GL·iNet



Manual de usuario

GL-B3000 / Marble

Enrutador doméstico Wi-Fi 6 de doble banda

Versión de firmware 4.5.22

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 8

1.1 Descripción general del producto 9

1.1.1 Apariencia 9

1.1.2 Interfaz y botón 10

1.1.3 LED 11

1.2 Especificaciones 11

1.3 Contenido del paquete 13

Capítulo 2 Conexión de hardware 14

2.1 Elección de una ubicación 15

2.2 Conexión del enrutador 15

Capítulo 3 Iniciar sesión en el enrutador 17

Capítulo 4 Configurar la conexión a Internet 19

4.1 Conectarse a Internet mediante un cable Ethernet 21

4.1.1 Configuración básica 21

4.1.2 Protocolo 22

4.2 Conectarse a Internet mediante una red Wi-Fi existente 25

4.2.1 Configuración básica 25

4.2.2 Opciones de repetidor 28

Capítulo 5 Red inalámbrica 29

5.1 Wi-Fi de 5 GHz 30

5.2 Wi-Fi de 2,4 GHz 32

Capítulo 6 Clientes 34

6.1 Detalles del dispositivo 36

6.2 Acción 38

6.3 Eliminar clientes 40

6.4 Ordenar 41

Capítulo 7 Conozca la VPN 42

7.1 Introducción 43

7.2 Escenarios de aplicación 44

Capítulo 8 Panel de VPN 46

8.1 Cliente VPN 47

8.1.1 Opciones del cliente 48
8.1.2 Modo de política 50
8.1.3 Opciones globales 51
8.2 Servidor VPN 54
8.2.1 Opciones del servidor 55
8.2.2 Regla de ruta del servidor 56
8.2.3 Opciones globales 58
Capítulo 9 Configurar el servidor VPN 59
9.1 Configurar el servidor OpenVPN 60
9.1.1 Preparación 60
9.1.2 Pasos de configuración 61
9.1.3 Solución de problemas 63
9.2 Configurar el servidor WireGuard 65
9.2.1 Preparación 65
9.2.2 Pasos de configuración 66
9.2.3 Solución de problemas 69
Capítulo 10 Configurar el cliente VPN 70
10.1 Configurar el cliente OpenVPN 71
10.1.1 Preparación 71
10.1.2 Configurar NordVPN 71
10.1.3 Configurar el cliente OpenVPN manualmente (para otros proveedores) 77
10.2 Configurar el cliente WireGuard 80
10.2.1 Preparación 80
10.2.2 Configurar AzireVPN 81
10.2.3 Configurar Mullvad 84
10.2.4 Configurar el cliente WireGuard manualmente (para otros proveedores) 88
Capítulo 11 Tor 92
Capítulo 12 Aplicaciones 94
12.1 Complementos 95
12.2 DNS dinámico 96
12.2.1 Habilitar DDNS 96
12.2.2 Comprobar si DDNS funciona 99
12.2.3 Acceso remoto HTTPS 101
12.2.4 Acceso remoto SSH 103

12.3 GoodCloud 105
12.3.1 Habilitar GoodCloud 106
12.3.2 Administrar el enrutador 110
12.3.3 Desvincular el dispositivo 115
12.4 AdGuard Home 116
12.5 Control parental 118
12.5.1 Configuración rápida 118
12.5.2 Solución de problemas 126
12.6 ZeroTier 127
12.6.1 Configurar ZeroTier 128
12.6.2 Permitir el acceso remoto a la WAN 132
12.6.3 Permitir el acceso remoto a la LAN 133
12.7 Tailscale 134
12.7.1 Configurar Tailscale 135
12.7.2 Permitir el acceso remoto a la WAN 138
12.7.3 Permitir el acceso remoto a la LAN 139
12.7.4 Nodos de salida personalizados 140
Capítulo 13 Red 141
13.1 Cortafuegos 142
13.1.1 Reenvío de puertos 142
13.1.2 Abrir puertos en el enrutador 144
13.1.3 DMZ 145
13.2 Multi-WAN 146
13.2.1 Seguimiento del estado de la interfaz 146
13.2.2 Modo Multi-WAN 149
13.3 LAN 152
13.3.1 Configuración básica 152
13.3.2 Servidor DHCP 153
13.3.3 Reserva de direcciones 155
13.4 Red de invitados 156
13.4.1 Configuración básica 156
13.4.2 Servidor DHCP 157
13.5 DNS 159
13.5.1 Configuración general 159

13.5.2 Configuración del servidor DNS 160
13.5.3 Editar hosts 162
13.6 Modo de red 164
13.7 IPv6 167
13.7.1 Modo IPv6 168
13.7.2 Método de obtención de DNS 168
13.8 Dirección MAC 169
13.9 Puerta de enlace directa 171
13.10 Inspección IGMP 174
13.11 Aceleración de red 175
13.12 Configuración NAT 176
Capítulo 14 Sistema 177
14.1 Descripción general 178
14.2 Actualización 179
14.2.1 Actualización en línea 179
14.2.2 Actualización local 181
14.3 Tareas programadas 183
14.3.1 Programación de los indicadores LED 183
14.3.2 Programar reinicio 184
14.3.3 Programación de Wi-Fi de 5 GHz 185
14.3.4 Programación de Wi-Fi de 2,4 GHz 188
14.4 Zona horaria 191
14.5 Registro 192
14.6 Seguridad 193
14.6.1 Contraseña de administrador 193
14.6.2 Control de acceso local 194
14.6.3 Control de acceso remoto 196
14.7 Restablecer firmware 197
14.8 Configuración avanzada 198

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

El enrutador Marble (GL-B3000) es un arte en sí mismo, inteligentemente exhibido como un marco de fotos para albergar su obra de arte favorita y elevar su espacio vital. No solo es un deleite visual para la vista, el enrutador Marble (GL-B3000) ofrece un rendimiento de primer nivel al incluir Wi-Fi 6 y admitir capacidades VPN.

1.1.1 Apariencia

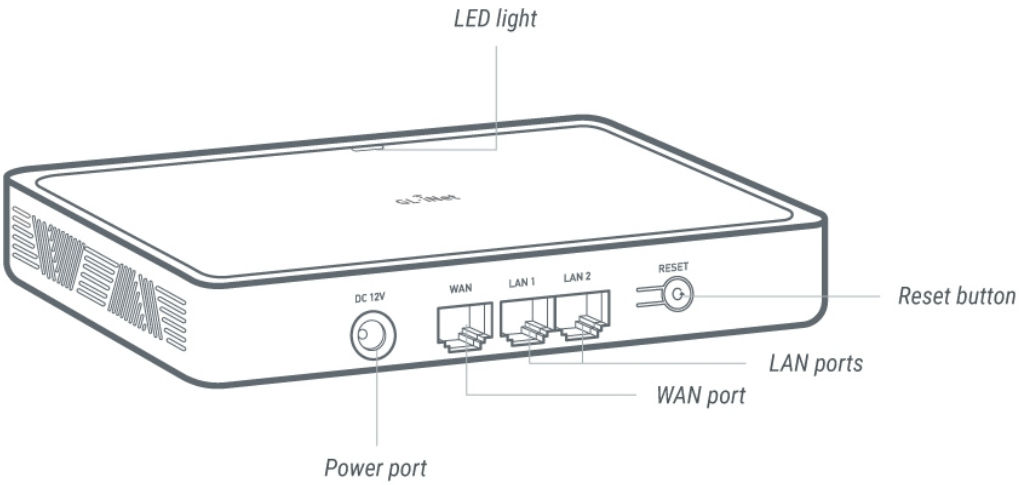








1.1.2 Interfaz y botón



Artículo	Descripción
Puerto de alimentación	Se conecta al adaptador de corriente.
Puerto WAN	Se conecta a un módem o a una toma Ethernet para Internet.
Puerto LAN	Se conecta a dispositivos cableados si es necesario.
Botón Restablecer	Mantenga presionado durante **4 segundos** para reparar su red; Presione y mantenga presionado durante **10 segundos** y luego suelte para restablecer el enrutador a los valores predeterminados de fábrica.

1.1.3 LED

Estado	Indicación
Azul sólido	Arranque del sistema
Parpadea en azul lentamente	Red de búsqueda
Azul parpadeante rápidamente	Actualizando firmware
Blanco sólido	Trabajando normalmente

1.2 Especificaciones

Interfaz	1 x puerto Ethernet WAN 2 x puerto LAN Ethernet 1 entrada de CC de 12 V/1,5 A 1 x botón Restablecer
CPU	Qualcomm de doble núcleo, @1GHz
Memoria/Almacenamiento	DDR3L 512 MB / NAND Flash 128 MB
Protocolo	IEEE 802.11a/b/g/n/ac/ax
Velocidad de Wi-Fi	574Mbps (2,4 GHz), 2402 Mbps (5 GHz)
Antenas	4 x antenas internas
Velocidad de Ethernet	10/100/1000Mbps
Entrada de energía	DC5521, 12V/1,5A (5,5*2,1 mm)
Consumo de energía	< 13W
Temperatura de funcionamiento	0 ~ 40°C (32 ~ 104°F)
Temperatura de almacenamiento	-20 ~ 70°C (-4 ~ 158°F)

Dimensión/Peso	Enrutador: 155 x 120 x 23 mm / 275 g Marco de fotos: 235 x 197 x 32 mm (se adapta a una foto de 8 pulgadas)
Otras herramientas	Hoja de datos / Firmware / Aplicación / Unboxing / Tutoriales

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

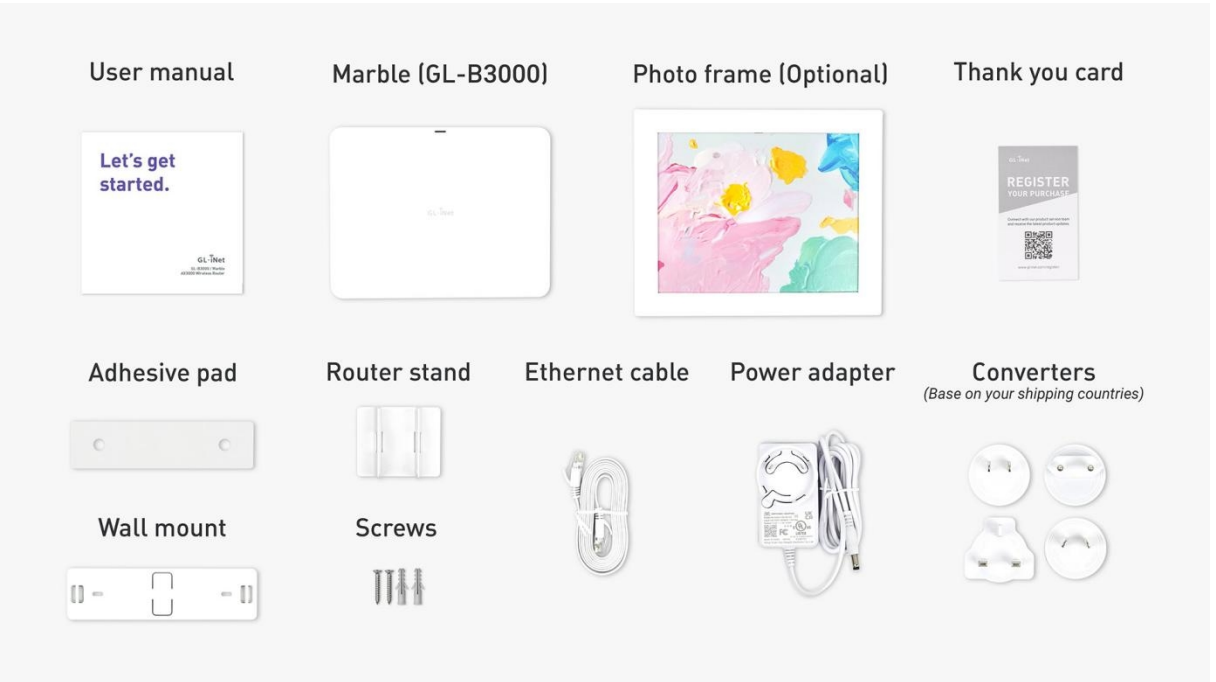
*El uso de Wi-Fi 6 (802.11ax) y sus funciones (OFDMA, MU-MIMO, 1024-QAM, HT160) requiere que los dispositivos cliente admitan las tecnologías correspondientes.

1.3 Contenido del paquete

Tenga en cuenta que el adaptador dentro del paquete depende de su país de envío.

El paquete incluye:

- 1 x Marble (GL-B3000)
- 1 manual de usuario
- 1 x Tarjeta de agradecimiento
- 1 cable Ethernet
- 1 x kit de montaje en pared
- 1 x almohadilla adhesiva
- 1 x soporte para enrutador
- 1 x marco de fotos (opcional)
- 1 x adaptador de corriente
- 1 x Convertidor (según su país de envío)



Capítulo 2

Conexión de hardware

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

2.1 Elección de una ubicación

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

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

2.2 Conexión del enrutador

1. **Encendido**

   Junte el adaptador de corriente de dos piezas. Conéctelo al enrutador y conéctelo a una toma de corriente.
2. **Conecte un dispositivo al enrutador**

   Conecte un dispositivo (por ejemplo, una computadora portátil o un teléfono inteligente) al enrutador a través de Wi-Fi o. un cable Ethernet.
   - **Wi-Fi**: En su dispositivo, vaya a Configuración > WLAN, ubique el nombre de la red Wi-Fi del enrutador' en la lista de redes disponibles e ingrese la contraseña. Puede encontrar el nombre de red predeterminado y la contraseña impresos en su enrutador's etiqueta.
   - **Ethernet**: Conecte su dispositivo al puerto LAN del enrutador'a través de un cable Ethernet.
3. **Inicie sesión en enrutador**

El Internet está undisponible al conectarse al enrutador para el 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

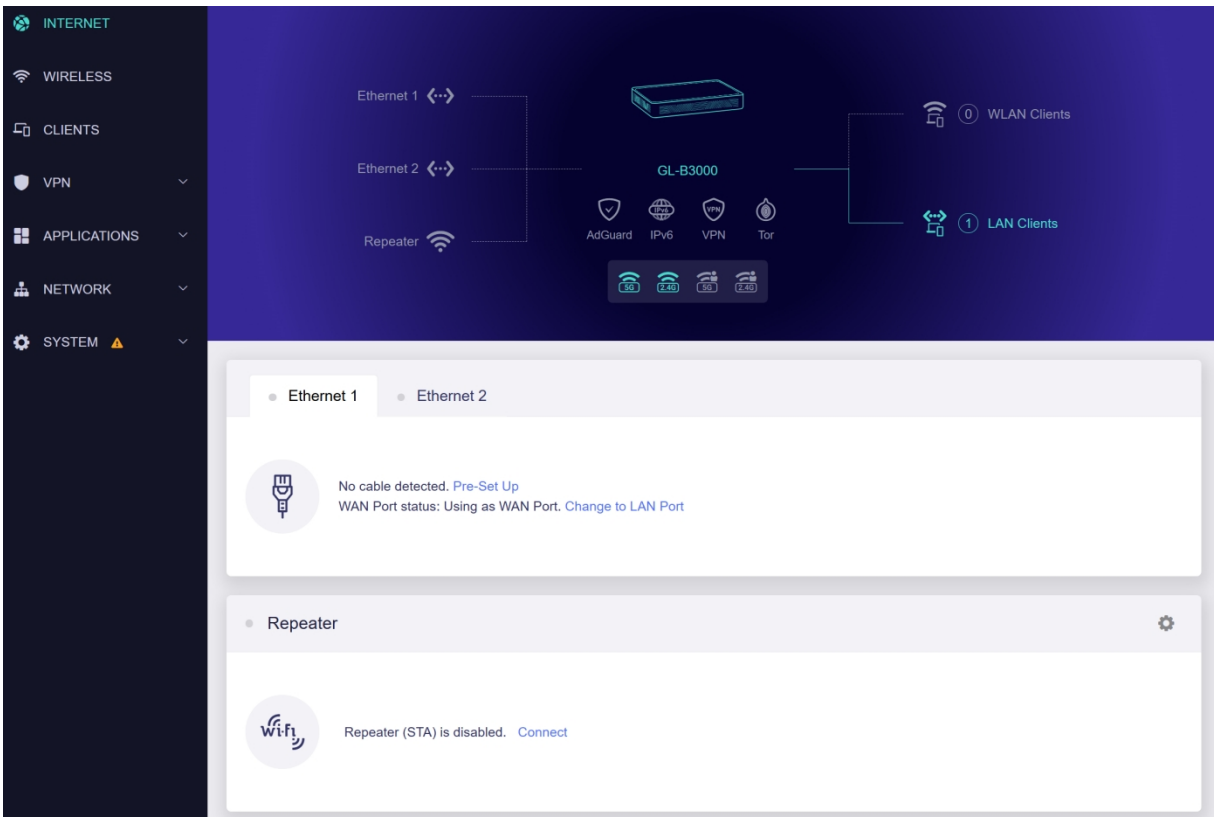
Este capítulo lo guía para iniciar sesión en su enrutador a través del panel de administración web

Configurar y. Administre su enrutador a través de una interfaz de administración basada en web, a la que se puede acceder desde cualquier sistema operativo Windows, Maceinterfaz de configuración, a la que se puede acceder desde cualquier Windows o Mac o Linux con un navegador web, como Microsoft Edge. Google Chrome, Mozilla Firefox o Apple Safari.

Nota: Si prefiere que nosotrosing el GL.aplicación iNet en lugar de la web admin panel, descarga la aplicación y siga las indicaciones que aparecen en pantalla.

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 enrutador mediante Wi-Fi o un cable Ethernet.
2. Abrir un navegador web (se recomienda Chrome y Edge) y visite http://192.168.8.1. Serás dirigido a la página de inicio de sesión de la web admin panel. Si no puede acceder a la web undmin panel, consulte aquí para solucionar problemas.
3. Sconfigure su contraseña de administrador. Se recomienda una contraseña segura por motivos de seguridad. Luego haga clic en **Siguiente** para continuar.
4. Ylo hará luego ingrese al router'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 diversas redes. entornos.

Marble admite dos métodos de conexión a Internet: Ethernet, y Repetidor, Celija el método apropiado según sus necesidades de uso.

1. **Ethernet (RJ45)**: conecte el enrutador a una red de banda ancha utilizando un cablen 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 fijo de banda ancha.

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

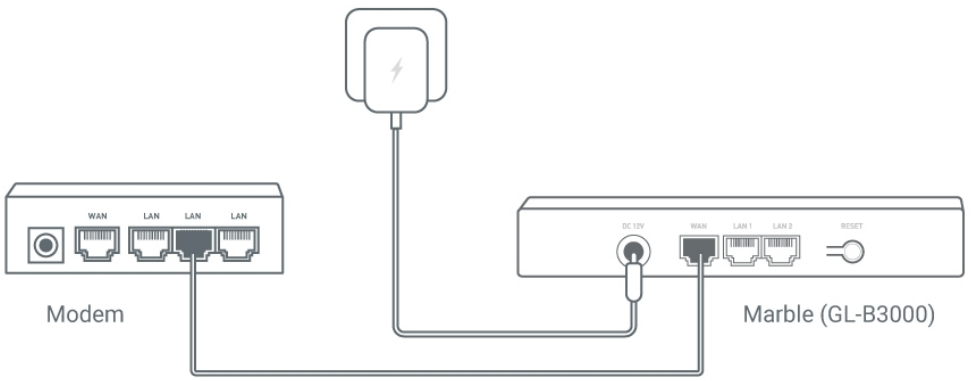
4.1 Conectarse a Internet mediante un cable Ethernet

Conecte el enrutador a una red de banda ancha usando un cablen 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.

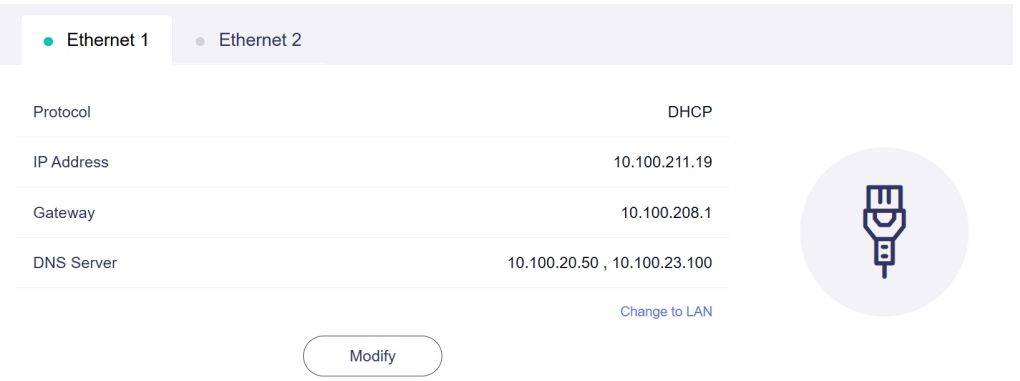
4.1.1 Configuración básica

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

1. Conecte el **WAN** puerto 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.

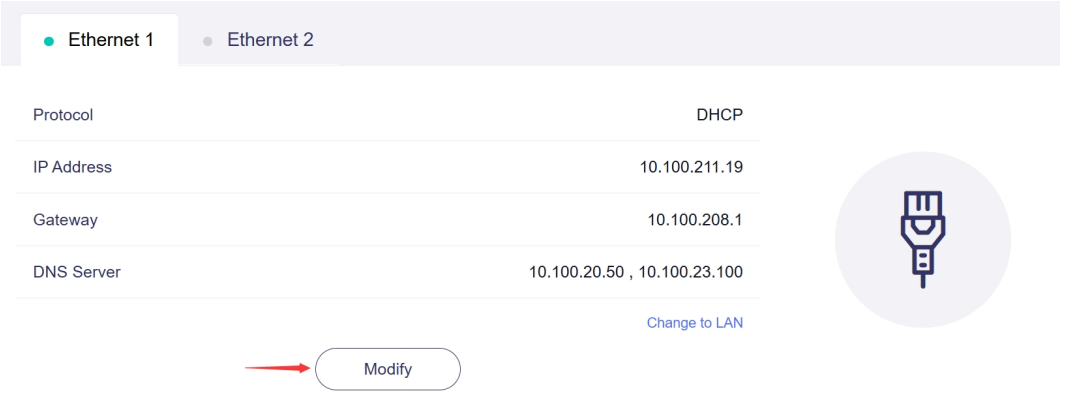


2. Inicie sesión en el el enrutador'panel de administración web y navegue a **INTERNET** > **Ethernet**. Si la conexión se realiza correctamente, la sección Ethernet mostrará red detalles, incluidos protocolo, dirección IP, puerta de enlace, y DNS Servidor.



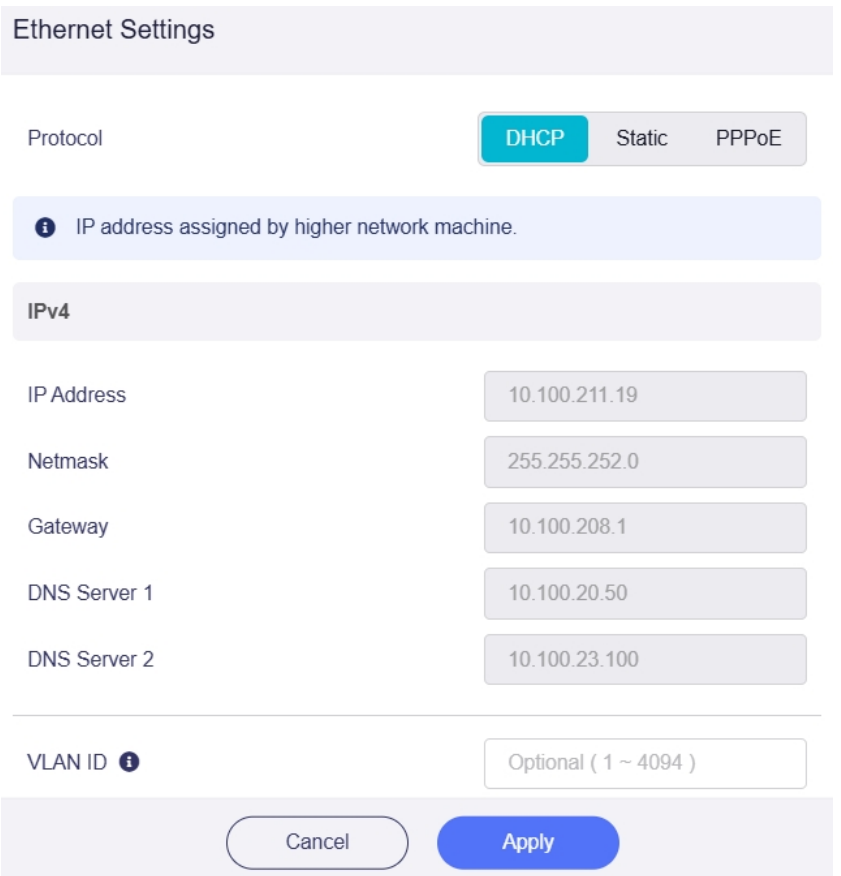
4.1.2 Protocolo

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



- **DHCP**

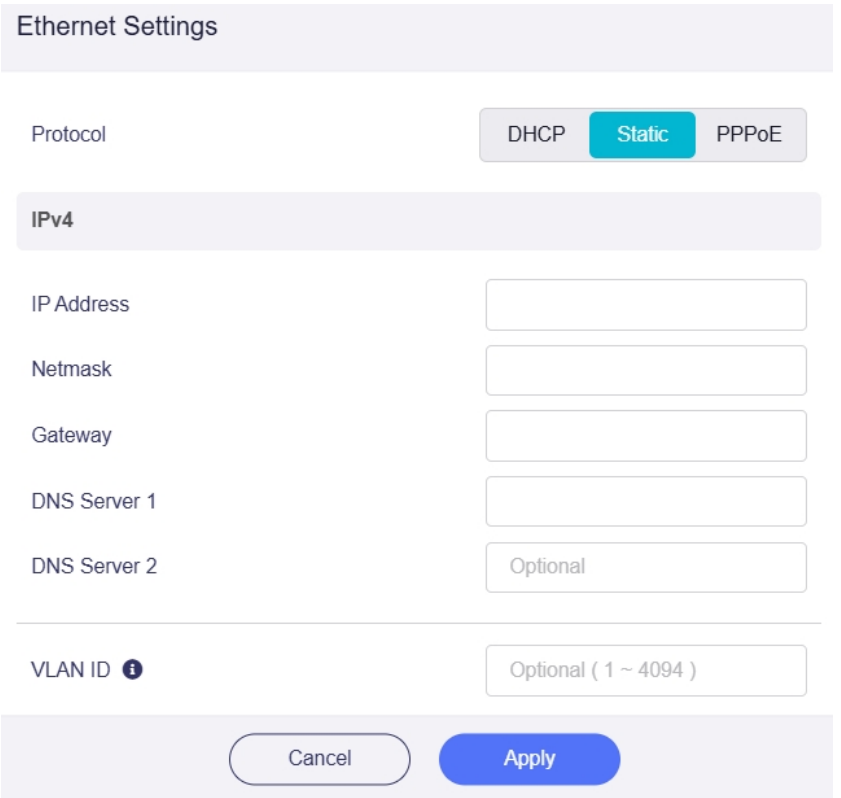
  DHCP es el protocolo de red predeterminado y más común, que asigna automáticamente direcciones IP y otros parámetros de configuración de red a dispositivos en una red IP a través de un modelo cliente-servidor. Puede configurar un **ID de VLAN** si su proveedor de servicios requiere que la interfaz utilice un ID de VLAN etiquetado específico.



Puede configurar un **VLAN ID** si su proveedor de servicios requiere que la interfaz utilice un VLAN ID etiquetado específico.

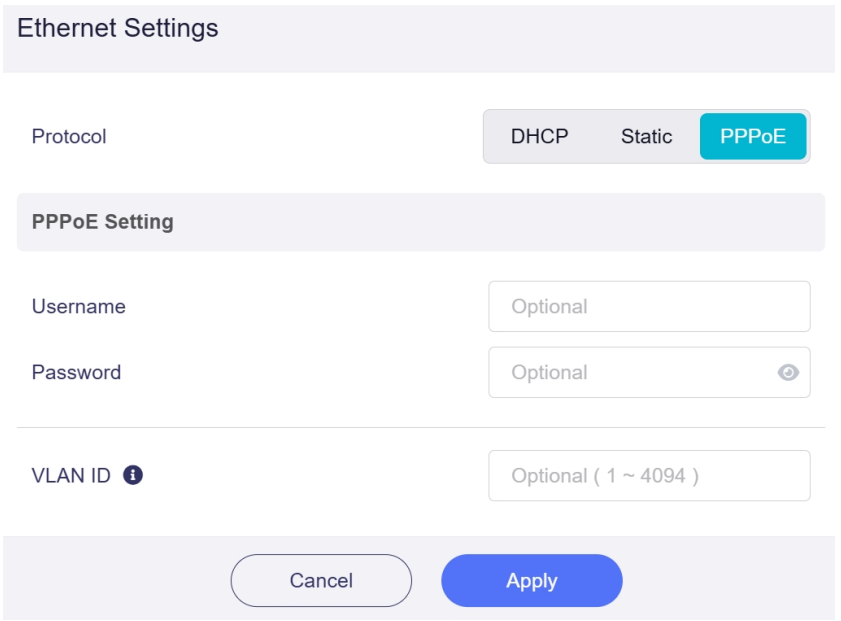
- **Estática**

  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). Puede configurar un **ID de VLAN** si su proveedor de servicios requiere que la interfaz utilice un ID de VLAN etiquetado específico.



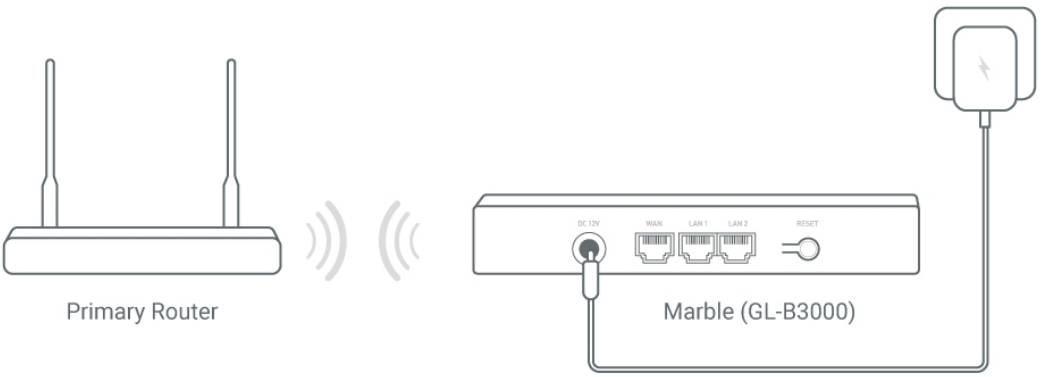
- **PPPoE**

  PPPoE (Protocolo punto a punto 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. Puede configurar una **ID de VLAN** si su proveedor de servicios requiere que la interfaz utilice un ID de VLAN etiquetado específico.


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

4.2 Conectarse a Internet mediante una red Wi-Fi existente

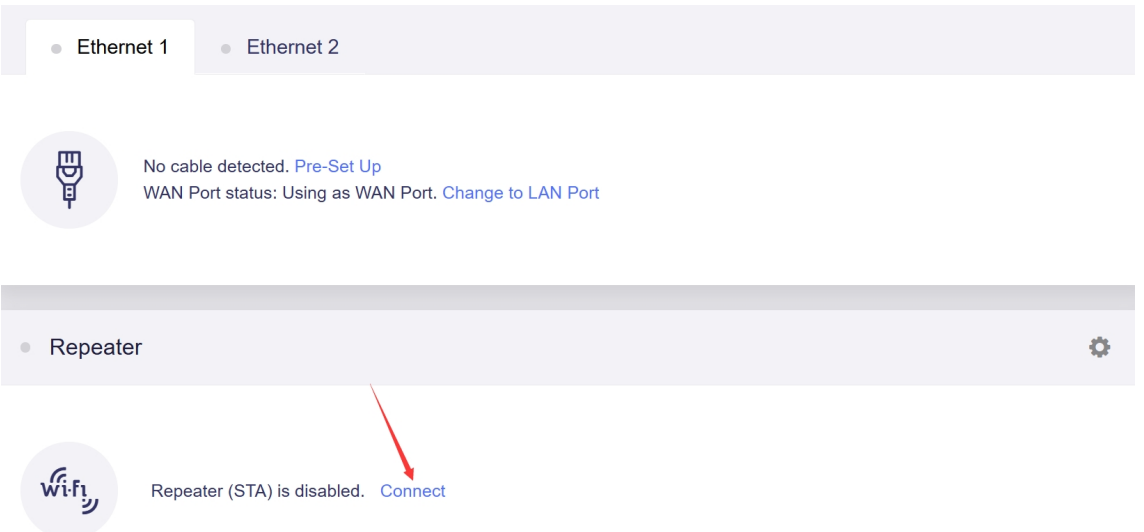
Conecte el enrutador como repetidor a la red inalámbrica existente para aumentar las señales Wi-Fi-Fi y crear una red local aislada de la red principal. Cuando en hoteles o cafeterías con puntos de acceso públicos gratuitos, el uso de un repetidor no solo fortaleces Wi-Fi, sino que también proporcionas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



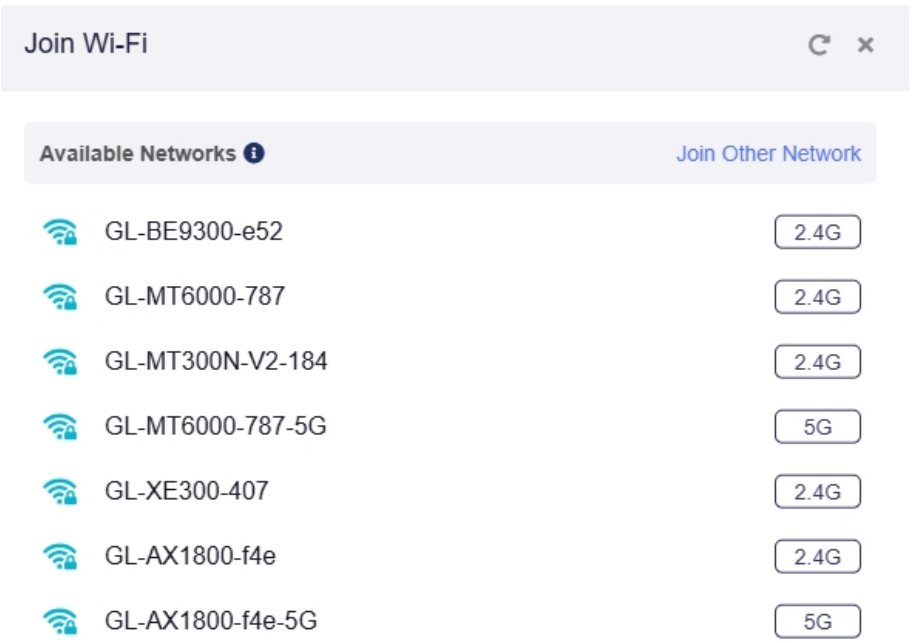
Repetidor GL.iNet Esta característica funciona en modo WISP (Proveedor de servicios de Internet inalámbrico) de forma predeterminada, lo que significa que el enrutador creará su propia subred y actuará como un firewall para protegerlo de la red pública.

4.2.1 Configuración básica

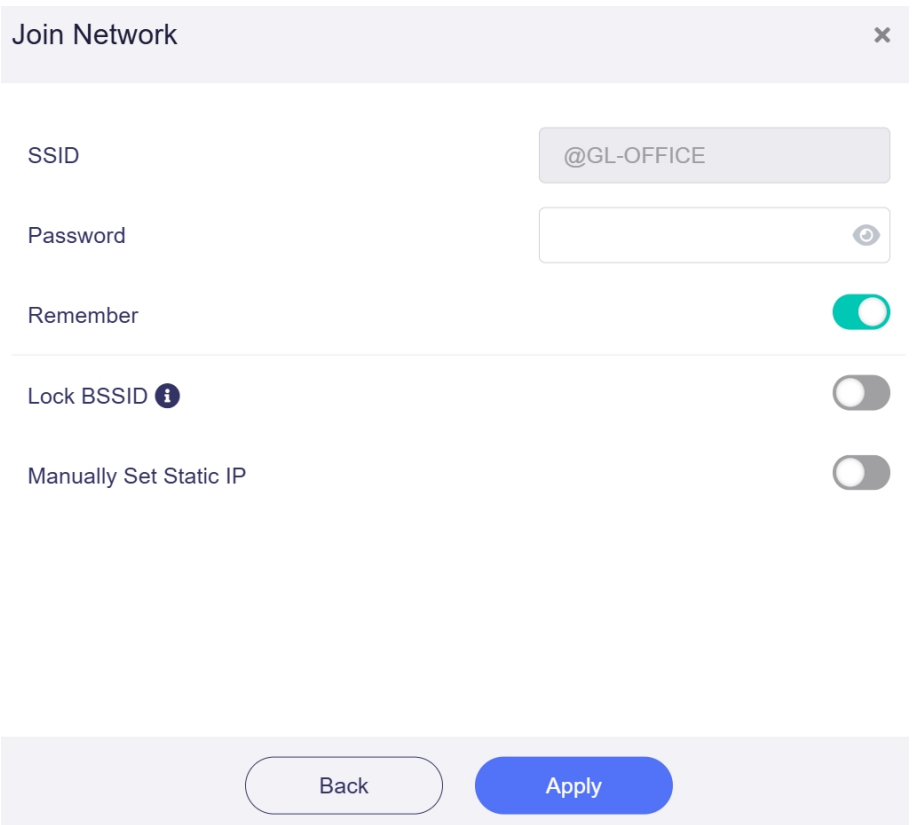
1. Registro acceda al del enrutador'panel de administración web y navegue a **INTERNET** > **Repetidor**. Haga clic en **Conectar**.



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



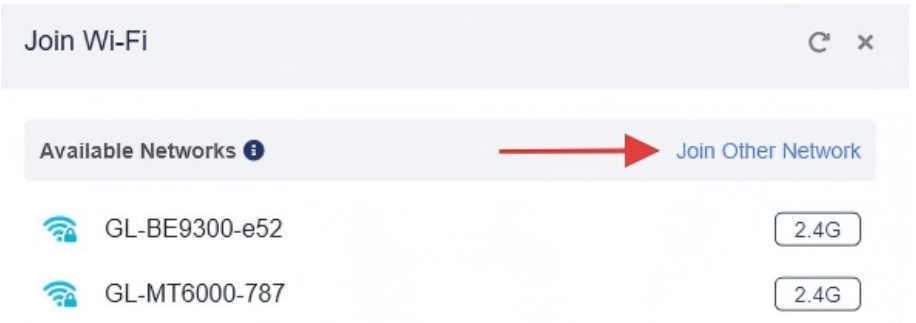
3. Eingrese la contraseña de Wi-Fi correcta y haga clic en **Aplicar**.



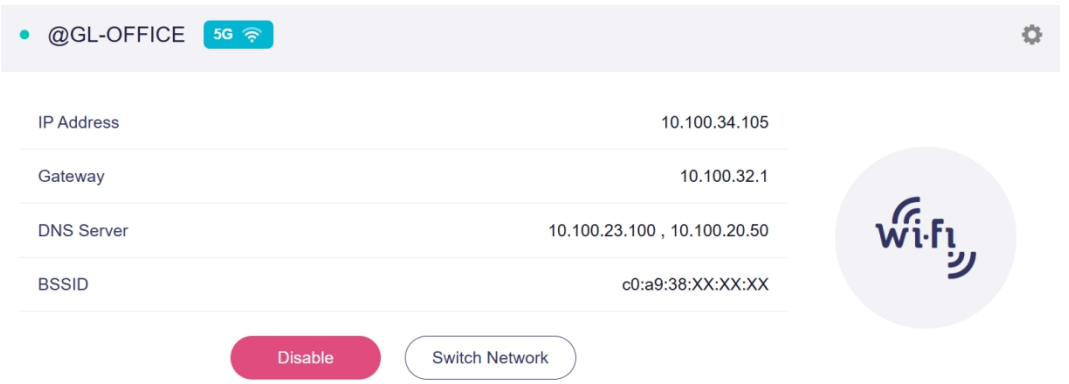
- **Recordar**: habilite esta opción para recordar la red Wi-Fi actual repetida.

- **Bloquear BSSID**: cuando está habilitado, el enrutador se conectará solo al punto de acceso (AP) específico correspondiente al BSSID seleccionado, incluso cuando otros AP compartan el mismo SSID.
- **Manualmente Set SIP estática**: si está habilitado, puede configurar manualmente la dirección IP, la máscara de subred, la puerta de enlace y los servidores DNS, en lugar de obtener la configuración de IP automáticamente a través de DHCP.

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

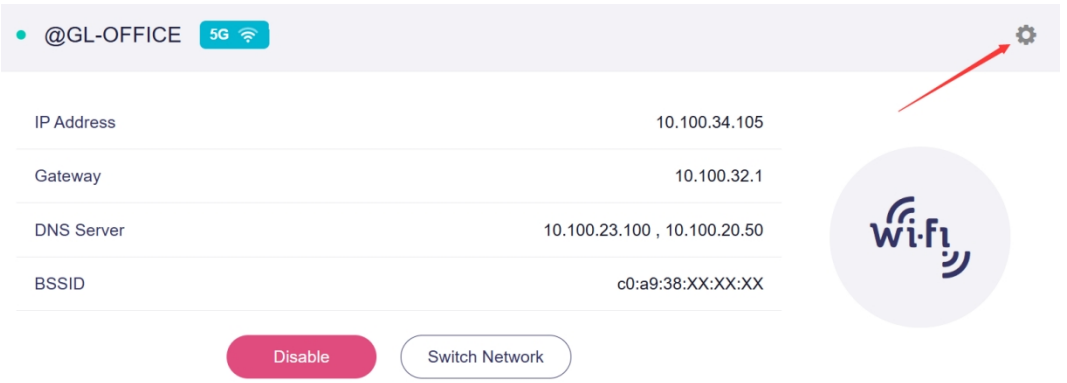


5. Espere un minuto hasta que el enrutador se conecte. Una vez conectada, la página se muestra a continuación.

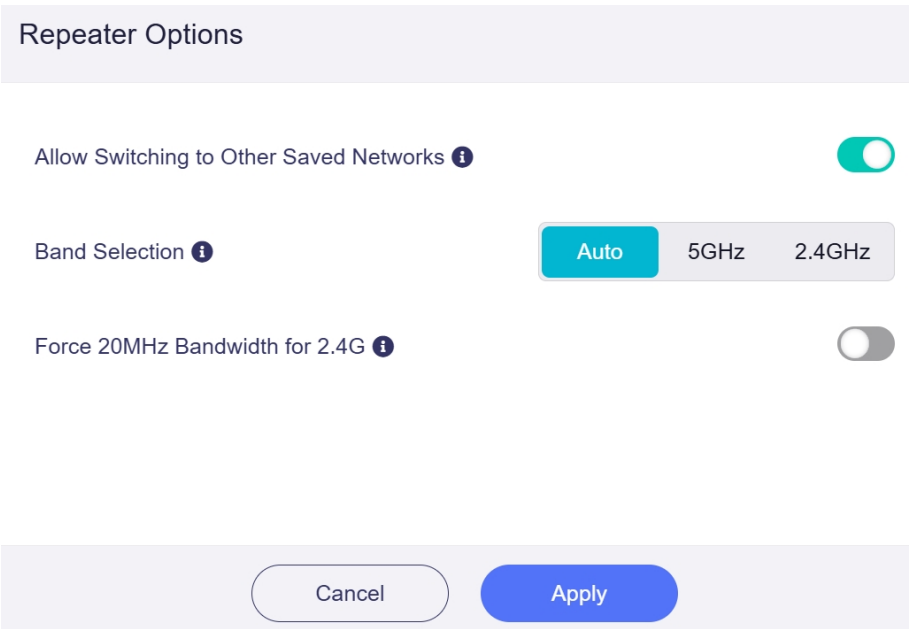


4.2.2 Opciones de repetidor

Haga clic en el ícono de ajustes en la esquina superior derecha para configurar las opciones del repetidor.



La página puede varían debido a las diferentes versiones de firmware.



- **Permitir cambiar a otras redes guardadas**: si la opción está habilitada, el enrutador se conectará automáticamente a otras redes guardadas cuando no pueda conectarse a la red Wi-Fi actual.
- **Selección de banda**: si seleccionas manualmente una banda, el enrutador no escaneará ni se conectará a ningún Wi-Fi que esté usando otra banda.
- **Forzar un ancho de banda de 20 MHz para 2,4 G**: Si esta opción está habilitada, el dispositivo mejorará la estabilidad de la conexión reduciendo la velocidad de conexión.
  Nota: Solo funciona cuando se repite Wi-Fi 2.4G.

Capítulo 5

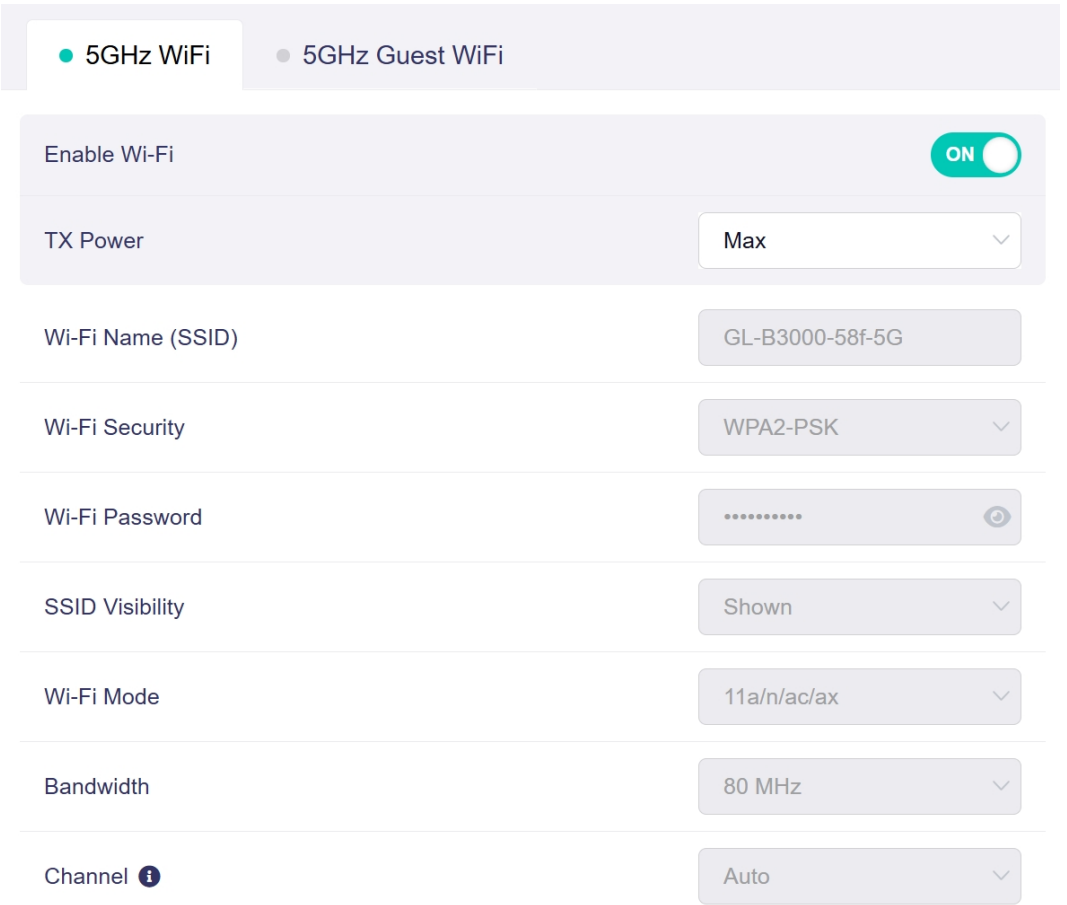
Red inalámbrica

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

Inicie sesión en el panel de administración web del enrutador y navegue hasta **Inalámbrica**. La página inalámbrica muestra la configuración de Wi-Fi del router's 5GHz y 2.4 GHz, con cada dividida en redes Wi-Fi principal y Wi-Fi para invitados-Fi para una administración flexible .

5.1 Wi-Fi de 5 GHz

El Wi-Fi principal de 5 GHz le permite configurar múltiples ajustes, incluyendo habilitar/deshabilitar Wi-Fi, configurar la potencia de transmisión, configurar Wi-Fi nombre (SSID), seguridad, contraseña, visibilidad de SSID, modo, ancho de banda, y canal.

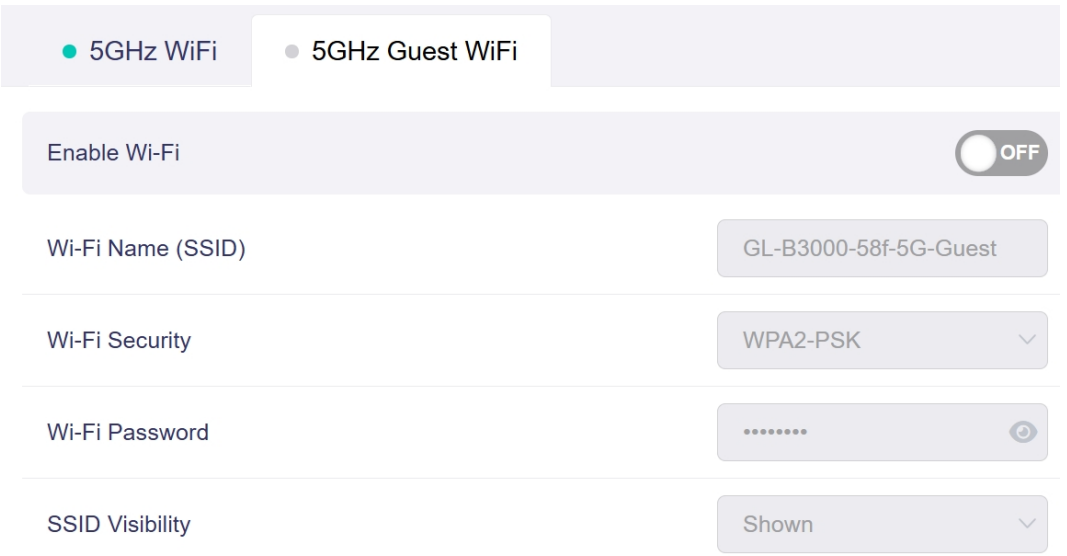


Nota:

1. El **Ancho de banda** y **Canal** nono se puede modificar cuando el enrutador está configurado como a repeater, ya que siguen el de la red repetida.
2. Cuando **Canal** es establezca en **Auto**, el enrutador's Wi-Fi no cambiará automáticamente al DFS canal.

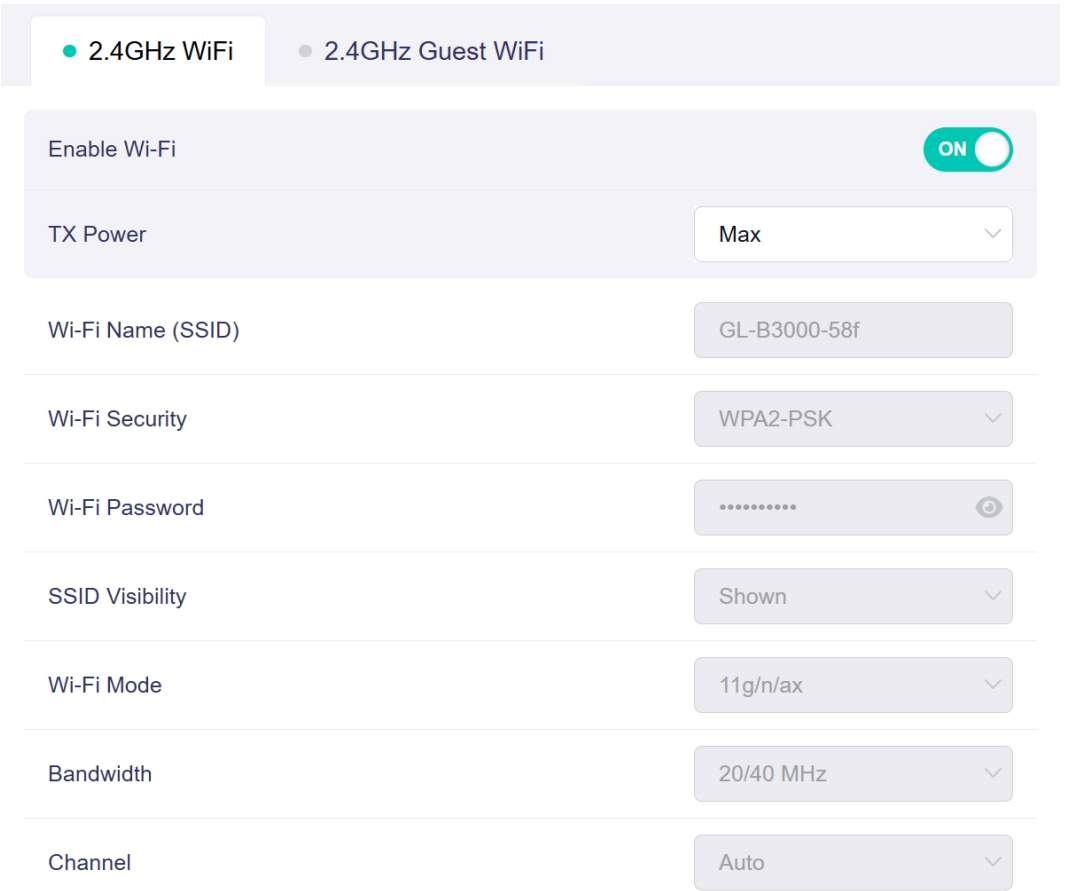
3. Cuando **Ancho de banda** está configurado en **160 MHz** (solo disponible en algunos modelos), el Wi-Fi siempre usará el canal DFS, incluso si selecciona un canal que no es DFS o configúrelo en Auto.

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



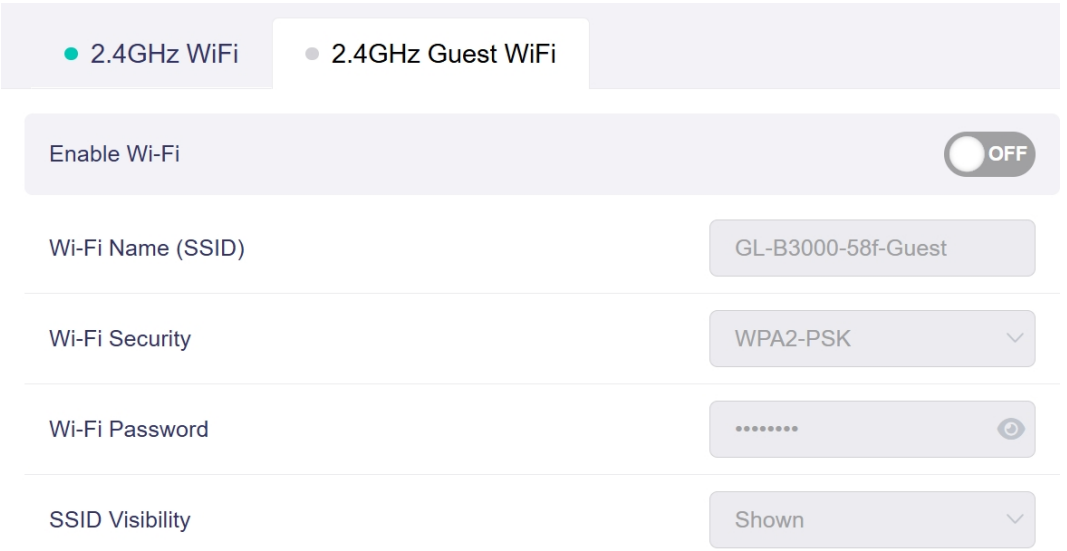
5.2 Wi-Fi de 2,4 GHz

El 2.4 Wi-Fi principal de GHz le permite usted configurar múltiples ajustes, incluida activar/deshabilitar Wi-Fi, configurar la potencia de TX, configurar nombre de Wi-Fi (SSID), seguridad, contraseña, visibilidad de SSID, modo, ancho de banda y canal.



Nota: El **Ancho de banda** y **Canal** nono se puede modificar cuando el enrutador está configurado como a repetidor, ya que siguen el de la red repetida.

El 2.4 GHz Invitado Wi-Fi le permite usted configurar simplificado configuración, incluyeg habilitación/deshabilitación Wi-Fi, configuración Nombre de Wi-Fi (SSID), seguridad, contraseña y visibilidad de SSID.


2.4GHz WiFi
2.4GHz Guest WiFi
Enable Wi-Fi
OFF
Wi-Fi Name (SSID)
GL-B3000-58f-Guest
Wi-Fi Security
WPA2-PSK
Wi-Fi Password
SSID Visibility
Shown

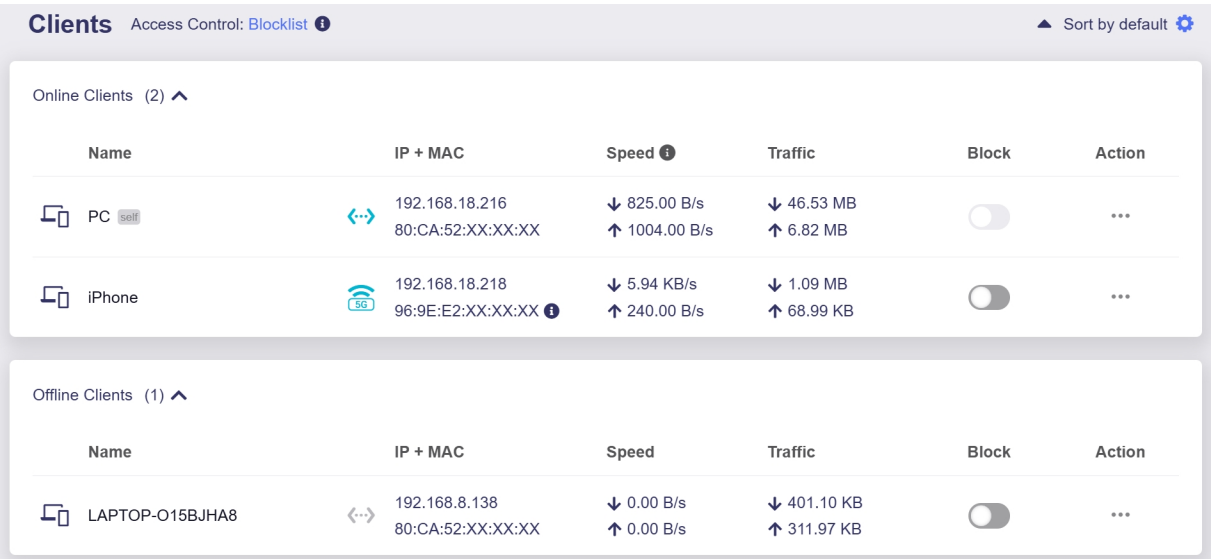
Capítulo 6

Clientes

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

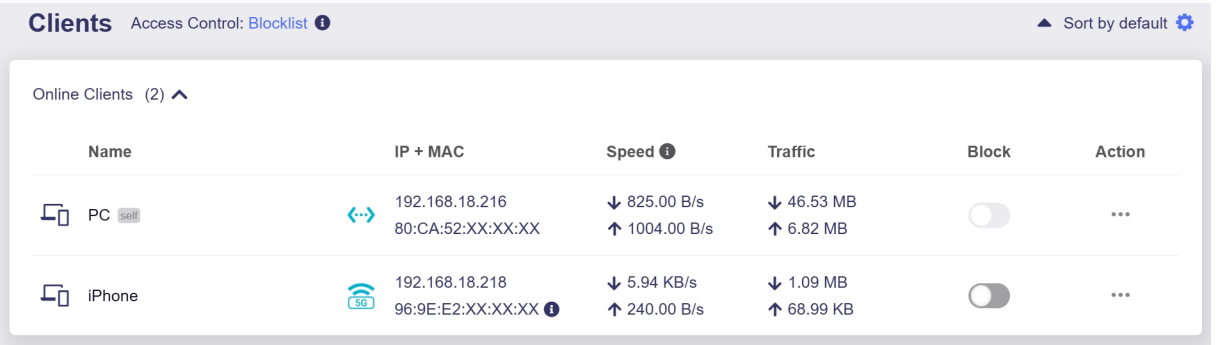
Inicie sesión en el enrutador’s web admin panel y navegue hasta **CLIENTES**.

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



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

6.1 Detalles del dispositivo



1. **Nombre del dispositivo**

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

2. **Dirección IP y MAC**

   La segunda columna enumera las direcciones IP y MAC del dispositivo conectado. Si los dispositivos conectados utilizan direcciones MAC aleatorias , aparecerá un mensaje, que indica que esto es una dirección MAC aleatoria.



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

3. **Velocidad**

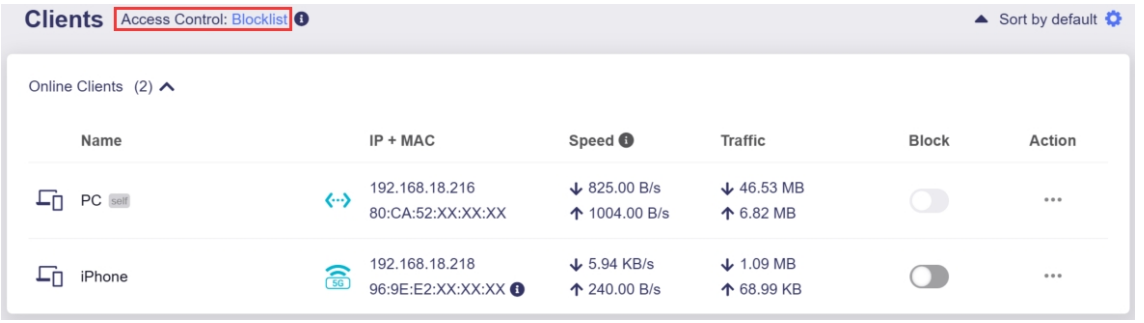
   La tercera columna muestra la velocidad de Internet del dispositivo conectado. Laes velocidad representa la velocidad promedio durante los últimos 3 minutos. El sistema comienza a calcular la velocidad promedio cuando se abre esta página (por ejemplo, si la página solo ha estado abierta durante 10 segundos,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

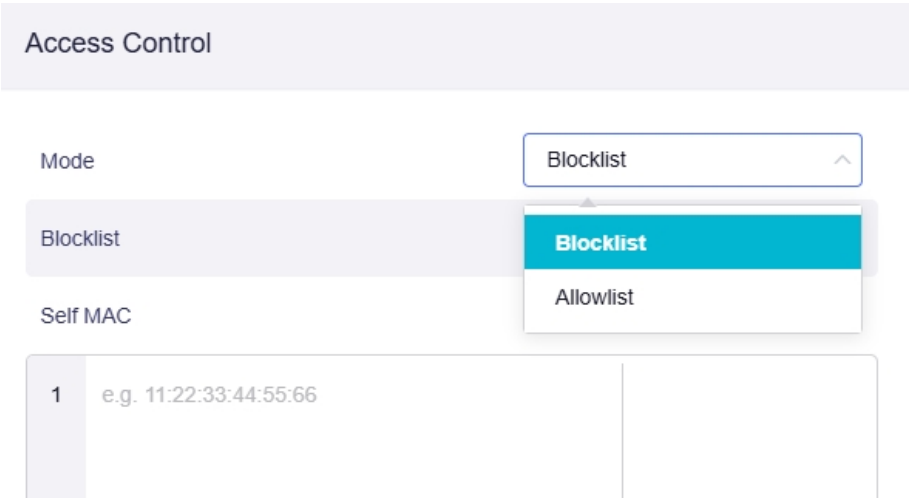
4. **Tráfico**: La cuarta columna muestra el tráfico de Internet del dispositivo conectado.

5. **Lista de bloqueo**

En la quintaésima columna, puede bloquear dispositivos conectados específicos con un clic.

El Unacceso Cla regla de control es Lista de bloqueo de forma predeterminada y puede cambiarla a Lista de permitidos desde la parte superior si es necesario.



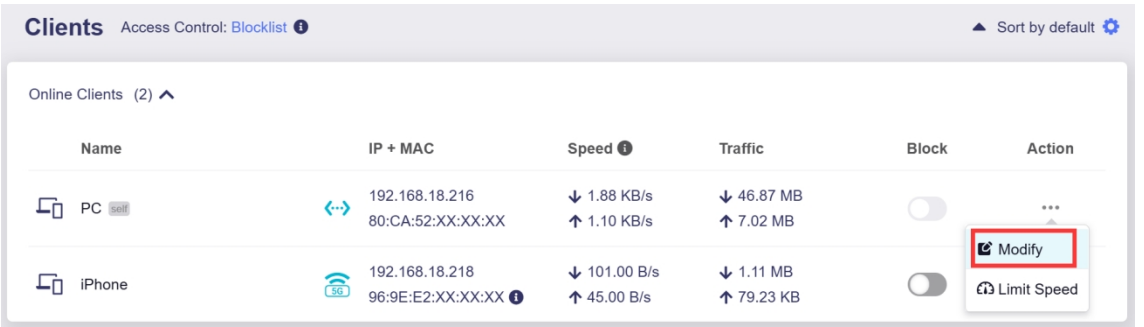


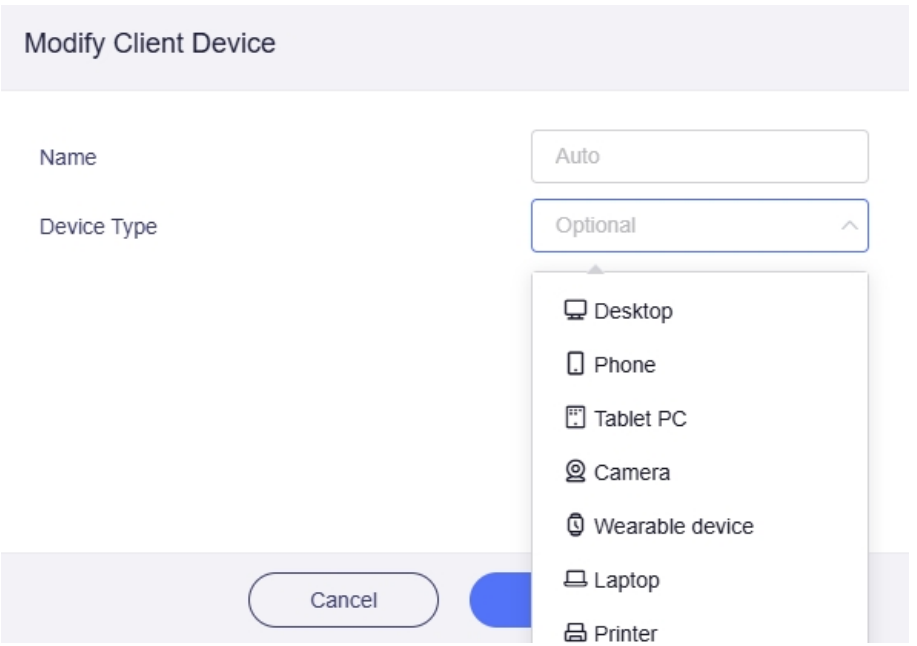
- **Lista negra**: Dispositivos con direcciones MAC en el negrolist no puede conectarse a este enrutador. Tenga en cuenta que el bloqueo del cliente se basa en la dirección MAC del dispositivo. Si el dispositivo bloqueado usa una dirección MAC diferente la próxima vez, aún podrá conectarse al enrutador.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

6.2 Acción

1. **Modificar**

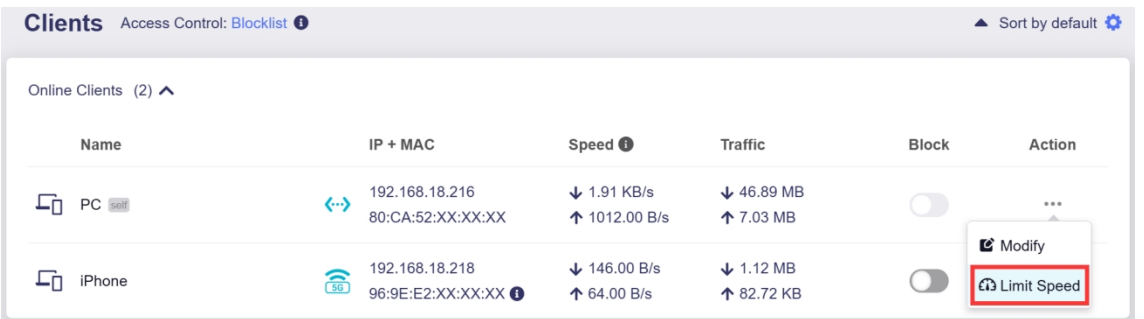
   Haga clic en el icono de tres puntos en **Acción** y haga clic en **Modificar** desde el menú desplegable para modifique el nombre y tipo del dispositivo.



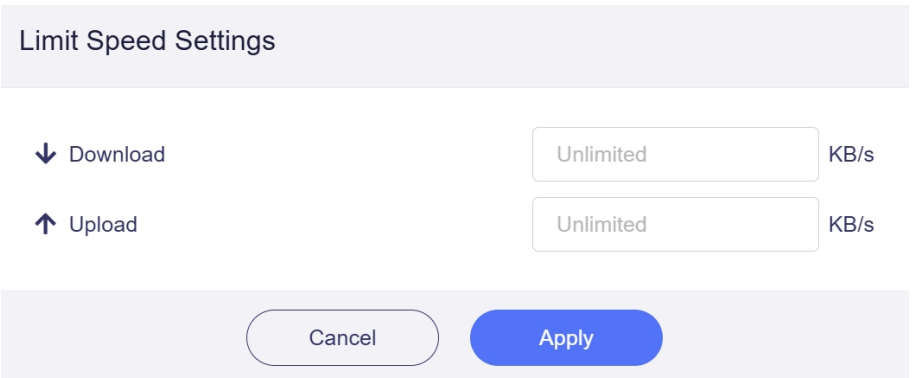


2. **Limitar velocidad**

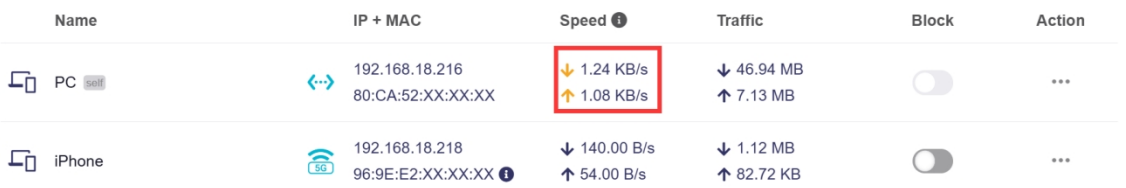
   Haga clic en el icono de tres puntos en la **Acción** columna y haga clic en **Limitar velocidad** en el menú desplegable.



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

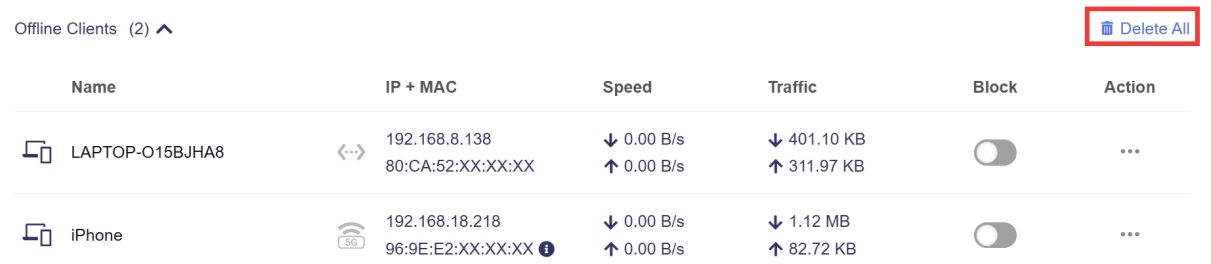


Si se ha aplicado una limitación de velocidad a un dispositivo, las flechas de velocidad de carga/descarga girarán amarillo.

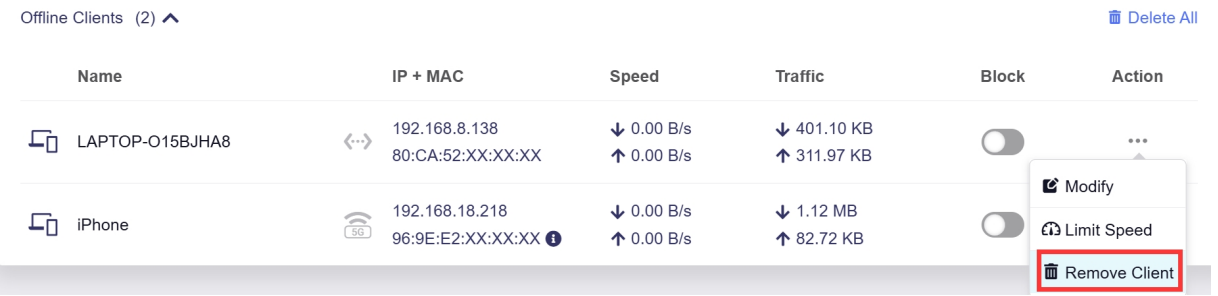


6.3 Eliminar clientes

En **Osin conexión Cclientes** sección, puede hacer clic en **Eliminar todo** en la esquina para eliminar todos los clientes sin conexión.

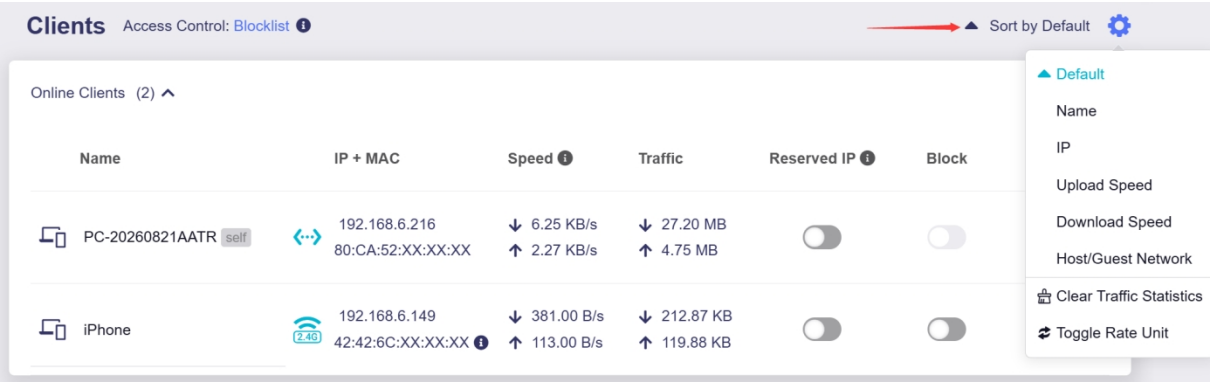


Si desea eliminar un cliente específico, haga clic en el ícono de tres puntos en la columna **Acción**, luego haga clic en **Eliminar cliente** de el desplegable menú.



6.4 Ordenar

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



El orden predeterminadoing es como siguiente:

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

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

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



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

Capítulo 7

Conozca la VPN

Este capítulo presenta VPN conceptos y uso común 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 sitios privados o restringidos. redes.

Enrutador VPN

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

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

OpenVPN

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

WireGuard

WireGuard es un protocolo VPN ligero, 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

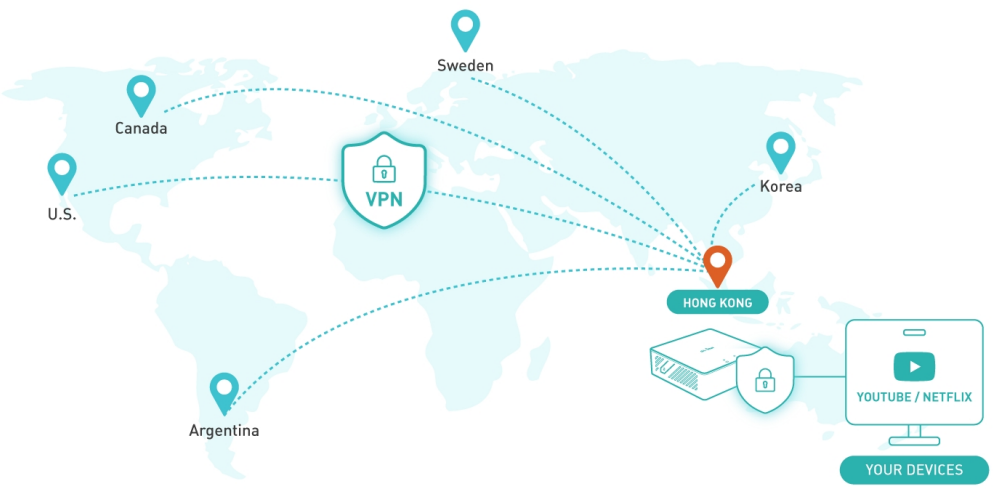
1. **Datos personales Privacidad**

   El servicio VPN es compatible con una amplia gama de dispositivos a través de nuestro enrutador, incluidos solo computadoras portátiles, teléfonos y tabletas, sino también consolas de juegos, televisores y dispositivos de transmisión. Tus datos estarán protegidos ya sea a través de conexiones inalámbricas o por cable. Incluso puedes personalizar políticas de VPN para lograr una protección flexible para ciertos dispositivos.



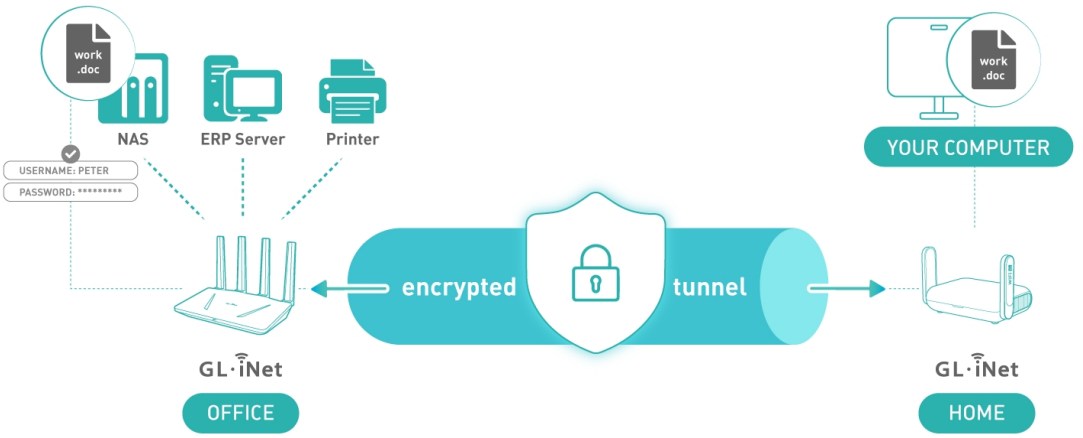
2. **Acceso sin restricciones en todo el mundo**

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



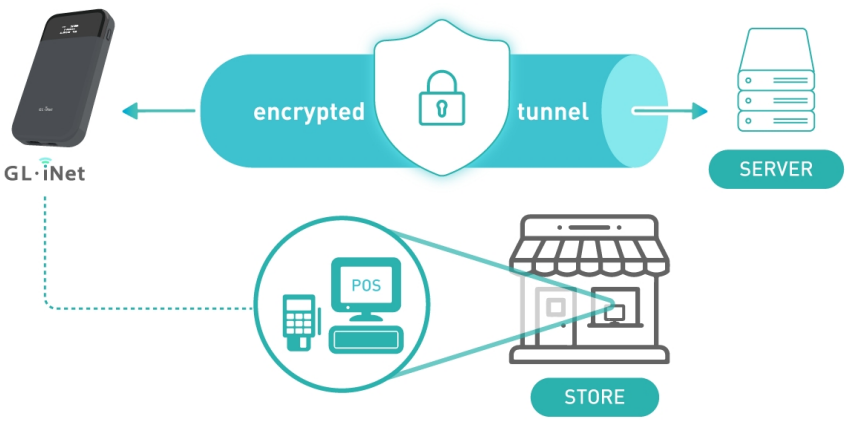
3. **Seguridad de datos para pequeñas empresas**

Muchas personas trabajan en-espacios de trabajo o cafeterías y dependen de servicios públicos gratuitos. Wi- 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 pequeños propietarios minoristas deben manejar las credenciales de pago de los clientes cuando realizan negocios en el sitio. Usando una VPN enrutador, su máquina POSs puede cargar información de tarjetas de crédito a través de una VPN cifrada tunnel para garantizar la seguridad de los pagos.



Capítulo 8

Panel de VPN

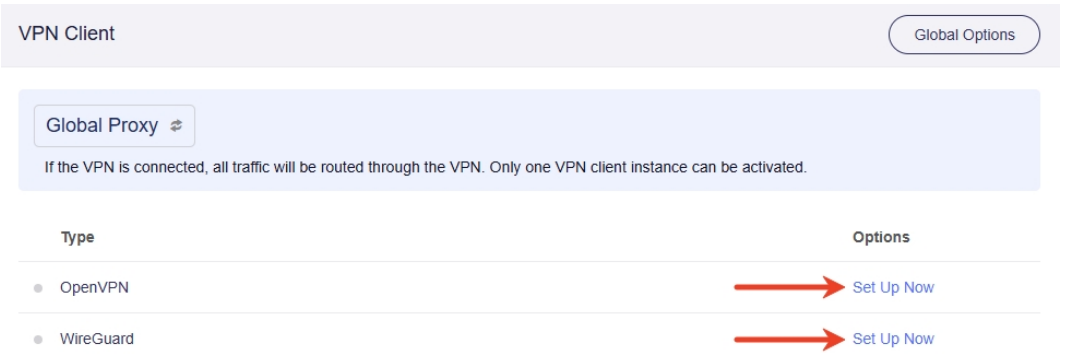
Este capítulo presenta cómo administrar conexiones VPN a través del panel de administración web.

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

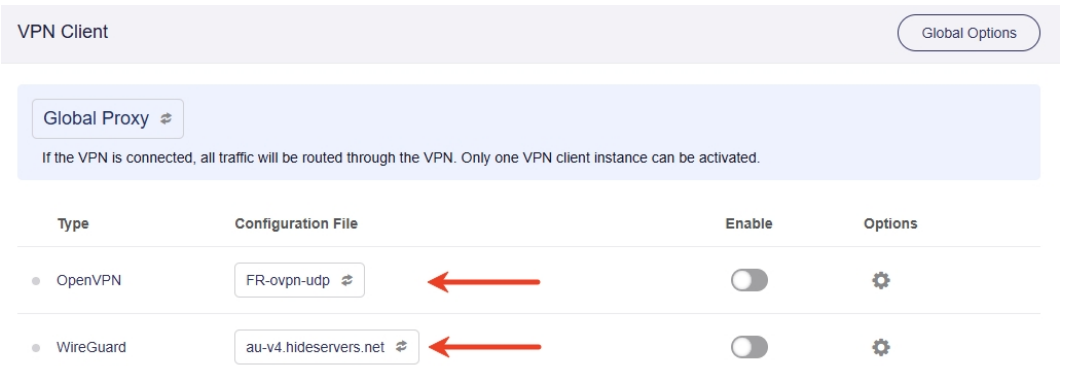
Cuando el enrutador está configurado como un cliente VPN activo, el El panel de VPN muestra detalles de la conexión VPN, como la dirección del servidor, estadísticas de tráfico, IP virtual del cliente y registro de conexión. También le permite configurar ajustes avanzados como Bloquear tráfico que no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

8.1 Cliente VPN

Cuando ingresa al **Panel de VPN** por primera vez y no hay archivos de configuración OpenVPN o WireGuard disponibles, la página se muestra de la siguiente manera. Haga clic en **Establecer Up Now** y serás dirigido a la página **Cliente OpenVPN** o **Cliente WireGuard** para cargar tu archivo de configuración de VPNs.

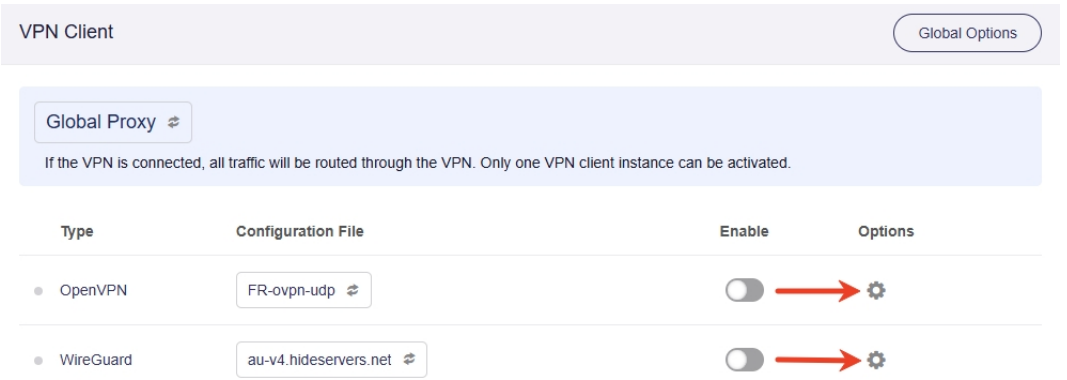


Una vez cargada, su configuración se mostrará en la columna **Archivo de configuración**. Si tiene varios archivos de configuración cargados, puede cambiar de archivo haciendo clic en el cuadro.

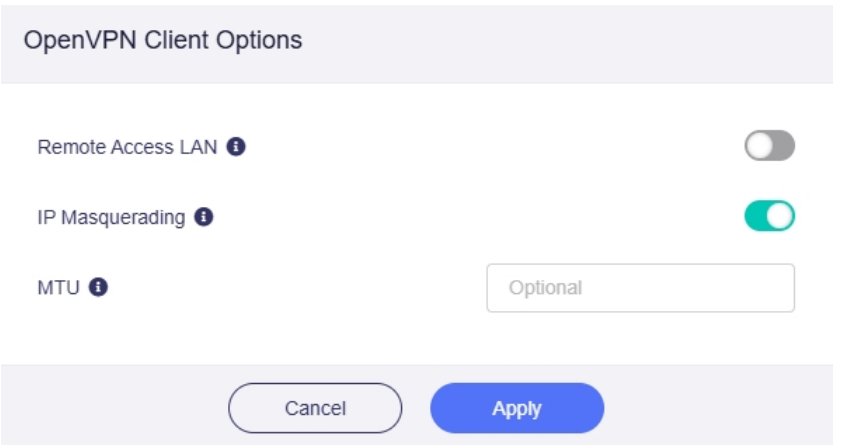


8.1.1 Opciones del cliente

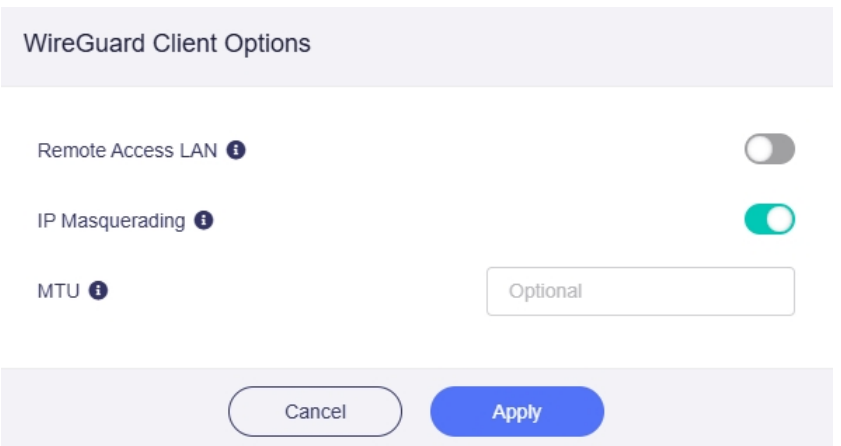
Haga clic en el ícono de ajustes a la derecha para acceder a las opciones del cliente OpenVPN o WireGuard.



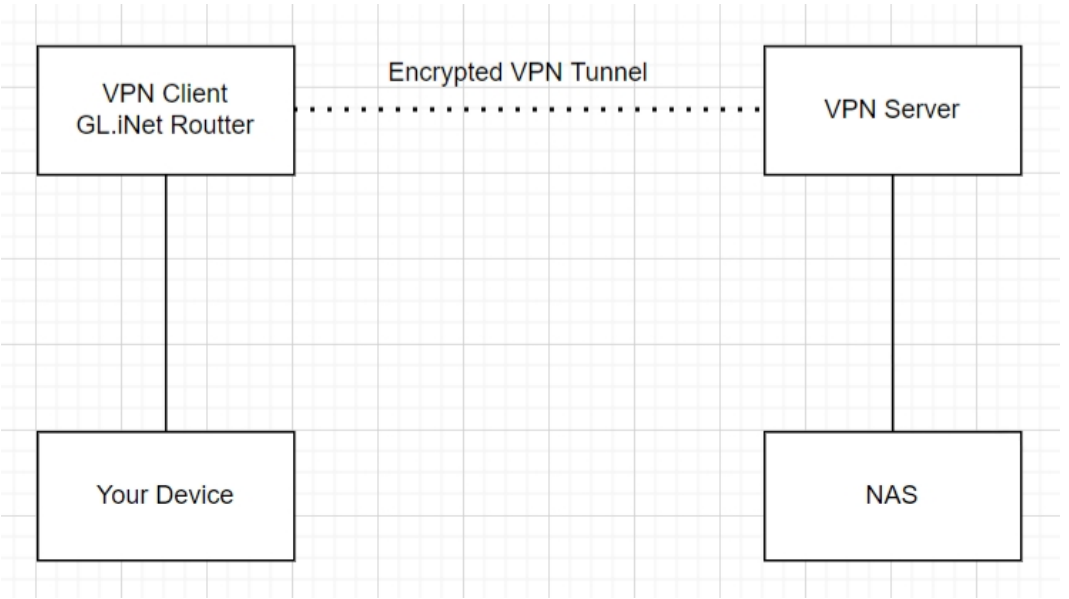
Las opciones del cliente OpenVPN se muestran de la siguiente manera.



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



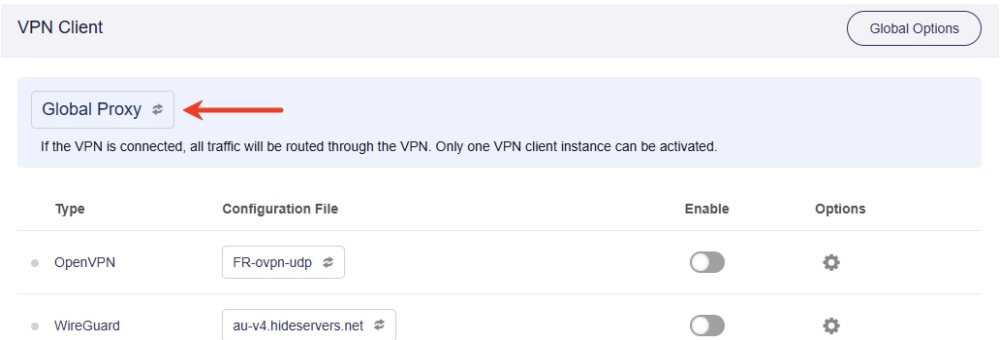
- **LAN de acceso remoto**: si está habilitado, acceso remoto a este enrutador y sus dispositivos LAN a través de VPN será permitido. El servidor VPN debe anunciar una ruta a la subred LAN de este enrutador.
  Por ejemplo, como se muestra en el siguiente diagrama, el enrutador GL.iNet se ejecuta como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



- **Enmascaramiento de IP**: si está habilitado, las direcciones IP de origen de los clientes LAN se reescribirán en la IP del túnel VPN del enrutador. Desactive 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 de política

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



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

1. **Proxy global**

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

2. **Modo de política**

   Este modo se puede dividir en tres políticas.

   - **Según el dominio 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**

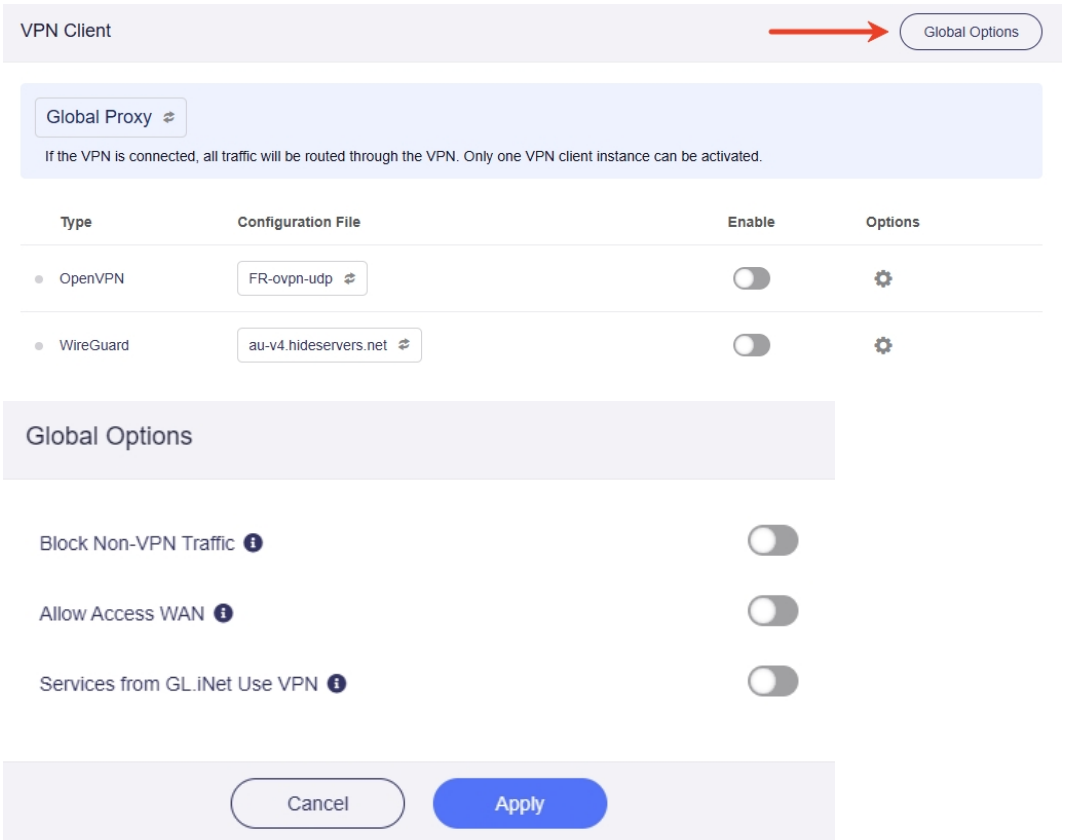
     Se utilizarán las reglas de enrutamiento definidas en cada archivo de configuración de cliente VPN o emitidas por el servidor VPN.

   - **Personalizar reglas de enrutamiento**

     Puedes configurar manualmente reglas de enrutamiento para cada cliente VPN instancia.

8.1.3 Opciones globales

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



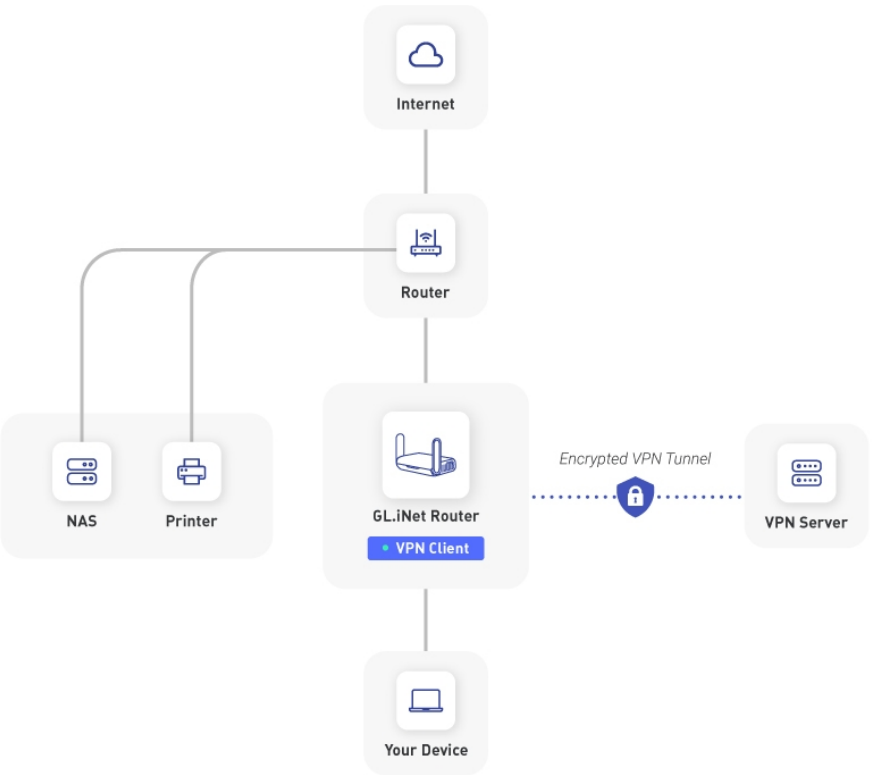
- **Bloquear tráfico que no sea VPN**: si está habilitado, todo el tráfico de Internet se ve obligado a pasar exclusivamente a través del túnel VPN y no se puede enrutar a través de otras interfaces como la WAN del ISP local. Si la conexión VPN se cae inesperadamente, todo el tráfico de Internet se bloquea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

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

  a. Fuga de DNS
  b. Fuga de IPv6

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

- **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.



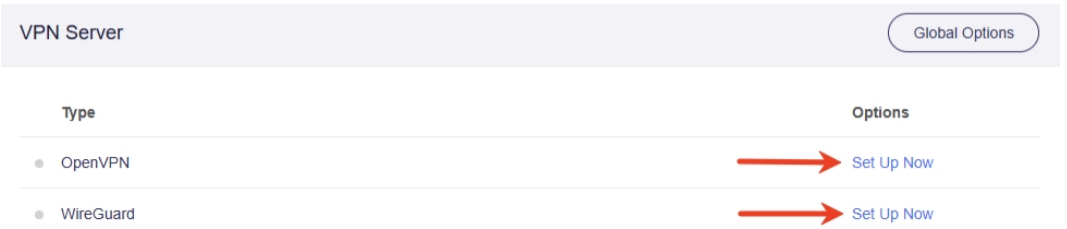
Como se muestra en el diagrama anterior, habilitar esta función permite que sus dispositivos locales lleguen a los hosts en la subred ascendente, como impresoras y NAS.

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 acceso a WAN** y **Bloquear tráfico no VPN** son mutuamente excluyentes y no se pueden habilitar simultáneamente.

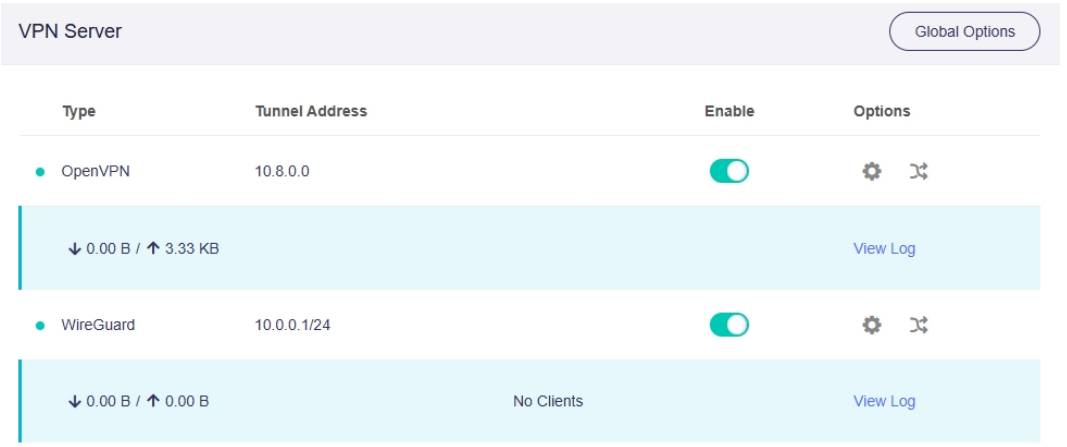
- **Servicios de GL.iNet usan VPN**: si están habilitados, los servicios GoodCloud, DDNS y rtty transmitirán paquetes a través de túneles VPN. Esta opción está deshabilitada de forma predeterminada, ya que estos servicios normalmente requieren la dirección IP real del dispositivo para funcionar correctamente.

8.2 Servidor VPN

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

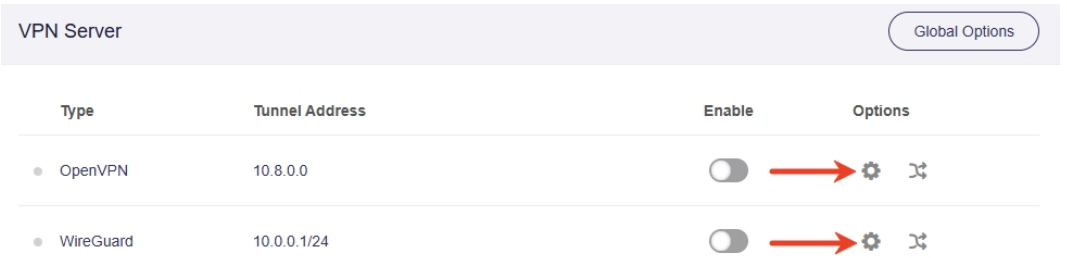


Después de habilitar el servidor OpenVPN o WireGuard, la página mostrará el estado del servidor de la siguiente manera.

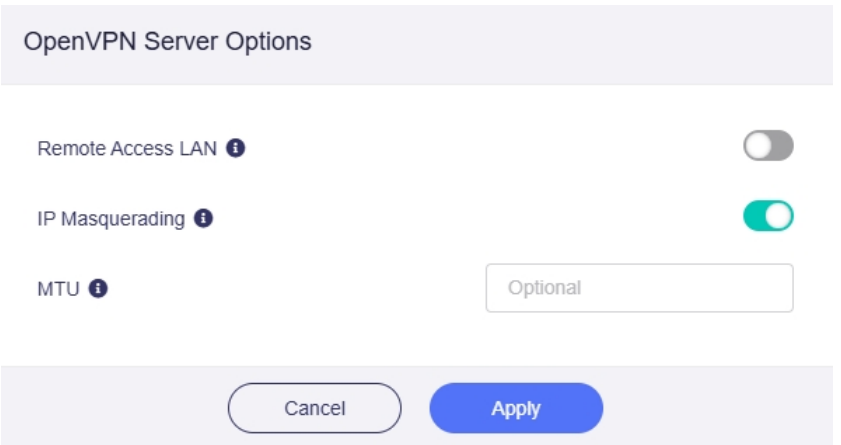


8.2.1 Opciones del servidor

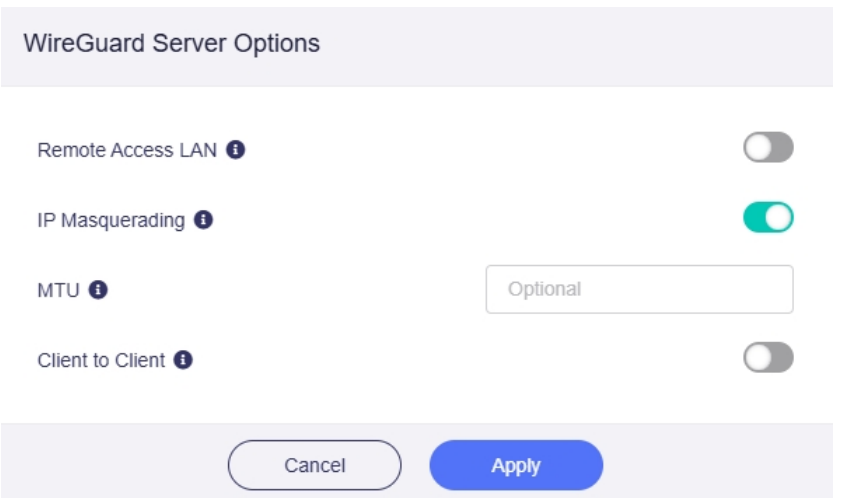
Haga clic en el ícono de ajustes a la derecha para acceder a las opciones del servidor OpenVPN o WireGuard.



Las opciones del servidor OpenVPN se muestran a continuación.



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

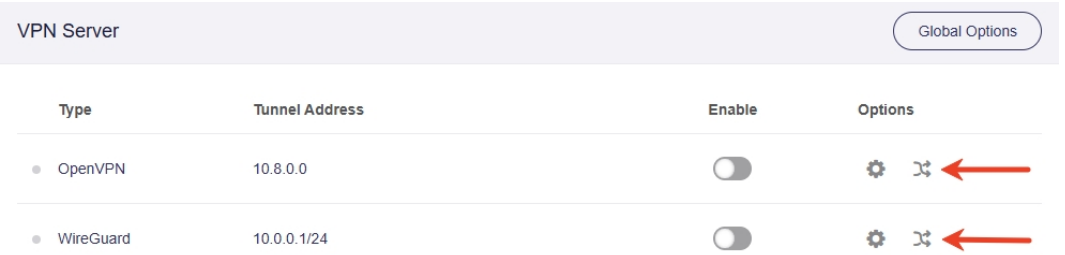


- **LAN de acceso remoto**: si está habilitado, se puede acceder a los recursos dentro de la subred LAN del servidor a través del túnel VPN.

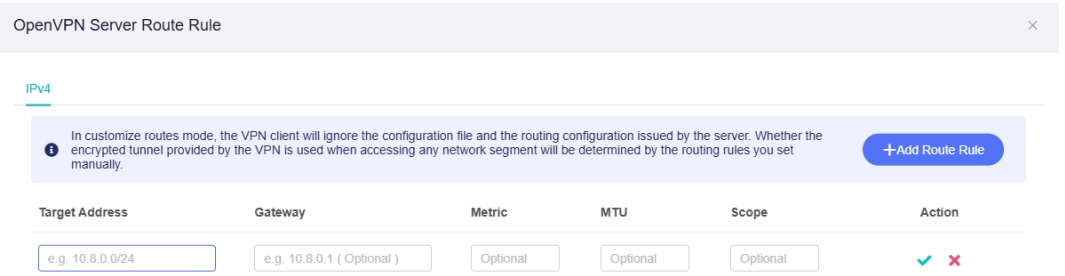
- **Enmascaramiento de IP**: si está habilitado, las direcciones IP de origen de los clientes LAN se reescribirán en la IP del túnel VPN del enrutador. Desactive esto solo para configuraciones de sitio a sitio donde el par remoto conoce sus subredes LAN.
- **MTU**: abreviatura de Unidad de transmisión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

8.2.2 Regla de ruta del servidor

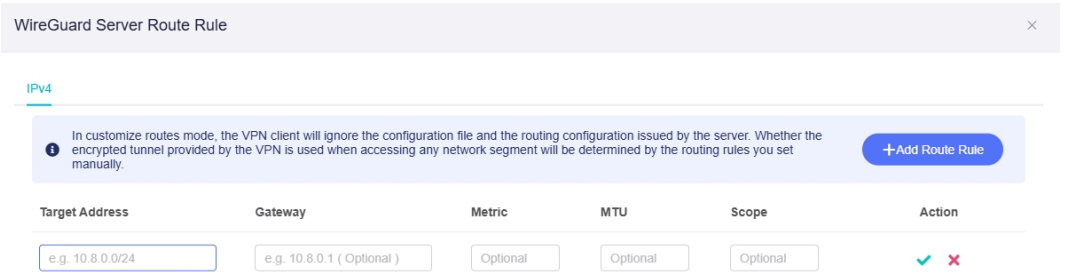
Haga clic en el icono de ruta a la derecha para personalizar las reglas de ruta OpenVPN o WireGuard como necesario.



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 en ícono de verificación verde para aplicar.



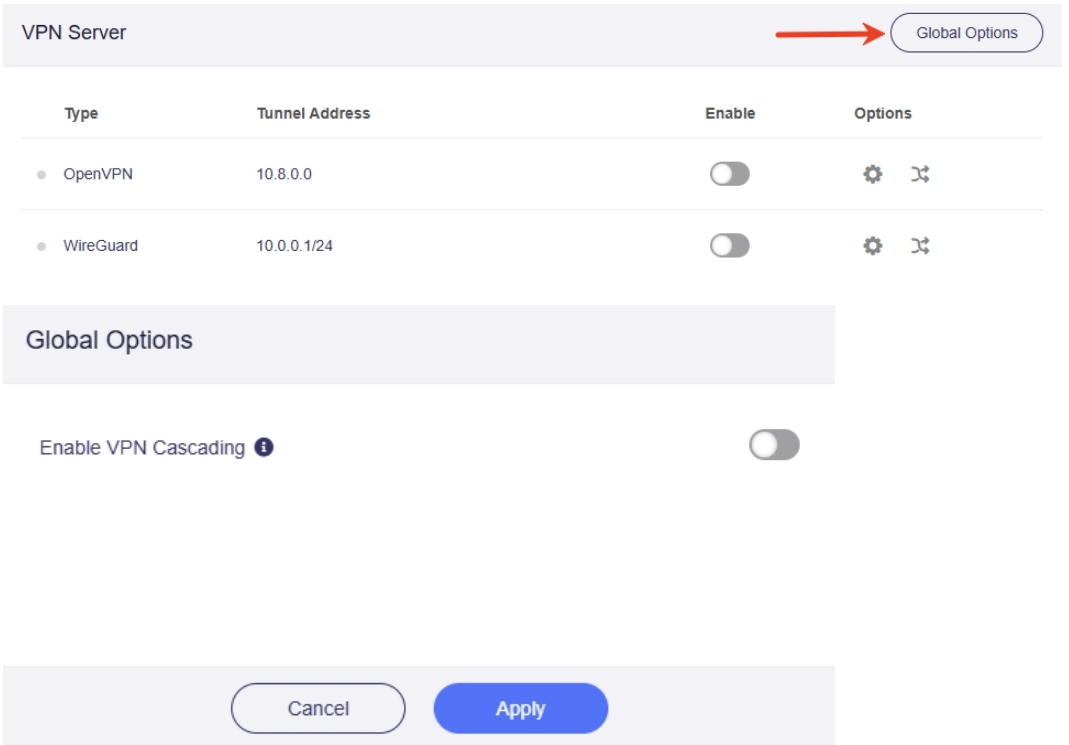
La regla de ruta del servidor WireGuard se muestra de la siguiente manera. Haga clic en **Agregar regla de ruta**, ingrese la **Dirección de destino** y **Puerta de enlace** y luego haga clic en el ícono de verificación verde. para aplicar.



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

8.2.3 Opciones globales

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



Si **VPN en cascada** está habilitado, cuando este enrutador actúa como una VPN servidor y un 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 está utilizando como cliente VPN. Más información sobre VPN en cascada.

Capítulo 9

Configurar el servidor VPN

Este capítulo presenta cómo configurar una 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 conexiones seguras punto a punto y de sitio a sitio. Para configurar el servidor OpenVPN en un enrutador GL.iNet, mire este video o consulte los pasos a continuación.

9.1.1 Preparación

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

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

   Si no, su enrutador no se puede configurar como servidor OpenVPN.

   Métodos alternativos:

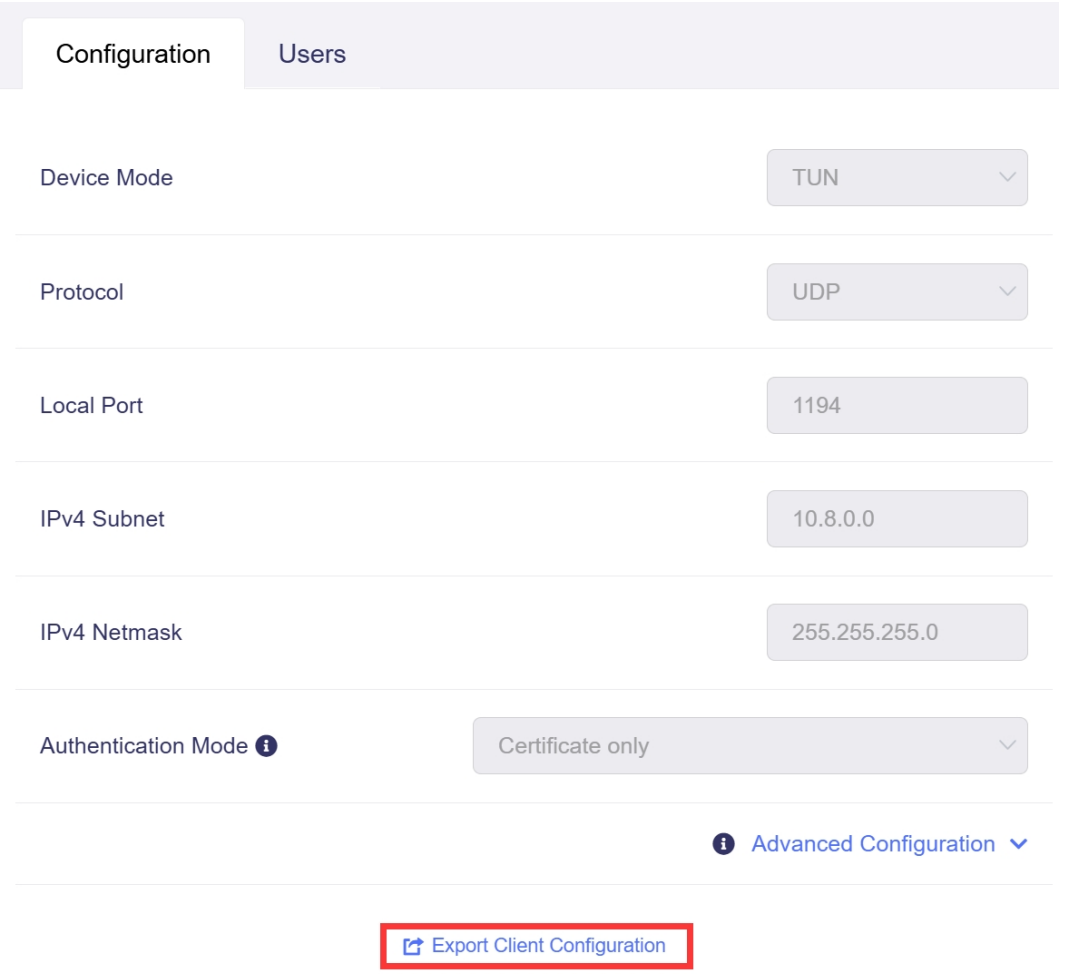
   - Si tiene un enrutador principal aguas arriba de su enrutador GL.iNet, inicie sesión en él y verifique que tenga una dirección IP pública asignada por su ISP.
   - Pregunte Solicite a su ISP una dirección IP pública. Esto puede generar un cargo adicional.

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

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

9.1.2 Pasos de configuración

1. Inicie sesión en el panel de administración web del enrutador, navegue hasta **VPN** > **Servidor OpenVPN**, 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.



- **Modo de dispositivo**: 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 cliente y las incrustará en el archivo de

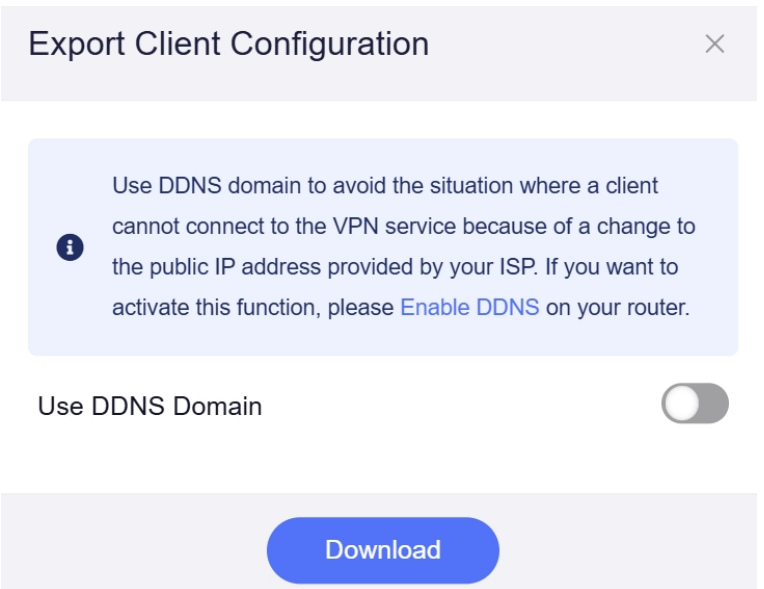
configuración. Cuando carga la configuración en el cliente, no se requieren credenciales adicionales.

- **Solo nombre de usuario/contraseña**: si se selecciona, el enrutador generará la configuración del cliente sin claves de certificado. Usted necesita primero agregar un nombre de usuario y contraseña en la pestaña **Usuarios** antes de exportar la configuración del cliente. Al cargar la configuración al cliente, ingrese estas credenciales para la autenticación.
- **Nombre de usuario/contraseña y certificado**: si está seleccionado, necesita primero agregar un nombre de usuario y una contraseña en la pestaña **Usuarios** antes de exportar la configuración del cliente; en segundo lugar, el enrutador generará automáticamente claves de certificado de servidor y cliente y las incrustará en el archivo de configuración. Al cargar la configuración 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 si es necesario.

3. Exportar configuración del cliente.

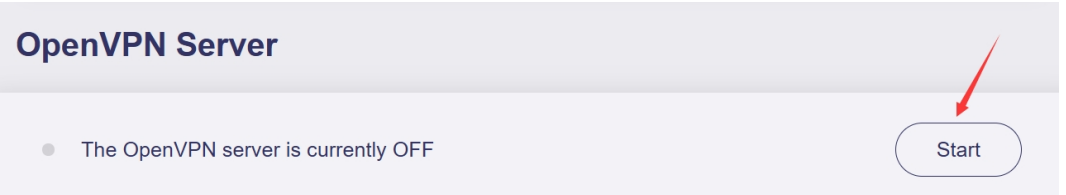
   Después de hacer clic **Exportar configuración del cliente** en la parte inferior de la pestaña Configuración (o aplicar la configuración modificada), aparecerá una ventana como la siguiente. Haga clic en **Descargar** para exportar la configuración.



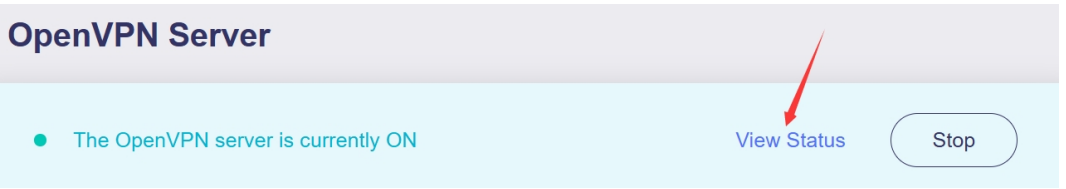
Consejo: Si su IP pública dirección cambia con frecuencia, vaya a **APLICACIONES** > **DNS dinámico** y habilitar DDNS. Luego puede usar el dominio DDNS como su dirección de servidor.

4. Inicie el servidor OpenVPN.

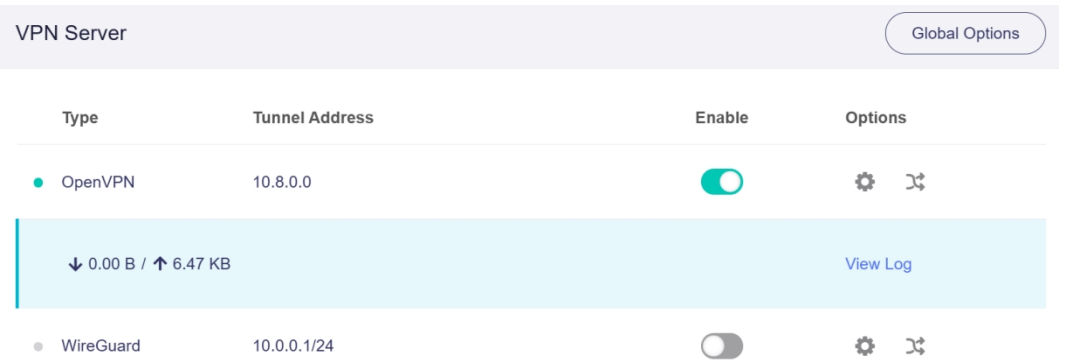
   En la página **Servidor OpenVPN**, haga clic en **Iniciar** en la esquina superior derecha para iniciar el servidor.



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



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



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 vídeo o consulte los pasos a continuación.

9.2.1 Preparación

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

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

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

   Métodos alternativos:

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

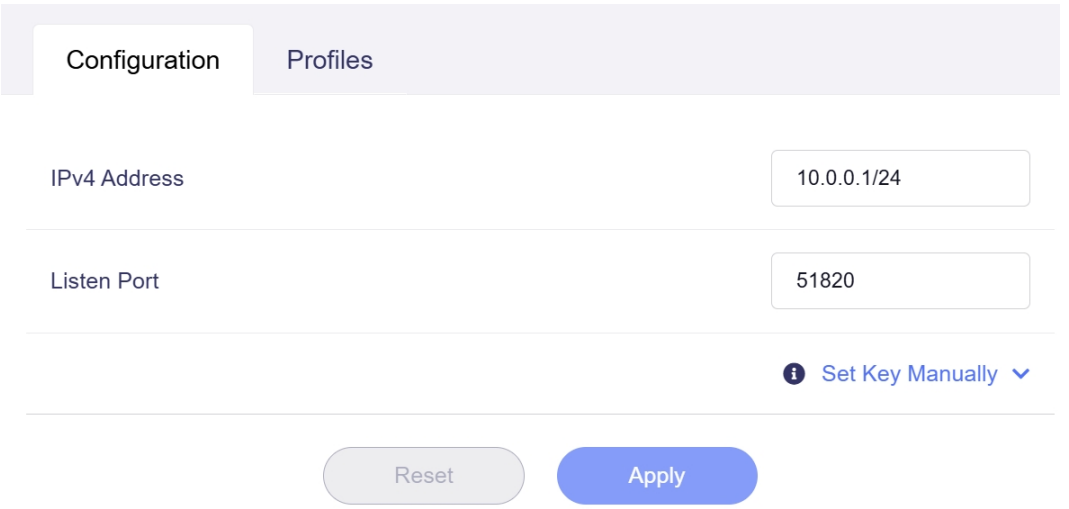
2. **Confirme si se requiere reenvío de puerto**

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

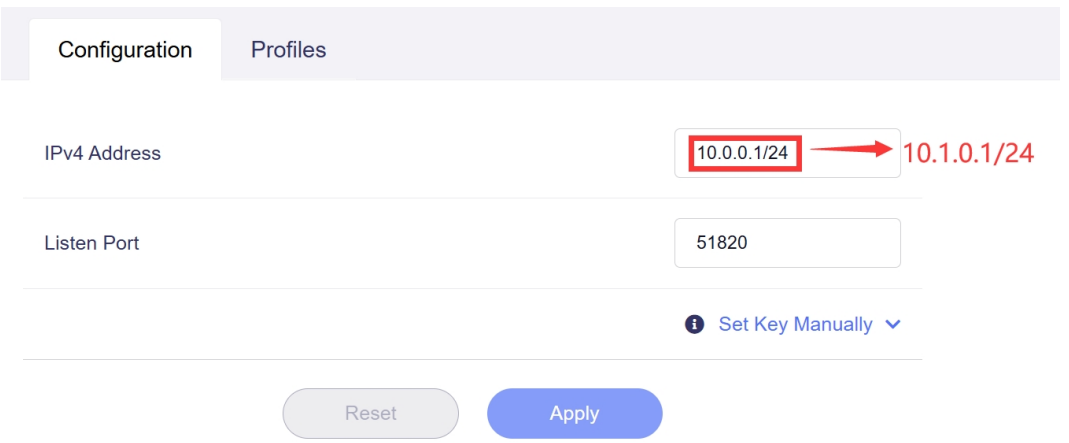
9.2.2 Pasos de configuración

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 el 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.

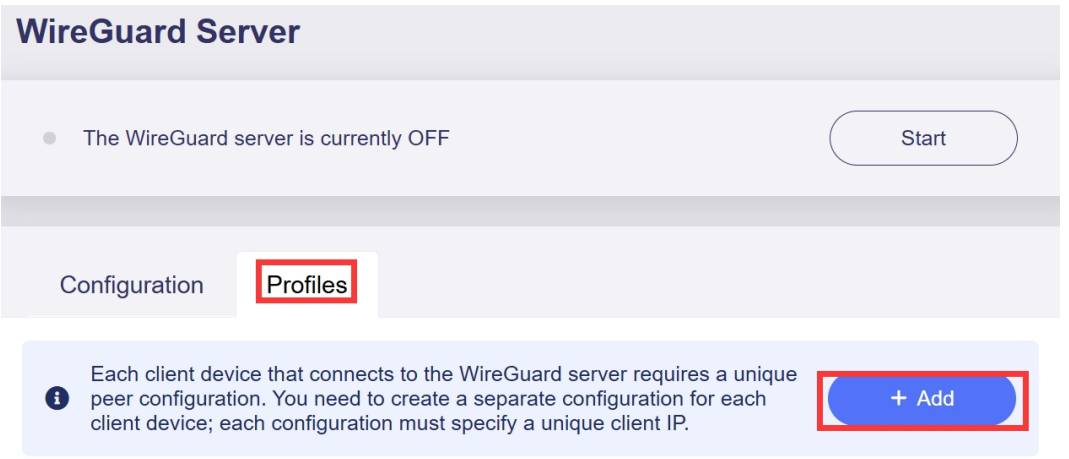


   Si el La dirección IPv4 entra en conflicto con la puerta de enlace de su enrutador ascendente, modifique la dirección IPv4 a otra una (por ejemplo, **10.1.0.1/24**) y haga clic en **Aplicar**. Asegúrese de que se incluya la notación CIDR "/24" para evitar problemas de conectividad.

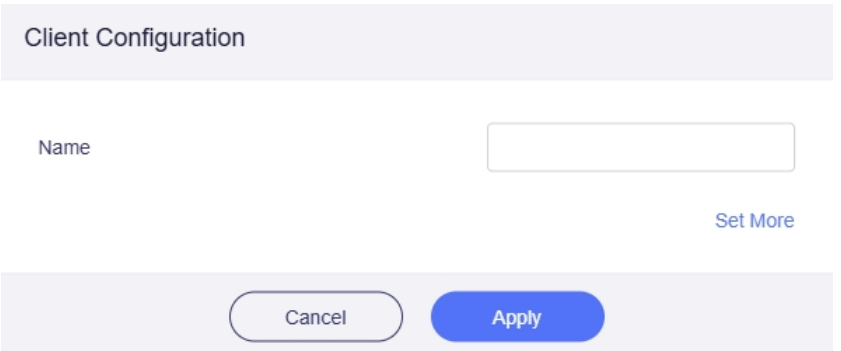


3. Agregue un perfil.

Cambiar a **Perfiles** , haga clic en el botón **Agregar** para generar un perfil para su dispositivo.



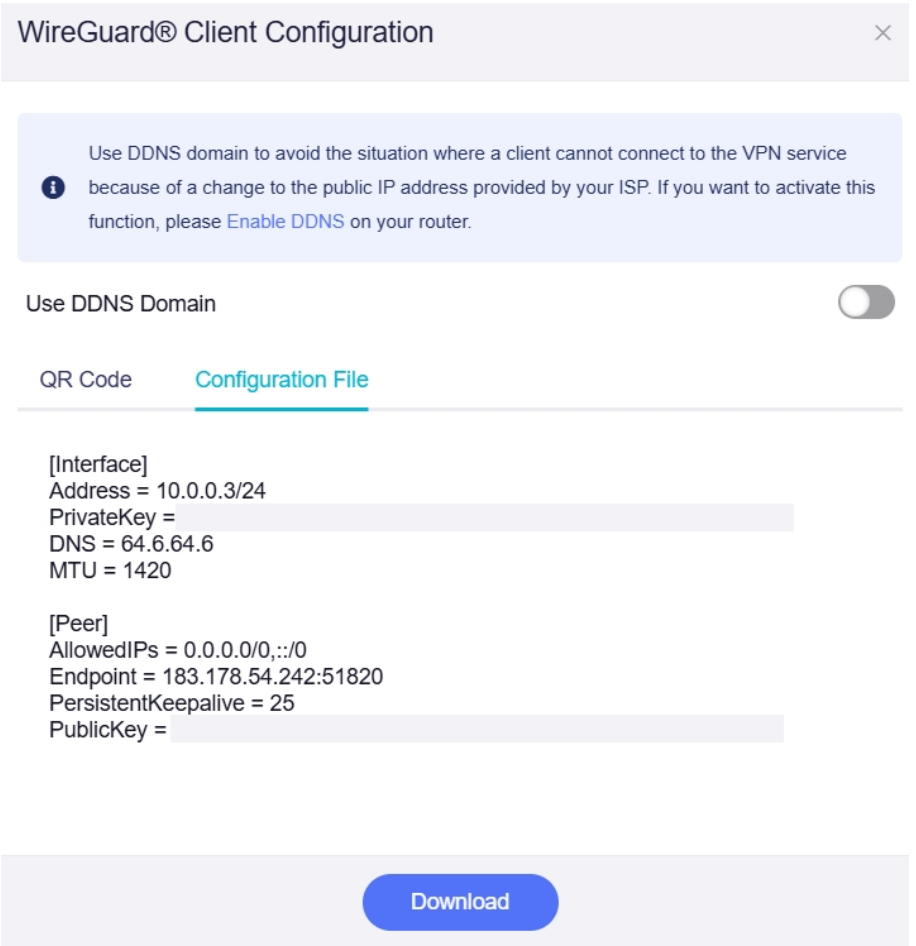
Establezca un nombre descriptivo y haga clic en **Aplicar** para continuar.



4. Descargar configuración.

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

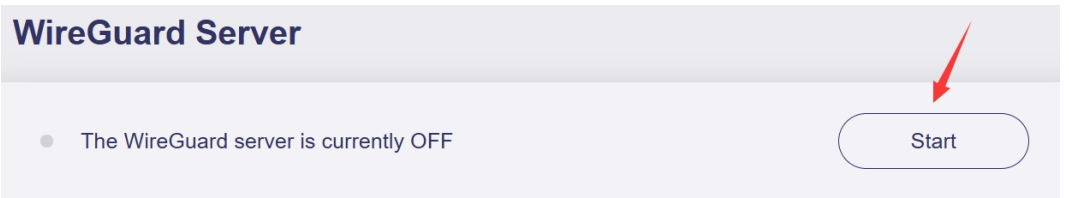
   - **código QR**: Adecuado para dispositivos (por ejemplo, teléfonos inteligentes, tabletas, computadoras portátiles) con la aplicación WireGuard instalada. Si desea configurar un dispositivo específico como cliente WireGuard, simplemente abra la aplicación WireGuard y escanee el código QR para importar un archivo de configuración.
   - **Texto sin formato**: en texto sin formato formato, puede revisar los detalles de configuración y copiarlos y pegarlos cómodamente en otro lugar para la configuración manual, como la aplicación WireGuard o un enrutador GL.iNet.
   - **archivo .conf**: haga clic en **Descargar** para guardar el archivo .conf en su dispositivo local. También es conveniente y se puede cargar directamente en la aplicación WireGuard o en un enrutador GL.iNet.



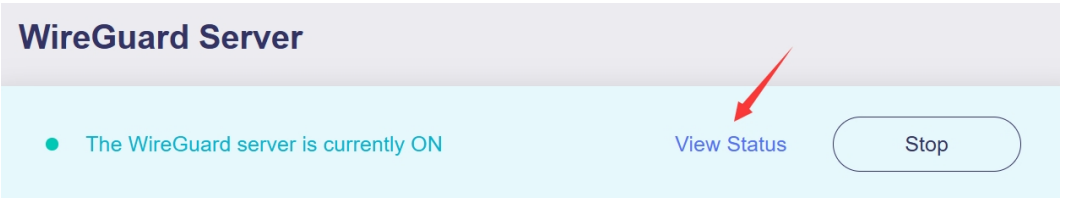
Consejo: Si su dirección IP pública cambia con frecuencia, vaya a **APLICACIONES** > **DNS dinámico** y habilitar DDNS. Luego puede usar el dominio DDNS como su dirección de servidor.

5. Inicie el servidor WireGuard.

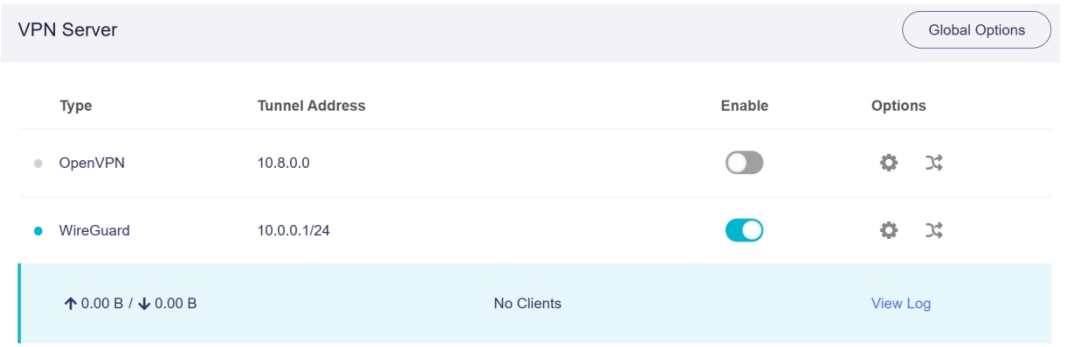
   En la página **Servidor WireGuard**, haga clic en **Iniciar** en la esquina superior derecha para iniciar el servidor.



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



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



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 necesites 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.

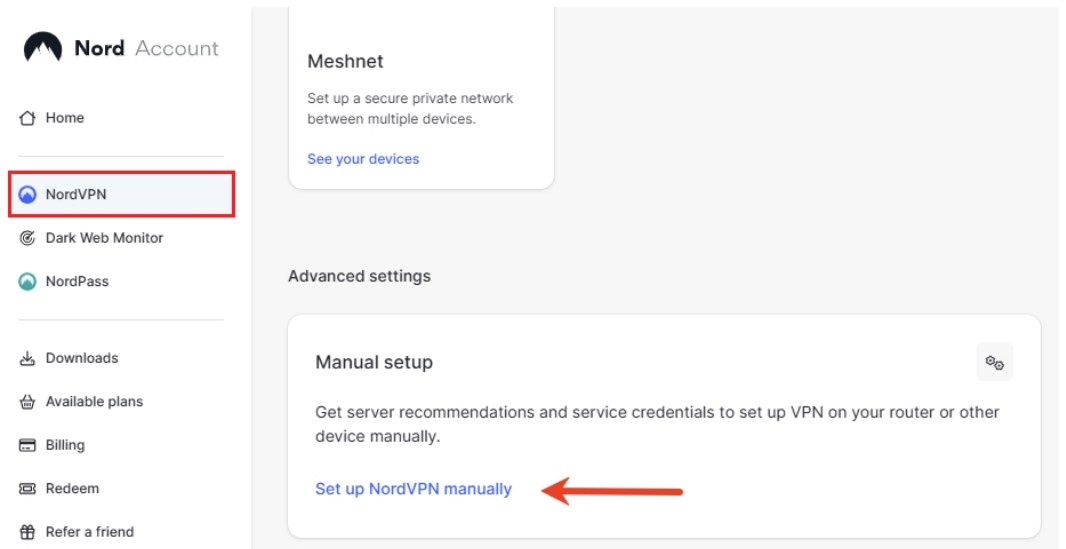
Siguiente, visite el sitio web oficial del proveedor de servicios VPN al que se suscribió y obtener las credenciales de servicio o el archivo de configuración. Si no sabe cómo obtener el archivo de configuración, consulte este enlace o póngase en contacto con su soporte.

10.1.2 Configurar NordVPN

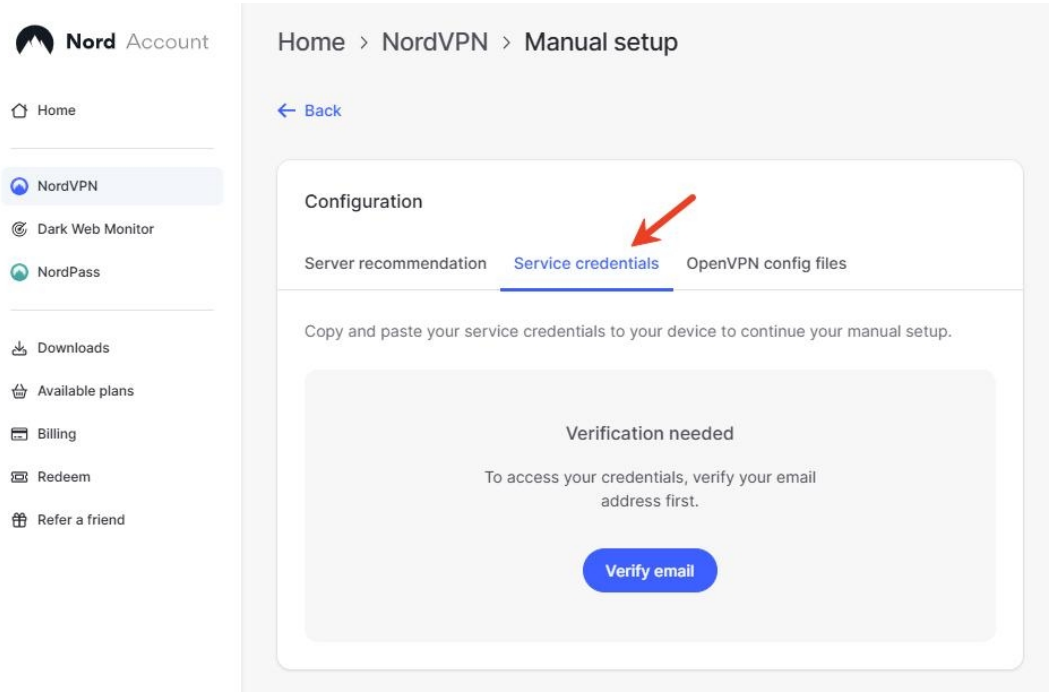
NordVPN está integrado en el panel de administración GL.iNet web . Puede adquirir archivos de configuración para todos los servidores NordVPN introduciendo las credenciales de su cuenta (obtenidas del Panel de NordVPN) en el panel de administración web del enrutador o en la aplicación móvil GL.iNet ,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

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

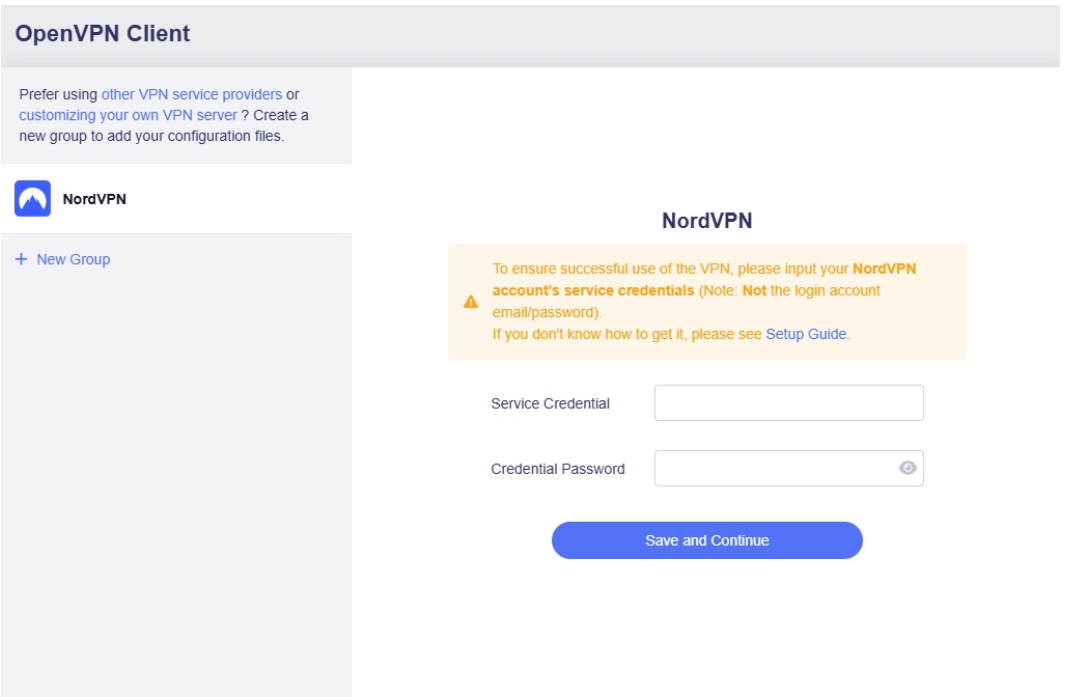
1. Inicie sesión en su cuenta web de NordVPN aquí.
2. Oen el Panel de Nord, haga clic en **NordVPN**, luego haga clic en **Configurar NordVPN manualmente**.



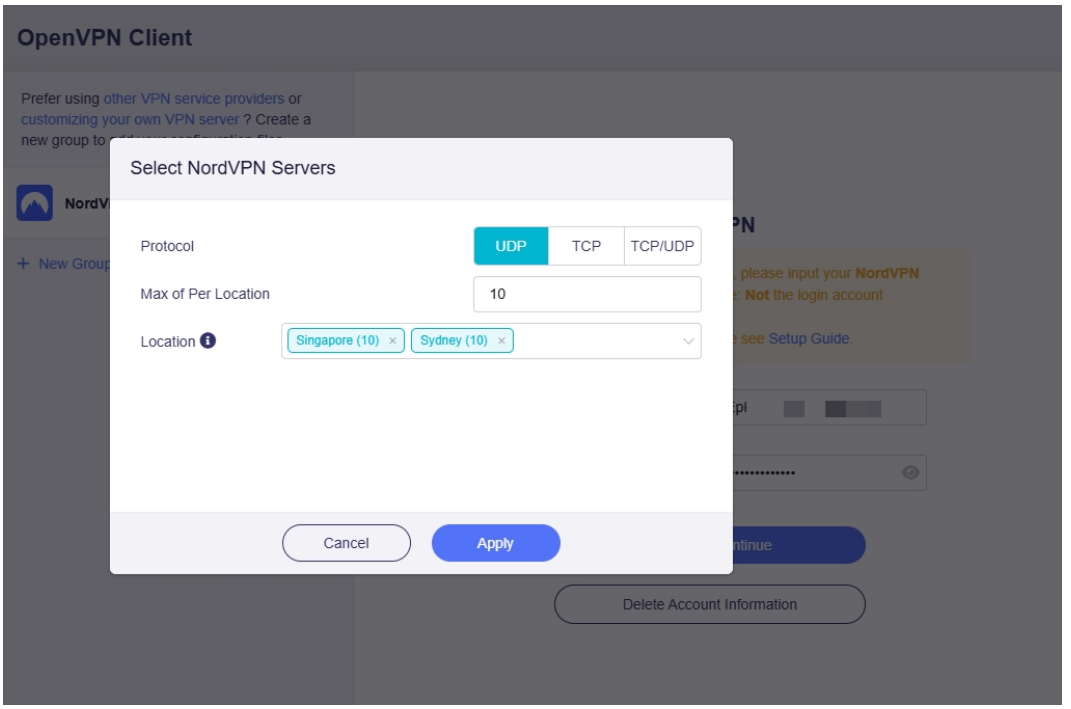
Encontrará las **credenciales de servicio**. Cópialos para usarlos más adelante.



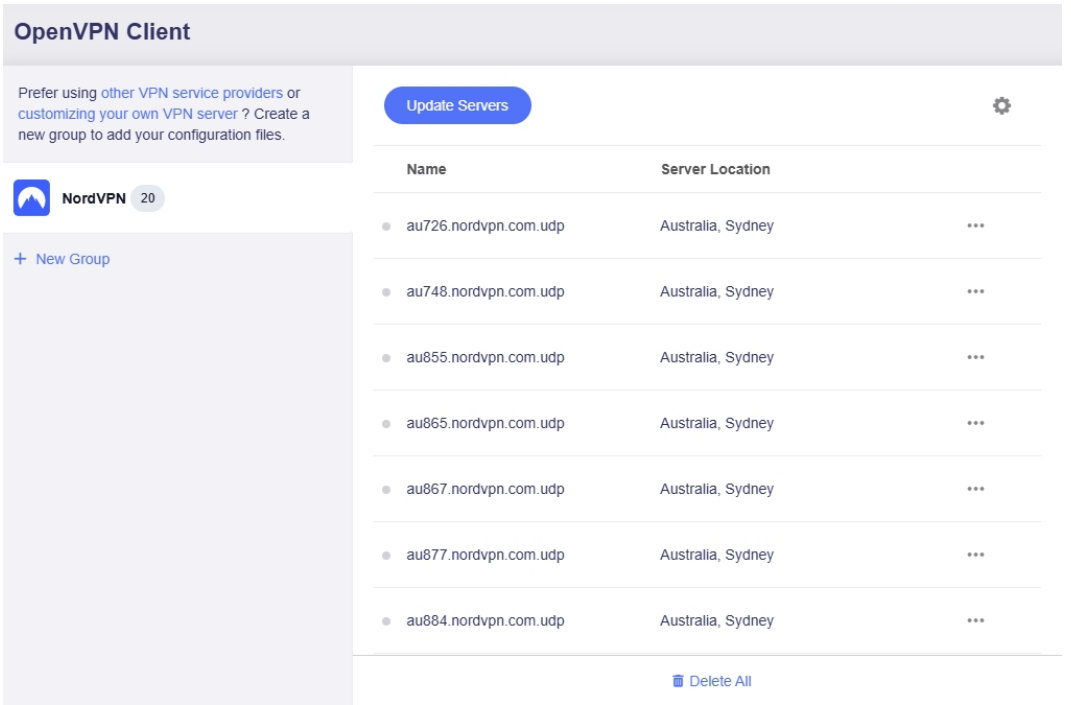
3. Inicie sesión en el panel de administración web de su enrutador y navegue a **VPN** > **Cliente OpenVPN** > **NordVPN**. Ingrese las credenciales de servicio (Nota: NO es el correo electrónico ni la contraseña de la cuenta de inicio de sesión), luego haga clic en **Guardar y continuar**.



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

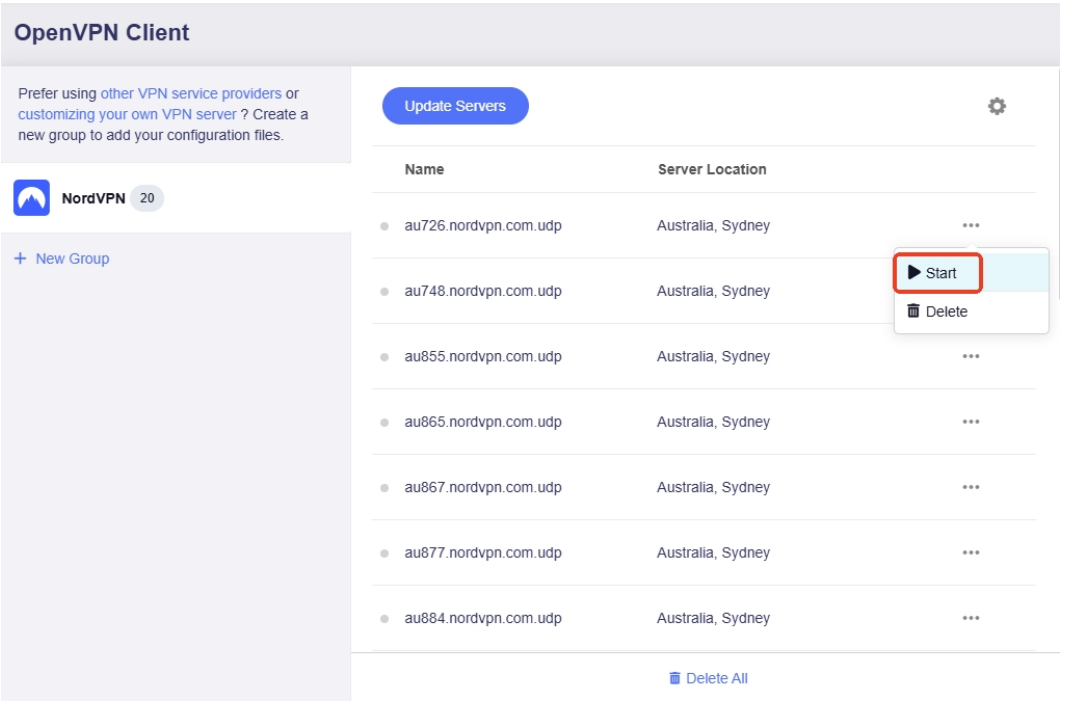


Descargará los archivos de configuración.

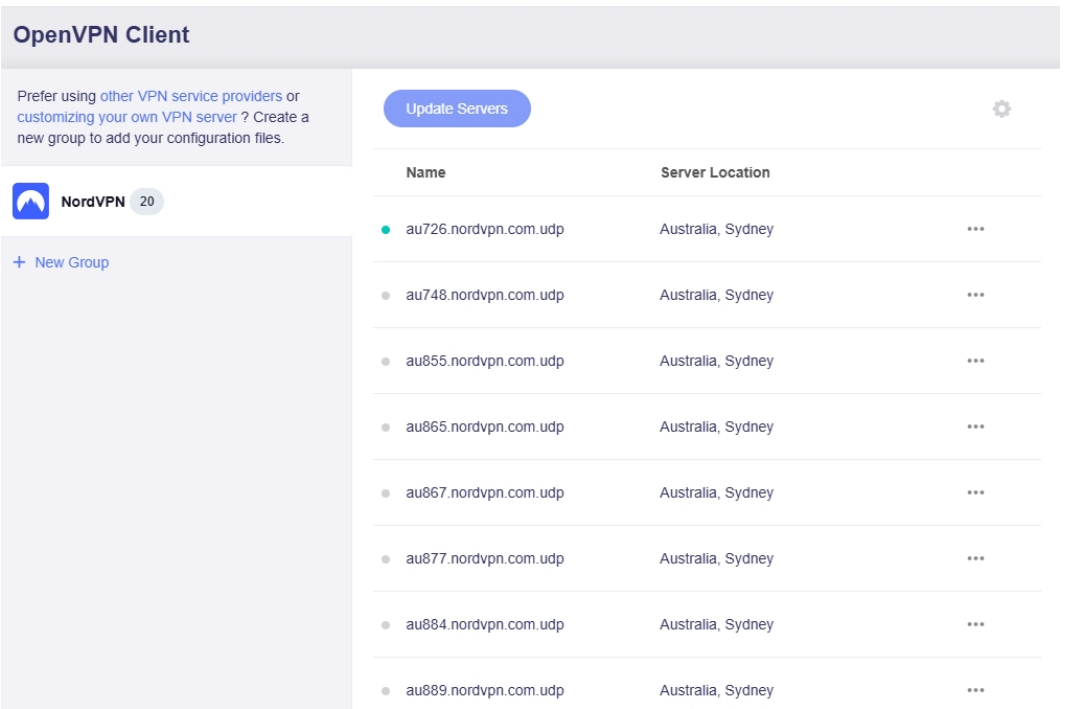


5. Iniciará una conexión.

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



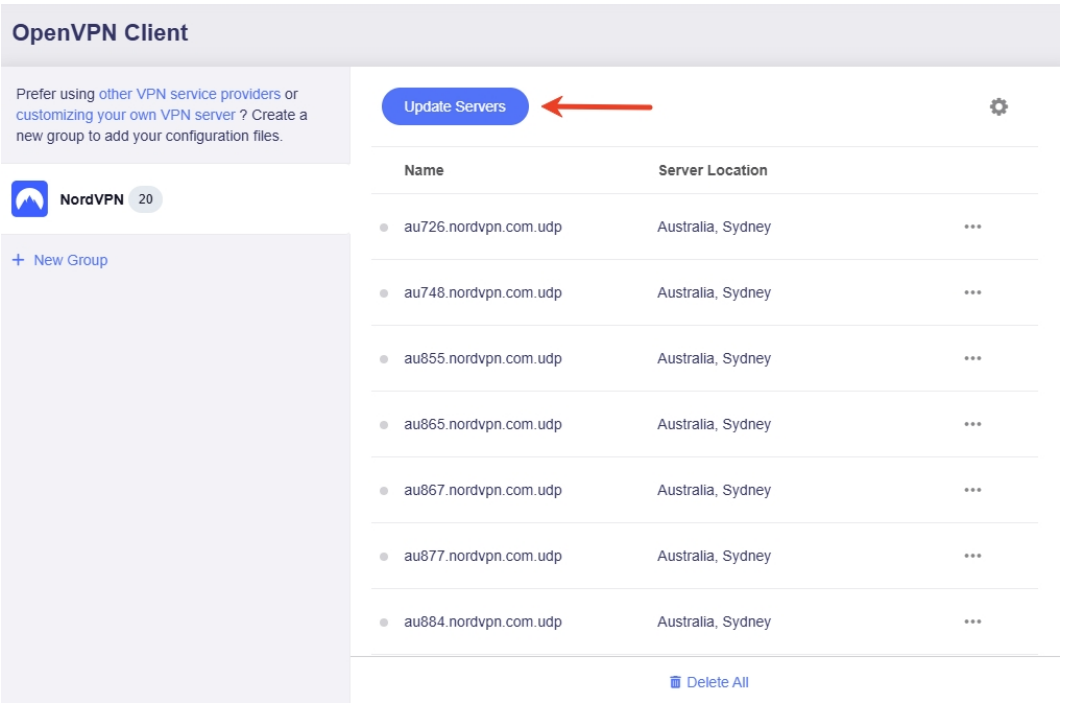
6. Una vez conectado, aparecerá un punto verde junto al archivo de configuración.



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

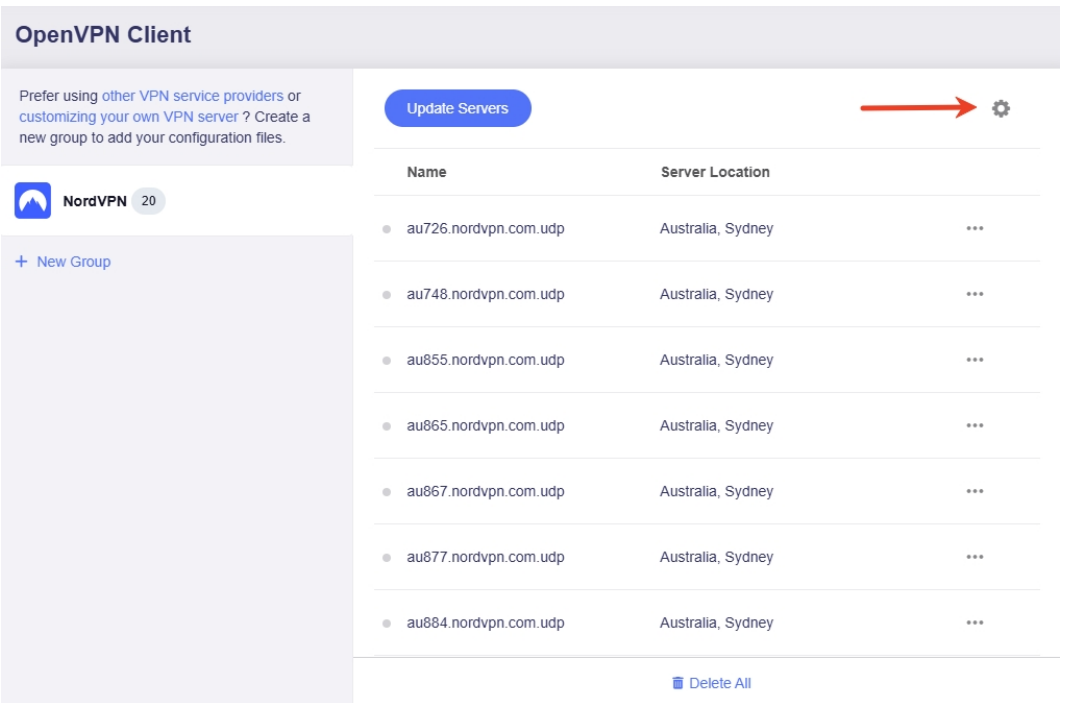
7. Actualizar servidores.

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.



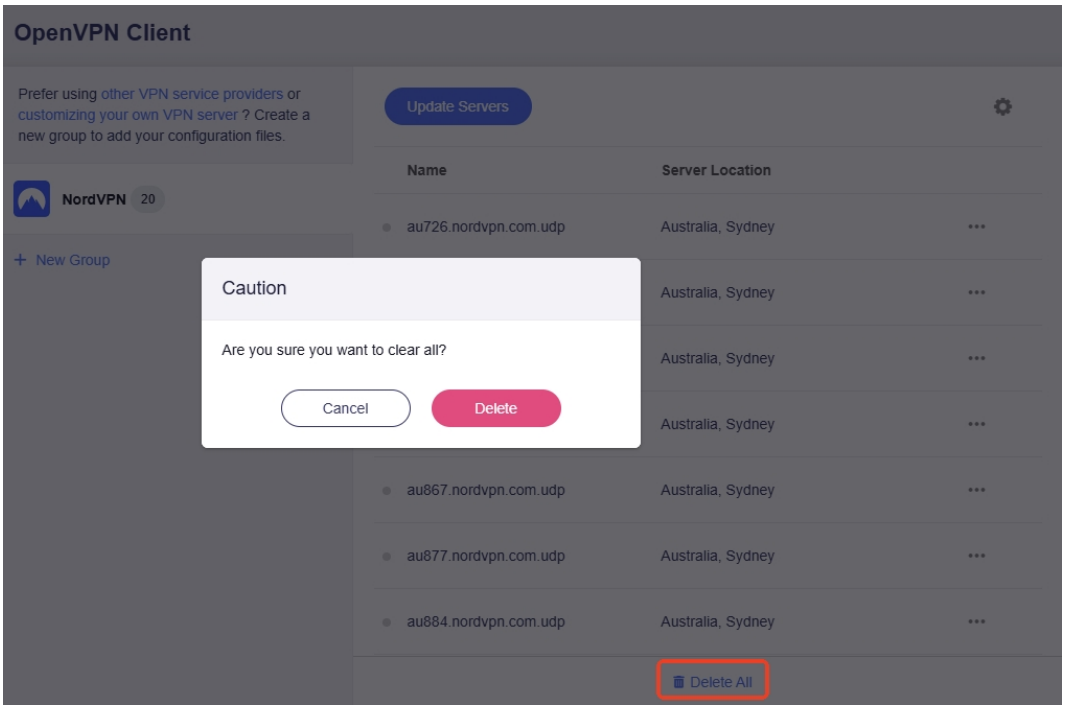
8. Editar credenciales.

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



9. Eliminar todos los archivos.

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

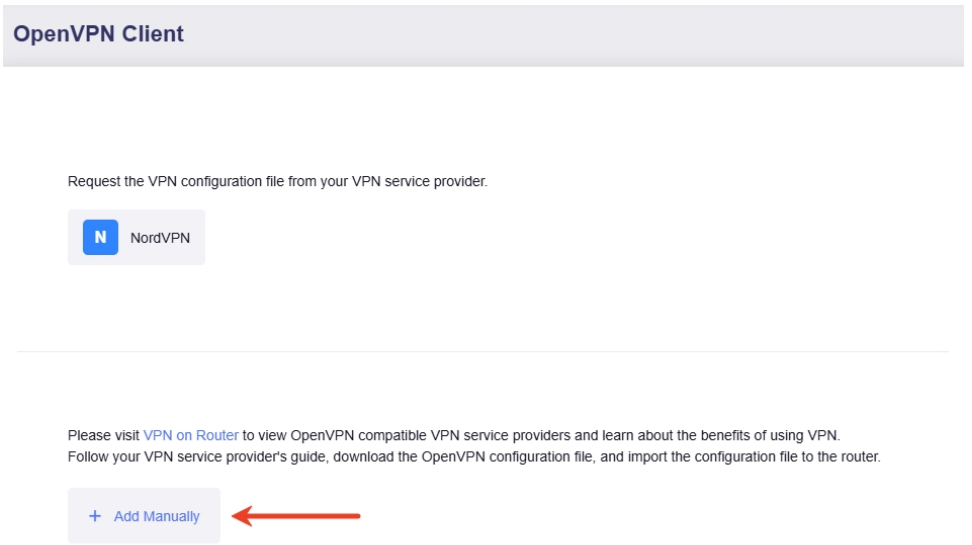


10.1.3 Configurar el cliente OpenVPN manualmente (para otros proveedores)

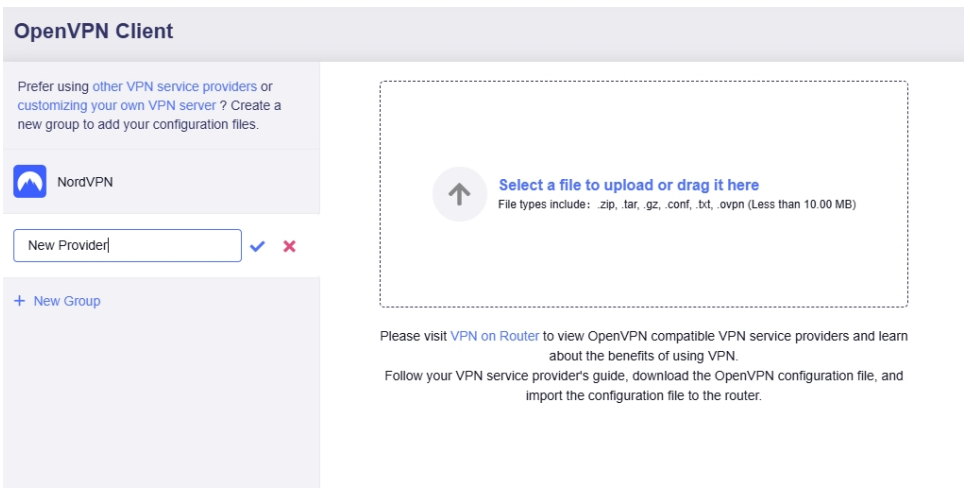
Si su servicio OpenVPN El proveedor no está integrado en nuestro panel de administración, primero visite el sitio web oficial de su proveedor de servicios suscrito para obtener el archivo de configuración. Luego cárguelo en el enrutador para configurar un cliente OpenVPN.

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

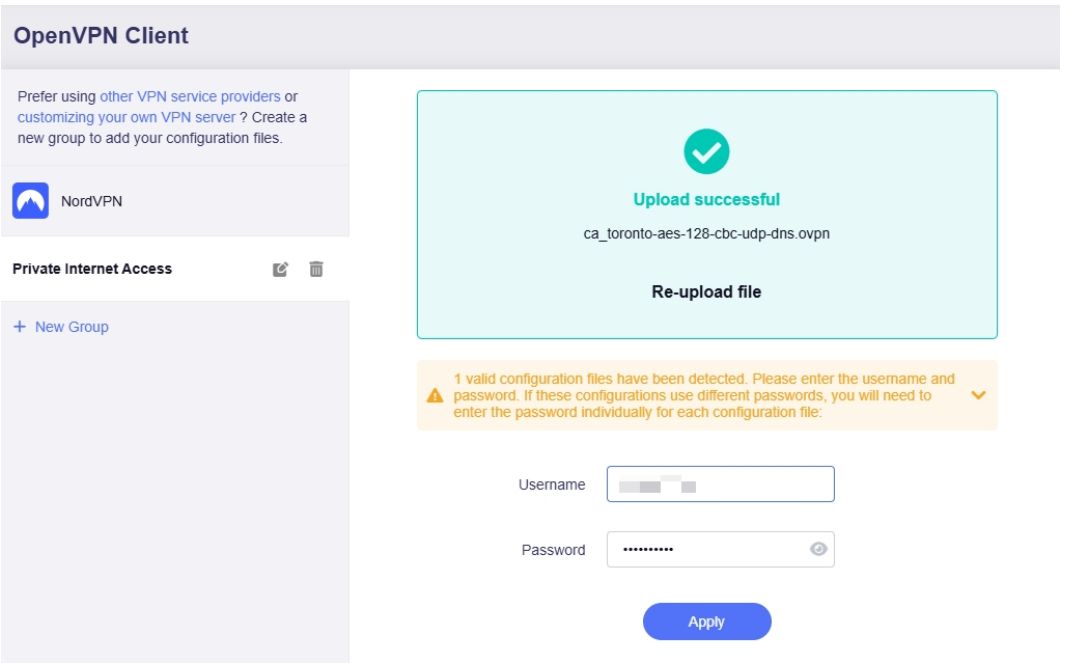
1. Descargue un archivo de configuración del sitio web oficial de Private Internet Access.
2. Inicie sesión en el panel de administración web de su enrutador, navegue hasta **VPN** > **Cliente OpenVPN** y haga clic en **Agregar. Manualmente**.



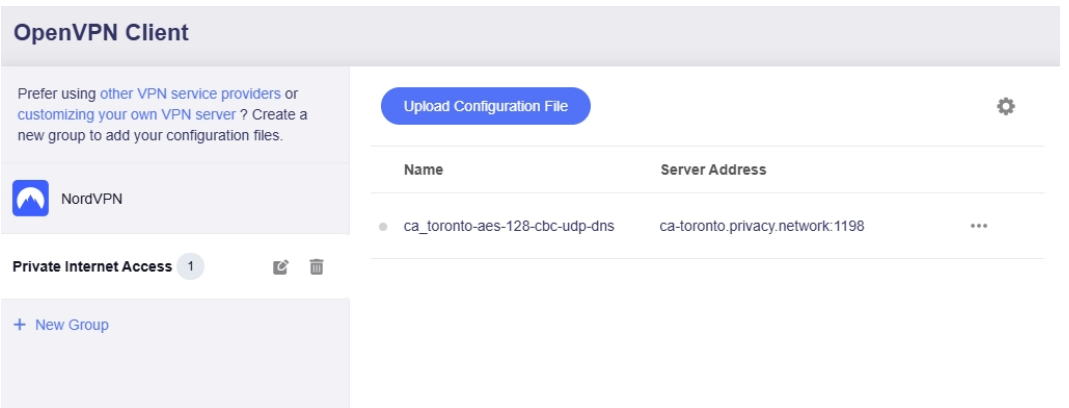
3. Creará un grupo en la barra lateral izquierda.Establezca un nombre descriptivo para el grupo.



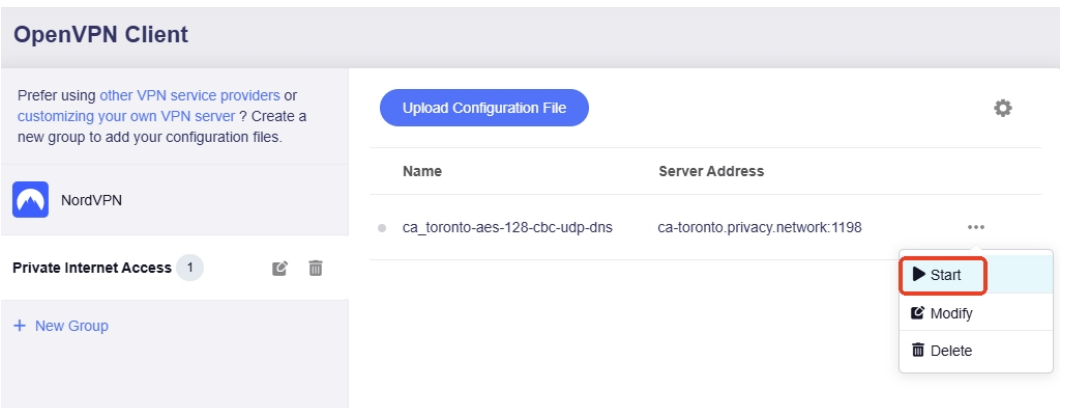
4. Cargue su archivo de configuración de OpenVPN. Ingrese las credenciales si es necesario, luego haga clic en **Aplicar**.



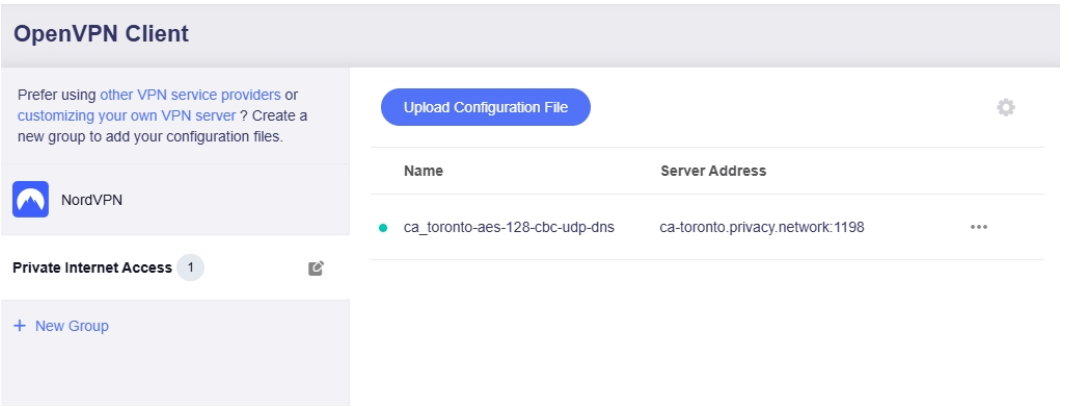
Yverá el archivo de configuración cargado.



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 puedes 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 una VPN proveedor de servicios que admita la configuración manual WireGuard. Consulte aquí para conocer los proveedores WireGuard compatibles con GL.iNet.

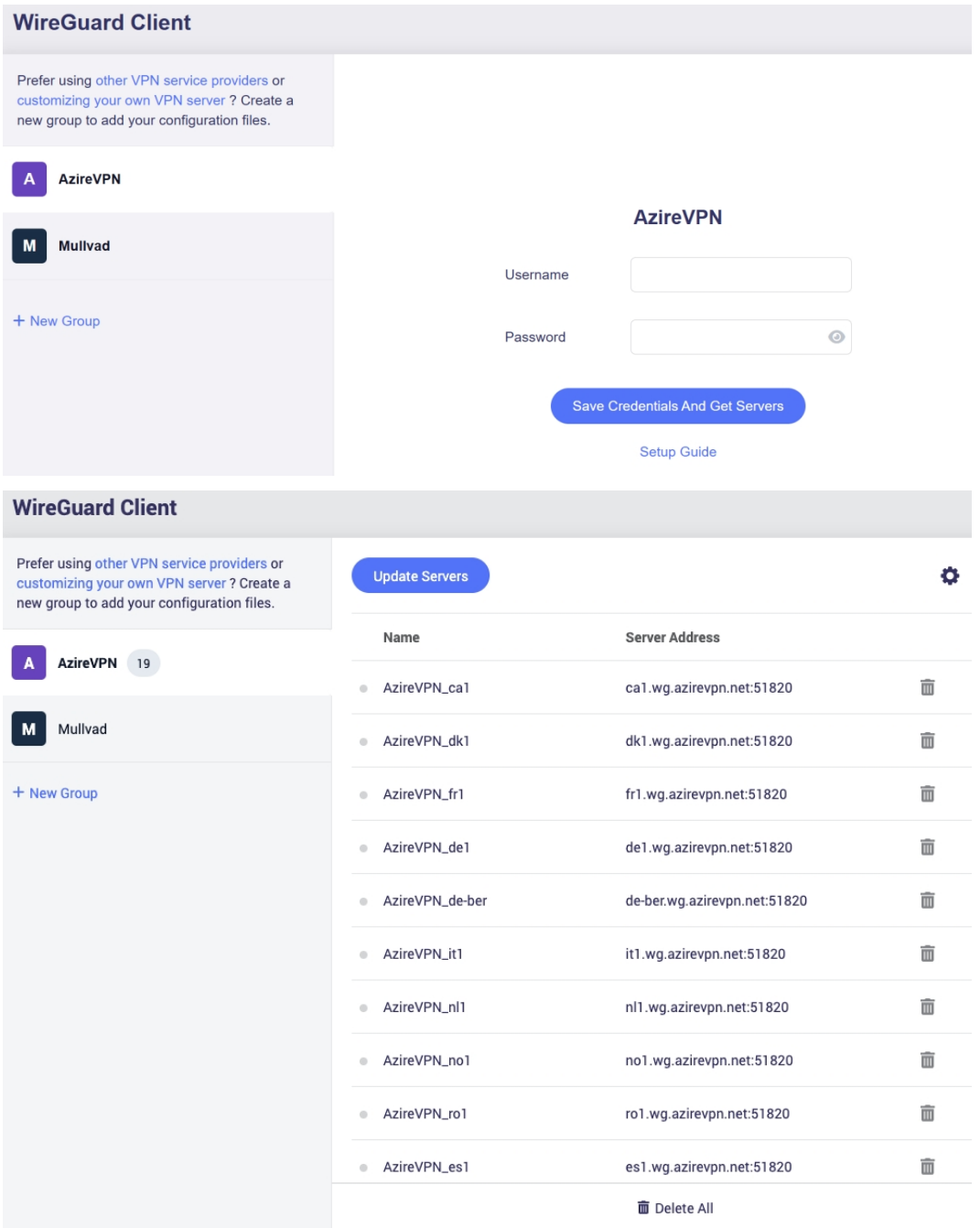
A continuación, sseleccione el proveedor de servicios WireGuard correspondiente a continuación para localizar rápidamente las instrucciones paso a paso.

- Configurar AzireVPN
- Configurar Mullvad
- Configurar el cliente WireGuard manualmente (para otros proveedores)

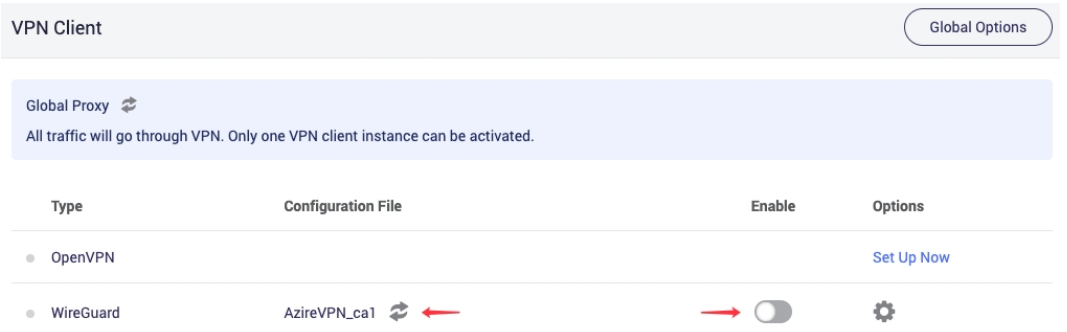
10.2.2 Configurar AzireVPN

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

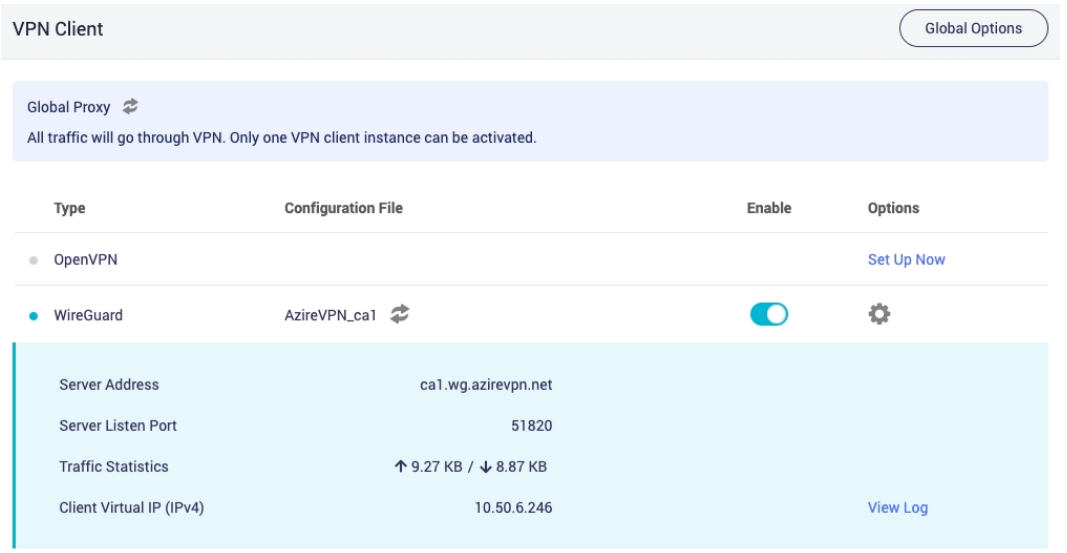
1. Inicie sesiónn en su enrutador’s web admin panel y vaya a **VPN** > **Cliente WireGuard** > **AzireVPN**.
2. Ingrese el nombre de usuario y la contraseña, luego haga clic en **Guardar credenciales y obtener servidores**. Generará archivos de configuración para cada servidor.



3. Vaya al Panel de VPN para habilitar la conexión.

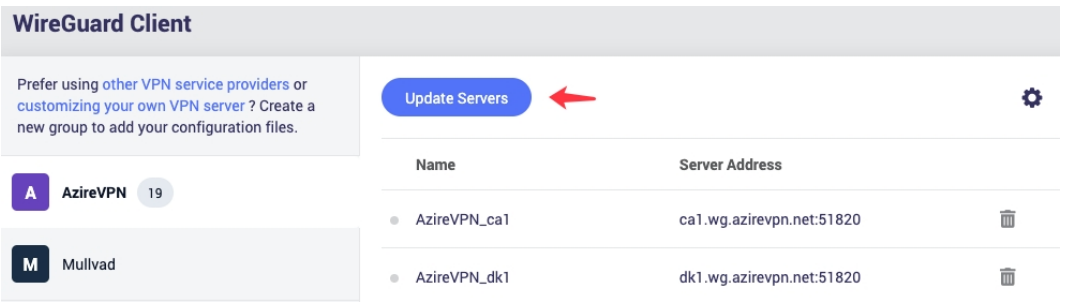


Una vez conectado, debería ver su dirección IP de usuario y la cantidad de bytes enviados/recibidos.



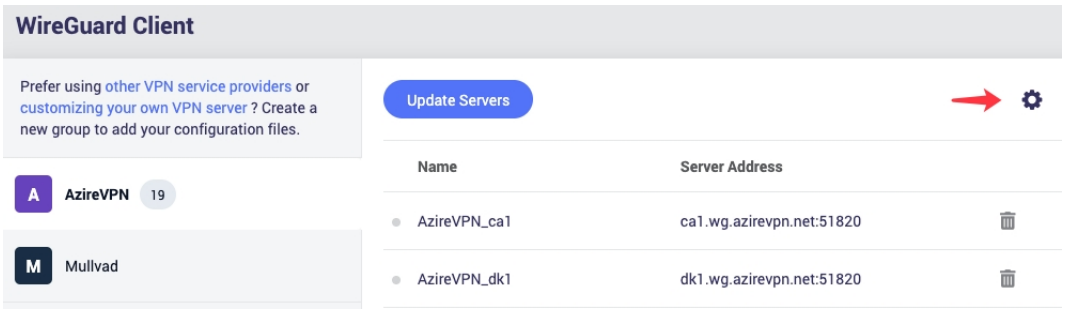
4. Actualizar servidores.

   AzireVPN puede mantener o apagar algunos servidores, lo que provocará que la conexión falle. Puede **Actualizar servidores** para obtener la última versión disponible. servidores.



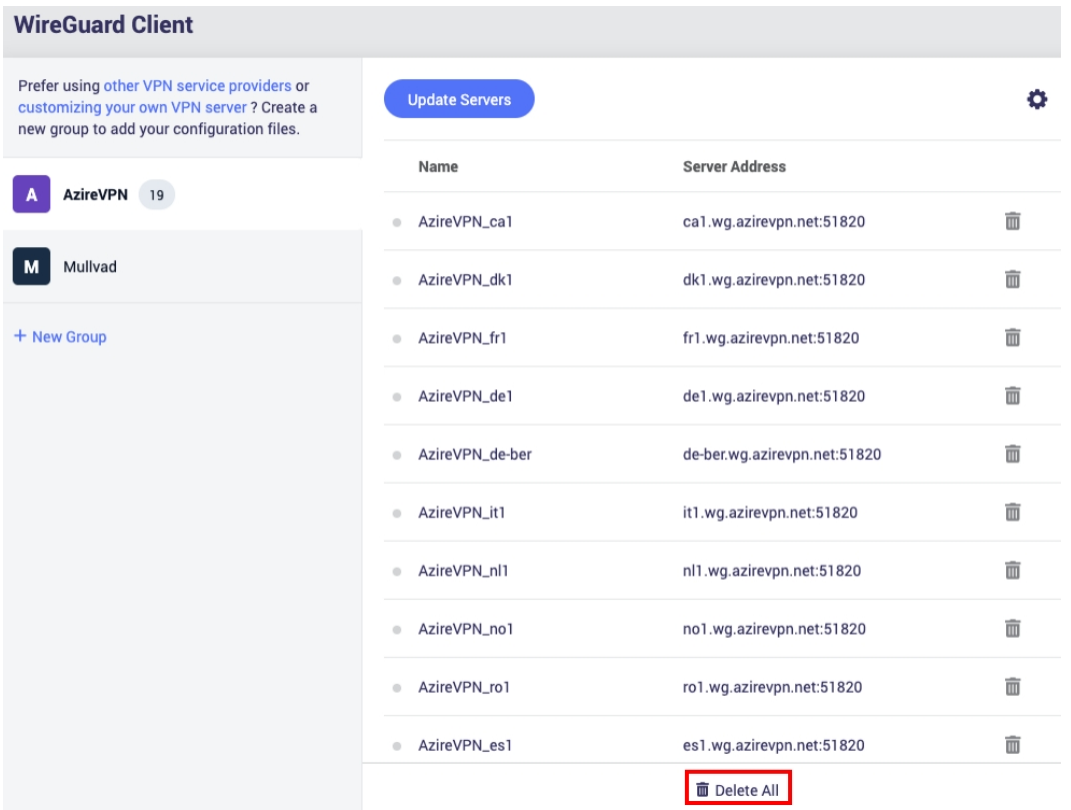
5. Editar credenciales.

   Haga clic en el icono de engranaje para editar la credencial.



6. Eliminar todos los archivos.

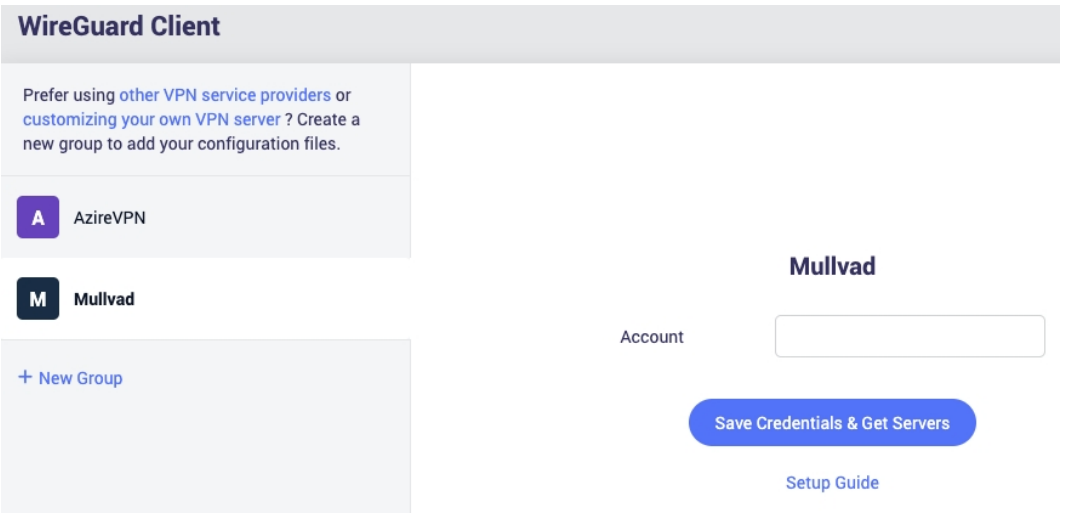
Puede hacer clic en **Eliminar todo** para eliminar todos los archivos de configuración con un solo clic.



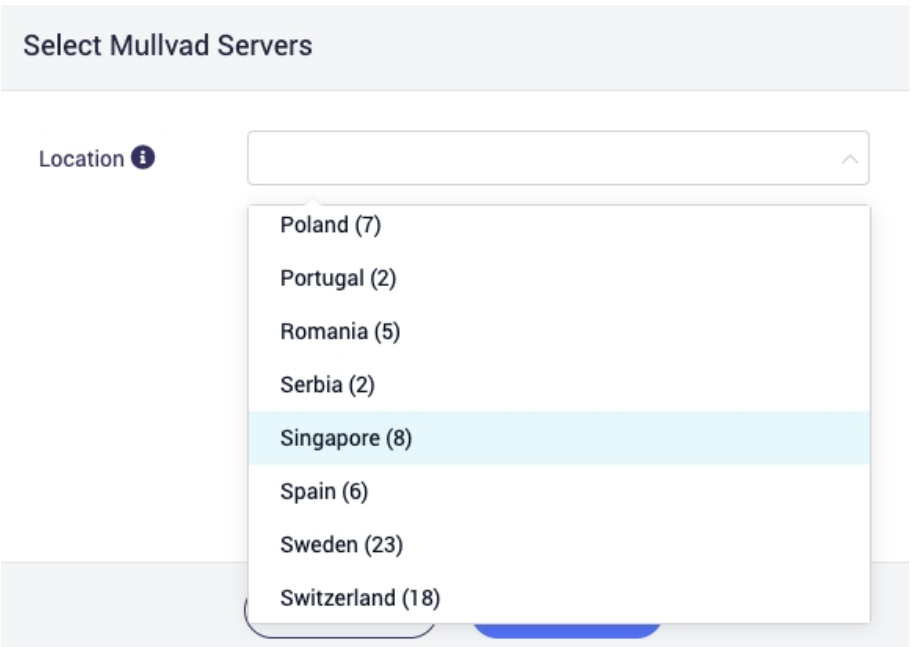
10.2.3 Configurar Mullvad

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

1. Iniciar sesiónn a su enrutador's web admin panel y vaya a **VPN** > **WireGuard Client** > **Mullvad**.
2. Ingrese su cuenta Mullvad (número de 16 dígitos), luego haga clic en **Guardar credenciales y obtener servidores**.

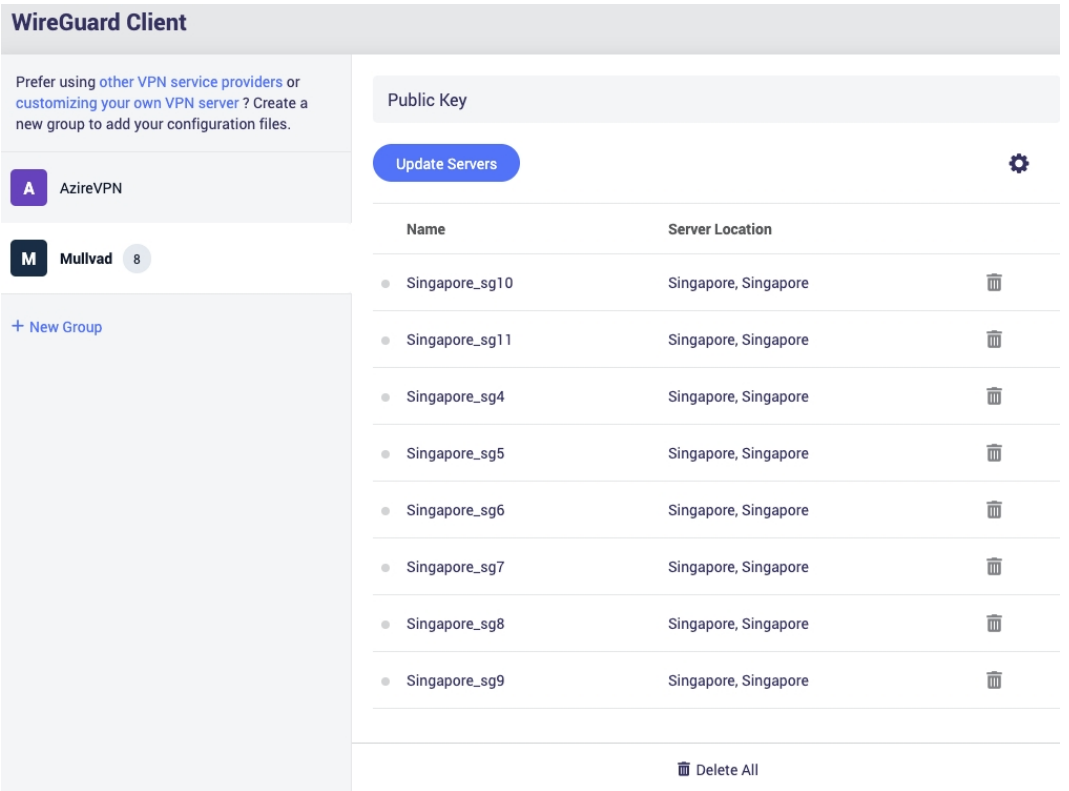


Aparecerá un cuadro de diálogo para seleccionar una ubicación.

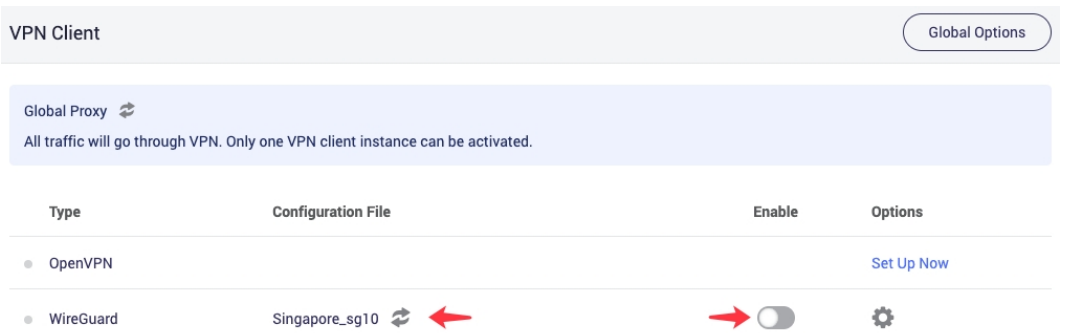


Luego generará los archivos de configuración del servidor de ubicación seleccionado.

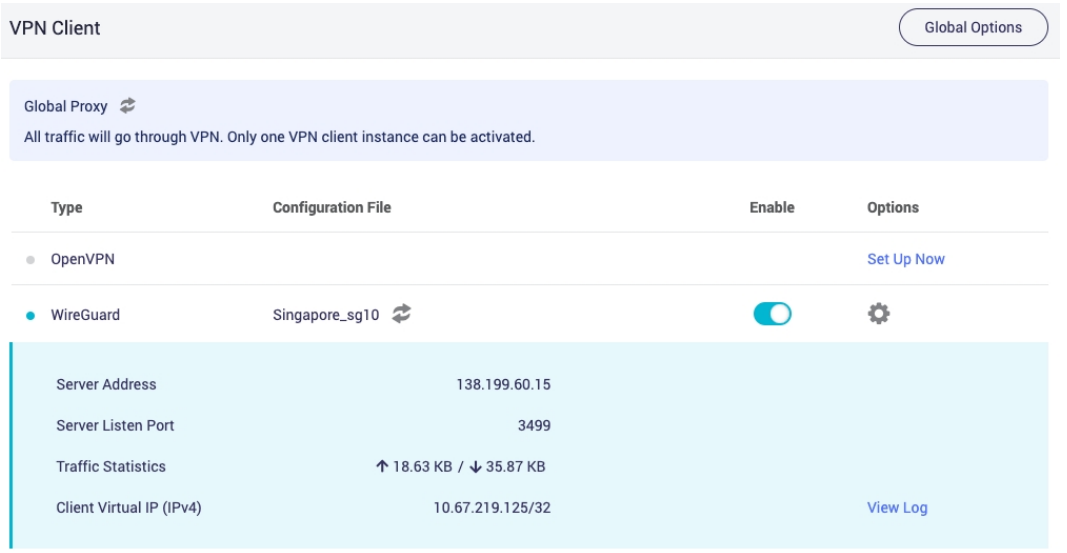
La **clave pública** es la clave pública de WireGuard para enviar al servidor Mullvad. YPuedes tener hasta cinco claves al mismo tiempo, y administrar claves WireGuard en su página de cuenta de Mullvad.



3. Vaya al Panel de VPN para habilitar la conexión.

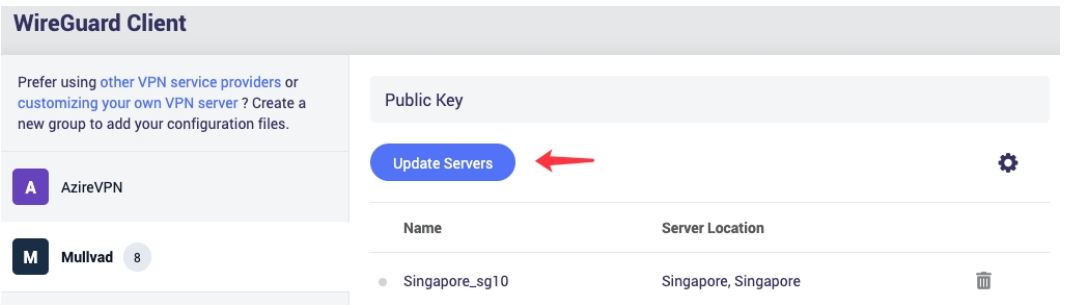


Una vez conectado, debería ver su dirección IP de usuario y la cantidad de bytes enviados/recibidos.



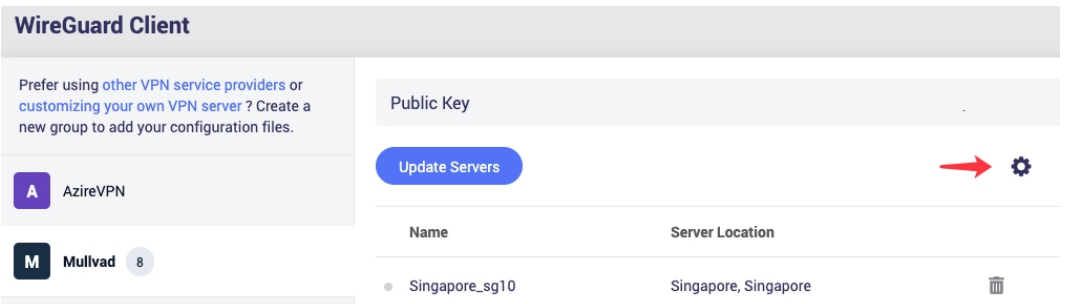
4. Actualizar servidores.

   Mullvad puede mantener o apagar algunos servidores, lo que provocará que la conexión falle. Puede **Actualizar servidores** para obtener los últimos servidores disponibles.



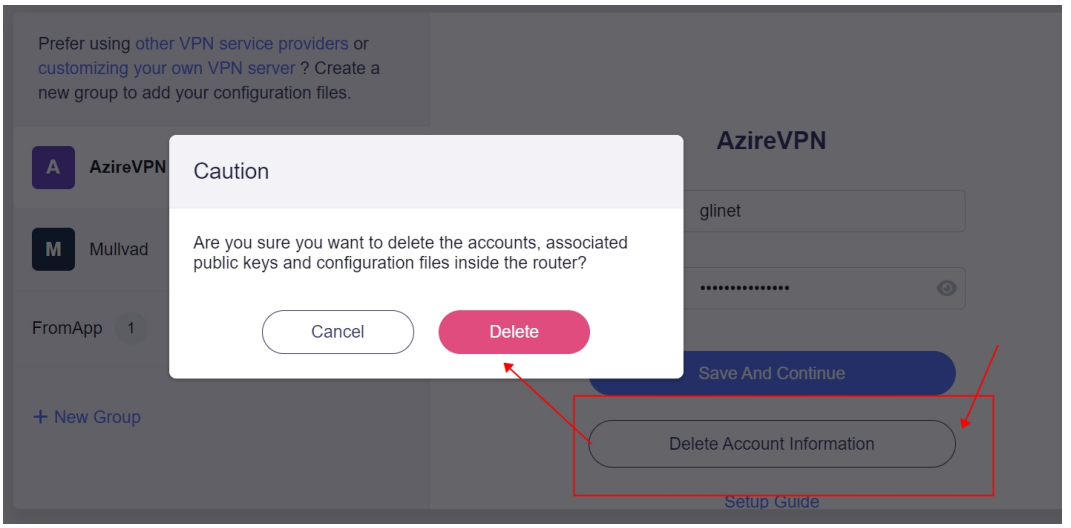
5. Editar credenciales

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



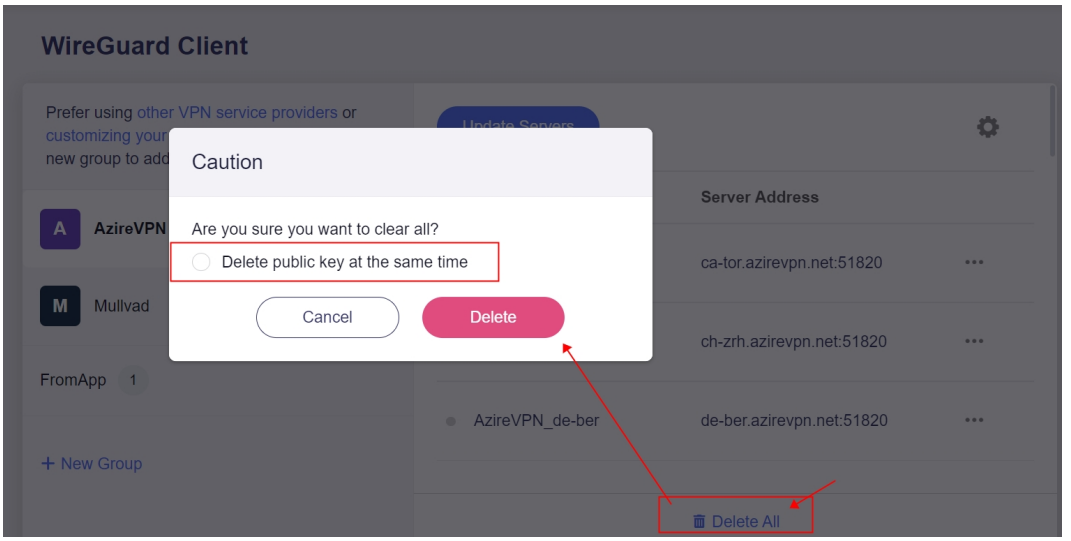
6. Eliminar información de la cuenta

   Si hace clic en **Eliminar**, eliminará la credencial de la cuenta, la clave privada, la clave pública y los archivos de configuración **en el enrutador**.



7. Eliminar

Permita eliminar todos los archivos de configuración con un solo clic y proporcione un mensaje para eliminar también la clave privada y la clave pública.

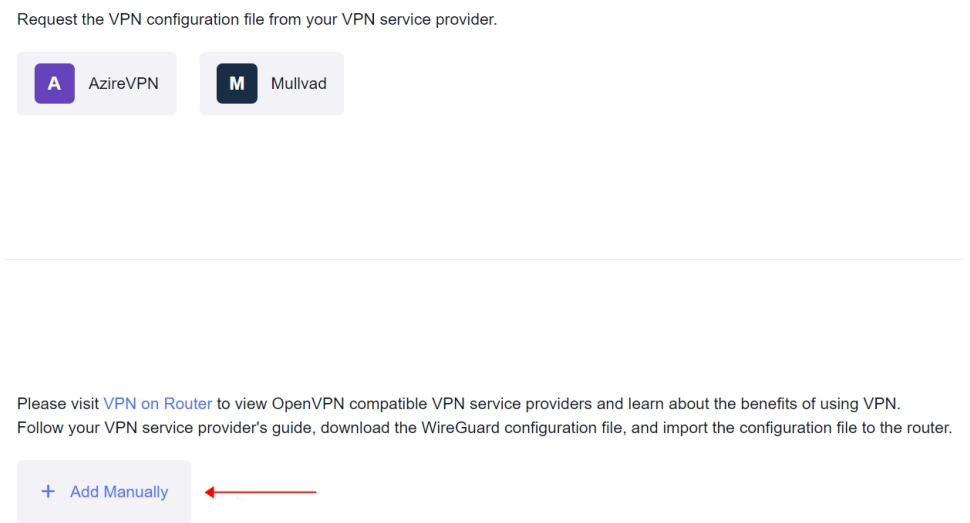


10.2.4 Configurar el cliente WireGuard manualmente (para otros proveedores)

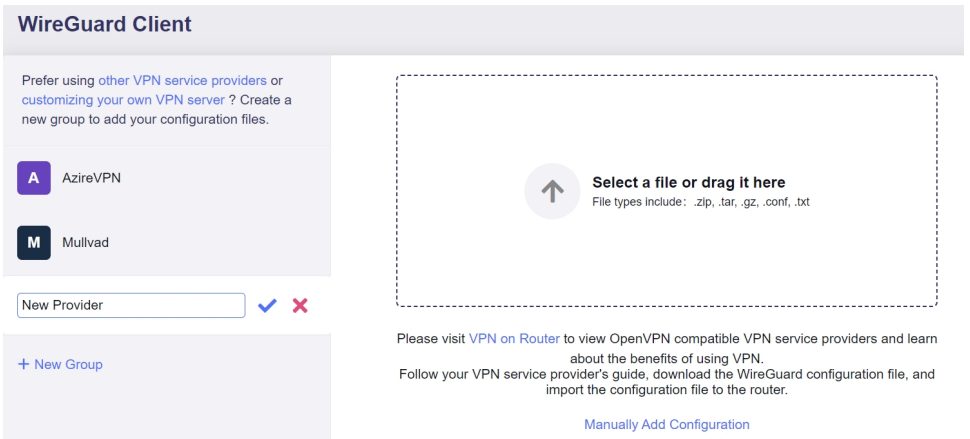
Si su proveedor de servicios WireGuard no está integrado en el panel de administración web, visite Primero, visite el sitio web oficial de su proveedor de servicios suscrito para obtener el archivo de configuración. Luego cárguelo en el enrutador para configurar un cliente WireGuard. Si no sabes cómo 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 al enrutador para configurar un cliente WireGuard.

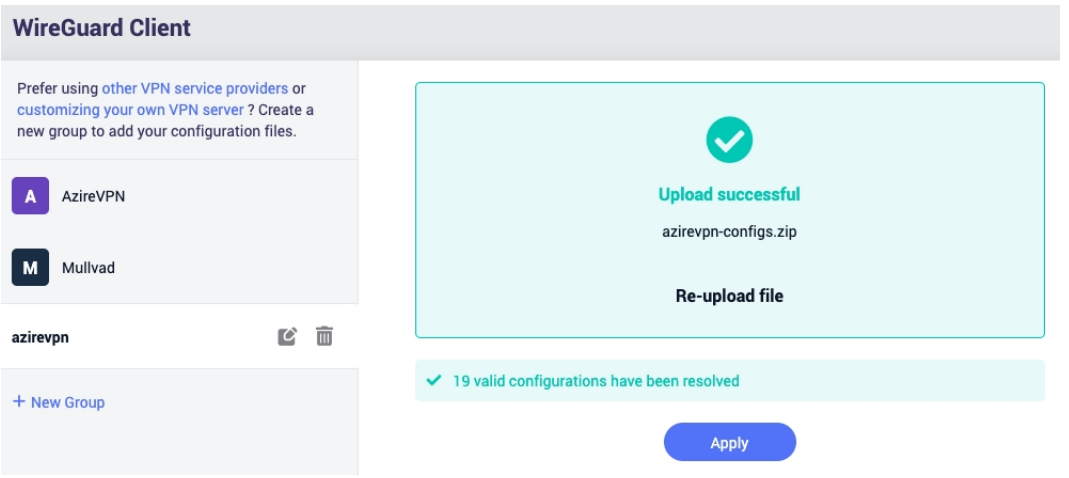
1. Iniciar sesiónn a su enrutador's web admin panel y navegue hasta **VPN** > **WireGuard Client** > **Agregar manualmente**.



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

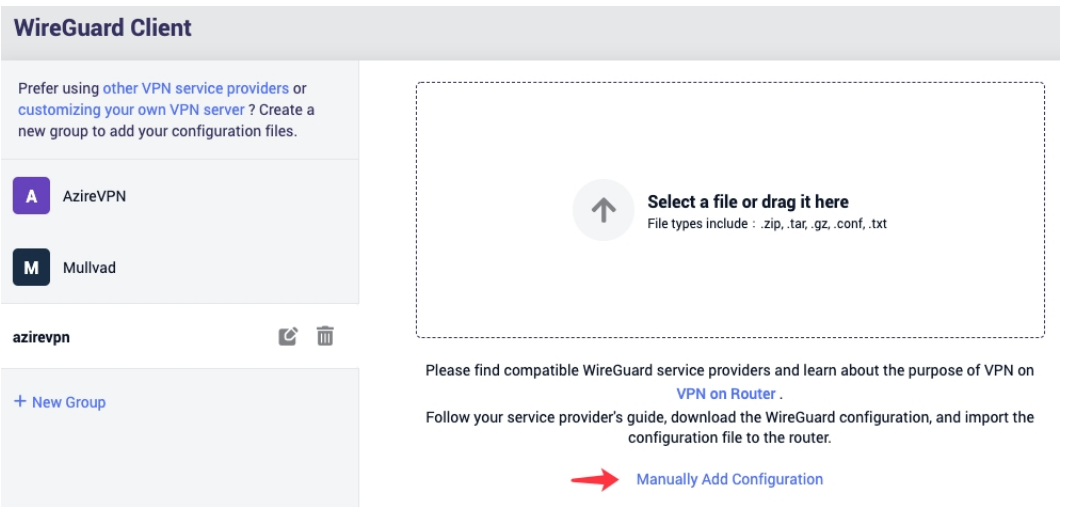


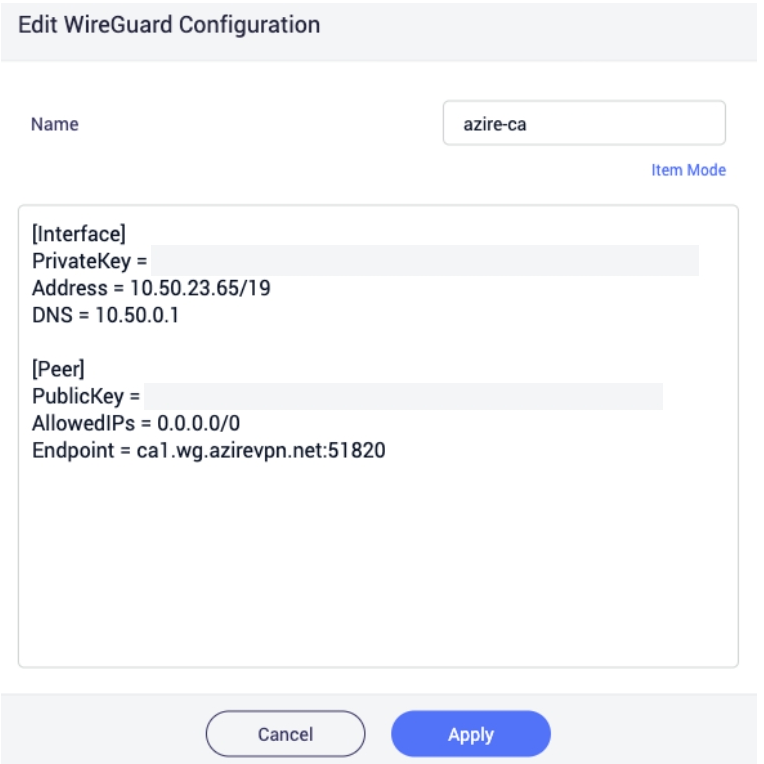
3. Click el área de carga para cargar su archivo de configuración de WireGuard (formatos admitidos: zip, tar, gz, conf, txt) y haga clic en **Aplicar**.



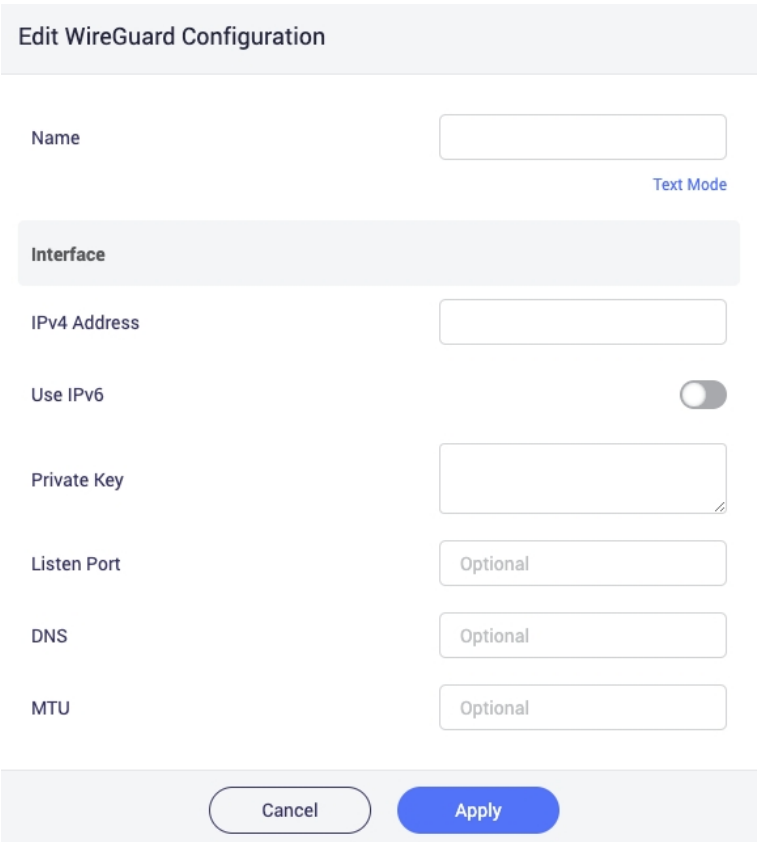
Si carga un archivo comprimido que contiene varios archivos de configuración, se descomprimirá automáticamente.

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

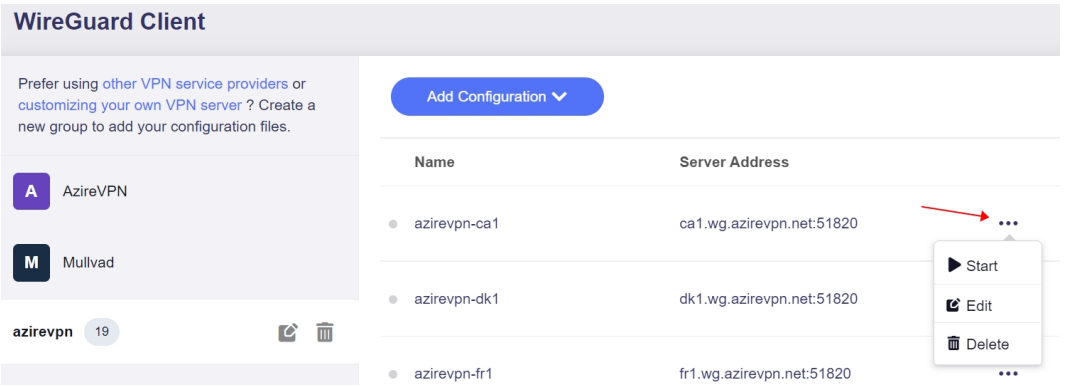




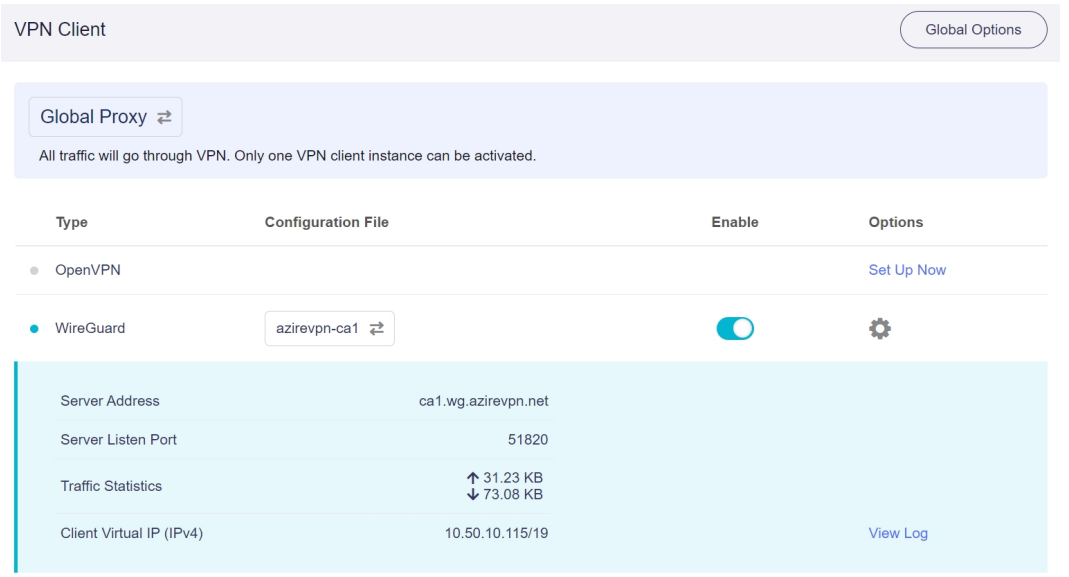
Si desea verificar cada elemento, puede cambiar al modo Elemento y verificar la configuraciónuración detalles, then haga clic en **Aplicar**.



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 el **Panel de VPN**.



Capítulo 11

Tor

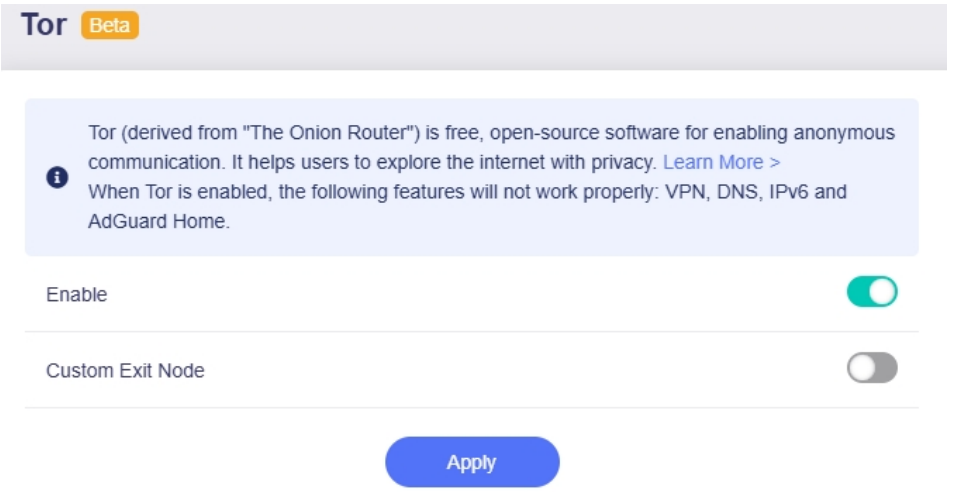
Este capítulo proporciona una breve introducción a Tor (The Onion Router), un software gratuito y de código abierto para permitir la comunicación anónima.

Tor (derivado de **The Onion Router**) 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 queesta función se encuentra actualmente en versión beta y puede tener algunos errores.

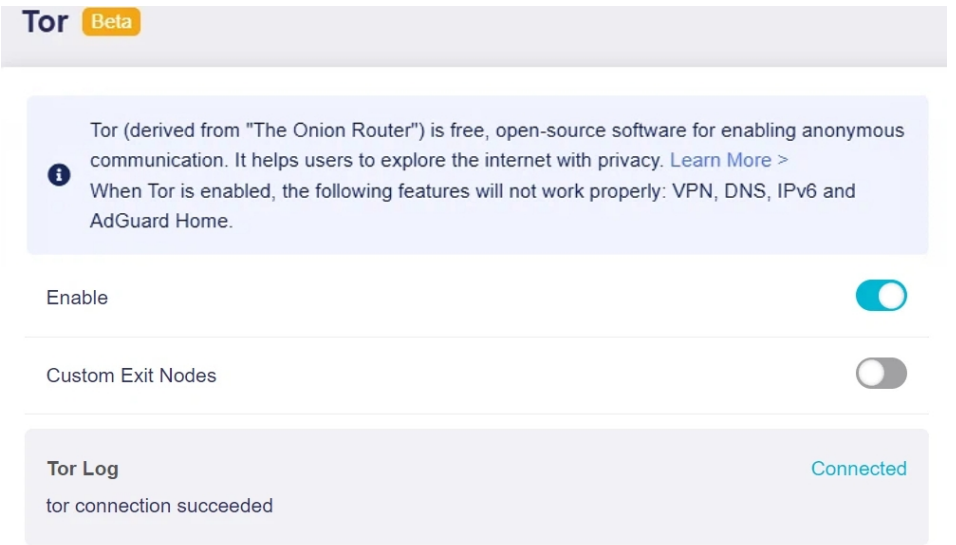
Cuando Tor está habilitado, las siguientes características no funcionarán correctamente:Las siguientes funciones no funcionarán correctamente: VPN, DNS, IPv6 y AdGuard Home.

Siga los pasos a continuación para configurar Tor si es necesario.

1. Inicie sesión en el panel de administración web de su enrutador' y navegue hasta **VPN** > **Tor**. Tcambie el interruptor para habilitarlo, habilite nodos de salida personalizados si es necesario, y haga clic en **Aplicar**.



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



Capítulo 12

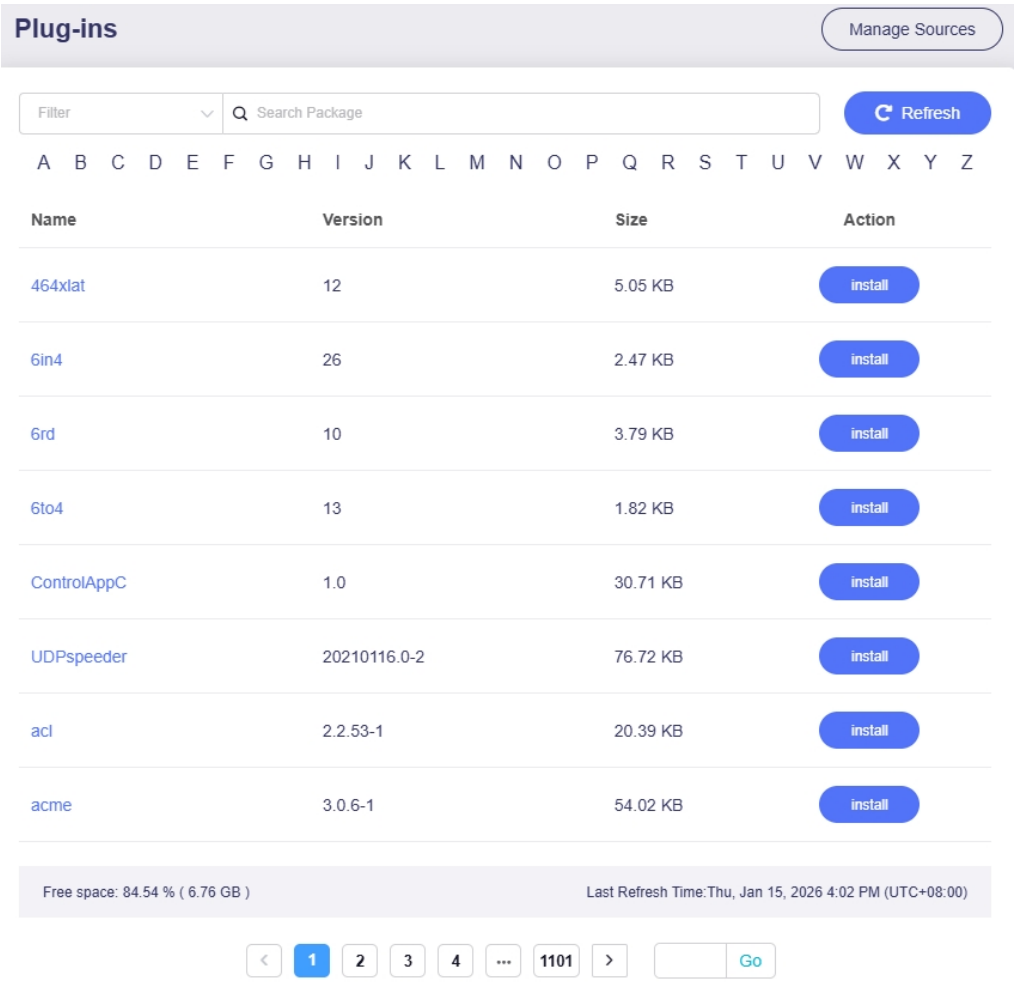
Aplicaciones

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

12.1 Complementos

La Complementos página le permite administrar OpenWrt paquetes.

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



Nota:

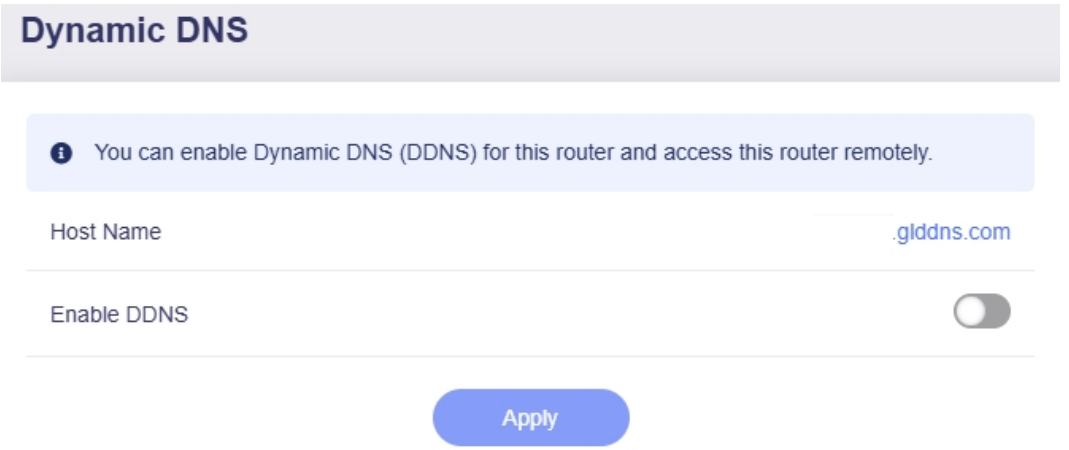
1. No se recomienda actualizar los complementos preinstalados en el firmware oficial de GL.iNet, como nginx, adguard home, tailscale, etc.
2. Los complementos de terceros instalados manualmente por los usuarios se pueden actualizar; sin embargo, GL.iNet no es responsable de ningún problema de seguridad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

12.2 DNS dinámico

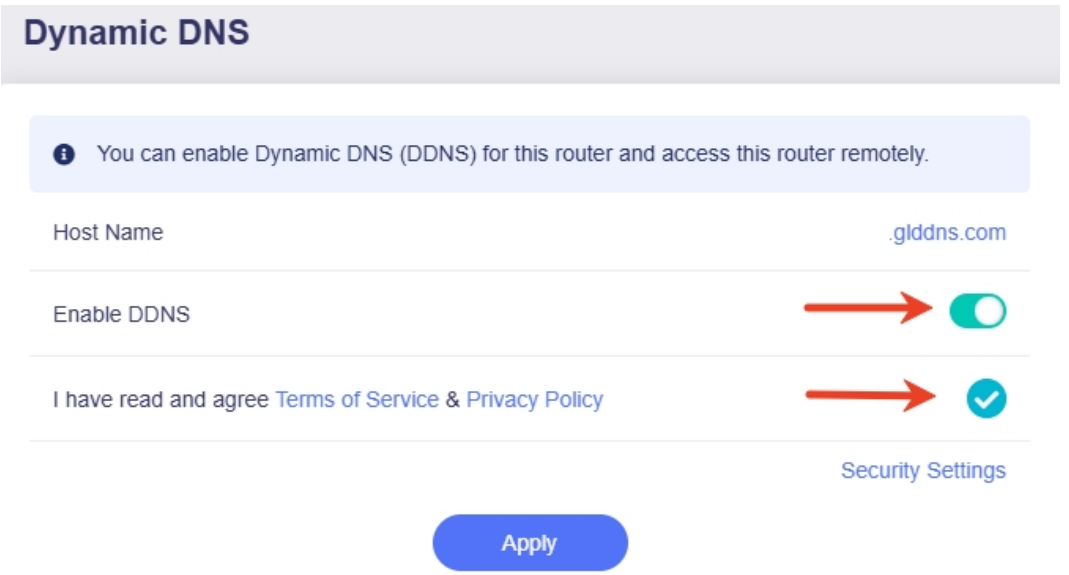
Dinámico El servicio de nombres de dominio (DDNS o DNS dinámico) es un servicio que se utiliza para asignar un nombre de dominio al dominio dinámico. Dirección IP de un dispositivo de red. Con DNS dinámico, puede acceder a su enrutador de forma remota. Se requiere una dirección IP pública para esta funcionalidad.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

12.2.1 Habilitar DDNS

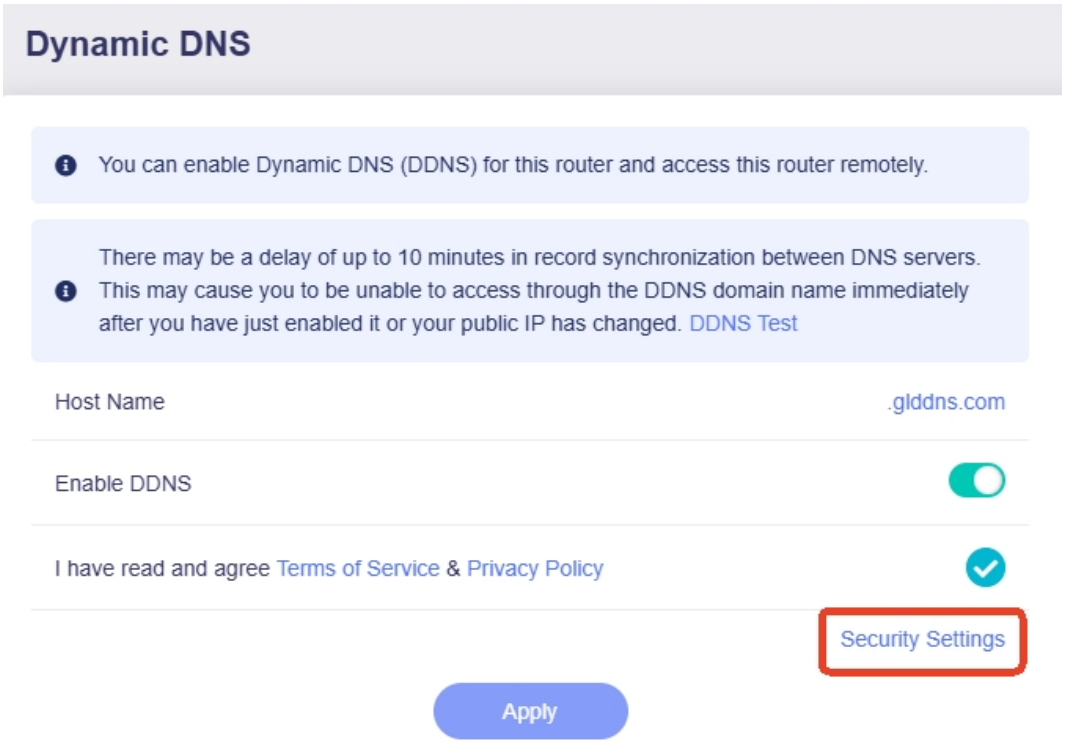
1. Inicie sesión en su enrutador's web admin panel, navegue hasta **APLICACIONES** > **DNS dinámico**, la página se muestra a continuación.



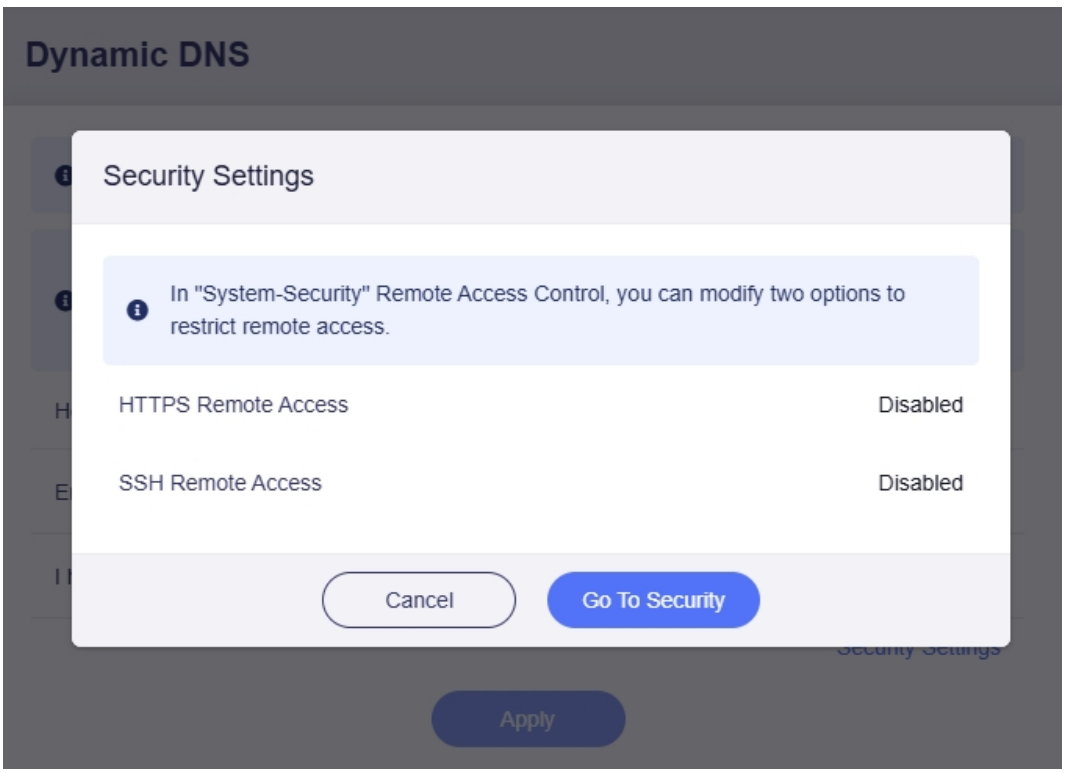
2. Activar **Habilitar DDNS**, lea y acepte los **Términos de servicios y política de privacidad**, luego haga clic en **Aplicar**.



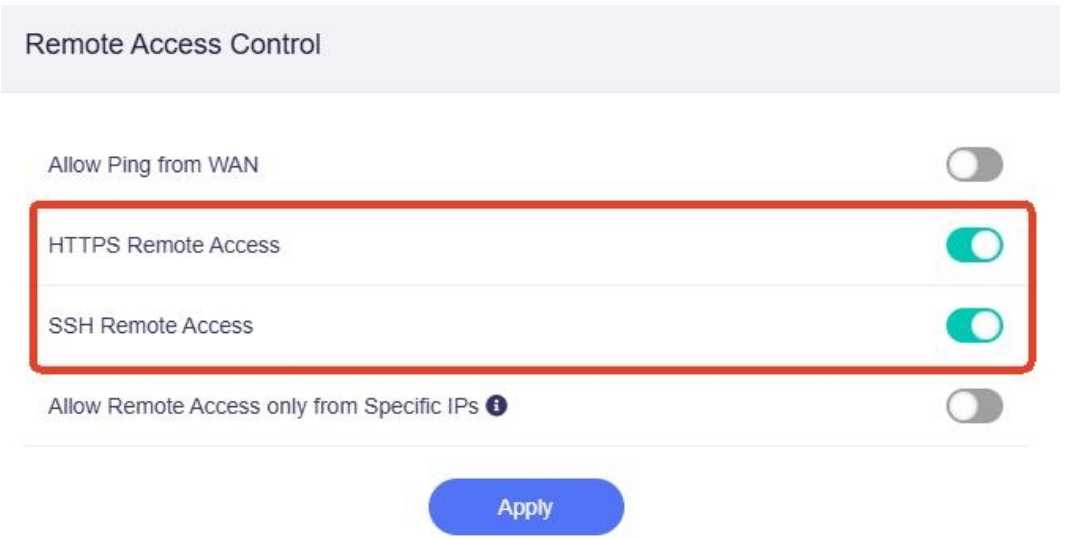
3. Haga clic en **Configuración de seguridad** en la esquina inferior derecha.



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



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



Nota:

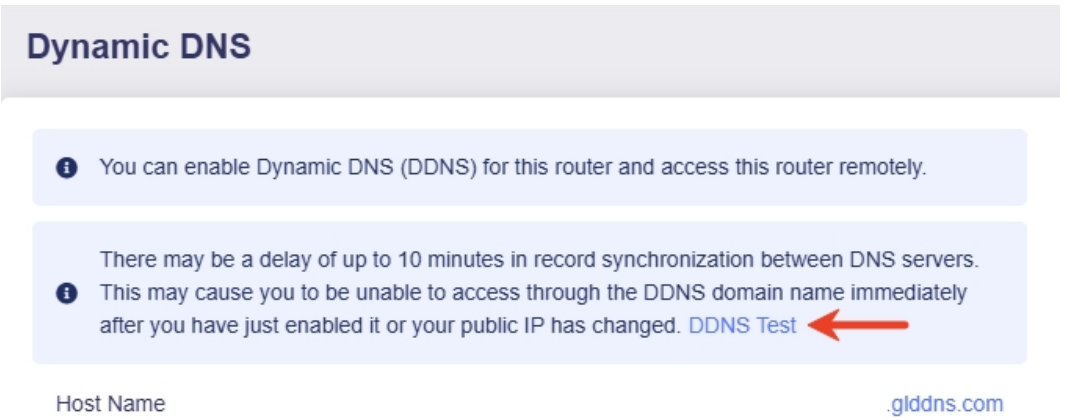
1. Puede haber un retraso de hasta 10 minutos en el registro sincronización entre servidores DNS. Esto puede impedirle acceder a través del nombre de dominio DDNS inmediatamente después de habilitarlo o cuando cambie su IP pública.
2. Si habilita DDNS y el Cliente VPN al mismo tiempo, enseguro de que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

12.2.2 Comprobar si DDNS funciona

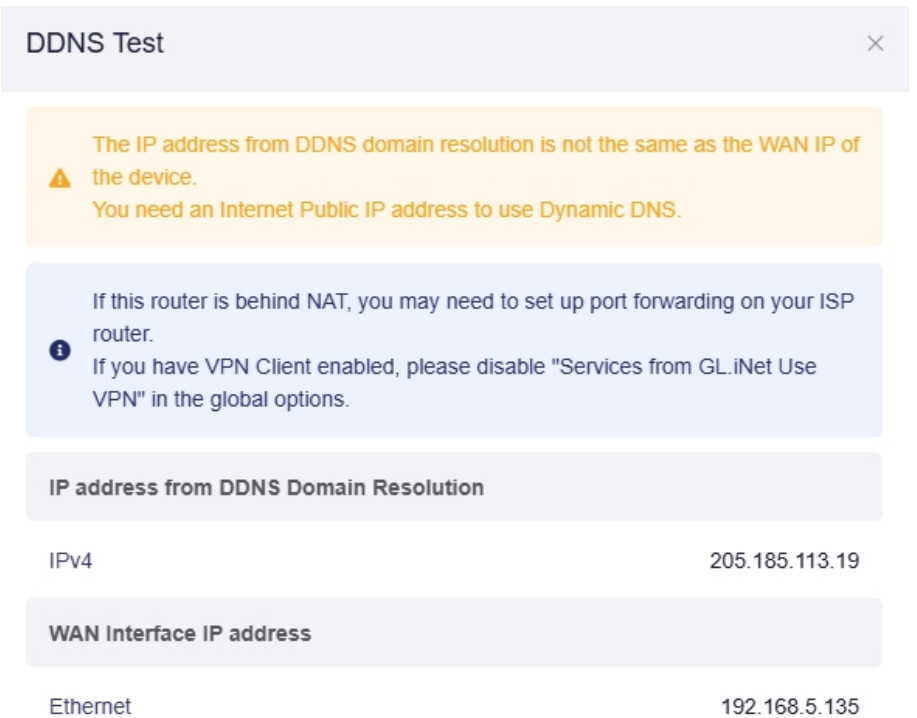
Puede comprobar si DDNS funciona utilizando la herramienta de prueba de DDNS o manualmente mediante comandos.

Método 1. Utilícese 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 debe configurar el reenvío de puertos en el enrutador ascendente.



Método 2. Usar comandos

1. Usar nslookup comando *nslookup xxxxxxx.glddns.com 8.8.8.8* para obtener la asignación entre el nombre de dominio y la dirección IP, como se muestran a continuación.



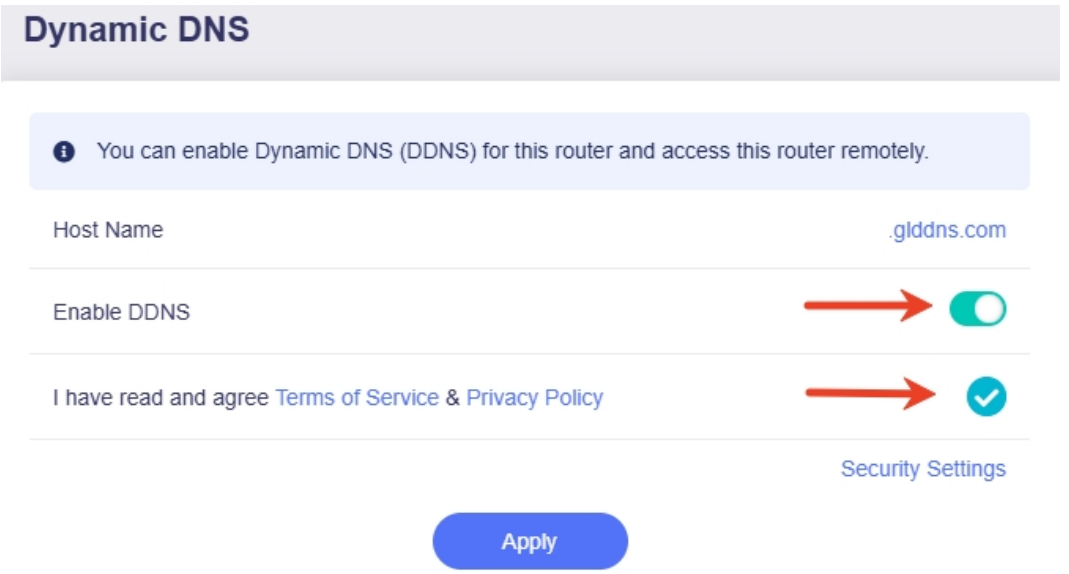
   - Reemplace “xxxxxxx.glddns.com” en la imagen de arriba con su nombre de host.
   - El “8.8.8.8” es el DNS de Google. Uconsúltelo o reemplácelo con otros, luego presione Entrar.
2. Si obtiene una dirección IP pública como “183.178.10.100” en La imagen de arriba indica que su dominio DDNS se ha asignado correctamente a una dirección IP pública. Si recibe un mensaje como “el servidor no puede’no encontrar xxxxxxx.glddns.com”, puede indicar que la resolución del dominio falló y que su dominio DDNS no se ha asignado correctamente a una dirección IP pública. Continúe con el siguiente paso para verificar.
3. Inicie sesión en la web de su enrutador’s 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

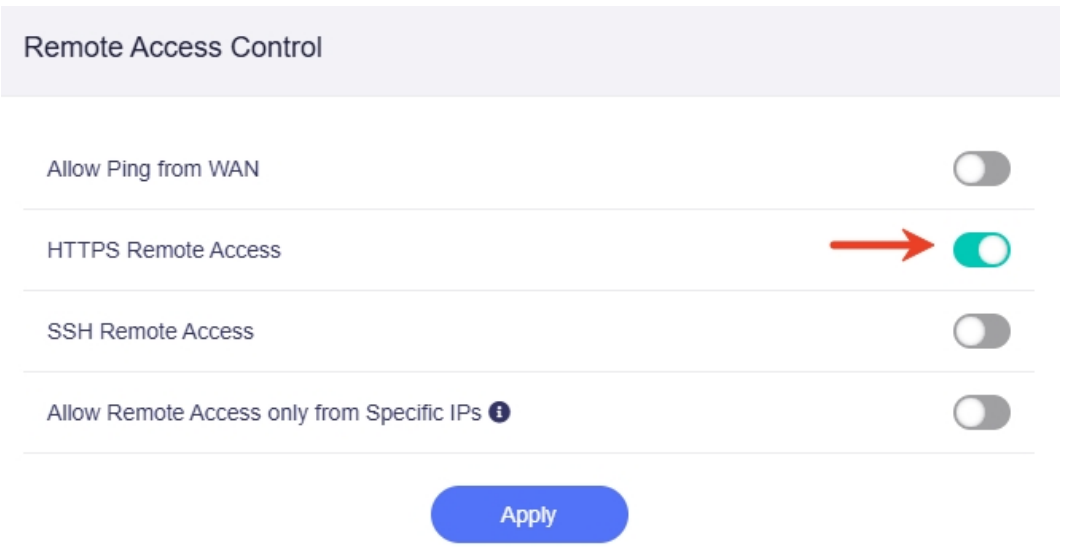
Una **Dirección IP pública** es necesario para el acceso remoto HTTPS. Consulte aquí parapara verificar si su ISP le asigna una IP pública. dirección. Si su enrutador está detrás de NAT, configure el reenvío de puertos (**puerto 443**) en el enrutador ascendente para acceso HTTPS.

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

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

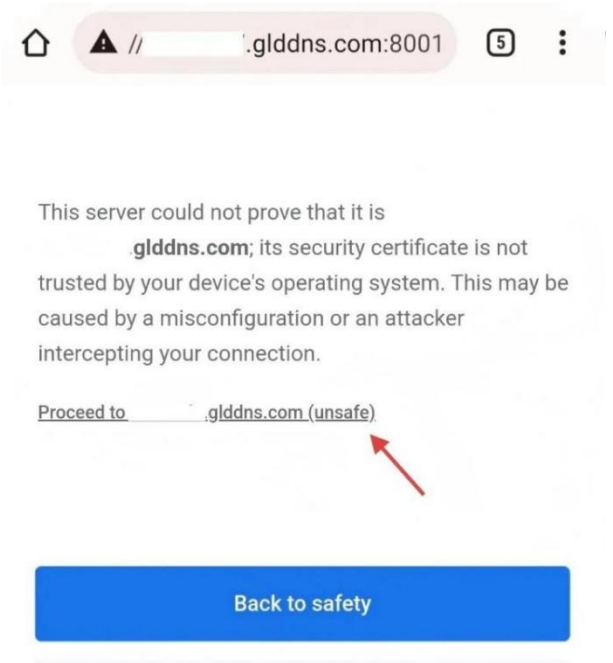


2. En el panel de administración web, vaya a **SISTEMA** > **Seguridad** > **Control de acceso remoto**. Habilitar **Acceso remoto HTTPS**, y haga clic en **Aplicar**.



3. Una vez habilitado, puede acceder al panel de administración del enrutador' desde cualquier lugar usando DDNS host nombre sobre HTTPS, por ejemplo, **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.



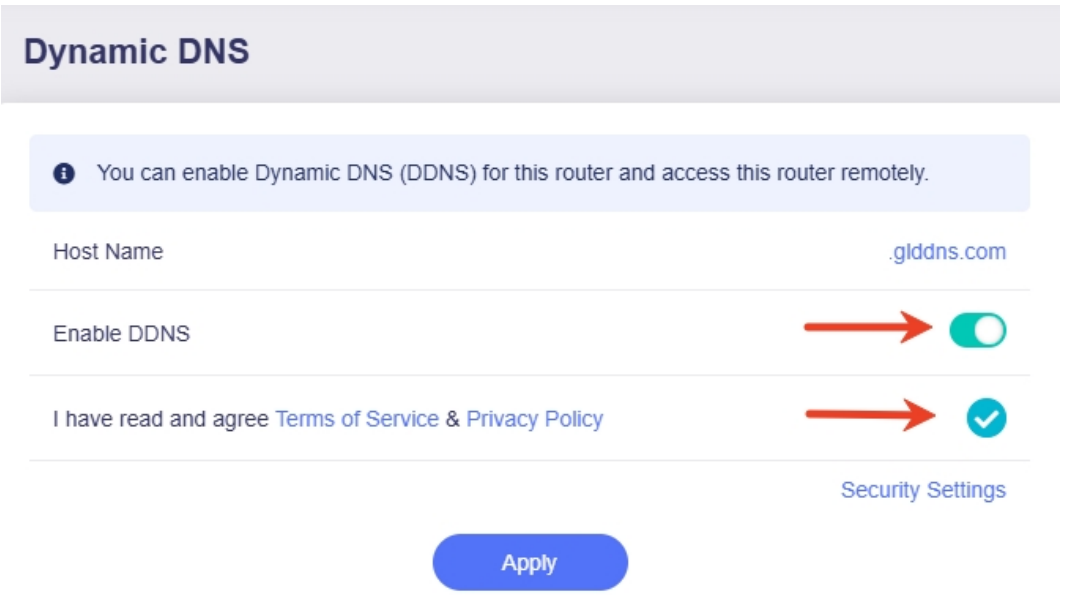
Luego podrá acceder a enrutador's panel de administración web usando el DDNS host nombre sobre **HTTPS**.

12.2.4 Acceso remoto SSH

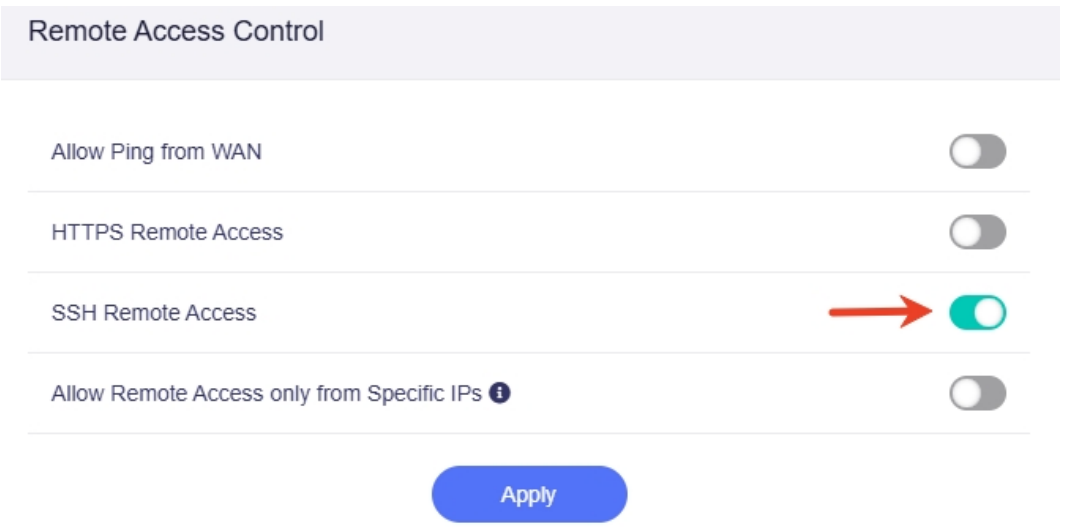
Se requiere una **dirección IP pública** para el acceso remoto SSH. Consulte aquí tpara verificar si su ISP le asigna una dirección IP pública. Si su enrutador está detrás de NAT, configure el reenvío de puertos (**puerto 22**) en el enrutador ascendente para SSH acceso remoto .

Siga los pasos a continuación para habilitar el acceso remoto SSH 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 SSH** y haga clic en **Aplicar**.



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

12.3 GoodCloud

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

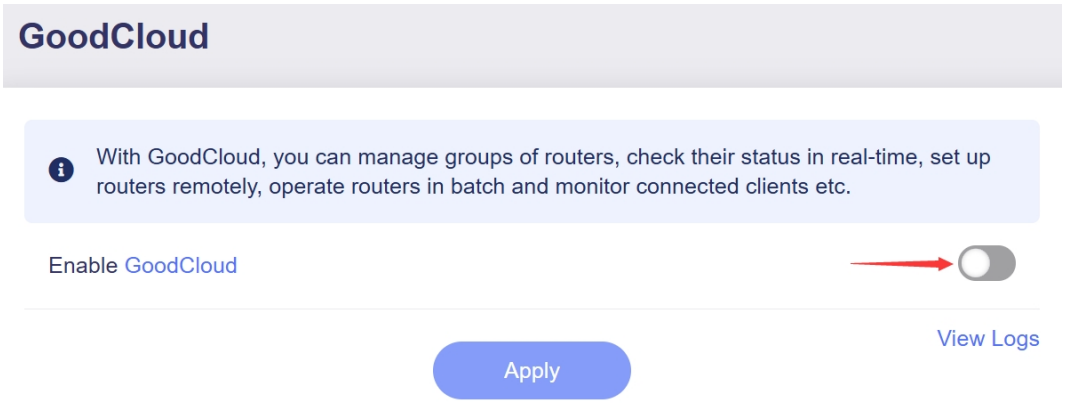
Con GoodCloud, puede:

- Comprueba el estado de tu enrutador’en tiempo real
- Madministrar grupos de enrutadores
- Configurar enrutadores de forma remota
- Monitor conectado clientes
- Operar enrutadores por lotes
- Establecer Sitio-al-Sitio conexión

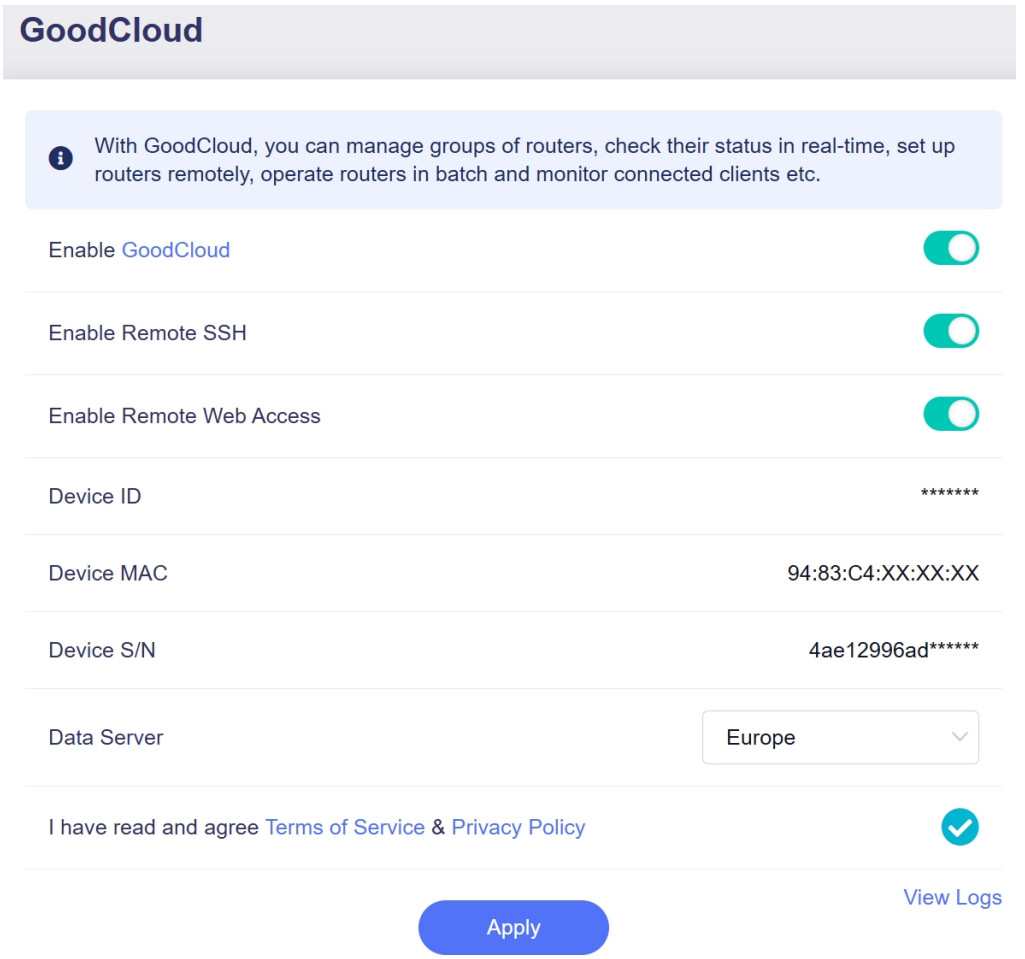
Algunas funciones están disponibles en el plan Enterprise y el plan VAR (revendedor de valor agregado). Consulte aquí para obtener más detalles.

12.3.1 Habilitar GoodCloud

1. Inicie sesión en el Panel de administración web de su enrutador y navegue hasta **APLICACIONES** > **GoodCloud**. Mueva el interruptor para habilitar GoodCloud.

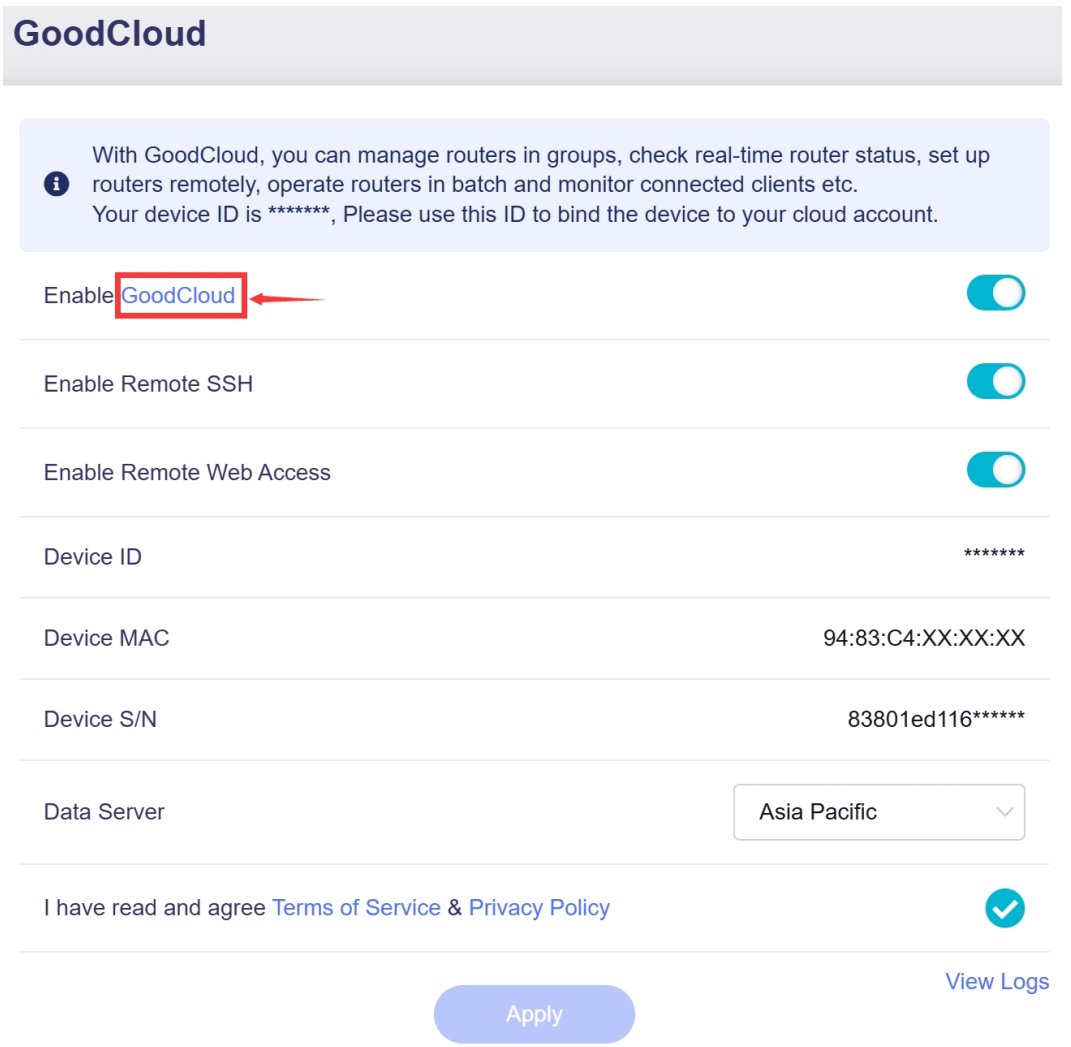


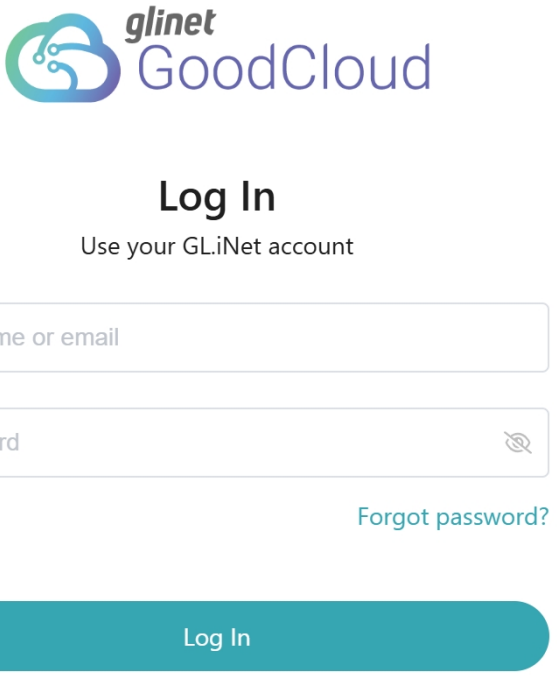
Habilite **Acceso remoto SSH** y **Acceso web remoto** si es necesario, seleccione el servidor más cercano, lea y acepte los **Términos de servicio y política de privacidad** y luego haga clic en **Aplicar**.



- **SSH remoto**: Para acceder de forma remota al terminal del enrutador a través de SSH desde la plataforma GoodCloud.
- **Acceso web remoto**: Para acceder de forma remota al Panel de administración web del enrutador a través de HTTP/HTTPS desde la plataforma GoodCloud.
- **Servidor de datos**: elija el servidor más cercano a la ubicación de su dispositivo. Hay tres opciones: Asia Pacífico (Japón), América (Oregón) y Europa (Irlanda).
- **Ver registros**: Redirigir a la página de registro y mostrar la nube log.

2. Haga clic en GoodCloud para ir a la página de inicio de sesión e inicie sesión con su cuenta GL.iNet Cloud. Si'no tiene una cuenta, regístrese para obtener una e inicie sesión. Una vez haya iniciado sesión, el enrutador se vinculará a su cuenta automáticamente.

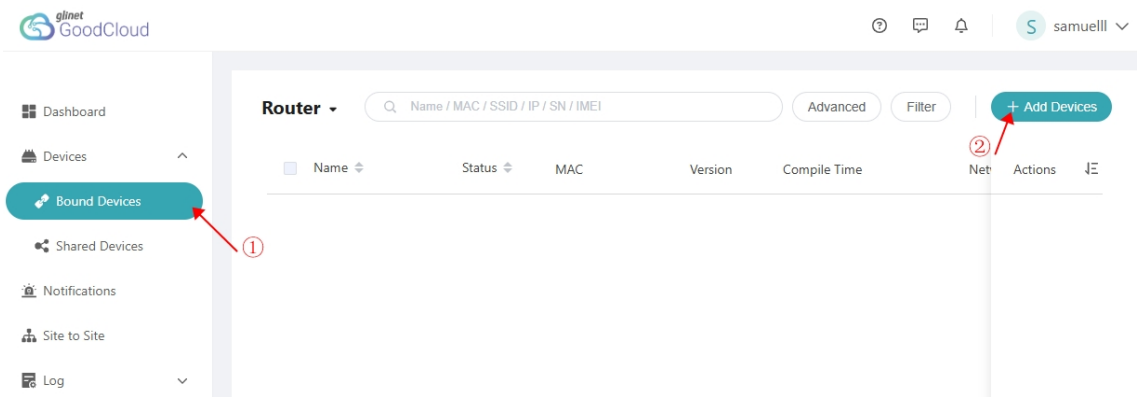




Consejos:

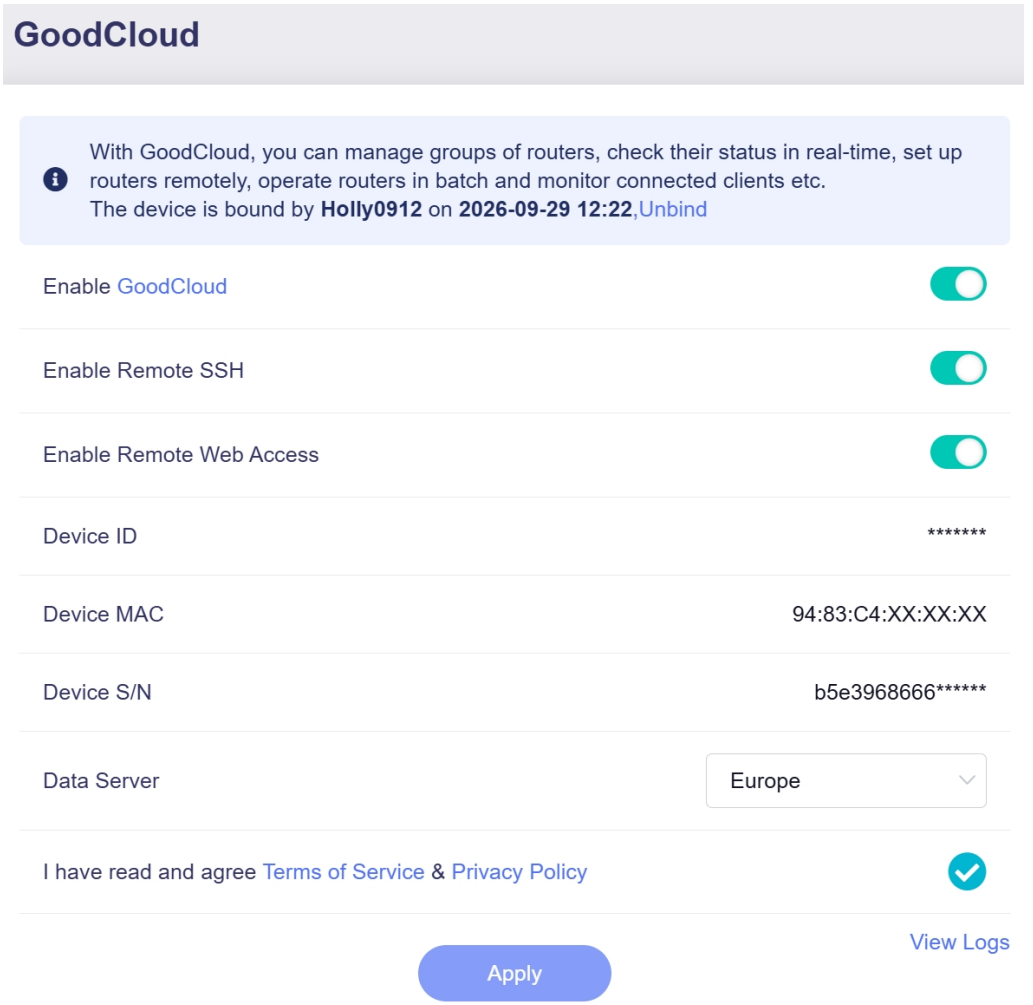
- Los pasos de vinculación de GoodCloud difieren según la versión del firmware.
- Si no recibe el correo electrónico de verificación, revise su carpeta de correo no deseado o inténtelo nuevamente más tarde. Para más ayuda, contáctenos en support@gl-inet.com.

3. En la plataforma en la nube, navegue hasta **Dispositivos** > **Dispositivos vinculados** > **Agregar dispositivos**.



Existen tres métodos para vincular el dispositivo a su cuenta de GoodCloud: descubrimiento automático, adición manual e importación masiva. Haga clic aquí para obtener más detalles.

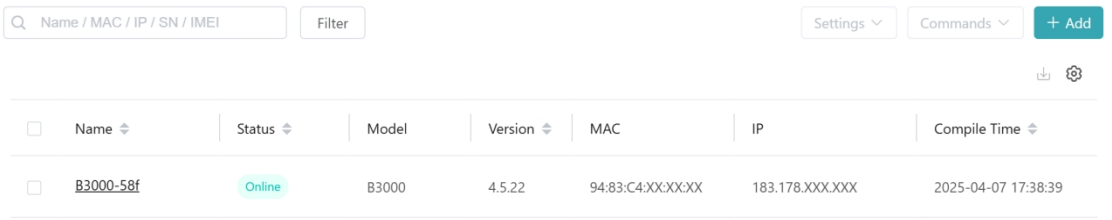
4. Después de la vinculación exitosa, regrese al Panel de administración web del enrutador y navegue hasta **APLICACIONES** > **GoodCloud**. Esta página muestra los detalles de vinculación, incluido el nombre de usuario y la hora de vinculación.



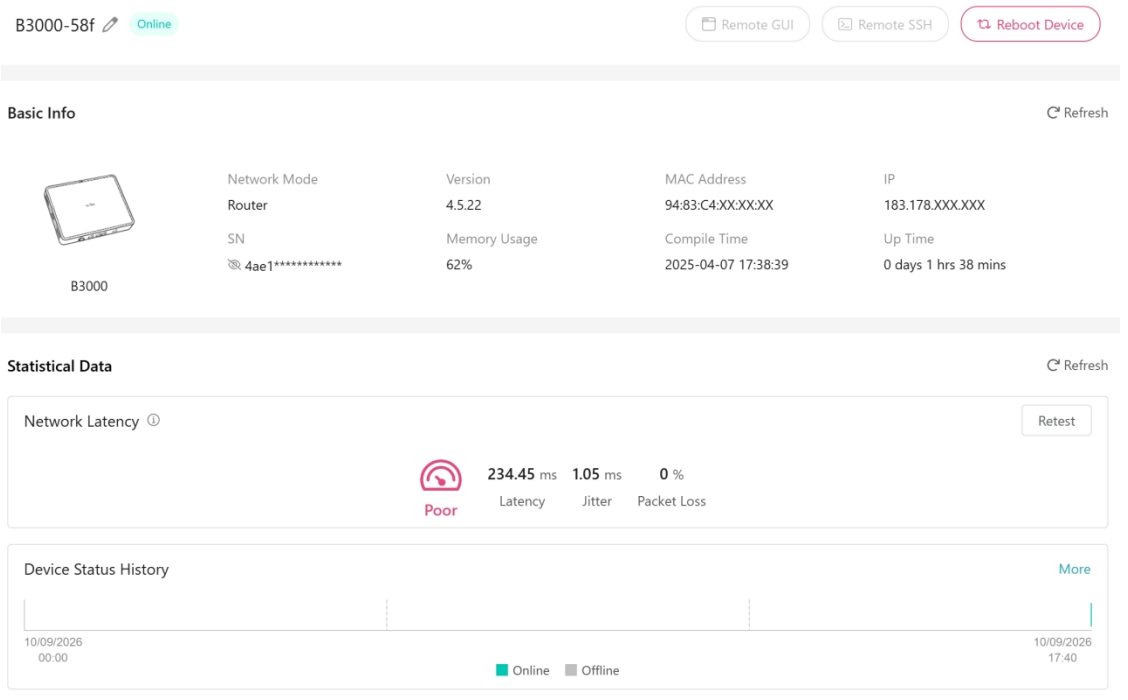
12.3.2 Administrar el enrutador

Consultar los detalles del dispositivo

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

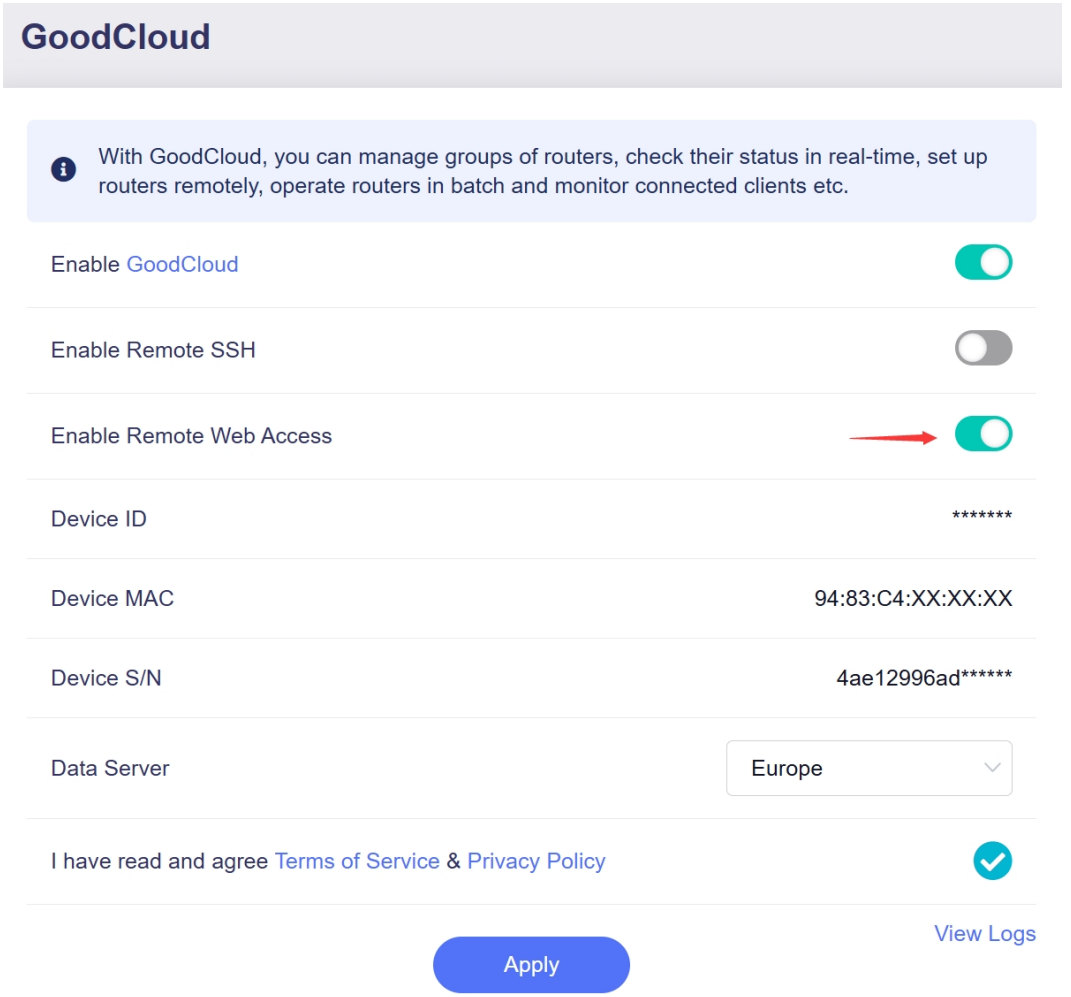


Haga clic en el nombre del dispositivo para ingrese a la página de detalles del dispositivo, que muestras información básica, datos estadísticos, descripción general de la red, lista de clientes y cronograma. También puede realizar operaciones avanzadas, como acceso remotolying al enrutador, y reiniciando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

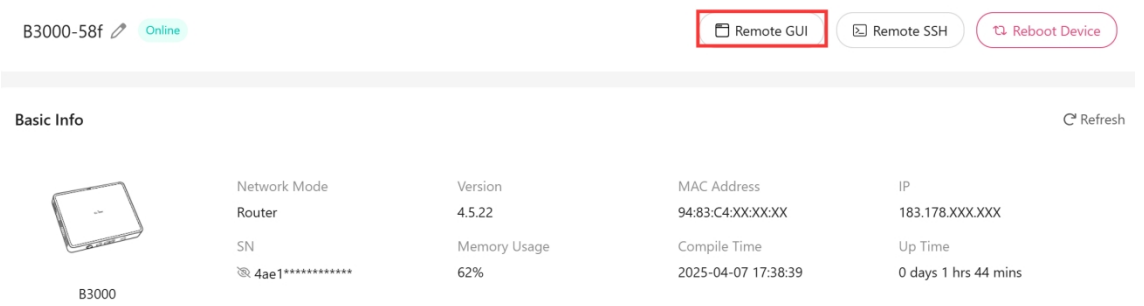


Acceso web remoto

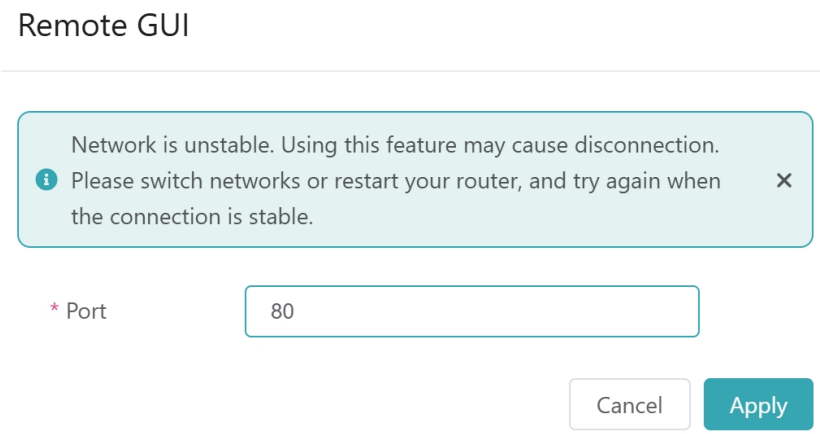
1. Inicie sesión en el panel de administración web del enrutador', navegue hasta **APLICACIONES** > **GoodCloud**, habilite **Acceso web remoto**, luego haga clic en **Aplicar**.



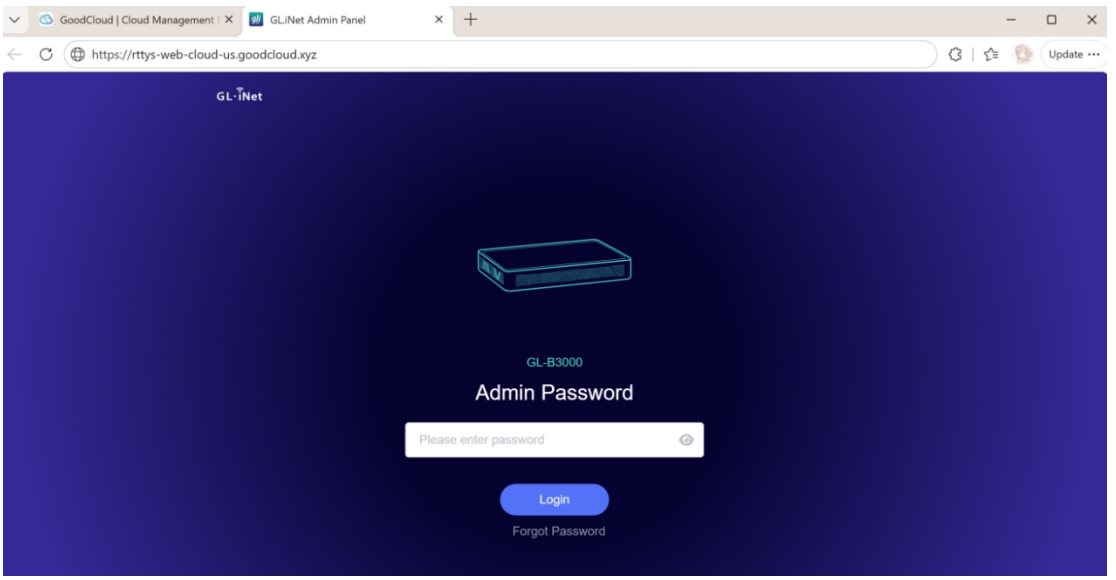
2. Inicie sesión en la plataforma GoodCloud y navegue hasta **Dispositivos** > **Dispositivos vinculados**. Haga clic en el dispositivo al que desea acceder e ingresará a la página de detalles del dispositivo.
3. En la página de detalles del dispositivo, haga clic en **GUI remota** en la esquina superior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



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

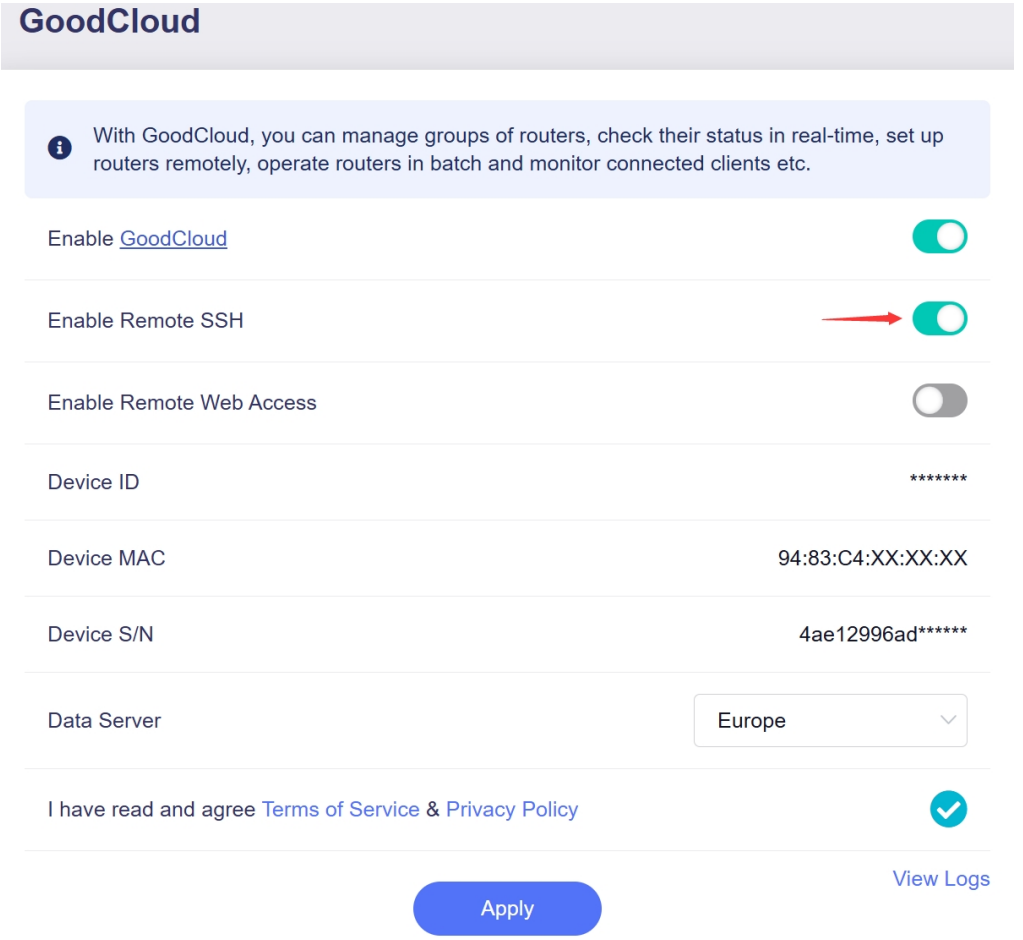


5. Será redirigido a la página de inicio de sesión del enrutador'. Ingrese la contraseña de administrador para acceder de forma remota al panel de administración web del enrutador'.

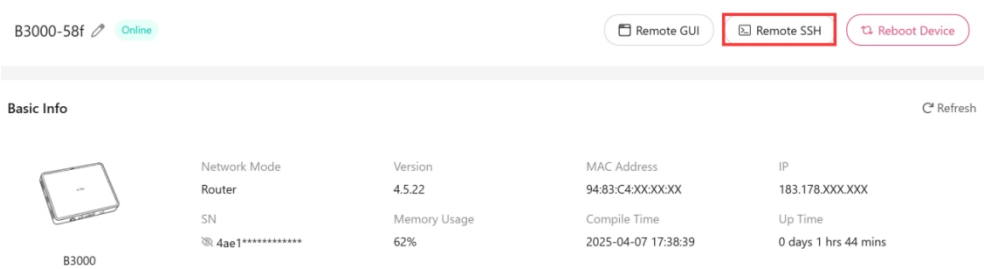


Acceso remoto SSH

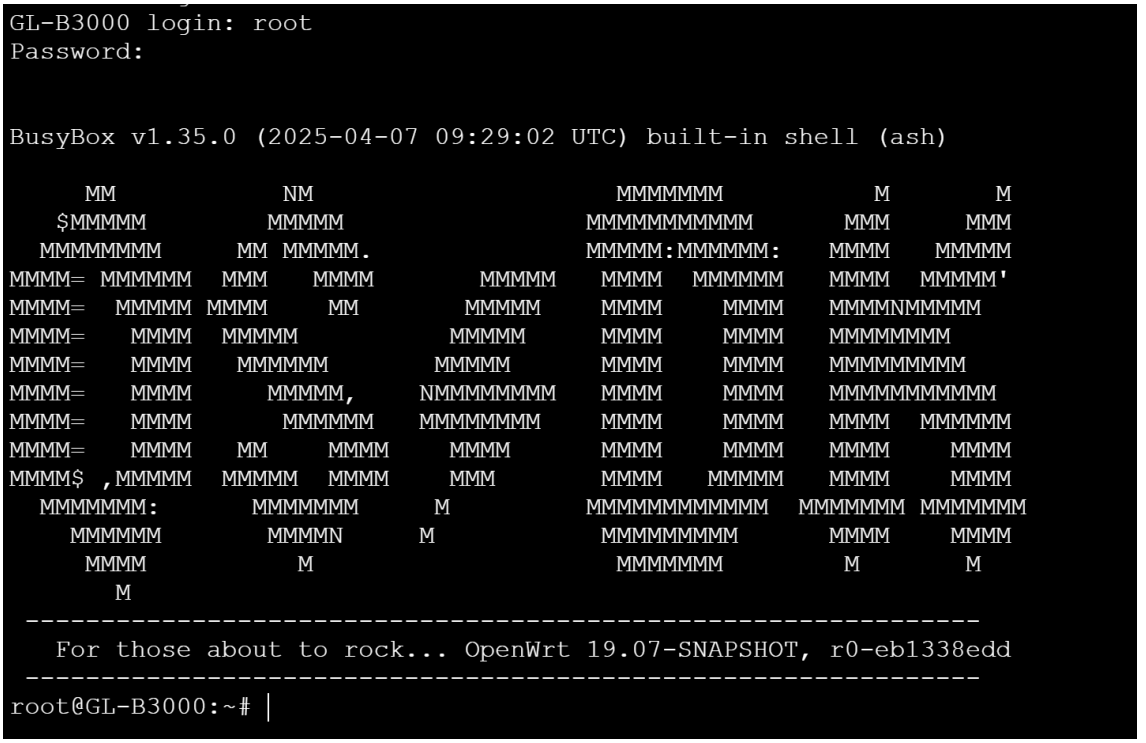
1. Inicie sesión en el panel de administración web del enrutador', navegue hasta **APLICACIONES** > **GoodCloud**, habilite **Acceso remoto SSH**, luego haga clic en **Aplicar**.



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

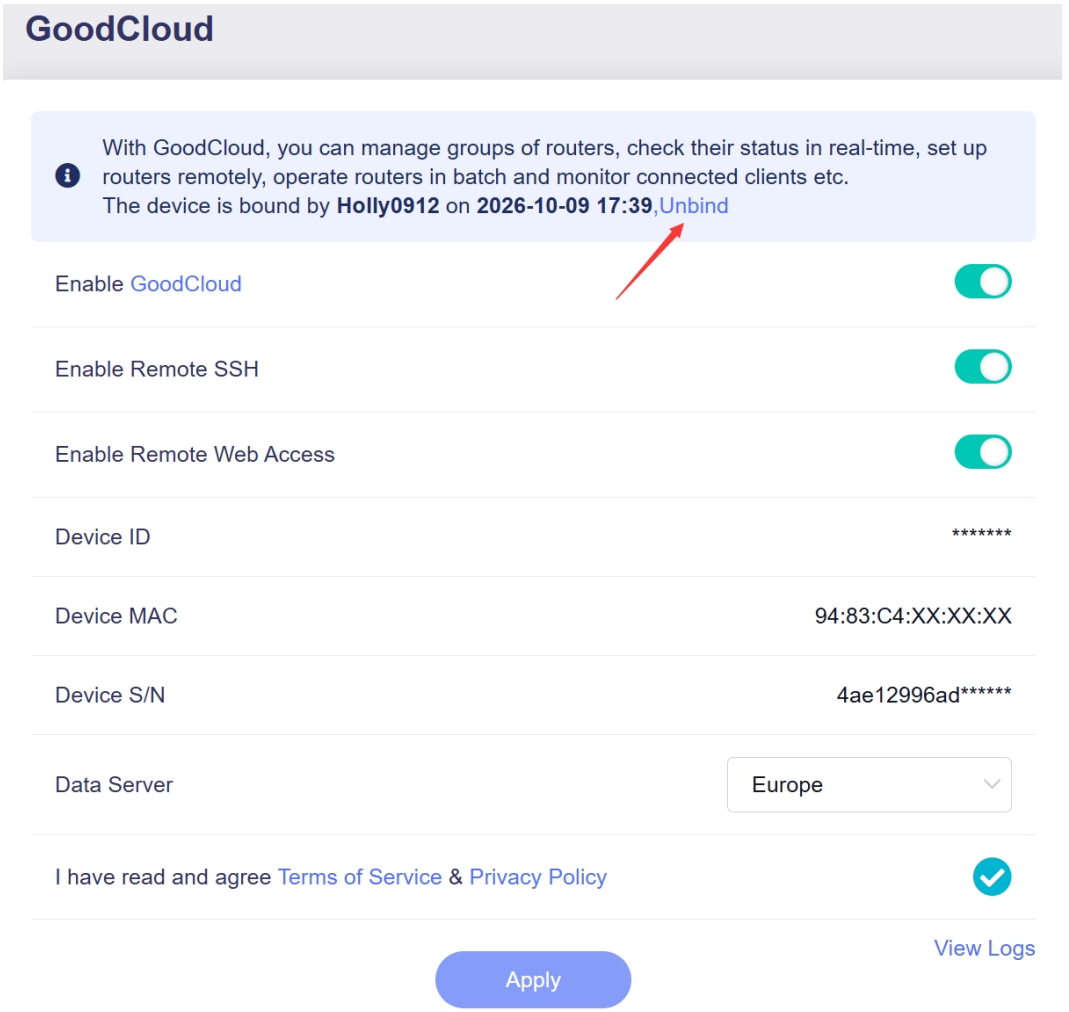


4. Inicie sesión como **root** e ingrese la contraseña para acceder al terminal de su enrutador.

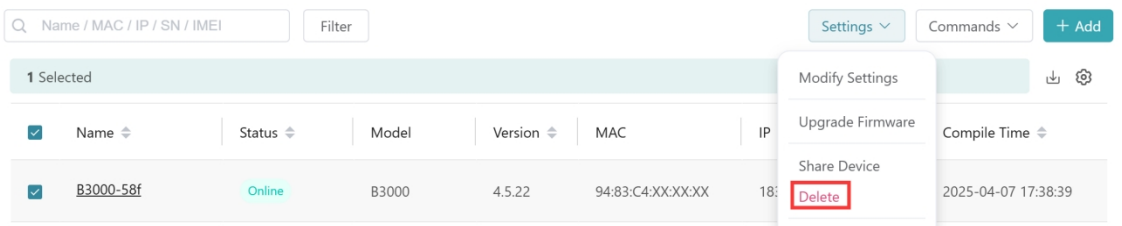


12.3.3 Desvincular el dispositivo

En el panel de administración web del enrutador', haga clic en **Desvincular**. Su dispositivo se desvinculará de su cuenta de GoodCloud.



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

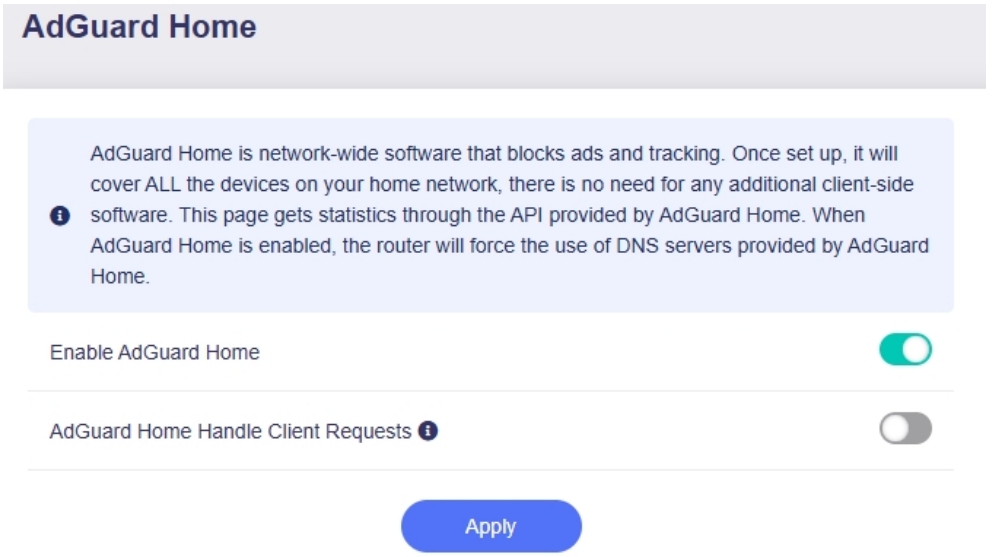


12.4 AdGuard Home

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

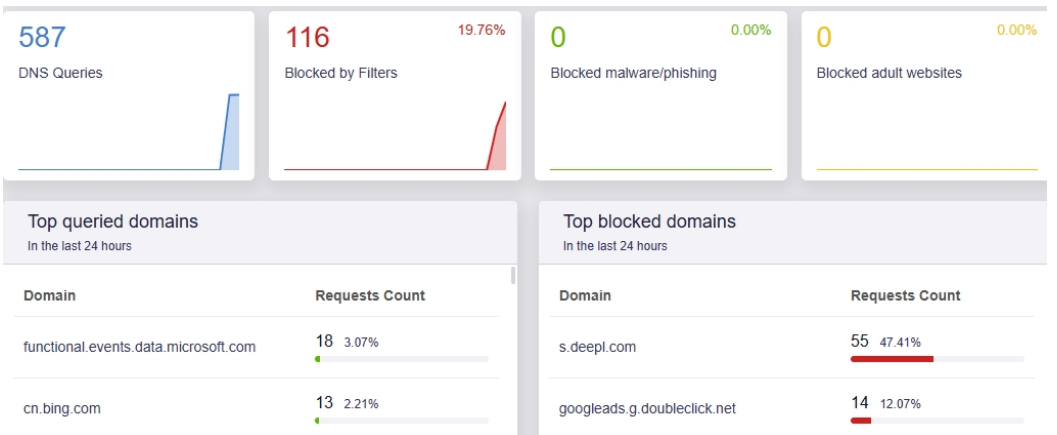
Siga estos pasos para configurar AdGuard Home.

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

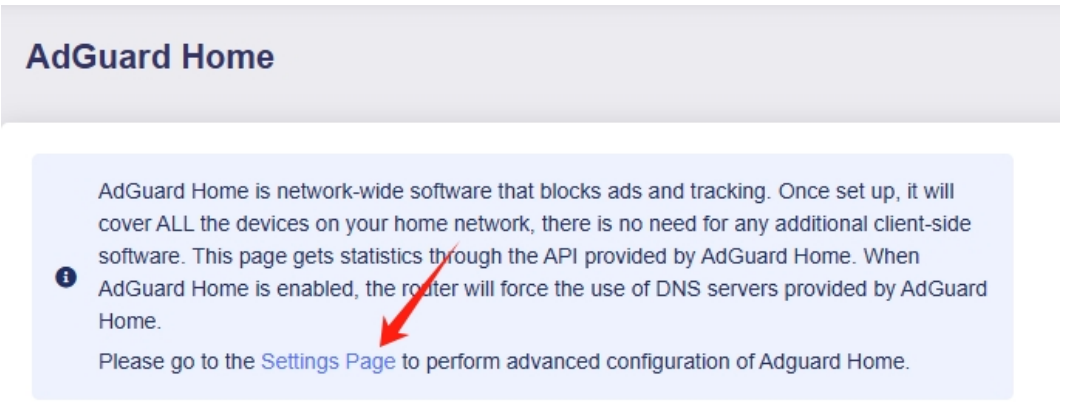


- **AdGuard Home Handles Solicitudes de clientes**: si está habilitado, AdGuard Home manejará directamente las consultas de DNS de los dispositivos cliente, pero esto hará que las políticas VPN basadas en dominios falla.

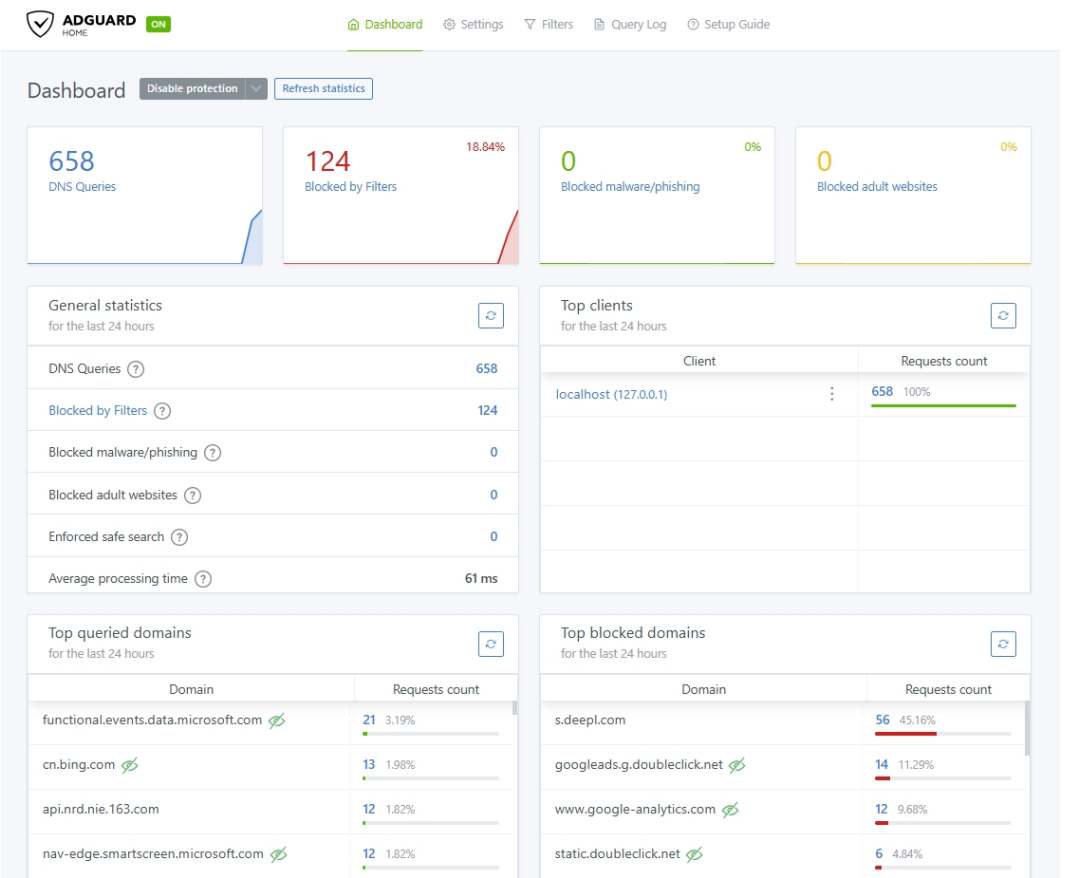
2. La página cargará automáticamente estadísticas DNS (consultas, dominios bloqueados, etc.) a través de la API proporcionada por AdGuard Home.



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



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



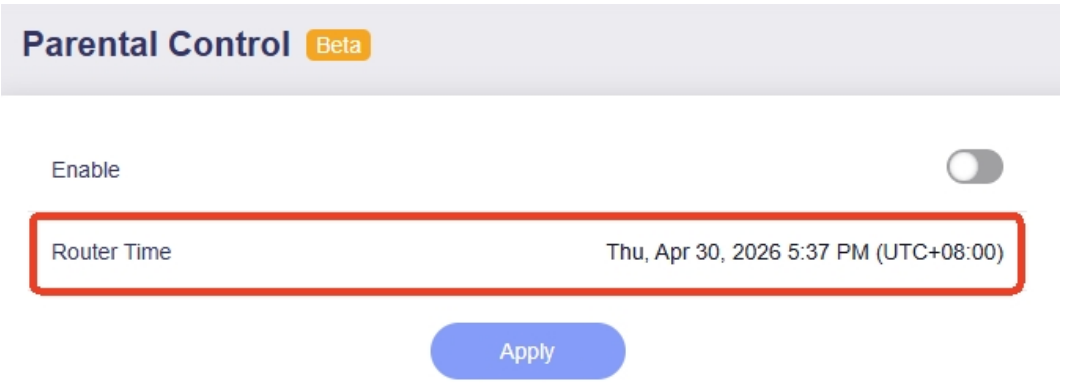
12.5 Control parental

El control parental es una forma de mantener a los niños seguros en línea mediante bloquear sitios web inapropiados y limitar el tiempo que utilizan 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.

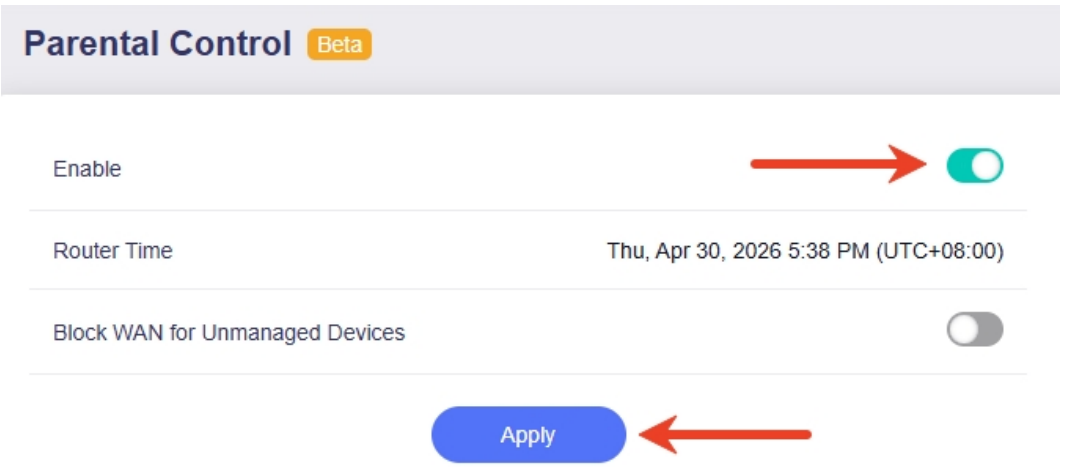
12.5.1 Configuración rápida

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

1. Inicie sesión en el enrutador's web admin panel y vaya a **APLICACIONES** > **Control parental.** Asegúrese de que la hora del enrutador sea precisa. Si no, ve a **SISTEMA** > **Zona horaria** para sincronizarlo primero.



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



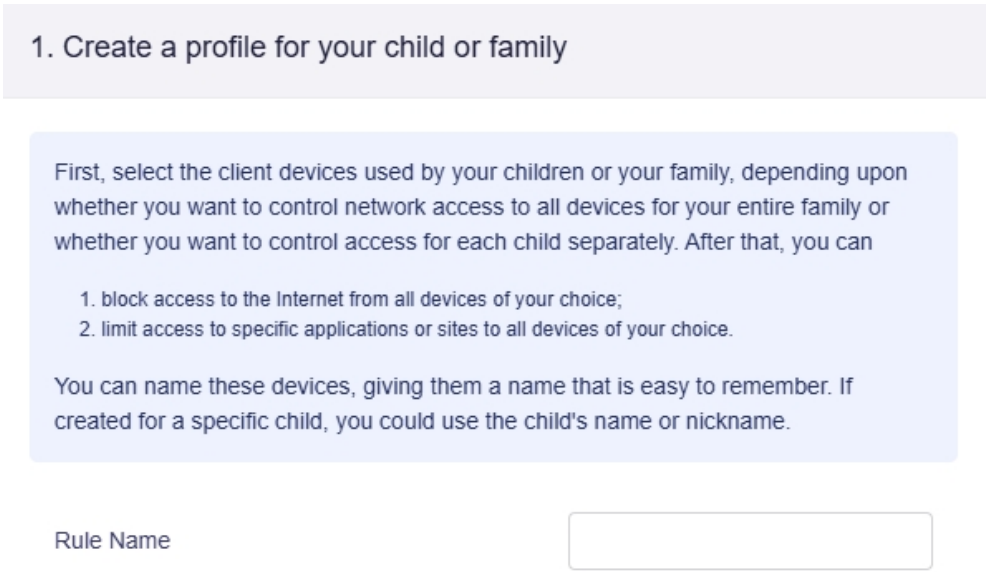
- **Bloquear WAN para dispositivos no administrados**: Bloquea el acceso a Internet para todos los dispositivos que no están en la lista de Control parental.

Aquí hay un caso de uso para su referencia.

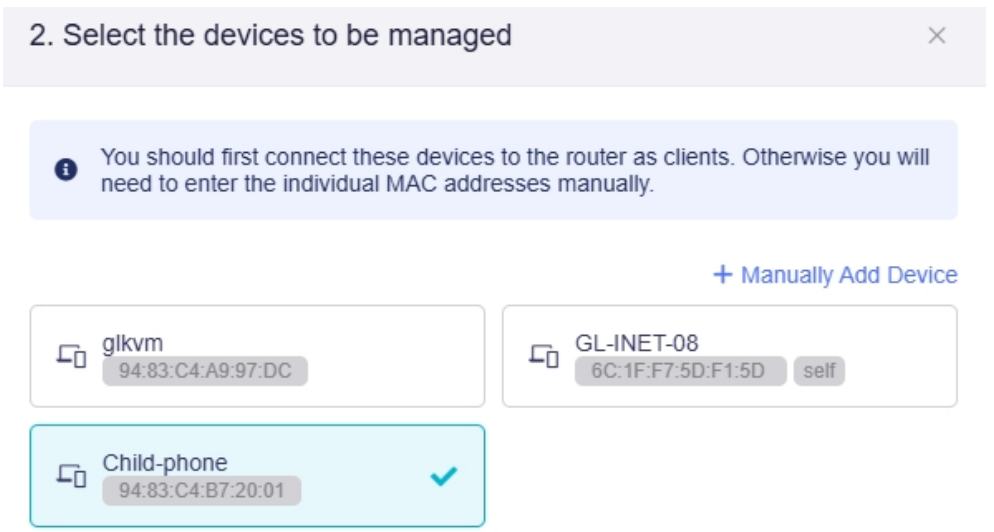
Escenario: Los dispositivos en estees perfil solo pueden acceder a Internet para estudiar desde las 8 a.m. a 11 a. m. de lunes a viernes y para juegos de 6 p. m. a 8 p. m. los fines de semana. El acceso a Internet está bloqueado de forma predeterminada en todos los demás momentos.

Pasos de configuración:

1. Cree un perfil y personalice un nombre.



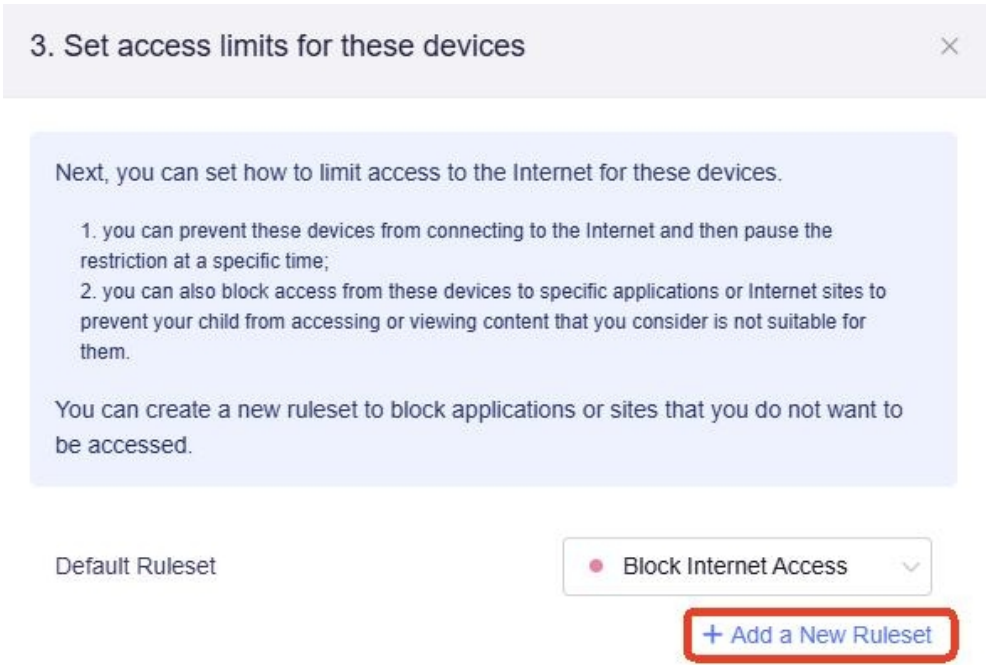
2. Seleccione los dispositivos que desea administrar. Conéctelos primero al enrutador. Si no se han conectado al enrutador, agréguelos manualmente ingresando sus direcciones MAC.



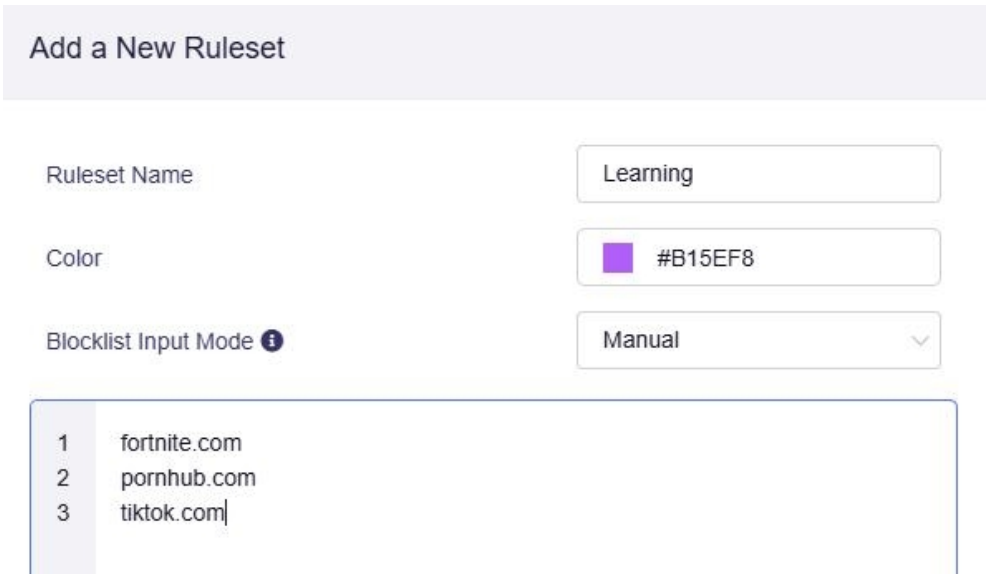
3. Establezca el límite de acceso.

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

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

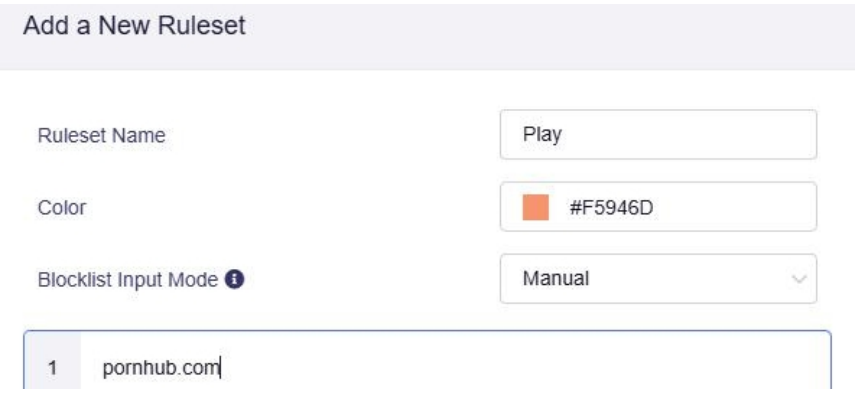


   Especifique el nombre del conjunto de reglas (por ejemplo, Aprendizaje) y color, ingresar a la websitios to bloquear, luegoluego haga clic en **Aplicar**.

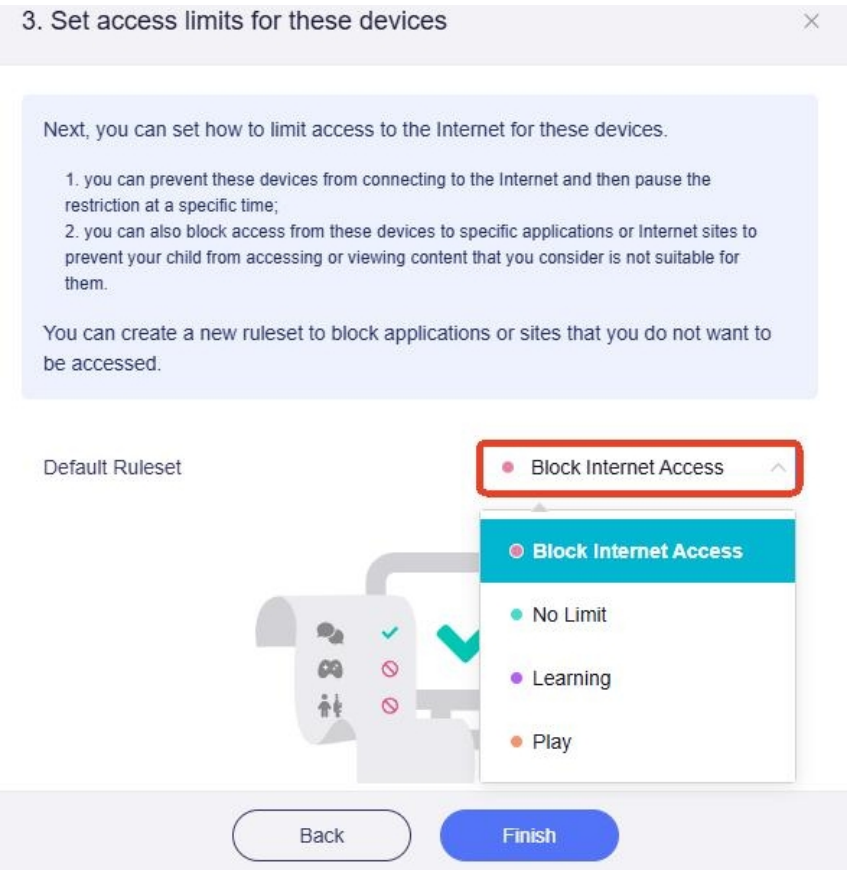


Nota: Los nombres de dominio ingresados en la lista de bloqueo deben incluyen sus subdominios. Por ejemplo, si se ingresa "ejemplo.com", también incluye cualquier subdominio, como "subdominio.example.com".

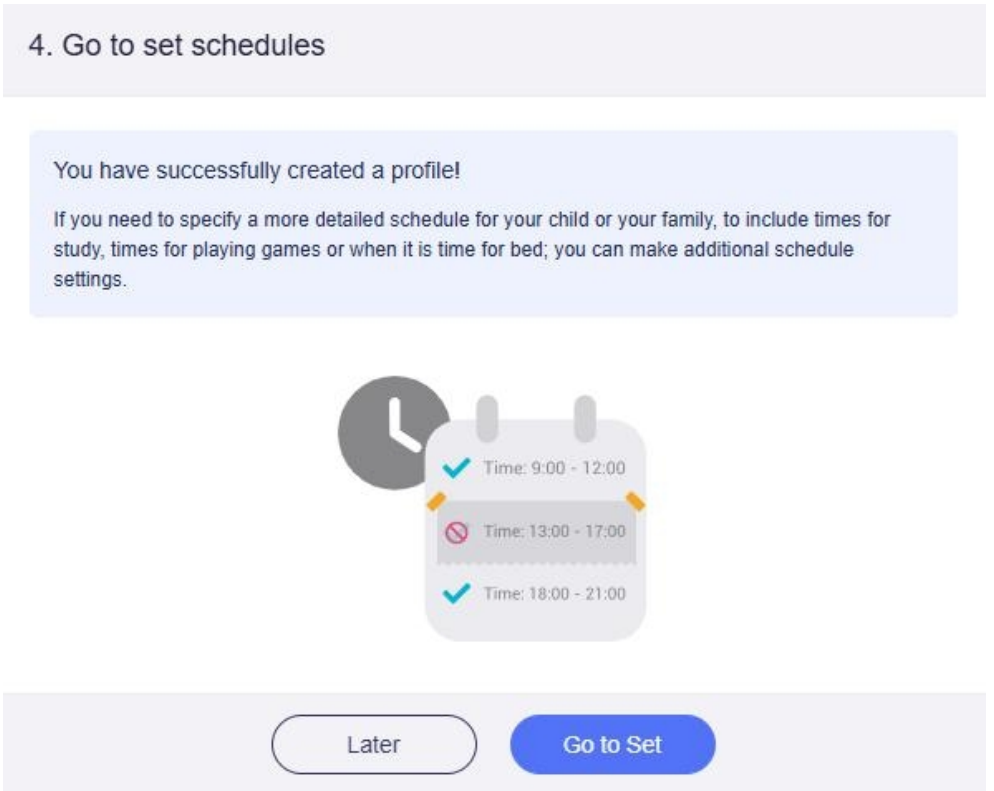
Del mismo modo, cree otro conjunto de reglas. Especifique el nombre del conjunto de reglas (por ejemplo, Reproducir) y el color, ingrese los sitios web que desea bloquear y luego haga clic en **Aplicar**.



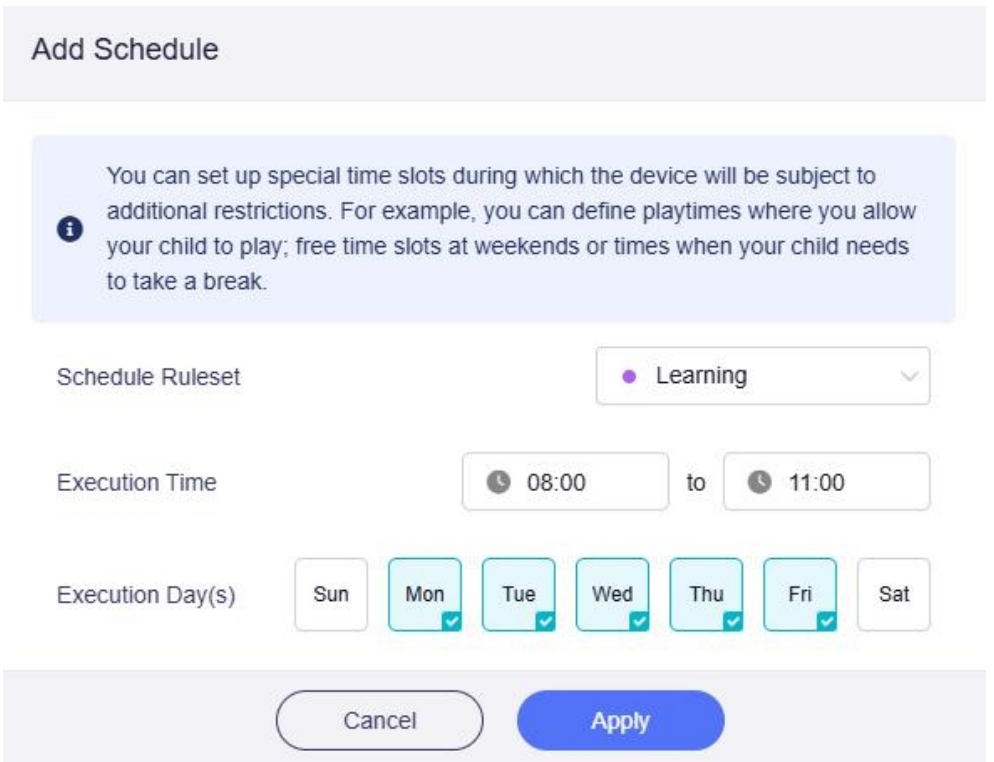
Al aplicared, habrá un total de cuatro conjuntos de reglas. Sseleccione **Bloquear acceso a Internet** como el **predeterminado Conjunto de reglas** y haga clic en **Finalizar**.



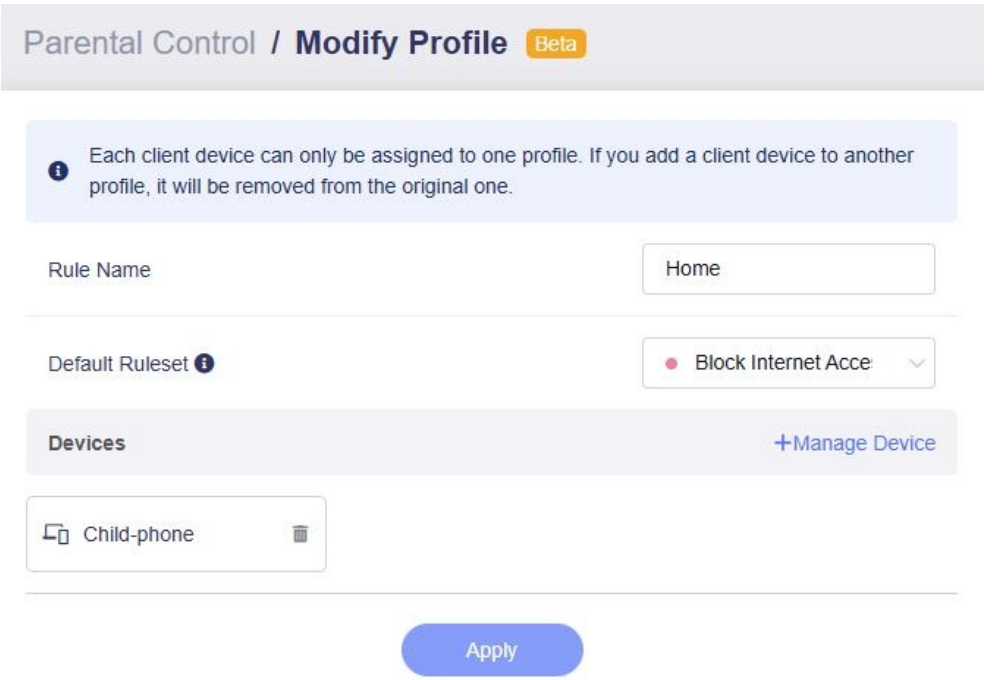
4. A continuación, establezca la programación para su perfil. Haga clic en **Ir a Establecer**.



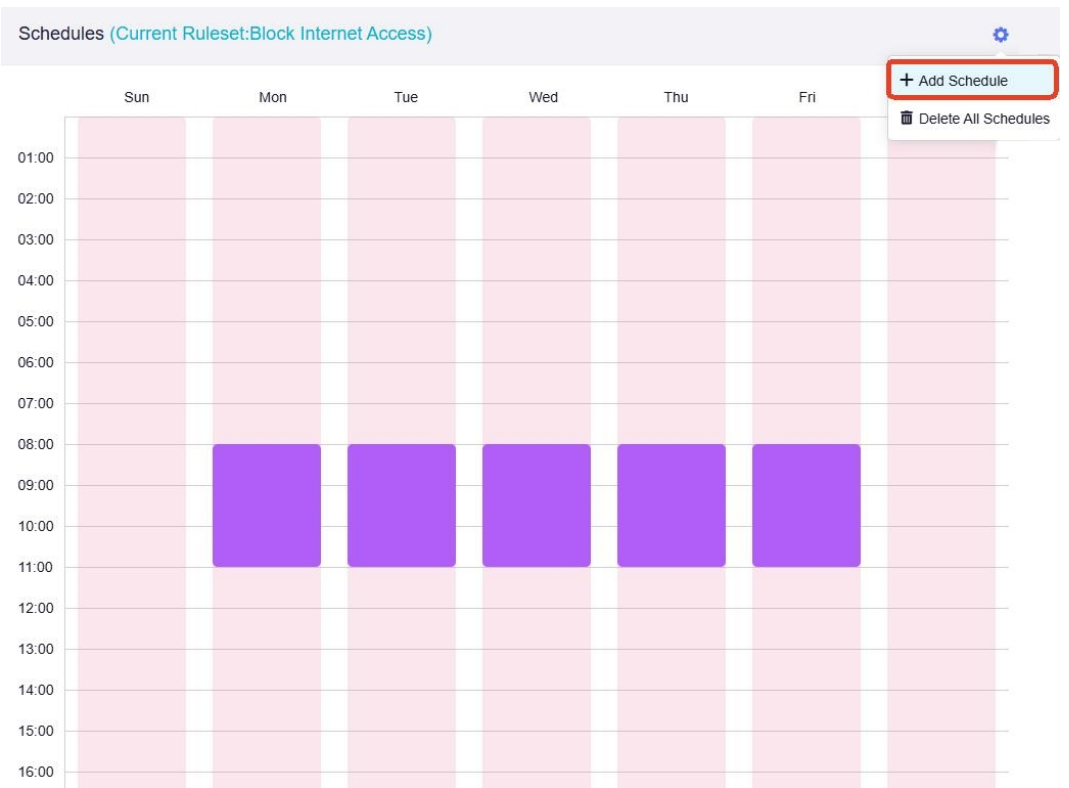
Agregue el conjunto de reglas **Aprendizaje** a la programación. Establezca el **Hora de ejecución** de 8 a.m. a 11 a.m. de lunes a viernes y luego haga clic en**Aplicar**.



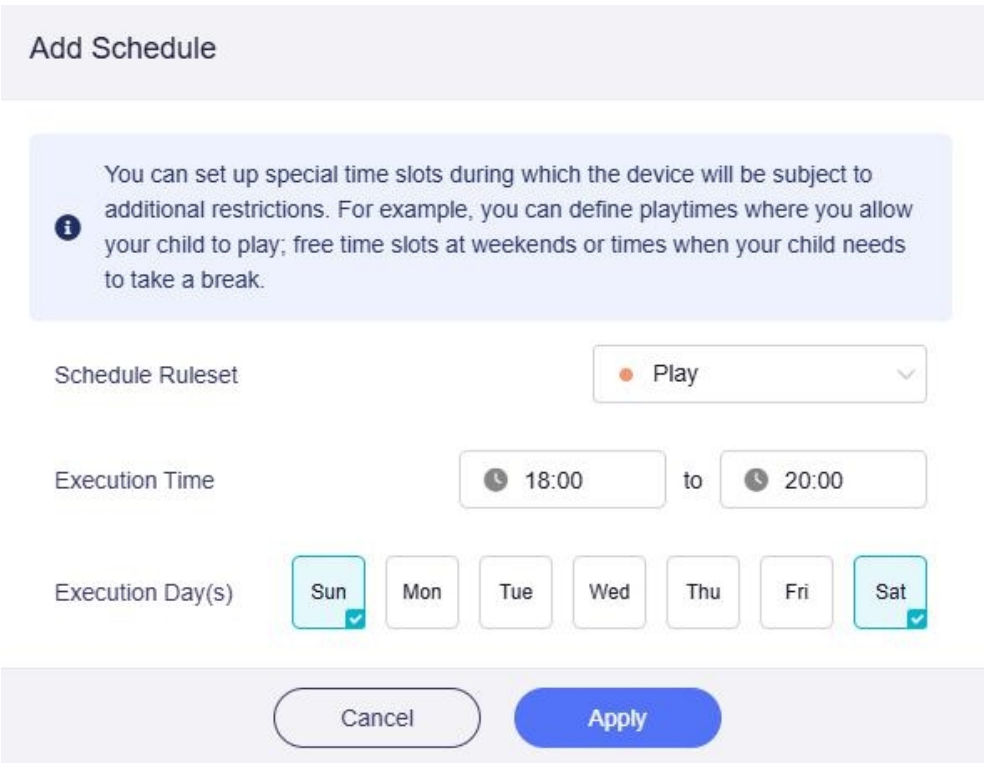
5. Será redireccionado a la página de edición del perfil creado.



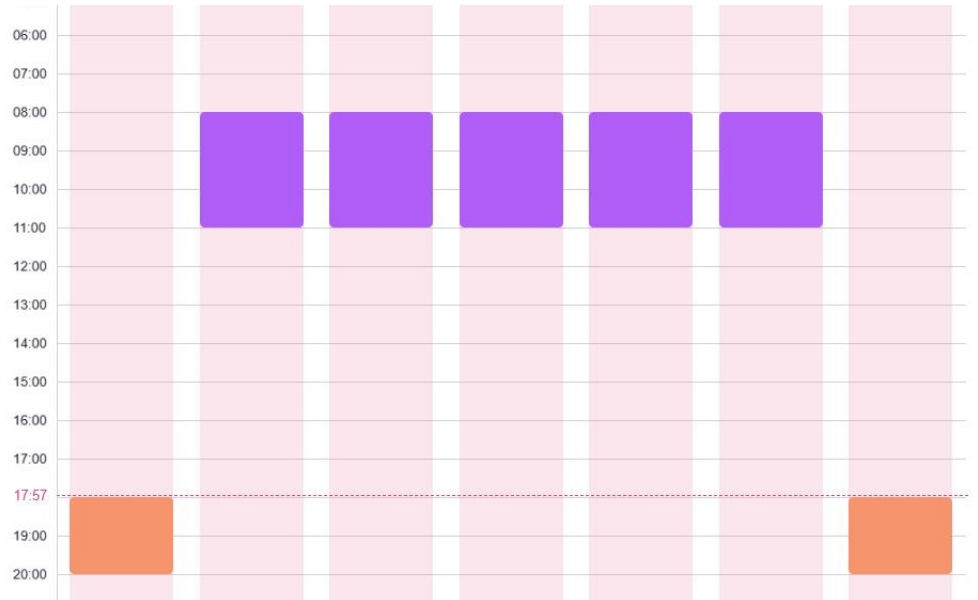
Vaya al final y verá que se ha creado un cronograma. Haga clic en el ícono de ajustes en la esquina superior derecha y seleccione **Agregar programación**.



6. Agregar otro conjunto de reglas **Reproducir** a la programación. Configure el **Tiempo de ejecución** de 6 PM a 8 PM en weekends, luego click **Aplicar**.



El conjunto de reglas de Play se agregará al cronograma.

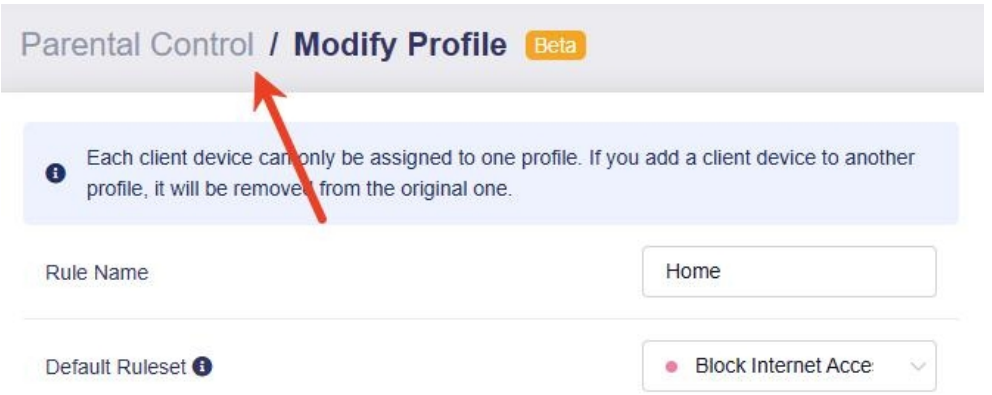


Consejos:

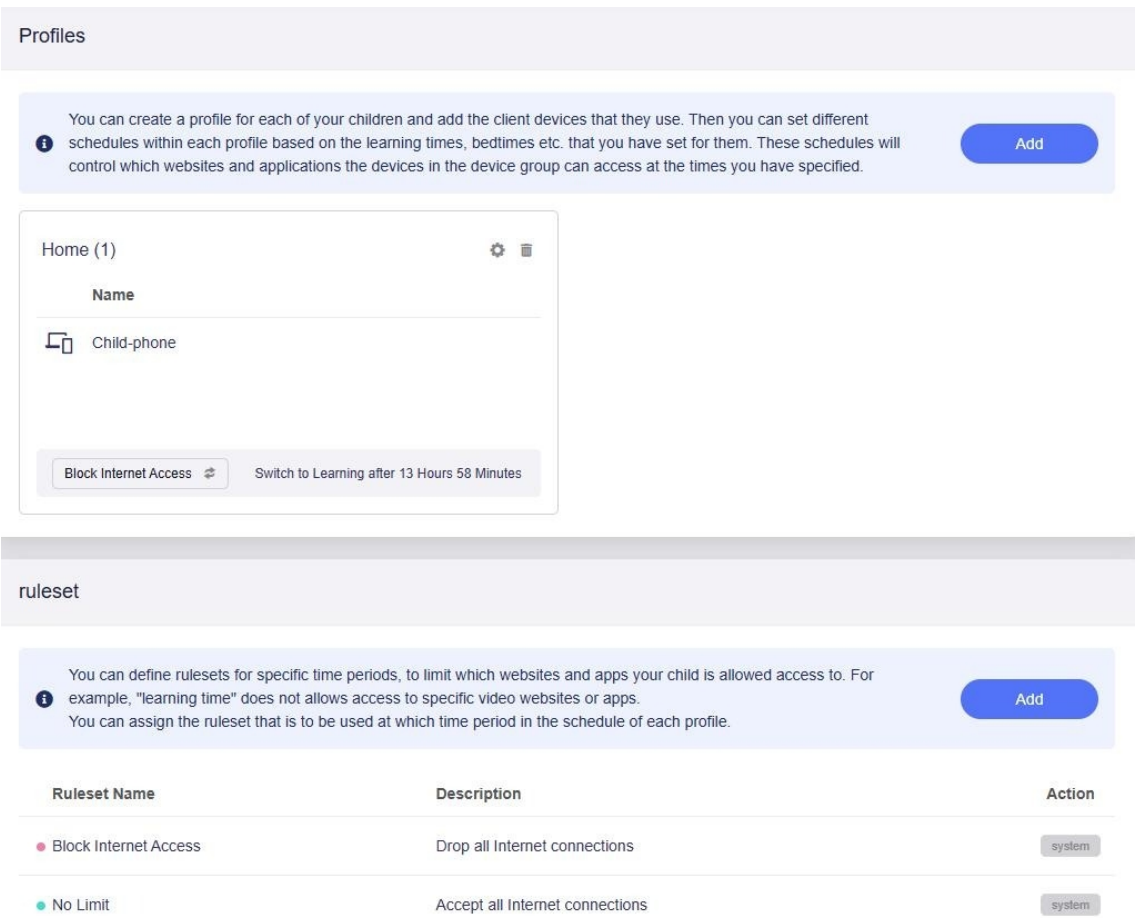
- La línea discontinua roja indica la situación actual tiempo.

- Ypuede modificar el tiempo de ejecución por haciendo clic en en un 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 si es necesario.



12.5.2 Solución de problemas

Si los ajustes configurados no surten efecto, verifique lo siguiente posible causas.

1. Problema de caché de DNS.

   Los navegadores y sistemas operativos mantienen cachés de DNS, lo que puede retrasar la aplicación de 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 Para descubrirlo, 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 MAC aleatoria dirección para cada conexión de red, que impides que las reglas de acceso entren en vigor. Deshabilitar aleatoria Dirección MAC en el dispositivo de destino y luego vuelva a agregar el dispositivo a su perfil.

12.6 ZeroTier

ZeroTier es una red privada virtual (VPN) basada en software que permite comunicaciones seguras y cifradas entre dispositivos a través de Internet. Crea una red virtual privada que permite que los dispositivos se comuniquen como si estuvieran en la misma red local, independientemente de su ubicación física o topología de red. ZeroTier está diseñado para ser fácil de configurar y usar, y ofrece funciones como cifrado de extremo a extremo, segmentación de red y capacidades de puente 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, así como a sus recursos WAN y LAN.

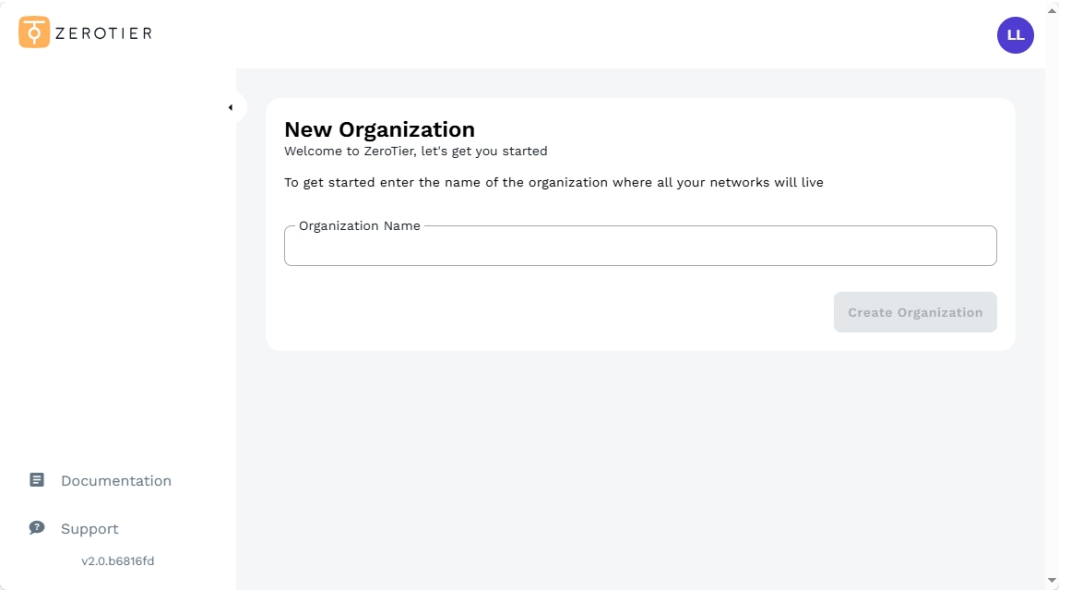
Nota:

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, Sitio a sitio de GoodCloud y Tailscale.
2. Esta función se encuentra actualmente en versión beta y puede tener algunos errores.

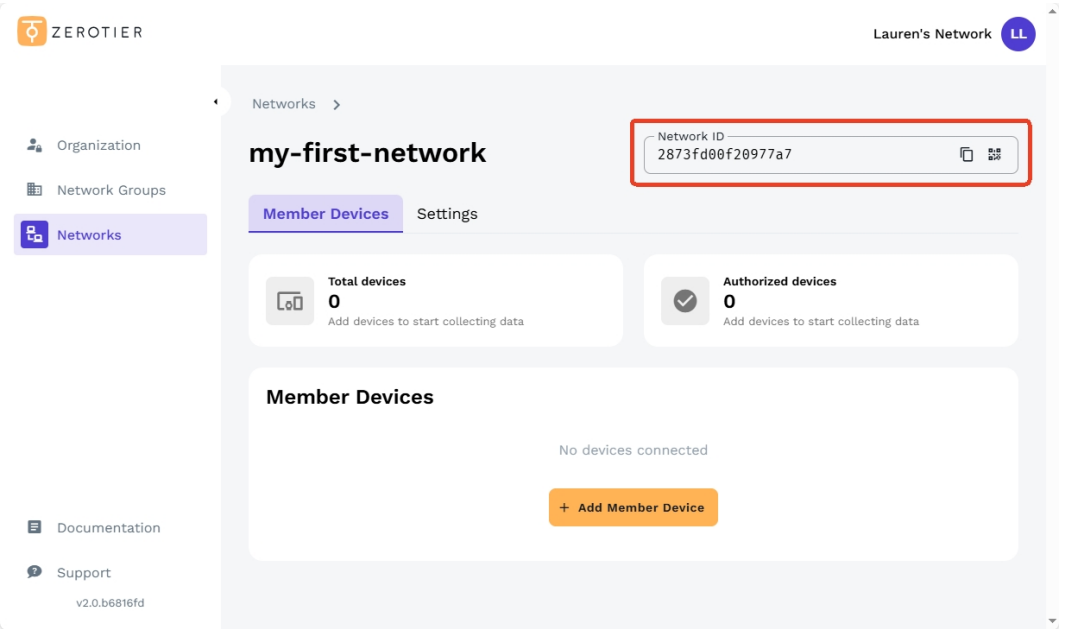
12.6.1 Configurar ZeroTier

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. Crea una organización.

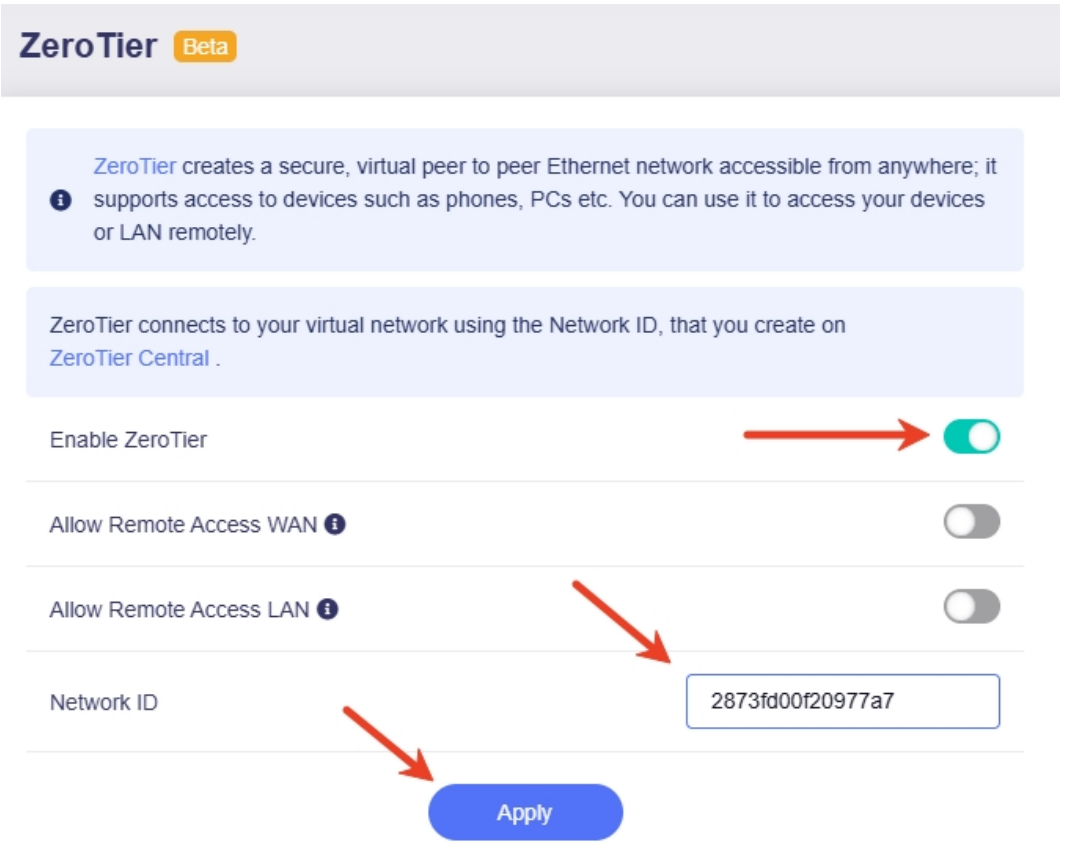


3. Selecciona un plan. Aquí elegimos **plan personal** como ejemplo, que incluye 10 dispositivos, 1 administrador de red y 1 red. Si necesita crear más redes, agregar más dispositivos o agregar rutas y DNS personalizados, elija otro plan pago.
4. Ahora se ha creado su red ZeroTier.

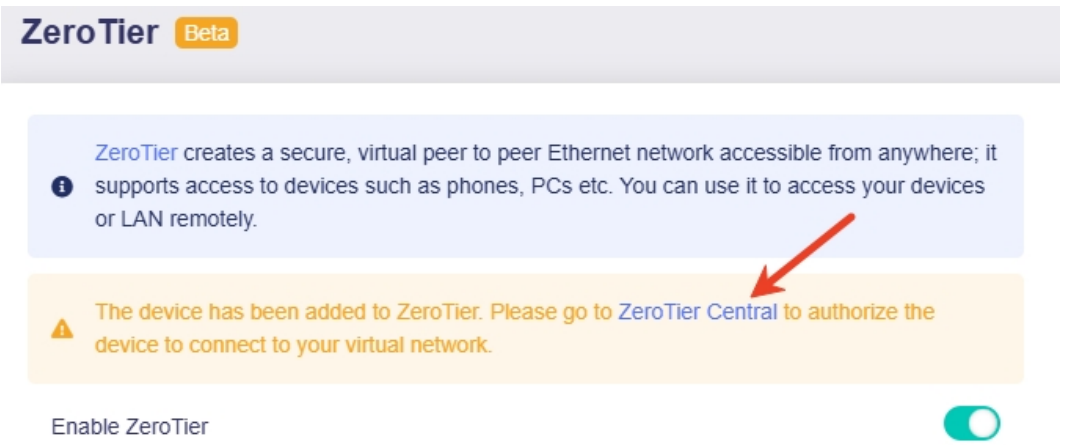


Tome nota del **ID de red**, que es una combinación alfanumérica de 16 caracteres en la esquina superior derecha, ya que será necesario cuando conecte otros dispositivos más adelante.

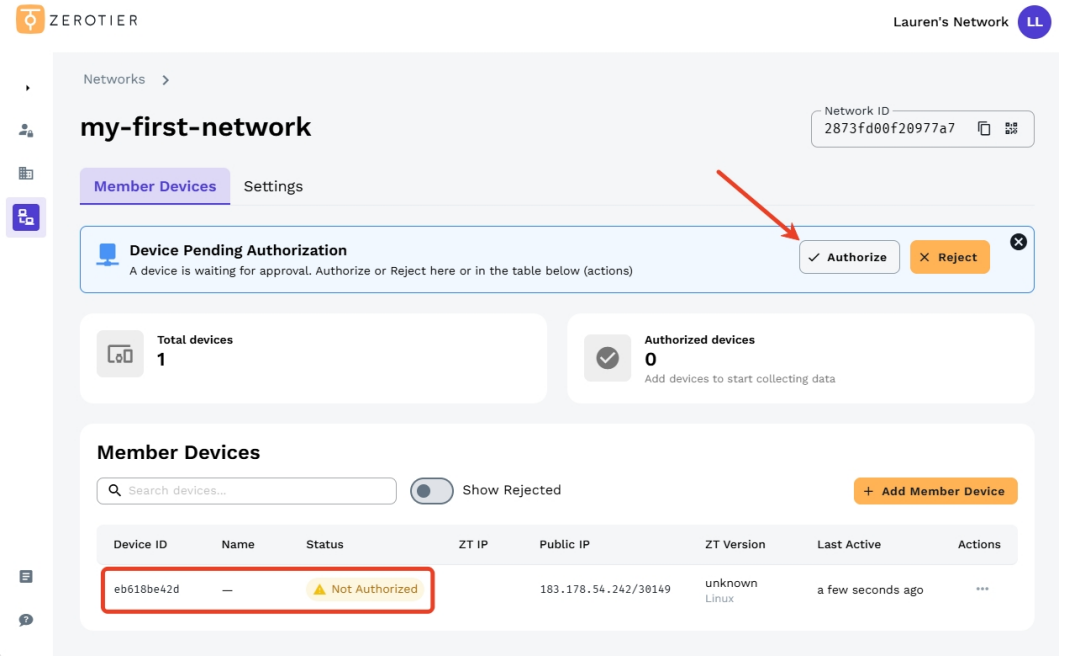
5. Inicie sesión en el panel de administración web de su enrutador y navegue hasta **APLICACIONES** > **ZeroTier**. Habilite ZeroTier, ingrese el **ID de red**, luego haga clic en **Aplicar**.



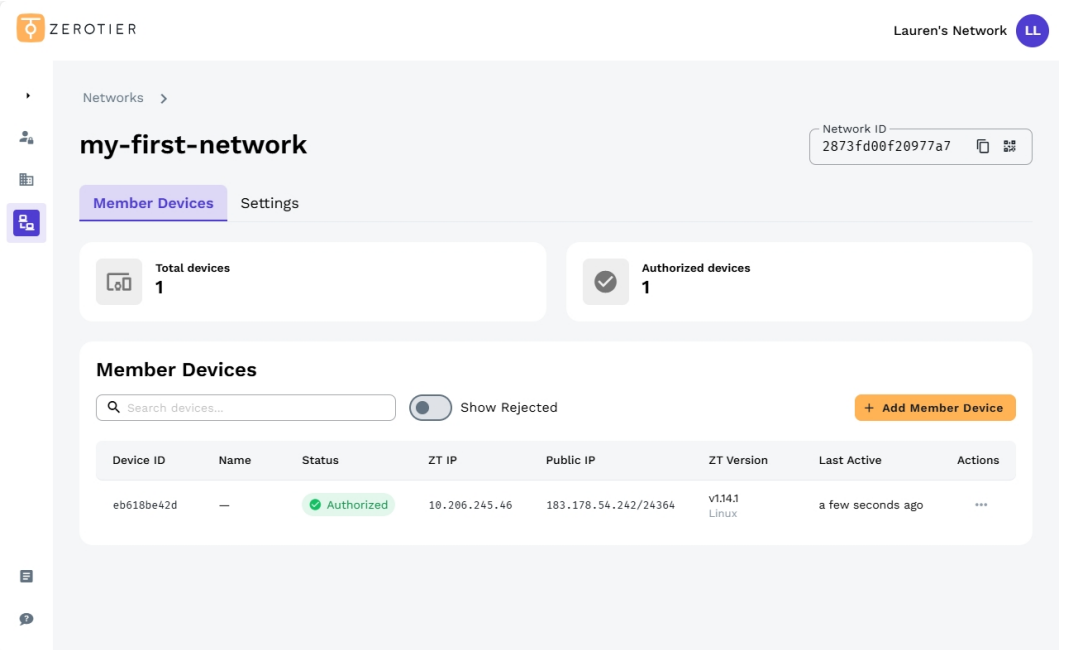
Después de un momento, page indicará que se requiere autorización. Haga clic en el **ZeroTier Central** hipervínculo para redirigir a ZeroTier Central.



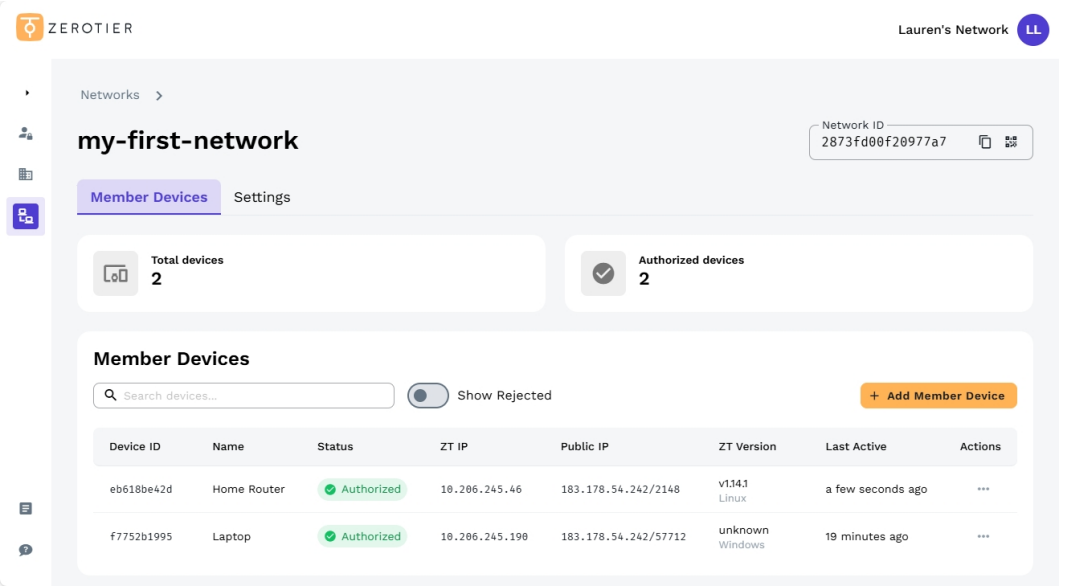
6. En ZeroTier Central, localice el dispositivo pendiente y autorícelo.



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

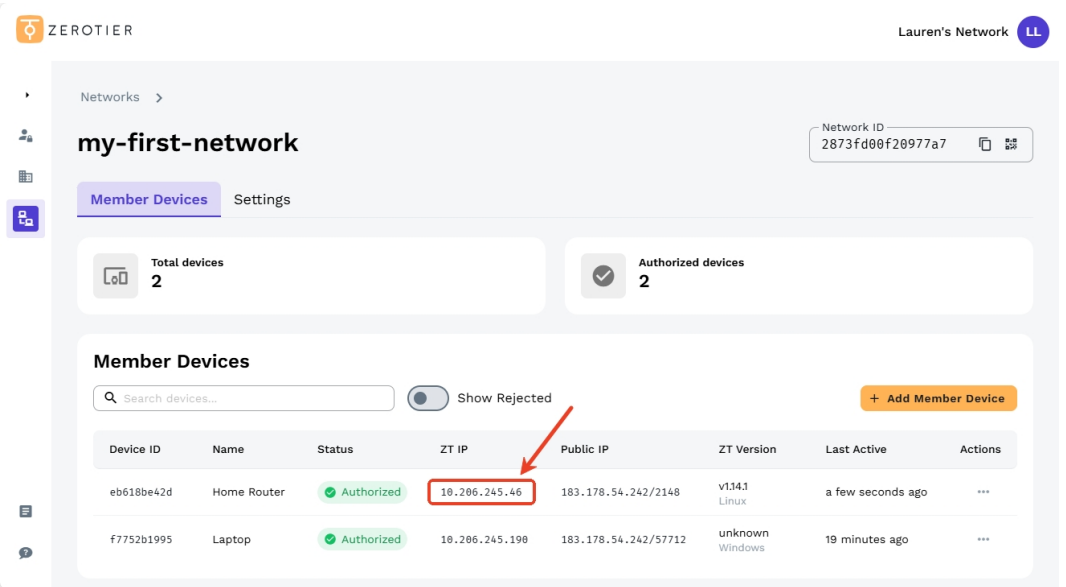


7. Agregue otro dispositivo (como una computadora o un teléfono inteligente) a la misma red ZeroTier siguiendo esta guía. Una vez agregado correctamente, la página se muestra de la siguiente manera. Verá los detalles de los dispositivos miembros, como **ID del dispositivo**, **Nombre**, **Estado**, **IP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



Consejo: 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 la **IP administrada** del enrutador para copiarla.



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

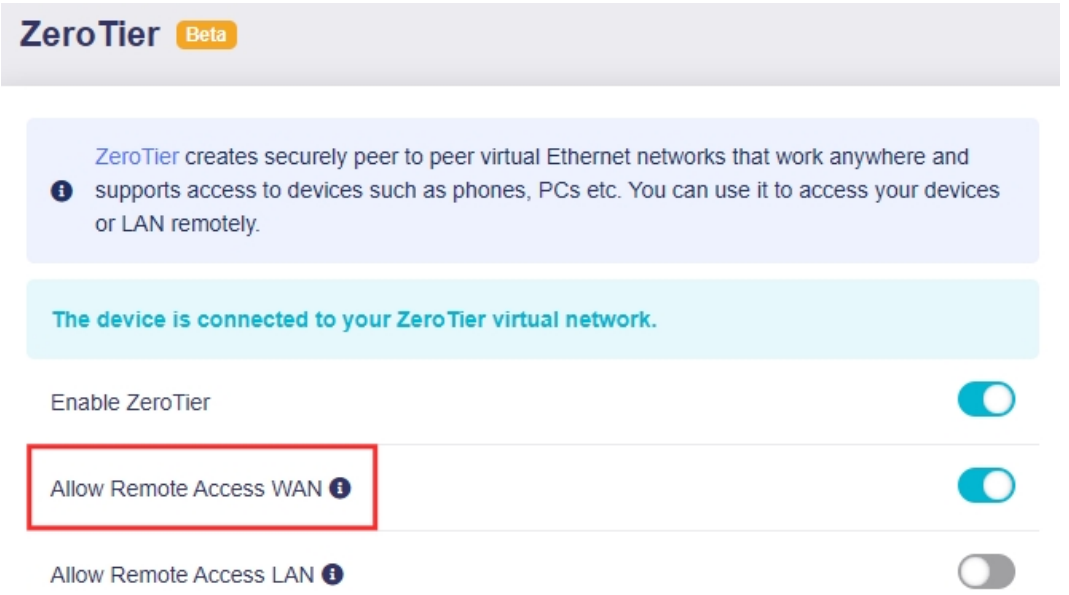
9. Pruebe la conectividad.

   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

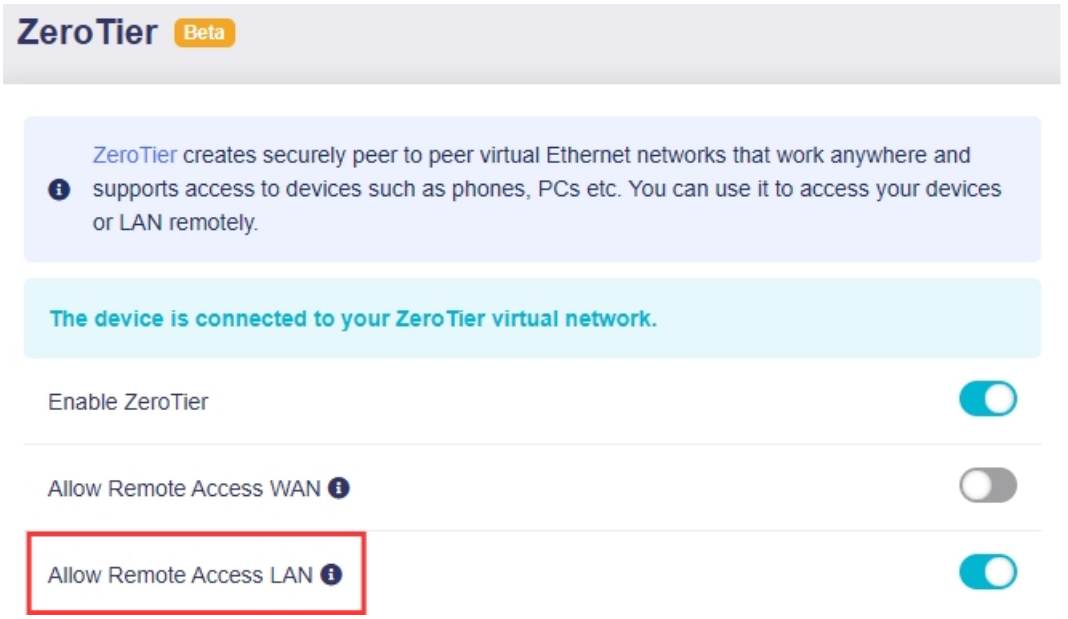
Si esta opción está habilitada, los recursos en el lado WAN del dispositivo pueden ser a la que se accede a través de la red virtual ZeroTier. Consulte aquí para obtener más detalles.



Nota: esta función requiere reglas de enrutamiento para agregarse 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. Consulta 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. Consulta aquí para detalles de precios.

12.7 Tailscale

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

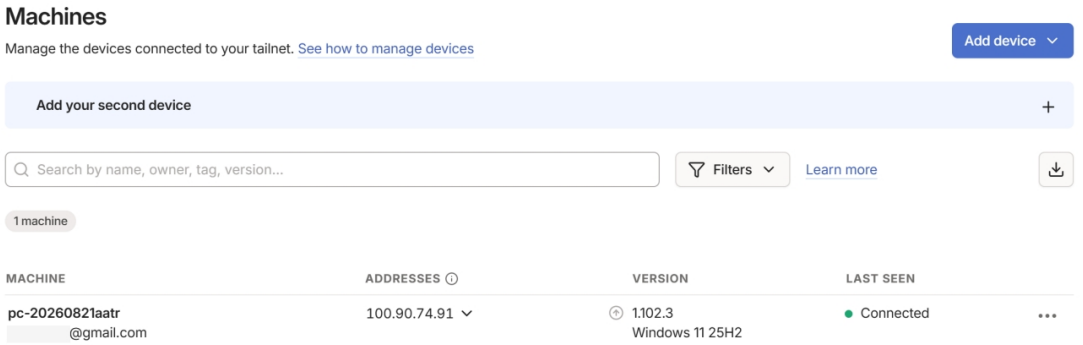
El La función Tailscale en los enrutadores GL.iNet permite que el enrutador se una a una red virtual de Tailscale, lo que permite el acceso remoto al enrutador mismo, así como a sus recursos del lado WAN y LAN.

Nota:

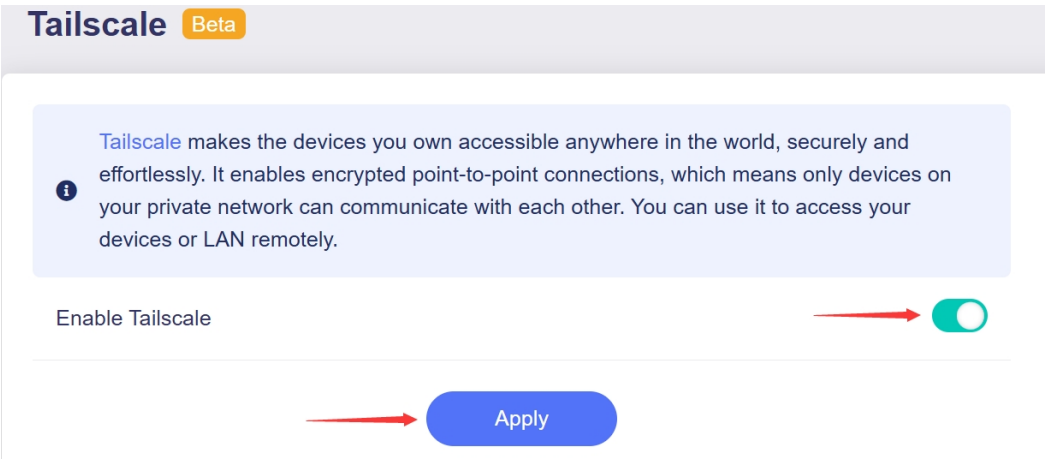
1. Dado que Tailscale se basa en WireGuard, no se recomienda utilizar Tailscale con ninguno de los siguientes funciones o servicios simultáneamente, ya que esto puede causar conflictos de enrutamiento: cliente OpenVPN, cliente WireGuard, sitio a sitio GoodCloud, ZeroTier.
2. Esta función se encuentra actualmente en versión beta y puede tener algunos errores.

12.7.1 Configurar Tailscale

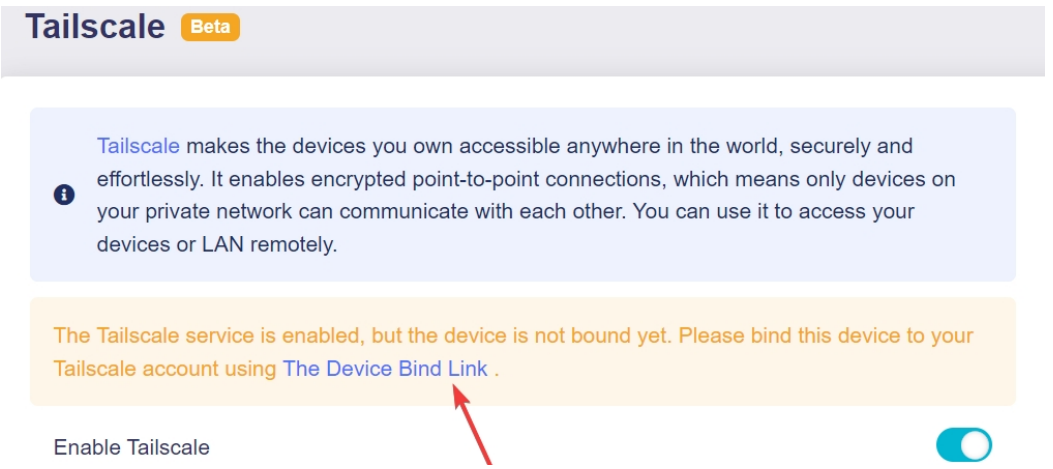
1. Rregistre primero una cuenta de Tailscale y vincule uno o dos dispositivos a su cuenta de Tailscale paracon fines de prueba. Después de vincular, verá sus dispositivos en la suela Tailscale C.



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



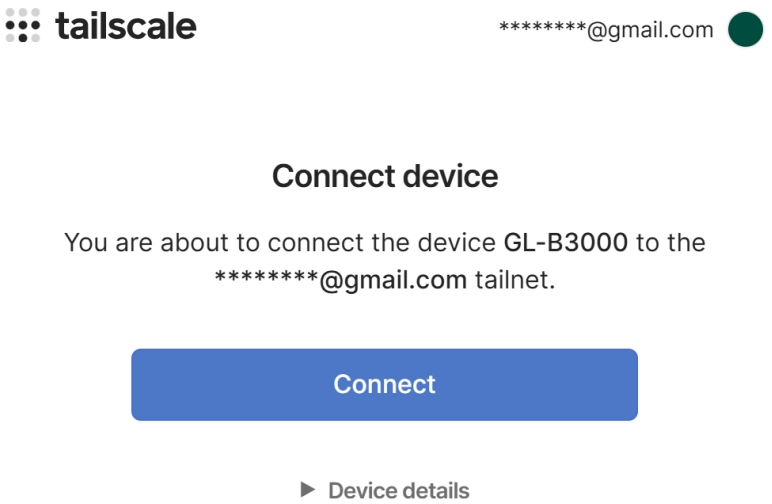
3. La página le indicará para vincular el dispositivo. Haga clic en **Enlace de vinculación del dispositivo**.



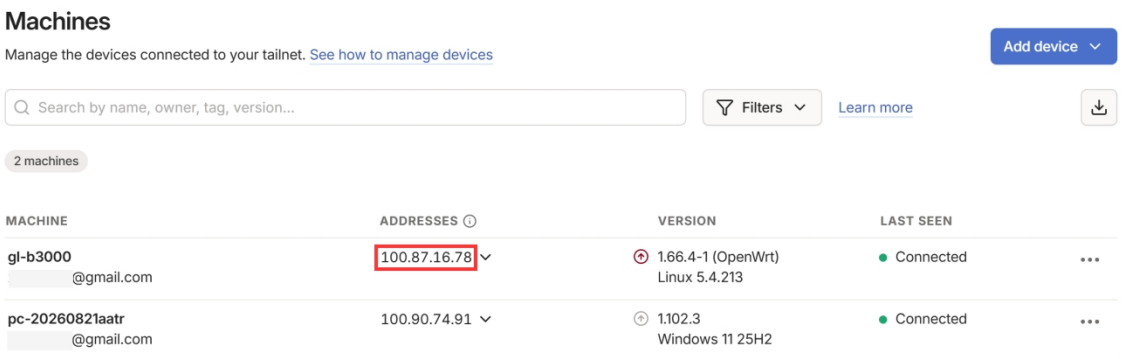
4. En el ventana emergente, haga clic en el enlace e inicie sesión con su cuenta de Tailscale.



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



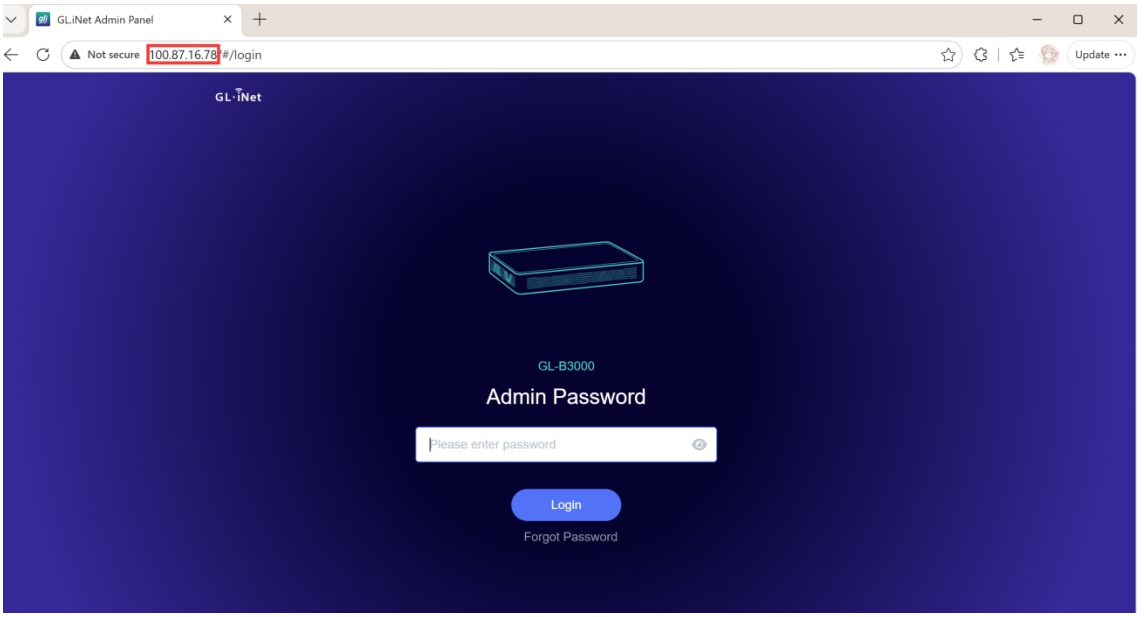
6. Yserá luego será redirigido a Escala trasera consola de administración. Ahora el enrutador se ha agregado a la red virtual de Tailscale y se puede acceder a él de forma remota mediante la IP virtual de Tailscale. **100.87.16.78**.



7. Pruebe la conectividad.

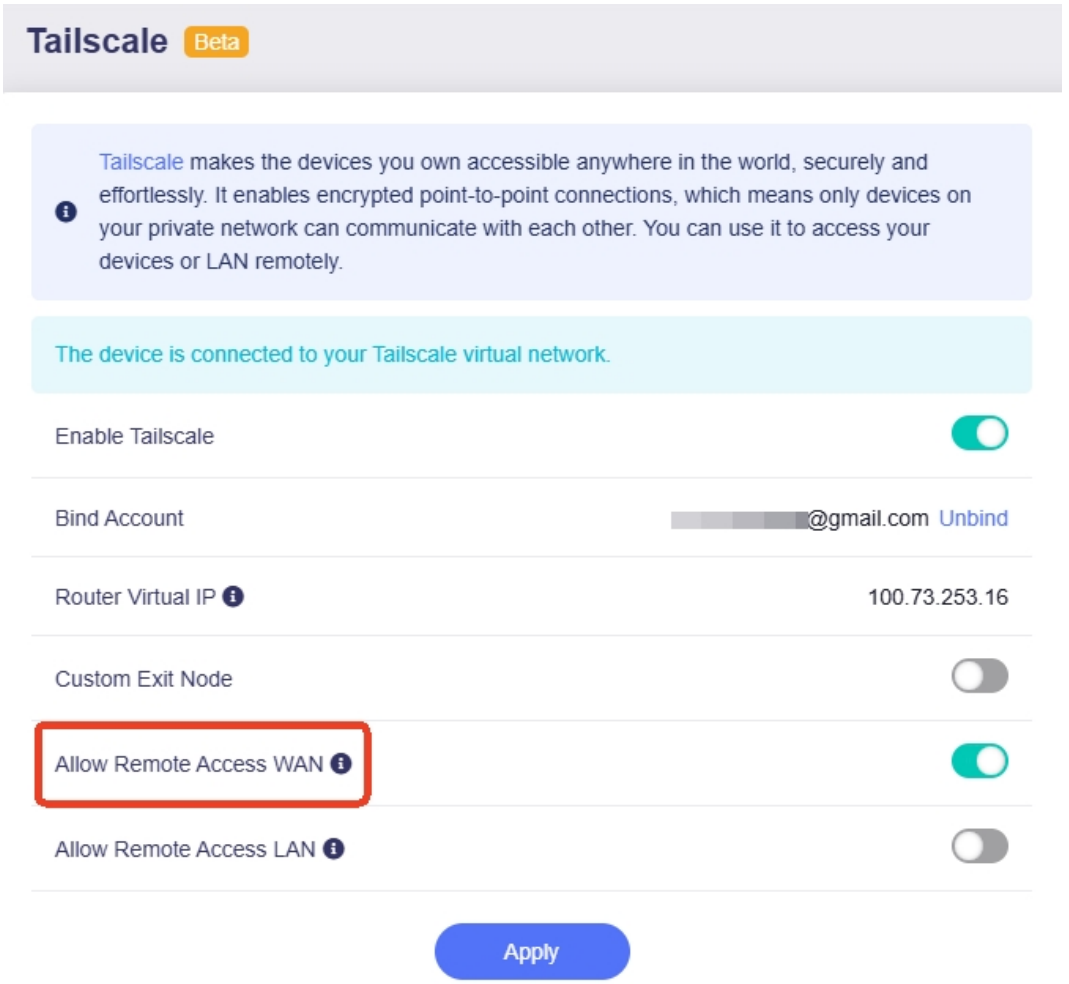
   En otro dispositivo conectado a la misma red de Tailscale, abra un navegador web e ingrese la IP virtual del enrutador en la barra de direcciones. Si puede acceder al panel

de administración web del enrutador, significa que Tailscale está funcionando. También puede utilizar el comando ping o iniciar sesión SSH en el terminal del enrutador'IP virtual en la barra de direcciones. Si puedes acceder al 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.



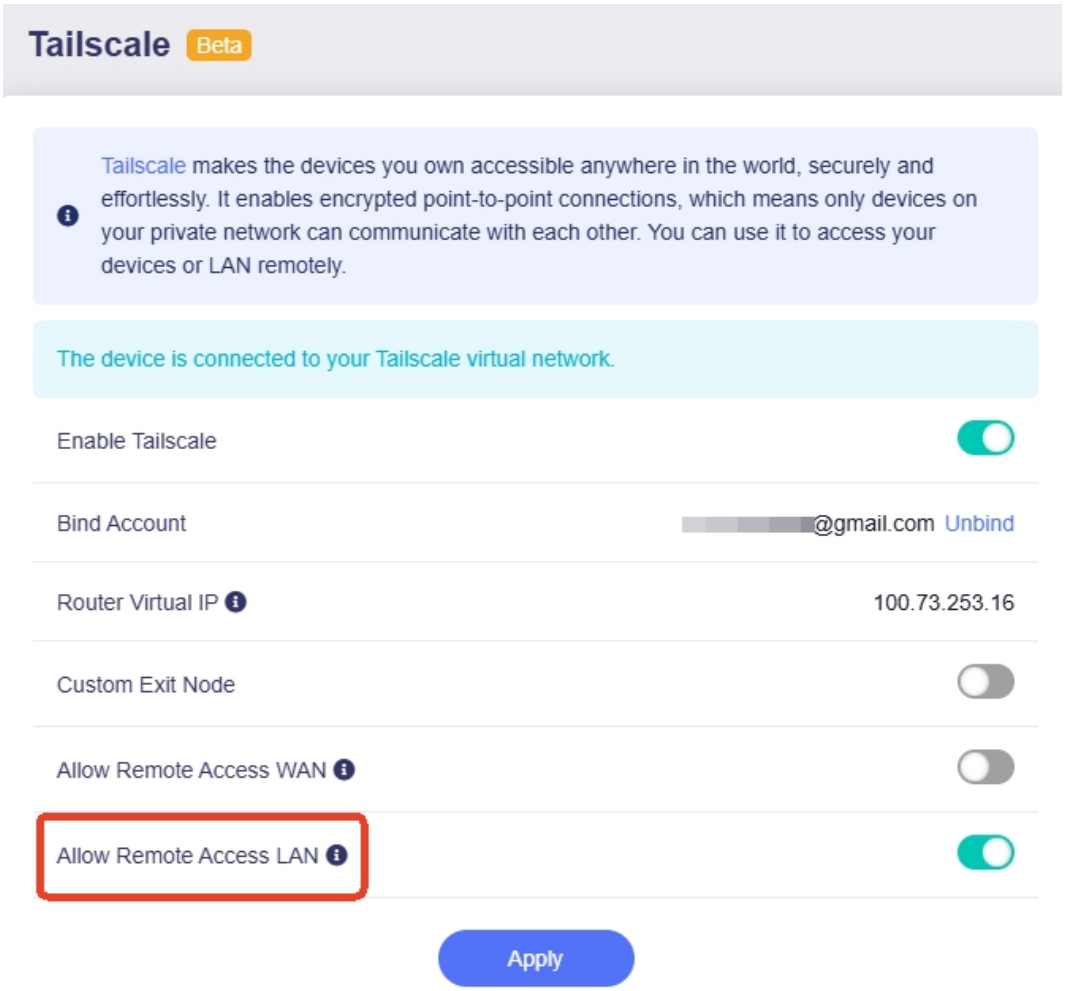
12.7.2 Permitir el acceso remoto a la WAN

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



12.7.3 Permitir el acceso remoto a la LAN

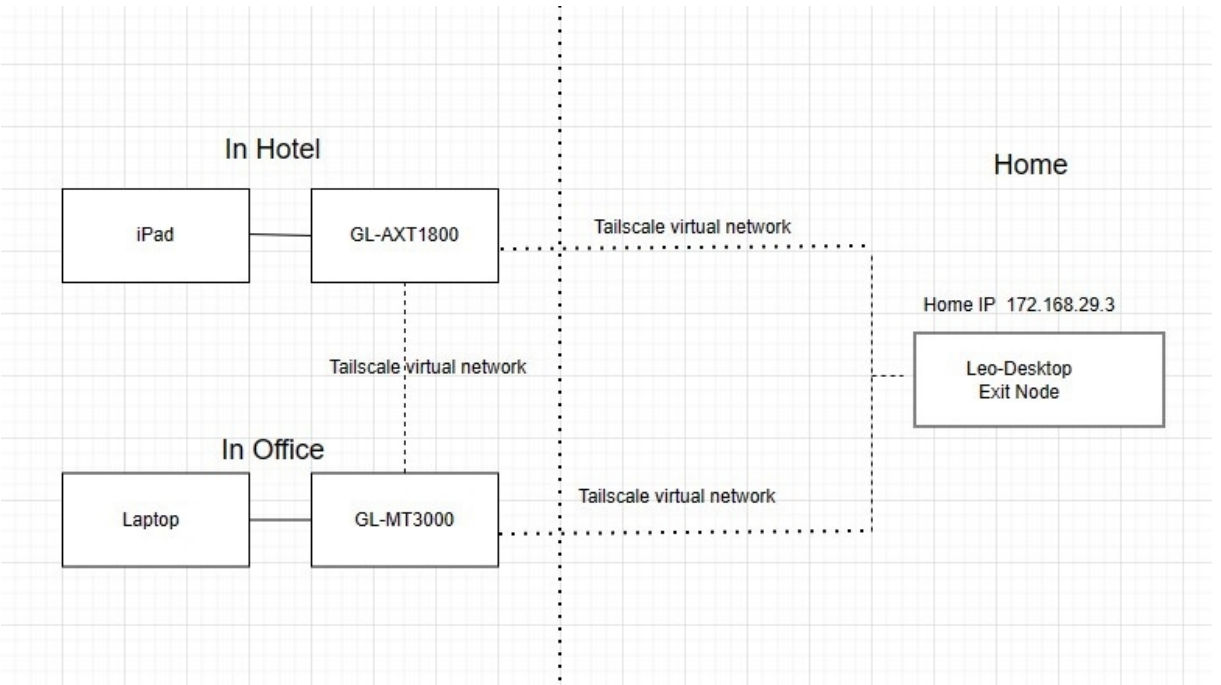
Si esta opción está habilitada, se puede acceder a los recursos en el lado LAN del dispositivo a través de la red virtual Tailscale. Consulte aquí para obtener más detalles.



12.7.4 Nodos de salida personalizados

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

Sin embargo, puede haber ocasiones en las que desee que Tailscale enrute su tráfico de Internet público. 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 "Exit Nodo". Para configurar un nodo de salida personalizado en enrutadores GL.iNet, consulte este tutorial.

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 cuando ejecute 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 y IPv6.

13.1 Cortafuegos

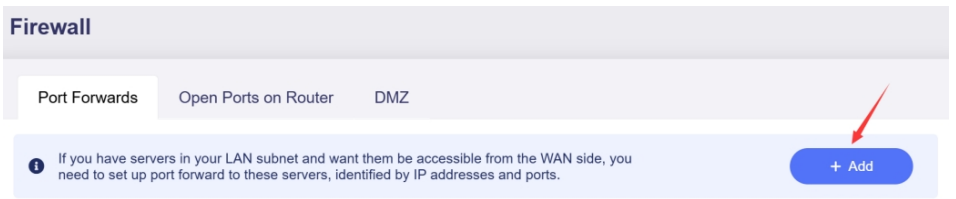
Firewall es una función de red que enruta solicitudes externas a dispositivos específicos en su red local. Cortafuegos la página incluyetres funciones clave: **Reenvío de puertos** (para acceso dirigido a puertos específicos de (para acceso completo directo a un único dispositivo)., **Abrir puertos en el enrutador** (para acceder a servicios que se ejecutan en el enrutador) y **DMZ** (para acceso completo directo a un único dispositivo).

13.1.1 Reenvío de puertos

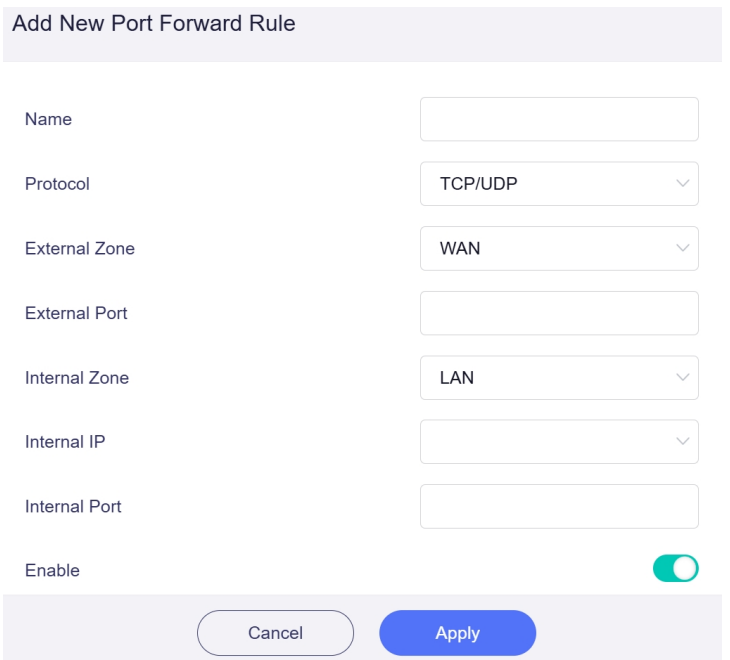
Reenvío de puertos permite que las computadoras remotas conéctese a una computadora o servidor local detrás del firewall de LAN (por ejemplo, servidores web, servidores FTP).

Si necesitaconfigurar el puerto de reenvíos, siga los pasos a continuación.

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



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

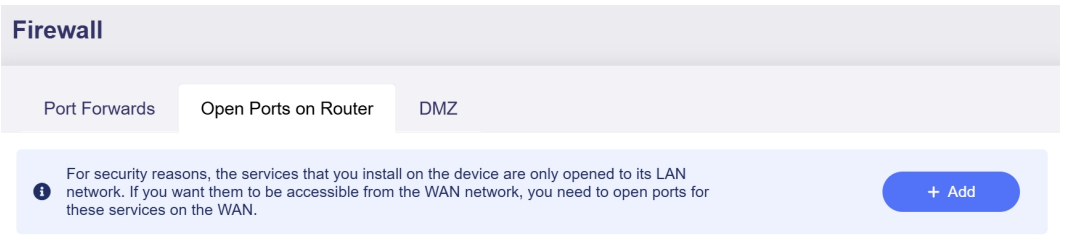


- **Nombre**: El nombre de la regla que puede especificar el usuario.
- **Protocolo**: El protocolo utilizado. Puede elegir TCP, UDP o TCP y UDP.
- **Zona externa**: las opciones disponibles son WAN, Cliente WireGuard, Servidor WireGuard, Cliente OpenVPN, Servidor OpenVPN, LAN e Invitado.
- **Puerto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

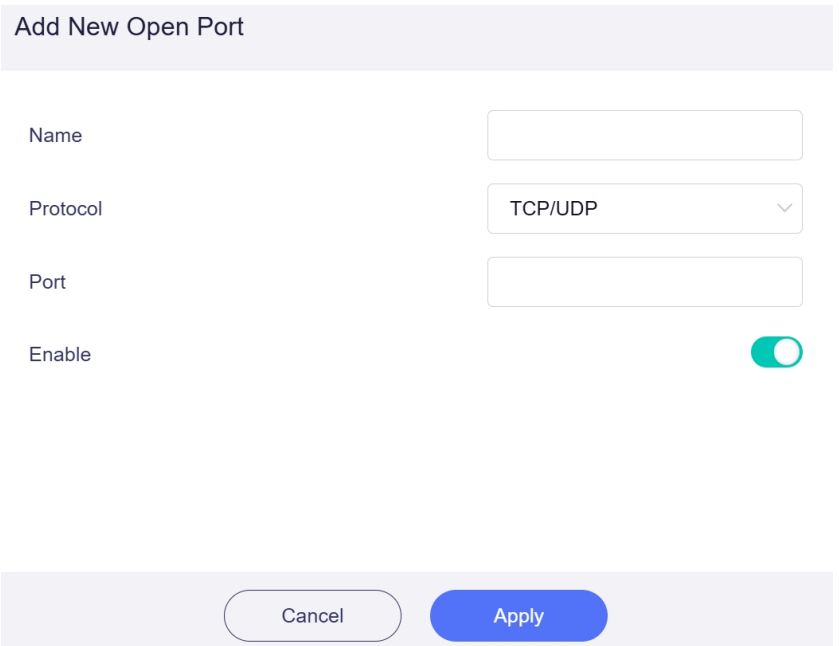
13.1.2 Abrir puertos en el enrutador

Los servicios del enrutador, como web y FTP, requieren que sus respectivos puertos estén abiertos en el enrutador para que sean accesibles públicamente.

Para abrir un puerto, cambie a la pestaña Abrir puertos en el enrutador y luego haga clic en Agregar.



En en la ventana emergente, abra un nuevo puerto y haga clic en Aplicar.



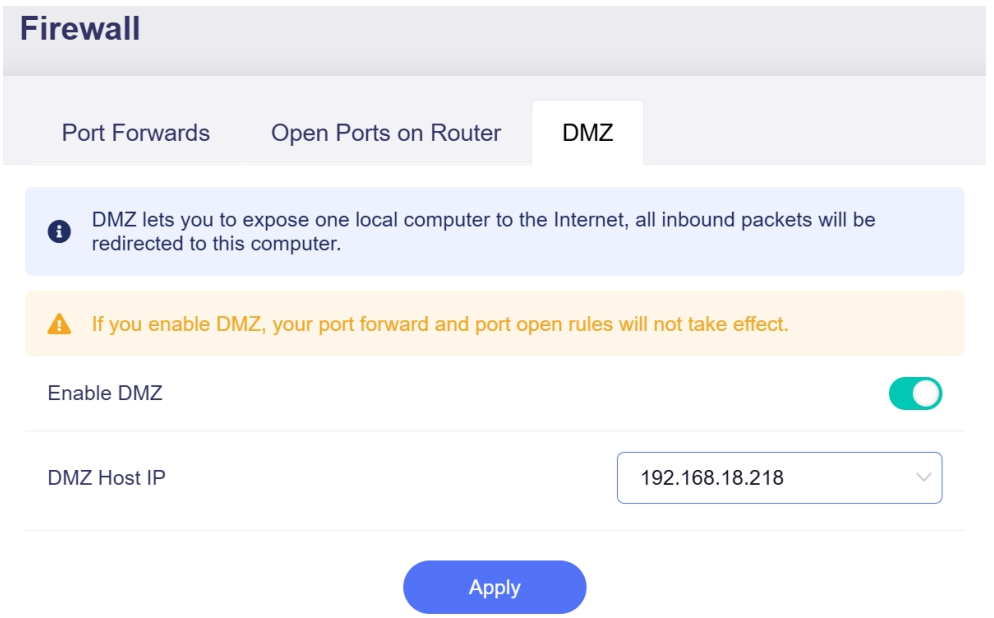
- **Nombre**: el nombre de la regla que puede especificar el usuario.
- **Protocolo**: El protocolo utilizado, puede elegir TCP, UDP o TCP y UDP.
- **Puerto**: El número de puerto que desea abrir.

13.1.3 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 si es necesario.

1. Inicie sesión en el panel de administración web de su enrutador' y navegue hasta **RED** > **Cortafuegos** > **DMZ** sección.
2. Tactiva **Habilitar DMZ**, luego seleccione lae **IP del host DMZ** de la lista desplegable. El dispositivo seleccionado recibe todos los paquetes entrantes. Haga clic en **Aplicar** para guardar la configuración.



13.2 Multi-WAN

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

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

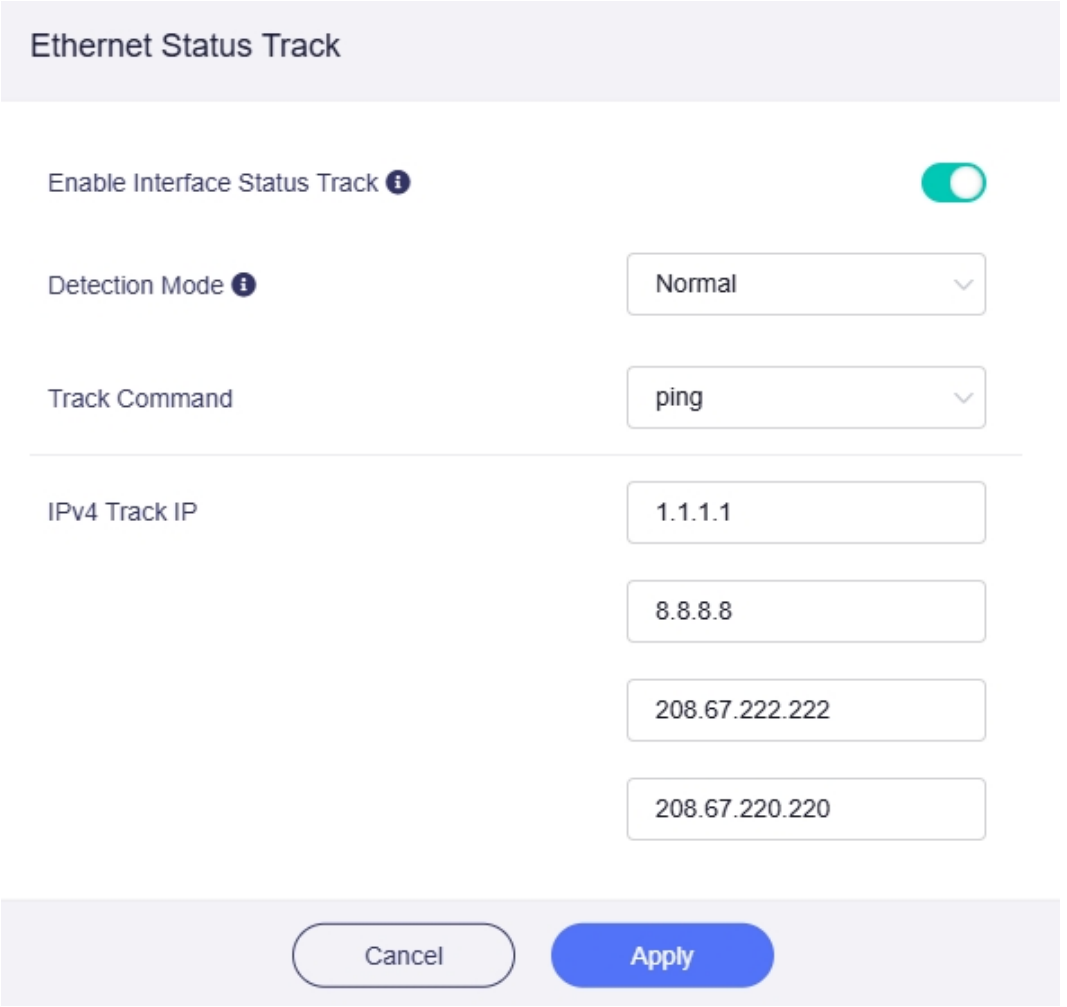
Inicie sesión en el panel de administración web de su enrutador' y navegue hasta **RED** > **Multi-WAN**. Esta página incluye dos secciones: Seguimiento del estado de la interfaz y modo Multi-WAN.

13.2.1 Seguimiento del estado de la interfaz

Los enrutadores GL.iNet utilizan **ping** comando 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.



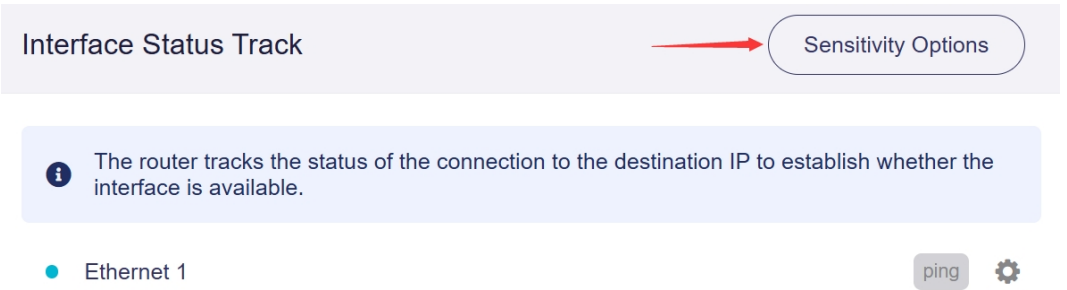
En la sección **Seguimiento del estado de la interfaz**, haga clic en el ícono de ajustes a la derecha para acceder a la configuración de seguimiento del estado para cada interfaz de red. A continuación se muestran las configuraciones de seguimiento de estado para la interfaz Ethernet. La misma lógica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



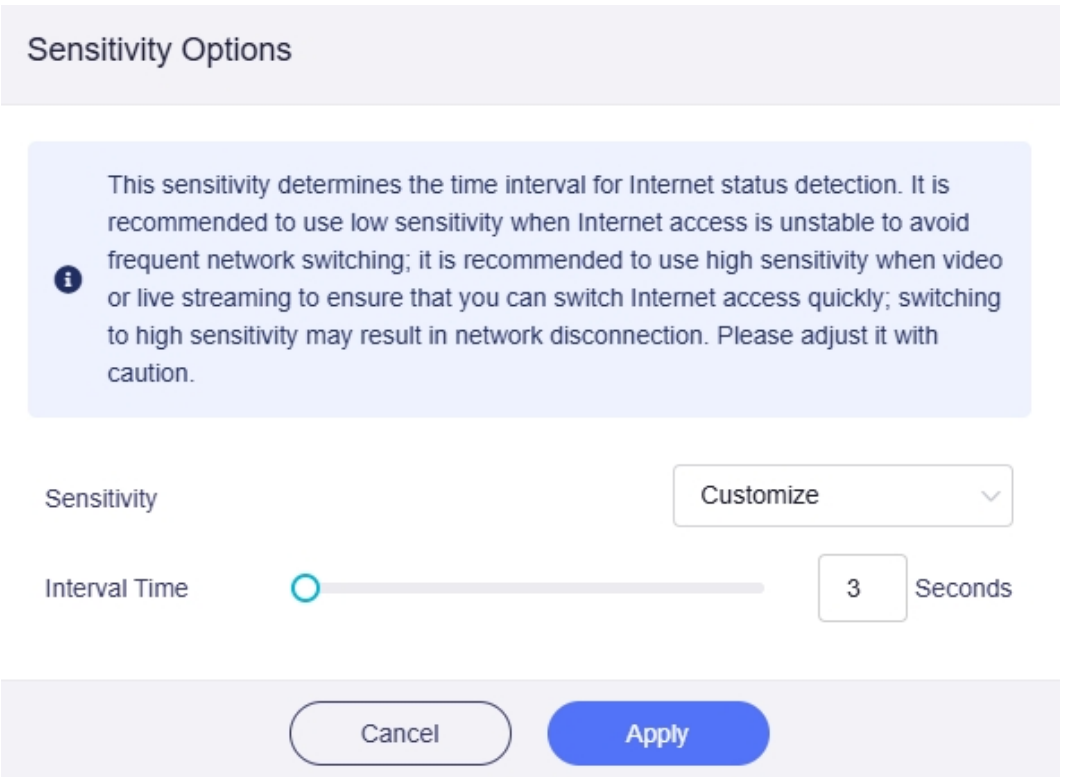
- **Habilitar seguimiento del estado de la interfaz**: Está habilitadode forma predeterminada. Si está deshabilitado, el enrutador determinará el estado de la interfaz según las condiciones (por ejemplo, si el cable Ethernet está enchufado).
- **Modo de detección**: esta característica se introdujo como baja Modo de datos en firmware v4.5, luego renombrado Modo de detección en firmware v4.7. Hay tres modos disponibles: Modo normal, Modo de datos bajos y Modo estricto.
  - **Normal**: Se utilizade forma predeterminada.
  - **Datos bajos**: 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**: determina la interfaz estado basado exclusivamente en los resultados de un comando de detección enviado a una IP pública.

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

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



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



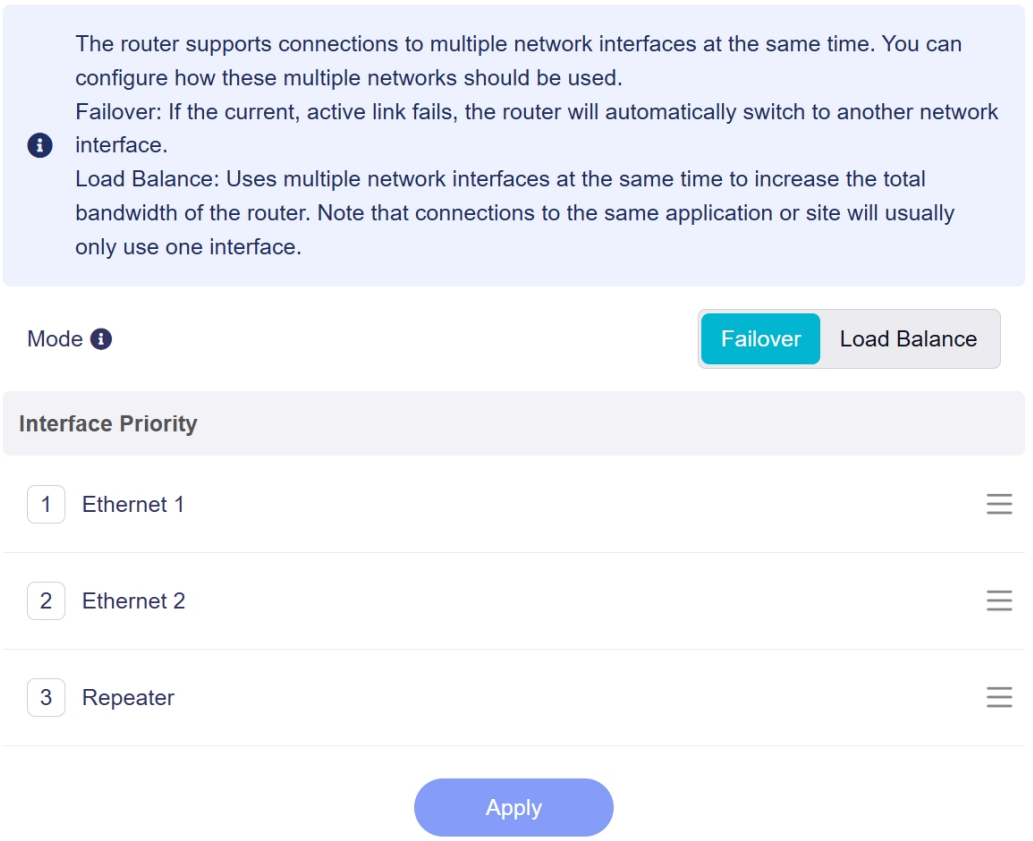
13.2.2 Modo Multi-WAN

Tdos modos están 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 a ella.

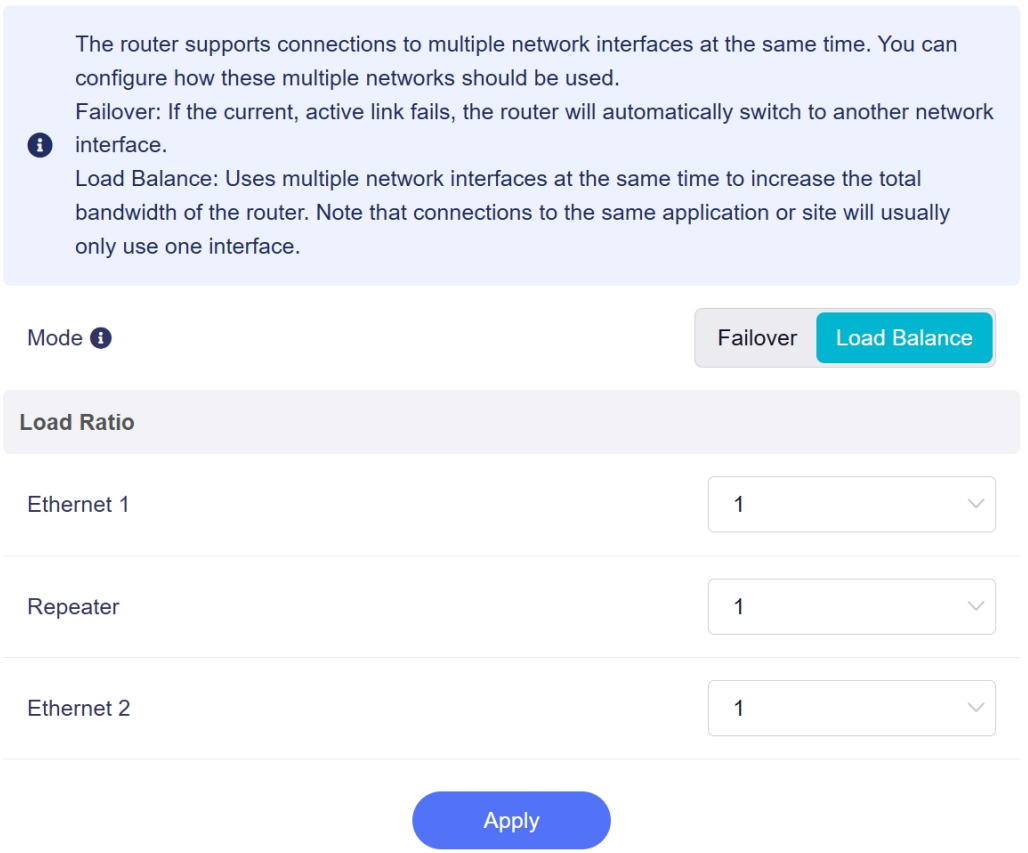


Equilibrio de carga

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

La relación de carga se refiere a la proporción entre cada interfaz de red. El sistema asignará interfaces para manejar nuevas conexiones según esta proporción configurada.

Por ejemplo, si el enrutador está conectado a tres redes (por ejemplo, Ethernet 1, Repetidor, y Ethernet 2) simultáneamente y todas las interfaces están disponibles para acceso a Internet, habilitar el equilibrio de carga y establecer una relación 1:1:1 significa que tres interfaces compartirán el ancho de banda de la red por igual. El sistema distribuirá nuevas conexiones a través de estas interfaces de acuerdo con la relación de carga 1:1:1 configurada.



También puede personalizar la relación de carga si es necesario. Por ejemplo, si Ethernet 1 tiene un ancho de banda de 100 Mbps, Repetidor tiene 200 Mbps y no hay otras conexiones

activas, configure la carga las proporciones son 1 para Ethernet 1, 2 para Repetidor r y 0 para Ethernet 2. Luego, el sistema distribuirá nuevas conexiones a través de estas interfaces de acuerdo con la proporción 1:2 configurada, lo que significa que Ethernet 1 manejará la mitad de conexiones que el Repetidor. A diferencia del modo de conmutación por error, este modo optimiza la eficiencia del rendimiento general al equilibrar la carga de tráfico en todas las interfaces disponibles.

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

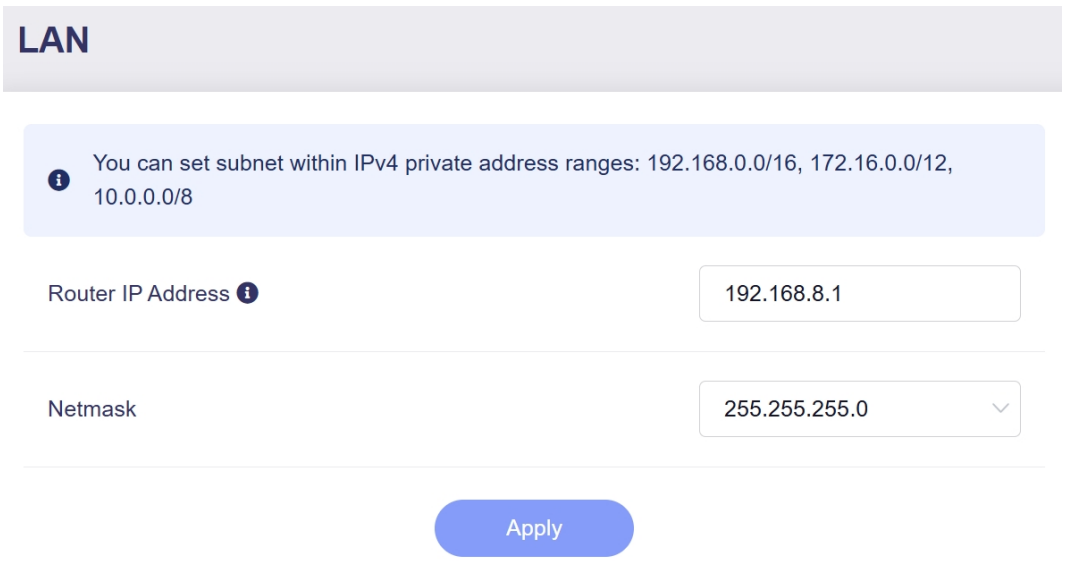
13.3 LAN

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

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

13.3.1 Configuración básica

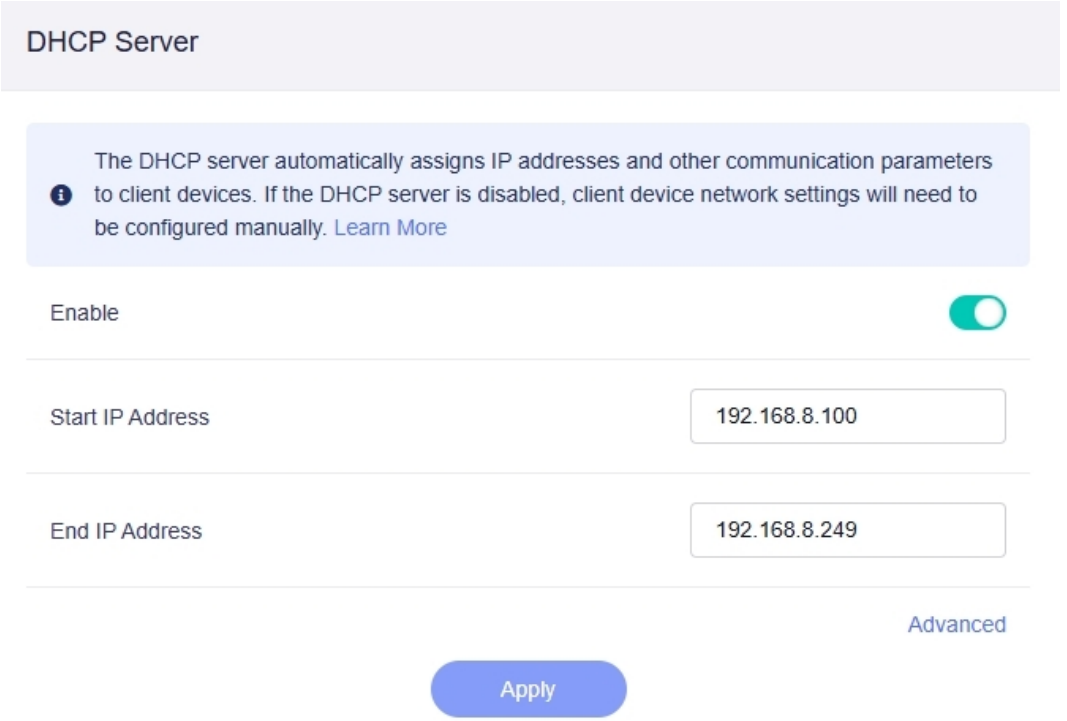
Los ajustes básicos incluyen la dirección IP del enrutador y Máscara de red. Puede configurar la subred dentro de los rangos de direcciones privadas IPv4: 192.168.0.0/16, 172.16.0.0/12, 10.0.0.0/8



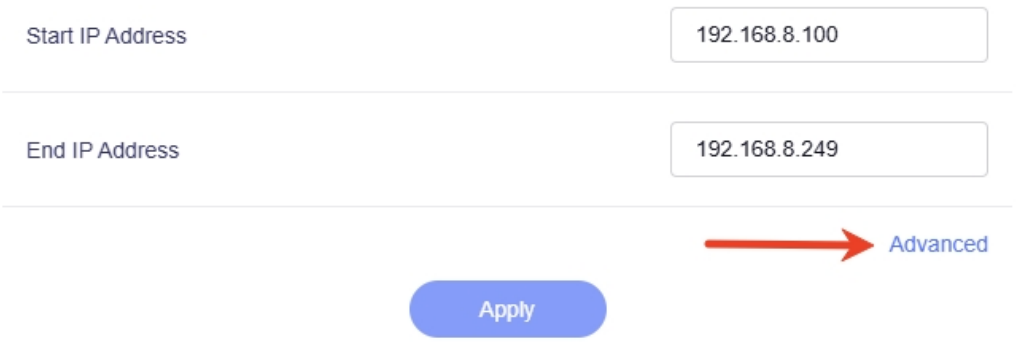
- **Dirección IP del enrutador**: esta es la dirección ingresada en la barra de direcciones del navegador para acceder al panel de administración del enrutador'. Es 192.168.8.1 de forma predeterminada y se puede cambiar si entra en conflicto con la red ascendente.
- **Máscara de red**: Hay dos opciones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

13.3.2 Servidor DHCP

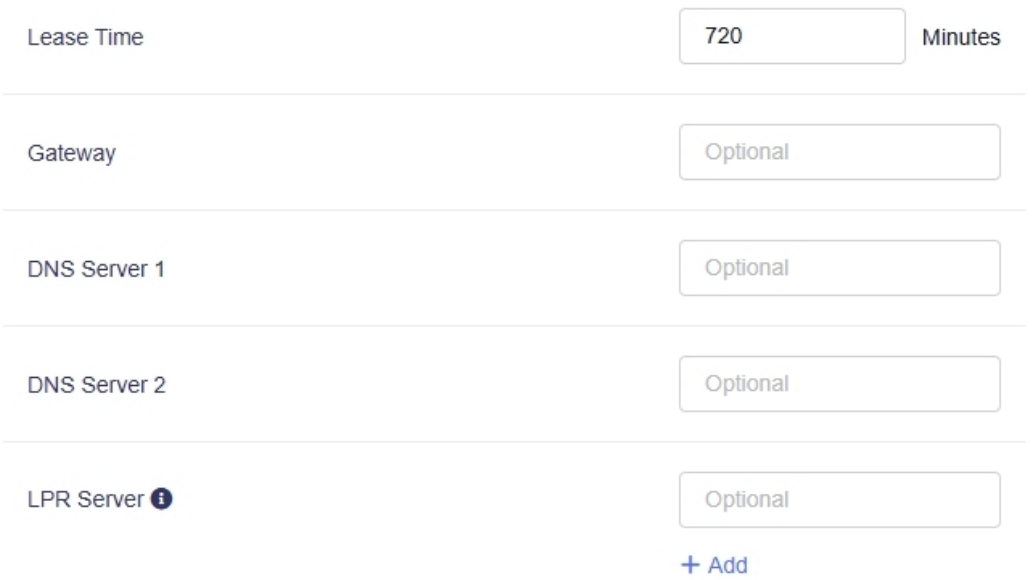
El servidor DHCP asigna automáticamente direcciones IP y otros parámetros de comunicación a cada conectado cliente. El servidor DHCP del enrutador GL.iNet está habilitado de forma predeterminada y el grupo de direcciones IP del servidor DHCP varía de 192.168.8.100 a 192.168.8.249. Puede personalizar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



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



Podrá configurar ajustes avanzados, incluidos el tiempo de concesión, la puerta de enlace y el DNS. Servidor(es), y servidor LPR.



- **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 la red local y las redes externas (por ejemplo, Internet).
- **Servidor DNS 1**: el servidor principal responsable de traducir los nombres de dominio a direcciones IP.
- **Servidor DNS 2**: un servidor de respaldo utilizado para resolver nombres de dominio si el servidor DNS primario falla.
- **Servidor LPR**: (Servidor remoto de impresora de línea) Un servicio que administra trabajos de impresión y permite que los dispositivos en red envíen solicitudes de impresión a impresoras remotas. Se pueden configurar múltiples puertos LPR para impresoras.

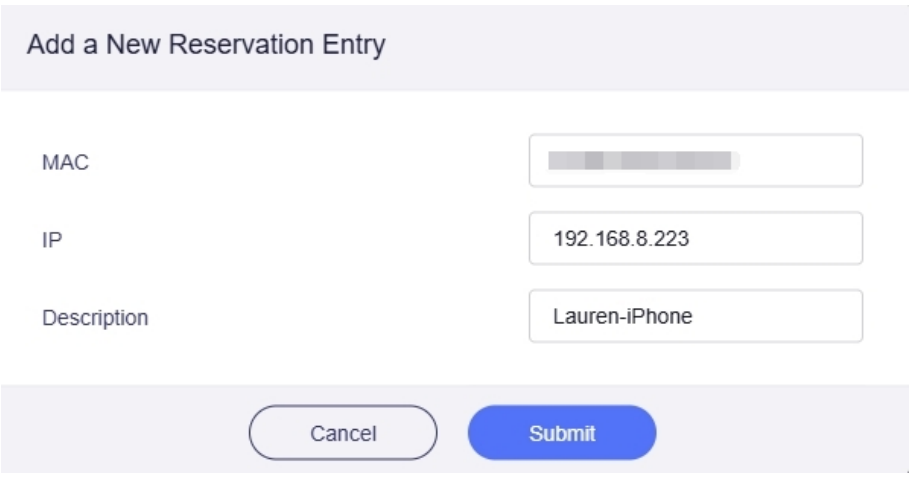
Nota: Si el servidor DHCP está deshabilitado, debe configurar la IP estática y otros parámetros de comunicación manualmente para cada cliente. Consulte aquí para obtener más detalles.

13.3.3 Reserva de direcciones

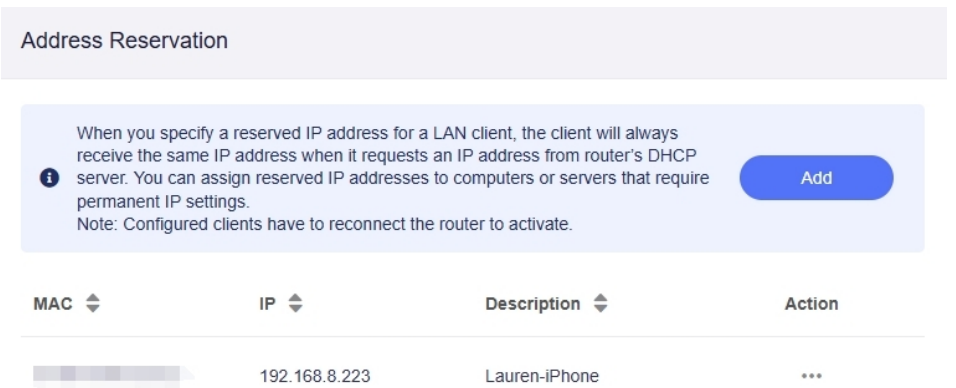
La reserva de dirección le permite especificar una dirección IP fija para un cliente LAN, de modo que el cliente siempre reciba la misma dirección IP cada vez que acceda al servidor DHCP del enrutador. Puede asignar direcciones IP reservadas a computadoras o servidores que requieren una configuración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

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



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



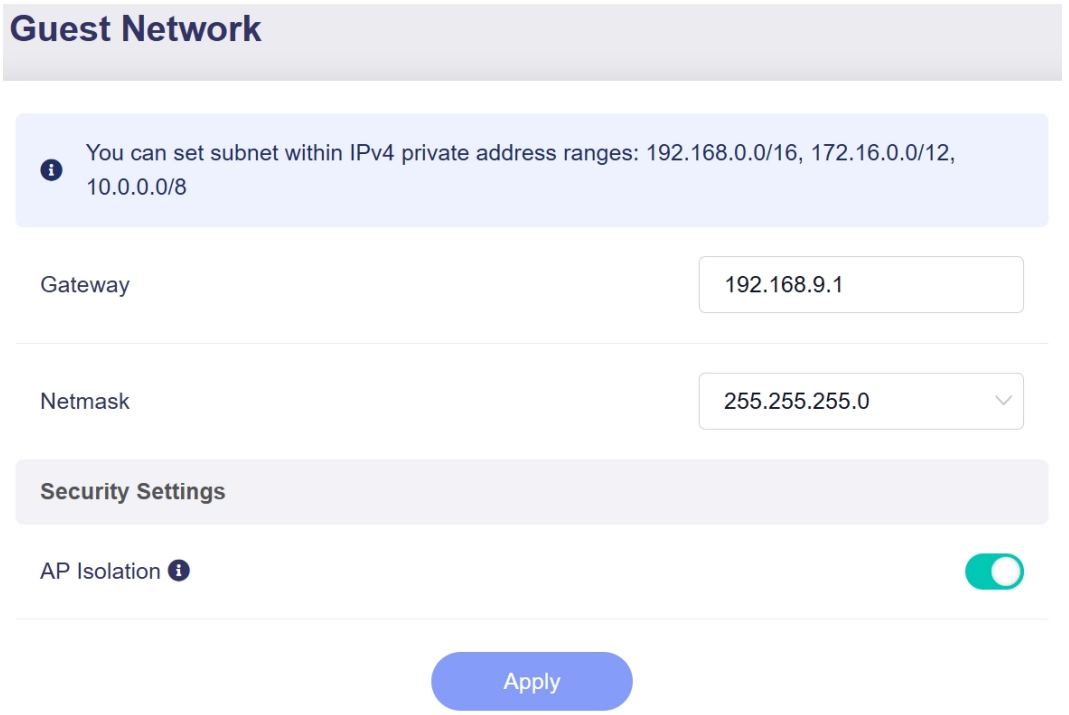
13.4 Red de invitados

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

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

13.4.1 Configuración básica

Las configuraciones básicas incluyen Puerta de enlace, máscara de red, y Aislamiento de AP.

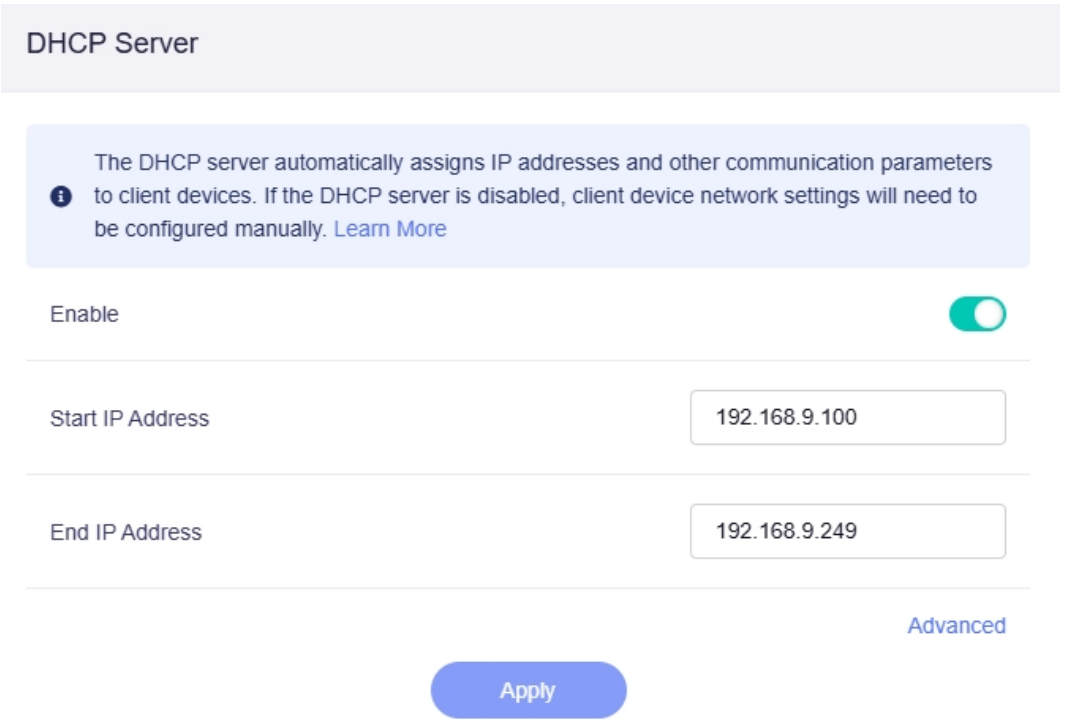


- **Puerta de enlace**: Es 192.168.9.1 de forma predeterminada y se puede cambiar si es necesario, pero no debe entrar en conflicto con la puerta de enlace de la red principal.
- **Máscara de red**: Hay dos opciones disponibles: 255.255.255.0 y 255.255.0.0.
- **Aislamiento de AP**: se utiliza para aislar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

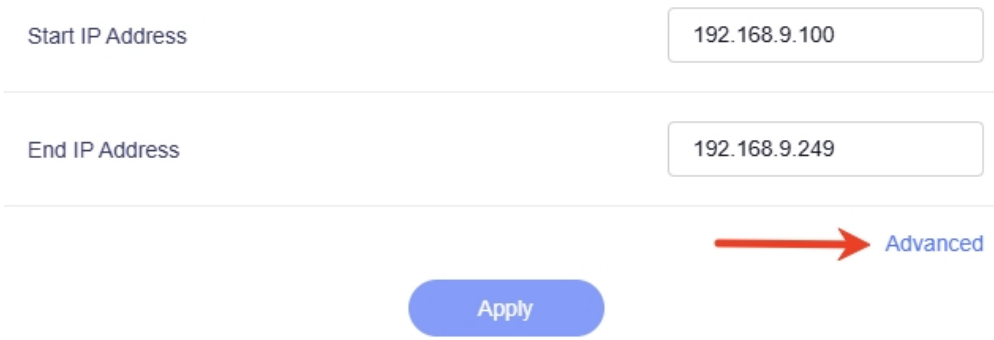
13.4.2 Servidor DHCP

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

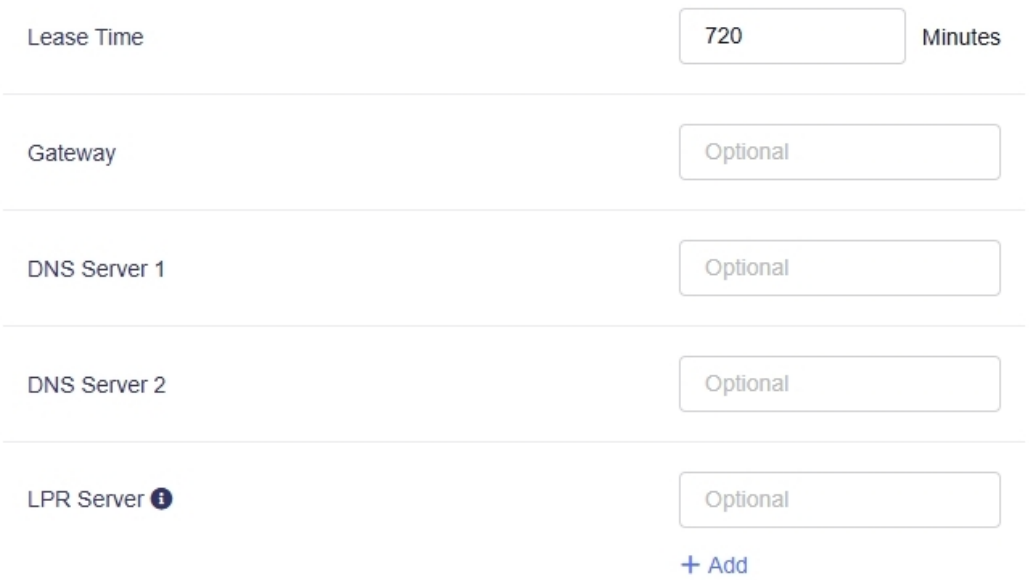
Cuando está habilitado, el servidor DHCP asigna automáticamente direcciones IP y otros parámetros de comunicación a cada cliente conectado. El grupo de direcciones IP del servidor DHCP para la red de invitados oscila entre 192.168.9.100 y 192.168.9.249. Puede personalizar el rango de direcciones si es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



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



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



- **Tiempo de concesión**: la duración durante la cual un dispositivo puede usar una dirección IP asignada a través de el DHCP de la red de invitados.
- **Puerta de enlace**: el componente del enrutador que enruta el tráfico entre el gusuario 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 falla el servidor DNS principal.
- **Servidor LPR**: (Servidor remoto de impresora de línea) Un servicio que administra trabajos de impresión y permite que los dispositivos en red envíen solicitudes de impresión a impresoras remotas. Se pueden configurar varios puertos LPR para impresoras.

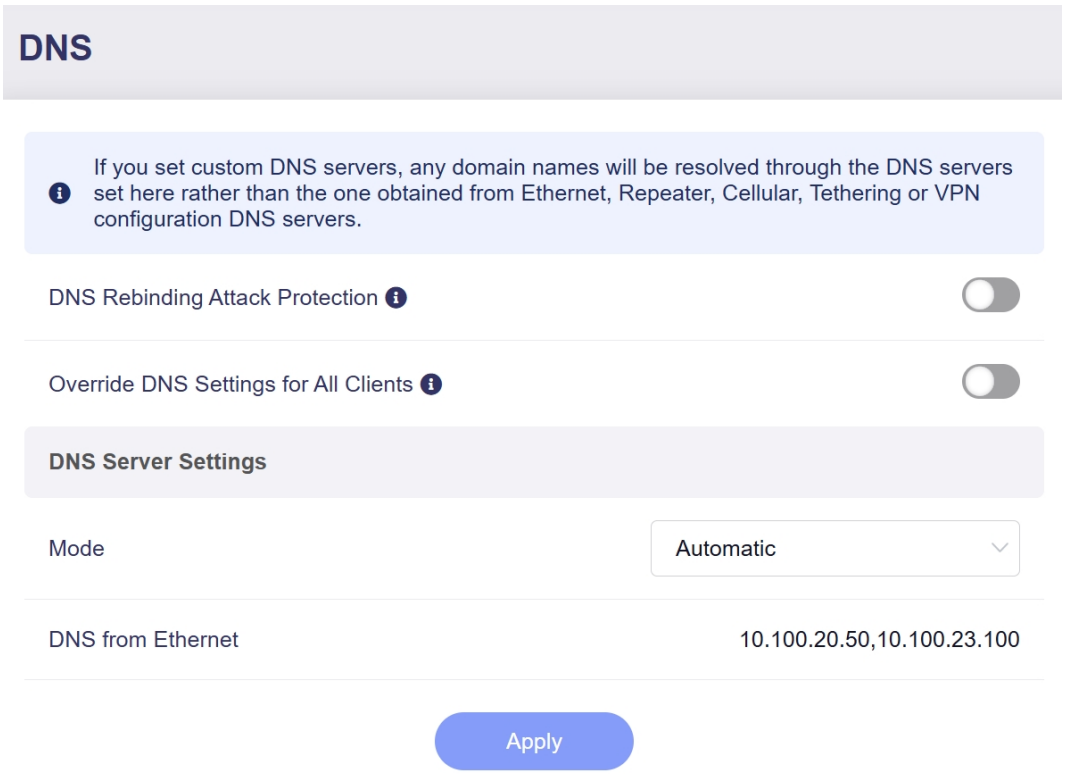
13.5 DNS

DNS (Sistema de nombres de dominio) es un servicio que traduce nombres de dominio legibles por humanos, como www.google.com, en direcciones IP para que los dispositivos puedan localizar y conectarse a sitios web y en línea. servicios.

En un enrutador, la configuración de DNS generalmente determina qué servidores DNS utilizan los dispositivos conectados. En la mayoría de los casos, el enrutador obtiene las direcciones del servidor DNS automáticamente del ISP o de la red ascendente, o permite a los usuarios especificar manualmente servidores DNS públicos, como 8.8.8.8, en la interfaz de administración web. Una vez configuradas, estas configuraciones de DNS generalmente se distribuyen automáticamente a los dispositivos conectados, por lo que no es necesario configurar DNS por separado en cada dispositivo.

Inicie sesión en el panel de administración web de su enrutador y navegue hasta **RED** > **DNS**. Esta página le permite configurar ajustes relacionados con DNS.

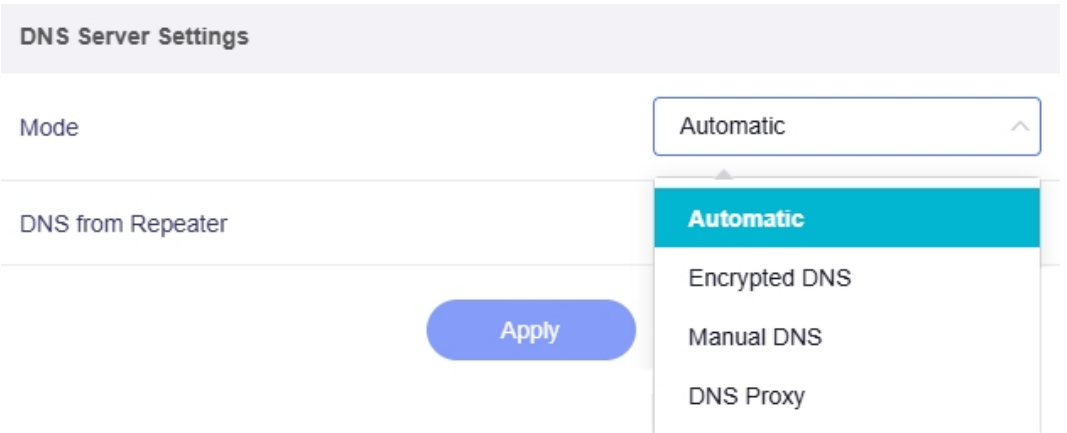
13.5.1 Configuración general



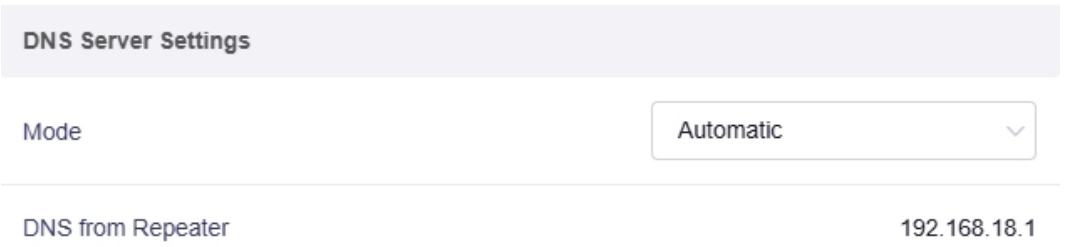
- **DNS Protección contra ataques de rebinding**: protege contra ataques de rebinding de DNS al bloquear intentos maliciosos de resolución de DNS. Tenga en cuenta que habilitarlo puede causar fallas en la búsqueda de DNS privado; deshabilítelo si su red utiliza un portal cautivo (por ejemplo, páginas de inicio de sesión Wi-Fi públicas).
- **Anule la configuración DNS de todos los clientes**: Si está habilitado, todos los conectados dispositivos se verá obligado a utilizar los servidores DNS configurados en el enrutador, ignorando sus propias configuraciones DNS originales. Permite la configuración DNS unificada para todos los dispositivos.

13.5.2 Configuración del servidor DNS

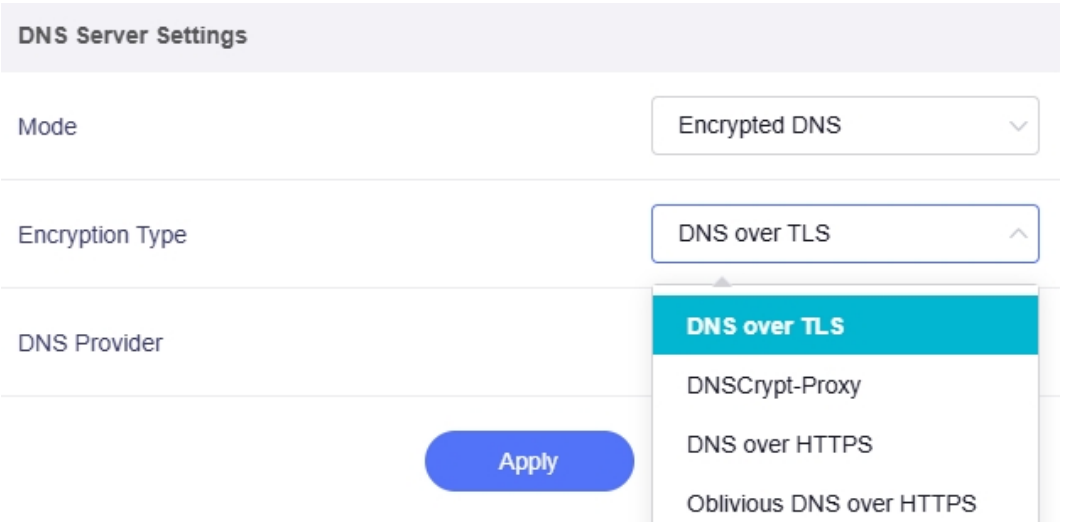
Hay cuatro modos para el servidor DNS: Automático, DNS cifrado, DNS manual y proxy DNS.



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

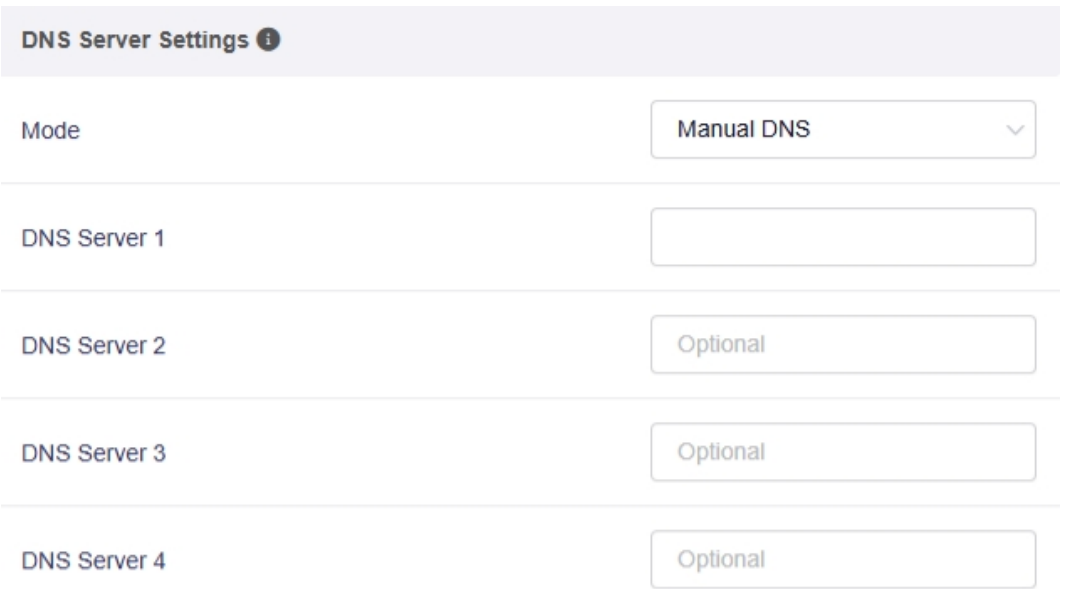


2. **Cifrado DNS**: cuando se selecciona, el enrutador utilizará protocolos cifrados para procesar consultas de DNS, protegiendo los datos de resolución contra escuchas o alteraciones.
   Tiene cuatro tipos de cifrado: DNS sobre TLS, DNSCrypt-Proxy, DNS sobre HTTPS y DNS ajeno a través de HTTPS.



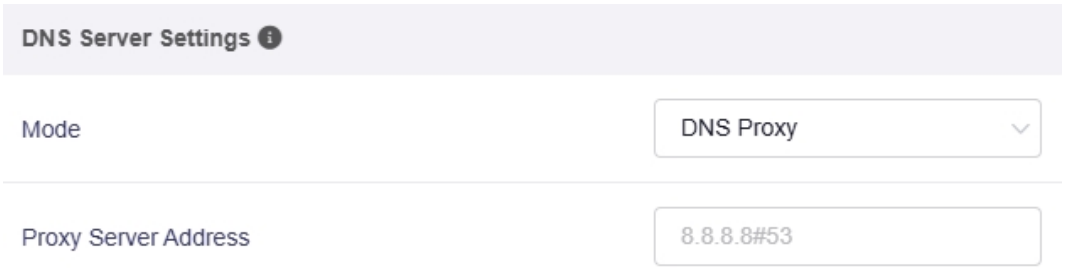
- Para DNS sobre TLS, seleccione un proveedor de DNS entre Control D, NextDNS y Cloudflare.
- Para los otros tres (es decir, DNSCrypt-Proxy, DNS sobre HTTPS y DNS ajeno a través de HTTPS), seleccione al menos un servidor DNS del repositorio. Se pueden seleccionar hasta 8 servidores. Cuando se seleccionan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

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



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

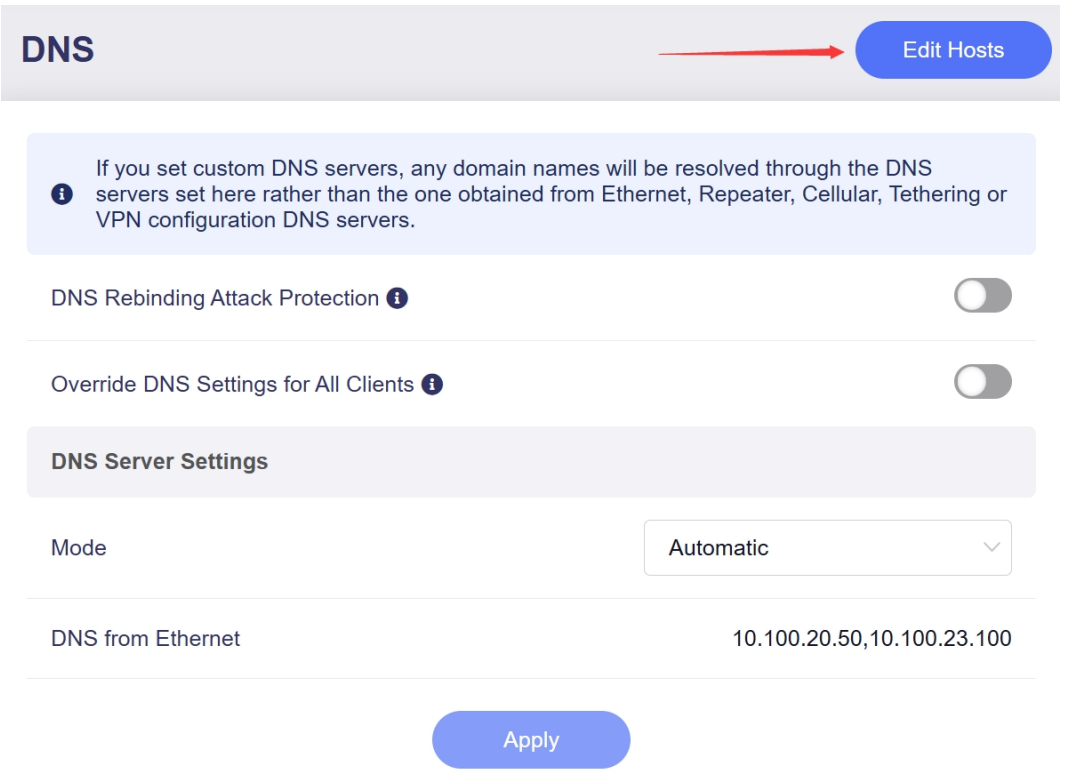
4. **Proxy DNS**: cuando se selecciona, el enrutador reenvía todas las consultas DNS a través de un servidor proxy, permitirresolución a través del entorno de red del proxy para necesidades de acceso específicas.



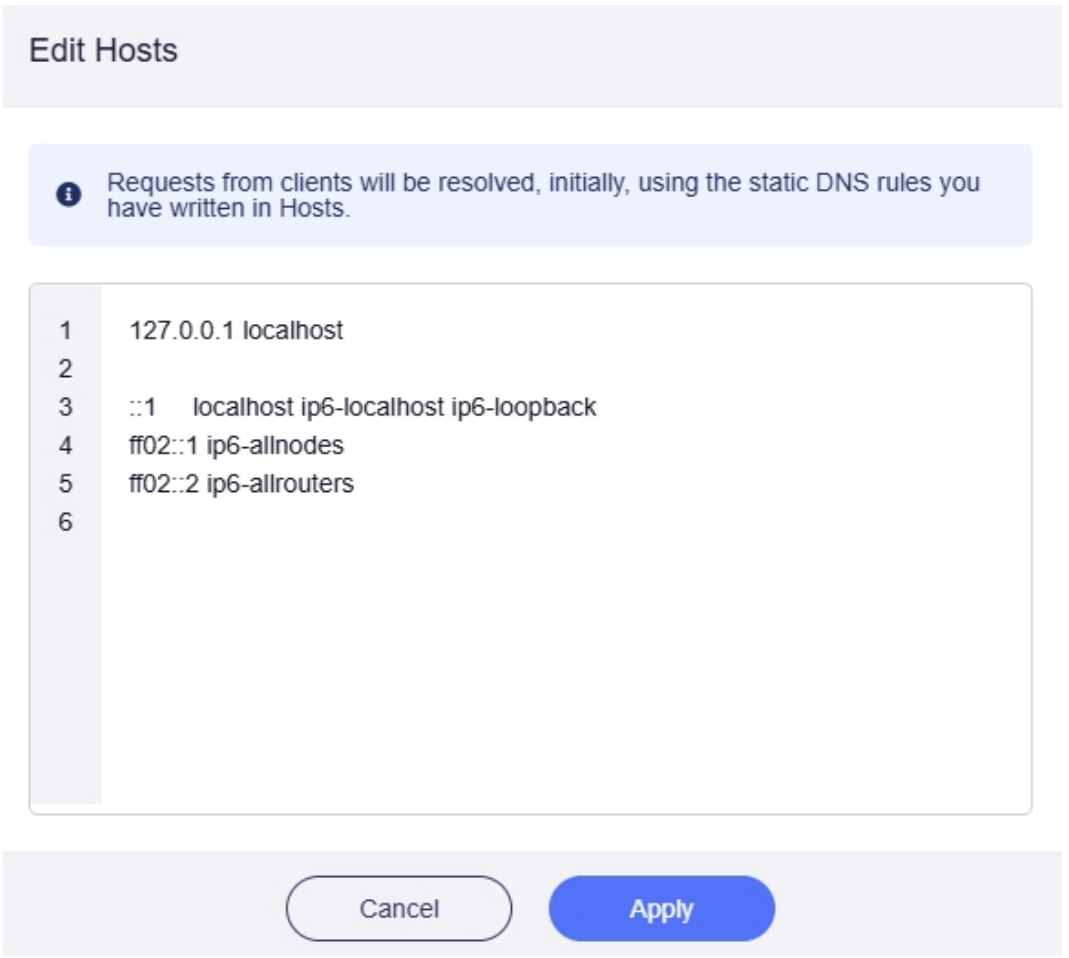
13.5.3 Editar hosts

Puede definir reglas de resolución de DNS estáticas si necesario.

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



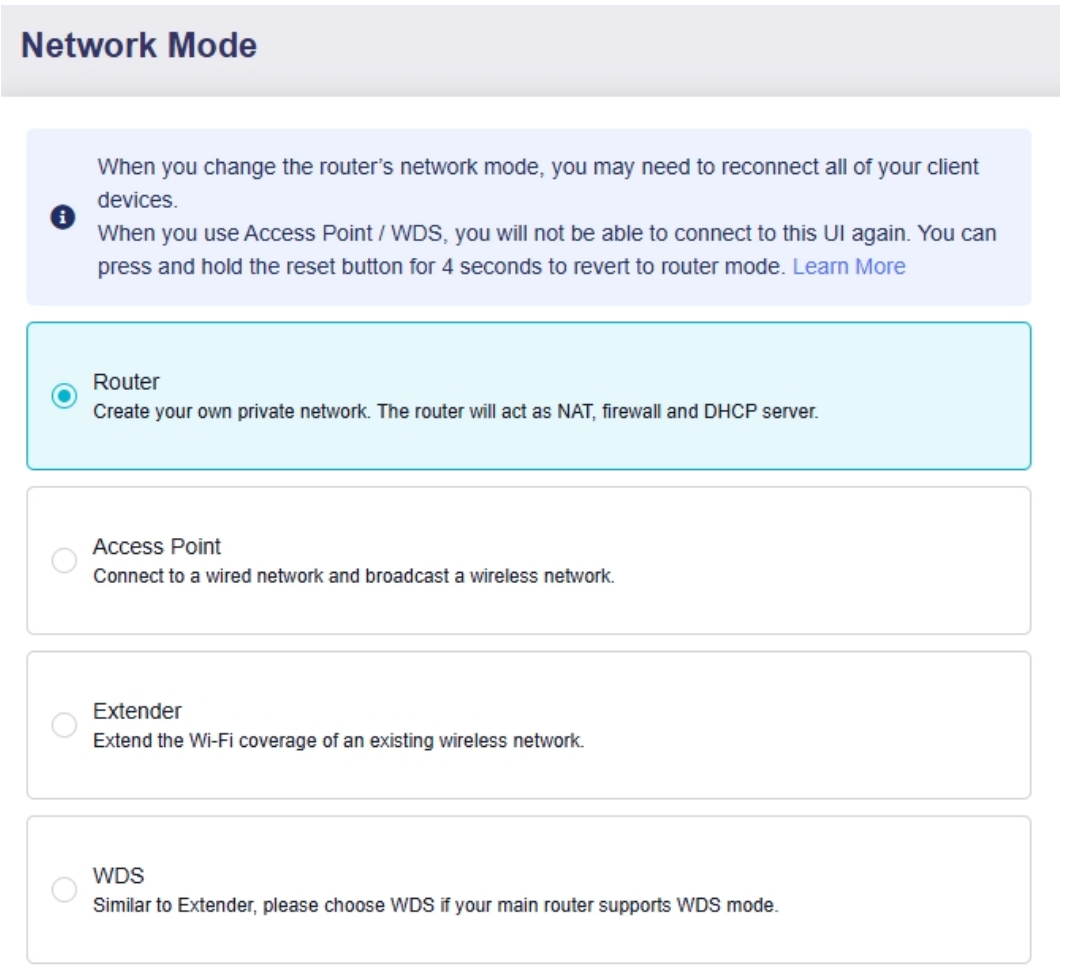
Las solicitudes de los clientes se resolverán preferentemente utilizando el Reglas de DNS estáticas escritas aquí, que le permiten asignar manualmente direcciones IP a nombres de host (por ejemplo, las entradas predeterminadas como 127.0.0.1 localhost para loopback local) para un control personalizado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


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

13.6 Modo de red

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

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



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

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

Nota:

1. Cuando se cambia el modo de red, todos los dispositivos cliente se volverán a conectar al enrutador para una conectividad de red estable.
2. **En modo Punto de acceso/WDS, no podrá 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.

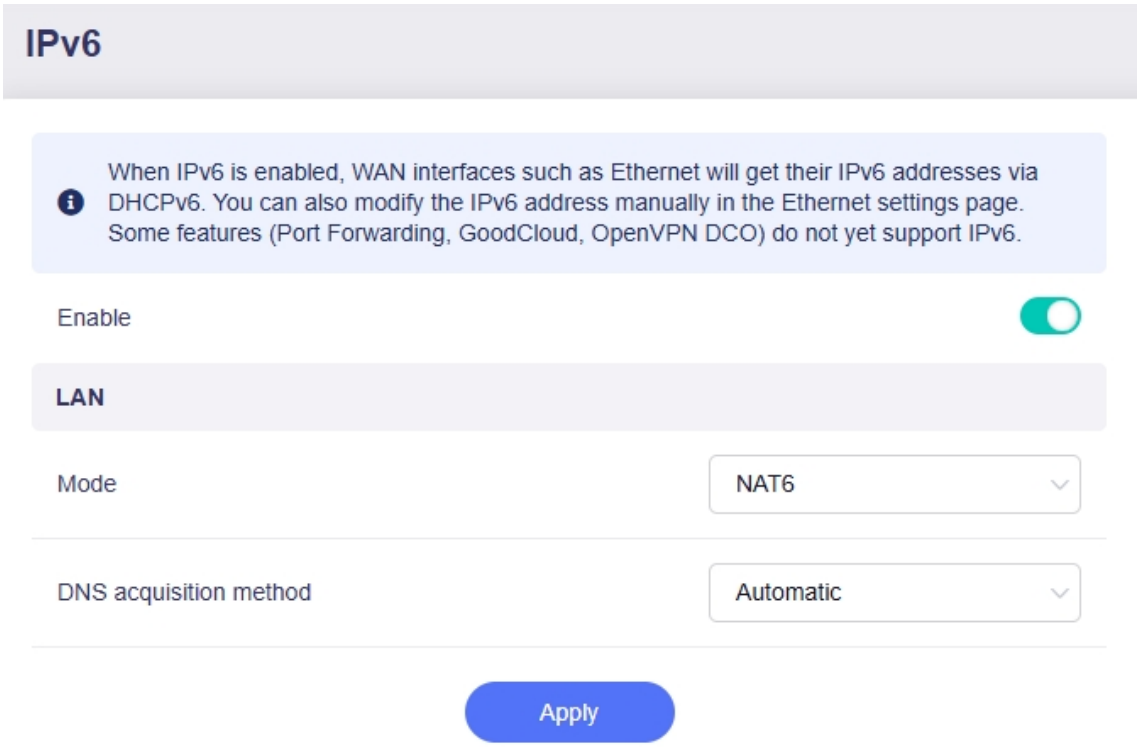
3. **En el modo Punto de acceso/Extensor/WDS, las siguientes funciones no estarán disponibles**: Control de acceso (listas permitidas y listas de bloqueo), VPN, AdGuard Home, Control parental, ZeroTier, Tailscale, Firewall, Multi-WAN, Servidor DHCP, Reserva de direcciones, Red de invitados, DNS, IPv6, Puerta de enlace directa, vigilancia IGMP, 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.

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



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

13.7.1 Modo IPv6

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

- **Nativo**: Este modo se aplica cuando el enrutador obtiene directamente una dirección pública IPv6 , 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.
- **Paso**: 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 Adecuado para escenarios en los que se utiliza un enrutador como puerta de enlace para asignar direcciones IPv6 internas dinámicas a cada dispositivo de 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. adecuado para escenarios en los que se utiliza un enrutador como puerta de enlace para asignar direcciones IPv6 internas dinámicas a cada dispositivo de 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.

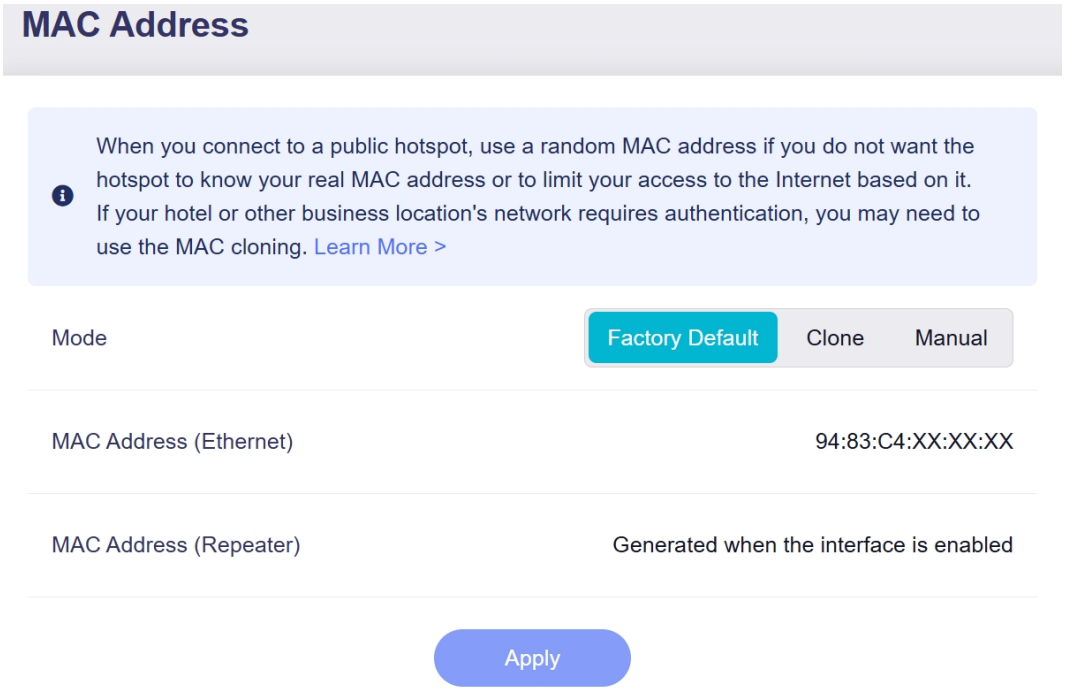
13.7.2 Método de obtención de DNS

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

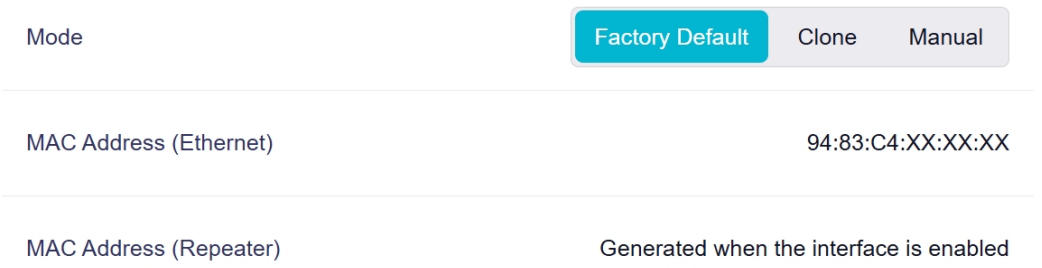
- **Automático**: el enrutador obtendrá direcciones de servidor DNS IPv6 de forma dinámica (por ejemplo, a través de DHCPv6).
- **Manual**: ingrese direcciones de servidor DNS IPv6 personalizadas. Sin embargo, dado que DNS se utiliza para resolver nombres de dominio en sus direcciones IP correspondientes,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

13.8 Dirección MAC

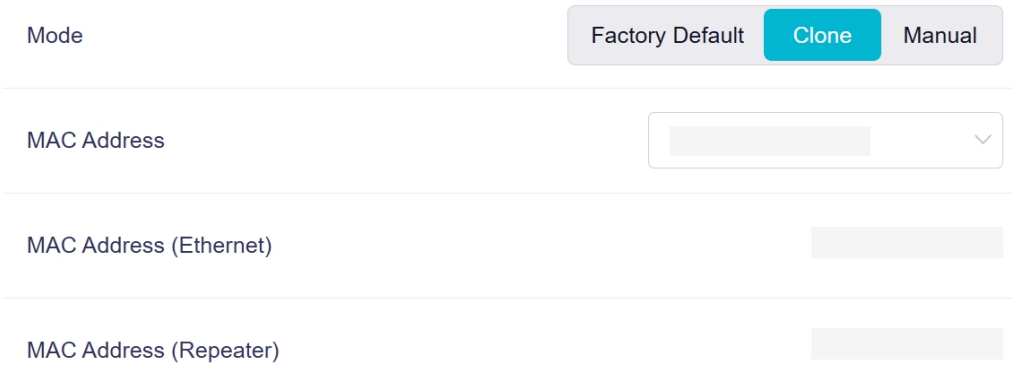
La Dirección MAC página mostrars la dirección MAC predeterminada del enrutador, clonar la dirección MAC de un cliente, ingresar una dirección MAC manualmente o generar una dirección MAC aleatoria. Si el dispositivo admite la configuración de varios puertos Ethernet para usarlos como puertos WAN, puede configurar la dirección MAC para cada puerto por separado. Tenga en cuenta que la configuración de la dirección MAC solo es válida cuando el puerto Ethernet se utiliza como puerto WAN.



- **La dirección MAC predeterminada de fábrica.**

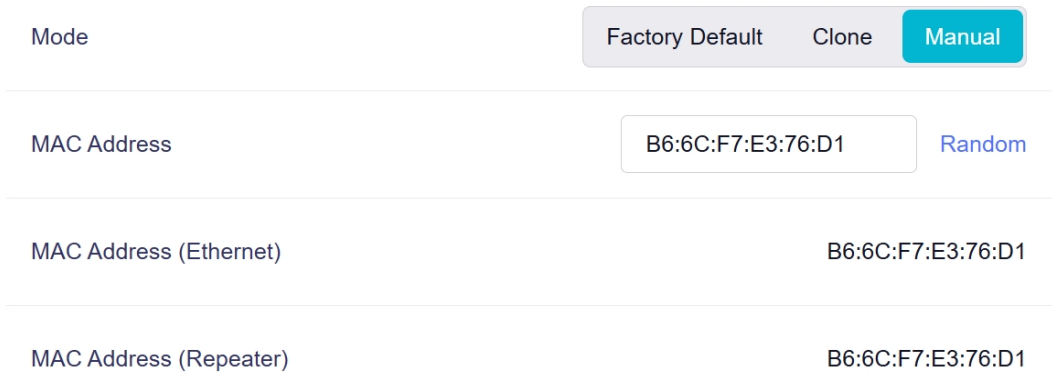


- **Clonar la dirección MAC de un cliente.**



Nota: Muchos dispositivos nuevos ahora usan una dirección MAC aleatoria diferente para conectarse a diferentes Wi-Fi, por lo que la dirección MAC que se muestra aquí puede no ser la dirección MAC real del dispositivo del usuario. La MAC aleatoria también puede denominarse dirección Wi-Fi privada o dirección de hardware aleatoria en diferentes dispositivos.

- **Ingrese manualmente o genere una dirección MAC aleatoria.**

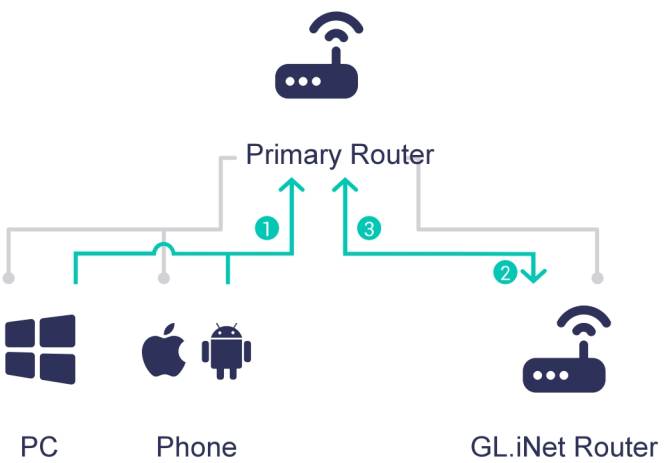


13.9 Puerta de enlace directa

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

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

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

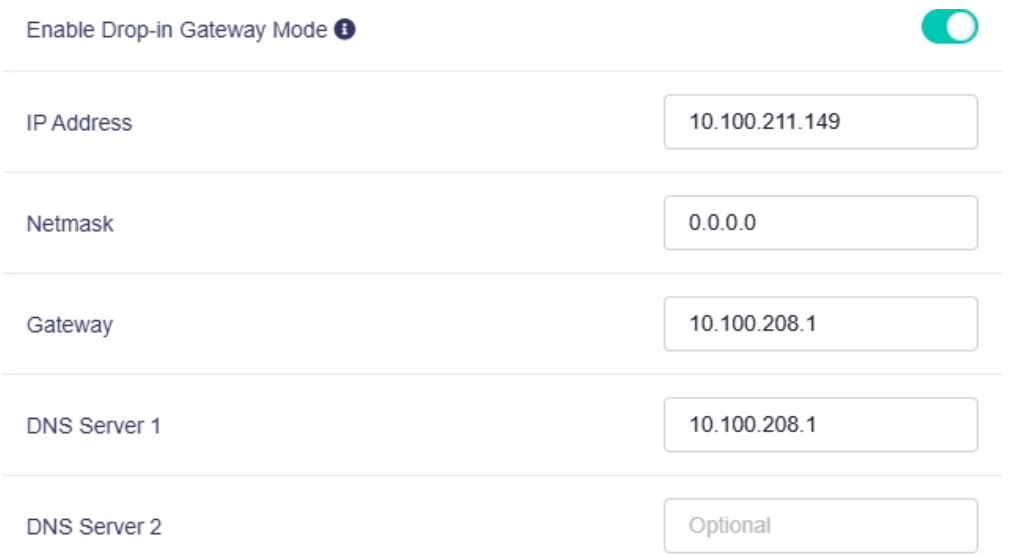


El diagrama anterior consta de dos tipos de líneas: líneas grises y líneas verdes marcadas con tres flechas, cada una etiquetada con su correspondiente número.

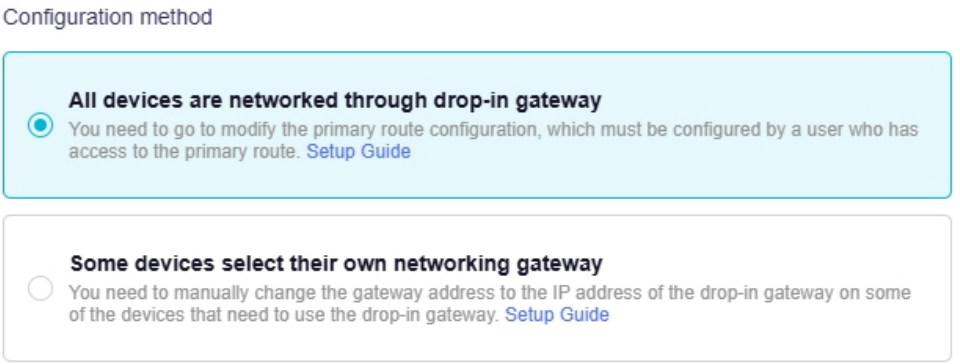
- **Gray lines** ilustran la conexión física Topología: dispositivos cliente (por ejemplo, computadora, computadora portátil) se conectan al enrutador principal, y el puerto LAN del enrutador principal se vincula al puerto WAN del enrutador GL.iNet (con Drop-in Gateway habilitado) a través de un Cable Ethernet.
- **Glíneas verdes** representan la ruta de transmisión de datos secuencial cuando Drop-in Gateway está activo, con las flechas numeradas indicando el flujo de tráfico orden:
  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 del procesamiento, el tráfico se envía de regreso al enrutador principal, que luego entrega los datos finales a los dispositivos cliente originales o los enruta a Internet.

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

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



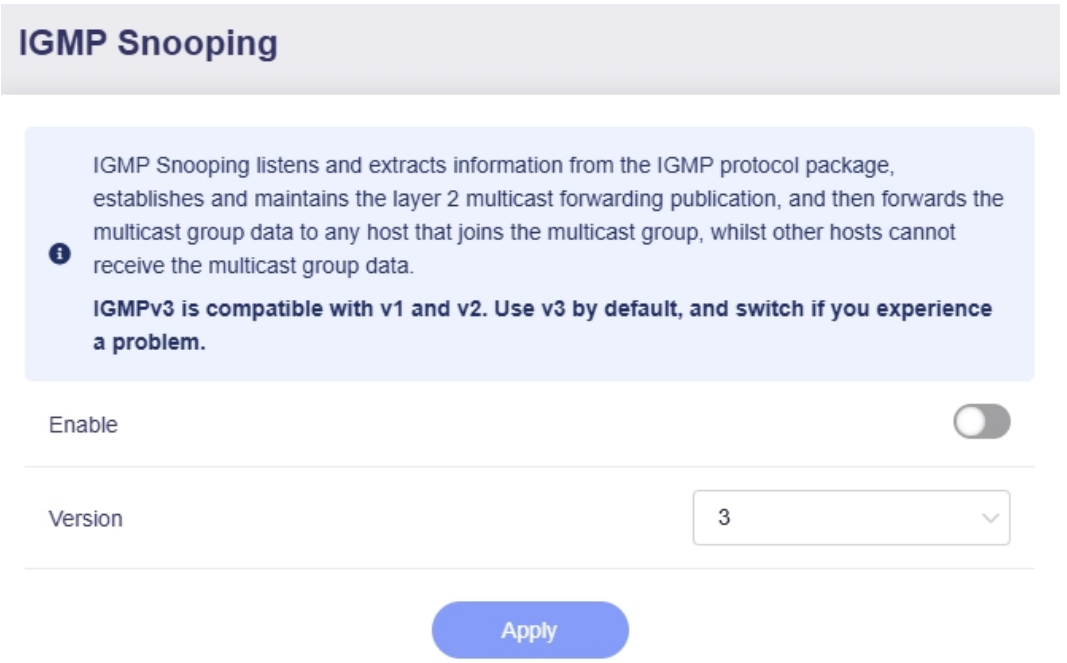
2. Seleccione el método de configuración y luego haga clic en **Aplicar**. Consulte este tutorial para detalless.


Configuration method
All devices are networked through drop-in gateway
You need to go to modify the primary route configuration, which must be configured by a user who has access to the primary route. Setup Guide
Some devices select their own networking gateway
You need to manually change the gateway address to the IP address of the drop-in gateway on some of the devices that need to use the drop-in gateway. Setup Guide

13.10 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.

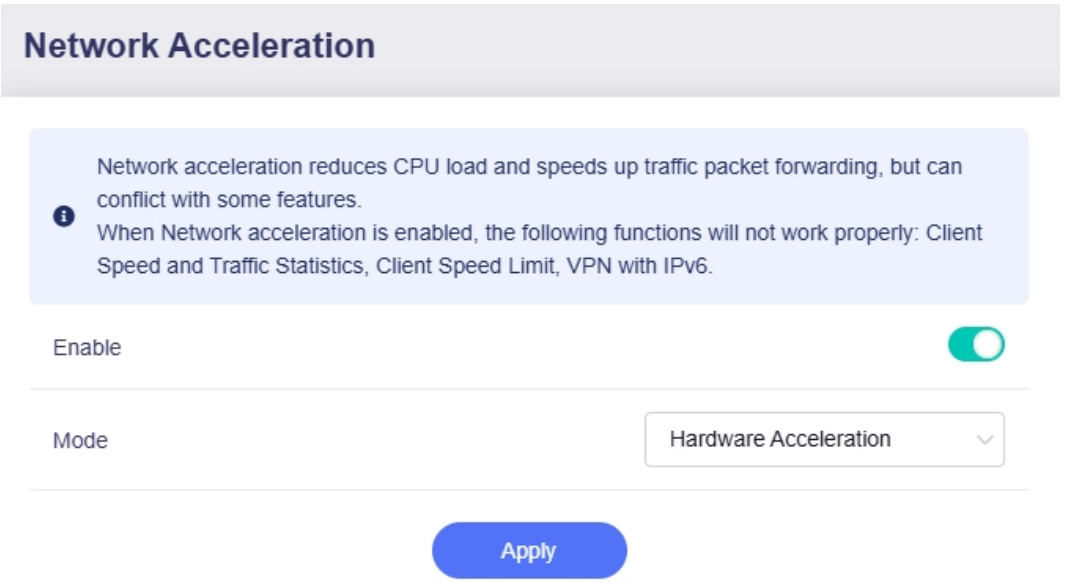
Inicie sesión en el panel de administración web de su enrutador' y navegue hasta **RED** > **Inspección IGMP**. Puede habilitar para utilizar la función de multidifusión en su enrutador si es necesario.



13.11 Aceleración de red

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

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

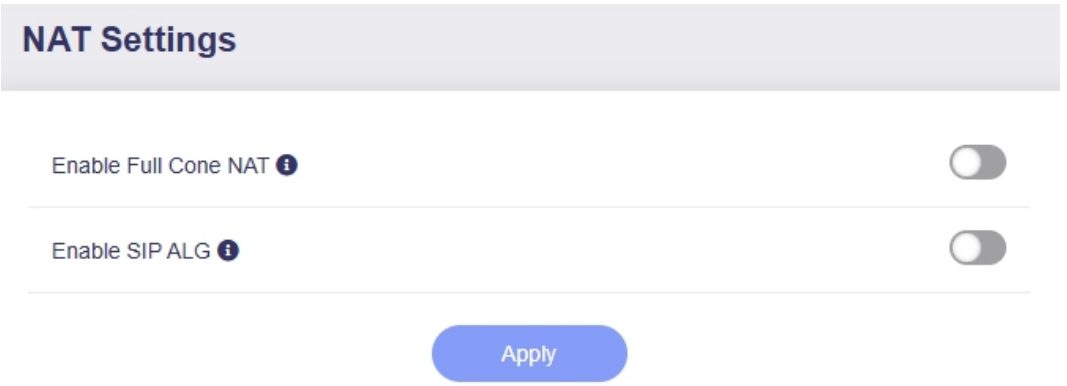


Modo de aceleración de hardware descarga tareas de red de alta frecuencia (por ejemplo, NAT, reenvío de paquetes, verificación de suma de comprobación) a hardware dedicado, como NPU o chips HWNAT. Funciona específicamente en conexiones Ethernet y repetidoras, sobresaliendo en estos escenarios con rutas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

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

13.12 Configuración NAT

Inicie sesión en su enrutador’panel de administración web 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**: Puede usarse para reducir la latencia del juego, mejorando la capacidad de respuesta de los juegos en línea. Sin embargo, habilitar Full Cone NAT 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

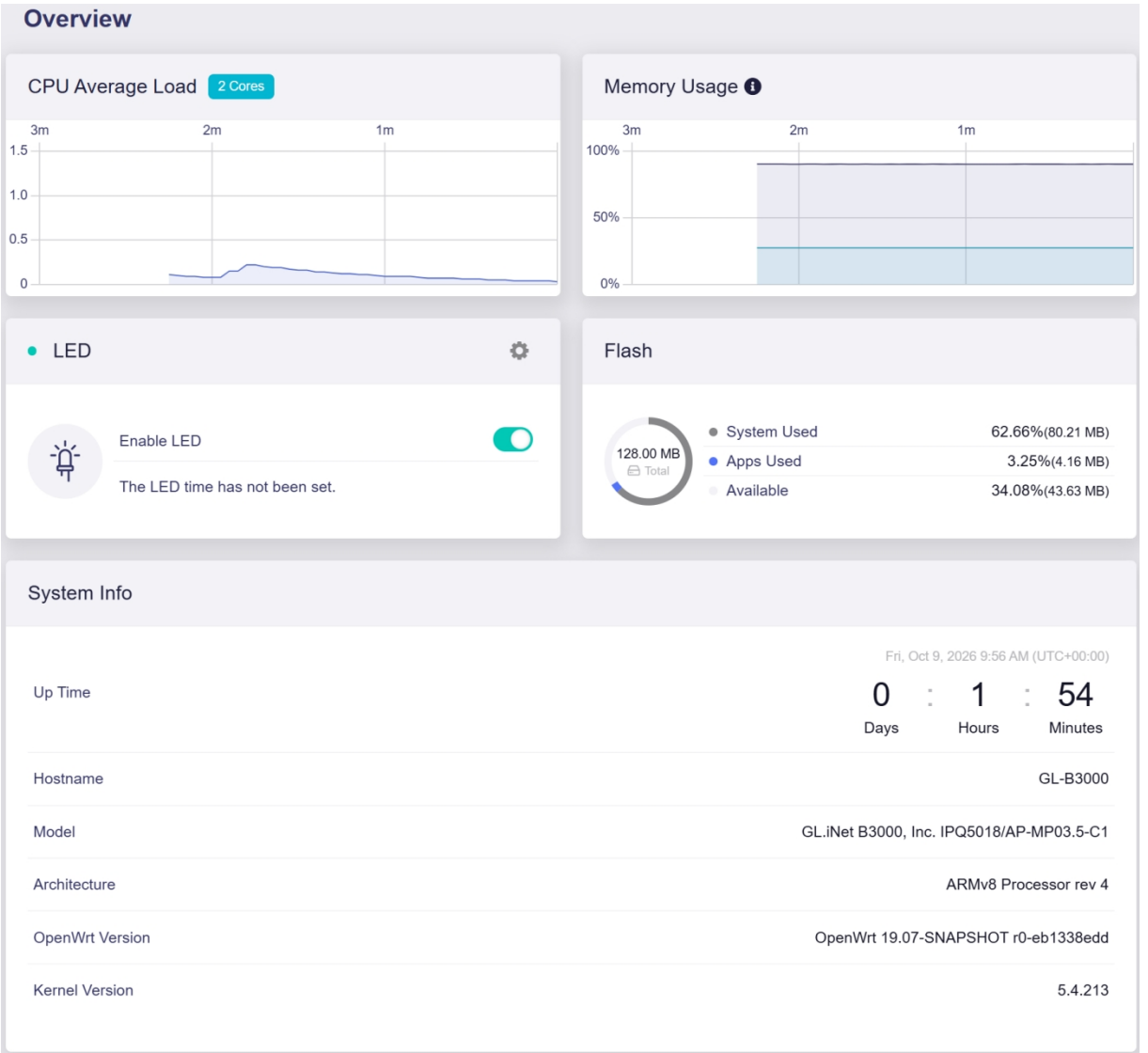
Sistema

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

14.1 Descripción general

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

- CPU, memoria, y Flash Estado
- LED Control
- Dispositivo IInformación

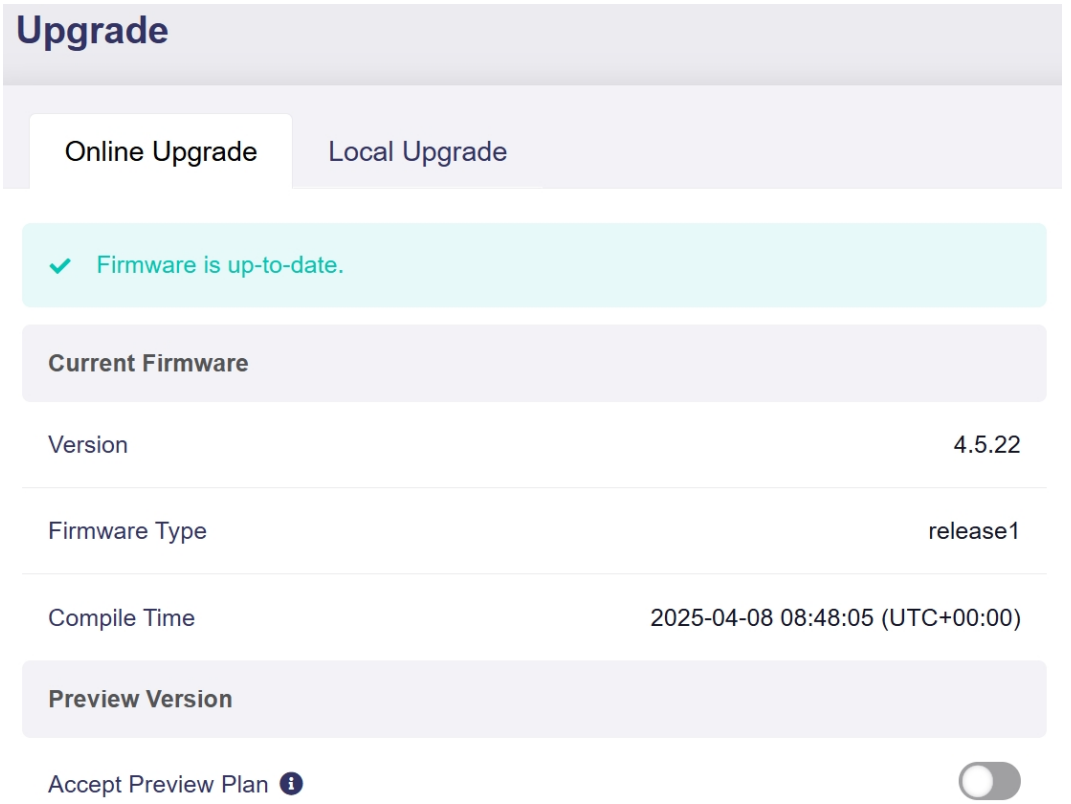


14.2 Actualización

Inicie sesión en el administrador web de su enrutador panel 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. Si su enrutador está conectado a Internet, compruebe si hay una versión de firmware más reciente disponible para descargar.

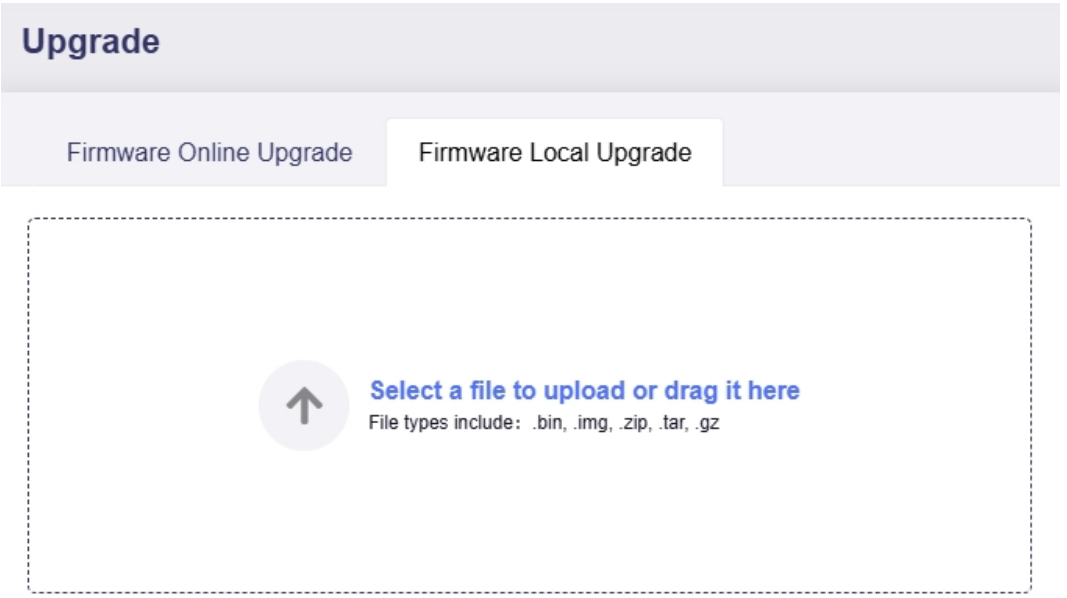


Si **Aceptar plan de vista previa** está habilitado, puede probar nuevas funciones antes de que se emita la versión final y brindarnos sus comentarios. Configúrelo una vez y permanecerá activado. Tenga en cuenta que es posible que estas actualizaciones no sean estables.

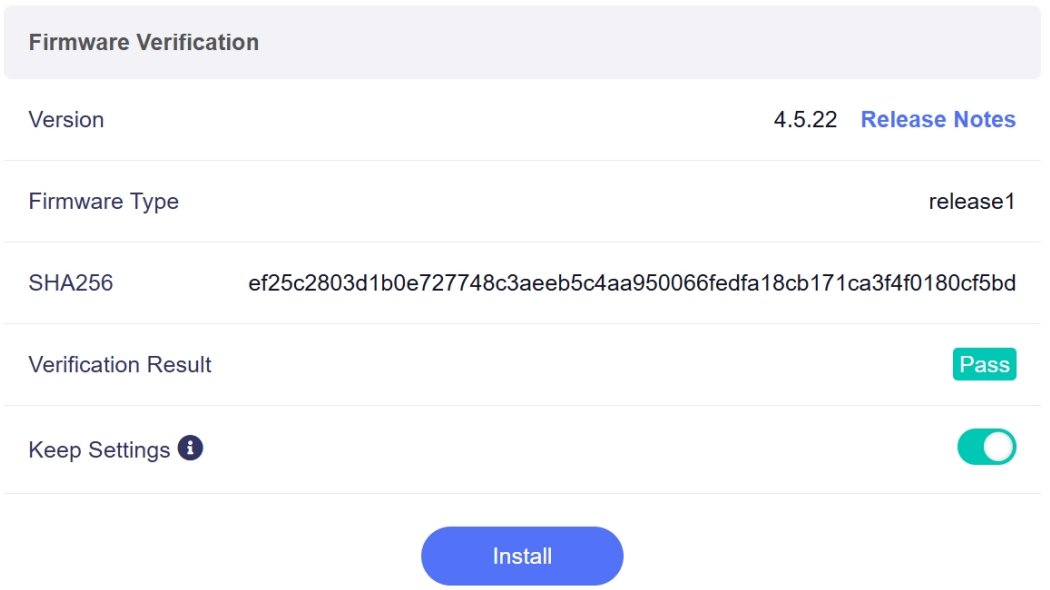
Consejo: Al intentar realizar una actualización en línea, si muestra **Error en la descarga**, navegue hasta **SISTEMA** > **Zona horaria** y corrija el error de zona horaria (sincronización con el navegador).

14.2.2 Actualización local

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



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



Si **Mantener configuración** 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.

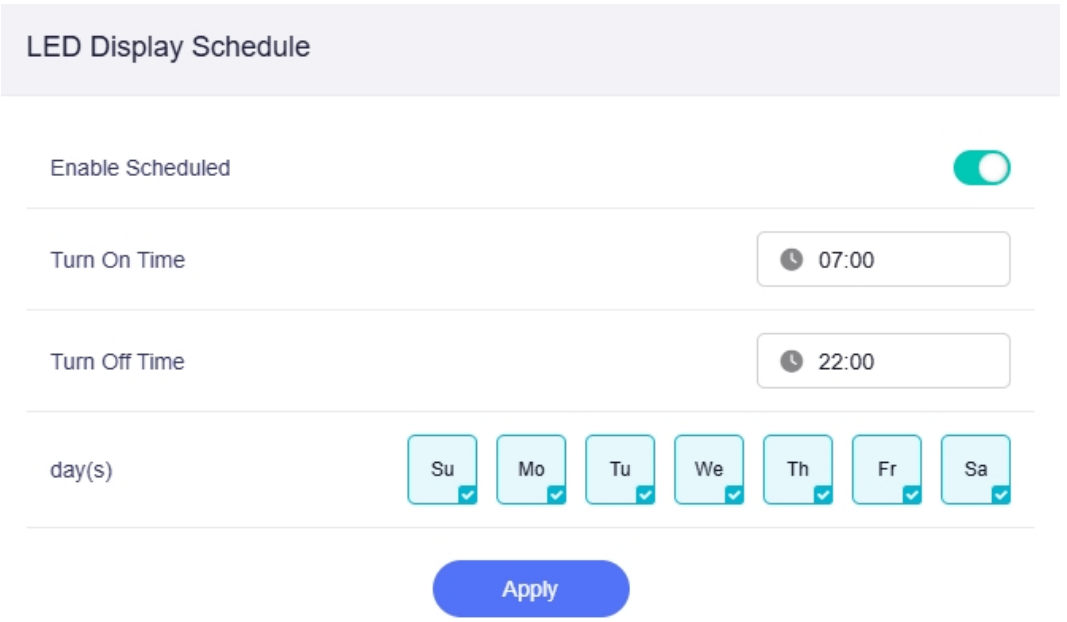
14.3 Tareas programadas

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 cambio de luz LED encendido y apagado, y reiniciar el enrutador.

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

14.3.1 Programación de los indicadores LED

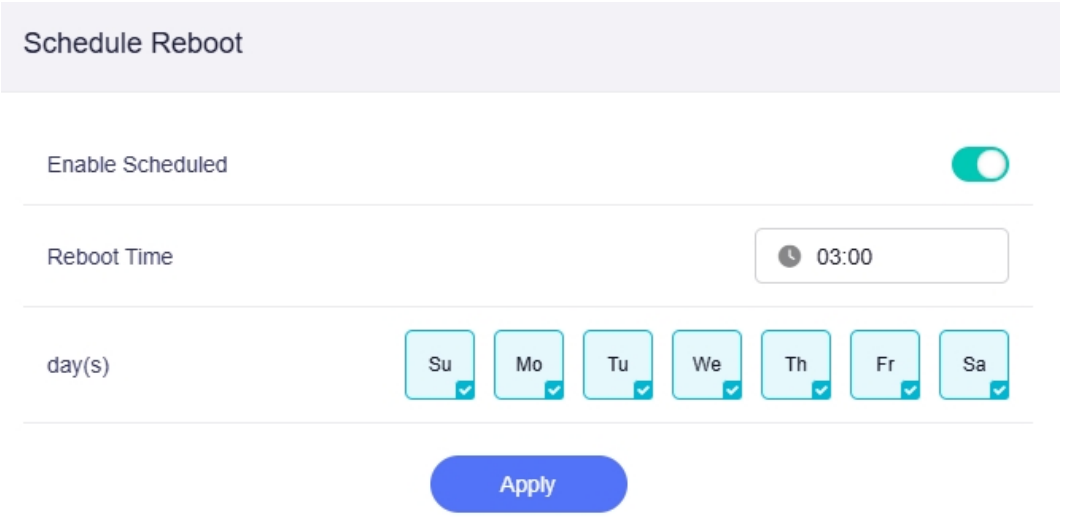
Set a programe la luz LED de su enrutador si es necesario, luego haga clic **Aplicar**.



- **Habilitar programado**: active este interruptor para habilitar el LED programación de visualización.
- **hora 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 La luz LED se apagará.
- **día(s)**: Seleccione los días efectivos de la semana para esta configuración.

14.3.2 Programar reinicio

Sestablezca un programa para reiniciar automáticamente su enrutador si es necesario, luego haga clic **Aplicar**.



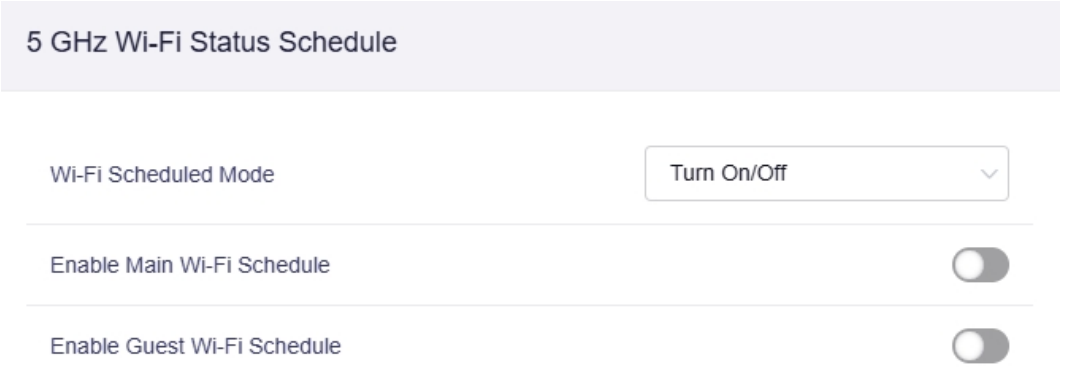
- **Habilitar programado**: active este interruptor para habilitar el reinicio programado.
- **Tiempo de reinicio**: establece la hora específica (por ejemplo, 03:00) a la que se reiniciará el enrutador.
- **día(s)**: Seleccione los días efectivos de la semana para esta configuración.

14.3.3 Programación de Wi-Fi de 5 GHz

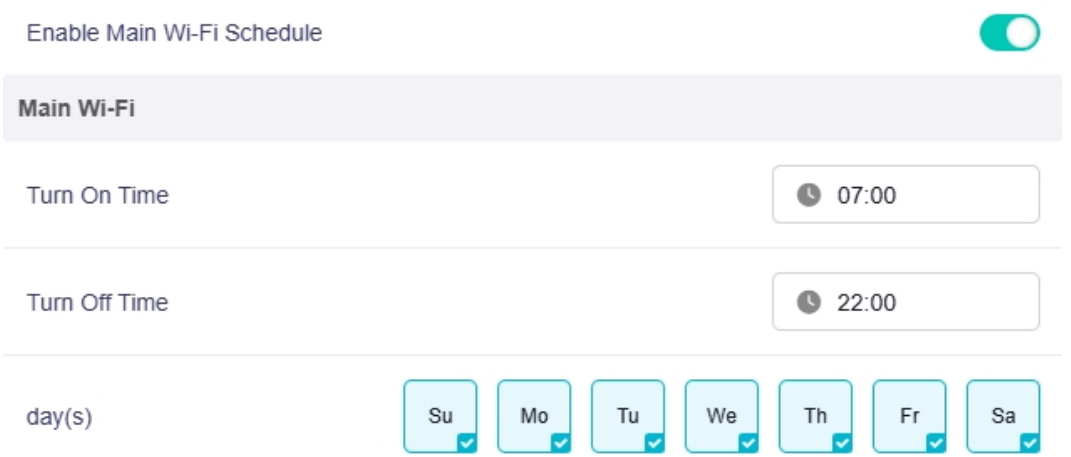
Esta función le permite establecer un horario para su Wi-Fi de 5GHz. Hay dos modos: encender/apagar y cambiar la alimentación de TX.

Modo 1: Encender/apagar

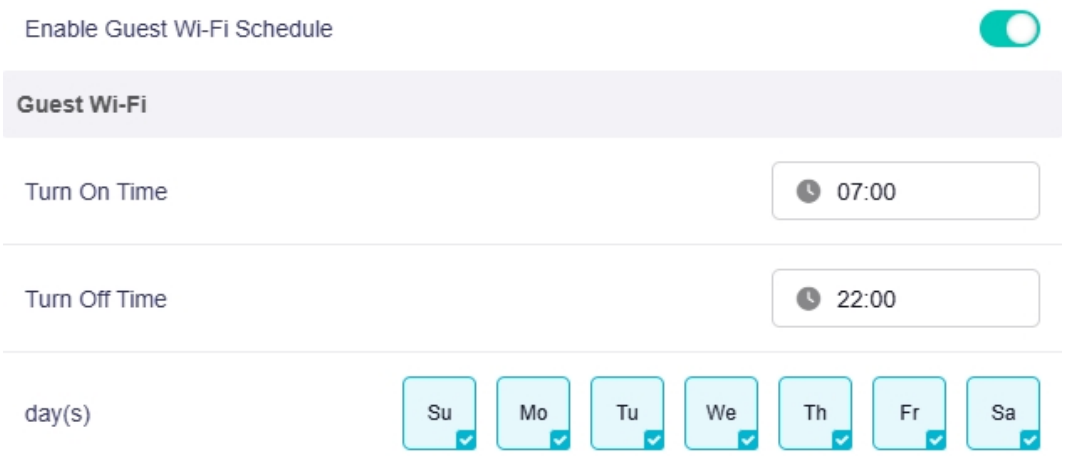
Puedes habilitar el programa de encendido/apagado tanto para el Wi-Fi principal de 5 GHz como para los invitados. Wi-Fi.



- **Programación de Wi-Fi principal**: Cuando esté habilitado, configure los horarios de encendido y apagado de su Wi-Fi principal de 5 GHz y seleccione una fecha efectiva para la semana.

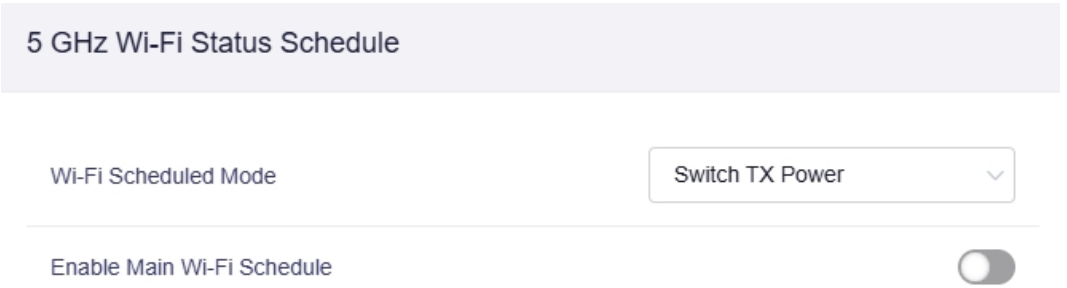


- **Wi-Fi para invitados Programación**: cuando esté habilitado, configure los horarios de encendido y apagado de su Wi-Fi para invitados de 5 GHz y seleccione una fecha efectiva para la semana.

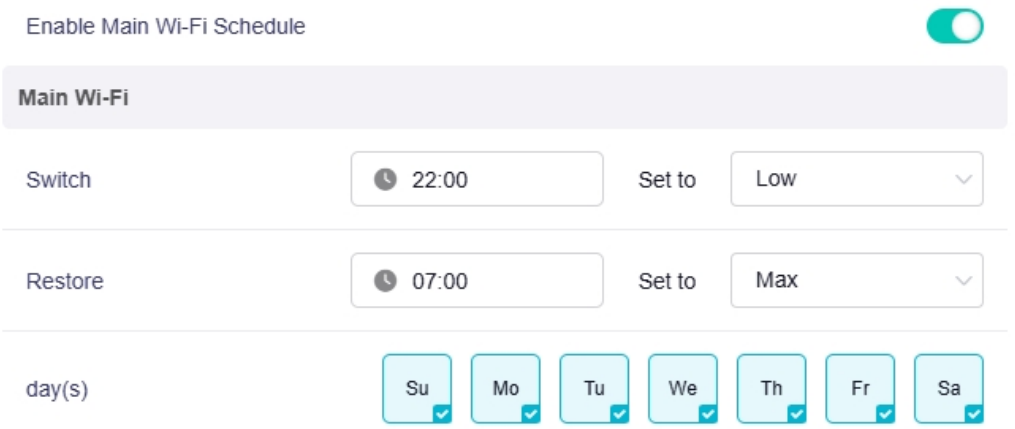


Modo 2: cambie la alimentación de TX

Ypuede habilitar el cambio de energía TX programación para el 5GHz principal Wi-Fi.



Cuando esté habilitado, configure dos acciones cronometradas para que su Wi-Fi principal de 5 GHz cambie la alimentación de transmisión y seleccione una fecha efectiva para la semana.



- **Cambiar**: Sestablece la potencia de TX a un cierto nivel (por ejemplo, bajo) at un hora (por ejemplo, 22:00).

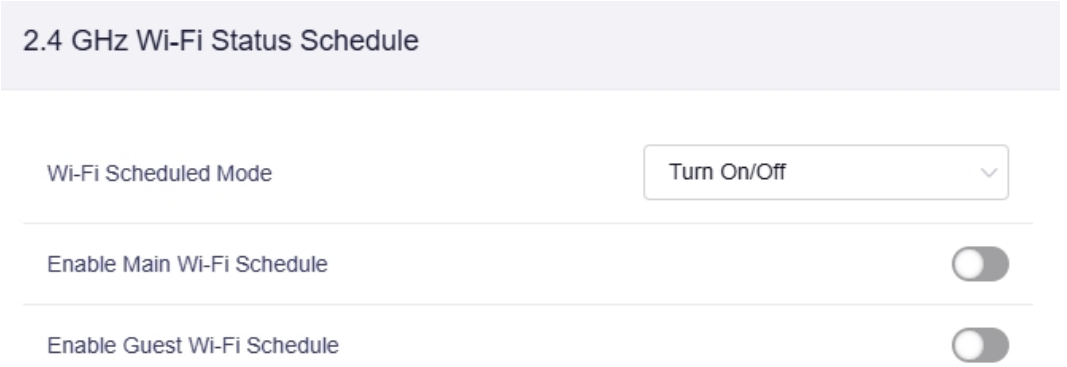
- **Restaurar**: Restablecer energía TX en unotro nivel (por ejemplo, Max) at en otro momento (por ejemplo, 07:00).
- **días**: Seleccione el nivel efectivo días de la semana para estas configuraciones.

14.3.4 Programación de Wi-Fi de 2,4 GHz

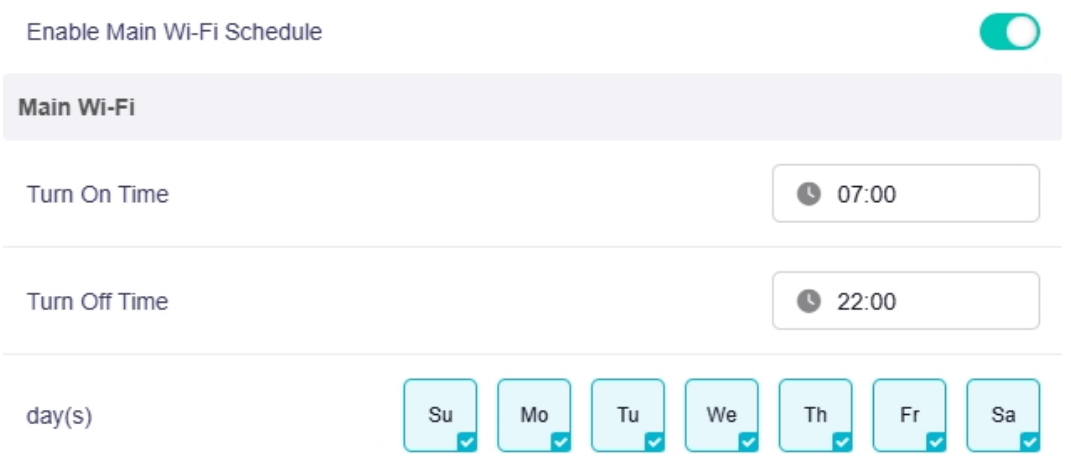
Esta función le permite establecer una programación para su Wi-Fi de 2,4 GHz. Hay dos modos: encender/apagar y cambiar la alimentación de TX.

Modo 1: Encender/apagar

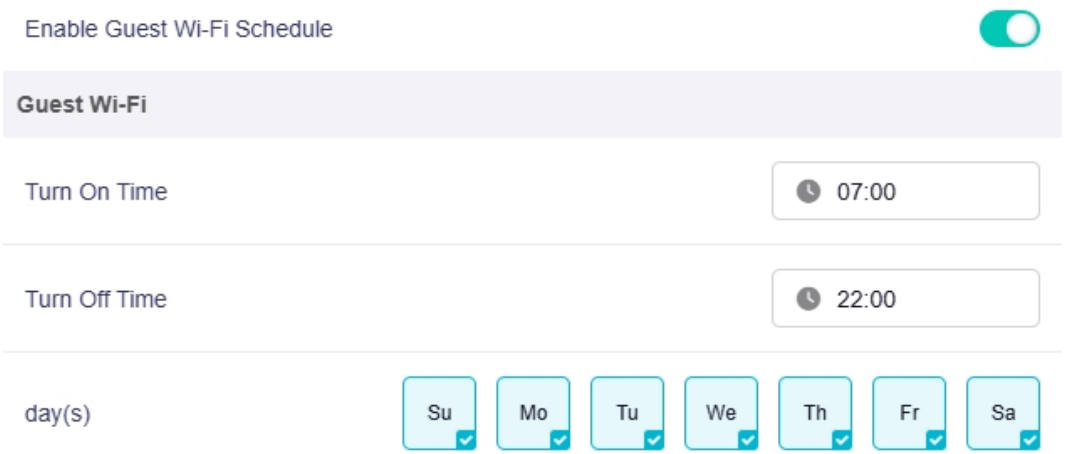
Puedes habilitar el horario de encendido/apagado tanto para el Wi-Fi principal de 2,4 GHz como para los invitados. Wi-Fi.



- **Programación de Wi-Fi principal**: Cuando esté habilitado, configure los horarios de encendido y apagado de su Wi-Fi principal de 2,4 GHz y seleccione una fecha efectiva para la semana.

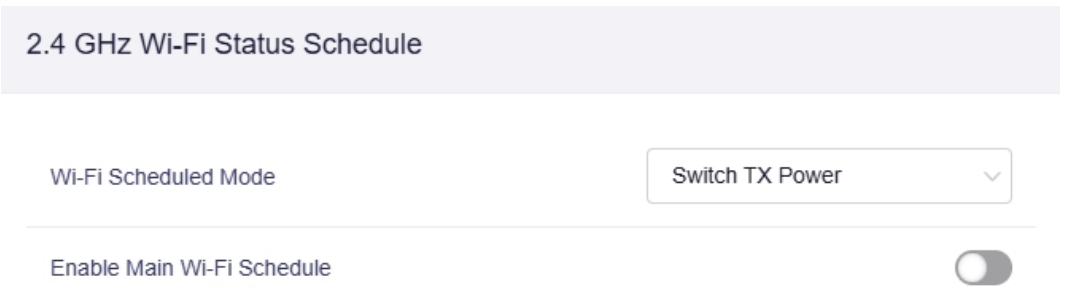


- **Wi-Fi para invitados Programación**: cuando esté habilitado, configure los horarios de encendido y apagado de su Wi-Fi para invitados de 2,4 GHz y seleccione una fecha efectiva para la semana.

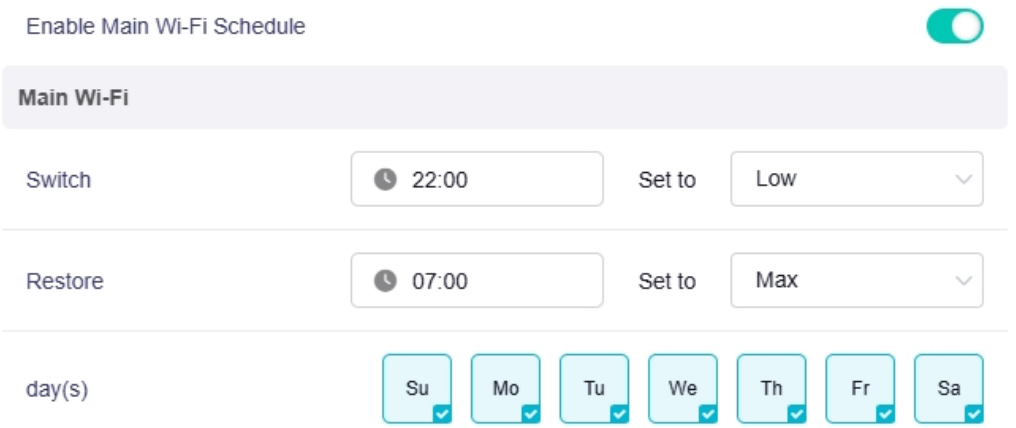


Modo 2: cambie la alimentación de TX

Ypuede habilitar el programación de conmutación de alimentación TX para el 2,4 GHz Wi-F principali.



Cuando esté habilitado, configure dos acciones cronometradas para que su Wi-Fi principal de 2,4 GHz cambie la alimentación de TX y seleccione una fecha efectiva para la semana.

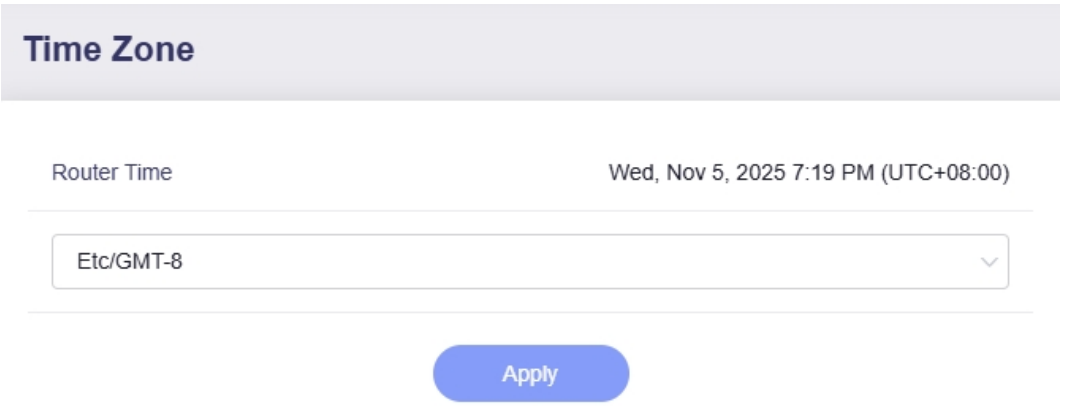


- **Cambiar**: Set TX Power a un cierto nivel (por ejemplo, bajo) aen una hora específica (por ejemplo, 22:00).

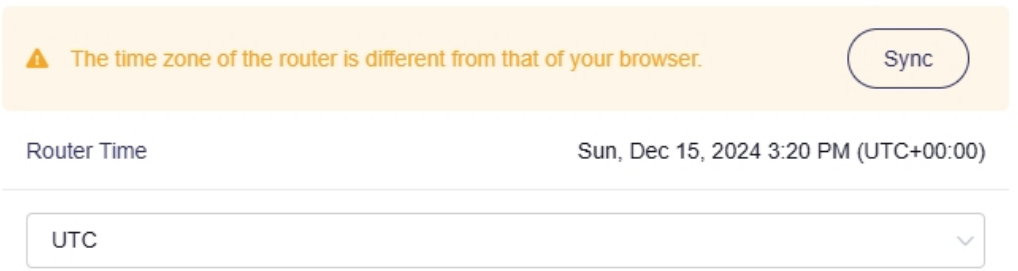
- **Restaurar**: Restore TX Power aotro nivel (por ejemplo, Max) at en otro momento (por ejemplo, 07:00).
- **días**: Seleccione los días efectivos de la semana para esta configuración.

14.4 Zona horaria

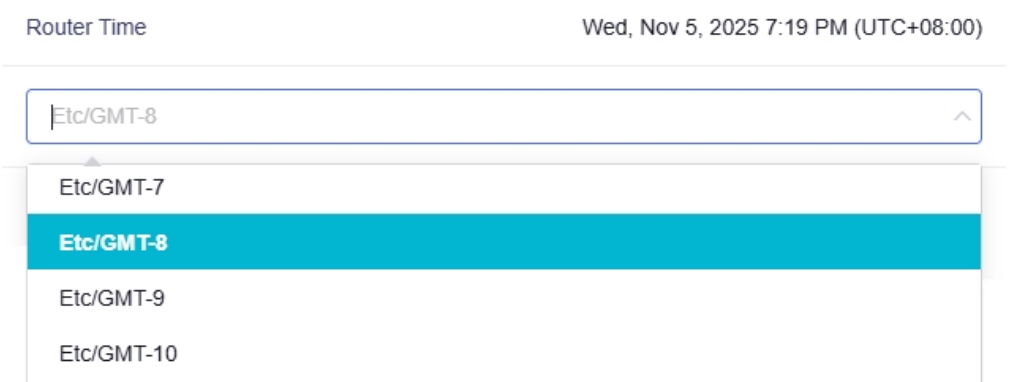
Inicie sesión en el panel de administración web de su enrutador y navegue hasta **SISTEMA** > **Zona horaria**. Esta página muestra la la hora, indicando la fecha, la hora y el desplazamiento de zona horaria correspondiente.



Algunas funciones dependen del tiempo del sistema del enrutador’para surtir efecto. 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.

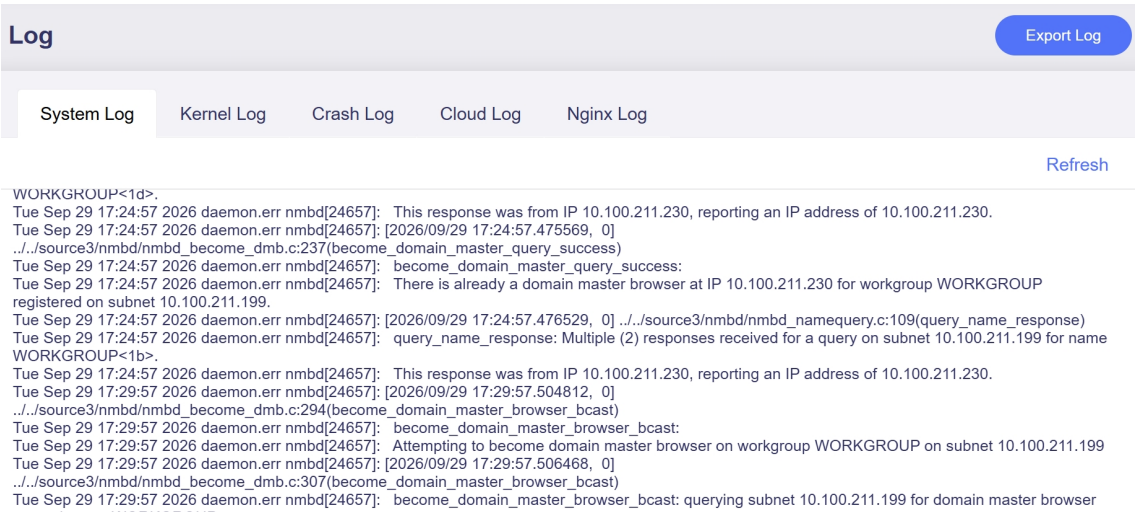


Para cambiar zona horaria, sseleccione la zona horaria adecuada de la lista para garantizar que la hora del sistema coincida con su hora local.



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, bloqueo, nube y Nginx para análisis y solución de problemas.



- **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.

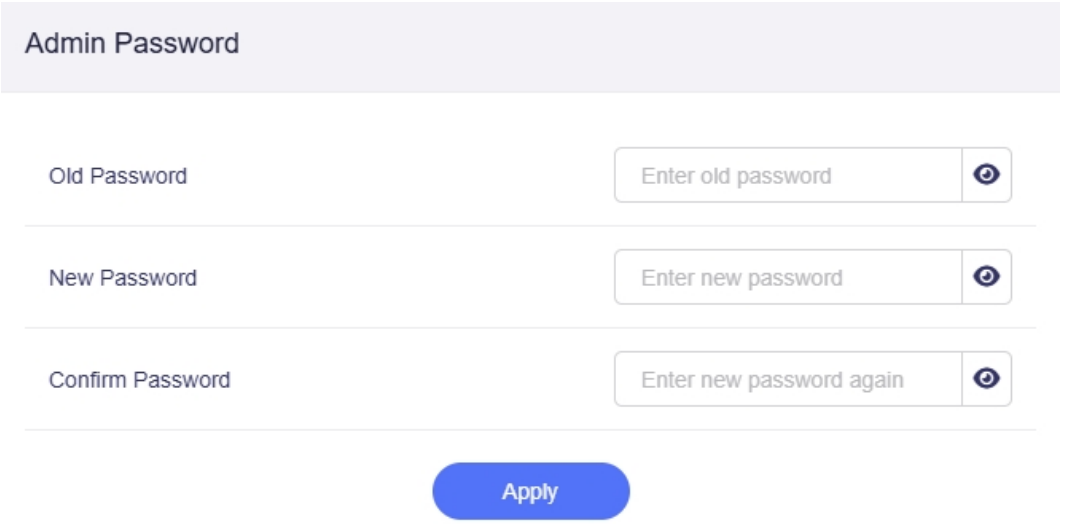
14.6 Seguridad

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 local para web panel de administración, LuCI y SSH
- Remote HTTPS/SSH uncceso
- Opuertos de lápiz en rexterno

14.6.1 Contraseña de administrador

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

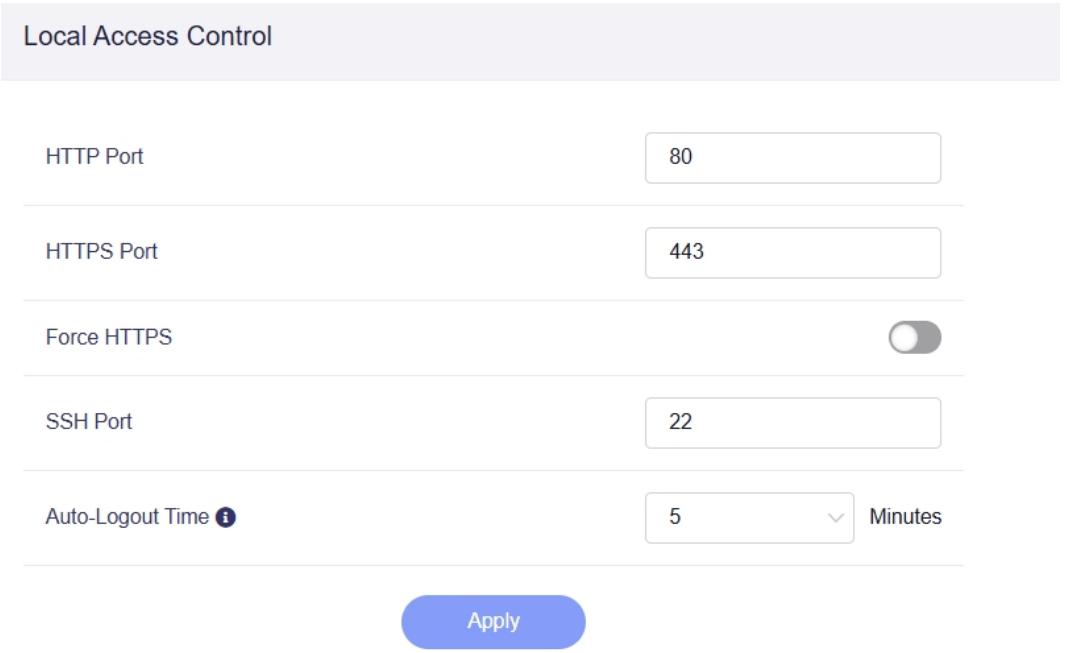


Los requisitos para la contraseña de administrador son los siguientes:

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

14.6.2 Control de acceso local

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

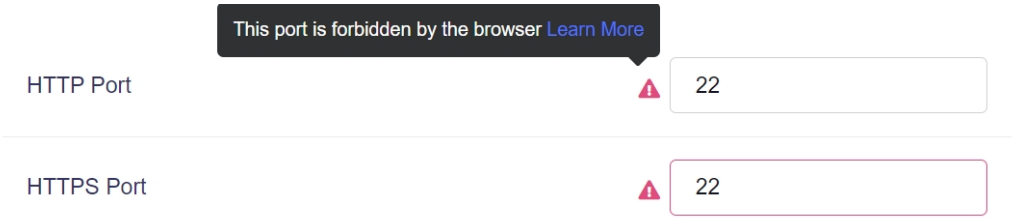


Panel de administración

- **Puerto HTTP**: el valor predeterminado es 80, utilizado para el acceso HTTP sin cifrar al administrador web. panel.
- **Puerto HTTPS**: el valor predeterminado es 443, utilizado para el acceso HTTPS seguro al panel de administración web.
- **Forzar HTTPS**: Cuando está habilitado, se exige el acceso al panel de administración web para utilizar una conexión HTTPS segura.
- **Puerto SSH**: el valor predeterminado es 22, el puerto utilizado para el acceso SSH al enrutador.
- **Cierre de sesión automático Tiempo**: configurado en 5 minutos de forma predeterminada, cierra automáticamente las sesiones de administración inactivas después de esta duración por motivos de seguridad. Puede personalizar el tiempo de cierre de sesión automático, que oscila entre 1 minuto y 3 horas.

Nota:

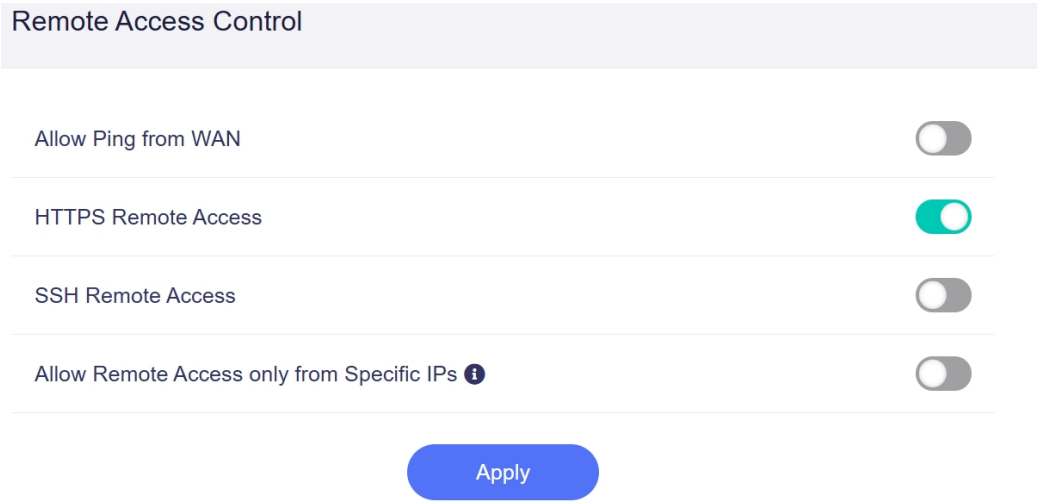
1. Si asigna un número de puerto que entra en conflicto con un puerto reservado (o uno reservado para servicios específicos por navegadores/convenciones de red), aparecerá un mensaje que indicará "Este puerto está prohibido por el navegador".



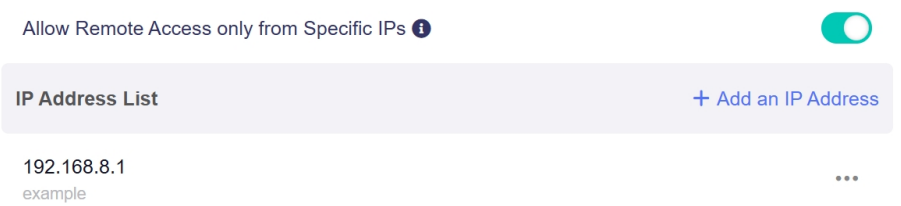
2. Si el número de puerto se modifica en el firmware, deberá ingresar el número de puerto correcto para acceder al panel de administración. Si olvidó el número de puerto, reinicie el enrutador. para restaurar el número de puerto predeterminado.

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. para restringir el acceso desde direcciones IP específicas, logrando un equilibrio entre accesibilidad remota y seguridad de la red.



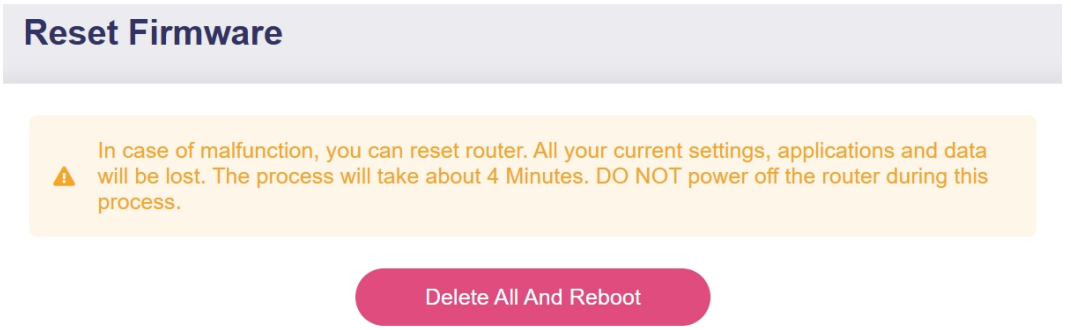
- **Permitir ping desde WAN**: Apermitir ping desde el lado WAN del enrutador puede ayudar a los usuarios a comprobar si se puede acceder al enrutador a través de la WAN wcuando hay un problema de red, así como a determinar la latencia de la red y la pérdida de paquetes.
- **Acceso remoto HTTPS**: El 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 cifrada cuando se administra el enrutador de forma remota a través de un navegador web.
- **Acceso remoto SSH**: El acceso remoto SSH permite la seguridad 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.



14.7 Restablecer firmware

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

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



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

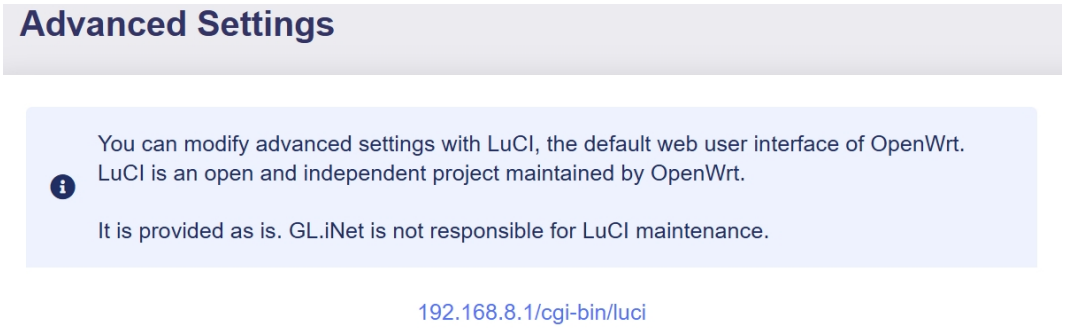
Si no puede acceder al panel de administración web del enrutador', intente restablecer su enrutador usando el botón de reinicio físico en el lado.

14.8 Configuración avanzada

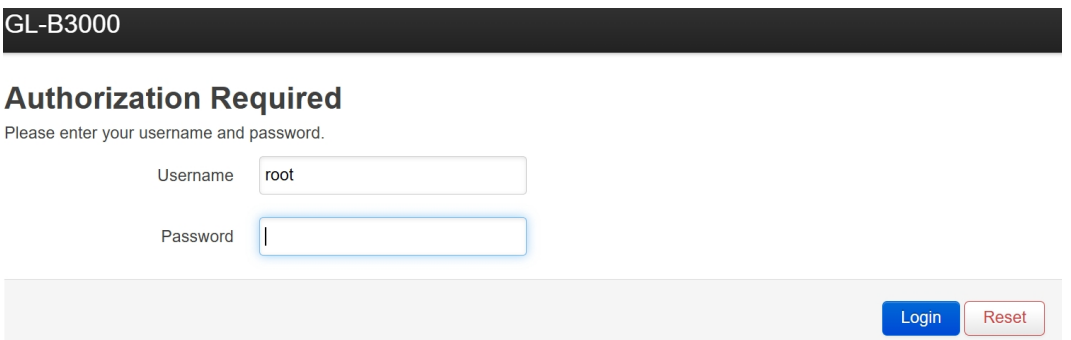
Inicie sesión en el panel de administración web de su enrutador y navegue hasta **SISTEMA** > **Configuración avanzada**. Esta página le permitemodificar la configuración avanzada a modificar configuración avanzada en LuCI, que es la interfaz de usuario web predeterminada de OpenWrt. Como proyecto abierto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

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

1. Click el acceso enlace, y será redirigido a la página de inicio de sesión de LuCI.



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



Yusted luego registrar en en el LuCI interfaz.

