GL·iNet



# Manual de usuario

GL-X2000 / Spitz Plus

Enrutador celular Wi-Fi 6 con doble SIM

Versión de firmware 4.7.13

# Acerca de este manual

Este manual es su recurso de referencia para comenzar a usar su dispositivo, y cubre información básica del producto, conexiones de hardware, inicio de sesión en la interfaz de administración web, configuración inicial e instrucciones detalladas para todas las funciones del software en el panel de administración web.

**Con esta guía, podrá**:

- Comprender los detalles clave del producto
- Elegir una ubicación adecuada para el dispositivo
- Completar las conexiones de hardware siguiendo las instrucciones paso a paso
- Iniciar sesión fácilmente en la interfaz de administración web
- Configurar los ajustes iniciales y conocer todas las funciones del software en el panel de administración web

## Convenciones de formato

Estos símbolos y colores le ayudarán a seguir los pasos con mayor rapidez.

| Convención | Qué significa |
|---|---|
| Texto verde azulado subrayado | Enlace en el que se puede hacer clic y que puede abrir una página web o una sección específica |
| Texto en negrita | Enfatiza o marca alguna información clave en este documento, como títulos, hipervínculos y nombres exactos de menú/elementos en la interfaz web del dispositivo |
| > | La ruta para cargar la página correspondiente (p. ej., Sistema > Firmware) |
| Nota | Información clave para configuración, operaciones y seguridad. Ignorar esto podría provocar fallos en la configuración, mal funcionamiento del dispositivo o daños |
| Consejos | Consejos para aprovechar mejor su dispositivo |

**Nota:**

- Las características del dispositivo pueden variar según el modelo y la versión de firmware.
- La disponibilidad del producto está sujeta a diferencias regionales o especificaciones del ISP.
- Todas las imágenes, procedimientos y descripciones de esta guía tienen fines ilustrativos únicamente y pueden diferir de su experiencia de uso real.

## ¿Necesita más ayuda o información?

- Actualización de firmware: Centro de descarga de firmware GL.iNet | Enrutador
- Comunidad: analice nuestros productos y comparta ideas en Foro de la comunidad GL.iNet
- Soporte técnico: comuníquese con nuestro soporte técnico en Página de contacto

**Copyright © 2026 GL.iNet Technology (HK) Ltd. Todos los derechos reservados.**
Ninguna parte de este manual puede reproducirse, transcribirse, traducirse o distribuirse de ninguna forma ni por ningún medio, sin el permiso previo por escrito de GL.iNet Technology (HK) Ltd. GL.iNet es una marca registrada de GL.iNet Technology (Hong Kong) Ltd. en China y/u otros países y regiones. Todas las demás marcas y nombres de productos mencionados aquí son marcas comerciales o marcas comerciales registradas de sus respectivos propietarios.
El contenido de este documento está sujeto a cambios sin previo aviso debido a actualizaciones de versión del producto u otros motivos. A menos que se acuerde lo contrario, este documento se proporciona únicamente con fines informativos y todas las declaraciones, información y recomendaciones contenidas en este documento no constituyen ningún tipo de garantía.

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

# Contenido


Capítulo 1 Conozca su enrutador ..... 6
1.1 Descripción general del producto ..... 7
1.1.1 Apariencia ..... 7
1.1.2 Interfaz y botón ..... 8
1.1.3 LED ..... 9
1.2 Especificaciones ..... 10
1.3 Contenido del paquete ..... 11
Capítulo 2 Conexión de hardware ..... 12
2.1 Elección de una ubicación ..... 13
2.2 Conexión del enrutador ..... 13
Capítulo 3 Iniciar sesión en el enrutador ..... 15
Capítulo 4 Configurar la conexión a Internet ..... 17
4.1 Asistente de configuración rápida ..... 18
4.2 Configurar manualmente la conexión a Internet ..... 19
4.2.1 Conectarse a Internet mediante un cable Ethernet ..... 20
4.2.2 Conectarse a Internet mediante una red Wi-Fi existente ..... 24
4.2.3 Conectarse a Internet mediante conexión compartida por USB ..... 31
4.2.4 Conectarse a Internet mediante la red móvil ..... 36
Capítulo 5 Red inalámbrica ..... 44
5.1 Visualización del estado de Wi-Fi ..... 45
5.2 Configuración inalámbrica ..... 46
5.2.1 Wi-Fi de 5 GHz ..... 46
5.2.2 Wi-Fi de 2,4 GHz ..... 48
Capítulo 6 Clientes ..... 50
6.1 Detalles del dispositivo ..... 52
6.2 Acción ..... 54
6.3 Eliminar clientes ..... 56
6.4 Ordenar ..... 57
Capítulo 7 Servicios en la nube ..... 58
7.1 GoodCloud ..... 59
7.1.1 Habilitar GoodCloud ..... 59
7.1.2 Administrar el enrutador ..... 62

7.1.3 Desvincular el dispositivo ..... 67
7.1.4 Desactivar GoodCloud ..... 67
**Capítulo 8 Conozca la VPN ..... 68**
8.1 Introducción ..... 69
8.2 Escenarios de aplicación ..... 70
**Capítulo 9 Panel de VPN ..... 72**
9.1 Asistente de configuración de VPN ..... 73
9.2 Cliente VPN ..... 76
9.2.1 Opciones del cliente ..... 77
9.2.2 Modo de política ..... 79
9.2.3 Opciones globales ..... 81
9.3 Servidor VPN ..... 84
9.3.1 Opciones del servidor ..... 85
9.3.2 Regla de ruta del servidor ..... 86
9.3.3 Opciones globales ..... 87
**Capítulo 10 Configurar el servidor VPN ..... 88**
10.1 Configurar el servidor OpenVPN ..... 89
10.1.1 Preparación ..... 89
10.1.2 Pasos de configuración ..... 90
10.1.3 Solución de problemas ..... 92
10.2 Configurar el servidor WireGuard ..... 93
10.2.1 Preparación ..... 93
10.2.2 Pasos de configuración ..... 94
10.2.3 Solución de problemas ..... 97
**Capítulo 11 Configurar el cliente VPN ..... 99**
11.1 Configurar el cliente OpenVPN ..... 100
11.1.1 Preparación ..... 100
11.1.2 Configurar NordVPN ..... 100
11.1.3 Configurar el cliente OpenVPN manualmente (para otros proveedores) ..... 106
11.2 Configurar el cliente WireGuard ..... 109
11.2.1 Preparación ..... 109
11.2.2 Configurar AzireVPN ..... 110
11.2.3 Configurar Hide.me ..... 114
11.2.4 Configurar IPVanish ..... 117

11.2.5 Configurar Mullvad ..... 121
11.2.6 Configurar NordVPN ..... 125
11.2.7 Configurar PIA (Private Internet Access) ..... 130
11.2.8 Configurar Surfshark ..... 134
11.2.9 Configurar el cliente WireGuard manualmente (para otros proveedores) ..... 138
**Capítulo 12 Aplicaciones ..... 143**
12.1 Complementos ..... 144
12.2 DNS dinámico ..... 145
12.2.1 Habilitar DDNS ..... 145
12.2.2 Comprobar si DDNS funciona ..... 148
12.2.3 Acceso remoto HTTPS ..... 150
12.2.4 Acceso remoto SSH ..... 152
12.3 Almacenamiento en red ..... 154
12.3.1 Conectar una unidad de almacenamiento ..... 154
12.3.2 Configurar Samba ..... 155
12.3.3 Configurar WebDAV ..... 158
12.3.4 Configurar DLNA ..... 161
12.4 AdGuard Home ..... 162
12.5 Control parental ..... 164
12.5.1 Configuración rápida ..... 164
12.5.2 Solución de problemas ..... 172
12.6 Tailscale ..... 173
12.6.1 Configurar Tailscale ..... 174
12.6.2 Permitir el acceso remoto a la WAN ..... 177
12.6.3 Permitir el acceso remoto a la LAN ..... 178
12.6.4 Nodos de salida personalizados ..... 179
12.7 Gestión de eSIM ..... 181
12.7.1 Estado actual de la eSIM ..... 182
12.7.2 Lista de perfiles eSIM ..... 183
**Capítulo 13 Red ..... 190**
13.1 Reenvío de puertos ..... 191
13.1.1 DMZ ..... 191
13.1.2 Reenvío de puertos ..... 193
13.2 Multi-WAN ..... 195

13.2.1 Seguimiento del estado de la interfaz ..... 195
13.2.2 Modo Multi-WAN ..... 198
13.3 LAN ..... 201
13.3.1 Configuración básica ..... 201
13.3.2 Servidor DHCP ..... 202
13.3.3 Reserva de direcciones ..... 204
13.4 Red de invitados ..... 205
13.4.1 Configuración básica ..... 205
13.4.2 Servidor DHCP ..... 206
13.5 DNS ..... 208
13.5.1 Configuración del servidor DNS ..... 210
13.5.2 Editar hosts ..... 212
13.6 Gestión de puertos ..... 213
13.7 Modo de red ..... 214
13.8 IPv6 ..... 217
13.8.1 Modo IPv6 ..... 218
13.8.2 Método de obtención de DNS ..... 218
13.9 Puerta de enlace directa ..... 219
13.10 Inspección IGMP ..... 221
13.11 Aceleración de red ..... 222
13.12 Configuración NAT ..... 223
13.12.1 NAT de cono completo ..... 223
13.12.2 ALG SIP ..... 224
**Capítulo 14 Sistema ..... 225**
14.1 Descripción general ..... 226
14.2 Actualización ..... 227
14.2.1 Actualización de firmware ..... 227
14.2.2 Actualización de módem ..... 230
14.3 Tareas programadas ..... 231
14.3.1 Programación de los indicadores LED ..... 231
14.3.2 Programar reinicio ..... 232
14.3.5 Programación de Wi-Fi de 5 GHz ..... 232
14.3.6 Programación de Wi-Fi de 2,4 GHz ..... 234
14.4 Zona horaria ..... 237

14.5 Registro ..... 238
14.6 Seguridad ..... 240
14.6.1 Contraseña de administrador ..... 240
14.6.2 Control de acceso ..... 241
14.6.3 Control de acceso remoto ..... 244
14.6.4 Abrir puertos en el enrutador ..... 245
14.7 Restablecer firmware ..... 247
14.8 Configuración avanzada ..... 248

Capítulo 1

# Conozca su enrutador

Este capítulo cubre la descripción general, las especificaciones y el contenido del paquete del enrutador.

## 1.1 Descripción general del producto

Spitz Plus (GL-X2000) es una puerta de enlace celular Wi-Fi 6 4G LTE de doble SIM diseñada para proporcionar conexiones rápidas y confiables, especialmente en áreas remotas y durante viajes por carretera. Con agregación de 3 operadores, el enrutador transmite datos en tres bandas de operadores simultáneamente, proporcionando 3 veces el ancho de banda disponible para evitar la congestión. Ofrece cuatro métodos de acceso a Internet: Celular (tarjetas SIM), ethernet, repetidor y anclaje a red. Admite múltiples WAN (conmutación por error y equilibrio de carga), VPN (OpenVPN y WireGuard), controles parentales, AdGuard Home, reenvío de puertos, Tailscale y más.

### 1.1.1 Apariencia

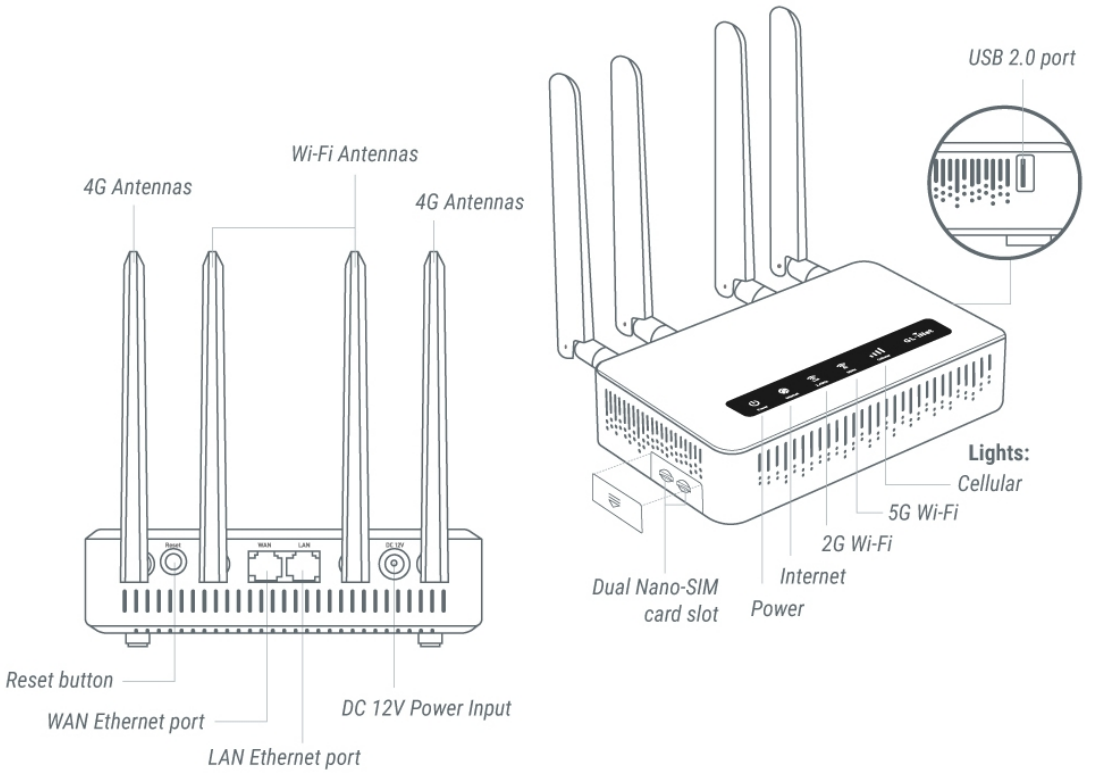









## 1.1.2 Interfaz y botón




| Artículo | Descripción |
|---|---|
| Entrada de alimentación de 12 V CC | Se conecta al adaptador de corriente. |
| Puerto Ethernet WAN | Se conecta a un módem o a una toma Ethernet para Internet. |
| Puerto LAN Ethernet | Se conecta a dispositivos cableados si es necesario. |
| Puerto USB 2.0 | Para dispositivos de almacenamiento USB, conexión USB de teléfono y<br>dongles celulares compatibles. |
| Antenas Wi-Fi | Para transmisión y recepción de señal Wi-Fi de doble banda de 2,4 GHz y 5 GHz. |
| Antenas 4G | Para transmisión y recepción de señal de red celular 4G LTE. |
| Ranura para tarjeta Nano-SIM dual | Para insertar dos tarjetas Nano-SIM. Solo puede haber una SIM activa a la vez. |

| | |
|---|---|
| Botón Restablecer | Presione y mantenga presionado durante **3 segundos** y luego suelte para reparar su red. |
| | Mantenga presionado durante **8 segundos** y luego suelte para restablecer el enrutador a los valores predeterminados de fábrica. |

### 1.1.3 LED

| **Estado de condición** | **Alimentación** | **Internet** | **2.4Ghz** | **5Ghz** | **Celular** |
|---|---|---|---|---|---|
| Normal (conectado a Internet) | Verde | Verde | Verde | Verde | Verde |
| No conectado a Internet | Verde | Desactivado | Verde | Verde | Verde |
| Actualizando firmware | Verde | Verde parpadeante (cada 0,5 s) | Verde parpadeante (cada 0,5 s) | Verde parpadeante (cada 0,5 s) | Verde |
| Restableciendo el enrutador (mantenga presionado el botón "reset" durante > 3 segundos) | Parpadea en verde (cada 1 segundo) | Verde | Verde | Verde | Verde |
| Restaurando el enrutador a la configuración de fábrica (mantenga presionado el botón "reset" durante 10 segundos) | Parpadeo rápido en verde (cada 0,25 s) | Verde | Verde | Verde | Verde |

## 1.2 Especificaciones

| | |
|---|---|
| Interfaz | 1 x puerto Ethernet WAN<br>1 x puerto LAN Ethernet<br>1 x puerto USB 2.0<br>2 x ranuras para tarjetas Nano SIM<br>1 x botón Restablecer |
| CPU | Qualcomm de doble núcleo, @1GHz |
| Memoria/Almacenamiento | DDR3L 512 MB / NAND Flash 128 MB |
| Protocolo | IEEE 802.11a/b/g/n/ac/ax |
| Velocidad de Wi-Fi | 574Mbps (2,4 GHz), 2402 Mbps (5 GHz) |
| Velocidad de Ethernet | 10/100/1000Mbps |
| Antenas | 2 x antenas celulares (SMA, 600M~3.8GHz)<br>2 x antenas Wi-Fi (PR-SMA, 2,4G~2,5GHz, 5,15~5,84GHz) |
| LED | Alimentación / Internet / Wi-Fi 2.4G / Wi-Fi 5G / Intensidad de la señal celular |
| Entrada de energía | DC5521, 12V/2.5A (5.5*2.1mm) [adaptador predeterminado] / 9V~36V |
| Consumo de energía | < 14W |
| Temperatura de funcionamiento | 0 ~ 40°C (32 ~ 104°F) |
| Temperatura de almacenamiento | -20 ~ 70°C (-4 ~ 158°F) |
| Dimensión/Peso | 141 x 86 x 36 mm / 443 g |
| Otras herramientas | Hoja de datos / Firmware / Aplicación / Unboxing / Tutoriales / Kit de medios |

*Las velocidades inalámbricas se basan en los estándares IEEE 802.11 (por ejemplo, 802.11ax para Wi-Fi 6). El rendimiento y el alcance reales pueden ser inferiores debido a obstáculos ambientales (paredes, metal), congestión de la red o capacidades del dispositivo cliente.

*El uso de Wi-Fi 6 (802.11ax) y sus funciones (OFDMA, MU-MIMO, 1024-QAM) requiere que los dispositivos cliente admitan las tecnologías correspondientes.

## 1.3 Contenido del paquete

El paquete incluye:

- 1 x Spitz Plus (GL-X2000)
- 1 manual de usuario
- 4 x antenas externas
- 1 x Tarjeta de agradecimiento
- 1 cable Ethernet
- 1 x kit de montaje en pared
- 1 x almohadilla adhesiva
- 1 x adaptador de corriente
- 1 x convertidor (según su país de envío)



1 x User manual



1 x Thank you card


1 x RJ45 Ethernet cable


1 x Power adapter (1.8 meters)


4 x External antennas


1 x Wall mount kit


1 x Adhesive pad


1 x Spitz Plus (GL-X2000)


Converters
* EU, UK & AU Plug for Quectel EG120K-EA Module
* US Plug for Quectel EG120K-NA Module

Capítulo 2

# Conexión de hardware

Este capítulo cubre la selección de la ubicación del enrutador y los pasos de conexiónion.

## 2.1 Elección de una ubicación

Siga estos consejos para elegir ubicación para obtener el mejor rendimiento.

- **Evite la humedad y el calor**t: No coloque el enrutador en áreas expuestas al agua, humedad o altas temperaturas (por ejemplo, fregaderos, radiadores).
- **Ventilación y fríoing**: Colocar el router en un- área fresca y bien ventilada para una adecuada disipación del calor.
- **Ubicación central**: coloque el enrutador donde pueda conectarse a la alimentación y a varios dispositivos fácilmente (por ejemplo, la zona).
- **Cable conveniencia**: coloque los cables y el cable de alimentación de forma segura para evitar riesgos de tropiezos.
- **Ubicación**: coloque el enrutador en una superficie plana y estable (estante, escritorio) o móntelo en la pared usando el kit de montaje en pared incluido.
- **Evitación de EMI**: mantenga el enrutador alejado de fuentes de interferencia electromagnética (dispositivos Bluetooth, microondas) para minimizar la interferencia de la señal.

## 2.2 Conexión del enrutador

1. **Encendido**

   Junte el adaptador de corriente de dos piezas. Conéctelo al enrutador y conéctelo a una toma de corriente. Se iniciará automáticamente.

2. **Conecte un dispositivo al enrutador**

   Conecte un dispositivo (por ejemplo, una computadora portátil o un teléfono inteligente) al enrutador mediante Wi-Fi o un cable Ethernet.

   - **Wi-Fi**: En su dispositivo, vaya a Configuración > WLAN, busque el nombre de la red Wi-Fi del enrutador en la lista de redes disponibles e ingrese la contraseña. Puede encontrar el nombre de red predeterminado y la contraseña impresos en la etiqueta de su enrutador’nombre de la red Wi-Fi en la lista de redes disponibles e ingrese la contraseña. Puede encontrar el nombre de red predeterminado y la contraseña impresos en su enrutador’.
   - **Ethernet**: Conecte su dispositivo al puerto LAN del enrutador’a través de un cable Ethernet.

3. **Inicie sesión en enrutador**

El Internet está nodisponible cuando se conecta al enrutador por primera vez. Inicie sesión en el enrutador como se indica en el Capítulo 3 para completar la configuración inicial antes de accedering a Internet.

Capítulo 3

# Iniciar sesión en el enrutador

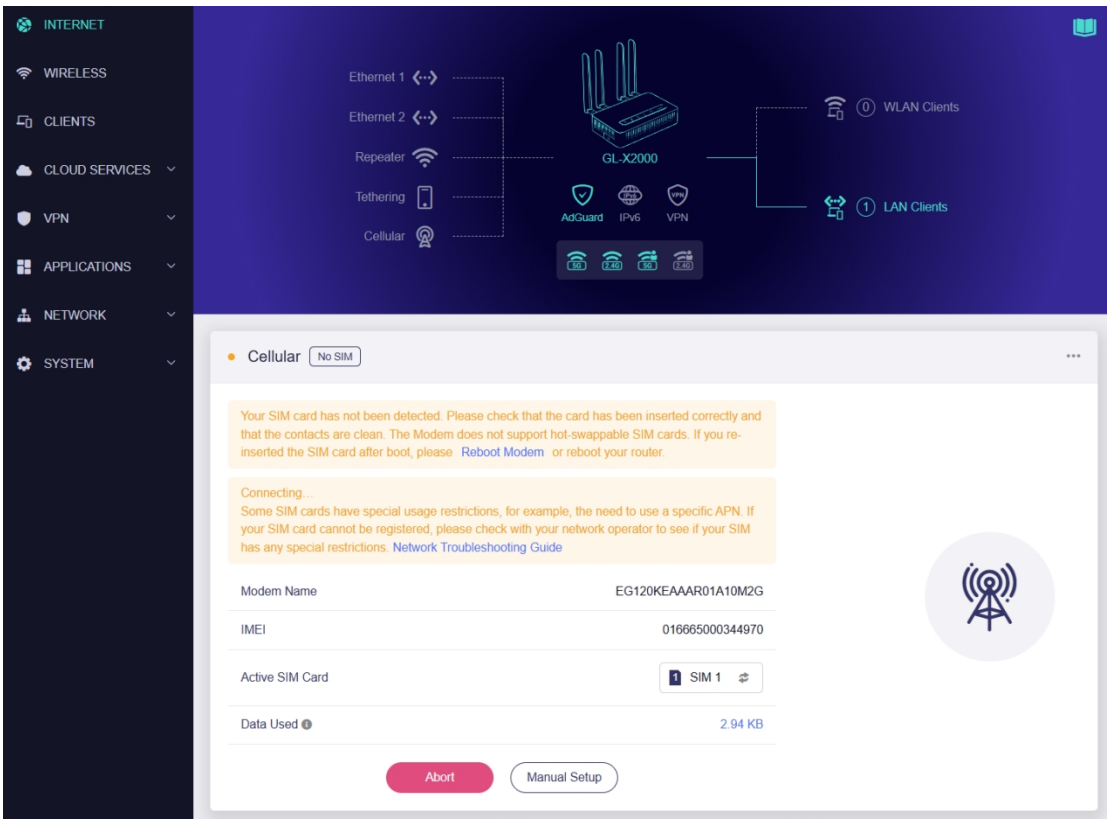
Este capítulo lo guía para iniciar sesión en su enrutador a través del panel de administración web.

Configure y administre su enrutador a través de una interfaz de administración basada en webement, a la que se puede acceder desde cualquier sistema operativo Windows, Mac o Linux con wnavegador eb, como Microsoft Edge, Google Chrome, Mozilla Firefox o Apple Safari.

**Nota**: Si prefiere nosotrosing la aplicación GL.iNet en lugar de la web admin panel, descarga la aplicación y sigue las indicaciones en pantalla.

**Sigue los pasos a continuación para iniciar sesión in a su enrutador a través del panel de administración web**.

1. Conecte un dispositivo (por ejemplo, una computadora o computadora portátil) al enrutador mediante Wi-Fi o un cable Ethernet.
2. Abra un navegador web (Chrome y Edge) y visite http://192.168.8.1. Serás dirigido a la página de inicio de sesión de la web admin panel. Si no puede acceder a la web undmin panel, consulte aquí para solucionar problemas.
3. Sconfigure su contraseña de administrador. Se recomienda una contraseña segura por motivos de seguridad. Luego haga clic en **Siguiente** para continuar.
4. Yluego ingresará el enrutador's web admin panel.



Capítulo 4

# Configurar la conexión a Internet

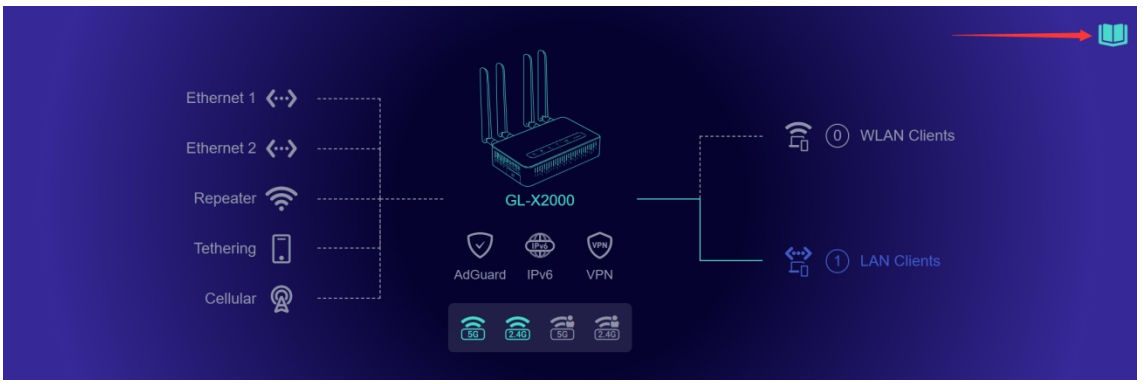
Este capítulo presenta múltiples métodos de conexión a Internet para que el enrutador se adapte a diversos entornos de red.

## 4.1 Asistente de configuración rápida

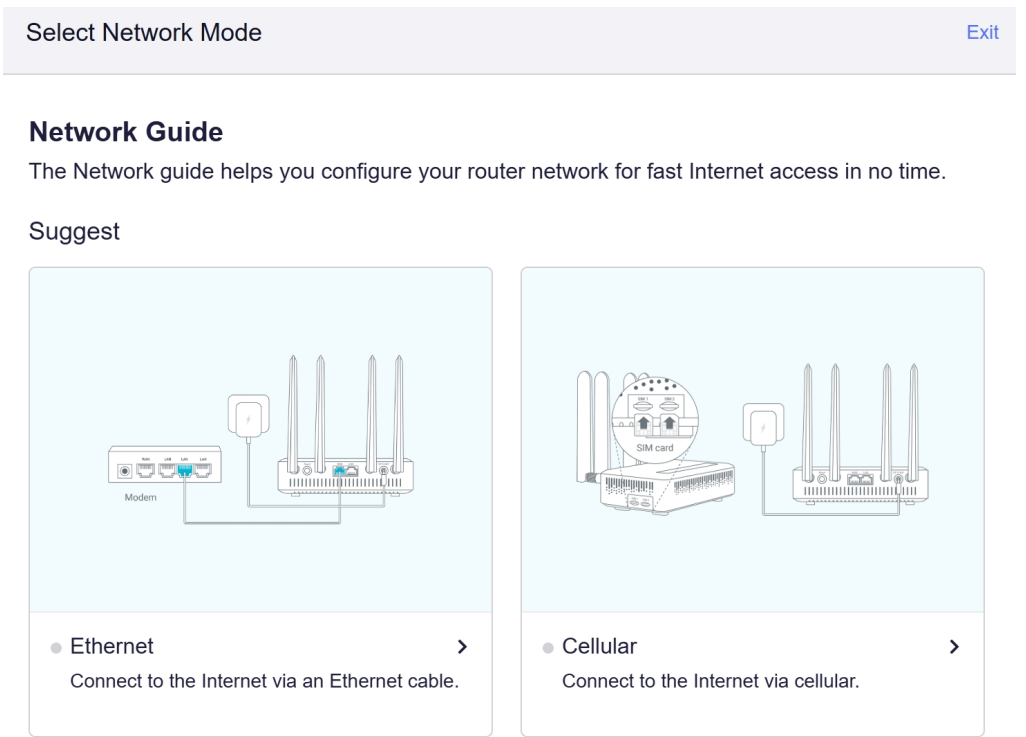
El asistente de configuración basado en web lo guiará a través de la configuración de red del enrutador.

Siga los pasos a continuación para iniciar el asistente.

1. Inicie sesión en el panel de administración web del enrutador’como se indica en el Capítulo 3.
2. En la casapágina, haga clic en el ícono del libro en la esquina superior derecha.




3. Fsiga el Asistente de configuración para configurar su enrutador y establezca una conexión a Internet.




Si utiliza el aplicación GL.iNet, siga las instrucciones en pantallas para configurar internet acceso.

## 4.2 Configurar manualmente la conexión a Internet

Si bien el asistente de configuración es conveniente para una configuración rápida de la red, la configuración manual le permite ajustar la configuración avanzada de la red para requisitos específicos y verificar o modificar las conexiones existentes si es necesario.

Spitz Plus admite cuatro métodos de conexión a Internet: Ethernet, Repetidor, Anclaje a red USB y módem USB. Celija el método apropiado según sus necesidades de uso.

1. **Etherne (RJ45)t**: conecte el enrutador a una red de banda ancha usando unn Ethernet conectado al puerto WAN. El enrutador normalmente obtiene una dirección IP automáticamente a través de DHCP. Los usuarios pueden también manualmente configurar una IP estática o configuración PPPoE. Este método ofrece alta estabilidad y alta velocidad, lo que lo hace ideal para entornos domésticos y de oficina con acceso de banda ancha fija.

2. **Repetidor (Repeater)**: este modo habilitas el enrutador a conéctese a una red Wi-Fi existente para ampliar la señal Wi-Fi y crear una red local separada y segura. Tenga en cuenta que las velocidades de transmisión pueden reducirse hasta cierto punto. Es ideal para zonas muertas de Wi-Fi que requieren extensión de señal o lugares públicos donde se necesita seguridad de red mejorada.

3. **Anclaje a red USB (USB Tethering)**: conecte un teléfono inteligente u otro dispositivo compatible al enrutador mediante un cable USB para compartir la conexión de datos móviles del dispositivo (por ejemplo, 4G/5G) con el enrutador. Esta es una solución conveniente para el acceso temporal a Internet, especialmente en exteriores o en áreas sin banda ancha fija.

4. **Celular**: inserte una o dos tarjetas Nano-SIM en la ranura para SIM dual integrada-del enrutador. Luego, el enrutador se conectará a Internet a través de redes móviles 4G, proporcionando conectividad independiente de la banda ancha de línea fija. Este método ofrece alta movilidad y es adecuado para situaciones como el uso en vehículos o actividades al aire libre. Cuando se insertan dos tarjetas SIM, solo una tarjeta SIM puede estar activa a la vez.

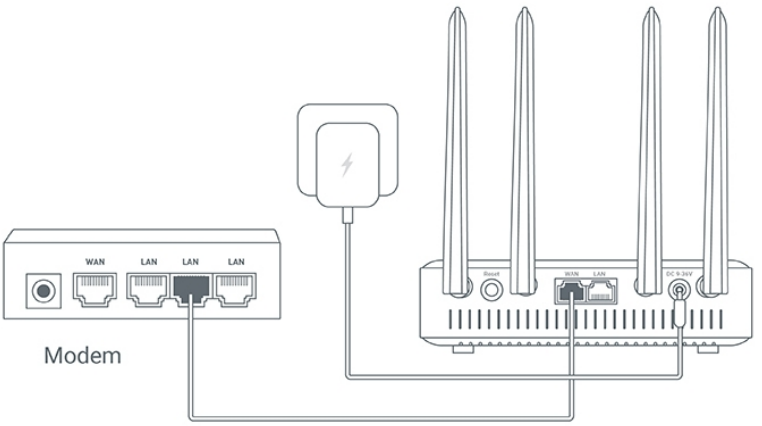
## 4.2.1 Conectarse a Internet mediante un cable Ethernet

Conecte el enrutador a una red de banda ancha usando unn cable Ethernet conectado al puerto WAN. El enrutador normalmente obtiene una dirección IP automáticamente a través de DHCP. Los usuarios pueden también manualmente configurar una IP estática o configuración PPPoE. Este método ofrece alta estabilidad y alta velocidad, lo que lo hace ideal para entornos domésticos y de oficina con acceso de banda ancha fija.

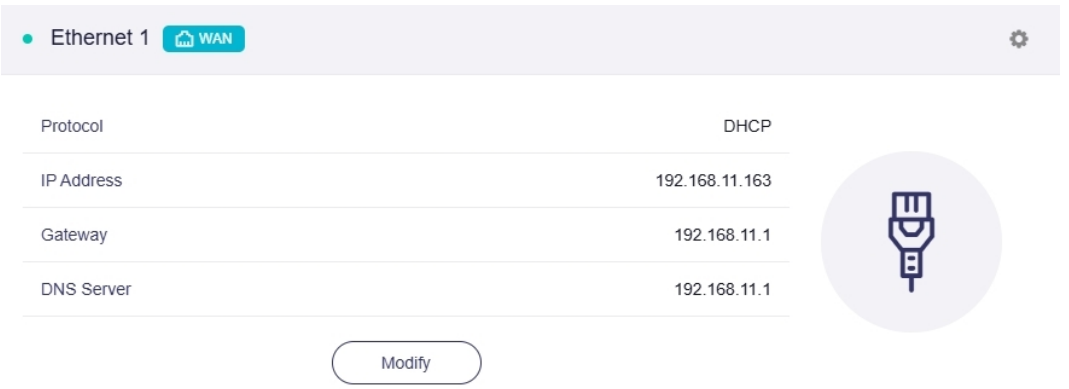
## Configuración básica

Siga los pasos a continuación para conectar su enrutador a Internet mediante un cable Ethernet.

1. Conecte el puerto **WAN** de su enrutador al el dispositivo ascendente (por ejemplo, un módem ISP, un enrutador principal, un conmutador de red o un conector Ethernet) a través de un Ethernet cable.

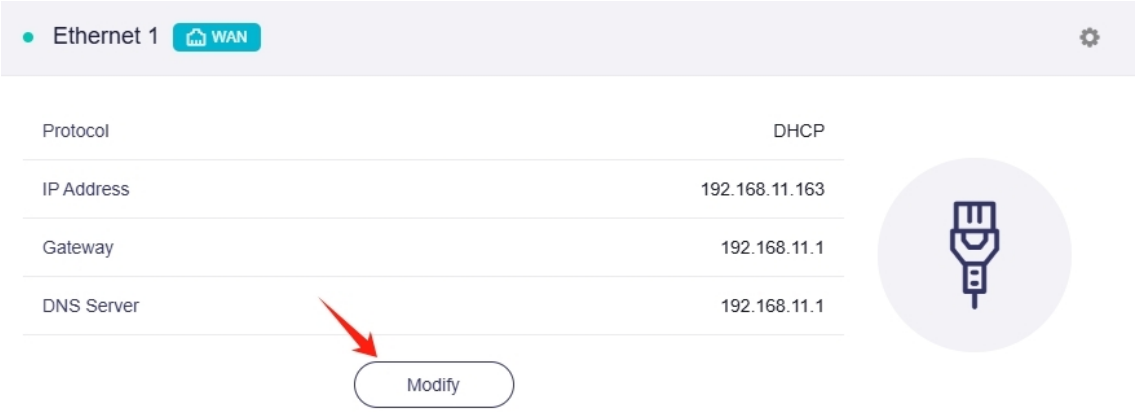



2. Inicie sesión en el enrutador’panel de administración web y navegue a **INTERNET** > **Ethernet**. Si la conexión se realiza correctamente, la sección Ethernet mostrará red detalles, incluidos protocolo, dirección IP, puerta de enlace, y DNS servidor.



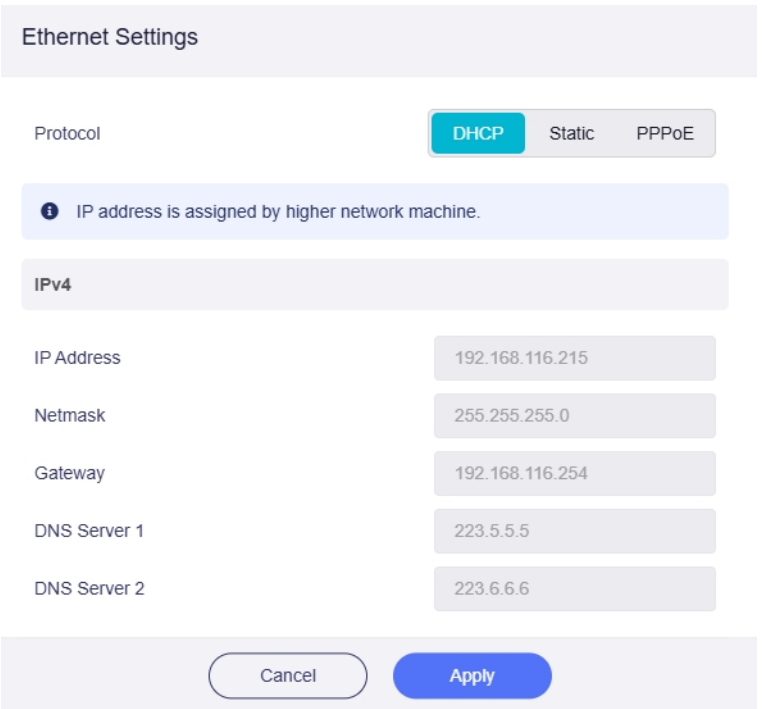
## Protocolo

Hay tres tipos de protocolos: DHCP, Estático y PPPoE. Haga clic en **Modificar** para cambiar.



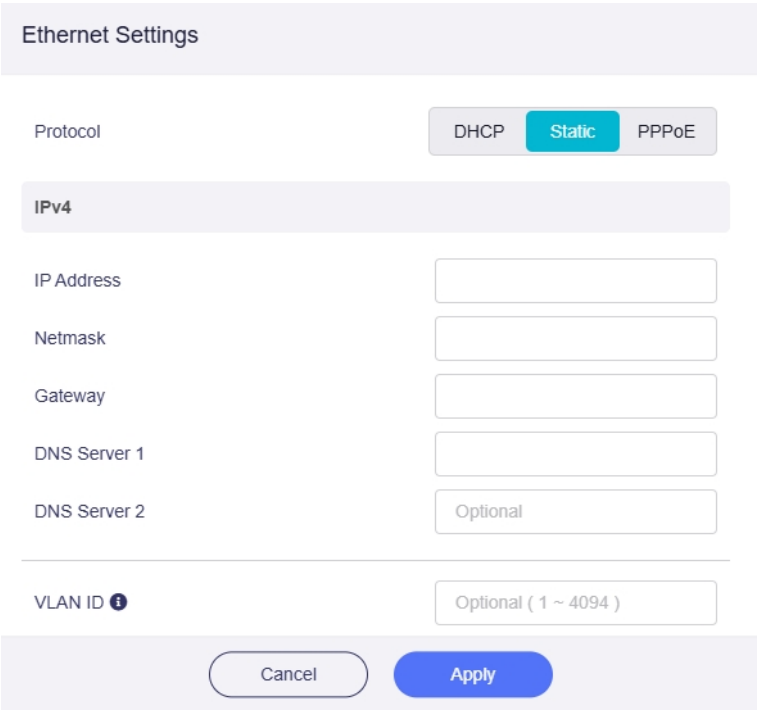

- **DHCP**

  DHCP es el protocolo de red predeterminado y más común, que asigna automáticamente direcciones IP y otros parámetros de configuración de red a dispositivos en una red IP a través de un modelo cliente-servidor.



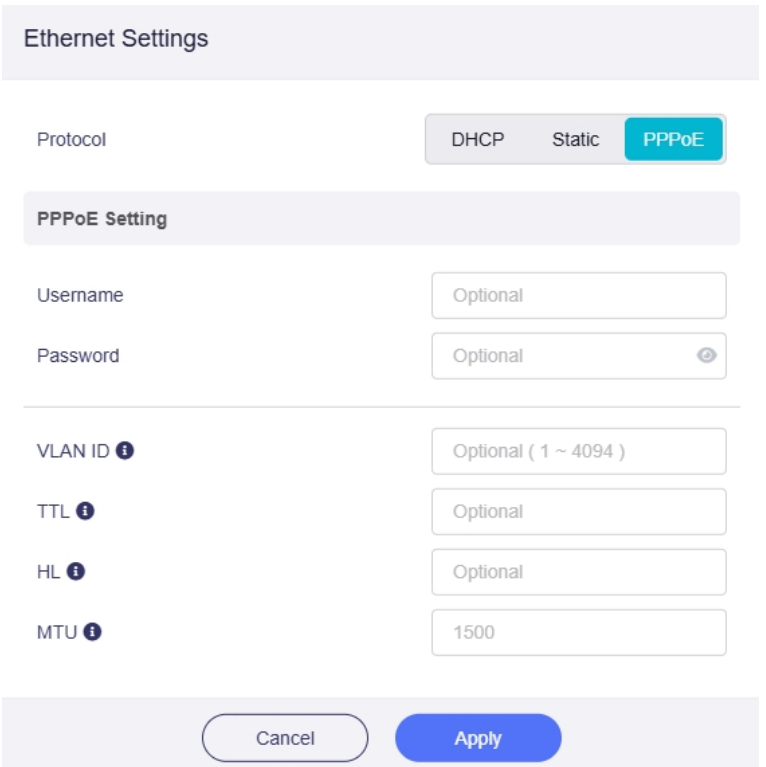

- **Estática**

  Se requiere una dirección IP estática si su ISP (proveedor de servicios de Internet) asigna una dirección IP pública fija o si necesita configurar manualmente los parámetros de red (por ejemplo, dirección IP, puerta de enlace, máscara de subred).



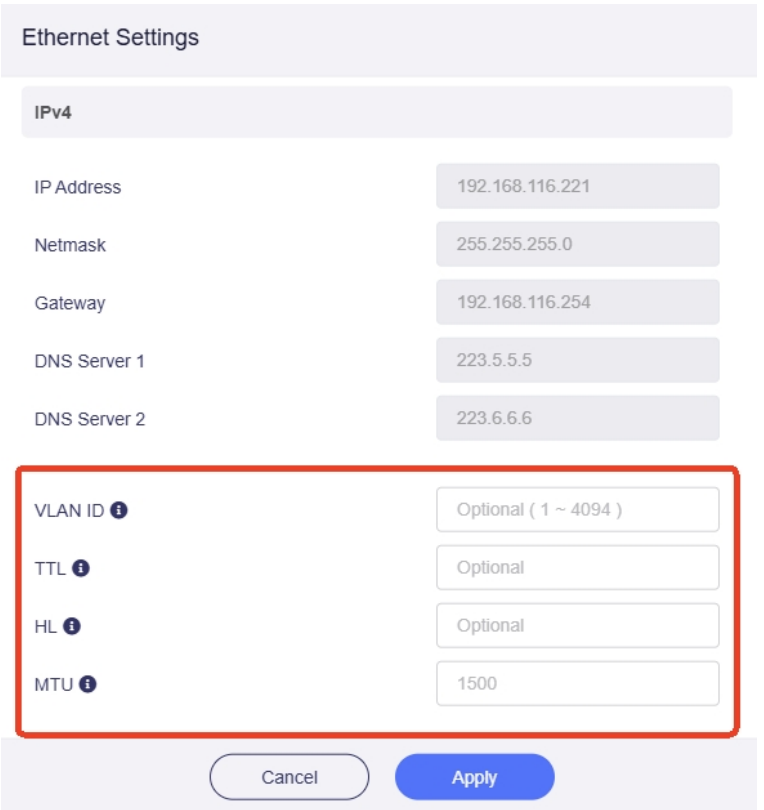

- **PPPoE**

  PPPoE (punto a punto) Protocolo sobre Ethernet) es un protocolo de red ampliamente utilizado por los ISP. Por lo general, proporcionarán un módem junto con un nombre de usuario y una contraseña únicos, necesarios para configurar una conexión a Internet.



## Configuración avanzada

Además de las configuraciones esenciales, también hay algunas configuraciones avanzadas opcionales para los tres protocolos anteriores.




- **VLAN ID**

  Esta configuración es necesaria solo si el servidor del proveedor requiere que la interfaz utilice un ID de VLAN etiquetado específico.

- **TTL**

  TTL (tiempo de vida) define el tiempo máximo que los paquetes pueden sobrevivir en la red. De forma predeterminada, el enrutador disminuye el TTL de los paquetes entrantes de los dispositivos cliente en 1 antes de reenviarlos. Si necesita anularlo, puede establecer un valor fijo aquí. La configuración TTL es válida solo para IPv4.

- **HL**

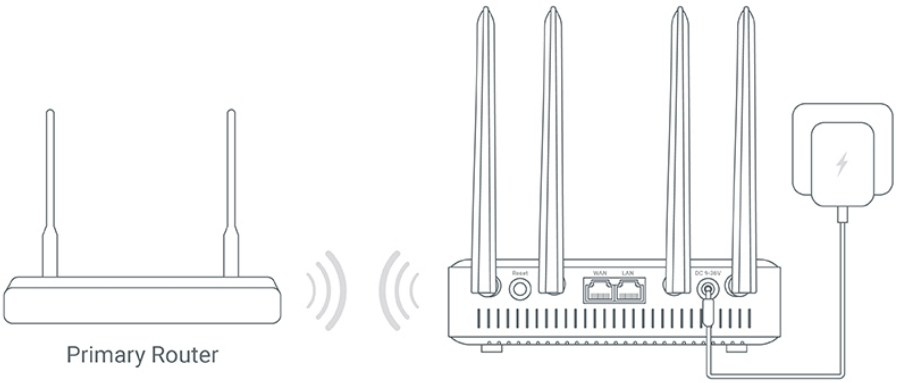
  En IPv6, el campo HL (Límite de saltos) limita el número de saltos de transmisión para paquetes de datos en la red, sirviendo como el equivalente de TTL en IPv4.

- **MTU**

  El valor de MTU predeterminado es 1500 bytes.

## 4.2.2 Conectarse a Internet mediante una red Wi-Fi existente

Conecte el enrutador como repetidor a la red inalámbrica existente para aumentar las señales de Wi-Fi-Fi y cree una red local aislada de la red principal. Cuando en hoteles o cafeterías con puntos de acceso públicos gratuitos, utilice un repetidor no solo fortaleces Wi-señales Fi, sino que también proporcionas acceso por cable e inalámbrico para múltiples dispositivos y proteges su red seguridad.

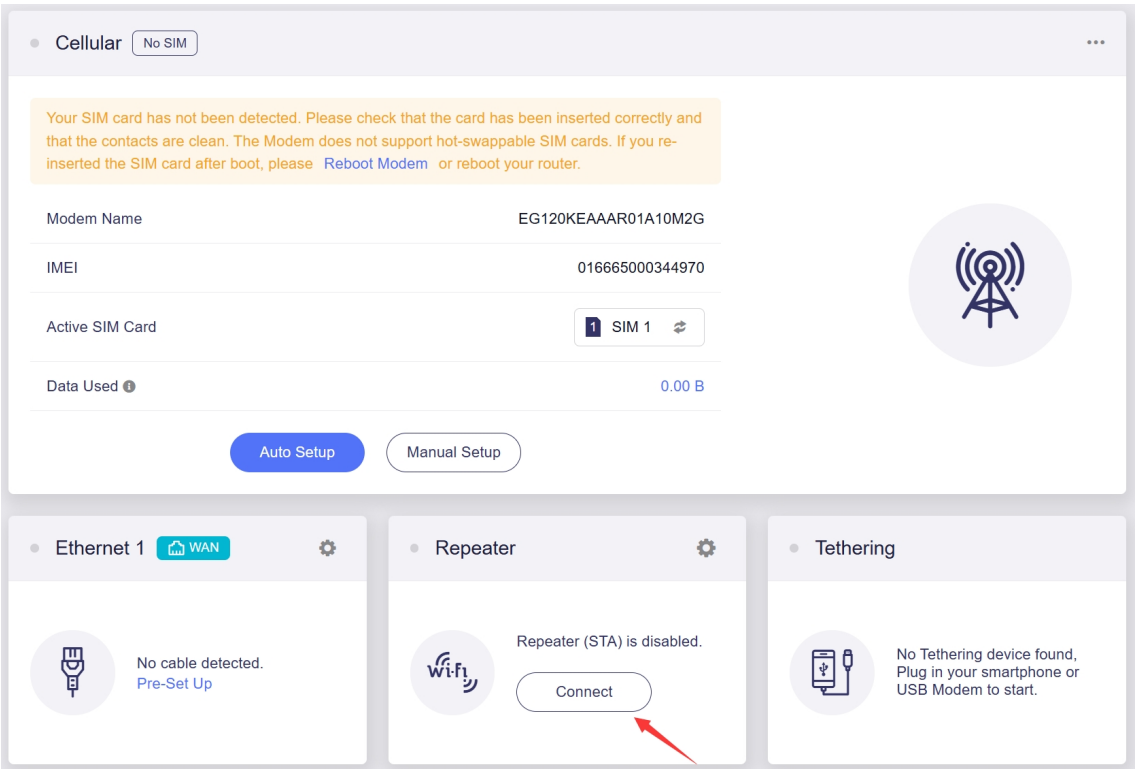



La función de repetidor GL.iNet funciona en modo WISP (Proveedor de servicios de Internet inalámbrico) de forma predeterminada, lo que significa que el enrutador creará su propia subred y actuará como un firewall para protegerlo de la red pública.

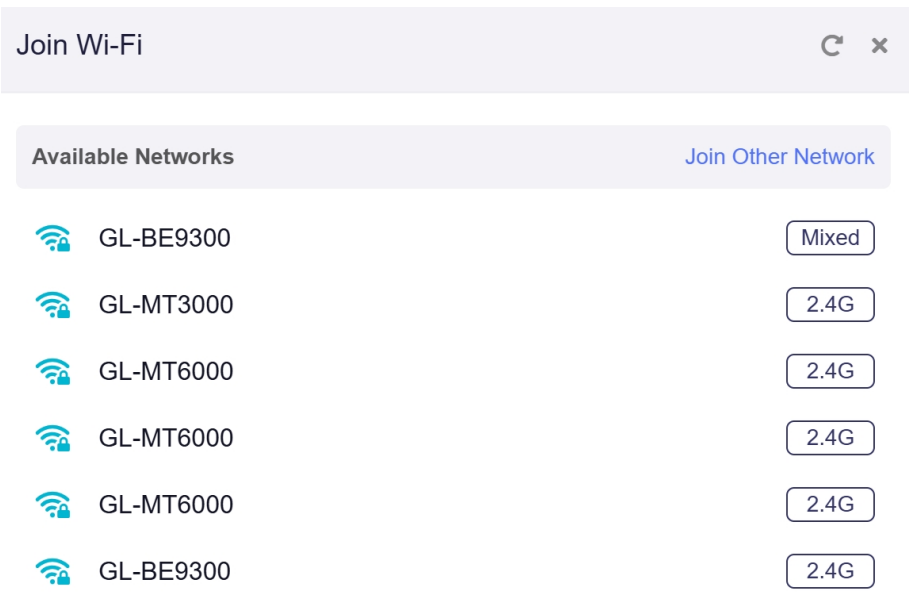
## Configuración básica

Siga los pasos a continuación para conectar su enrutador a una red Wi-Fi existente como repetidor.

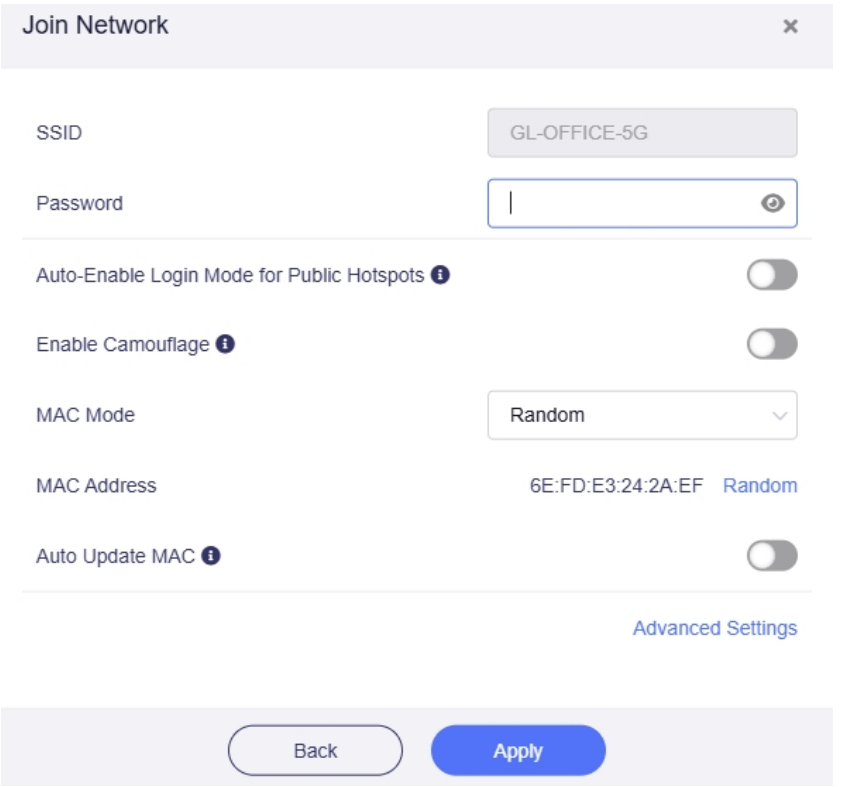
1. Inicie sesión en el enrutador', y navegue a **INTERNET** > **Repetidor**. Clic **Conectar**.



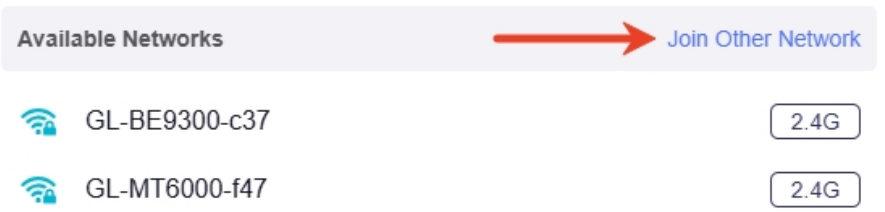

2. En la ventana emergente, celija la red Wi-Fi que desea conectarse de la lista de redes disponibles.



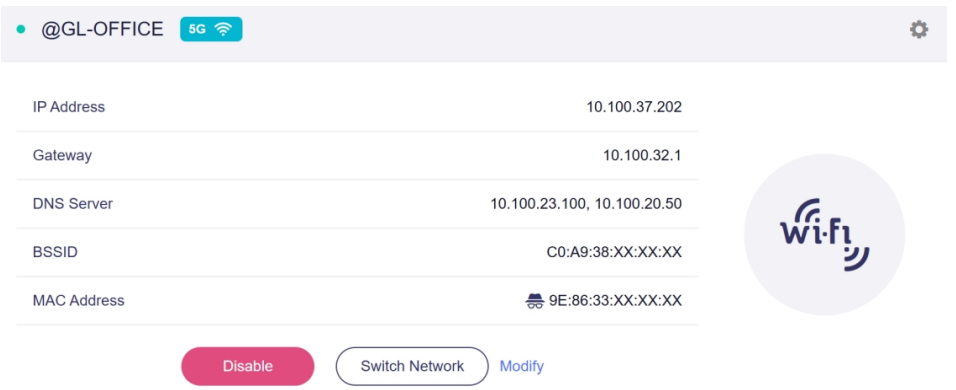
3. Eingrese la contraseña de Wi-Fi correcta y haga clic en **Aplicar**.




Si el SSID de Wi-Fi de destino no está en la lista de redes disponibles, haga clic en **Conectarse a otra red** en la esquina superior derecha, ingrese manualmente el SSID de Wi-Fi y otra información requerida, y haga clic en **Aplicar**.

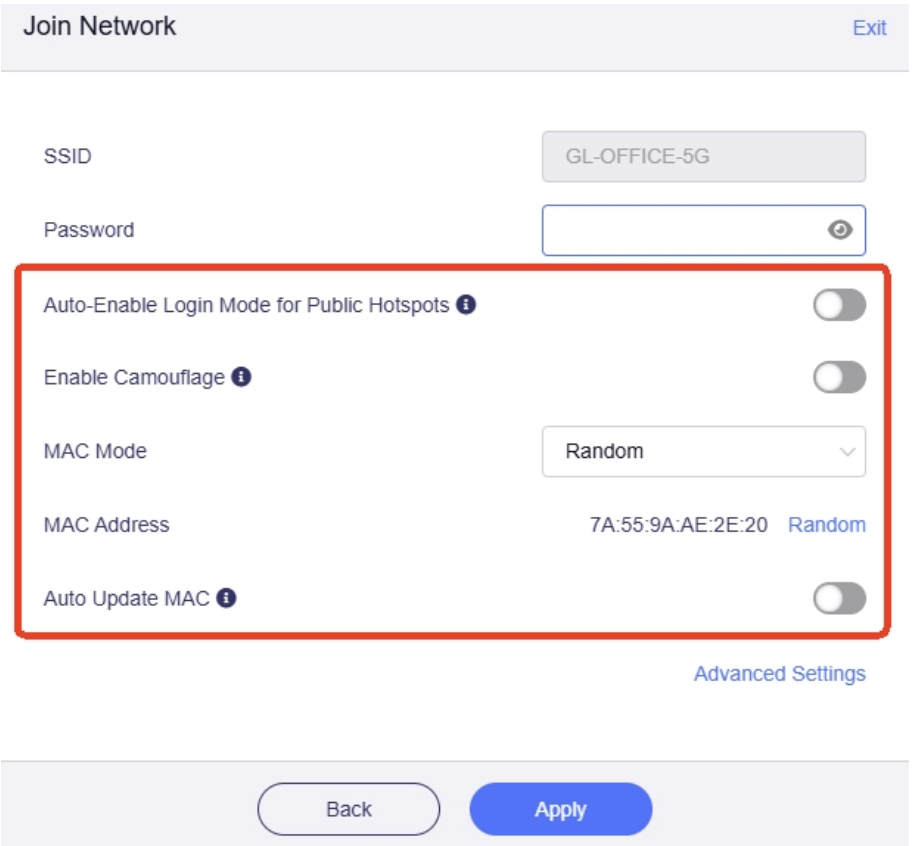



4. Espere un minuto hasta que el enrutador se conecte. Una vez conectado, la página se muestra a continuación.



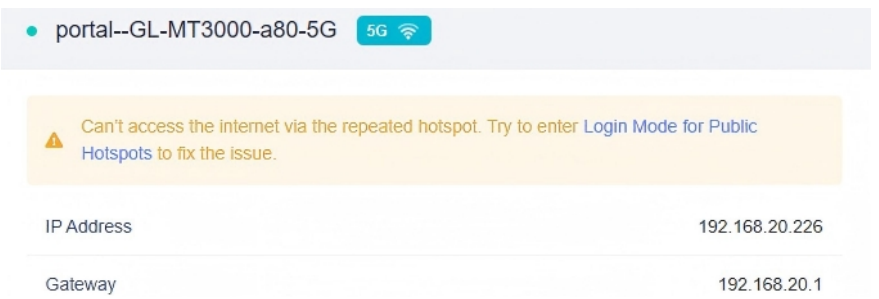
## Configuración del punto de acceso público

Al conectar el enrutador a un punto de acceso público con un portal cautivo, se recomienda activare las siguientes funciones para mejorar la tasa de éxito de la conexión.




- **Habilitar automáticamente el modo de inicio de sesión para puntos de acceso públicos**

  Si está habilitado, el enrutador ingresa automáticamente Modo de inicio de sesión de punto de acceso público cuando está conectado a un punto de acceso pero no a Internet. En este modo, algunos servicios se suspenderán mientras el modo DNS cambia a automático, lo que puede filtrar su actividad de red al proveedor de red (por ejemplo, hotel, centro comercial). Incluso si está deshabilitado, el enrutador le pedirá que ingrese a este modo si detecta un portal cautivo de punto de acceso o no puede iniciar sesión.



- **Habilitar camuflaje**

  Si está habilitado, el enrutador se hará pasar por el dispositivo cliente que usa para acceder al panel de administración emulando la dirección MAC de ese dispositivo.
- **Modo MAC**

  Elija qué dirección MAC usa el enrutador para conectarse al punto de acceso público.

  **Fábrica**: Utiliza la dirección MAC original asignada de fábrica al dispositivo.

  **Clonar**: clona la dirección MAC de un dispositivo cliente para la conexión.

  Si la MAC deseada no aparece en la lista, ingrese manualmente la dirección MAC que desea clonar. Nota: Muchos dispositivos utilizan direcciones MAC aleatorias (a menudo llamadas dirección Wi-Fi privada o dirección de hardware aleatoria) cuando se conectan a redes Wi-Fi. Como resultado, es posible que la dirección MAC que se muestra aquí no coincida con la MAC física real del dispositivo.

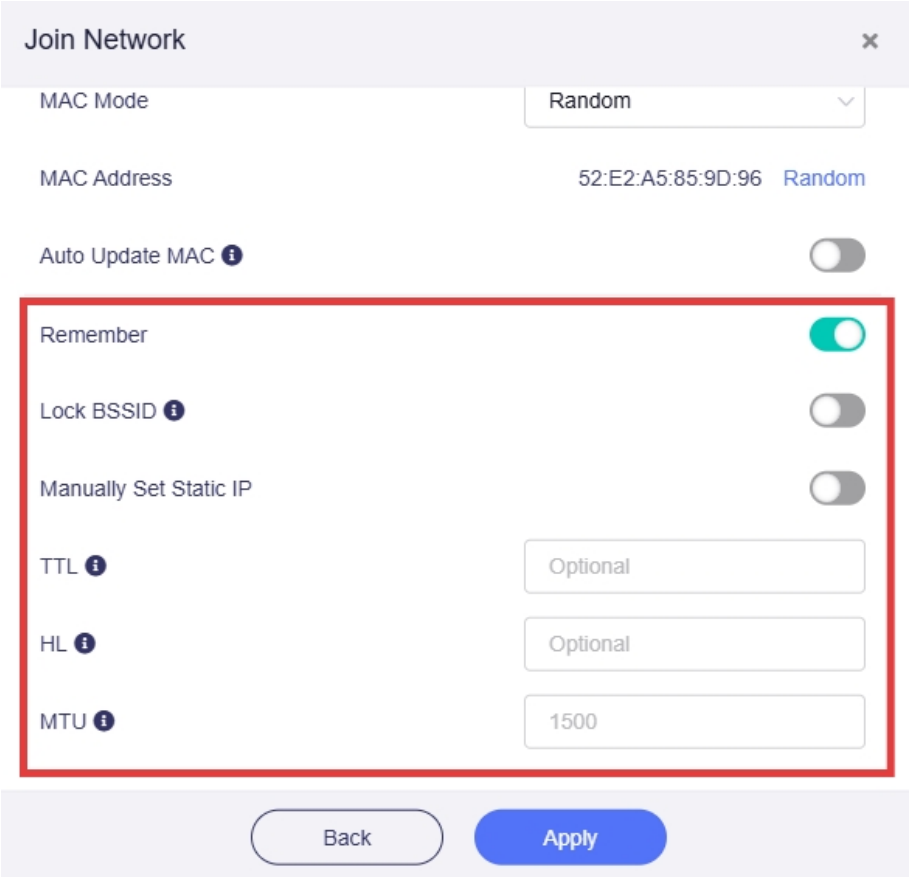
  **Aleatoria**: genera automáticamente una dirección MAC aleatoria para la conexión.
- **Actualización automática de MAC**

  Si esta opción está habilitada, la dirección MAC se actualizará automáticamente.

Al guardar la configuración de red, el modo MAC, incluida cualquier dirección MAC clonada o aleatoria, se vinculará al SSID específico que guarde. Puede cambiar manualmente esta configuración para cada SSID en cualquier momento.

## Configuración avanzada

Al unirse a la red, hay algunas configuración avanzada opcional.

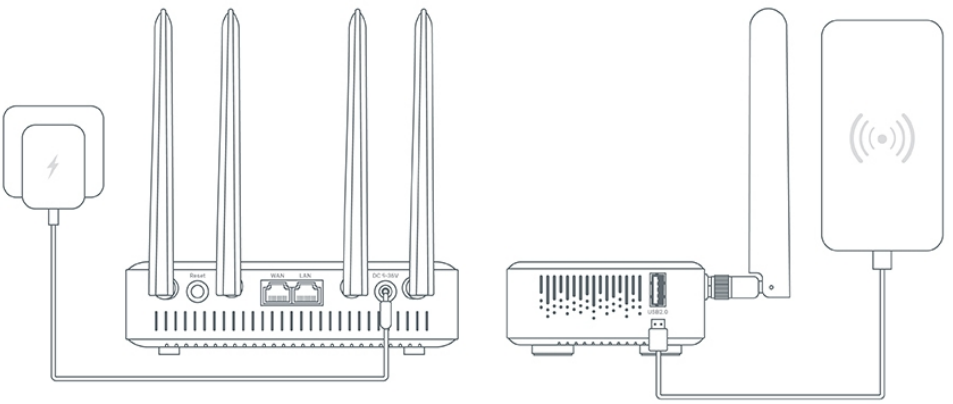



- **Recordar**: habilite esta opción para recordar la red Wi-Fi repetida actual.
- **Bloquear BSSID**: cuando habilitado, el enrutador se conectará solo al punto de acceso (AP) específico correspondiente al BSSID seleccionado, incluso cuando otros AP compartan el mismo SSID.
- **Configurar IP estática manualmente**: cuando está habilitado, puede configurar manualmente una dirección IPv4 fija, una máscara de red, una puerta de enlace y servidores DNS para la conexión repetidora del enrutador, en lugar de obtener estas configuraciones automáticamente.
- **TTL**: TTL (Time To Live) define el tiempo máximo que los paquetes pueden sobrevivir en la red. De forma predeterminada, el enrutador reduce en 1 el TTL de los paquetes entrantes de los dispositivos cliente antes de reenviarlos. Si necesita anular/falsificar el TTL, eingrese el TTL efectivo deseado más 1 para compensar la disminución automática. TTL es válido solo para IPv4.

- **HL**: En IPv6, el campo HL (Hop Limit) se utiliza para limitar el número de saltos de transmisión de paquetes de datos en la red, lo que equivale al TTL en IPv4.
- **MTU**: El valor predeterminado es 1500.

## 4.2.3 Conectarse a Internet mediante conexión compartida por USB

Conectar un teléfono inteligente al enrutador mediante un cable USB se denomina anclaje a red, y puede compartir la red de datos móviles del dispositivo (por ejemplo, 4G/5G) con el enrutador. Este es un método conveniente para el acceso temporal a Internet, especialmente en exteriores o en áreas sin banda ancha fija.

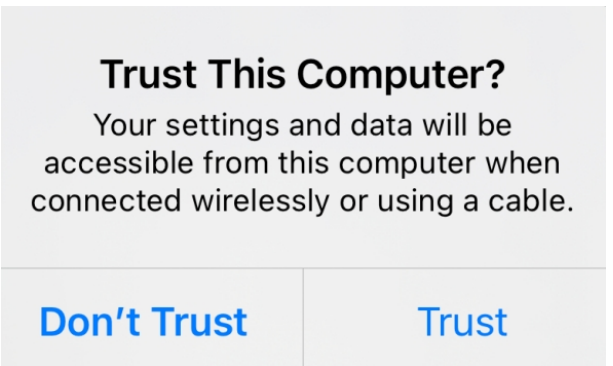


El módem sin host también funciona en Tethering durante la configuración del módem.

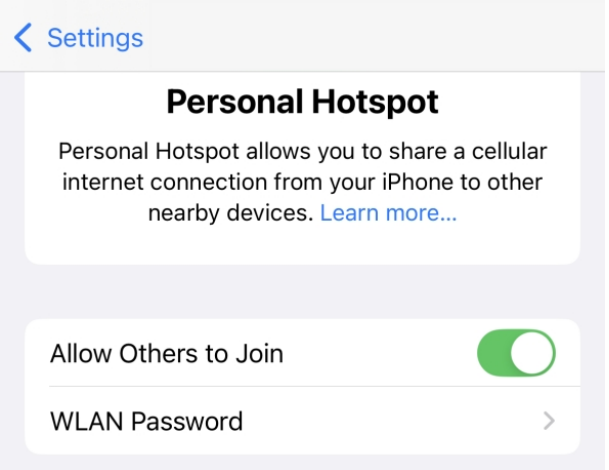
**Nota**: Algunos operadores de telefonía móvil limitan o cobran más por atadura. Recomendamos consultar con su operador.

### Conexión compartida desde un iPhone

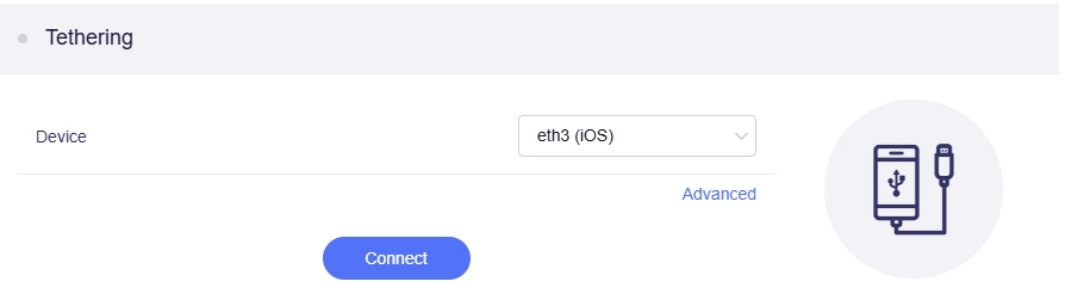
1. Conecte un iPhone al puerto USB del enrutador usando un cable USB. Aparecerá un cuadro de diálogo del sistema preguntando si se debe confiar en el dispositivo. Toque **Confiar** para continuar.



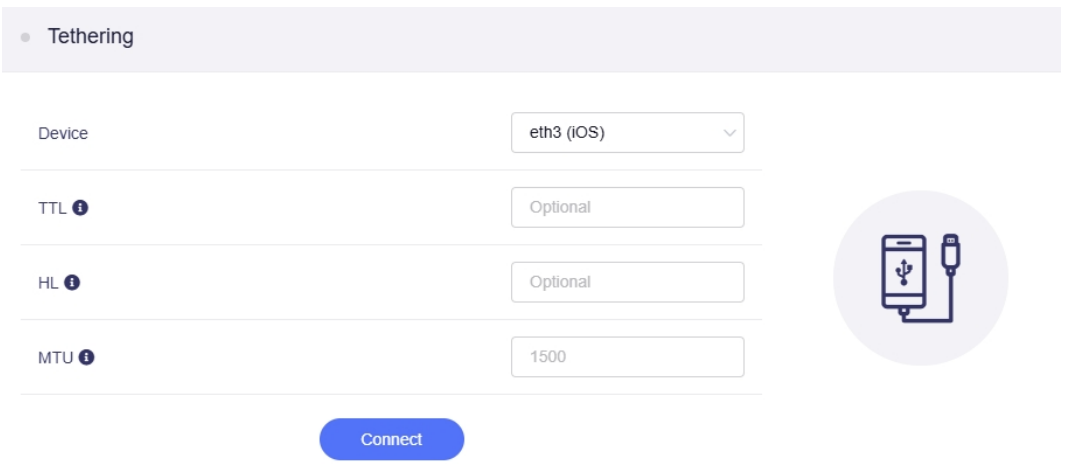
2. Ir a iPhone **Configuración** > **Punto de acceso personal**. Activar **Permitir que otros se unan**.



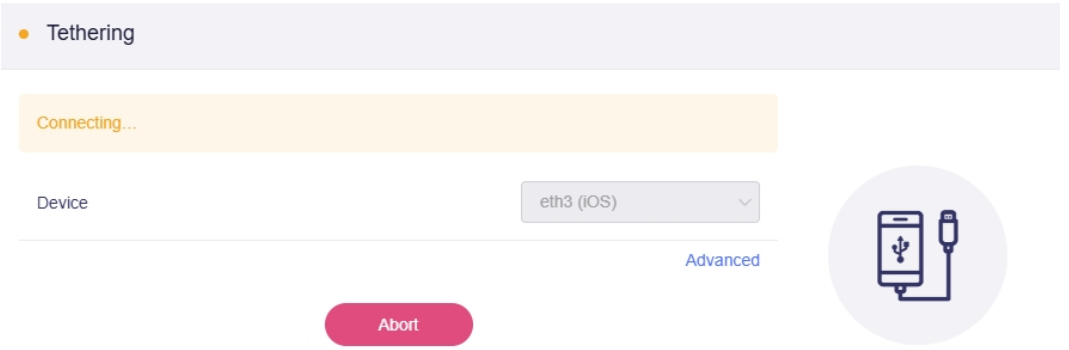

3. Conecte una computadora u otro teléfono al enrutador. Inicie sesión en el panel de administración web del enrutador y navegue hasta **INTERNET** > **Conexión**, luego haga clic en **Conectar**.



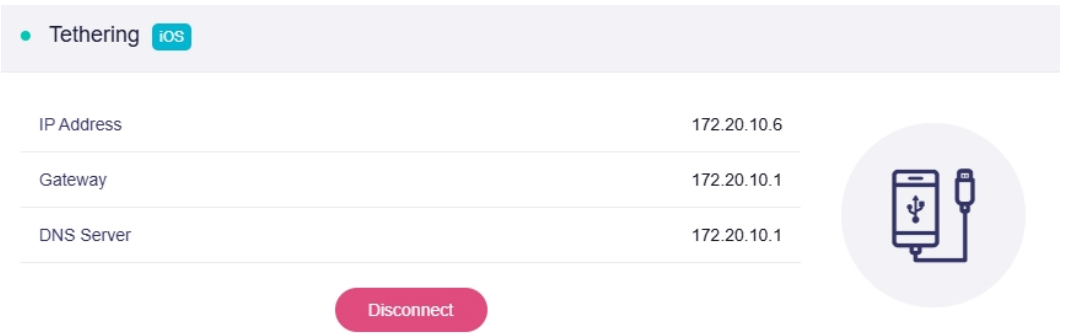

Si necesita configurar configuraciones avanzadas, como TTL, HL y MTU, haga clic **Avanzado** para personalizar estas configuraciones antes haga clicing **Conectar**.




4. Comenzará a conectarse.

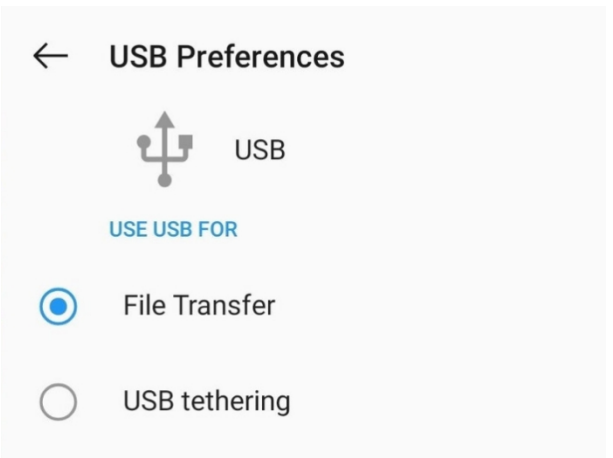



Una vez conectado, thes página mostrará la conexión Tethering detalles.

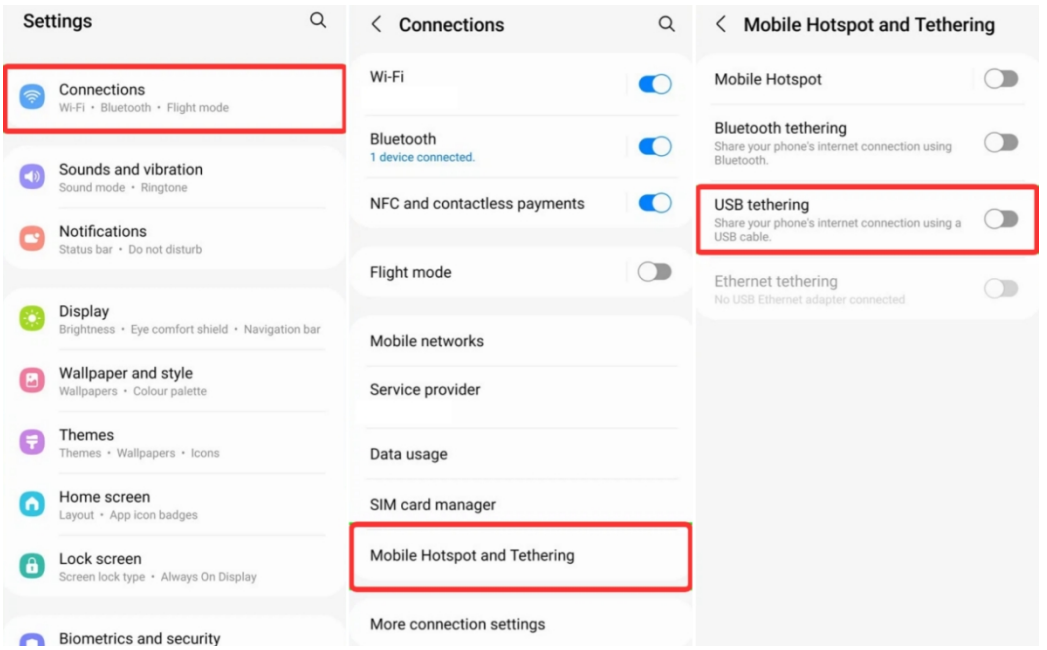



## Conexión compartida desde Android

1. Conectar un teléfono Android al puerto USB del enrutador mediante un cable USB. Puede aparecer un cuadro de diálogo del sistema preguntando USB preferencias. Seleccione **Anclaje a red USB** o **Archivo Transferir** si se le solicita.

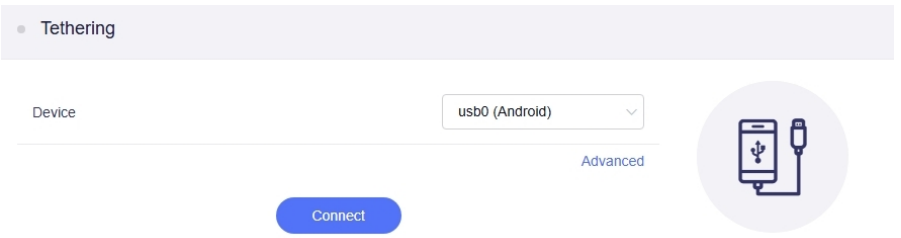



2. Vaya a la **Configuración** > **Red e Internet** > **Punto de acceso personal**. Activar **Personal Punto de acceso** o **Anclaje a red USB**.

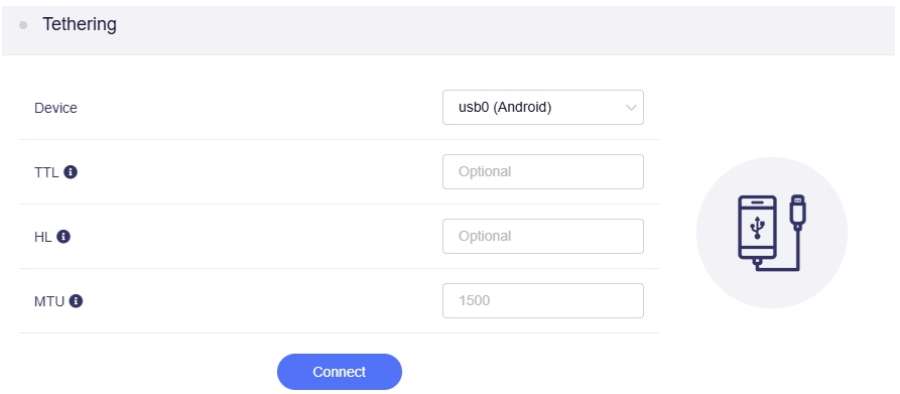



(Los pasos para habilitar el Anclaje a red USB varían según la marca. Verifique la configuración de su dispositivo para conocer la ubicación exacta y comuníquese con el soporte técnico del fabricante si es necesario).

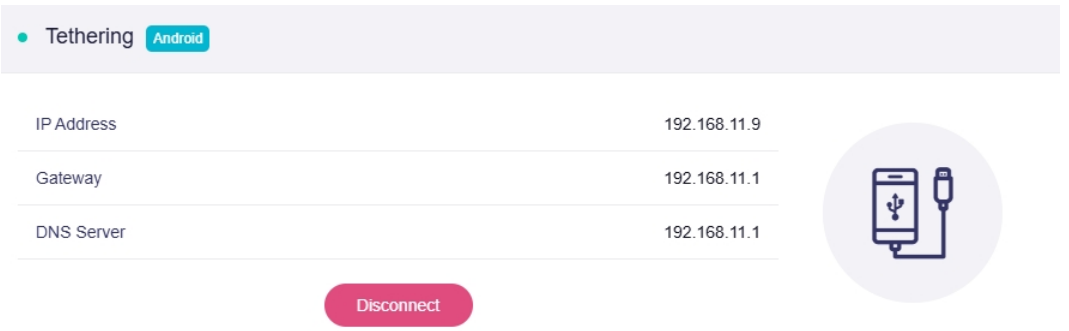
3. Conecte una computadora u otro teléfono al enrutador y luego inicie sesión a el panel de administración web del enrutador, navegue a **INTERNET** > **Anclaje a red**. Click **Conectar**.




Si necesita establecer configuraciones avanzadas como TTL, HL y MTU, haga clic en **Avanzado** para personalizar estas configuraciones antes de hacer clic en **Conectar**.



4. Comenzará a conectarse. Una vez conectado, estaes página mostrará Conexión estado de conexión.




## Solución de problemas

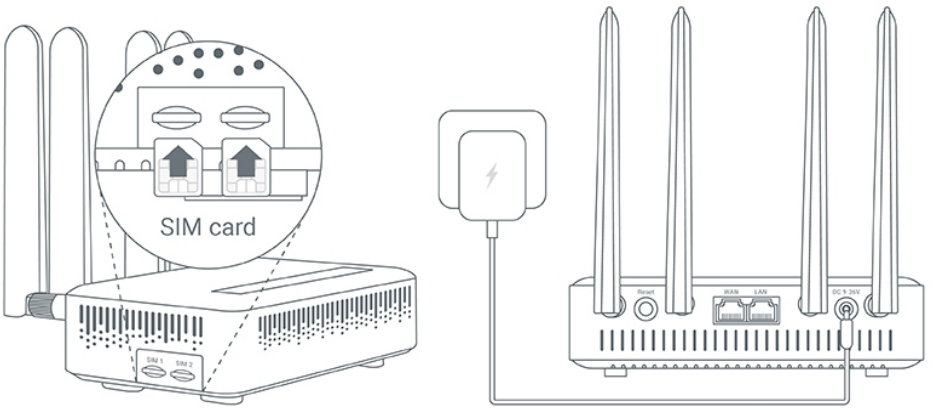
Si la conexión Tethering falla, prueba estos pasos para solucionar el problema:

- Utiliza la fuente de alimentación original para el enrutador.
- Desconecta y vuelve a conectar el cable USB.
- Utiliza otro cable USB. Asegúrese de que admita la transferencia de datos (no solo la carga).
- Desactive y active "Anclaje a red USB" varias veces (para teléfonos Android).
- Desactive y active "Permitir que otros se unan" varias veces (para iPhone).
- Reinicie su teléfono inteligente e inténtelo de nuevo.

Si el problema persiste, comuníquese con nuestro soporte técnico en support@gl-inet.com.

## 4.2.4 Conectarse a Internet mediante la red móvil

Conecte el enrutador a Internet insertando una o dos tarjetas SIM en su ranura para tarjeta Nano-SIM dual. Esto permite que el enrutador se conecte a Internet a través de redes 4G/5G, brindando conectividad sin depender de la banda ancha de línea fija. Es adecuado para uso en vehículos o actividades al aire libre. Tenga en cuenta que esta conexión se implementa a través del módem celular del enrutador'.

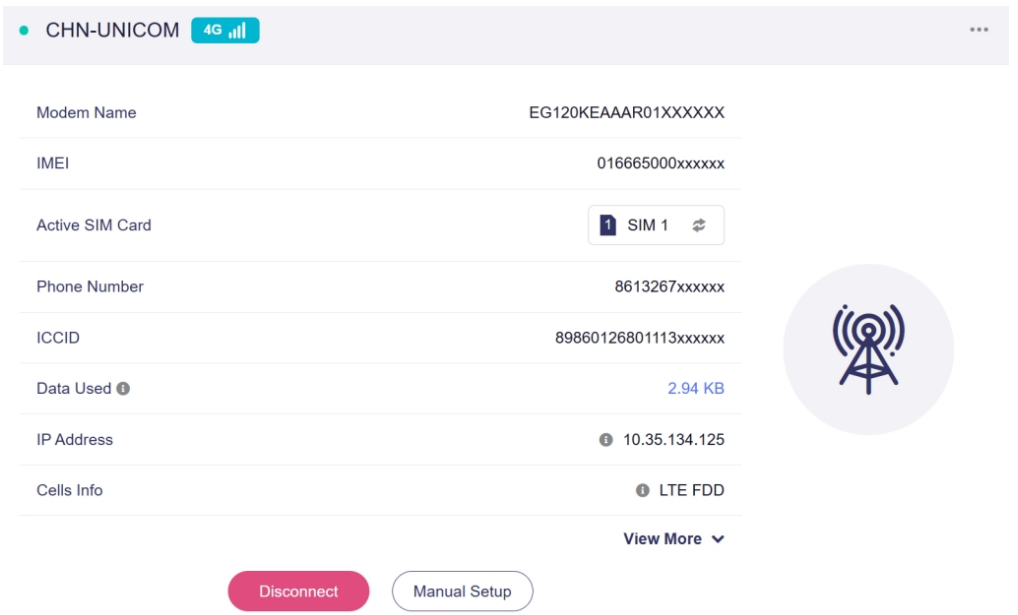



**Nota**: la funcionalidad eSIM de Spitz Plus está disponible en el firmware v4.7 y superior. Aprenda a utilizar la tarjeta física eSIM en el enrutador GL.iNet aquí.

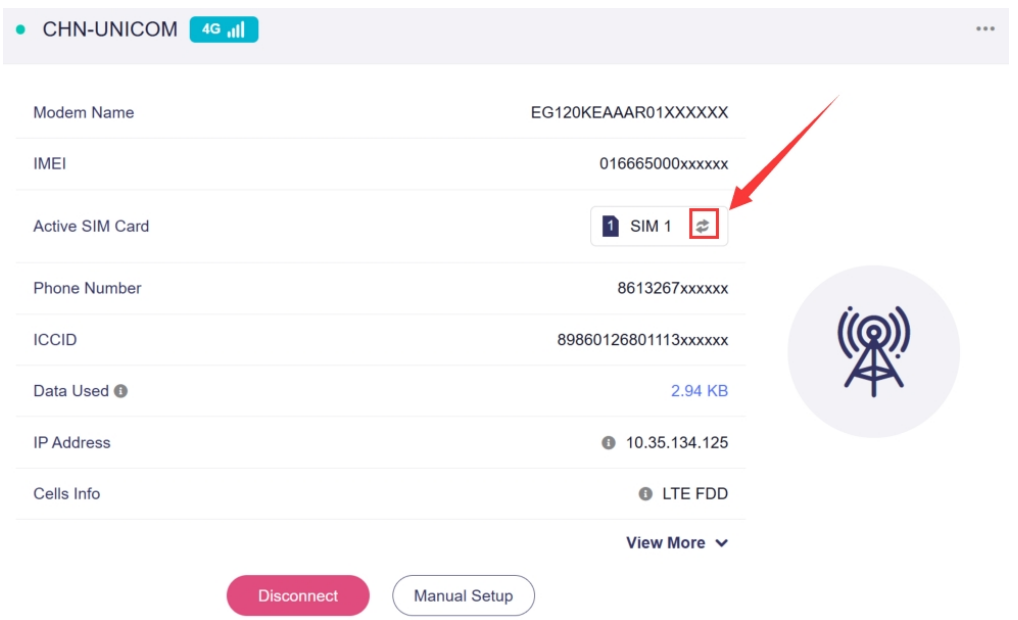
## Configuración básica

Siga los pasos a continuación para conectar su enrutador a Internet a través del celular.

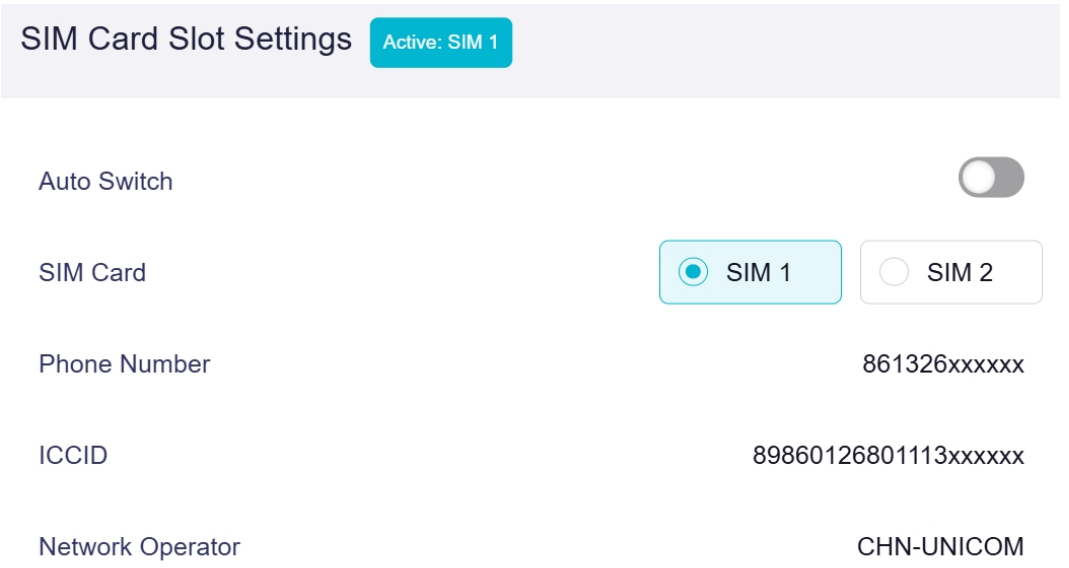
1. Inserte una o dos tarjetas SIM en el enrutador y se establecerá la conexión a Internet automáticamente.
2. Inicie sesión en el enrutador’s web admin panel y navega hasta **INTERNET** > **Cellula**r. Deberías ver el nombre de tu operador SIM y un punto verde en la sección Celular. De lo contrario, apaga el enrutador, vuelve a insertar la tarjeta SIM y enciéndelo.




3. Cuando se inserten dos tarjetas SIM, haz clic en el ícono de cambio a la derecha de Tarjeta SIM activa.

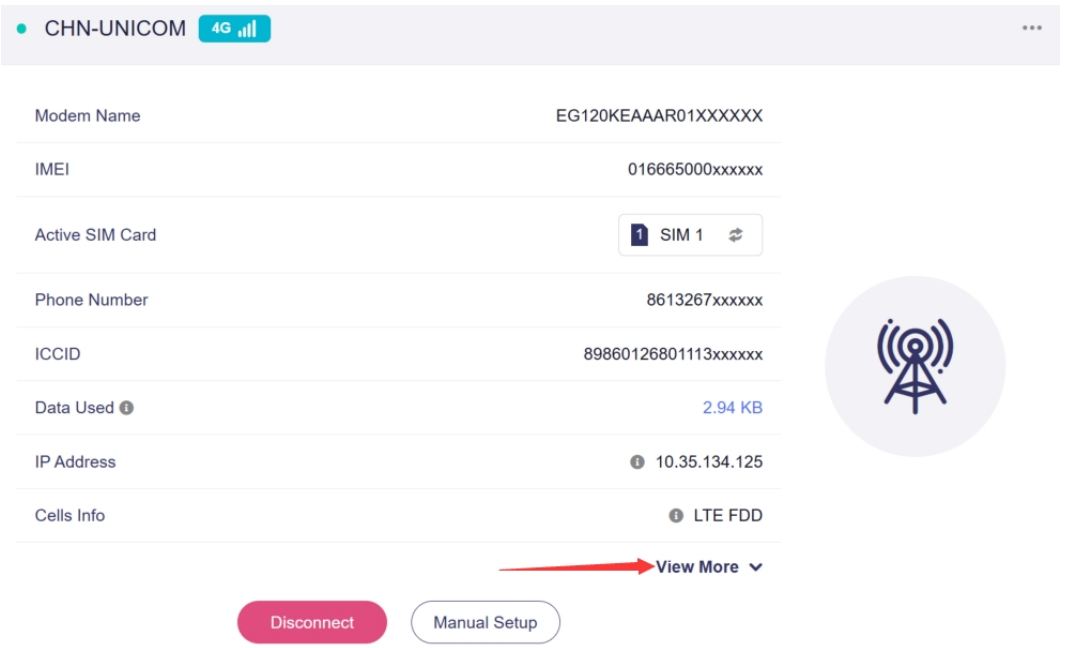


Active **Cambio automático** para cambiar entre SIM 1 y SIM 2 automáticamente.

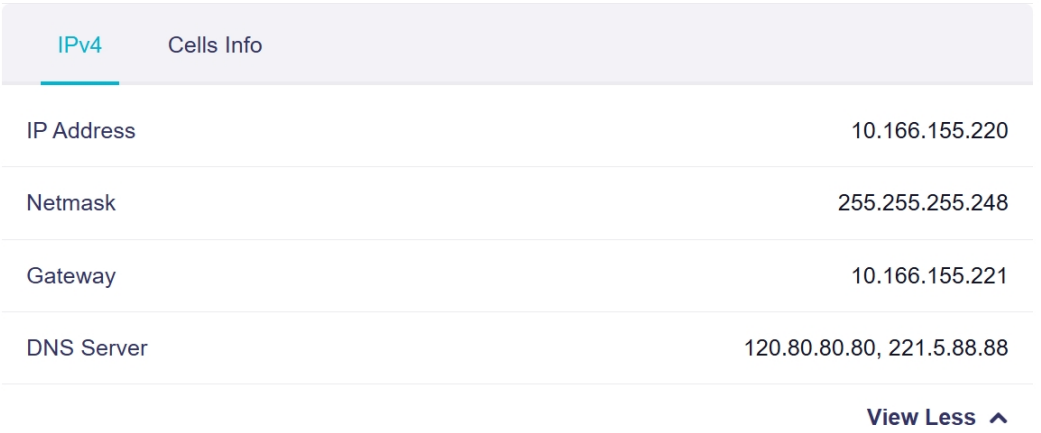



**Nota**: cuando se insertan dos tarjetas SIM, solo una tarjeta SIM puede estar activa a la vez.

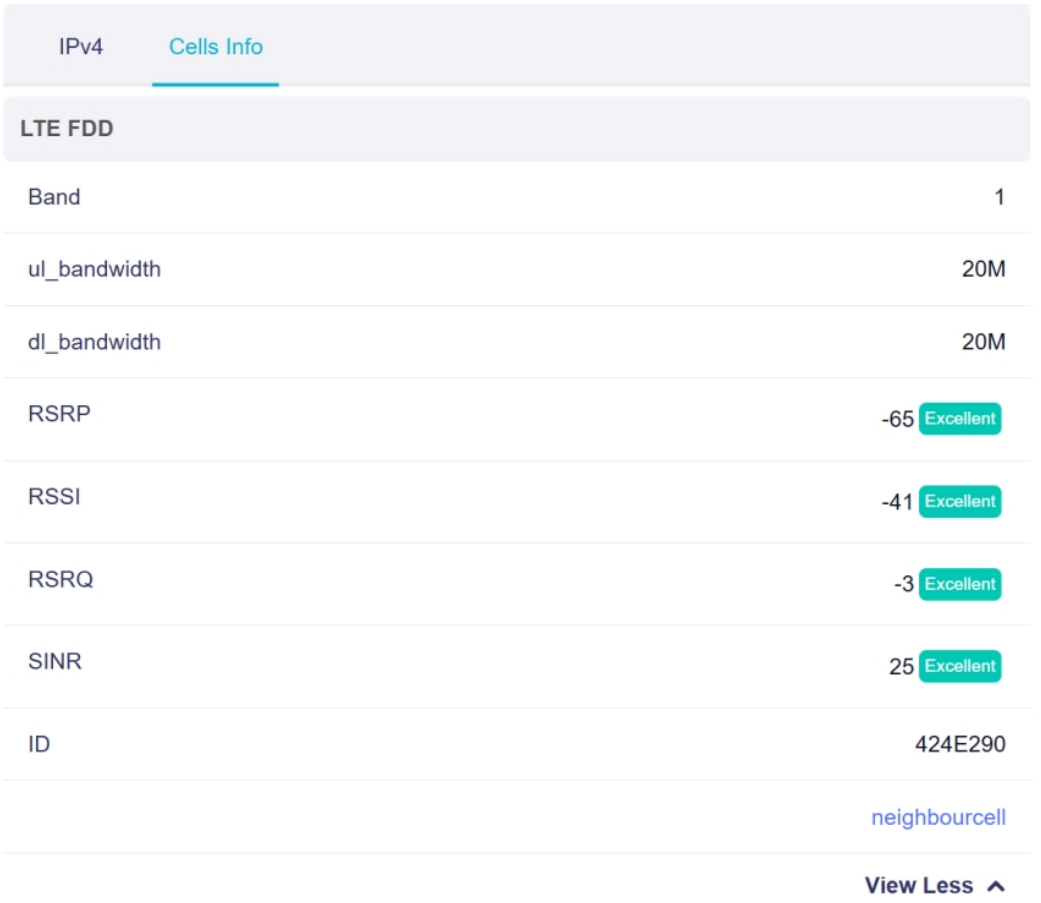
4. Haga clic en **Ver más** para ver más información celular, incluidos detalles del módem, detalles de la tarjeta SIM, detalles de Internet y señal celular.




Puede ver los detalles de la WAN.



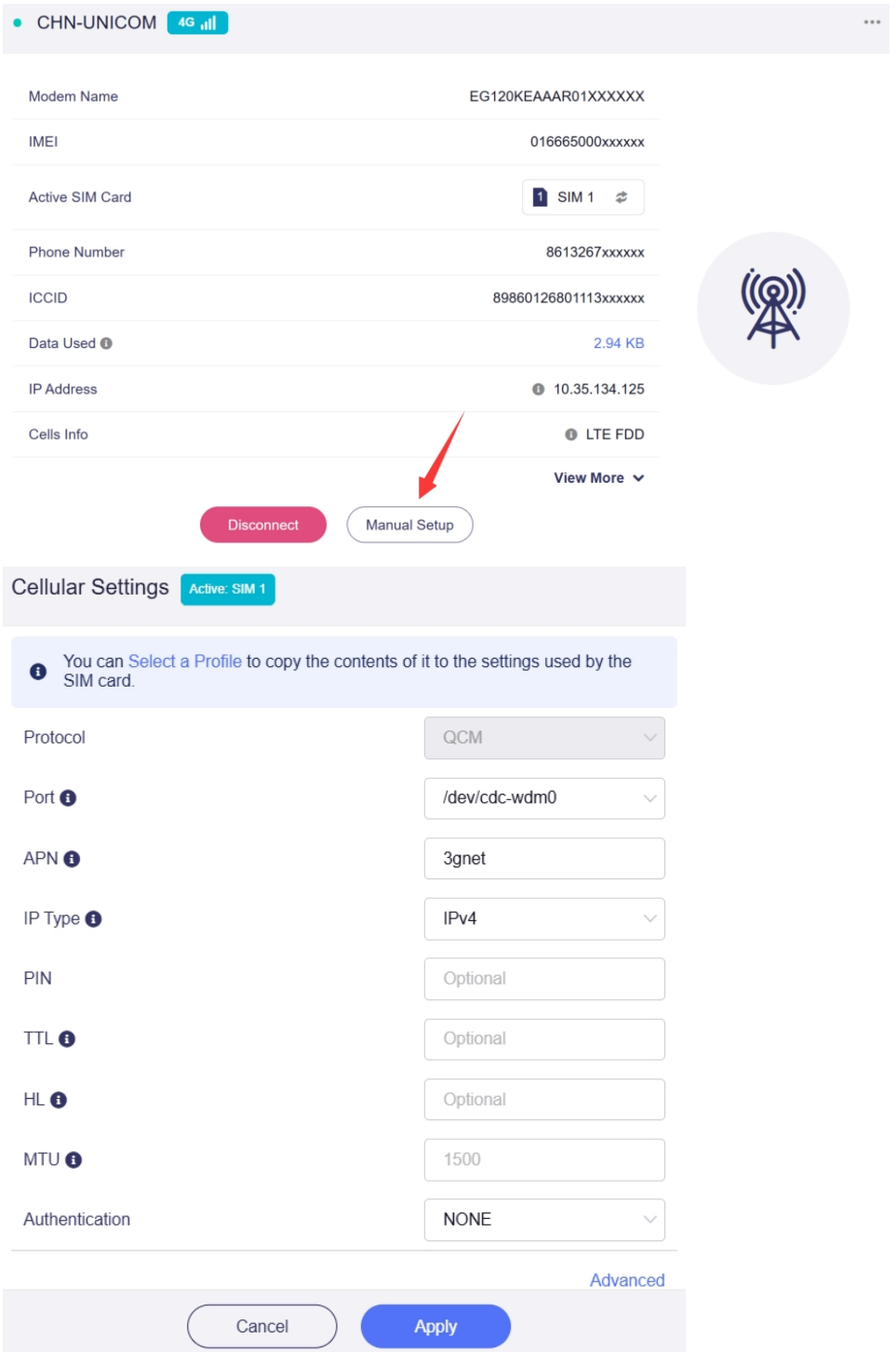

Haga clic en **Información de las celdas** para ver los detalles de las celdas si es necesario.




Si encuentra algún problema, consulte Guía de solución de problemas de redes móviles.

## Configuración avanzada

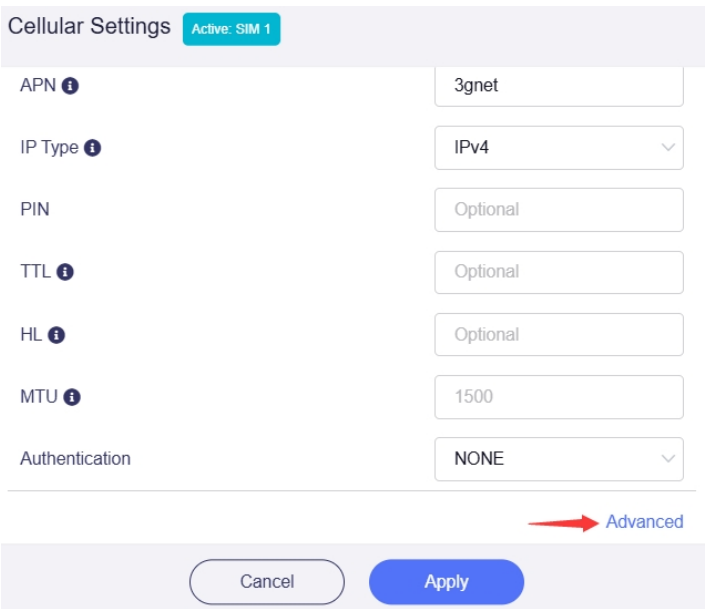
El enrutador proporciona configuraciones avanzadas opcionales para conexiones celulares. Haga clic en **Configuración manual** para configurarlos.

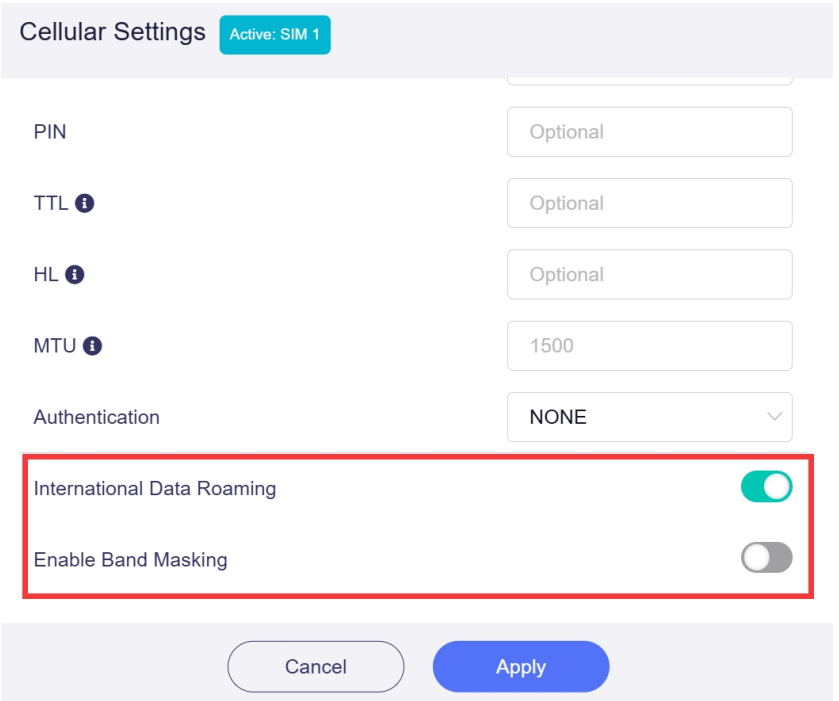



- **Port**: El puerto cdc-wcdm0 es más rápido y el puerto ttyUSBX tiene mejores compatibilidad.

- **APN**: algunas tarjetas SIM requieren un APN específico. Si no conoce el APN correcto, consulte a su operador de red.
- **Tipo de IP**: Si la tarjeta SIM no admite la configuración de tipo de IP actual, o cuando se selecciona IPv6 pero el conmutador global de IPv6 no está activado, se pueden producir anomalías en la marcación.
- **PIN**: ingrese el PIN de la tarjeta SIM si la protección mediante PIN está habilitada.
- **TTL**: TTL (tiempo de vida) define el tiempo máximo que los paquetes pueden sobrevivir en la red. De forma predeterminada, el enrutador reduce en 1 el TTL de los paquetes entrantes de los dispositivos cliente antes de reenviarlos. Si necesita anular/falsificar el TTL, eingrese el TTL efectivo deseado más 1 para compensar la disminución automática. TTL es válido solo para IPv4.
- **HL**: En IPv6, el campo HL (Hop Limit) se utiliza para limitar el número de saltos de transmisión de paquetes de datos en la red, lo que equivale al TTL en IPv4.El campo HL (Límite de saltos) se utiliza para limitar el número de saltos de transmisión de paquetes de datos en la red, lo que equivale al TTL en IPv4.
- **MTU**: el valor predeterminado es 1500.
- **Autenticación**: elija el método de autenticación requerido por su proveedor (por ejemplo, NINGUNO, PAP, CHAP). Por lo general, esto se establece en NINGUNO si no se necesitan credenciales.

Haga clic **Avanzado** para habilitar roaming de datos internacional o enmascaramiento de banda si es necesario.

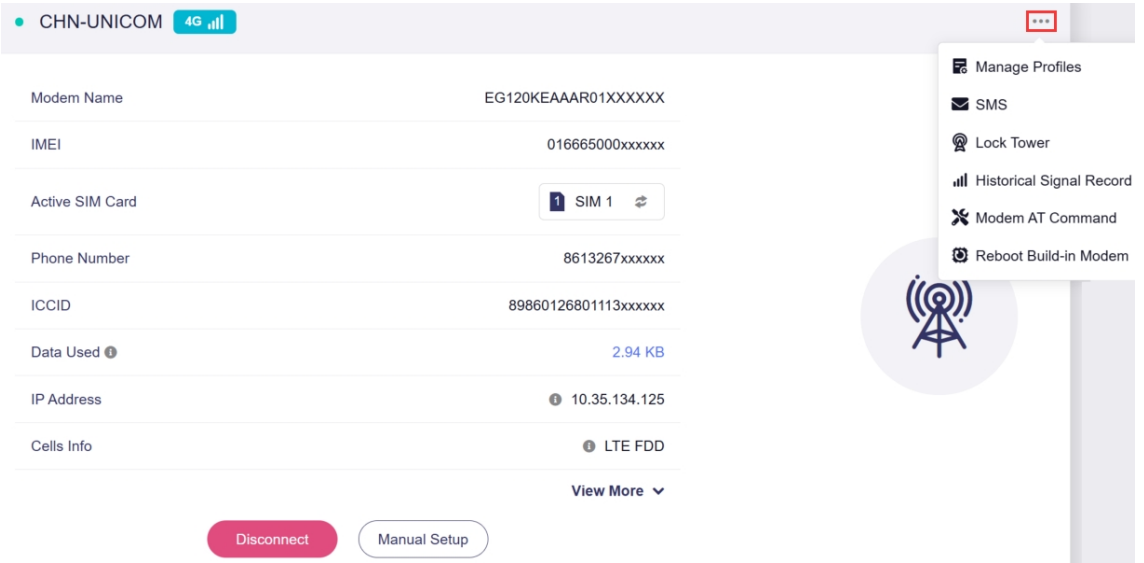





- **roaming de datos internacional**: si esta opción está habilitada, la tarjeta SIM puede usar datos móviles mientras está en roaming en el extranjero. Es posible que se apliquen cargos de roaming adicionales. Esta opción está habilitada de forma predeterminada.
- **Habilitar enmascaramiento de banda**: si esta opción está habilitada, puede seleccionar o excluir manualmente bandas de frecuencia celulares específicas.

## Configuración avanzada del módem

Además de la configuración celular básica, puede habilitar funciones avanzadas del módem para administrar perfiles celulares, mensajes SMS, registros de señal y más. Haga clic en el icono de menú en la esquina superior derecha.




- **Administrar perfiles**: cree y administre perfiles celulares para cambiar rápidamente APN y otras configuraciones celulares.
- **SMS**: envíe, reciba y vea mensajes SMS a través del integrado módem celular.
- **Fijar la estación base**: bloquea el enrutador en una estación base específica para conexiones celulares estables. La torre debe admitir bandas de frecuencia coincidentes, o la conexión puede fallar.
- **Registro histórico de señales**: vea registros históricos de intensidad de la señal celular para evaluar la calidad de la conexión.
- **Comando AT del módem**: envíe comandos AT para verificar el estado y depurar la red celular módem.
- **Reiniciar el módem incorporado**: reinicie el módem celular incorporado sin reiniciar todo el enrutador.

Para obtener instrucciones detalladas sobre la configuración avanzada del módem, consulte Conectarse a Internet mediante la red móvil.

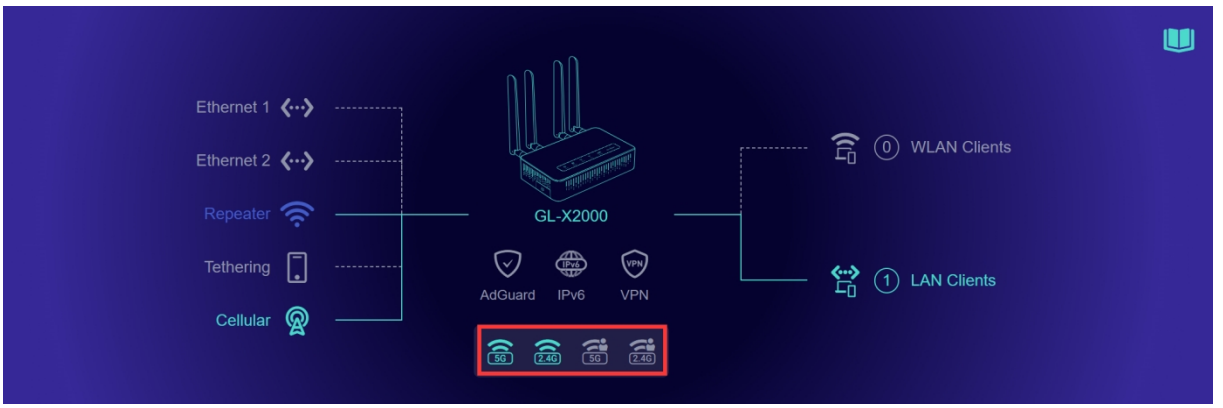
Capítulo 5

# Red inalámbrica

Este capítulo lo guía para verificar el estado de Wi-Fi y configurar los ajustes inalámbricos.

## 5.1 Visualización del estado de Wi-Fi

El enrutador’s Las redes Wi-Fi están habilitadas de forma predeterminada, y el icono de Wi-Fi correspondiente se iluminará debajo de la imagen del modelo del dispositivo en la Página INTERNET.




Sisi el cursor se sitúa sobre el icono de Wi-Fi habilitado, aparecerá un código QR de Wi-Fi se mostrará de la siguiente manera. Puedes escanear el código QR de Wi-Fi para conectarte rápidamente al Wi-Fi correspondiente.

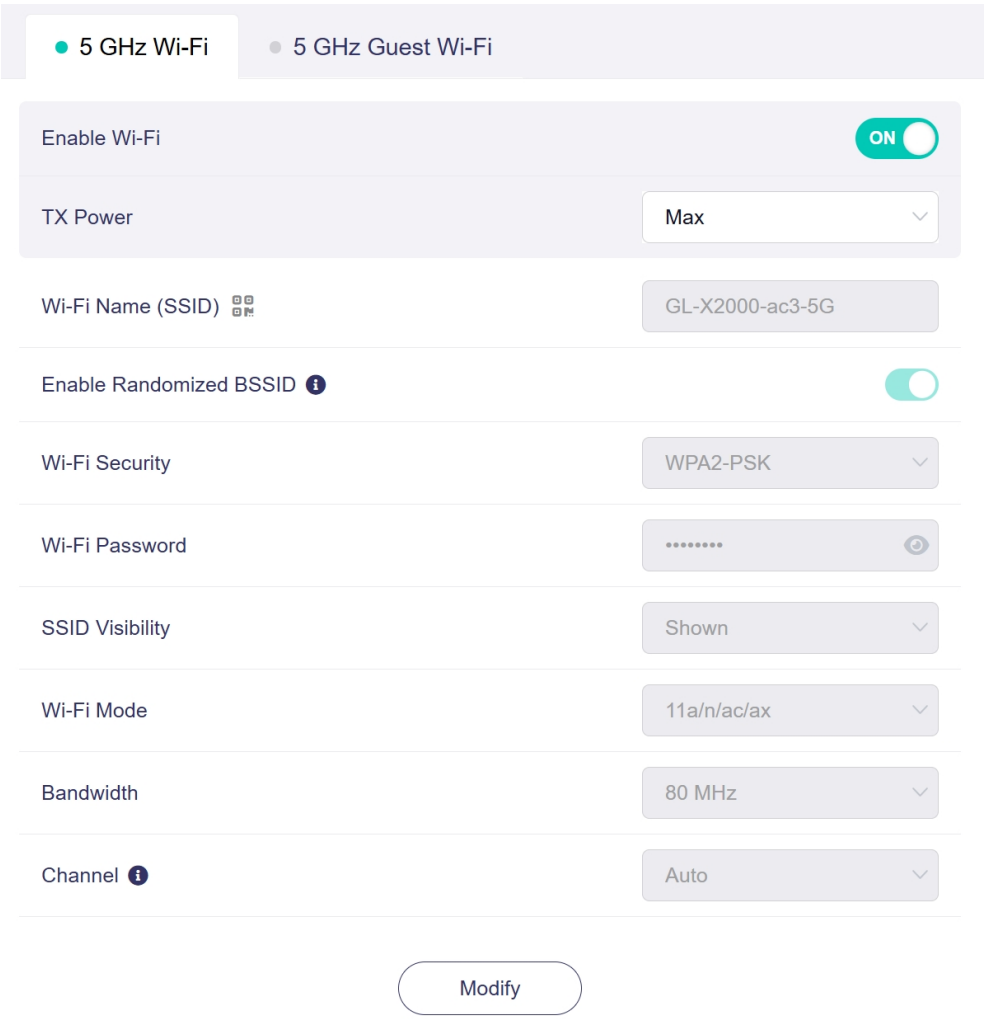


## 5.2 Configuración inalámbrica

Inicie sesión en el panel de administración web del enrutador y navegue hasta **Inalámbrica**. La página inalámbrica muestra las configuraciones de Wi-Fi 5 GHz y 2.4 GHz del enrutador, con cada una más dividido en redes Wi-Fi principal y Wi-Fi para invitados para una administración flexible

### 5.2.1 Wi-Fi de 5 GHz

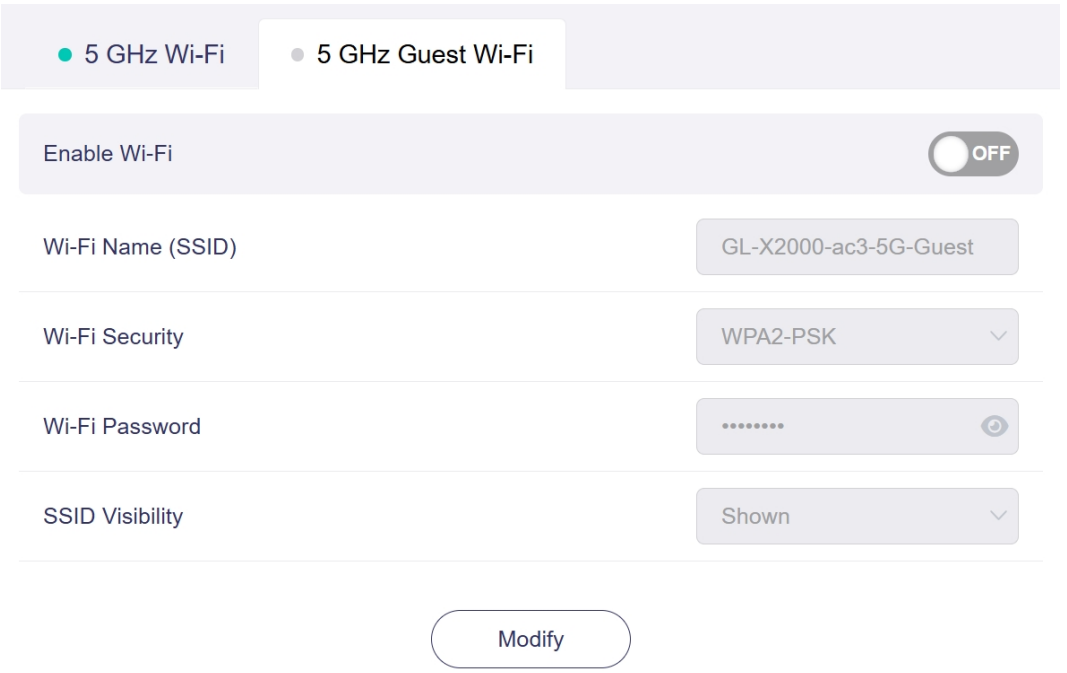
El Wi-Fi principal de 5 GHz le permite configurar múltiples ajustes, incluida la activación/desactivación Wi-Fi, configuración de potencia de TX, activación/desactivación de BSSID aleatorio, configuración de nombre de Wi-Fi (SSID), seguridad, contraseña, visibilidad de SSID, modo, ancho de banda y canal.




**Nota**:

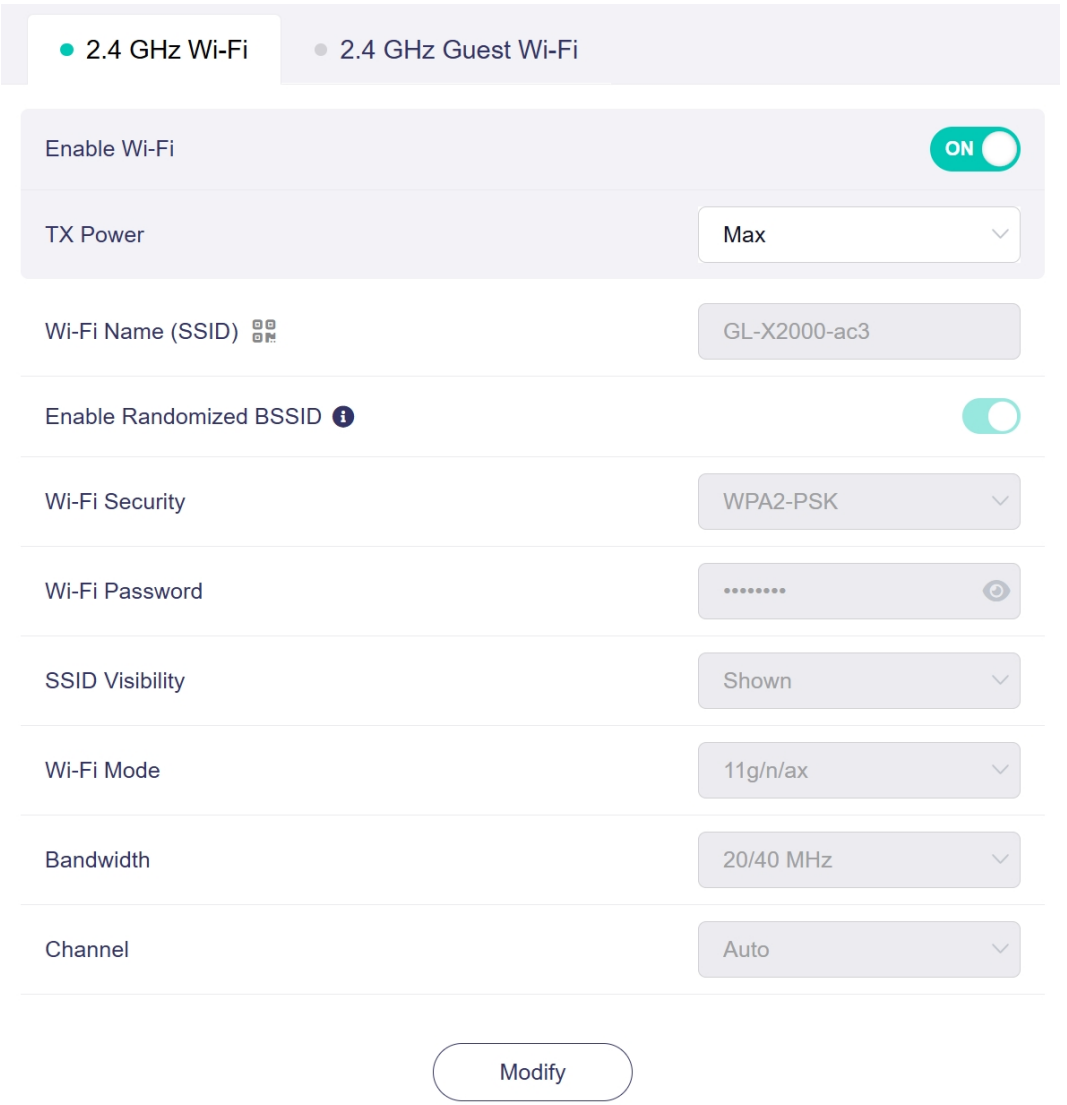
1. **BSSID aleatorio** está habilitado de forma predeterminada. Ayuda a evitar que el enrutador sea rastreado a través de un BSSID fijo, ya que los dispositivos cliente pueden informar BSSID cercanos y sus propios datos de ubicación a los proveedores de sistemas operativos/dispositivos, quienes los utilizan para crear una base de datos de BSSID a ubicación. Cuando está habilitado, el enrutador utiliza un BSSID generado aleatoriamente y lo renueva en cada reinicio, por lo que el BSSID no se puede vincular a una ubicación fija.
2. El **Ancho de banda** y **Canal** no se puedemodificar cuando el enrutador está configurado como a repeater, ya que siguen el de la red repetida.
3. Cuando **Canal** está configurado en **Auto**, el enrutador's Wi-Fi no cambiará automáticamente al canal DFS.
4. Cuando **Ancho de banda** está configurado en **160 MHz** (solo disponible en algunos modelos), el Wi-Fi siempre usará el canal DFS, incluso si selecciona un canal que no es DFS o configúrelo en Auto.

El 5GHz Invitado Wi-Fi le permite configurar ajustes simplificados, incluida la activación/desactivación de Wi-Fi, la configuración del nombre de Wi-Fi (SSID), la seguridad, la contraseña y la visibilidad de SSID.



## 5.2.2 Wi-Fi de 2,4 GHz

El Wi-Fi principal de 2,4 GHz le permite configurar múltiples ajustes, incluidos a configurar múltiples ajustes, incluido habilitar/deshabilitar Wi-Fi, configurar la potencia de TX, habilitar/deshabilitar BSSID aleatorio, configurar nombre de Wi-Fi (SSID), seguridad, contraseña, visibilidad de SSID, modo, ancho de banda y canal.



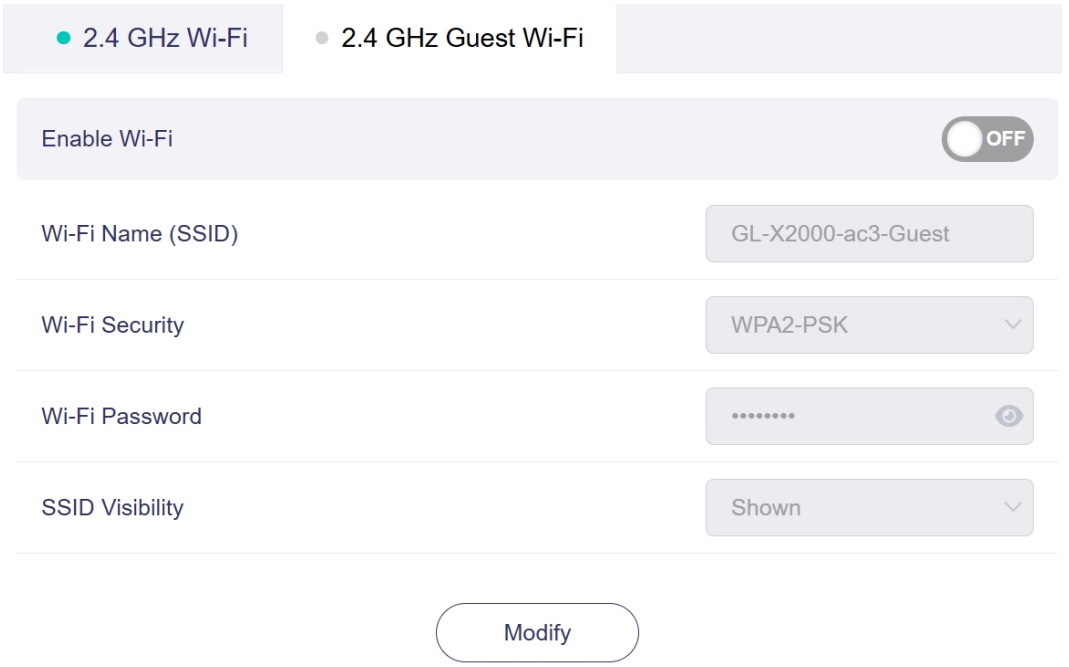

**Nota**:

1. **BSSID aleatorio** está habilitado de forma predeterminada. Ayuda a evitar que el enrutador sea rastreado a través de un BSSID fijo, ya que los dispositivos cliente pueden informar BSSID cercanos y sus propios datos de ubicación a los proveedores de sistemas operativos/dispositivos, quienes los utilizan para crear una base de datos de BSSID a ubicación. Cuando está habilitado, el enrutador utiliza un BSSID generado

aleatoriamente y lo renueva en cada reinicio, por lo que el BSSID no se puede vincular a una ubicación fija.

2. El **Ancho de banda** y **Canal** no se pueden modificar cuando el enrutador está configurado como repetidor, ya que siguen el de la red repetida.

El 2,4 GHz Invitado Wi-Fi permite te configuración simplificada configuración, incluidag habilitación/ deshabilitar Wi-Fi, configurar nombre de Wi-Fi (SSID), seguridad, contraseña y visibilidad de SSID.



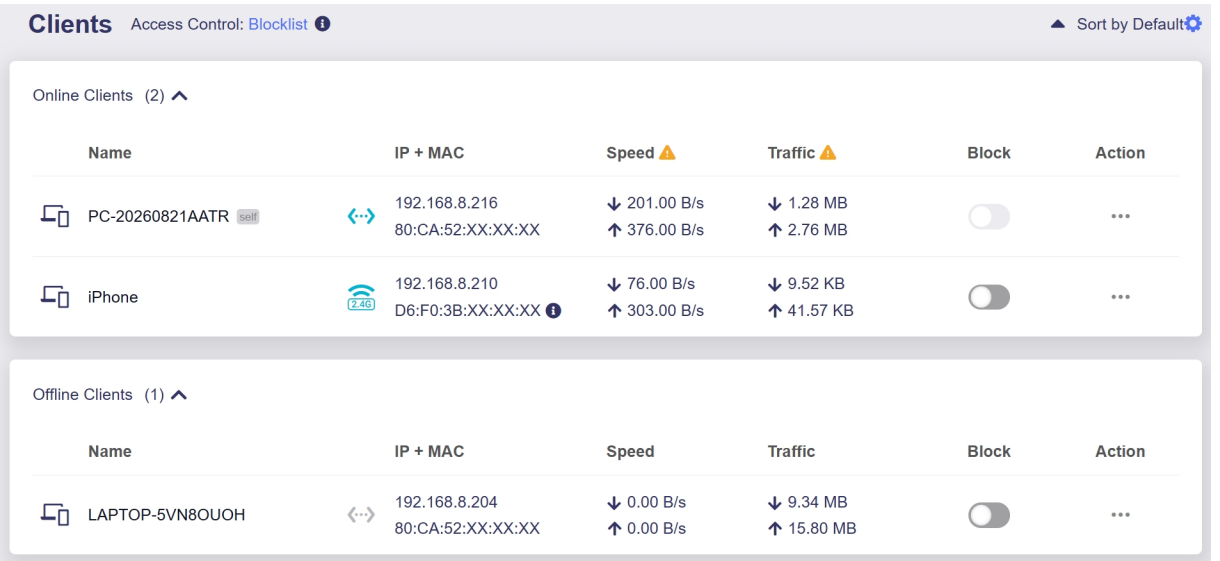
Capítulo 6

# Clientes

Este capítulo lo guía para ver los detalles de los dispositivos conectados y administrar sus conexiones.

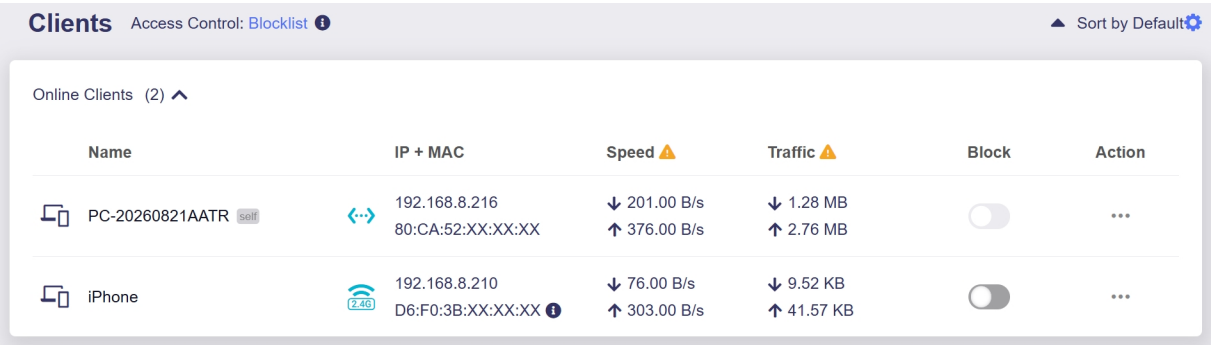
Inicie sesión en el enrutador’s web admin panel y navegue hasta **CLIENTES**.

La página Clientes muestra información sobre los dispositivos conectados, incluido el nombre del dispositivo, el tipo de conexión, la dirección IP y MAC, la velocidad y el tráfico, ordenados de izquierda a derecha. También proporciona acceso rápido a reservar IP, bloquear cliente o realizar otras acciones.




- **Clientes en línea**: Se refiere a los dispositivos actualmente conectados a la red del enrutador.
- **Clientes sin conexión**: se refiere a dispositivos que se han conectado previamente al enrutador pero que ahora están desconectados de la red.

# 6.1 Detalles del dispositivo




1. **Nombre del dispositivo**

   La primera columna muestra el nombre del dispositivo y tipo, que depende del nombre de host del operador del dispositivo. El icono azul junto a el nombre del dispositivo representa el método de conexión, indicating que el dispositivo está conectado al enrutador a través de un Ecable Ethernet.

2. **Dirección IP y MAC**

   La segunda columna enumera las direcciones IP y MAC del dispositivo conectado. Si los dispositivos conectados utilizan direcciones MAC aleatorias , aparecerá un, indicando que se trata de una dirección MAC aleatoria.




   Yof el segundo carácter de la dirección MAC es 2, 6, A o E (Ignorar mayúsculas y minúsculas), se considera como una dirección MAC aleatoria. Sin embargo, algunos dispositivos pueden usar una regla diferente para generar una dirección MAC aleatoria, por lo que este método de detección puede no ser preciso.

3. **Velocidad**

   La tercera columna muestra la velocidad de Internet del dispositivo conectado. Laes velocidad representa la velocidad promedio durante el pasado 3 minutos. El sistema comienza a calcular la velocidad promedio cuando se abre esta página (por ejemplo, si la página solo ha estado abierta durante 10 segundos, la velocidad promedio se basará en solo 10 segundos de datos).

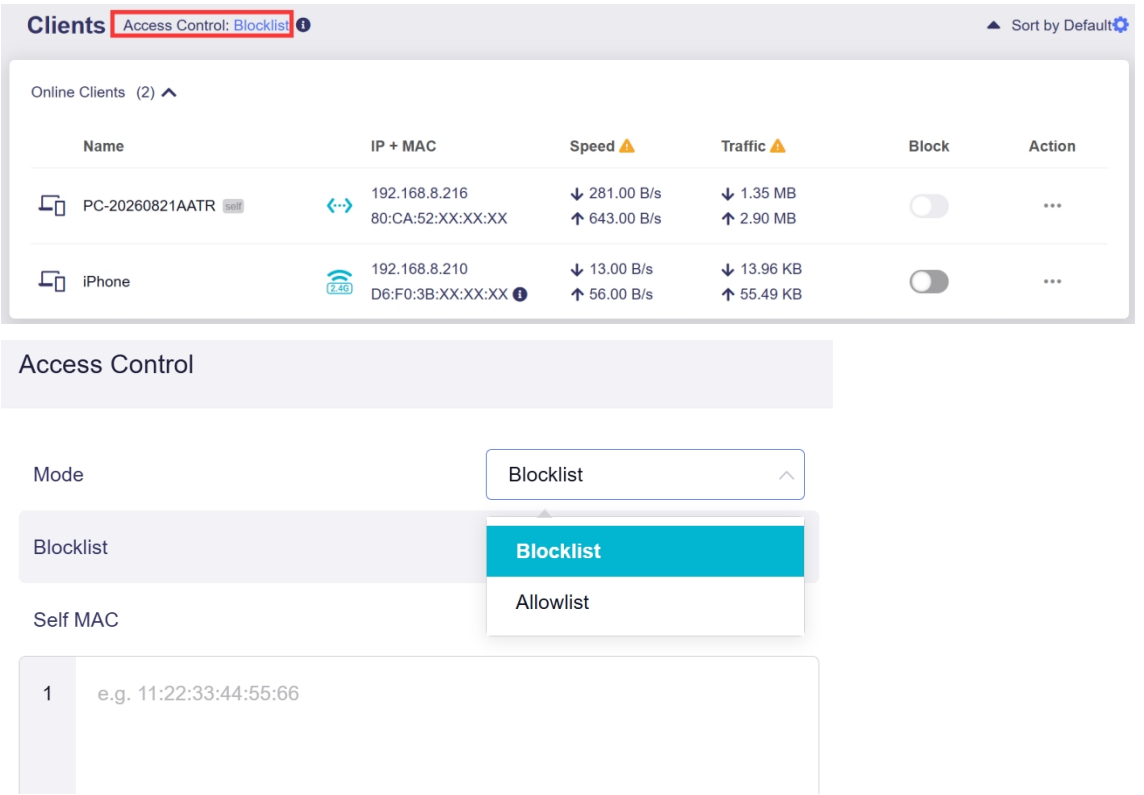
4. **Tráfico**: La cuarta columna muestra el tráfico de Internet de el dispositivo conectado.

5. **Reservar IP**

En la quinta columna, puede reservar la dirección IP para dispositivo conectado con un clic. Cuándo habilitado, siempre recibirá la misma dirección IP cada vez que se conecte a el enrutador.

6. **Lista de bloqueo**

En la sexta columna, puede bloquear dispositivos conectados específicos con un clic. La la regla de control de acceso está predeterminada en Lista de bloqueo, y puede cambiarla a Lista de permitidos desde la parte superior si es necesario.

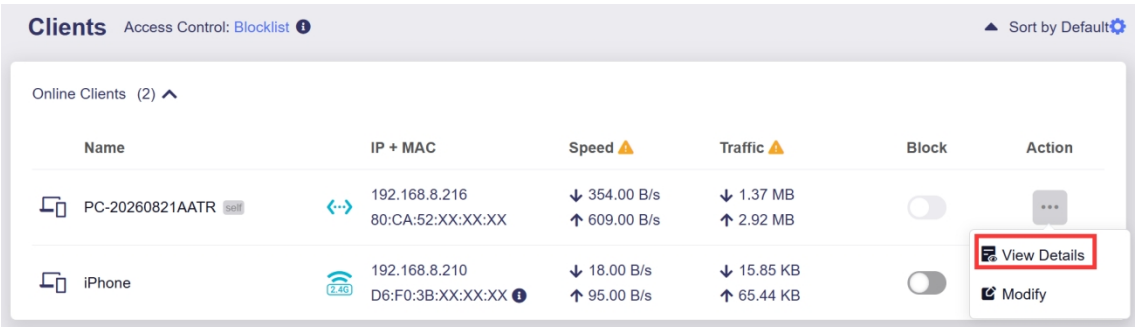


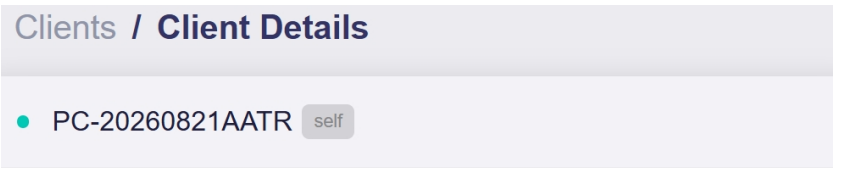

- **Lista negra**: dispositivos con direcciones MAC en la lista negrano puede conectarse a este enrutador. Tenga en cuenta que el bloqueo del cliente se basa en la dirección MAC del dispositivo. Si el dispositivo bloqueado usa una dirección MAC diferente la próxima vez, aún podrá conectarse al enrutador.
- **Lista de permitidos**: solo los dispositivos con direcciones MAC específicas pueden conectarse a este enrutador, adecuado para dispositivos IoT y redes empresariales gestión.

## 6.2 Acción

1. **Ver detalles**

   Haga clic en el icono de tres puntos en la **Acción** columna y haga clic en **Ver detalles** en el menú desplegable para ver los detalles del dispositivo en una sola página.

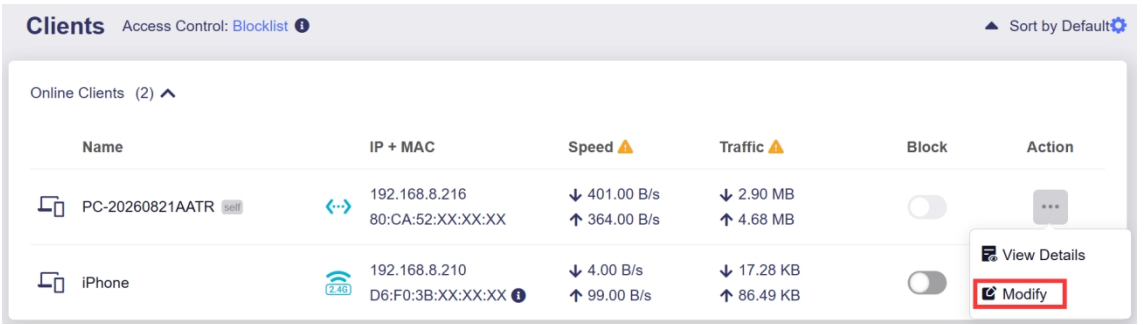


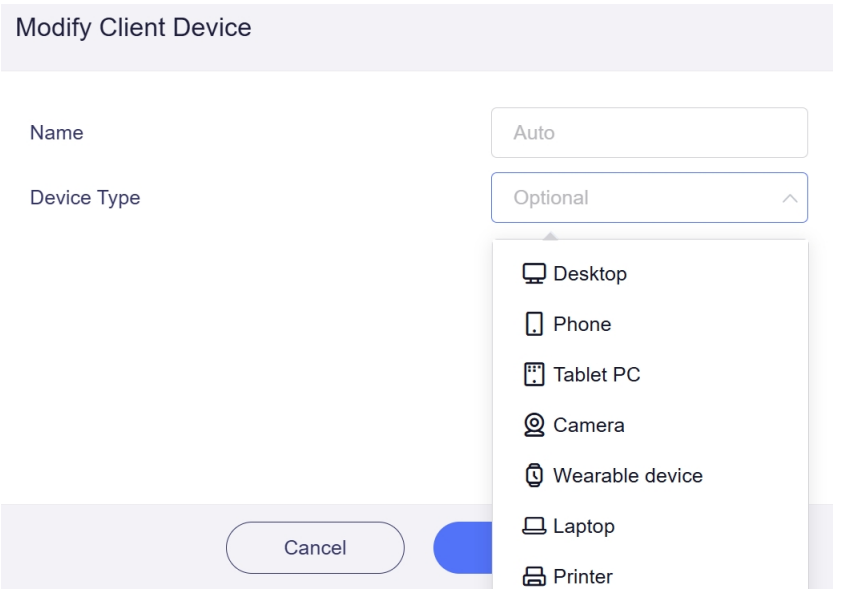




| | |
|---|---|
| Hostname | PC-20260821AATR |
| Connection Method | Ethernet |
| MAC | 80:CA:52:XX:XX:XX |
| Speed | 345.00 B/s<br>489.00 B/s |
| Traffic | 1.40 MB<br>2.95 MB |
| Block | OFF |
| IP Address | 192.168.8.216 |

2. **Modificar**

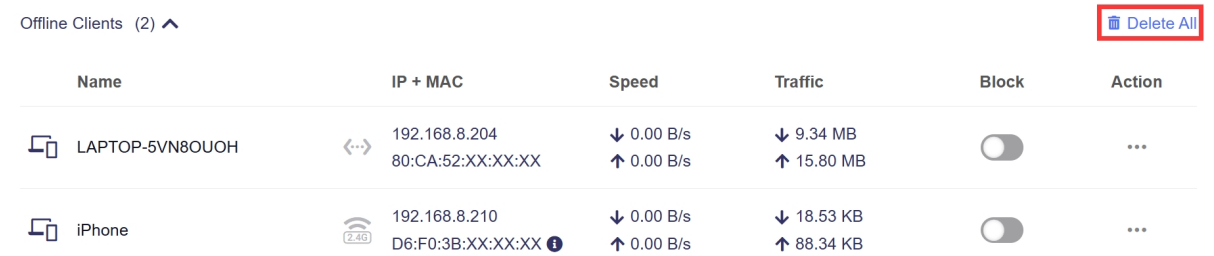
Haga clic en icono de tres puntos en la columna **Acción** y haga clic en **Modificar** desde menú desplegable para modificar el nombre y tipo del dispositivo.



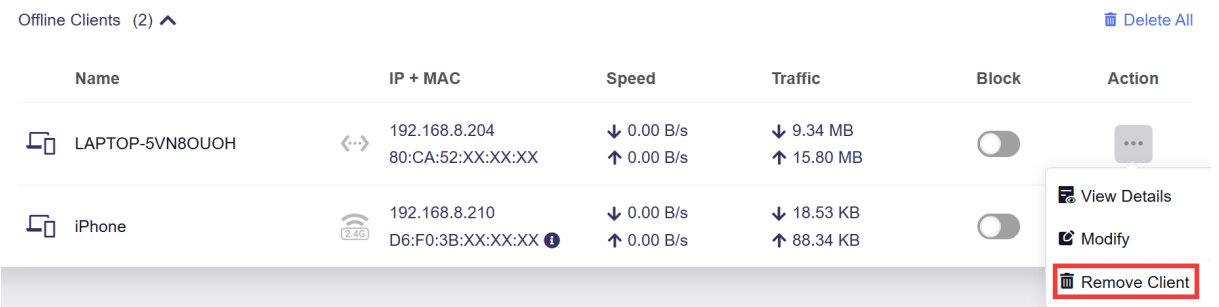



## 6.3 Eliminar clientes

Yon el **Clientes sin conexión**, puede hacer clic en **Eliminar todo** en la esquina superior derecha para eliminar todos clientes sin conexión.

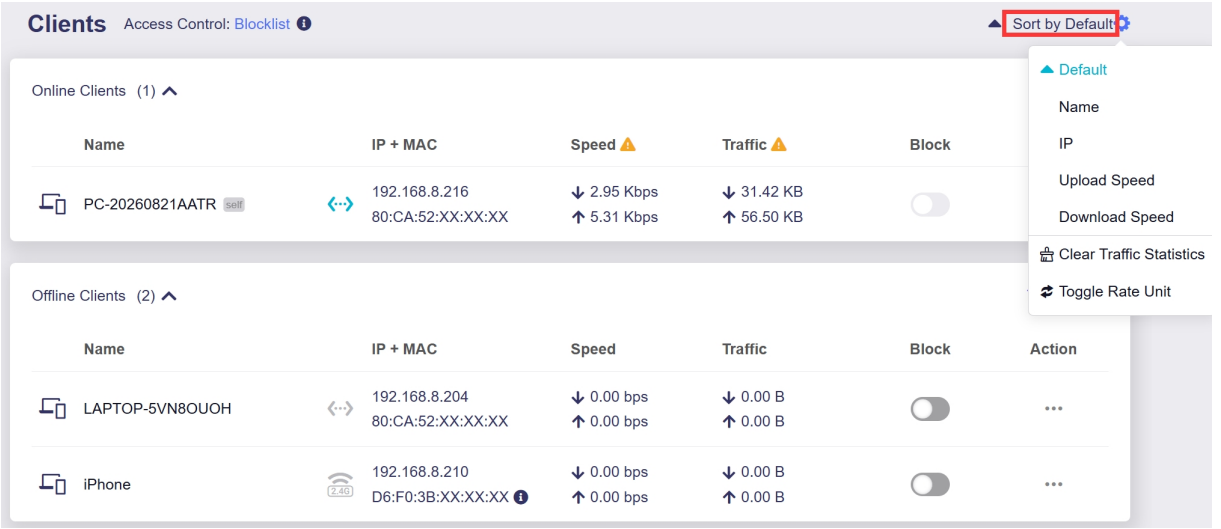



Si desea eliminar un cliente específico, haga clic en el ícono de tres puntos en la columna **Acción**, luego haga clic en **Eliminar cliente** en el menú desplegable.



## 6.4 Ordenar

Puede configurar la regla de clasificación de dispositivos para la página Cliente en el arriba esquina derecha.




La clasificación predeterminadaing es la siguiente:

- El yo-dispositivo (es decir, el dispositivo que está utilizando para acceder al panel de administración del enrutador') siempre aparece en la parte superior.
- En el **Oen línea Cclientes** sección, los dispositivos aparecen más arriba si se conectaron antes.
- En la línea **ApagadoCclientes**, los dispositivos aparecen en una lista más alta si desconectados antes.

Además de las reglas de clasificación, el menú desplegable también proporciona las siguientes funciones:

- **Borrar estadísticas de tráfico**: borre las estadísticas de tráfico para todos los clientes en línea con un solo clic. Una vez aplicada, la columna de estadísticas de tráfico se restablecerá a cero y luego se reiniciarán las estadísticas.




- **Alternar unidad de tarifa**: cambie la unidad de velocidad para la columna de velocidad entre **KB/s** y **Kbps**.

Capítulo 7

# Servicios en la nube

Este capítulo presenta el servicio en la nube: GoodCloud.

## 7.1 GoodCloud

GL.iNet GoodCloud es un plataforma diseñada para simplificar la implementación y administración remota de dispositivos conectados. proporciona una manera fácil de remota acceder y administrar GL.enrutadores iNet. Al centralizar los dispositivos de red en la nube, los usuarios pueden realizar de manera eficiente tareas de administración por lotes, como implementar configuraciones de red y ejecutar software actualizaciones. También pueden acceder de forma remota al panel de administración web del enrutador o conectarse al terminal del enrutador a través de SSH, logrando una administración de dispositivos de red interregional y de extremo a extremo.

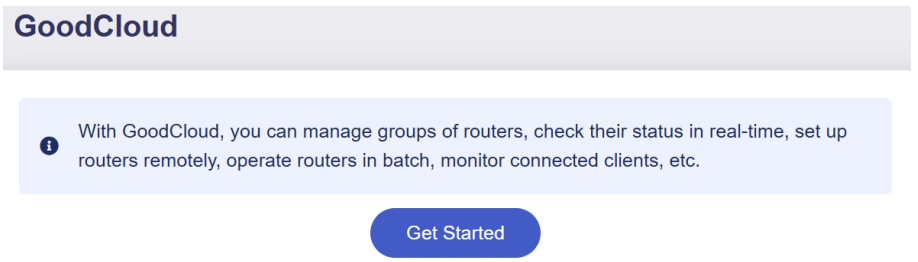
Con GoodCloud, puede:

- Verificar el estado de su enrutador'en tiempo real
- Madministrar grupos de enrutadores
- Configurar enrutadores de forma remota
- Monitorr clientes conectados
- Operar enrutadores por lotes
- Establecer Sitio-a-Sitio conexión

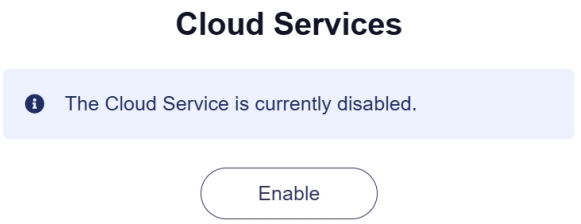
Algunas funciones están disponibles en el plan Enterprise y VAR (revendedor de valor agregado). Consulte aquí para obtener más detalles.

### 7.1.1 Habilitar GoodCloud

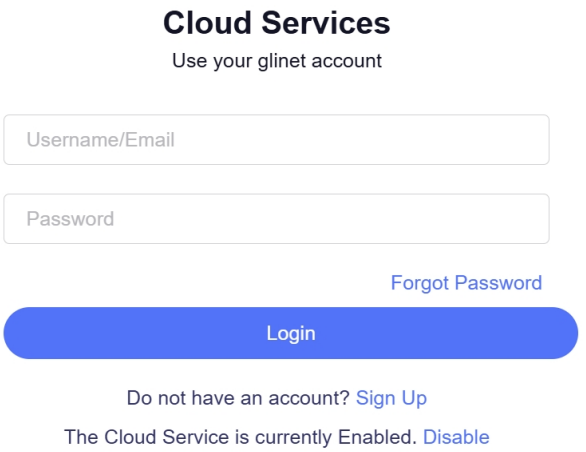
1. Inicie sesión en el panel de administración web de su enrutador', navegue hasta **SERVICIO EN LA NUBE** > **GoodCloud**, y click **Obtener Started.**



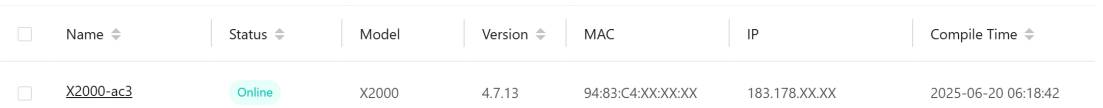

2. En la ventana emergente, haga clic en **Activar**.




3. Log en con su cuenta GL.iNet. Si no’no tiene una cuenta, regístrese para obtener una e inicie sesión.



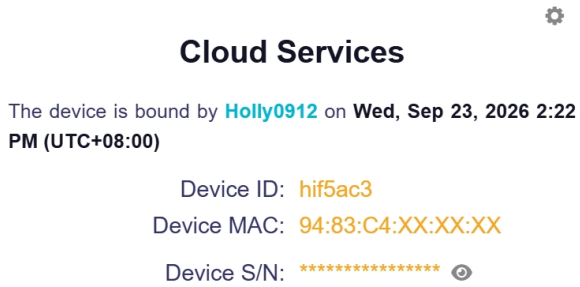

4. Confirme su cuenta y la información del dispositivo en el siguiente paso, luego haga clic en **Enlazar**. Puede iniciar sesión en la plataforma GoodCloud para verificar que su enrutador esté vinculado a su cuenta.



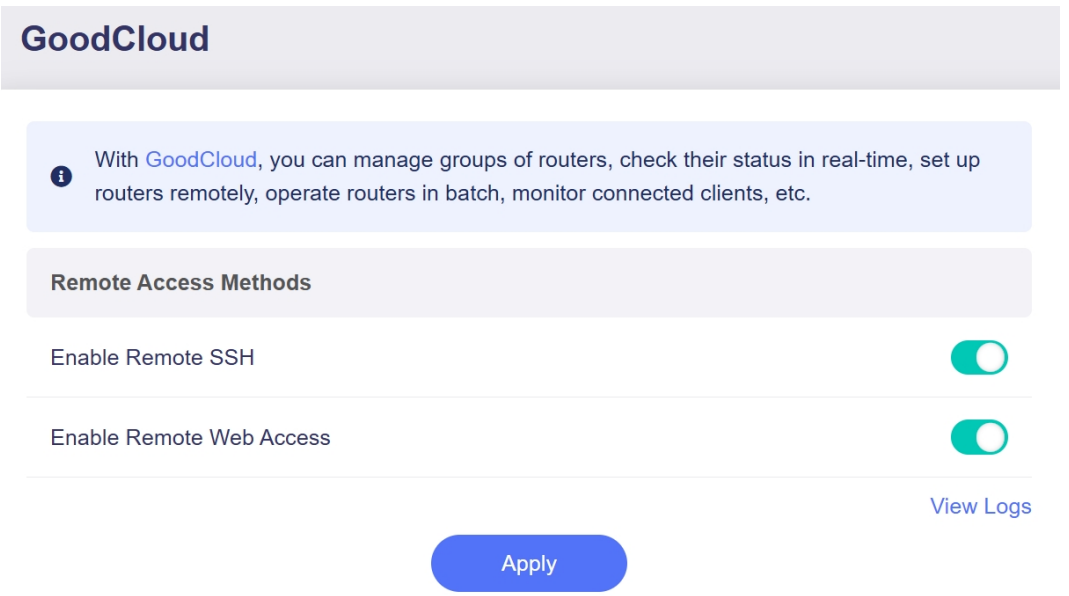

**Consejos**:

- Los pasos de vinculación de GoodCloud difieren según la versión de firmware.
- Si no recibe el correo electrónico de verificación durante el registro, revise su carpeta de correo no deseado o vuelva a intentarlo más tarde. Para más ayuda, contáctenos en support@gl-inet.com.

5. Después de vincular con éxito, haga clic en el **icono de nube** en la esquina superior derecha del panel de administración web. Verá los detalles del dispositivo vinculado, incluida la cuenta vinculada, la fecha de vinculación, la ID del dispositivo, la MAC del dispositivo y el S/N del dispositivo.




6. En el panel de administración web del enrutador', nnavegue a **SERVICIOS EN LA NUBE > GoodCloud** y habilite el acceso remoto al panel de administración web y al terminal del enrutador vinculado'. Esto es particularmente útil para la administración remota y la resolución de problemas.

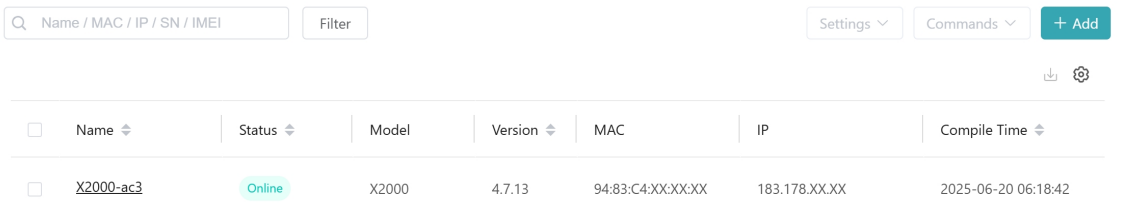



- **Acceso remoto SSH**: acceda de forma remota al terminal del enrutador desde GoodCloud usando SSH.
- **Acceso web remoto**: Remotely accede a la web del enrutador admin panel de GoodCloud a través de HTTP/HTTPS.
- **Ver registros**: Redirigir a la página de registro y mostrar la nube log.

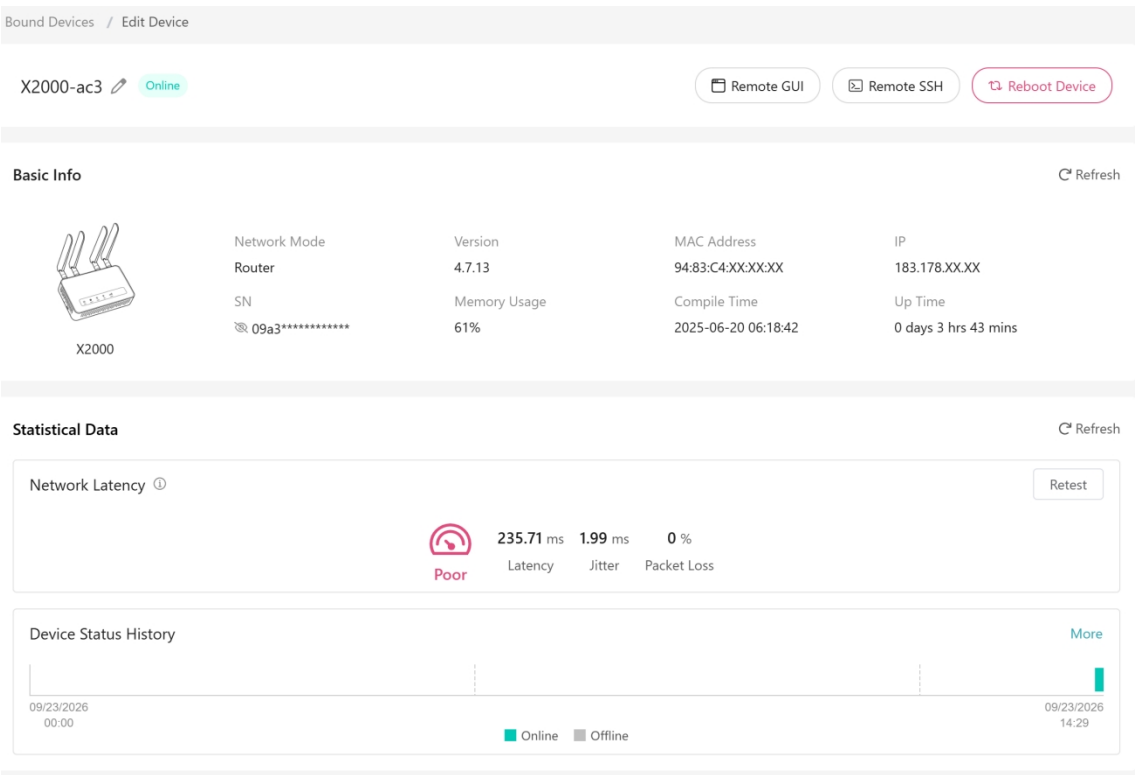
## 7.1.2 Administrar el enrutador

### Consultar los detalles del dispositivo

Inicie sesión en la plataforma GoodCloud y navegue a **Dispositivos** > **Dispositivos vinculados**. Ypuedes ver puede ver el dispositivo's información básica, como nombre de host, estado (en línea/fuera de línea), modelo, versión de firmware, y MAC dirección.

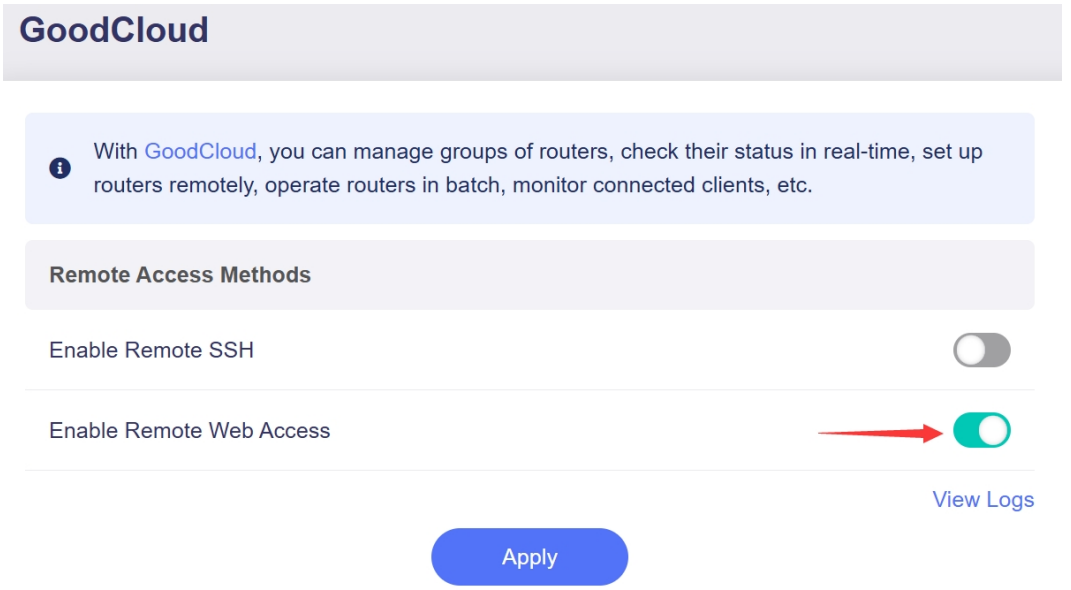



Haga clic el nombre del dispositivo para ingrese a la página de detalles del dispositivo, que muestrainformación básica, datos estadísticos, descripción general de la red, lista de clientes y cronograma. También puede realizar operaciones avanzadas, como acceso remotolying al enrutador, y reiniciando el dispositivo.

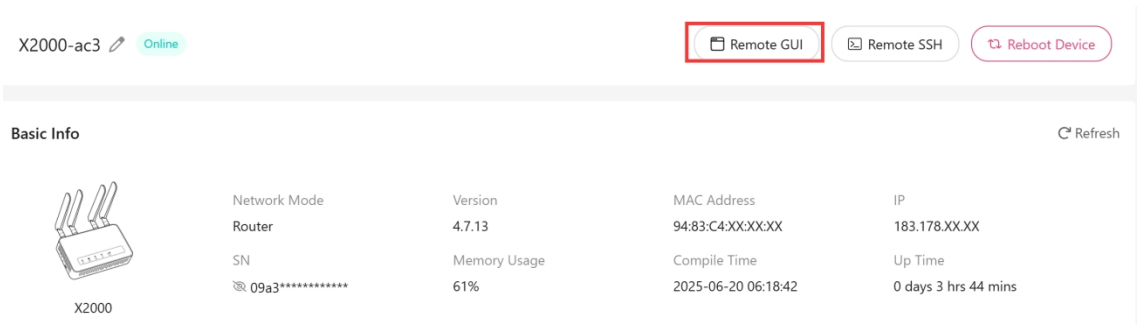


## Acceso web remoto

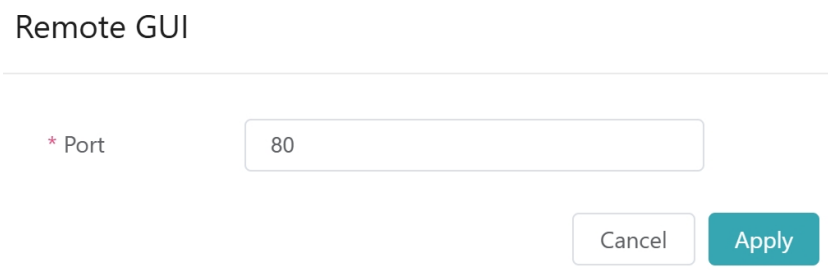
1. Inicie sesión en el enrutador'panel de administración web, navegue hasta **SERVICIOS EN LA NUBE** > **GoodCloud**, habilite **Acceso web remoto**, luego haga clic en **Aplicar**.



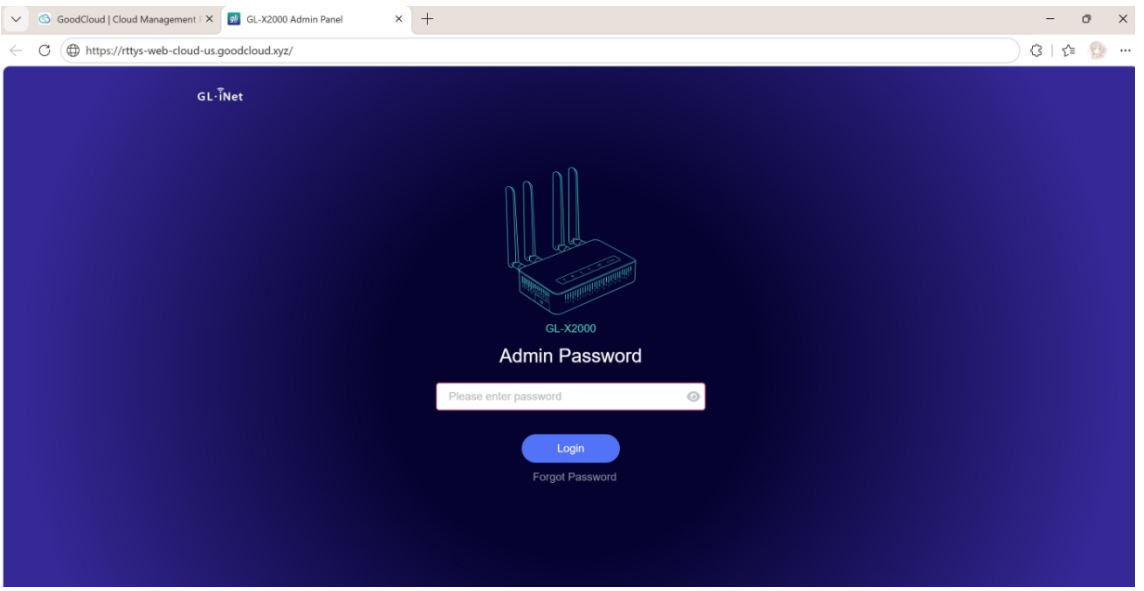

2. Inicie sesión en la plataforma GoodCloud y navegue hasta **Dispositivos** > **Dispositivos vinculados**. Haga clic en el dispositivo al que desea acceder e ingresará a la página de detalles del dispositivo.
3. En la página de detalles del dispositivo, haga clic en **Remoto GUI** botón en la esquina superior derecha.




4. Seleccione el protocolo y el puerto de transferencia. Los valores predeterminados son **HTTP** y Puerto **80**. Puede cambiar el protocolo a HTTPSpuedes cambiar el protocolo a HTTPS si es necesario y el puerto cambiará automáticamente a 443. Luego haga clic en **Aplicar**.

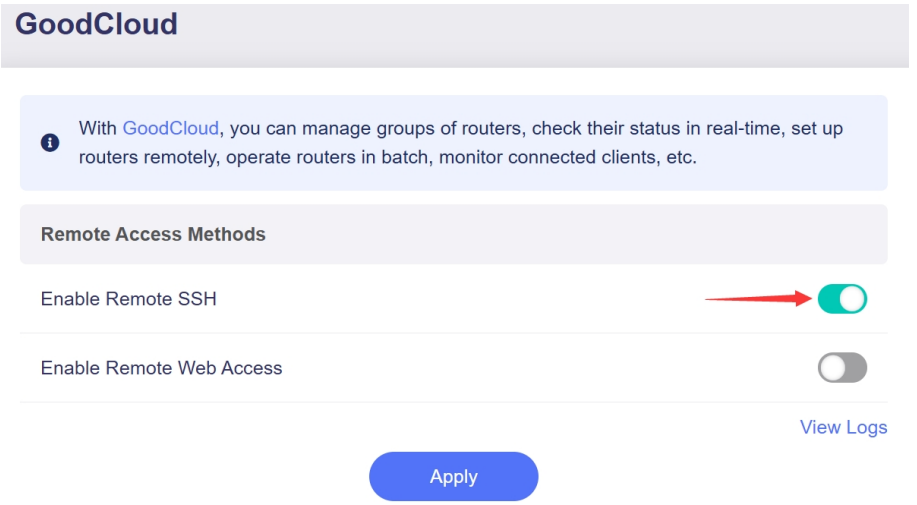



5. Será redirigido a la página de inicio de sesión del enrutador'. Ingrese la contraseña de administrador para acceder de forma remota al panel de administración web del enrutador'.

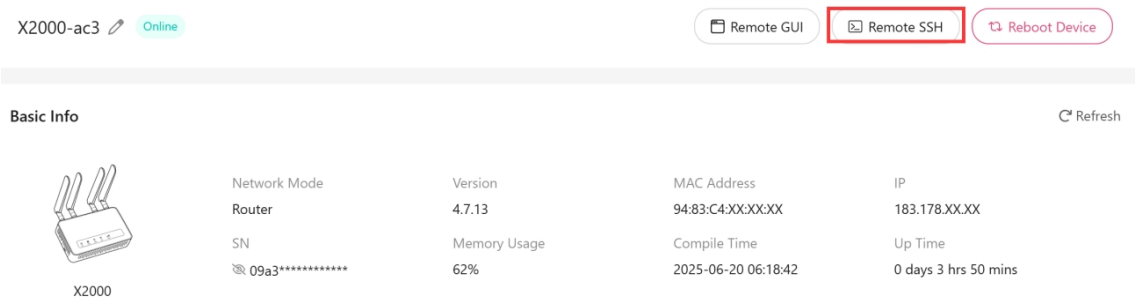


## Acceso remoto al terminal

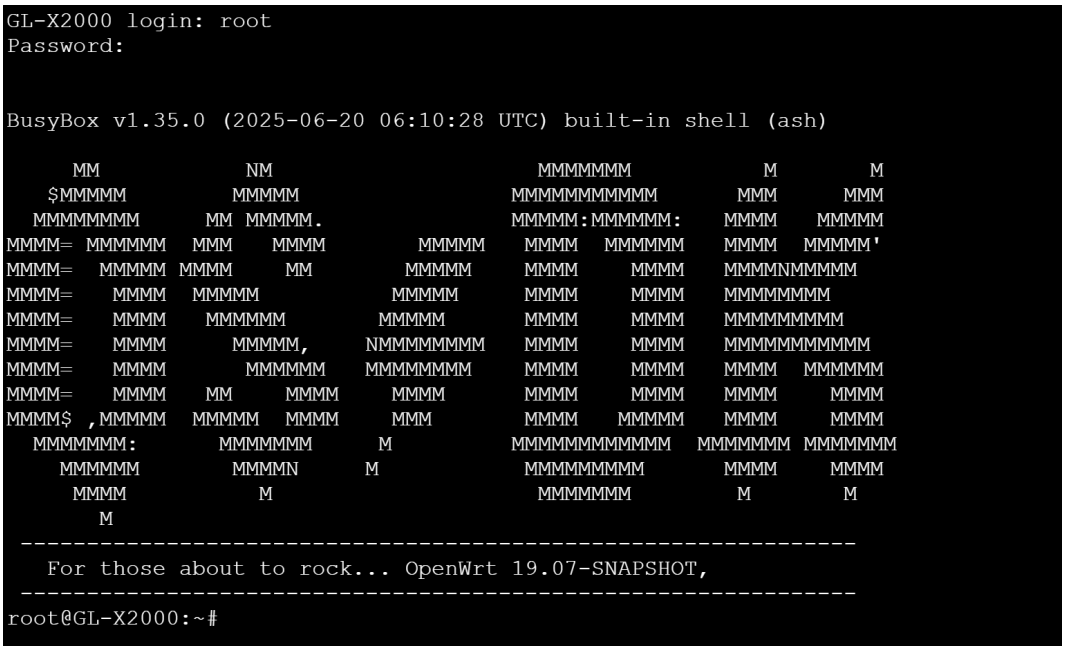
1. Inicia sesión en panel de administración web del enrutador', navegue hasta **SERVICIOS EN LA NUBE** > **GoodCloud**, habilite **Acceso remoto SSH**, luego haga clic en **Aplicar**.




2. Inicie sesión en la plataforma GoodCloud y navegue hasta **Dispositivos** > **Dispositivos vinculados**. Haga clic en el dispositivo al que desea acceder e ingresará a la página de detalles del dispositivo.
3. En la página de detalles del dispositivo, haga clic en **Acceso remoto SSH** en la esquina superior derecha.

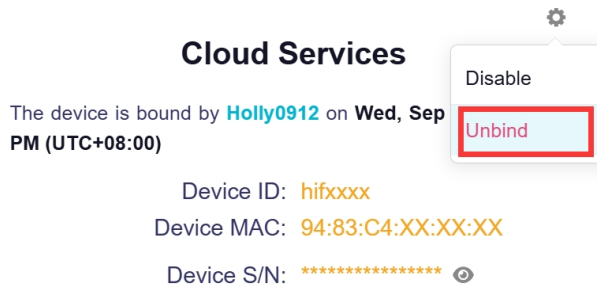



4. Inicie sesión como **root** e ingrese la contraseña para acceder al terminal de su enrutador.

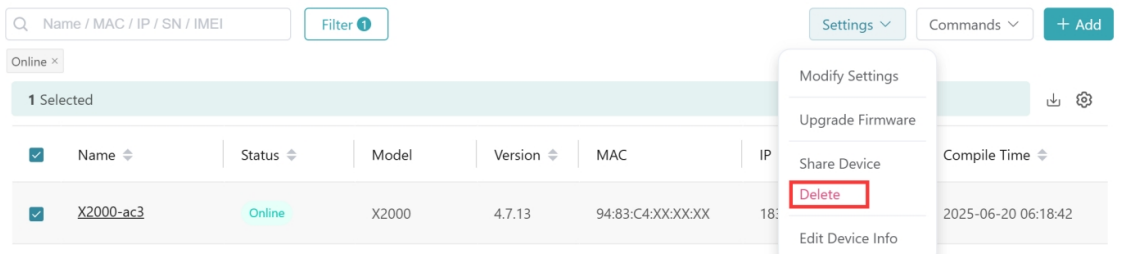

GL-X2000 login: root
Password:
BusyBox v1.35.0 (2025-06-20 06:10:28 UTC) built-in shell (ash)
For those about to rock... OpenWrt 19.07-SNAPSHOT,
root@GL-X2000:~#

## 7.1.3 Desvincular el dispositivo

En el panel de administración web del enrutador, haga clic en el icono de nube en la esquina superior derecha. En el menú desplegable, haga clic en el ícono de ajustes y seleccione **Desvincular**. Su dispositivo se desvinculará de su cuenta de GoodCloud.

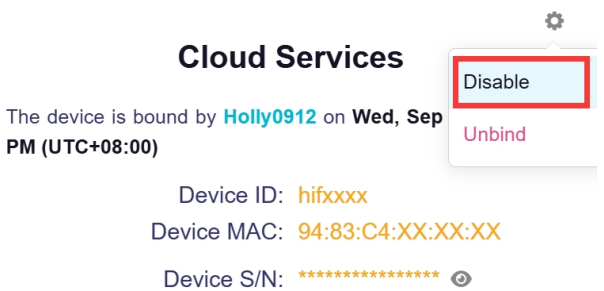



Como alternativa, inicie sesión en la plataforma en la nube y navegue hasta **Dispositivos** > **Dispositivos vinculados**. Seleccione el dispositivo que desea desvincular, haga clic en **Configuración** en la esquina superior derecha y luego seleccione **Eliminar**. Su dispositivo se desvinculará. su cuenta de GoodCloud.




## 7.1.4 Desactivar GoodCloud

Si ya no desea que el dispositivo esté conectado a la nube, haga clic en el icono de nube en la esquina superior derecha. En el menú desplegable, haga clic en el ícono de ajustes y seleccione **Desactivar**.




El servicio en la nube se desactivará.

Capítulo 8

# Conozca la VPN

Este capítulo presenta VPN conceptos y escenarios de uso común.

# 8.1 Introducción

## VPN

VPN, abreviatura de Virtual Private Network, establece una red cifrada y privada túnel entre un dispositivo y un servidor remoto, protegiendo la transmisión de datos y permitiendo el acceso seguro a redes privadas o restringidas.

## Enrutador VPN

Un enrutador VPN cuenta con funcionalidad VPN preinstalada, que protege todos los dispositivos conectados a través de VPN. A diferencia de configurar una VPN en dispositivos individuales, configurar el enrutador como un cliente VPN enruta todo el tráfico a través de un túnel cifrado, sin necesidad de una configuración separada por dispositivo. Esto protege varios dispositivos a la vez, ahorra tiempo, y garantiza configuraciones de VPN consistentes, reduceing riesgos de personas inadecuadas. configuración.

Los enrutadores GL.iNet admiten más de 30 servicios comerciales populares de OpenVPN y WireGuard VPN. Cargue sus archivos de configuración de VPN para activar la conexión VPN para una red segura. Consulte aquí para obtener la lista completa de proveedores de VPN externos.

## OpenVPN

OpenVPN es un protocolo VPN de código abierto que utiliza seguridad basada en SSL/TLS para conexiones de punto a sitio o de sitio a sitio. Admite múltiples métodos de cifrado, TCP/UDP y una fácil omisión de firewall/NAT.

## WireGuard

WireGuard es un protocolo VPN ligero y rápido, más simple y eficiente que OpenVPN. Cuenta con criptografía moderna para mayor eficiencia, una pequeña base de código para una auditoría y seguridad más sencillas y algoritmos de última generación (ChaCha20/Poly1305) para cifrado e integridad de datos.

## 8.2 Escenarios de aplicación

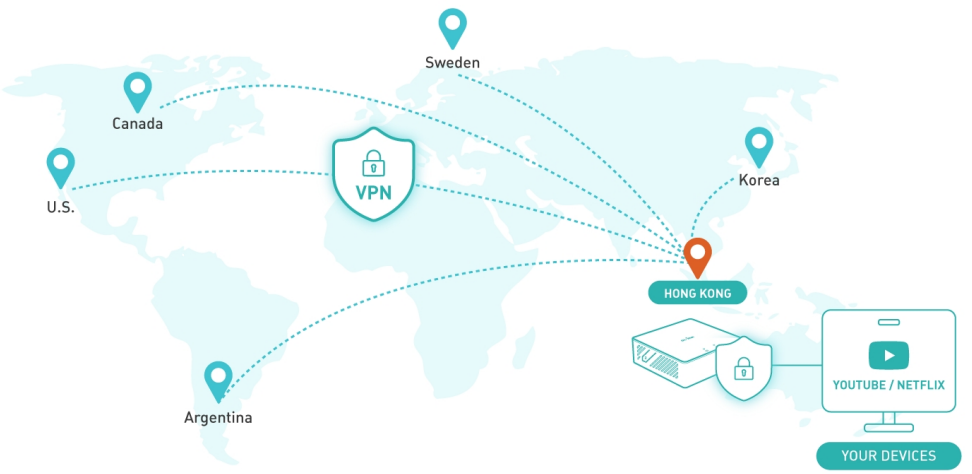
1. **Privacidad de datos personales**

   El servicio VPN es compatible con una amplia gama de dispositivos a través de nuestro enrutador, incluidos no solo computadoras portátiles, teléfonos y tabletas, sino también consolas de juegos, televisores y dispositivos de transmisión. Sus datos estarán protegidos ya sea a través de conexiones inalámbricas o por cable. Incluso puede personalizar las políticas de VPN para lograr una protección flexible para ciertos dispositivos.



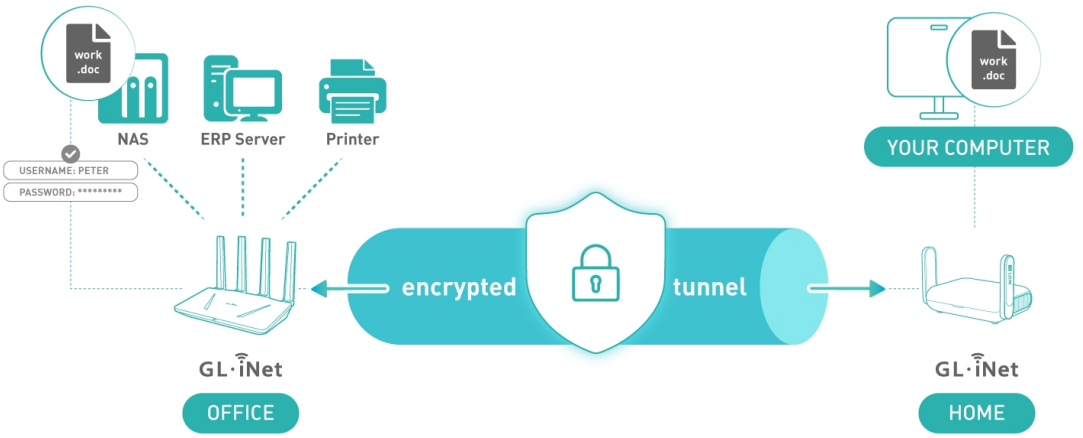

2. **Acceso sin restricciones en todo el mundo**

   El acceso a algunos sitios puede estar restringido según la ubicación. Con VPN habilitada, puedes desbloquear cualquier sitio cuando sea necesario. Al conectarse a diferentes servidores de terceros, se le asignarán diferentes direcciones IP para navegar o acceder a sitios bloqueados por región.



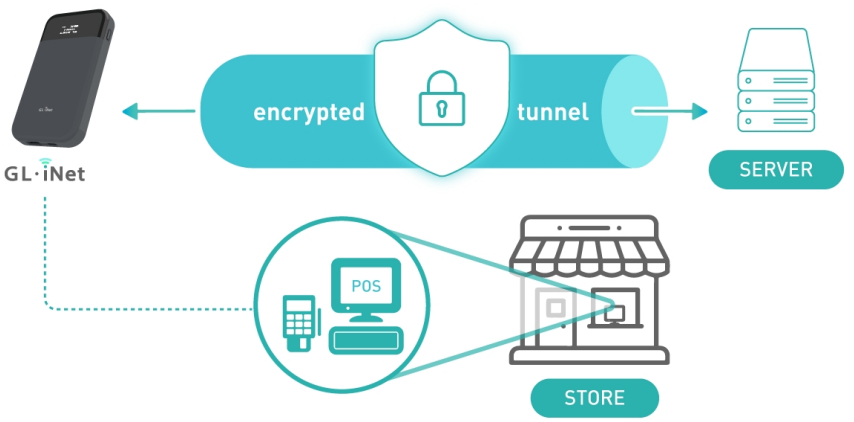
3. **Seguridad de datos para pequeñas empresas**

Muchas personas trabajan en co-espacios de trabajo o cafeterías y dependen de Wi-Fi público gratuito-Fi. Estas redes son vulnerables a los ataques de los ciberdelincuentes. Al configurar su enrutador de viaje como cliente VPN, podrá disfrutar de una conectividad segura para trabajar en cualquier lugar.




4. **Infraestructura de pago segura**

Los propietarios de pequeñas tiendas minoristas deben manejar las credenciales de pago de los clientes cuando realizan negocios en el sitio. Usando un VPN enrutador, su POS La máquinas puede cargar información de la tarjeta de crédito a través de una VPN cifrada tunnel para garantizar la seguridad del pago.



Capítulo 9

# Panel de VPN

Este capítulo presenta cómo administrar conexiones VPN a través del panel de administración web.

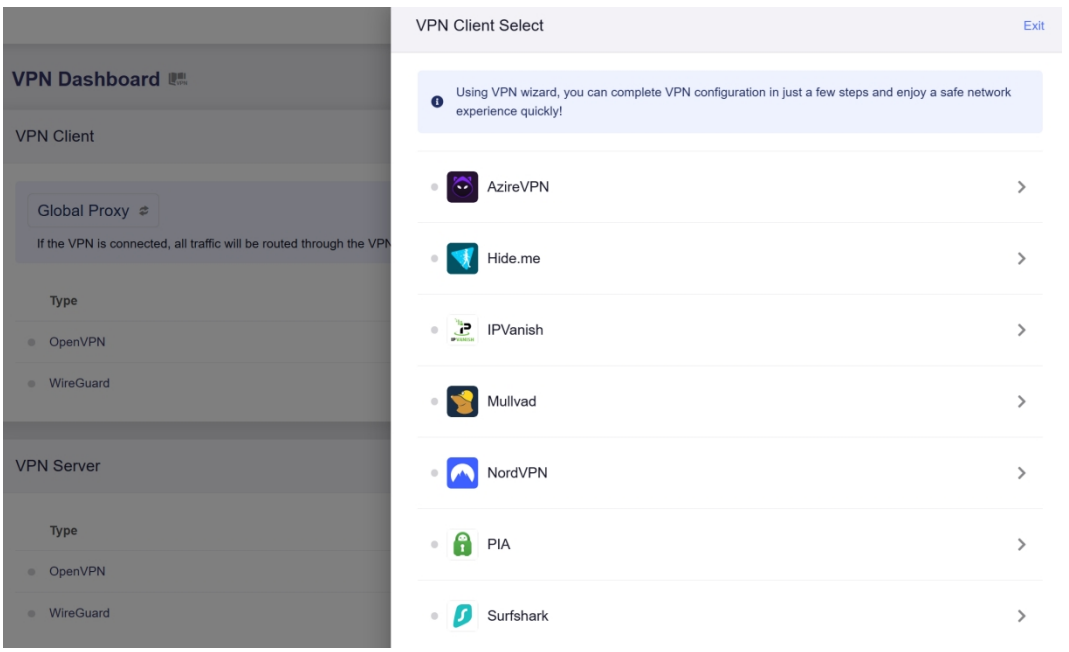
Inicie sesión en enrutador's web admin panel y navega a **VPN** > **Panel de VPN**.

Cuando el enrutador está configurado como cliente VPN activo, el panel de VPN muestra detalles de la conexión VPN, como la dirección del servidor, estadísticas de tráfico, IP virtual del cliente y registro de conexión. También le permite configurar ajustes avanzados como Bloquear tráfico que no sea VPN, Permitir acceso a WAN y Servicios de GL.iNet Usar VPN.

## 9.1 Asistente de configuración de VPN

Para empezar, click el ícono del libro en la esquina superior izquierda y siga el Asistente de configuración de VPN para completar la configuración de VPN rápidamente.



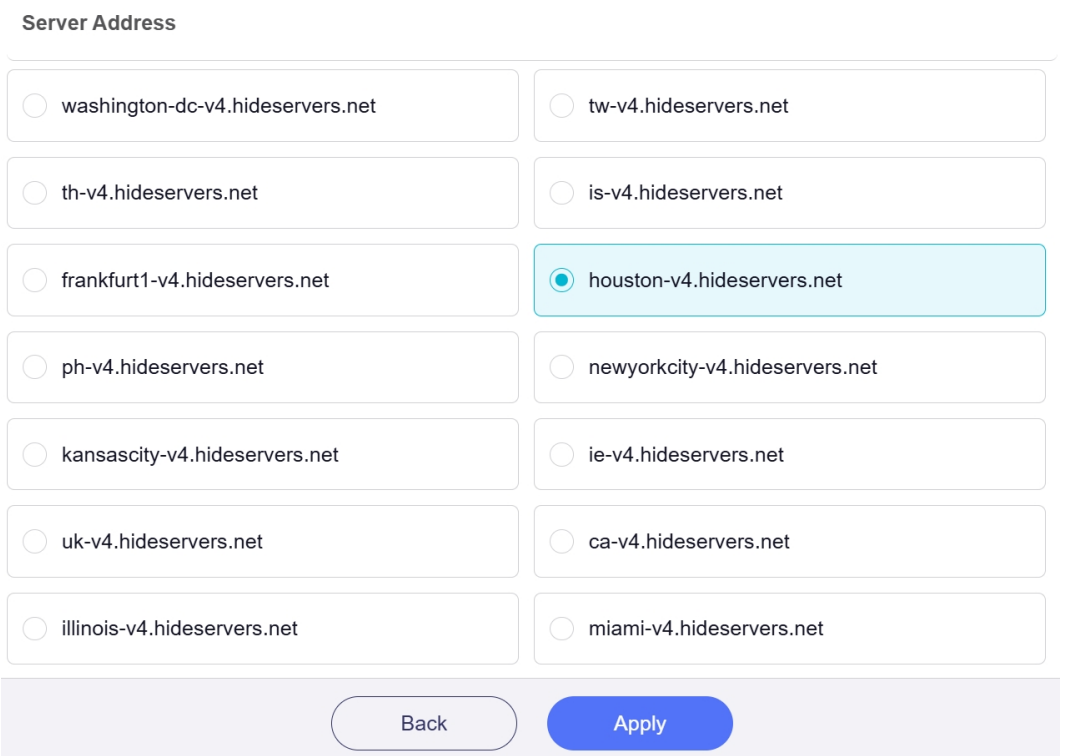



**Nota**: El Asistente de configuración de VPN es solo para los servicios VPN integrados, incluidos AzireVPN, Hide.me, IPVanish, Mullvad, NordVPN, PIA y Surfshark. Para otros proveedores de VPN, omita el asistente y vaya a **VPN** > **Cliente OpenVPN** o **Cliente WireGuard** para configurar la VPN. manualmente.

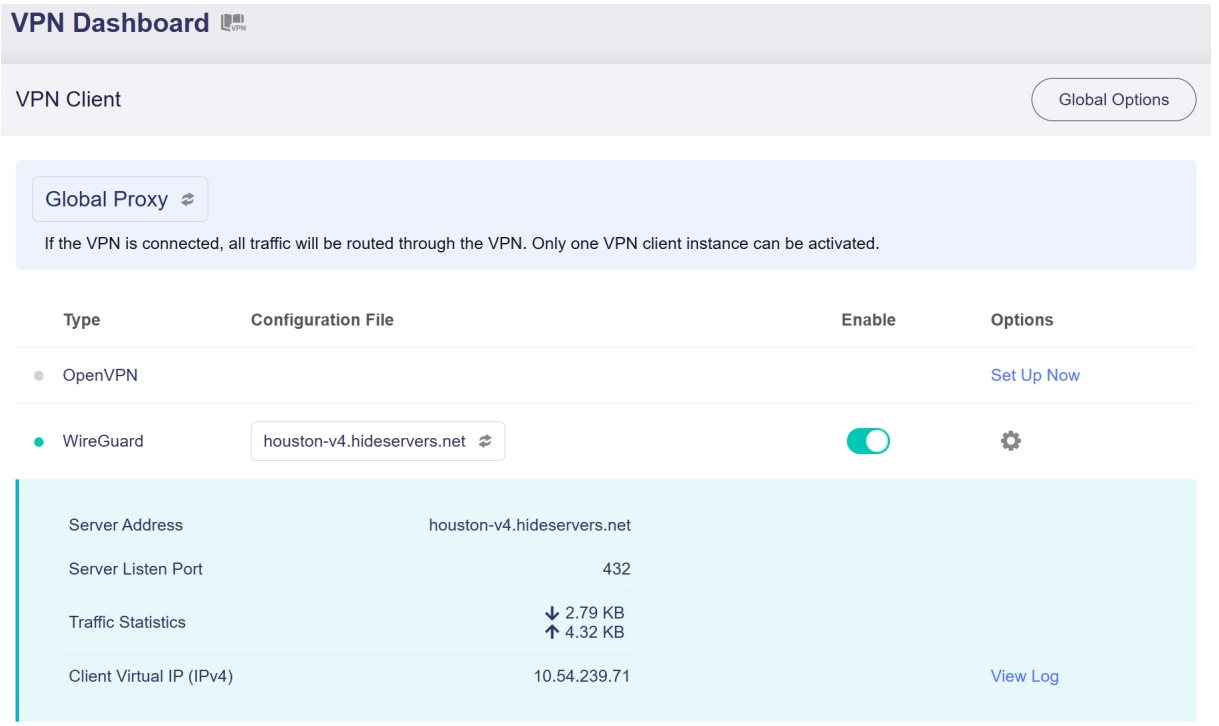
Aquí hay un ejemplo con **Hide.me**. Inicie sesión con las credenciales de Hide.me.




Seleccione un servidor VPN y haga clic en **Aplicar**. Este es el servidor al que se conectará y su dirección IP pública parecerá ser la de la ubicación del servidor seleccionado.

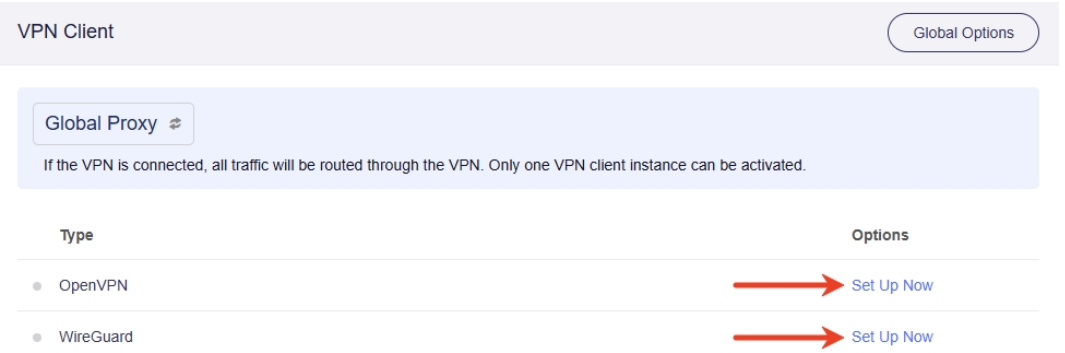


Se conectará automáticamente. Una vez conectado, vaya al **Panel de VPN**. Verá que se ha habilitado un túnel VPN, que muestra detalles que incluyen el protocolo VPN (por ejemplo, WireGuard), el archivo de configuración, la dirección del servidor, el puerto de escucha del servidor, las estadísticas de tráfico y la dirección IP virtual del cliente. También puede ver los registros de conexión en la parte inferior derecha corner.

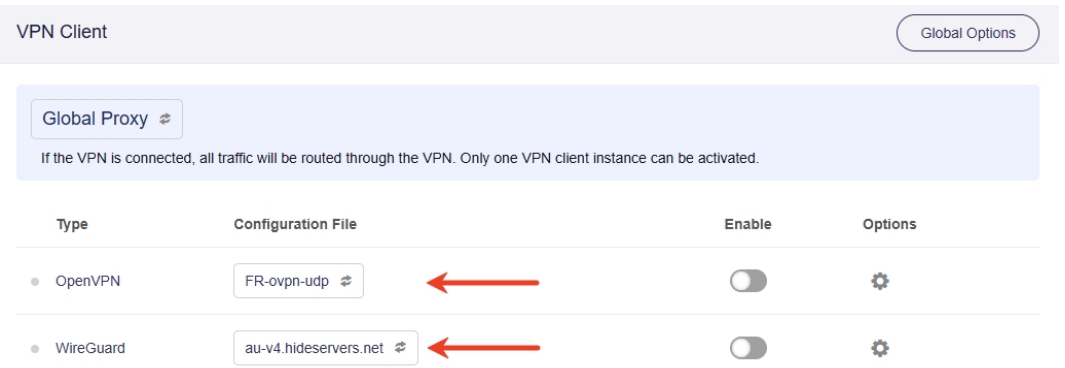


## 9.2 Cliente VPN

Cuando ingresa al **Panel de VPN** por primera vez y no hay archivos de configuración OpenVPN o WireGuard disponibles, la página se muestra de la siguiente manera. Haga clic en **Configurar ahora** y será dirigido al **Cliente OpenVPN** o **Cliente WireGuard** página para cargar sus archivos de configuración de VPN.

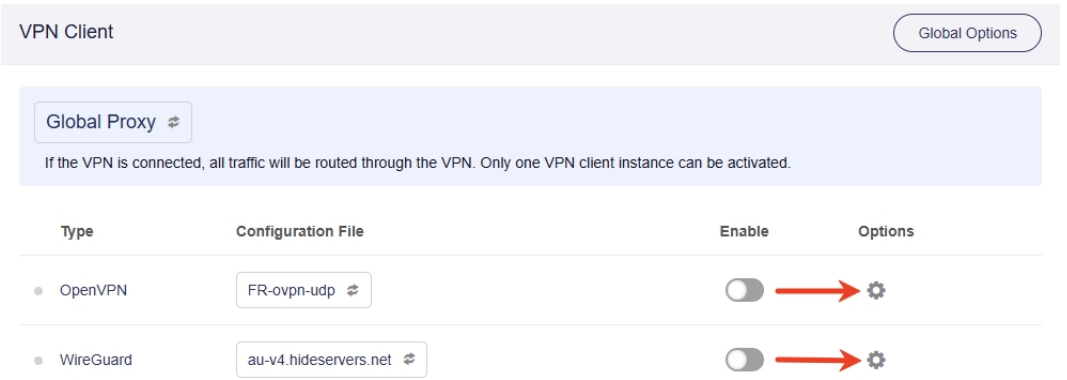



Una vez cargada, su configuración se mostrará en la columna **Archivo de configuración**. Si tiene varios archivos de configuración cargados, puede cambiar de archivo haciendo clic en el cuadro.

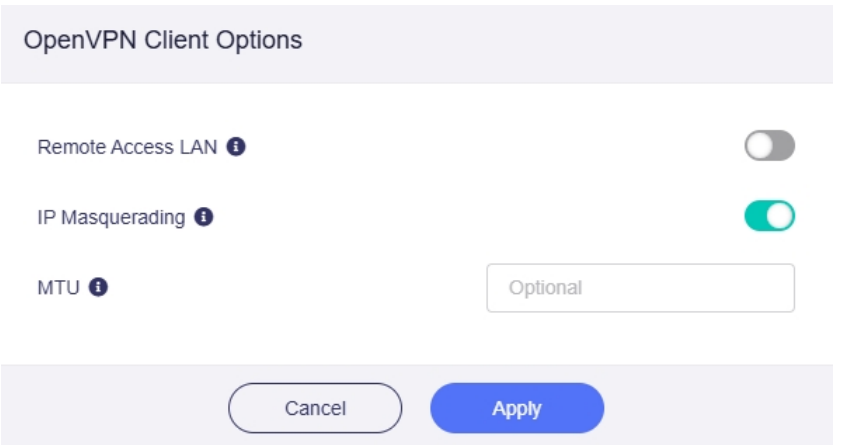


## 9.2.1 Opciones del cliente

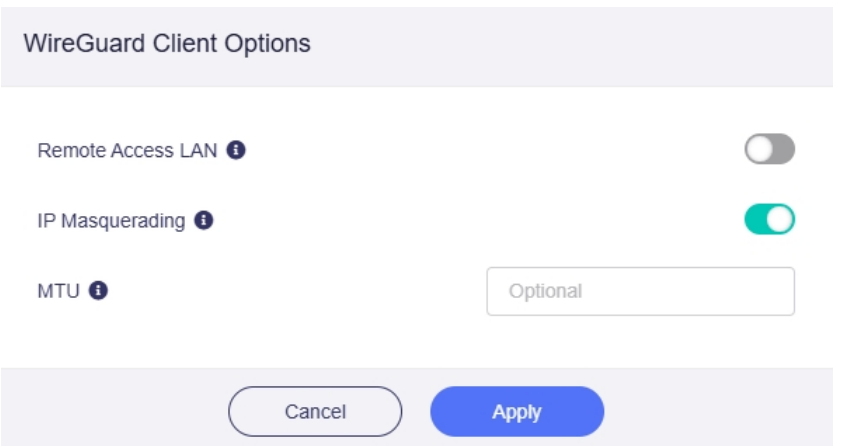
Haga clic en el ícono de ajustes a la derecha para acceder a las opciones del cliente OpenVPN o WireGuard.



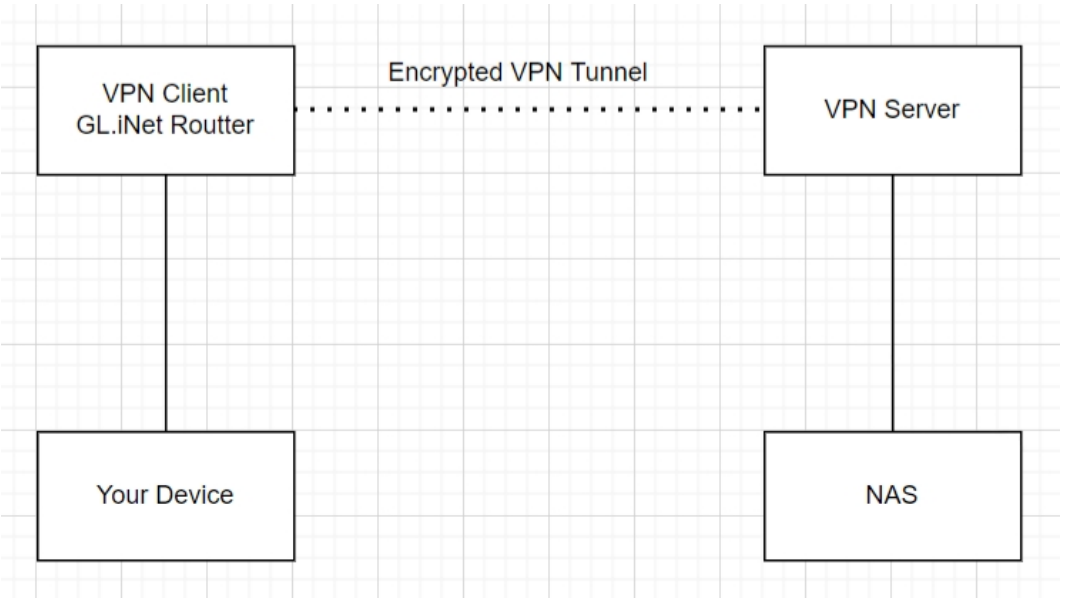

Las opciones del cliente OpenVPN se muestran a continuación.




Las opciones del cliente WireGuard se muestran a continuación.



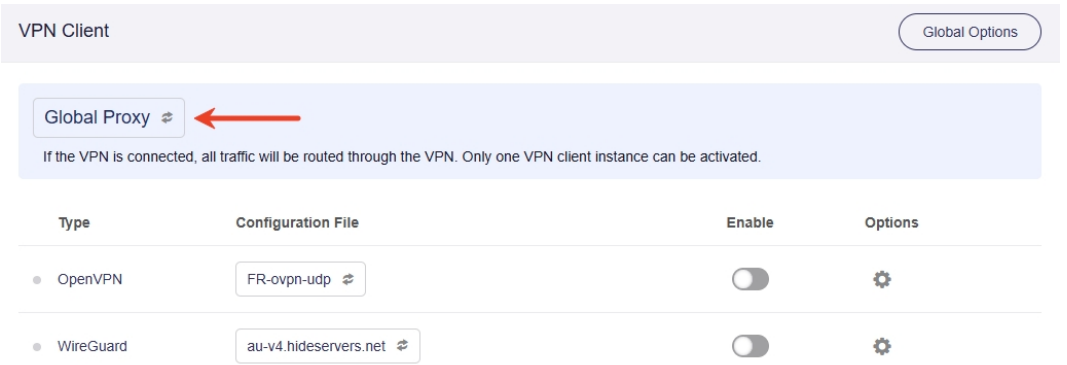
- **LAN de acceso remoto**: Si está habilitado, se permitirá el acceso remoto a este enrutador y sus dispositivos LAN a través de VPN. El servidor VPN debe anunciar una ruta a la subred LAN de este enrutador.
  Por ejemplo, como se muestra en el siguiente diagrama, el enrutador GL.iNet se ejecuta como un cliente VPN y se conecta a un servidor VPN a través del túnel VPN. Cuando esta opción está habilitada, los dispositivos del lado del servidor VPN (por ejemplo, NAS) pueden acceder tanto al enrutador GL.iNet como a sus dispositivos del lado LAN. Esto requiere que agregue una regla de enrutamiento en el servidor VPN para llegar a la subred LAN del enrutador GL.iNet.




- **Enmascaramiento de IP**: si está habilitado, las direcciones IP de origen de los clientes LAN se reescribirán en la IP del túnel VPN del enrutador. Deshabilite esto solo para configuraciones de sitio a sitio donde el par remoto conoce sus subredes LAN.
- **MTU**: abreviatura de Unidad de transmisión máxima. Esta configuración opcional le permite personalizar la MTU del túnel VPN, que anula el valor definido en el archivo de configuración.

## 9.2.2 Modo de política

El modo de proxy predeterminado para la conexión VPN es **Proxy global**. Puede hacer clic en el cuadro en la esquina superior derecha para cambiar a otros modos de proxy.




Hay tres modos de proxy disponibles: Proxy global, modo de política y modo de ruta.

1. **Proxy global**

   En este modo, todo el tráfico se enrutará a través de la VPN. Solo se puede activar una instancia de cliente VPN.

2. **Modo de política**

   Este modo se puede dividir en tres políticas.

   - **Según el dominio o IP de destino**

     En este modo, solo se enrutará el tráfico de ciertos sitios web identificados por dirección IP o nombre de dominio. VPN. Solo se puede activar una instancia de cliente VPN.
   - **Según el dispositivo cliente**

     En este modo, solo el tráfico de ciertos dispositivos LAN identificados por direcciones MAC se enrutará a través de VPN. Solo se puede activar una instancia de cliente VPN.
   - **Según la VLAN**

     En este modo, solo el tráfico de cierta VLAN se enrutará a través de VPN. Solo se puede activar una instancia de cliente VPN.

3. **Modo de ruta**

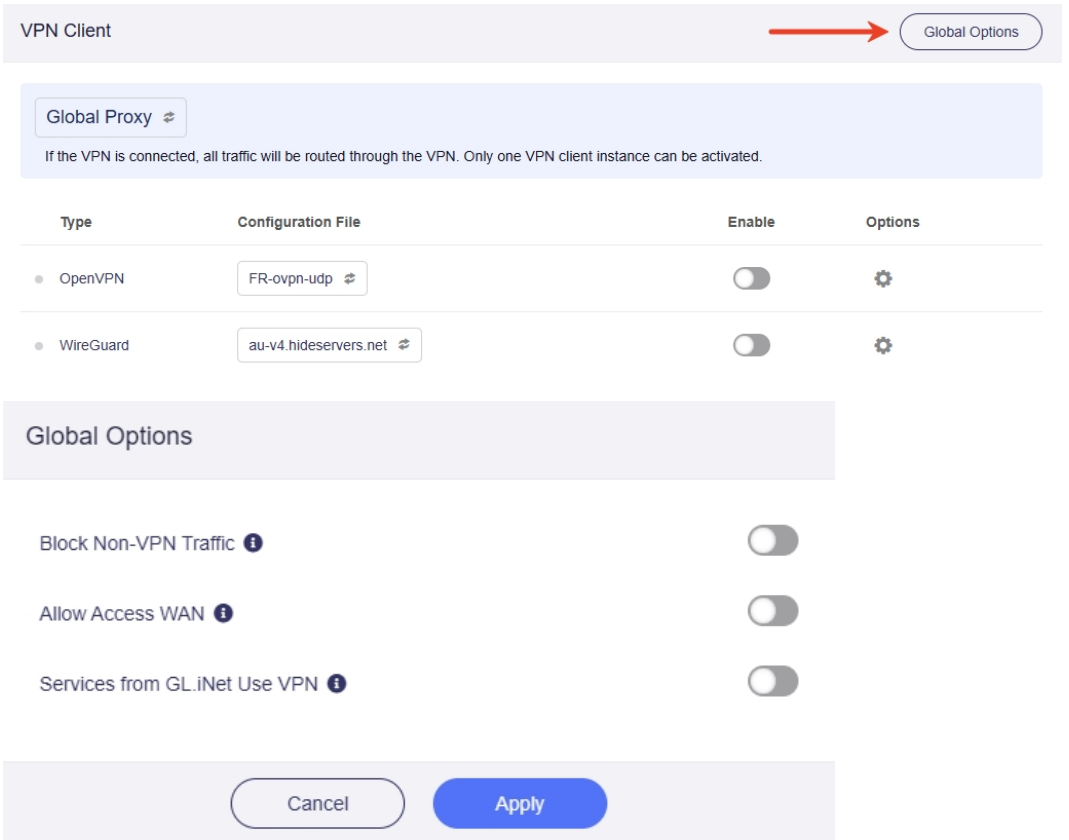
   - **Detección automática**

     Se utilizarán las reglas de enrutamiento definidas en cada archivo de configuración de cliente VPN o emitidas por el servidor VPN.

- **Personalizar reglas de enrutamiento**
  Puede configurar manualmente reglas de enrutamiento para cada instancia de cliente VPN.

## 9.2.3 Opciones globales

Haga clic en **Opciones globales** en la esquina superior derecha para configurar ajustes avanzados para su VPN client.



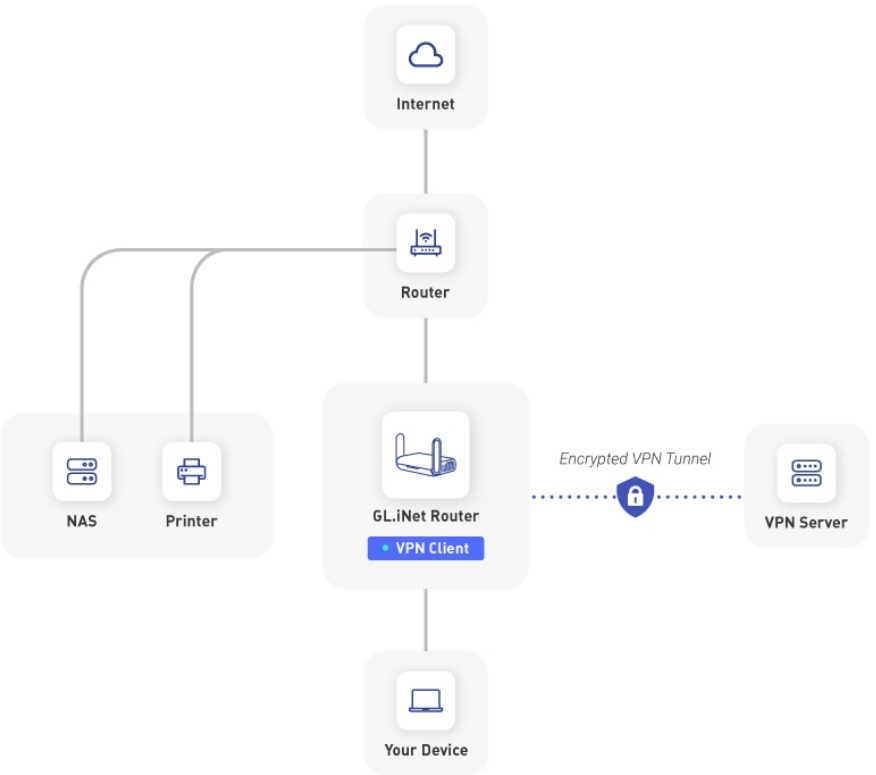

- **Bloquear tráfico que no sea VPN**: si está habilitado, todo el tráfico de Internet se ve obligado a pasar exclusivamente a través del túnel VPN y no se puede enrutar a través de otras interfaces como la WAN del ISP local. Si la conexión VPN se cae inesperadamente, todo el tráfico de Internet se bloquea completamente para evitar el retorno a la WAN normal. Esto evita fugas de VPN causadas por fallas de VPN, configuraciones incorrectas de DNS del cliente y problemas similares.

  Esta característica también se conoce como VPN Kill Switch. Evita que los datos del usuario queden expuestos en línea. Un Kill Switch típico corta automáticamente el acceso a Internet cuando falla la conexión VPN. La función Bloquear tráfico no VPN en los enrutadores GL.iNet proporciona una protección más amplia contra fugas y cubre los siguientes escenarios:

  a. Fuga de DNS
  b. Fuga de IPv6

c. Fuga de WebRTC
d. Caída de conexión VPN
e. Aplicaciones lanzadas antes del establecimiento de VPN
f. Fugas de tráfico por aplicación

- **Permitir acceso a WAN**: si está habilitado, los dispositivos cliente locales aún pueden acceder a los servicios del lado WAN (por ejemplo, impresoras, NAS y otros dispositivos en la subred ascendente) mientras la VPN está activa.



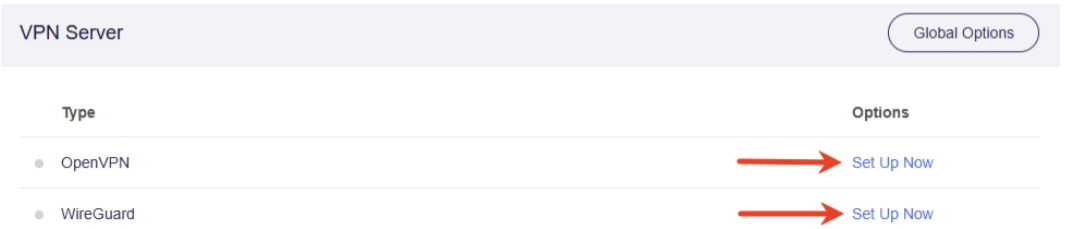

Como se muestra en el diagrama anterior, habilitar esta función permite que sus dispositivos locales lleguen a hosts en la subred ascendente, como impresoras y NAS.

Esta opción está diseñada principalmente para permitir que los clientes accedan a dispositivos dentro de la subred ascendente. Sin embargo, el enrutador no puede distinguir el tráfico de subred ascendente del tráfico de Internet normal. Si los dispositivos cliente acceden a los recursos directamente a través de IP públicas, existe un riesgo potencial de fuga de tráfico. Por este motivo, **Permitir acceso a WAN** y **Bloquear tráfico no VPN** son mutuamente excluyentes y no se pueden habilitar simultáneamente.

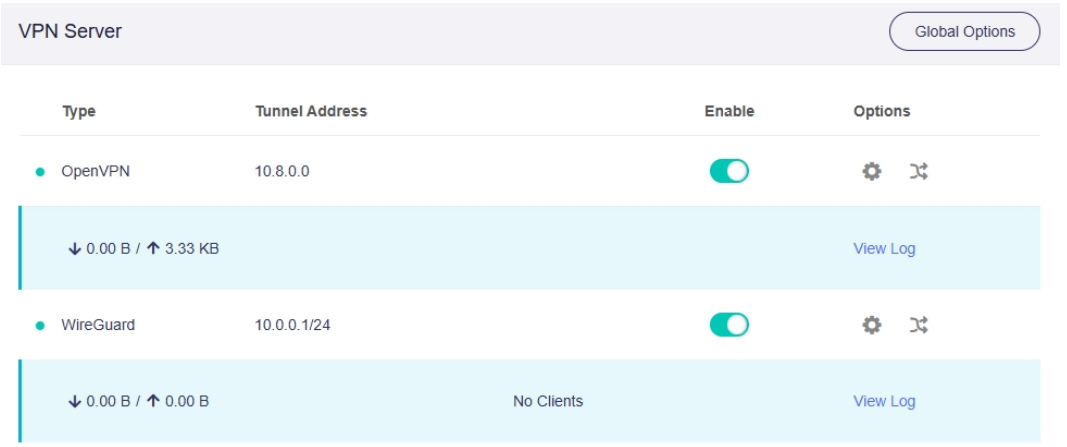
- **Servicios de uso de GL.iNet VPN**: si están habilitados, los servicios GoodCloud, DDNS y rtty transmitirán paquetes a través de túneles VPN. Esta opción está deshabilitada de forma predeterminada, ya que estos servicios normalmente requieren la dirección IP real del dispositivo para funcionar correctamente.

## 9.3 Servidor VPN

Si el enrutador nunca se ha configurado como servidor OpenVPN o WireGuard, la página aparecerá como se muestra a continuación. Haga clic en **Configurar ahora** y será dirigido a la página **Servidor OpenVPN** o **Servidor WireGuard** para inicializar su servidor VPN.

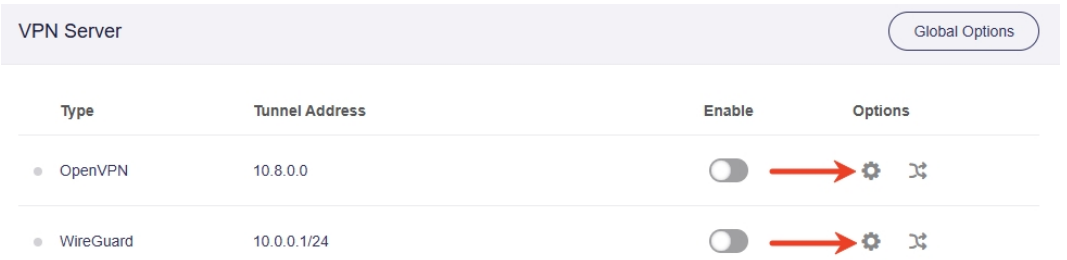



Después de habilitar el servidor OpenVPN o WireGuard, la página mostrará el estado del servidor de la siguiente manera.

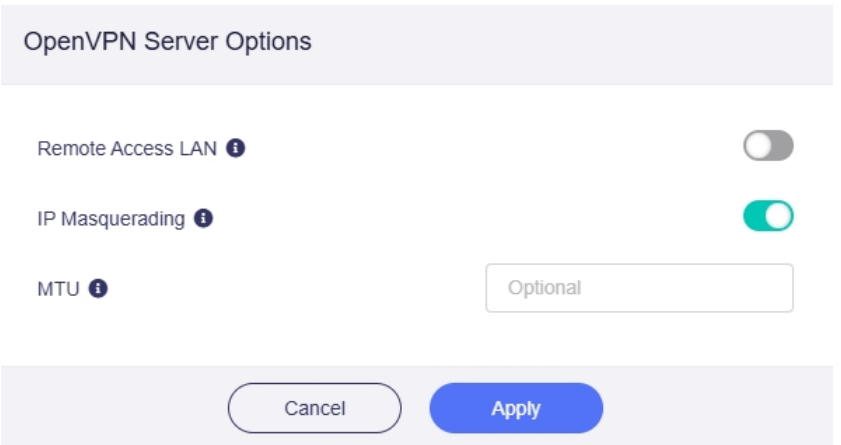


## 9.3.1 Opciones del servidor

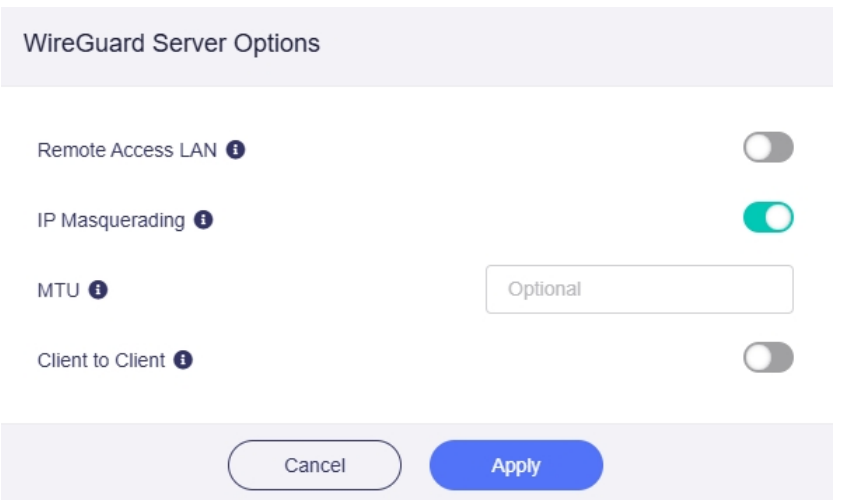
Haga clic en el ícono de ajustes a la derecha para acceder a las opciones del servidor OpenVPN o WireGuard.




Las opciones del servidor OpenVPN se muestran de la siguiente manera.




Las opciones del servidor WireGuard se muestran de la siguiente manera.

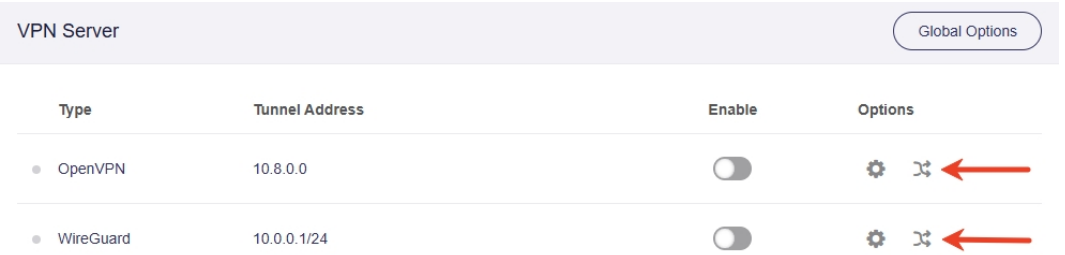



- **LAN de acceso remoto**: si está habilitado, se puede acceder a los recursos dentro de la subred LAN del servidor a través del túnel VPN.

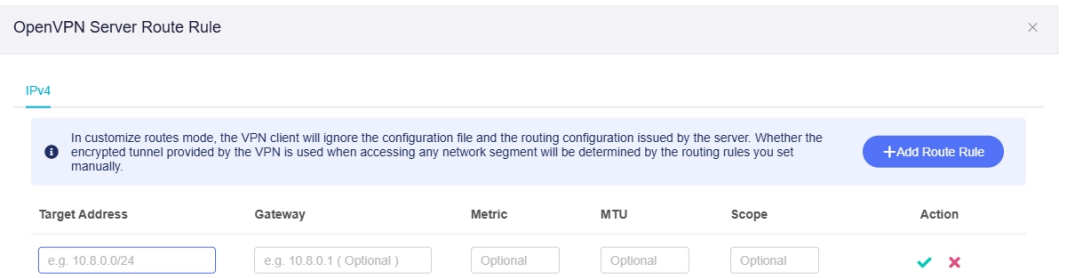
- **Enmascaramiento de IP**: si está habilitado, las direcciones IP de origen de los clientes LAN se reescribirán en la IP del túnel VPN del enrutador. Deshabilite esto solo para configuraciones de sitio a sitio donde el par remoto conoce sus subredes LAN.
- **MTU**: abreviatura de Unidad de transmisión máxima. El valor de MTU que establezca para el túnel anulará la configuración de MTU en el archivo de configuración.
- **Comunicación entre clientes**: si está habilitado, los clientes VPN conectados a este servidor pueden acceder entre sí a través de sus IP de túnel VPN. Si desea permitir que los clientes también accedan a las subredes LAN de otros, debe agregar reglas de enrutamiento en el servidor VPN para anunciar esas subredes LAN remotas.

## 9.3.2 Regla de ruta del servidor

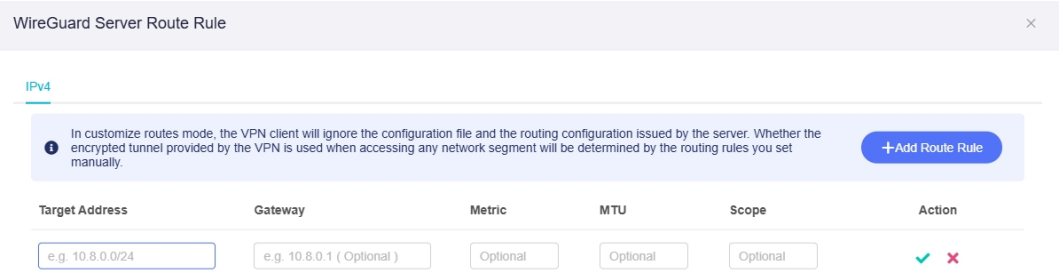
Haga clic en el icono de ruta a la derecha para personalizar las reglas de ruta OpenVPN o WireGuard según sea necesario.




La ruta del servidor OpenVPN La regla se muestra de la siguiente manera. Haga clic en **Agregar regla de ruta**, ingrese la **Dirección de destino** y la **Puerta de enlace** y luego haga clic en ícono de verificación verde para aplicar.



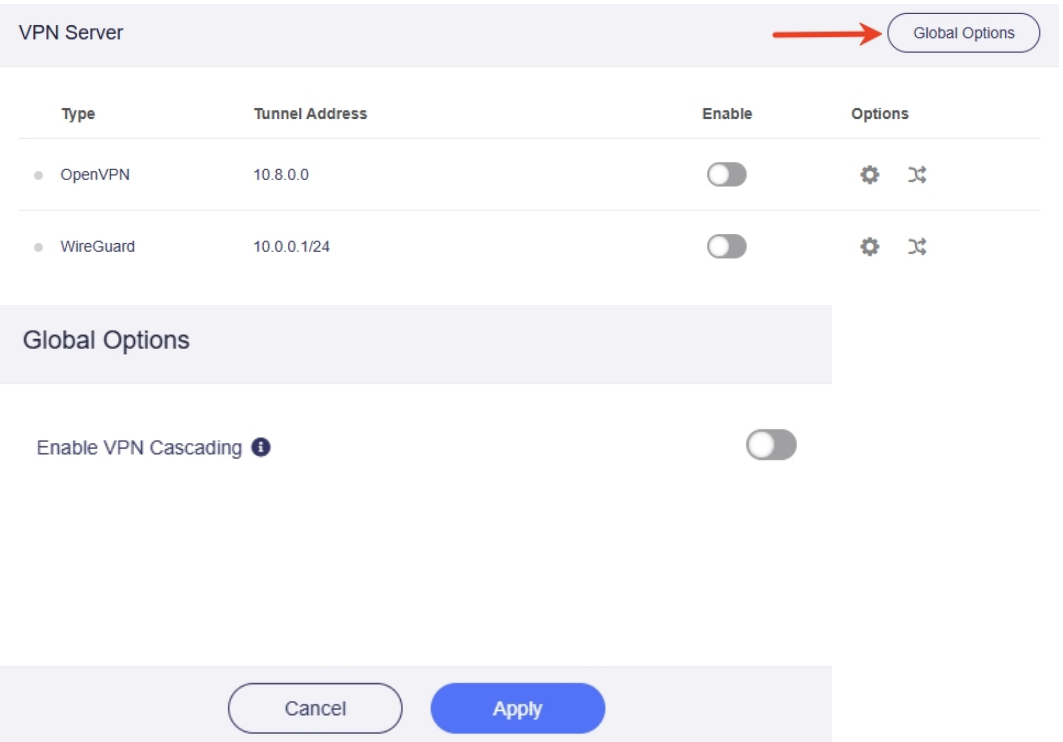

La regla de ruta del servidor WireGuard se muestra a continuación. Haga clic en **Agregar regla de ruta**, ingrese la **Dirección de destino** y **Puerta de enlace** y luego haga clic en el ícono de verificación verde para aplicar.




**Nota**: En el modo de personalizar rutas, el cliente VPN ignorará el archivo de configuración y la configuración de enrutamiento emitida por el servidor. El uso del túnel cifrado VPN al acceder a cualquier segmento de red está determinado por las reglas de enrutamiento que establezca manualmente.

## 9.3.3 Opciones globales

Haga clic en **Opciones globales** en la esquina superior derecha para configurar ajustes avanzados para su servidor VPN.




- **VPN en cascada**: si está habilitado, cuando este enrutador actúa como un servidor VPN y una VPN cliente simultáneamente, los clientes VPN remotos conectados al servidor VPN de este enrutador tendrán su tráfico enrutado a través del túnel VPN ascendente que este enrutador está utilizando como cliente VPN. Más información sobre VPN en cascada.

Capítulo 10

# Configurar el servidor VPN

Este capítulo presenta cómo configurar un enrutador GL.iNet como servidor OpenVPN o WireGuard.

## 10.1 Configurar el servidor OpenVPN

OpenVPN es un protocolo VPN de código abierto que utiliza cifrado SSL/TLS para conexiones seguras punto a punto y de sitio a sitio. Para configurar el servidor OpenVPN en un enrutador GL.iNet, mire este video o consulte los pasos a continuación.

### 10.1.1 Preparación

1. **Asegúrese de tener una dirección IP pública**

   Haga clic aquí para verificar si su proveedor de servicios de Internet (ISP) asigna una dirección IP pública.

   De lo contrario, su enrutador no se puede configurar como servidor OpenVPN.

   Métodos alternativos:

   - Si tiene un enrutador principal ascendente de su enrutador GL.iNet, inicie sesión en él y verifique que tenga una dirección IP pública asignada por su ISP.
   - Pídale a su ISP una dirección IP pública. Esto puede generar un cargo adicional.

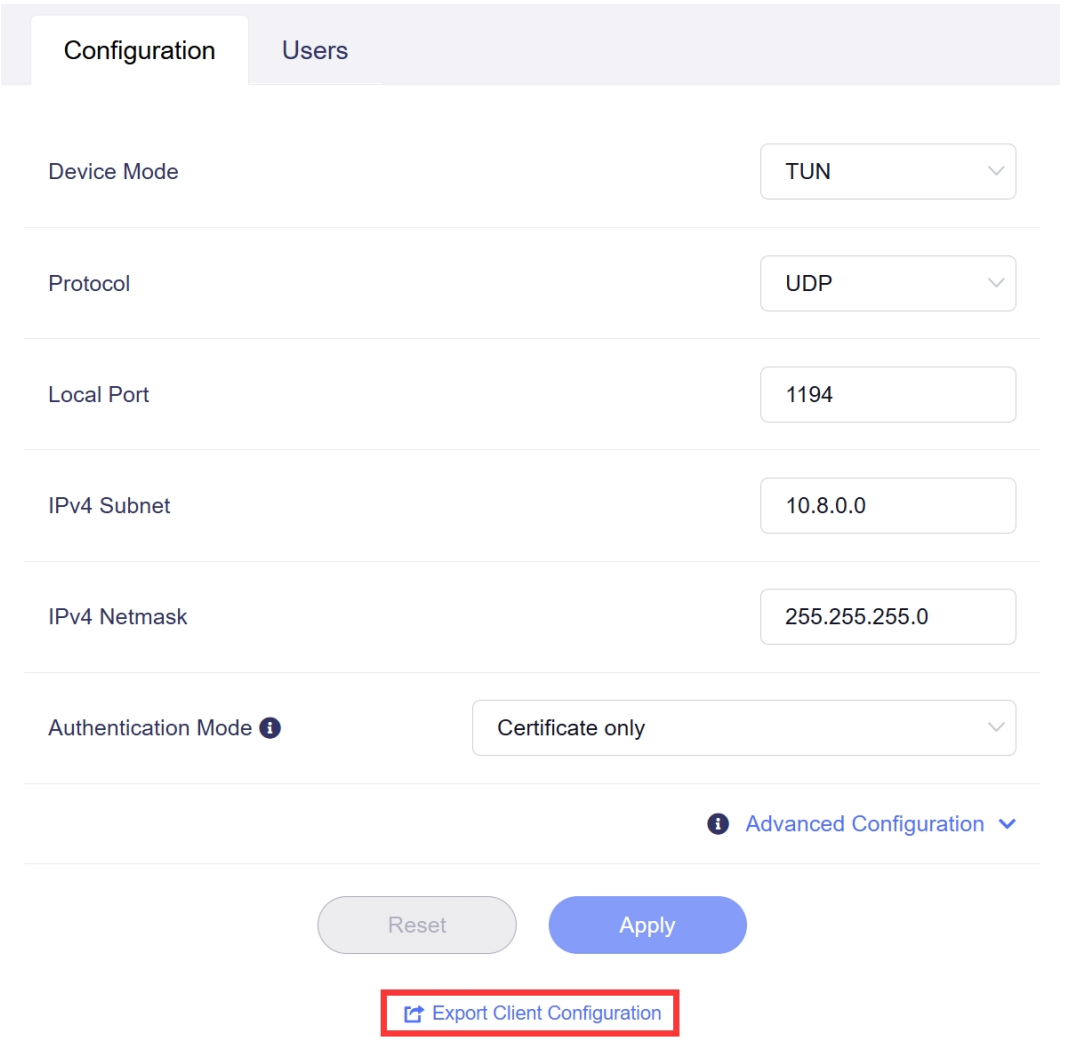
2. **Confirme si se requiere reenvío de puertos**

   - Si su enrutador GL.iNet es el enrutador principal de su red, no se requiere configuración de reenvío de puertos. Continúe con el siguiente paso.
   - Si ya hay un enrutador principal en uso y su enrutador GL.iNet está configurado como enrutador secundario, deberá configurar el reenvío de puertos en el enrutador principal.
   - Si su enrutador GL.iNet está en varios niveles descendentes desde el enrutador principal, configure el reenvío de puertos en cada dispositivo intermedio.

## 10.1.2 Pasos de configuración

1. Inicie sesión en En el panel de administración web del enrutador, navegue hasta **VPN** > **Servidor OpenVPN** y luego haga clic en **Generar configuración** (para la configuración inicial del servidor VPN). solamente).
2. Aplicar la configuración.

   La configuración predeterminada funciona en la mayoría de los casos. Haga clic en **Exportar configuración del cliente** en la parte inferior y continúa con el paso 3. Si has modificado la configuración, haz clic en **Aplicar** antes de exportarla.



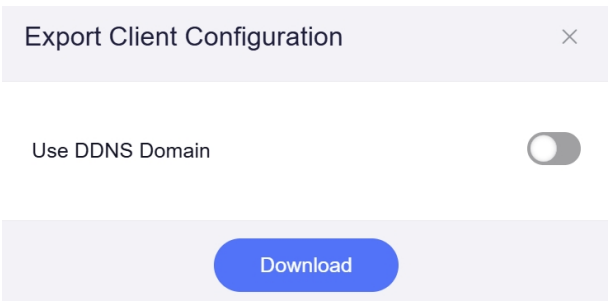

- **Modo de dispositivo**: TAP-S2S o Túnel. Consulte aquí para las diferencias.
- **Protocolo**: UDP o TCP. Consulte aquí para las diferencias.
- **Modo de autenticación**: Esto determina el método de autenticación utilizado cuando el cliente se conecta al servidor. Hay tres opciones:

- **Solo certificado**: si se selecciona, el enrutador generará automáticamente claves de certificado de servidor y de cliente y las incrustará en el archivo de configuración. Cuando carga la configuración al cliente, no se requieren credenciales adicionales.
- **Solo nombre de usuario/contraseña**: si se selecciona, el enrutador generará la configuración del cliente sin claves de certificado. Primero debe agregar un nombre de usuario y contraseña en **Usuarios** pestaña antes de exportar la configuración del cliente. Al cargar la configuración al cliente, ingrese estas credenciales para autenticación.
- **Nombre de usuario/Contraseña y certificado**: si se selecciona, primero debe agregar un nombre de usuario y contraseña en la pestaña **Usuarios** antes de exportar la configuración del cliente; en segundo lugar, el enrutador generará automáticamente claves de certificado de servidor y cliente y las incrustará en el archivo de configuración. Al cargar la configuración al cliente, primero se verificará la clave del certificado, seguida de la autenticación de nombre de usuario/contraseña para seguridad 2FA.

- **Configuración avanzada**: personalice más configuraciones del servidor si es necesario.

3. Exportar configuración del cliente.

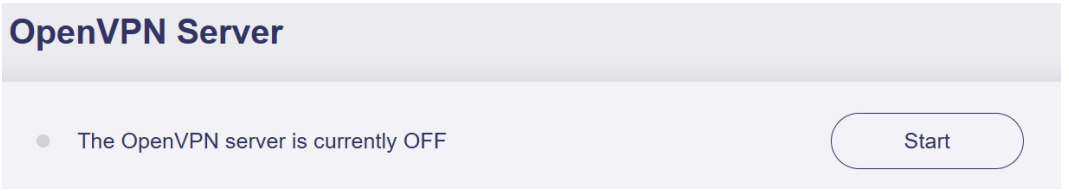
   Después de hacer clic **Exportar configuración del cliente** en la parte inferior de la pestaña Configuración (o aplicar la configuración modificada), aparecerá una ventana como la siguiente. Haga clic en **Descargar** para exportar la configuración.



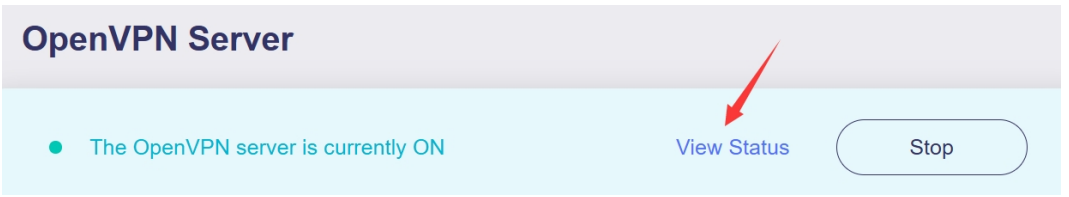

   **Consejo**: si su dirección IP pública cambia con frecuencia, vaya a **APLICACIONES** > **DNS dinámico** y habilitar DDNS. Luego podrá utilizar el dominio DDNS como dirección de su servidor.

4. Inicie el servidor OpenVPN.

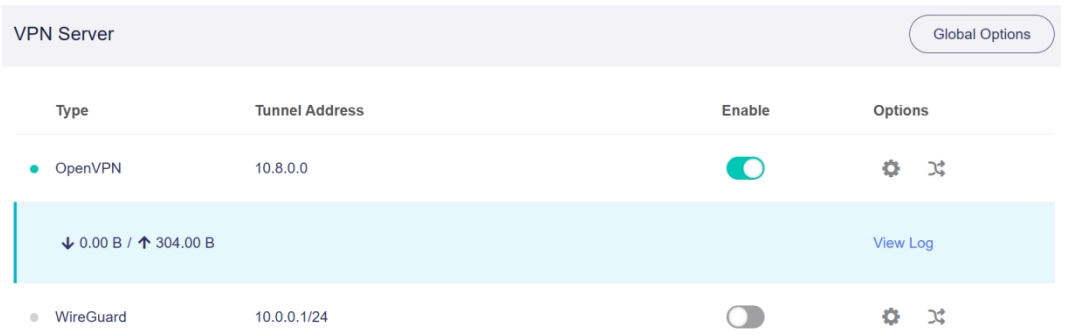
   En la página **Servidor OpenVPN**, haga clic en **Iniciar** en la esquina superior derecha para iniciar el servidor.




Si desea ver el estado de la conexión del servidor, haga clic en **Ver estado**.




Será redirigido al panel de VPN. Si lasestadísticas de tráfico de carga y descarga en esta página, el servidor OpenVPN se está ejecutando.




## 10.1.3 Solución de problemas

Si la conexión falla, existen varias razones comunes:

- El servidor VPN no tiene una dirección IP pública. Consulta aquí para solucionar problemas.
- Es posible que tengas que configurar el reenvío de puertos. Consulte aquí para solucionar problemas.
- El puerto utilizado para el servidor OpenVPN está bloqueado por su proveedor de servicios de Internet. Cambie a otro puerto o comuníquese con su ISP para obtener ayuda.
- La conexión VPN puede estar bloqueada en ciertos países o regiones.

## 10.2 Configurar el servidor WireGuard

WireGuard® es una VPN simple pero rápida y moderna que utiliza criptografía de última generación. Su objetivo es ser más rápido, más simple y más útil que IPSec, evitando al mismo tiempo el enorme dolor de cabeza. Pretende tener un rendimiento considerablemente mayor que OpenVPN. Para configurar el servidor WireGuard en un enrutador GL.iNet, mire este video o consulte los pasos a continuación.

### 10.2.1 Preparación

1. **Asegúrese de tener una dirección IP pública**

   Haga clic aquí para verificar si su proveedor de servicios de Internet le asigna una dirección IP pública.

   De lo contrario, su enrutador no se puede configurar como servidor WireGuard.

   Alternativa métodos:

   - Si tiene un enrutador principal ascendente de su enrutador GL.iNet, inicie sesión en él y verifique que tenga una dirección IP pública asignada por su ISP.
   - Solicite a su ISP una dirección IP pública. Esto puede generar un cargo adicional.

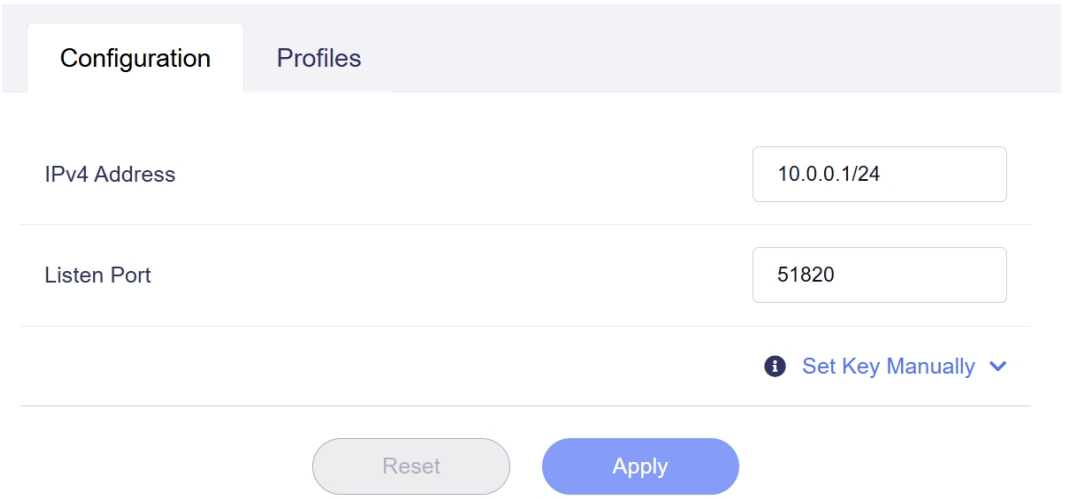
2. **Confirme si se requiere reenvío de puertos**

   - Si su enrutador GL.iNet es el enrutador principal de su red, no se requiere configuración de reenvío de puertos. Continúe con el siguiente paso.
   - Si ya hay un enrutador principal en uso y su enrutador GL.iNet está configurado como enrutador secundario, deberá configurar el reenvío de puertos en el enrutador principal.
   - Si su enrutador GL.iNet está en varios niveles descendentes desde el enrutador principal, configure el reenvío de puertos en cada dispositivo intermedio.

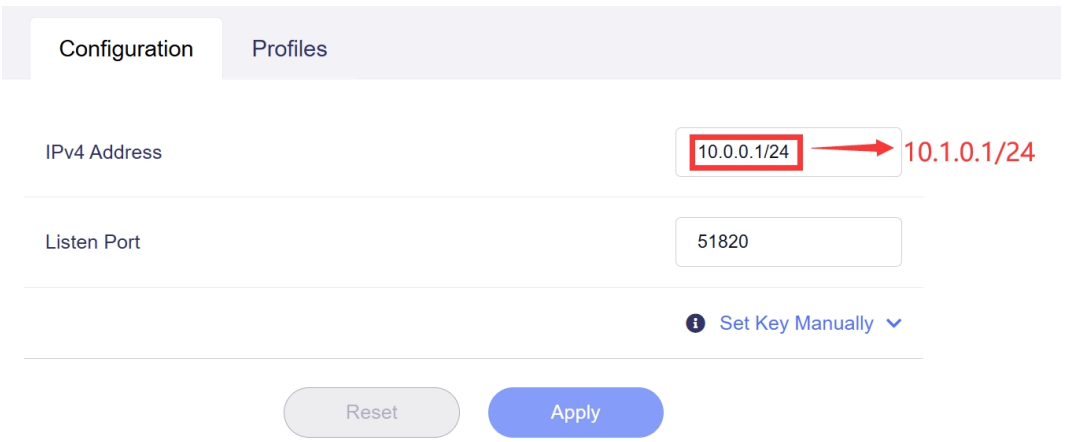
## 10.2.2 Pasos de configuración

1. Inicie sesión en el panel de administración web del enrutador', navegue hasta **VPN** > **Servidor WireGuard** y luego haga clic en **Generar configuración** (solo para la configuración inicial del servidor VPN).
2. Aplicar la configuración.

   La configuración predeterminada funciona en la mayoría de los casos. No es necesario modificar la dirección IPv4 a menos que it conflictos con la puerta de enlace del enrutador ascendente.

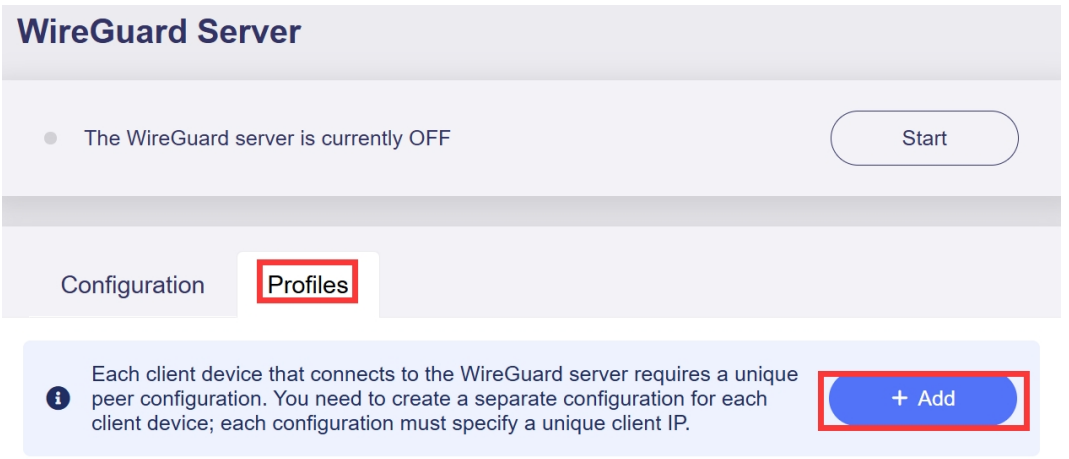



   Si la dirección IPv4 entra en conflicto con la puerta de enlace de su enrutador ascendente, modifique la dirección IPv4 a otra una (por ejemplo, **10.1.0.1/24**) y haga clic en **Aplicar**. Asegúrese de que se incluya la notación CIDR "/24" para evitar problemas de conectividad.

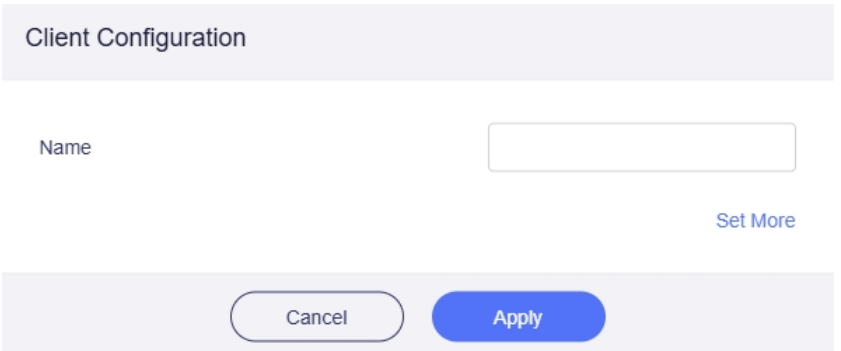



3. Agregue un perfil.

Cambie a **Perfiles** pestaña, haga clic en **Agregar** para generar un perfil para su dispositivo.




Establezca un nombre descriptivo y haga clic en **Aplicar** para continuar.



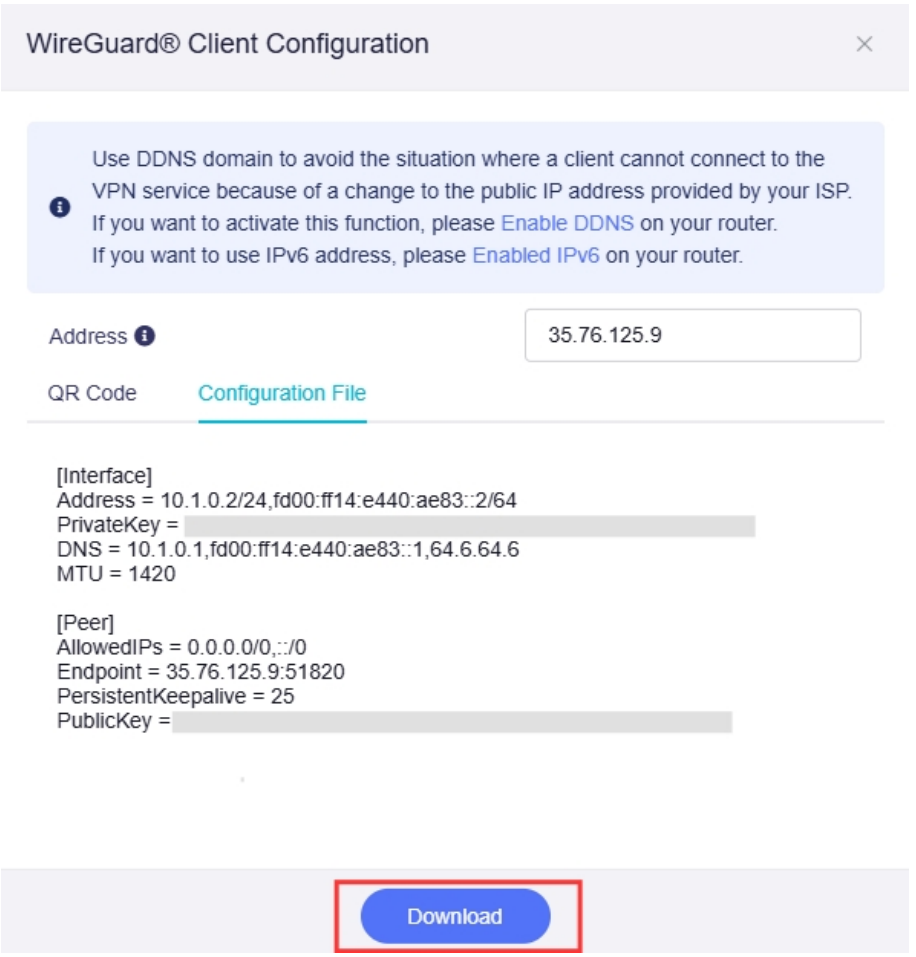

**Consejo**: si desea acceder a los dispositivos LAN del cliente WireGuard desde su servidor WireGuard, cambie a la pestaña **Reglas de ruta** para configurar las reglas de ruta. Consulte aquí para obtener más detalles.

4. Descargar la configuración.

   Después de agregar un perfil, el enrutador generará un archivo de configuración en tres formatos: código QR, texto sin formato y archivo .conf. Elija su método preferido para obtener el archivo de configuración.

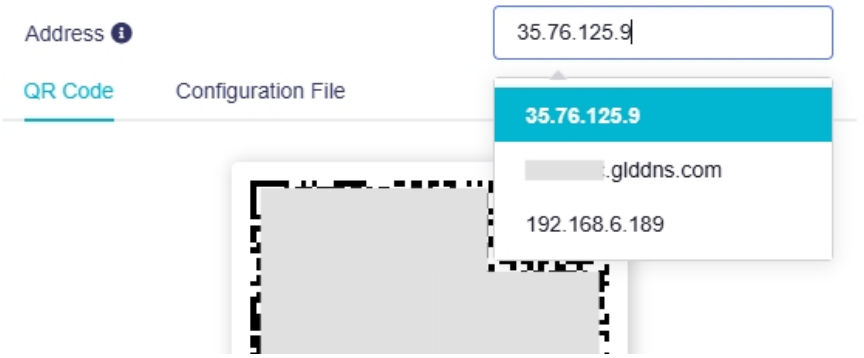
   - **Código QR**: Adecuado para dispositivos (por ejemplo, teléfonos inteligentes, tabletas, computadoras portátiles) con la aplicación WireGuard instalada. Si desea configurar un dispositivo específico como cliente WireGuard, simplemente abra la aplicación WireGuard y escanee el código QR para importar un archivo de configuración.

- **Texto sin formato**: en formato de texto sin formato, puede revisar los detalles de configuración y copiarlos y pegarlos cómodamente en otro lugar para la configuración manual, como la aplicación WireGuard o un enrutador GL.iNet.
- **archivo .conf**: haga clic en **Descargar** para guardar el archivo .conf en su dispositivo local. También es conveniente y se puede cargar directamente en la aplicación WireGuard o en un enrutador GL.iNet.



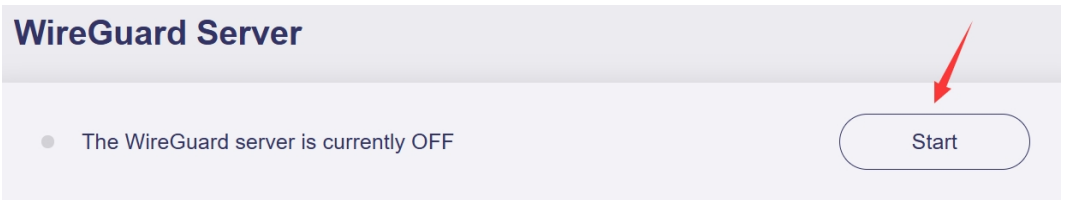

**Consejos**:

- Si su IP pública dirección cambia con frecuencia, vaya a **APLICACIONES** > **DNS dinámico** y habilite DDNS. Entonces puedes usar el dominio DDNS como su dirección de servidor.
- Desde firmware v4.8, puede seleccionar la dirección del servidor de una lista desplegable antes de exportar el archivo de configuración: IP pública, dominio DDNS y dirección IP WAN actual. Una vez seleccionada, la dirección del servidor en el archivo de configuración se actualizará automáticamente. Vuelva a descargar el archivo de configuración si se cambia la dirección del servidor.

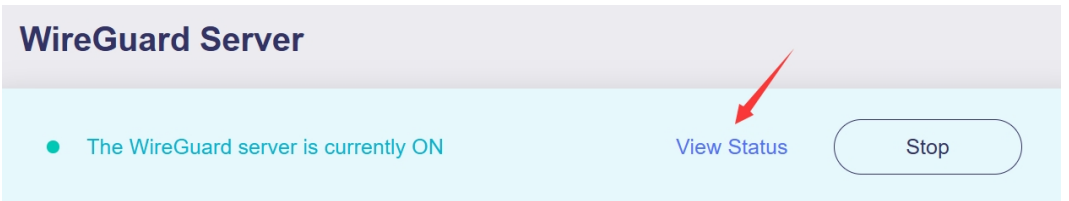



5. Inicie el servidor WireGuard.

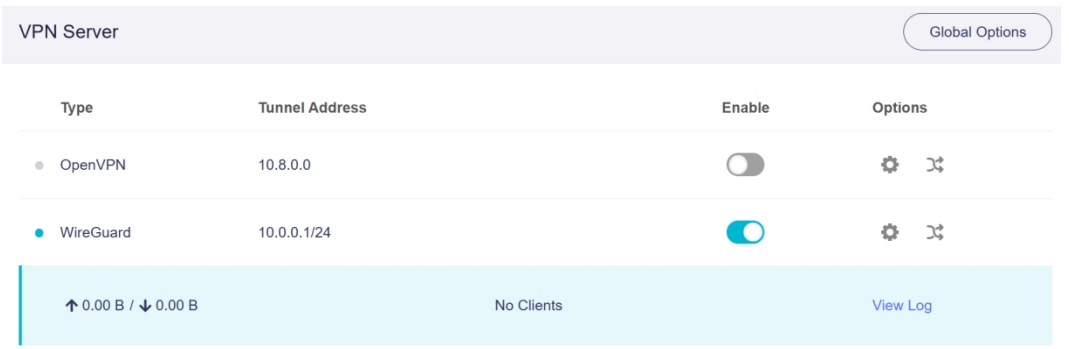
   En la página **Servidor WireGuard**, haga clic en **Iniciar** en la esquina superior derecha para iniciar el servidor.




   Si desea ver el estado de la conexión del servidor, haga clic en **Ver estado**.




   Será redirigido al panel de VPN. Si lasestadísticas de tráfico de carga y descarga en esta página, el servidor OpenVPN se está ejecutando.




## 10.2.3 Solución de problemas

Si la conexión falla, existen varias razones comunes:

- El servidor VPN no tiene una dirección IP pública. Consulte aquí para solucionar problemas.
- Es posible que deba configurar el reenvío de puertos. Consulte aquí para solucionar problemas.
- El puerto utilizado para WireGuard El servidor está bloqueado por su proveedor de servicios de Internet. Cambie a otro puerto o comuníquese con su ISP para obtener ayuda.
- La conexión VPN puede estar bloqueada en ciertos países o regiones.

Capítulo 11

# Configurar el cliente VPN

Este capítulo presenta cómo configurar un enrutador GL.iNet como cliente OpenVPN o WireGuard.

# 11.1 Configurar el cliente OpenVPN

## 11.1.1 Preparación

Primero, asegúrese de tener una suscripción activa con un proveedor de servicios VPN que admita la configuración manual de OpenVPN. Consulte aquí para conocer los proveedores de OpenVPN compatibles con GL.iNet.

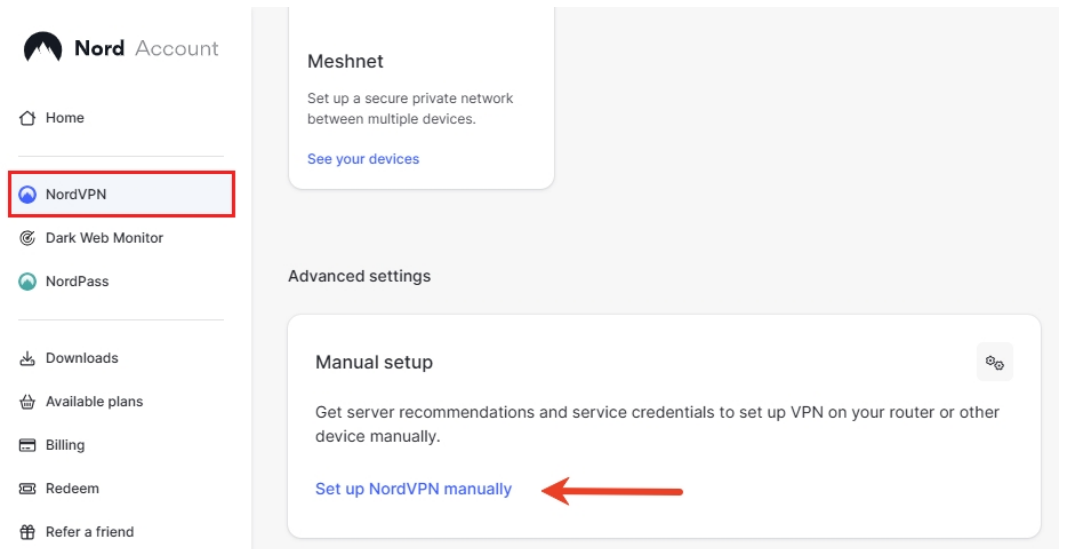
Siguiente, visite el sitio web oficial del proveedor de servicios VPN al que se suscribió y obtener las credenciales de servicio o el archivo de configuración. Si no sabe cómo obtener el archivo de configuración, consulte este enlace o póngase en contacto con su soporte.

## 11.1.2 Configurar NordVPN

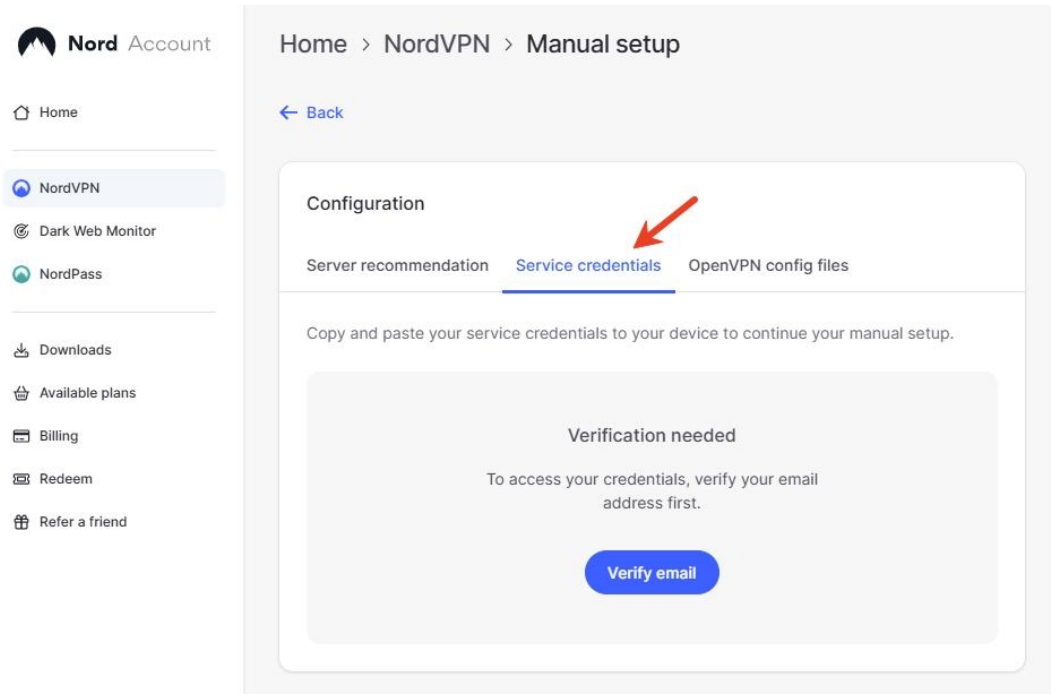
NordVPN está integrado en GL.iNet web panel de administración. Puede adquirir archivos de configuración para todos los servidores NordVPN introduciendo las credenciales de su cuenta (obtenidas del Panel de NordVPN) en el panel de administración web del enrutador o en la aplicación móvil GL.iNet , lo que elimina la necesidad de cargar archivos manualmente.

Siga los pasos a continuación para configurar su enrutador como NordVPN cliente.

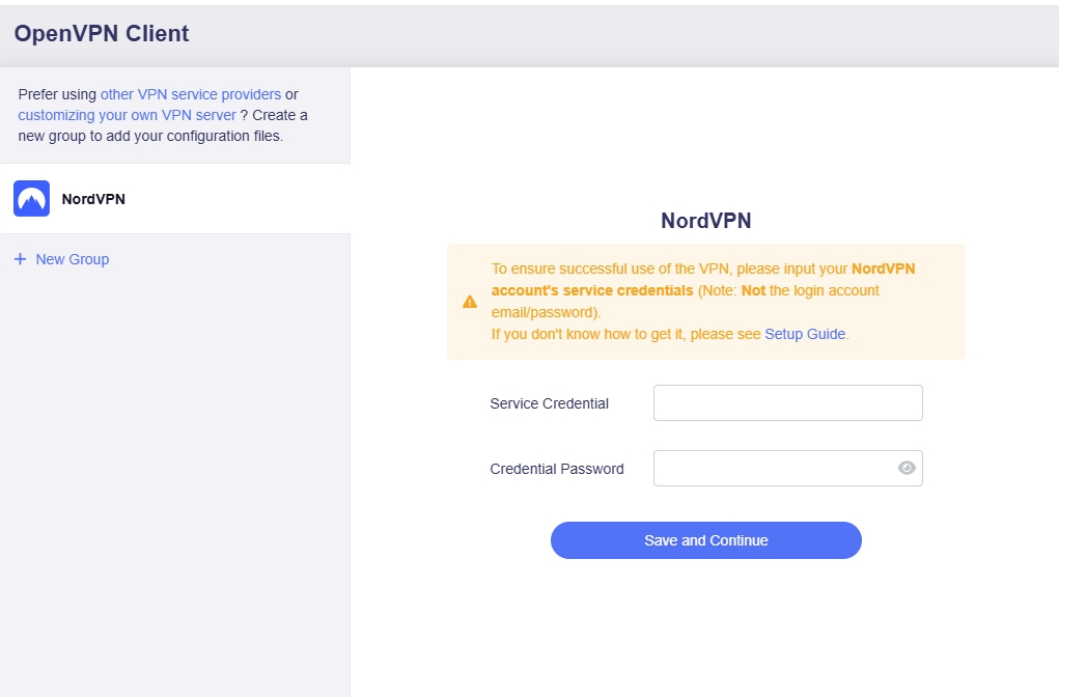
1. Inicie sesión en su cuenta web de NordVPN aquí.
2. Oen el Panel de control de Nord, haga clic en **NordVPN**, luego haga clic en **Configurar NordVPN manualmente**.



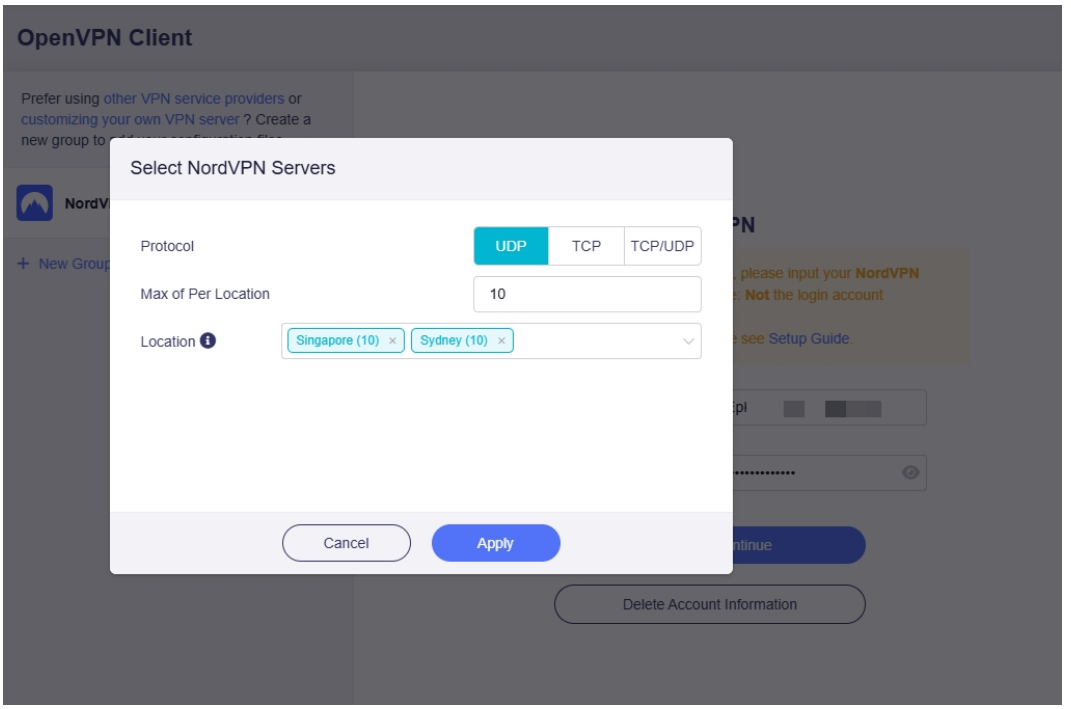

Encontrará las **credenciales de servicio**. Cópielos para usarlos más adelante.



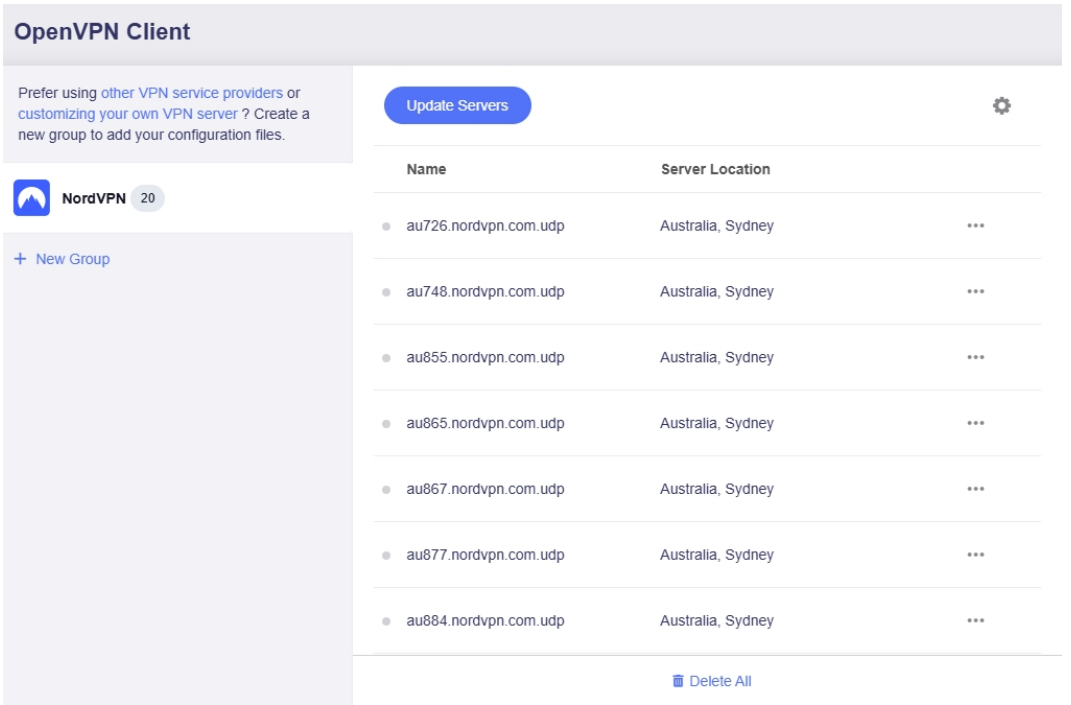

3. Inicie sesión en el panel de administración web de su enrutador y navegue hasta **VPN** > **Cliente OpenVPN** > **NordVPN**. Introduzca las credenciales del servicio (Nota: NO es el correo electrónico ni la contraseña de la cuenta de inicio de sesión), luego haga clic en **Guardar y continuar**.




4. Seleccione el protocolo, el número máximo de servidores de cada ubicación y ubicaciones, luego haga clic en **Aplicar**.

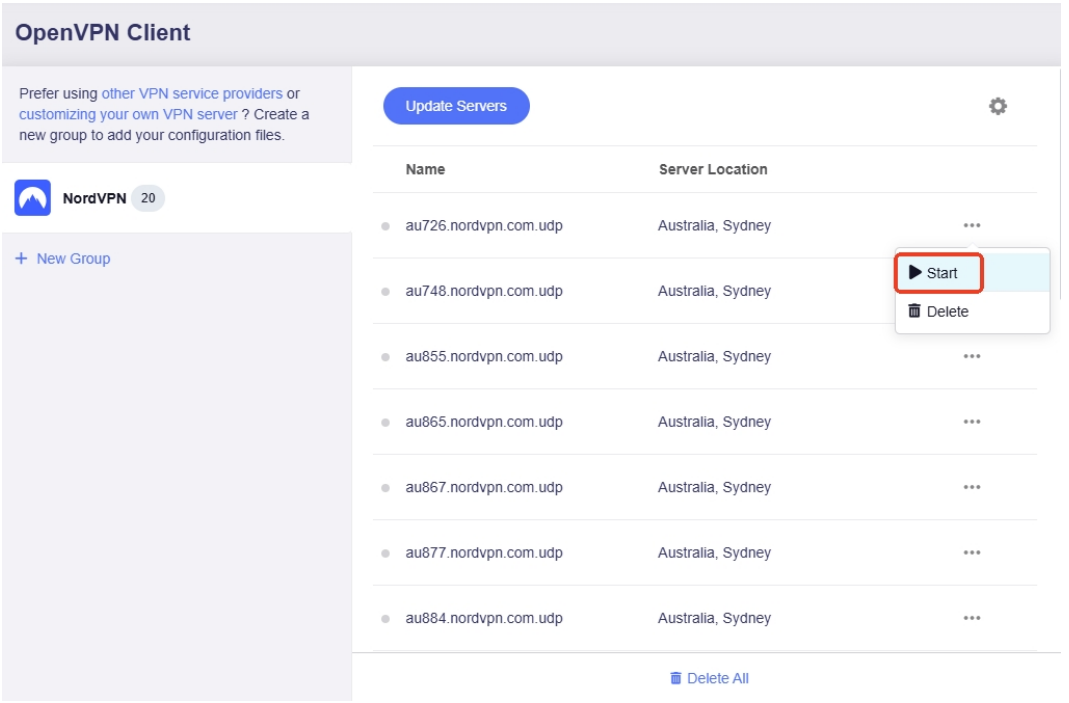



Descargará archivos de configuración.

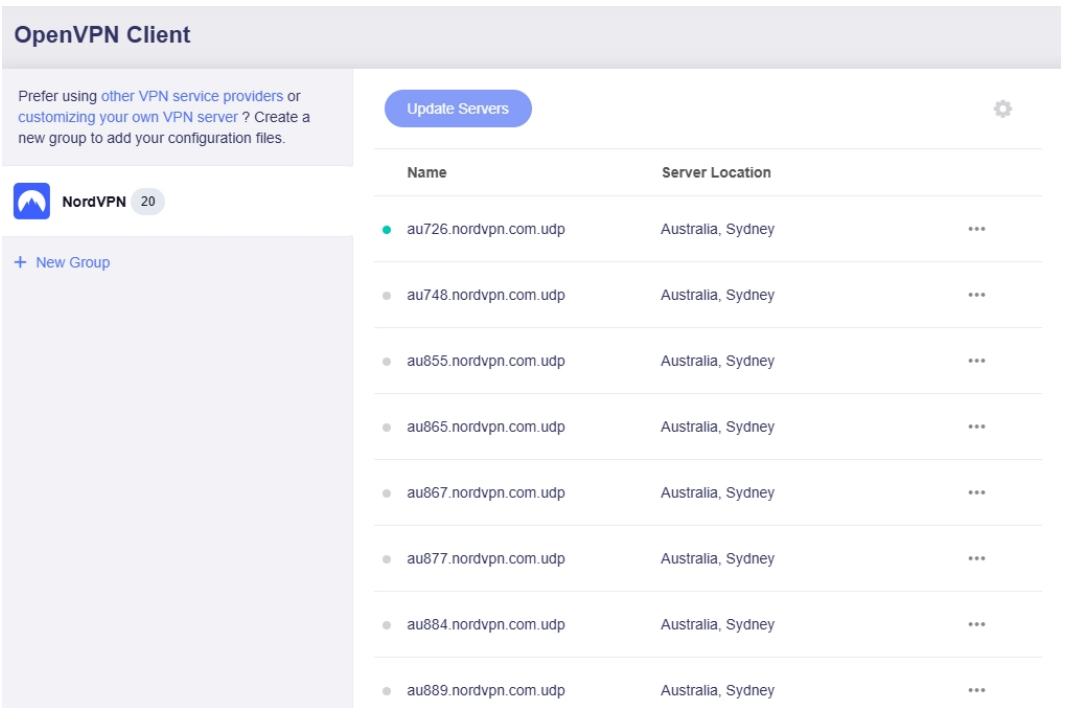



5. Iniciará una conexión.

   Seleccione un servidor y haga clic en el icono de tres puntos a la derecha para iniciar una conexión.



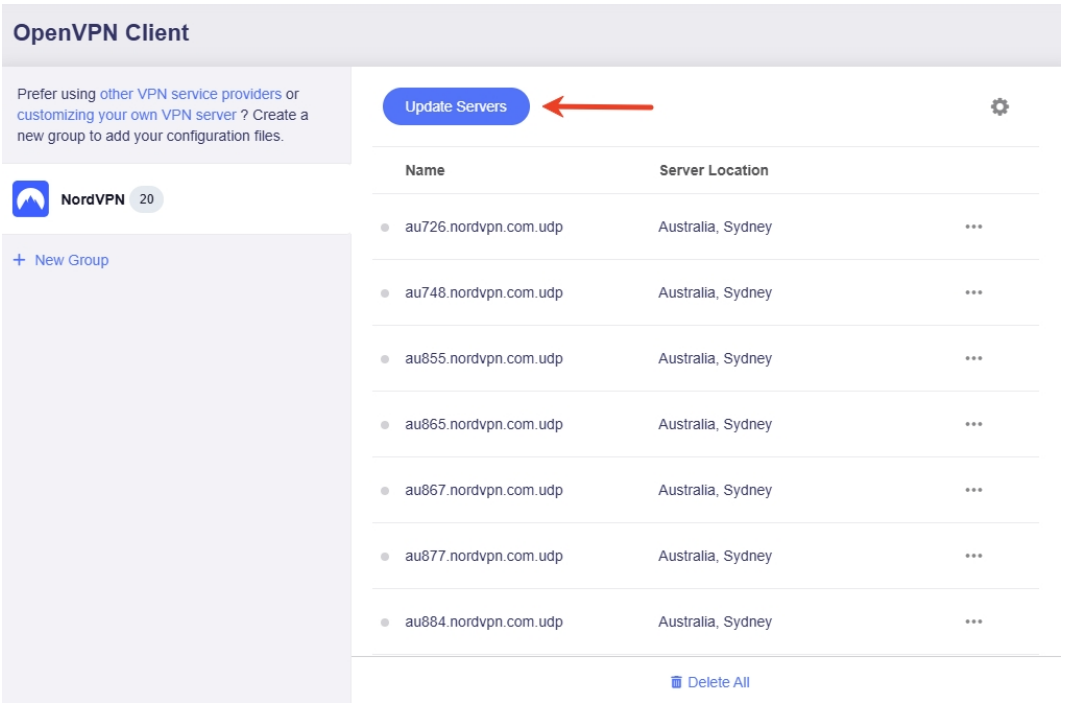

6. Una vez conectado, aparecerá un punto verde aparecerá junto al archivo de configuración.




También puede consultar los detalles de la conexión VPN en el **Panel de VPN**.

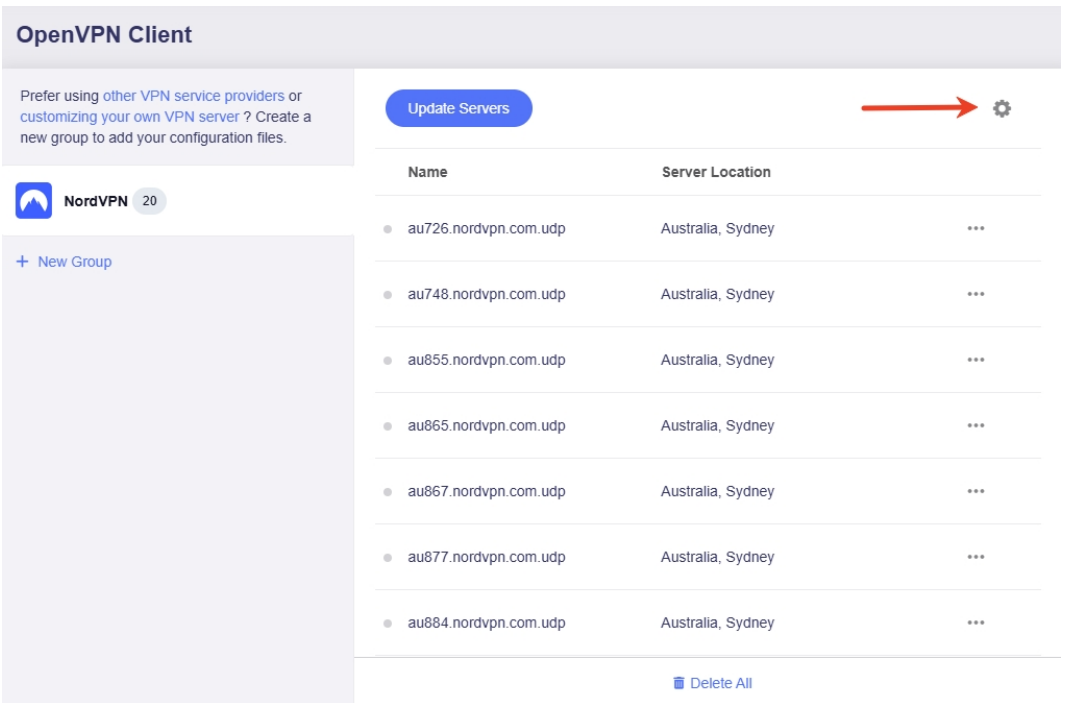
7. Actualizar servidores.

Puede hacer clic en **Actualizar Servidores** para obtener la última lista de servidores disponibles, evitando fallas de conexión causadas por el mantenimiento o el apagado del servidor.



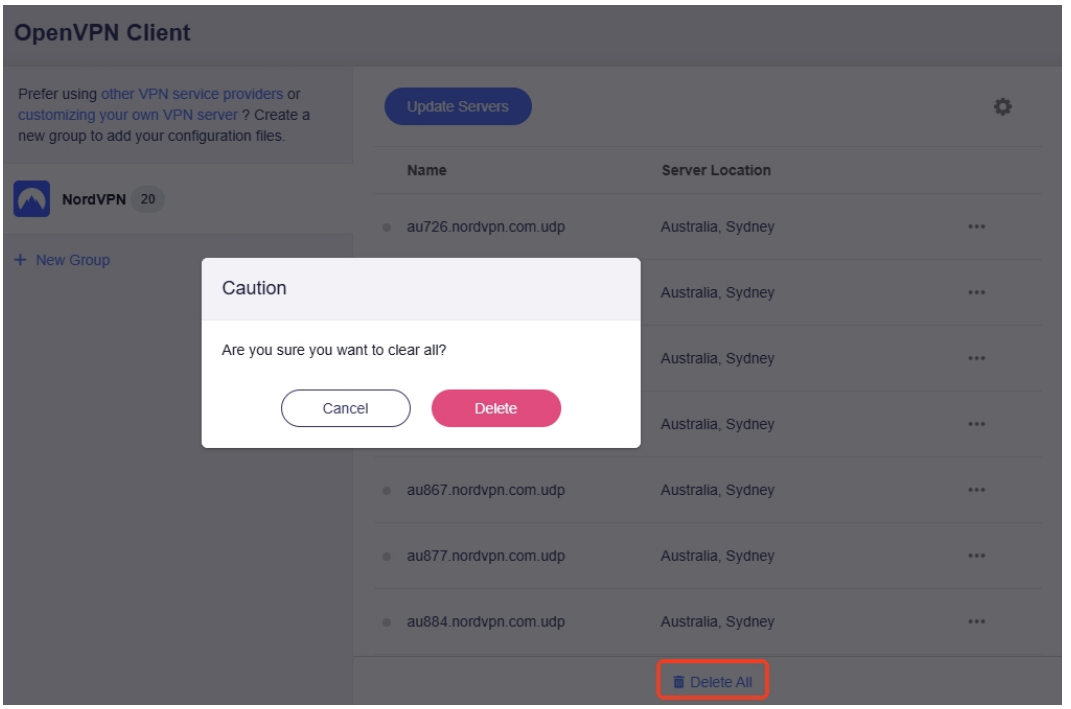

8. Edite las credenciales.

   Haga clic en el ícono de ajustes para editar sus credenciales de inicio de sesión.




9. Elimine todos los archivos.

Puede hacer clic en **Eliminar todo** para eliminar todos los archivos de configuración con un solo clic.

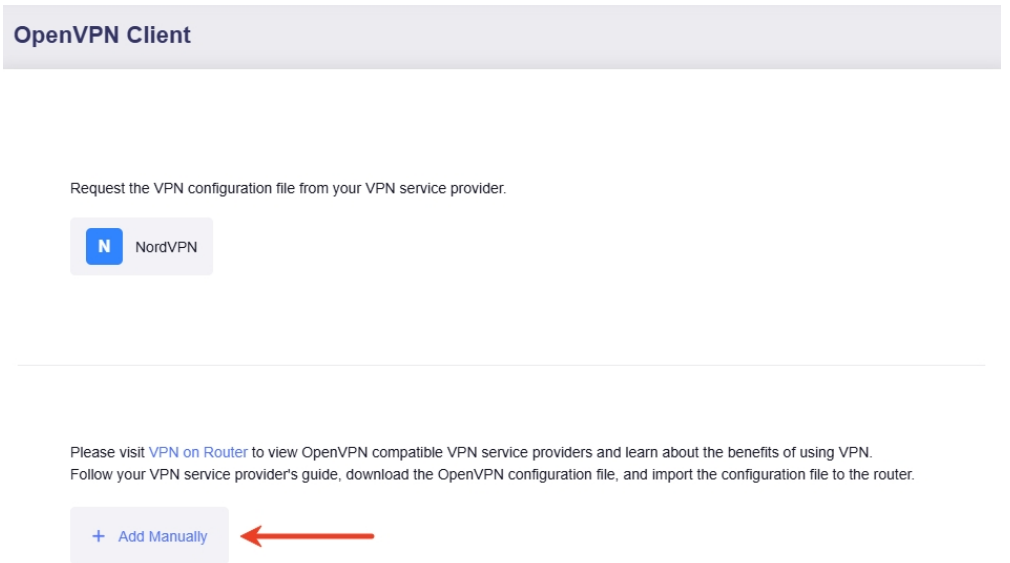


## 11.1.3 Configurar el cliente OpenVPN manualmente (para otros proveedores)

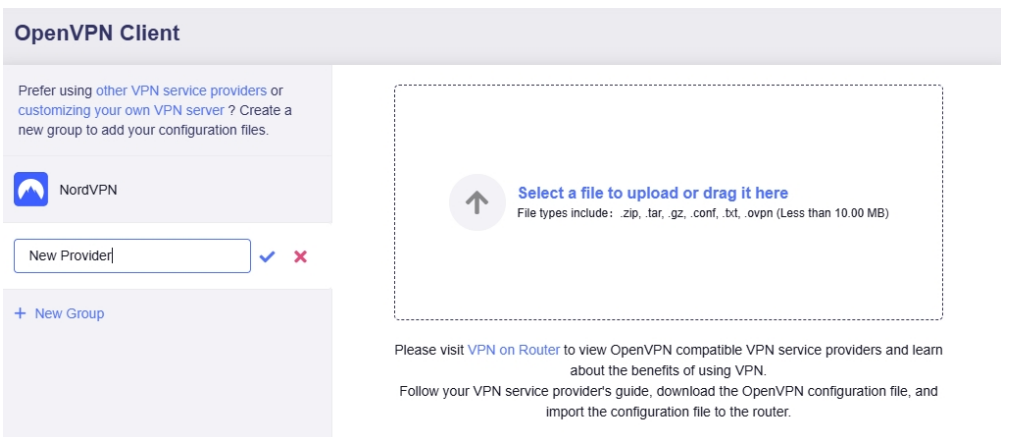
Si su proveedor de servicios OpenVPN es no está integrado en nuestro panel de administración, primero visite el sitio web oficial de su proveedor de servicios suscrito para obtener el archivo de configuración. Luego cárguelo en el enrutador para configurar un cliente OpenVPN.

En los siguientes pasos, usaremos PIA (Private Internet Access) como ejemplo.

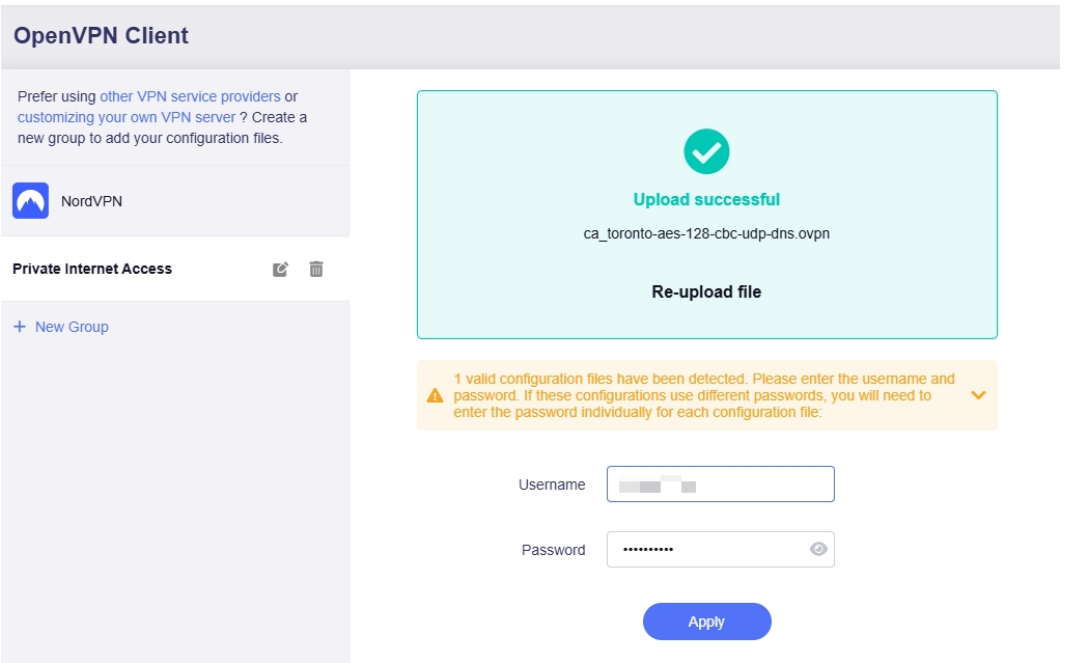
1. Descargue un archivo de configuración del sitio web oficial de Private Internet Access.
2. Inicie sesión en el panel de administración web de su enrutador, navegue hasta **VPN** > **Cliente OpenVPN** y haga clic en **Agregar manualmente**.



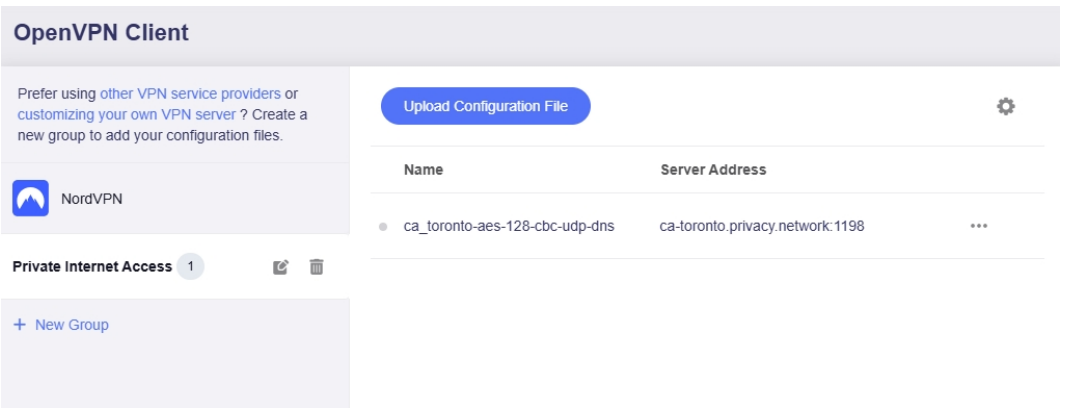

3. Se creará un grupo en la barra lateral izquierda. Establezca un nombre descriptivo para el grupo.



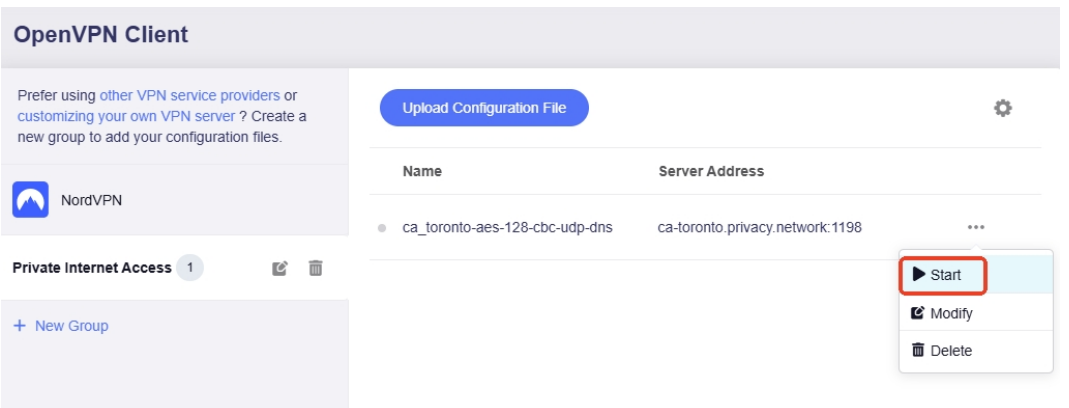
4. Cargue su archivo de configuración OpenVPN. Ingrese las credenciales si es necesario, luego haga clic en **Aplicar**.



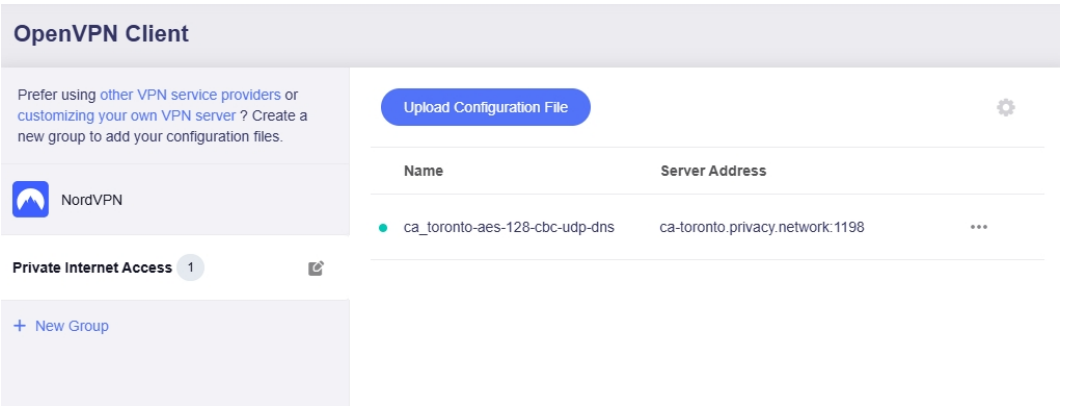

YVerá el archivo de configuración cargado.




5. Haga clic en el ícono de tres puntos a la derecha para iniciar una conexión.



6. Una vez conectado, aparecerá un punto verde junto al archivo de configuración.




También puede consultar los detalles de la conexión VPN en el **Panel de VPN**.

## 11.2 Configurar el cliente WireGuard

Puede configurar WireGuard Client a través de la aplicación móvil GL.iNet o el panel de administración web.

- La aplicación móvil integra algunos proveedores de servicios WireGuard, como AzireVPN, Mullvad VPN, OVPN, StrongVPN, PIA VPN. Puede configurarlo fácilmente ingresando las credenciales de inicio de sesión del servicio WireGuard al que se suscribió. Abra la aplicación y siga las instrucciones en pantalla para configurarla.
- El panel de administración web no solo integra algunos proveedores de servicios WireGuard, sino que también proporciona una entrada para la configuración manual. Puede ingresar las credenciales de su servicio WireGuard suscrito para una configuración rápida o cargar manualmente un archivo de configuración para completar la configuración.

### 11.2.1 Preparación

Primero, asegúrese de tener una suscripción activa con un proveedor de servicios VPN que admita configuración manual de WireGuard. Consulte aquí para conocer los proveedores WireGuard compatibles con GL.iNet.

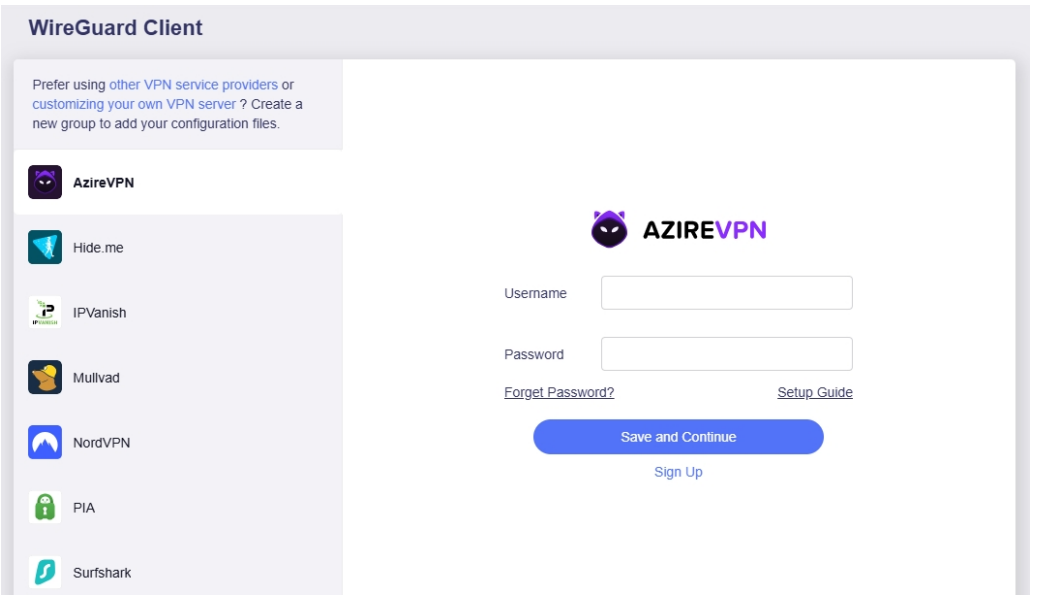
A continuación, sseleccione el proveedor de servicios WireGuard correspondiente a continuación para localizar rápidamente las instrucciones paso a paso.

- Configurar AzireVPN
- Configurar Hide.me
- Configurar IPVanish
- Configurar Mullvad
- Configurar NordVPN
- Configurar PIA (Private Internet Access)
- Configurar Surfshark
- Configurar el cliente WireGuard manualmente (para otros proveedores)

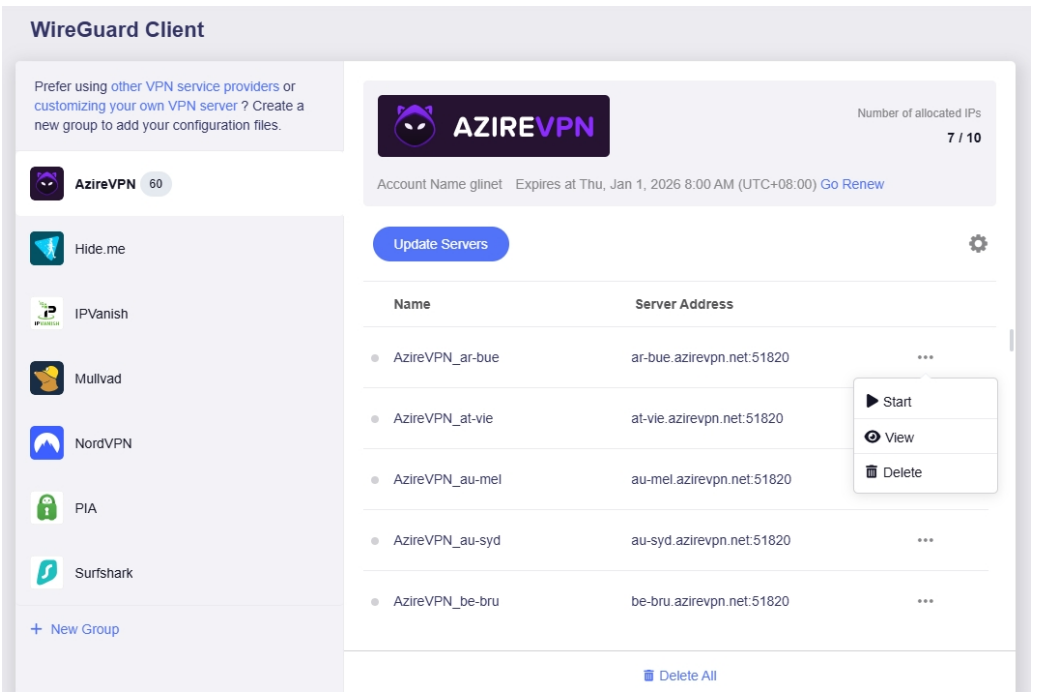
## 11.2.2 Configurar AzireVPN

Siga los pasos a continuación para configurar su enrutador como cliente AzireVPN.

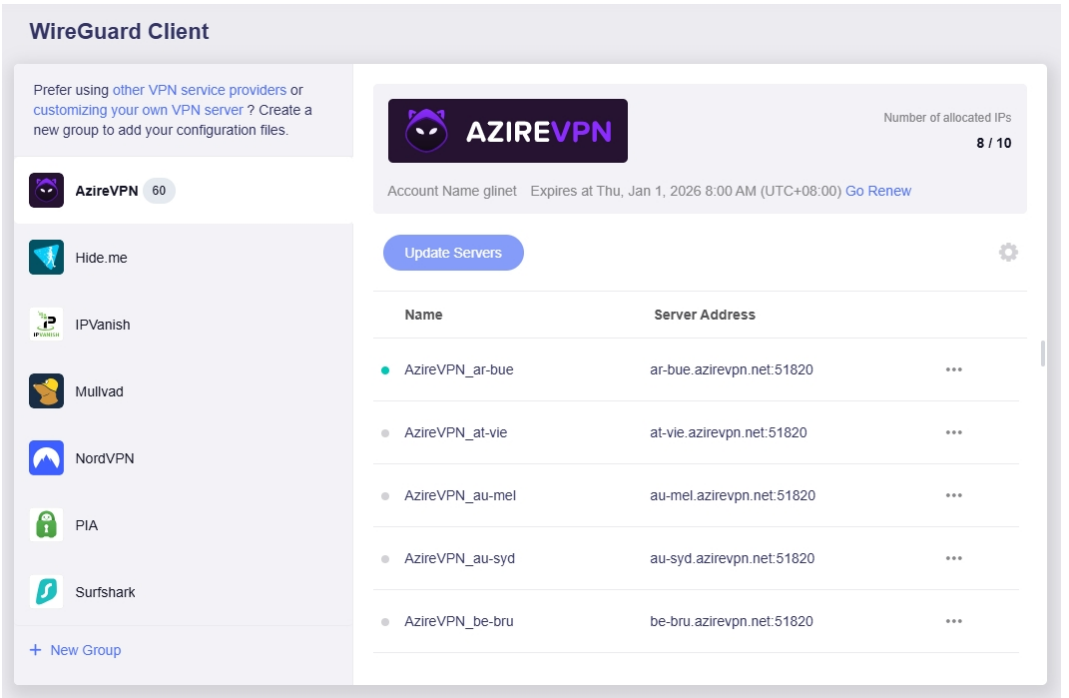
1. Inicie sesiónn en su enrutador’s web admin panel y vaya a **VPN** > **WireGuard Client** > **AzireVPN**.
2. Ingrese nombre de usuario y contraseña, luego haga clic en **Guardar y continuar**. Generará archivos de configuración para cada servidor.




3. Seleccione un servidor preferido y haga clic en el icono de tres puntos a la derecha para iniciar una conexión.



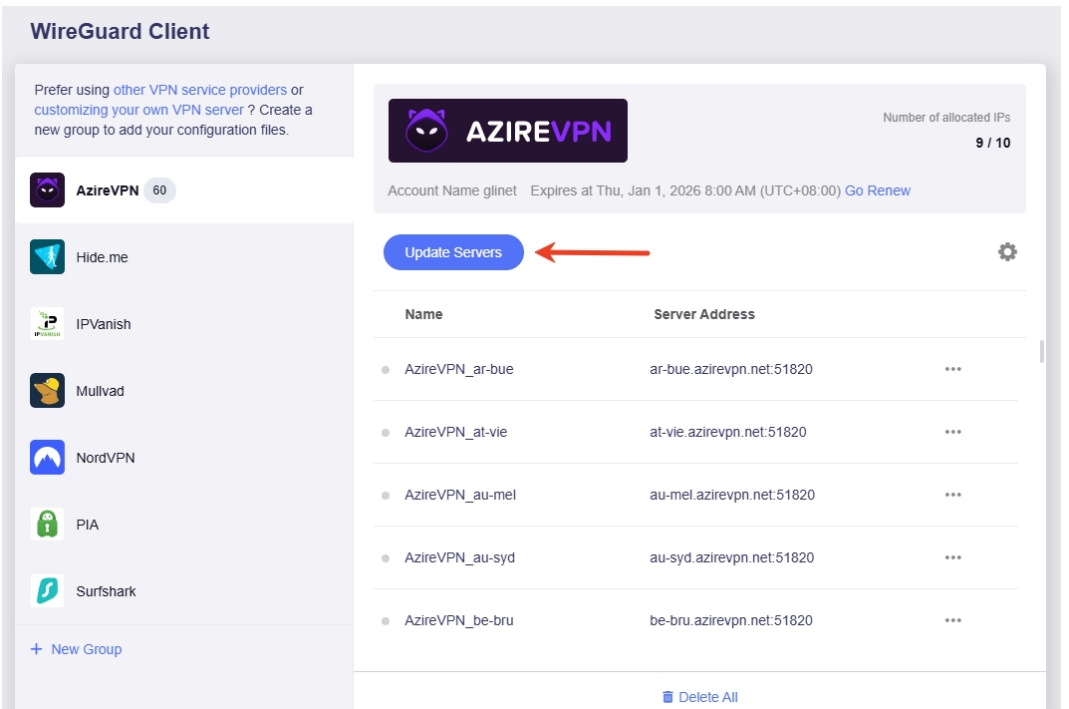
4. Una vez conectado, aparecerá un punto verde junto al archivo de configuración.




Usted puede también verifique los detalles de la conexión VPN en **Panel de VPN**.

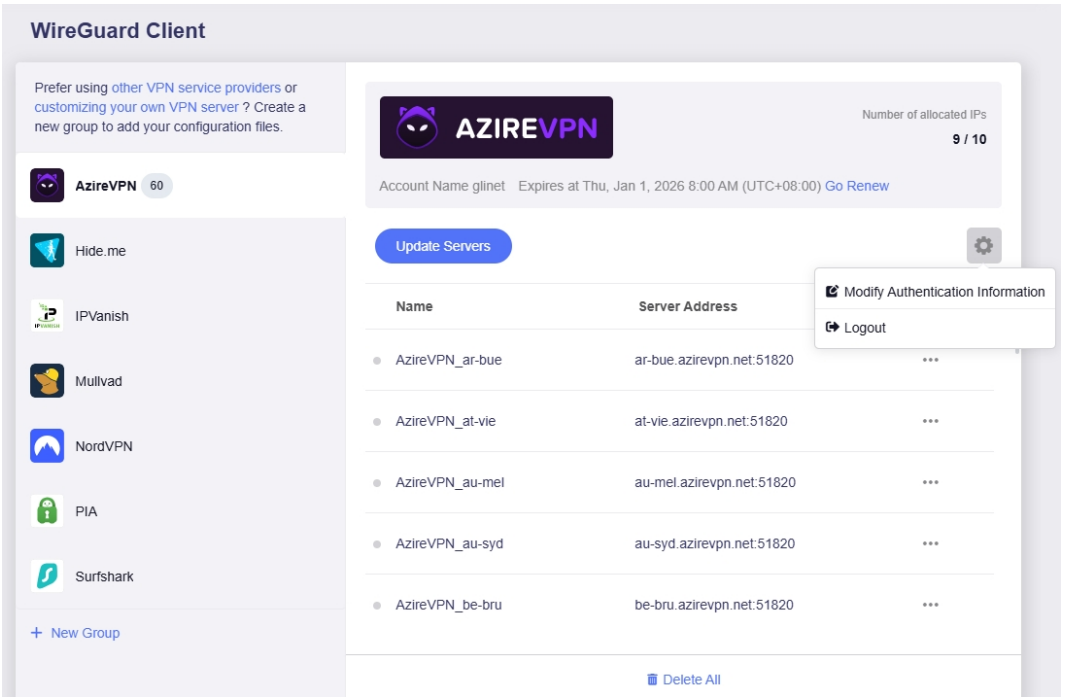
5. Actualizar servidores.

Puedes hacer clic en **Actualice servidores** para obtener la última lista de servidores disponibles, evitando fallas de conexión causadas por el mantenimiento o el apagado del servidor.



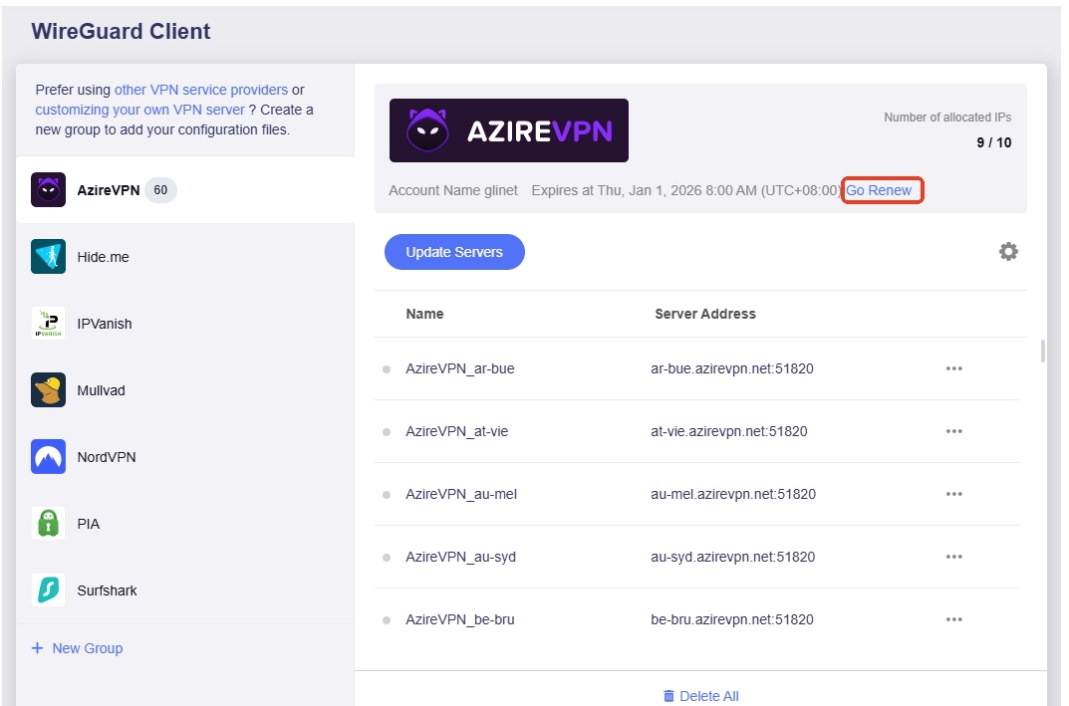
6. Edite las credenciales o cierre sesión.

   Haga clic en el ícono de ajustes para editar sus credenciales de inicio de sesión o cerrar sesión.



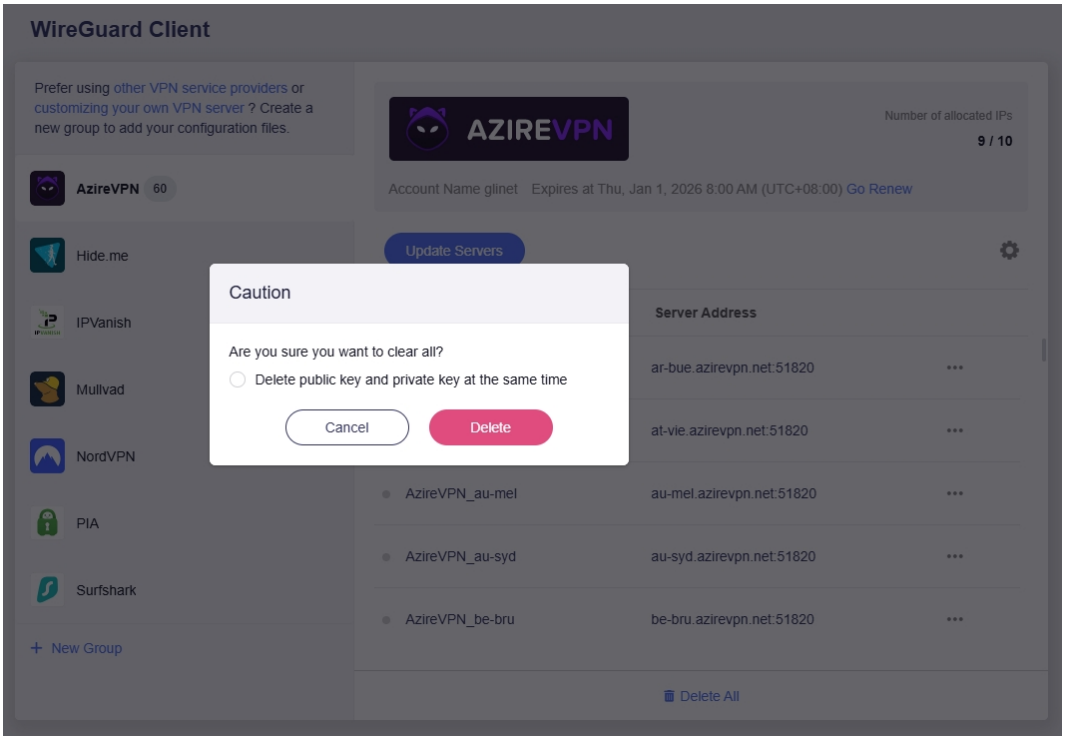

7. Ir a renovar.

   Si haces clic en **Ir a renovar**, serás redirigido al sitio web oficial para renovar tu suscripción.



8. Eliminar todos los archivos.

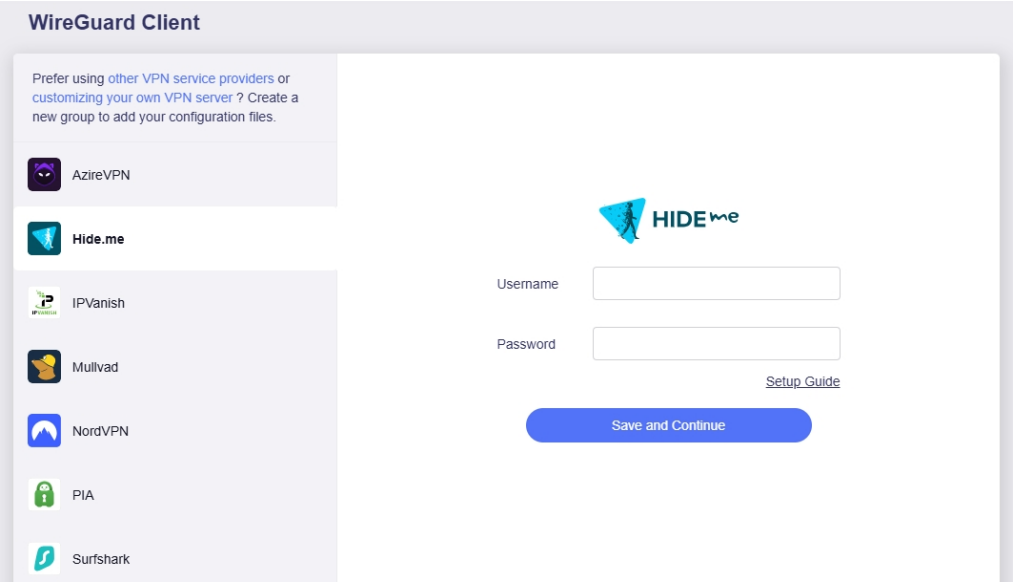
Puede hacer clic en **Eliminar todo** para eliminar todos los archivos de configuración con un solo clic y elegir si desea eliminar las claves públicas y privadas simultáneamente.



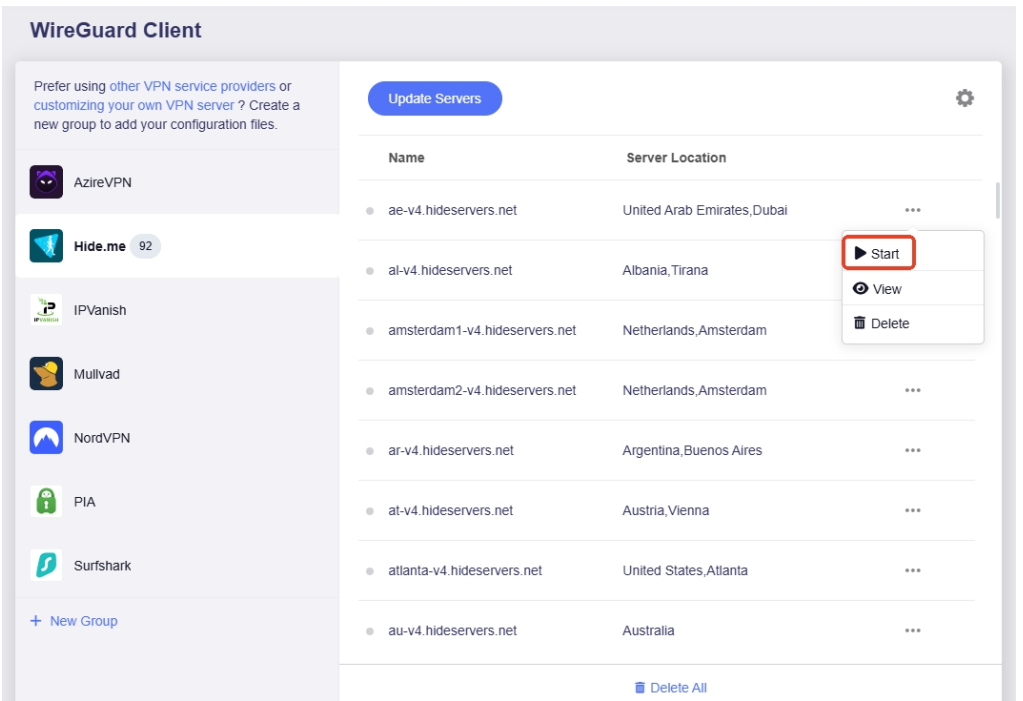
## 11.2.3 Configurar Hide.me

Siga los pasos siguientes para configurar su enrutador como cliente Hide.me.

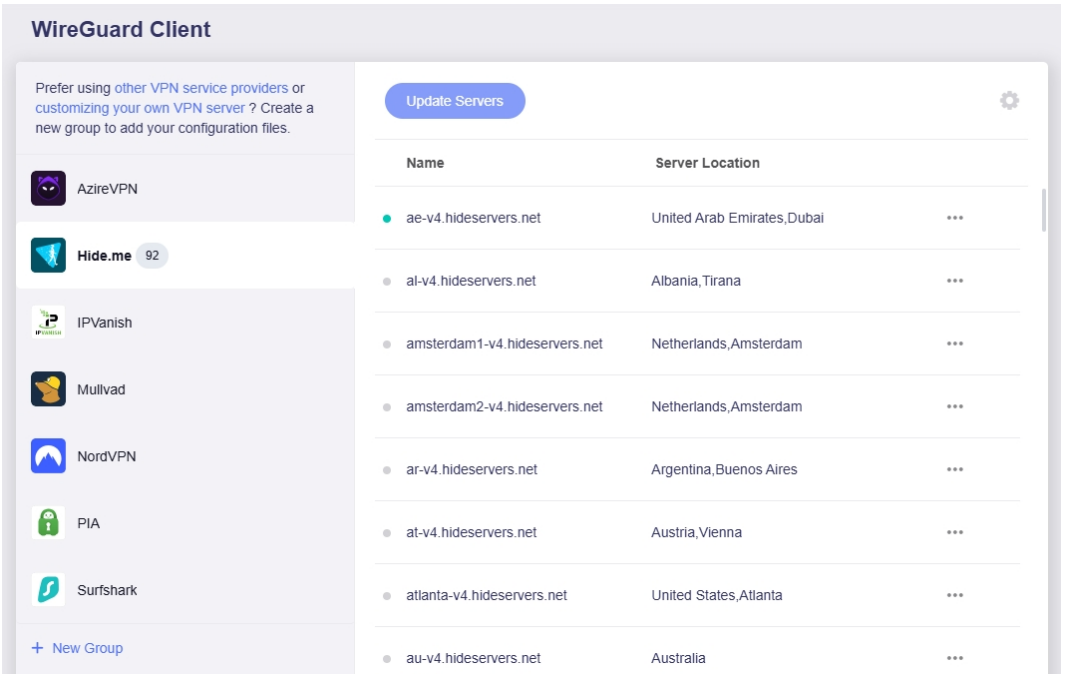
1. Inicie sesiónn en su enrutador’s web admin panel y vaya a **VPN** > **WireGuard Client** > **Hide.me**.
2. Ingrese nombre de usuario y contraseña, luego haga clic en **Guardar y continuar**. Generará archivos de configuración para cada servidor.




3. Seleccione un servidor preferido y haga clic en el icono de tres puntos a la derecha para iniciar una conexión.



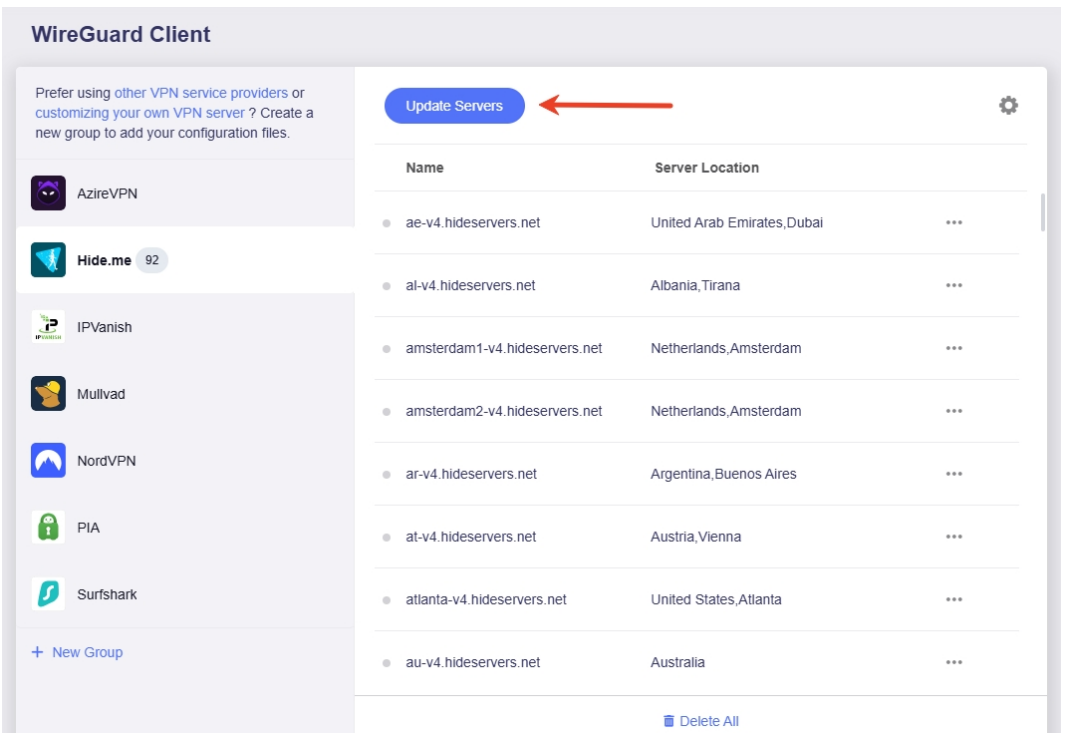
4. Una vez conectado, aparecerá un punto verde junto al archivo de configuración.




Usted puede también verifique los detalles de la conexión VPN en **Panel de VPN**.

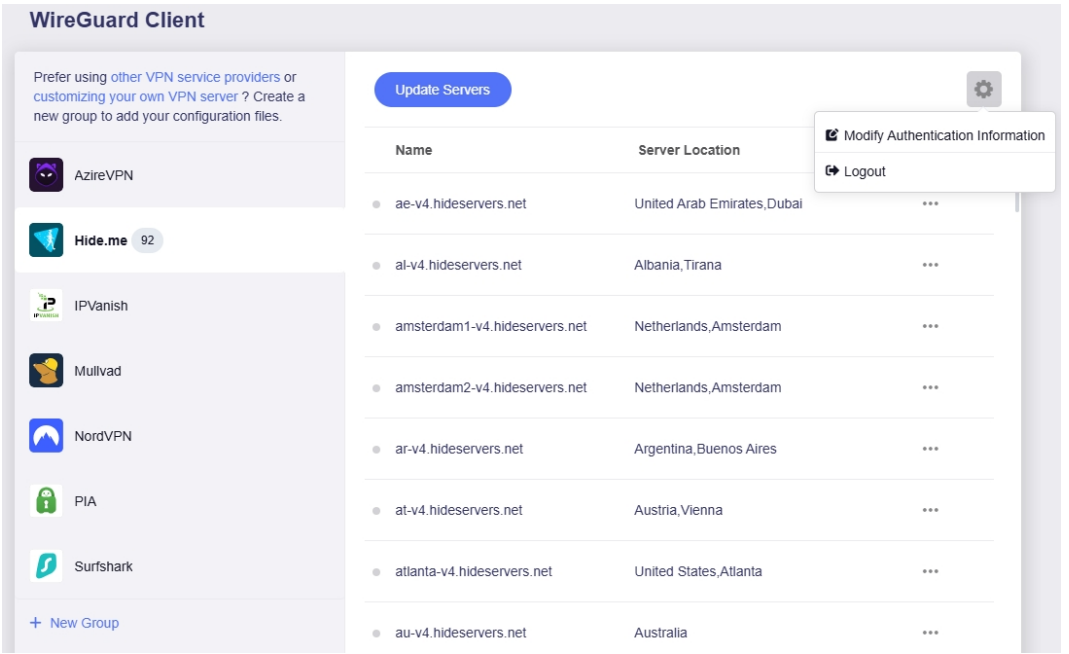
5. Actualizar servidores.

Puede hacer clic en **Actualizar servidores** para obtener la lista de servidores más reciente disponible, evitando fallas de conexión causadas por el mantenimiento o el apagado del servidor.



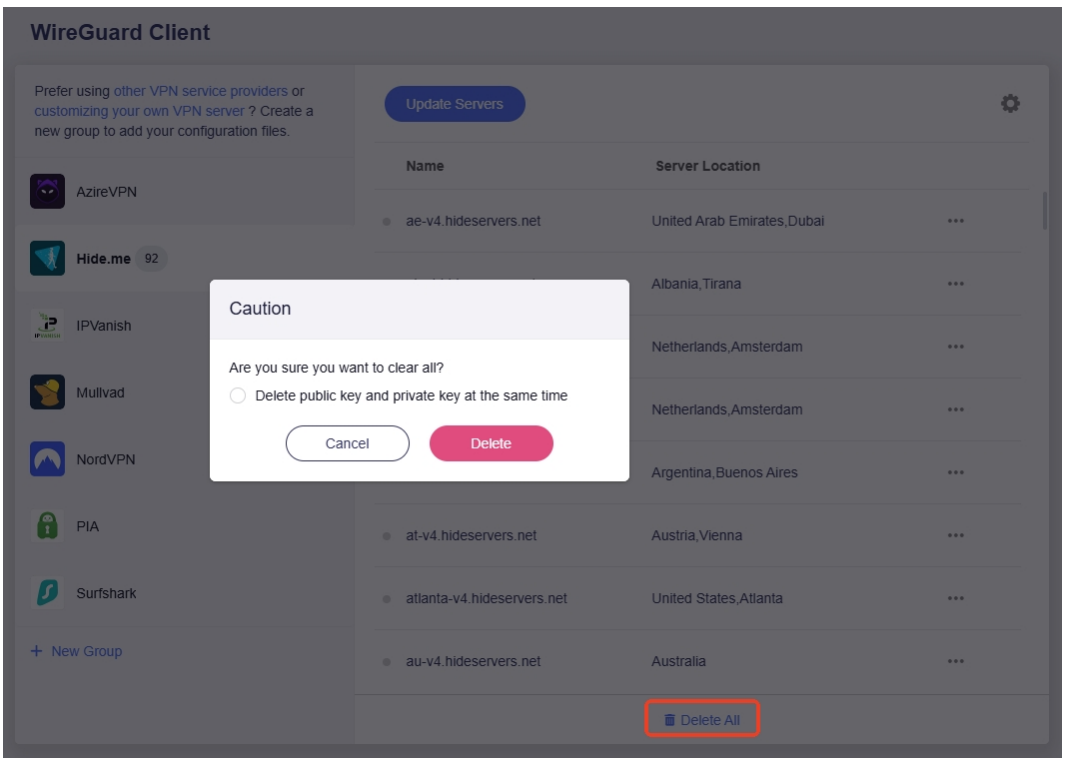
6. Editar credenciales o cerrar sesión.

   Haga clic en el ícono de ajustes para editar sus credenciales de inicio de sesión o cerrar sesión.




7. Eliminar todos los archivos.

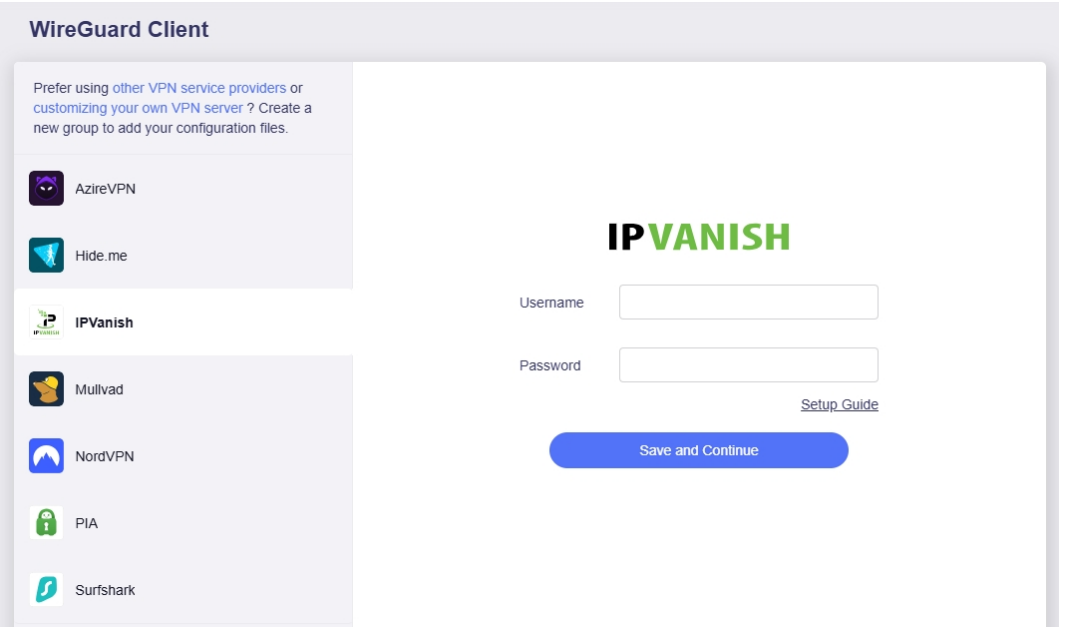
   Puede hacer clic en **Eliminar todo** para eliminar todos los archivos de configuración con un solo clic y elegir si desea eliminar las claves públicas y privadas simultáneamente.



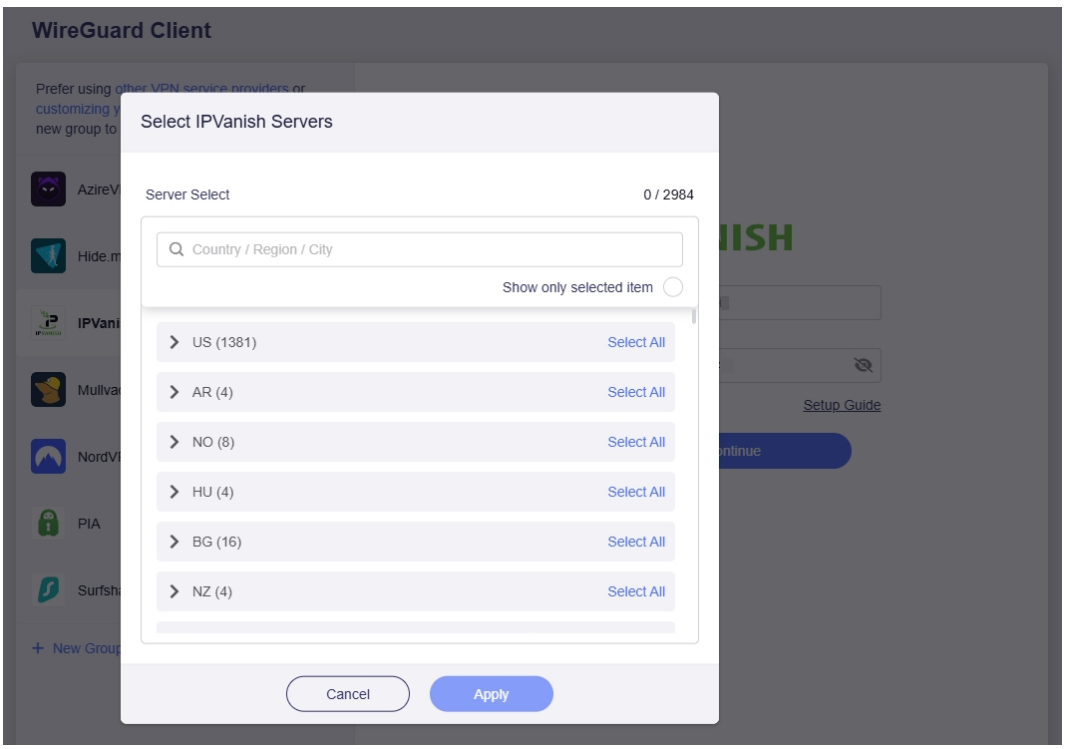
## 11.2.4 Configurar IPVanish

Siga los pasos a continuación para configurar su enrutador como cliente IPVanish.

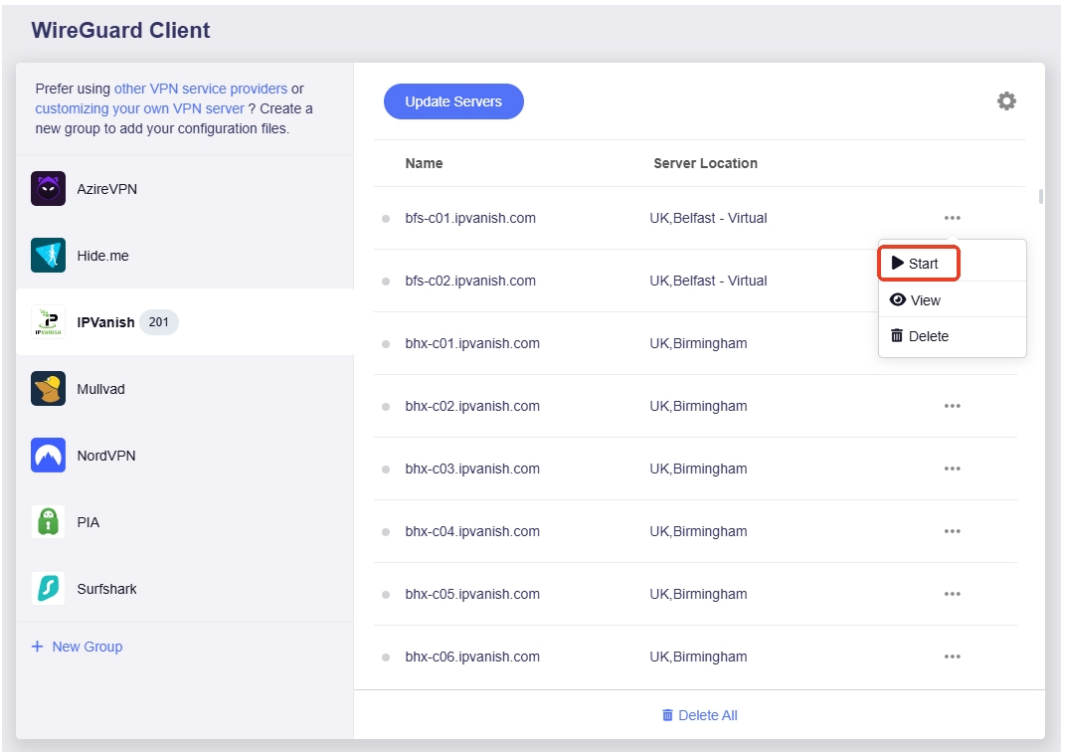
1. Inicie sesiónn en su enrutador’s web admin panel y vaya a **VPN** > **Cliente WireGuard** > **IPVanish**.
2. Ingrese nombre de usuario y contraseña, luego haga clic en **Guardar y continuar**.



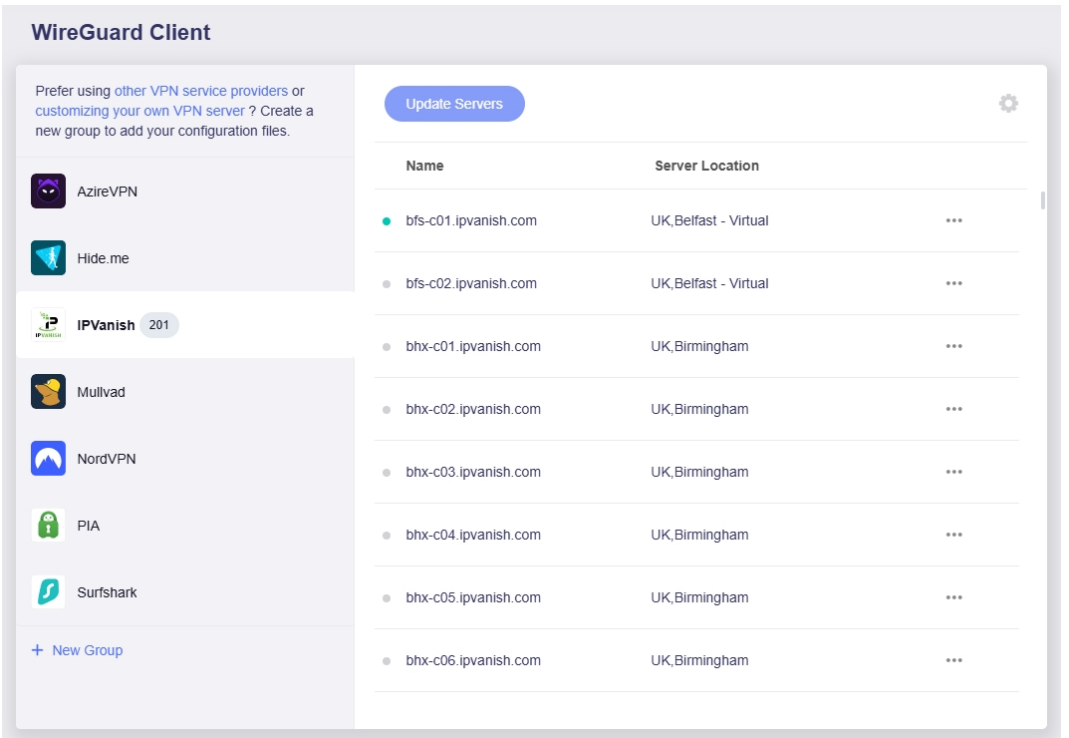

3. Seleccione los servidores a los que desea conectarse y haga clic en **Aplicar**.



4. Seleccione un servidor preferido y haga clic en el icono de tres puntos a la derecha para iniciar una conexión.



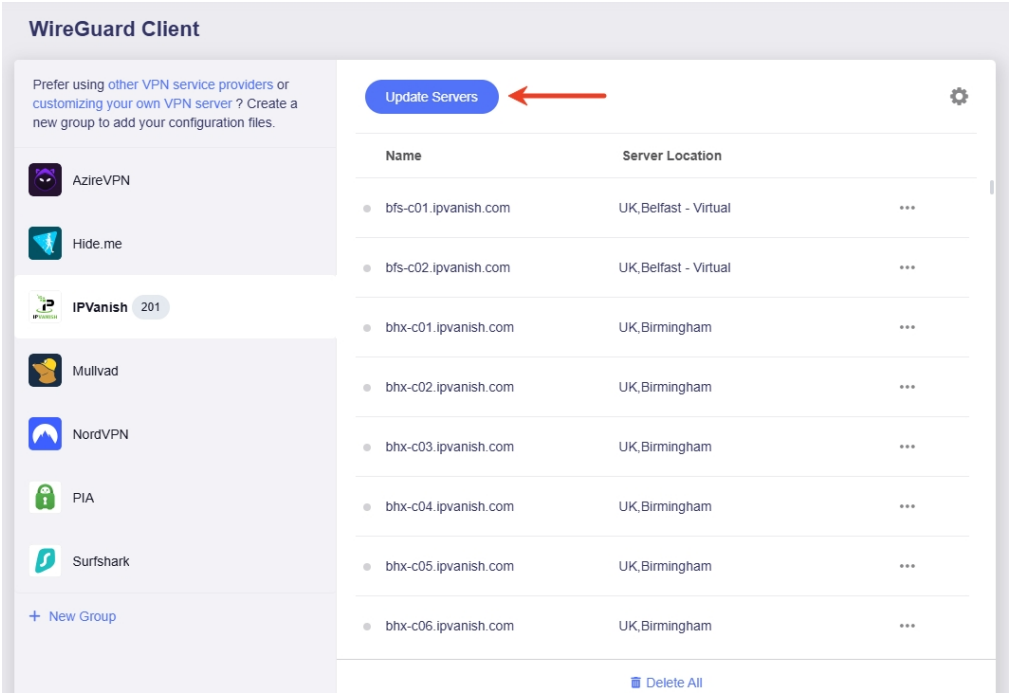

5. Una vez conectado, aparecerá un punto verde junto al archivo de configuración.




Usted puede también verificar los detalles de conexión VPN en **Panel de VPN**.

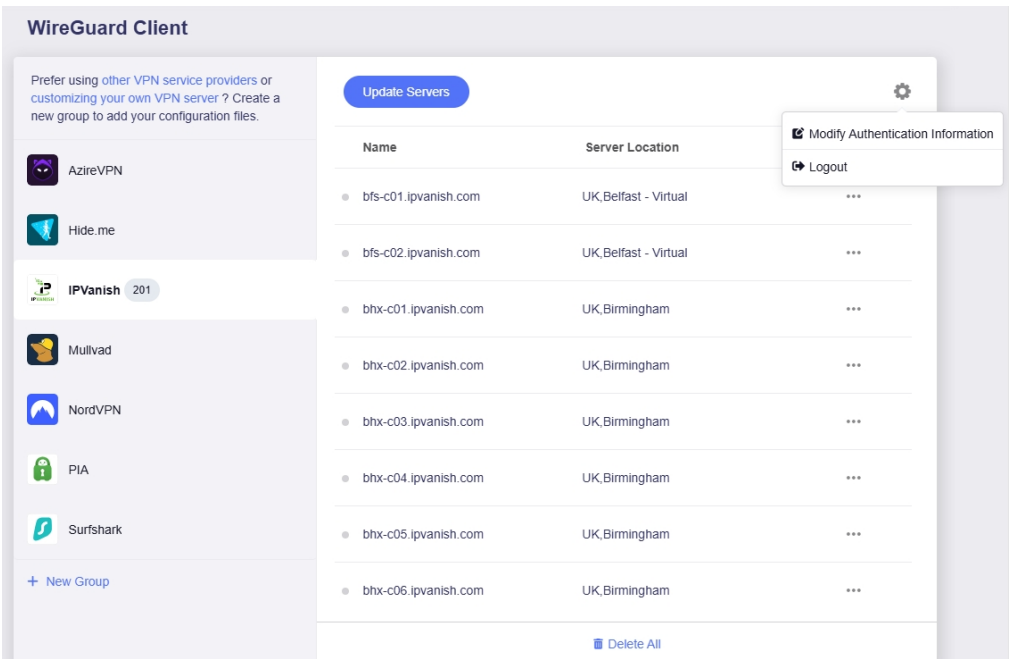
6. Actualizar servidores.

Puedes hacer clic en **Actualizar servidores** para obtener la lista de servidores más reciente disponible, evitando fallas de conexión causadas por el mantenimiento o el apagado del servidor.



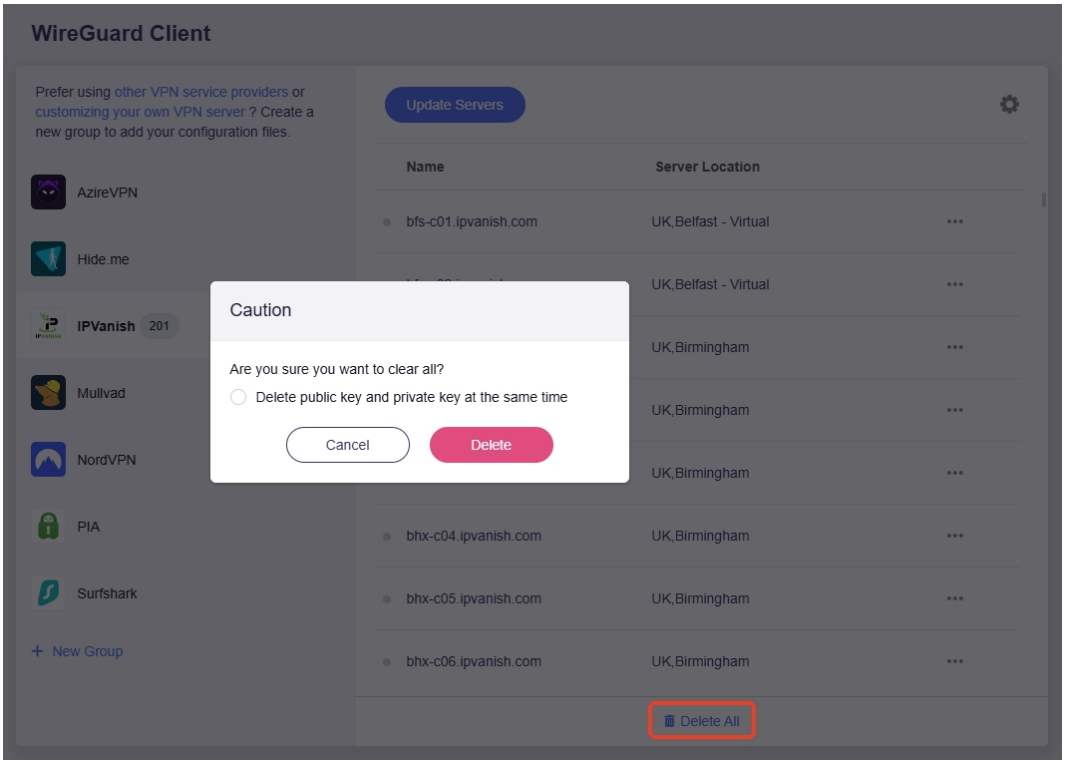

7. Edite las credenciales o cierre sesión.

Haga clic en el ícono de ajustes para editar sus credenciales de inicio de sesión o cerrar sesión.



8. Eliminar todos los archivos.

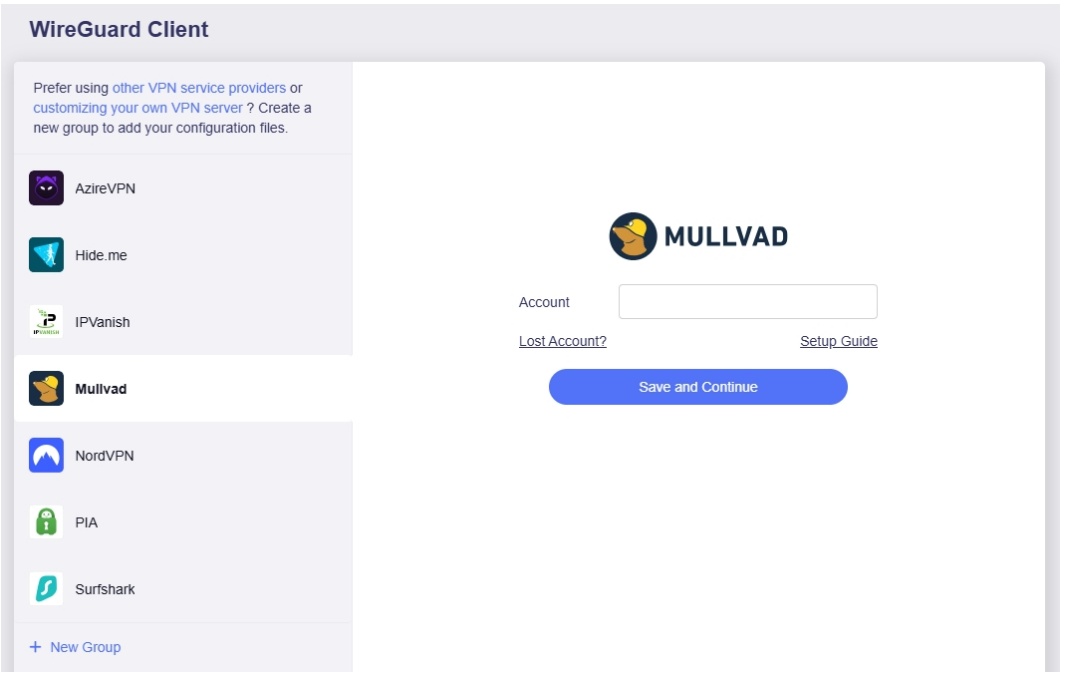
Puede hacer clic en **Eliminar todo** para eliminar todos los archivos de configuración con un solo clic y elegir si desea eliminar las claves públicas y privadas simultáneamente.



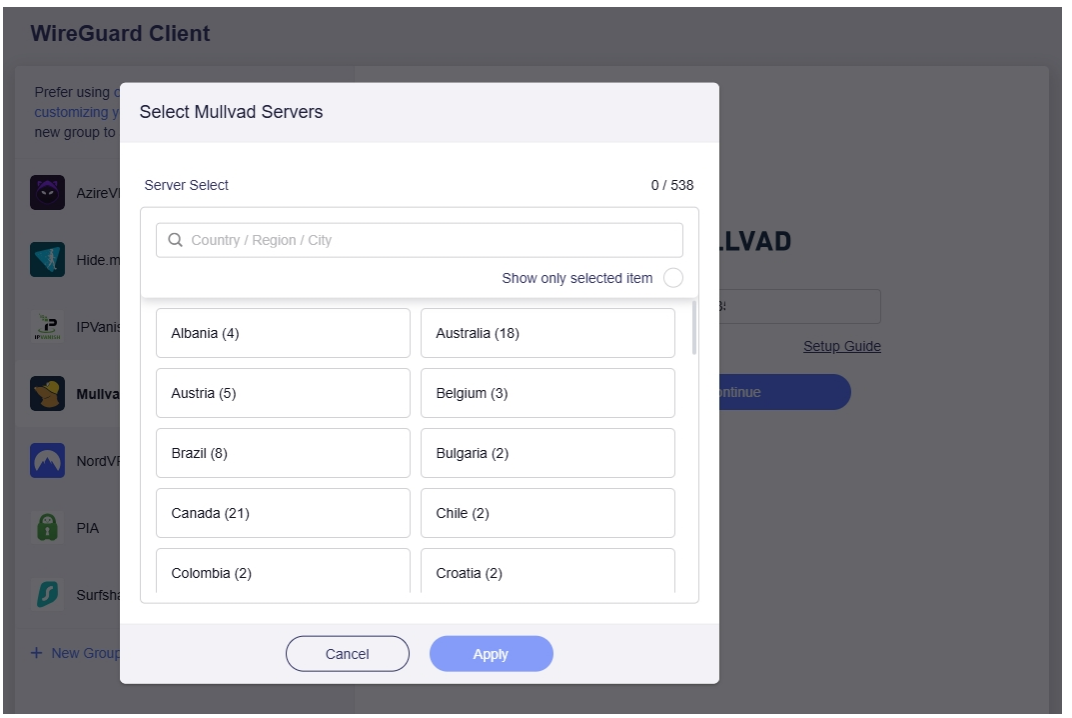
## 11.2.5 Configurar Mullvad

Siga los pasos siguientes para configurar su enrutador como cliente Mullvad.

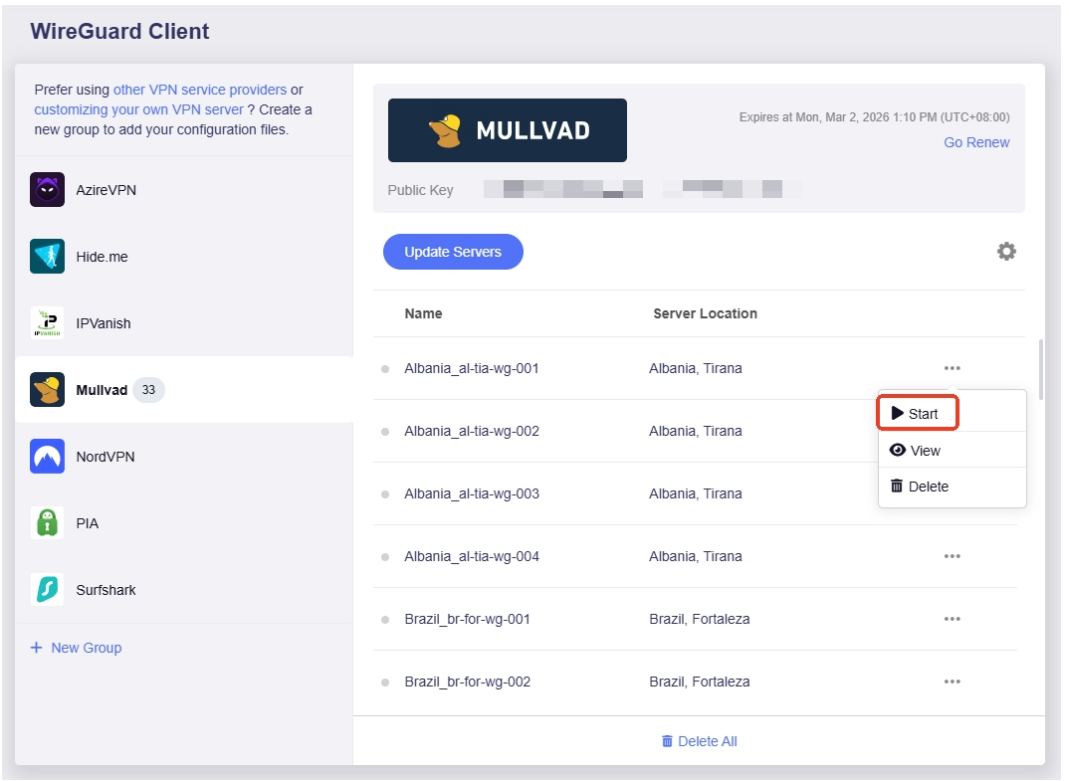
1. Inicie sesiónn en su enrutador’s web admin panel y vaya a **VPN** > **WireGuard Client** > **Mullvad**.
2. Ingrese el nombre de usuario y la contraseña, luego haga clic en **Guardar y Continuar**.



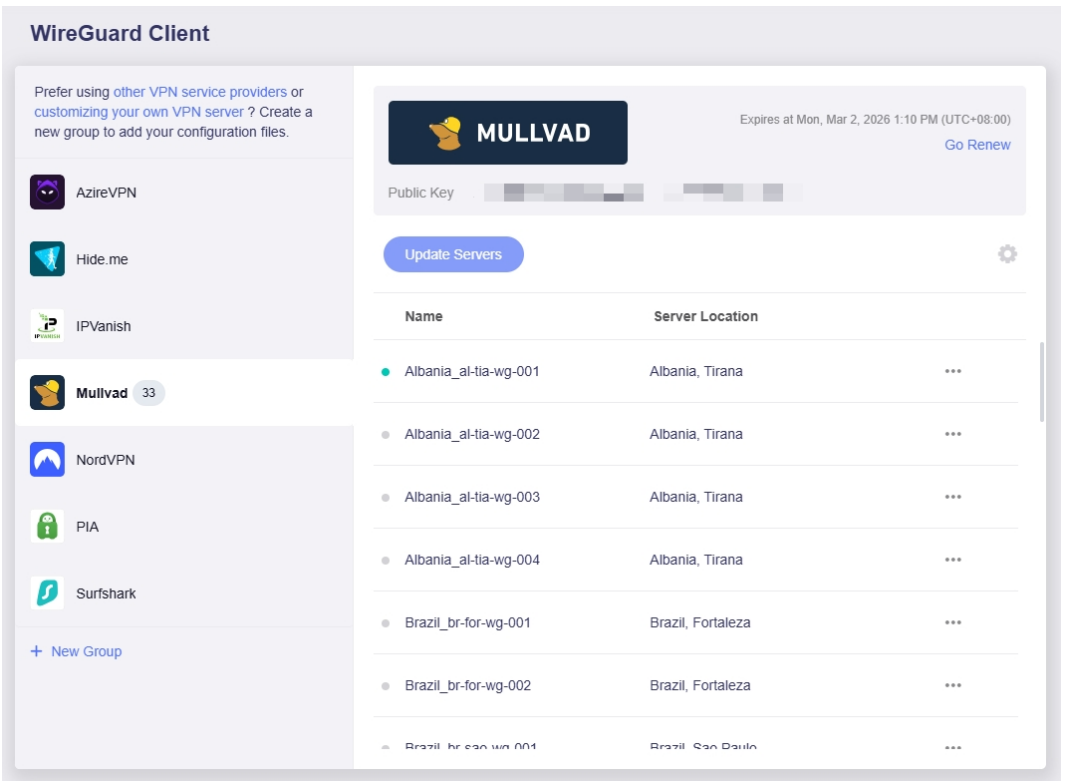

3. Seleccione los servidores a los que desea conectarse y haga clic en **Aplicar**.



4. Seleccione un servidor preferido y haga clic en el icono de tres puntos a la derecha para iniciar una conexión.



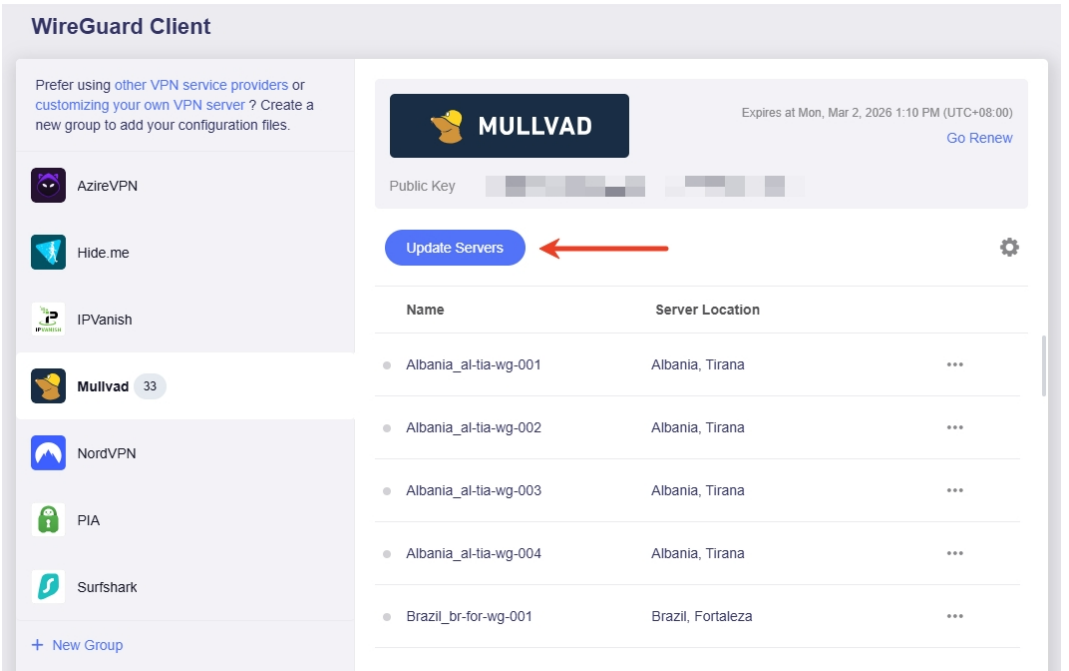

5. Una vez conectado, aparecerá un punto verde junto al archivo de configuración.



Tú puedes también verifique los detalles de la conexión VPN en el **Panel de VPN**.

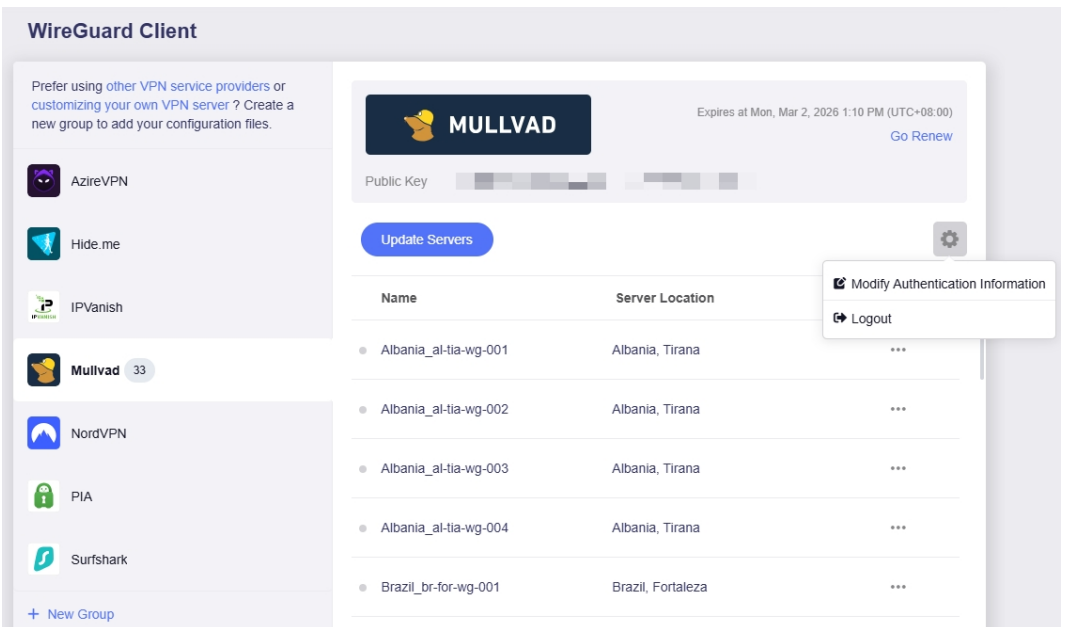
6. Actualizar servidores.

   Puede hacer clic en **Actualizar servidores** para obtener la lista de servidores más reciente disponible, evitando fallas de conexión causadas por el mantenimiento o el apagado del servidor.



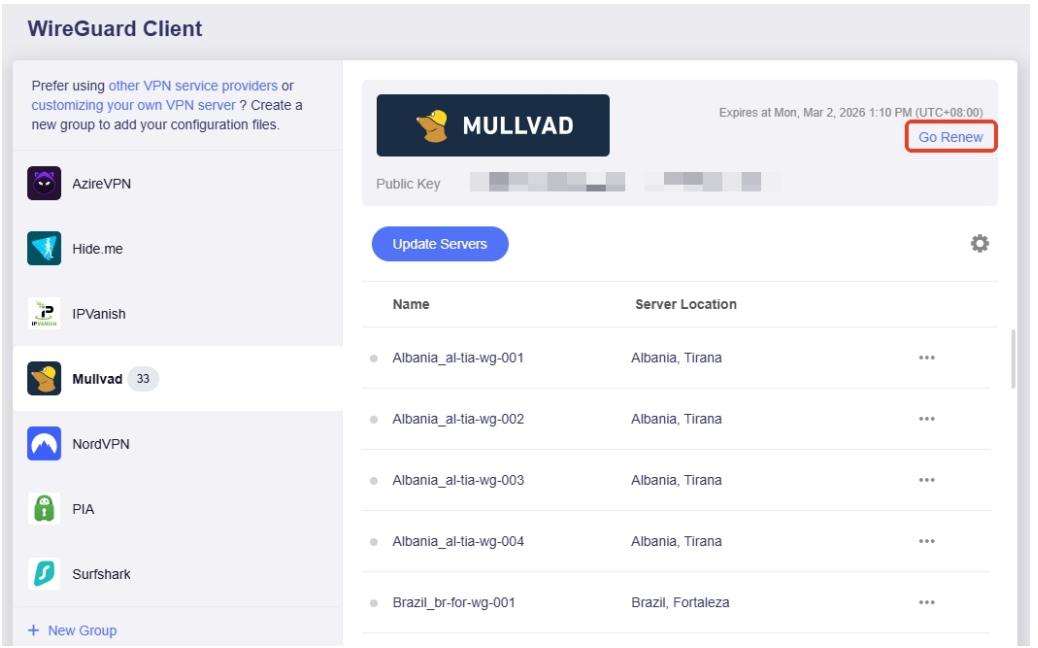

7. Editar credenciales o cerrar sesión.

   Haga clic en el ícono de ajustes para editar sus credenciales de inicio de sesión o cerrar sesión.



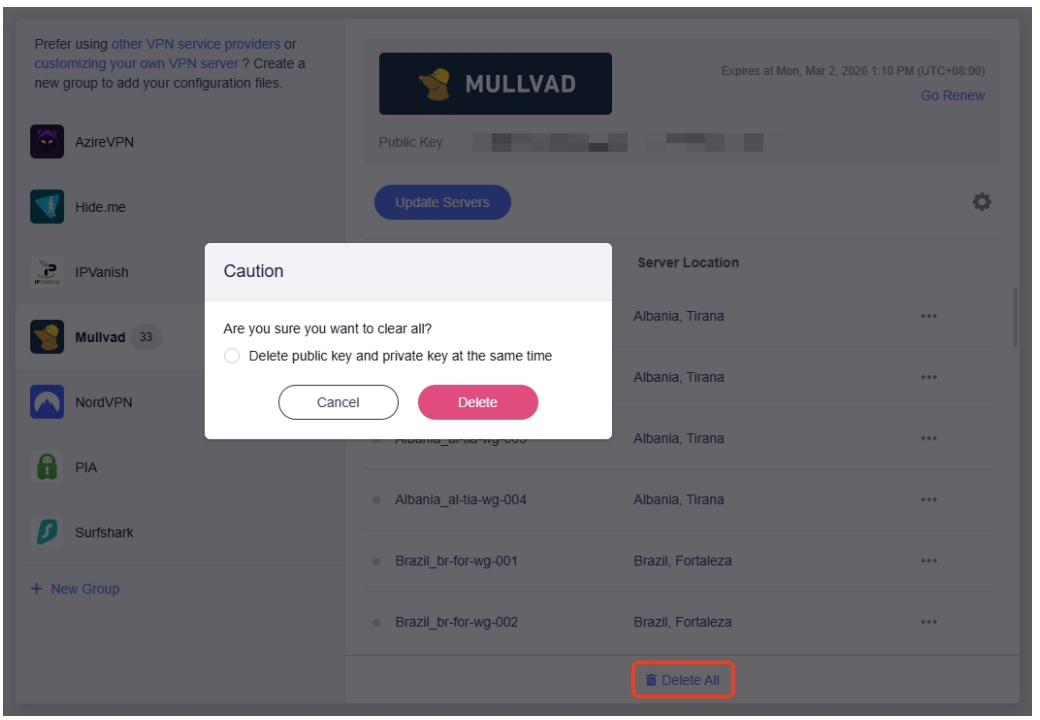
8. Ir a renovar.

   Si hace clic en **Ir a renovar**, será redirigido a sitio web oficial para renovar su suscripción.




9. Eliminar todos los archivos.

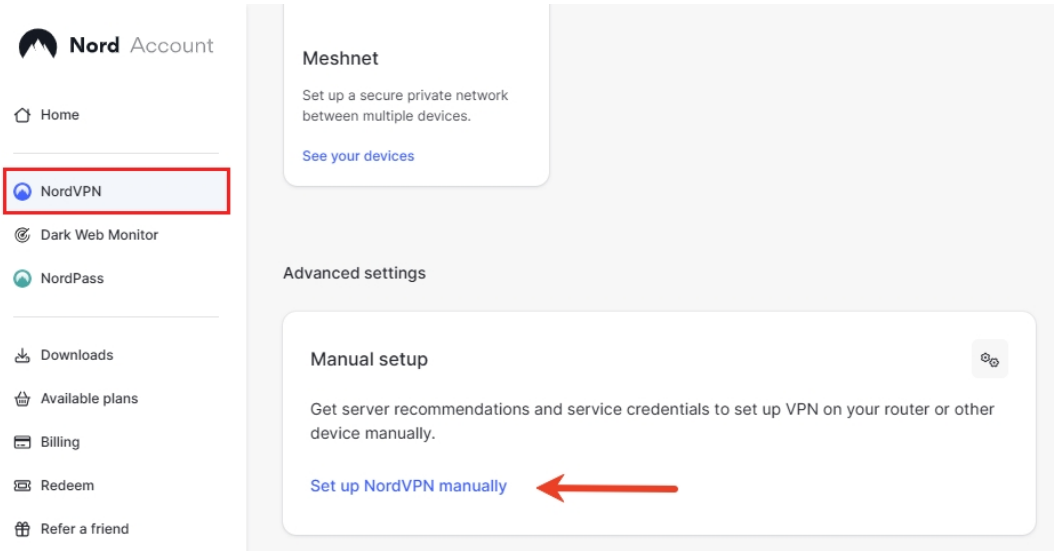
   Puede hacer clic en **Eliminar todo** para eliminar todos los archivos de configuración con un solo clic y elegir si desea eliminar el archivo privado. y claves públicas simultáneamente.



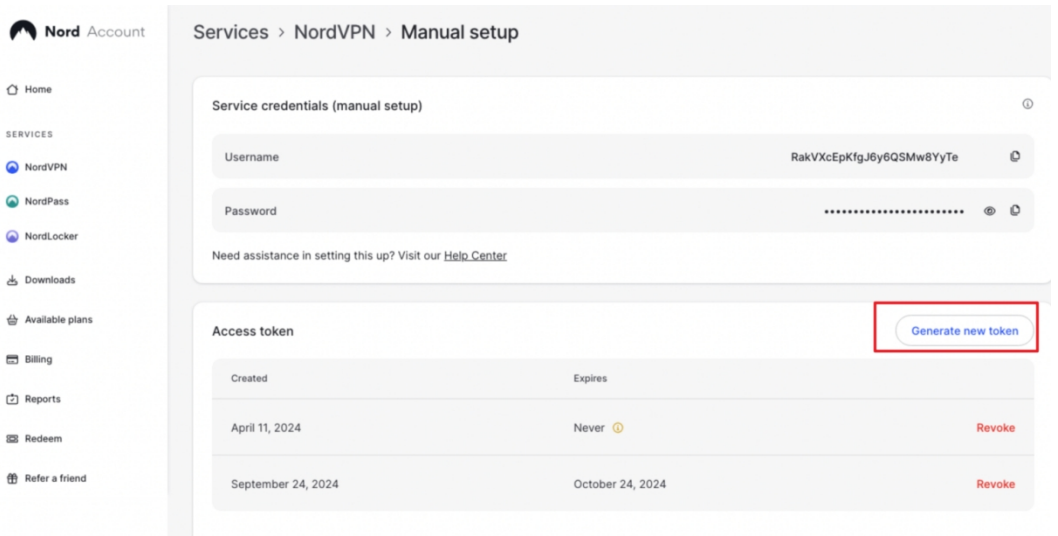
## 11.2.6 Configurar NordVPN

Siga los pasos a continuación para configurar su enrutador como cliente NordVPN.

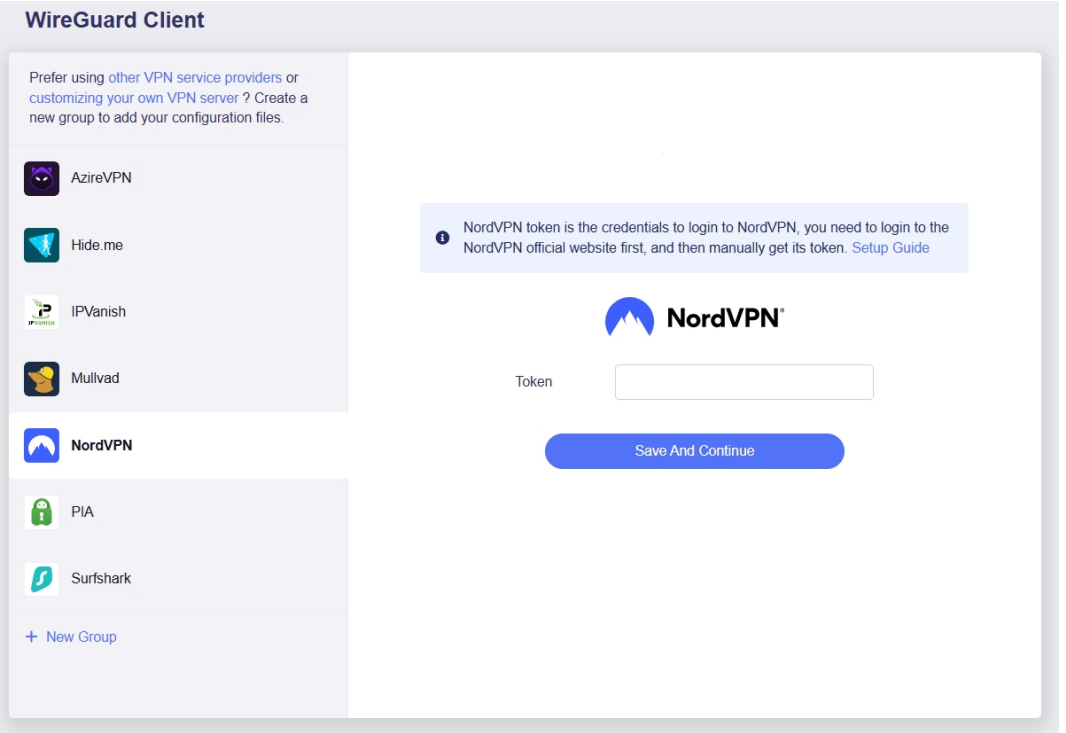
1. Inicie sesión en su cuenta web NordVPN aquí.
2. Oen el Nord Dashboard, haga clic en **NordVPN** y luego haga clic en **Configurar NordVPN manualmente**.



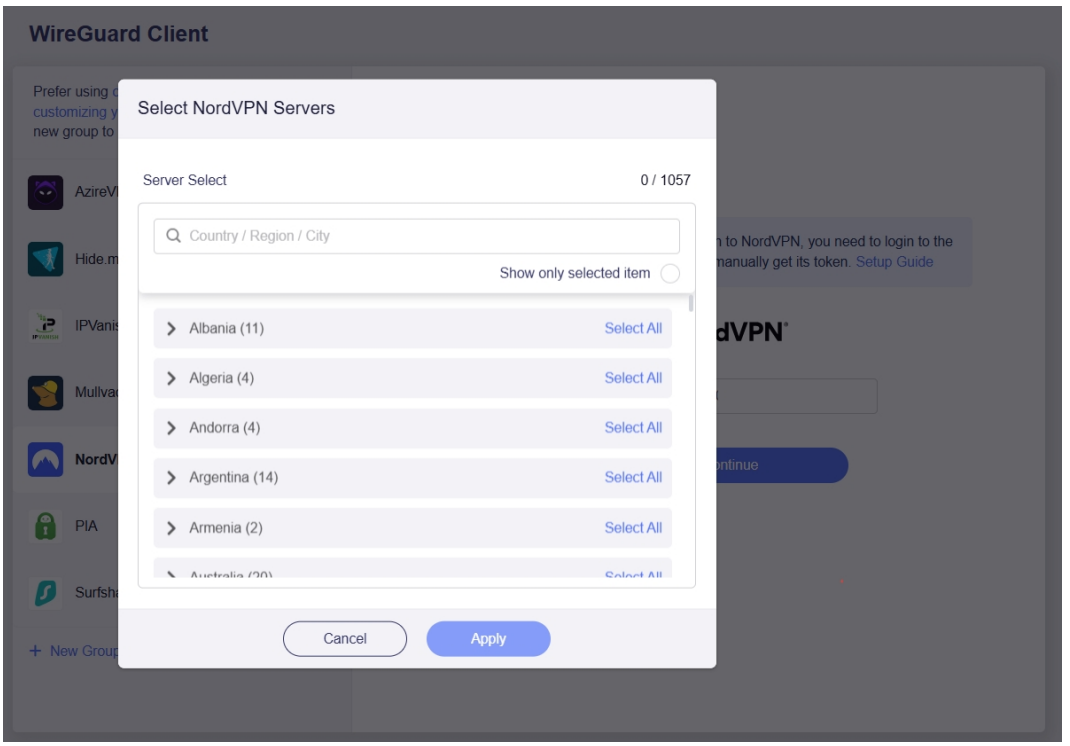

Encontrará el **Token de acceso**. Cree un token de acceso y copiecopia para usarlo más adelante.



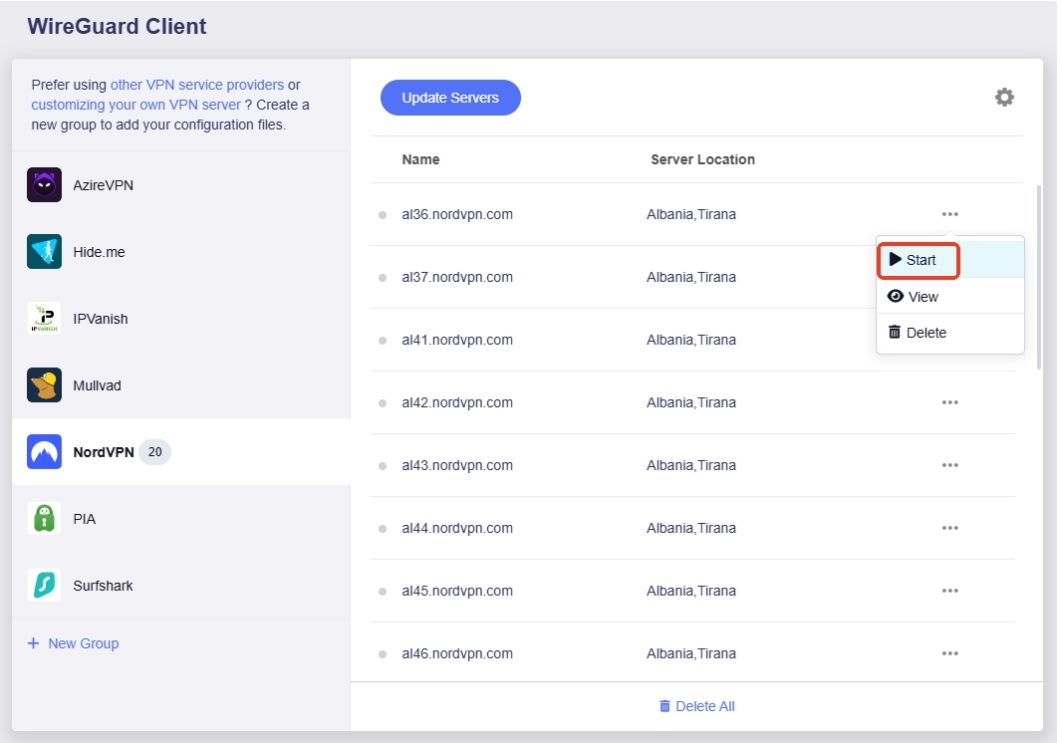

3. Inicie sesiónn en su enrutador's web admin panel y vaya a **VPN** > **Cliente WireGuard** > **NordVPN**.
4. Entrada token, y haga clic en **Guardar y continuar**.



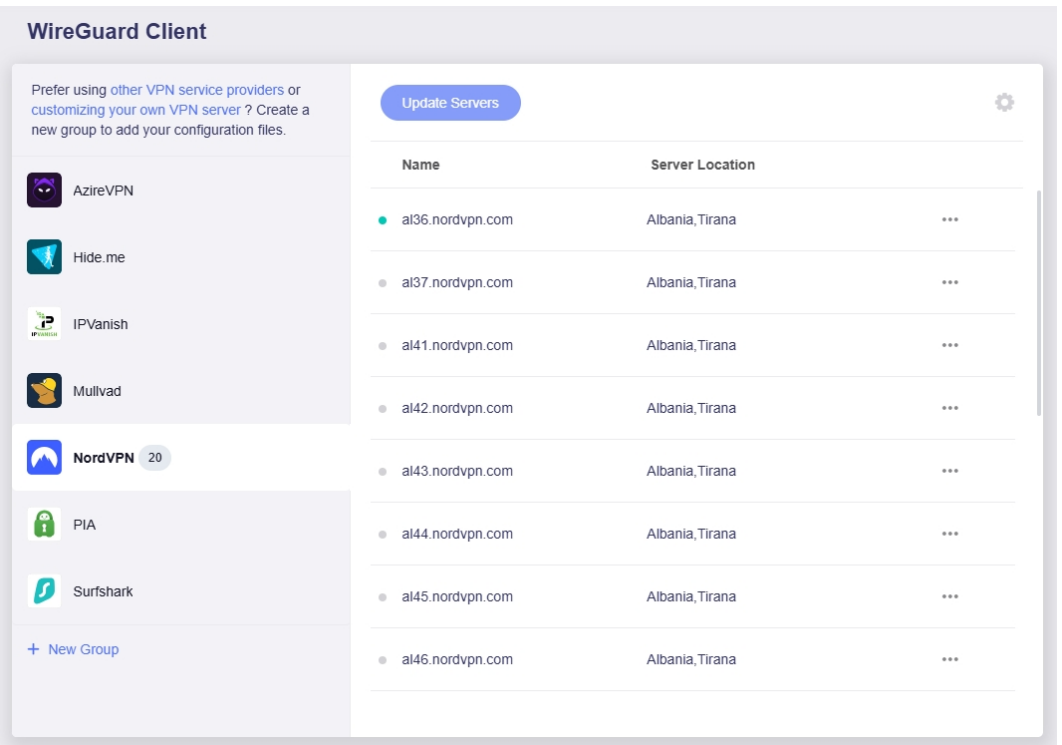

5. Seleccione los servidores a los que desea conectarse y haga clic en **Aplicar**.




6. Seleccione un servidor preferido y haga clic en el icono de tres puntos a la derecha para iniciar una conexión.



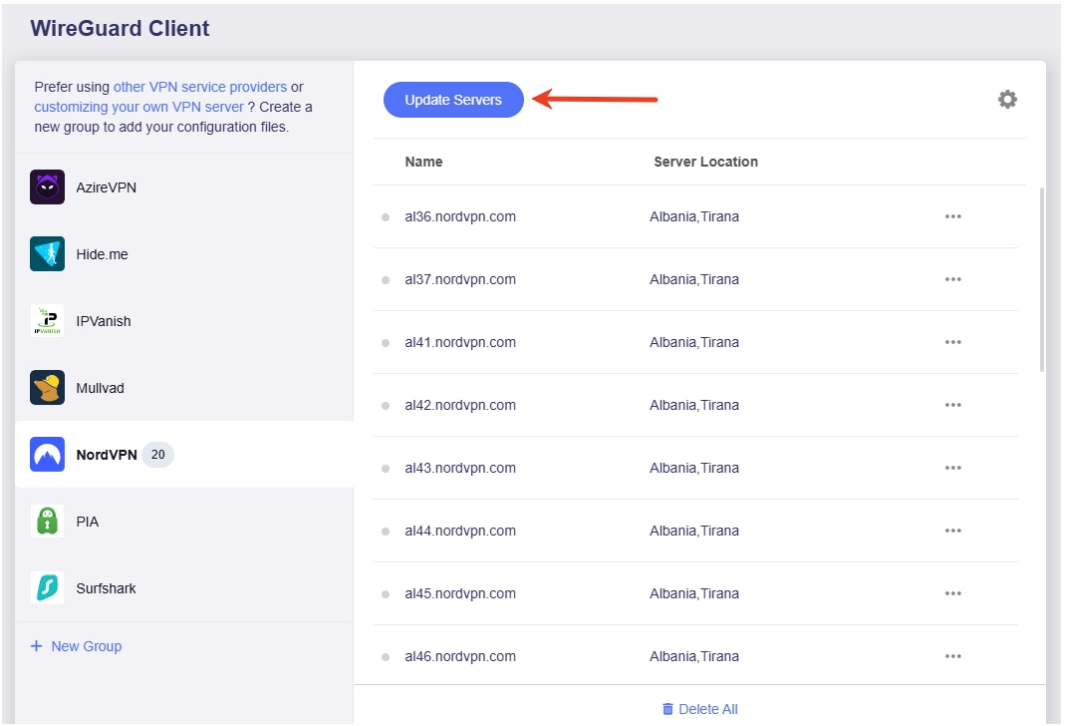

7. Una vez conectado, aparecerá un punto verde junto al archivo de configuración.




Tú puedes también comprobar el Detalles de la conexión VPN en **Panel de VPN**.

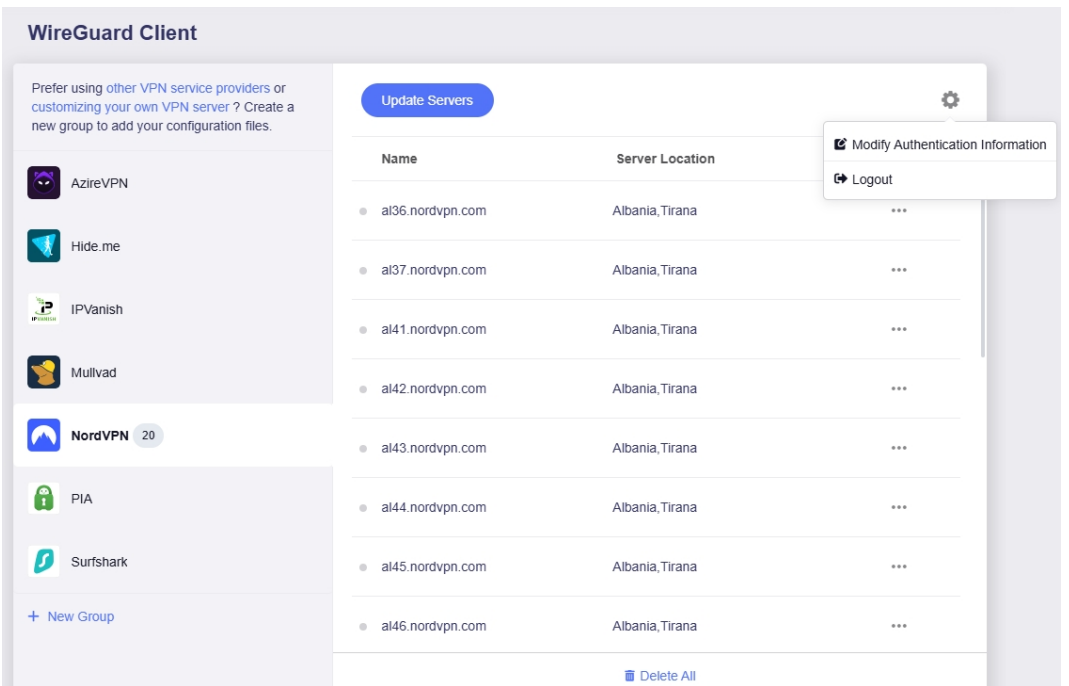
8. Actualizar servidores.

Puedes hacer clic en **Actualice servidores** para obtener la última lista de servidores disponibles, evitando fallas de conexión causadas por el mantenimiento o el apagado del servidor.



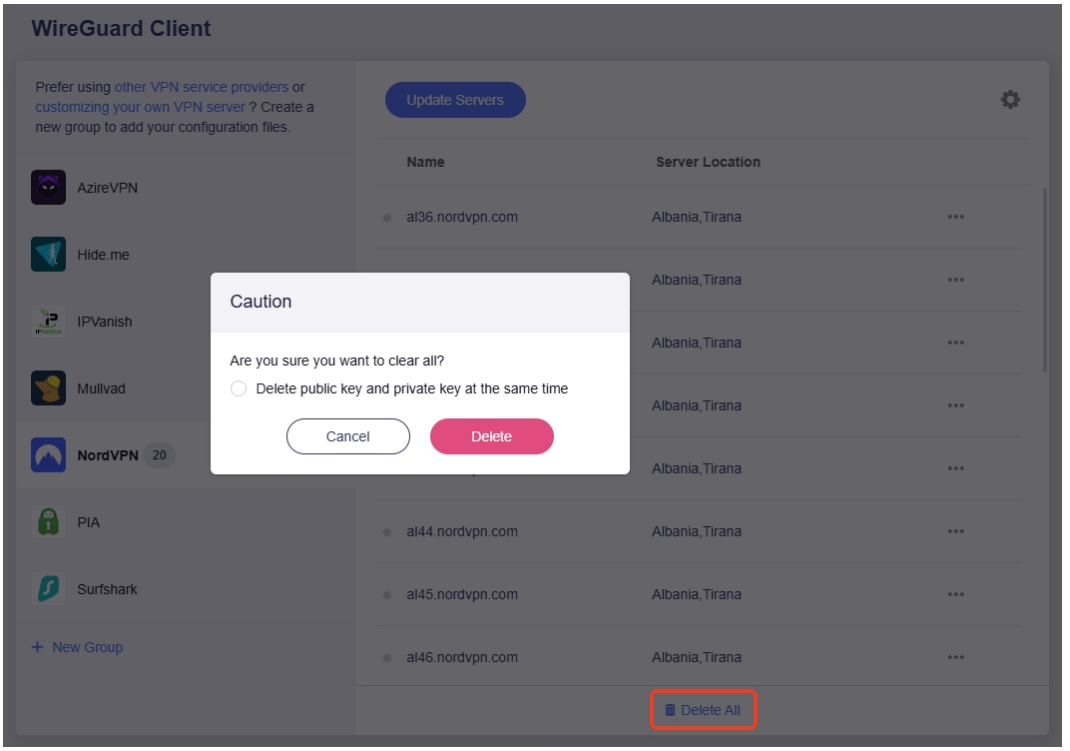

9. Edite las credenciales o cierre sesión.

   Haga clic en el ícono de ajustes para editar sus credenciales de inicio de sesión o cerrar sesión.



10. Eliminar todos los archivos.

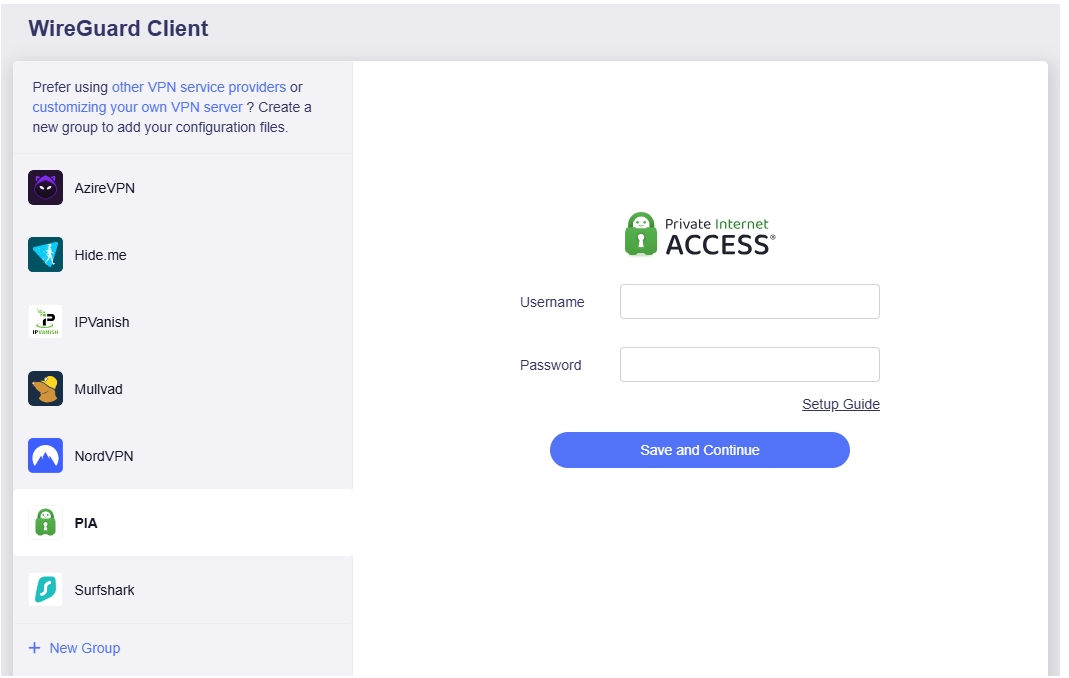
    Puede hacer clic en **Eliminar todo** para eliminar todos los archivos de configuración con un solo clic y elegir si desea eliminar las claves pública y privada simultáneamente.



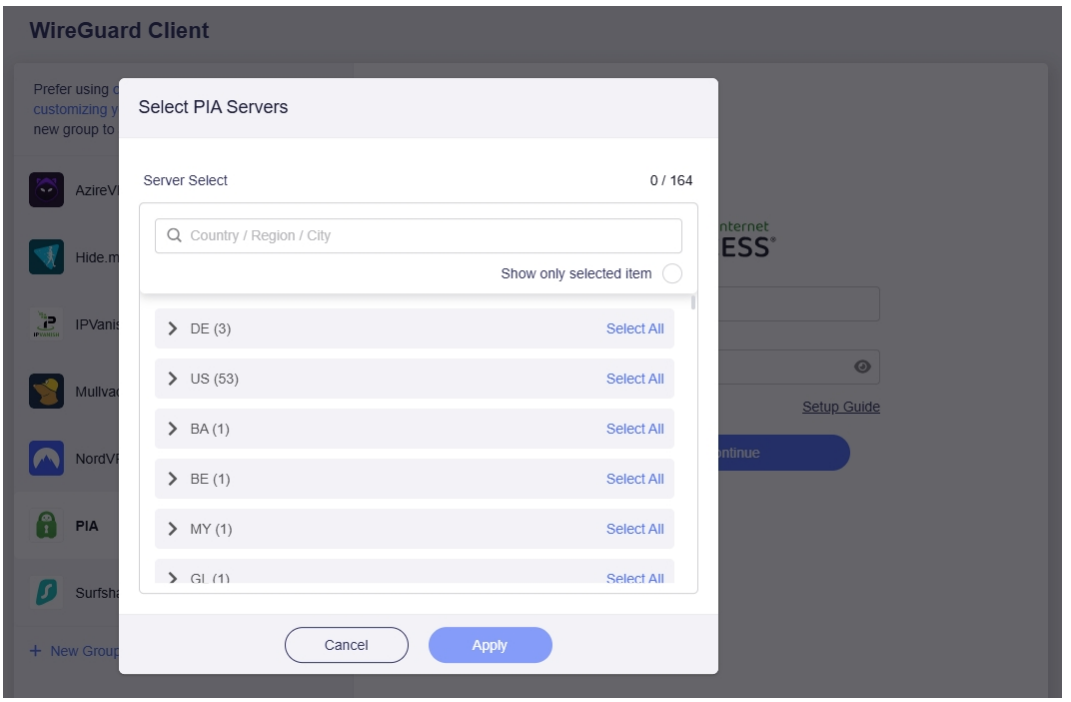
## 11.2.7 Configurar PIA (Private Internet Access)

Siga los pasos siguientes para configurar su enrutador como cliente PIA.

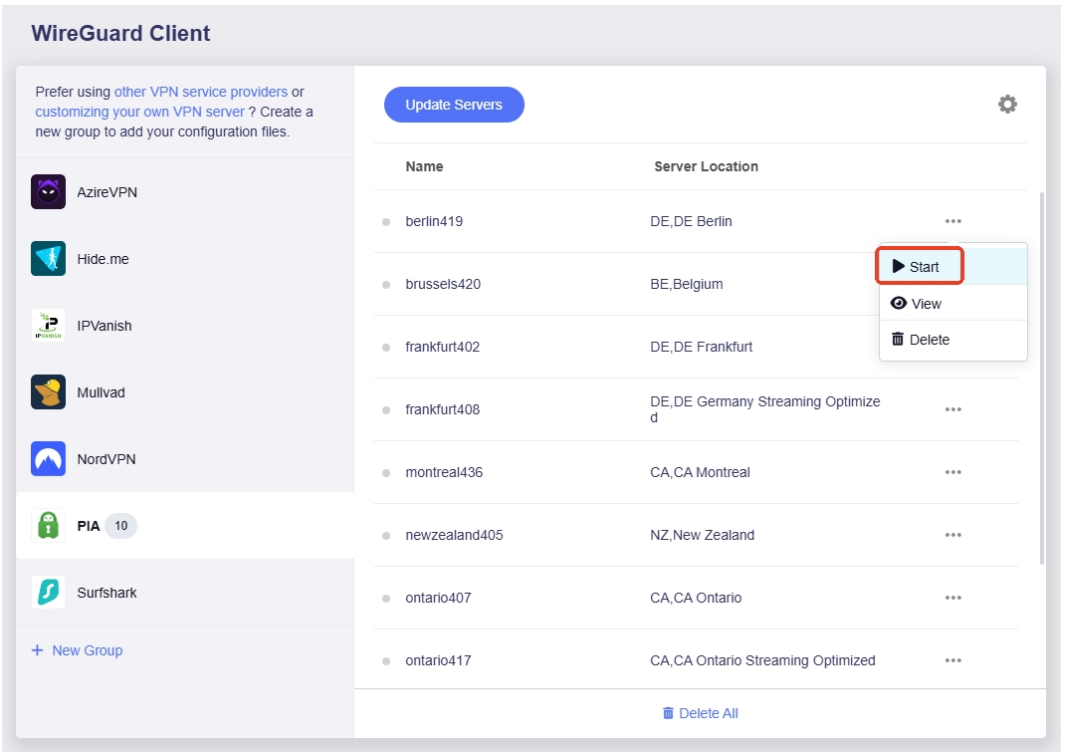
1. Inicie sesiónn en su enrutador’s web admin panel y vaya a **VPN** > **WireGuard Client** > **PIA**.
2. Ingrese el nombre de usuario y la contraseña, luego haga clic en **Guardar y continuar**.



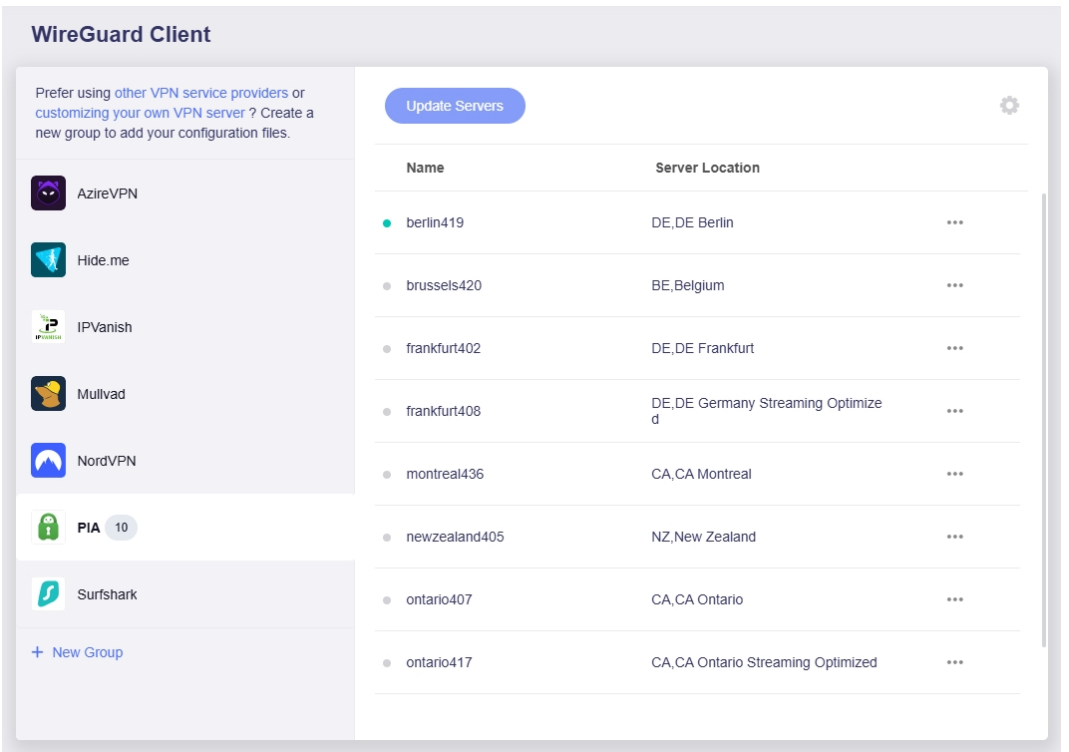

3. Seleccione los servidores a los que desea conectarse y haga clic en **Aplicar**.



4. Seleccione uno preferido. servidor y haga clic en el icono de tres puntos a la derecha para iniciar una conexión.



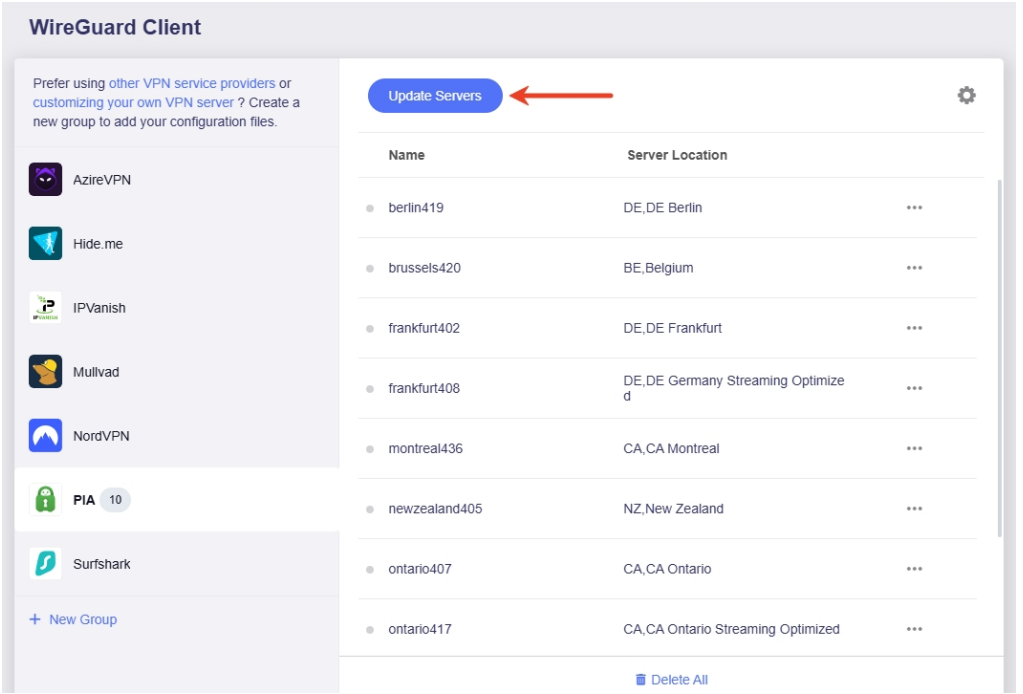

5. Una vez conectado, aparecerá un punto verde junto al archivo de configuración.




También puede comprobar los detalles de la conexión VPN en el **Panel de VPN**.

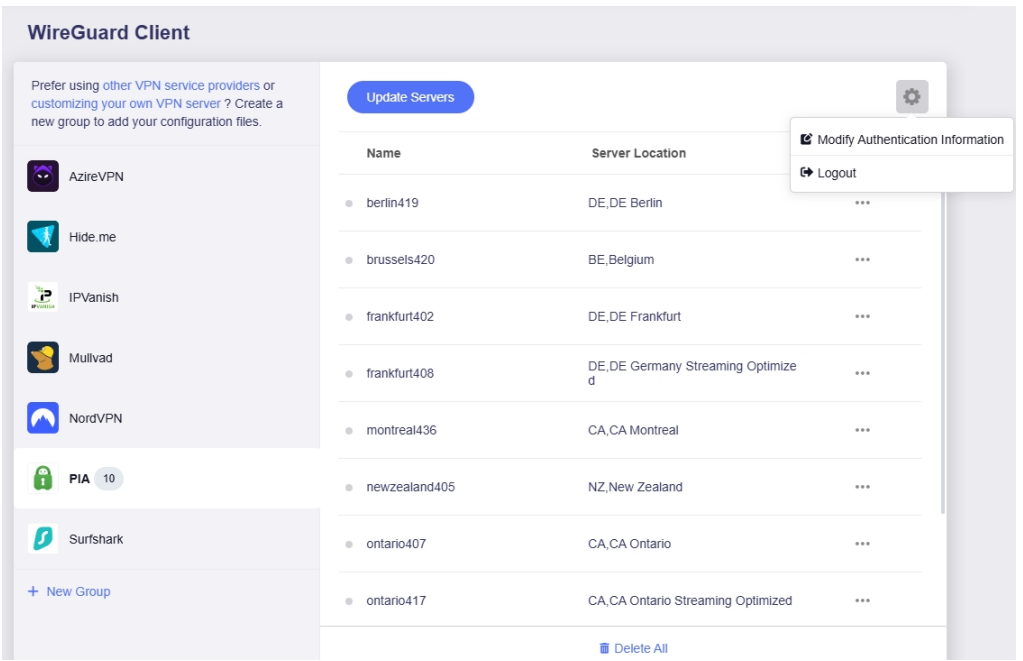
6. Actualizar servidores.

Puedes haga clic en **Actualizar servidores** para obtener la última lista de servidores disponibles, evitando fallas de conexión causadas por el mantenimiento o el apagado del servidor.



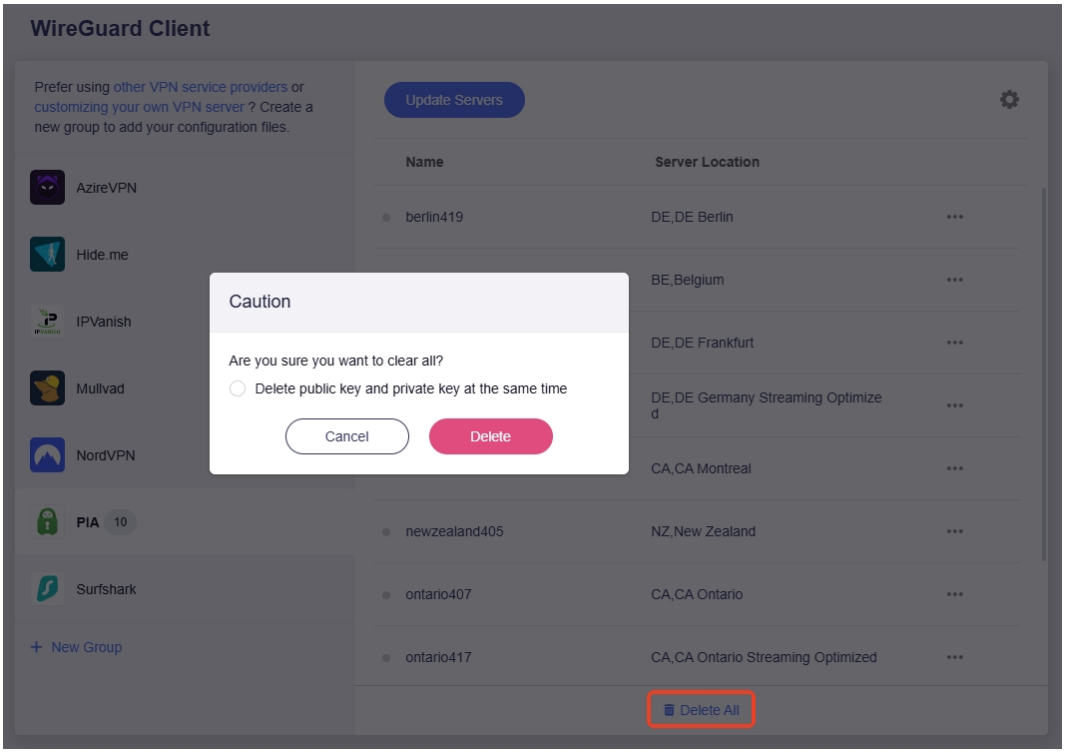

7. Edite las credenciales o cierre sesión.

Haga clic en el ícono de ajustes para editar sus credenciales de inicio de sesión o cerrar sesión.



8. Eliminar todos los archivos.

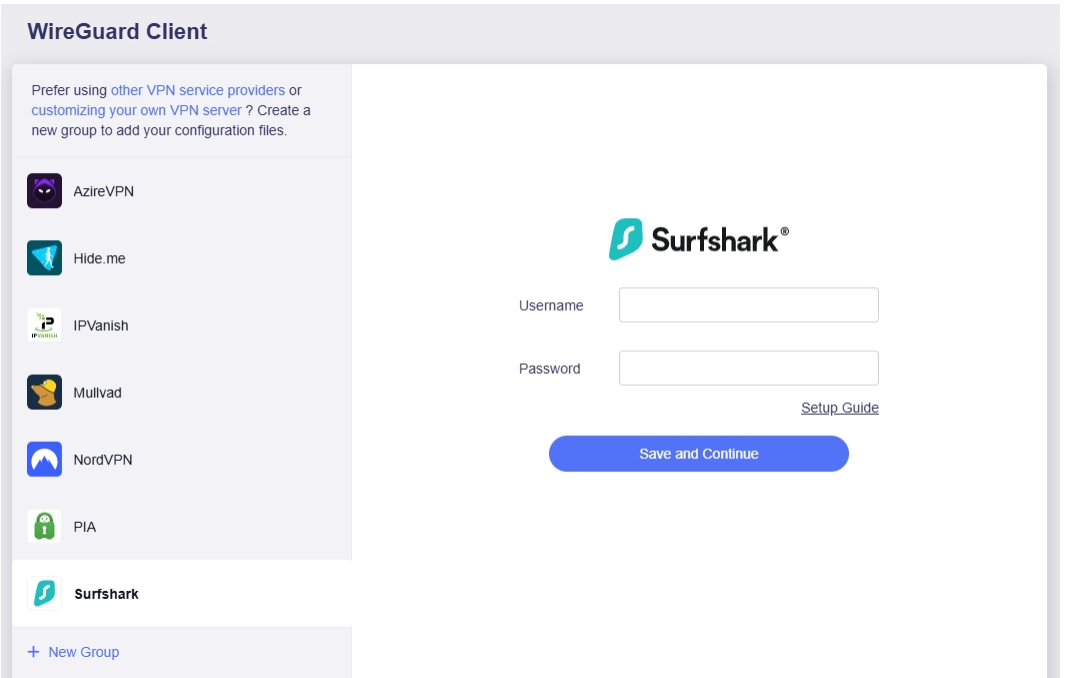
Puedes hacer clic en **Eliminar todo** para eliminar todos los archivos de configuración con un solo clic y elija si desea eliminar las claves pública y privada simultáneamente.



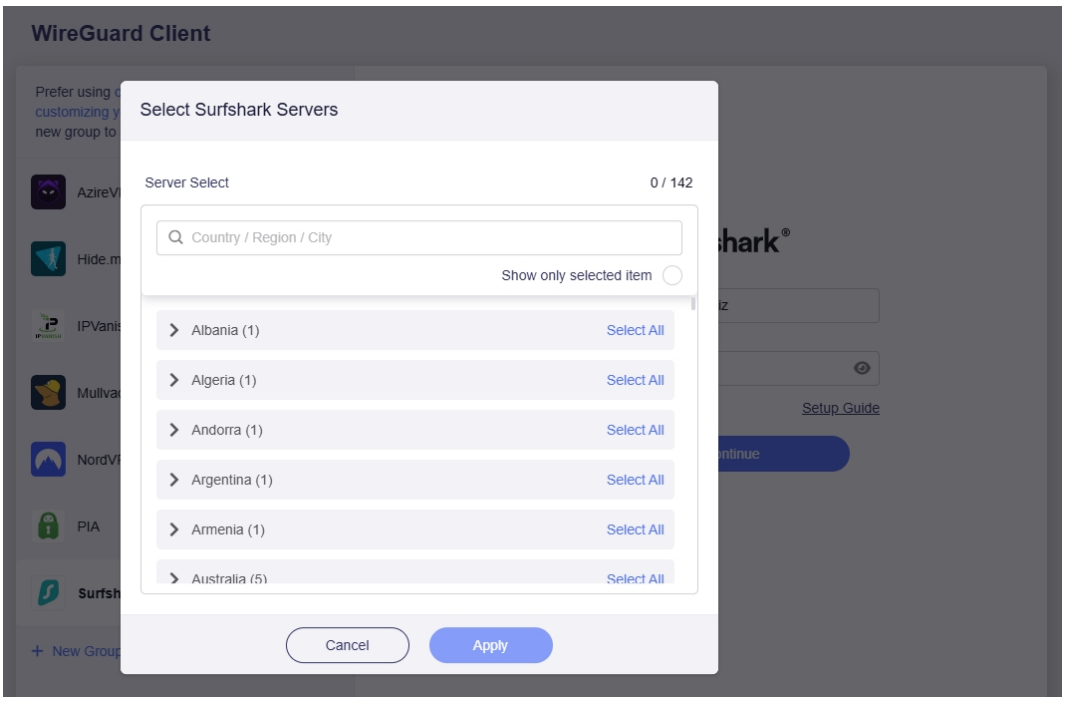
## 11.2.8 Configurar Surfshark

Siga los pasos a continuación para configurar su enrutador como cliente Surfshark.

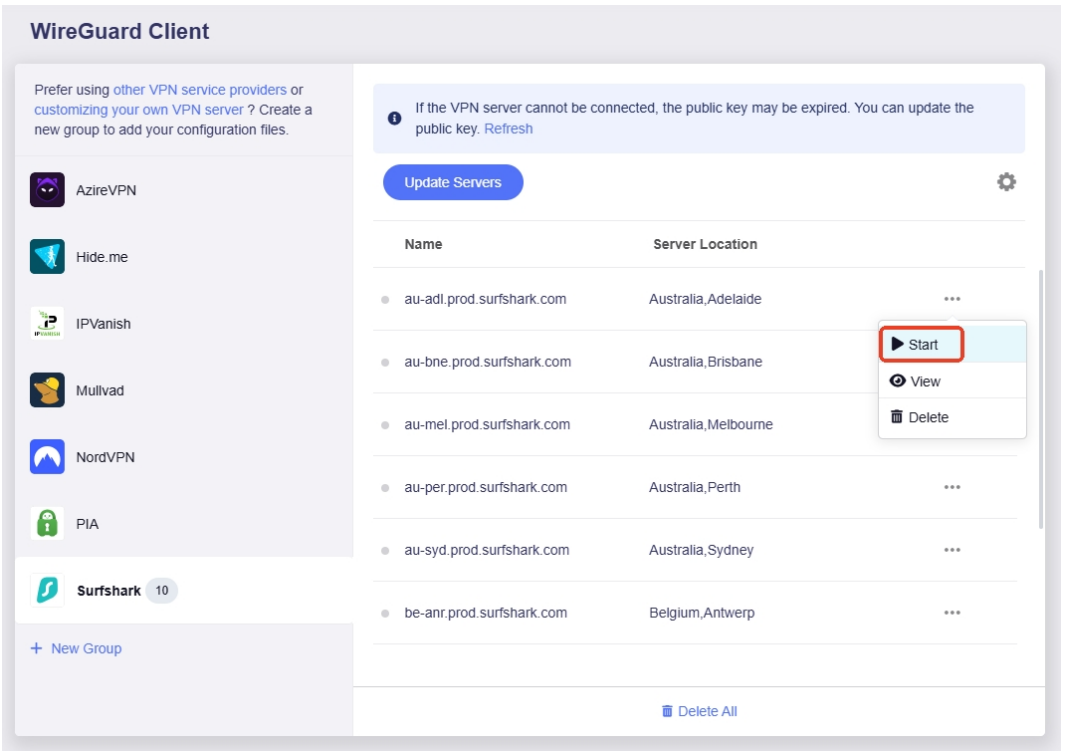
1. Inicie sesiónn en su enrutador’s web admin panel y vaya a **VPN** > **Cliente WireGuard** > **Surfshark**.
2. Ingrese el nombre de usuario y la contraseña, luego haga clic en **Guardar y continuar**.



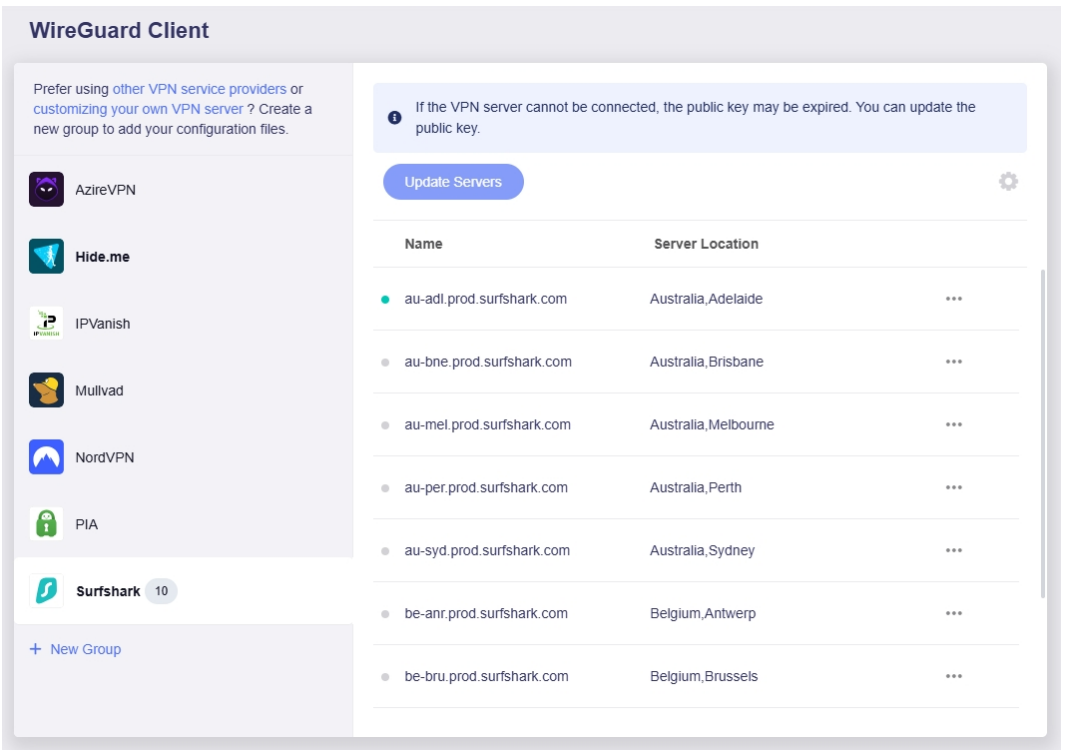

3. Seleccione los servidores a los que desea conectarse y haga clic en **Aplicar**.



4. Seleccione un servidor preferido y haga clic en el icono de tres puntos a la derecha para iniciar una conexión.



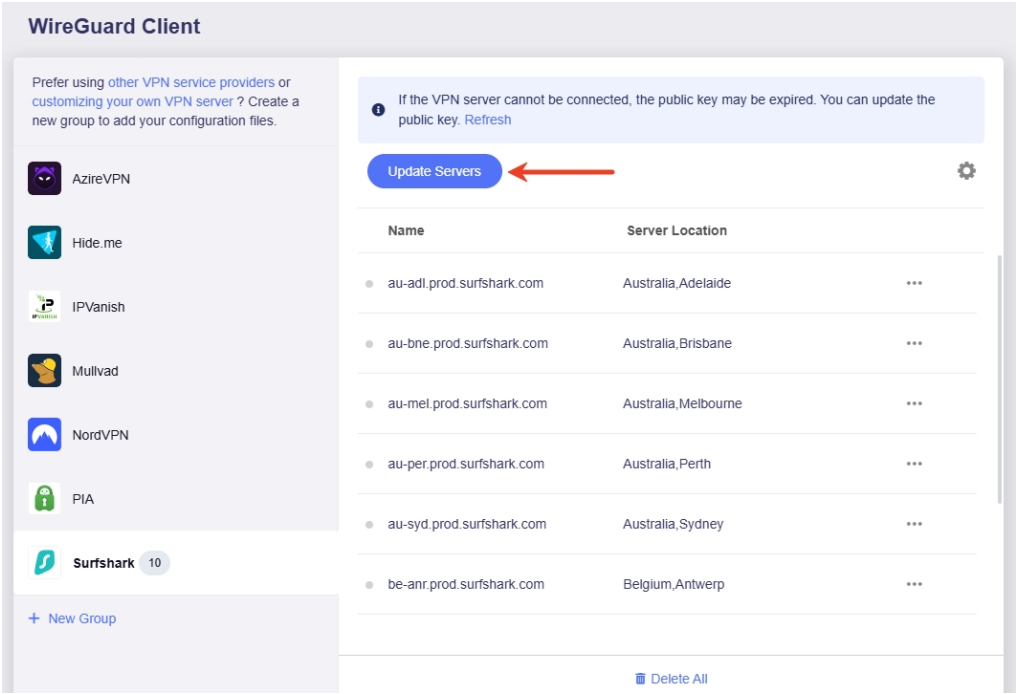

5. Una vez conectado, aparecerá un punto verde junto al archivo de configuración.




Tú puedes también verifique los detalles de la conexión VPN en el **Panel de VPN**.

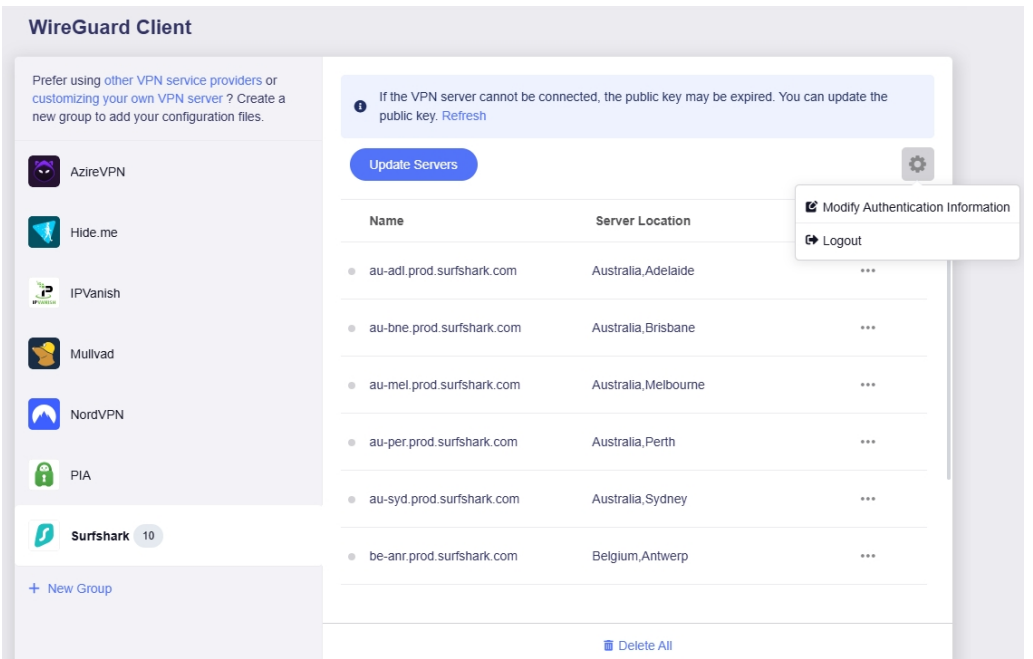
6. Actualizar servidores.

Puede hacer clic en **Actualizar servidores** para obtener la lista de servidores más reciente disponible, evitando fallas de conexión causadas por el mantenimiento o el apagado del servidor.



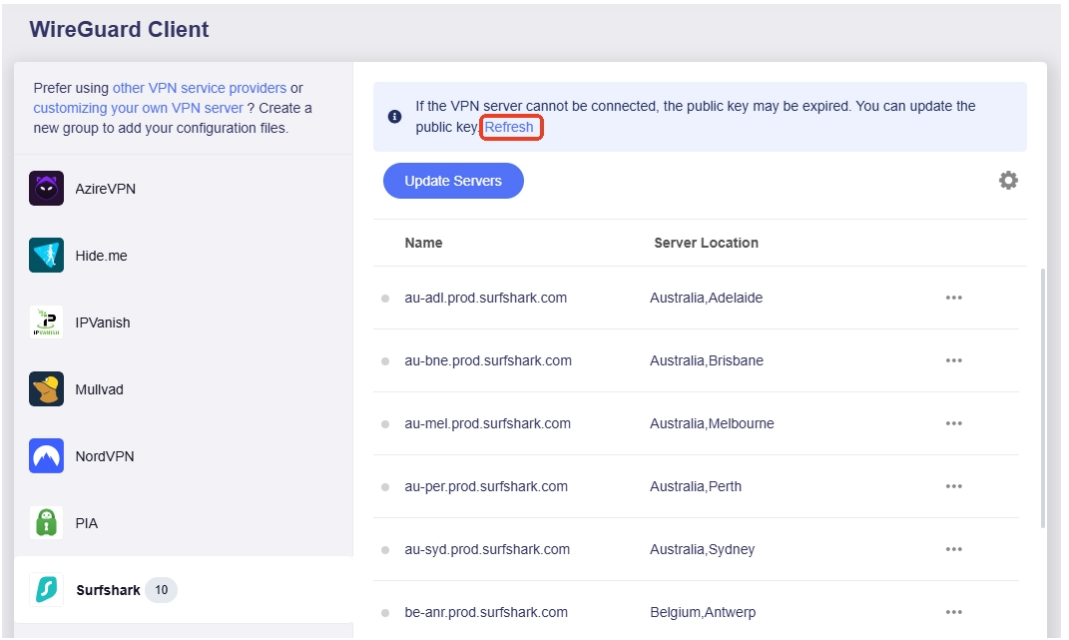

7. Editar credenciales o cerrar sesión.

Haga clic en el ícono de ajustes para editar sus credenciales de inicio de sesión o cerrar sesión.



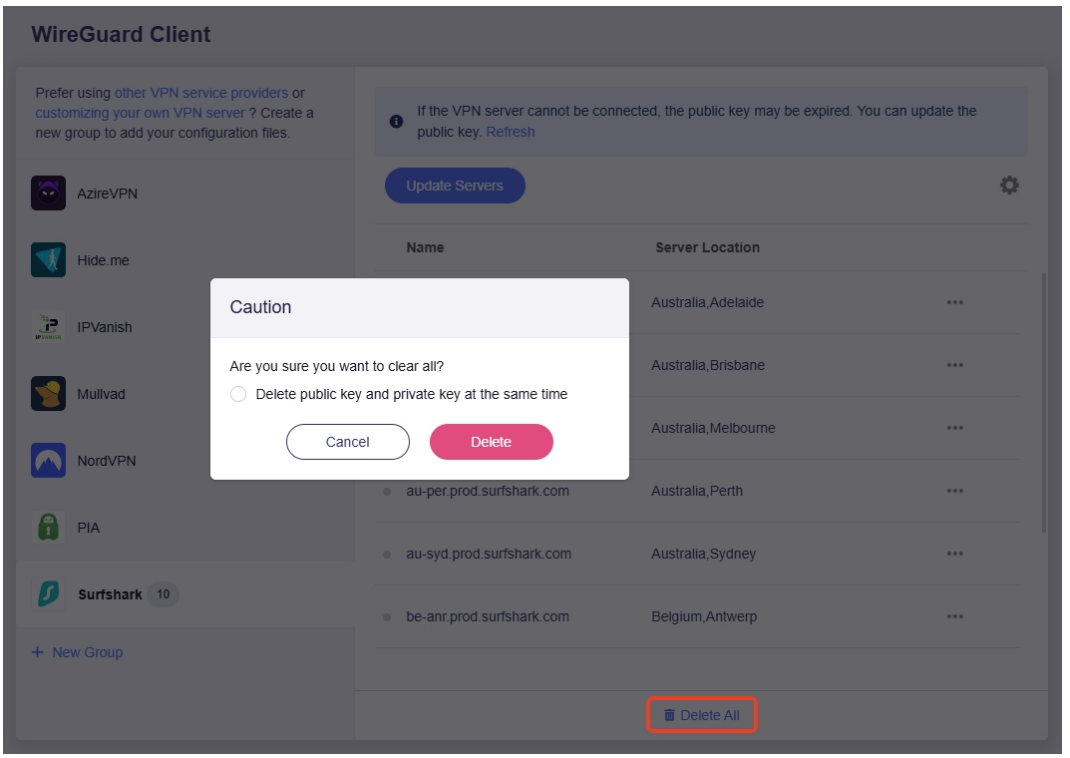
8. Actualizar.

Puede hacer clic en **Actualizar** para actualizar la clave pública cuando el servidor VPN no puede ser conectado.




9. Eliminar todos los archivos.

Puede hacer clic en **Eliminar todo** para eliminar todos los archivos de configuración con un solo clic y elegir si desea eliminar las claves públicas y privadas. simultáneamente.

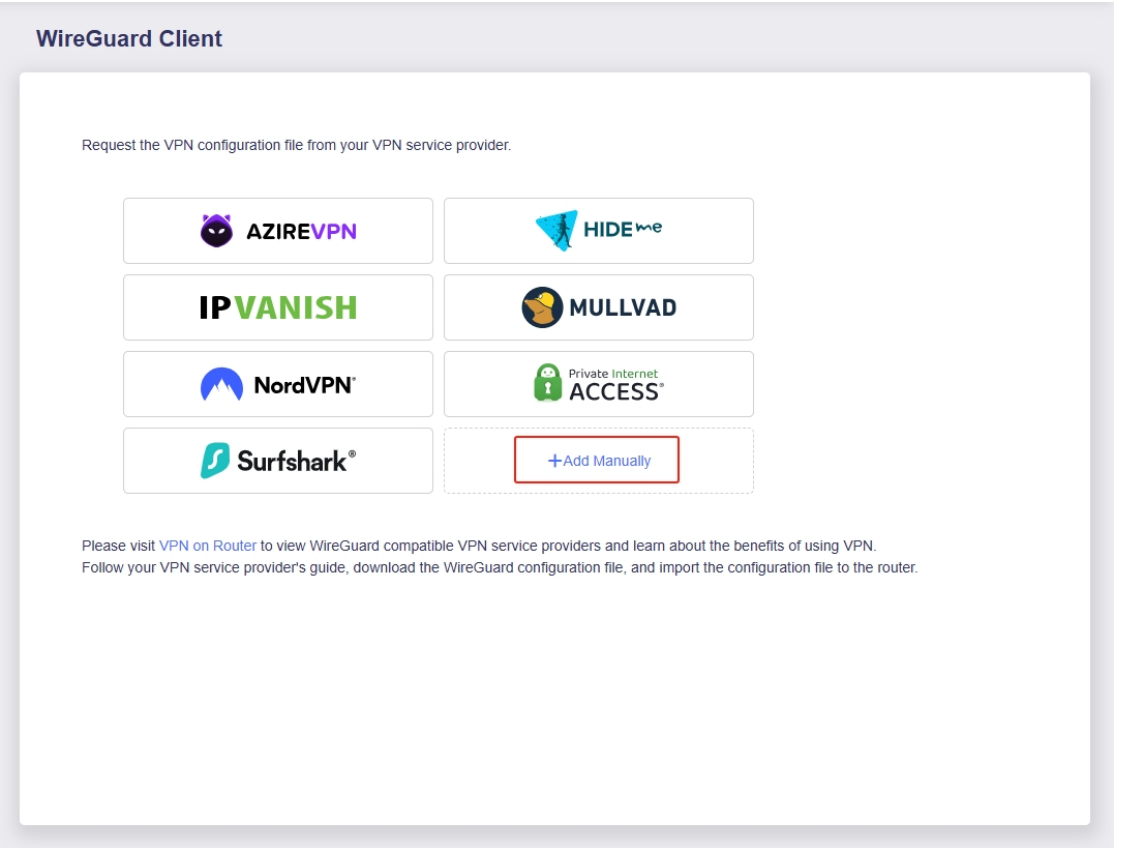


## 11.2.9 Configurar el cliente WireGuard manualmente (para otros proveedores)

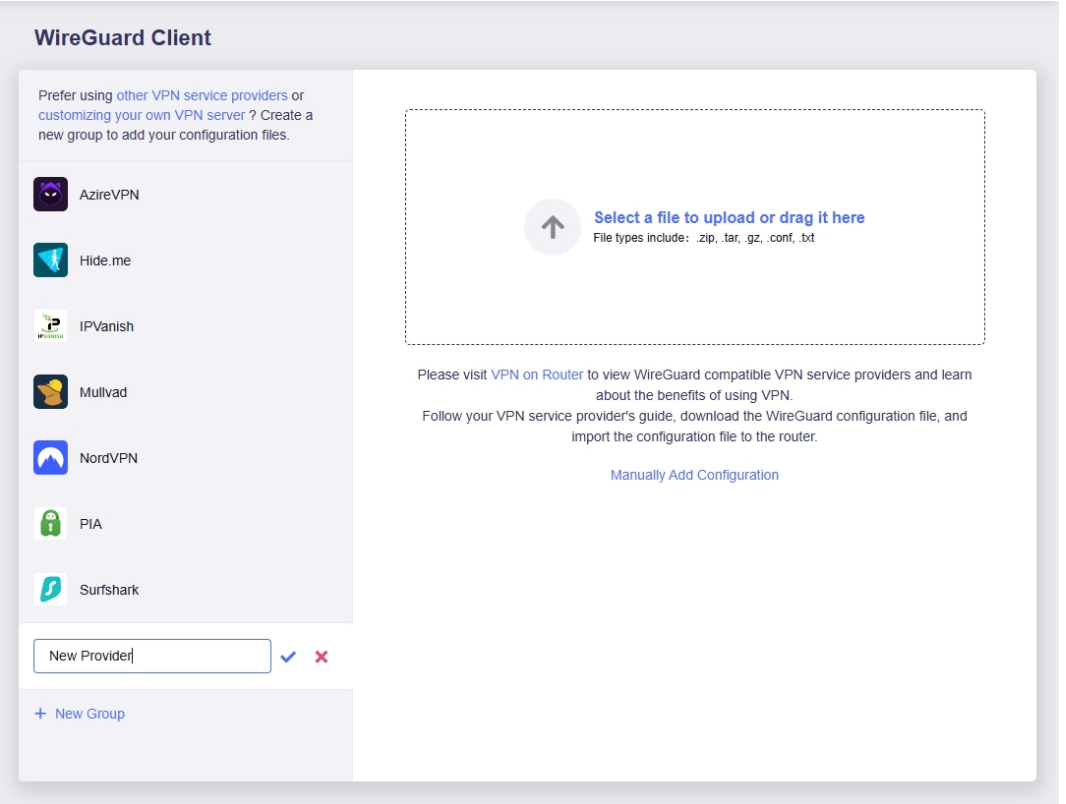
Si su proveedor de servicios WireGuard no está integrado en el panel de administración web, visite primero el sitio web oficial de su proveedor de servicios suscrito para obtener el archivo de configuración. Luego cárguelo en el enrutador para configurar un cliente WireGuard. Si no sabes cómo descargar los archivos de configuración, consulta esta guía o ponte en contacto con su soporte.

A continuación se detallan los pasos para cargue el archivo de configuración en el enrutador para configurar un cliente WireGuard.

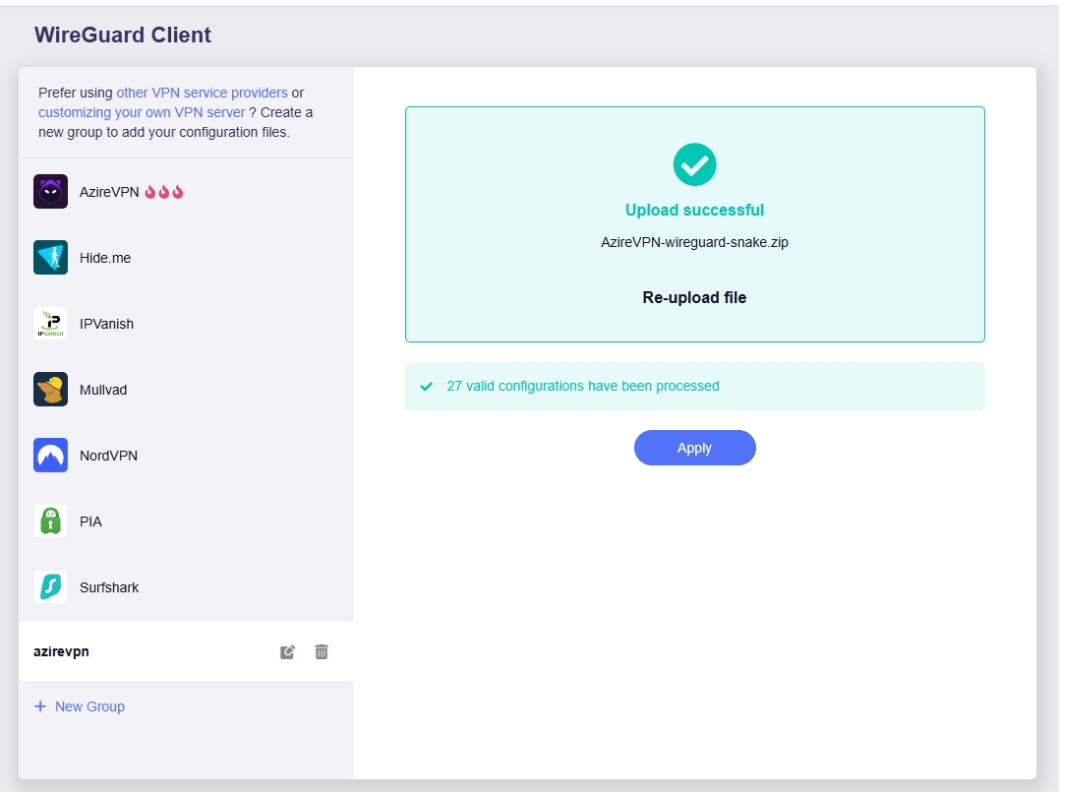
1. Inicie sesiónn en su enrutador's web admin panel y navega hasta **VPN** > **Cliente WireGuard** > **Agregar manualmente**.



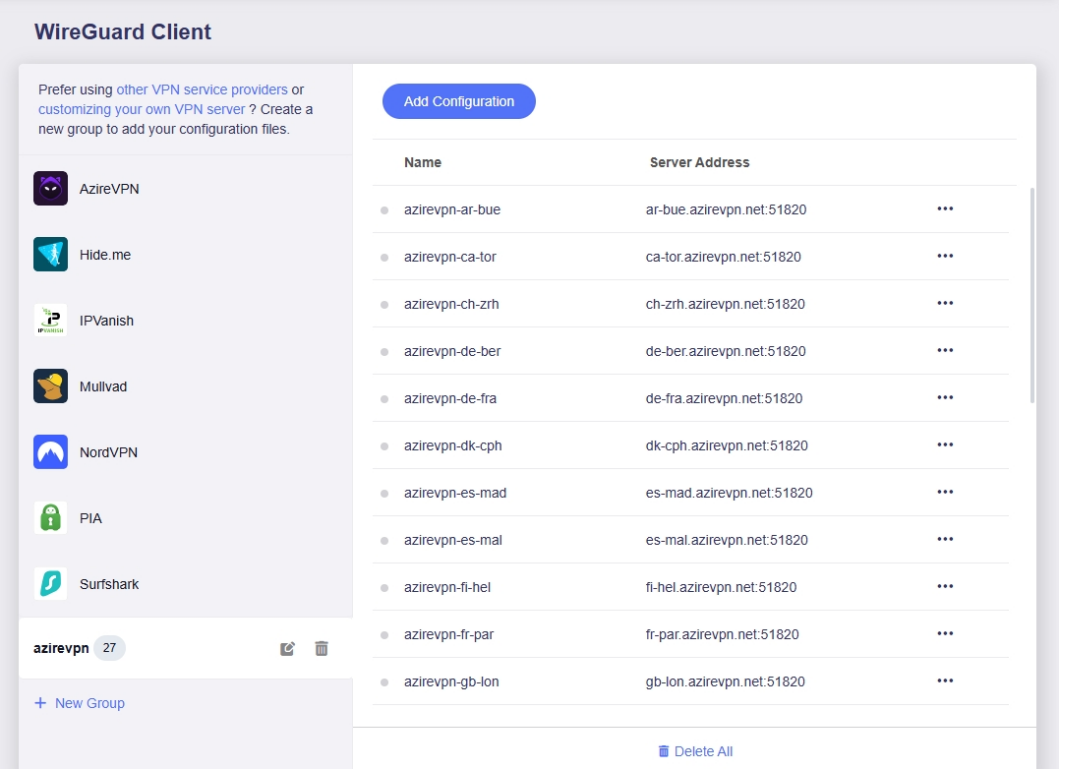

2. Creará un grupo en la barra lateral izquierda. Establezca un nombre descriptivo para el grupo.



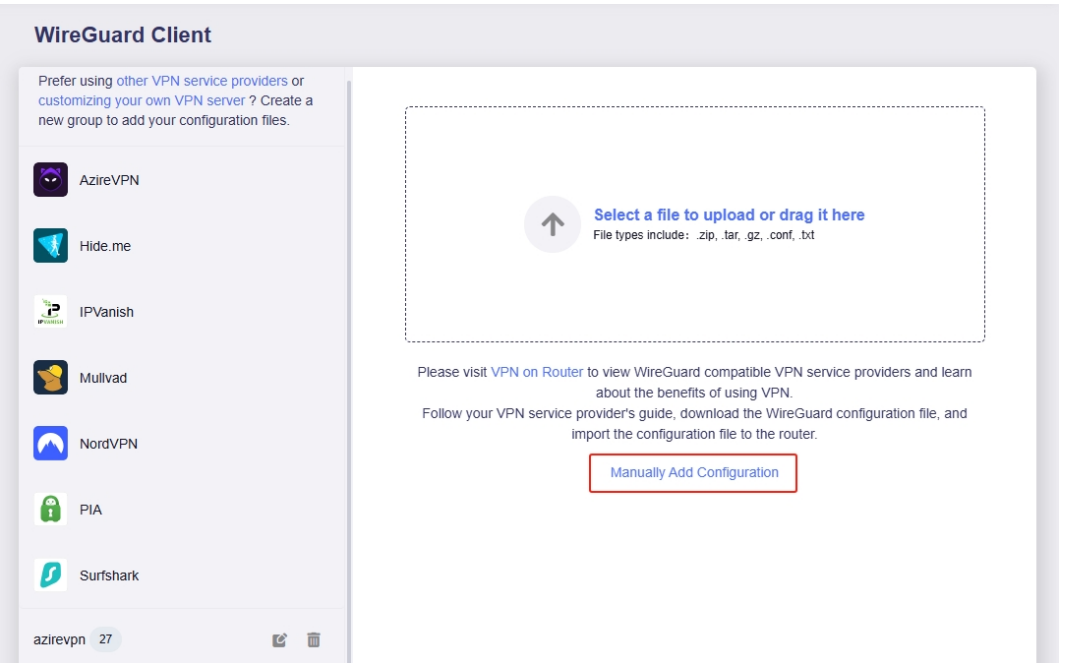

3. Click el área de carga para cargar su archivo de configuración WireGuard (formatos admitidos: zip, tar, gz, conf, txt) y haga clic en **Aplicar**.

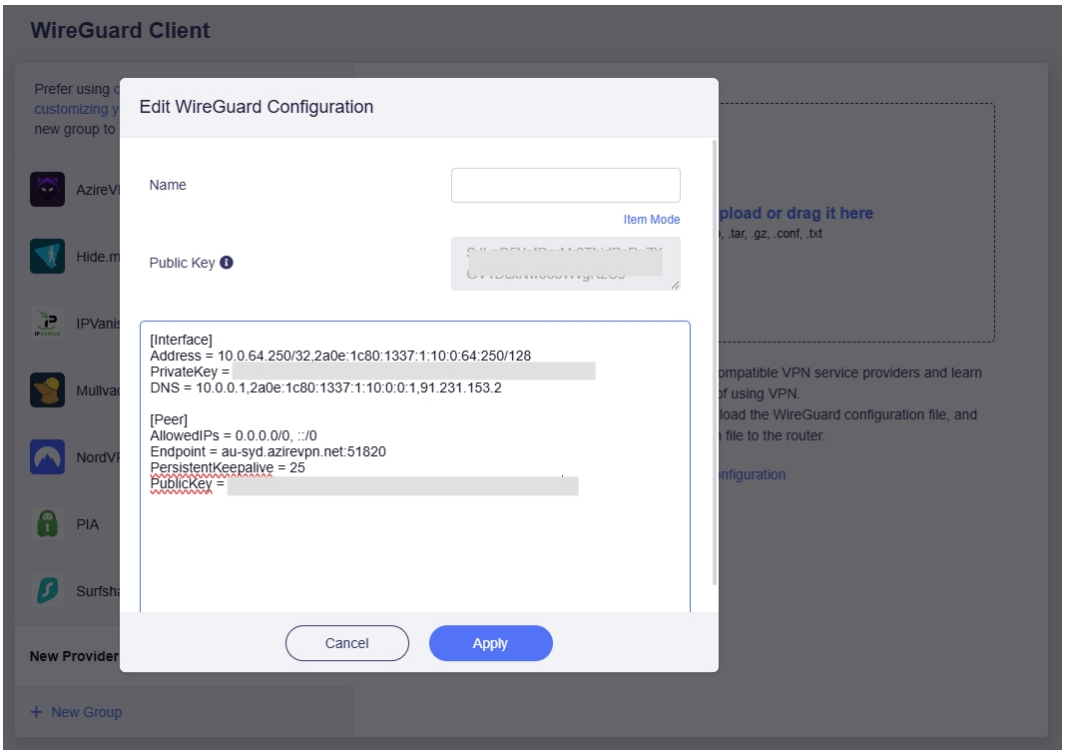


Si carga un archivo comprimido que contiene varios archivos de configuración, se descomprimirá automáticamente, como se muestra a continuación.

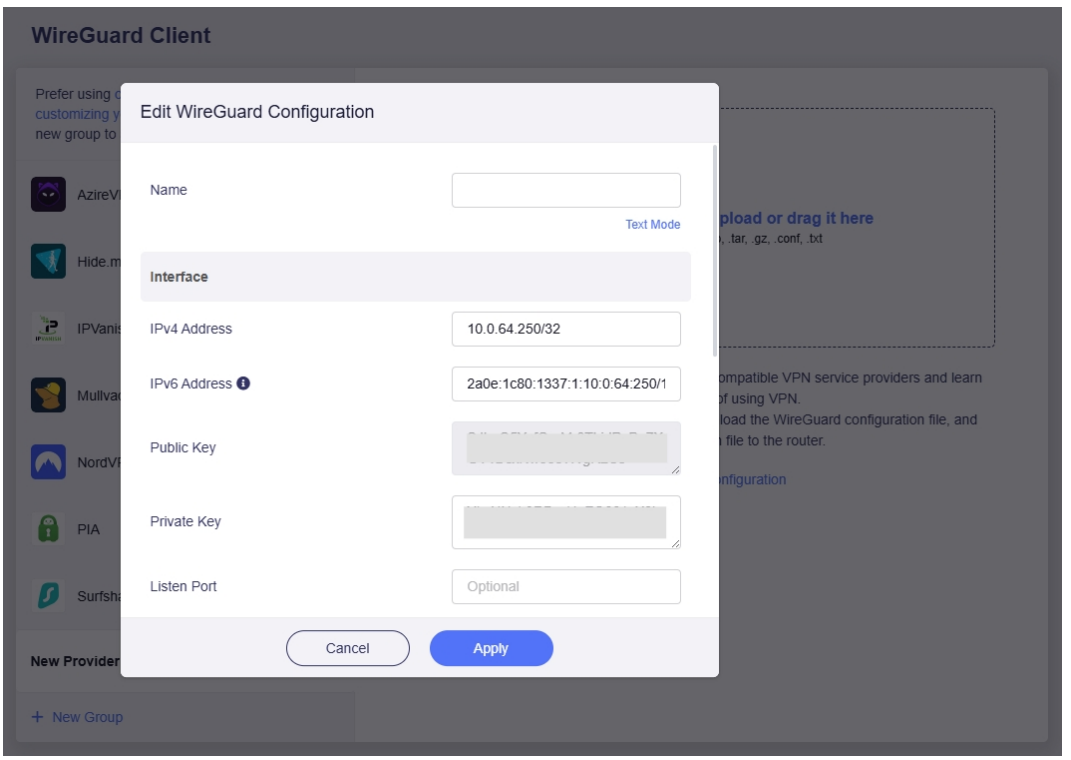



Como alternativa, puede hacer clic en **Agregar configuración manualmente** en la parte inferior del área de carga, agregue los detalles de configuración en forma de texto y haga clic en **Aplicar**.

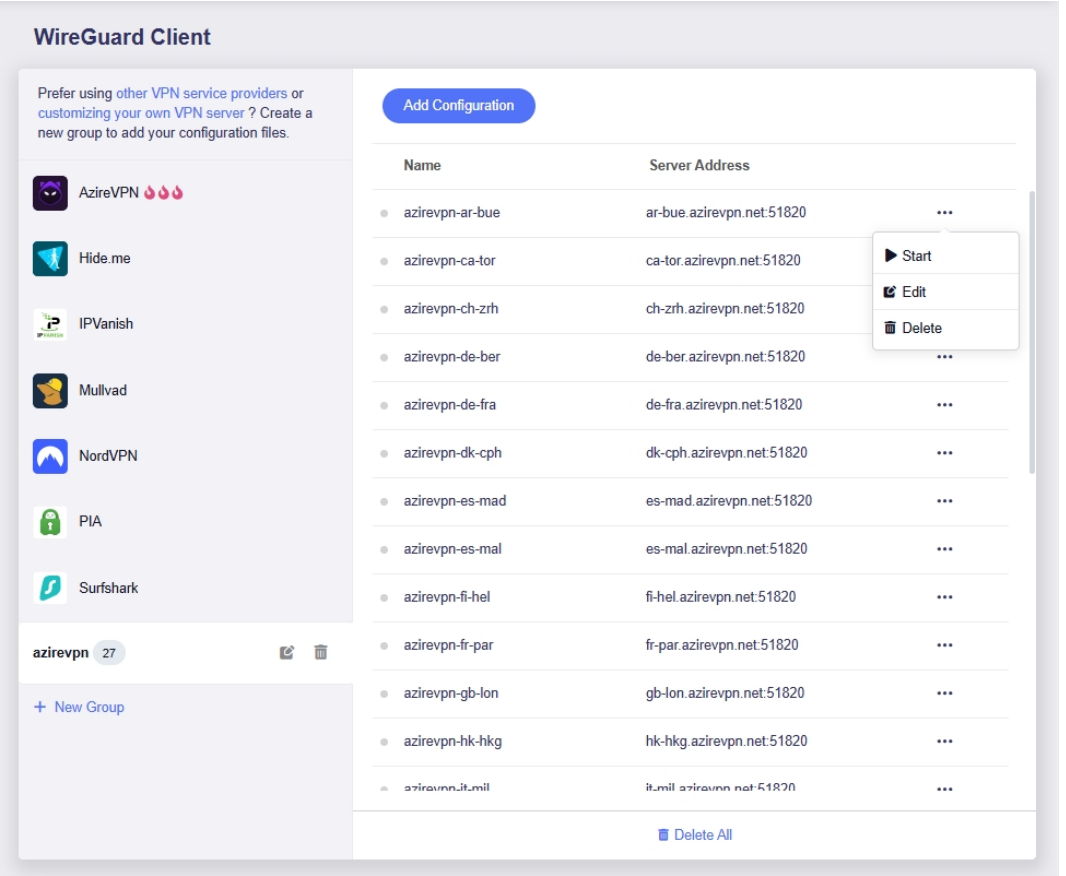





Si desea verificar cada elemento, puede cambiar al modo Elemento y verificar la configuraciónuración detalles, luegoluego haga clic en **Aplicar**.




4. Haga clic en el ícono de tres puntos en el lado derecho para iniciar la conexión.




5. Una vez conectado, aparecerá un punto verde junto al archivo de configuración. Usted puede verificar el Detalles de la conexión VPN en el **Panel de VPN**.

Capítulo 12

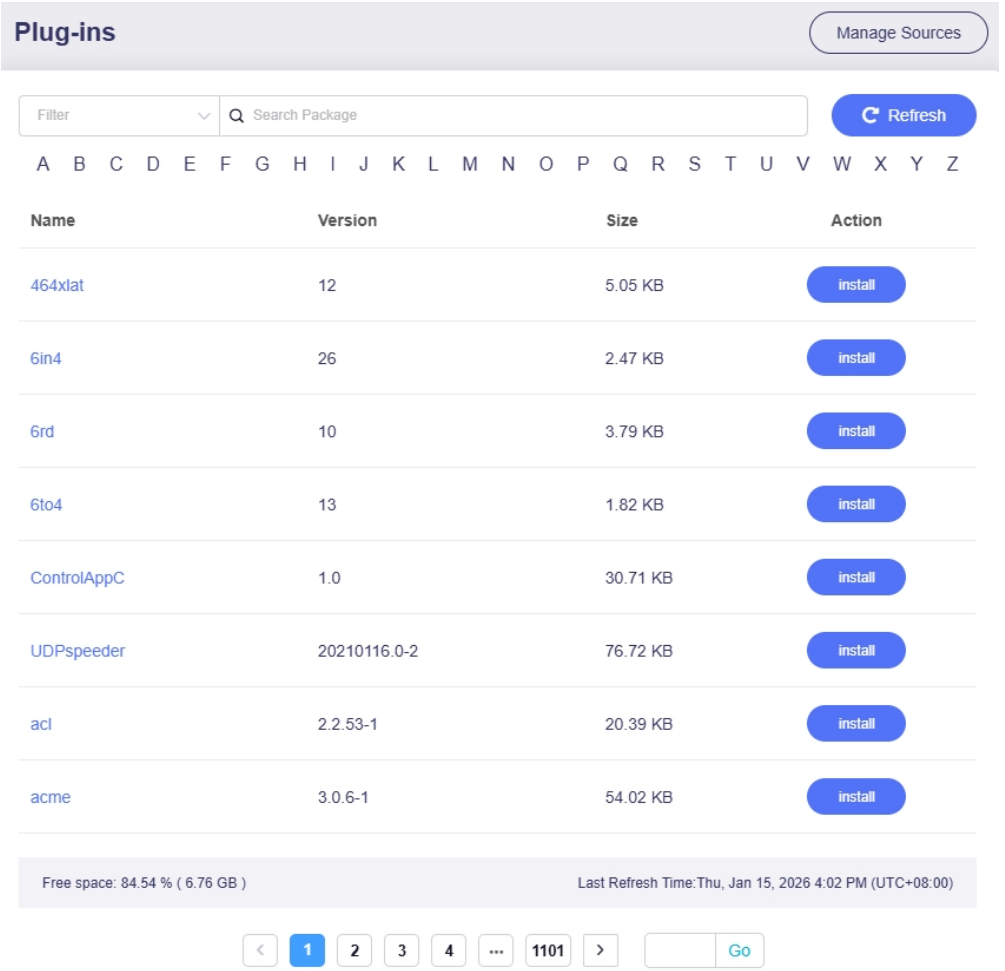
# Aplicaciones

Este capítulo presenta algunas aplicaciones en enrutadores GL.iNet, por ejemplo, Complementos, DNS dinámico, almacenamiento de red, AdGuard Home, control parental, escala trasera y administración de eSIM.

# 12.1 Complementos

La Página de complementos le permite administrar paquetes OpenWrt.

Inicie sesión en su enrutador's web admin panel, navegar a **APLICACIONES** > **Complementos.** Puedes instalar o eliminar cualquier paquetee disponible en el repositorio. Haz clic en **Botón Actualizar** para actualizar la lista de paquetes antes de instalar complementos.




**Nota**:

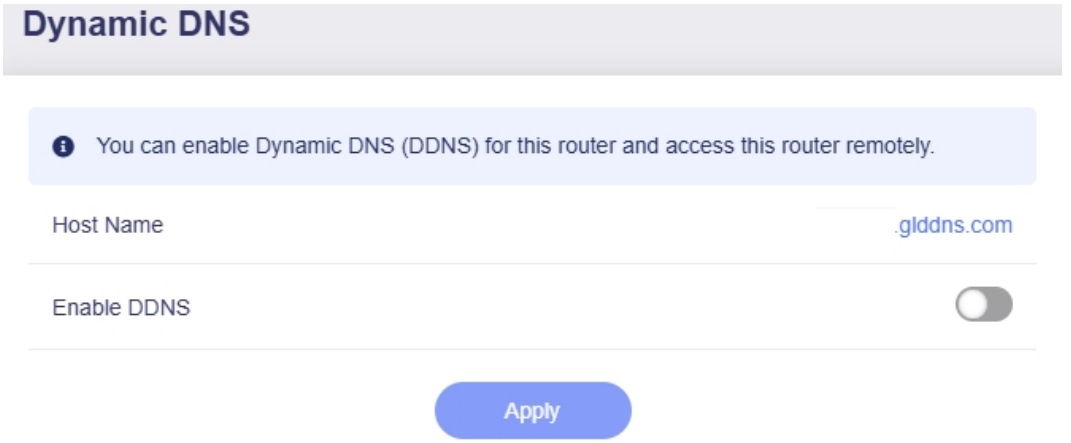
1. No se recomienda actualizar los complementos preinstalados en el firmware oficial de GL.iNet, como nginx, adguard home, tailscale, etc.
2. Los complementos de terceros instalados manualmente por los usuarios se pueden actualizar; sin embargo, GL.iNet no es responsable de ningún problema de seguridad causado por complementos de terceros. Si tiene consultas, comuníquese con los respectivos autores de complementos externos.

## 12.2 DNS dinámico

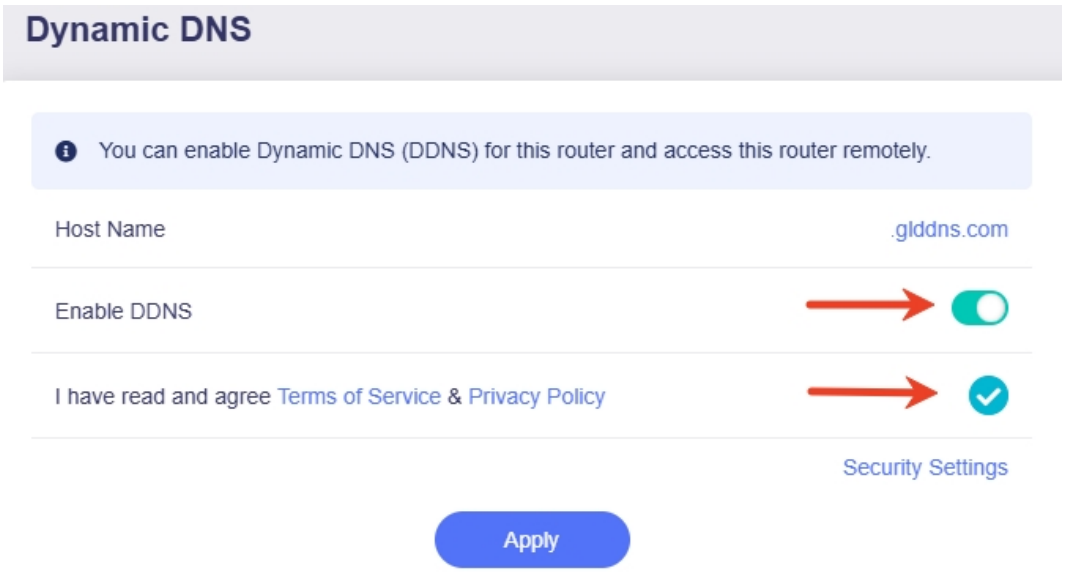
Dinámico El servicio de nombres de dominio (DDNS o DNS dinámico) es un servicio que se utiliza para asignar un nombre de dominio a la dirección IP dinámica de un dispositivo de red. Con DNS dinámico, puede acceder a su enrutador de forma remota. Se requiere una dirección IP pública para esta funcionalidad.  Se requiere una dirección IP pública para esta funcionalidad.

### 12.2.1 Habilitar DDNS

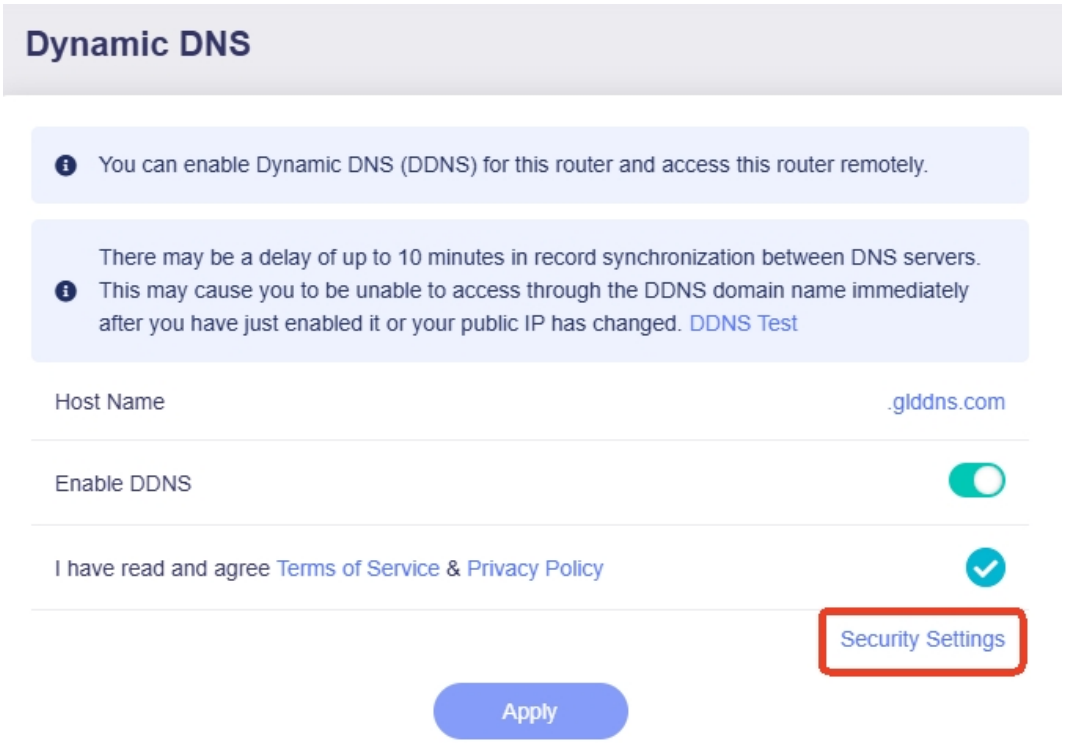
1. Inicie sesión en el panel de administración web de su enrutador, navegue hasta **APLICACIONES** > **DNS dinámico**, la página se muestra como a continuación.



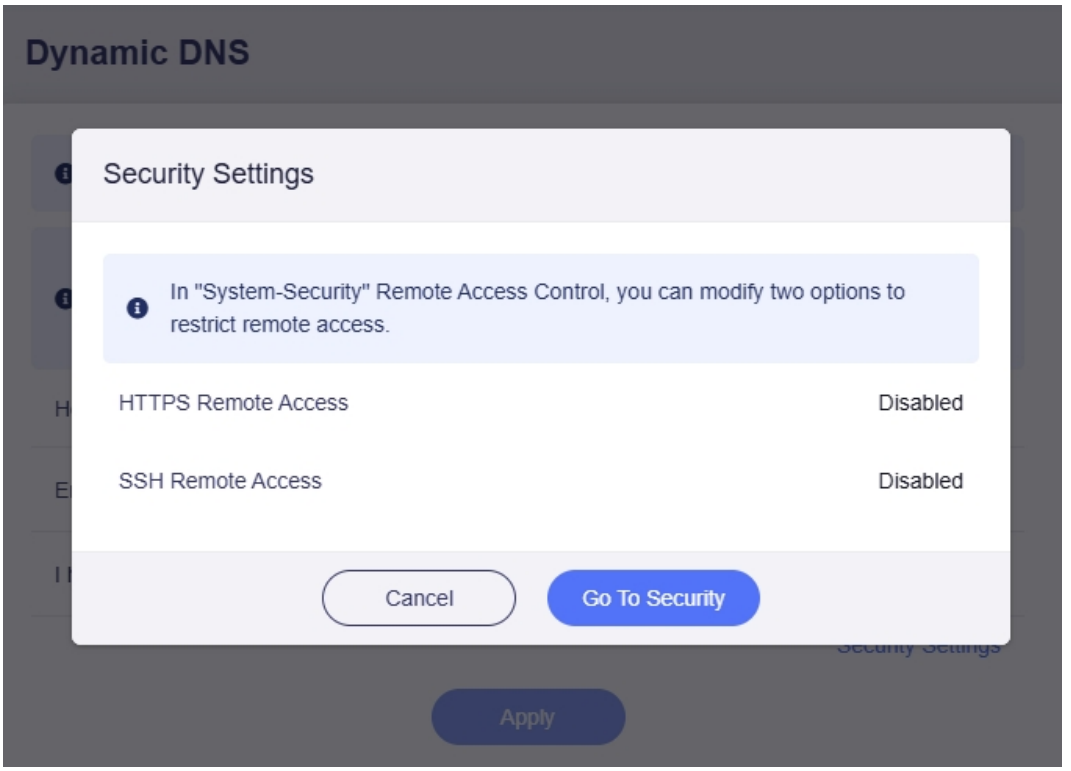

2. Activar **Habilitar DDNS**, leer y aceptar los los **Términos de servicios y política de privacidad**, luego haga clic en **Aplicar**.



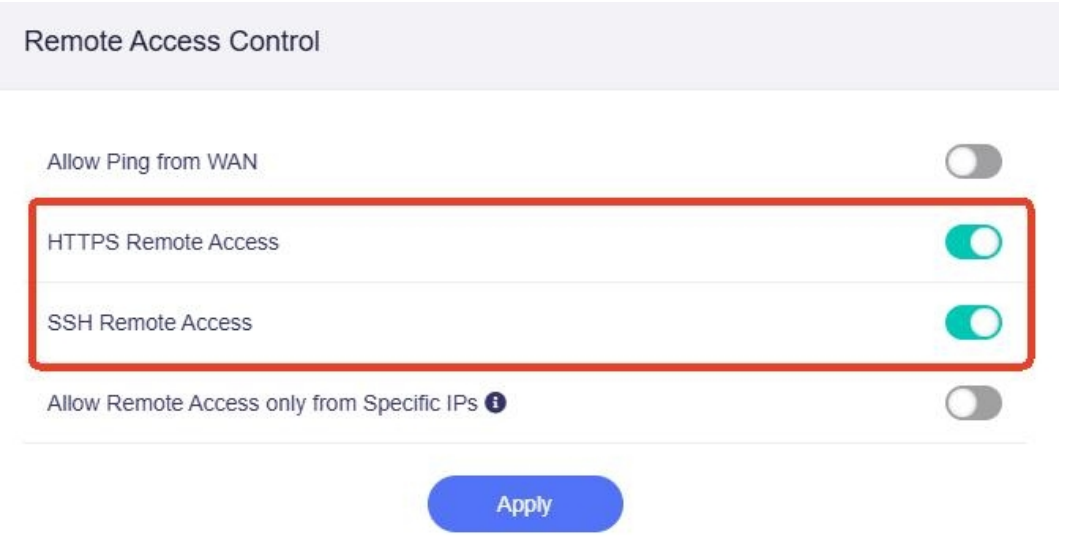
3. Haga clic en **Configuración de seguridad** en la esquina inferior derecha.




4. En el ventana emergente, verifique si el acceso remoto que desea utilizar está habilitado.



Si no, vaya a **SSISTEMA** >**Seguridad** > **Control de acceso remoto** para habilitarlopara habilitarlo y haga clic en **Aplicar**.




**Nota**:

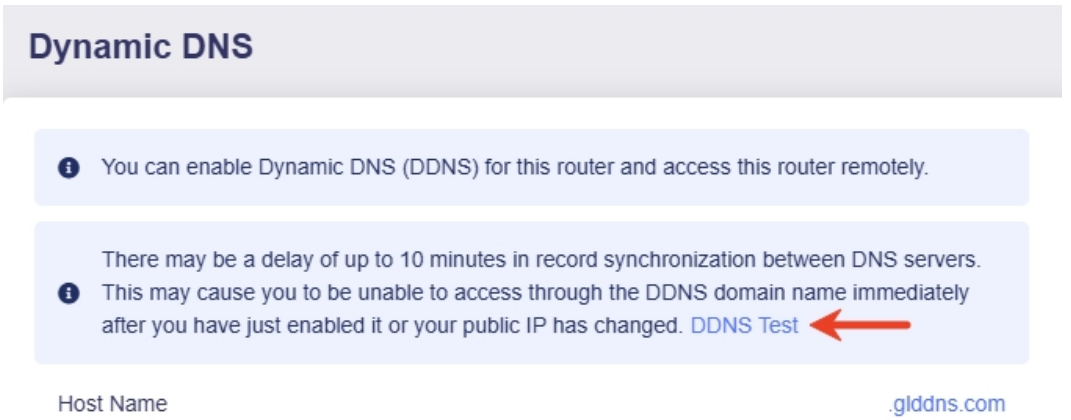
1. Puede haber un retraso de hasta 10 minutos en la sincronización de registros entre servidores DNS. Esto puede impedirle acceder a través del nombre de dominio DDNS inmediatamente después de habilitarlo o cuando cambie su IP pública.
2. Si habilita DDNS y el Cliente VPN al mismo tiempo, enseguro que servicios de GL.iNet Usar VPN está deshabilitado.

## 12.2.2 Comprobar si DDNS funciona

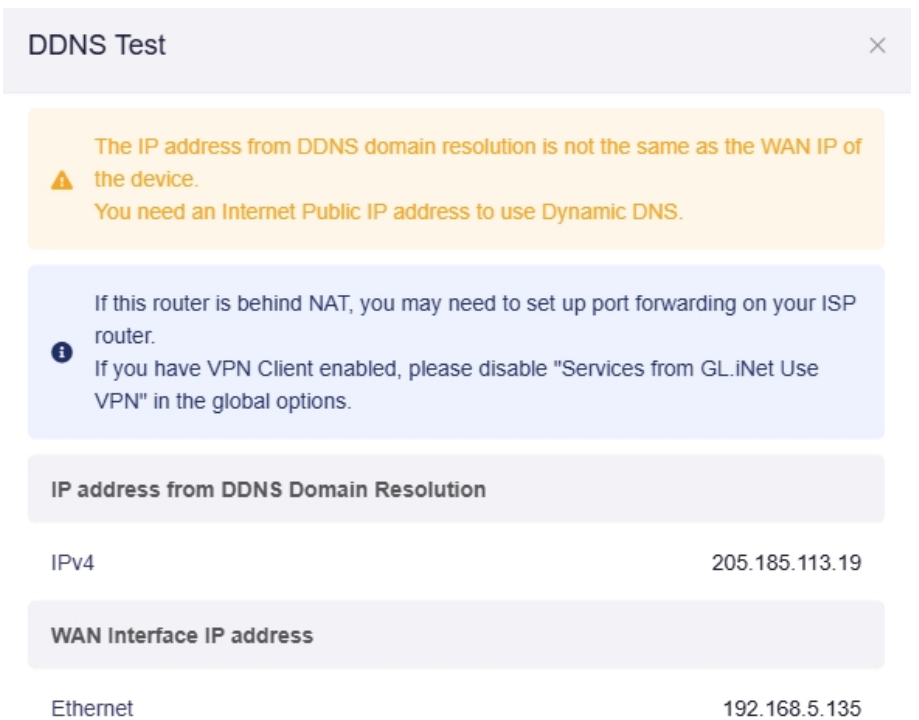
Puede comprobar si DDNS funciona utilizando el Herramienta de prueba DDNS o manualmente mediante comandos.

**Método 1. Use Herramienta de prueba DDNS**

1. En la página DNS dinámico, haga clic en **DDNS Pruebat**.




2. Asegúrese de que la dirección IP de la resolución del dominio DDNS coincida con la IP WAN del enrutador. De lo contrario, aparecerá un mensaje amarillo en la parte superior, lo que indica que el enrutador podría estar detrás de NAT y que debe configurar el reenvío de puertos en el enrutador ascendente.



**Método 2. Usar comandos**

1. Usar nslookup comando *nslookup xxxxxxx.glddns.com 8.8.8.8* para obtener la asignación entre el nombre de dominio y la dirección IP. A continuaciónelow es un ejemplo de Beryl AX GL-MT3000.



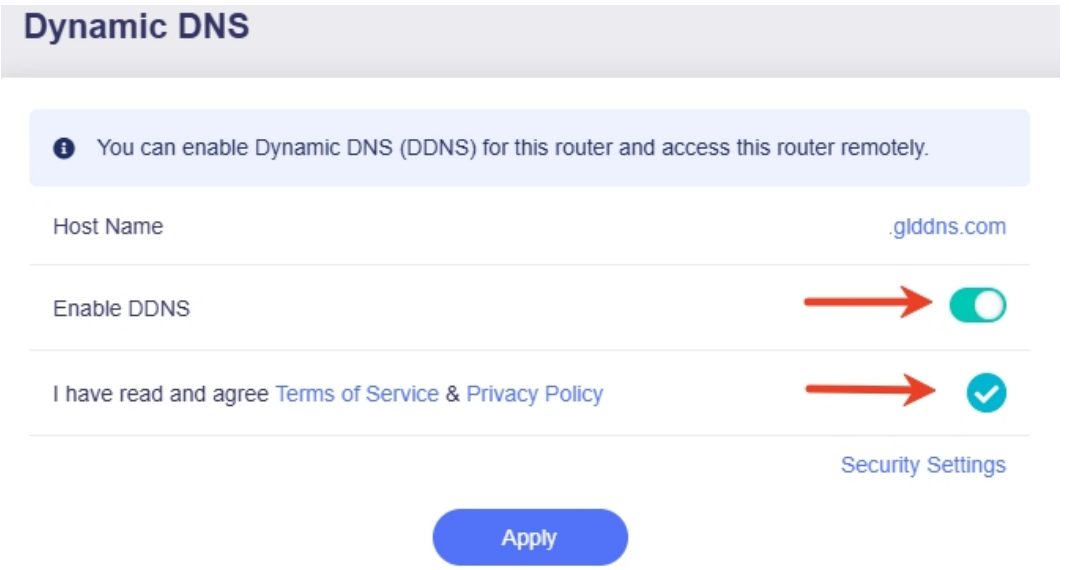

   - Reemplace “xxxxxxx.glddns.com” en la imagen de arriba con su Nombre del host.
   - El “8.8.8.8” es el DNS de Google. Uconsúltelo o reemplácelo con otros, luego presione Entrar.
2. Si obtiene una dirección IP pública como “183.178.10.100” en la imagen de arriba, indica que su dominio DDNS se ha implementado exitosamente. asignado a una dirección IP pública. Si recibe un mensaje como “el servidor no puede’no encontrar xxxxxxx.glddns.com”, puede indicar que la resolución del dominio falló y que su dominio DDNS no se ha asignado correctamente a una dirección IP pública. Continúe con el siguiente paso para verificar.
3. Inicie sesión en su router’s web admin panel y navega hasta **INTERNET**. Encuentra tu enrutador’ en la interfaz activa actual. Compare esta dirección IP con la dirección IP pública obtenida anteriormente. Si son iguales, el DDNS está vigente; de lo contrario, no lo está.

## 12.2.3 Acceso remoto HTTPS

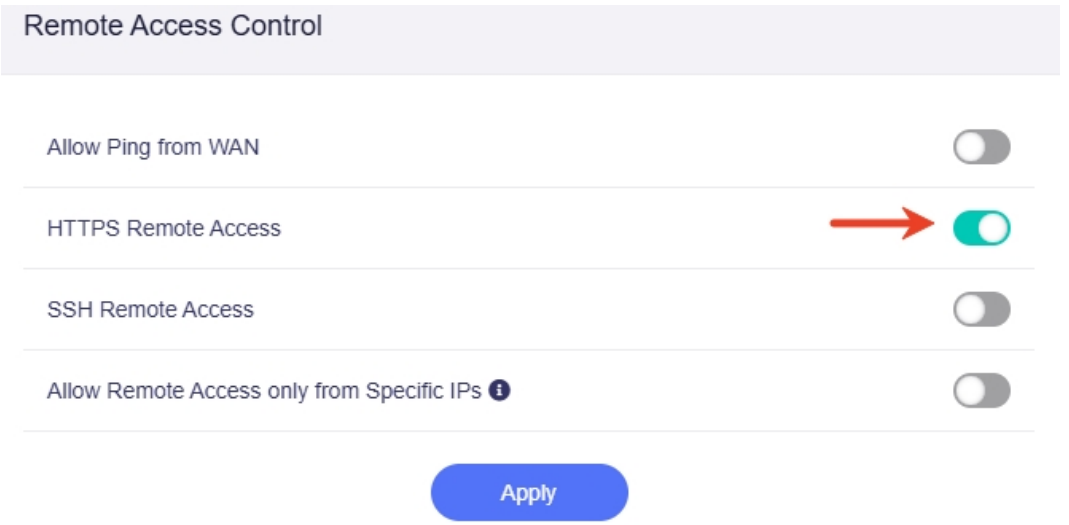
Una **Dirección IP pública** es necesario para el acceso remoto HTTPS. Consulte aquí tpara verificar si su ISP le asigna un dirección IP pública. Si su enrutador está detrás de NAT, configure el reenvío de puertos (**puerto 443**) en el enrutador ascendente para acceso HTTPS.

Siga los pasos a continuación para habilitar el acceso remoto HTTPS para su enrutador.

1. En la página DNS dinámico, active **Habilitar DDNS**, acepte los **Términos de servicios y privacidad Política**, luego haga clic en **Aplicar**.

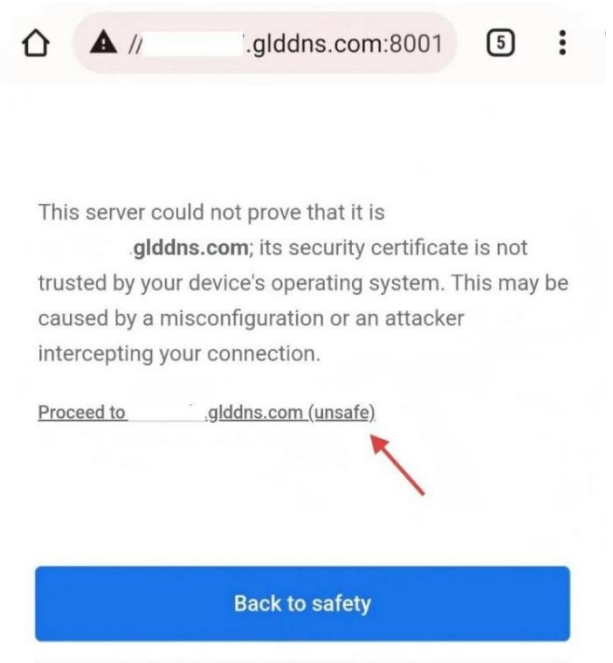



2. En el panel de administración web, vaya a **SSISTEMA** > **Seguridad** > **Control de acceso remoto**. Activar **Acceso remoto HTTPS** y haga clic en **Aplicar**.



Una vez habilitado, puede acceder al panel de administración del enrutador’desde cualquier lugar utilizando el DDNS host nombre sobre HTTPS, p. ej., **https://xxxxxxx.glddns.com**. Si el reenvío de puertos está configurado, acceda a él como **https://xxxxxxx.glddns.com:external_port** (reemplazar el externo_puerto con su real puerto número).

**Nota**: Esta función utiliza certificados autofirmados; por lo tanto, los navegadores indicarán "Su conexión no es privada" al acceder al panel de administración del enrutador a través del nombre de host DDNS a través de HTTPS. Para continuar con el acceso remoto HTTPS, haga clic en **Avanzado** en la parte inferior, luego haga clic en **Continuar con xxxxxxx.glddns.com** para continuar.



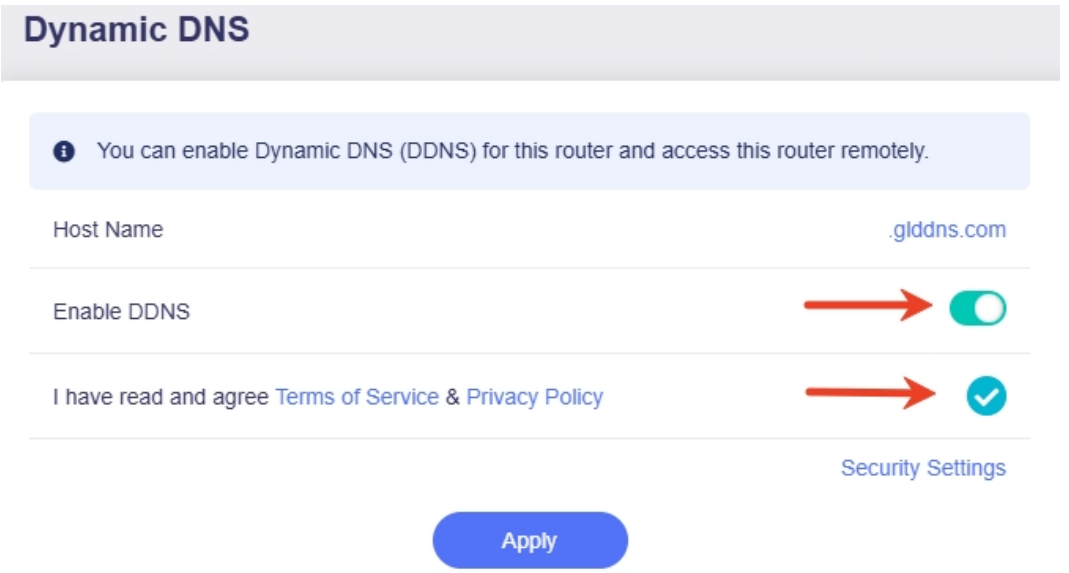

Luego podrá acceder al enrutador’s panel de administración web usando el DDNS host nombre sobre **HTTPS**.

## 12.2.4 Acceso remoto SSH

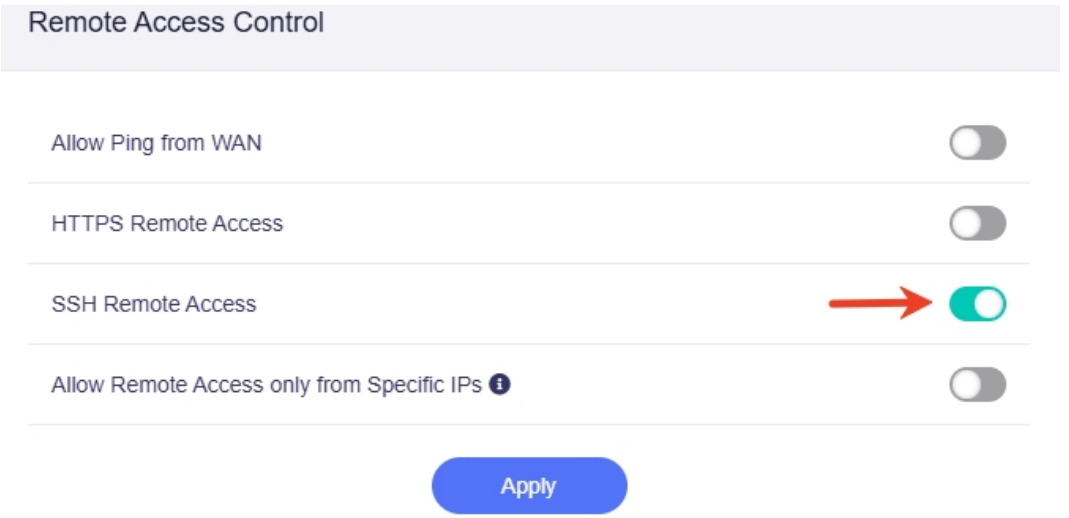
Se requiere una **Dirección IP pública** para el acceso remoto SSH. Consulte aquí para verificar si su ISP le asigna una dirección IP pública. Si su enrutador está detrás de NAT, configure el reenvío de puertos (**puerto 22**) en el enrutador ascendente para acceso remoto SSH.

Siga los pasos a continuación para habilitar el acceso remoto SSH para su enrutador.

1. En la página DNS dinámico, active **Habilitar DDNS**, acepte las **Condiciones de servicios y política de privacidad**, luego haga clic en **Aplicar**.




2. En el panel de administración web, vaya a **SSISTEMA** >**Seguridad** > **Control de acceso remoto**. Habilitar **Acceso remoto SSH** y haga clic en **Aplicar**.



Una vez habilitado, puede acceder al panel de administración del enrutador’desde cualquier lugar utilizando DDNS host nombre sobre SSH, p. ej., **ssh root@xxxxxxx.glddns.com**. Si el reenvío de puertos está configurado, acceda a él como **ssh root@xxxxxxx.glddns.com:external_port** (reemplace el externo_puerto con su real puerto número).

## 12.3 Almacenamiento en red

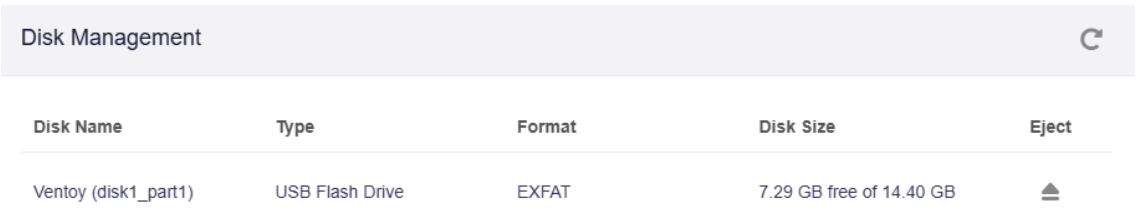
El almacenamiento en red permite compartir archivos de forma inalámbrica entre dispositivos conectando una unidad USB o una tarjeta SD a su enrutador. El enrutador convierte el dispositivo de almacenamiento en una unidad de red compartida, accesible para todos los dispositivos conectados a Wi-Fi.

Flint 3 está equipado con un puerto USB, compatible con unidades flash USB y discos duros externos portátiles. Puede configurar Samba, WebDAV o DLNA para estos dispositivos de almacenamiento con formatos comunes como NTFS, FAT32 y EXT4.

**Nota**: El consumo de energía del disco duro USB es bastante alto. Úselo con una fuente de alimentación externa; de lo contrario, puede causar un mal funcionamiento.

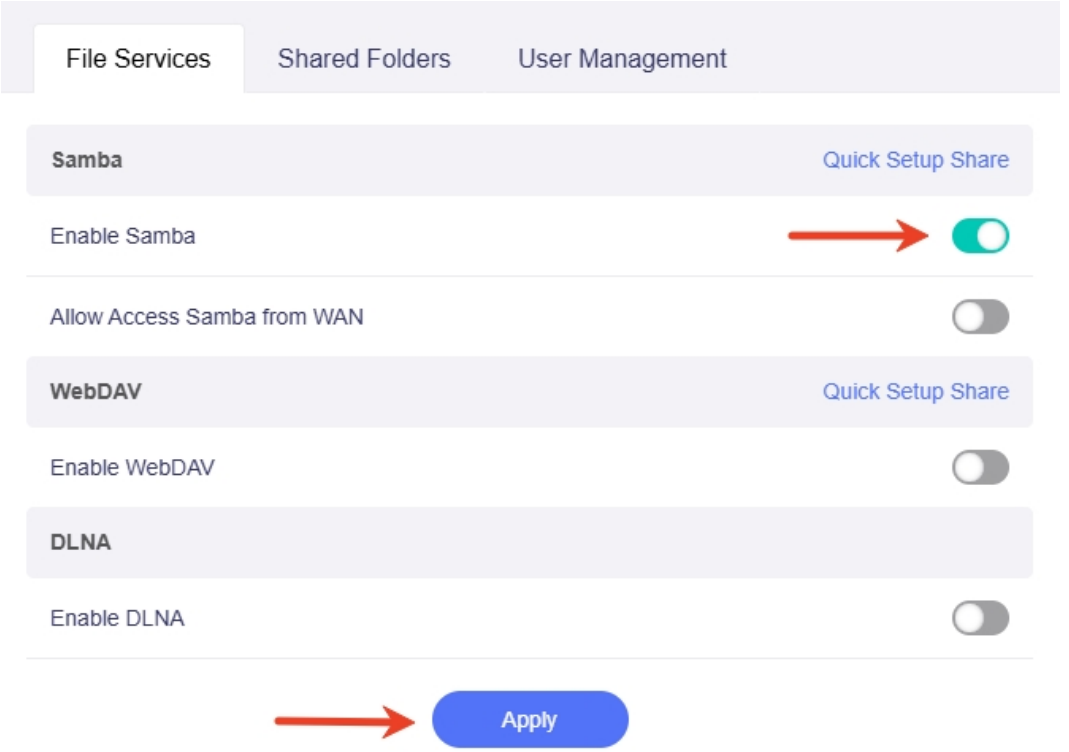
### 12.3.1 Conectar una unidad de almacenamiento

1. Conecte su dispositivo de almacenamiento al enrutador.
   - Para una unidad USB: conéctelo directamente al puerto USB.
   - Para un disco duro externo: conéctelo a una fuente de alimentación separada (si es necesario) y luego conéctelo al enrutador.
2. Inicie sesión en su enrutador’s panel de administración web, navegue hasta **APLICACIONES** > **Almacenamiento en red**. Puede habilitar servicios de transferencia de archivos y administrar la carpeta compartida aquí.
3. Si el dispositivo de almacenamiento es detectado, la **Administración de discos** se mostrará de la siguiente manera.



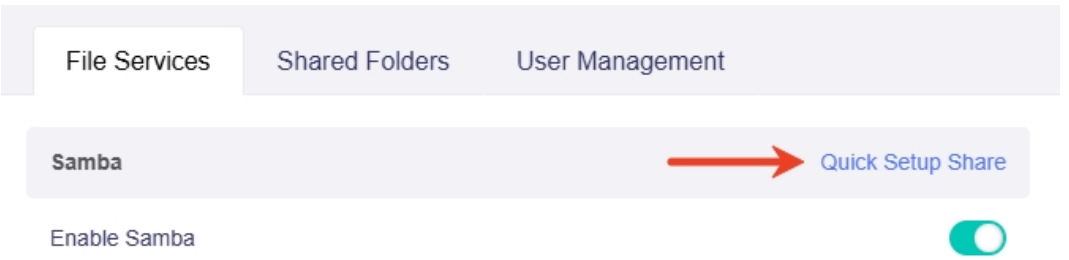
## 12.3.2 Configurar Samba

1. En el **Servicios de archivos**, talternar en **Enable Samba**, y haga clic en **Aplicar**.

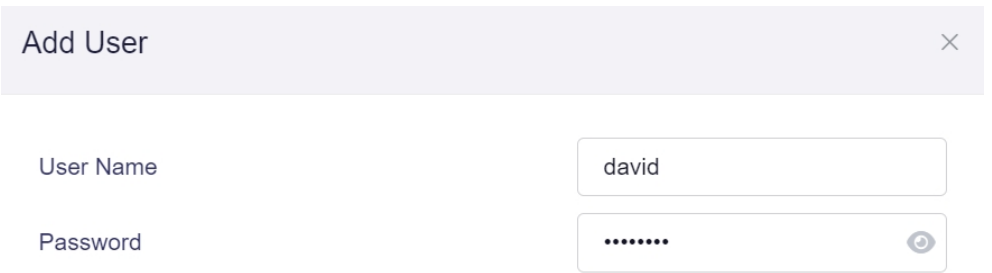



   - **Permitir acceso a Samba desde WAN**: habilítelo si desea que los dispositivos ascendentes accedan el servicio Samba.

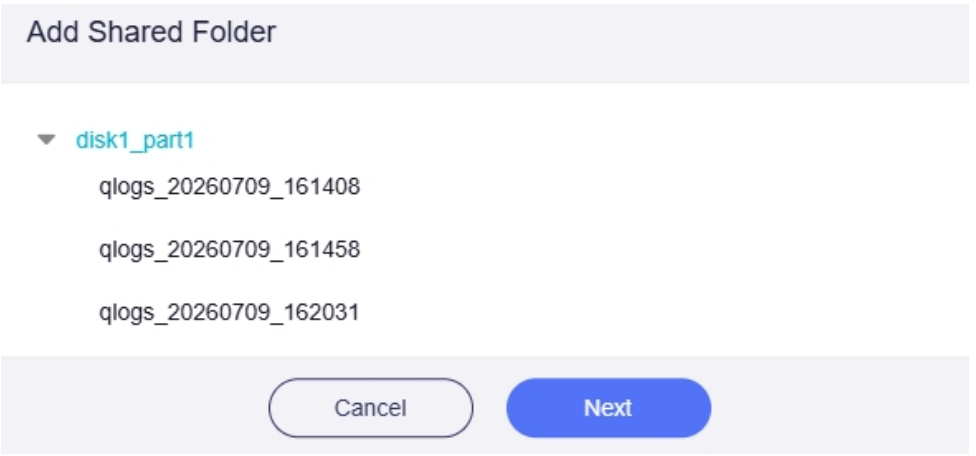
2. Haga clic en **Compartir configuración rápida** para establecer el enlace compartido.



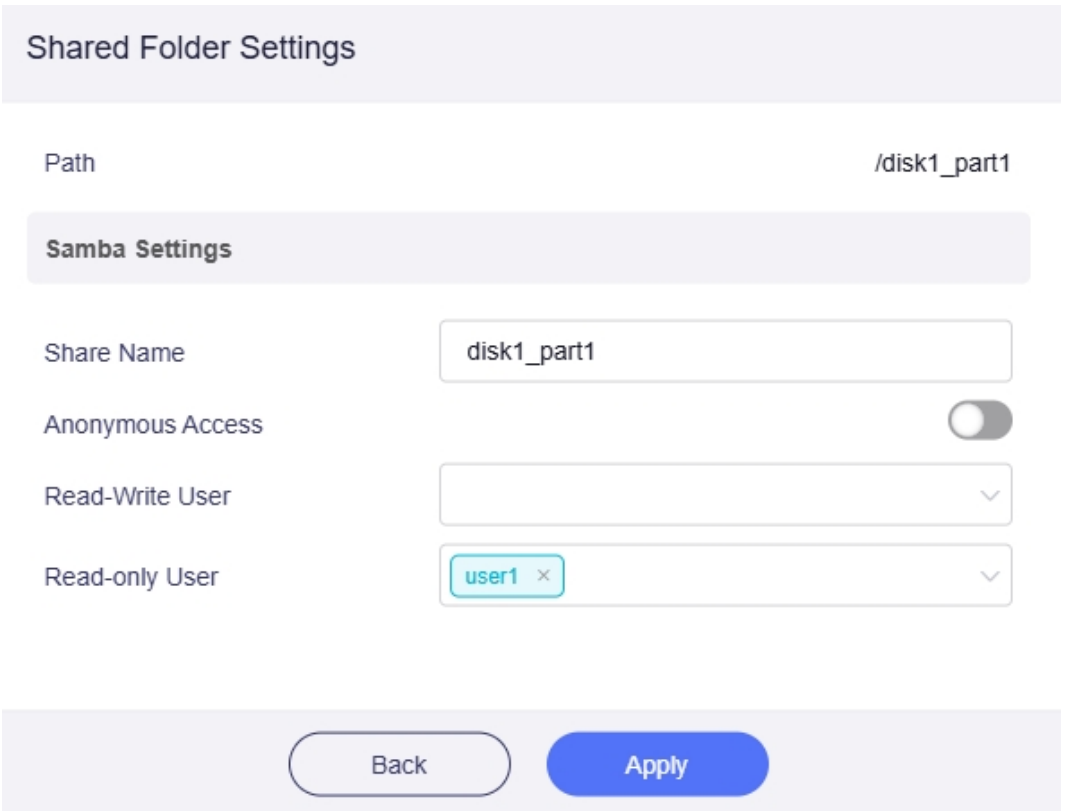

3. Agregue un usuario y haga clic en **Siguiente**. Este paso se omitirá si ya tiene una cuenta.



4. Haga clic en el ícono del triángulo para mostrar todas las carpetas. Sseleccione una carpeta para compartir, tluego haga clic **Siguiente**. Sisi lo desea para compartir el disco completo, haga clic en el nombre del disco (p. ej., disk1_part1).



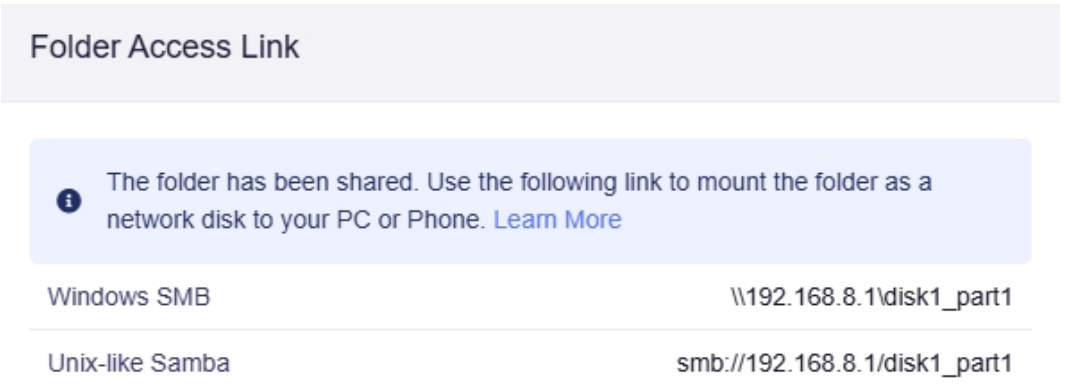

5. Configura la scarpeta compartida.
   Tel usuario creado en el paso anterior se agregará a **Usuario de solo lectura** de forma predeterminada. Si desea que este usuario pueda escribir o eliminar archivos, eliminarlo de Usuario de solo lectura y agregarlo a **Lectura-Escritura Usuario**, then haga clic en **Aplicar**.



**Consejo**: Por razones de seguridad, no se recomienda habilitar el acceso anónimo.

6. Obtenga el enlace de acceso a la carpeta .

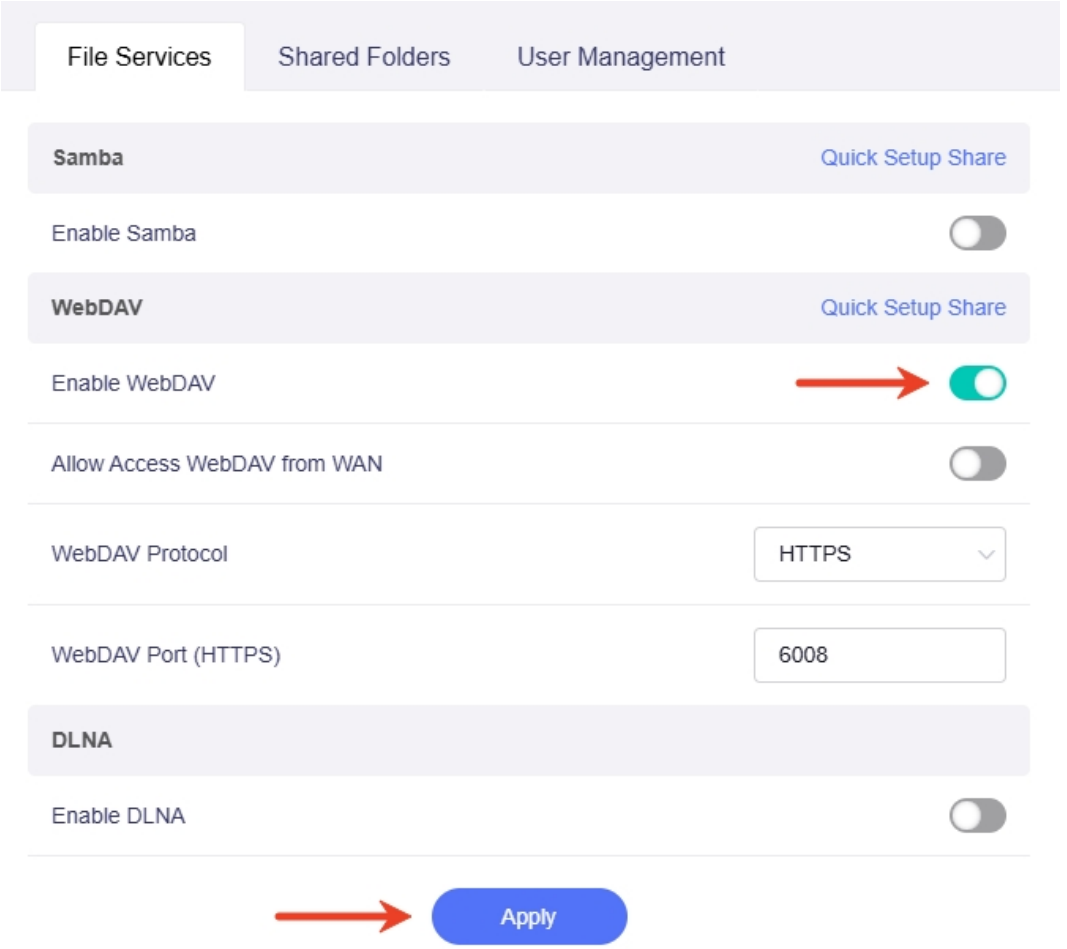
   La página mostrará el enlaces para Windows y sistemas operativos tipo Unix. El sistema tipo Unix incluyes Android, iOS, macOS, Ubuntu, etc. Ahora puedes acceder su carpeta compartida a través del servicio Samba a través de estos enlaces.




**Nota**: si habilita **Permitir acceso a Samba desde WAN** y acceda a la carpeta compartida desde red ascendente, reemplace la IP del enrutador (predeterminada: 192.168.8.1) en el enlace de acceso con su enrutador’s IP WAN, que se puede encontrar en la página INTERNET del panel de administración web.

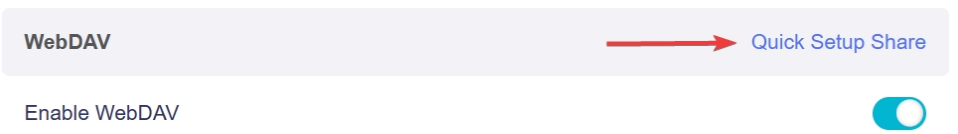
## 12.3.3 Configurar WebDAV

1. En **Servicios de archivos**, active **EwebDAV habilitable** y haga clic en **Aplicar**.

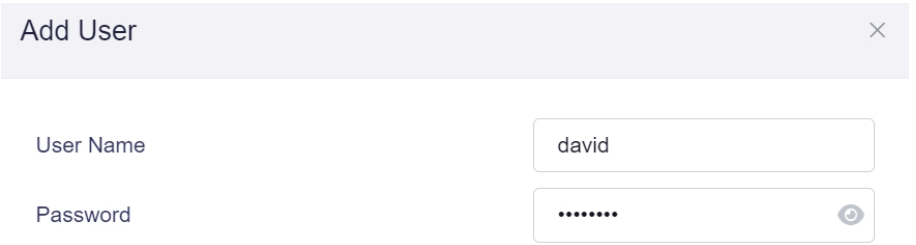



- **Permitir el acceso a WebDAV desde WAN**: habilítelo si desea que los dispositivos ascendentes acceder al servicio WebDAV.
- **Protocolo WebDAV**: HTTP no está cifrado; uso bajo su propio riesgo. HTTPS está cifrado y utiliza certificado autofirmado.
- **Puerto WebDAV**: no es necesario modificar el número de puerto a menos que haya un conflicto. El recomendado puerto número rango es 1024 - 65535.

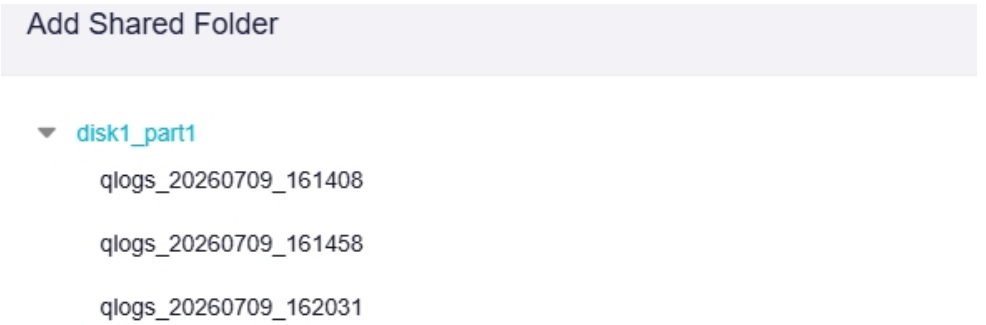
2. Haga clic en **Configuración rápida Compartir** para sconfigurar el enlace compartido.



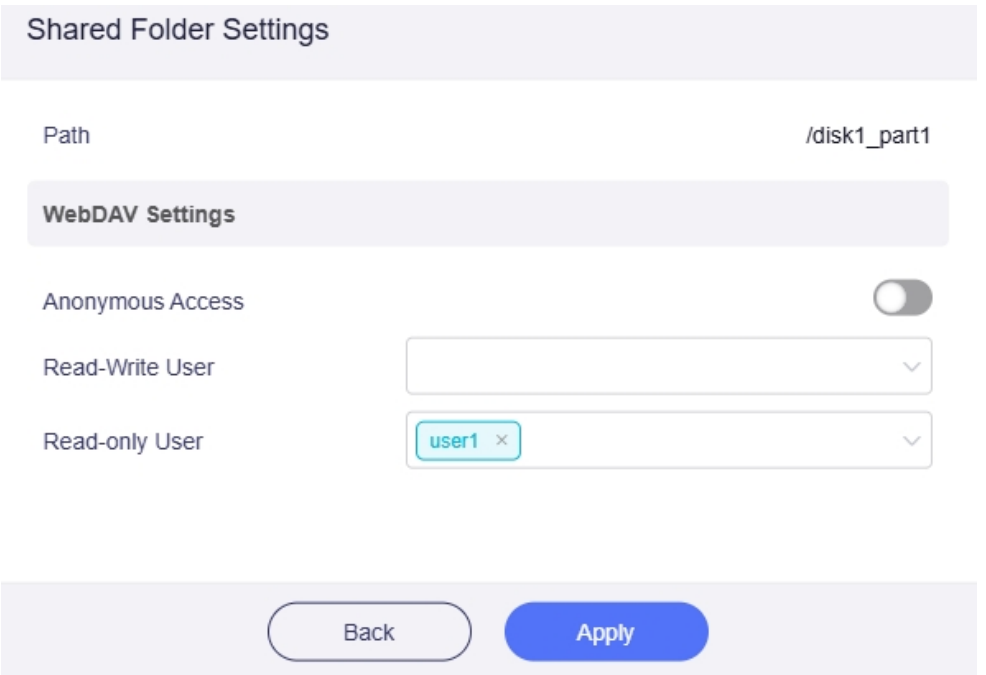

3. Agregue un usuario y haga clic en **Siguiente**. Este paso se omitirá si ya tienes una cuenta.




4. Haga clic en el ícono del triángulo para mostrar todas las carpetas. Sseleccione una carpeta para compartir. Sisi desea compartir el completo disco, haga clic en el nombre del disco (por ejemplo, disk1_part1).

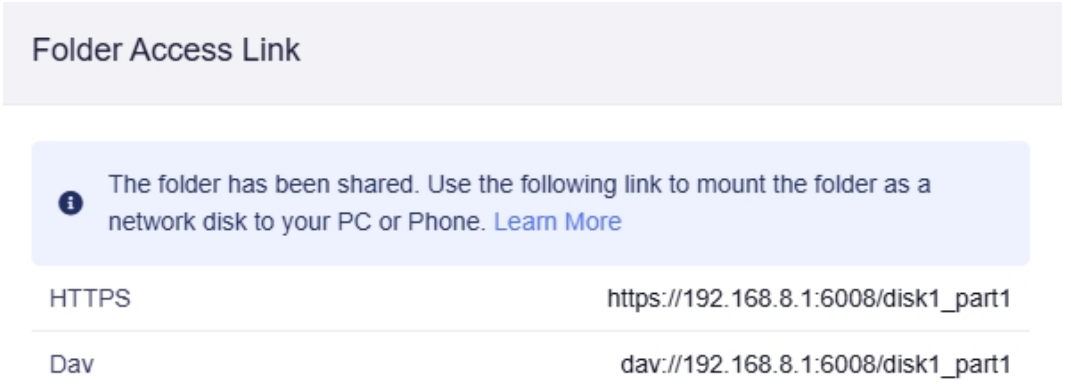



5. Configure la carpeta compartida.
   El usuario creado en el paso anterior se agregará a **Usuario de solo lectura** de forma predeterminada.
   Si desea que este usuario pueda escribir o eliminar archivos, elimínelo del Usuario de solo lectura y agréguelo a **Usuario de lectura y escritura** y luego haga clic en **Aplicar**.



6. Obtener el enlace de acceso a la carpeta.

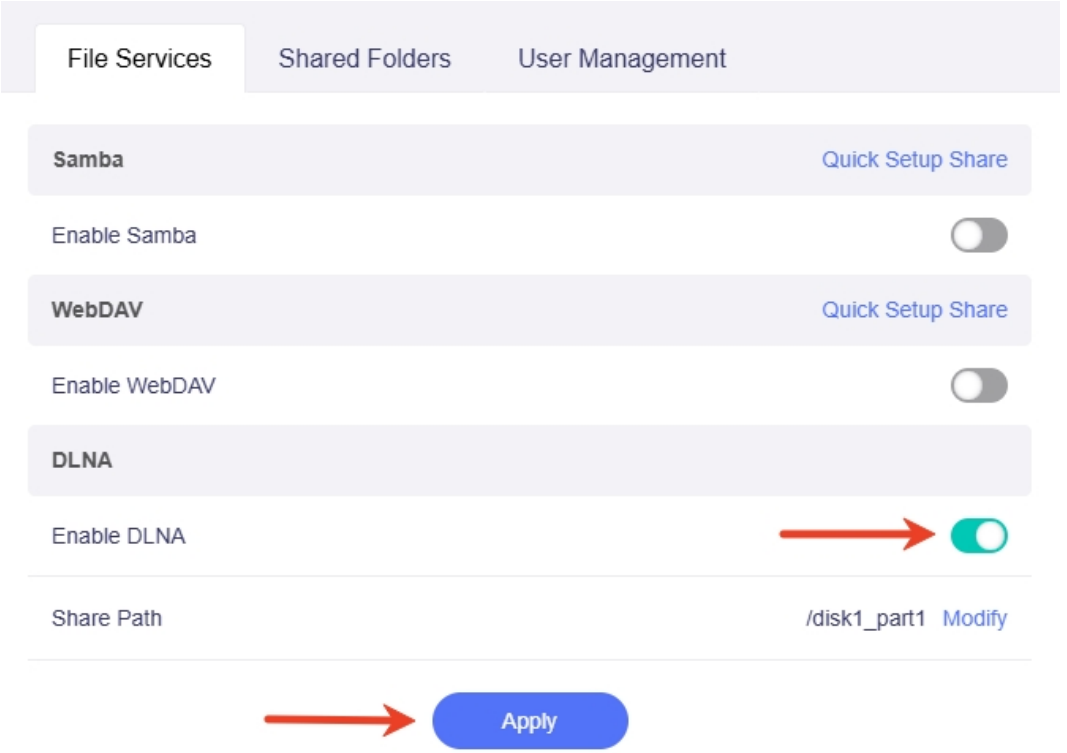
   La página mostrará los enlaces para Windows y sistemas operativos tipo Unix. Los sistemas tipo Unix incluyen Android, iOS, macOS, Ubuntu, etc. Ahora puede acceder a su carpeta compartida a través del servicio WebDAV a través de estos enlaces.



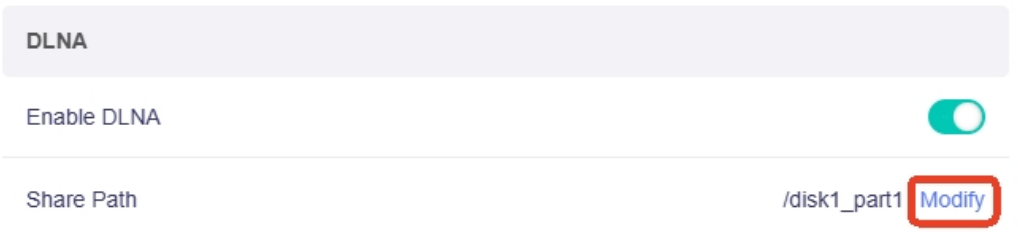

**Nota**: si habilita **Permitir acceso WebDAV desde WAN** y acceda la carpeta compartida de red ascendente, reemplace la IP del enrutador (predeterminada: 192.168.8.1) en enlace de acceso con la IP WAN de tu enrutador’s, que se puede encontrar en la página INTERNET del panel de administración web.

## 12.3.4 Configurar DLNA

1. En la sección **Servicios de archivos**, active **Ehabilite DLNA**, y haga clic en **Aplicar**.




2. Modifique la ruta compartida a la derecha si es necesario.



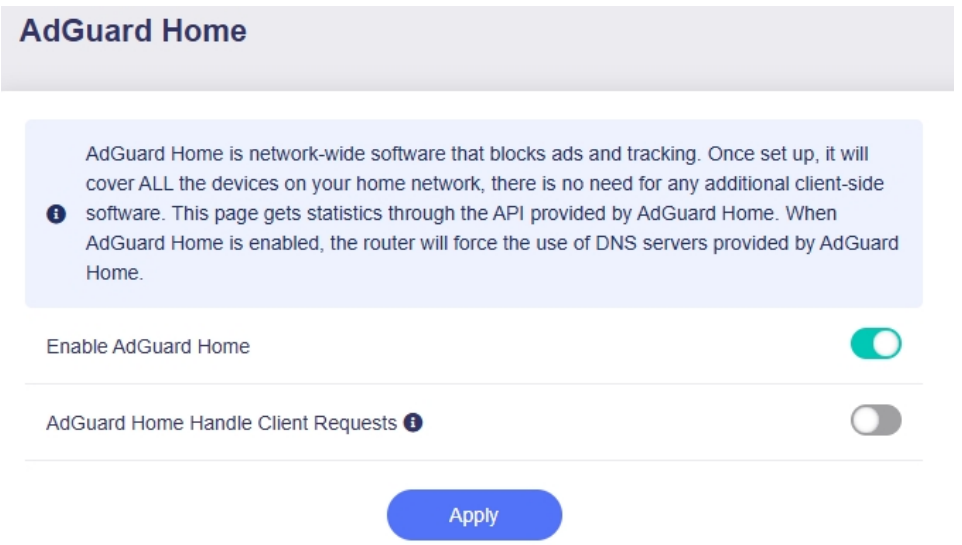

3. Conecte su televisor inteligente al enrutador. Es encontrará el DLNA sservidor automáticamente.

## 12.4 AdGuard Home

AdGuard Home es una red software de bloqueo de anuncios y prevención de seguimiento. Una vez configurado, cubrirá todos los dispositivos cliente sin necesidad de software adicional del lado del cliente.

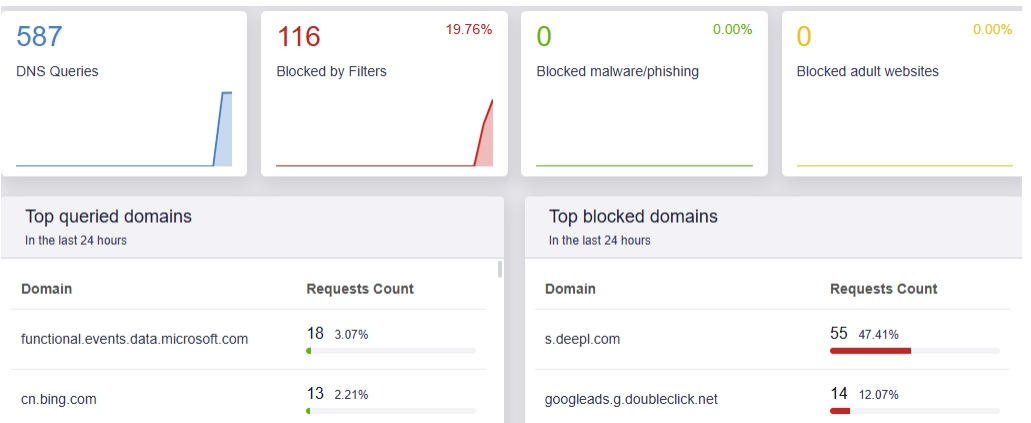
Siga estos pasos para configurar AdGuard Home.

1. Inicie sesión en el panel de administración web del enrutador, navegue hasta **APLICACIONES** > **AdGuard Home**. Active **Habilitar AdGuard Home** y haga clic en **Aplicar**.

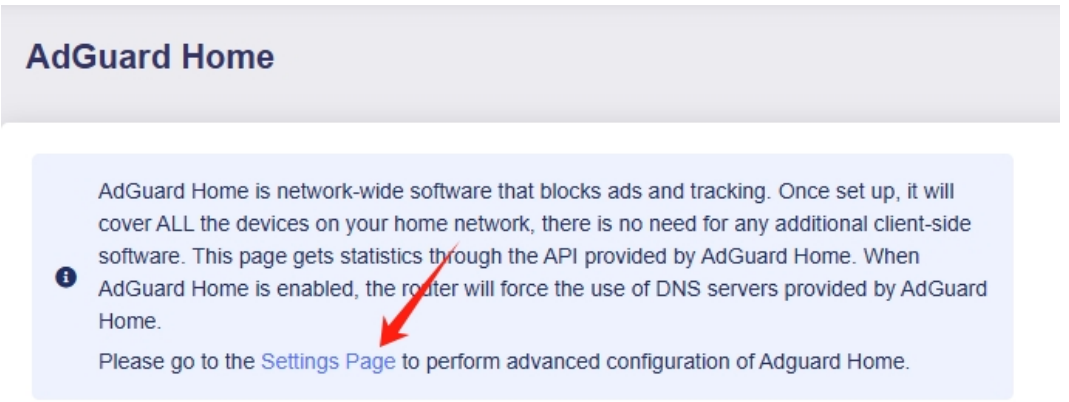



- **AdGuard Home Handles Cliente Solicitudes**: si está habilitado, las consultas de DNS de los dispositivos cliente serán manejadas directamente por AdGuard Home, pero esto hará que las políticas de VPN basadas en dominios fallen.

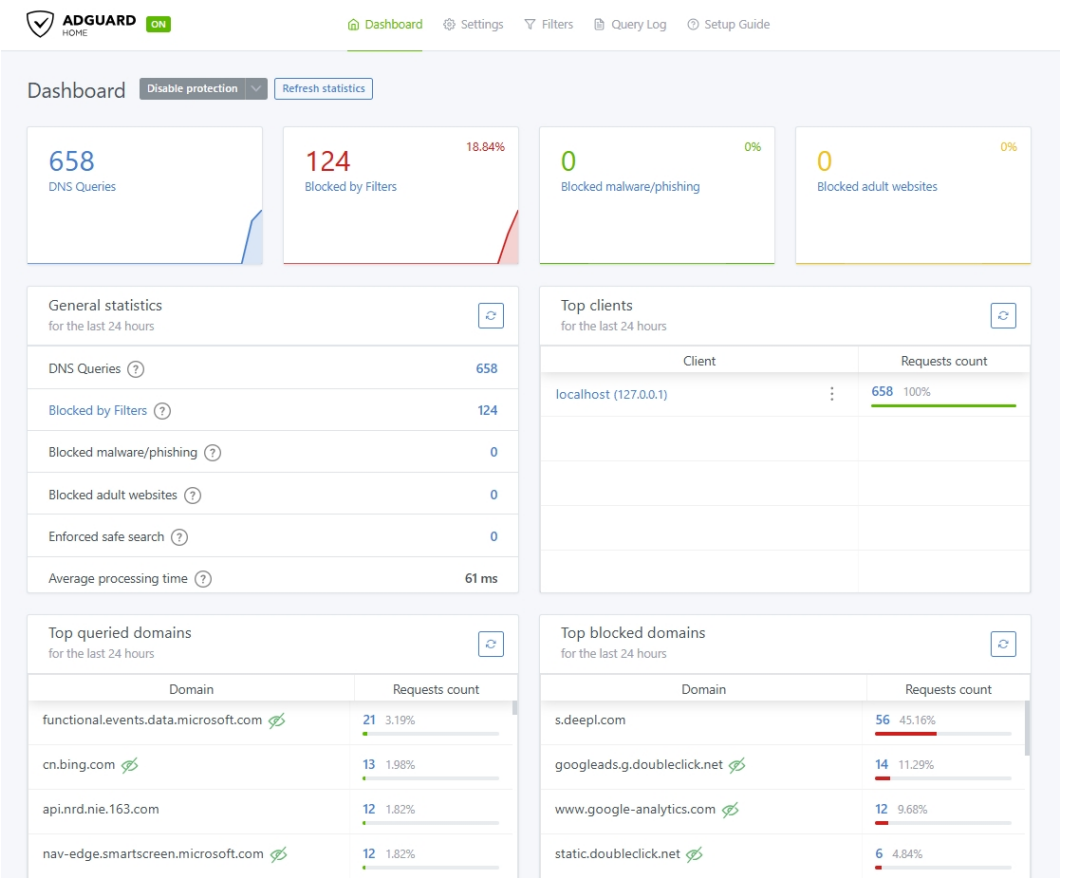
2. La página cargará automáticamente estadísticas de DNS (consultas, dominios bloqueados, etc.) a través de la API proporcionada por AdGuard Home.



3. Haga clic en **Página de configuración** para configurar avanzado configuración para AdGuard Home.




4. Será redirigido a la página de configuración de AdGuard Home'. visite la [AdGuard Inicio Soporte Centro] para asistencia.



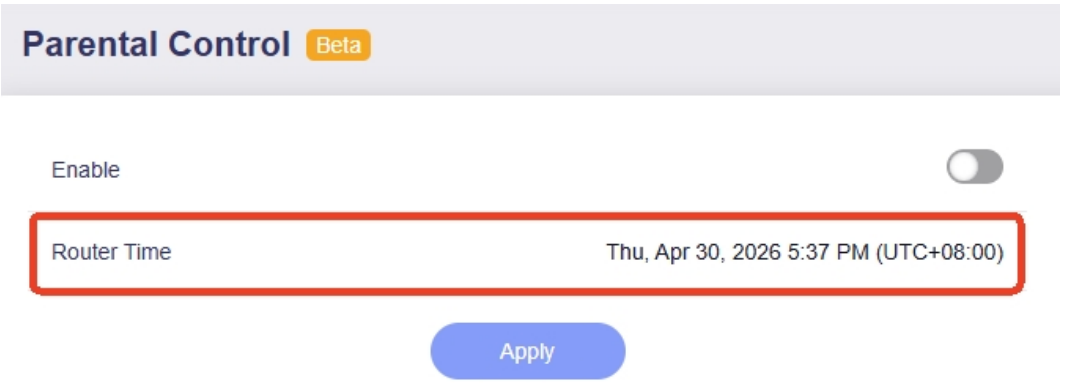
## 12.5 Control parental

El control parental es una forma de mantener a los niños seguros en línea bloqueando sitios web inapropiados y limitando el tiempo que usan los dispositivos. Ayuda a prevenir el acceso a contenido dañino, administrar el tiempo frente a la pantalla y garantizar que los niños usen Internet de manera responsable.

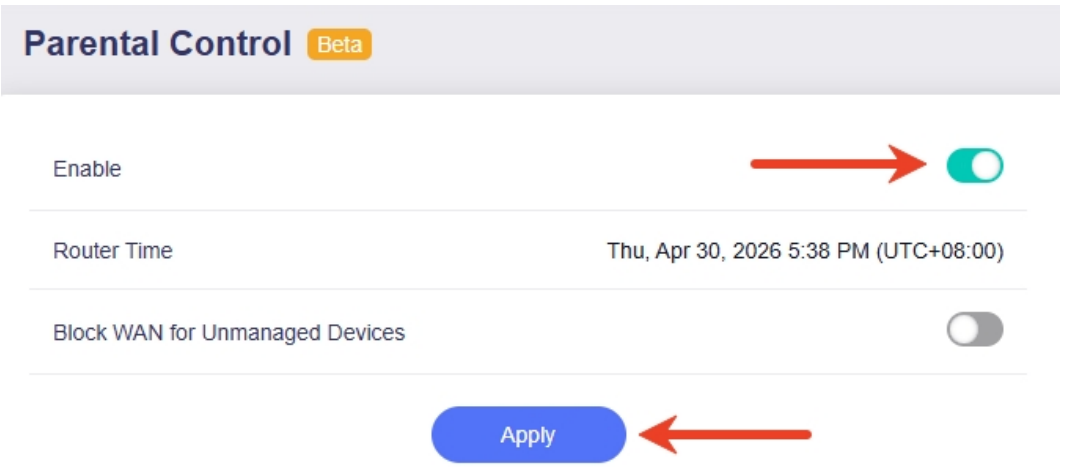
### 12.5.1 Configuración rápida

Siga estos pasos para configurar Control parental en GL.enrutador iNets.

1. Inicie sesión en el enrutador's web admin panel y vaya a **APLICACIONES** > **Control parental.** Asegúrese de que la hora del enrutador sea precisa. De lo contrario, vaya a **SISTEMA** > **Zona horaria** para sincronizarlo primero.




2. Habilitar control parental y haga clic en **Aplicar**. Luego siga el asistente de configuración para configurar el control parental. También puedes ver el vídeo de configuración aquí.



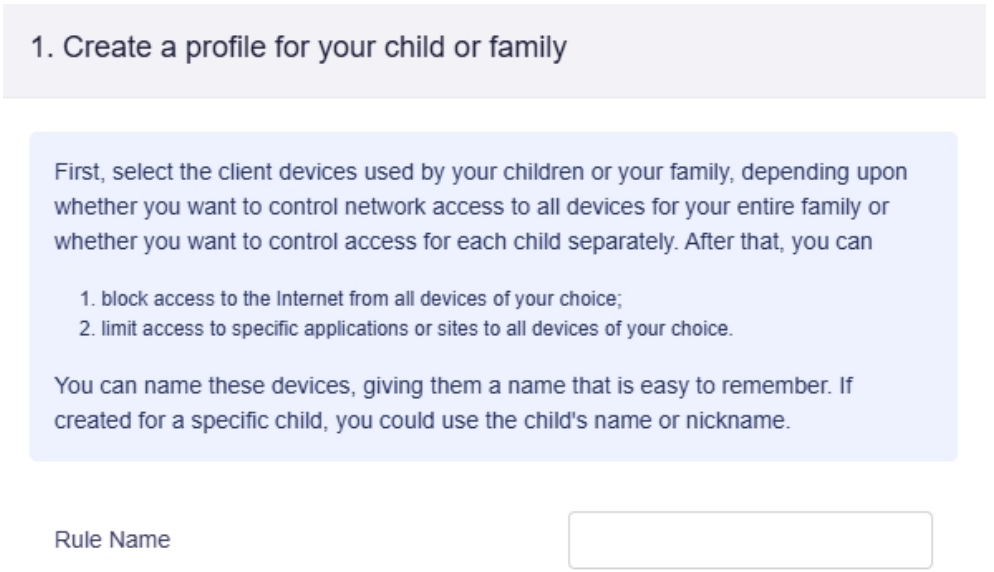

- **Bloquear WAN para dispositivos no administrados**: Bloquea el acceso a Internet para todos los dispositivos que no están en la lista de Control parental.

Aquí tienes un caso de uso para tu referencia.

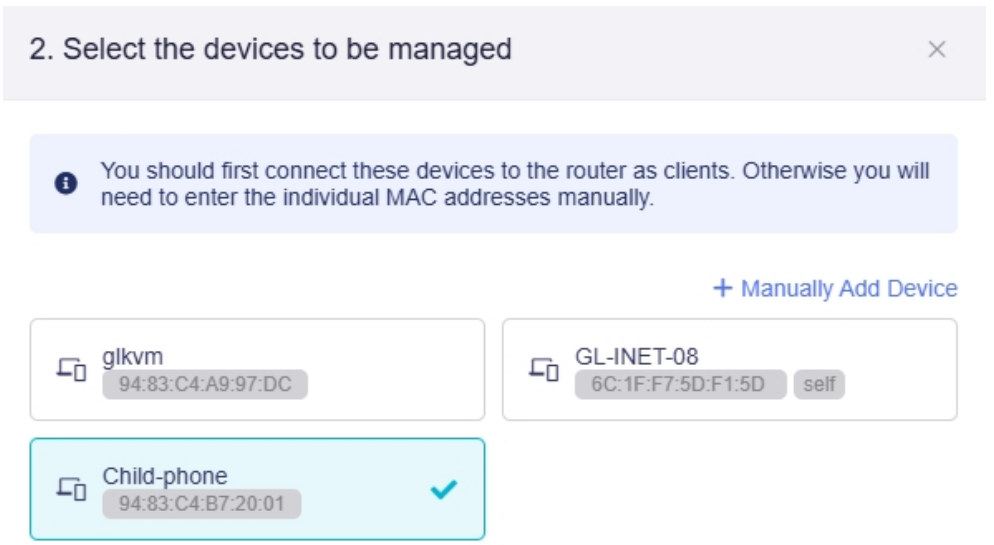
**Escenario:** Los dispositivos en este perfil solo pueden acceder a Internet para estudiar de 8 a.m. a 11 a.m. de lunes a viernes y para jugar de 6 p.m. a 8 p.m. los fines de semana. El acceso a Internet está bloqueado de forma predeterminada en todos los demás momentos.

**Pasos de configuración:**

1. Cree un perfil y personalice un nombre.



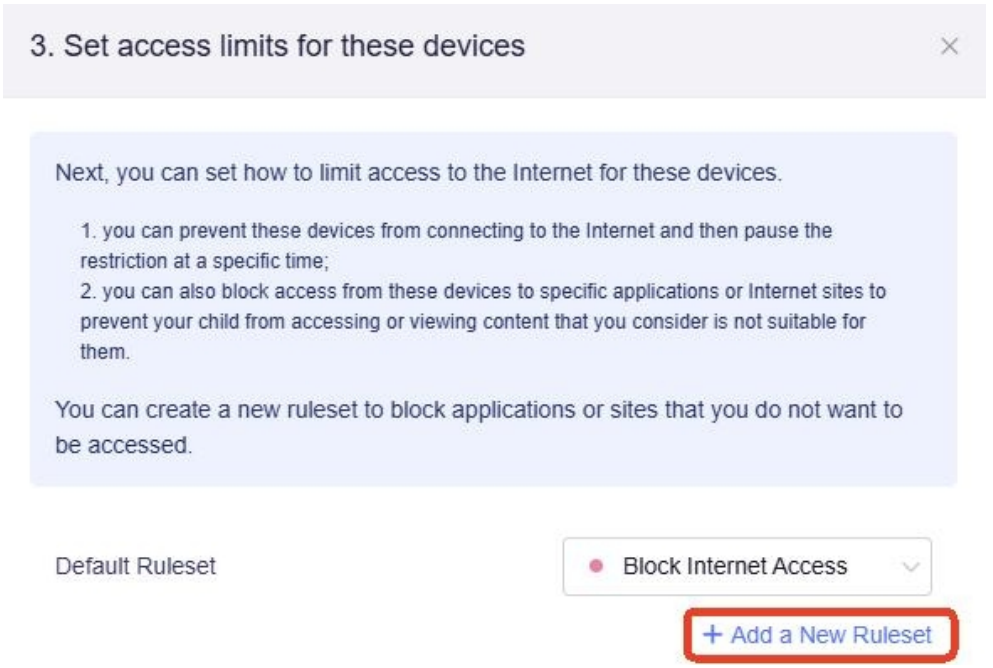

2. Seleccione los dispositivos que desea administrar. Conéctelos primero al enrutador. Si no se han conectado al enrutador, agréguelos manualmente ingresando sus direcciones MAC.



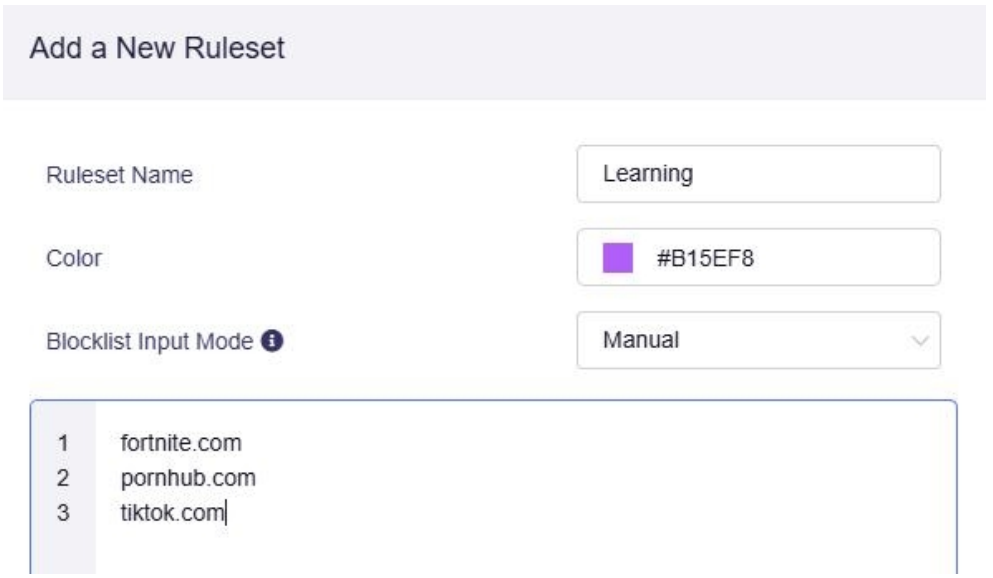
3. Establezca el límite de acceso.

Hay dos conjuntos de reglas predeterminados: **Bloquear el acceso a Internet** y **Sin límite**.

Haga clic en **Agregar un nuevo conjunto de reglas** para crearcrear dos conjuntos de reglas más para su uso posterior: **Aprendizaje** y **Reproducir**.

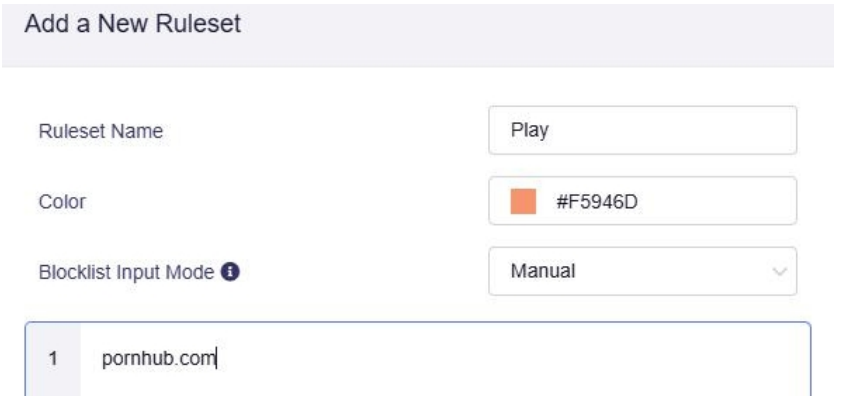



Especifique el nombre del conjunto de reglas (por ejemplo, Aprendizaje) y color, ingresa a la websitios tpara bloquear, tluego haga clic en **Aplicar**.

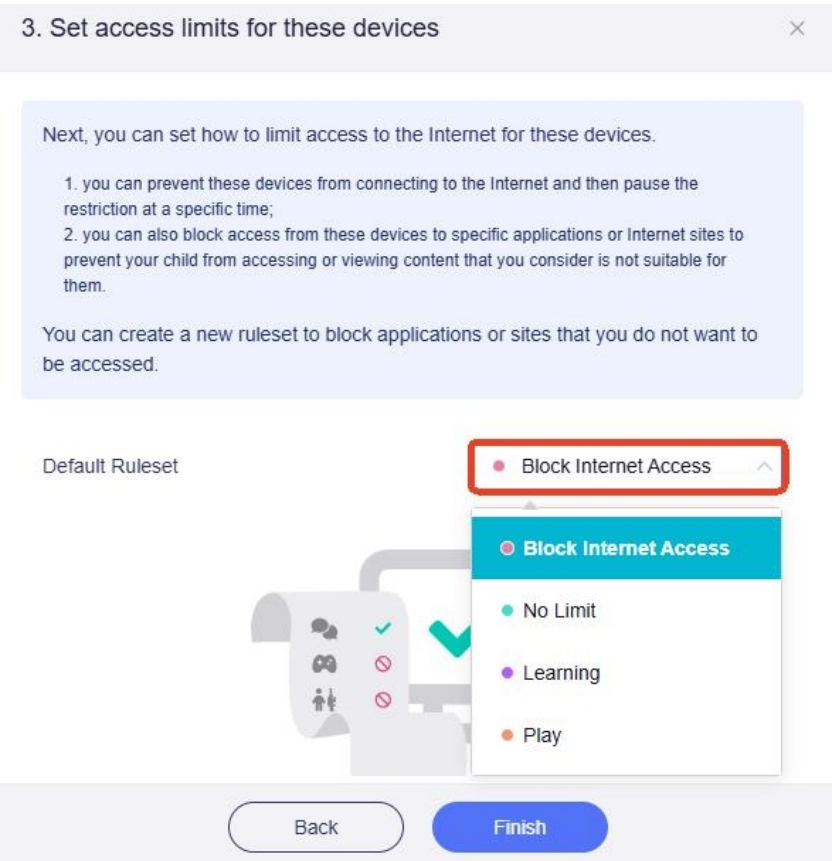


**Nota**: Los nombres de dominio ingresados en la lista de bloqueo deben incluir sus subdominios. Por ejemplo, si se ingresa "ejemplo.com", también incluye cualquier subdominio, como "subdominio.example.com".

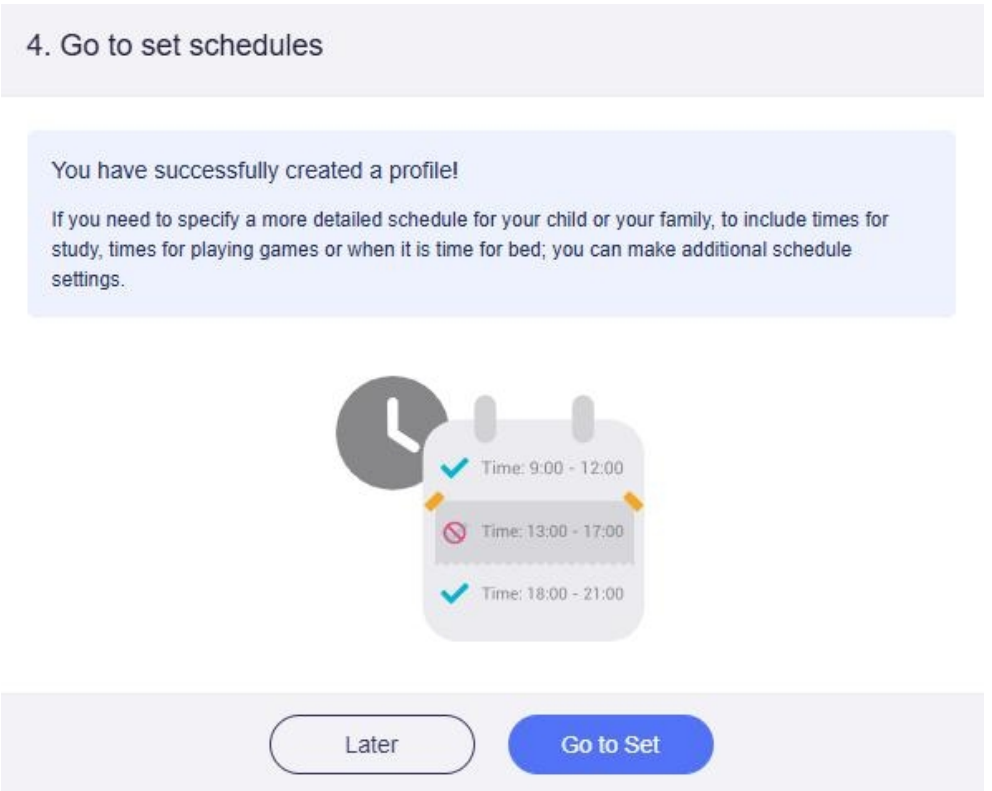
Del mismo modo, cree otro conjunto de reglas. Especifique el nombre del conjunto de reglas (por ejemplo, Reproducir) y el color, ingrese los sitios web que desea bloquear y luego haga clic en **Aplicar**.



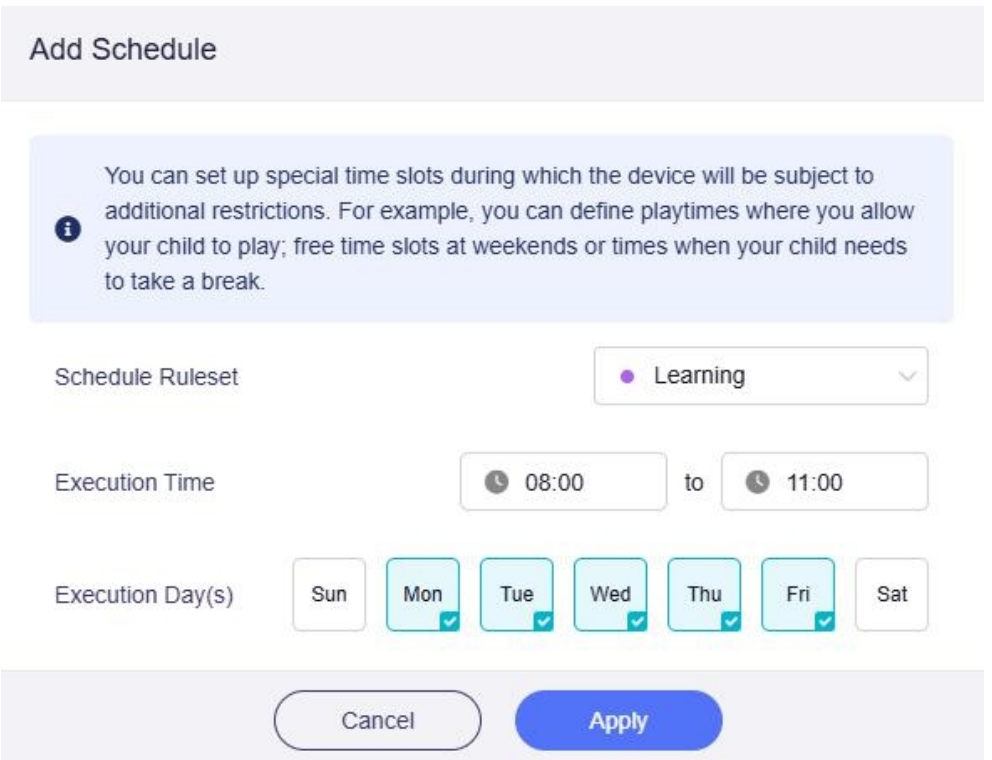

Al aplicared, habrá un total de cuatro conjuntos de reglas. Sseleccione **Bloquear acceso a Internet** como el **Conjunto de reglas predeterminado** y haga clic en **Finalizar**.



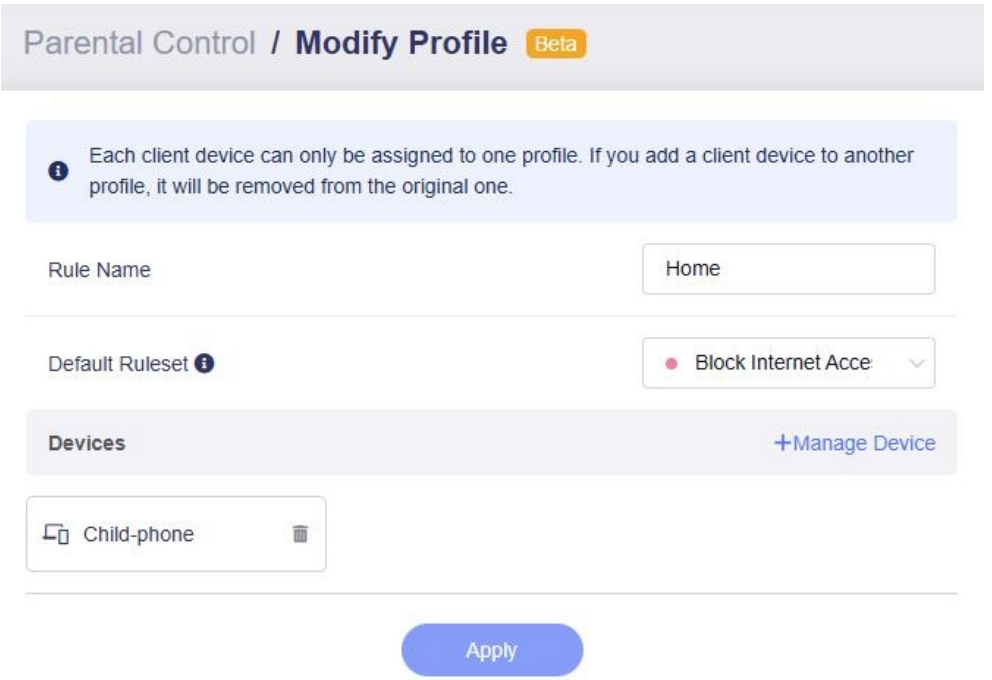
4. A continuación, establezca la programación para su perfil. Haga clic en **Ir a conjunto**.



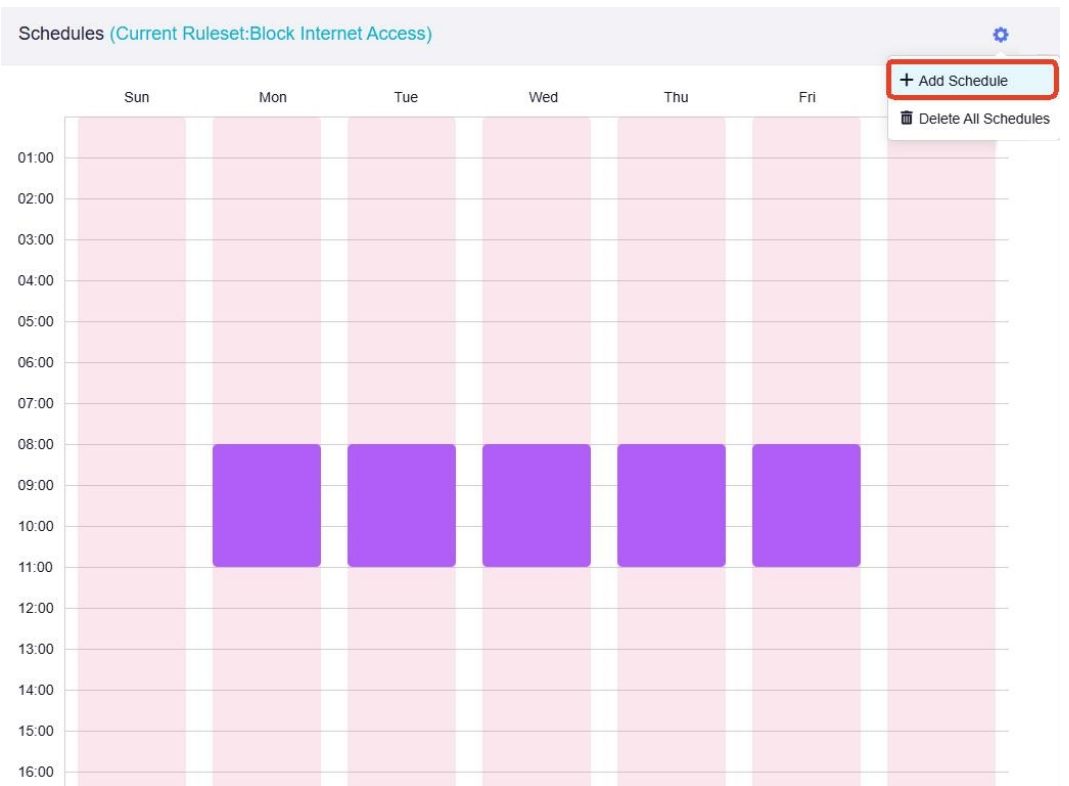

Agregue el conjunto de reglas **Aprendizaje** a la programación. Establezca el **Hora de ejecución** de 8 a. m. a 11 a. m. de lunes a viernes y luego haga clic en**Aplicar**.



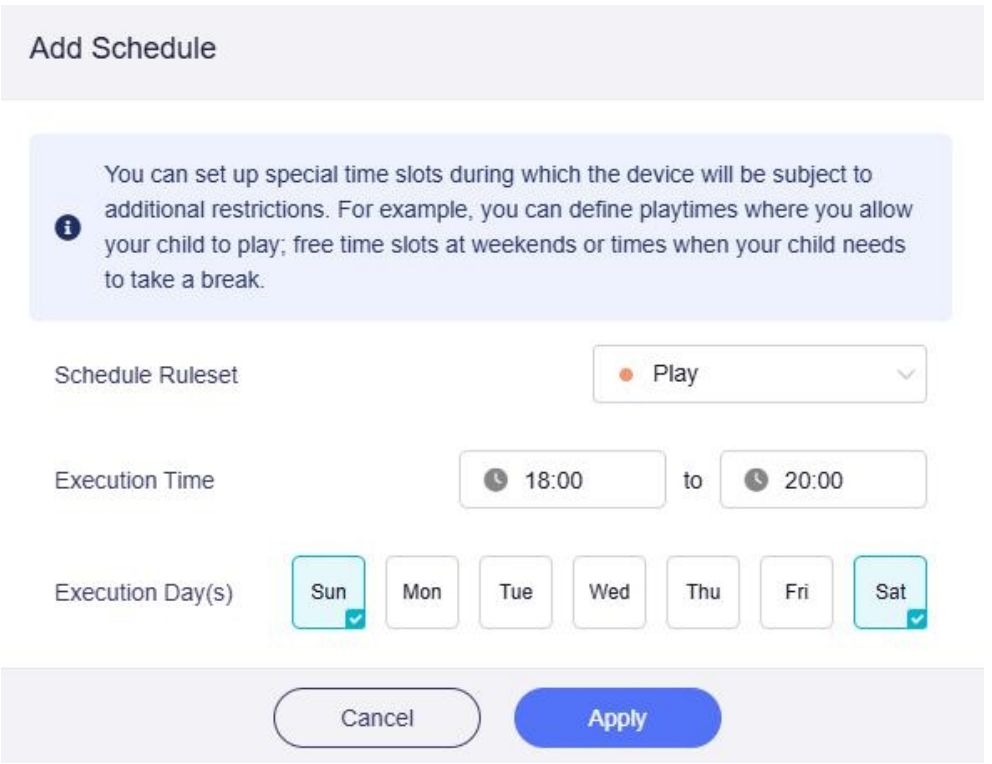
5. Será redireccionado a la página de edición del perfil creado.



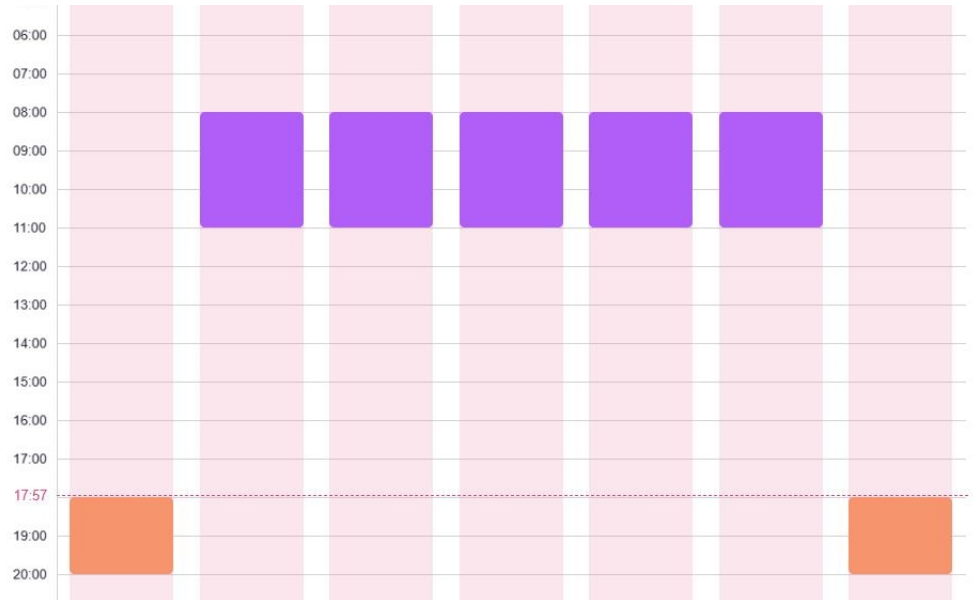

Muévase al final y podrá Verá que se ha creado un horario. Haga clic en el ícono de ajustes en la parte superior derecha y seleccione **Agregar programación**.



6. Agregar otro conjunto de reglas **Reproducir** al cronograma. Establezca el **Tiempo de ejecución** de 6:00 p. m. a 8:00 p. m. los fines de semana y luego haga clic en **Aplicar**.




El conjunto de reglas de Play se agregará al cronograma.

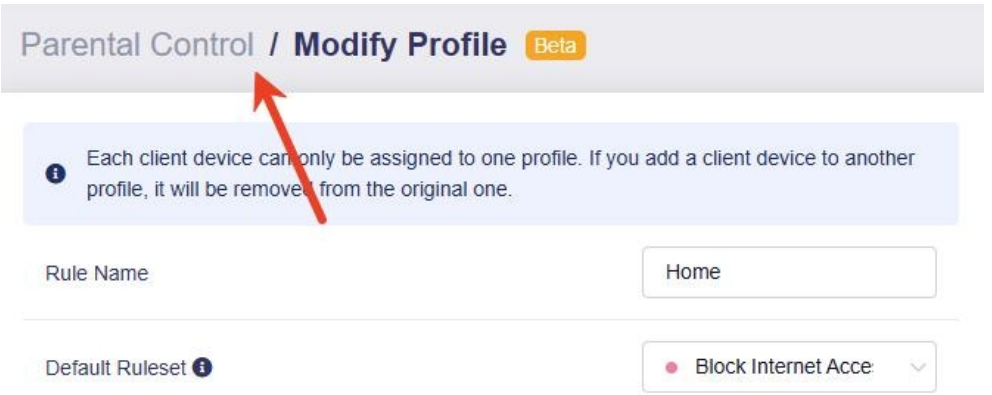



**Consejos**:

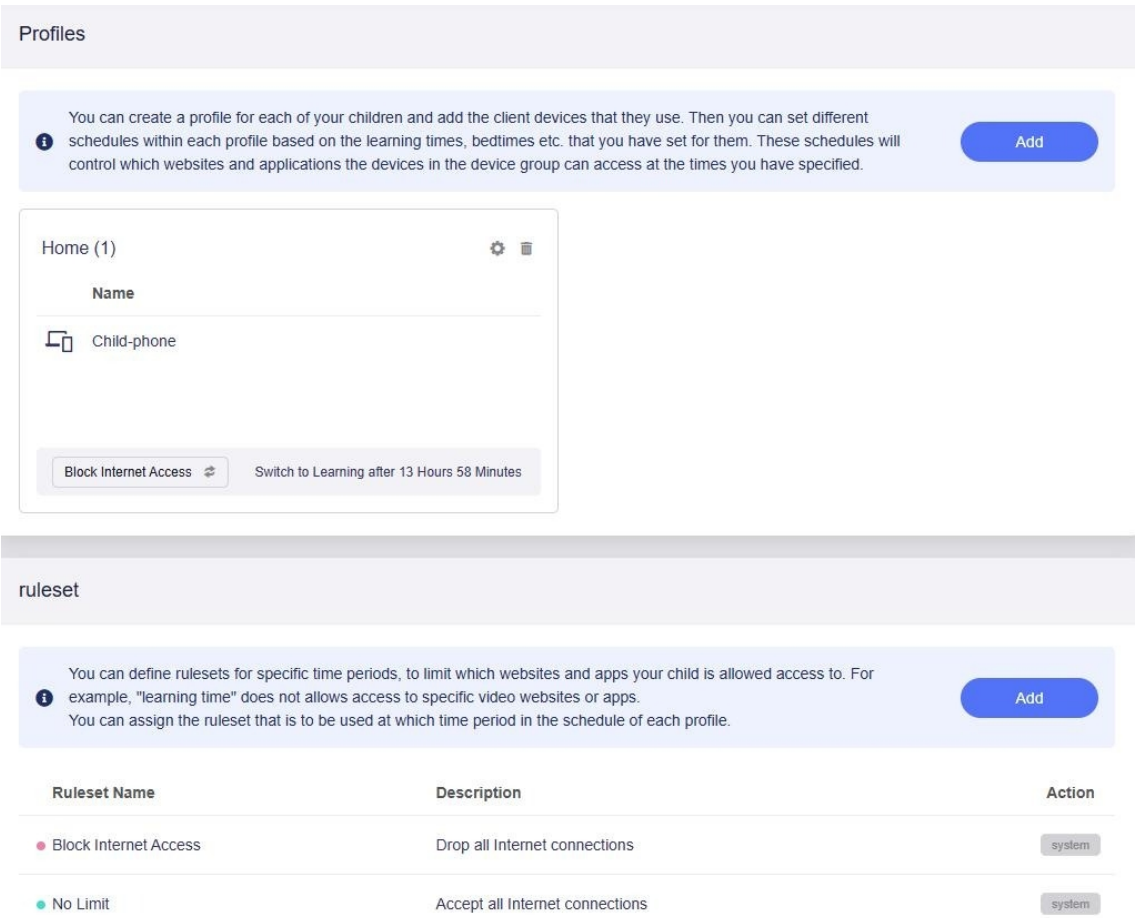
- La línea discontinua roja indica la hora actual.

- Ypuede modificar el tiempo de ejecución haciendo clic en en un cierto conjunto de reglas en la programación.

7. Click **Control parental** en la parte superior para regresar a la página Control parental.




Verá la configuración final. El control parental ahora está entrando en vigor según el cronograma. Puede modificar perfiles y conjuntos de reglas existentes, o agregar otros nuevos si es necesario.



## 12.5.2 Solución de problemas

Si los ajustes configurados no surten efecto, verifique las siguientes causas posibles.

1. Caché DNS problema.

   Los navegadores y los sistemas operativos mantienen cachés de DNS, lo que puede retrasar la aplicación de los cambios de configuración. Borre la caché de DNS para aplicar los cambios inmediatamente.
2. La programación del perfil aún no ha comenzado.
3. El nombre de dominio ingresado puede ser incorrecto.

   Si bien el dominio público de un sitio web es fácil de encontrar, los dominios API utilizados por las aplicaciones a menudo no están disponibles públicamente. Para localizar el dominio correcto, utilice una herramienta de captura de paquetes como Wireshark o busque la información relevante del dominio.

   Por ejemplo, al bloquear “www.google.com”, ingresar “google.com” ofrece mejores resultados que “www.google.com”.
4. El dispositivo de destino utiliza una dirección MAC aleatoria para cada conexión de red, que impide ques las reglas de acceso entren en vigor. Deshabilitar aleatorio MAC dirección en el dispositivo de destino y luego vuelva a agregar el dispositivo a su perfil.

## 12.6 Tailscale

Tailscale es un servicio VPN que hace que sus dispositivos y aplicaciones personales sean accesibles en todo el mundo, de forma segura y sin esfuerzo. Consulte aquí para obtener más detalles.

La función Tailscale en los enrutadores GL.iNet permite que el enrutador se una a una red virtual Tailscale, lo que permite el acceso remoto al enrutador mismo, así como a sus recursos WAN y LAN.

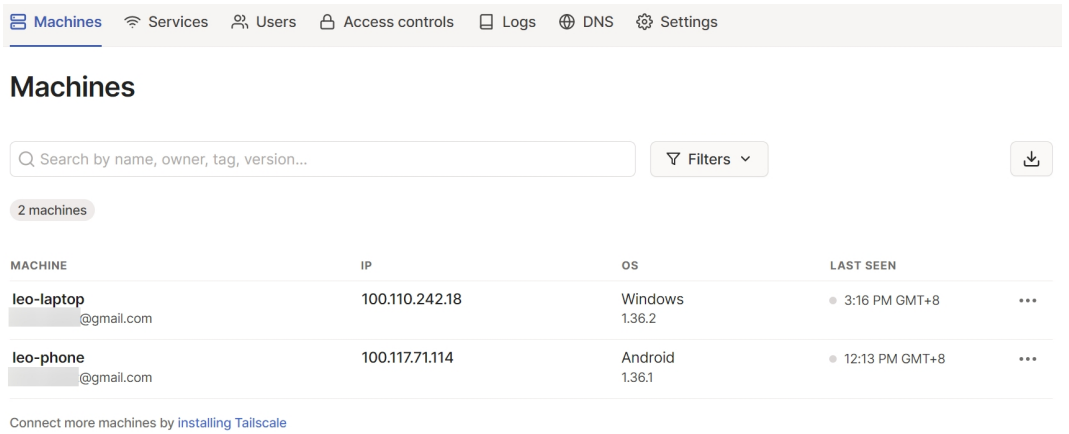
**Nota**:

1. Dado que Tailscale se basa en WireGuard, no se recomienda utilizar Tailscale con ninguna de las siguientes funciones o servicios simultáneamente, ya que esto puede causar conflictos de enrutamiento: Cliente OpenVPN, Cliente WireGuard, GoodCloud Site to Site, ZeroTier, AstroWarp.
2. Esta función se encuentra actualmente en versión beta y puede tener algunos errores.

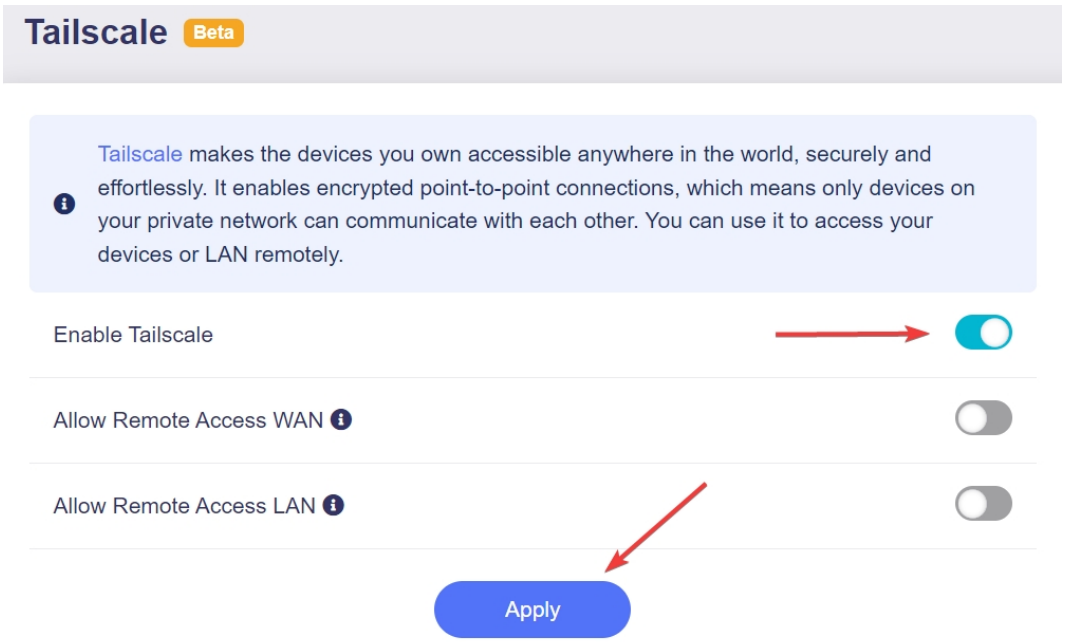
## 12.6.1 Configurar Tailscale

Aquí se muestra un ejemplo del uso de GL-MT2500 para configurar la red Tailscale.

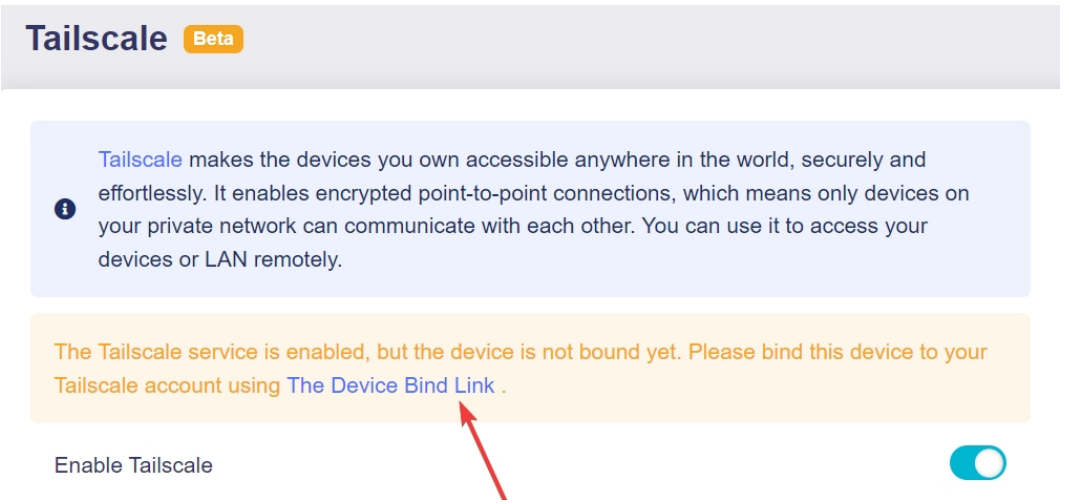
1. Primero registre una cuenta de Tailscale y vincule una o dos dispositivos a su cuenta de Tailscale para fines de prueba. Después de vincular, verá sus dispositivos en la consola Tailscale.




2. Inicie sesión en el panel de administración web de su enrutador' y navegue hasta **APLICACIONES** > **Tailscale**. Activa **Habilitar Escala de cola** y haz clic en **Aplicar**.



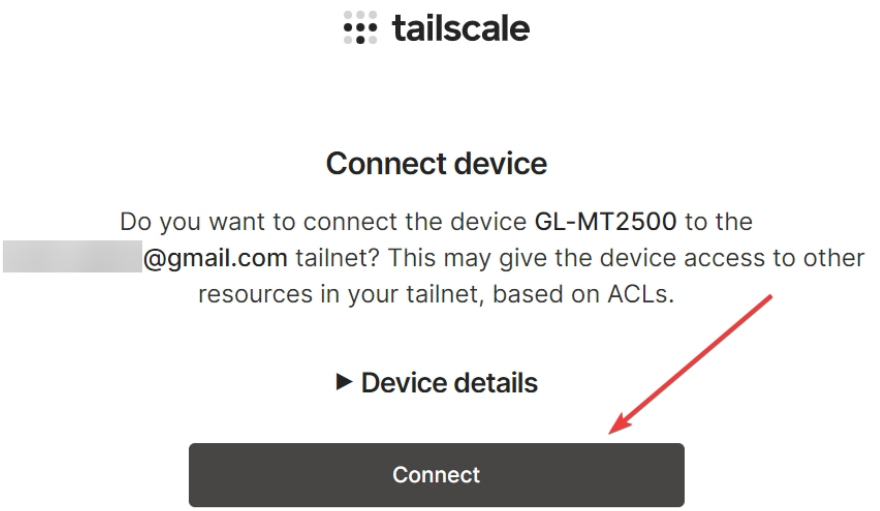

3. La página le pedirá que enlace el dispositivo. Haga clic en **Enlace de enlace de dispositivo**.



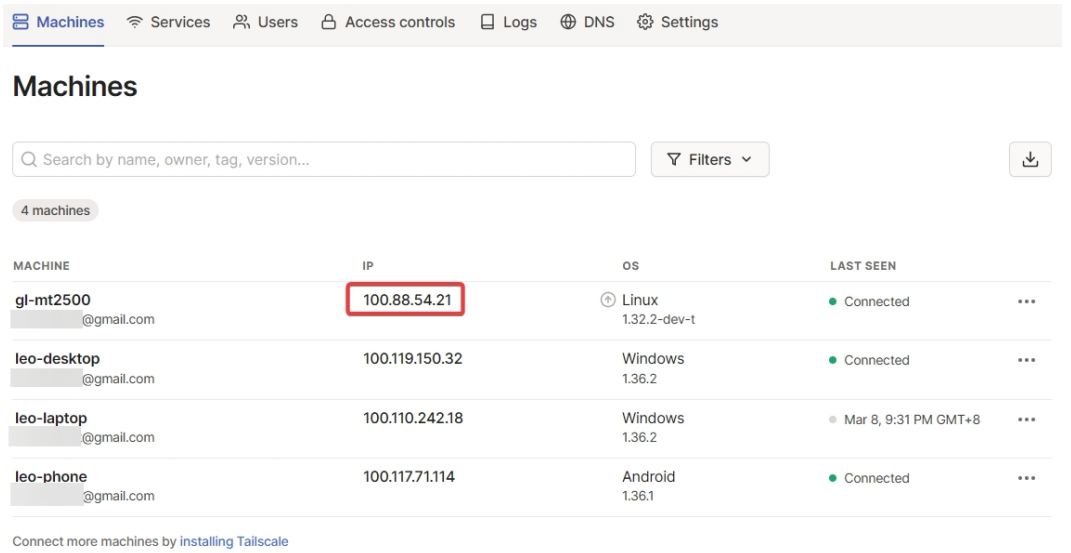

4. En el ventana emergente, haga clic en el enlace e inicie sesión con su cuenta de Tailscale.




5. Una vez que haya iniciado sesión, se le pedirá que confirme el dispositivo. Haga clic en **Conectar**.



6. Yserá luego será redirigido a Tailscale consola de administración. Ahora el enrutador se ha agregado a la red virtual de Tailscale y se puede acceder a él de forma remota mediante la IP virtual de Tailscale. 100.88.54.21.

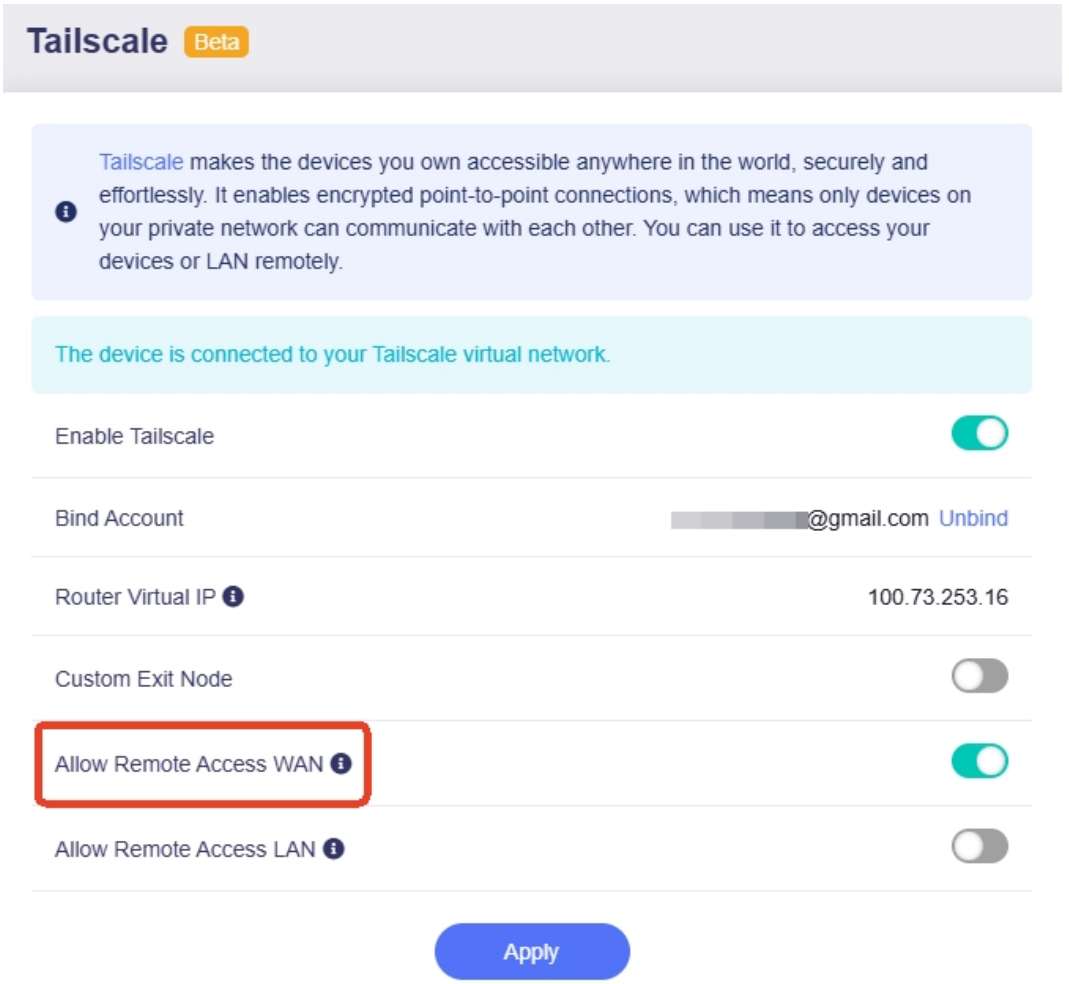



7. Pruebe la conectividad.

   En otro dispositivo conectado a la misma red de Tailscale, abra un navegador web e ingrese el enrutador's IP virtual en la barra de direcciones. Si puede acceder al panel de administración web del enrutador, significa que Tailscale está funcionando. También puede usar el comando ping o iniciar sesión SSH en el terminal del enrutador'panel de administración web, significa que Tailscale está funcionando. También puede utilizar el comando ping o iniciar sesión SSH en el enrutador'por su IP virtual para probar la conectividad.

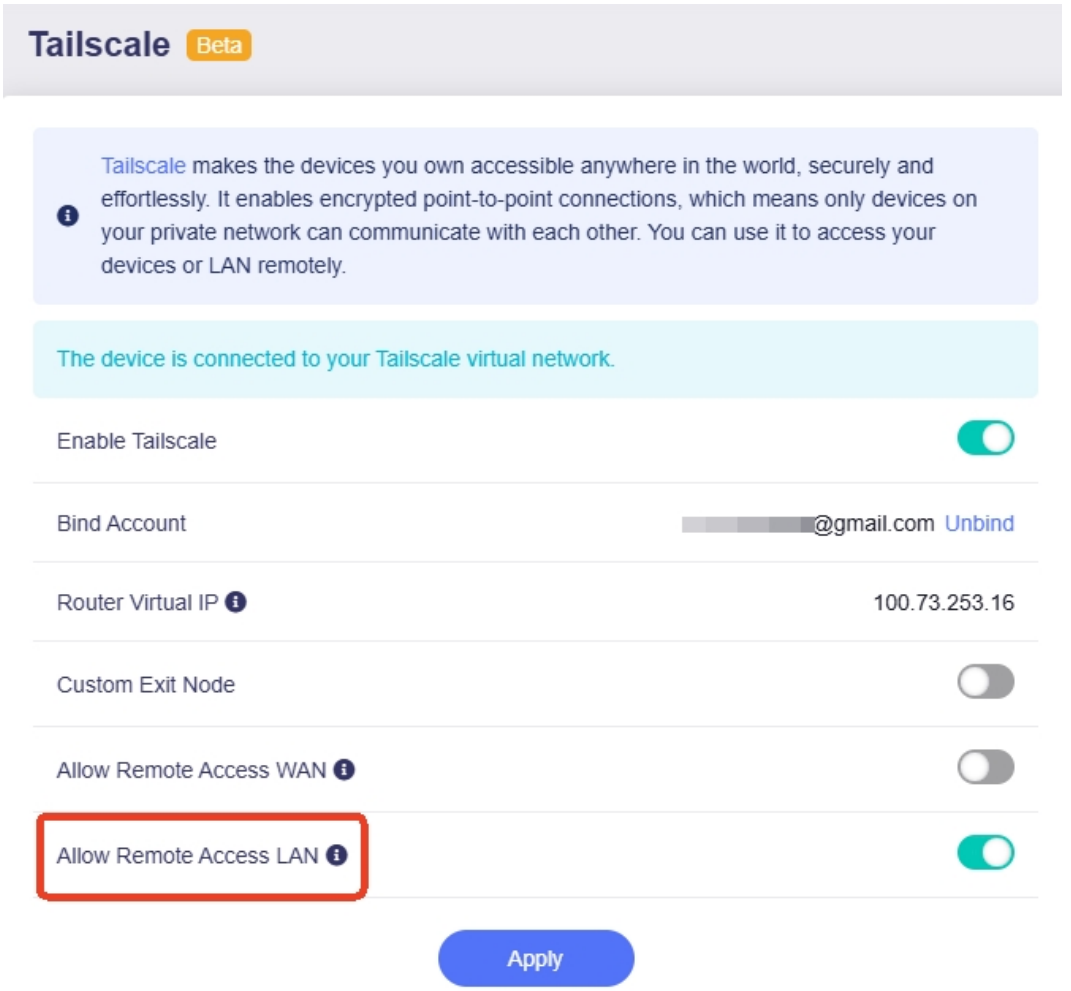
## 12.6.2 Permitir el acceso remoto a la WAN

Si esta opción está habilitada, se puede acceder a los recursos en el lado WAN del dispositivo a través de la red virtual Tailscale. Consulte aquí para obtener más detalles.



## 12.6.3 Permitir el acceso remoto a la LAN

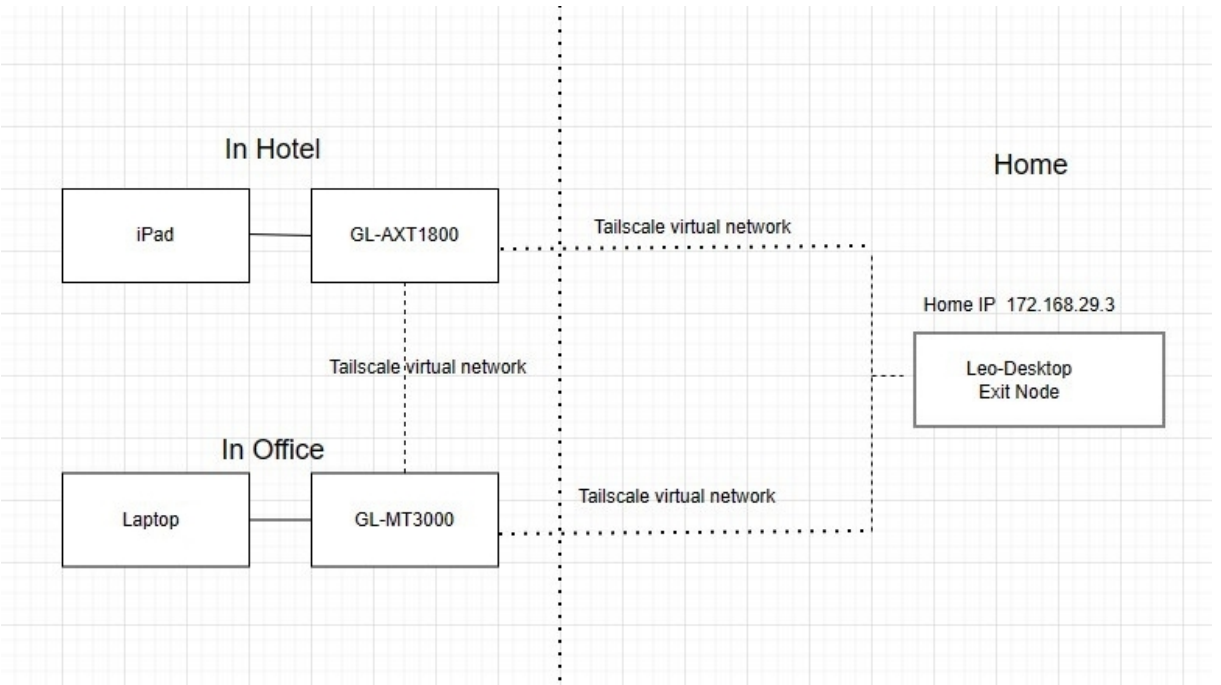
Si esta opción está habilitada, se puede acceder a los recursos en el lado LAN del dispositivo a través de la red virtual Tailscale. Consulte aquí para obtener más detalles.



## 12.6.4 Nodos de salida personalizados

De forma predeterminada, Tailscale actúa como una red superpuesta: solo enruta el tráfico entre dispositivos que ejecutan Tailscale y no procesa su tráfico público de Internet, como al navegar sitios web como Google.

Sin embargo, puede haber ocasiones en las que desee que Tailscale enrute su tráfico público de Internet. Por ejemplo, cuando está fuera de casa o viaja al extranjero, si necesita acceder a servicios en línea (como banca) que solo están disponibles en su país de origen, puede configurar el escritorio de su hogar con una IP pública como nodo de salida y configurar otros dispositivos en la misma Tailnet, como el GL-AXT1800 y el GL-MT3000 en la imagen a continuación, para enviar su tráfico a través de él. Esto permite que todo su tráfico público de Internet se reenvíe a través del nodo de salida.



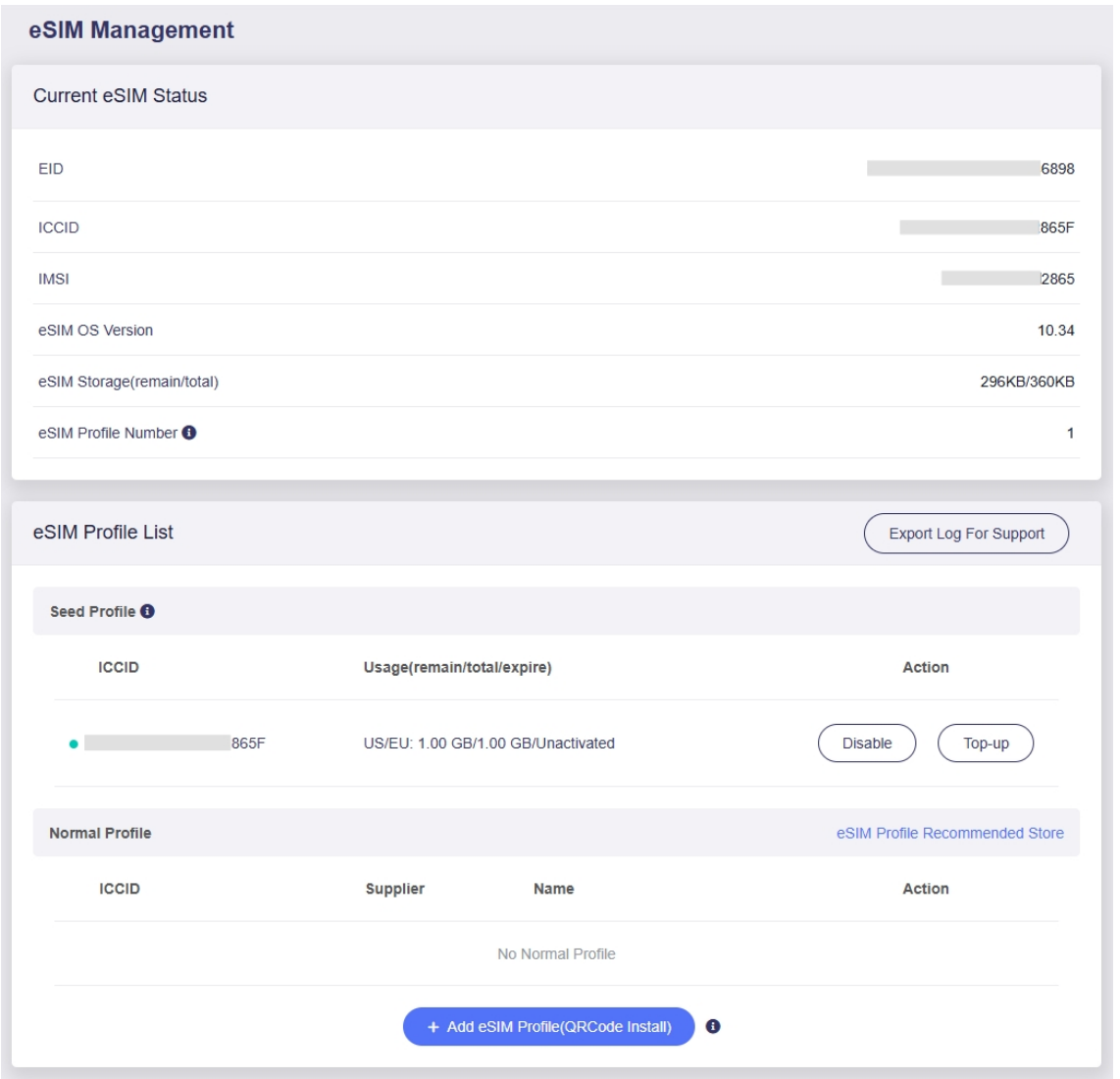

En resumen, un nodo de salida enruta el tráfico de Internet saliente desde sus dispositivos Tailnet, actuando efectivamente como servidores VPN. Cuando se conecta a un nodo de salida, todo su tráfico de Internet que no es de Tailscale parece originarse desde su ubicación, lo que le ayuda a acceder a contenido restringido geográficamente y mejorar su privacidad en línea. El dispositivo que maneja este reenvío de tráfico se conoce como "nodo de salida". Consulte aquí para obtener más detalles.

**Nota**: Si el servidor DNS del enrutador es privado Dirección IP a la que solo se puede acceder en la red local; es posible que pierda el acceso a Internet al ejecutar los nodos de salida. Para evitar esto, configure un servidor DNS público (por ejemplo, 8.8.8.8) manualmente para su enrutador.

## 12.7 Gestión de eSIM

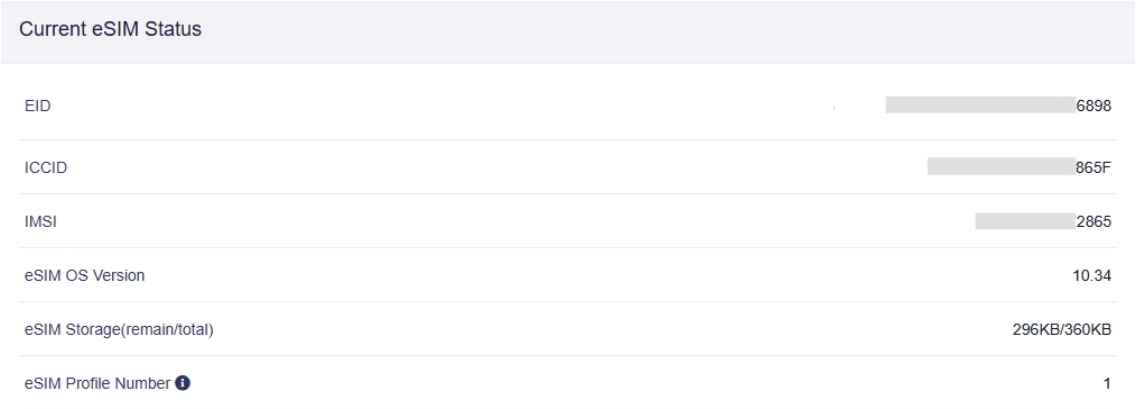
La administración de eSIM le permite verificar el estado de la tarjeta física eSIM y administrar perfiles eSIM. Consta de dos partes: **Estado actual de la eSIM** y **Lista de perfiles eSIM**.

En el lado izquierdo del Panel de administración web, vaya a **APLICACIONES** > **Gestión de eSIM**.



## 12.7.1 Estado actual de la eSIM

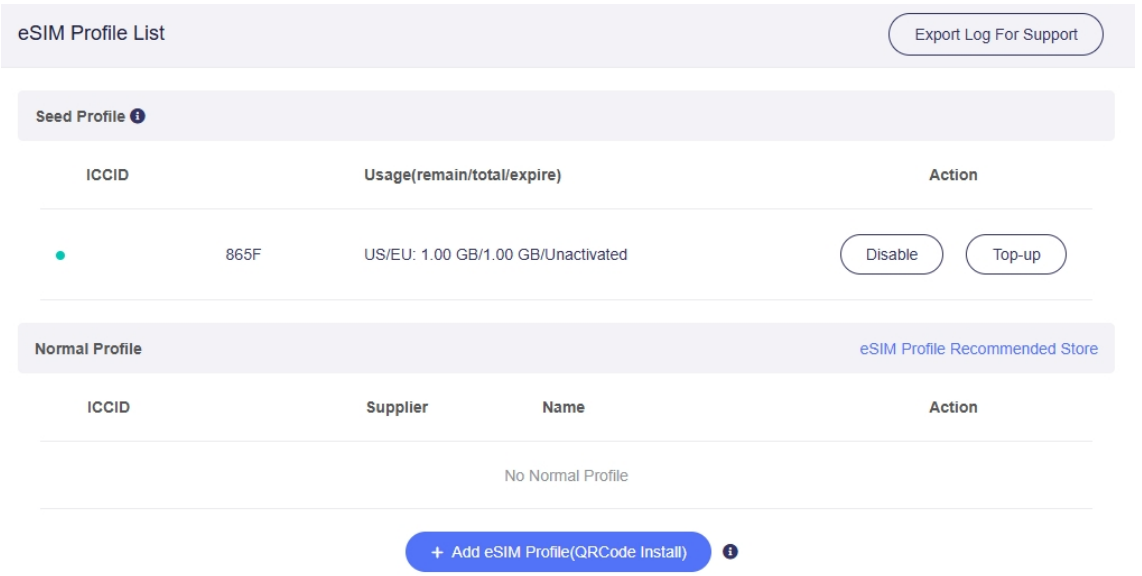
Esta sección muestra información básica y detalles sobre el perfil eSIM actualmente activo.




- **EID**: el identificador único global del eUICC (chip eSIM), utilizado para la identificación y la gestión de perfiles.
- **ICCID**: el identificador de tarjeta de circuito integrado del perfil eSIM actualmente activo.
- IMSI: la identidad del suscriptor móvil internacional del perfil eSIM actualmente activo.
- **Versión del sistema operativo eSIM**: la versión del sistema operativo de la eUICC, que define su compatibilidad y capacidades admitidas.
- **Almacenamiento eSIM (restante/total)**: Capacidad de almacenamiento total y disponible en la eUICC para almacenar perfiles eSIM.
- **Número de perfil eSIM**r: Número de perfiles eSIM almacenados actualmente en la eUICC. Tenga en cuenta que los perfiles eSIM ofrecidos por diferentes operadores varían en tamaño, por lo que la cantidad de perfiles que se pueden almacenar en la eUICC también será diferente.

## 12.7.2 Lista de perfiles eSIM

Esta sección muestra información sobre el perfil inicial eSIM y los perfiles normales.



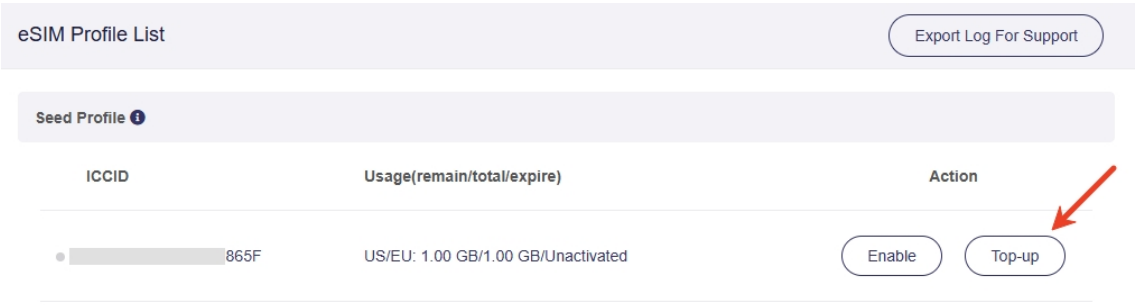

- **Perfil inicial**: el perfil inicial viene precargado con 1 GB de datos gratuitos para EE. UU. y Europa, además de 100 MB de datos globales, válidos por 1 año a partir de la fecha de activación. Estos datos le permiten descargar otros perfiles en cualquier parte del mundo. También puede controlar el uso del perfil semilla, incluidos los datos restantes, la asignación total de datos y la fecha de vencimiento.
- **Perfil normal**: si compra un perfil eSIM y lo carga mediante un código QR o un código de activación, el perfil se mostrará aquí.

## Recargar el perfil inicial

GL.iNet proporciona un perfil inicial precargado con 100 MB de datos globales y 1 GB de datos válidos en Europa y EE. UU. para la configuración inicial y la activación del perfil eSIM. Este plan está diseñado para descargar nuevos perfiles eSIM cuando llegas a un destino sin acceso a Internet.

Si has agotado los datos gratuitos precargados o si los datos gratuitos han caducado y deseas continuar usando el servicio, puedes recargar tu perfil semilla.

En la sección Perfil semilla, haz clic en **Botón de recarga** a la derecha.




En la ventana emergente, escanea el código QR y sigue las instrucciones para completar tu recarga.



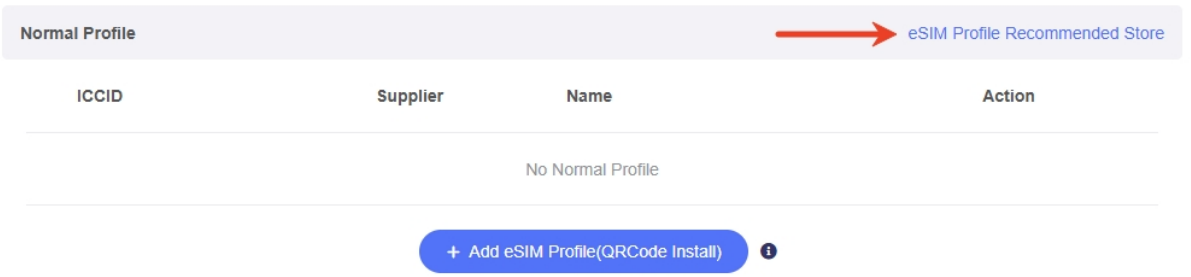

## Comprar perfil eSIM

Puedes comprar perfiles eSIM en nuestras tiendas recomendadas, tiendas probadas u otros proveedores de eSIM externos.

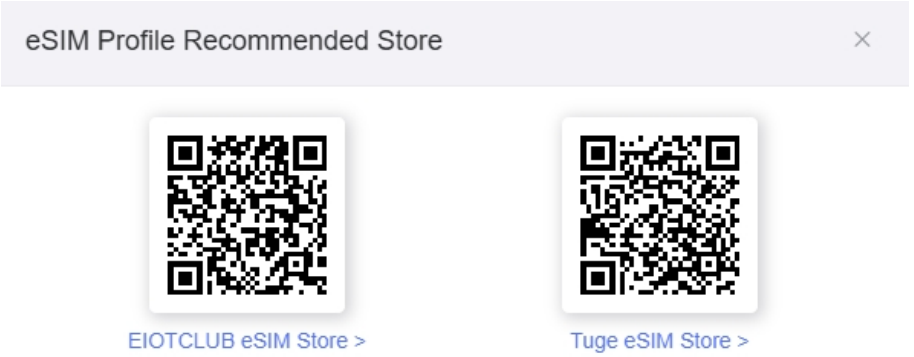
**Opción 1: comprar derom our rrecomendado stiendas.**

Hay dos tiendas recomendadas: Tienda eSIM EIOTCLUB y Tienda eSIM Tuge.

En la sección Perfil normal, haga clic en **Tienda recomendada de perfil eSIM** a la derecha.




Escanee el código QR o haga clic en los enlaces para comprar perfiles eSIM.




**Nota**: Todos los paquetes de perfiles eSIM comprados en estas dos tiendas son totalmente compatibles con los enrutadores GL.iNet. Si tiene alguna pregunta, comuníquese con nuestro equipo de soporte en support@gl-inet.com.

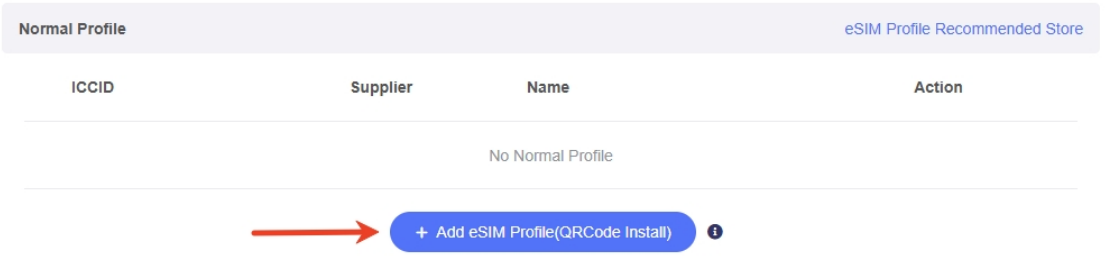
**Opción 2: comprar from testado stiendas.**
Consulte este enlace para ver una lista de tiendas probadas por GL.iNet.
**Nota**: No podemos garantizar la compatibilidad total con los enrutadores GL.iNet para todos los perfiles o paquetes de estas tiendas. Dado que GL.iNet no tiene asociaciones con ellos, no podemos brindar soporte posventa ni ayudar con los reembolsos.

**Opción 3: comprar dede other third-party eSIM providers.**
También puede optar por comprar perfiles eSIM de otros proveedores externos de su elección.
Sin embargo, no podemos garantizar la compatibilidad total con los enrutadores GL.iNet para perfiles eSIM comprados a otros proveedores externos. Compre a su propia discreción.
GL.iNet no es responsable de ningún problema de incompatibilidad.
Para soporte posventa o reembolsos, comuníquese con el proveedor de eSIM correspondiente.

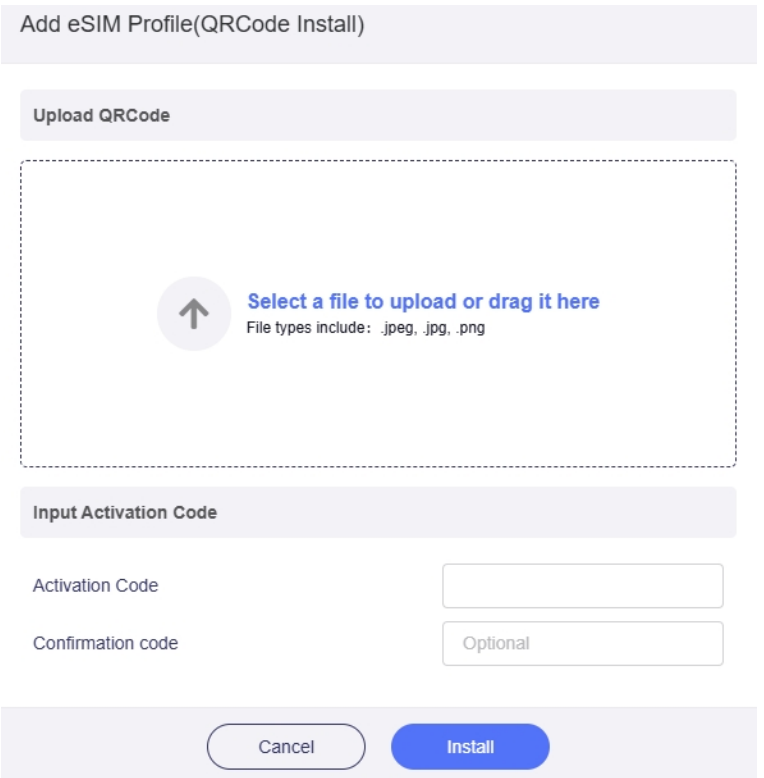
## Cargar perfil eSIM

Después de comprar un perfil eSIM, normalmente recibirá un código QR (o un código de activación). Guarde este código QR localmente y luego siga los pasos a continuación para cargar su perfil eSIM.

1. En la sección Perfil normal, haga clic en **Agregar perfil eSIM** en la parte inferior.




2. Cargue su código QR eSIM o ingrese el código de activación, luego haga clic en **Instalar**. Luego descargará e instalará el perfil eSIM en su enrutador.



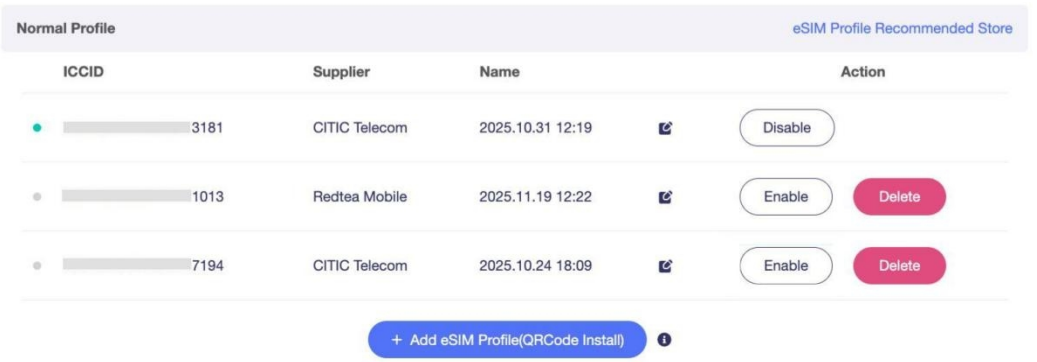

**Nota**:

1. La mayoría de los perfiles eSIM solo se pueden descargar e instalar una vez.
2. Un código QR con el formato correcto mostrará un código de activación que comienza con **LPA**:. However, some non-standard QR codes may only provide a raw activation code without the LPA prefix. In this case, manually add LPA: at the beginning of the code before clicking the Install button.

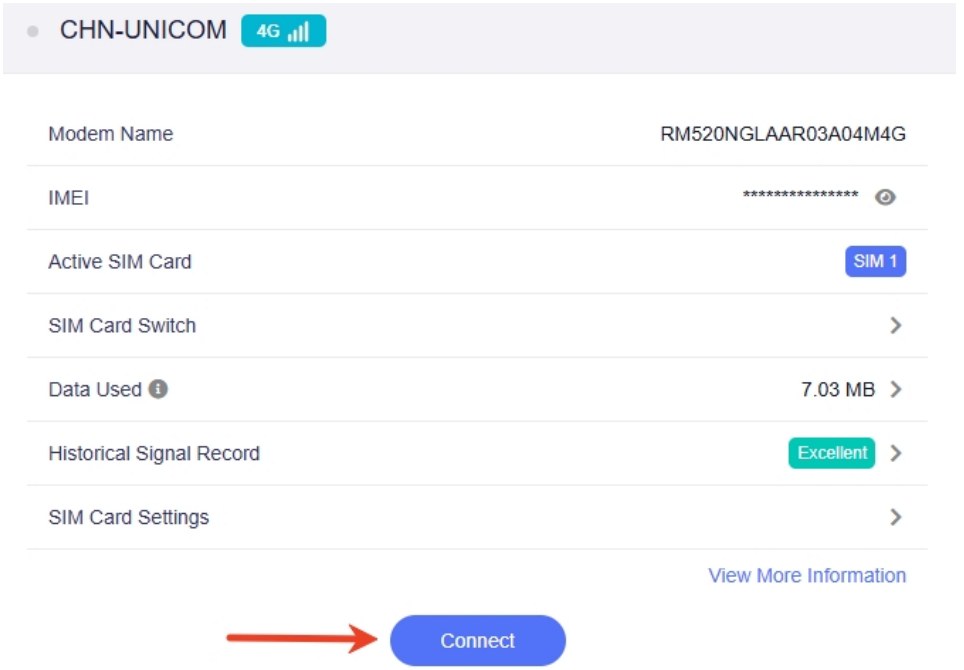



3. Si no ha comprado ningún perfil eSIM, puede comprar uno en la Tienda recomendada de perfiles eSIM. Consulta Comprar perfil eSIM para obtener más detalles.

3. Habilite su perfil eSIM.
   Después de la carga exitosa, su nuevo perfil eSIM aparecerá en la Lista de **Perfil normal**. Haga clic en **Activar** para activarlo.

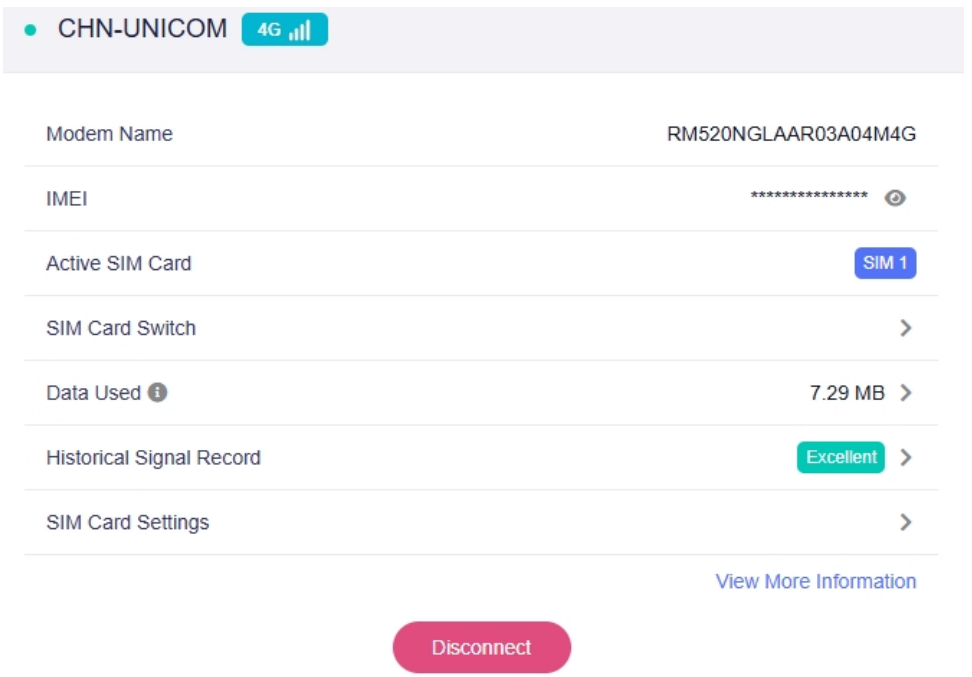



4. Conéctese a Internet.
   Después de habilitar su perfil eSIM, vaya a **INTERNET** > **Celular**. Haga clic en **Conectar** para establecer una conexión a Internet a través de su perfil eSIM.



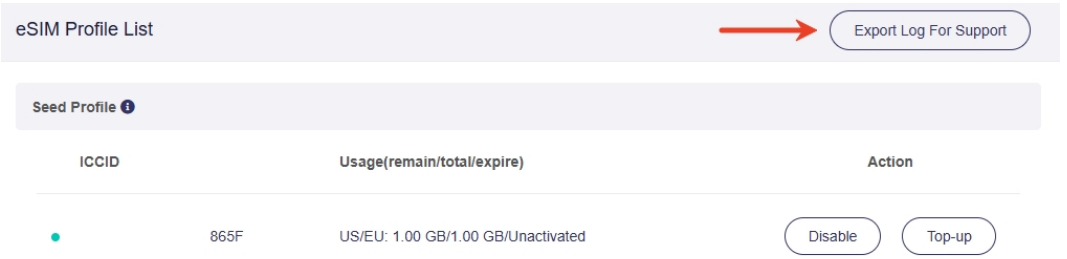

**Nota**: Algunos perfiles eSIM pueden requerir configuración adicional, como configuraciones de APN, PIN o TTL. Si es necesario, haga clic en **Configuración manual** o **Configuración de la tarjeta SIM** para ajustar estos parámetros. En algunos casos, es posible que deba reiniciar el dispositivo para establecer una conexión a Internet.

5. Una vez que el enrutador se conecta correctamente a través del perfil eSIM, la página se mostrará de la siguiente manera:



## Exportar registro para soporte

Haga clic en Exportar registro para soporte para ver todos los registros relacionados con eSIM. Si tiene algún problema y necesita soporte técnico, exporte los registros de eSIM y compártalos con nuestro equipo de soporte por correo electrónico en support@gl-inet.com.



Capítulo 13

# Red

Este capítulo presenta los ajustes relacionados con la red para la configuración y administración, como LAN, DNS e IPv6.

## 13.1 Reenvío de puertos

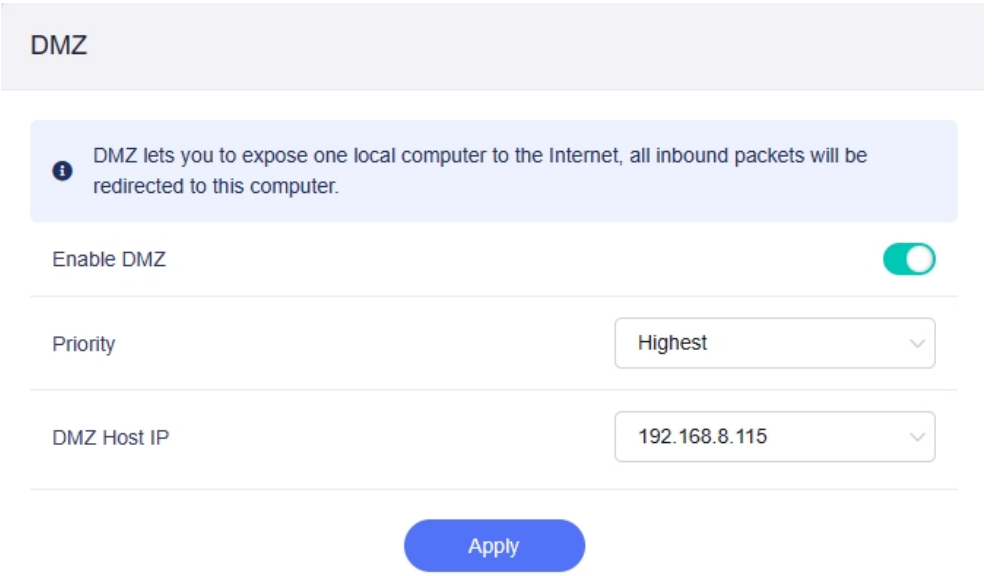
El reenvío de puertos es una función de red que enruta solicitudes externas a dispositivos específicos en su red local. La página de reenvío de puertos incluye dos funciones clave: **DMZ** (para acceso completo directo a un único dispositivo) y **Reenvío de puertos** (para acceso dirigido a puertos específicos de dispositivos).

### 13.1.1 DMZ

DMZ le permite exponer una computadora a Internet, por lo que todos los paquetes entrantes serán redirigidos a esta computadora.

Siga los pasos a continuación para habilitar DMZ si es necesario.

1. Inicie sesión en el panel de administración web de su enrutador y navegue a **RED** > **Reenvío de puertos** > **DMZ** sección.
2. Activar **Habilitar DMZ**. Sseleccione la Prioridad y la IP del host DMZ de la lista desplegable y haga clic en **Aplicar**.




- **Prioridad**: configúrelo como Más alto o Más bajo. Si la prioridad de la DMZ es mayor que las reglas de reenvío de puertos, todas las reglas de reenvío de puertos quedarán invalidadas. De lo contrario, las solicitudes se reenviarán al dispositivo cliente DMZ solo si el puerto al que se accede no tiene una regla de reenvío de puerto correspondiente.

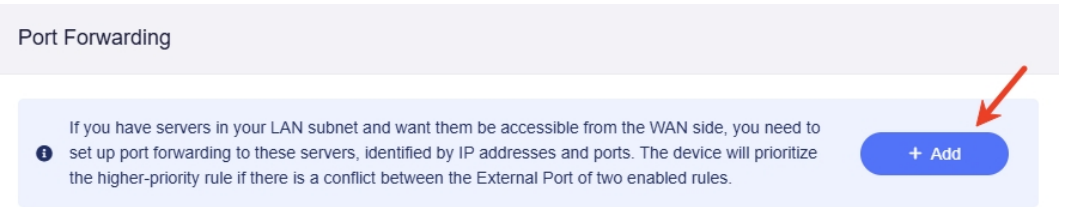
- **IP del host DMZ**: seleccione la dirección IP interna del el dispositivo que recibir todos los paquetes entrantes.

## 13.1.2 Reenvío de puertos

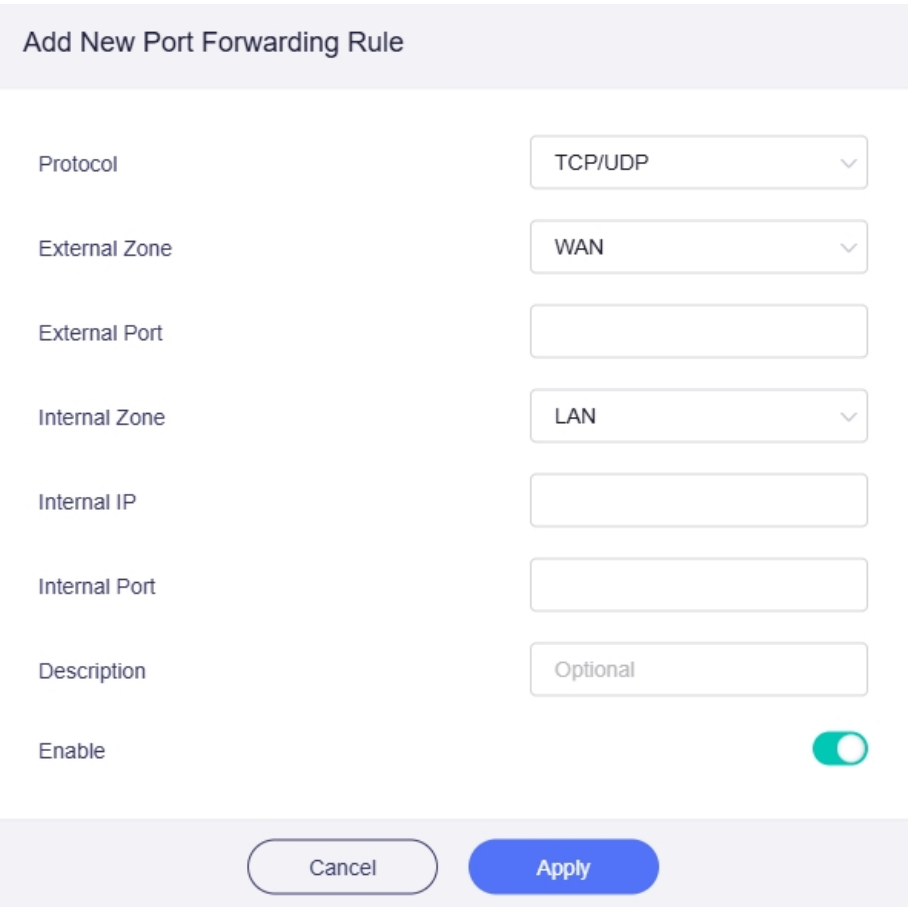
El reenvío de puertos permite que las computadoras remotas se conecten a una computadora o servidor local detrás del firewall de la LAN (por ejemplo, servidores web, servidores FTP).

Si necesita configurar el reenvío de puertos, siga los pasos a continuación.

1. Inicie sesión en el panel de administración web de su enrutador, vaya a **RED** > **Reenvío de puertos** > **Reenvío de puertos** sección y haga clic enhaga clic en **Agregar**.




2. En la ventana emergente, ingrese o seleccione los parámetros requeridos de la lista desplegable para agregar una regla de reenvío de puerto, luego haga clic en **Aplicar**.




- **Protocolo**: El protocolo utilizado. Puede elegir TCP, UDP o TCP y UDP.

- **Zona externa**: las opciones disponibles son WAN, Cliente WireGuard, Servidor WireGuard, Cliente OpenVPN, Servidor OpenVPN, LAN e Invitado.
- **Puerto externo**: El número de puertos externos. Introduzca aquí un número de puerto específico. El rango de puertos es 1–65535. Puede configurar un solo puerto o un rango de puertos concatenando el primer y el último número de puerto con un guión (por ejemplo, 501-510).
- **Zona interna**: las opciones disponibles son LAN, Invitado, Cliente WireGuard, Servidor WireGuard, Cliente OpenVPN, Servidor OpenVPN y WAN.
- **IP interna**: la dirección IP asignada por el enrutador al dispositivo que necesita acceso remoto. Si configura un solo puerto en Puerto externo, configure un solo puerto aquí. Si configura un rango de puertos en Puerto externo, configure el rango de puertos correspondiente aquí.
- **Puerto interno**: el número de puerto interno del dispositivo. Introduzca un número de puerto específico. Déjelo en blanco si coincide con el puerto externo.
- **Descripción**: establezca un nombre o agregue una descripción para la regla de reenvío de puerto (opcional).
- **Habilitar**: habilite o deshabilite esta regla.

## 13.2 Multi-WAN

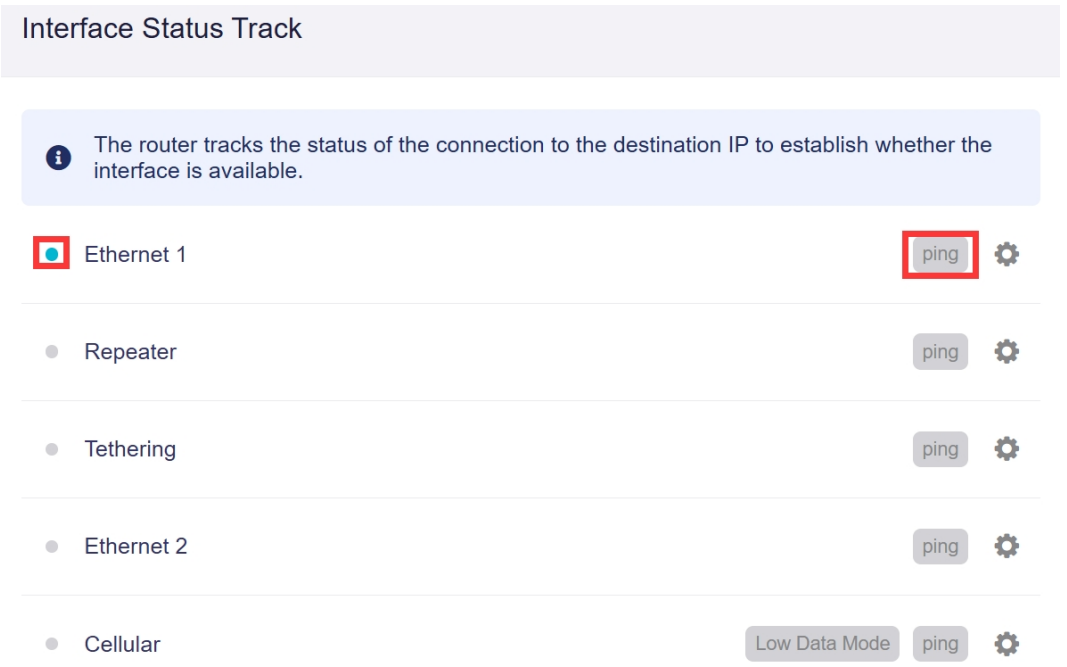
Multi-WAN permite el uso simultáneo de múltiples métodos de acceso a Internet, lo que permite la configuración de diversas opciones de conectividad en el enrutador. Ofrece dos modos de trabajo:

- **Conmutación por error**: cambia automáticamente a una conexión alternativa en poco tiempo si la conexión principal falla, lo que garantiza un acceso ininterrumpido a la red.
- **Equilibrio de carga**: distribuye el tráfico de red entre todas las conexiones disponibles en una proporción establecida para el uso simultáneo de múltiples conexiones, optimizando la utilización del ancho de banda.

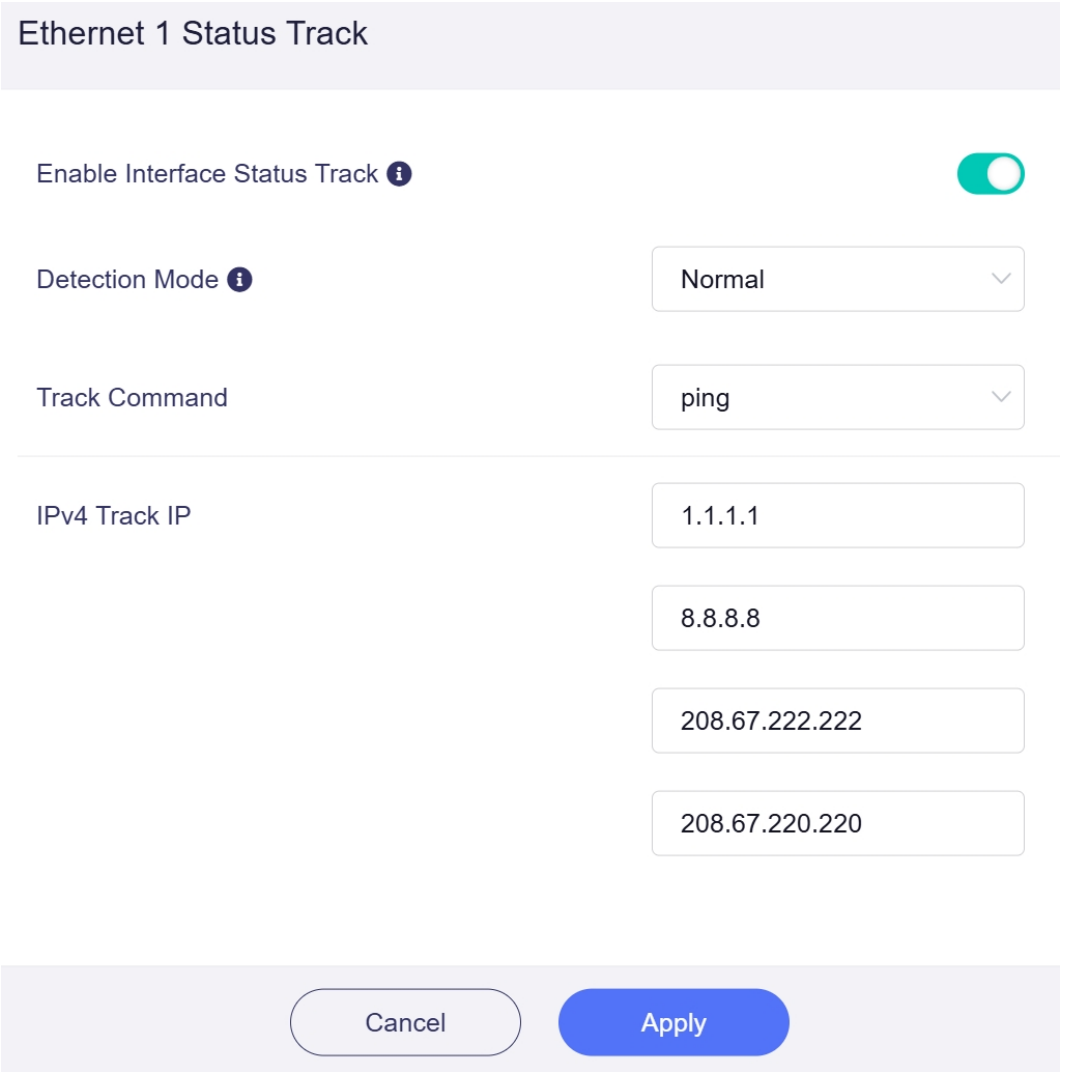
Inicie sesión en el panel de administración web de su enrutador' y navegue hasta **RED** > **Multi-WAN**. Esta página incluye dos secciones: Seguimiento del estado de la interfaz y modo Multi-WAN.

### 13.2.1 Seguimiento del estado de la interfaz

Los enrutadores GL.iNet utilizan el comando **ping** para monitorear el estado de la conexión a la IP de destino y determinar si la interfaz está disponible. Si la interfaz está disponible, se mostrará un punto verde a la izquierda; de lo contrario será gris.



En la sección **Seguimiento del estado de la interfaz**, Haga clic enhaga clic en el ícono de ajustes a la derecha para acceder a la configuración de seguimiento de estado para cada interfaz de red. A continuación se la configuración de seguimiento de estadoings para la interfaz Ethernet. La misma lógica de configuración se aplica a otras interfaces.

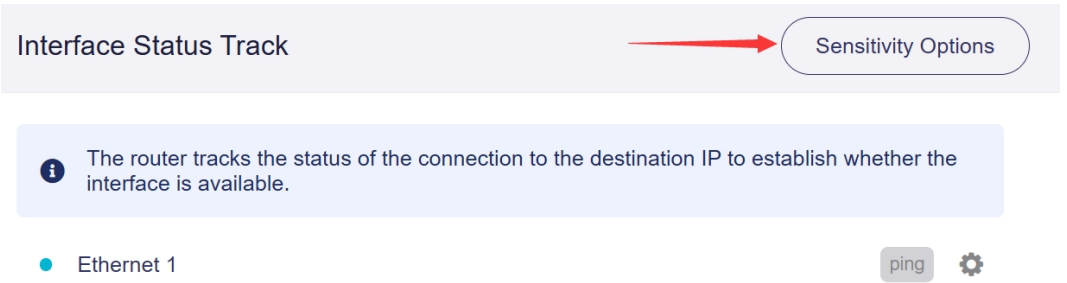



- **Habilitar seguimiento del estado de la interfaz**: Está habilitadode forma predeterminada. Si está deshabilitado, el enrutador determinará el estado de la interfaz según las condiciones (por ejemplo, si el cable Ethernet está enchufado).
- **Modo de detección**: esta característica se introdujo como modo de datos bajos en firmware v4.5, luego renombrado Modo de detección en firmware v4.7. Hay tres modos disponibles: Modo normal, Modo de datos bajos y Modo estricto.
    - **Normal Modo**: Es used de forma predeterminada.

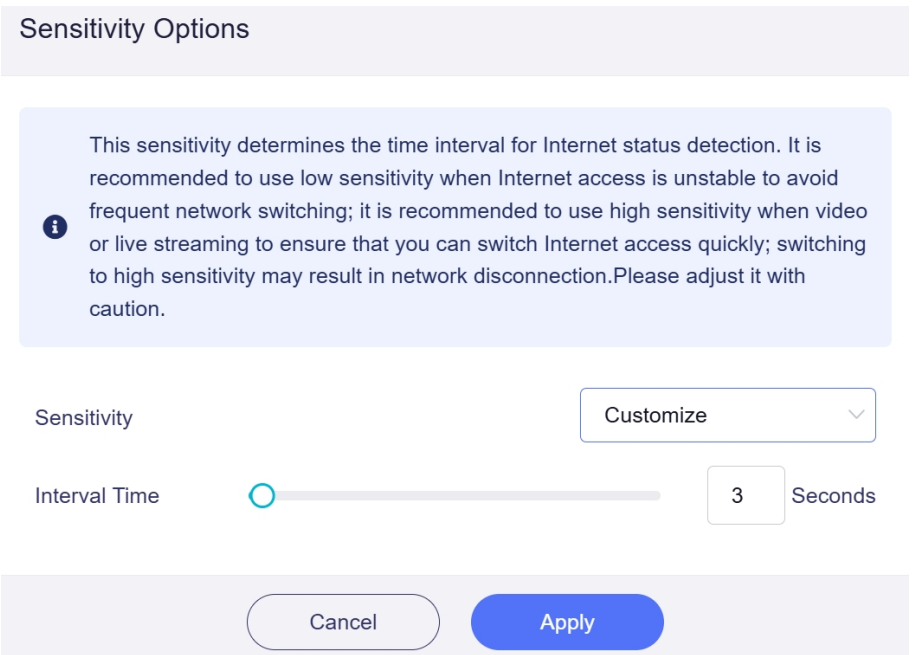
- **Datos bajos Modo**: Solo activa el seguimiento cuando se produce un error de red en la red interfaz. Utilice este modo si tiene un plan de datos limitado. Tenga en cuenta que la reconexión después de una desconexión puede ser un poco más lenta que en el modo normal y está habilitado de forma predeterminada solo para la interfaz celular.
- **Estricto Modo**: Determina el estado de la interfaz exclusivamente en función de los resultados de un comando de detección enviado a una IP pública.

- **Comando Track**: El comando ping se utiliza para monitorear el estado de la conexión a la IP de destino y verificar la disponibilidad de la interfaz.
- **IPv4 Track IP**: Cpersonalice las direcciones IP de seguimiento IPv4 si es necesario.

Haga clic en **Sensibilidad Opciones** en la esquina superior derecha.




Puedes establecer el intervalo de tiempo para la detección del estado de Internet en Bajo, Medio, Alto o personalizarlo. El tiempo de intervalo ajustable varía de 0,5 segundos a 90 segundos.



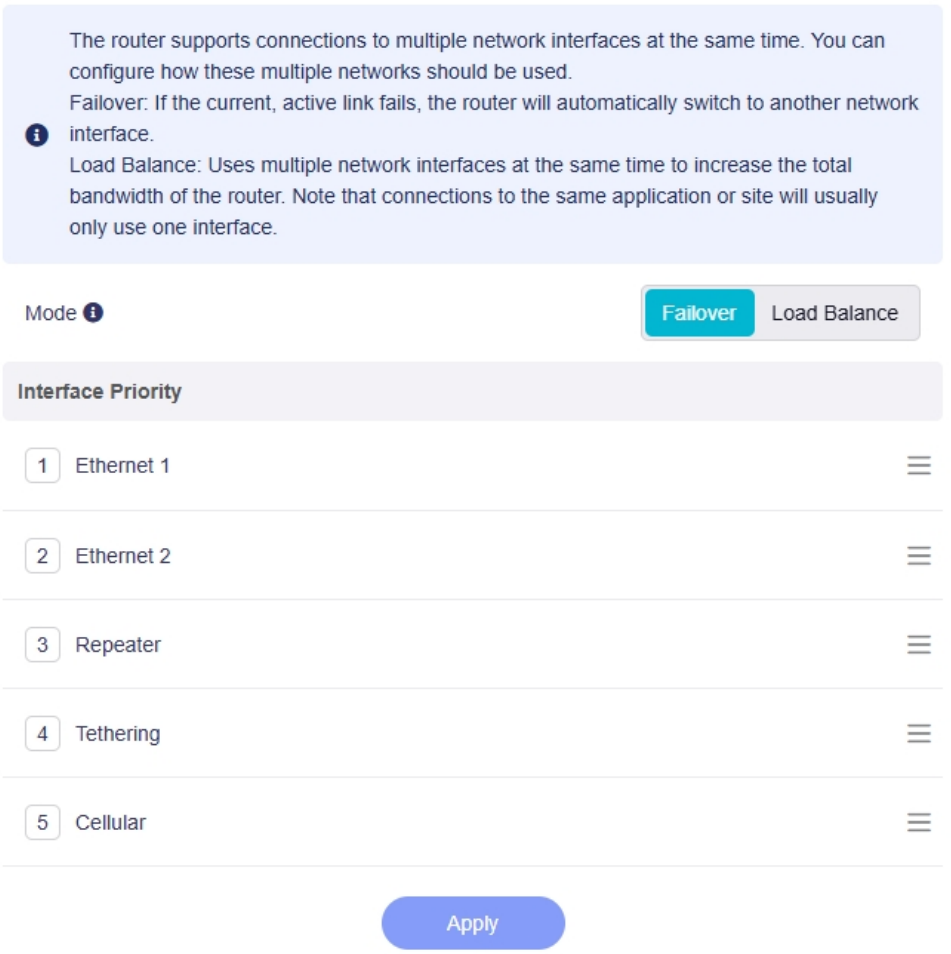
## 13.2.2 Modo Multi-WAN

Tdos hay disponibles dos modos para Multi-WAN: **Conmutación por error** y **Equilibrio de carga**. Tenga en cuenta que estos modos son mutuamente excluyentes.

## Conmutación por error

Conmutación por error es el modo predeterminado cuando se ejecutan múltiples Las conexiones están configuradas. Si el enlace activo falla, el enrutador cambiará automáticamente a otra interfaz de red para acceder a Internet.

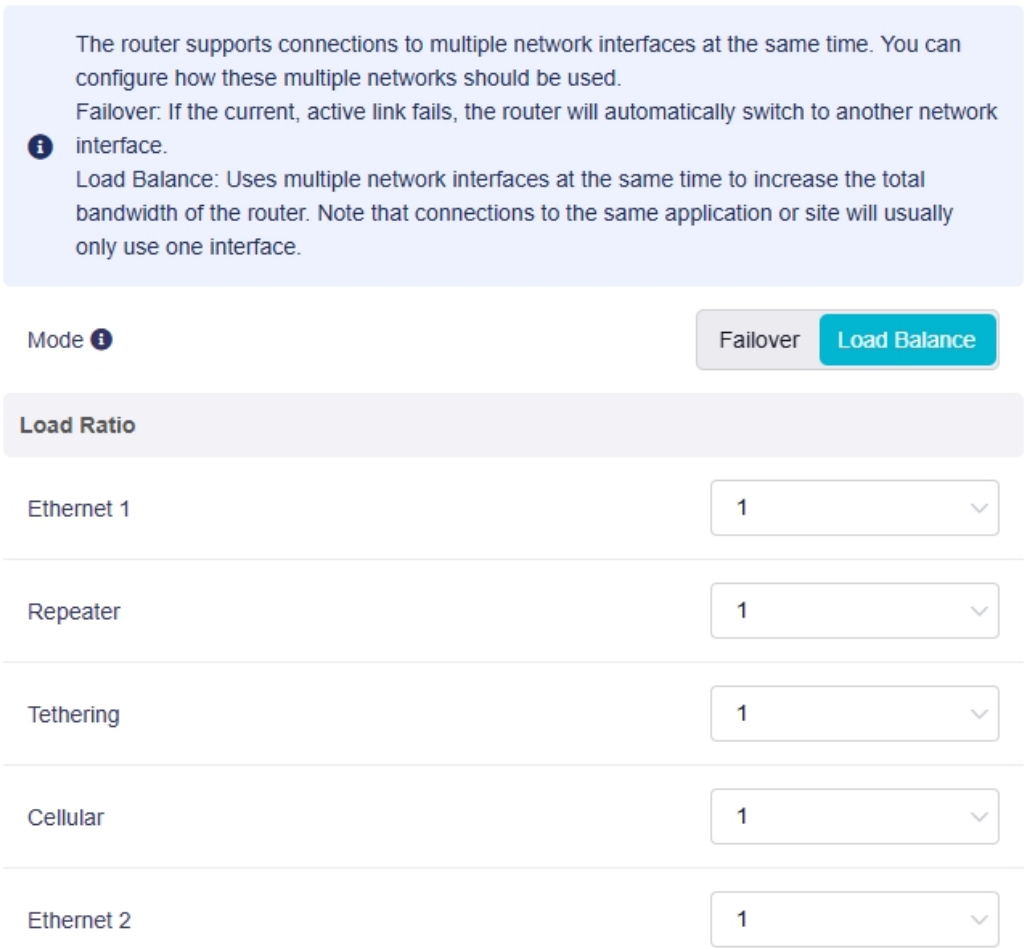
Puede establecer niveles de prioridad para cada interfaz: cuando la interfaz utilizada actualmente falla, el enrutador cambia a la siguiente interfaz disponible con la mayor prioridad. Una vez que se restablece una conexión de mayor prioridad, el enrutador volverá automáticamente a ella.



## Equilibrio de carga

El modo Equilibrio de carga utiliza múltiples interfaces de red simultáneamente para aumentar el ancho de banda total del enrutador, y el sistema distribuye nuevas conexiones entre las interfaces de acuerdo con una relación de carga configurada. Tenga en cuenta que las conexiones a la misma aplicación o sitio web normalmente utilizarán solo una interfaz.

La relación de carga se refiere a la proporción entre cada interfaz de red. El sistema asignará interfaces para manejar nuevas conexiones según esta proporción configurada. Por ejemplo, si el enrutador está conectado a cinco redes (por ejemplo, Ethernet 1, repetidor, anclaje a red, celular y Ethernet 2) simultáneamente y todas las interfaces están disponibles para acceso a Internet, habilitar el equilibrio de carga y establecer una relación 1:1:1:1:1 significa que las cinco interfaces compartirán el ancho de banda de la red por igual. El sistema distribuirá nuevas conexiones a través de estas interfaces de acuerdo con la relación de carga configurada.



También puede personalizar la relación de carga si es necesario. Por ejemplo, si Ethernet 1 tiene un ancho de banda de 100 Mbps, el Repetidor tiene 200 Mbps y no hay otras conexiones activas, establezca las relaciones de carga en 1 para Ethernet 1, 2 para el Repetidor y 0 para Anclaje a red, Celular y Ethernet 2. Luego, el sistema distribuirá nuevas conexiones a través de estas interfaces de acuerdo con la relación 1:2 configurada, lo que significa que Ethernet 1 manejará la mitad de conexiones que el Repetidor. A diferencia del modo de conmutación por error, este modo optimiza la eficiencia del rendimiento general al equilibrar la carga de tráfico en todas las interfaces disponibles.

**Nota**: No se garantiza que las conexiones o el tráfico existentes se alineen con la relación de carga. La distribución real se acercará gradualmente a la proporción configurada con un uso prolongado.

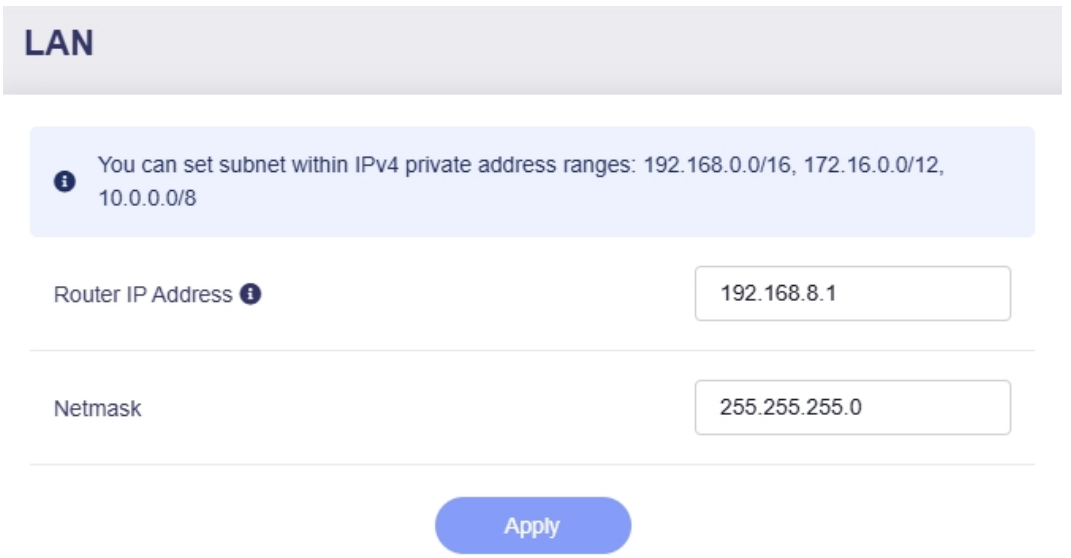
## 13.3 LAN

LAN (red de área local) se refiere a la red local privada a la que se conectan sus dispositivos mediante cables Ethernet.

Inicie sesión en el panel de administración web de su enrutador y navegue hasta **RED** > **LAN**. Aquí puede configurar los ajustes de LAN, incluidos los ajustes básicos, el servidor DHCP y la reserva de direcciones.

### 13.3.1 Configuración básica

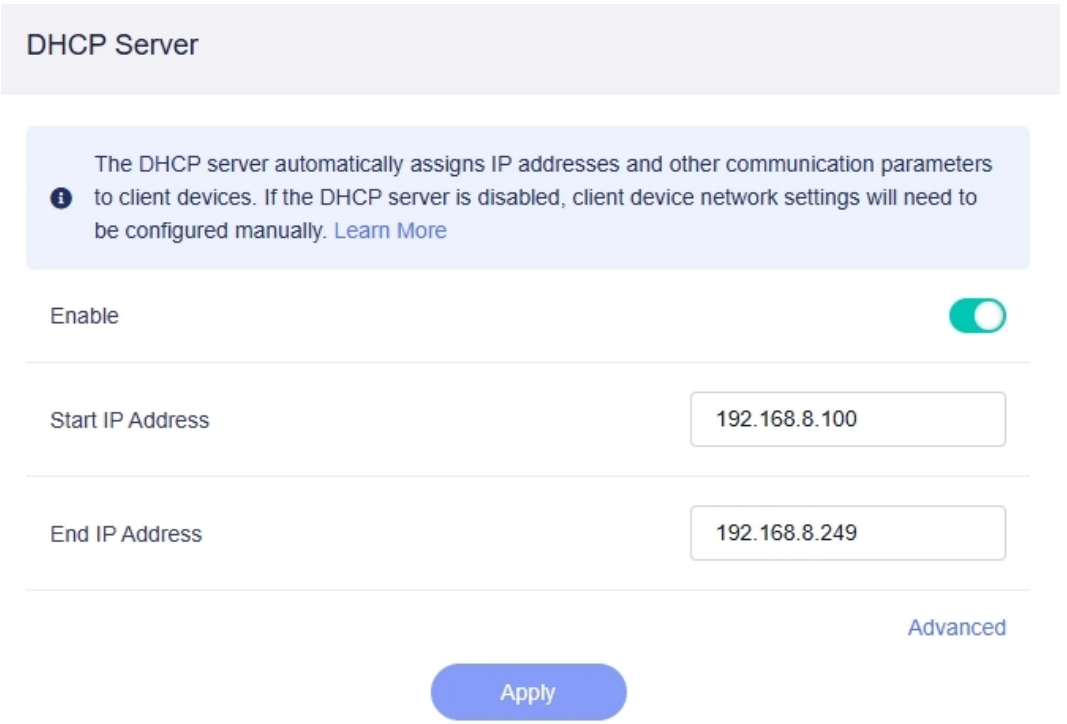
Los ajustes básicos incluyen la dirección IP del enrutador y Máscara de red. Puede configurar la subred dentro de rangos de direcciones privadas IPv4: 192.168.0.0/16, 172.16.0.0/12, 10.0.0.0/8



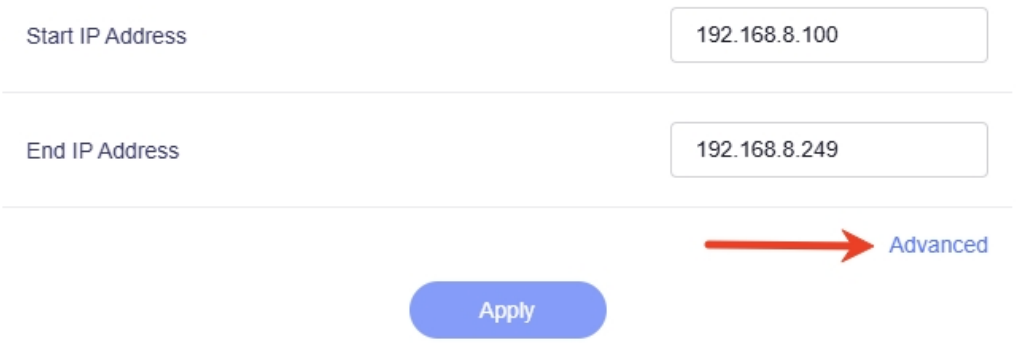

- **Dirección IP del enrutador**: esta es la dirección ingresada en la barra de direcciones de un navegador para acceder al panel de administración del enrutador. Es 192.168.8.1 de forma predeterminada y se puede cambiar si entra en conflicto con la red ascendente.'panel de administración. Es 192.168.8.1 de forma predeterminada y se puede cambiar si entra en conflicto con la red ascendente.
- **Máscara de red**: Hay dos opciones disponibles: 255.255.255.0 y 255.255.0.0.

## 13.3.2 Servidor DHCP

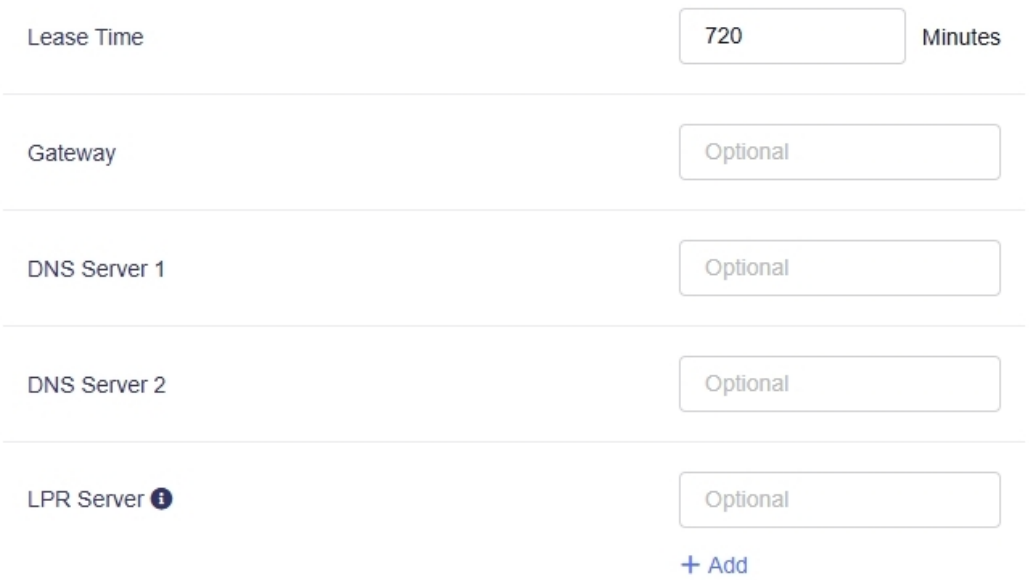
El servidor DHCP asigna automáticamente direcciones IP y otros parámetros de comunicación a cada cliente conectado. El servidor DHCP del enrutador GL.iNet'está habilitado de forma predeterminada y el servidor DHCP'va desde 192.168.8.100 a 192.168.8.249. Puede personalizar el rango de direcciones si es necesario.




Haga clic en **Avanzado** en la esquina inferior derecha.




Podrá configurar ajustes avanzados, incluidos el tiempo de arrendamiento, la puerta de enlace, los servidores DNS, y LPR Servidor.




- **Tiempo de concesión**: la duración durante la cual un dispositivo puede usar una dirección IP asignada a través de DHCP.
- **Puerta de enlace**: el componente del enrutador que enruta el tráfico entre local red y redes externas (por ejemplo, Internet).
- **Servidor DNS 1**: el servidor principal responsable de traducir nombres de dominio en direcciones IP.
- **Servidor DNS 2**: un servidor de respaldo utilizado para resolver nombres de dominio si el servidor DNS principal falla.
- **Servidor LPR**: (Servidor remoto de impresora de línea) Un servicio que administra trabajos de impresión y permite que los dispositivos en red envíen solicitudes de impresión a impresoras remotas. Múltiples LPR se pueden configurar puertos para impresoras.

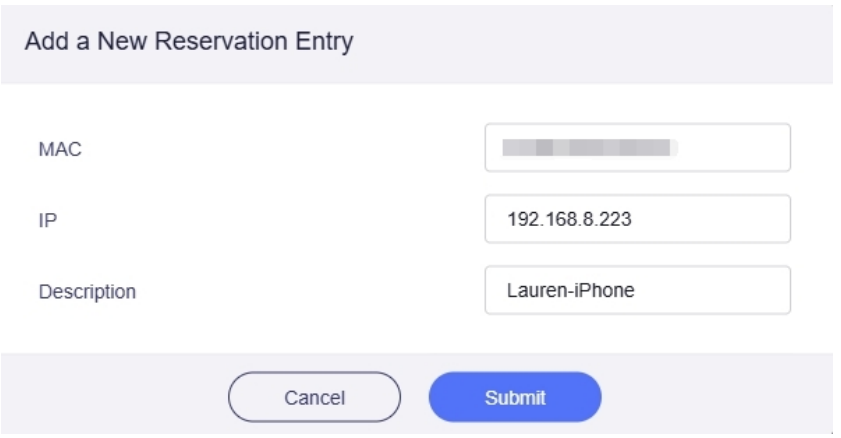
**Nota**: Si el servidor DHCP está deshabilitado, deberá configurar manualmente la IP estática y otros parámetros de comunicación para cada cliente. Consulte aquí para obtener más detalles.

## 13.3.3 Reserva de direcciones

La reserva de dirección le permite especificar una dirección IP fija para un cliente LAN, de modo que el cliente siempre reciba la misma dirección IP cada vez que acceda al servidor DHCP del enrutador. Puede asignar direcciones IP reservadas a computadoras o servidores que requieren una configuración de IP permanente. Tenga en cuenta que los clientes con la reserva de dirección configurada deben volver a conectarse al enrutador para activar la configuración.

Siga los pasos a continuación para configurar la reserva de dirección si es necesario.

1. Inicie sesión en el panel de administración web de su enrutador, navegue hasta **RED** > **LAN** > **Reserva de direcciones** y haga clic en **Agregar**.
2. En la ventana emergente, seleccione la dirección MAC de la lista desplegable; luego se mostrará la dirección IP correspondiente para la MAC seleccionada. autocompletado. Introduzca un nombre descriptivo y haga clic en **Enviar**.




3. Después de agregar una nueva reserva de dirección IP, la página mostrará la entrada reservada, como se muestra a continuación.



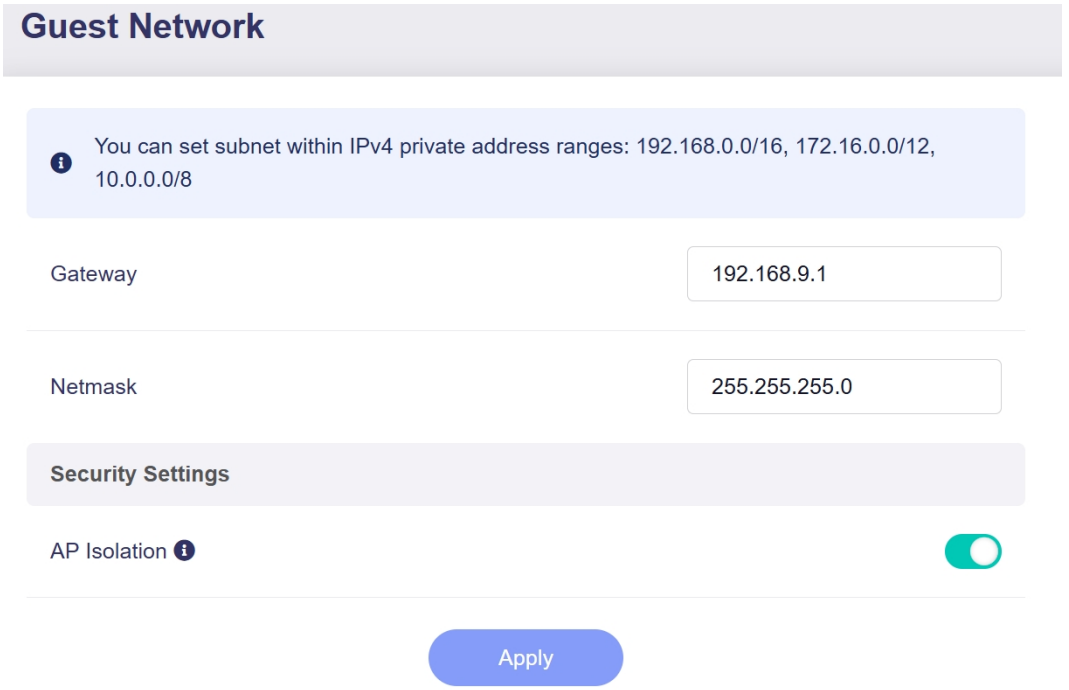
## 13.4 Red de invitados

Red de invitados se refiere a una red dedicada a la que los visitantes pueden conectarse, aislándolos de su LAN principal para proteger la seguridad de su red privada.

Inicie sesión en el panel de administración web de su enrutador y ir a **RED** > **Red de invitados**. Esta página le permite configurar los ajustes de la red de invitados, incluido configuración básica y servidor DHCP.

### 13.4.1 Configuración básica

La configuración básica incluye puerta de enlace, máscara de red, y Aislamiento AP.

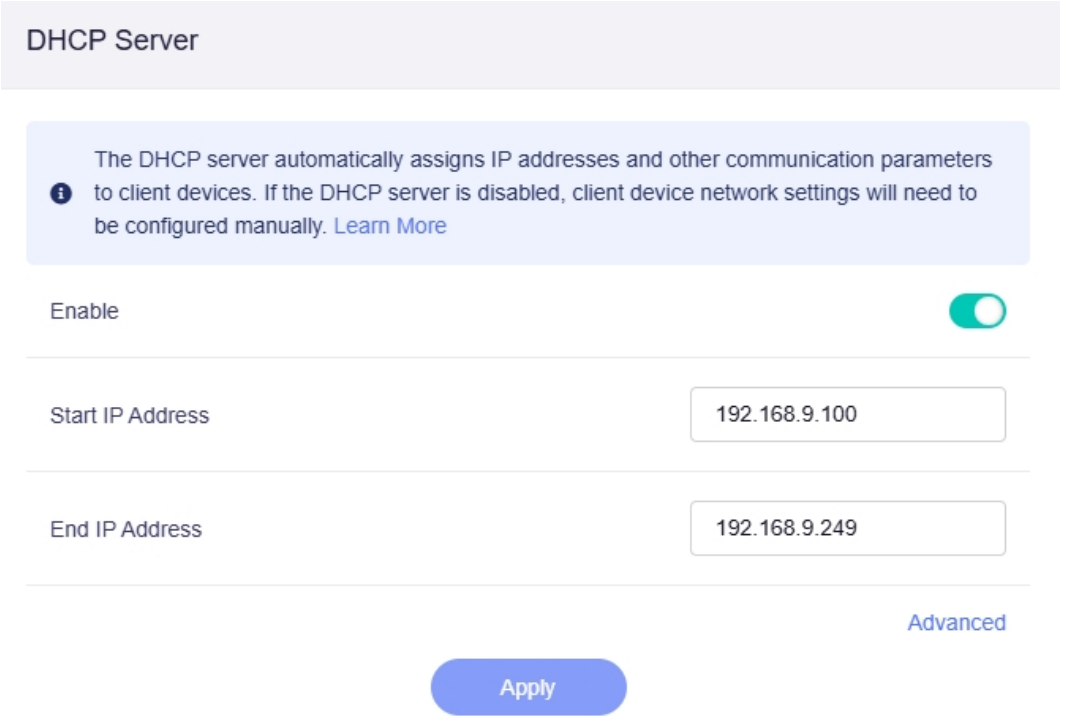



- **Puerta de enlace**: Es 192.168.9.1 de forma predeterminada y se puede cambiar si es necesario, pero no debe entrar en conflicto con la puerta de enlace de la red principal.
- **Máscara de red**: Hay dos opciones disponibles: 255.255.255.0 y 255.255.0.0.
- **Aislamiento AP**: se utiliza para aislar a los clientes de la red invitada en segmentos separados para que no puedan comunicarse con otros dispositivos en la misma red.

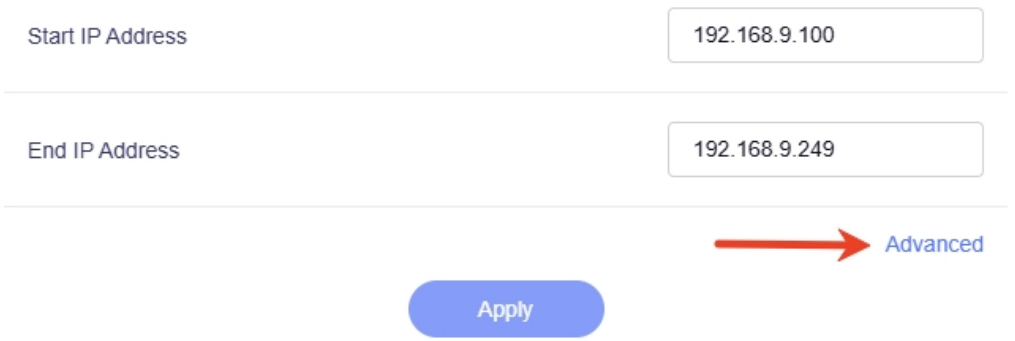
## 13.4.2 Servidor DHCP

Dado que la red de invitados está deshabilitada de forma predeterminada, su servidor DHCP está deshabilitado y oculto hasta que se habilita manualmente.

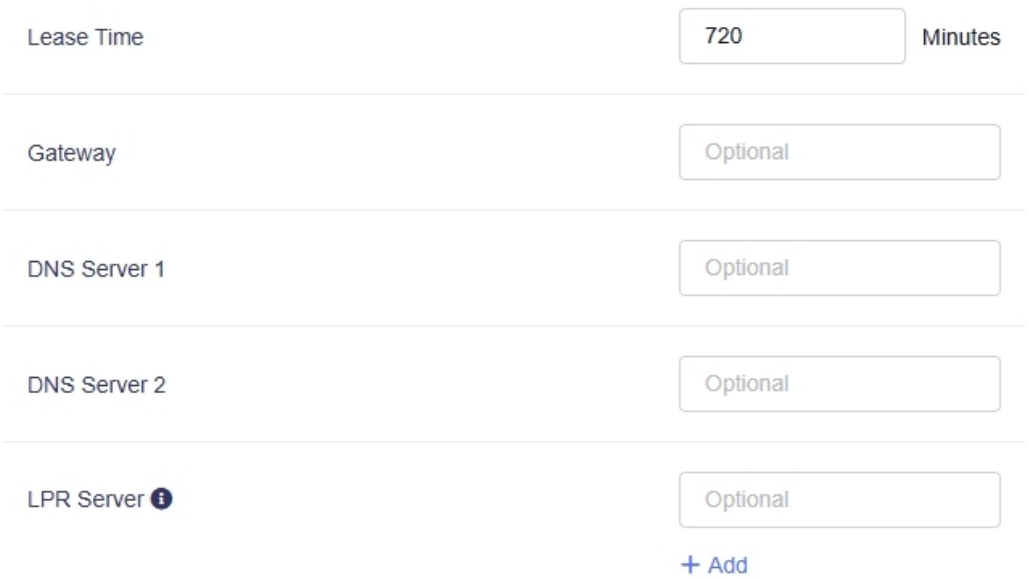
Cuando está habilitado, el servidor DHCP asigna automáticamente direcciones IP y otros parámetros de comunicación a cada cliente conectado. El grupo de direcciones IP del servidor DHCP para la red de invitados oscila entre 192.168.9.100 y 192.168.9.249. Puede personalizar el rango de direcciones si es necesario.




Haga clic en **Avanzado** en la esquina inferior derecha.




Podrá configurar ajustes avanzados, incluidos el tiempo de arrendamiento, la puerta de enlace, Servidores DNS, y servidor LPR.



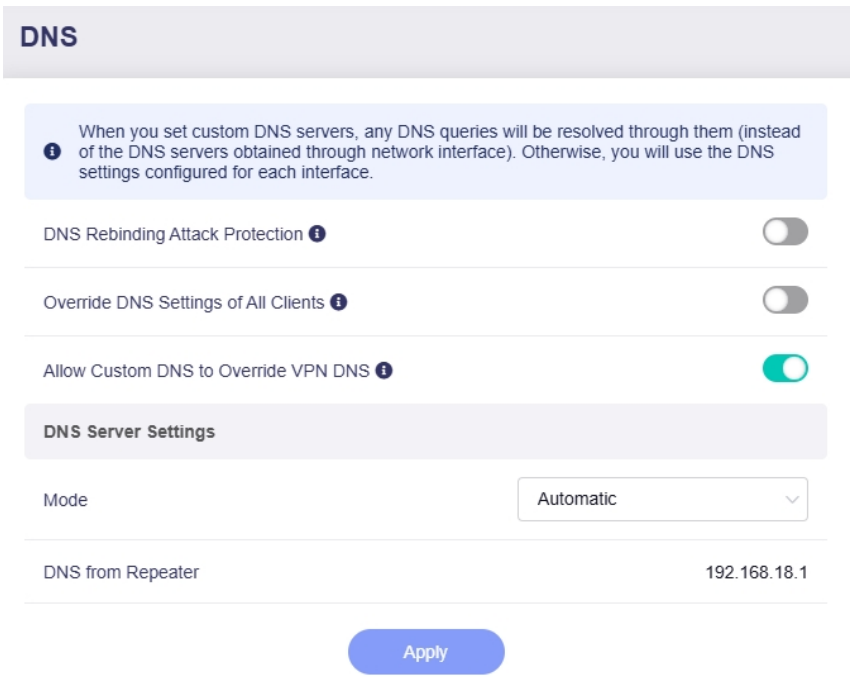

- **Tiempo de concesión**: el tiempo durante el cual un dispositivo puede usar una dirección IP asignada a través el DHCP de la red de invitados.
- **Puerta de enlace**: el componente del enrutador que enruta el tráfico entre la gred de invitados y las redes externas (por ejemplo, Internet).
- **Servidor DNS 1**: el servidor principal responsable de traducir los nombres de dominio en direcciones IP.
- **Servidor DNS 2**: un servidor de respaldo utilizado para resolver nombres de dominio si el servidor DNS primario falla.
- **Servidor LPR**: (Servidor remoto de impresora de línea) Un servicio que administra trabajos de impresión y permite que los dispositivos en red envíen solicitudes de impresión a impresoras remotas. Se pueden configurar varios puertos LPR para impresoras.

## 13.5 DNS

DNS (Sistema de nombres de dominio) es un servicio de red que traduce nombres de dominio legibles por humanos (p. ej., www.google.com) en direcciones IP reconocibles por máquinas (p. ej., 142.250.185.142), lo que permite que los dispositivos se conecten a sitios web o servicios de destino.

El servidor DNS del enrutador se refiere al servicio DNS integrado en el enrutador, que proporciona traducción de nombre de dominio a IP para todos los dispositivos conectados. Por lo general, funciona de dos maneras: primero, obtiene automáticamente direcciones DNS de la red ascendente para proporcionar servicios de traducción predeterminados; en segundo lugar, los usuarios pueden configurar manualmente direcciones DNS públicas personalizadas (por ejemplo, 8.8.8.8) en el panel de administración web del enrutador' para optimizar el acceso a la red o mejorar la seguridad. Una vez configurados, todos los dispositivos conectados utilizarán este servidor DNS unificado de forma predeterminada, lo que elimina la necesidad de configurar DNS por separado en cada dispositivo.

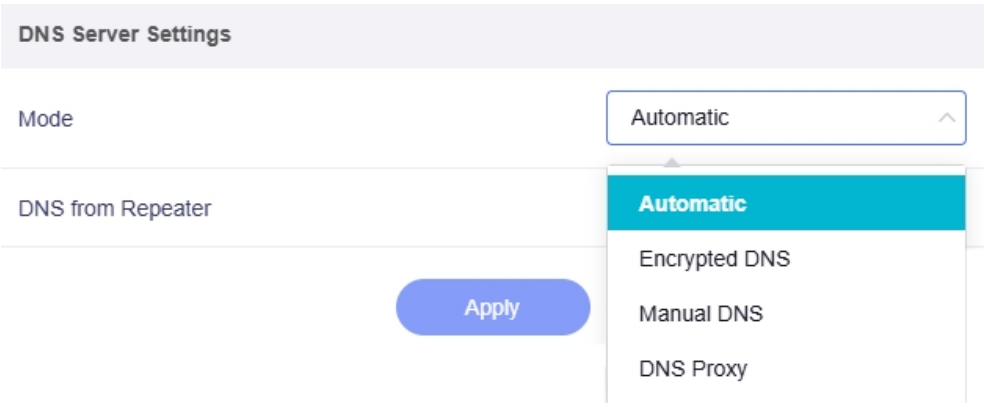
Inicie sesión en el panel de administración web de su enrutador y navegue hasta **RED** > **DNS**. Esta página le permite configurar ajustes relacionados con DNS, incluidas opciones de seguridad, modos de servidor y reglas de prioridad de DNS para diferentes escenarios de red.



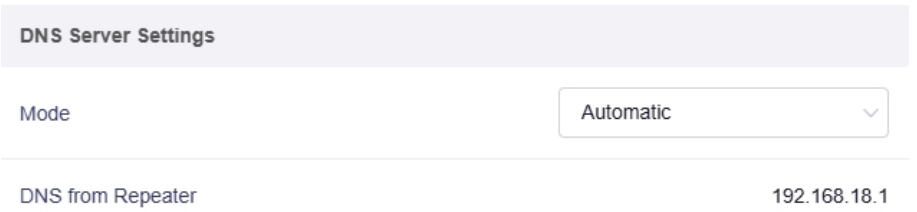
- **Protección contra ataques de revinculación de DNS**: protege contra ataques de revinculación de DNS bloqueando intentos maliciosos de resolución de DNS. Tenga en cuenta que habilitarlo puede causar fallas en la búsqueda de DNS privado; deshabilítelo si su red utiliza un portal cautivo (por ejemplo, páginas de inicio de sesión Wi-Fi públicas).
- **Anular la configuración DNS de todos los clientes**: Si está habilitado, todos los dispositivoss se verá obligado a utilizar los servidores DNS configurados en el enrutador, ignorando sus propias configuraciones DNS originales. Permite la configuración de DNS unificada para todos los dispositivos.
- **Permitir que DNS personalizado anule el DNS de VPN**: Cuando está habilitado, si ha configurado DNS personalizado, los paquetes transmitidos a través del túnel VPN utilizarán el DNS personalizado para la resolución, en lugar de los servidores DNS de la conexión VPN. Esto garantiza que sus reglas de resolución de DNS personalizadas se apliquen normalmente al utilizar VPN.

## 13.5.1 Configuración del servidor DNS

Hay cuatro modos para el servidor DNS: Automático, DNS cifrado, DNS manual y Proxy DNS.

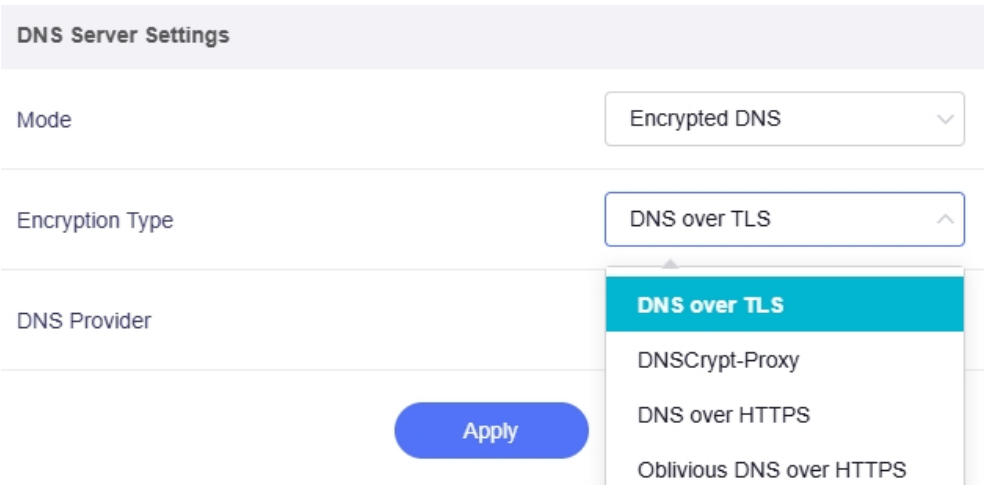



1. **Automático**: cuando se selecciona, el enrutador obtendrá automáticamente las direcciones del servidor DNS de la red ascendente y las aplicará a todos los dispositivos conectados.



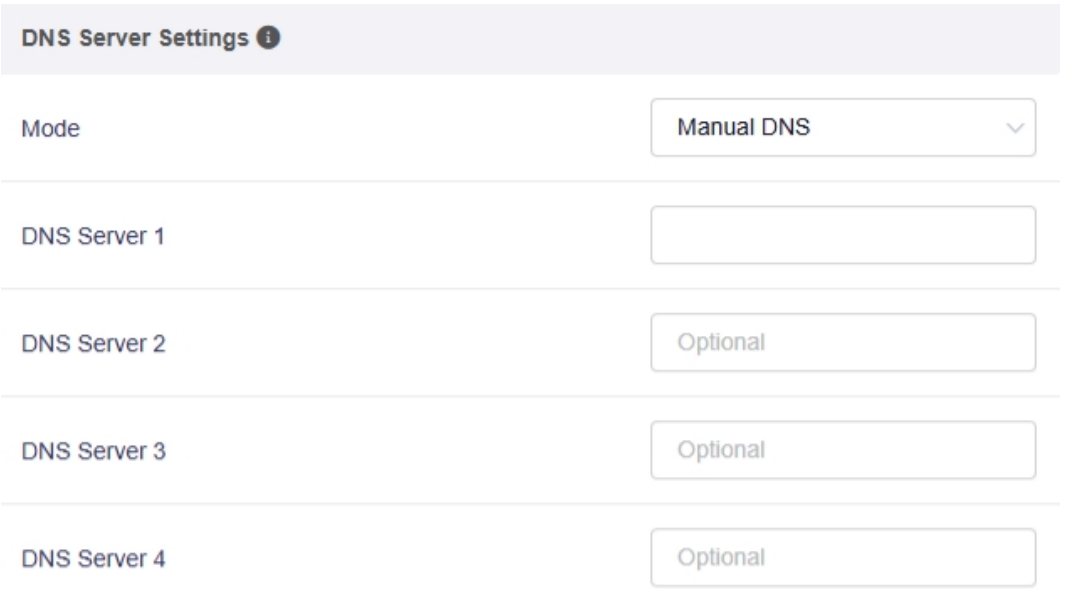

2. **Cifrado DNS**: cuando se selecciona, el enrutador utilizará protocolos cifrados para procesar consultas de DNS, protegiendo los datos de resolución contra escuchas o alteraciones.

   Tiene cuatro tipos de cifrado: DNS sobre TLS, DNSCrypt-Proxy, DNS sobre HTTPS y DNS ajeno a través de HTTPS.



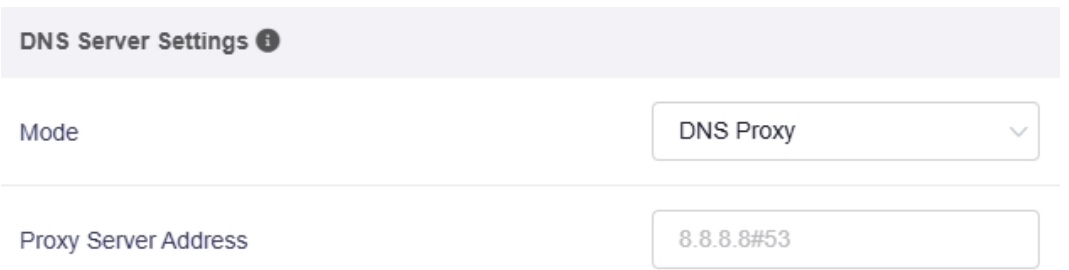
- Para DNS sobre TLS, seleccione un proveedor de DNS entre Control D, NextDNS y Cloudflare.
- Para los otros tres (es decir, DNSCrypt-Proxy, DNS sobre HTTPS y DNS ajeno a HTTPS), seleccione al menos un servidor DNS del repositorio. Se pueden seleccionar hasta 8 servidores. Cuando se seleccionan varios servidores, el enrutador utilizará el más rápido automáticamente.

3. **DNS manual**: cuando se selecciona, puede personalizar los servidores DNS de su enrutador. Haga clic en Servidor DNS 1 y elija un servidor DNS de la lista desplegable. Los campos DNS restantes se actualizarán automáticamente.




**Nota**: si necesita utilizar direcciones IPv6 para DNS manual, habilite IPv6 en su enrutador primero.

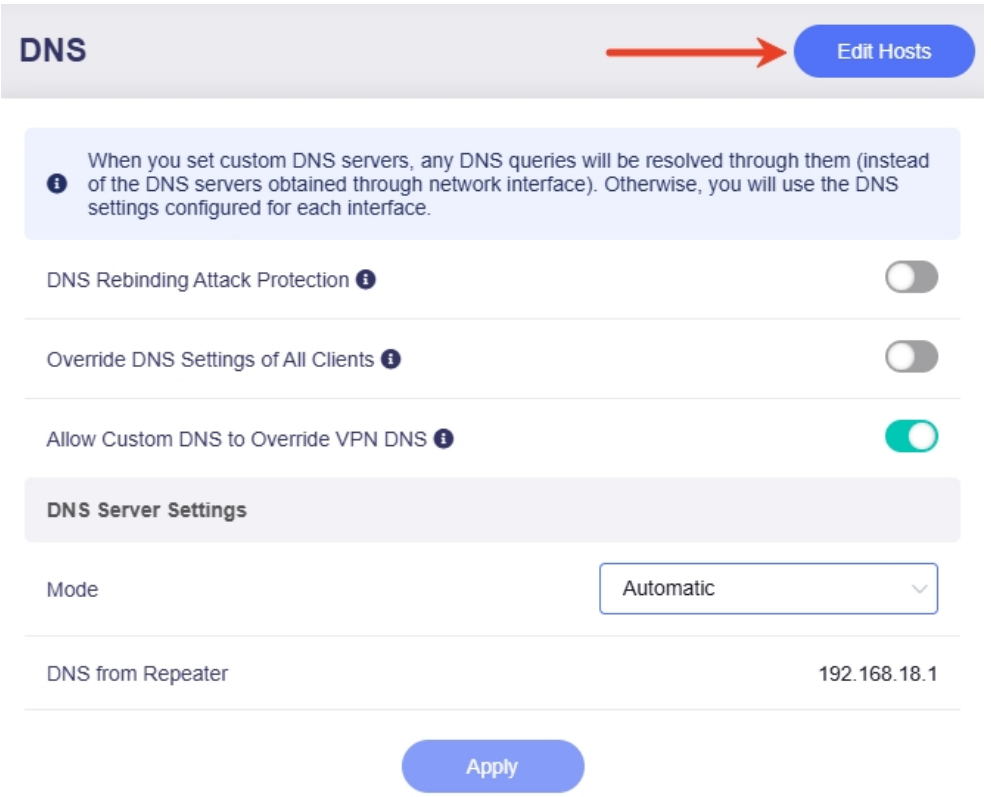
4. **Proxy DNS**: cuando se selecciona, el enrutador reenvía todas las consultas DNS a través de un servidor proxy, permiteresolución a través de el entorno de red del proxy para necesidades de acceso específicas.



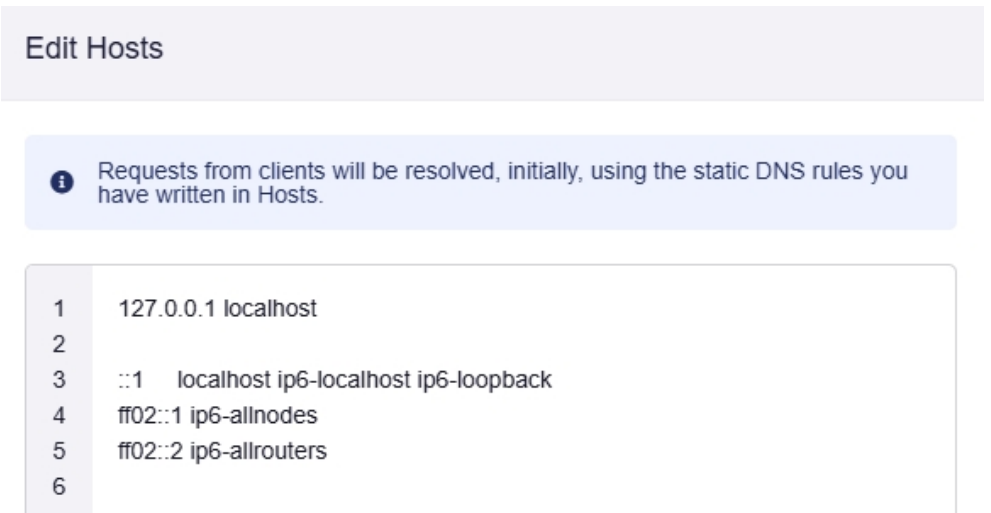
## 13.5.2 Editar hosts

Puede definir reglas de resolución de DNS estáticas si es necesario.

En la página DNS, haga clic en **Editar hosts** en la esquina superior derecha.



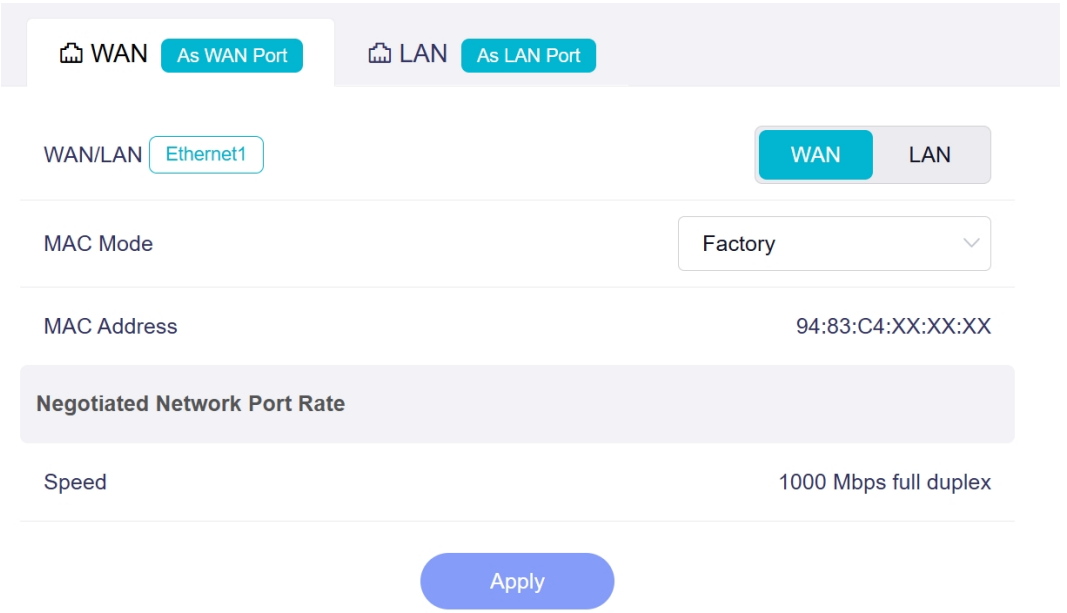

Las solicitudes de los clientes se resolverán preferentemente utilizando las reglas DNS estáticas escritas aquí, lo que le permitirá asignar manualmente direcciones IP a nombres de host (por ejemplo, las entradas predeterminadas como 127.0.0.1 localhost para loopback local) para un control personalizado de la resolución de nombres de dominio.



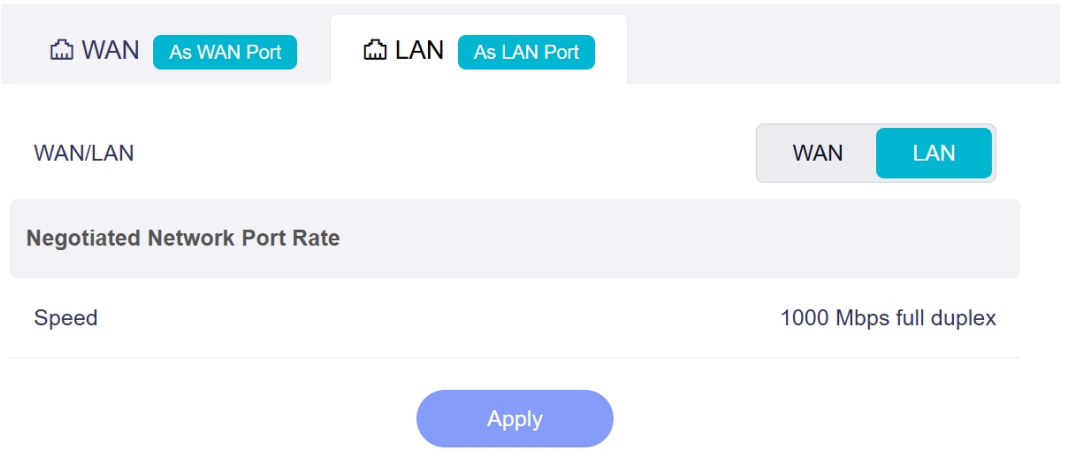
## 13.6 Gestión de puertos

Inicie sesión en el panel de administración web de su enrutador' y navegue hasta **RED** > **Gestión de puertos**. Esta página le permite administrar los puertos Ethernet del enrutador'sección.

La sección **WAN** muestra la función del puerto (WAN o LAN), la dirección MAC y la velocidad negociada.




El **LAN** le permite cambiar de LAN a WAN. Puede cambiar la función del puerto y verificar la tarifa negociada aquí.



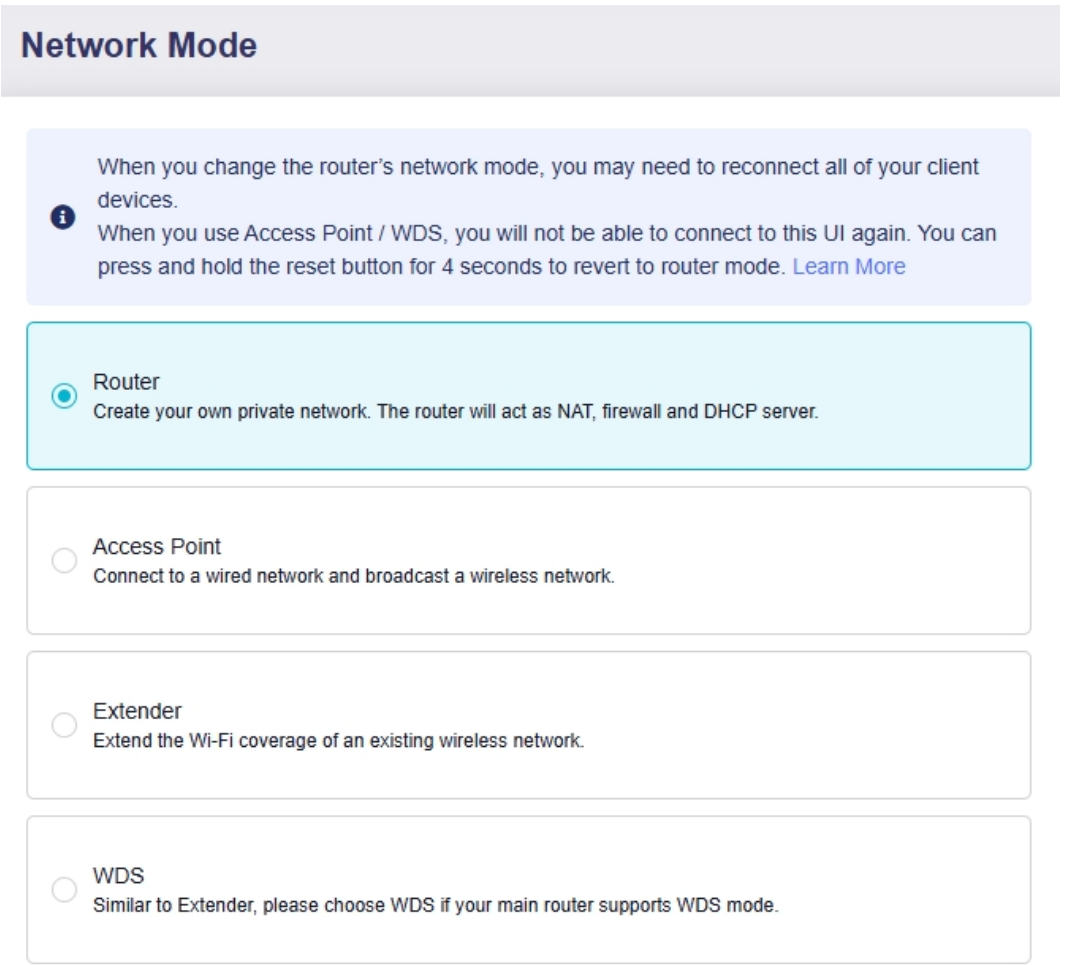

**Nota**: La tarifa negociada para el puerto WAN y LAN se muestra solo cuando hay un cable Ethernet

conectado. Depende tanto del puerto Ethernet como del cable Ethernet.

## 13.7 Modo de red

El modo de red se refiere a los diferentes roles y funciones operativas que un enrutador puede asumir para satisfacer diversas necesidades de implementación de red.

Inicie sesión en el panel de administración web de su enrutador' y navegue hasta **RED** > **Modo de red**. Puede cambiar el modo de red de su enrutador.




- **Enrutador**: este es el modo operativo predeterminado para la mayoría de los enrutadores domésticos y de pequeñas oficinas, diseñado para crear una red de área local (LAN) privada y actuar como una puerta de enlace dedicada entre la Internet pública y los dispositivos conectados. En este modo, el enrutador habilita funciones principales que incluyen NAT, DHCP y un firewall integrado. Se conecta a una línea ascendente, como fibra de banda ancha, asigna automáticamente direcciones IP privadas a los dispositivos conectados y proporciona seguridad de red para toda la red privada.

- **Punto de acceso**: este modo permite que un enrutador se conecte a una red cableada a través de un cable LAN y transmita señales inalámbricas, ampliando la cobertura de Wi-Fi en espacios grandes para permitir que más dispositivos accedan a la red. En este modo, el enrutador desactiva sus funciones NAT y DHCP, funcionando exclusivamente como un transmisor y conmutador de señal inalámbrica en lugar de una puerta de enlace independiente.
- **Extensor**: este modo está diseñado para ampliar la cobertura Wi-Fi de una red inalámbrica existente y eliminar zonas muertas de señal en áreas con mala conectividad. Permite que el enrutador reciba señales del enrutador principal de forma inalámbrica, las amplifique y retransmita la señal potenciada. A diferencia del modo Punto de acceso, no requiere conexión por cable al enrutador principal, pero puede reducir el ancho de banda a la mitad, ya que el dispositivo tiene que manejar la recepción y transmisión de señales simultáneas.
- **WDS**: el modo Sistema de distribución inalámbrica (WDS) es similar al modo Extensor, ya que extiende la cobertura Wi-Fi de forma inalámbrica, pero admite puentes inalámbricos entre múltiples enrutadores compatibles. Se recomienda para la expansión de la red inalámbrica cuando el enrutador ascendente tiene funcionalidad WDS.
  Este modo es ideal para escenarios como cubrir edificios de varios pisos o campus de oficinas pequeñas donde varios enrutadores necesitan trabajar juntos para formar una red inalámbrica unificada. A diferencia del modo Extensor, que solo transmite señales desde un enrutador principal a un único extensor, el modo WDS permite que los enrutadores interconectados envíen y reciban señales, lo que permite una cobertura perfecta en áreas más grandes con múltiples nodos de señal.

**Nota**:

1. Cuando se cambia el modo de red, todos los dispositivos cliente se volverán a conectar al enrutador para una conectividad de red estable.
2. **En el modo Punto de acceso/WDS, no podrá acceder al panel de administración web utilizando la dirección IP original**. En su lugar, debe iniciar sesión en el enrutador ascendente para encontrar la dirección IP que ha asignado a este enrutador y luego usar esta dirección IP para acceder al panel de administración web. Si no tiene acceso al enrutador ascendente, presione y mantenga presionado el botón de reinicio durante 4 segundos para revertirlo al modo de enrutador predeterminado.

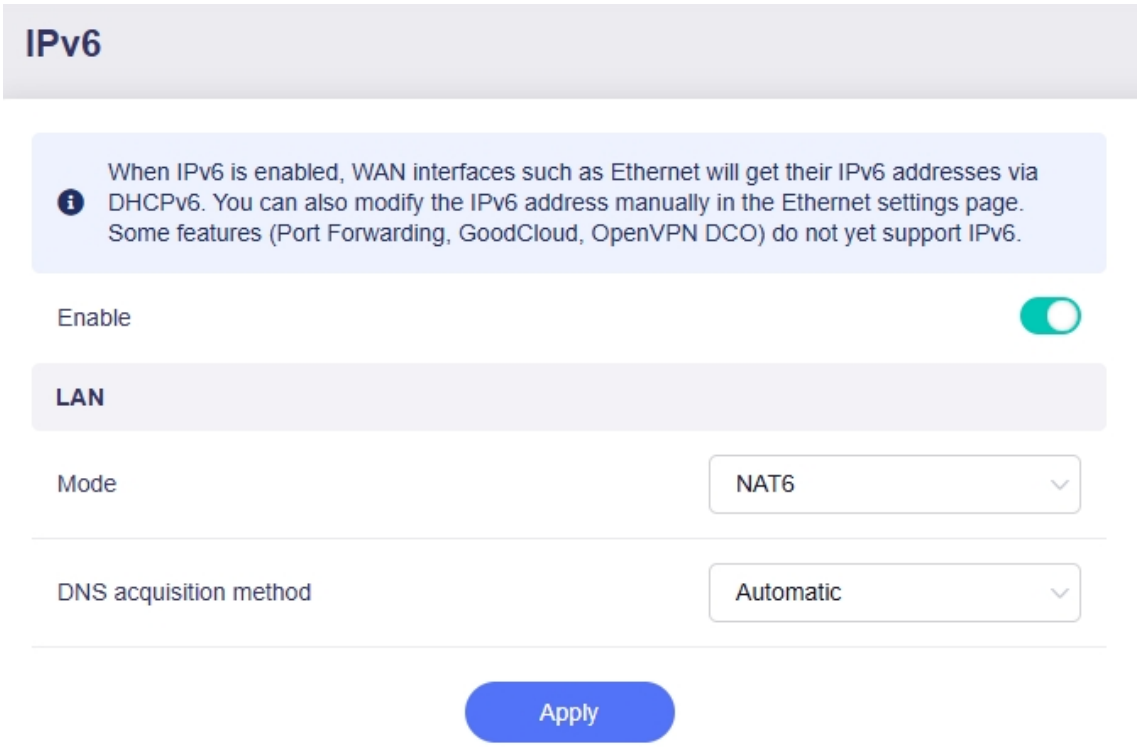
3. **En el modo Punto de acceso/Extensor/WDS, las siguientes funciones no estarán disponibles**: Control de acceso (lista de permitidos y de bloqueo), AstroWarp, VPN, AdGuard Home, Control parental, ZeroTier, Tailscale, Reenvío de puertos, Multi-WAN, Servidor DHCP, Reserva de direcciones, Red de invitados, DNS, Administración de puertos, IPv6, Drop-in Puerta de enlace, vigilancia IGMP, aceleración de red, configuración NAT.

## 13.8 IPv6

IPv6 (Protocolo de Internet versión 6) es el último protocolo de Internet diseñado para reemplazar IPv4. Ofrece un grupo más grande de IP únicas, lo que resuelve el problema de agotamiento de direcciones de IPv4 y admite el creciente número de dispositivos conectados en todo el mundo.

Inicie sesión en el panel de administración web de su enrutador y navegue hasta **RED** > **IPv6**. Esta página le permite habilitar y configurar IPv6 en su enrutador. Cuando IPv6 está habilitado, las interfaces WAN como Ethernet obtendrán sus direcciones IPv6 a través de DHCPv6.

Active **Habilitar**, seleccione el modo para su red principal y el método de adquisición de DNS, luego haga clic en **Aplicar.**




**Nota**: Algunas características (por ejemplo, firewall, GoodCloud, OpenVPN DCO) aún no son compatibles con IPv6. Si habilita estas características e IPv6 al mismo tiempo, es probable que cause problemas de conectividad .

### 13.8.1 Modo IPv6

Hay cuatro modos disponibles: Nativo, Passthrough, NAT6 e IPv6 estático.

- **Nativo**: este modo se aplica cuando el enrutador obtiene directamente una dirección IPv6 pública y el enrutador asigna automáticamente direcciones IPv6 a los dispositivos en línea. Este modo puede satisfacer las necesidades de acceso a IPv6 de la mayoría de los usuarios.
- **Passthrough**: este modo se aplica cuando los paquetes IPv6 deben pasar directamente sin ningún procesamiento ni conversión. Por ejemplo, algunas aplicaciones o servicios específicos pueden requerir la preservación completa del contenido del paquete IPv6 para su posterior procesamiento o análisis. Este modo lo utiliza el personal técnico para la depuración de la red o el análisis de seguridad.
- **NAT6**: este modo es adecuado para escenarios en los que se utiliza un enrutador como puerta de enlace para asignar direcciones IPv6 internas dinámicas a cada dispositivo en la red. En este modo, los dispositivos terminales se conectan a través de una terminal de red óptica y obtienen una dirección IPv6 de red de área local.
- **IPv6 estático**: este modo es adecuado para dispositivos o servicios que requieren una dirección IPv6 fija, como servidores o impresoras de red. Este modo asegura que el dispositivo utilice siempre la misma dirección IPv6, facilitando la gestión y el acceso.

### 13.8.2 Método de obtención de DNS

Determina cómo el enrutador obtiene las direcciones del servidor DNS IPv6. Hay dos opciones: Automático y Manual.

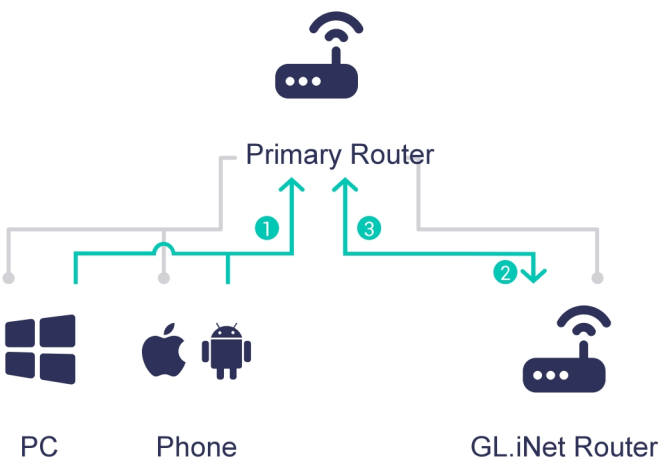
- **Automático**: el enrutador obtendrá direcciones de servidor DNS IPv6 dinámicamente (por ejemplo, a través de DHCPv6).
- **Manual**: Ingrese direcciones de servidor DNS IPv6 personalizadas. Sin embargo, dado que DNS se utiliza para resolver nombres de dominio en sus direcciones IP correspondientes, la configuración manual del servidor DNS puede provocar fallas en la búsqueda de DNS. Úselo con precaución.

## 13.9 Puerta de enlace directa

Drop-in Gateway es una función de extensión que permite la expansión de la capacidad de un enrutador principal existente sin reemplazarlo ni reconfigurarlo. Al conectar el enrutador GL.iNet al enrutador principal mediante un cable Ethernet, los usuarios pueden agregar funciones avanzadas a la infraestructura de red existente, por ejemplo:

- Filtrar anuncios a través de AdGuard Home
- Habilitar cliente VPN
- Usar DNS cifrado

Drop-in Gateway funciona como un sistema de red intermedio, enrutando el tráfico de datos desde los dispositivos cliente a través del enrutador GL.iNet para su procesamiento antes de transmitirlo a través del enrutador principal. Durante este proceso, no solo conserva la configuración de red existente para garantizar una conectividad ininterrumpida para todos los dispositivos conectados, sino que también le permite administrar el tráfico de red para todos o para dispositivos cliente específicos si es necesario.




El diagrama anterior consta de dos tipos de líneas: líneas grises y líneas verdes marcadas con tres flechas, cada una etiquetada con un número correspondiente.

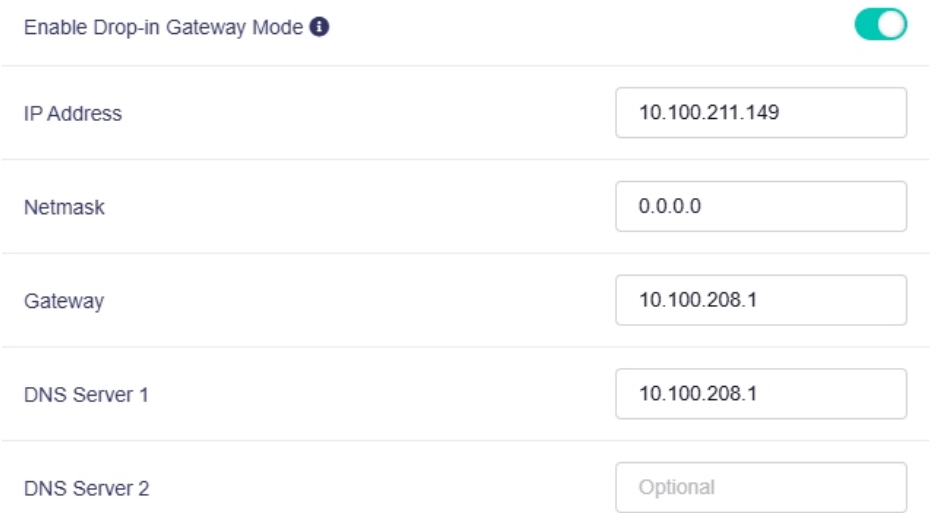
- **Gray lines** ilustran la topología de conexión física: dispositivos cliente (por ejemplo, computadora, computadora portátil) se conecta al enrutador principal, y el puerto LAN del

enrutador principal se vincula al puerto WAN del enrutador GL.iNet (con Drop-in Gateway habilitado) a través de un cable Ethernet.

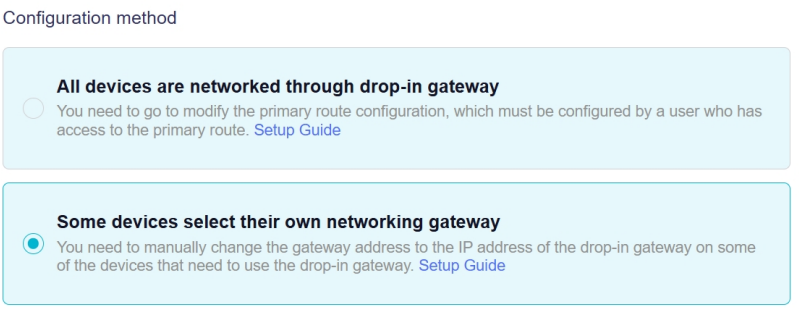
- **Glíneas verdes** representan la ruta de transmisión de datos secuencial cuando Drop-in Gateway está activo, con las flechas numeradas que indican el orden del flujo de tráfico:
  1. El tráfico de los dispositivos cliente se enruta primero al enrutador principal;
  2. El enrutador principal reenvía el tráfico al enrutador GL.iNet para su procesamiento (por ejemplo, filtrado de anuncios, cifrado VPN);
  3. Después el procesamiento, el tráfico se envía de regreso al enrutador principal, que luego entrega los datos finales a los dispositivos cliente originales o los enruta a Internet.

Siga los pasos a continuación para habilitar Drop-in Gateway si es necesario.

1. Inicie sesión en el panel de administración web de su enrutador' y navegue hasta **RED** > **Puerta de enlace directa**. Alternar en **Enable Modo de puerta de enlace directa**, y confirme los parámetros de red.



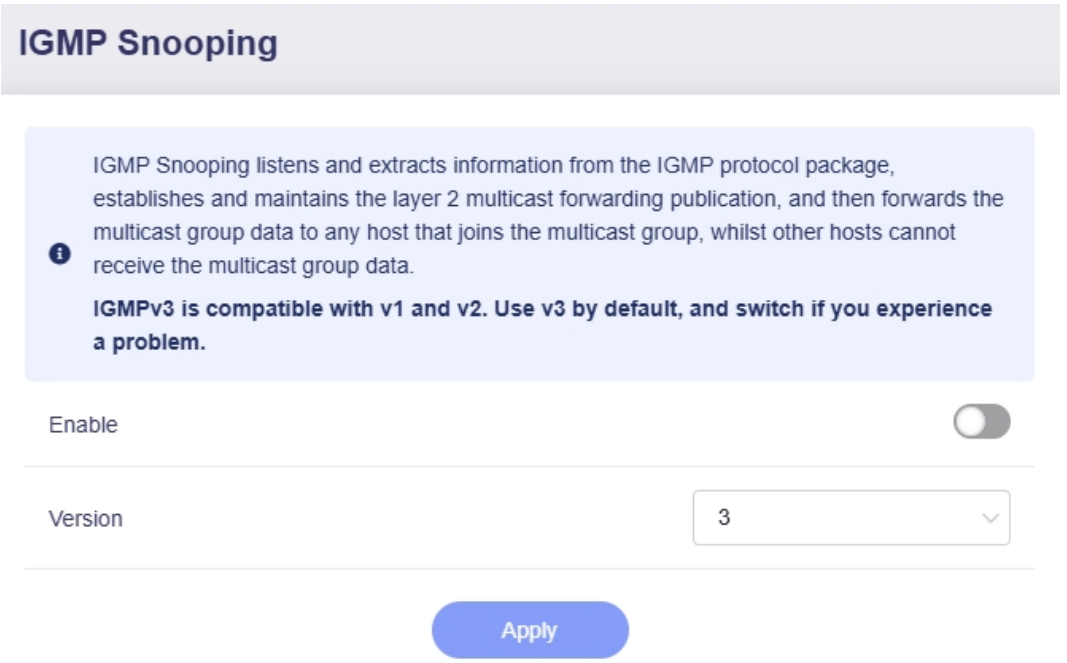

2. Seleccione el método de configuración, luego haga clic en **Aplicar**. Consulte este tutorial para detalless.



## 13.10 Inspección IGMP

IGMP Snooping escucha el paquete del protocolo IGMP y extrae el correspondiente información, establece y mantiene la tabla de reenvío de multidifusión de capa 2 y luego reenvía los datos del grupo de multidifusión al host que se une al grupo de multidifusión, mientras que otros hosts no pueden recibir los datos del grupo de multidifusión.

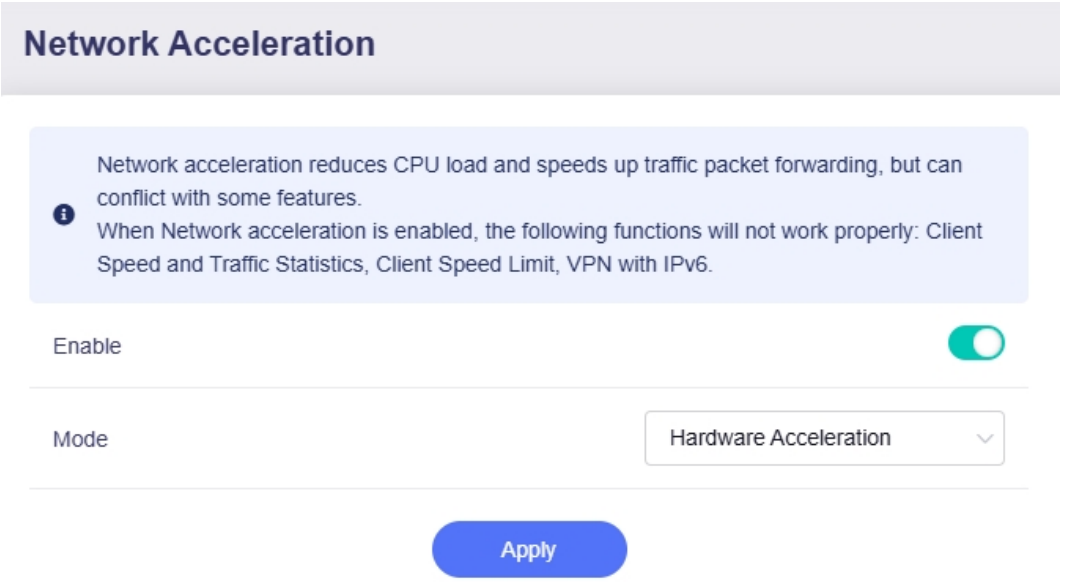
Inicie sesión en el panel de administración web de su enrutador' y navegue hasta **RED** > **Inspección IGMP**. Puede habilitar para usar la función de multidifusión en su enrutador si es necesario.



## 13.11 Aceleración de red

La aceleración de red reduce la carga de la CPU y acelera el reenvío de paquetes de tráfico, pero puede entrar en conflicto con algunas funciones.

Inicie sesión en el panel de administración web de su enrutador y navegue hasta **RED** > **Aceleración de red**. Esta página le permite habilitar la aceleración de red y seleccionar el modo Aceleración de hardware.



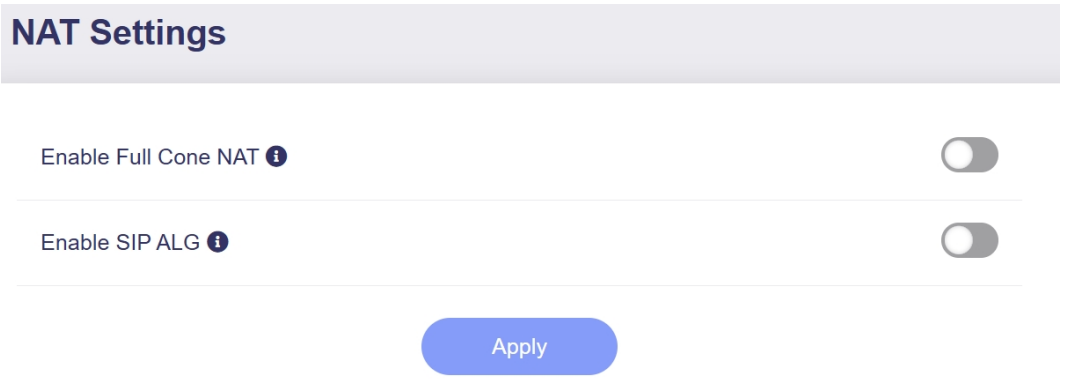

**Aceleración de hardware** modo descarga tareas de red de alta frecuencia (por ejemplo, NAT, reenvío de paquetes, verificación de suma de comprobación) a hardware dedicado, como NPU o chips HWNAT. Funciona específicamente en conexiones Ethernet y repetidoras, sobresaliendo en estos escenarios con rutas fijas y reglas simples para ofrecer alto rendimiento, baja latencia y carga mínima de CPU para la transmisión de datos a velocidad de cable.

**Nota**: Cuando la aceleración de red Aes habilitadas, las siguientes funciones no funcionarán correctamente: Estadísticas de velocidad del cliente, Estadísticas de tráfico, Límite de velocidad, Control parental y VPN con IPv6.

## 13.12 Configuración NAT

La configuración NAT controla los comportamientos de traducción de direcciones de red, optimizando las conexiones P2P y los servicios VoIP, pero habilitar ciertas opciones puede debilitar la seguridad de la red o desencadenar anomalías en las llamadas.

Inicie sesión en el panel de administración web de su enrutador' y navegue hasta **RED** > **Configuración NAT**. Esta página le permite habilitar Full Cone NAT para mejora la estabilidad de la conexión punto a punto para aplicaciones como juegos o streaming, y SIP ALG para solucionar problemas de compatibilidad con servicios telefónicos basados en VoIP/SIP.




### 13.12.1 NAT de cono completo

Full Cone NAT actúa como un "atajo directo" para dispositivos como consolas de juegos o teléfonos cuando se conectan con otros en línea (por ejemplo, en juegos multijugador o videollamadas).

Al permitir que los dispositivos externos lleguen directamente a los dispositivos locales a través del enrutador, en lugar de ocultarlos detrás de varias capas, mejora la estabilidad de la conexión punto a punto (P2P), reduce la latencia y resuelve la conexión. fallas en aplicaciones P2P.

Nota: Habilitar esta función puede reducir la seguridad en comparación con otros tipos de NAT, ya que expone los puertos del dispositivo a la red pública.

### 13.12.2 ALG SIP

SIP ALG (Application Layer Gateway) funciona como un "traductor" de enrutador para Servicios de comunicación basados en VoIP/SIP, como teléfonos de escritorio empresariales o llamadas basadas en aplicaciones.

Diseñado para abordar los desafíos transversales de NAT, ajusta los datos de las llamadas para garantizar una transmisión fluida a través de múltiples capas NAT, común en redes con múltiples enrutadores (por ejemplo, un enrutador principal y un enrutador GL.iNet), mitigando así los conflictos y evitando interrupciones en las llamadas.

**Nota**: SIP ALG incompatible o mal implementado puede degradar la calidad de la llamada, lo que genera problemas que incluyen audio unidireccional, timbres que no responden, llamadas interrumpidas o llamadas que se enrutan directamente al correo de voz.

Capítulo 14

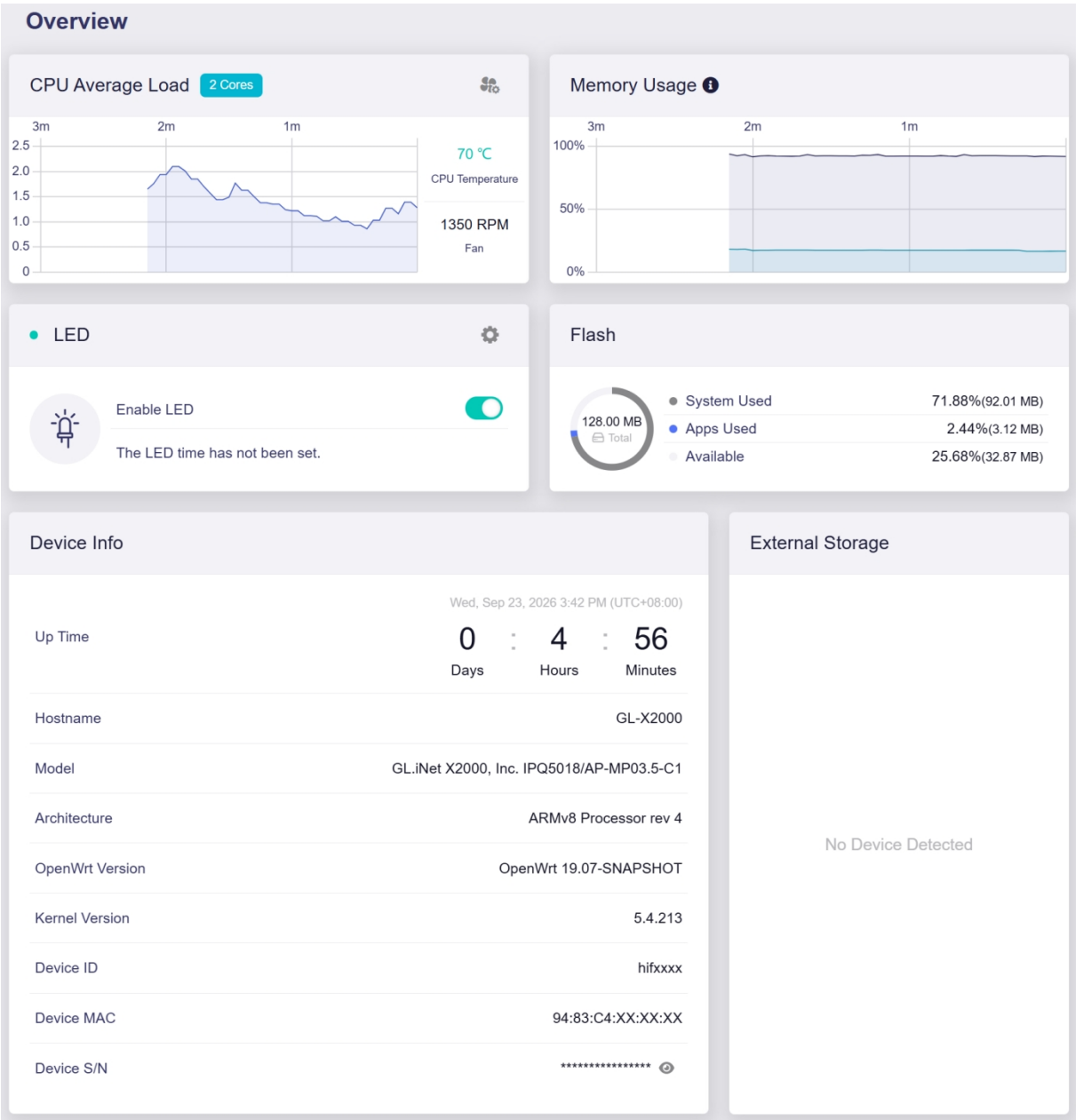
# Sistema

Este capítulo cubre las herramientas de administración del sistema para el dispositivo, como descripción general del sistema, actualización, tareas programadas, zona horaria, registro, restablecimiento de firmware y configuración avanzada.

## 14.1 Descripción general

Inicie sesión en el panel de administración web de su enrutador' y navegue hasta **SISTEMA** > **Descripción general**. Esta página muestra estado del hardware y admite algunos controles simples, que incluyen:

- CPU, memoria, y Flash Estado
- LED Control
- Dispositivo IInformación
- Almacenamiento externo Conmutador de protocolo



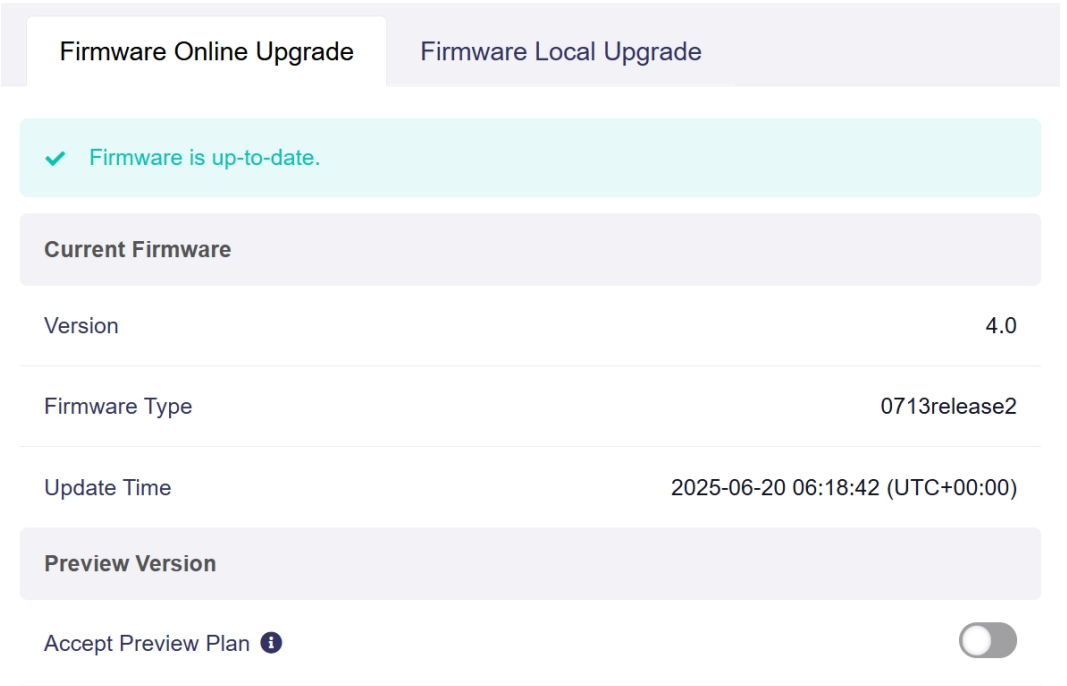
## 14.2 Actualización

Inicie sesión en el panel de administración web de su enrutador y navegue hasta **SISTEMA** > **Actualización**. Puede actualizar el firmware del enrutador y del módem mediante una actualización local o en línea.

### 14.2.1 Actualización de firmware

#### Actualización en línea

Puede buscar el firmware actual detalles aquí, incluida la versión del firmware, el tipo de firmware (por ejemplo, versión, beta) y el tiempo de actualización.



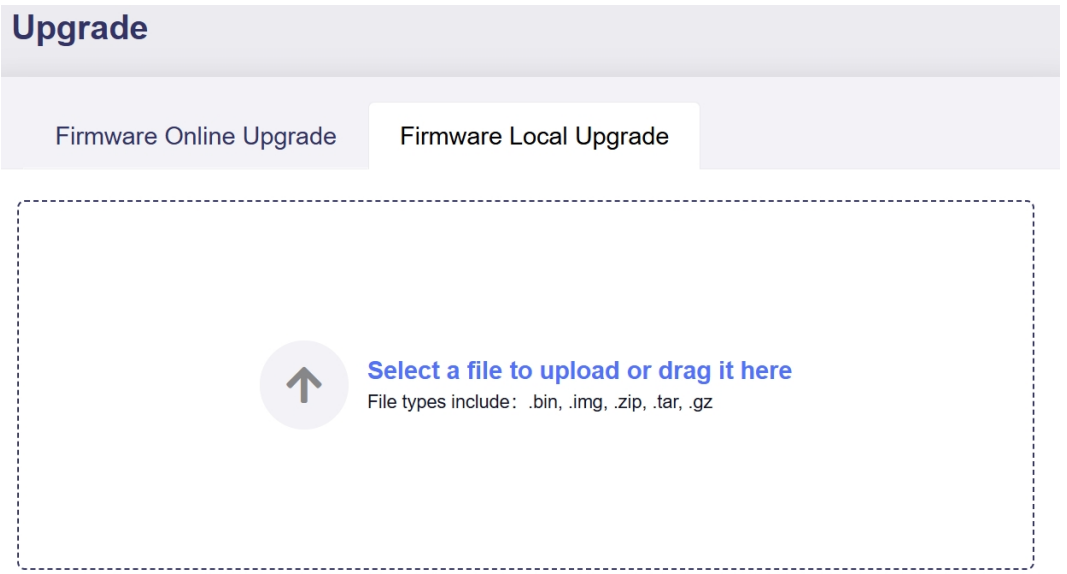

- **Aceptar plan de vista previa**: Si esta opción está habilitada, puede probar nuevas funciones antes de que se emita la versión final y enviarnos sus comentarios. Configúrelo una vez y permanecerá encendido. Tenga en cuenta que es posible que estas actualizaciones no sean estables.

Si su enrutador está conectado a Internet, buscará la versión de firmware más reciente disponible para descargar.

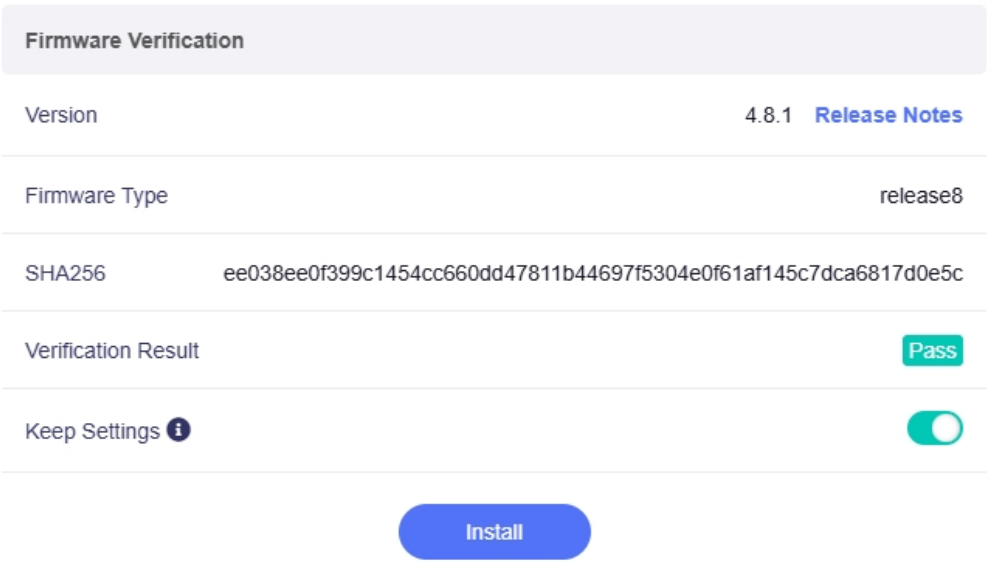
**Consejo**: Al intentar realizar una actualización en línea, si muestra **Error de descarga**, navegue hasta **SYSTEM** > **Zona horaria** y solucione el error de zona horaria (sincronización con el navegador).

## Actualización local

La actualización local no depende de una conexión a Internet para el enrutador. Descargue el paquete de firmware correcto (que coincida con el modelo de su enrutador) desde el Centro de descargas oficial a su dispositivo local. Luego inicie sesión en el's panel de administración web del enrutador, navegue hasta **SISTEMA** > **Actualización** > **Actualización local** y cargue el paquete de firmware.




TLa página mostrará los detalles del firmware. Verifique estos detalles antes de hacer clic en **Instalar**.

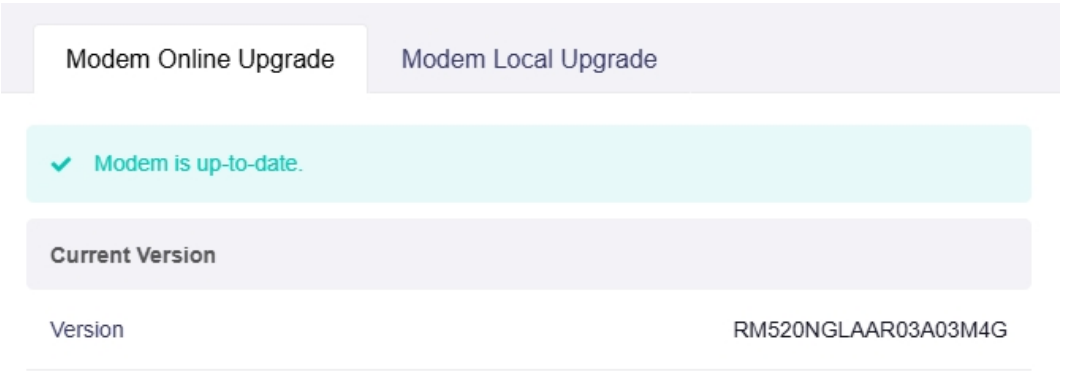


- **Mantener configuración**: si está habilitado, se conserva la configuración actual. Sin embargo, cualquier paquete instalado manualmente debe reinstalarse una vez completada la actualización. No habilite esta opción al degradar el firmware.

### 14.2.2 Actualización de módem

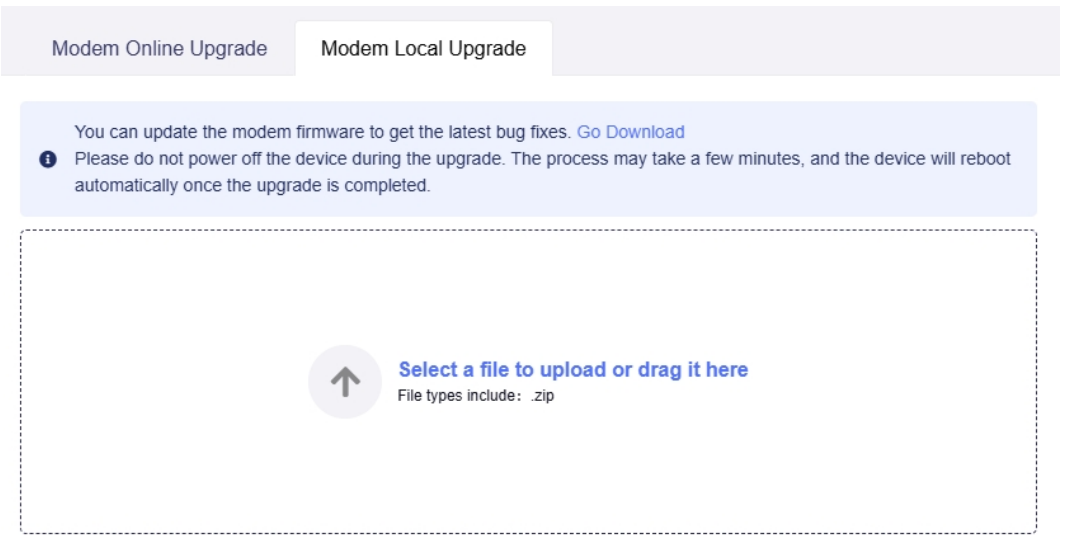
## Actualización en línea

Puede encontrar la versión actual del módem celular aquí. Si su enrutador está conectado a Internet, buscará automáticamente la última versión del módem celular desde el servidor del fabricante, lo que simplifica el proceso de actualización.




## Actualización local

Cargue manualmente un archivo de firmware del módem desde su computadora para actualizar el módem celular si es necesario.



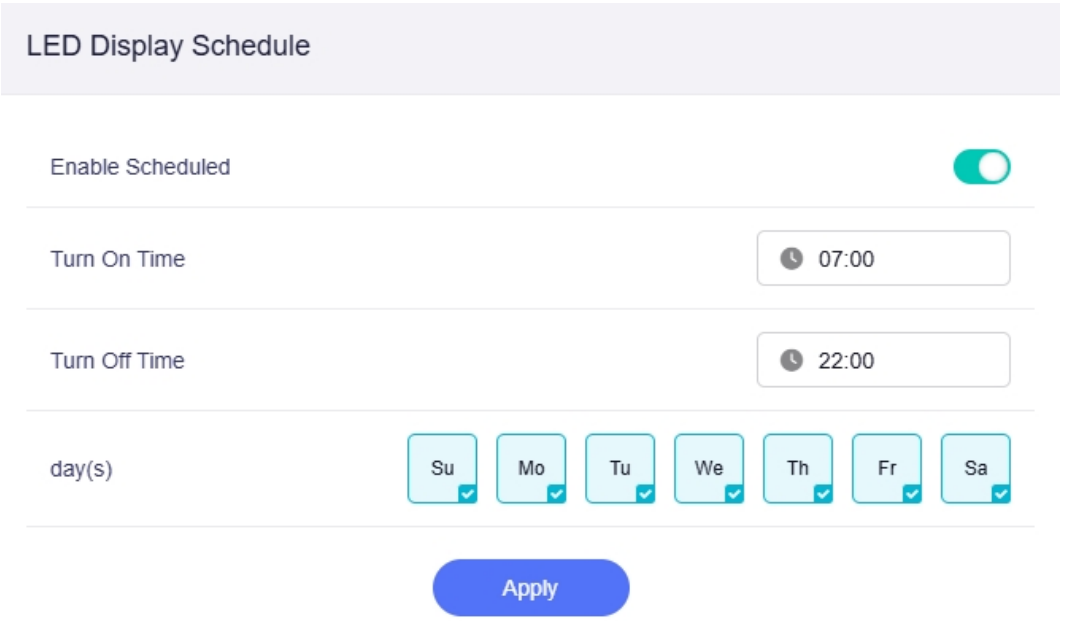
## 14.3 Tareas programadas

Inicie sesión en el panel de administración web de su enrutador y navegue hasta **SISTEMA** > **Tareas programadas**. Esta página le permite configurar una programación diaria para algunas acciones básicas, como encender y apagar luz LED , reiniciar el enrutador, encender y apagar Wi-Fi, etc..

**Nota**: sincronice la hora en la Zona horaria antes de utilizar esta función. Si el dispositivo se apaga a la hora programada, la tarea no se ejecutará.

### 14.3.1 Programación de los indicadores LED

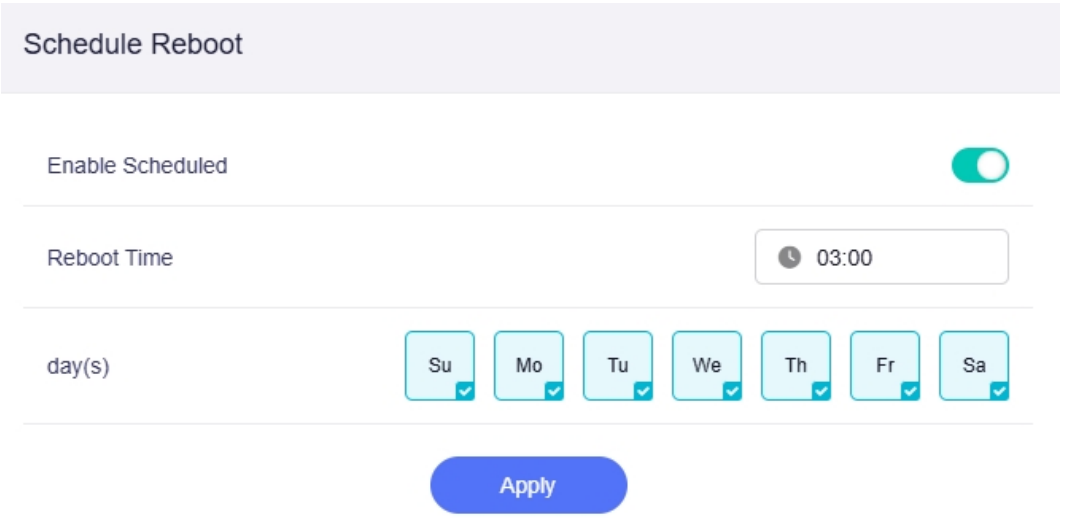
Set an encendido/apagado programar la luz LED de su enrutador si es necesario.
Cuando esté habilitado, configure las horas de encendido y apagado, seleccione las fechas efectivas semanales y luego haga clic en **Aplicar**.



## 14.3.2 Programar reinicio

Set un programe para reinicie automáticamente su enrutador si es necesario.

Cuando esté habilitado, establezca las horas de reinicio, seleccione las fechas efectivas semanales y luego haga clic en **Aplicar**.

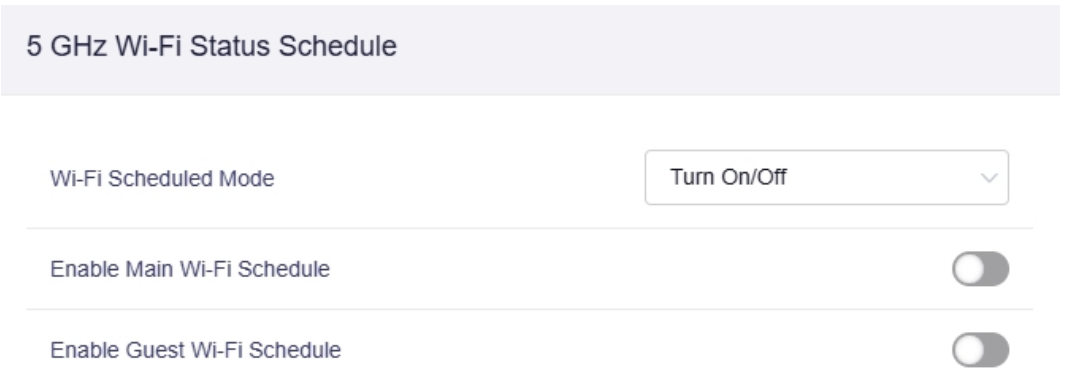



## 14.3.5 Programación de Wi-Fi de 5 GHz

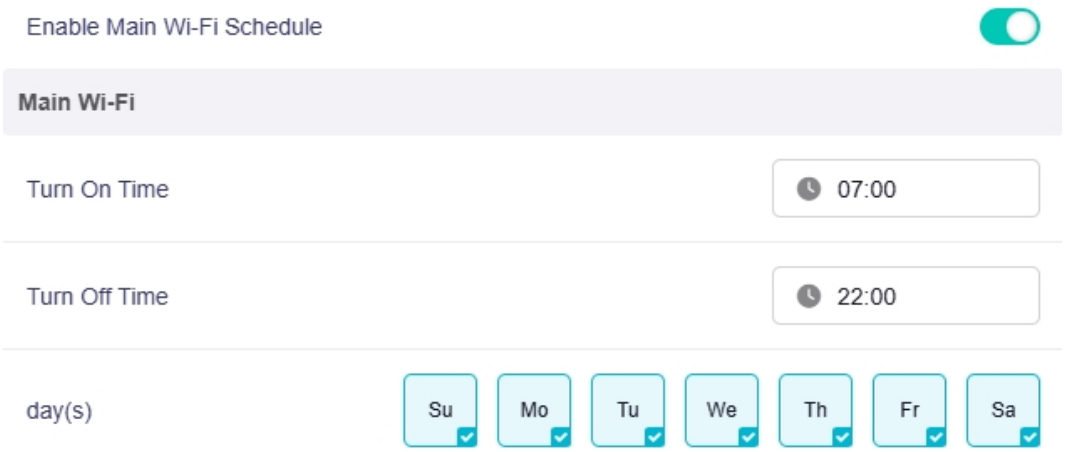
Establezca un horario para su Wi-Fi de 5 GHz en dos modos: encender/apagar y cambiar la alimentación de TX.

**Modo 1: Encender/apagar**

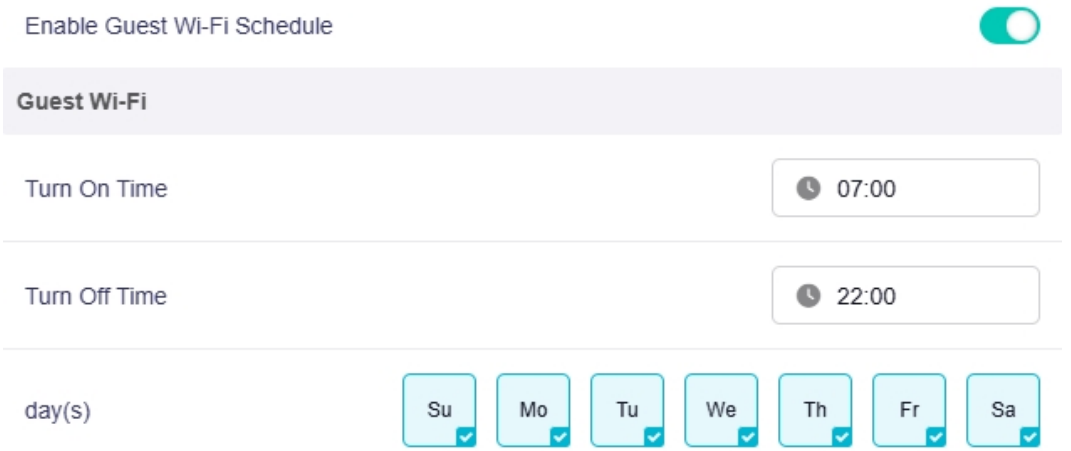
Puede habilitar el horario de encendido/apagado tanto para el Wi-Fi principal de 5 GHz como para los invitados Wi-Fi.




- **Programación de Wi-Fi principal**: Cuando esté habilitado, configure los horarios de encendido y apagado de su Wi-Fi principal de 5 GHz, seleccione las fechas efectivas semanales y luego haga clic en **Aplicar**.

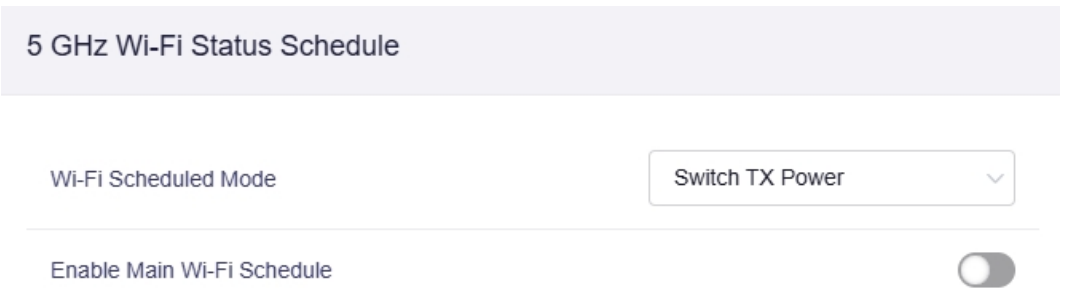



- **Programación de Wi-Fi para invitados**: cuando esté habilitado, configure los horarios de encendido y apagado de su Wi-Fi para invitados de 5 GHz, seleccione las fechas efectivas semanales y luego haga clic en **Aplicar**.

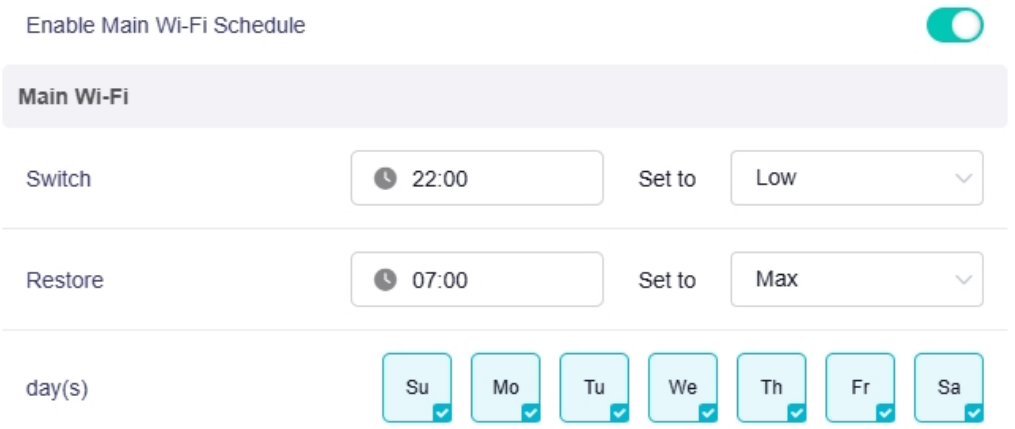



**Modo 2: cambiar la alimentación de TX**

Ypuede habilitar el Conmutación de alimentación TX programación para el 5 GHz Wi-F principali.



Cuando esté habilitado, configure dos acciones cronometradas para que su Wi-Fi principal de 5 GHz cambie la alimentación de TX, seleccione las fechas efectivas semanales y luego haga clic en **Aplicar**.

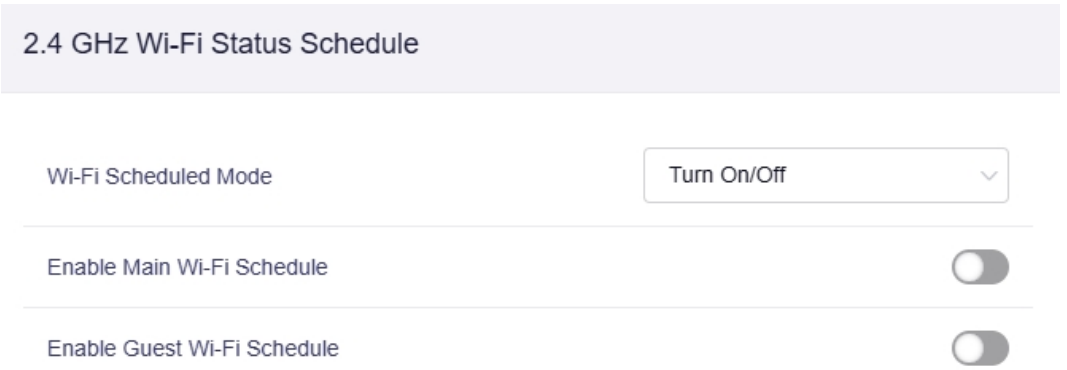



## 14.3.6 Programación de Wi-Fi de 2,4 GHz

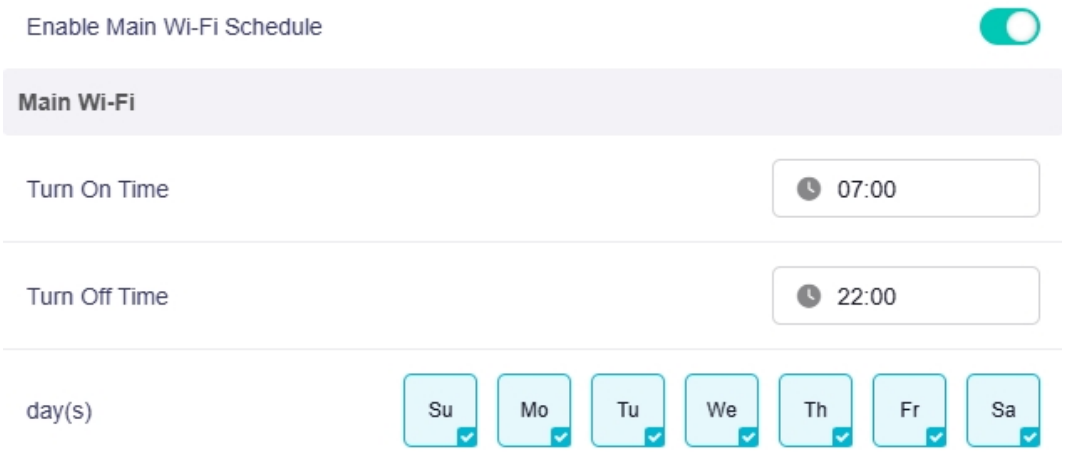
Establezca una programación para su Wi-Fi de 2,4 GHz en dos modos: encender/apagar y cambiar la alimentación de TX.

**Modo 1: Encender/apagar**

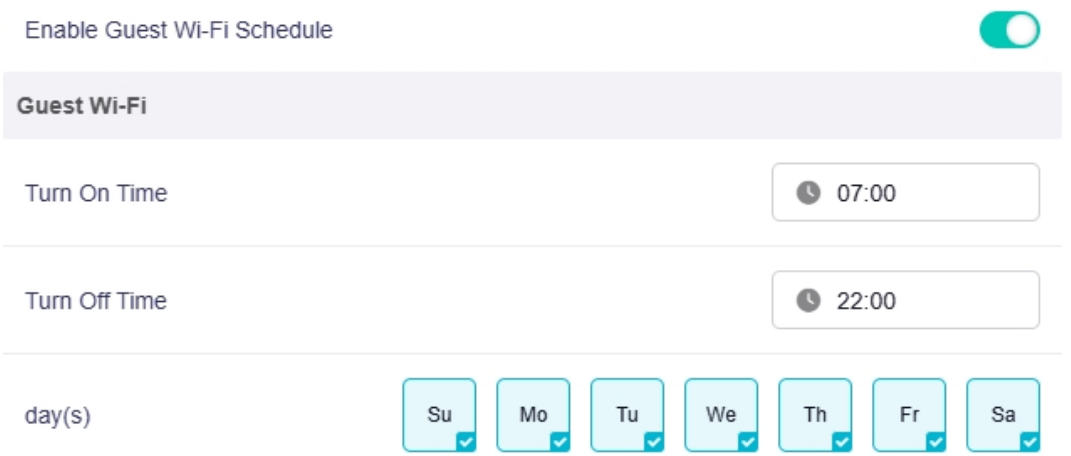
Puedes habilitar el horario de encendido/apagado tanto para el Wi-Fi principal de 2,4 GHz como para el Wi-Fi para invitados.




- **Horario de Wi-Fi principal**: Cuando esté habilitado, configura los horarios de encendido y apagado para tu Wi-Fi principal de 2,4 GHz, selecciona las fechas efectivas semanales, luego haga clic en **Aplicar**.

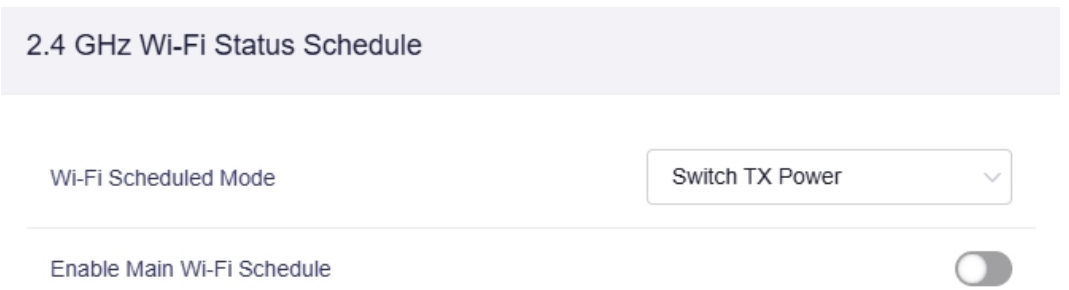



- **Programación de Wi-Fi para invitados**: cuando esté habilitado, configure los horarios de encendido y apagado para su Wi-Fi para invitados de 2,4 GHz, seleccione las fechas efectivas semanales y luego haga clic **Aplicar**.

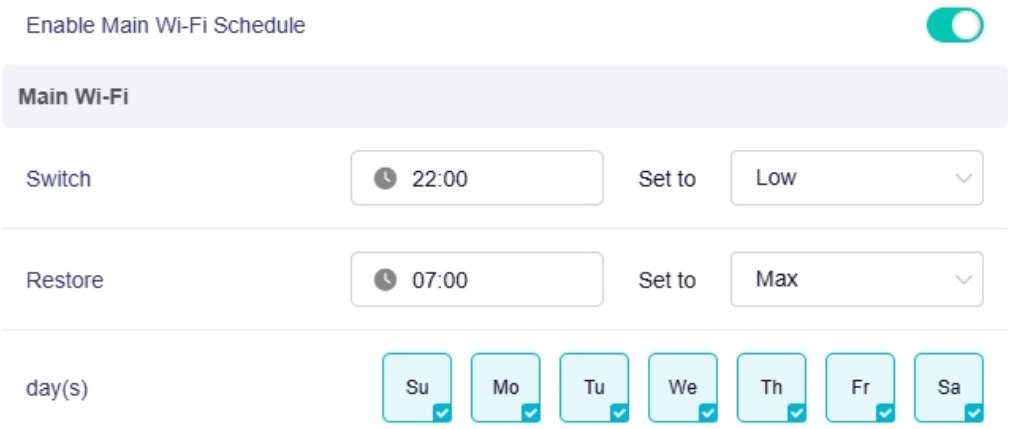



**Modo 2: Cambiar alimentación de TX**

YPuedes habilitar la Conmutación de alimentación de TX programar para el Wi-F principal de 2,4 GHzi.

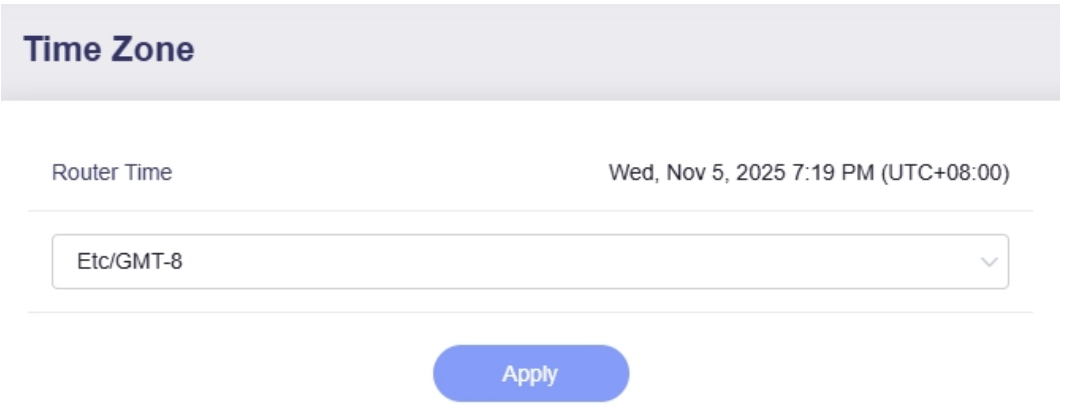


Cuando esté habilitado, establezca dos acciones cronometradas para su Wi-Fi principal de 2,4 GHz para cambiar la alimentación de TX, seleccione las fechas efectivas semanales, luego haga clic en **Aplicar**.

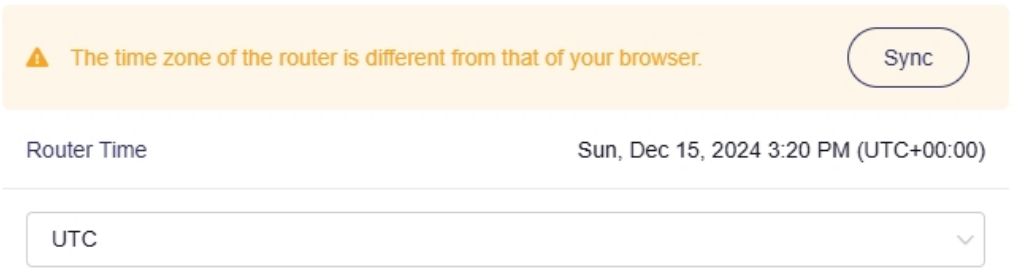


## 14.4 Zona horaria

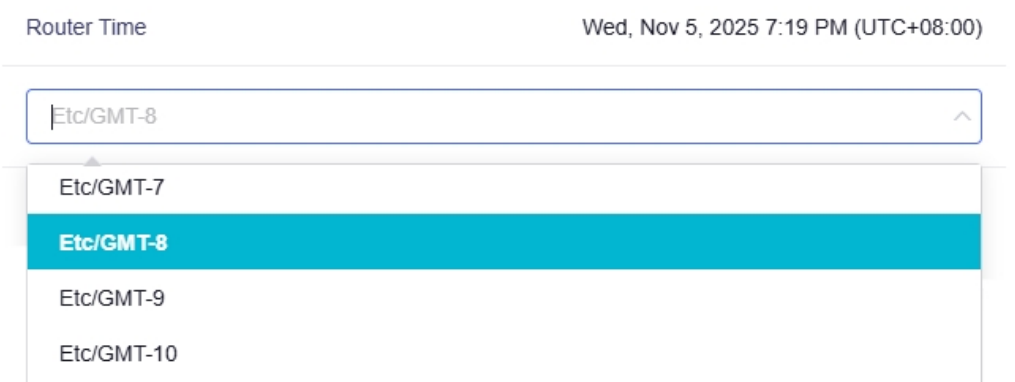
Inicie sesión en el panel de administración web de su enrutador y navegue hasta **SISTEMA** > **Zona horaria**. Esta página muestra la información de su enrutador sistema hora, que indica la fecha, la hora y el desplazamiento de zona horaria correspondiente.




Algunas funciones dependen de la hora del sistema del enrutador' para surtir efecto. Por lo tanto, asegúrese de que la zona horaria correcta esté sincronizada correctamente. Si la zona horaria del enrutador'es diferente a la de su navegador, se mostrará el siguiente mensaje. Haga clic en el botón **Sincronizar** para sincronizar la zona horaria.

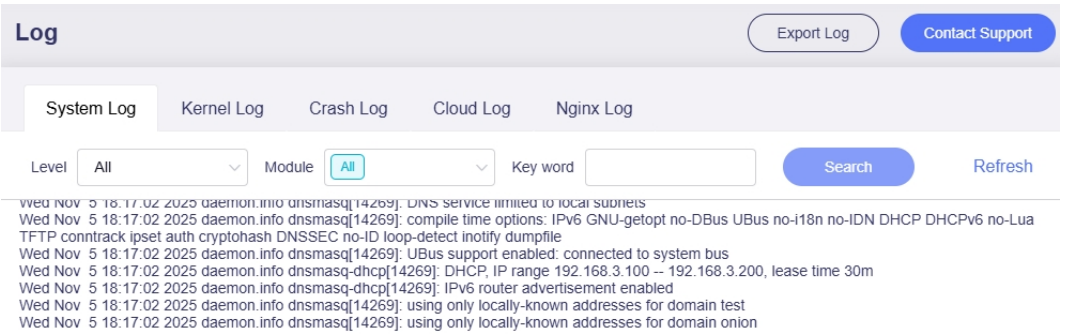



Para cambiar la zona horaria, sseleccione la zona horaria apropiada de la lista para garantizar que la hora del sistema coincida con su hora local.

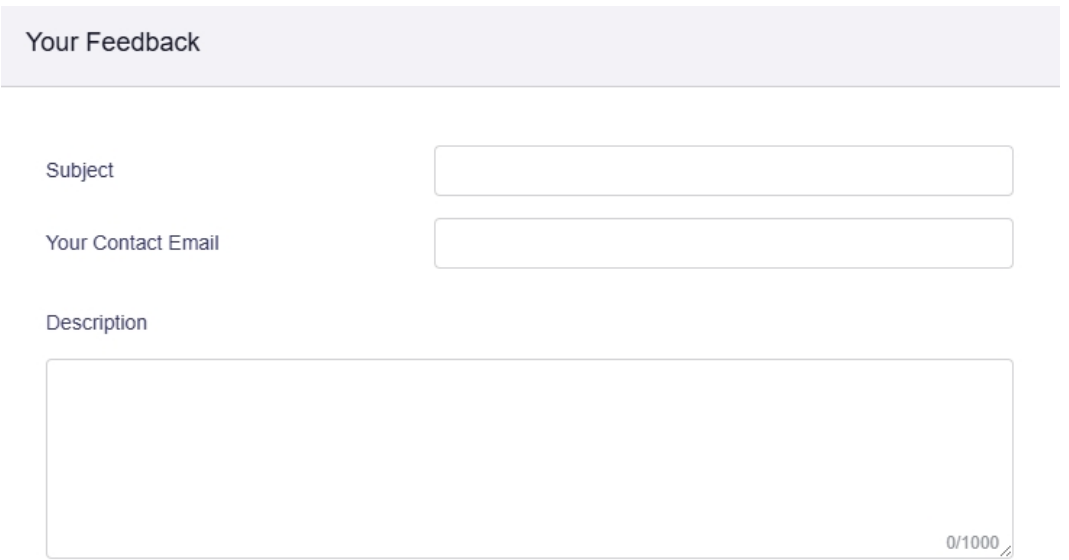


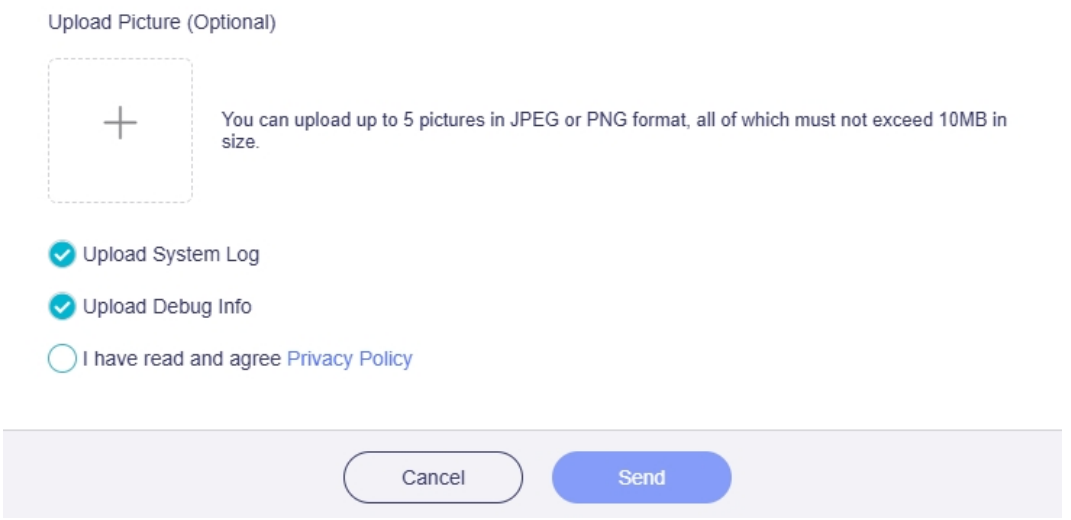
## 14.5 Registro

Inicie sesión en el panel de administración web de su enrutador y navegue hasta **SISTEMA** > **Registro**. Esta página le permite ver registros de System, Kernel, Crash, Cloud y Nginx para análisis y solución de problemas. Además, algunos modelos de celular que admiten eSIM también proporcionan registros de eSIM.




- **Buscar**: la página de registro del sistema proporciona filtrado para una búsqueda rápida. Puede seleccionar el nivel de registro (p. ej., todo, información, error) o el módulo (p. ej., IPv6, Conexión, Celular) de la lista desplegable, o ingresar palabras clave para consultar registros rápidamente.
- **Actualizar**: Haga clic en este botón para actualizar registros.
- **Exportar registro**: Haga clic en este botón para exportar información de depuración junto con los registros.
- **Comuníquese con el soporte técnico**: haga clic en este botón, complete la información detallada en la ventana emergente de la derecha y luego haga clic en **Enviar**. Sus comentarios se enviarán directamente a GL.iNet Soporte técnico.




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

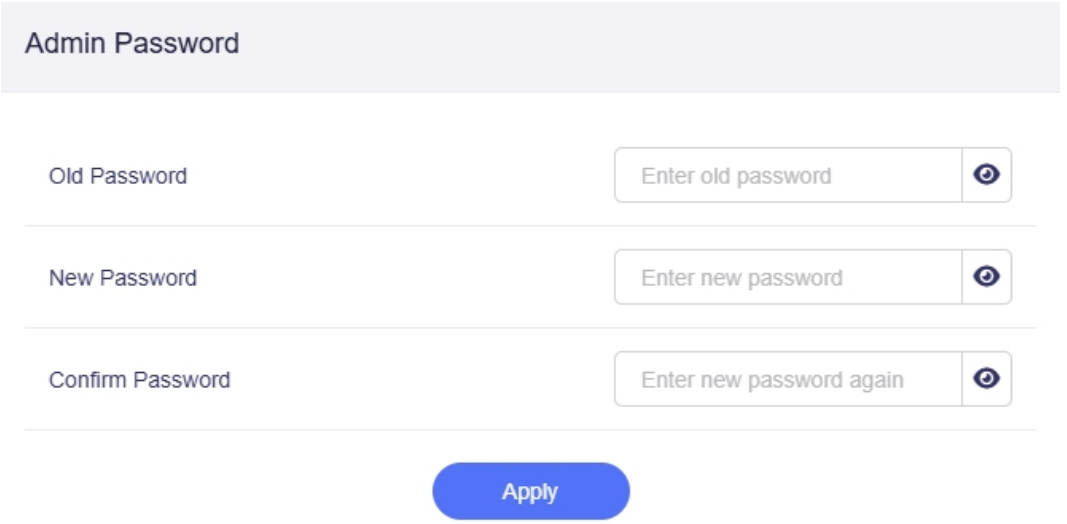
## 14.6 Seguridad

Inicie sesión en el panel de administración web de su enrutador y navegue hasta **SISTEMA** > **Seguridad**. Esta página contiene opciones de configuración para la administración local y remota del enrutador, incluyendo:

- Aadministrador password
- Acceso local para web panel de administración, LuCI y SSH
- Remote HTTPS/SSH unacceso
- Opuertos de lápiz en rexterno

### 14.6.1 Contraseña de administrador

En esta sección, puede cambiar la contraseña de inicio de sesión del panel de administración web.

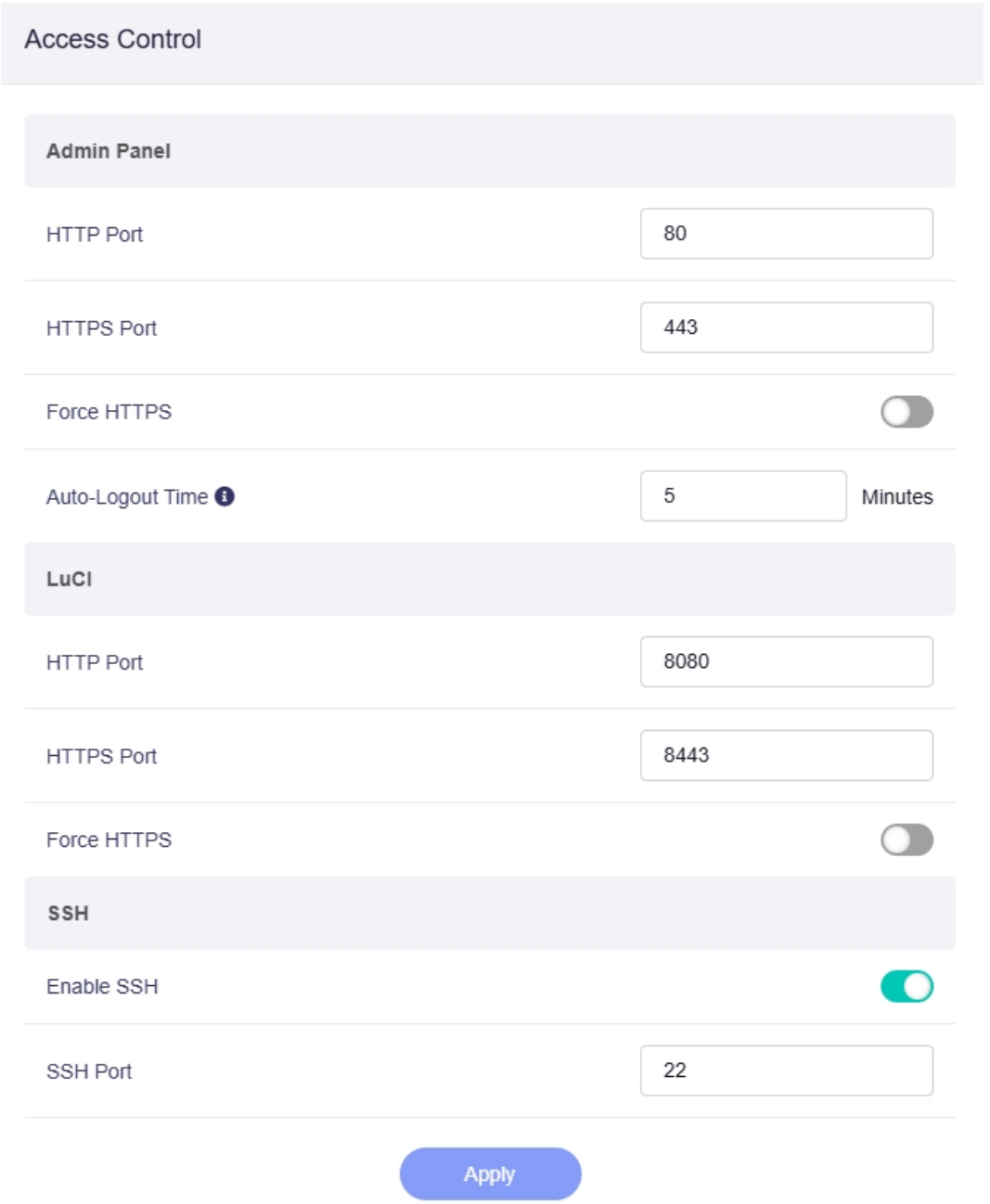



Los requisitos para la contraseña de administrador son los siguientes:

1. Mínimo 10 caracteres y máximo 63 caracteres de longitud.
2. Letras (distingue entre mayúsculas y minúsculas), números y símbolos (por ejemplo, ! @ # $ % ^ & * ( ) _ + - = , . > < | ? / \ [ ] { } : ; " ' ` ~ ) están permitidos.
3. Se requieren al menos dos tipos (letras mayúsculas, minúsculas, números y símbolos).

## 14.6.2 Control de acceso

Esta sección administra el acceso a las múltiples interfaces del enrutador' (Admin Panel, LuCI y SSH). Puede evitar intentos de escaneo e intrusión en el puerto predeterminado y evitar problemas de red causados por conflictos de puertos.




**Panel de administración**

- **Puerto HTTP**: el valor predeterminado es 80, utilizado para el acceso HTTP sin cifrar al panel de administración web.

- **Puerto HTTPS**: el valor predeterminado es 443, utilizado para el acceso HTTPS seguro al panel de administración web.
- **Forzar HTTPS**: cuando está habilitado, se exige el acceso al panel de administración web para utilizar una conexión HTTPS segura.
- **Tiempo de cierre de sesión automático**: establecido en 5 minutos de forma predeterminada, cierra automáticamente las sesiones de administración inactivas después de esta duración por motivos de seguridad. Puede personalizar el tiempo de cierre de sesión automático, desde 1 minuto hasta 3 horas.

**LuCI**

**Nota**: instale LuCI en la Configuración avanzada antes de realizar la configuración. el control de acceso.

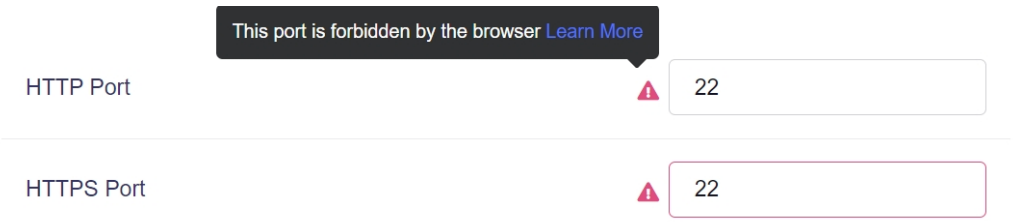
- **Puerto HTTP**: El valor predeterminado es 8080, para acceso HTTP no cifrado a la interfaz LuCI.
- **Puerto HTTPS**: El valor predeterminado es 8443, para un acceso HTTPS seguro al mismo. Interfaz LuCI.
- **Forzar HTTPS**: cuando está habilitado, se exige el acceso a la interfaz LuCI para utilizar una conexión HTTPS segura.

**SSH**

- **Habilitar SSH**: Ehabilitado de forma predeterminada, controla si el el acceso SSH al enrutador está permitido.
- **Puerto SSH**: El valor predeterminado es 22, el puerto utilizado para el acceso SSH al enrutador.

**Nota**:

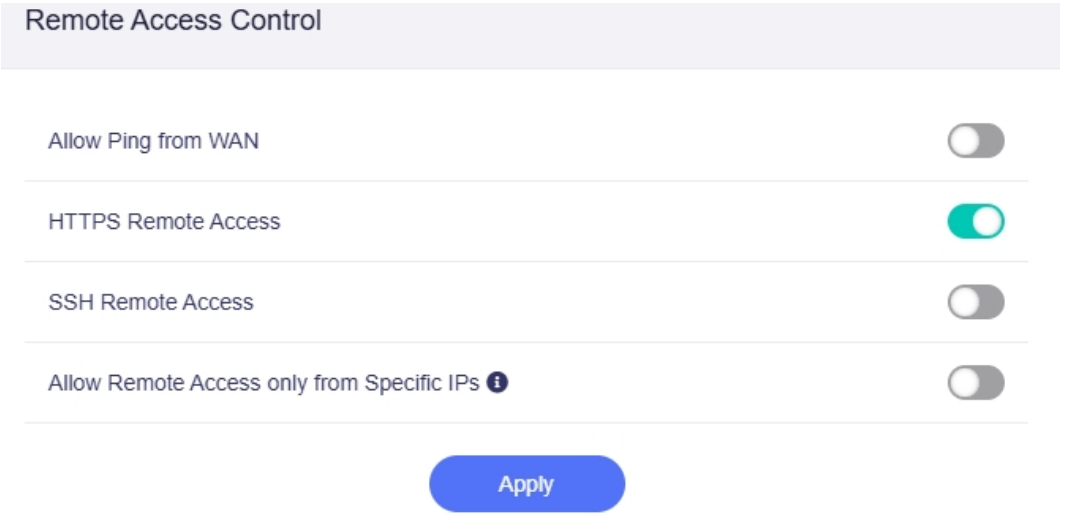
1. Si asigna un número de puerto que entra en conflicto con un puerto reservado (o uno reservado para servicios específicos por navegadores/convenciones de red), aparecerá un mensaje que indica "Este puerto está prohibido por el navegador".



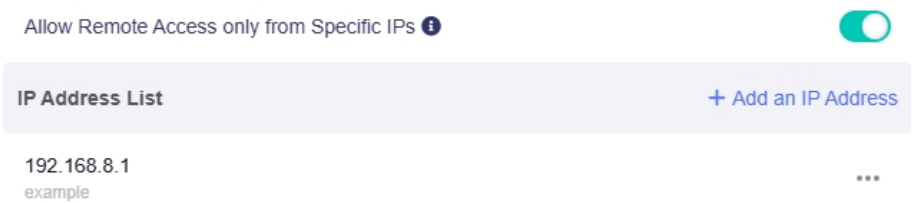
2. Si el número de puerto se modifica en el firmware, usted Debe ingresar el número de puerto correcto para acceder al panel de administración. Si olvidó el número de puerto, reinicie el enrutador para restaurar el número de puerto predeterminado.
3. La configuración de acceso a LuCI está disponible solo después de instalar LuCI. Si estas configuraciones no están visibles, vaya a **SISTEMA** > **Configuración avanzada** para instalar LuCI.

## 14.6.3 Control de acceso remoto

Esta sección administra el acceso remoto a las interfaces del enrutador, incluidos HTTPS, SSH y ping del lado WAN. También le permite restringir el acceso desde direcciones IP específicas, logrando un equilibrio entre accesibilidad remota y seguridad de la red.

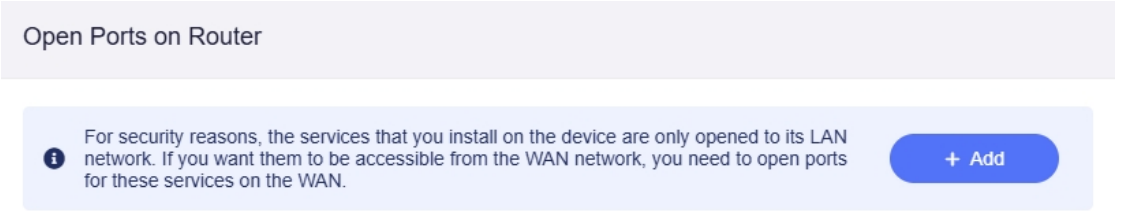



- **Permitir ping desde WAN**: Apermitir ping desde la WAN del enrutador lado puede ayudar a los usuarios a verificar si se puede acceder al enrutador a través de la WAN cuandocuando hay una red problema, así como determinar la latencia de la red y la pérdida de paquetes.
- **Acceso remoto HTTPS**: El acceso remoto HTTPS permite el acceso remoto seguro al panel de administración web del enrutador a través del protocolo HTTPS. Garantiza la transmisión de datos cifrados al administrar el enrutador de forma remota a través de un navegador web.
- **Acceso remoto SSH**: El acceso remoto SSH permite un acceso seguro al enrutador terminal. Permite a los usuarios administrar remotamente el enrutador a través de SSH, estableciendo un túnel cifrado para tareas.
- **Permitir acceso remoto desde IP específicas**: esta función solo está disponible cuando cualquiera de las tres funciones anteriores está habilitada. Puede agregar varias direcciones IP especificadas para administrar de forma remota el enrutador solo desde dispositivos con estas IP.

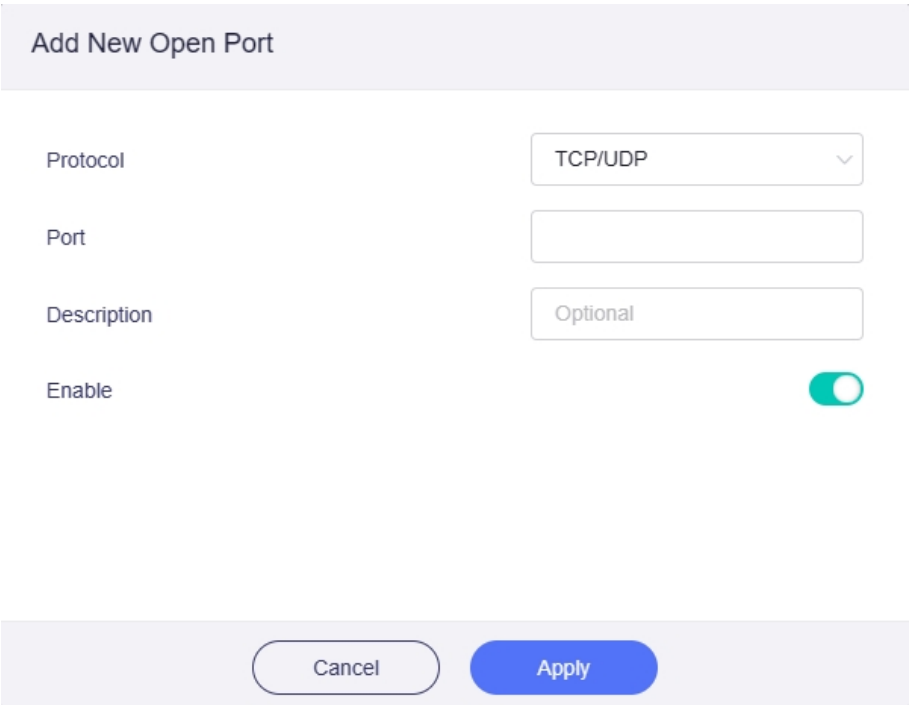


## 14.6.4 Abrir puertos en el enrutador

Esta sección administra el reenvío de puertos para los servicios en su enrutador. Algunos servicios, como web y FTP, requieren que sus respectivos puertos estén abiertos en el enrutador para poder acceder públicamente desde la red WAN. Por razones de seguridad, solo se puede acceder a los servicios instalados en el dispositivo dentro de la LAN de forma predeterminada. Si necesita habilitar dicho acceso WAN, puede abrir puertos específicos aquí.




Para abrir un puerto, haga clic en **Agregar** e ingrese la información requerida en la ventana emergente.



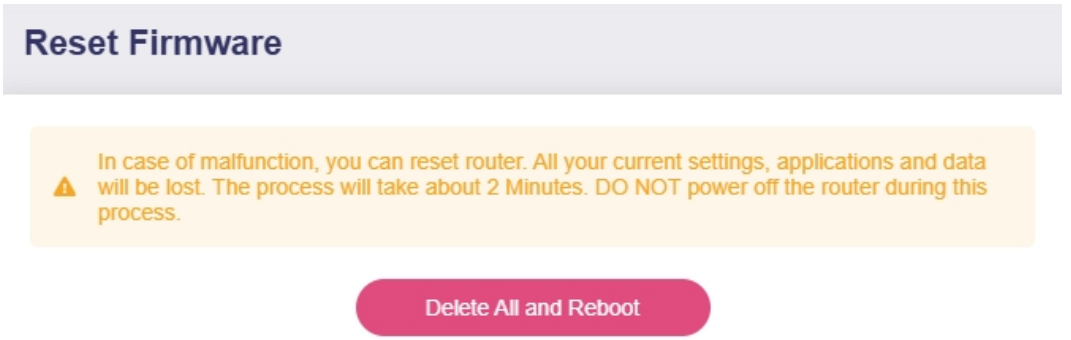

- **Protocolo**: seleccione el protocolo de red (TCP, UDP o TCP/UDP) para el puerto. Esto determina cómo se transmiten los datos para el servicio asociado con el puerto.
- **Puerto**: ingrese el número de puerto específico que desea abrir.

- **Descripción** (Opcional): agregue una breve nota para describir el propósito de este puerto abierto (por ejemplo, “Servidor web” o “Servicio FTP”) para una administración más sencilla.
- **Activar**: active este interruptor para activar o desactivar la regla de reenvío de puertos.

## 14.7 Restablecer firmware

Si el enrutador no funciona correctamente, puede intentar resolvering solucione el problema restableciendo el firmware.

Inicie sesión en el panel de administración web de su enrutador y navegue hasta **SISTEMA** > **Restablecer firmware**. Haga clic en **Eliminar todo y reiniciar** para restablecer el firmware si es necesario.




**Nota**: todas sus configuraciones, aplicaciones y datos actuales se borrados. El proceso durará unos 2 minutos. NoNo apague el enrutador durante este proceso.

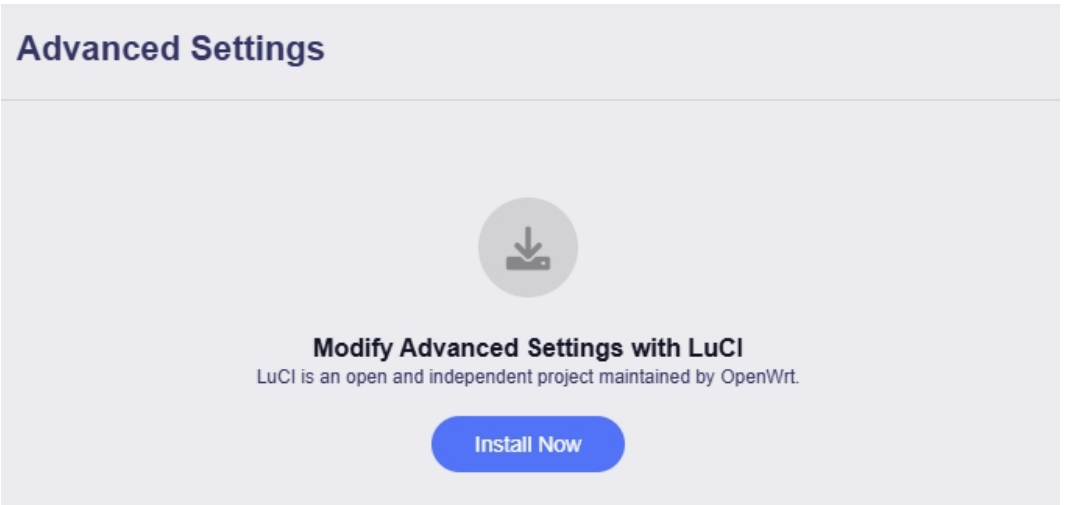
Si no puede acceder al panel de administración web del enrutador', intente restablecer su enrutador usando el botón de reinicio físico en el costado.

## 14.8 Configuración avanzada

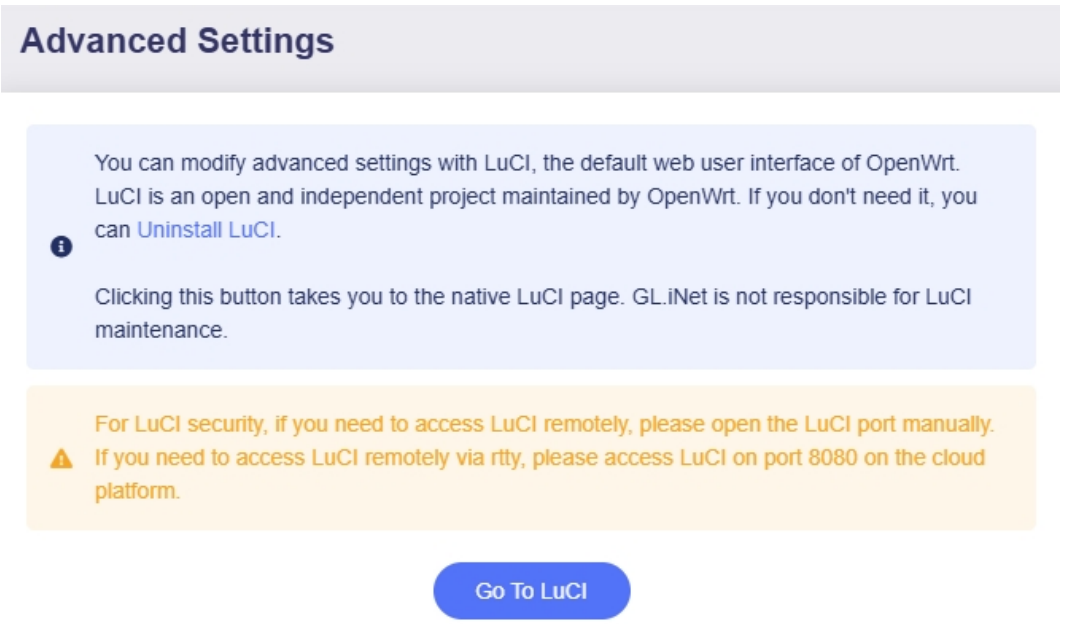
Inicie sesión en el panel de administración web de su enrutador y navegue hasta **SISTEMA** > **Configuración avanzada**. Esta página le permitemodificar la configuración avanzada a modificar configuración avanzada en LuCI, que es la interfaz de usuario web predeterminada de OpenWrt. Como proyecto abierto e independiente mantenido por OpenWrt, LuCI se proporciona tal cual. GL.iNet no es responsable del mantenimiento de LuCI.

Siga los pasos siguientes para iniciar sesión en la interfaz LuCI.

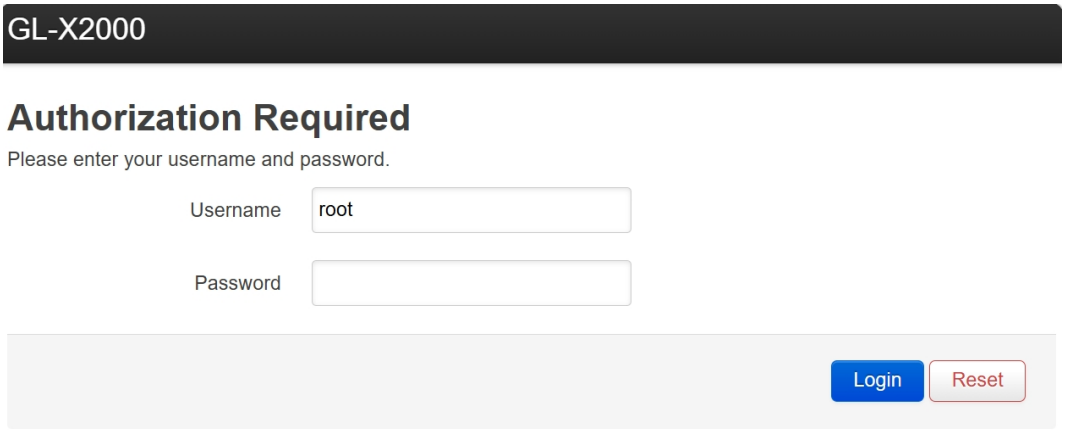
1. Haga clic en **Instalar ahora** y se instalará la interfaz LuCI.




2. Click **Vaya a LuCI**, y será redirigido a la página de inicio de sesión de LuCI.



3. Ingrese la contraseña de inicio de sesión, que es la misma que la contraseña del panel de administración web.




Yusted luego log en a la interfaz.

