GL·iNet



Manual de usuario

GL-BE9300 / Flint 3

Enrutador doméstico Wi-Fi 7 de tres bandas

Versión de firmware 4.9.0

Acerca de este manual

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

Con esta guía, podrá:

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

Convenciones de formato

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

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

Nota:

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

¿Necesita más ayuda o información?

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

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

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

Contenido

Capítulo 1 Conozca su enrutador 6

1.1 Descripción general del producto 7

1.1.1 Apariencia 7

1.1.2 Interfaz y botón 8

1.1.3 LED 9

1.2 Especificaciones 9

1.3 Contenido del paquete 11

Capítulo 2 Conexión de hardware 12

2.1 Elección de una ubicación 13

2.2 Conexión del enrutador 13

Capítulo 3 Iniciar sesión en el enrutador 14

Capítulo 4 Configurar la conexión a Internet 16

4.1 Asistente de configuración rápida 17

4.2 Configurar manualmente la conexión a Internet 18

4.2.1 Conectarse a Internet mediante un cable Ethernet 19

4.2.2 Conectarse a Internet mediante una red Wi-Fi existente 23

4.2.3 Conectarse a Internet mediante conexión compartida por USB 30

4.2.4 Conectarse a Internet mediante un módem USB 35

Capítulo 5 Red inalámbrica 37

5.1 Visualización del estado de Wi-Fi 38

5.2 Configuración inalámbrica 39

5.2.1 Wi-Fi MLO 39

5.2.2 Red principal 41

5.2.3 Red de invitados 42

5.2.4 Red de IoT 44

Capítulo 6 Clientes 46

6.1 Detalles del dispositivo 48

6.2 Acción 50

6.3 Ordenar 53

6.4 Configuración 54

Capítulo 7 Servicios en la nube 55

7.1 GoodCloud 56
7.1.1 Habilitar GoodCloud 56
7.1.2 Administrar el enrutador 59
7.1.3 Desvincular el dispositivo 63
7.1.4 Desactivar GoodCloud 64
7.2 AstroWarp 65
7.2.1 Configuración rápida 65
7.2.2 Comprobar la conectividad 69
Capítulo 8 Conozca la VPN 70
8.1 Introducción 71
8.2 Escenarios de aplicación 72
Capítulo 9 Panel de VPN 74
9.1 Cargar perfil VPN 75
9.2 Agregar túnel VPN 78
9.2.1 Pasos generales 78
9.2.2 Referencia del caso 81
9.3 Bloqueo de tráfico sin VPN (Kill Switch) 97
9.4 Todo el resto del tráfico 98
9.5 Opciones de túnel 99
9.6 Prioridad del túnel 101
Capítulo 10 Configurar el servidor VPN 103
10.1 Configurar el servidor OpenVPN 104
10.1.1 Preparación 104
10.1.2 Pasos de configuración 105
10.1.3 Solución de problemas 108
10.2 Configurar el servidor WireGuard 109
10.2.1 Preparación 109
10.2.2 Pasos de configuración 110
10.2.3 Solución de problemas 114
Capítulo 11 Configurar el cliente VPN 115
11.1 Configurar el cliente OpenVPN 116
11.1.1 Preparación 116
11.1.2 Configurar NordVPN 116
11.1.3 Configurar el cliente OpenVPN manualmente (para otros proveedores) 122

11.2 Configurar el cliente WireGuard 125
11.2.1 Preparación 125
11.2.2 Configurar AzireVPN 126
11.2.3 Configurar Hide.me 130
11.2.4 Configurar IPVanish 133
11.2.5 Configurar Mullvad 137
11.2.6 Configurar NordVPN 141
11.2.7 Configurar PIA (Private Internet Access) 146
11.2.8 Configurar Surfshark 150
11.2.9 Configurar el cliente WireGuard manualmente (para otros proveedores) ... 154
Capítulo 12 Red 159
12.1 Multi-WAN 160
12.1.1 Seguimiento del estado de la interfaz 160
12.1.2 Modo Multi-WAN 163
12.2 LAN 166
12.2.1 Configuración básica 166
12.2.2 Servidor DHCP 167
12.2.3 Reserva de direcciones 169
12.3 Red de invitados 170
12.3.1 Configuración básica 170
12.3.2 Servidor DHCP 171
12.4 Red de IoT 173
12.4.1 Configuración básica 173
12.4.2 Servidor DHCP 174
12.5 DNS 176
12.5.1 Configuración del servidor DNS 177
12.5.2 Editar hosts 181
12.6 Puerto Ethernet 182
12.7 IPv6 183
12.7.1 Modo IPv6 184
12.7.2 Método de obtención de DNS 184
12.8 Inspección IGMP 185
12.9 Modo de red 186
12.10 Puerta de enlace directa 189

12.11 Aceleración de red 191
Capítulo 13 Control de flujo 192
13.1 Motor DPI 193
13.2 Estadísticas de datos 195
13.2.1 Configuración rápida 195
13.2.2 Reglas de almacenamiento de datos 197
13.2.3 Cambiar el intervalo de tiempo 197
13.2.4 Borrar estadísticas 198
13.3 Filtro de contenido 199
13.4 Calidad de servicio (QoS) 201
13.5 Gestión inteligente de colas (SQM) 203
13.6 Control parental 205
Capítulo 14 Seguridad 211
14.1 Reenvío de puertos 212
14.1.1 DMZ 212
14.1.2 Reenvío de puertos 213
14.2 Lista de control de acceso (ACL) 215
14.3 Acceso de administrador 217
14.3.1 Control de acceso 217
14.3.2 Control de acceso remoto 220
14.3.3 Abrir puertos en el enrutador 221
14.4 Modo NAT 223
Capítulo 15 Aplicaciones 224
15.1 Complementos 225
15.2 DNS dinámico 226
15.2.1 Habilitar DDNS 226
15.2.2 Comprobar si DDNS funciona 229
15.2.3 Acceso remoto HTTPS 231
15.2.4 Acceso remoto SSH 233
15.3 Almacenamiento en red 235
15.3.1 Conectar una unidad de almacenamiento 235
15.3.2 Configurar Samba 236
15.3.3 Configurar WebDAV 239
15.3.4 Configurar DLNA 242

15.4 AdGuard Home 243
15.5 Bark 245
15.6 Tailscale 247
15.6.1 Configurar Tailscale 248
15.6.2 Anunciar subredes WAN 251
15.6.3 Anunciar subredes LAN 252
15.6.4 Nodos de salida personalizados 253
15.6.5 Activar el nodo de salida 254
15.7 ZeroTier 261
15.7.1 Configurar ZeroTier 262
15.7.2 Permitir el acceso remoto a la WAN 266
15.7.3 Permitir el acceso remoto a la LAN 267
15.8 Tor 268
Capítulo 16 Sistema 269
16.1 Descripción general 270
16.2 Contraseña de administrador 271
16.3 Actualización 272
16.3.1 Actualización en línea 272
16.3.2 Actualización local 274
16.4 Tareas programadas 276
16.4.1 Programación de los indicadores LED 276
16.4.2 Programar reinicio 277
16.4.3 Programación de Wi-Fi MLO 277
16.4.4 Programación de Wi-Fi de 6 GHz 278
16.4.5 Programación de Wi-Fi de 5 GHz 280
16.4.6 Programación de Wi-Fi de 2,4 GHz 282
16.5 Zona horaria 284
16.6 Restablecer firmware 285
16.7 Registro 286
16.8 Configuración avanzada 288
Declaración de Conformidad 290

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

Flint 3 es el primer enrutador doméstico Wi-Fi 7 de GL.iNet, diseñado para usuarios domésticos y oficinas pequeñas. Ofrece velocidades ultrarrápidas de Wi-Fi 7, 5 puertos 2.5G y sólidas capacidades de VPN, junto con AdGuard Home y controles parentales. Flint 3 está diseñado para satisfacer las demandas cambiantes de las redes modernas con eficiencia y confiabilidad.

1.1.1 Apariencia

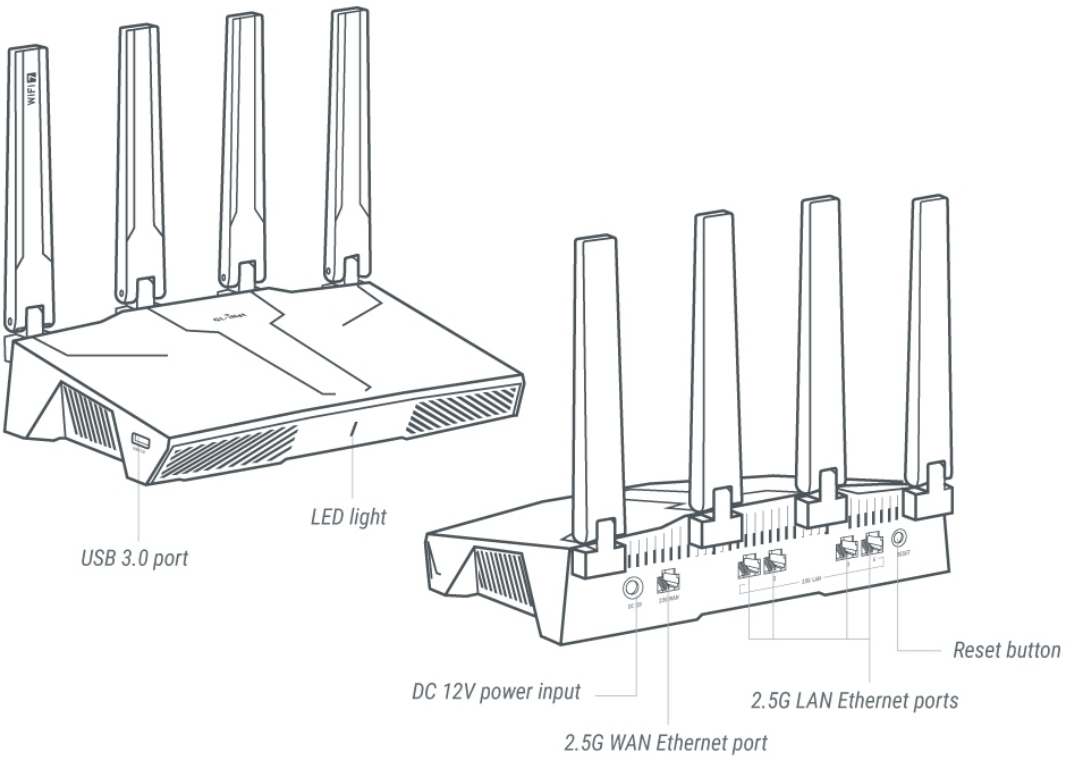








1.1.2 Interfaz y botón



Artículo	Descripción
Puerto de alimentación	Se conecta al adaptador de corriente.
Puerto WAN 2.5G	Se conecta a un módem o a una toma Ethernet para Internet.
Puerto LAN 2.5G	Se conecta a dispositivos cableados si es necesario.
Puerto USB 3.0	Para dispositivos de almacenamiento USB, conexión USB de teléfono y dongles celulares compatibles.
Botón Restablecer	Presione y mantenga presionado durante **4 segundos** y luego suelte para reparar su red.
	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	Iniciando
Pulsando en azul lentamente	Iniciado pero sin conexión a Internet
Blanco sólido	Conectado a Internet
Azul parpadeante rápidamente	Restableciendo

1.2 Especificaciones

Interfaz	1 puerto Ethernet WAN 2,5G 1 puerto Ethernet WAN/LAN de 2,5G 3 puertos Ethernet LAN 2.5G 1 x puerto USB 3.0 1 x botón de reinicio
CPU	Qualcomm de cuatro núcleos a 1,5 GHz
Memoria/Almacenamiento	DDR4 1GB / eMMC 8GB
Protocolo	IEEE 802.11a/b/g/n/ac/ax/be
Velocidad de Wi-Fi	688Mbps (2,4 GHz), 2882 Mbps (5 GHz), 5765 Mbps (6 GHz)
Antenas	4 x antenas Wi-Fi externas plegables
Velocidad de Ethernet	10/100/1000/2500Mbps
Entrada de energía	DC5521, 12V/4A (5,5 x 2,1 mm)
Consumo de energía	Sin carga USB: <25W Con carga USB: <37.2W
Temperatura de funcionamiento	0 ~ 40°C (32 ~ 104°F)
Temperatura de almacenamiento	-20 ~ 70°C (-4 ~ 158°F)

Dimensión/Peso	240 x 157 x 74 mm / 848 g
Otras herramientas	Hoja de datos / Firmware / Aplicación / Unboxing / Tutoriales

*Las velocidades inalámbricas se basan en los estándares IEEE 802.11 (por ejemplo, 802.11be para Wi-Fi 7). 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 7 (802.11be) y sus características (OFDMA, MU-MIMO, 4096-QAM, MLO) requiere que los dispositivos cliente admitan las tecnologías correspondientes.

1.3 Contenido del paquete

El paquete incluye:

- 1 x Flint 3 (GL-BE9300)
- 1 x Manual del usuario (Guía de inicio rápido)
- 1 cable Ethernet
- 1 x Tarjeta de agradecimiento
- 1 x adaptador de corriente
- 1 x Convertidor (Dependiendo de su país de envío)



1 x User manual



1 x Flint 3 (GL-BE9300)



1 x Thank you card



1 x Ethernet cable



1 x Power adapter



Converter

(Base on your shipping country)

Capítulo 2

Conexión de hardware

Este capítulo cubre la selección y conexión de la ubicación del enrutadorion pasos.

2.1 Elección de una ubicación

Siga estos consejos para elegir una 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 adecuada disipación del calor.
- **Ubicación central**: coloque el enrutador donde pueda conéctese fácilmente a la alimentación y a varios dispositivos (por ejemplo, la zona).
- **Cable conveniencia**: enrute los cables y el cable de alimentación de forma segura para evitar riesgos de tropiezos.
- **Estable superficie**: coloque el enrutador en una superficie plana y horizontal (estante, escritorio) para mayor estabilidad.
- **Evitación de EMI**: mantenga el enrutador alejado de fuentes de interferencias electromagnéticass (dispositivos Bluetooth, microondas) para minimice 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 un tomacorriente.

2. **Conecte un dispositivo al enrutador**

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

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

3. **Inicie sesión en enrutador**

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

Capítulo 3

Iniciar sesión en el enrutador

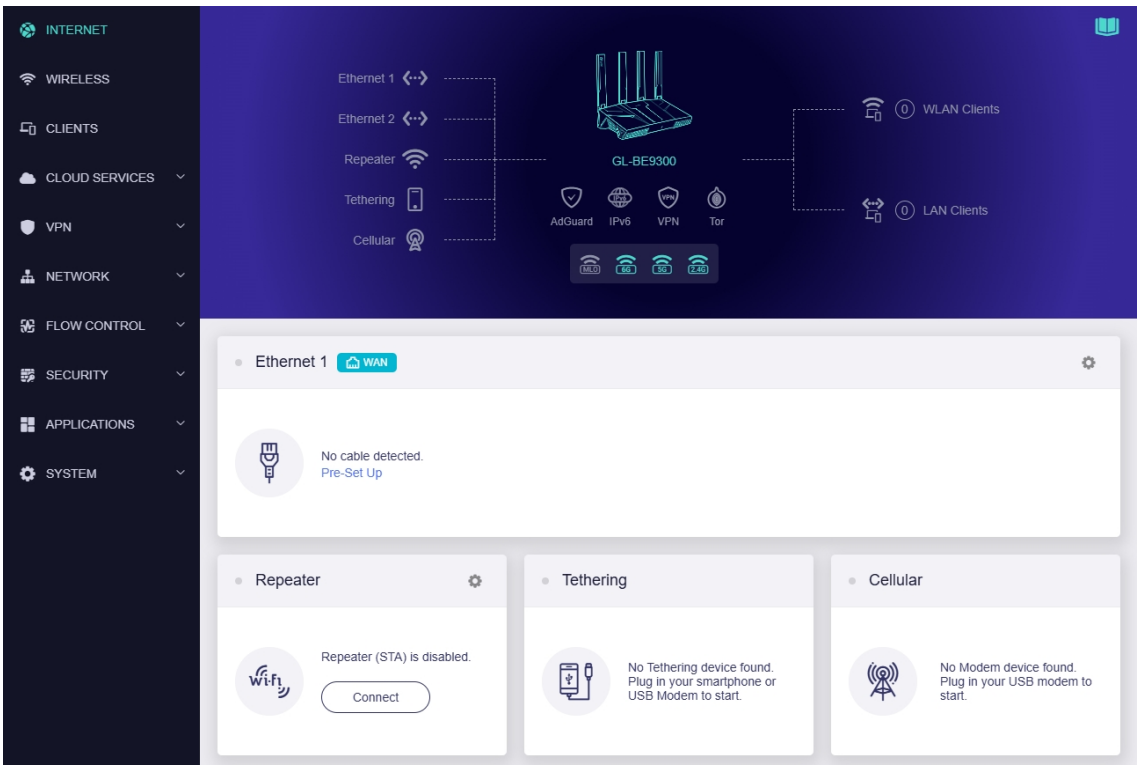
Este capítulo lo guía para iniciar sesión en su enrutador a través del panel de administración web.

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

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

Siga los pasos siguientes 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. Abra un navegador web (se recomiendan Chrome y Edge) y visita http://192.168.8.1. Serás dirigido a la página de inicio de sesión de la web admin panel. Si no puede acceder a la web undmin panel, consulte aquí para solucionar problemas.
3. Set arriba su contraseña de administrador. Se recomienda una contraseña segura por motivos de seguridad. Luego haga clic en **Siguiente** para continuar.
4. Yluego ingresará el enrutador's web admin panel.



Capítulo 4

Configurar la conexión a Internet

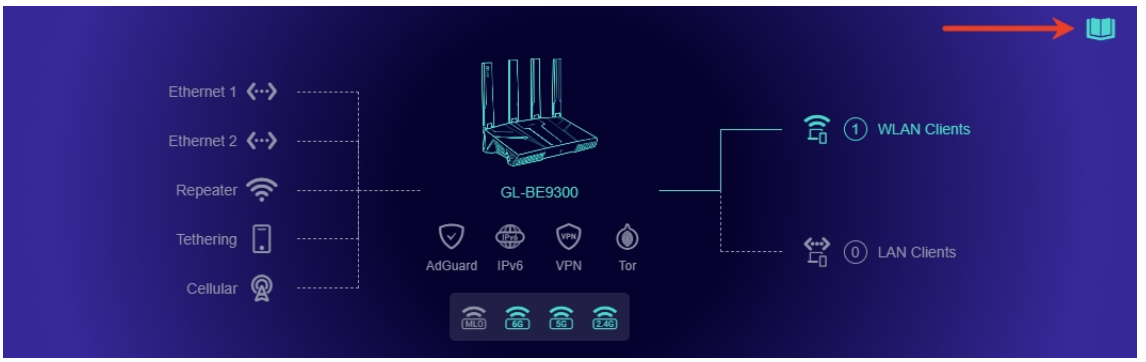
Este capítulo presenta múltiples métodos de conexión a Internet para que el enrutador se adapte a diversos entornos de red.

4.1 Asistente de configuración rápida

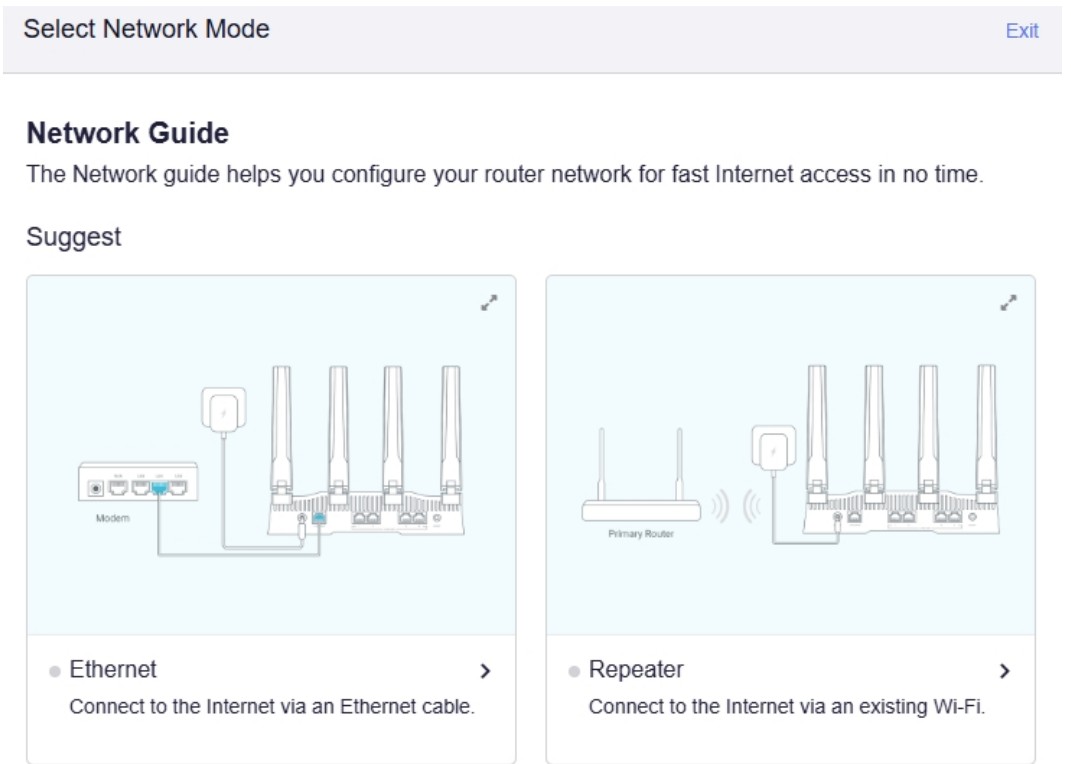
El asistente de configuración basado en web lo guiará a través de la red del enrutador configuración.

Siga los pasos a continuación para iniciar el asistente.

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



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



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

4.2 Configurar manualmente la conexión a Internet

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

Flint 3 admite cuatro métodos de conexión a Internet: Ethernet, Repetidor, Anclaje a red USB y módem USB. Celija el método apropiado según sus necesidades de uso.

1. **Ethernet (RJ45)**: 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.

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

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

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

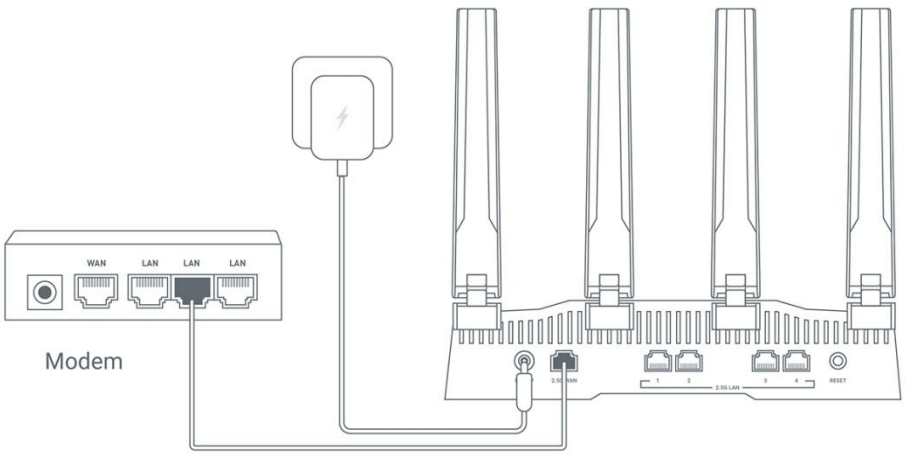
4.2.1 Conectarse a Internet mediante un cable Ethernet

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

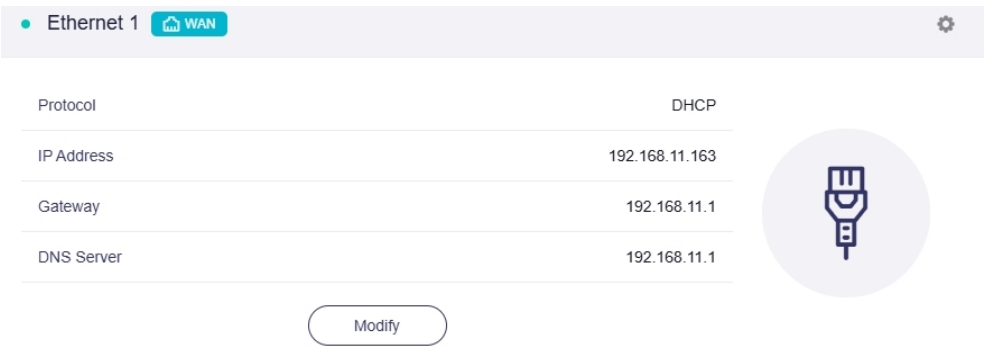
Configuración básica

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

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

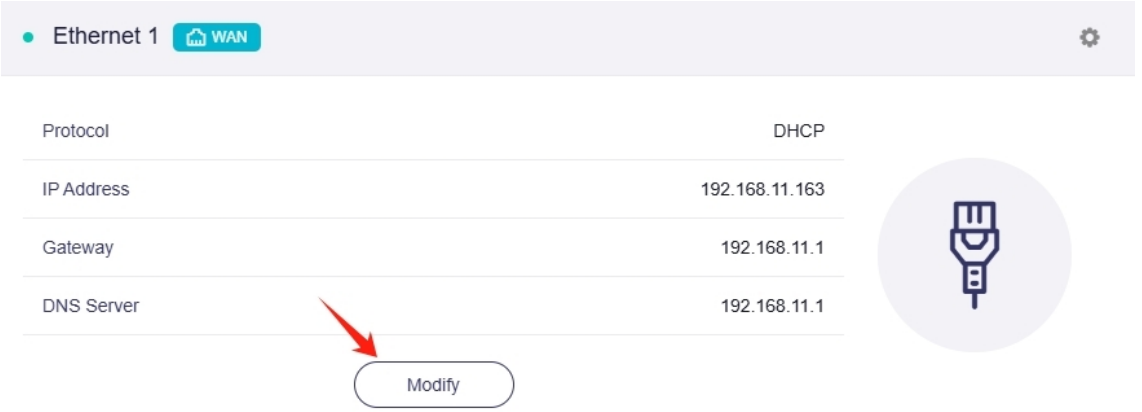


2. Inicie sesión en el panel de administración web del enrutador' y navegue a **INTERNET** > **Ethernet**. Si la conexión se realiza correctamente, la sección Ethernet muestra red detalles, incluidos protocolo, dirección IP, puerta de enlace, y DNS servidor.



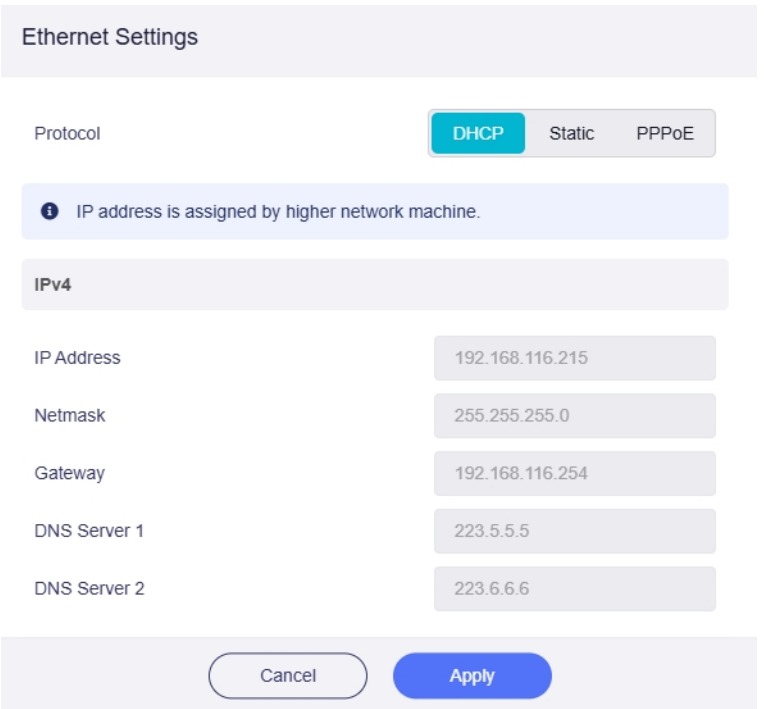
Protocolo

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



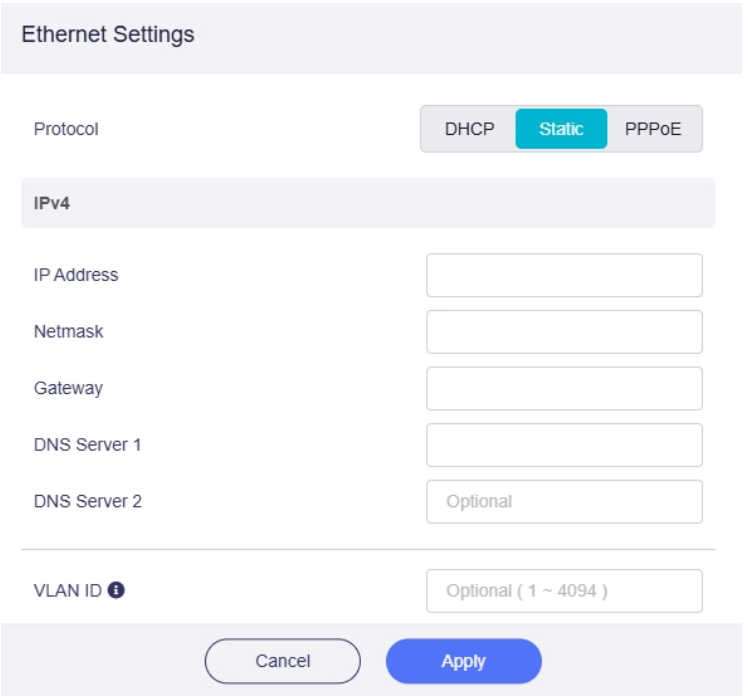
- **DHCP**

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



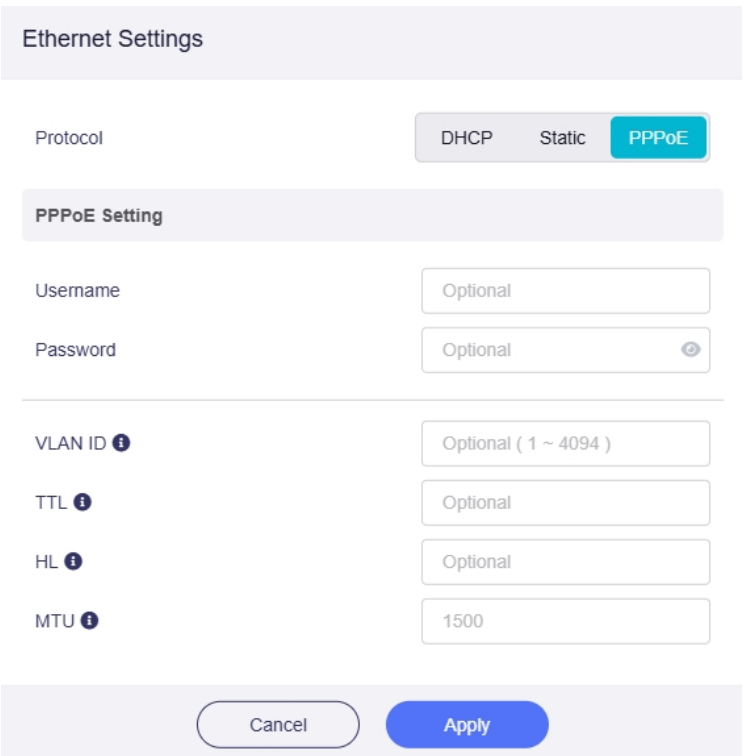
- **Estática**

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



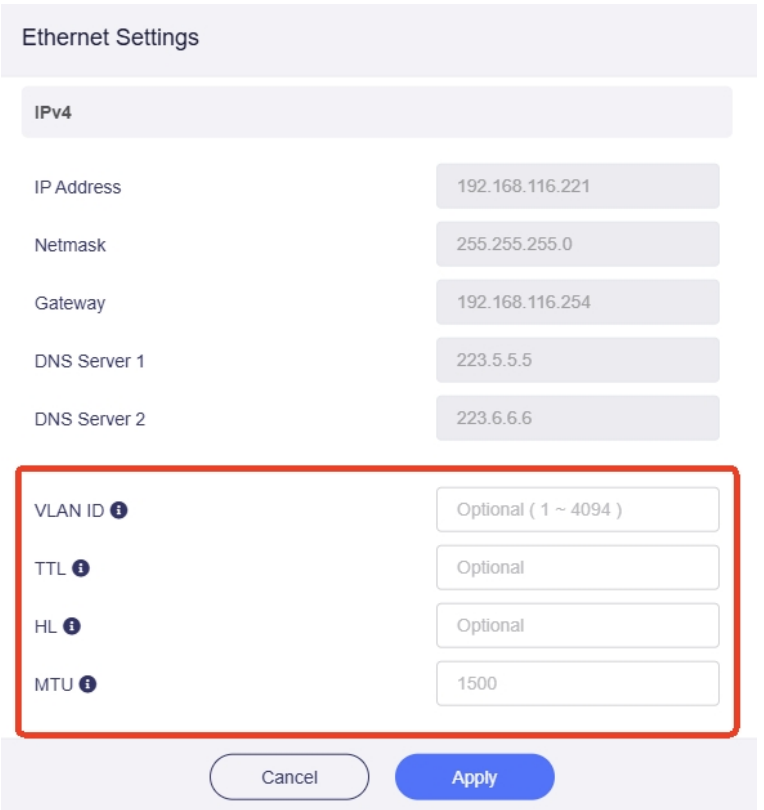
- **PPPoE**

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



Configuración avanzada

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



- **ID de VLAN**

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

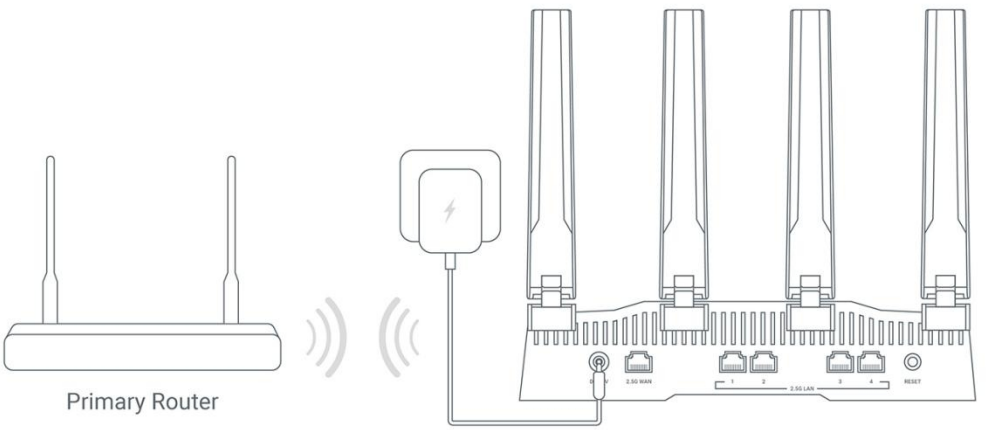
  TTL (tiempo de vida) define el tiempo máximo que los paquetes pueden sobrevivir en la red. De forma predeterminada, el enrutador disminuye el TTL de los paquetes entrantes paquetes de dispositivos cliente en 1 antes de reenviarlos. Si necesita anularlo, puede establecer un valor fijo aquí. La configuración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

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

  El valor de MTU predeterminado es 1500 bytes.

4.2.2 Conectarse a Internet mediante una red Wi-Fi existente

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

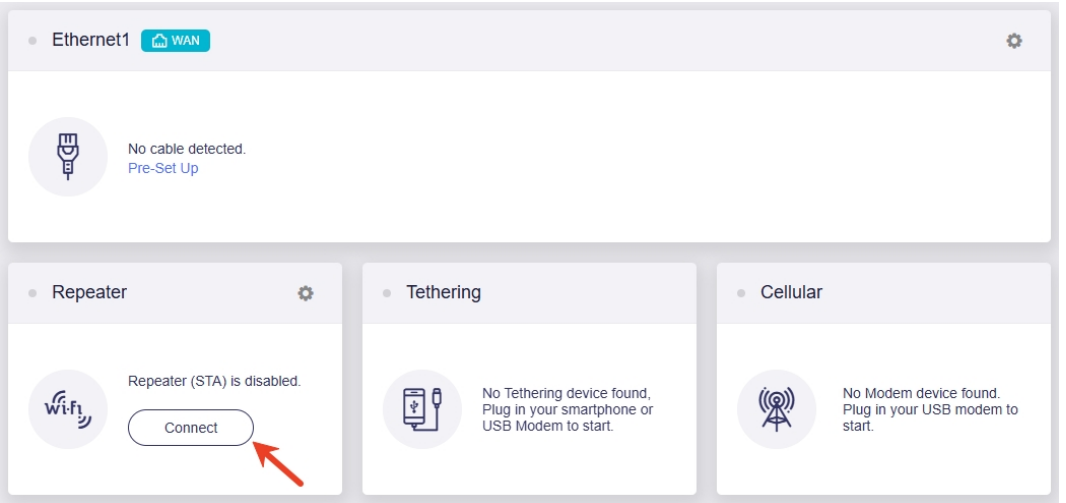


función de repetidor GL.iNet funciona en modo WISP (Proveedor de servicios de Internet inalámbrico) de forma predeterminada, lo que significa que el enrutador creará su propia subred y actuará como un firewall para protegerte de la red pública.

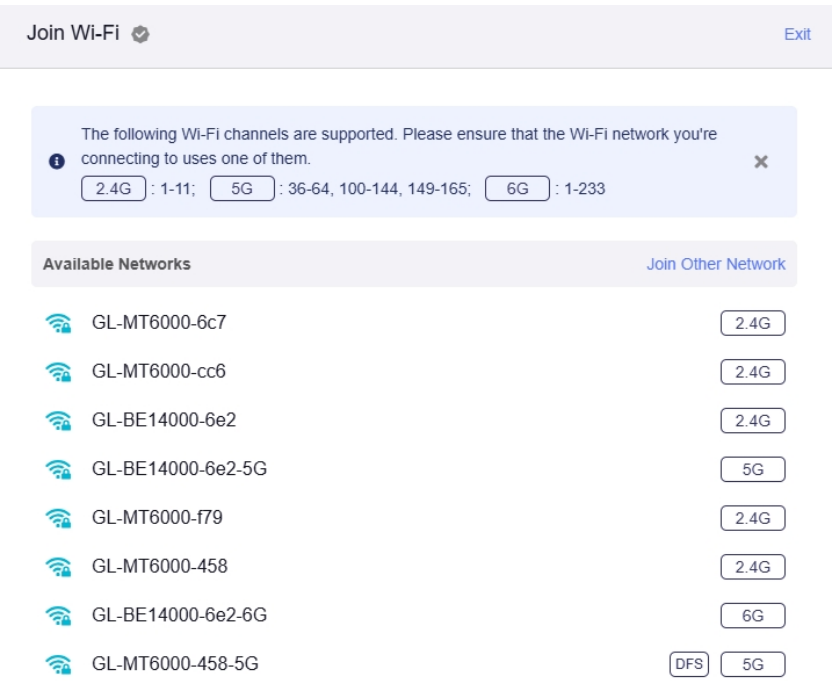
Configuración básica

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

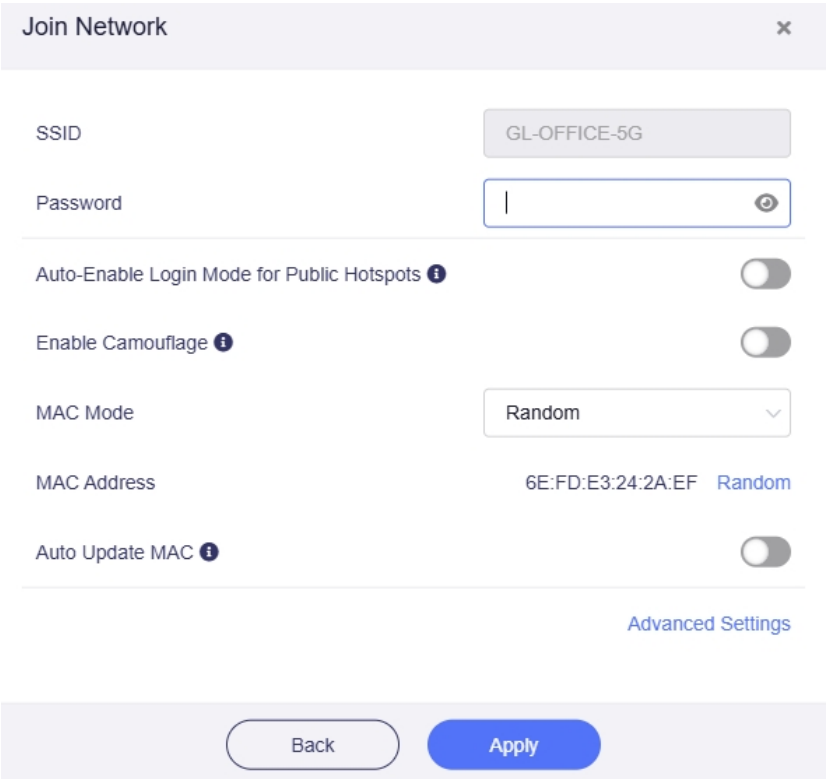
1. Inicie sesión en el administrador web del enrutador' panel, y navegue hasta **INTERNET** > **Repetidor**. Haga clic en **Conectar**.



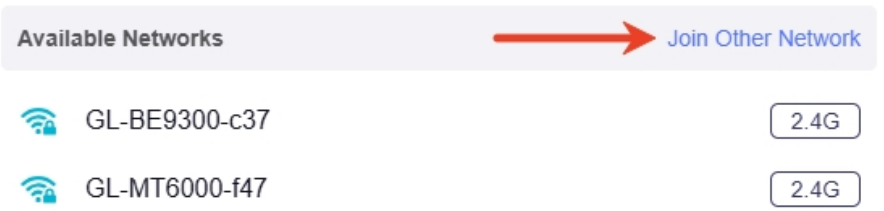
2. En la ventana emergente, elija la red Wi-Fi que desea conectarse de la lista de redes disponibles.



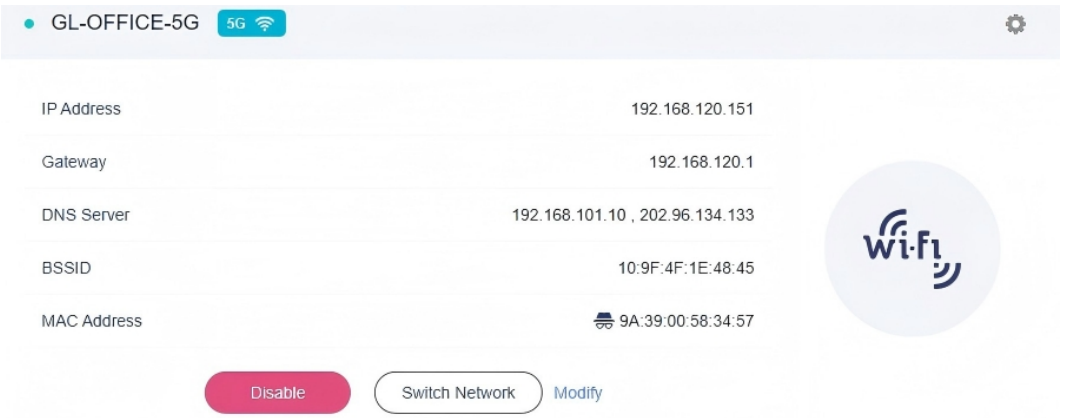
3. Eingrese la contraseña de Wi-Fi correcta y haga clic en **Aplicar**.



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

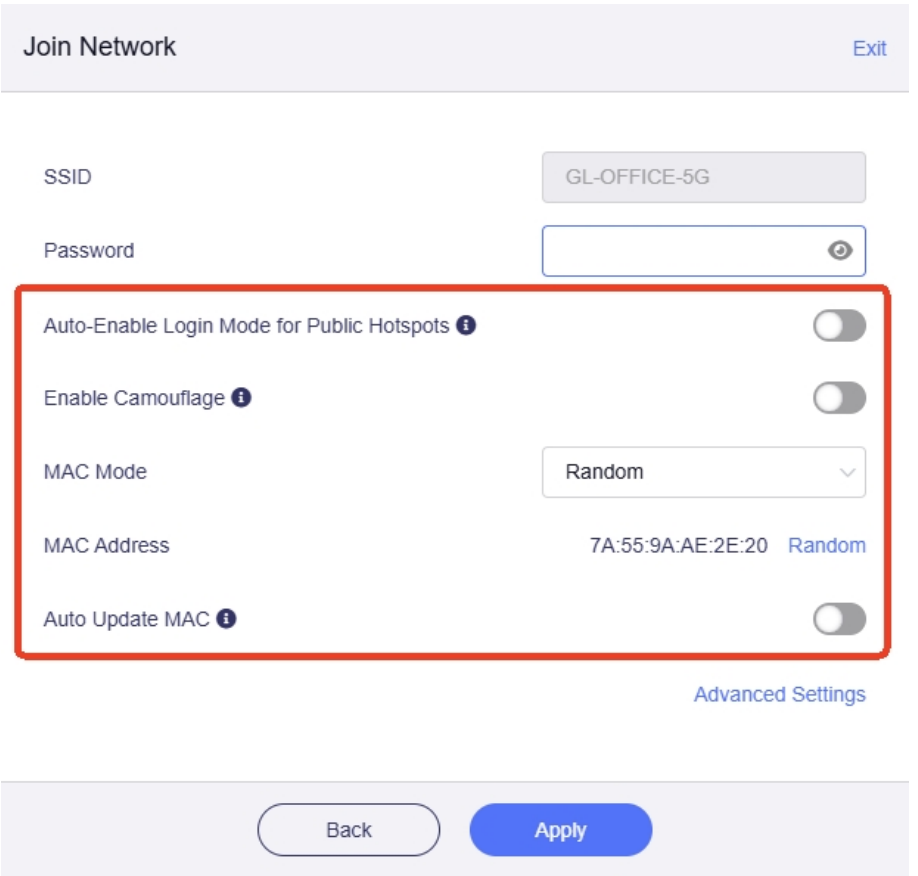


4. Espera un minuto hasta que el enrutador se conecte. Una vez conectado, la página se muestra a continuación.



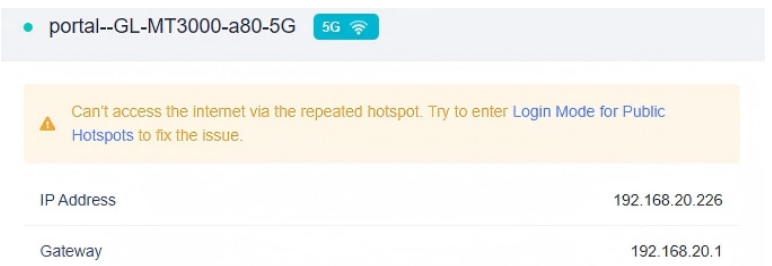
Configuración del punto de acceso público

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



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

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



- **Habilitar camuflaje**

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

  Celija qué dirección MAC utiliza el enrutador para conectarse al punto de acceso público.

  Factory: utiliza la dirección MAC original asignada de fábrica del dispositivo.

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

  Si la MAC deseada no’no aparece en la lista, ingrese manualmente la MAC dirección que desea clonar. Nota: Mcualquier dispositivos utilizan direcciones MAC aleatorias (a menudo denominadas dirección Wi-Fi privada o hardware aleatorio dirección MAC) al conectarse a redes Wi-Fi. Como resultado, es posible que la dirección MAC que se muestra aquí no coincida con la MAC física real del dispositivo’.

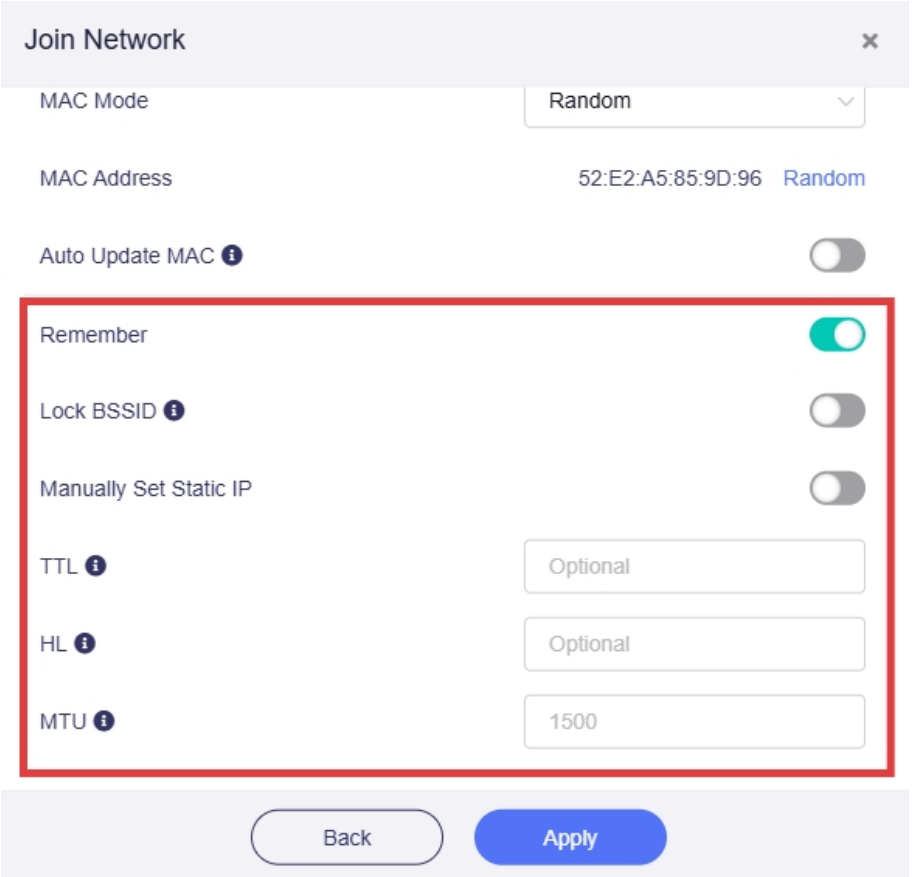
  Aleatoria: genera automáticamente una dirección MAC aleatoria para conexión.
- **Actualización automática de MAC**

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

Al guardar la configuración de red, el modo MAC, incluido cualquier clonado o MAC aleatorio dirección, estará vinculada al SSID específico que guarde. Puede cambiar manualmente esta configuración para cada SSID en cualquier momento.

Configuración avanzada

Al unirse a la red, hay algunas configuraciones avanzadas opcionales.

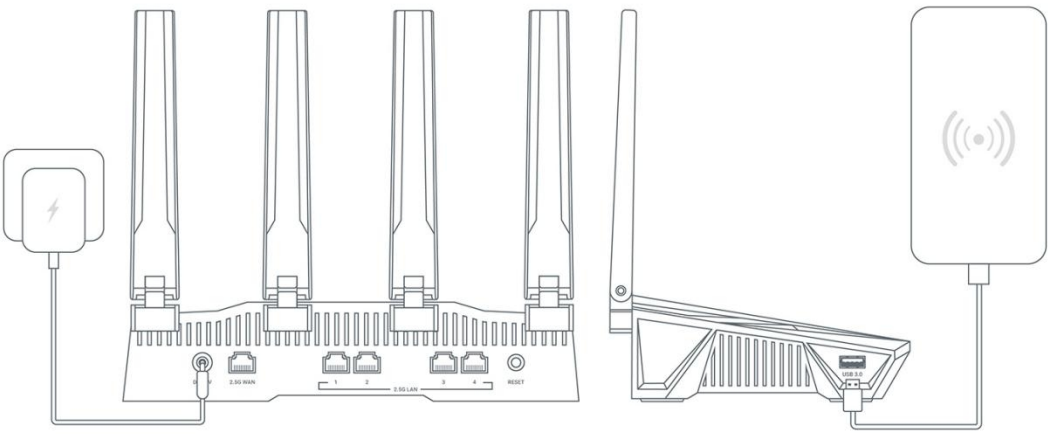


- **Recordar**: habilite esto para recordar la red Wi-Fi repetida actualmente.
- **Bloquear BSSID**: cuando esté habilitado, el enrutador se conectará solo al punto de acceso (AP) específico correspondiente al BSSID seleccionado, incluso cuando otros AP compartan el mismo SSID.
- **Configuración estática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

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

4.2.3 Conectarse a Internet mediante conexión compartida por USB

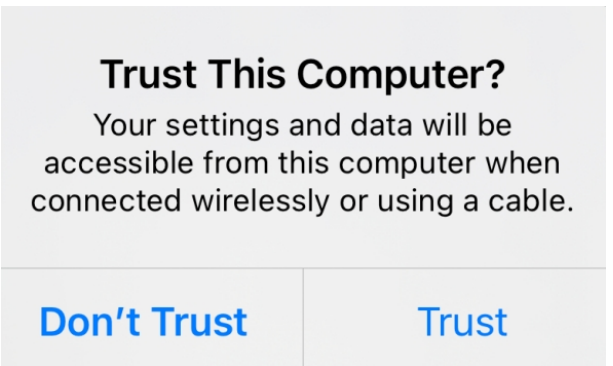
Cconecte un inteligenteteléfono al enrutador a través de un El cable USB se llama Tethering y puede compartir la red de datos móviles del dispositivo (por ejemplo, 4G/5G) con el enrutador. Este es un método para el acceso temporal ia Internet, especialmente cuando al aire libre o en áreas sin banda ancha fija .



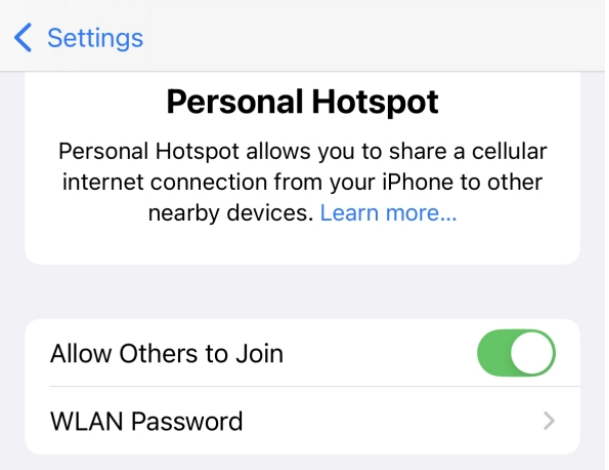
El módem sin host funciona en Tethering como bien durante la configuración del módem.
Nota: Algunos operadores de telefonía móvil limitan o cobran más por la conexión. Recomendamos consultar con su operador.

Conexión compartida desde un iPhone

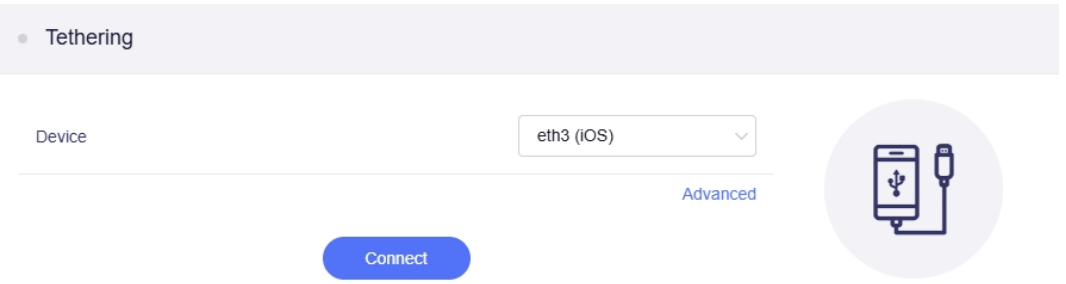
1. Conecte un iPhone al puerto USB del enrutador mediante un cable USB. Aparecerá un cuadro de diálogo del sistema preguntando si se debe confiar en el dispositivo. Toque **Confiar** para continuar.



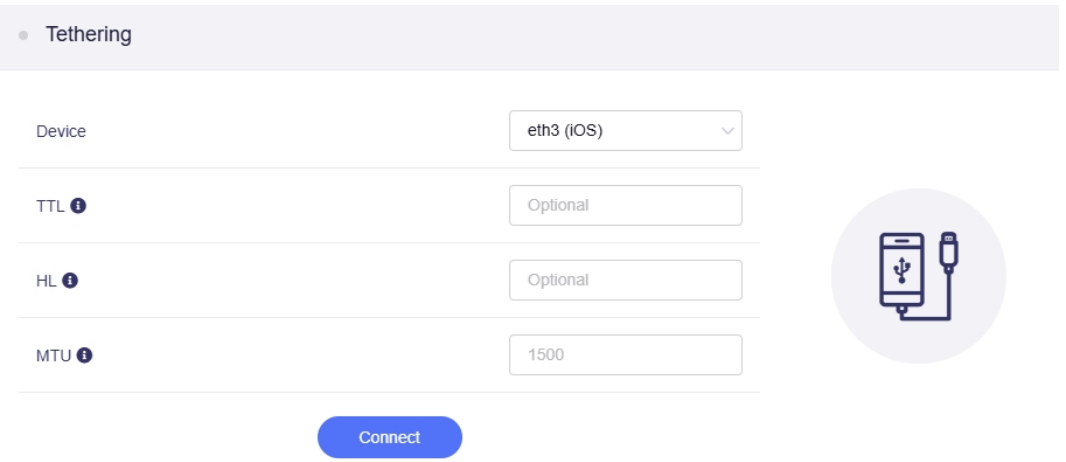
2. Ir a iPhone **Configuración** > **Punto de acceso personal**. Activar **Permitir que otros se unan**.



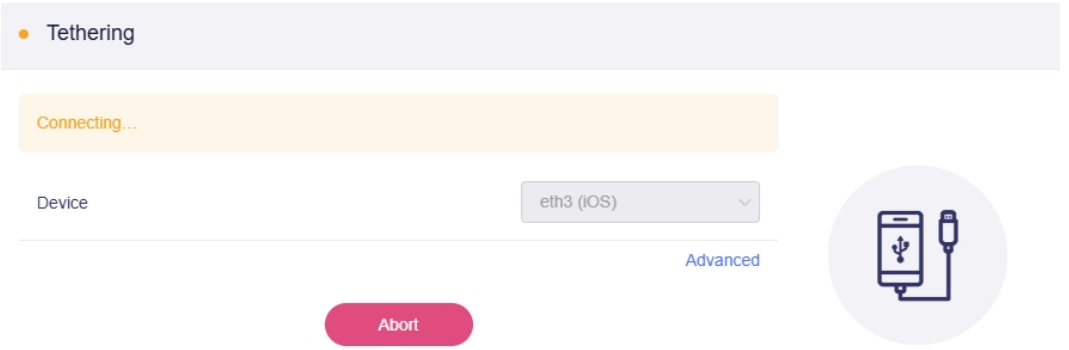
3. Conecte una computadora u otro teléfono al enrutador. Inicie sesión en el panel de administración web del enrutador y navegue hasta **INTERNET** > **Conexión**, luego haga clic en **Conectar**.



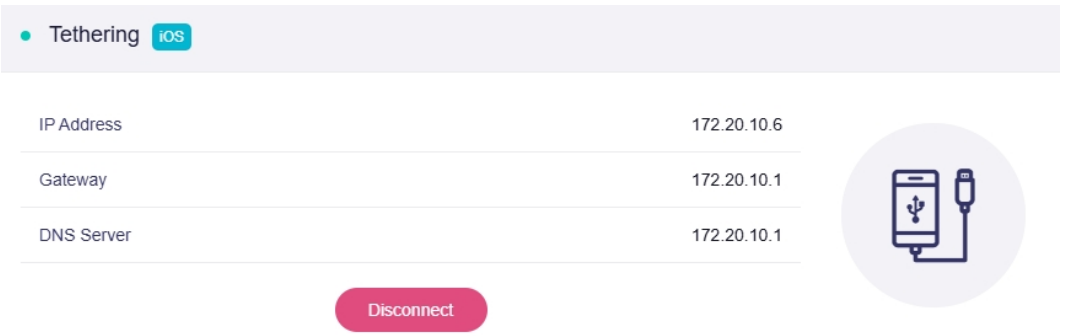
Si necesita establecer configuraciones avanzadas, como TTL, HL y MTU, haga clic **Avanzado** para personalizar estas configuraciones antes de hacer clicing **Conectar**.



4. Comenzará a conectarse.

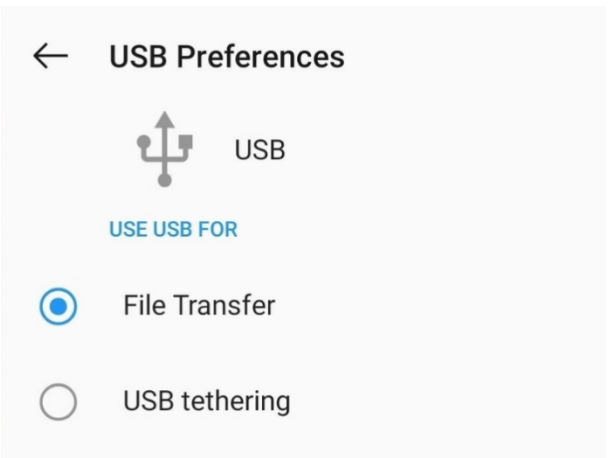


Una vez conectado, thes la página mostrará la conexión Tethering detalles.

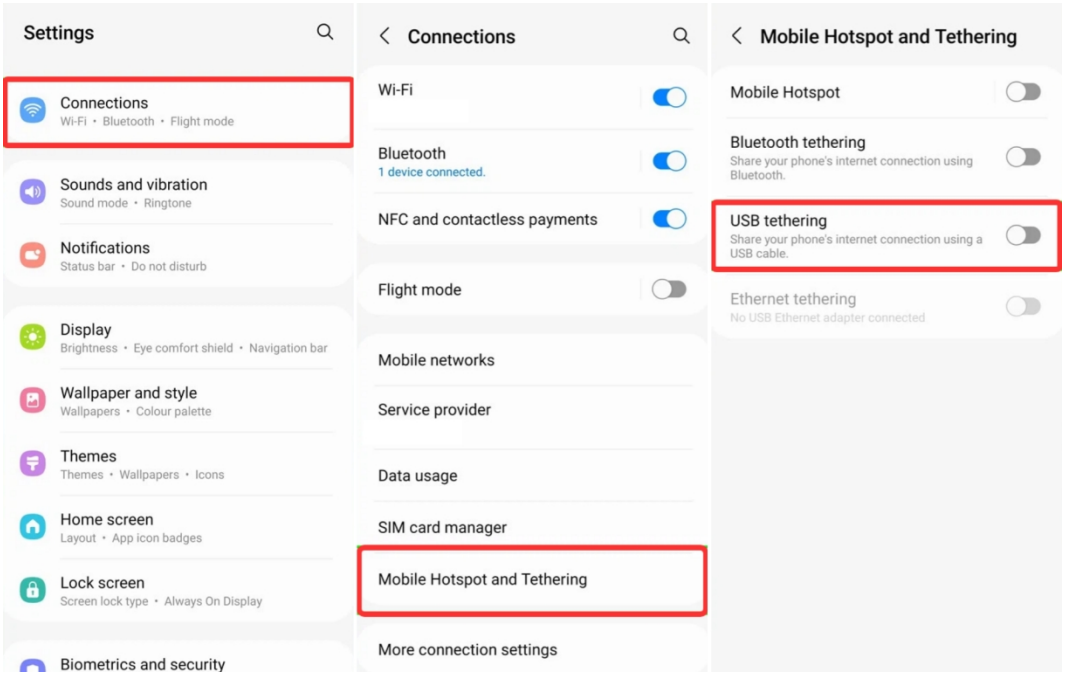


Conexión compartida desde Android

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

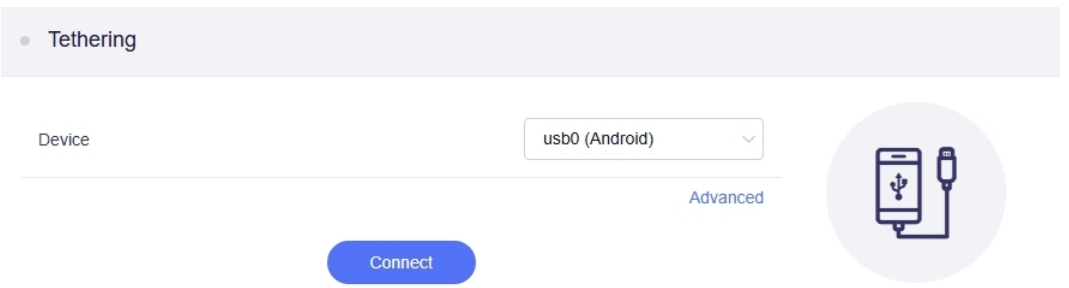


2. Vaya a la **Configuración** > **Red e Internet** > **Punto de acceso personal**. Activar **Personal Punto de acceso** o **Anclaje a red USB**.

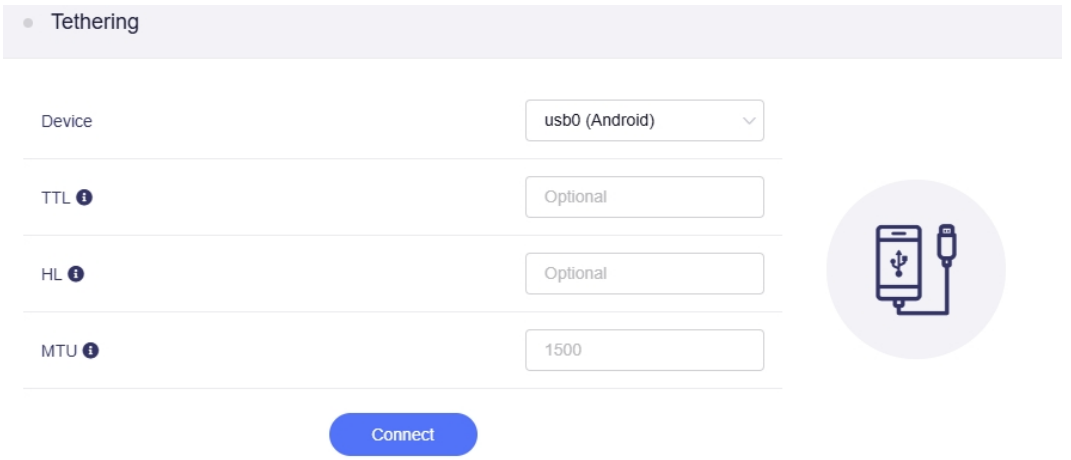


(Los pasos para habilitar la conexión USB varían según la marca. Verifique la configuración de su dispositivo para conocer la ubicación exacta y comuníquese con el soporte técnico del fabricante si es necesario).

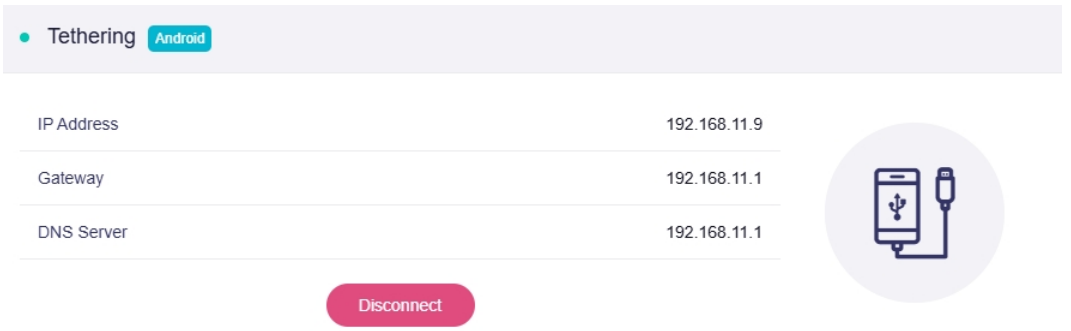
3. Conecte una computadora u otro teléfono al enrutador, luego inicie sesión en el panel de administración web del enrutador, navegar a **INTERNET** > **Anclaje a red**. Click **Conectar**.



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



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



Solución de problemas

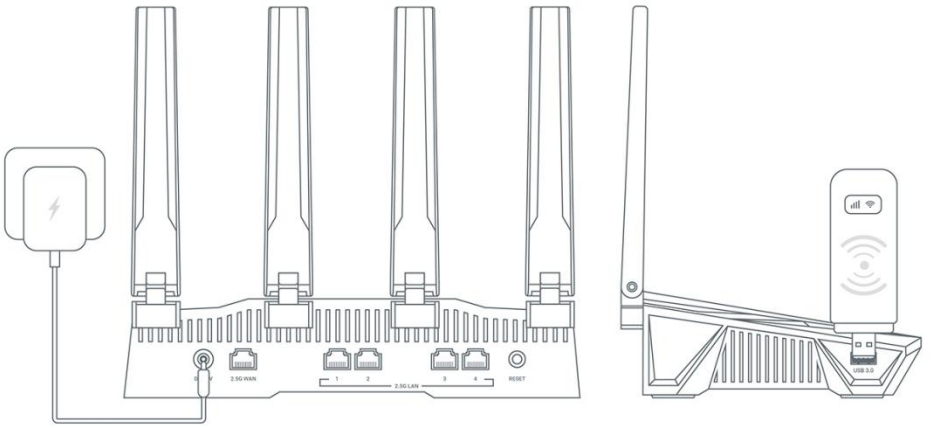
Si Anclaje a red la conexión falla, intente estos pasos para solucionar el problema:

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

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

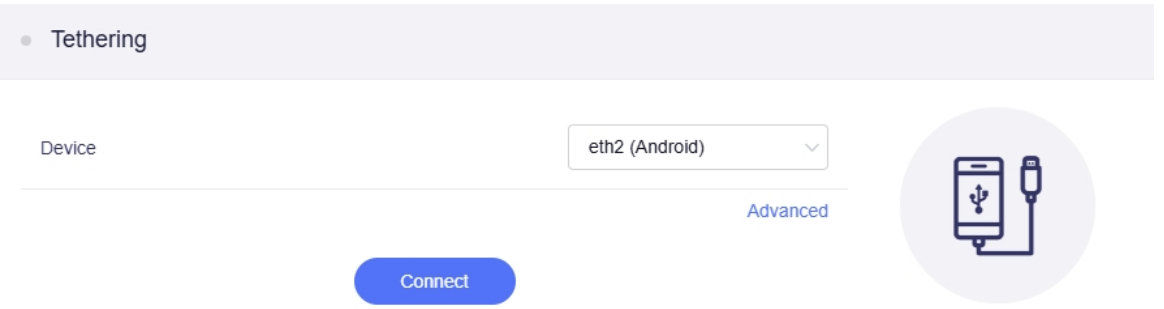
4.2.4 Conectarse a Internet mediante un módem USB

Conecte el enrutador a Internet insertando un módem USB con capacidad celular en su puerto USB. Esto permite que el enrutador se conecte a Internet a través de redes 4G/5G, brindando conectividad sin depender de la banda ancha de línea fija. Es adecuado para uso en vehículos o actividades al aire libre. Tenga en cuenta que esta conexión se implementa a través de la interfaz Tethering o Cellular del enrutador. ’s Interfaz de anclaje a red o celular.

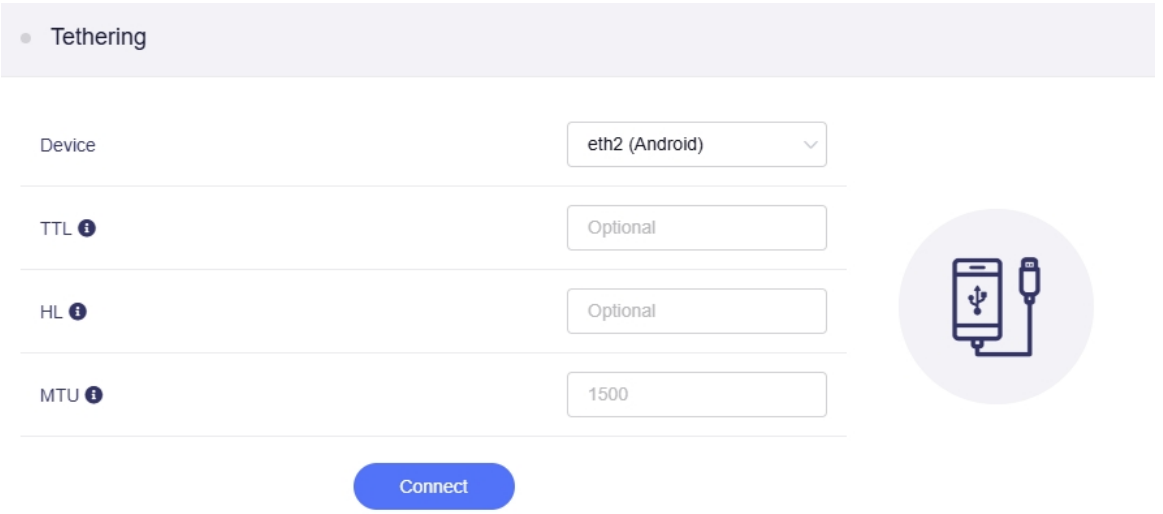


Siga los pasos a continuación para conectar su enrutador a Internet a través de un módem USB.

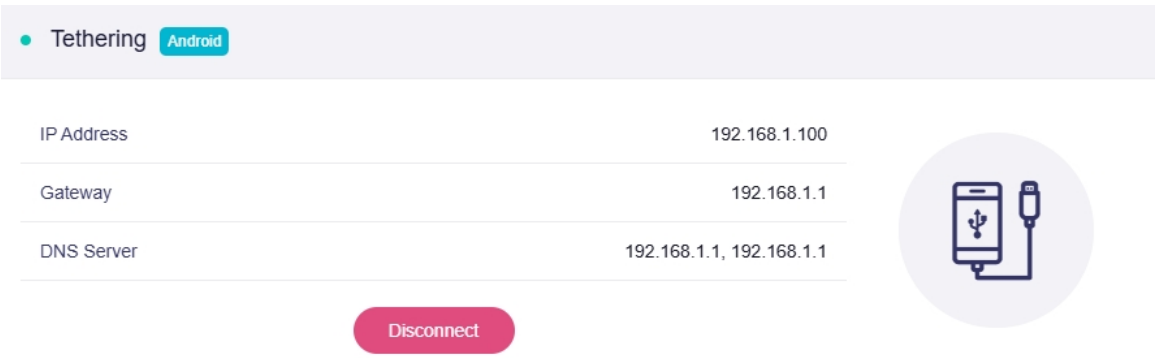
1. Plug un módem USB con una tarjeta SIM preinstalada en el puerto USB del enrutador’ antes de encenderlo.
2. Inicie sesión en el enrutador’s web admin panel, navegue hasta **INTERNET** > **Conexión** y luego haga clic en **Conectar**.



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

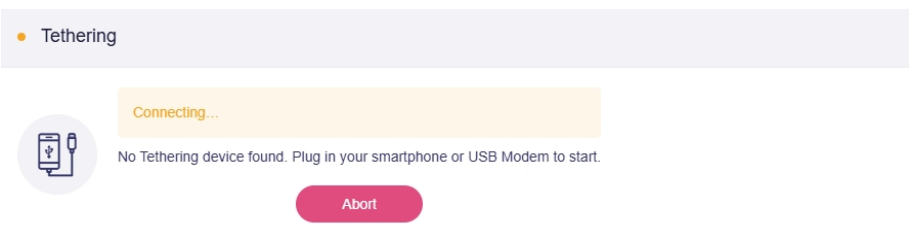


3. Comenzará a conectarse. Una vez conectado, esta página mostrará los red detalles.



Consejos:

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



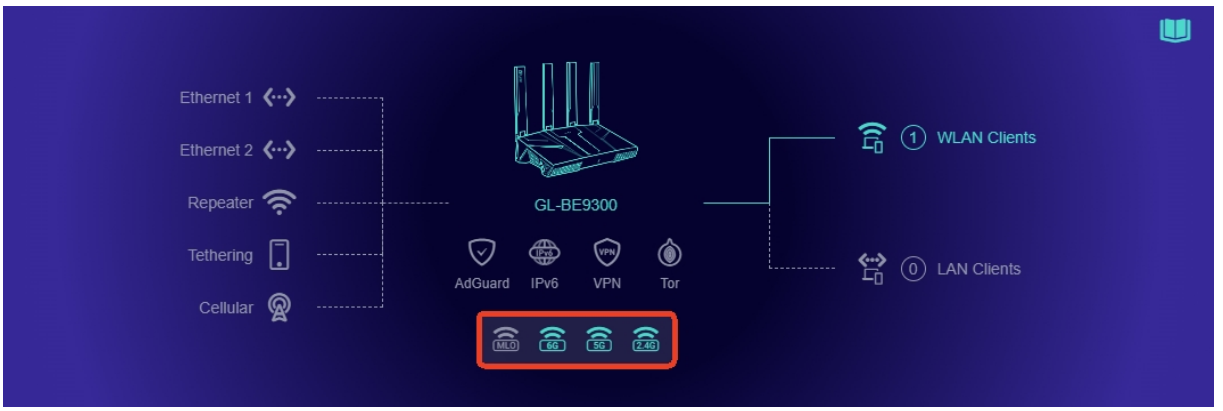
Capítulo 5

Red inalámbrica

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

5.1 Visualización del estado de Wi-Fi

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



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



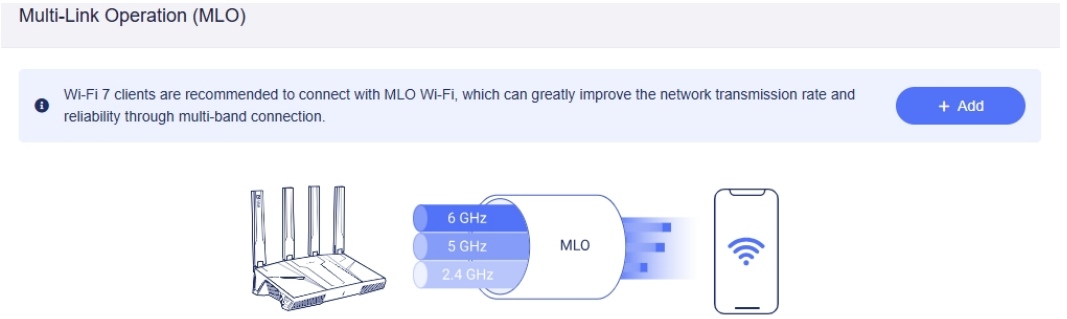
5.2 Configuración inalámbrica

Inicie sesión en el panel de administración web del enrutador y navegue hasta **Inalámbrica**. La página Inalámbrica te permite configurar varias conexiones Wi-Fi. redes, incluyendo MLO Wi-Fi (disponible en modelos seleccionados), red principal, red de invitados y red IoT. Las bandas de Wi-Fi admitidas varían según el modelo.

5.2.1 Wi-Fi MLO

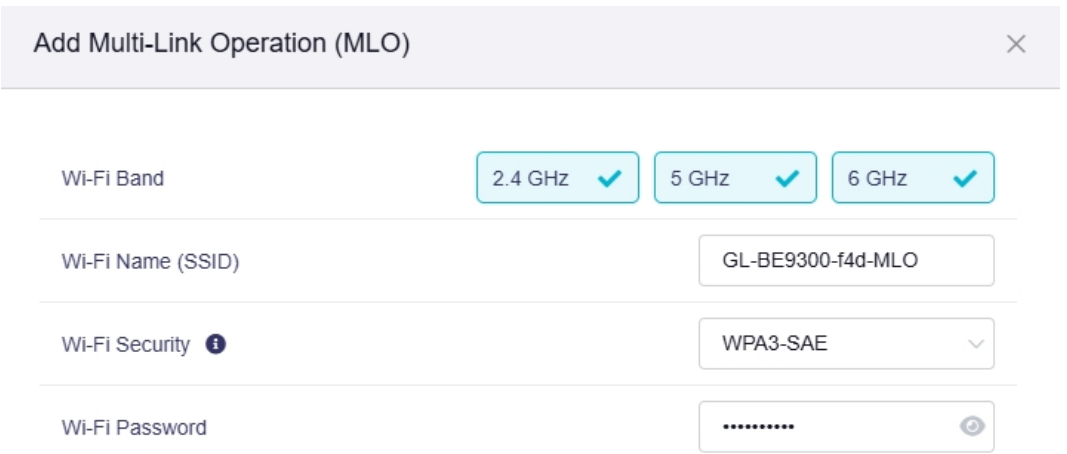
MLO (operación de enlace múltiple) es una de las características principales de Wi-Fi 7 (802.11be), diseñada para mejorar el rendimiento de la red, reducir significativamente la latencia y mejorar la estabilidad de la conexión mediante el uso de múltiples frecuencias. bandas simultáneamente como 2,4 GHz, 5 GHz y 6 GHz.

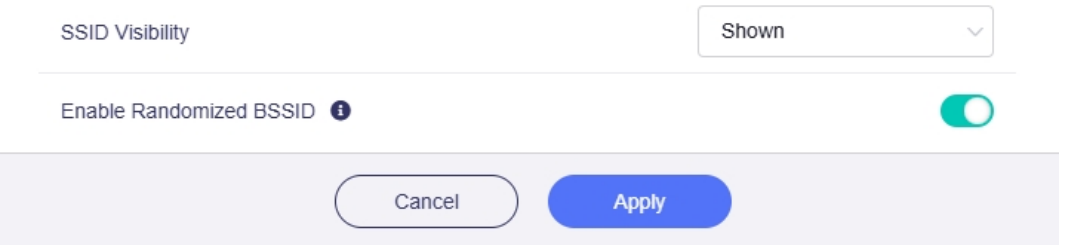
Para crear una red Wi-Fi MLO, haga clic en el botón **Agregar** a la derecha.



Seleccione al menos dos bandas de Wi-Fi, configure los detalles de Wi-Fi y luego haga clic **Aplicar**.

Nota: Laslas bandas Wi-Fi disponibles varían según el modelo.





- **Banda Wi-Fi**: seleccione al menos dos bandas de radio. TLas bandas de Wi-Fi disponibles varían según el modelo.
- **Seguridad de Wi-Fi**: Establezca el modo de seguridad de Wi-Fi en ABIERTO, WPA2-PSK, WPA/WPA2-PSK, WPA3-SAE, o WPA2-PSK/WPA3-SAE.
- **Habilitar BSSID aleatorio**: está habilitado de forma predeterminada. Ayuda a evitar que el enrutador sea rastreado a través de un BSSID fijo, ya que los dispositivos cliente pueden informar BSSID cercanos y sus propios datos de ubicación a los proveedores de sistemas operativos/dispositivos, quienes los utilizan para crear una base de datos de BSSID a ubicación. Cuando está habilitado, el enrutador utiliza un BSSID generado aleatoriamente y lo renueva en cada reinicio, por lo que el BSSID no se puede vincular a una ubicación fija.

Una vez habilitado, la página aparece como se muestra a continuación.

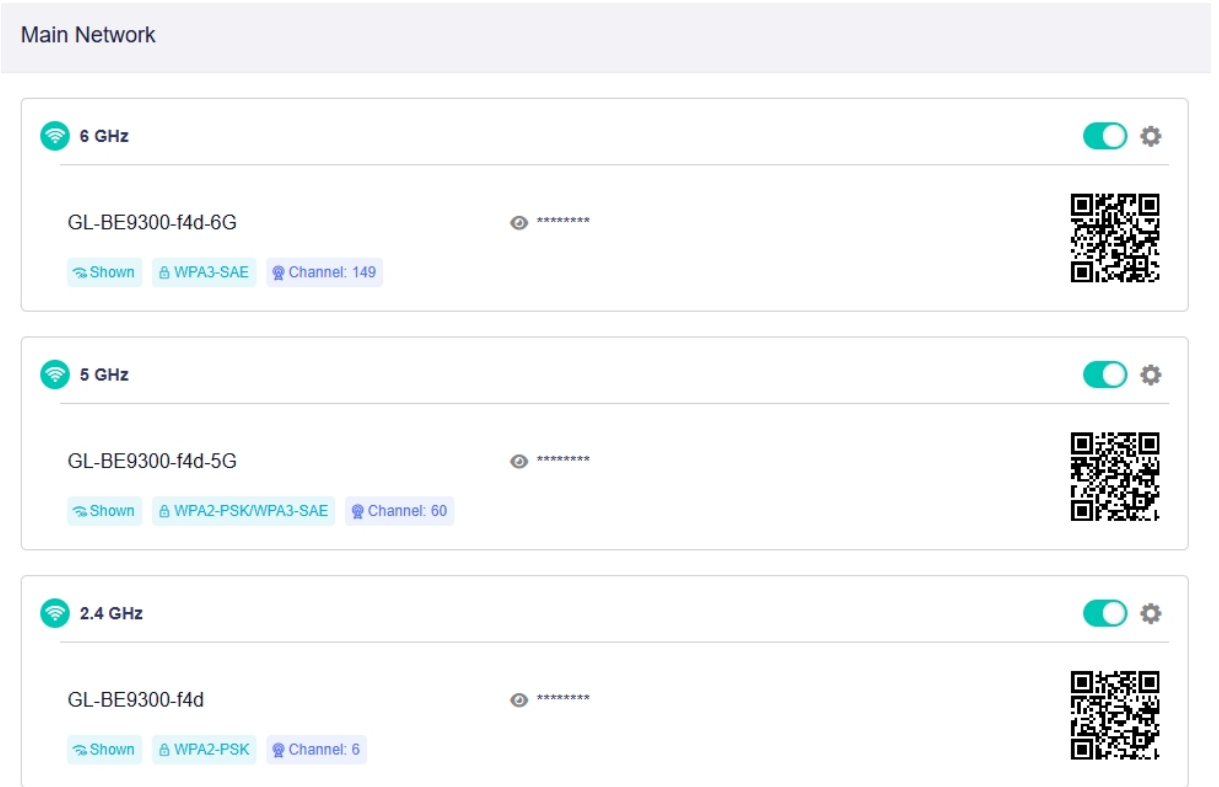


5.2.2 Red principal

La red principal es su red Wi-Fi principal y admite conexión simultánea transmisiones en diferentes bandas de radio, todas habilitadas de forma predeterminada.

Haga clic en el ícono de ajustes a la derecha para ver o modificar la configuración de Wi-Fi para cada banda, como SSID de Wi-Fi, seguridad, contraseña, BSSID aleatorio, potencia de TX, ancho de banda y Wi-Fi canal.

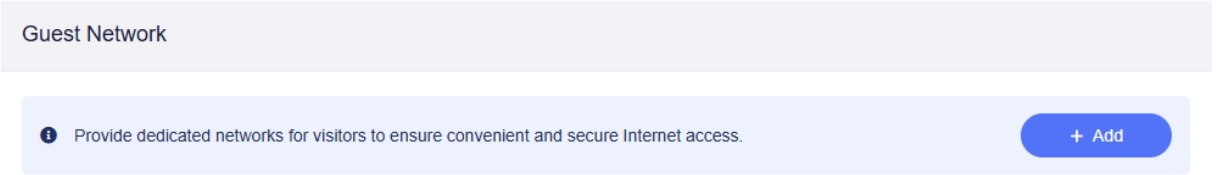
Nota: Las bandas Wi-Fi disponibles varían según el modelo.Las bandas de Wi-Fi disponibles varían según el modelo.



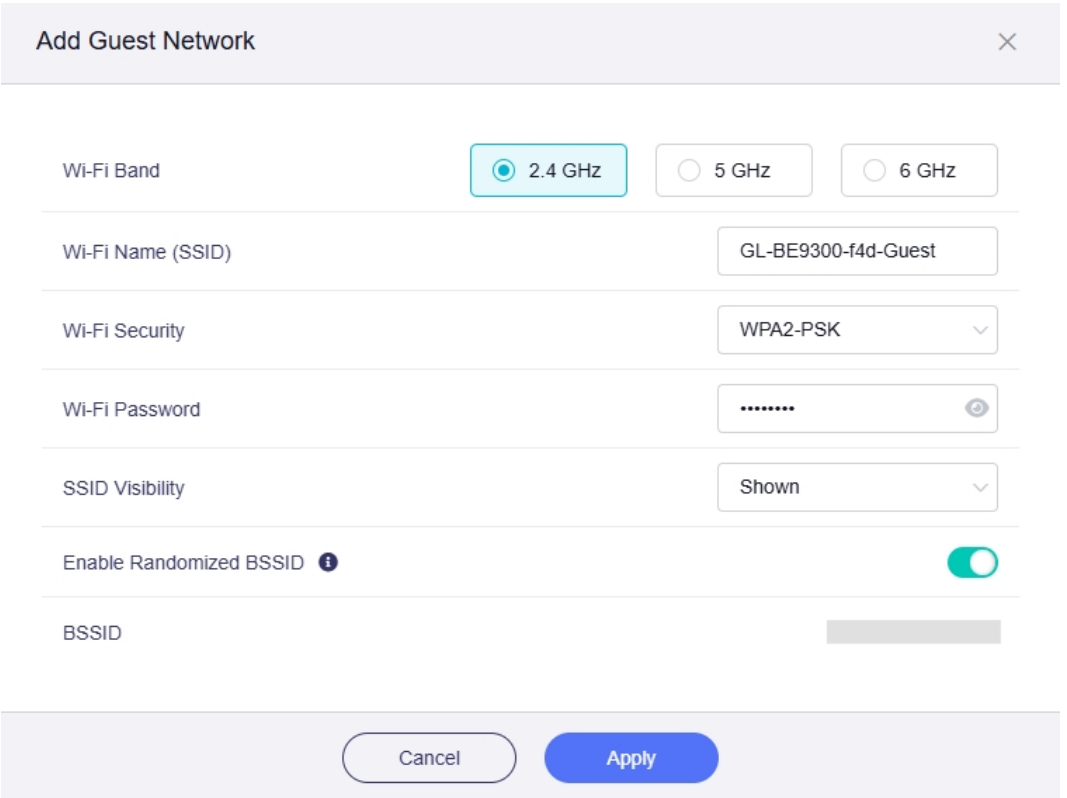
5.2.3 Red de invitados

La Red para invitados es una red Wi-Fi dedicada para visitantes, con todas las bandas desactivadas de forma predeterminada. Puede habilitar y configurar ajustes de red básicos para cada banda, como el SSID de Wi-Fi, el modo de seguridad, la contraseña y habilitar BSSID aleatorio.

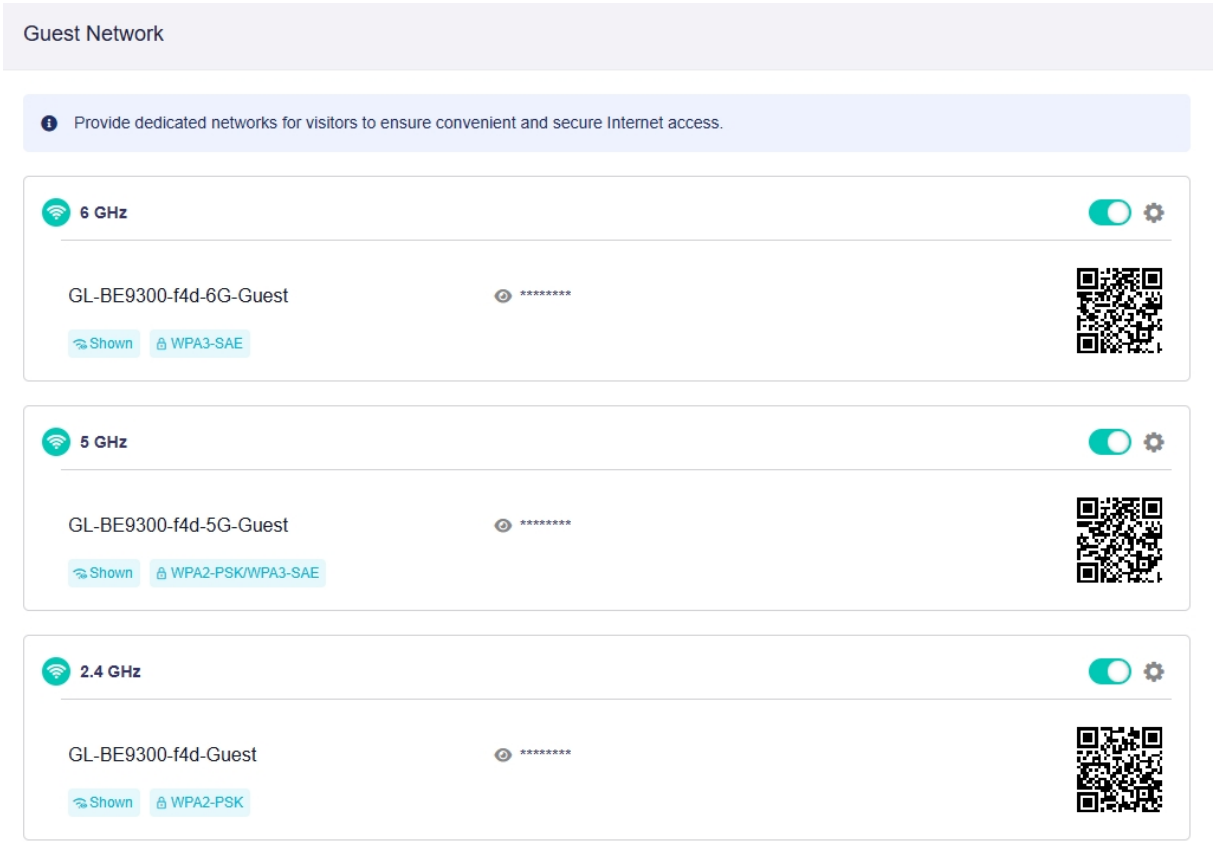
To crear una red Wi-Fi para invitados, haga clic en el botón **Agregar** a la derecha.



Seleccione una banda de Wi-Fi, configure los detalles de Wi-Fi y luego haga clic en **Aplicar**.
Nota: Las bandas Wi-Fi disponibles varían según el modelo.Las bandas de Wi-Fi disponibles varían según el modelo.



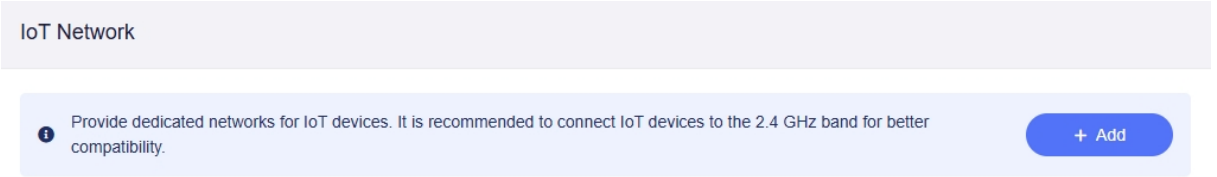
Una vez habilitada, la página aparece como se muestra a continuación.


Guest Network
Provide dedicated networks for visitors to ensure convenient and secure Internet access.
6 GHz
GL-BE9300-f4d-6G-Guest
****
Shown
WPA3-SAE
5 GHz
GL-BE9300-f4d-5G-Guest
****
Shown
WPA2-PSK/WPA3-SAE
2.4 GHz
GL-BE9300-f4d-Guest
****
Shown
WPA2-PSK

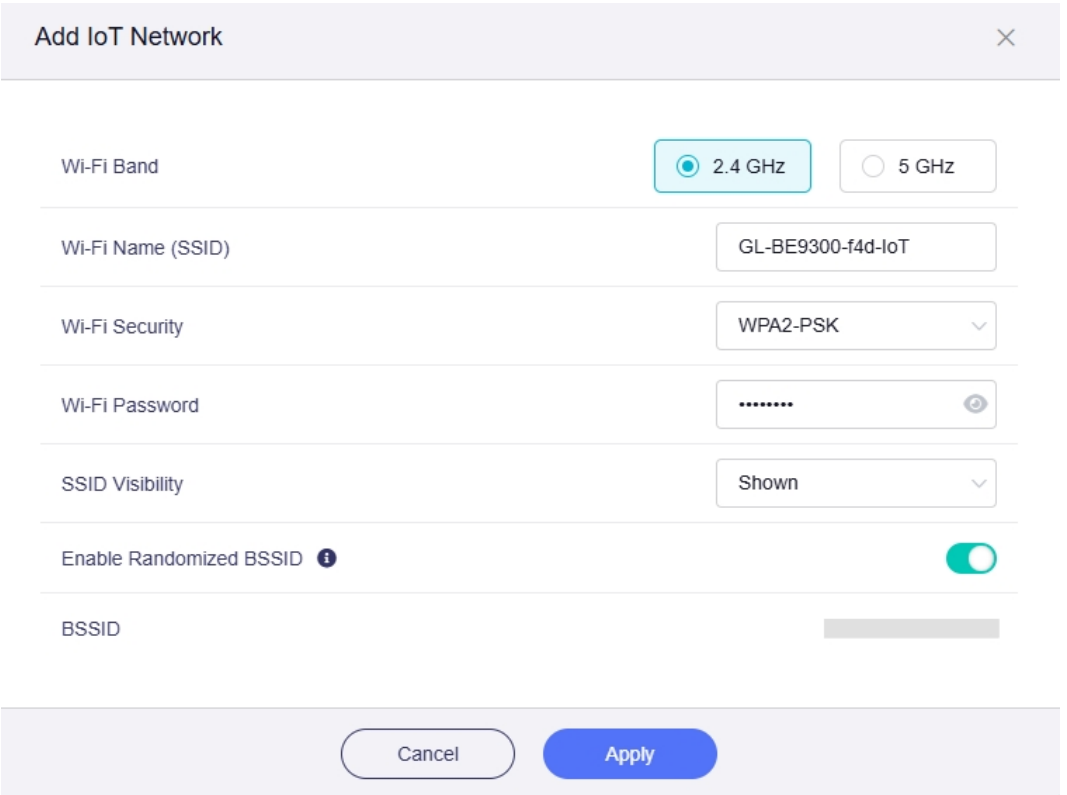
5.2.4 Red de IoT

La red IoT es una red Wi-Fi dedicada para dispositivos inteligentes, con todas las bandas desactivadas de forma predeterminada. Puede habilitar y configurar ajustes de red básicos para cada banda, como el SSID de Wi-Fi, el modo de seguridad, la contraseña y habilitar BSSID aleatorio.

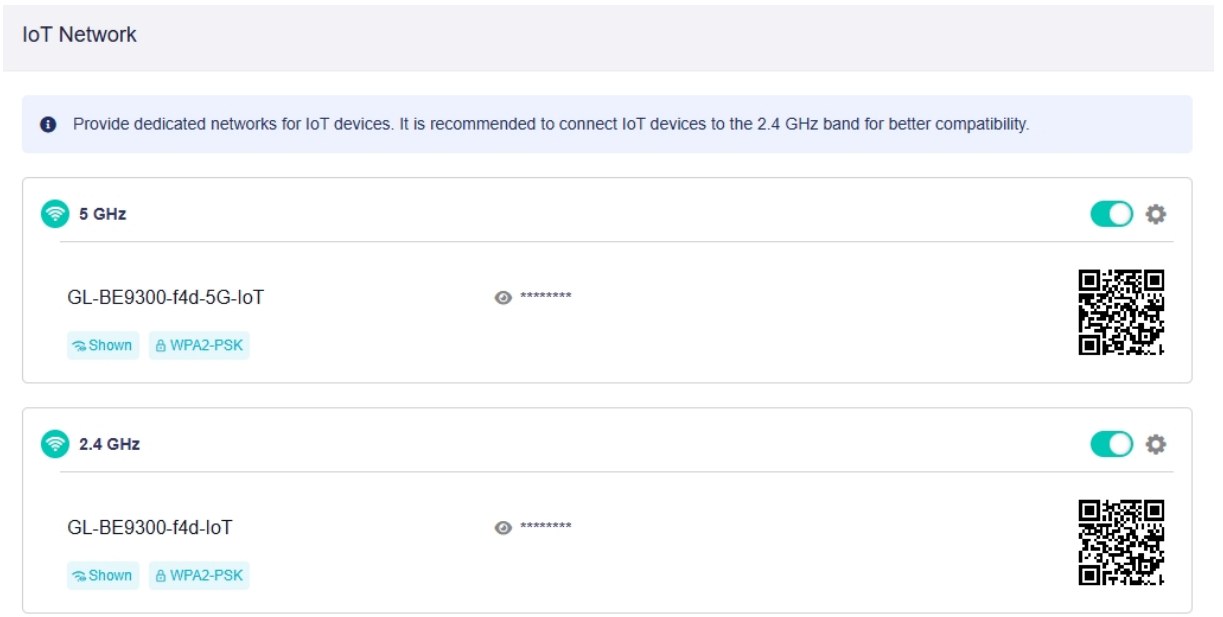
To crea an IoT red Wi-Fi, haga clic en **Agregar** a la derecha.



Seleccione una banda Wi-Fi, configure los detalles de Wi-Fi y luego haga clic en **Aplicar**.
Nota: La red IoT no incluye la banda de 6 GHz ni la disponible Las bandas de Wi-Fi varían según el modelo.



Una vez habilitada, la página aparece como se muestra a continuación.


IoT Network
Provide dedicated networks for IoT devices. It is recommended to connect IoT devices to the 2.4 GHz band for better compatibility.
5 GHz
GL-BE9300-f4d-5G-IoT
****
Shown
WPA2-PSK
2.4 GHz
GL-BE9300-f4d-IoT
****
Shown
WPA2-PSK

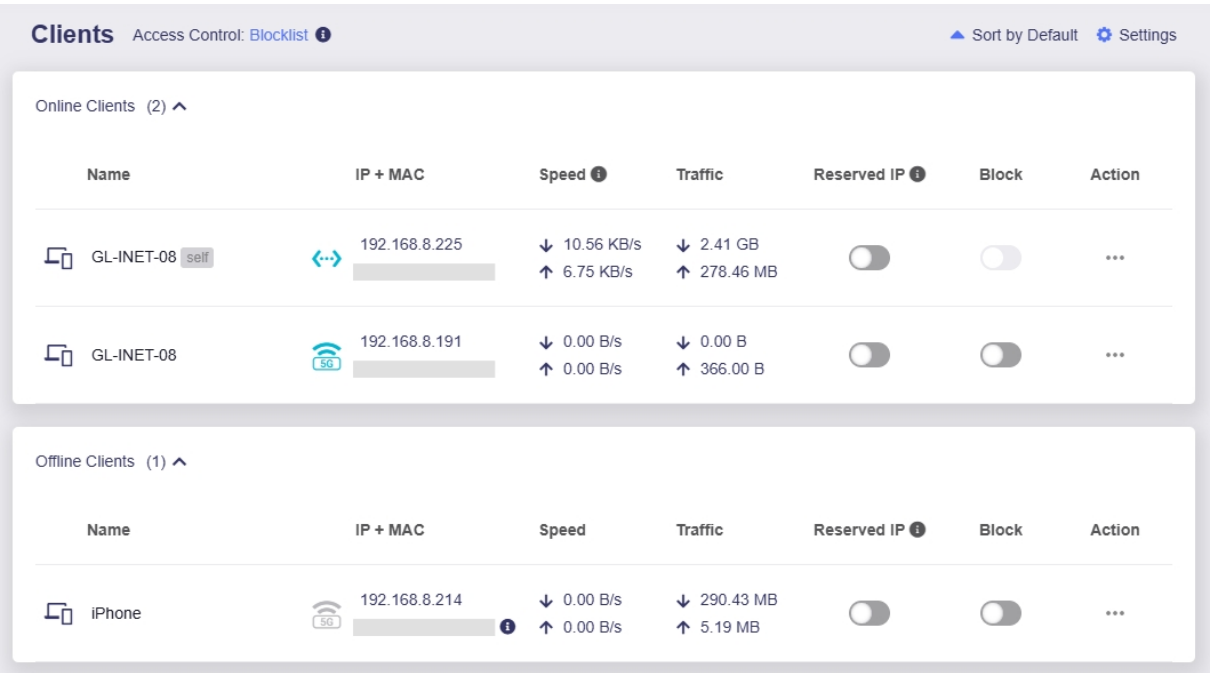
Capítulo 6

Clientes

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

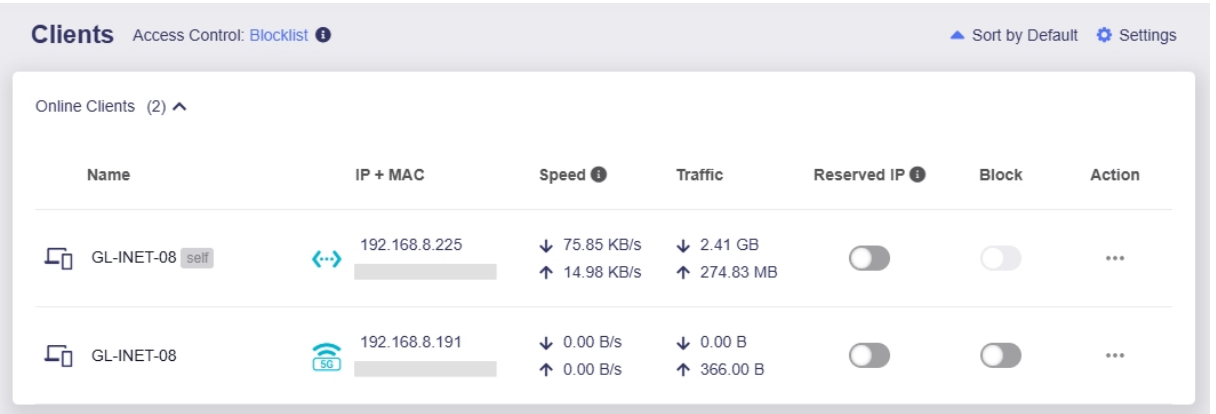
Inicie sesión en el enrutador’s web admin panel y navegue hasta **CLIENTES**.

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



- **Clientes en línea**: Se refiere a los dispositivos actualmente conectados a la red del enrutador.
- **Clientes sin conexión**: Se refiere a los 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 router 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 se trata de un Dirección MAC aleatoria.



   Yosi 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 los 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 en solo 10 segundos de datos).

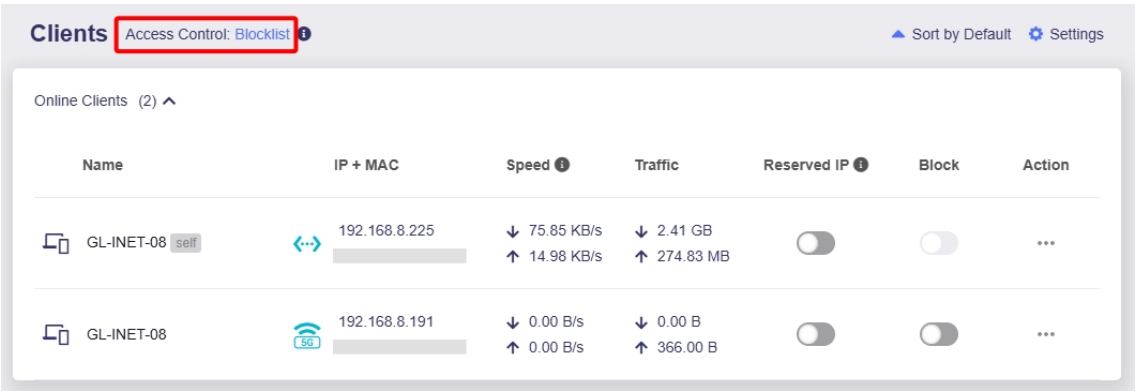
4. **Tráfico**: La cuarta columna muestra el tráfico de Internet del dispositivo conectado.

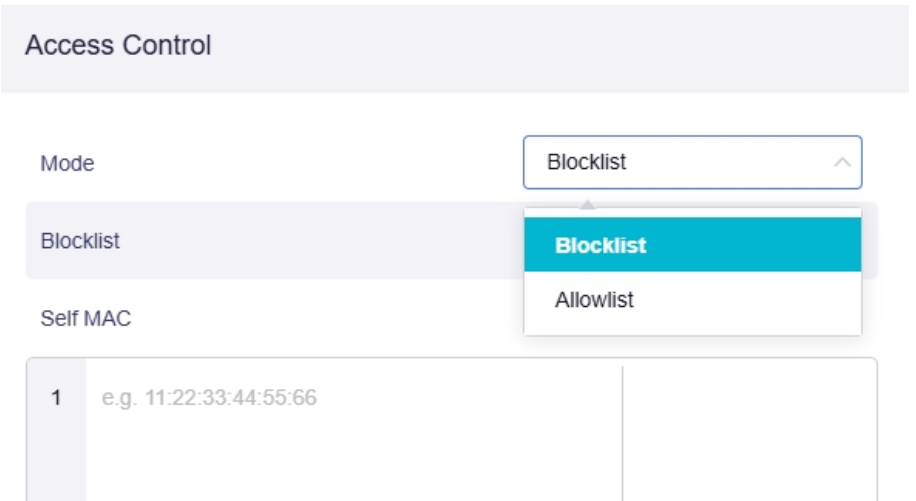
5. **Reservar IP**

En la quinta columna, puede reservar la dirección IP para dispositivo conectado con un clic. Cuando esté habilitado,, recibir siempre la misma dirección IP cada vez que se conecta al enrutador.

6. **Lista de bloqueo**

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



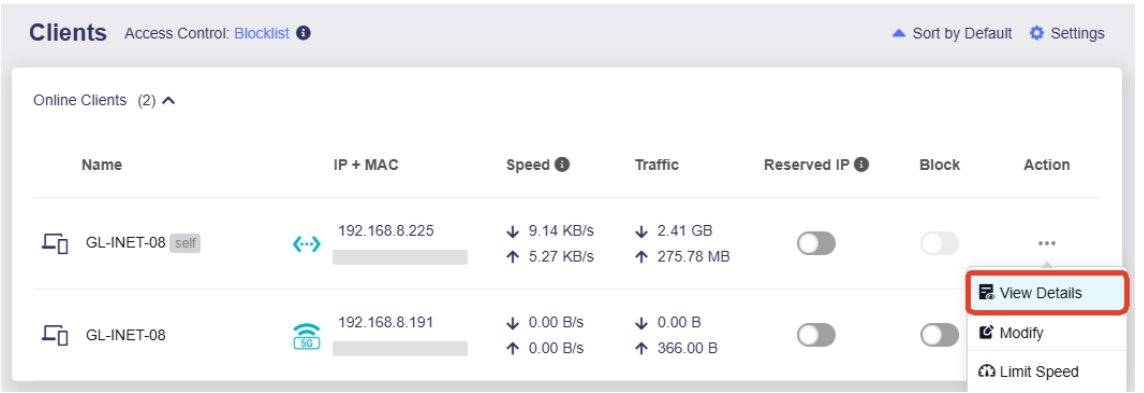


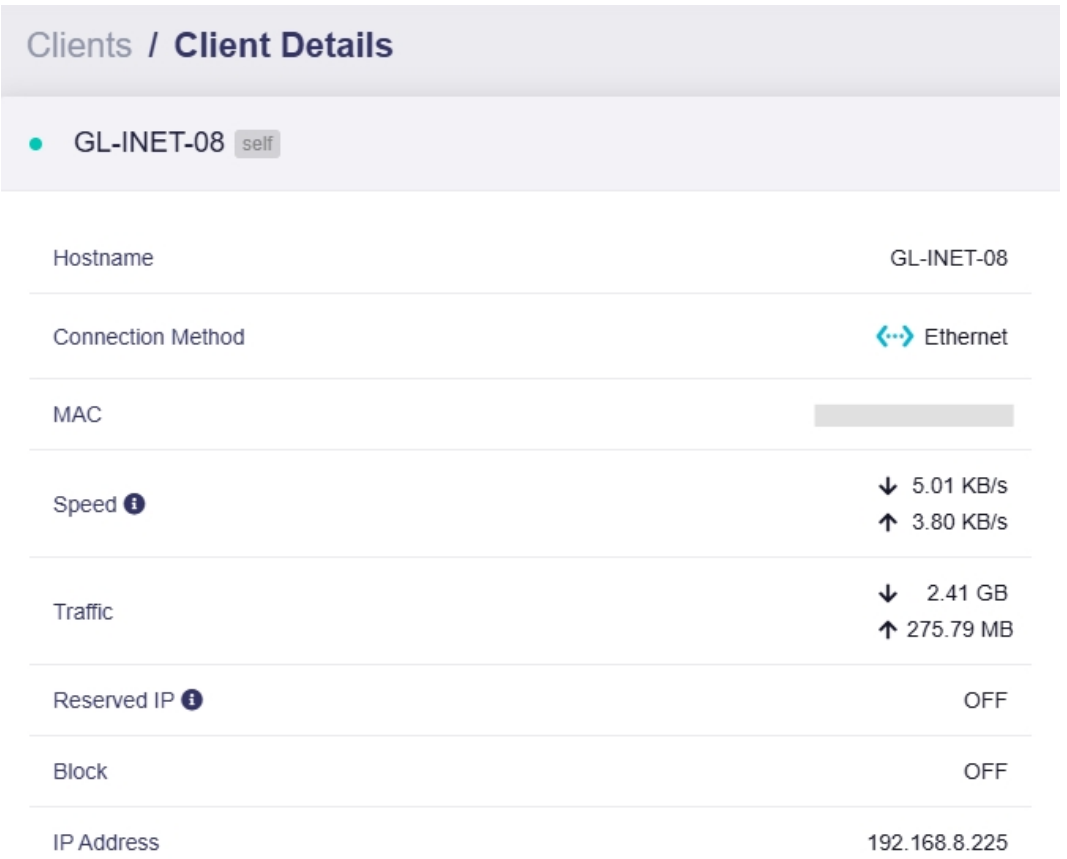
- **Lista negra**: dispositivos con direcciones MAC en el negrolist no puede conectarse a este enrutador. Tenga en cuenta que el bloqueo del cliente se basa en la dirección MAC del dispositivo. Si el dispositivo bloqueado usa una dirección MAC diferente la próxima vez, aún podrá conectarse al enrutador.
- **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. **Ver detalles**

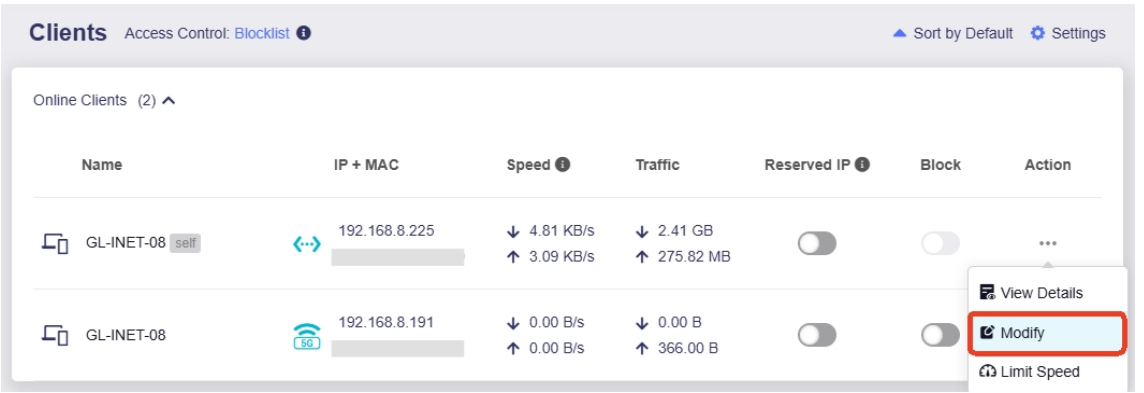
   Haga clic en el icono de tres puntos en la **Acción** columna y haga clic en **Ver detalles** en el menú desplegable para ver los detalles del dispositivo en una sola página.

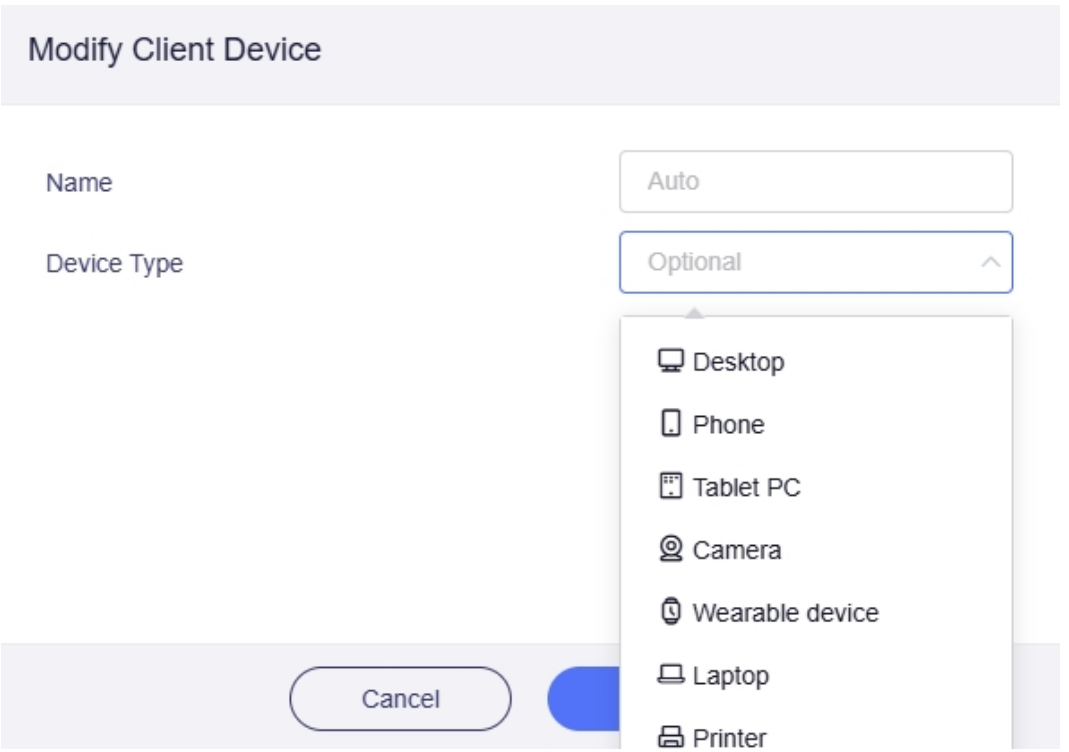




2. **Modificar**

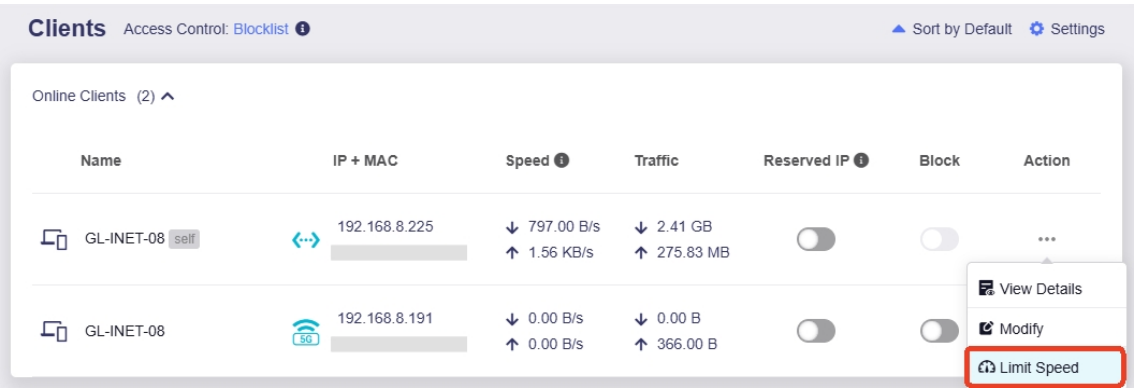
Haga clic en el ícono de tres puntos en la columna **Acción** y haga clic en **Modificar** desde el menú desplegable menú para modificar el nombre y el tipo del dispositivo.



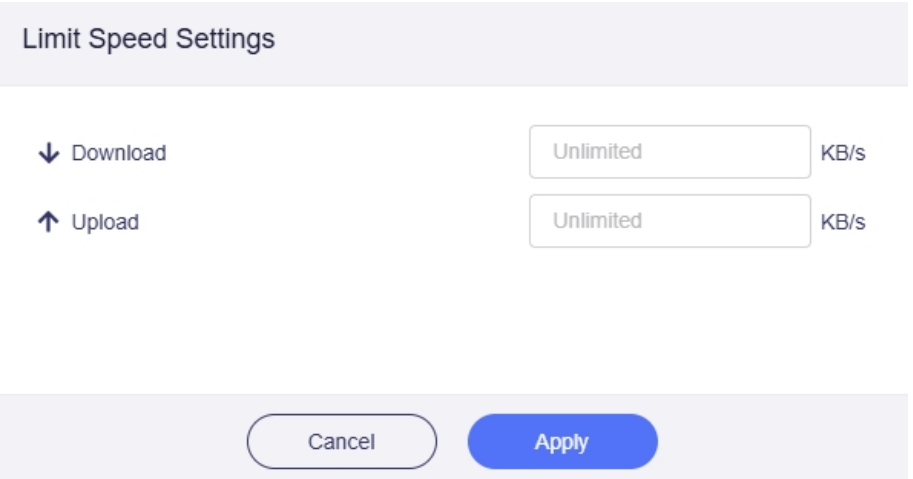


3. **Limitar velocidad**

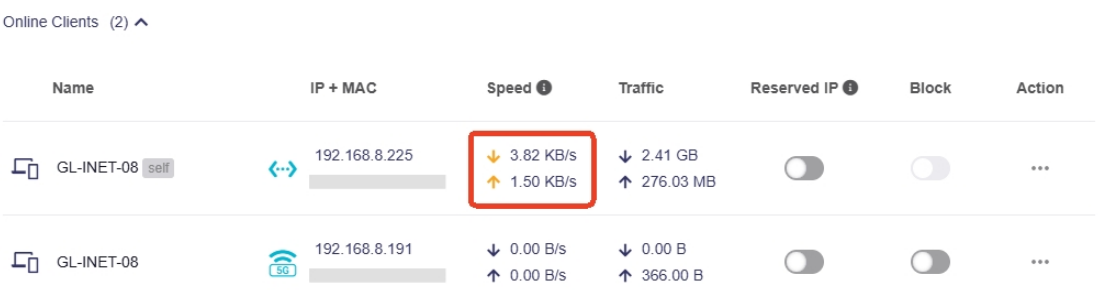
Haga clic en el icono de tres puntos en la **Acción** columna y haga clic en **Limitar velocidad** en el menú desplegable.



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



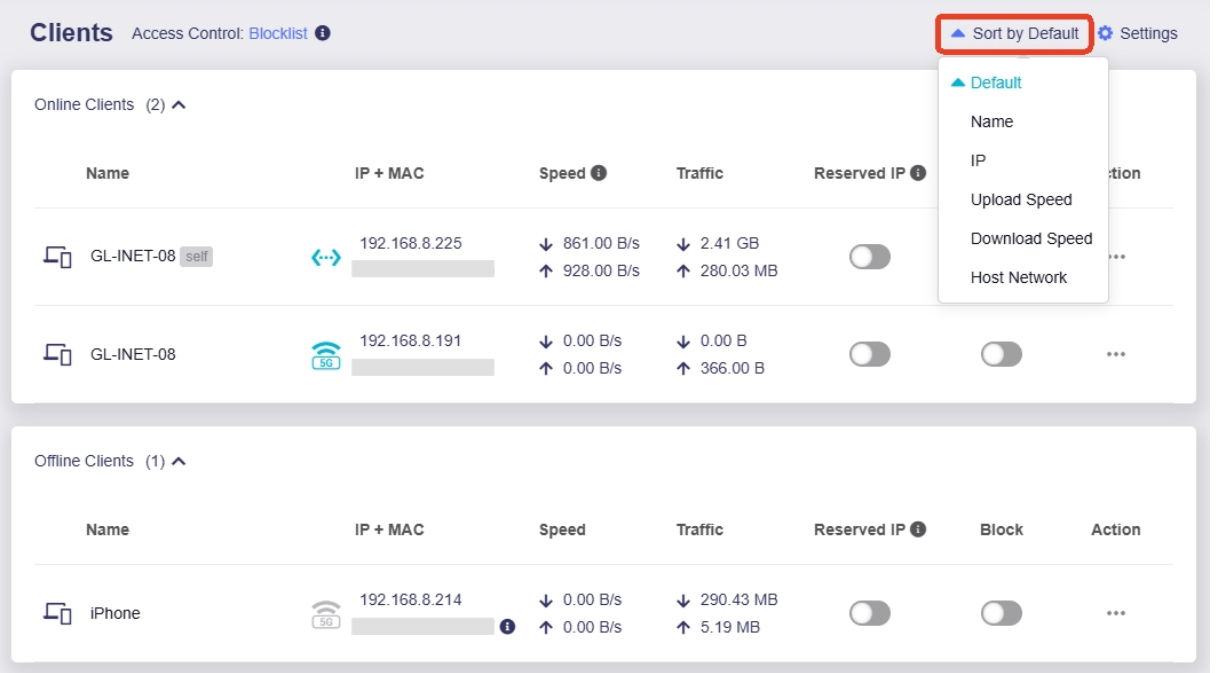
Si se ha aplicado una limitación de velocidad a un dispositivo, las flechas de velocidad de carga/descarga se volverán amarillas.



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

6.3 Ordenar

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

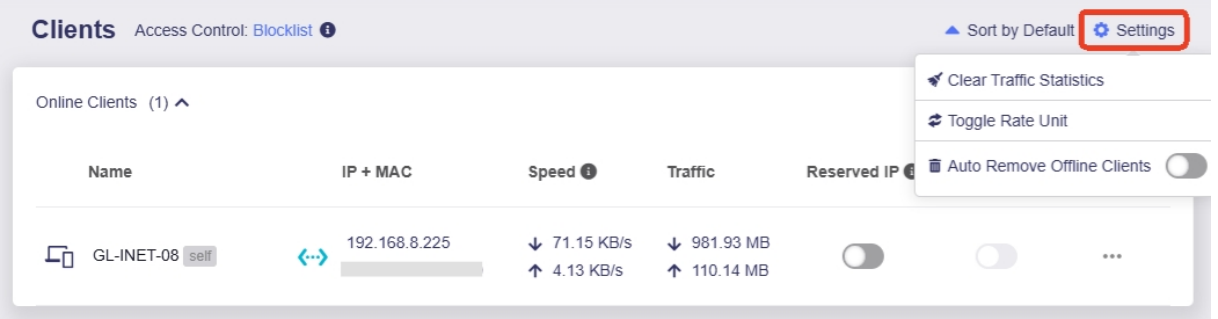


La clasificación predeterminadaing el orden es el siguiente:

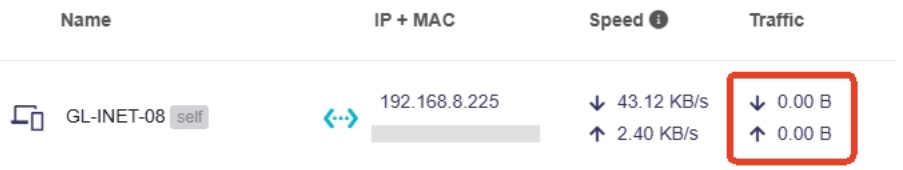
- El propio-dispositivo (es decir, el dispositivo que está utilizando para acceder al administrador del enrutador' Panel) siempre aparece en la parte superior.
- En el **Oen línea Clients** sección, los dispositivos aparecen en una lista superior si se conectaron antes.
- En el **Desactivadolínea Cclientes**, los dispositivos aparecen en una lista más alta si desconectados antes.

6.4 Configuración

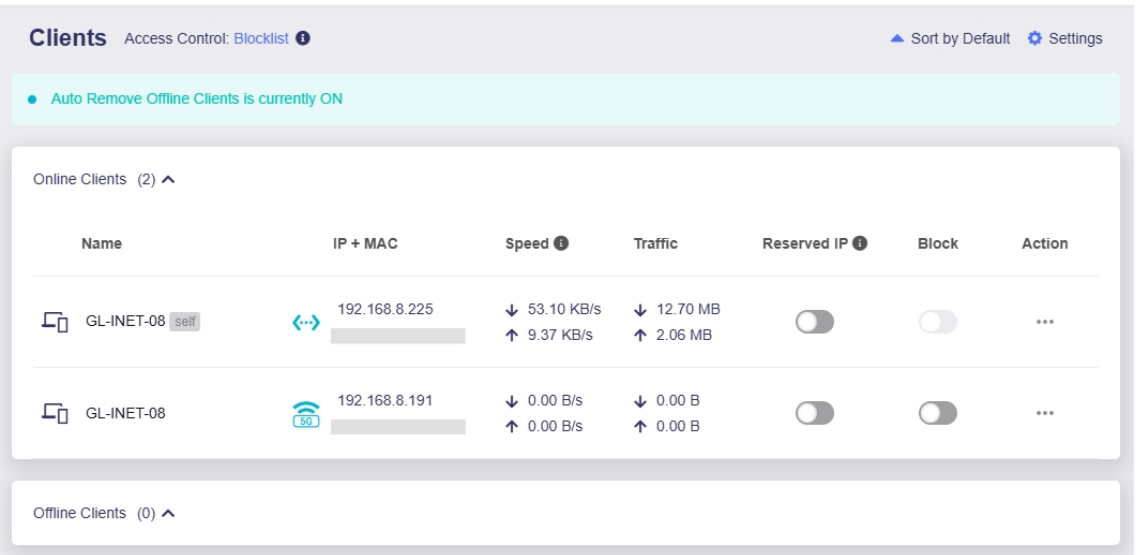
Haga clic en el botón **Configuración** en la esquina superior derecha para realizar más operaciones.



- **Borrar estadísticas de tráfico**: borrar estadísticas de tráfico para todos los clientes online 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**.
- **Eliminación automática de clientes sin conexión**: esta función se introdujo en el firmware v4.9. Una vez habilitado, todos los clientes sin conexión se borrarán inmediatamente y no se mostrarán en la sección Clientes sin conexión.



Capítulo 7

Servicios en la nube

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

7.1 GoodCloud

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

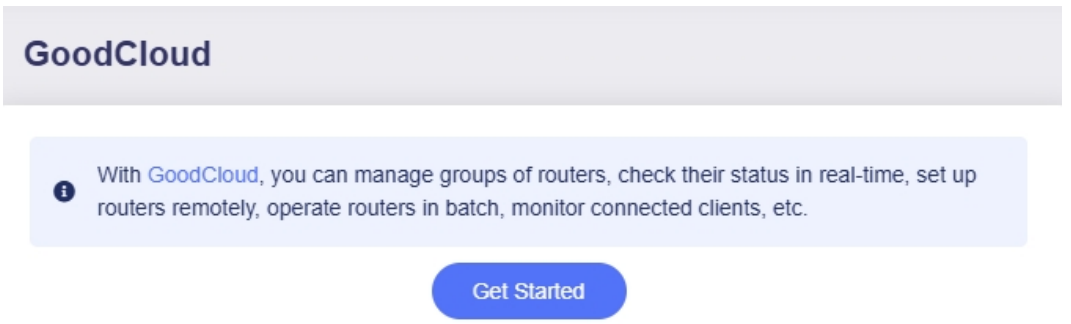
Con GoodCloud, puede:

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

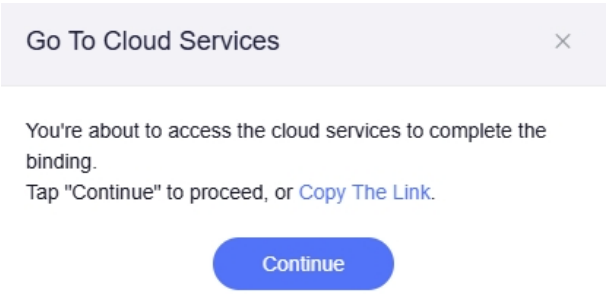
Algunas funciones están disponibles en el plan Enterprise y VAR (revendedor de valor agregado). Consulte aquí para obtener más detalles.

7.1.1 Habilitar GoodCloud

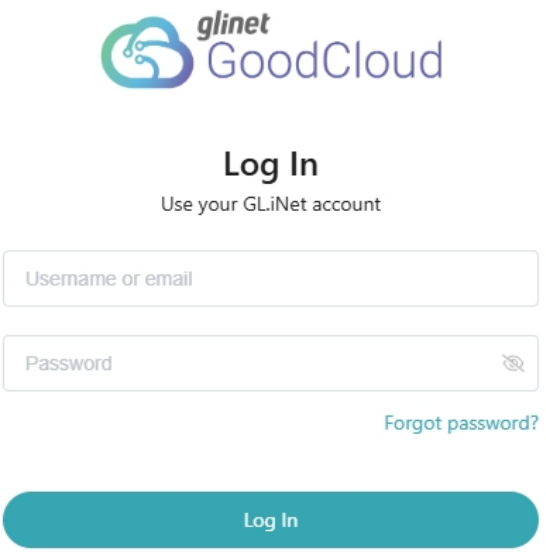
1. Inicie sesión en el panel de administración web de su enrutador', navegue hasta **SERVICIO EN LA NUBE** > **GoodCloud**, y click **Obtener Started.**



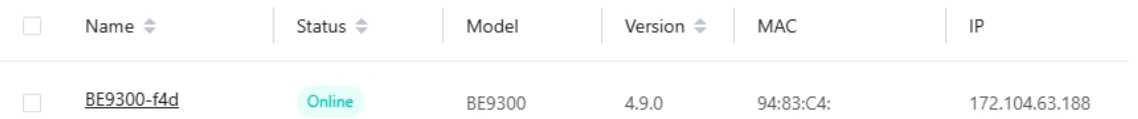
2. En la ventana emergente, haga clic en **Continuar**.



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



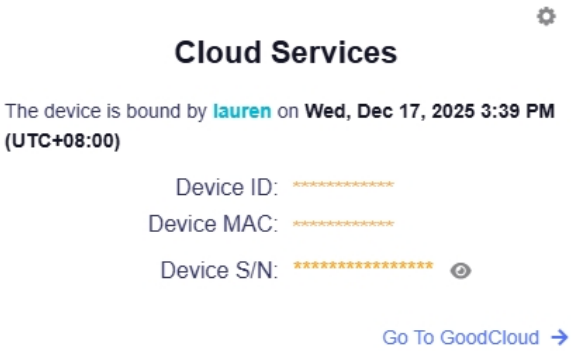
4. Confirme la información de su cuenta y dispositivo en el siguiente paso, luego haga clic en **Vincular**. Luego serás redirigido a la plataforma GoodCloud, donde podrás verificar que tu enrutador se haya vinculado a tu cuenta.



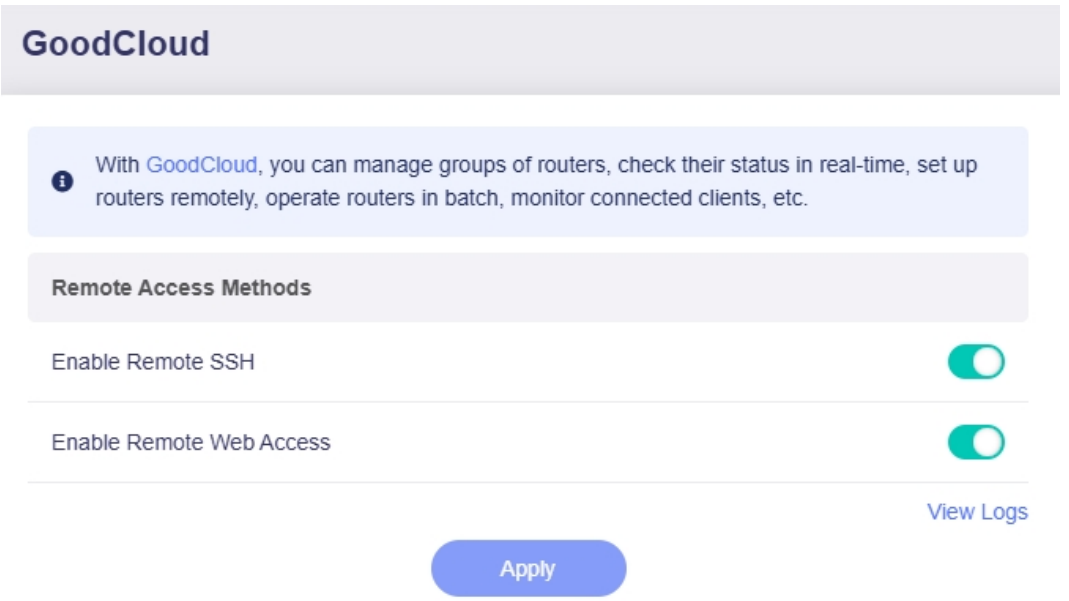
Consejos:

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

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



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

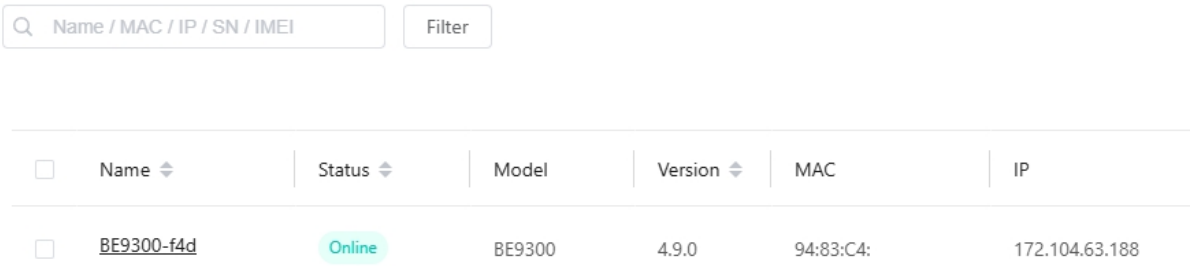


- **Acceso remoto SSH**: acceda de forma remota al terminal del enrutador desde GoodCloud usando SSH.
- **Acceso web remoto**: Remotely accede a la web del enrutador admin panel de GoodCloud a través de HTTP/HTTPS.
- **Ver registros**: Redirigir a la página de registro y mostrar la nube log.

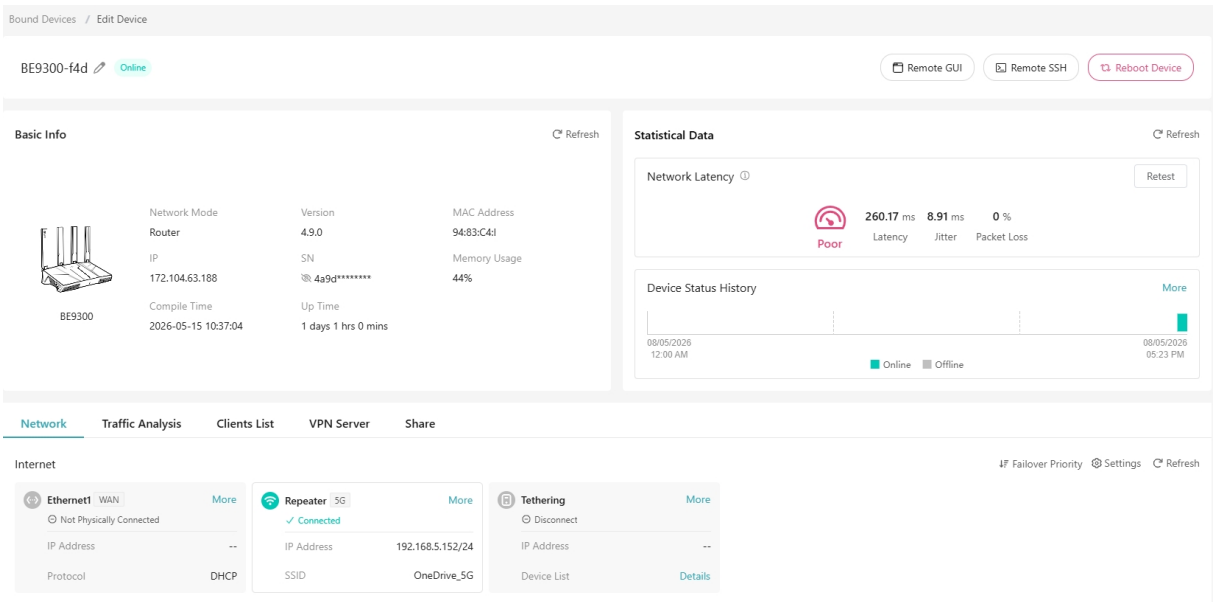
7.1.2 Administrar el enrutador

Consultar los detalles del dispositivo

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

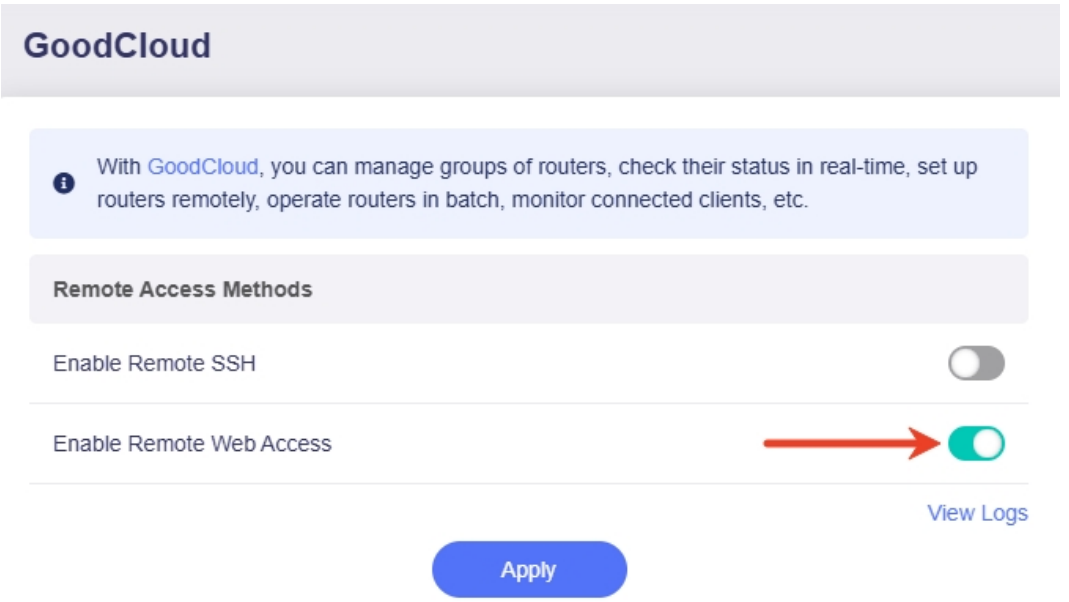


Haga clic en el nombre del dispositivo para ingrese a la página de detalles del dispositivo, que muestrainformación básica, datos estadísticos, descripción general de la red, lista de clientes y cronograma. También puede realizar operaciones avanzadas, como acceso remotolying al enrutador, y reiniciando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

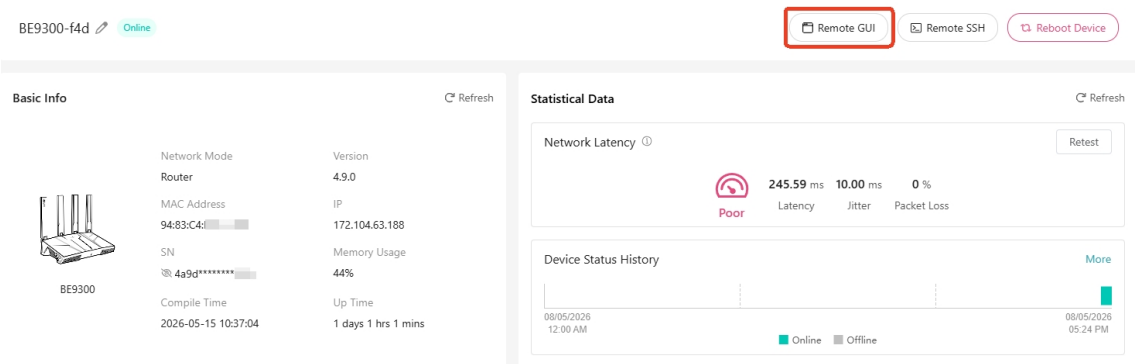


Acceso web remoto

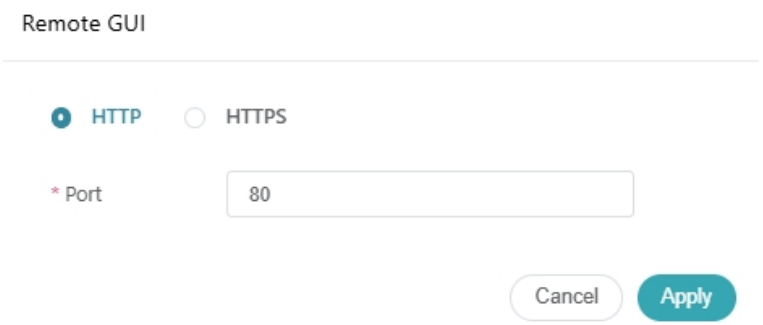
1. Inicie sesión en el enrutador’panel de administración web, navegue hasta **SERVICIOS EN LA NUBE** > **GoodCloud**, habilite **Acceso web remoto** y luego haga clic **Aplicar**.



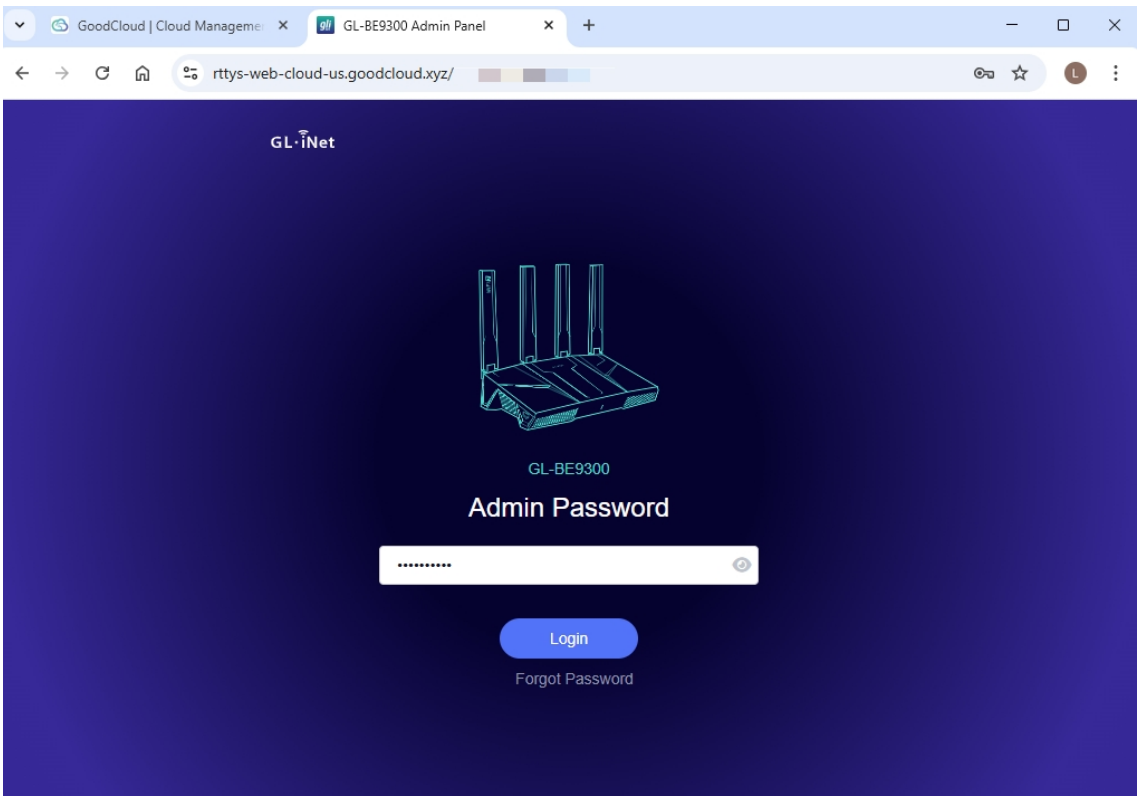
2. Inicie sesión en la plataforma GoodCloud y navegue a **Dispositivo** > **Dispositivos vinculados**. Haga clic en el dispositivo al que desea acceder y accederá a la página de detalles del dispositivo.
3. En la página de detalles del dispositivo, haga clic en el botón **GUI remota** en la esquina superior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



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

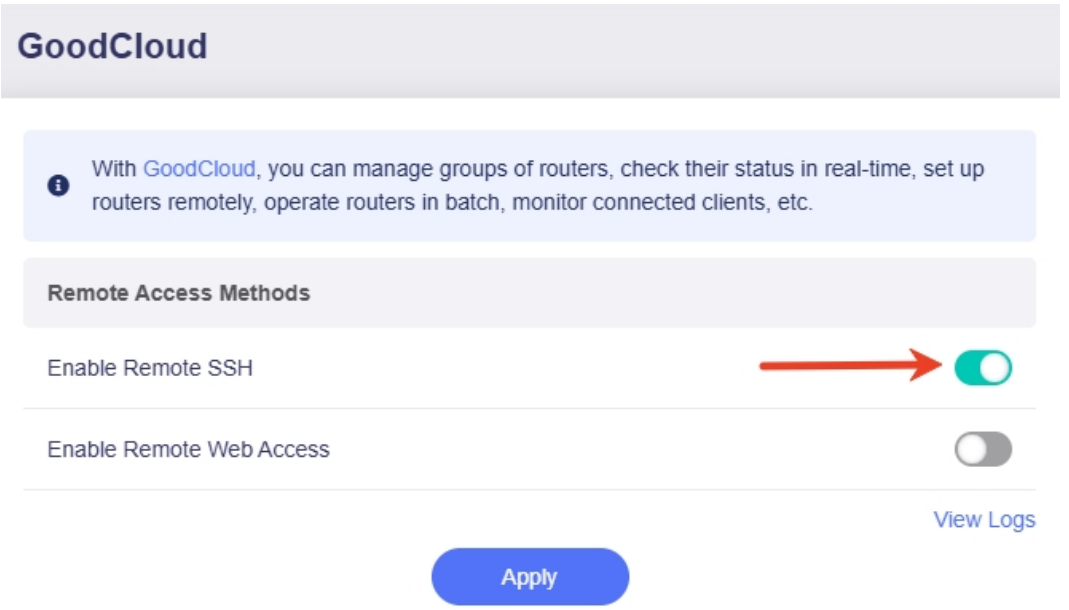


5. Será redirigido a la página de inicio de sesión del enrutador'. Ingrese la contraseña de administrador para acceder de forma remota al panel de administración web del enrutador'.

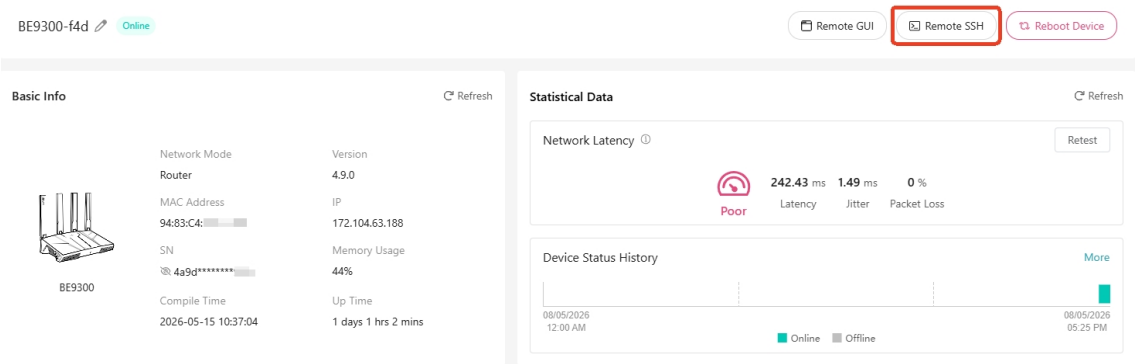


Acceso remoto al terminal

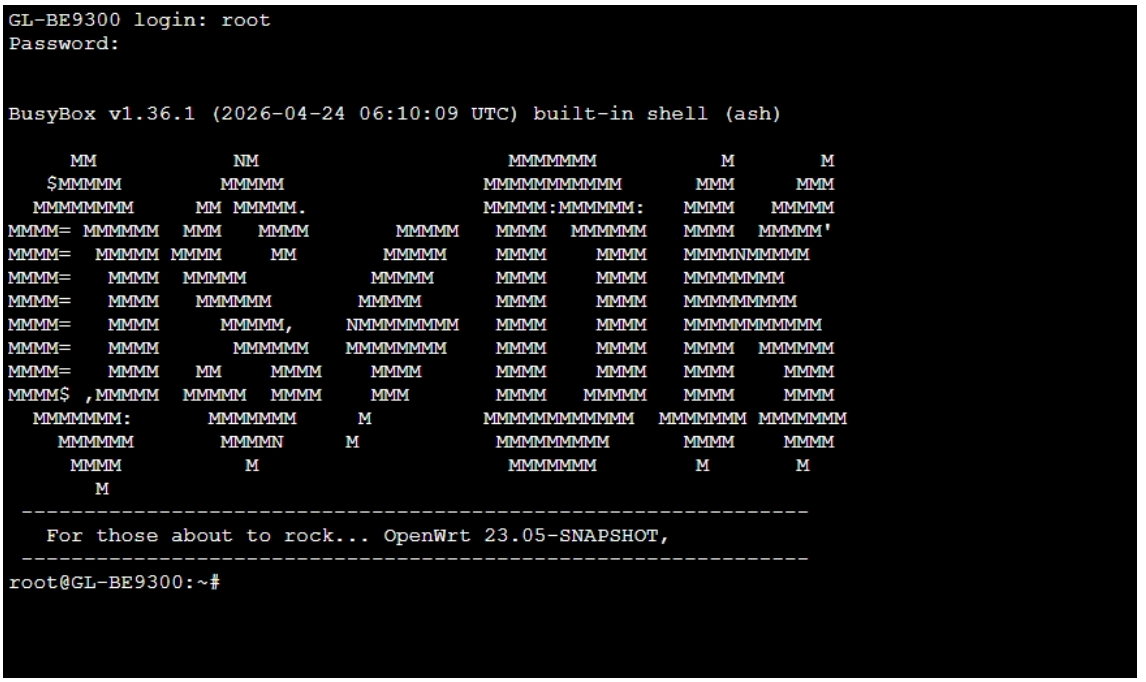
1. Inicie sesión en el panel de administración web del router', navegue hasta **SERVICIOS EN LA NUBE** > **GoodCloud**, habilite **Acceso remoto SSH**, luego haga clic en **Aplicar**.



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

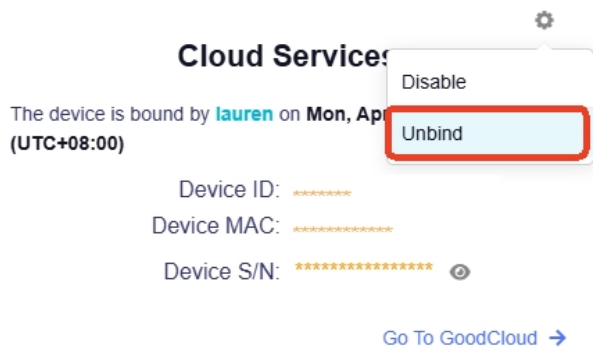


4. Inicie sesión como **root** e ingrese la contraseña para acceder al terminal de su enrutador.

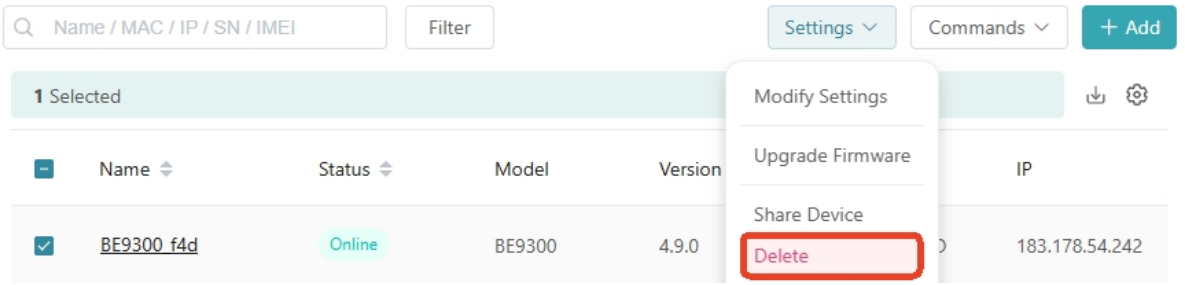


7.1.3 Desvincular el dispositivo

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

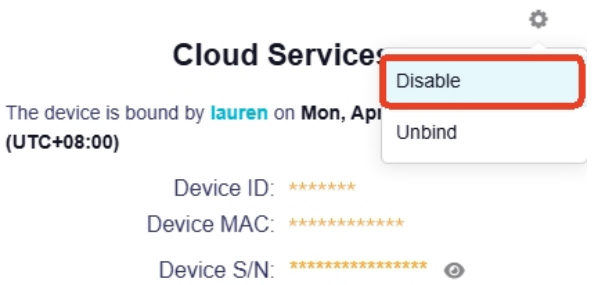


Como alternativa, inicie sesión en la plataforma en la nube y navegue hasta **Dispositivo** > **Dispositivos vinculados**. Seleccione el dispositivo que desea desvincular, haga clic en **Configuración** en la esquina superior derecha y luego seleccione **Eliminar**. Su dispositivo se desvinculará de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



7.1.4 Desactivar GoodCloud

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



El servicio en la nube se desactivará.

7.2 AstroWarp

AstroWarp es una característica de red avanzada diseñada para GL.enrutador iNets para proporcionar una perfecta y remota redes y administración de dispositivos. Iintegrado en el SDK del enrutador GL.iNet, adopta el protocolo AmneziaWG con ofuscación de tráfico incorporada, lo que ofrece conexiones estables y seguras para un acceso remoto confiable en cualquier momento y lugar.

Esta función permite un acceso remoto perfecto a su red doméstica. Puede configurar y emparejar dispositivos directamente a través de un código de acceso dinámico en el Panel de administración web, estableciendo rápidamente una conexión segura entre su enrutador de viaje y su red doméstica en solo segundos, sin necesidad de registrarse ni iniciar sesión.

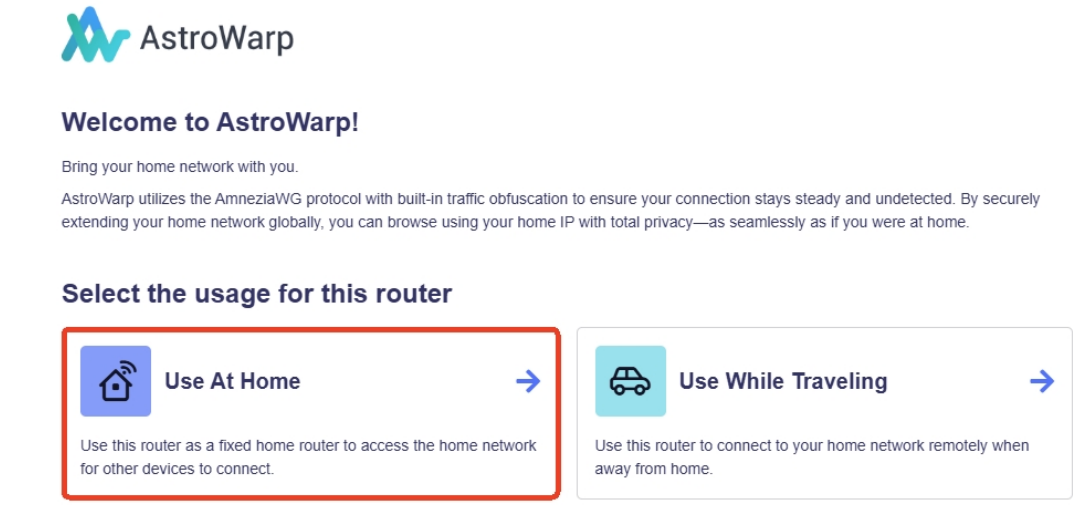
Nota:

1. No se recomienda utilizar AstroWarp con cualquiera de las siguientes funciones al mismo tiempo, ya que esto puede causar conflictos de enrutamiento: GoodCloud de sitio a sitio, ZeroTier, Tailscale, Tor.
2. Cuando AstroWarp está habilitado, el modo de red no se puede utilizar.

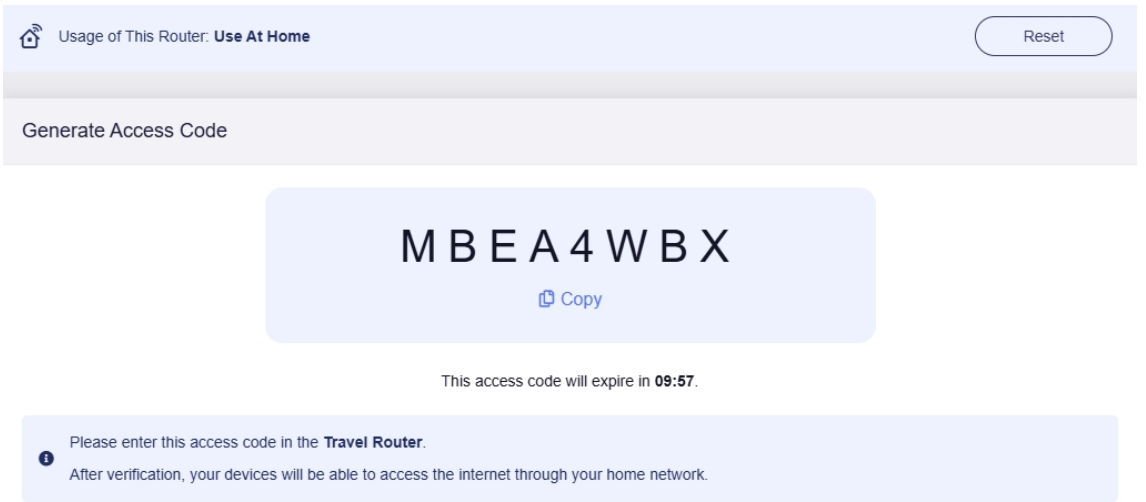
7.2.1 Configuración rápida

A continuación se muestra un ejemplo de usando Flint 3 (GL-BE9300) y Slate 7 (GL-BE3600) para configurar una red AstroWarp. Flint 3 es el enrutador doméstico, mientras que Slate 7 es el enrutador de viaje que enruta el tráfico de red de regreso a Flint 3 para acceder a Internet.

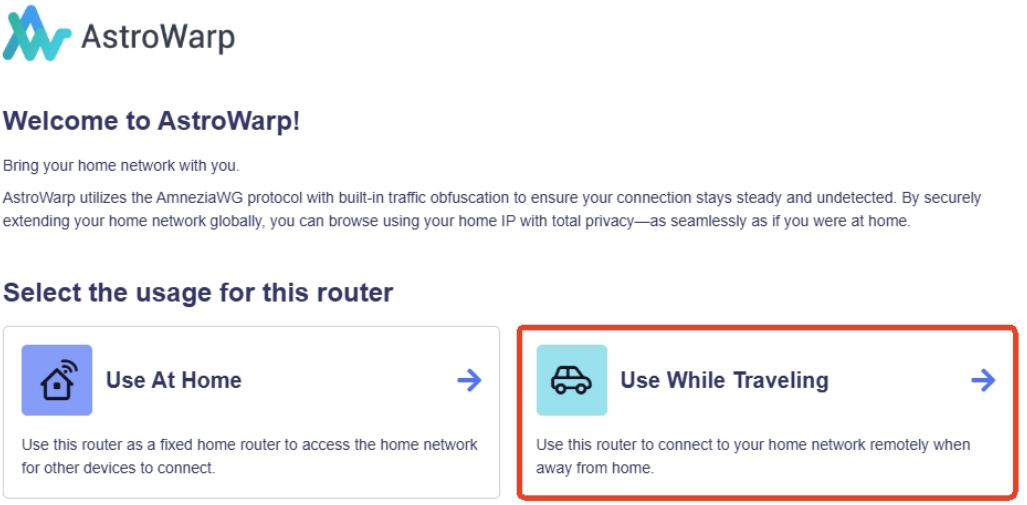
1. Configure Flint 3 para Internet.
   Inicie sesión en el panel de administración web de Flint 3 y navegue hasta la página INTERNET. Conéctelo a Internet usando uno de los métodos de conexión a Internet admitidos: Ethernet, repetidor, anclaje a red y celular.
2. Ien el panel de administración web de Flint 3, navegue hasta **SERVICIOS EN LA NUBE** > **AstroWarp**. Haga clic en **Usar en casa**.



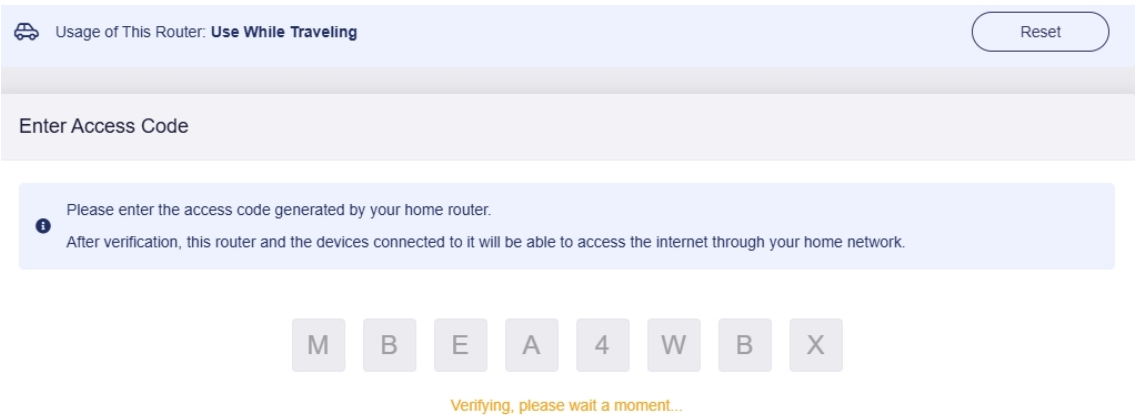
Se generará un **Código de acceso**. Copie este código para usarlo más adelante.



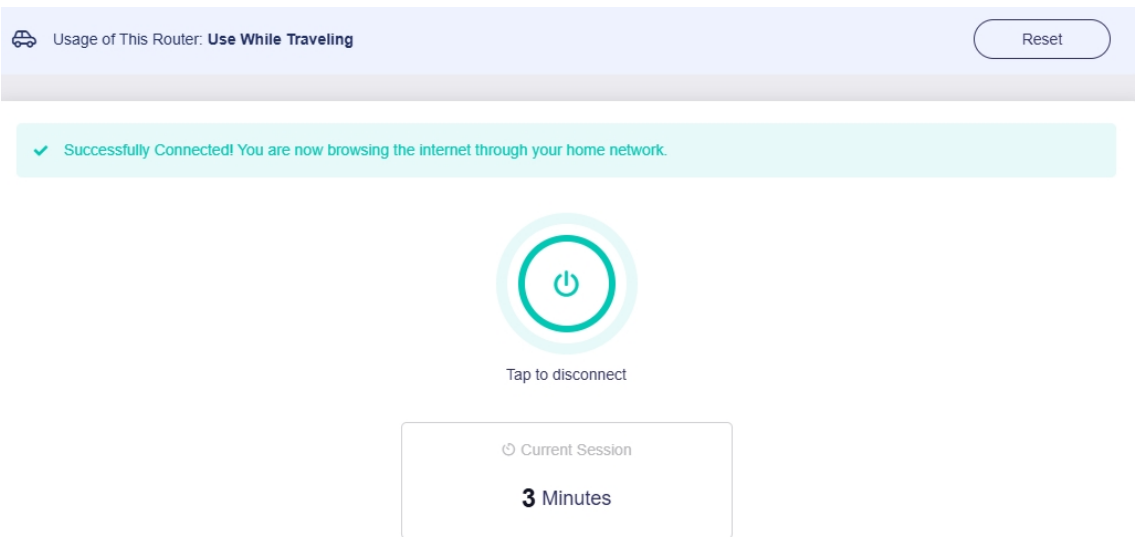
3. Configure Slate 7 para Internet.
   Inicie sesión en el panel de administración web de Slate 7 y navegue hasta la página INTERNET. Conéctelo a Internet usando uno de los métodos de conexión a Internet admitidos: Ethernet, repetidor, anclaje a red y celular.
4. Ingrese el código de acceso.
   En el panel de administración web del Slate 7, navegue hasta **CLOUD SERVICIOS** > **AstroWarp**. Clic **Usar mientras viajaing**.



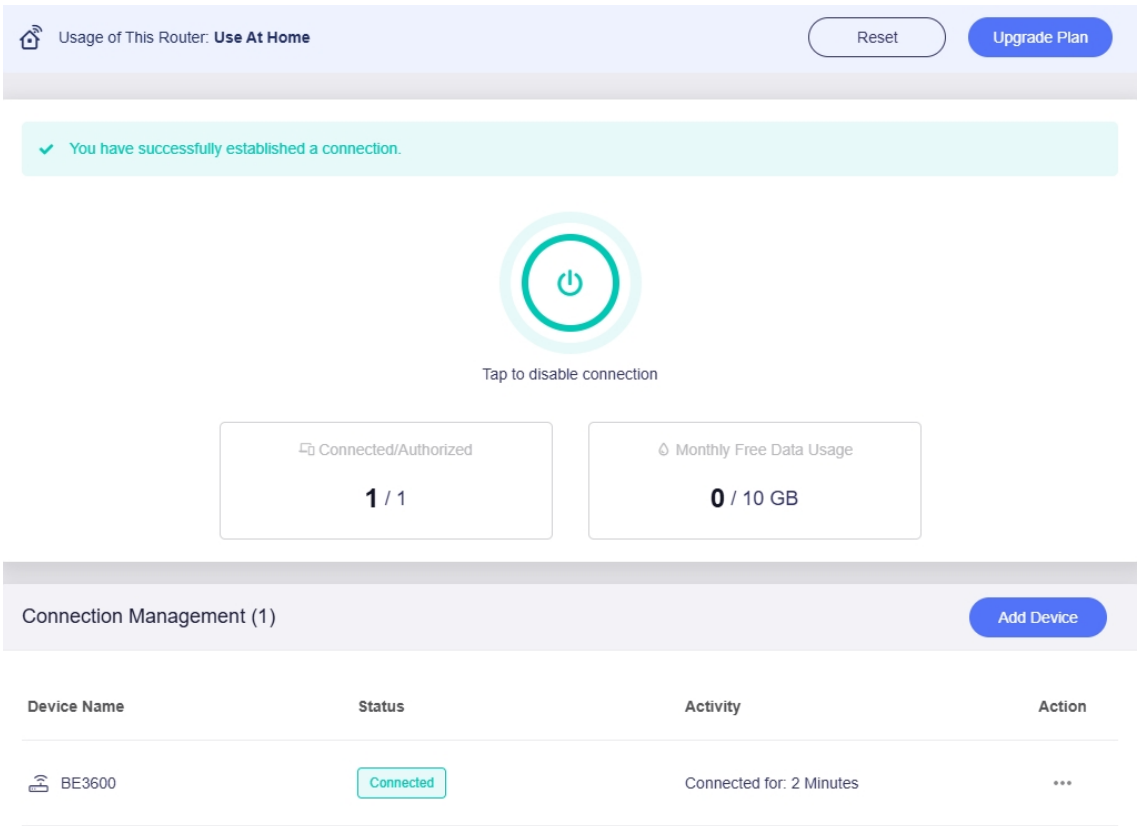
Ingrese el Código de acceso obtenido en el paso 2 y espere a que se complete la verificación.espera a que se complete la verificación.



Luego se conectará exitosamente al enrutador doméstico Flint 3. Ahora puede navegar por Internet a través de su red doméstica de forma segura.



5. Enen el panel de administración web de Flint 3, también se muestra el estado de la conexión, como se muestra a continuación.



7.2.2 Comprobar la conectividad

1. Conecte una computadora portátil o un teléfono inteligente a la red Wi-Fi del enrutador de viaje Slate 7.
2. Abra un navegador y visite ipcheck.ing o cualquier otro sitio web de búsqueda de direcciones IP. Mostrará la dirección IP pública de Flint 3, lo que indica que Slate 7 está accediendo a Internet a través de su enrutador doméstico Flint 3.



3. Desconecte la conexión AstroWarp en Slate 7, luego actualice la página web para volver a enviar la solicitud de consulta de IP. mostrará la dirección IP pública de Slate 7, lo que indica que Slate 7 está accediendo a Internet a través de su red local.



Capítulo 8

Conozca la VPN

Este capítulo presenta VPN conceptos y uso escenarios.

8.1 Introducción

VPN

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

Enrutador VPN

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

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

OpenVPN

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

WireGuard

WireGuard es un protocolo VPN ligero, 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.

8.2 Escenarios de aplicación

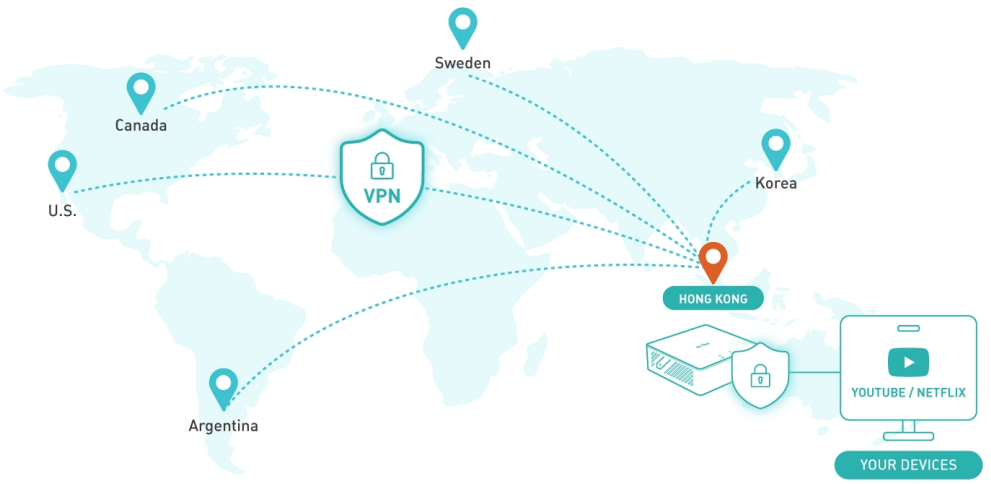
1. **Privacidad de datos personales**

   El servicio VPN es compatible con una amplia gama de dispositivos a través de nuestro enrutador, incluidos 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.



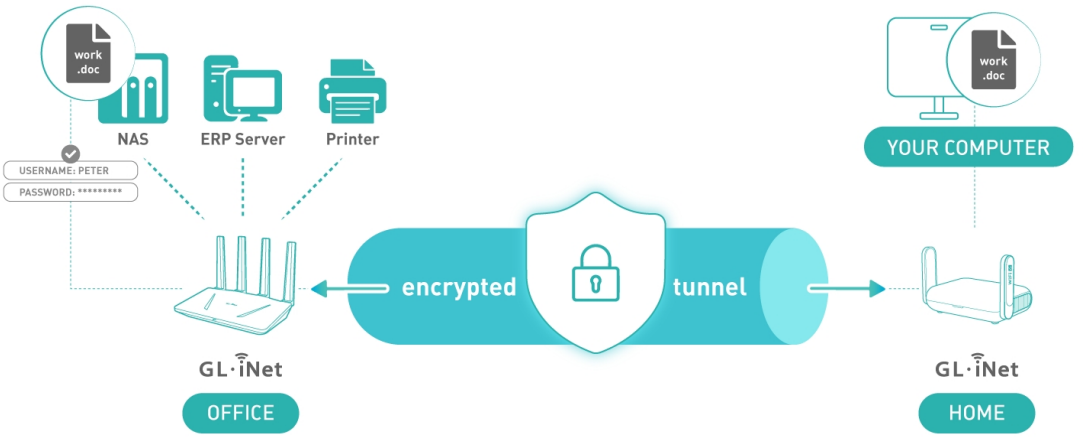
2. **Sin restricciones Acceso en todo el mundo**

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



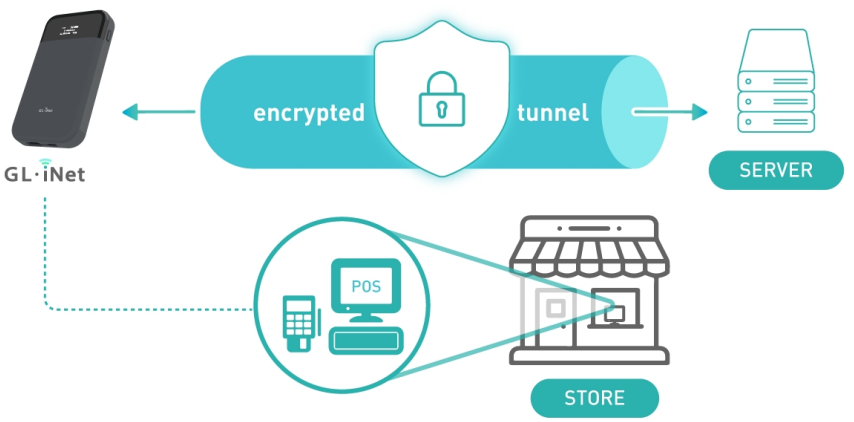
3. **Seguridad de datos para pequeñas empresas**

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



4. **Infraestructura de pago segura**

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



Capítulo 9

Panel de VPN

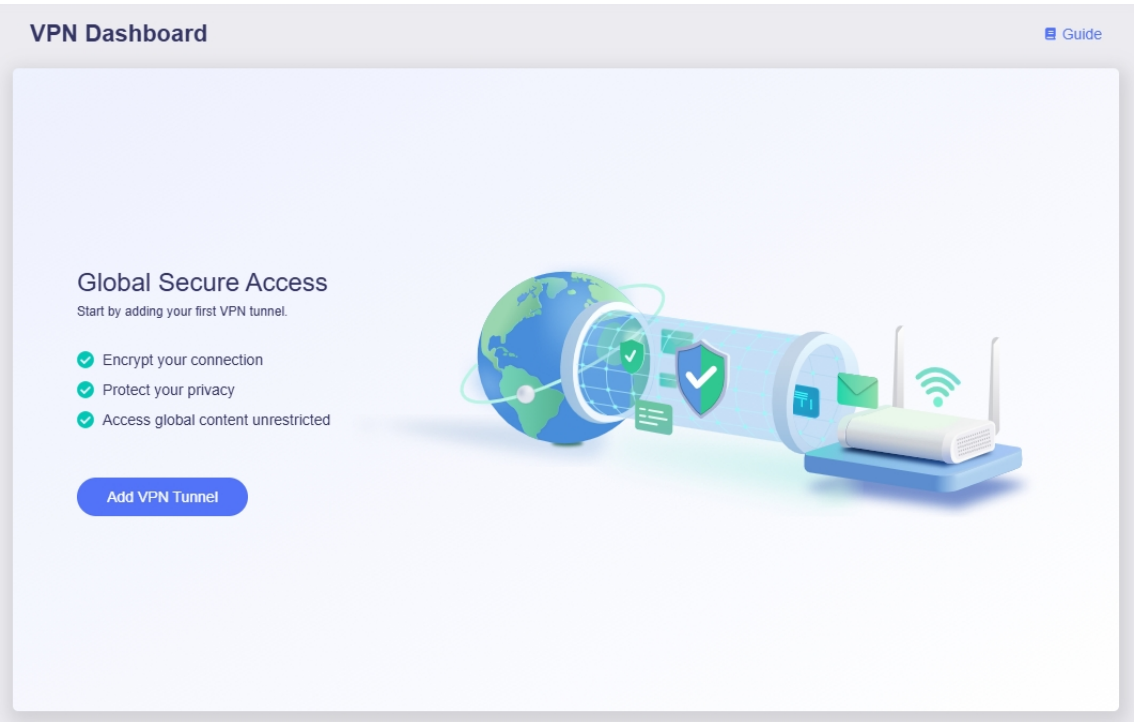
Este capítulo presenta cómo administrar conexiones VPN a través del panel de administración web.

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

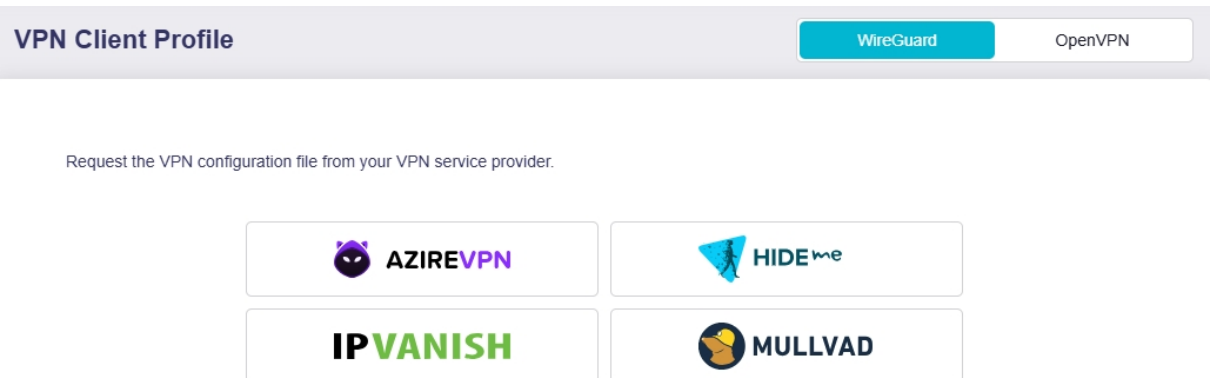
El panel de VPN muestra detalles de la conexión VPN, como reglas de enrutamiento, servidor conectado y tráfico. estadísticas, IP virtual del cliente y registro de conexión, y permite a los usuarios configurar ajustes avanzados como VPN Kill Switch, enmascaramiento de IP y MTU.

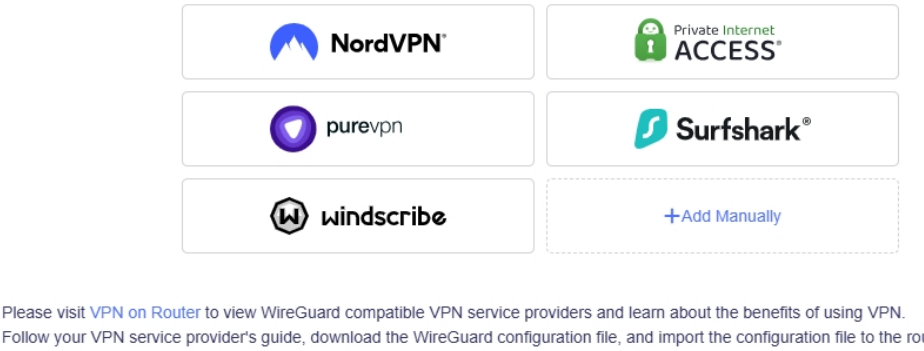
9.1 Cargar perfil VPN

Al ingresar a esta página por primera vez, si no se han creado túneles, la página aparece de la siguiente manera. Haga clic en **Agregar túnel VPN** para comenzar.



Se le dirigirá a la página **Perfil de cliente VPN**. Seleccione un proveedor de VPN e inicie sesión.

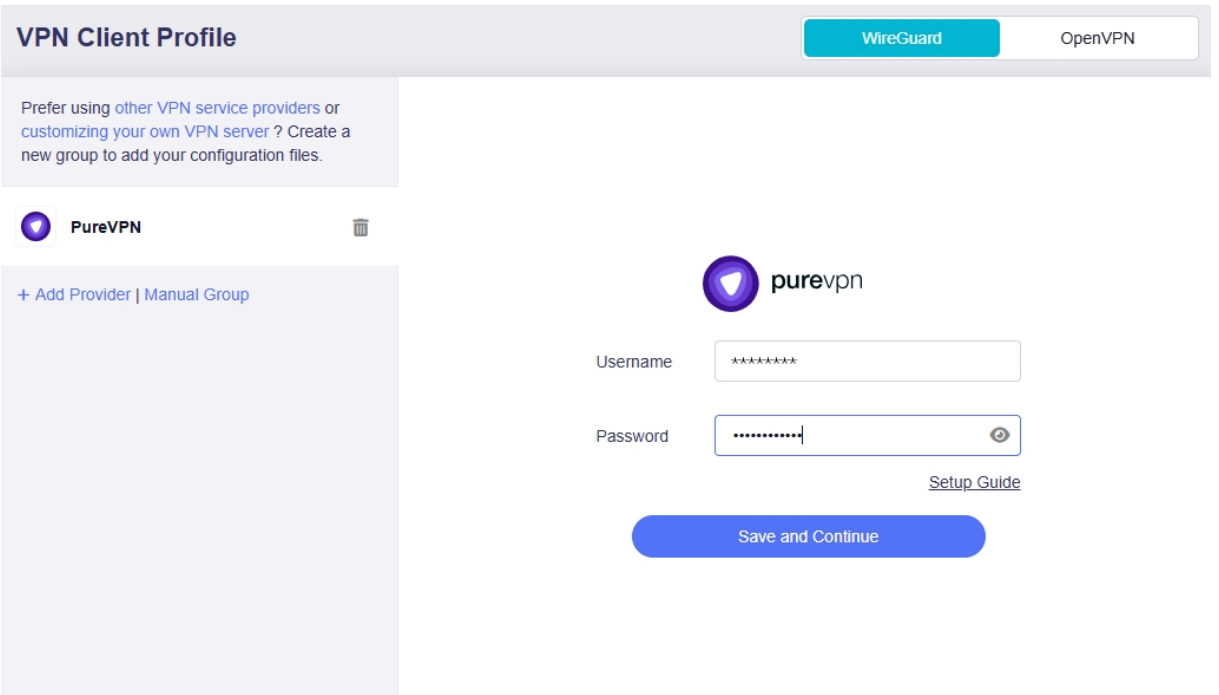




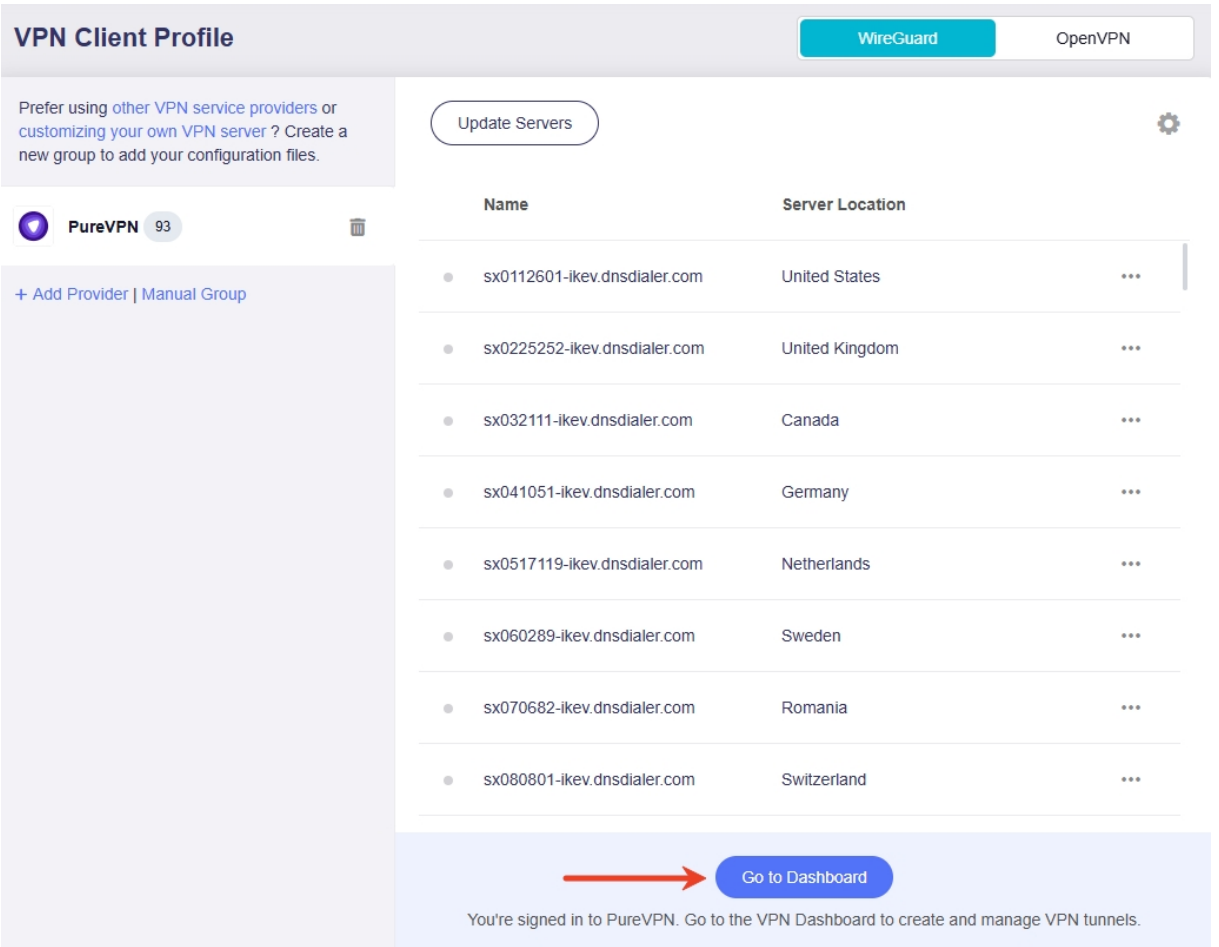
Consejos:

1. Los proveedores de VPN enumerados están integrados en el panel de administración web del enrutador GL.iNet. Con una suscripción activa, los usuarios simplemente ingresan sus credenciales para iniciar sesión instantáneamente y obtener archivos de configuración para conexiones VPN.
2. Si se ha suscrito a otros proveedores de VPN o si desea cargar sus configuraciones personales de VPN, haga clic en **Agregar manualmente** y cargue sus configuraciones.

Tome PureVPN como ejemplo. Haga clic en PureVPN e inicie sesión con credenciales válidas.



Obtendrá una lista de perfiles VPN, como se muestra a continuación. Haga clic en Ir al panel en la parte inferior y luego será dirigido al panel de VPN para configurar su túnel VPN y su política de VPN.



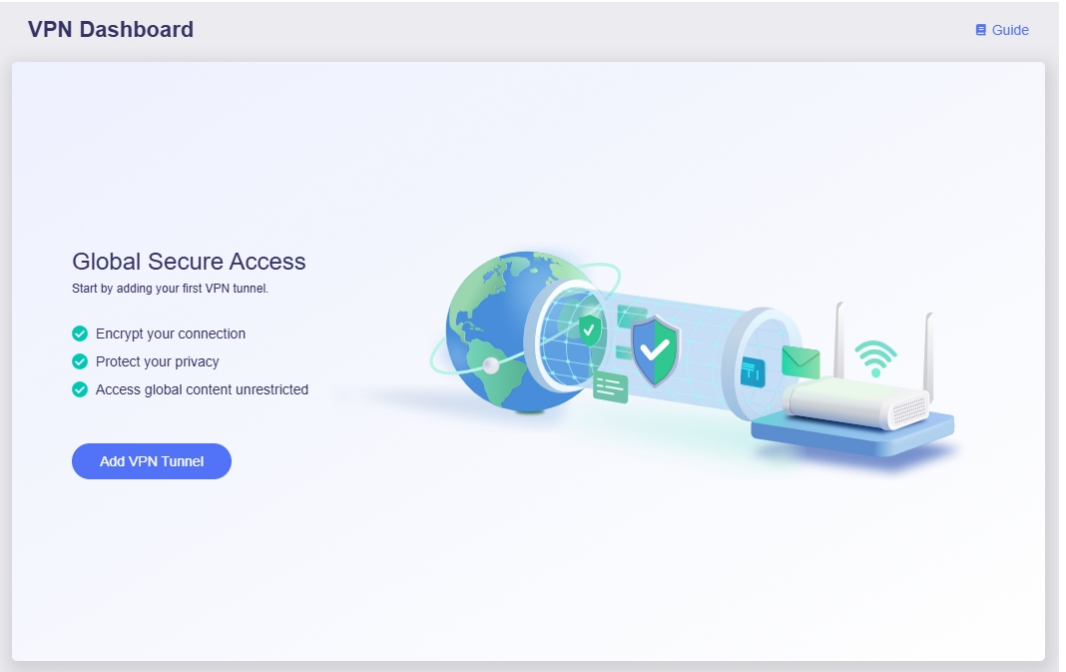
Consejo: Para algunos proveedores de servicios VPN, es posible que deba seleccionar un protocolo VPN o servidores/ciudades preferidos antes de que aparezca la lista de perfiles.

9.2 Agregar túnel VPN

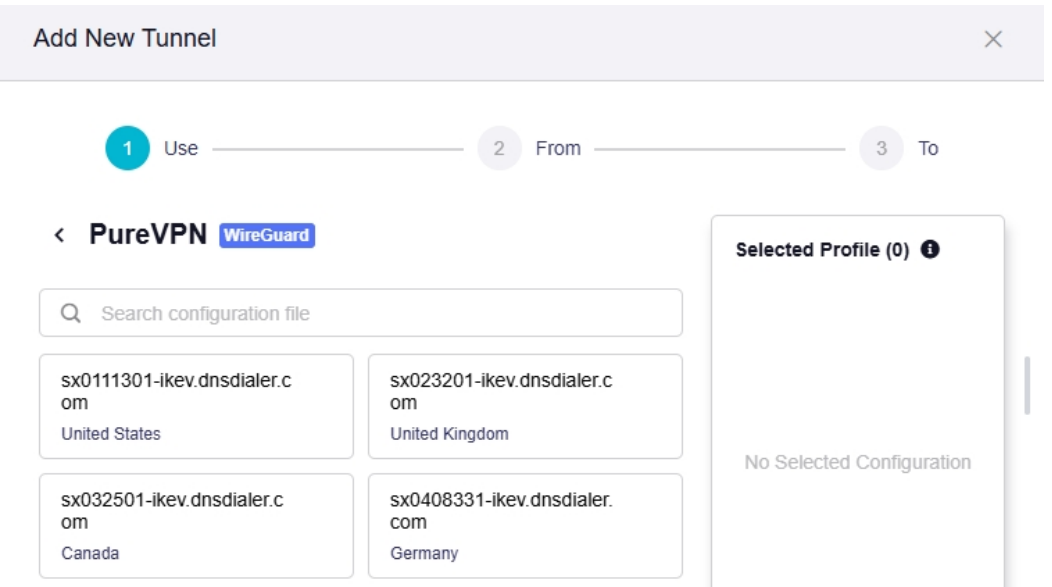
9.2.1 Pasos generales

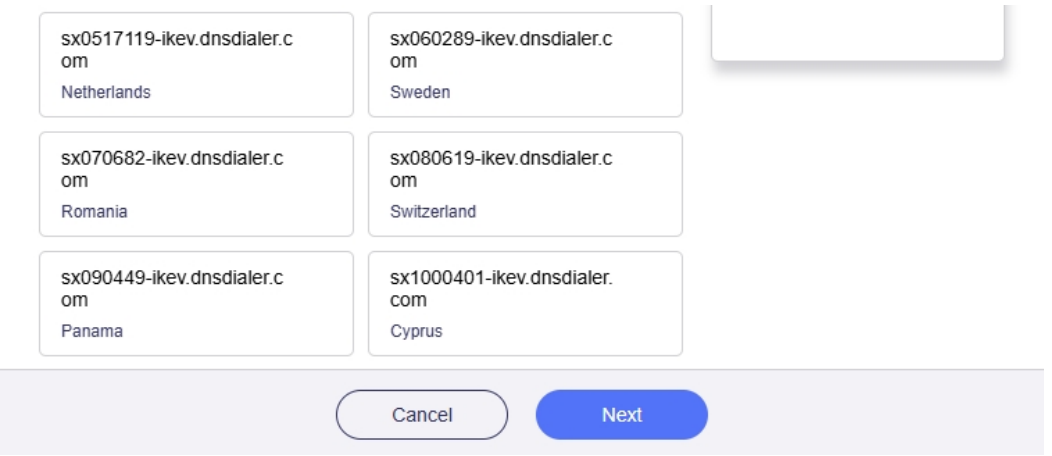
Siga los pasos a continuación para agregar su túnel VPN y configurar políticas VPN. Consulte Referencia del caso si es necesario.

1. En el panel de VPN, haga clic en **Agregar túnel VPN**. Aparecerá un asistente de configuracióna la derecha.



2. Seleccione uno o varios perfiles y ajuste su prioridad a la derecha si es necesario, luego haga clic en **Siguiente**.





Nota: cuando se seleccionan varios perfiles, el túnel intentará conectarse usando cada perfil en orden de prioridad hasta que se establezca una conexión exitosamente. Si todos los perfiles dentro de un único túnel no logran conectarse, el sistema determinará si se debe cambiar a la red local (WAN) del enrutador según el estado del interruptor de apagado en las Opciones de túnel y Todo el resto del tráfico configuración.

3. Seleccione la fuente del cliente y luego haga clic en **Siguiente**. Hay cuatro opciones:
   - **Todos los clientes**: si se selecciona, el tráfico de todos los dispositivos coincidirá con esta regla.
   - **Tipos de conexión específicos**: si se selecciona, el tráfico de tipos de conexión específicos (por ejemplo, subred LAN, acceso directo) Gateway, Guest Network) coincidirá con esta regla.
   - **Dispositivos especificados**: si se selecciona, el tráfico de los dispositivos especificados (identificados por la dirección MAC) coincidirá con esta regla.
   - **Excluir dispositivos especificados**: si se selecciona, el tráfico de los dispositivos especificados (identificados por la dirección MAC) no coincidirá con esta regla.
4. Seleccione el destino de destino y luego haga clic en **Aplicar**. Hay tres opciones:
   - **Todos los destinos**: si se selecciona, el tráfico que coincida con esta regla se enrutará a todos los destinos.
   - **Lista de IP/dominio especificada**: si se selecciona, el tráfico que coincida con esta regla se enrutará a dominios o direcciones IP específicos. Debe ingresarlos manualmente.
   - **Excluir lista de IP/dominio especificada**: si se selecciona, el tráfico que coincida con esta regla no se enrutará a dominios o direcciones IP específicos. Debe ingresarlos manualmente.

5. Se agregó correctamente un túnel VPN. Se le dirigirá al **Panel de VPN**. Agregue más túneles VPN si es necesario. Por seguridad, vaya a Todo el resto del tráfico y Opciones de túnel para comprobar **Eliminar Cambiar** estado antes de habilitar su túnel VPN.

9.2.2 Referencia del caso

Aquí se muestran dos casos típicos de configuración de políticas VPN con instrucciones paso a paso instrucciones para su referencia.

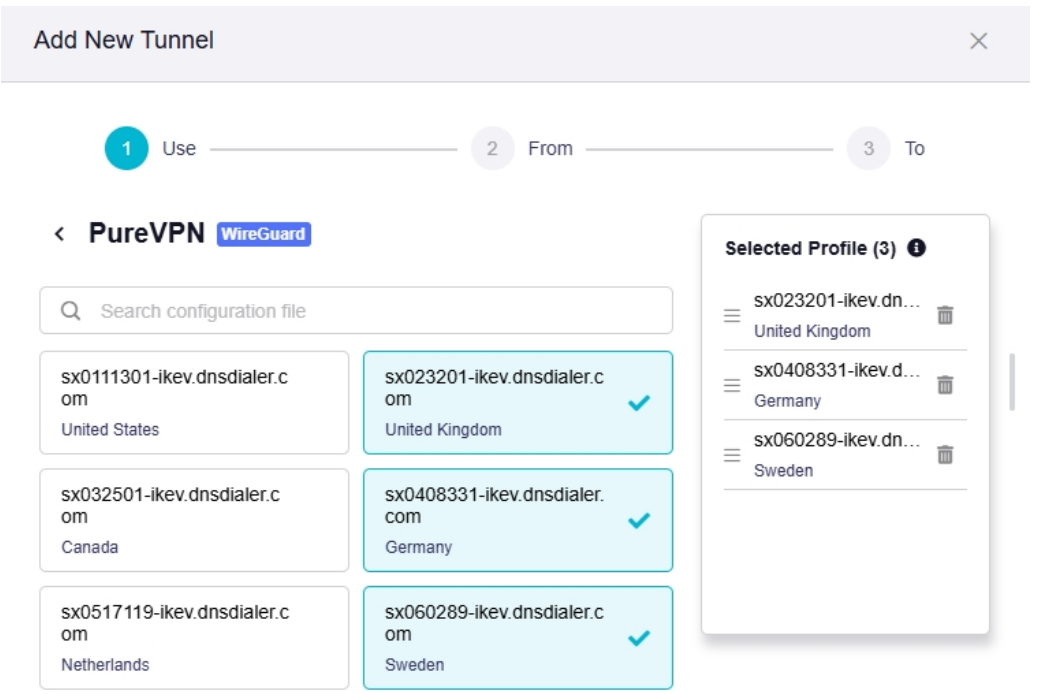
Caso 1: Enrutar solo dispositivos específicos a través de VPN

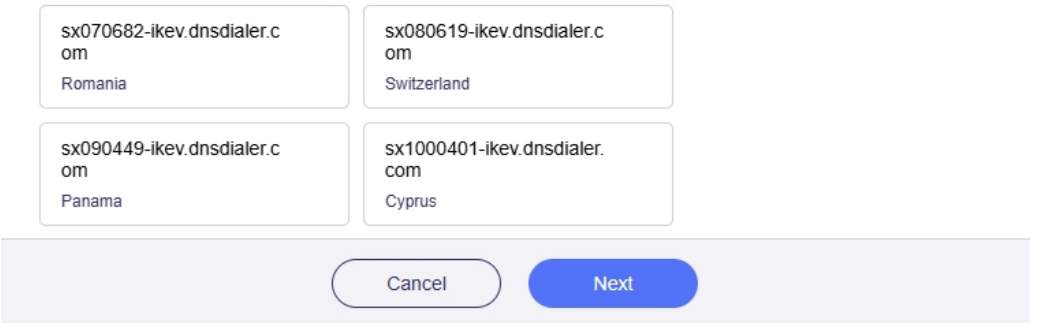
Requisitos:

1. Solo dispositivos específicos conectados a este enrutador acceden a Internet a través de la VPN. Todos los demás dispositivos acceden a Internet a través de la WAN local.
2. Los dispositivos seleccionados deben usar únicamente la conexión VPN. Si la VPN se desconecta inesperadamente, el acceso a Internet para estos dispositivos se bloqueará para evitar fugas de DNS y seguimiento de IP.

Pasos de configuración:

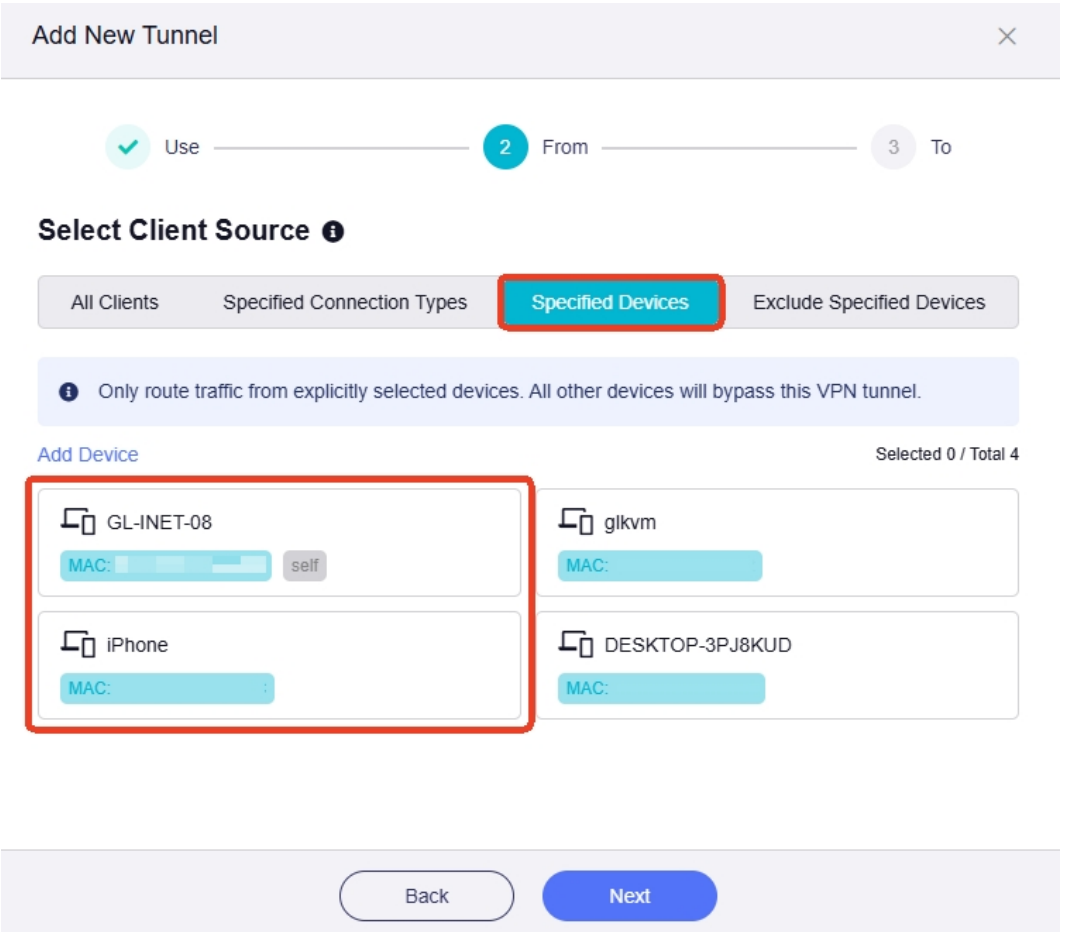
1. Seleccione el perfil de VPN.
   Si inició sesión con alguna credencial de servicio VPN integrado o cargó un archivo de configuración, los perfiles disponibles se enumerarán aquí. De lo contrario, vaya a **Perfil de cliente VPN** para iniciar sesión con sus credenciales o cargar un archivo de configuración manualmente.
   Tome PureVPN como ejemplo. Seleccione uno o varios perfiles y ajuste su prioridad a la derecha si es necesario.





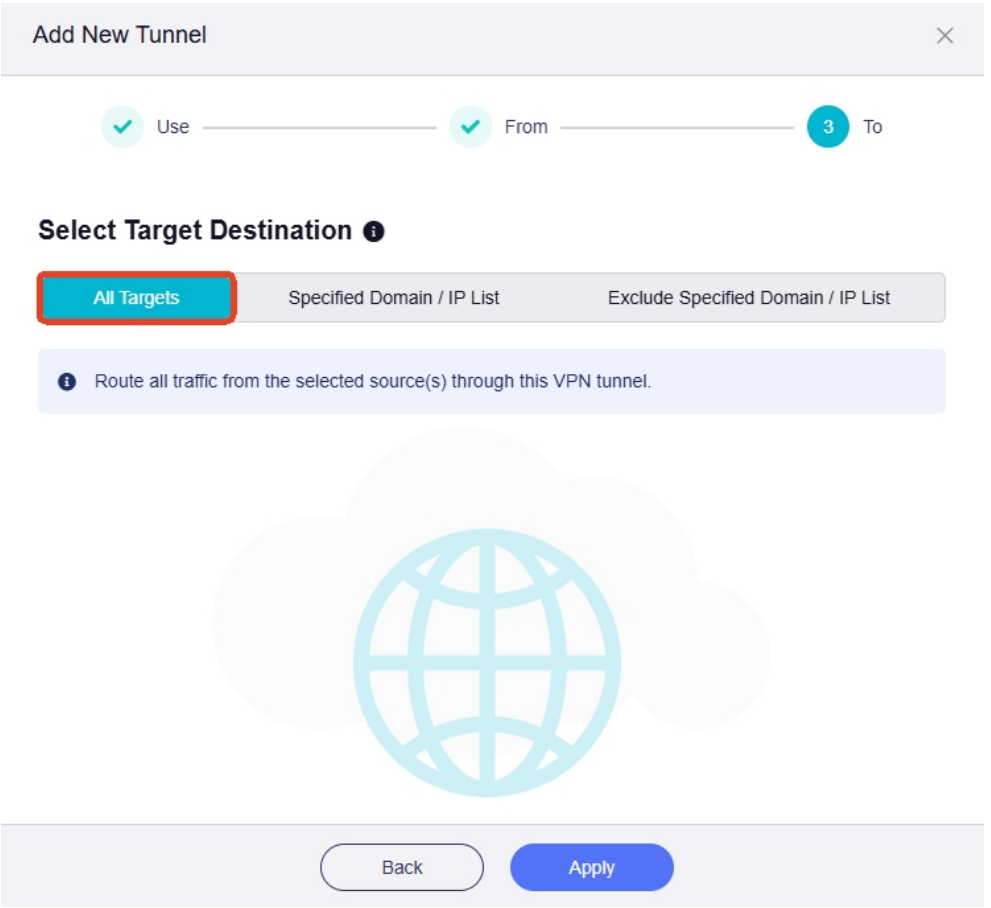
2. Seleccione la fuente del cliente.

   Haga clic en la pestaña **Dispositivos especificados** . seleccione dispositivos que usarán la VPN y luego haga clic en **Siguiente**.

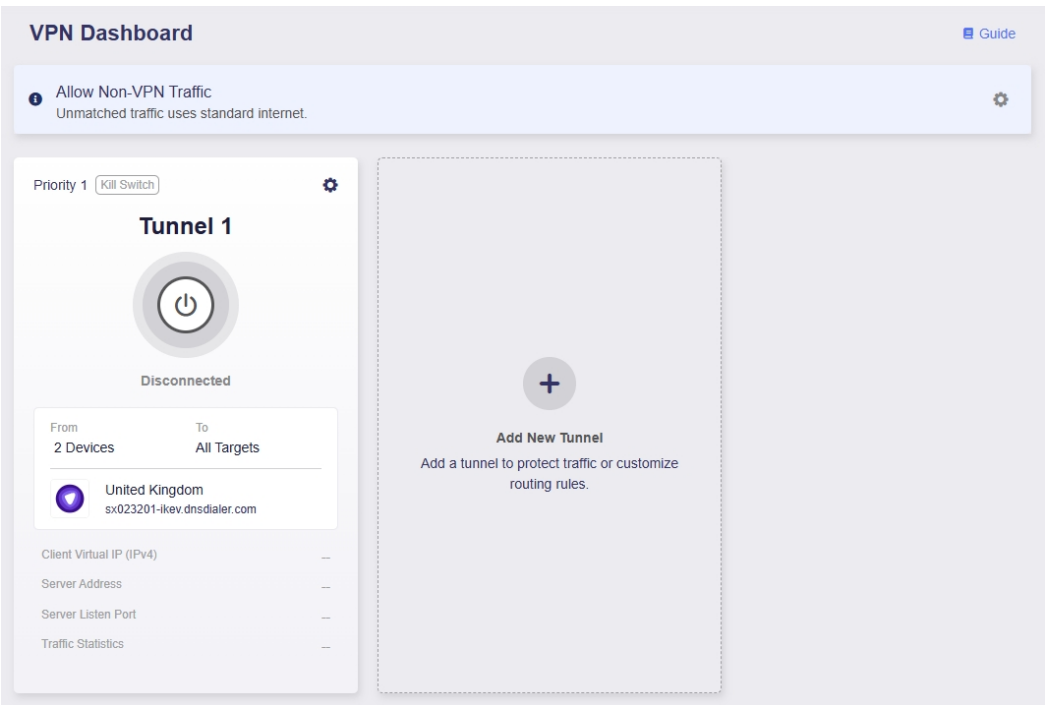


3. Seleccione el destino de destino.

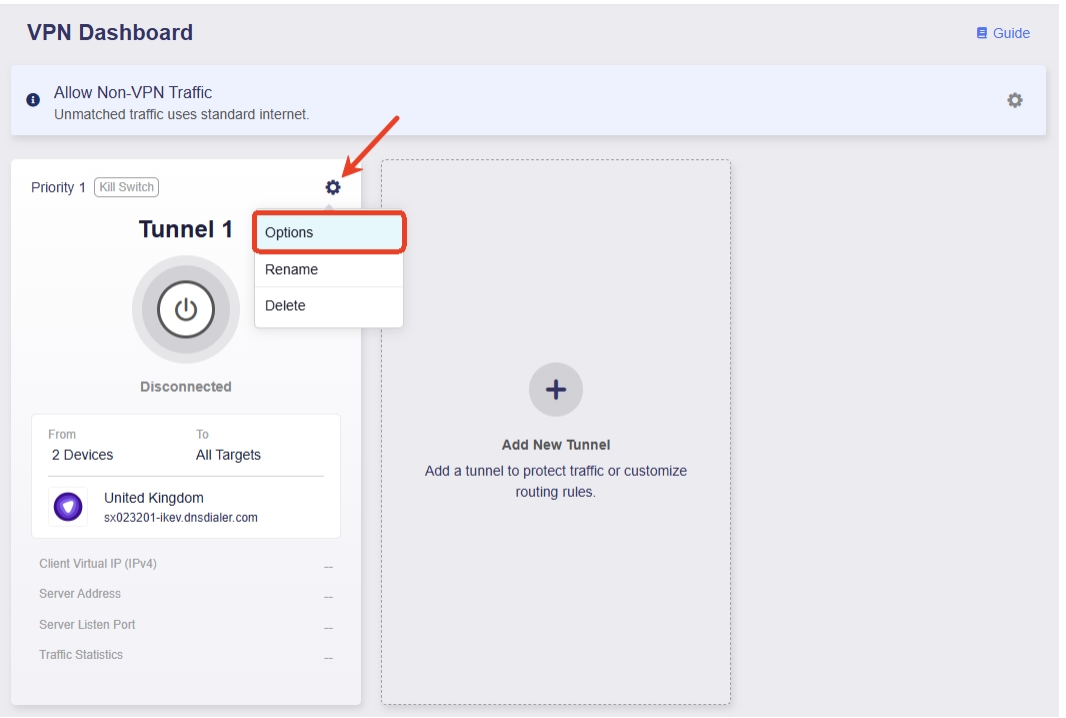
   Haga clic en **Todos los objetivos** , configúrelo como destino del tráfico y luego haga clic en **Aplicar**.

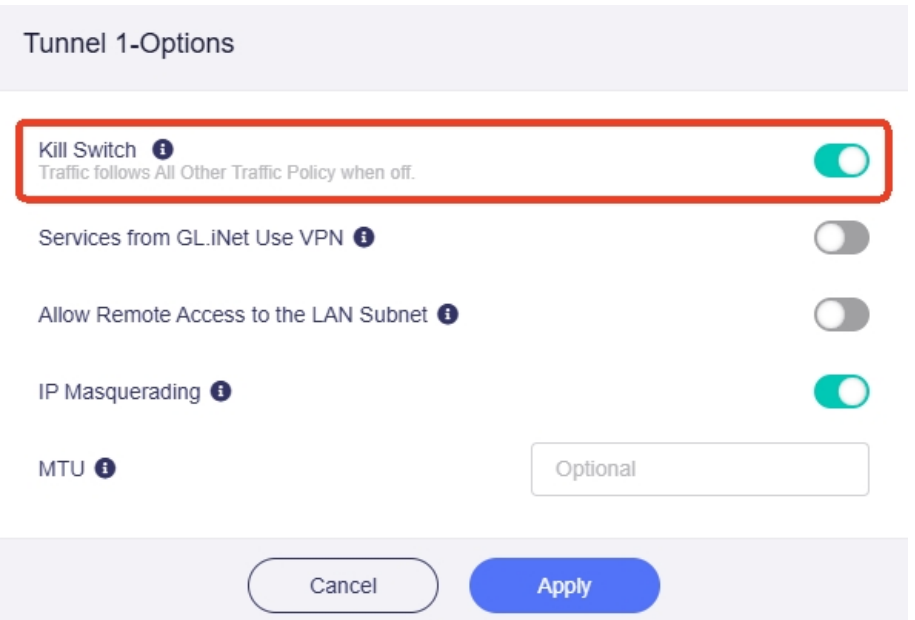


4. Se le dirigirá al panel de VPN. Ahora se ha agregado correctamente un túnel VPN, como se muestra a continuación.

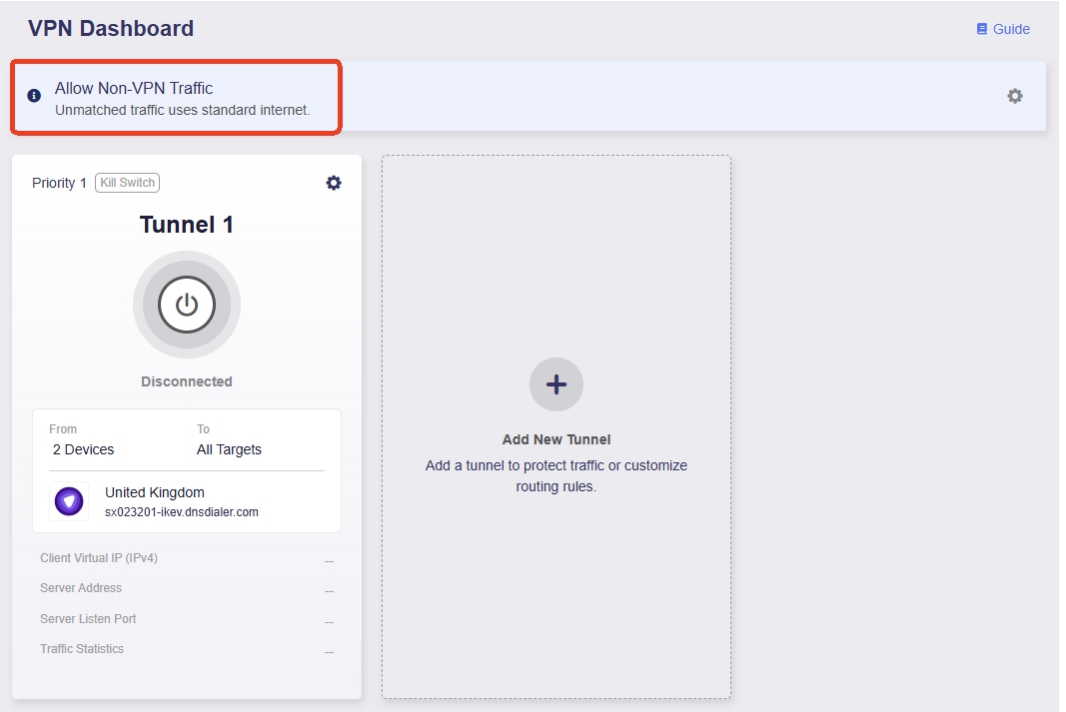


5. Asegúrese de que el **Bloqueo de tráfico sin VPN (Kill Switch)** para este túnel esté habilitado. Si la VPN se desconecta inesperadamente, se bloqueará el acceso a Internet para el tráfico que coincida con este túnel para evitar fugas de DNS y seguimiento de IP.

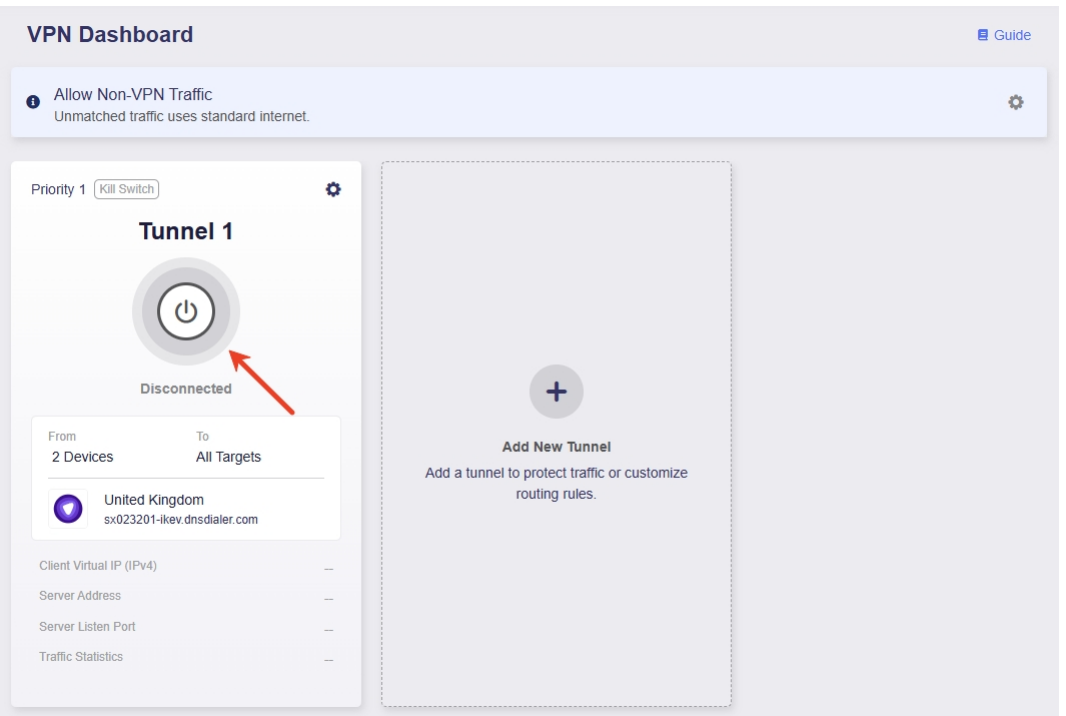




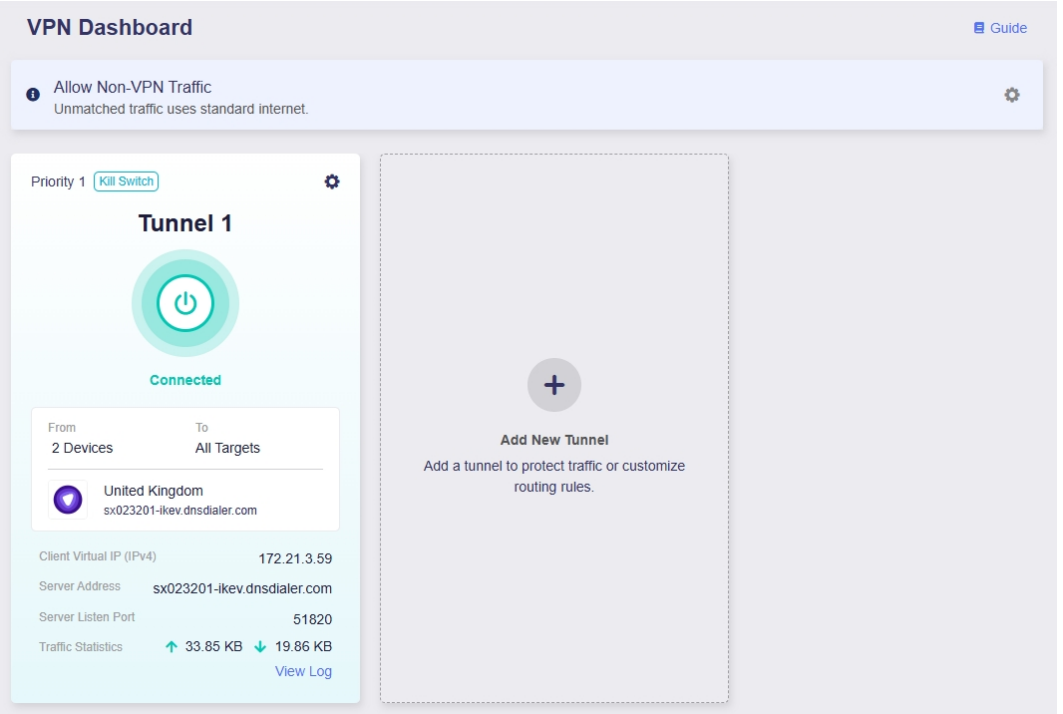
6. Asegúrese de que **Permitir tráfico que no sea VPN** está habilitado. Esto está habilitado de forma predeterminada para garantizar que el tráfico que no coincida con el túnel VPN aún pueda acceder a Internet a través de la WAN local.



7. Haga clic en el botón central para activar este túnel.



8. Una vez conectado, la página mostrará los detalles de la conexión VPN, incluida la política de VPN, las estadísticas de tráfico, la dirección del servidor, el puerto de escucha y la dirección IP virtual.



Ahora, solo dos dispositivos específicos acceden a Internet a través de VPN. Si la VPN se desconecta inesperadamente, se bloqueará el acceso a Internet de estos dispositivos para evitar fugas de DNS y seguimiento de IP. Todos los demás dispositivos accederán a Internet a través de la WAN local.

Caso 2: enrute todos los dispositivos a través de VPN 1 para sitios web específicos y enrute todo el tráfico restante a través de VPN 2.

Requisitos:

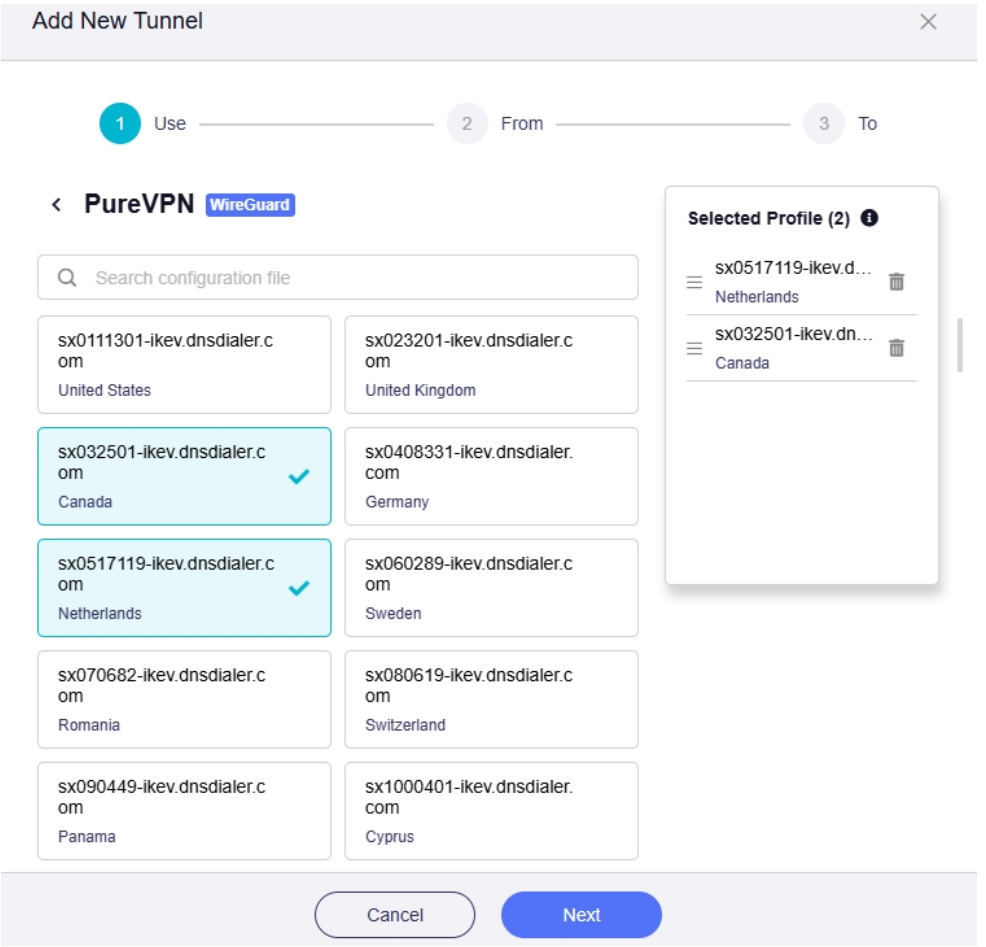
1. Todos los dispositivos utilizan VPN Tunnel 1 al acceder a dominios de redes sociales y servicios de streaming específicos, y use VPN Tunnel 2 para todos los demás accesos a Internet.
2. Si los túneles VPN se desconectan inesperadamente, el acceso a Internet para todos los dispositivos se bloqueará para evitar fugas de DNS y seguimiento de IP.

Pasos de configuración:

1. Seleccione el perfil VPN para el túnel 1.
   Si inició sesión con alguna credencial de servicio VPN integrado o cargó un archivo de configuración, los perfiles disponibles se enumerarán aquí. De lo contrario, vaya a **Perfil**

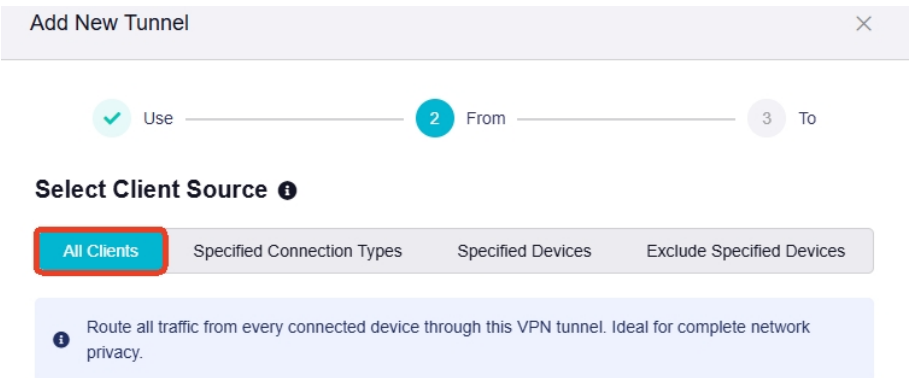
de cliente VPN para iniciar sesión con sus credenciales o cargar un archivo de configuración manualmente.

Tome PureVPN como ejemplo. Seleccione uno o varios perfiles y ajuste su prioridad a la derecha si es necesario, luego haga clic en **Siguiente**.



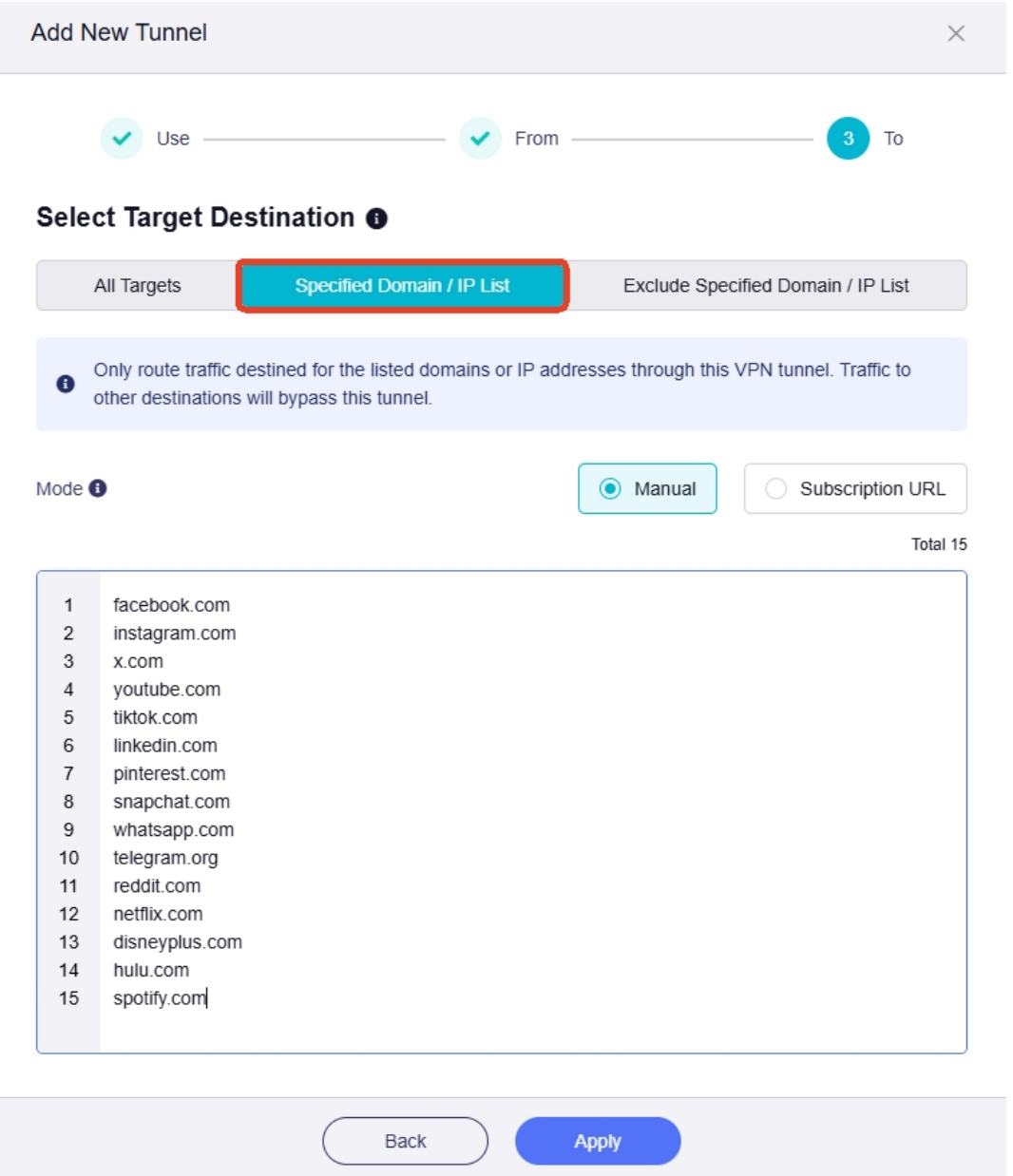
2. Seleccione la fuente del cliente.

   Haga clic en la pestaña **Todos los clientes** , configúrelo como origen del cliente para el túnel 1 y luego haga clic en **Siguiente**.

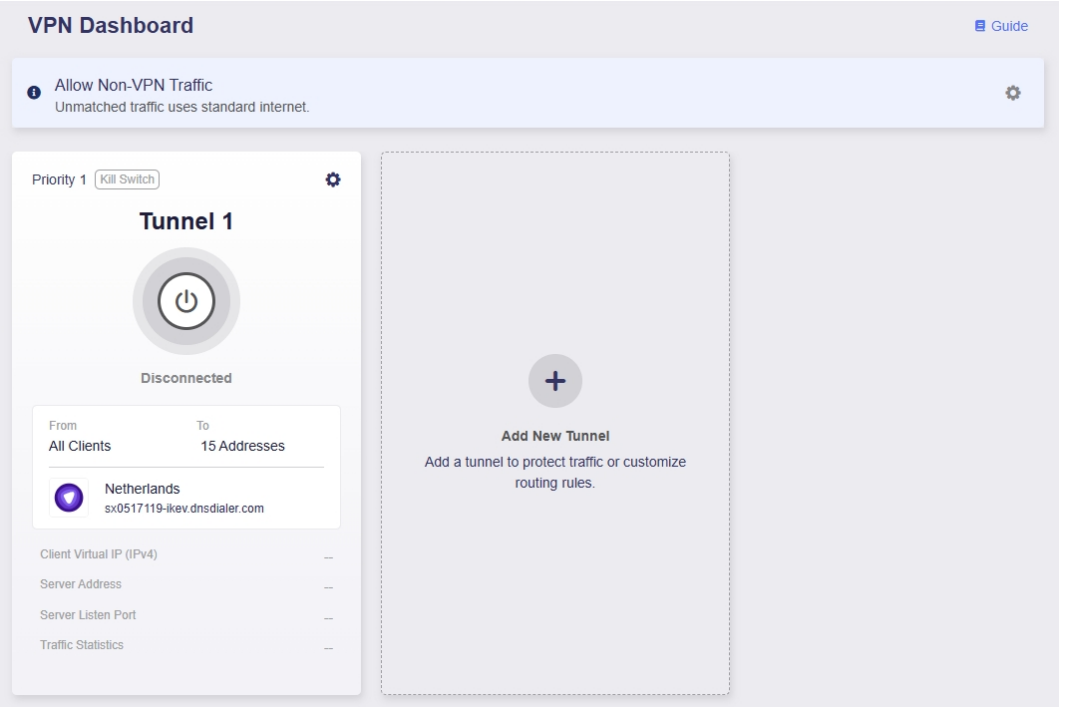


3. Seleccione el destino de destino.

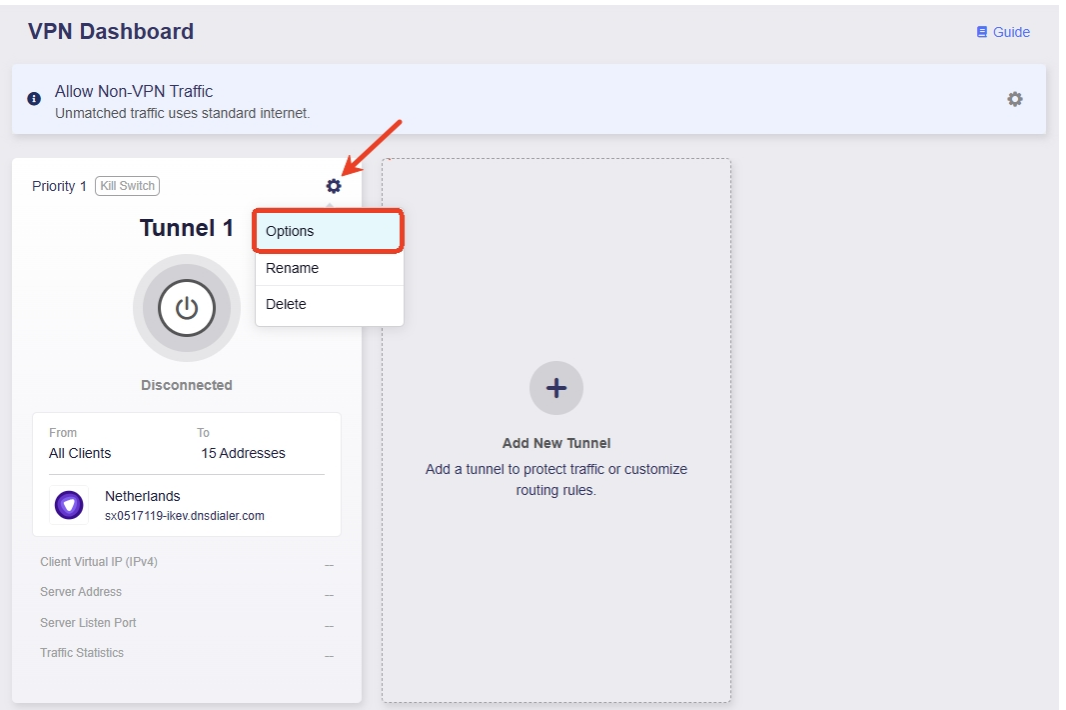
   Haga clic en la pestaña **Lista de direcciones IP/dominio especificada** , ingrese los dominios de algunas redes sociales y servicios de streaming comunes, como se muestra a continuación, luego haga clic en **Aplicar**.

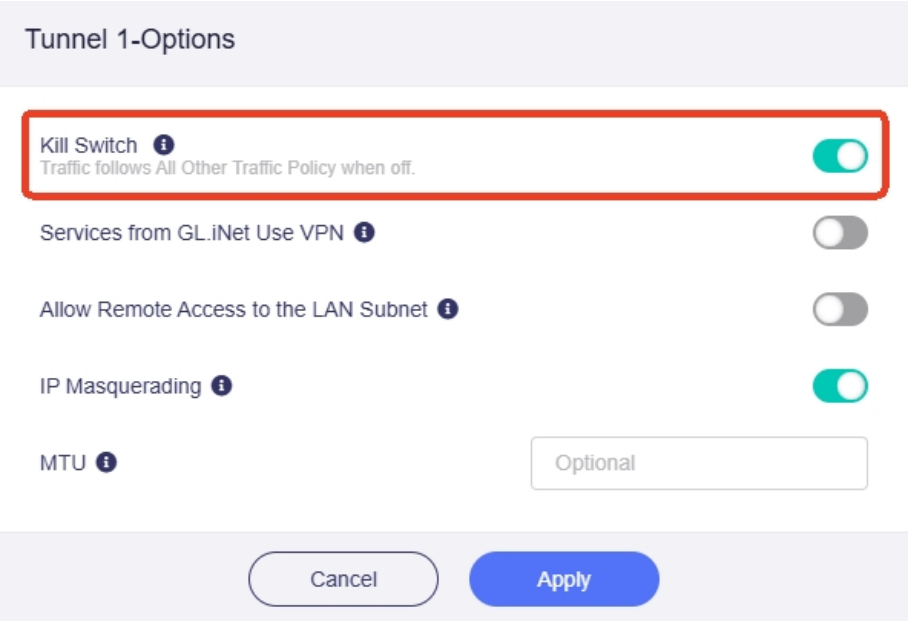


4. Se le dirigirá al panel de VPN. Ahora el túnel VPN 1 se ha agregado correctamente.

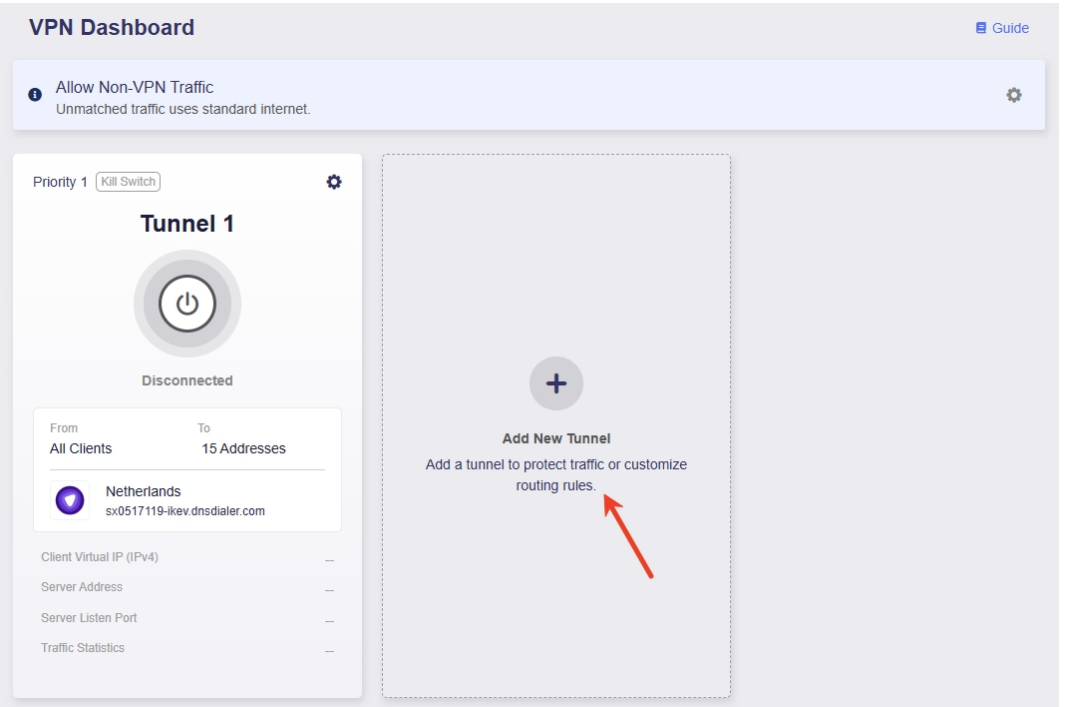


5. Asegúrese de que el **Bloqueo de tráfico sin VPN (Kill Switch)** para el túnel 1 está habilitado. Si la VPN se desconecta inesperadamente, se bloqueará el acceso a Internet para el tráfico que coincida con este túnel para evitar fugas de DNS y seguimiento de IP.





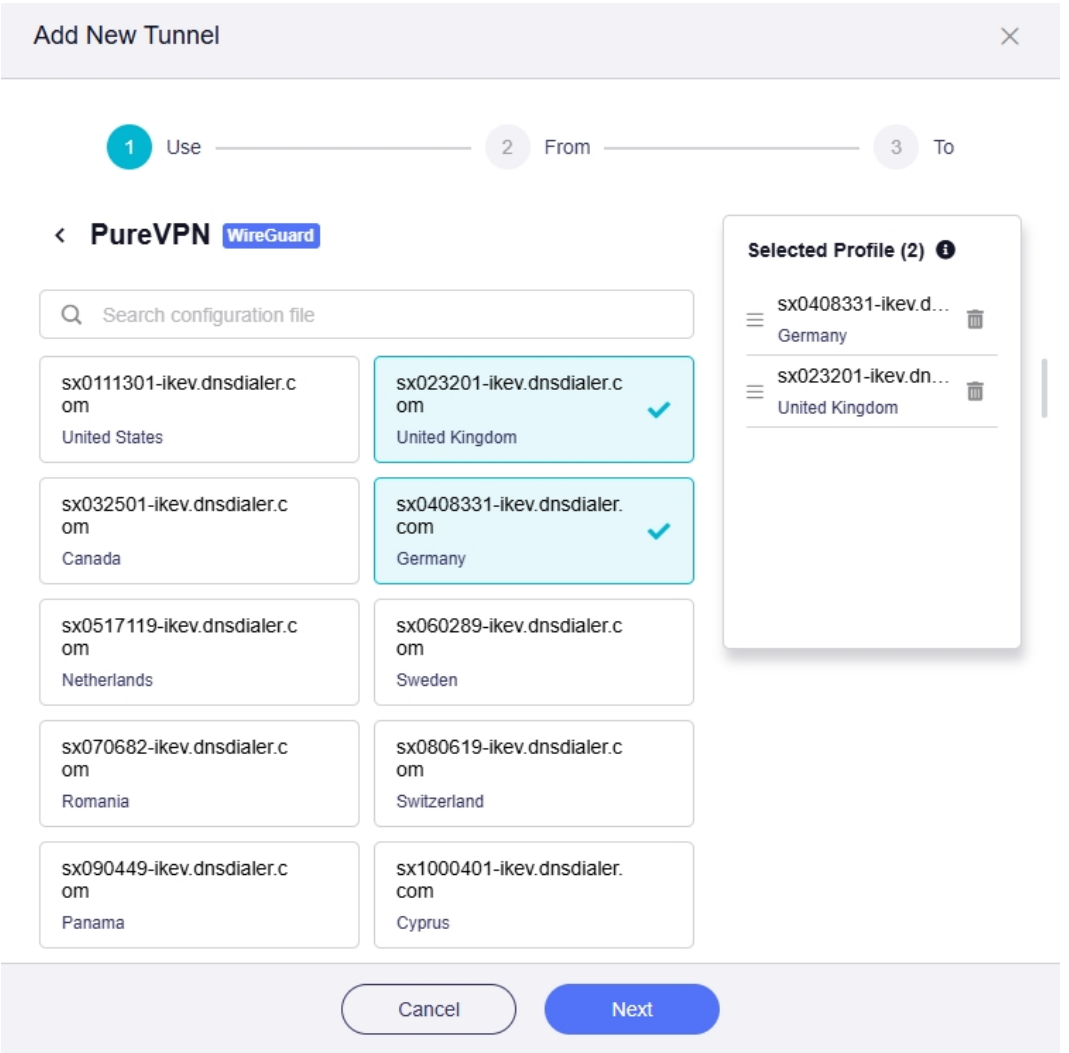
6. Haga clic en **Agregar nuevo túnel** para agregar el túnel 2.



7. Seleccione el perfil de VPN para el túnel 2.

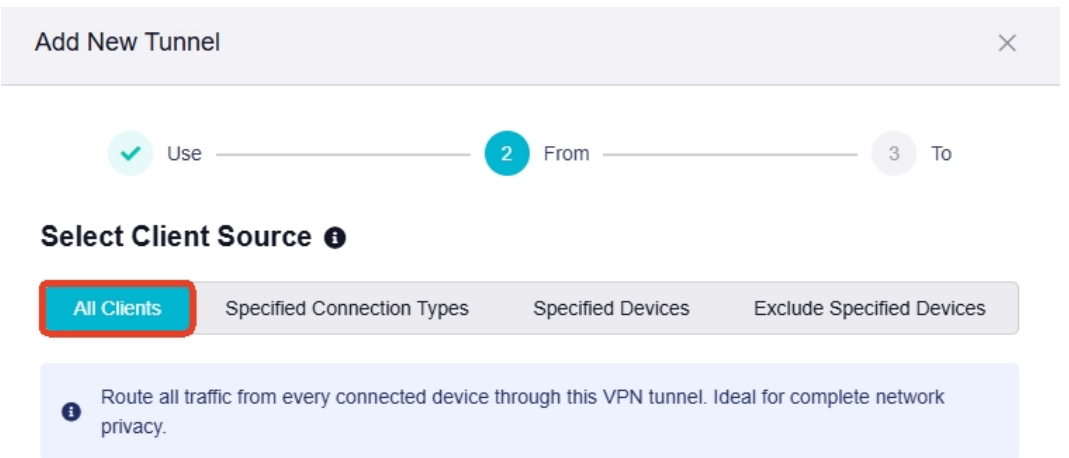
   Seleccione uno o varios perfiles y ajuste su prioridad a la derecha si es necesario.

   Tcuando haga clic **Siguiente**.



8. Seleccione la fuente del cliente.

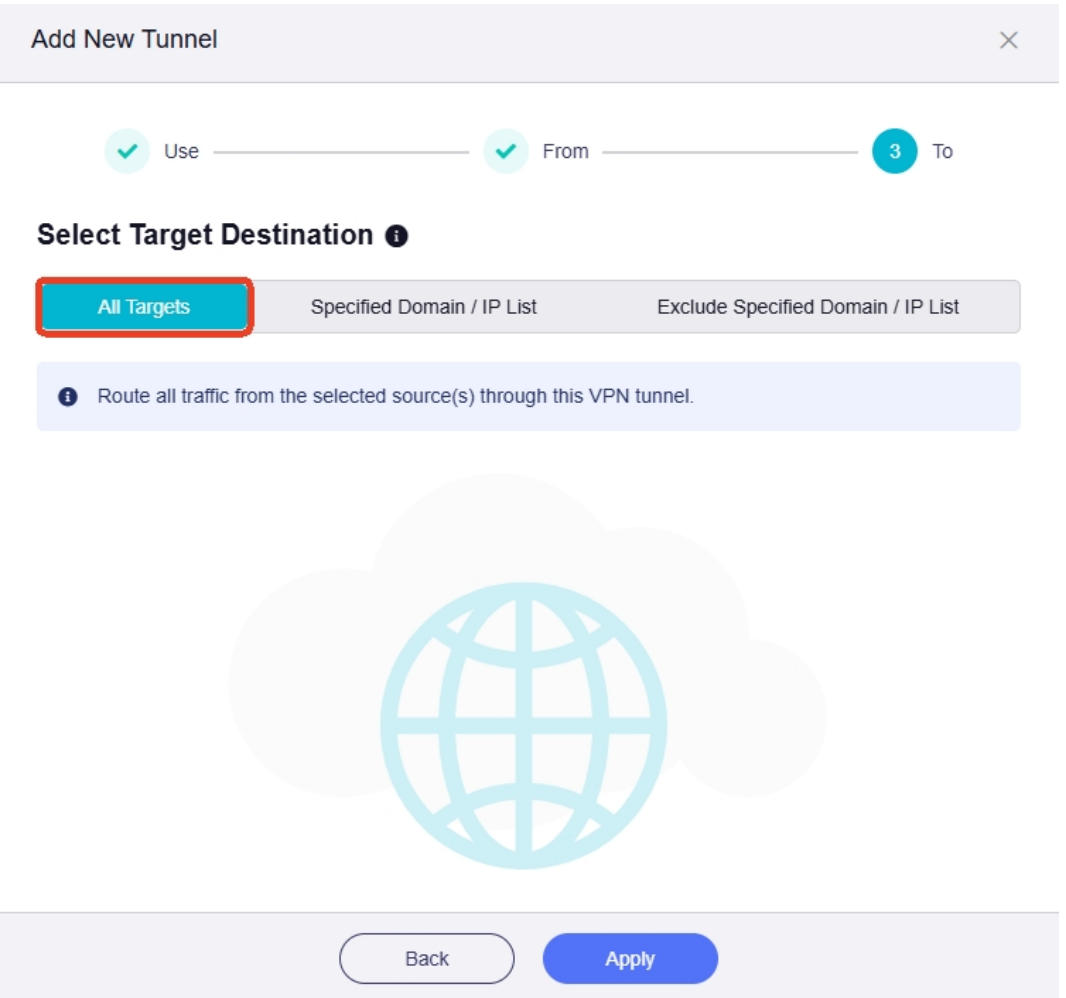
Haga clic en la pestaña **Todos los clientes** , configúrela como la fuente del cliente para el Túnel 2 y luego haga clic en **Siguiente**.



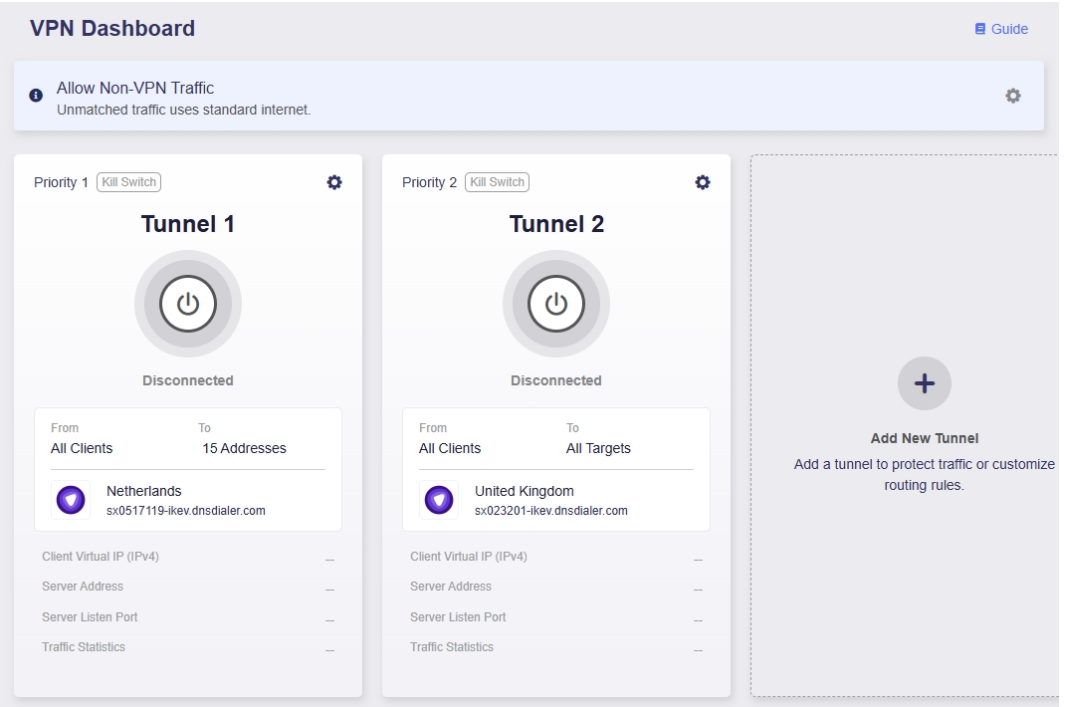


9. Seleccione el destino de destino.

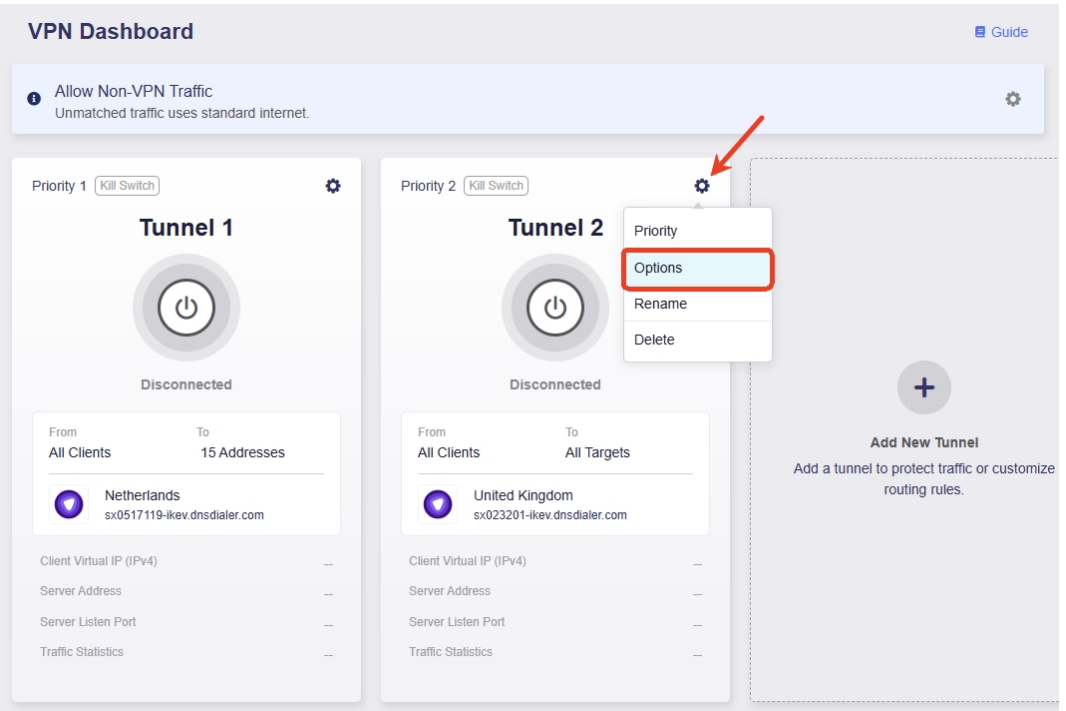
Haga clic en la pestaña **Todos los destinos** , configúrelo como destino del tráfico para el túnel 2 y luego haga clic en **Aplicar**.

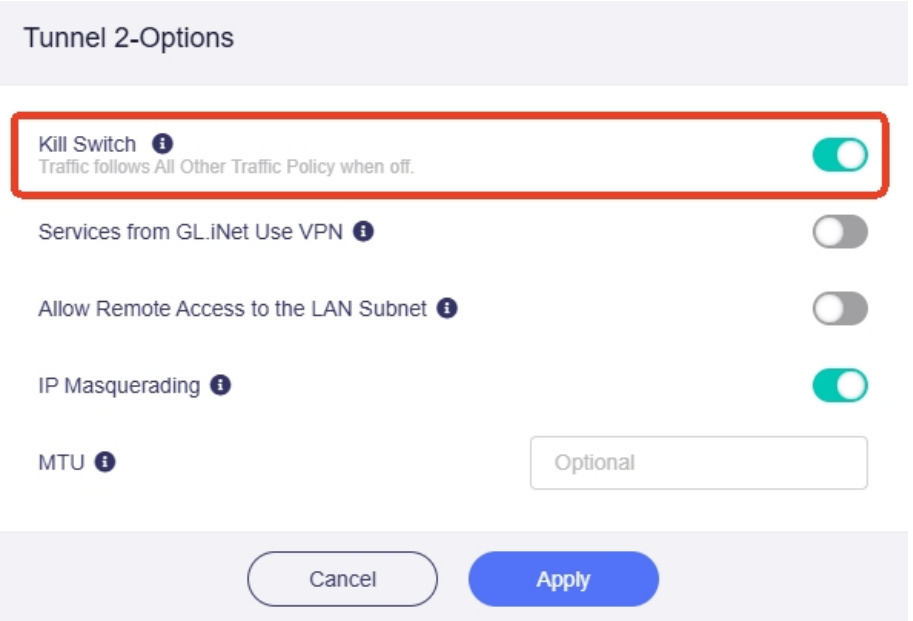


10. Se le dirigirá al panel de VPN. Ahora el túnel VPN 2 se ha agregado correctamente.

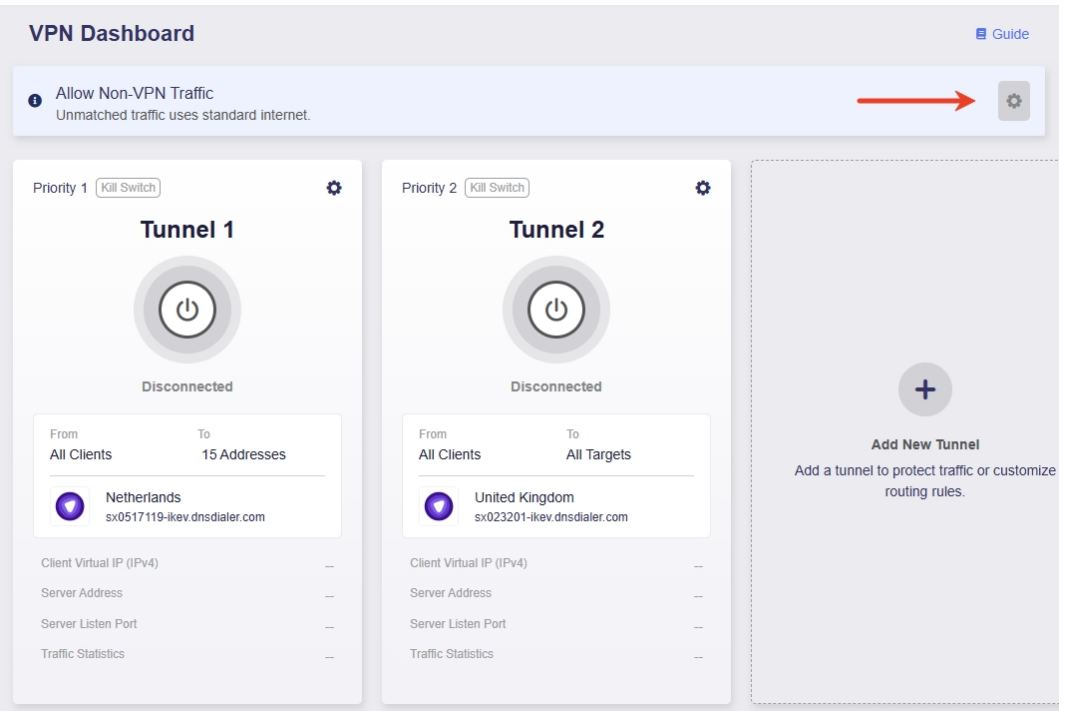


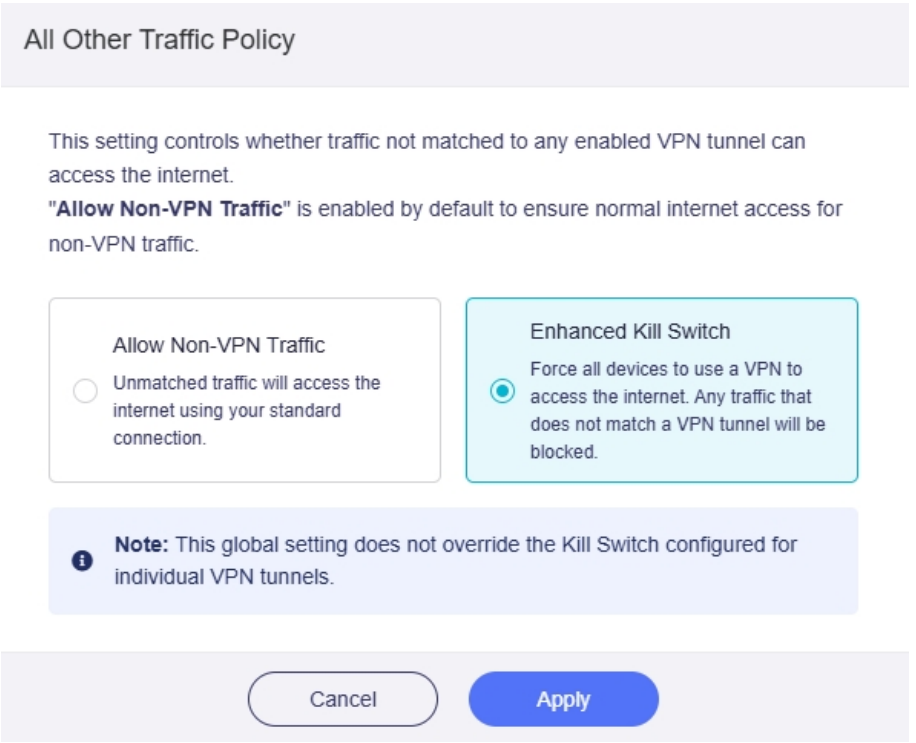
11. Asegúrese de que el **Bloqueo de tráfico sin VPN (Kill Switch)** para el túnel 2 está habilitado. Si la VPN se desconecta inesperadamente, se bloqueará el acceso a Internet para el tráfico que coincida con este túnel para evitar fugas de DNS y seguimiento de IP.



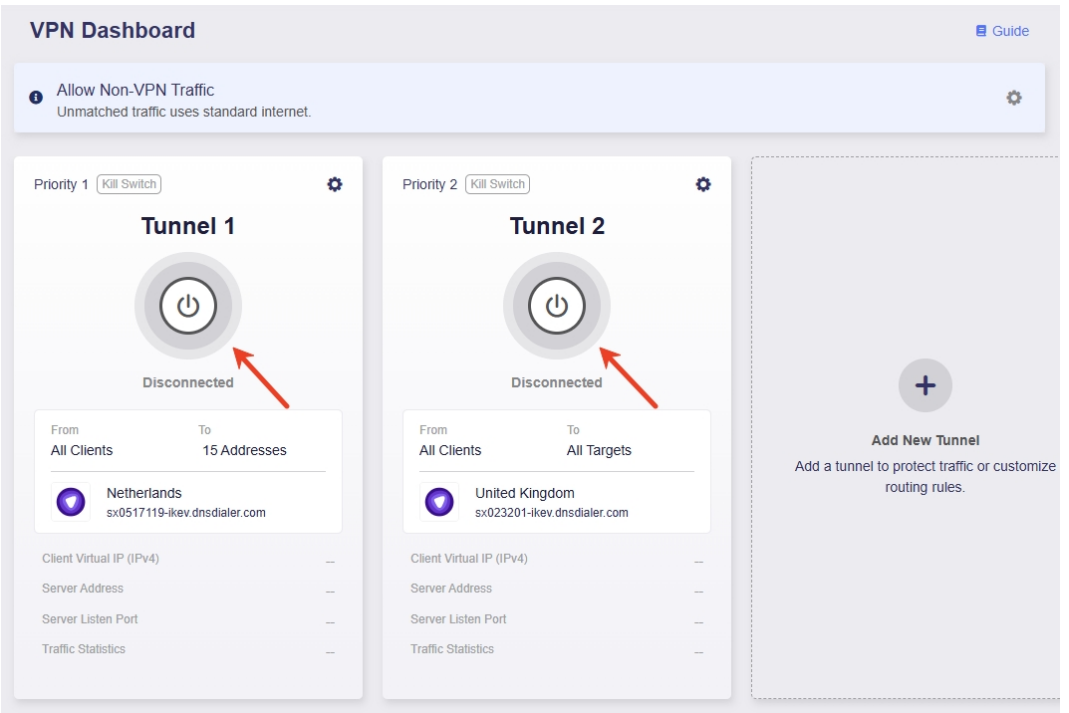


12. Haga clic en el ícono de ajustes en la parte superior derecha para habilitar **Interruptor de apagado mejorado**. Esto garantiza que todo el tráfico debe acceder a Internet a través de la VPN.

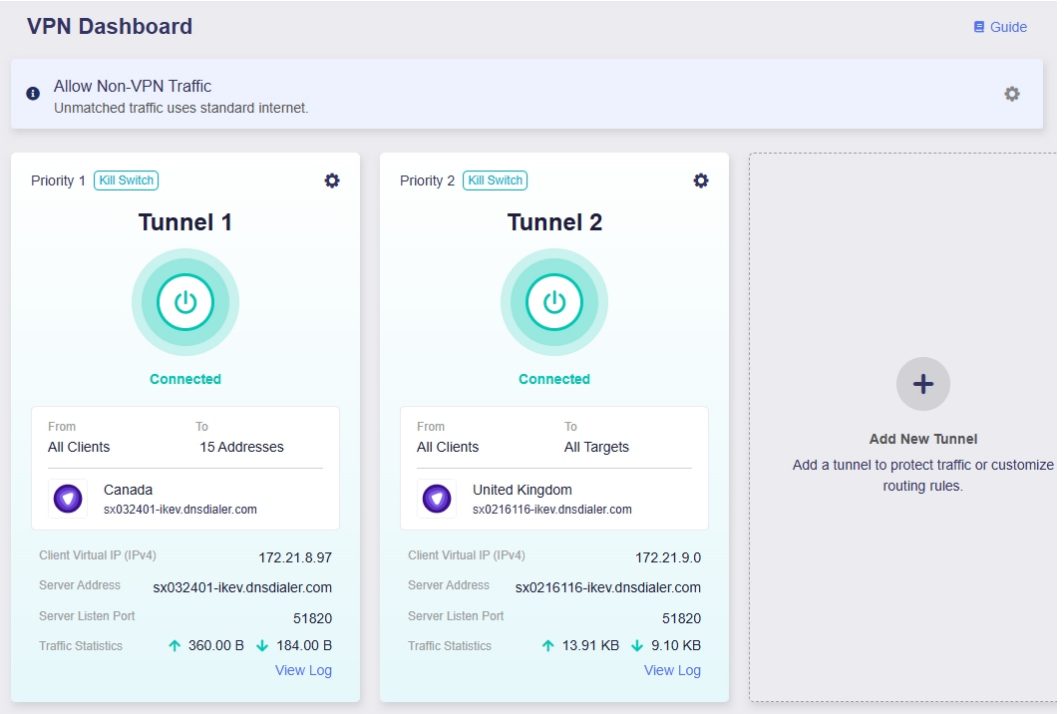




13. Haga clic en el botón central para activar el túnel 1 y el túnel 2.



14. Una vez conectado, la página mostrará los detalles de la conexión VPN, incluida la política de VPN, las estadísticas de tráfico, la dirección del servidor, el puerto de escucha y la dirección IP virtual.



Ahora, todos los dispositivos utilizarán el túnel VPN. 1 al acceder a dominios específicos y utilice VPN Tunnel 2 para todos los demás accesos a Internet. Si los túneles VPN se desconectan inesperadamente, se bloqueará el acceso a Internet para todos los dispositivos para evitar fugas de DNS y seguimiento de IP.

9.3 Bloqueo de tráfico sin VPN (Kill Switch)

Kill Switch es una característica de seguridad para conexiones VPN. Corta automáticamente todo el acceso a Internet para su red local si la conexión VPN se cae inesperadamente, evitando que su dirección IP real y sus datos en línea queden expuestos y garantizando privacidad y seguridad continuas. Esta característica es particularmente útil para mantener un acceso a Internet seguro y anónimo, como cuando se utilizan redes públicas, se procesan datos confidenciales o se oculta su dirección IP real.

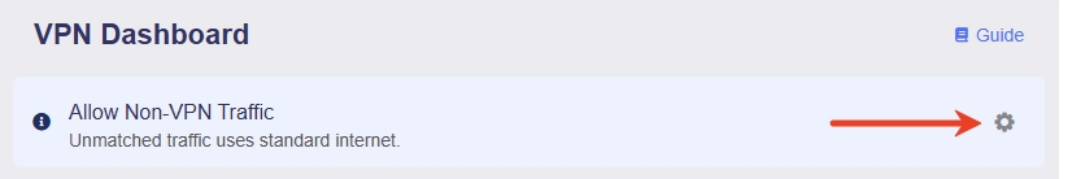
Cuando está habilitada, bloquea cualquier tráfico de cliente que intente evitar el túnel VPN, deteniendo efectivamente las fugas de VPN causadas por problemas de configuración de DNS, desconexiones inesperadas, solicitudes de IP directas y otros escenarios similares.

Desde el firmware v4.8, GL.iNet Los enrutadores admiten la configuración Kill Switch para la conexión VPN global, así como para cada túnel VPN individual.

- Para configurar Kill Switch para la conexión VPN global, consulte Todo el resto del tráfico.
- Para configurar Kill Switch para cada túnel VPN individual, consulte Opciones de túnel.

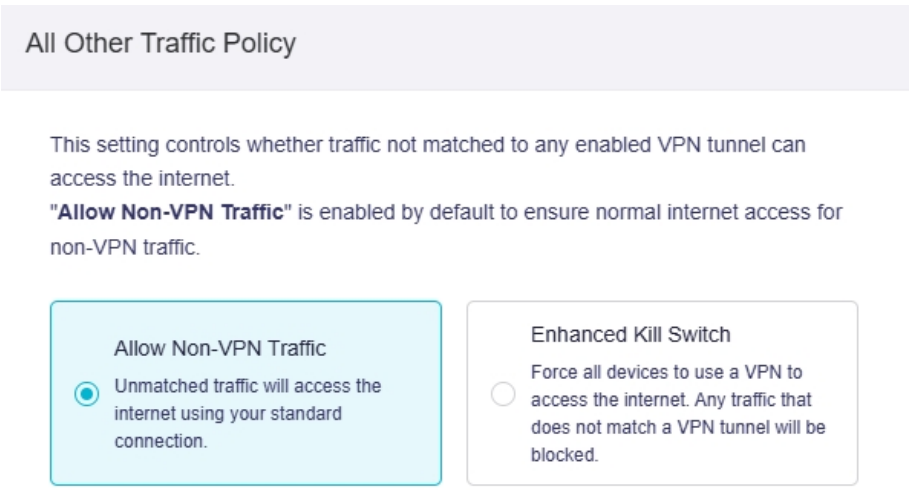
9.4 Todo el resto del tráfico

Haga clic en el ícono de ajustes en la parte superior derecha para configurar la política para tráfico que no coincide con el túnel VPN.

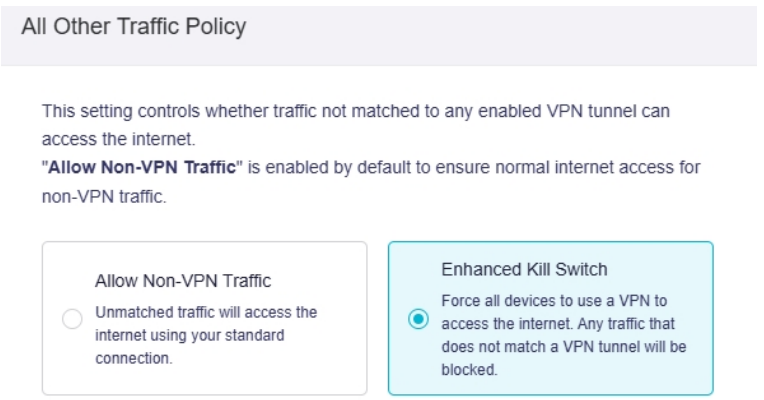


Esta política controla si el tráfico que no coincide con ninguno de sus grupos de túneles VPN puede acceder a Internet o no. Tiene dos opciones:

- **Permitir tráfico que no sea VPN**: Habilitado de forma predeterminada para garantizar el acceso normal a Internet para personas que no son VPN tráfico.



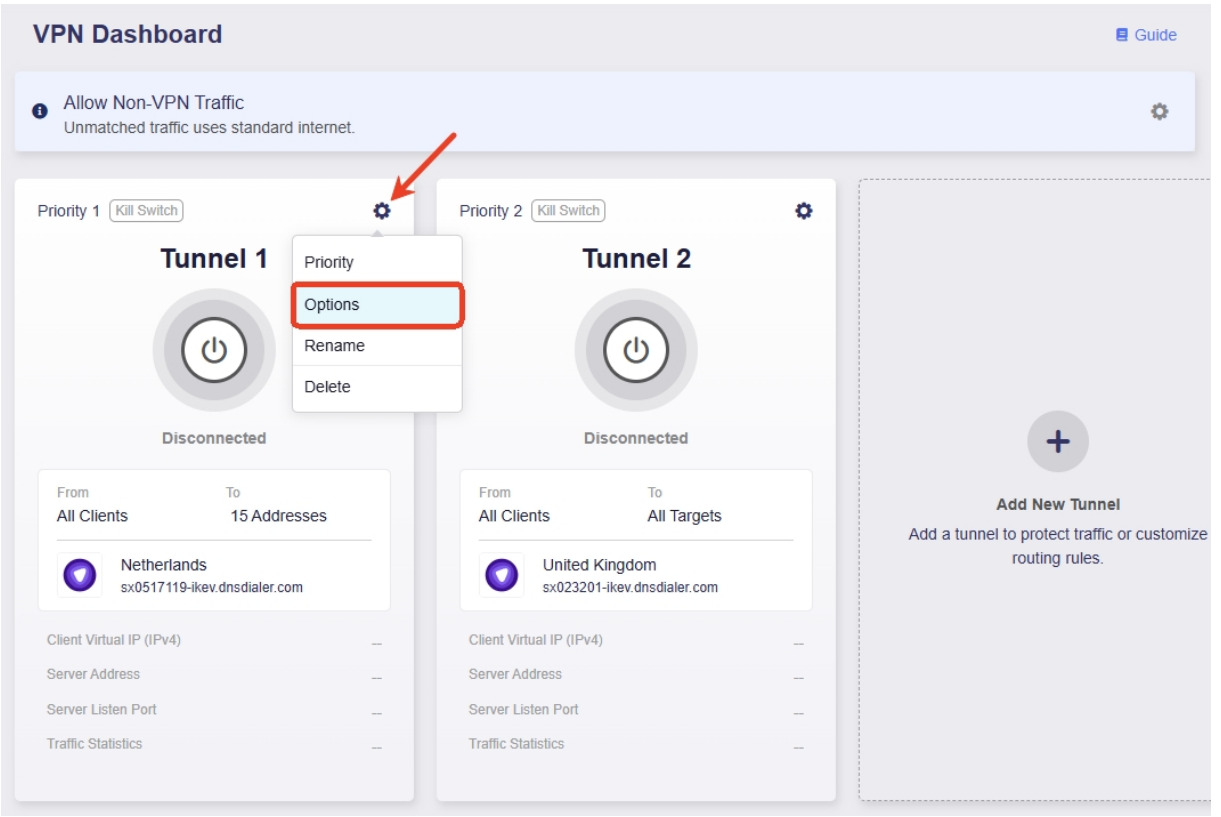
- **Interruptor de interrupción mejorado**: obliga a todos los dispositivos a acceder a Internet a través de una VPN. Se bloqueará cualquier tráfico que no coincida con un túnel VPN. Esta configuración global no anula el interruptor de interrupción configurado para túneles VPN individuales.

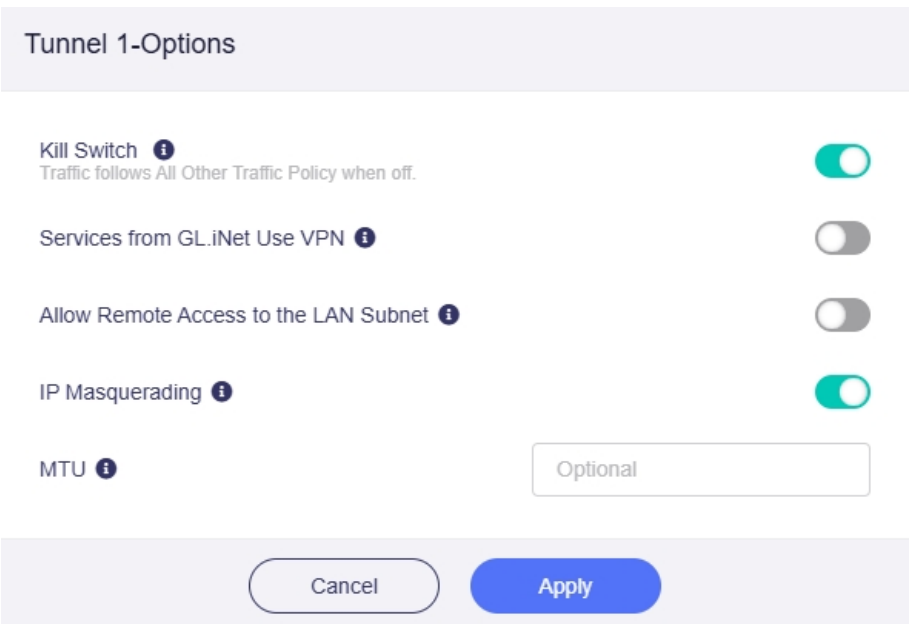


9.5 Opciones de túnel

Puede configurar ajustes avanzados para cada túnel VPN, como el interruptor de interrupción de VPN, enmascaramiento de IP y MTU.

Haga clic en el ícono de ajustes en un grupo de túneles y seleccione **Opciones**.

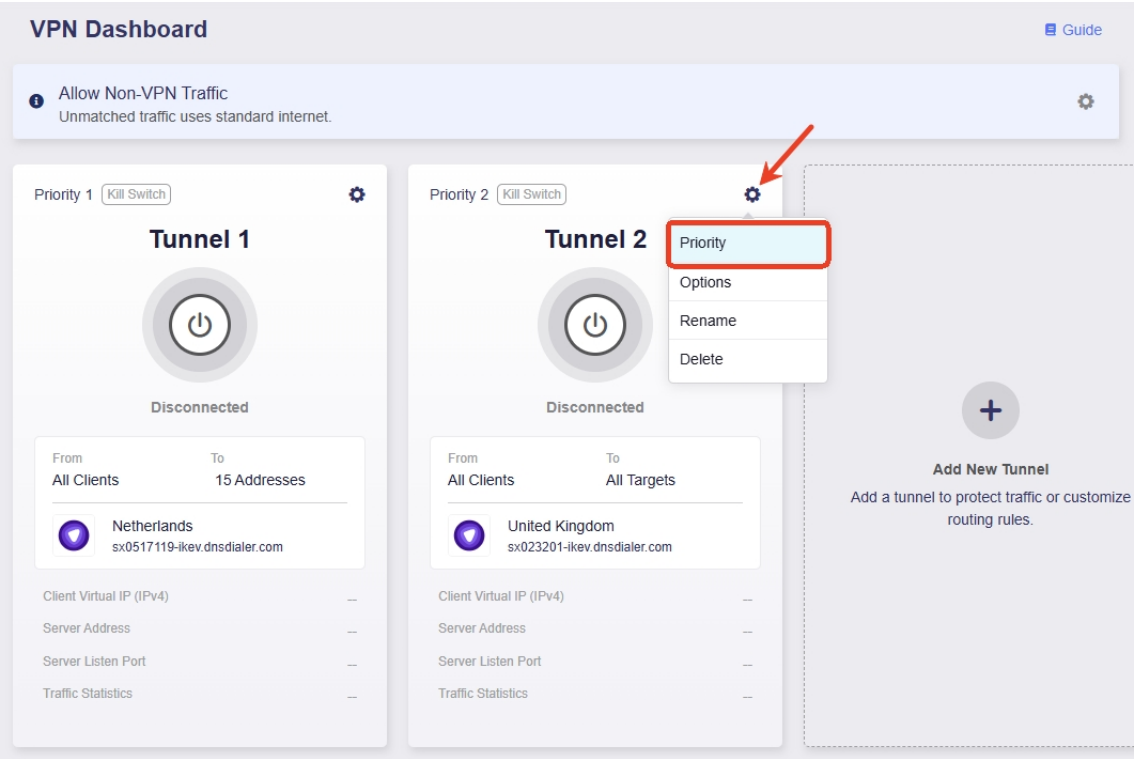




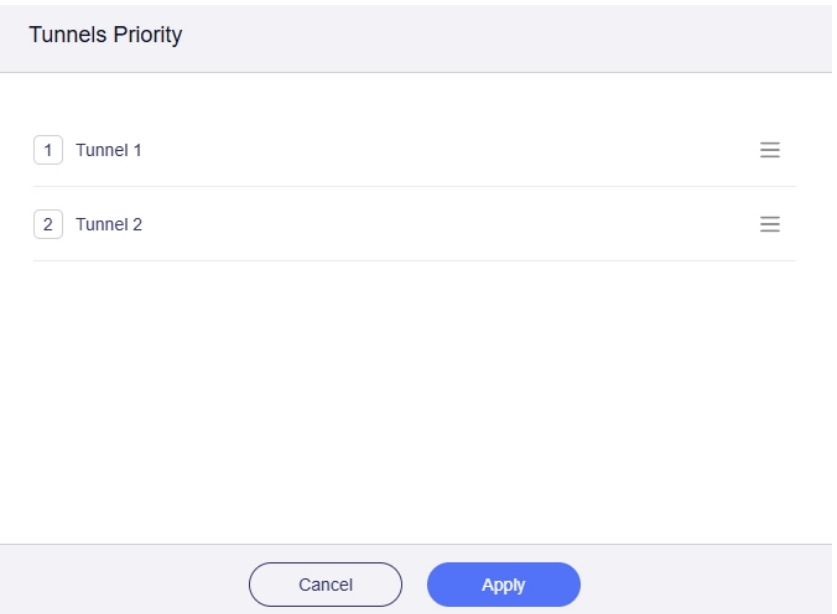
- **Bloqueo de tráfico sin VPN (Kill Switch)**: si está habilitado, el tráfico que coincida con este túnel VPN se bloqueará si la conexión VPN falla inesperadamente. Si está deshabilitado, dicho tráfico pasará por error al túnel Todo el resto del tráfico .
- **Los servicios de GL.iNet usan VPN**: si están habilitados, los servicios GoodCloud, DDNS y rtty transmitirán paquetes a través de túneles VPN. Esta opción está deshabilitada de forma predeterminada, ya que estos servicios normalmente requieren la dirección IP real del dispositivo para funcionar correctamente.
- **Permitir acceso remoto a la subred LAN**: si está habilitado, se permitirá el acceso remoto a este enrutador y sus dispositivos LAN a través de la VPN. Requiere que el servidor VPN anuncie una ruta de regreso a su subred LAN.
- **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**: el valor de MTU que establezca para el túnel anulará la configuración de MTU en el archivo de configuración.

9.6 Prioridad del túnel

Para ajuste la prioridad del túnel, haga clic en el ícono de ajustes en un grupo de túneles y seleccione **Prioridad**.



Haga clic y mantenga presionado el ícono de tres líneas a la derecha para reordenar los túneles, luego haga clic en **Aplicar**.



Cuando se habilitan varios túneles, el enrutador enruta el tráfico de acuerdo según las siguientes reglas:

1. El tráfico intentará primero coincidir con la regla de túnel de mayor prioridad. Si coincide, será encaminado a través de ese túnel; de lo contrario, intentará el siguiente túnel de prioridad, y así sucesivamente.
2. Cada grupo de túneles funciona de forma independiente. Una vez que el tráfico coincida con una regla de túnel, se enrutará a través de ese túnel y no realizará conmutación por error entre grupos de túneles.
3. Se pueden seleccionar varios perfiles dentro de cada grupo de túneles para habilitar la conmutación por error dentro del túnel. Cuando el perfil de mayor prioridad en un grupo de túneles deja de funcionar, el túnel se conectará automáticamente usando el segundo perfil de mayor prioridad, y así sucesivamente.
4. Si un túnel VPN se desconecta inesperadamente, el sistema determinará si se debe realizar una conmutación por error del tráfico al túnel Todo el resto del tráfico en función de si el **Bloqueo de tráfico sin VPN (Kill Switch)** está habilitado.
    - Si el interruptor de interrupción está habilitado, el tráfico se bloqueará y no conmutará por error al túnel para todo el resto del tráfico.
    - Si el interruptor de interrupción está deshabilitado, el tráfico se conmutará por error al túnel para el resto de tráfico.
5. En el túnel **Todo el resto del tráfico** , diferentes modos determinan si el tráfico que no coincide con el túnel VPN puede acceder a Internet.
    - **Permitir tráfico que no sea VPN**: está habilitado de forma predeterminada para garantizar que el tráfico que no coincide con los túneles VPN aún puede acceder a Internet a través de la WAN local.
    - **Kill Switch mejorado**: Obliga a todos los dispositivos a acceder a Internet a través de una VPN. Se bloqueará cualquier tráfico que no coincida con un túnel VPN. Esta configuración global no anula el Kill Switch configurado para túneles VPN individuales. En resumen, fortalece el Kill Switch y bloquea el acceso regular a Internet para evitar fugas de IP.

Capítulo 10

Configurar el servidor VPN

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

10.1 Configurar el servidor OpenVPN

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

10.1.1 Preparación

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

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

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

   Métodos alternativos:

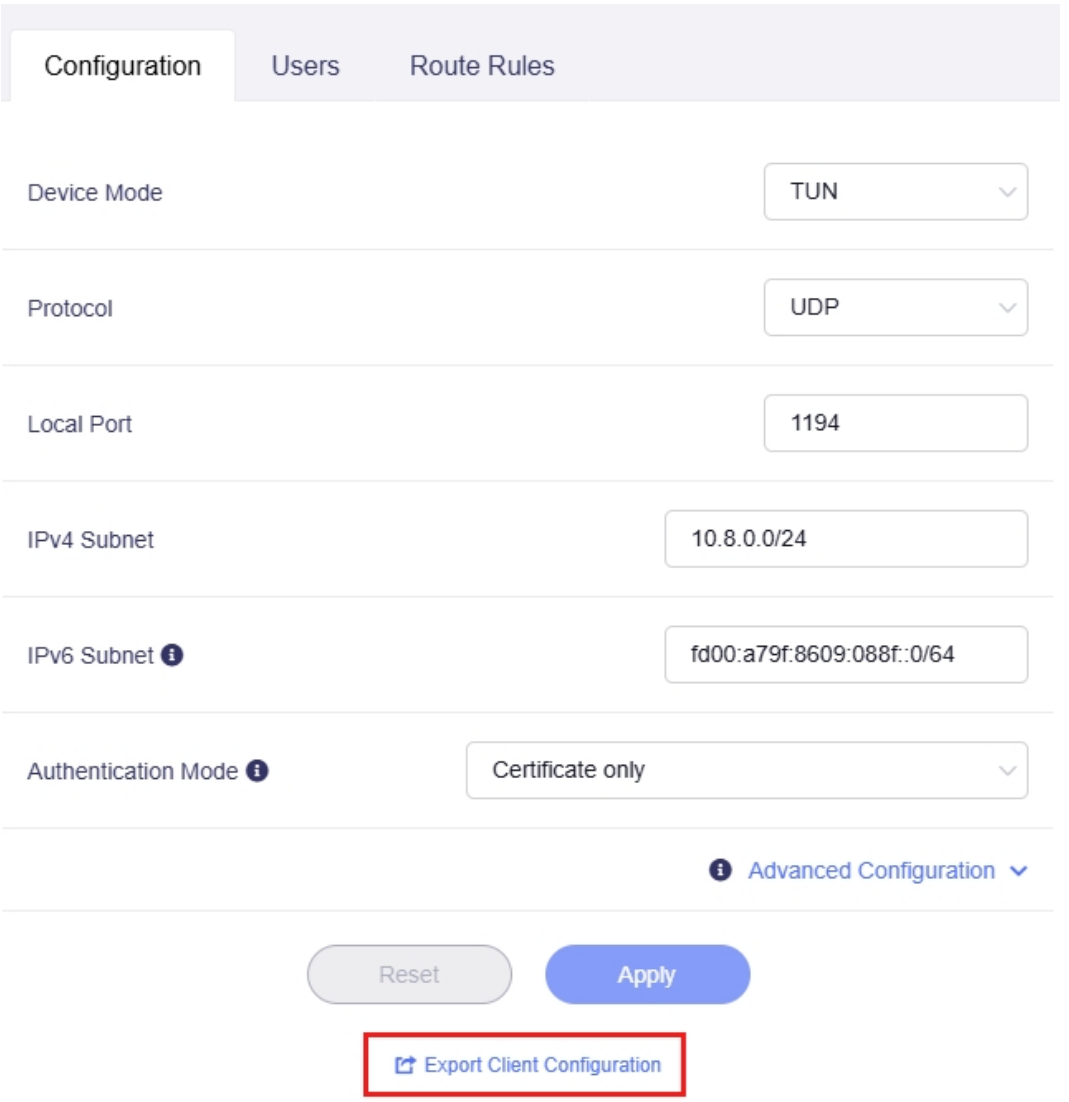
   - Si tiene un enrutador principal ascendente de su enrutador GL.iNet, inicie sesión en él y verifique que tenga una dirección IP pública asignada por su ISP.
   - Solicite a su ISP una dirección IP pública. Esto puede generar una tarifa adicional.
   - Si los dos métodos anteriores no funcionan (por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

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

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

10.1.2 Pasos de configuración

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

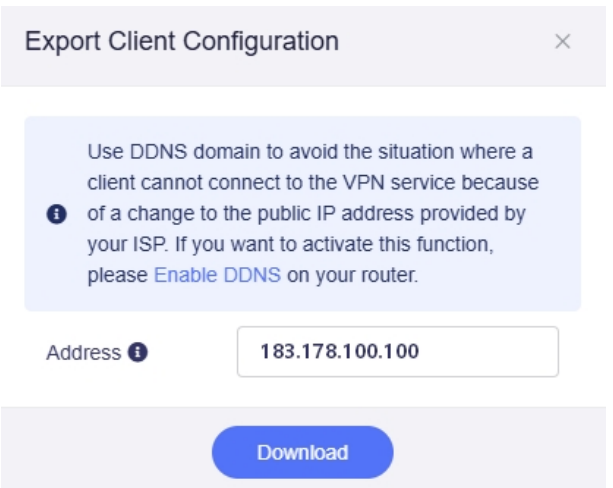


- **Modo de dispositivo**: TAP-S2S o Túnel. Consulte aquí para las diferencias.
- **Protocolo**: UDP o TCP. Consulte aquí para las diferencias.

- **Modo de autenticación**: Esto determina el método de autenticación utilizado cuando el cliente se conecta al servidor. Hay tres opciones:
  - **Solo certificado**: si se selecciona, el enrutador generará automáticamente claves de certificado de servidor y cliente y las incrustará en el archivo de configuración. Cuando carga la configuración en el cliente, no se requieren credenciales adicionales.
  - **Solo nombre de usuario/contraseña**: si se selecciona, el enrutador generará la configuración del cliente sin claves de certificado. Usted necesita primero agregue un nombre de usuario y contraseña en **Usuarios** antes de exportar la configuración del cliente. Al cargar la configuración en el cliente, ingrese estas credenciales para la autenticación.
  - **Nombre de usuario/Contraseña y Certificado**: si se selecciona, necesita agregar primero un nombre de usuario y contraseña en la pestaña **Usuarios** antes de exportar la configuración del cliente; en segundo lugar, el enrutador generará automáticamente claves de certificado de servidor y cliente y las incrustará en el archivo de configuración. Al cargar la configuración al cliente, primero se verificará la clave del certificado, seguida de la autenticación de nombre de usuario/contraseña para 2FA seguridad.
- **Configuración avanzada**: Personalizar more server settings if needed.

3. Export Client Configuration.

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

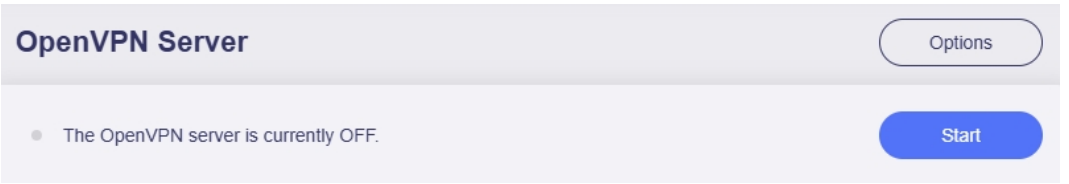


Consejos:

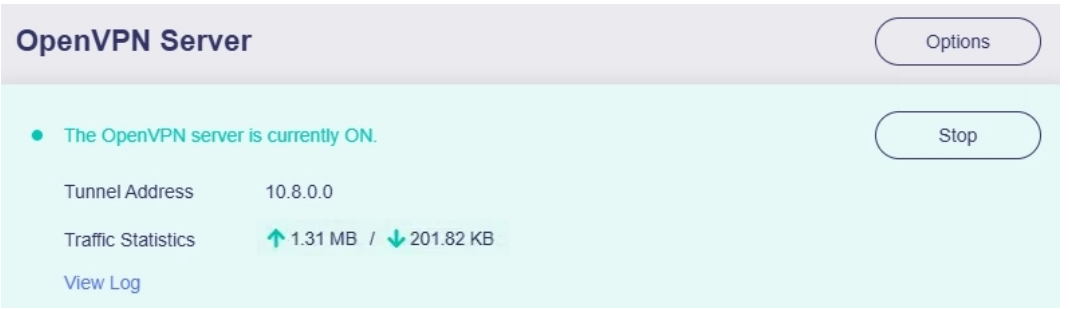
- Si su IP pública dirección cambia con frecuencia, vaya a **APLICACIONES** > **DNS dinámico** y habilite DDNS. Entonces puedes usar el dominio DDNS como su dirección de servidor.
- Desde firmware v4.8, puede seleccionar la dirección del servidor de una lista desplegable antes de exportar el archivo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

4. Inicie el servidor OpenVPN.

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



   El servidor estado de conexión se se muestra en la arriba. Si muestra estadísticas de tráfico de carga y descarga, significa que el servidor OpenVPN se está ejecutando.



10.1.3 Solución de problemas

Si la conexión falla, existen varias razones comunes:

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

10.2 Configurar el servidor WireGuard

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

10.2.1 Preparación

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

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

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

   Alternativa métodos:

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

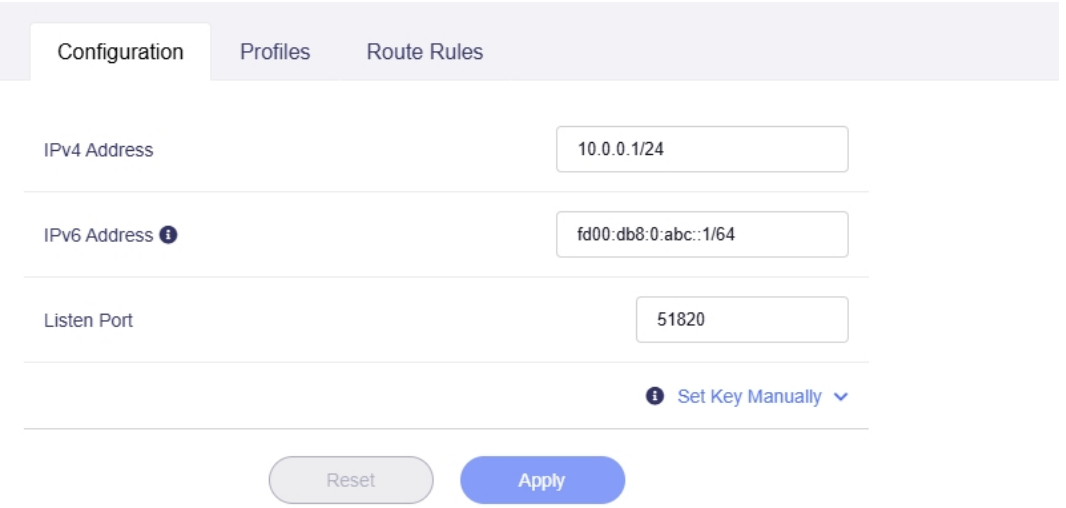
2. **Confirme si se requiere reenvío de puertos**

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

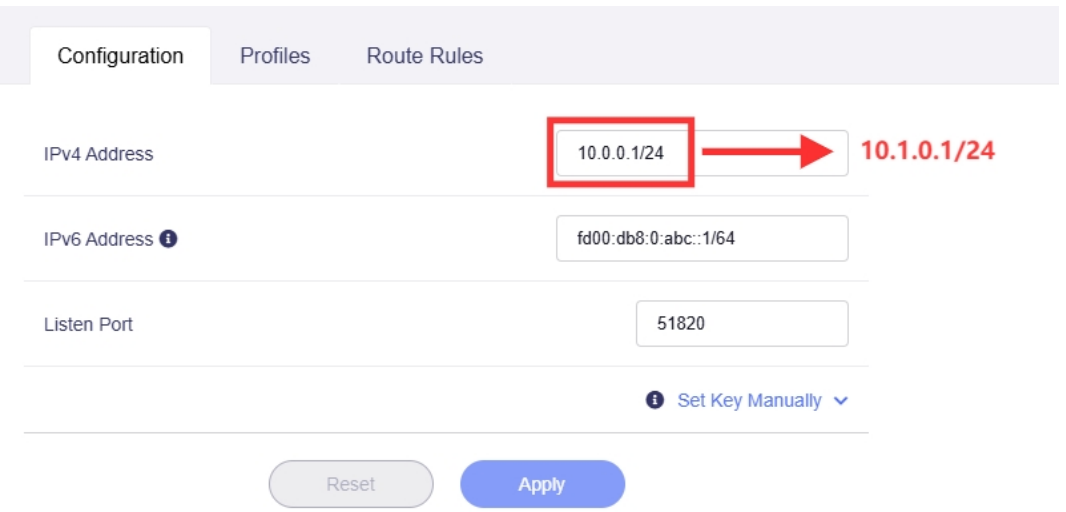
10.2.2 Pasos de configuración

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

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

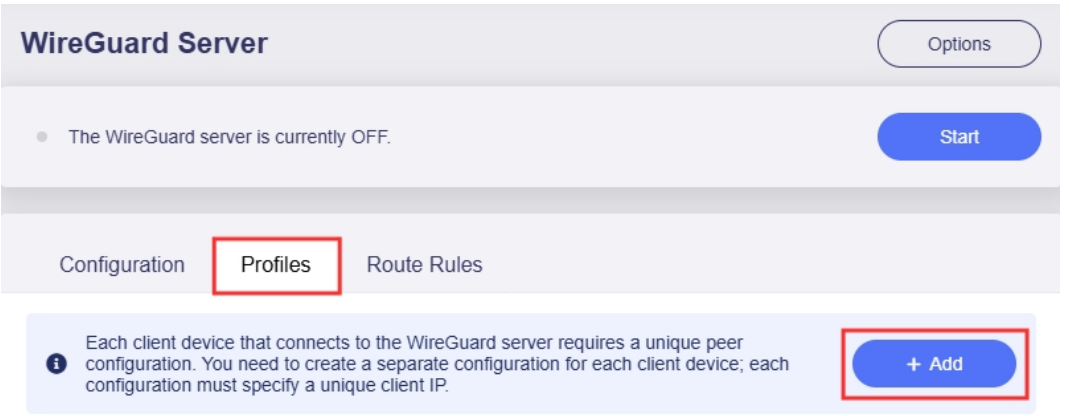


   Si la dirección IPv4 entra en conflicto con la puerta de enlace de su enrutador ascendente, modifique la dirección IPv4 a otra una (por ejemplo, **10.1.0.1/24**) y haga clic en **Aplicar**. Asegúrese de que se incluya la notación CIDR "/24" para evitar problemas de conectividad.

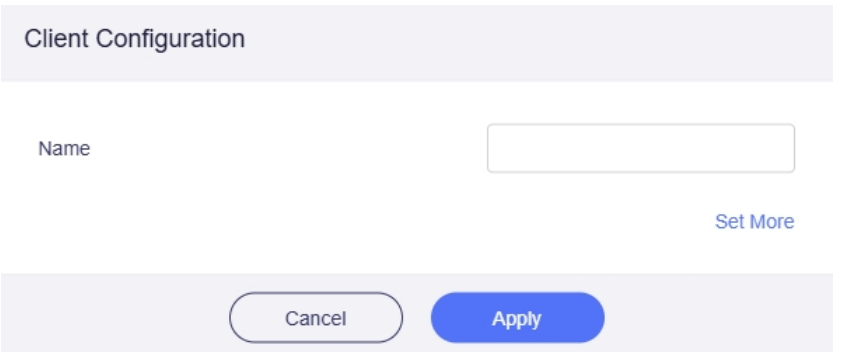


3. Agregue un perfil.

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



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



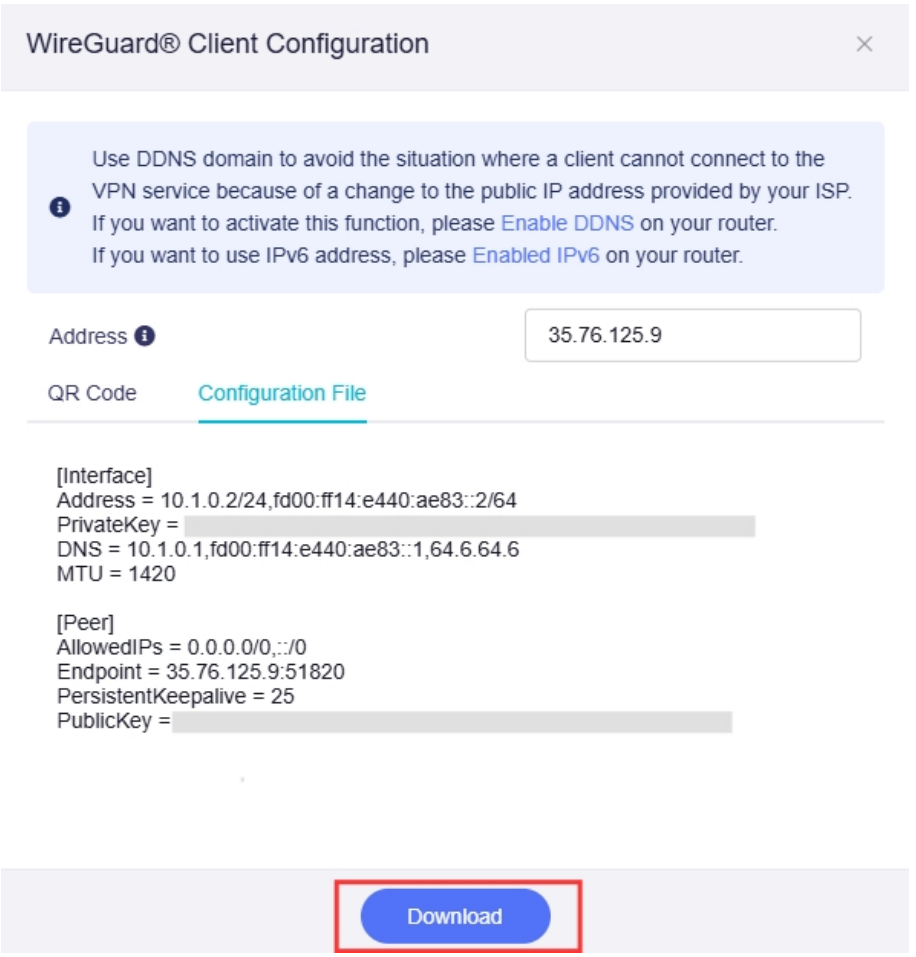
   Consejo: Si desea acceder a los dispositivos LAN del cliente WireGuard desde su servidor WireGuard , cambie a la pestaña **Reglas de ruta** para configurar reglas de ruta. Consulte aquí para detalless.

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. Elige tu método preferido para obtener el archivo de configuración.

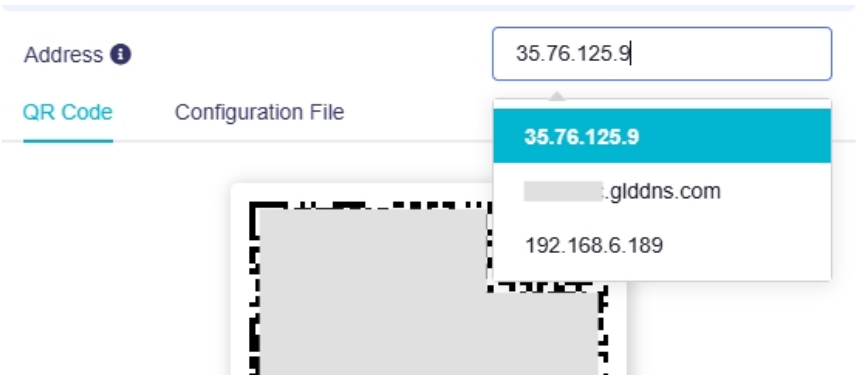
   - **Código QR**: Adecuado para dispositivos (por ejemplo, teléfonos inteligentes, tabletas, computadoras portátiles) con la aplicación WireGuard instalada. Si desea configurar un dispositivo específico como cliente WireGuard, simplemente abra la aplicación WireGuard y escanee el código QR para importar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

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



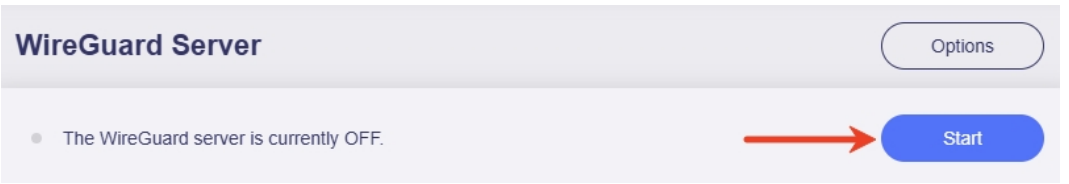
Consejos:

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

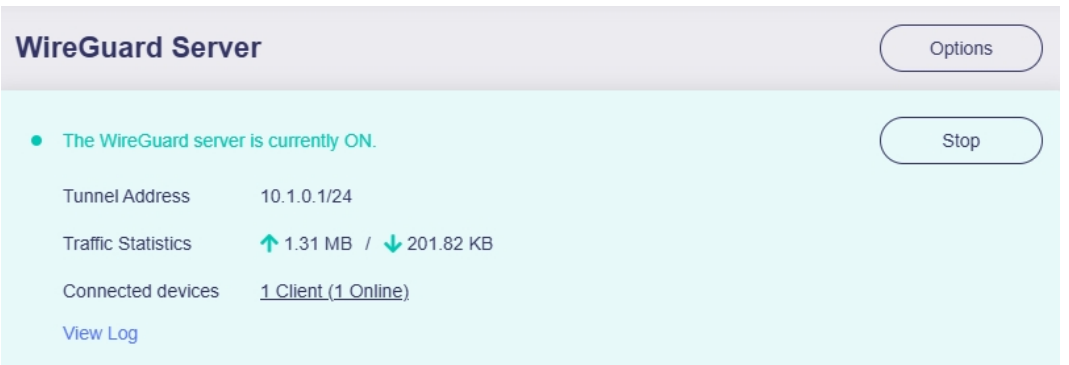


5. Inicie el servidor WireGuard.

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



   Se muestra el servidor estado de conexión en la top. Si muestra estadísticas de tráfico de carga, descarga, y dispositivos conectados en línea, significa que el servidor WireGuard se está ejecutando.



10.2.3 Solución de problemas

Si la conexión falla, existen varias razones comunes:

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

Capítulo 11

Configurar el cliente VPN

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

11.1 Configurar el cliente OpenVPN

11.1.1 Preparación

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

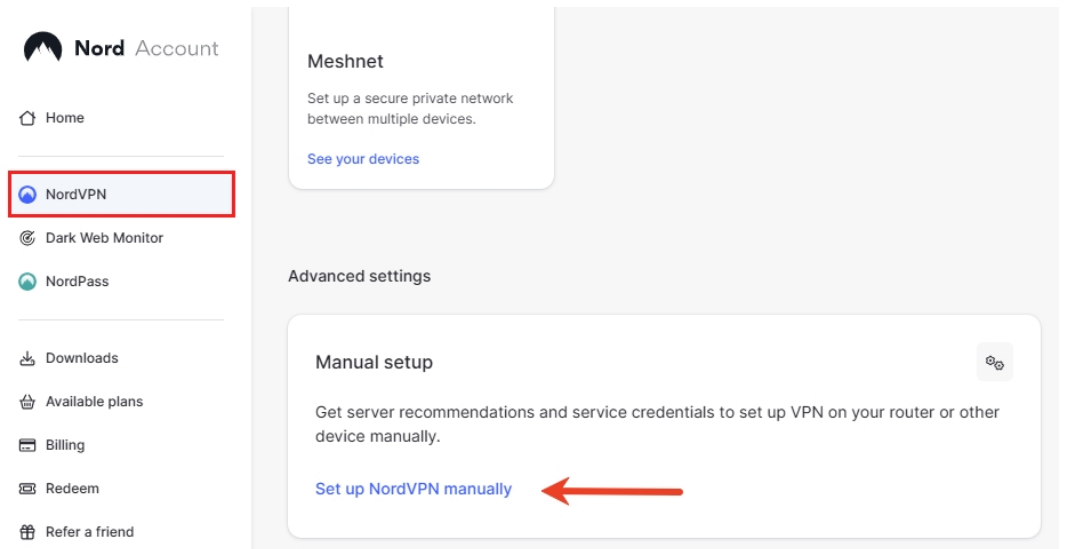
Siguiente, visite el sitio web oficial del proveedor de servicios VPN al que se suscribió y obtenga las credenciales del servicio o el archivo de configuración. Si no sabe cómo obtener el archivo de configuración, consulte este enlace o póngase en contacto con su soporte.

11.1.2 Configurar NordVPN

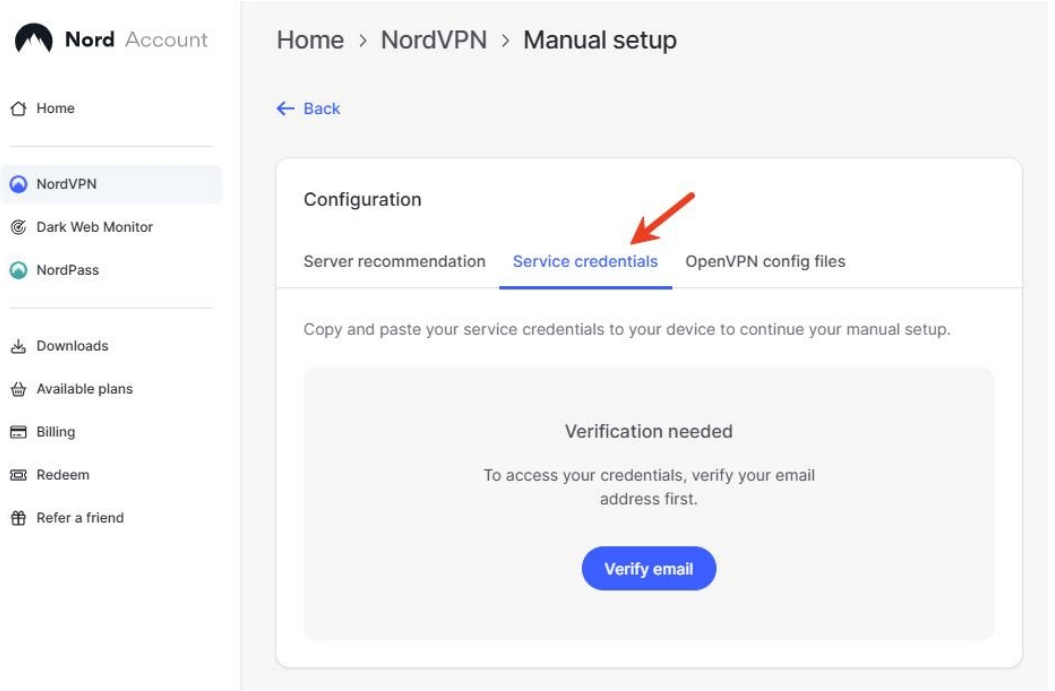
NordVPN está integrado en el panel de administración GL.iNet web . Puede adquirir archivos de configuración para todos los servidores NordVPN introduciendo las credenciales de su cuenta (obtenidas del Panel de NordVPN) en el panel de administración web del enrutador o en la aplicación móvil GL.iNet ,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

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

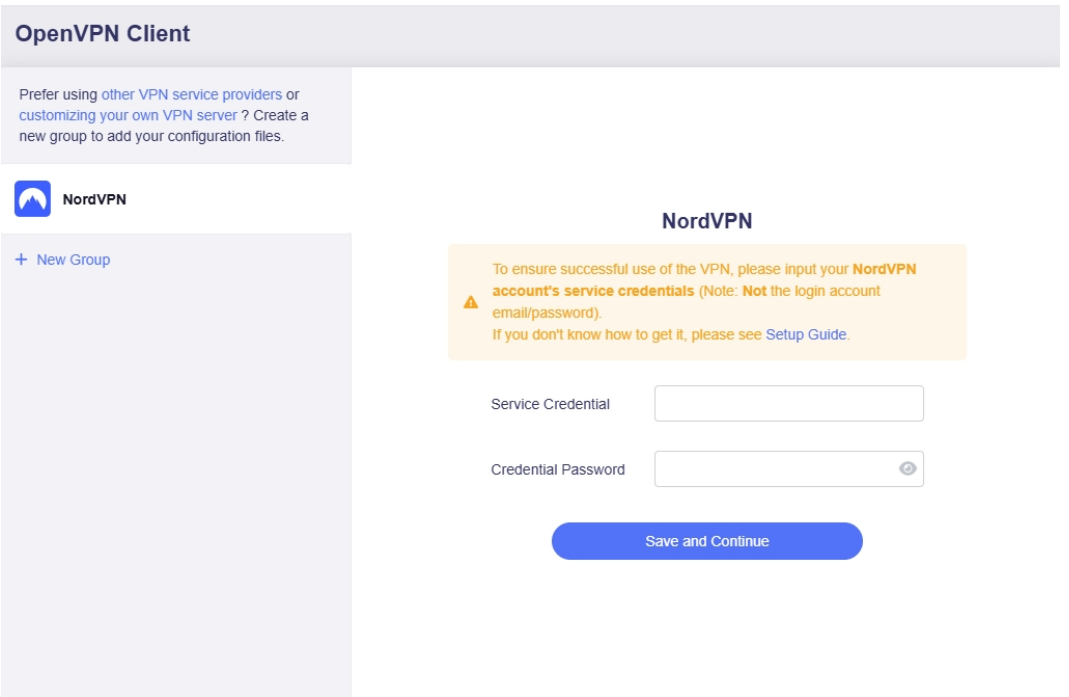
1. Inicie sesión en su cuenta web de NordVPN aquí.
2. Oen el Panel de control de Nord, haga clic en **NordVPN**, luego haga clic en **Configurar NordVPN manualmente**.



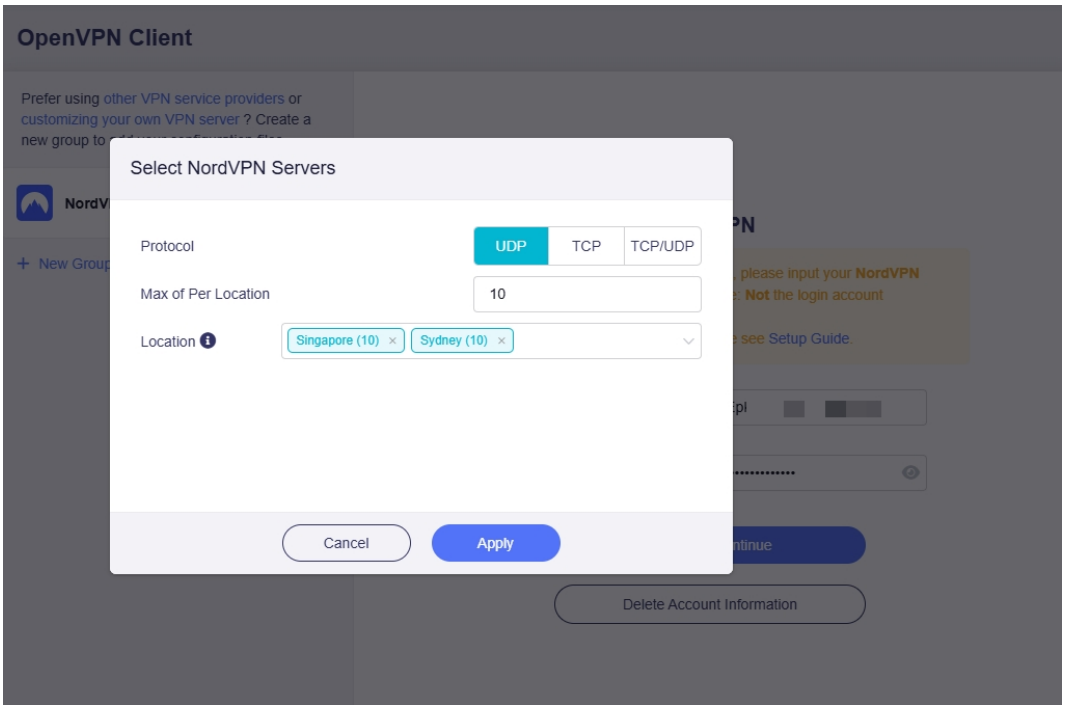
Encontrará las **credenciales de servicio**. Cópialos para usarlos más adelante.



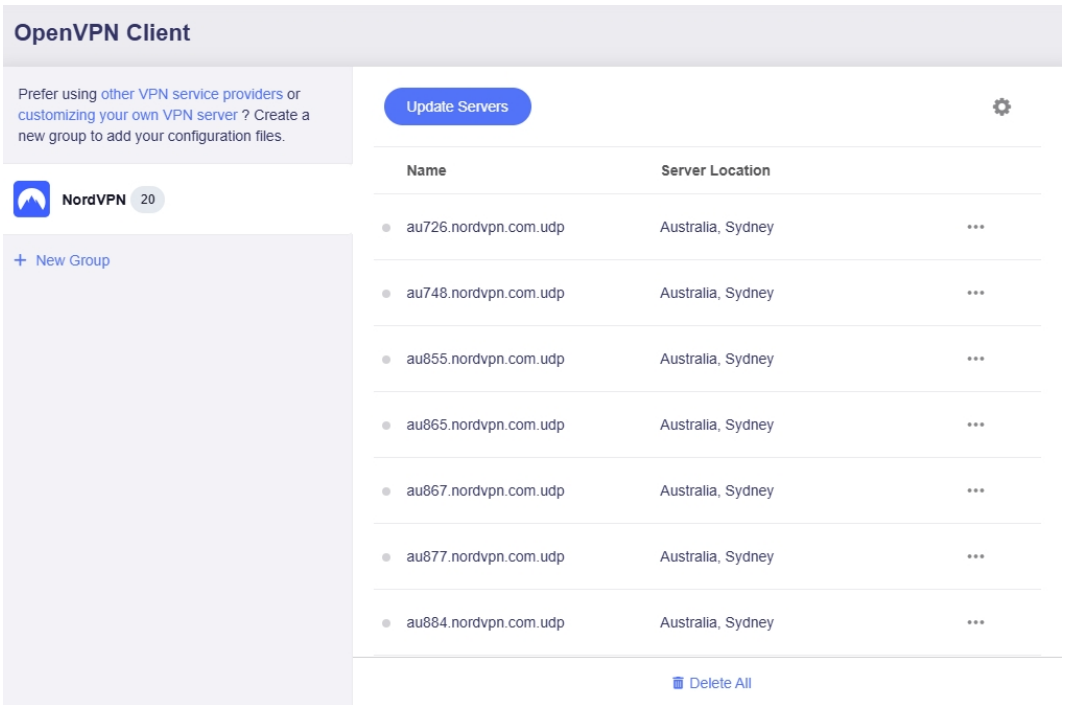
3. Inicie sesión en el panel de administración web de su enrutador y navegue hasta **VPN** > **Cliente OpenVPN** > **NordVPN**. Introduzca las credenciales del servicio (Nota: NO es el correo electrónico ni la contraseña de la cuenta de inicio de sesión), luego haga clic en **Guardar y continuar**.



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

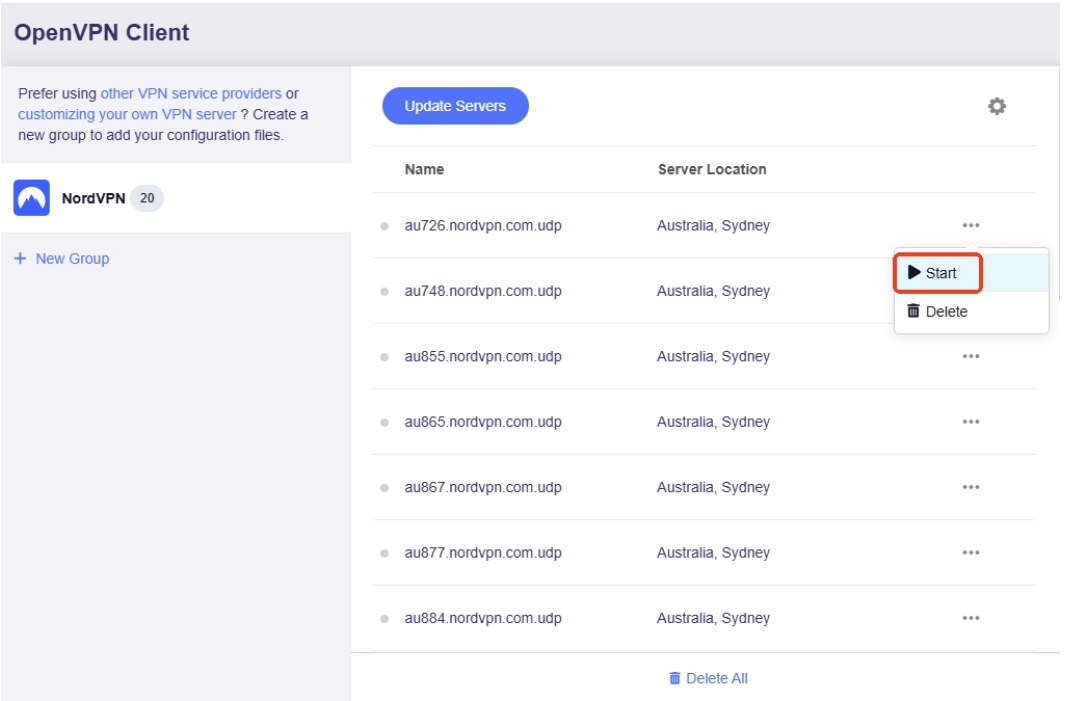


Descargará archivos de configuración.

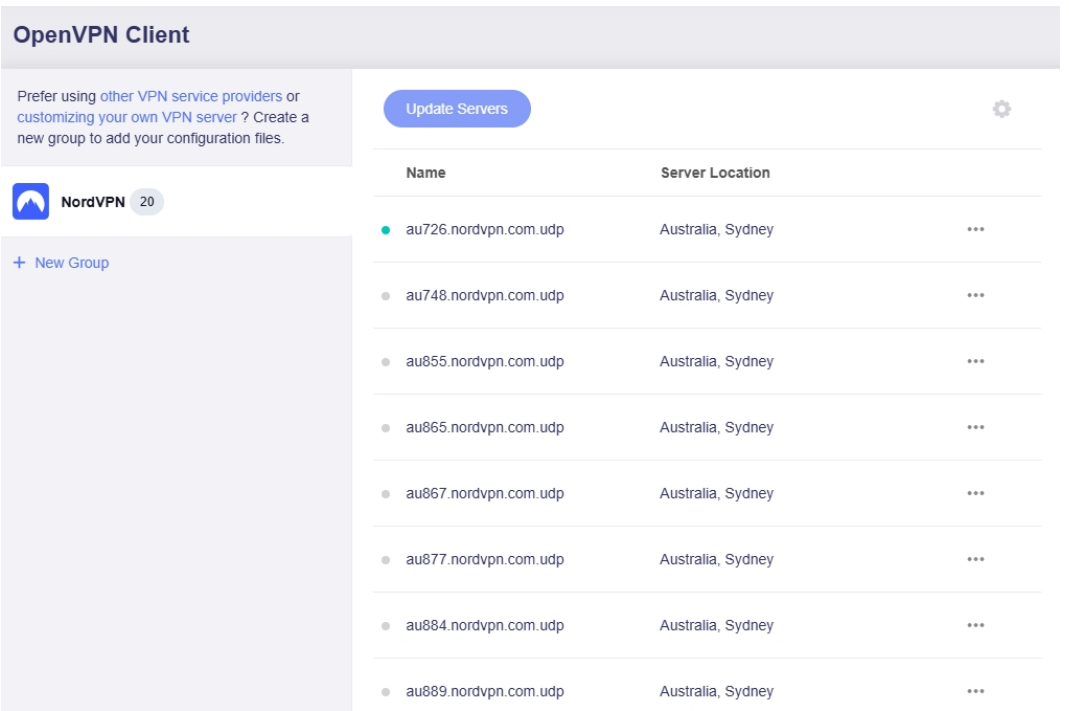


5. Iniciará una conexión.

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



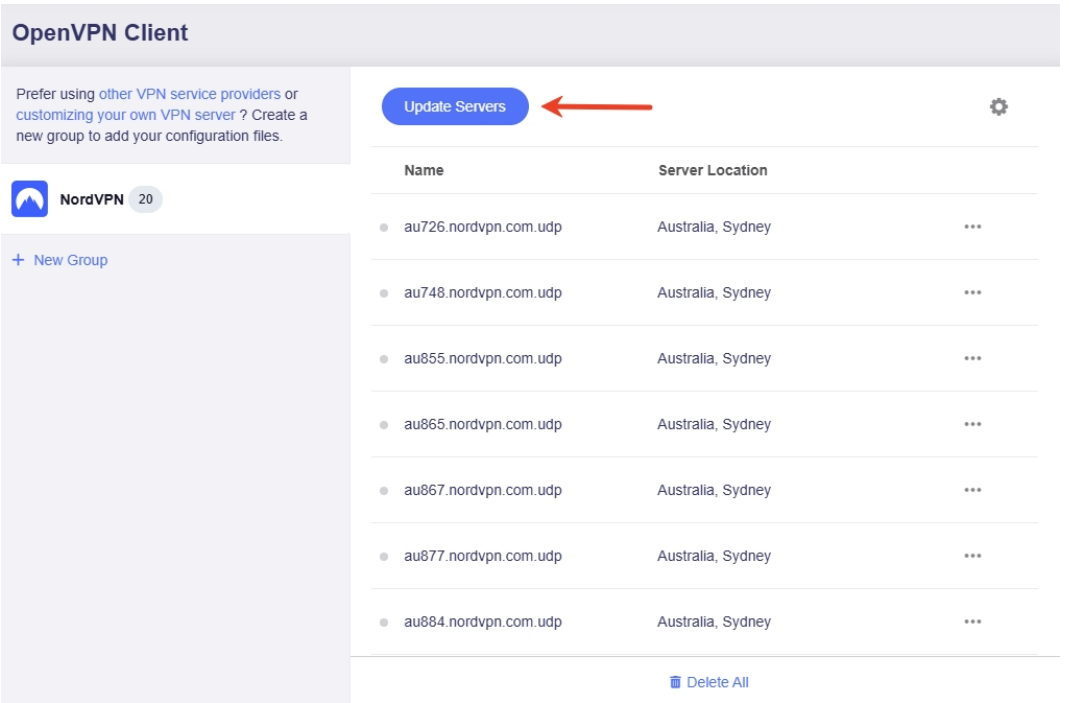
6. Una vez conectado, aparecerá un punto verde junto a el archivo de configuración.



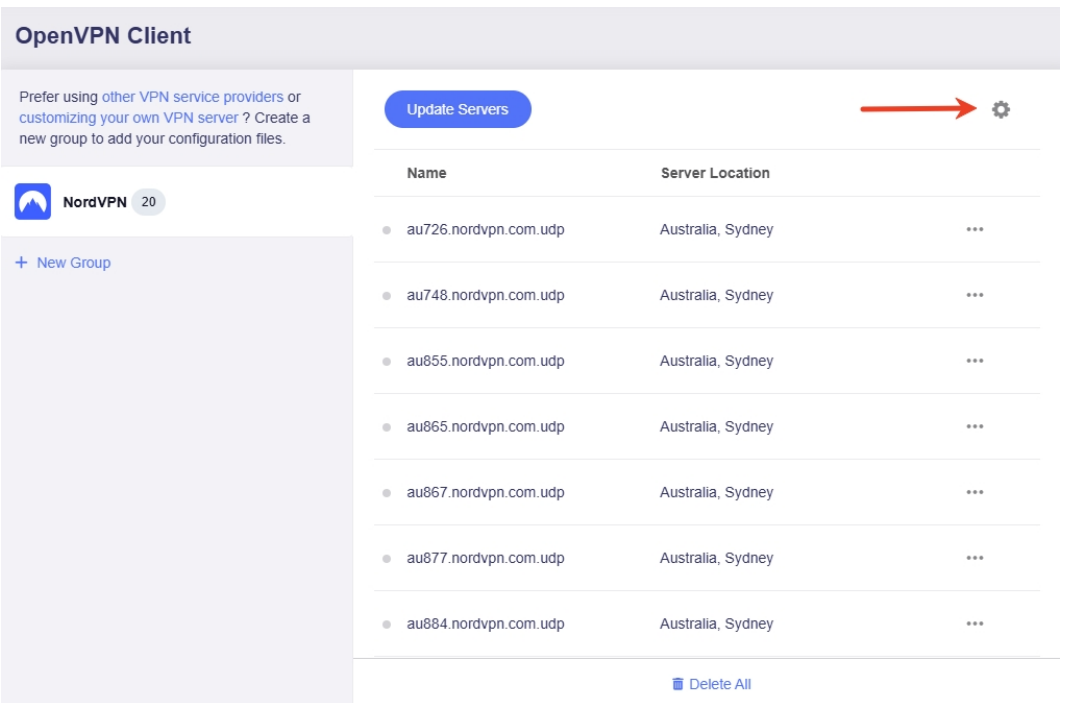
También puede consultar los detalles de la conexión VPN en el **Panel de VPN**.

7. Actualizar servidores.

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.

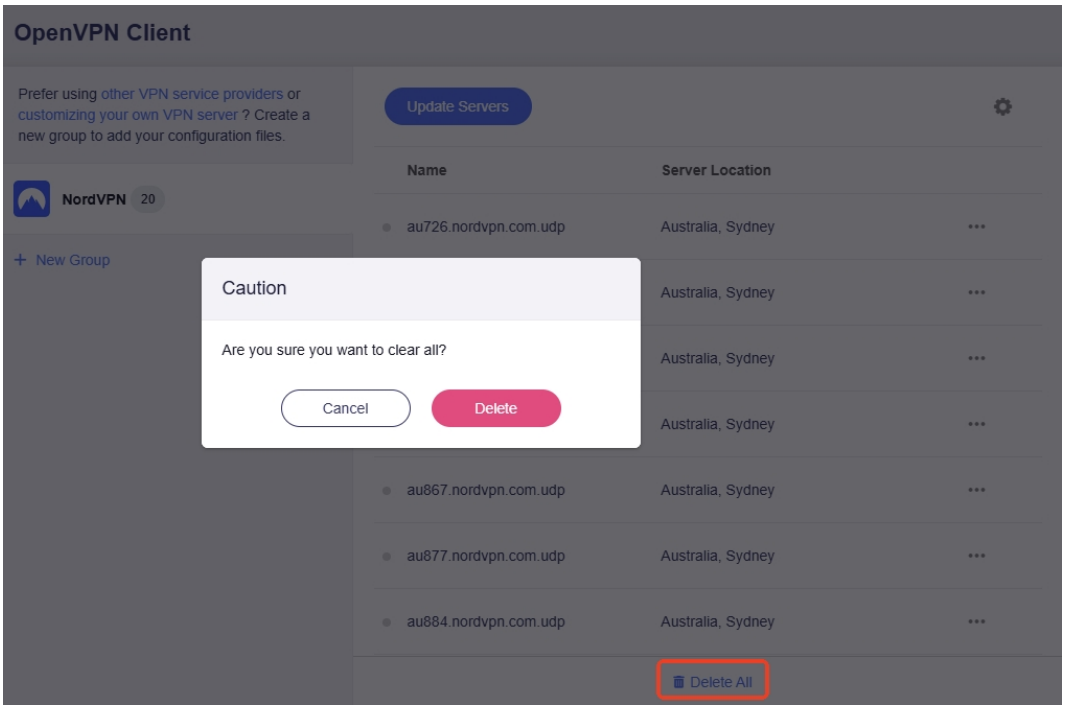


8. Editar credenciales.
   Haga clic en el ícono de ajustes para editar sus credenciales de inicio de sesión.



9. Eliminar todos los archivos.

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

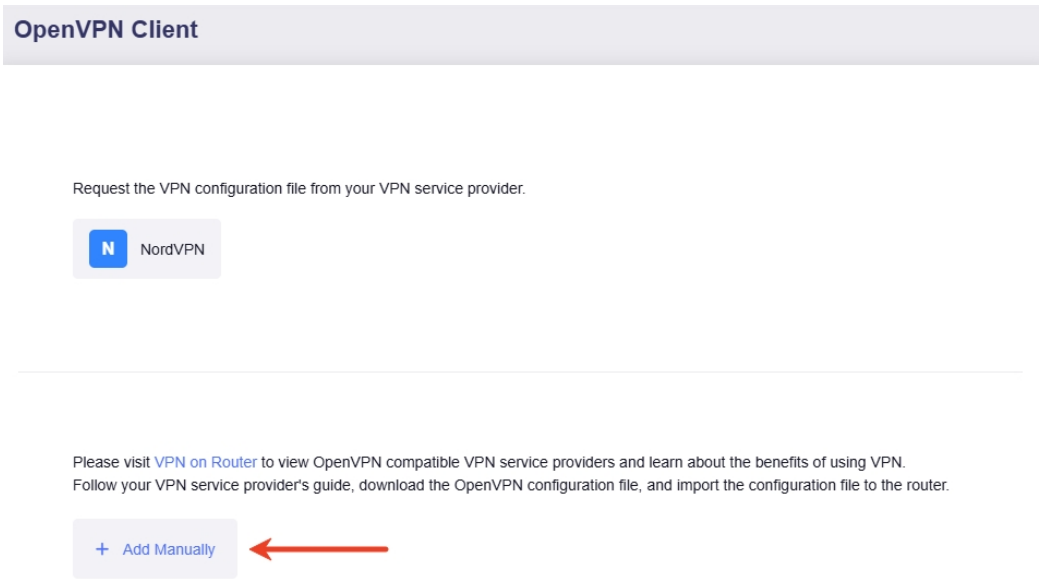


11.1.3 Configurar el cliente OpenVPN manualmente (para otros proveedores)

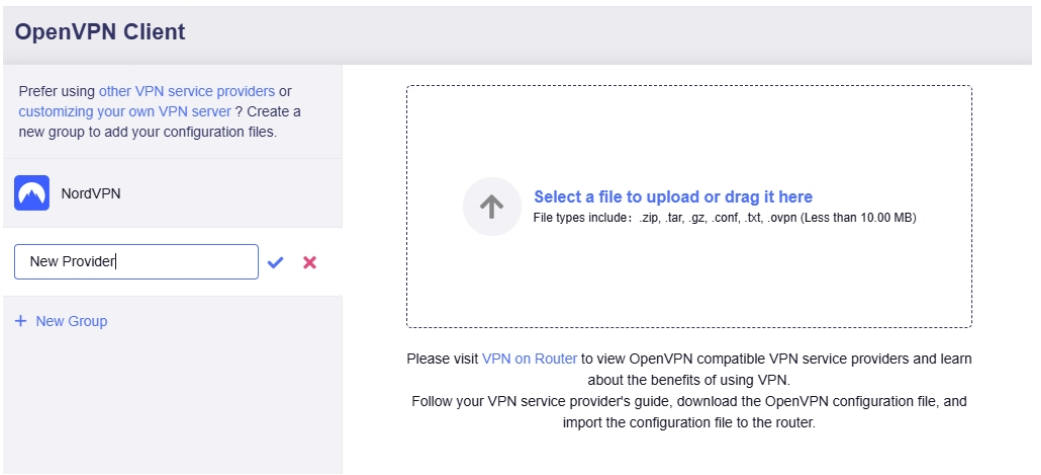
Si su proveedor de servicios OpenVPN no está integrado en nuestro panel de administración, primero visite el sitio web oficial de su proveedor de servicios suscrito para obtener el archivo de configuración. Luego cárguelo en el enrutador para configurar un cliente OpenVPN.

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

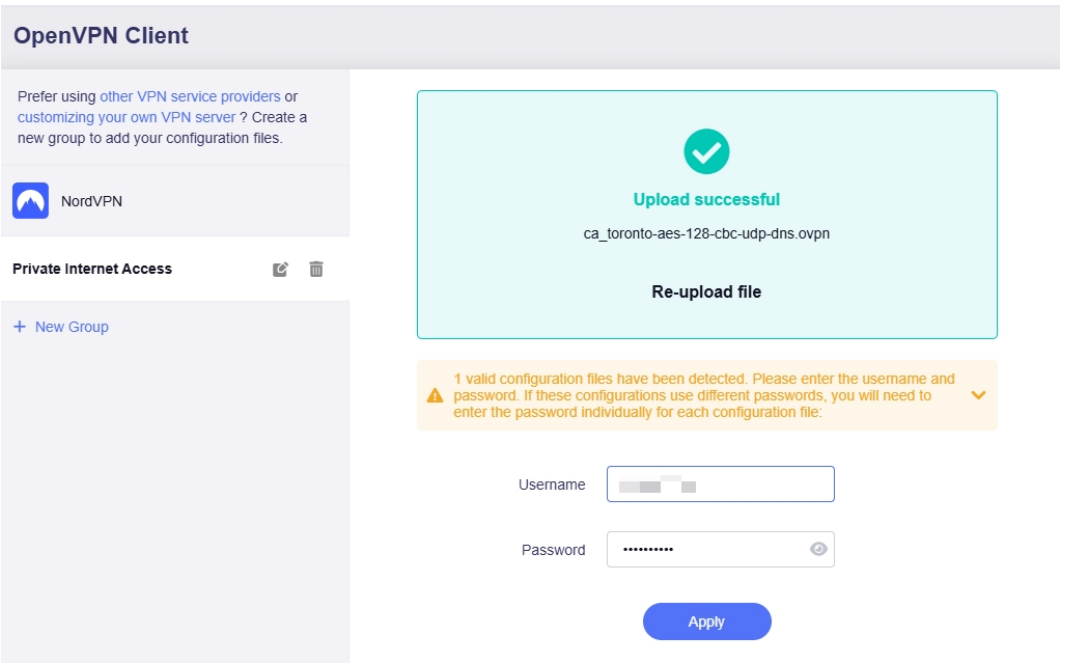
1. Descargue un archivo de configuración del sitio web oficial de Private Internet Access.
2. Inicie sesión en el panel de administración web de su enrutador, navegue hasta **VPN** > **Cliente OpenVPN** y haga clic en **Agregar manualmente**.



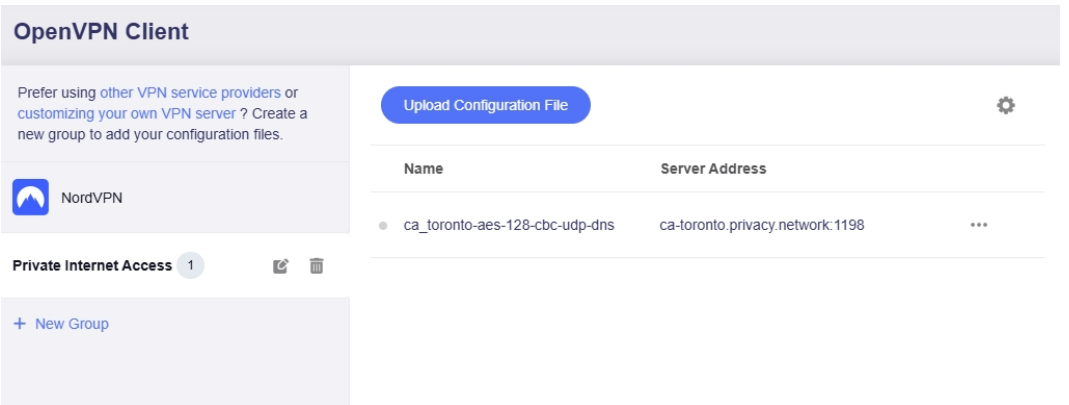
3. Se creará un grupo en la barra lateral izquierda.Establezca un nombre descriptivo para el grupo.



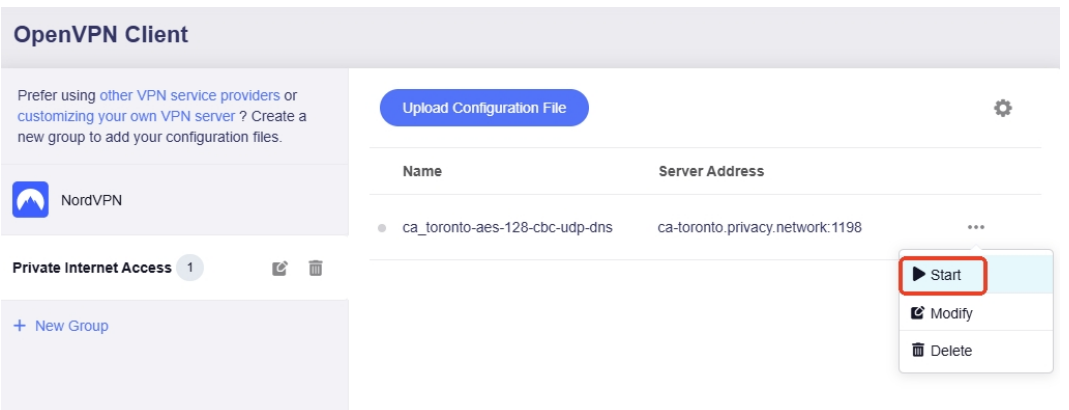
4. Cargue su archivo de configuración OpenVPN. Ingrese las credenciales si es necesario, luego haga clic en **Aplicar**.



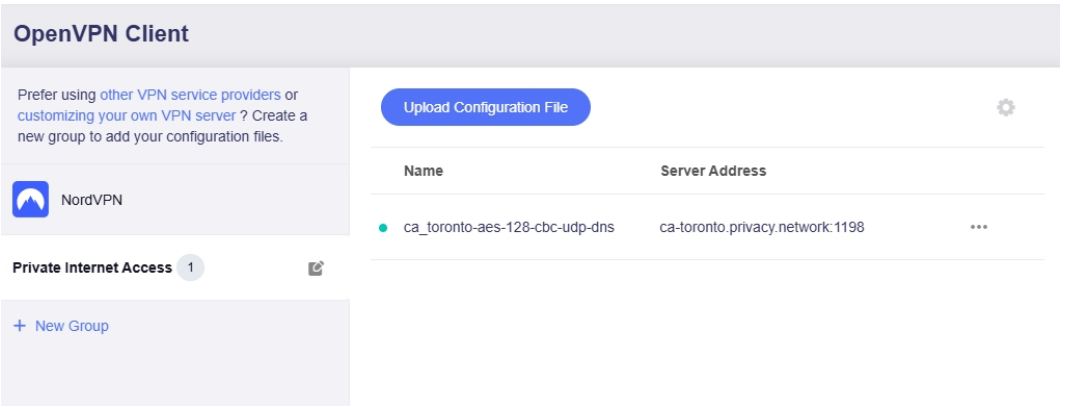
YVerá el archivo de configuración cargado.



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

11.2 Configurar el cliente WireGuard

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

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

11.2.1 Preparación

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

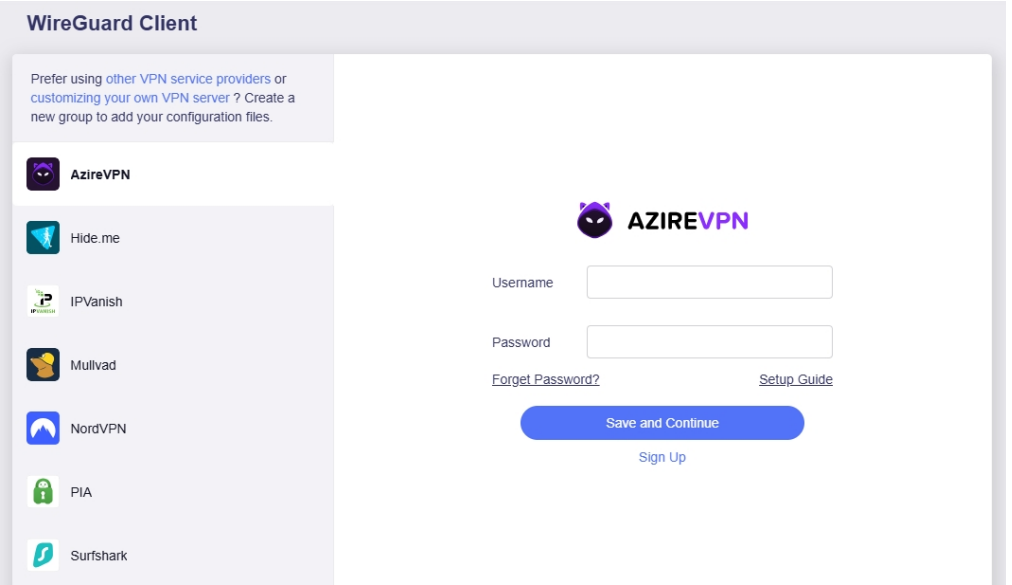
A continuación, sseleccione el proveedor de servicios WireGuard correspondiente a continuación para localizar rápidamente las instrucciones paso a paso.

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

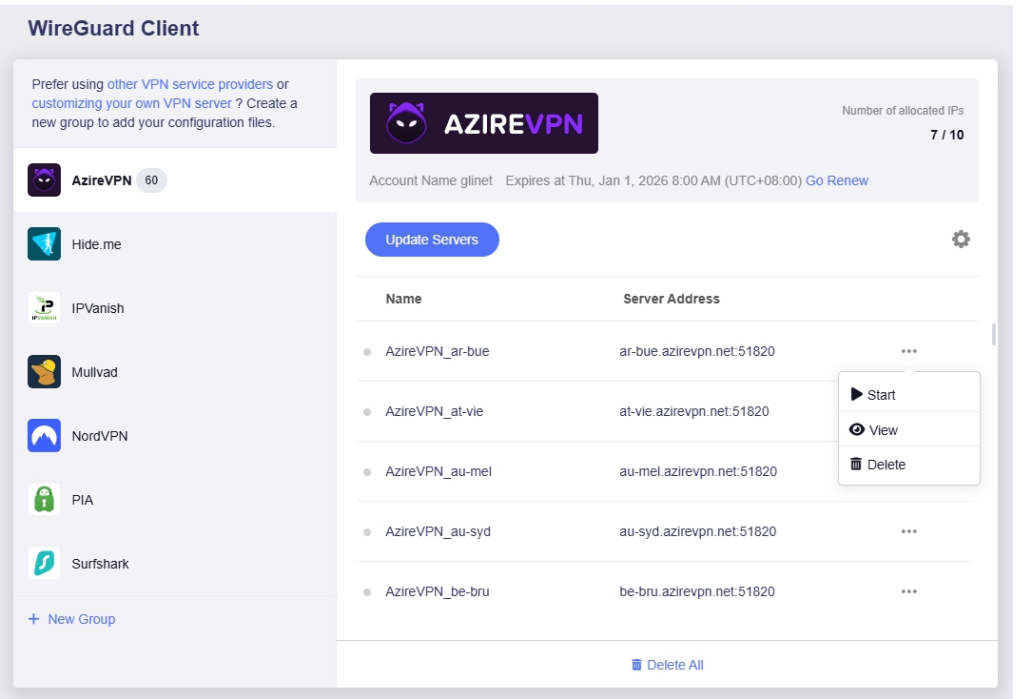
11.2.2 Configurar AzireVPN

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

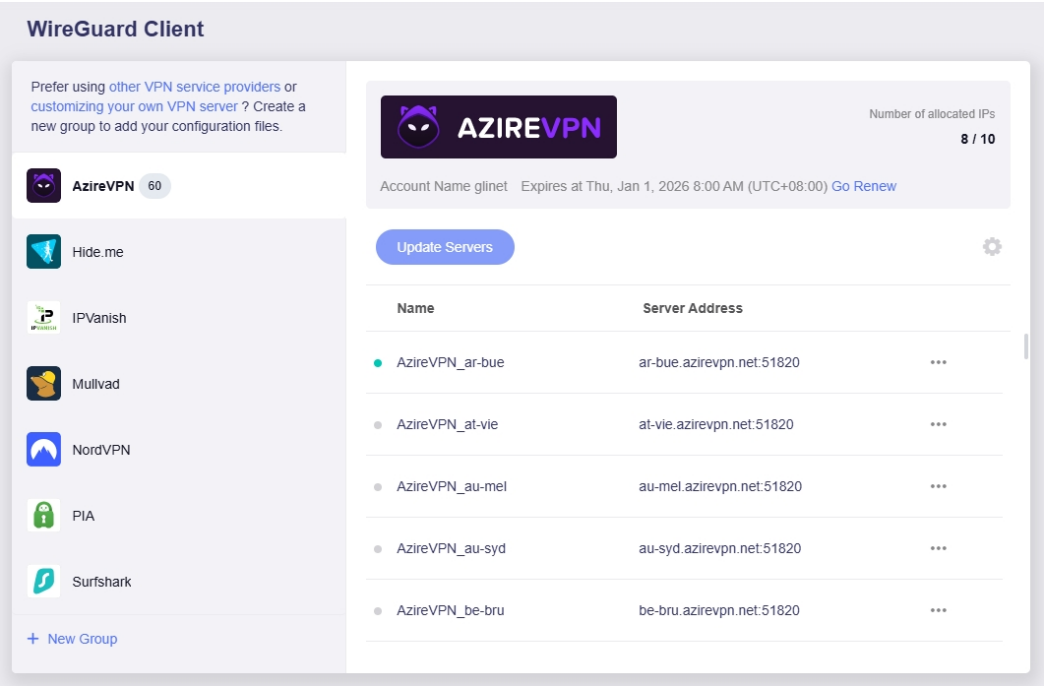
1. Inicie sesiónn en su enrutador’s web admin panel y vaya a **VPN** > **Cliente WireGuard** > **AzireVPN**.
2. Ingrese nombre de usuario y contraseña, luego haga clic en **Guardar y continuar**. Generará archivos de configuración para cada servidor.



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



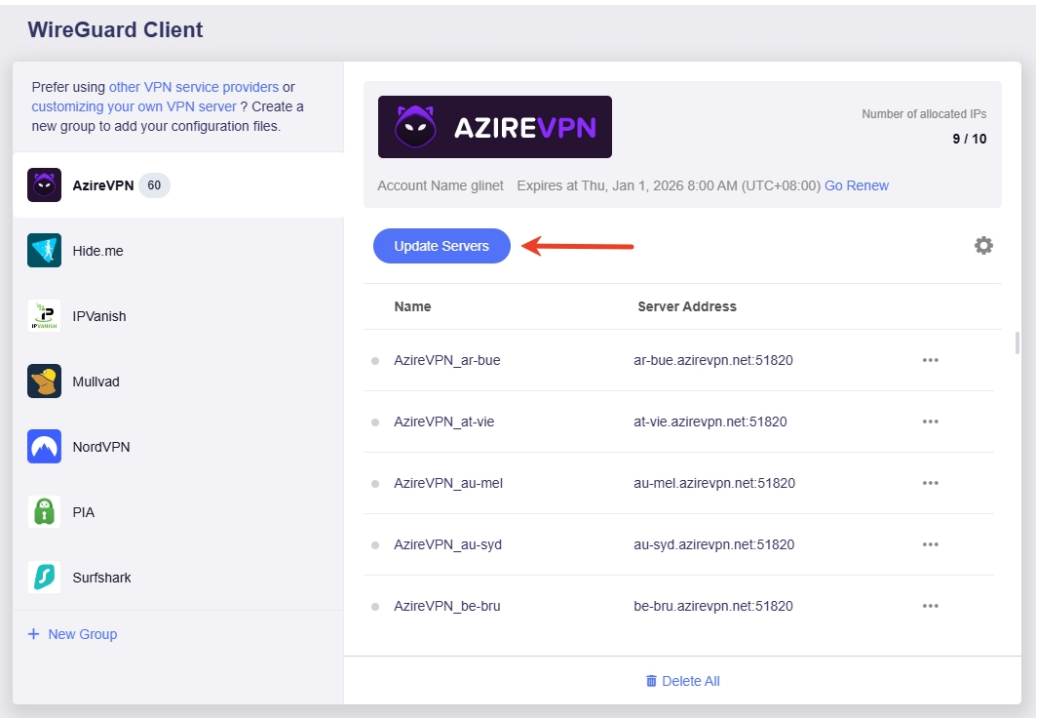
4. Una vez conectado, aparecerá un punto verde junto al archivo de configuración.



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

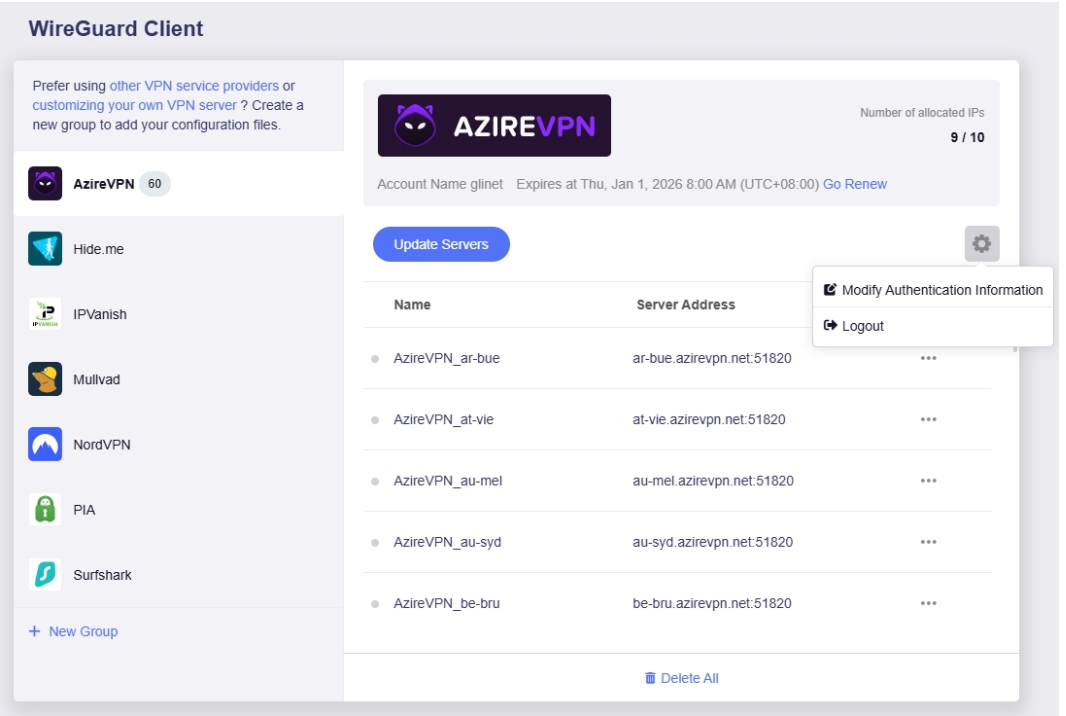
5. Actualizar servidores.

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



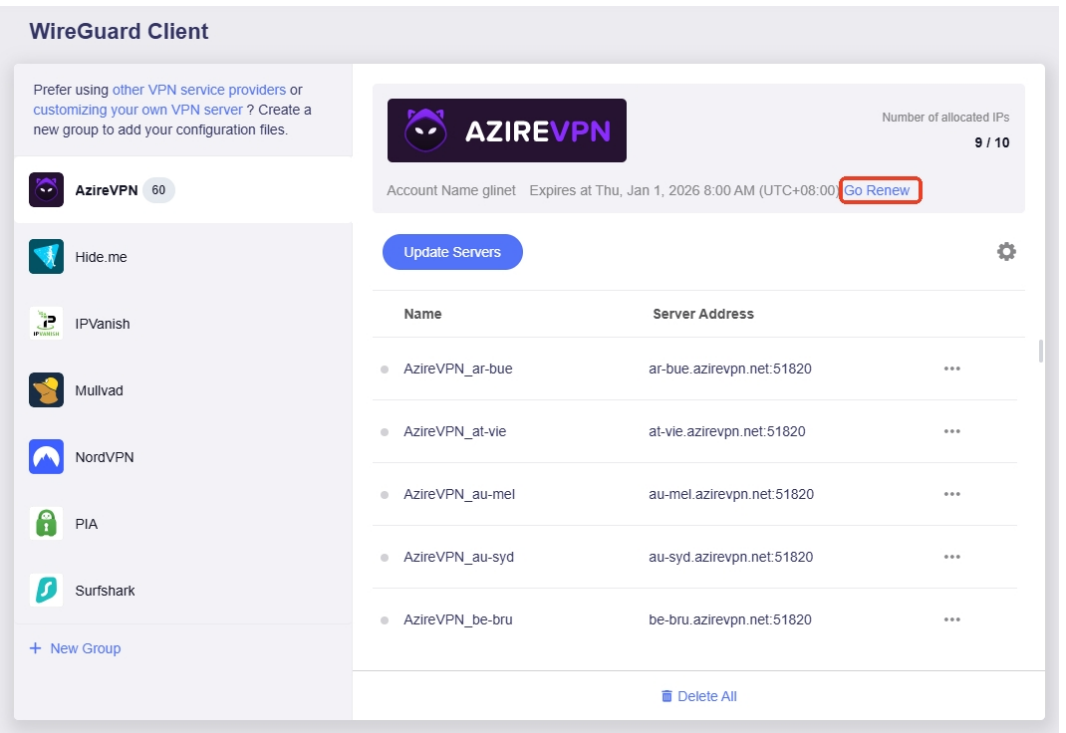
6. Editar credenciales o cerrar sesión.

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



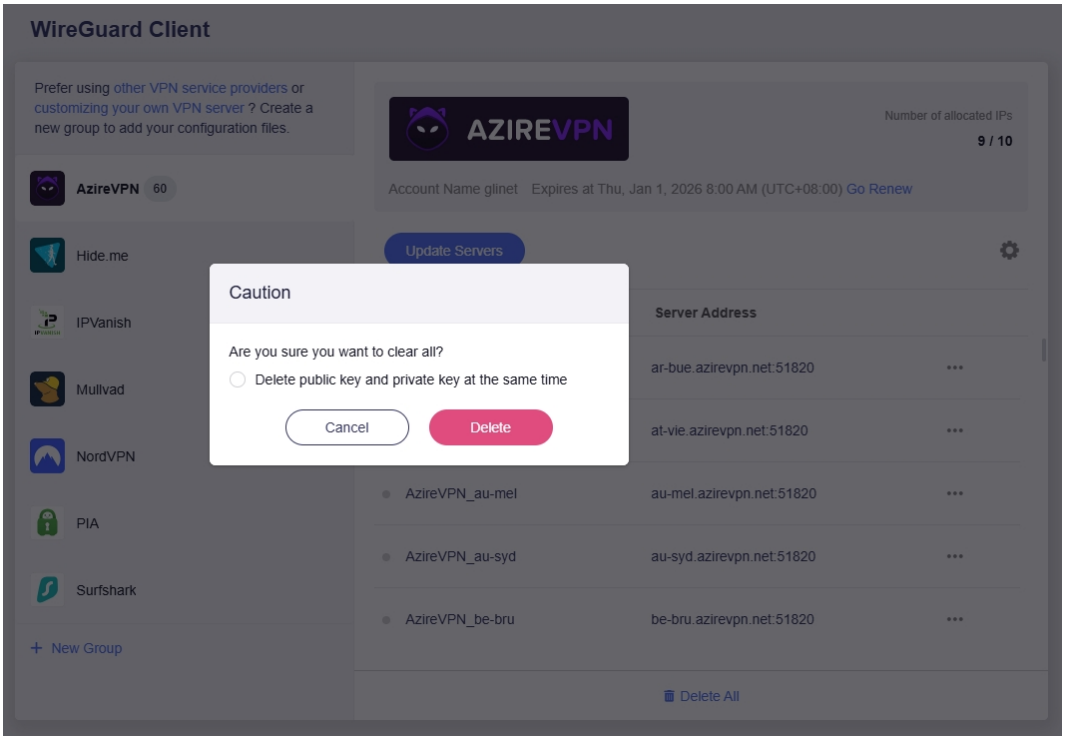
7. Ir a renovar.

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



8. Eliminar todos los archivos.

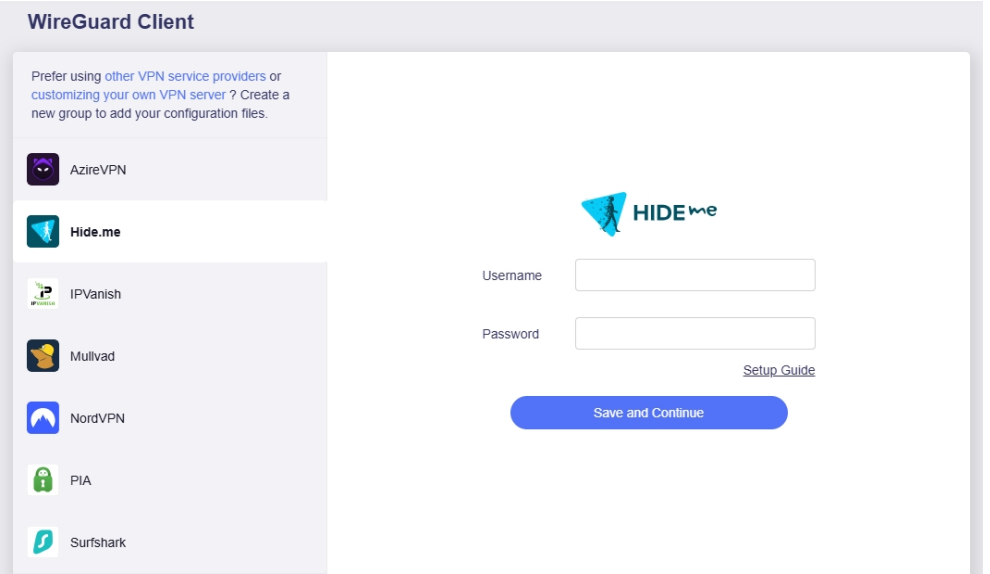
   Puede hacer clic en **Eliminar todo** para eliminar todos los archivos de configuración con un solo clic y elegir si desea eliminar el archivo privado. y claves públicas simultáneamente.



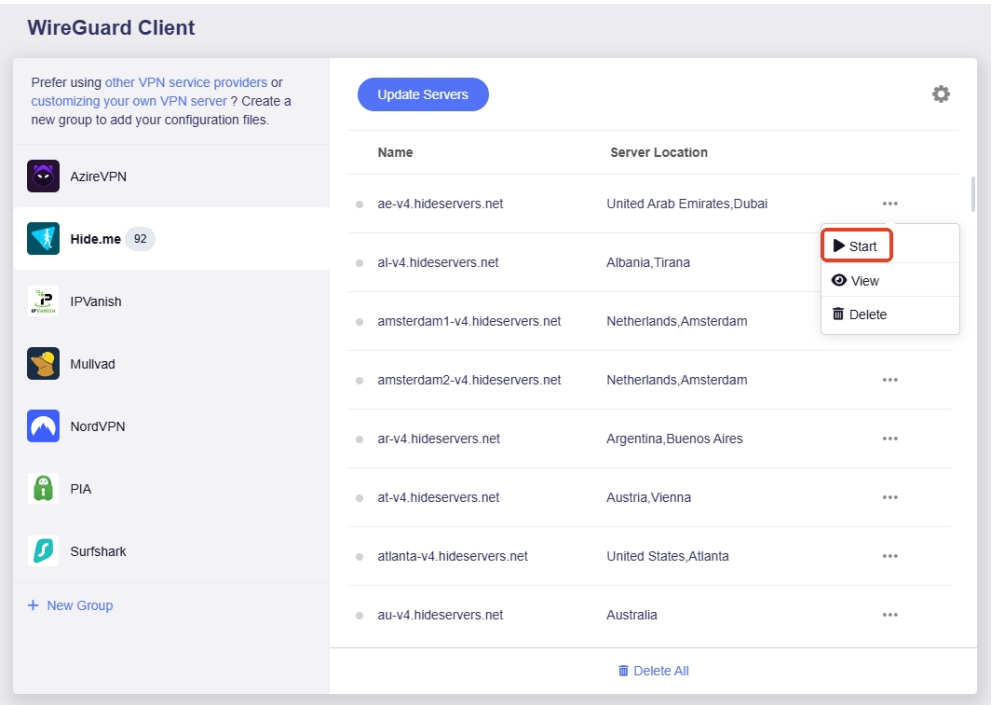
11.2.3 Configurar Hide.me

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

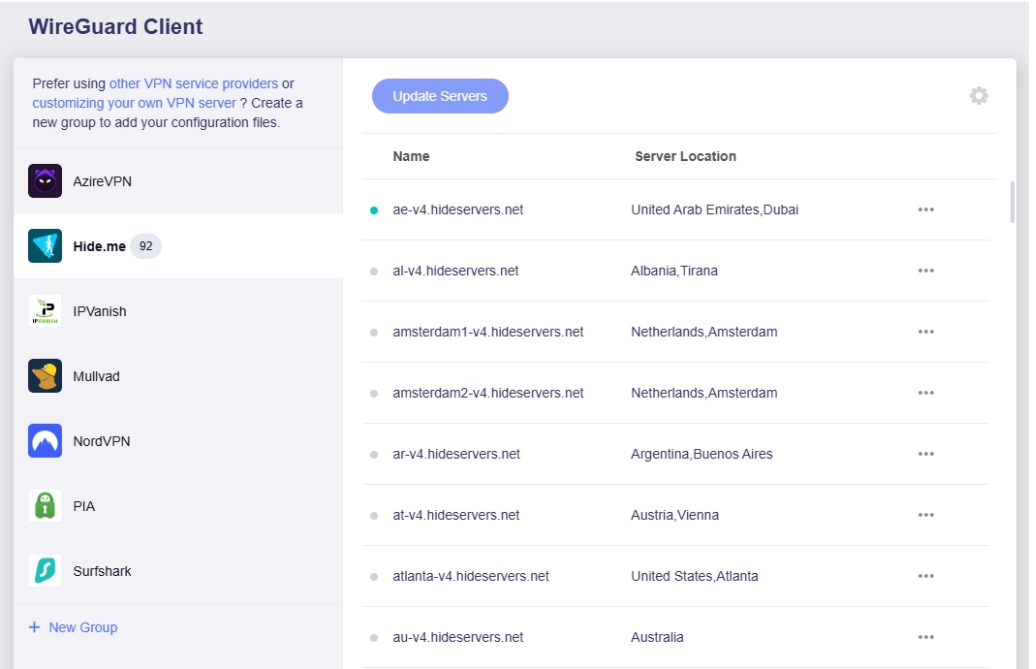
1. Inicie sesiónn en su enrutador’s web admin panel y vaya a **VPN** > **Cliente WireGuard** > **Hide.me**.
2. Ingrese nombre de usuario y contraseña, luego haga clic en **Guardar y continuar**. Generará archivos de configuración para cada servidor.



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



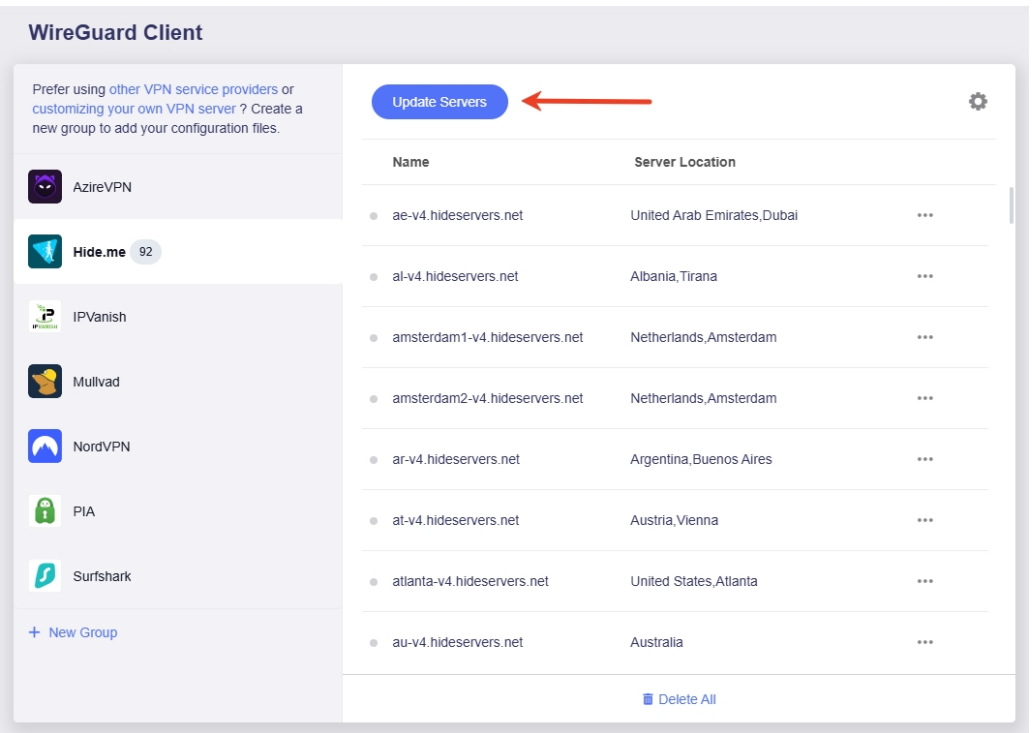
4. Una vez conectado, aparecerá un punto verde junto al archivo de configuración.



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

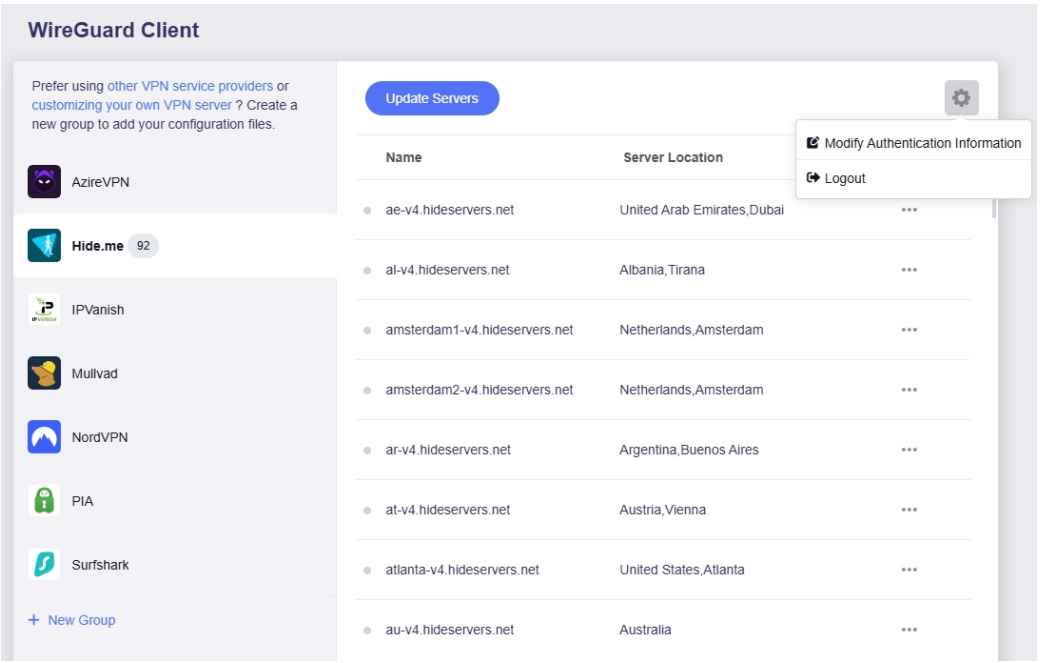
5. Actualizar servidores.

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



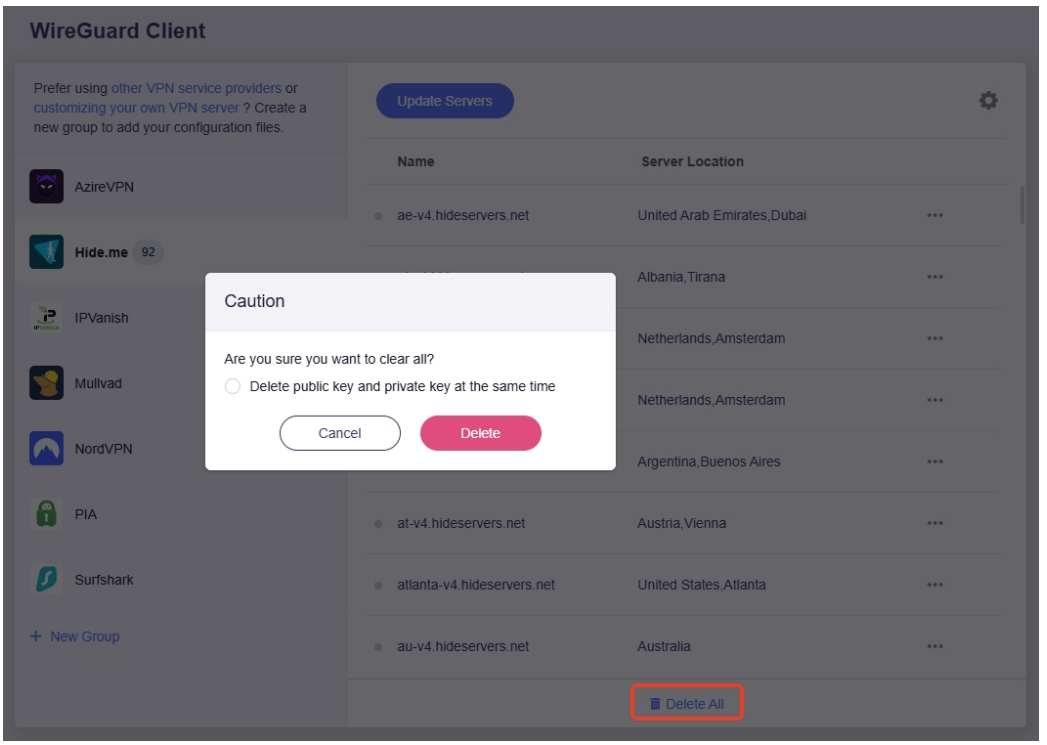
6. Editar credenciales o cerrar sesión.

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



7. Eliminar todos los archivos.

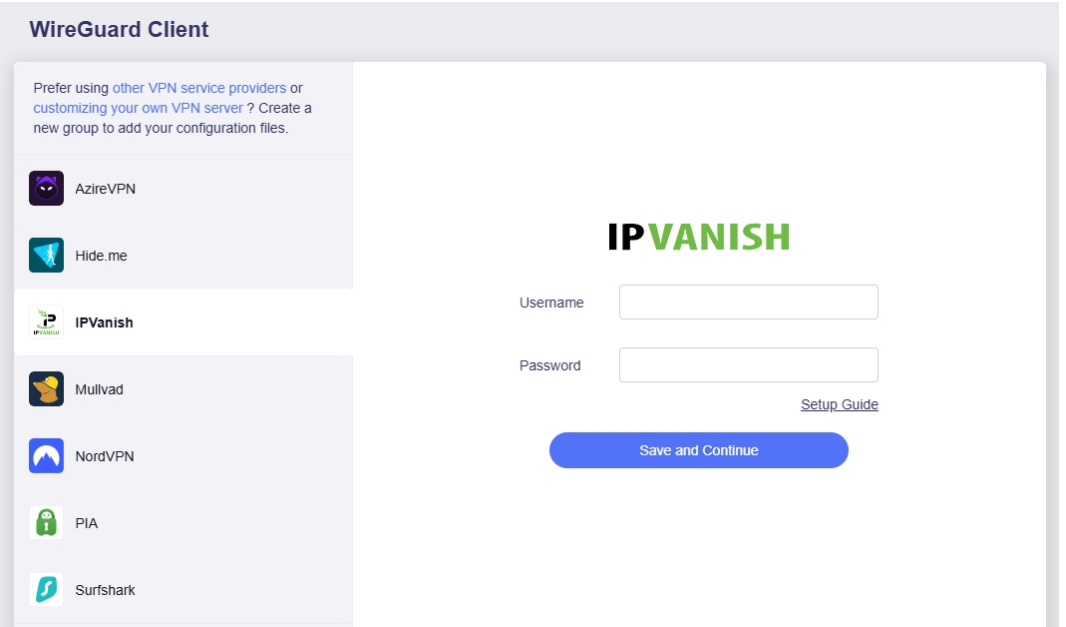
   Puede hacer clic en **Eliminar todo** para eliminar todos los archivos de configuración con un solo clic y elegir si desea eliminar las claves públicas y privadas simultáneamente.



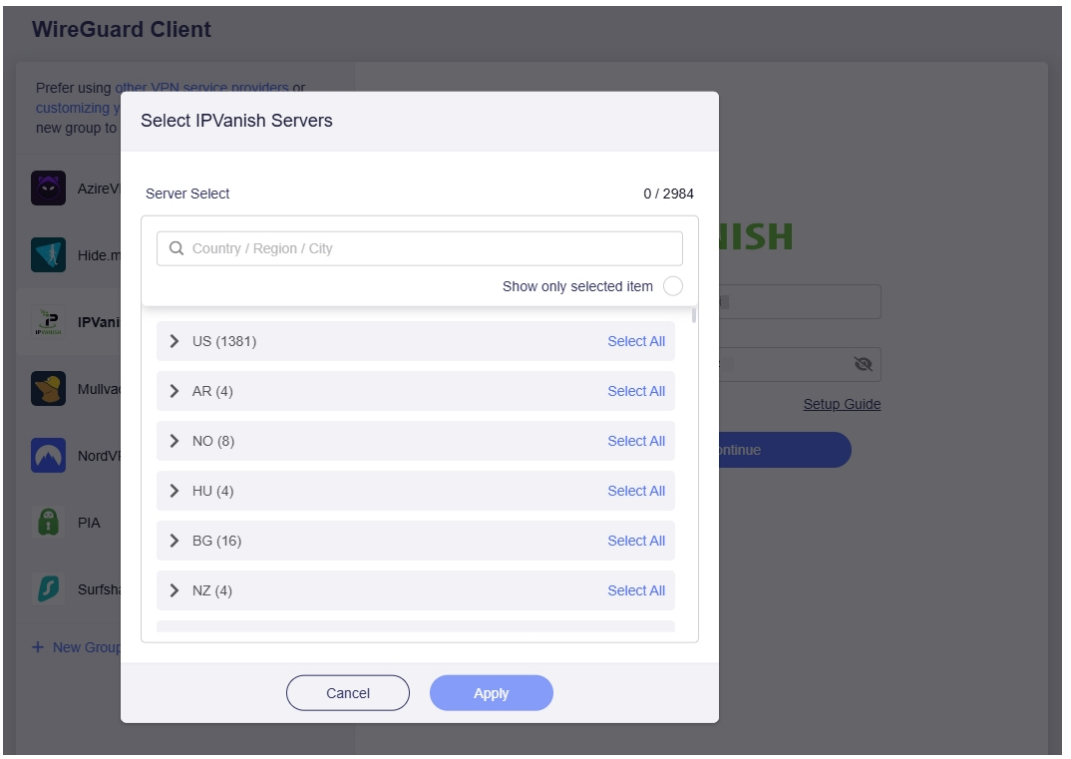
11.2.4 Configurar IPVanish

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

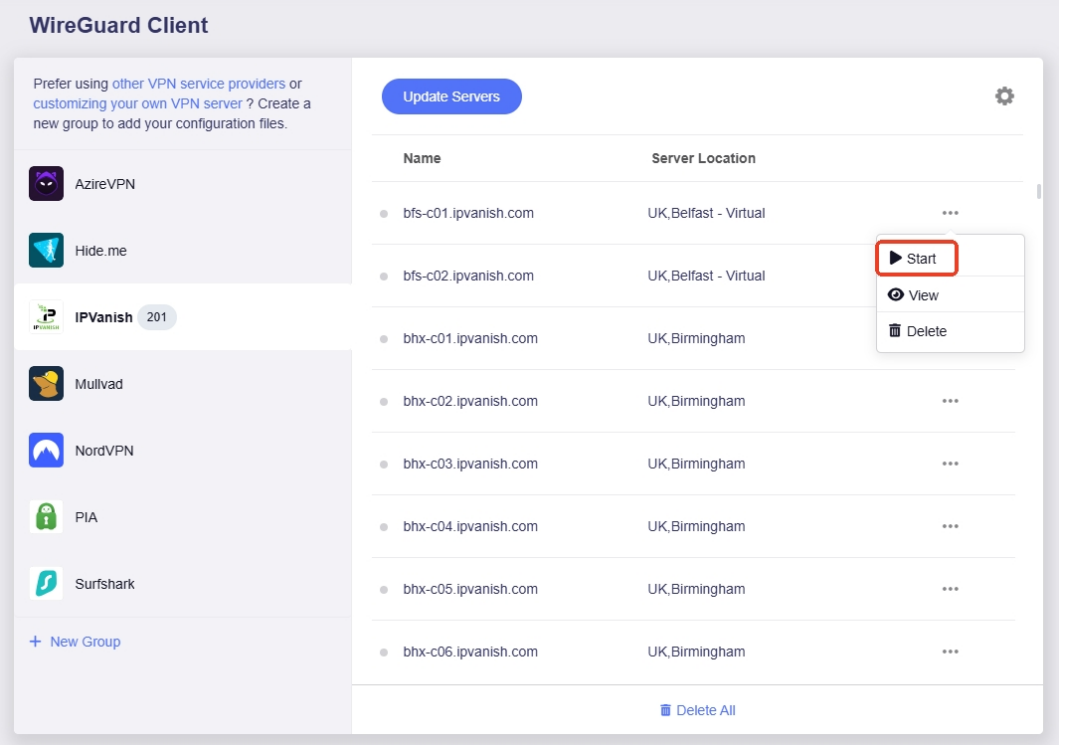
1. Inicie sesiónn en su enrutador’s web admin panel y vaya a **VPN** > **Cliente WireGuard** > **IPVanish**.
2. Ingrese nombre de usuario y contraseña, luego haga clic en **Guardar y continuar**.



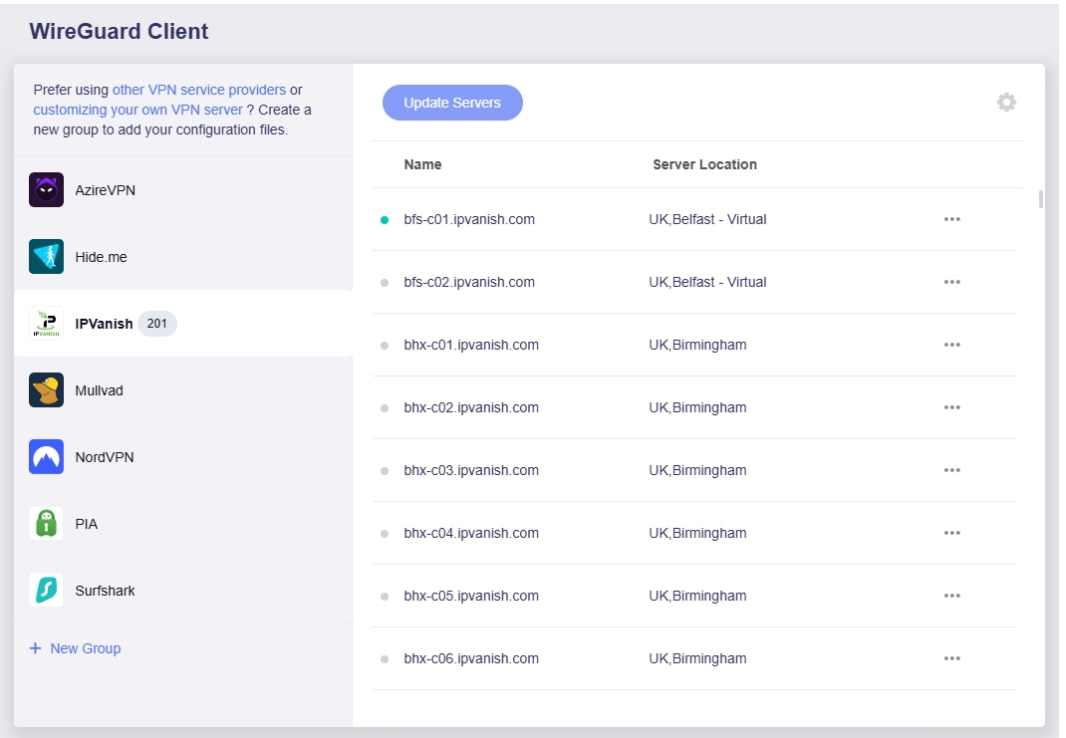
3. Seleccione los servidores a los que desea conectarse y haga clic en **Aplicar**.



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



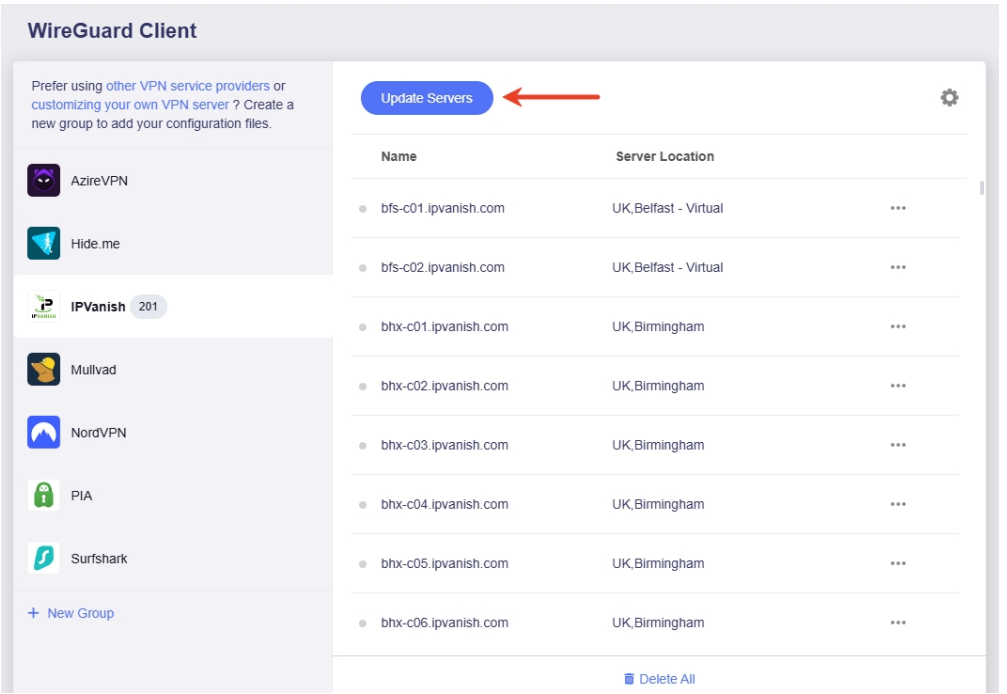
5. Una vez conectado, aparecerá un punto verde junto al archivo de configuración.



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

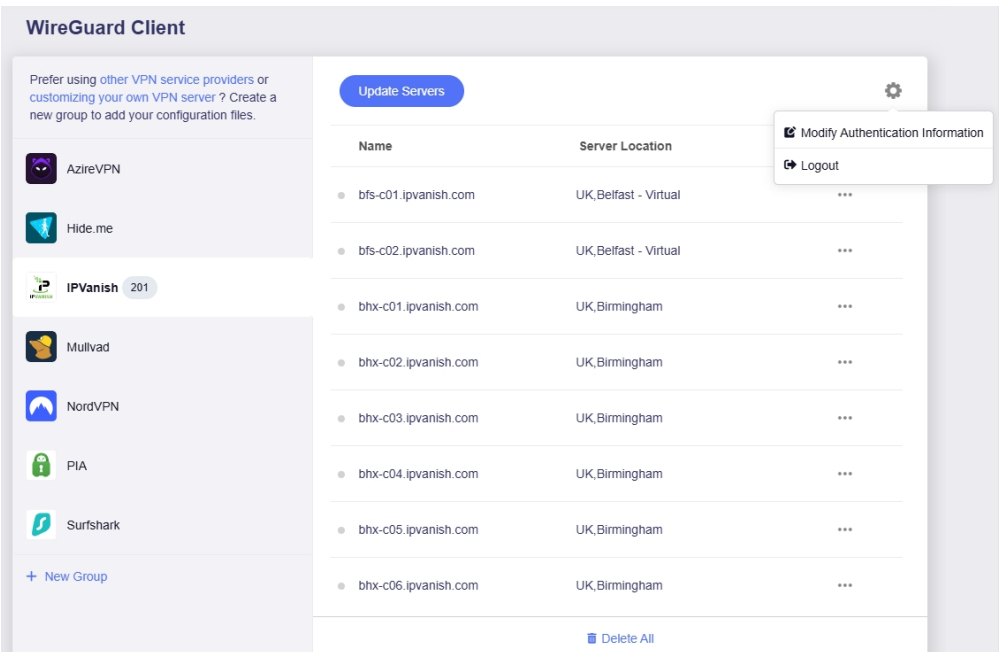
6. Actualizar servidores.

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



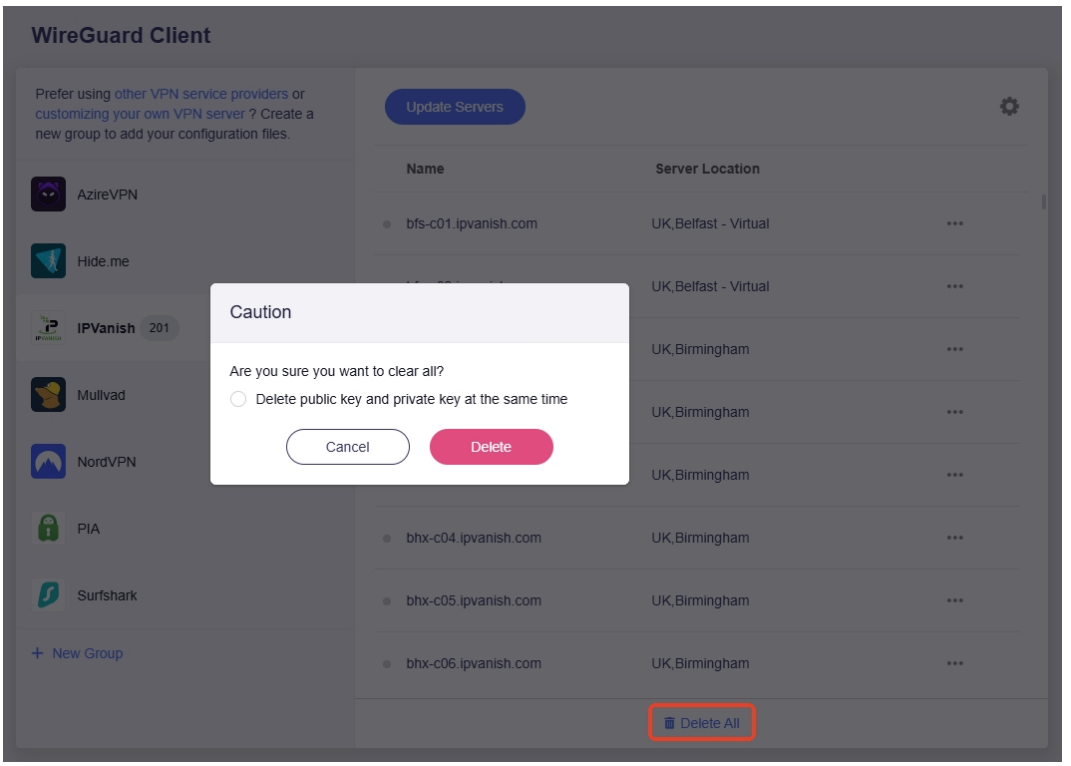
7. Edite las credenciales o cierre sesión.

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



8. Eliminar todos los archivos.

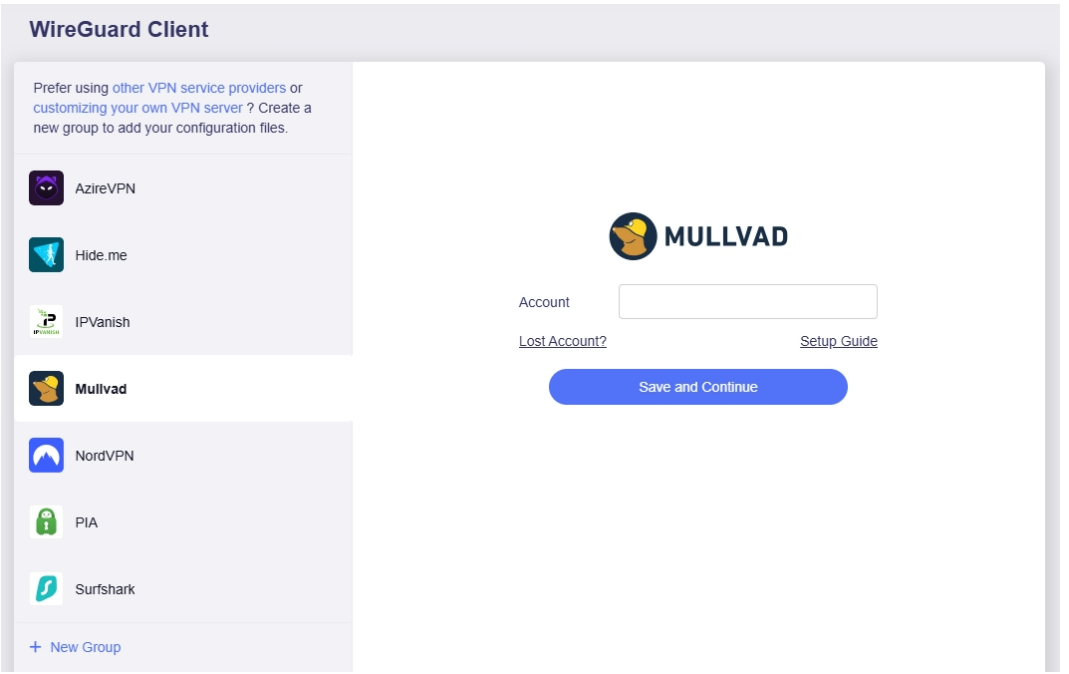
   Puede hacer clic en **Eliminar todo** para eliminar todos los archivos de configuración con un solo clic y elegir si desea eliminar las claves pública y privada simultáneamente.



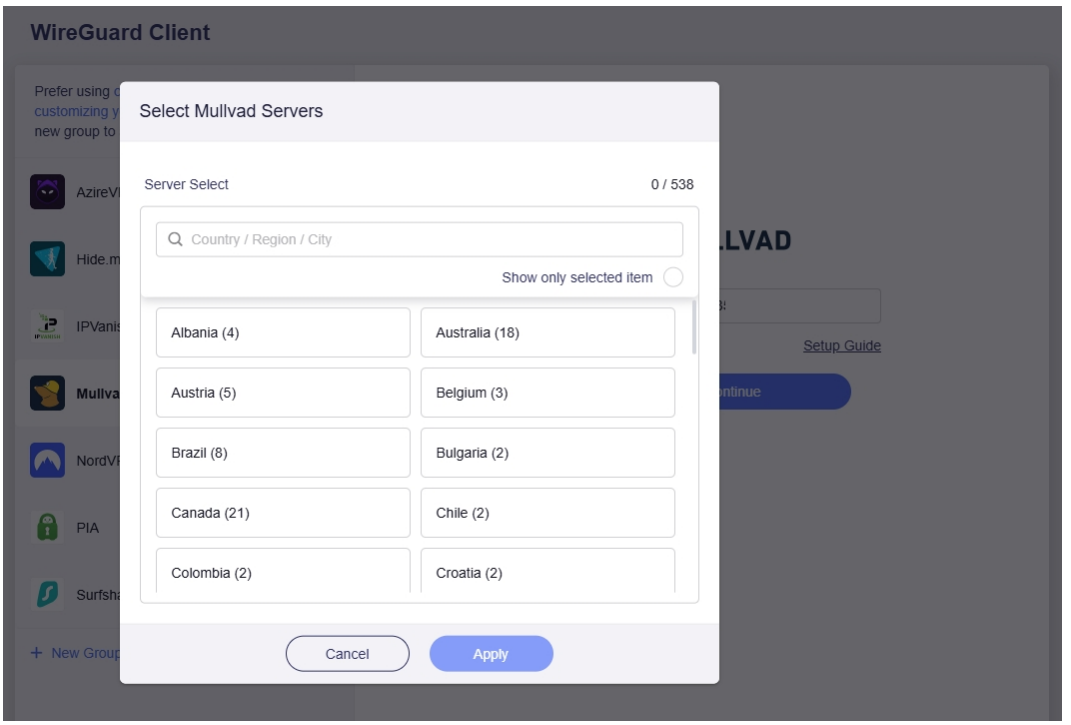
11.2.5 Configurar Mullvad

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

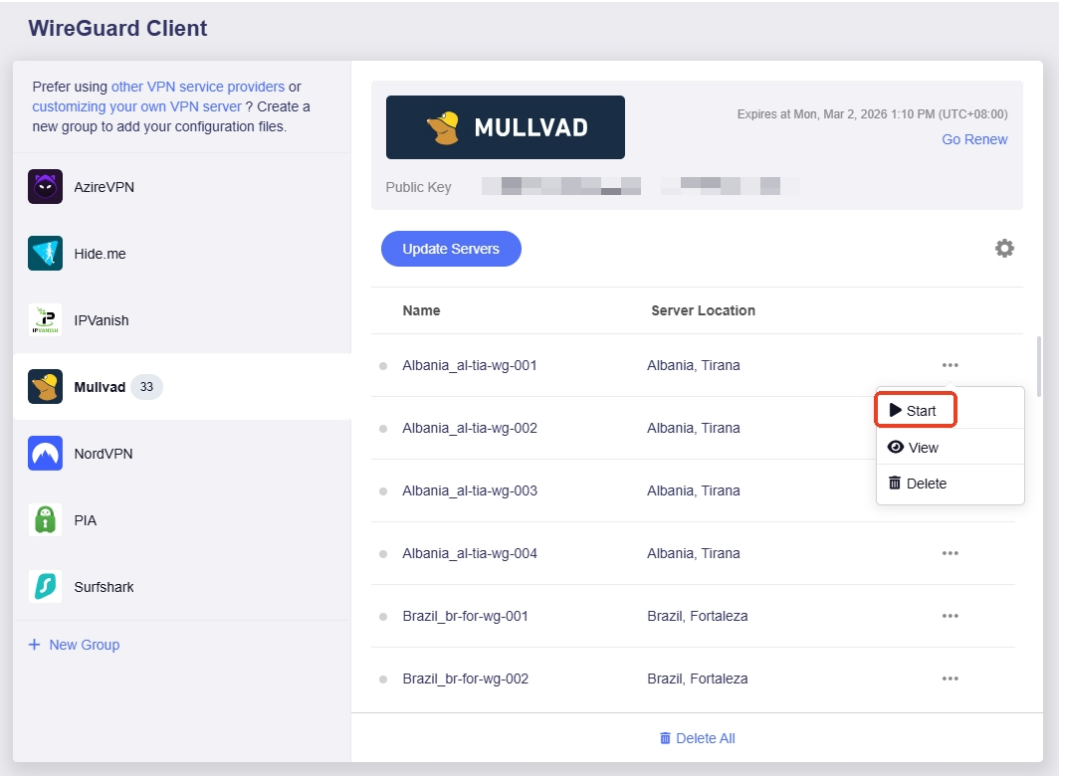
1. Iniciar sesiónn a su enrutador’s web admin panel y vaya a **VPN** > **Cliente WireGuard** > **Mullvad**.
2. Ingrese nombre de usuario y contraseña, luego haga clic en **Guardar y continuar**.



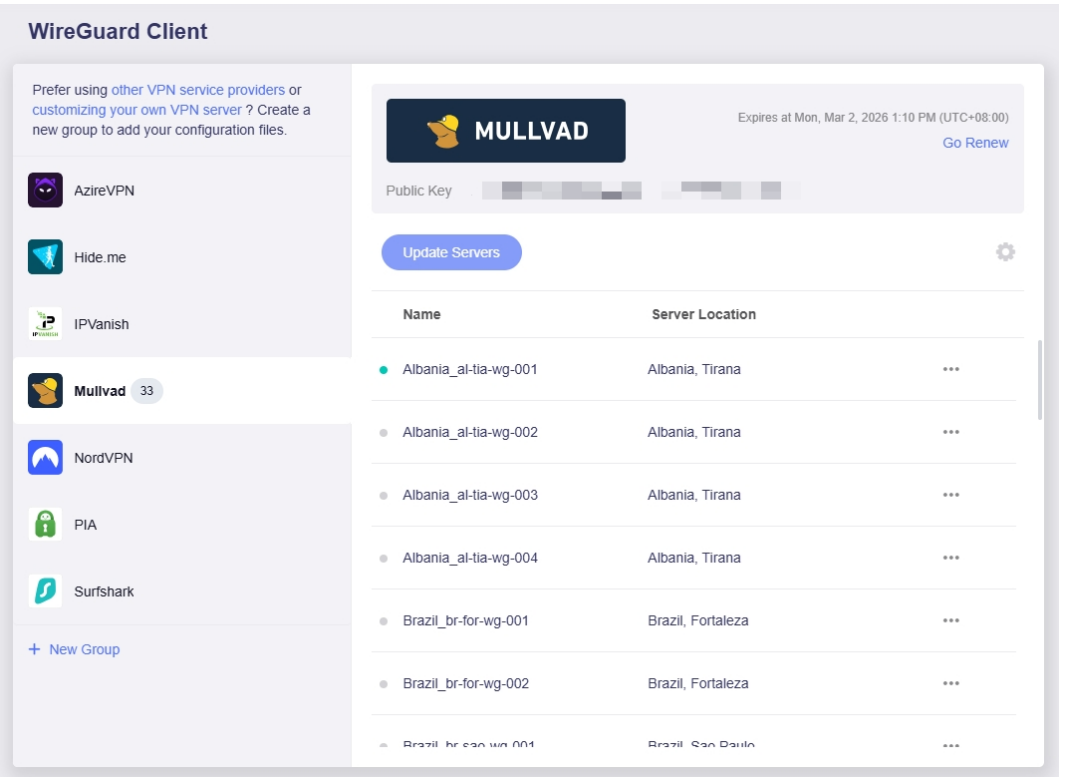
3. Seleccione los servidores a los que desea conectarse y haga clic en **Aplicar**.



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



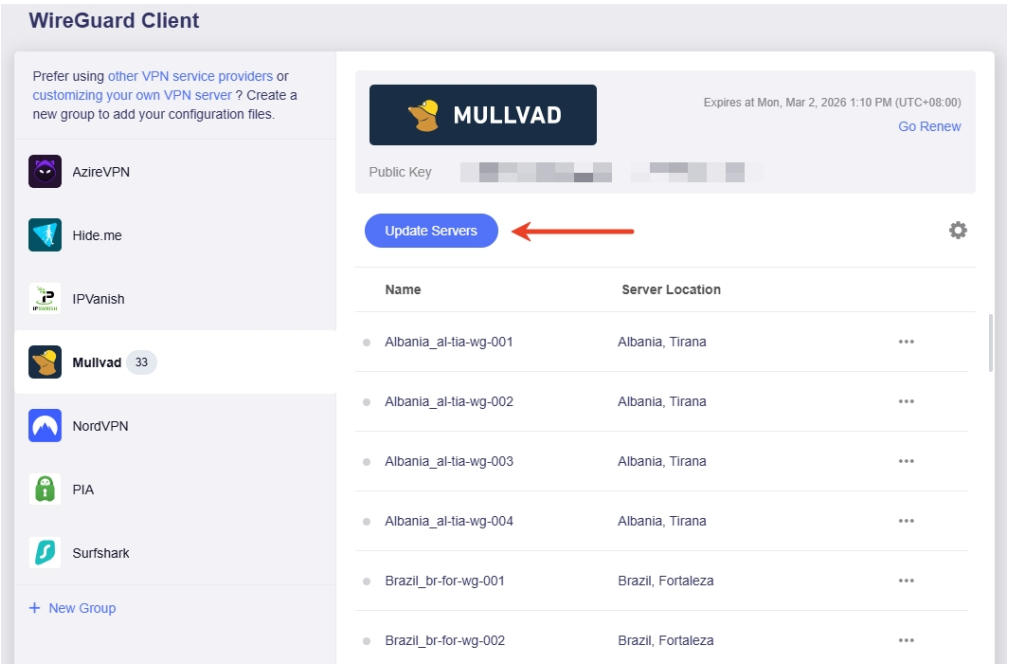
5. Una vez conectado, aparecerá un punto verde junto al archivo de configuración.



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

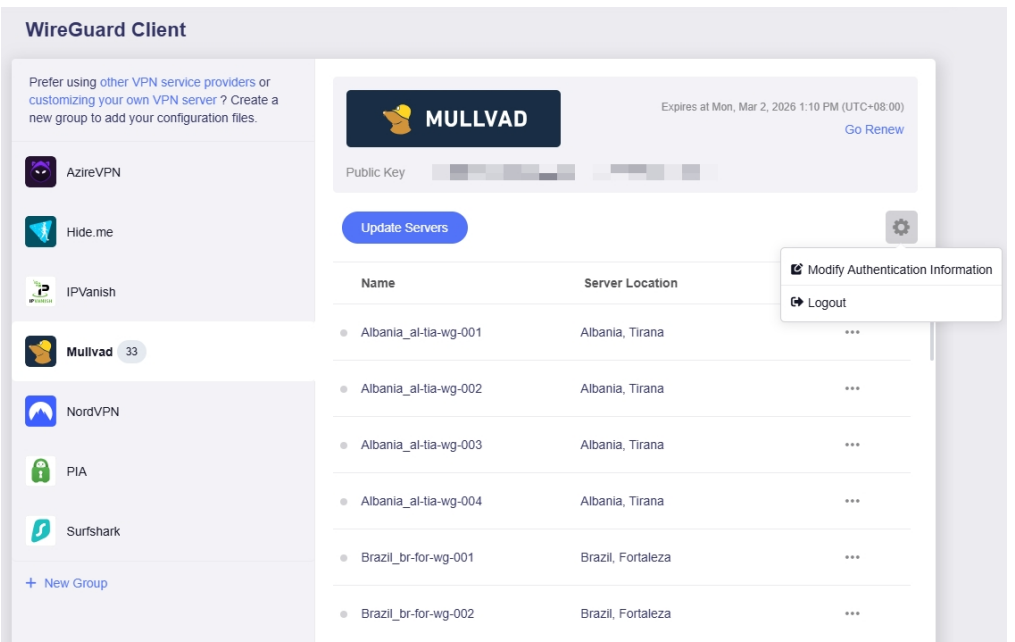
6. Actualice los servidores.

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



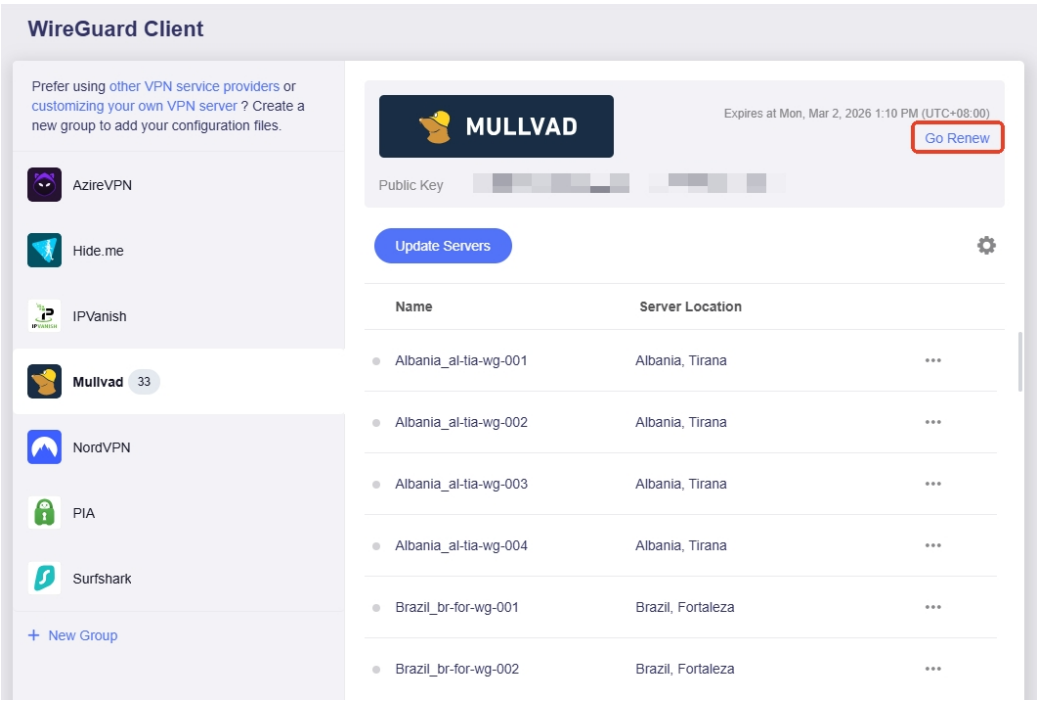
7. Edite las credenciales o cierre sesión.

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



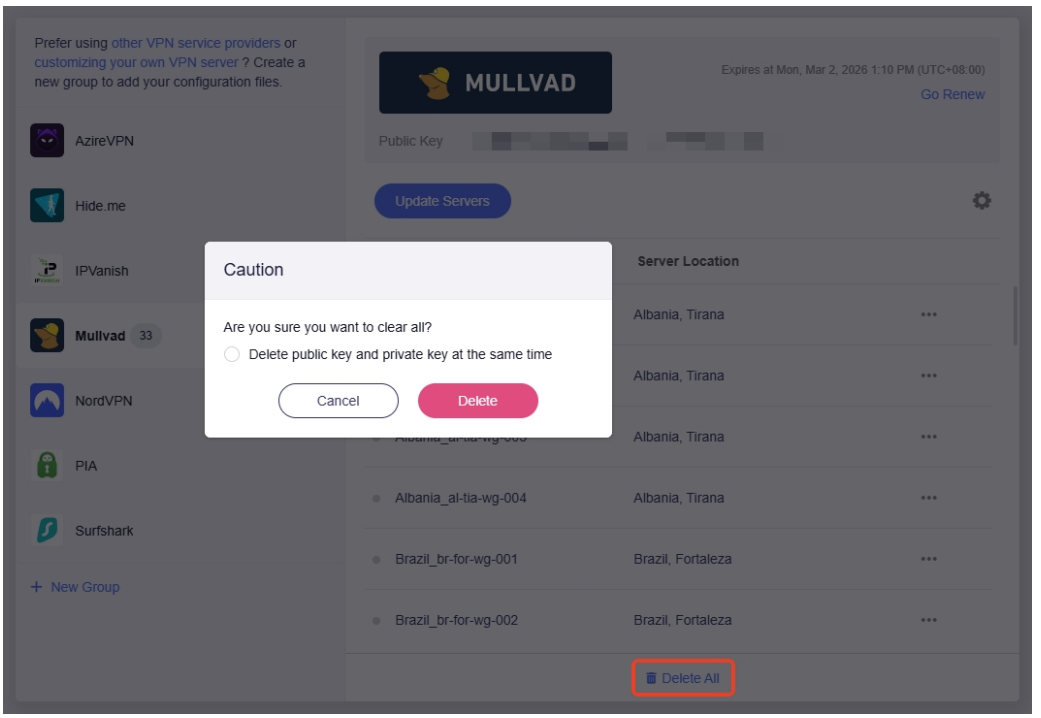
8. Ir a renovar.

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



9. Eliminar todos los archivos.

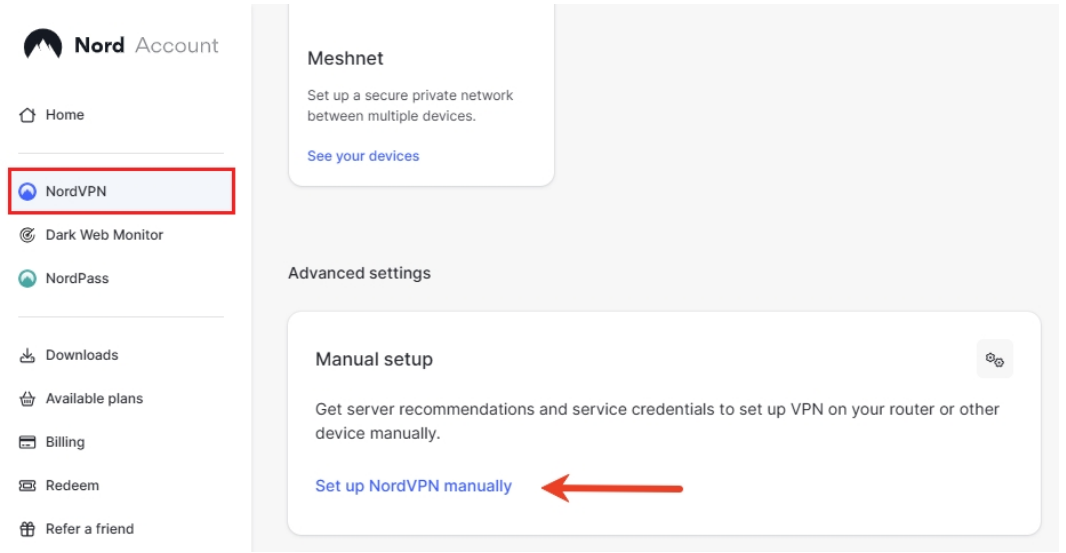
   Puedes hacer clic en **Eliminar todo** para eliminar todos los archivos de configuración con un solo clic y elija si desea eliminar las claves pública y privada simultáneamente.



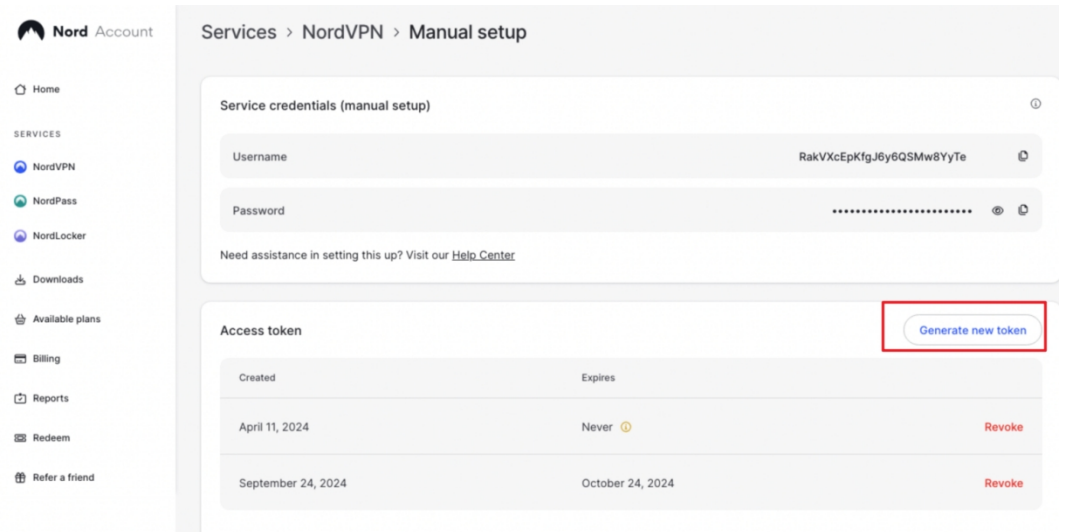
11.2.6 Configurar NordVPN

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

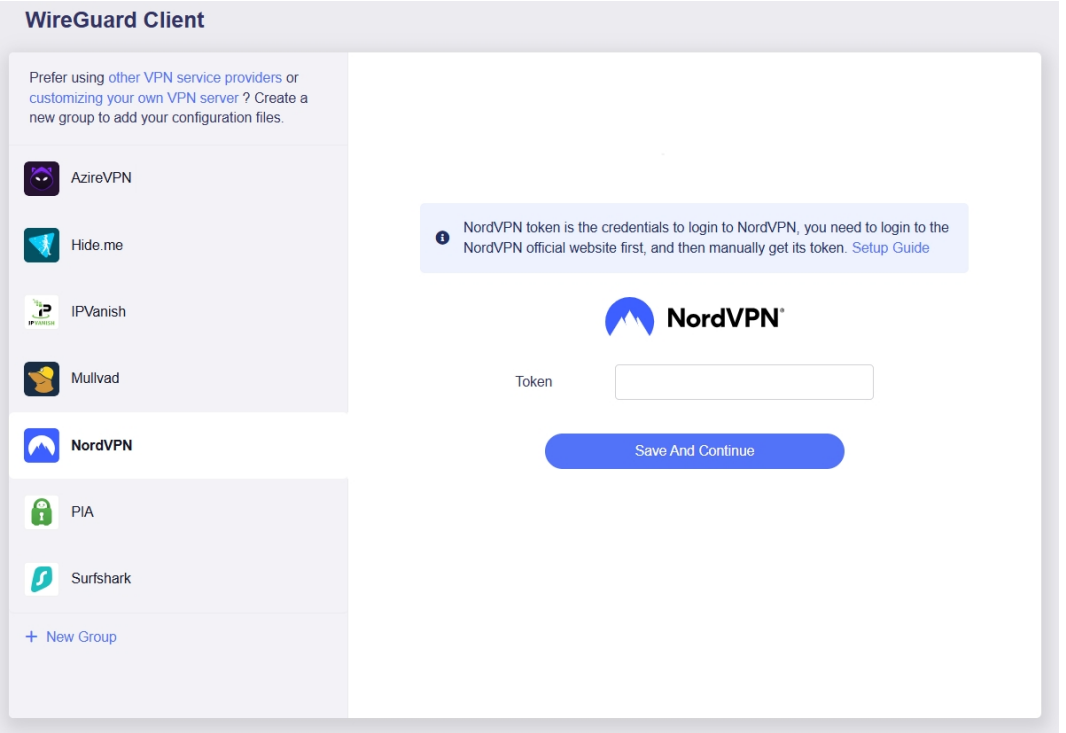
1. Inicie sesión en su cuenta web de NordVPN aquí.
2. Oen el Panel de control de Nord, haga clic en **NordVPN** y luego haga clic en **Configurar NordVPN manualmente**.



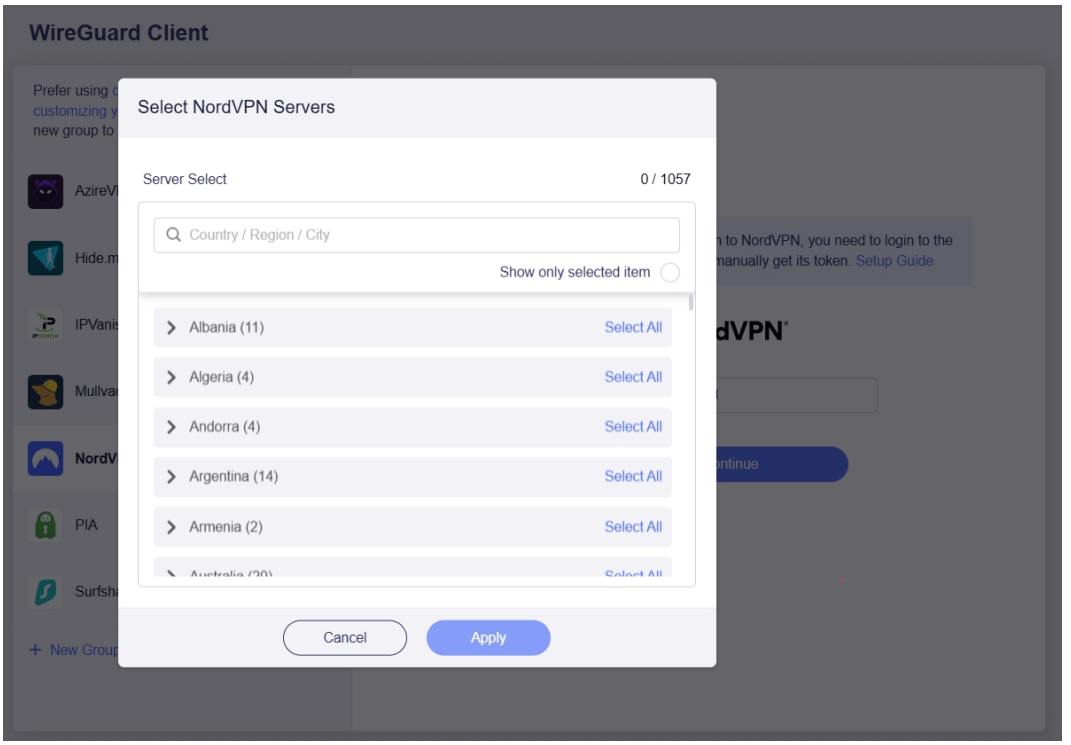
Encontrará el **Token de acceso**. Crear un token de acceso y ccopia para uso posterior.



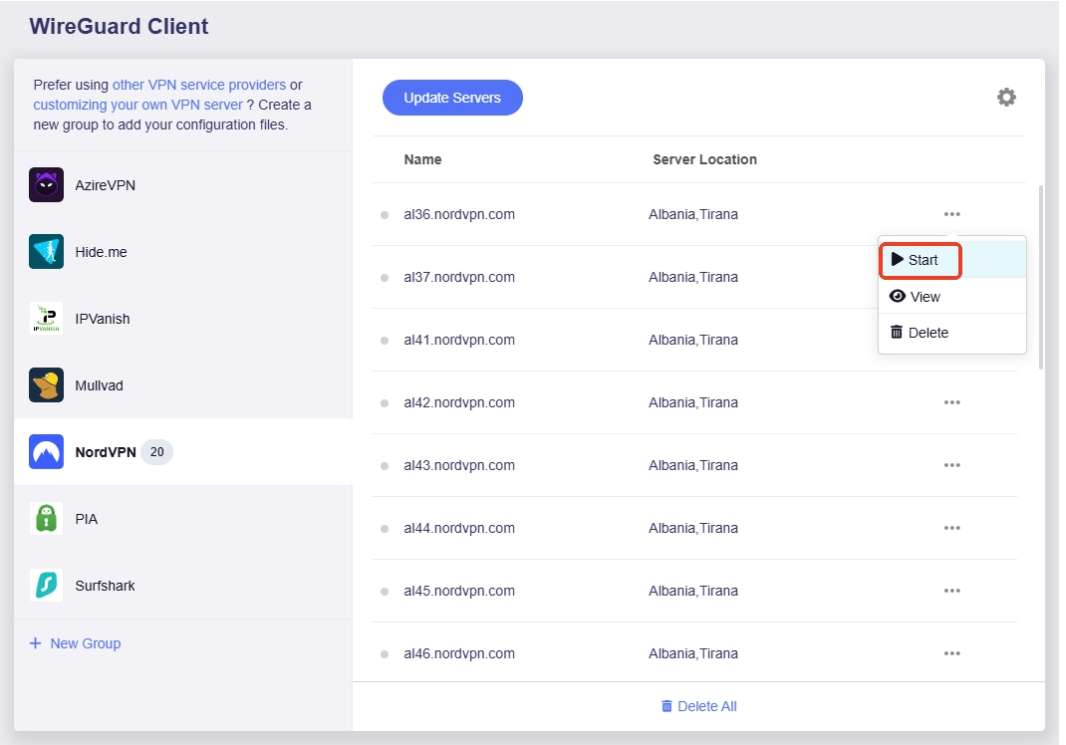
3. Inicie sesiónn en su enrutador's web admin panel y vaya a **VPN** > **Cliente WireGuard** > **NordVPN**.
4. Ingrese token, y haga clic en **Guardar y continuar**.



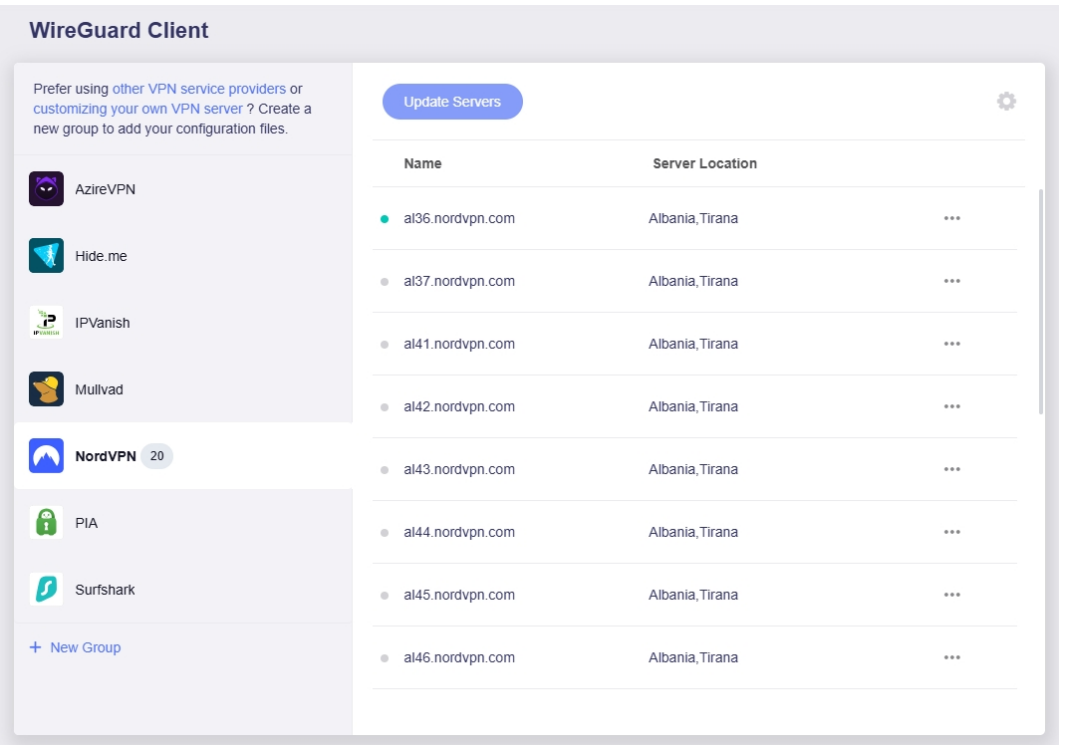
5. Seleccione los servidores a los que desea conectarse y haga clic en **Aplicar**.



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



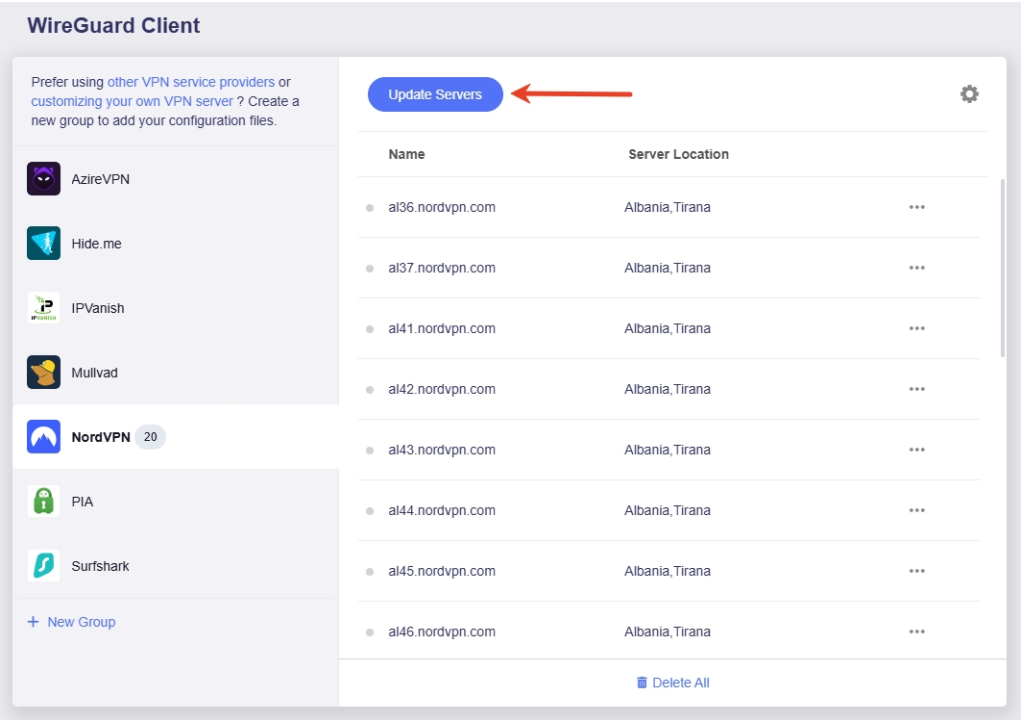
7. Una vez conectado, aparecerá un punto verde junto a la configuración. archivo.



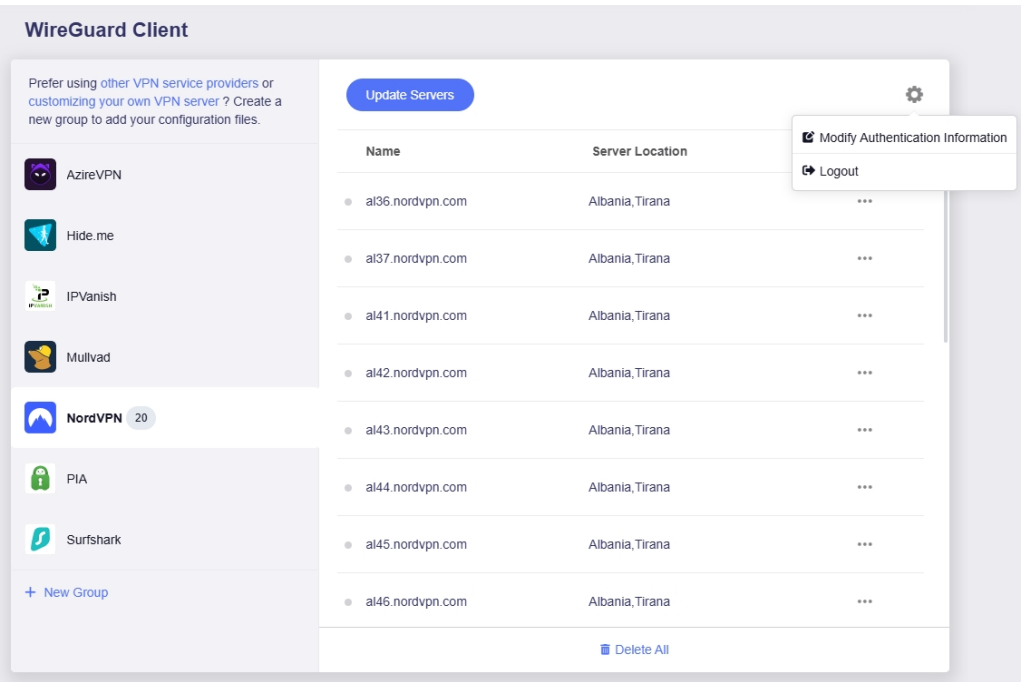
Usted puede también verificar los detalles de la conexión VPN en el **Panel de VPN**.

8. Actualizar servidores.

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

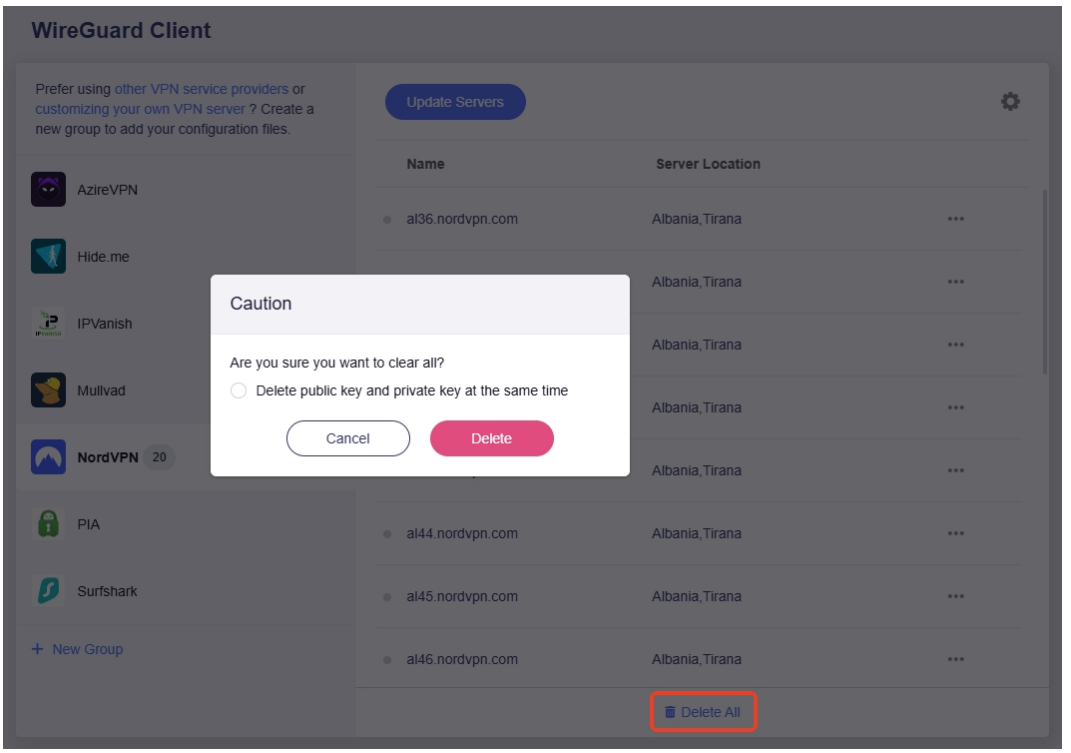


9. Edite las credenciales o cierre la sesión.
   Haga clic en el ícono de ajustes para editar sus credenciales de inicio de sesión o cierre la sesión.



10. Elimine todos los archivos.

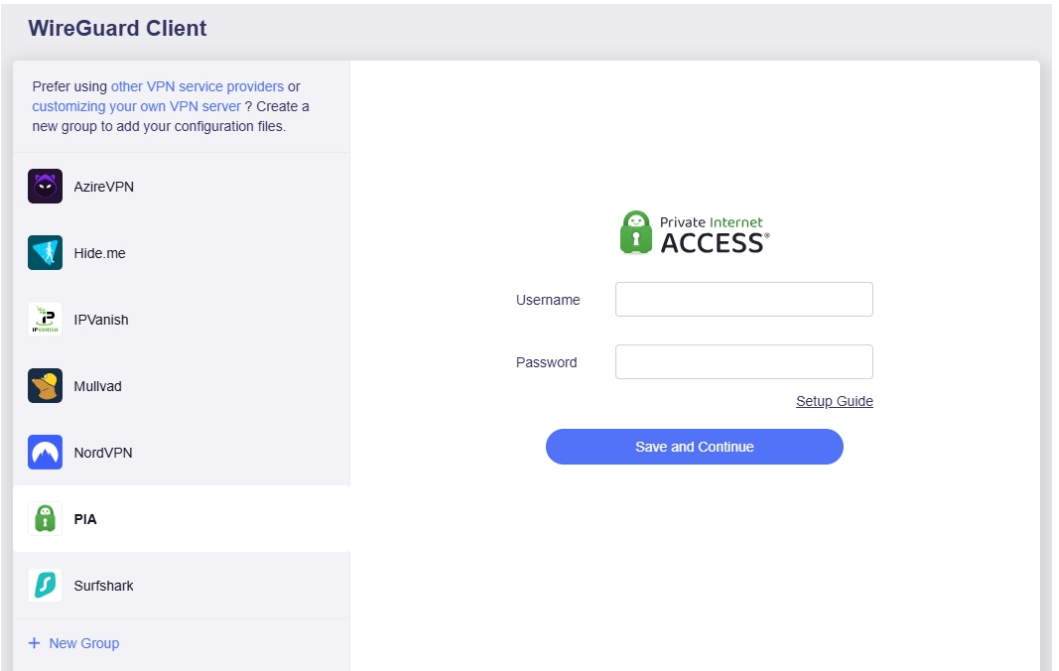
    Puedes hacer clic en **Eliminar todo** para eliminar todos los archivos de configuración con un solo clic y elija si desea eliminar las claves pública y privada simultáneamente.



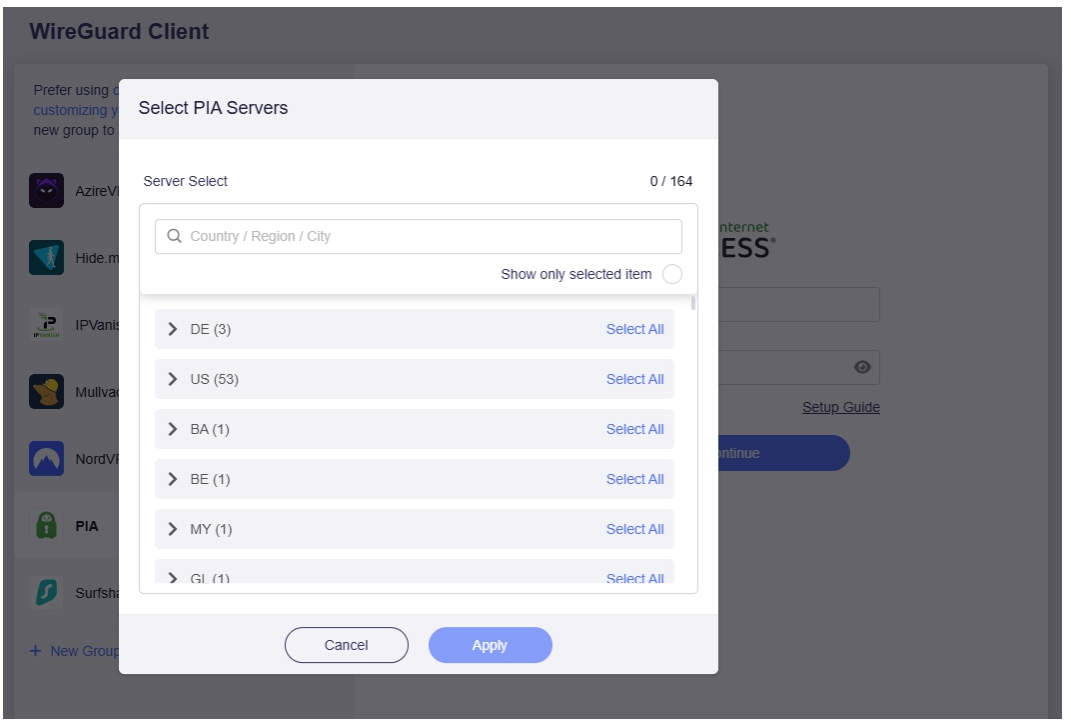
11.2.7 Configurar PIA (Private Internet Access)

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

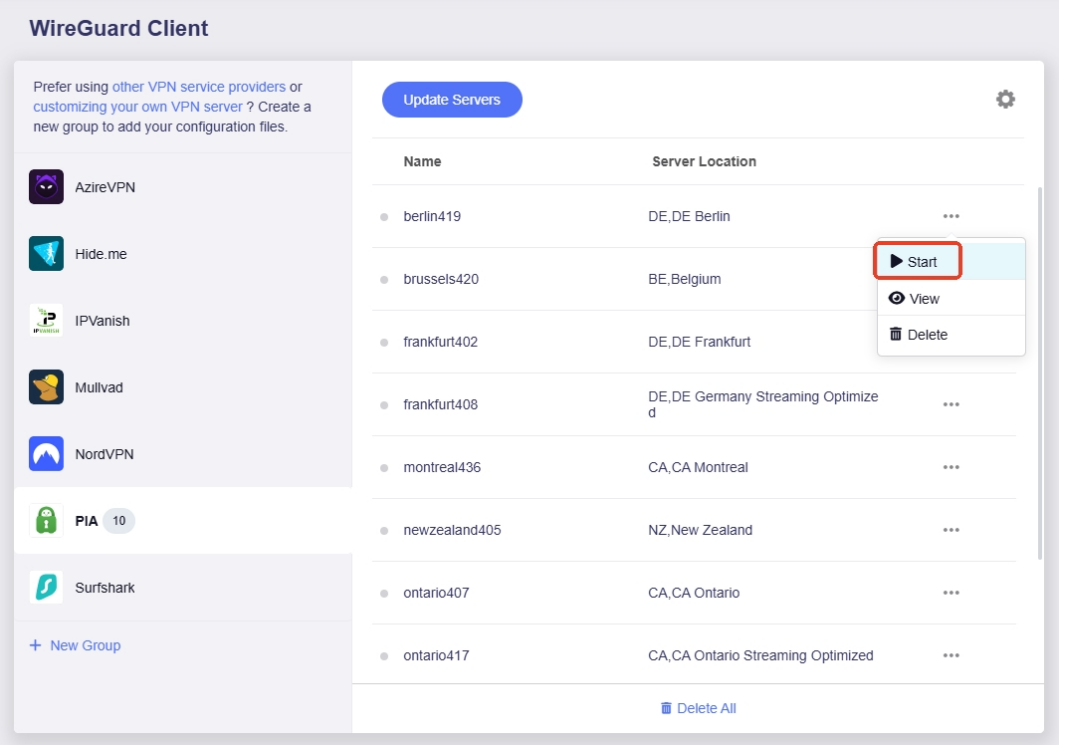
1. Iniciar sesión in a su enrutador's web admin panel y vaya a **VPN** > **WireGuard Client** > **PIA**.
2. Ingrese nombre de usuario y contraseña, luego haga clic en **Guardar y continuar**.



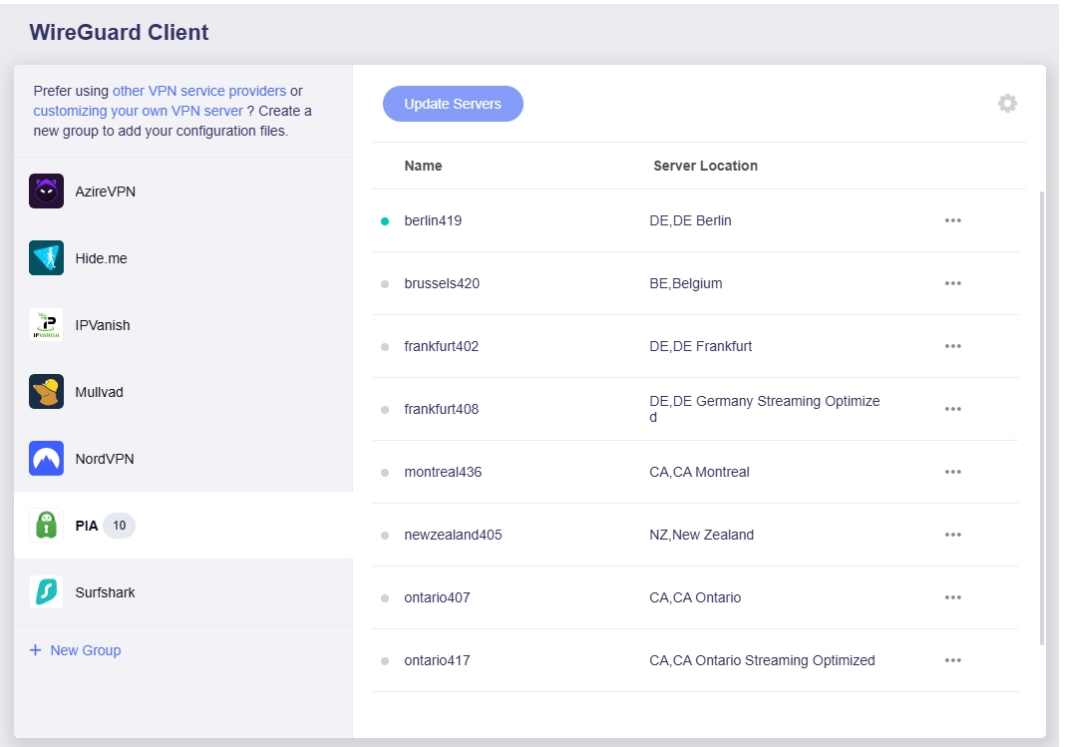
3. Seleccione los servidores a los que desea conectarse y haga clic en **Aplicar**.



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



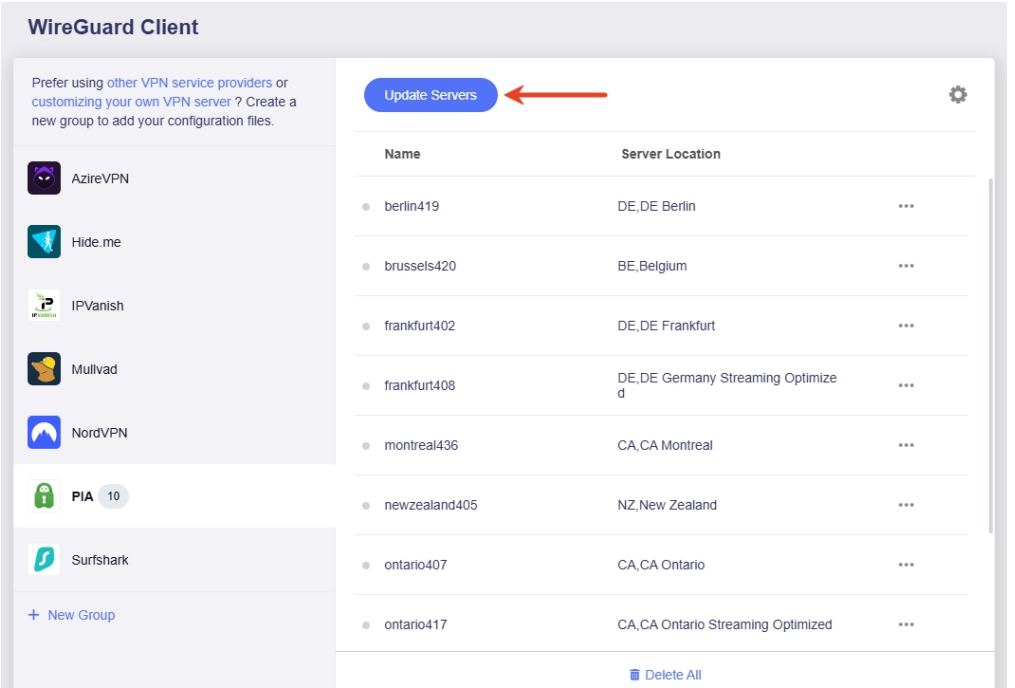
5. Una vez conectado, aparecerá un punto verde junto al archivo de configuración.



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

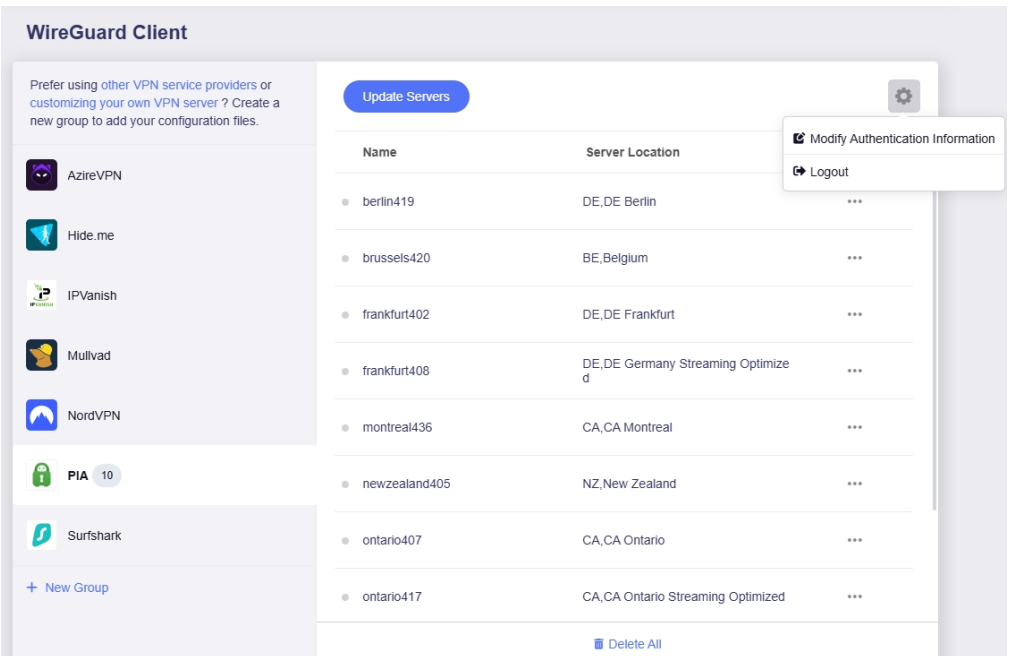
6. Actualizar servidores.

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



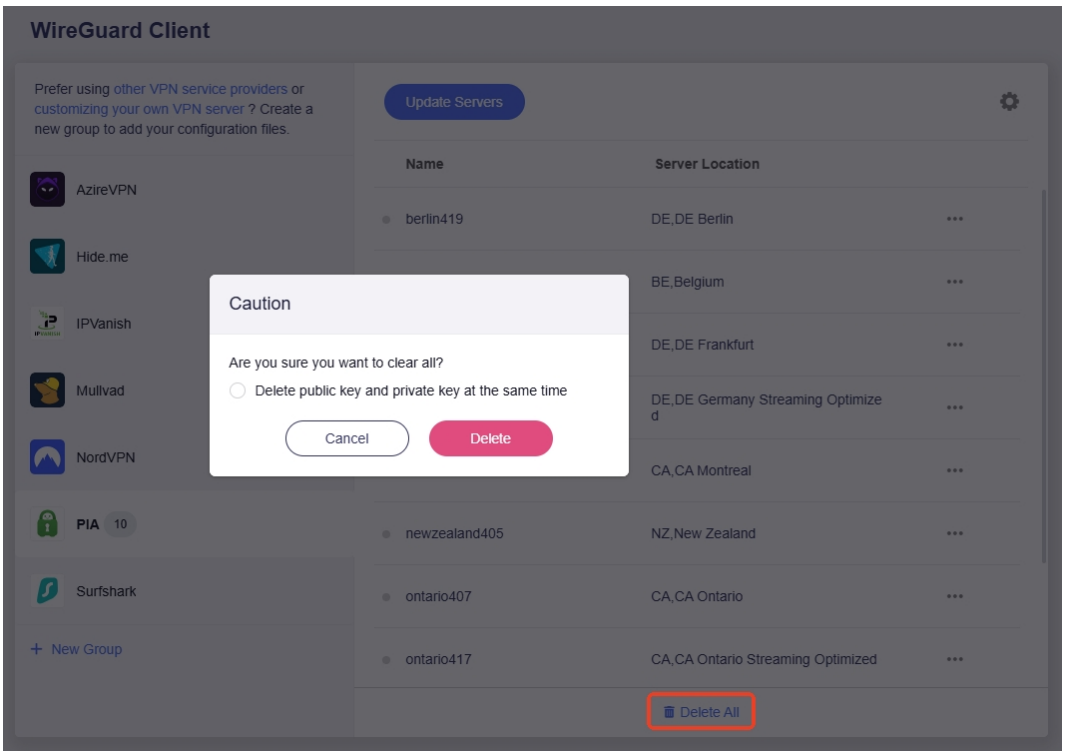
7. Edite las credenciales o cierre sesión.

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



8. Eliminar todos los archivos.

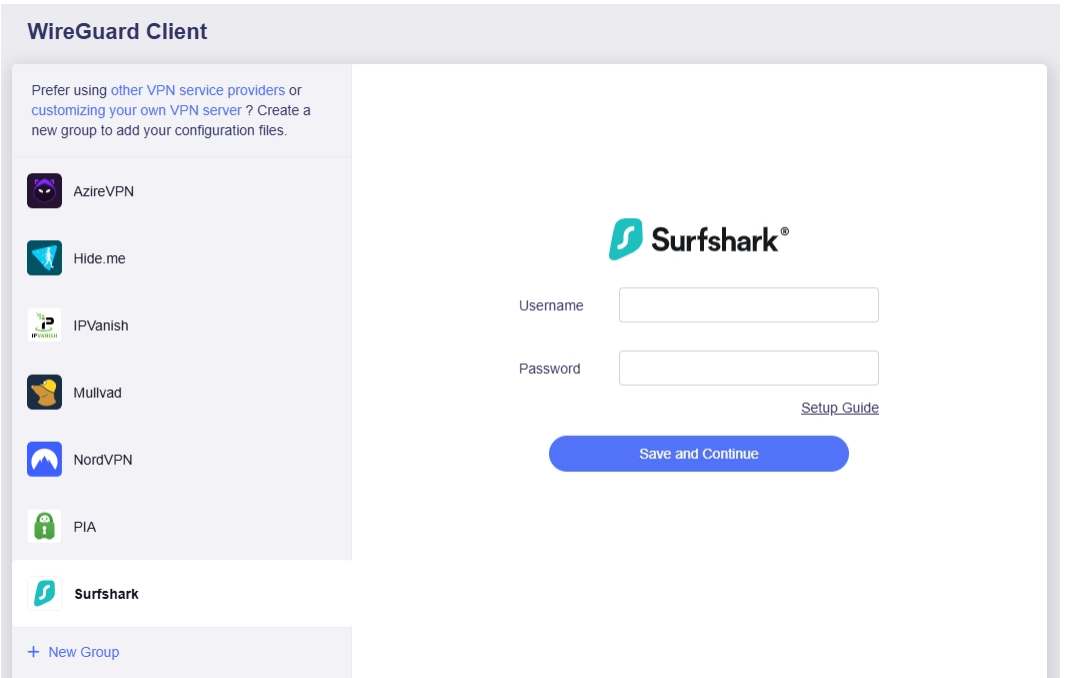
   Puede hacer clic en **Eliminar todo** para eliminar todos los archivos de configuración con un solo clic y elegir si desea eliminar los claves privadas y públicas simultáneamente.



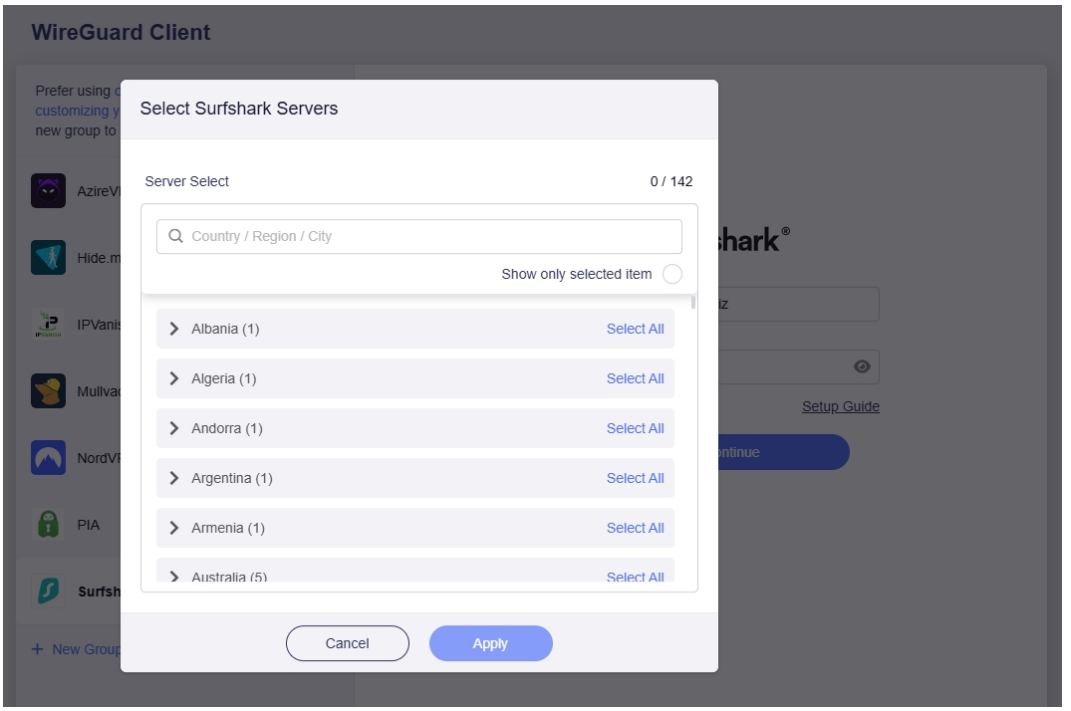
11.2.8 Configurar Surfshark

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

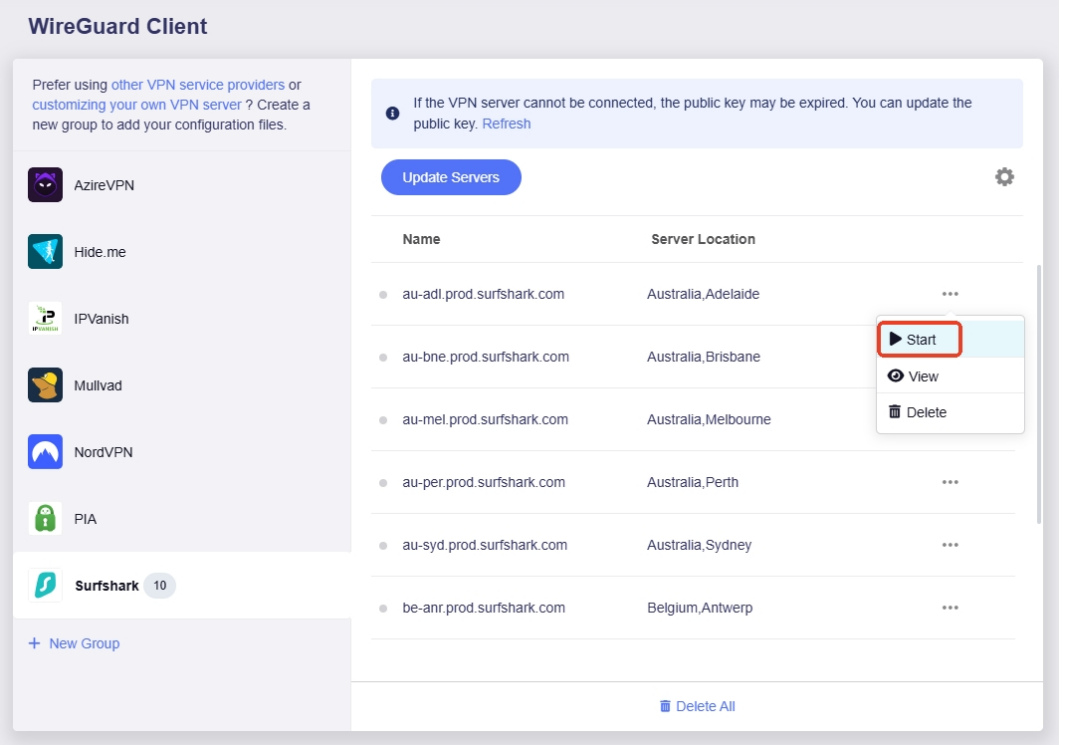
1. Iniciar sesiónn a su enrutador’s web admin panel y vaya a **VPN** > **WireGuard Client** > **Surfshark**.
2. Ingrese nombre de usuario y contraseña, luego haga clic en **Guardar y continuar**.



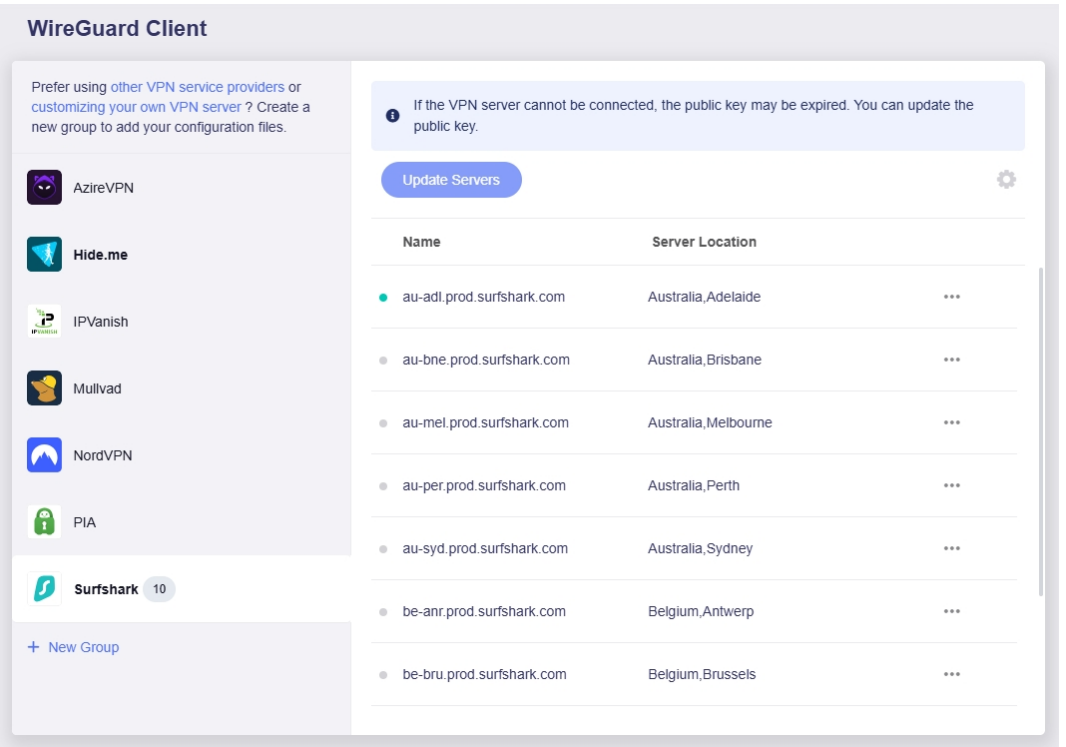
3. Seleccione los servidores a los que desea conectarse y haga clic en **Aplicar**.



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



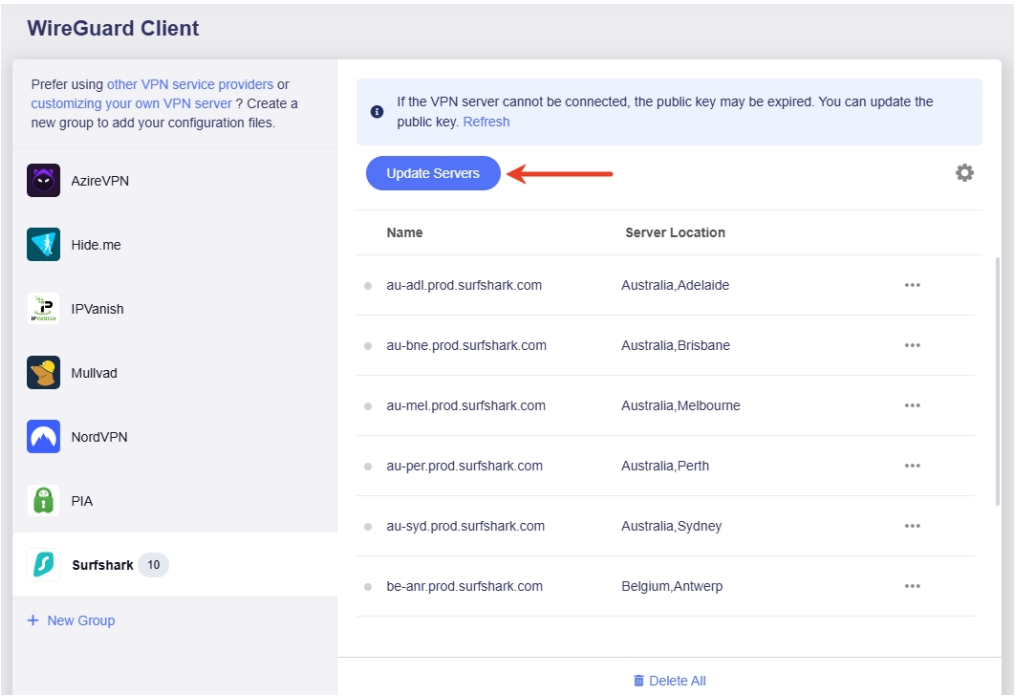
5. Una vez conectado, aparecerá un punto verde junto al archivo de configuración.



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

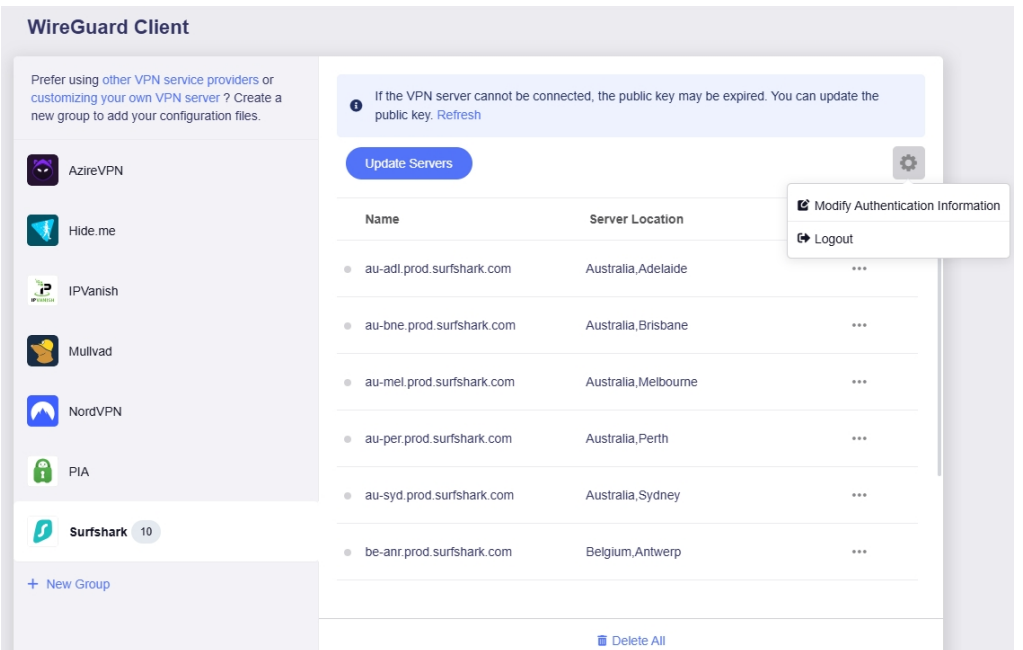
6. Actualizar servidores.

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



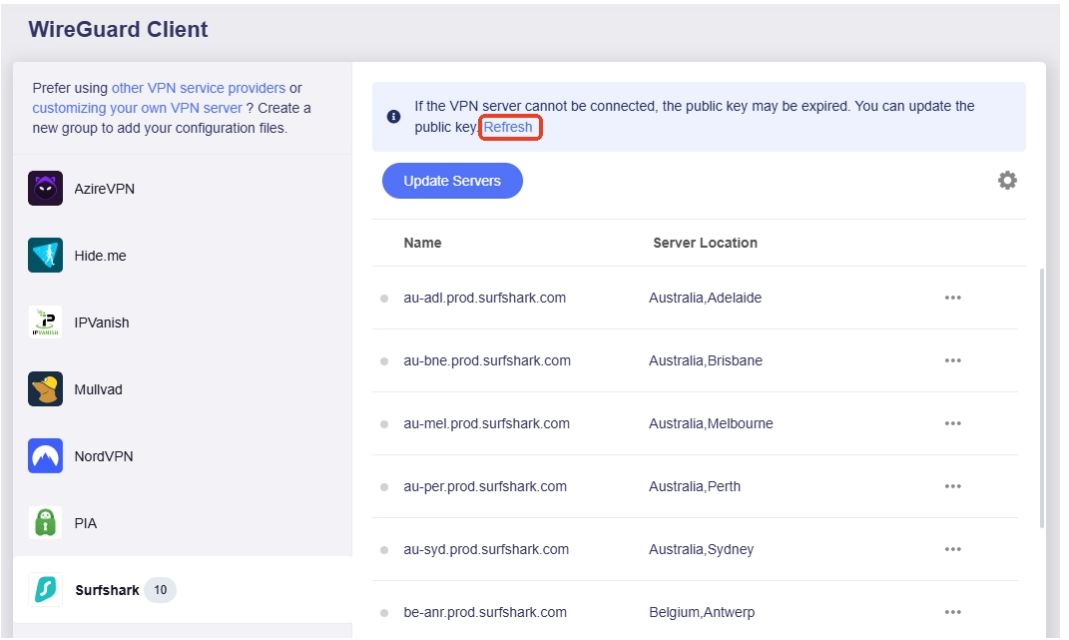
7. Editar credenciales o cerrar sesión.

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



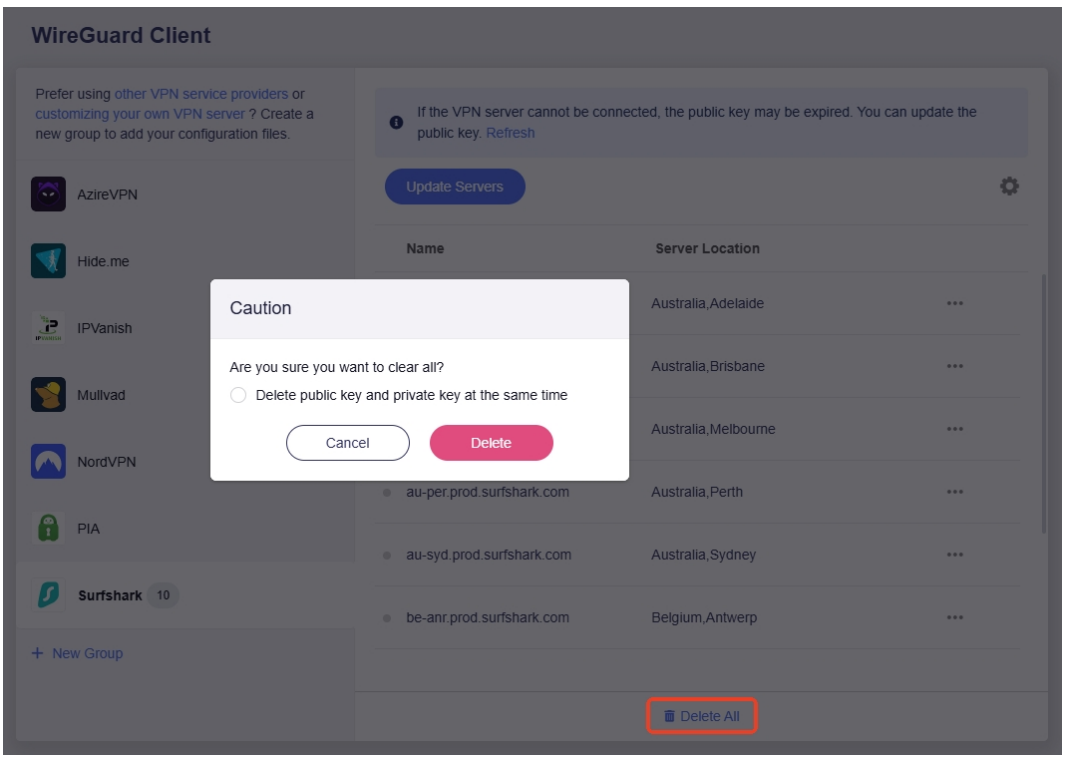
8. Actualizar.

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



9. Eliminar todos los archivos.

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

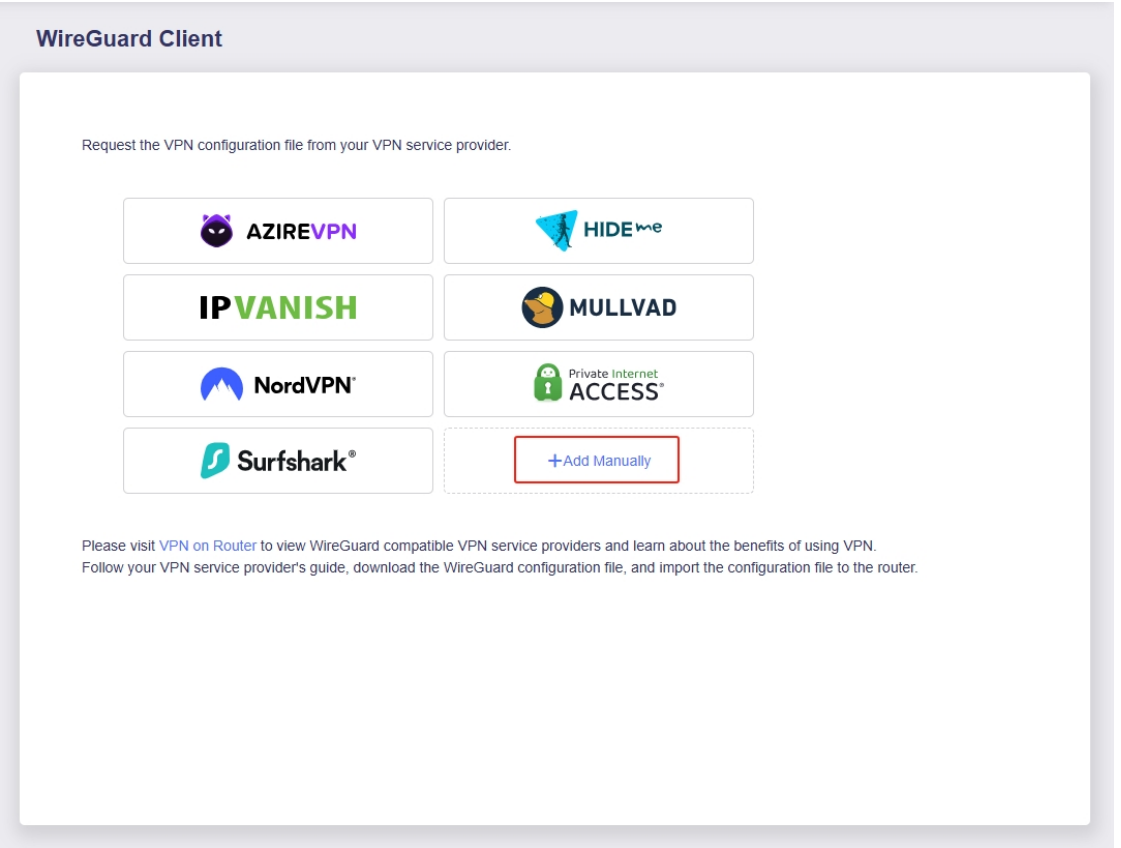


11.2.9 Configurar el cliente WireGuard manualmente (para otros proveedores)

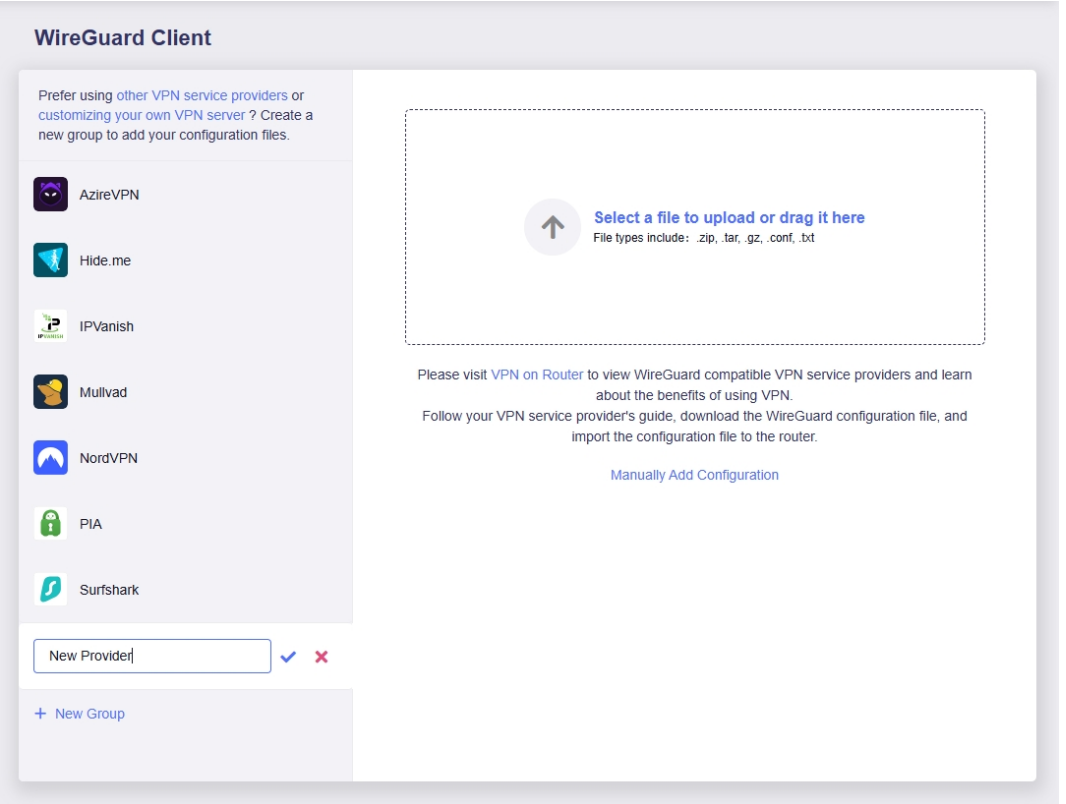
Si su proveedor de servicios WireGuard no está integrado en el panel de administración web, visite primero el sitio web oficial de su proveedor de servicios suscrito para obtener el archivo de configuración. Luego cárguelo en el enrutador para configurar un cliente WireGuard. Si no sabes cómo descargar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

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

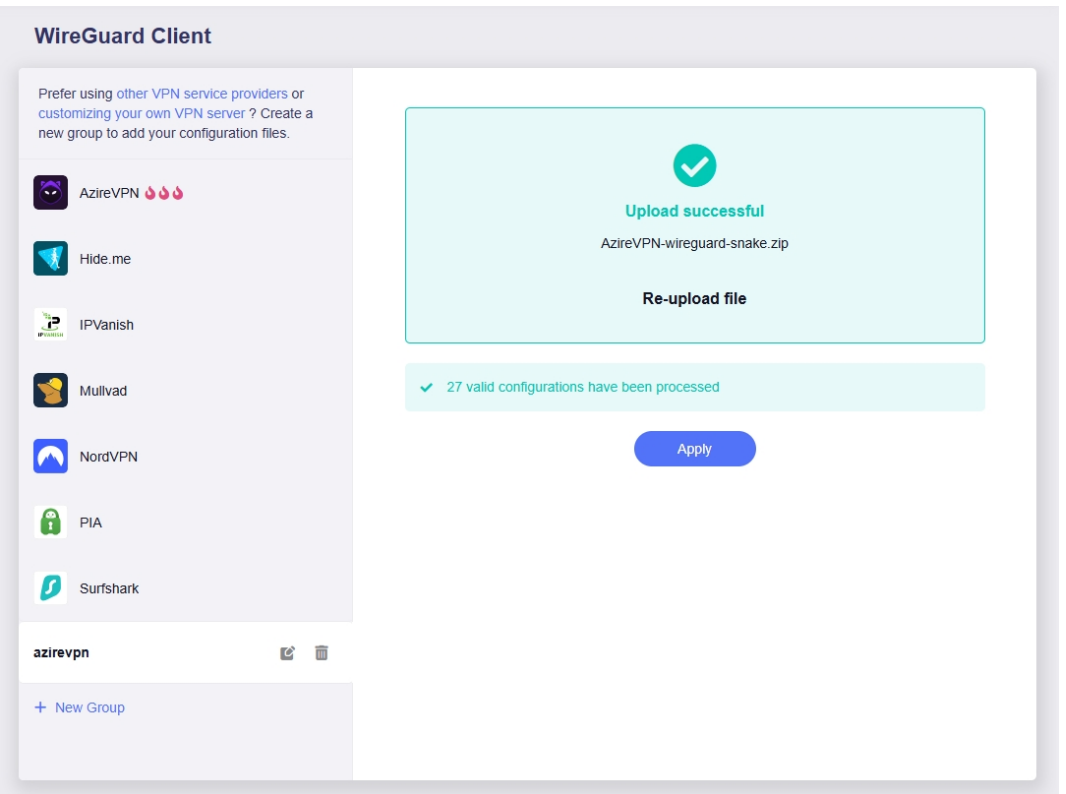
1. Inicie sesiónn en su enrutador's web admin panel y navegue hasta **VPN** > **Cliente WireGuard** > **Agregar manualmente**.



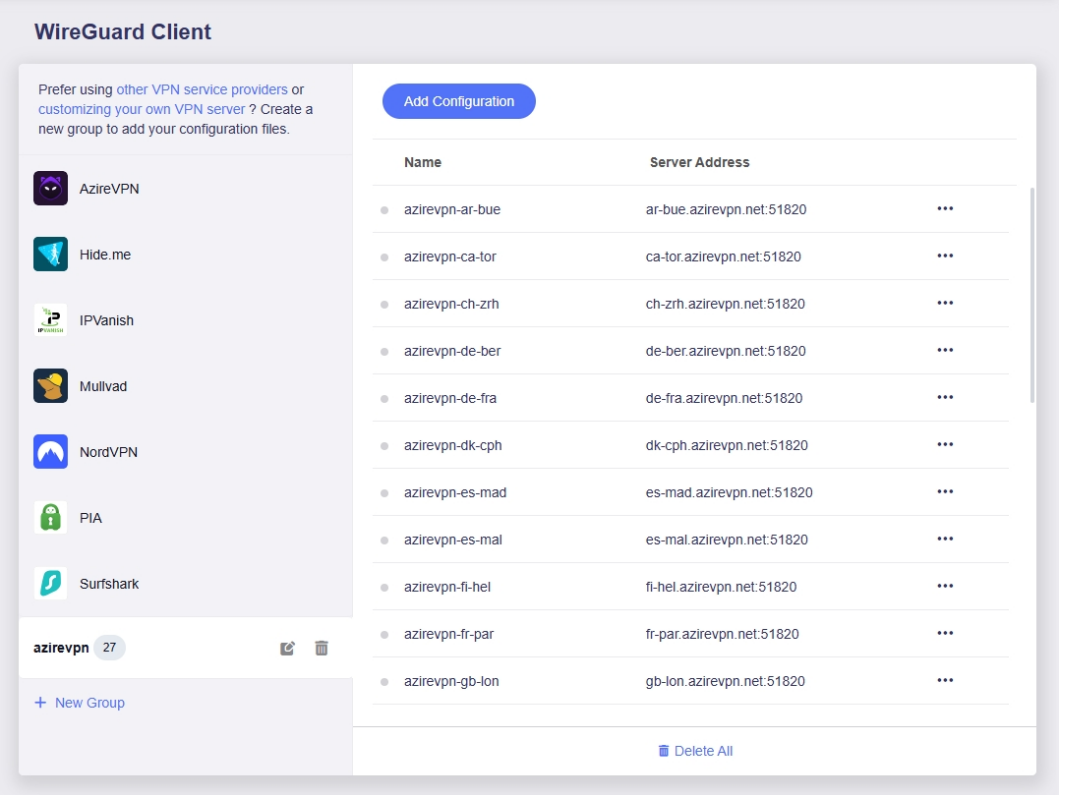
2. Se creará un grupo en la barra lateral izquierda. Establezca un nombre descriptivo para el grupo.



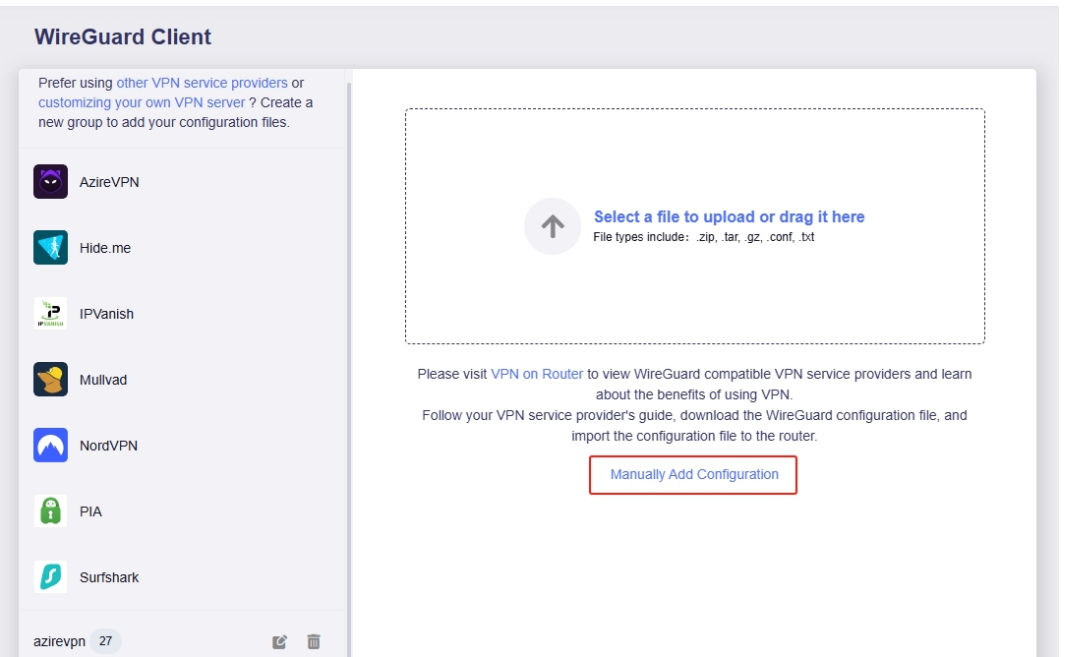
3. Click el área de carga para cargar su archivo de configuración WireGuard (formatos admitidos: zip, tar, gz, conf, txt), y haga clic en **Aplicar**.

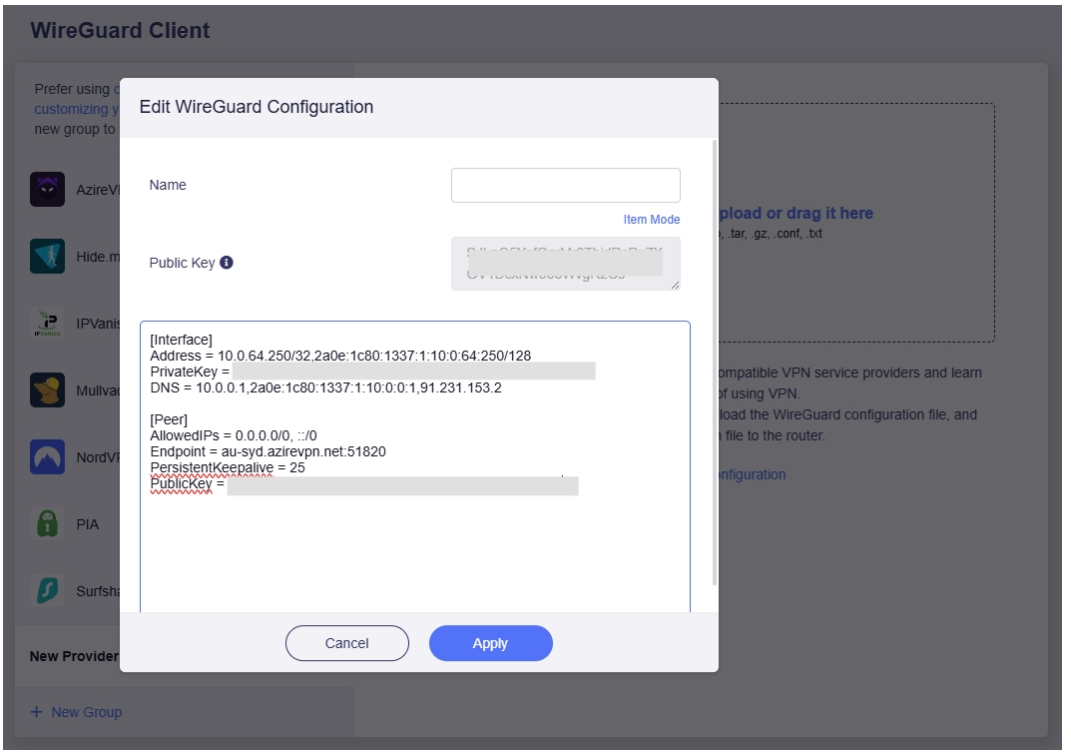


Si carga un archivo comprimido que contiene varios archivos de configuración, se descomprimirá automáticamente, como se muestra a continuación.

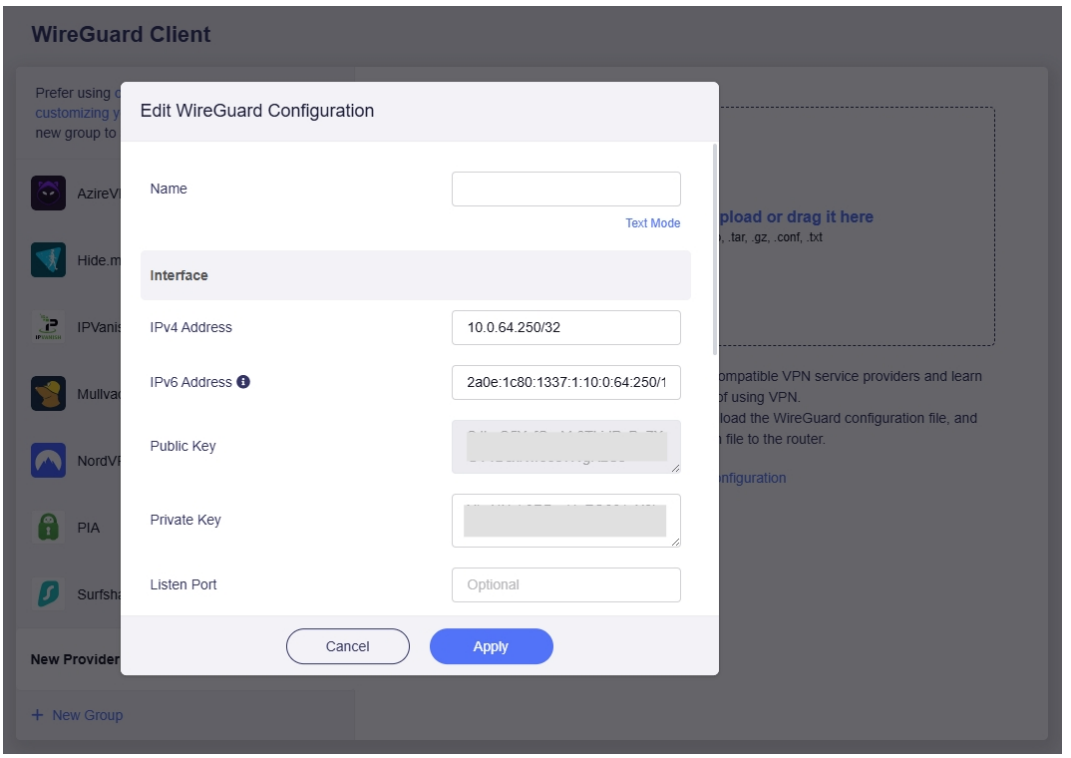


Como alternativa, puede hacer clic en **Agregar configuración manualmente** en en la parte inferior del área de carga, agregue los detalles de configuración en forma de texto y haga clic en **Aplicar**.

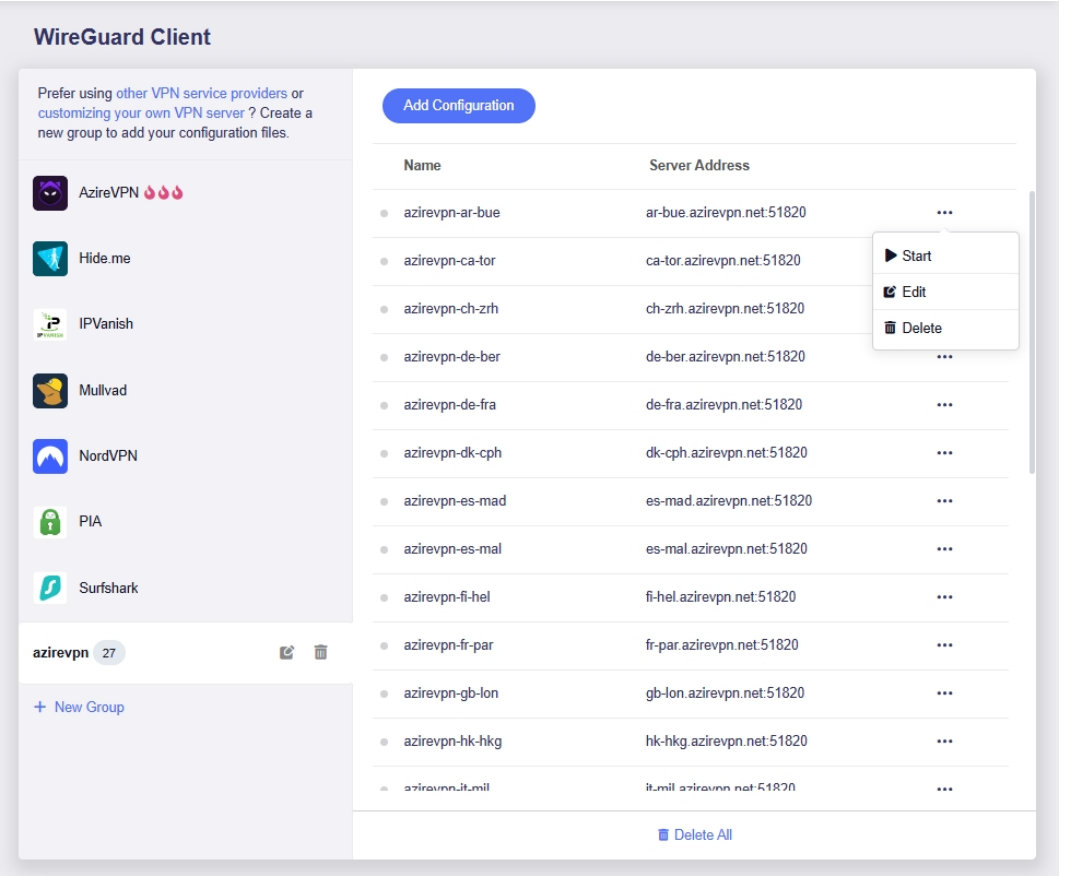




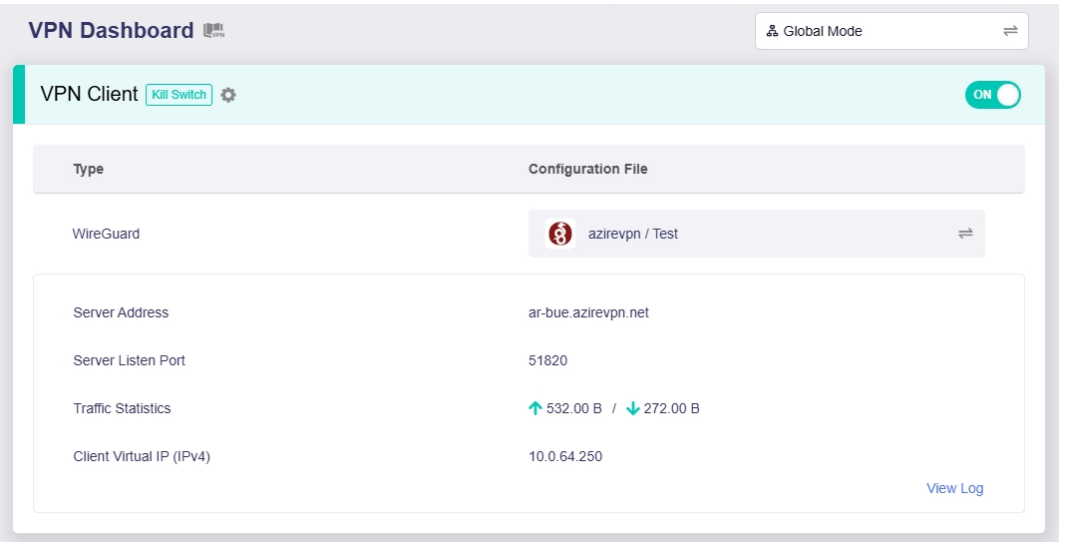
Si desea verificar cada elemento, puede cambiar al modo Elemento y verificar la configuraciónuración detalles, luegoluego haga clic en **Aplicar**.



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



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



Capítulo 12

Red

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

12.1 Multi-WAN

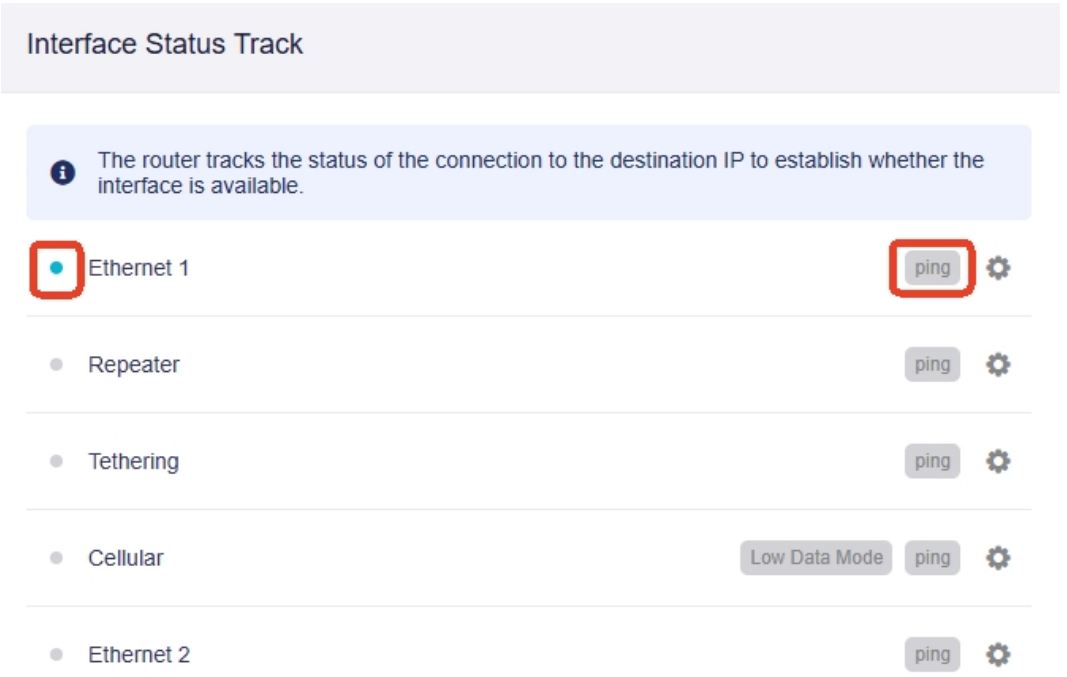
Multi-WAN permite el uso simultáneo de múltiples métodos de acceso a Internet, lo que permite la configuración de diversas opciones de conectividad en el enrutador. Ofrece dos modos de trabajo:

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

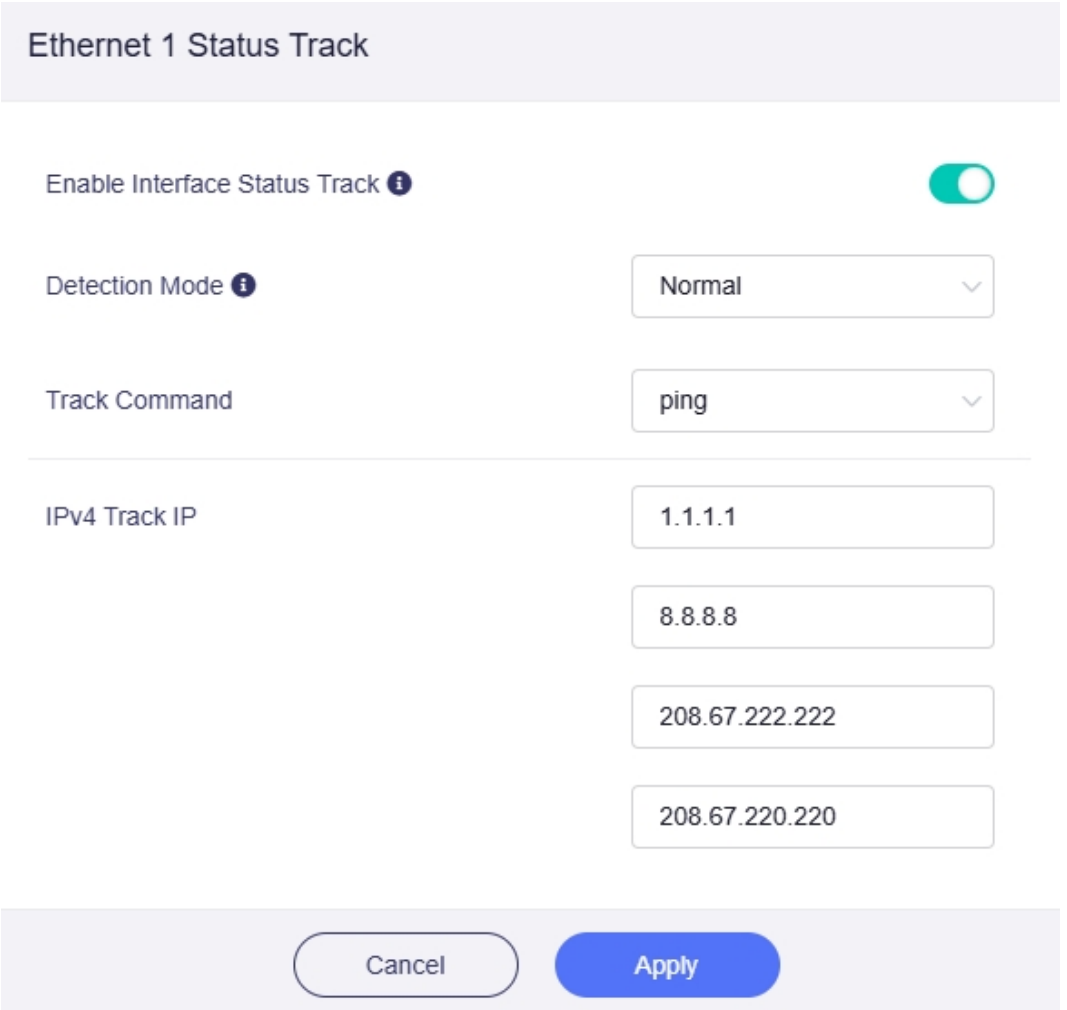
Inicie sesión en el panel de administración web de su enrutador' y navegue hasta **RED** > **Multi-WAN**. Esta página incluye dos secciones: Seguimiento del estado de la interfaz y modo Multi-WAN.

12.1.1 Seguimiento del estado de la interfaz

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



En la sección **Seguimiento del estado de la interfaz**, haga clic 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.



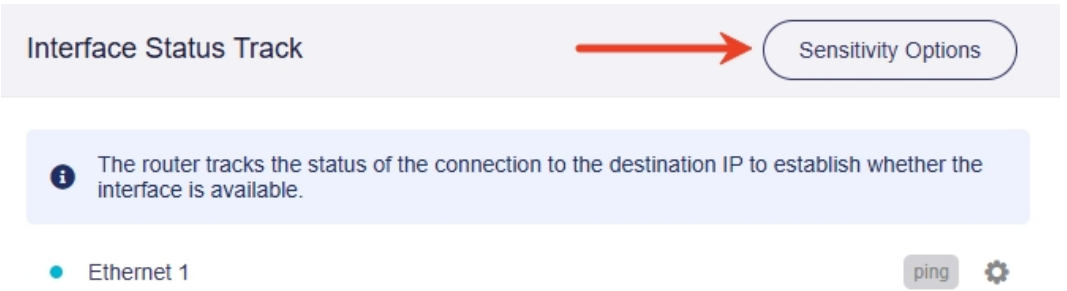
- **Habilitar seguimiento del estado de la interfaz**: Está habilitadode forma predeterminada. Si está deshabilitado, el enrutador determinará el estado de la interfaz según las condiciones (por ejemplo, si el cable Ethernet está enchufado).
- **Modo de detección**: esta función se introdujo como modo de datos bajos en firmware v4.5, luego renombrado Modo de detección en firmware v4.7. Hay tres modos disponibles: Modo normal, Modo de datos bajos y Modo estricto.
  - **Normal Modo**: Es used de forma predeterminada.
  - **Datos bajos Modo**: Solo activa el seguimiento cuando se produce un error de red en la red interfaz. Utilice este modo si tiene un plan de datos limitado. Tenga en cuenta que la reconexión después de una desconexión puede ser un poco más lenta que en

el modo normal y está habilitado de forma predeterminada solo para la interfaz celular.

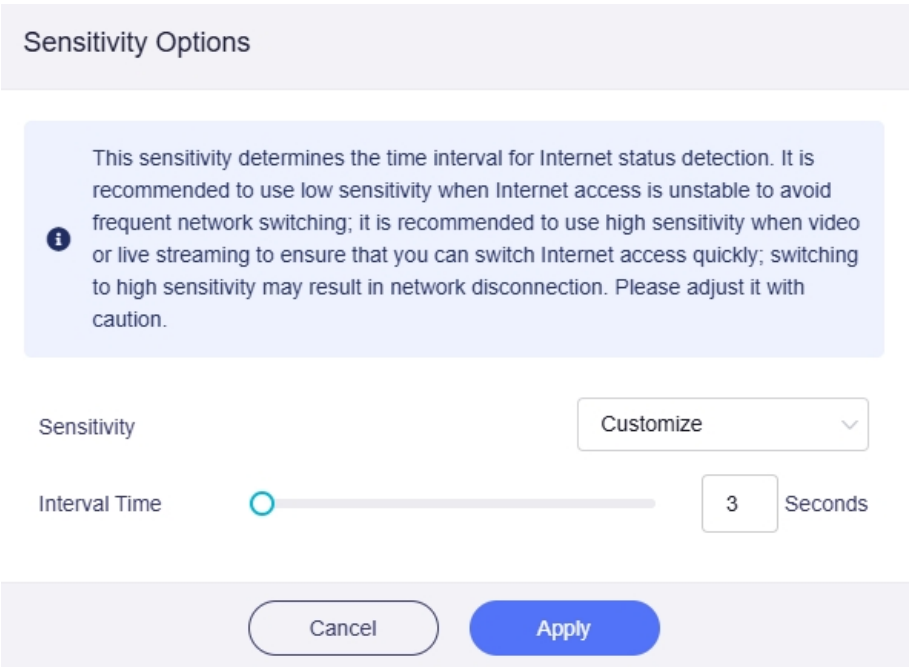
- **Estricto Modo**: Determina el estado de la interfaz exclusivamente en función de los resultados de un comando de detección enviado a una IP pública.

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

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



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



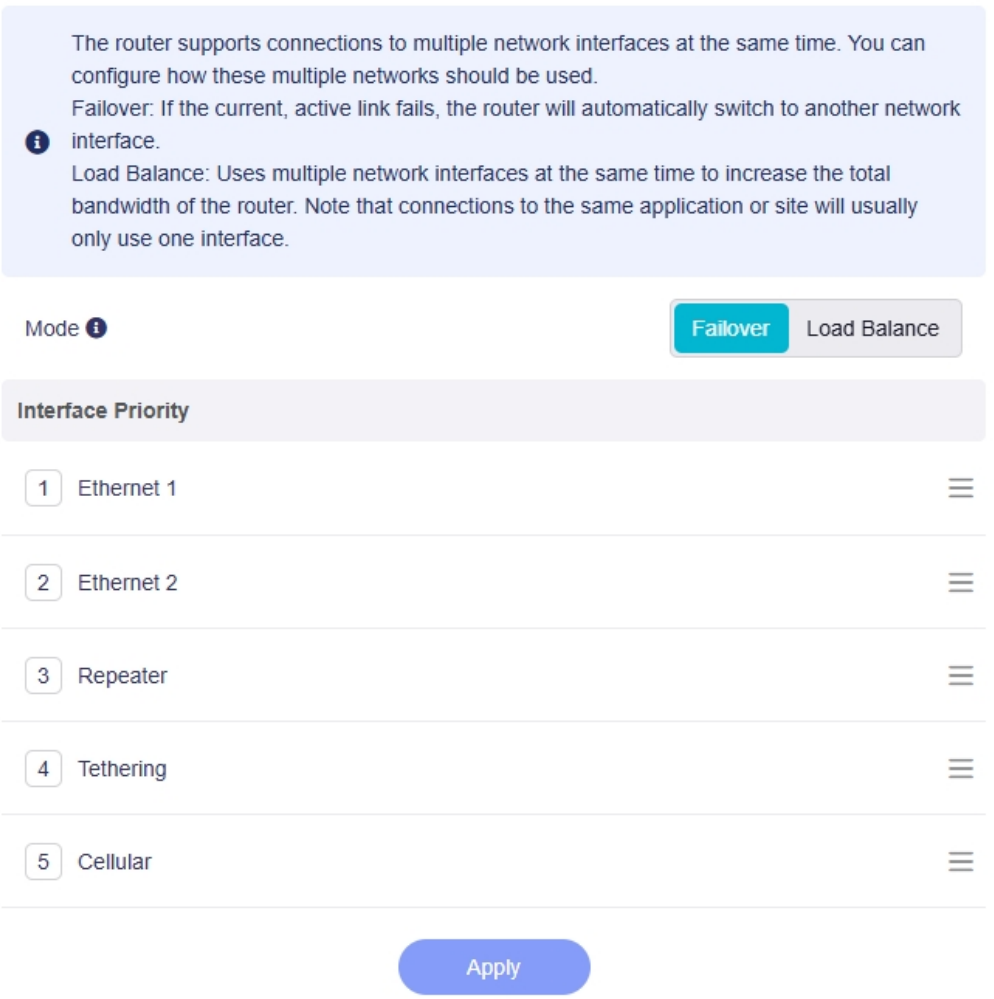
12.1.2 Modo Multi-WAN

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

Conmutación por error

Conmutación por error es el modo predeterminado cuando se configuran varias conexiones. Si el enlace activo falla, el enrutador cambiará automáticamente a otra interfaz de red para acceder a Internet.

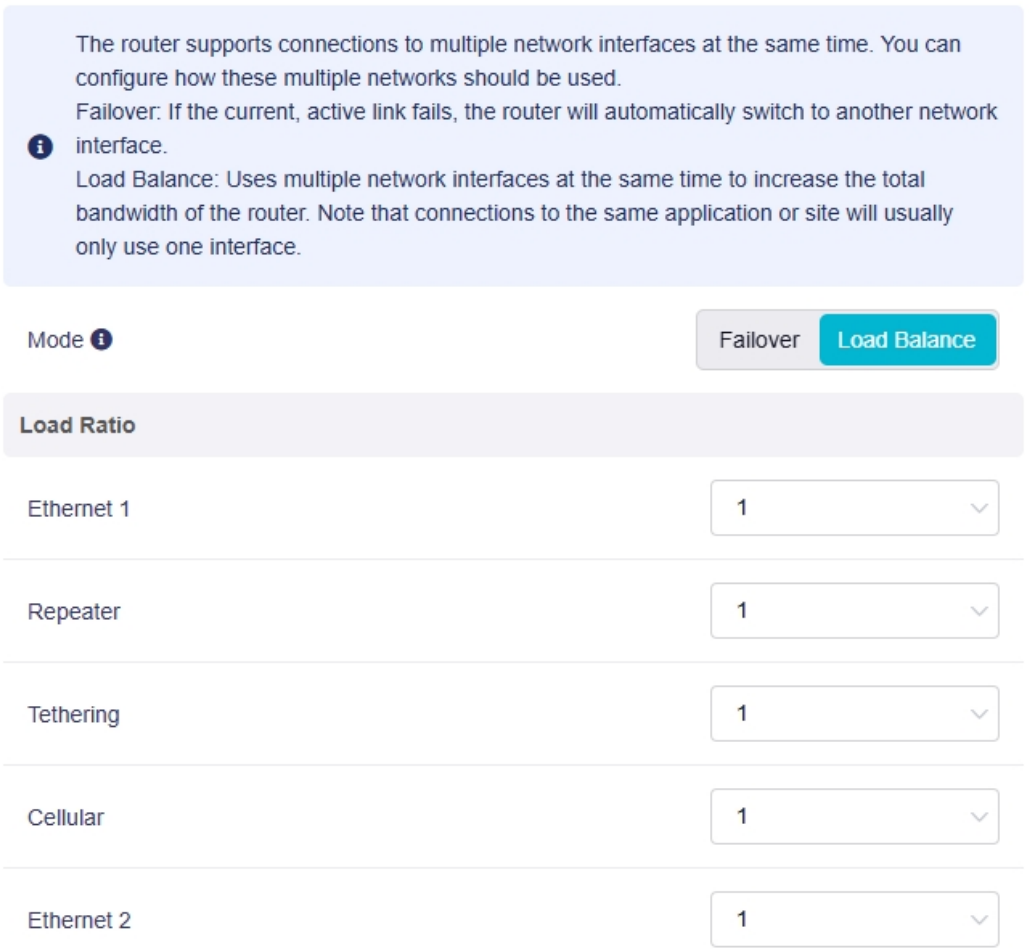
Puede establecer niveles de prioridad para cada interfaz: cuando la interfaz utilizada actualmente falla, el enrutador cambia a la siguiente interfaz disponible con la mayor prioridad. Una vez que se restablece una conexión de mayor prioridad, el enrutador volverá automáticamente a su modo.



Equilibrio de carga

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

La relación de carga se refiere a la proporción entre cada interfaz de red. El sistema asignará interfaces para manejar nuevas conexiones según esta proporción configurada. Por ejemplo, si el enrutador está conectado a cinco redes (por ejemplo, Ethernet 1, Repetidor, Anclaje a red, Celular y Ethernet 2) simultáneamente y todas las interfaces están disponibles para el acceso a Internet, habilitar el equilibrio de carga y establecer una relación 1:1:1:1:1 significa que las cincocinco interfaces compartirán el ancho de banda de la red por igual. data-r="2775">interfaces según la interfaces según lo configurado relación de carga configurada.



También puede personalizar la relación de carga si es necesario Por ejemplo, si Ethernet 1 tiene una. ancho de banda de 100 Mbps, Repetidor tiene 200 Mbps y ningún otro están activas, establezca las relaciones de carga en 1 para Ethernet 1, 2 para Repetidor y 0 para Tethering, Celular y 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.

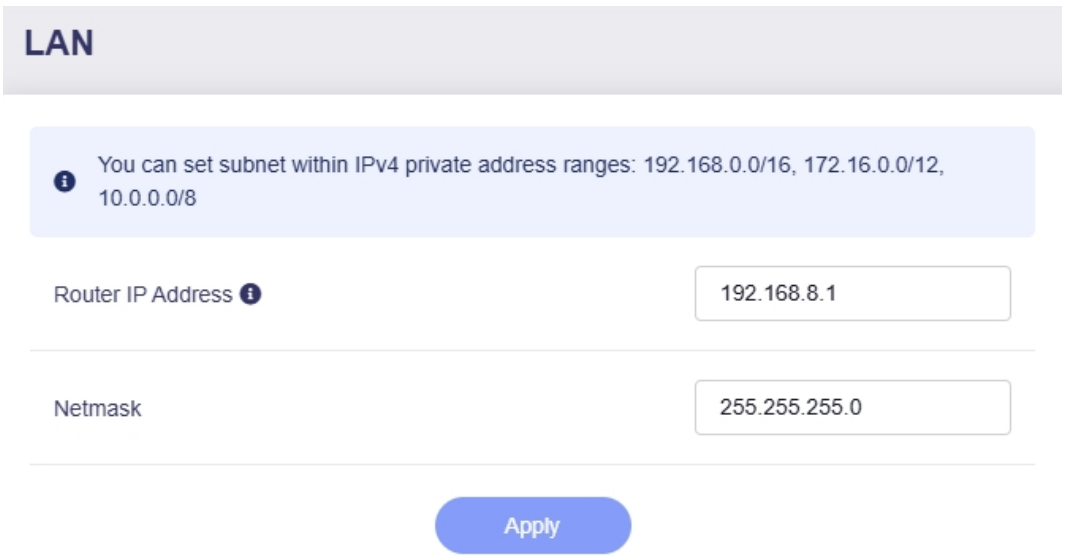
12.2 LAN

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 a **RED** > **LAN**. Aquí puede configurar los ajustes de LAN, incluidos los ajustes básicos, el servidor DHCP y la reserva de direcciones.

12.2.1 Configuración básica

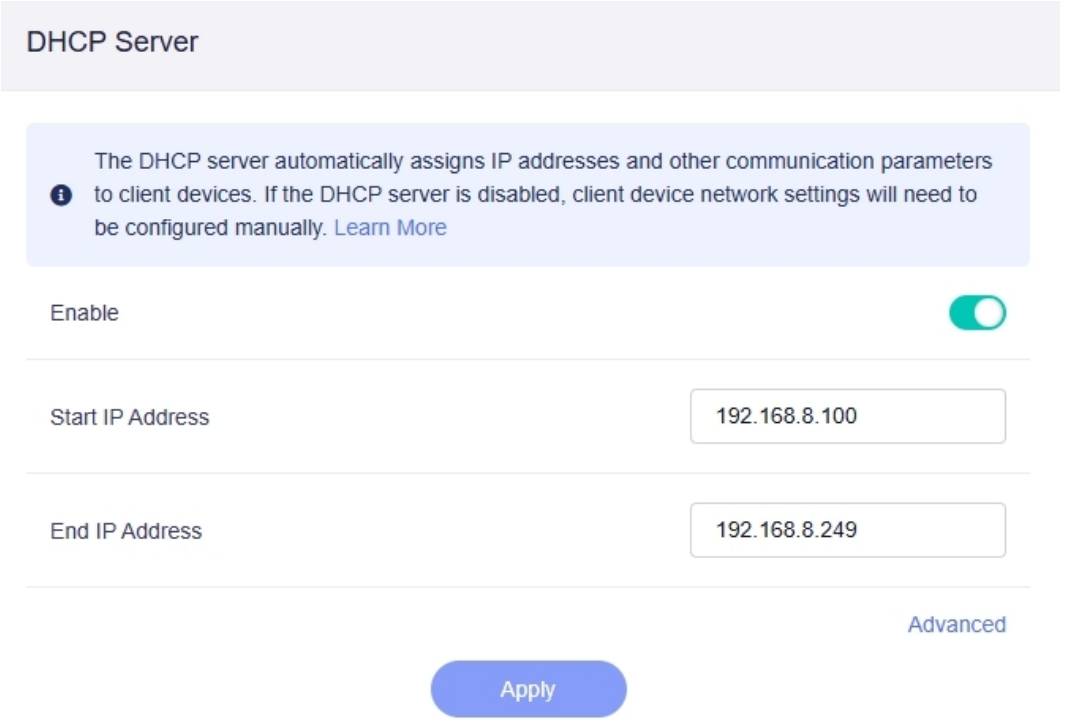
Los ajustes básicos incluyen la dirección IP del enrutador y Máscara de red. Puede configurar la subred dentro de los rangos de direcciones privadas IPv4: 192.168.0.0/16, 172.16.0.0/12, 10.0.0.0/8



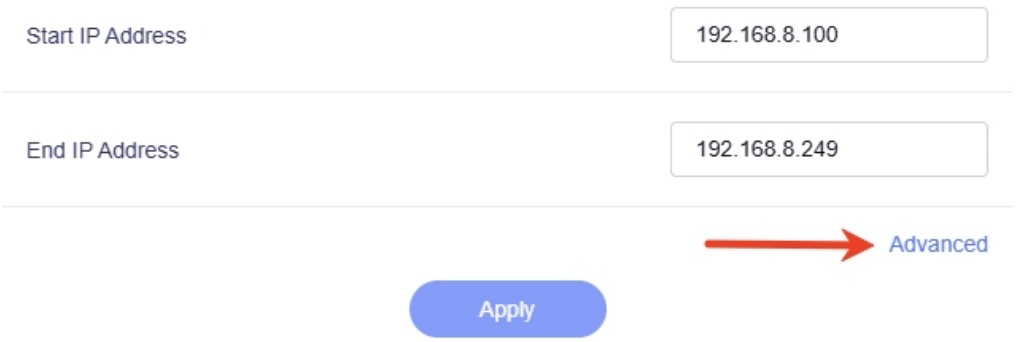
- **Dirección IP del enrutador**: esta es la dirección ingresada en la barra de direcciones del navegador para acceder al panel de administración del enrutador'. Es 192.168.8.1 de forma predeterminada y se puede cambiar si entra en conflicto con la red ascendente.
- **Máscara de red**: Hay dos opciones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

12.2.2 Servidor DHCP

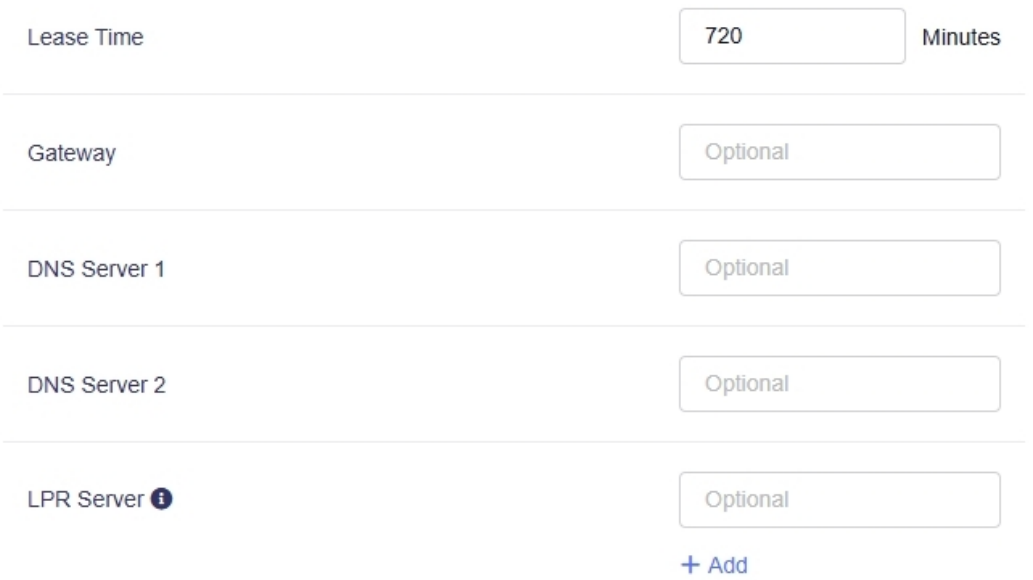
El servidor DHCP asigna automáticamente direcciones IP y otros parámetros de comunicación a cada cliente conectado. El servidor DHCP del enrutador GL.iNet está habilitado de forma predeterminada y el grupo de direcciones IP del servidor DHCP varía de 192.168.8.100 a 192.168.8.249. Puede personalizar 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 arrendamiento, la puerta de enlace, los servidores DNS, y LPR Servidor.



- **Tiempo de concesión**: la duración durante la cual un dispositivo puede usar una dirección IP asignada a través de DHCP.
- **Puerta de enlace**: el componente del enrutador que enruta el tráfico entre local red y redes externas (por ejemplo, Internet).
- **Servidor DNS 1**: el servidor principal responsable de traducir nombres de dominio a direcciones IP.
- **Servidor DNS 2**: Se utiliza un servidor de respaldo 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 múltiples puertos LPR para impresoras.

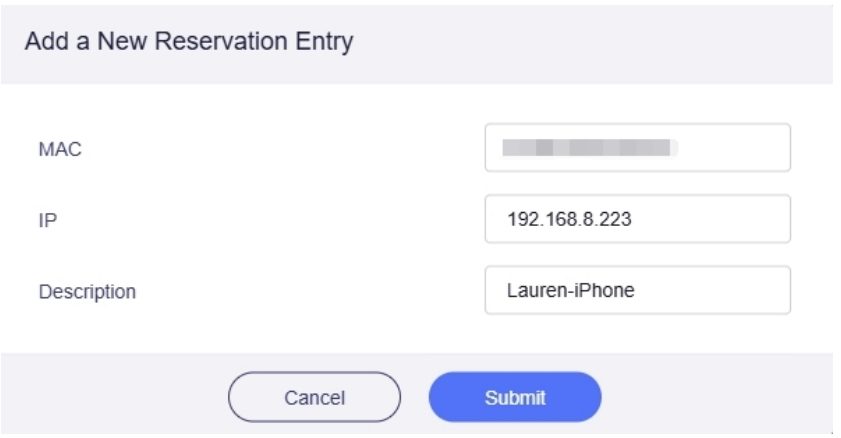
Nota: Si el servidor DHCP está deshabilitado, debe configurar manualmente la IP estática y otros parámetros de comunicación para cada cliente. Consulte aquí para obtener más detalles.

12.2.3 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 IP permanente. Tenga en cuenta quelos clientes con reserva de dirección configurada deben volver a conectarse al enrutador para activar la configuración.

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

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



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



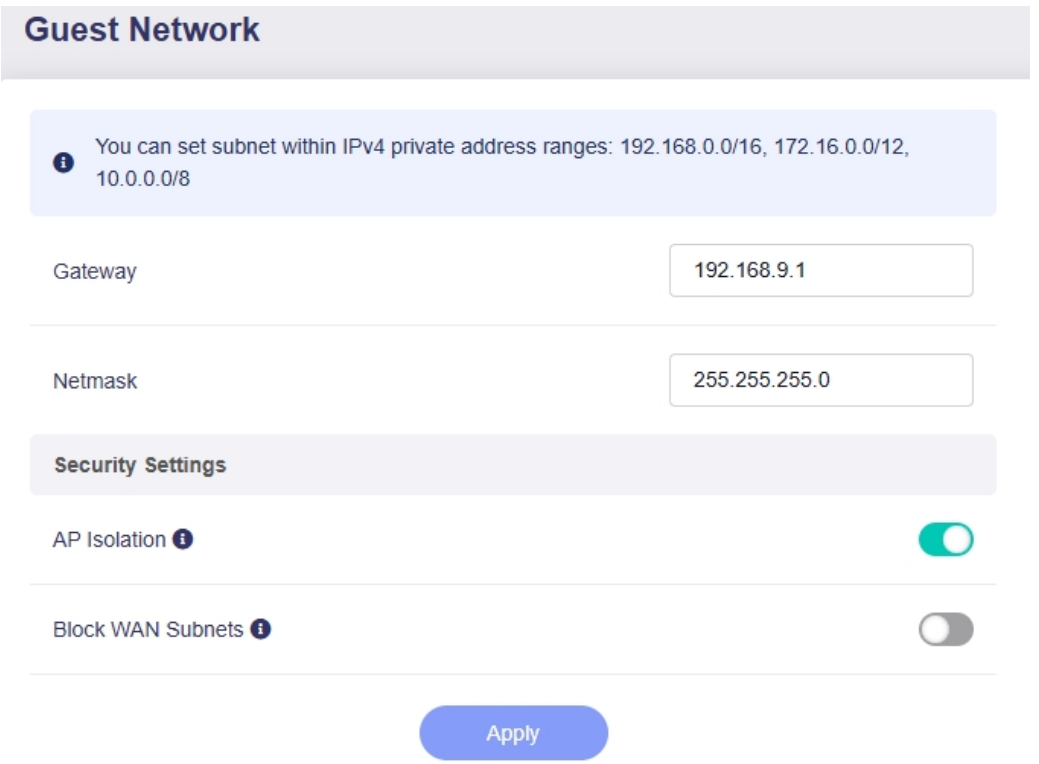
12.3 Red de invitados

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 vaya a **RED** > **Red de invitados**. Esta página le permite configurar los ajustes de la red de invitados, incluyendo configuraciones básicas y servidor DHCP.

12.3.1 Configuración básica

Las configuraciones básicas incluyen Puerta de enlace, Máscara de red, Aislamiento de AP y bloque de subredes WAN.

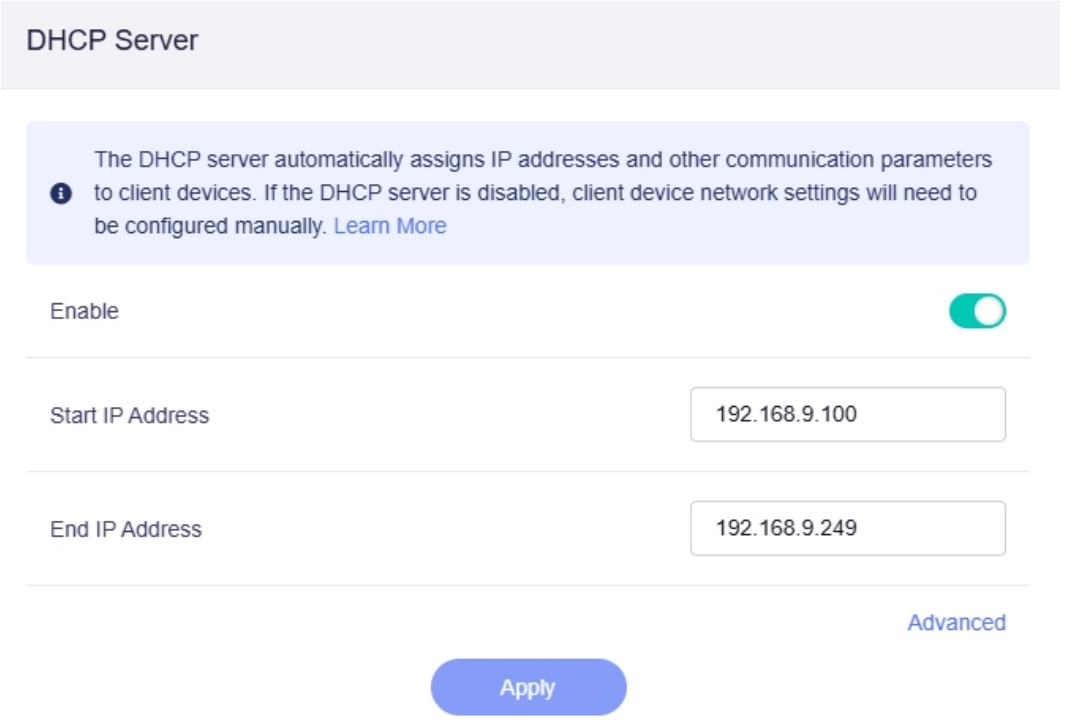


- **Puerta de enlace**: Es 192.168.9.1 de forma predeterminada y se puede cambiar si es necesario, pero no debe entrar en conflicto con el puerta de enlace de la red principal.
- **Máscara de red**: Hay dos opciones disponibles: 255.255.255.0 y 255.255.0.0.
- **Aislamiento AP**: se utiliza para aislar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

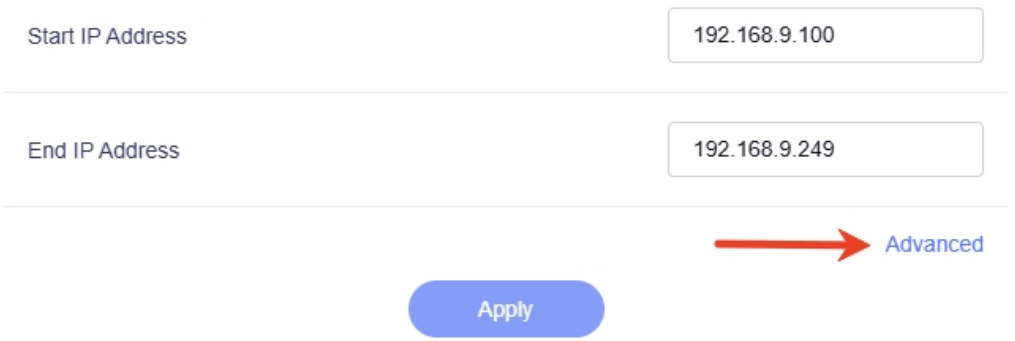
12.3.2 Servidor DHCP

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

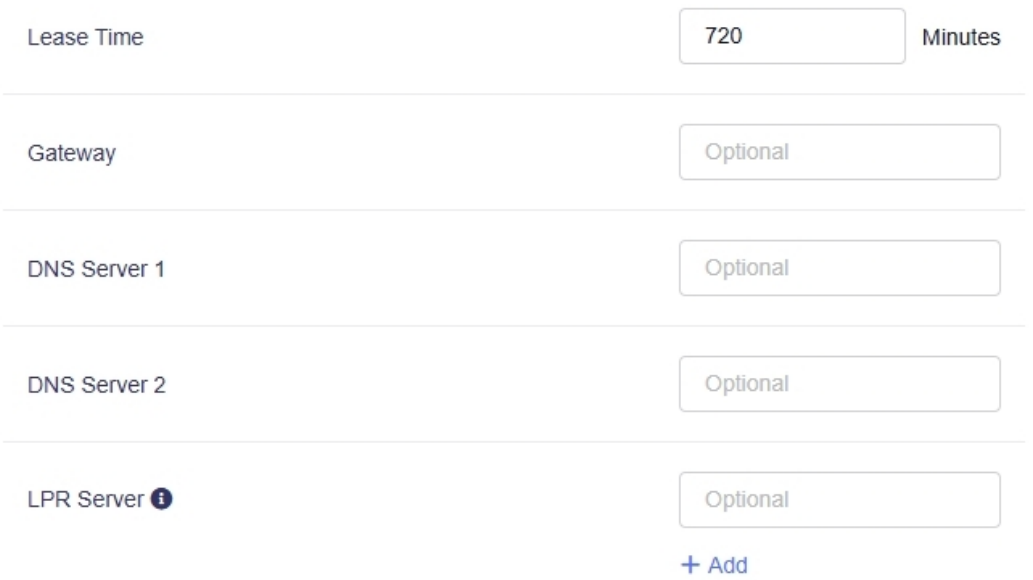
Cuando está habilitado, el servidor DHCP asigna automáticamente direcciones IP y otros parámetros de comunicación a cada cliente conectado. El grupo de direcciones IP del servidor DHCP para la red de invitados oscila entre 192.168.9.100 y 192.168.9.249. Puede personalizar el rango de direcciones si es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



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



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



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

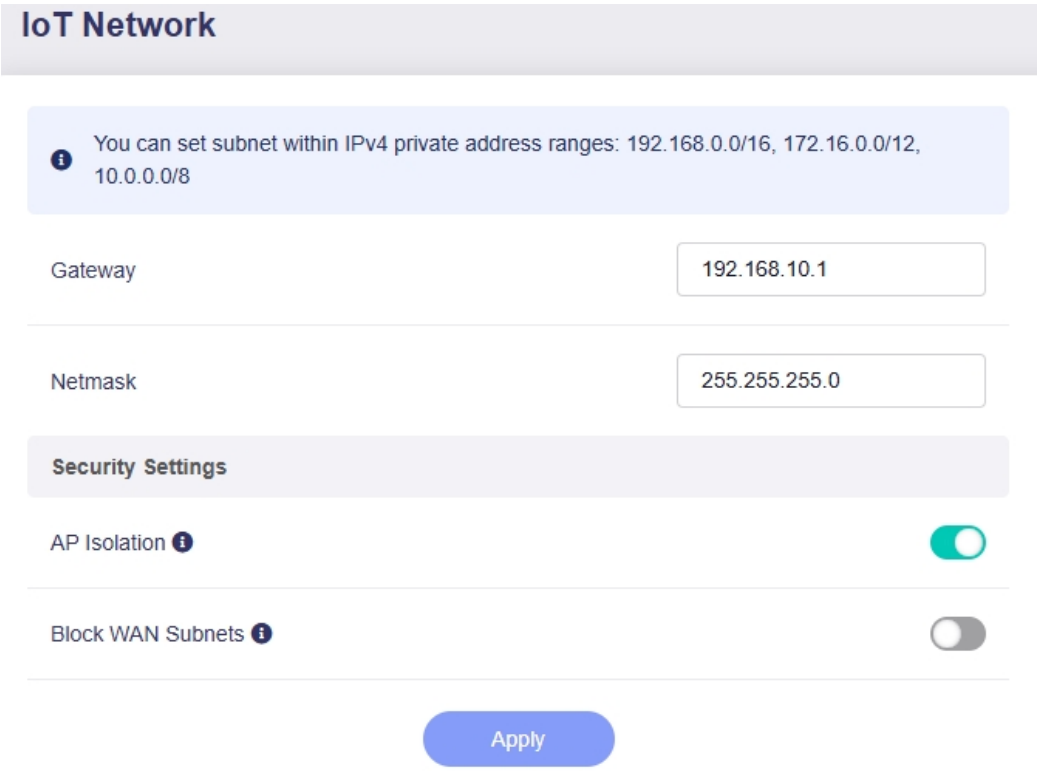
12.4 Red de IoT

IoT Red se refiere a una red dedicada para IoT dispositivos, aislándolos de su LAN principal para brindar mayor compatibilidad y seguridad.

Inicie sesión en el panel de administración web de su enrutador y vaya a **RED** > **Red de IoT**. Esta página le permite configurar IoT Red configuración, incluyendo configuración básica y servidor DHCP.

12.4.1 Configuración básica

La configuración básica incluye puerta de enlace, Máscara de red, Aislamiento de AP y bloque de subredes WAN.

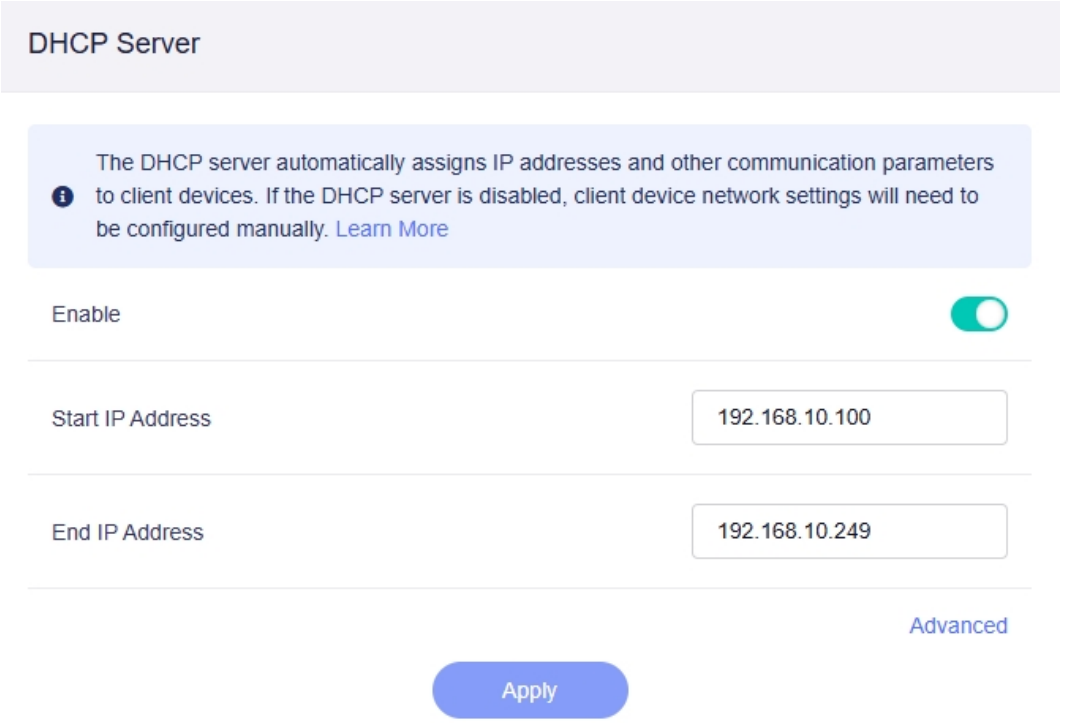


- **Puerta de enlace**: Es 192.168.10.1 de forma predeterminada y se puede cambiar si es necesario, pero no debe entrar en conflicto con el puerta de enlace de la red principal.
- **Máscara de red**: Hay dos opciones disponibles: 255.255.255.0 y 255.255.0.0.
- **AP Aislamiento**: se utiliza para aislar a los clientes de la red IoT en segmentos separados para que no puedan comunicarse con otros dispositivos en la misma red.
- **Bloquear subredes WAN**: si está habilitado, la red IoT no podrá acceder a la red ascendente ni a su segmento de red correspondiente.

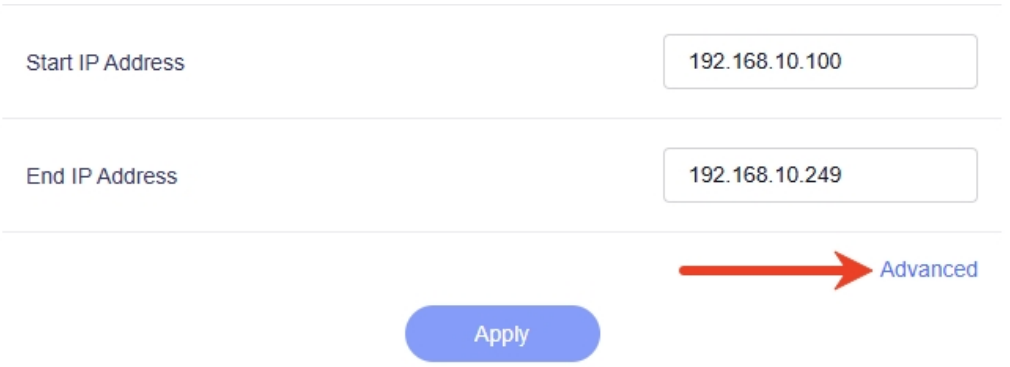
12.4.2 Servidor DHCP

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

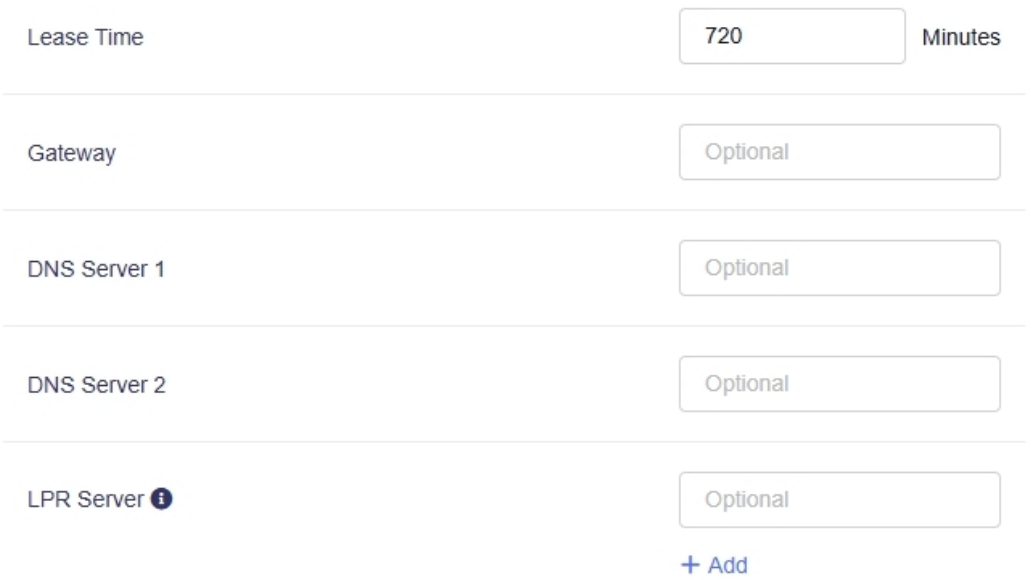
Cuando está habilitado, el El servidor DHCP asigna automáticamente direcciones IP y otros parámetros de comunicación a cada cliente conectado. El grupo de direcciones IP del servidor DHCP para la red IoT varía de 192.168.10.100 a 192.168.10.249. Puede personalizar el rango de direcciones si es necesario.



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



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



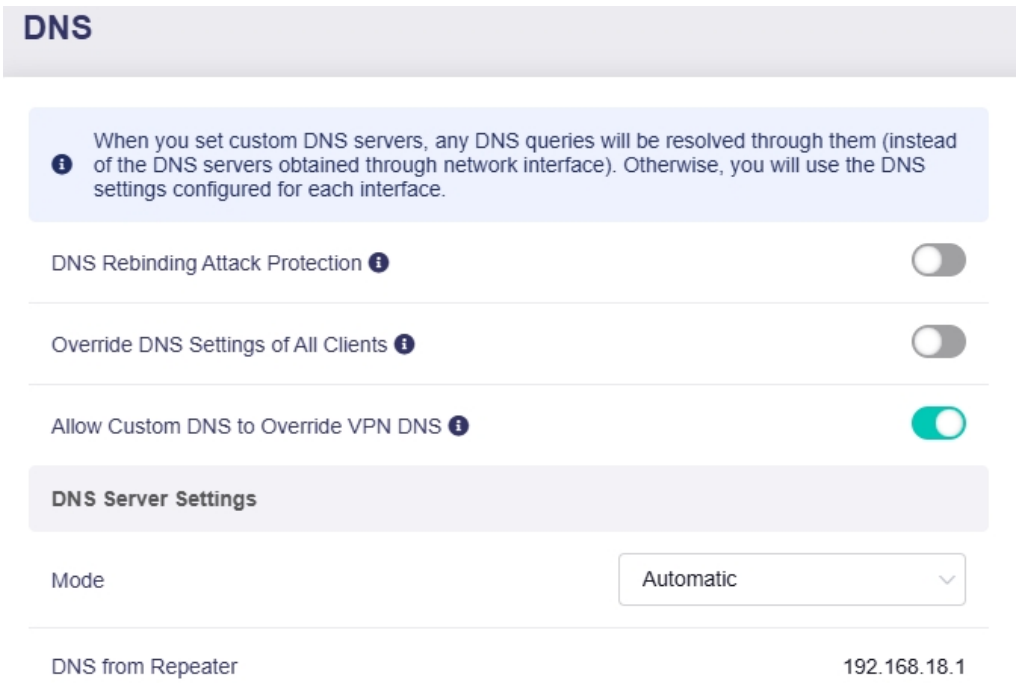
- **Tiempo de concesión**: la duración durante la cual un dispositivo puede usar una dirección IP asignada a través de IoT DHCP de la red.
- **Puerta de enlace**: el componente del enrutador que enruta el tráfico entre la red IoT y las redes externas (por ejemplo, Internet).
- **Servidor DNS 1**: el servidor principal responsable de traducir nombres de dominio a direcciones IP.
- **Servidor DNS 2**: un servidor de respaldo utilizado para resolver nombres de dominio si falla el servidor DNS principal.
- **LPR Servidor**: (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.

12.5 DNS

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

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

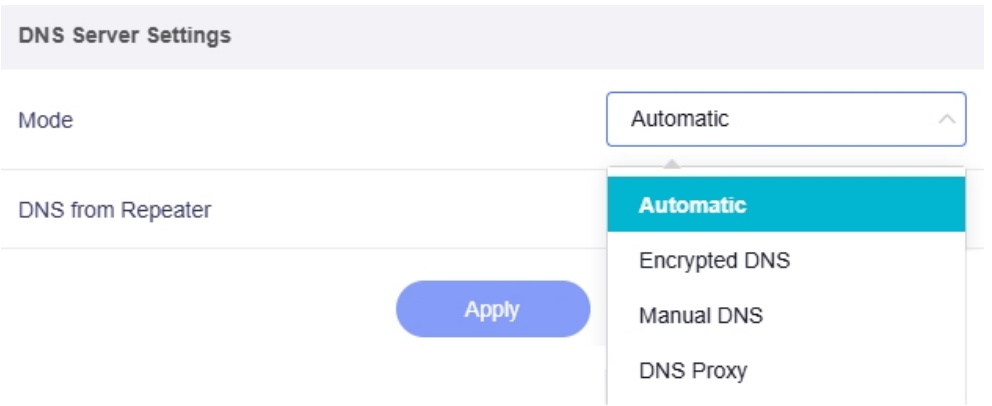
Inicie sesión en el panel de administración web de su enrutador y navegue hasta **RED** > **DNS**. Esta página le permite configurar ajustes relacionados con DNS, incluidas opciones de seguridad, modos de servidor y reglas de prioridad de DNS para diferentes escenarios de red.



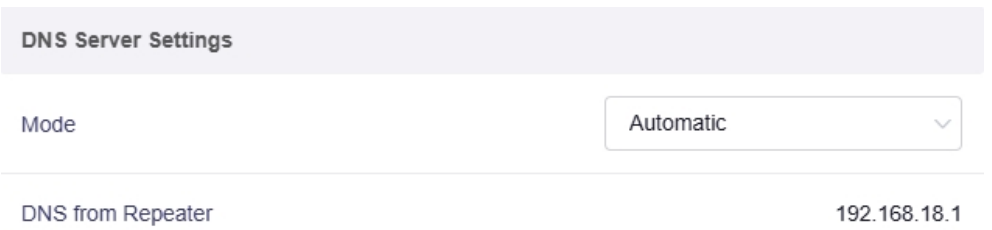
- **Protección contra ataques de revinculación de DNS**: protege contra ataques de revinculación de DNS bloqueando intentos maliciosos de resolución de DNS. Tenga en cuenta que habilitarlo puede causar fallas en la búsqueda de DNS privado; deshabilítelo si su red utiliza un portal cautivo (por ejemplo,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

12.5.1 Configuración del servidor DNS

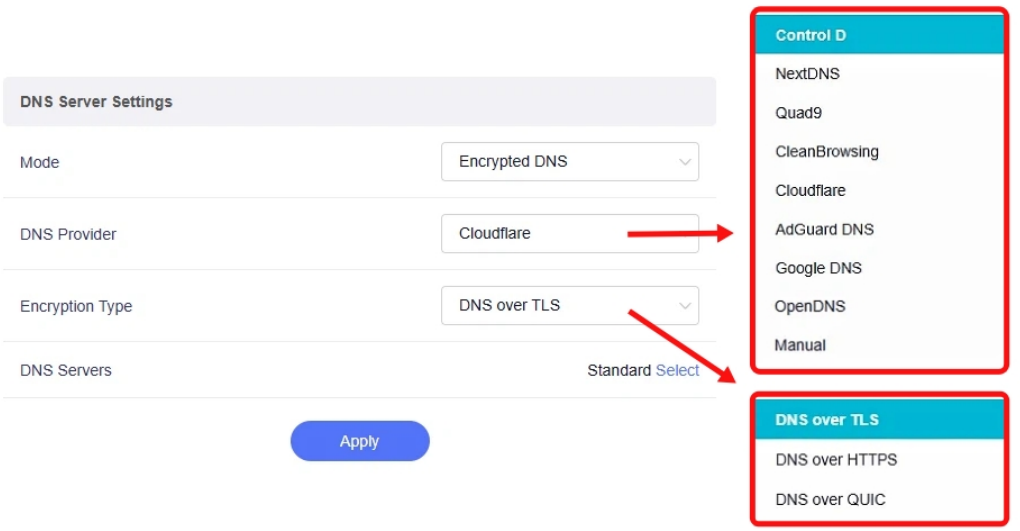
Hay cuatro modos para el servidor DNS: Automático, DNS cifrado, DNS manual y Proxy DNS.



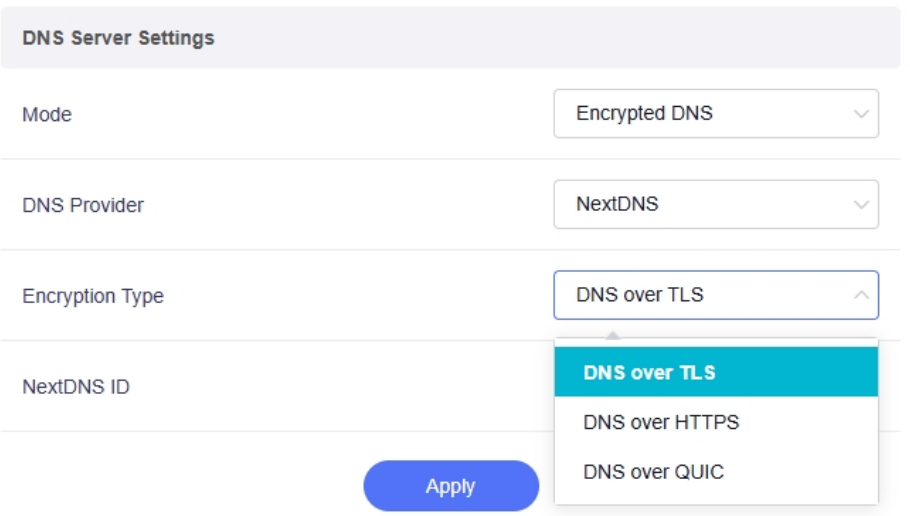
1. **Automático**: cuando se selecciona, el enrutador obtendrá automáticamente las direcciones del servidor DNS de la red ascendente y las aplicará a todos los dispositivos conectados.



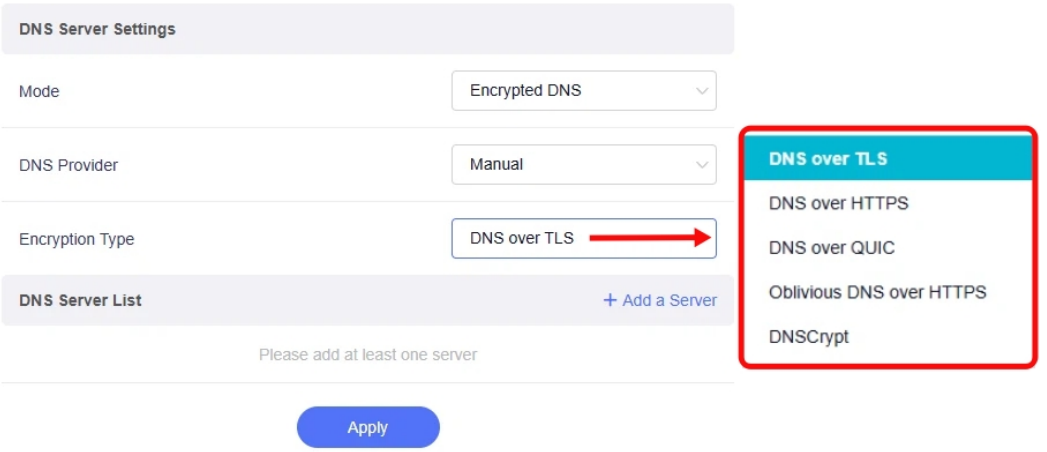
2. **DNS cifrado**: cuando se selecciona, el enrutador utilizará protocolos cifrados para procesar consultas DNS, protegiendo los datos de resolución contra escuchas o manipulación.
   Admite múltiples proveedores de DNS para el modo DNS cifrado, incluidos Control D, NextDNS, Cloudflare,Quad9, CleanBrowsing, AdGuard DNS, Google DNS y OpenDNS. Primero seleccione el proveedor de DNS. Las opciones restantes cambiarán según su selección.



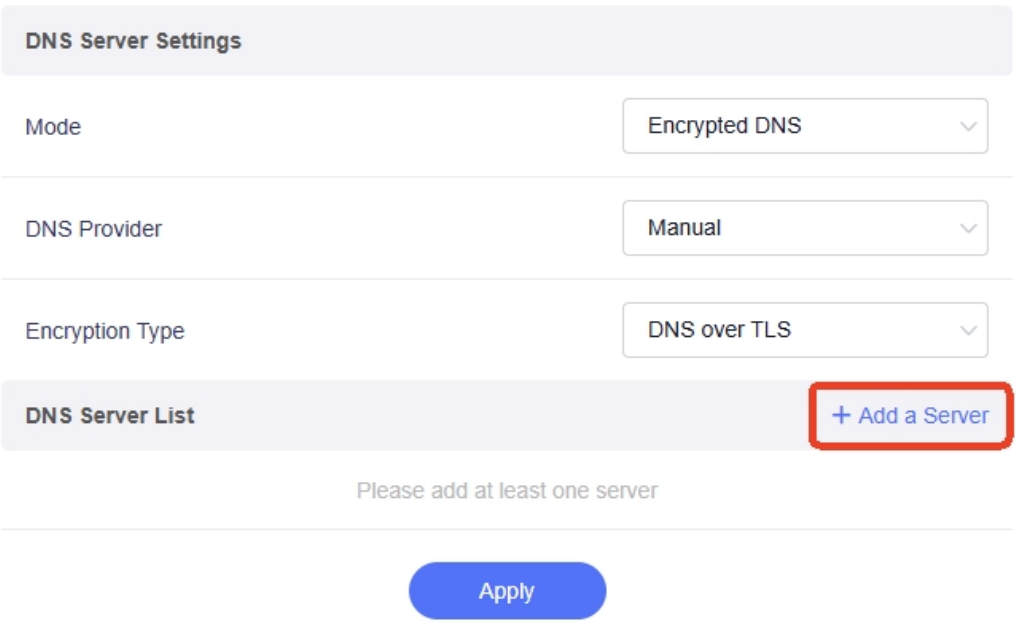
- Si selecciona un proveedor de DNS específico (por ejemplo, NextDNS), elija un tipo de cifrado entre DNS sobre TLS (DoT), DNS sobre HTTPS (DoH) y DNS sobre QUIC (DoQ). Tenga en cuenta que DNS sobre QUIC (DoQ) se introdujo en el firmware v4.9 y solo está disponible cuando se utiliza Control D, NextDNS o AdGuard DNS como proveedor de DNS.



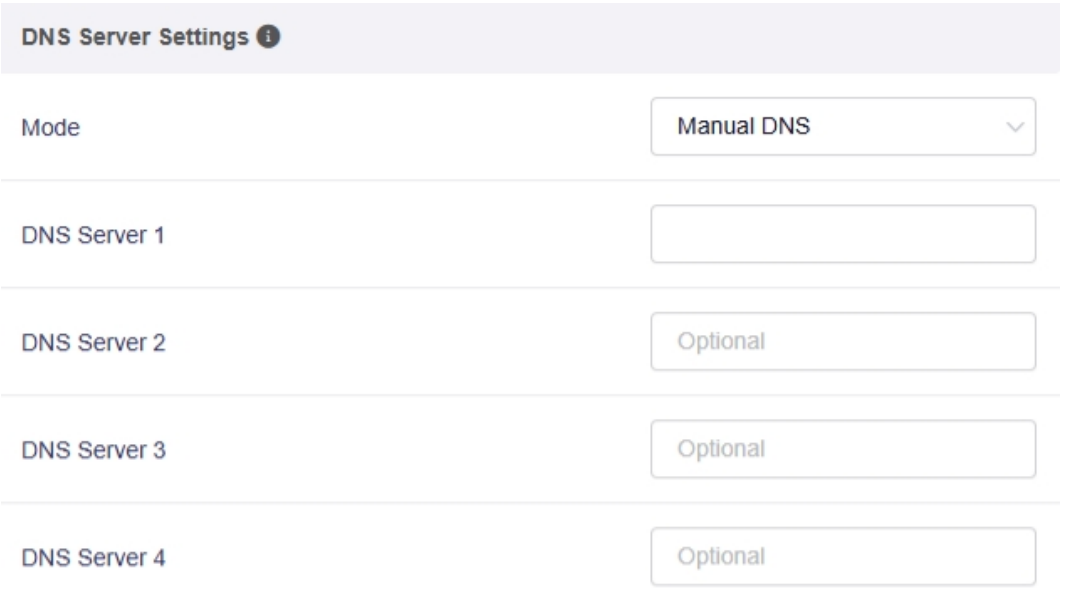
- Si selecciona Manual como proveedor de DNS, elija un tipo de cifrado entre DNS sobre TLS (DoT), DNS sobre HTTPS (DoH), DNS sobre QUIC (DoQ), DNS ajeno a HTTPS y DNSCrypt.



A continuación, haga clic en **Agregar un servidor** para agregar al menos un servidor DNS. Puede ingresar directamente la URL o el formato de sello del DNS cifrado. Para obtener una lista de servidores públicos, consulte https://dnscrypt.info/public-servers.

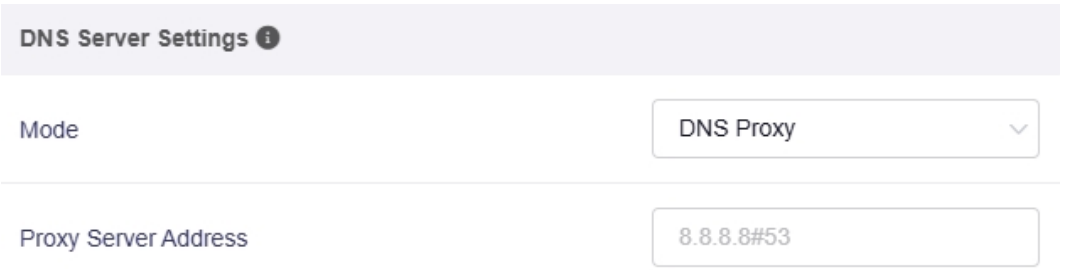


3. **DNS manual**: cuando lo seleccione, puede personalizar los servidores DNS de su enrutador. Haga clic en Servidor DNS 1 y elija un servidor DNS de la lista desplegable. Los campos DNS restantes se actualizarán automáticamente.



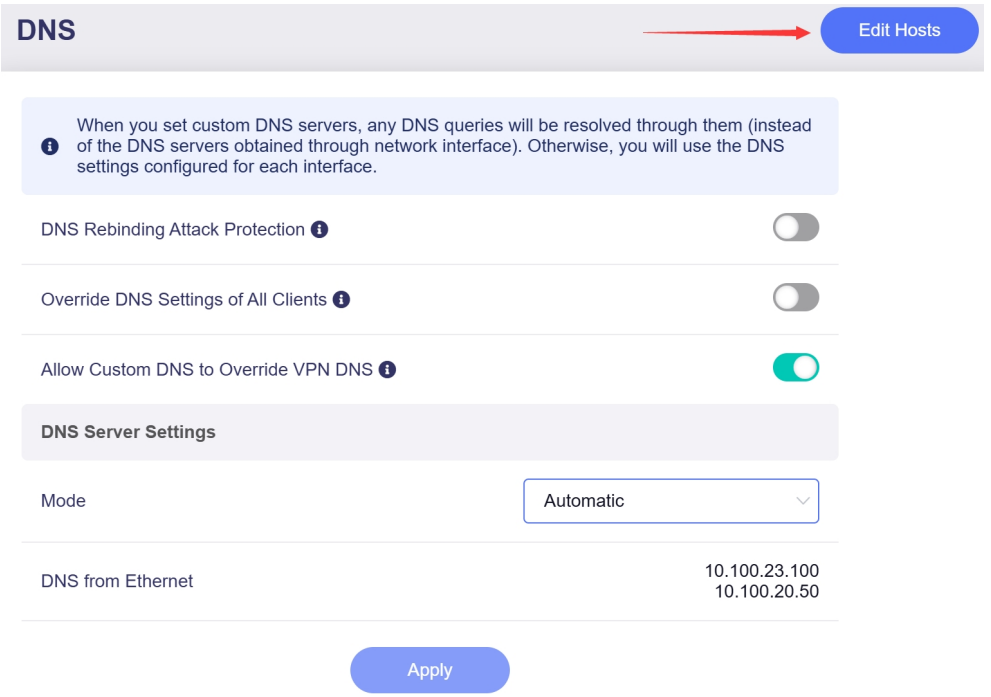
Nota: si necesita utilizar direcciones IPv6 para DNS manual, habilite IPv6 en su enrutador primero.

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

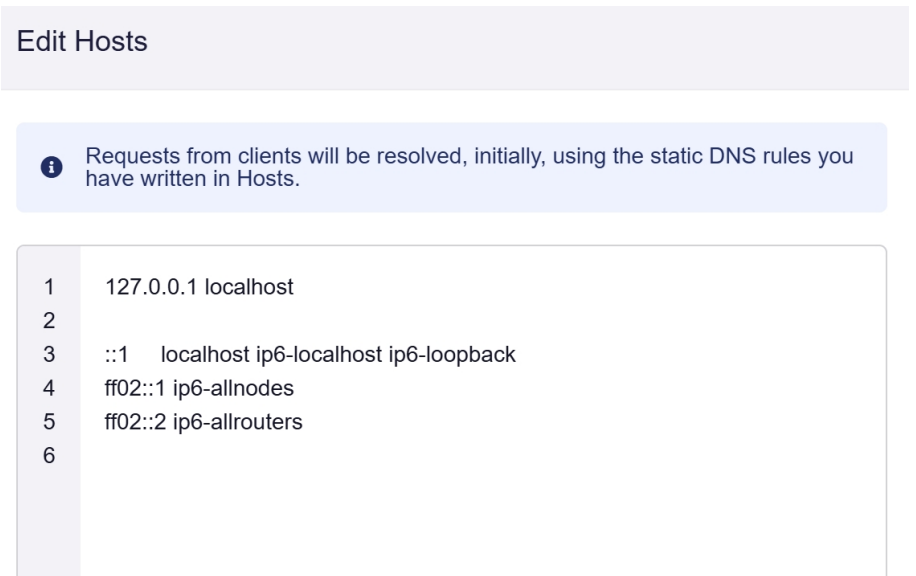


12.5.2 Editar hosts

Puede definir la resolución de DNS estática reglas si es necesario. En la página DNS, haga clic en **Editar hosts** en la esquina superior derecha.

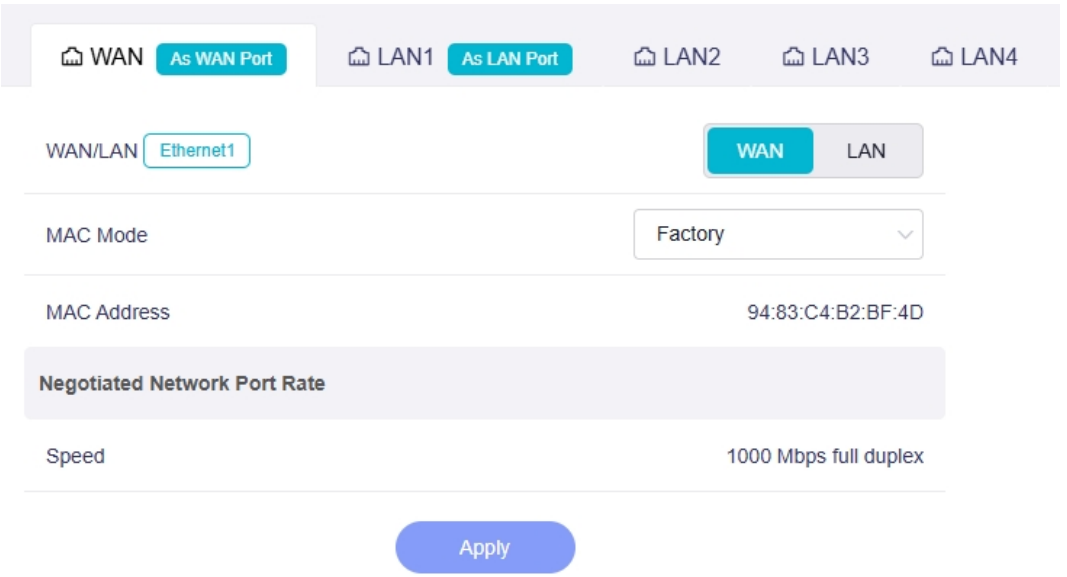


Las solicitudes de los clientes se resolverán preferentemente utilizando las reglas de DNS estáticas escritas aquí, lo que le permitirá asignar manualmente direcciones IP a nombres de host (por ejemplo, las entradas predeterminadas como 127.0.0.1 localhost para loopback local) para un control personalizado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

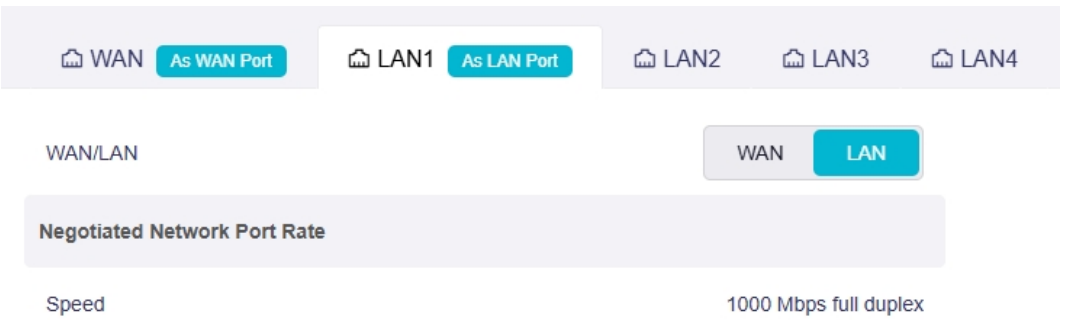


12.6 Puerto Ethernet

Inicie sesión en el panel de administración web de su enrutador' y navegue hasta **RED** > **Ethernet Puerto**. Esta página le permite administrar los puertos Ethernet del enrutador's. El **WAN** muestra la función del puerto (WAN o LAN), la dirección MAC y la tarifa negociada.



La sección **LAN 1** le permite cambiar la LAN 1 a WAN. Puede cambiar la función del puerto y verificar la tarifa negociada aquí.



Las otras secciones **LAN** muestran la tarifa negociada para cada puerto LAN correspondiente.



Nota: La tarifa negociada para Los puertos WAN y LAN se muestran solo cuando hay un cable Ethernet

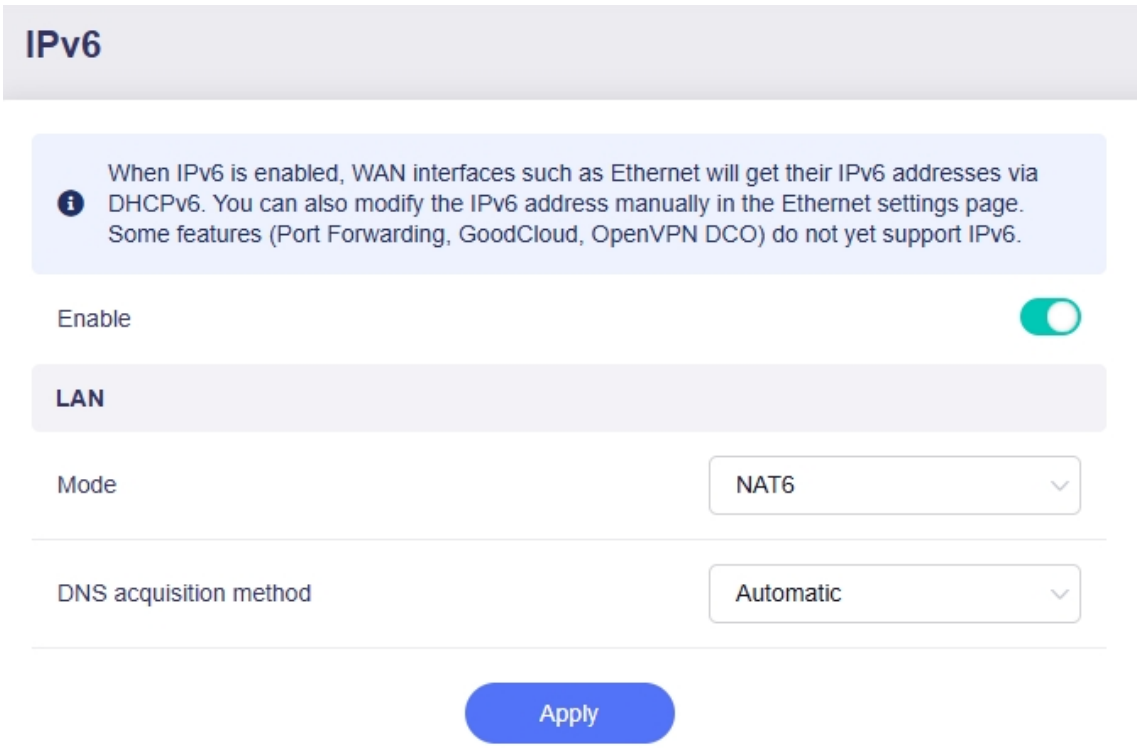
conectado. Depende tanto del puerto Ethernet como del cable Ethernet.

12.7 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, OpenVPN DCO) aún no son compatibles con IPv6. Si habilita estas funciones e IPv6 al mismo tiempo, es probable que cause problemas de conectividad .

12.7.1 Modo IPv6

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

- **Nativo**: este modo se aplica cuando el enrutador obtiene directamente un pública IPv6 dirección y el enrutador asigna automáticamente direcciones IPv6 a los dispositivos en línea. Este modo puede satisfacer las necesidades de acceso a IPv6 de la mayoría de los usuarios.
- **Passthrough**: este es aplicable cuando los paquetes IPv6 deben pasar directamente sin ningún procesamiento o conversión. Por ejemplo, algunas aplicaciones o servicios específicos pueden requerir la preservación completa del contenido del paquete IPv6 para su posterior procesamiento o análisis. Este modo lo utiliza el personal técnico para la depuración de la red o el análisis de seguridad.
- **NAT6**: este modo es sadecuado 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.

12.7.2 Método de obtención de DNS

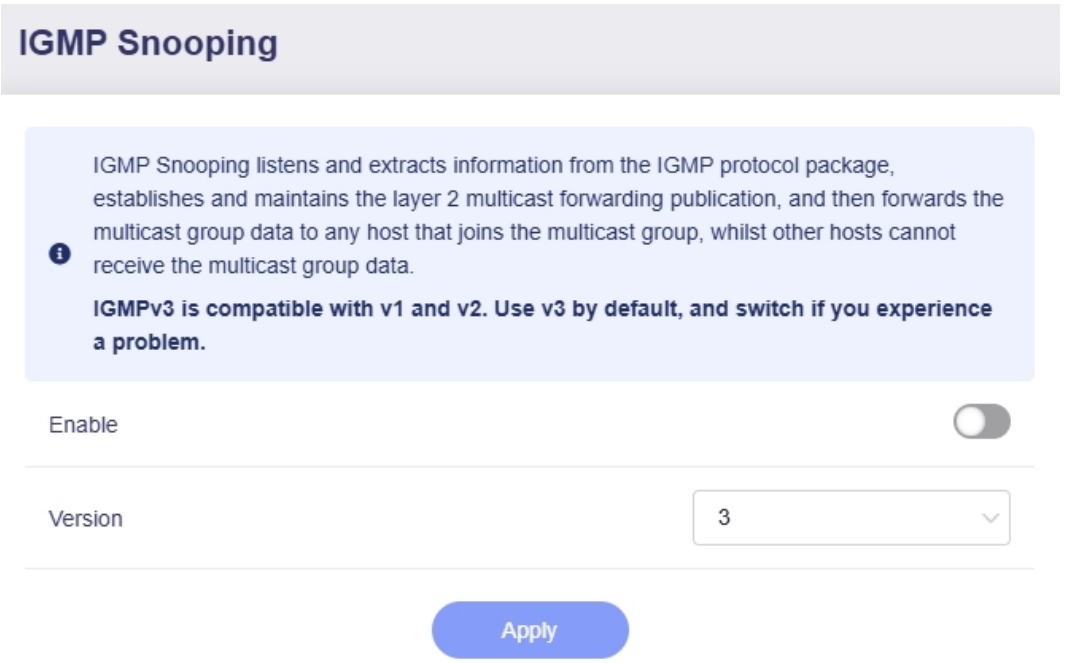
Determina cómo obtiene el router Direcciones de servidor DNS IPv6. Hay dos opciones: Automático y Manual.

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

12.8 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.

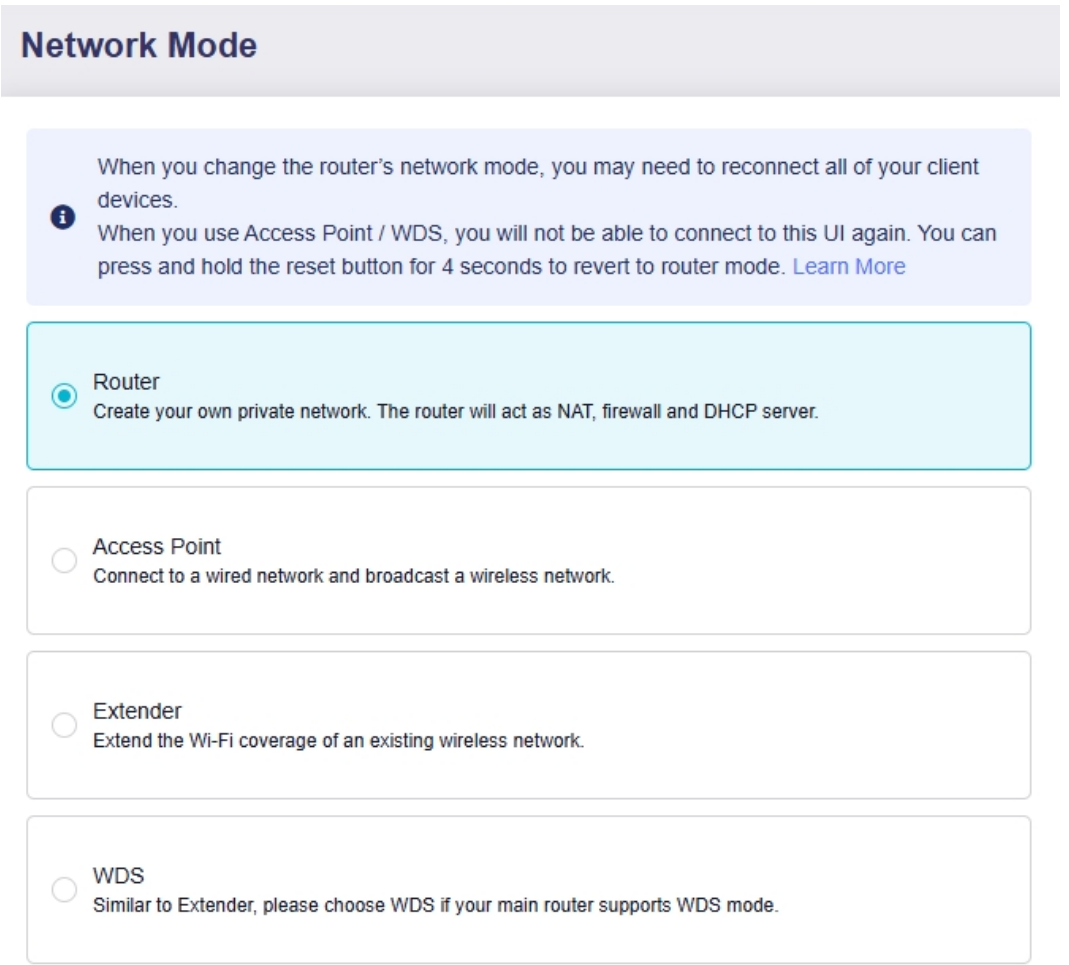
Inicie sesión en el panel de administración web de su enrutador' y navegue hasta **RED** > **Inspección IGMP**. Puede habilitar para usar la función de multidifusión en su enrutador si es necesario.



12.9 Modo de red

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

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



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

- **Punto de acceso**: este modo permite que un enrutador se conecte a una red cableada a través de un cable LAN y transmita señales inalámbricas, ampliando la cobertura de Wi-Fi en grandes espacios para permitir que más dispositivos accedan a la red. En este modo, el enrutador desactiva sus funciones NAT y DHCP, funcionando únicamente como un transmisor de señal inalámbrica 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 reducir el ancho de banda a la mitad, ya que el dispositivo tiene que manejar la recepción y transmisión de señales simultáneas.
- **WDS**: el modo Sistema de distribución inalámbrica (WDS) es similar al modo Extensor, ya que extiende la cobertura Wi-Fi de forma inalámbrica, pero admite puentes inalámbricos entre múltiples enrutadores compatibles. Se recomienda para la expansión de la red inalámbrica cuando el enrutador ascendente tiene funcionalidad WDS.
  Este modo es ideal para escenarios como cubrir edificios de varios pisos o campus de oficinas pequeñas donde varios enrutadores deben 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 utilizando la dirección IP original**. En su lugar, deberá iniciar sesión en el enrutador ascendente para encontrar la dirección IP que ha asignado a este enrutador, luego use esta dirección IP para acceder al panel de administración web. Si no tiene acceso al enrutador ascendente, presione y mantenga presionado el botón de reinicio durante 4 segundos para revertirlo al modo de enrutador predeterminado.

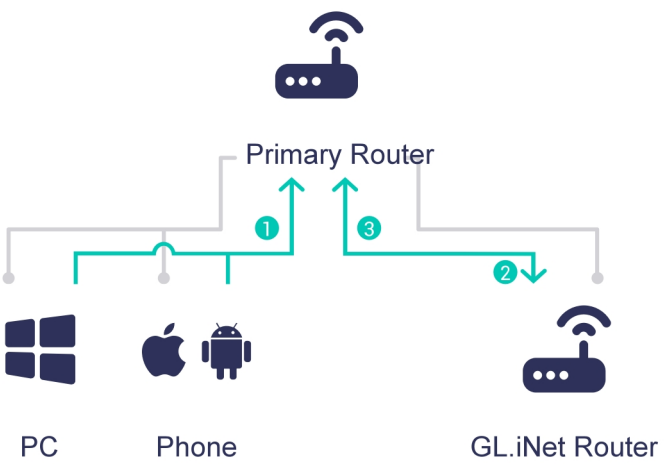
3. **En el modo Punto de acceso/Extensor/WDS, las siguientes funciones no estarán disponibles**: Control de acceso (lista de permitidos y de bloqueo), AstroWarp, VPN, AdGuard Home, Control parental, ZeroTier, Tailscale, Reenvío de puertos, Multi-WAN, Servidor DHCP, Reserva de direcciones, Red de invitados,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

12.10 Puerta de enlace directa

La puerta de enlace directa es una función de extensión que permite la expansión de la capacidad de un enrutador primario existente sin reemplazarlo ni volver a 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 para dispositivos cliente específicos si es necesario.



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

- **Gray lines** ilustran la topología de conexión física: dispositivos cliente (por ejemplo, computadora, computadora portátil) se 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.

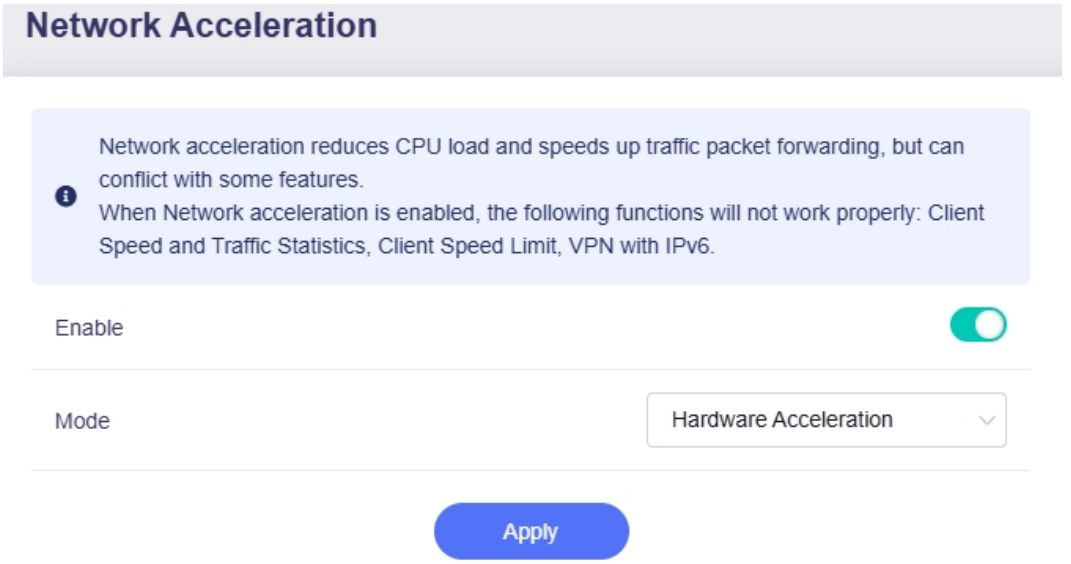
- **Glíneas verdes** representan la ruta de transmisión de datos secuencial cuando Drop-in La puerta de enlace está activa y las flechas numeradas indican el orden del flujo de tráfico:
    1. El tráfico de los dispositivos cliente se enruta primero al enrutador principal;
    2. El enrutador principal reenvía el tráfico al enrutador GL.iNet para su procesamiento (por ejemplo, filtrado de anuncios, cifrado VPN);
    3. Después 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.

Puede habilitar Drop-in Gvía para todos los o dispositivos específicos conectados a tu dispositivo principal enrutador. Consulte este enlace para obtener más detalless.

12.11 Aceleración de red

La aceleración de la 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 entre Aceleración de hardware y Aceleración de software.



- **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 de repetidor, sobresaliendo en estos escenarios con rutas fijas y reglas simples para ofrecer alto rendimiento, baja latencia y carga mínima de CPU para la transmisión de datos a velocidad de cable.
- **Aceleración de software**: se basa en la CPU general de un enrutador emparejada con núcleos o controladores optimizados (por ejemplo, SWNAT). Funciona con acceso celular (4G/5G), normalmente el escenario principal donde la aceleración de hardware no está disponible, y ofrece una gran compatibilidad y soporte para protocolos complejos. Si bien es flexible, puede generar cuellos de botella en la CPU bajo cargas de ancho de banda elevadas, especialmente cuando se ejecutan funciones avanzadas.

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

Capítulo 13

Control de flujo

Este capítulo presenta funciones de control de flujo, proporcionando herramientas dedicadas para el tráfico de red y la gestión de contenidos.

13.1 Motor DPI

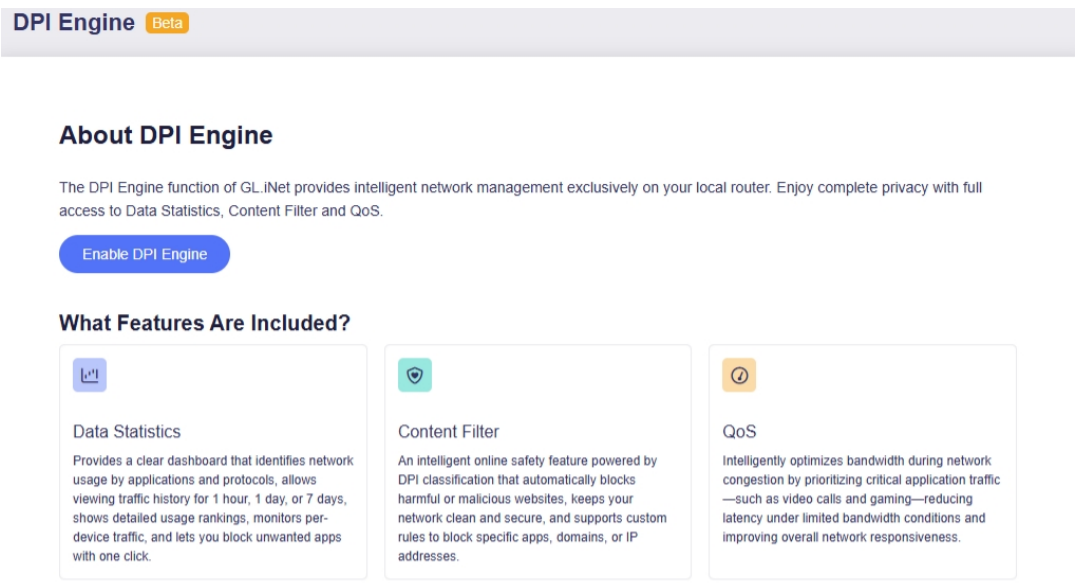
DPI (inspección profunda de paquetes) es una tecnología central para la gestión inteligente de redes. A diferencia de los enrutadores tradicionales que solo identifican las direcciones de origen y destino, DPI realiza un análisis en profundidad de las cargas útiles de los paquetes e identifica con precisión aplicaciones y sitios web utilizando una biblioteca de coincidencia de funciones, lo que permite una clasificación y control detallados del tráfico.

GL.iNet DPI Engine se ejecuta localmente en su enrutador para ofrecer una gestión de red inteligente con total privacidad. Proporciona acceso completo a estadísticas de tráfico, filtrado de contenido y QoS para un control integral del tráfico. Integrado con Netify, un agente DPI integrado liviano para la administración inteligente de redes, GL.iNet DPI utiliza la base de datos de firmas en línea actualizada automáticamente de Netify' para brindar un control de red confiable, preciso y eficiente.

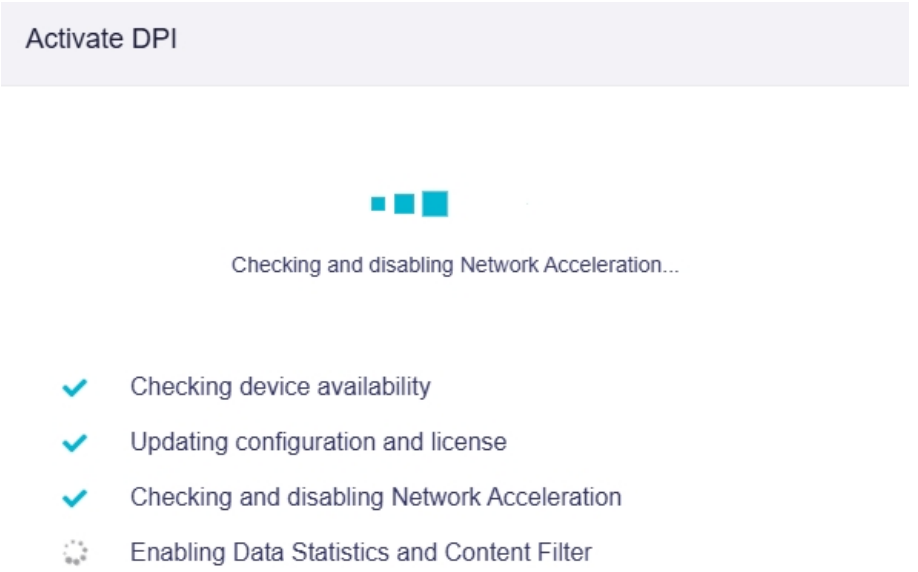
Nota:

1. Cuando el enrutador está en modo de puerta de enlace directa, las funciones DPI (incluidas estadísticas de datos, filtro de contenido y QoS) y SQM no tendrán efecto.
2. Cuando DPI está habilitado, la aceleración de red se deshabilitará automáticamente para garantizar un rendimiento estable.

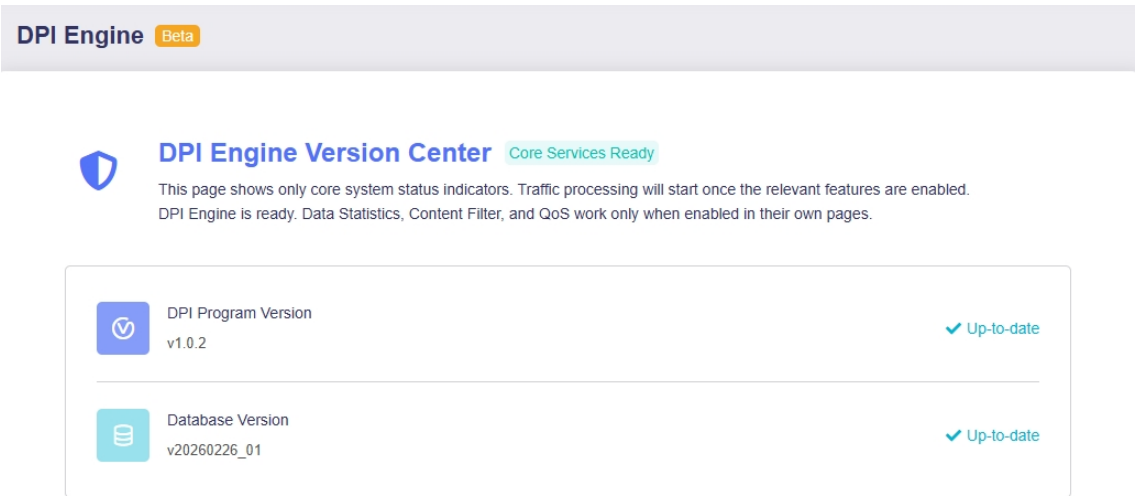
Inicie sesión en el panel de administración web del enrutador' y navegue hasta **CONTROL DE FLUJO** > **Motor DPI**. Haga clic en **Habilitar motor DPI**.



En la ventana emergente, lea y acepte los Términos de servicio y la Política de privacidad, luego haga clic en **Aplicar**. Luego, el enrutador iniciará la inicialización de DPI. Deshabilitará la aceleración de red, mientras que habilitaráing **Estadísticas de datos** y **Filtro de contenido**.



Una vez activado, yse le dirigirá al **Centro de versiones de DPI Engine**, donde puede ver la versión del programa DPI y la versión de la base de datos. Puede actualizar la base de datos aquí cuando haya una versión más nueva disponible.



Nota: Esta página muestra solo indicadores de estado del sistema central. El procesamiento del tráfico comenzará una vez que se habiliten las funciones relevantes.

13.2 Estadísticas de datos

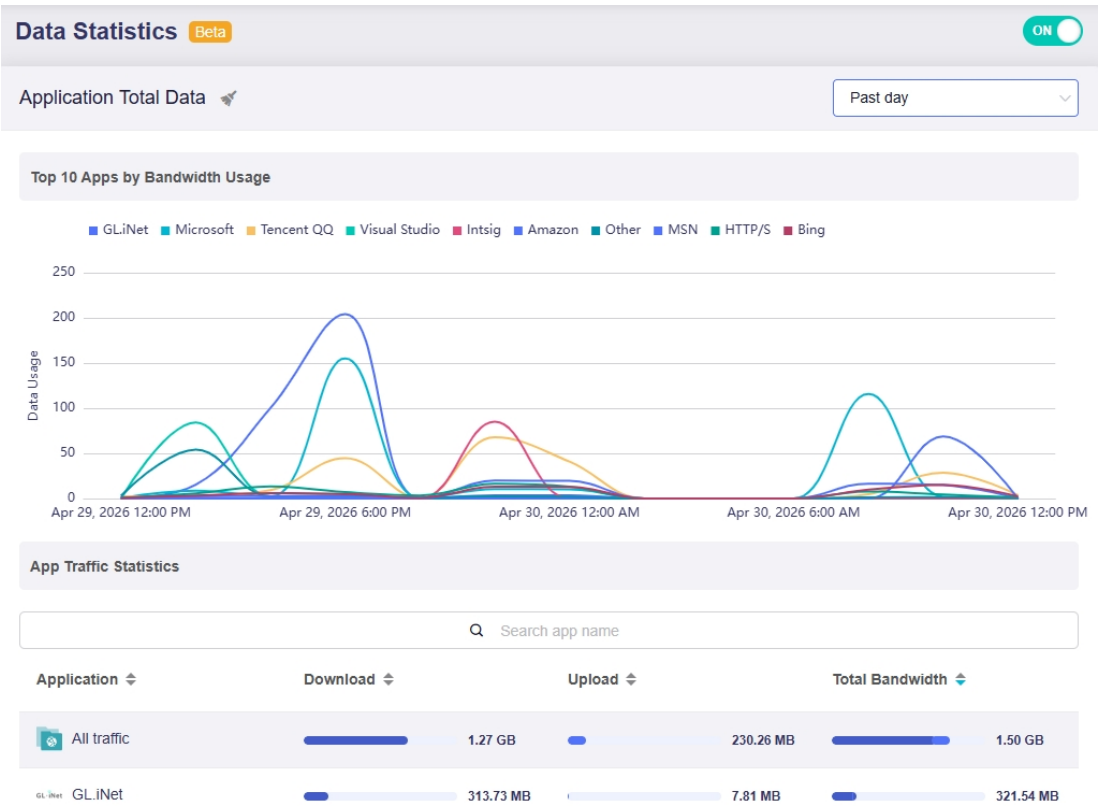
Estadísticas de datos proporciona un panel de tráfico intuitivo que identifica el uso de la red por aplicación y protocolo. Admite la visualización de tendencias históricas de 1-hora, 1-día y 7-día, muestra clasificaciones de uso, monitorea el tráfico por-dispositivo y permite bloquear con un solo-el contenido no deseado. apps.

Nota:

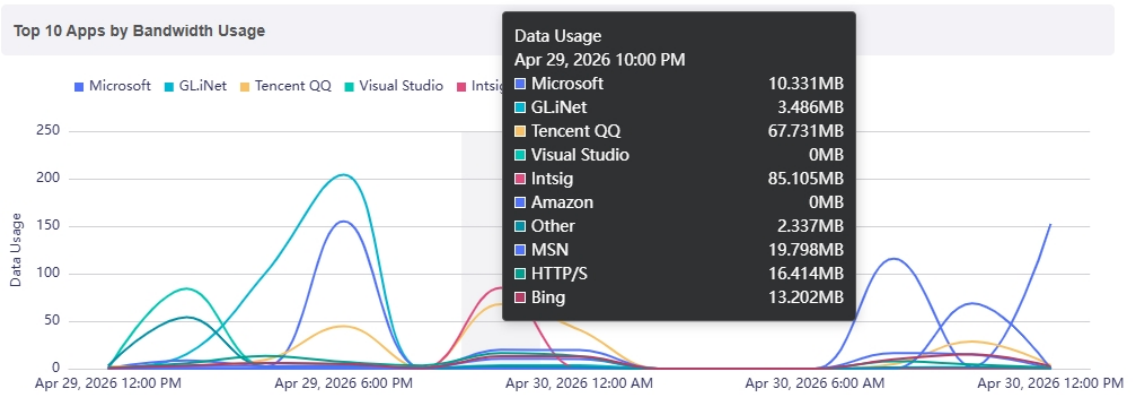
1. Las estadísticas de datos no tendrán efecto cuando el enrutador esté en modo de puerta de enlace directa.
2. Las estadísticas de datos no pueden funcionar con la aceleración de red. Al habilitar las estadísticas de datos, se deshabilitará automáticamente la aceleración de la red para garantizar un rendimiento estable.

13.2.1 Configuración rápida

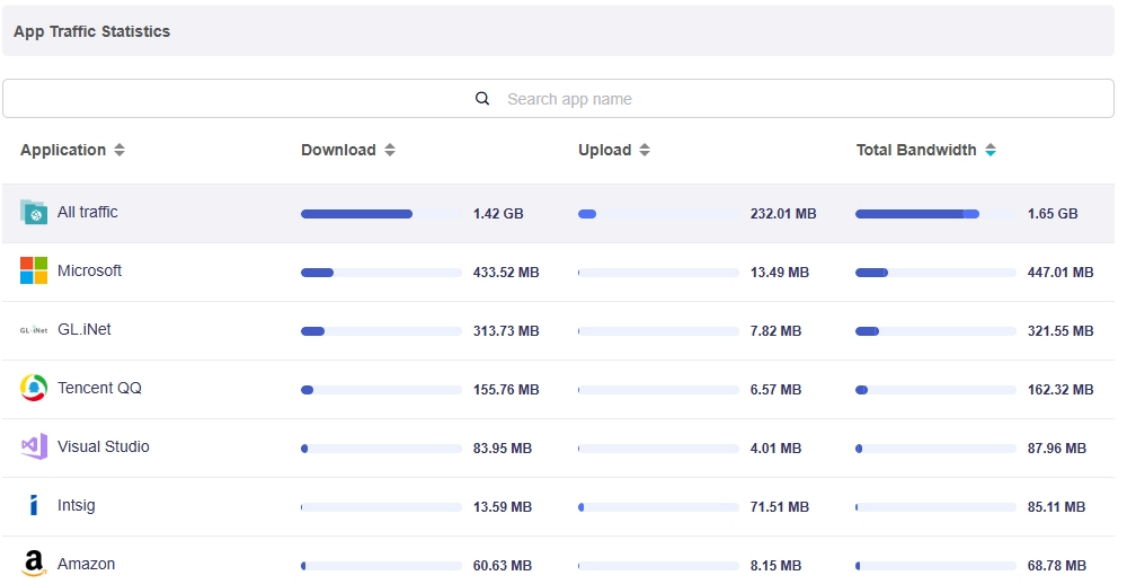
Inicie sesión en el panel de administración web del enrutador' y navegue hasta **CONTROL DE FLUJO** > **Estadísticas de datos**. Mueva el interruptor en la esquina superior derecha para ver los **Datos totales de aplicaciones**.



- **Las 10 aplicaciones principales por uso de ancho de banda**: presenta un gráfico de tendencias basado en el tiempo (por ejemplo, para el último día) para mostrar el consumo de ancho de banda de las 10 aplicaciones principales durante el período seleccionado. Pase el mouse sobre el gráfico para ver el uso de datos de las 10 aplicaciones que consumen más ancho de banda en un momento específico.



- **Estadísticas de tráfico de aplicaciones**: muestra métricas de tráfico detalladas para cada aplicación, incluidos datos de descarga, carga y ancho de banda total. Busque aplicaciones específicas en la barra de búsqueda si es necesario. Puede hacer clic en la flecha de clasificación junto al encabezado de la columna para ordenar la lista en orden ascendente o descendente.

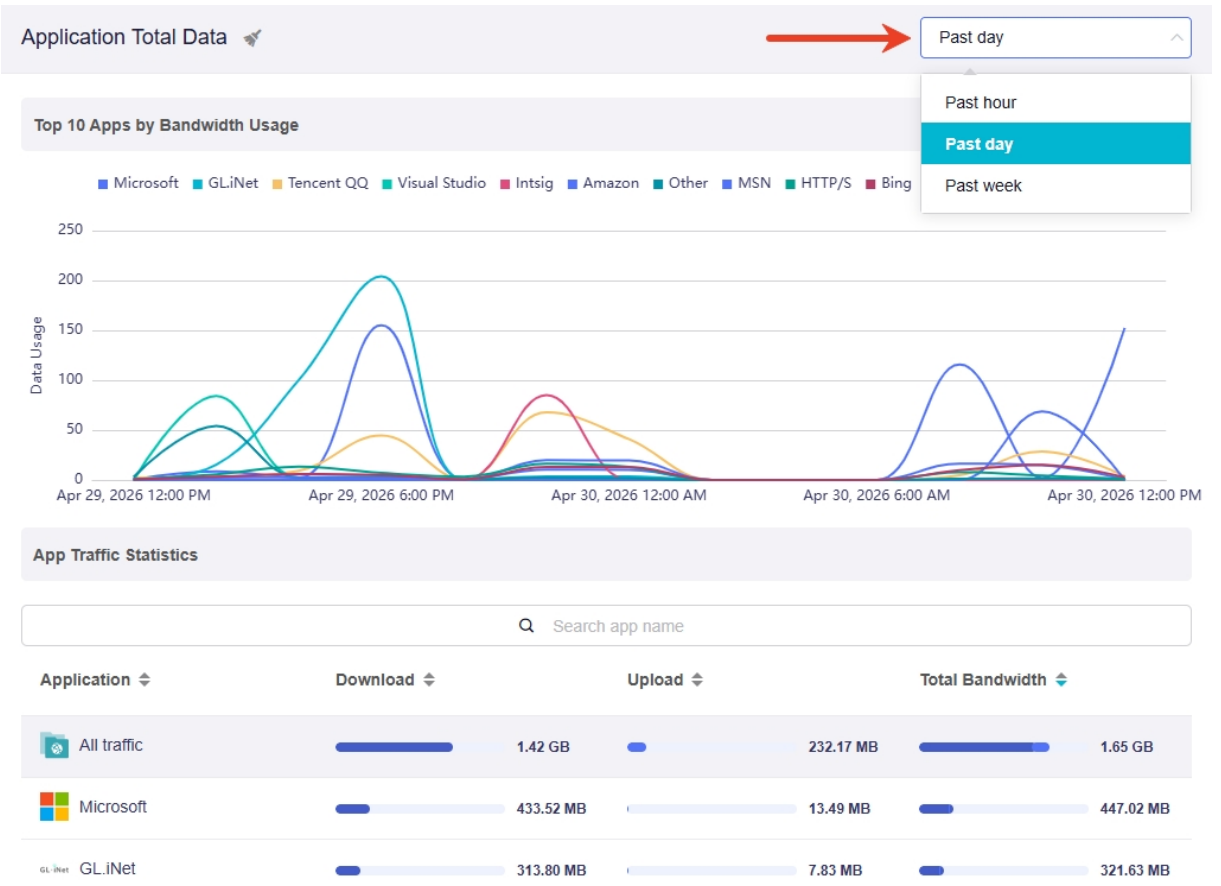


13.2.2 Reglas de almacenamiento de datos

1. Las estadísticas de tráfico se guardan en la RAM cada 15 segundos y se almacenan en la memoria flash cada 1 hora. Se evitan las escrituras flash frecuentes para proteger la vida útil de la memoria flash.
2. Un reinicio suave no provocará la pérdida de datos. El sistema primero escribe datos de la RAM en la memoria flash antes de reiniciar.
3. Un reinicio completo (desconectar y volver a conectar la alimentación) o una actualización del firmware (conservar la configuración) puede provocar la pérdida de datos hasta la hora más reciente.

13.2.3 Cambiar el intervalo de tiempo

Puede cambiar el rango de tiempo entre Última hora, Último día y La semana pasada, si es necesario.

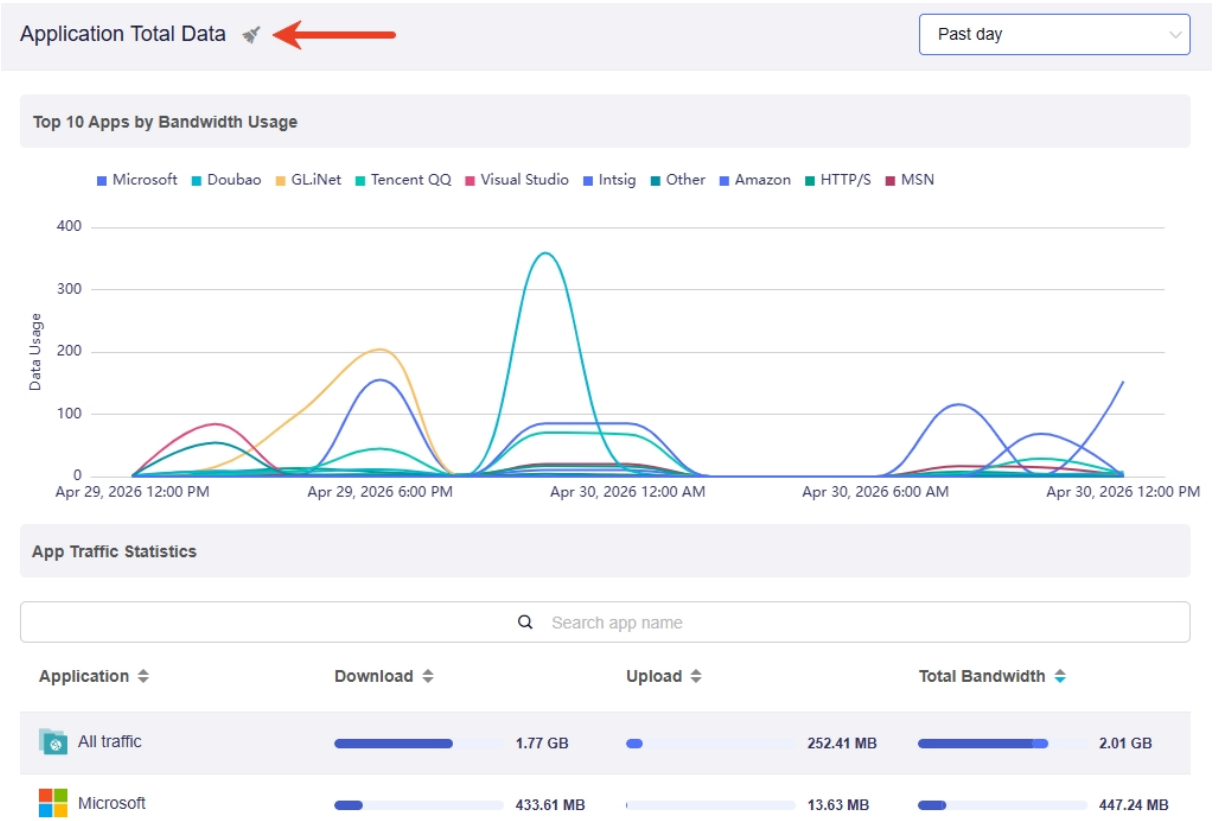


El intervalo de tiempo que elija determina cómo se muestran los datos:

- **Para una mirada más cercana (por ejemplo, hora pasada)**: el gráfico muestra fluctuaciones detalladas en tiempo real. Los picos son más altos y las caídas más pronunciadas, lo que facilita detectar picos repentinos en el uso del ancho de banda.
- **Para obtener una descripción general amplia (por ejemplo, el último día o la semana pasada)**: el gráfico condensa los datos en una línea de tiempo más larga. Las curvas se vuelven más suaves y muestran la tendencia general del tráfico en lugar de cada pequeño cambio.

13.2.4 Borrar estadísticas

Haga clic en el ícono de la escoba en la esquina superior izquierda para borrar las estadísticas si es necesario.



Después de borrar, la página no mostrará datos. Espere un momento a que se completen nuevas estadísticas.

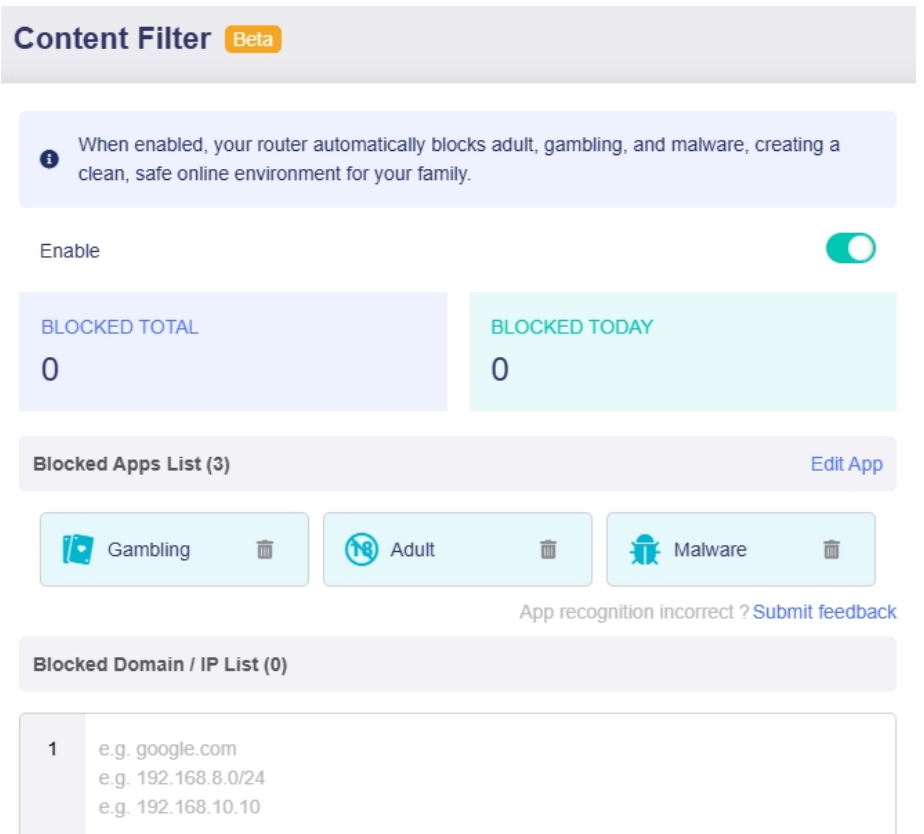
13.3 Filtro de contenido

El filtro de contenido es una función inteligente de seguridad en línea impulsada por la clasificación DPI. Bloquea sitios web dañinos y maliciosos automáticamente para mantener su red limpia y segura, y también admite reglas personalizadas para bloquear aplicaciones, dominios o direcciones IP específicas.

Nota:

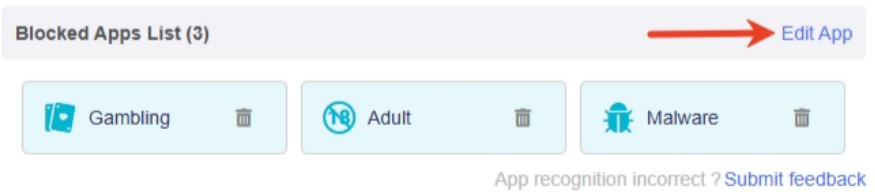
1. El filtro de contenido no tendrá efecto cuando el enrutador esté en modo de puerta de enlace directa.
2. El filtro de contenido no puede funcionar con la aceleración de red. Al habilitar el filtro de contenido, se deshabilitará automáticamente la aceleración de red para garantizar un rendimiento estable.

Inicie sesión en el panel de administración web del enrutador'y navegue hasta **CONTROL DE FLUJO** > **Filtro de contenido**.
Activa el interruptor en la esquina superior derecha, personaliza el contenido bloqueado y luego haz clic en **Aplicar**.

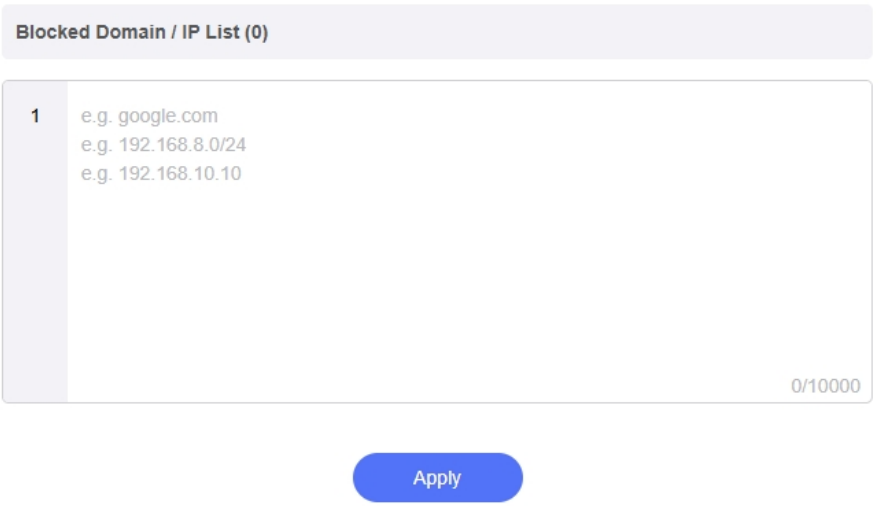


Esta página consta de dos partes:

- **Lista de aplicaciones bloqueadas**: esta sección incluye tres categorías preseleccionadas: Juegos de apuestas, Adultos y Malware. Cuando esté habilitado, se bloquearán todos los sitios web, servicios o aplicaciones relacionados con estas tres categorías. Puede hacer clic en **Editar aplicación** para agregar otras categorías (por ejemplo, juegos, redes sociales, compras) si es necesario.



- **Lista de IP/dominios bloqueados**: esta sección le permite ingresar manualmente dominios específicos (por ejemplo, google.com), rango CIDR (p. ej., 192.168.8.0/24) o direcciones IP (p. ej., 192.168.10.10) para bloquear el acceso a ellos. La lista admite hasta 10000 entradas.
  Ingrese los dominios o direcciones IP que desea bloquear y luego haga clic en **Aplicar**.



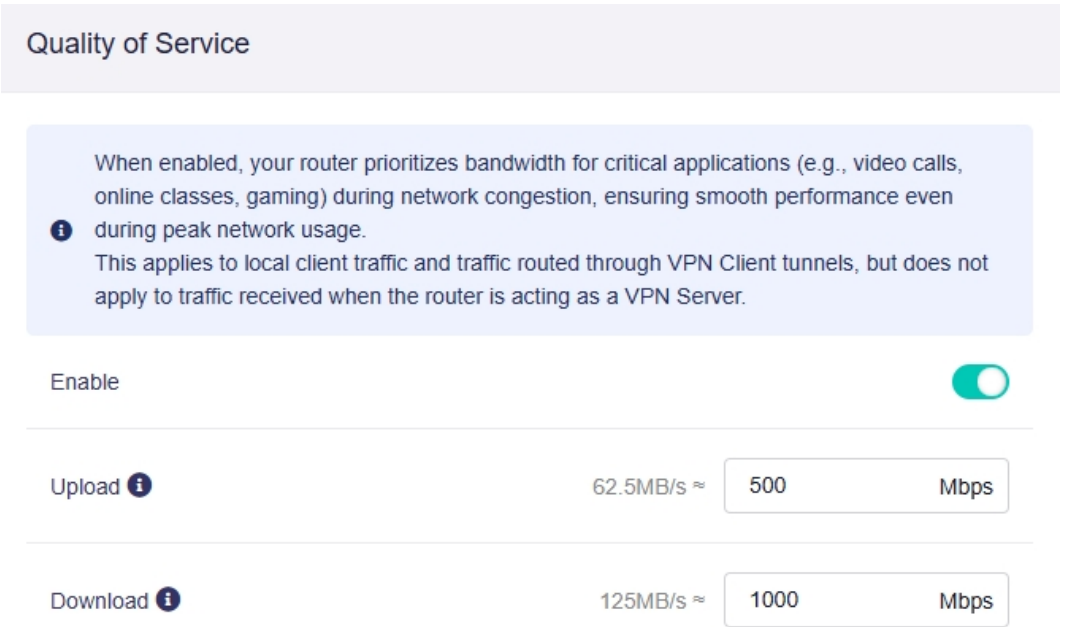
13.4 Calidad de servicio (QoS)

QoS (calidad de servicio) optimiza la asignación de ancho de banda al priorizar el tráfico sensible a la latencia, como las videollamadas. y juegos durante la congestión de la red, lo que reduce la latencia y mejora el rendimiento general de la red.

Nota:

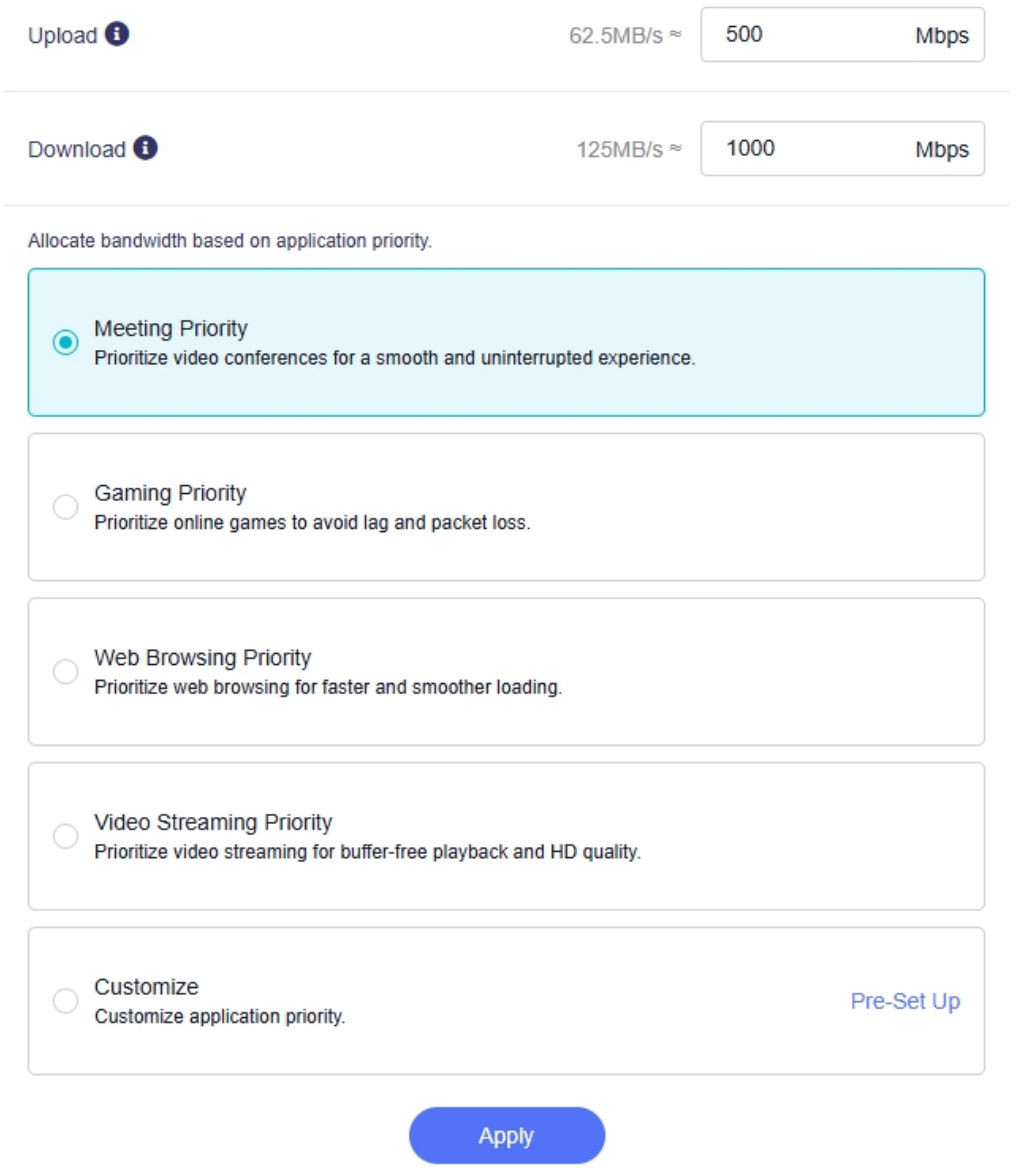
1. Esta característica solo afecta el tráfico que pasa a través del enrutador cuando funciona como puerta de enlace, incluido el tráfico de clientes locales y el tráfico de clientes VPN. No se aplica al tráfico entrante cuando el enrutador actúa como servidor VPN.
2. QoS no tendrá efecto cuando el enrutador esté en modo Drop-in Gateway.
3. QoS y SQM no se pueden habilitar simultáneamente.
4. QoS no puede funcionar con aceleración de red. Al habilitar QoS se deshabilitará automáticamente la aceleración de red para garantizar un rendimiento estable.

Inicie sesión en el panel de administración web del enrutador', vaya a **CONTROL DE FLUJO** > **Calidad de servicio (QoS)** y habilítelo. Establezca sus velocidades máximas de carga y descarga (rango de entrada: 1-10000) para la programación del tráfico. Combínelos con su ancho de banda de Internet real para obtener mejores resultados.



Consejo: Los valores ingresados en el campo de entrada están en **Mbps** (megabits por segundo). Se muestra el equivalente en MB/s (megabytes por segundo) para su referencia.

Luego, establezca prioridades para diferentes aplicaciones. El enrutador asignará el ancho de banda en consecuencia.



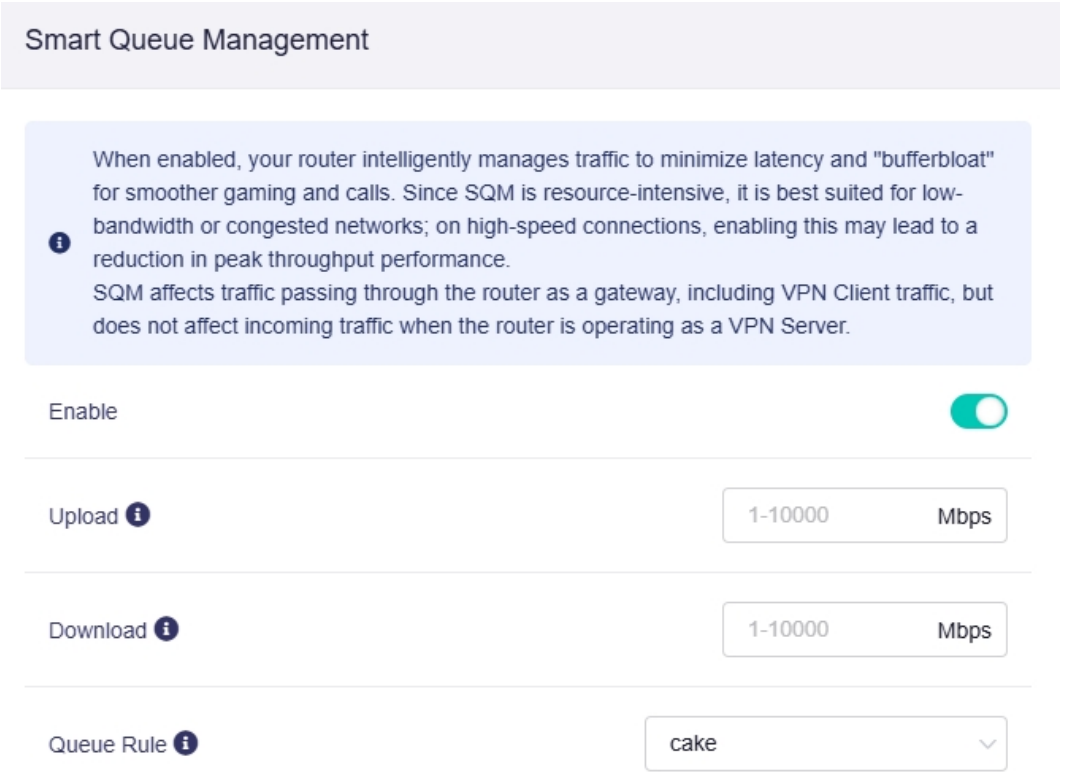
13.5 Gestión inteligente de colas (SQM)

SQM (Smart Queue Management) administra de manera inteligente el tráfico de red de su enrutador para minimizar la latencia y el "bufferbloat", lo que garantiza juegos y llamadas de voz más fluidos.

Nota:

1. Esta característica solo afecta el tráfico que pasa a través del enrutador cuando funciona como puerta de enlace, incluido el tráfico de clientes locales y el tráfico de clientes VPN. No se aplica al tráfico entrante cuando el enrutador actúa como servidor VPN.
2. Dado que SQM consume muchos recursos, funciona mejor para redes congestionadas o con poco ancho de banda. Habilitarlo en conexiones de alta velocidad puede reducir el rendimiento máximo.
3. SQM no tendrá efecto cuando el enrutador esté en modo Drop-in Gateway.
4. SQM y QoS no se pueden habilitar simultáneamente.
5. SQM no puede funcionar con aceleración de red. Al habilitar SQM, se deshabilitará automáticamente la aceleración de red para garantizar un rendimiento estable.

Inicie sesión en el panel de administración web del enrutador', vaya a **CONTROL DE FLUJO** > **Gestión inteligente de colas (SQM)** y habilítelo. Primero establezca sus velocidades máximas de carga y descarga (rango de entrada: 1-10000) para la programación del tráfico. Combínelos con su ancho de banda de Internet real para obtener los mejores resultados.



Para **Regla de cola**, hay dos opciones disponibles:

- **pastel**: configuración de tráfico inteligente y automática con control de latencia general superior. (recomendado).
- **fq_codel**: colas justas, simples y eficientes con reducción de latencia básica.

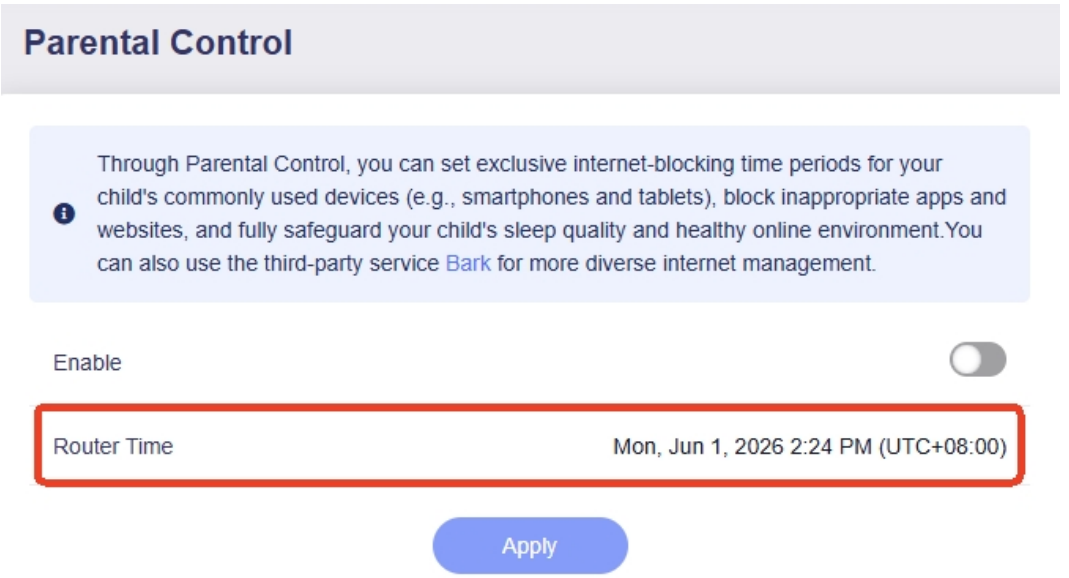
Consejo: una diferencia entre la configuración de QoS y SQM es que la QoS le permite establecer las prioridades de las aplicaciones y el enrutador asigna el ancho de banda en consecuencia; mientras que el SQM permite seleccionar una regla de cola.

13.6 Control parental

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

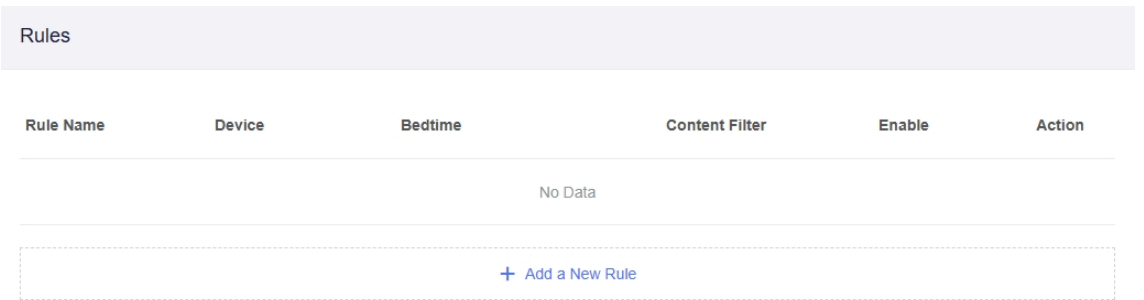
Siga los pasos a continuación para configurar su control parental.

1. Inicie sesión en el panel de administración web del enrutador y vaya a **CONTROL DE FLUJO** -> **Control parental**. Asegúrese de que la hora del enrutador sea precisa.

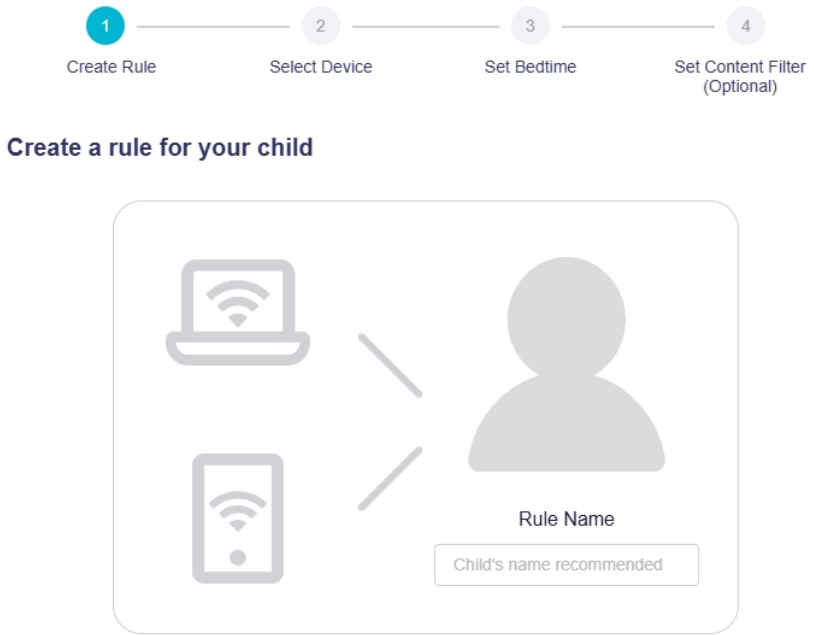


   Si no, vaya a **SISTEMA** -> **Zona horaria** para sincronizarlo primero.

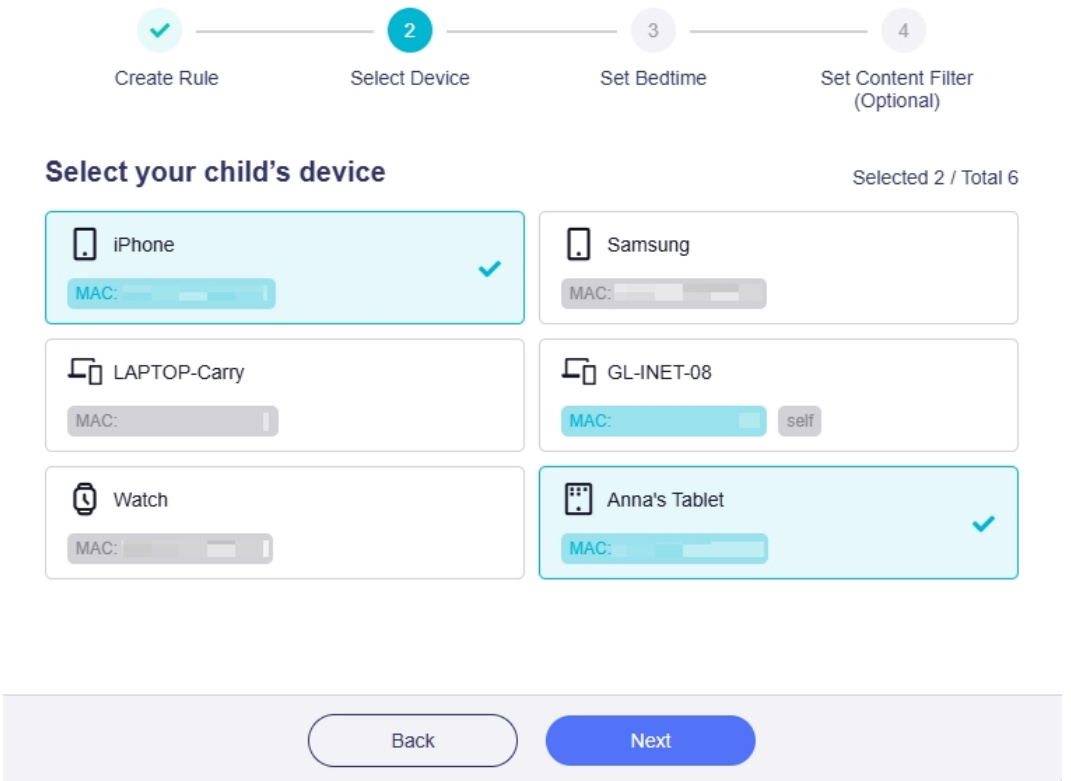
2. Habilite el control parental y haga clic en **Aplicar**.
3. Verá una lista de reglas como la siguiente. Haga clic en **Agregar una nueva regla**.



4. En la ventana emergente, cree una regla y establezca un nombre personalizado, luego haga clic en **Siguiente**.

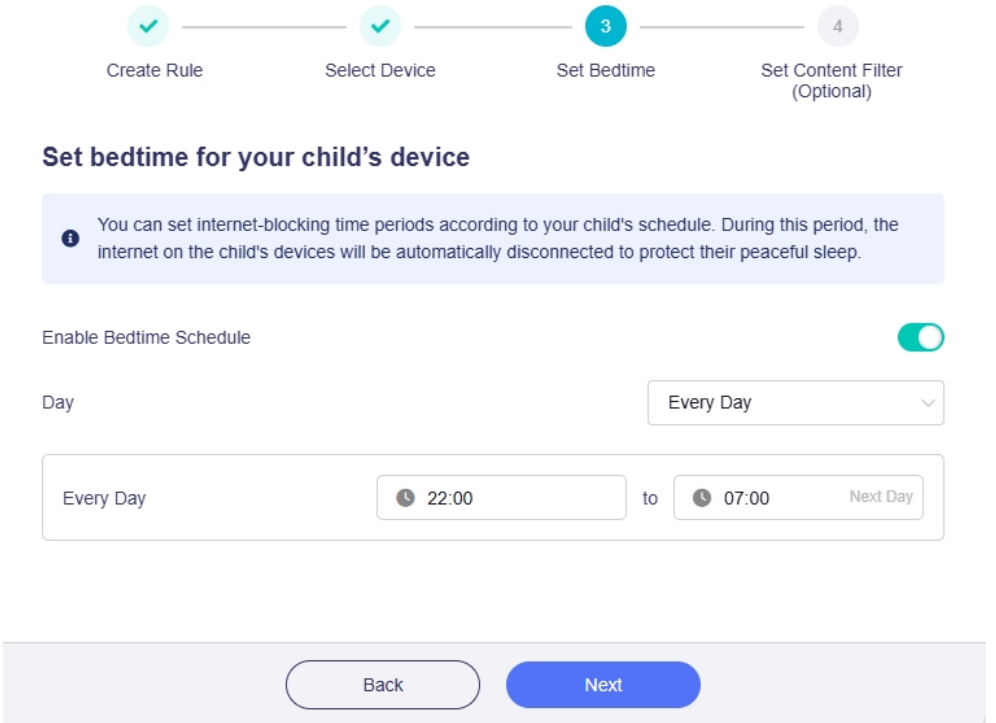


5. Seleccione el dispositivo de su hijo, luegoluego haga clic en **Siguiente**. Ddispositivos solo aparecerán en esta página si están conectados al enrutador a través de Wi-Fi o Ethernet. El cian indica el estado en línea, mientras que el gris indica el estado fuera de línea.



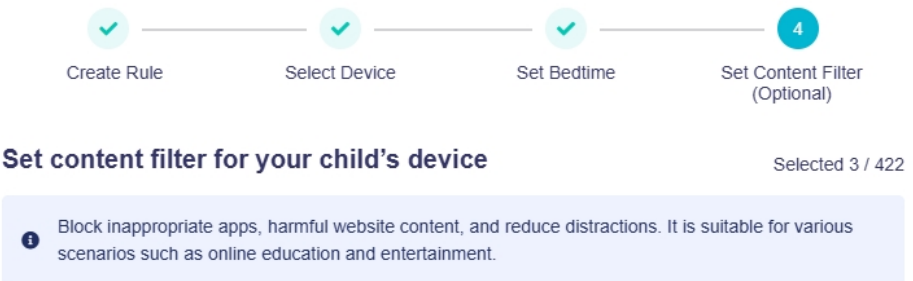
Consejo: si desea distinguir los dispositivos conectados, vaya a la página **CLIENTE** y personalice los nombres de los dispositivos.

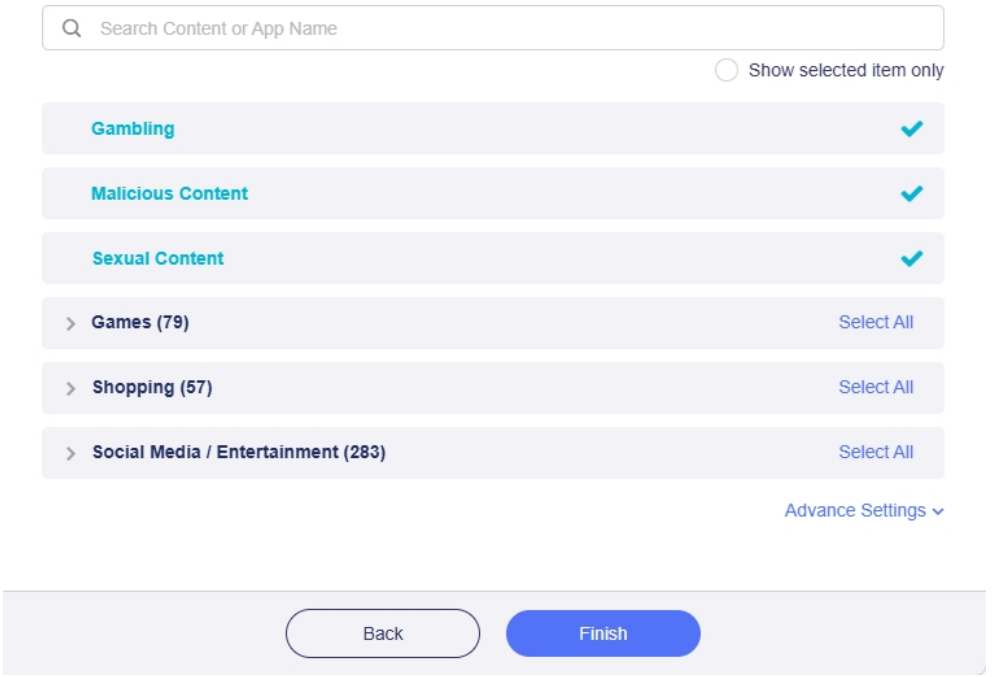
6. Establezca la hora de acostarse para el dispositivo de su hijo y luego haga clic en **Siguiente**. Internet en los dispositivos seleccionados no estará disponible durante este período. Lala hora de acostarse es la misma todos los días de forma predeterminada.



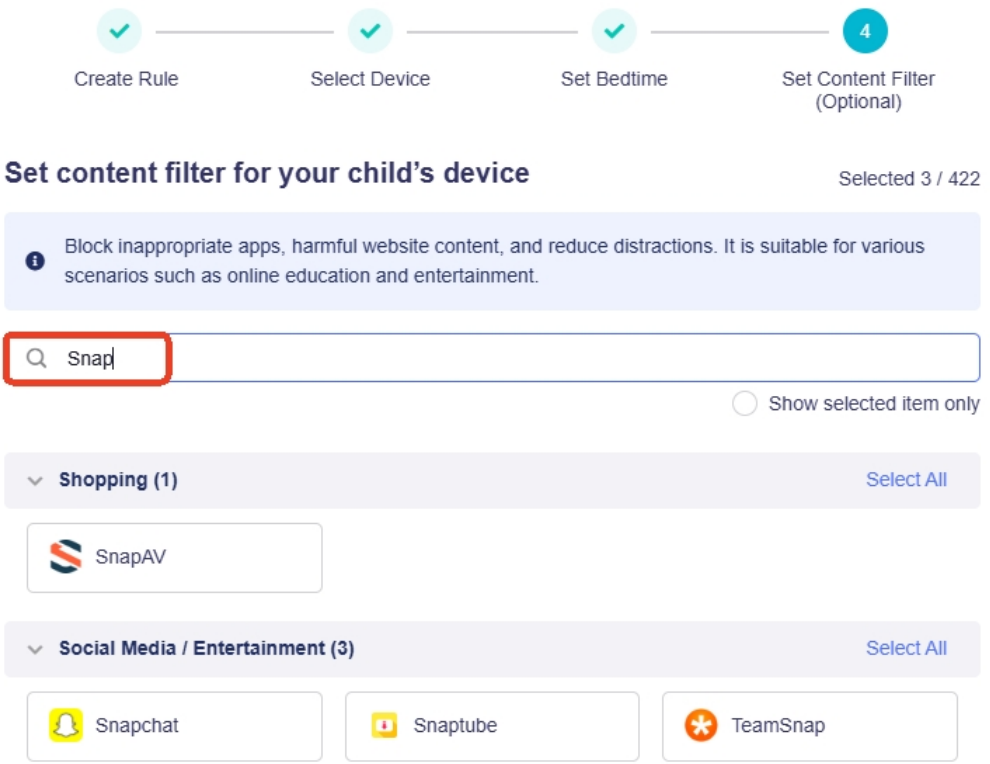
Si desea establecer diferentes horas de acostarse para cada día de la semana, seleccione **Personalizar Días** y establezca diferentes horas de acostarse, luego haga clic en **Siguiente**.

7. Seleccione el filtro de contenido.
   Se han seleccionado tres categoríascted por predeterminado: **Apuestas**, **Contenido malicioso Contenido** y **Contenido sexual**. Puede seleccionar otras categorías si es necesario. como como **Juegos**, **Compras**, **Social Medios**, **Entretenimiento**, etc.

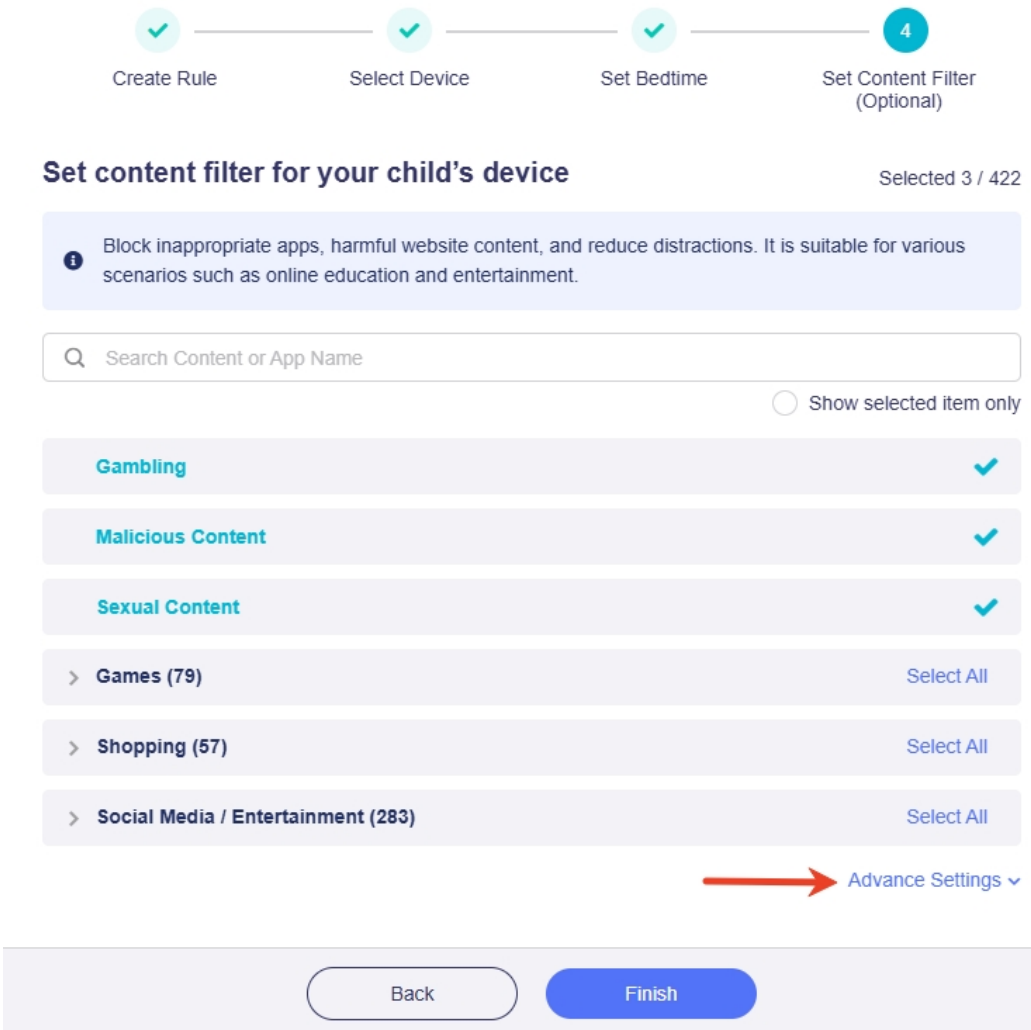




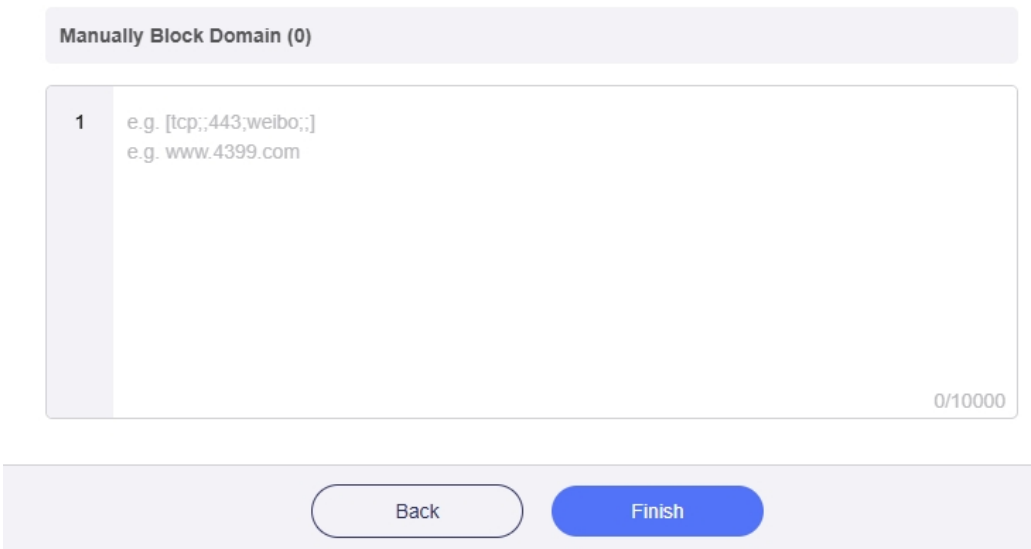
Si es difícil encontrar una determinada aplicación que deseas bloquear, puedes buscarla en la parte superior.



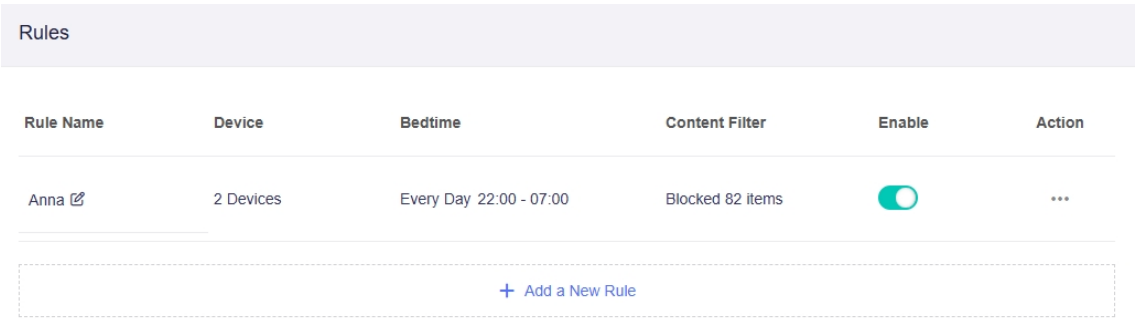
8. Si necesitas bloquear ciertos dominios, haz clic en **Configuración avanzada** en la parte inferior derecha.



Ingrese los dominios manualmente y luego haga clic en **Finalizar**.



9. La regla ya está agregada. La lista muestra el nombre de la regla, el número de dispositivos conectados, el horario de acostarse, el contenido filtrado y el estado de la regla (habilitado/deshabilitado).



Capítulo 14

Seguridad

Este capítulo administra la seguridad de la red, como el reenvío de puertos, la configuración de acceso de administrador y el modo NAT.

14.1 Reenvío de puertos

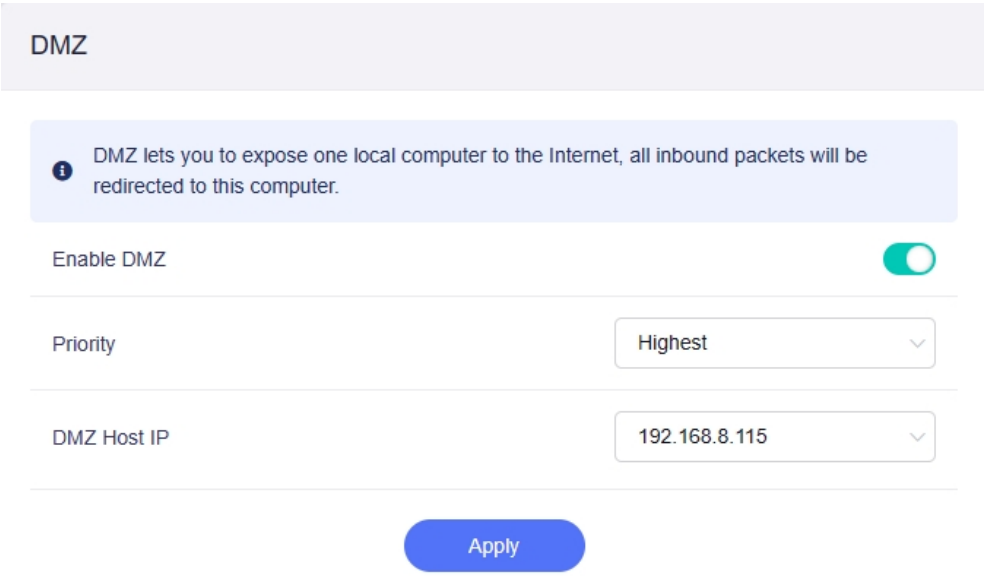
El reenvío de puertos es una función de red que enruta solicitudes externas a dispositivos específicos en su red local. La página de reenvío de puertos incluye dos funciones clave: **DMZ** (para acceso completo directo a un único dispositivo) y **Reenvío de puertos** (para acceso dirigido a puertos específicos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

14.1.1 DMZ

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

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

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



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

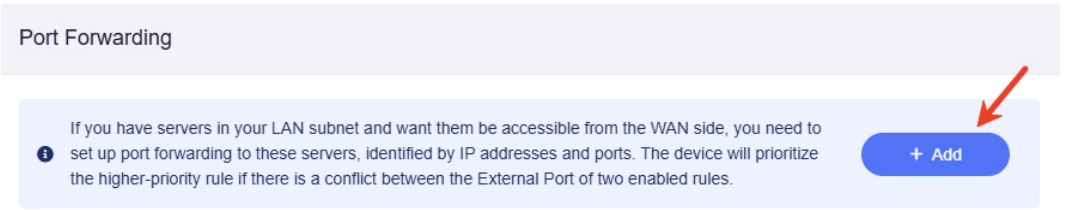
- **IP del host DMZ**: seleccione la dirección IP interna de el dispositivo que recibirá todos los paquetes entrantes.

14.1.2 Reenvío de puertos

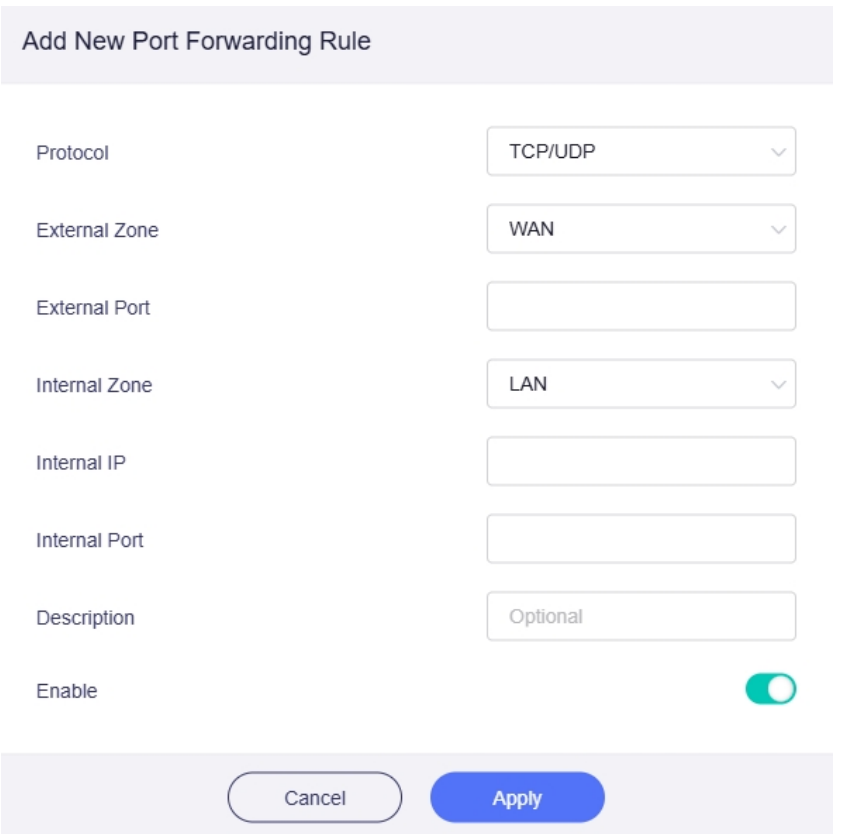
El reenvío de puertos permite que las computadoras remotas se conecten a una computadora o servidor local detrás del firewall de la LAN (por ejemplo, servidores web, servidores FTP).

Fsiga los pasos siguientes tpara configurar el reenvío de puertos if necesario.

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



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



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

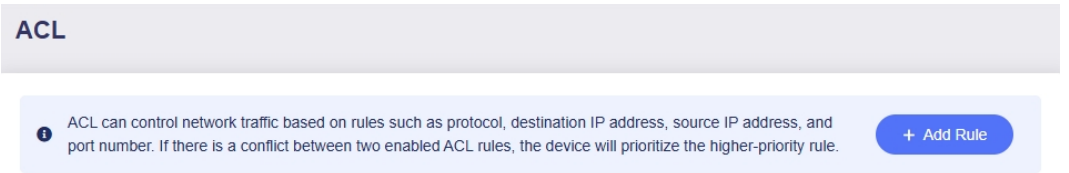
14.2 Lista de control de acceso (ACL)

ACL, abreviatura de Lista de control de acceso, le permite crear reglas para administrar el tráfico de red según protocolos de conexión, direcciones de dispositivos y puertos. Controla si se permite o bloquea el acceso a la red. Si varias reglas de ACL entran en conflicto, el sistema aplica la que tiene mayor prioridad.

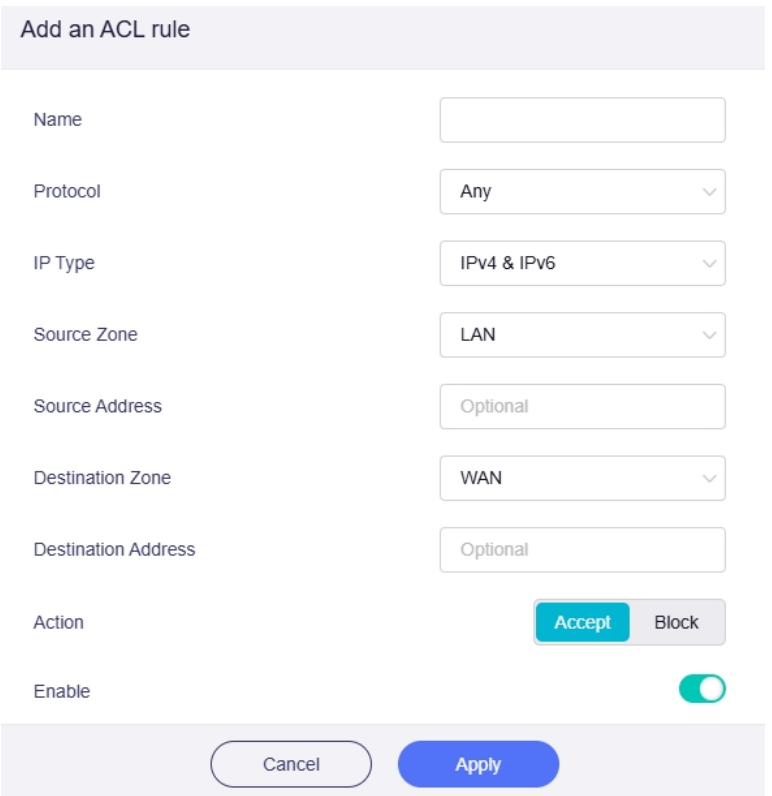
Ddiferente de Port Forwarding, ACL principalmente permite o bloquea el acceso a la red por motivos de seguridad, mientras que Port Forwarding redirige el tráfico externo a dispositivos específicos en su red local. para habilitar el acceso remoto a los servicios locales.

Fsiga los pasos siguientes tpara configurar la Lista de control de acceso if necesario.

1. Inicie sesión en el panel de administración web de su enrutador' y vaya a **SEGURIDAD** > **Lista de control de acceso (ACL)**. Haga clic en el botón **Agregar regla** a la derecha.



2. Cree su regla ACL en la ventana emergente, luego haga clic en **Aplicar**.



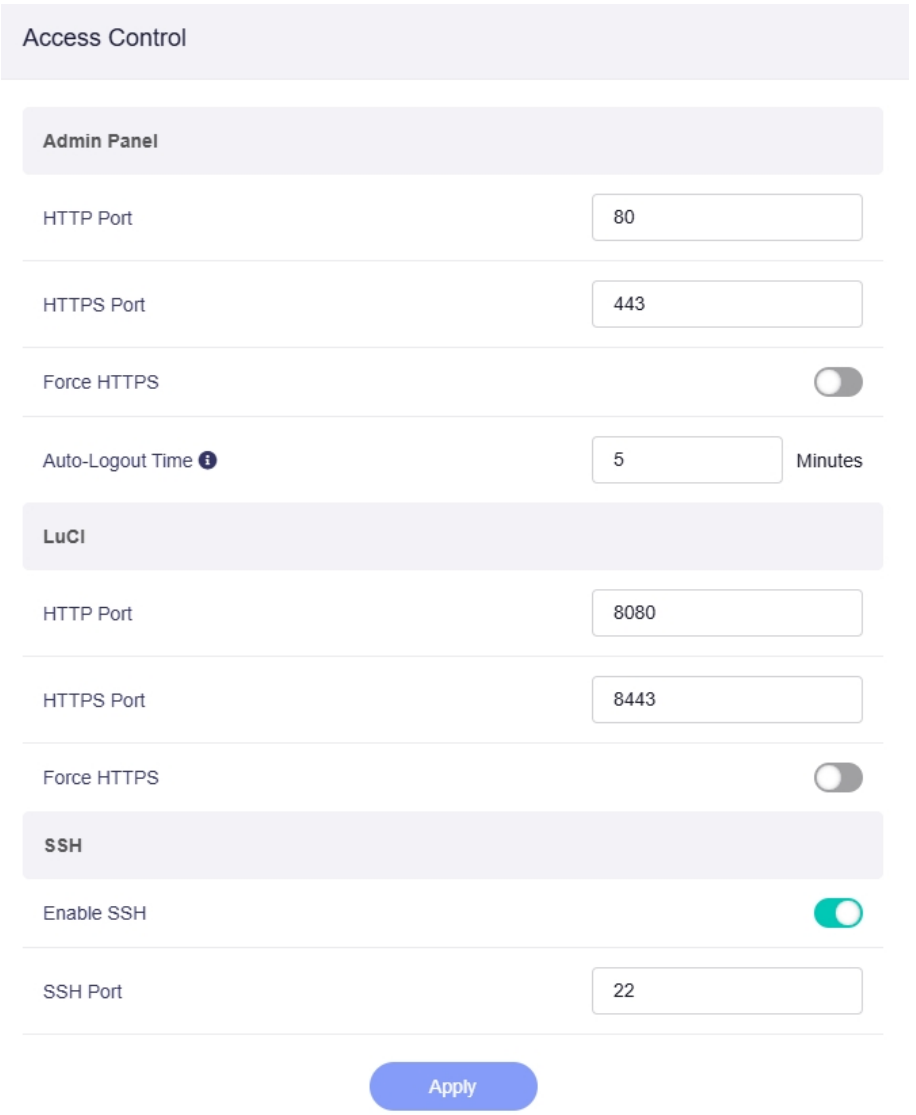
- **Nombre**: ingrese un nombre personalizado para la regla.
- **Protocolo**: especifique a qué tipo de tráfico de red se aplica la regla. Seleccione un protocolo de conexión entre Cualquiera, TCP, UDP, TCP+UDP e ICMP.
- **Tipo de IP**: defina el formato de dirección IP para el tráfico de red. Seleccione el tipo de IP entre IPv4 e IPv6, IPv4 e IPv6.
- **Zona de origen**: seleccione la zona de red donde se origina el tráfico. Opciones disponibles: LAN, Invitado, IoT y WAN.
- **Dirección de origen**: (Opcional) restrinja la regla a dispositivos de origen o direcciones IP específicos. Puede seleccionar una dirección de origen de la lista desplegable.
- **Zona de destino**: aquí es hacia donde se dirige el tráfico de la red. Seleccione la zona de red de destino. Opciones disponibles: LAN, Invitado, IoT y WAN.
- **Dirección de destino**: (Opcional) restrinja la regla a dispositivos de destino o direcciones IP específicos. Puede seleccionar una dirección de destino de la lista desplegable.
- **Acción**: elija Aceptar o bloquear el tráfico de red que coincida con esta regla.
- **Habilitar**: alterne para habilitar o deshabilitar esta regla.

14.3 Acceso de administrador

Inicie sesión en el panel de administración web de su enrutador y navegue hasta **SEGURIDAD** > **Acceso de administrador**. Esta página le permite configurar el acceso local del enrutador, el acceso remoto HTTPS/SSH y administrar los puertos abiertos en el enrutador, protegiendo su enrutador y su red del acceso no autorizado.

14.3.1 Control de acceso

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



Panel de administración

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

LuCI

Instale LuCI en la Configuración avanzada antes de configurar el control de acceso.

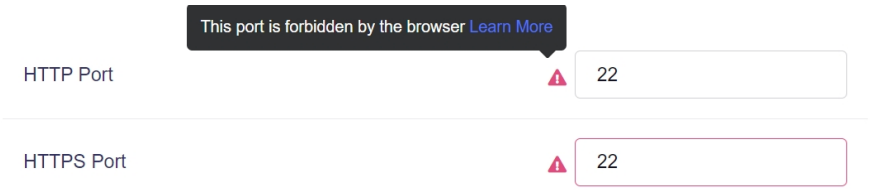
- **Puerto HTTP**: El valor predeterminado es 8080, para acceso HTTP sin cifrar a la interfaz LuCI.
- **Puerto HTTPS**: El valor predeterminado es 8443, para acceso HTTPS seguro a la interfaz LuCI.
- **Forzar HTTPS**: cuando está habilitado, se exige el acceso a la interfaz LuCI para utilizar una conexión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

SSH

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

Nota:

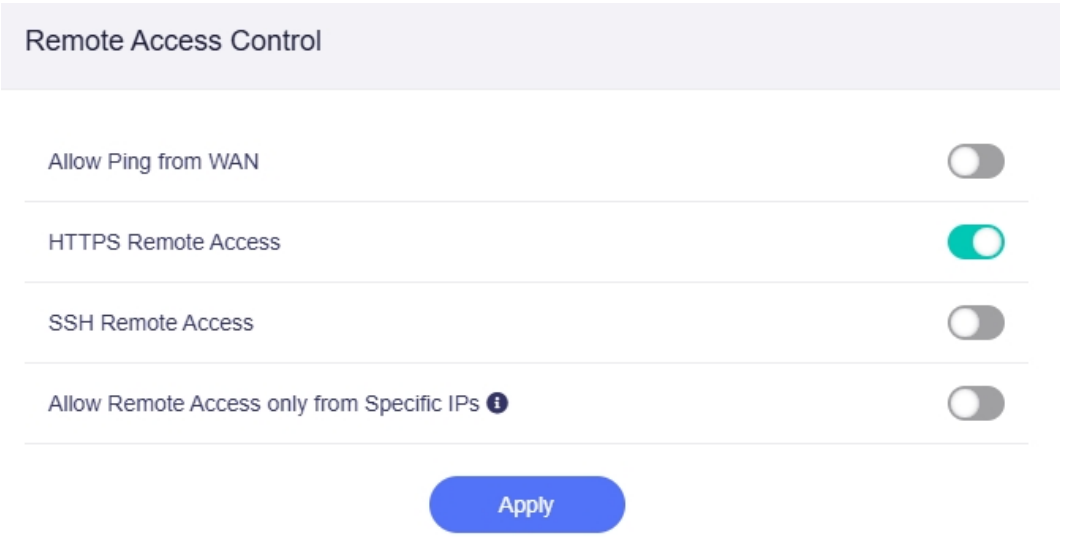
1. Si asigna un número de puerto que entra en conflicto con un puerto reservado (o uno reservado para servicios específicos por navegadores/convenciones de red), aparecerá un mensaje que indicará "Este puerto está prohibido por el navegador".



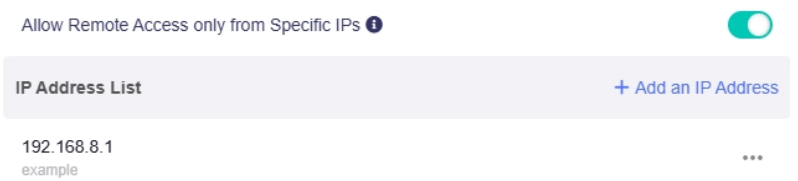
2. Si el número de puerto se modifica en el firmware, deberá ingresar el número de puerto correcto para acceder al panel de administración. Si olvidó el número de puerto, reinicie el enrutador para restaurar el número de puerto predeterminado.

14.3.2 Control de acceso remoto

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

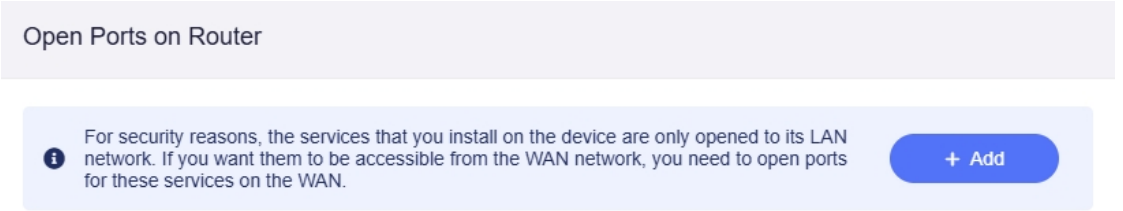


- **Permitir ping desde WAN**: Apermitir ping desde el lado WAN del enrutadorpuede ayudar a los usuarios a verificar si se puede acceder al enrutador a través de la WAN wcuando hay un problema de red, así como a determinar la latencia de la red y la pérdida de paquetes.
- **Acceso remoto HTTPS**: El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

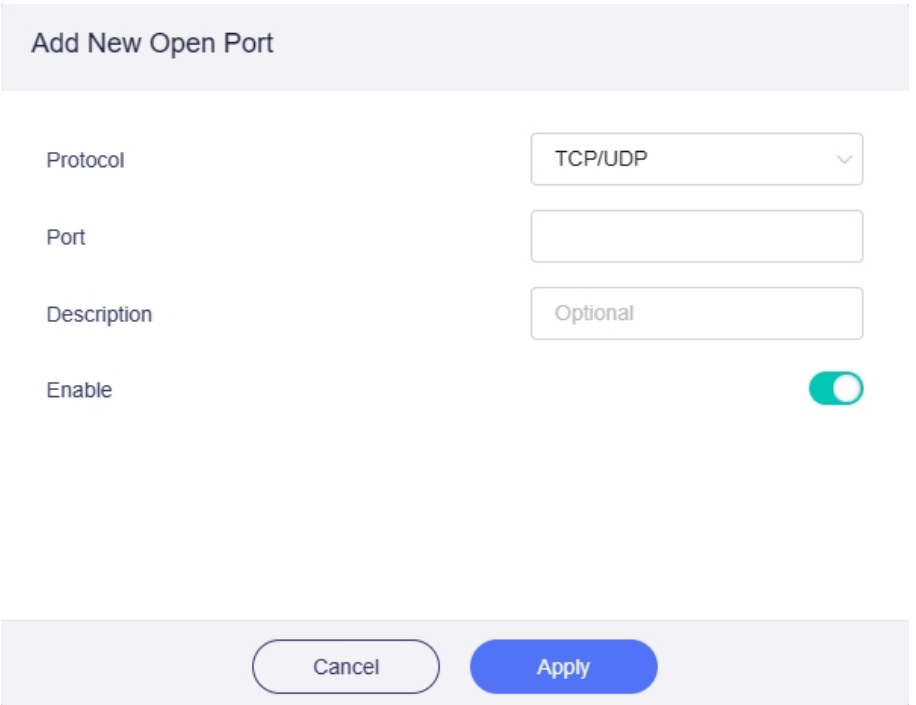


14.3.3 Abrir puertos en el enrutador

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



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

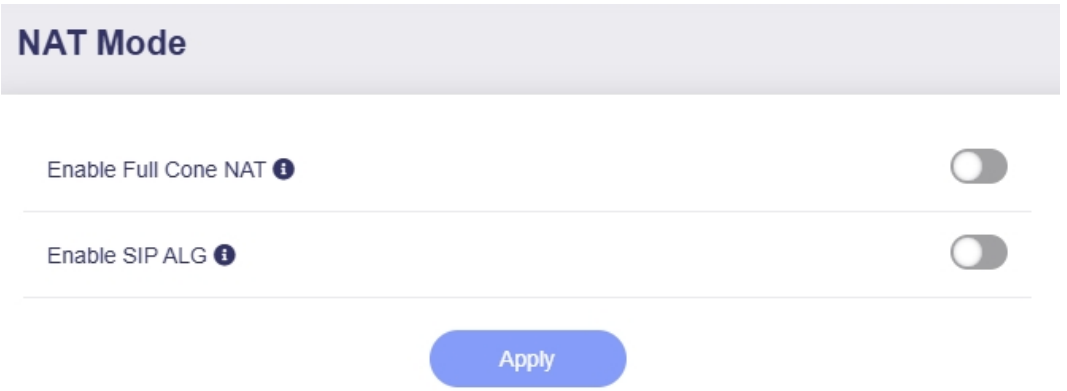


- **Protocolo**: seleccione el protocolo de red (TCP, UDP o TCP/UDP) para el puerto. Esto determina cómo se transmiten los datos para el servicio asociado con el puerto.
- **Puerto**: ingrese el número de puerto específico que desea abrir.

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

14.4 Modo NAT

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



- **NAT de cono completo**: se puede utilizar para reducir 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**: Su objetivo es mitigar los efectos de múltiples NAT en el tráfico SIP (Protocolo de inicio de sesión) . 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 15

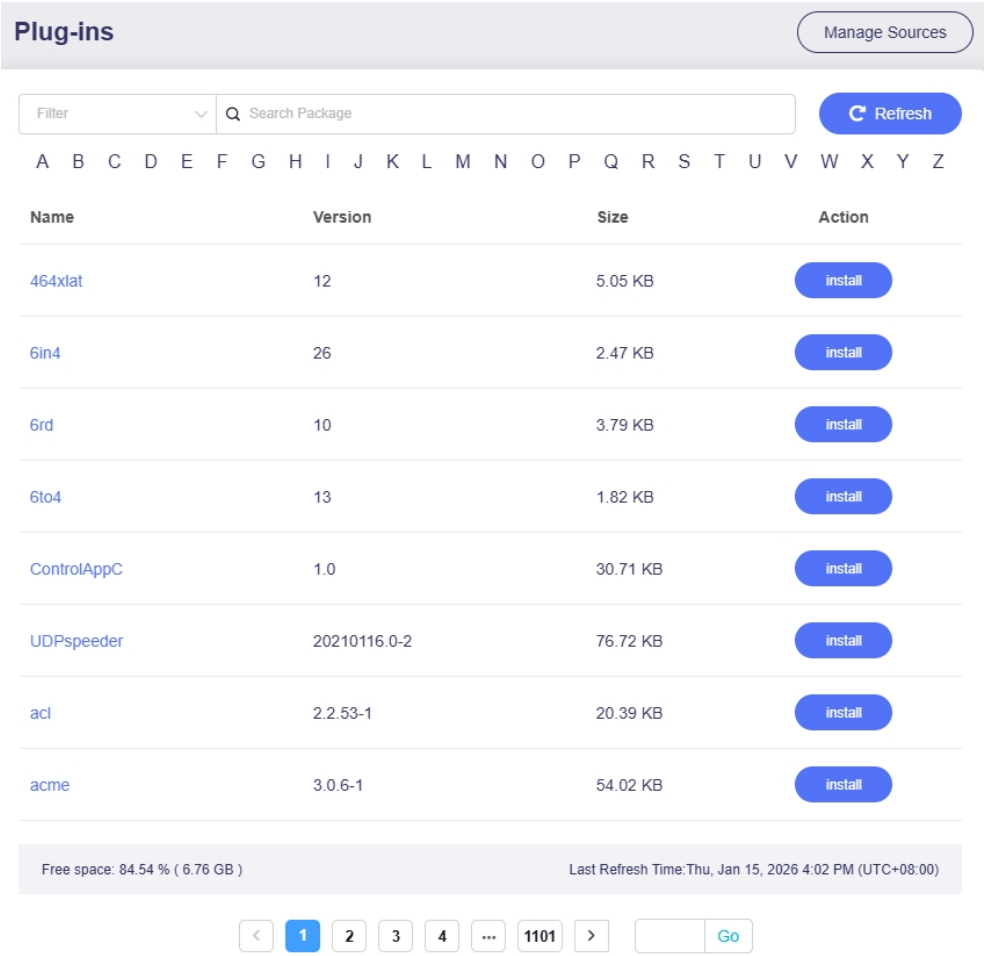
Aplicaciones

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

15.1 Complementos

La Página de complementos le permite administrar paquetes OpenWrt.

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



Nota:

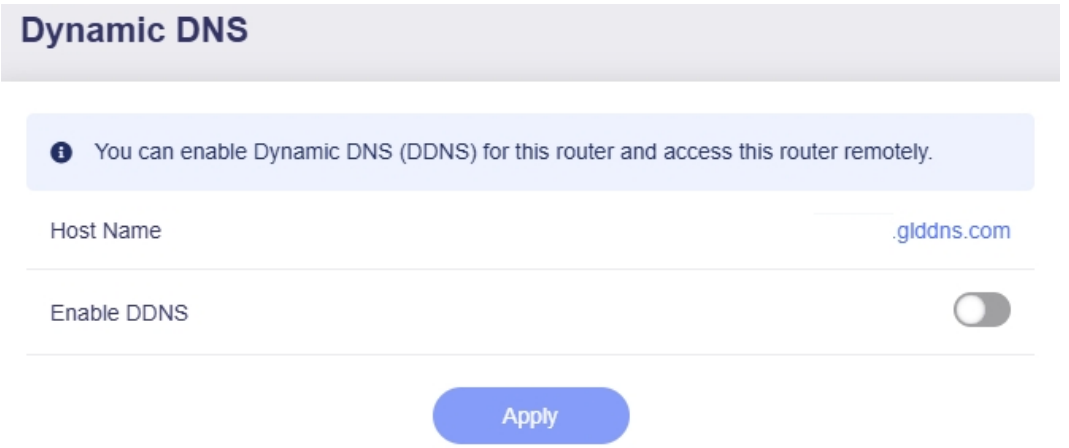
1. No se recomienda actualizar los complementos preinstalados en el firmware oficial de GL.iNet, como nginx, adguard home, tailscale, etc.
2. Los complementos de terceros instalados manualmente por los usuarios se pueden actualizar; sin embargo, GL.iNet no es responsable de ningún problema de seguridad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

15.2 DNS dinámico

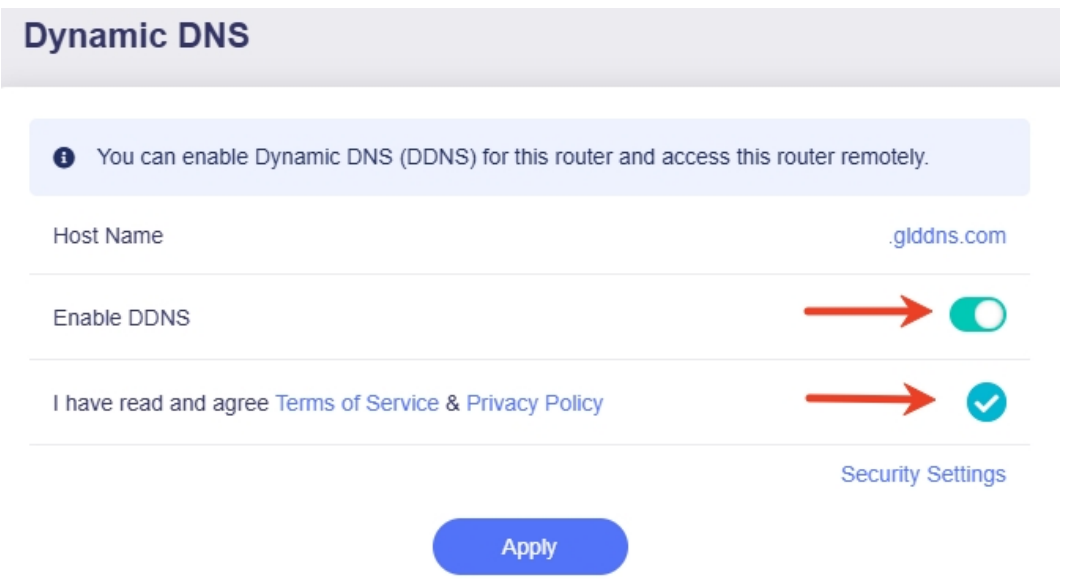
Dinámico El servicio de nombres de dominio (DDNS o DNS dinámico) es un servicio que se utiliza para asignar un nombre de dominio a la dirección IP dinámica de un dispositivo de red. Con DNS dinámico, puede acceder a su enrutador de forma remota. Se requiere una dirección IP pública para esta funcionalidad.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

15.2.1 Habilitar DDNS

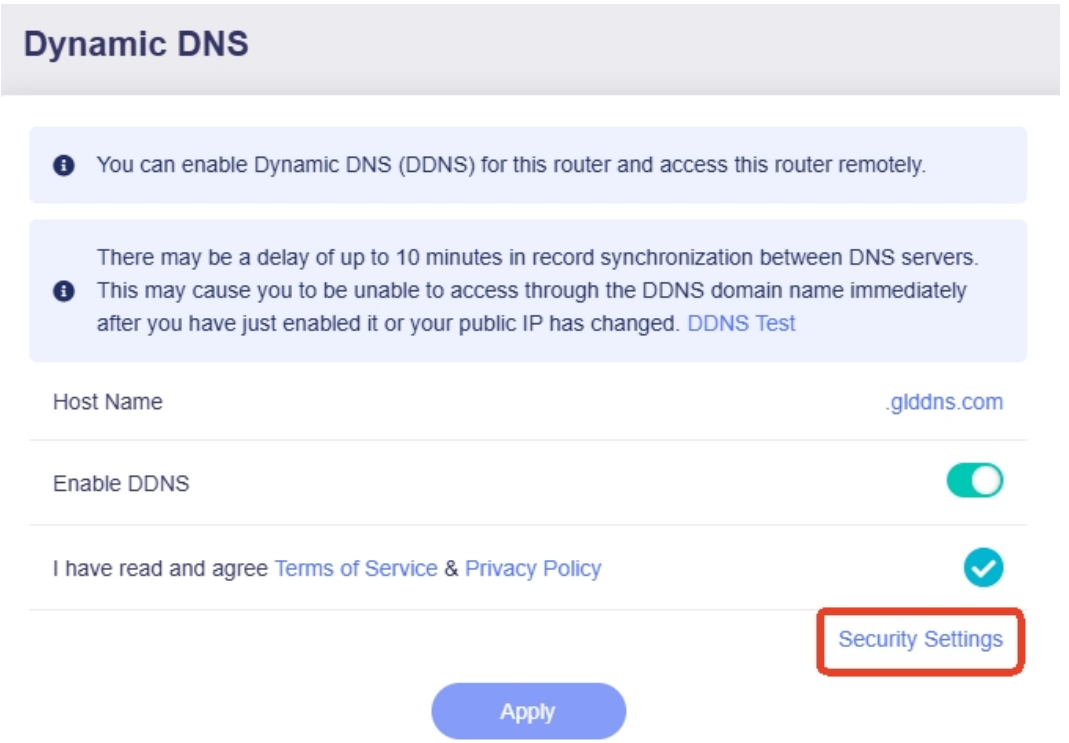
1. Inicie sesión en su enrutador's web admin panel, navegue hasta **APLICACIONES** > **DNS dinámico**, la página se muestra como a continuación.



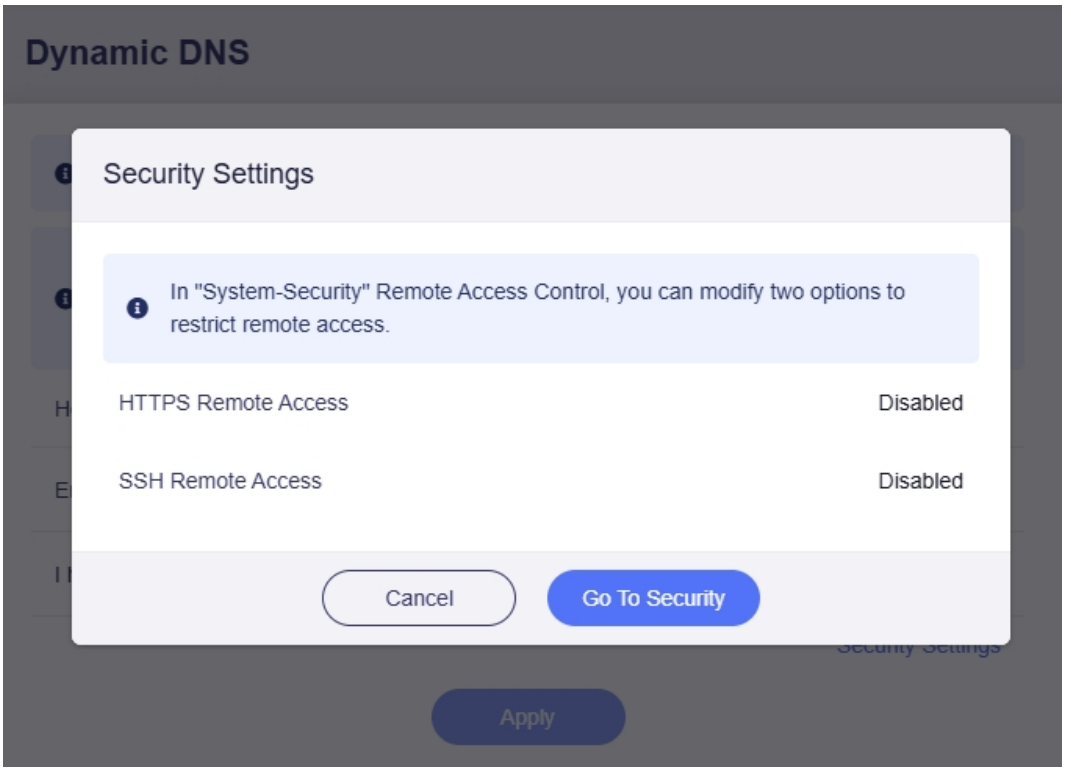
2. Active **Habilitar DDNS**, lectura y acepta los los **Términos de servicios y política de privacidad** y luego haz clic en **Aplicar**.



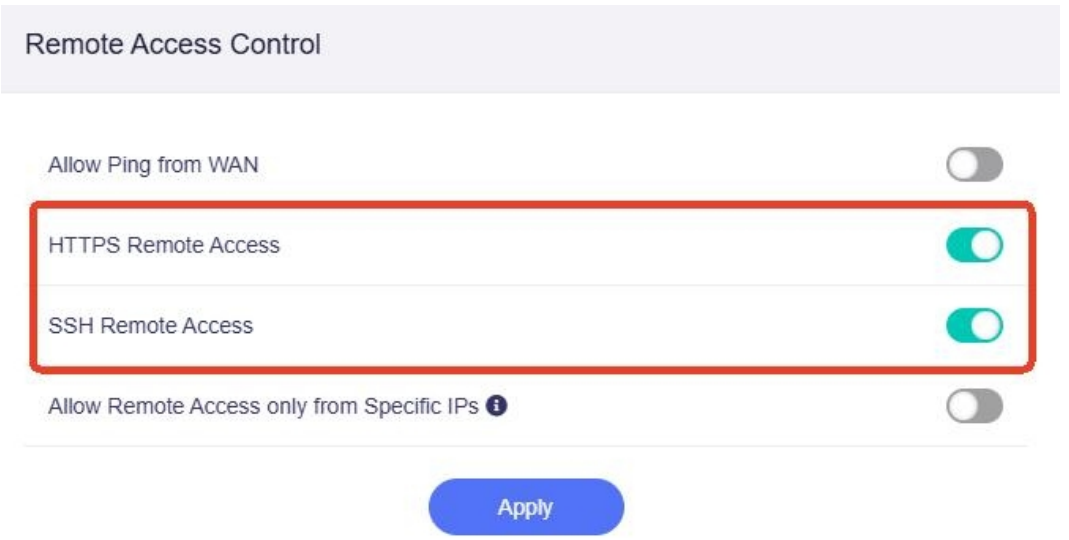
3. Haga clic en **Configuración de seguridad** en la esquina inferior derecha.



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



Si no, vaya a **SECURITY** > **Acceso de administrador** > **Control de acceso remoto** para habilitar it y haga clic en **Aplicar**.



Nota:

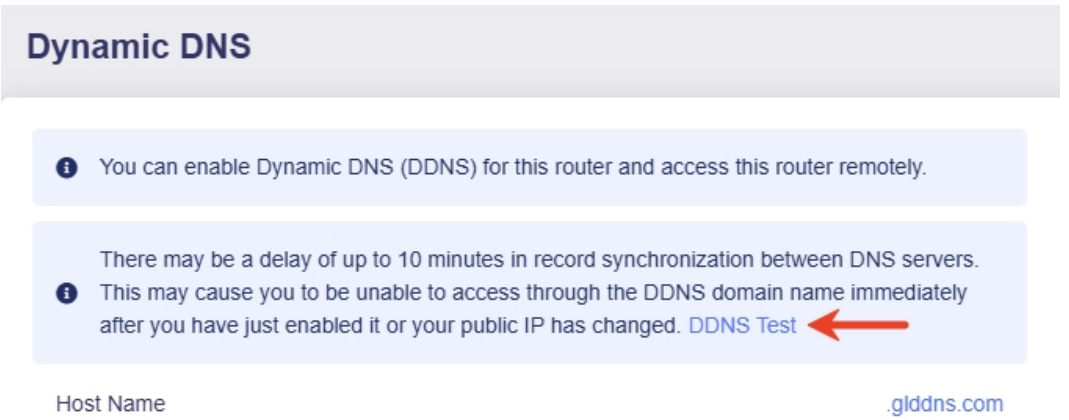
1. Puede haber un retraso de hasta 10 minutos en la sincronización de registros entre servidores DNS. Esto puede impedirle acceder a través del nombre de dominio DDNS inmediatamente después de habilitarlo o cuando cambie su IP pública.
2. Si habilita DDNS y el Cliente VPN al mismo tiempo, enseguro que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

15.2.2 Comprobar si DDNS funciona

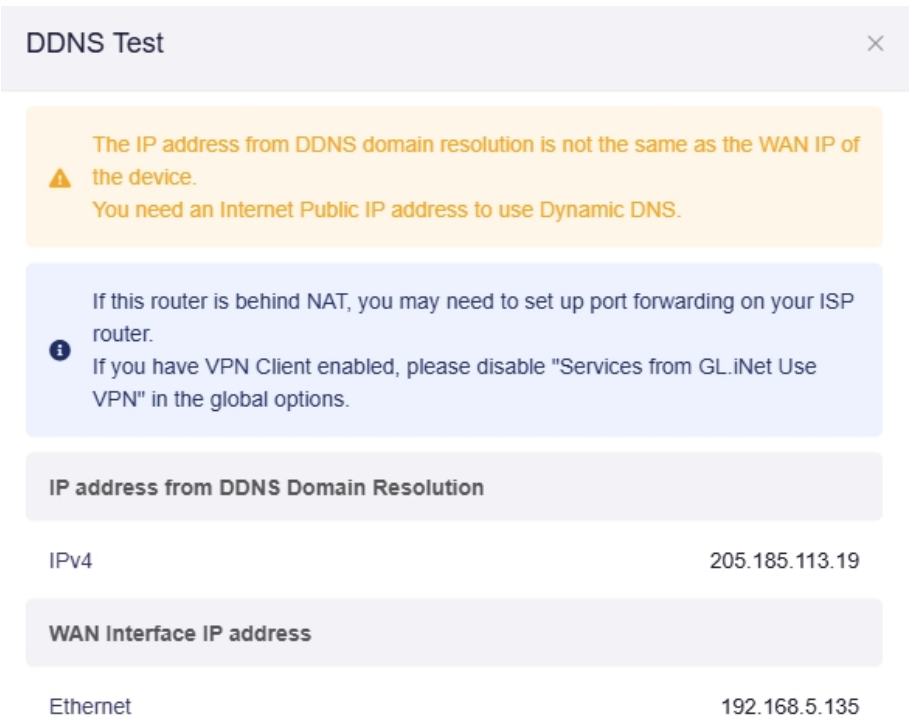
Puede comprobar si DDNS funciona utilizando la herramienta de prueba de DDNS o manualmente mediante comandos.

Método 1. Use Herramienta de prueba DDNS

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



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



Método 2. Usar comandos

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



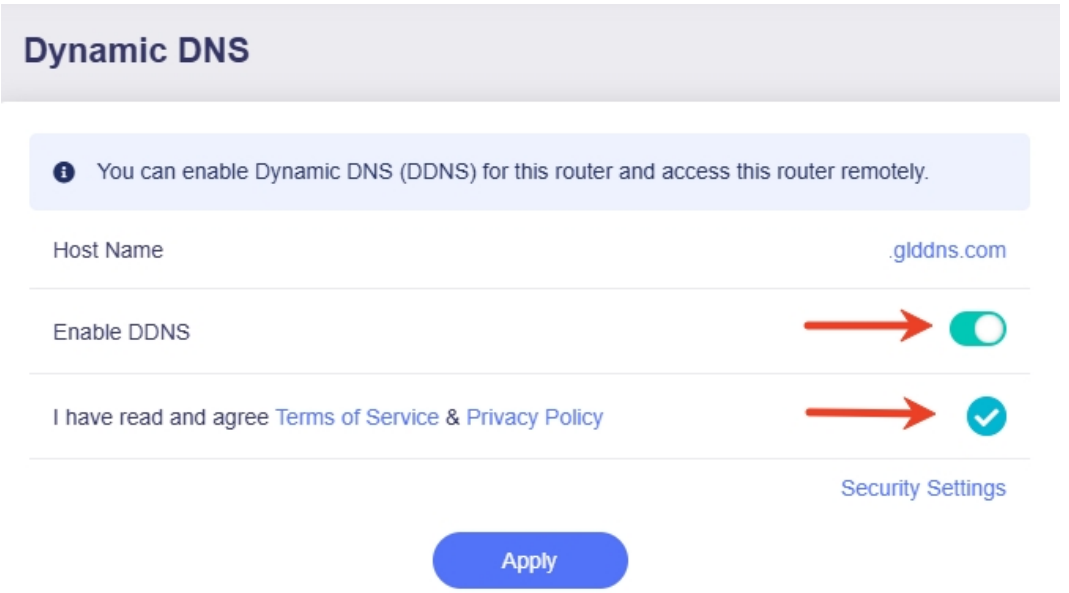
   - Reemplace “xxxxxxx.glddns.com” en la imagen de arriba con su Nombre del host.
   - El “8.8.8.8” es el DNS de Google. Úseloúselo o reemplácelo por otros, luego presione Entrar.
2. Si obtiene una dirección IP pública como “183.178.10.100” en la imagen de arriba, indica que su dominio DDNS se ha asignado 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 su router’s web admin panel y navega hasta **INTERNET**. Encuentra tu enrutador’ en la interfaz activa actual. Compare esta dirección IP con la dirección IP pública obtenida anteriormente. Si son iguales, el DDNS está vigente; de lo contrario, no lo está.

15.2.3 Acceso remoto HTTPS

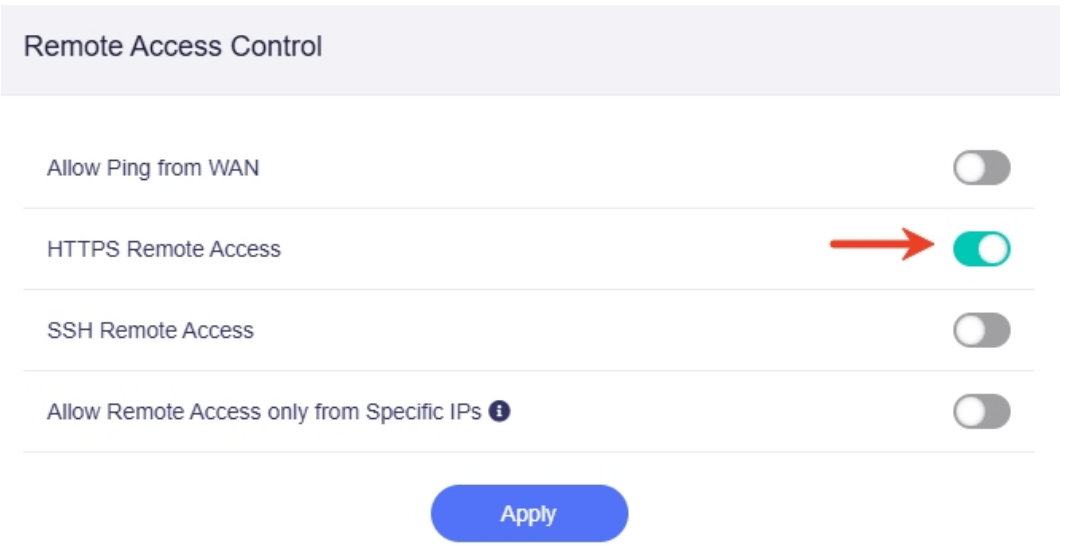
Se requiere una **Dirección IP pública** para el acceso remoto HTTPS. Ver aquí tpara verificar si su ISP le asigna una dirección IP pública. Si su enrutador está detrás de NAT, configure el reenvío de puertos (**puerto 443**) en el enrutador ascendente para acceso HTTPS.

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**.

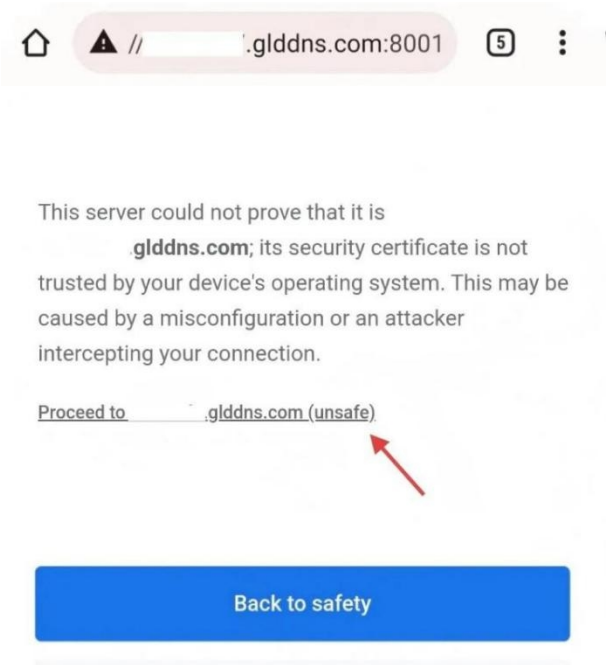


2. En el panel de administración web, vaya a **SECURITY** > **Acceso de administrador** > **Control de acceso remoto**. Habilitar **Acceso remoto HTTPS** y haga clic en **Aplicar**.



Una vez habilitado, podrá acceder al panel de administración del'desde cualquier lugar usando el 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.



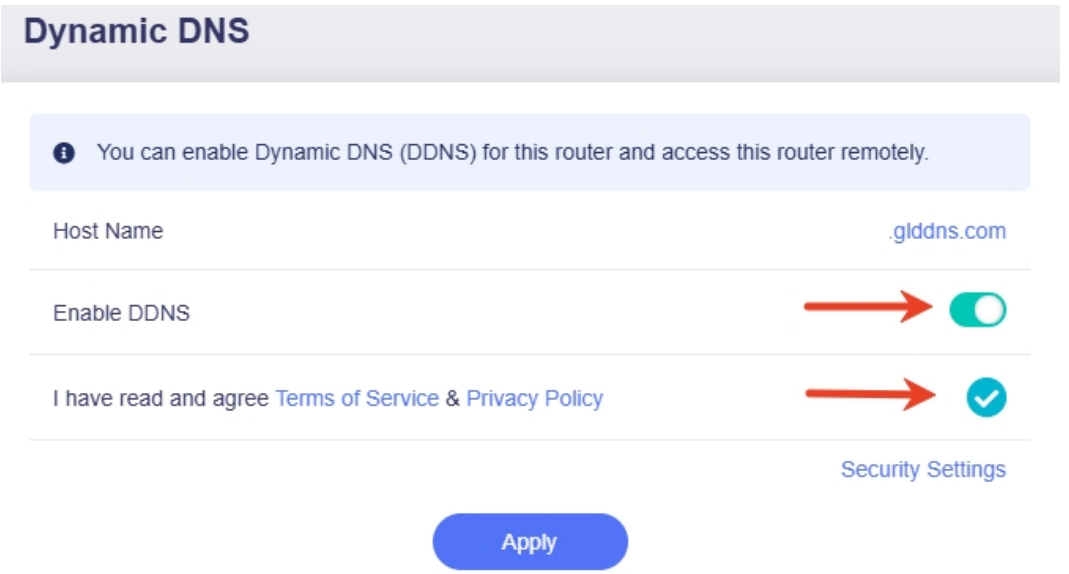
Luego podrá acceder al enrutador's panel de administración web usando DDNS host nombre sobre **HTTPS**.

15.2.4 Acceso remoto SSH

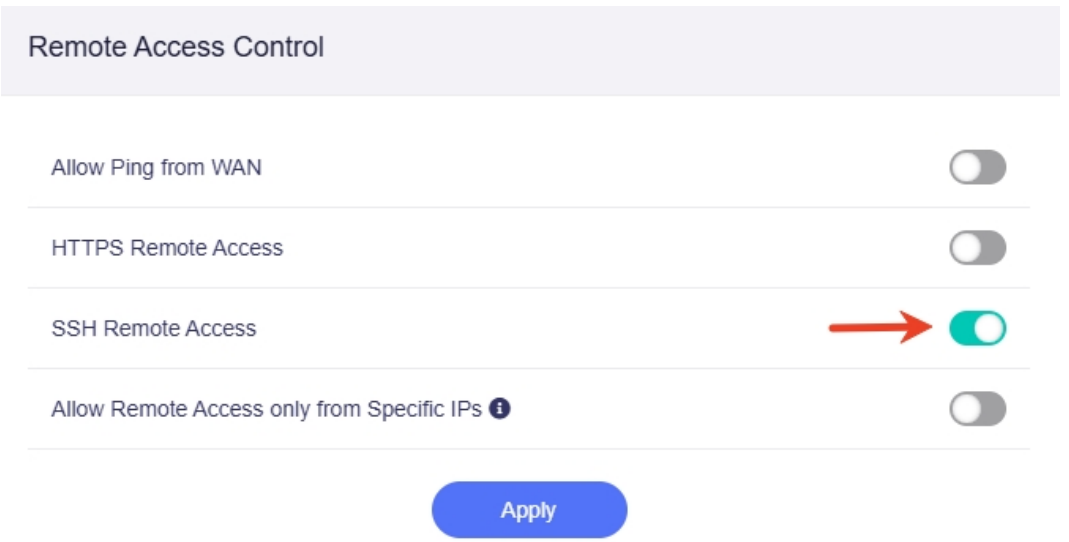
Se requiere una **Dirección IP pública** para el acceso remoto SSH.Consulte aquí tpara verificar si su ISP le asigna una dirección IP pública. Si su enrutador está detrás de NAT, configure el reenvío de puertos (**puerto 22**) en el enrutador ascendente para SSH remoto acceso.

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

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



2. En el panel de administración web, vaya a **SECURITY** > **Acceso de administrador** > **Control de acceso remoto**. Habilite **Acceso remoto SSH** y haga clic en **Aplicar**.



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

15.3 Almacenamiento en red

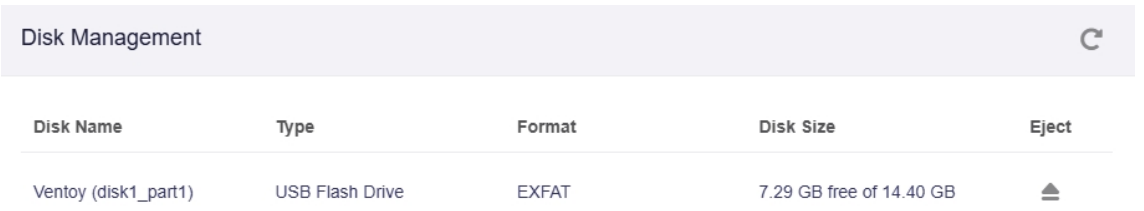
El almacenamiento en red permite compartir archivos de forma inalámbrica entre dispositivos conectando una unidad USB o una tarjeta SD a su enrutador. El enrutador convierte el dispositivo de almacenamiento en una unidad de red compartida, accesible para todos los dispositivos conectados a Wi-Fi.

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

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

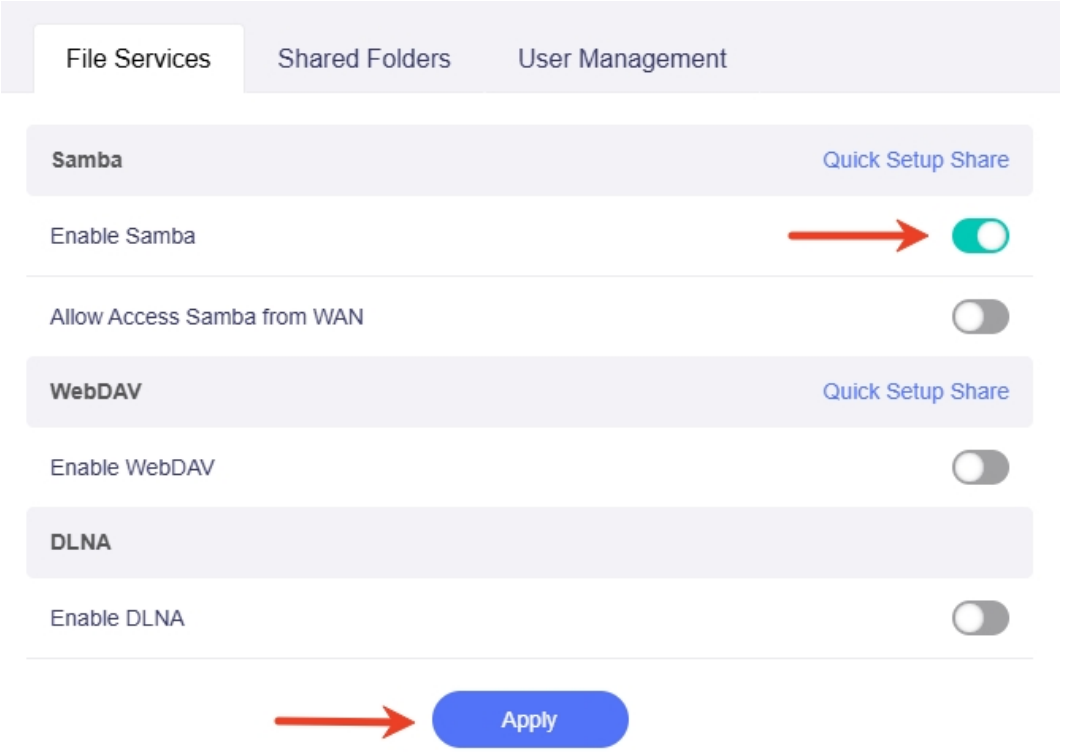
15.3.1 Conectar una unidad de almacenamiento

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



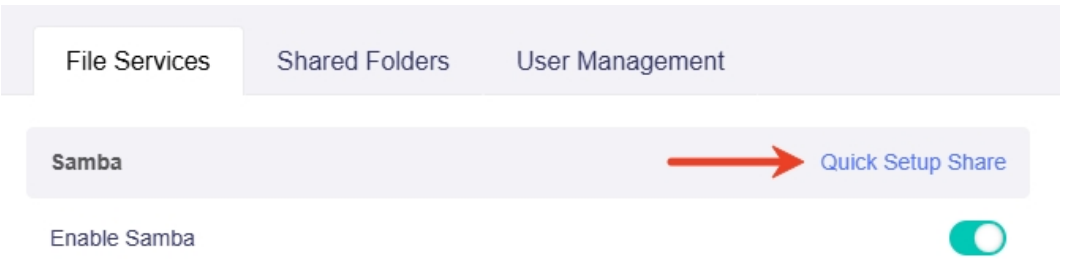
15.3.2 Configurar Samba

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

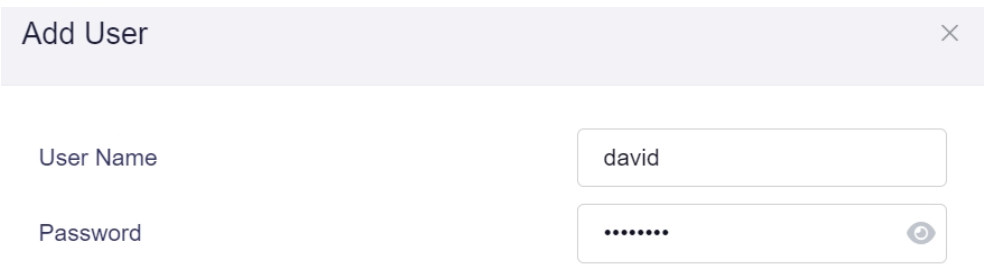


- **Permitir acceso a Samba desde WAN**: habilítela si desea que los dispositivos ascendentes accedan al servicio Samba.

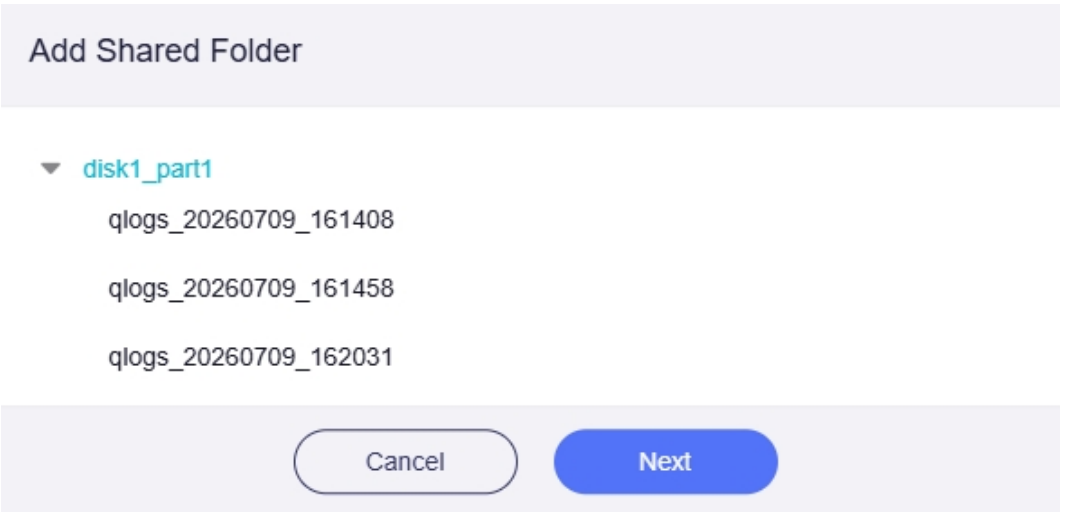
2. Haga clic en **Configuración rápida compartida** para establecer el enlace compartido.



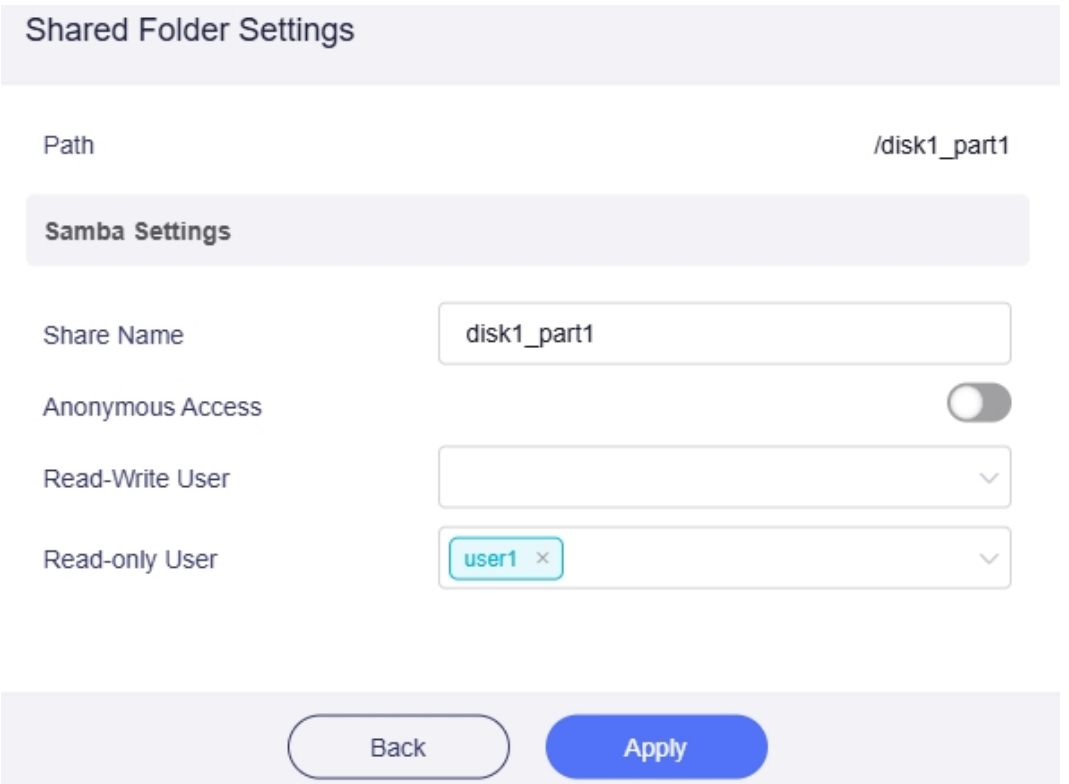
3. Agregue un usuario y haga clic en **Siguiente**. Este paso se omitirá si ya tienes una cuenta.



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

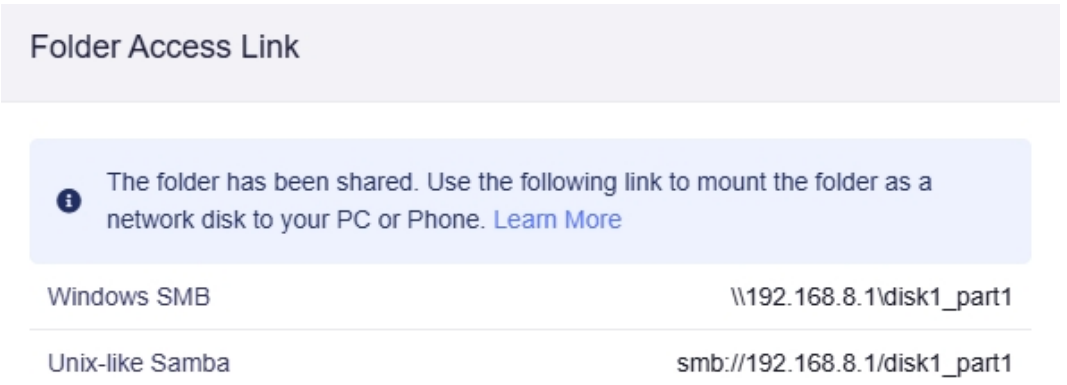


5. Configura la carpeta compartida s.
   Tel usuario creado en el paso anterior se agregará a **Usuario de solo lectura** de forma predeterminada. Si desea esto usuario para poder escribir o eliminar archivos, eliminelo de Usuario de solo lectura y agréguelo a **Lectura-Escritura Usuario**, luegoluego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



Consejo: Por razones de seguridad, no se recomienda habilitar Anónimo Acceso.

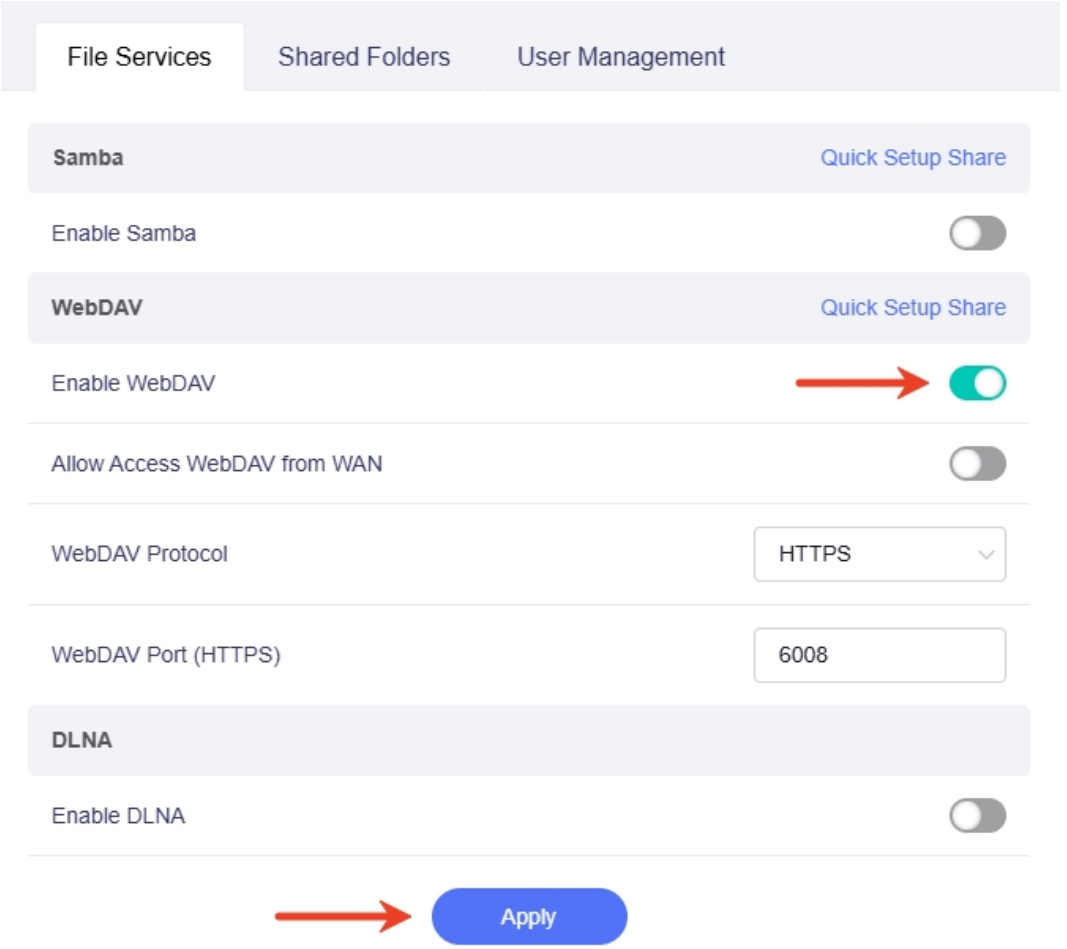
6. Obtenga el enlace de acceso a la carpeta
   La página mostrará el enlaces para Windows y sistemas operativos tipo Unix. El sistema tipo Unix incluyes Android, iOS, macOS, Ubuntu, etc. Ahora puedes acceder a tu carpeta compartida a través de Samba servicio a través de estos enlaces.



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

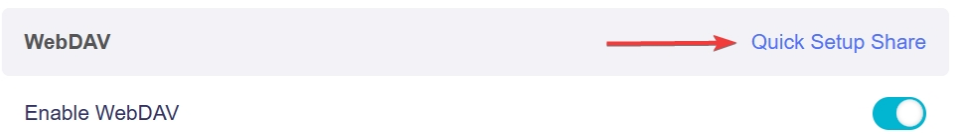
15.3.3 Configurar WebDAV

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

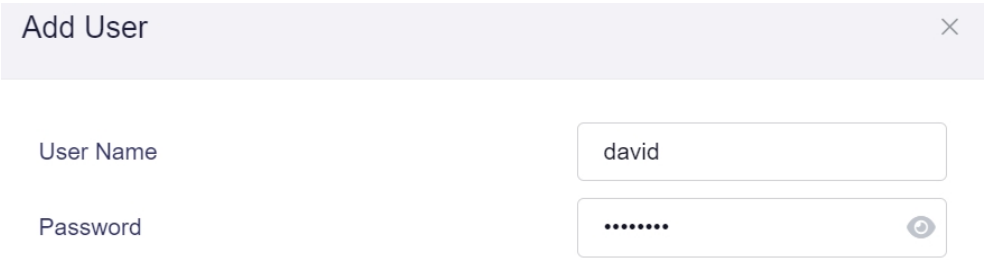


- **Permitir acceso a WebDAV desde WAN**: habilitar it si desea que los dispositivos ascendentes accedan al servicio WebDAV.
- **Protocolo WebDAV**: HTTP no está cifrado; úselo bajo su propia responsabilidad. HTTPS está cifrado y utiliza certificado autofirmado.
- **Puerto WebDAV**: no es necesario modificar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

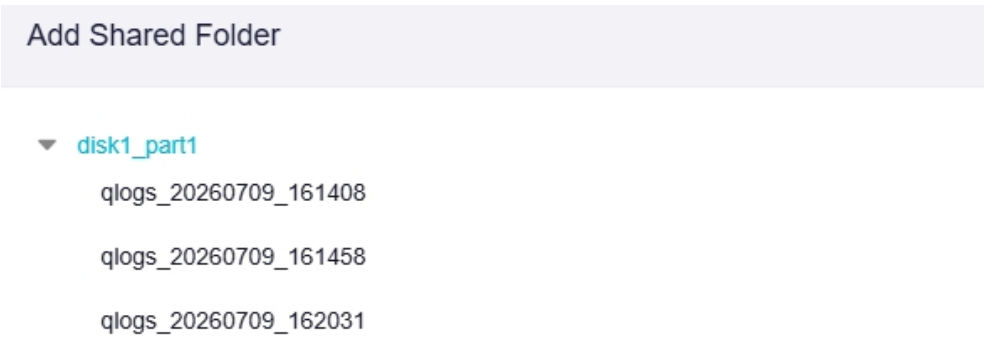
2. Haga clic en **Configuración rápida Compartir** con sconfigura el enlace compartido.



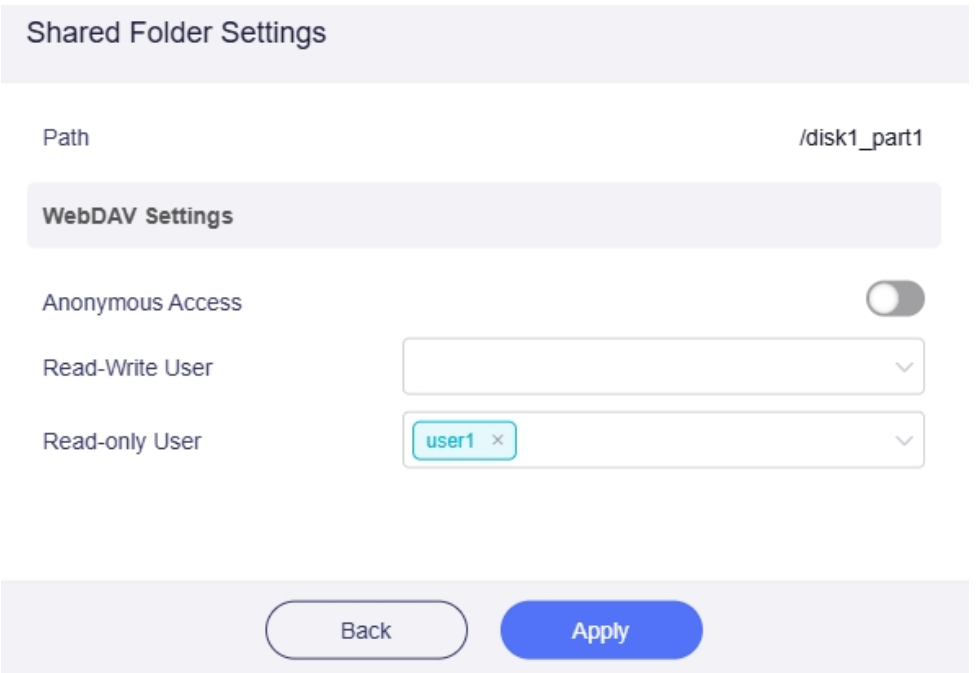
3. Agrega un usuario y haz clic en **Siguiente**. Este paso se omitirá si ya tiene una cuenta.



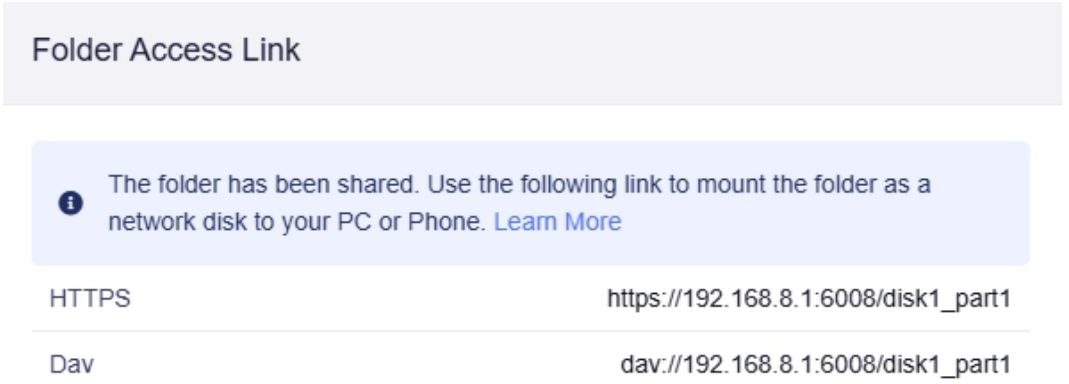
4. Haga clic en el ícono del triángulo para mostrar todas las carpetas. Sseleccione una carpeta para compartir. Sisi desea compartir el completo disco, haga clic en el nombre del disco (por ejemplo, disk1_part1).



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



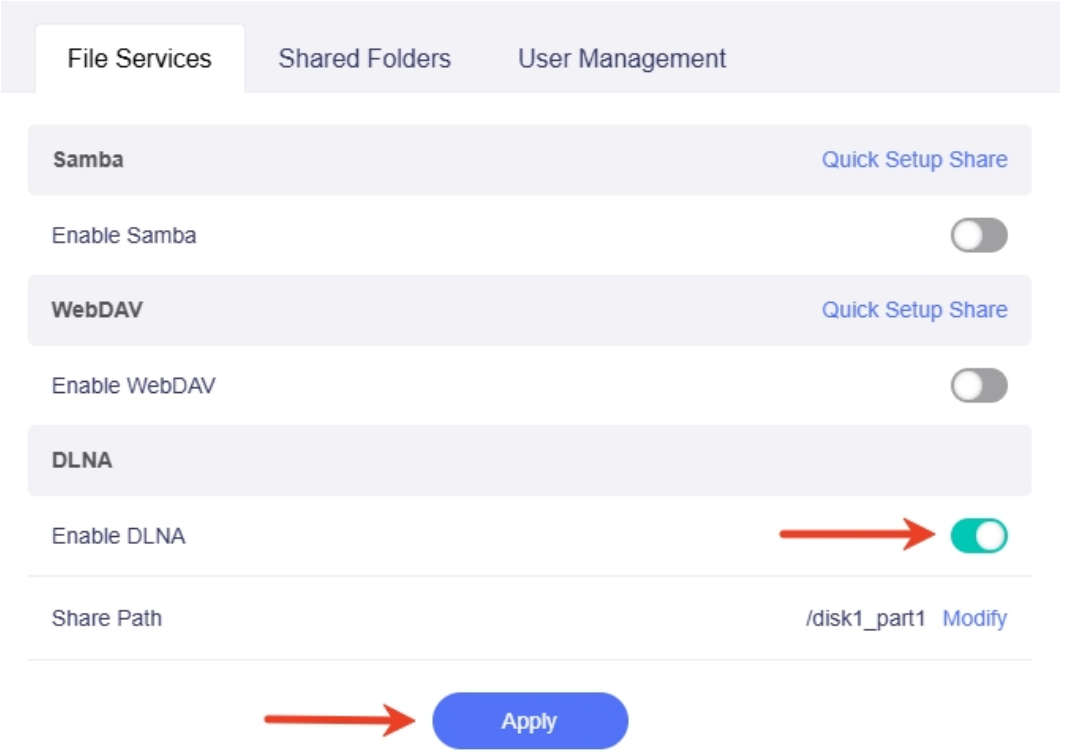
6. Obtener el enlace de acceso a la carpeta.
   La página mostrará el enlaces para Windows y sistemas operativos tipo Unix. Los sistemas tipo Unix incluyens Android, iOS, macOS, Ubuntu, etc. Ahora puede acceder a su carpeta compartida a través del servicio WebDAV a través de estos enlaces.



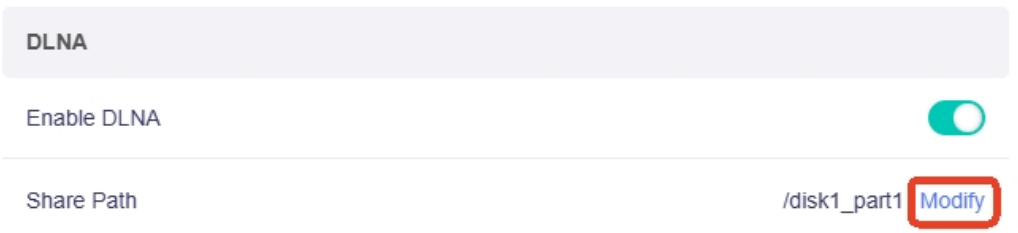
Nota: si habilita **Permitir acceso WebDAV desde WAN** y acceda la carpeta compartida de red ascendente, reemplace la IP del enrutador (predeterminada: 192.168.8.1) en el enlace de acceso con su enrutador's WAN IP, que se puede encontrar en la página INTERNET del panel de administración web.

15.3.4 Configurar DLNA

1. En el **Servicios de archivos**, active **Eactivable DLNA**, y haga clic en **Aplicar**.



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



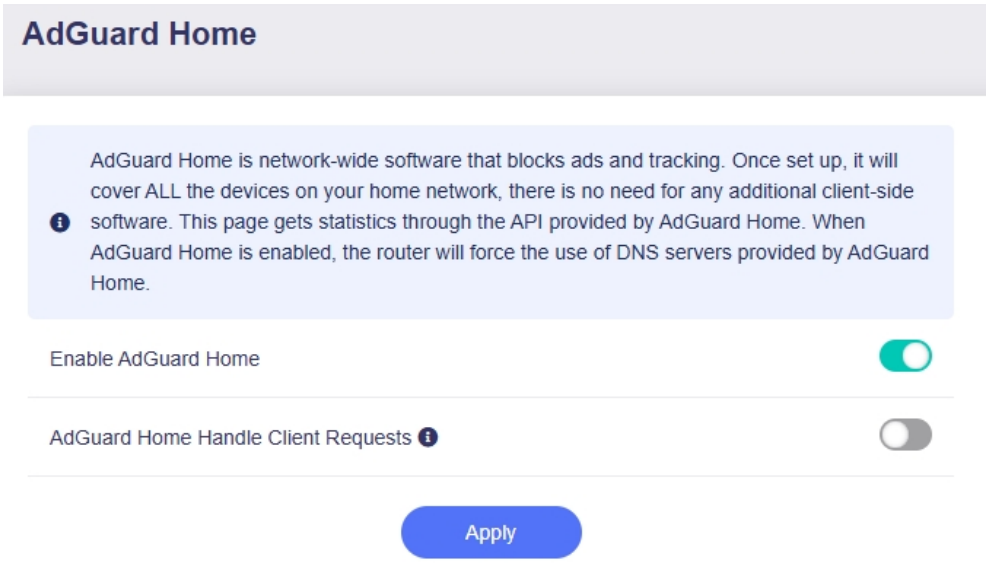
3. Conecte su televisor inteligente al enrutador. encontrará el DLNA sservidor automáticamente.

15.4 AdGuard Home

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

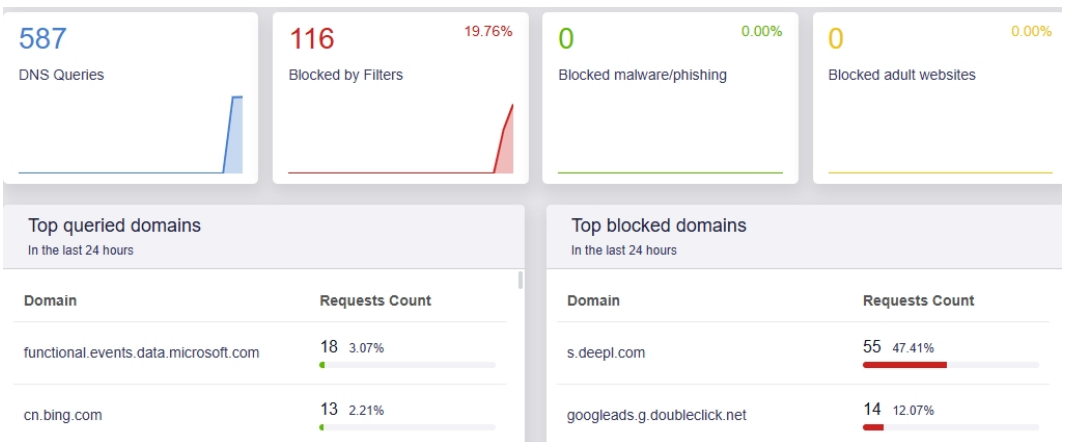
Siga estos pasos para configurar AdGuard Home.

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

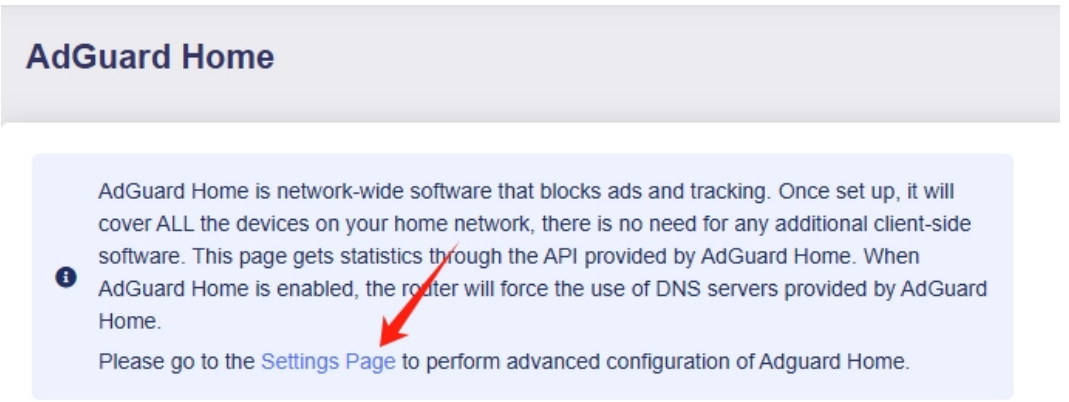


- **Inicio de AdGuard Gestionars solicitudes de clientes**: si está habilitado, las consultas de DNS de los dispositivos cliente serán manejadas directamente por AdGuard Home, pero esto hará que las políticas de VPN basadas en dominios fallen.

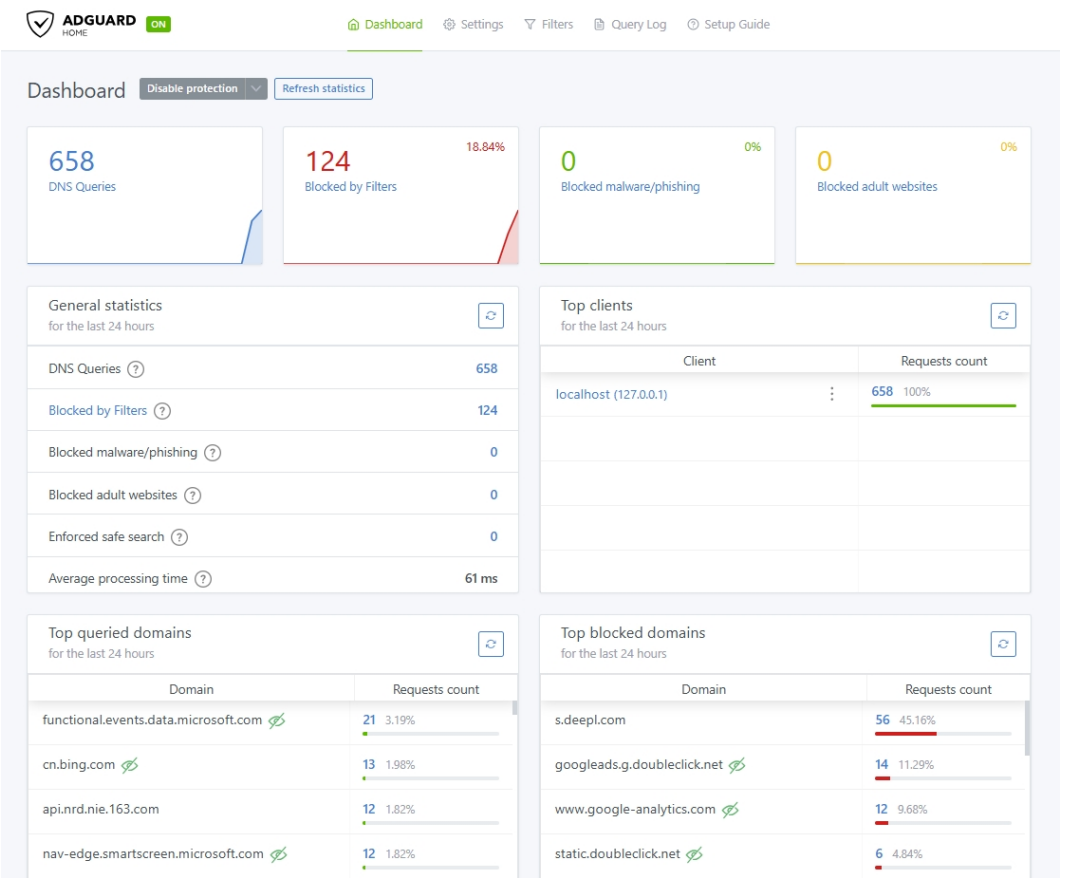
2. La página cargará automáticamente estadísticas de DNS (consultas, bloqueadas) dominios, etc.) a través de la API proporcionada por AdGuard Home.



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



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



15.5 Bark

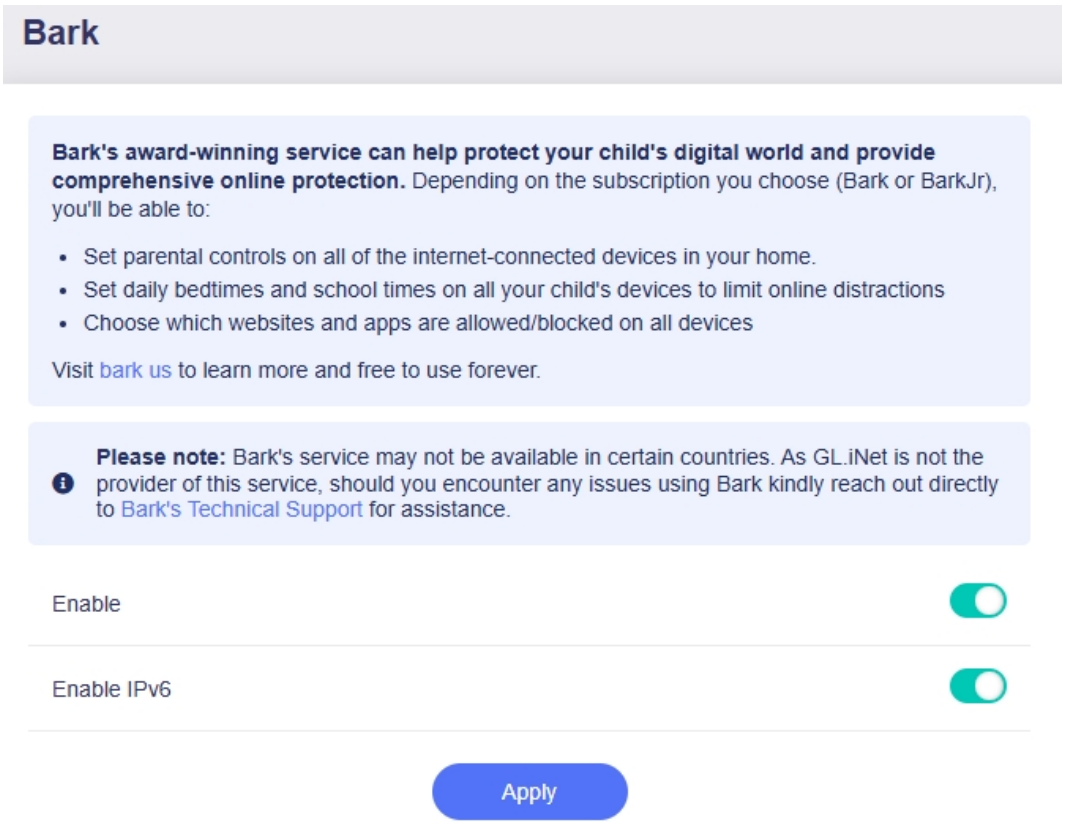
El servicio Bark puede ayudar a proteger el mundo digital de su hijo y brindarle una protección en línea integral. Por lo general, requiere una suscripción paga. Sin embargo, como parte de nuestra asociación con Bark, GL.iNet ofrece el plan Bark Home de forma gratuita **en determinados modelos de enrutador incluido Flint 3**, lo que proporciona monitoreo avanzado y alertas sin costo adicional.

Nota:

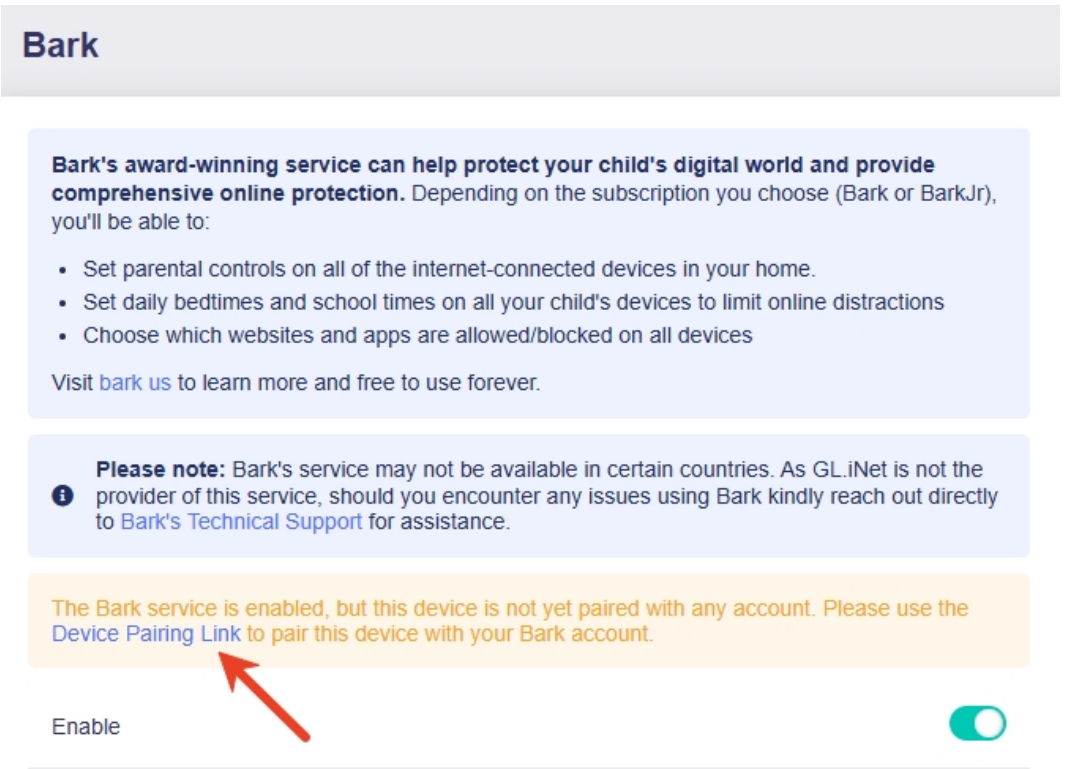
1. El servicio Bark está disponible **solo en Estados Unidos, Australia y Sudáfrica**. Haga clic aquí para obtener más detalles.
2. Bark y GL.iNet Parental Control no se pueden habilitar simultáneamente, ya que esto puede desencadenar conflictos.

Siga estos pasos para use el servicio Bark si es necesario.

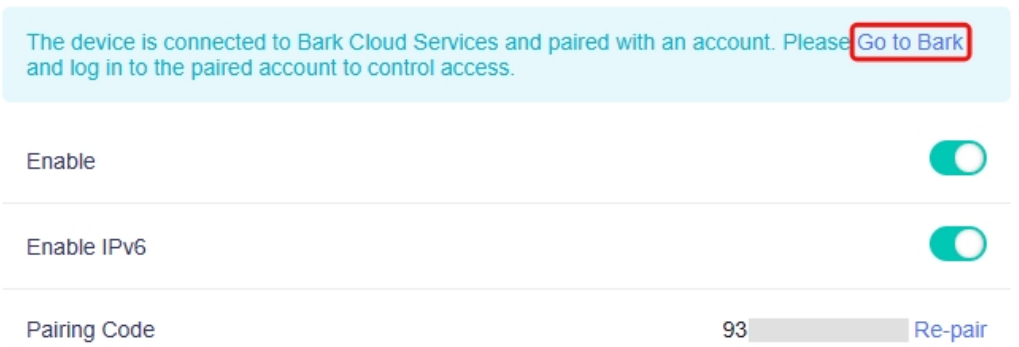
1. Inicie sesión en el panel de administración web del enrutador y navegue hasta **APLICACIONES** -> **Bark**. Active el interruptor para habilitar Bark y luego haga clic en **Aplicar**.



2. A continuación, vincule su dispositivo con su cuenta de Bark. Haga clic en **Enlace de emparejamiento de dispositivos** para emparejar este enrutador con su cuenta de Bark.



3. Será redirigido al sitio web de Bark. Siga las instrucciones en pantalla para iniciar sesión, vincular su dispositivo, crear un perfil y finalizar la configuración inicial.
4. Una vez que su dispositivo se conecte a los servicios de Bark Cloud y esté vinculado con su cuenta, el panel de administración web del enrutador mostrará un hipervínculo. Haga clic en **Vaya a Bark** para iniciar sesión en el panel de Bark y configurar sus reglas de control parental.



Nota: Dado que GL.iNet no es el proveedor de este servicio, si encuentra algún problema al usar Bark, comuníquese directamente con Soporte técnico de Bark para obtener ayuda.

15.6 Tailscale

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

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

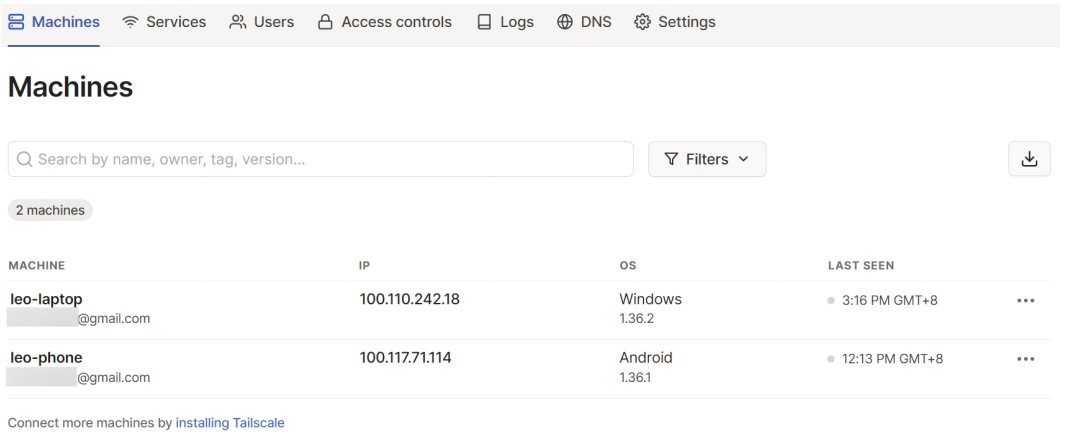
Nota:

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

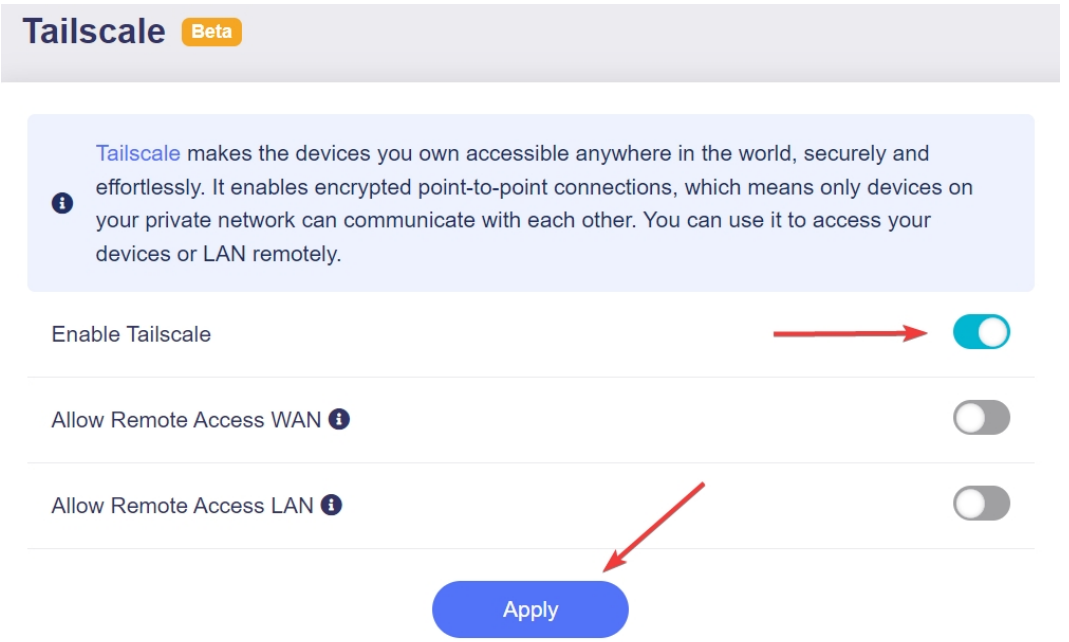
15.6.1 Configurar Tailscale

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

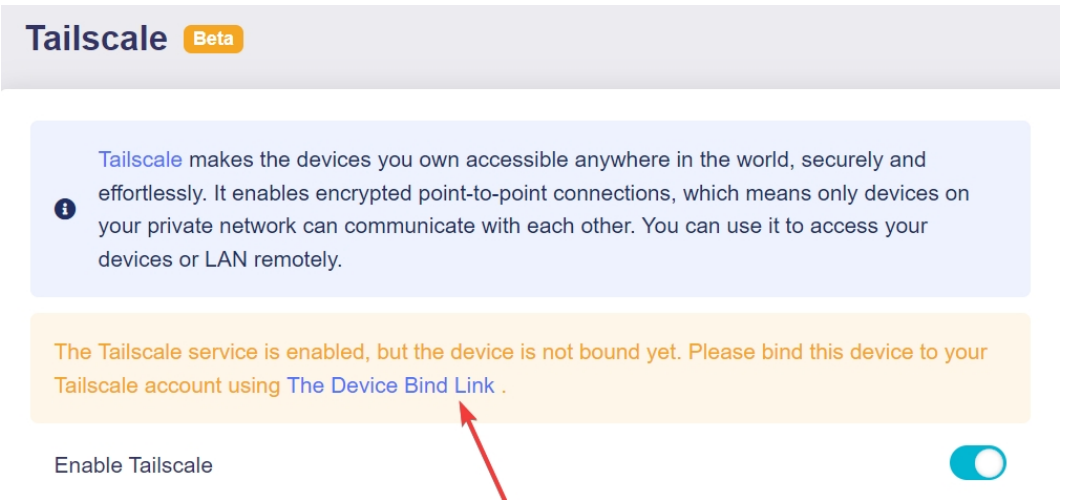
1. Rregistre primero una cuenta de Tailscale y vincule una o dos dispositivos a su cuenta de Tailscale parao fines de prueba. Después de vincular, verá sus dispositivos en la plantilla Tailscale C.



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



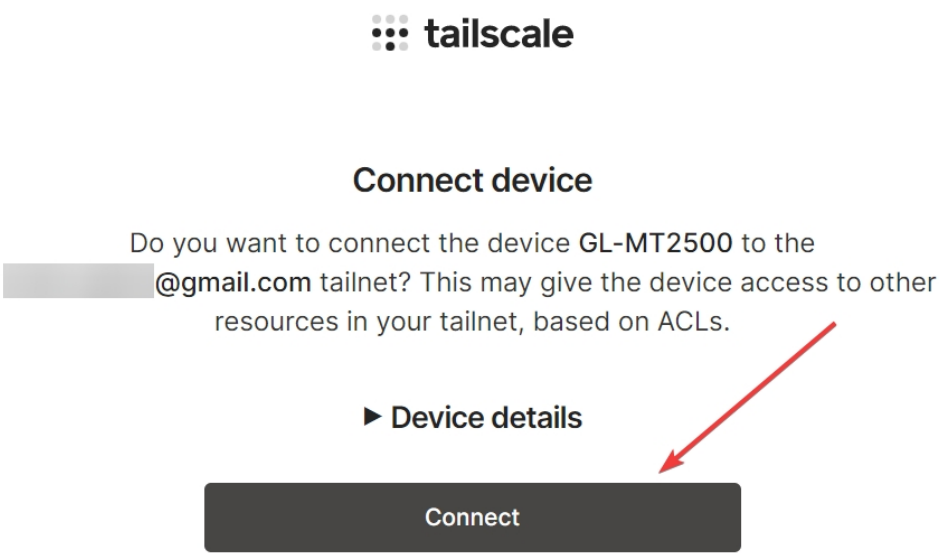
3. La página le pedirá que vincula el dispositivo. Haga clic en **Enlace de vinculación del dispositivo**.



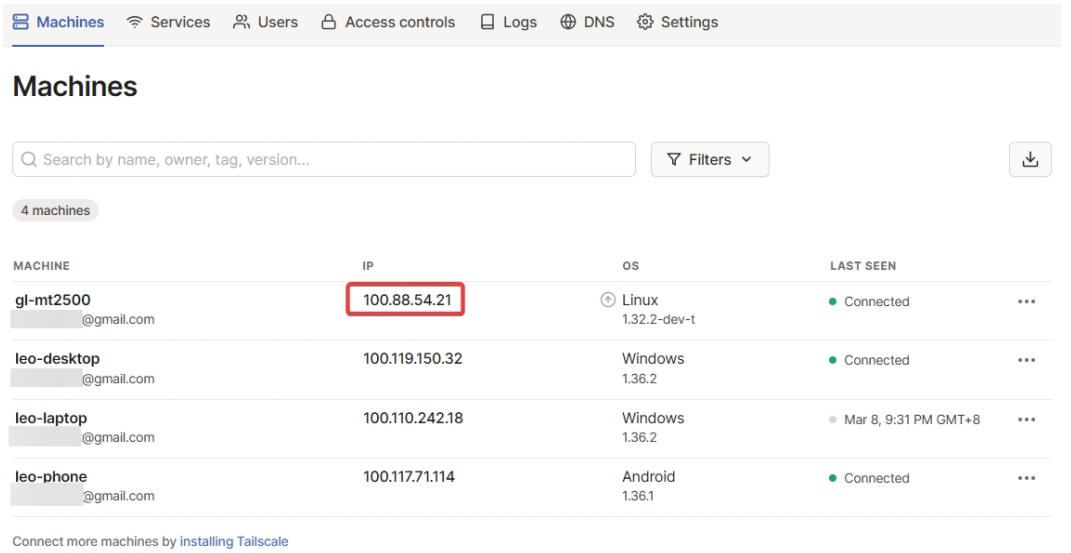
4. En la ventana emergente , haga clic en el enlace y registre en con su cuenta de Tailscale.



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



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

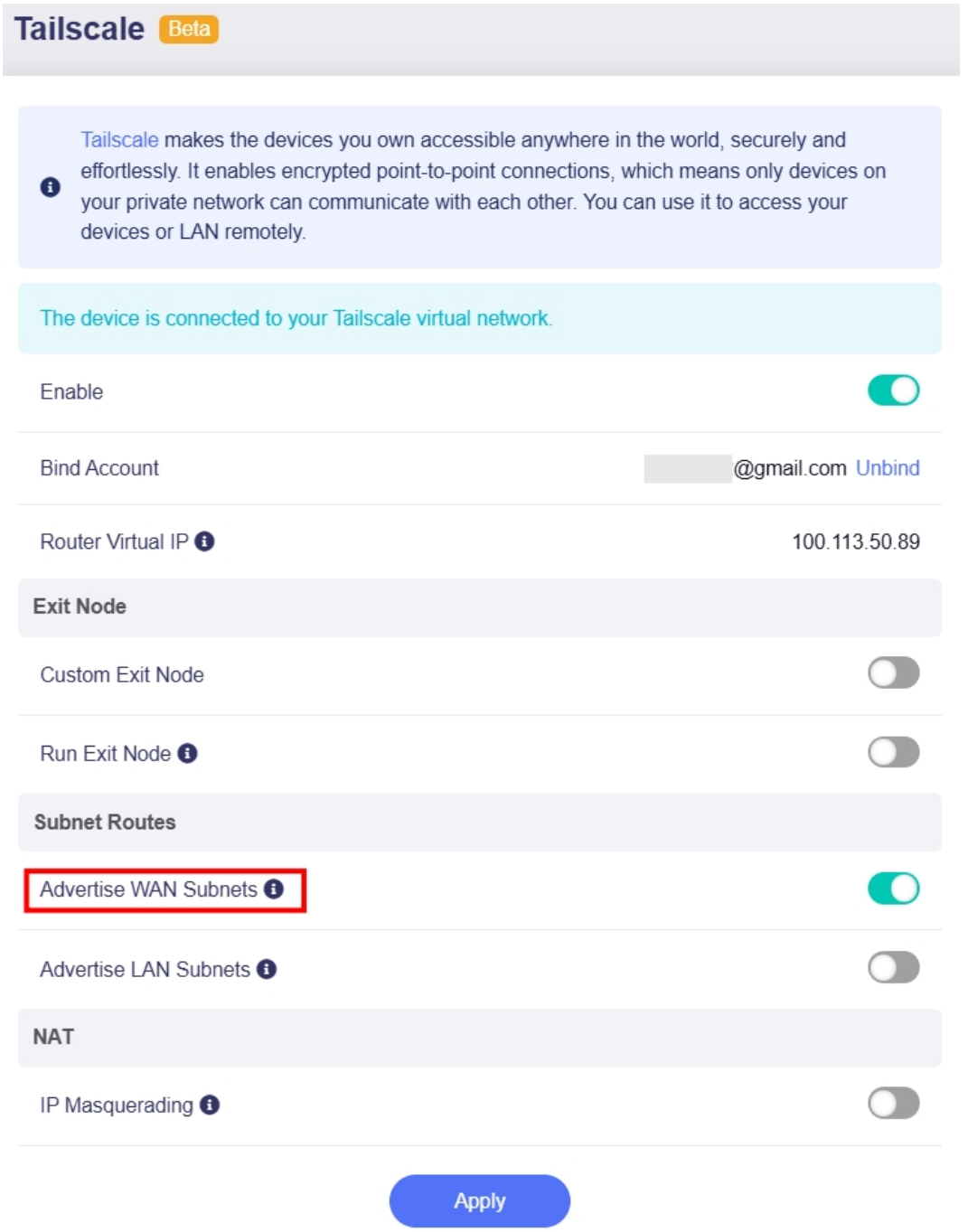


7. Pruebe la conectividad.

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

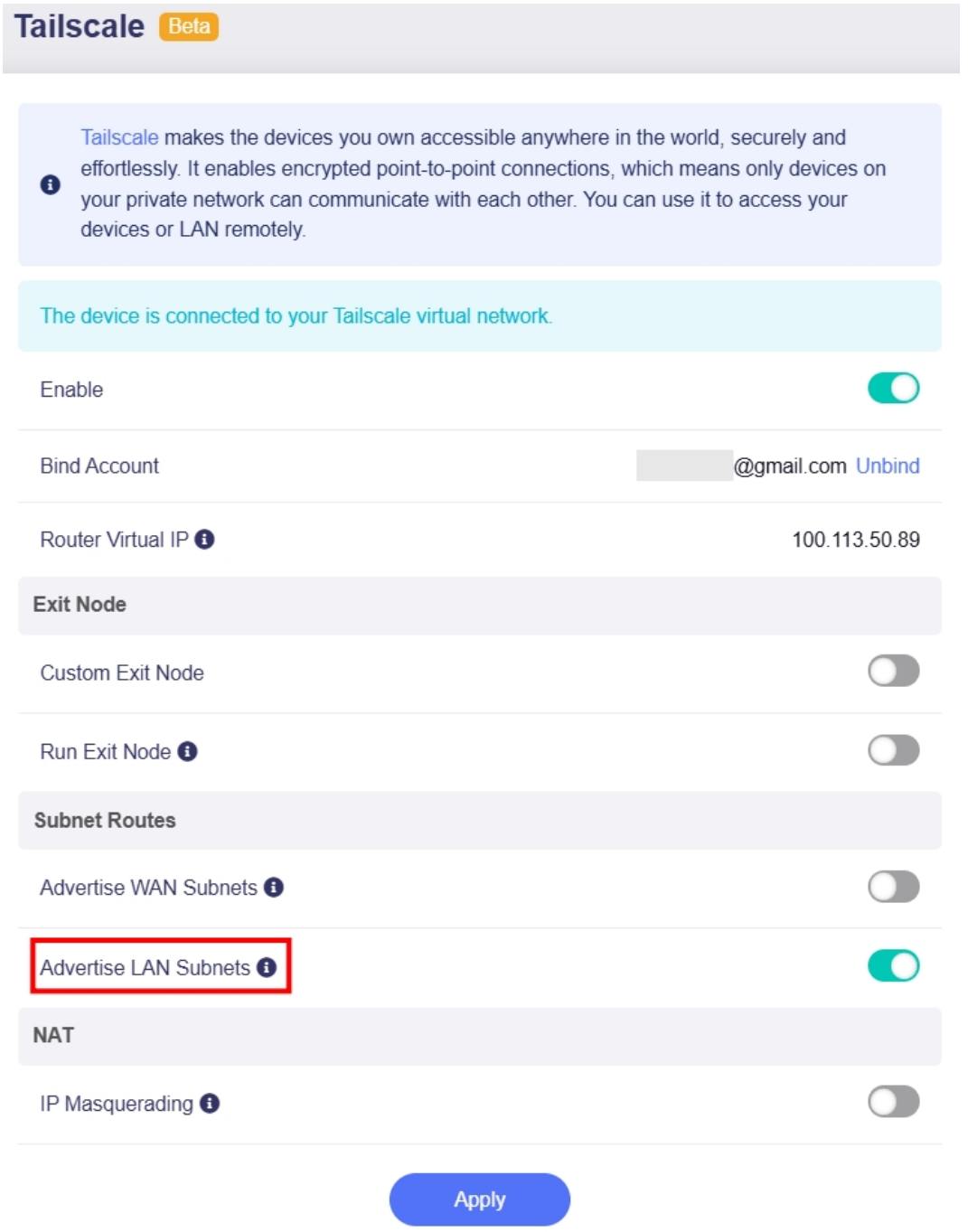
15.6.2 Anunciar subredes WAN

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



15.6.3 Anunciar subredes LAN

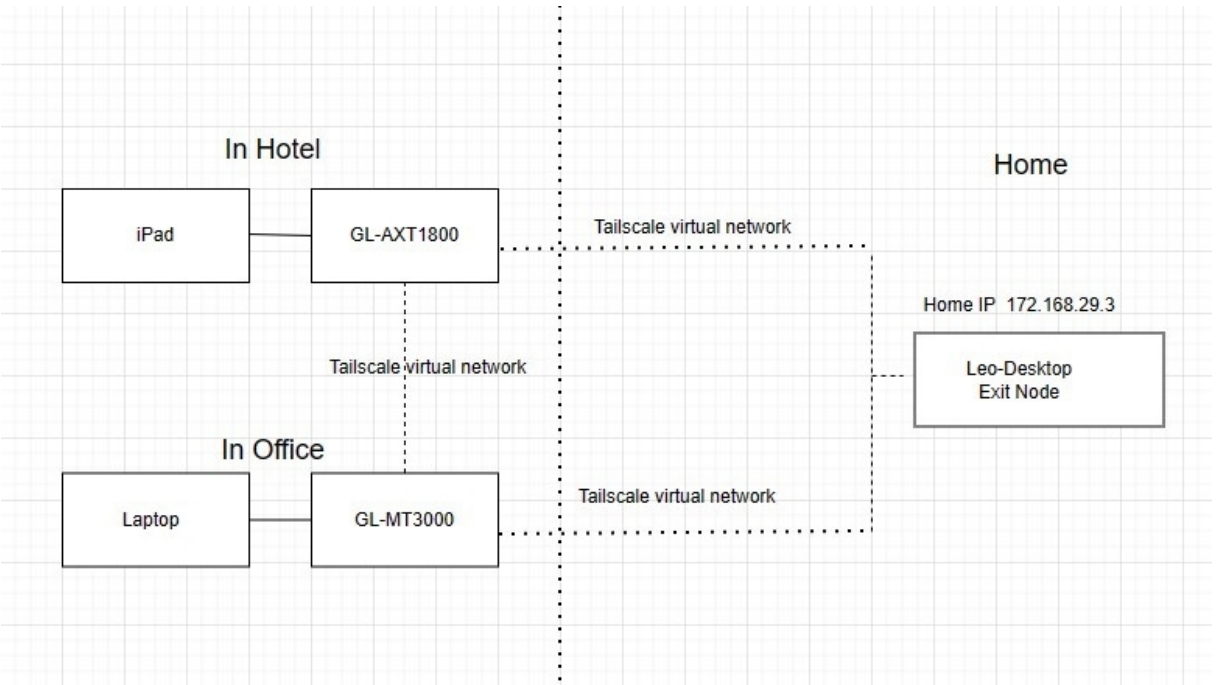
Si esta opción está habilitada, se puede acceder a los recursos en el lado LAN del dispositivo a través de la red virtual Tailscale. Consulte aquí para obtener más detalles.



15.6.4 Nodos de salida personalizados

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

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



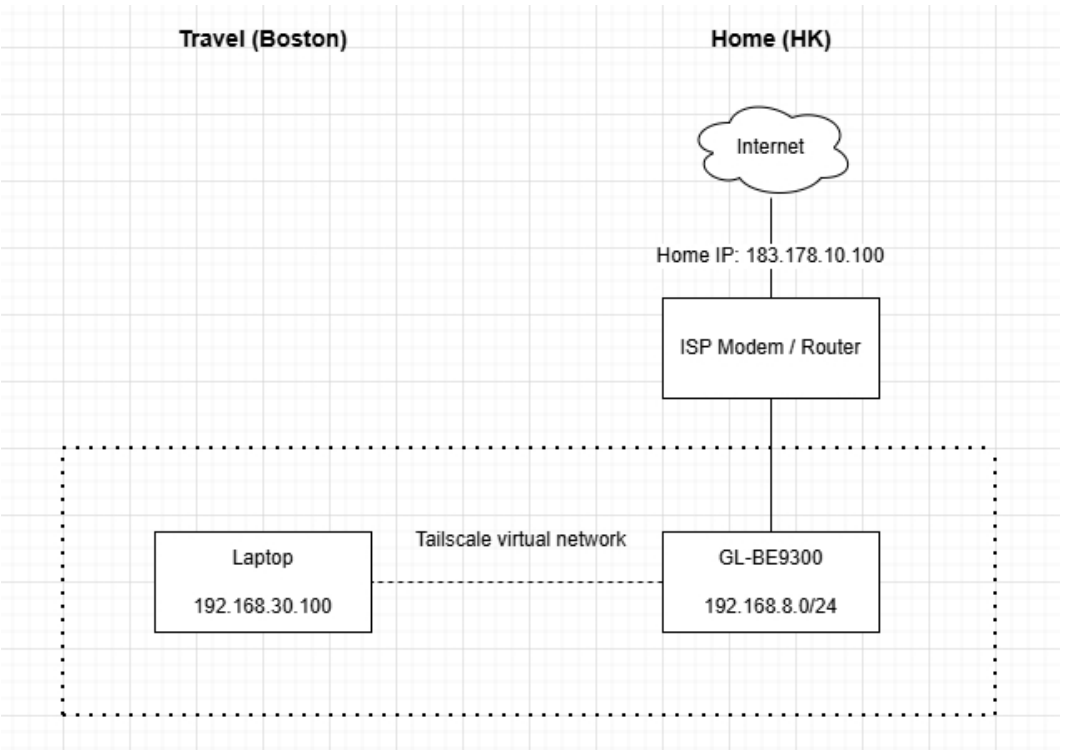
En resumen, un nodo de salida enruta el tráfico de Internet saliente desde sus dispositivos Tailnet, actuando efectivamente como servidores VPN. Cuando se conecta a un nodo de salida, todo su tráfico de Internet que no es de Tailscale parece originarse desde su ubicación, lo que le ayuda a acceder a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

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

15.6.5 Activar el nodo de salida

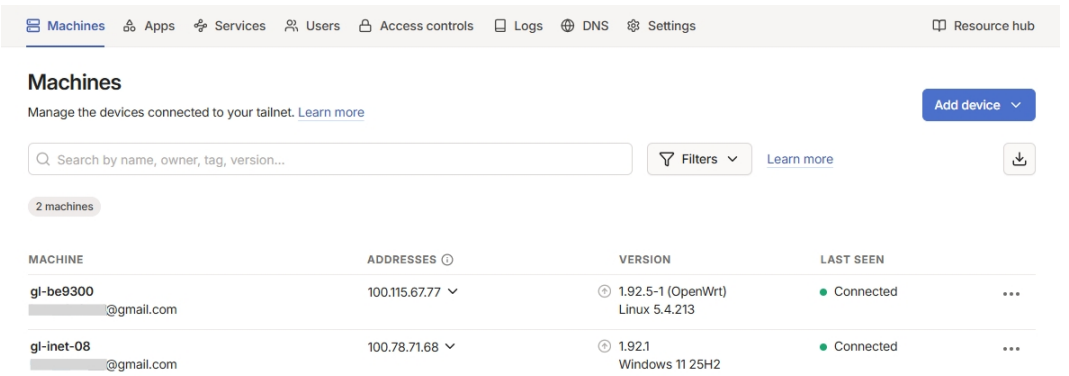
La ejecución de un nodo de salida en su enrutador permite que otros dispositivos dentro de su tailnet enruten todo el tráfico de Internet saliente a través de la IP pública de este enrutador.

En la topología siguiente, una computadora portátil está en Boston, mientras que un enrutador GL-BE9300 está en Hong Kong. Ambos se han agregado a la misma red Tailscale. Si configura el GL-BE9300 como nodo de salida, todo el tráfico saliente de la computadora portátil saldrá a través de este enrutador para acceder a Internet, y la IP pública de la computadora portátil se resolverá en una dirección IP de Hong Kong en lugar de una de Boston.

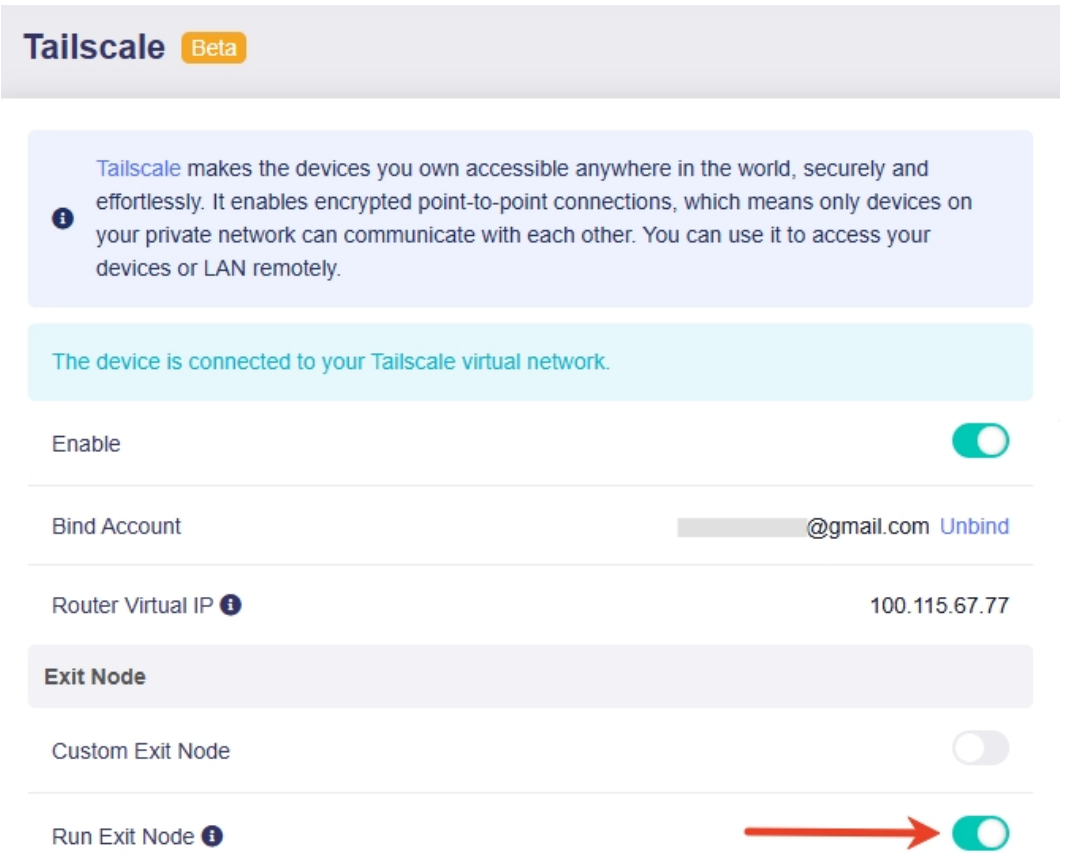


Estos son los pasos para configurar el GL-BE9300 como un nodo de salida.

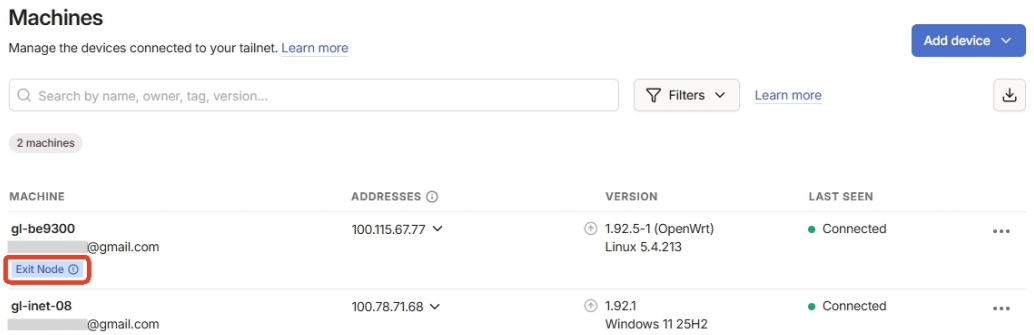
1. Inscriba ambos enrutadores GL-BE9300 y computadora portátil de viaje a la misma red trasera de Tailscale.



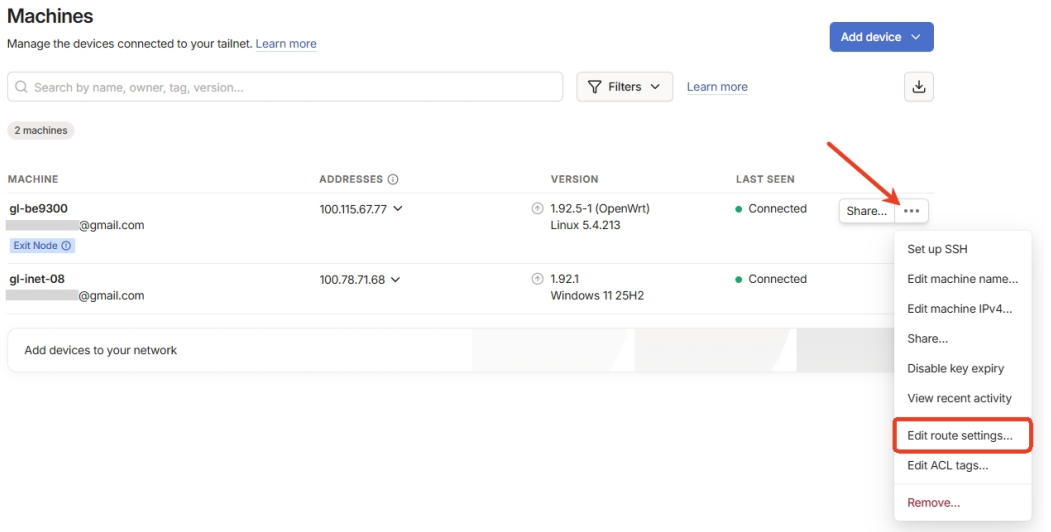
2. En el panel de administración web GL-BE9300, vaya a **APLICACIONES** > **Tailscale**. habilite **Activar el nodo de salida** y haga clic en **Aplicar**.



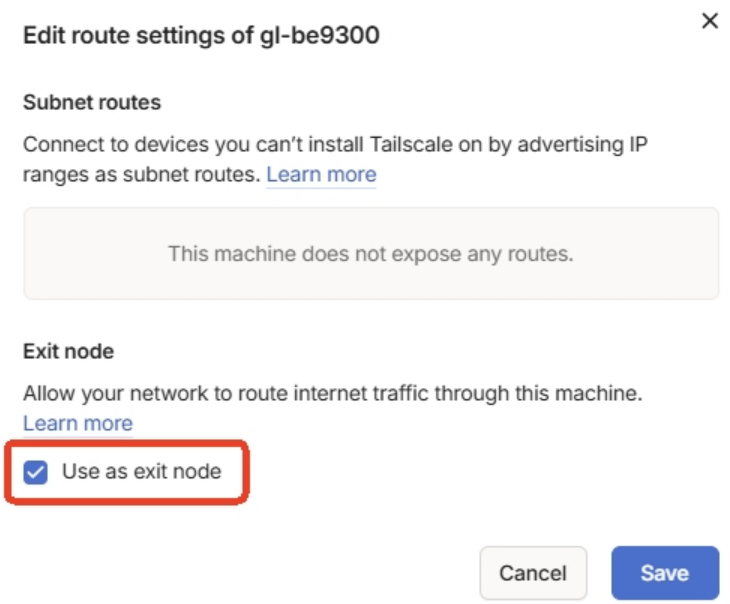
3. Vaya a la consola de administración de Tailscale y verá una etiqueta "Nodo de salida" debajo de GL-BE9300.



4. Haga clic en el icono de tres puntos a la derecha de GL-BE9300 y seleccione **Editar configuración de ruta**.



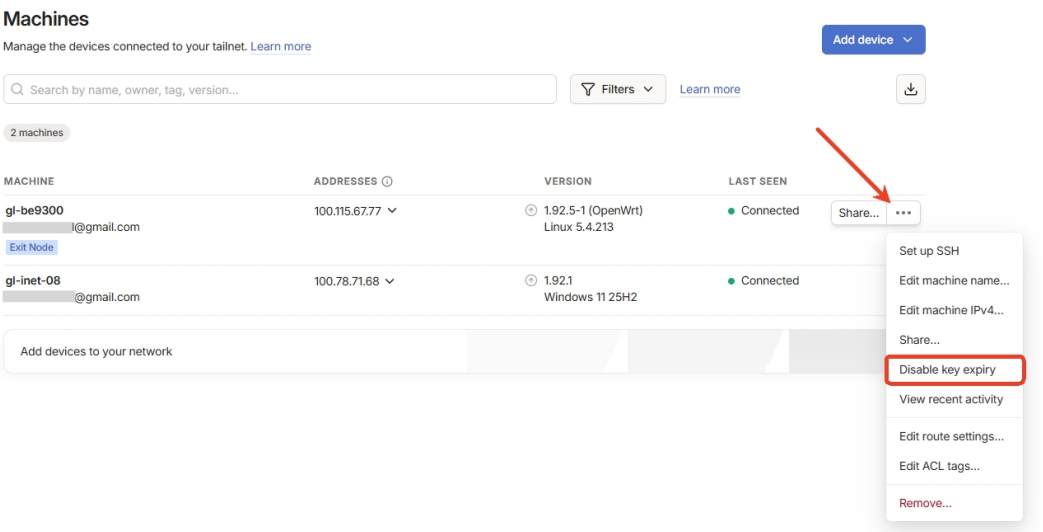
5. En la ventana emergente, marque **Usar como nodo de salida** y haga clic en **Guardar**.



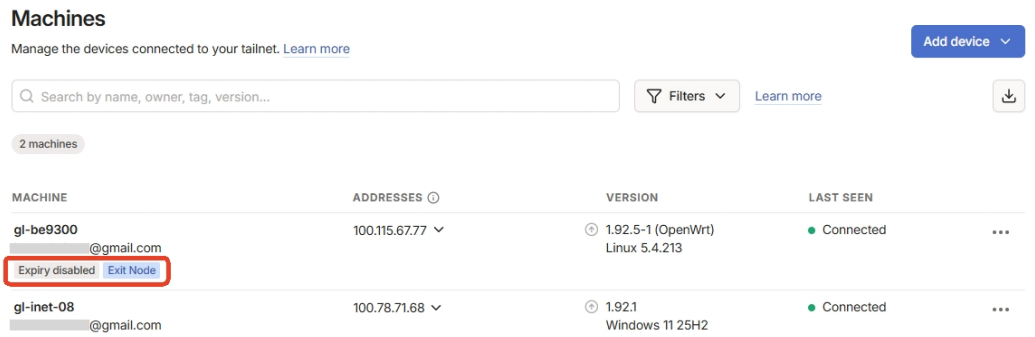
6. Desactivar la caducidad de la clave.

   Como característica de seguridad, los usuarios deben volver a autenticarse periódicamente en cada uno de sus dispositivos. Para evitar desconexiones cuando caduque la clave de autenticación del nodo de salida, recomendamos deshabilitar la caducidad de la clave para su nodo de salida. Haga clic aquí para obtener más detalles sobre la caducidad de la clave.

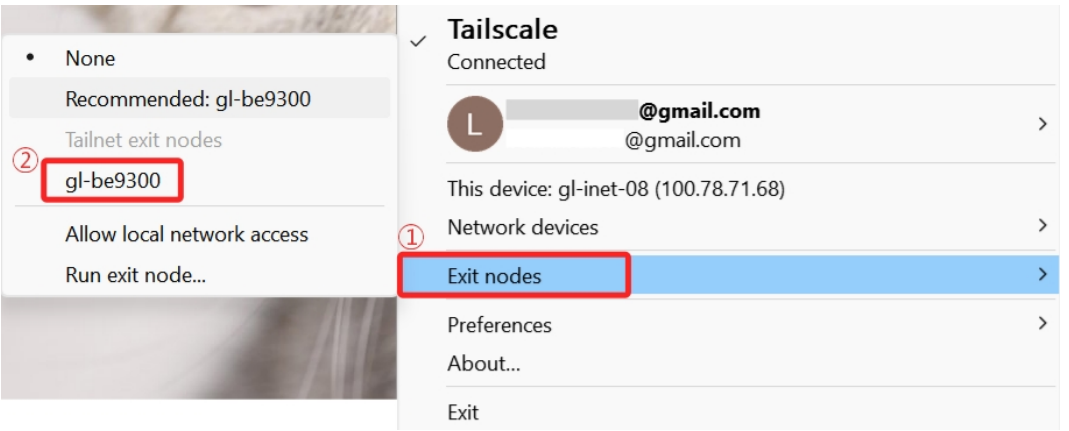
   Haga clic en el icono de tres puntos a la derecha del GL-BE9300 y seleccione Desactivar caducidad de la clave.



Una vez aplicada, aparecerá una etiqueta "Caducidad" deshabilitado" aparecerá debajo de GL-BE9300.



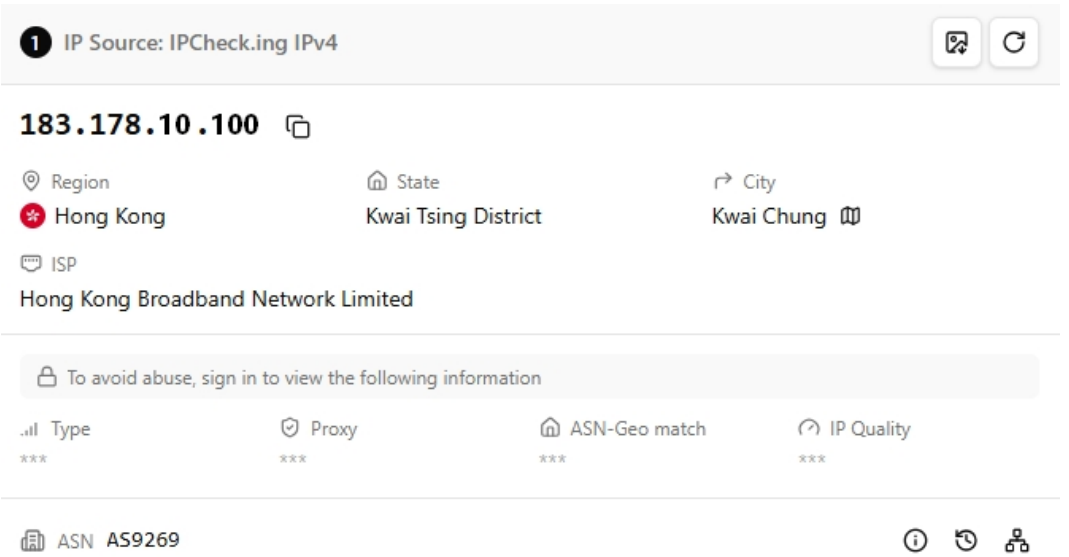
7. Ejecute Tailscale en su computadora portátil de viaje. El icono de Tailscale aparecerá en la bandeja del sistema en la esquina inferior derecha. Haga clic con el botón derecho en el icono, haga clic en **Salir de nodos** y seleccione **gl-be9300**.



Ahora, todo el tráfico saliente de esta computadora portátil de viaje saldrá a través de GL-BE9300 para acceder al Internet.

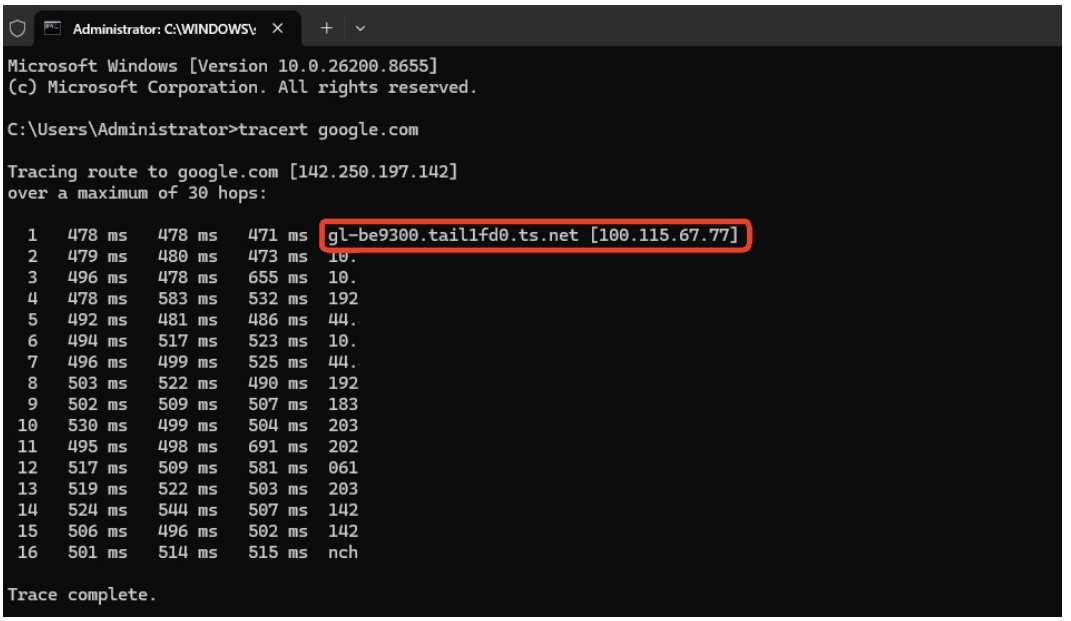
8. Pruebe la conectividad.

(1) En su computadora portátil de viaje, abra un navegador web y visite ipcheck.ing o cualquier otro sitio web de búsqueda de IP. La página mostrará la dirección IP pública que pertenece a su nodo de salida de Tailscale, lo que confirma que la computadora portátil está accediendo a Internet a través del nodo de salida (el GL-BE9300 ubicado en Hong Kong, en este ejemplo).

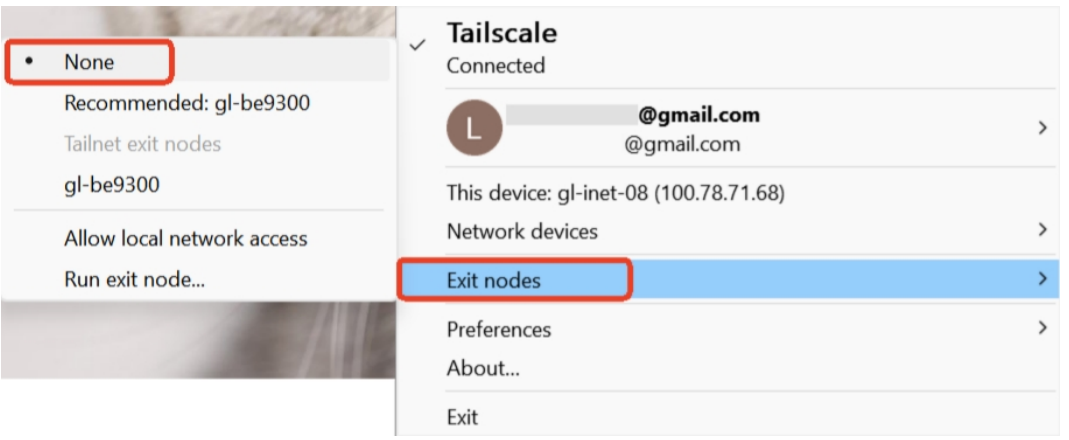


(2) Presione *Win+R*, escriba *cmd* para iniciar el símbolo del sistema y luego ejecute *tracert google.com* para rastrear las rutas de tráfico saliente. El resultado del comando enumera todos los saltos de enrutamiento para su tráfico de Internet. Si se configura correctamente, el primer salto externo se enrutará a través del nodo de salida,

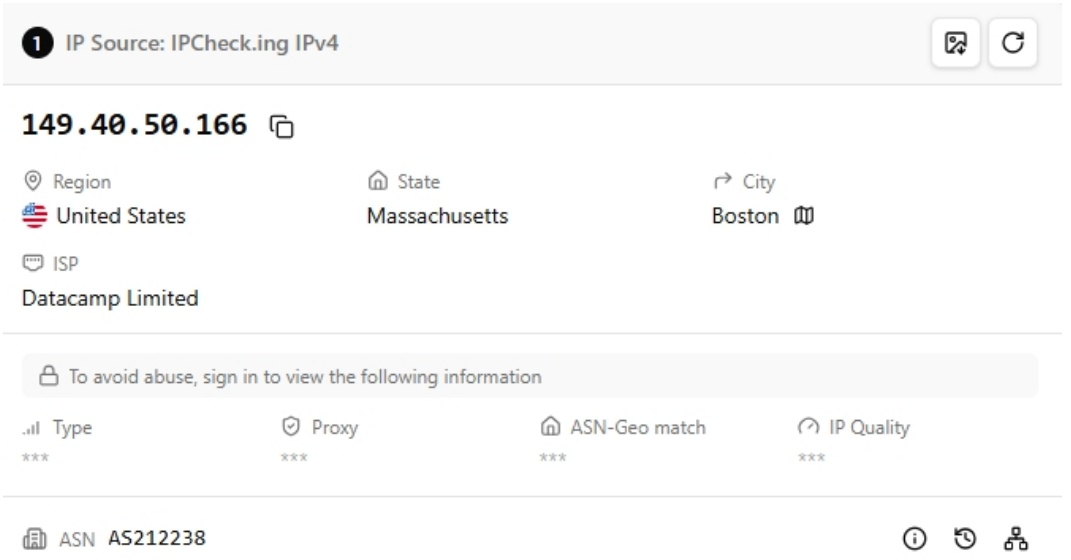
como se muestra a continuación, verificando todas las salidas del tráfico de Internet saliente a través de este enrutador.



(3) Desconecte el nodo de salida para una prueba comparativa. Haga clic con el botón derecho en el icono de Tailscale en la bandeja del sistema en la esquina inferior derecha, haga clic en **Nodos de salida** y luego seleccione **Ninguno** para dejar de usar el nodo de salida.



(4) Abra una nueva pestaña del navegador y visite ipcheck.ing o cualquier servicio de búsqueda de IP. Ahora mostrará la dirección IP pública nativa de su computadora portátil, lo que demuestra que el dispositivo está usando su conexión a Internet local (Boston, en este ejemplo).


1 IP Source: IPCheck.ing IPv4
149.40.50.166
Region
United States
State
Massachusetts
City
Boston
ISP
Datacamp Limited
To avoid abuse, sign in to view the following information
Type
***
Proxy
***
ASN-Geo match
***
IP Quality
***
ASN AS212238

15.7 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 mismo, así como a sus recursos WAN y LAN.

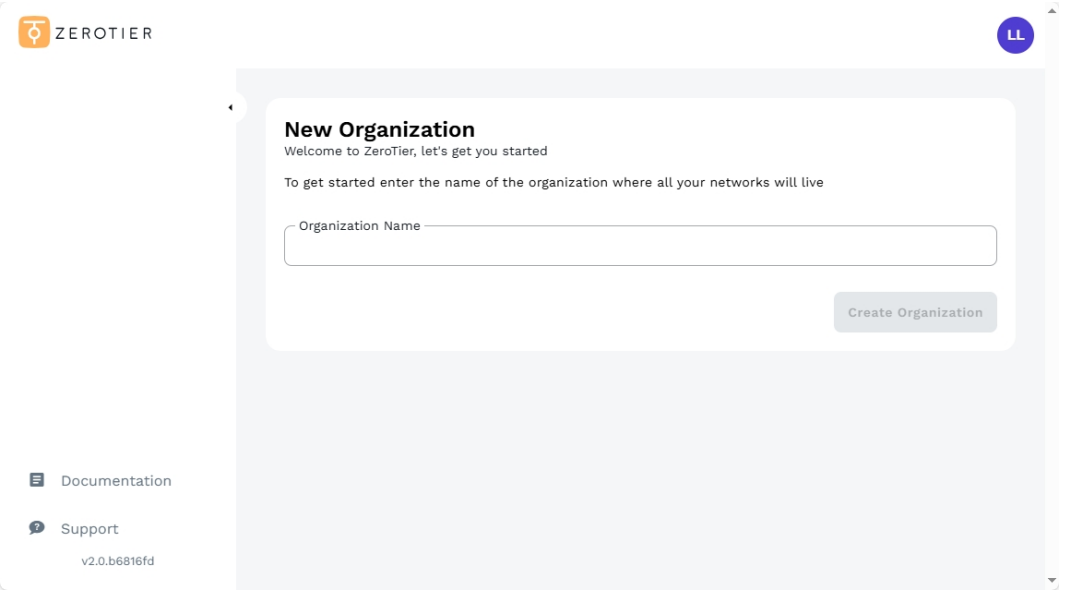
Nota:

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

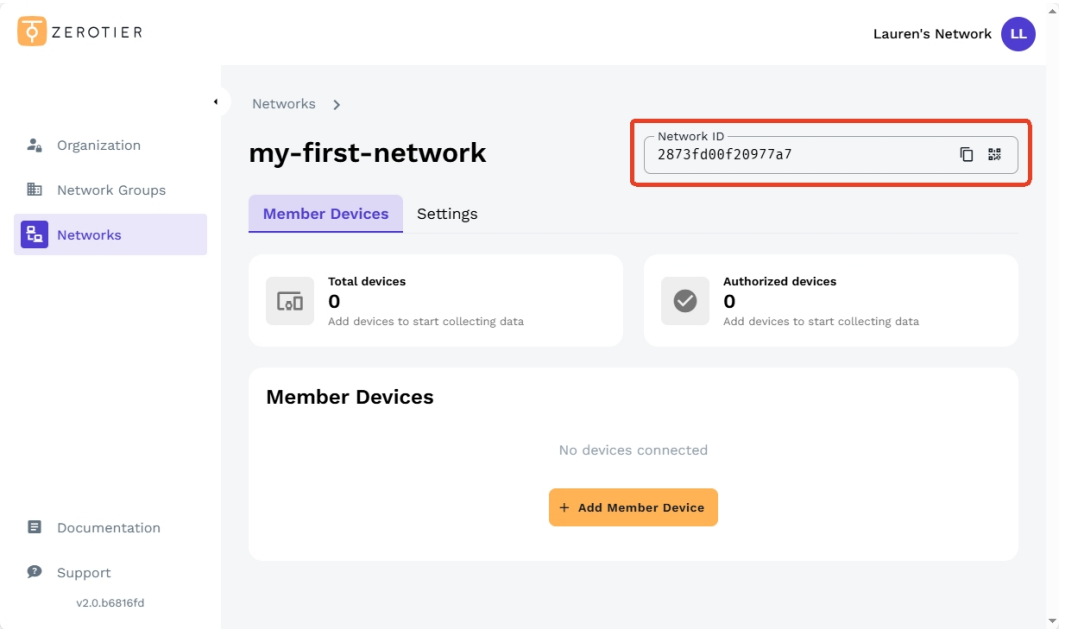
15.7.1 Configurar ZeroTier

Hay dos versiones de ZeroTier Central disponibles: New Central y Legacy Central. Los siguientes pasos utilizan New Central como ejemplo.

1. Visita Sitio web oficial de ZeroTier e inicia sesión con tu cuenta.
2. Crea una organización.

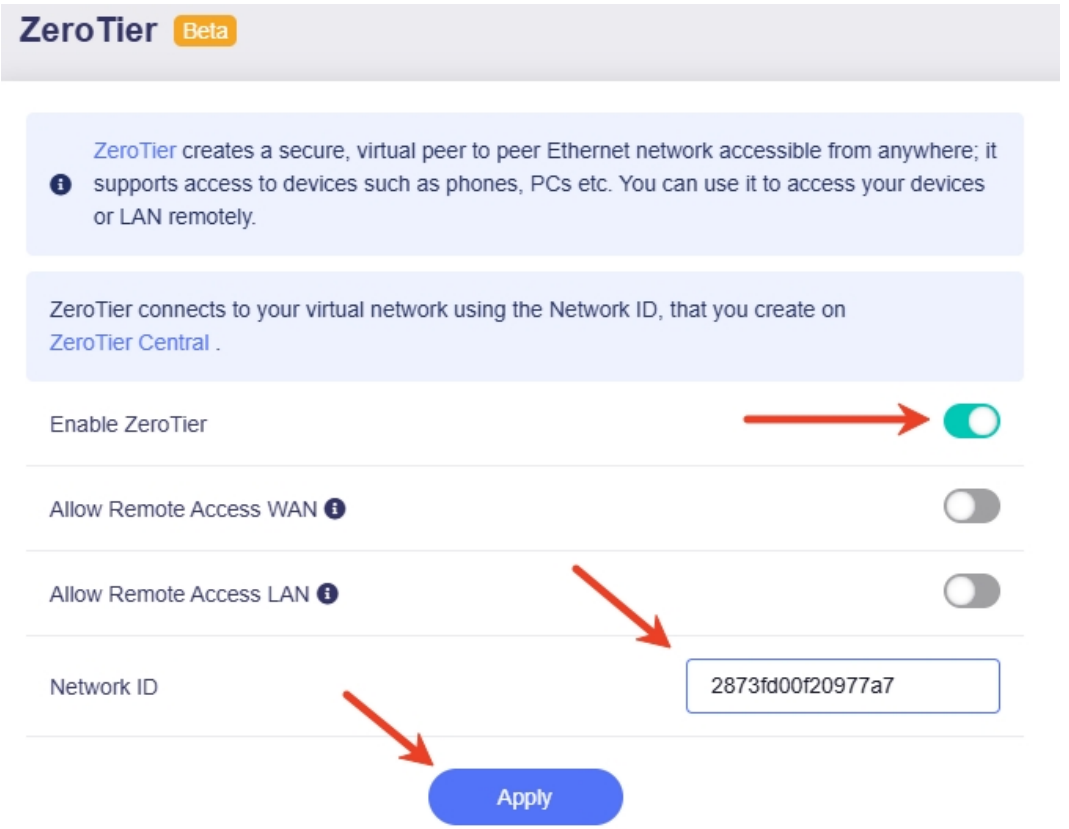


3. Seleccione un plan. Aquí elegimos **plan personal** como ejemplo, que incluye 10 dispositivos, 1 administrador de red y 1 red. Si necesita crear más redes, agregar más dispositivos o agregar rutas y DNS personalizados, elija otro plan pago.
4. Ahora se ha creado su red ZeroTier.

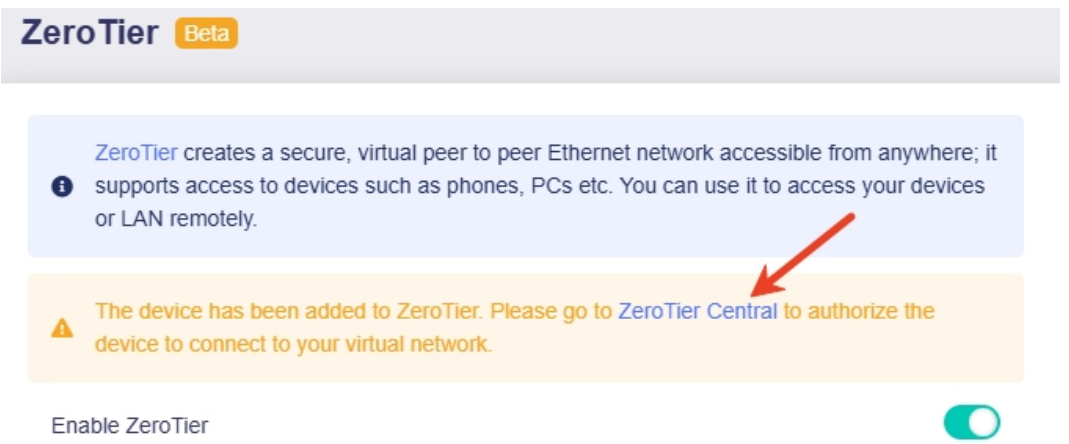


Tome nota del **ID de red**, que es una combinación alfanumérica de 16 caracteres en la esquina superior derecha, ya que será necesaria cuando conecte otros dispositivos más adelante.

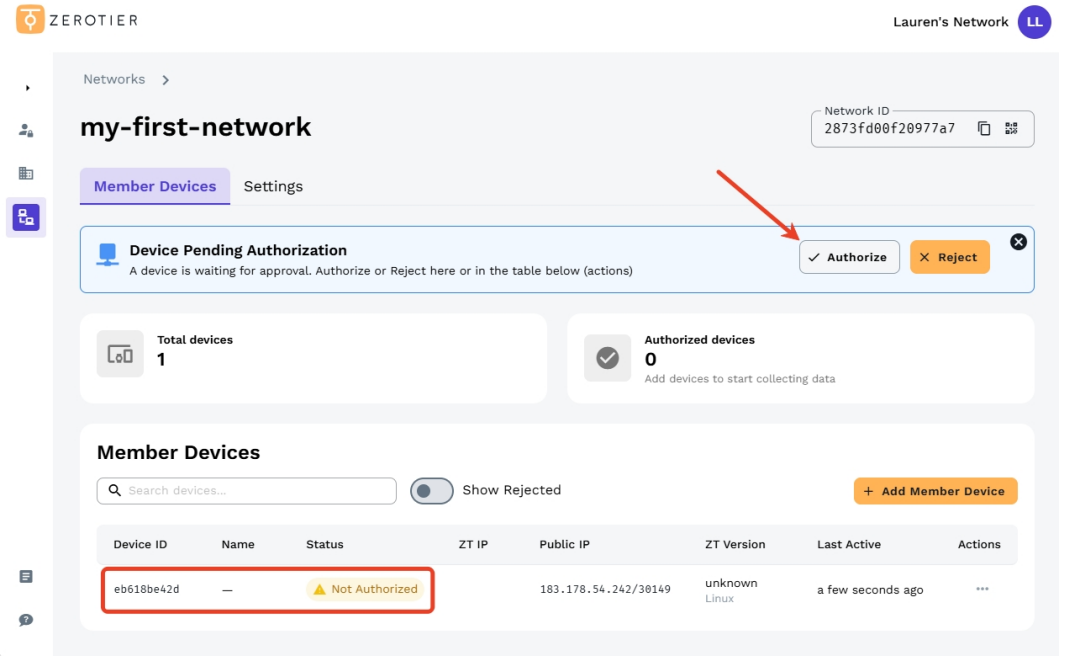
5. Inicie sesión en la web de su enrutador Panel de administración y navegue hasta **APLICACIONES** > **ZeroTier**. Habilite ZeroTier, ingrese el **ID de red**, luego haga clic en **Aplicar**.



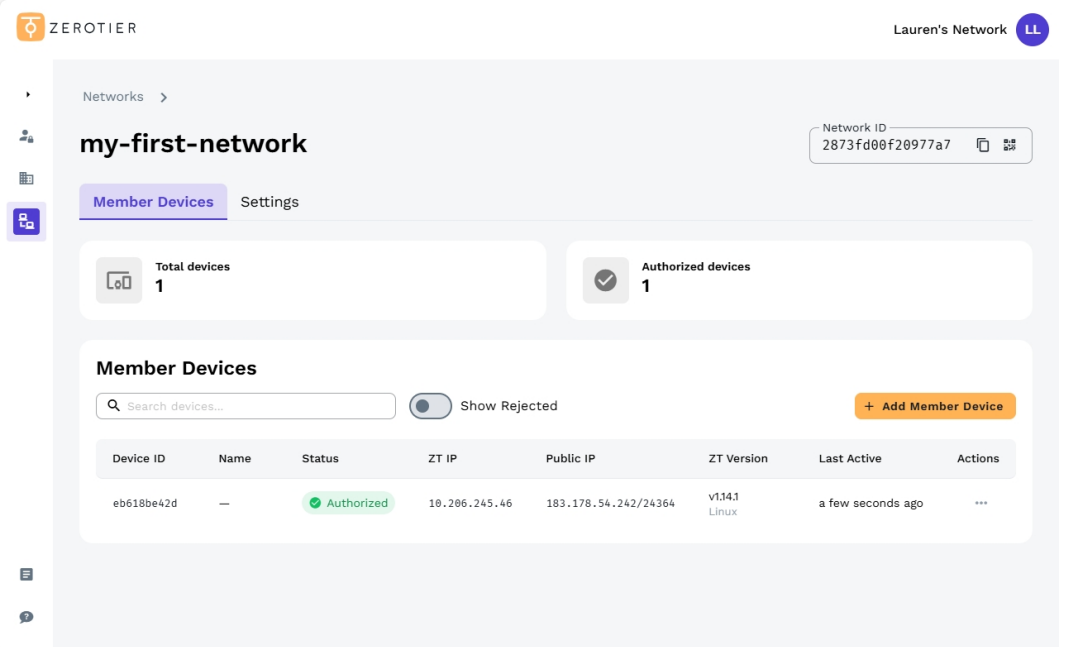
Después de un momento, la página indicará que se requiere autorización. Haga clic en el **ZeroTier Central** hipervínculo para redirigir a ZeroTier Central.



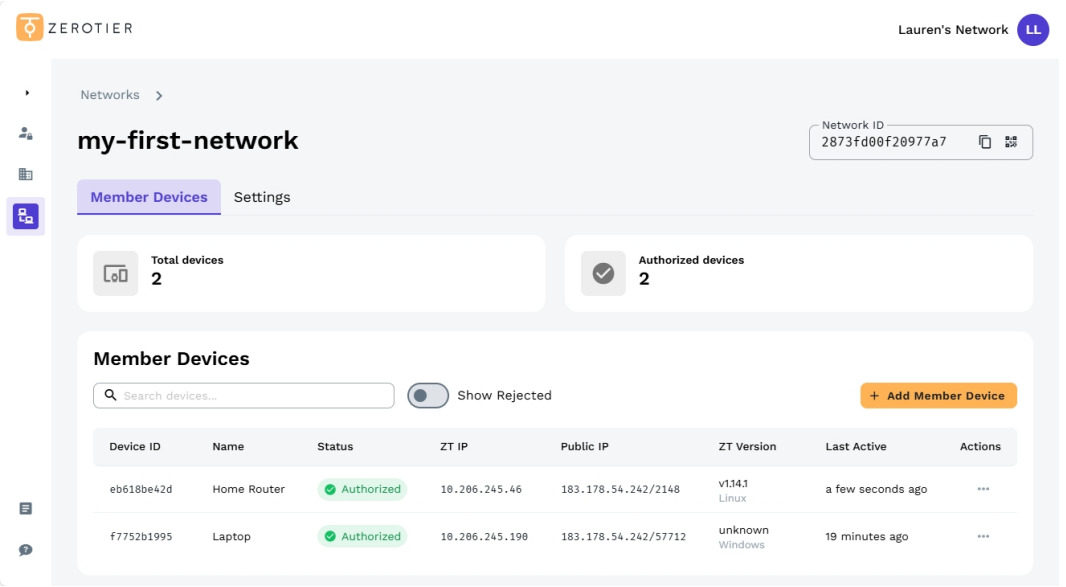
6. En ZeroTier Central, localice el dispositivo pendiente y autorícelo.



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

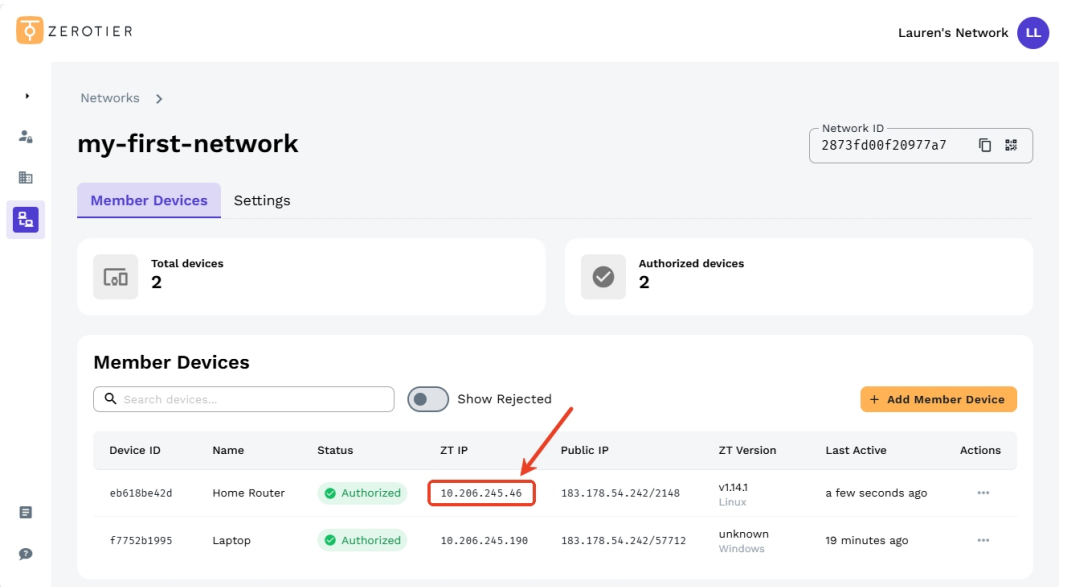


7. Agregue otro dispositivo (como una computadora o un teléfono inteligente) a la misma red ZeroTier siguiendo esta guía. Una vez agregado correctamente, se muestra la página como sigue. Verá los detalles de los dispositivos miembros, como **ID del dispositivo**, **Nombre**, **Estado**, **IP administrada**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



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

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



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

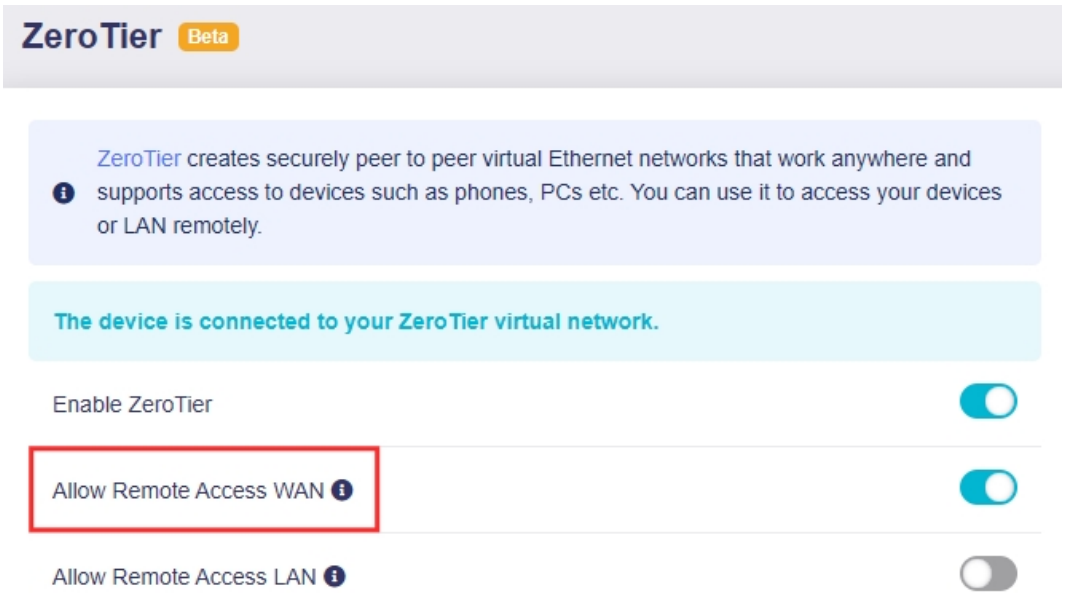
9. Pruebe la conectividad.

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

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

15.7.2 Permitir el acceso remoto a la WAN

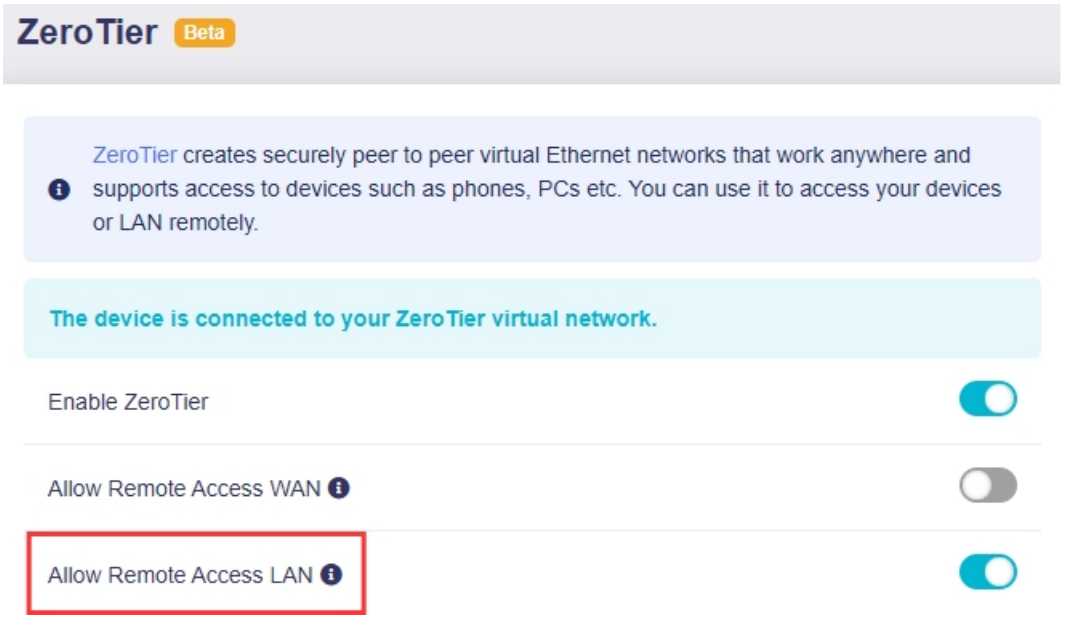
Si esta opción está habilitada, se puede acceder a los recursos en el lado WAN del dispositivo a través de la red virtual ZeroTier. Consulte aquí para obtener más detalles.



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

15.7.3 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 ZeroTier. Consulte aquí para obtener más detalles.



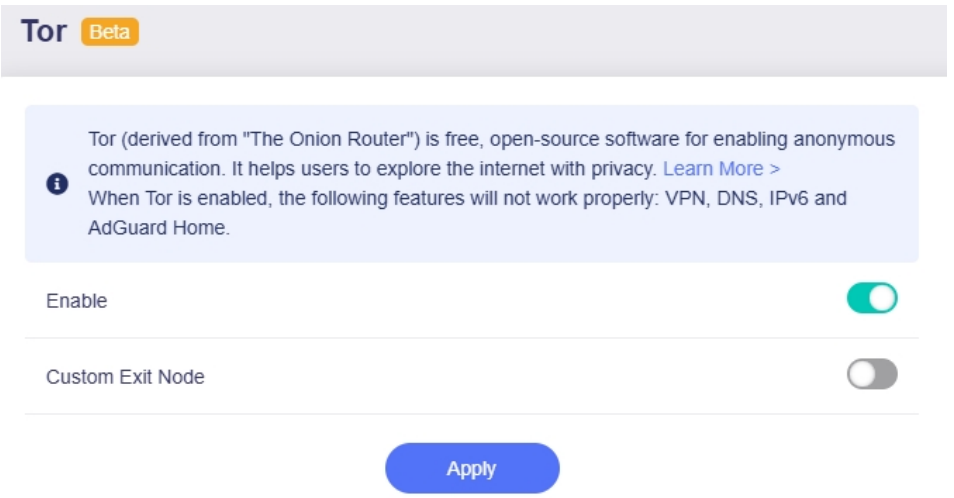
Nota: esta característica requiere que se agreguen reglas de enrutamiento a la red ZeroTier para que surta efecto. Se puede agregar una ruta personalizada de forma gratuita en Legacy Central, mientras que en New Central solo puedes configurar rutas personalizadas con un plan Essential o superior. Consulte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

15.8 Tor

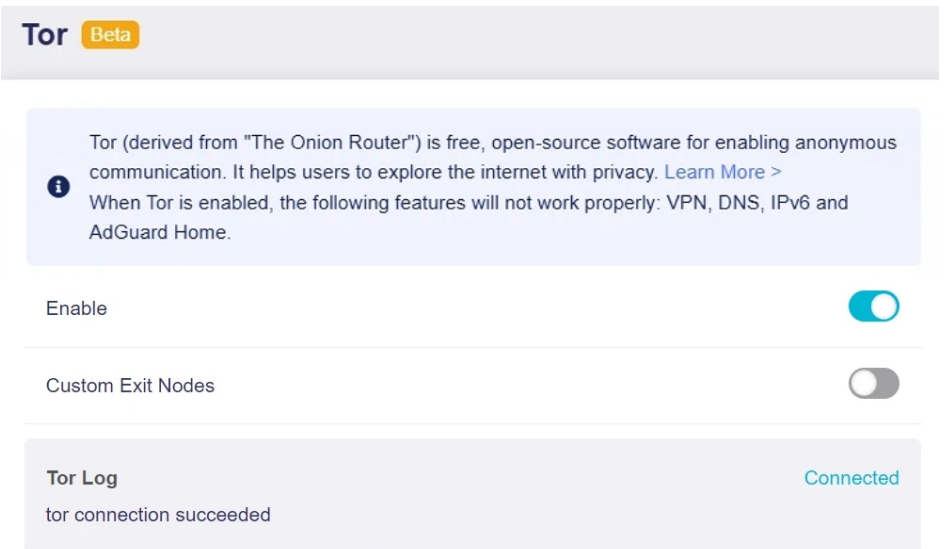
Tor (derivado de **The Onion Router**) es un software gratuito y de código abierto que permite la comunicación anónima. Ayuda a los usuarios a explorar Internet con privacidad. Tenga en cuenta que esta característicaestá actualmente en versión beta y puede tener algunos errores. Cuando Tor está habilitado, laslas siguientes funciones no funcionarán correctamente: VPN, DNS, IPv6, y AdGuard Home.

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

1. Inicie sesión en su enrutador'panel de administración web y navegue hasta **APLICACIONES** > **Tor**. Taleje cambie 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 16

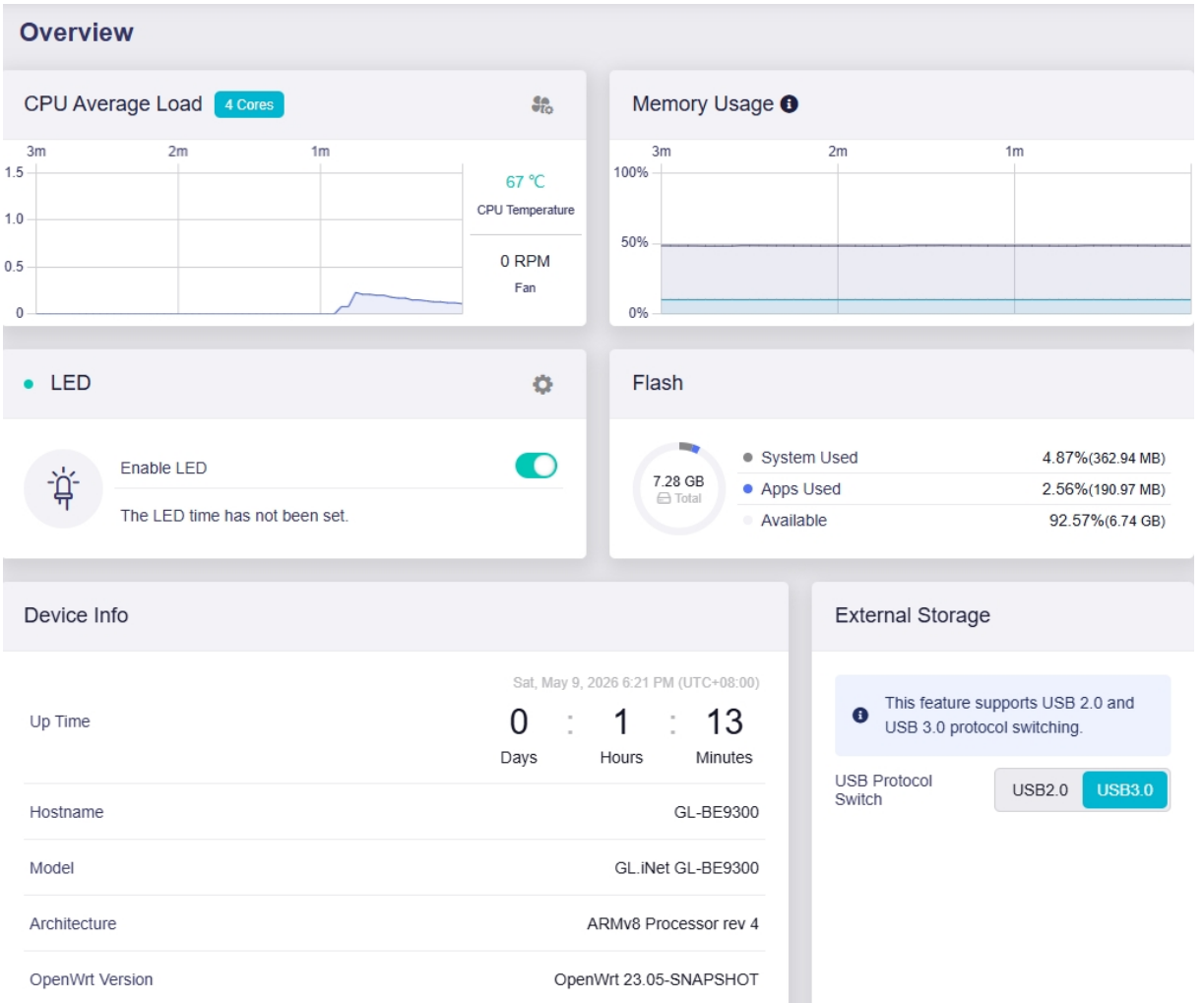
Sistema

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.

16.1 Descripción general

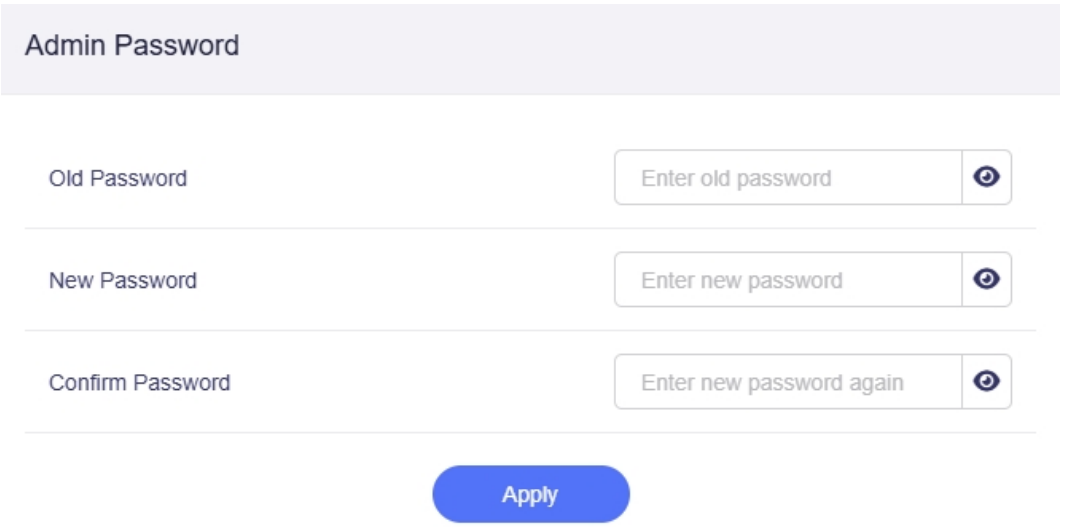
Inicie sesión en el panel de administración web de su enrutador' y navegue hasta **SISTEMA** > **Descripción general**. Esta página muestra estado del hardware y admite algunos controles simples, que incluyen:

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



16.2 Contraseña de administrador

Inicie sesión en su panel de administración web del enrutador y navegue hasta **SISTEMA** > **Contraseña de administrador**. ensu página, puede cambiar la contraseña de inicio de sesión del panel de administración web.



Los requisitos para la contraseña de administrador son los siguientes:

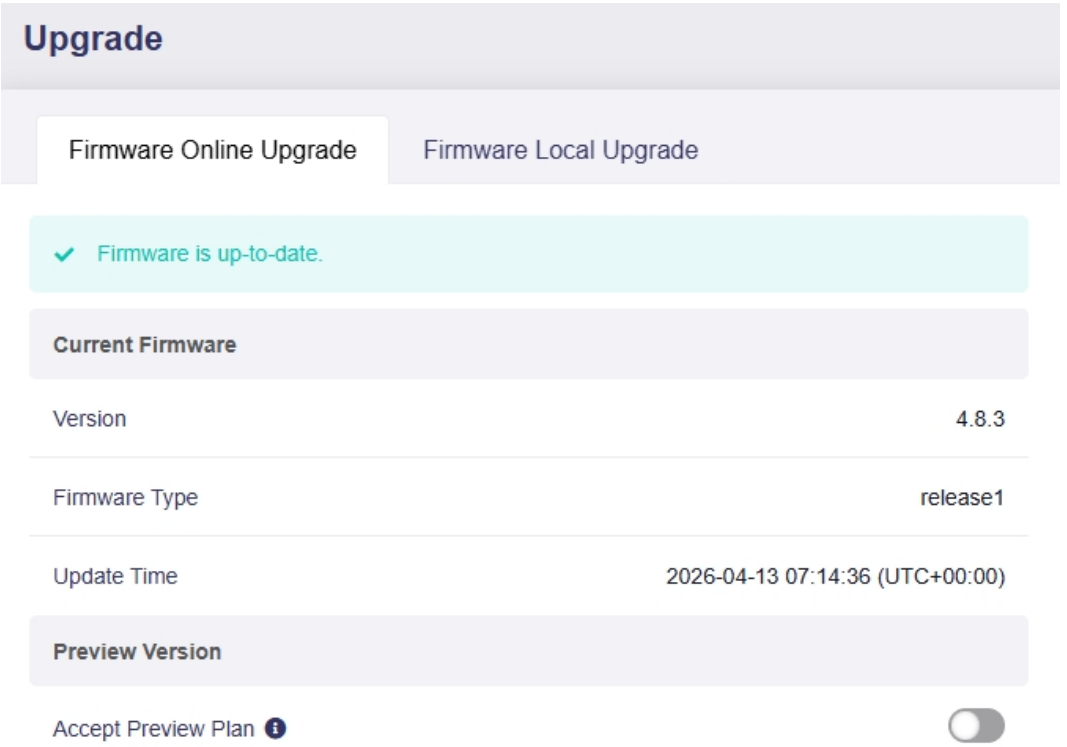
1. Mínimo 10 caracteres y máximo 63 caracteres de longitud.
2. Letras (distingue entre mayúsculas y minúsculas), números y símbolos (por ejemplo, ! @ # $ % ^ & * ( ) _ + - = , . > < | ? / \ [ ] { } : ; " ' ` ~) son necesarios.
3. Se requieren al menos dos tipos (letras mayúsculas, minúsculas, números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

16.3 Actualización

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

16.3.1 Actualización en línea

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



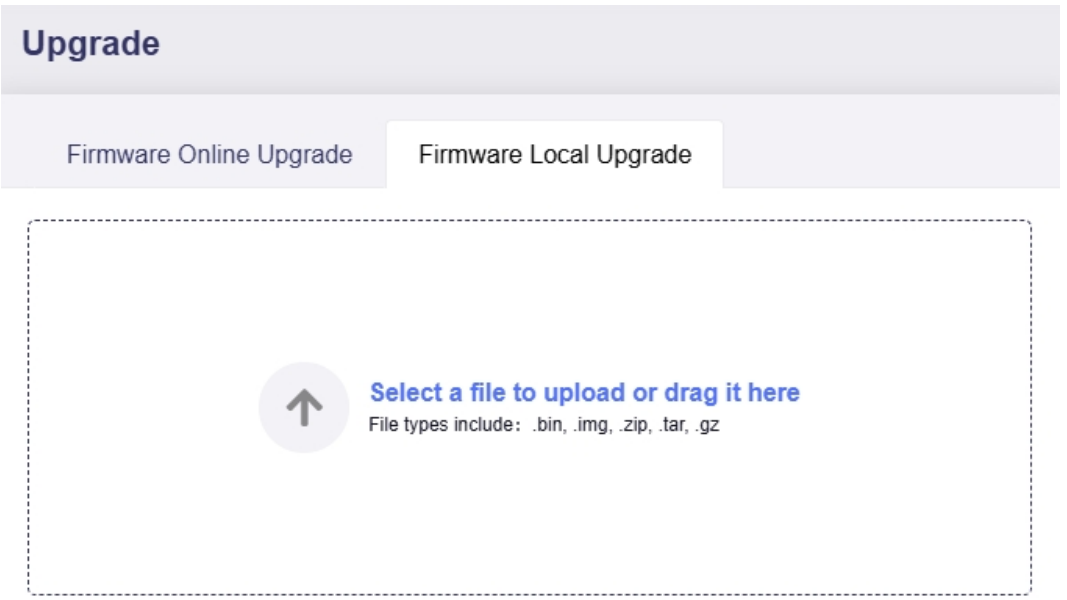
- **Aceptar plan de vista previa**: Si esta opción está habilitada, puede probar nuevas funciones antes de que se emita la versión final y enviarnos sus comentarios. Configúrelo una vez y permanecerá activado. Tenga en cuenta que es posible que estas actualizaciones no sean estables.

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

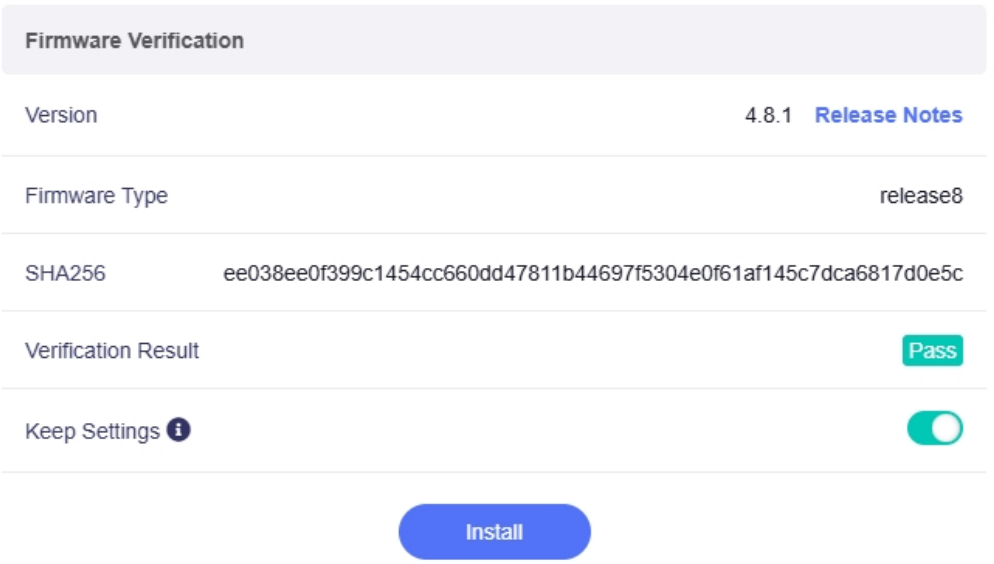
Consejo: Al intentar realizar una actualización en línea, si muestra **Error en la descarga**, navegue hasta **SYSTEM** > **Zona horaria** y solucione el error de zona horaria (sincronización con el navegador).

16.3.2 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**.



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

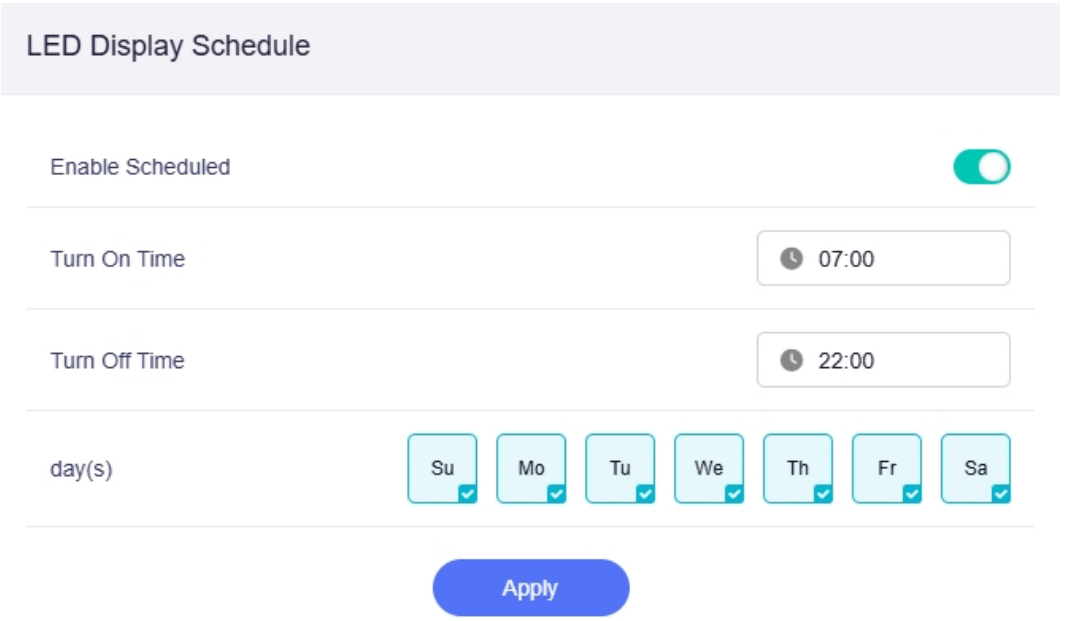
16.4 Tareas programadas

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

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.

16.4.1 Programación de los indicadores LED

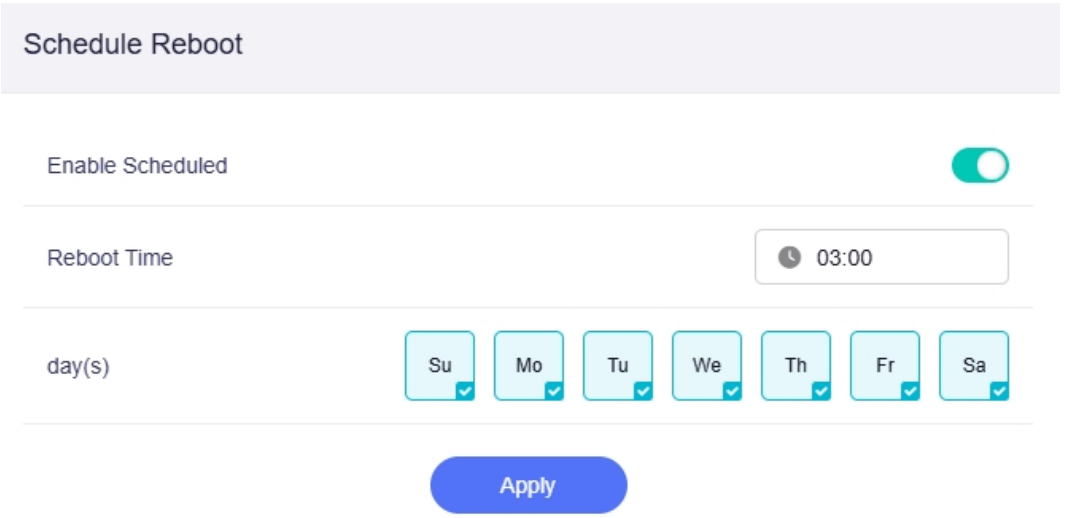
Set an encendido/apagado programe la luz LED de su enrutador si es necesario.
Cuando esté habilitado, configure las horas de encendido y apagado, seleccione las fechas efectivas semanales y luego haga clic en **Aplicar**.



16.4.2 Programar reinicio

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

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

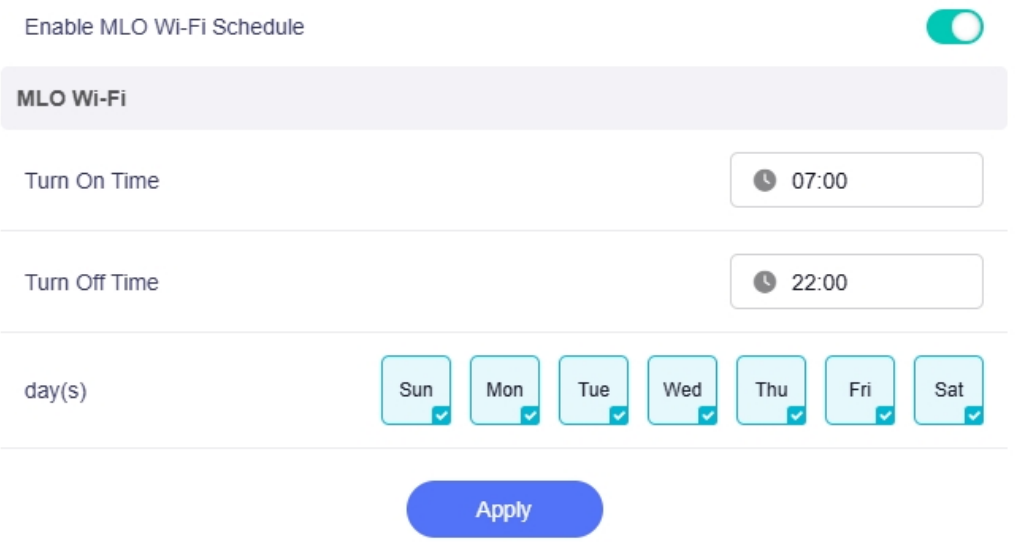


16.4.3 Programación de Wi-Fi MLO

Nota: esta función solo está disponible si el Wi-Fi de MLO está habilitado.

Establezca un horario de encendido/apagado para su Wi-Fi de MLO si es necesario.

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

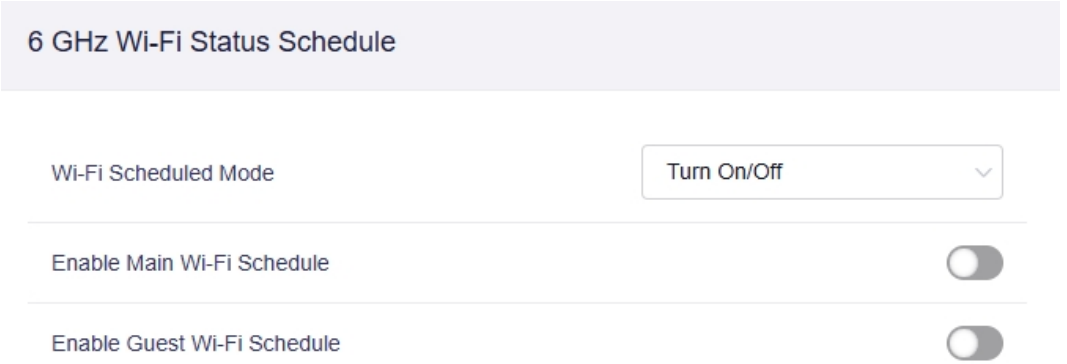


16.4.4 Programación de Wi-Fi de 6 GHz

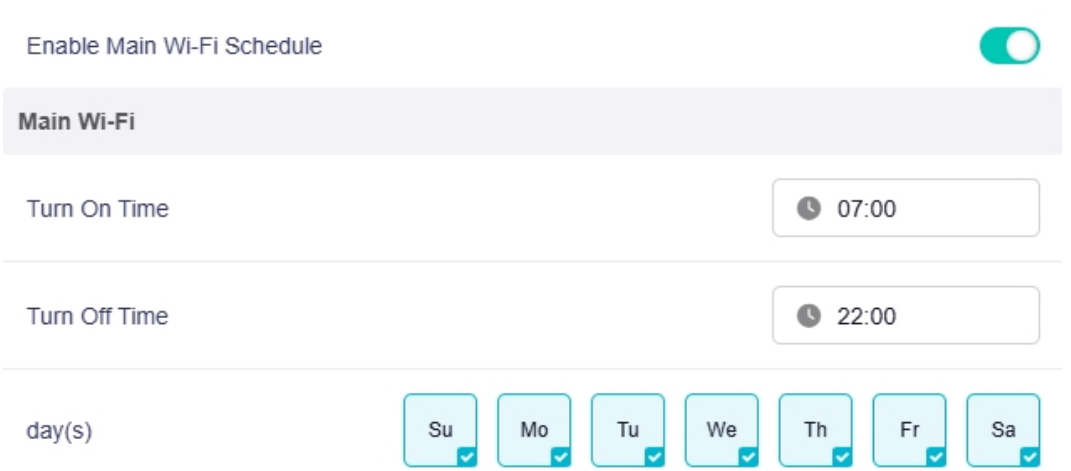
Establezca una programación para su Wi-Fi de 6 GHz en dos modos: Encienda Encender/Apagar y cambiar la alimentación de TX.

Modo 1: Encender/Apagar

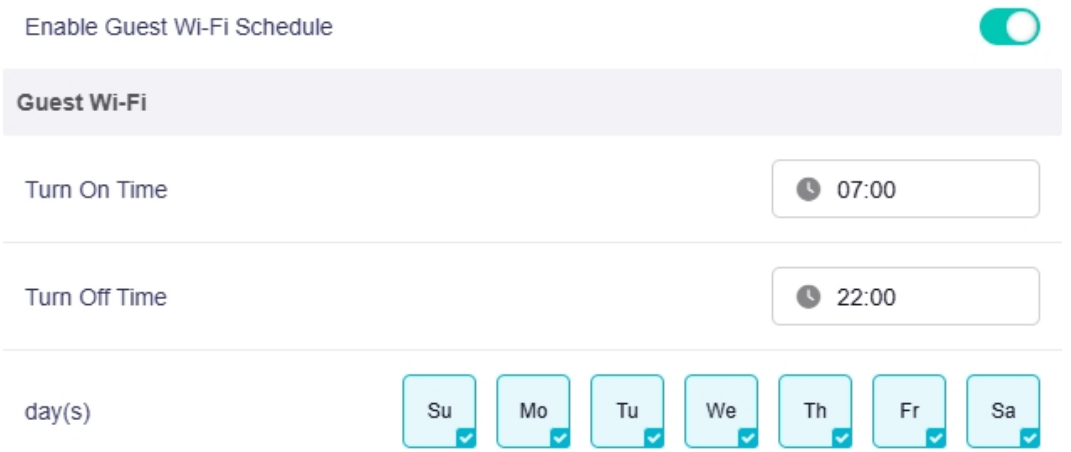
Puede habilitar el horario de encendido/apagado tanto para el Wi-Fi principal de 6 GHz como para el Wi-Fi para invitados.



- **Programador de Wi-Fi principal**: Cuando esté habilitado, configure los horarios de encendido y apagado de su Wi-Fi principal de 6 GHz, seleccione las fechas efectivas semanales y luego haga clic en **Aplicar**.

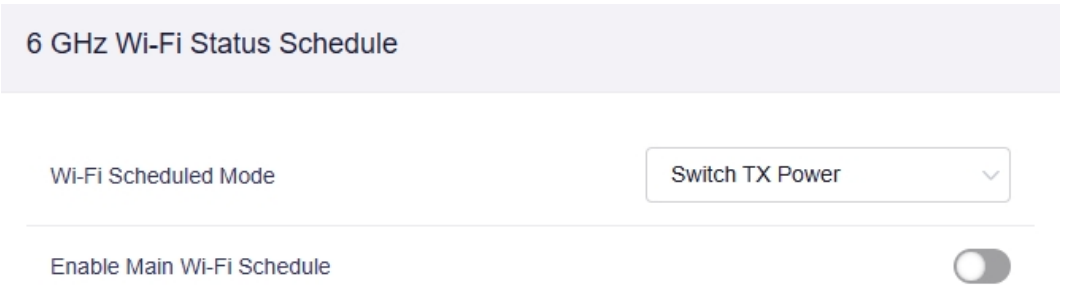


- **Programación de Wi-Fi para invitados**: cuando esté habilitado, configure los horarios de encendido y apagado de su Wi-Fi para invitados de 6 GHz, seleccione las fechas efectivas semanales y luego haga clic en **Aplicar**.

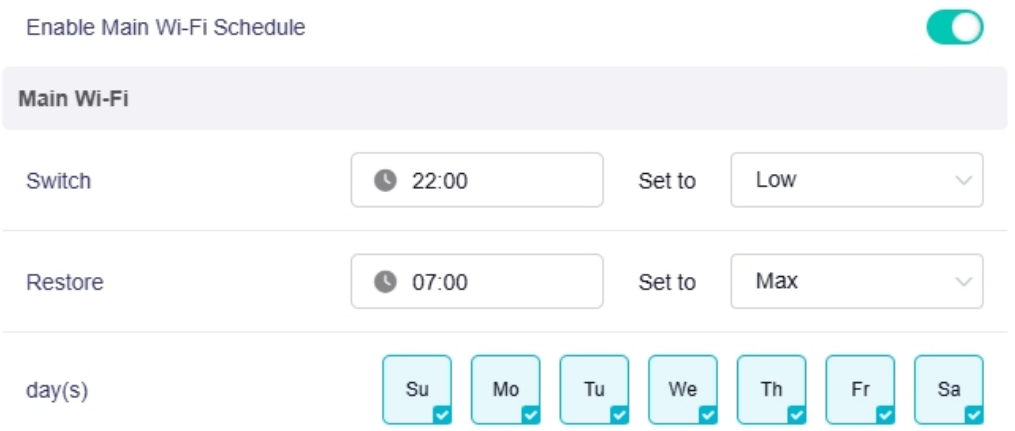


Modo 2: cambiar la alimentación de TX

Ypuede habilitar el cambio de energía TX programación para el 6GHz principal Wi-Fi.



Cuando esté habilitado, configure dos acciones cronometradas para su Wi-Fi principal de 6 GHz para cambiar la alimentación de TX, seleccione las fechas efectivas semanales y luego haga clic en **Aplicar**.

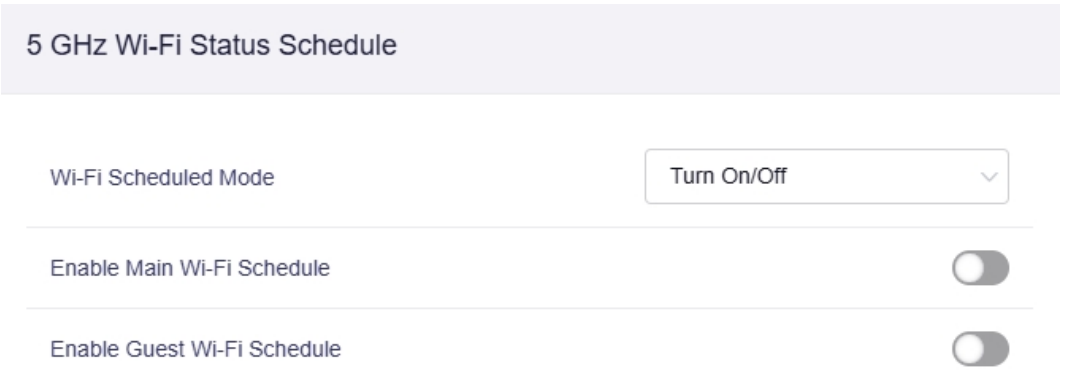


16.4.5 Programación de Wi-Fi de 5 GHz

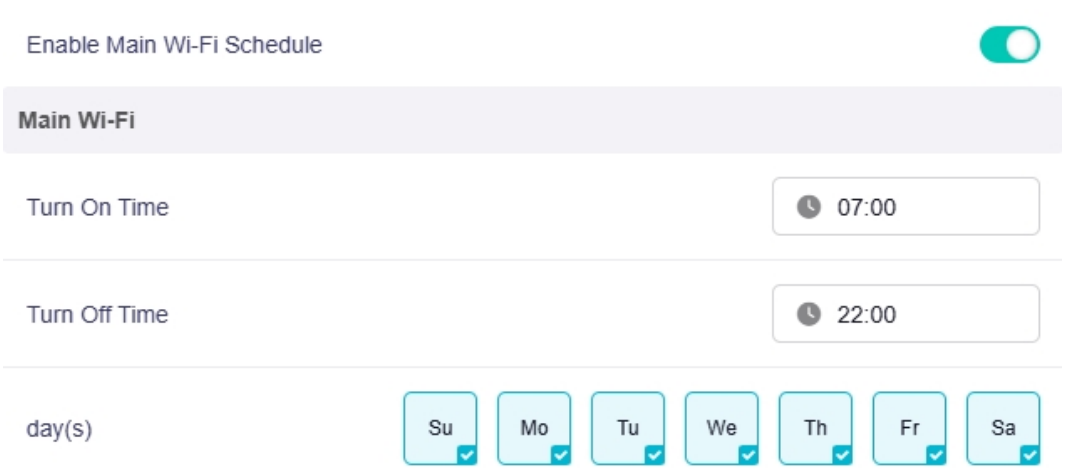
Establezca una programación para su Wi-Fi de 5 GHz en dos modos: encender/apagar y cambiar la alimentación de transmisión.

Modo 1: Encender/apagar

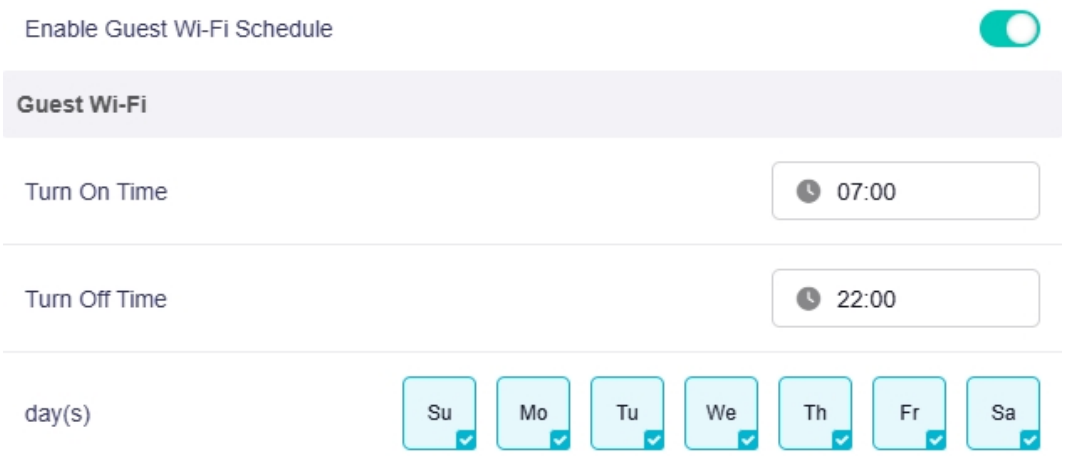
Puede habilitar la programación de encendido/apagado tanto para el Wi-Fi principal de 5 GHz como para invitados Wi-Fi.



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

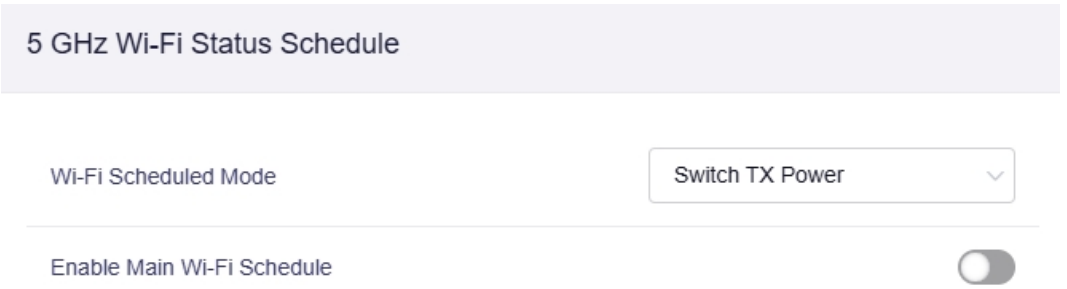


- **Programación de Wi-Fi para invitados**: cuando esté habilitado, configure los horarios de encendido y apagado de su Wi-Fi para invitados de 5 GHz, seleccione las fechas efectivas semanales y luego haga clic en **Aplicar**.

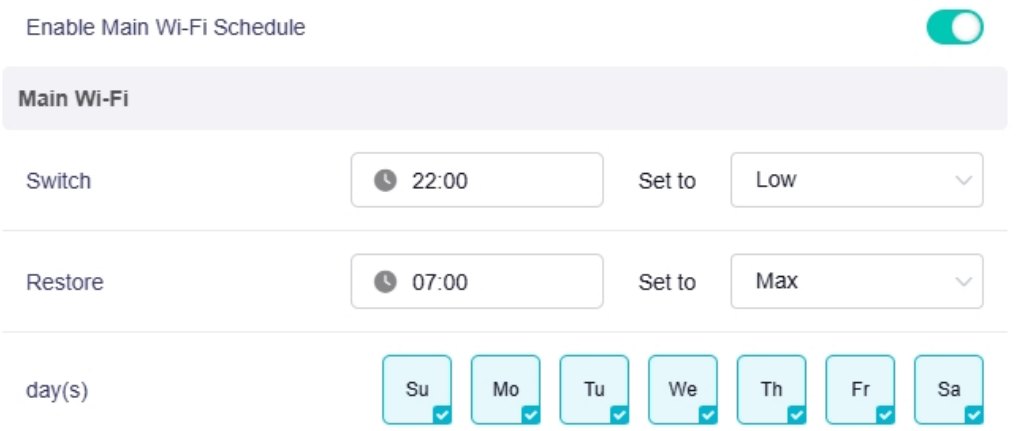


Modo 2: Cambiar alimentación de TX

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



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

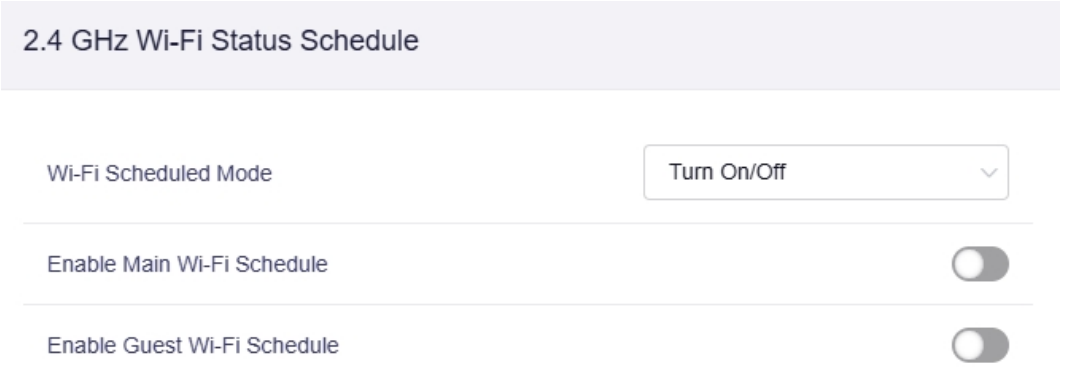


16.4.6 Programación de Wi-Fi de 2,4 GHz

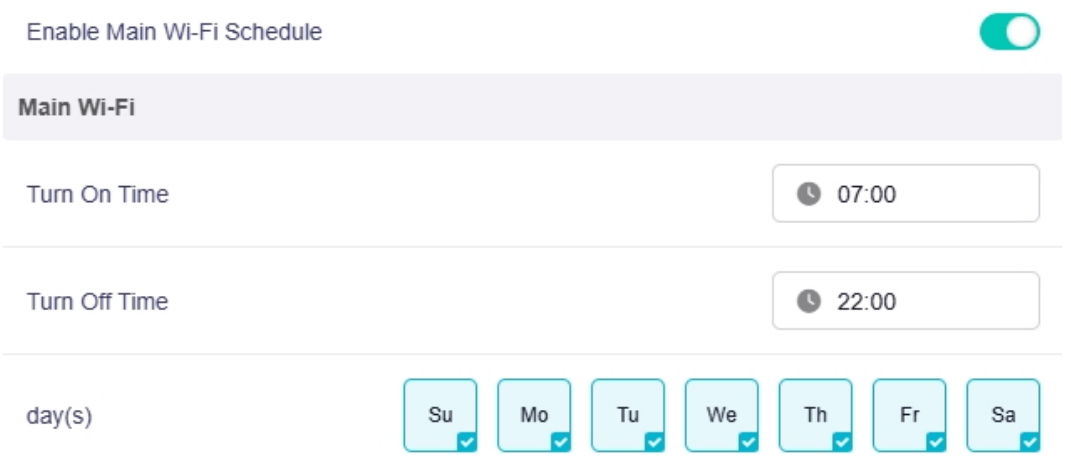
Establezca una programación para su Wi-Fi de 2,4 GHz en dos modos: encender/apagar y cambiar la alimentación de transmisión.

Modo 1: Activar/Apagar

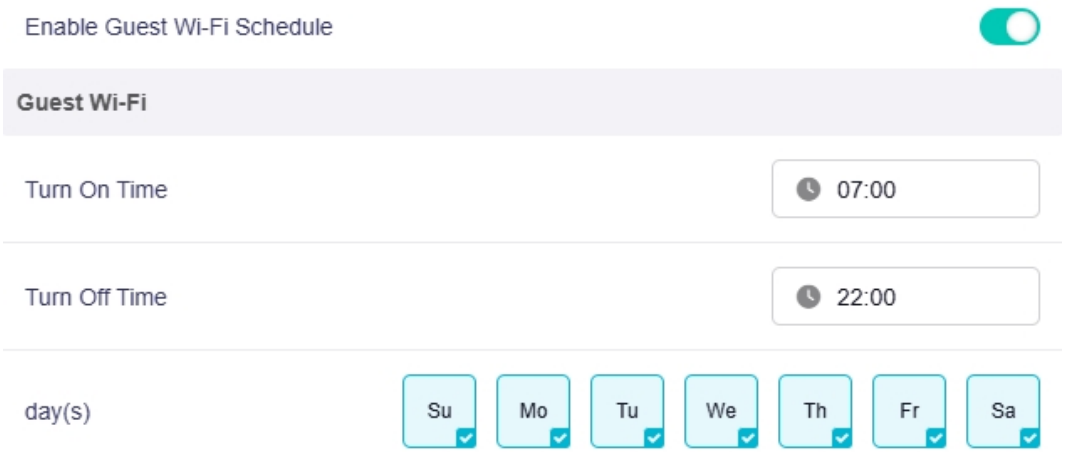
Puede habilitar el horario de encendido/apagado tanto para el Wi-Fi principal de 2,4 GHz como para el Wi-Fi para invitados.



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

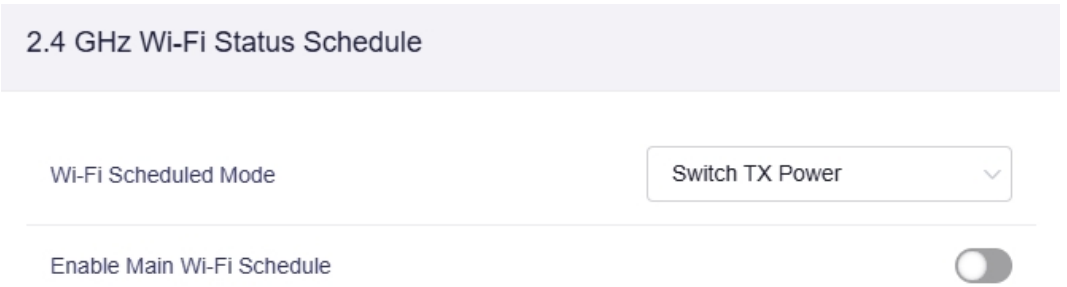


- **Programación de Wi-Fi para invitados**: cuando esté habilitado, configure los horarios de encendido y apagado de su Wi-Fi para invitados de 2,4 GHz, seleccione las fechas efectivas semanales, luego haga clic en **Aplicar**.

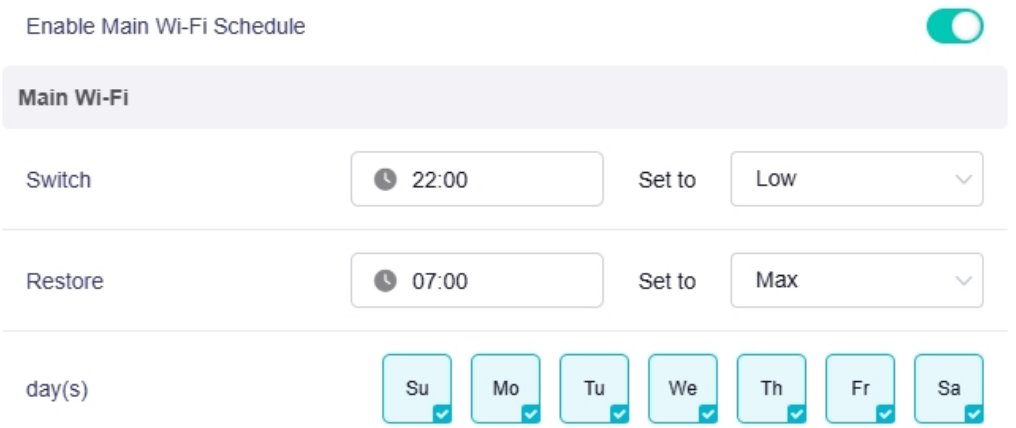


Modo 2: Cambiar alimentación de TX

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

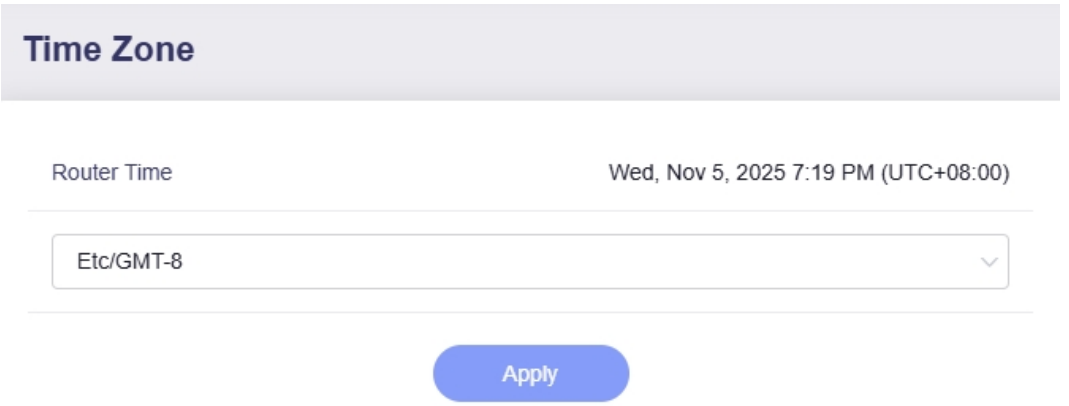


Cuando esté habilitado, configure dos acciones cronometradas para su Wi-Fi principal de 2,4 GHz para cambiar la alimentación de TX, seleccione las fechas efectivas semanales, luego haga clic en **Aplicar**.

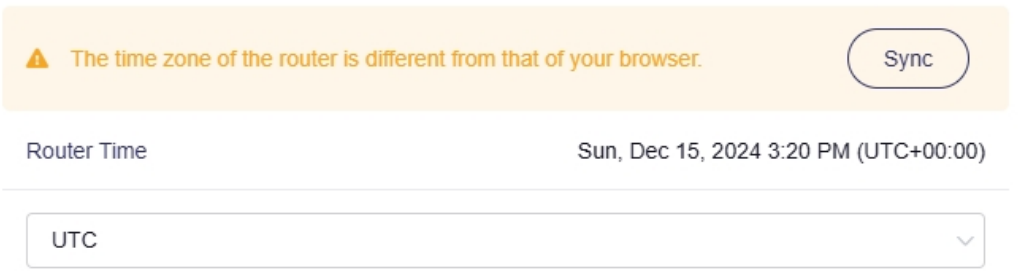


16.5 Zona horaria

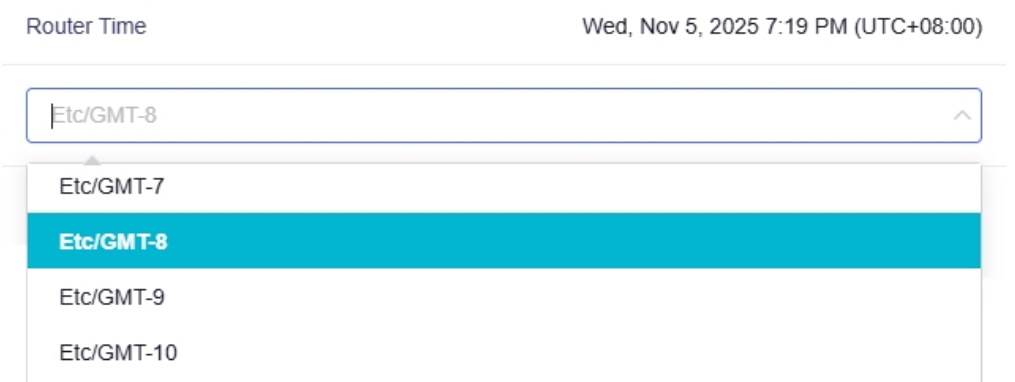
Inicie sesión en el panel de administración web de su enrutador y navegue hasta **SISTEMA** > **Zona horaria**. Esta página muestra la la hora, indicando la fecha, la hora y el desplazamiento de zona horaria correspondiente.



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



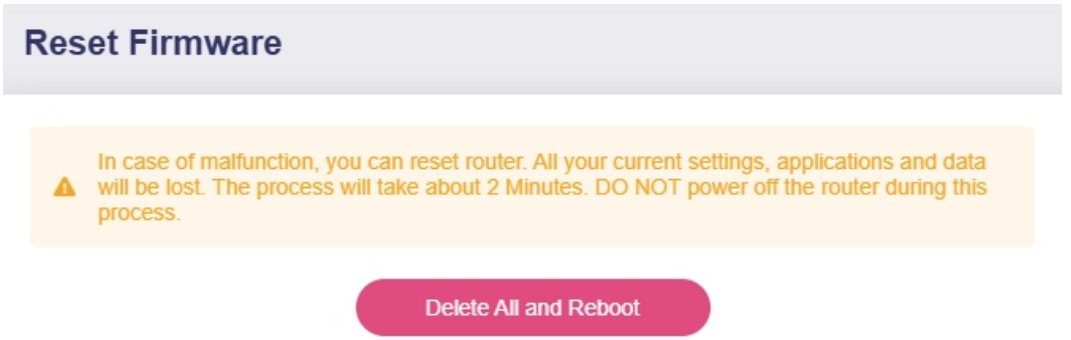
Para cambiar zona horaria, sseleccione la zona horaria adecuada de la lista para garantizar que la hora del sistema coincida con su hora local.



16.6 Restablecer firmware

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

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

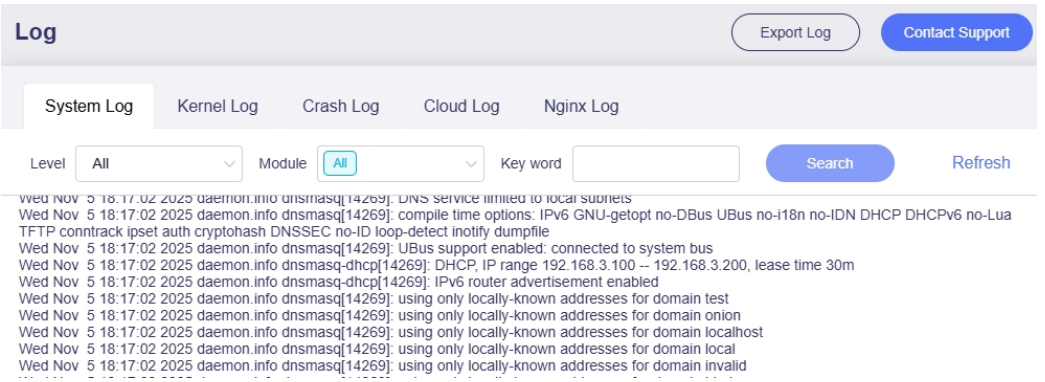


Nota: todas sus configuraciones, aplicaciones y datos actuales se borrados. El proceso durará unos 2 minutos. Nono apague el enrutador durante este proceso.

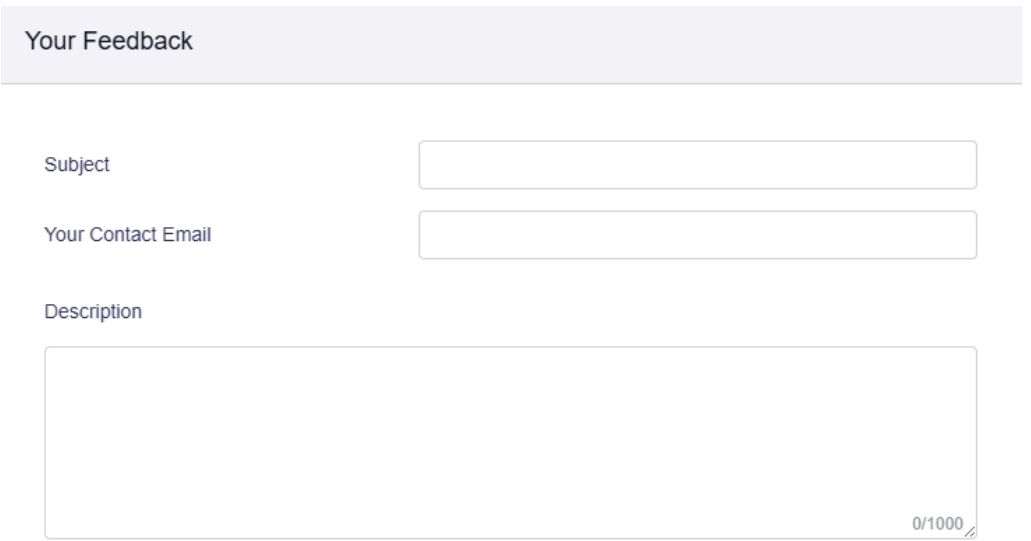
Si no puede acceder al panel de administración web del enrutador', intente restablecer su enrutador usando el botón de reinicio físico en el costado.

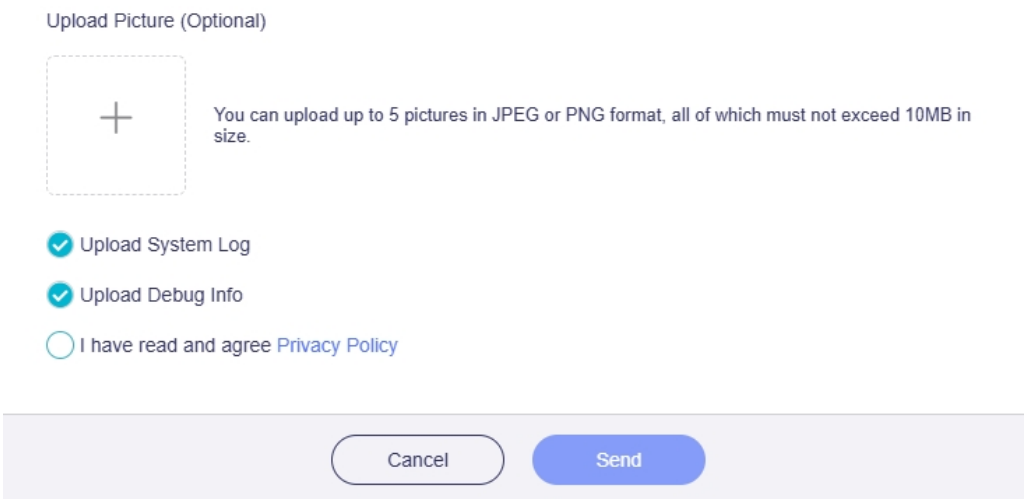
16.7 Registro

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



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



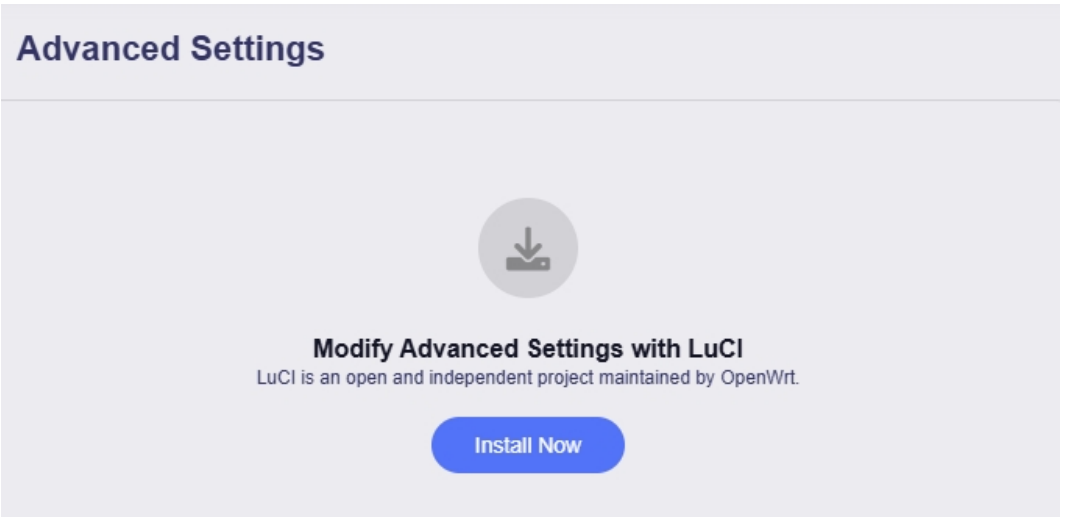

Upload Picture (Optional)
You can upload up to 5 pictures in JPEG or PNG format, all of which must not exceed 10MB in size.
Upload System Log
Upload Debug Info
I have read and agree Privacy Policy
Cancel
Send

16.8 Configuración avanzada

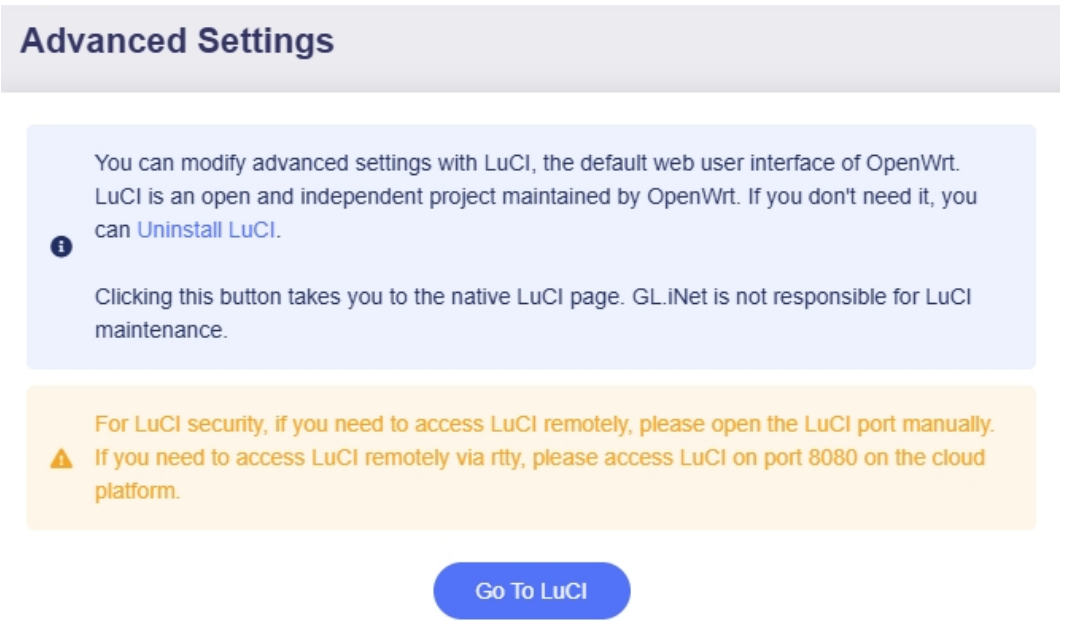
Inicie sesión en el panel de administración web de su enrutador y navegue hasta **SISTEMA** > **Configuración avanzada**. Esta página le permitepuedes para modificar la configuración avanzada en LuCI, que es la interfaz de usuario web predeterminada de OpenWrt. Como proyecto abierto e independiente mantenido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

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

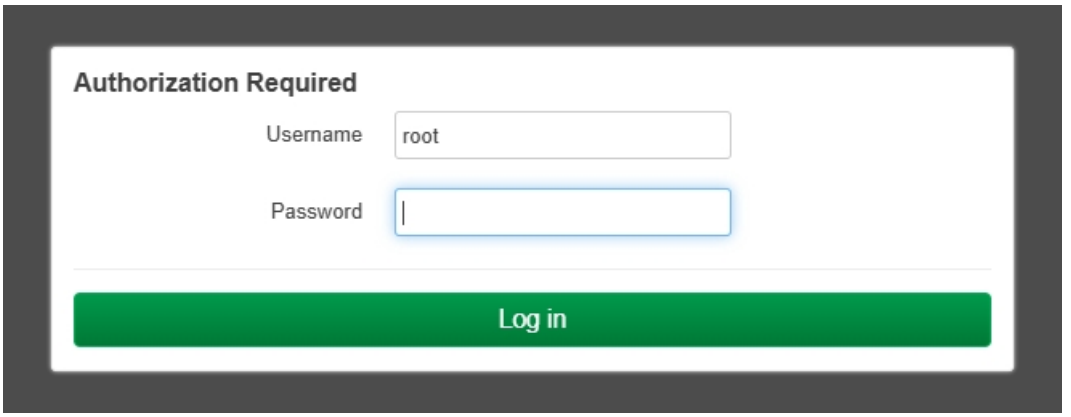
1. Haga clic en **Instalar ahora** y se instalará la interfaz LuCI.



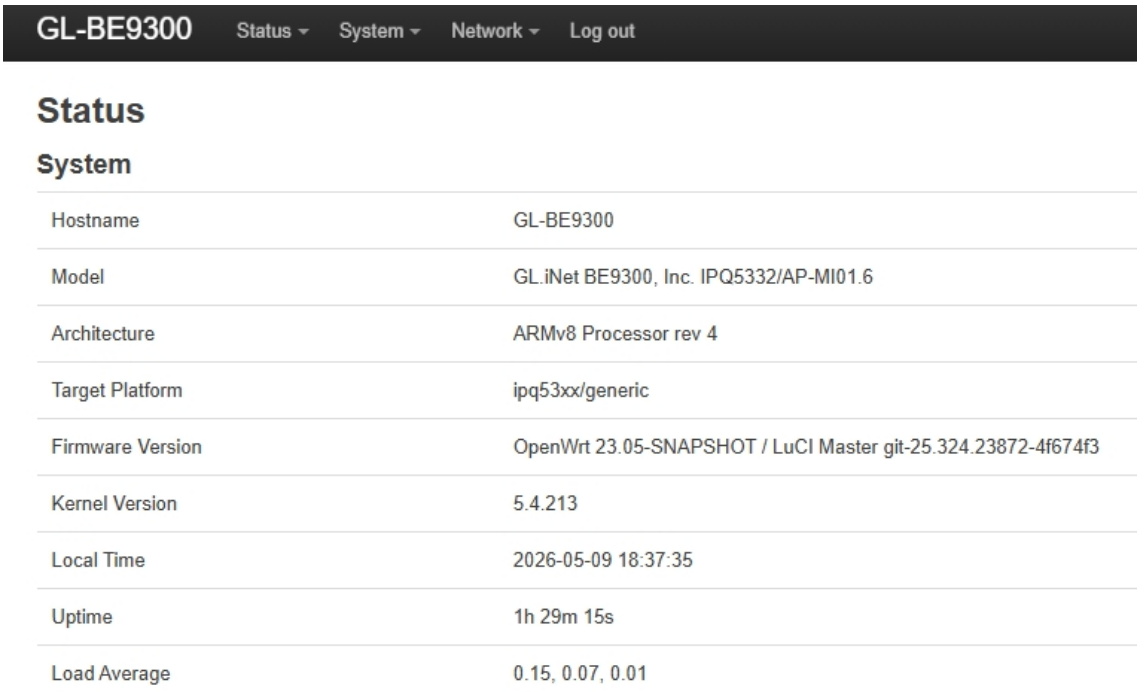
2. Click **Vaya a LuCI**, y será redirigido a la página de inicio de sesión de LuCI.



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



Yusted luego log en a la interfaz LuCI .



Declaración de Conformidad

Por la presente, GL TECHNOLOGIES (HONG KONG) LIMITED declara que el tipo de equipo de radio [Router Wi-Fi 7 BE9300, GL-BE9300] cumple los requisitos esenciales y demás disposiciones pertinentes de la Directiva 2014/53/UE. El texto completo de la declaración UE de conformidad está disponible en la siguiente dirección de internet: https://www.gl-inet.com/products/certificate.