

Manual de usuario

GL-MT2500 / Brume 2

Puerta de enlace de seguridad

Versión de firmware 4.7.4

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 5

1.1 Descripción general del producto 6

1.1.1 Apariencia 6

1.1.2 Interfaz y botón 7

1.1.3 LED 8

1.2 Especificaciones 8

1.3 Contenido del paquete 9

Capítulo 2 Conexión de hardware 10

2.1 Elección de una ubicación 11

2.2 Conexión del enrutador 11

Capítulo 3 Iniciar sesión en el enrutador 12

Capítulo 4 Configurar la conexión a Internet 14

4.1 Usar el asistente de configuración rápida 15

4.2 Configurar manualmente la conexión a Internet 16

4.2.1 Conectarse a Internet mediante un cable Ethernet 17

4.2.2 Conectarse a Internet mediante conexión compartida por USB 21

4.2.3 Conectarse a Internet mediante un módem USB 26

Capítulo 5 Clientes 28

5.1 Detalles del dispositivo 29

5.2 Acción 31

5.3 Eliminar clientes 34

5.4 Ordenar 35

Capítulo 6 Servicios en la nube 36

6.1 GoodCloud 37

6.1.1 Habilitar GoodCloud 38

6.1.2 Administrar el enrutador 41

6.1.3 Desvincular el dispositivo 46

6.1.4 Desactivar GoodCloud 46

6.2 AstroWarp 47

Capítulo 7 Conozca la VPN 48

7.1 Introducción 49

7.2 Escenarios de aplicación 50
Capítulo 8 Panel de VPN 52
8.1 Cliente VPN 54
8.1.1 Opciones del cliente 54
8.1.2 Modo proxy 56
8.1.3 Opciones globales 57
8.2 Servidor VPN 60
8.2.1 Opciones del servidor 60
8.2.2 Regla de ruta del servidor 62
8.2.3 Opciones globales 63
Capítulo 9 Configurar el servidor VPN 64
9.1 Configurar el servidor OpenVPN 65
9.1.1 Preparación 65
9.1.2 Pasos de configuración 66
9.1.3 Solución de problemas 68
9.2 Configurar el servidor WireGuard 69
9.2.1 Preparación 69
9.2.2 Pasos de configuración 70
9.2.3 Solución de problemas 73
Capítulo 10 Configurar el cliente VPN 74
10.1 Configurar el cliente OpenVPN 75
10.1.1 Preparación 75
10.1.2 Configurar NordVPN 75
10.1.3 Configurar el cliente OpenVPN manualmente (para otros proveedores) 81
10.2 Configurar el cliente WireGuard 84
10.2.1 Preparación 84
10.2.2 Configurar AzireVPN 85
10.2.3 Configurar Hide.me 89
10.2.4 Configurar IPVanish 92
10.2.5 Configurar Mullvad 96
10.2.6 Configurar NordVPN 100
10.2.7 Configurar PIA (Private Internet Access) 105
10.2.8 Configurar Surfshark 109
10.2.9 Configurar el cliente WireGuard manualmente (para otros proveedores) ... 113

Capítulo 11 Tor 118
Capítulo 12 Aplicaciones 120
12.1 Complementos 121
12.2 DNS dinámico 122
12.2.1 Habilitar DDNS 122
12.2.2 Comprobar si DDNS funciona 125
12.2.3 Acceso remoto HTTPS 127
12.2.4 Acceso remoto SSH 129
12.3 Almacenamiento en red 131
12.3.1 Conectar una unidad de almacenamiento 131
12.3.2 Configurar Samba 132
12.3.3 Configurar WebDAV 135
12.3.4 Configurar DLNA 138
12.4 AdGuard Home 139
12.5 Control parental 141
12.5.1 Configuración rápida 141
12.5.2 Solución de problemas 150
12.6 ZeroTier 151
12.6.1 Configurar ZeroTier 152
12.6.2 Permitir el acceso remoto a la WAN 156
12.6.3 Permitir el acceso remoto a la LAN 157
12.7 Tailscale 158
12.7.1 Configurar Tailscale 158
12.7.2 Permitir el acceso remoto a la WAN 162
12.7.3 Permitir el acceso remoto a la LAN 162
12.7.4 Nodos de salida personalizados 163
Capítulo 13 Red 165
13.1 Reenvío de puertos 166
13.1.1 DMZ 166
13.1.2 Reenvío de puertos 168
13.2 Multi-WAN 170
13.2.1 Seguimiento del estado de la interfaz 170
13.2.2 Modo Multi-WAN 174
13.3 LAN 177

13.3.1 Configuración básica 177
13.3.2 Servidor DHCP 178
13.3.3 Reserva de direcciones 180
13.4 DNS 181
13.4.1 Configuración del servidor DNS 182
13.4.2 Editar hosts 184
13.5 Gestión de puertos 186
13.6 Modo de red 187
13.7 IPv6 189
13.7.1 Modo IPv6 190
13.7.2 Método de obtención de DNS 190
13.8 Puerta de enlace directa 191
13.9 Inspección IGMP 193
13.10 Aceleración de red 194
13.11 Configuración NAT 196
Capítulo 14 Sistema 197
14.1 Descripción general 198
14.2 Actualización 199
14.2.1 Actualización en línea 199
14.2.2 Actualización local 201
14.3 Tareas programadas 202
14.3.1 Programación de los indicadores LED 202
14.3.2 Programar reinicio 203
14.4 Zona horaria 204
14.5 Registro 205
14.6 Seguridad 207
14.6.1 Contraseña de administrador 207
14.6.2 Control de acceso 208
14.6.3 Control de acceso remoto 211
14.6.4 Abrir puertos en el enrutador 212
14.7 Restablecer firmware 214
14.8 Configuración avanzada 215

Capítulo 1

Conozca su enrutador

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

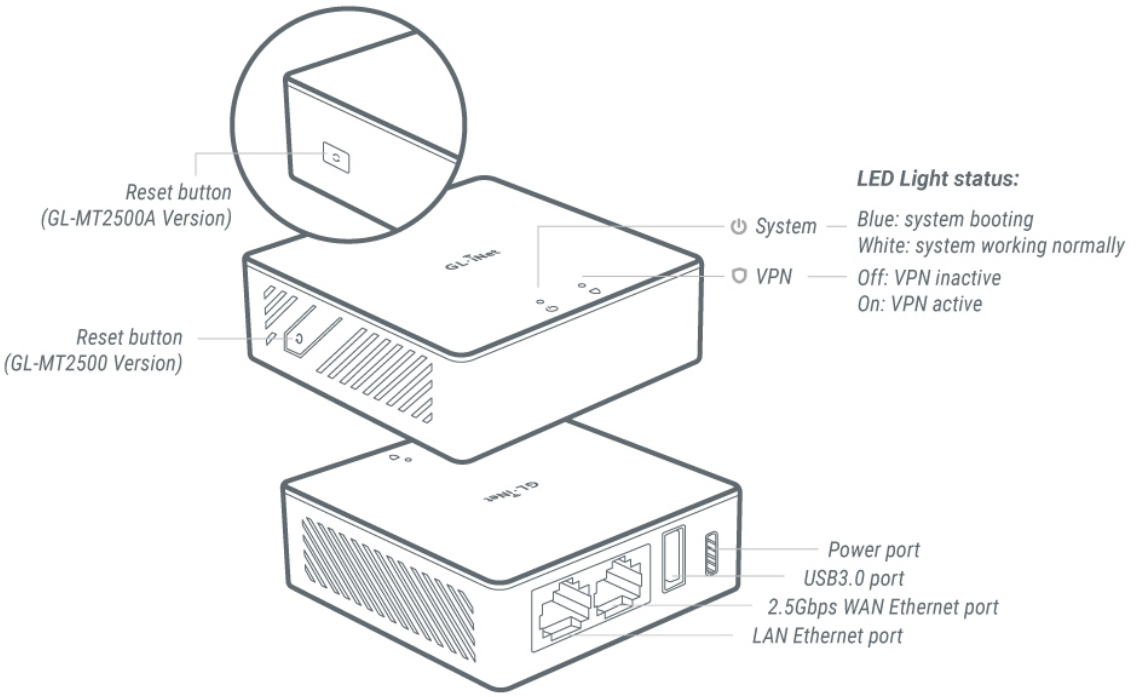
1.1 Descripción general del producto

Brume 2 (GL-MT2500/GL-MT2500A) es una puerta de enlace VPN ligera y potente que se ejecuta en el sistema operativo OpenWrt v21.02. Está diseñado de forma compacta para alojar un servidor VPN en casa o ejecutar SD-WAN (sitio a sitio) para pequeñas y medianas empresas. Viene en dos variantes: GL-MT2500 con carcasa de plástico y GL-MT2500A con carcasa de aluminio.

1.1.1 Apariencia



1.1.2 Interfaz y botón



Artículo	Descripción
Puerto de alimentación	Se conecta al adaptador de corriente.
Puerto WAN 2.5G	Se conecta a un módem o a una toma Ethernet para Internet.
Puerto LAN	Se conecta a dispositivos cableados si es necesario.
Puerto USB 3.0	Para dispositivos de almacenamiento USB, conexión USB de teléfono y dongles celulares compatibles.
Botón Restablecer	Presione y mantenga presionado durante **4 segundos** y luego suelte para reparar su red. El LED del sistema se volverá azul y parpadeará lentamente hasta su red está restaurada.
	Presione y mantenga presionado durante **10 segundos** y luego suelte para restablecer enrutador a los valores predeterminados de fábrica. El LED del sistema se volverá azul y parpadea rápidamente. Todos los datos se borrarán cuando el LED se encienda azul fijo.

1.1.3 LED

LED	Estado
Sistema	Azul: Arranque del sistema
	Blanco: Conectado a Internet
VPN	Desactivado: VPN inactiva
	Activado: VPN activa

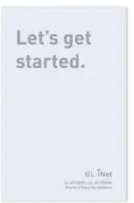
1.2 Especificaciones

Interfaz	1 puerto Ethernet WAN 2,5G 2 puertos Ethernet LAN 2.5G 1 x puerto USB 3.0 tipo C 1 x puerto de alimentación tipo C 1 x botón Restablecer
CPU	MediaTek MT7981B de doble núcleo, @1,3 GHz
Memoria/Almacenamiento	DDR4 1GB / eMMC 8GB
Velocidad de Ethernet	Puerto WAN: 10/100/1000/2500Mbps Puerto LAN: 10/100/1000 Mbps
Entrada de energía	Tipo C, 5V/2A
Consumo de energía	< 2,6W
Temperatura de funcionamiento	0 ~ 40°C (32 ~ 104°F)
Temperatura de almacenamiento	-20 ~ 70°C (-4 ~ 158°F)
Dimensión/Peso	GL-MT2500: 70 x 70 x 22 mm / 60 g GL-MT2500A: 70 x 70 x 22 mm / 157 g
Otras herramientas	Hoja de datos / Firmware / Aplicación / Unboxing / Tutoriales

1.3 Contenido del paquete

El paquete incluye:

- 1 x Brume 2 (GL-MT2500/GL-MT2500A)
- 1 x Manual del usuario (Guía de inicio rápido)
- 1 cable Ethernet
- 1 x Tarjeta de agradecimiento
- 1 x Tarjeta de garantía
- 1 x adaptador de corriente
- 1 x Convertidor (Dependiendo de su país de envío)



1 x User manual



1 x Brume 2 (GL-MT2500)



1 x Ethernet cable



1 x Thank you card



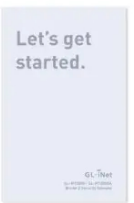
1 x Warranty card



1 x Power adapter



Converters
(Base on your shipping countries)



1 x User manual



1 x Brume 2 (GL-MT2500A)



1 x Ethernet cable



1 x Thank you card



1 x Warranty card



1 x Power adapter



Converters
(Base on your shipping countries)

Capítulo 2

Conexión de hardware

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

2.1 Elección de una ubicación

Siga estos consejos para elegir una ubicación para un 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 refrigeración**: coloque el enrutador en un lugar fresco, bien- área 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.
- **Superficie estable**: coloque el enrutador en una superficie plana y horizontal (estante, escritorio) para mayor estabilidad.

2.2 Conexión del enrutador

1. **Encendido**
   Junte el adaptador de corriente de dos piezas. Conéctelo a su Brume 2 y conéctelo a una toma de corriente. Se iniciará automáticamente.
2. **Conecte un dispositivo al enrutador**
   Conecte un dispositivo con cable (por ejemplo, una computadora o computadora portátil) al puerto LAN del Brume 2’con un cable Ethernet.
3. **Inicie sesión en el enrutador**
   El Internet no estará noal conectarse 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

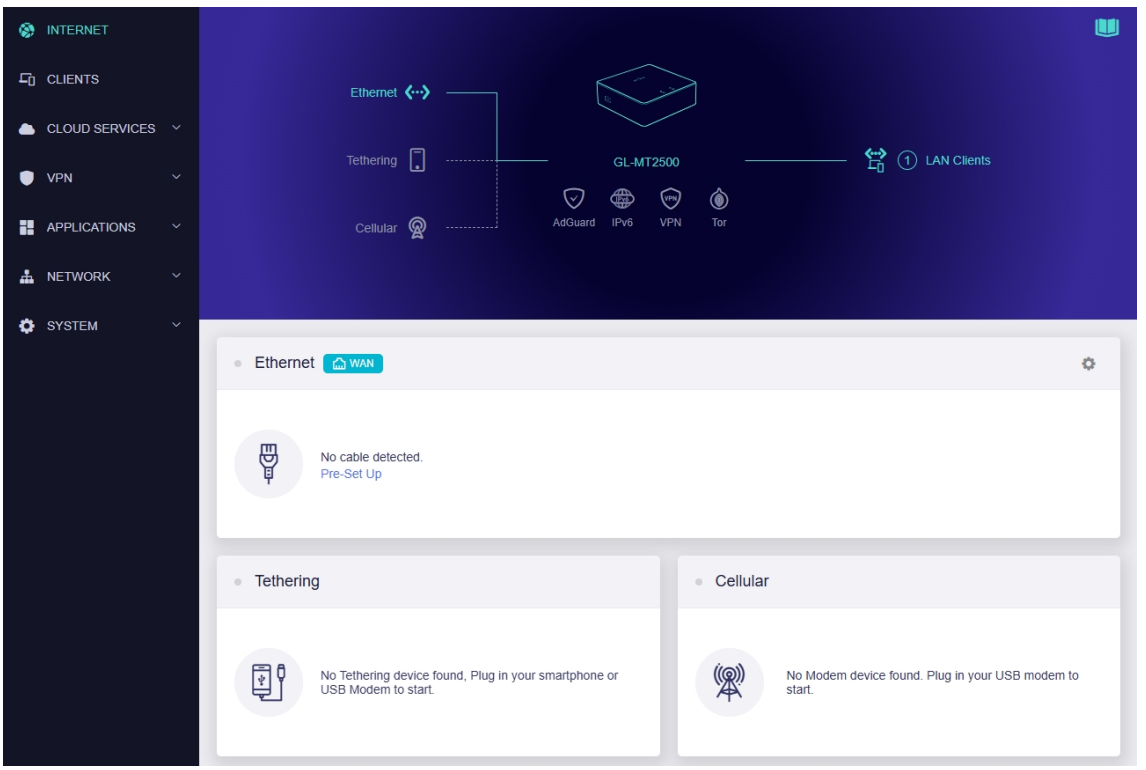
Iniciar sesión en el enrutador

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 Windows, Mac sistema operativo o sistema operativo Linux con un navegador web, como Microsoft Edge, Google Chrome, Mozilla Firefox o Apple Safari.

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

1. Conecte un dispositivo (por ejemplo, una computadora o computadora portátil) al puerto LAN del Brume 2 con un cable Ethernet. 'puerto LAN con un cable Ethernet.
2. Abra un navegador web (se recomiendan Chrome y Edge) y visita 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 Brume 2'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 Usar el asistente de configuración rápida

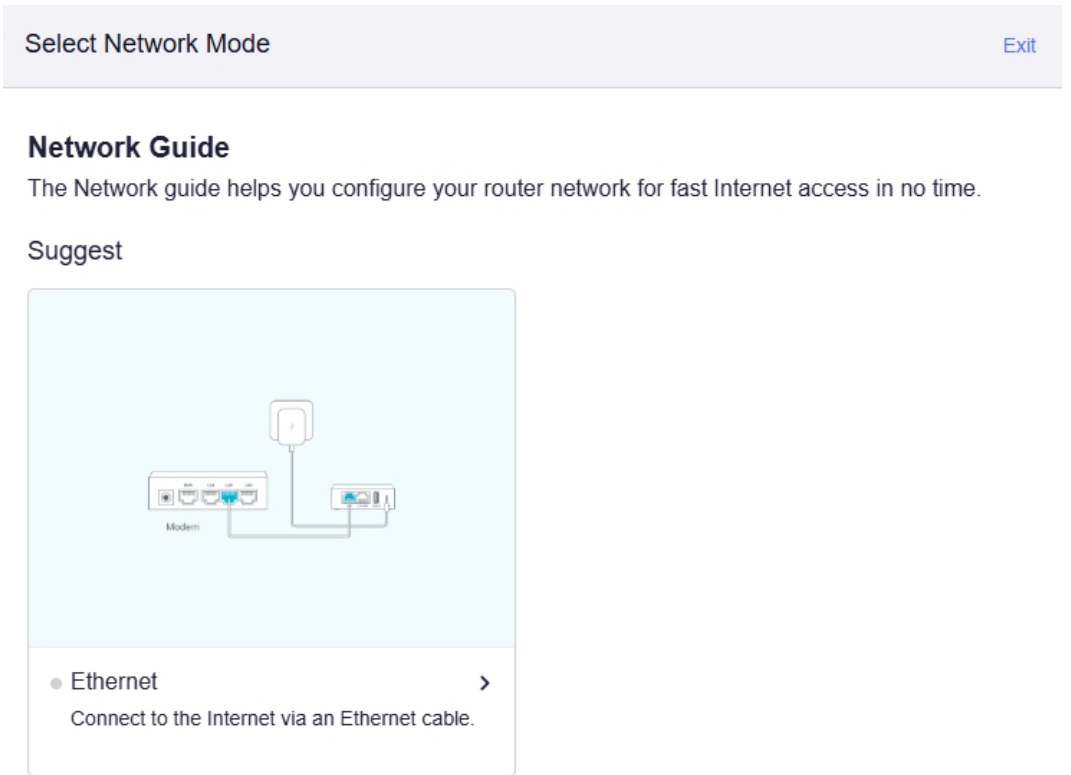
El El asistente de configuración basado en web lo guiará a través de la configuración de red del enrutador.

Siga los pasos a continuación para iniciar el asistente.

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



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



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 de red avanzada para requisitos específicos y verificar o modificar las conexiones existentes según sea necesario.

Brume 2 admite tres métodos de conexión a Internet: Ethernet, Anclaje a red USB y módem/celular USB. Celija el método apropiado según sus necesidades de uso.

1. **Ethernet (RJ45)**: conecte el enrutador a una red de banda ancha usando an 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. **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.

3. **Módem/celular USB (USB Modem/Cellular)**: inserte un módem celular USB con una tarjeta SIM preinstalada en el enrutador. Luego, el enrutador se conectará a Internet a través de redes móviles 4G/5G, proporcionando conectividad independiente de la banda ancha de línea fija. Este método ofrece alta movilidad y es adecuado para escenarios como el uso en vehículos o actividades al aire libre.

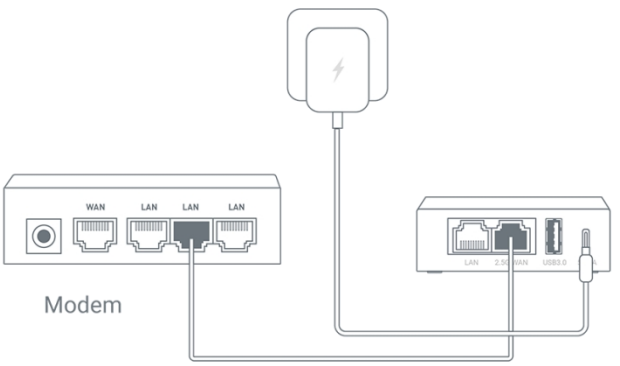
4.2.1 Conectarse a Internet mediante un cable Ethernet

Conecte el enrutador a una red de banda ancha usando an 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. This method ofrece alta estabilidad y alta velocidad, lo que lo hace ideal para entornos domésticos y de oficina con acceso de banda ancha fija.

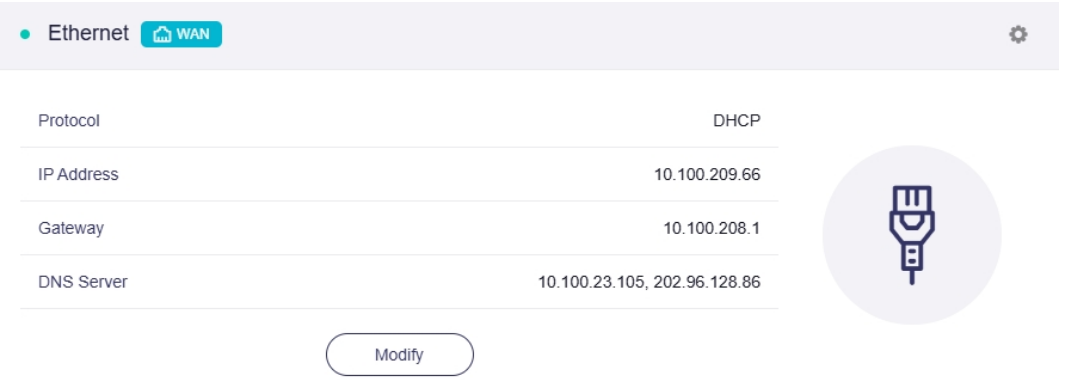
Configuración básica

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.

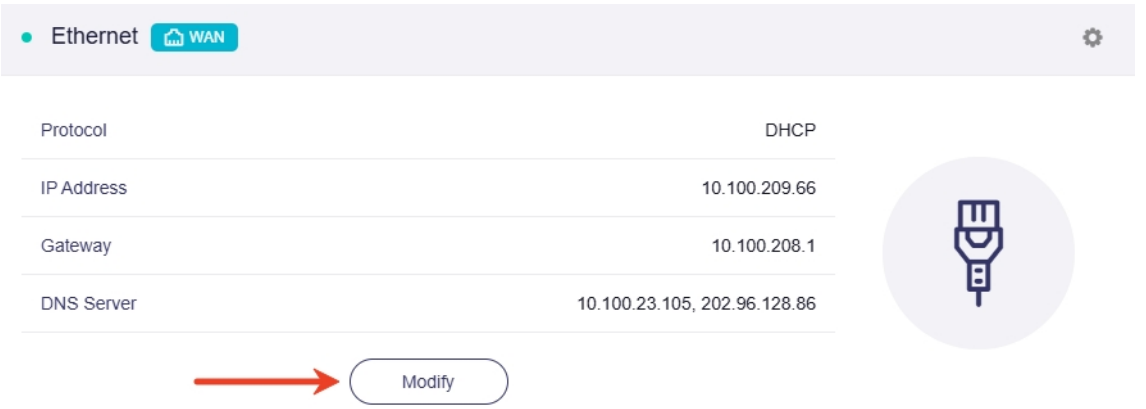


2. Inicie sesión en el enrutador'panel de administración web y naveguen a **INTERNET** > **Ethernet**. Si la conexión se realiza correctamente, sección Ethernet mostrará detalles de la red, incluidos protocolo, dirección IP, puerta de enlace, y DNS Servidor.



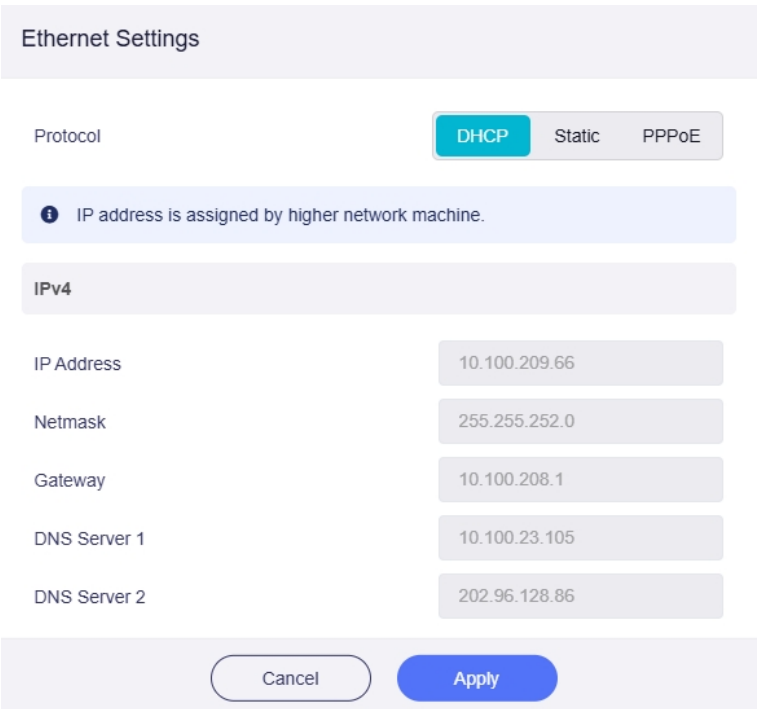
Protocolo

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



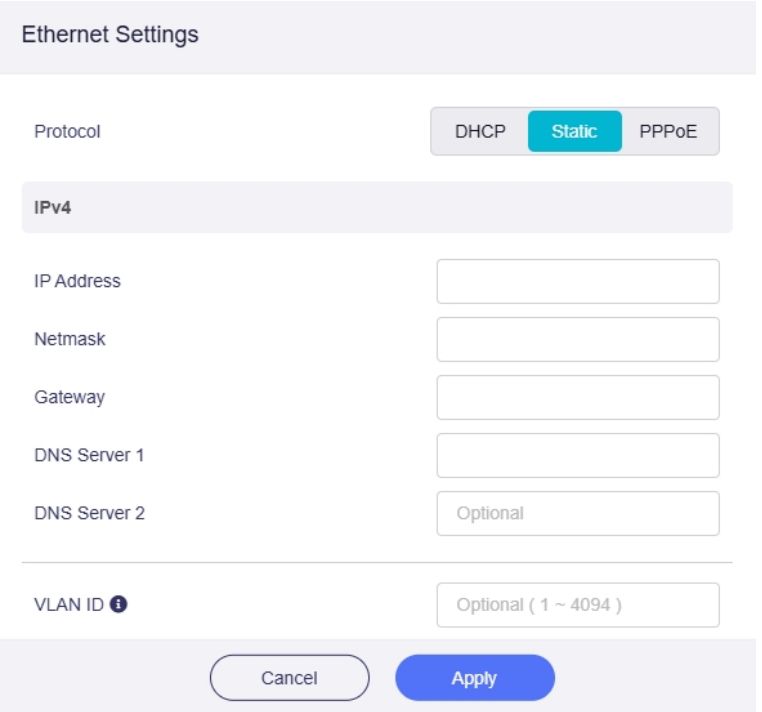
- **DHCP**

  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.



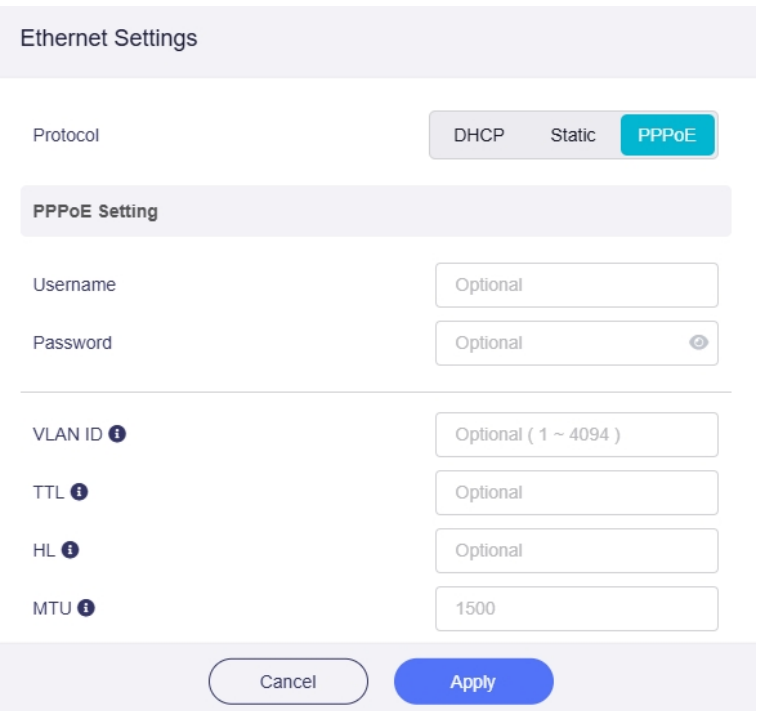
- **Estática**

  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).



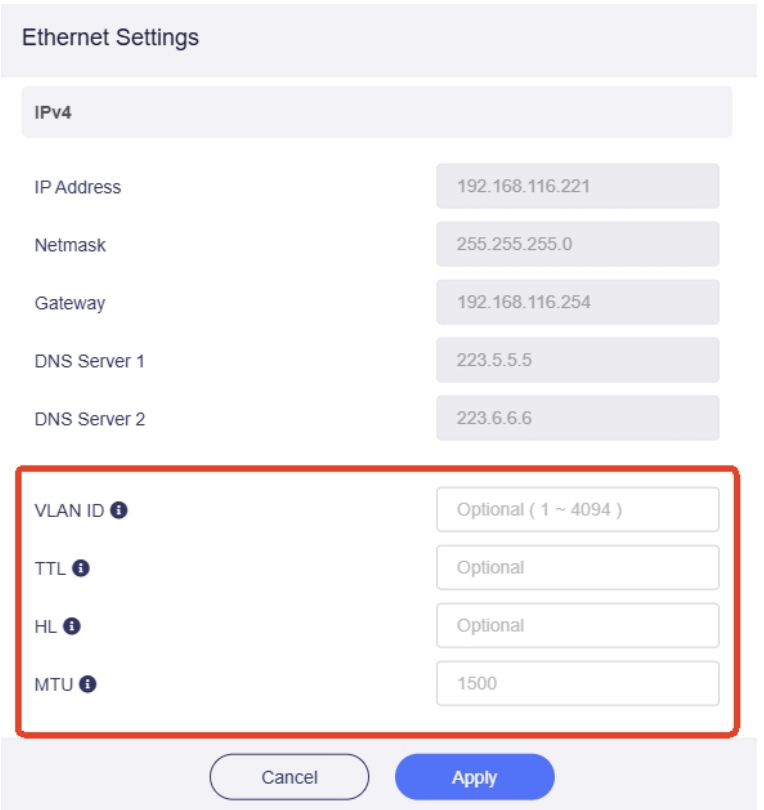
- **PPPoE**

  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, que son necesarios para configurar una conexión a Internet.



Configuración avanzada

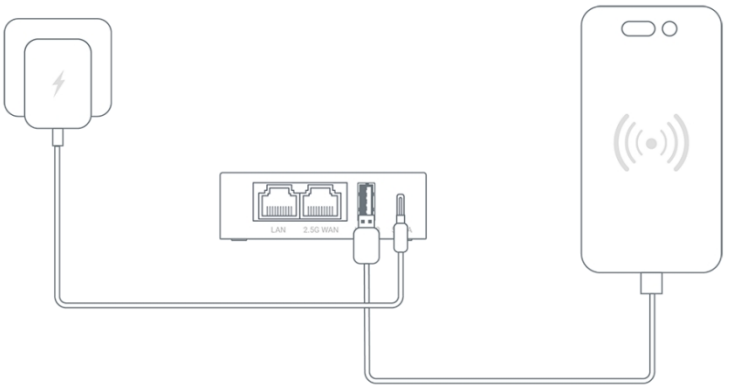
Además de las configuraciones esenciales, también hay algunas configuraciones avanzadas opcionales para arriba tres protocolos.



- **ID de VLAN**
  Esta configuración es necesaria solo si el servidor del proveedor requiere que la interfaz utilice una ID de VLAN etiquetada específica.
- **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 el cambio automático. decremento. TTL es válido solo para IPv4.
- **HL**
  En IPv6, el campo HL (límite de salto) 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 conexión compartida por USB

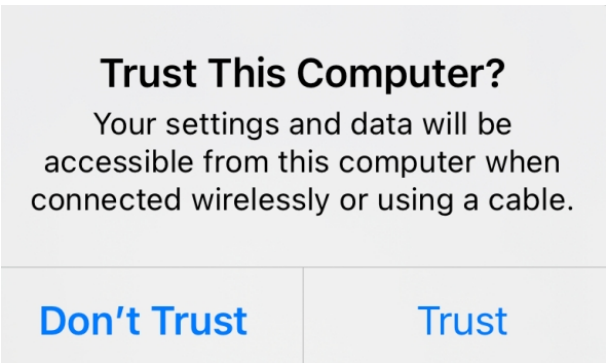
Cconexión de un inteligenteteléfono al enrutador a través de un cable USB se llama Tethering, que puede compartir la red de datos móviles del dispositivo (por ejemplo, 4G/5G) con el enrutador. Éste es un método para iacceso a Internet, especialmente cuando al aire libre o en áreasin fijo banda ancha.



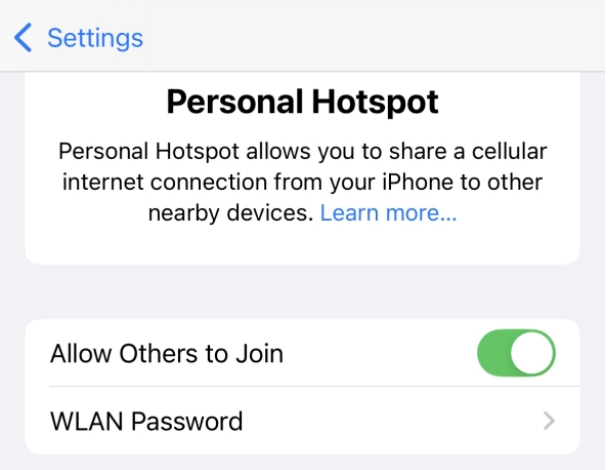
El módem sin host también funciona en Tethering durante la configuración del módem.
Nota: Algunos dispositivos móviles Los operadores limitan o cobran más por la conexión. Recomendamos consultar con su operador.

Conexión compartida desde un iPhone

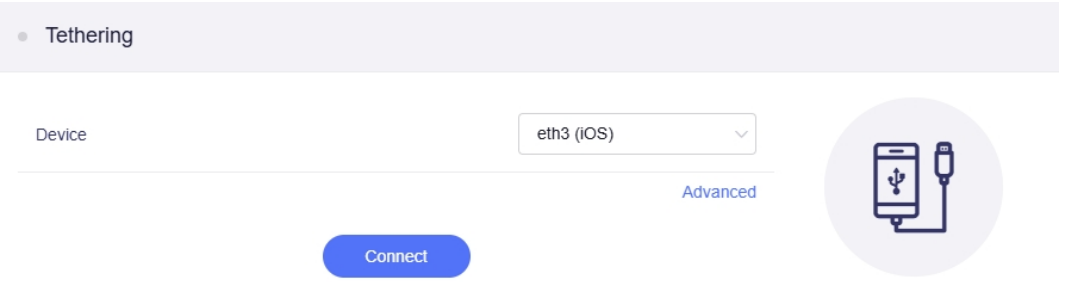
1. Conecte un iPhone al puerto USB del enrutador usando un cable USB. Aparecerá un cuadro de diálogo del sistema preguntando si se debe confiar en el dispositivo. Toque **Confiar** para continuar.



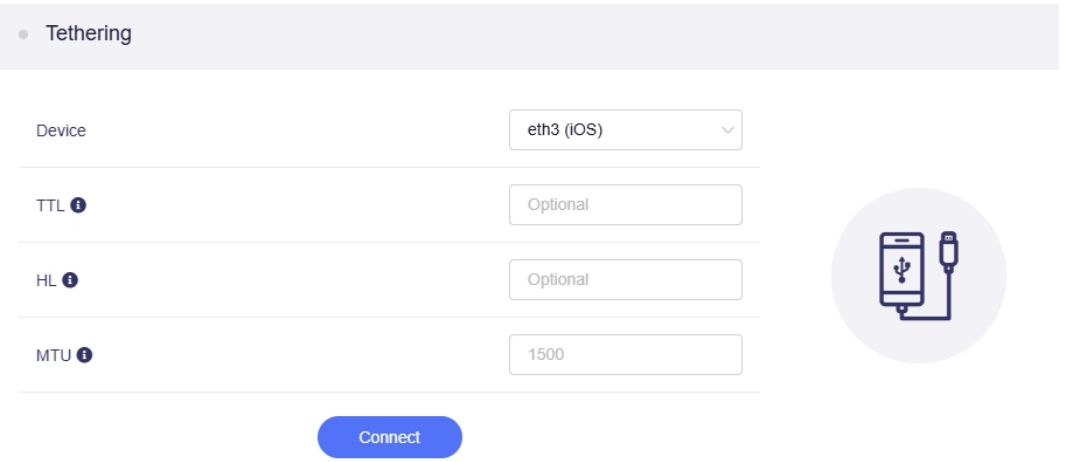
2. Ir a iPhone **Configuración** > **Punto de acceso personal**. Activar **Permitir que otros se unan**.



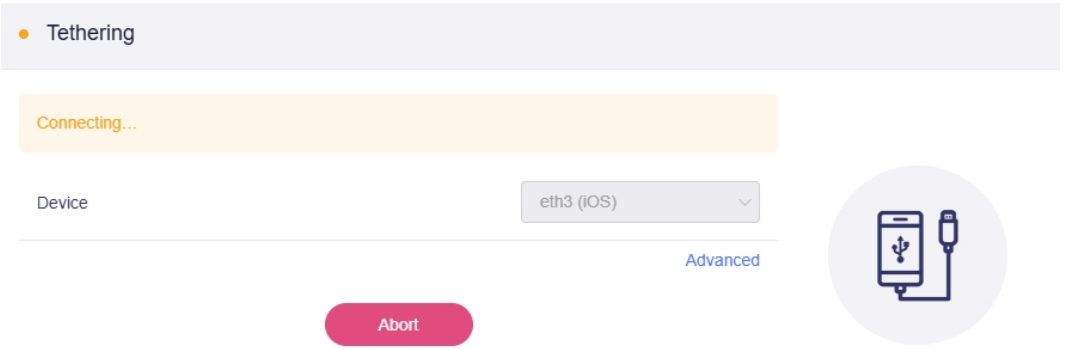
3. Conecte una computadora u otro teléfono al enrutador. Inicie sesión en el enrutador's web admin panel y navega hasta **INTERNET** > **Conexión**, luego haz clic **Conectar**.



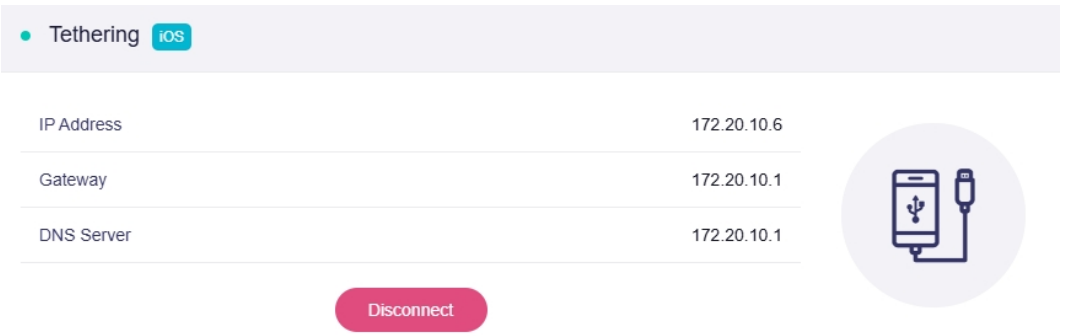
Si necesita establecer configuraciones avanzadas, como TTL, HL y MTU, haga clic **Avanzado** para personalizar estas configuraciones antes de hacer clicing **Conectar**.



4. Comenzará a conectarse.

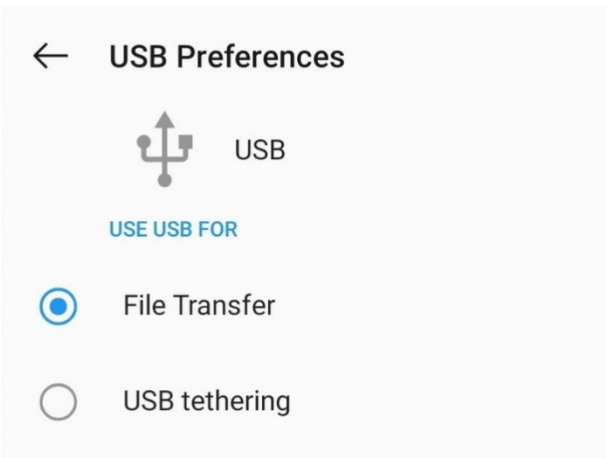


Una vez conectado, thesta página mostrará el Conexión de anclaje a red detalles.

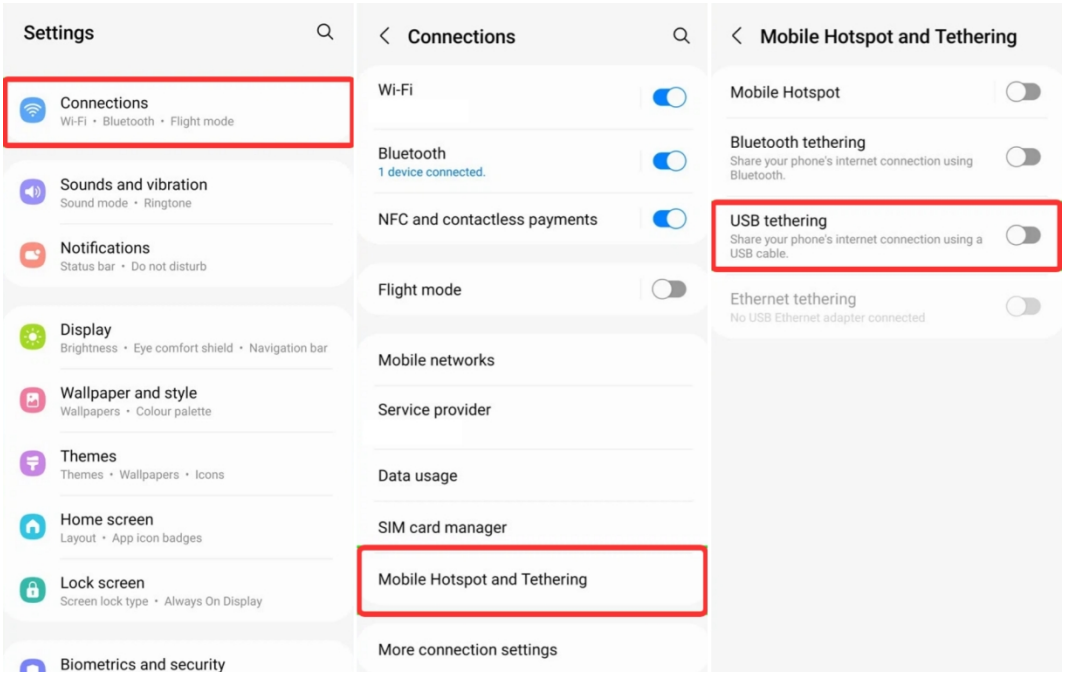


Conexión compartida desde Android

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

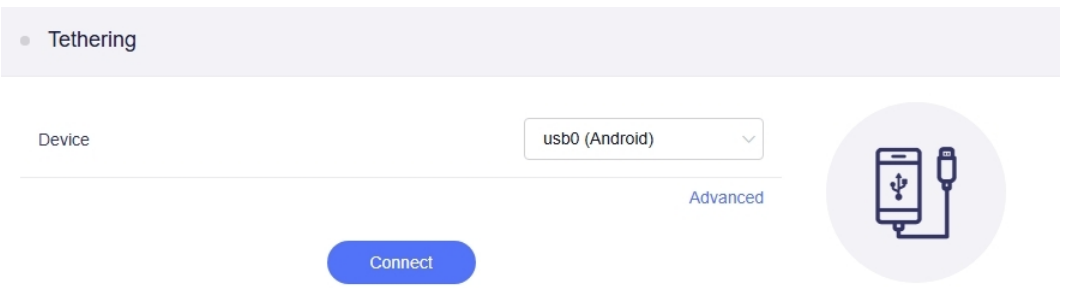


2. Vaya a la **Configuración** > **Red e Internet** > **Punto de acceso personal**. Activar **Personal Punto de acceso** o **Anclaje a red USB**.

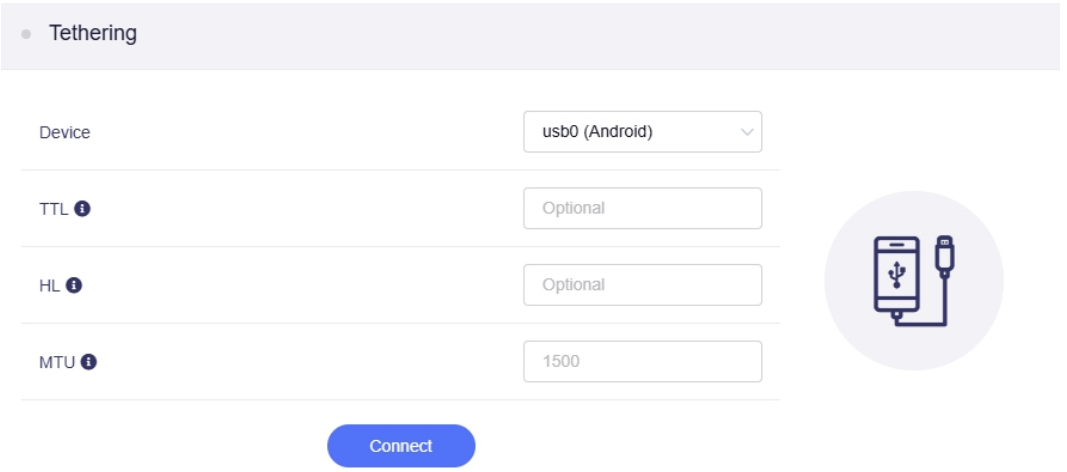


(Los pasos para habilitar el Anclaje a red USB varían según la marca. Verifique la configuración de su dispositivo para conocer la ubicación exacta y comuníquese con el soporte técnico del fabricante si es necesario).

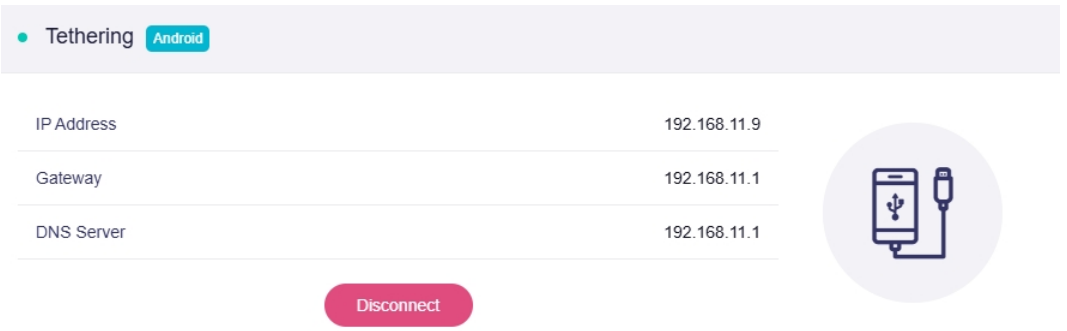
3. Conecte una computadora u otro teléfono al enrutador, luego inicie sesión a el panel de administración web del enrutador, navegue a **INTERNET** > **Anclaje a red**. Click **Conectar**.



Si necesita establecer configuraciones avanzadas como TTL, HL y MTU, haga clic **Avanzado** para personalice esta configuración antes de hacer clic **Conectar**.



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



Solución de problemas

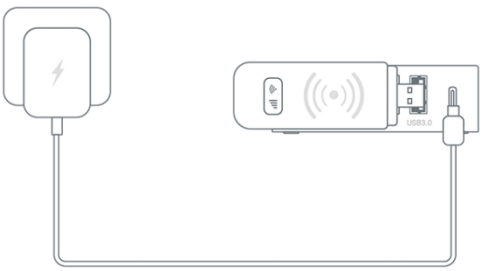
Si falla la conexión , intenta estos pasos para solucionar el problema:

- Utiliza la fuente de alimentación original para el enrutador.
- Desenchufa y vuelva a enchufar el cable USB.
- Utilice otro cable USB. Asegúrese de que admita la transferencia de datos (no solo la carga).
- Desactive y active "Anclaje a red USB" unas cuantas veces (para teléfonos Android).
- Desactive y active "Permitir que otros se unan" unas cuantas 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.

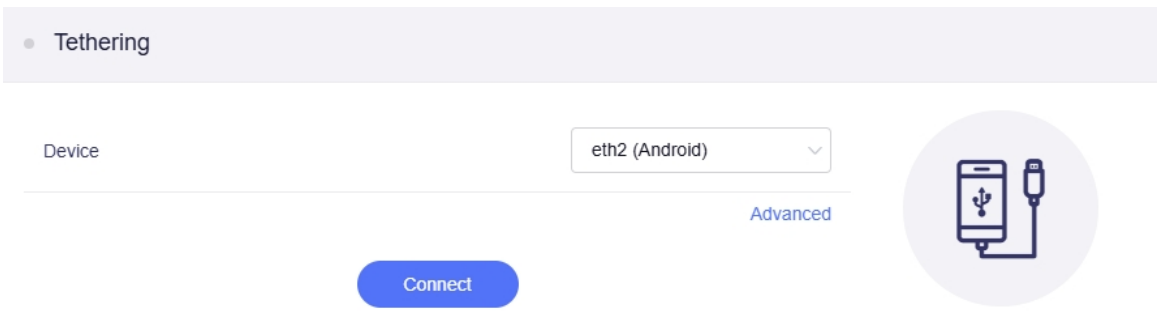
4.2.3 Conectarse a Internet mediante un módem USB

Conecte el enrutador a Internet insertando un módem USB con capacidad celular en su puerto USB. 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 de la interfaz Tethering o Cellular del enrutador. 'Interfaz de anclaje a red o celular.

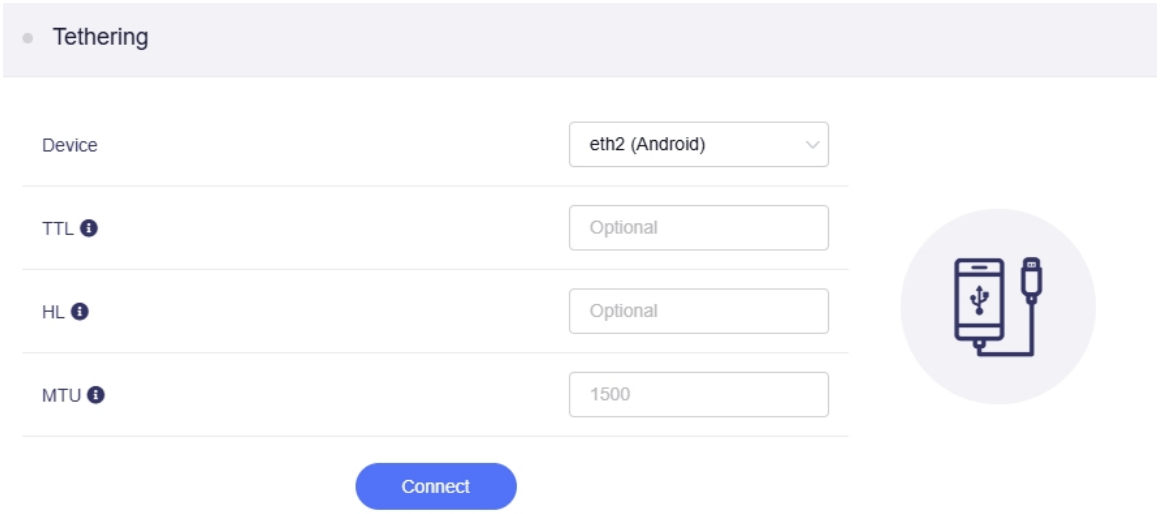


Siga los pasos siguientes para conectar su enrutador a Internet a través de un módem USB.

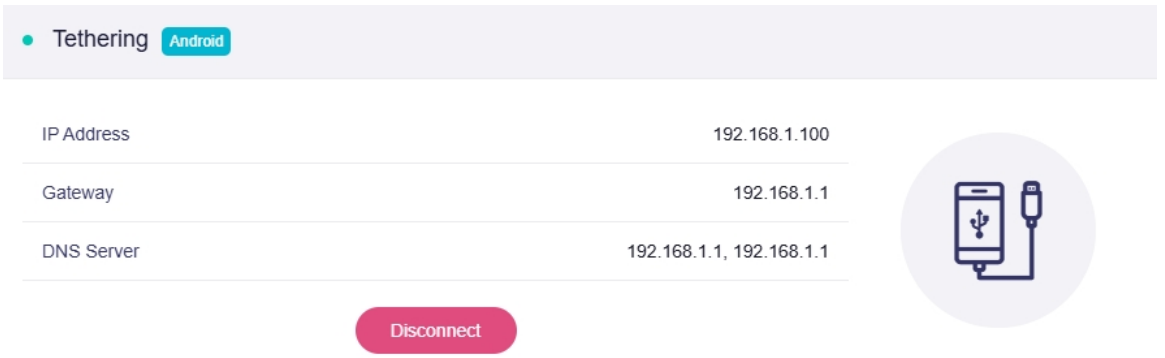
1. Pconecte un módem USB con una tarjeta SIM preinstalada al puerto USB del enrutador' antes de encenderlo. en.
2. Inicie sesión en el enrutador's web admin panel, navegue hasta **INTERNET** > **Conexión** y luego haga clic en **Conectar**.



Si debe establecer configuraciones avanzadas, como TTL, HL y MTU, haga clic **Avanzado** para personalizar estos configuración, luego haga clic en **Conectar**.

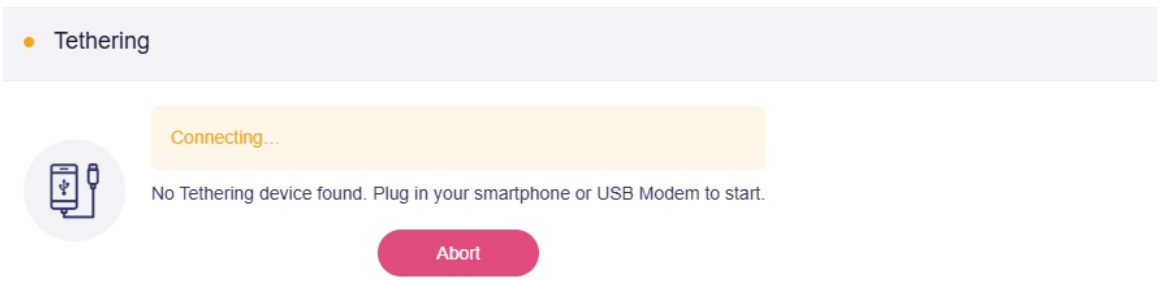


3. Comenzará a conectarse. Una vez conectado, esta página mostrará los red detalles.



Consejos:

1. Después de la configuración inicial, si reinicia el enrutador con el módem USB aún conectado, o re-inserte el módem en el enrutador, el USB módem será automáticamente reconocido, y una conexión de red establecerá sin volver a hacer clic en "Conectar".
2. Si desconecta el módem USB, la página mostrará el estado que se muestra a continuación, indicando “No se encontró ningún dispositivo de anclaje a red”, mientras que la interfaz de anclaje a red permanecerá en el estado “Conectando”.



Capítulo 5

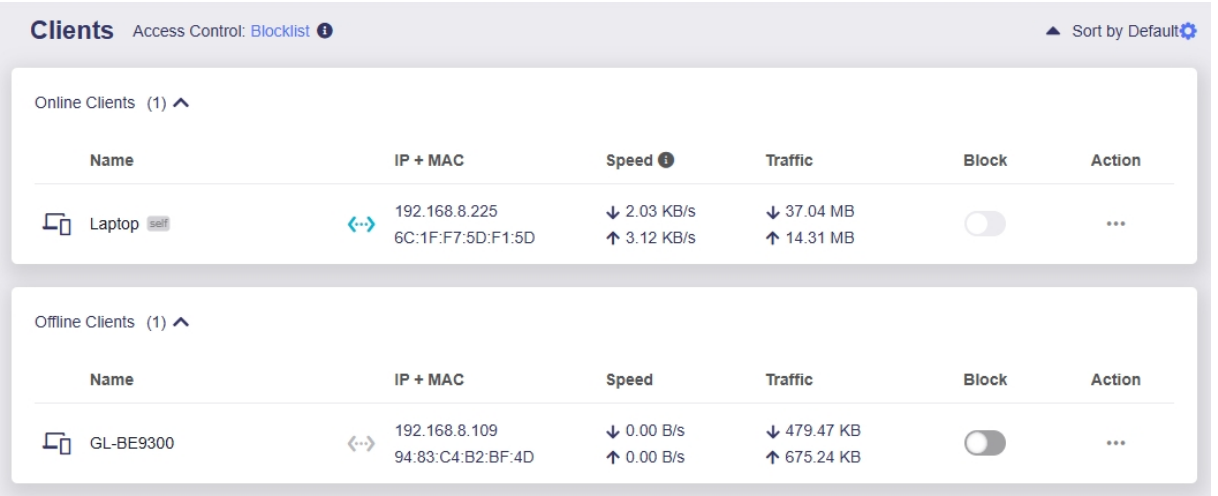
Clientes

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 navega hasta **CLIENTES**.

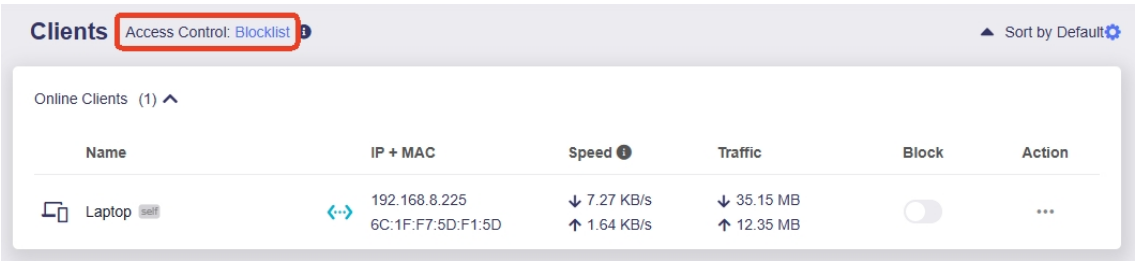
La página Clientes muestra información sobre los dispositivos conectados, incluido el nombre del dispositivo, el tipo de conexión, la dirección IP y MAC, la velocidad y el tráfico, ordenados de izquierda a derecha. También proporciona acceso rápido a reservar IP, bloquear cliente o realizar otras acciones.

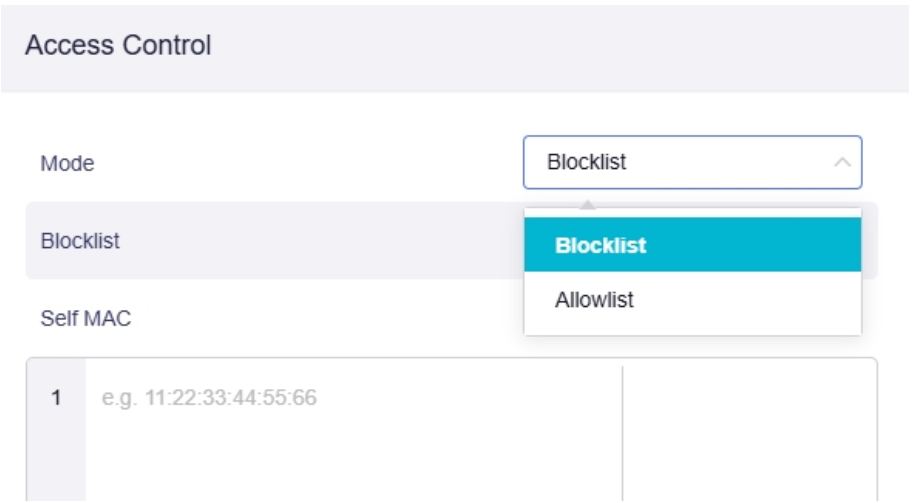
5.1 Detalles del dispositivo



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, indicaing que el dispositivo esté conectado al enrutador a través de un Ecable thenet.
2. **Dirección IP y MAC**
   La segunda columna enumera las direcciones IP y MAC del dispositivo conectado.
3. **Velocidad**
   La tercera columna muestra la velocidad de Internet del dispositivo conectado. Thes velocidad representa la velocidad promedio durante los últimos 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 del dispositivo conectado.
5. **Bloquear**

En la quinta columna, puede bloquear un dispositivo conectado específico con un clic. La regla de control de acceso es Lista negra de forma predeterminada y puede cambiarla a Lista permitida desde la parte superior según sea necesario.



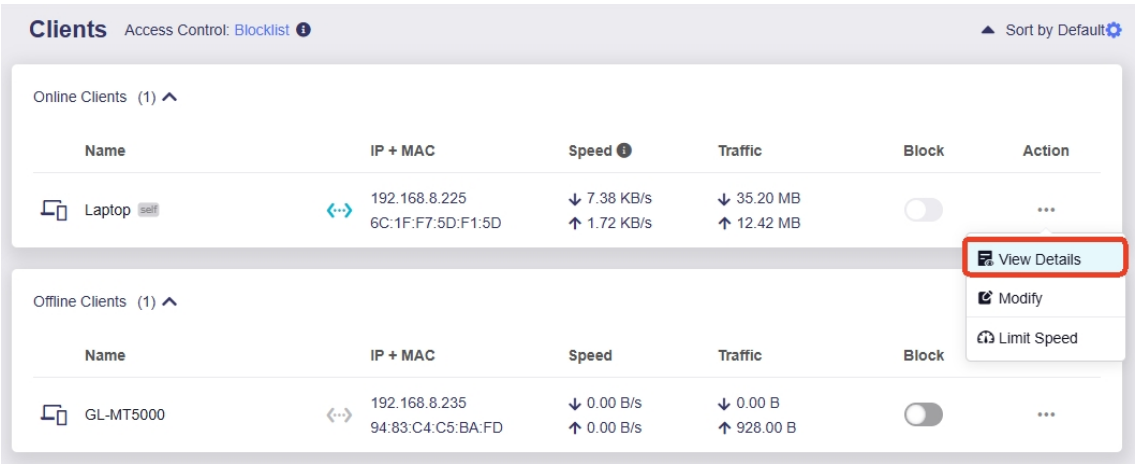


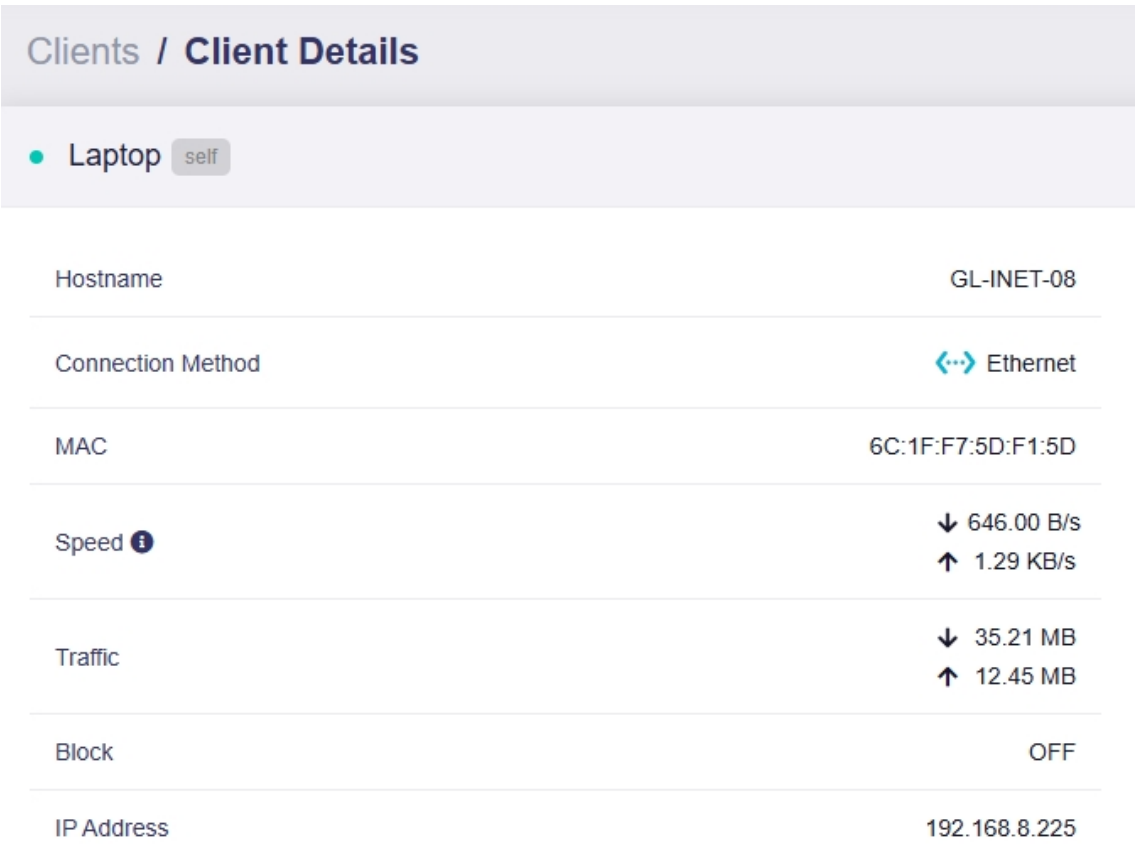
- **Lista negra**: dispositivos con direcciones MAC en blacklist no pueden conectarse a este enrutador. Tenga en cuenta que el bloqueo del cliente se basa en la dirección MAC del dispositivo. Si el dispositivo bloqueado usa una dirección MAC diferente la próxima vez, aún podrá conectarse al enrutador.
- **Lista de permitidos**: solo los dispositivos con direcciones MAC específicas pueden conectarse a este enrutador, adecuado para dispositivos IoT y administración de redes empresariales.

5.2 Acción

1. **Ver detalles**

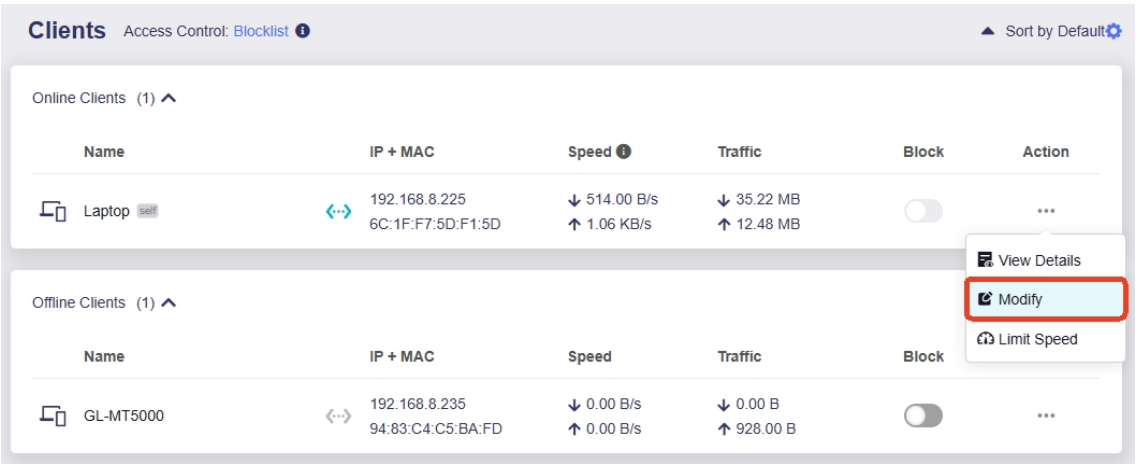
   Haga clic en el icono de tres puntos en la **Acción** columna y haga clic en **Ver detalles** en el menú desplegable para ver los detalles del dispositivo en una sola página.

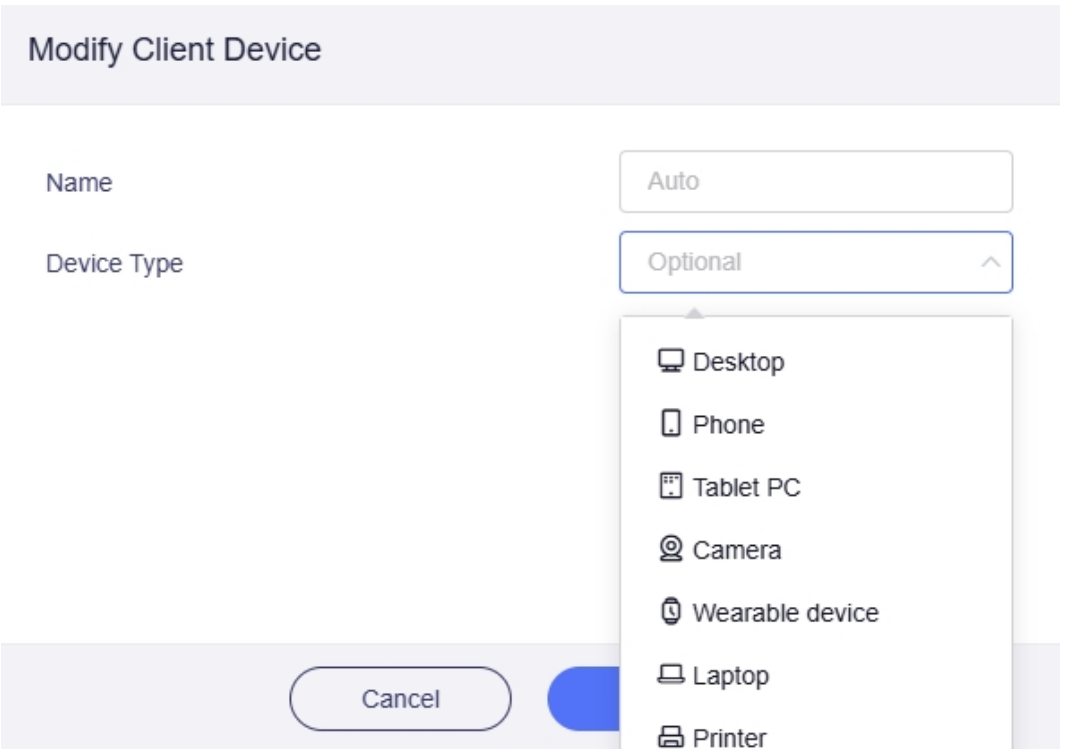




2. **Modificar**

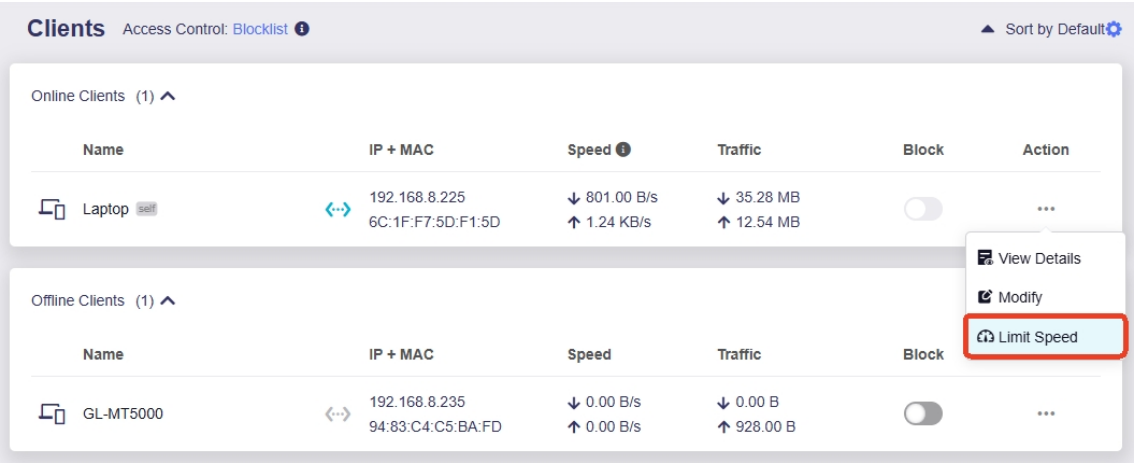
Haga clic en el icono de tres puntos en la columna **Acción** y haga clic en **Modificar** desde el menú desplegable para modificar el nombre y tipo del dispositivo.



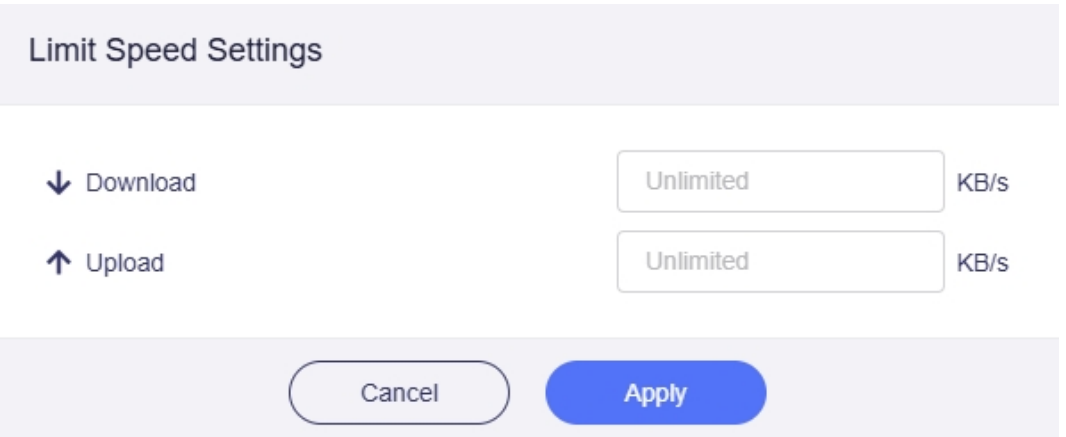


3. **Limitar velocidad**

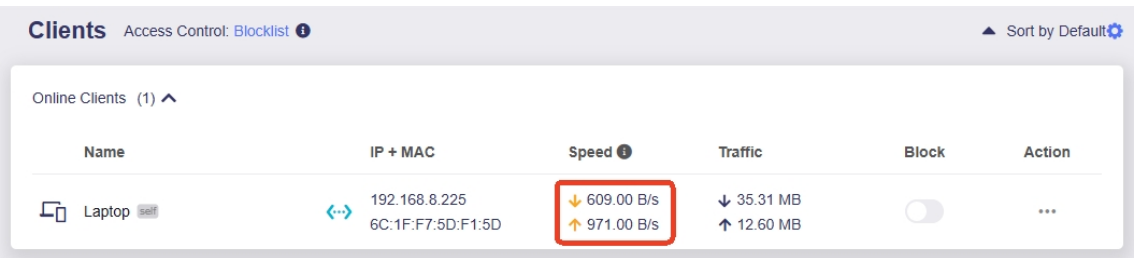
Haga clic en el icono de tres puntos en la **Acción** columna y haga clic en **Limitar velocidad** en el menú desplegable.



Podrás limitar la velocidad de un dispositivo conectado, con la unidad configurada en KB/s.



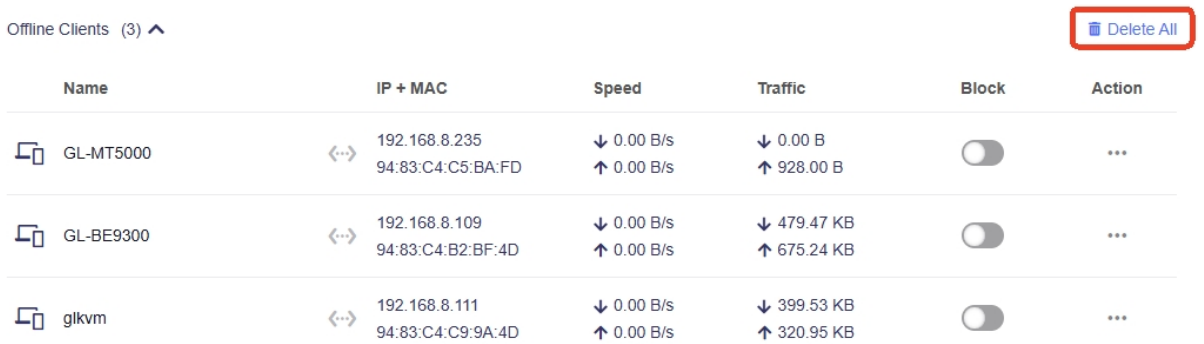
Si se ha aplicado una limitación de velocidad a un dispositivo, las flechas de velocidad de carga/descarga se volverán amarillas.



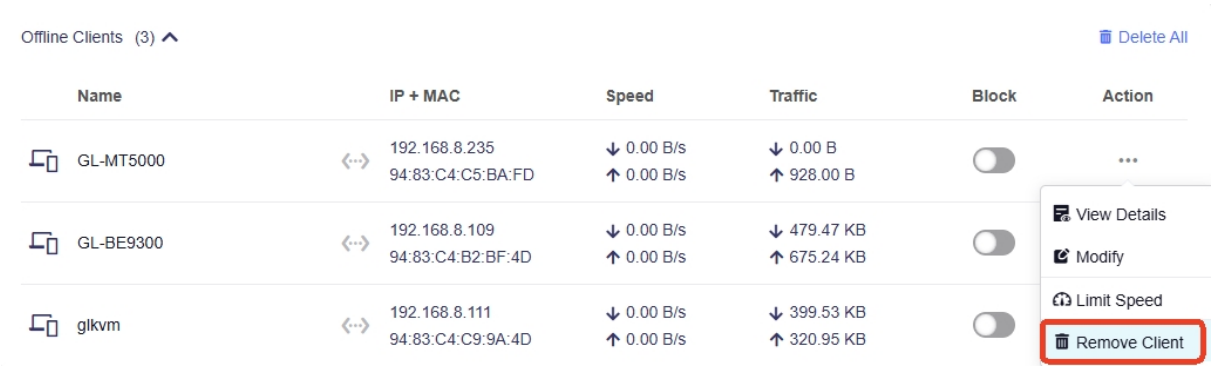
Consejo: Si la opción Limitar velocidad no está visible, vaya a **RED** > **Aceleración de red** y deshabilítela. La opción Limitar velocidad estará disponible.

5.3 Eliminar clientes

En el **Offline Cclientes** sección, puede hacer clic en **Eliminar Todo** en la esquina superior derecha para eliminar todos los clientes fuera de línea.

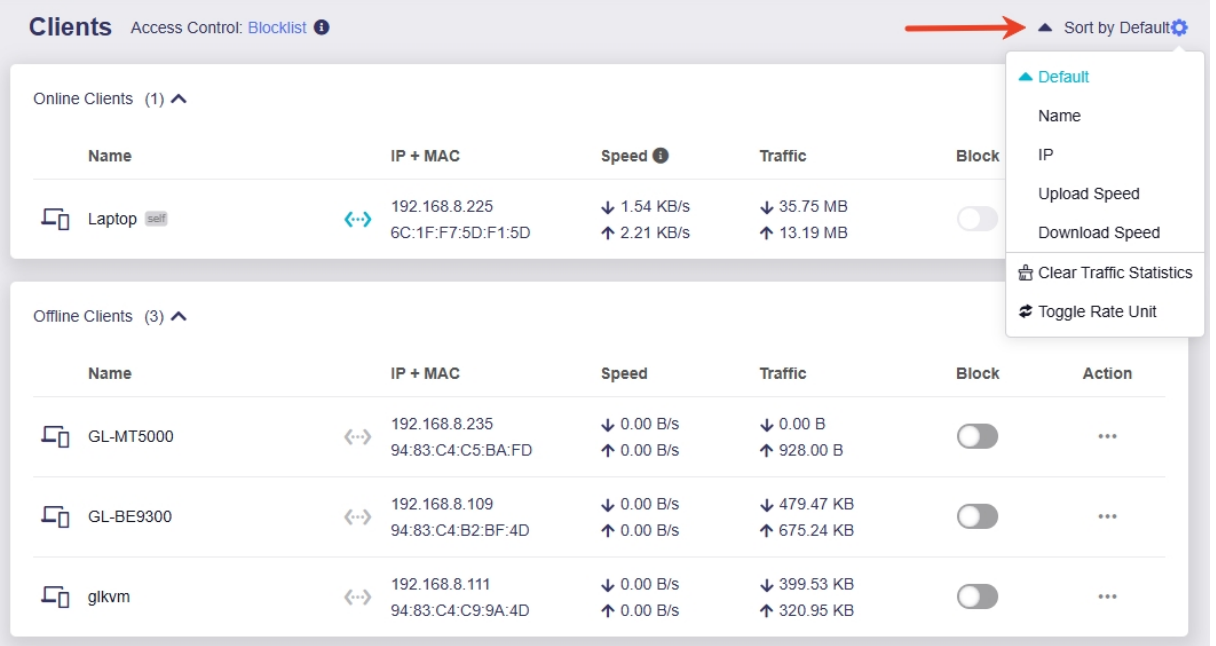


Si desea eliminar a cliente específico, haga clic en el ícono de tres puntos en la columna **Acción**, luego haga clic en **Quitar Cliente** desde el menú desplegable.



5.4 Ordenar

Puedes configurar la regla de clasificación del dispositivo para la página Cliente en la superior esquina derecha.



La clasificación predeterminadaing reglas son de la siguiente manera:

- El dispositivo propio (es decir, el dispositivo utilizado para acceder al enrutador’s panel de administración web) siempre aparece en primer lugar.
- En **Oen línea Clients**, los dispositivos aparecen en una lista superior si se conectaron antes.
- En el **Desactivadolínea Cclientes** sección, los dispositivos aparecen en una lista superior si desconectados anteriormente.

Capítulo 6

Servicios en la nube

Este capítulo presenta dos servicios en la nube: GoodCloud y AstroWarp.

6.1 GoodCloud

GL.iNet GoodCloud es una plataforma diseñado para simplificar la implementación y administración remota de dispositivos conectados. proporciona una forma sencilla 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 de lotes, como implementar configuraciones de red y realizar actualizaciones de software. 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.

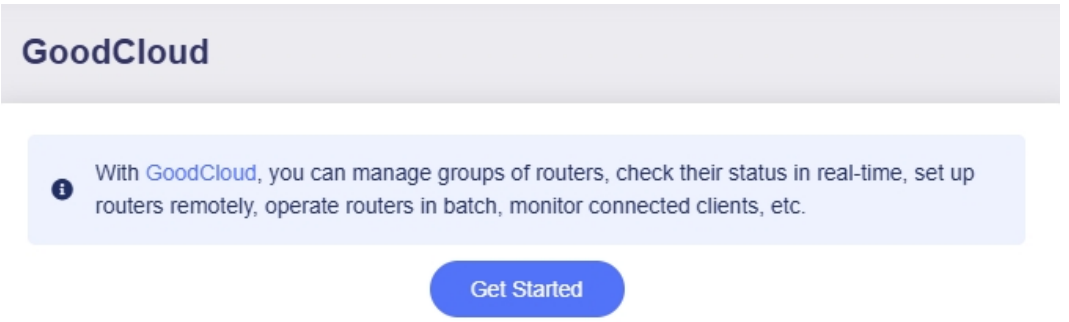
Con GoodCloud, puede:

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

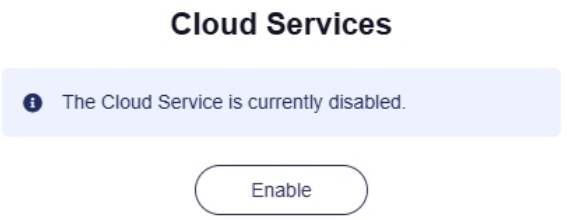
Algunas funciones están disponibles en el Plan Enterprise y el Plan VAR (revendedor de valor agregado). Consulte aquí para obtener más detalles.

6.1.1 Habilitar GoodCloud

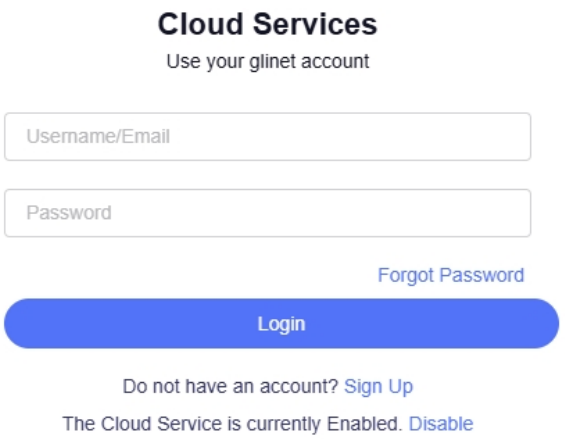
1. Inicie sesión en el panel de administración web de su enrutador', navegue hasta **SERVICIO EN LA NUBE** > **GoodCloud**, y click **Obtener Started.**



2. Aparecerá una ventana desplegable en la esquina superior derecha. Haga clic en **Habilitar**.



3. Log en con su cuenta GL.iNet Cloud. Si'no tienes una cuenta, regístrate para obtener una e inicia sesión. Una vez ha iniciado sesión, el enrutador se vinculará a su cuenta automáticamente.

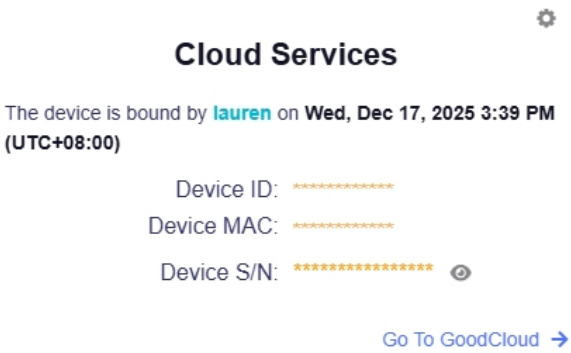


Consejos:

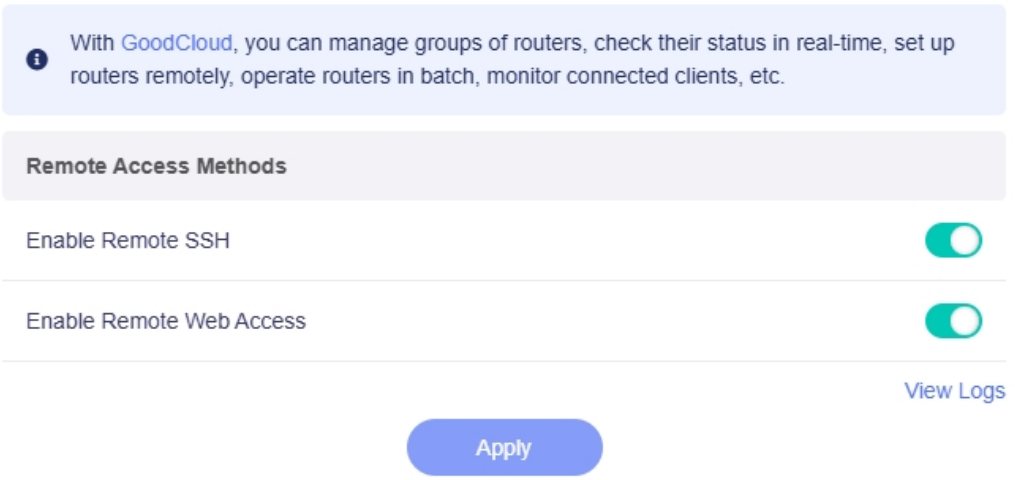
- Los pasos de vinculación de GoodCloud difieren según la versión del firmware.

- Si no recibe el correo electrónico de verificación, revise su carpeta de correo no deseado o vuelva a intentarlo más tarde. Para más ayuda, contáctenos en support@gl-inet.com.

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



5. Nnavegue a **SERVICIOS EN LA NUBE** > **GoodCloud** y habilite el acceso remoto. GoodCloud permite el acceso remoto al enrutador vinculado'. Esto es particularmente útil para la administración remota, configuración de red y resolución de problemas. Puede habilitar o deshabilitar el acceso remotopuedes habilitar o deshabilitar el acceso remoto para su enrutador aquí.



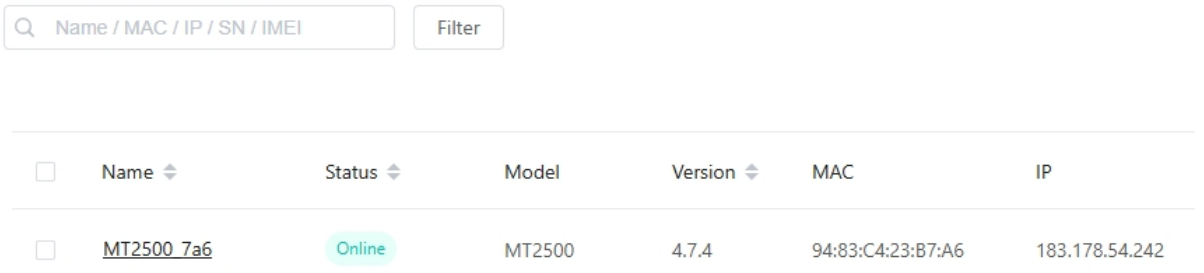
- **Acceso remoto SSH**: acceso remoto el terminal del enrutador desde GoodCloud usando SSH.

- **Acceso web remoto**: Remotely acceso a la web del enrutador admin panel desde GoodCloud a través de HTTP/HTTPS.
- **Ver registros**: Redirigir a la página de registro y mostrar la nube log.

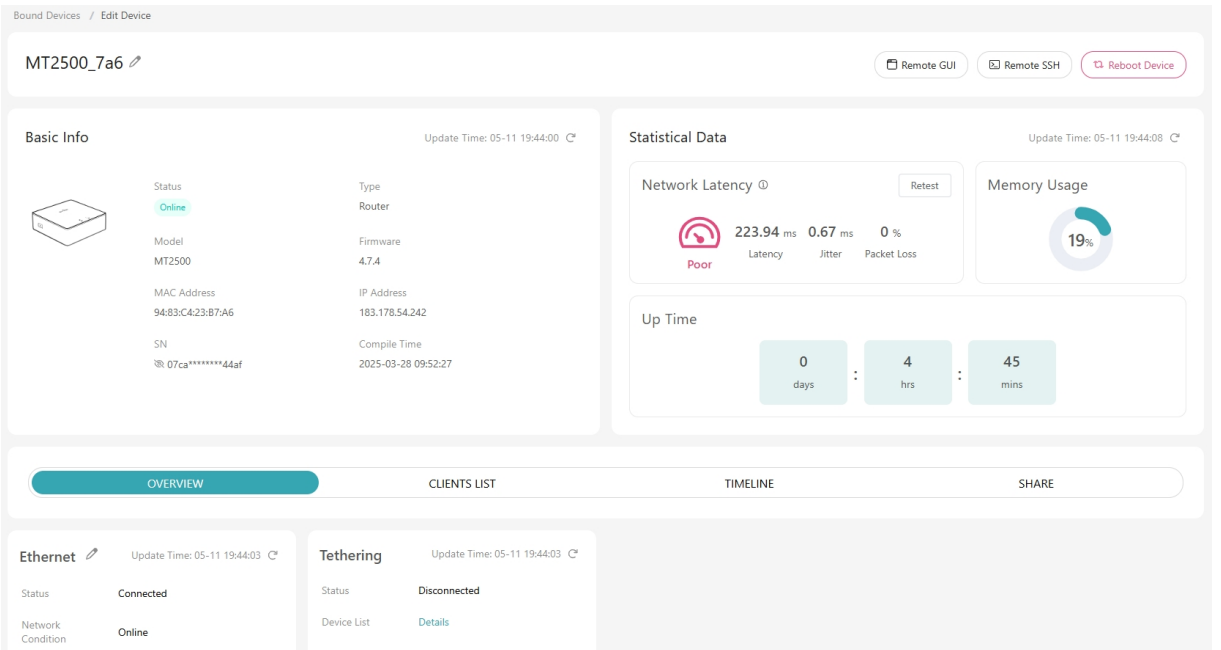
6.1.2 Administrar el enrutador

Consultar los detalles del dispositivo

Inicie sesión en el GoodCloud plataforma y navegue hasta **Dispositivo** > **Dispositivos vinculados**. You puede ver el dispositivo’s información básica, como el nombre del host, el estado (en línea/fuera de línea), el modelo, versión de firmware, y MAC dirección.

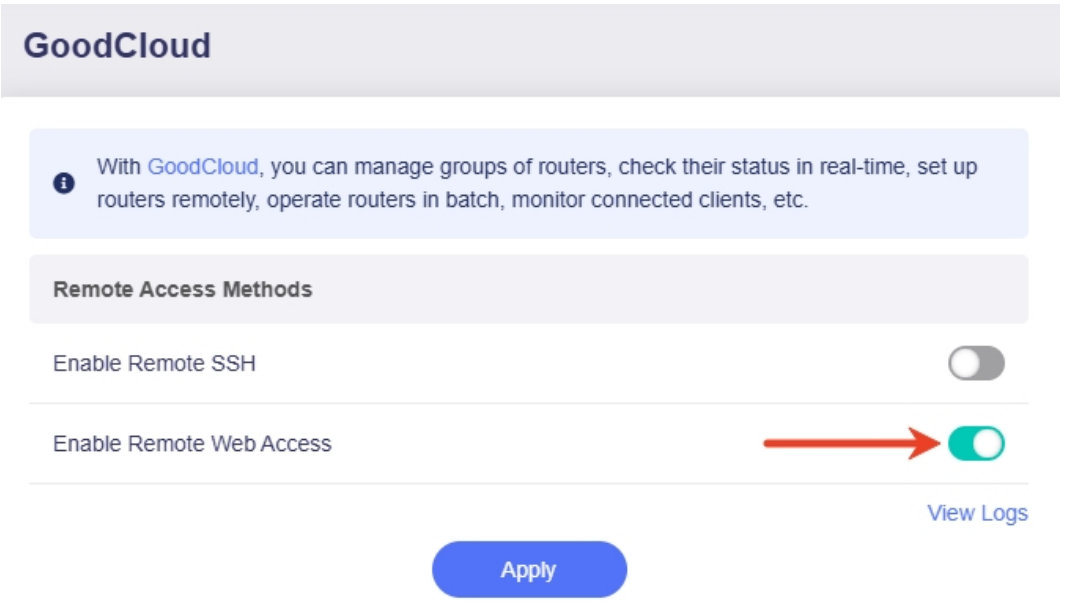


Haga clic en el nombre del dispositivo para ingresar a la página de detalles del dispositivo, que muestrainformación básica, datos estadísticos, descripción general de la red, lista de clientes y cronograma. También puede realizar operaciones avanzadas, como acceso remotolying al enrutador, y reiniciando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

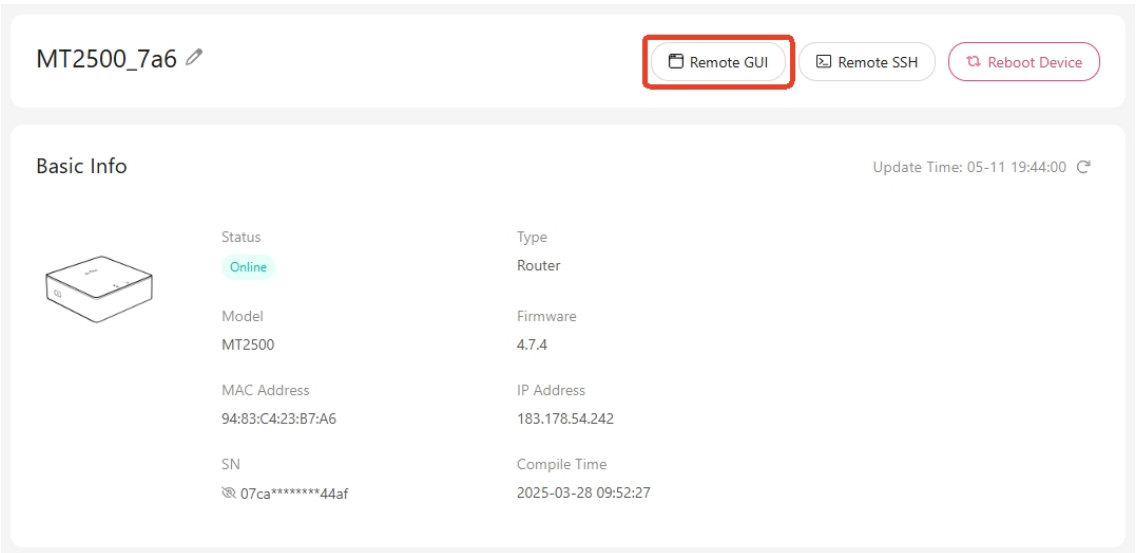


Acceso web remoto

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

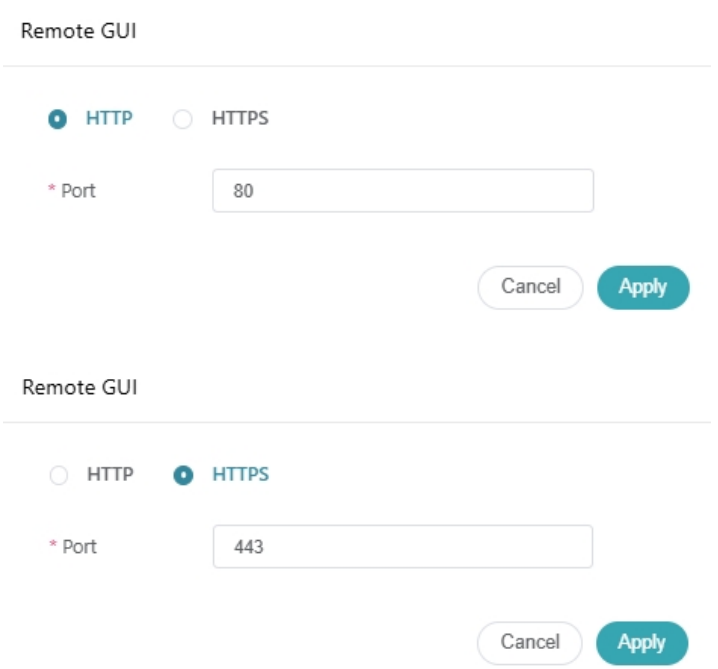


2. Inicie sesión en la plataforma GoodCloud y navegue hasta **Dispositivo** > **Dispositivos vinculados**. Haga clic en el dispositivo al que desea acceder e ingresará a la página de detalles del dispositivo.
3. En la página de detalles del dispositivo, haga clic en **Remoto GUI** botón en la esquina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

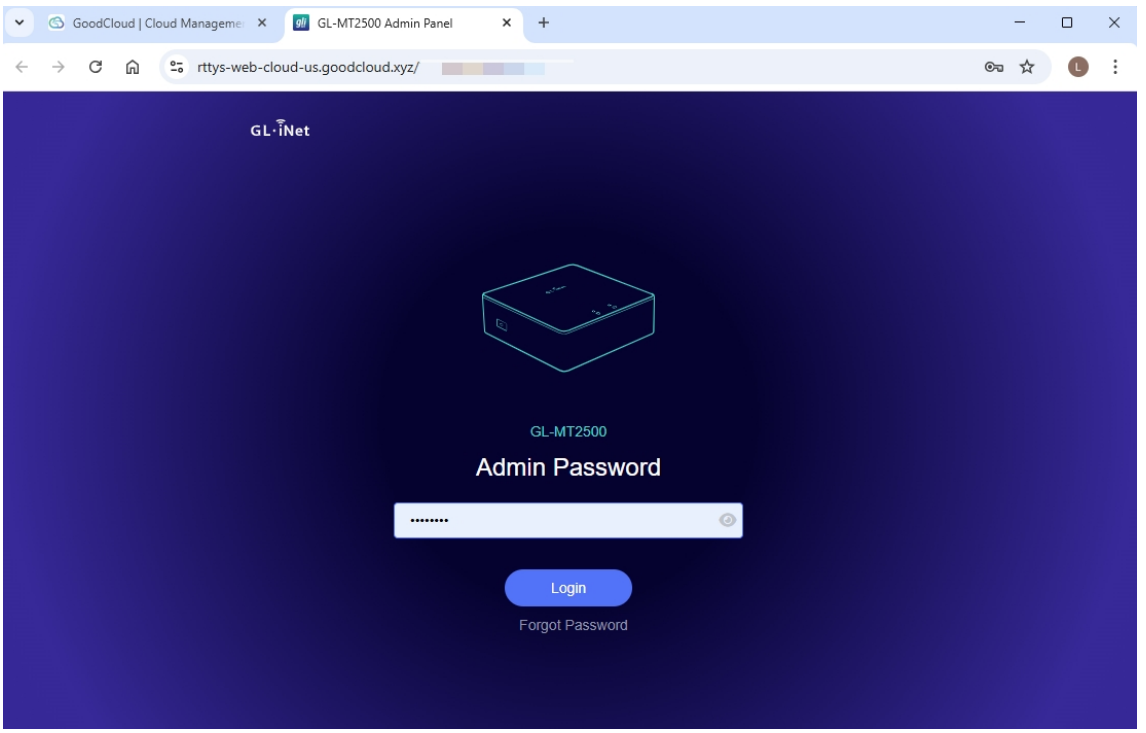


4. Seleccione el protocolo y el puerto de transferencia. Los valores predeterminados son **HTTP** y Puerto **80**. Puede cambiar el protocolo a HTTPSpuedes cambiar el protocolo a

HTTPS según sea necesario y el puerto cambiará automáticamente a 443. Luego haga clic en **Aplicar**.

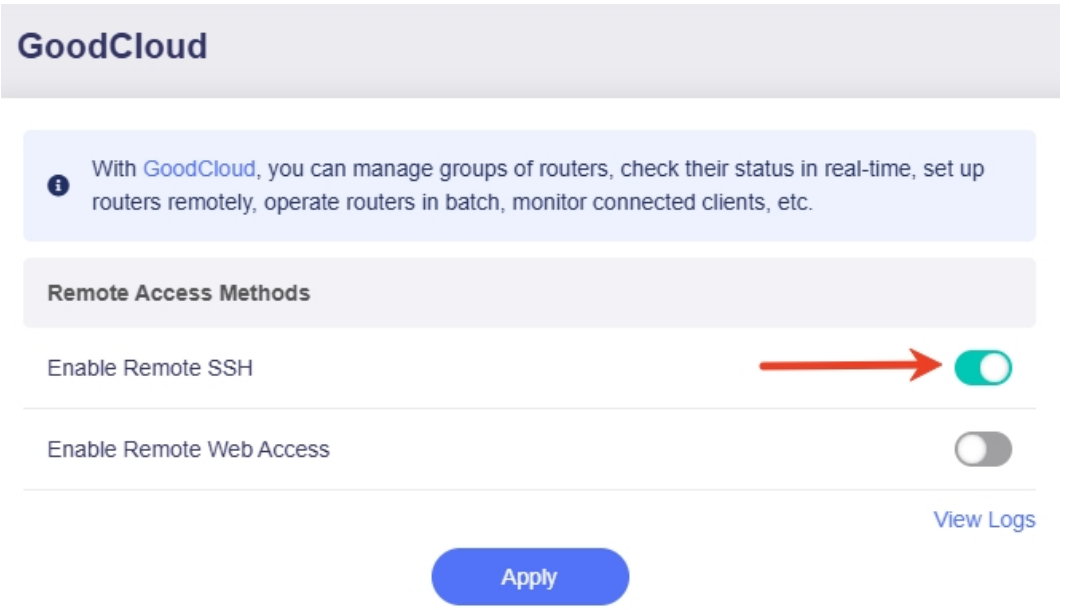


5. Será redirigido a la página de inicio de sesión del enrutador'. Ingrese la contraseña de administrador para acceder de forma remota al panel de administración web del enrutador'.

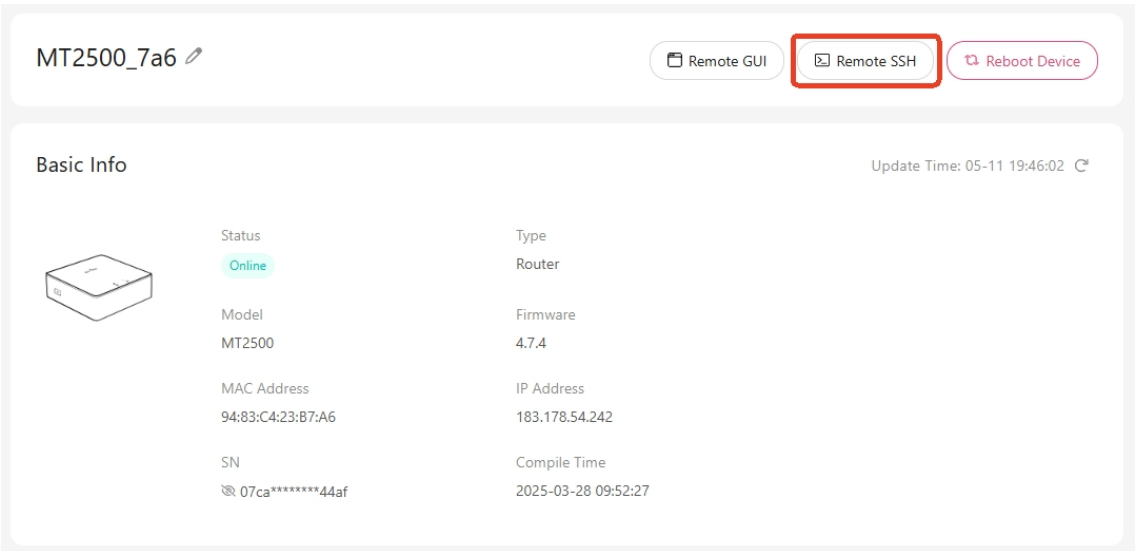


Acceso remoto al terminal

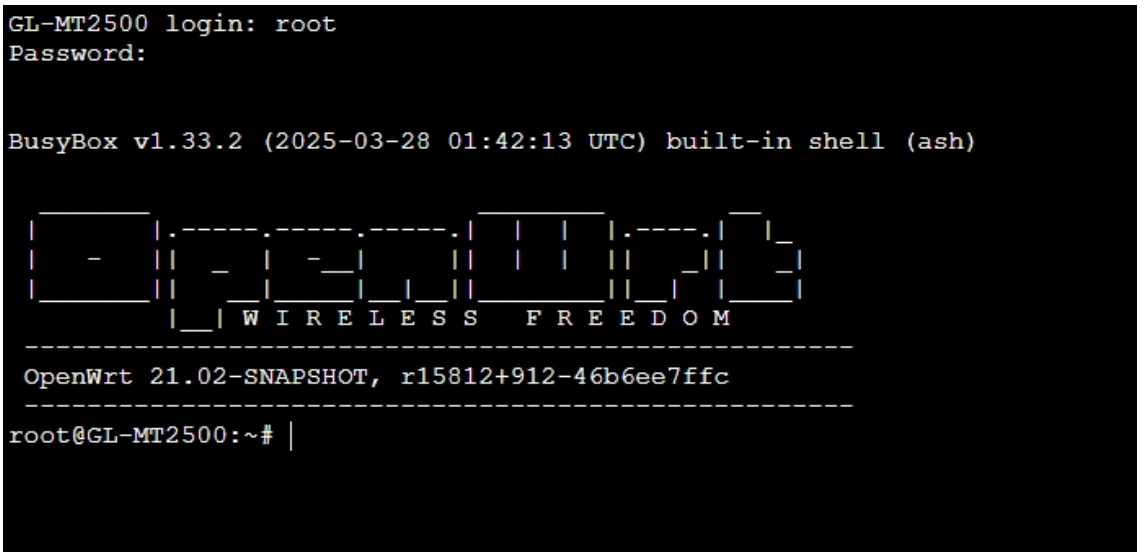
1. Inicia sesión en panel de administración web del enrutador', navegue hasta **SERVICIOS EN LA NUBE** > **GoodCloud**, habilite **Acceso remoto SSH**, luego haga clic en **Aplicar**.



2. Inicie sesión en la plataforma GoodCloud y navegue hasta **Dispositivo** > **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.

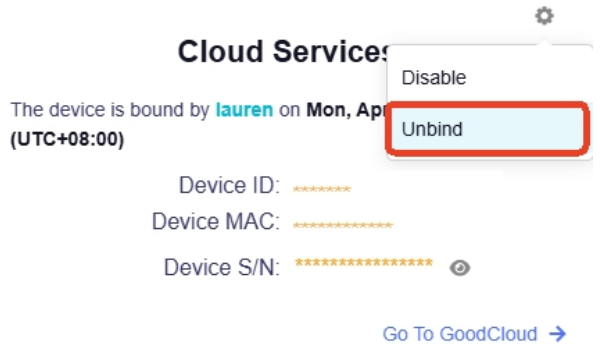


4. Inicie sesión como **root** e ingrese la contraseña para acceder al terminal de su enrutador.

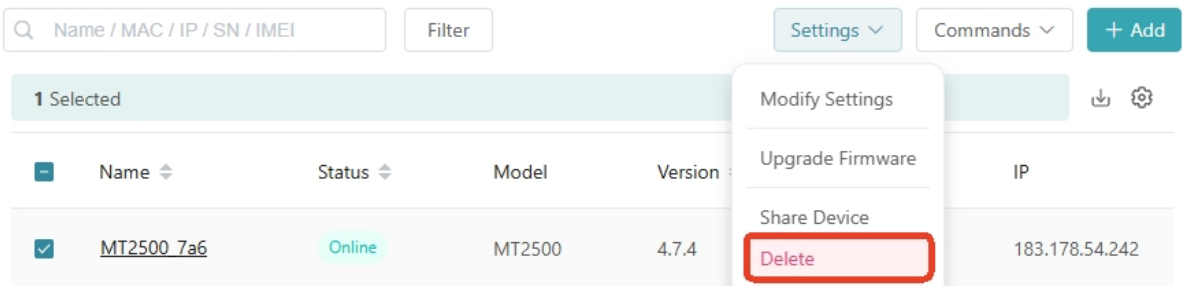

GL-MT2500 login: root
Password:
BusyBox v1.33.2 (2025-03-28 01:42:13 UTC) built-in shell (ash)
W I R E L E S S F R E E D O M
OpenWrt 21.02-SNAPSHOT, r15812+912-46b6ee7ffc
root@GL-MT2500:~#

6.1.3 Desvincular el dispositivo

En el panel de administración web del enrutador', haga clic en el icono de nube en el 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.

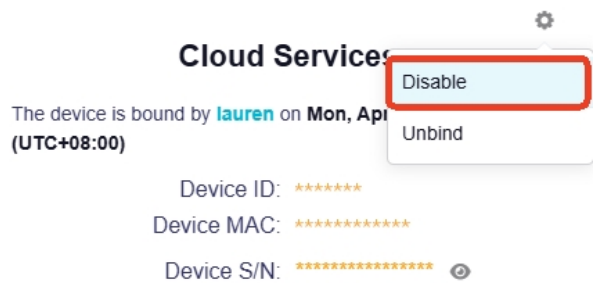


Como alternativa, inicie sesión en la plataforma en la nube y navegue hasta **Dispositivo** > **Bound Dispositivos**. Seleccione el dispositivo que desea desvincular, haga clic en **Configuración** en la esquina superior derecha y luego seleccione **Eliminar**. Su dispositivo se desvinculará. su cuenta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



6.1.4 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.



6.2 AstroWarp

AstroWarp es una plataforma de red avanzada diseñada para proporcionar redes remotas sin interrupciones y administración remota de dispositivos.

Creado específicamente para la integración del enrutador GL.iNet, AstroWarp admite la administración integral de dispositivos en redes completas, lo que permite el control superior e inferior del dispositivo.

Con un enfoque en la administración de toda la red y el soporte futuro para el control a nivel de hardware, AstroWarp ofrece una solución más sólida y confiable para administrar dispositivos y mantener redes seguras y estables.

Consulte astrowarp.net para obtener más información. información.

Capítulo 7

Conozca la VPN

Este capítulo presenta VPN conceptos y uso escenarios.

7.1 Introducción

VPN

VPN, abreviatura de Virtual Private Network, establece un túnel cifrado y privado 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 presenta una 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 y garantiza configuraciones VPN consistentes, reduceing riesgos de configuraciones individuales inadecuadas.

Los enrutadores GL.iNet admiten más de 30 servicios VPN comerciales populares OpenVPN y WireGuard. 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, rápido, más simple y más eficiente que OpenVPN. Cuenta con criptografía moderna para mayor eficiencia, una pequeña base de código para facilitar la auditoría y la seguridad, y algoritmos de última generación (ChaCha20/Poly1305) para el cifrado y la integridad de los datos.

7.2 Escenarios de aplicación

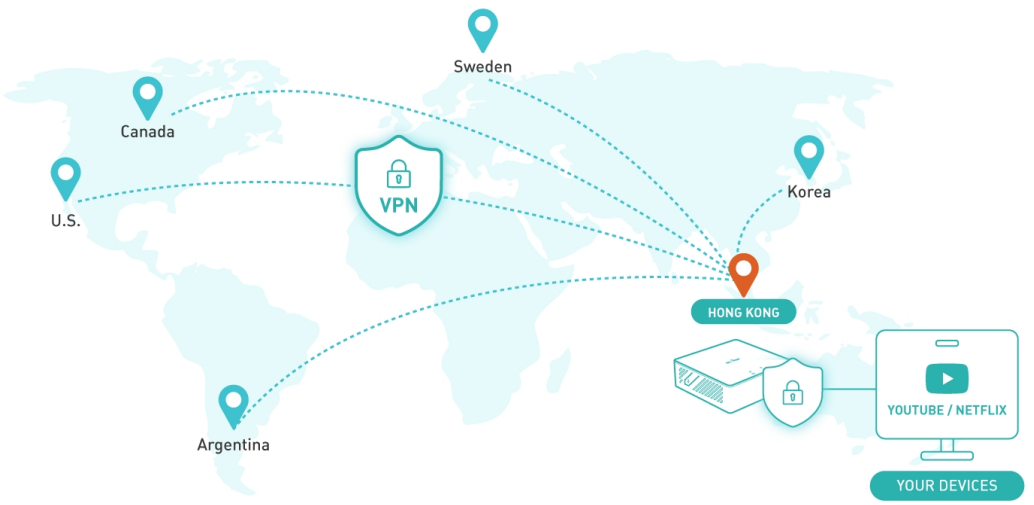
1. **Privacidad de datos personales**

   El servicio VPN de este enrutador funciona con una amplia gama de dispositivos cableados, incluidos equipos de escritorio, portátiles, consolas de juegos, televisores inteligentes y dispositivos de transmisión. Todos sus datos transmitidos a través de conexiones por cable están protegidos por la VPN. También puede personalizar las políticas de VPN para permitir una protección flexible para dispositivos específicos.



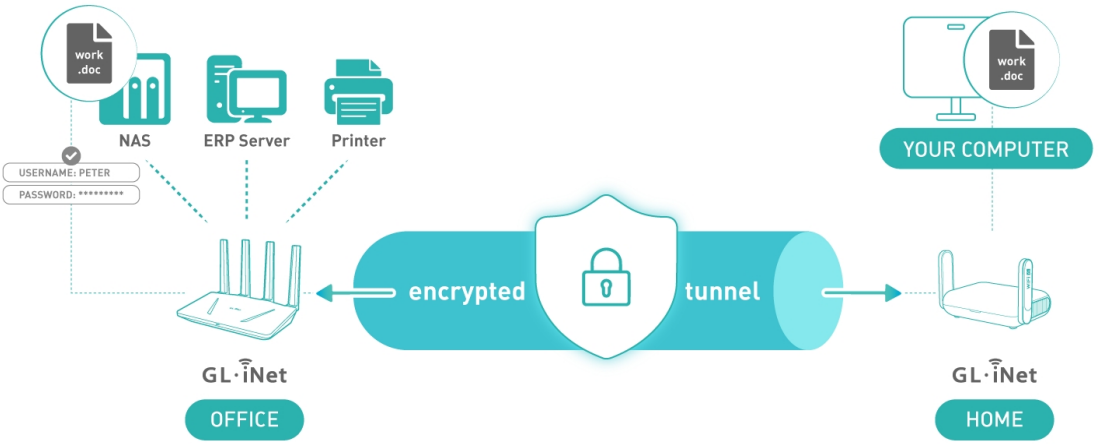
2. **Acceso sin restricciones en todo el mundo**

   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.



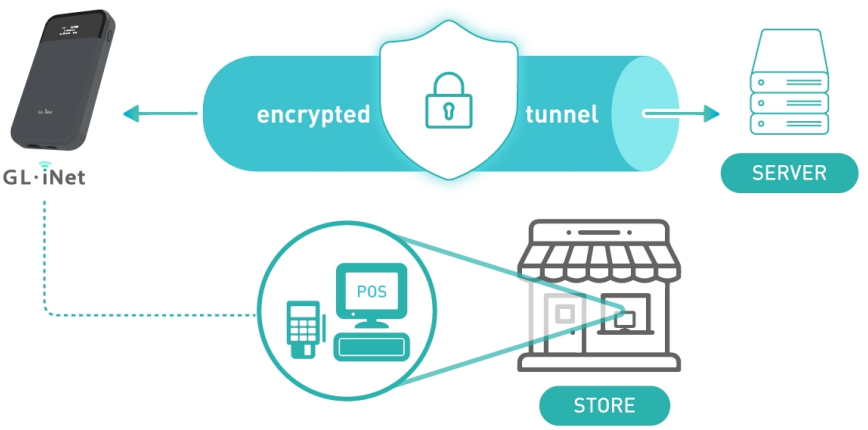
3. Seguridad de datos para pequeñas empresas

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, puede disfrutar de una conectividad segura para trabajar en cualquier lugar.



4. Infraestructura de pago segura

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



Capítulo 8

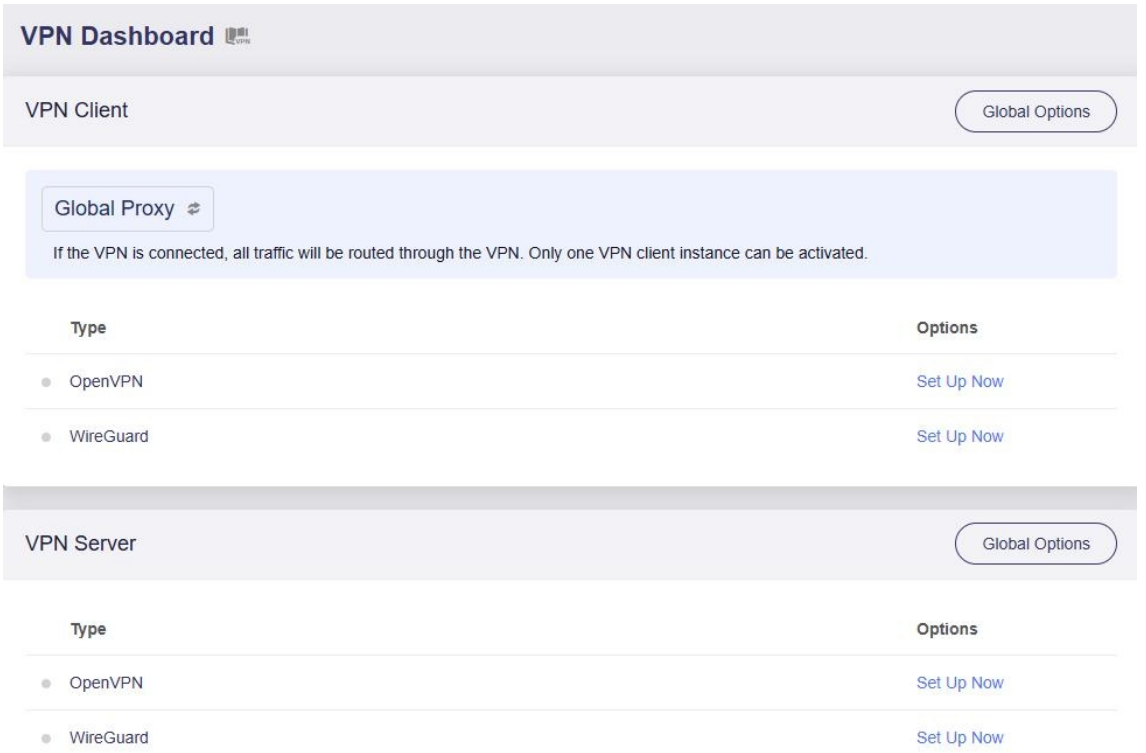
Panel de VPN

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

Inicie sesión en el enrutador’s web admin panel y navegue a **VPN** > **Panel de VPN**.

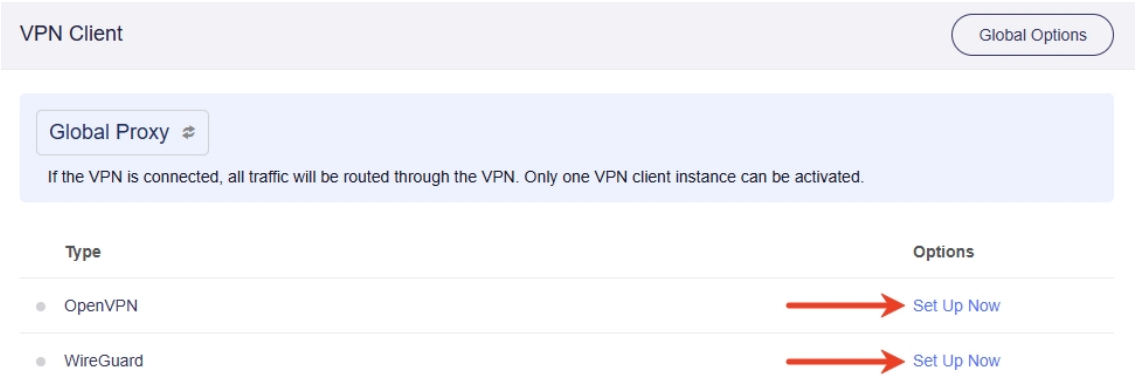
El panel de VPN muestra detalles de la conexión VPN, como dirección del servidor, estadísticas de tráfico, cliente virtual IP y registro de conexión. También permite a los usuarios configurar ajustes avanzados como VPN Kill Switch, política de VPN, enmascaramiento de IP, MTU y VPN. En cascada.

Esta página se divide en dos secciones: idividido en dos secciones: **Cliente VPN** y **Servidor VPN**.

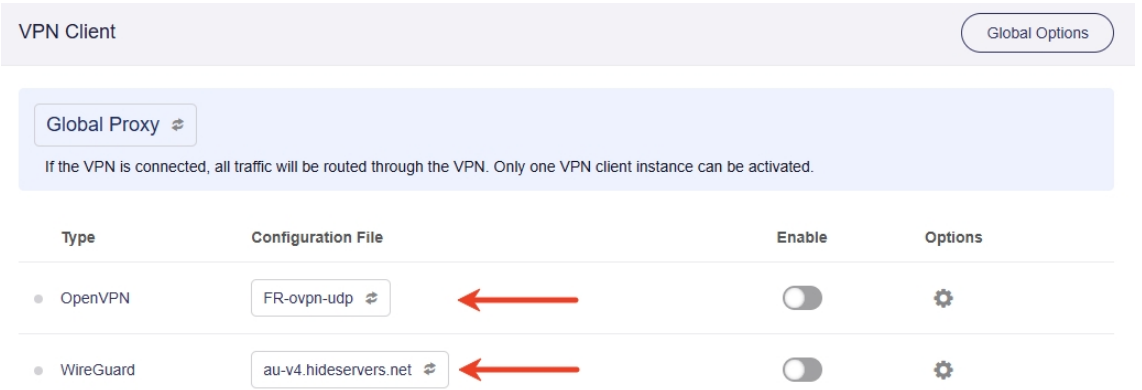


8.1 Cliente VPN

Al ingresar a esta página por primera vez, si no hay ningún archivo de configuración disponible para OpenVPN y WireGuard, la página se muestra de la siguiente manera. Haga clic en **Configurar ahora** y será redirigido al Cliente OpenVPN o al Cliente WireGuard para cargar su archivo de configuración de VPN.



Una vez cargado, 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.

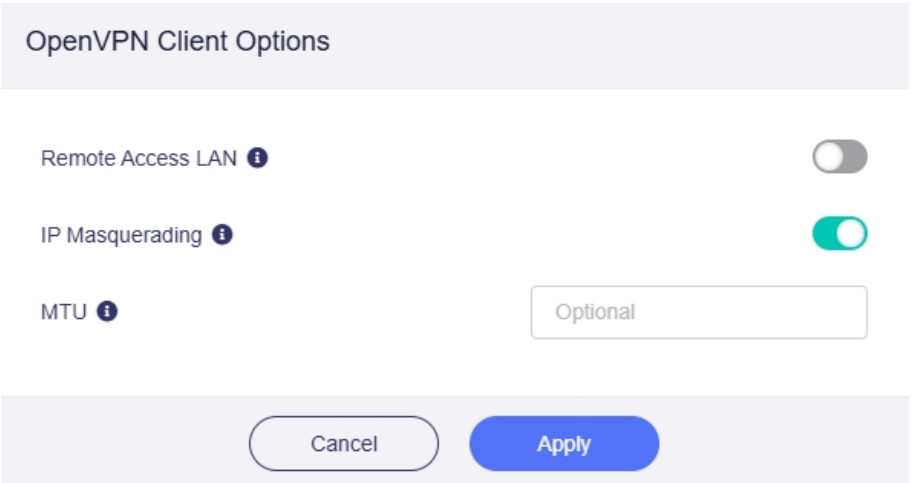


8.1.1 Opciones del cliente

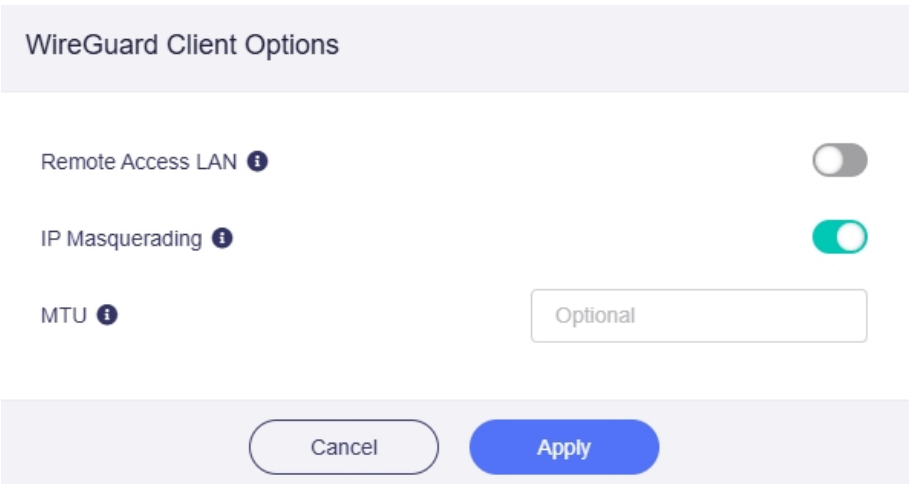
Haga clic en el ícono de ajustes a la derecha para acceder a las opciones de cliente OpenVPN o WireGuard.



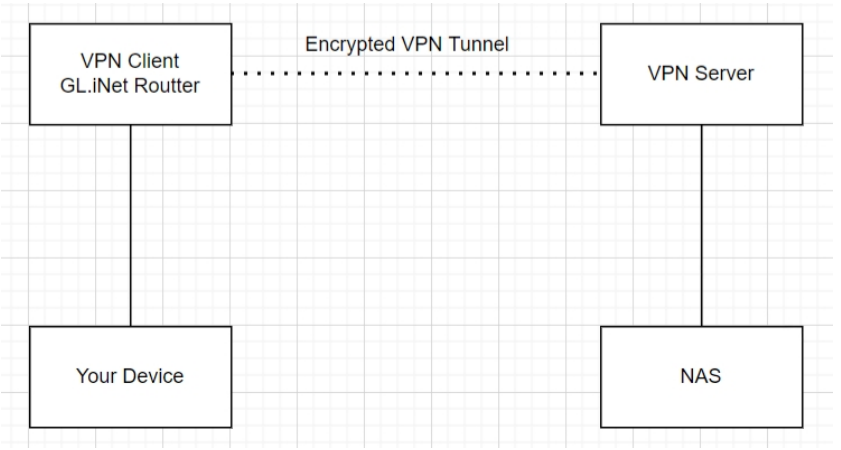
Las Opciones de cliente OpenVPN se muestran a continuación.



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.

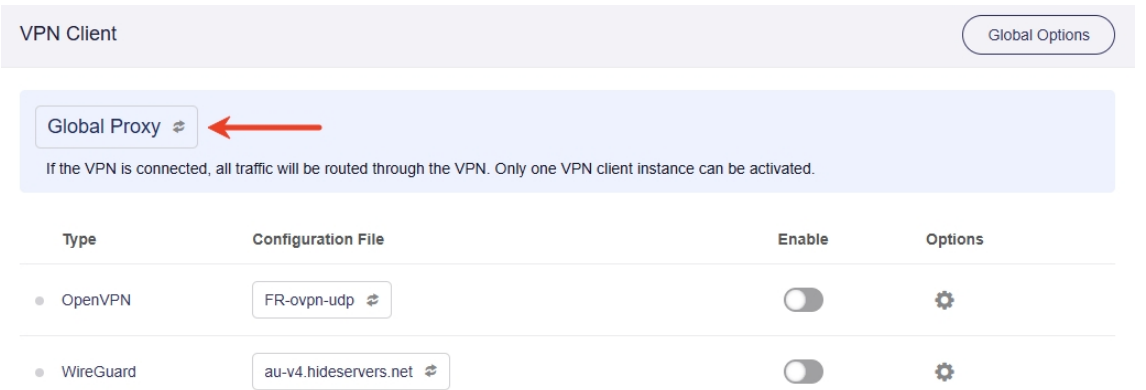


Por ejemplo, como se muestra en el diagrama arriba, el enrutador GL.iNet se ejecuta como un cliente VPN y se conecta a un servidor VPN a través del túnel VPN. Cuando esta opción está habilitada, los dispositivos del lado del servidor VPN (por ejemplo, NAS) pueden acceder tanto al enrutador GL.iNet como 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.

8.1.2 Modo proxy

El modo proxy predeterminado para la conexión VPN es **Proxy global**. Puede hacer clic en el cuadro de 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.

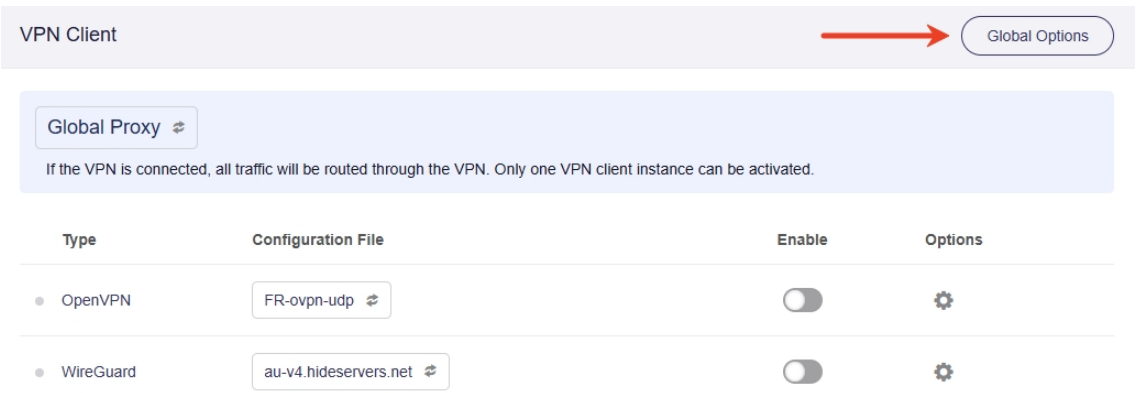
   - **Según el dominio de destino o IP**: En este modo, solo el tráfico de ciertos sitios web identificados por dirección IP o nombre de dominio se enrutará a través de VPN. Solo se puede activar una instancia de cliente VPN.
   - **Según el dispositivo cliente**: En este modo, solo el tráfico de ciertos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

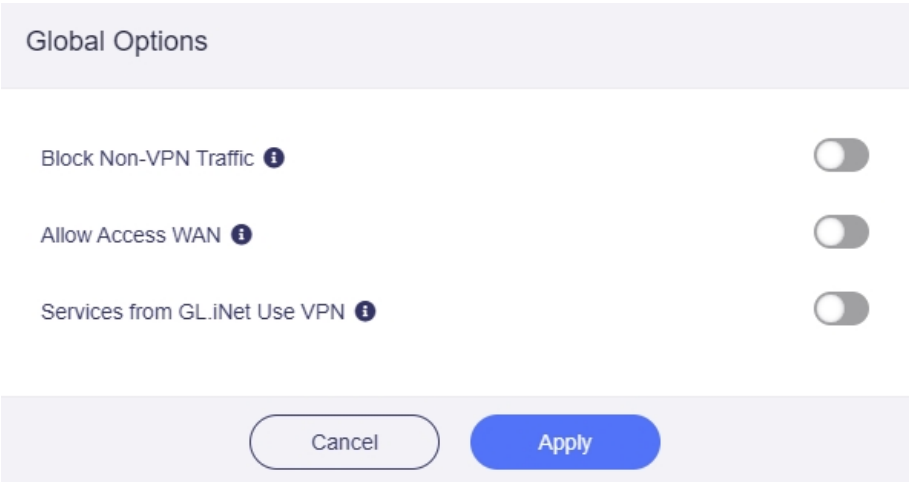
   - **Detección automática**: Se utilizarán las reglas de enrutamiento definidas en cada archivo de configuración de cliente VPN o emitidas por el servidor VPN.
   - **Personalizar reglas de enrutamiento**: Puede configurar manualmente reglas de enrutamiento para cada instancia de cliente VPN.

8.1.3 Opciones globales

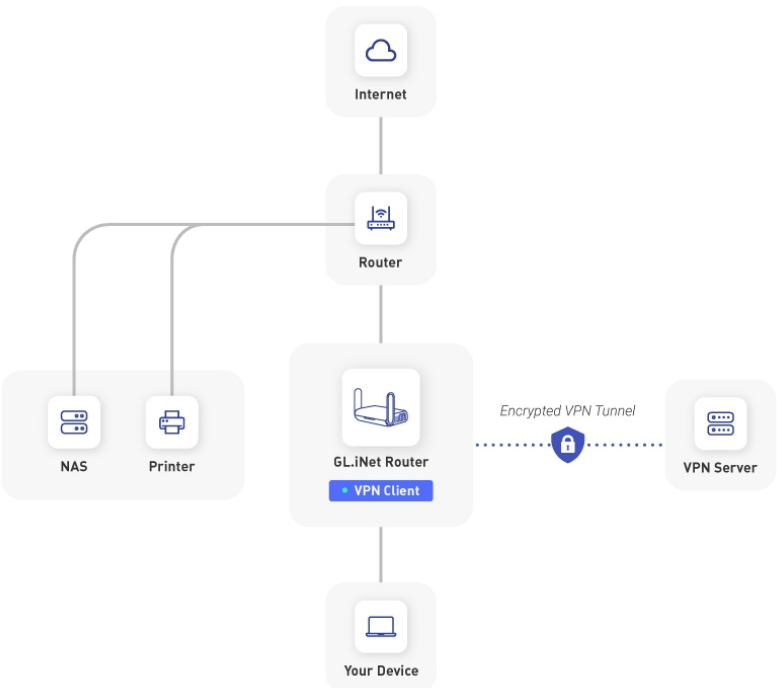
Haga clic en **Opciones globales** en la esquina superior derecha para configurar configuración para su cliente VPN.



Aparecerá una ventana emergente como se muestra a continuación.



- **Bloquear tráfico que no sea VPN**: También se conoce como **Interruptor de interrupción 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.
- **Permitir acceso a WAN**: si está habilitado, los dispositivos cliente locales aún pueden acceder a 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 ynuestros dispositivos locales lleguen a los hosts en la subred ascendente, como impresoras y NAS.

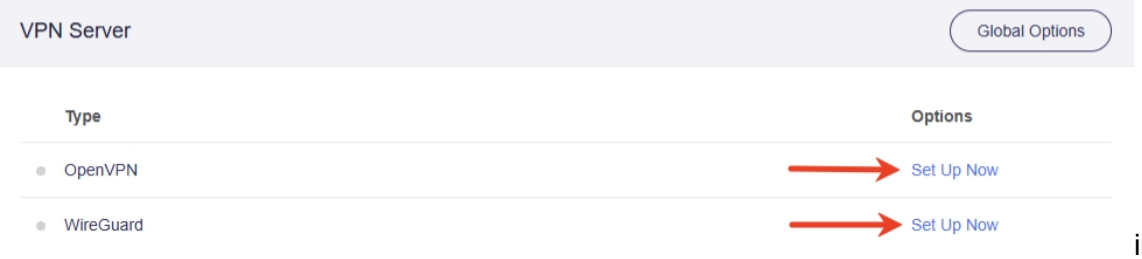
Esta opción está diseñada principalmente para permitir que los clientes accedan a dispositivos dentro de la subred ascendente. Sin embargo, el enrutador no puede distinguir el tráfico de subred ascendente del tráfico de Internet normal. Si los dispositivos cliente acceden a los recursos directamente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

- **Los servicios de GL.iNet usan 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.

8.2 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 redirigido a la página OpenVPN

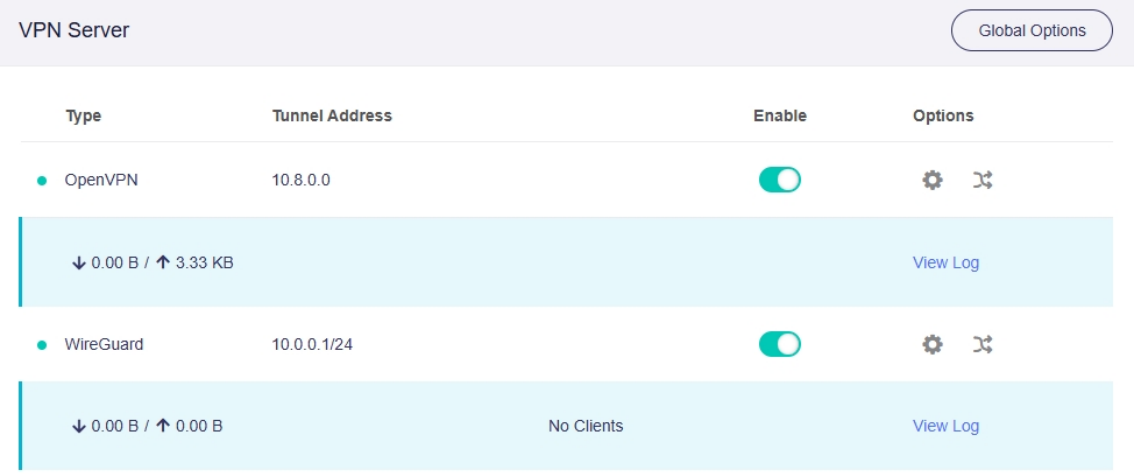
Server o W



ireGu

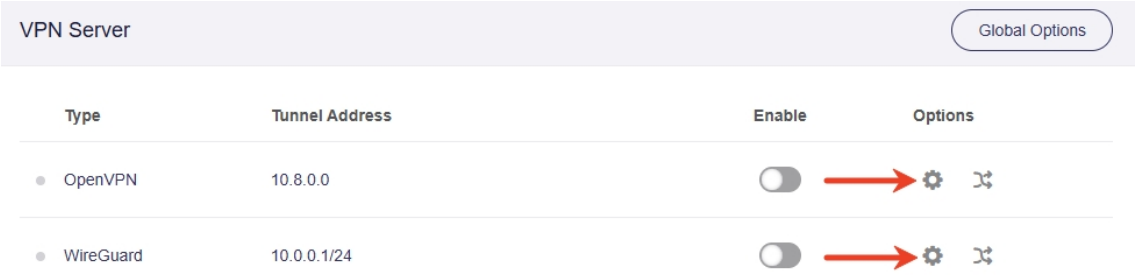
ard Server para inicializar su servidor VPN.

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

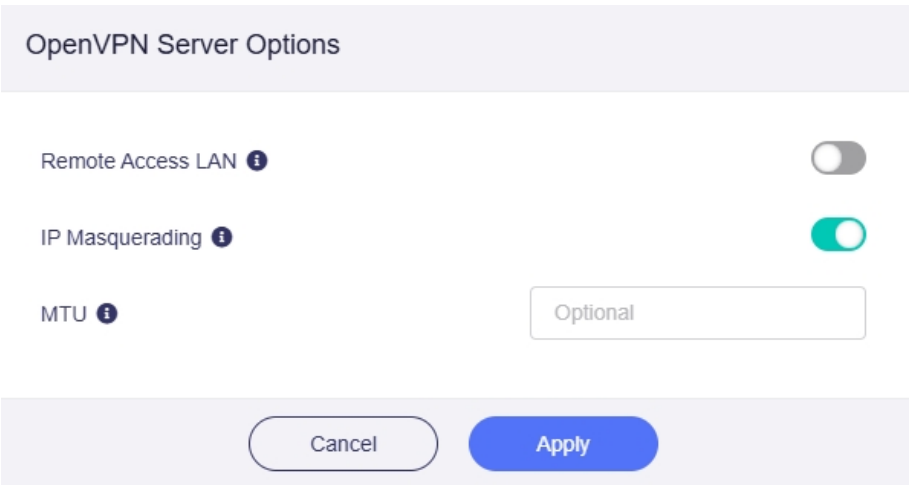


8.2.1 Opciones del servidor

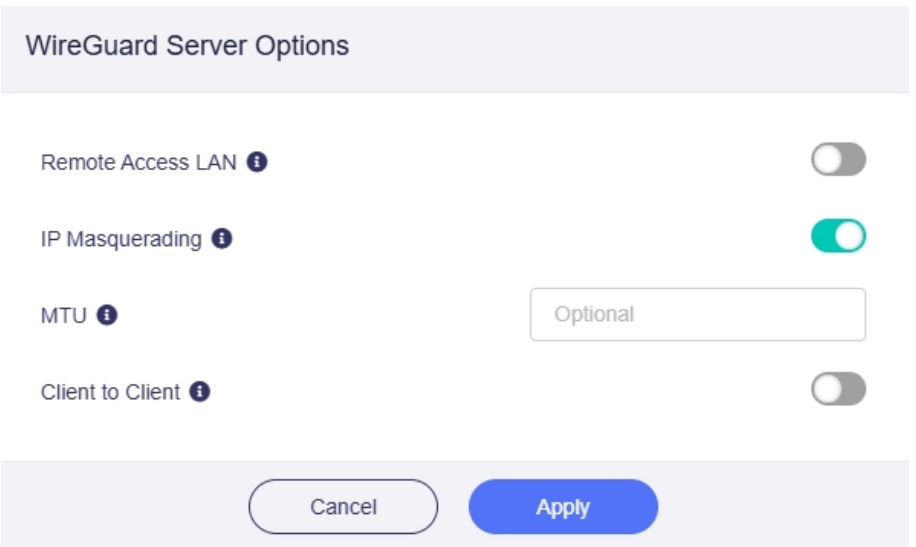
Haga clic en el ícono de ajustes a la derecha para acceder a las opciones del servidor OpenVPN o WireGuard.



Las opciones del servidor OpenVPN se muestran como siguiente.



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

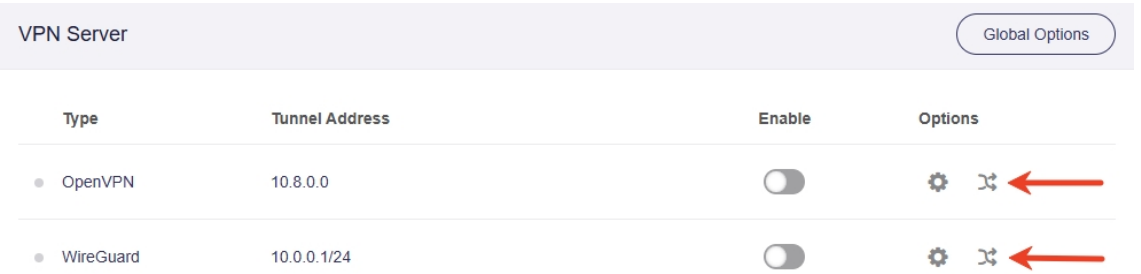


- **LAN de acceso remoto**: si está habilitado, se puede acceder a los recursos dentro de la subred LAN del servidor'a través del túnel VPN.
- **IP Enmascarado**: Si está habilitado, las direcciones IP de origen de los clientes LAN se reescribirán en la IP del túnel VPN del enrutador. Deshabilite esto solo para configuraciones de sitio a sitio donde el par remoto conoce sus subredes LAN.

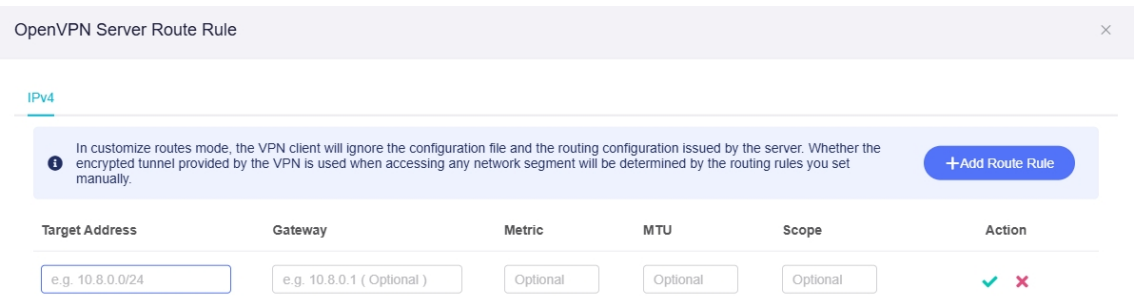
- **MTU**: abreviatura de Unidad de transmisión máxima. El valor de MTU que establezca para el túnel anulará la configuración de MTU en el archivo de configuración.
- **Comunicación entre clientes**: si está habilitado, los clientes VPN conectados a este servidor pueden acceder entre sí a través de sus IP de túnel VPN. Si desea permitir que los clientes también accedan a las subredes LAN de otros, el servidor VPN debe anunciar las rutas correspondientes a esas subredes LAN remotas.

8.2.2 Regla de ruta del servidor

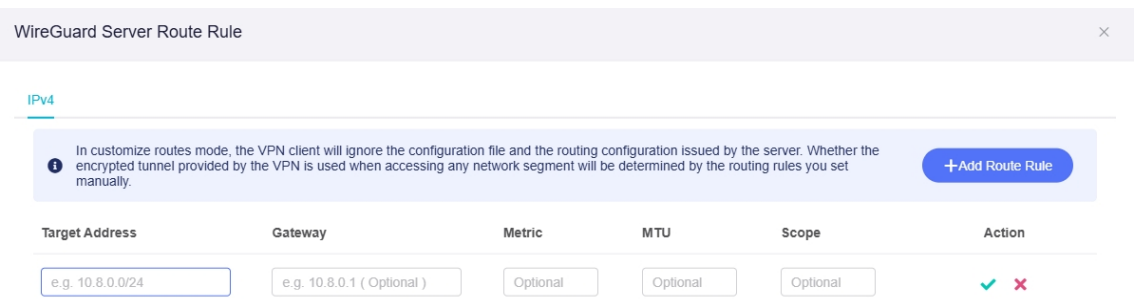
Haga clic en el icono de ruta a la derecha para personalizar las reglas de ruta OpenVPN o WireGuard según sea necesario.



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

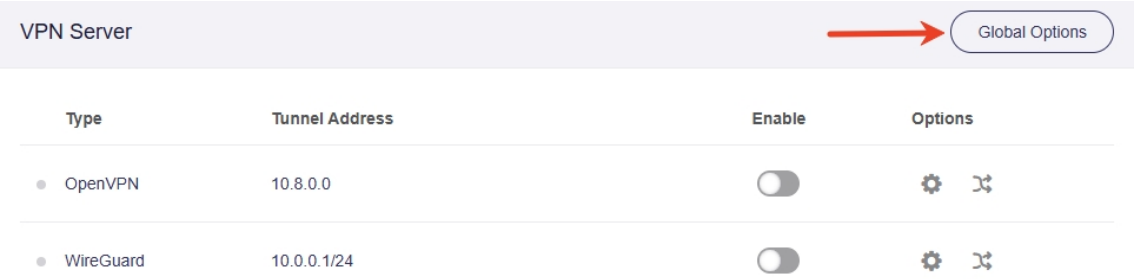


La regla de ruta del servidor WireGuard se muestra de la siguiente manera. Haga clic en **Agregar regla de ruta**, ingrese la **Dirección de destino** y **Gateway**, luego haga clic en el ícono de verificación verde para aplicar.

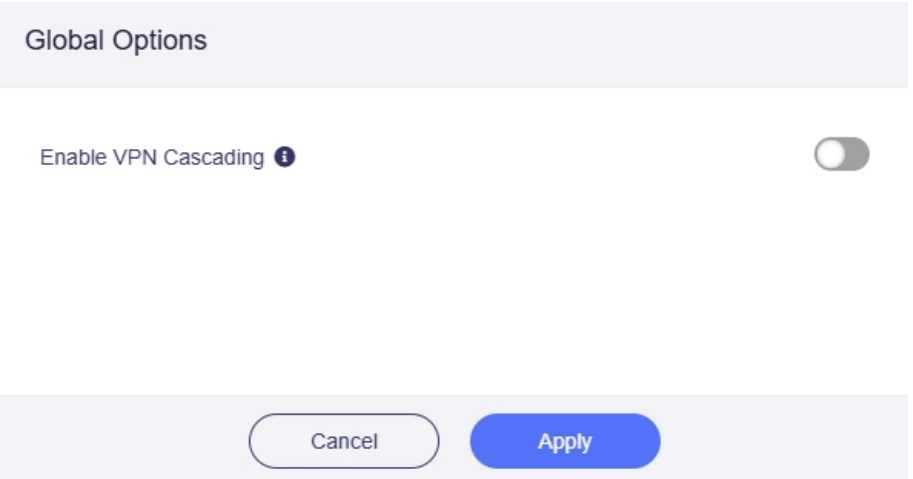


8.2.3 Opciones globales

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



Aparecerá una ventana emergente como se muestra a continuación.



- **VPN en cascada**: si está habilitado, cuando este enrutador actúa como servidor VPN y cliente VPN 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 utiliza como cliente VPN. Consulte aquí para más detalles.

Capítulo 9

Configurar el servidor VPN

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

9.1 Configurar el servidor OpenVPN

OpenVPN es un protocolo VPN de código abierto que utiliza cifrado SSL/TLS para seguridad Conexiones 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.

9.1.1 Preparación

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

   Haz clic aquí para verificar si tu proveedor de servicios de Internet (ISP) te asigna una dirección IP pública.

   Si no, tu enrutador no puede configurarse como un servidor OpenVPN.

   Métodos alternativos:

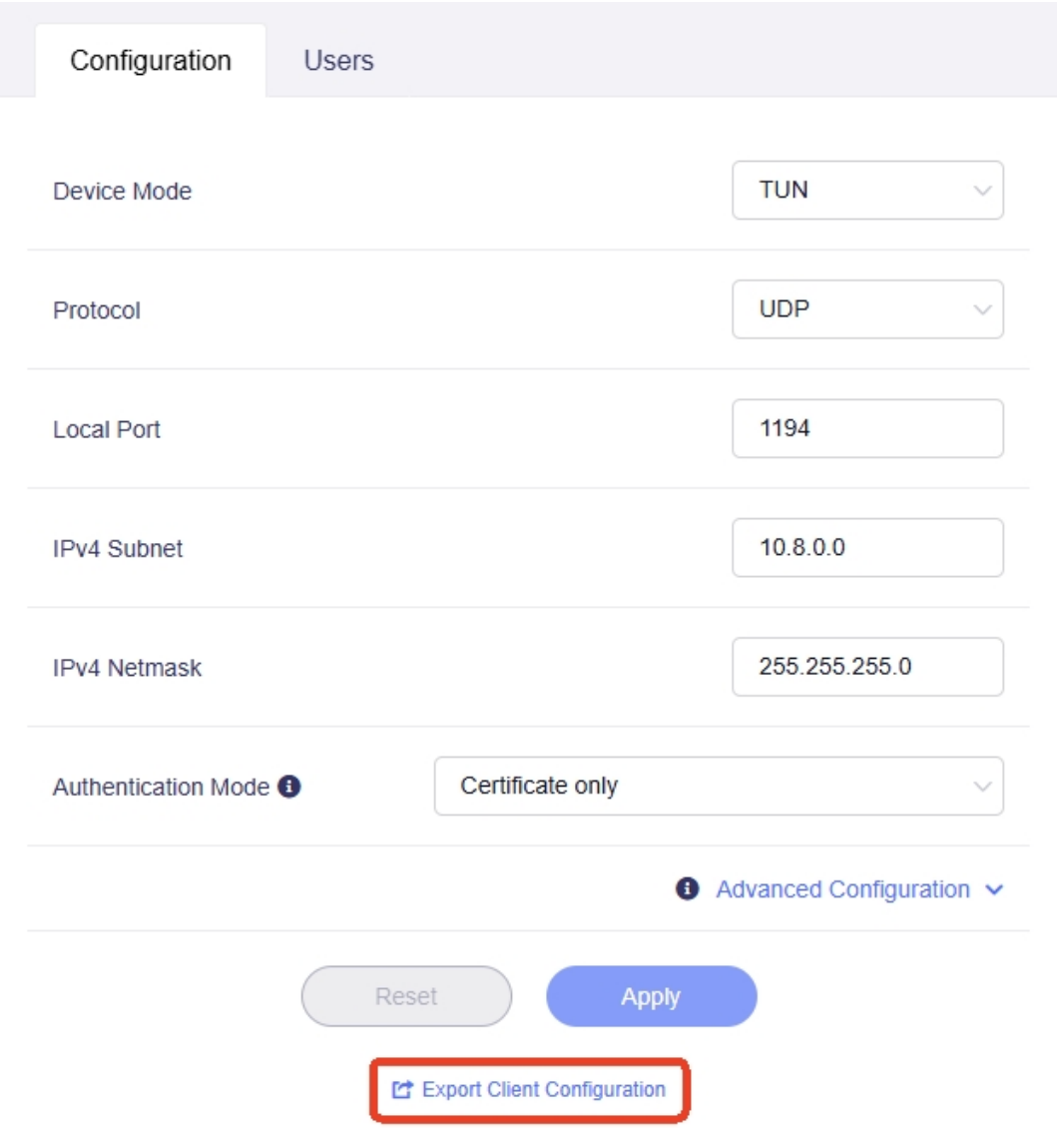
   - Si tiene un enrutador principal ascendente a su enrutador GL.iNet, inicie sesión en él y verifique que tenga una dirección IP pública asignada por su ISP.
   - Solicite a su ISP una dirección IP pública. Esto puede generar una tarifa adicional.
   - Si los dos métodos anteriores no funcionan (por ejemplo, si su red está detrás de CGNAT), puede probar nuestra solución SD-WAN AstroWarp.

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 se encuentra en varios niveles posteriores al enrutador principal, configure el reenvío de puertos en cada dispositivo intermedio.

9.1.2 Pasos de configuración

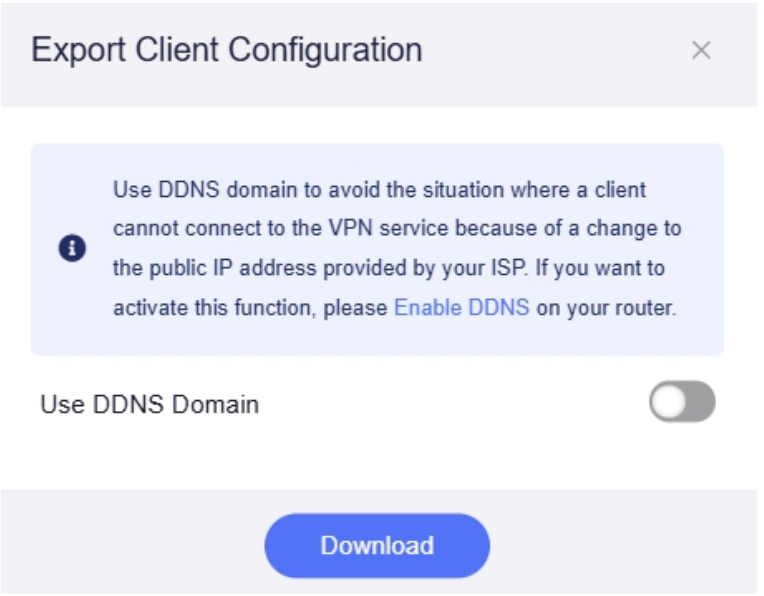
1. Inicie sesión en el panel de administración web del enrutador, navegue hasta **VPN** > **Servidor OpenVPN** y luego haga clic en **Generar configuración** (solo para la configuración inicial del servidor VPN).
2. Aplique la configuración.
   La configuración predeterminada funciona en la mayoría de los casos. Haga clic en **Exportar configuración del cliente** en la parte inferior y continúe con el paso 3. Si ha modificado la configuración, haga clic en **Aplicar** antes de exportarla.



- **Dispositivo Modo**: TAP-S2S o Tun. Consulte aquí para las diferencias.
- **Protocolo**: UDP o TCP. Consulte aquí para las diferencias.

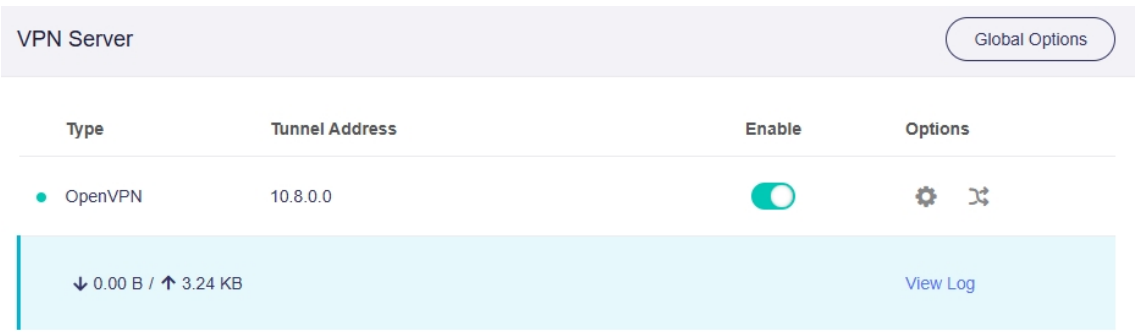
- **Modo de autenticación**: Esto determina el método de autenticación utilizado cuando el cliente se conecta al servidor. Hay tres opciones:
  - **Solo certificado**: si se selecciona, el enrutador generará automáticamente claves de certificado de servidor y de cliente y las incrustará en el archivo de configuración. Cuando carga la configuración en el 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. Usted necesita primero agregue un nombre de usuario y contraseña en la pestaña **Usuarios** antes de exportar la configuración del cliente. Al cargar la configuración en el cliente, ingrese estas credenciales para la autenticación.
  - **Nombre de usuario/contraseña y certificado**: si se selecciona, necesita primero agregar un nombre de usuario y una contraseña en **Usuarios** pestaña 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 en el cliente, primero se verificará la clave del certificado, seguida de la autenticación de nombre de usuario/contraseña para 2FA seguridad.
- **Configuración avanzada**: Personalizar más configuraciones del servidor según necesario.

3. 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. **Nota**: si su IP pública cambia con frecuencia, habilite DDNS antes de hacer clic en Descargar. Luego podrá utilizar el dominio DDNS como dirección de su servidor.



4. Habilitar OpenVPN servidor.

   Vaya al **Panel de VPN**, active el interruptor para habilitar el servidor OpenVPN. Comenzará a ejecutarse como se muestra a continuación.



9.1.3 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.

9.2 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.

9.2.1 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.

   Métodos alternativos:

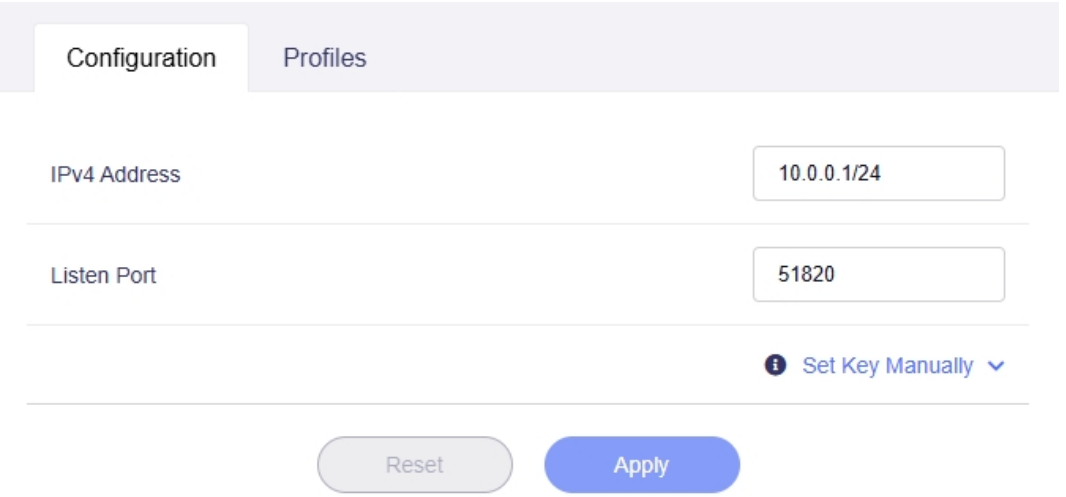
   - Si tiene un enrutador principal aguas arriba de su enrutador GL.iNet, inicie sesión en él y verifique que tenga una dirección IP pública asignada por su ISP.
   - Pregunte a su ISP para una dirección IP pública. Esto puede generar una tarifa adicional.
   - Si los dos métodos anteriores no funcionan (por ejemplo, si su red está detrás de CGNAT), puede probar nuestra solución SD-WAN AstroWarp.

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

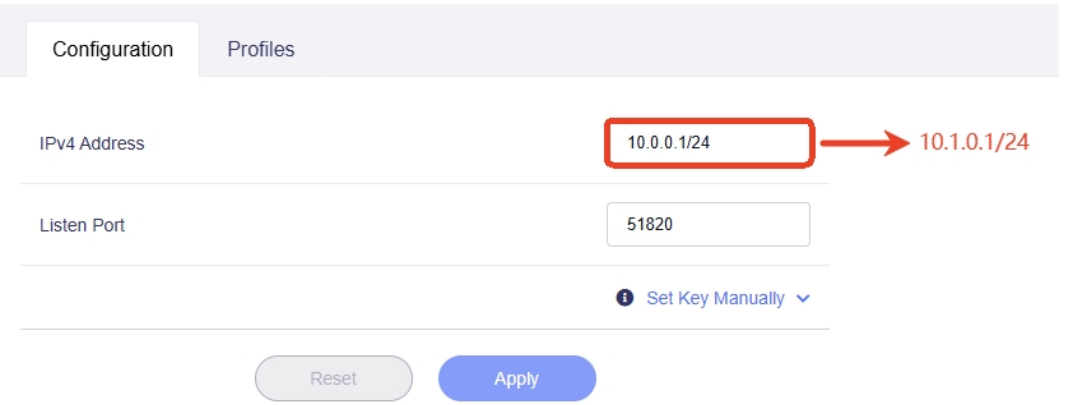
   - Si su enrutador GL.iNet es el enrutador principal de su red, no se requiere configuración de reenvío de puertos. Continúe con el siguiente paso.
   - Si ya hay un enrutador principal en uso y su enrutador GL.iNet está configurado como enrutador secundario, deberá configurar el reenvío de puertos en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

9.2.2 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. Aplique 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.



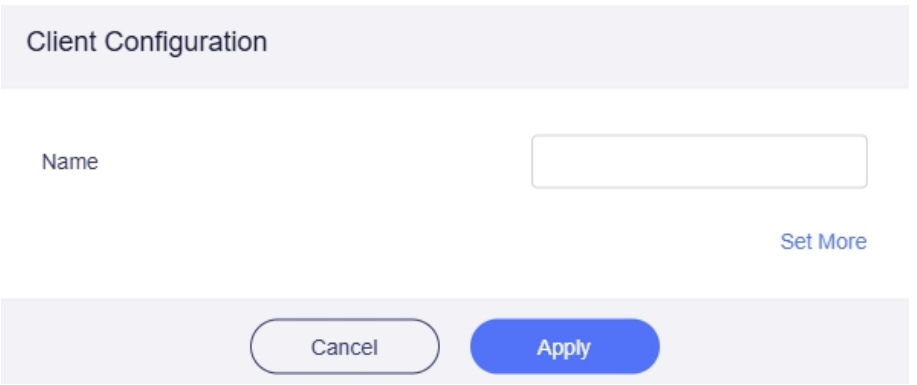
   Si la dirección IPv4 entra en conflicto con la puerta de enlace de su enrutador ascendente, modifique la dirección IPv4 a otra una (por ejemplo, **10.1.0.1/24**) y haga clic en **Aplicar**. Asegúrese de que se incluya la notación CIDR "/24" para evitar problemas de conectividad.



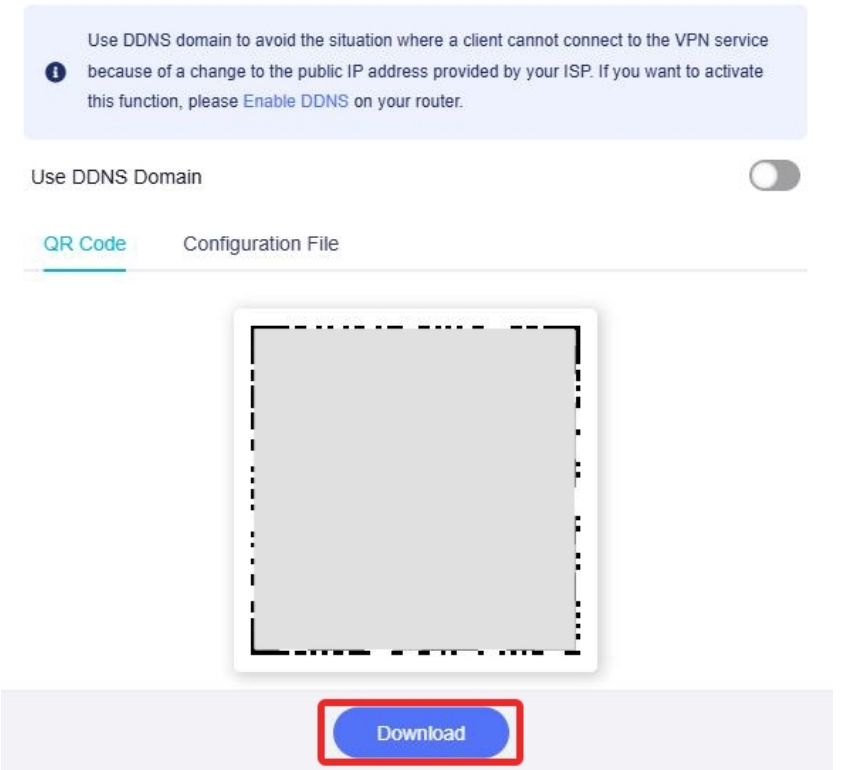
3. Agregue un perfil.
   Cambie a **Perfiles** pestaña, haga clic en **Agregar** para generar un perfil para su dispositivo.



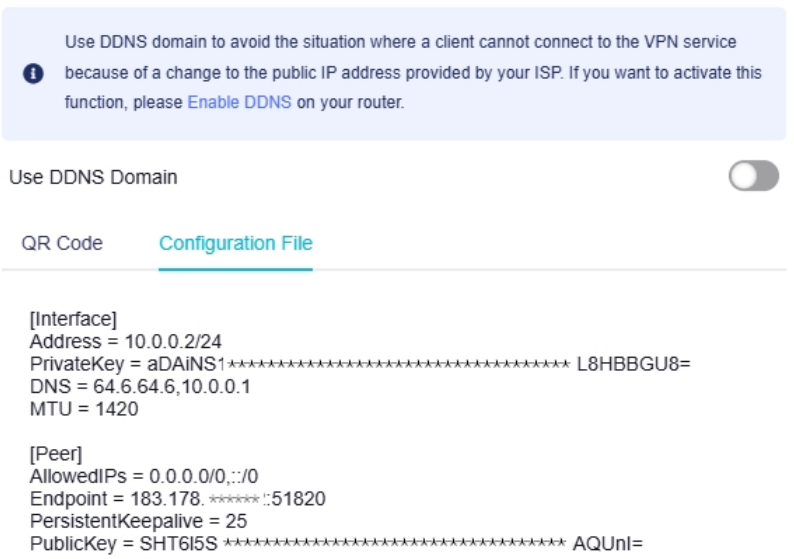
Establezca un nombre descriptivo y haga clic en **Aplicar** para continuar.



4. Después agregando un perfil, el enrutador generará un archivo de configuración en tres formatos: código QR, archivo .conf y texto sin formato. Elija su formato. **Nota**: Si su IP pública dirección cambia frecuentemente, habilite DDNS antes de descargar el archivo.
   - **Código QR**: Adecuado para dispositivos (por ejemplo, teléfonos inteligentes, tabletas, computadoras portátiles) con 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.
   - **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.

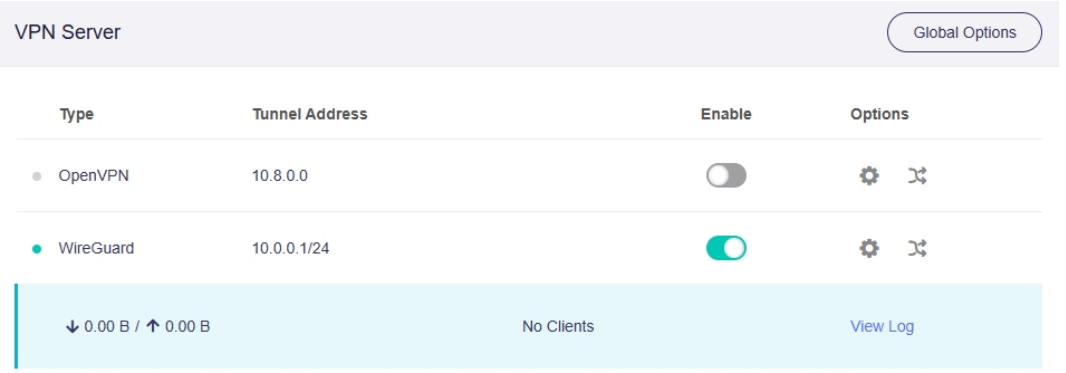


- **Texto sin formato**: en formato de texto sin formato, puede revisar los detalles de configuración y copiarlos y pegarlos cómodamente en otro lugar para la configuración manual, como la aplicación WireGuard o un enrutador GL.iNet.



5. Activar servidor WireGuard.

   Vaya al **Panel de VPN**, active el interruptor para habilitar su servidor WireGuard. Comenzará a ejecutarse como se muestra a continuación.



9.2.3 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. Consulta aquí para solucionar problemas.
- El puerto utilizado para el servidor WireGuard 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 10

Configurar el cliente VPN

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

10.1 Configurar el cliente OpenVPN

10.1.1 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.

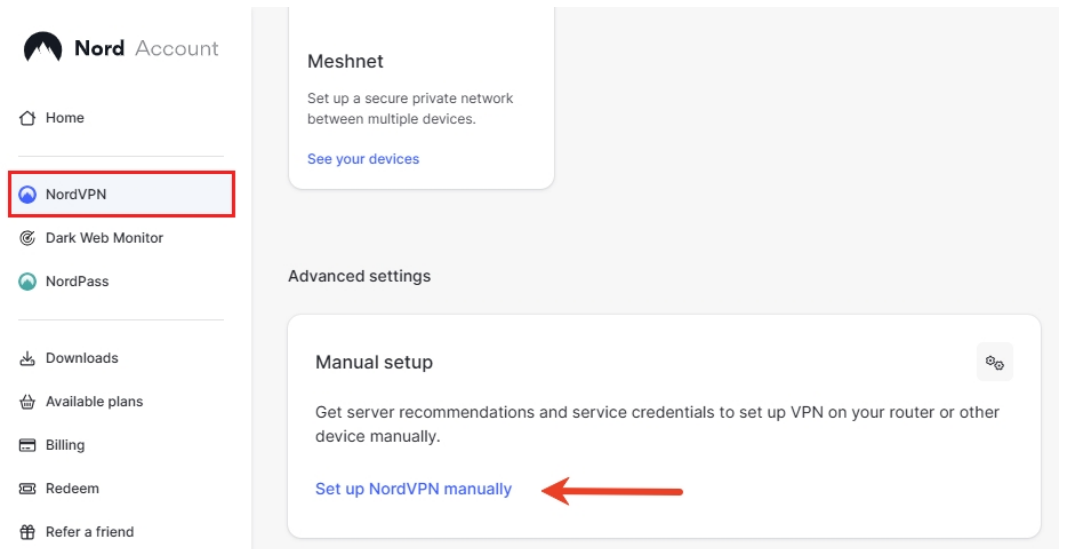
Siguiente, visite el sitio web oficial del proveedor de servicios VPN al que se suscribió y obtener las credenciales de servicio o el archivo de configuración. Si no sabe cómo obtener el archivo de configuración, consulte este enlace o póngase en contacto con su soporte.

10.1.2 Configurar NordVPN

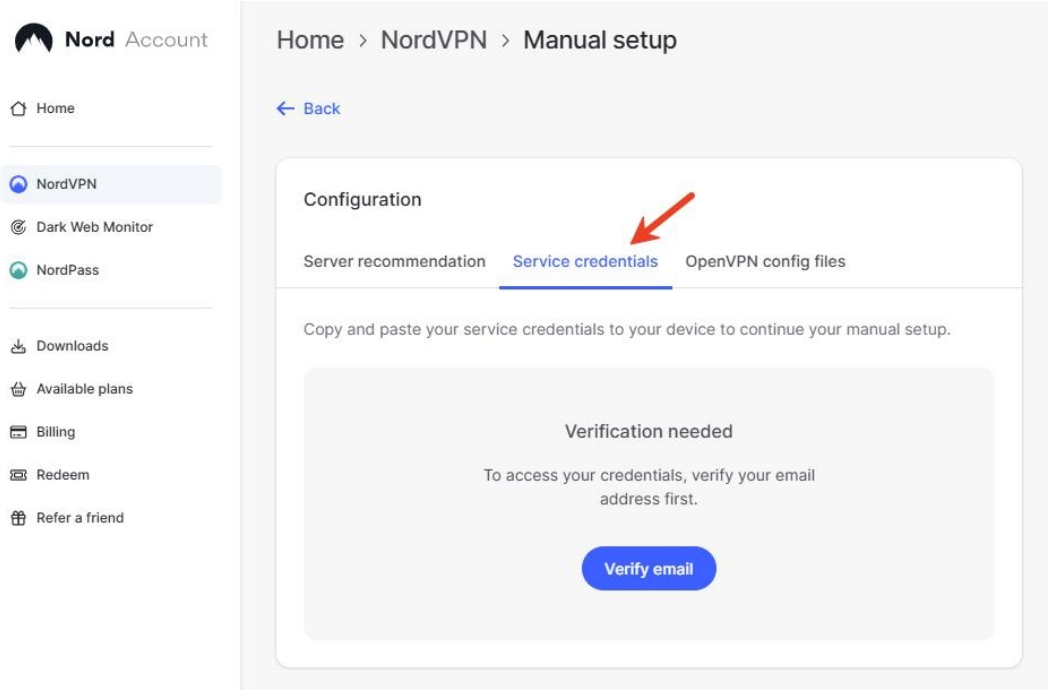
NordVPN está integrado en el panel de administración GL.iNet web . Puede adquirir archivos de configuración para todos los servidores NordVPN introduciendo las credenciales de su cuenta (obtenidas del Panel de NordVPN) en el panel de administración web del enrutador o en la aplicación móvil GL.iNet ,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

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

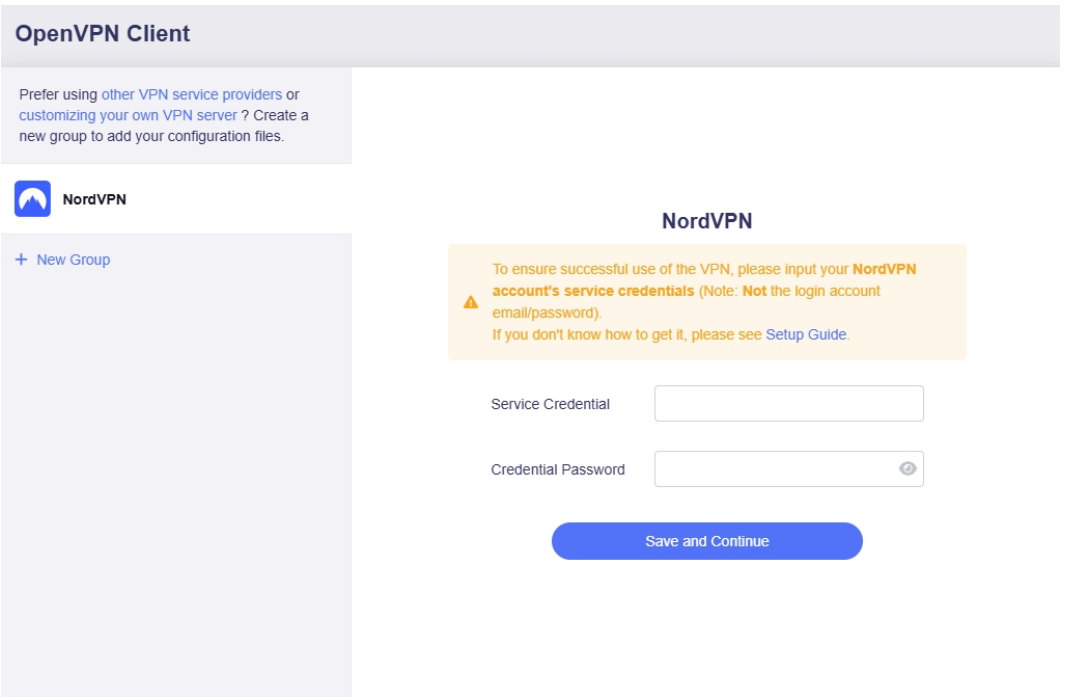
1. Inicie sesión en su cuenta web de NordVPN aquí.
2. Oen el Panel de control de Nord, haga clic en **NordVPN**, luego haga clic en **Configurar NordVPN manualmente**.



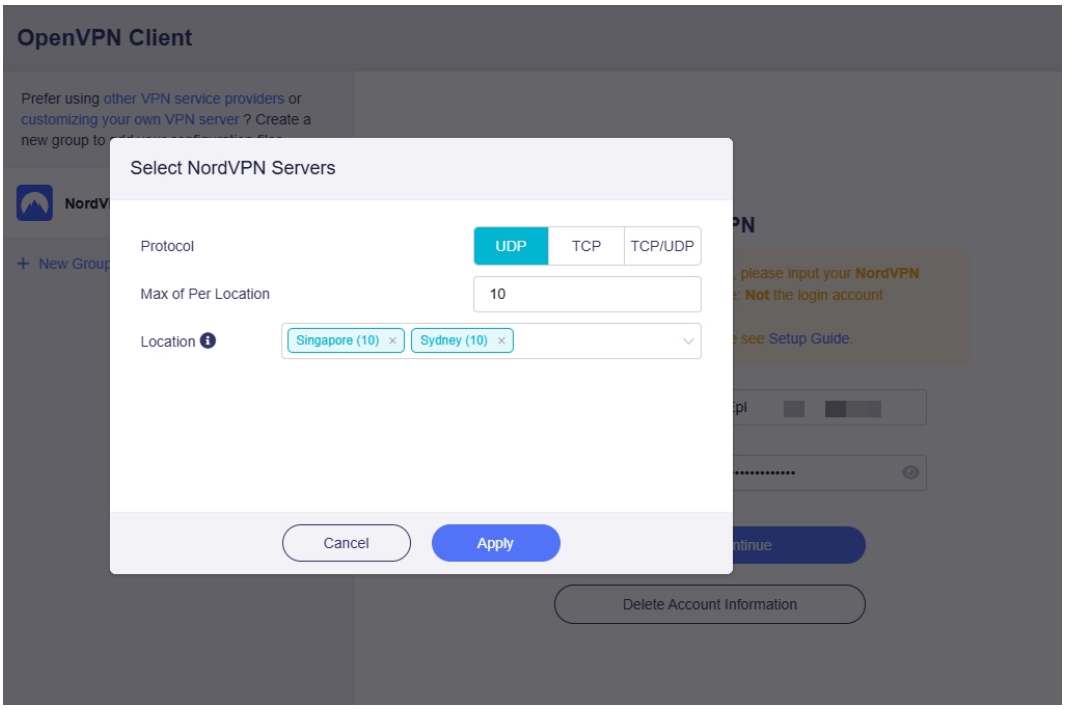
Encontrará las **credenciales de servicio**. Cópielos para usarlos más adelante.



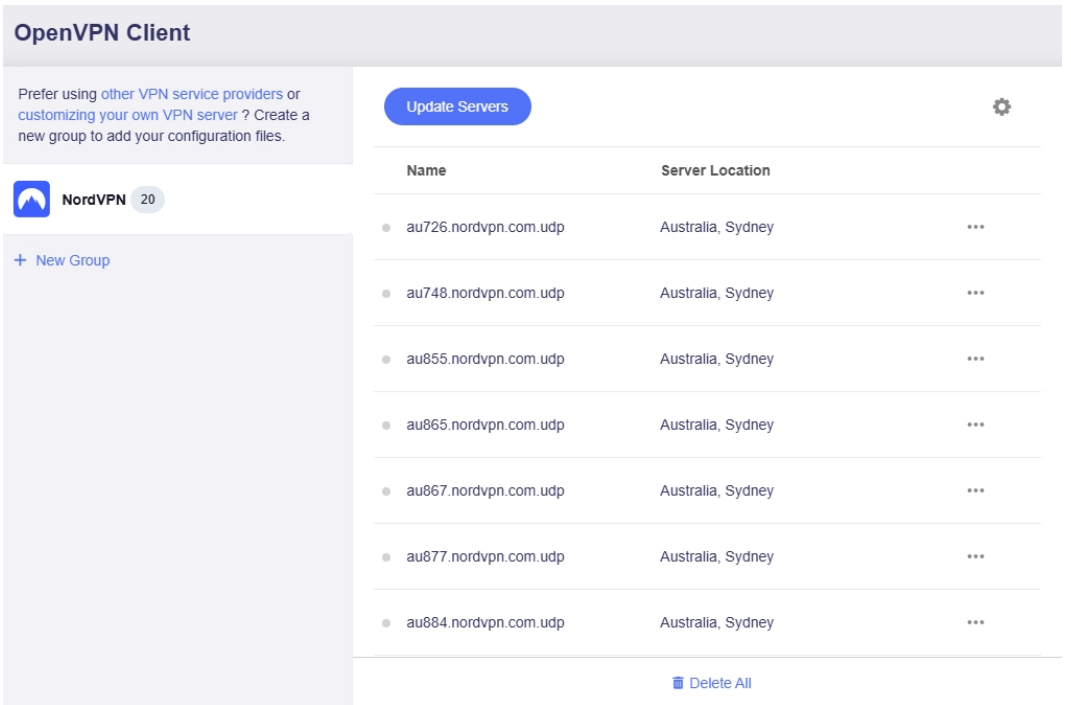
3. Inicie sesión en el panel de administración web de su enrutador y navegue hasta **VPN** > **Cliente OpenVPN** > **NordVPN**. Introduzca las credenciales del servicio (Nota: NO es el correo electrónico ni la contraseña de la cuenta de inicio de sesión), luego haga clic en **Guardar y continuar**.



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

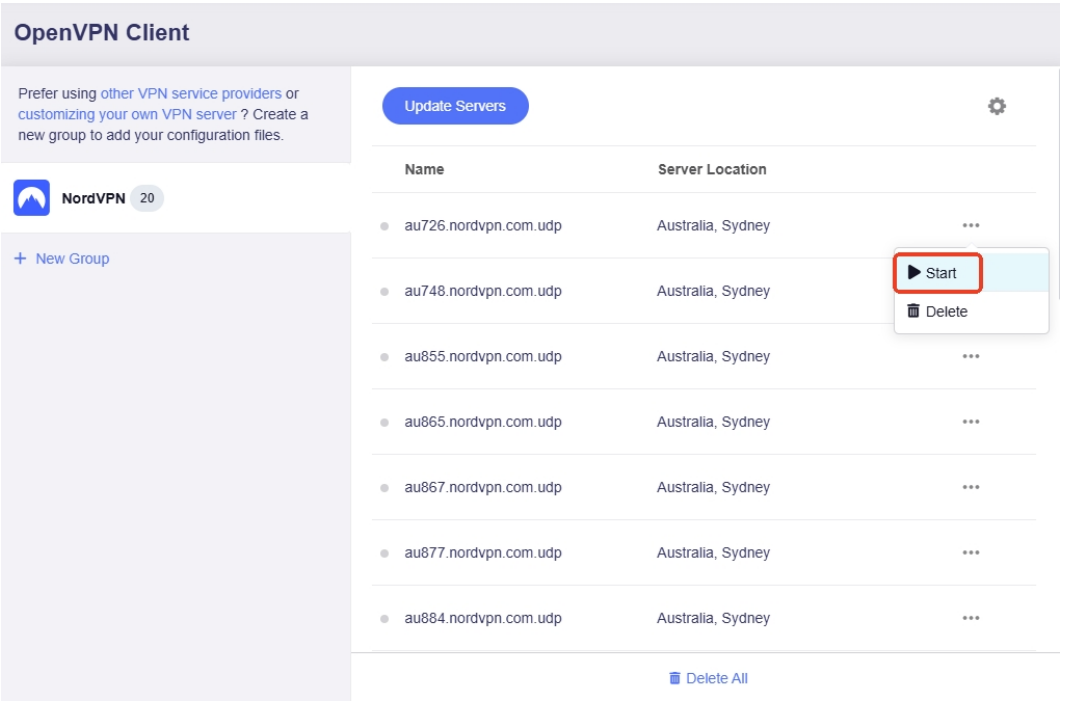


Descargará archivos de configuración.

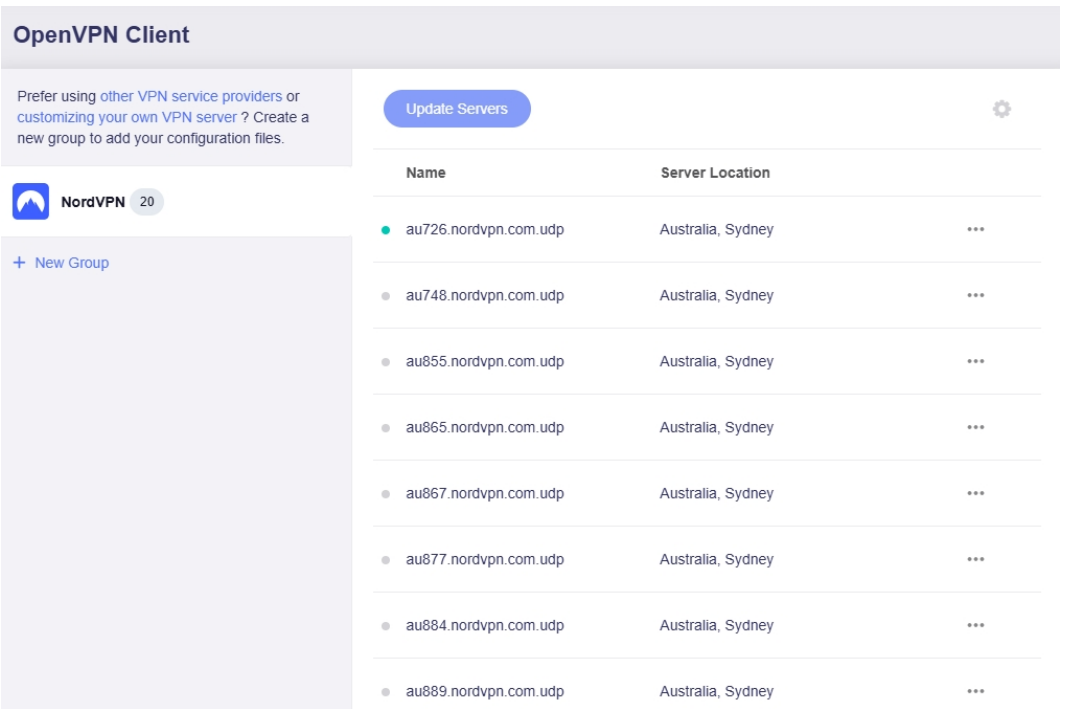


5. Iniciará una conexión.

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



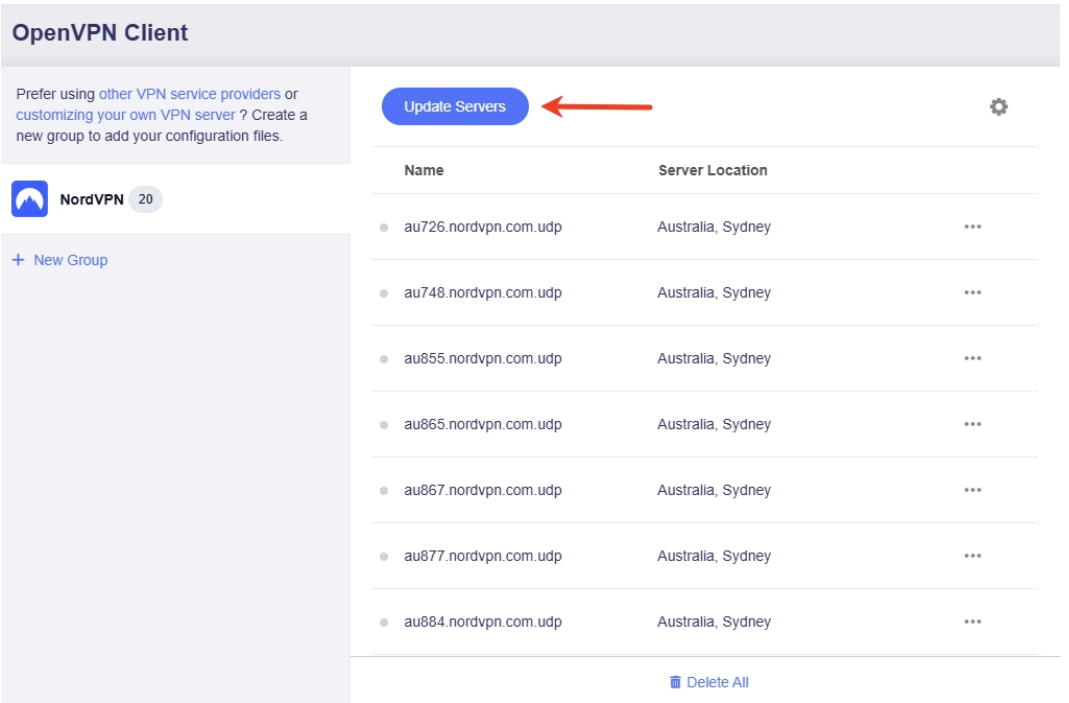
6. Una vez conectado, aparecerá un punto verde junto a el archivo de configuración.



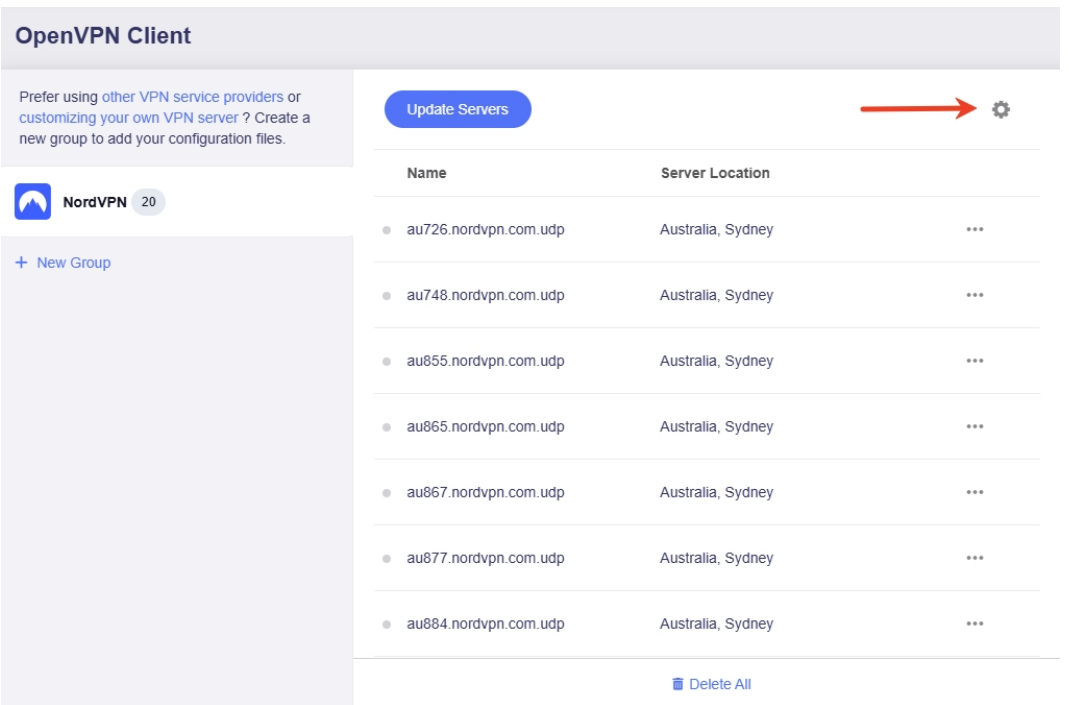
También puede consultar los detalles de la conexión VPN en el **Panel de VPN**.

7. 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.

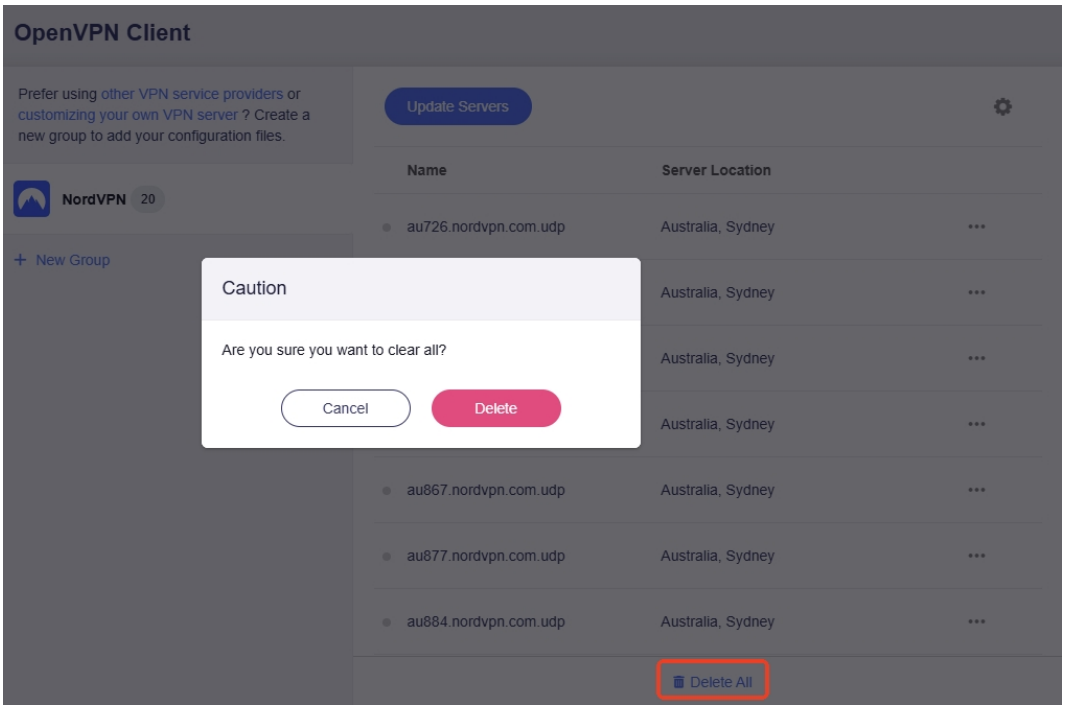


8. Edite las credenciales.
   Haga clic en el ícono de ajustes para editar sus credenciales de inicio de sesión.



9. Elimine todos los archivos.

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

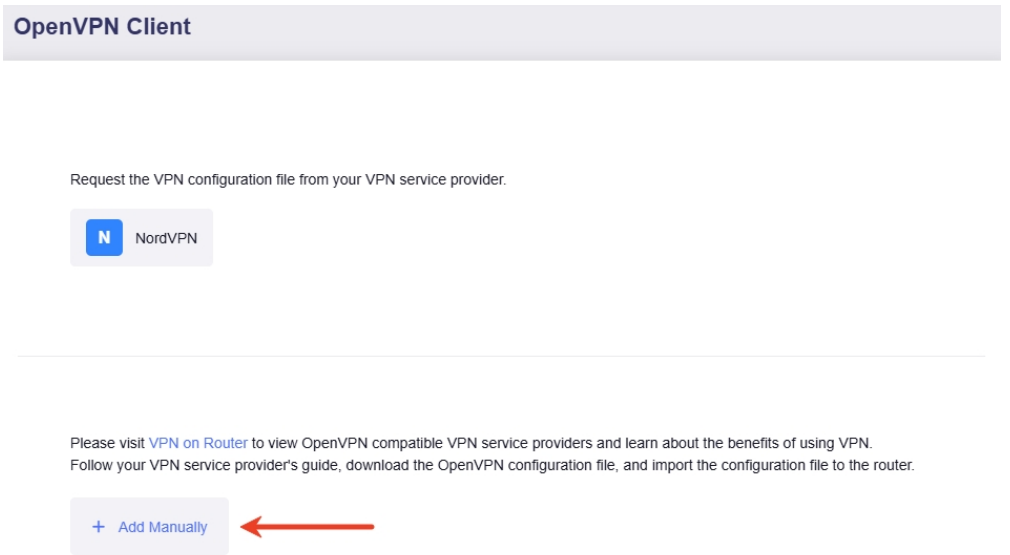


10.1.3 Configurar el cliente OpenVPN manualmente (para otros proveedores)

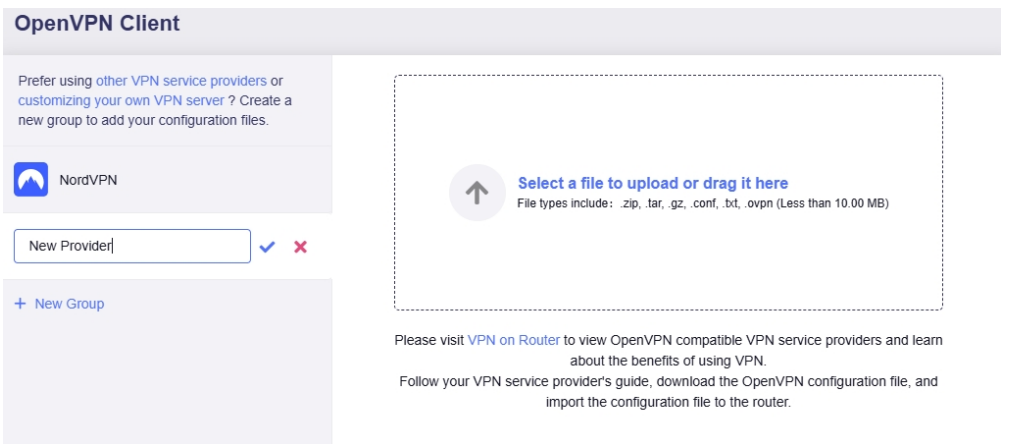
Si su proveedor de servicios OpenVPN es no está integrado en nuestro panel de administración, primero visite el sitio web oficial de su proveedor de servicios suscrito para obtener el archivo de configuración. Luego cárguelo en el enrutador para configurar un cliente OpenVPN.

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

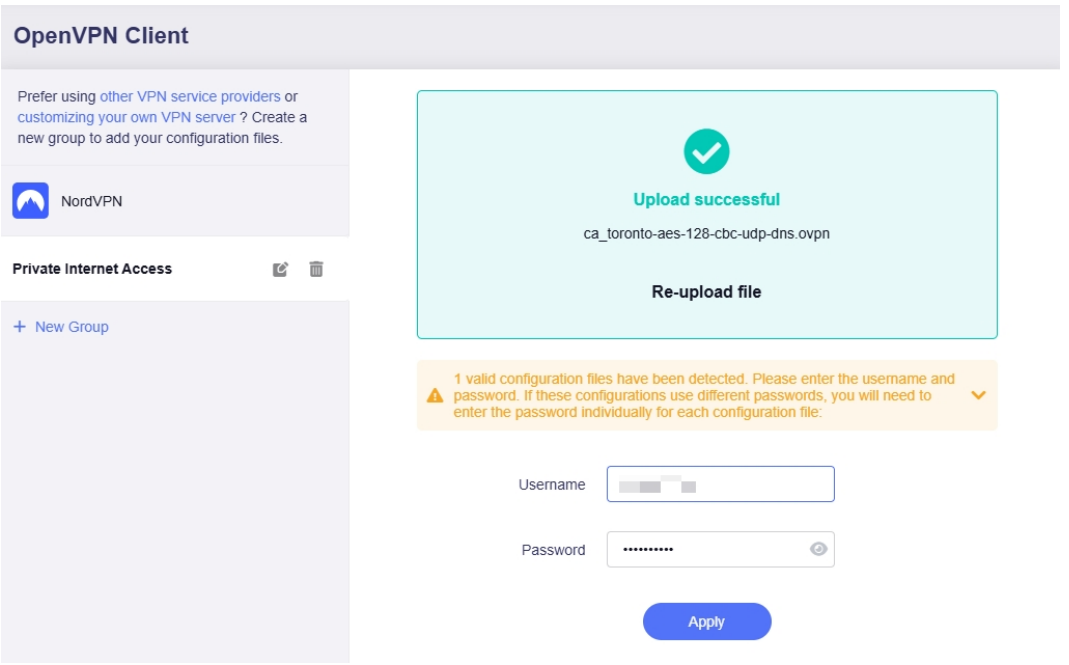
1. Descargue un archivo de configuración del sitio web oficial de Private Internet Access.
2. Inicie sesión en el panel de administración web de su enrutador, navegue hasta **VPN** > **Cliente OpenVPN** y haga clic en **Agregar manualmente**.



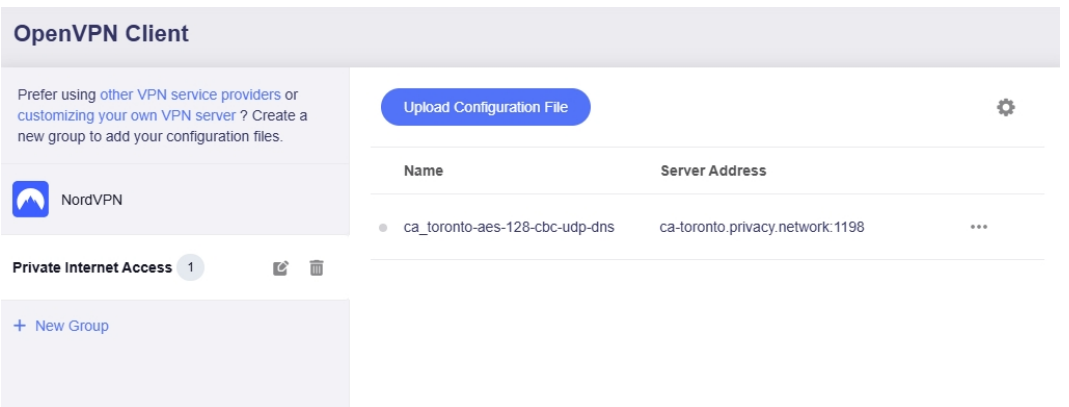
3. Se creará un grupo en la barra lateral izquierda.Establezca un nombre descriptivo del grupo.



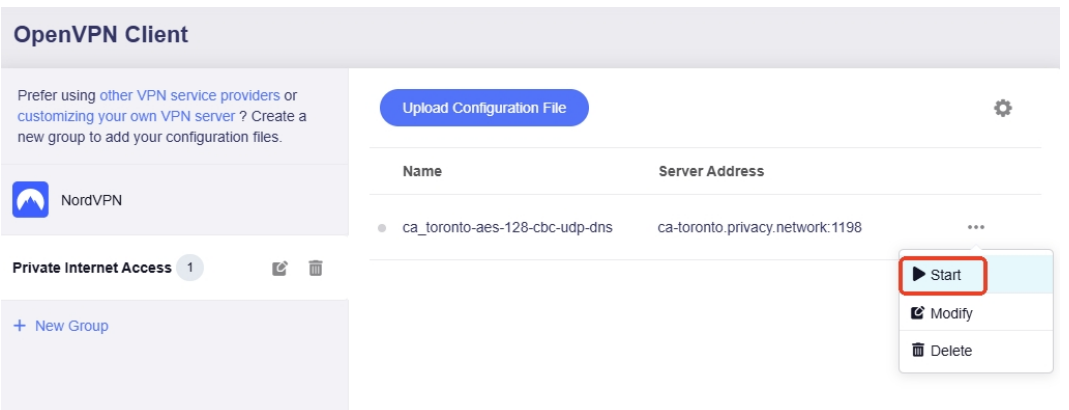
4. Cargue su archivo de configuración de OpenVPN. Ingrese las credenciales si es necesario, luego haga clic en **Aplicar**.



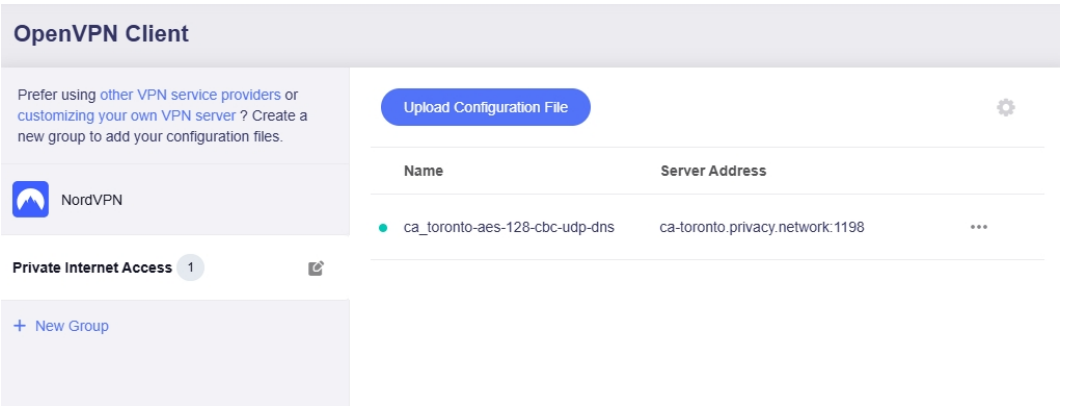
YVerá el archivo de configuración cargado.



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**.

10.2 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.

10.2.1 Preparación

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

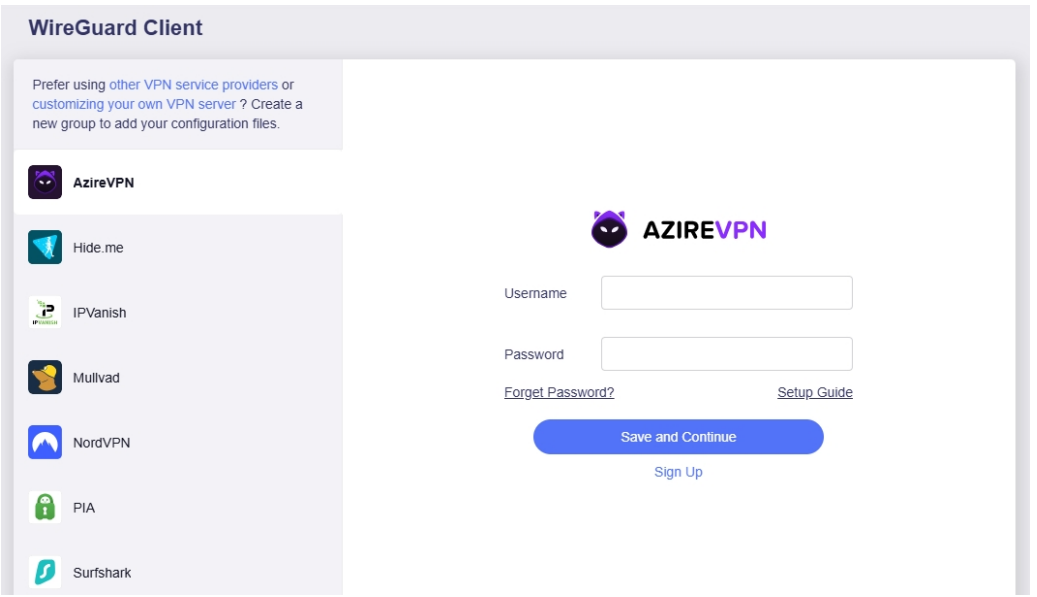
A continuación, sseleccione el proveedor de servicios WireGuard correspondiente a continuación para localizar rápidamente las instrucciones paso a paso.

- 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)

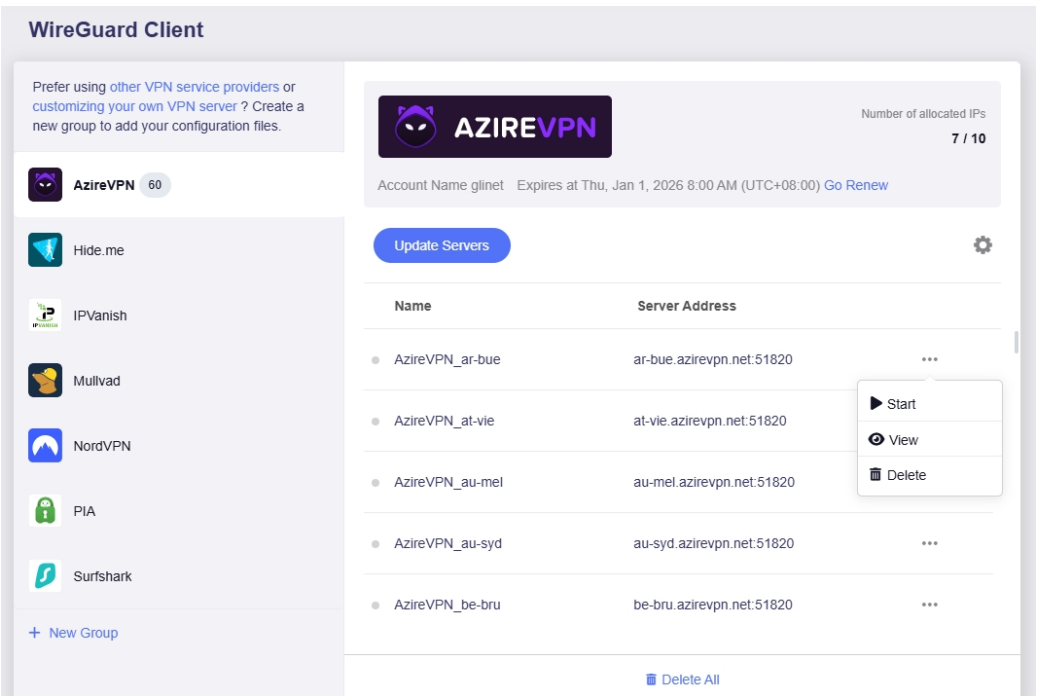
10.2.2 Configurar AzireVPN

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

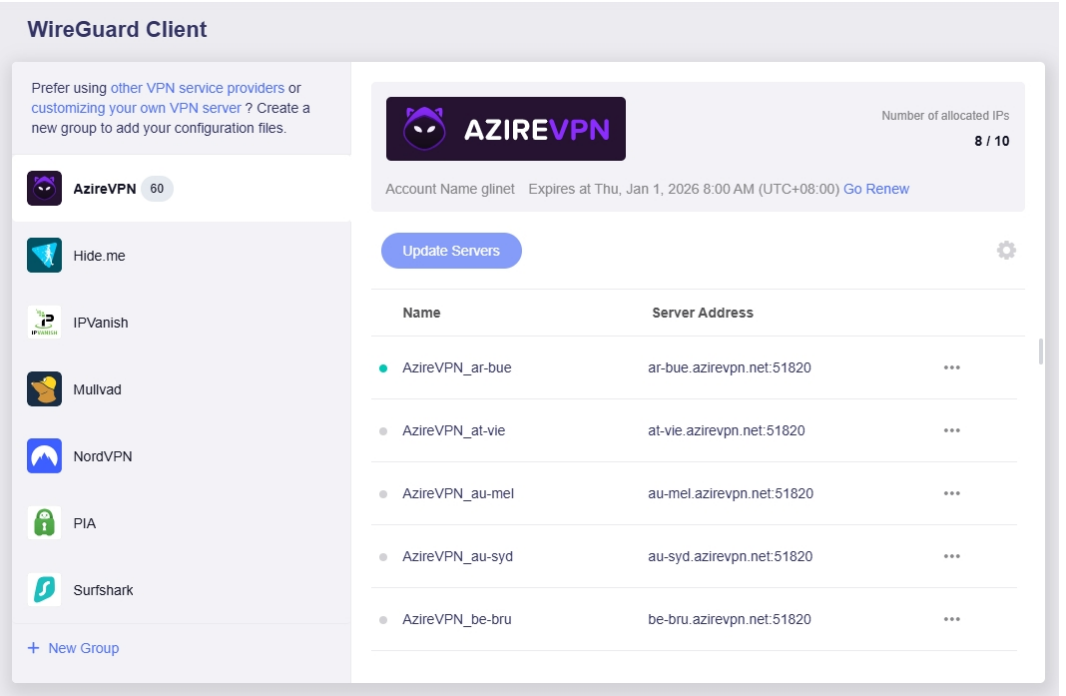
1. Inicie sesiónn en su enrutador’s web admin panel y vaya a **VPN** > **Cliente WireGuard** > **AzireVPN**.
2. Ingrese nombre de usuario y contraseña, luego haga clic en **Guardar y continuar**. Generará archivos de configuración para cada servidor.



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



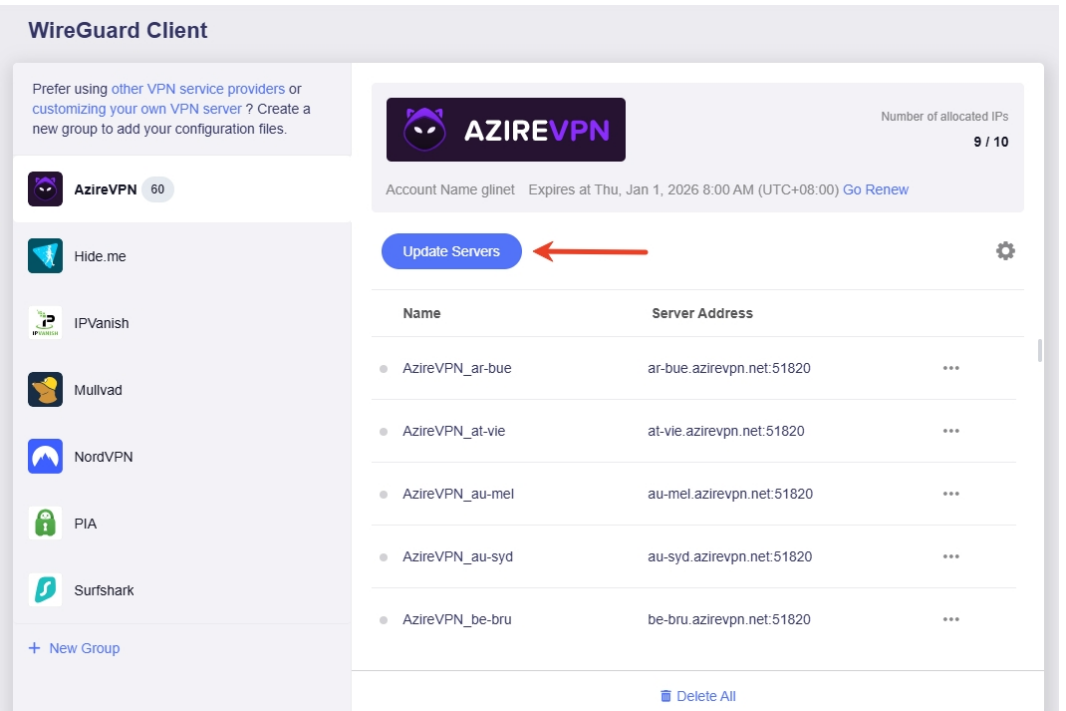
4. Una vez conectado, aparecerá un punto verde junto al archivo de configuración.



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

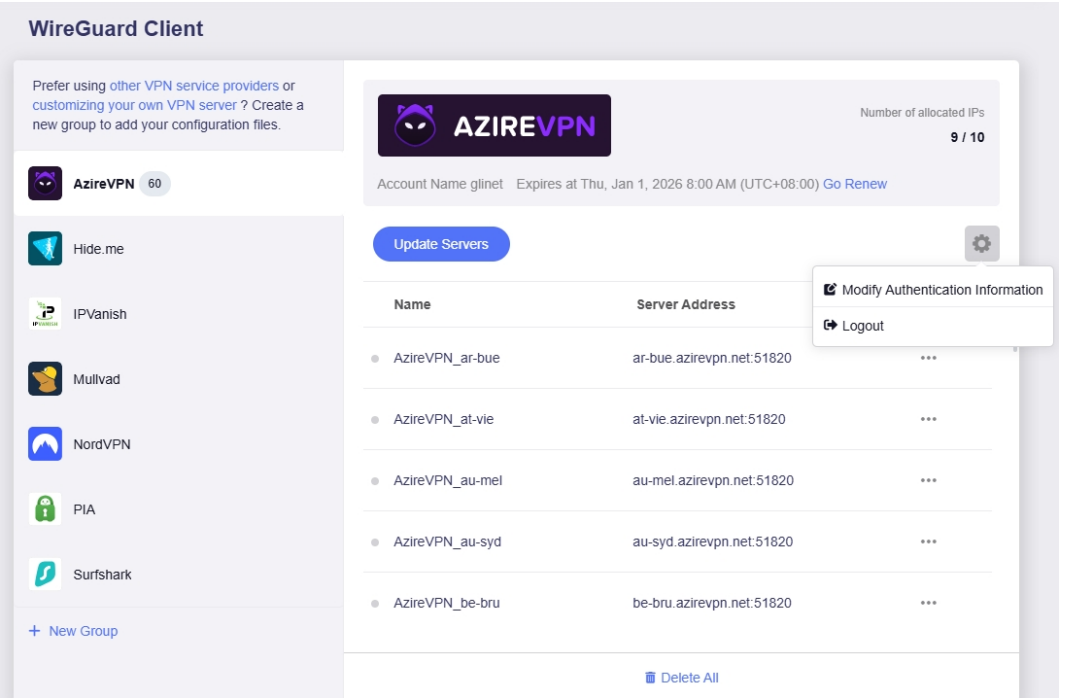
5. Actualizar servidores.

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.



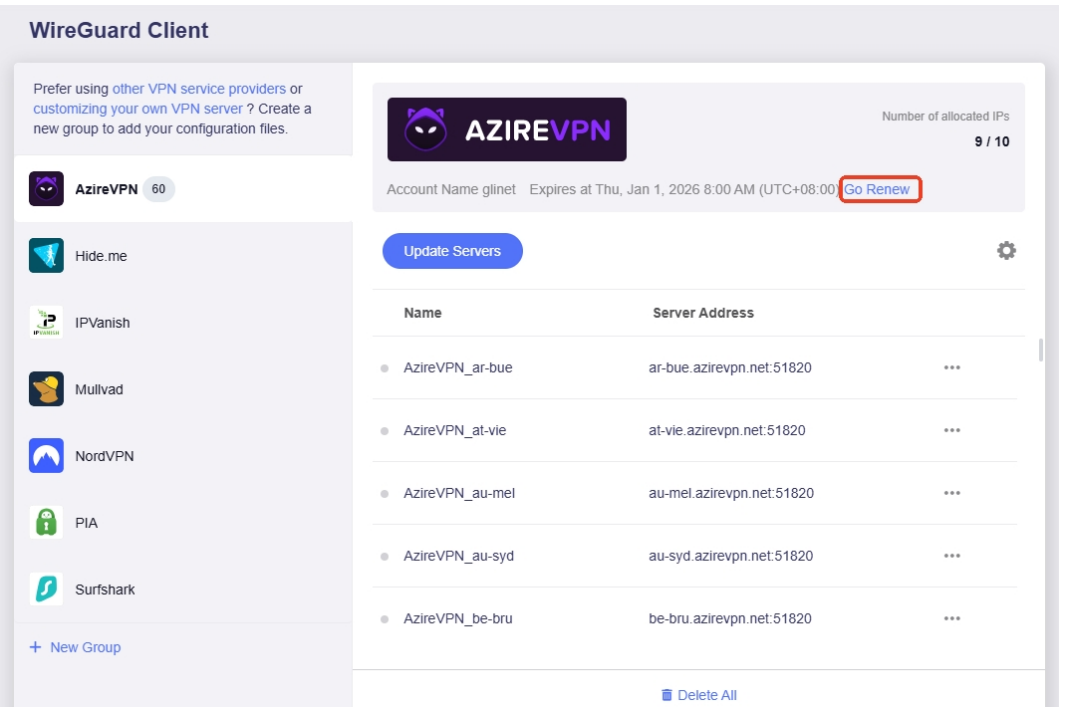
6. Editar credenciales o cerrar sesión.

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



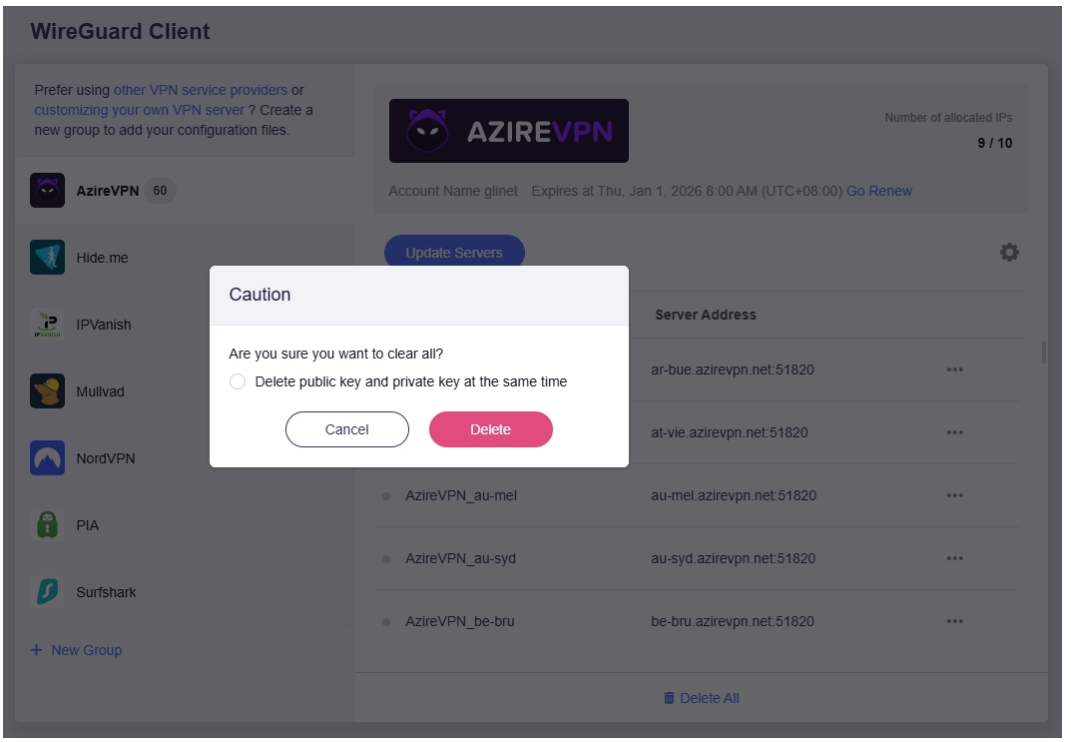
7. Ir a renovar.

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



8. Eliminar todos los archivos.

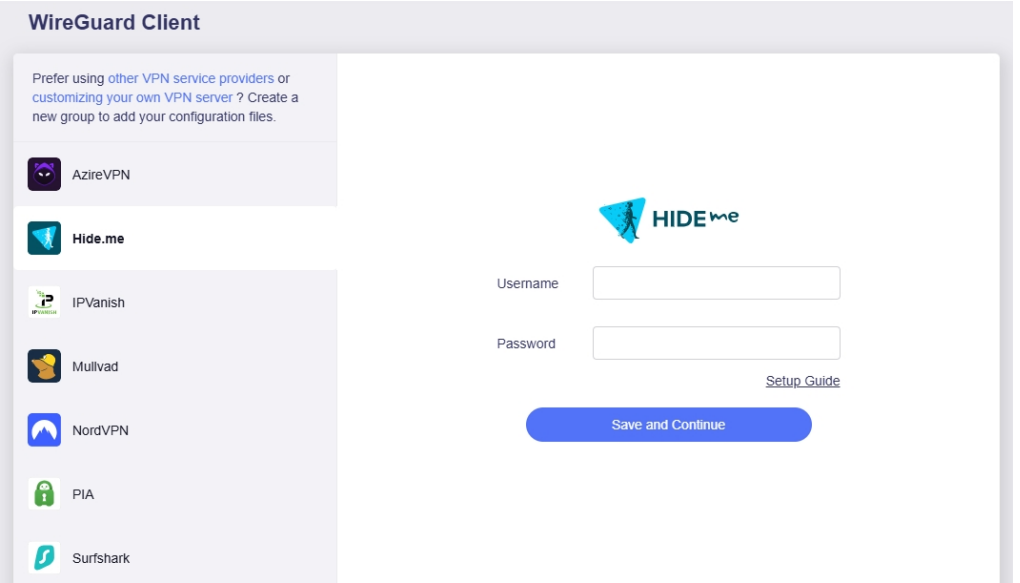
   Puedes hacer clic en **Eliminar todo** para eliminar todos los archivos de configuración con un solo clic y elija si desea eliminar las claves pública y privada simultáneamente.



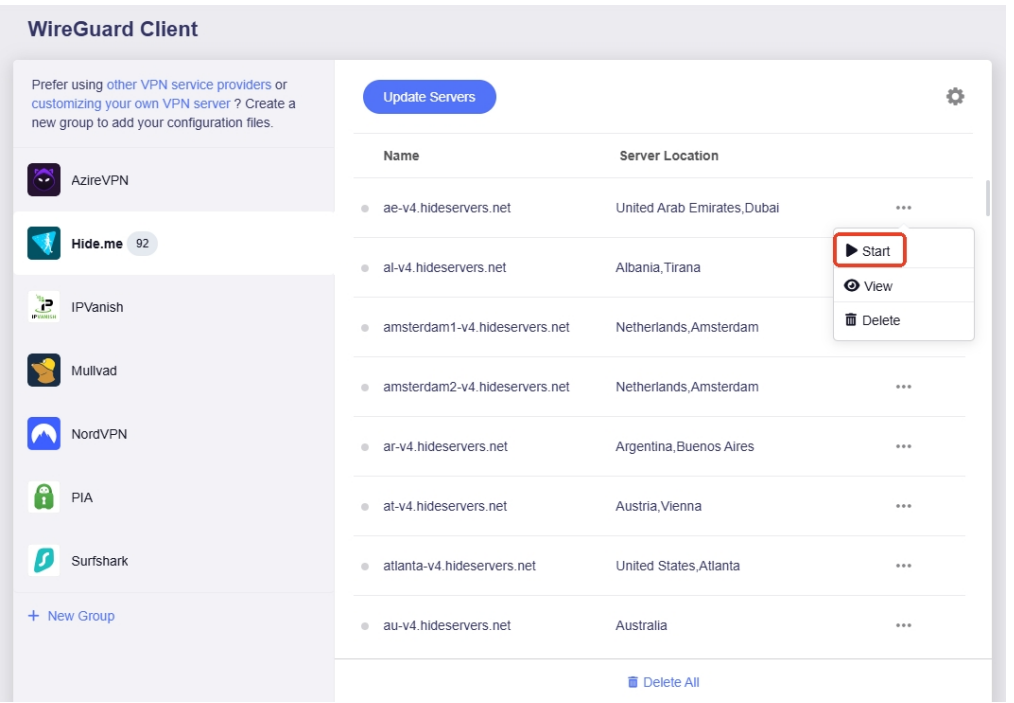
10.2.3 Configurar Hide.me

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

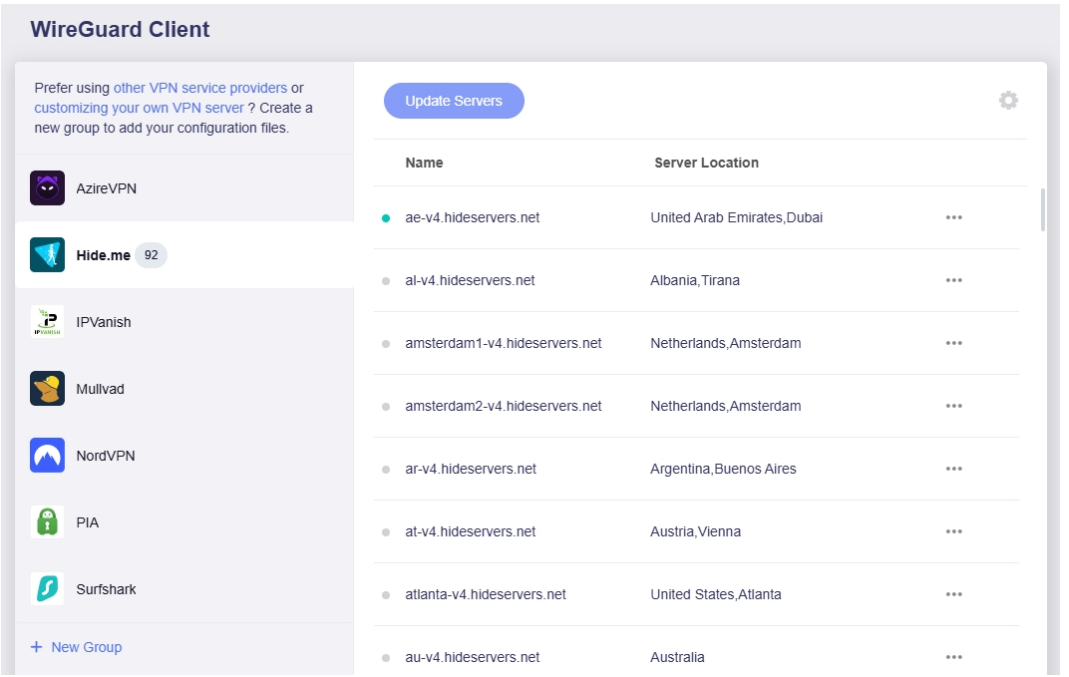
1. Iniciar sesión in a su enrutador’s web admin panel y vaya a **VPN** > **WireGuard Client** > **Hide.me**.
2. Ingrese nombre de usuario y contraseña, luego haga clic en **Guardar y continuar**. Generará archivos de configuración para cada servidor.



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



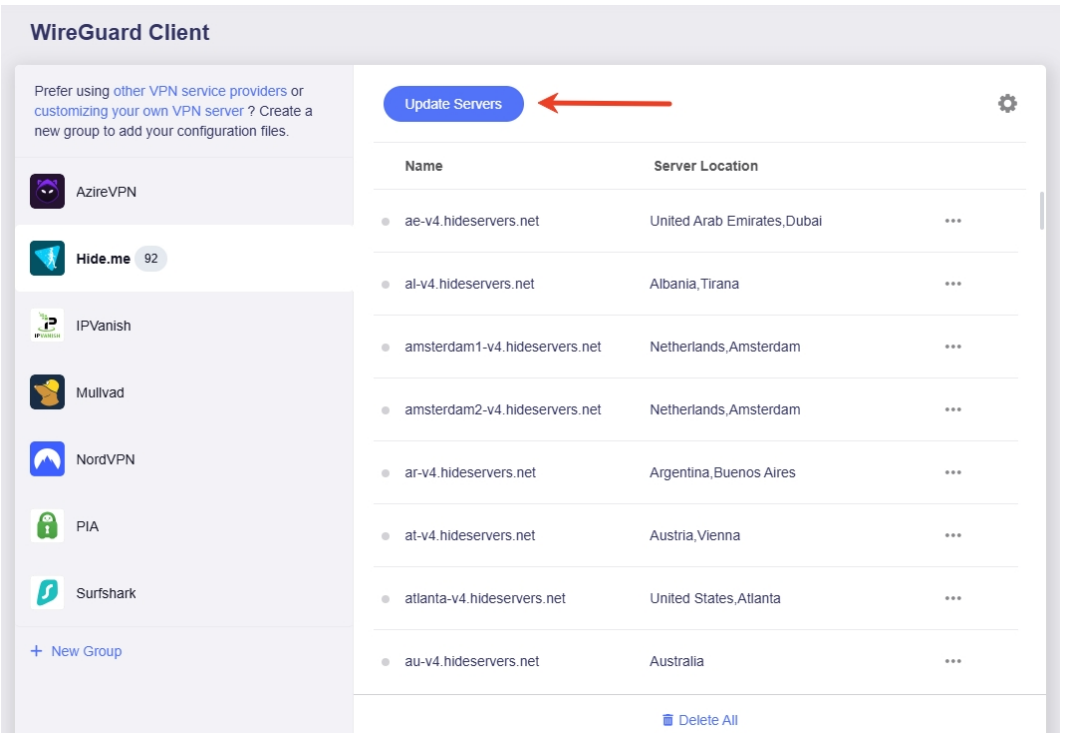
4. Una vez conectado, aparecerá un punto verde junto al archivo de configuración.



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

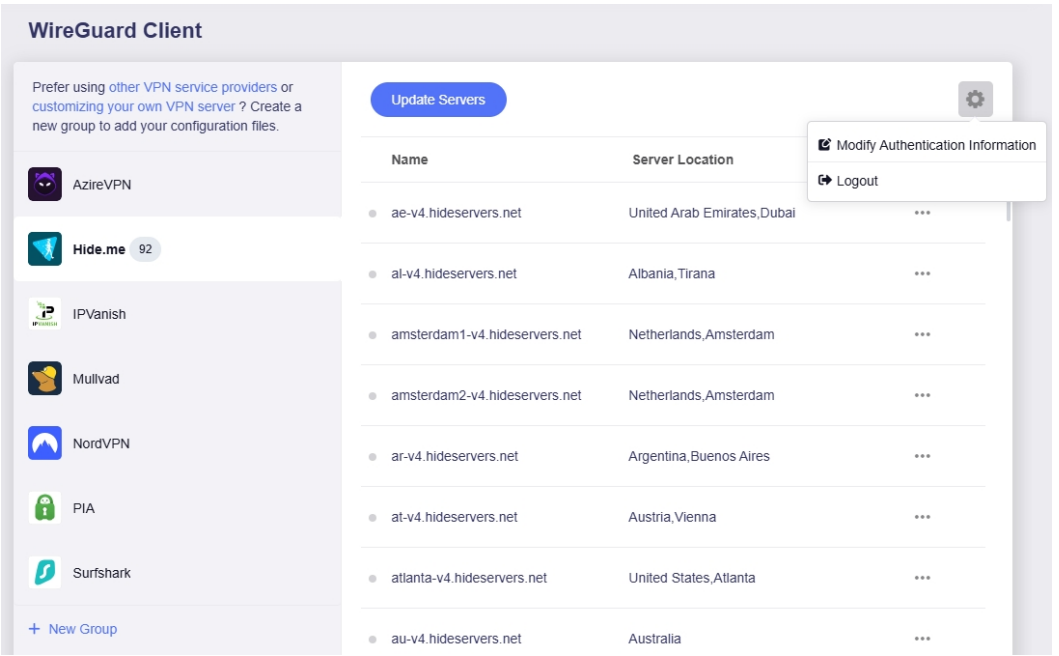
5. Actualizar servidores.

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.



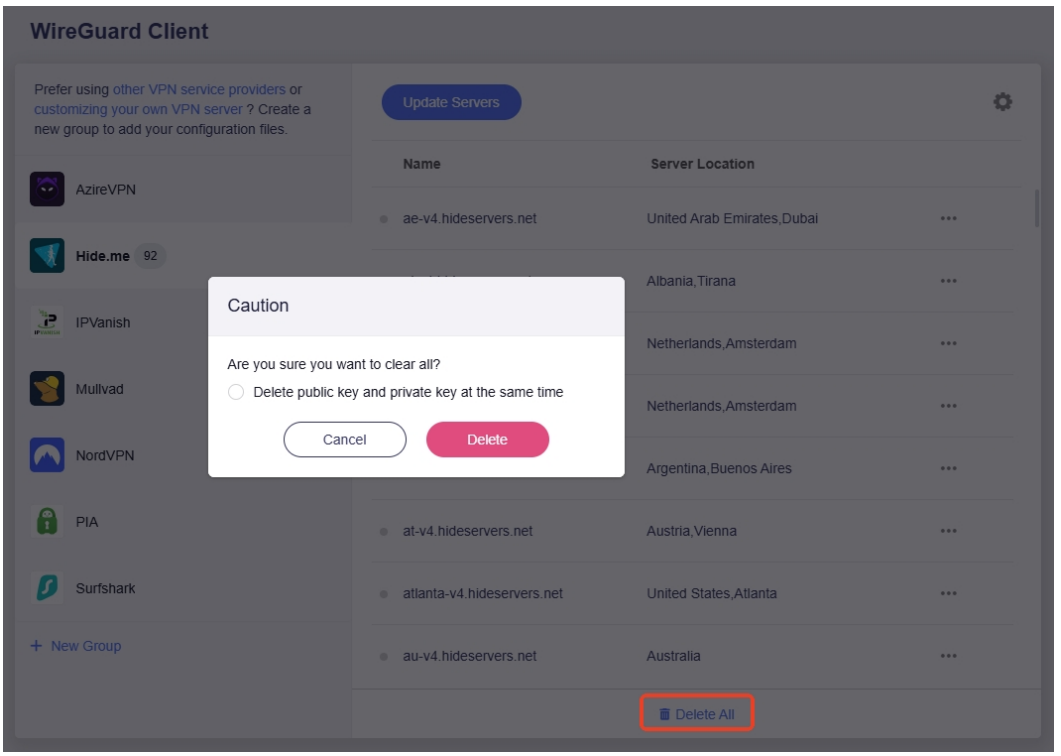
6. Edite las credenciales o cierre sesión.

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



7. Eliminar todos los archivos.

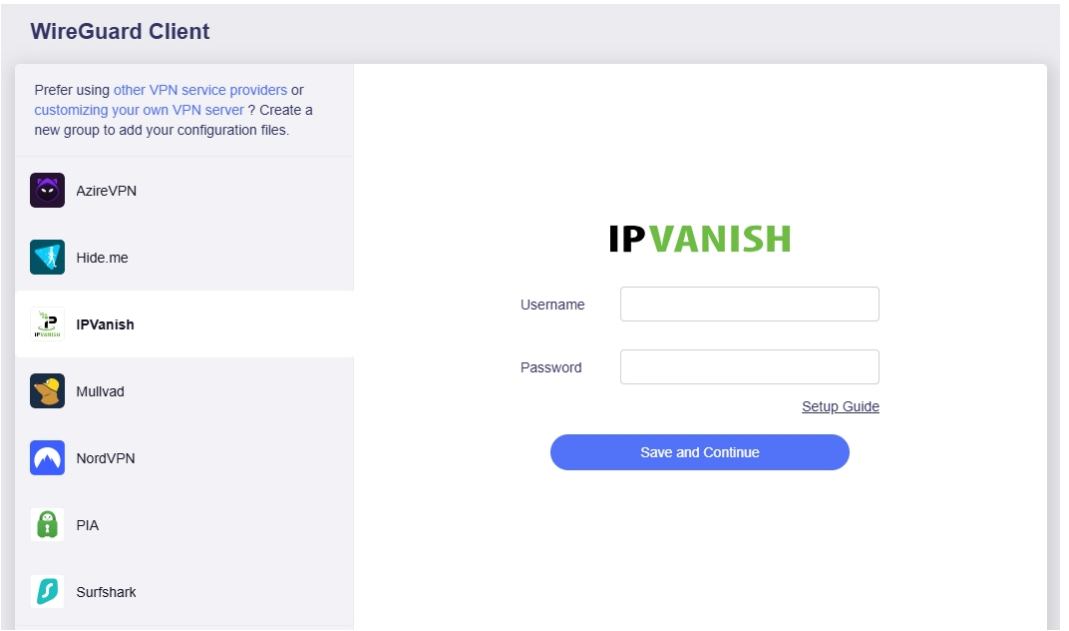
   Puede hacer clic en **Eliminar todo** para eliminar todos los archivos de configuración con un solo clic y elegir si desea eliminar las claves pública y privada simultáneamente.



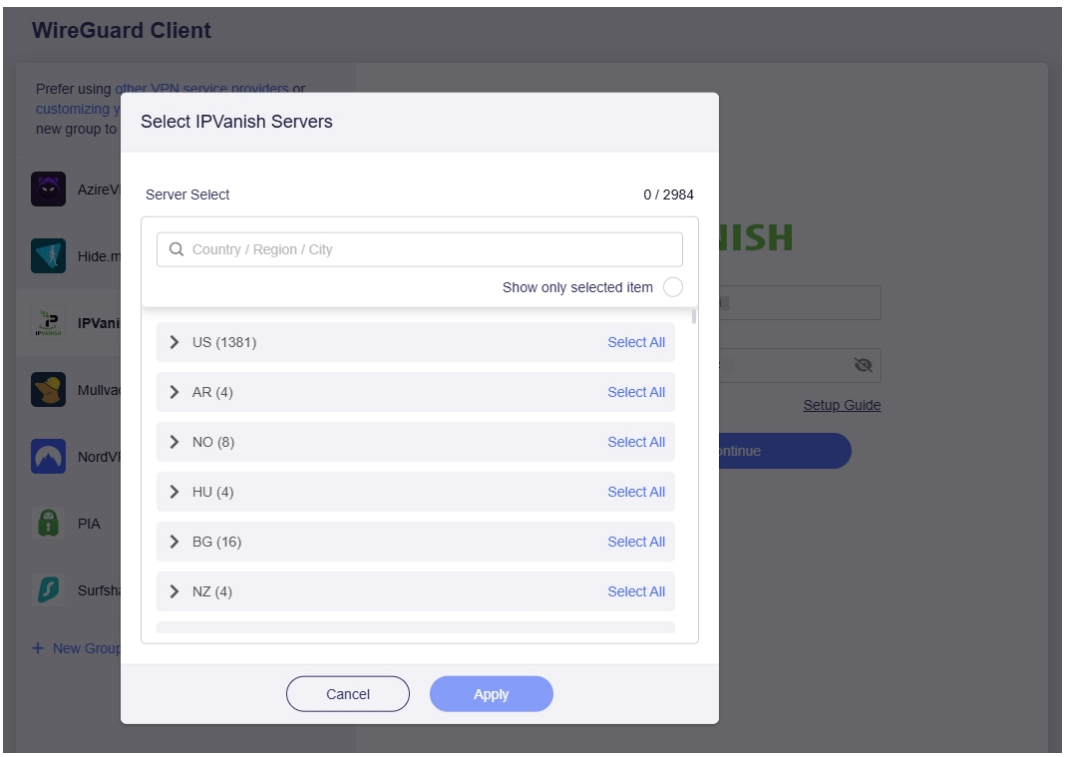
10.2.4 Configurar IPVanish

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

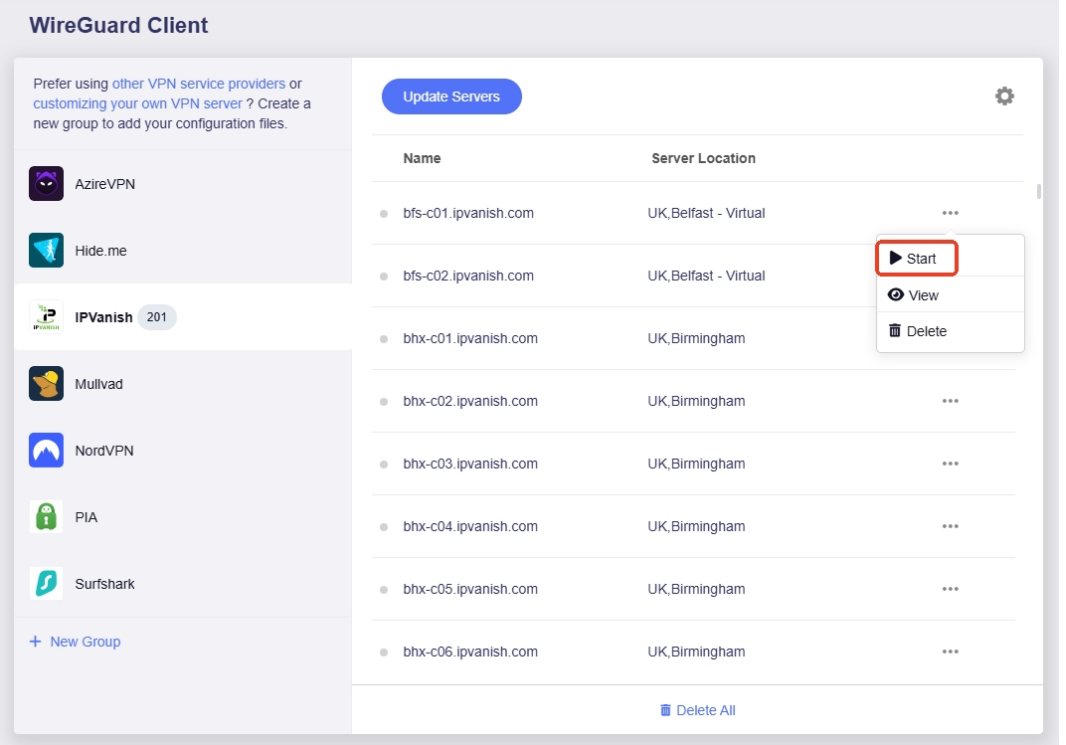
1. Registro in a su enrutador’s web admin panel y vaya a **VPN** > **WireGuard Client** > **IPVanish**.
2. Ingrese nombre de usuario y contraseña, luego haga clic en **Guardar y continuar**.



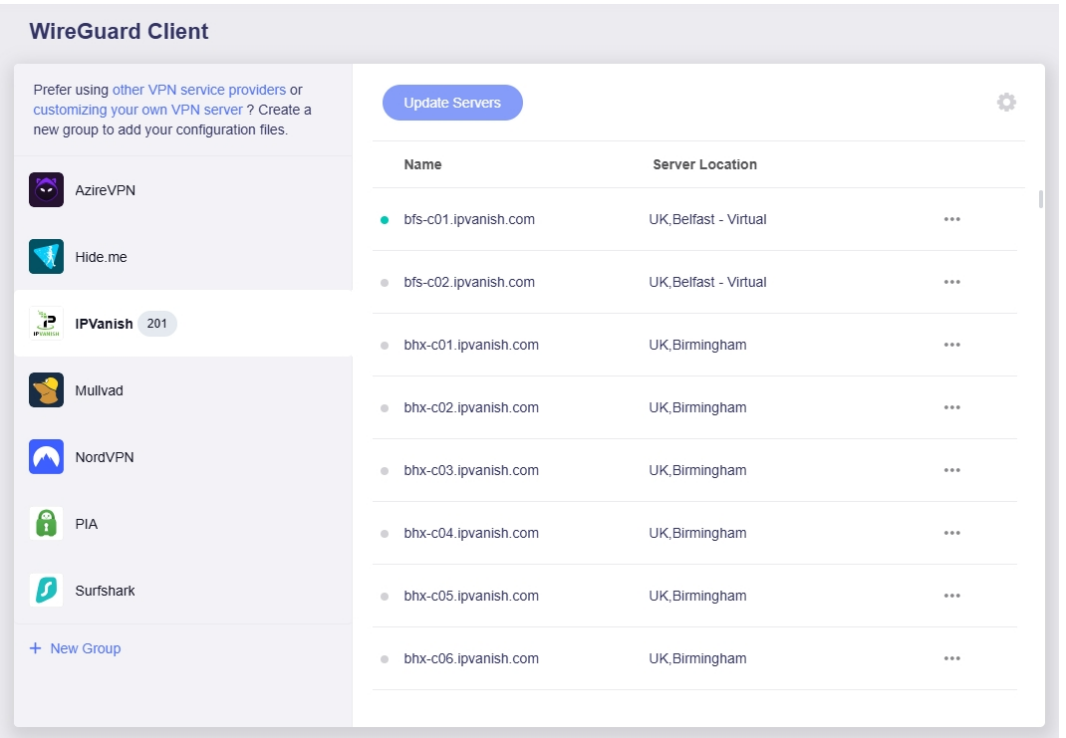
3. Seleccione los servidores a los que desea conectarse y haga clic en **Aplicar**.



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



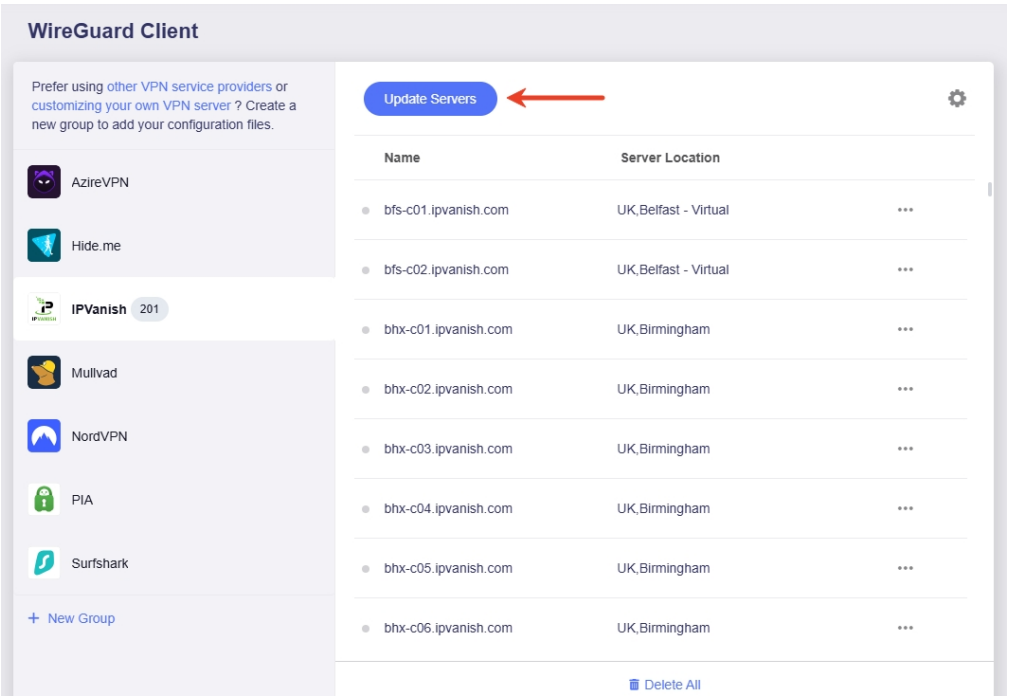
5. Una vez conectado, aparecerá un punto verde junto al archivo de configuración.



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

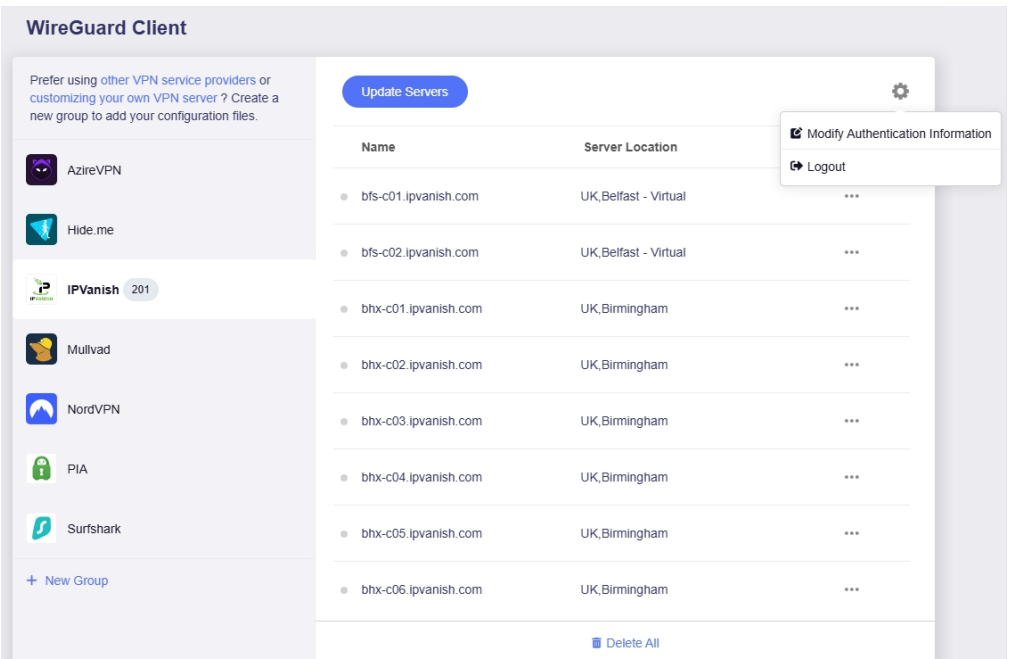
6. Actualizar servidores.

   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.



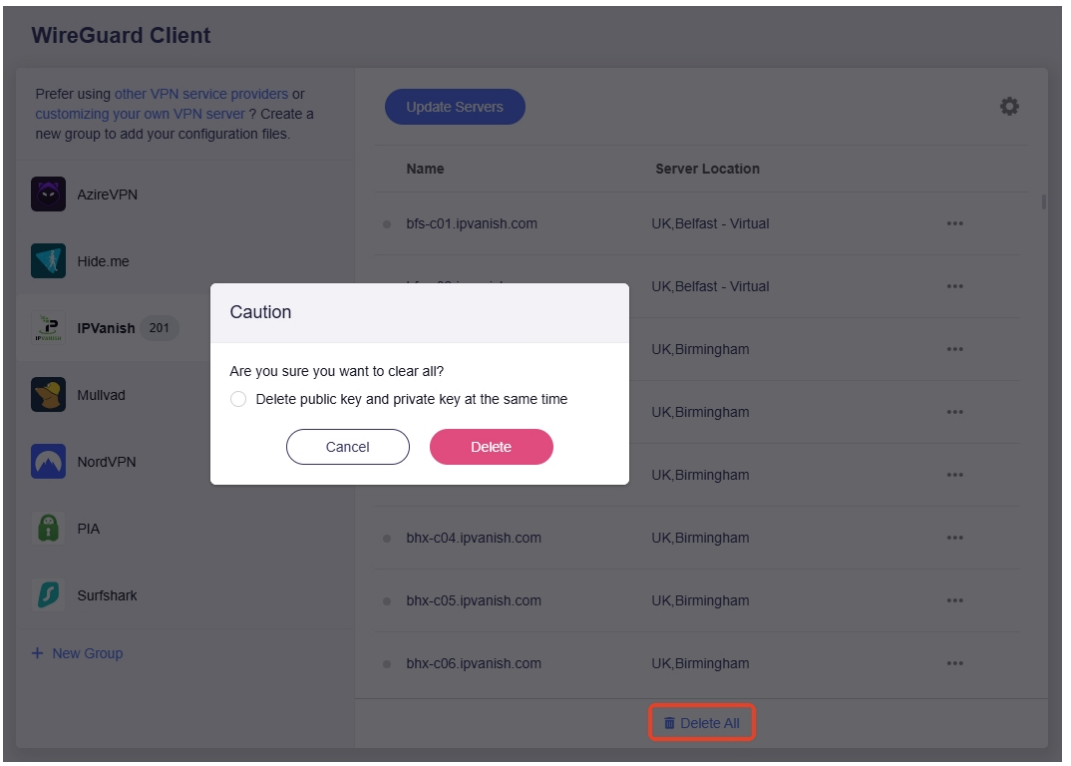
7. Editar credenciales o cerrar sesión.

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



8. Eliminar todos los archivos.

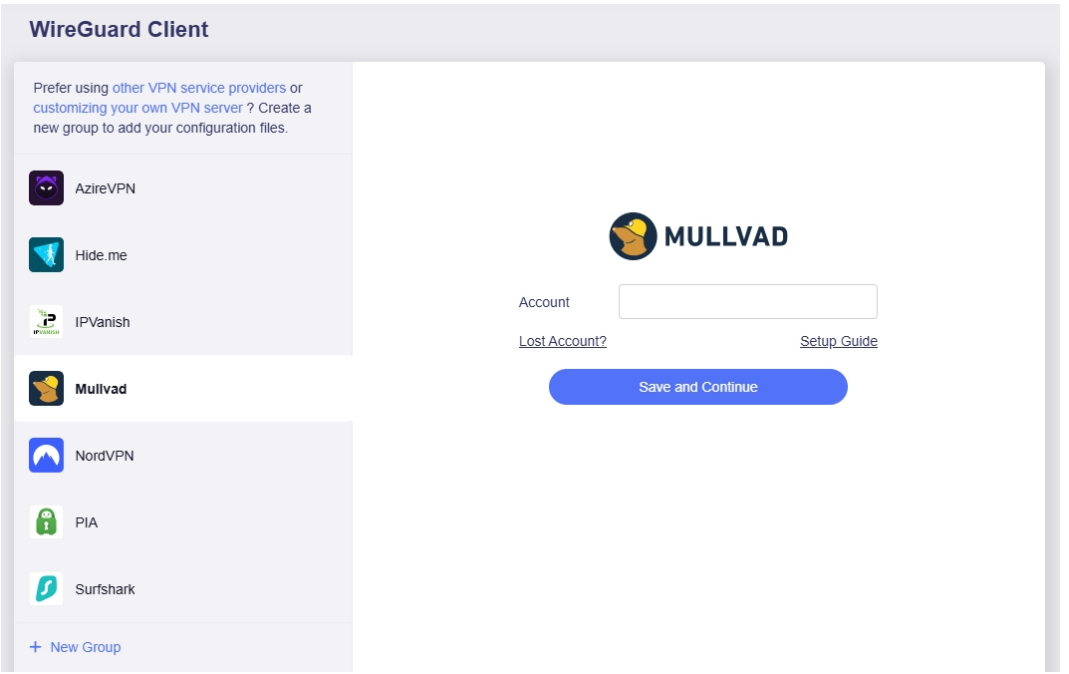
   Puede hacer clic en **Eliminar todo** para eliminar todos los archivos de configuración con un solo clic y elija si desea eliminar las claves públicas y privadas simultáneamente.



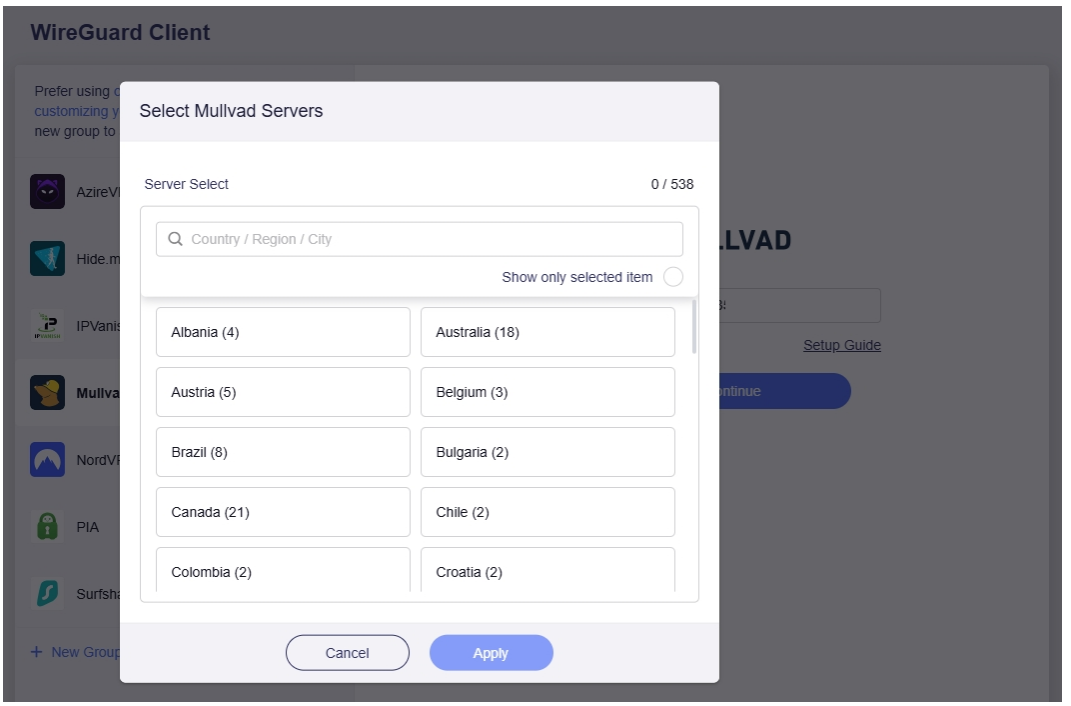
10.2.5 Configurar Mullvad

Siga los pasos a continuación para configurar su enrutador como Cliente Mullvad.

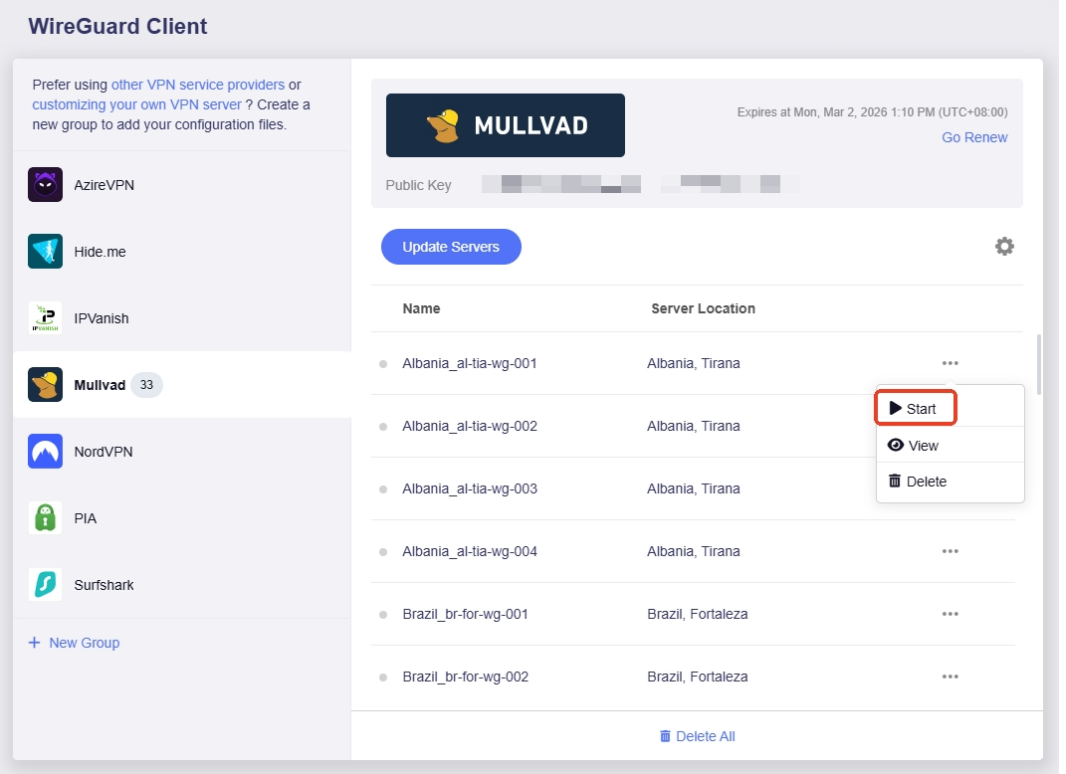
1. Inicie sesiónn en su enrutador’s web admin panel y vaya a **VPN** > **WireGuard Client** > **Mullvad**.
2. Ingrese nombre de usuario y contraseña, luego haga clic en **Guardar y continuar**.



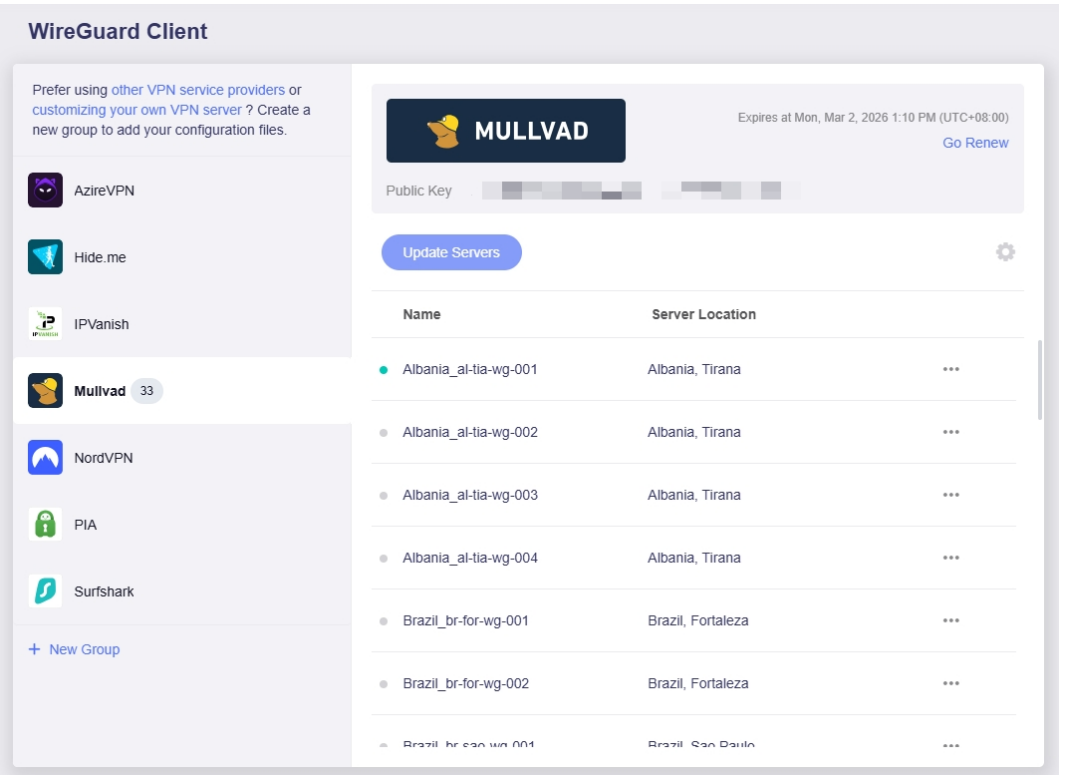
3. Seleccione los servidores a los que desea conectarse y haga clic en **Aplicar**.



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



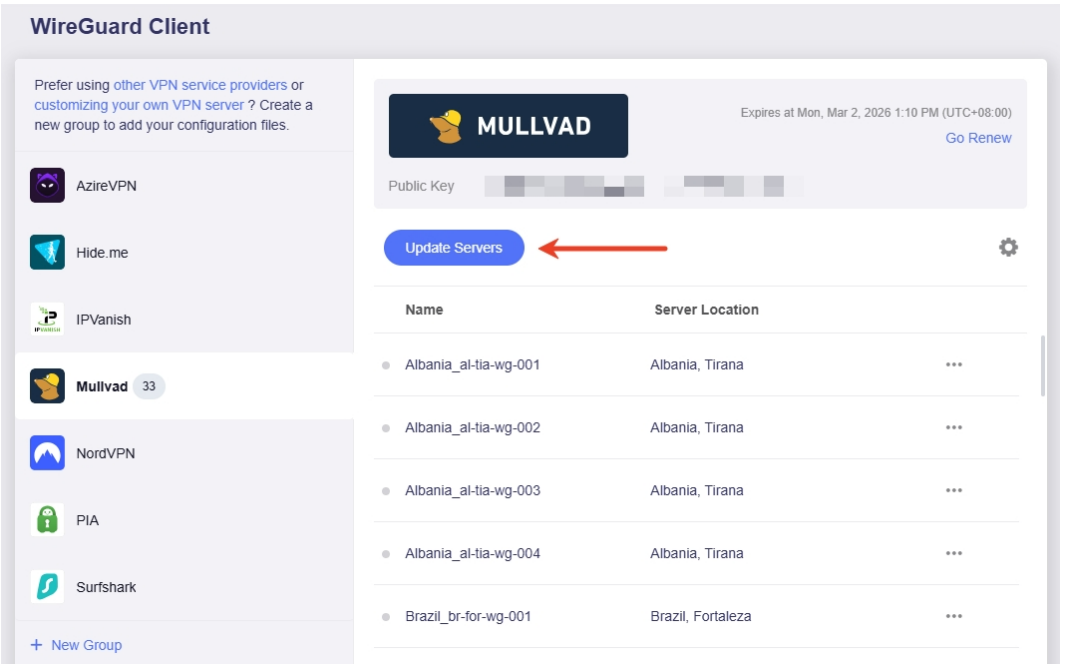
5. Una vez conectado, aparecerá un punto verde junto al archivo de configuración.



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

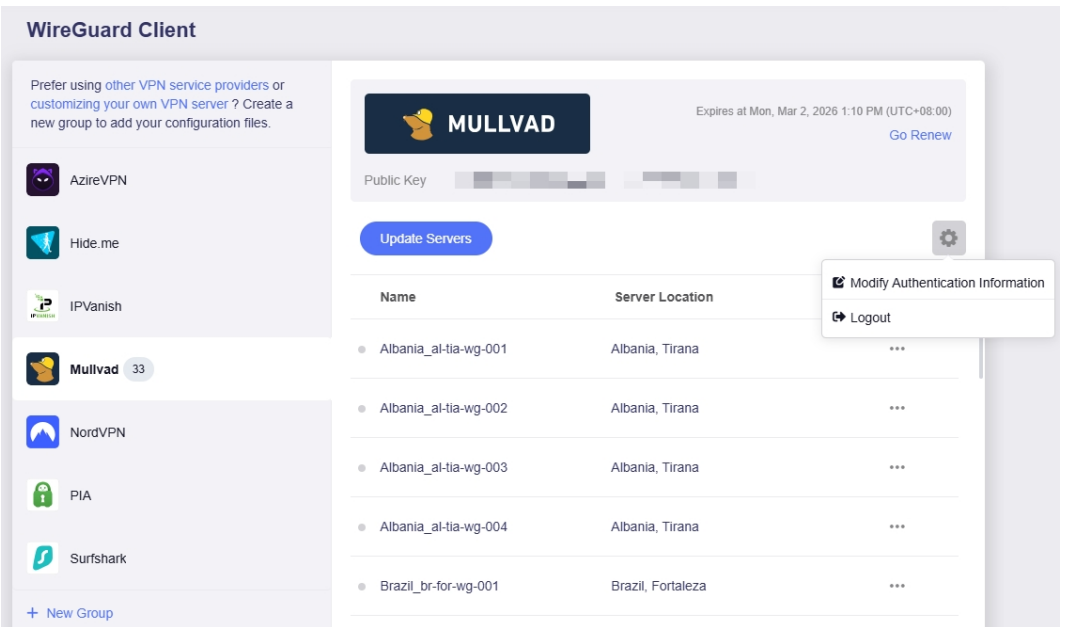
6. Actualizar servidores.

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



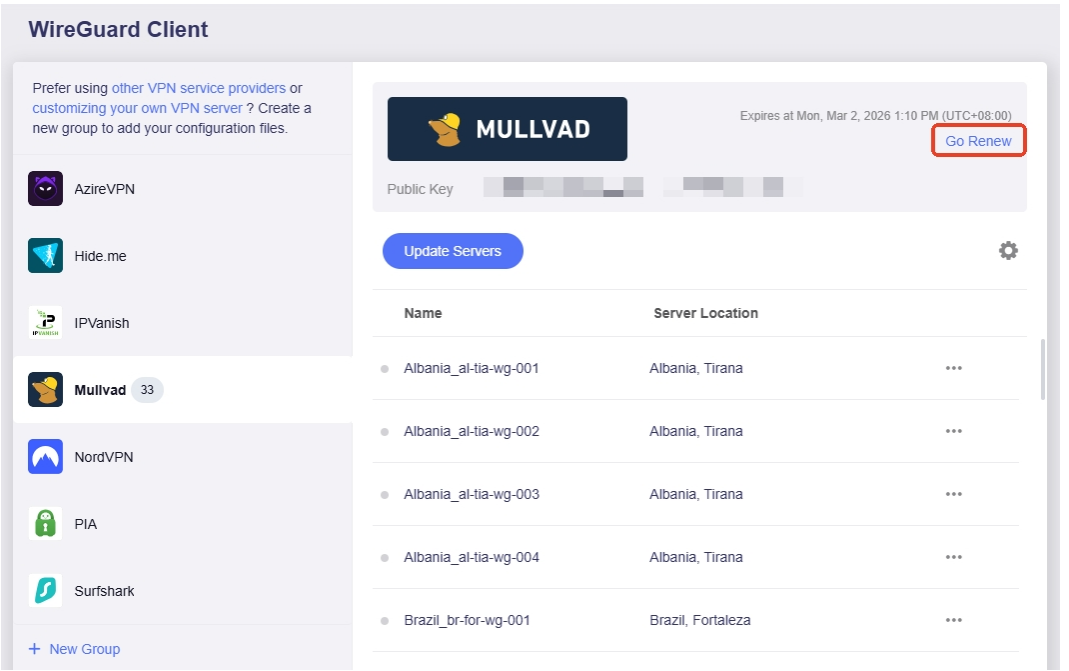
7. Edite las credenciales o cierre sesión.

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



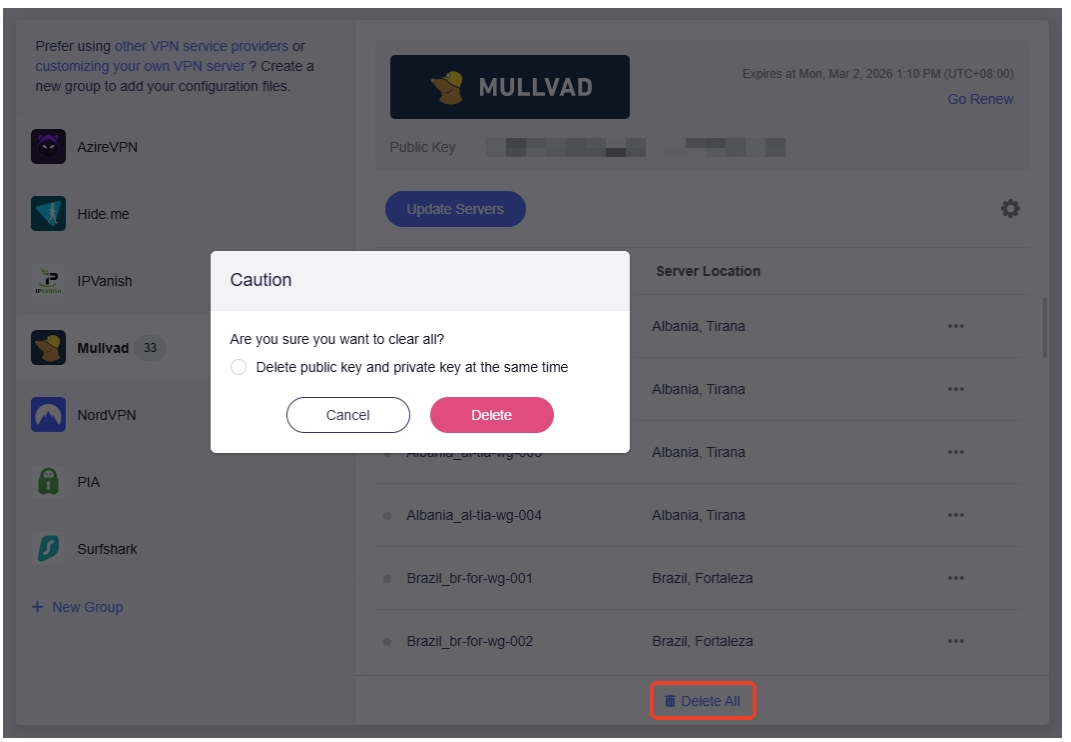
8. Vaya a renovar.

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



9. Eliminar todos los archivos.

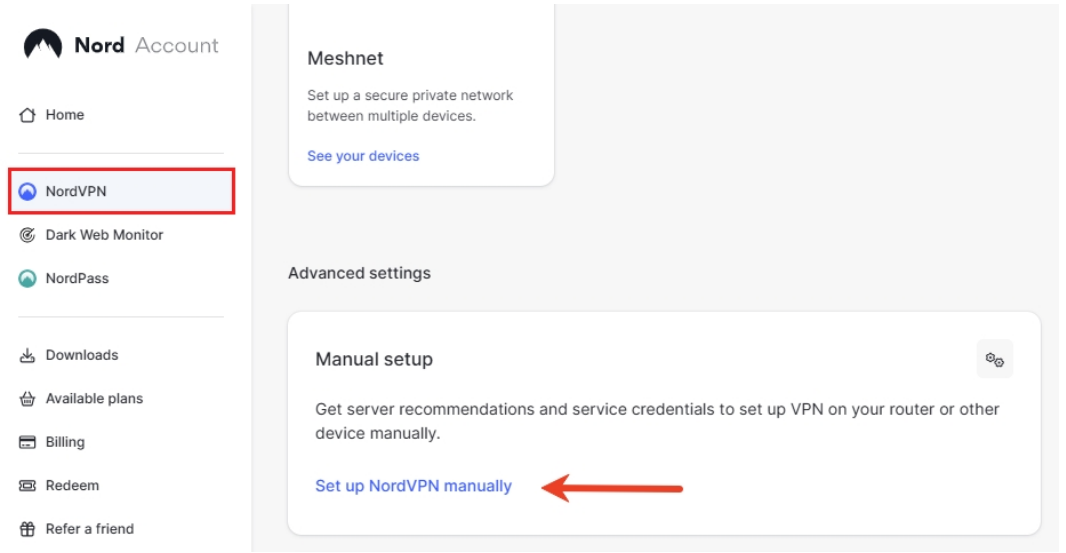
   Puede hacer clic en **Eliminar todo** para eliminar todos los archivos de configuración con un solo clic y elegir si desea eliminar las claves pública y privada simultáneamente.



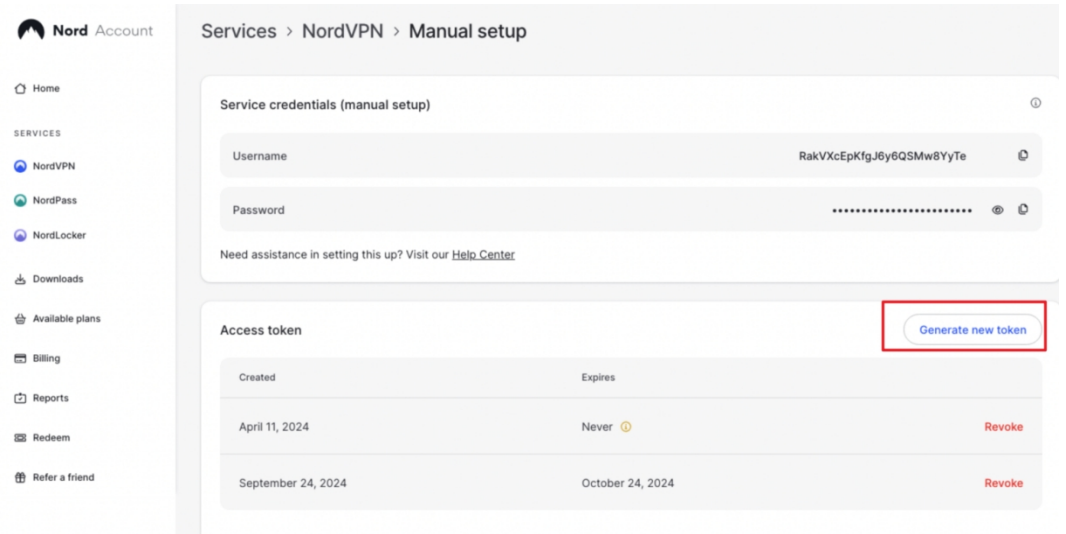
10.2.6 Configurar NordVPN

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

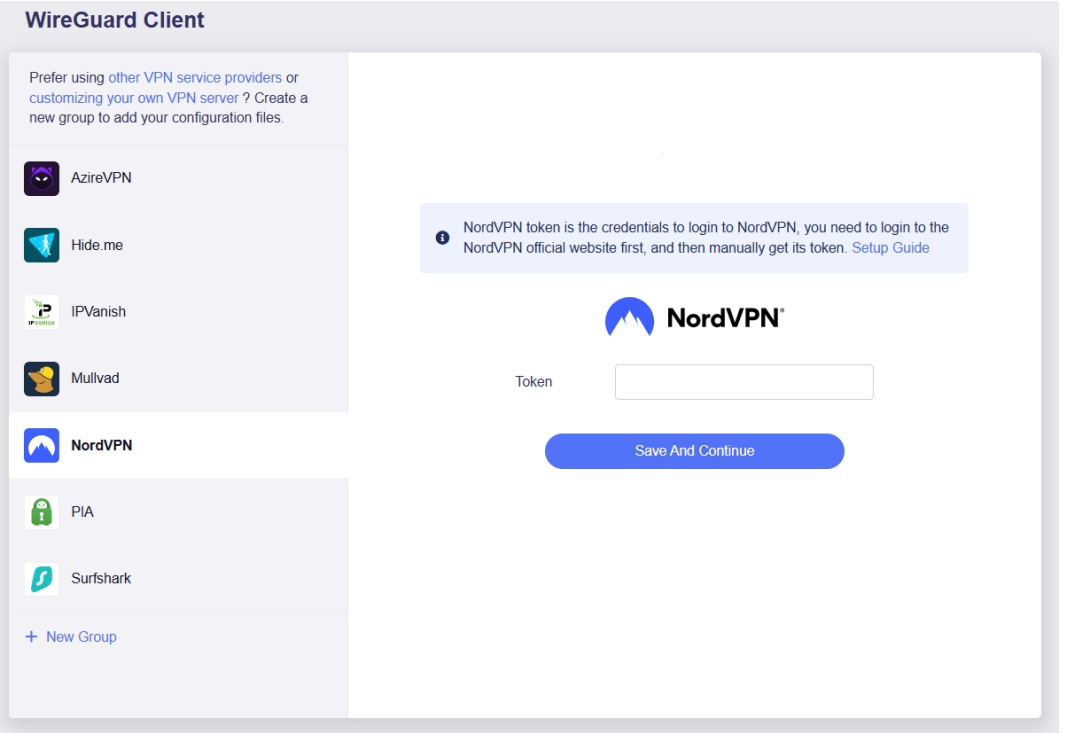
1. Inicie sesión en su cuenta web NordVPN aquí.
2. Oen Nord Dashboard, haga clic en **NordVPN**, luego haga clic en **Configurar NordVPN manualmente**.



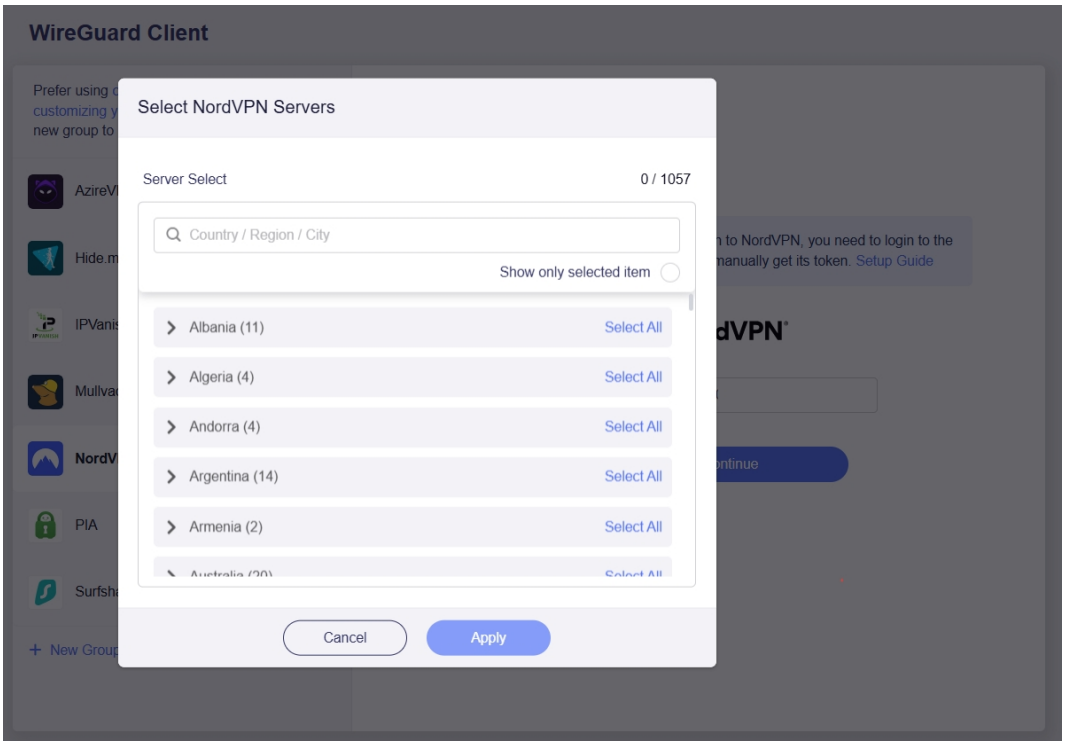
Encontrará el **Token de acceso**. Cree un token de acceso y Ccopia para su uso posterior.



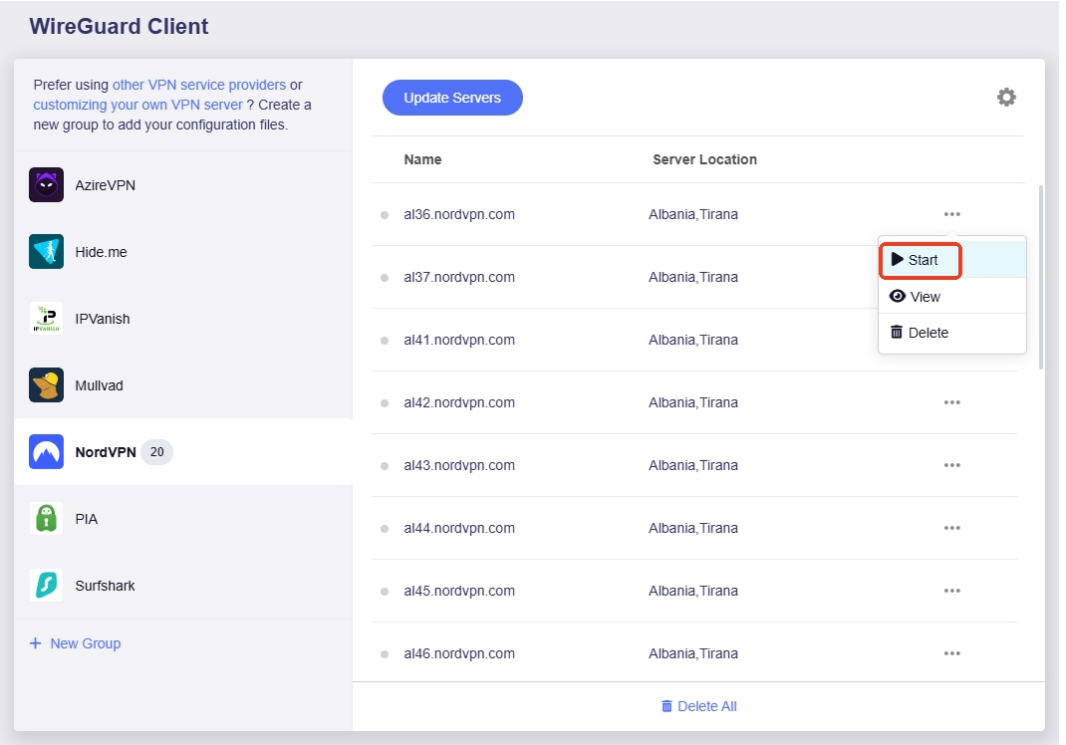
3. Inicie sesiónn en su enrutador's web admin panel y vaya a **VPN** > **Cliente WireGuard** > **NordVPN**.
4. Entrada token, y haga clic en **Guardar y continuar**.



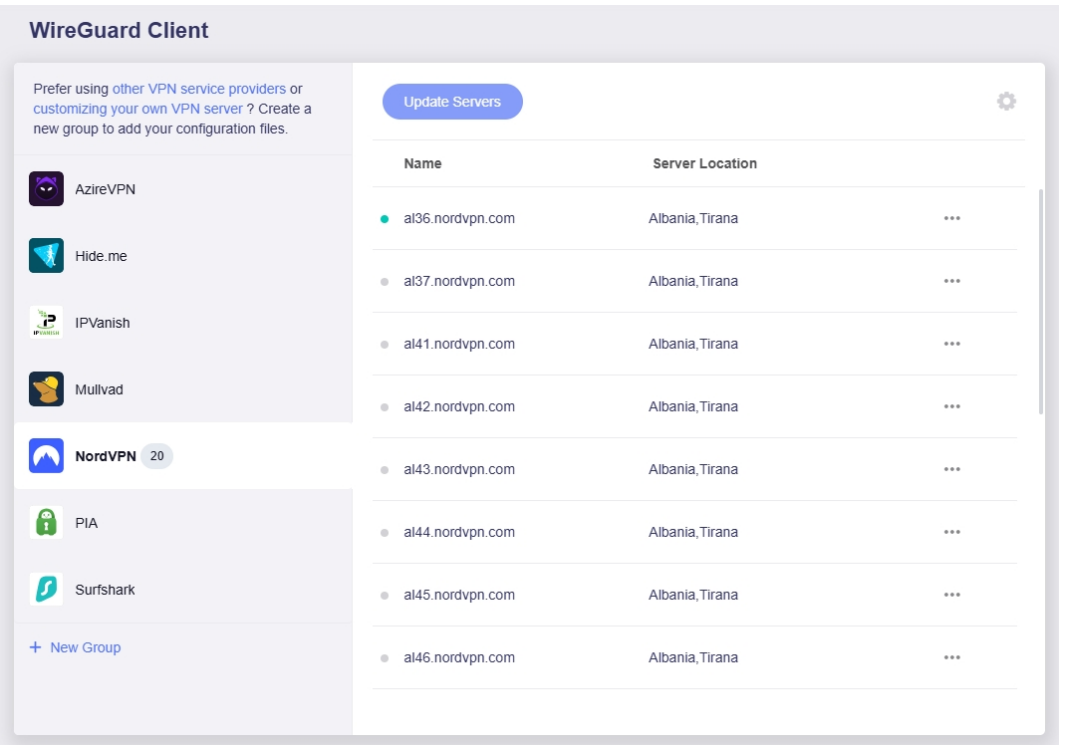
5. Seleccione los servidores a los que desea conectarse y haga clic en **Aplicar**.



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



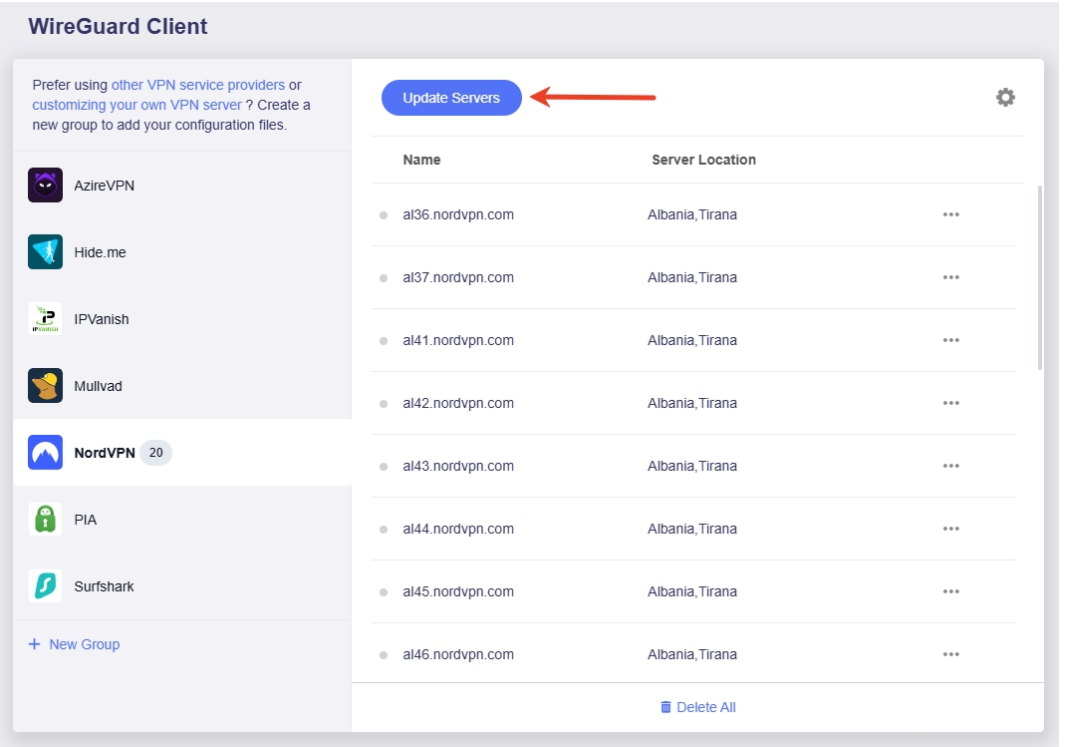
7. Una vez conectado, aparecerá un punto verde junto al archivo de configuración.



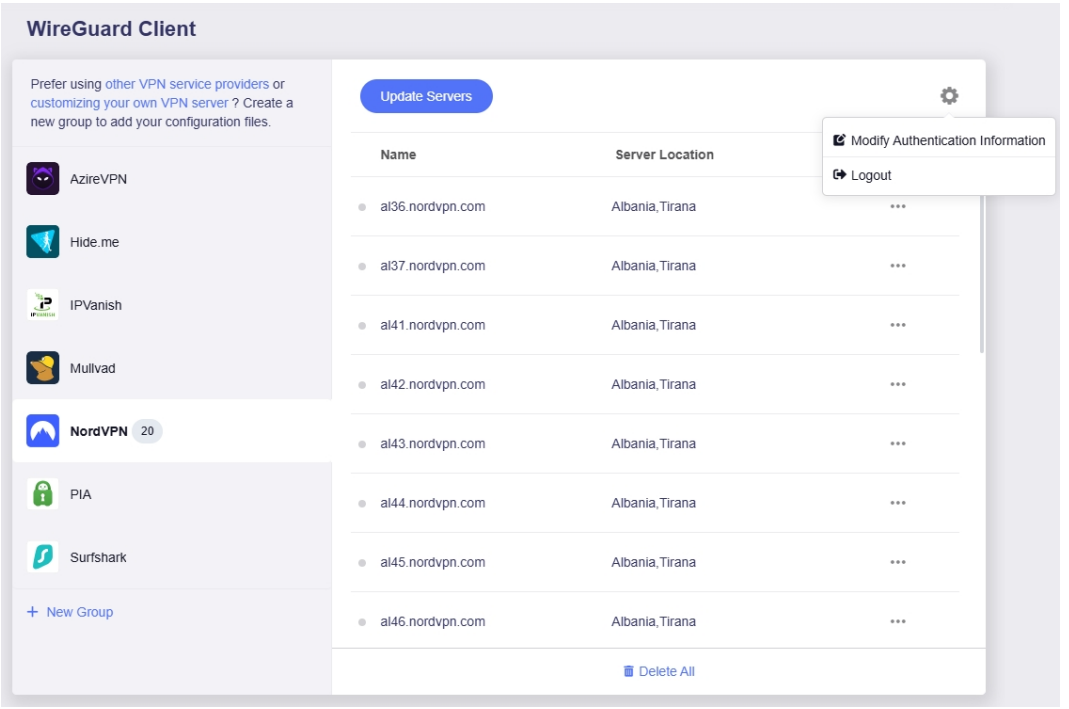
Usted puede también comprobar el Detalles de la conexión VPN en **Panel de VPN**.

8. Actualizar servidores.

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

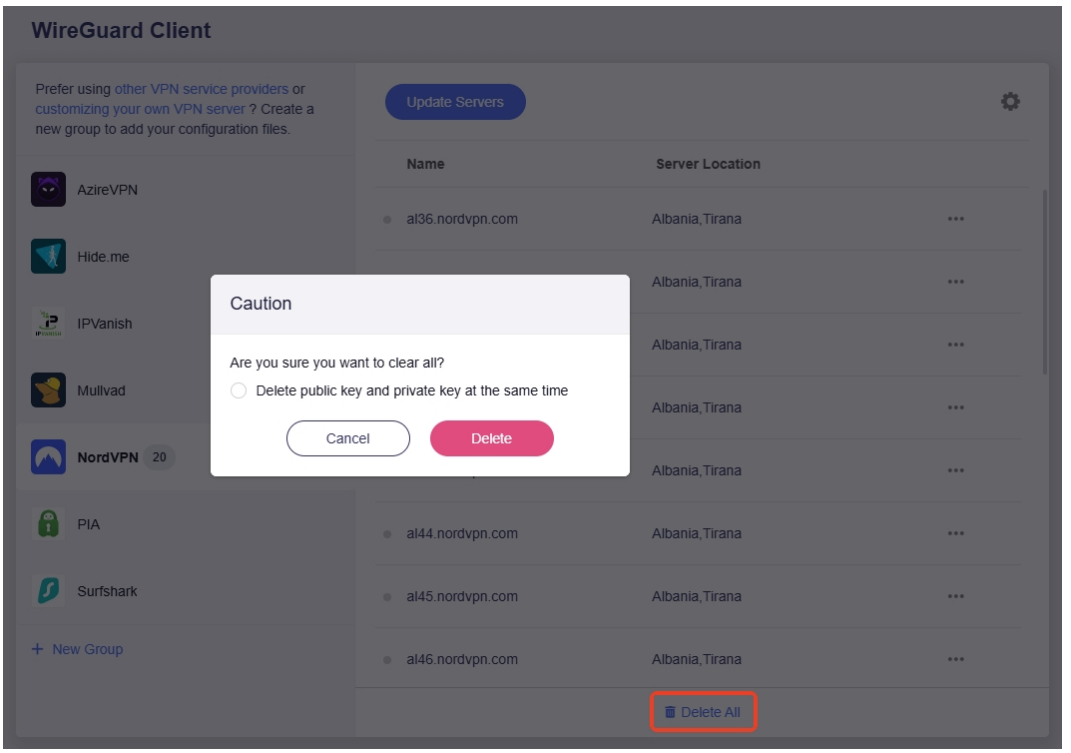


9. Edite las credenciales o cierre sesión.
   Haga clic en el ícono de ajustes para editar sus credenciales de inicio de sesión o cerrar sesión.



10. Eliminar todos los archivos.

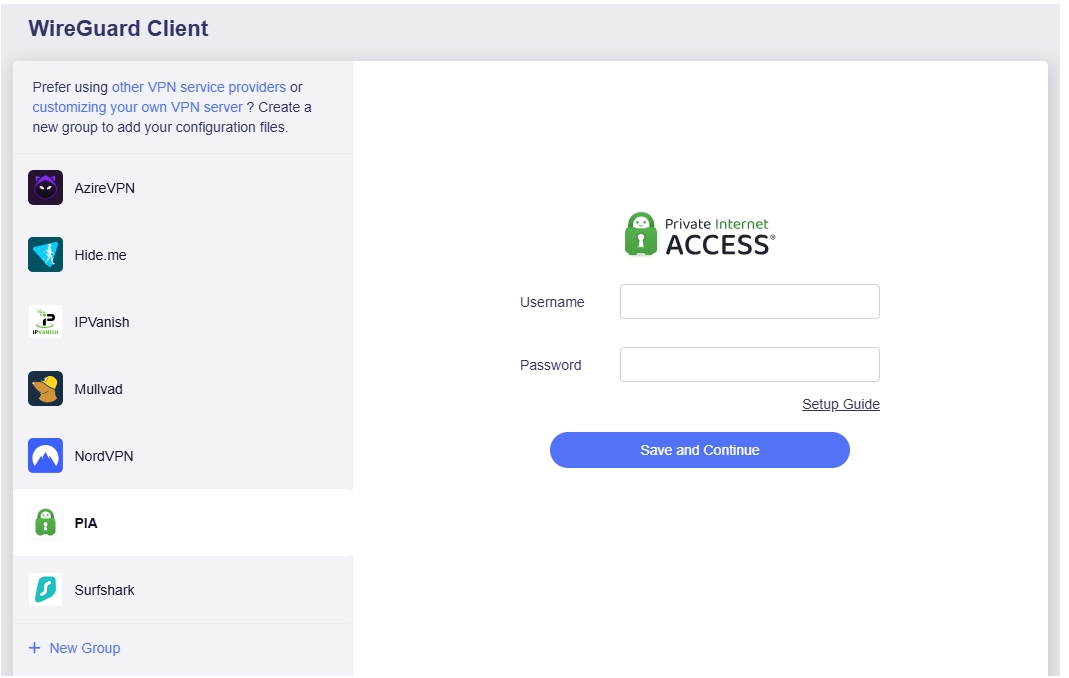
    Puedes hacer clic en **Eliminar todo** para eliminar todos los archivos de configuración con un solo clic y elija si desea eliminar las claves pública y privada simultáneamente.



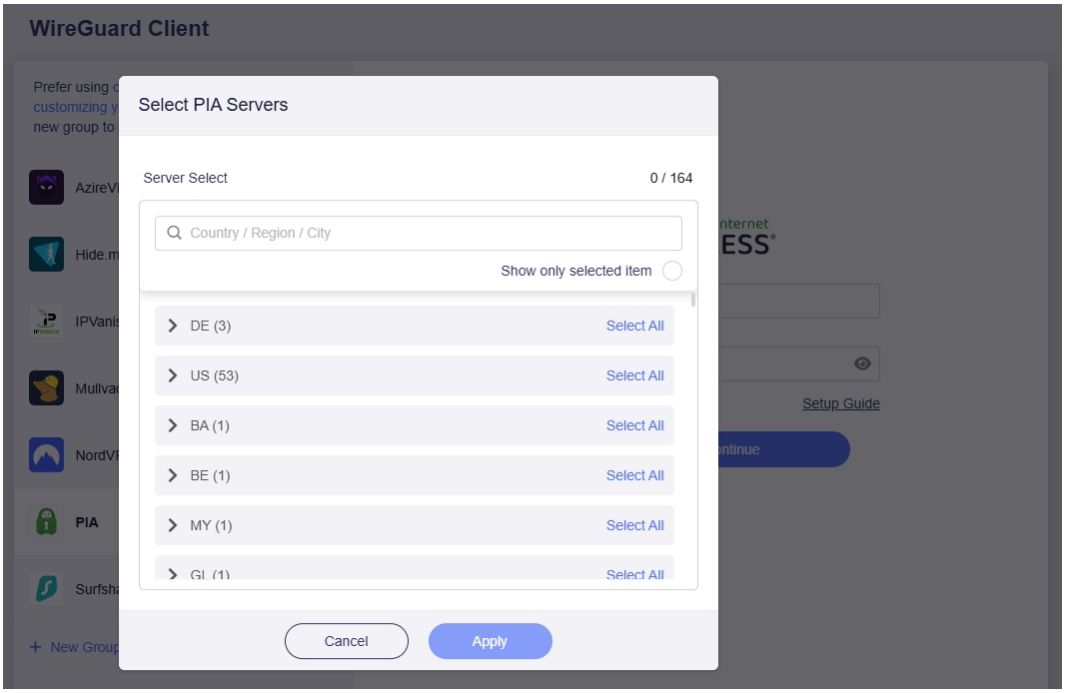
10.2.7 Configurar PIA (Private Internet Access)

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

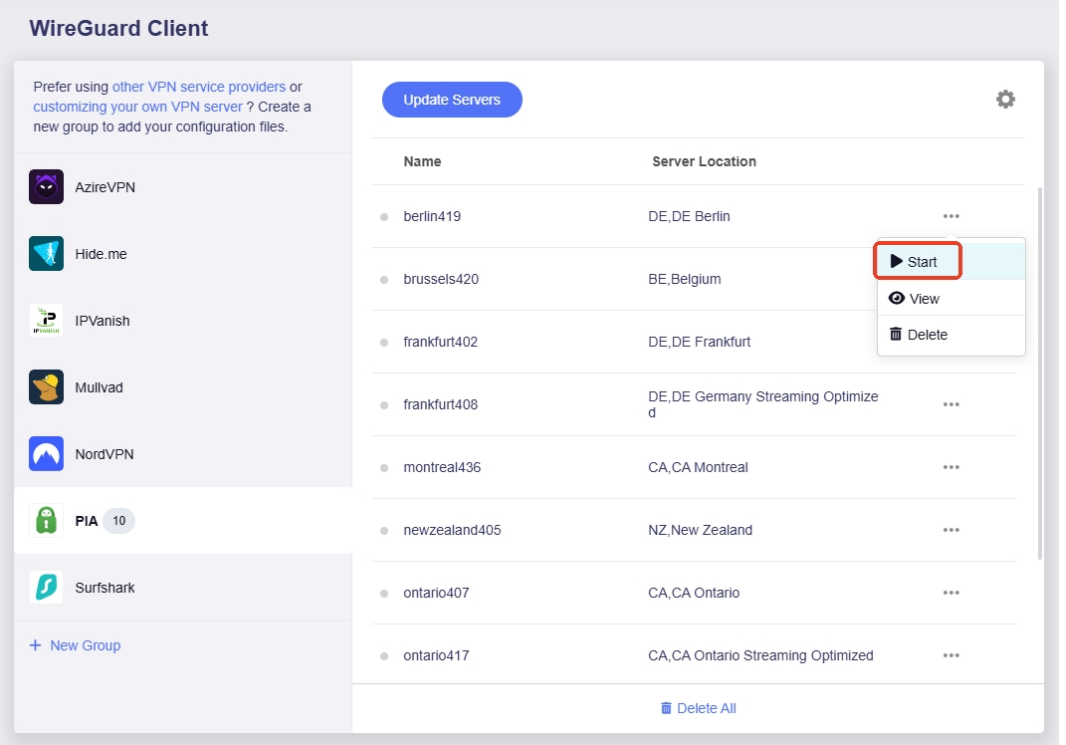
1. Iniciar sesión in a su enrutador's web admin panel y vaya a **VPN** > **WireGuard Client** > **PIA**.
2. Ingrese el nombre de usuario y la contraseña, luego haga clic en **Guardar y continuar**.



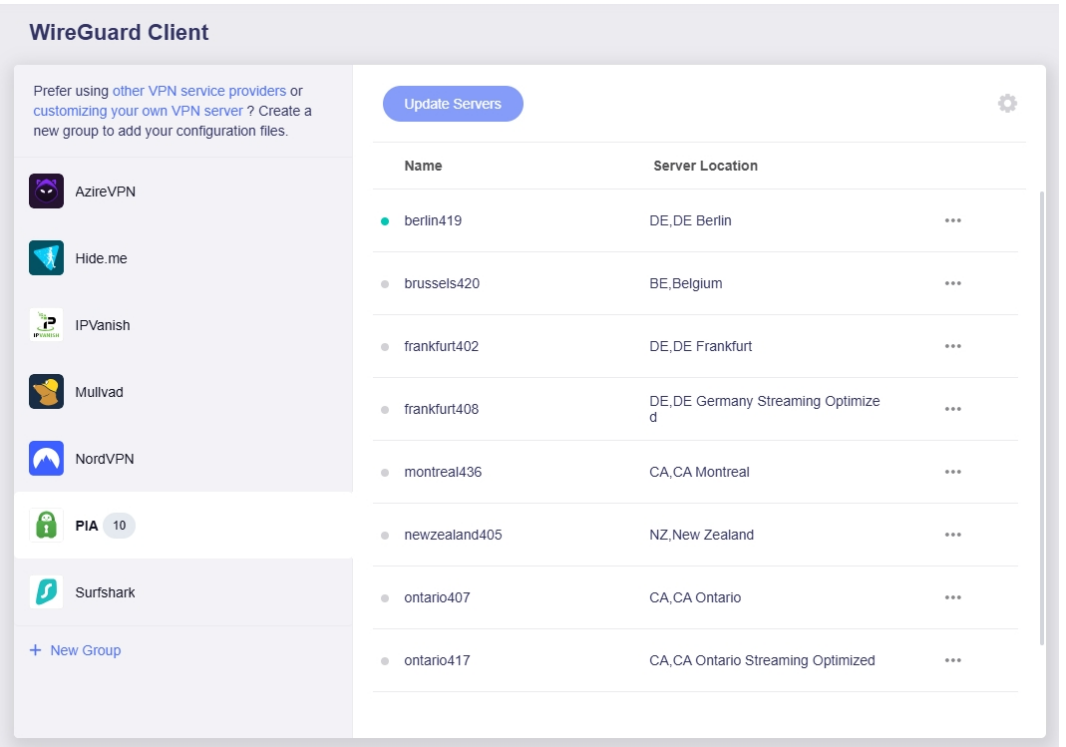
3. Seleccione los servidores a los que desea conectarse y haga clic en **Aplicar**.



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



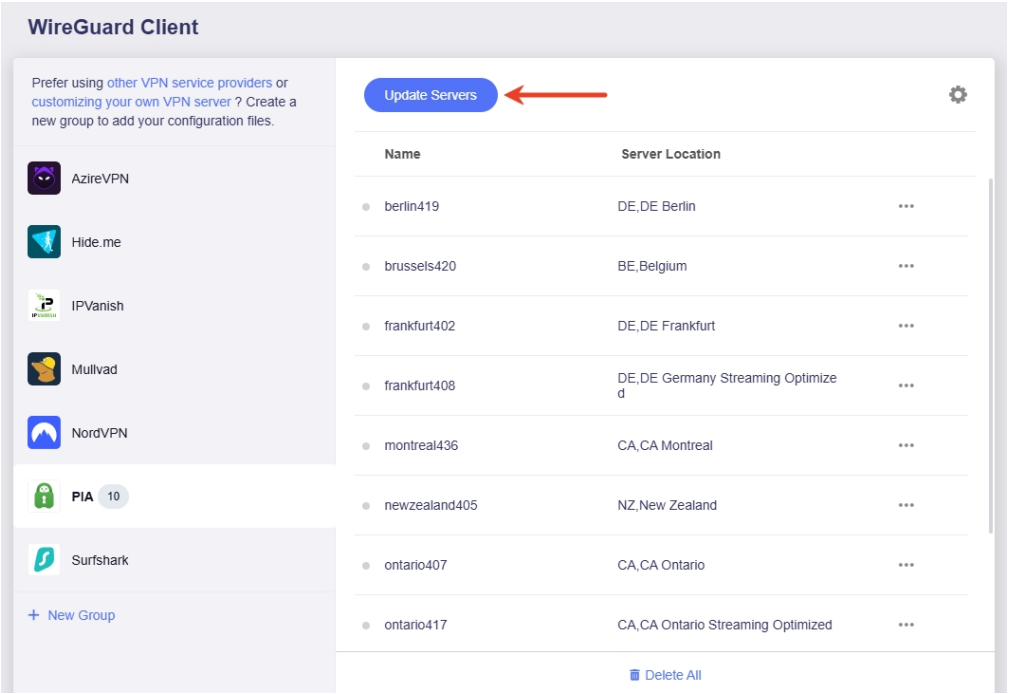
5. Una vez conectado, aparecerá un punto verde al lado del archivo de configuración.



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

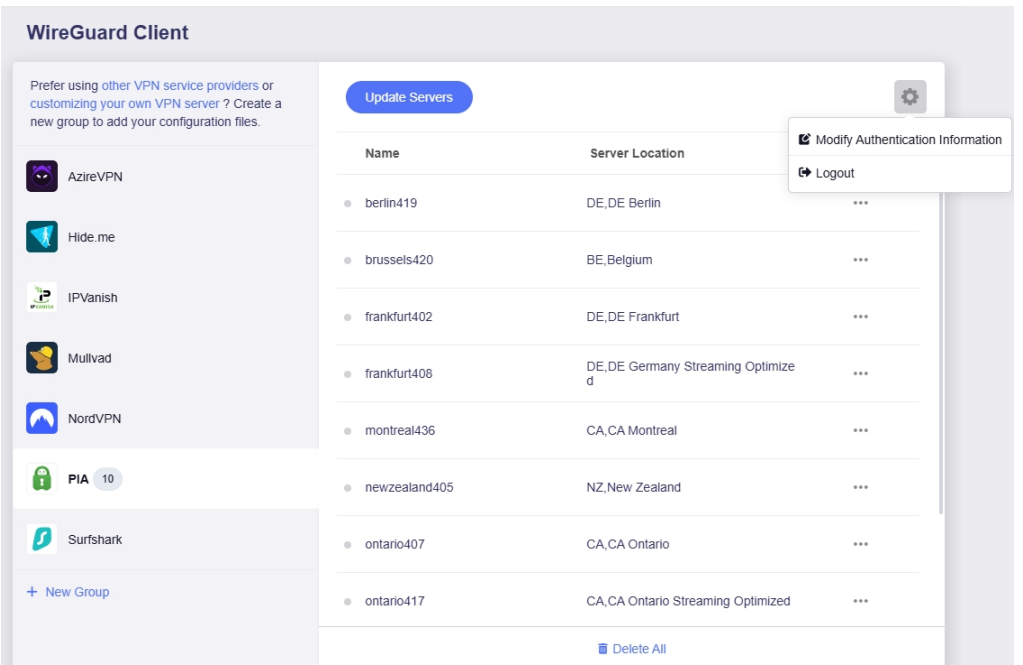
6. Actualizar servidores.

   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.



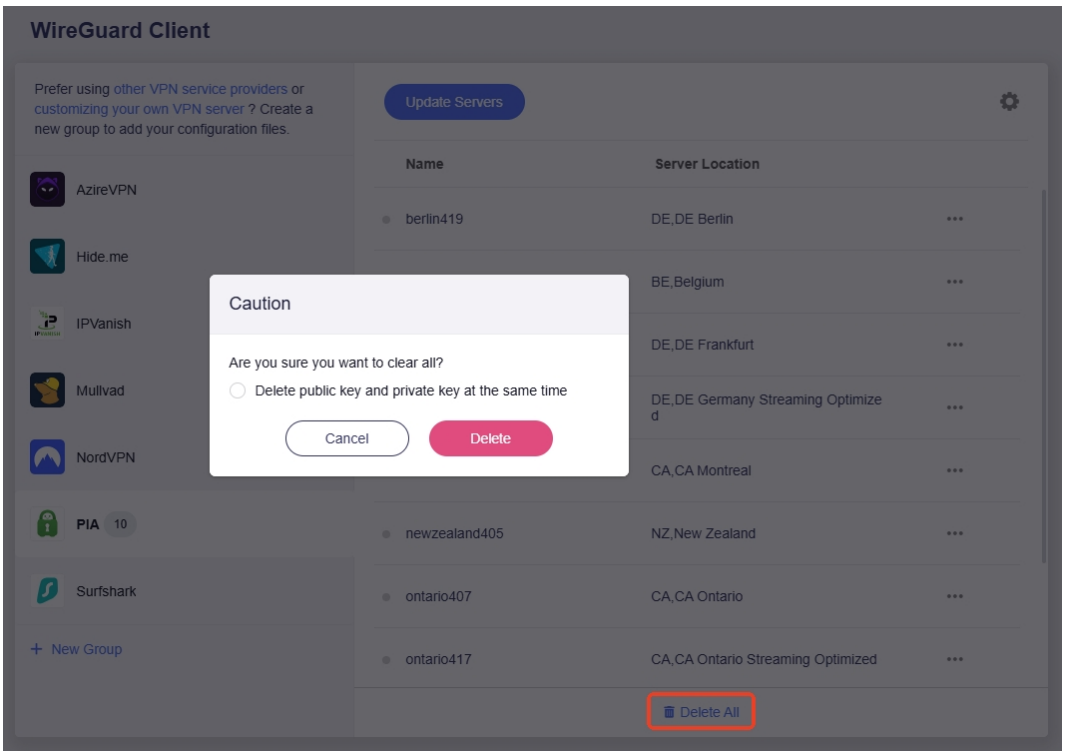
7. Edite las credenciales o cierre sesión.

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



8. Eliminar todos los archivos.

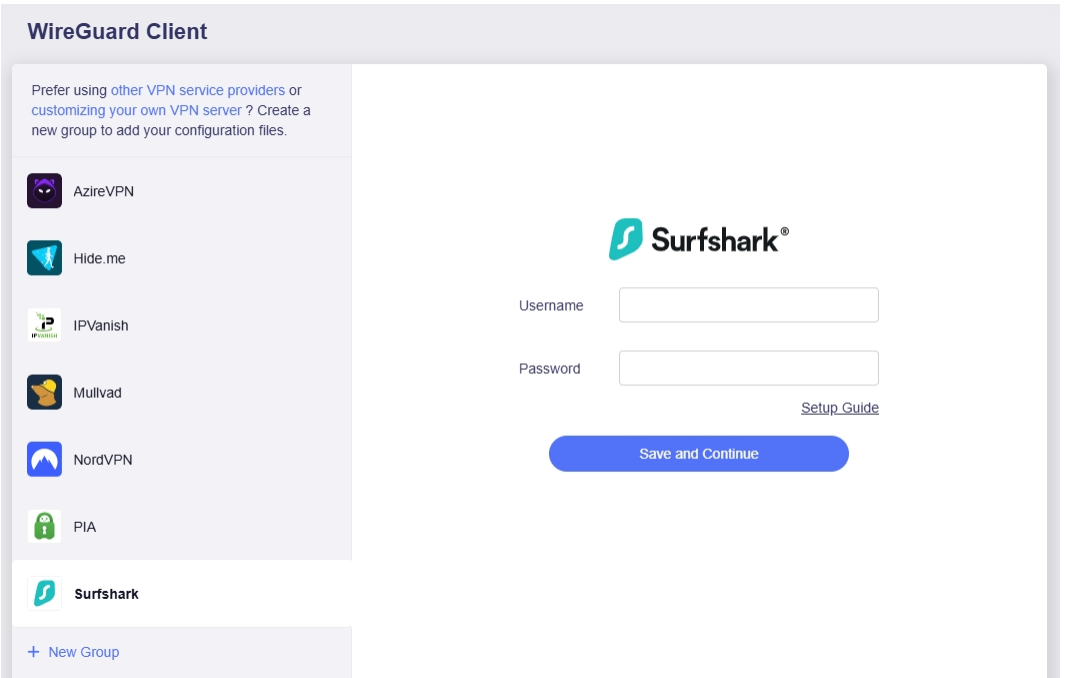
   Puede hacer clic en **Eliminar todo** para eliminar todos los archivos de configuración con un solo clic y elegir si desea eliminar los claves privadas y públicas simultáneamente.



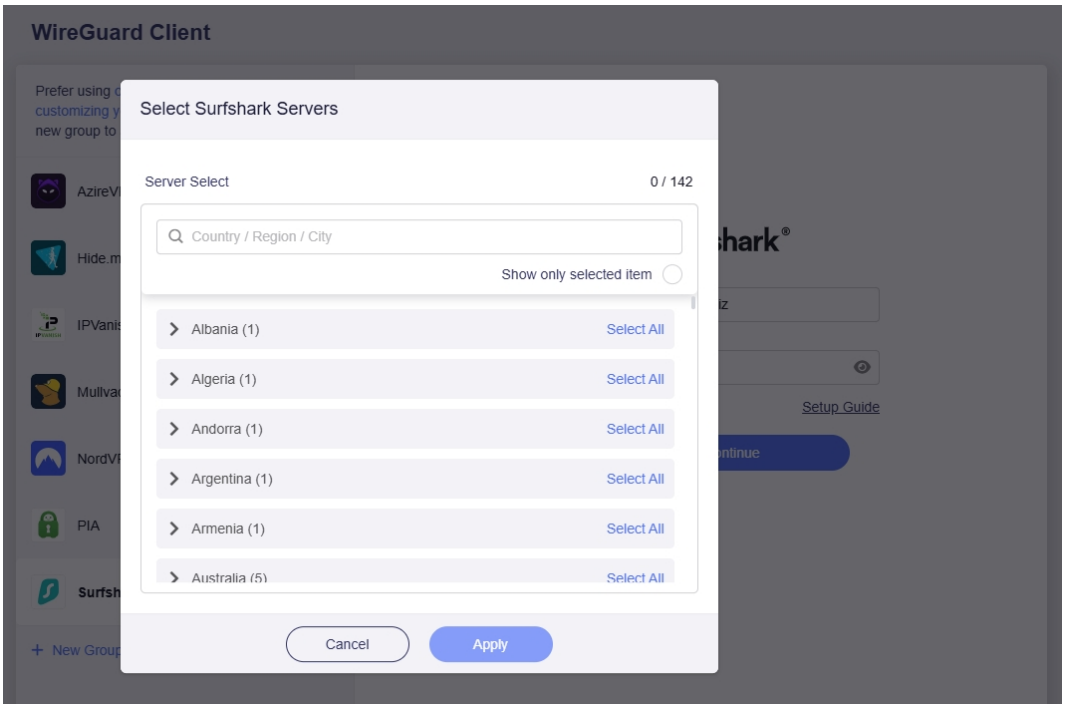
10.2.8 Configurar Surfshark

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

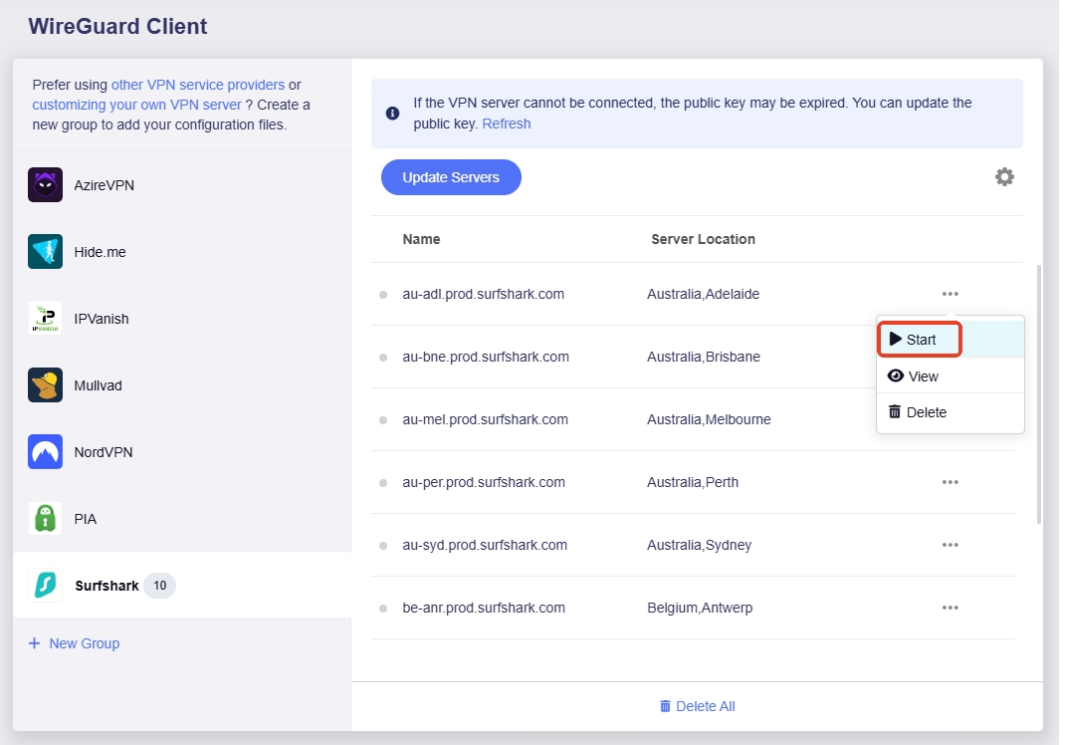
1. Iniciar sesiónn a su enrutador’s web admin panel y vaya a **VPN** > **WireGuard Client** > **Surfshark**.
2. Ingrese nombre de usuario y contraseña, luego haga clic en **Guardar y continuar**.



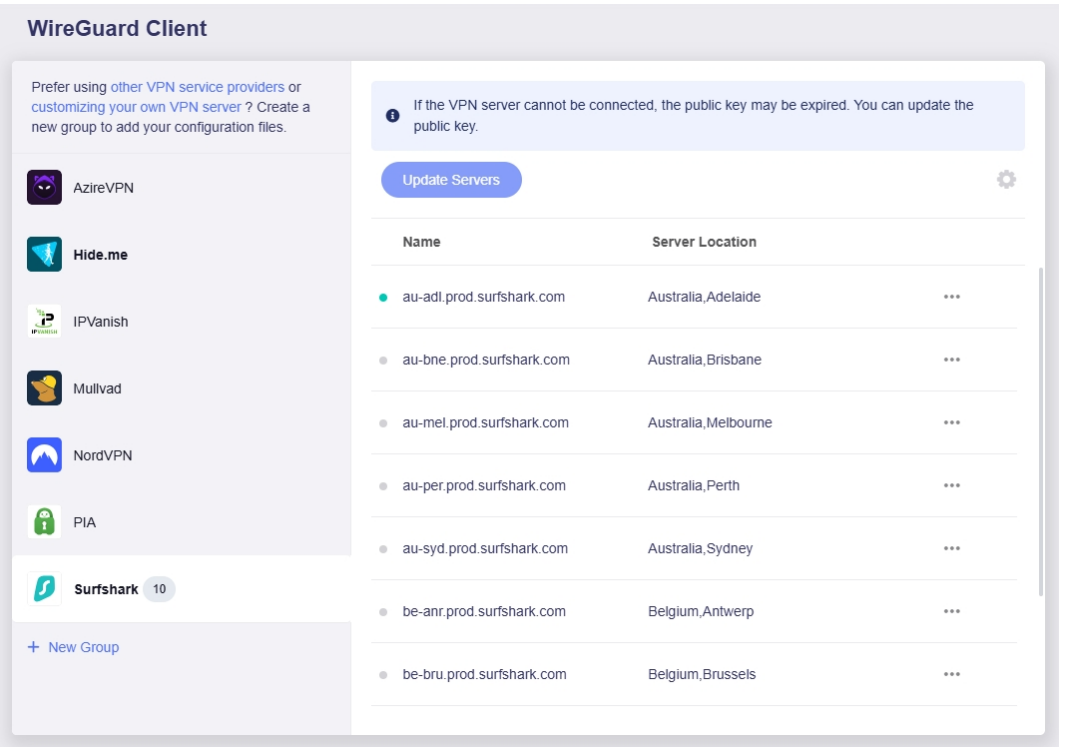
3. Seleccione los servidores a los que desea conectarse y haga clic en **Aplicar**.



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



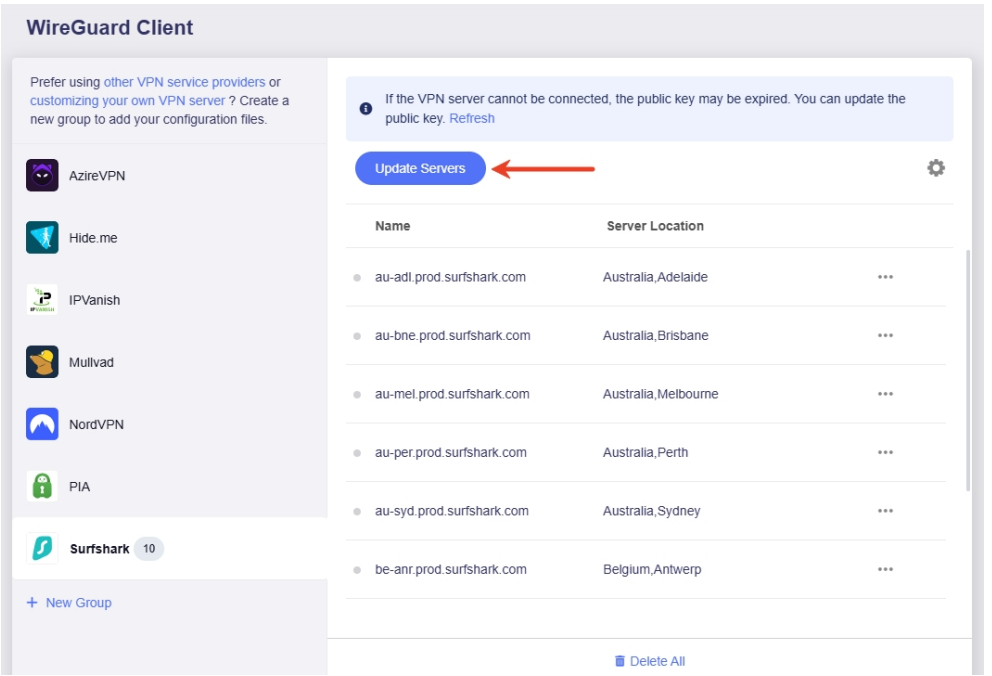
5. Una vez conectado, aparecerá un punto verde junto al archivo de configuración.



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

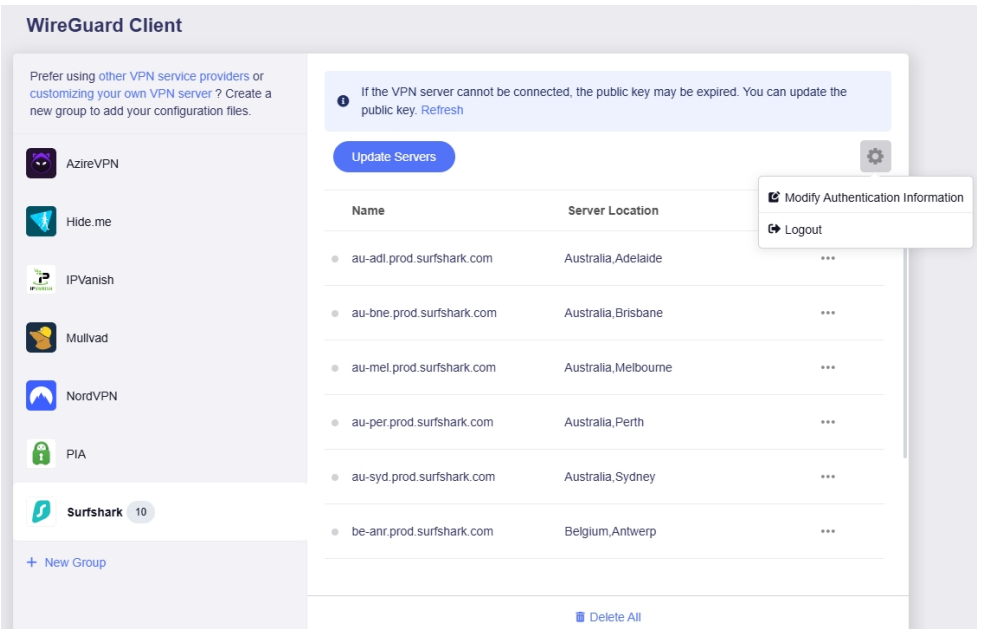
6. Actualizar servidores.

   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.



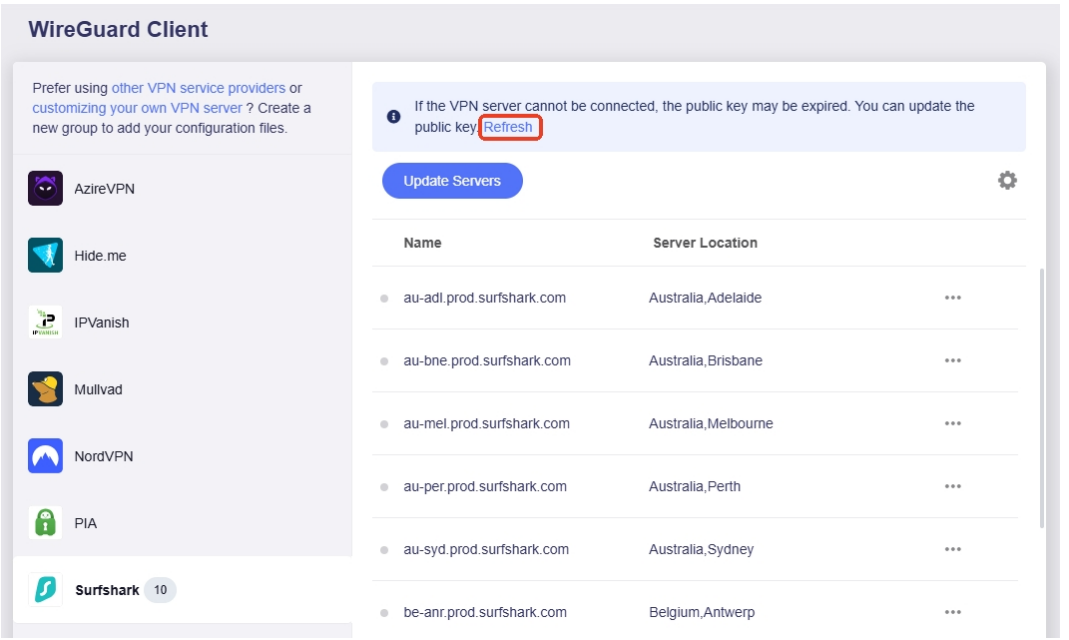
7. Editar credenciales o cerrar sesión.

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



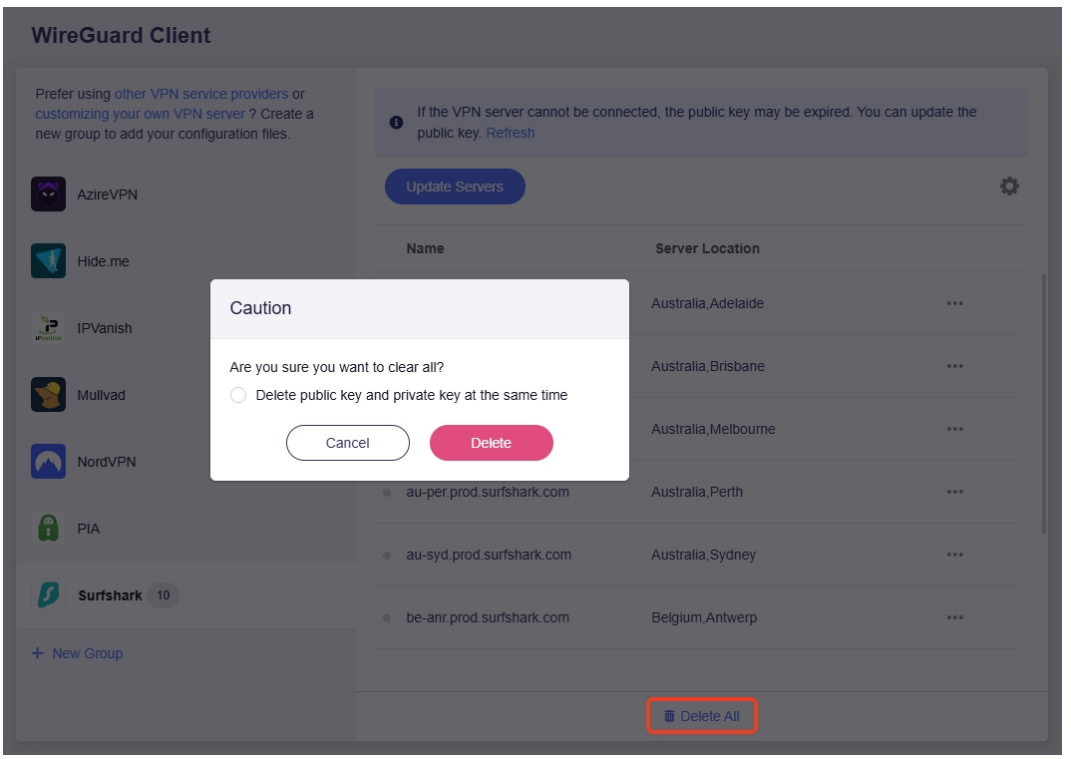
8. Actualizar.

   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.

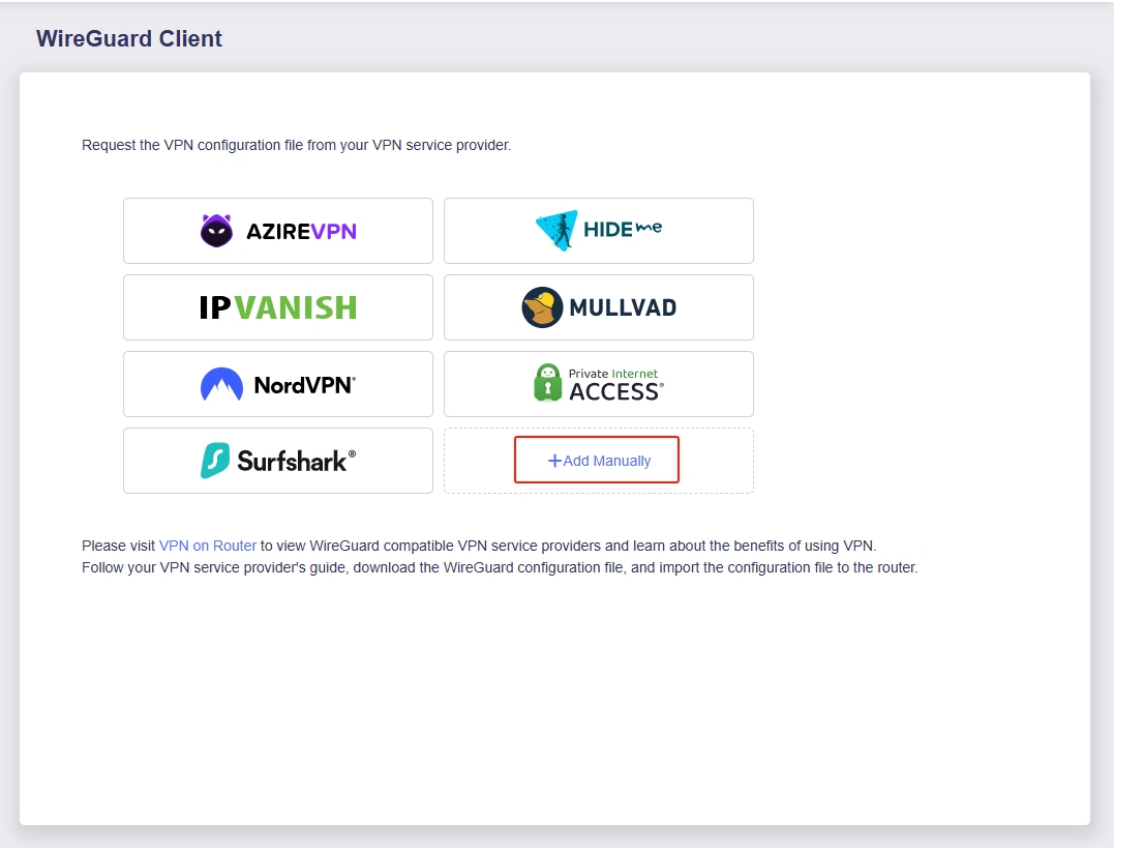


10.2.9 Configurar el cliente WireGuard manualmente (para otros proveedores)

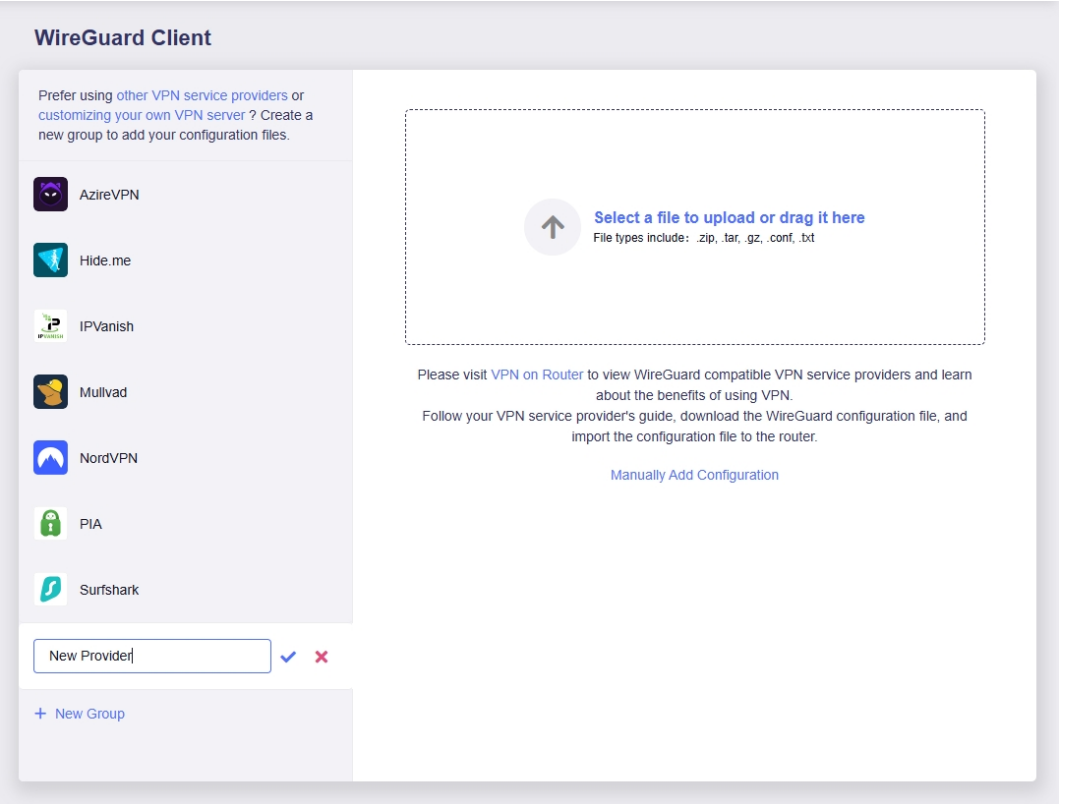
Si su proveedor de servicios WireGuard no está integrado en el panel de administración web, visite primero el sitio web oficial de su proveedor de servicios suscrito para obtener el archivo de configuración. Luego cárguelo en el enrutador para configurar un cliente WireGuard. Si no sabes cómo descargar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

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

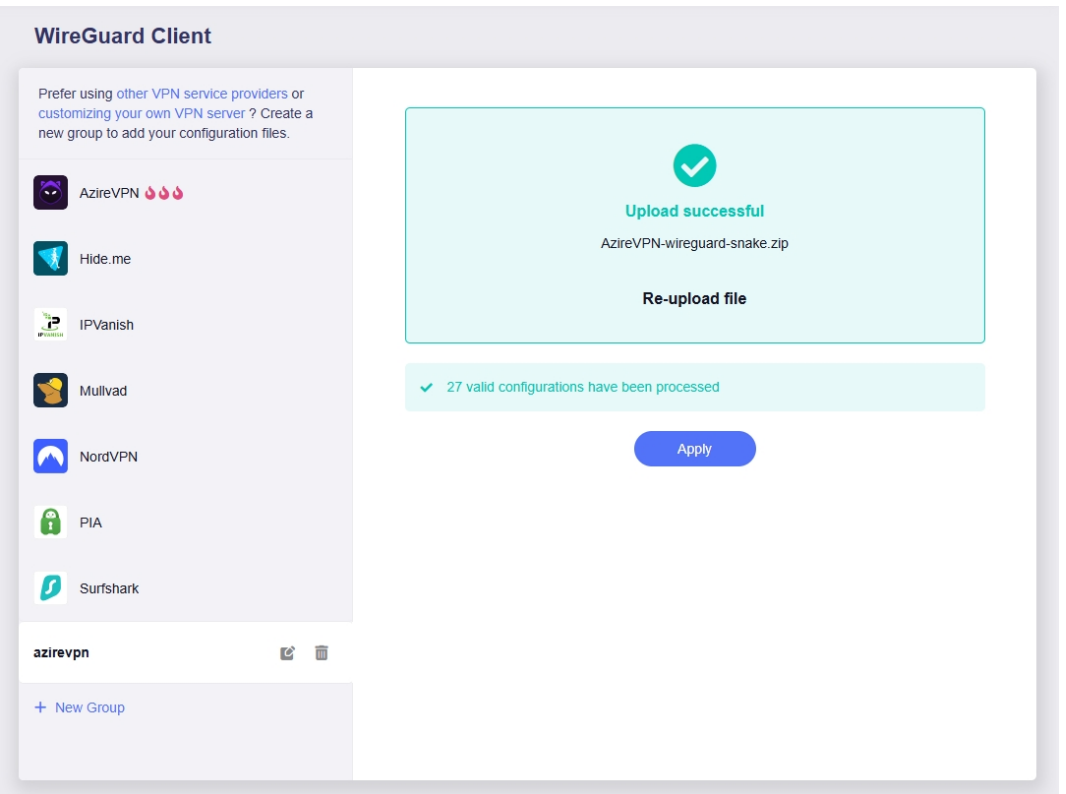
1. Inicie sesiónn en su enrutador's web admin panel y navegue hasta **VPN** > **Cliente WireGuard** > **Agregar manualmente**.



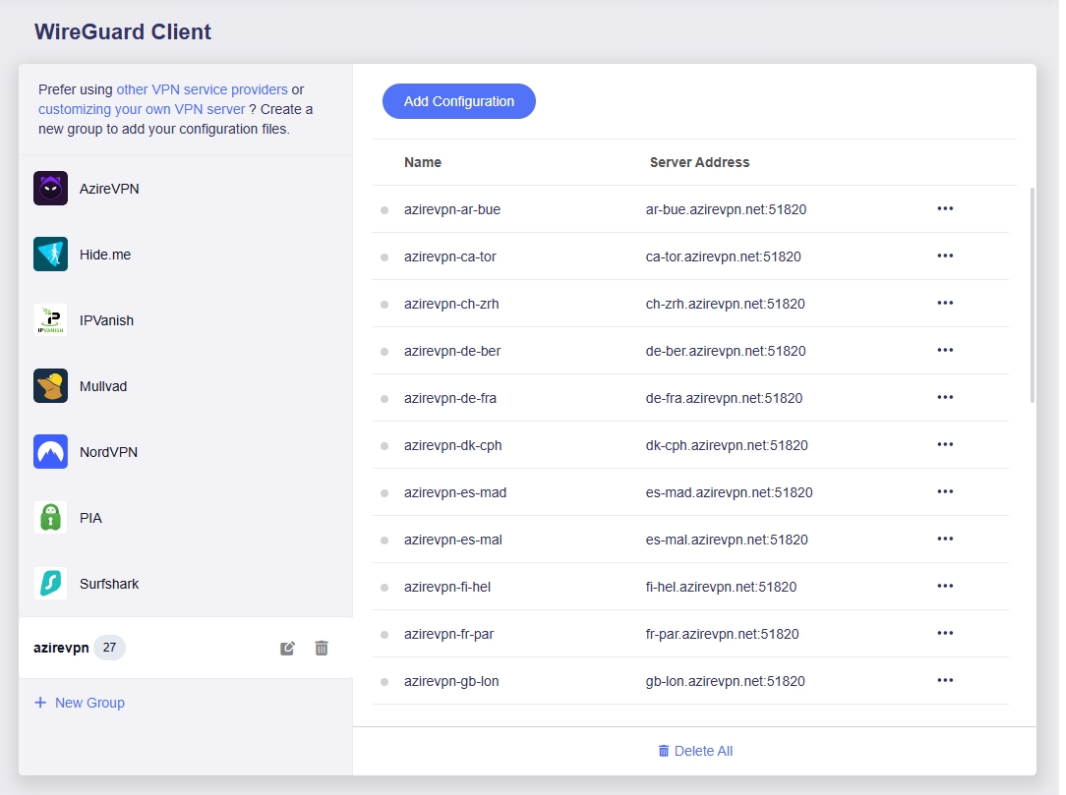
2. Se creará un grupo en la barra lateral izquierda. Establezca un nombre descriptivo para el grupo.



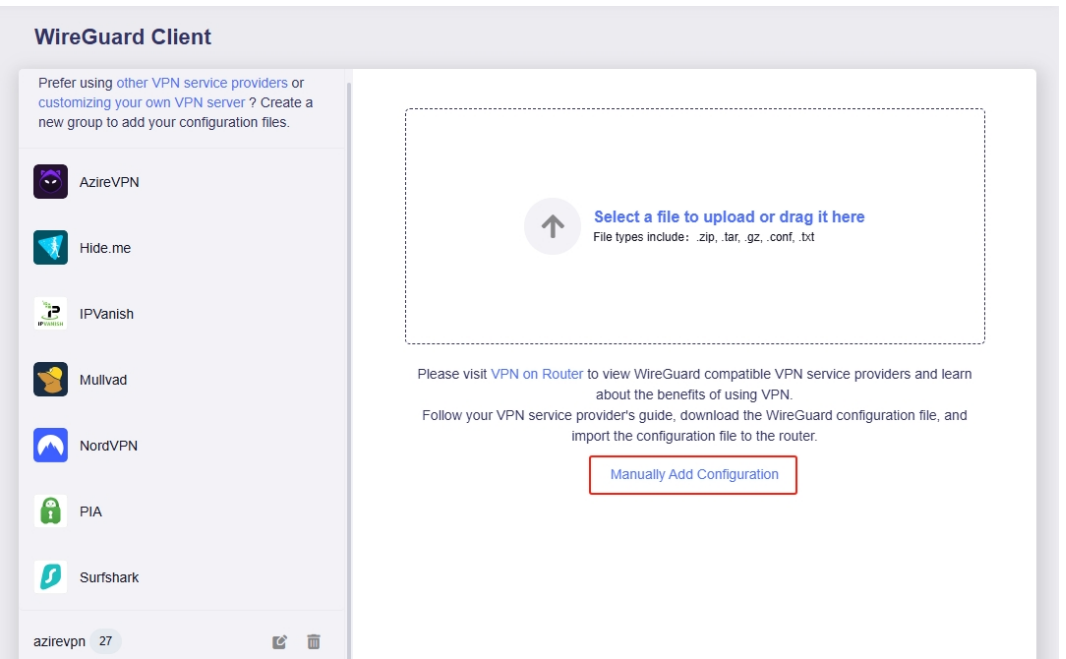
3. Click el área de carga para cargar su archivo de configuración WireGuard (formatos admitidos: zip, tar, gz, conf, txt), y haga clic en **Aplicar**.

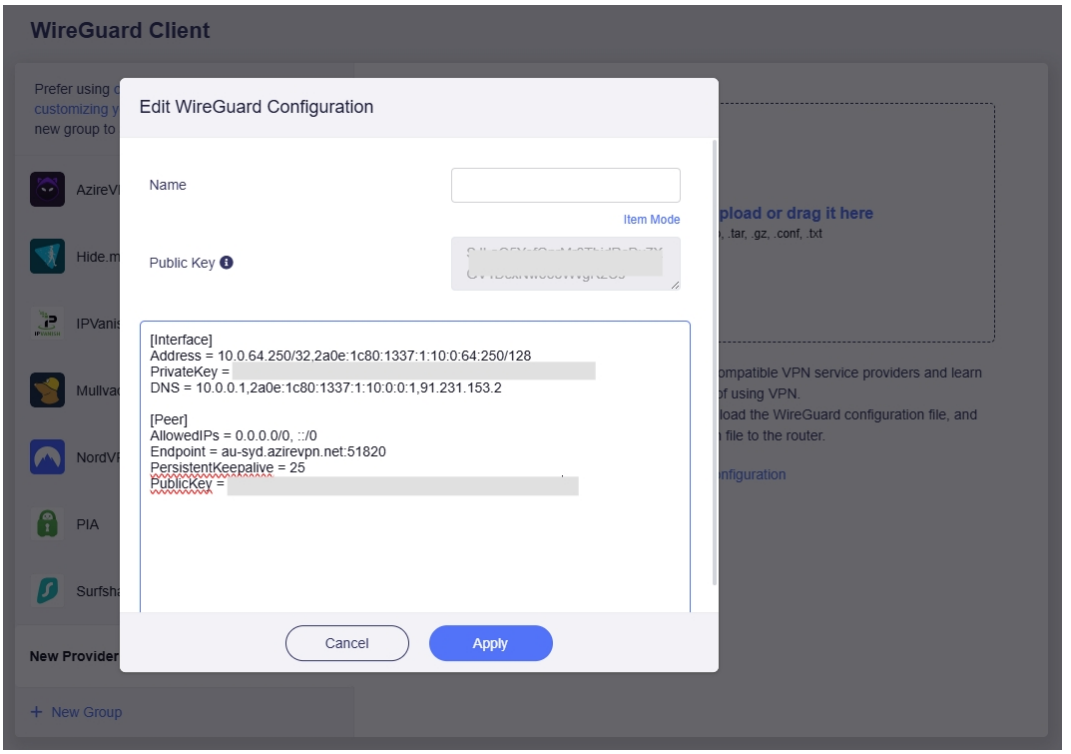


Si subes un archivo comprimido que contiene varios archivos de configuración, se descomprimirá automáticamente, como se muestra a continuación.

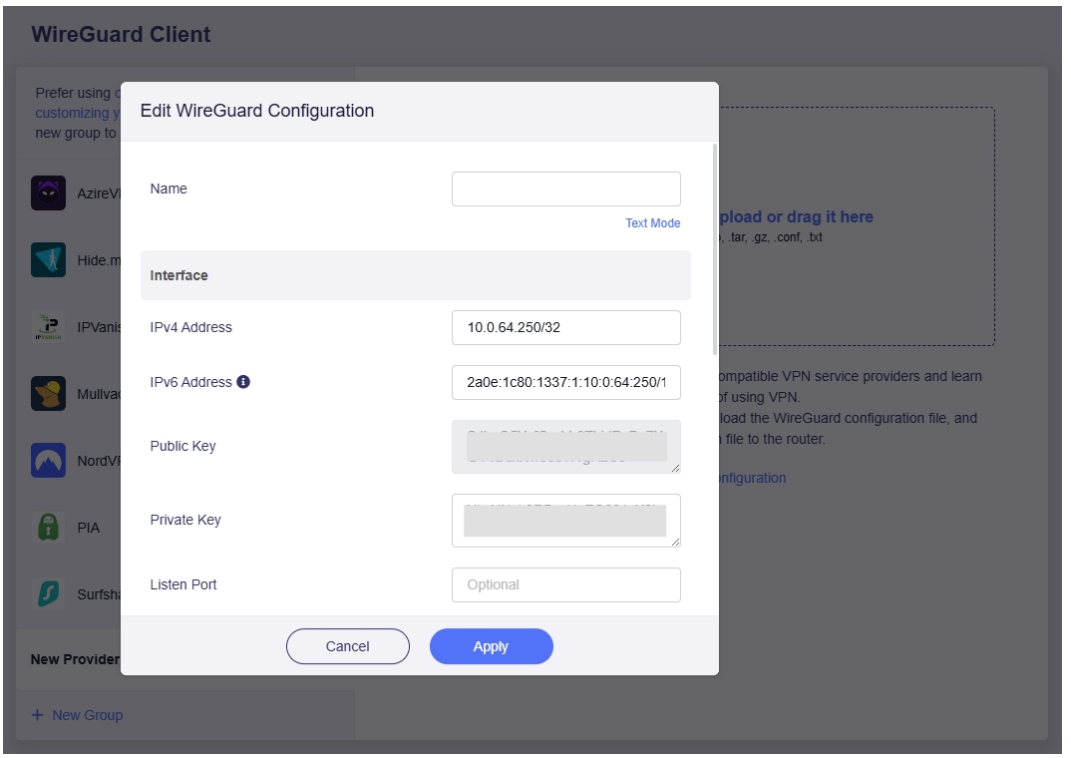


Como alternativa, puedes hacer clic en **Agregar configuración manualmente** en en la parte inferior del área de carga, agregue los detalles de configuración en forma de texto y haga clic en **Aplicar**.

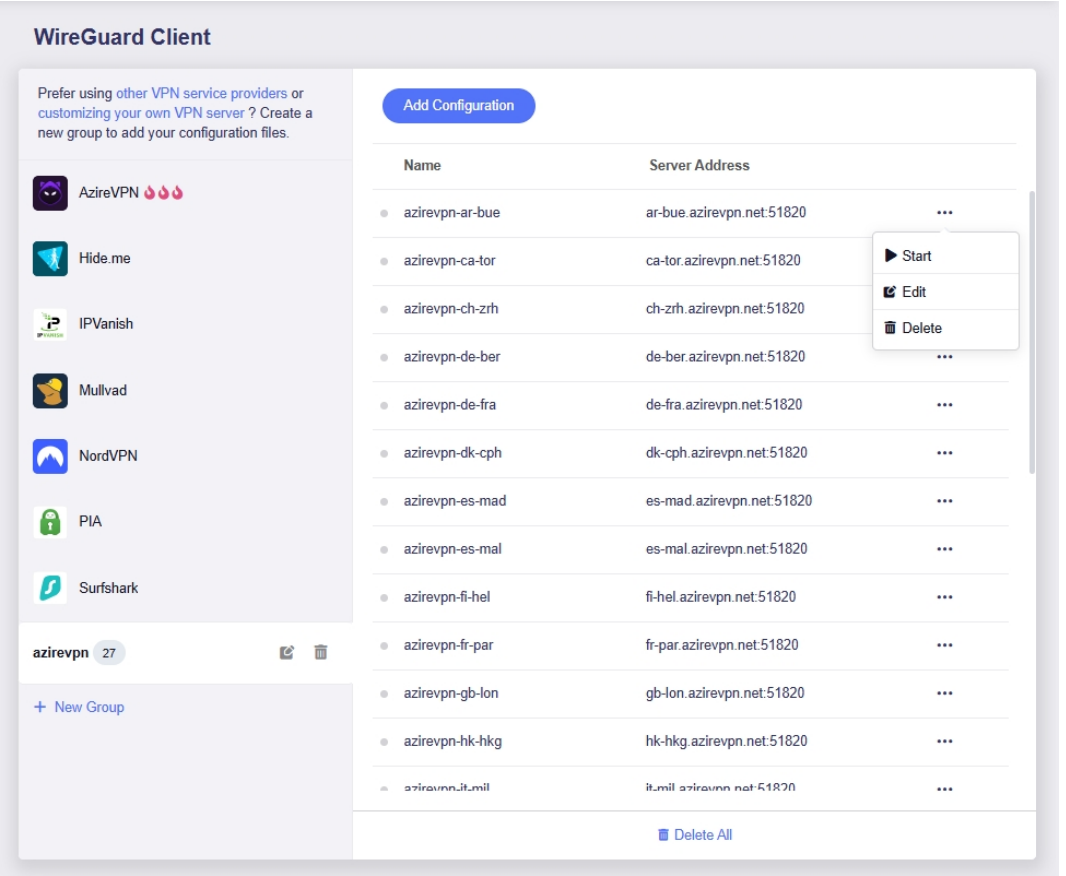




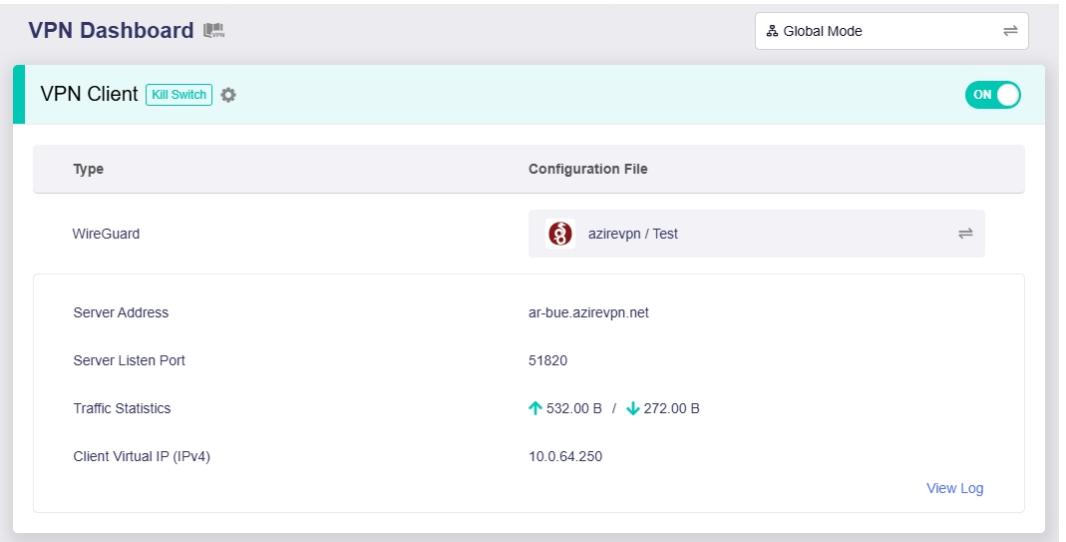
Si desea verificar cada elemento, puede cambiar al modo Elemento y verificar la configuraciónuración detalles, luegoluego haga clic en **Aplicar**.



4. Haga clic en el icono 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 los detalles de la conexión VPN en **Panel de VPN**.



Capítulo 11

Tor

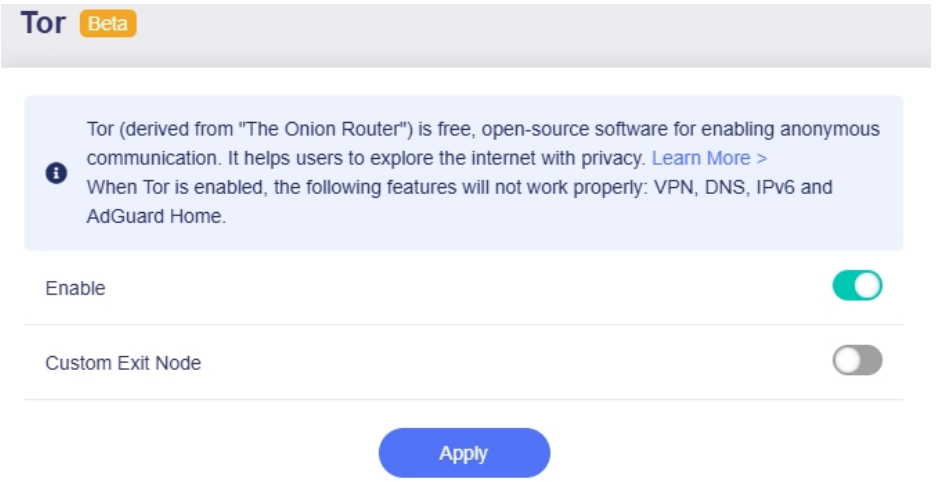
Este capítulo proporciona una breve introducción a Tor (The Onion Router), un software gratuito y de código abierto para permitir la comunicación anónima.

Tor (derivado) de **El enrutador cebolla**) es un software gratuito y de código abierto que permite la comunicación anónima. Ayuda a los usuarios a explorar Internet con privacidad. Tenga en cuenta que esta característicaestá actualmente en versión beta y puede tener algunos errores.

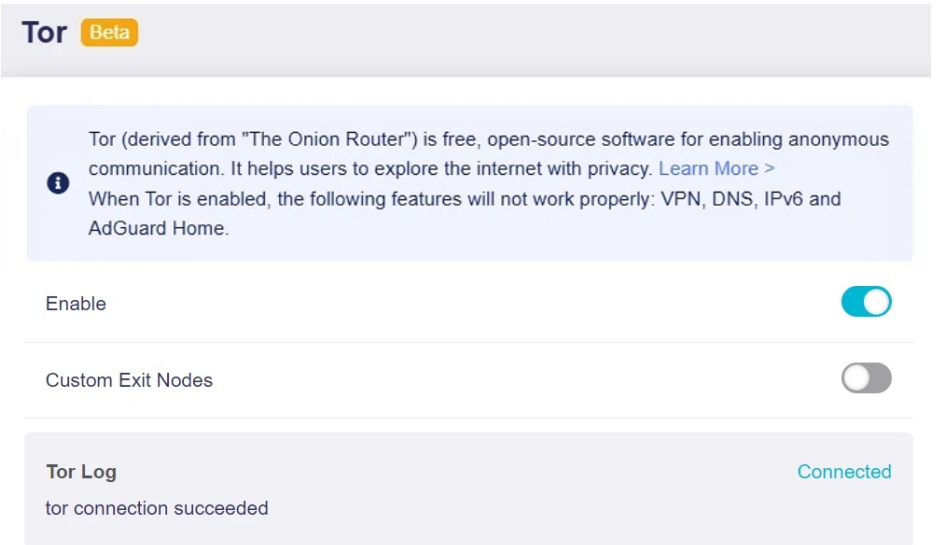
Cuando Tor está habilitado, laslas siguientes funciones no funcionarán correctamente: VPN, DNS, IPv6, y AdGuard Home.

Siga los pasos a continuación para configurar Tor según sea necesario.

1. Inicie sesión en su enrutador’s panel de administración web y navegue hasta **VPN** > **Tor**. Taleje el cambie para habilitarlo, habilite Nodos de salida personalizados según sea necesario y haga clic en **Aplicar**.



2. Comenzará a conectarse. Si su red cumples los requisitos, se mostrará conectado.



Capítulo 12

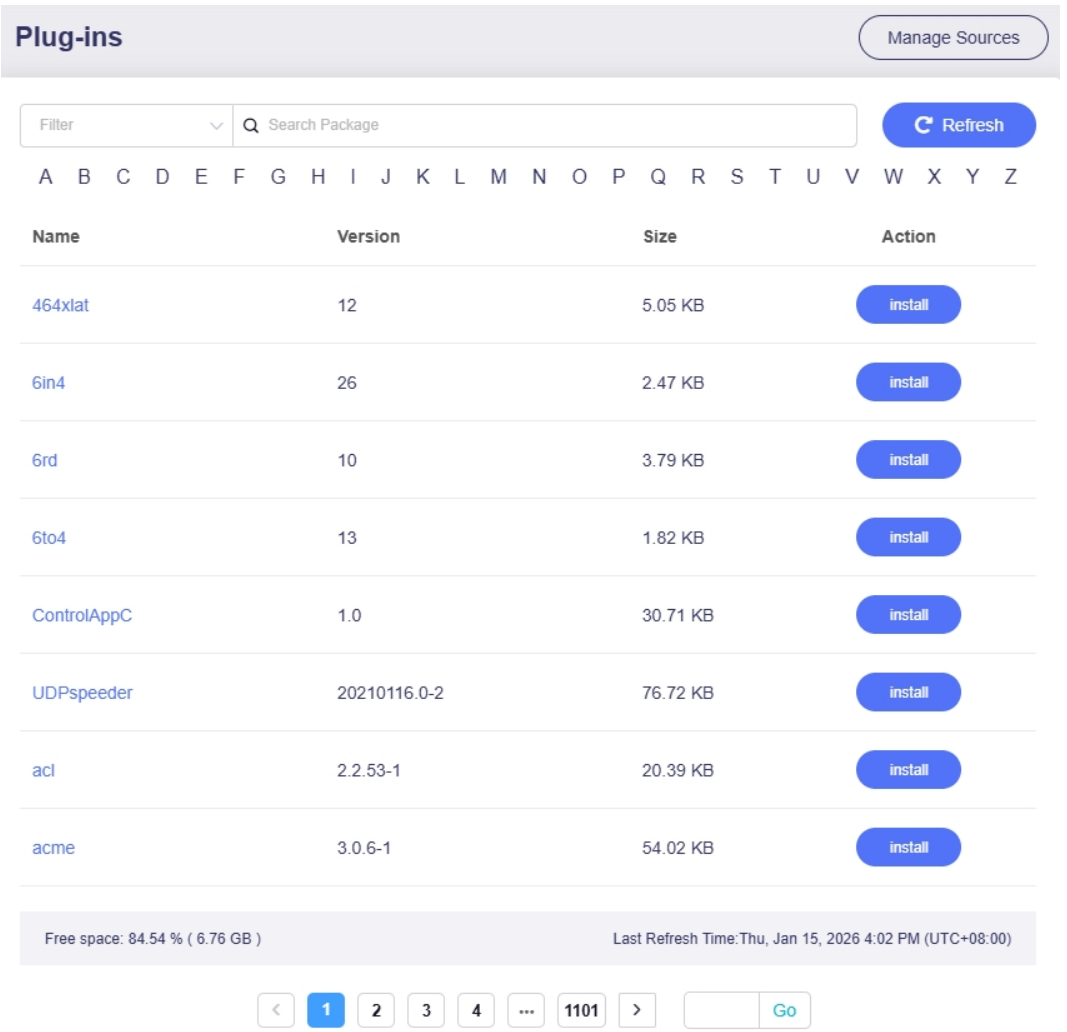
Aplicaciones

Este capítulo presenta algunas aplicaciones en enrutadores GL.iNet, por ejemplo, Complementos, DNS dinámico, Almacenamiento de red, AdGuard Home, Control parental, ZeroTier y Tailscale.

12.1 Complementos

La Página de complementos le permite administrar paquetes OpenWrt.

Inicie sesión en su enrutador’s web admin panel, navegue hasta **APLICACIONES** > **Complementos.** Puede instalar o eliminar cualquier paquetedisponible en el repositorio. Haga clic en **Actualizar** para actualizar la lista de paquetes antes de instalar complementos.



Nota:

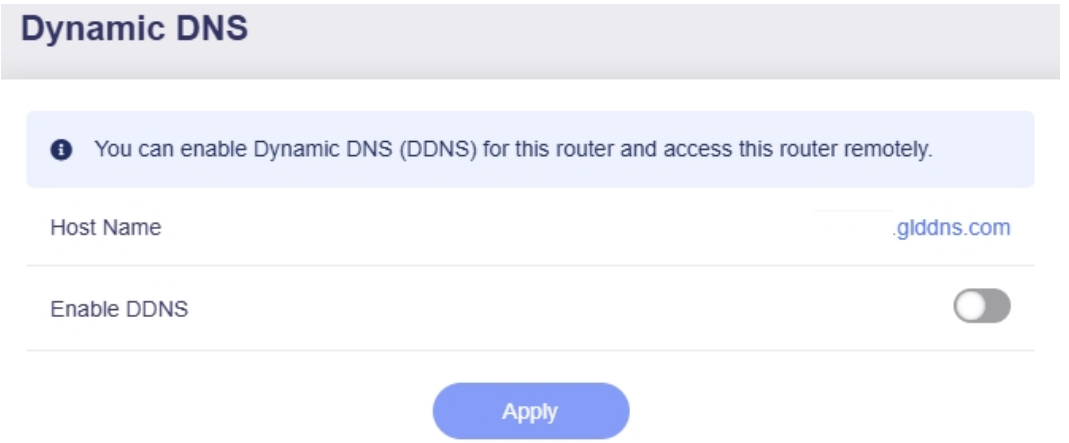
1. No se recomienda actualizar los complementos preinstalados en el firmware oficial de GL.iNet, como nginx, adguard home, tailscale, etc.
2. Los complementos de terceros instalados manualmente por los usuarios se pueden actualizar; sin embargo, GL.iNet no es responsable de ningún problema de seguridad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

12.2 DNS dinámico

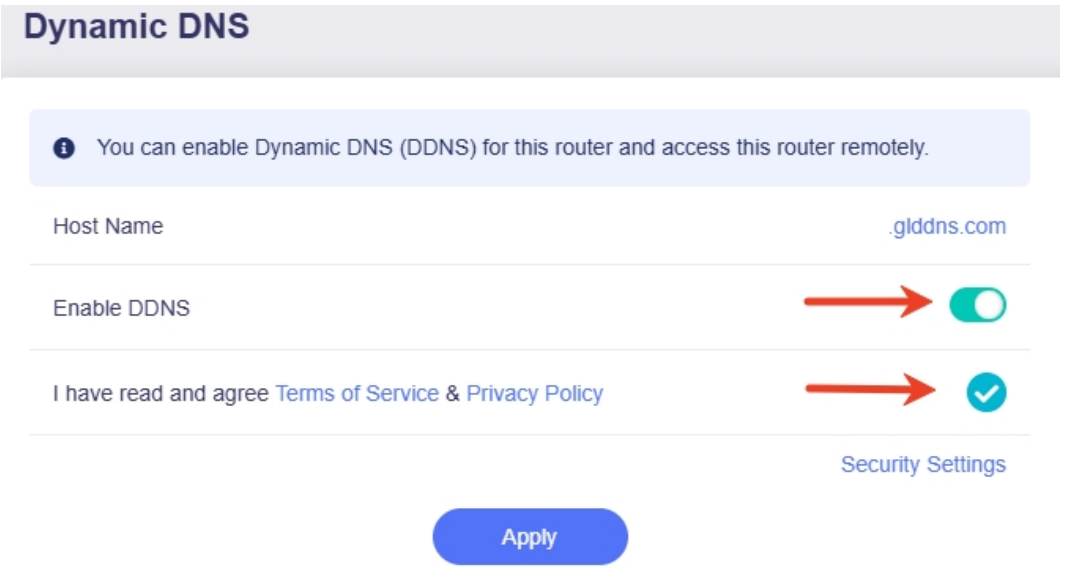
Dinámico El servicio de nombres de dominio (DDNS o DNS dinámico) es un servicio que se utiliza para asignar un nombre de dominio a la dirección IP dinámica de un dispositivo de red. Con DNS dinámico, puede acceder a su enrutador de forma remota. Se requiere una dirección IP pública para esta funcionalidad.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

12.2.1 Habilitar DDNS

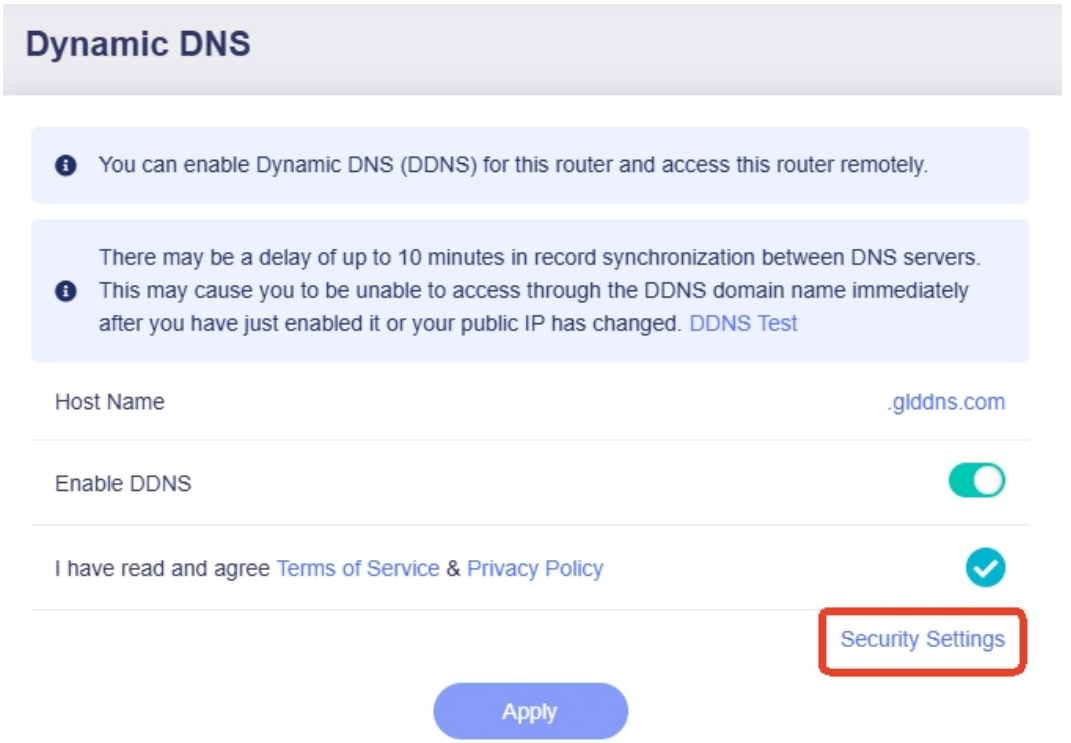
1. Inicie sesión en su enrutador's web admin panel, navegue hasta **APLICACIONES** > **DNS dinámico**, la página se muestra como a continuación.



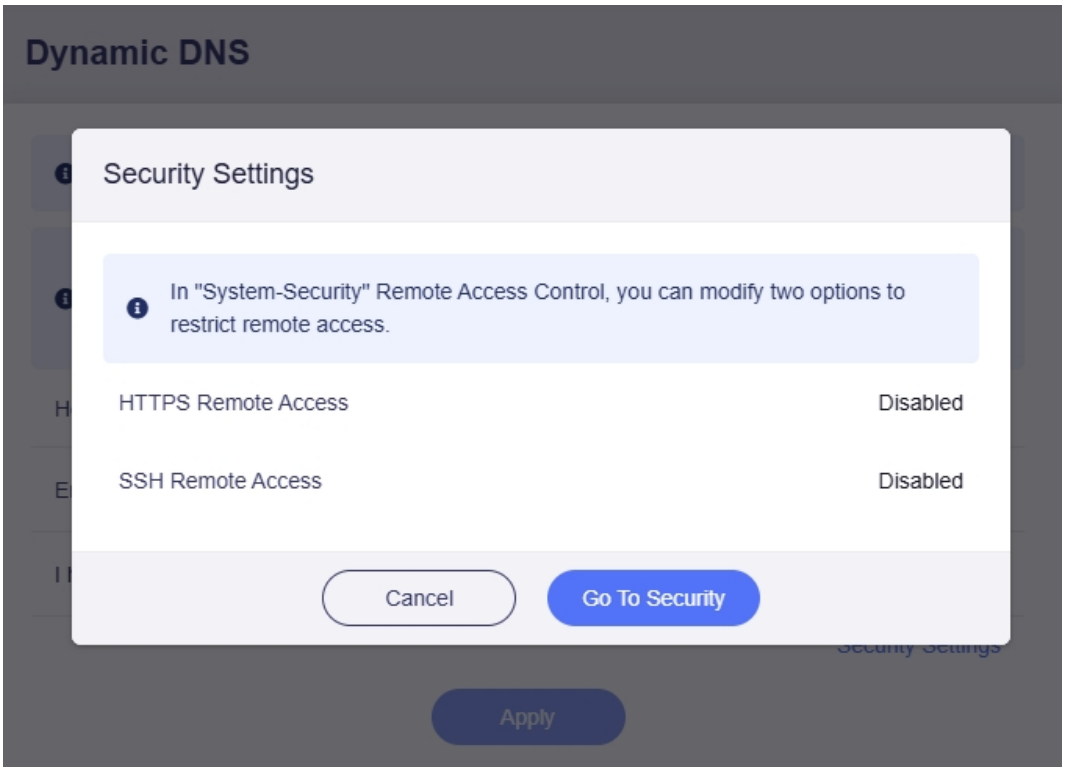
2. Active **Habilitar DDNS**, leer y aceptar los **Términos de servicios y política de privacidad**, luego haga clic en **Aplicar**.



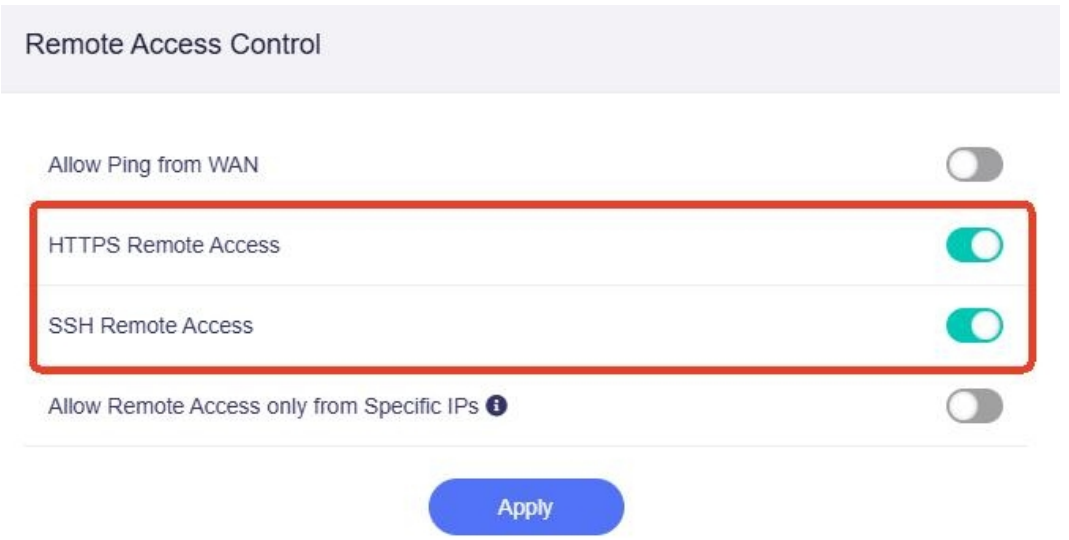
3. Haga clic **Configuración de seguridad** en la esquina inferior derecha.



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



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



Nota:

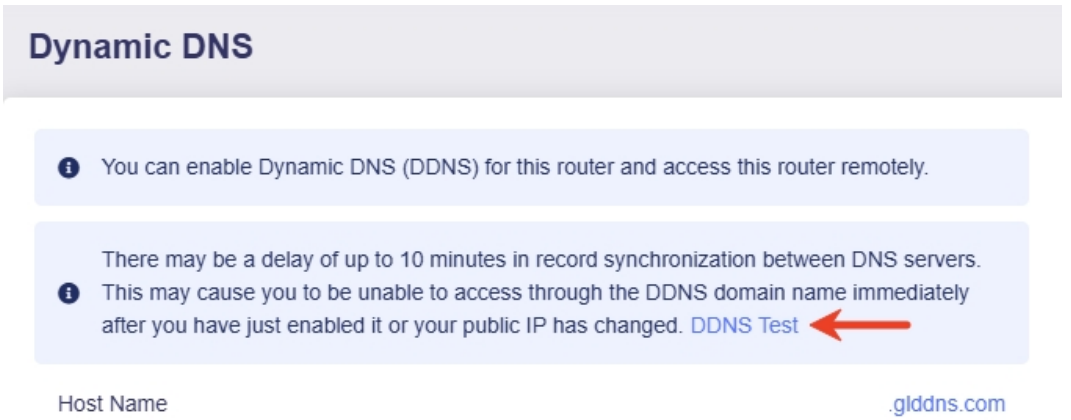
1. Puede haber un retraso de hasta 10 minutos en la sincronización de registros entre servidores DNS. Esto puede impedirle acceder a través del nombre de dominio DDNS inmediatamente después de habilitarlo o cuando cambie su IP pública.
2. Si habilita DDNS y el Cliente VPN al mismo tiempo, enseguro que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

12.2.2 Comprobar si DDNS funciona

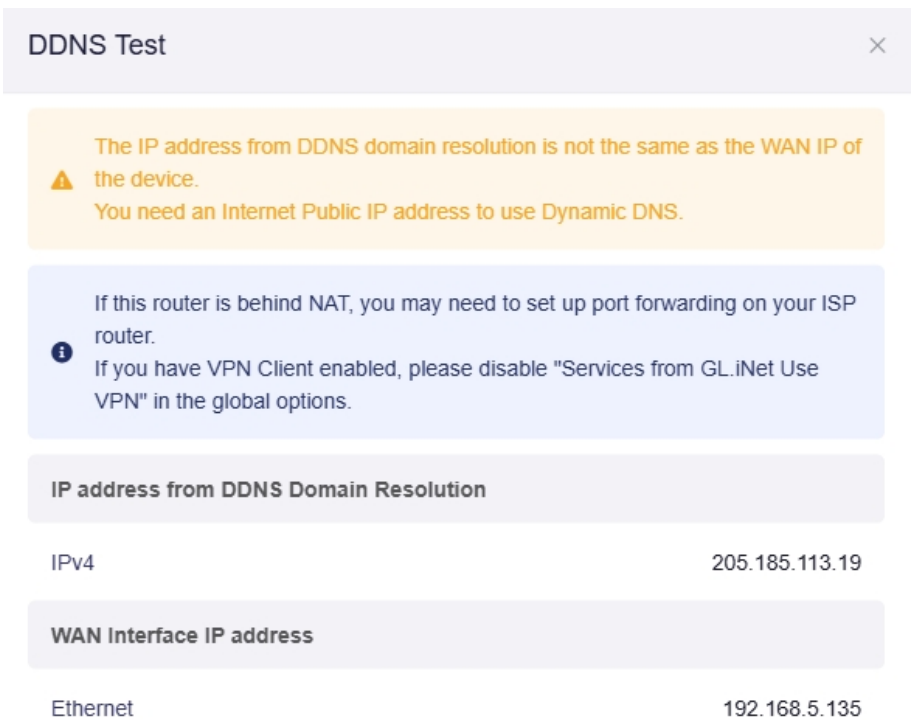
Puede comprobar si DDNS funciona utilizando la herramienta de prueba de DDNS o manualmente mediante comandos.

Método 1. Use Herramienta de prueba DDNS

1. En la página DNS dinámico, haga clic en **Pruebas DDNSt**.



2. Asegúrese de que la dirección IP de la resolución del dominio DDNS coincida con la IP WAN del enrutador. Si no, aparecerá un mensaje amarillo en la parte superior, indicando que el enrutador podría estar detrás de NAT y que necesita 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.



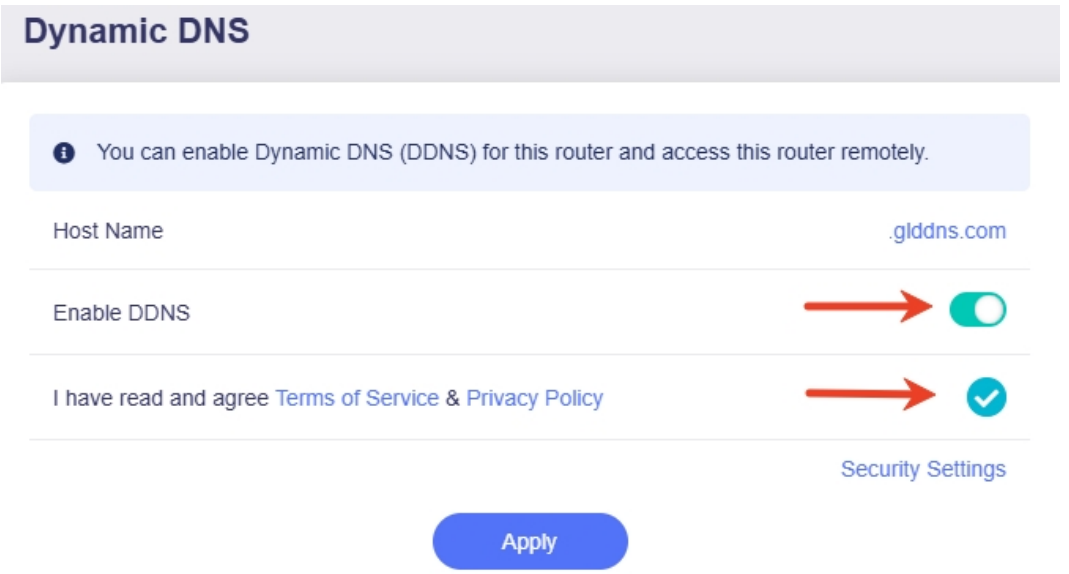
   - Reemplace “xxxxxxx.glddns.com” en la imagen de arriba con su Nombre del host.
   - El “8.8.8.8” es el DNS de Google. Úselo o reemplácelo con otros, luego presione Entrar.
2. Si obtiene una dirección IP pública como “183.178.10.100” en la imagen de arriba, indica que su DDNS El dominio se ha asignado correctamente a una dirección IP pública. Si recibe un mensaje como “el servidor puede’no encuentra xxxxxxx.glddns.com”, puede indicar que la resolución del dominio falló y que su dominio DDNS no se ha asignado correctamente a un sitio público. Dirección IP. Continúe con el siguiente paso para verificar.
3. Inicie sesión en la web ’de su enrutador admin panel y navegue hasta **INTERNET**. Busque la dirección IP WAN de su 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

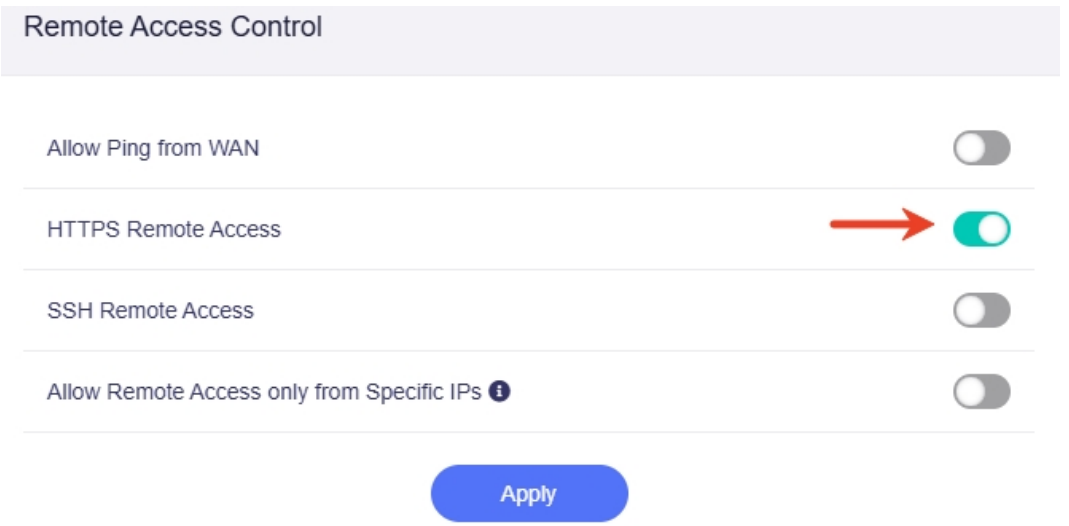
Se requiere una **Dirección IP pública** para el acceso remoto HTTPS.Consulte aquí parapara verificar si su ISP le asigna una dirección IP pública. Si su enrutador está detrás de NAT, configure el reenvío de puertos (**puerto 443**) en el enrutador ascendente para HTTPS acceso.

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

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

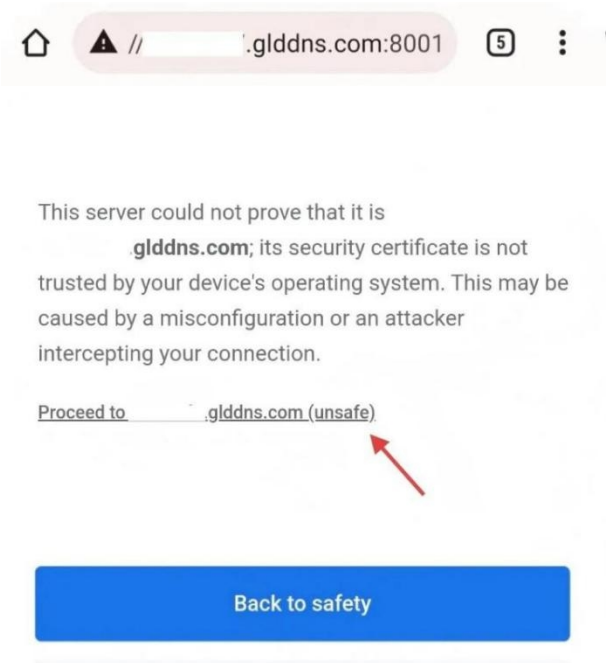


2. En el panel de administración web, vaya a **SISTEMA** > **Seguridad** > **Control de acceso remoto**. Habilitar **Acceso remoto HTTPS** y haga clic en **Aplicar**.



Una vez habilitado, puede acceder al panel de administración del enrutador’desde cualquier lugar usando 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.



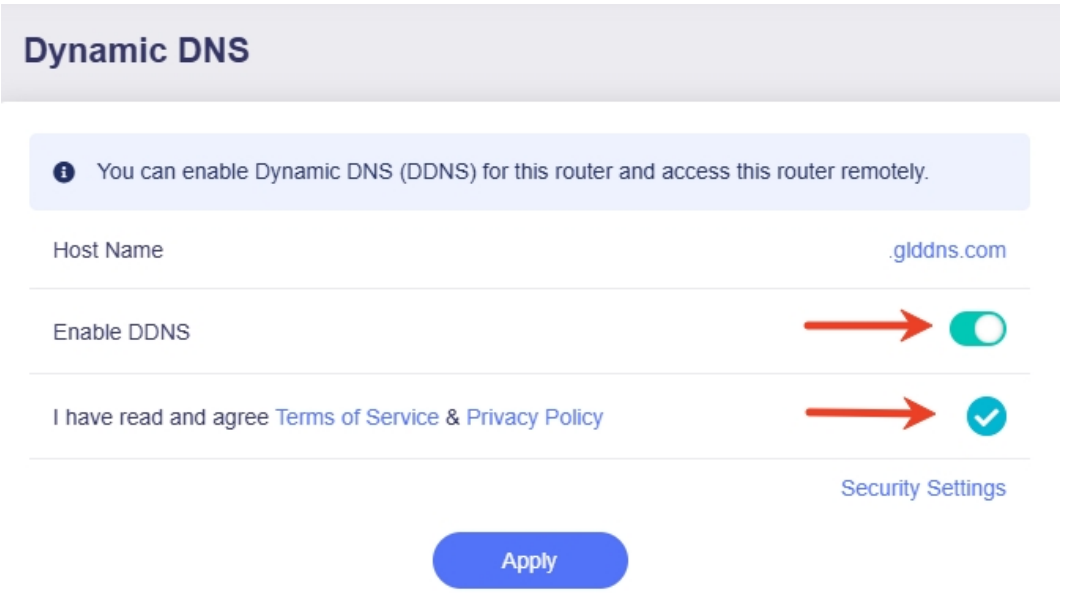
Luego podrá acceder al enrutador’s panel de administración web usando el DDNS host nombre sobre **HTTPS**.

12.2.4 Acceso remoto SSH

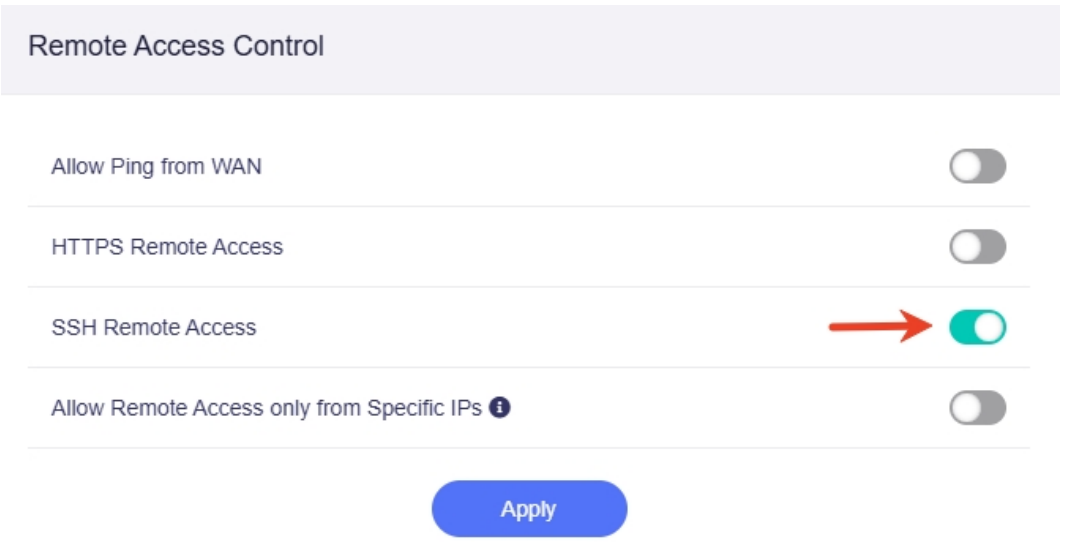
A **Dirección IP pública** es necesario para SSH acceso remoto.Consulte aquí tpara verificar si su ISP le asigna una dirección IP pública. Si su enrutador está detrás de NAT, configure el reenvío de puertos (**puerto 22**) en el enrutador ascendente para SSH remoto acceso.

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

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



2. En el panel de administración web, vaya a **SISTEMA** > **Seguridad** > **Control de acceso remoto**. Habilite **Acceso remoto SSH** 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 SSH, por ejemplo, **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

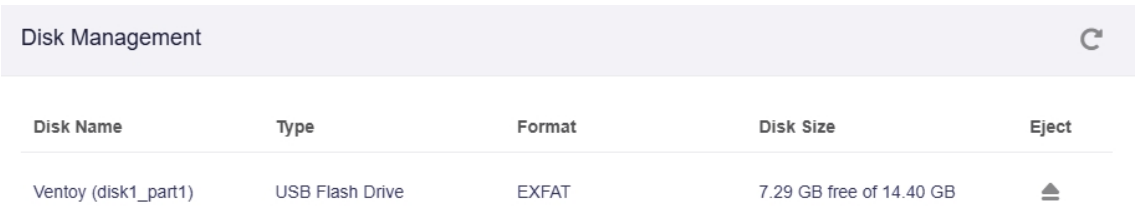
El almacenamiento en red permite compartir archivos entre dispositivos conectando una unidad USB o una tarjeta SD a su enrutador. El enrutador convierte el dispositivo de almacenamiento en una unidad de red compartida, accesible para todos dispositivos conectados.

Brume 2 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 podría causar un mal funcionamiento.

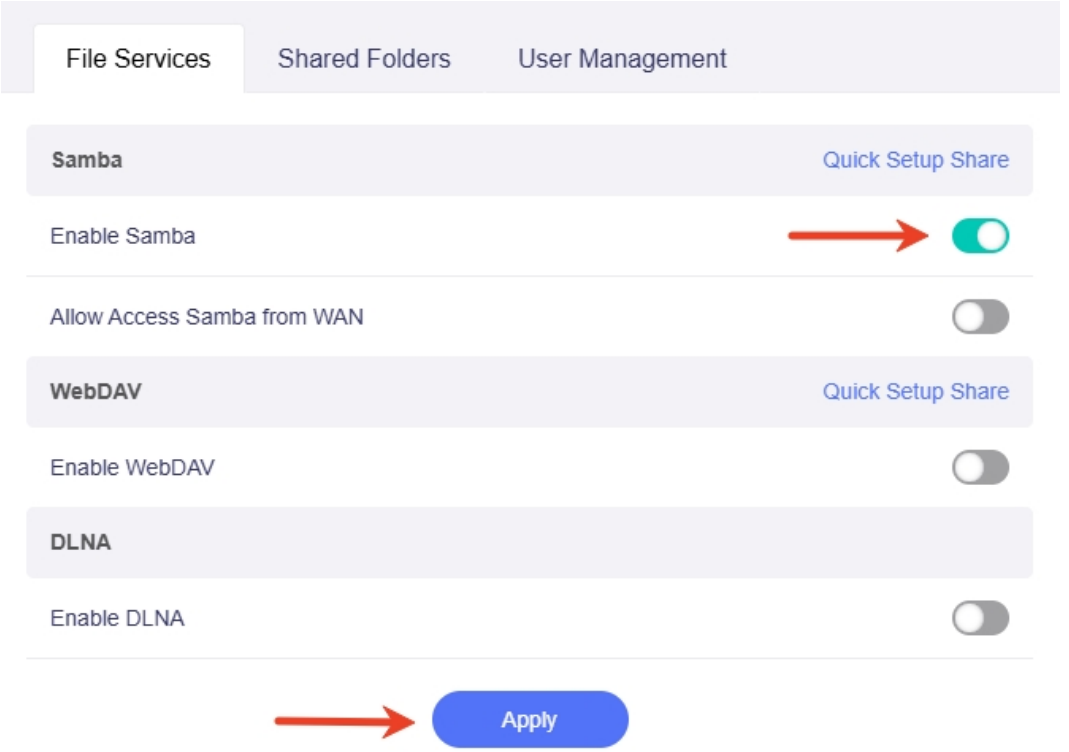
12.3.1 Conectar una unidad de almacenamiento

1. Conecte su dispositivo de almacenamiento al enrutador.
   - Para una unidad USB: conéctela 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.



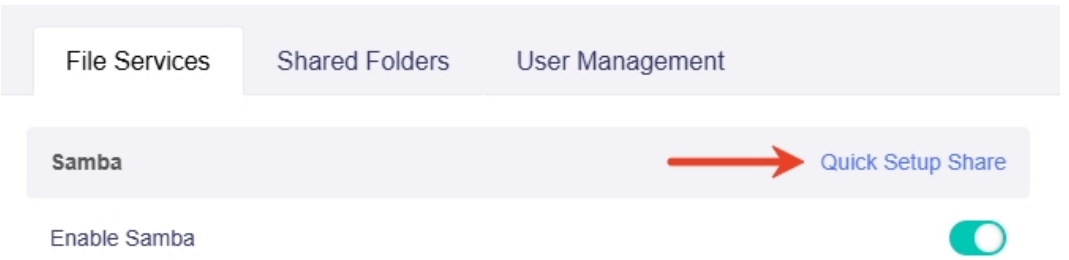
12.3.2 Configurar Samba

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

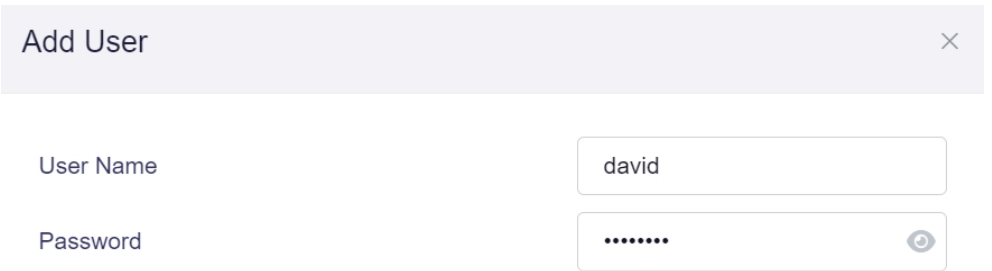


- **Permitir acceso a Samba desde WAN**: Habilitar it si desea que los dispositivos ascendentes accedan al servicio Samba.

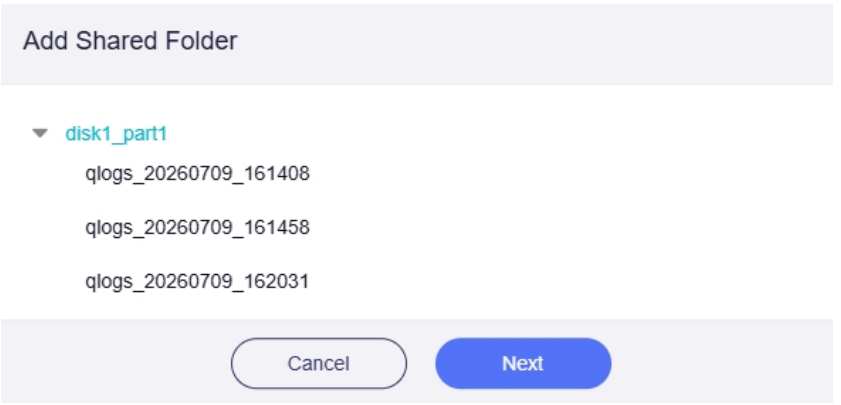
2. Haga clic en **Configuración rápida Compartir** para establezca el enlace compartido.



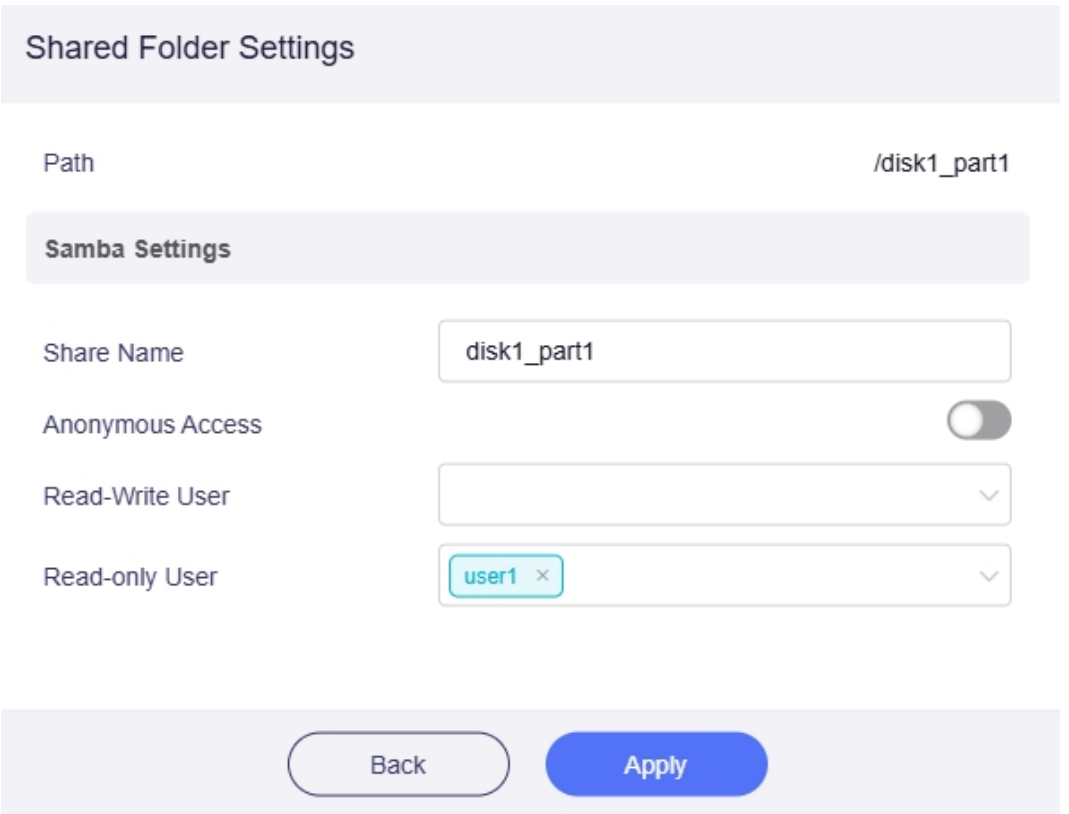
3. Agregue un usuario y haga clic en **Siguiente**. Este paso se omitirá si ya tiene una cuenta.



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).

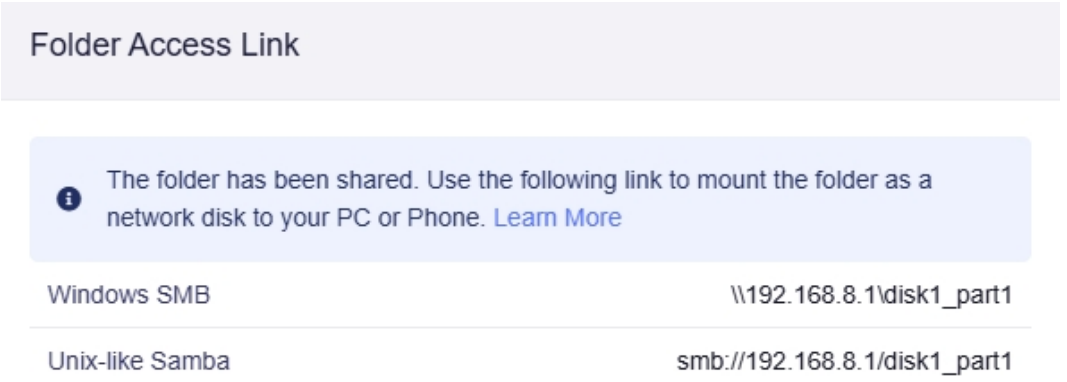


5. Configura la scarpeta compartida.
   Tel usuario creado en el paso anterior se agregará a **Usuario de solo lectura** de forma predeterminada. Si desea este usuario para poder escribir o eliminar archivos, eliminelo de Usuario de solo lectura y agréguelo a **Lectura-Escritura Usuario**, luegoluego haga clic **Aplicar**.



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

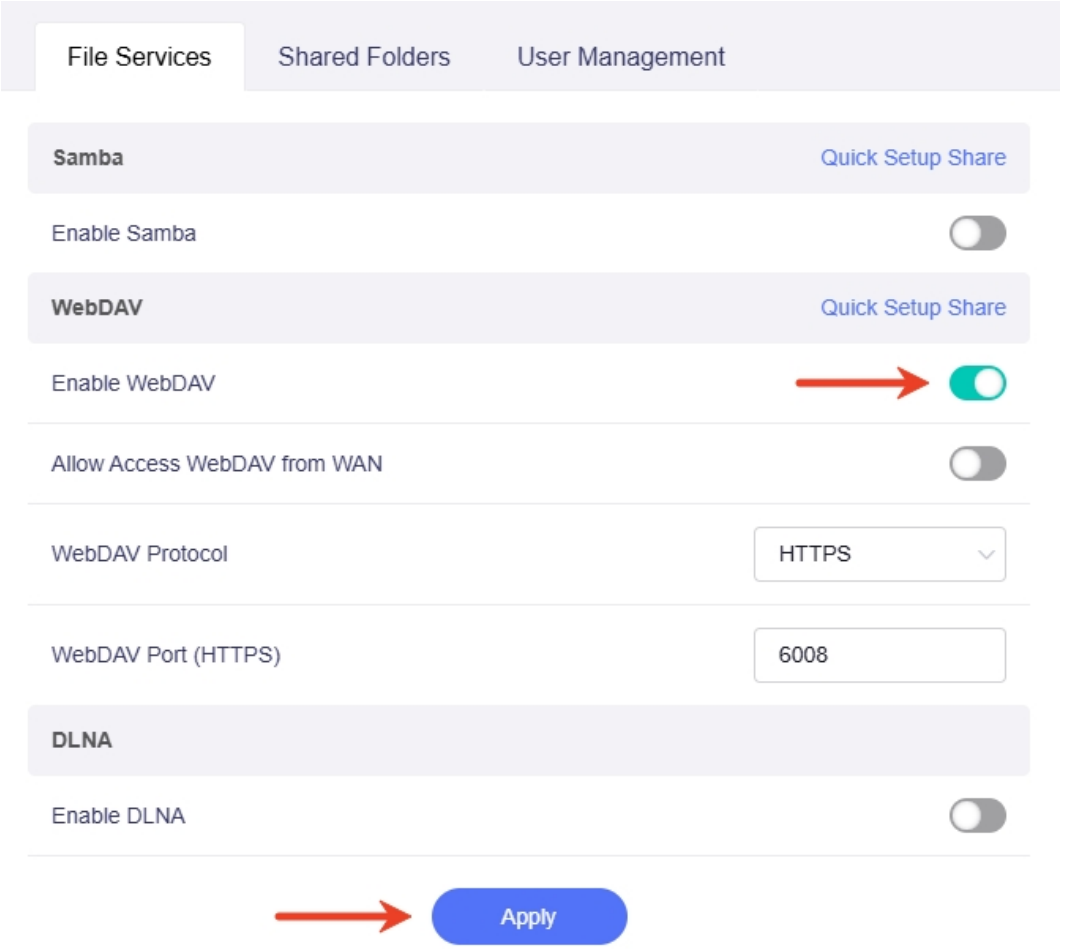
6. Obtenga el enlace de acceso a la carpeta.
   La página mostrará el enlaces para Windows y sistemas operativos tipo Unix. El sistema tipo Unix incluyes Android, iOS, macOS, Ubuntu, etc. Ahora puedes acceder su carpeta compartida a través del servicio Samba a través de estos enlaces.



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 tu enrutador’s IP WAN, que se puede encontrar en la página INTERNET del panel de administración web.

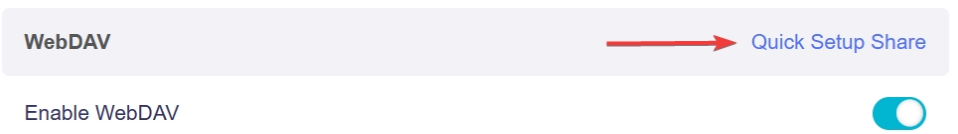
12.3.3 Configurar WebDAV

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

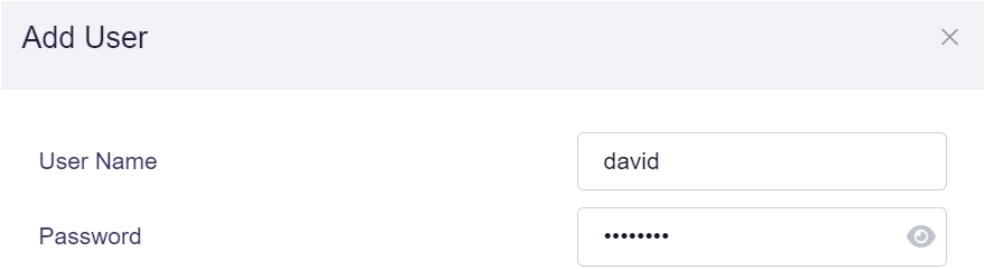


- **Permitir acceso a WebDAV desde WAN**: habilitar it si desea que los dispositivos ascendentes accedan al servicio WebDAV.
- **Protocolo WebDAV**: HTTP no está cifrado; Úselo bajo su propia responsabilidad. HTTPS está cifrado y utiliza certificado autofirmado.
- **Puerto WebDAV**: no es necesario modificar el número de puerto a menos que haya un conflicto. El puerto número rango es 1024 - 65535.

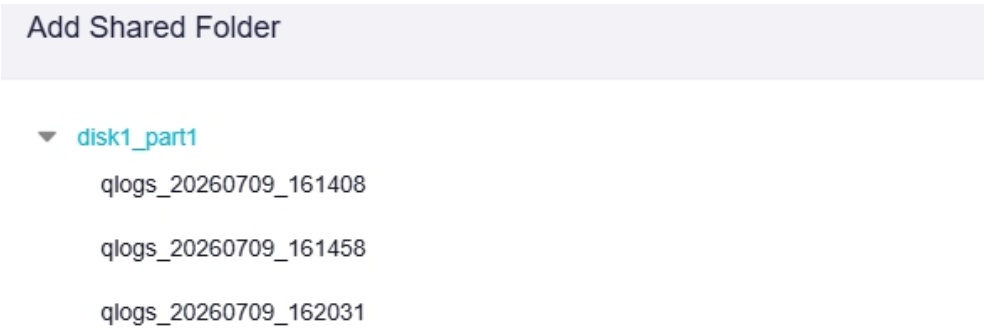
2. Haga clic en **Configuración rápida Compartir** a sestablezca el enlace compartido.



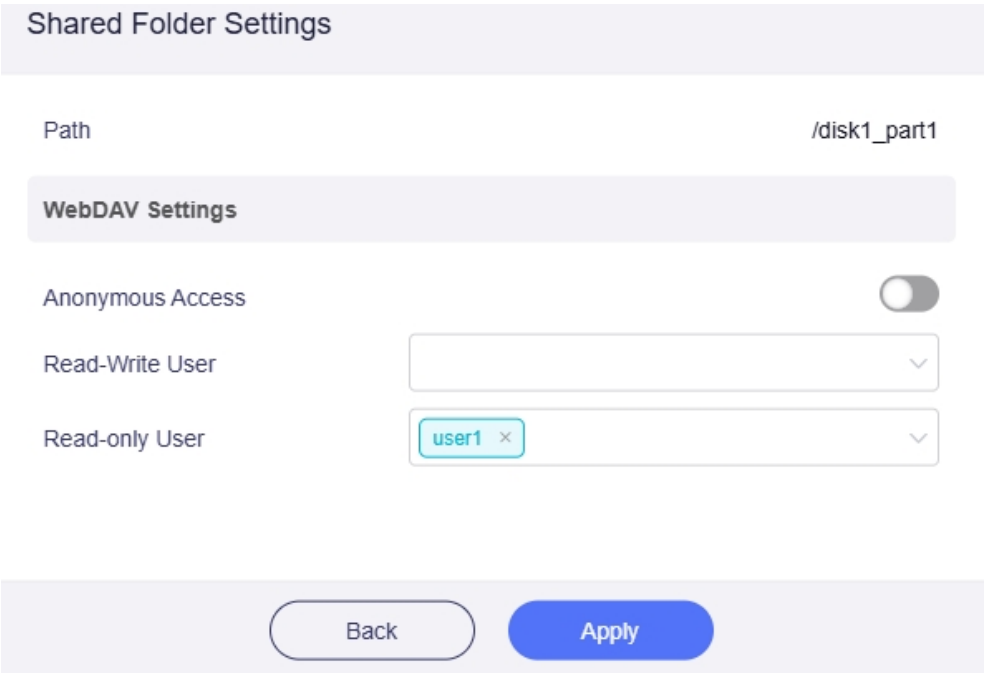
3. Agregue un usuario y haga clic en **Siguiente**. Este paso se omitirá si ya tiene una cuenta.



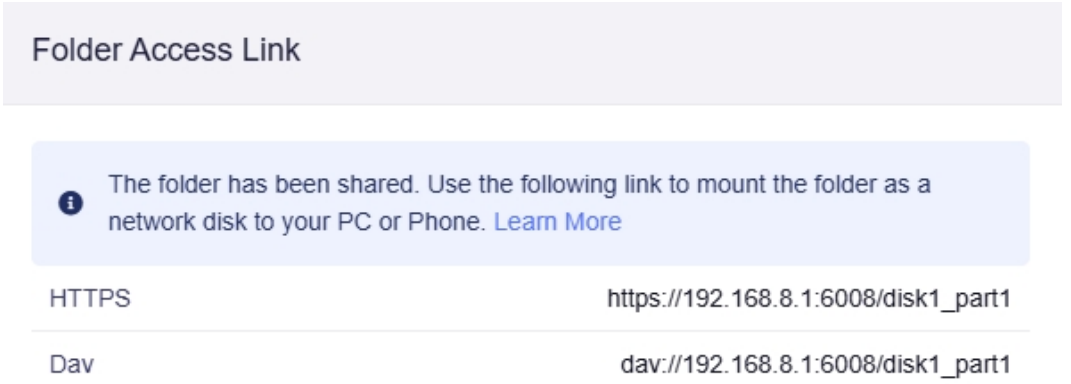
4. Haga clic en el ícono del triángulo para mostrar todas las carpetas. Sseleccione una carpeta para compartir. Sisi desea compartir el completo disco, haga clic en el nombre del disco (por ejemplo, disk1_part1).



5. Configurar el scarpeta compartida.
   El usuario creado en el paso anterior se agregará a **Usuario de solo lectura** de forma predeterminada. Si desea que este
   Si quieres esto usuario pueda escribir o eliminar archivos, eliminelo del usuario de solo lectura y agréguelo a **lectura-escriturae Usuario**, luego haga clic **Aplicar**.



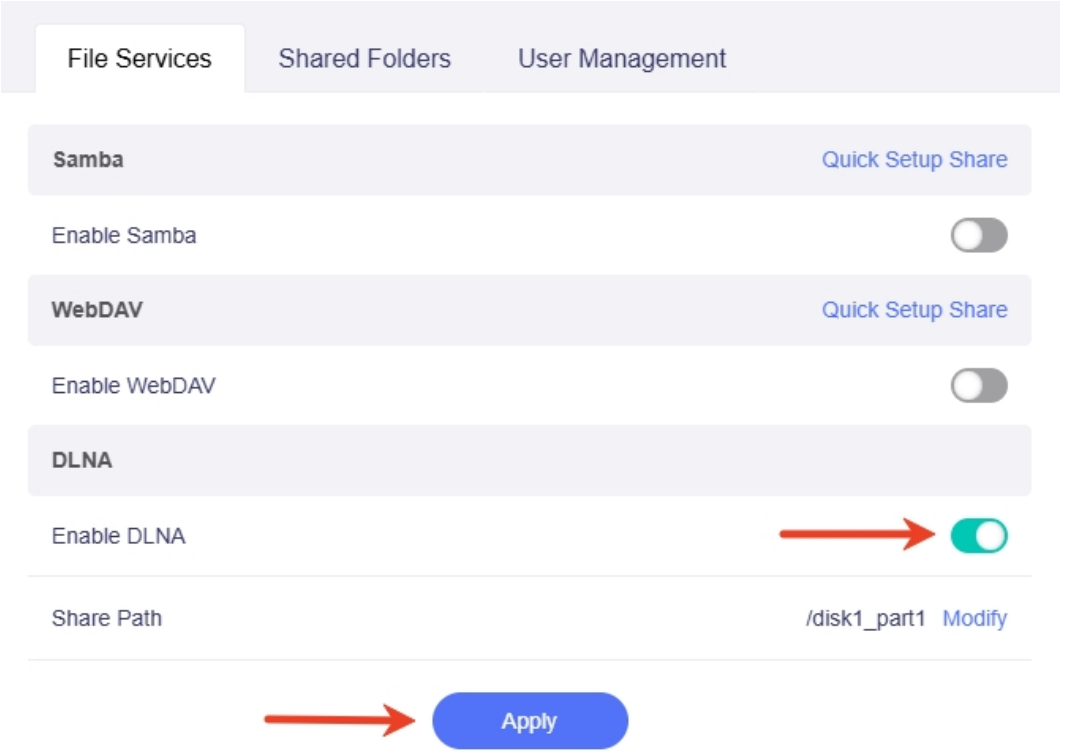
6. Obtenga el enlace de acceso a la carpeta.
   La página mostrará el enlaces para Windows y sistemas operativos tipo Unix. Los sistemas tipo Unix incluyens Android, iOS, macOS, Ubuntu, etc. Ahora puede acceder a su carpeta compartida a través del servicio WebDAV a través de estos enlaces.



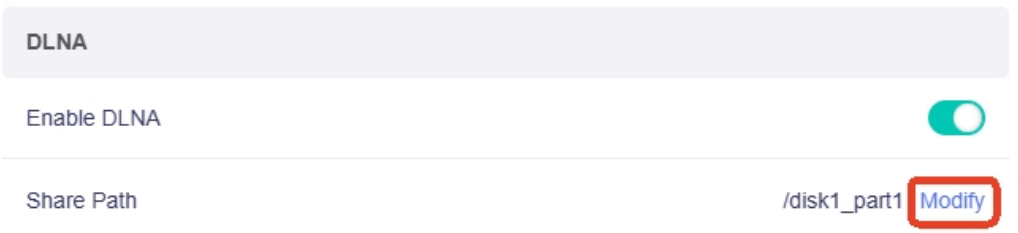
Nota: si habilita **Permitir acceso WebDAV desde WAN** y acceda la carpeta compartida de red ascendente, reemplace la IP del enrutador (predeterminada: 192.168.8.1) en el enlace de acceso con la IP WAN de tu enrutador’s, que se puede encontrar en la página INTERNET del panel de administración web.

12.3.4 Configurar DLNA

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



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



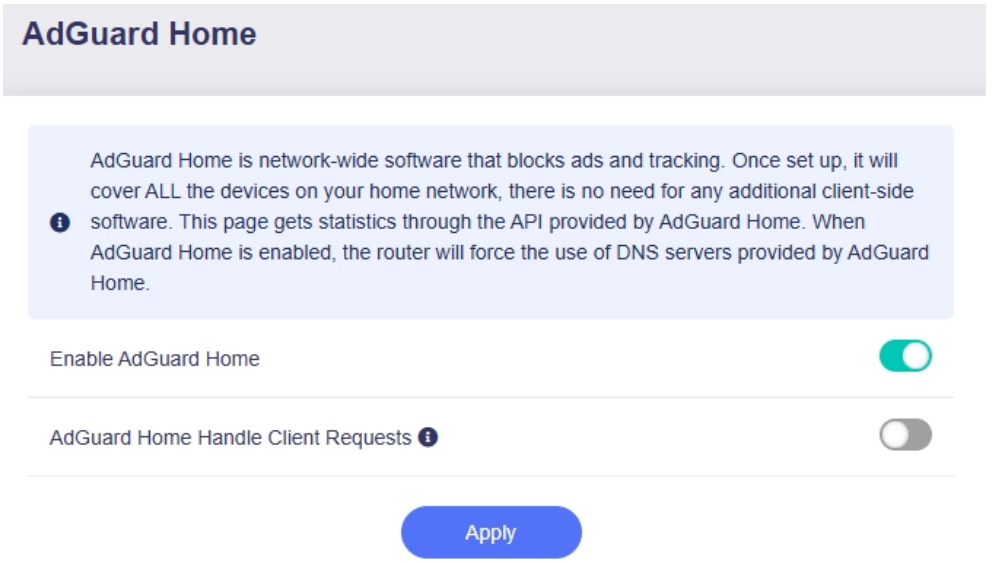
3. Conecte su televisor inteligente al enrutador. encontrará el DLNA sservidor automáticamente.

12.4 AdGuard Home

AdGuard Home es un software de bloqueo de publicidad y prevención de seguimiento en toda la red. Una vez configurado, cubrirá todos los dispositivos cliente sin necesidad de software adicional del lado del cliente.

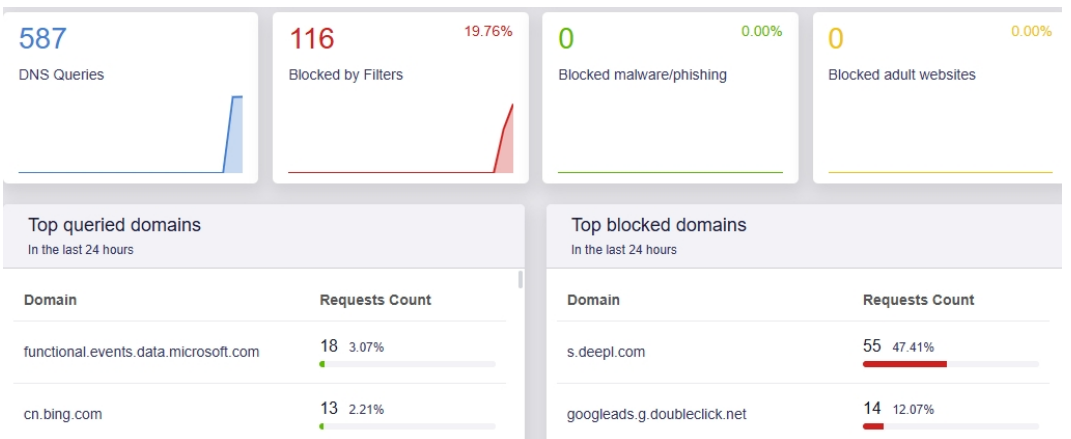
Siga estos pasos para configurar AdGuard Home.

1. Inicie sesión en el enrutador's web undmin panel, navegue hasta **APLICACIONES** > **AdGuard Home**. Active en **Ehabilite Inicio de AdGuard** y haga clic en **Aplicar**.

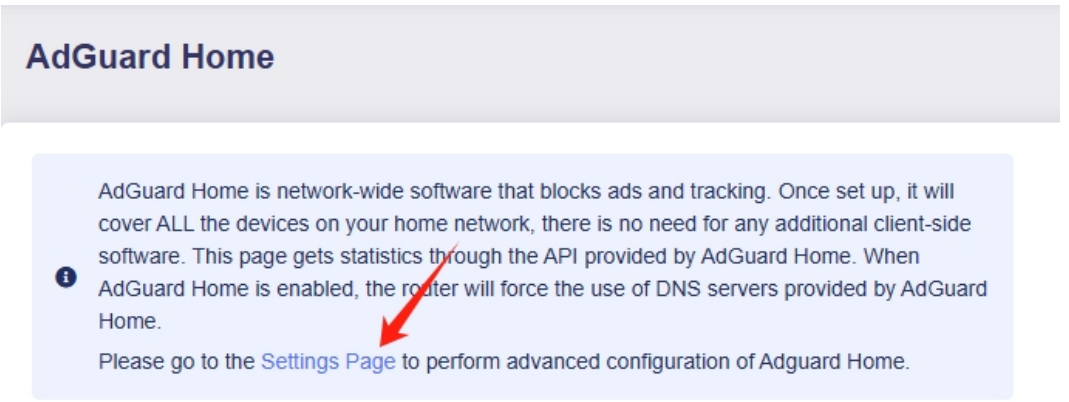


- **AdGuard Home Handles Solicitudes de clientes**: si está habilitado, las consultas de DNS de los dispositivos cliente serán manejadas directamente por AdGuard Home, pero esto hará que las políticas de VPN basadas en dominios fallen.

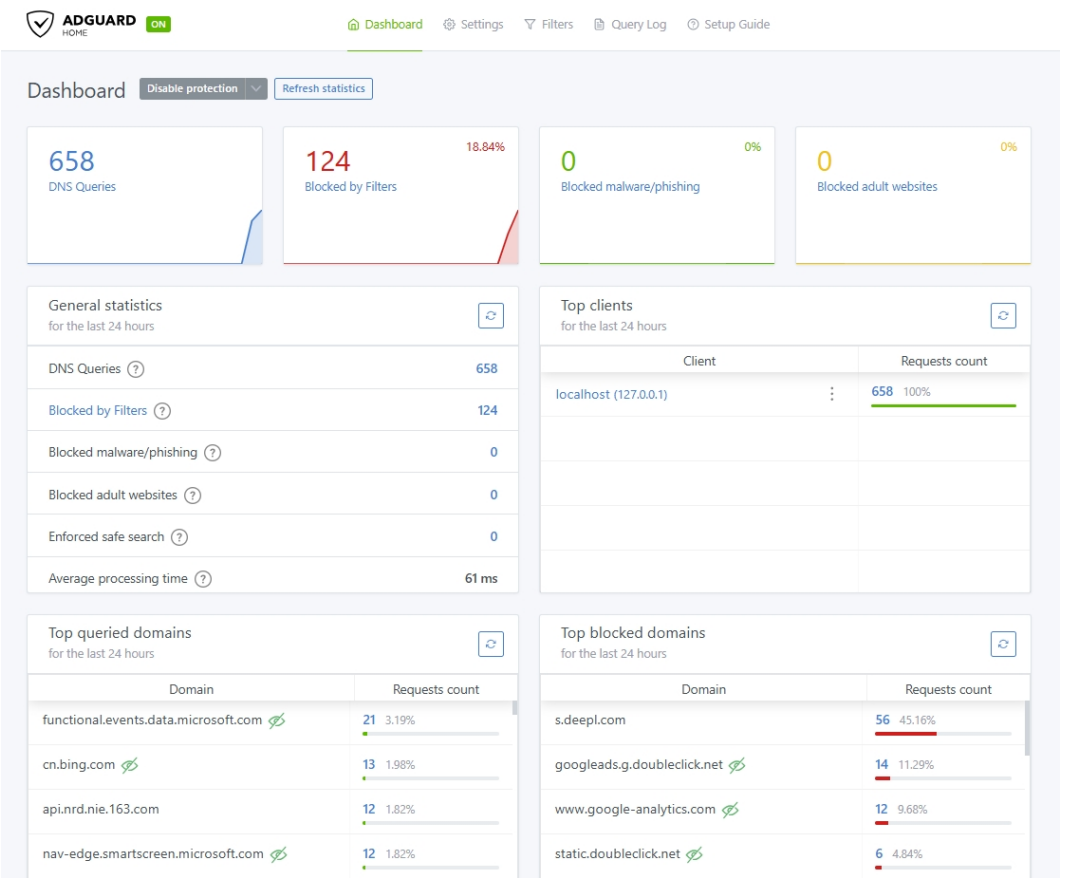
2. La página cargará automáticamente estadísticas DNS (consultas, dominios bloqueados, etc.) a través de la API proporcionada por AdGuard Home.



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



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



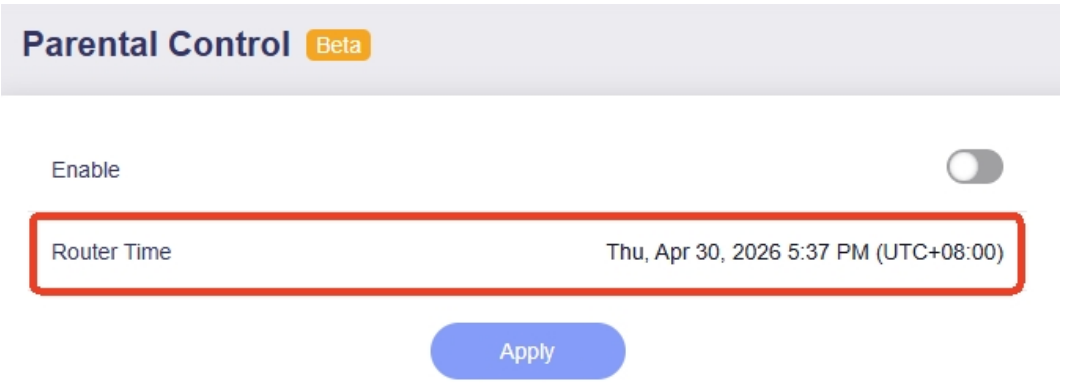
12.5 Control parental

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.

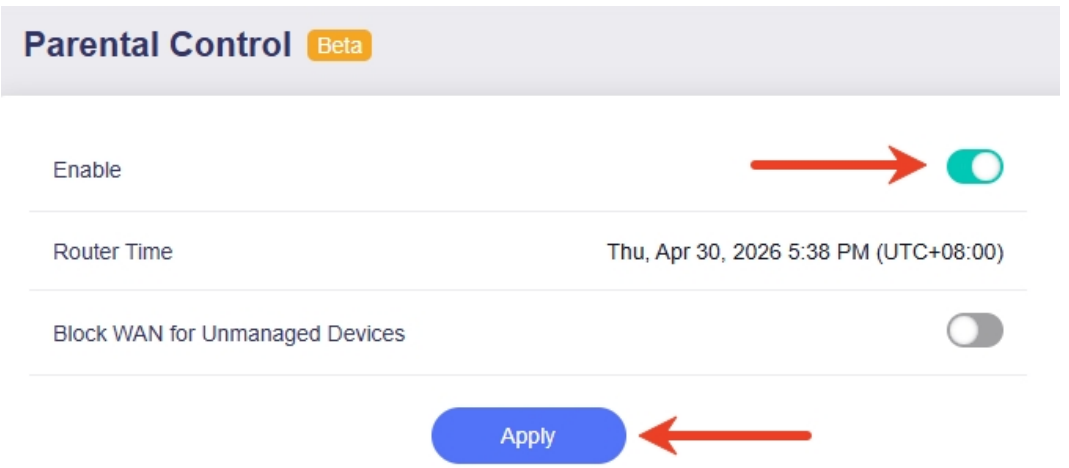
12.5.1 Configuración rápida

Siga estos pasos para configurar Control parental en GL.router 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.



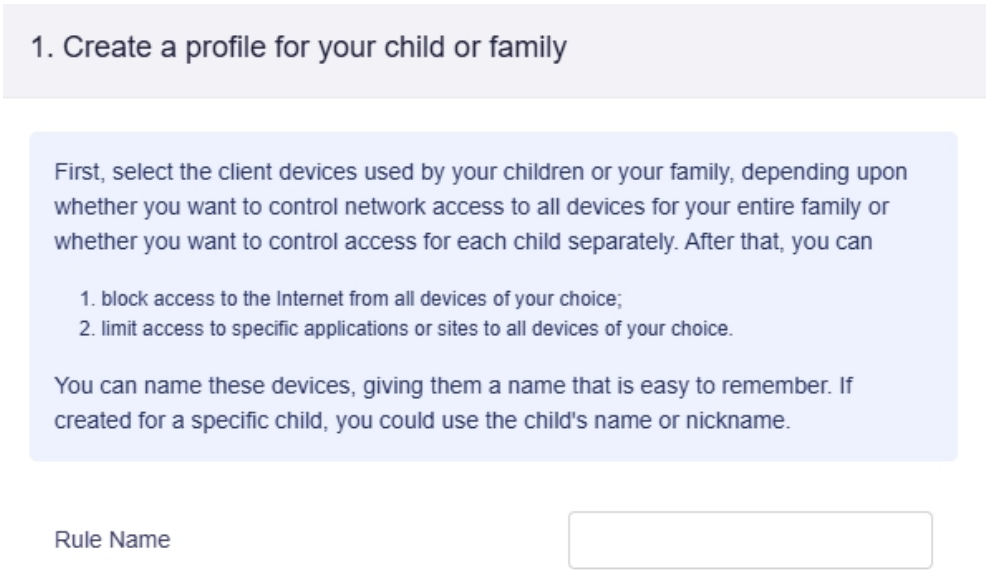
- **Bloquear WAN para dispositivos no administrados**: Bloquea el acceso a Internet para todos los dispositivos que no están en la lista de Control parental.

Aquí tienes un caso de uso para tu referencia.

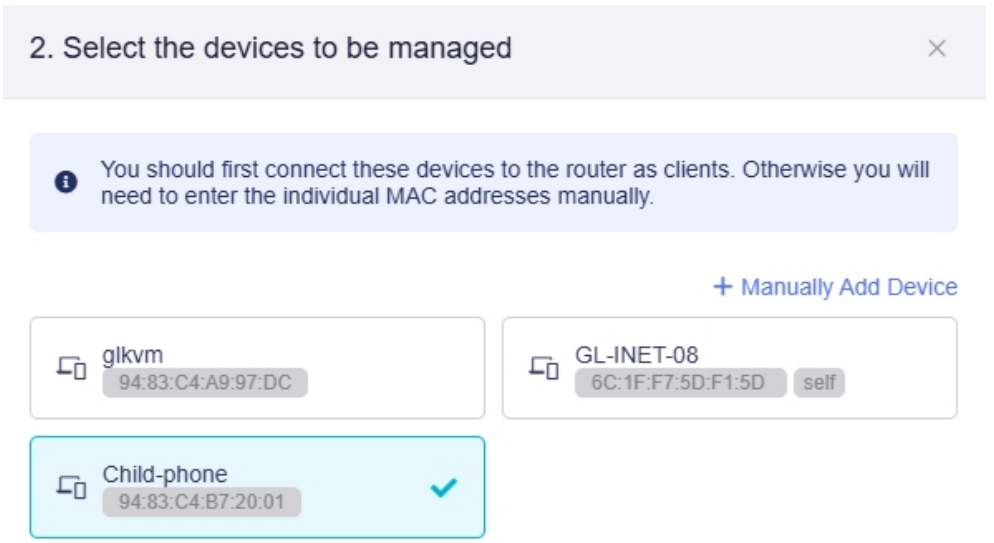
Escenario: Dispositivos en estees solo pueden acceder a Internet para estudiar de 8 a.m. a 11 a.m. de lunes a viernes y para jugar de 6 p.m. a 8 p.m. los fines de semana. El acceso a Internet está bloqueado de forma predeterminada en todos los demás momentos.

Pasos de configuración:

1. Cree un perfil y personalice un nombre.

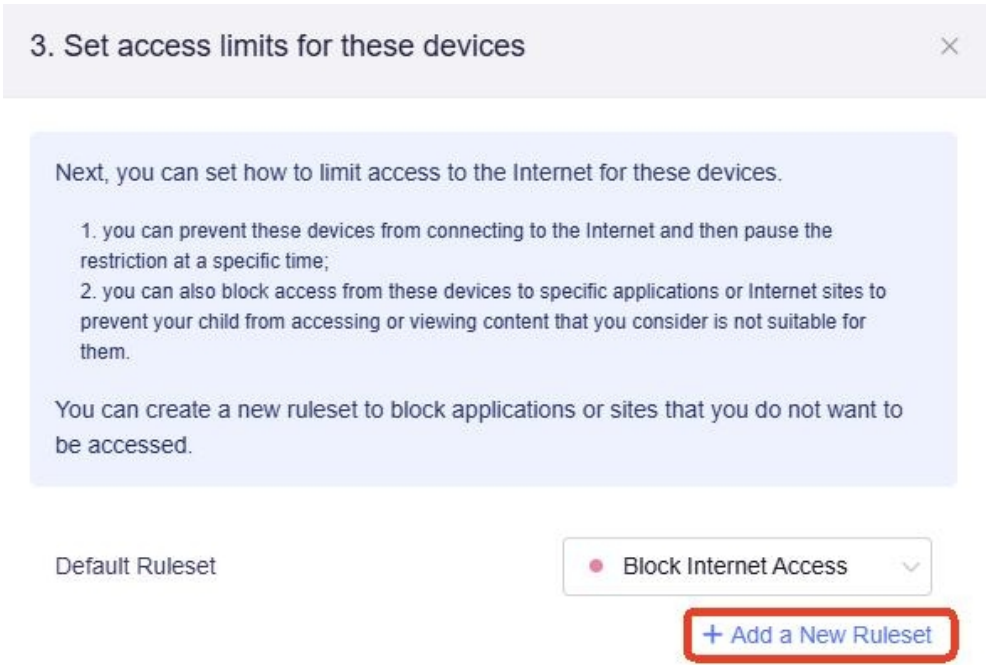


2. Seleccione los dispositivos que desea administrar. Conéctelos primero al enrutador. Si no se han conectado al enrutador, agréguelos manualmente ingresando sus direcciones MAC.

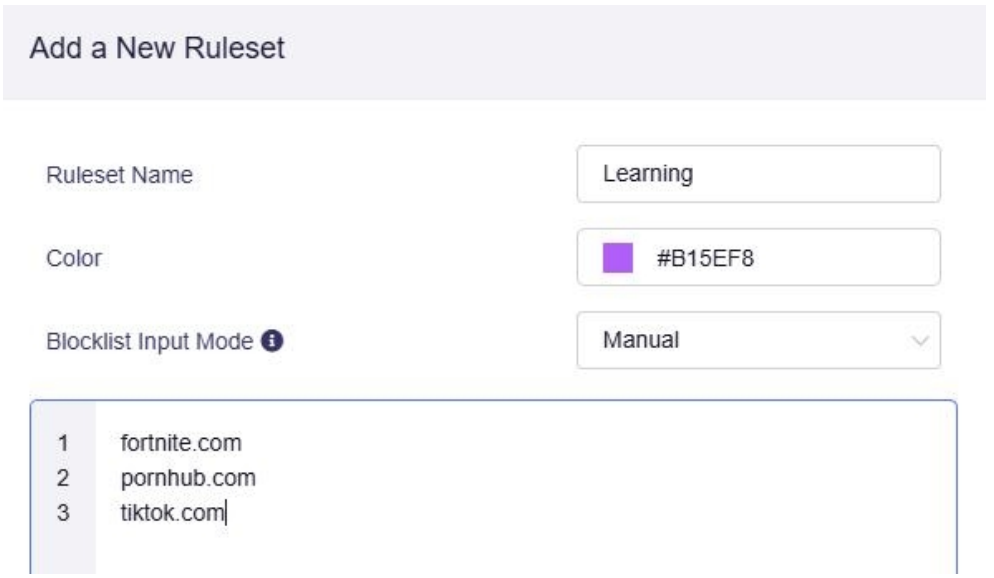


3. Establezca el límite de acceso.

   Hay dos conjuntos de reglas predeterminados: **Bloquear acceso a Internet** y **Sin límite**. Hacer clic **Agregue un nuevo conjunto de reglas** para crearcrear dos conjuntos de reglas más para su uso posterior: **Aprendizaje** y **Jugar**.

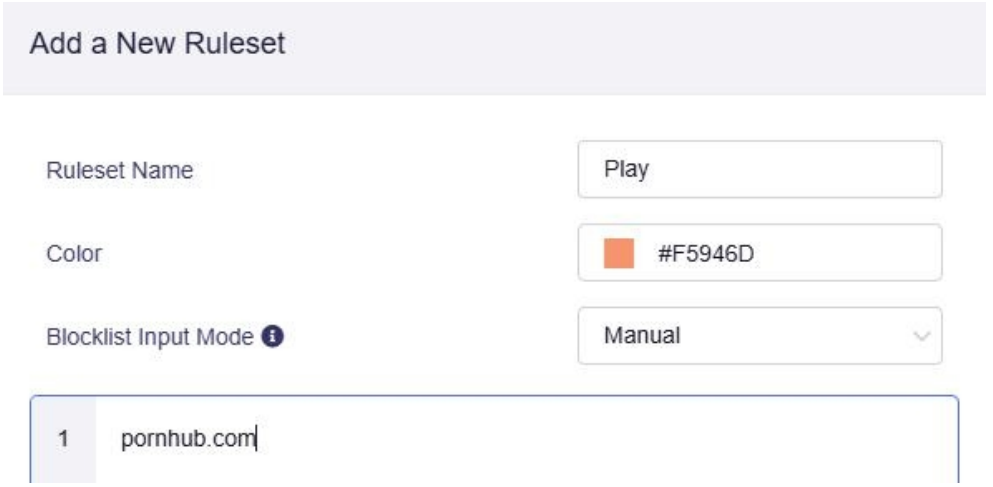


   Especifique el nombre del conjunto de reglas (p. ej., Aprendizaje) y color, ingrese a la websitios to bloquear, luegoluego haga clic en **Aplicar**.

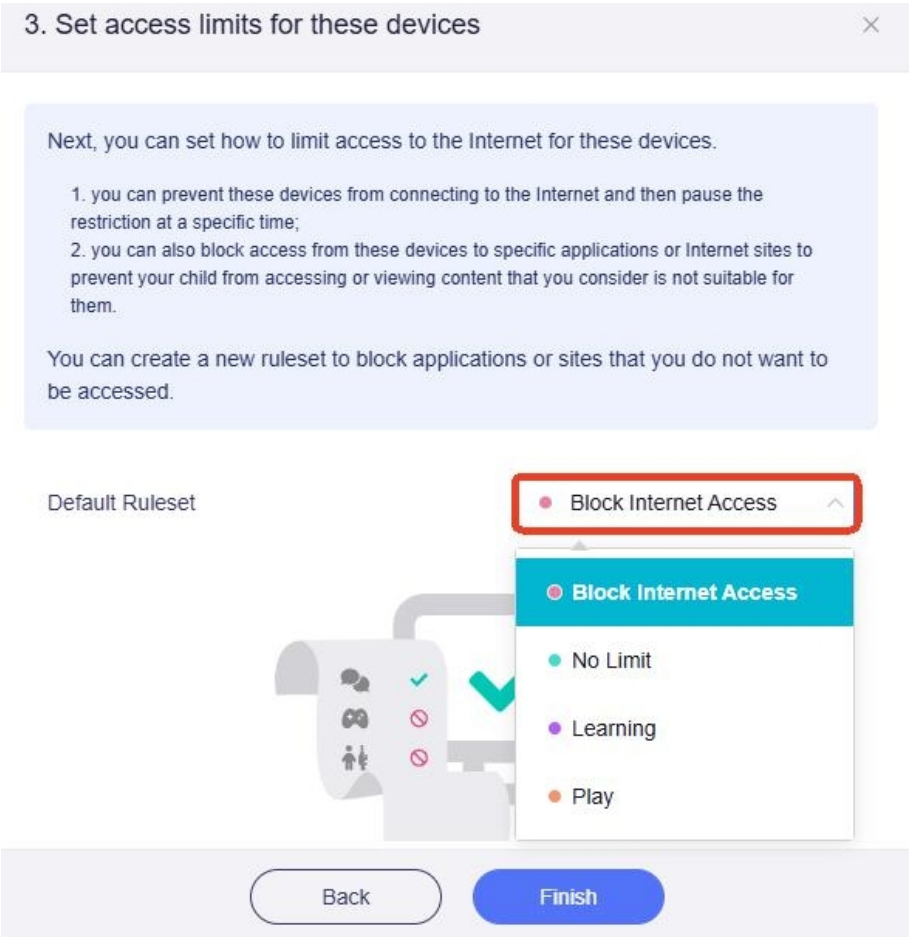


   Nota: Los nombres de dominio ingresados en la lista de bloqueo deben incluir sus subdominios. Por ejemplo, si se ingresa "ejemplo.com", también incluye cualquier subdominio, como "subdominio.example.com".

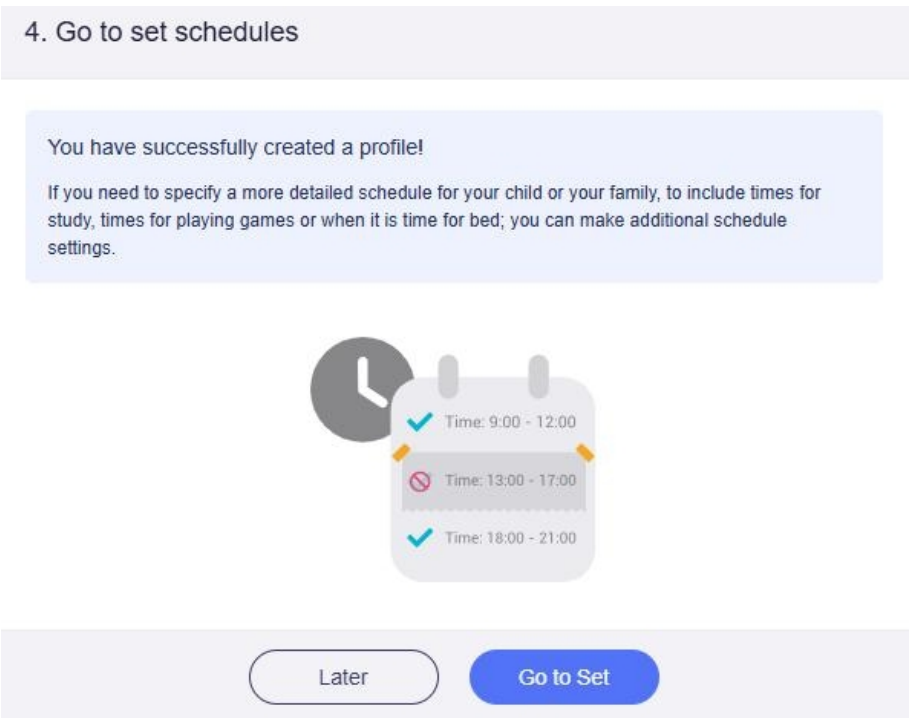
Del mismo modo, cree otro conjunto de reglas. Especifique el nombre del conjunto de reglas (por ejemplo, Reproducir) y el color, ingrese los sitios web que desea bloquear y luego haga clic en **Aplicar**.



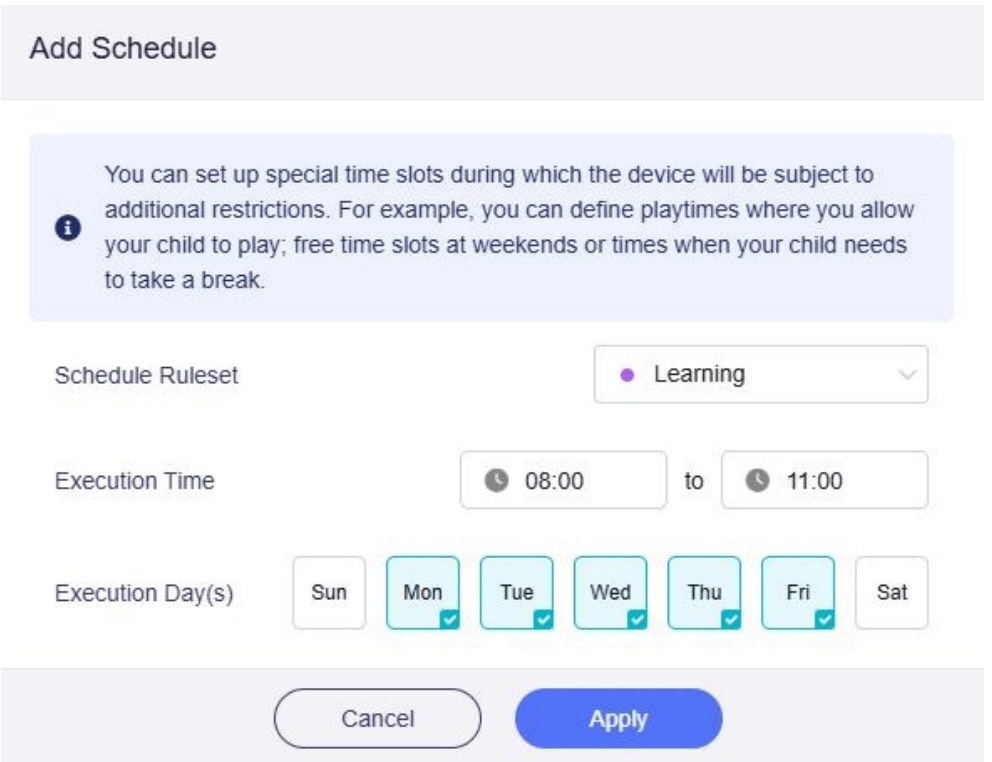
Al aplicared, habrá un total de cuatro conjuntos de reglas. Sseleccione **Bloquear el acceso a Internet** como el **Conjunto de reglas predeterminado** y haga clic en **Finalizar**.



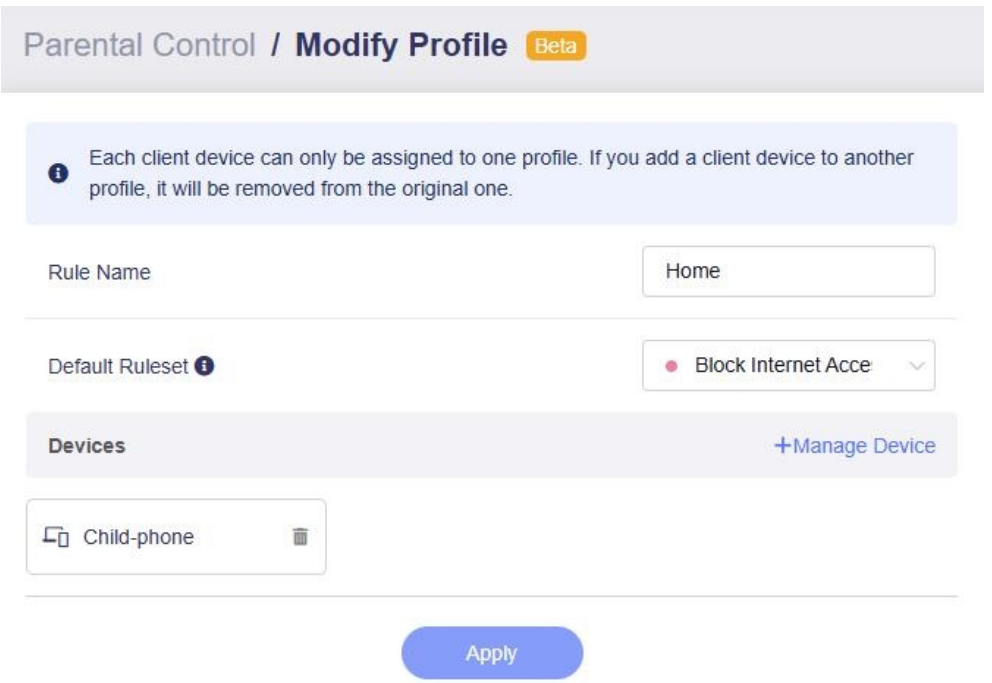
4. A continuación, establezca la programación para su perfil. Haga clic en **Ir a conjunto**.



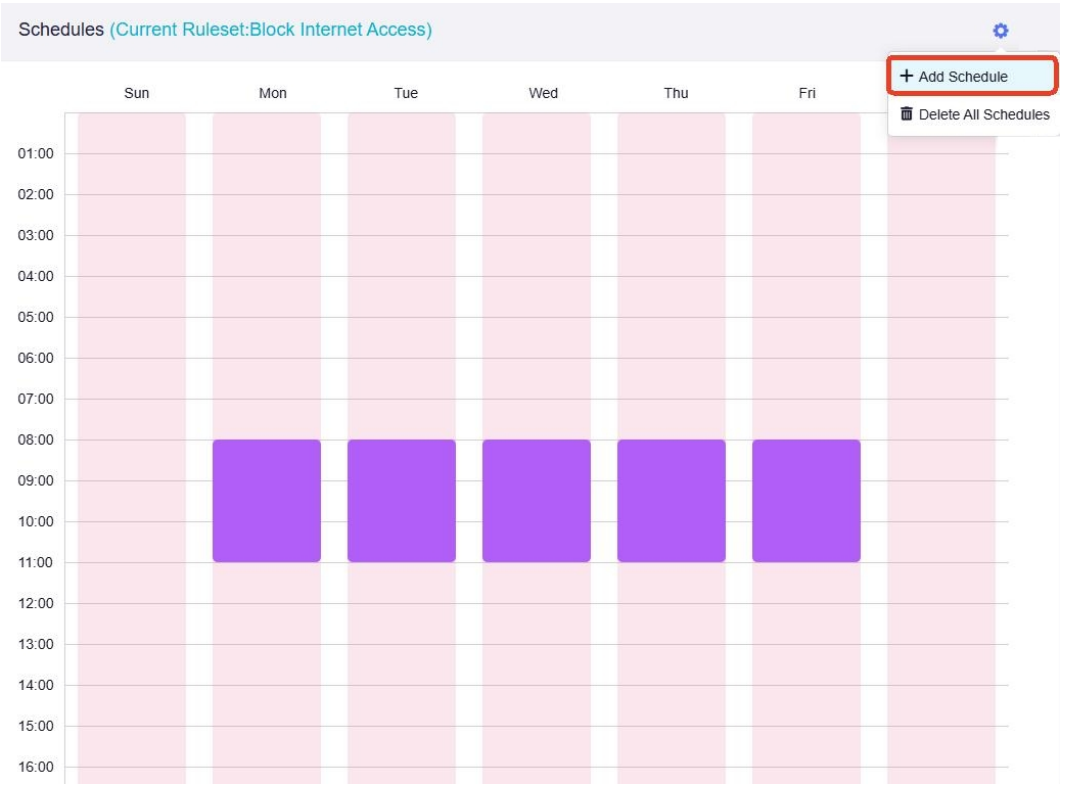
Agregue el **Aprendizaje** conjunto de reglas al cronograma. Establezca el **Hora de ejecución** de 8 a. m. a 11 a. m. de lunes a viernes y luego haga clic en **Aplicar**.



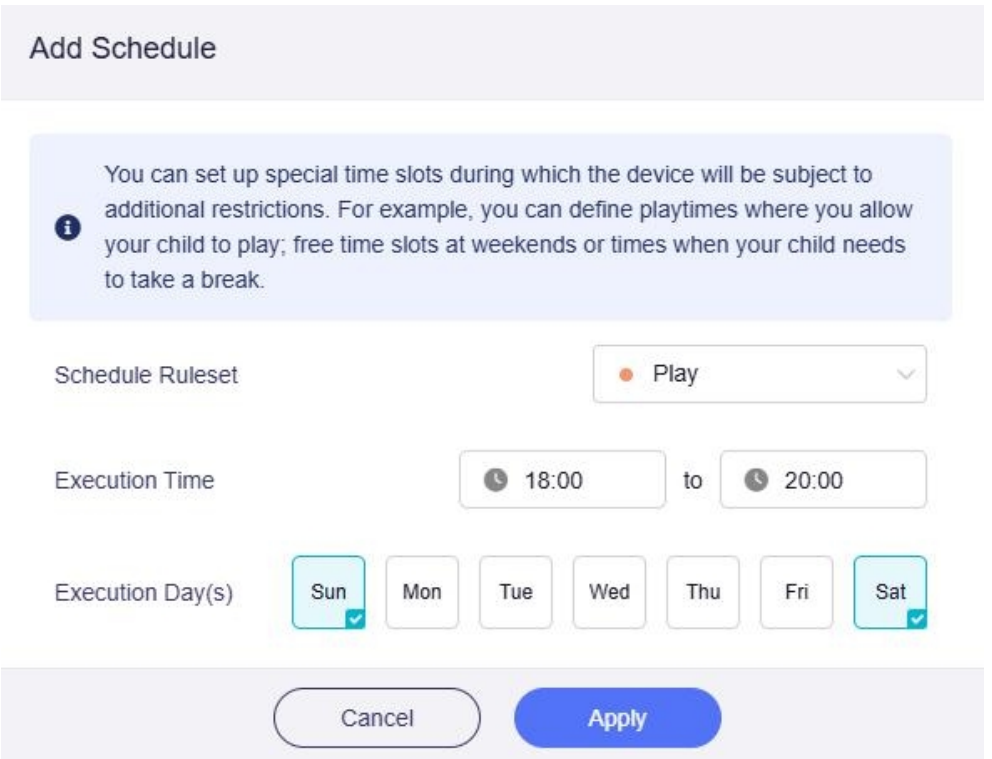
5. Serás redirigido a la página de edición del perfil creado.



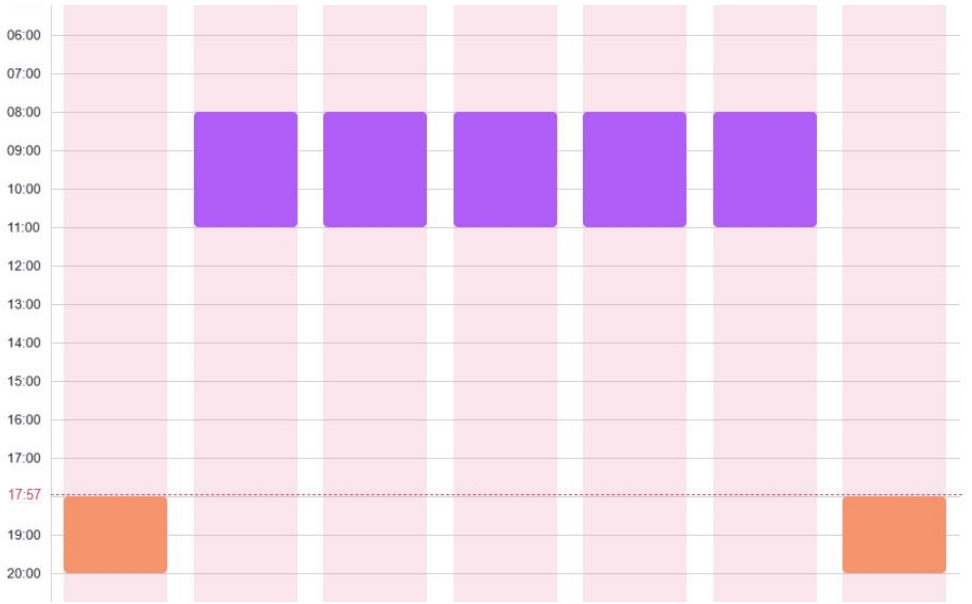
Vaya hasta la parte inferior y verá que se ha creado un cronograma. Haga clic en el ícono de ajustes en la esquina superior derecha y seleccione **Agregar programación**.



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**.



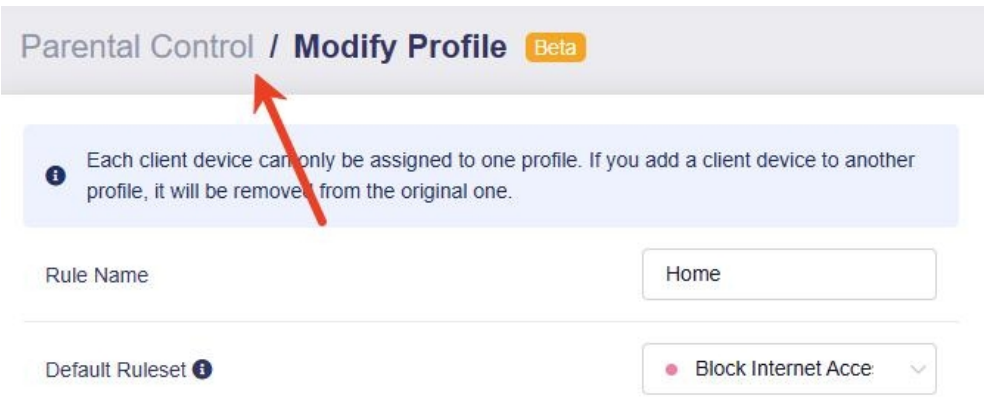
El conjunto de reglas de Play se agregará al cronograma.



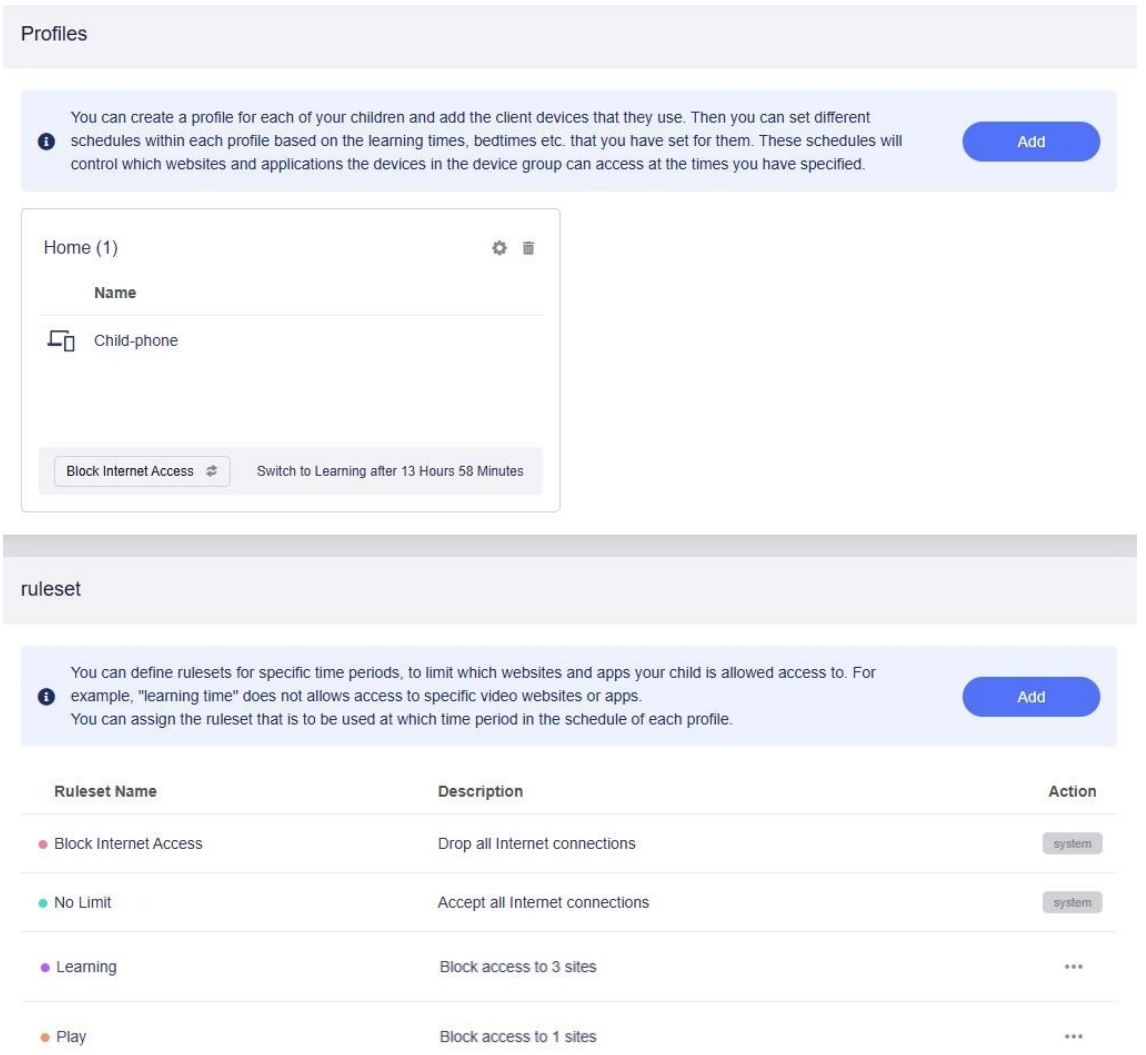
Consejos:

- La línea discontinua roja indica la hora actual.
- Ypuedes modifique el tiempo de ejecución haciendo clic en a cierto conjunto de reglas en la programación.

7. Haga clicick **Control parental** en la parte superior para volver a la página Control parental.



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


Profiles
You can create a profile for each of your children and add the client devices that they use. Then you can set different schedules within each profile based on the learning times, bedtimes etc. that you have set for them. These schedules will control which websites and applications the devices in the device group can access at the times you have specified.
Add
Home (1)
Name
Child-phone
Block Internet Access
Switch to Learning after 13 Hours 58 Minutes
ruleset
You can define rulesets for specific time periods, to limit which websites and apps your child is allowed access to. For example, "learning time" does not allows access to specific video websites or apps.
You can assign the ruleset that is to be used at which time period in the schedule of each profile.
Add
Ruleset Name
Description
Action
Block Internet Access
Drop all Internet connections
system
No Limit
Accept all Internet connections
system
Learning
Block access to 3 sites
Play
Block access to 1 sites

12.5.2 Solución de problemas

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

1. Problema de caché de DNS.
   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, cual evitar ques las reglas de acceso entren en vigor. Deshabilitar aleatoria Dirección MAC en el dispositivo de destino, luego vuelva a agregar el dispositivo a su perfil.

12.6 ZeroTier

ZeroTier es una VPN definida por software que permite una comunicación cifrada segura entre dispositivos a través de Internet. Crea una red virtual privada que permite que los dispositivos se comuniquen como si estuvieran en la misma LAN, independientemente de la ubicación física o la topología de la red. ZeroTier presenta una configuración sencilla y facilidad de uso, junto con cifrado de extremo a extremo, segmentación de red y puentes de red.

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

Nota:

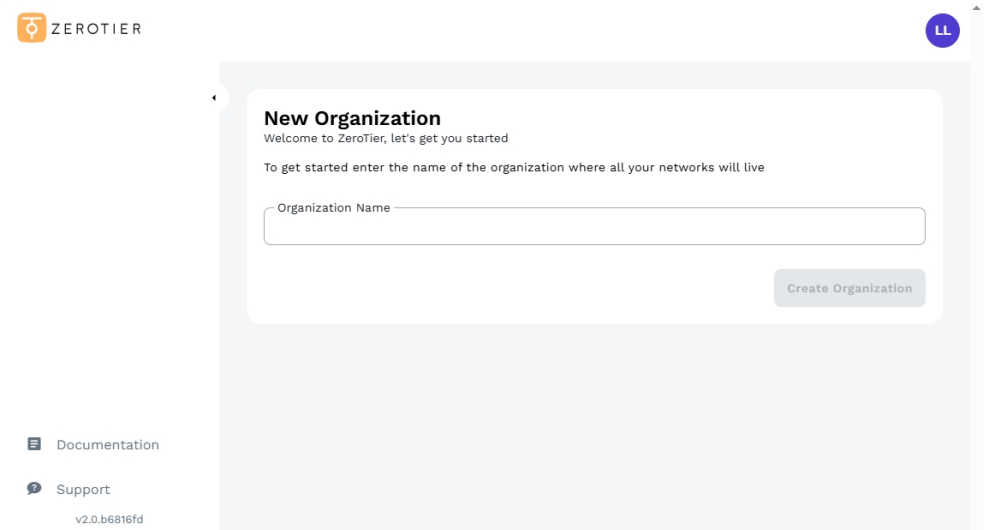
1. No se recomienda utilizar ZeroTier simultáneamente con cualquiera de las siguientes funciones o servicios, ya que esto puede causar conflictos de enrutamiento: Cliente OpenVPN, Cliente WireGuard, GoodCloud Site to Site, Tailscale y AstroWarp.
2. Esta función se encuentra actualmente en versión beta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

12.6.1 Configurar ZeroTier

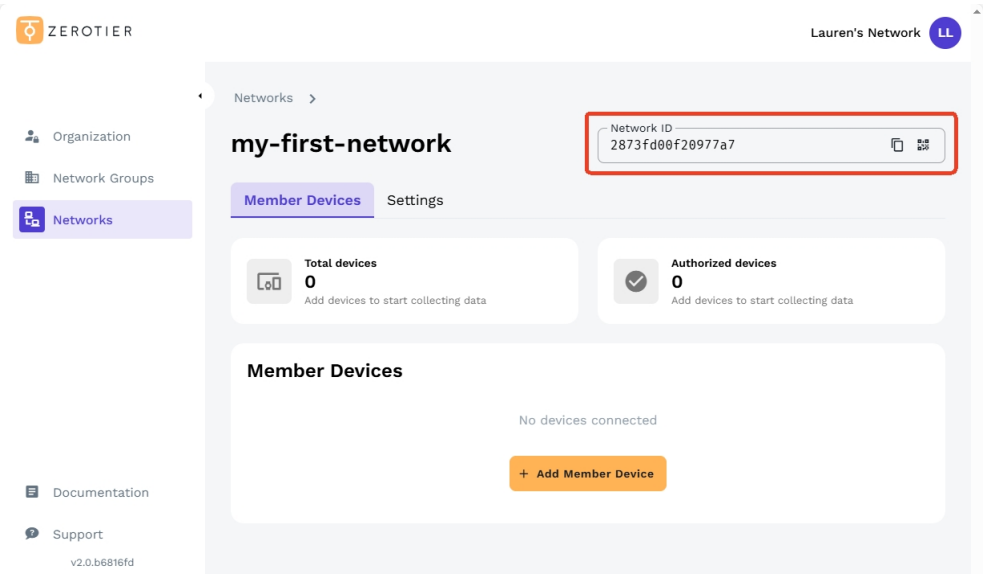
Hay dos versiones de ZeroTier Central disponibles: New Central y Legacy Central.

Los siguientes pasos utilizan New Central como ejemplo.

1. Visite [sitio web oficial de ZeroTier] e inicie sesión con su cuenta.
2. Cree una organización.

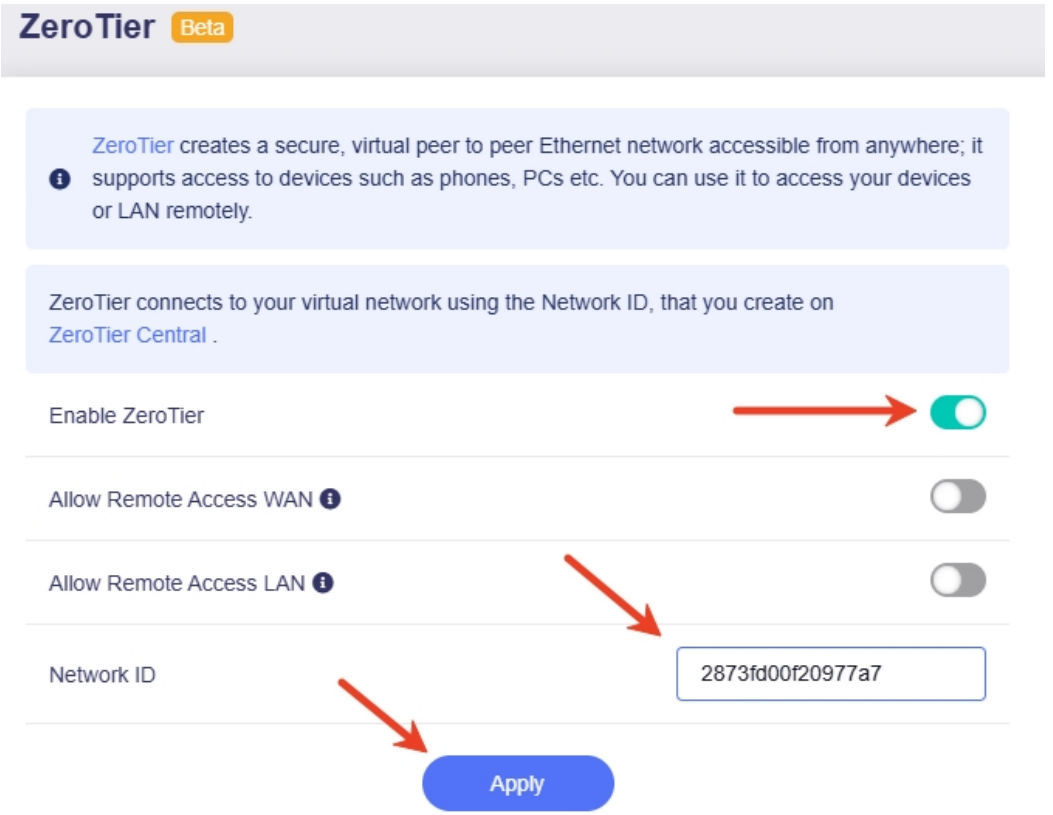


3. Seleccione un plan. Aquí elegimos **plan personal** como ejemplo, que incluye 10 dispositivos, 1 administrador de red y 1 red. Si necesita crear más redes, agregar más dispositivos o agregar rutas y DNS personalizados, elija otro plan pago.
4. Ahora se ha creado su red ZeroTier.

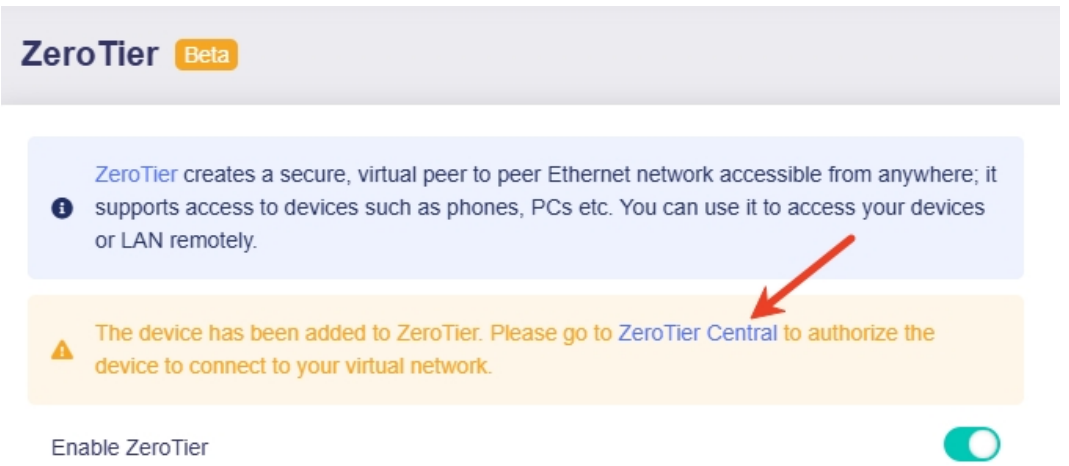


Tome nota del **ID de red**, que es una combinación alfanumérica de 16 caracteres en la esquina superior derecha, ya que será necesaria cuando conecte otros dispositivos más adelante.

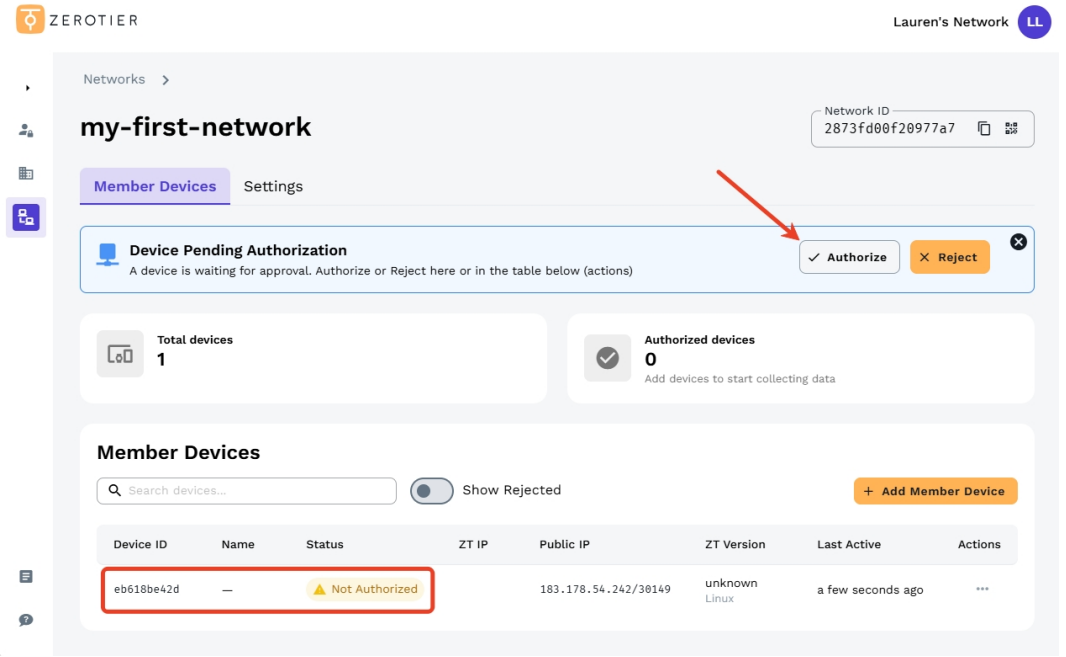
5. Inicie sesión en la web de su enrutador Panel de administración y navegue hasta **APLICACIONES** -> **ZeroTier**. Habilite ZeroTier, ingrese el **ID de red**, luego haga clic en **Aplicar**.



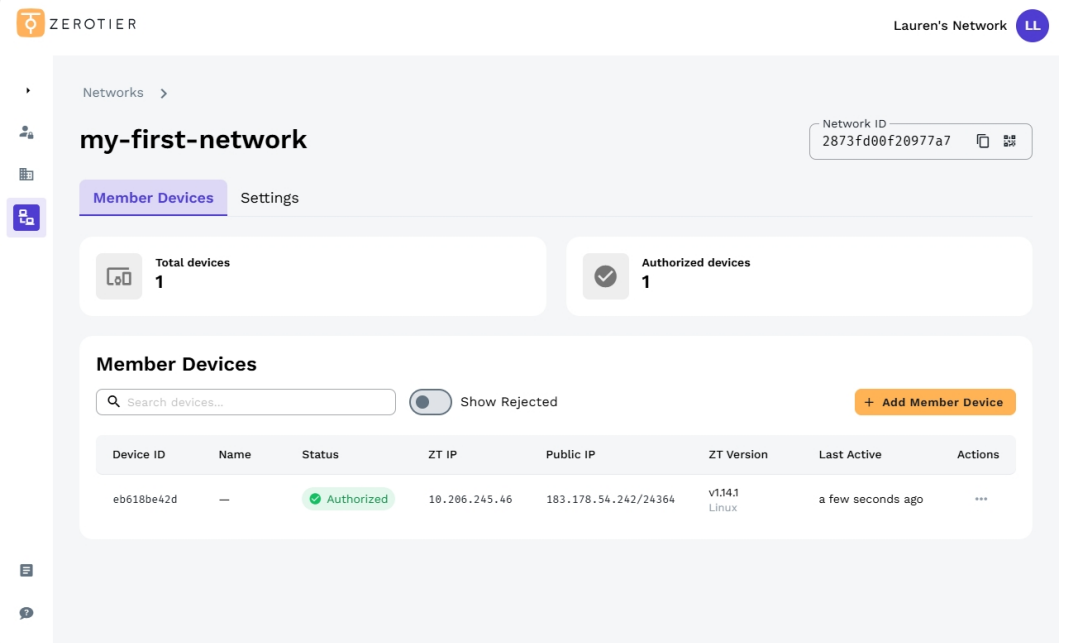
Después de un momento, la página indicará que se requiere autorización. Haz clic en **ZeroTier Central** hipervínculo para redirigir a ZeroTier Central.



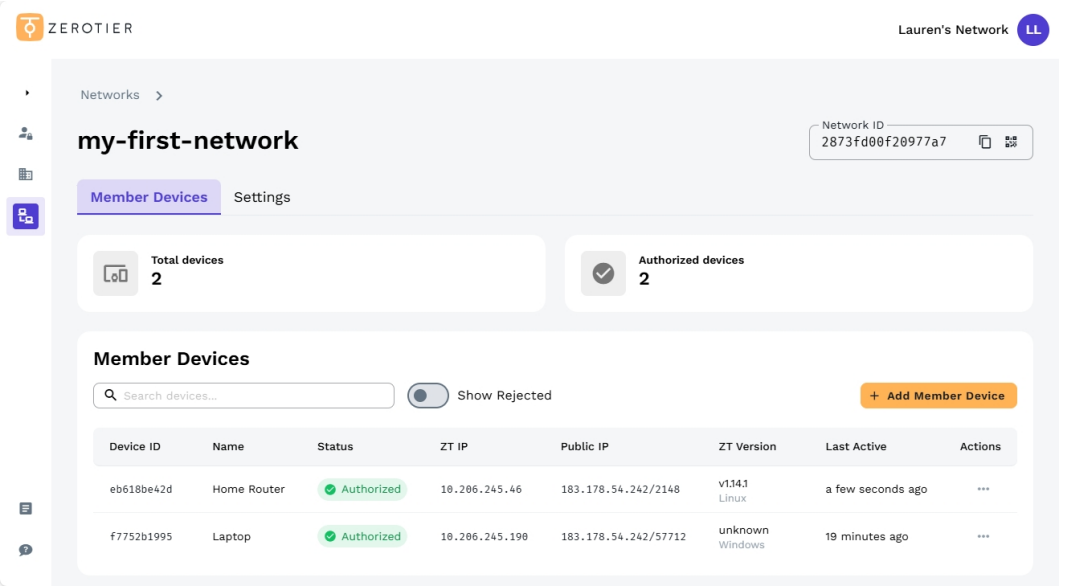
6. En ZeroTier Central, ubique el dispositivo pendiente y autorícelo.



Una vez autorizado, la página se muestra de la siguiente manera.

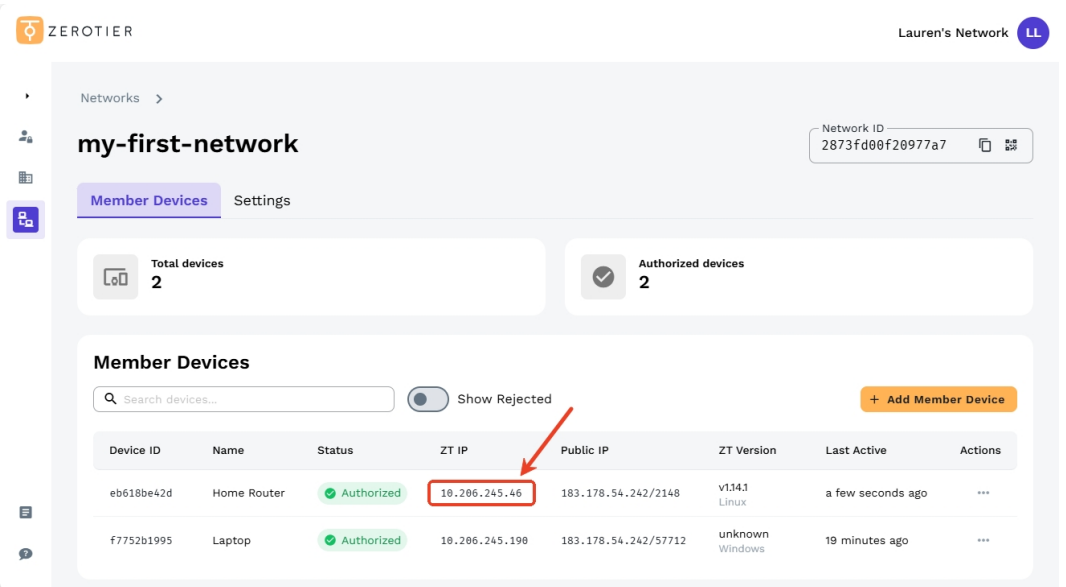


7. Agregue otro dispositivo (como una computadora o un teléfono inteligente) a la misma red ZeroTier siguiendo esta guía. Una vez agregado correctamente, la página se muestra a continuación. Verá los detalles de los dispositivos miembros, como **ID del dispositivo**, **Nombre**, **Estado**, **IP administrada** y **IP pública**.



Consejos: puede hacer clic en el ícono de tres puntos a la derecha para editar la configuración del dispositivo miembro, incluido el nombre del dispositivo, las IP administradas y la configuración avanzada.

8. Haga clic en el **IP administrada** para copiarla.



Luego puede usar esta IP administrada para acceder al enrutador desde su computadora portátil que está en la misma red ZeroTier.

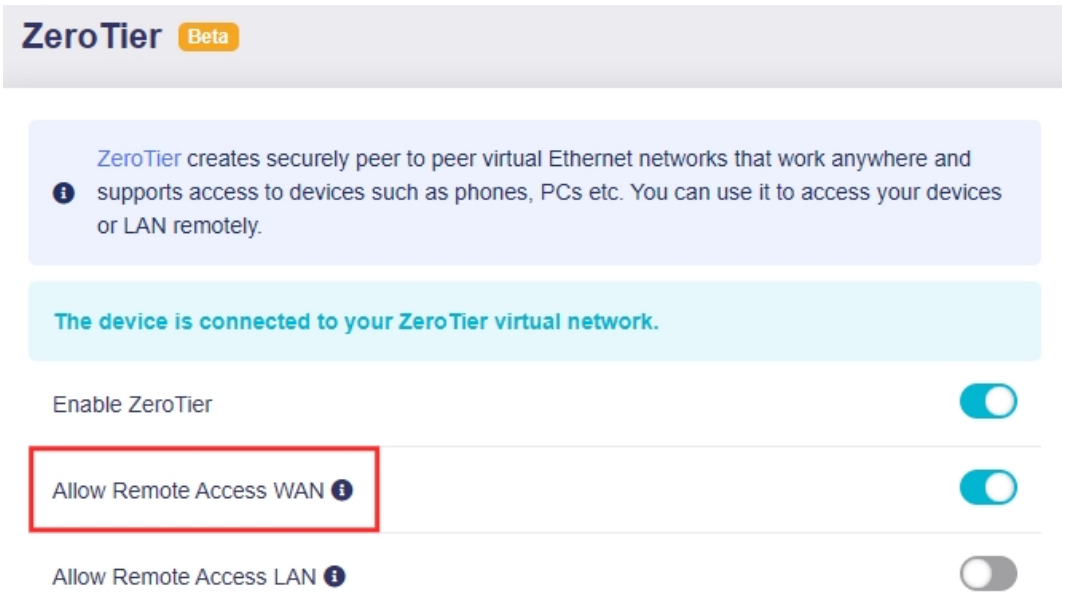
9. Pruebe la conectividad.

   En la computadora portátil conectada a la misma red ZeroTier, abra un navegador web e ingrese la IP administrada del enrutador obtenida en el paso anterior. Si puede acceder

al panel de administración web del enrutador, la conexión ZeroTier se realizó correctamente.

12.6.2 Permitir el acceso remoto a la WAN

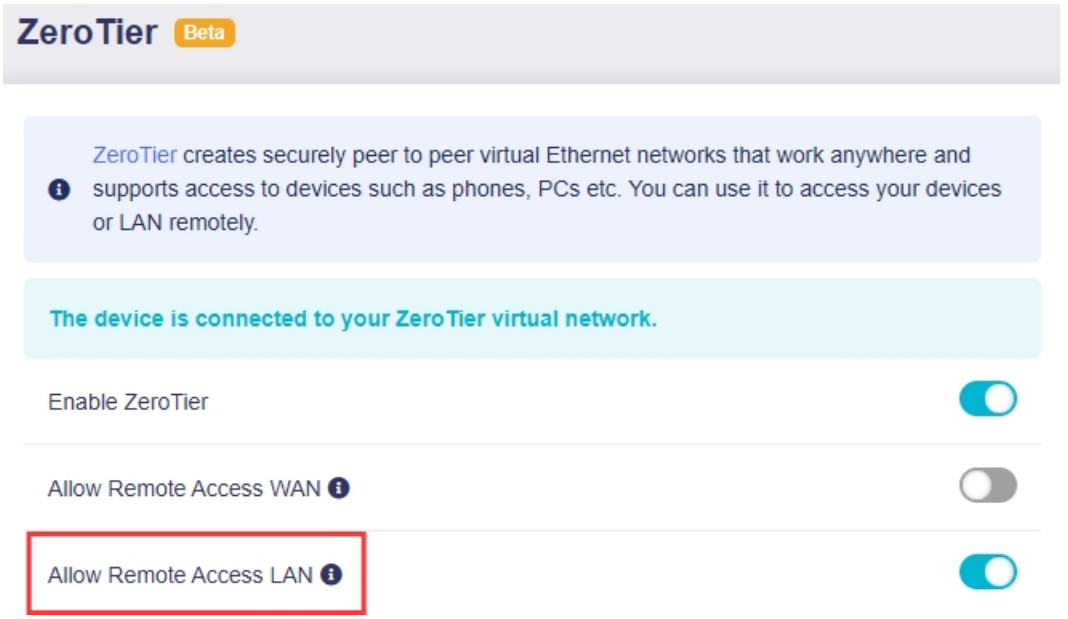
Si esta opción está habilitada, se puede acceder a los recursos en el lado WAN del dispositivo a través de la red virtual ZeroTier. Consulte aquí para obtener más detalles.



Nota: esta característica requiere que se agreguen reglas de enrutamiento a la red ZeroTier para que entre en vigor. Se puede agregar una ruta personalizada de forma gratuita en Legacy Central, mientras que en New Central solo puedes configurar rutas personalizadas con un plan Essential o superior. Consulte aquí para detalles de precios.

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 ZeroTier. Consulte aquí para obtener más detalles.



Nota: esta característica requiere que se agreguen reglas de enrutamiento a la red ZeroTier para que surta efecto. Se puede agregar una ruta personalizada de forma gratuita en Legacy Central, mientras que en New Central solo puedes configurar rutas personalizadas con un plan Essential o superior. Consulte aquí para detalles de precios.

12.7 Tailscale

Tailscale es una VPN servicio 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.

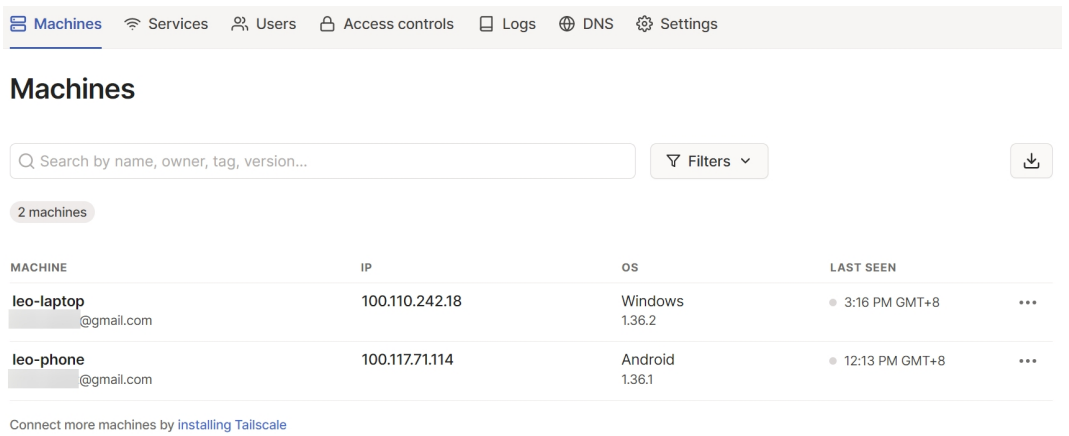
Nota:

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 algunas errores.
3. Los enrutadores GL.iNet aún no están disponibles como nodos de salida.

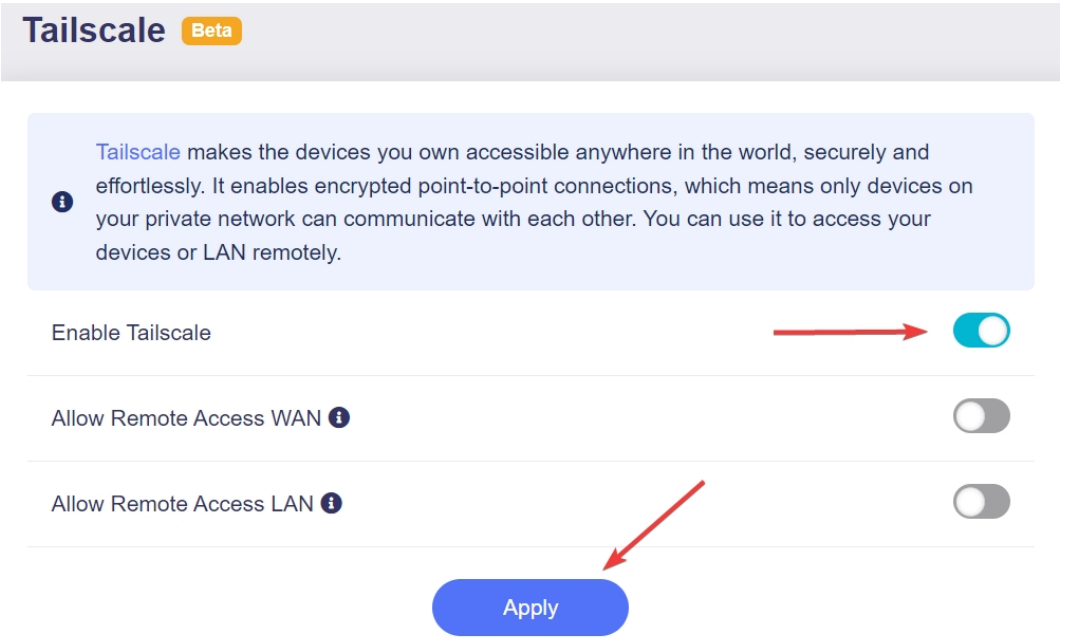
12.7.1 Configurar Tailscale

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

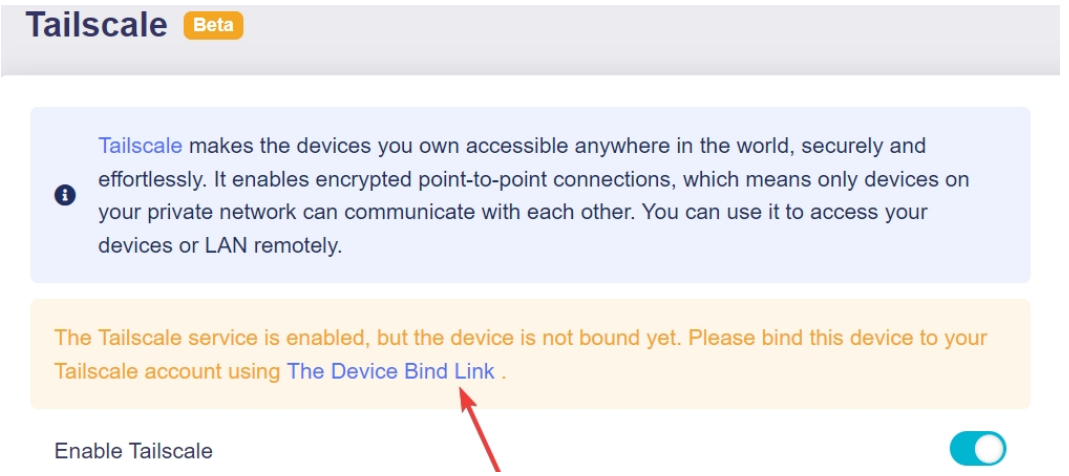
1. Rregistre primero una cuenta de Tailscale y vincule uno o dos dispositivos a su Cuenta Tailscale paracon fines de prueba. Después de vincular, verá sus dispositivos en la plantilla Tailscale C.



2. Inicie sesión en el panel de administración web de su enrutador' y navegue hasta **APLICACIONES** > **Tailscale**. Active **Activar Tailscale** y haga clic en **Aplicar**.



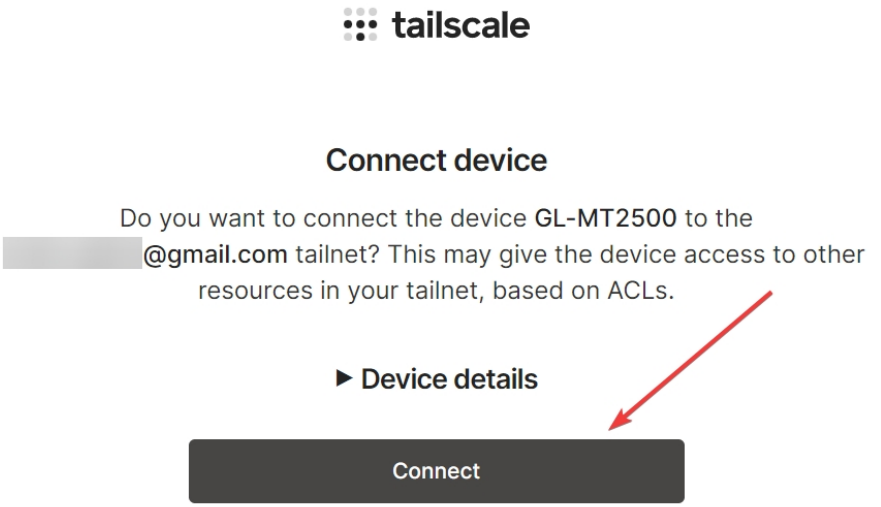
3. La página le pedirá que enlace el dispositivo. Haga clic en **Enlace de enlace del dispositivo**.



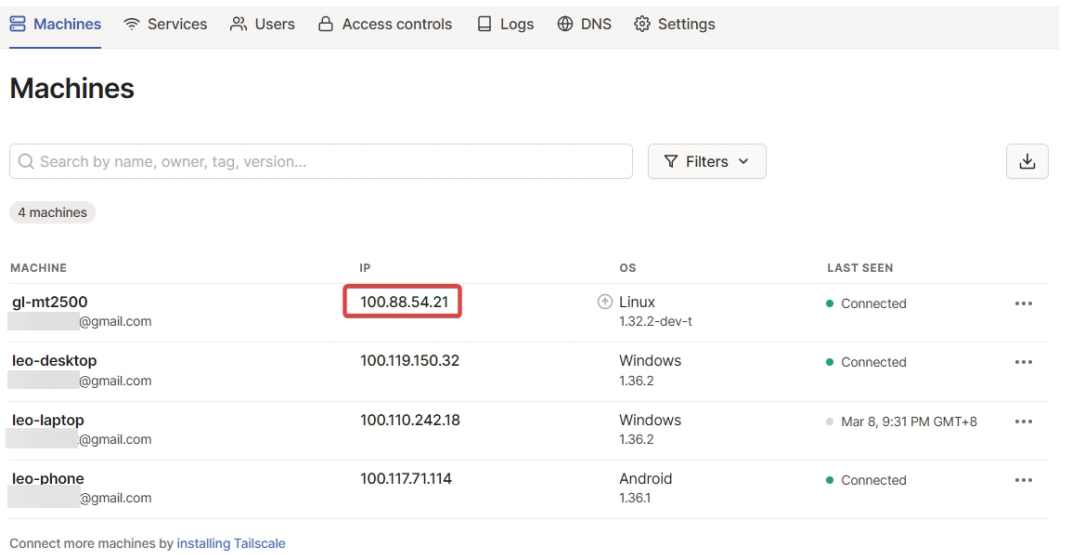
4. En la ventana emergente, haga clic en el enlace e inicie sesión con su cuenta de Tailscale.



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



6. Yserá luego ser redirigido a la 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.



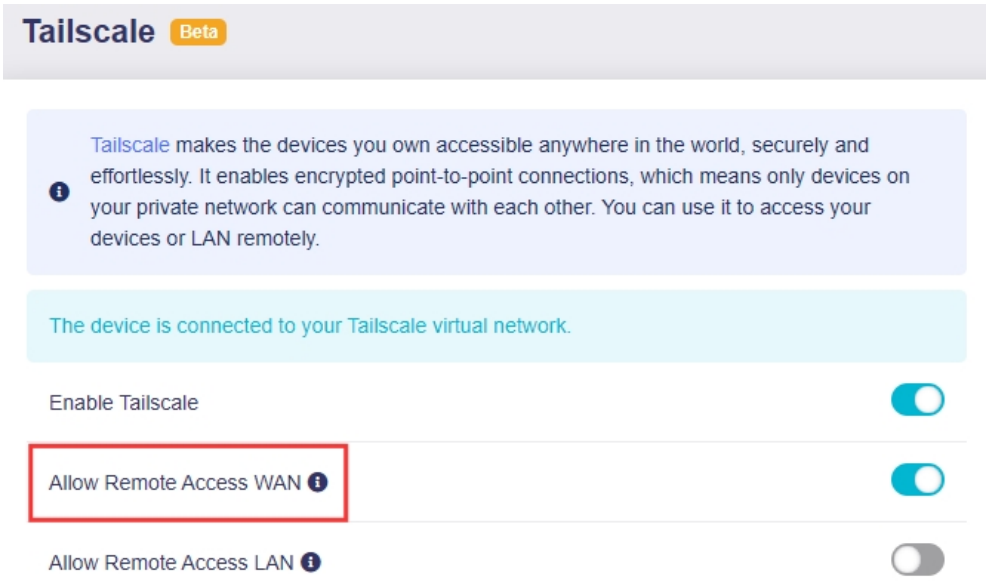
7. Pruebe la conectividad.

   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.

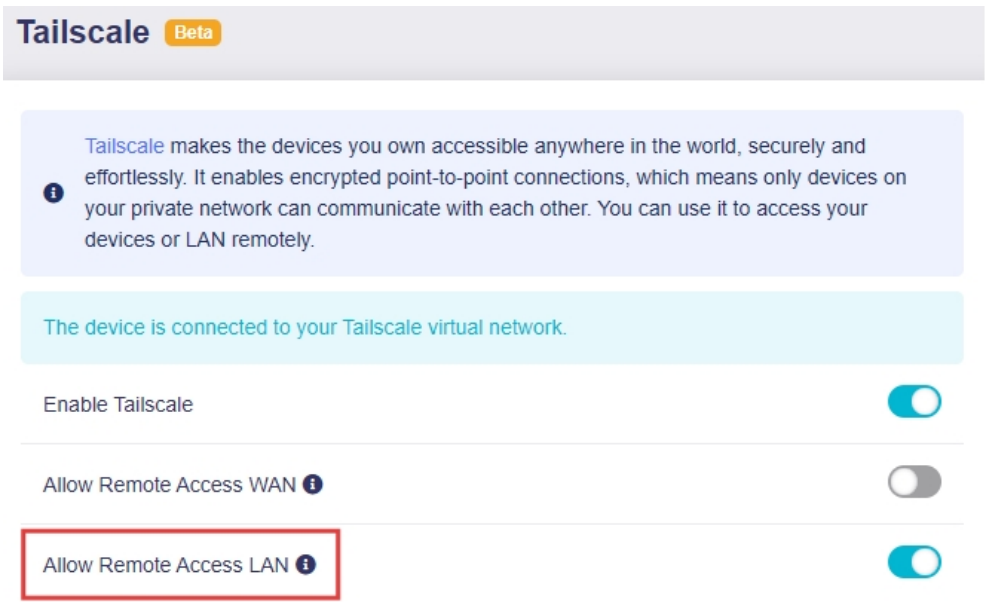
12.7.2 Permitir el acceso remoto a la WAN

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.



12.7.3 Permitir el acceso remoto a la LAN

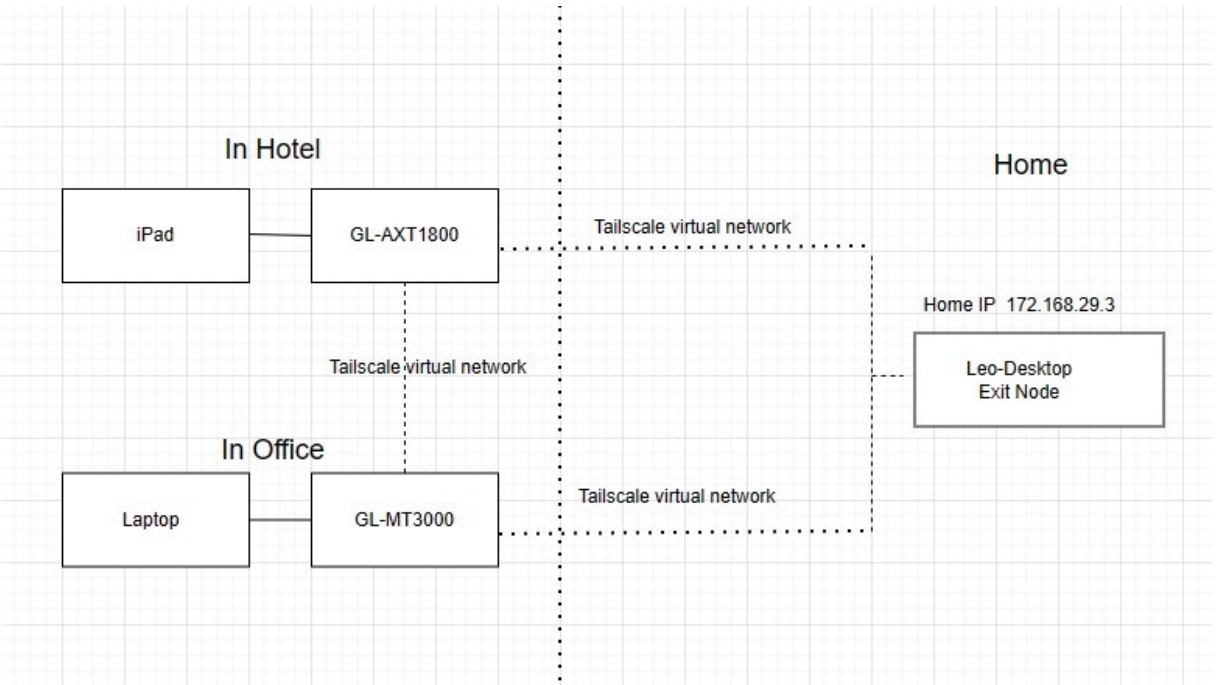
Si esta opción está habilitada, se puede acceder a los recursos en el lado LAN del dispositivo a través de la red virtual Tailscale. Consulte aquí para obtener más detalles.



12.7.4 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 cuando navega 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 una dirección IP privada 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.

Capítulo 13

Red

Este capítulo presenta las configuraciones relacionadas con la red para la configuración y administración, como LAN, DNS e IPv6.

13.1 Reenvío de puertos

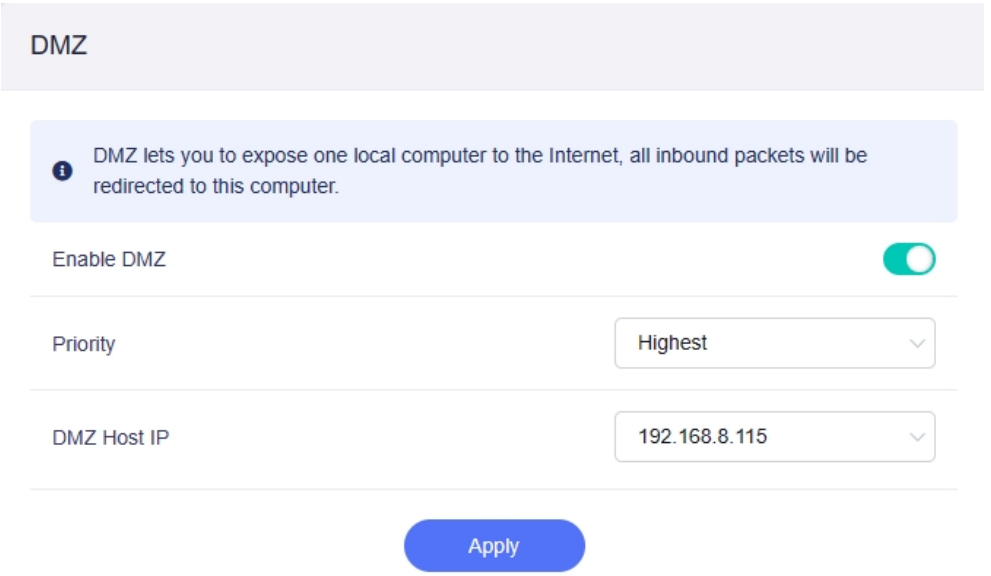
El reenvío de puertos es una función de red que enruta solicitudes externas a dispositivos específicos en su red local. La página de reenvío de puertos incluye dos funciones clave: **DMZ** (para acceso completo directo a un único dispositivo) y **Reenvío de puertos** (para acceso dirigido a puertos específicos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

13.1.1 DMZ

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

Siga los pasos a continuación para habilitar DMZ según sea necesario.

1. Inicie sesión en el panel de administración web de su enrutador' y navegue hasta **RED** > **Reenvío de puertos** > **DMZ** sección.
2. Active **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.

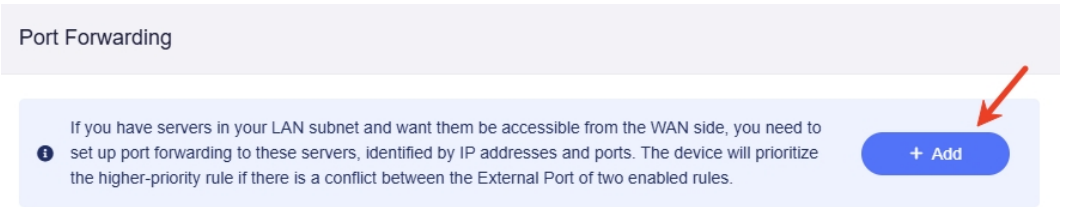
- **IP del host DMZ**: seleccione la dirección IP interna de el dispositivo que recibirá todos los paquetes entrantes.

13.1.2 Reenvío de puertos

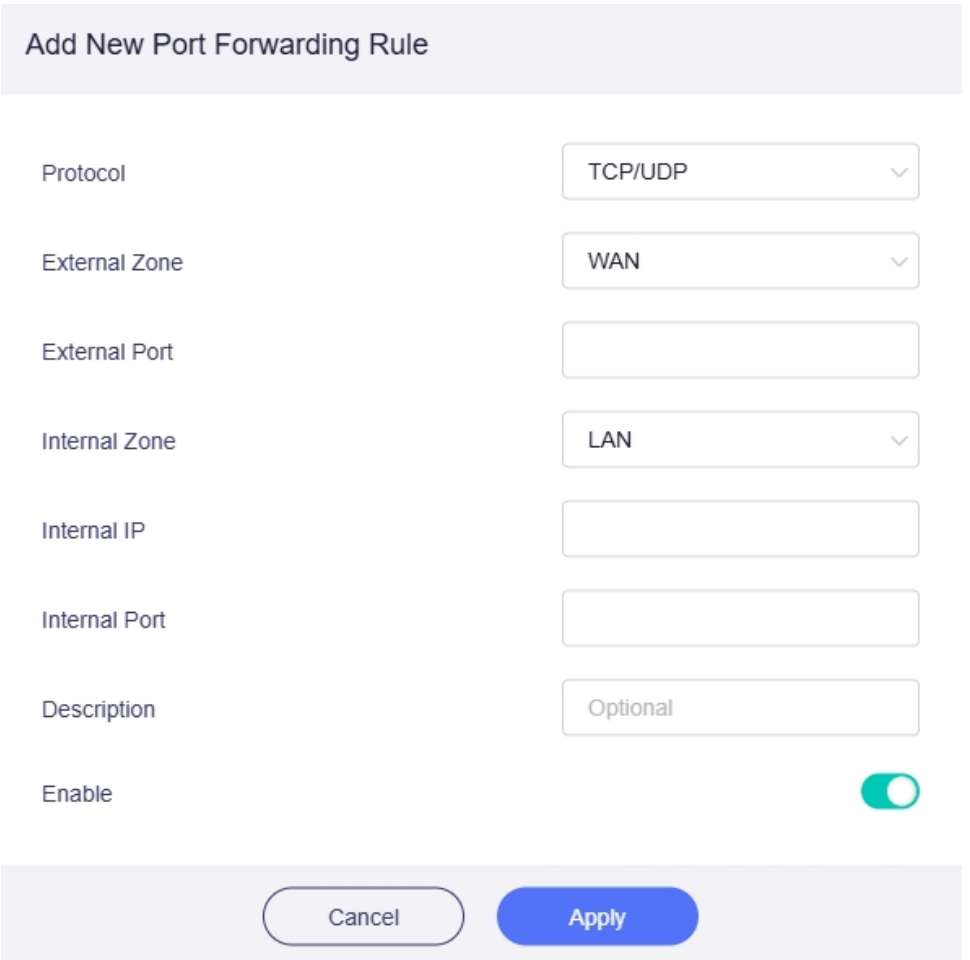
El reenvío de puertos permite que las computadoras remotas se conecten a una computadora o servidor local detrás del firewall de LAN (por ejemplo, servidores web, servidores FTP).

Si necesitaconfigurar 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 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 **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, y LAN.
- **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, WireGuard Client, WireGuard Server, OpenVPN Client, OpenVPN Server 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 falla la conexión principal, 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 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.

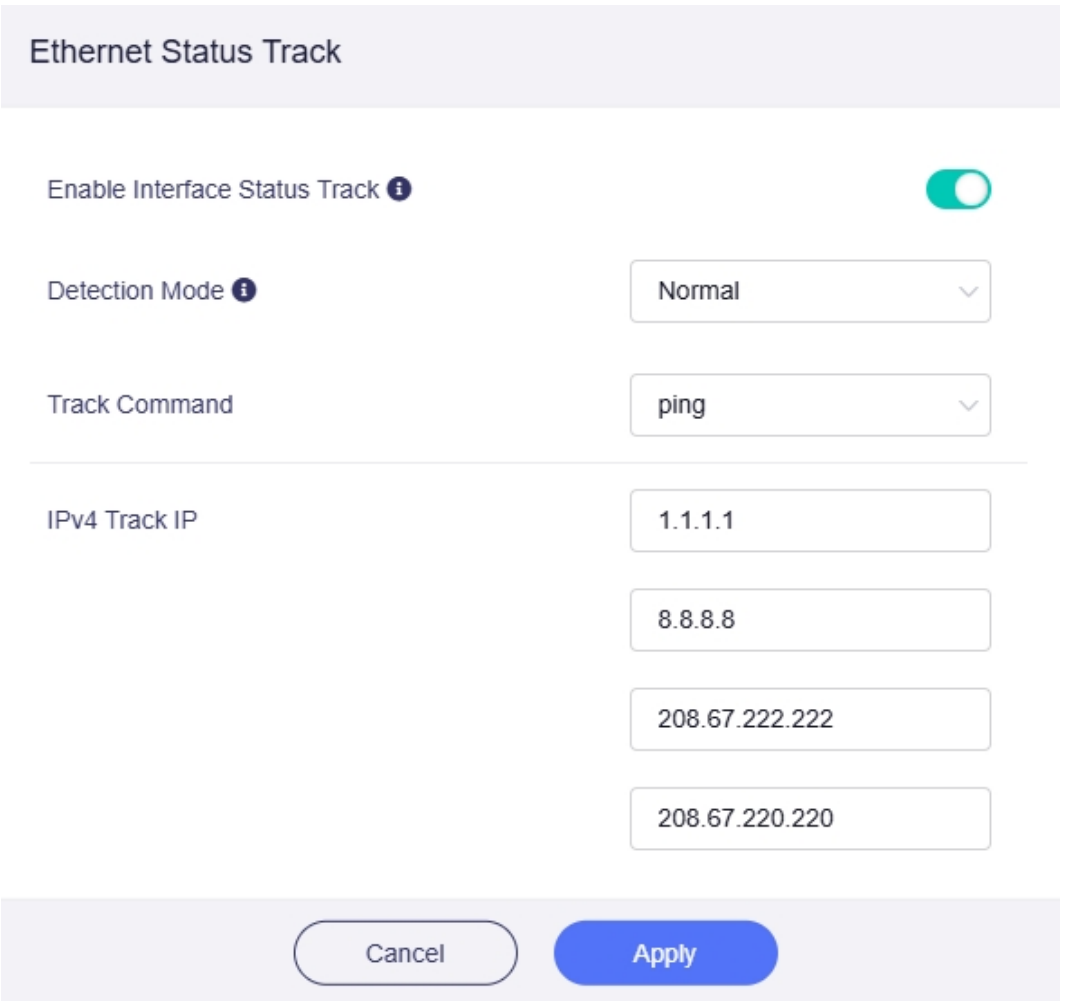
13.2.1 Seguimiento del estado de la interfaz

Brume 2 tiene dos interfaces para la conexión a Internet: Ethernet y Tethering. Es uses 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 en el ícono de ajustes a la derecha para acceder a la configuración de seguimiento del estado para cada interfaz de red.

A continuación se muestran la configuración de seguimiento de estadoing ss para la interfaz Ethernet. La misma lógica de configuración se aplica a la otra interfaz.

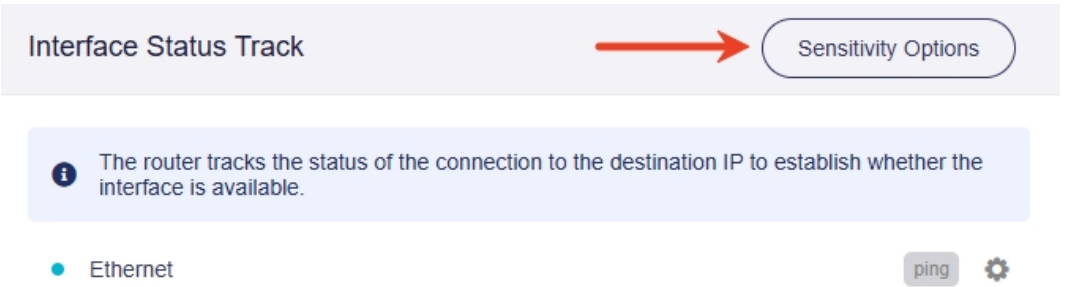


- **Habilitar seguimiento del estado de la interfaz**: Está habilitadode forma predeterminada. Si está deshabilitado, el enrutador determinará el estado de la interfaz según las condiciones (por ejemplo, si el cable Ethernet está enchufado).
- **Modo de detección**: esta característica se introdujo como modo de datos bajos en firmware v4.5, luego cambió el nombre de 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.

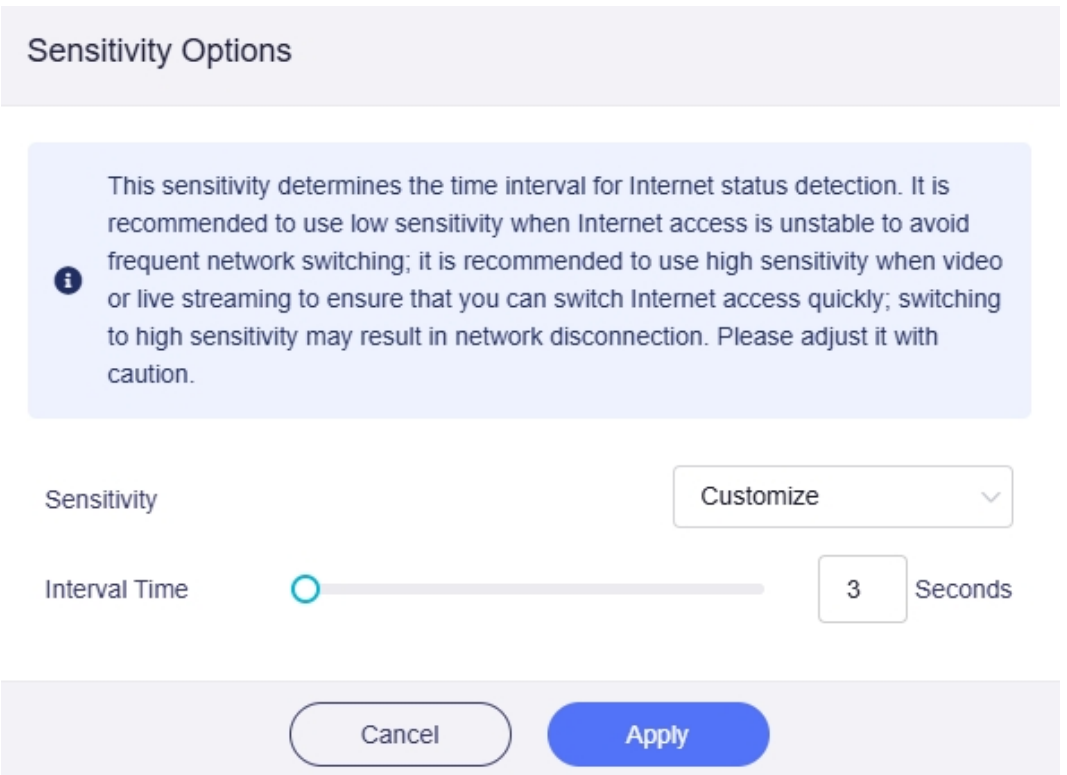
- **Estricto Modo**: Determina el estado de la interfaz exclusivamente en función de los resultados de un comando de detección enviado a una IP pública.

- **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**: Cpersonalizar IPv4 Track IP direcciones según sea necesario.

Haga clic en **Opciones de confidencialidad** 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 intervalo de tiempo ajustable varía de 0,5 segundos a 90 segundos.



Consejos: Si la red es estable, se recomienda una alta sensibilidad para un cambio rápido en caso de desconexión de la red. Esto es adecuado para escenarios como mirar videos, transmitir en vivo o jugar juegos. Si la red es inestable, se recomienda una sensibilidad baja para evitar cambios frecuentes de red y conexiones fallidas. Esto se aplica a escenarios como la descarga de archivos almacenados en caché.

Nota: Cambiar a alta sensibilidad puede provocar desconexiones ocasionales de la red durante el proceso. Ajústelo con precaución.

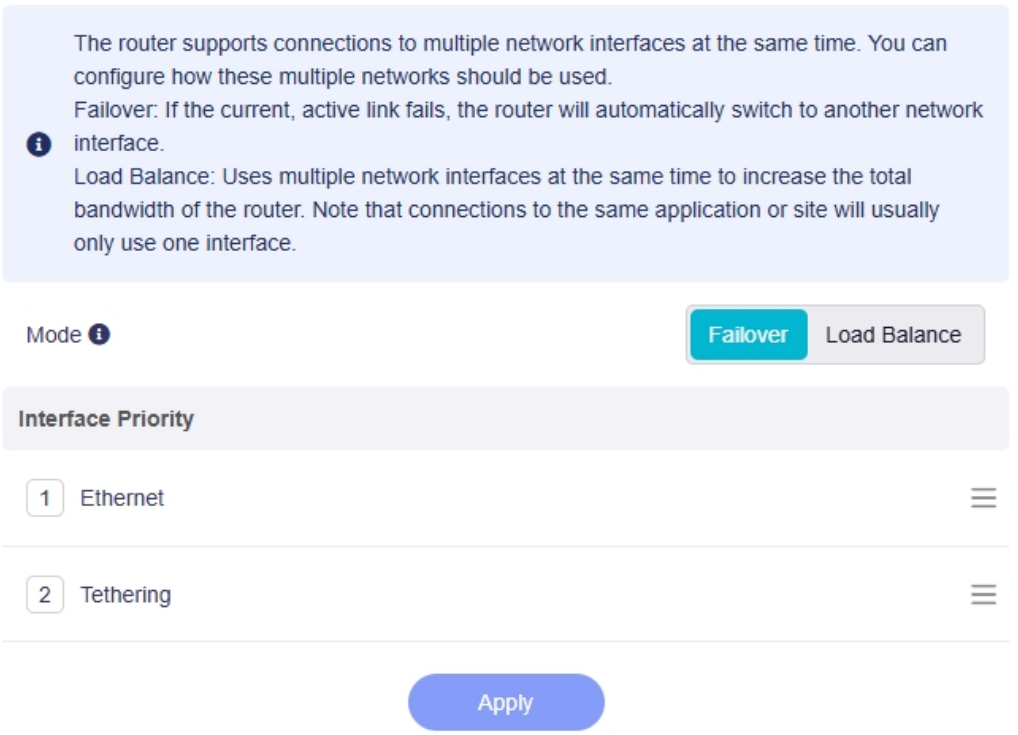
13.2.2 Modo Multi-WAN

Tdos modos disponibles 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 configuran varias conexiones. Si el enlace activo falla, el enrutador cambiará automáticamente a otra interfaz de red para acceder a Internet.

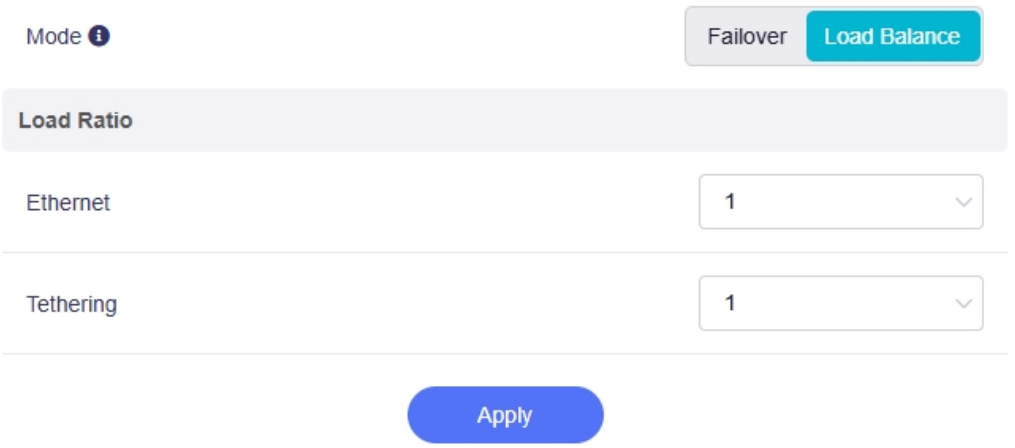
Puede establecer niveles de prioridad para cada interfaz: cuando la interfaz utilizada actualmente falla, el enrutador cambia a la siguiente interfaz disponible con la mayor prioridad. Una vez que se restablece una conexión de mayor prioridad, el enrutador volverá automáticamente al modo.



Equilibrio de carga

Load Balance utiliza múltiples interfaces de red simultáneamente para aumentar el ancho de banda total del enrutador, y el sistema distribuye nuevas conexiones entre interfaces según 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 dos redes (por ejemplo, Ethernet y Tethering) simultáneamente y las dos interfaces están disponibles para acceso a Internet, lo que permite el equilibrio de carga y establece una relación 1:1 significa que las cuatro interfaces compartirán el ancho de banda de la red por igual. El sistema distribuirá nuevas conexiones a través de estas cuatro interfaces de acuerdo con la relación de carga configurada.



Puede personalizar la relación de carga según sea necesario. Por ejemplo, si Ethernetpersonalice la relación de carga según sea necesario. Por ejemplo, si Ethernet tiene un ancho de banda de 100 Mbps, Anclaje tiene 200 Mbps, establezca las relaciones de carga en 1 para Ethernet y 2 para Conexión. Luego, el sistema distribuirá nuevas conexiones a través de las dos interfaces de acuerdo con la proporción 1:2 configurada, lo que significa que Ethernet manejará la mitad de conexiones que Tethering. 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.

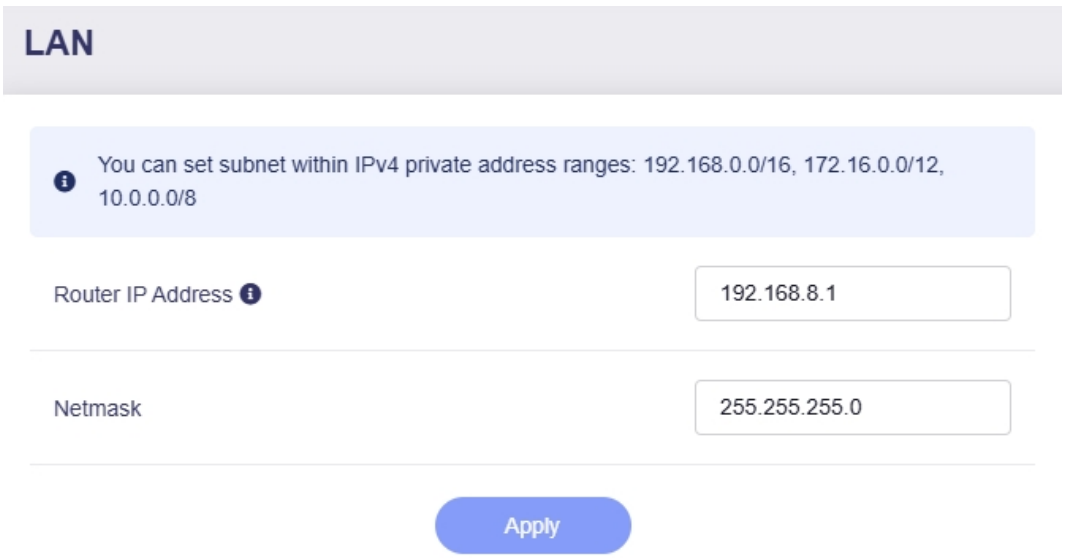
13.3 LAN

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 ajustes básicos, servidor DHCP y reserva de dirección.

13.3.1 Configuración básica

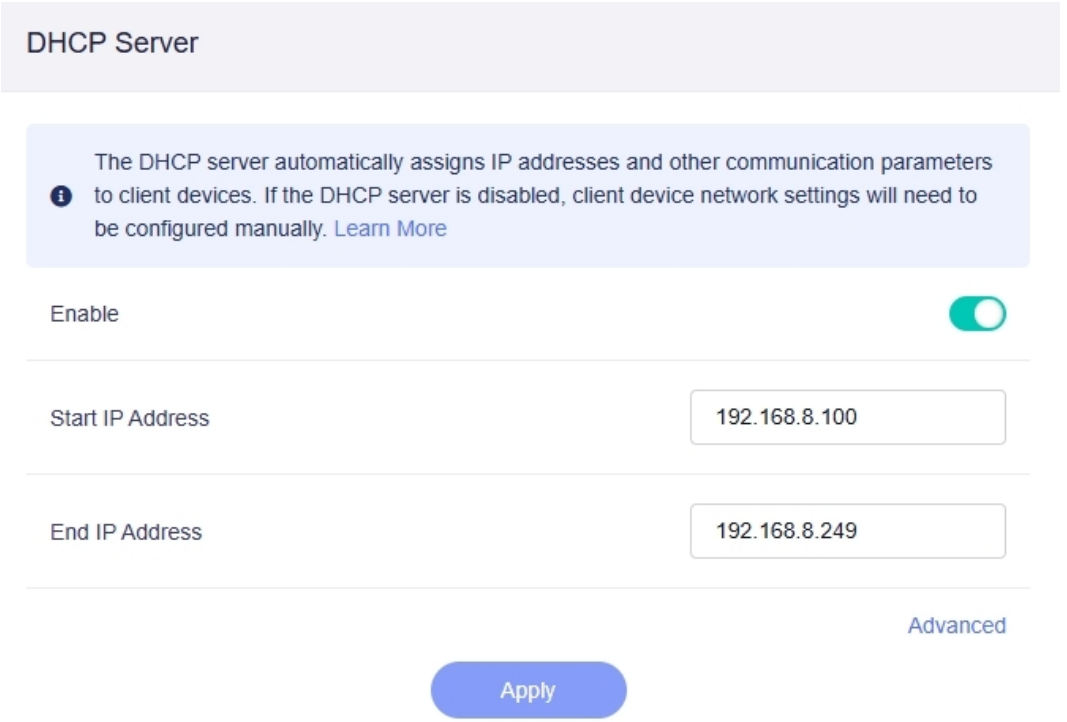
Los ajustes básicos incluyen la dirección IP del enrutador y Máscara de red. Puede configurar la subred dentro de rangos de direcciones privadas IPv4: 192.168.0.0/16, 172.16.0.0/12, 10.0.0.0/8



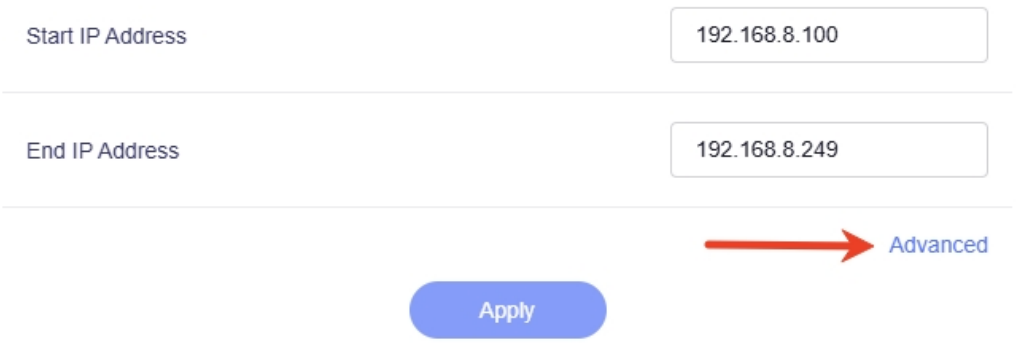
- **Dirección IP del enrutador**: esta es la dirección ingresada en la barra de direcciones de un navegador para acceder al panel de administración del enrutador. Es 192.168.8.1 de forma predeterminada y se puede cambiar si entra en conflicto con la red ascendente.'panel de administración. Es 192.168.8.1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

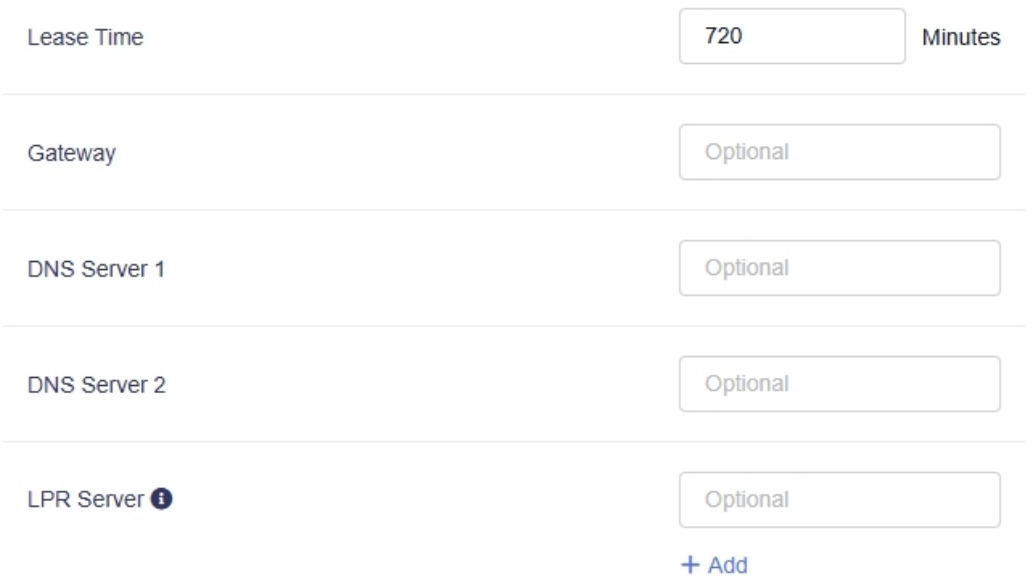
El servidor DHCP asigna automáticamente direcciones IP y otros parámetros de comunicación a cada cliente conectado. Enrutador GL.iNet' está habilitado de forma predeterminada y el grupo de direcciones IP del servidor DHCP' varía de 192.168.8.100 a 192.168.8.249. Puede personalizar el rango de direcciones según sea 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.

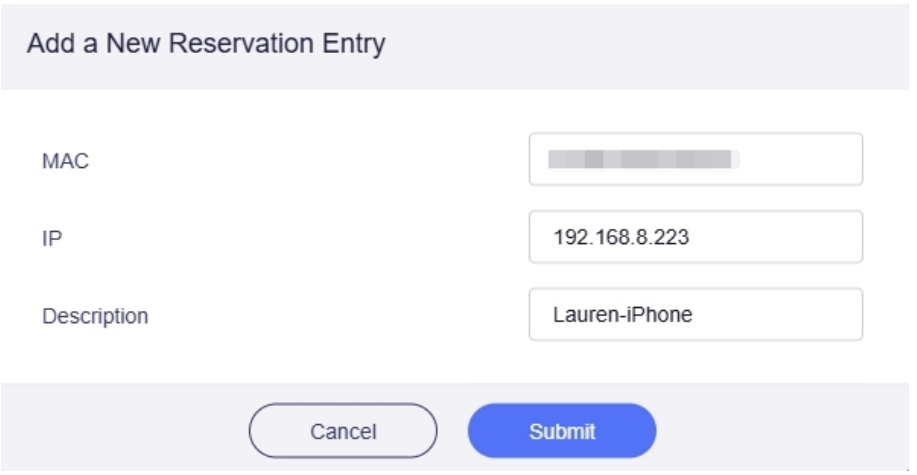
Nota: Si el servidor DHCP está deshabilitado, deberá configurar manualmente la IP estática y otros parámetros de comunicación para cada cliente. Consulte aquí para obtener más detalles.

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 configuración IP permanente. Tenga en cuenta que los clientescon 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 según sea necesario.

1. Registro ingrese al 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 lala correspondiente IP dirección para la MAC seleccionada se completará automáticamente. 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.

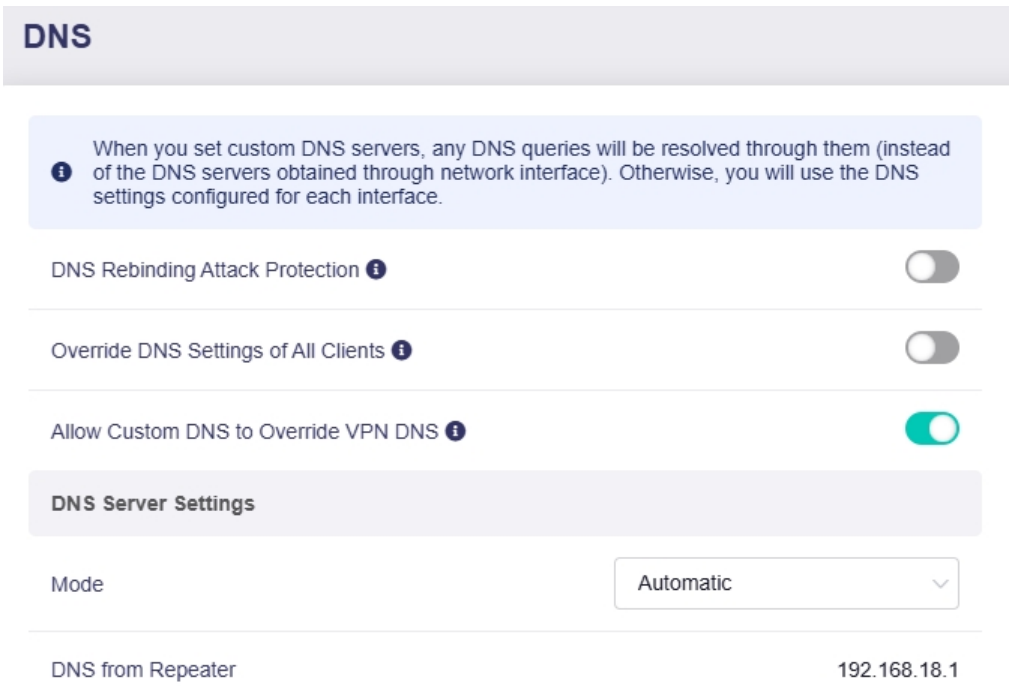


13.4 DNS

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 del nombre de dominio a IP para todos los conectados dispositivos. 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 redo mejorar la seguridad. Una vez configurados, todos los dispositivos conectados utilizarán este servidor DNS unificado de forma predeterminada, lo que elimina la necesidad de una configuración DNS independiente en cada dispositivo.

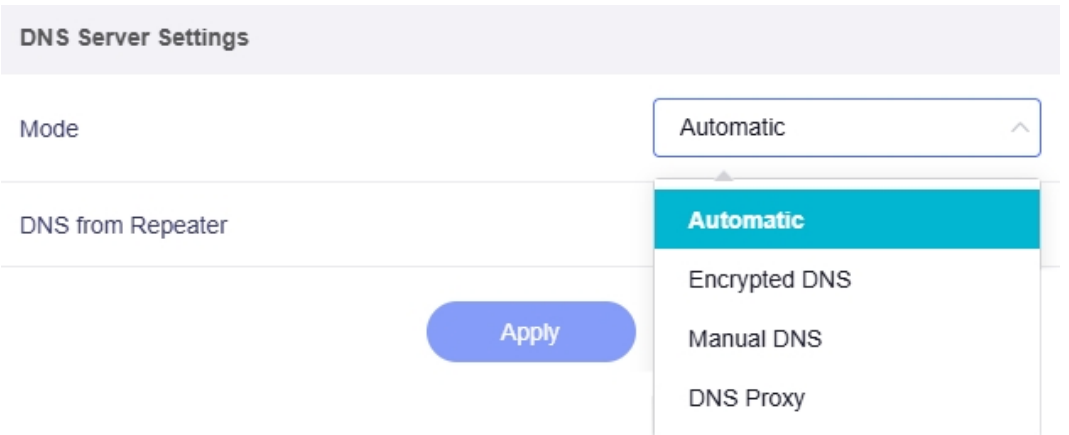
Inicie sesión en el panel de administración web de su enrutador y navegue hasta **RED** > **DNS**. Esta página le permite configurar ajustes relacionados con DNS, incluidas opciones de seguridad, modos de servidor y reglas de prioridad de DNS para diferentes escenarios de red.



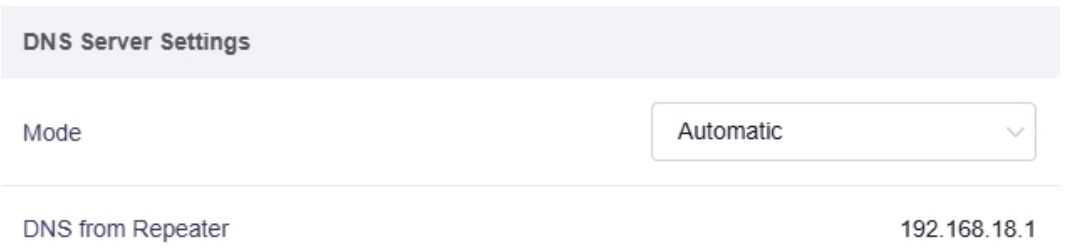
- **Protección contra ataques de revinculación de DNS**: protege contra ataques de revinculación de DNS bloqueando intentos maliciosos de resolución de DNS. Tenga en cuenta que habilitarlo puede provocar un error en la búsqueda de DNS privado.
- **Anular la configuración de DNS de todos los clientes**: Si está habilitado, todos los dispositivoss será forzado a utilizar los servidores DNS configurados en el enrutador, ignorando su propia configuración DNS original. 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.

13.4.1 Configuración del servidor DNS

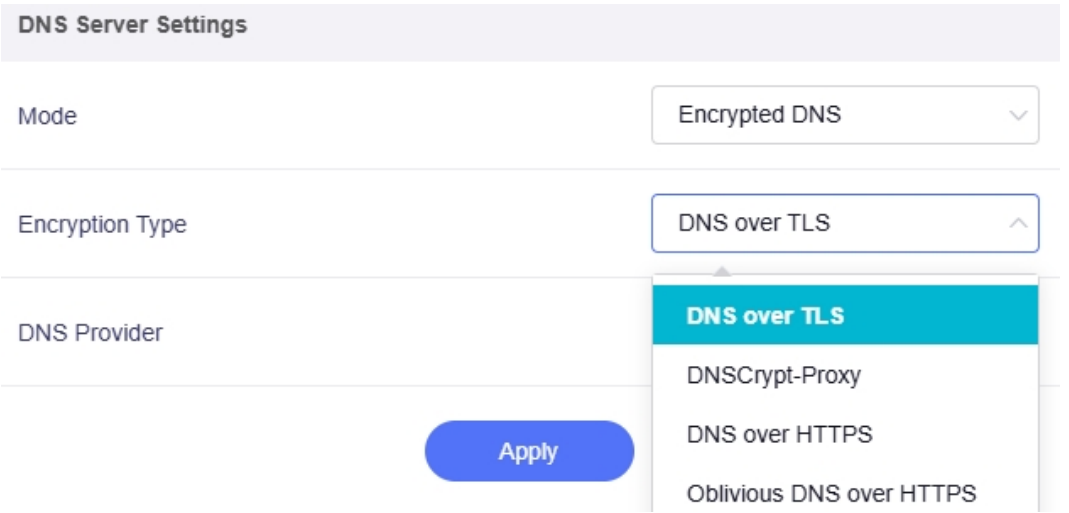
Hay cuatro modos para el servidor DNS: Automático, DNS cifrado, DNS manual y Proxy DNS.



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.

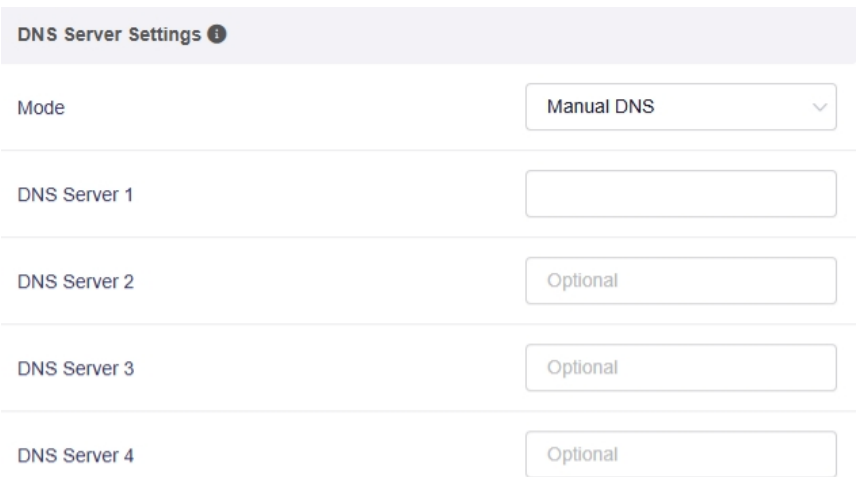


2. **DNS cifrado**: cuando se selecciona, el enrutador utilizará protocolos cifrados para procesar consultas DNS, protegiendo los datos de resolución contra escuchas o alteraciones.
   Tiene cuatro tipos de cifrado: DNS sobre TLS, DNSCrypt-Proxy, DNS sobre HTTPS y DNS ajeno a través de HTTPS.



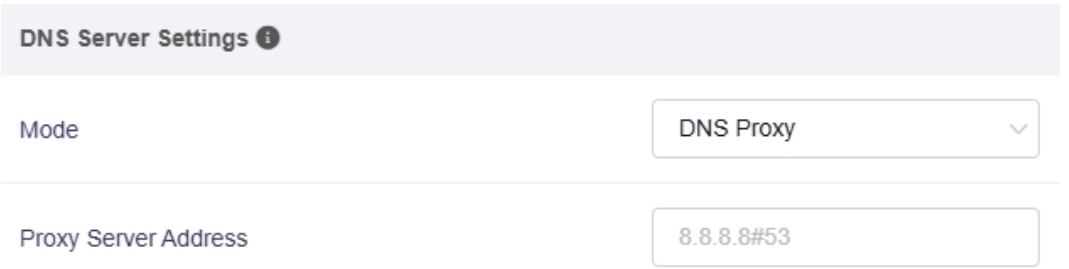
   - Para DNS sobre TLS, seleccione un proveedor de DNS entre Control D, NextDNS y Cloudflare.
   - Para los otros tres (es decir, DNSCrypt-Proxy, DNS sobre HTTPS y DNS ajeno a HTTPS), seleccione al menos un servidor DNS del repositorio. Se pueden seleccionar hasta 8 servidores. Cuando se seleccionan varios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

3. **DNS manual**: cuando lo 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 usar direcciones IPv6 para DNS manual, habilite IPv6 en su enrutador primero.

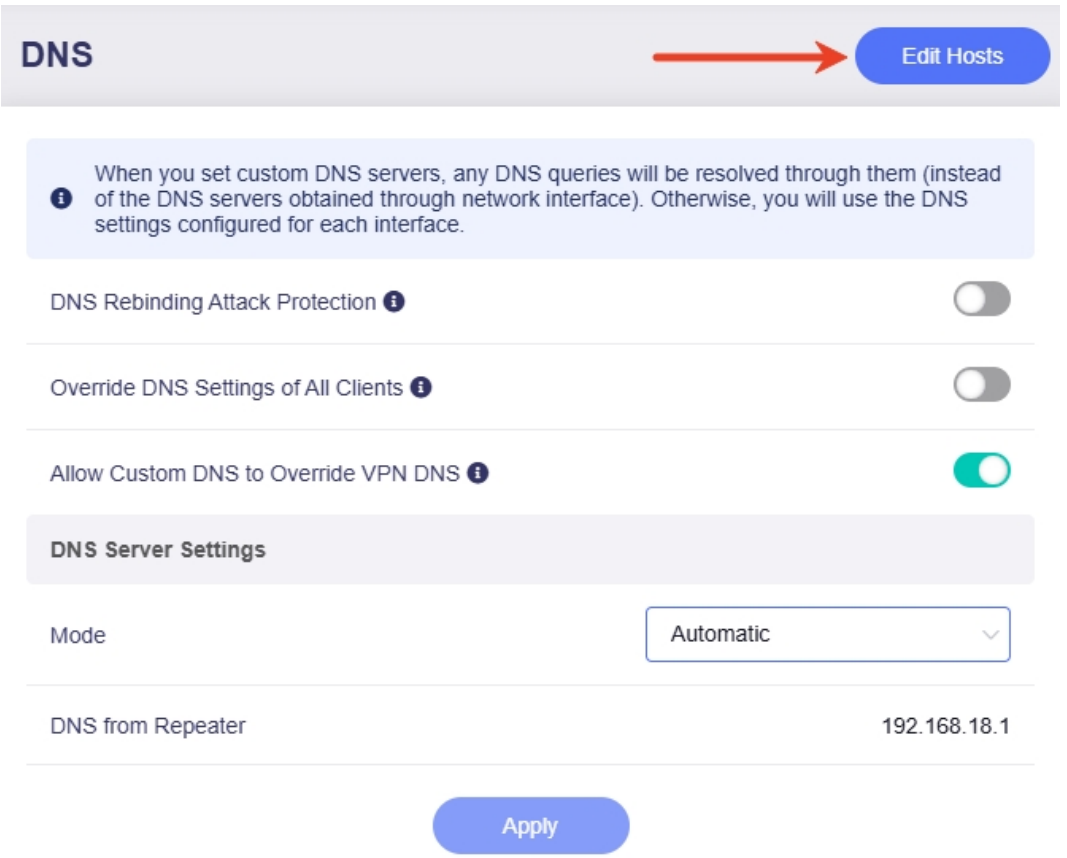
4. **Proxy DNS**: cuando se selecciona, el enrutador reenvía todas las consultas DNS a través de servidor proxy, permitela resolución a través del entorno de red del proxy para necesidades de acceso específicas.



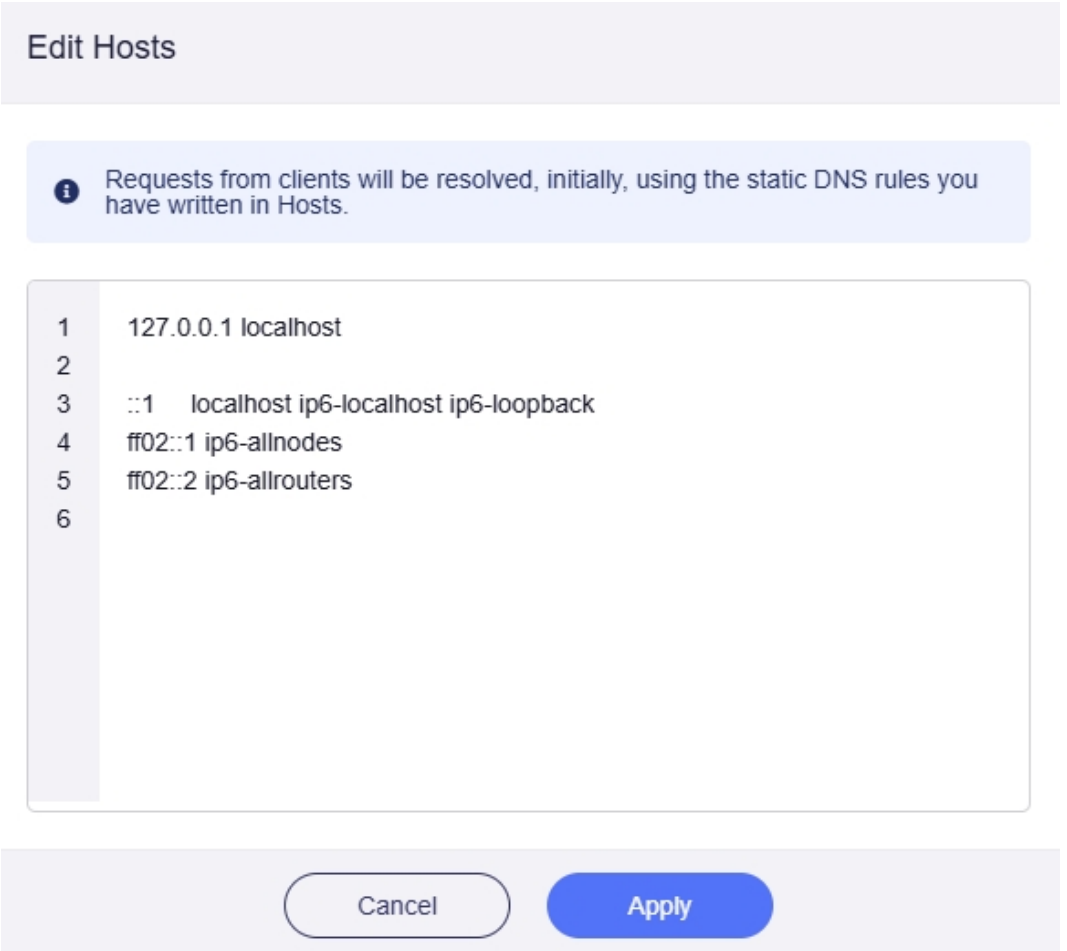
13.4.2 Editar hosts

Puede definir reglas de resolución de DNS estáticas como necesario.

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



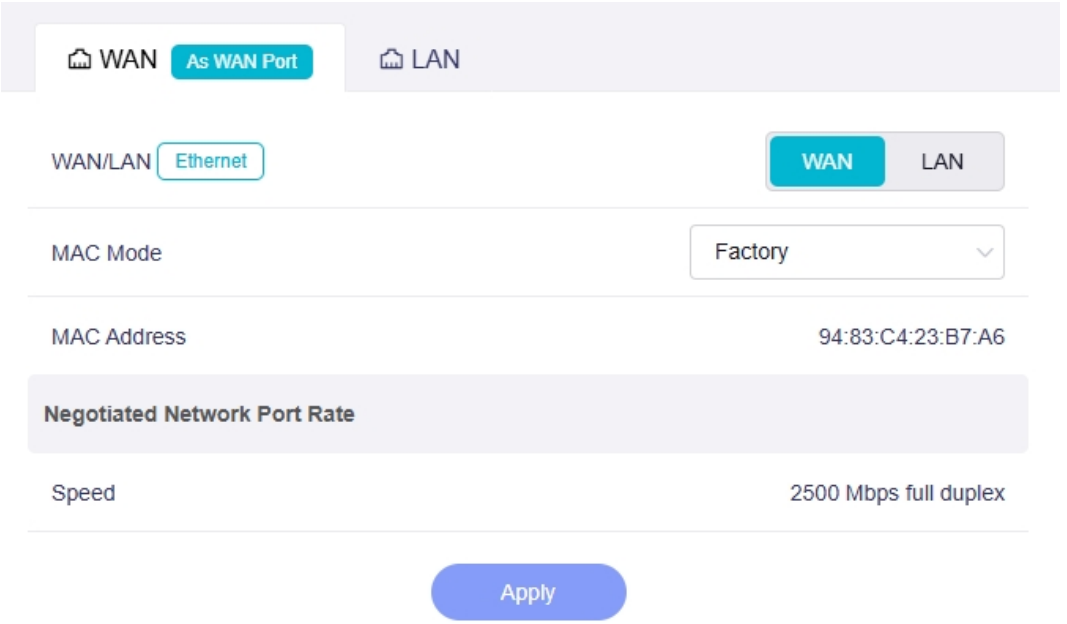
Las solicitudes de los clientes se resolverán preferentemente utilizando las reglas de DNS estáticas escritas aquí, lo que le permitirá asignar manualmente direcciones IP a nombres de host. (por ejemplo, las entradas predeterminadas como 127.0.0.1 localhost para loopback local) para un control personalizado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



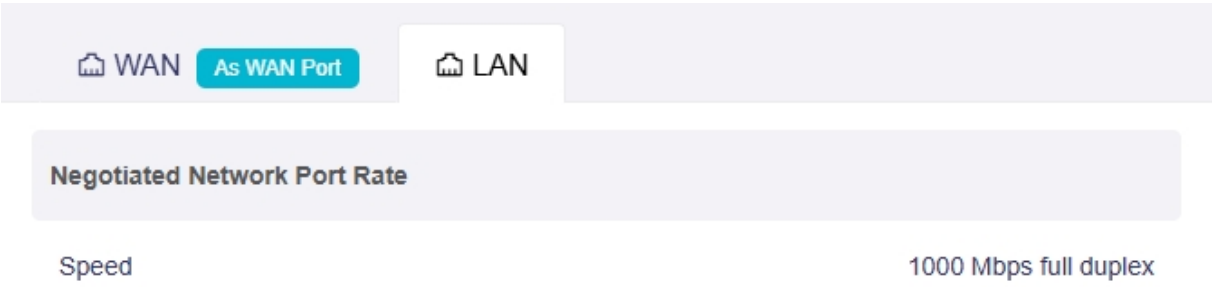
13.5 Gestión de puertos

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

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



La sección **LAN** muestra el puerto LAN negociado tarifa.

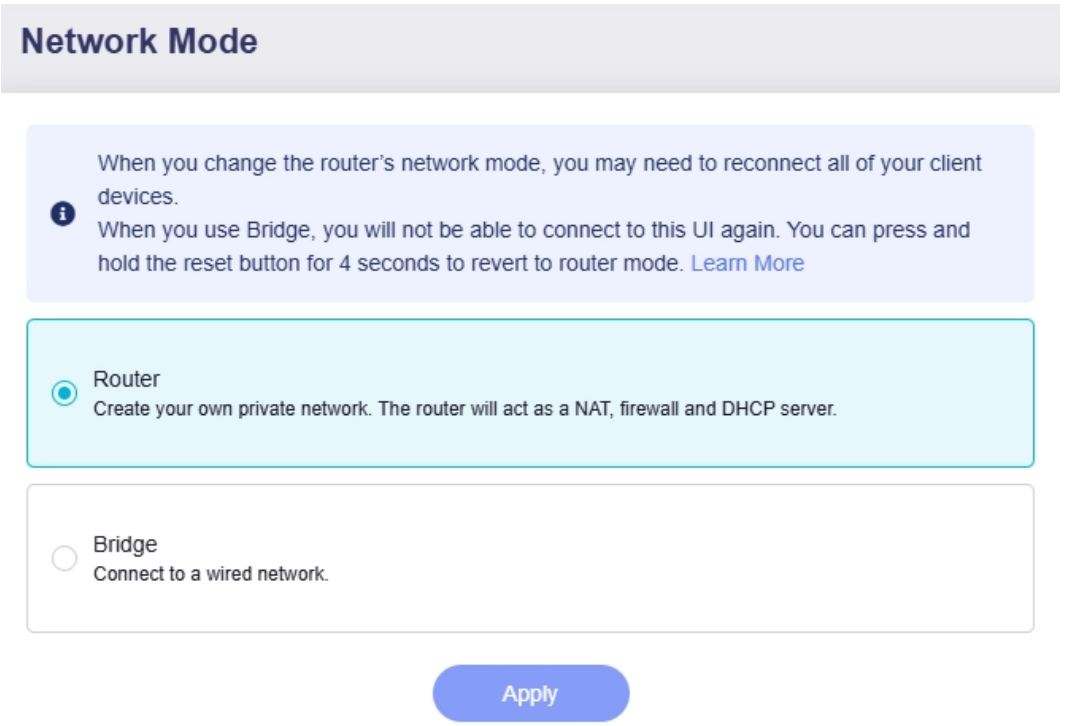


Nota: La tarifa negociada para los puertos WAN y LAN se muestra solo cuando hay un cable Ethernet conectado. Depende tanto del puerto Ethernet como del cable Ethernet.

13.6 Modo de red

El modo de red se refiere a los diferentes roles operativos y funcionalidades 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. Brume 2 soportas dos modos: enrutador y modo puente.



- **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.
- **Bridge**: permite que el enrutador se conecte a una red cableada y funcione como puente entre dispositivos de red. En este modo, el enrutador funciona esencialmente como un conmutador, reenviando datos entre dispositivos conectados sin realizar servicios NAT,

firewall o DHCP. Esto permite una comunicación fluida entre dispositivos en la misma red al actuar como un simple punto de conexión en lugar de una puerta de enlace de red.

Nota:

1. Cuando se cambia el modo de red , dispositivos necesita volver a conectarse al enrutador para garantizar una conexión estable.
2. **En modo puente, no podrá para acceder al panel de administración web usando 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 Puente, las siguientes funciones no estarán disponibles**: Control de acceso (listas permitidas y listas de bloqueo), AstroWarp, VPN, Tor, AdGuard Home, control parental, ZeroTier, Tailscale, reenvío de puertos, Multi-WAN, servidor DHCP, reserva de direcciones, DNS, administración de puertos, IPv6, puerta de enlace directa, vigilancia IGMP, aceleración de red, configuración NAT.

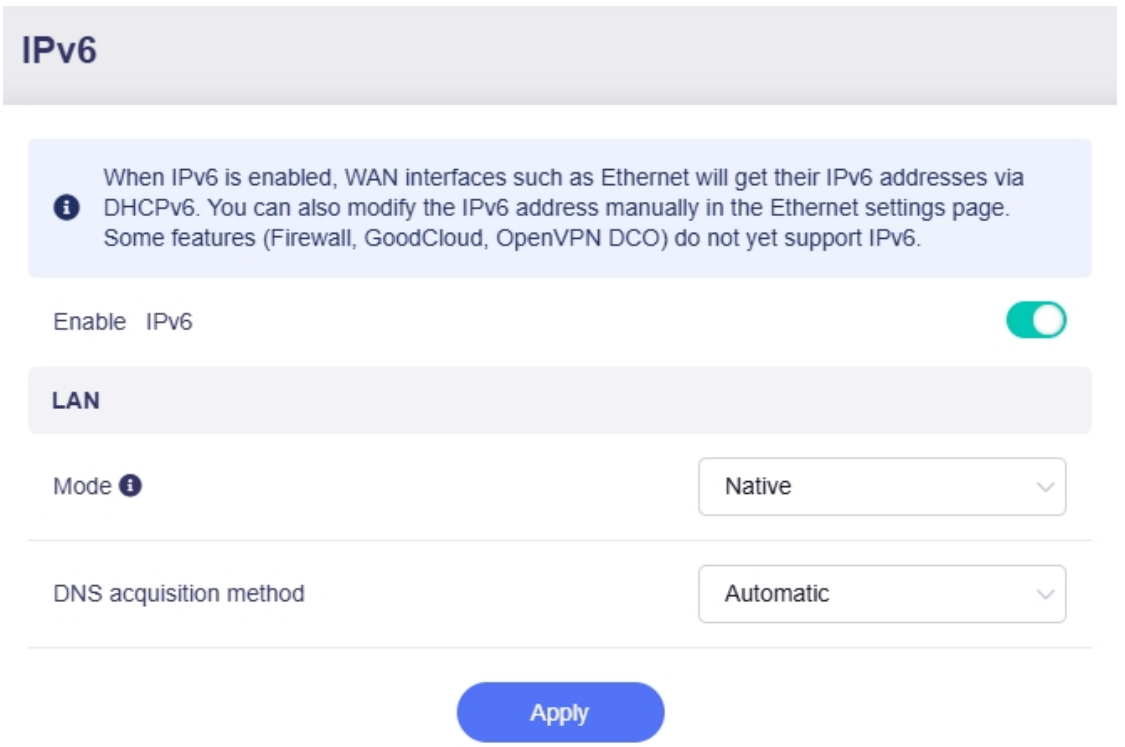
13.7 IPv6

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**. Estaesta 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.

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

Alternar en **Eactivar IPv6**, seleccione el modo para su red principal y el método de adquisición de DNS, luego haga clic en **Aplicar.**



13.7.1 Modo IPv6

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

- **Nativo**: este modo es aplicable cuando el enrutador obtiene directamente un público IPv6 dirección 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 es aplicable cuando los paquetes IPv6 deben pasar directamente sin ningún procesamiento o conversión. Por ejemplo, algunos específico 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 adecuadoadecuado 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.

13.7.2 Método de obtención de DNS

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

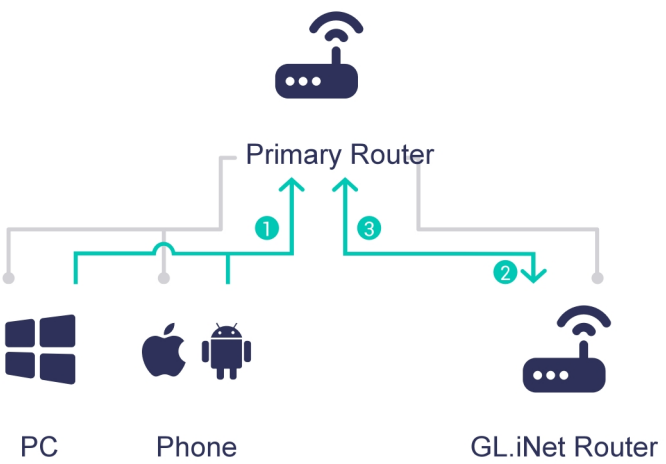
- **Automático**: el enrutador obtendrá direcciones de servidor DNS IPv6 dinámicamente (por ejemplo, a través de DHCPv6).
- **Manual**: Ingrese direcciones de servidor DNS IPv6 personalizadas. Sin embargo, dado que DNS se utiliza para resolver nombres de dominio en sus direcciones IP correspondientes,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

13.8 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 opera 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 según sea 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.

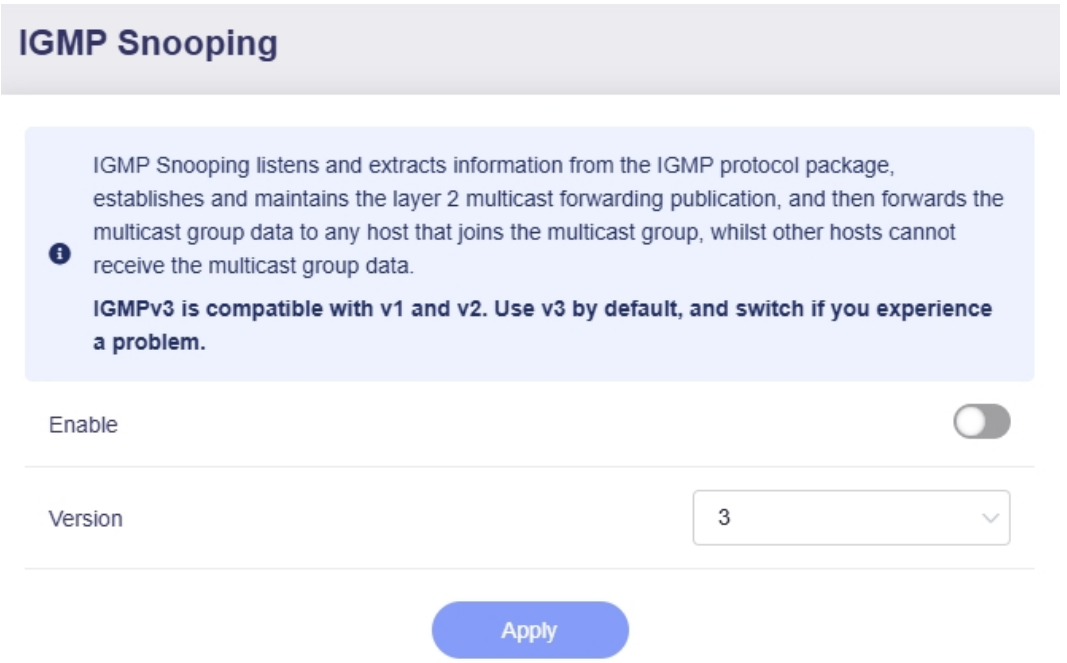
- **Glíneas verdes** representan la ruta de transmisión de datos secuencial cuando Drop-in Gateway está activo, con las flechas numeradas que indican el orden del flujo de tráfico:
  1. El tráfico de los dispositivos cliente se enruta primero al enrutador principal;
  2. El enrutador principal reenvía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

Puedes habilitar Drop-in Gateway para todos o dispositivos específicos conectados a su enrutador principal. Consulte este enlace para obtener más instrucciones.

13.9 Inspección IGMP

IGMP Snooping escucha el paquete de protocolo IGMP, extrae la información correspondiente, 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.

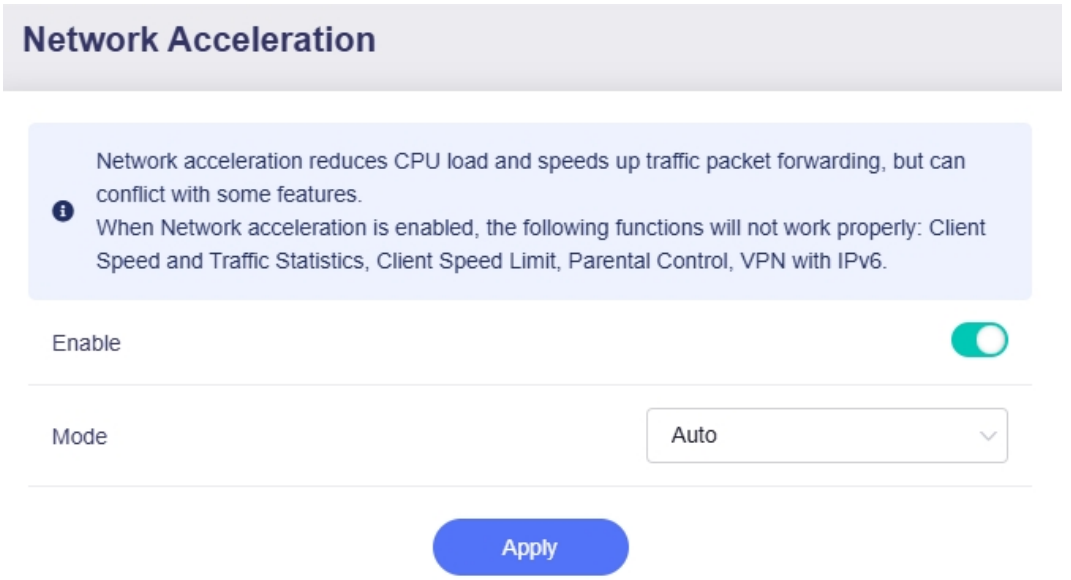
Registro acceda al panel de administración web de su enrutador' y navegue hasta **RED** > **Inspección IGMP**. Puede habilitarlo para usar la función de multidifusión en su enrutador según sea necesario.



13.10 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 de aceleración entre Automático, Aceleración de hardware y Aceleración de software.

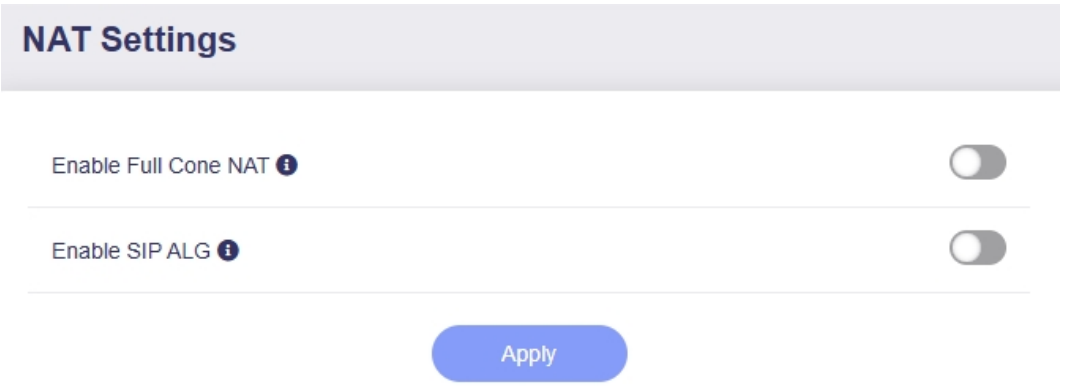


- **Auto**: cambia automáticamente entre los dos modos de aceleración según el uso real.
- **Aceleración de hardware**: descarga tareas de red de alta frecuencia (por ejemplo, NAT, reenvío de paquetes, verificación de suma de comprobación) a hardware dedicado como NPU o chips HWNAT. Funciona específicamente en conexiones Ethernet (WAN/LAN por cable) y repetidor (no disponible en Brume 2), 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.
- **Aceleración de software**: depende de la CPU general de un enrutador emparejada con núcleos o controladores optimizados (por ejemplo, SWNAT). Funciona en una conexión celular (4G/5G), normalmente el escenario principal donde la aceleración de hardware no está disponible, y ofrece una gran compatibilidad y soporte para protocolos complejos. Si bien es flexible, puede afectar los cuellos de botella de la CPU bajo cargas de gran ancho de banda, especialmente cuando se ejecutan funciones avanzadas como QoS o reenvío de puertos.

Nota: Cuando la aceleración de red está habilitada, las siguientes funciones no funcionarán correctamente: Estadísticas de velocidad del cliente, Estadísticas de tráfico, Límite de velocidad, Control parental, VPN con IPv6, Estadísticas de datos, Filtro de contenido, QoS y SQM.

13.11 Configuración NAT

Inicie sesión en el panel de administración web de su enrutador' y navegue hasta **RED** > **Configuración NAT**. Esta página le permite configurar dos funciones clave relacionadas con NAT: NAT de cono completo y SIP ALG.



- **NAT de cono completo**: se puede utilizar para reducir latencia del juego, mejorando la capacidad de respuesta de los juegos en línea. Sin embargo, habilitar NAT de cono completo puede ser menos seguro ya que permite conexiones entrantes sin restricciones.
- **ALG SIP**: está destinado a mitigar los efectos de múltiples NAT en SIP (Protocolo de inicio de sesión) tráfico. Sin embargo, en la mayoría de los casos, no ayudará e incluso puede afectar las llamadas VoIP, causando problemas como audio unidireccional, teléfonos que no suenan, caídas inesperadas de llamadas o llamadas que van directamente al correo de voz.

Capítulo 14

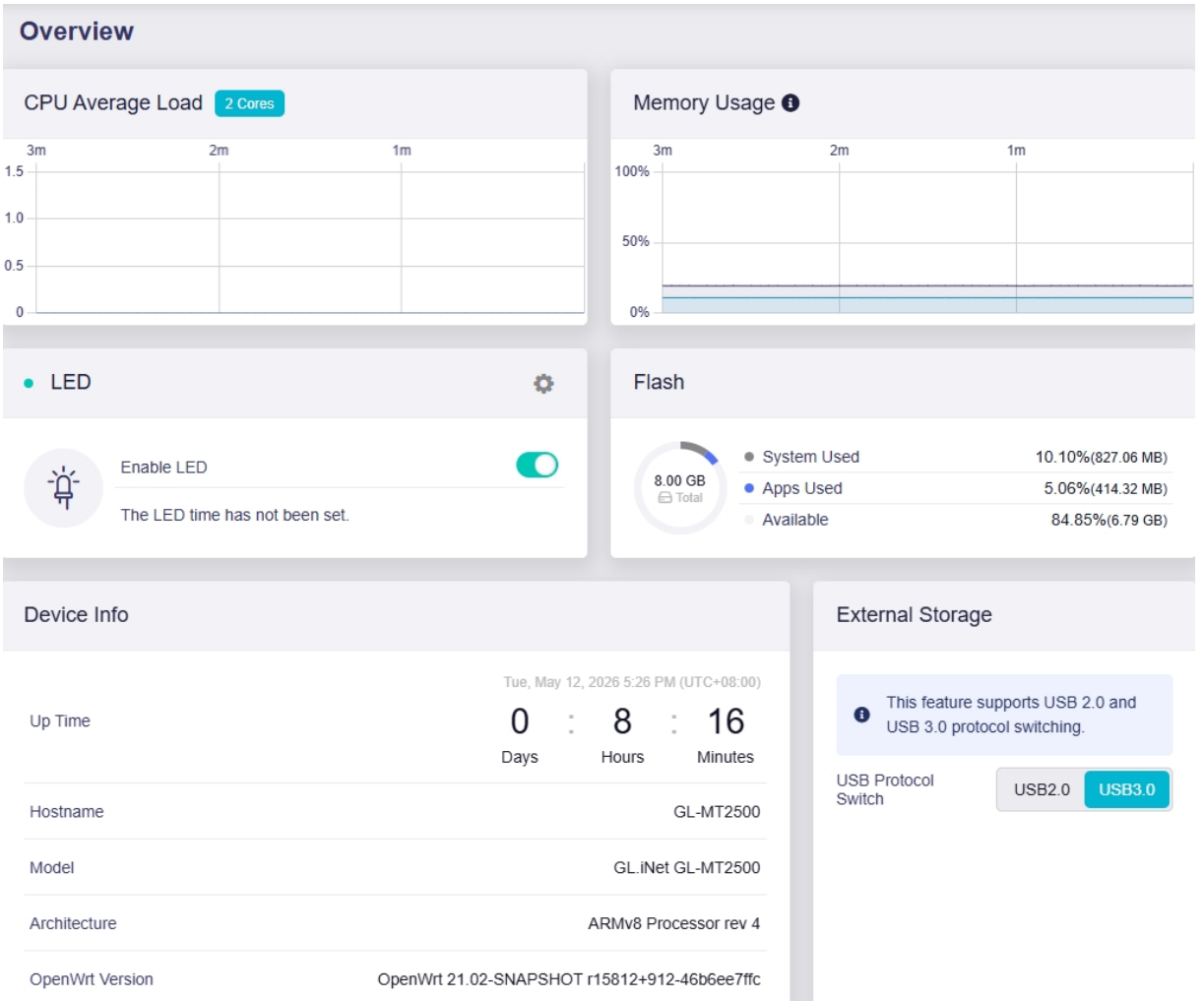
Sistema

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

14.1 Descripción general

Inicie sesión en el administrador 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

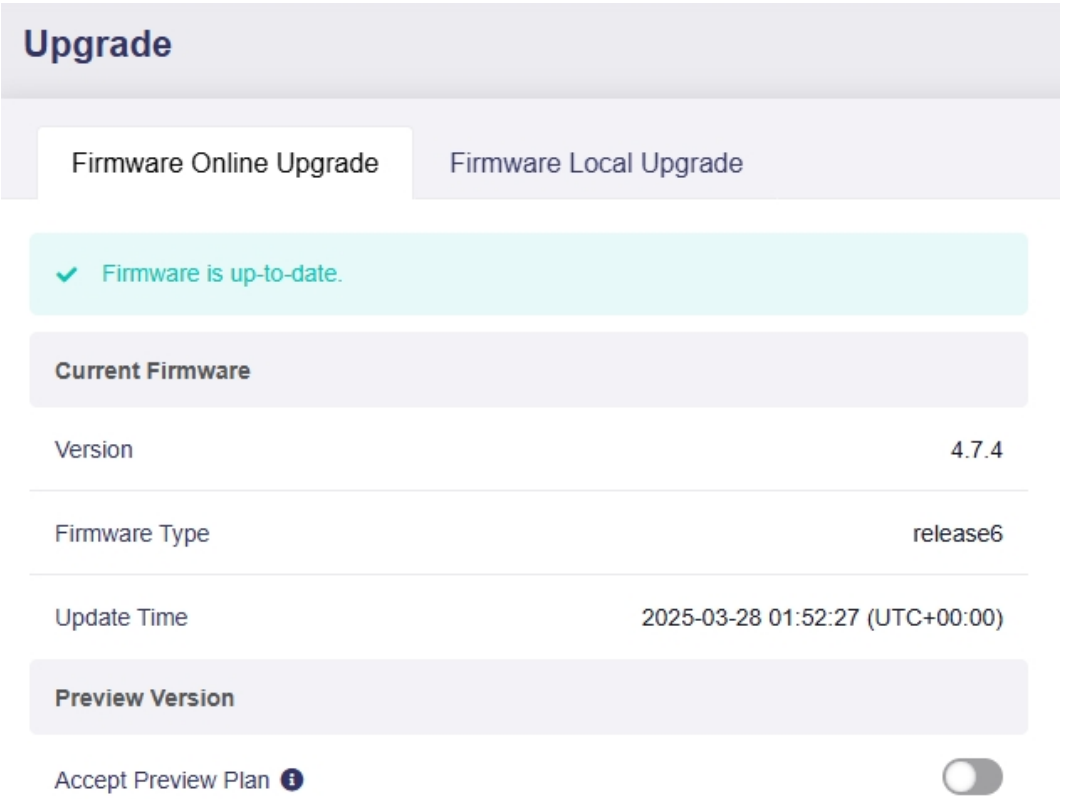


14.2 Actualización

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

14.2.1 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 publique la versión final. y envíenos sus comentarios. Configúrelo una vez y permanecerá encendido. Tenga en cuenta que es posible que estas actualizaciones no sean estables.

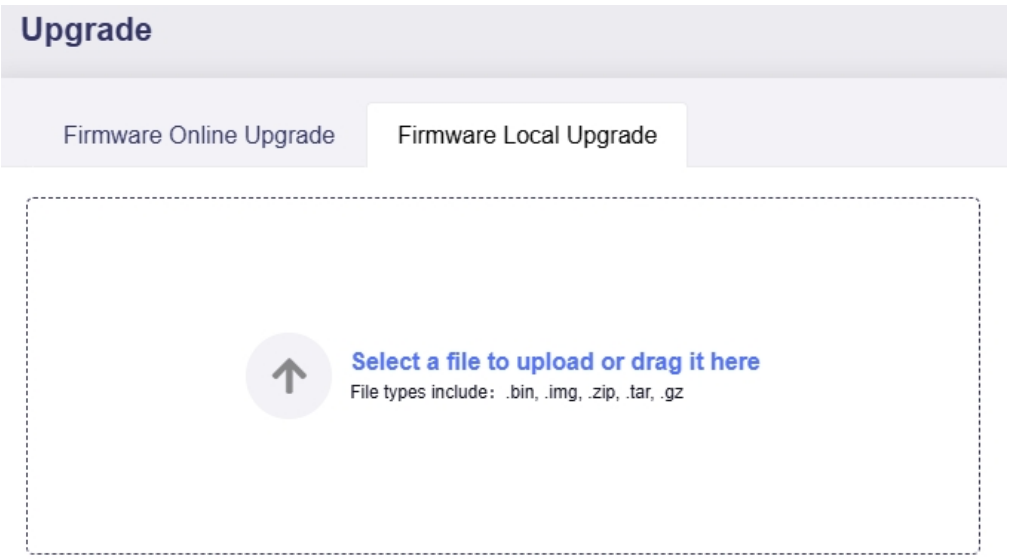
Si su enrutador está conectado a Internet, buscará la versión de firmware más reciente disponible para descargar.

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

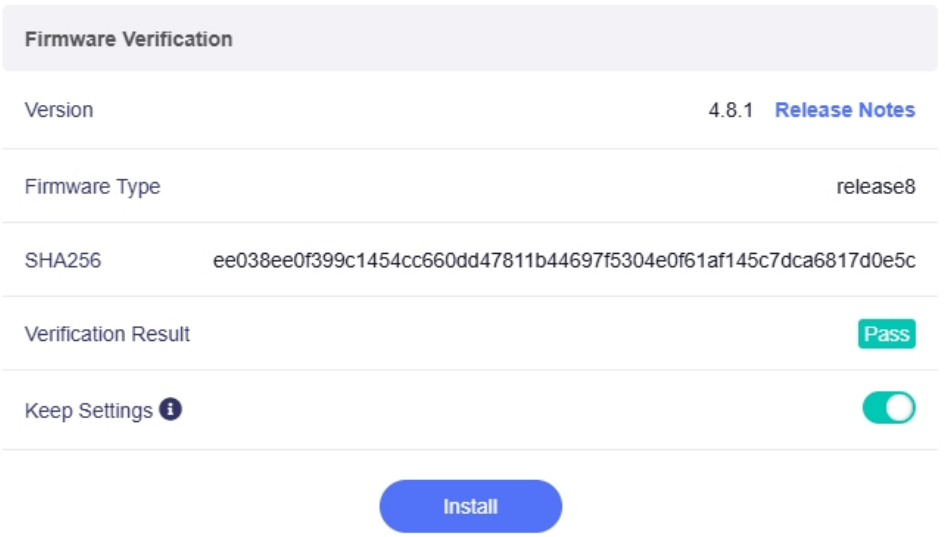
14.2.2 Actualización local

Este método 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.



Ta página mostrará los detalles del firmware. Verifique estos detalles antes de hacer clic **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.

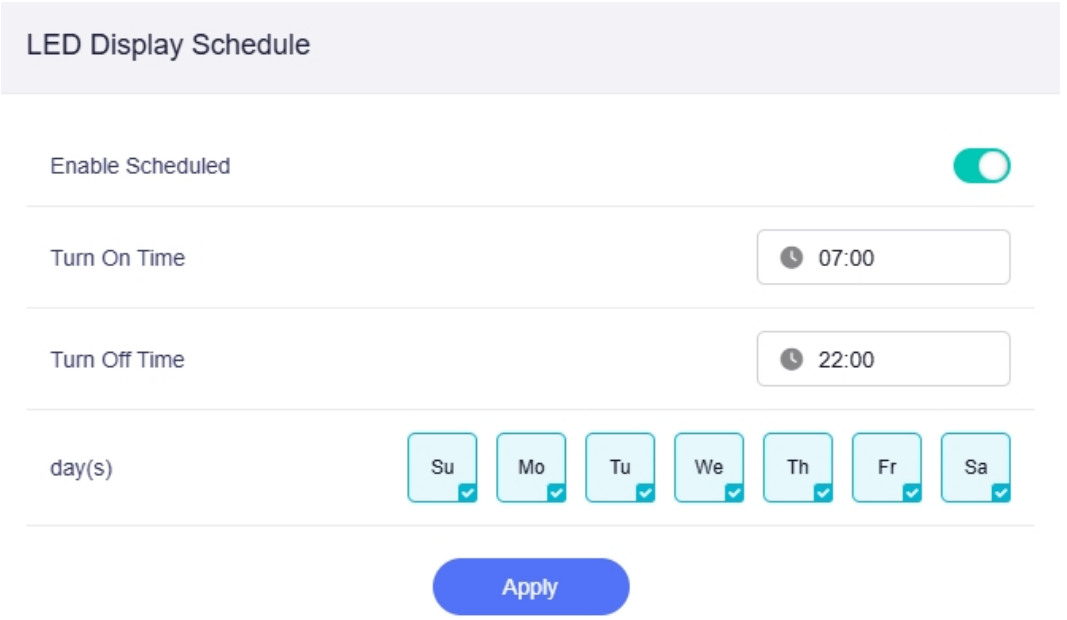
14.3 Tareas programadas

Inicie sesión en el panel de administración web de su enrutador y navegue hasta **SISTEMA** > **Tareas programadas**. Esta página le permite configurar un cronograma diario para algunas acciones básicas, incluido el encendido y apagado de la luz LED y reiniciar el enrutador.

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

14.3.1 Programación de los indicadores LED

Esta función le permite configurar un programa para la luz LED de su enrutador.

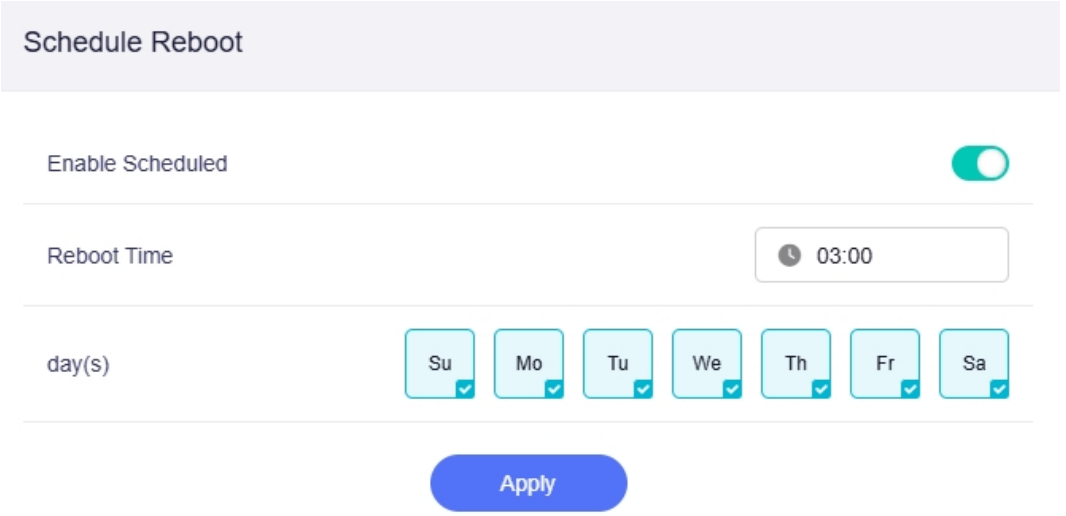


- **Habilitar programado**: cambie este interruptor para habilitar el LED mostrar el cronograma.
- **Tiempo de encendido**: establezca la hora (p. ej., 07:00) en la que se encenderá la luz LED .
- **hora de apagado**: establezca la hora (p. ej., 22:00) en la que se encienda la LED se apagará.
- **día(s)**: Seleccione los días efectivos de la semana para esta configuración.

Después de configurar, haga clic **Aplicar** para guardar su configuración.

14.3.2 Programar reinicio

Esta función le permite establecer un programa para reiniciar automáticamente su enrutador.

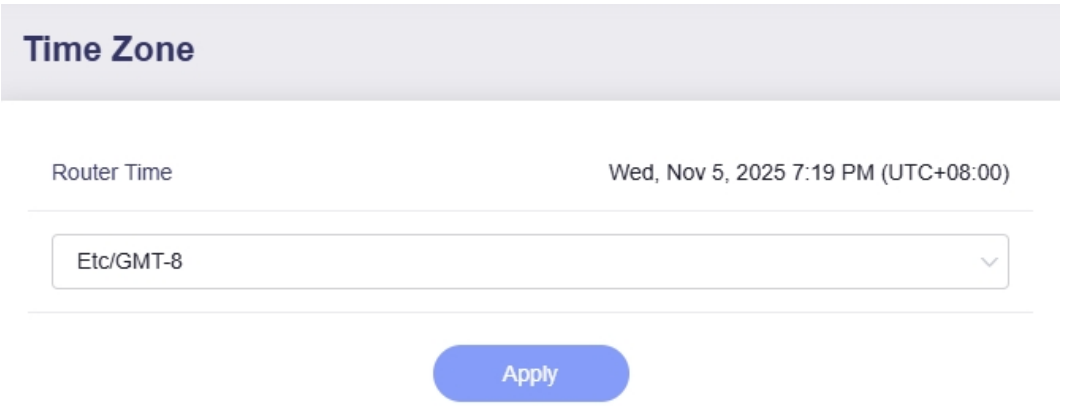


- **Habilitar programado**: active este interruptor para habilitar el reinicio programado.
- **Hora de reinicio**: establezca la hora específica (por ejemplo, 03:00) en la que se reiniciará el enrutador.
- **día(s)**: Seleccione los días efectivos de la semana para esta configuración.

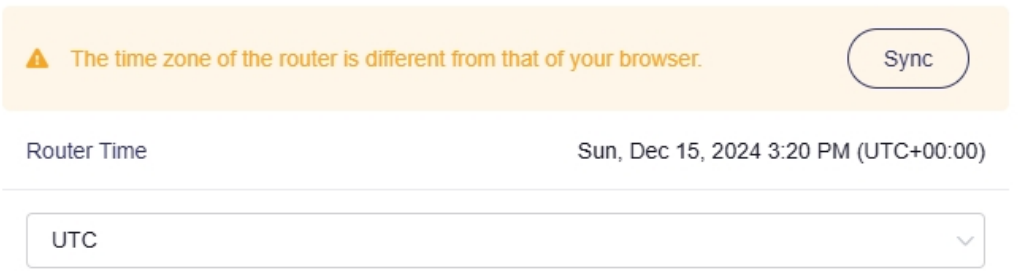
Después configurando, haga clic en **Aplicar** para guardar su configuración.

14.4 Zona horaria

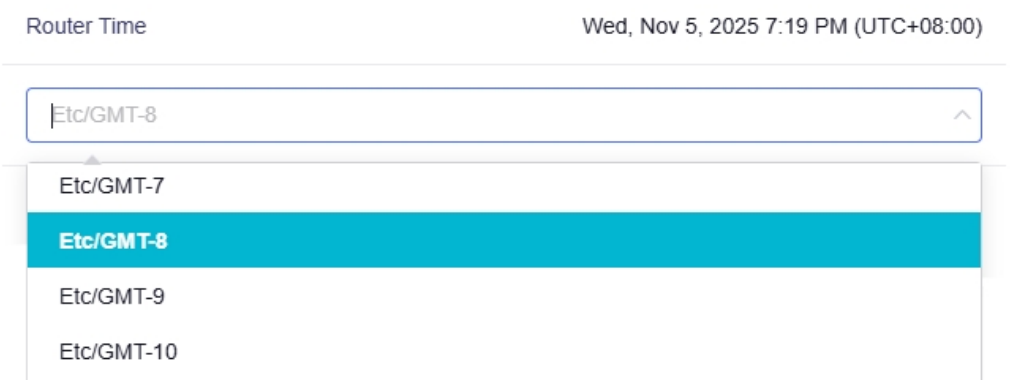
Inicie sesión en el panel de administración web de su enrutador y navegue hasta **SISTEMA** > **Zona horaria**. Esta página muestra la la hora del sistema, indicando la fecha, la hora y el desplazamiento de zona horaria correspondiente.



Algunas funciones dependen del tiempo 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.

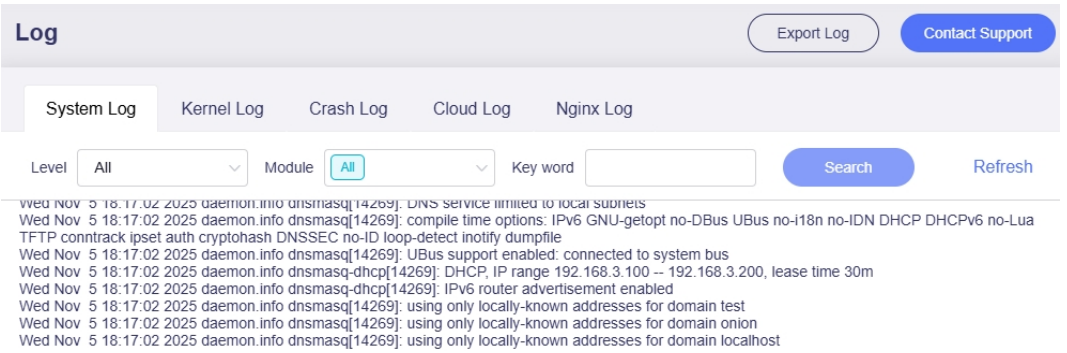


Para cambiar la zona horaria, sseleccione la zona horaria adecuada de la lista para garantizar que la hora del sistema coincida con su hora local.

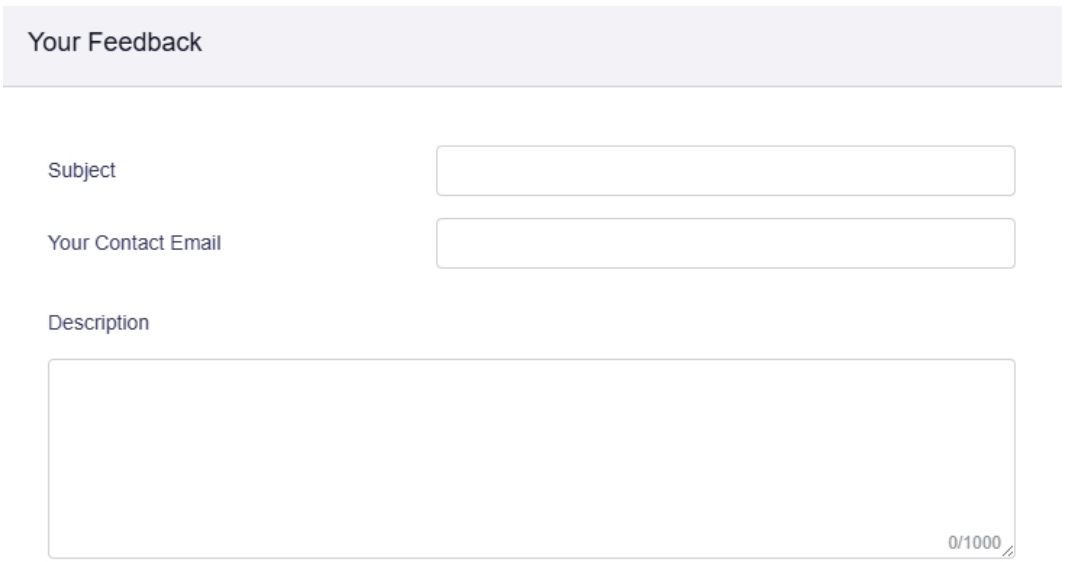


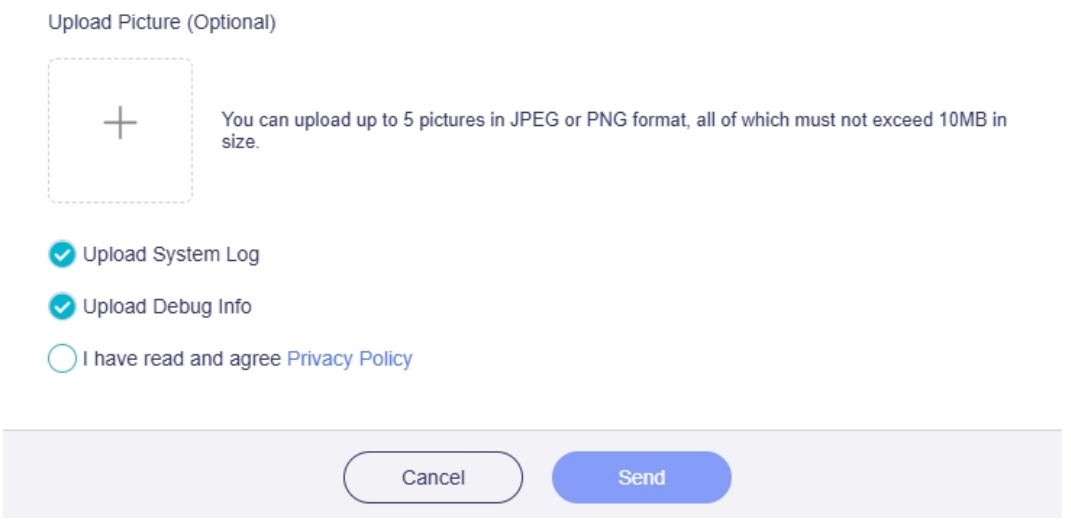
14.5 Registro

Inicie sesión en el panel de administración web de su enrutador y navegue hasta **SISTEMA** > **Registro**. Esta página le permite ver registros del sistema, kernel, fallas, nube y Nginx para análisis y solución de problemas. Además, algunos modelos de celular que admiten eSIM también proporcionan un registro 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

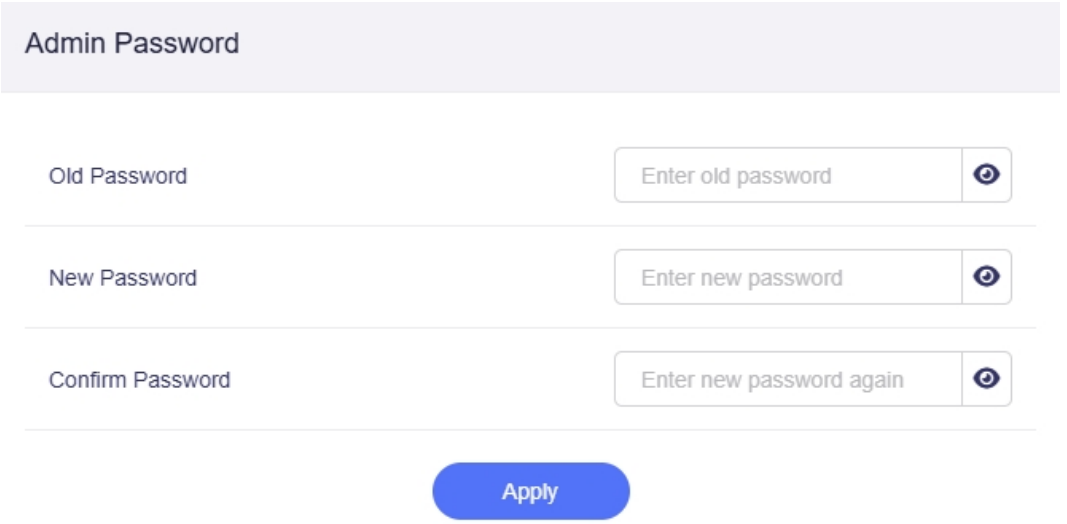
14.6 Seguridad

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, incluido:

- Admin password
- Acceso localcceso para web panel de administración, LuCI y SSH
- Remote HTTPS/SSH unacceso
- Administración de puertos abiertos del enrutador

14.6.1 Contraseña de administrador

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

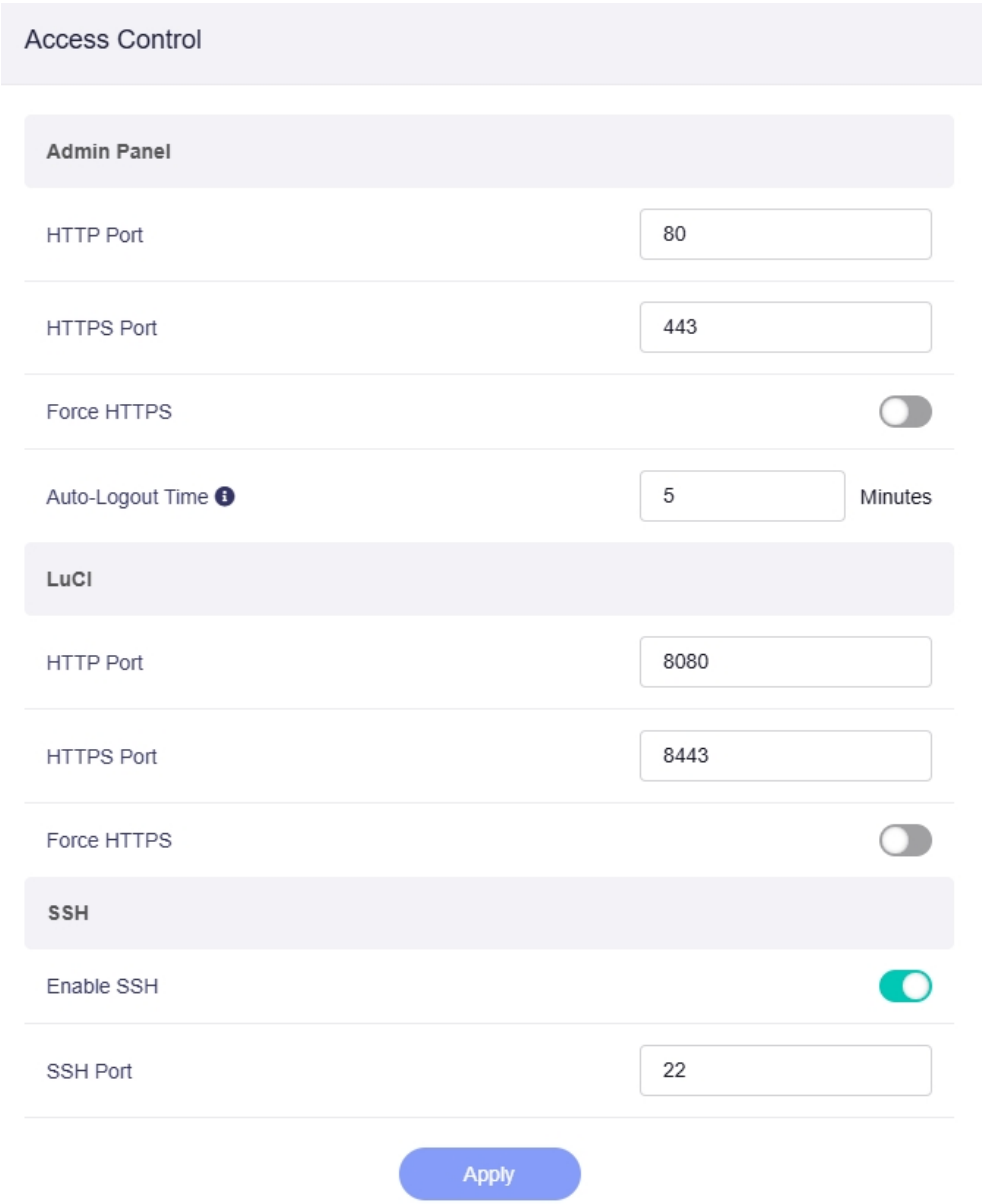


Los requisitos para la contraseña de administrador son los siguientes:

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

14.6.2 Control de acceso

Esta sección gestiona el acceso al enrutador's múltiples interfaces (Panel de administración, 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, el acceso al panel de administración web se aplica para utilizar una conexión HTTPS segura.
- **Tiempo de cierre de sesión automático**: configurado en 5 minutos de forma predeterminada, cierra automáticamente las sesiones de administrador 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.

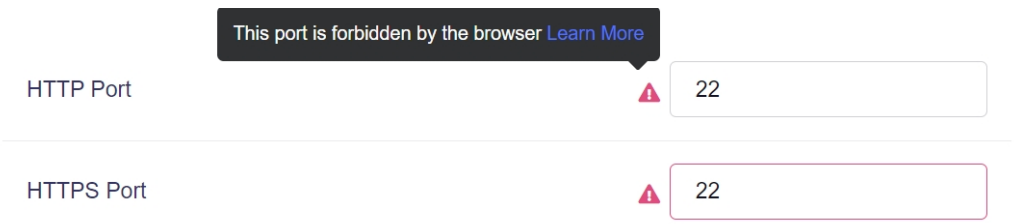
- **Puerto HTTP**: El valor predeterminado es 8080, para acceso HTTP sin cifrar a la interfaz LuCI.
- **Puerto HTTPS**: El valor predeterminado es 8443, para un acceso HTTPS seguro al mismo. Interfaz LuCI.
- **Forzar HTTPS**: cuando está habilitado, el acceso a la interfaz LuCI se aplica para utilizar una conexión HTTPS segura.

SSH

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

Nota:

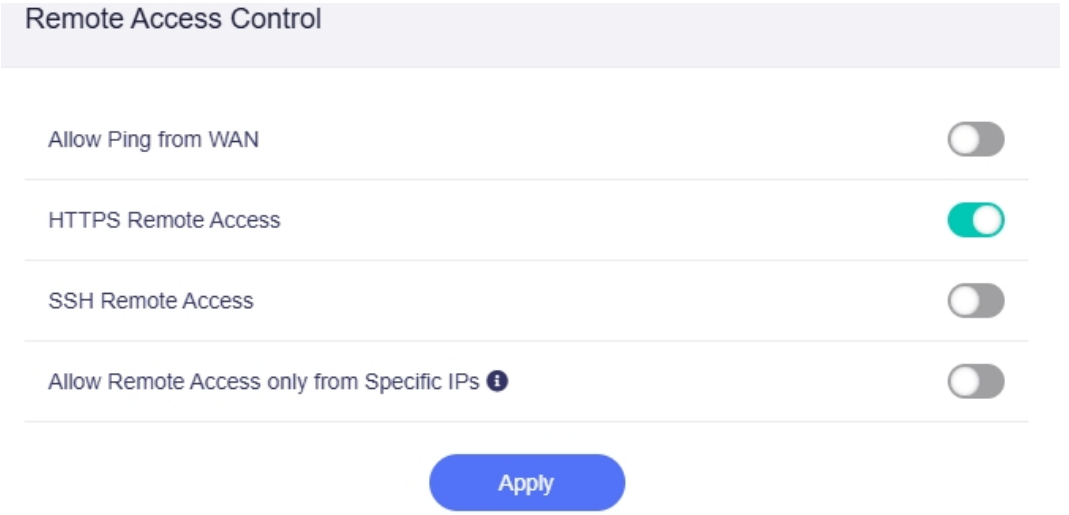
1. Si asigna un número de puerto que entra en conflicto con un puerto reservado (o uno reservado para servicios específicos por navegadores/convenciones de red), aparecerá un mensaje que indica "Este puerto está prohibido por el navegador".



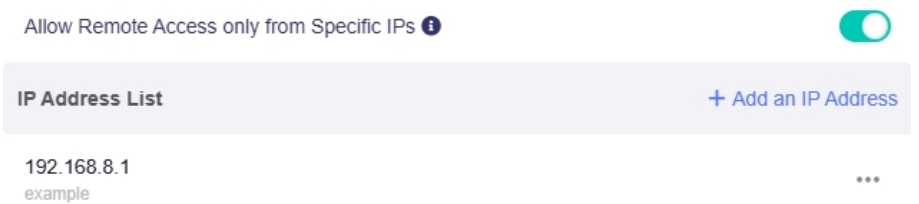
2. Si el número de puerto se modifica en el firmware, deberá ingresar el correcto número de puerto para acceder al panel de administración. Si olvidó el número de puerto, reinicie el enrutador para restaurar el número de puerto predeterminado.
3. La configuración de acceso a LuCI está disponible solo 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.

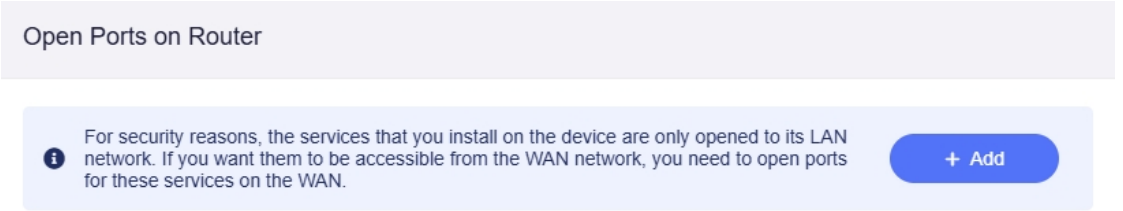


- **Permitir ping desde WAN**: Apermitir ping desde el lado WAN del enrutadorpuede ayudar a los usuarios a comprobar si se puede acceder al enrutador a través de la WAN wcuando hay un problema de red, así como a determinar la latencia de la red y la pérdida de paquetes.
- **Acceso remoto HTTPS**: El 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.

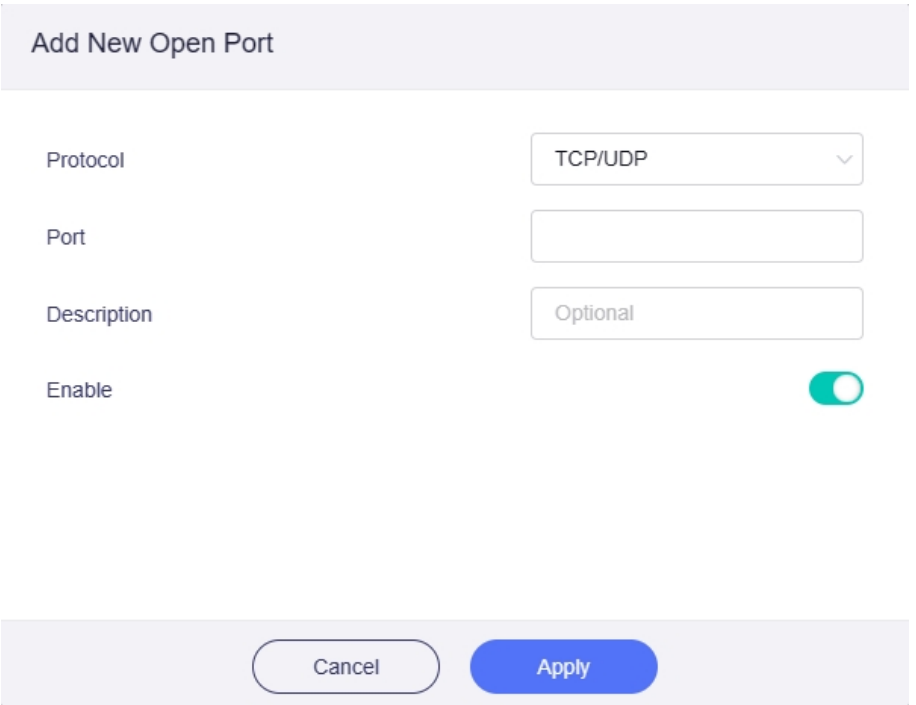


14.6.4 Abrir puertos en el enrutador

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.



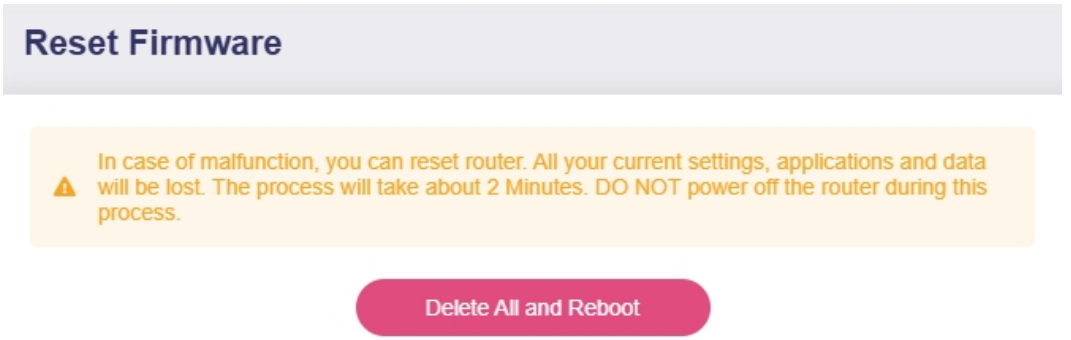
- **Protocolo**: seleccione el protocolo de red (TCP, UDP o TCP/UDP) para el puerto. Esto determina cómo se transmiten los datos para el servicio asociado con el puerto.
- **Puerto**: ingrese el número de puerto específico que desea abrir.

- **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

Inicie sesión en el panel de administración web de su enrutador y navegue hasta **SISTEMA** > **Restablecer firmware**. Si el enrutador no funciona correctamente, puede intentar resolver el problema restableciendo el firmware.

Haga clic en el botón **Eliminar todo y reiniciar** para restablecer el firmware según sea necesario.



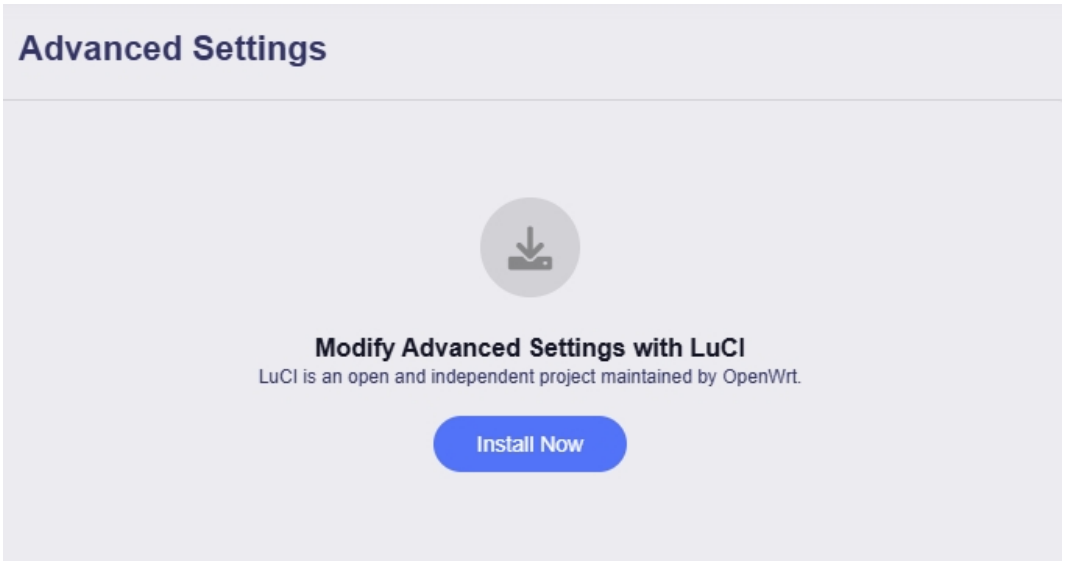
Nota: Todas sus configuraciones, aplicaciones y datos actuales serán borrados. El proceso durará unos 2 minutos. NoNo apague el enrutador durante este proceso.

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

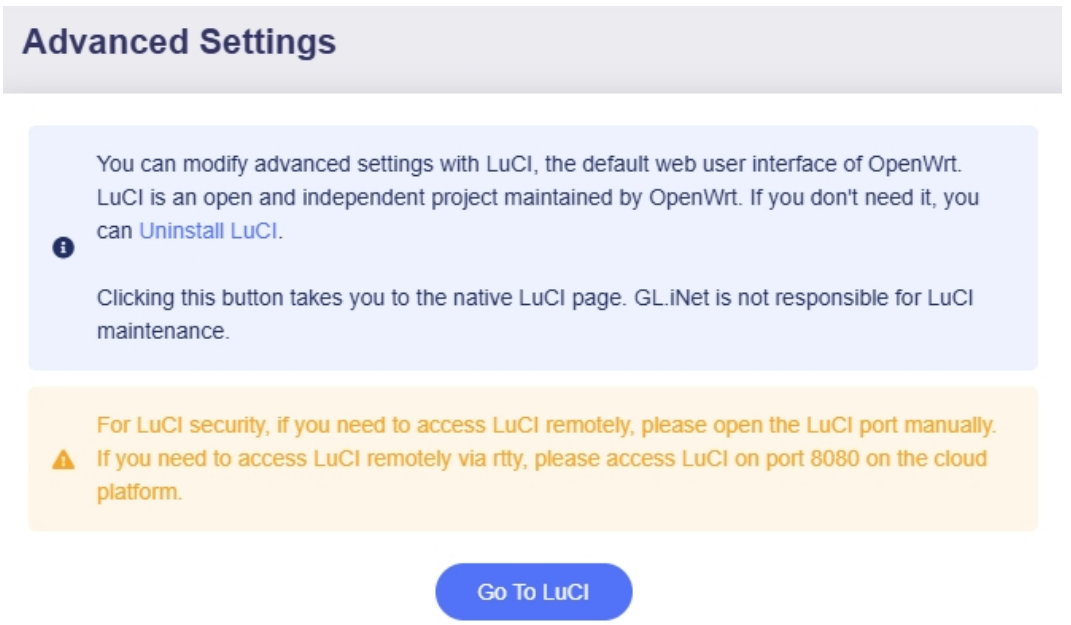
14.8 Configuración avanzada

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.

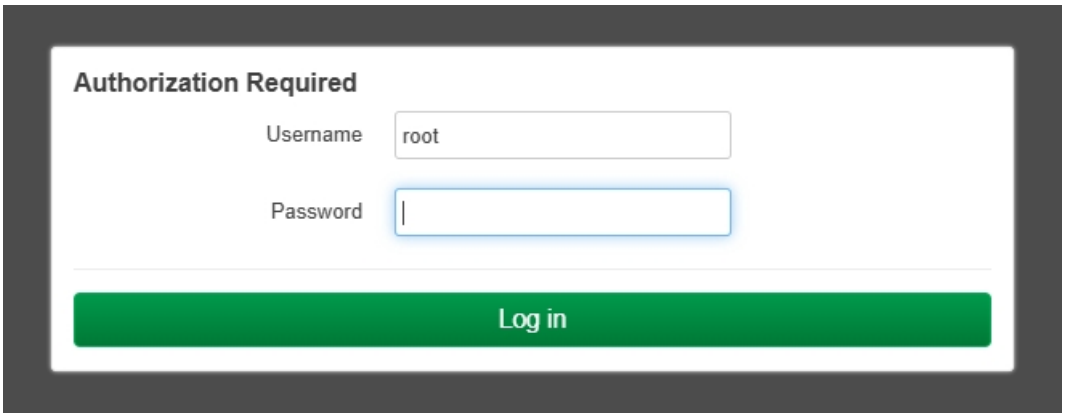
Haga clic en el botón **Instalar ahora** y se instalará la interfaz LuCI.



Haga clic en el **Ir a LuCI** botón, y será redirigido a la página de inicio de sesión de LuCI.



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



Luego iniciará sesión en la página de LuCI.

