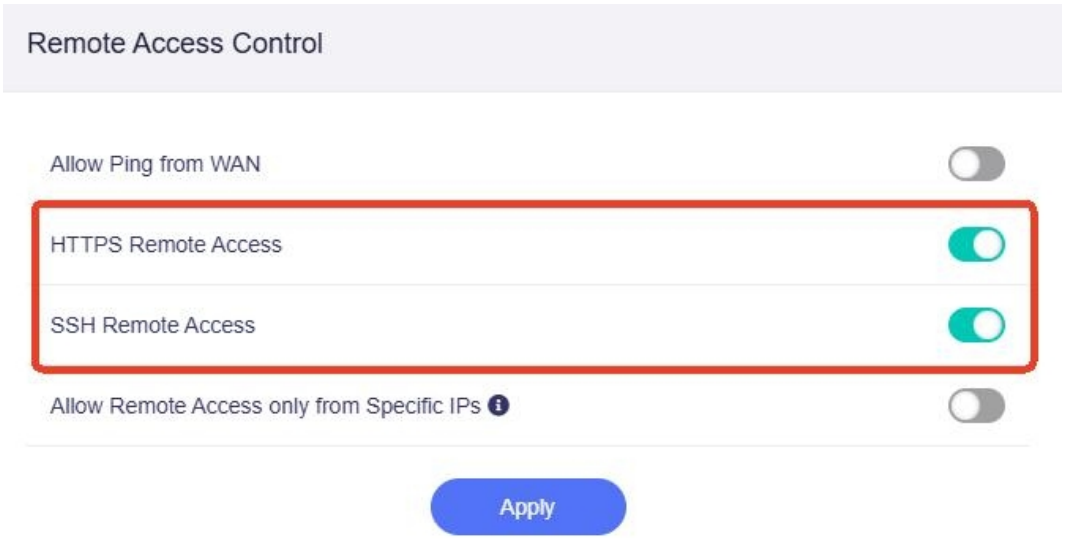
3. Cliquez sur **Paramètres de sécurité (Security Settings)** dans l'angle inférieur droit.



4. Dans la fenêtre qui s'affiche, vérifiez que l'accès distant souhaité est activé.



Sinon, ouvrez **SÉCURITÉ (SECURITY)** > **Accès administrateur (Admin Access)** > **Contrôle d'accès distant (Remote Access Control)** pour l'activer, puis cliquez sur **Appliquer (Apply)**.



Remarque :

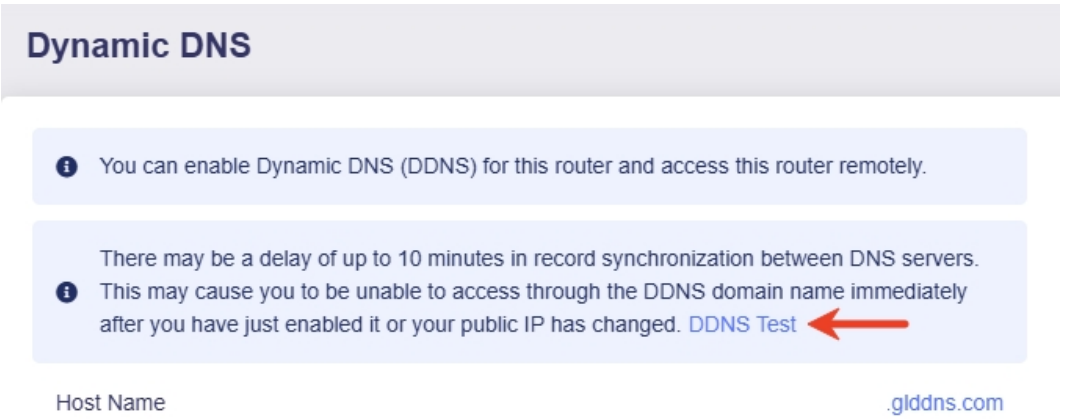
1. La synchronisation des enregistrements entre serveurs DNS peut prendre jusqu'à 10 minutes. L'accès par le domaine DDNS peut donc être indisponible immédiatement après son activation ou après un changement d'IP publique.
2. Si vous activez simultanément le DDNS et un client VPN, vérifiez que Services GL.iNet via le VPN (Services From GL.iNet Use VPN) est désactivé.

15.2.2 Vérification du fonctionnement du DDNS

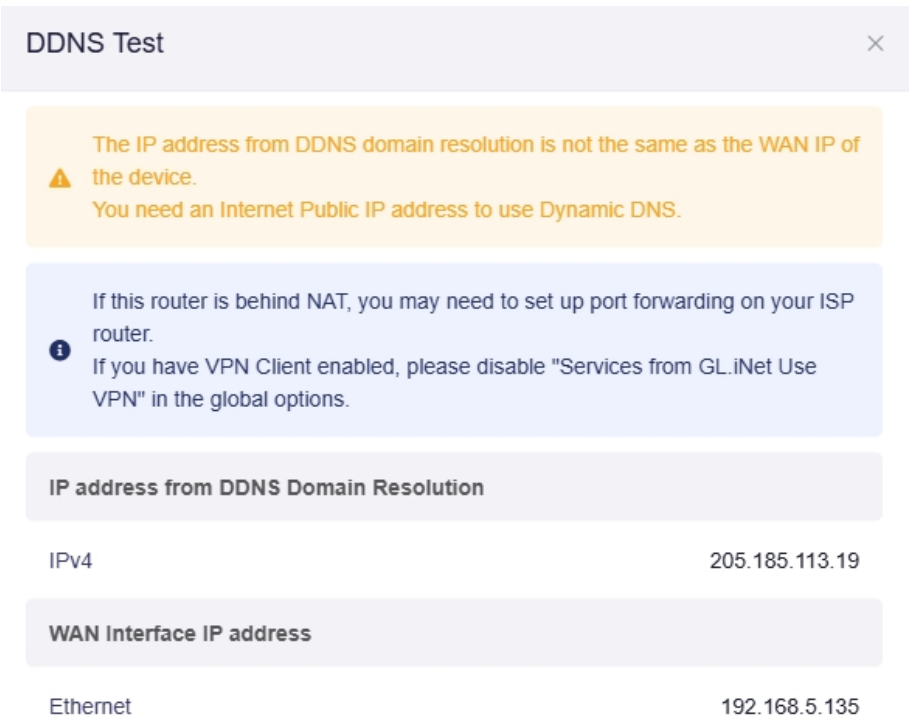
Vérifiez le DDNS avec l'outil de test intégré ou manuellement à l'aide de commandes.

Méthode 1 : outil de test DDNS

1. Sur la page DNS dynamique, cliquez sur **Test DDNS (DDNS Test)**.



2. Vérifiez que l'IP obtenue par résolution du domaine DDNS correspond à l'IP WAN du routeur. Sinon, un message jaune indique que le routeur peut se trouver derrière un NAT et qu'une redirection de port est nécessaire sur le routeur en amont.



Méthode 2 : commandes

1. Utilisez nslookup avec la commande *nslookup xxxxxxx.glddns.com 8.8.8.8* pour afficher l'adresse IP associée au domaine. L'exemple ci-dessous utilise Beryl AX (GL-MT3000).



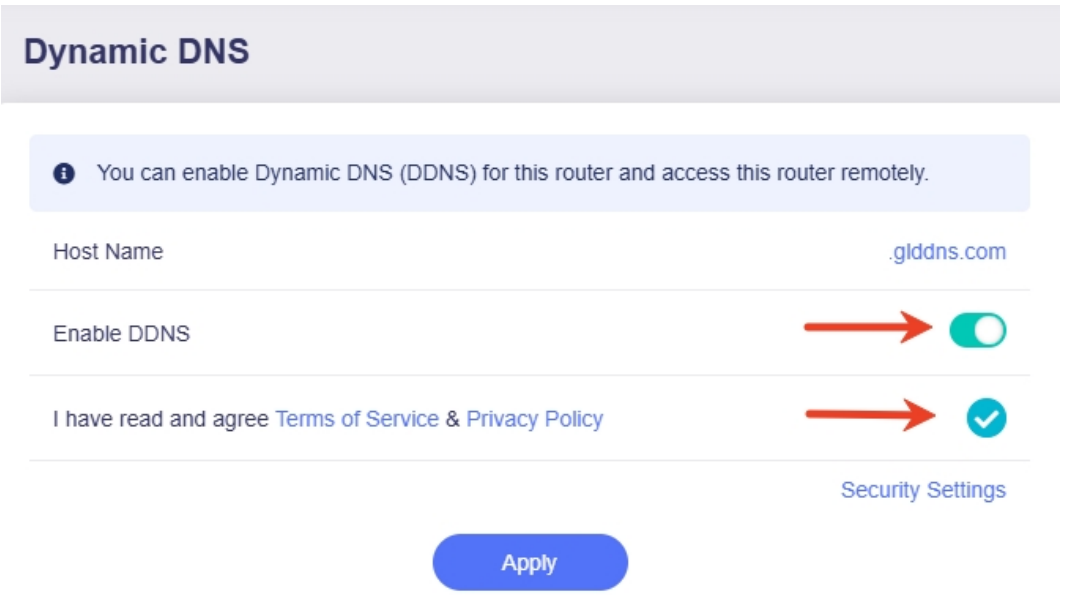
   - Remplacez « xxxxxxx.glddns.com » par votre nom d'hôte.
   - « 8.8.8.8 » est le DNS de Google. Utilisez-le ou indiquez un autre serveur, puis appuyez sur Entrée.
2. Une IP publique, comme « 183.178.10.100 » dans l'image, indique que le domaine DDNS est bien associé à une adresse publique. Un message comme « server can't find xxxxxxx.glddns.com » peut indiquer un échec de résolution. Passez à l'étape suivante pour vérifier.
3. Connectez-vous à l'interface d'administration Web du routeur et ouvrez **INTERNET**. Recherchez l'adresse IP WAN du routeur dans l'interface actuellement active. Comparez-la à l'adresse IP publique obtenue précédemment. Si elles sont identiques, le DDNS fonctionne ; sinon, il ne fonctionne pas.

15.2.3 Accès HTTPS à distance

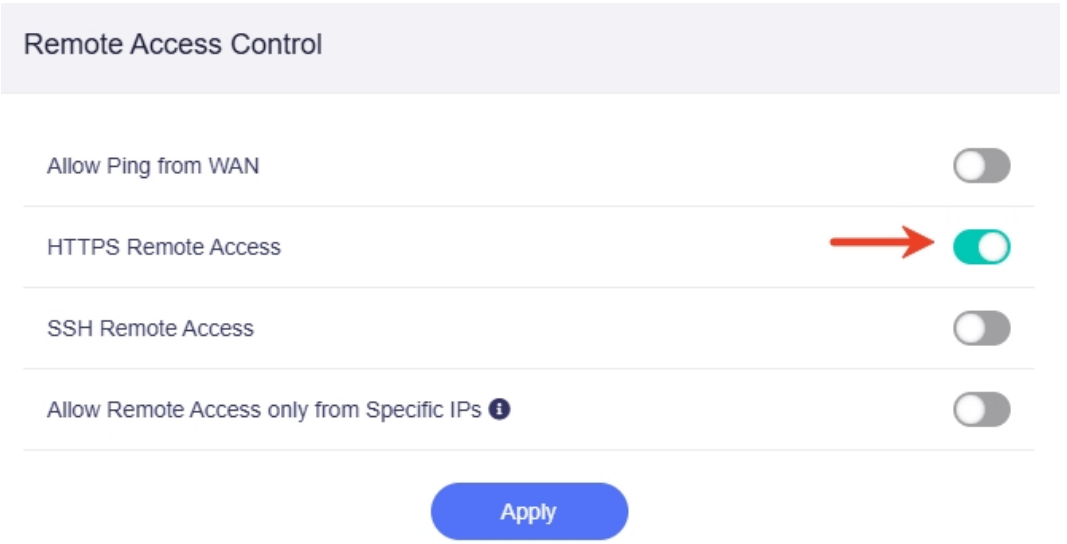
Une **adresse IP publique** est nécessaire. Consultez cette page pour vérifier si votre FAI vous en attribue une. Si le routeur est derrière un NAT, configurez une redirection du **port 443** sur le routeur en amont.

Pour activer l'accès HTTPS à distance, procédez comme suit.

1. Sur la page DNS dynamique, activez **Activer le DDNS (Enable DDNS)**, acceptez les **Conditions d'utilisation et la Politique de confidentialité (Terms of Services & Privacy Policy)**, puis cliquez sur **Appliquer (Apply)**.

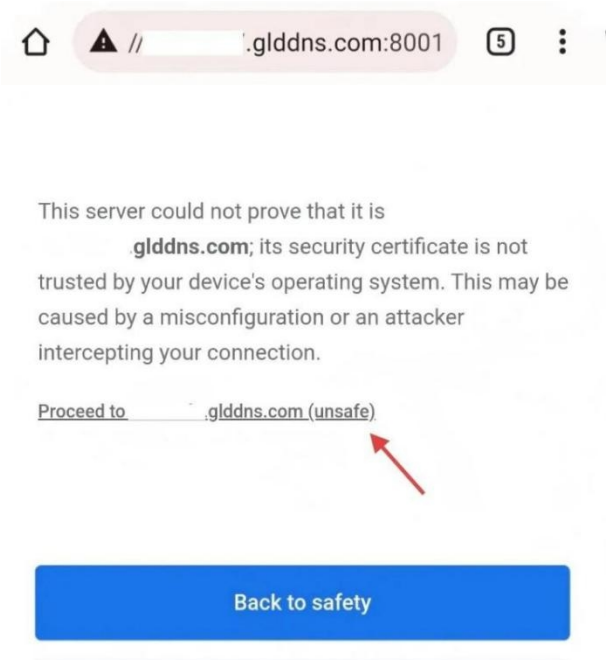


2. Dans l'interface d'administration Web, ouvrez **SÉCURITÉ (SECURITY)** > **Accès administrateur (Admin Access)** >**Contrôle de l'accès distant (Remote Access Control)**. Activez **Accès HTTPS distant (HTTPS Remote Access)**, puis cliquez sur **Appliquer (Apply)**.



Vous pouvez ensuite ouvrir l'interface depuis n'importe où avec le nom d'hôte DDNS en HTTPS, par exemple **https://xxxxxxx.glddns.com**. Si une redirection de port est configurée, utilisez **https://xxxxxxx.glddns.com:external_port** en remplaçant external_port par le numéro de port réel.

Remarque : cette fonction utilise des certificats autosignés. Le navigateur affiche donc « Votre connexion n'est pas privée » lors de l'accès HTTPS par le nom d'hôte DDNS. Cliquez sur **Avancé (Advanced)** en bas de la page, puis sur **Continuer vers xxxxxxx.glddns.com (Proceed to xxxxxxx.glddns.com)** pour poursuivre.



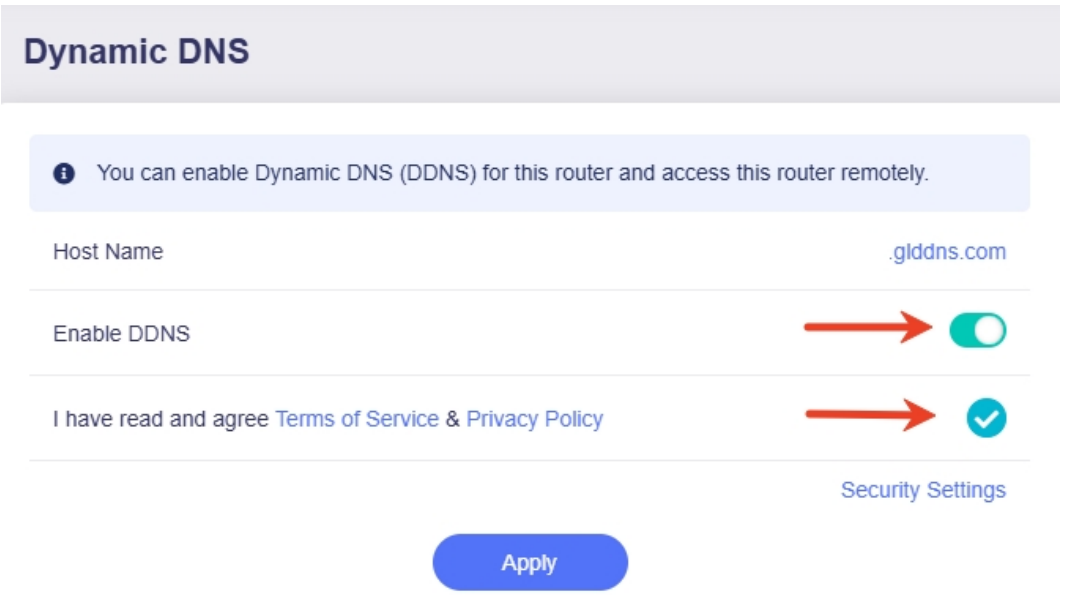
Vous pouvez ensuite accéder à l’interface d’administration Web du routeur avec son nom d’hôte DDNS via **HTTPS**.

15.2.4 Accès SSH à distance

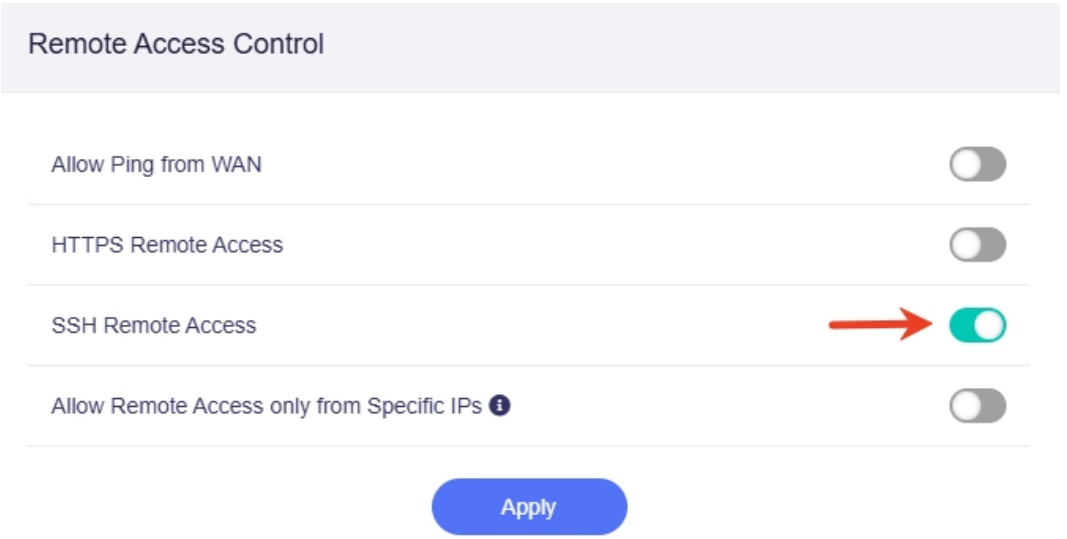
Une **adresse IP publique** est nécessaire. Consultez cette page pour vérifier si votre FAI vous en attribue une. Si le routeur est derrière un NAT, configurez une redirection du **port 22** sur le routeur en amont.

Pour activer l'accès SSH à distance, procédez comme suit.

1. Sur la page DNS dynamique, activez **Activer le DDNS (Enable DDNS)**, acceptez les **Conditions d'utilisation et la Politique de confidentialité (Terms of Services & Privacy Policy)**, puis cliquez sur **Appliquer (Apply)**.



2. Dans l'interface d'administration Web, ouvrez **SÉCURITÉ (SECURITY)** > **Accès administrateur (Admin Access)** >**Contrôle de l'accès distant (Remote Access Control)**. Activez **Accès SSH distant (SSH Remote Access)**, puis cliquez sur **Appliquer (Apply)**.



Vous pouvez ensuite accéder au routeur depuis n'importe où par SSH avec le nom d'hôte DDNS, par exemple **ssh root@xxxxxxx.glddns.com**. Si une redirection de port est configurée, utilisez **ssh root@xxxxxxx.glddns.com:external_port** en remplaçant external_port par le numéro de port réel.

15.3 Stockage réseau

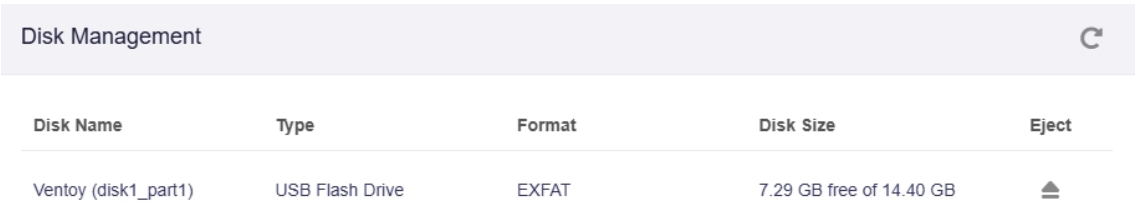
Le stockage réseau permet de partager des fichiers sans fil entre appareils en branchant un support USB ou une carte SD au routeur. Le support devient un lecteur réseau partagé, accessible aux appareils connectés par Wi-Fi.

Mango 2 possède un port USB compatible avec les clés USB et les disques durs externes portables. Vous pouvez configurer Samba pour ces supports de stockage aux formats courants, comme NTFS, FAT32 et EXT4.

Remarque : les disques durs USB consomment beaucoup d'énergie. Utilisez une alimentation externe pour éviter les dysfonctionnements.

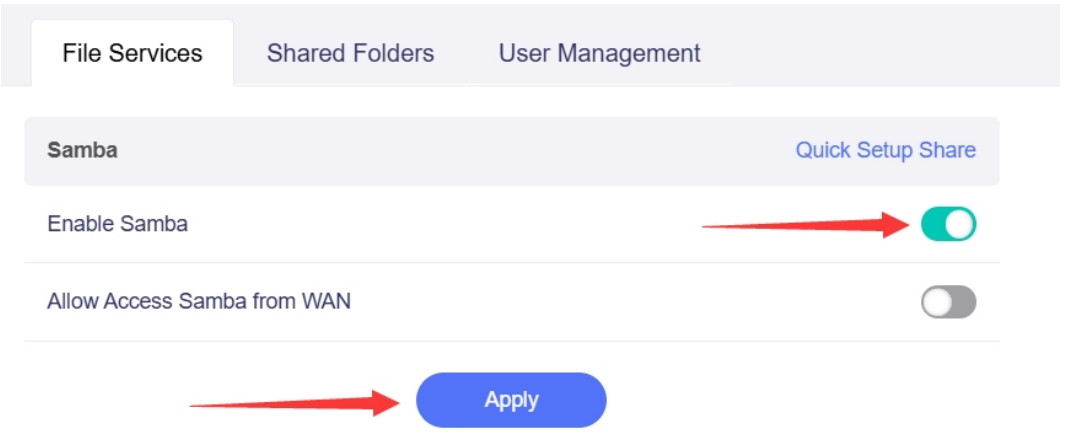
15.3.1 Branchement du stockage

1. Branchez le périphérique de stockage au routeur.
   - Pour une clé USB, branchez-la directement au port USB.
   - Pour un disque dur externe, branchez son alimentation séparée si nécessaire, puis reliez-le au routeur.
2. Connectez-vous à l'interface d'administration Web du routeur et ouvrez **APPLICATIONS** > **Stockage réseau (Network Storage)**. Vous pouvez y activer les services de transfert de fichiers et gérer le dossier partagé.
3. Si le support est détecté, la section **Gestion des disques (Disk Management)** s'affiche comme ci-dessous.



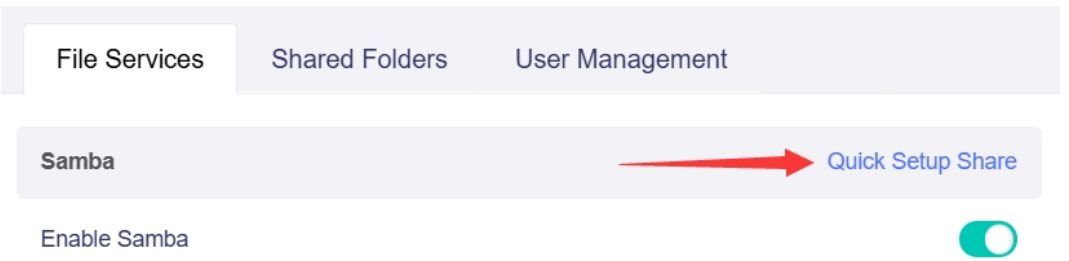
15.3.2 Configuration de Samba

1. Dans la section **Services de fichiers (File Services)**, activez **Activer Samba (Enable Samba)**, puis cliquez sur **Appliquer (Apply)**.

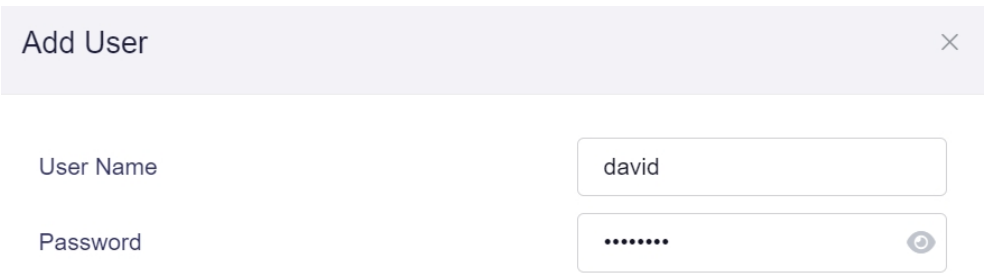


   - **Autoriser Samba depuis le WAN (Allow Access Samba from WAN)** : activez cette option pour que les appareils en amont accèdent à Samba.

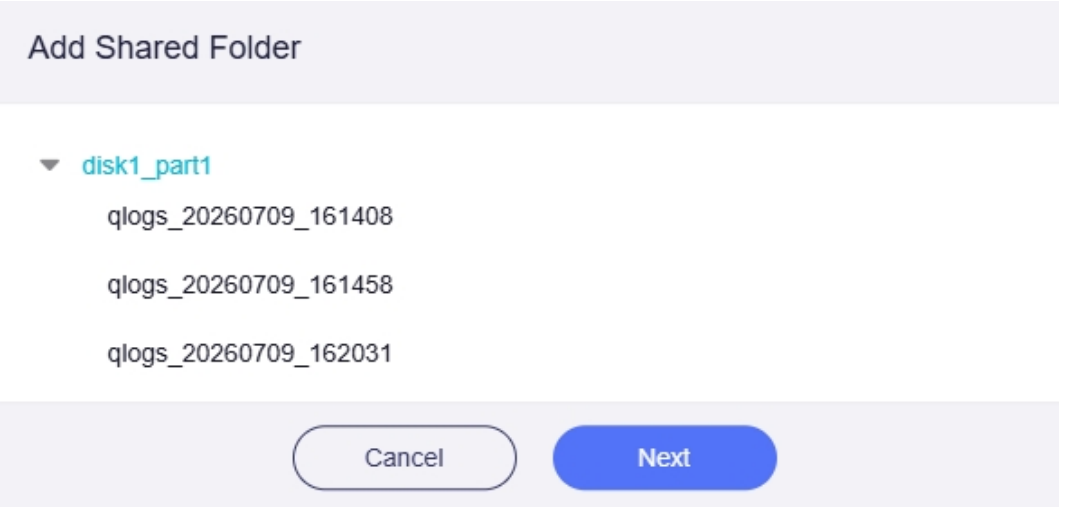
2. Cliquez sur **Configuration rapide du partage (Quick Setup Share)** pour créer le lien de partage.



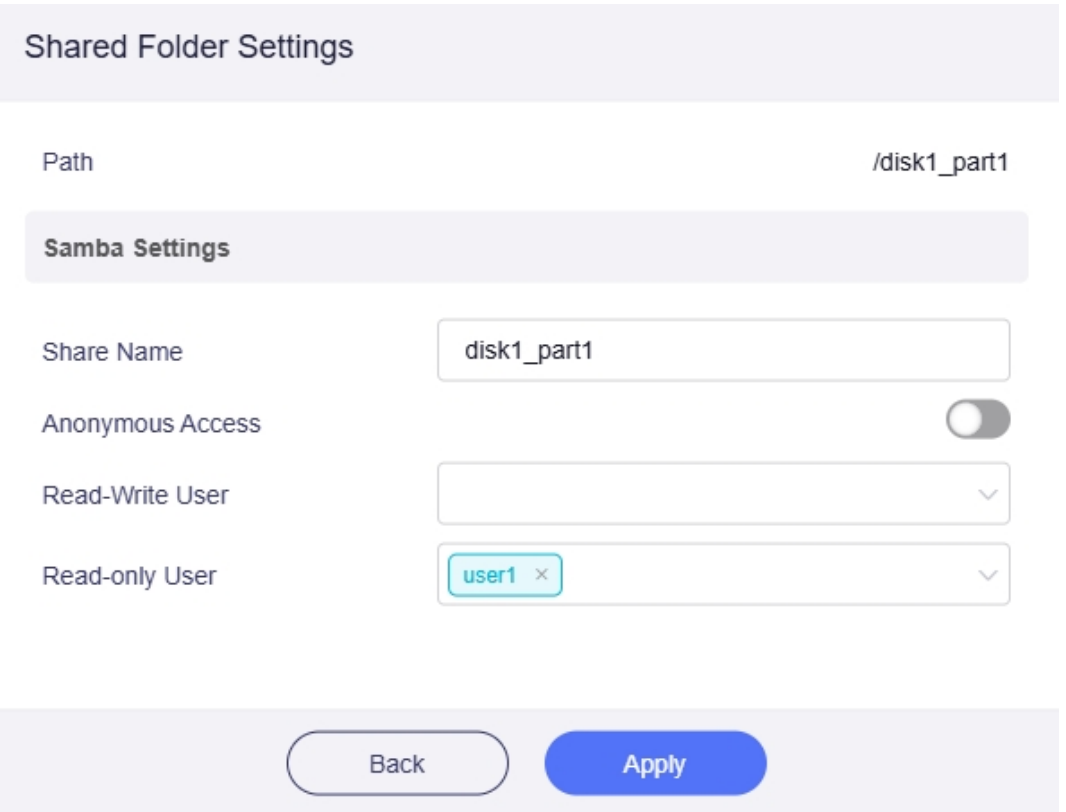
3. Ajoutez un utilisateur et cliquez sur **Suivant (Next)**. Cette étape est ignorée si un compte existe déjà.



4. Cliquez sur le triangle pour afficher tous les dossiers. Sélectionnez le dossier à partager, puis cliquez sur **Suivant (Next)**. Pour partager le disque entier, cliquez sur son nom, par exemple disk1_part1.

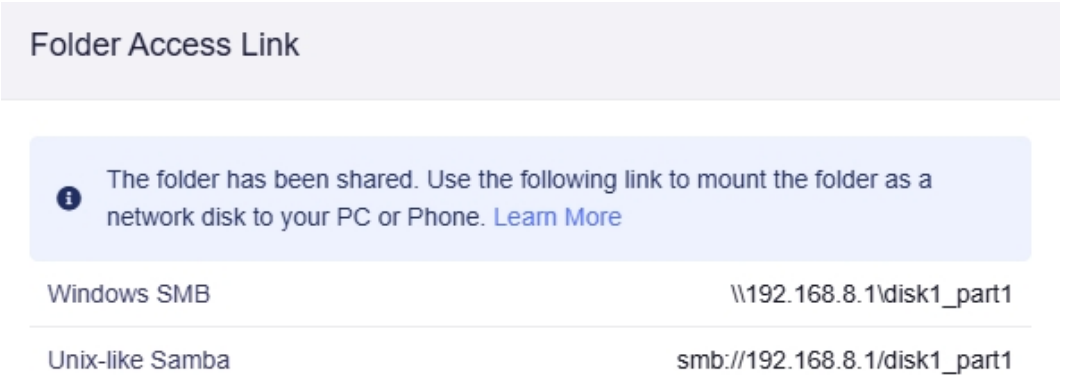


5. Configurez le dossier partagé.
   L'utilisateur créé est ajouté par défaut aux **Utilisateurs en lecture seule (Read-Only User)**. Pour lui permettre d'écrire ou de supprimer des fichiers, retirez-le de cette liste et ajoutez-le aux **Utilisateurs en lecture et écriture (Read-Write User)**, puis cliquez sur **Appliquer (Apply)**.



   Conseil : par sécurité, il est déconseillé d'activer l'accès anonyme.
6. Récupérez le lien d'accès au dossier.

La page affiche les liens pour Windows et les systèmes de type Unix, notamment Android, iOS, macOS et Ubuntu. Utilisez-les pour accéder au dossier partagé via Samba.



Remarque : si vous activez **Autoriser l’accès Samba depuis le WAN (Allow Access Samba from WAN)** et accédez au dossier partagé depuis le réseau en amont, remplacez l’adresse IP du routeur (192.168.8.1 par défaut) dans le lien d’accès par son adresse IP WAN, disponible sur la page INTERNET de l’interface d’administration Web.

15.4 Tailscale

Tailscale est un service VPN qui permet d'accéder à vos appareils et applications personnels depuis le monde entier, simplement et en toute sécurité. Consultez cette page pour en savoir plus.

La fonction Tailscale des routeurs GL.iNet permet de rejoindre un réseau virtuel Tailscale pour accéder à distance au routeur et aux ressources situées côté WAN et LAN.

Remarque :

1. Tailscale repose sur WireGuard. Il est déconseillé de l'utiliser simultanément avec les fonctions ou services suivants, car cela peut provoquer des conflits de routage : client OpenVPN, client WireGuard, GoodCloud Site to Site, ZeroTier et GoodPAS.
2. Cette fonction est actuellement en version bêta et peut présenter des anomalies.

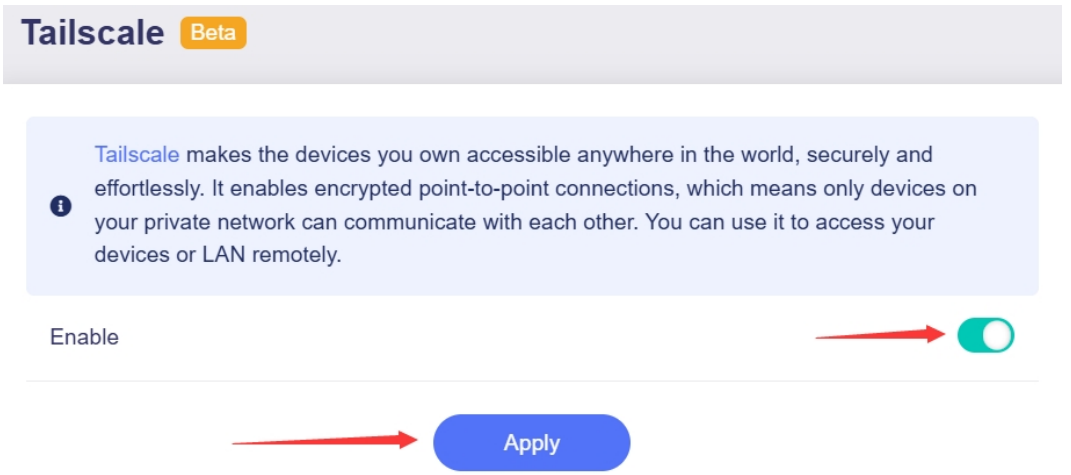
15.4.1 Configuration de Tailscale

Voici un exemple de configuration d'un réseau Tailscale avec GL-MG1300.

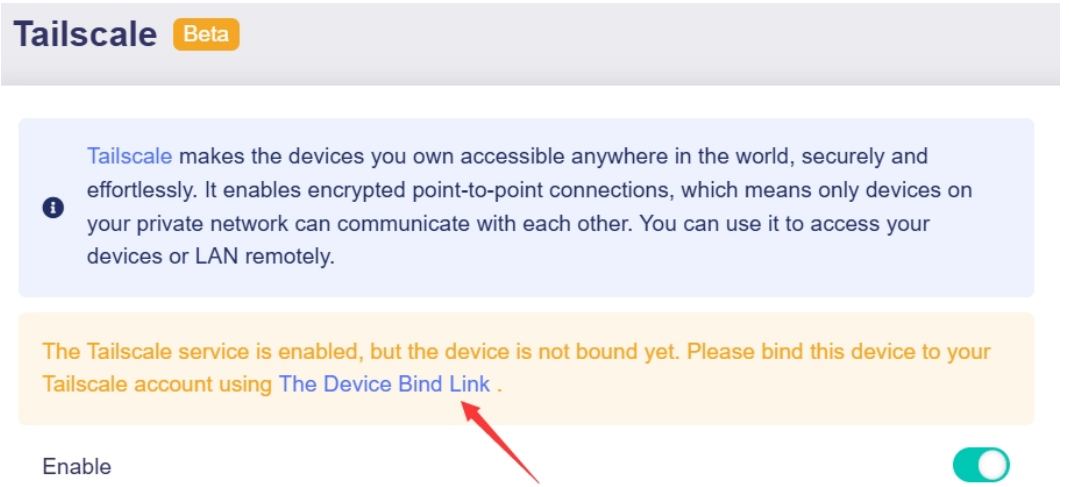
1. Créez d'abord un compte Tailscale et associez-y un ou deux appareils pour effectuer des tests. Ils apparaissent ensuite dans la console Tailscale.



2. Connectez-vous à l'interface d'administration Web du routeur et ouvrez **APPLICATIONS > Tailscale**. Activez **Activer Tailscale (Enable Tailscale)**, puis cliquez sur **Appliquer (Apply)**.



3. La page vous invite à associer l'appareil. Cliquez sur **Lien d'association de l'appareil (Device Bind Link)**.



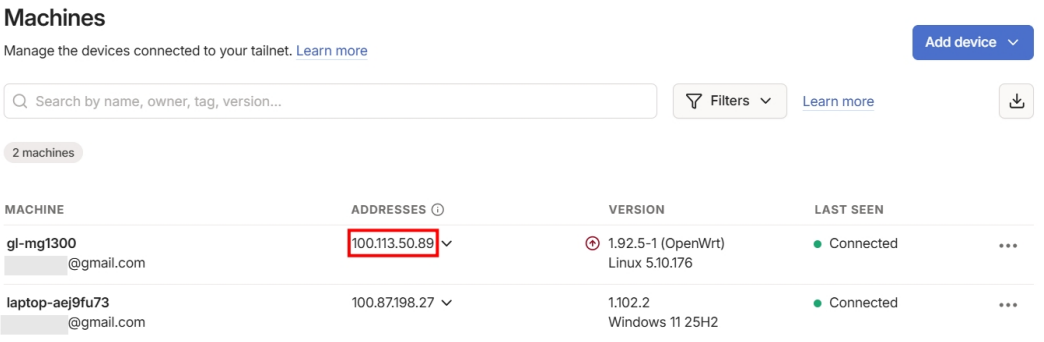
4. Dans la fenêtre qui s'affiche, cliquez sur le lien et connectez-vous à votre compte Tailscale.



5. Confirmez ensuite l'appareil en cliquant sur **Connecter (Connect)**.



6. Vous êtes redirigé vers la console d'administration Tailscale. Le routeur est maintenant ajouté au réseau virtuel Tailscale et accessible à distance via l'adresse IP virtuelle 100.113.50.89.

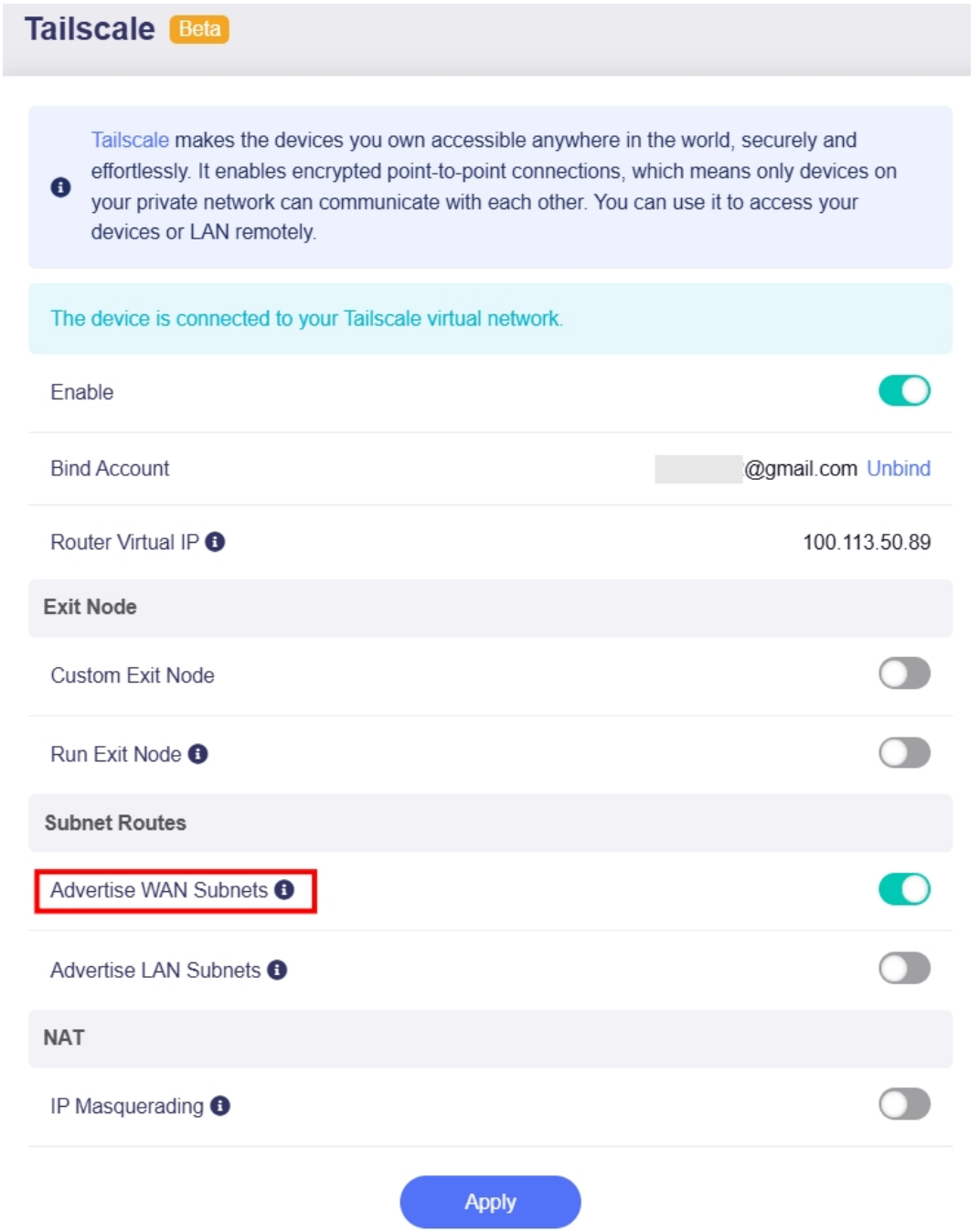


7. Testez la connexion.

   Sur un autre appareil connecté au même réseau Tailscale, ouvrez un navigateur Web et saisissez l'adresse IP virtuelle du routeur dans la barre d'adresse. Si vous pouvez accéder à l'interface d'administration Web du routeur, Tailscale fonctionne. Vous pouvez aussi utiliser la commande ping ou vous connecter à son terminal via SSH avec cette adresse IP virtuelle pour vérifier la connectivité.

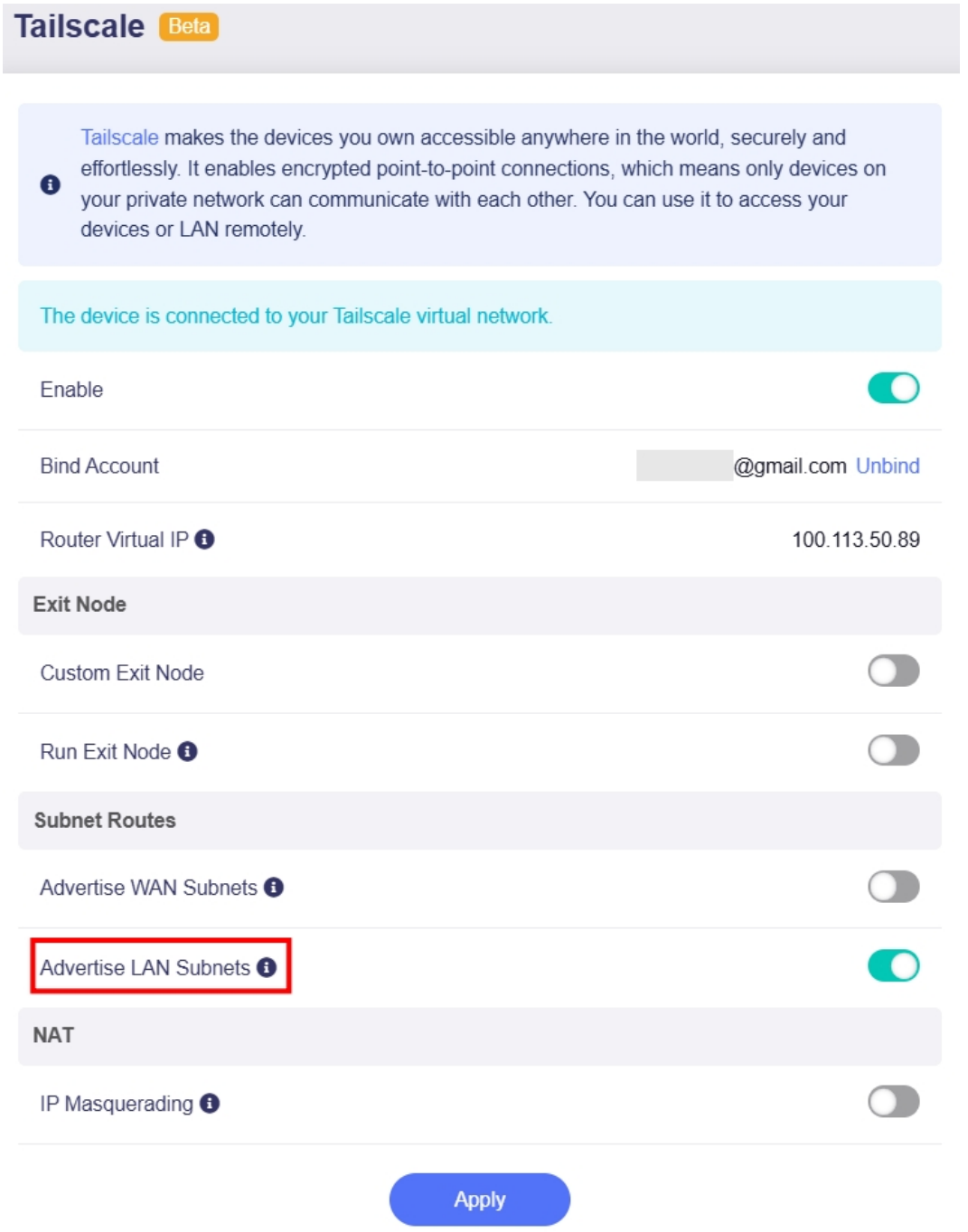
15.4.2 Annoncer les sous-réseaux WAN

Si cette option est activée, les ressources côté WAN de l'appareil sont accessibles par le réseau virtuel Tailscale. Consultez cette page pour en savoir plus.



15.4.3 Annoncer les sous-réseaux LAN

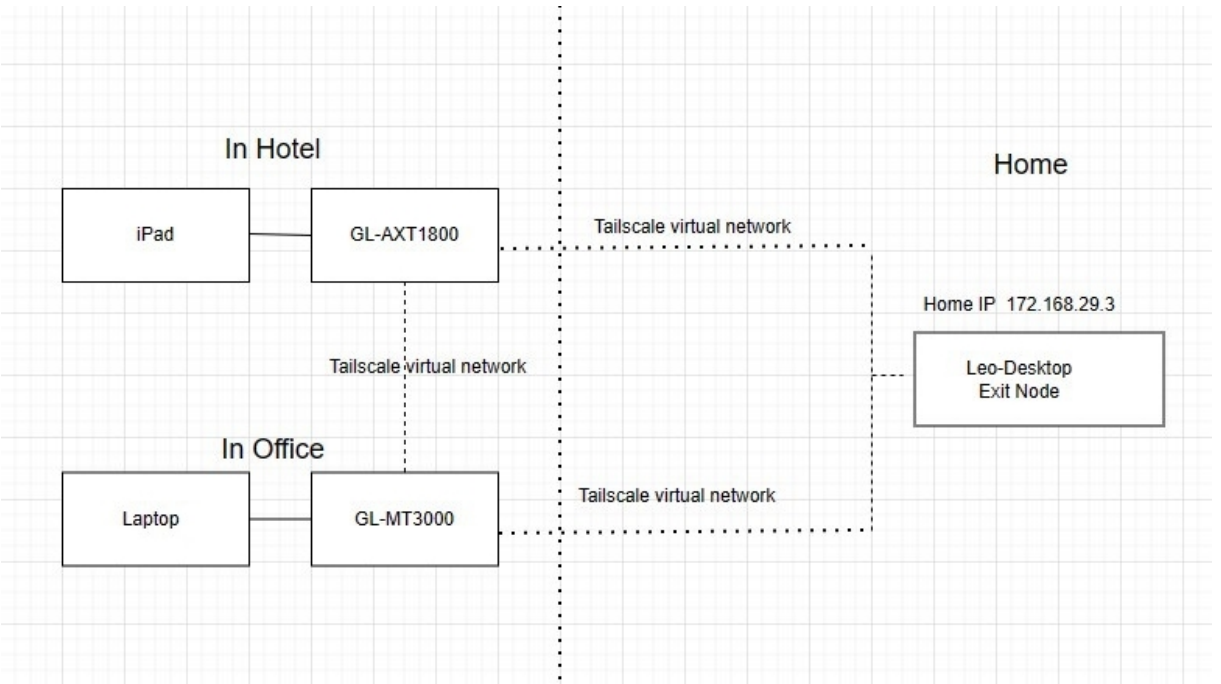
Si cette option est activée, les ressources côté LAN de l'appareil sont accessibles par le réseau virtuel Tailscale. Consultez cette page pour en savoir plus.



15.4.4 Nœuds de sortie personnalisés

Par défaut, Tailscale fonctionne comme un réseau superposé : il achemine uniquement le trafic entre les appareils utilisant Tailscale et ne traite pas votre trafic Internet public, comme la navigation sur Google.

Vous pouvez toutefois vouloir faire passer ce trafic par Tailscale. Par exemple, en déplacement à l'étranger, pour accéder à des services bancaires réservés à votre pays, configurez votre ordinateur domestique disposant d'une IP publique comme nœud de sortie. Réglez les autres appareils du même Tailnet, comme les GL-AXT1800 et GL-MT3000 ci-dessous, pour qu'ils l'utilisent. Tout leur trafic Internet public passe alors par ce nœud.



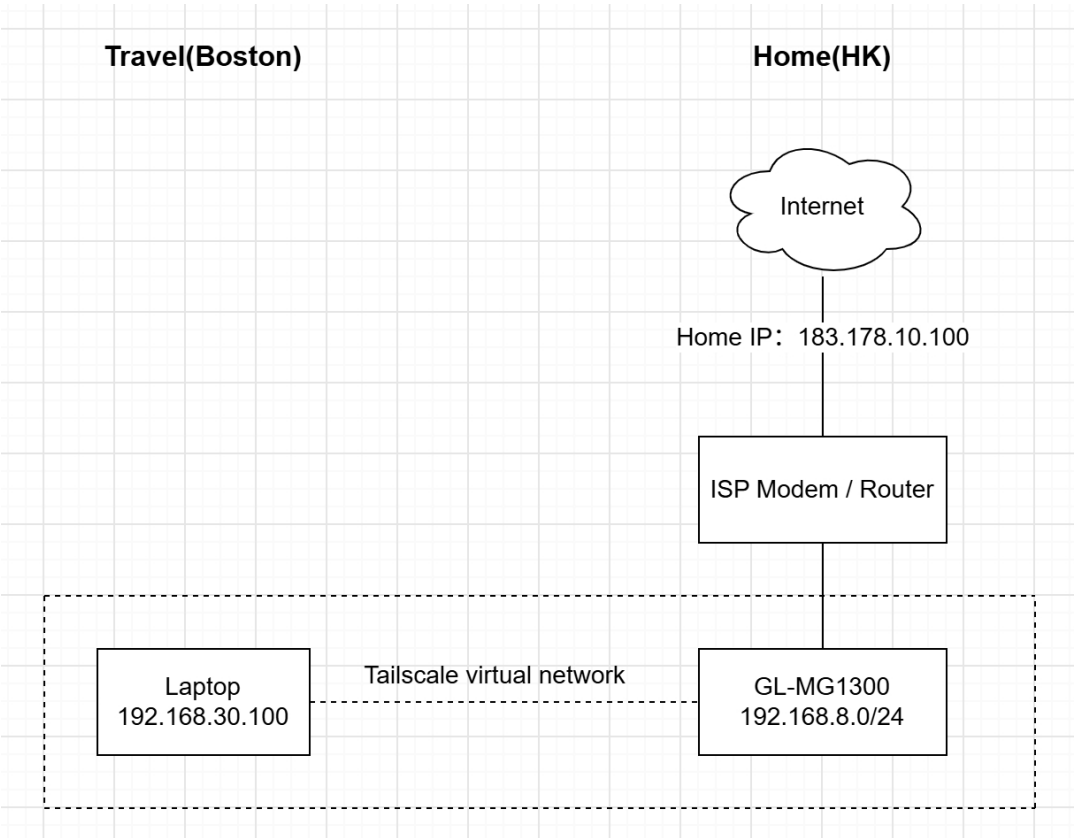
Un nœud de sortie achemine le trafic Internet sortant des appareils du Tailnet et joue ainsi le rôle d'un serveur VPN. Tout le trafic Internet extérieur à Tailscale semble provenir de son emplacement, ce qui facilite l'accès aux contenus géorestreints et renforce la confidentialité. L'appareil chargé de cet acheminement est appelé « nœud de sortie ». Consultez cette page pour en savoir plus.

Remarque : si le serveur DNS du routeur utilise une IP privée accessible uniquement sur le réseau local, l'emploi d'un nœud de sortie peut interrompre l'accès Internet. Définissez manuellement un DNS public, comme 8.8.8.8, pour l'éviter.

15.4.5 Exécuter un nœud de sortie

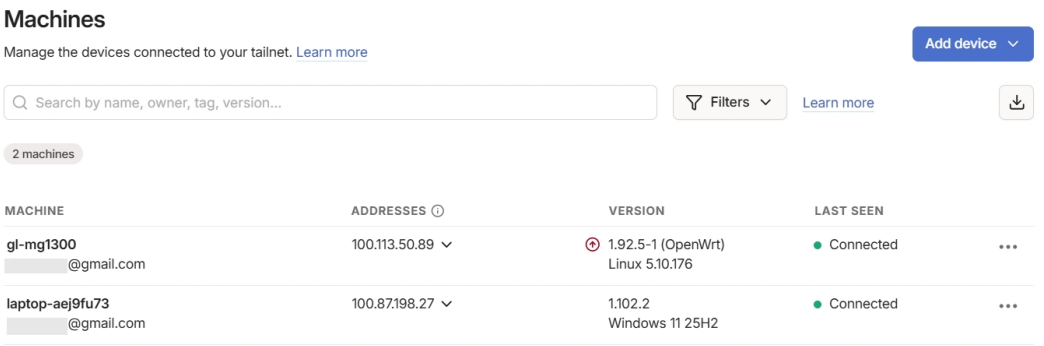
En exécutant un nœud de sortie sur votre routeur, vous permettez aux autres appareils de votre réseau Tailscale (tailnet) d'acheminer tout leur trafic Internet sortant via l'adresse IP publique de ce routeur.

Dans la topologie ci-dessous, un ordinateur portable se trouve à Boston et un routeur GL-MG1300 à Hong Kong. Tous deux appartiennent au même réseau Tailscale. Si vous configurez GL-MG1300 comme nœud de sortie, tout le trafic sortant de l'ordinateur portable passe par ce routeur pour accéder à Internet. L'adresse IP publique de l'ordinateur correspond alors à une adresse de Hong Kong plutôt qu'à une adresse de Boston.

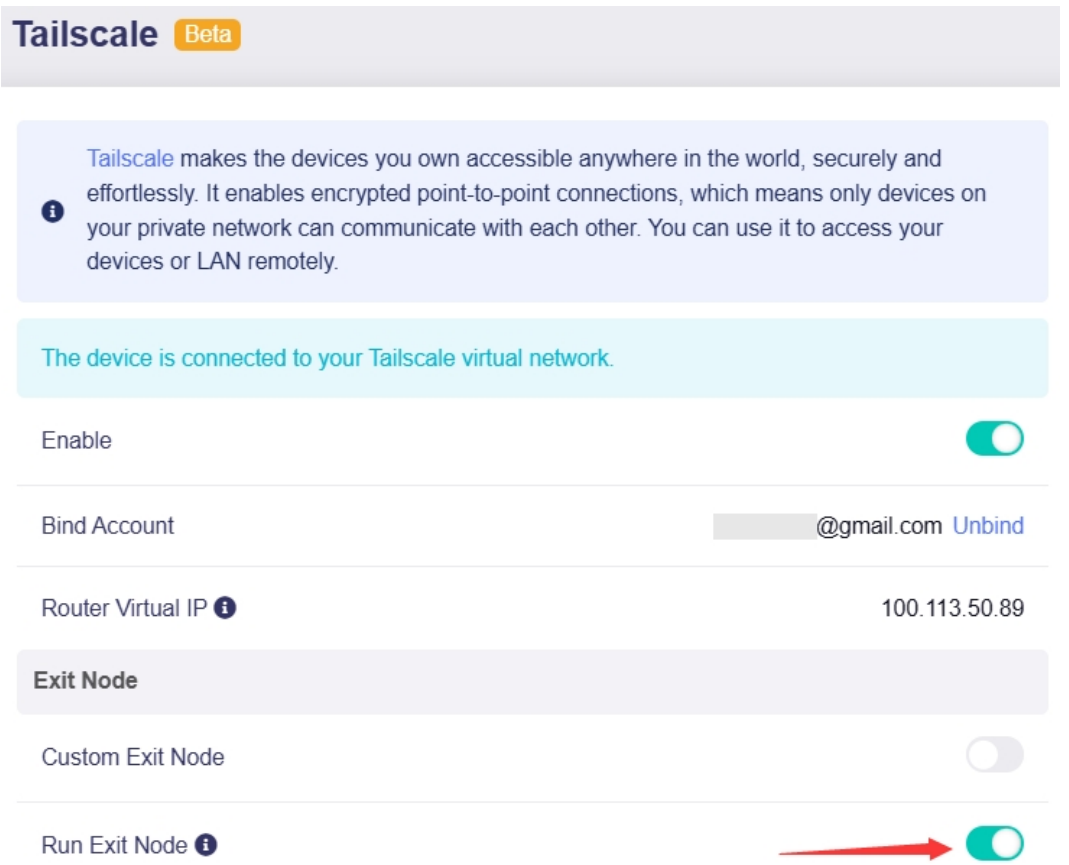


Voici les étapes pour configurer GL-MG1300 comme nœud de sortie.

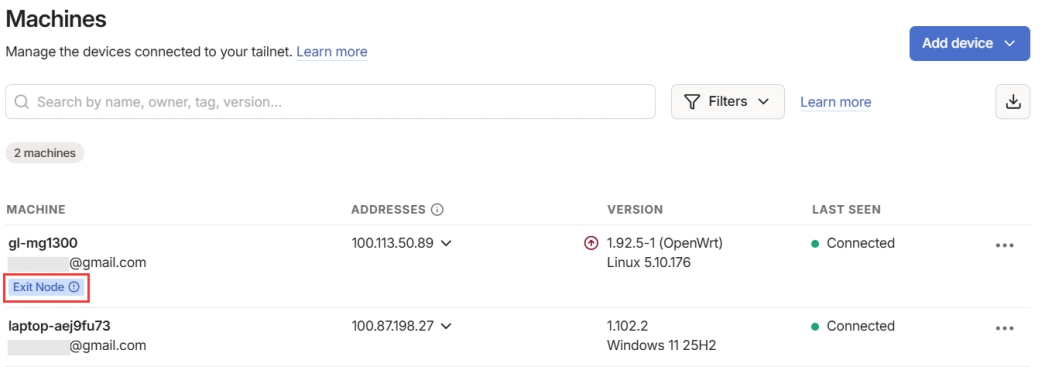
1. Ajoutez le routeur GL-MG1300 et l'ordinateur portable de voyage au même tailnet Tailscale.



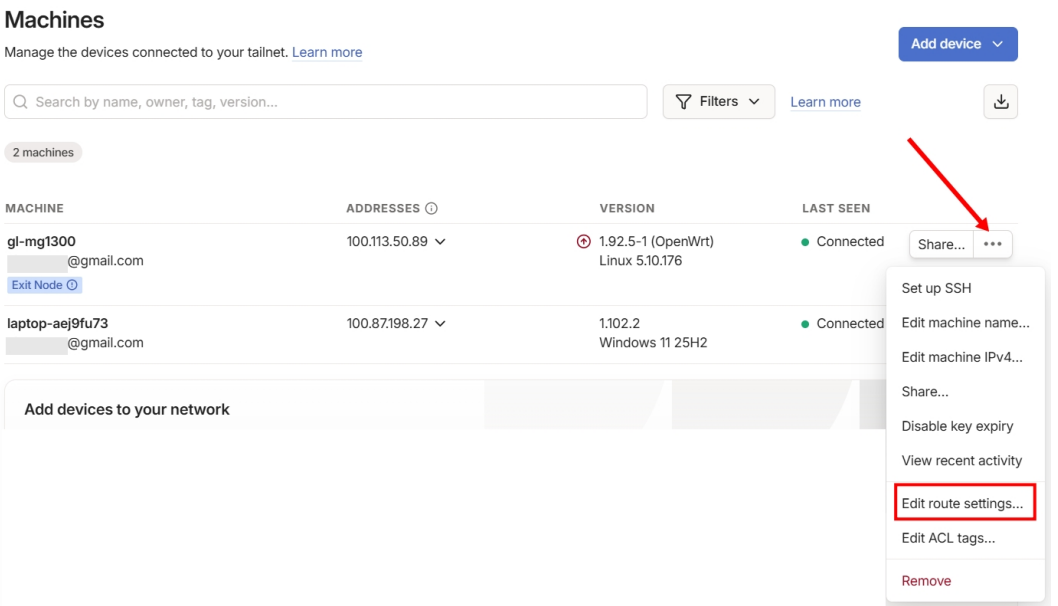
2. Dans l'interface d'administration Web de GL-MG1300, ouvrez **APPLICATIONS** > **Tailscale**. Activez **Exécuter comme nœud de sortie (Run Exit Node)**, puis cliquez sur **Appliquer (Apply)**.



3. Ouvrez la console d'administration Tailscale. L'étiquette « Exit Node » apparaît sous GL-MG1300.



4. Cliquez sur l'icône à trois points à droite de GL-MG1300 et sélectionnez **Modifier les paramètres des routes (Edit route settings)**.

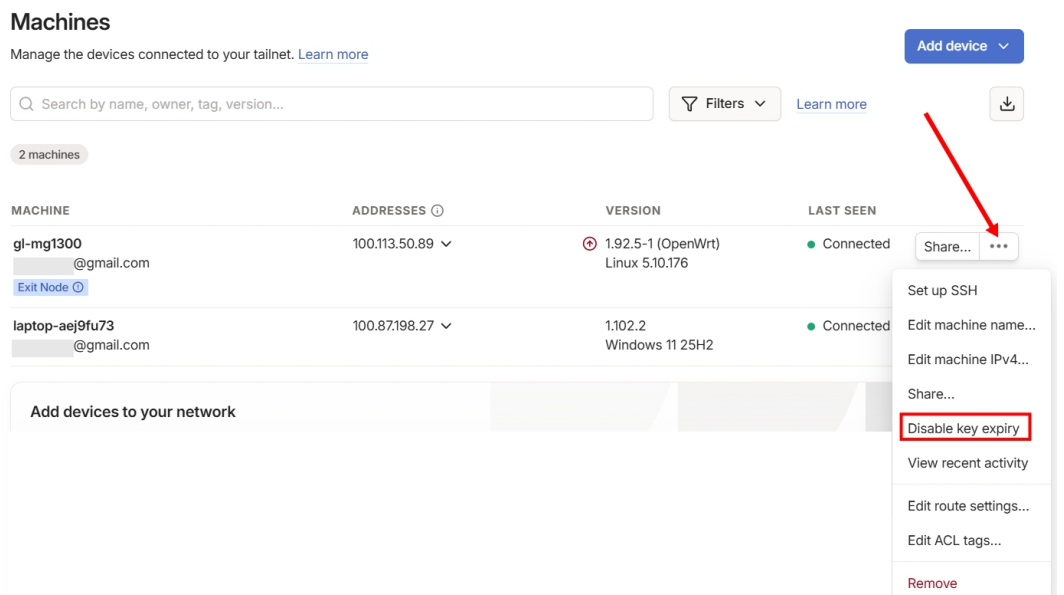


5. Dans la fenêtre qui s'ouvre, cochez **Utiliser comme nœud de sortie (Use as exit node)**, puis cliquez sur **Enregistrer (Save)**.

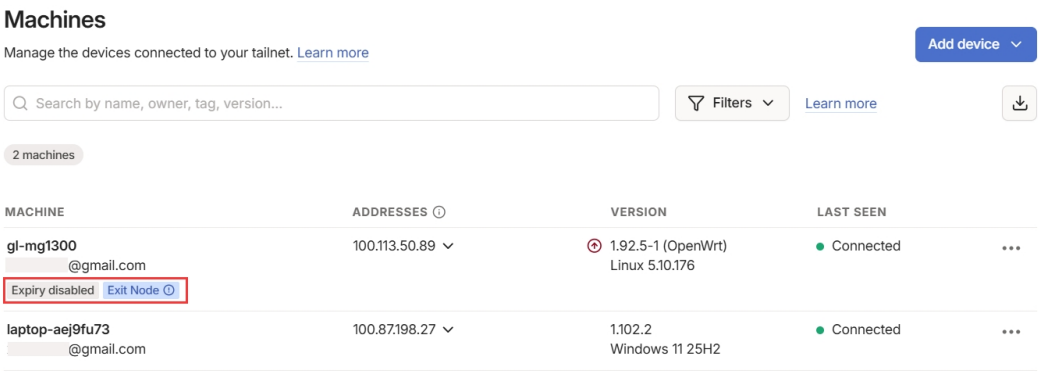


6. Désactivez l'expiration de la clé.

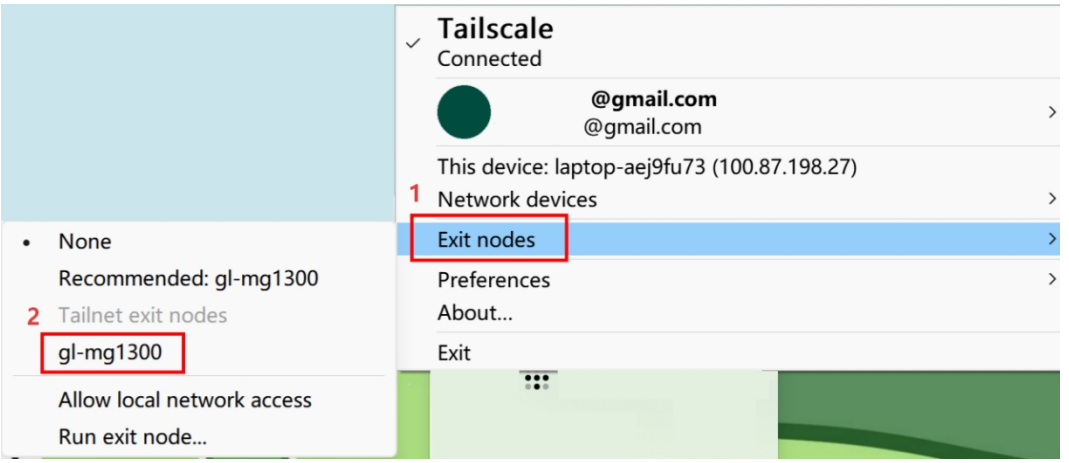
   Pour des raisons de sécurité, les utilisateurs doivent régulièrement s'authentifier à nouveau sur chacun de leurs appareils. Pour éviter les déconnexions lorsque la clé d'authentification du nœud de sortie expire, nous recommandons de désactiver son expiration pour ce nœud. Cliquez ici pour en savoir plus sur l'expiration des clés. Cliquez sur l'icône à trois points à droite de GL-MG1300 et sélectionnez Désactiver l'expiration de la clé (Disable key expiry).



   Après validation, l'étiquette « Expiry disabled » apparaît sous GL-MG1300.



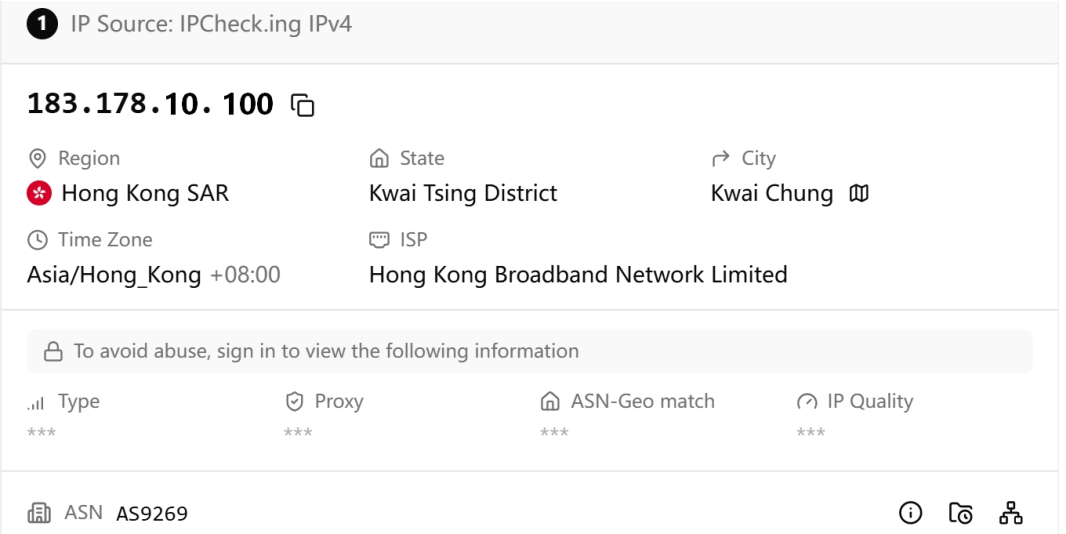
7. Exécutez Tailscale sur votre ordinateur portable de voyage. Son icône apparaît dans la zone de notification en bas à droite. Faites un clic droit sur cette icône, cliquez sur **Nœuds de sortie (Exit nodes)** et sélectionnez **gl-mg1300**.



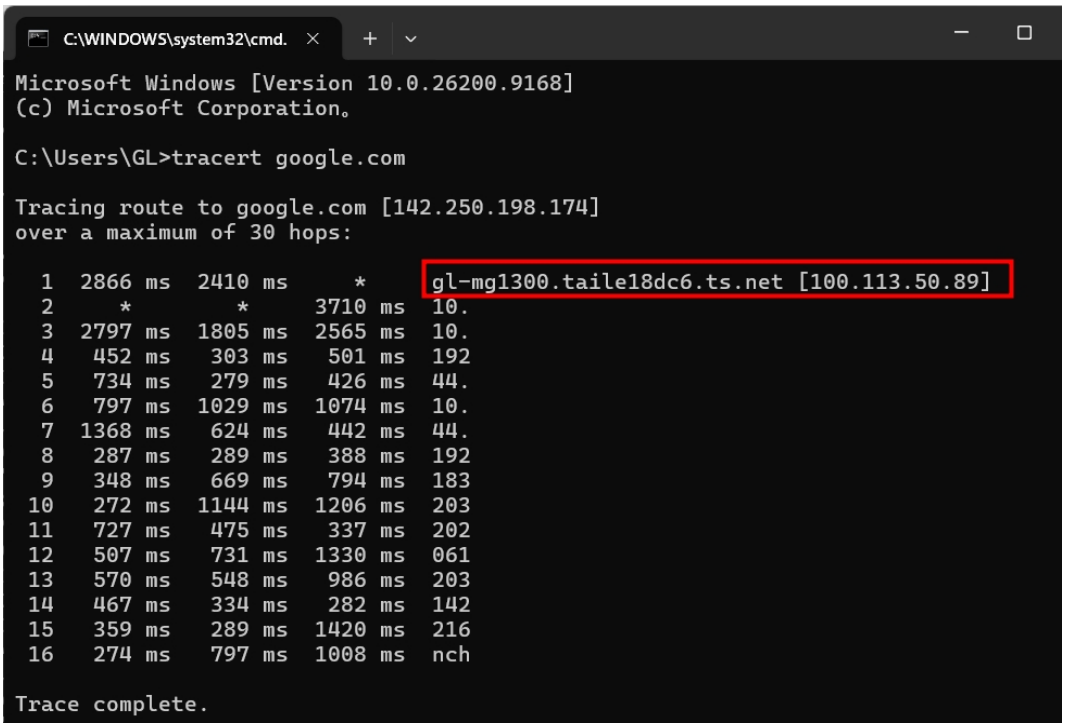
Tout le trafic sortant de cet ordinateur portable passe désormais par GL-BMG1300 pour accéder à Internet.

8. Testez la connexion.

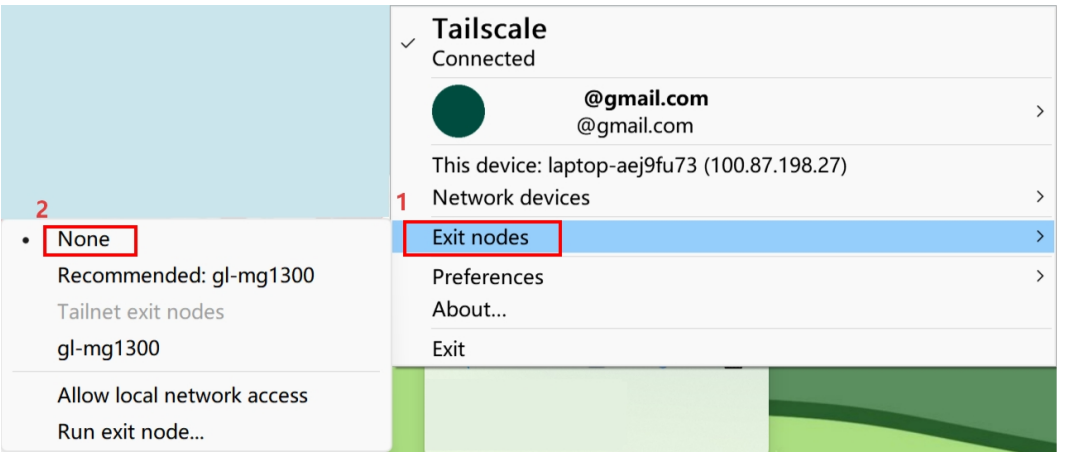
(1) Sur votre ordinateur portable de voyage, ouvrez un navigateur Web et accédez à ipcheck.ing ou à un autre site de vérification d'adresse IP. La page affiche l'adresse IP publique du nœud de sortie Tailscale, ce qui confirme que l'ordinateur accède à Internet via ce nœud, ici le GL-MG1300 situé à Hong Kong.



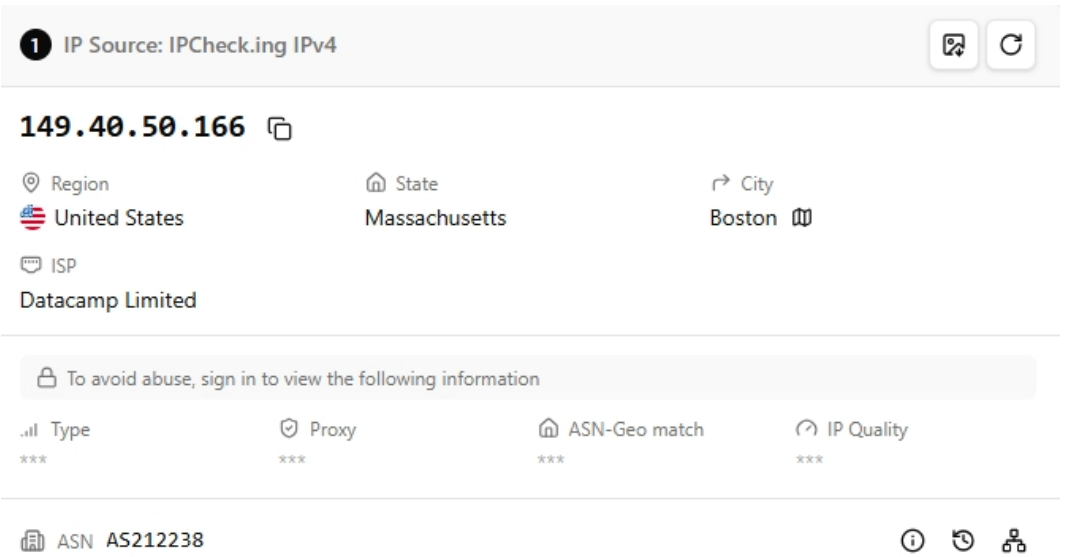
(2) Appuyez sur *Win+R*, saisissez *cmd* pour ouvrir l'invite de commandes, puis exécutez *tracert google.com* pour suivre le trajet du trafic sortant. Le résultat de la commande indique tous les sauts effectués par votre trafic Internet. Si la configuration est correcte, le premier saut externe passe par le nœud de sortie, comme ci-dessous, ce qui confirme que tout le trafic Internet sortant transite par ce routeur.



(3) Déconnectez le nœud de sortie pour comparer les résultats. Faites un clic droit sur l'icône Tailscale dans la zone de notification, en bas à droite, cliquez sur **Nœuds de sortie (Exit nodes)**, puis sélectionnez **Aucun (None)** pour cesser de l'utiliser.



(4) Ouvrez un nouvel onglet du navigateur et consultez ipcheck.ing ou un autre service de vérification d'adresse IP. L'adresse IP publique propre à votre ordinateur portable s'affiche désormais, ce qui prouve qu'il utilise votre connexion Internet locale (à Boston dans cet exemple).



Chapitre 16

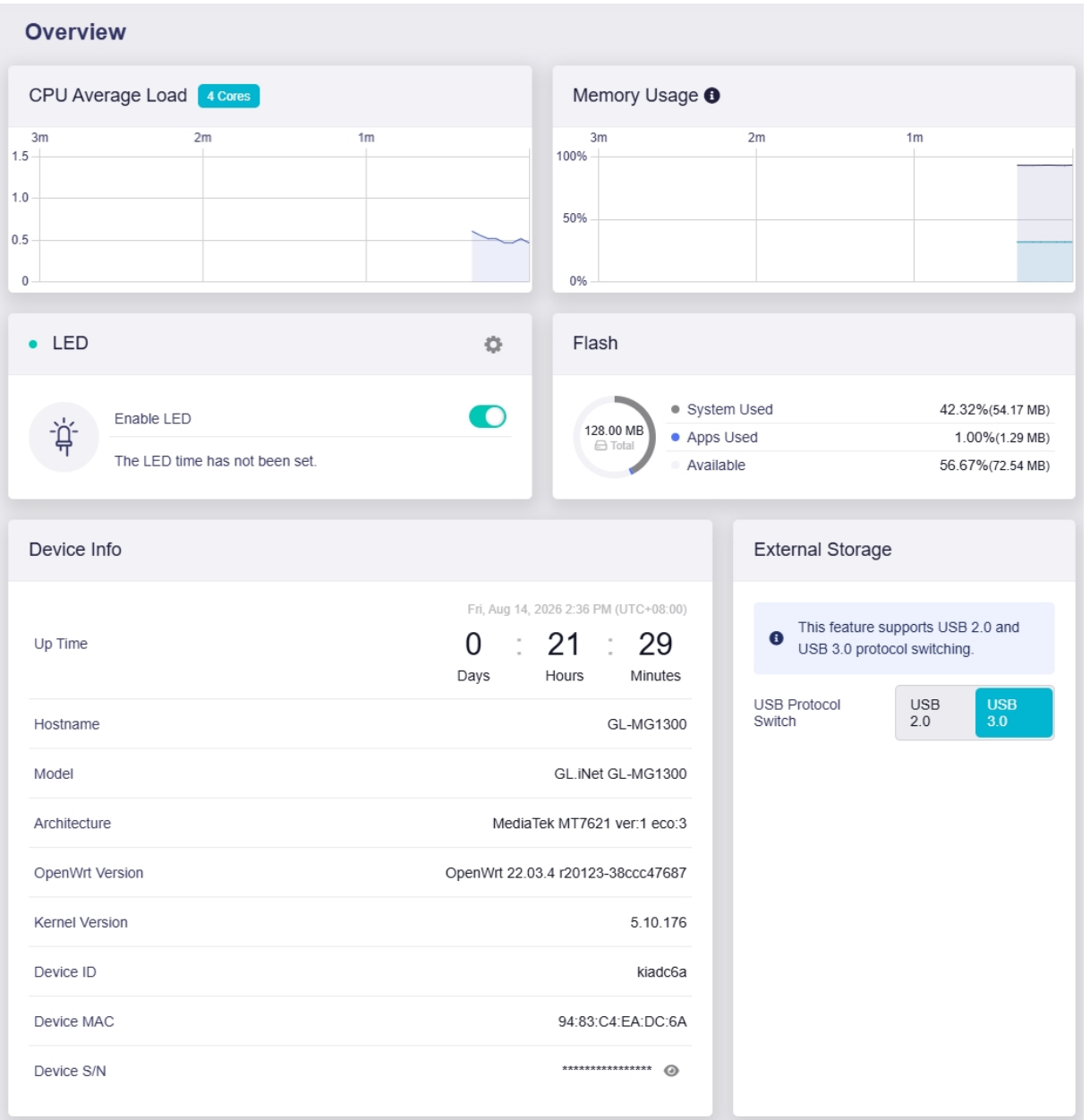
Système

Ce chapitre présente les outils de gestion de l’appareil : vue d’ensemble, mises à jour, tâches planifiées, fuseau horaire, journaux, réinitialisation du micrologiciel et paramètres avancés.

16.1 Vue d’ensemble

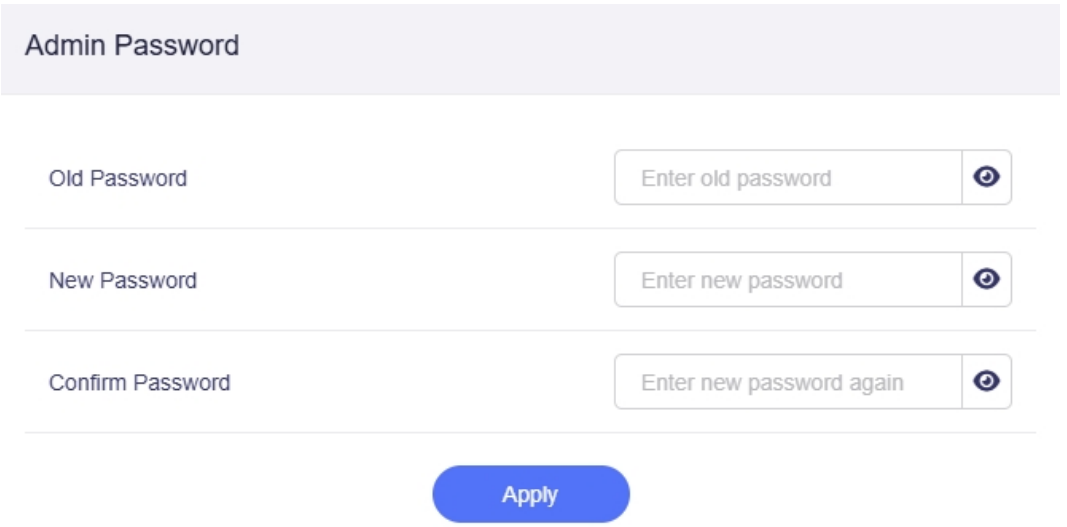
Connectez-vous à l’interface d’administration Web du routeur et ouvrez **SYSTÈME (SYSTEM)** > **Vue d’ensemble (Overview)**. Cette page affiche l’état du matériel et propose quelques commandes simples, notamment :

- État du processeur, de la mémoire et de la mémoire flash
- Commande du voyant LED
- Informations sur l’appareil
- Sélection du protocole de stockage externe



16.2 Mot de passe administrateur

Connectez-vous à l'interface d'administration Web du routeur et ouvrez **SYSTÈME (SYSTEM)** > **Mot de passe administrateur (Admin Password)**. Cette page permet de modifier le mot de passe de connexion à l'interface d'administration Web.



Le mot de passe administrateur doit respecter les règles suivantes :

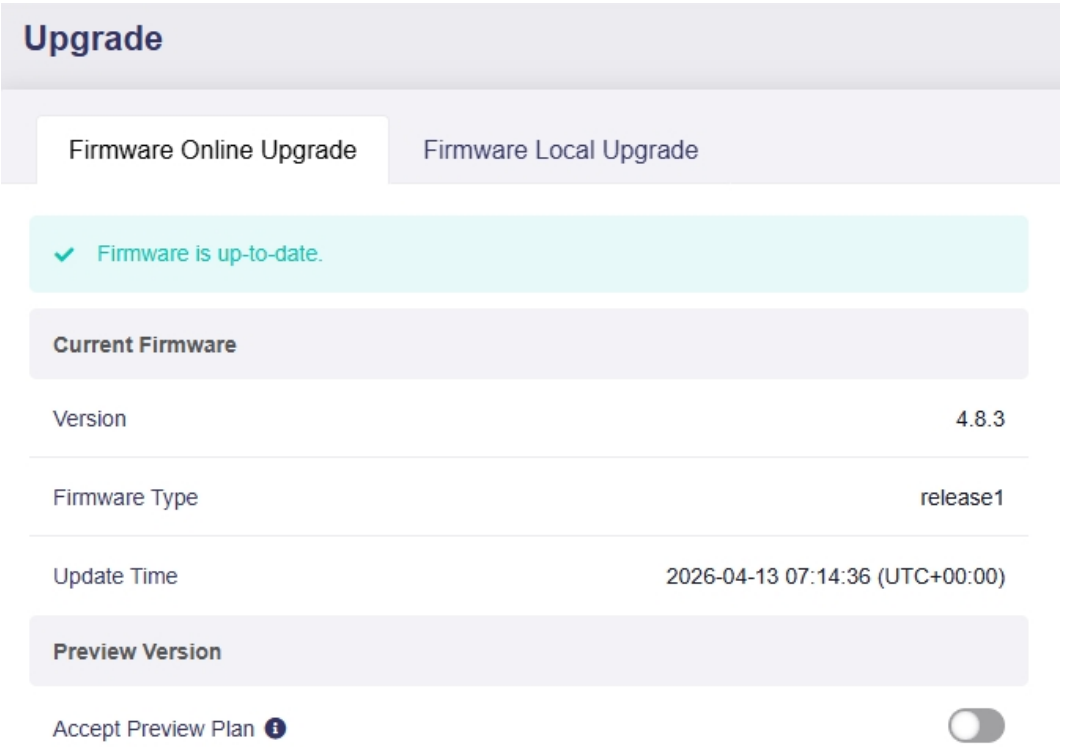
1. Entre 10 et 63 caractères.
2. Les lettres, avec distinction de casse, les chiffres et les symboles sont autorisés, par exemple : ! @ # $ % ^ & * ( ) _ + - = , . > < | ? / \ [ ] { } : ; " ' ` ~
3. Au moins deux catégories sont nécessaires parmi les majuscules, les minuscules, les chiffres et les symboles.

16.3 Mise à jour

Connectez-vous à l'interface d'administration Web du routeur et ouvrez **SYSTÈME (SYSTEM)** > **Mise à jour (Upgrade)**. Vous pouvez mettre à jour le micrologiciel du routeur en ligne ou localement.

16.3.1 Mise à jour en ligne

Cette page présente la version du micrologiciel, son type, par exemple stable ou bêta, et la date de mise à jour.



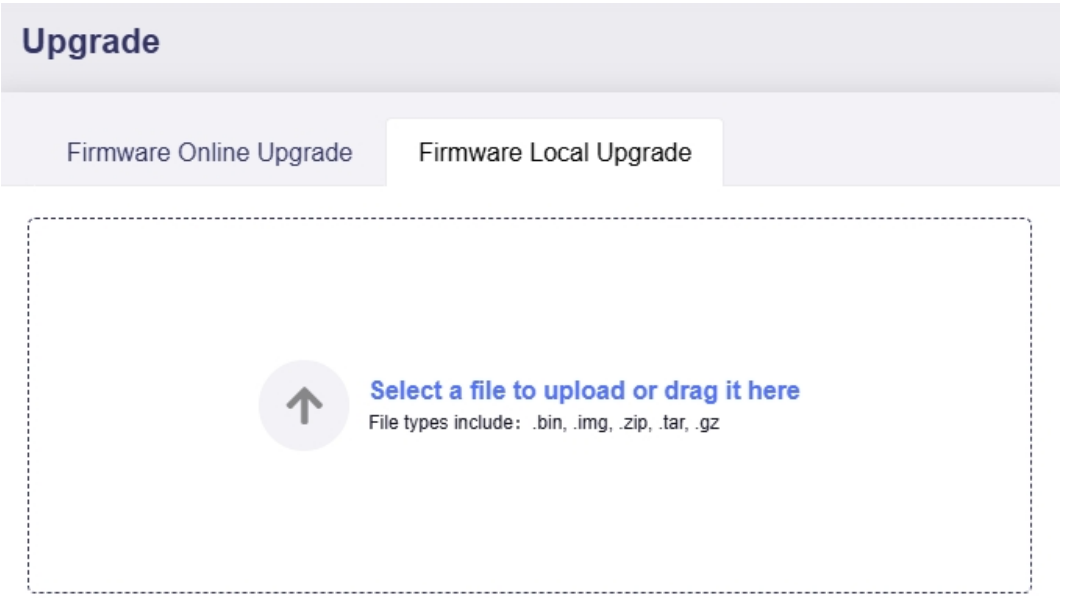
- **Participer au programme de préversion (Accept Preview Plan)** : activez cette option pour essayer de nouvelles fonctions avant leur version finale et nous transmettre vos commentaires. Une fois activée, elle le reste. Ces mises à jour peuvent être instables.

Si le routeur est connecté à Internet, il recherche une version plus récente du micrologiciel à télécharger.

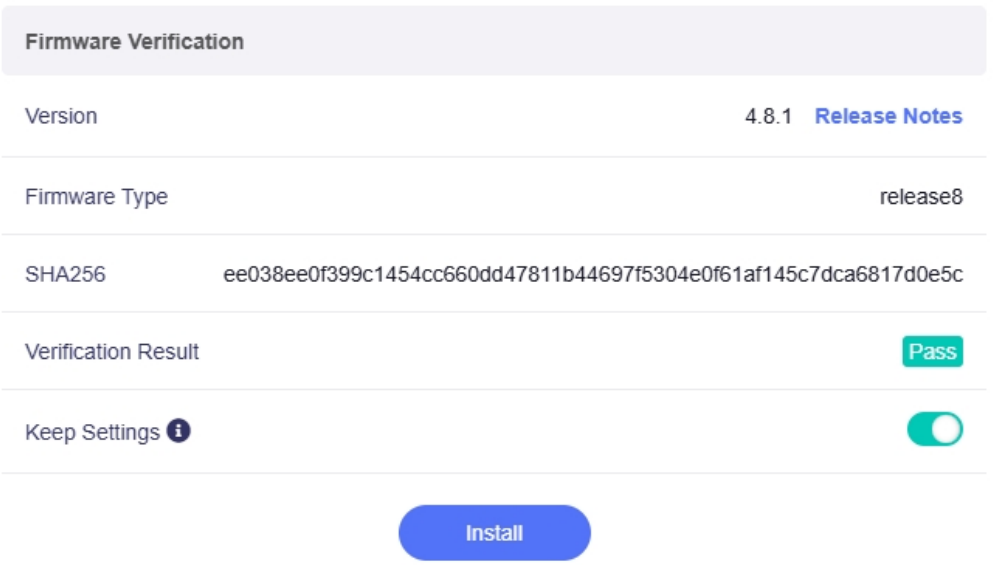
Conseil : si la mise à jour en ligne affiche **Échec du téléchargement (Download Failed)**, ouvrez **SYSTÈME (SYSTEM)** > **Fuseau horaire (Time Zone)** et corrigez l'heure en la synchronisant avec le navigateur.

16.3.2 Mise à jour locale

La mise à jour locale ne nécessite pas de connexion Internet sur le routeur. Téléchargez sur votre appareil local le micrologiciel correspondant au modèle de votre routeur depuis le Centre de téléchargement officiel. Connectez-vous ensuite à l'interface d'administration Web du routeur, ouvrez **SYSTÈME (SYSTEM)** > **Mise à jour (Upgrade)** > **Mise à jour locale (Local Upgrade)**, puis téléversez le fichier du micrologiciel.



Vérifiez les informations du micrologiciel affichées avant de cliquer sur **Installer (Install)**.



- **Conserver les paramètres (Keep Settings)** : conserve vos réglages actuels. Les paquets installés manuellement doivent toutefois être réinstallés après la mise à jour. Désactivez cette option lorsque vous installez une version antérieure.

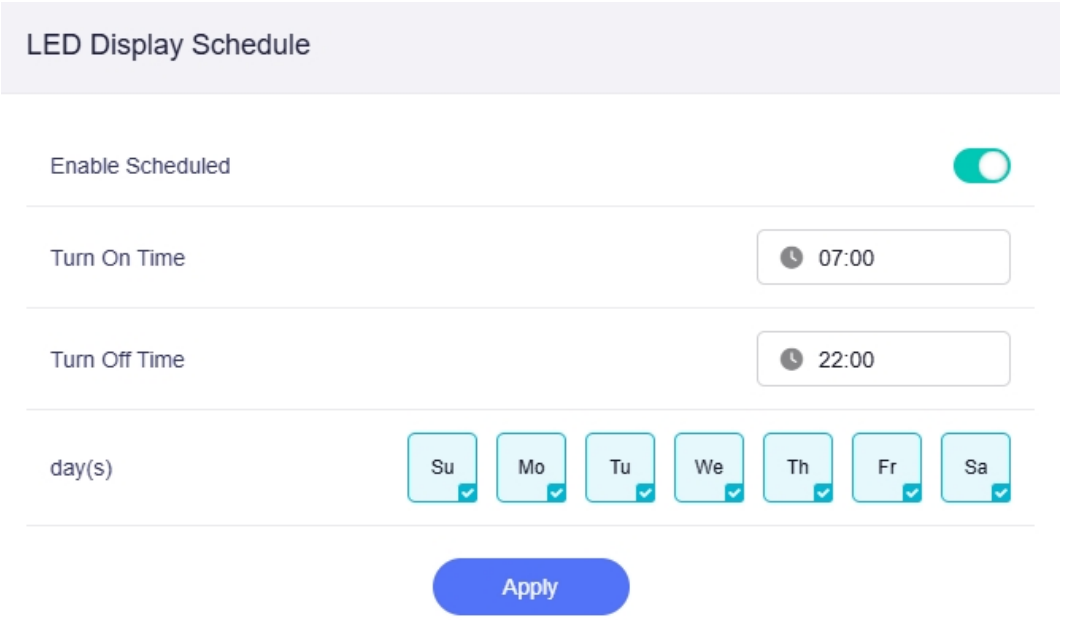
16.4 Tâches planifiées

Connectez-vous à l'interface d'administration Web du routeur et ouvrez **SYSTÈME (SYSTEM)** > **Tâches planifiées (Scheduled Tasks)**. Cette page permet de programmer quotidiennement certaines actions simples, notamment l'allumage et l'extinction du voyant LED et le redémarrage du routeur.

Remarque : synchronisez l'heure dans la section Fuseau horaire (Time Zone) avant d'utiliser cette fonction. Si l'appareil est éteint à l'heure prévue, la tâche n'est pas exécutée.

16.4.1 Programmation du voyant LED

Définissez si nécessaire une programmation pour le voyant du routeur.

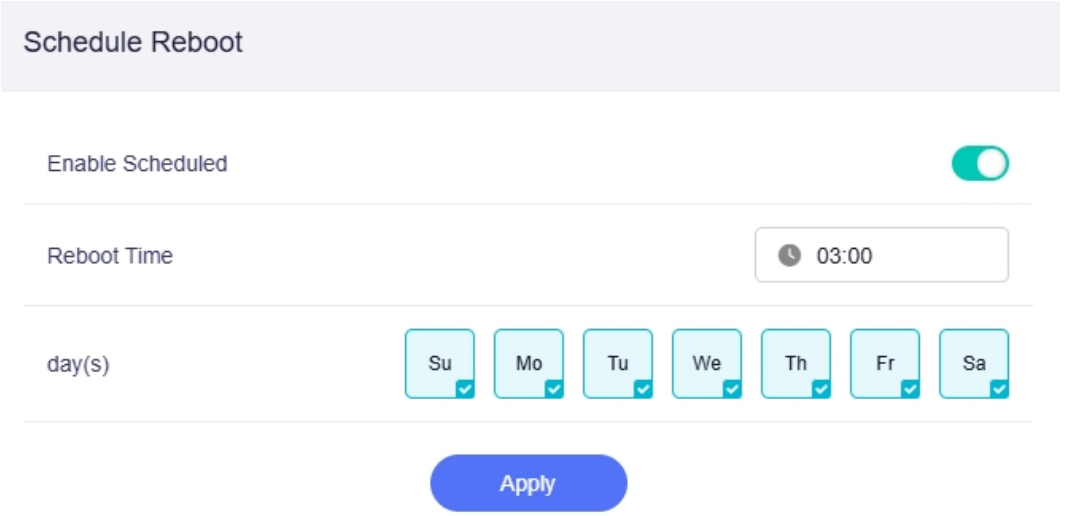


- **Activer la programmation (Enable Scheduled)** : active le planning du voyant.
- **Heure d'allumage (Turn On Time)** : heure d'allumage du voyant, par exemple 07:00.
- **Heure d'extinction (Turn Off Time)** : heure d'extinction du voyant, par exemple 22:00.
- **Jour(s) (day(s))** : jours de la semaine auxquels appliquer ces réglages.

Cliquez ensuite sur **Appliquer (Apply)** pour enregistrer les paramètres.

16.4.2 Redémarrage planifié

Définissez si nécessaire une programmation pour le redémarrage automatique du routeur.



- **Activer la programmation (Enable Scheduled)** : active le redémarrage planifié.
- **Heure de redémarrage (Reboot Time)** : heure à laquelle le routeur redémarre, par exemple 03:00.
- **Jour(s) (day(s))** : jours de la semaine auxquels appliquer ces réglages.

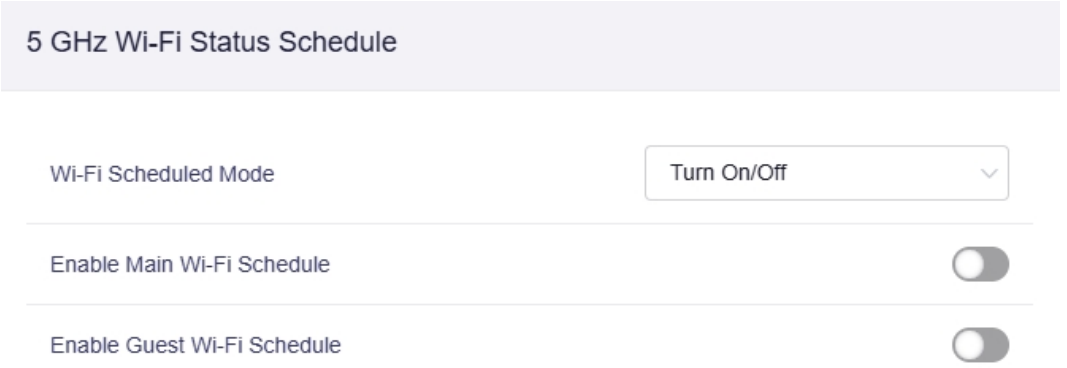
Cliquez ensuite sur **Appliquer (Apply)** pour enregistrer les paramètres.

16.4.3 Programmation du Wi-Fi 5 GHz

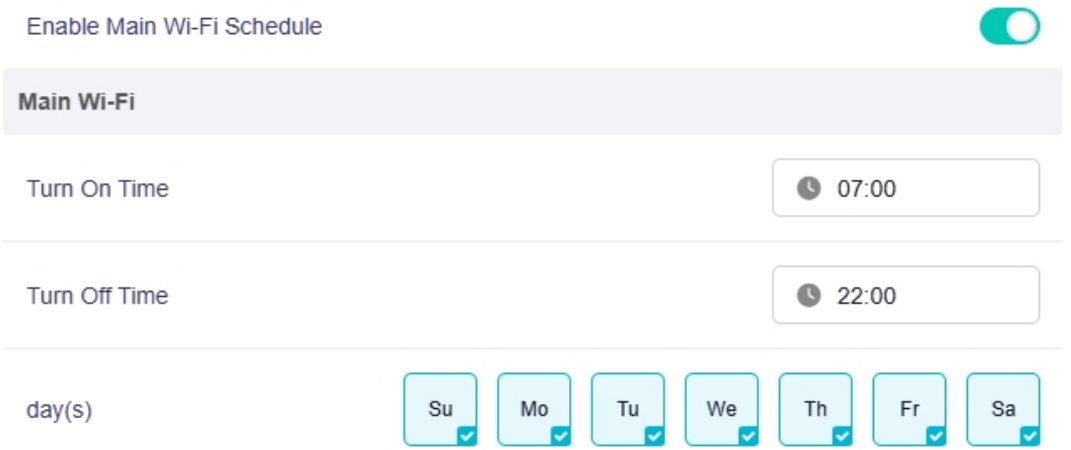
Cette fonction permet de programmer le Wi-Fi 5 GHz. Deux modes sont proposés : Allumer/Éteindre et Modifier la puissance d'émission.

Mode 1 : Allumer/Éteindre

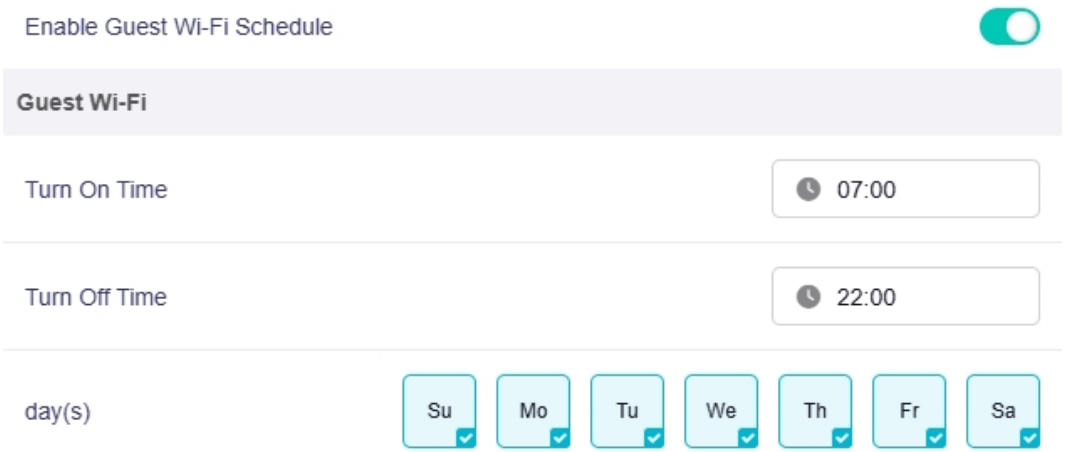
Vous pouvez programmer l'activation et la désactivation des réseaux principal et invité 5 GHz.



- **Programmation du Wi-Fi principal (Main Wi-Fi Schedule)** : une fois activée, définissez les heures d'allumage et d'extinction du réseau principal 5 GHz et les jours concernés.



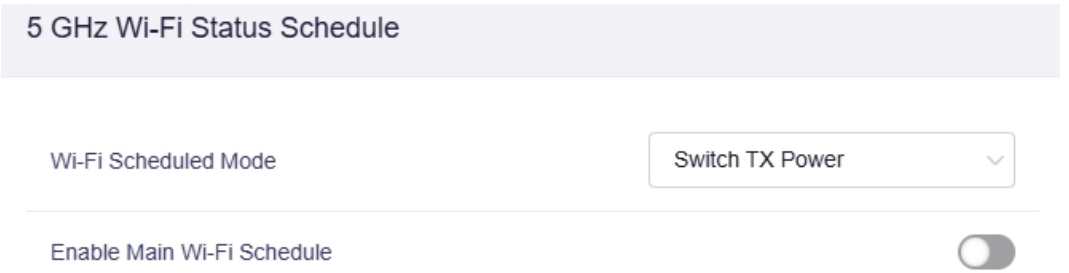
- **Programmation du Wi-Fi invité (Guest Wi-Fi Schedule)** : une fois activée, définissez les heures d'allumage et d'extinction du réseau invité 5 GHz et les jours concernés.



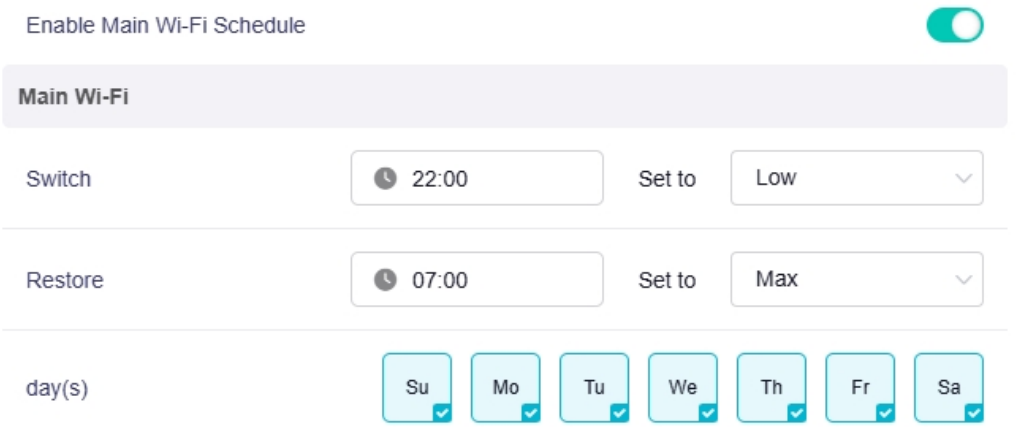
Cliquez ensuite sur **Appliquer (Apply)** pour enregistrer les paramètres.

Mode 2 : Modifier la puissance d’émission

Vous pouvez programmer les changements de puissance d’émission du réseau principal 5 GHz.



Une fois cette fonction activée, définissez deux actions horaires pour modifier la puissance du Wi-Fi principal 5 GHz, puis choisissez les jours concernés.



- **Modifier (Switch)** : applique un niveau de puissance, par exemple Faible, à une heure précise, par exemple 22:00.
- **Rétablir (Restore)** : applique un autre niveau, par exemple Maximum, à une autre heure, par exemple 07:00.
- **Jours (days)** : jours de la semaine auxquels appliquer ces réglages.

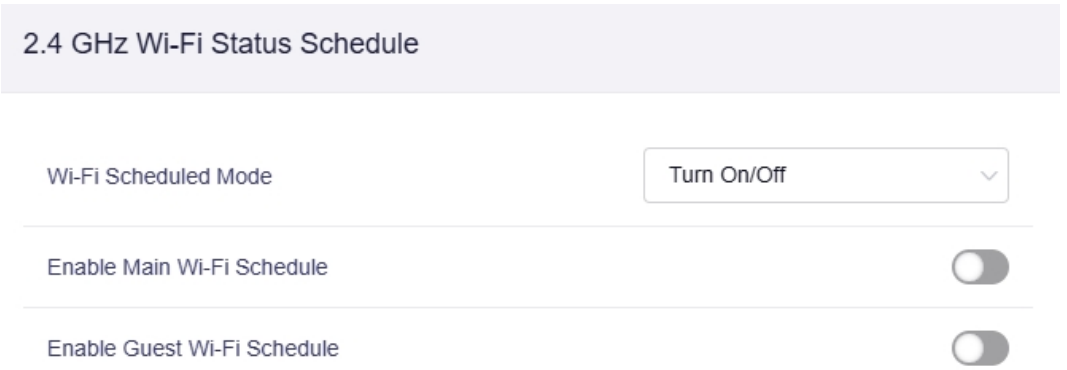
Cliquez ensuite sur **Appliquer (Apply)** pour enregistrer les paramètres.

16.4.4 Programmation du Wi-Fi 2,4 GHz

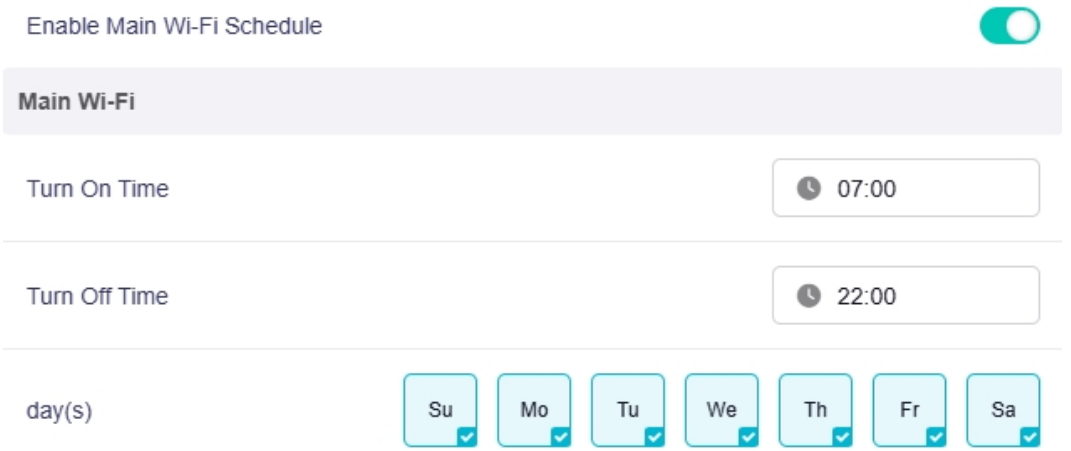
Cette fonction permet de programmer le Wi-Fi 2,4 GHz. Deux modes sont proposés : Allumer/Éteindre et Modifier la puissance d’émission.

Mode 1 : Allumer/Éteindre

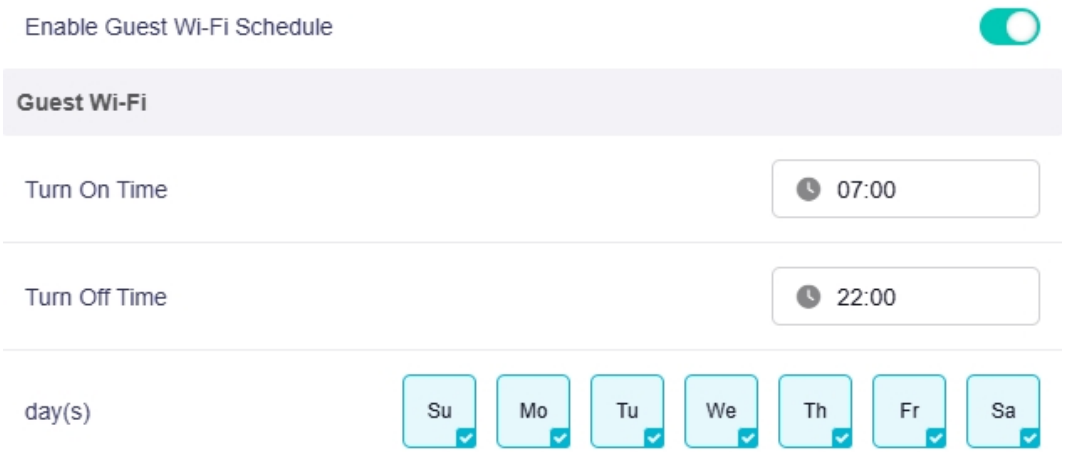
Vous pouvez programmer l’activation et la désactivation des réseaux principal et invité 2,4 GHz.



- **Programmation du Wi-Fi principal (Main Wi-Fi Schedule)** : une fois activée, définissez les heures d’allumage et d’extinction du réseau principal 2,4 GHz et les jours concernés.



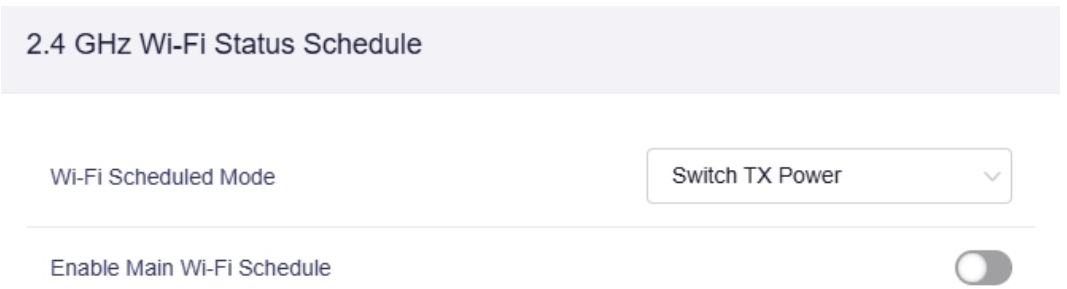
- **Programmation du Wi-Fi invité (Guest Wi-Fi Schedule)** : une fois activée, définissez les heures d’allumage et d’extinction du réseau invité 2,4 GHz et les jours concernés.



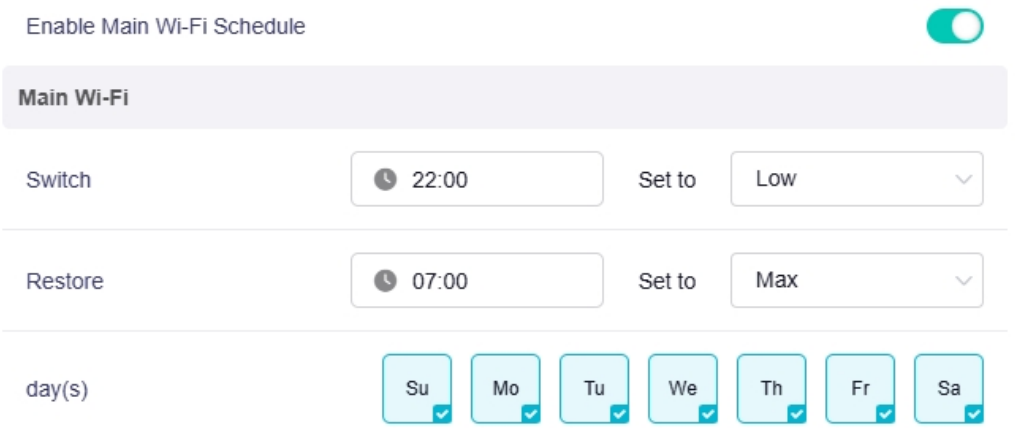
Cliquez ensuite sur **Appliquer (Apply)** pour enregistrer les paramètres.

Mode 2 : Modifier la puissance d'émission

Vous pouvez programmer les changements de puissance d'émission du réseau principal 2,4 GHz.



Une fois cette fonction activée, définissez deux actions horaires pour modifier la puissance du Wi-Fi principal 2,4 GHz, puis choisissez les jours concernés.



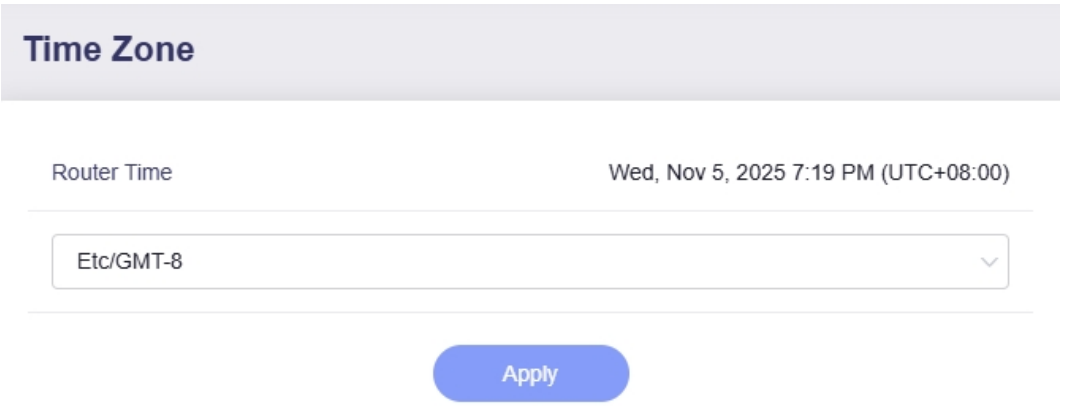
- **Modifier (Switch)** : applique un niveau de puissance, par exemple Faible, à une heure précise, par exemple 22:00.

- **Rétablir (Restore)** : applique un autre niveau, par exemple Maximum, à une autre heure, par exemple 07:00.
- **Jours (days)** : jours de la semaine auxquels appliquer ces réglages.

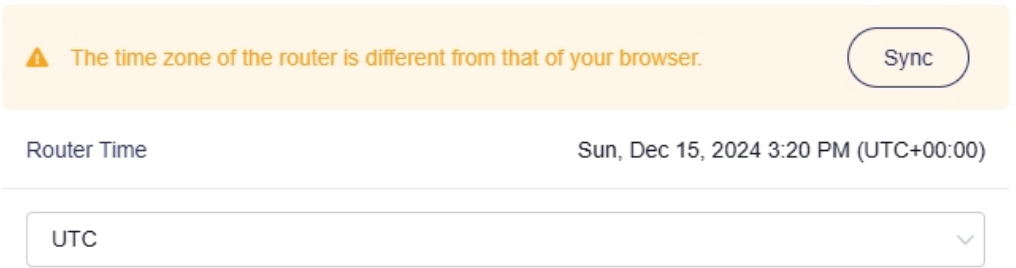
Cliquez ensuite sur **Appliquer (Apply)** pour enregistrer les paramètres.

16.5 Fuseau horaire

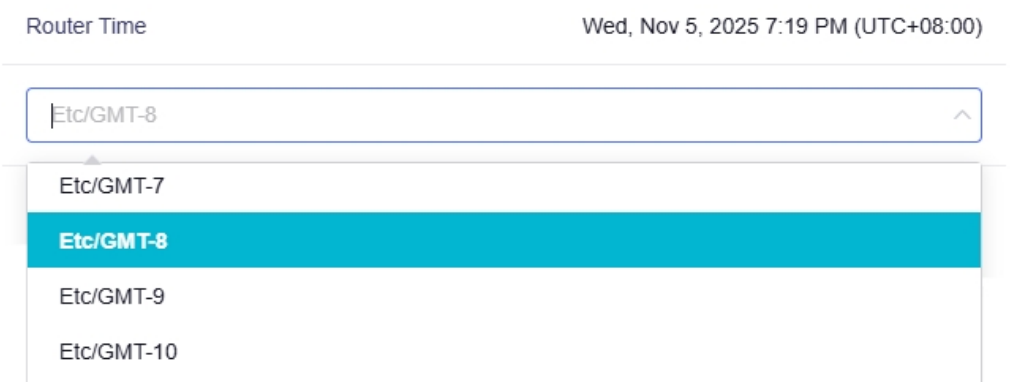
Connectez-vous à l'interface d'administration Web du routeur et ouvrez **SYSTÈME (SYSTEM)** > **Fuseau horaire (Time Zone)**. Cette page affiche l'heure système du routeur, avec la date, l'heure et le décalage du fuseau horaire correspondant.



Certaines fonctions dépendent de l'heure système. Vérifiez que le fuseau horaire est correctement synchronisé. S'il diffère de celui du navigateur, un message s'affiche. Cliquez sur **Synchroniser (Sync)** pour les aligner.



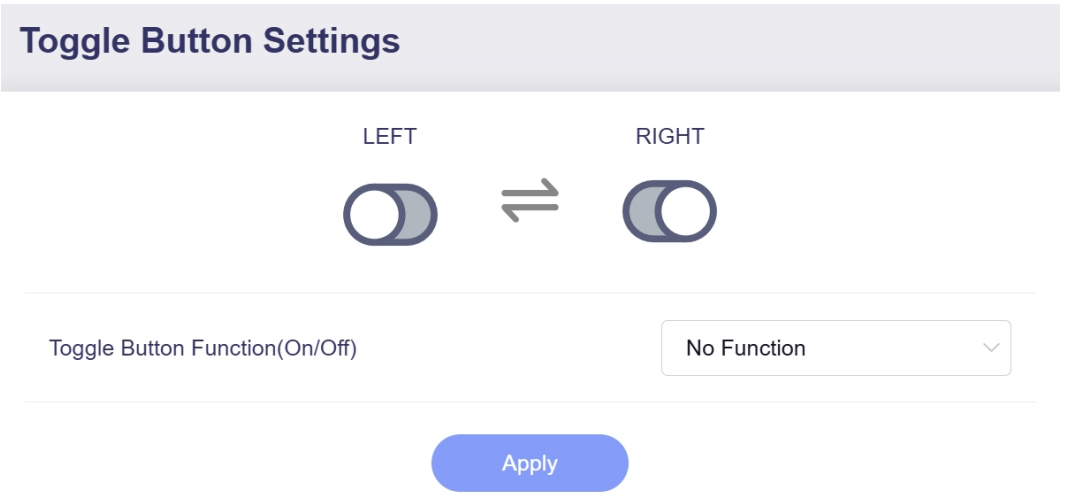
Pour changer de fuseau, sélectionnez celui qui convient dans la liste afin que l'heure du routeur corresponde à l'heure locale.



16.6 Paramètres du commutateur

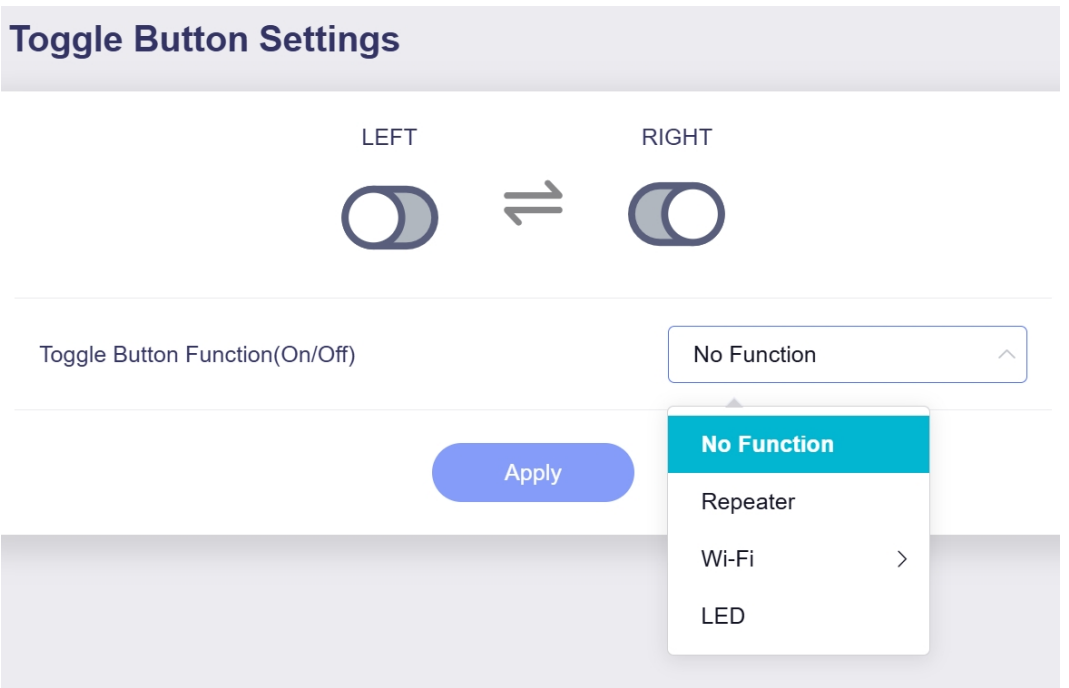
Connectez-vous à l'interface d'administration Web du routeur et ouvrez **SYSTÈME (SYSTEM)** > **Paramètres du commutateur (Toggle Button Settings)**.

Cette page permet de personnaliser la fonction du commutateur physique du routeur, situé sur le côté, pour en faciliter l'utilisation.



Par défaut, aucune fonction n'est attribuée au commutateur. Vous pouvez le personnaliser pour

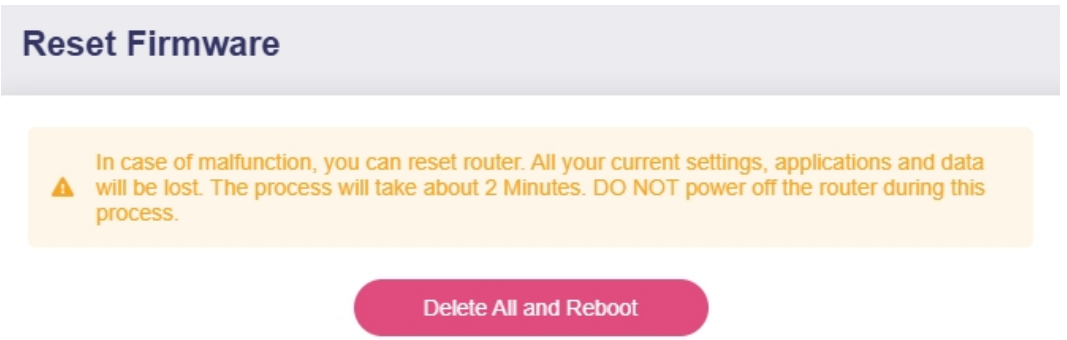
activer ou désactiver certaines fonctions d'un simple geste.



16.7 Réinitialisation du micrologiciel

En cas de dysfonctionnement, vous pouvez essayer de réinitialiser le micrologiciel.

Connectez-vous à l'interface d'administration Web du routeur et ouvrez **SYSTÈME (SYSTEM)** > **Réinitialiser le micrologiciel (Reset Firmware)**. Cliquez sur **Tout supprimer et redémarrer (Delete All and Reboot)** pour réinitialiser le micrologiciel si nécessaire.

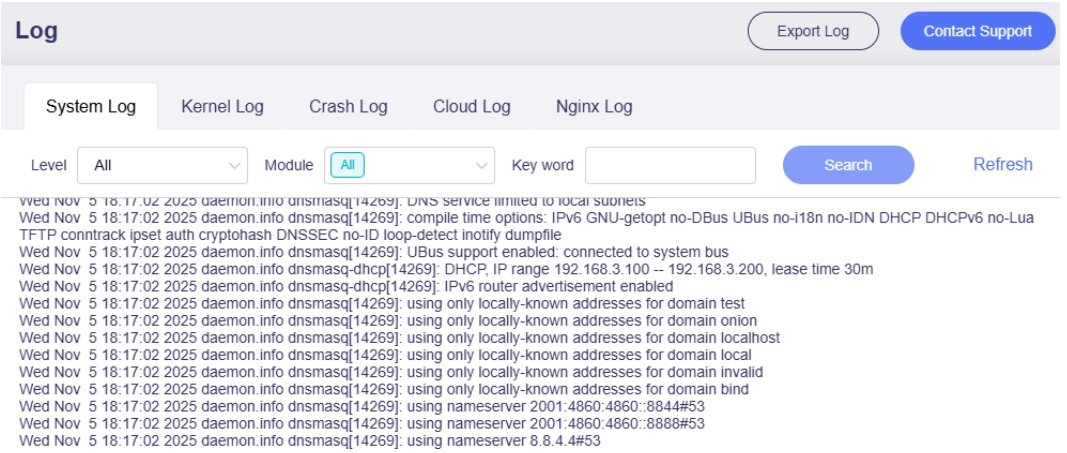


Remarque : tous vos paramètres, applications et données seront effacés. L'opération prend environ 2 minutes. N'éteignez pas le routeur pendant cette opération.

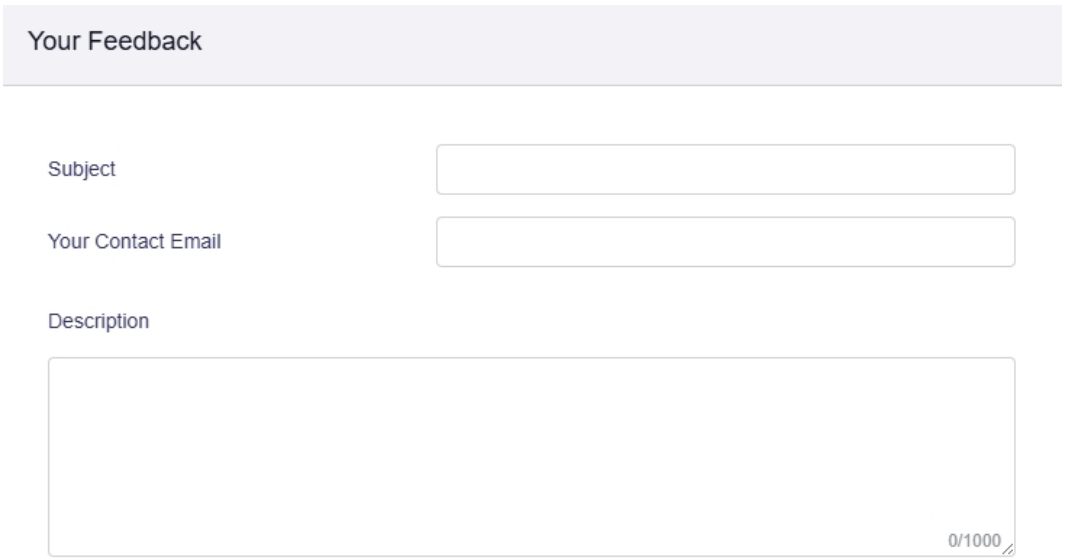
Si vous ne parvenez pas à accéder à l'interface d'administration Web du routeur, essayez de le réinitialiser avec le bouton de réinitialisation situé sur le côté.

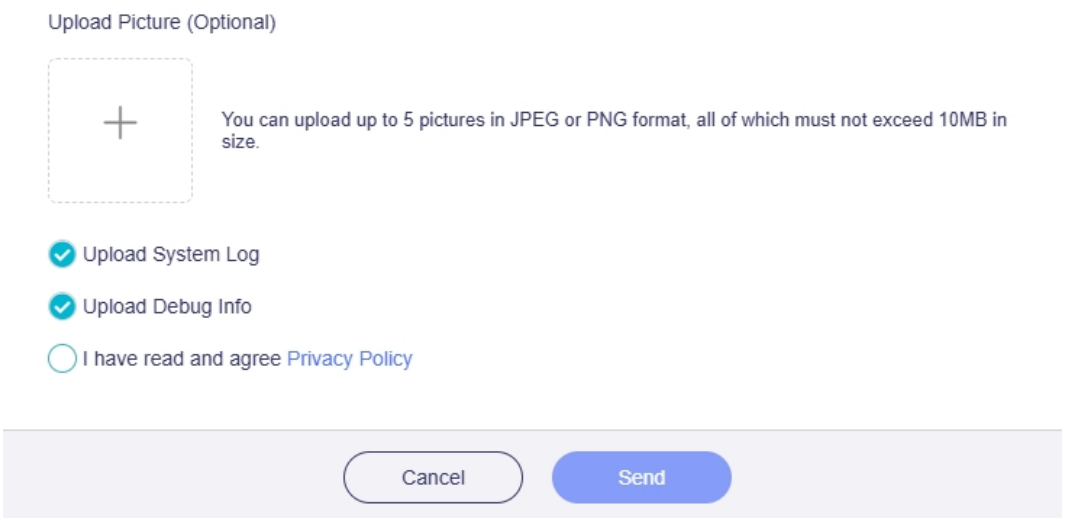
16.8 Journaux

Connectez-vous à l'interface d'administration Web du routeur et ouvrez **SYSTÈME (SYSTEM)** > **Journal (Log)**. Cette page permet de consulter les journaux système, noyau, plantages, cloud et Nginx pour l'analyse et le dépannage. Certains modèles cellulaires compatibles avec les eSIM proposent également un journal eSIM.



- **Recherche (Search)** : filtrez rapidement le journal système par niveau, par exemple Tous, Informations ou Erreur, ou par module, comme IPv6, Partage de connexion ou Cellulaire. Vous pouvez aussi saisir des mots-clés.
- **Actualiser (Refresh)** : met à jour les journaux.
- **Exporter le journal (Export Log)** : exporte les journaux et les informations de débogage.
- **Contacter l'assistance (Contact Support)** : cliquez sur ce bouton, renseignez les détails dans la fenêtre à droite, puis cliquez sur **Envoyer (Send)**. Votre message est transmis directement à l'assistance technique GL.iNet.



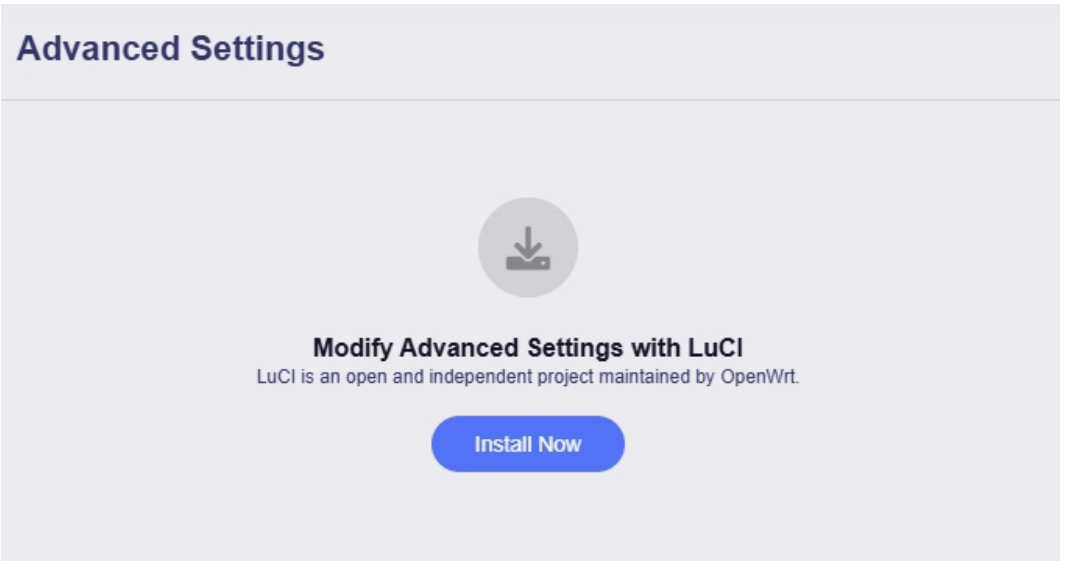

Upload Picture (Optional)
You can upload up to 5 pictures in JPEG or PNG format, all of which must not exceed 10MB in size.
Upload System Log
Upload Debug Info
I have read and agree Privacy Policy
Cancel
Send

16.9 Paramètres avancés

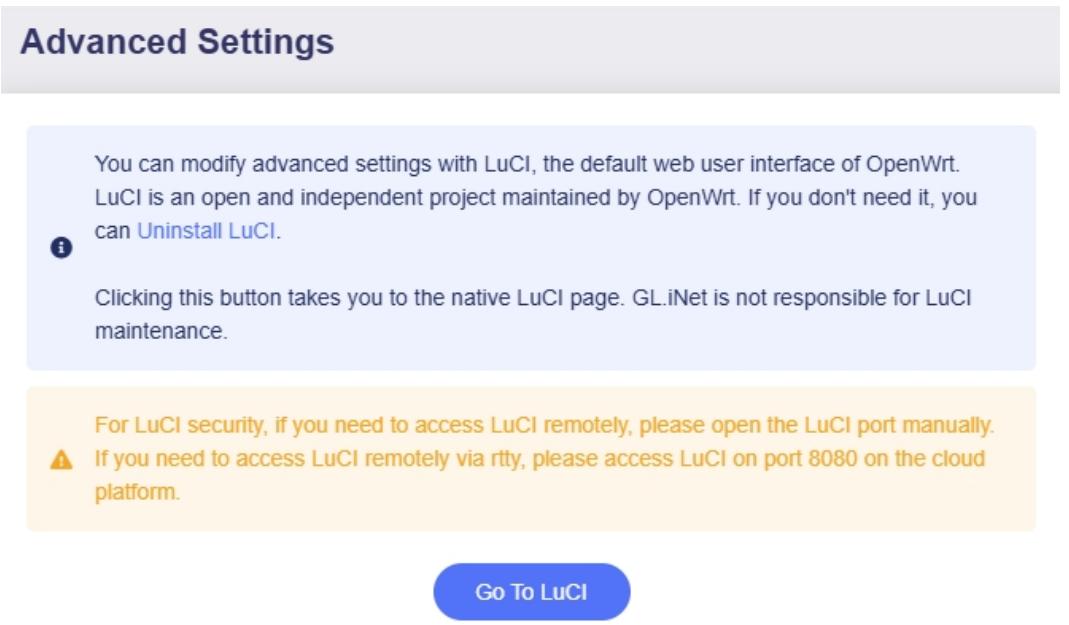
Connectez-vous à l'interface d'administration Web du routeur et ouvrez **SYSTÈME (SYSTEM)** > **Paramètres avancés (Advanced Settings)**. Cette page permet de modifier les paramètres avancés dans LuCI, l'interface Web par défaut d'OpenWrt. LuCI est un projet ouvert et indépendant maintenu par OpenWrt et fourni en l'état. GL.iNet n'assure pas sa maintenance.

Pour vous connecter à LuCI, procédez comme suit.

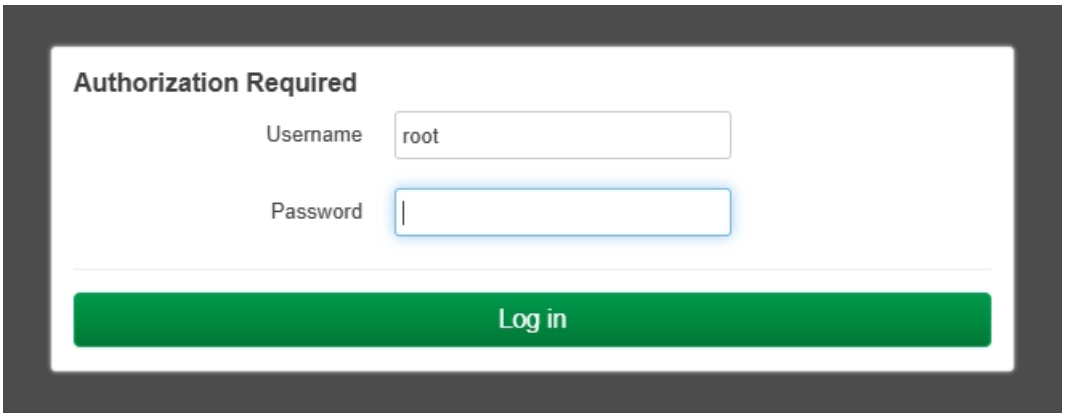
1. Cliquez sur **Installer maintenant (Install Now)** pour installer l'interface LuCI.



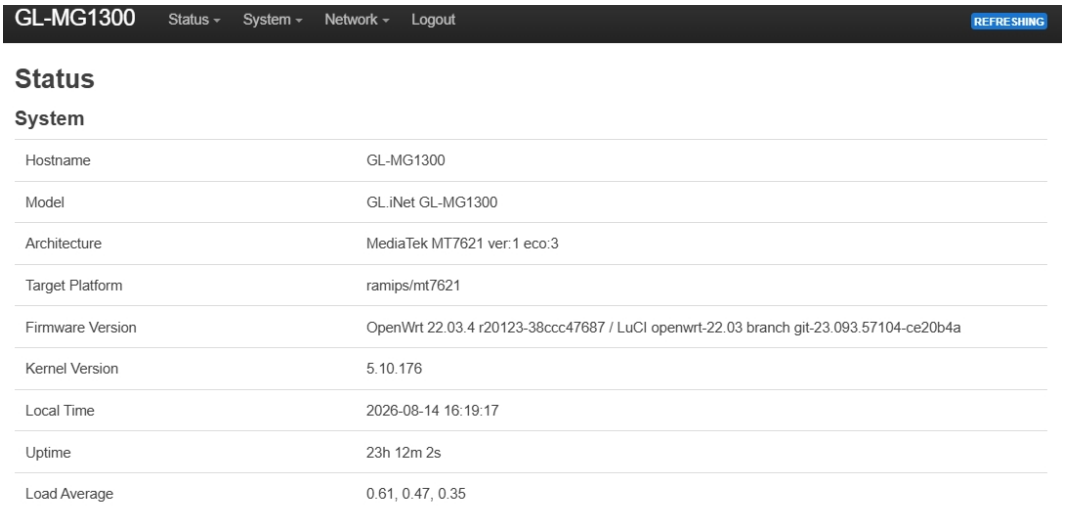
2. Cliquez sur **Accéder à LuCI (Go To LuCI)** pour ouvrir sa page de connexion.



3. Saisissez le mot de passe de connexion, identique à celui de l'interface d'administration Web.



L'interface LuCI s'ouvre.



Déclaration de conformité

Par la présente, GL TECHNOLOGIES (HONG KONG) LIMITED déclare que le type d'équipement radio [Mini routeur de voyage bi-bande, GL-MG1300] est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 2014/53/UE. Le texte intégral de la déclaration de conformité UE est disponible à l'adresse Internet suivante: https://www.gl-inet.com/products/certificate.