GL·iNet



Manual de usuario

GL-SFT1200 / Opal

Enrutador de viaje Wi-Fi 5

Versión de firmware 4.8.3

Acerca de este manual

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

Con esta guía, podrá:

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

Convenciones de formato

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

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

Nota:

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

¿Necesita más ayuda o información?

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

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

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

Contenido

Capítulo 1 Conozca su enrutador 5

1.1 Descripción general del producto 6

1.1.1 Apariencia 6

1.1.2 Interfaz y botón 7

1.1.3 LED 8

1.2 Especificaciones 8

1.3 Contenido del paquete 9

Capítulo 2 Conexión de hardware 10

2.1 Elección de una ubicación 11

2.2 Conexión del enrutador 11

Capítulo 3 Iniciar sesión en el enrutador 13

Capítulo 4 Configurar la conexión a Internet 15

4.1 Asistente de configuración rápida 16

4.2 Configurar manualmente la conexión a Internet 17

4.2.1 Conectarse a Internet mediante un cable Ethernet 18

4.2.2 Conectarse a Internet mediante una red Wi-Fi existente 22

4.2.3 Conectarse a Internet mediante conexión compartida por USB 30

4.2.4 Conectarse a Internet mediante un módem USB 34

Capítulo 5 Red inalámbrica 36

5.1 Visualización del estado de Wi-Fi 37

5.2 Configuración inalámbrica 38

5.2.1 Wi-Fi de 5 GHz 38

5.2.2 Wi-Fi de 2,4 GHz 40

5.2.3 BSSID aleatorio 42

Capítulo 6 Clientes 44

6.1 Detalles del dispositivo 46

6.2 Acción 48

6.3 Eliminar clientes 51

6.4 Ordenar 52

Capítulo 7 Servicios en la nube 53

7.1 GoodCloud 54

7.1.1 Habilitar GoodCloud 55
7.1.2 Administrar el enrutador 58
7.1.3 Desvincular el dispositivo 63
7.1.4 Desactivar GoodCloud 63
7.2 AstroWarp 64
Capítulo 8 Conozca la VPN 65
8.1 Introducción 66
8.2 Escenarios de aplicación 67
Capítulo 9 Panel de VPN 69
9.1 Asistente de configuración de VPN 70
9.2 Modo VPN 73
9.2.1 Modo global 74
9.2.2 Modo de política 75
Capítulo 10 Configurar el servidor VPN 86
10.1 Configurar el servidor OpenVPN 87
10.1.1 Preparación 87
10.1.2 Pasos de configuración 88
10.1.3 Solución de problemas 90
10.2 Configurar el servidor WireGuard 92
10.2.1 Preparación 92
10.2.2 Pasos de configuración 93
10.2.3 Solución de problemas 96
Capítulo 11 Configurar el cliente VPN 98
11.1 Configurar el cliente OpenVPN 99
11.1.1 Preparación 99
11.1.2 Configurar NordVPN 99
11.1.3 Configurar el cliente OpenVPN manualmente (para otros proveedores) 105
11.2 Configurar el cliente WireGuard 108
11.2.1 Preparación 108
11.2.2 Configurar AzireVPN 109
11.2.3 Configurar Hide.me 113
11.2.4 Configurar IPVanish 116
11.2.5 Configurar Mullvad 120
11.2.6 Configurar NordVPN 124

11.2.7 Configurar PIA (Private Internet Access) 129
11.2.8 Configurar Surfshark 133
11.2.9 Configurar el cliente WireGuard manualmente (para otros proveedores) ... 137
Capítulo 12 Red 142
12.1 Multi-WAN 143
12.1.1 Seguimiento del estado de la interfaz 143
12.1.2 Modo Multi-WAN 146
12.2 LAN 149
12.2.1 Configuración básica 149
12.2.2 Servidor DHCP 151
12.2.3 Reserva de direcciones 153
12.3 Red de invitados 154
12.3.1 Configuración básica 154
12.3.2 Servidor DHCP 155
12.4 DNS 157
12.4.1 Configuración general 158
12.4.2 Configuración del servidor DNS 159
12.4.3 Editar hosts 161
12.5 Puerto Ethernet 163
12.6 IPv6 164
12.6.1 Modo IPv6 165
12.6.2 Método de obtención de DNS 165
12.7 Inspección IGMP 166
12.8 Modo de red 167
12.9 Puerta de enlace directa 169
12.10 Aceleración de red 171
Capítulo 13 Seguridad 173
13.1 Reenvío de puertos 174
13.1.1 DMZ 174
13.1.2 Reenvío de puertos 175
13.2 Control de gestión 177
13.2.1 Control de acceso 177
13.2.2 Control de acceso remoto 180
13.2.3 Abrir puertos en el enrutador 181

13.3 Modo NAT 183
Capítulo 14 Aplicaciones 184
14.1 Complementos 185
14.2 DNS dinámico 186
14.2.1 Habilitar DDNS 186
14.2.2 Comprobar si DDNS funciona 189
14.2.3 Acceso remoto HTTPS 191
14.2.4 Acceso remoto SSH 193
14.3 Almacenamiento en red 195
14.3.1 Conectar una unidad de almacenamiento 195
14.3.2 Configurar Samba 196
Capítulo 15 Sistema 199
15.1 Descripción general 200
15.2 Contraseña de administrador 201
15.3 Actualización 202
15.3.1 Actualización en línea 202
15.3.2 Actualización local 203
15.4 Tareas programadas 205
15.4.1 Programación de los indicadores LED 205
15.4.2 Programar reinicio 206
15.4.3 Programación de Wi-Fi de 5 GHz 206
15.4.4 Programación de Wi-Fi de 2,4 GHz 208
15.5 Zona horaria 211
15.6 Configuración del botón de alternancia 212
15.7 Restablecer firmware 213
15.8 Registro 214
15.9 Configuración avanzada 216
Declaración de Conformidad 218

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

Opal (GL-SFT1200) es un enrutador de viaje de bolsillo que admite una velocidad de transferencia inalámbrica de 1200 Mbps. Tiene un diseño compacto para uso portátil y puede satisfacer las necesidades de acceso inalámbrico a Internet de pequeñas empresas, pequeños apartamentos o viajeros de negocios.

1.1.1 Apariencia

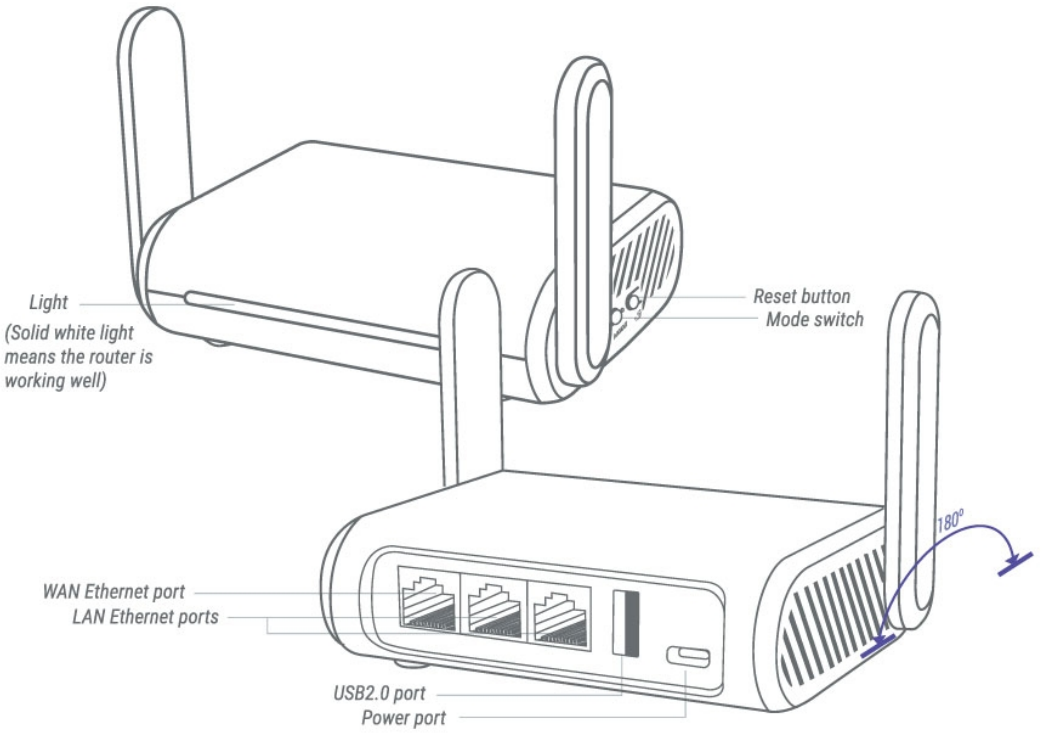








1.1.2 Interfaz y botón



Artículo	Descripción
Puerto de alimentación	Para conectar el adaptador de corriente.
Puerto WAN	Para conectarse a un módem o a una toma Ethernet.
Puerto LAN	Para conectar dispositivos cableados al enrutador.
Puerto USB 2.0	Para conectar un dispositivo de almacenamiento USB al enrutador.
Botón Restablecer	Mantenga presionado durante **4 segundos** para reparar su red; Presione y mantenga presionado durante **10 segundos** y luego suelte para restablecer el enrutador a los valores predeterminados de fábrica.
Botón de alternancia	Un interruptor físico que alterna la configuración del enrutador seleccionado con un voltear. Puedes configurarlo en el panel de administración web para habilitar cambio de funciones específicas con un solo clic.

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 x puerto Ethernet WAN 1 x puerto LAN Ethernet 1 x puerto USB 2.0 1 x entrada de alimentación tipo C 1 x botón Restablecer 1 x botón de alternancia
CPU	SF19A28, doble núcleo a 1 GHz
Memoria/Almacenamiento	DDR3 128MB / SPI NAND Flash 128MB
Protocolo	IEEE 802.11a/b/g/n/ac
Velocidad de Wi-Fi	300Mbps (2,4 GHz), 867 Mbps (5 GHz)
Antenas	2 x antenas Wi-Fi externas no desmontables
Velocidad de Ethernet	10/100/1000 Mbps
Entrada de energía	Tipo C, 5V/3A
Consumo de energía	< 6W
Temperatura de funcionamiento	0 ~ 40°C (32 ~ 104°F)
Temperatura de almacenamiento	-20 ~ 70°C (-4 ~ 158°F)

Dimensión/Peso	118 x 85 x 30 mm/145 g
Otras herramientas	Hoja de datos / Firmware / Aplicación / Unboxing / Tutoriales

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

1.3 Contenido del paquete

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

- 1 x Opal (GL-SFT1200)
- 1 x 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)

Capítulo 2

Conexión de hardware

Este capítulo cubre la selección de la ubicación del enrutador y su conexiónion 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**: coloque los cables y el cable de alimentación de forma segura para evitar riesgos de tropiezos.
- **Superficie estable**: coloque el enrutador en una superficie plana y horizontal (estante, escritorio) para mayor estabilidad.
- **Evitación de EMI**: mantenga el enrutador lejos de fuentes de interferencia electromagnética (dispositivos Bluetooth, microondas) para minimizar la interferencia de la señal.

2.2 Conexión del enrutador

1. **Encendido**

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

2. **Conecte un dispositivo al enrutador**

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

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

3. **Inicie sesión en enrutador**

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

Capítulo 3

Iniciar sesión en el enrutador

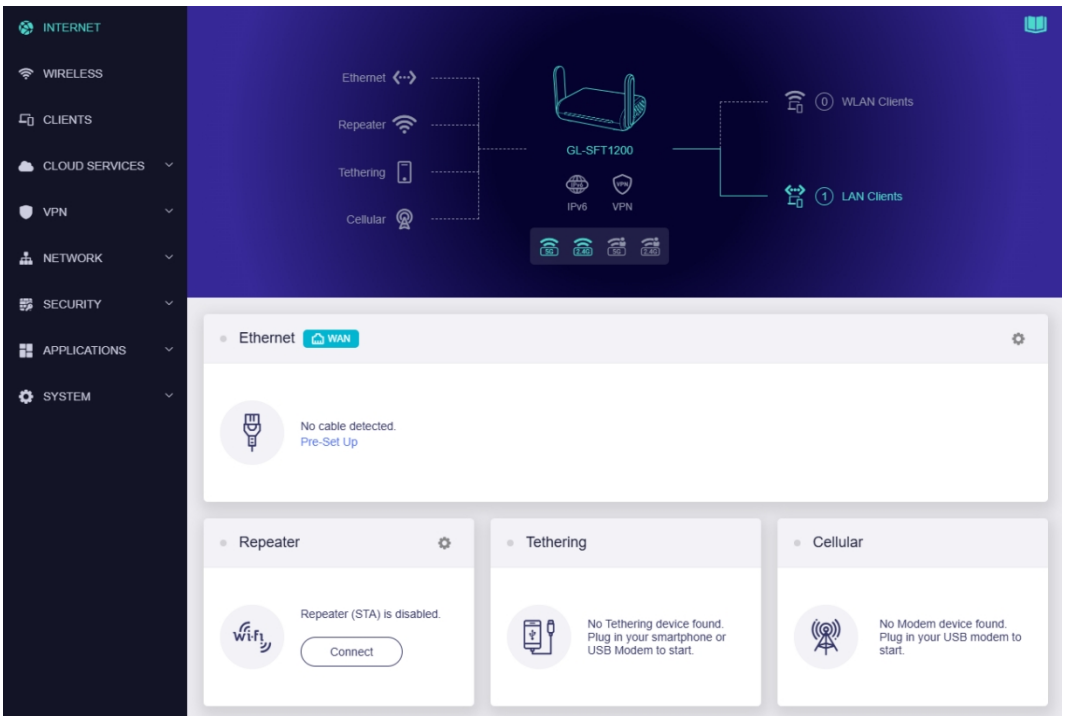
Este capítulo lo guía para iniciar sesión en su enrutador a través del panel de administración web.

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

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

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. Sconfigure su contraseña de administrador. Se recomienda una contraseña segura por motivos de seguridad. Luego haga clic en **Siguiente** para continuar.
4. Configura tu SSID y contraseña de Wi-Fi. Si ha modificado alguna información de Wi-Fi aquí, vuelva a conectarse al Wi-Fi actualizado. Luego haga clic en **Aplicar**.
5. Yluego ingrese el enrutador's web admin panel.



Capítulo 4

Configurar la conexión a Internet

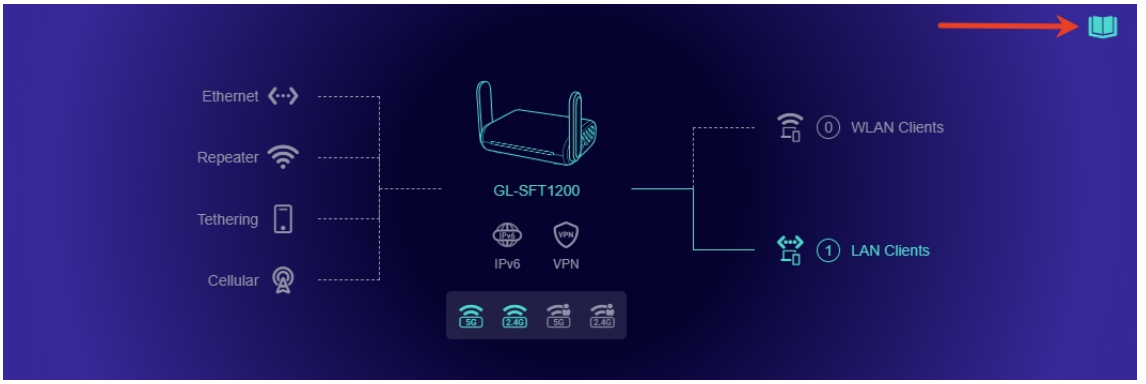
Este capítulo presenta múltiples métodos de conexión a Internet para que el enrutador se adapte a diversos entornos de red.

4.1 Asistente de configuración rápida

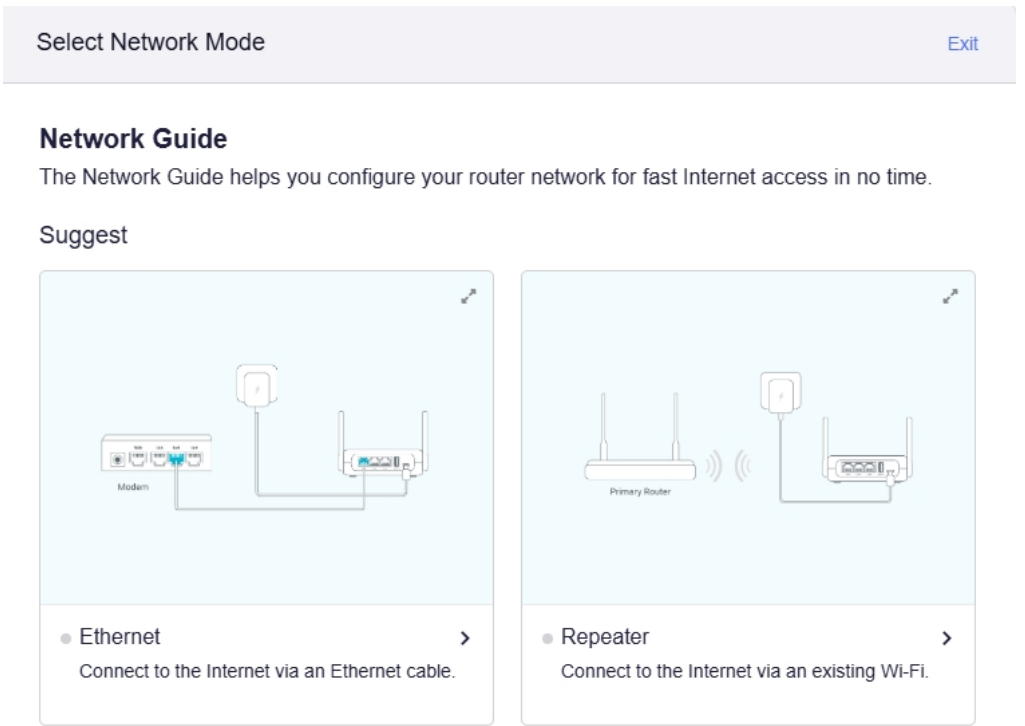
El asistente de configuración basado en web lo guiará a través de la configuración de la red del enrutador.

Siga los pasos a continuación para iniciar el asistente.

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



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



Si utiliza la aplicación GL.iNet, siga las instrucciones en pantallas para configurar iacceso a Internet.

4.2 Configurar manualmente la conexión a Internet

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

Opal admite cuatro métodos de conexión a Internet: Ethernet, Repetidor, Anclaje a red USB y módem USB. Cseleccione el método adecuado según sus necesidades de uso.

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

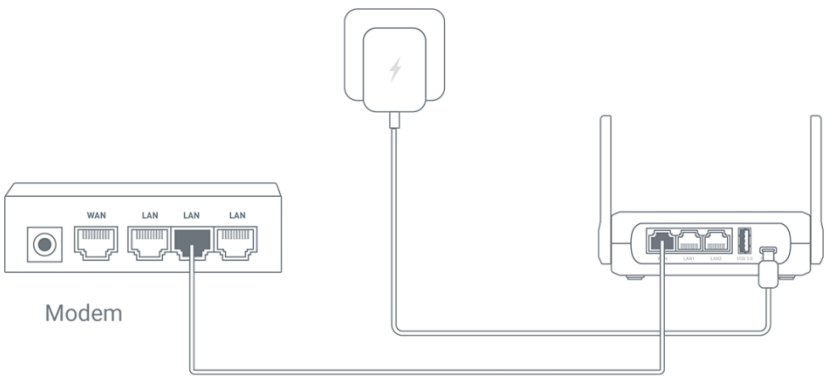
4.2.1 Conectarse a Internet mediante un cable Ethernet

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.

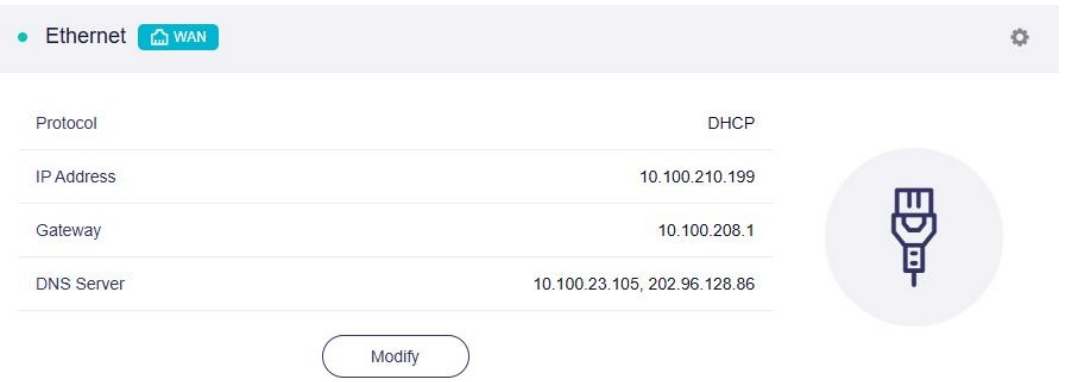
Configuración básica

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

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

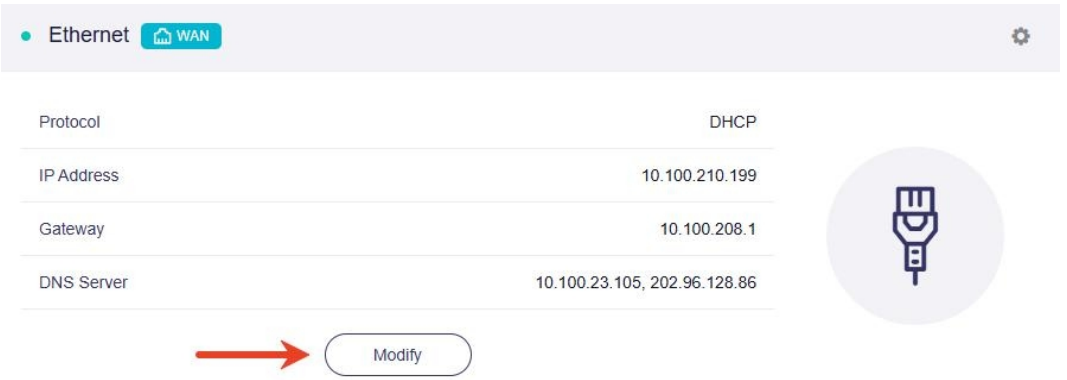


2. Inicie sesión en el enrutador'panel de administración web y navegue a **INTERNET** > **Ethernet**. Si la conexión se realiza correctamente, la sección Ethernet mostrará detalles de la red, incluidos protocolo, dirección IP, puerta de enlace, y DNS Servidor.



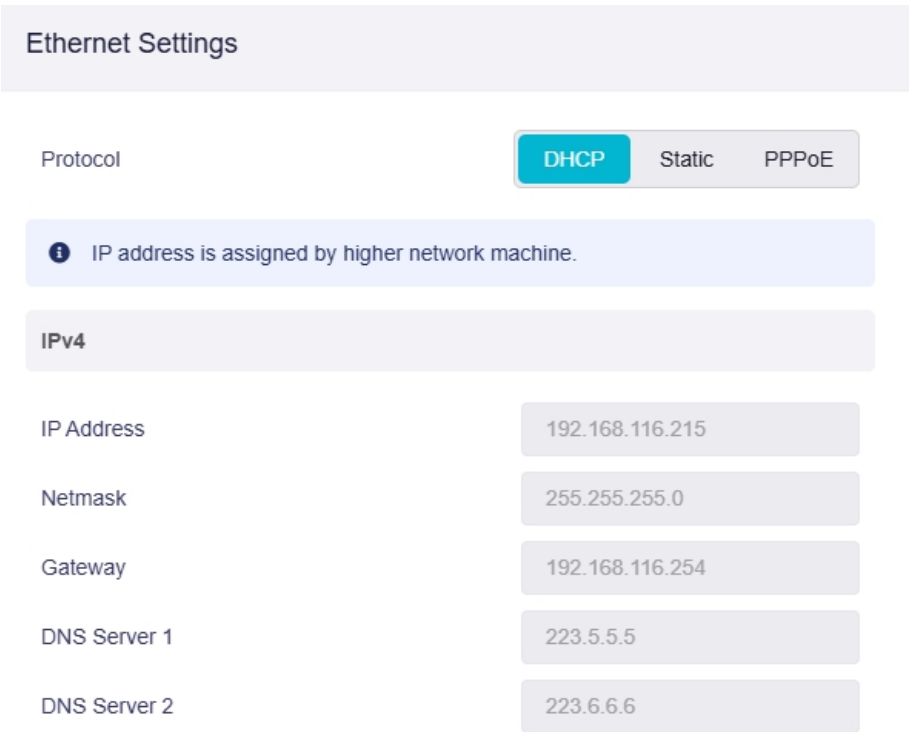
Protocolo

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



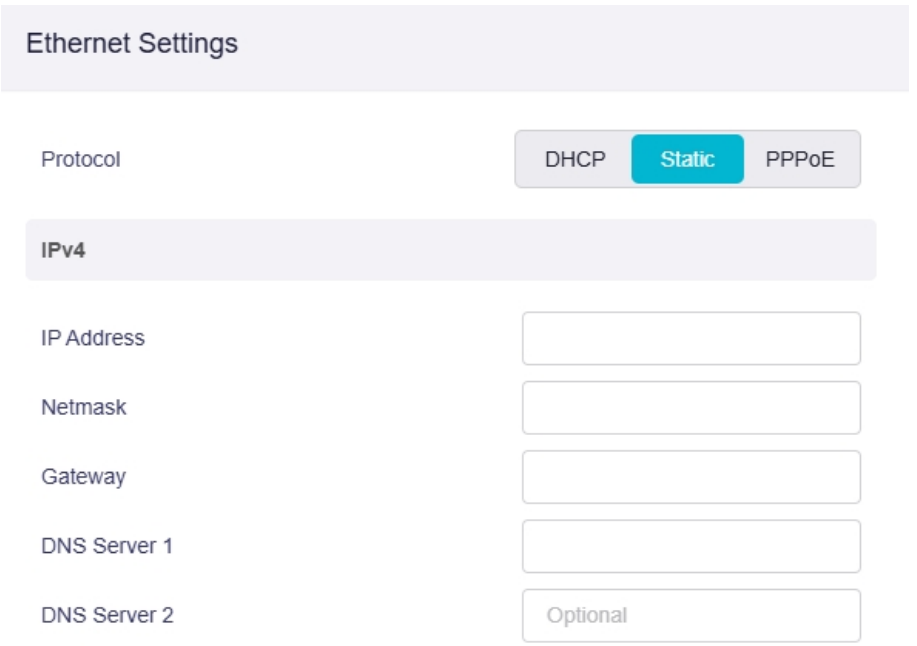
- **DHCP**

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



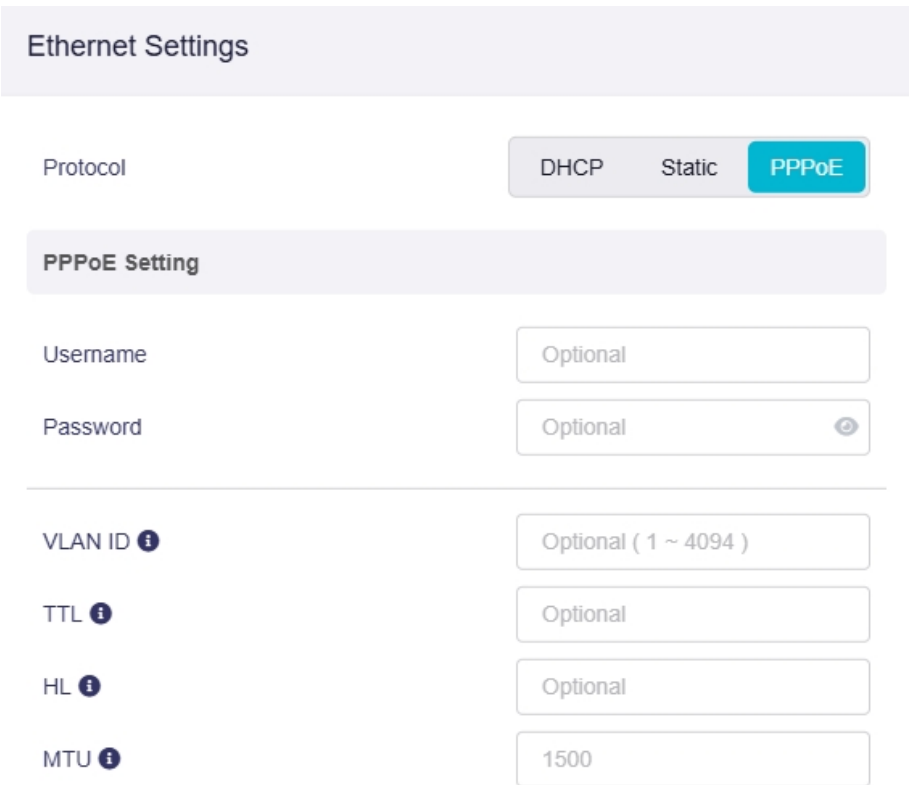
- **Estático**

  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).



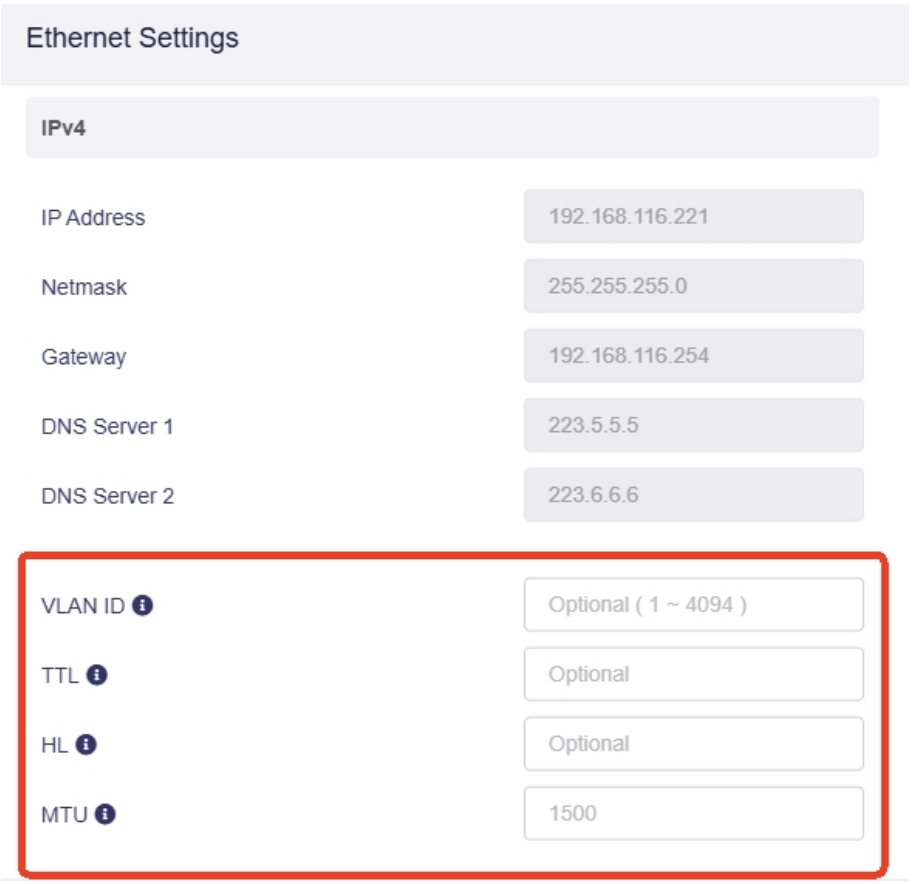
- **PPPoE**

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



Configuración avanzada

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



- **ID de VLAN**

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

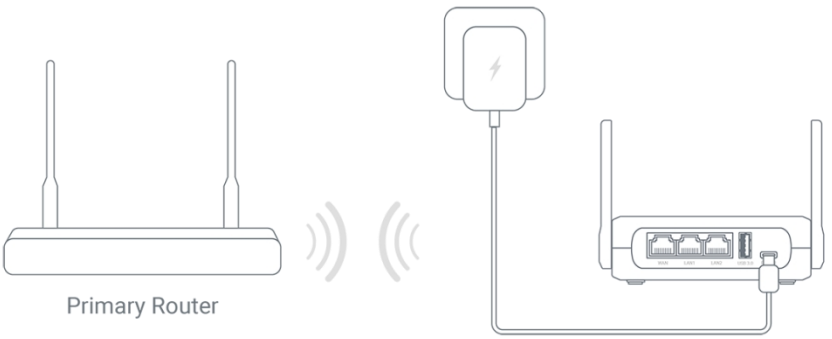
  TTL (Tiempo de vida) define el tiempo máximo que los paquetes pueden sobrevivir la red. De forma predeterminada, el enrutador disminuye en 1 el TTL de los paquetes entrantes de los dispositivos cliente antes de reenviarlos. Si necesita anularlo, puede establecer un valor fijo aquí. La configuración TTL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

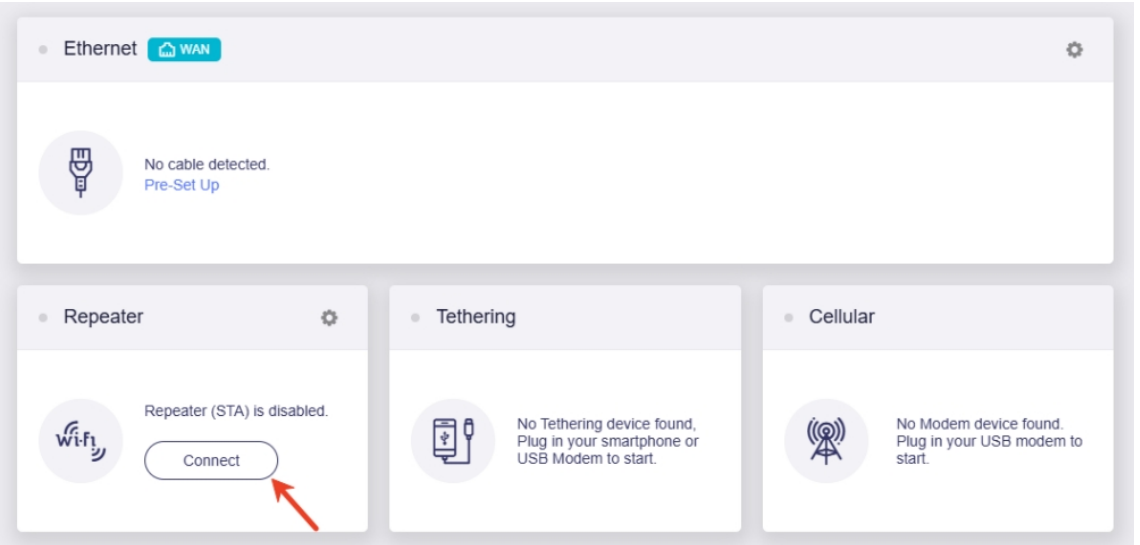
Conecte el enrutador como repetidor a la red inalámbrica existente para aumentar las señales de Wi-Fi-Fi y cree una red local aislada de la red principal. Cuando en hoteles o cafeterías con puntos de acceso públicos gratuitos, el uso de un repetidor no solo fortaleces Wi-Fi, sino que también proporcionas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



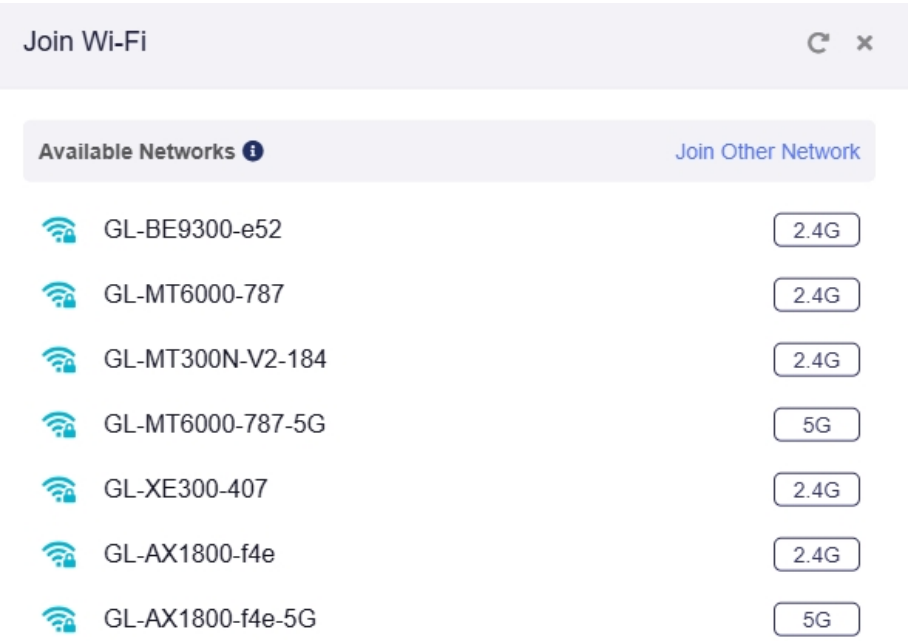
Función de repetidor GL.iNet funciona en modo WISP (Proveedor de servicios de Internet inalámbrico) de forma predeterminada, lo que significa que el enrutador creará su propia subred y actuará como un firewall para protegerlo de la red pública.

Configuración básica

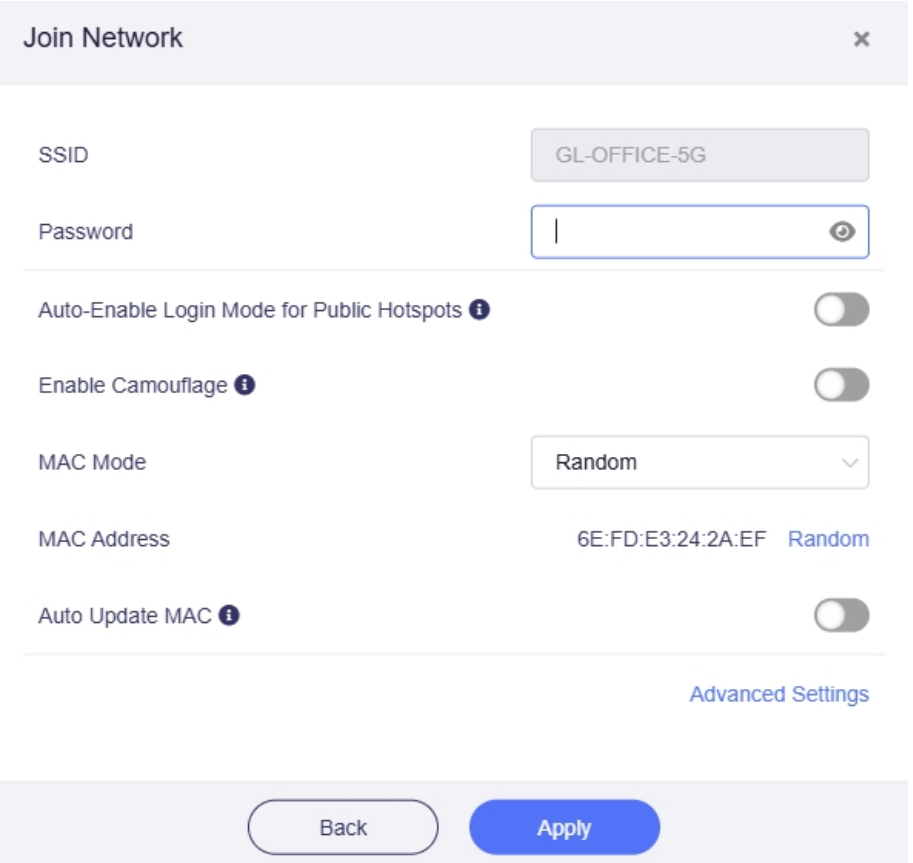
1. Inicie sesión en enrutador'panel de administración web y navegue a **INTERNET** -> **Repetidor**. Haga clic en **Conectar**.



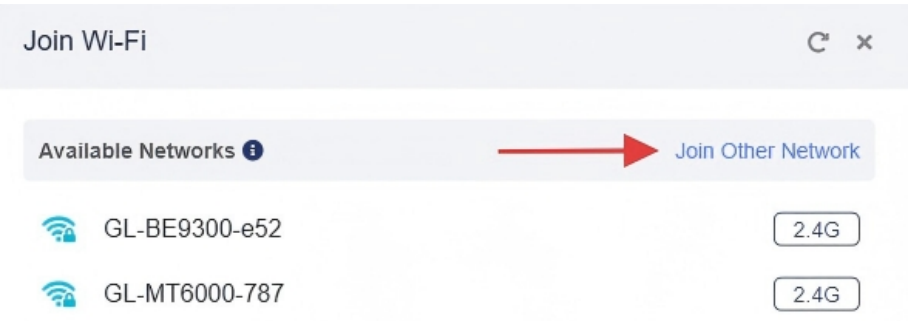
2. En la ventana emergente, celija la red Wi-Fi que desea conectarse de la lista de redes disponibles.



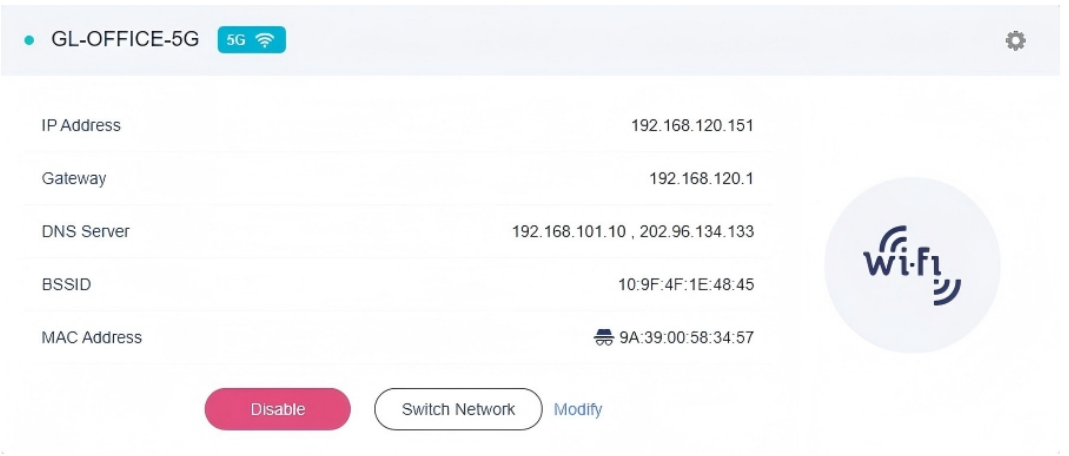
3. Eingrese la contraseña de Wi-Fi correcta y haga clic en **Aplicar**.



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

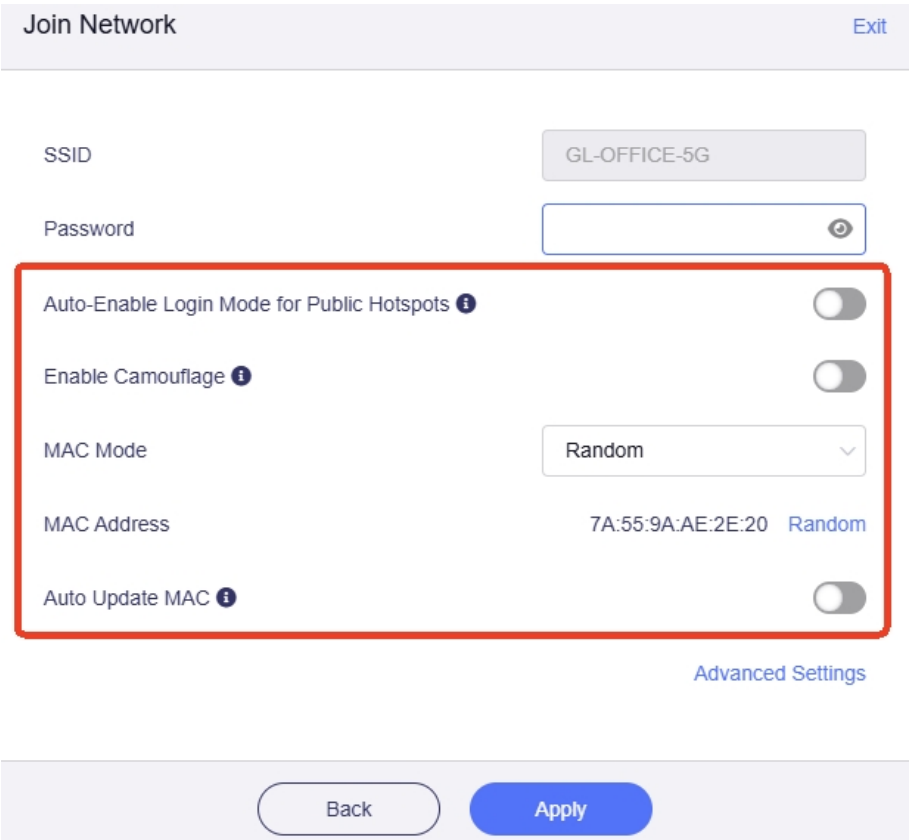


4. Espere un minuto hasta que el enrutador se conecte. Una vez conectado, la página se muestra a continuación.


GL-OFFICE-5G
5G
IP Address
192.168.120.151
Gateway
192.168.120.1
DNS Server
192.168.101.10 , 202.96.134.133
BSSID
10:9F:4F:1E:48:45
MAC Address
9A:39:00:58:34:57
Disable
Switch Network
Modify

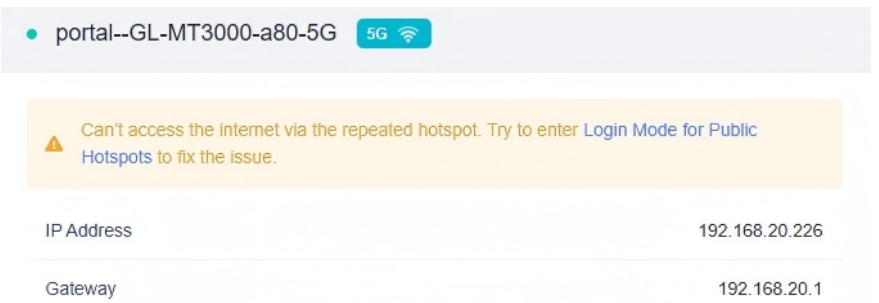
Configuración del punto de acceso público

Al conectar el enrutador a un punto de acceso público con un portal cautivo, se recomienda habilitare las siguientes características mejora 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 al modo de inicio de sesión de punto de acceso público cuandon 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 MAC dirección el enrutador utiliza para conectarse al punto de acceso público.

Fábrica	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 aparece en la lista, ingrese manualmente la dirección MAC que desea clonar. Tenga en cuenta que muchos dispositivos utilizan direcciones MAC aleatorias (a menudo denominadas dirección Wi-Fi privada o dirección de hardware aleatoria) cuando se conectan a redes Wi-Fi. Como resultado, es posible que la dirección MAC que se muestra aquí no coincida con la MAC física real del dispositivo.
Aleatorio	Genera automáticamente una dirección MAC aleatoria para la conexión.

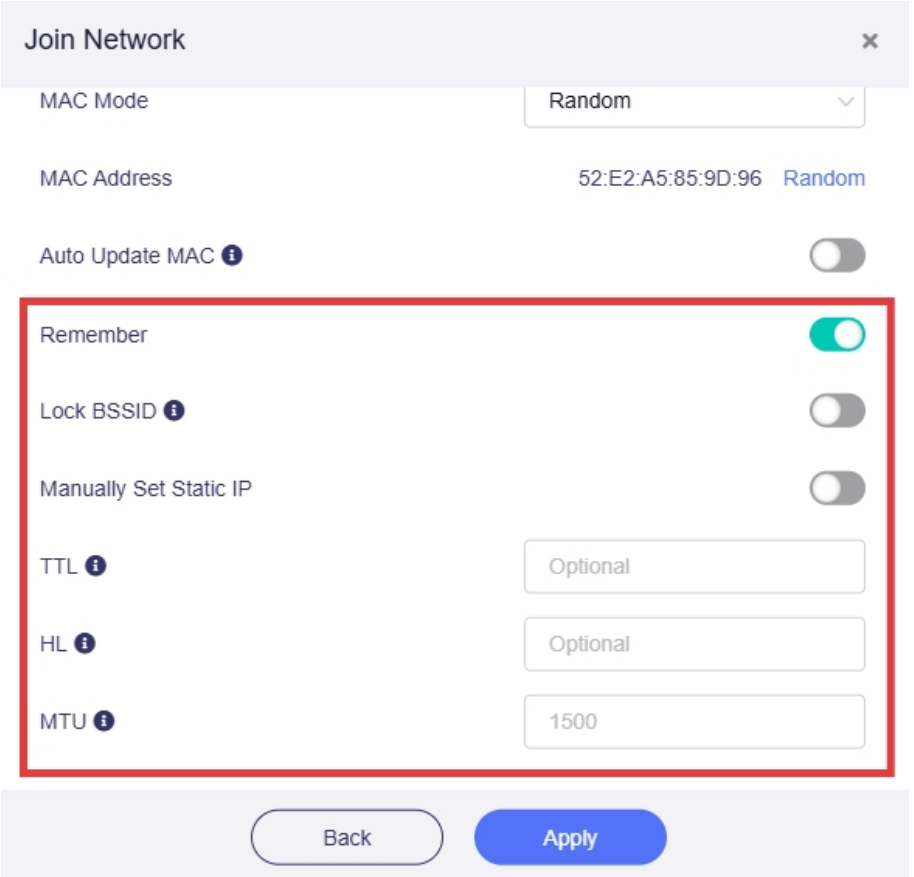
- **Actualización automática de MAC**

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

Al guardar la configuración de red, el Modo MAC, incluido cualquier clonado o aleatoria MAC 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.

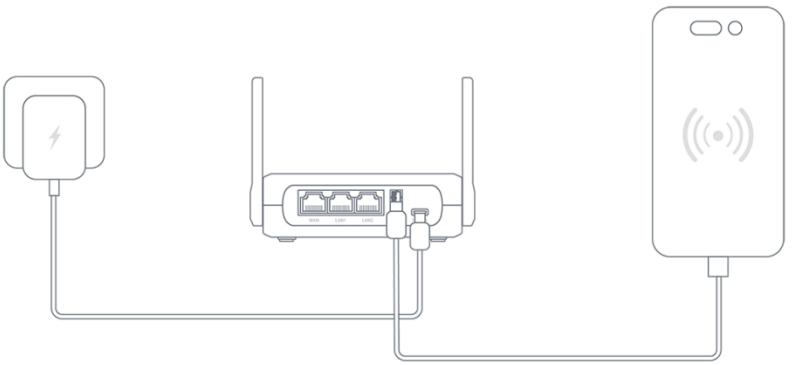


- **Recordar**: habilite esto para recordar la red Wi-Fi repetida actualmente.
- **Bloquear BSSID**: cuando esté habilitado, el enrutador se conectará solo al punto de acceso (AP) específico correspondiente al BSSID seleccionado, incluso cuando otros AP compartan el mismo SSID.
- **Configurar estática manualmente 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 (Límite de salto) 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

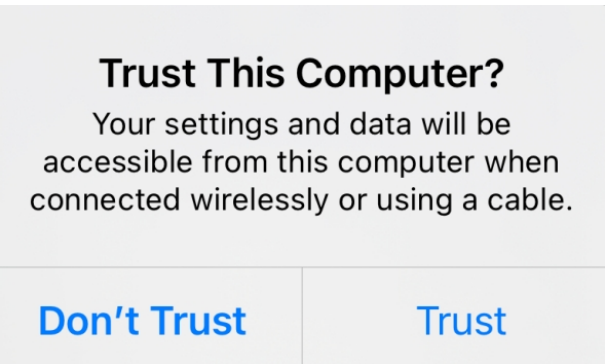
Cconexión de un inteligenteteléfono al enrutador a través de un cable USB se llama Tethering, que puede compartir la red de datos móviles del dispositivo (por ejemplo, 4G/5G) con el enrutador. Este es un método para el acceso temporal ia Internet, especialmente cuando al aire libre o en áreas sin banda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



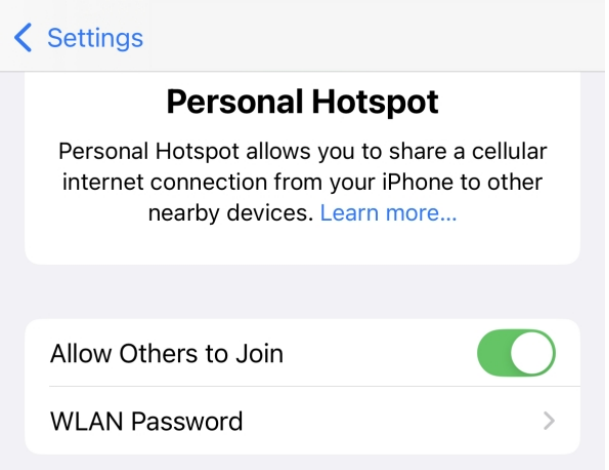
El módem sin host funciona en Tethering como bien durante la configuración del módem.
Nota: Algunos operadores de telefonía móvil limitan o cobran más por la conexión. Te recomendamos consultar con tu operador.

Conexión compartida desde un iPhone

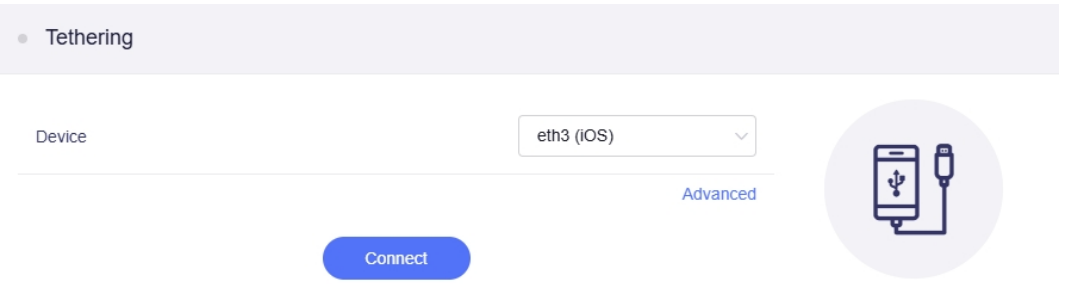
1. Conecte un iPhone al puerto USB del enrutador mediante un cable USB. Aparecerá un cuadro de diálogo del sistema preguntando si se debe confiar en el dispositivo. Toque **Confiar** para continuar.



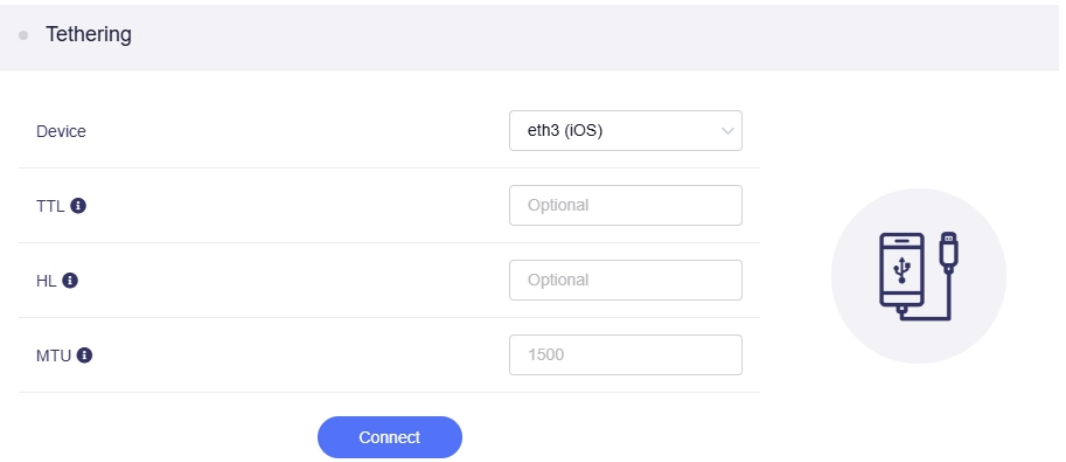
2. Ir a iPhone **Configuración** > **Punto de acceso personal**. Activar **Permitir que otros se unan**.



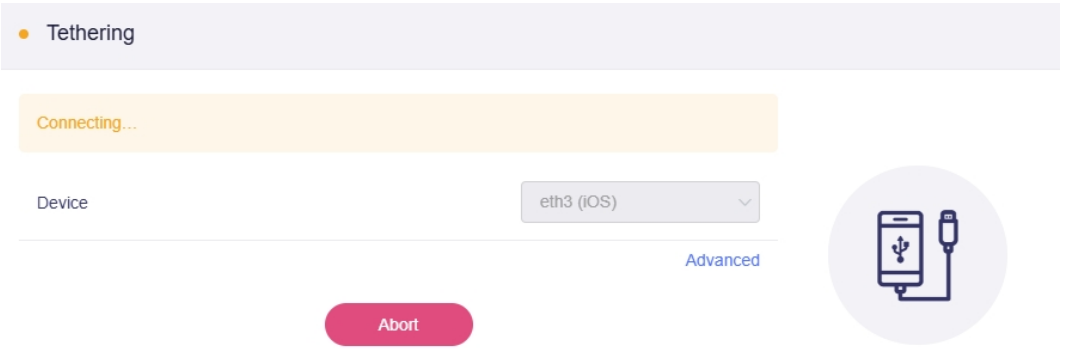
3. Conecte una computadora u otro teléfono al enrutador. Inicie sesión en el panel de administración web del enrutador y navegue hasta **INTERNET** > **Conexión**, luego haga clic en **Conectar**.



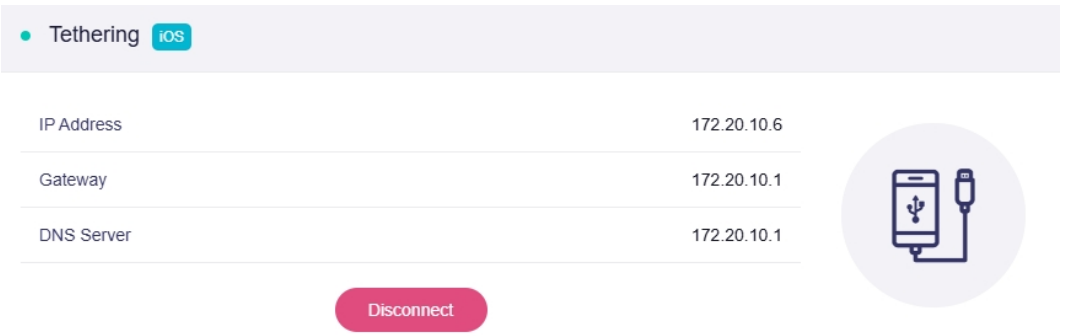
Si necesita establecer configuraciones avanzadas, como TTL, HL y MTU, haga clic **Avanzado** para personalizar estas configuraciones, luego haga clic en **Conectar**.



4. Comenzará a conectarse.

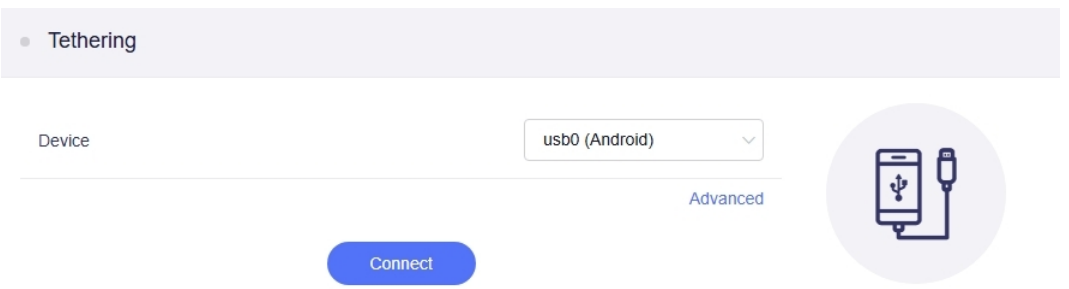


Una vez conectado, thesta página muestra los detalles.

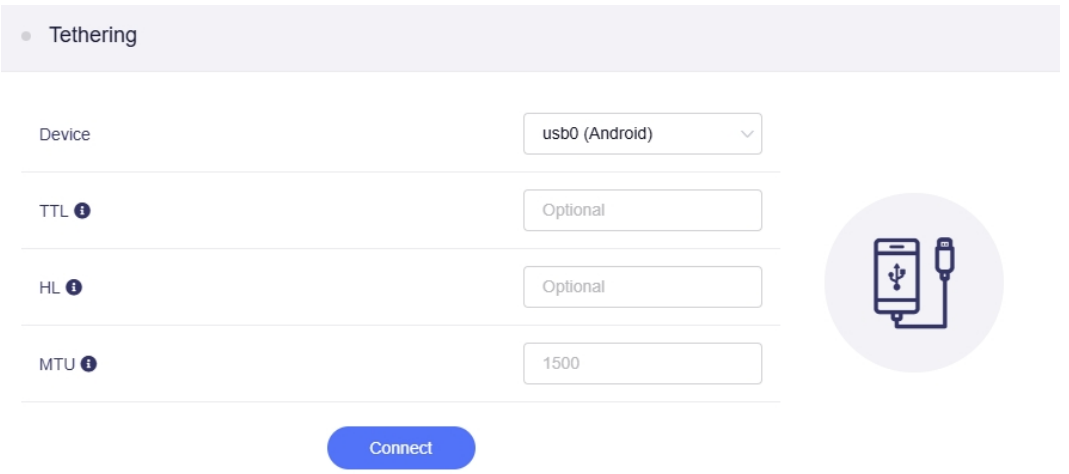


Conexión compartida desde Android

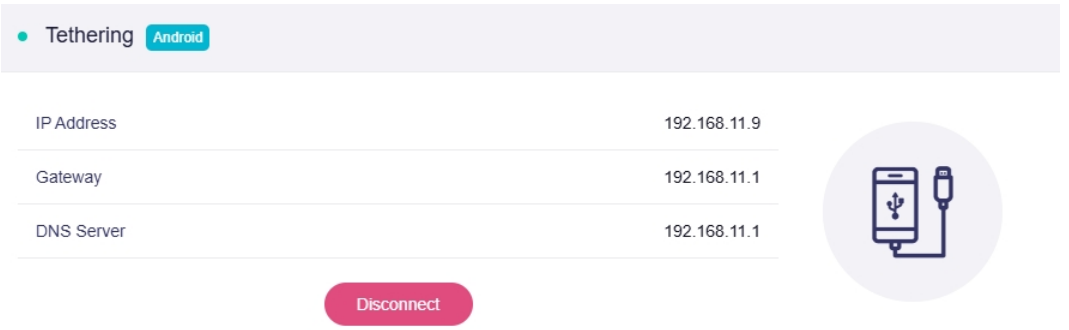
1. Conecta un teléfono Android al puerto USB del enrutador mediante un cable USB. Puede aparecer un cuadro de diálogo del sistema preguntando USB preferencias.
   Selecciona **Anclaje a red USB** o **Archivo Transferir** si se te solicita.
2. Vaya a la **Configuración** > **Red e Internet** > **Punto de acceso personal**. Habilite **Punto de acceso personal** o **Anclaje a red USB**.
   (Los pasos para habilitar el Anclaje a red USB varían según la marca. Verifique la configuración de su dispositivo para conocer la ubicación exacta y comuníquese con el soporte técnico de su fabricante si es necesario).
3. Conecte una computadora u otro teléfono al enrutador, luego inicie sesión en el panel de administración web del enrutador, navegue a **INTERNET** > **Conexión**. Click **Conectar**.



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



4. Una vez conectado, estapágina mostrará el Anclaje a red estado de conexión.



Solución de problemas

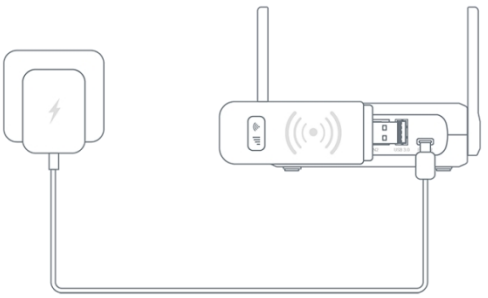
Si falla la conexión , intente estos pasos para solucionar el problema:

- 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.

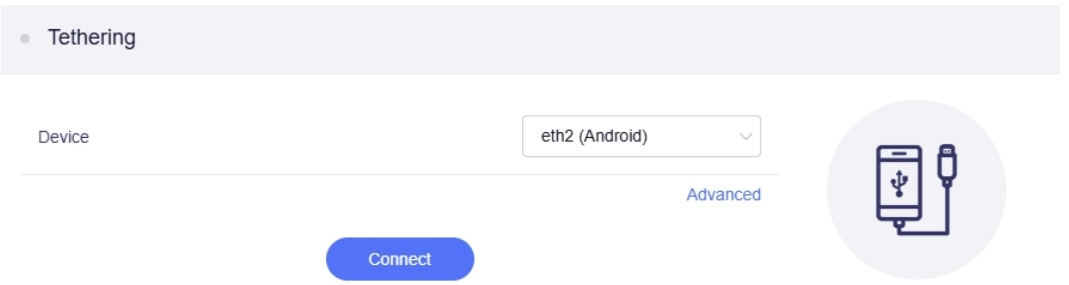
4.2.4 Conectarse a Internet mediante un módem USB

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. 'Interfaz de anclaje a red o celular.

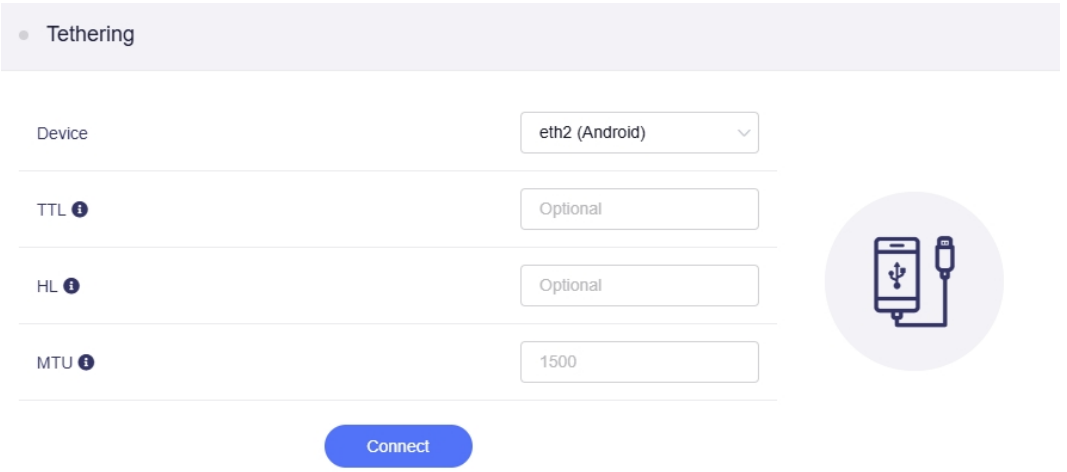


Siga los pasos a continuación para conectar su enrutador a Internet a través de un módem USB.

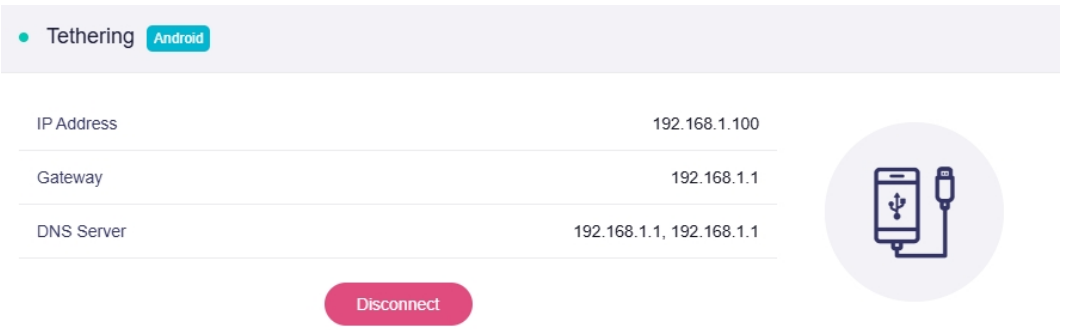
1. Plug un módem USB con una tarjeta SIM preinstalada en el puerto USB del enrutador' antes de encenderlo.
2. Inicie sesión en el enrutador's web admin panel y navegue hasta **INTERNET** > **Anclaje**. Haga clic en **Conectar**.



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

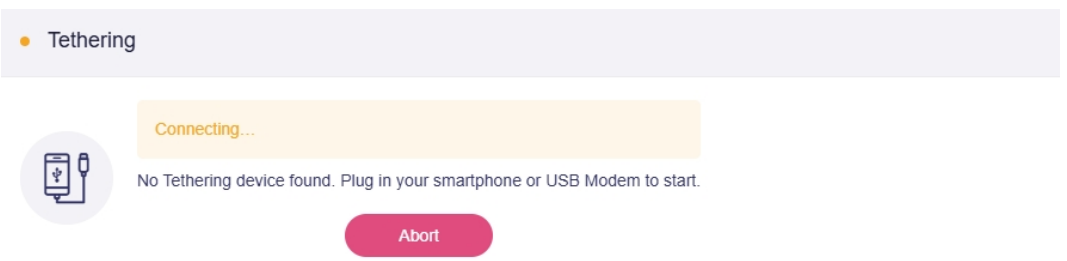


3. Comenzará a conectarse. Una vez conectado, esta página mostrará los red detalles.



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”.



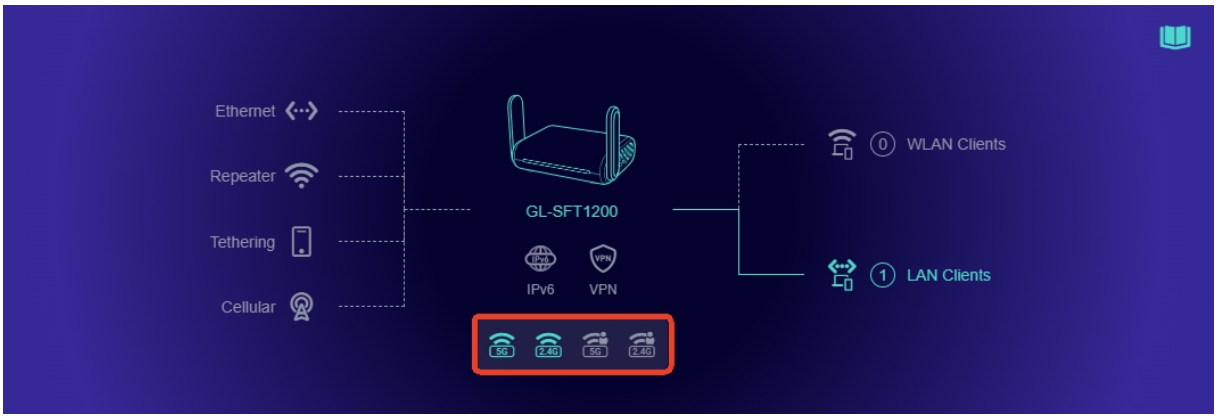
Capítulo 5

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 están habilitadas de forma predeterminada, y el ícono de Wi-Fi correspondiente se iluminará debajo de la imagen del modelo del dispositivo en INTERNET.



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

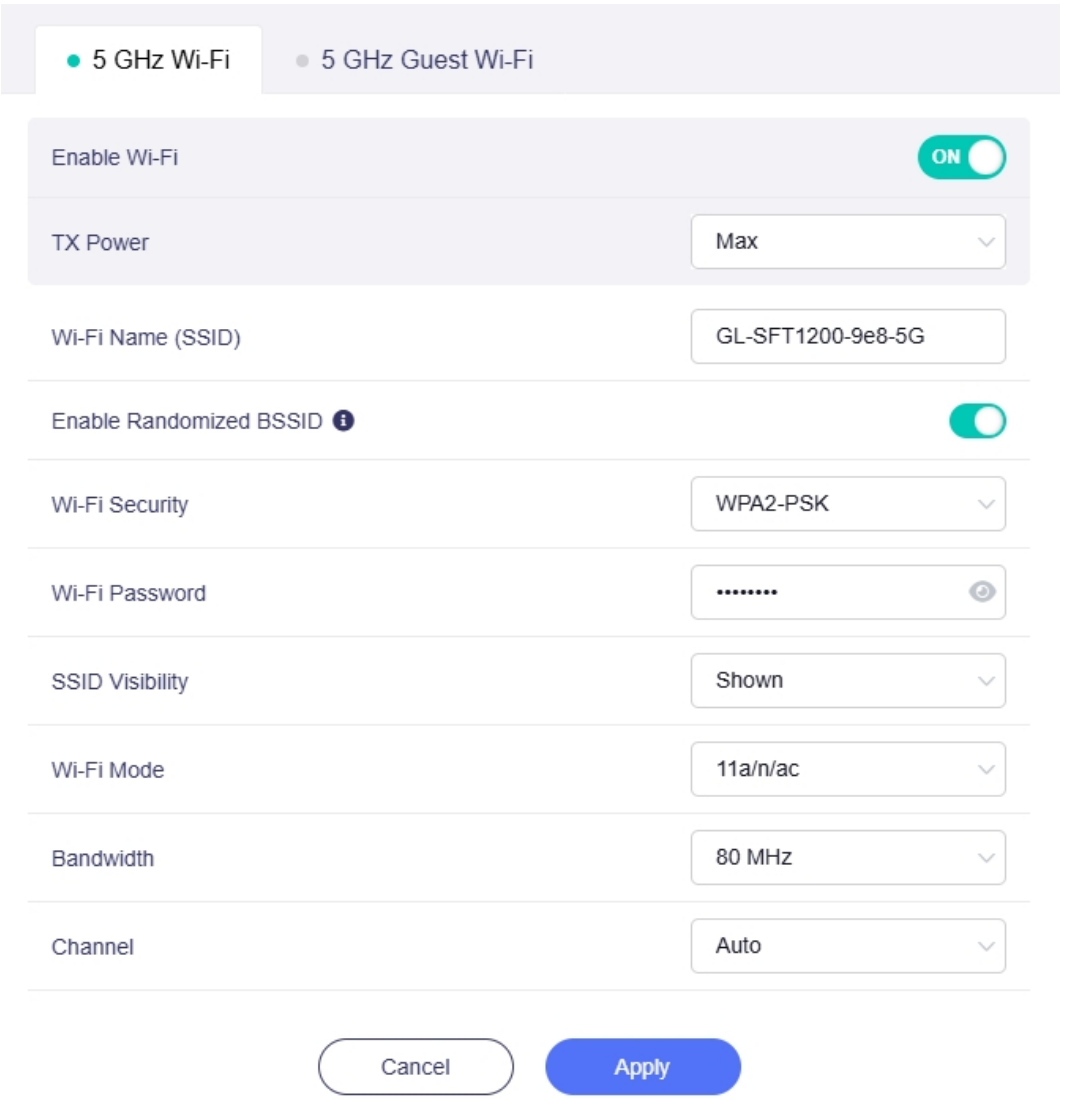


5.2 Configuración inalámbrica

Inicie sesión en el panel de administración web del enrutador y navegue hasta **Inalámbrica**. La página inalámbrica muestra la configuración de Wi-Fi del enrutador's 2,4 GHz y 5 GHz, con cada dividido en Wi principal-Fi y Wi-Fi para invitados-Redes Fi para una administración flexible .

5.2.1 Wi-Fi de 5 GHz

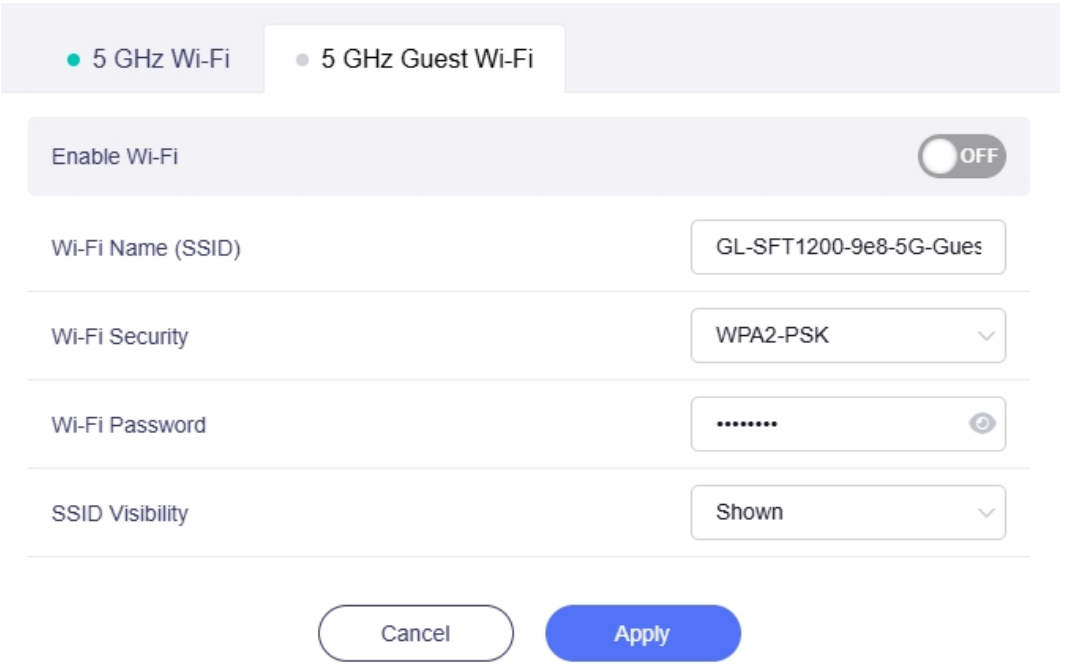
El principal de 5 GHz Wi-Fi le permite configurar múltiples ajustes, incluyendo habilitar/deshabilitar Wi-Fi, configurar la potencia de TX, habilitar/deshabilitar BSSID aleatorio, configurar Wi-Fi nombre (SSID), seguridad, contraseña, visibilidad de SSID, modo, ancho de banda y canal.



Nota:

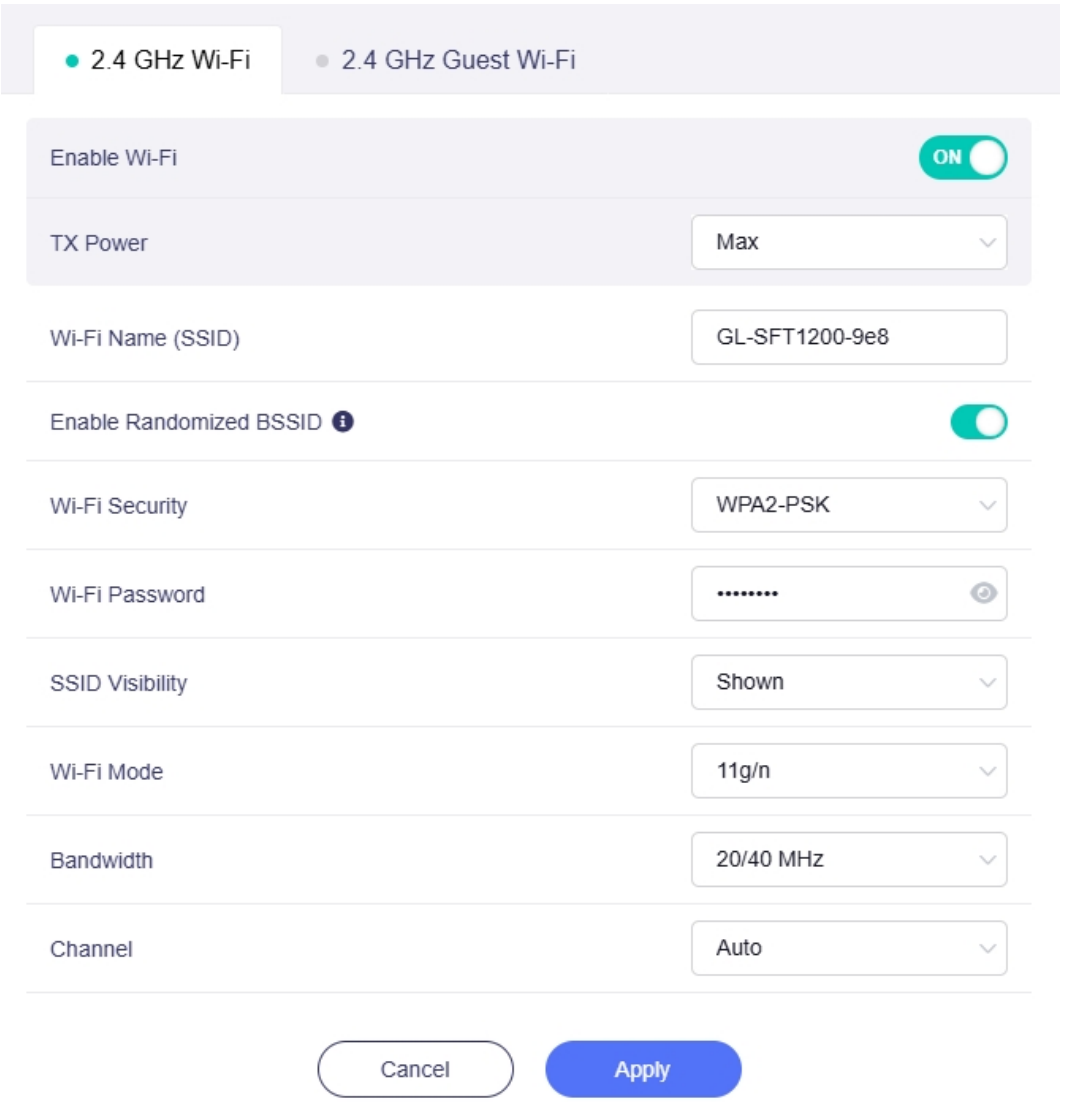
1. **BSSID aleatorio** está habilitado de forma predeterminada. Ayuda a evitar que el enrutador sea rastreado a través de un BSSID fijo, ya que los dispositivos cliente pueden informar BSSID cercanos y sus propios datos de ubicación a los proveedores de sistemas operativos/dispositivos, quienes los utilizan para crear una base de datos de BSSID a ubicación. Cuando está habilitado, el enrutador utiliza un BSSID generado aleatoriamente y lo renueva en cada reinicio, por lo que el BSSID no se puede vincular a una ubicación fija.
2. El **Ancho de banda** y **Canal** nono se puede modificar cuando el enrutador está configurado como a repetidor, ya que siguen el de la red repetida.

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



5.2.2 Wi-Fi de 2,4 GHz

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



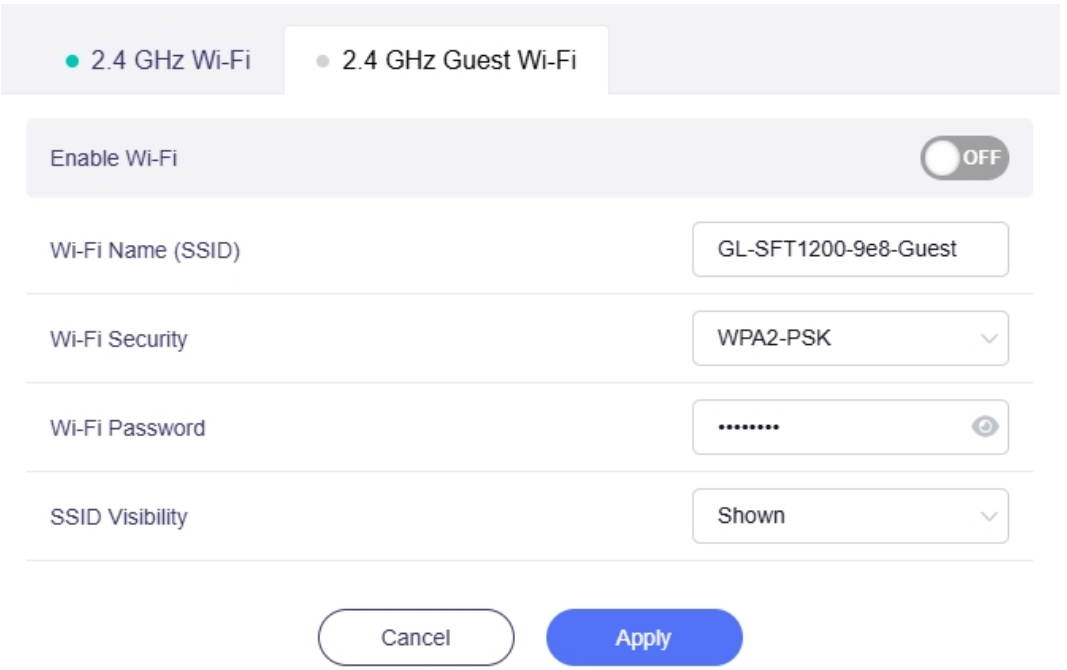
Nota:

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

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

2. El **Ancho de banda** y **Canal** no se pueden modificar cuando no se modificará cuando el enrutador se configura como a repeater, ya que siguen el de la red repetida.

El 2,4 GHz Invitado Wi-Fi le permite usted configurar configuraciones simplificadas , incluidag habilitación/ deshabilitar Wi-Fi, configurar nombre de Wi-Fi (SSID), seguridad, contraseña y visibilidad de SSID.



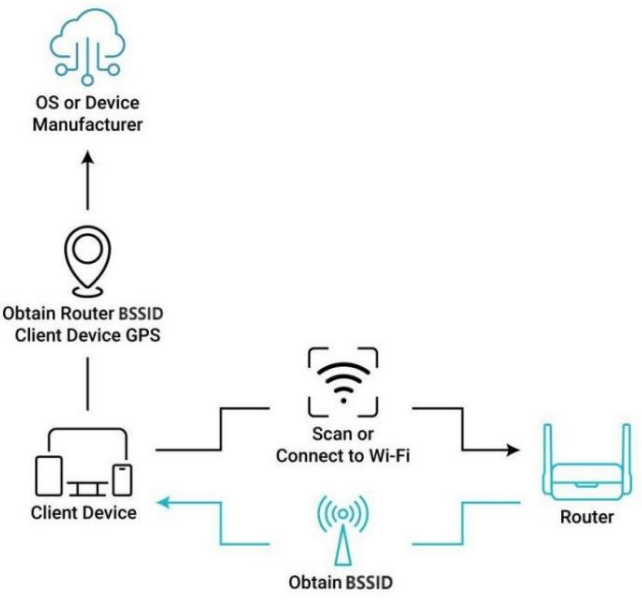
5.2.3 BSSID aleatorio

BSSID aleatorio es una función de privacidad disponible desde el firmware v4.6 y habilitada de forma predeterminada. Evita que su enrutador sea localizado y rastreado a través de un BSSID Wi-Fi fijo (la dirección MAC de la interfaz inalámbrica del enrutador).

Por qué un BSSID fijo es un riesgo para la privacidad

Los sistemas operativos móviles (por ejemplo, Android e iOS) dependen del posicionamiento Wi-Fi de fuentes múltiples para proporcionar servicios de ubicación:

1. Los dispositivos del cliente (teléfonos, computadoras portátiles) cargan periódicamente los BSSID que pueden ver, junto con su propia ubicación derivada del GPS, al servidor del proveedor del sistema operativo/dispositivo.
2. Los proveedores agregan estos datos en una base de datos global de BSSID a ubicación.
3. Cualquier dispositivo con Wi-Fi habilitado, incluso sin GPS, puede consultar esa base de datos para estimar su ubicación a partir de los BSSID que lo rodean.
4. Como resultado, un enrutador con un BSSID fijo actúa como una baliza de ubicación estacionaria: puede ser está geolocalizado de forma remota y sus movimientos (por ejemplo, cuando viaja con él) se pueden rastrear a lo largo del tiempo. Los atacantes también pueden consultar dichas bases de datos para localizar enrutadores o tomar huellas digitales a través de la información del proveedor (OUI) del BSSID.



Cómo te protege el BSSID aleatorio

Cuando esta función está habilitada, el enrutador genera un BSSID aleatorio y lo renueva en cada arranque. Dado que el BSSID sigue cambiando, ya no se puede vincular a una ubicación fija en las bases de datos del proveedor, lo que rompe la asociación BSSID-ubicación utilizada para el seguimiento.

Estado	Comportamiento
Habilitado (predeterminado)	Se genera y renueva un nuevo BSSID aleatorio en cada inicio
Deshabilitado	El enrutador utiliza su dirección MAC real de fábrica como BSSID

Notas:

1. El BSSID cambia solo cuando el enrutador se reinicia; permanece igual durante una sesión en ejecución.
2. Para Wi-Fi para invitados, el BSSID sigue siendo consistente con el BSSID de Wi-Fi principal en la misma banda de frecuencia.
3. El BSSID aleatorio bloquea el seguimiento a través del BSSID del enrutador, pero no impide que los dispositivos cliente informen su propia ubicación y no es una solución de privacidad completa: características de SSID, canal y señal. todavía se puede observar.

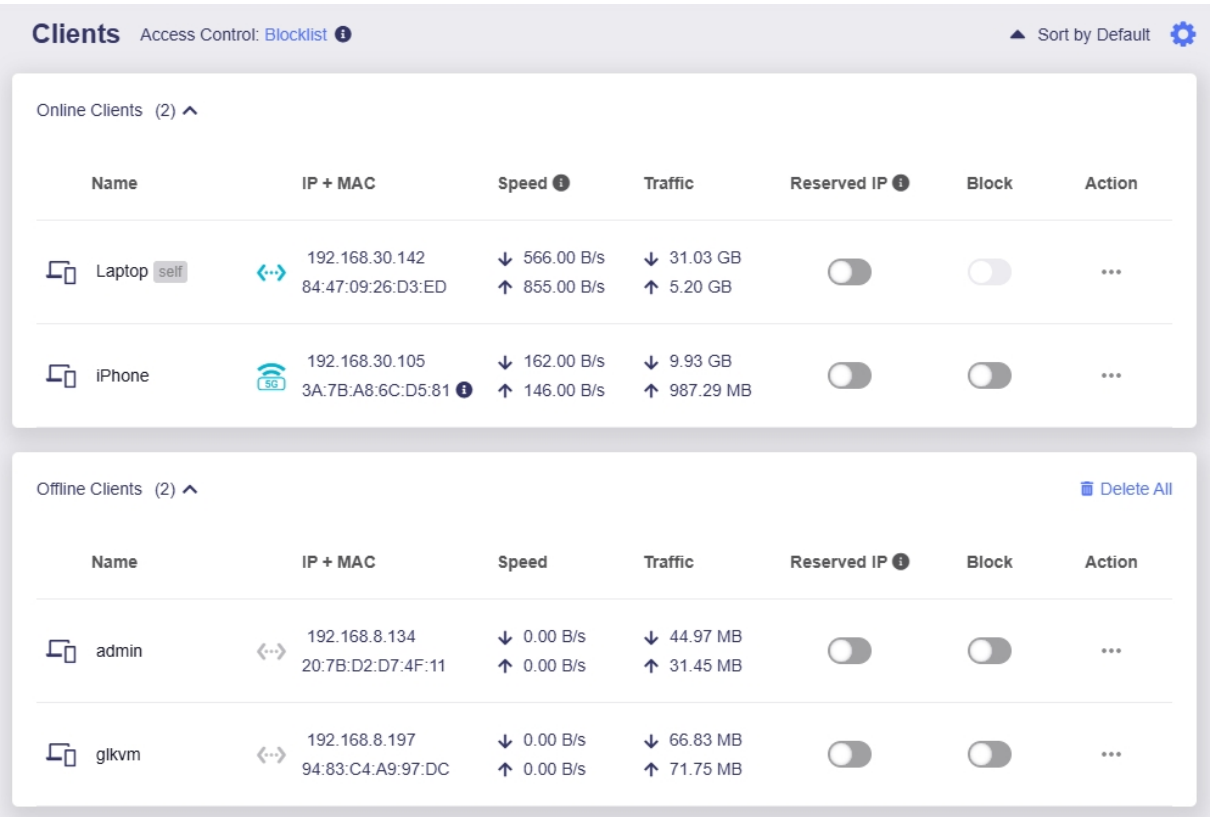
Capítulo 6

Clientes

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

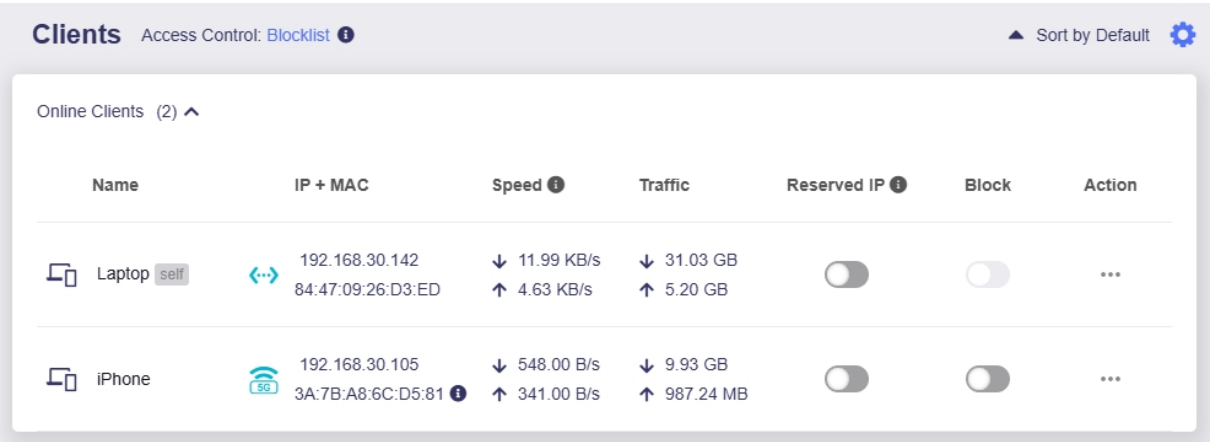
Inicie sesión en el enrutador’s web admin panel y navega hasta **CLIENTES**.

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



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

6.1 Detalles del dispositivo



1. **Nombre del dispositivo**

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

2. **Dirección IP y MAC**

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



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

3. **Velocidad**

   La tercera columna muestra la velocidad de Internet del dispositivo conectado. Estaes 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 data).

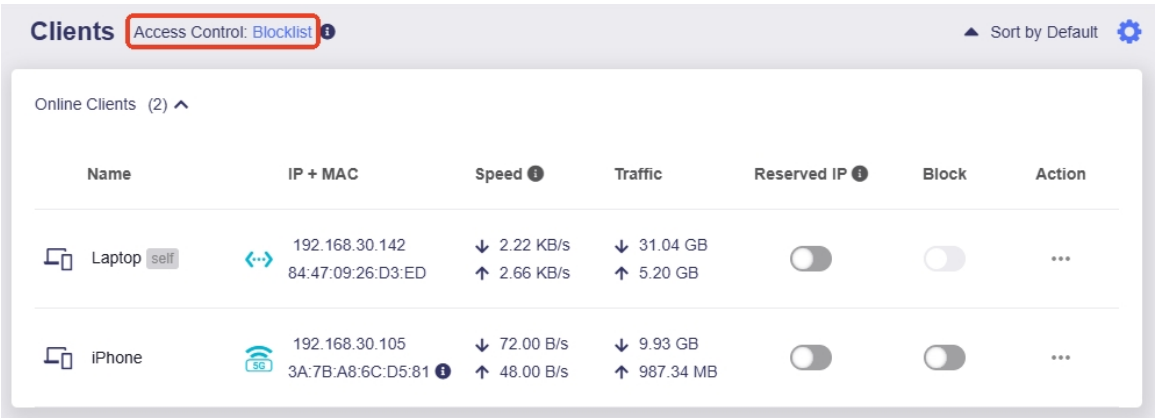
4. **Tráfico**: La cuarta columna muestra el tráfico de Internet del dispositivo conectado.

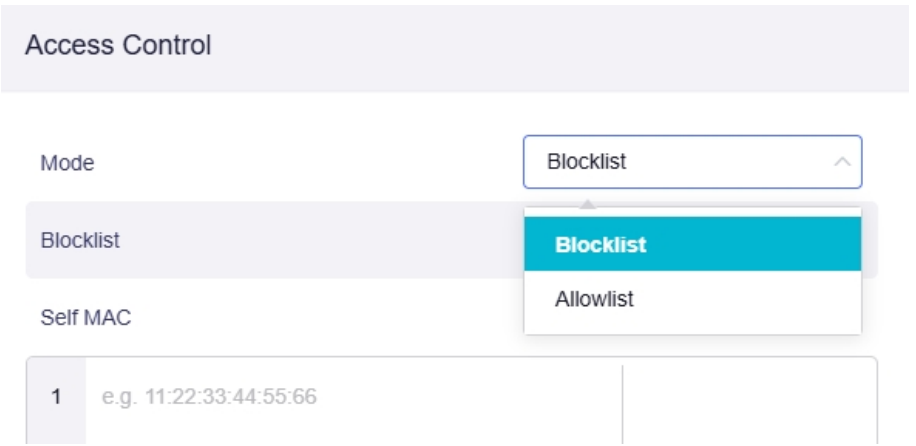
5. **Reservar IP**

   En la quinta columna, puede reservar la dirección IP para dispositivo conectado con un clic. Cuando especifica una dirección IP reservada para un cliente dentro de la red de área local,, siempre recibirá la misma Dirección IP cada vez que se conecta al el enrutador.

6. **Lista de bloqueo**

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



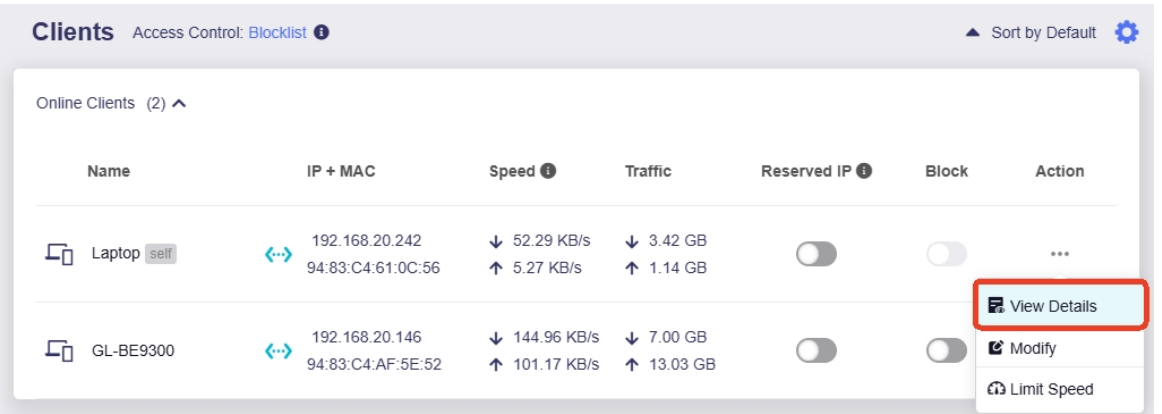


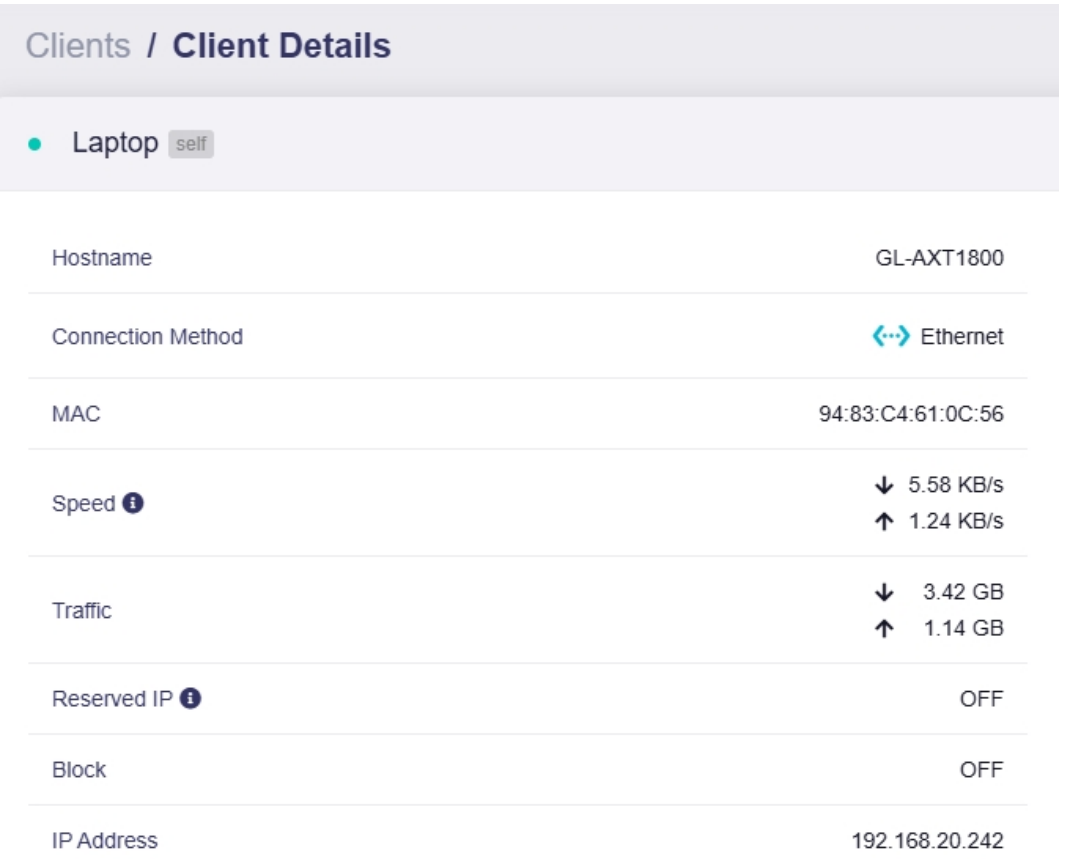
- **Lista negra**: dispositivos con direcciones MAC en la lista negrano puede conectarse a este enrutador. Tenga en cuenta que el bloqueo del cliente se basa en la dirección MAC del dispositivo. Si el dispositivo bloqueado usa una dirección MAC diferente la próxima vez, aún podrá conectarse al enrutador.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

6.2 Acción

1. **Ver detalles**

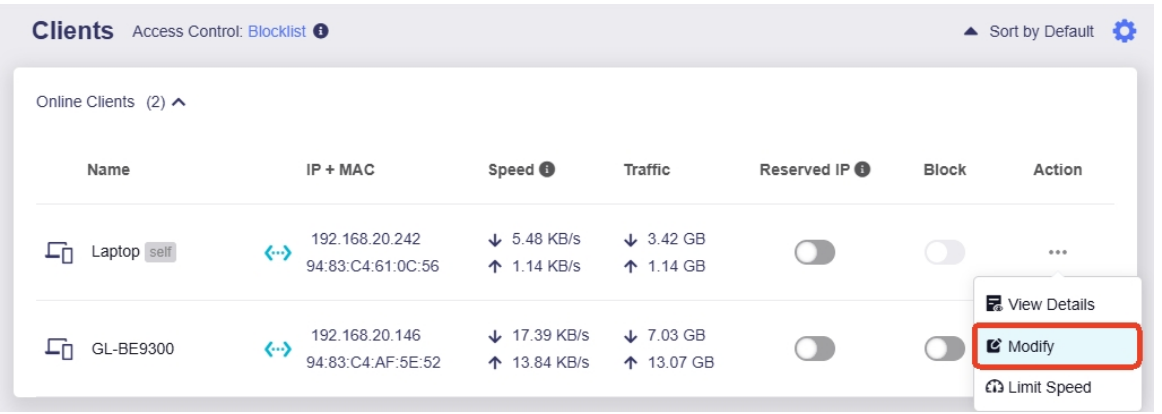
   Haga clic en el icono de tres puntos en la **Acción** columna y haga clic en **Ver detalles** en el menú desplegable para ver los detalles del dispositivo en una sola página.

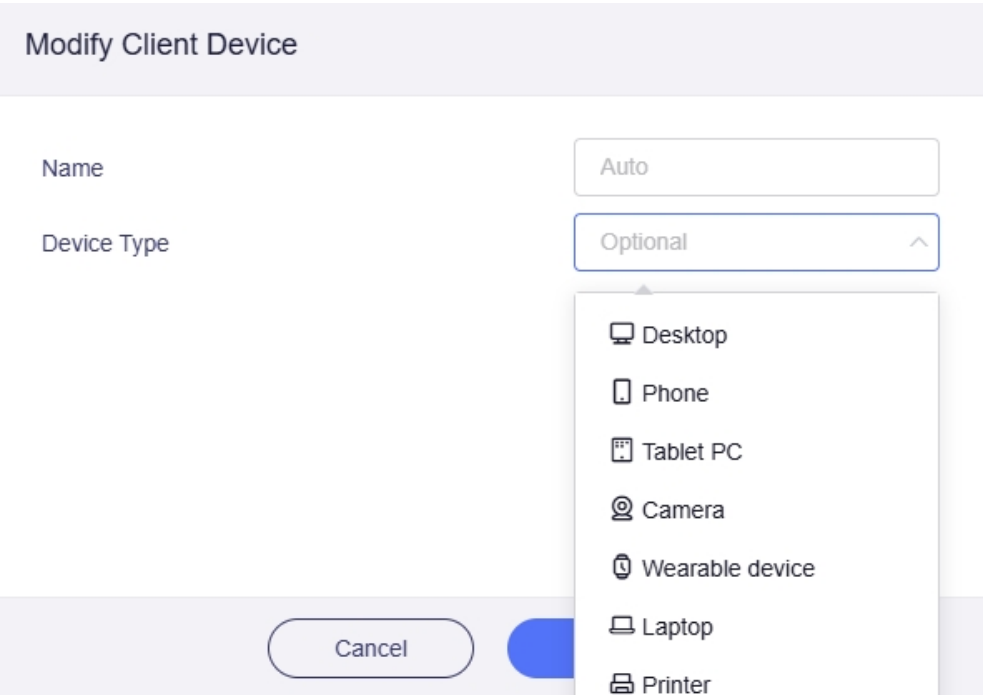




2. **Modificar**

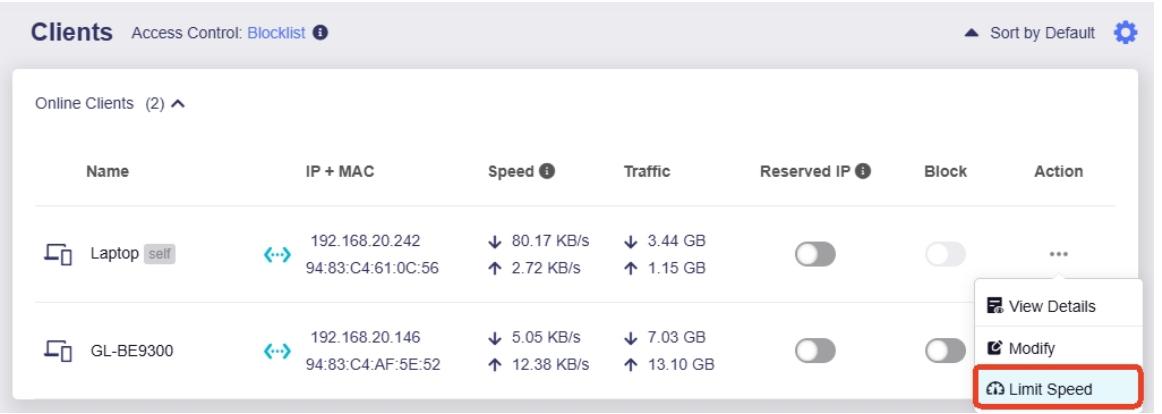
Haga clic en el icono de tres puntos en la columna **Acción** y haga clic en **Modificar** de el menú desplegable para modificar el nombre y tipo del dispositivo.



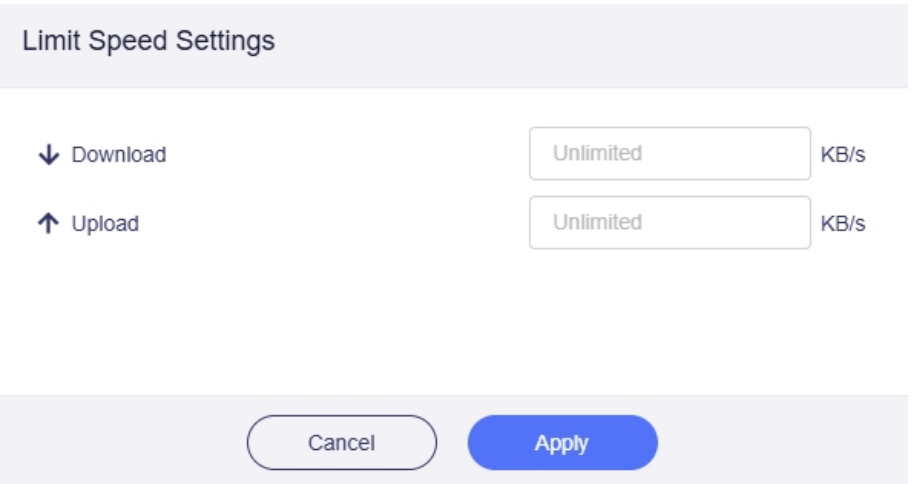


3. **Limitar velocidad**

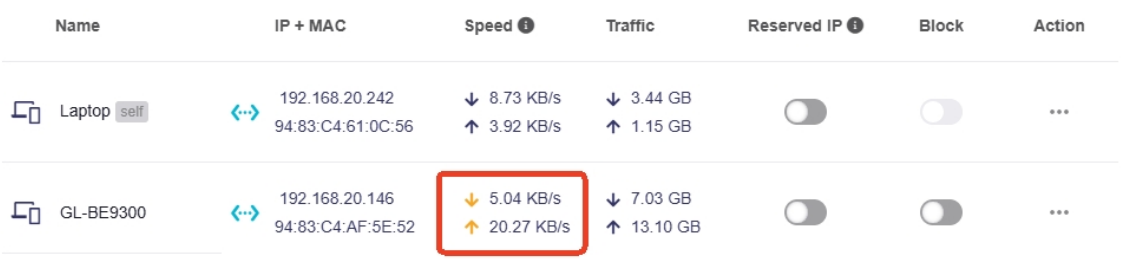
Haga clic en el icono de tres puntos en la **Acción** columna y haga clic en **Limitar velocidad** en el menú desplegable.



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



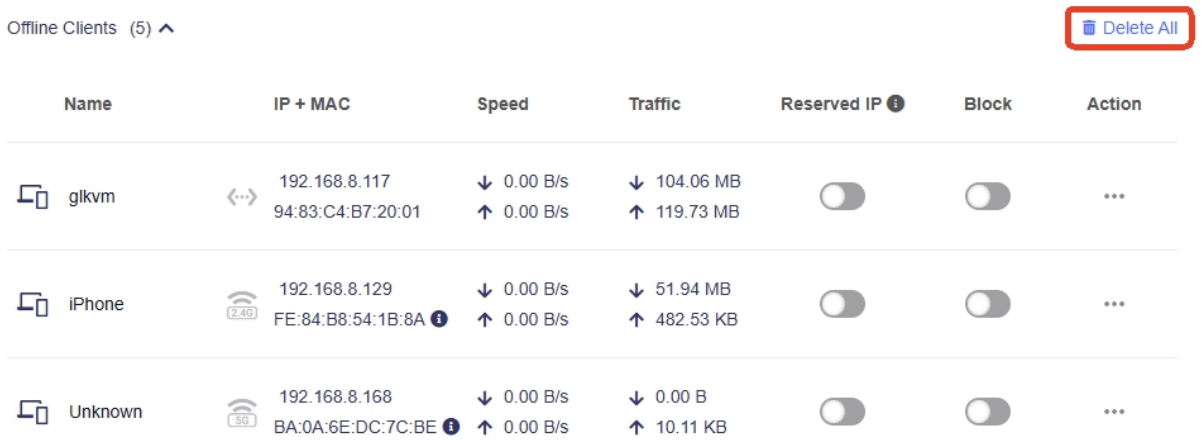
Si se ha aplicado una limitación de velocidad a un dispositivo, las flechas de velocidad de carga/descarga se volverán amarillas.



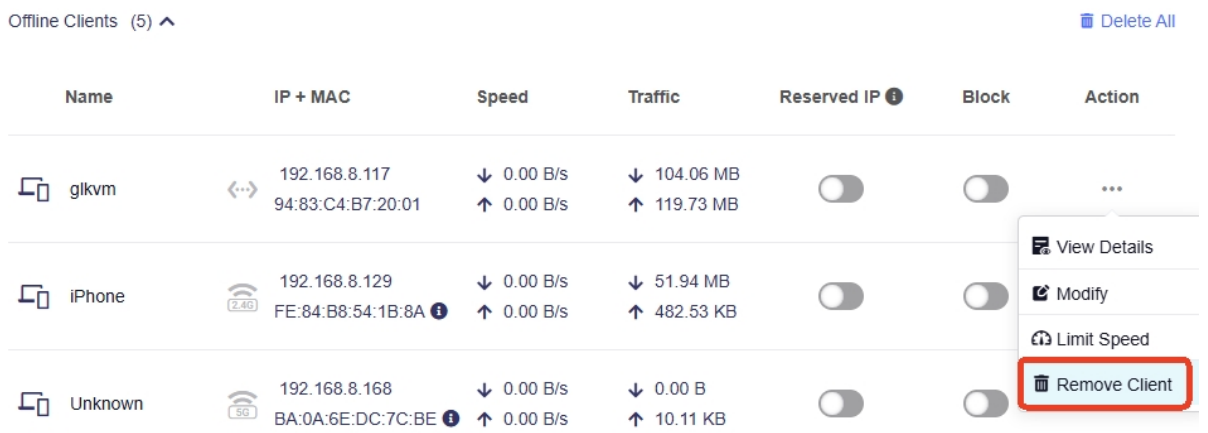
Consejo: Si la opción Limitar velocidad está activada no visible, vaya a **RED** > **Aceleración de red** y desactívela. La opción Limitar velocidad estará disponible.

6.3 Eliminar clientes

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

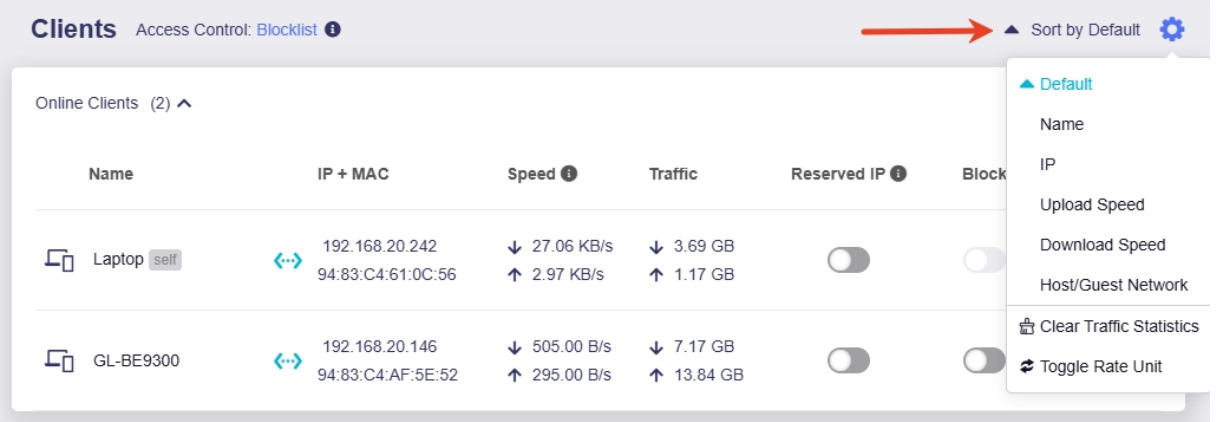


Si desea eliminar a cliente específico, haga clic en el ícono de tres puntos en la columna **Acción**, luego haga clic en **Quitar Cliente** desde el menú desplegable.



6.4 Ordenar

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



La clasificación predeterminadaing reglas son de la siguiente manera:

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

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.

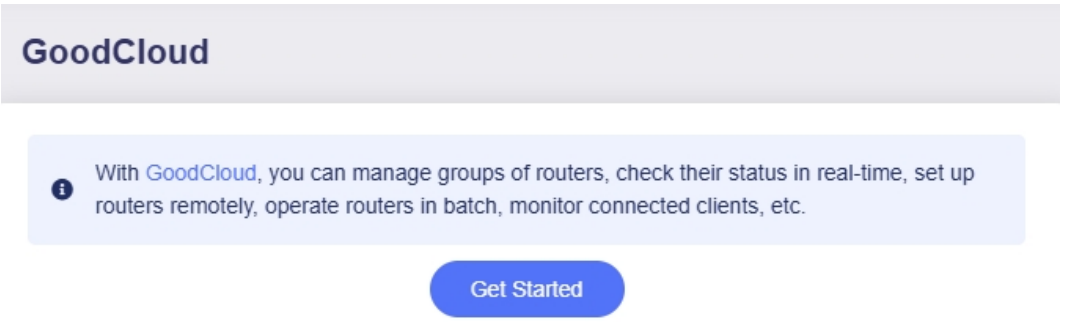
Con GoodCloud, puede:

- 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

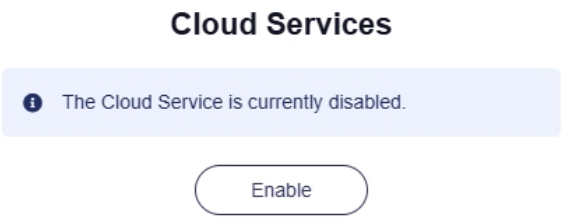
Algunas funciones están disponibles en el plan Enterprise y el plan VAR (revendedor de valor agregado). Consulte aquí para obtener más detalles.

7.1.1 Habilitar GoodCloud

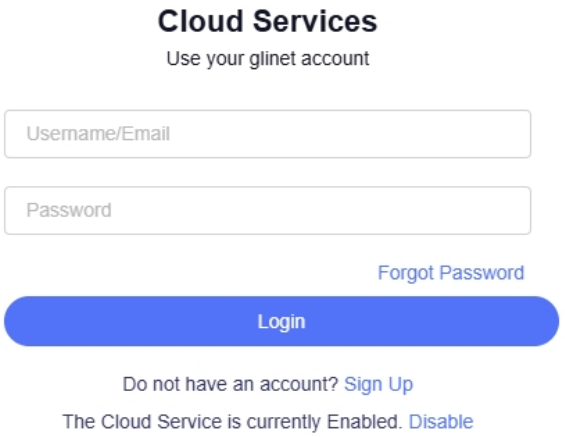
1. Inicie sesión en el panel de administración web de su enrutador', navegue hasta **SERVICIO EN LA NUBE** > **GoodCloud**, y click **Obtener Started.**



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



3. Log en con su cuenta GL.iNet Cloud. Si'no tienes una cuenta, regístrate para obtener una e inicie sesión. Una vez haya iniciado sesión, el enrutador estará vinculado a su cuenta automáticamente.

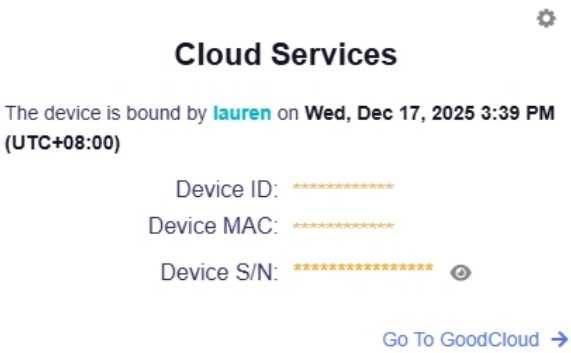


Consejos:

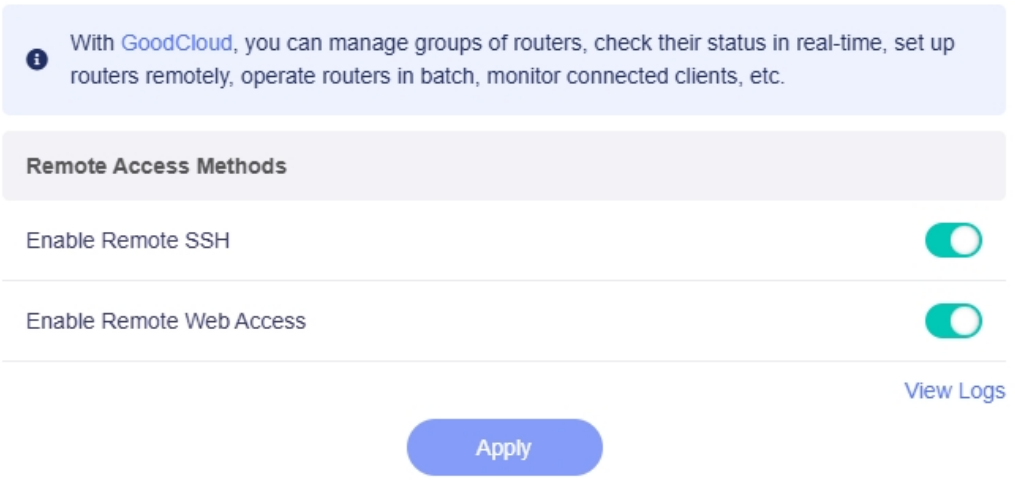
- Los pasos de vinculación de GoodCloud difieren según la versión del firmware.

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

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



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



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

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

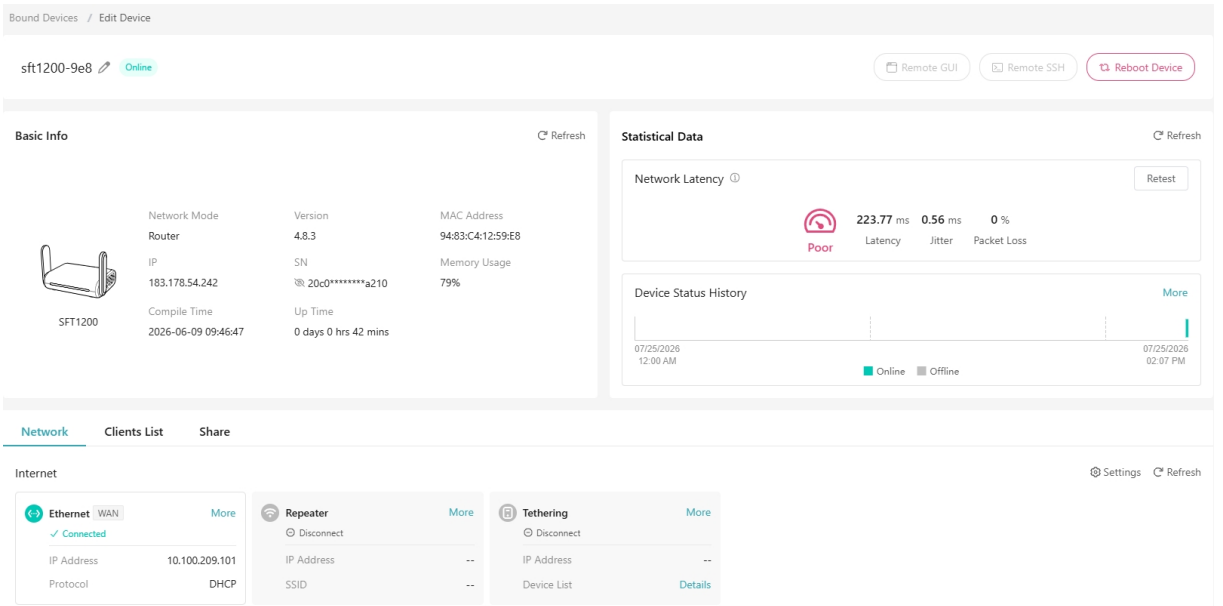
7.1.2 Administrar el enrutador

Consultar los detalles del dispositivo

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

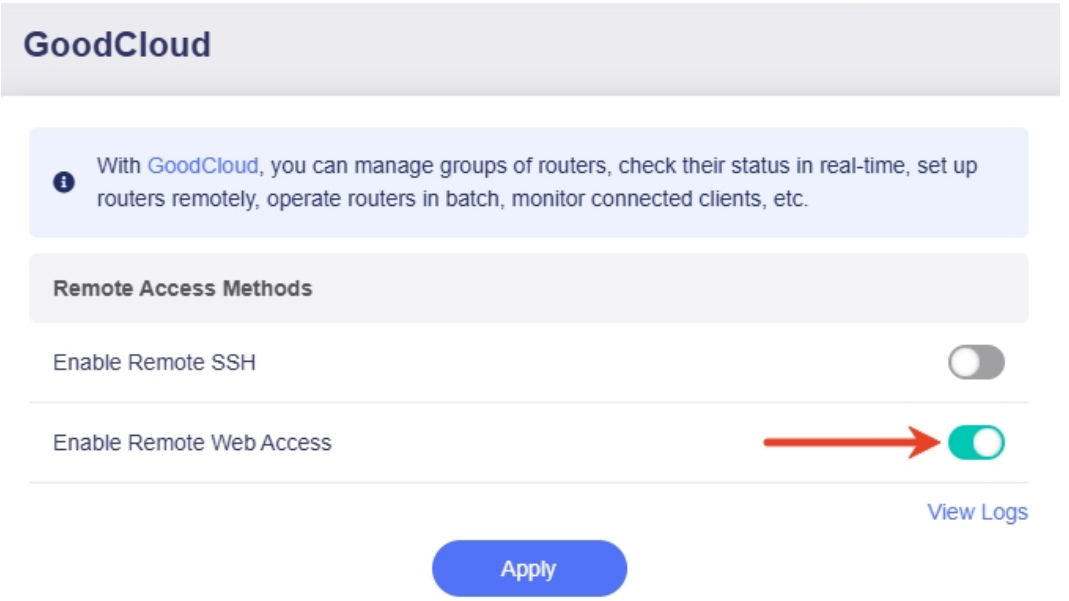


Haga clic en el nombre del dispositivo para ingresar a la página de detalles del dispositivo, que muestrainformación básica, datos estadísticos, descripción general de la red, lista de clientes y cronograma. También puede realizar operaciones avanzadas, como acceso remotolying al enrutador, y reiniciando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

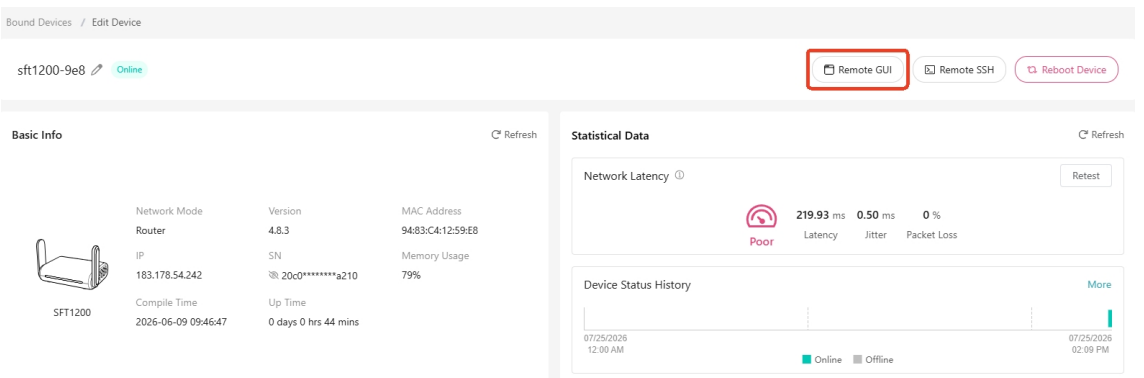


Acceso web remoto

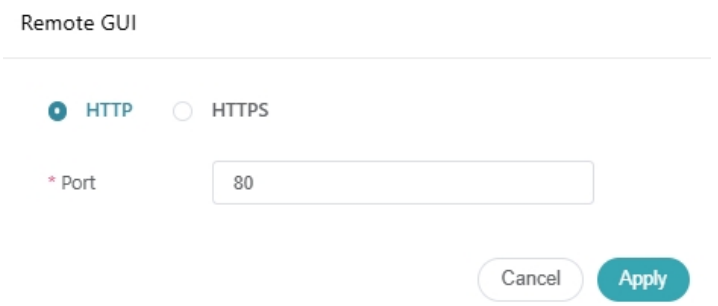
1. Inicie sesión en el panel de administración web del del enrutador', navegue hasta **SERVICIOS EN LA NUBE** > **GoodCloud**, habilite **Acceso web remoto**, luego haga clic en **Aplicar**.



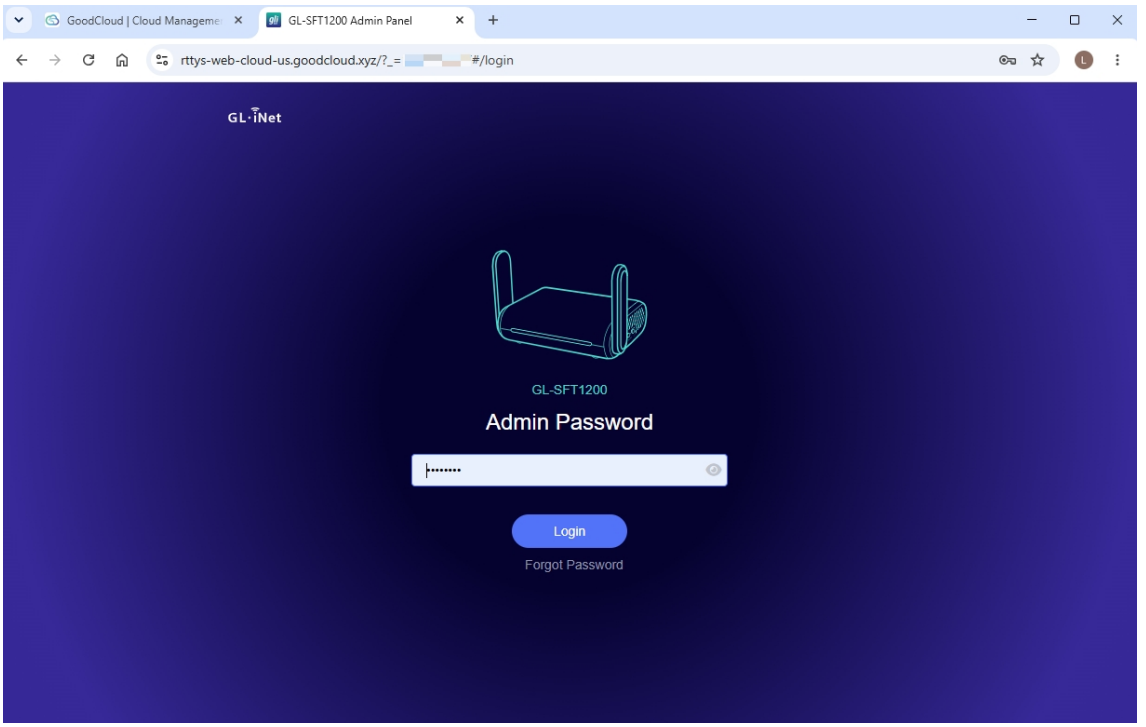
2. Inicie sesión en la plataforma GoodCloud y navegue hasta **Dispositivo** > **Dispositivos vinculados**. Haga clic en el dispositivo al que desea acceder e ingresará a la página de detalles del dispositivo.
3. En la página de detalles del dispositivo, haga clic en **Remoto GUI** botón en la esquina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



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

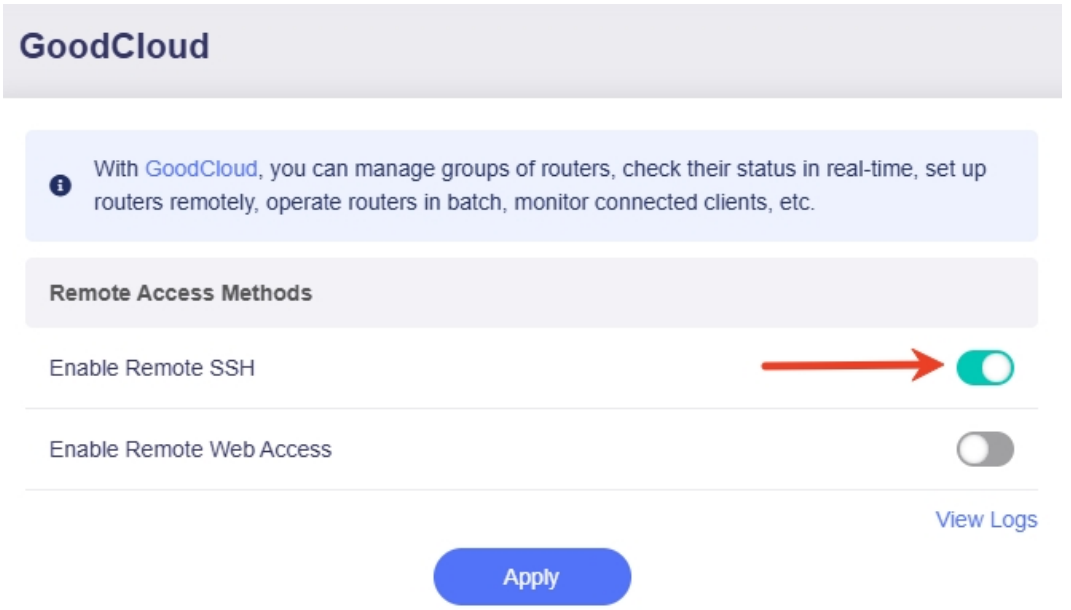


5. Será redirigido a la página de inicio de sesión del enrutador'. Ingrese la contraseña de administrador para acceder de forma remota al panel de administración web del enrutador'.

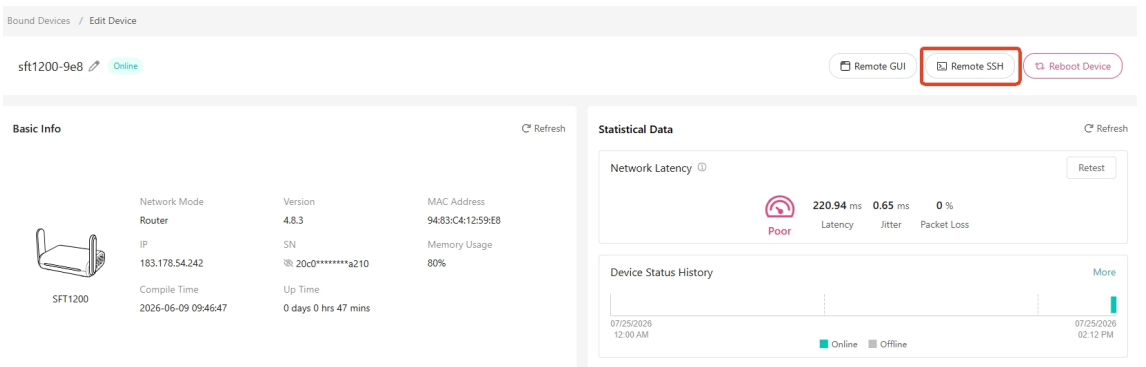


Acceso remoto SSH

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



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

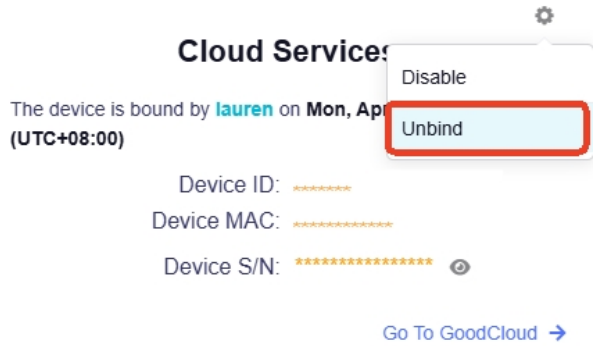


4. Inicie sesión como **root** e ingrese la contraseña para acceder al terminal de su enrutador.

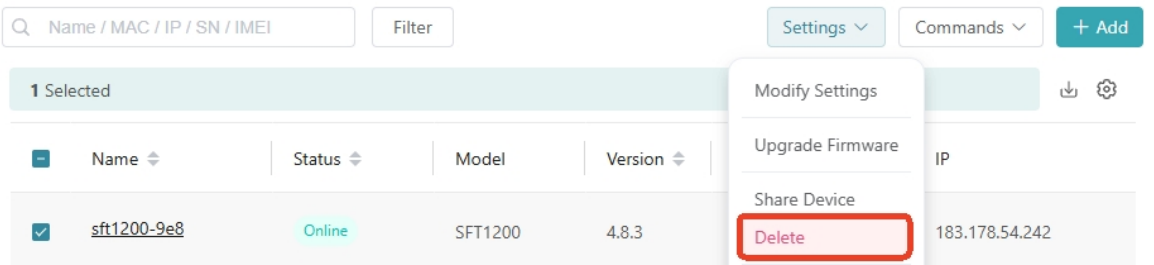

GL-SFT1200 login: root
Password:
BusyBox v1.29.3 () built-in shell (ash)
W I R E L E S S F R E E D O M
OpenWrt 18.06, LEDE
root@GL-SFT1200:~#

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 su cuenta de GoodCloud.

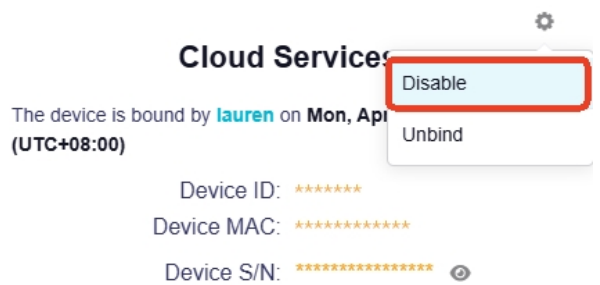


Como alternativa, inicie sesión en la plataforma en la nube y navegue hasta **Dispositivo** > **Dispositivos vinculados**. Seleccione el dispositivo que desea desvincular, haga clic en **Configuración** en la esquina superior derecha y luego seleccione **Eliminar**. Su dispositivo se desvinculará. su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



7.1.4 Desactivar GoodCloud

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



El servicio en la nube se desactivará.

7.2 AstroWarp

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

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

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

Consulte astrowarp.net para obtener más información. información.

Capítulo 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 y garantiza configuraciones VPN consistentes, reduceing riesgos de configuraciones individuales inadecuadas.

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

OpenVPN

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

WireGuard

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

8.2 Escenarios de aplicación

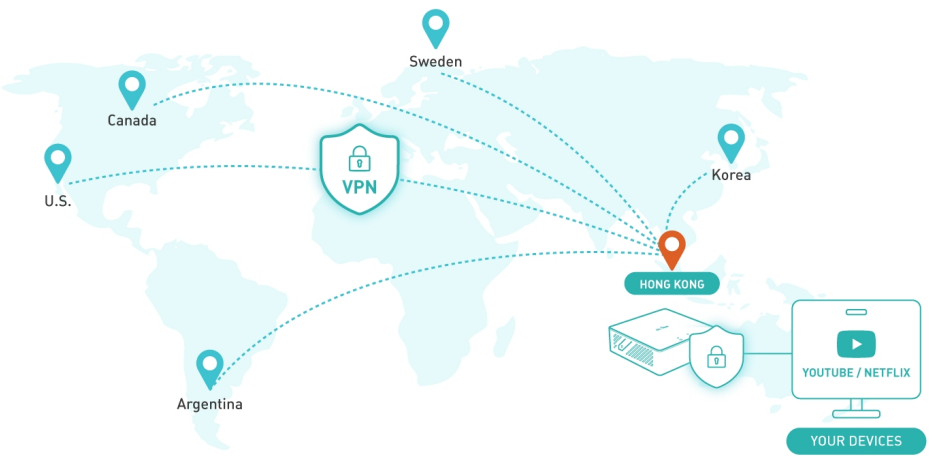
1. **Privacidad de datos personales**

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



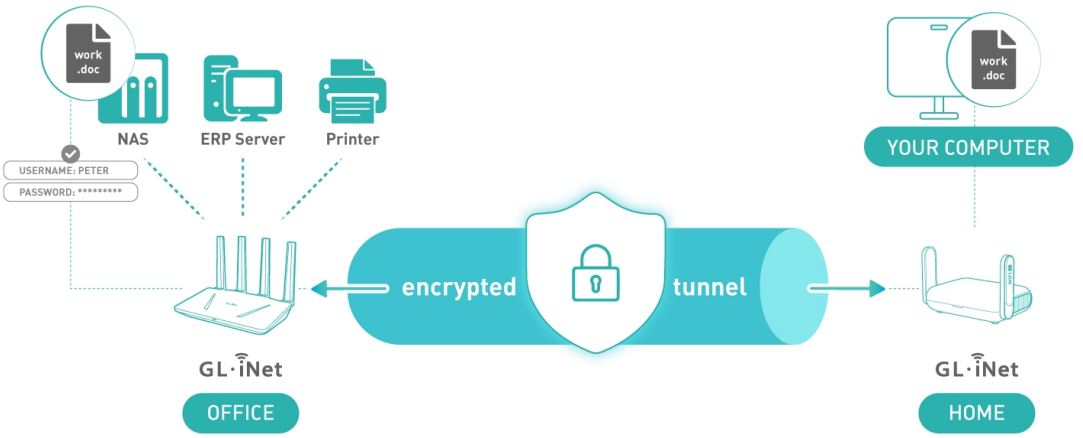
2. **Acceso sin restricciones en todo el mundo**

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



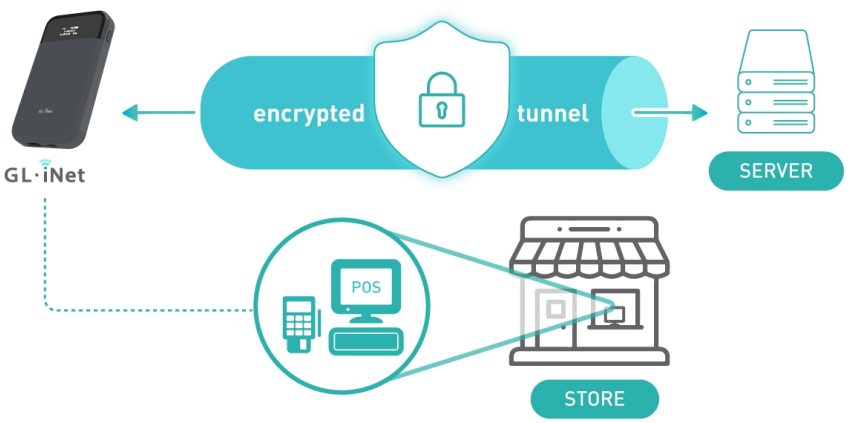
3. **Seguridad de datos para pequeñas empresas**

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

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



Capítulo 9

Panel de VPN

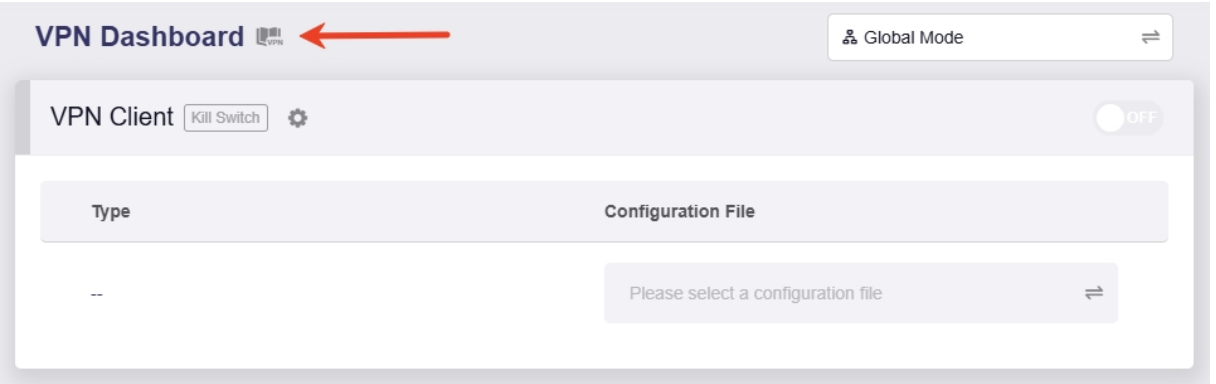
Este capítulo presenta cómo administrar conexiones VPN a través del panel de administración web.

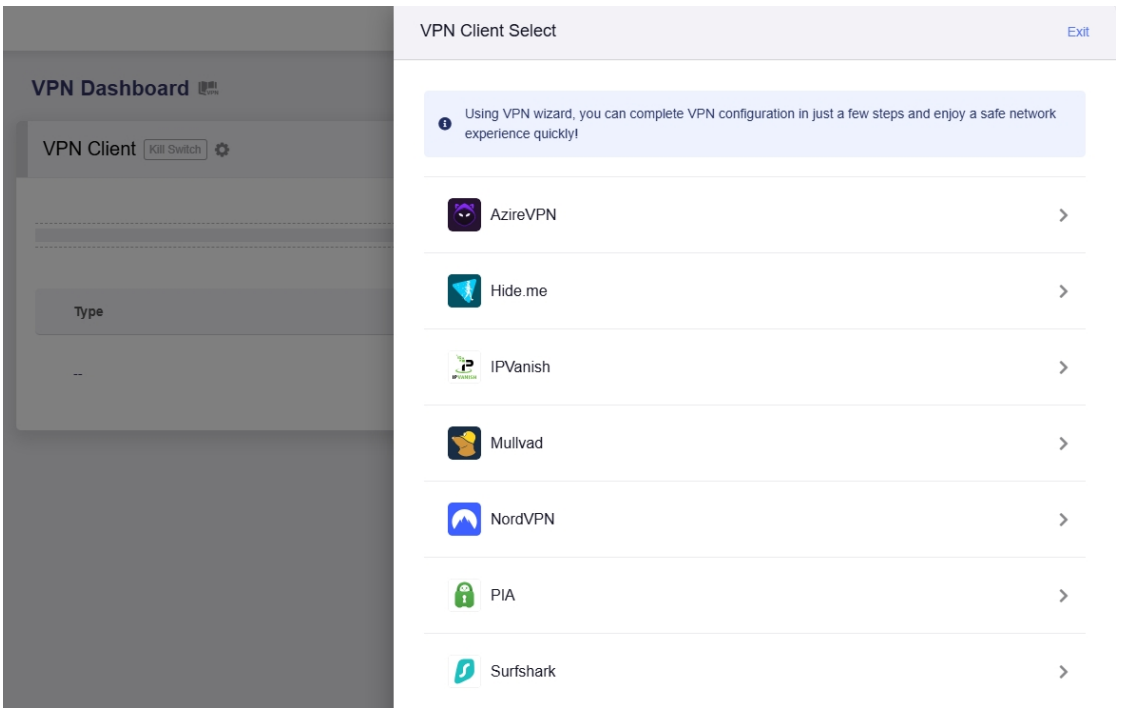
Inicie sesión en el enrutador’s web undmin panel y navegue a **VPN** > **Panel de VPN**.

Cuando Cuando el enrutador está configurado como cliente VPN activo, el panel de VPN muestra detalles de la conexión VPN, como reglas de túnel, dirección del servidor, estadísticas de tráfico, IP virtual del cliente y registro de conexión. También le permite configurar ajustes avanzados como VPN Kill Switch, IP Enmascaramiento y MTU. Puede activar varias conexiones VPN para escenarios de múltiples túneles.

9.1 Asistente de configuración de VPN

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



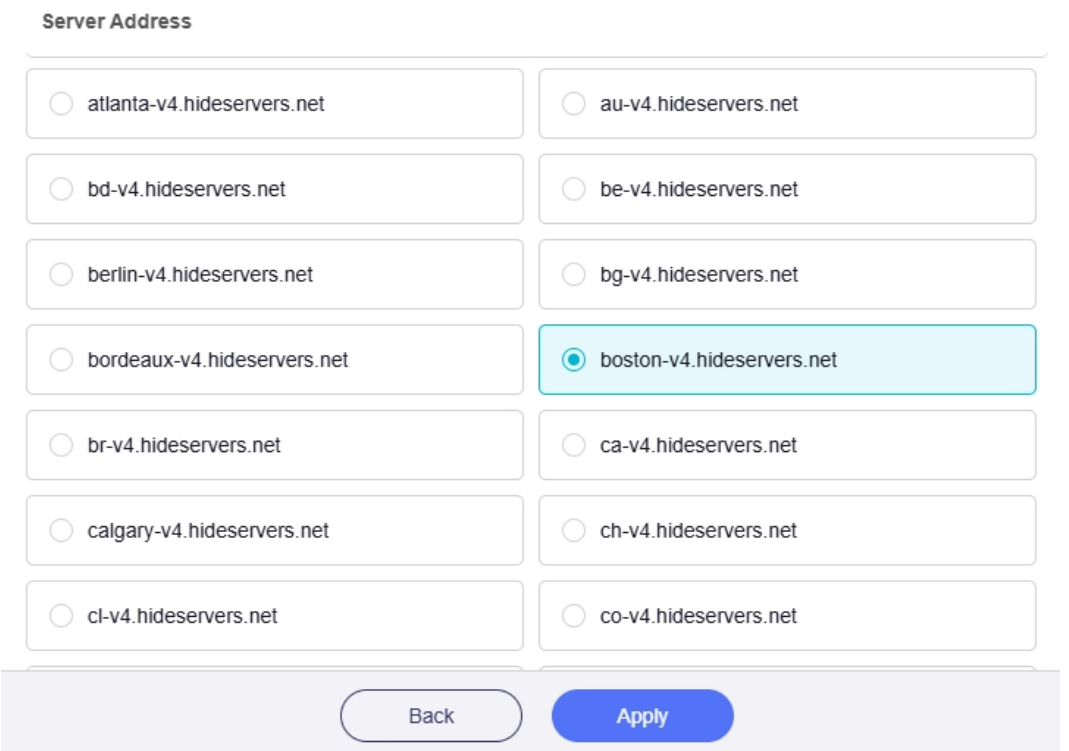


Nota: El asistente de configuración de VPN es solo para los servicios VPN integrados, incluidos AzireVPN, Hide.me, IPVanish, Mullvad, NordVPN, PIA y Surfshark. Para otros proveedores de VPN, omita el asistente y vaya a **VPN** > **Cliente OpenVPN** o **Cliente WireGuard** para configurar la VPN. manualmente.

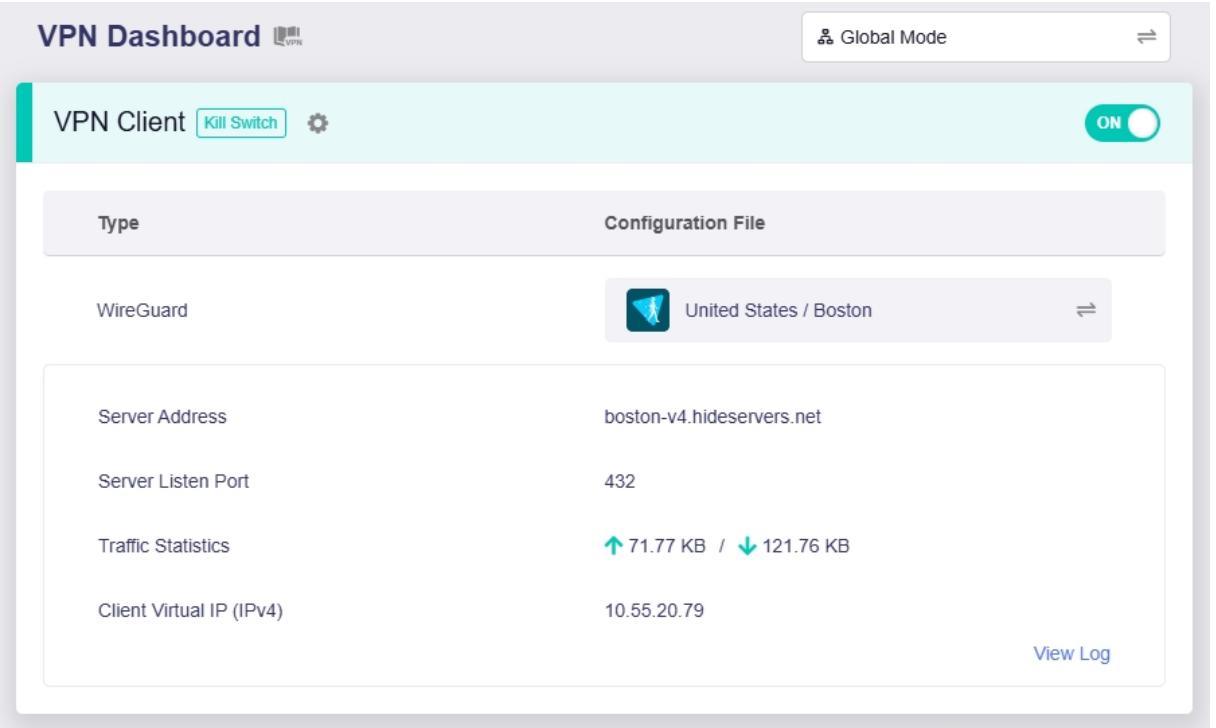
Aquí hay un ejemplo con **Hide.me**. Inicie sesión con las credenciales de Hide.me.



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

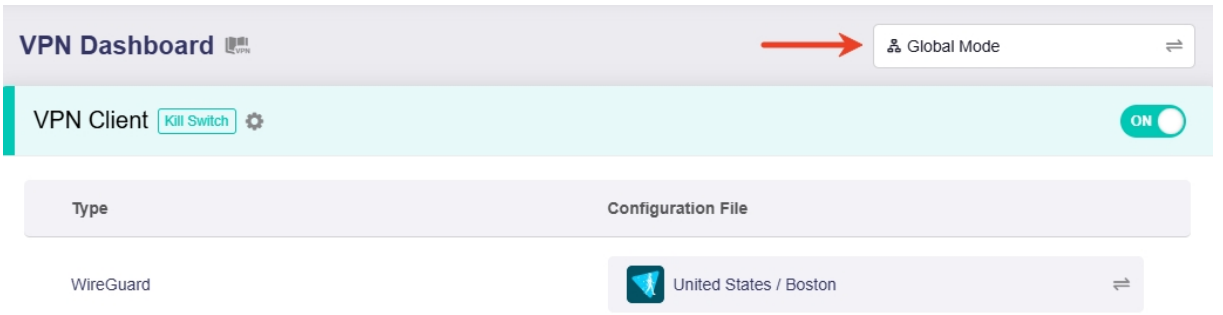


Se conectará automáticamente. Una vez conectado, vaya al **Panel de VPN**. Verá que se ha habilitado un túnel VPN, que muestra detalles que incluyen el protocolo VPN (por ejemplo, WireGuard), el archivo de configuración, la dirección del servidor, el puerto de escucha del servidor, las estadísticas de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

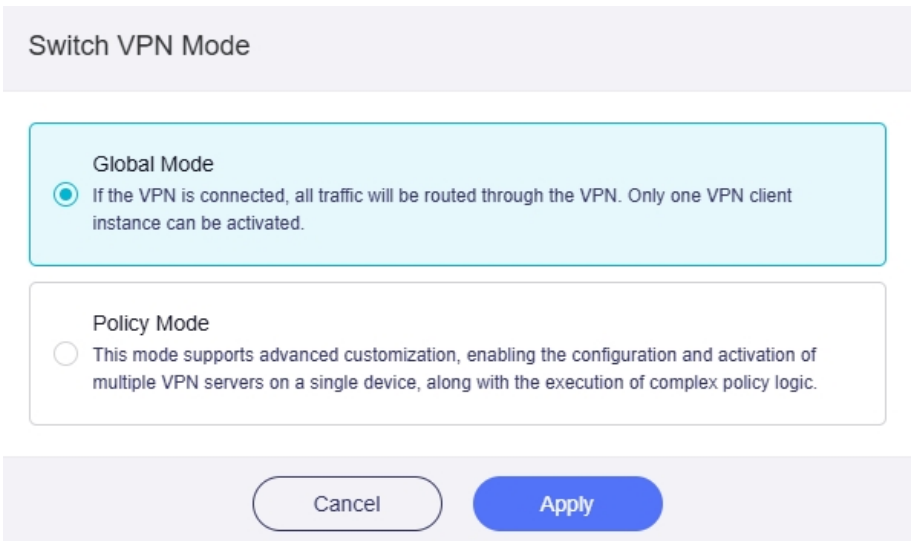


9.2 Modo VPN

Activado Panel de VPN, haga clic en el botón en la esquina superior derecha para cambiar los modos de VPN si es necesario.



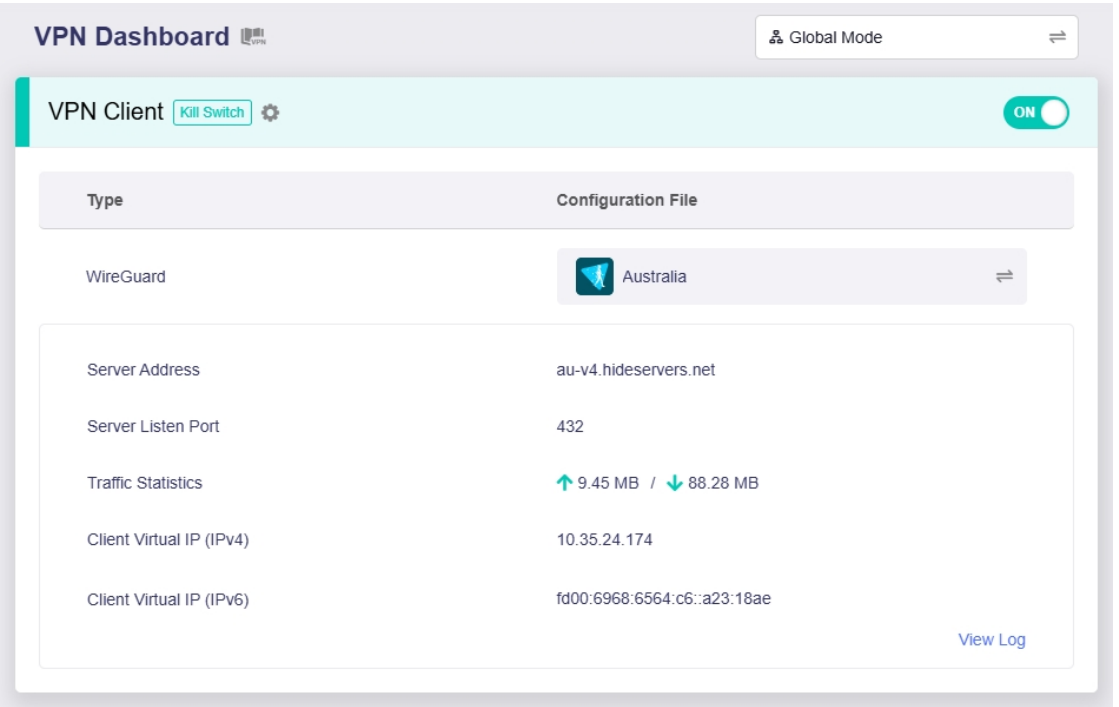
Hay dos modos disponibles: **Modo global** y **Modo de política**.



9.2.1 Modo global

En este modo, todo el tráfico se enrutará a través del túnel VPN y solo se puede conectar una instancia de cliente VPN. activado. Es ideal para escenarios que requieren que todo el tráfico del dispositivo pase a través de un único servidor VPN, como seguridad de red unificada o acceso a contenido específico de una región.

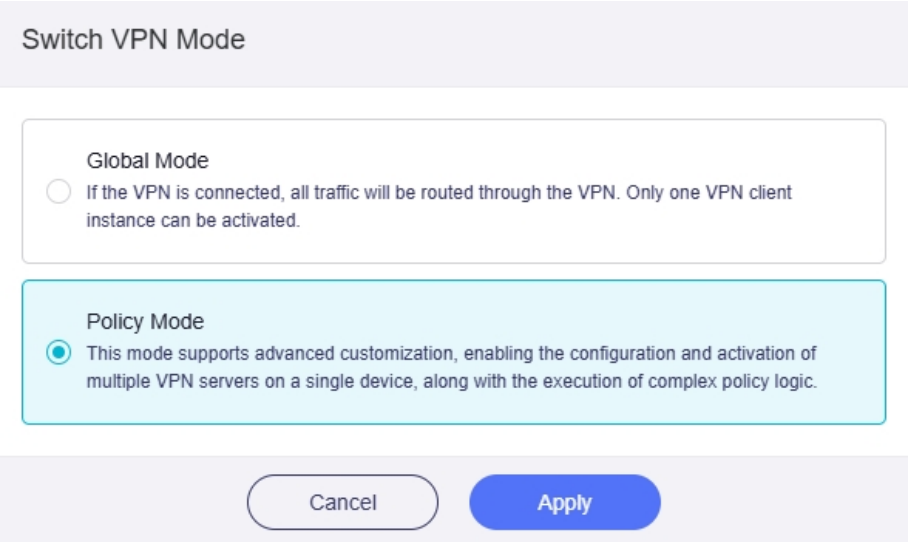
En el siguiente ejemplo, el enrutador se conecta a un servidor australiano mediante el protocolo WireGuard. Todo el tráfico de los clientes conectados se enrutará a través de este túnel VPN.



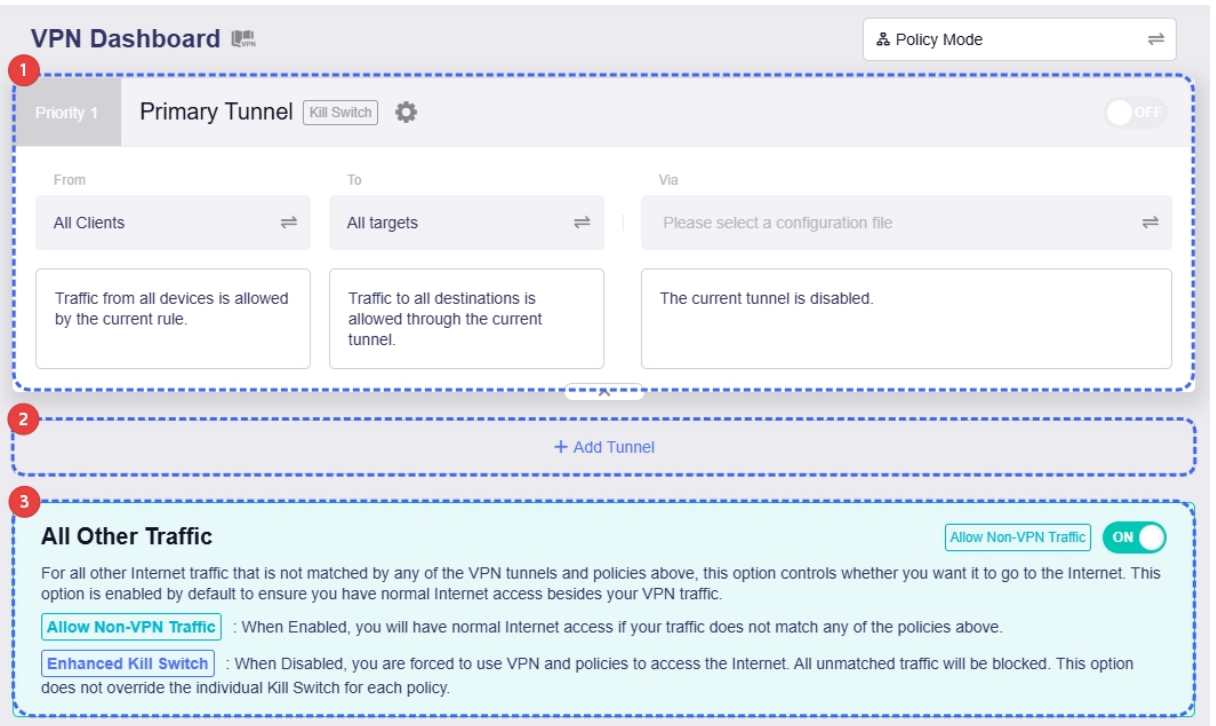
9.2.2 Modo de política

En este modo, puede conectar un único enrutador a varios servidores VPN y personalizar las reglas de VPN. Es adecuado para casos que necesitan una gestión de tráfico flexible, como enrutar tráfico diferente a diferentes destinos a través de múltiples servidores VPN.

Cambie el modo VPN a **Modo de política** y haga clic en **Aplicar**.



Después de cambiar, si la VPN no está habilitada, la página se muestra a continuación, e incluye tres secciones: **Túnel principal**, **Agregar túnel** y **Todo el resto del tráfico**.

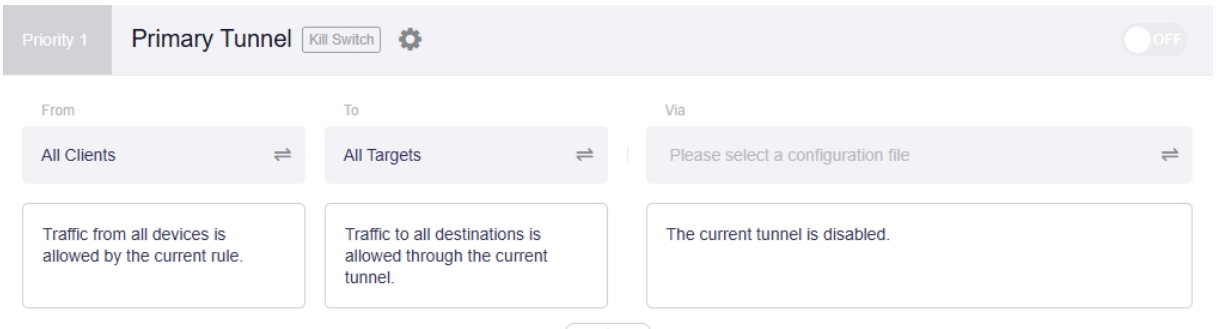


Túnel principal

El túnel principal es un túnel preestablecido en modo de política. Tiene la prioridad más alta de forma predeterminada y puede ajustar su prioridad cuando se configuran varios túneles.

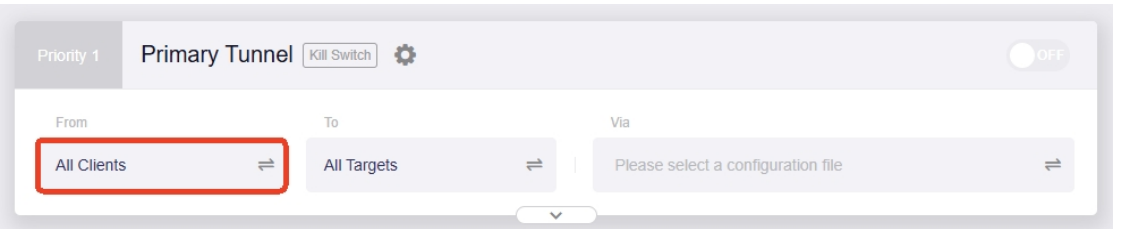
En este túnel, puede personalizar la regla del túnel estableciendo tres factores:

- **De**: se refiere a la fuente de tráfico, es decir, el tráfico que debe enrutarse a través de este túnel.
- **A**: se refiere al destino del tráfico, al cual se enruta el tráfico a través deles túnel.
- **Vía**: Se refiere al método de enrutamiento del tráfico, es decir, si se utiliza VPN.

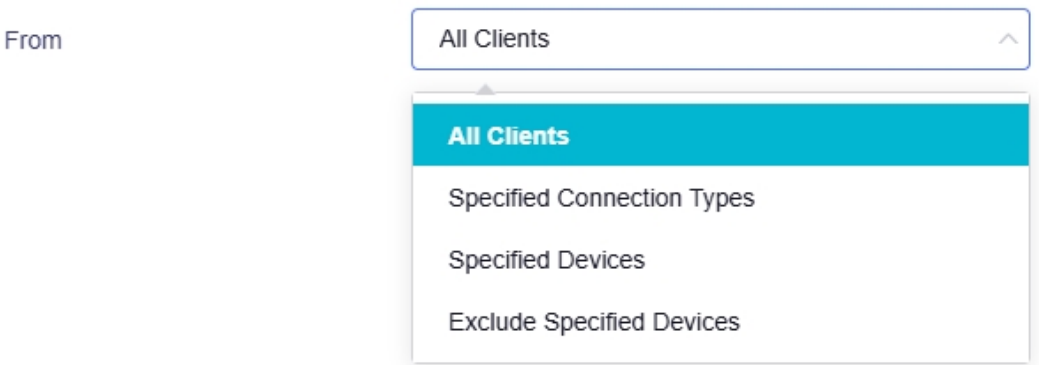


Siga los pasos a continuación para configurar su regla de túnel.

1. Haga clic en el cuadro atenuado de la izquierda.

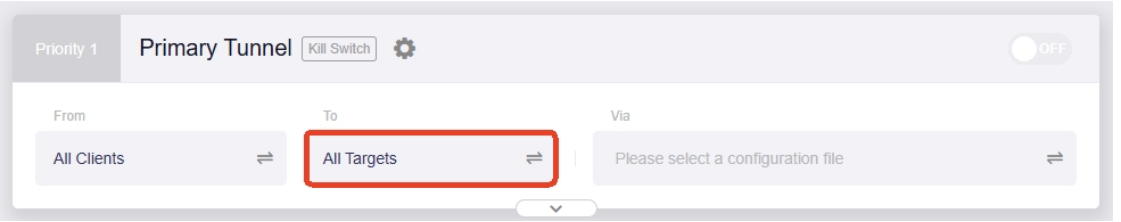


2. Seleccione la fuente de tráfico que desea coincidir con esta regla y haga clic en **Aplicar**.

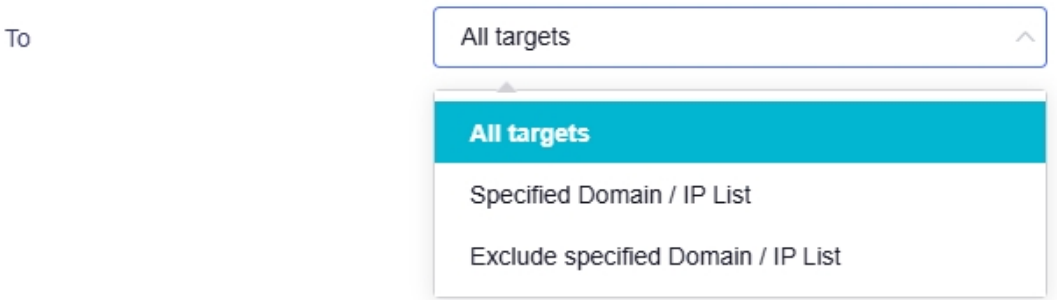


- **Todos los clientes**: Si se selecciona, el tráfico desde todos los dispositivos coincidirá esta regla.
- **Conexión especificada Tipos**: Si se selecciona, el tráfico desde el especificado tipo de conexión (por ejemplo, subred LAN, puerta de enlace directa, red de invitados) coincidirá esta regla.
- **Dispositivos especificados**: Si se selecciona, el tráfico de los dispositivos especificados (identificados por la dirección MAC) coincidirá esta regla.
- **Excluir dispositivos especificados**: Si se selecciona, el tráfico de dispositivos especificados (identificados por dirección MAC) sel **NO** coincide esta regla.

3. Haga clic en el medio gruncuadro sombreado.



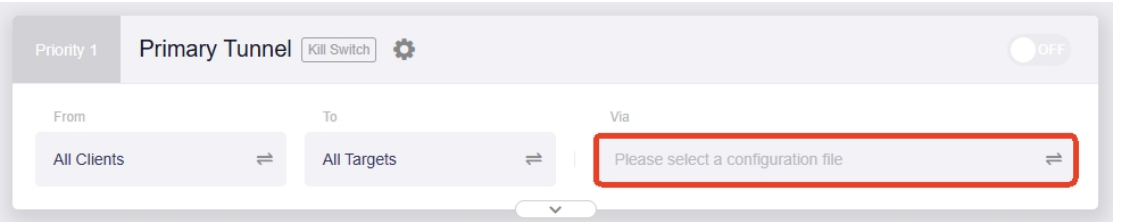
4. Seleccione el destino el tráfico será rutad a través de este túnel y haga clic en **Aplicar**.



- **Todos los Tobjetivos**: Si se selecciona, el tráfico que coincida con esta regla se enrutará a todos los destinos.
- **Dominio/IP especificados Lista**: Si se selecciona, el tráfico que coincida con esta regla se enrutará al dominio/IP especificado. Usted necesita ingrese el dominio/IP especificado manualmente, o ingrese el enlace URL de suscripción. Al especificar un dominio raíz se cubrirán todos sus subdominios.
- **Excluir la lista de IP/dominio especificada**: Si se selecciona, el tráfico que coincida con esta regla **NO** se enrutará al dominio/IP especificado. Tú necesita ingresar el dominio/IP especificado manualmente, o ingrese el enlace URL de suscripción. Al especificar un dominio raíz se cubrirán todos sus subdominios.

Nota: Si selecciona URL de suscripción, el nombre de dominio o la dirección IP en la URL se automáticamente se actualiza todos los días. Asegúrese de ingresar la URL correcta. La detección de URL verificará la validez del nombre de dominio o la dirección IP.

5. Haga clic en derecha gracuadro sombreado.

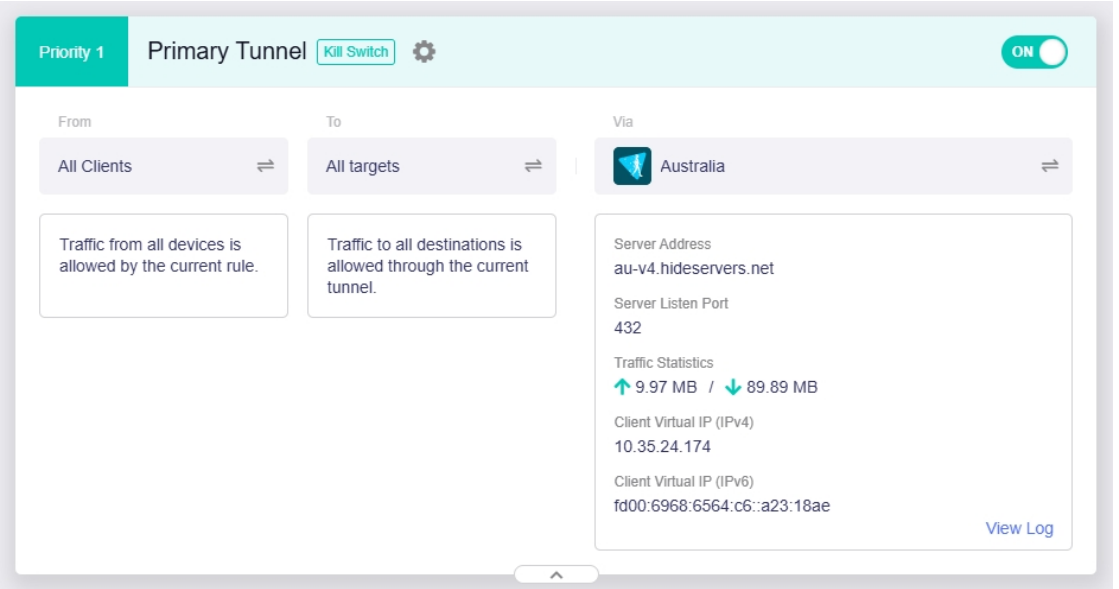


6. Seleccione el método de enrutamiento para este túnel: **Usar VPN** o **No usar VPN**.



- **Usar VPN**: Si se selecciona, trafica que coincida con esta regla se enrutará al destinos vía VPN túnel. Debe seleccionar un archivo de configuración de VPN para esta regla.
- **No usar VPN**: Si se selecciona, tráfico que coincida esta regla se enrutará al destinos a través de local WAN red en lugar de VPN.

7. Después configurar el origen del tráfico, el destino y el método de enrutamiento, se completa la configuración de la regla del túnel principal. En el siguiente ejemplo, túnella regla es: Todos los clientes conectados a este enrutador accederán a Internet a través de VPN; Su tráfico se enrutará a través de este túnel VPN al servidor de Australia y finalmente saldrá de este servidor a Internet.



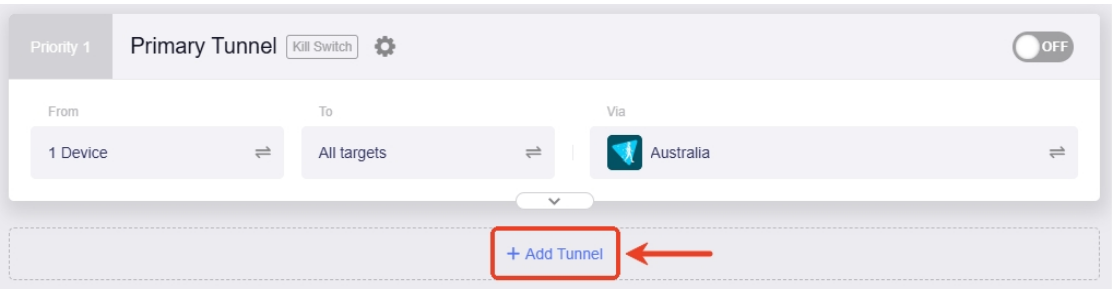
Nota: por seguridad, vaya a Todo el resto del tráfico y Opciones de túnel para verificar otras configuraciones antes de habilitar este túnel.

Agregar túnel

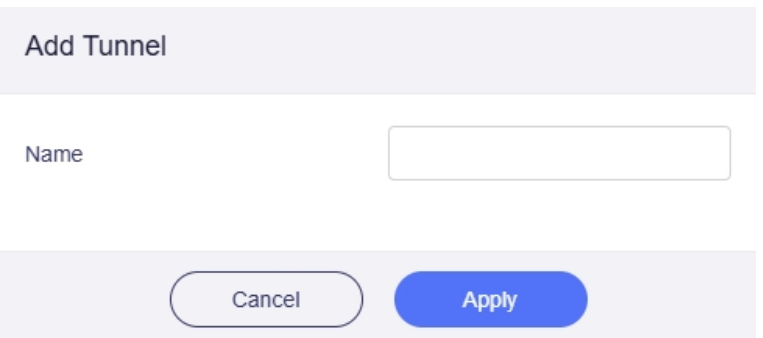
Agregue túneles si necesita enrutar el tráfico desde diferentes dispositivos a diferentes destinos.

Siga los pasos a continuación para agregar un túnel.

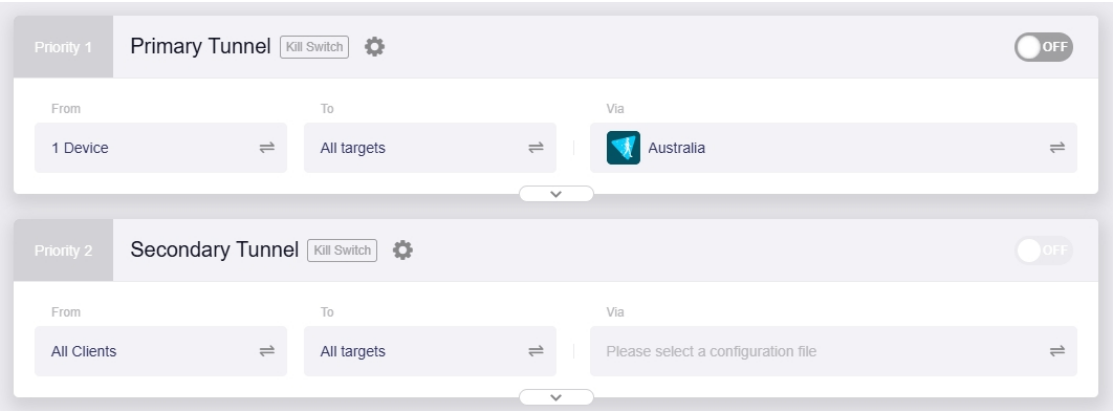
1. Haga clic en **Agregar túnel** debajo del túnel principal.



2. Nombra el túnel.



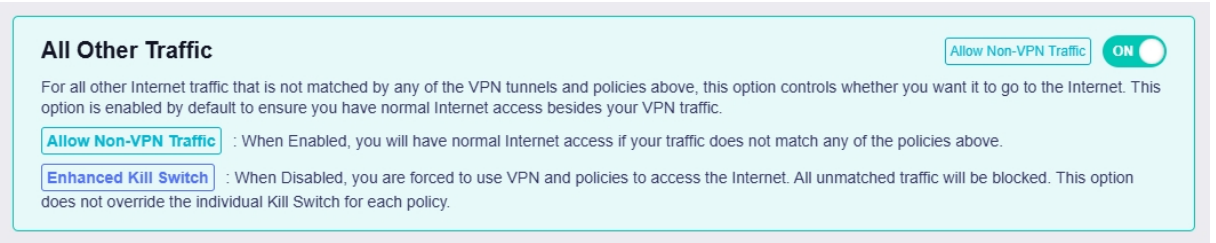
3. Yobtendrás un túnel más en el panel de VPN. Se pueden crear hasta 5 túneles (incluido el túnel principal preestablecido). túnel).



4. Configure reglas del túnel estableciendo el origen del tráfico, destinos y el enrutamiento método. Una vez terminado, verifique otras configuraciones en Todo el resto del tráfico y Opciones de túnel de seguridad antes de habilitar los túneles.

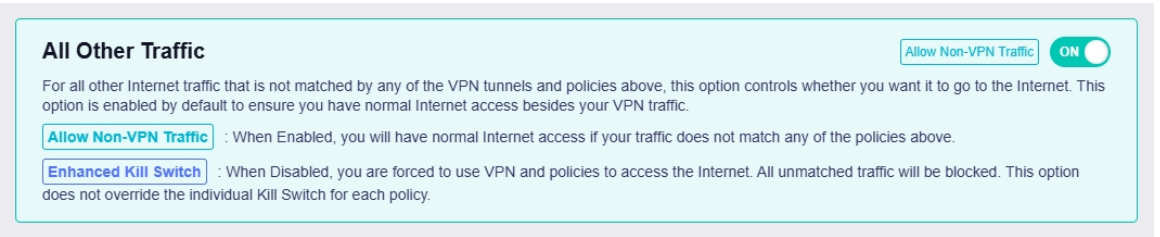
Todo el resto del tráfico

En el modo de política, se muestra un túnel predeterminado prehabilitado en la parte inferior del panel de VPN.

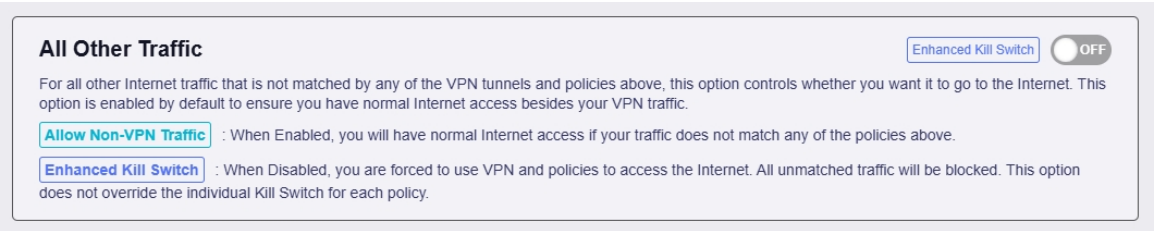


Este túnel controla si el tráfico que no coincide con ninguno de los grupos de túneles VPN anteriores puede acceder a Internet. Está habilitado de forma predeterminada para garantizar el acceso normal a Internet para el tráfico no enrutado a través de VPN.

- Cuando está habilitado, el tráfico incomparable aún puede acceder a Internet.



- Cuando está deshabilitado, solo el tráfico enrutado a través de VPN puede acceder a Internet. Se bloqueará todo el tráfico que no sea VPN y el tráfico que conmuta por error desde conexiones VPN. Esta opción no anula el Kill Switch individual para cada túnel VPN.

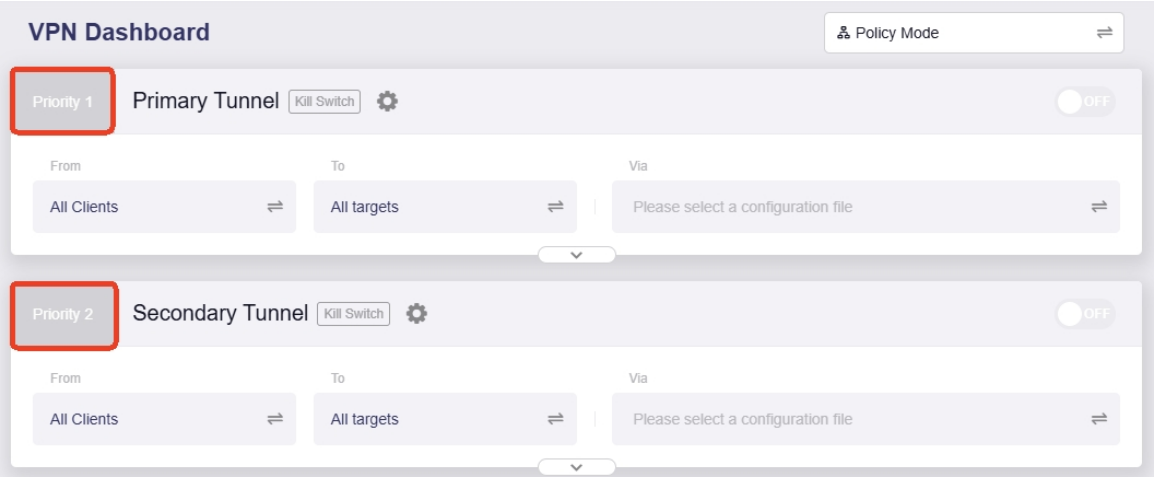


Prioridad del túnel

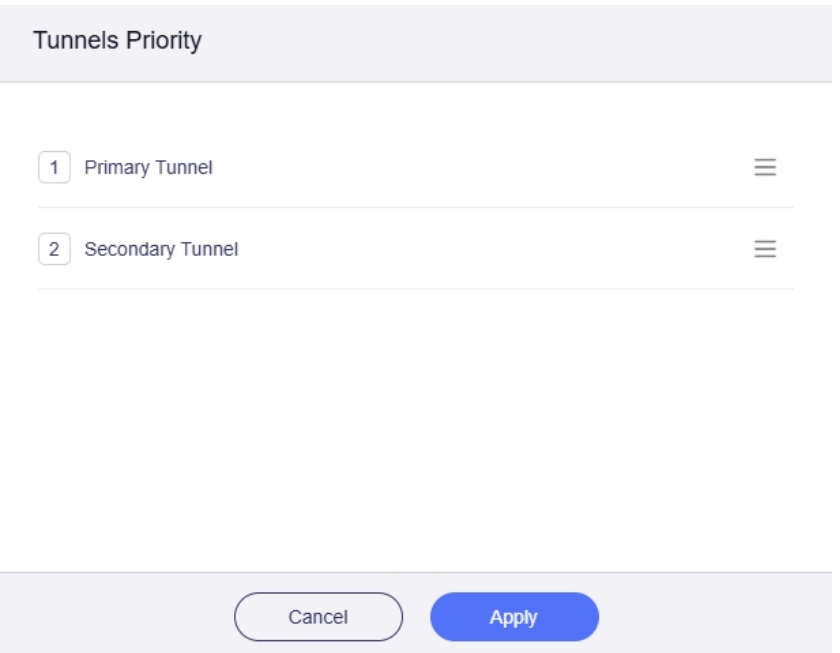
De forma predeterminada, el túnel primario preestablecido tiene la prioridad más alta, seguido de otro túnel agregado manualmente (si lo hay), y luego el resto preestablecido. Túnel de tráfico para garantizar conectividad de red a través de red ISP (WAN) local.

Si necesita parapara modificar la prioridad del túnel, siga los pasos que se indican a continuación.siga los pasos a continuación.

1. Click la etiqueta de prioridad en la esquina superior izquierda de cualquier túnel (por ejemplo, Prioridad 1 / Prioridad 2).



2. En la ventana emergente, haga clic en y mantenga presionado el ícono de tres líneas a la derecha para reordene el túnel, luego haga clic en **Aplicar**.

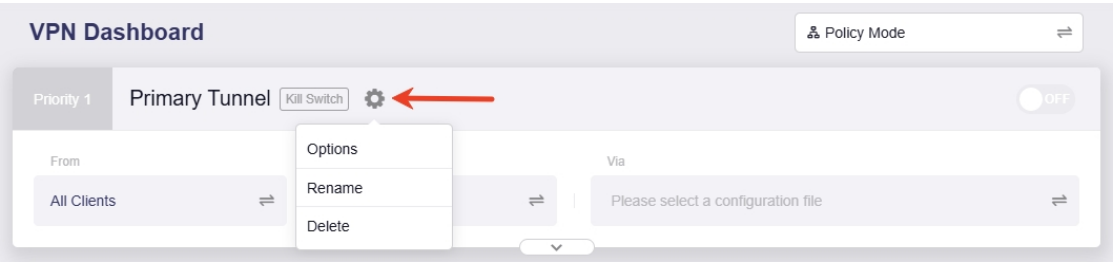


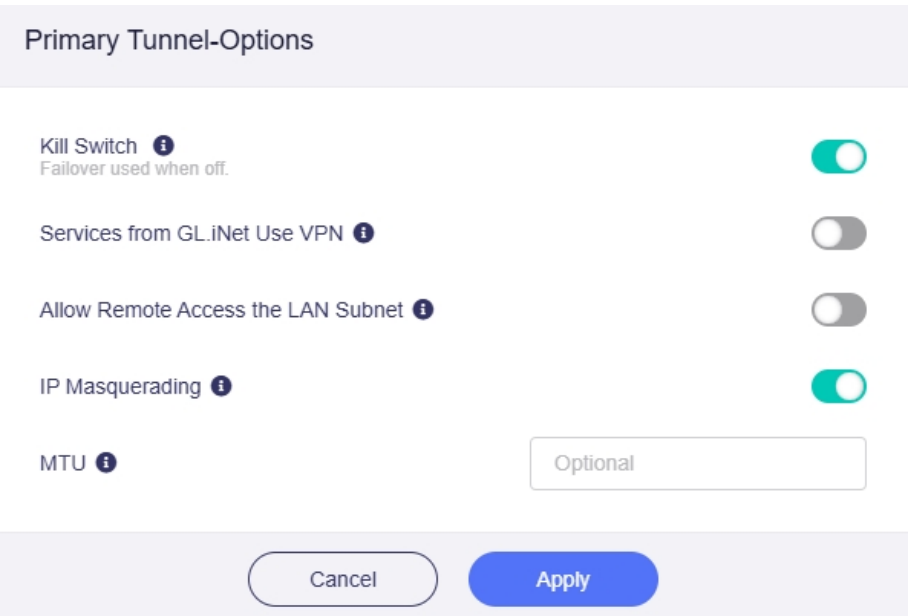
Cuando se habilitan varios túneles, el enrutador enrutará el tráfico en el siguiente orden:

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, probará el siguiente túnel de prioridad, y así sucesivamente, hasta que coincida con el túnel "Todo el resto del tráfico".
2. Si un túnel VPN se desconecta inesperadamente, el sistema determinará si conmutará por error el tráfico al siguiente túnel de prioridad en función de si el **Bloqueo de tráfico sin VPN (Kill Switch)** de este túnel está habilitado.
    - Cuando el interruptor de interrupción está habilitado, el tráfico se bloqueará y no pasará al siguiente túnel de prioridad.
    - Cuando el interruptor de interrupción está desactivado, el tráfico pasará al siguiente túnel de prioridad e intentará coincidir con sus reglas de túnel.
3. El **Todo el resto del tráfico** está habilitado de forma predeterminada para garantizar que el tráfico que no coincida con los túneles VPN aún pueda acceder a Internet.
    - Si está habilitado, enruta el tráfico no coincidente o de conmutación por error a través de la WAN local.
    - Si está deshabilitado, fortalece el Kill Switch y bloquea el acceso regular a Internet para evitar fugas de IP.

Opciones de túnel

Puedes configurar ajustes avanzados para cada túnel VPN, como VPN Kill Switch, enmascaramiento de IP y MTU. Haga clic en el ícono de ajustes al lado del nombre de un túnel.





- **Bloqueo de tráfico sin VPN (Kill Switch)**: si está habilitado, el tráfico que coincida con estees túnel VPN se bloqueado cuando la conexión fallaes inesperadamente; de lo contrario, conmutará por error a los túneles o WAN de siguiente prioridad.
- **Servicios de GL.iNet Use VPN**: si están habilitados, los servicios GoodCloud, DDNS y rtty transmitirán paquetes a través de VPN túneles. 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 (IP de túnel) y a los dispositivos LAN a través de la VPN. Requiere que el servidor VPN anuncie una ruta de regreso a este enrutador's Subred LAN.

- **Enmascaramiento de IP**: si está habilitado, las IP de origen del cliente LAN se reescribirán en la IP del túnel VPN del enrutador. Deshabilitado solo para configuraciones de sitio a sitio donde el par remoto conoce sus subredes LAN.
- **MTU**: la MTU que configuró para el túnel sobrescribirá el elemento MTU en el archivo de configuración.

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) le asigna una dirección IP pública.

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

   Métodos alternativos:

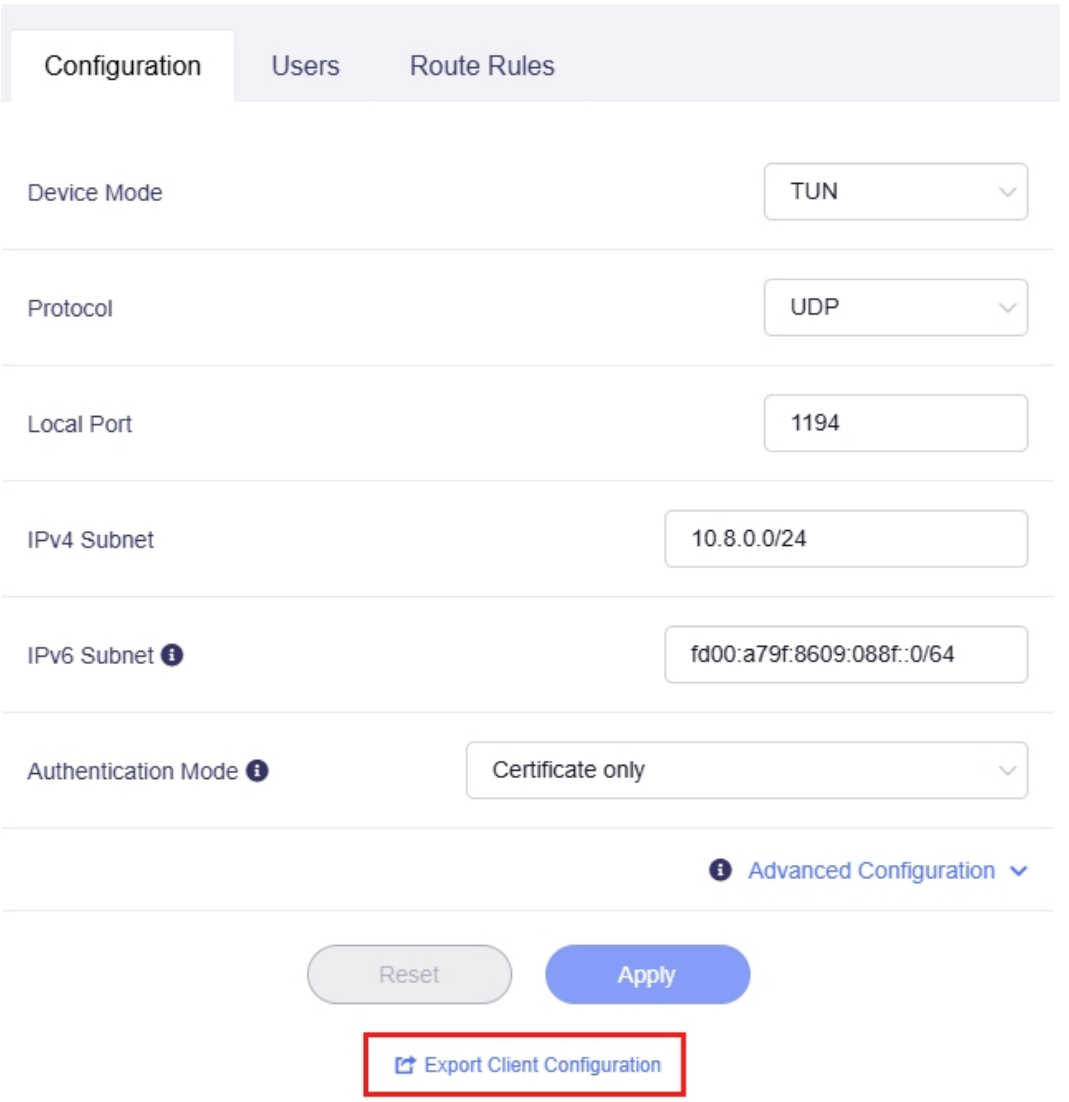
   - Si tiene un enrutador principal ascendente de su GL.iNet enrutador, inicie sesión en él y verifique que tenga una dirección IP pública asignada por su ISP.
   - Pídale a su ISP una dirección IP pública. Esto puede generar una tarifa adicional.
   - Si los dos métodos anteriores no funcionan (por ejemplo, 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. Aplicar la configuración.
   La configuración predeterminada funciona en la mayoría de los casos. Haga clic en **Exportar configuración del cliente** en la parte inferior y continúe con el paso 3. Si ha modificado la configuración, haga clic en **Aplicar** antes de exportarla.

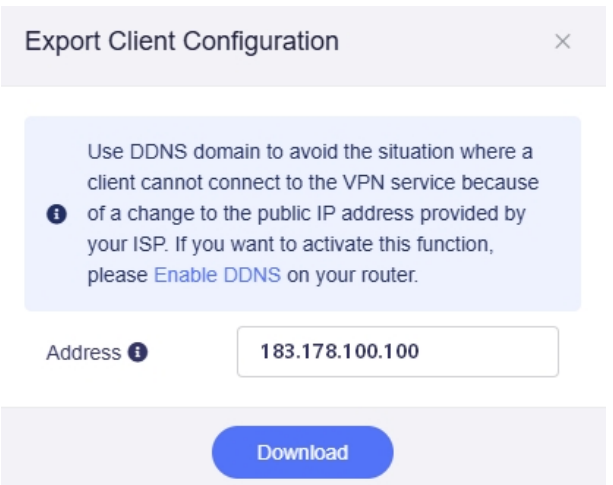


- **Dispositivo Modo**: TAP-S2S o Tun. Consulte aquí para las diferencias.
- **Protocolo**: UDP o TCP. Consulte aquí para las diferencias.

- **Modo de autenticación**: Esto determina el método de autenticación utilizado cuando el cliente se conecta al servidor. Hay tres opciones:
  - **Solo certificado**: si se selecciona, el enrutador generará automáticamente claves de certificado de servidor y de cliente y las incrustará en el archivo de configuración. Cuando carga la configuración en el cliente, no se requieren credenciales adicionales.
  - **Solo nombre de usuario/contraseña**: si se selecciona, el enrutador generará la configuración del cliente sin claves de certificado. necesita primero agregar un nombre de usuario y una contraseña en el **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 más configuraciones del servidor si es necesario.

3. Exportar configuración del cliente.

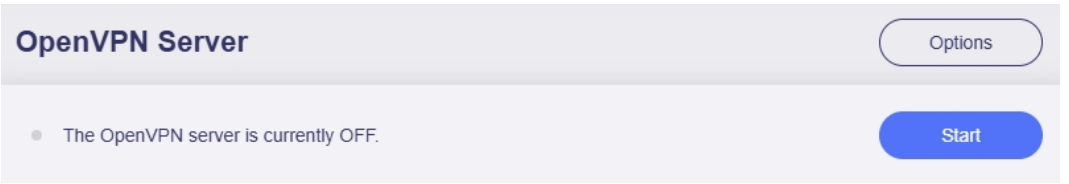
   Después de hacer clic **Exportar configuración del cliente** en la parte inferior de la pestaña Configuración (o aplicar la configuración modificada), aparecerá una ventana como la siguiente. Haga clic en **Descargar** para exportar la configuración.



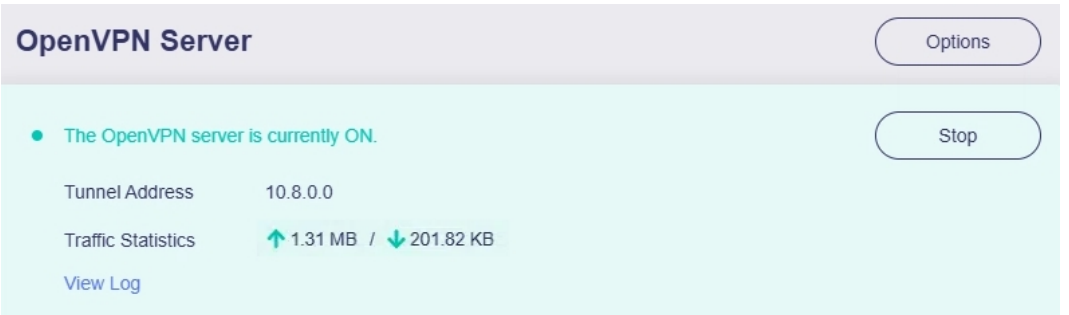
Consejos:

- Si su IP pública dirección cambia con frecuencia, vaya a **APLICACIONES** > **DNS dinámico** y habilitar DDNS. Luego podrá 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. Consulte aquí para solucionar problemas.
- Es posible que deba 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.

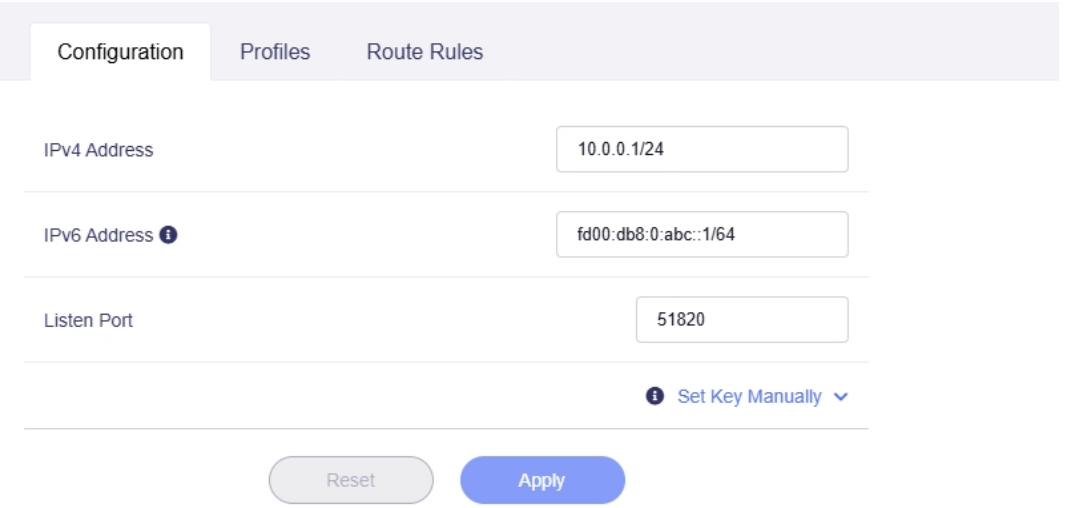
2. **Confirme si se requiere reenvío de puertos**

   - 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 se encuentra a varios niveles descendentes del enrutador principal, configure el reenvío de puertos en cada dispositivo intermedio.

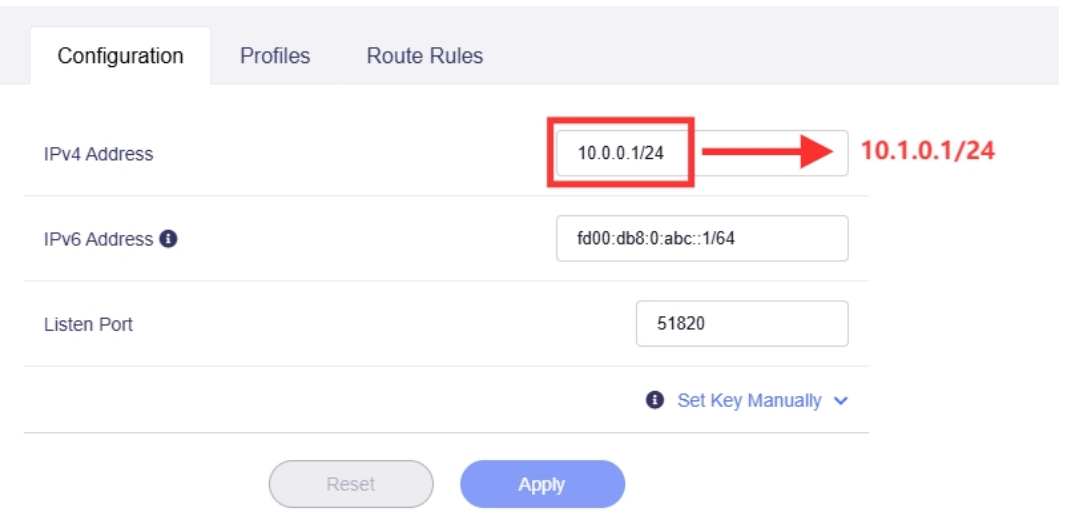
10.2.2 Pasos de configuración

1. Inicie sesión en el enrutador’panel de administración web, navegue hasta **VPN** > **Servidor WireGuard** y luego haga clic en **Generar configuración** (para el servidor VPN inicial). configuración solamente).
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.

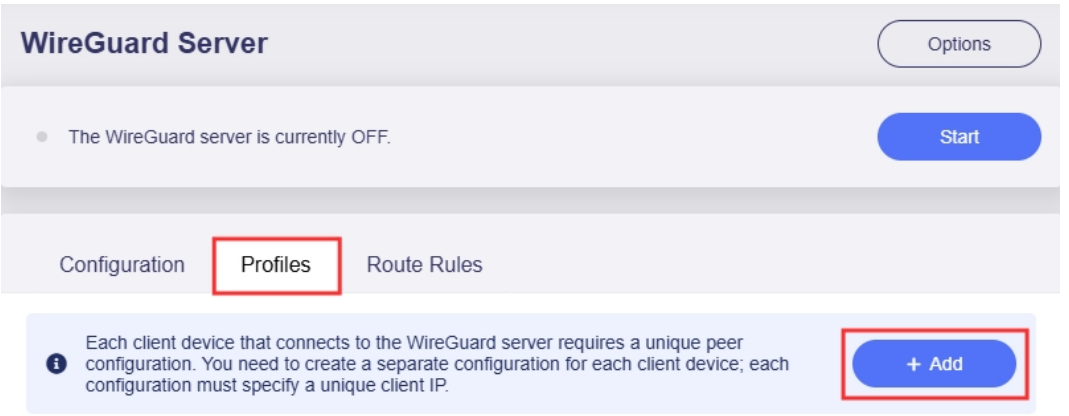


   Si la dirección IPv4 entra en conflicto con la puerta de enlace de su enrutador ascendente, modifique la dirección IPv4 a otra una (por ejemplo, **10.1.0.1/24**) y haga clic en **Aplicar**. Asegúrese de que se incluya la notación CIDR "/24" para evitar problemas de conectividad.

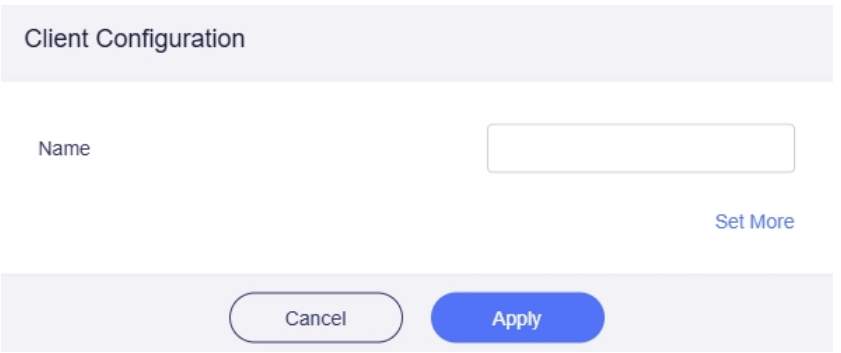


3. Agregue un perfil.

   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.



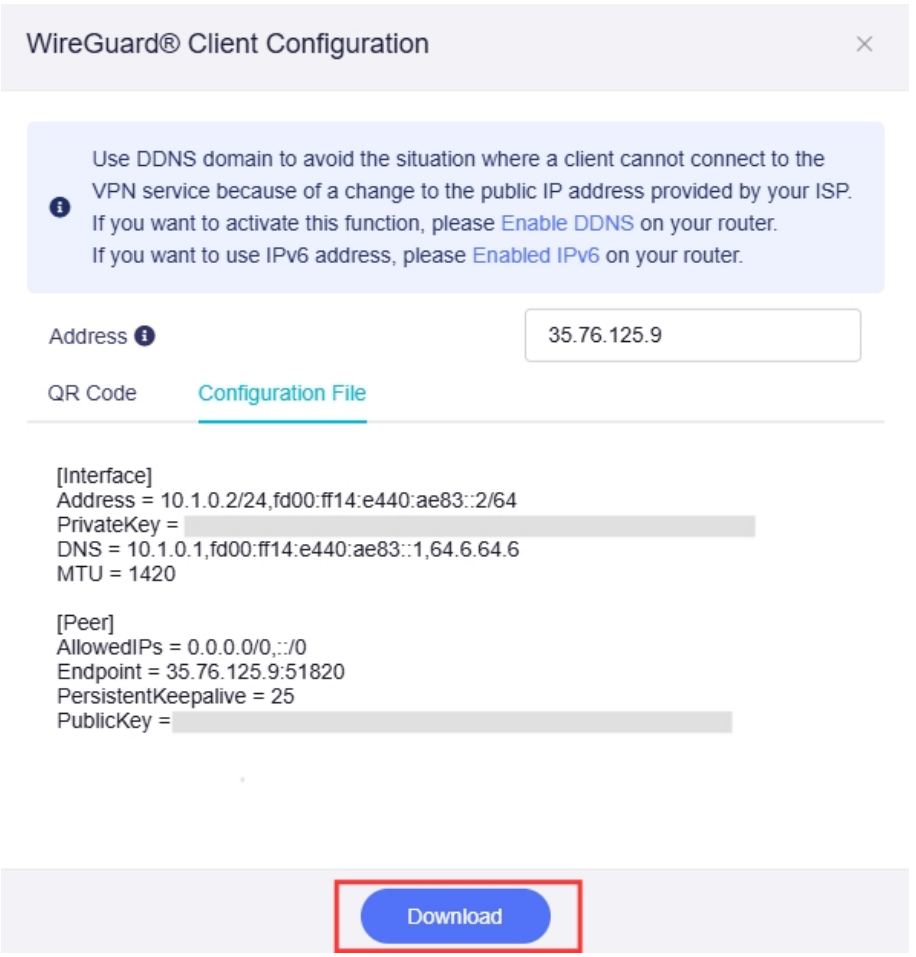
   Consejo: Si desea acceder a los dispositivos LAN del cliente WireGuard desde su servidor WireGuard , cambie a la pestaña **Reglas de ruta** para configurar reglas de ruta. Consulte aquí para detalless.

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. Elija su método preferido para obtener el archivo de configuración.

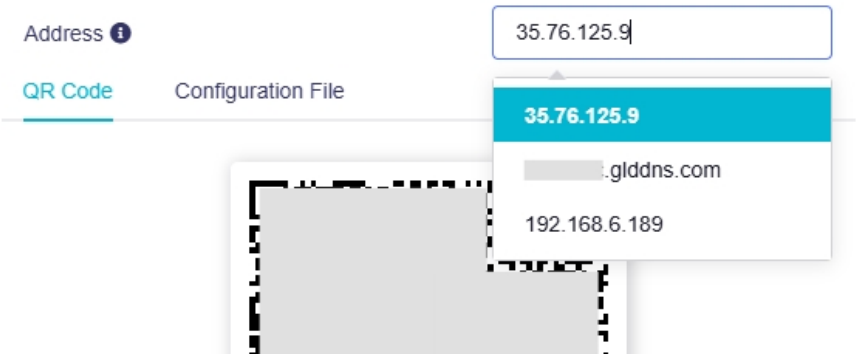
   - **Código QR**: Adecuado para dispositivos (por ejemplo, teléfonos inteligentes, tabletas, computadoras portátiles) con la aplicación WireGuard instalada. Si desea configurar un dispositivo específico como cliente WireGuard, simplemente abra la aplicación WireGuard y escanee el código QR para importar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

- **Texto sin formato**: en formato de texto sin formato, puede revisar los detalles de configuración y 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.

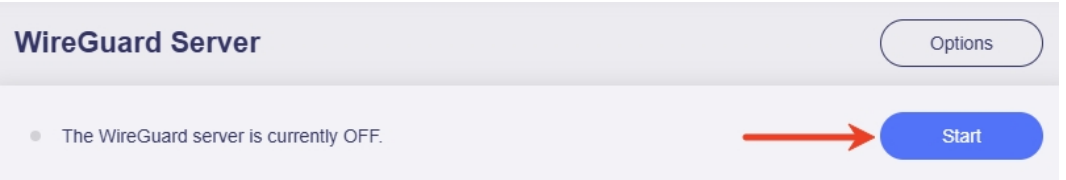


Consejos:

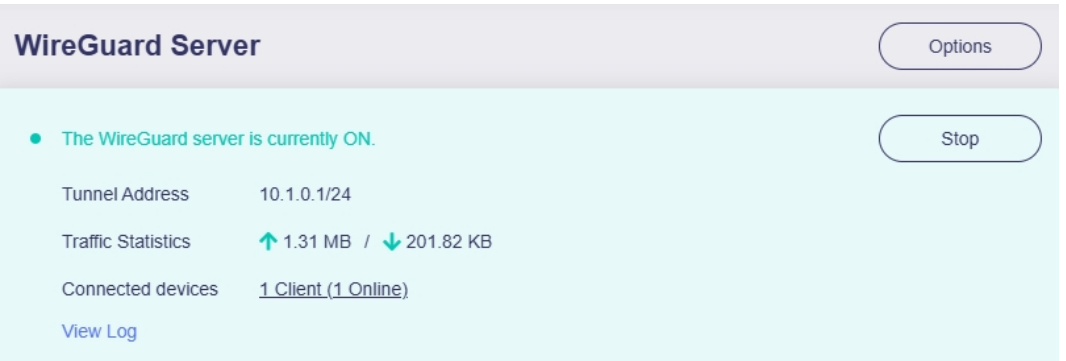
- Si su IP pública dirección cambia con frecuencia, vaya a **APLICACIONES** > **DNS dinámico** y habilite DDNS. Luego puede usar el dominio DDNS como su dirección de servidor.
- Desde firmware v4.8, puede seleccionar la dirección del servidor de una lista desplegable antes de exportar el archivo de configuración: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



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



   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. Ver aquí para los proveedores OpenVPN compatibles con GL.iNet.

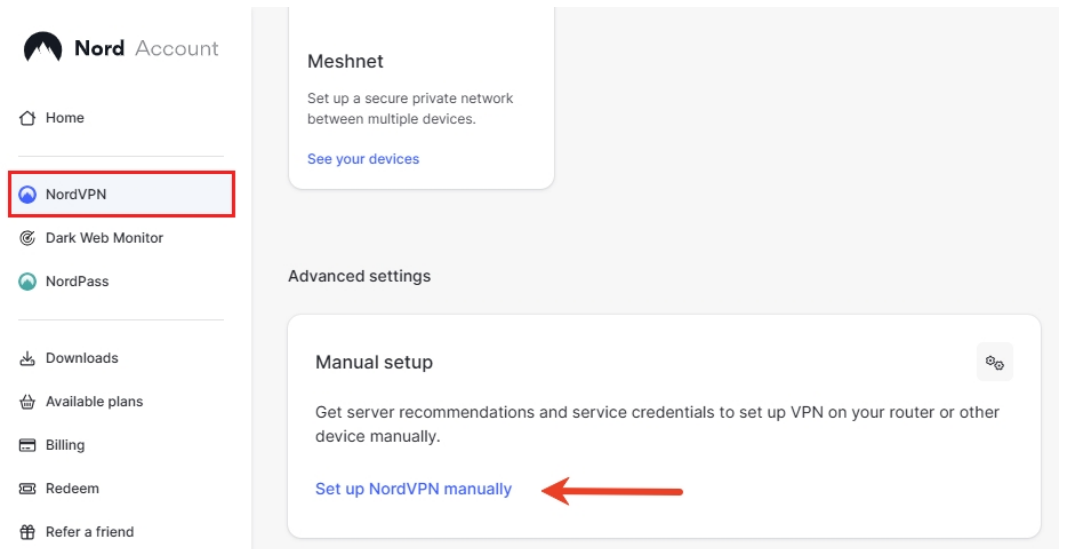
A continuación, visite el sitio web oficial del proveedor de servicios VPN al que se suscribió y obtenga las credenciales de servicio o el archivo de configuración. Si no sabe cómo obtener el archivo de configuración, consulte este enlace o póngase en contacto con su soporte.

11.1.2 Configurar NordVPN

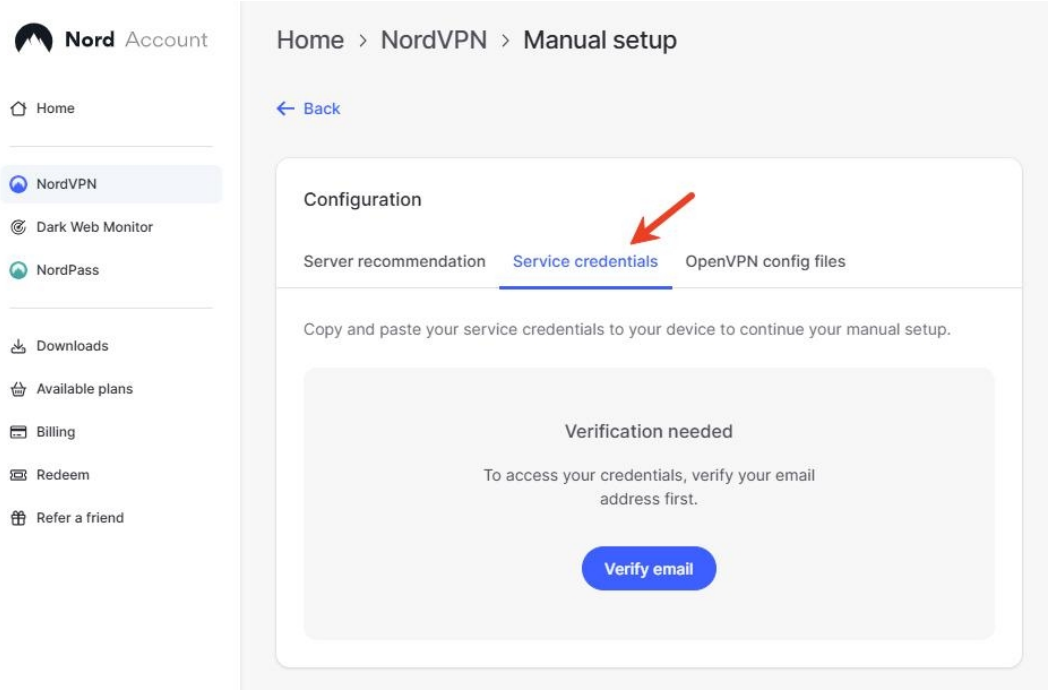
NordVPN está integrado en el panel de administración GL.iNet web . Puede adquirir archivos de configuración para todos los servidores NordVPN introduciendo las credenciales de su cuenta (obtenidas del Panel de NordVPN) en el panel de administración web del enrutador o en la aplicación móvil GL.iNet ,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

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

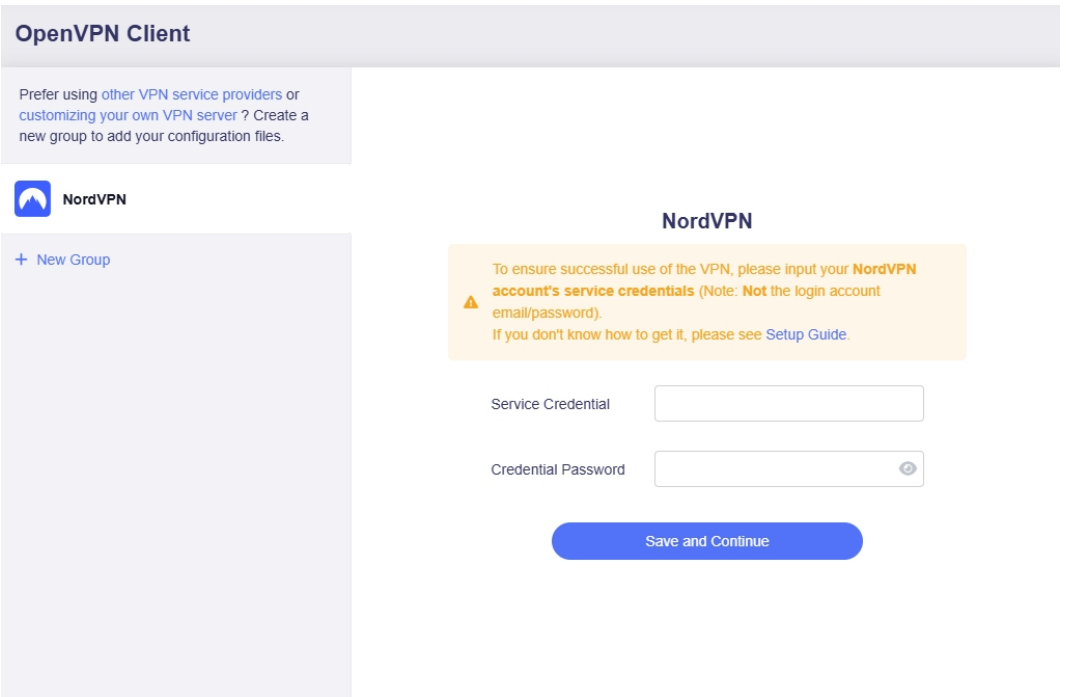
1. Inicie sesión en su cuenta web de NordVPN aquí.
2. Oen el Panel de Nord, haga clic en **NordVPN**, luego haga clic en **Configurar NordVPN manualmente**.



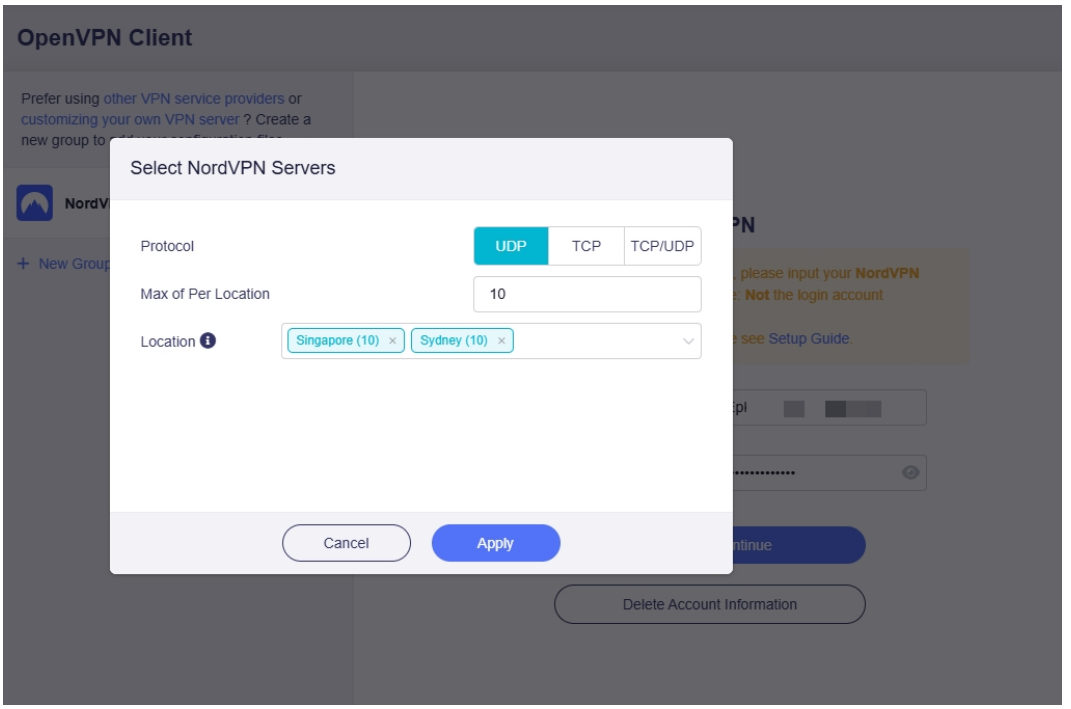
Encontrará el **credenciales de servicio**. Cópielos para usarlos más adelante.



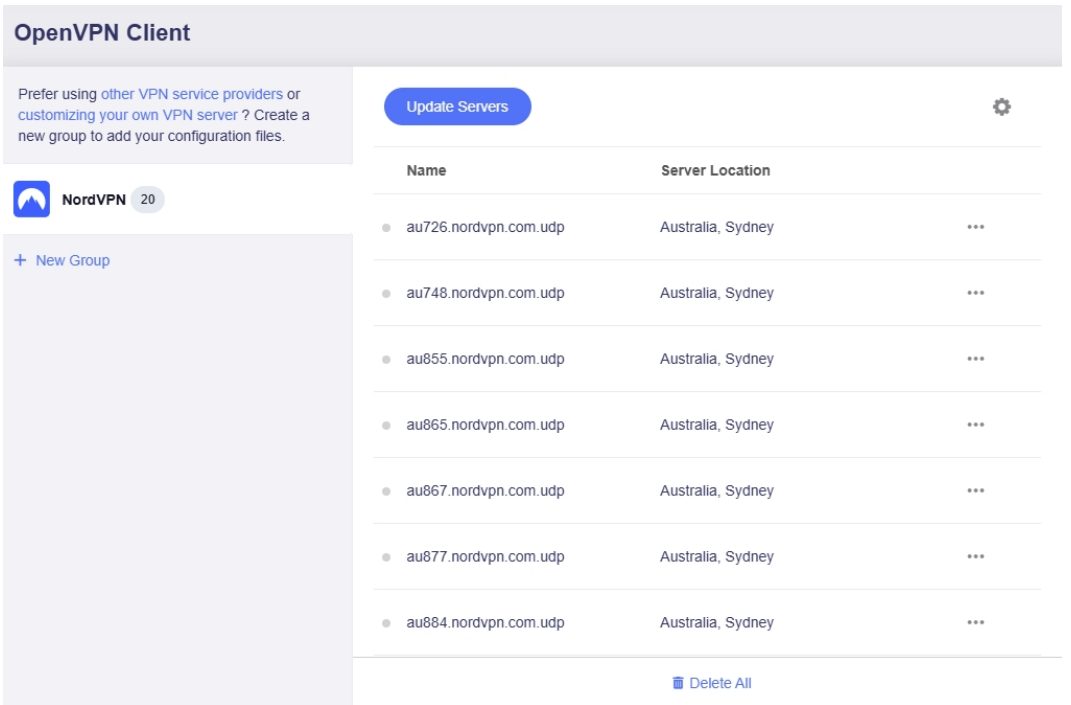
3. Inicie sesión en el panel de administración web de su enrutador y navegue hasta **VPN** > **Cliente OpenVPN** > **NordVPN**. Introduzca las credenciales del servicio (Nota: NO es el correo electrónico ni la contraseña de la cuenta de inicio de sesión), luego haga clic en **Guardar y continuar**.



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

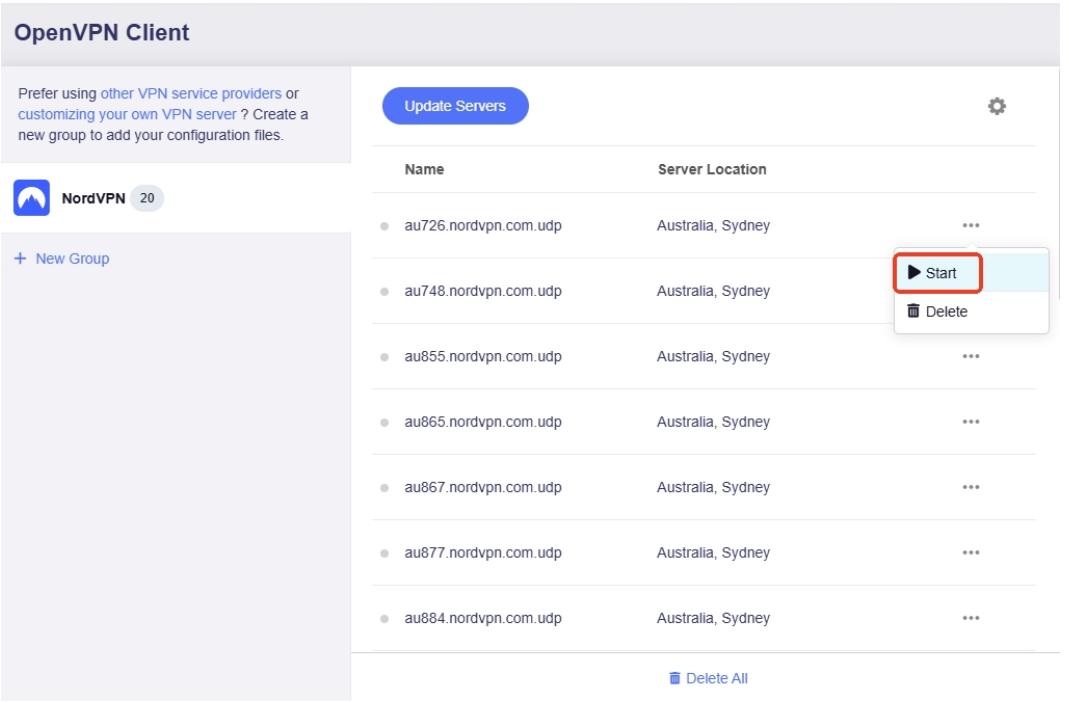


Descargará archivos de configuración.

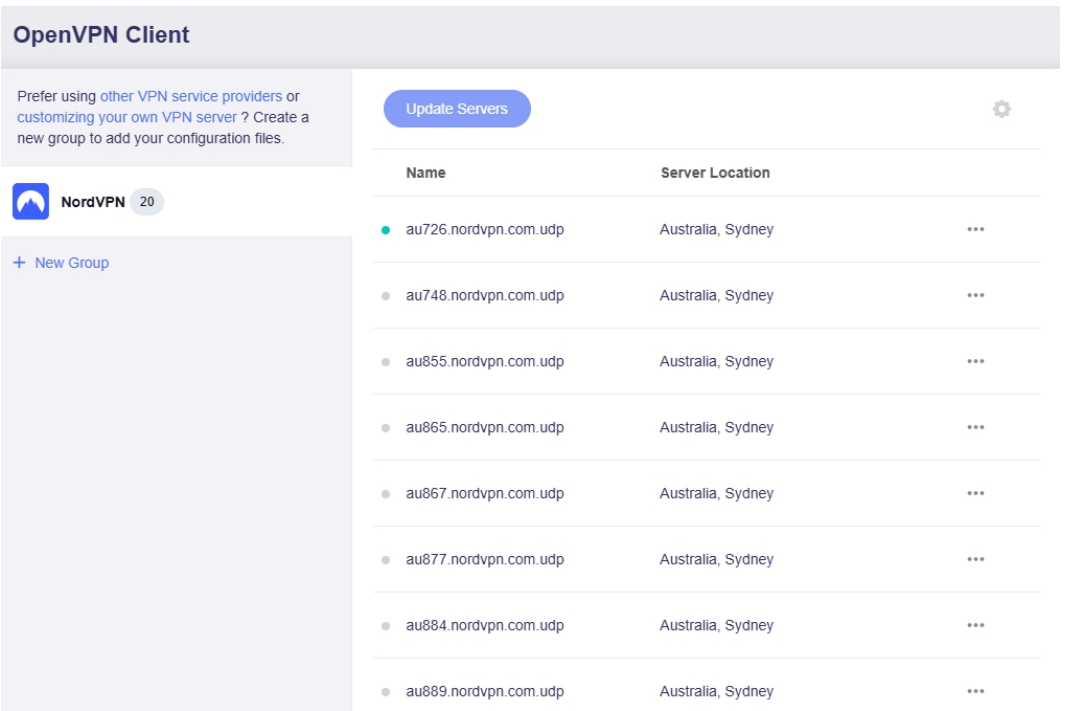


5. Iniciará una conexión.

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



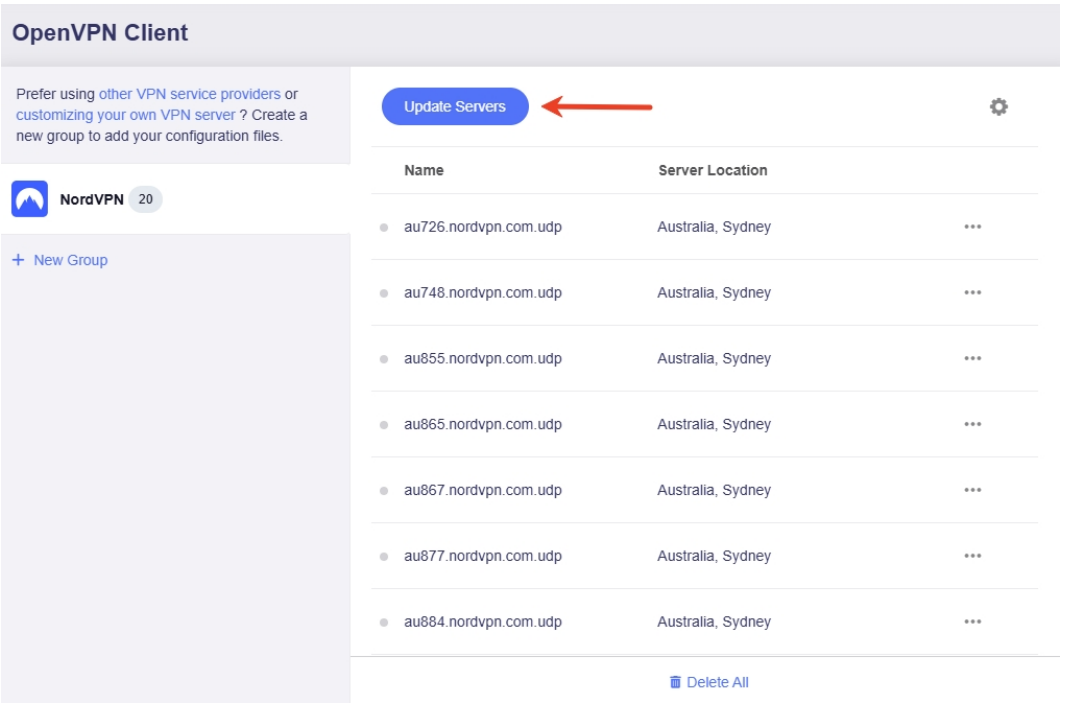
6. Una vez conectado, aparecerá un punto verde junto a el archivo de configuración.



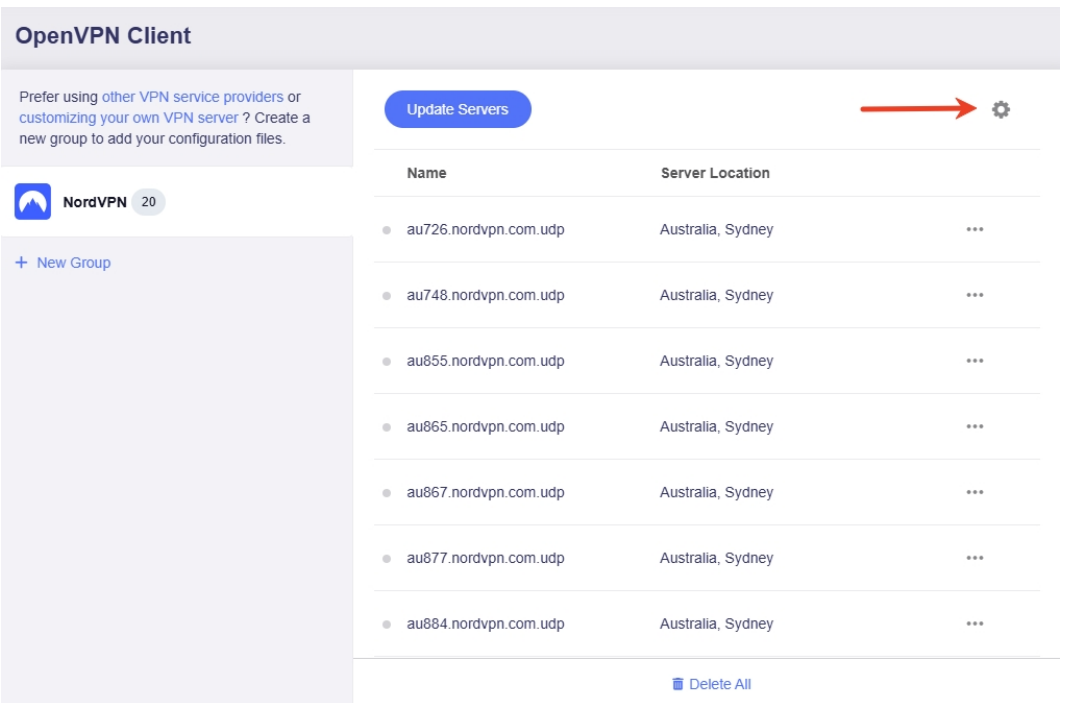
También puede consultar los detalles de la conexión VPN en el **Panel de VPN**.

7. Actualizar servidores.

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.

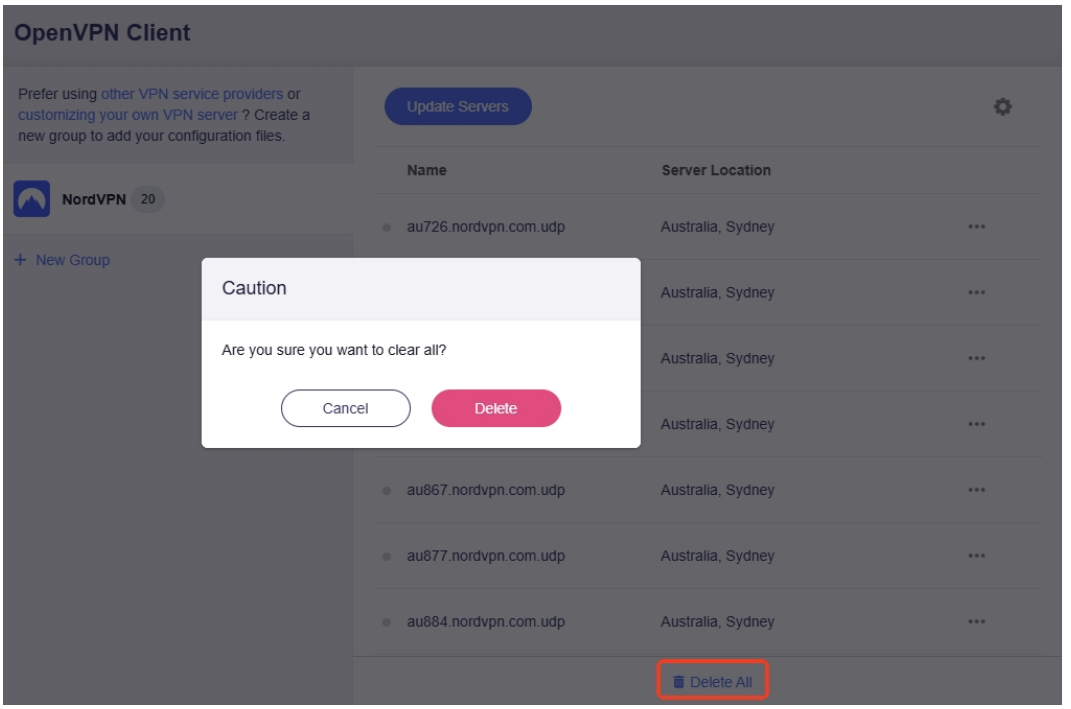


8. Editar credenciales.
   Haga clic en el ícono de ajustes para editar sus credenciales de inicio de sesión.



9. Eliminar todos los archivos.

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

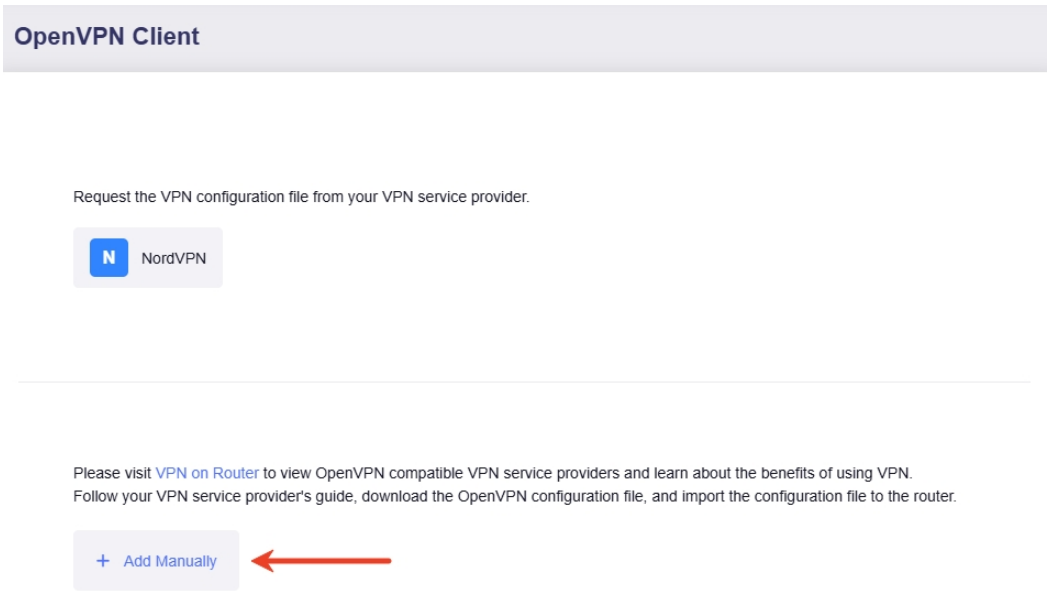


11.1.3 Configurar el cliente OpenVPN manualmente (para otros proveedores)

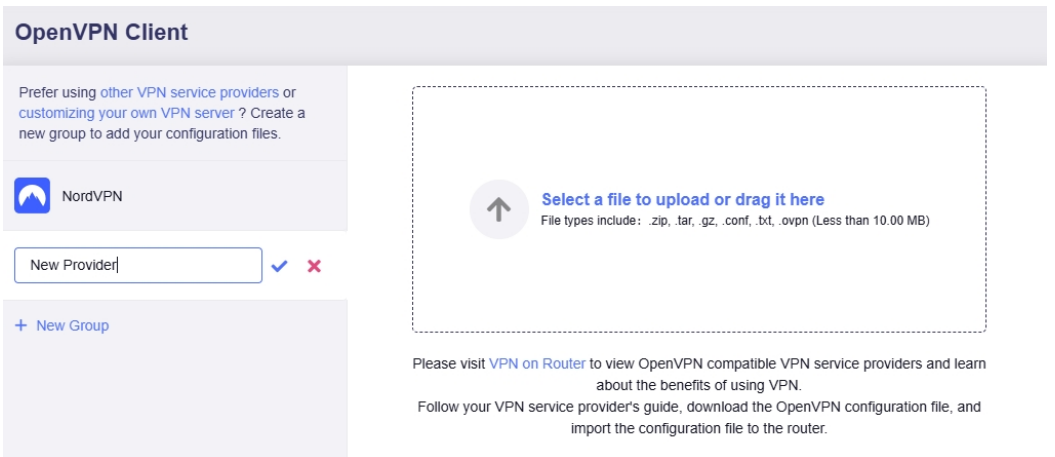
Si su proveedor de servicios OpenVPN no está integrado en nuestro panel de administración, primero visite el sitio web oficial de su proveedor de servicios suscrito para obtener el archivo de configuración. Luego cárguelo en el enrutador para configurar un cliente OpenVPN.

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

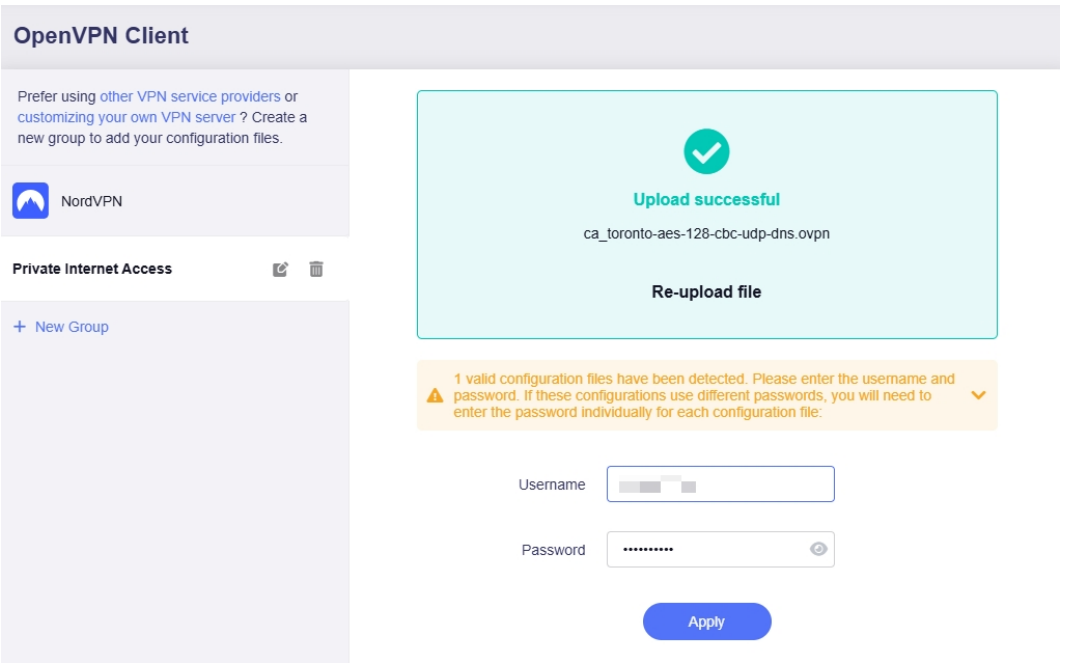
1. Descargue un archivo de configuración del sitio web oficial de Private Internet Access.
2. Inicie sesión en el panel de administración web de su enrutador, navegue hasta **VPN** > **Cliente OpenVPN** y haga clic en **Agregar manualmente**.



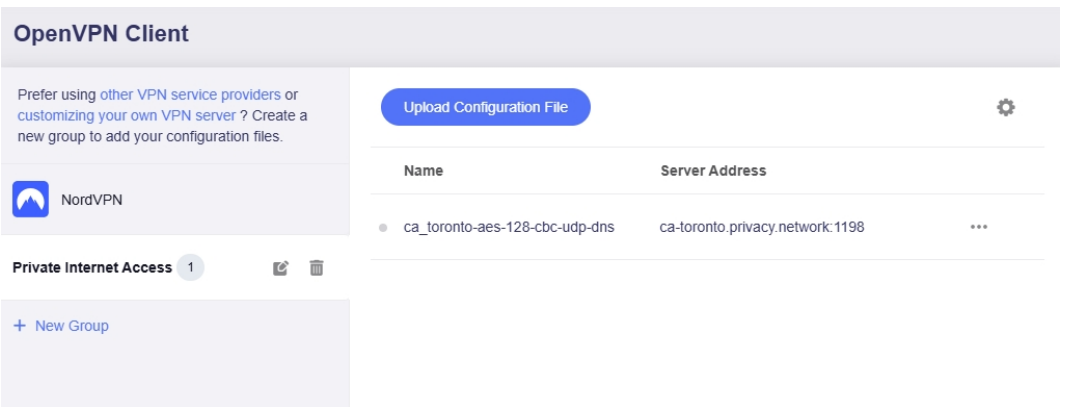
3. Se creará un grupo en la barra lateral izquierda.Establezca un nombre descriptivo para el grupo.



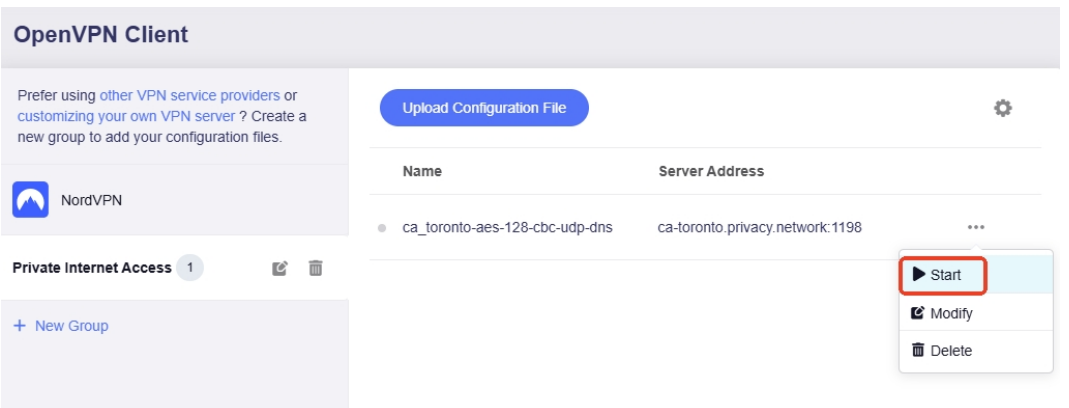
4. Cargue su archivo de configuración OpenVPN. Ingrese las credenciales si es necesario, luego haga clic en **Aplicar**.



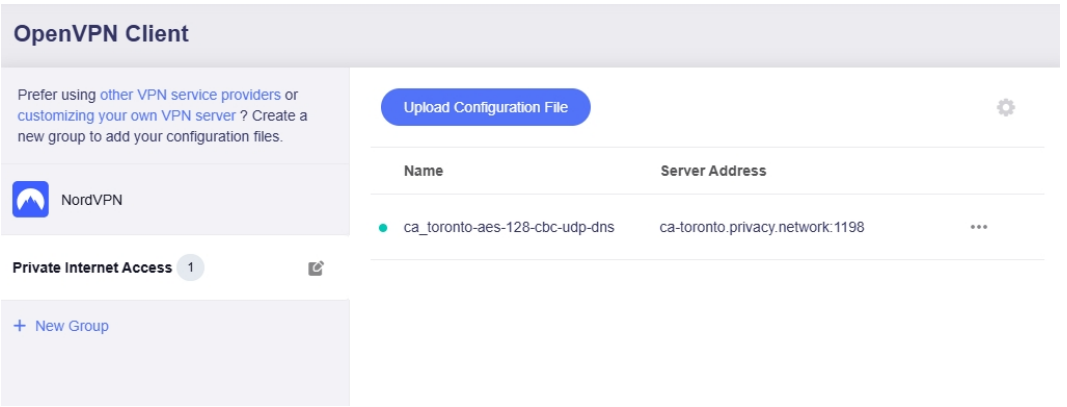
YVerá el archivo de configuración cargado.



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.

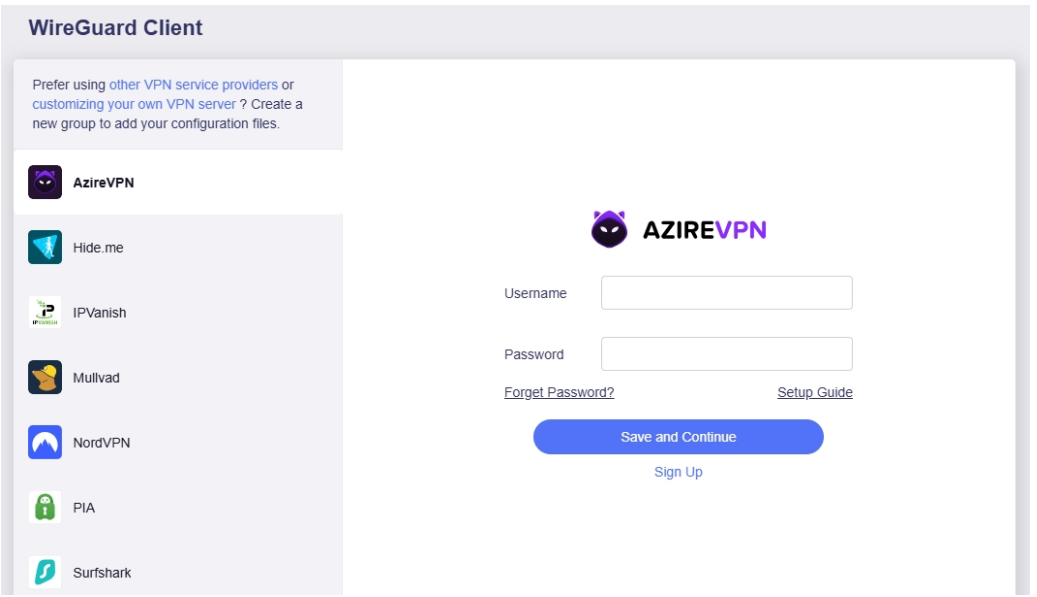
A continuación, sseleccione el proveedor de servicios WireGuard correspondiente a continuación para localizar rápidamente las instrucciones paso a paso.

- 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)

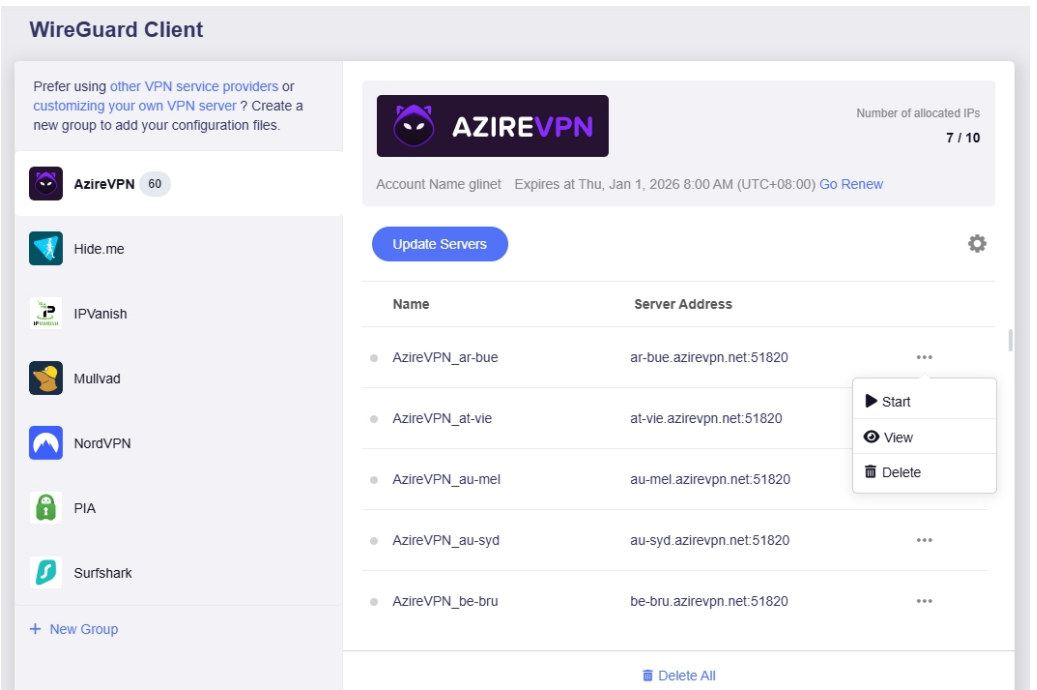
11.2.2 Configurar AzireVPN

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

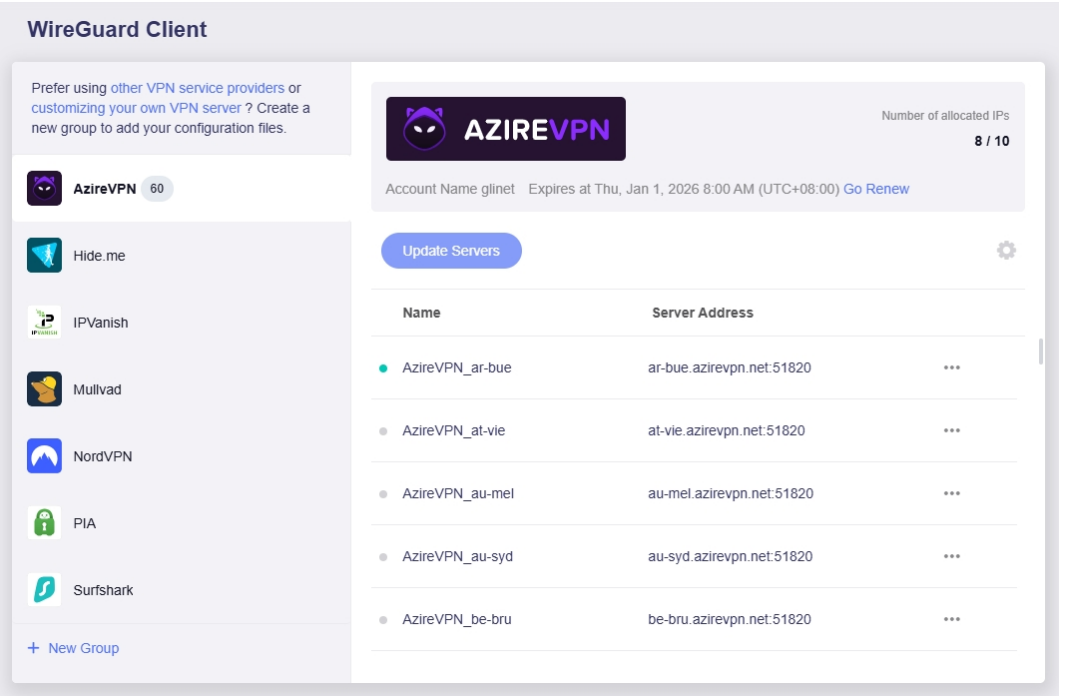
1. Inicie sesiónn en su enrutador’s web admin panel y vaya a **VPN** > **Cliente WireGuard** > **AzireVPN**.
2. Ingrese nombre de usuario y contraseña, luego haga clic en **Guardar y continuar**. Generará archivos de configuración para cada servidor.



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



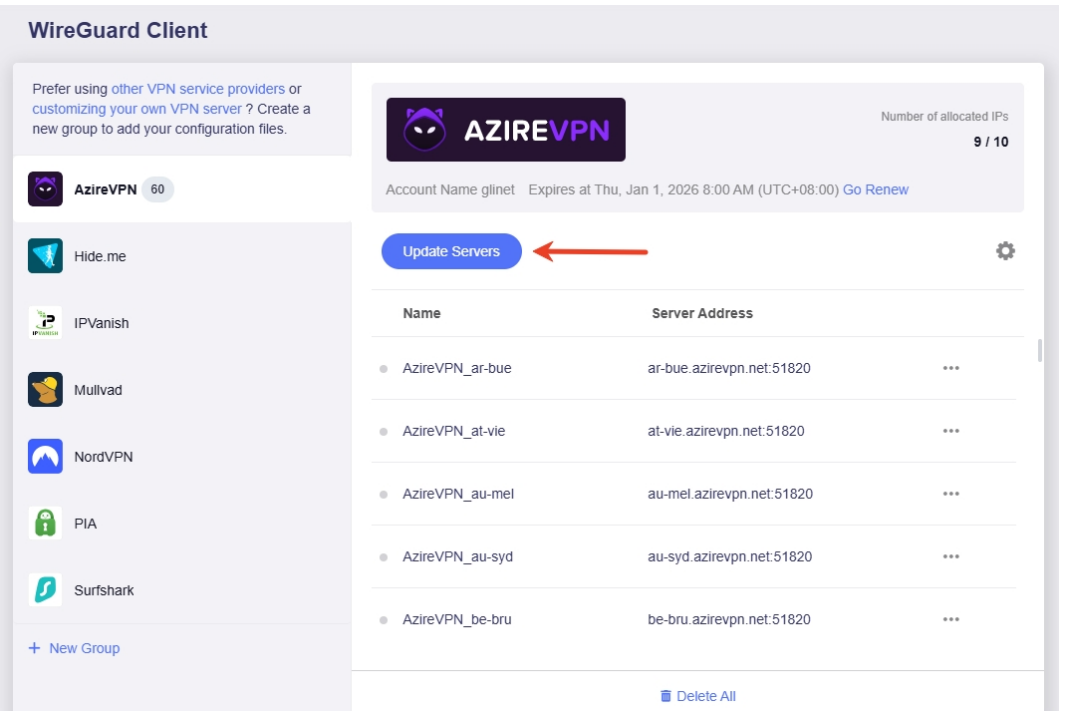
4. Una vez conectado, aparecerá un punto verde junto al archivo de configuración.



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

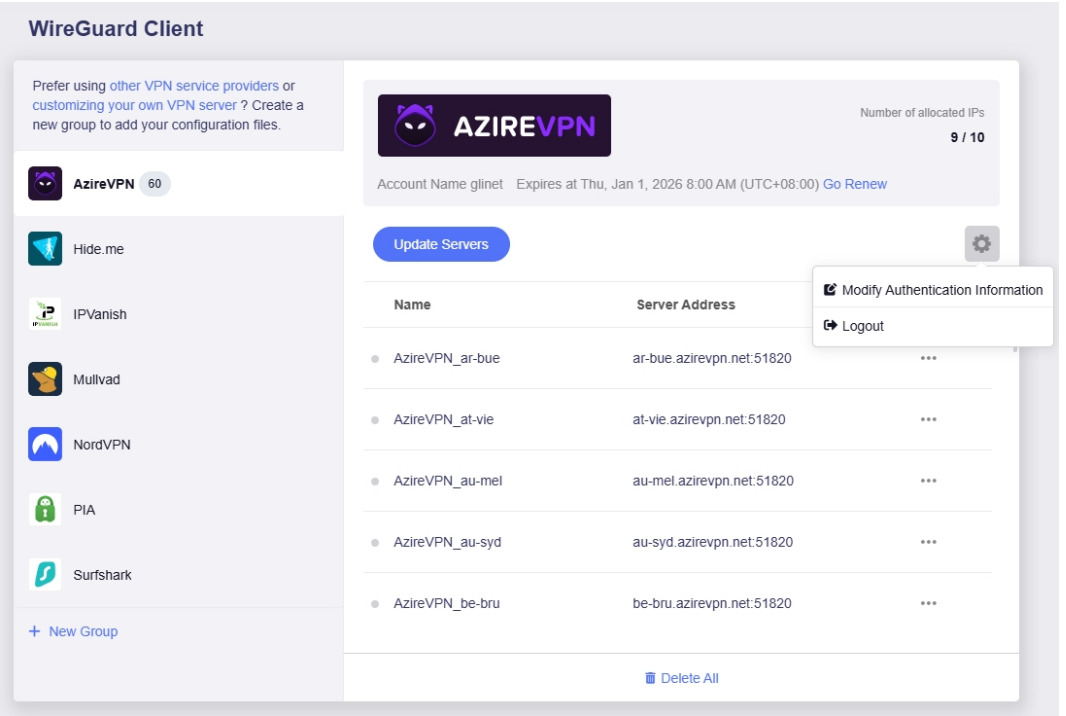
5. Actualizar servidores.

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



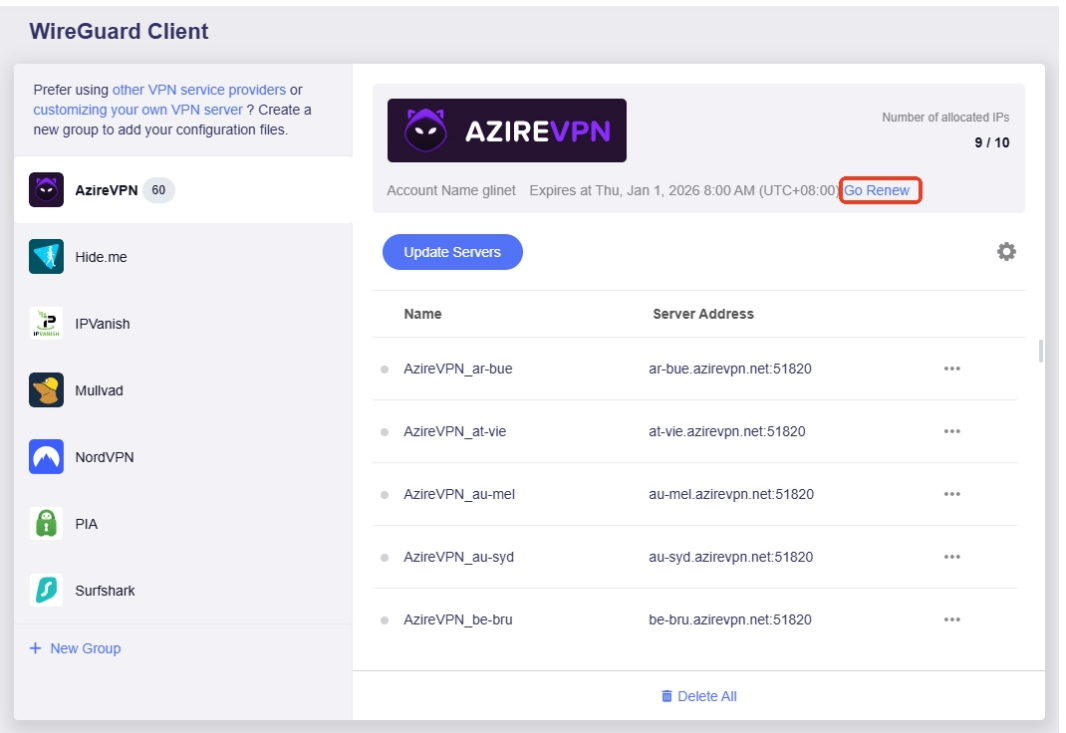
6. Editar credenciales o cerrar sesión.

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



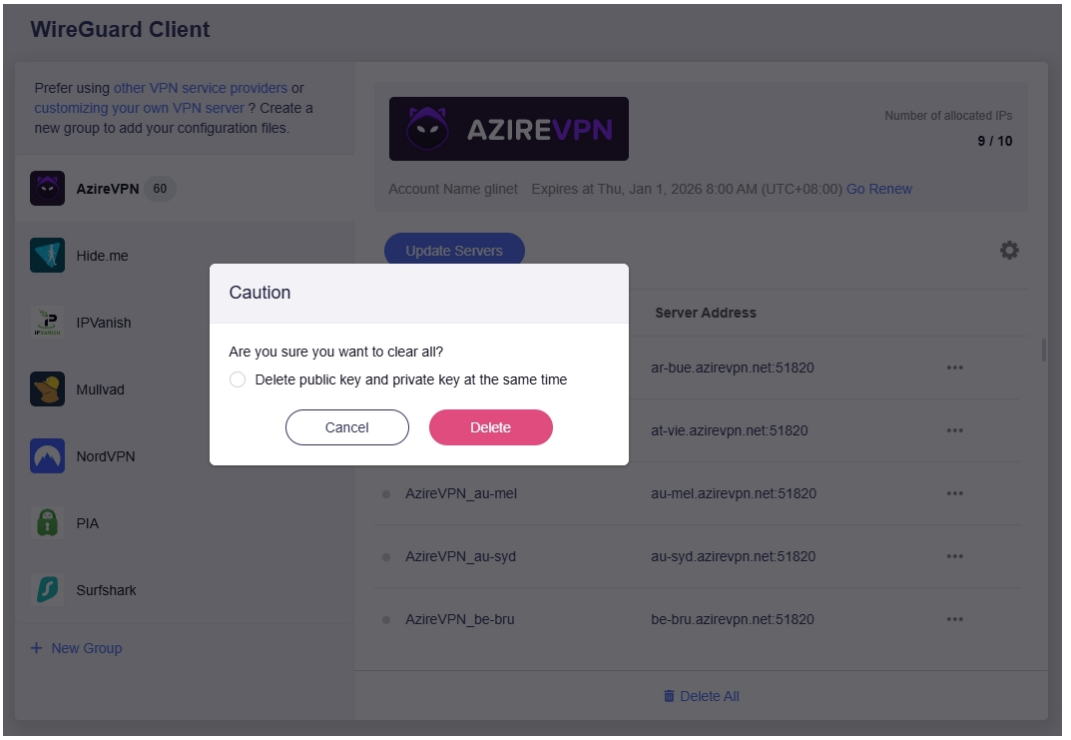
7. Ir a renovar.

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



8. Eliminar todos los archivos.

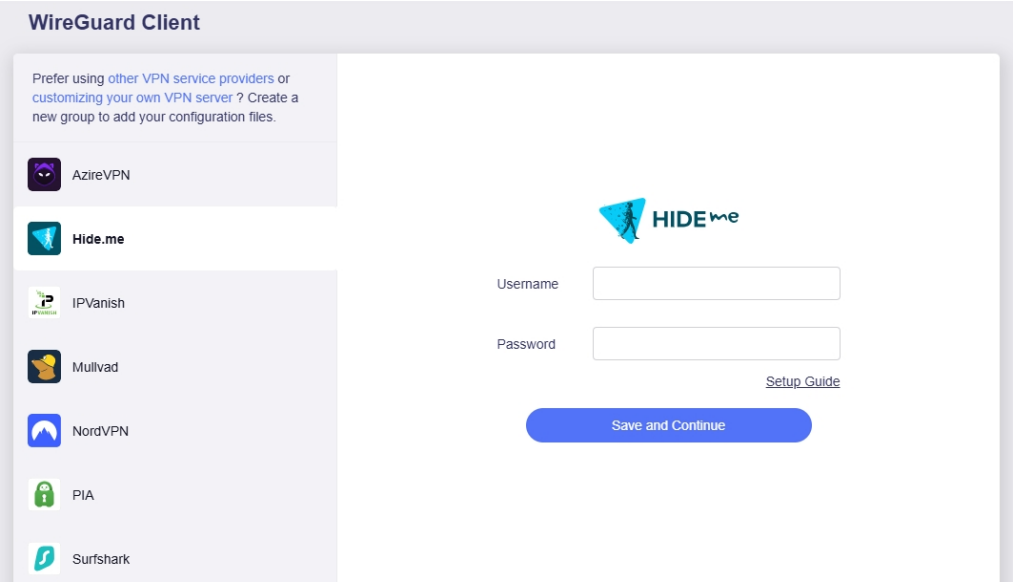
   Puede hacer clic en **Eliminar todo** para eliminar todos los archivos de configuración con un solo clic y elegir si desea eliminar el archivo privado. y claves públicas simultáneamente.



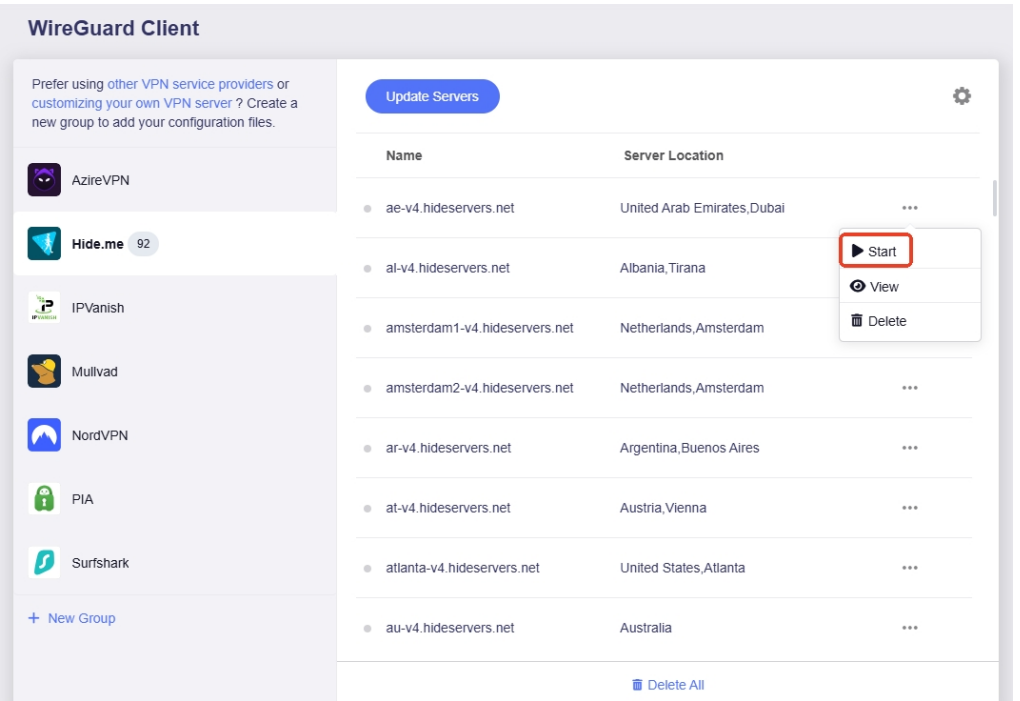
11.2.3 Configurar Hide.me

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

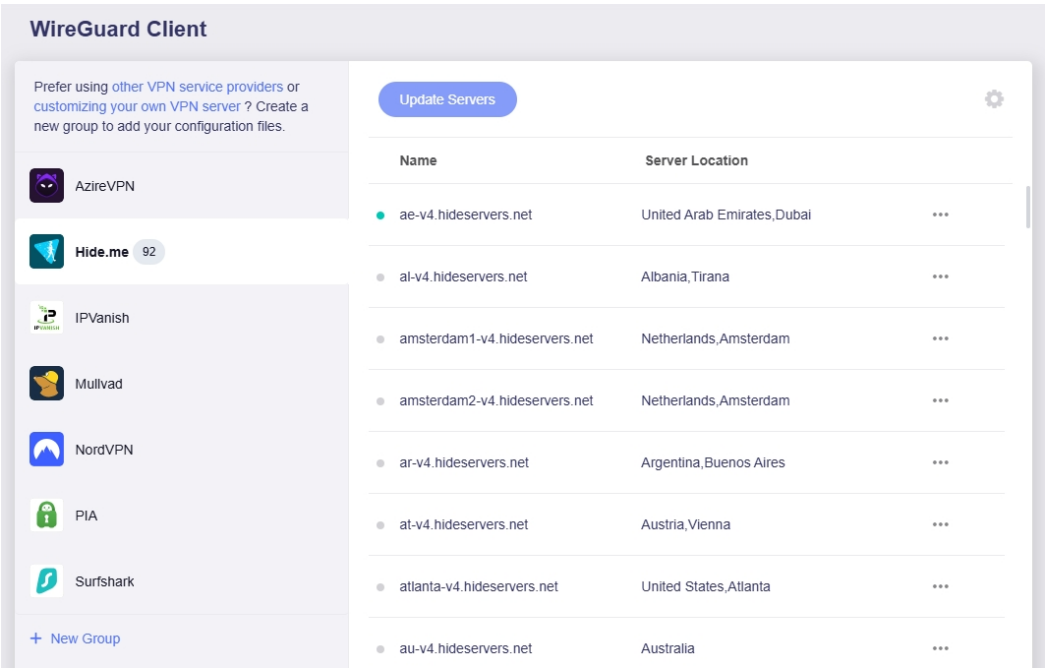
1. Inicie sesiónn en su enrutador’s web admin panel y vaya a **VPN** > **WireGuard Client** > **Hide.me**.
2. Ingrese nombre de usuario y contraseña, luego haga clic en **Guardar y continuar**. Generará archivos de configuración para cada servidor.



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



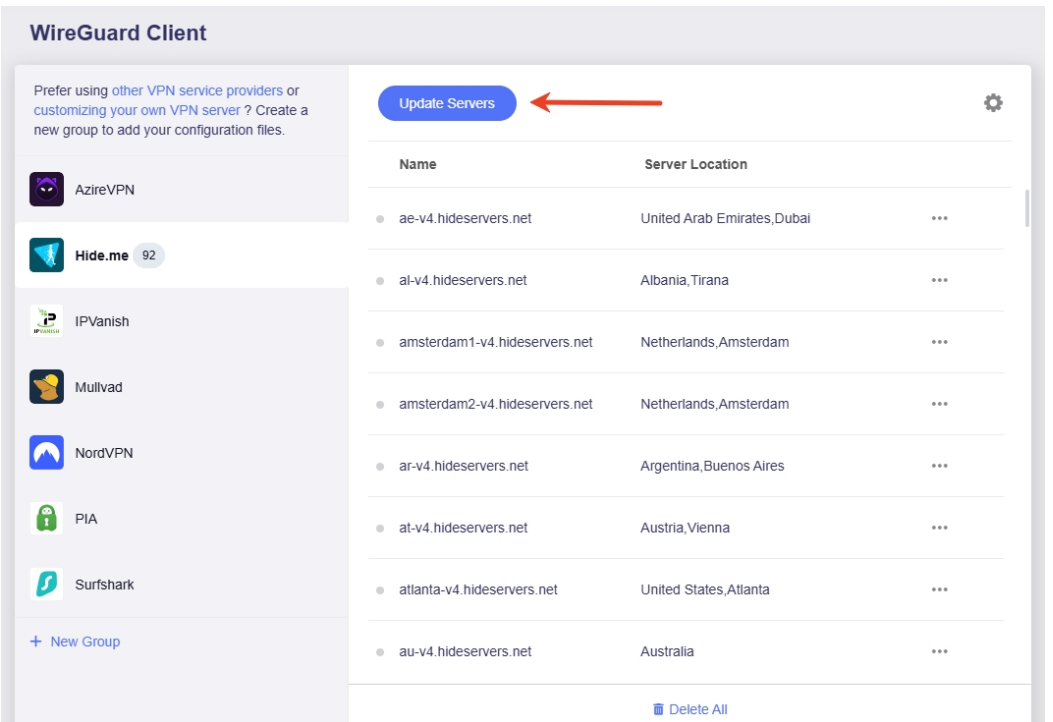
4. Una vez conectado, aparecerá un punto verde junto al archivo de configuración.



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

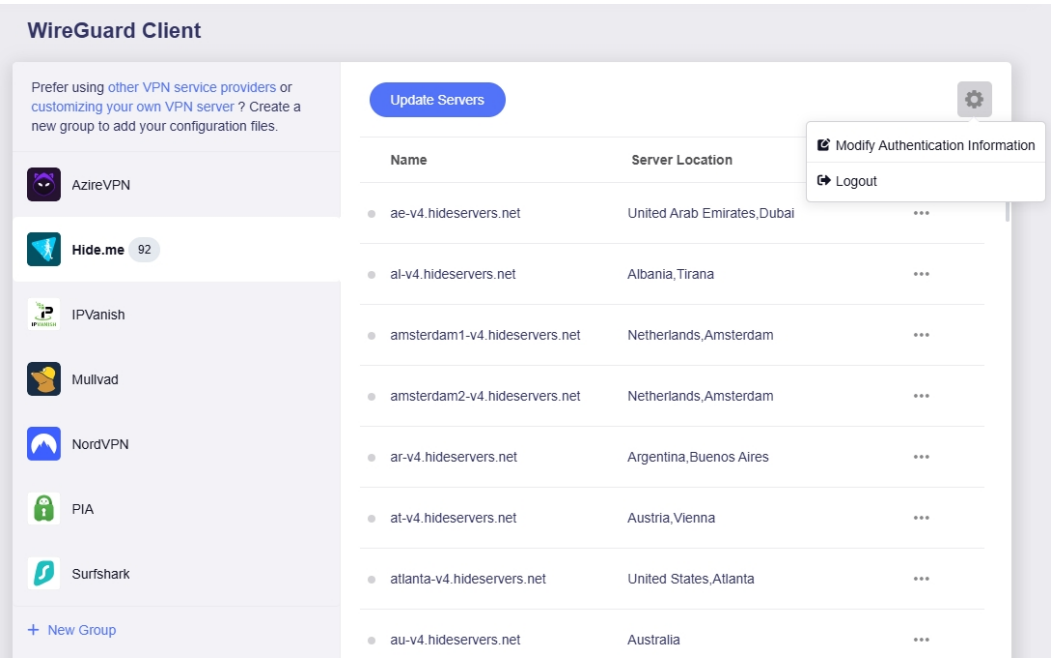
5. Actualizar servidores.

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



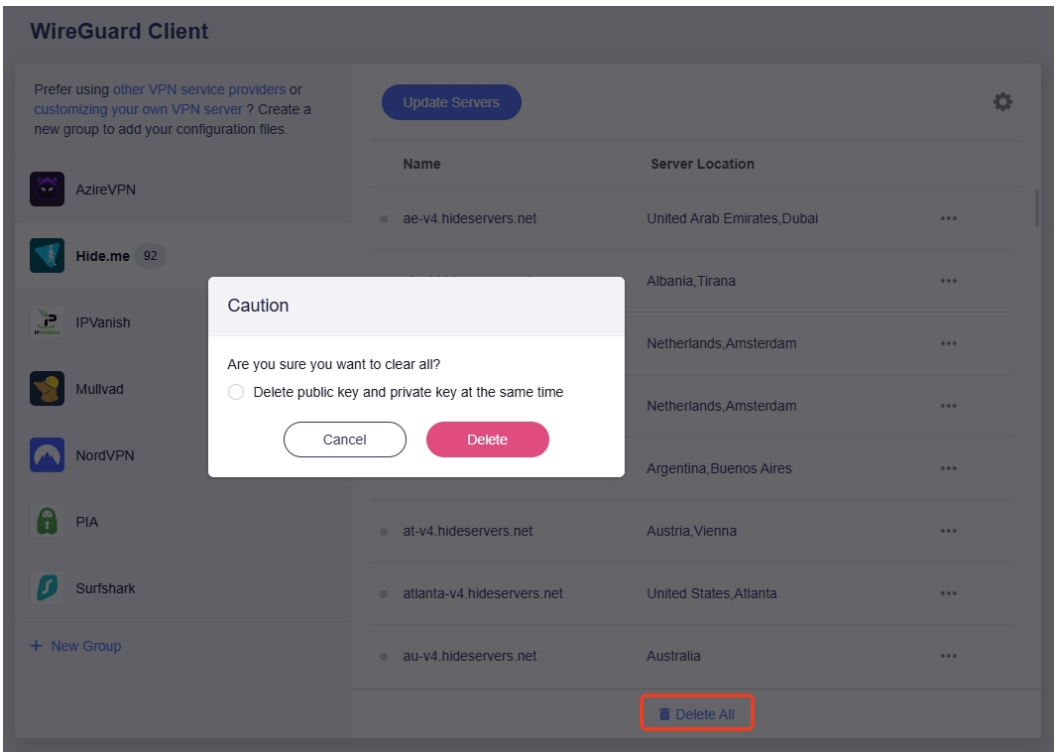
6. Editar credenciales o cerrar sesión.

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



7. Eliminar todos los archivos.

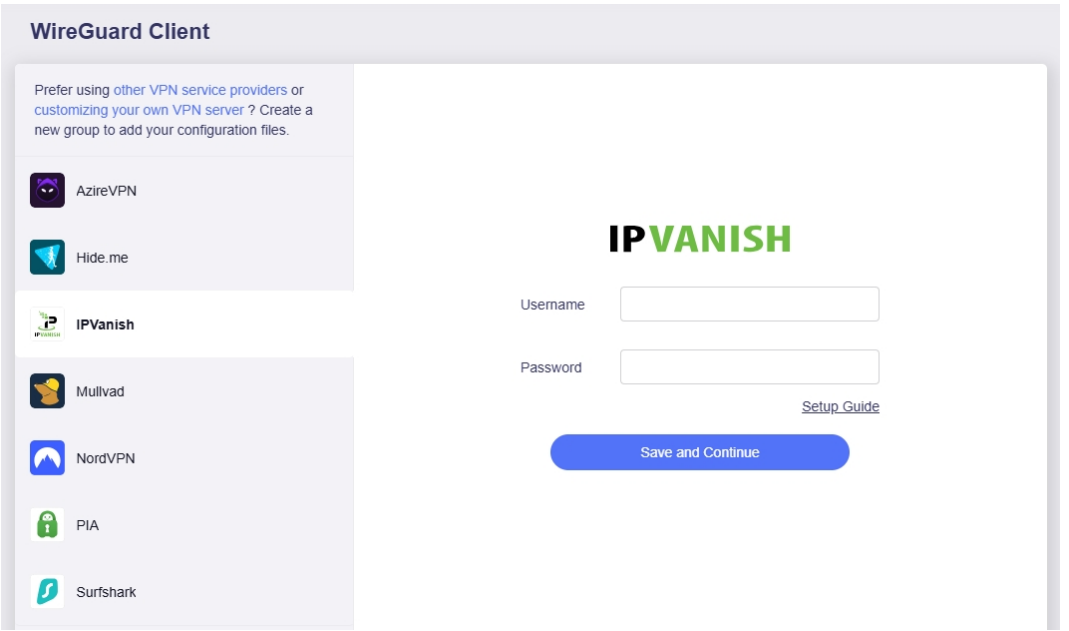
   Puede hacer clic en **Eliminar todo** para eliminar todos los archivos de configuración con un solo clic y elegir si desea eliminar las claves públicas y privadas simultáneamente.



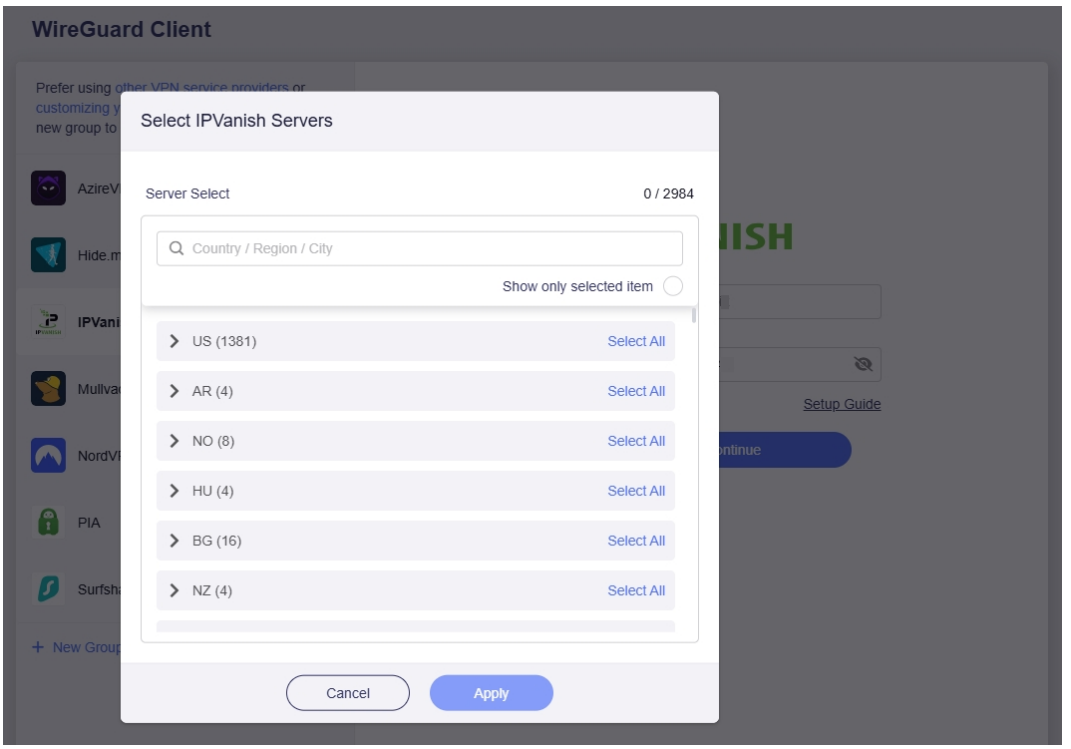
11.2.4 Configurar IPVanish

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

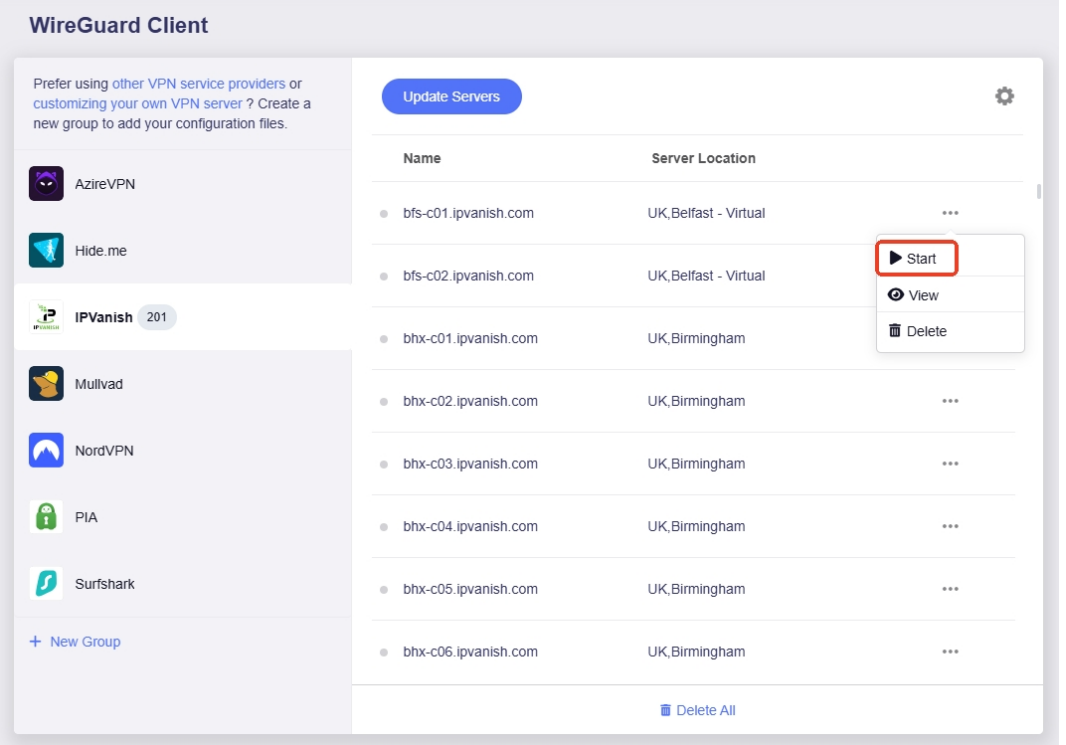
1. Inicie sesiónn en su enrutador’s web admin panel y vaya a **VPN** > **Cliente WireGuard** > **IPVanish**.
2. Ingrese nombre de usuario y contraseña, luego haga clic en **Guardar y continuar**.



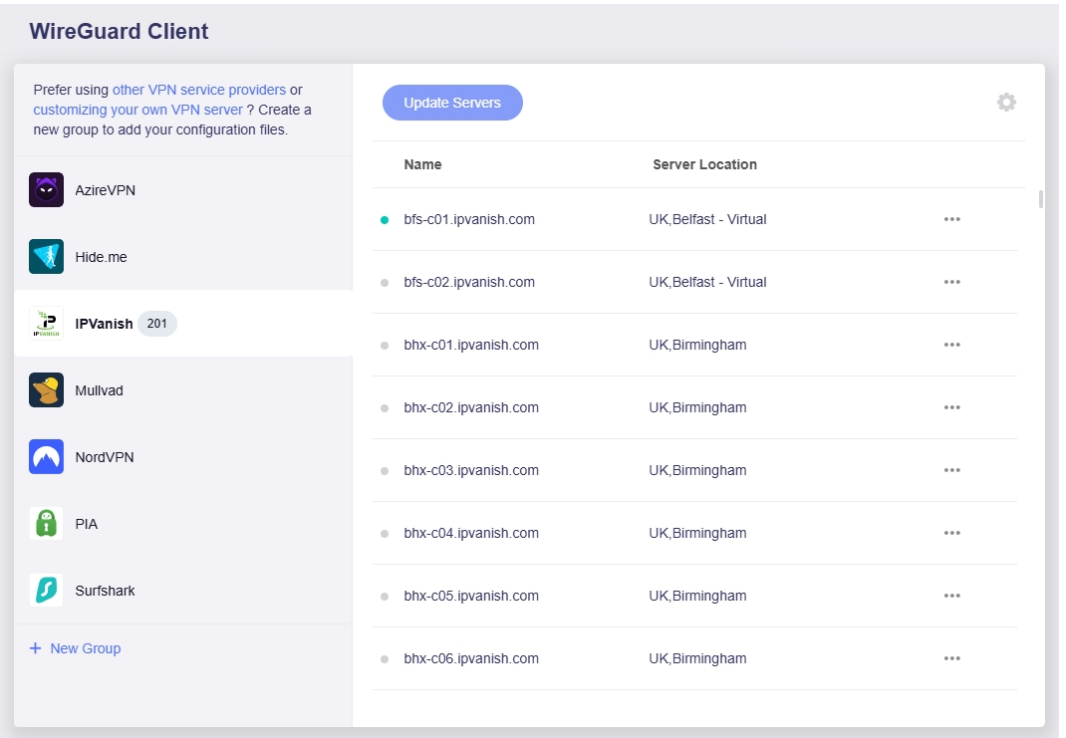
3. Seleccione los servidores a los que desea conectarse y haga clic en **Aplicar**.



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



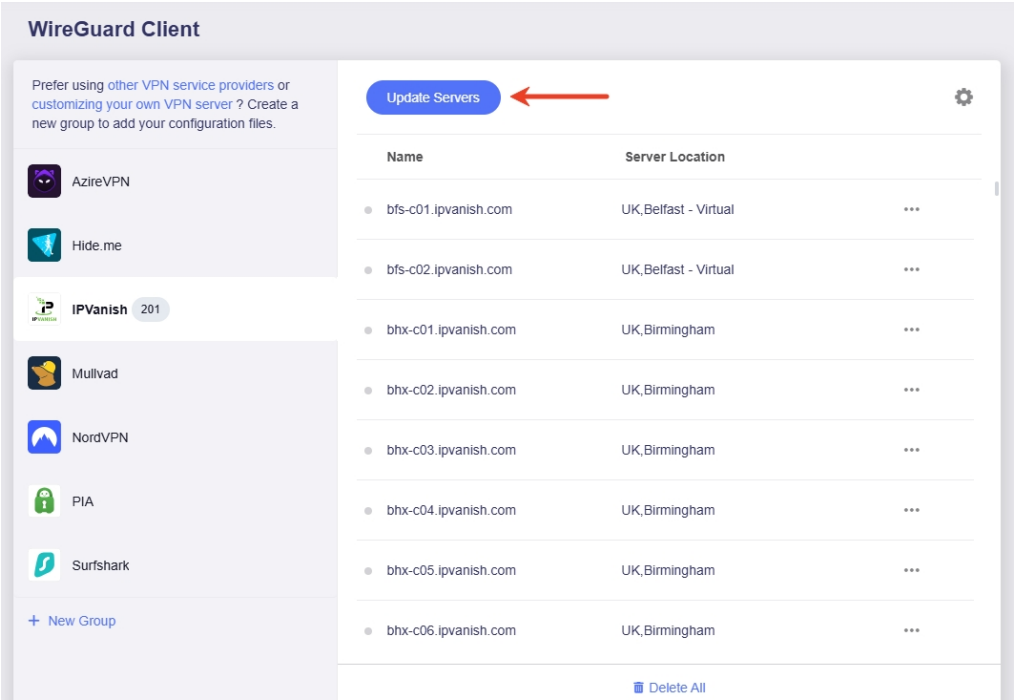
5. Una vez conectado, aparecerá un punto verde junto al archivo de configuración.



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

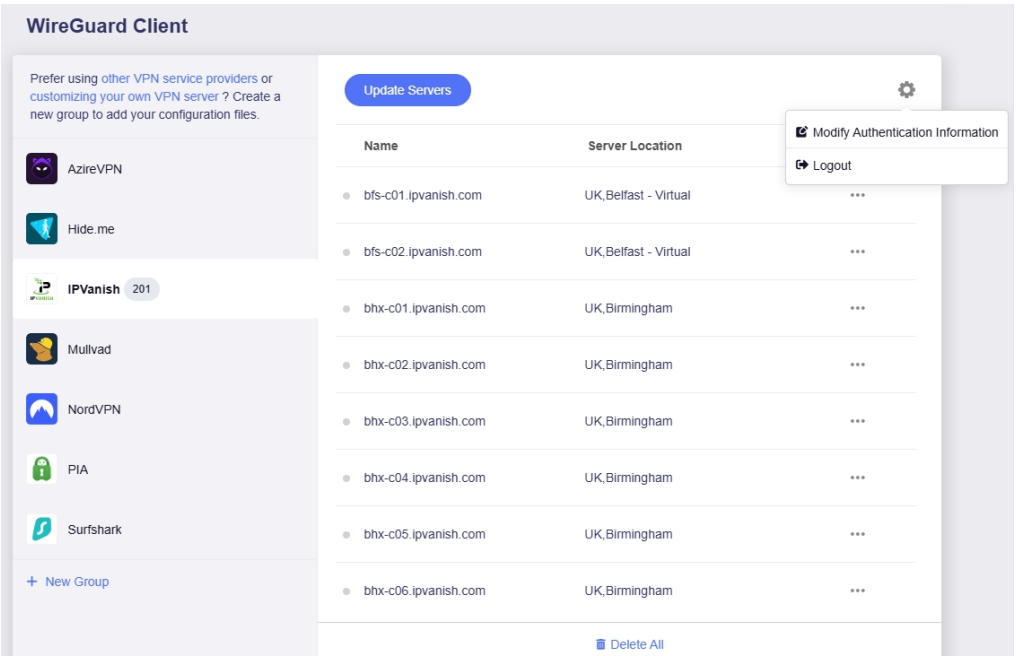
6. Actualizar servidores.

   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.



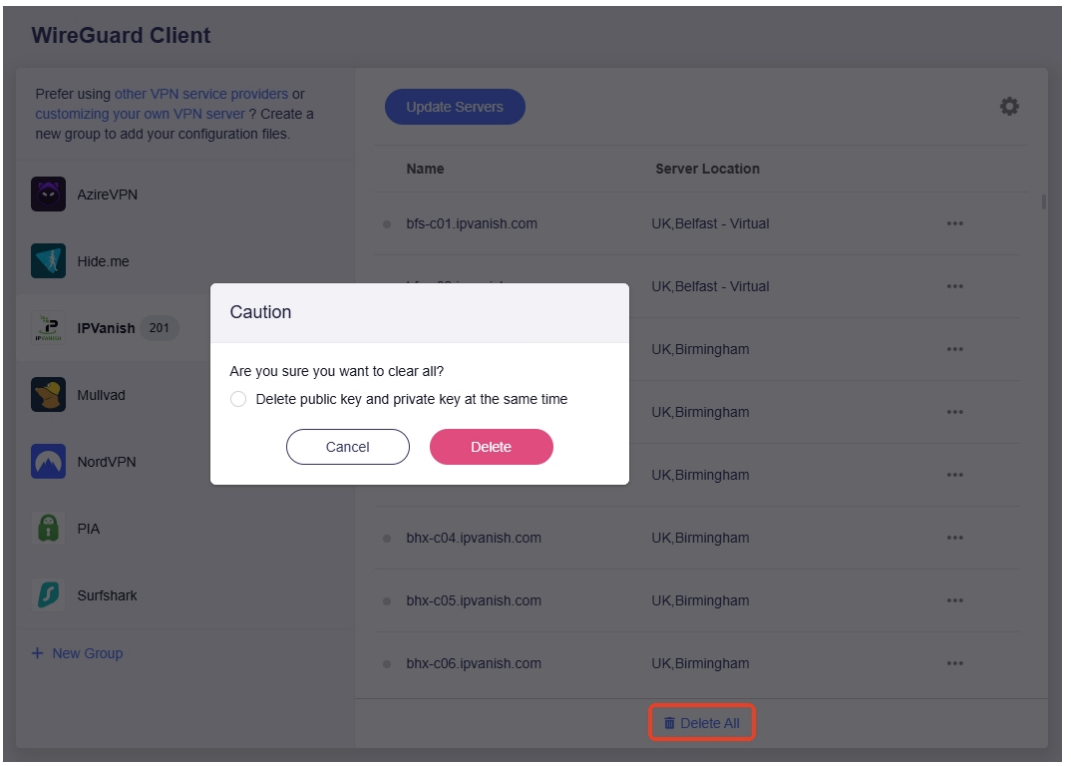
7. Edite las credenciales o cierre sesión.

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



8. Eliminar todos los archivos.

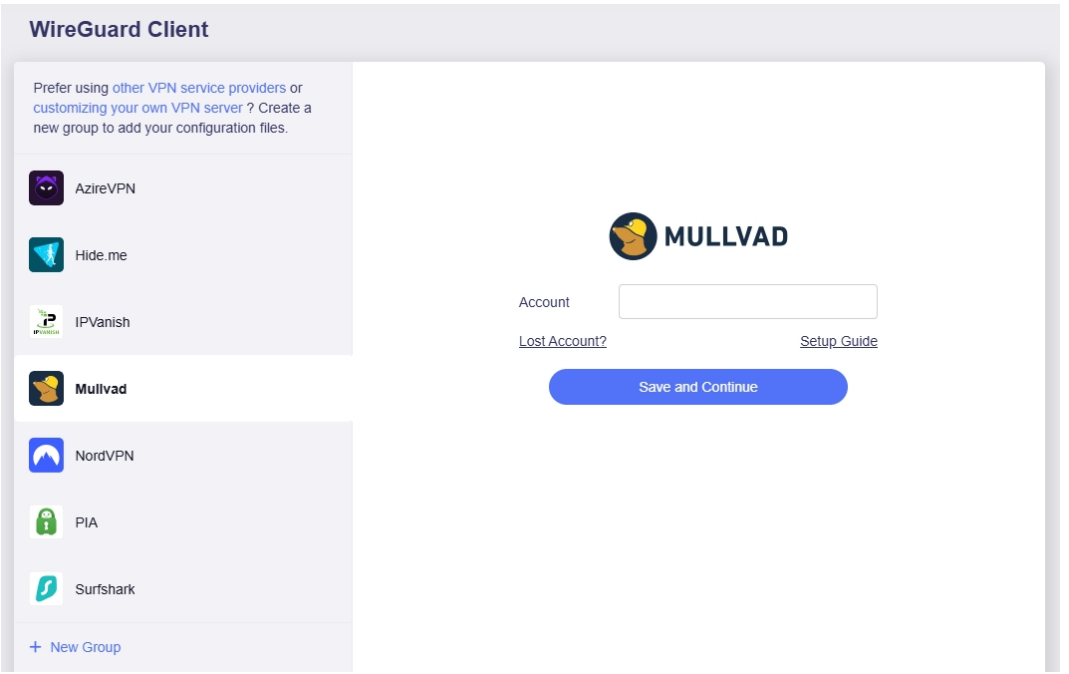
   Puede hacer clic en **Eliminar todo** para eliminar todos los archivos de configuración con un solo clic y elegir si desea eliminar las claves pública y privada simultáneamente.



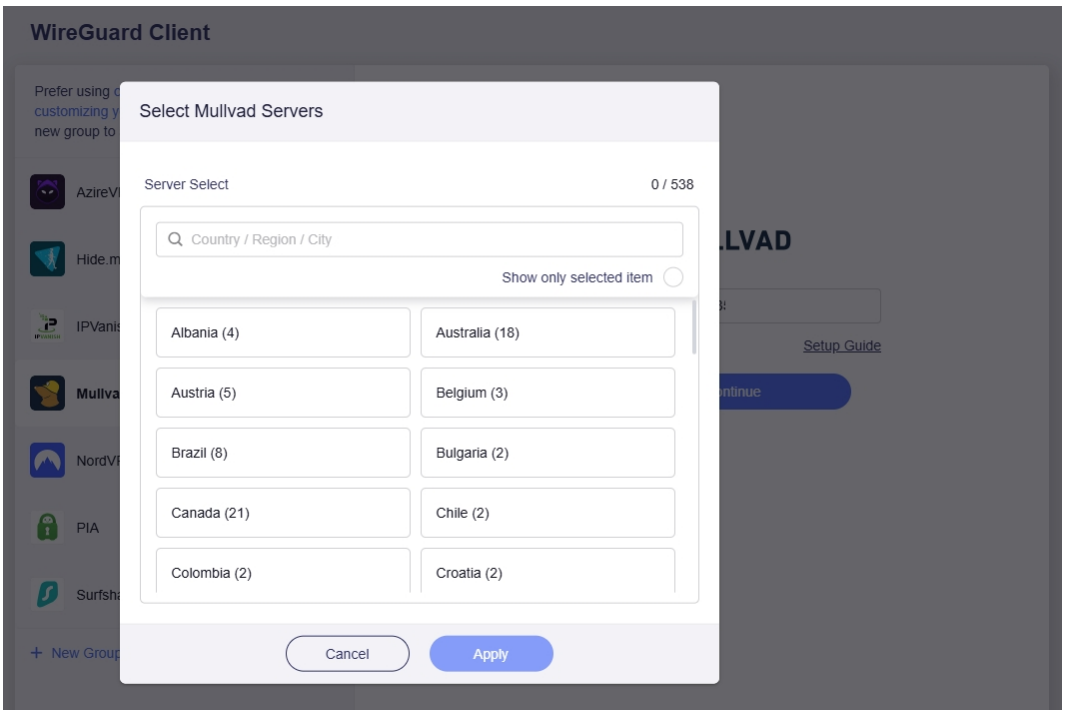
11.2.5 Configurar Mullvad

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

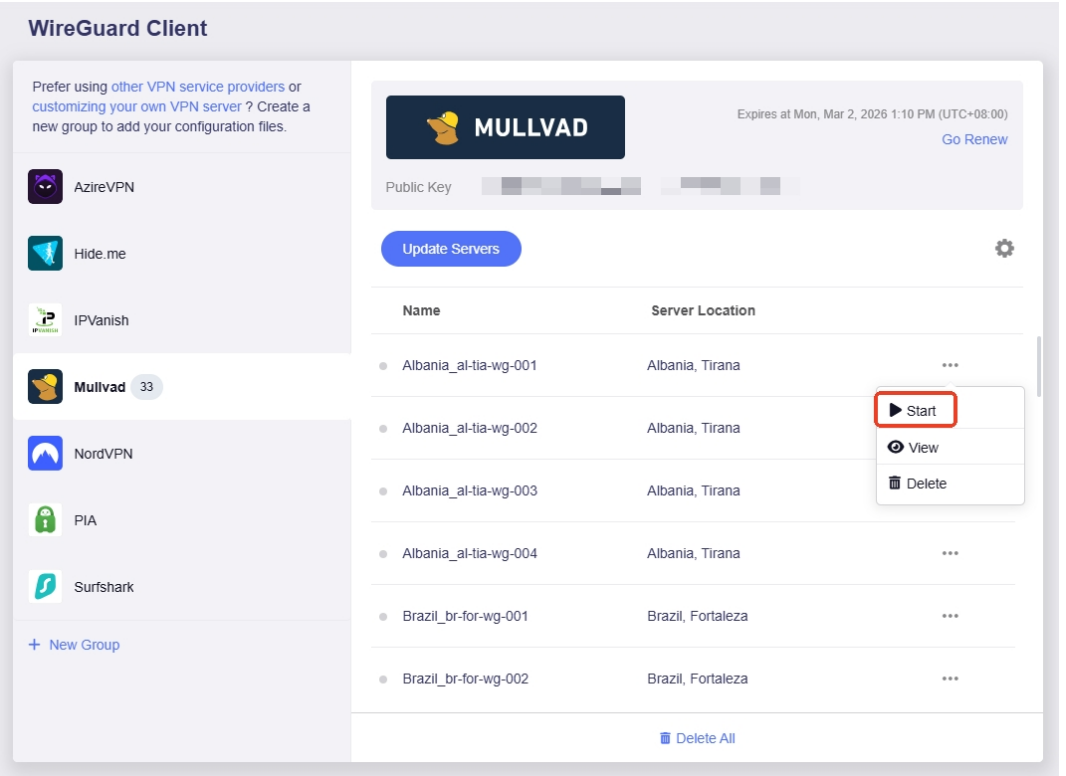
1. Iniciar sesiónn a su enrutador’s web admin panel y vaya a **VPN** > **WireGuard Client** > **Mullvad**.
2. Ingrese nombre de usuario y contraseña, luego haga clic en **Guardar y continuar**.



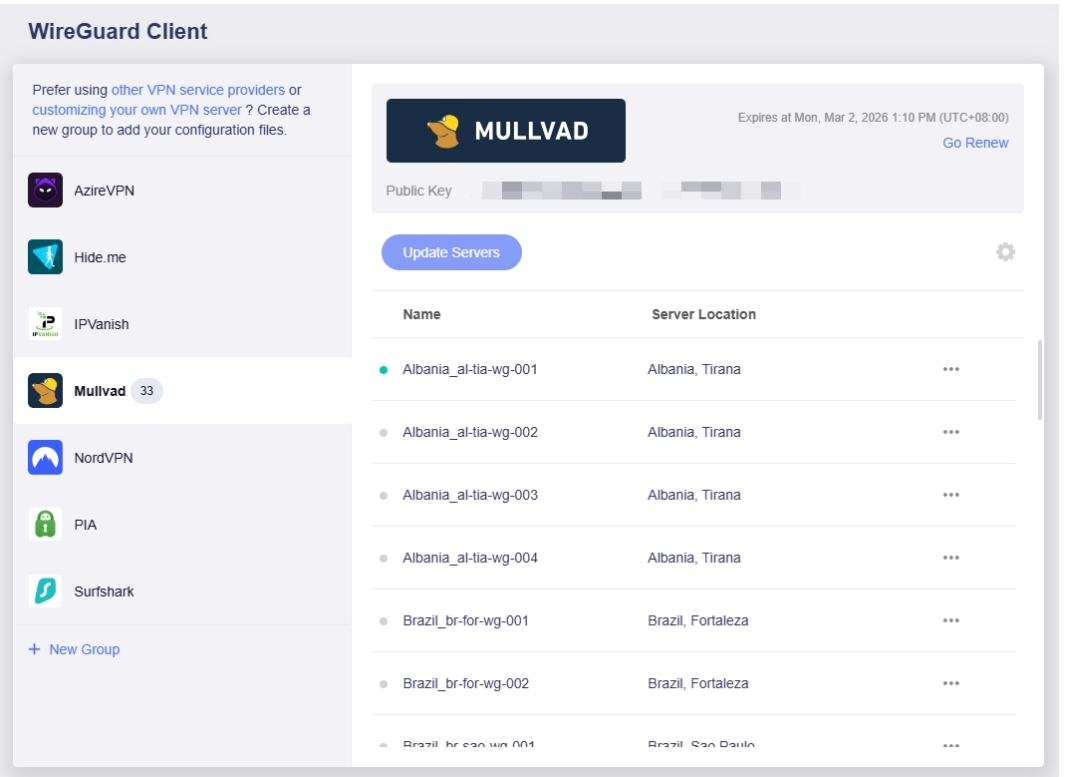
3. Seleccione los servidores a los que desea conectarse y haga clic en **Aplicar**.



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



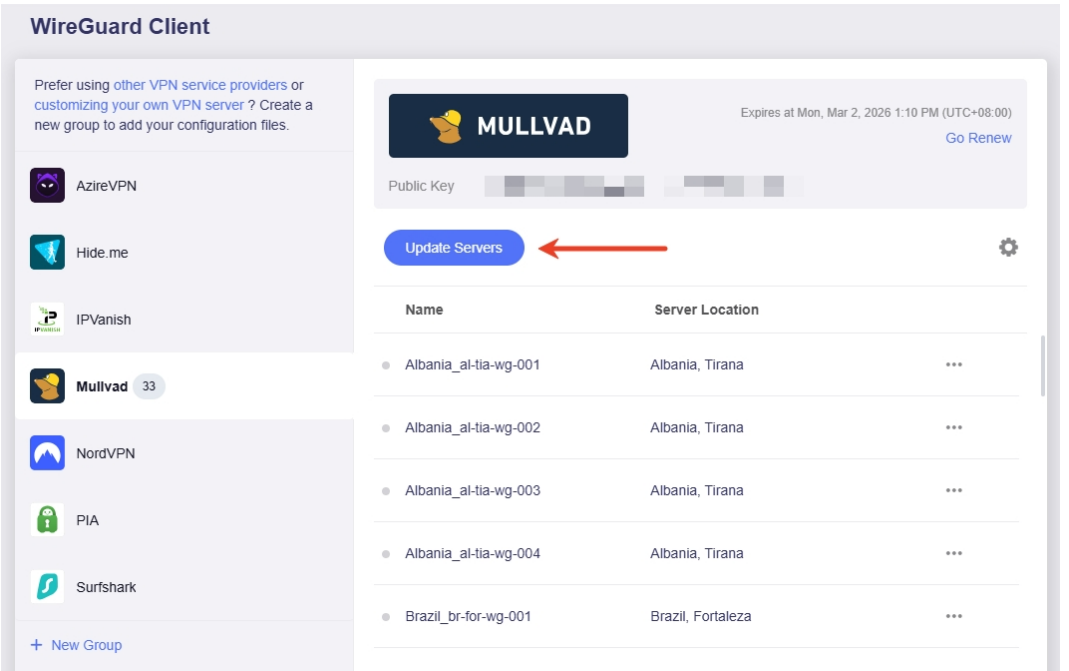
5. Una vez conectado, aparecerá un punto verde junto al archivo de configuración.



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

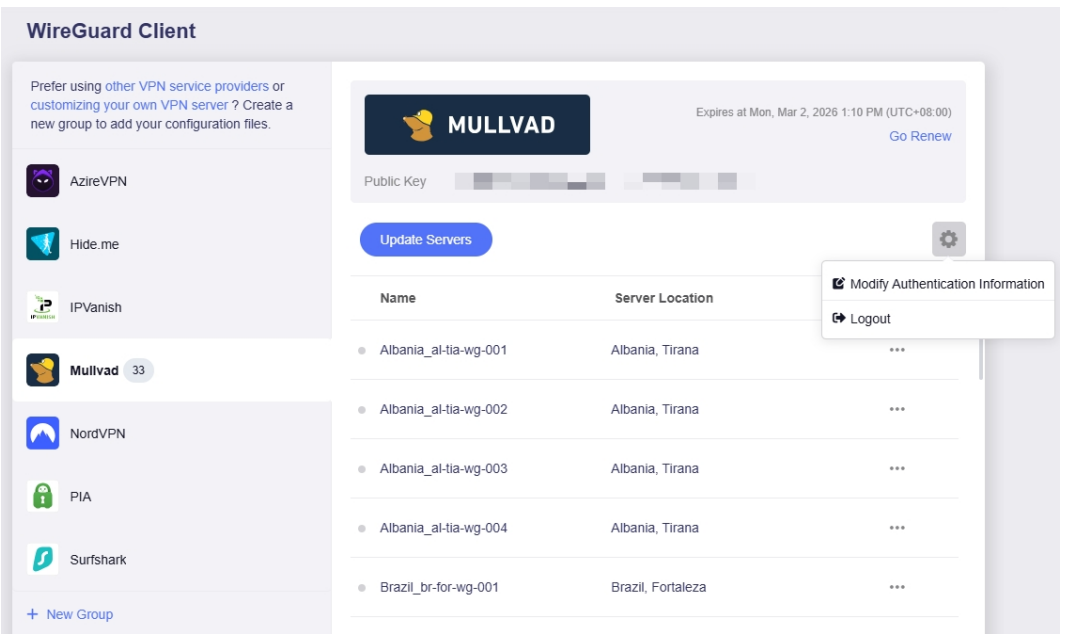
6. Actualice los servidores.

   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.



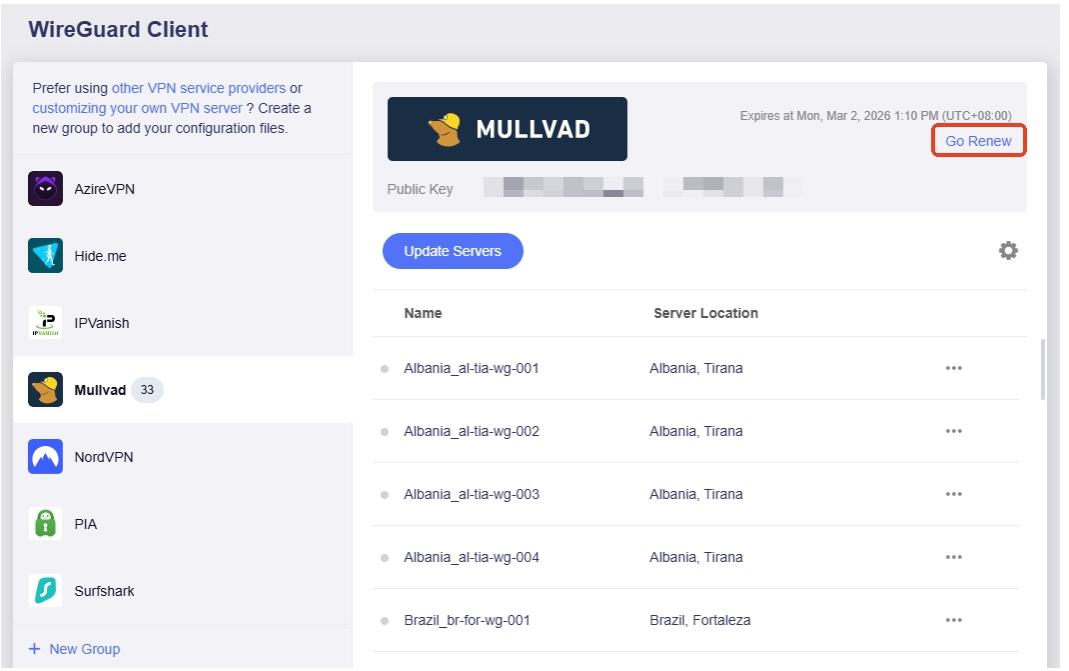
7. Edite las credenciales o cierre sesión.

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



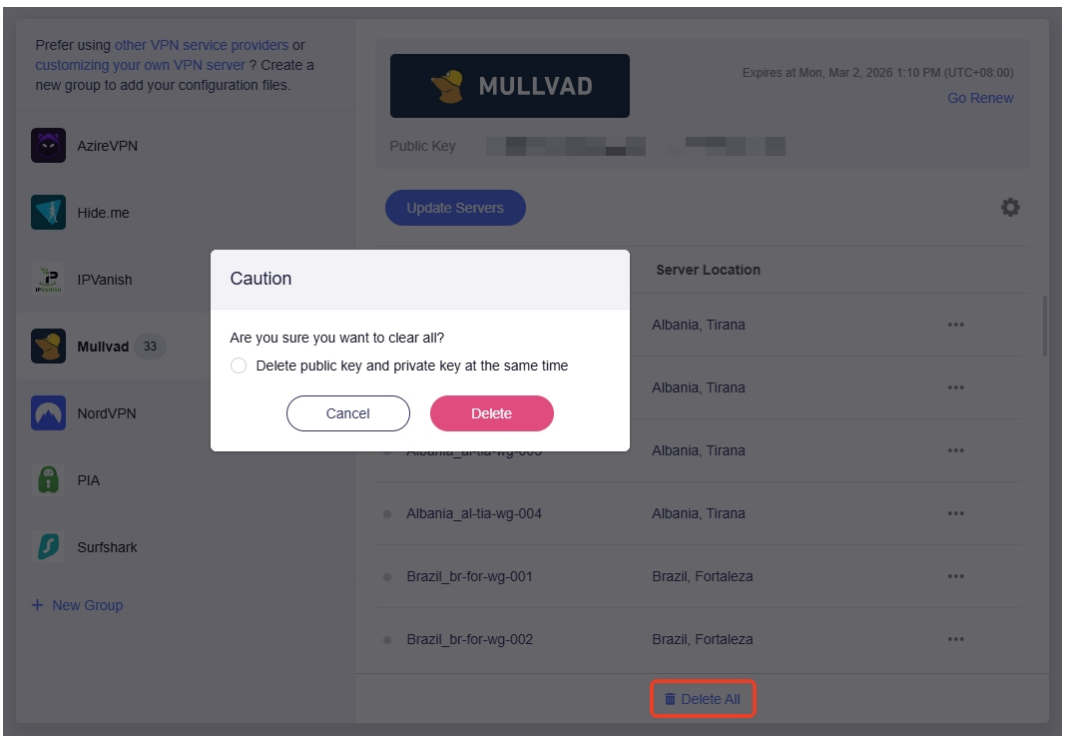
8. Ir a renovar.

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



9. Eliminar todos los archivos.

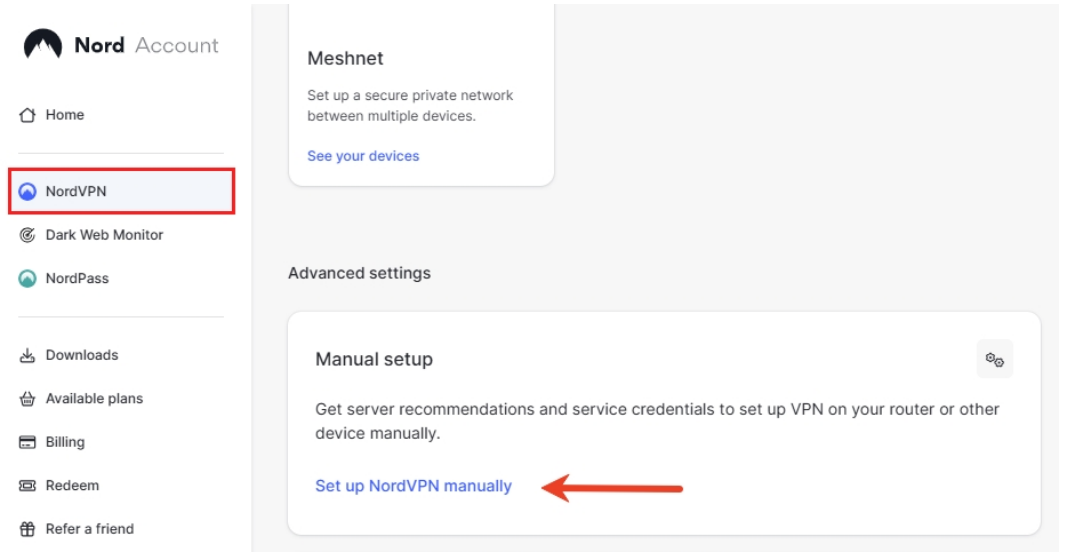
   Puedes hacer clic en **Eliminar todo** para eliminar todos los archivos de configuración con un solo clic y elija si desea eliminar las claves pública y privada simultáneamente.



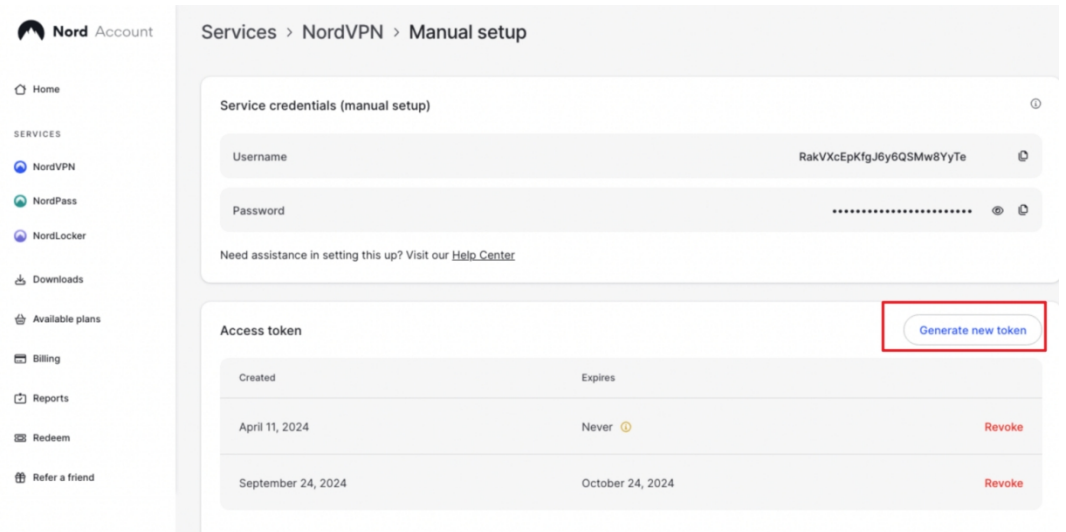
11.2.6 Configurar NordVPN

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

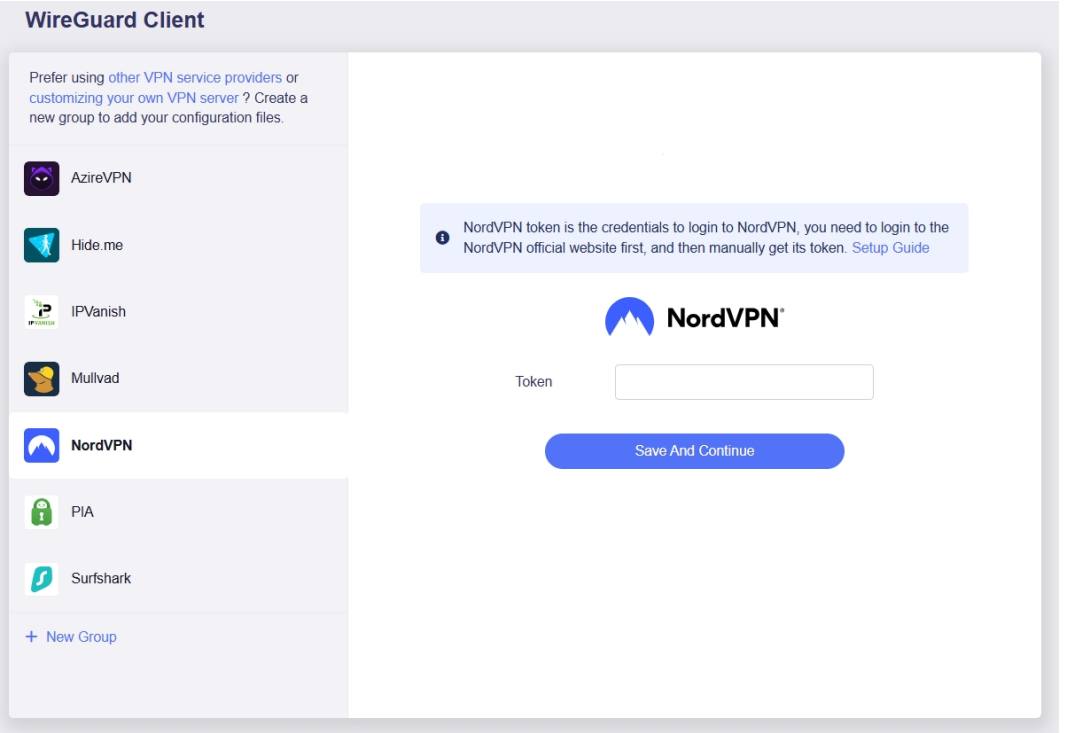
1. Inicie sesión en su cuenta web de NordVPN aquí.
2. Oen el Panel de control de Nord, haga clic en **NordVPN** y luego haga clic en **Configurar NordVPN manualmente**.



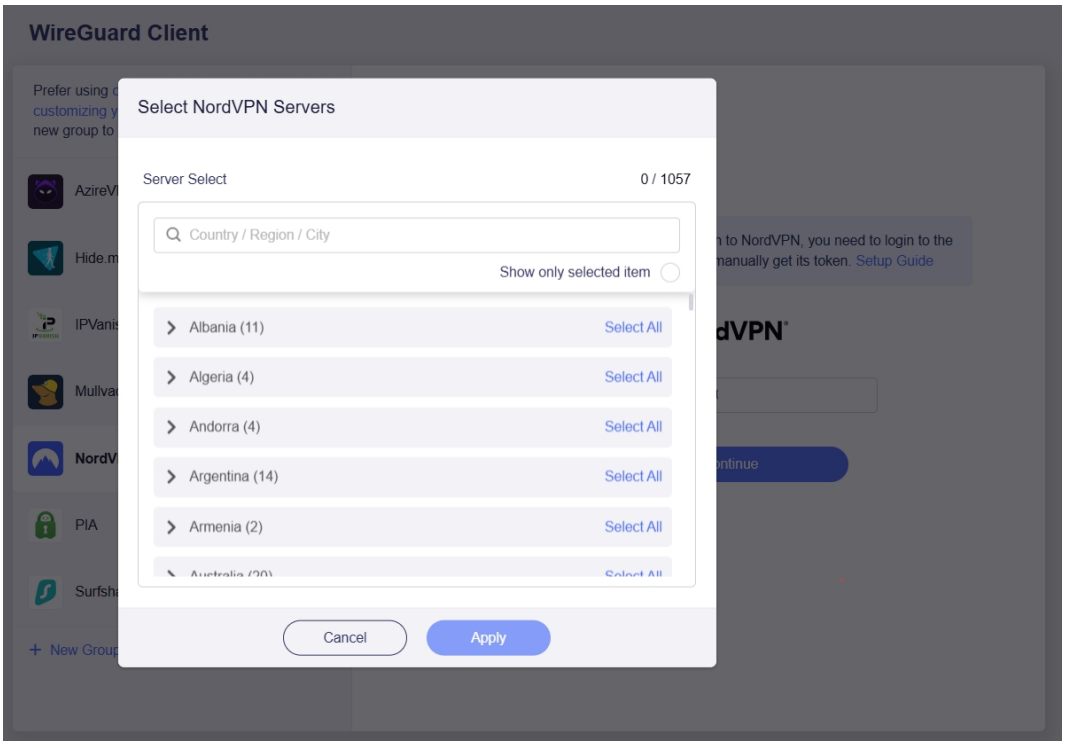
Encontrará el **Token de acceso**. Crear un token de acceso y ccopia para uso posterior.



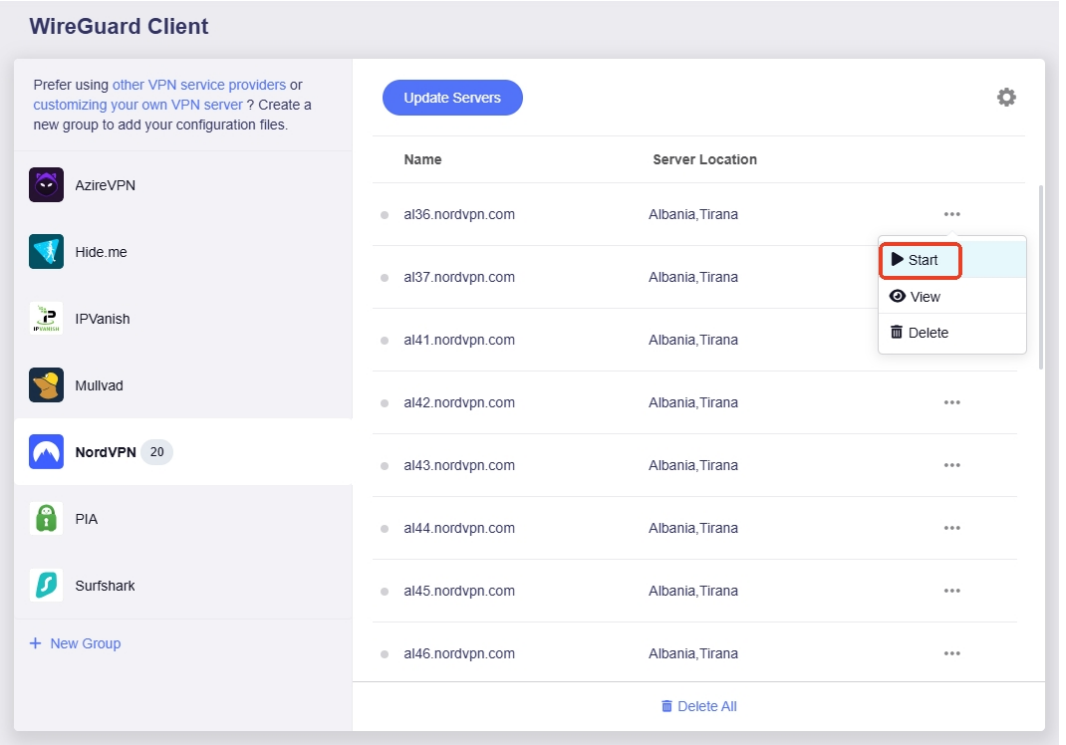
3. Inicie sesiónn en su enrutador's web admin panel y vaya a **VPN** > **Cliente WireGuard** > **NordVPN**.
4. Ingrese token, y haga clic en **Guardar y continuar**.



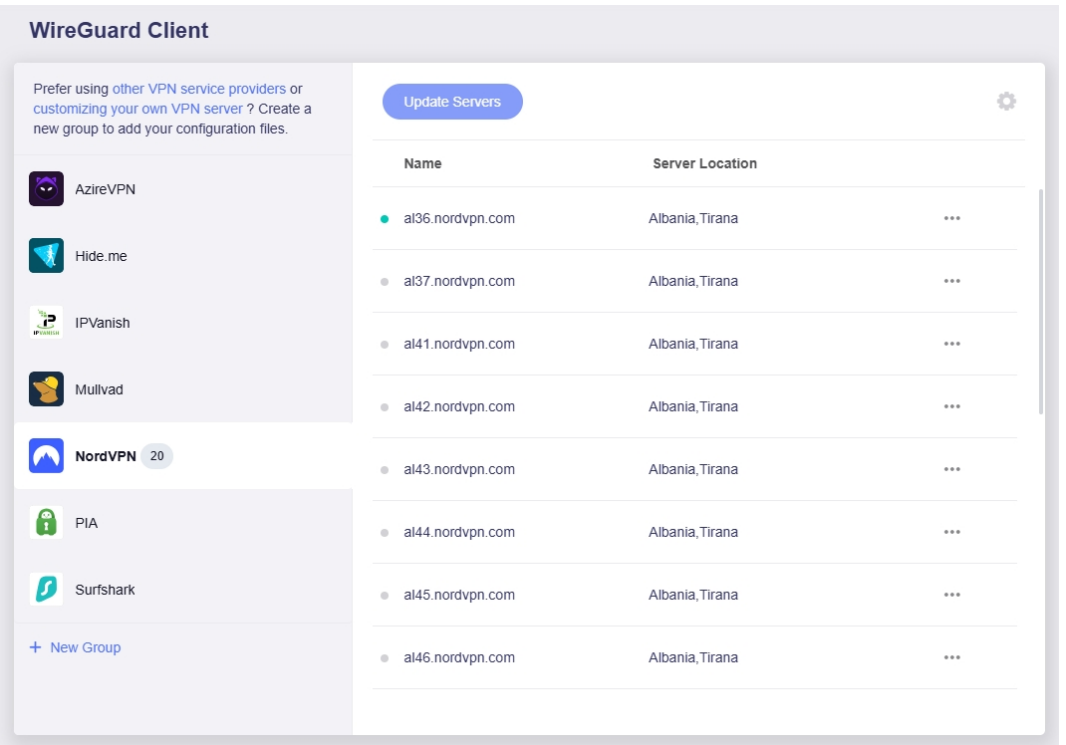
5. Seleccione los servidores a los que desea conectarse y haga clic en **Aplicar**.



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



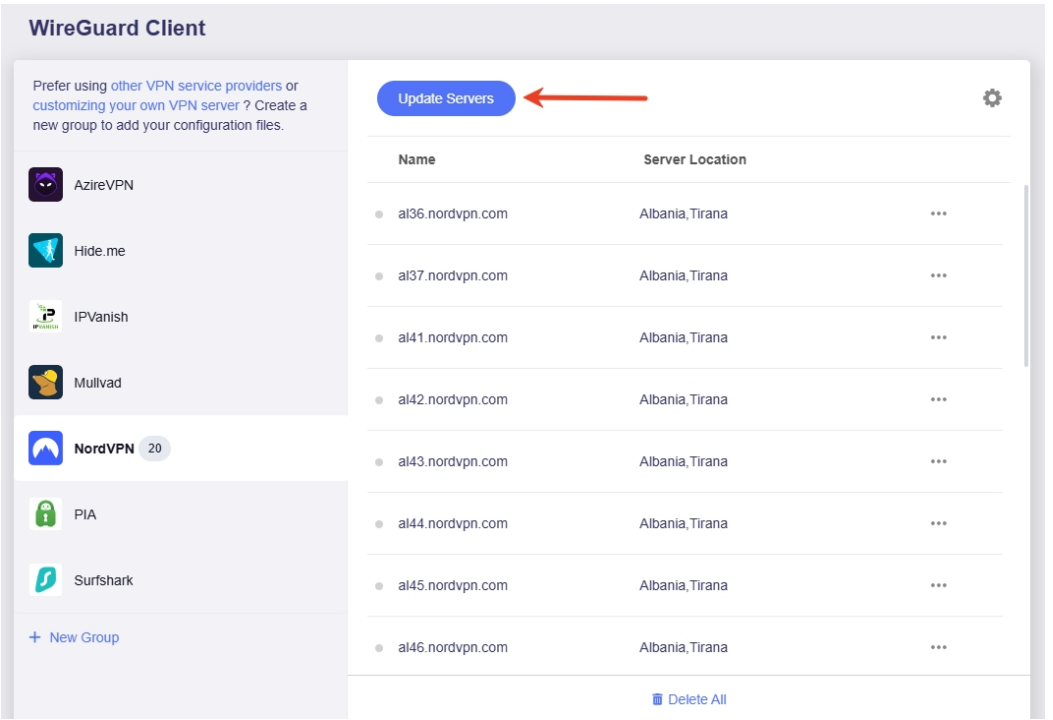
7. Una vez conectado, aparecerá un punto verde junto a la configuración. archivo.



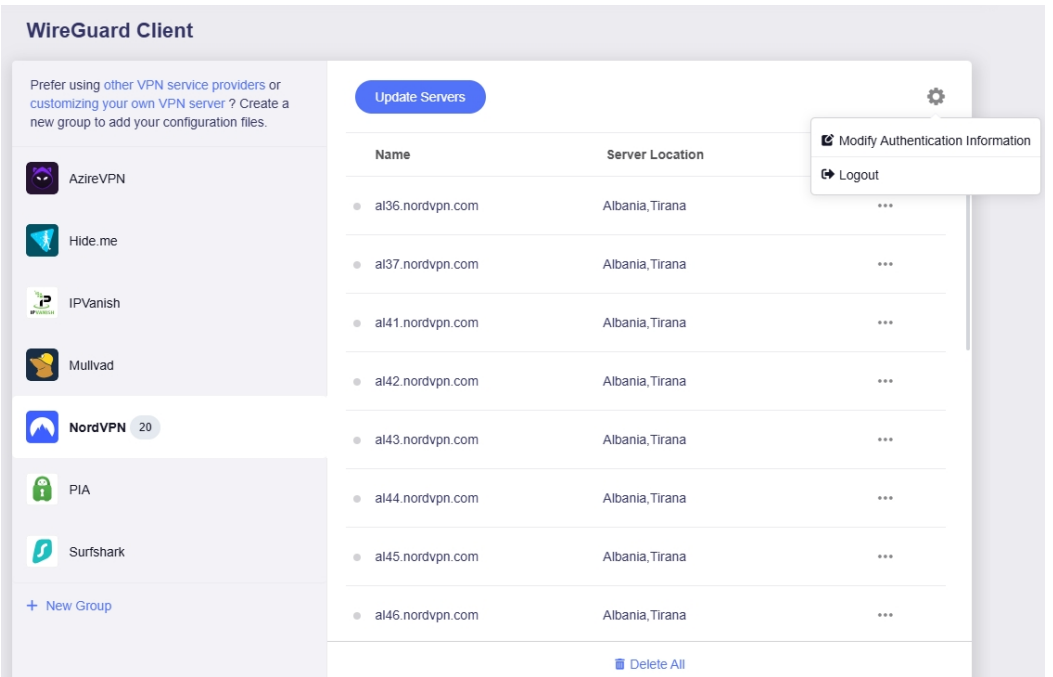
Usted puede también verificar los detalles de la conexión VPN en el **Panel de VPN**.

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.

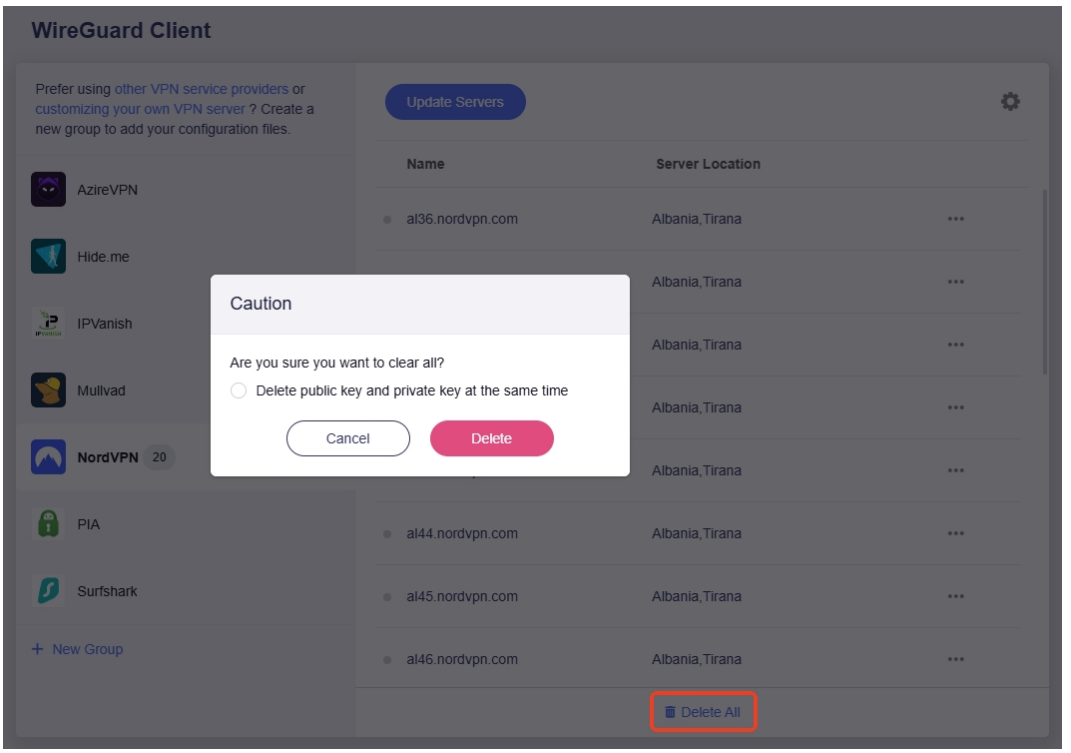


9. Edite las credenciales o cierre la sesión.
   Haga clic en el ícono de ajustes para editar sus credenciales de inicio de sesión o cierre la sesión.



10. Elimine todos los archivos.

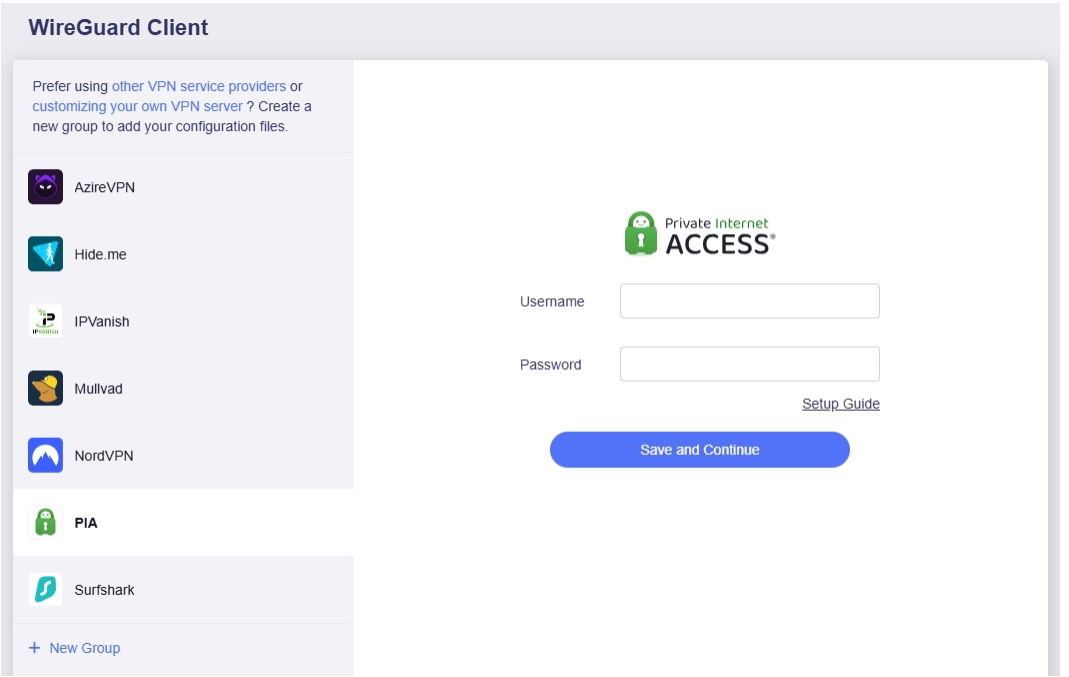
    Puedes hacer clic en **Eliminar todo** para eliminar todos los archivos de configuración con un solo clic y elija si desea eliminar las claves pública y privada simultáneamente.



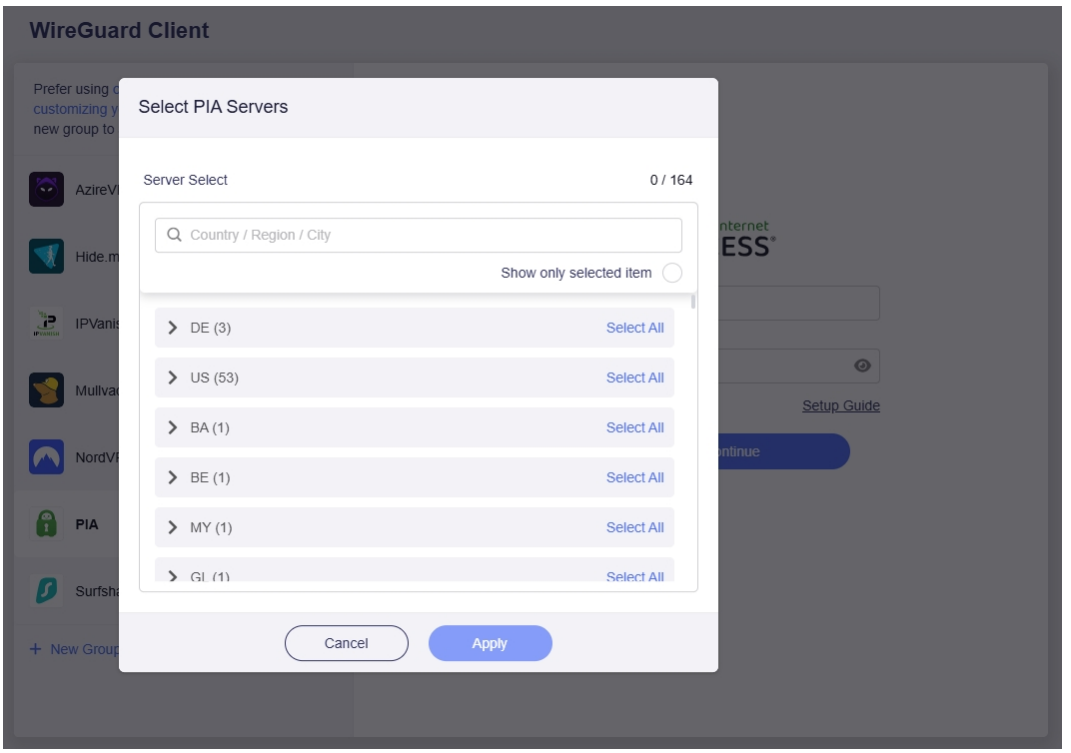
11.2.7 Configurar PIA (Private Internet Access)

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

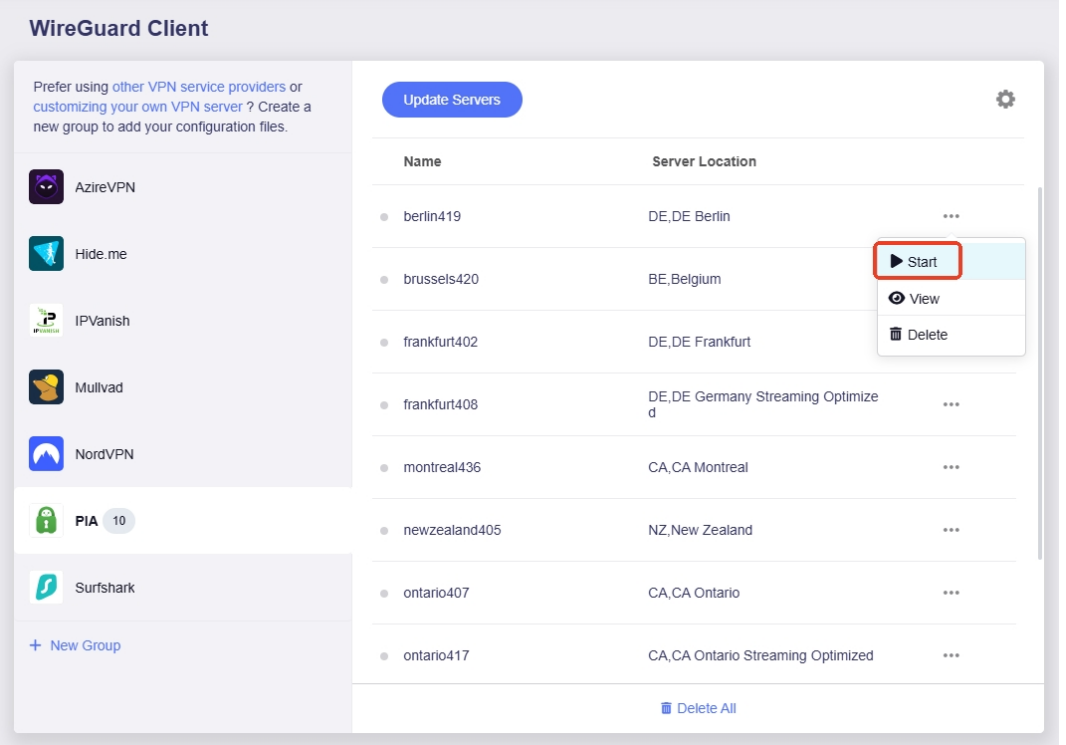
1. Registro in a su enrutador’s web admin panel y vaya a **VPN** > **WireGuard Client** > **PIA**.
2. Ingrese nombre de usuario y contraseña, luego haga clic en **Guardar y continuar**.



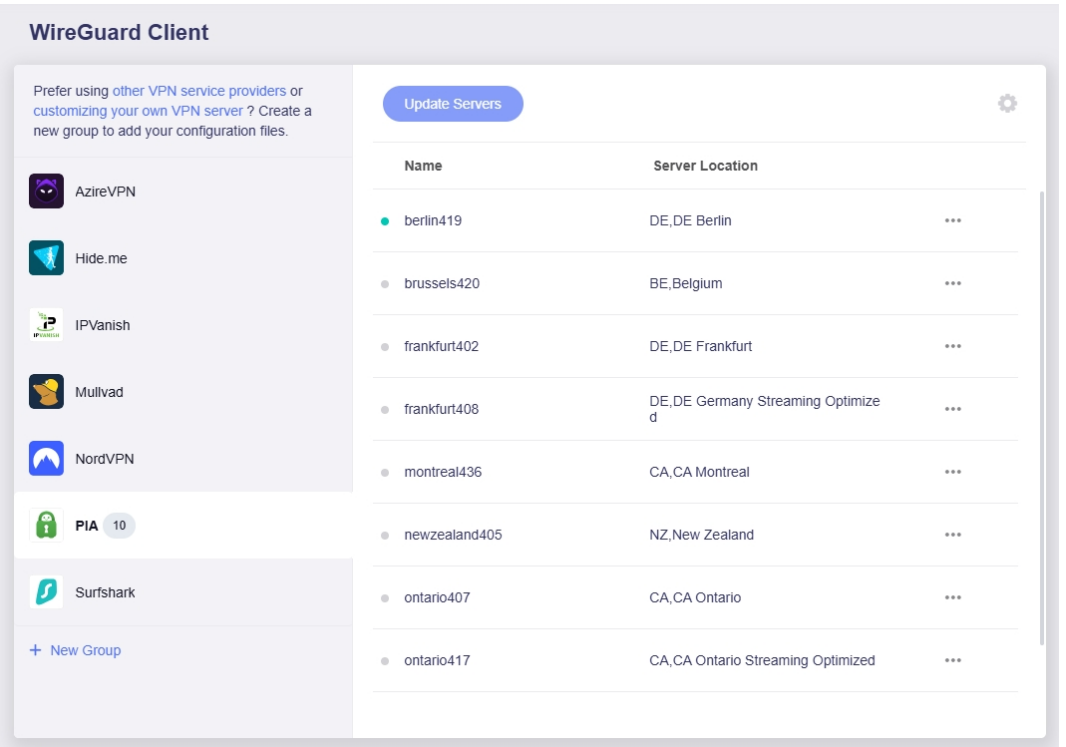
3. Seleccione los servidores a los que desea conectarse y haga clic en **Aplicar**.



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



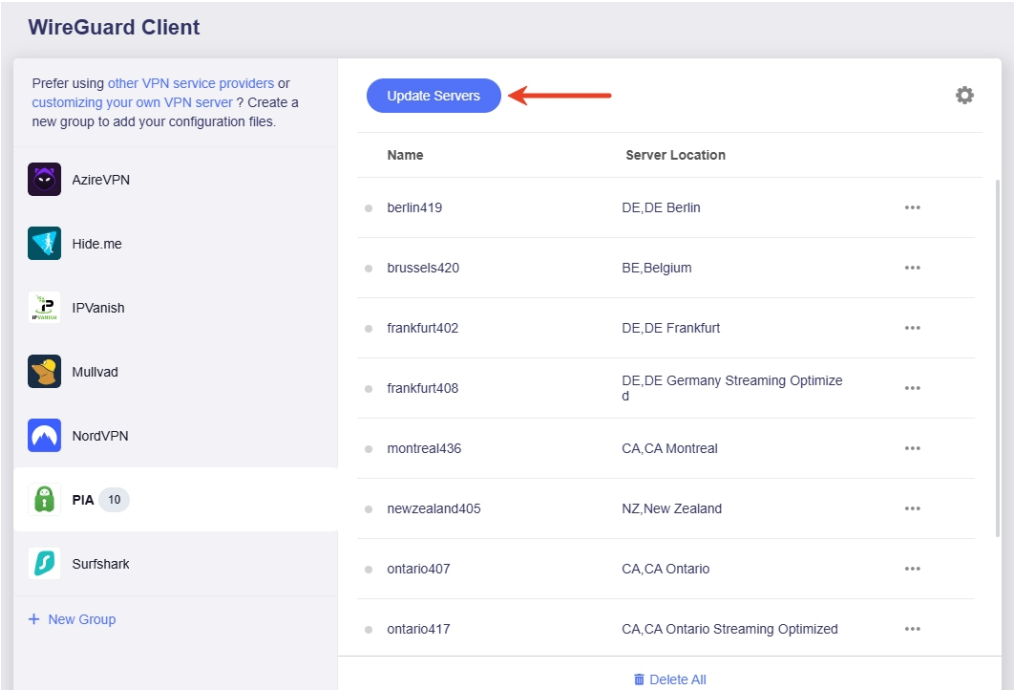
5. Una vez conectado, aparecerá un punto verde junto al archivo de configuración.



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

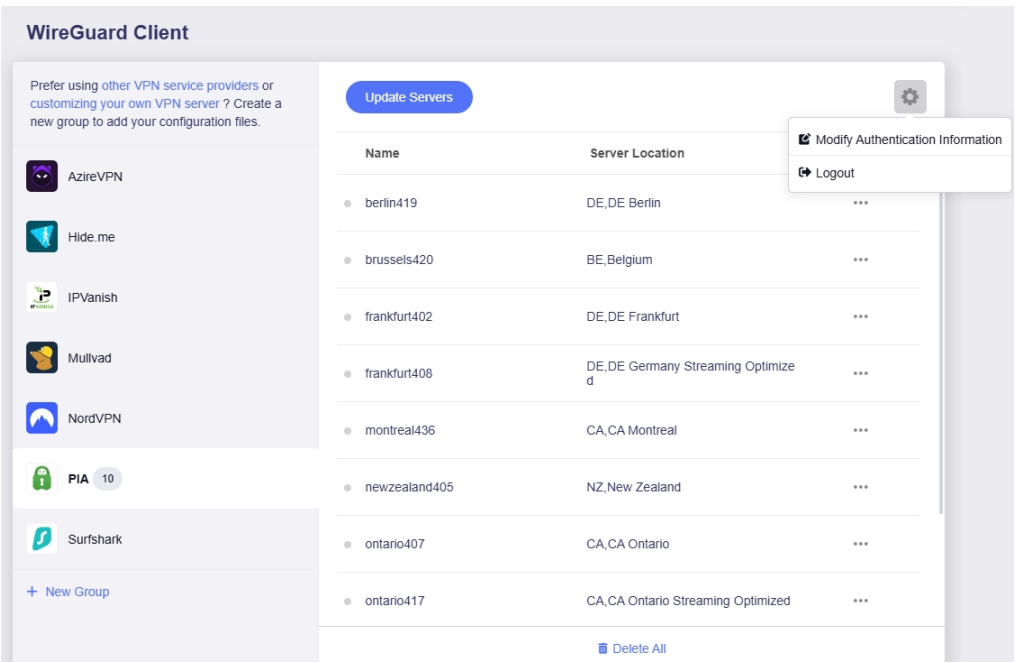
6. Actualizar servidores.

   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.



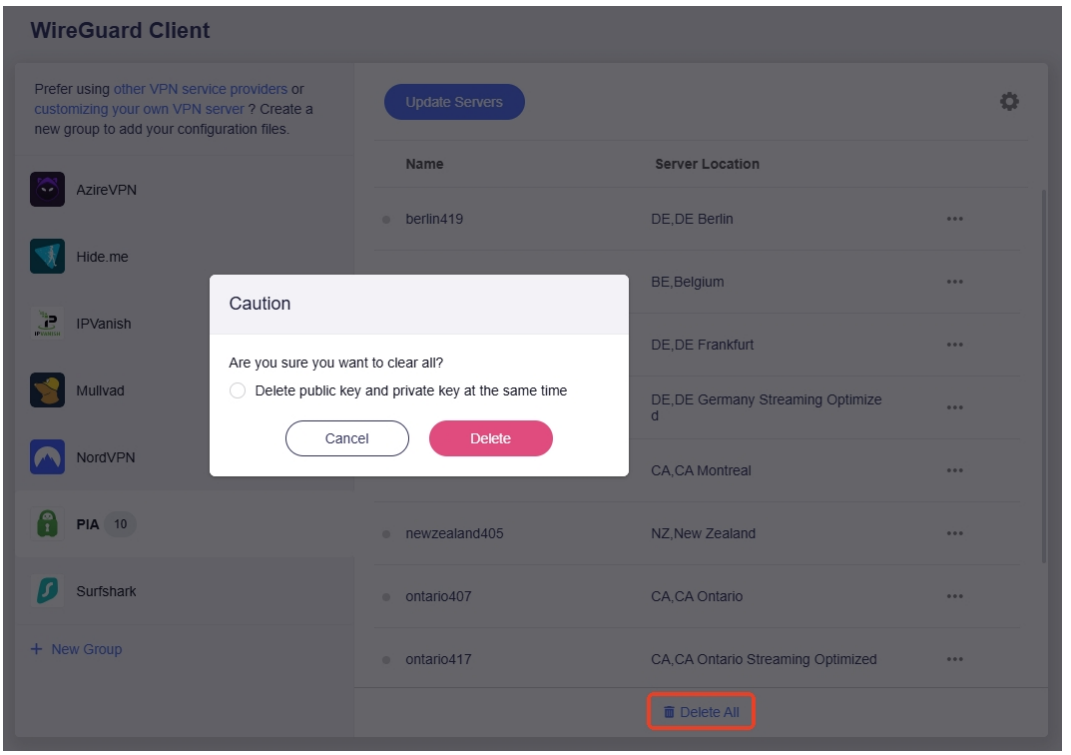
7. Edite las credenciales o cierre sesión.

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



8. Eliminar todos los archivos.

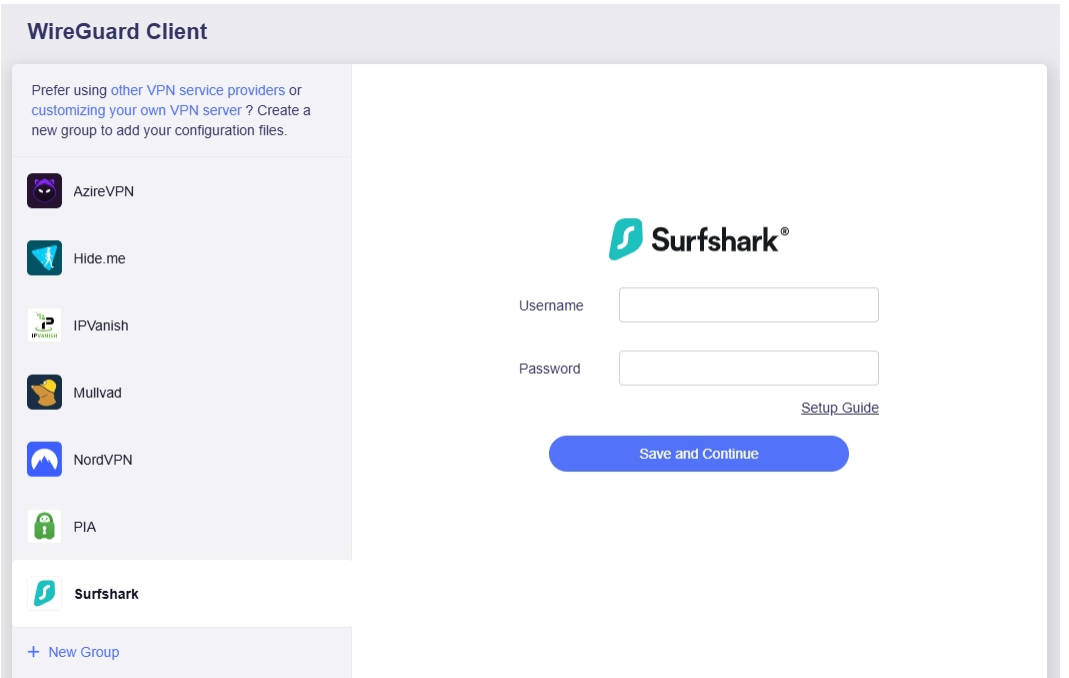
   Puede hacer clic en **Eliminar todo** para eliminar todos los archivos de configuración con un solo clic y elegir si desea eliminar los claves privadas y públicas simultáneamente.



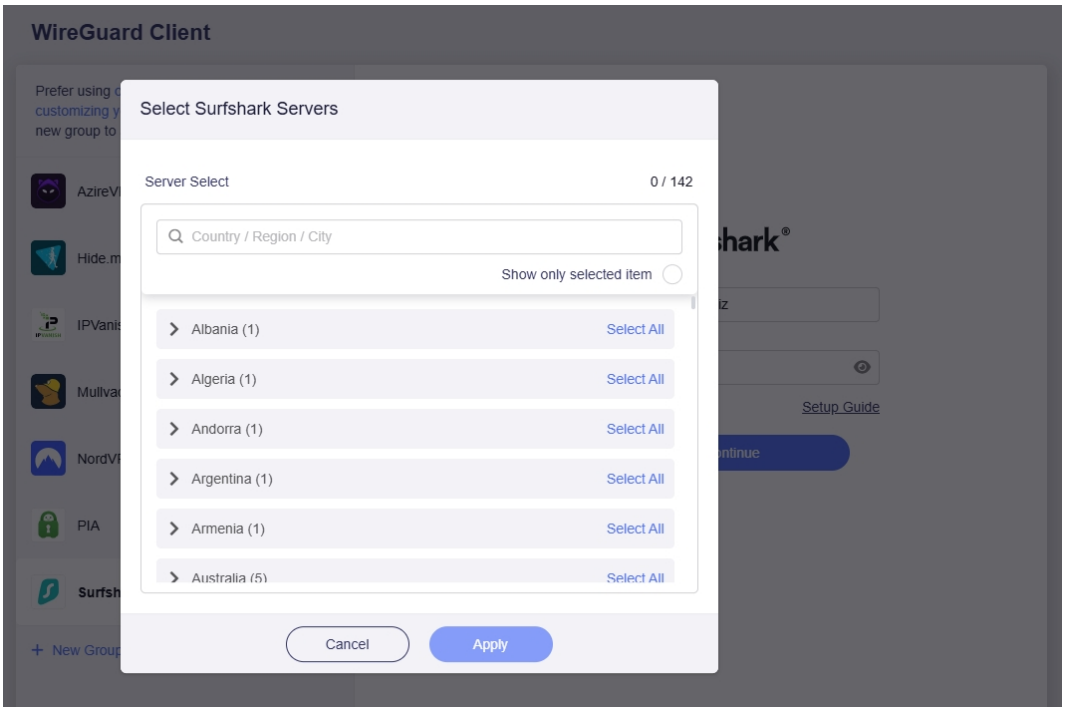
11.2.8 Configurar Surfshark

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

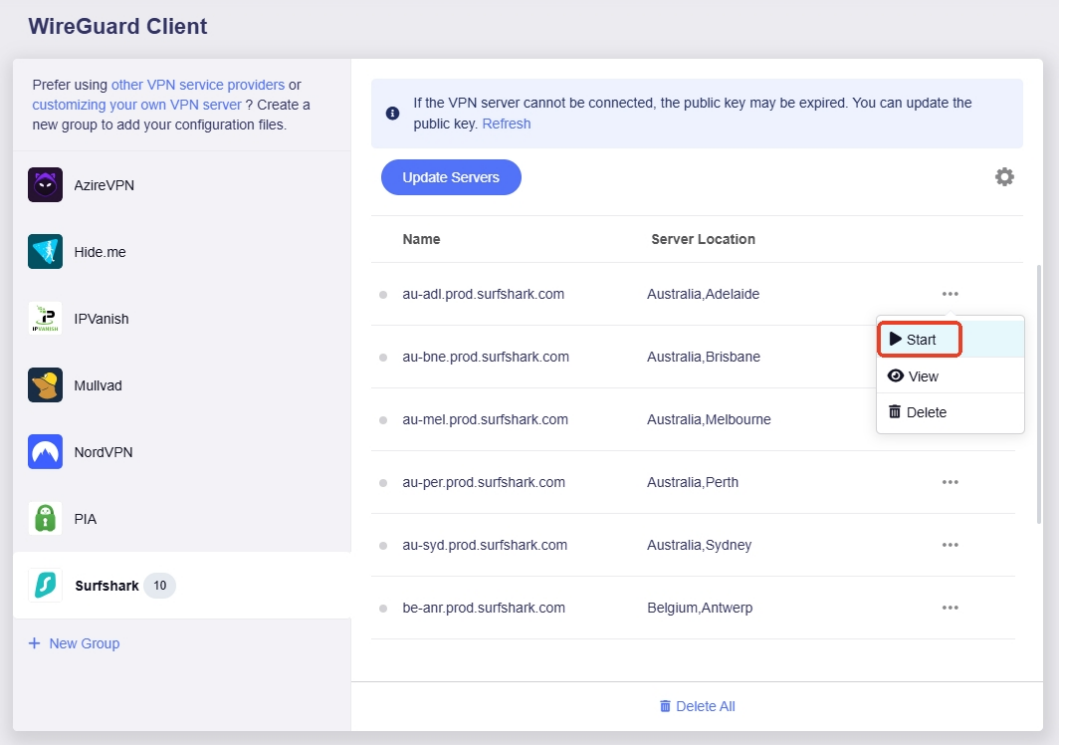
1. Iniciar sesiónn a su enrutador’s web admin panel y vaya a **VPN** > **WireGuard Client** > **Surfshark**.
2. Ingrese nombre de usuario y contraseña, luego haga clic en **Guardar y continuar**.



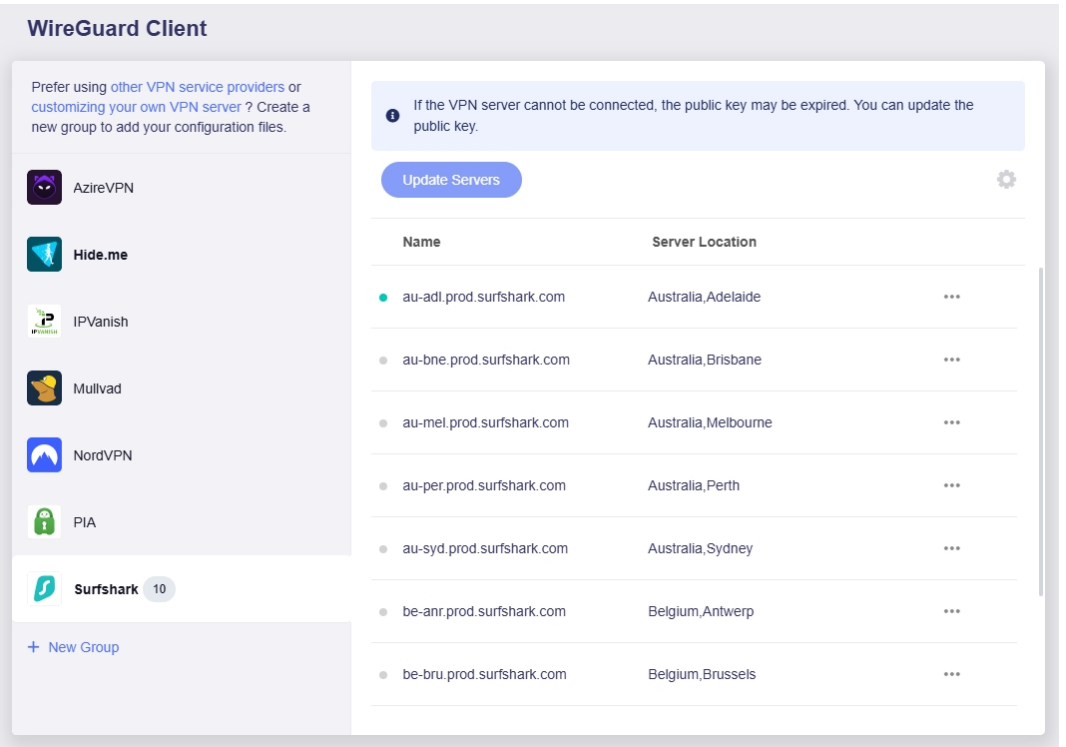
3. Seleccione los servidores a los que desea conectarse y haga clic en **Aplicar**.



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



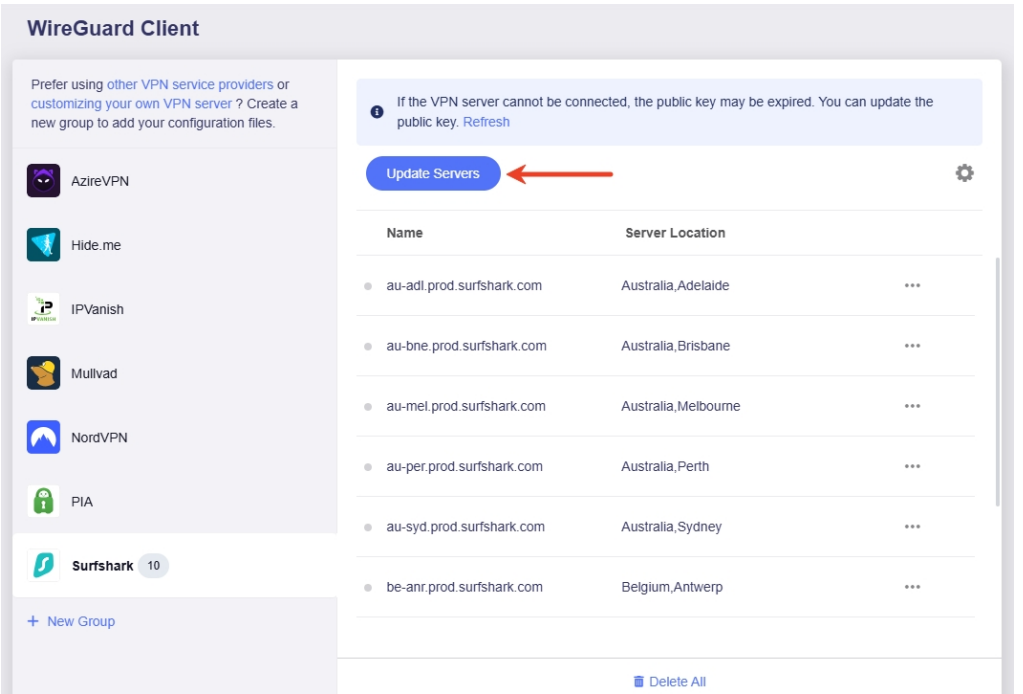
5. Una vez conectado, aparecerá un punto verde junto al archivo de configuración.



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

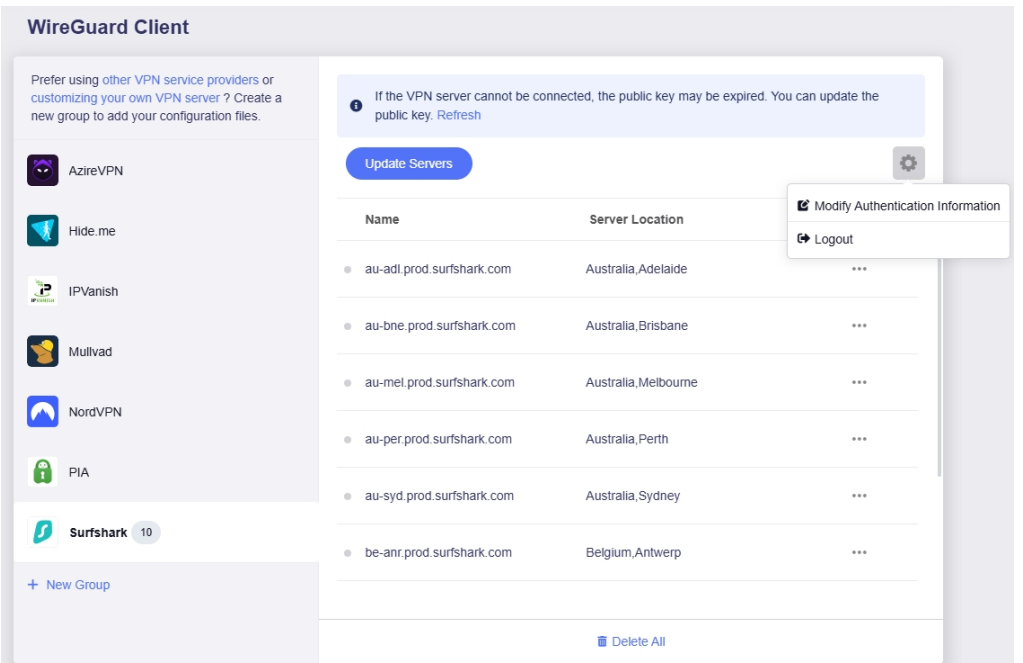
6. Actualizar servidores.

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



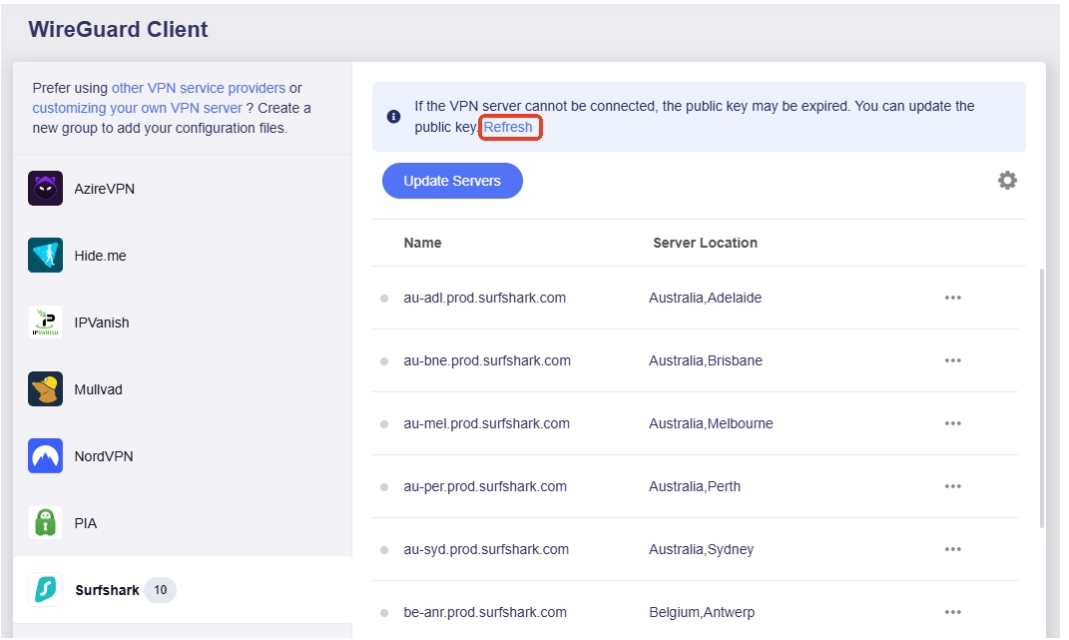
7. Editar credenciales o cerrar sesión.

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



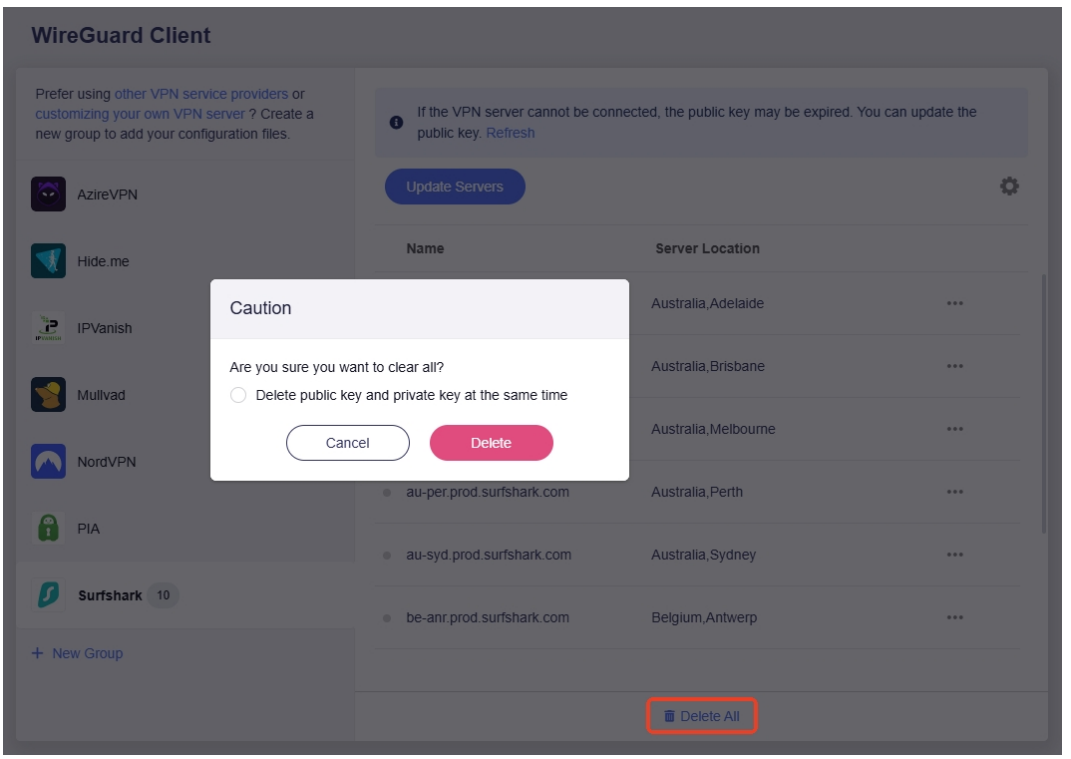
8. Actualizar.

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

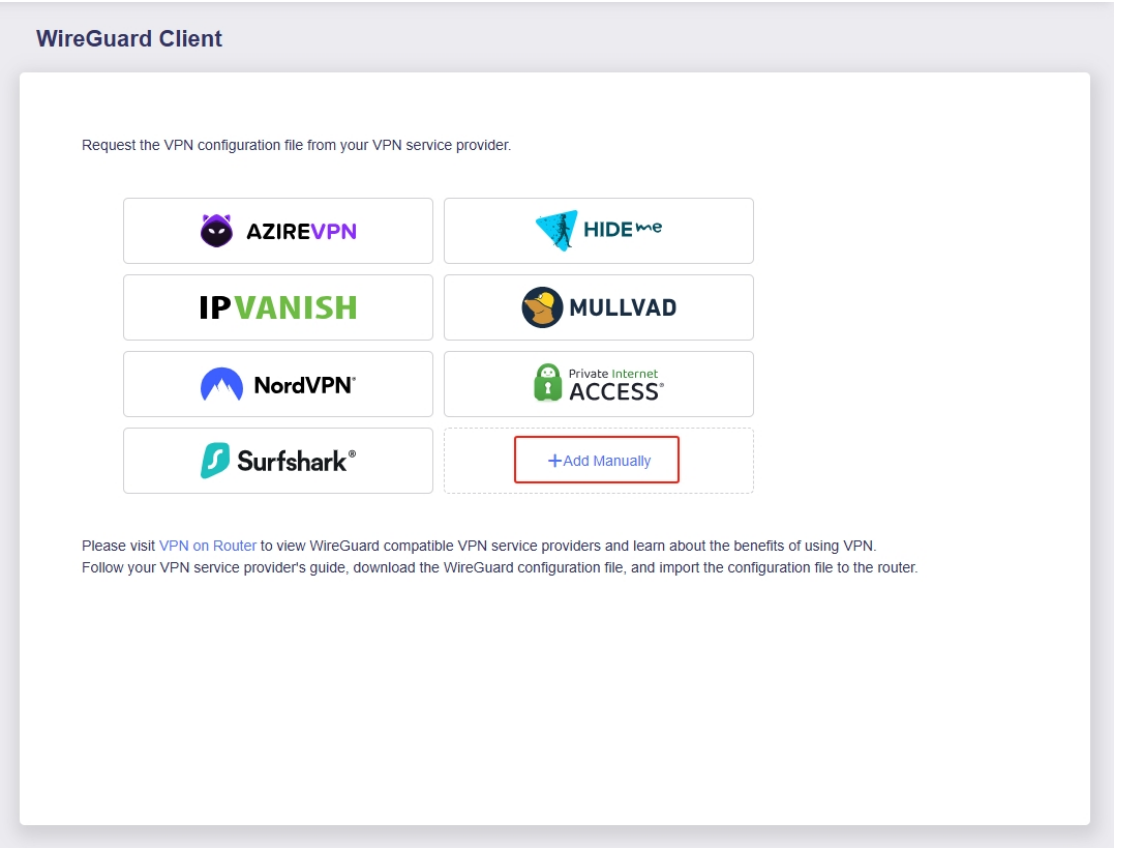


11.2.9 Configurar el cliente WireGuard manualmente (para otros proveedores)

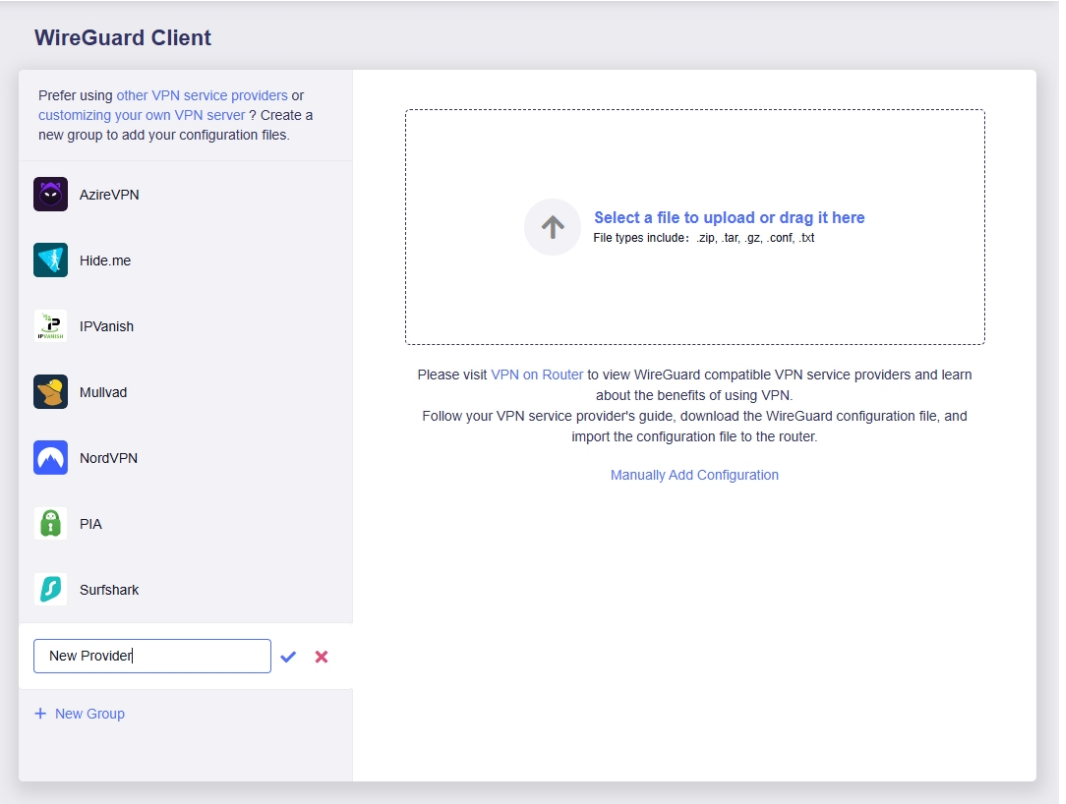
Si su proveedor de servicios WireGuard no está integrado en el panel de administración web, visite primero el sitio web oficial de su proveedor de servicios suscrito para obtener el archivo de configuración. Luego cárguelo en el enrutador para configurar un cliente WireGuard. Si no sabes cómo descargar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

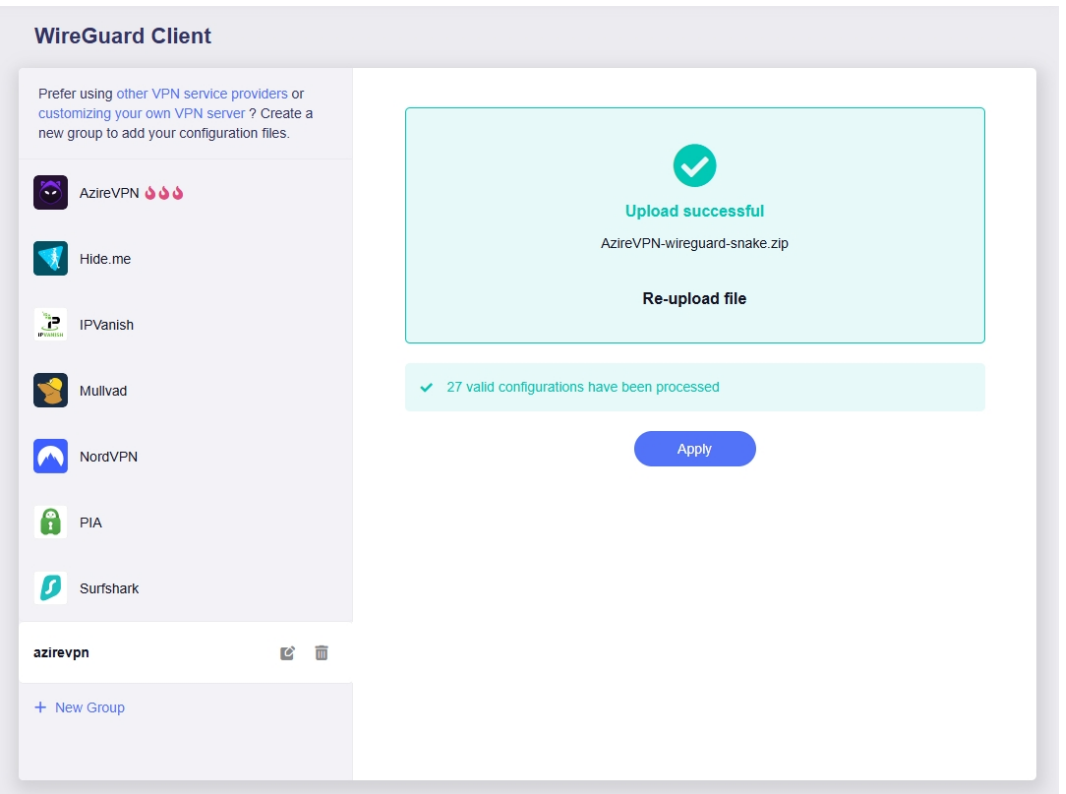
1. Inicie sesiónn en su enrutador's web admin panel y navegue hasta **VPN** > **Cliente WireGuard** > **Agregar manualmente**.



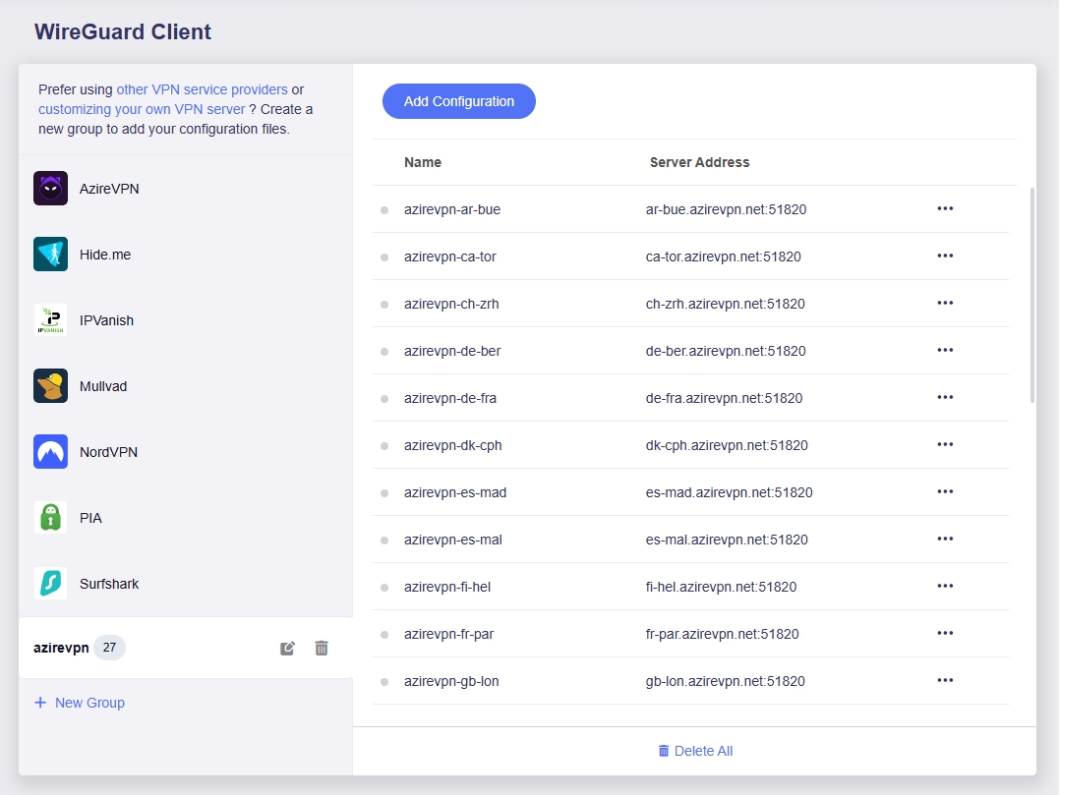
2. Se creará un grupo en la barra lateral izquierda. Establezca un nombre descriptivo para el grupo.



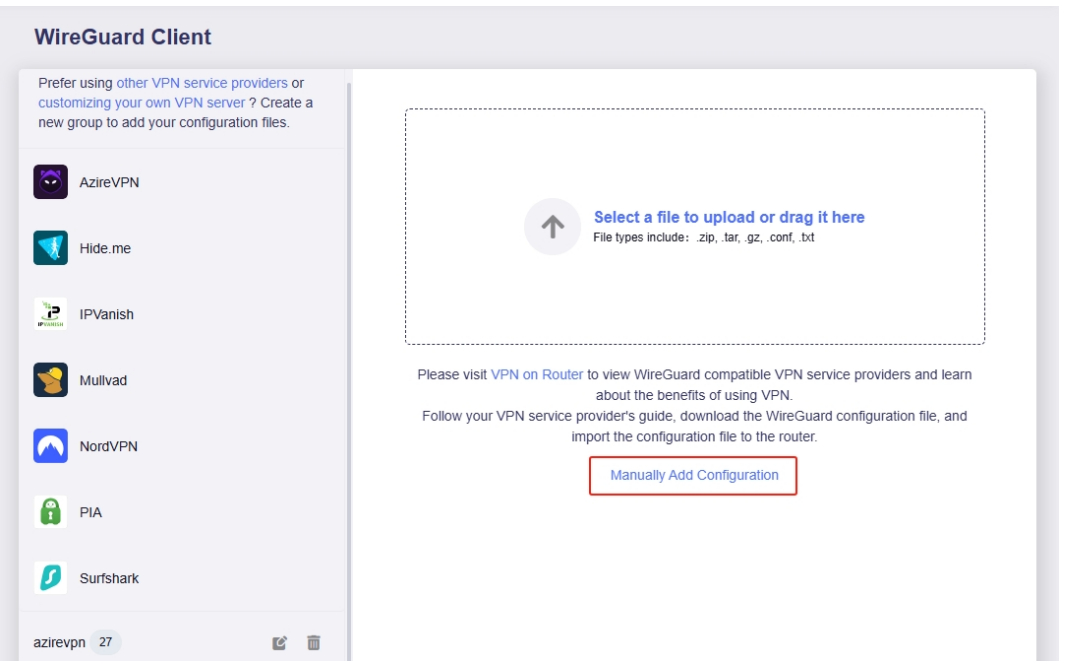
3. Click el área de carga para cargar su archivo de configuración WireGuard (formatos admitidos: zip, tar, gz, conf, txt), y haga clic en **Aplicar**.

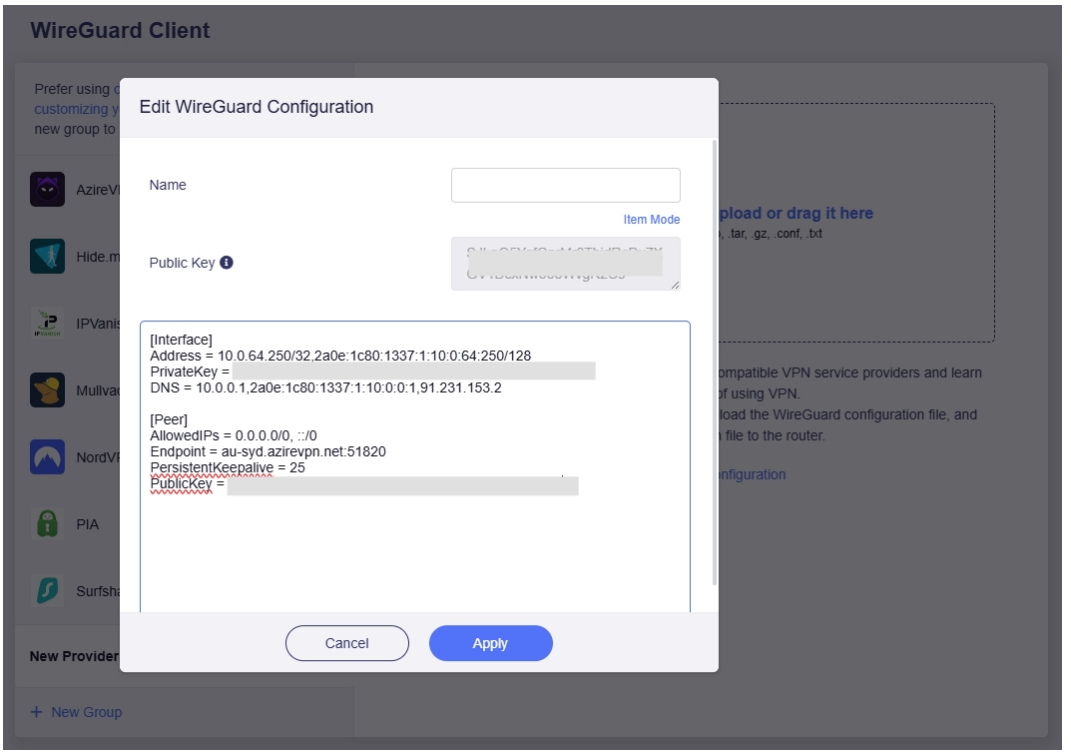


Si subes un archivo comprimido que contiene varios archivos de configuración, se descomprimirá automáticamente, como se muestra a continuación.

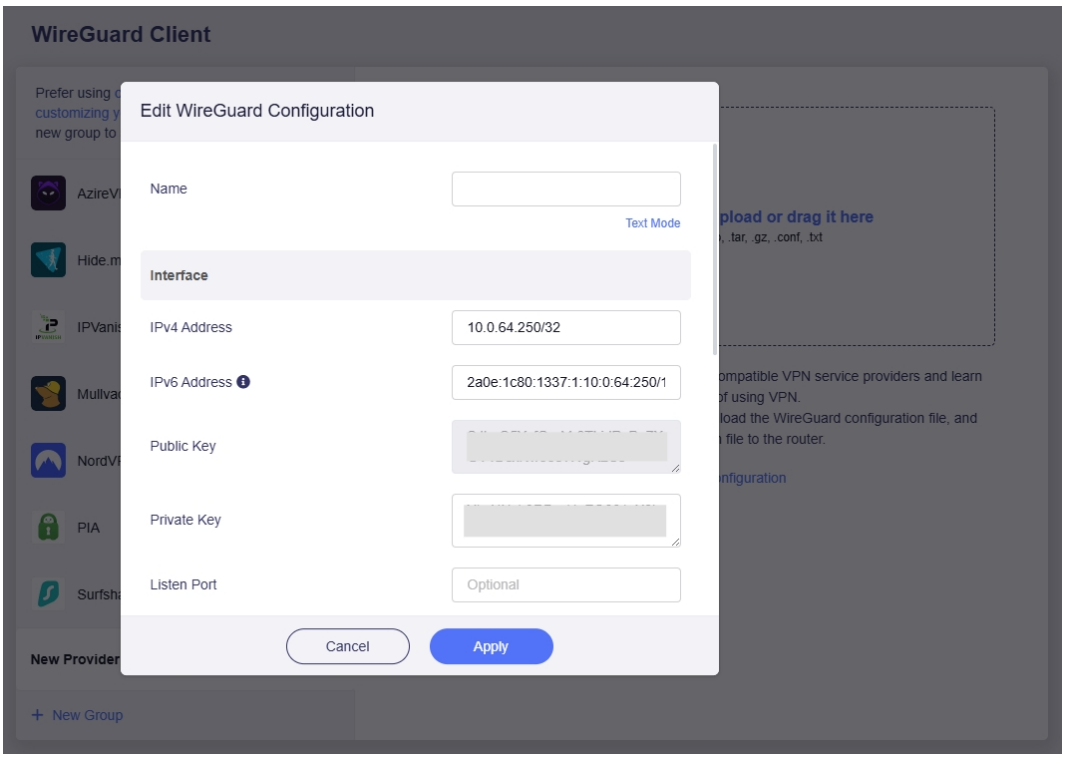


Como alternativa, puedes hacer clic en **Agregar configuración manualmente** en en la parte inferior del área de carga, agregue los detalles de configuración en forma de texto y haga clic en **Aplicar**.

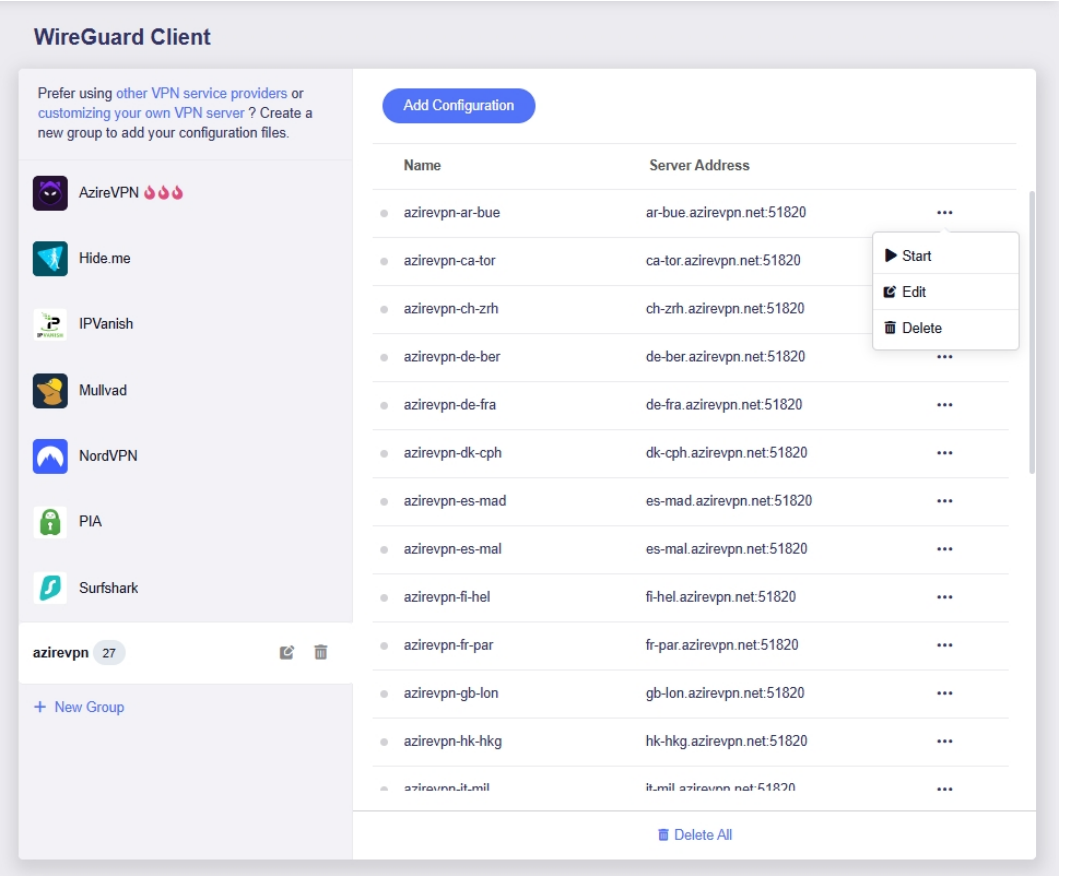




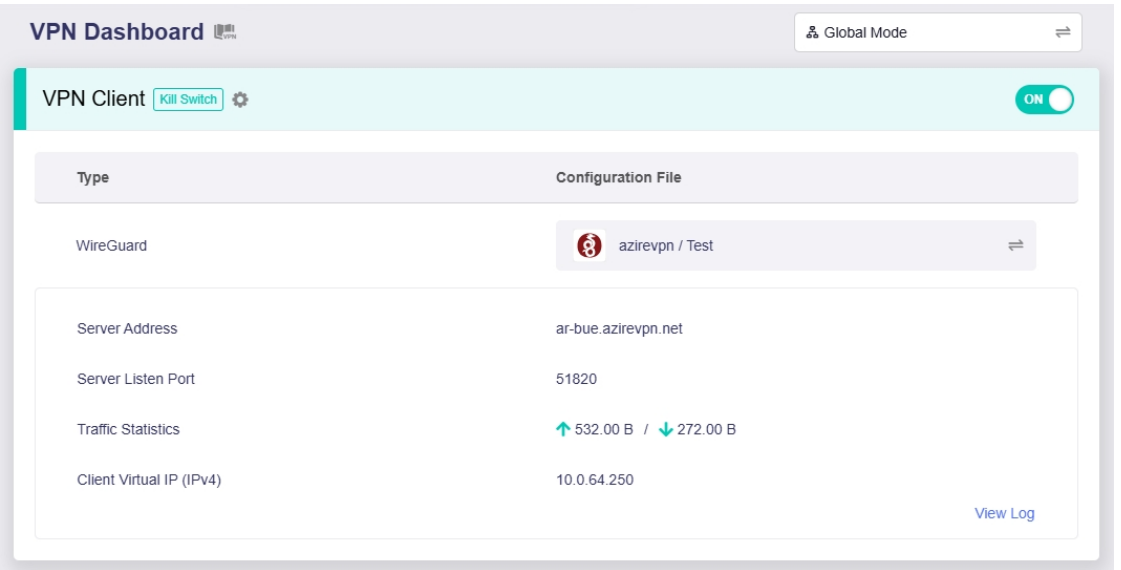
Si desea verificar cada elemento, puede cambiar al modo Elemento y verificar la configuraciónuración detalles, luegoluego haga clic en **Aplicar**.



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



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



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

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

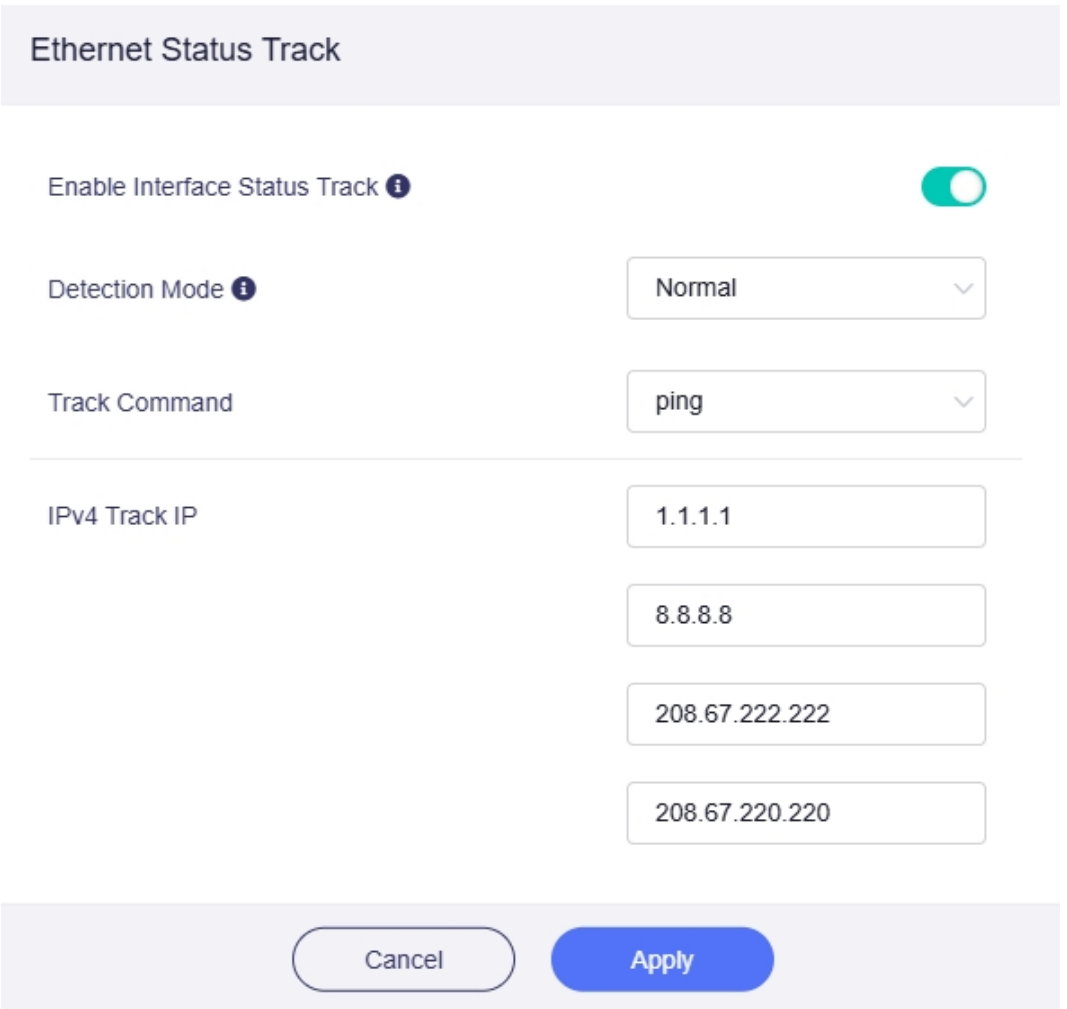
12.1.1 Seguimiento del estado de la interfaz

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



En la sección **Seguimiento del estado de la interfaz**, haga clic en el ícono de ajustes a la derecha para acceder a la configuración de seguimiento del estado para cada interfaz de red.

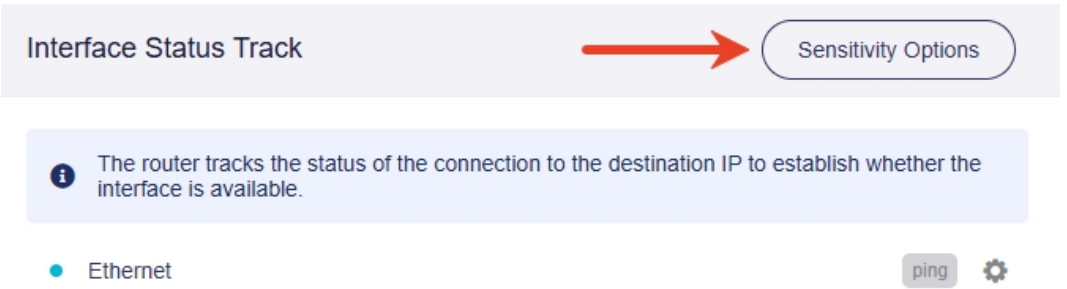
A continuación se muestran las configuraciones de seguimiento de estado para la interfaz Ethernet. La misma lógica de configuración se aplica a otras interfaces.



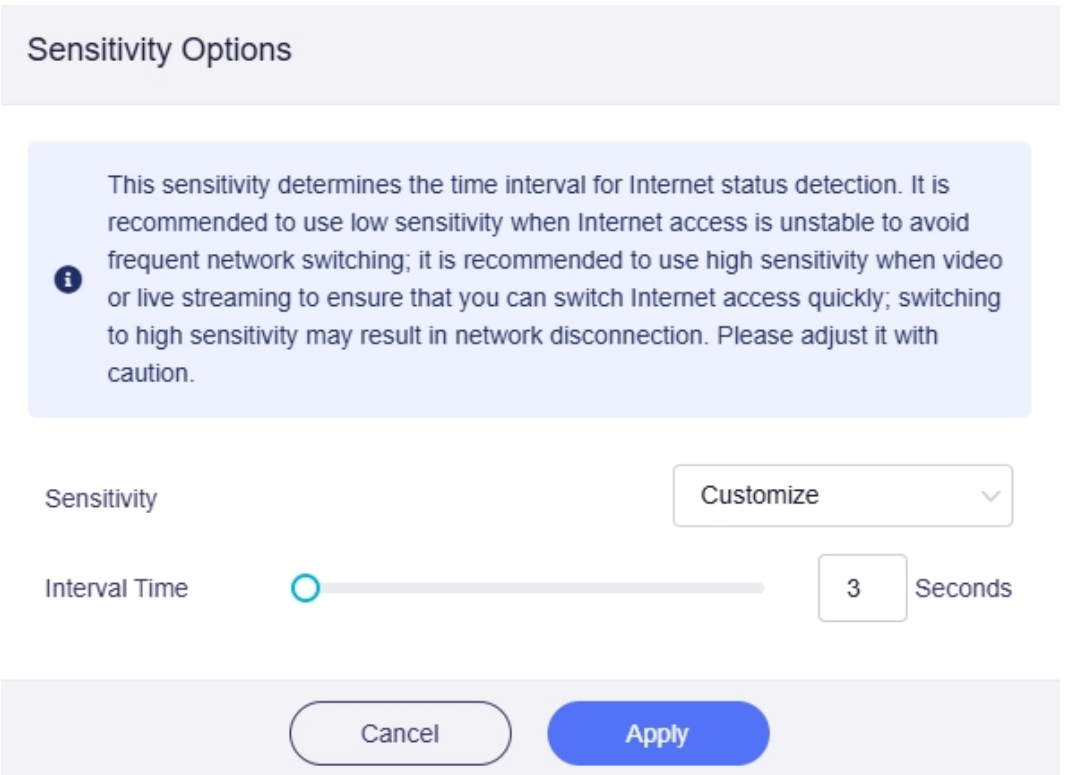
- **Habilitar seguimiento del estado de la interfaz**: Está habilitadode forma predeterminada. Si está deshabilitado, el enrutador determinará el estado de la interfaz según las condiciones (por ejemplo, si el cable Ethernet está enchufado).
- **Modo de detección**: esta función se introdujo como modo 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**: Se utilizade forma predeterminada.
  - **Datos bajos**: Solo activa el seguimiento cuando se produce un error de red en la red interfaz. Utilice este modo si tiene un plan de datos limitado. Tenga en cuenta que la reconexión después de una desconexión puede ser un poco más lenta que en el modo normal, y está habilitado de forma predeterminada solo para la interfaz celular.

    - **Estricto**: determina el estado de la interfaz basándose exclusivamente en los resultados de un comando de detección enviado a una IP pública.
- **Comando Track**: El comando ping se utiliza para monitorear el estado de la conexión a la IP de destino y verificar la disponibilidad de la interfaz.
- **IPv4 Track IP**: Cpersonalizar la IPv4 Seguimiento de direcciones IP si es necesario.

Haga clic en **Opciones de sensibilidad** 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.



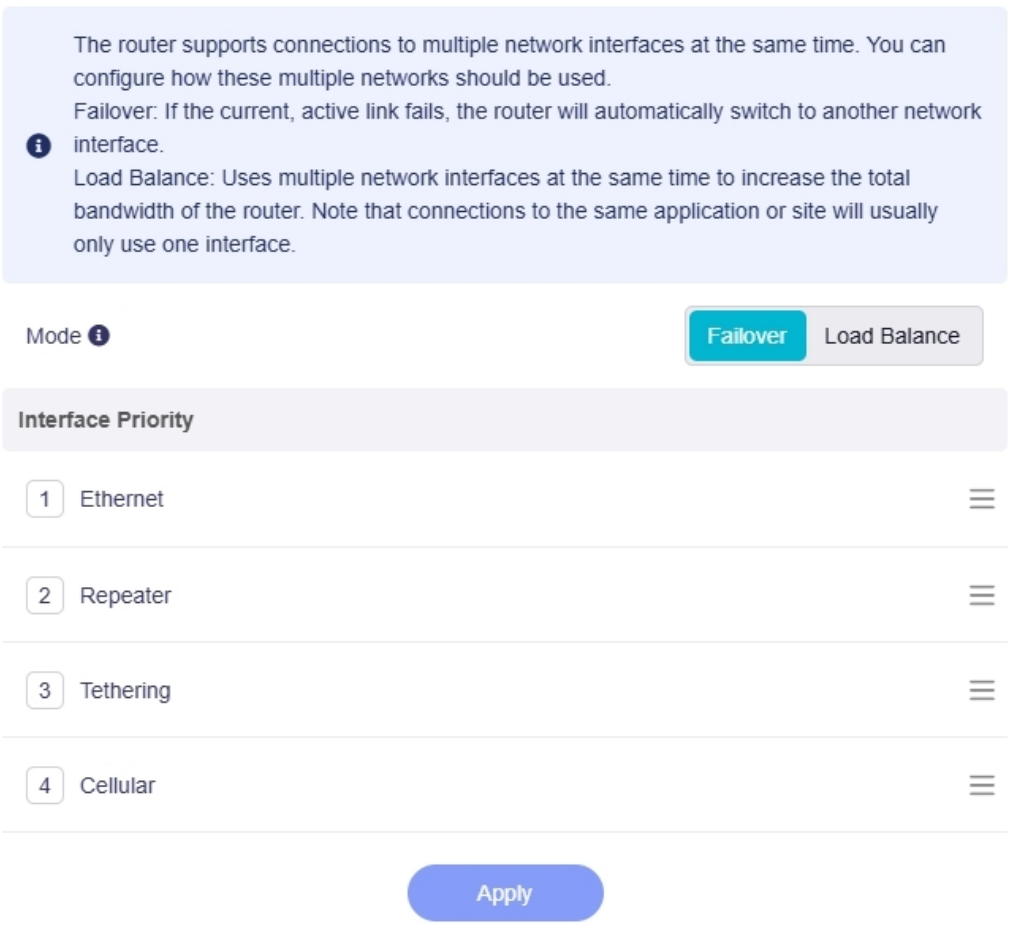
12.1.2 Modo Multi-WAN

THay dos 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.

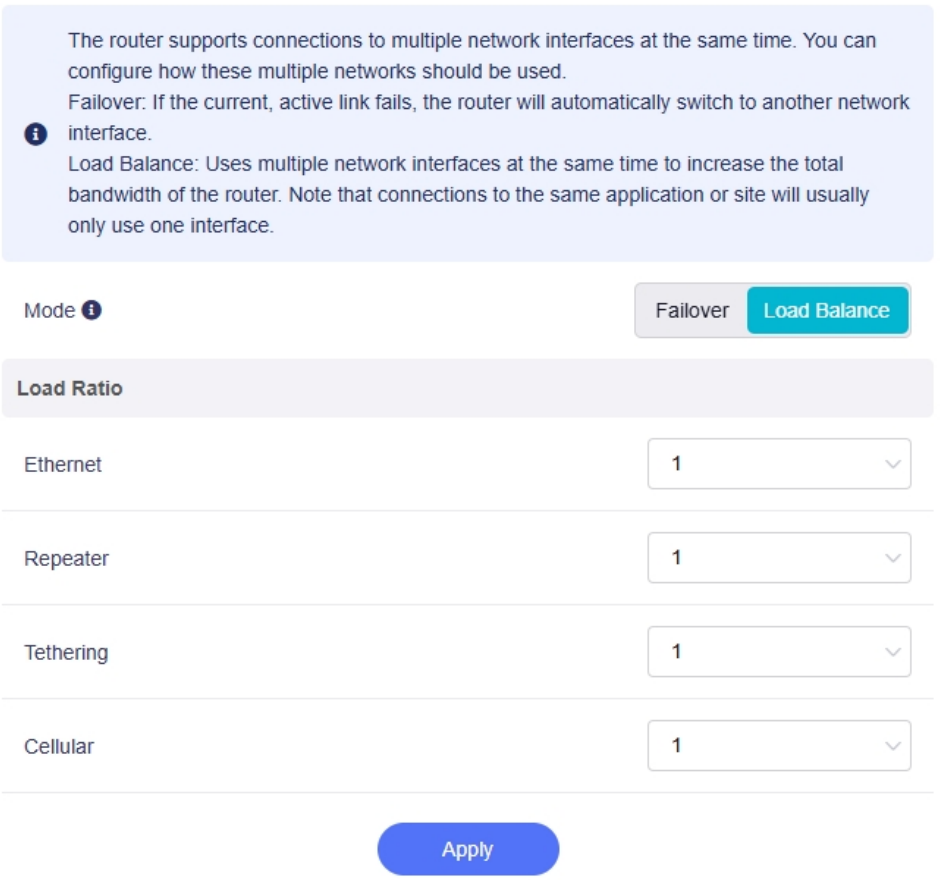


Equilibrio de carga

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 cuatro (por ejemplo, Ethernet, Repetidor, Anclaje a red, y Celular) simultáneamente y las cuatro interfaces están disponibles para acceso a Internet, habilitar el equilibrio de carga y establecer una proporción de 1:1:1:1 significa que las cuatro interfaces compartirán el ancho de banda de la red por igual. El sistema distribuirá nuevas conexiones a través de estas cuatro interfaces de acuerdo con la relación de carga 1:1:1:1 configurada.



También puede personalizar la relación de carga si es necesario. Por ejemplo, si Ethernet tiene un ancho de banda de 100 Mbps, Repetidor tiene 200 Mbps y no hay conexiones de anclaje a red o celulares activas, establezca las relaciones de carga en 1 para Ethernet, 2 para Repetidor y 0 para anclaje a red y celular. Luego, el sistema distribuirá nuevas conexiones a través de estas interfaces de acuerdo con la proporción 1:2 configurada, lo que significa que Ethernet 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.

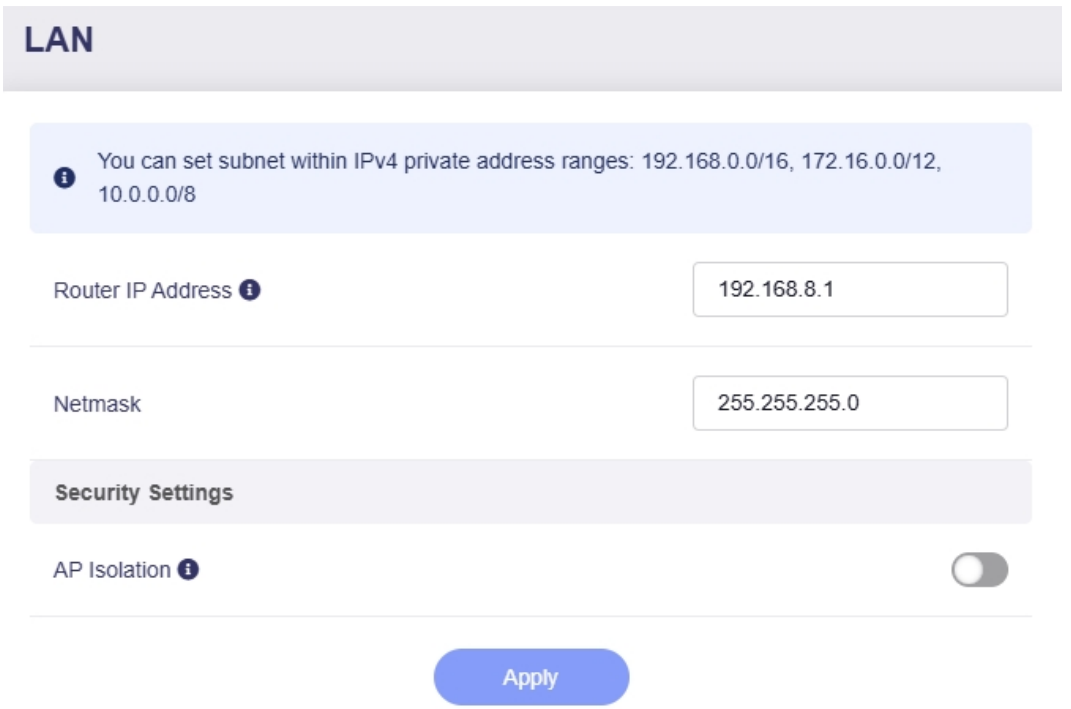
12.2 LAN

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 rangos de direcciones privadas IPv4: 192.168.0.0/16, 172.16.0.0/12, 10.0.0.0/8

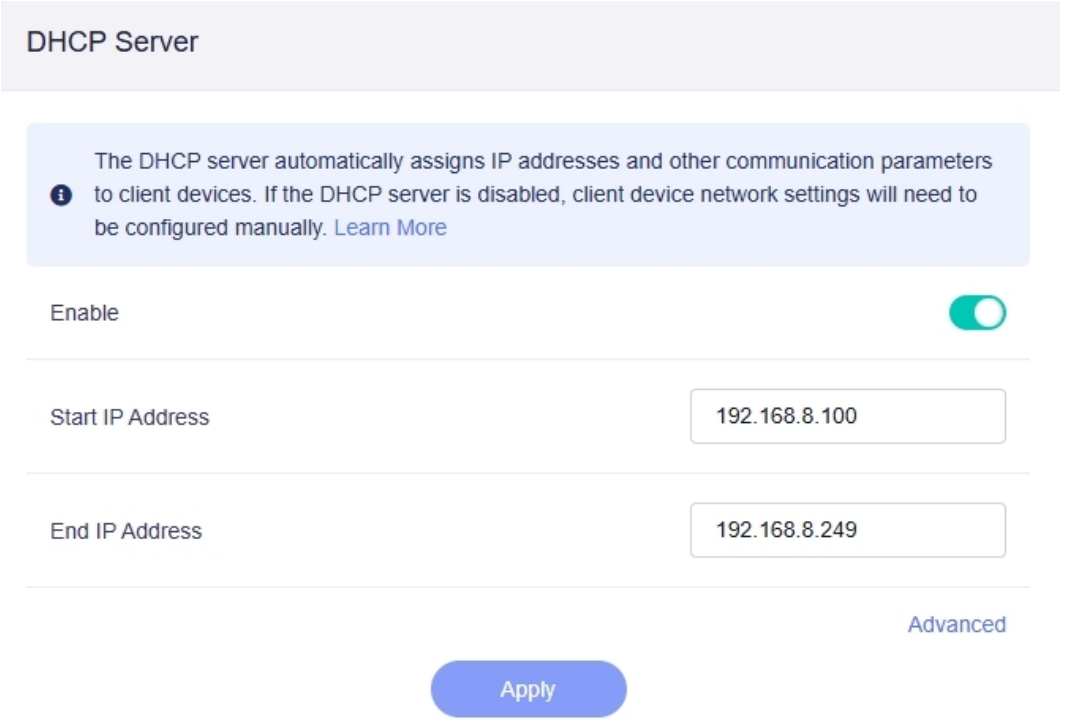


- **Dirección IP del enrutador**: esta es la dirección ingresada en la barra de direcciones de un navegador para acceder al panel de administración del enrutador. Es 192.168.8.1 de forma predeterminada y se puede cambiar si entra en conflicto con la red ascendente.'panel de administración. Es 192.168.8.1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

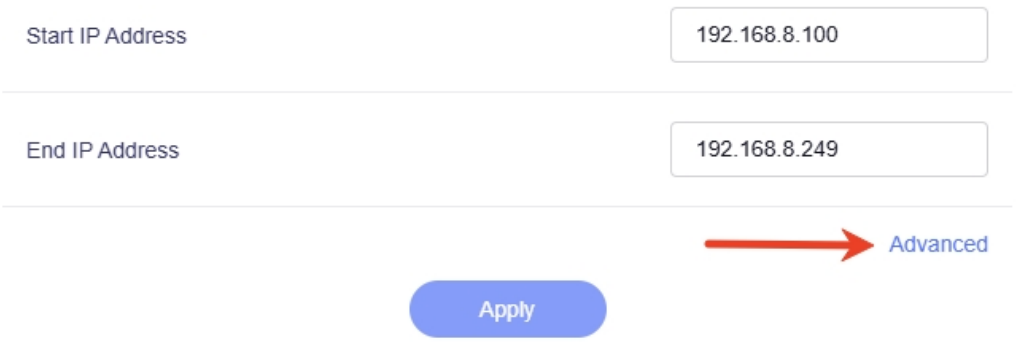
- **Aislamiento de AP**: puede aislar los dispositivos cliente de su red en un área de red separada. Estos dispositivos no pueden comunicarse con otros dispositivos en la red.

12.2.2 Servidor DHCP

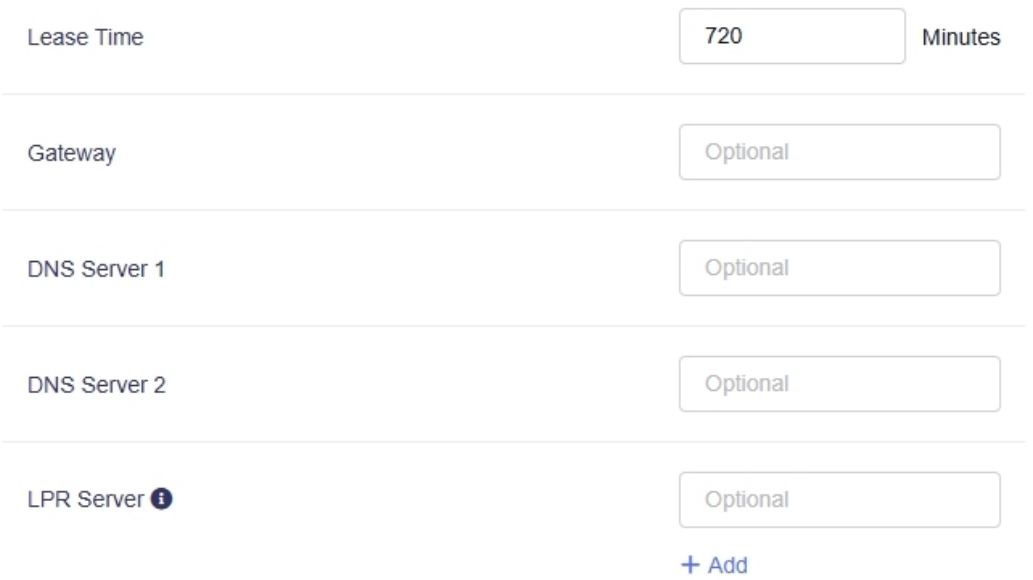
El servidor DHCP asigna automáticamente direcciones IP y otros parámetros de comunicación a cada cliente conectado. El servidor DHCP del enrutador GL.iNet está habilitado de forma predeterminada y el grupo de direcciones IP del servidor DHCP oscila entre 192.168.8.100 y 192.168.8.249. Puede personalizar 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 en direcciones IP.
- **Servidor DNS 2**: un servidor de respaldo utilizado para resolver nombres de dominio si el servidor DNS principal falla.
- **Servidor LPR**: (Servidor remoto de impresora de línea) Un servicio que administra trabajos de impresión y permite que los dispositivos en red envíen solicitudes de impresión a impresoras remotas. Múltiples puertos LPR para impresoras se puede configurar.

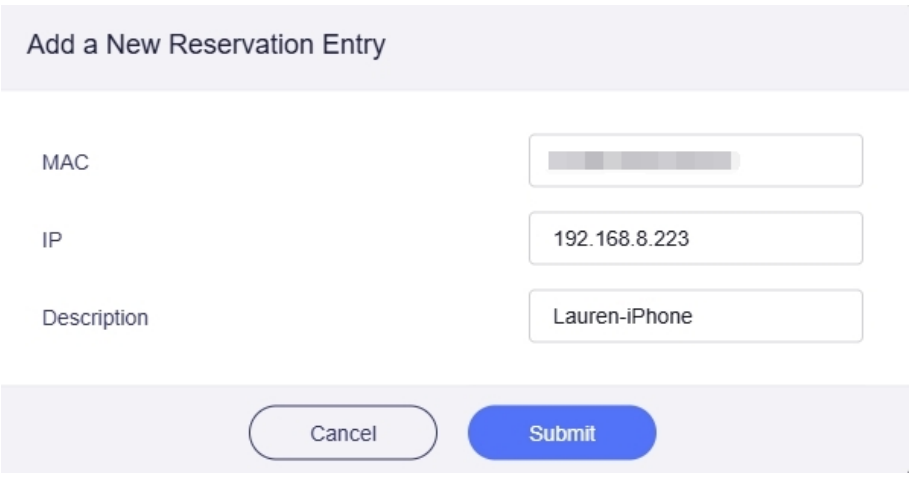
Nota: si el servidor DHCP está deshabilitado, debe configurar la IP estática y otros parámetros de comunicación manualmente para cada cliente. Consulte aquí para obtener más detalles.

12.2.3 Reserva de direcciones

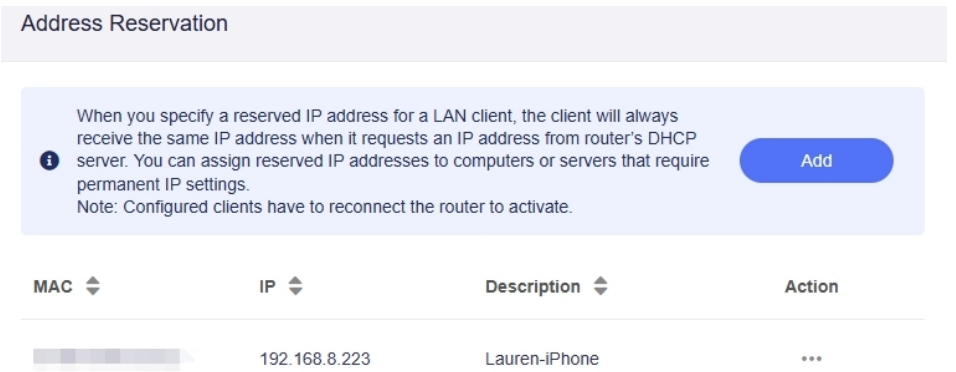
La reserva de dirección le permite especificar una dirección IP fija para un cliente LAN, de modo que el cliente siempre reciba la misma dirección IP cada vez que acceda al servidor DHCP del enrutador. Puede asignar direcciones IP reservadas a computadoras o servidores que requieren una configuración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

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

1. Registro Ingrese al panel de administración web de su enrutador', navegue hasta **RED** > **LAN** > **Reserva de direcciones** y haga clic en **Agregar**.
2. En la ventana emergente, seleccione la dirección MAC de la lista desplegable y luegoél 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.



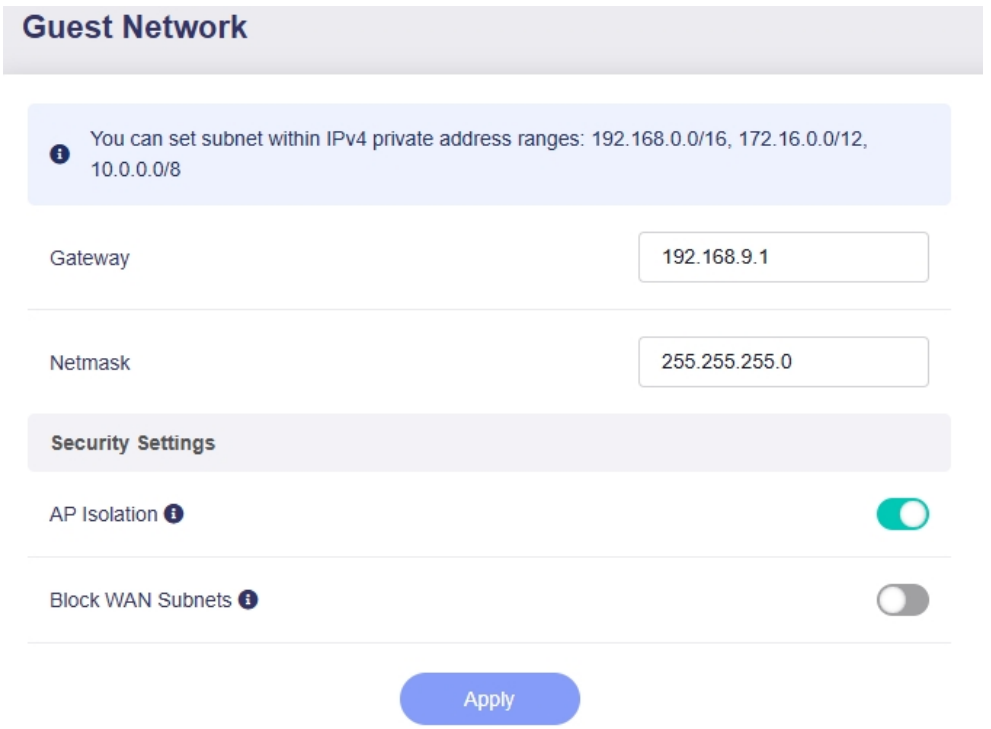
12.3 Red de invitados

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, incluidos los ajustes básicos y el servidor DHCP.

12.3.1 Configuración básica

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

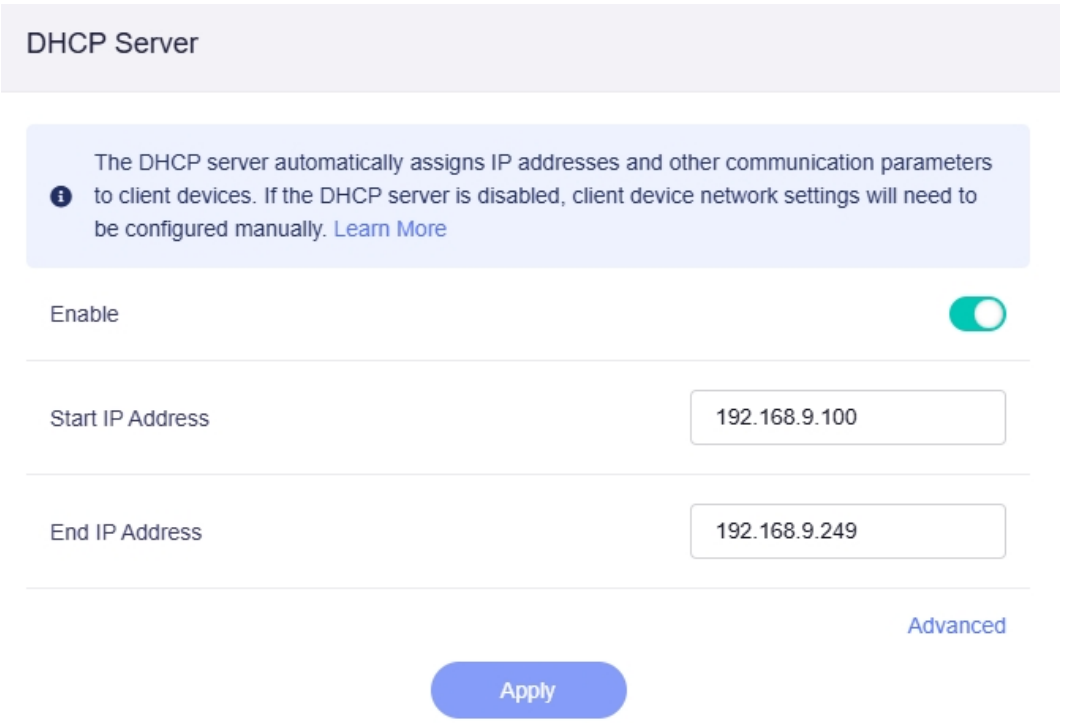


- **Puerta de enlace**: Es 192.168.9.1 de forma predeterminada y se puede cambiar si es necesario, pero no debe entrar en conflicto con la puerta de enlace de la red principal.
- **Máscara de red**: Hay dos opciones disponibles: 255.255.255.0 y 255.255.0.0.
- **Aislamiento AP**: se utiliza para aislar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

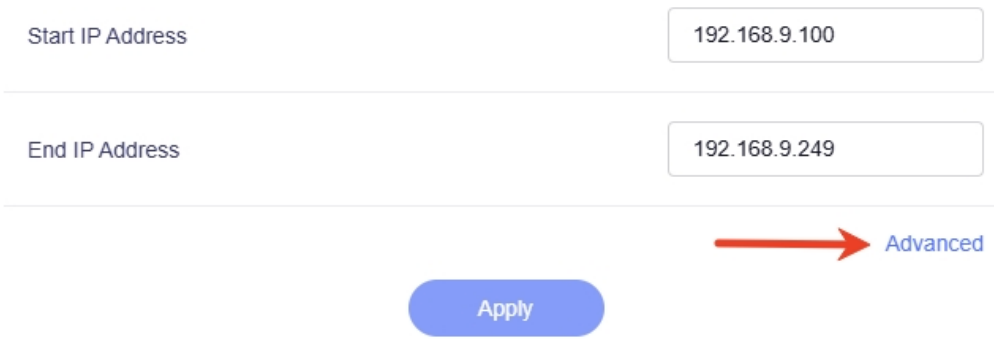
12.3.2 Servidor DHCP

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

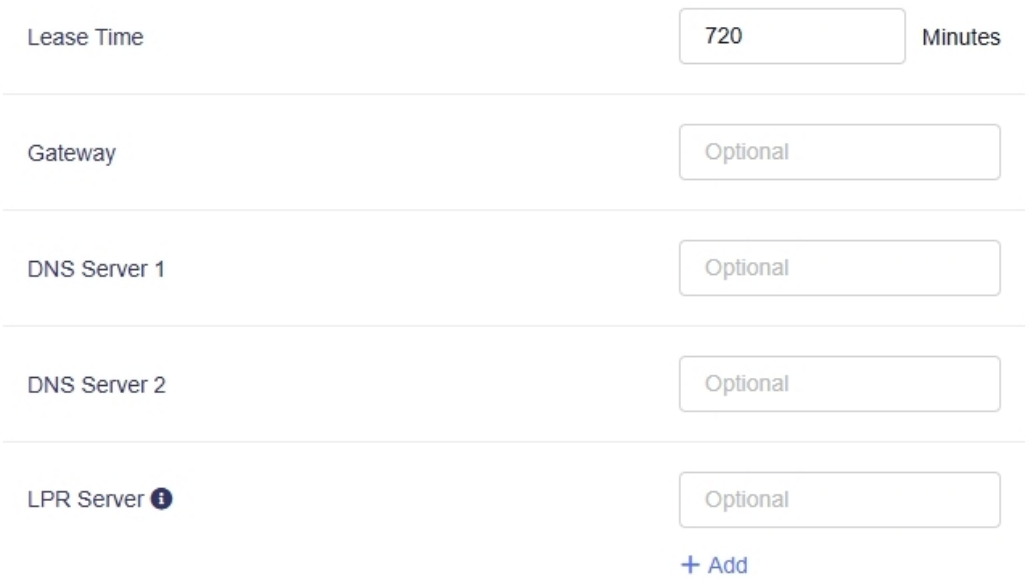
Cuando está habilitado, el servidor DHCP asigna automáticamente direcciones IP y otros parámetros de comunicación a cada cliente conectado. El grupo de direcciones IP del servidor DHCP para la red de invitados oscila entre 192.168.9.100 y 192.168.9.249. Puede personalizar el rango de direcciones si es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



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



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



- **Tiempo de concesión**: la duración durante la cual un dispositivo puede usar una dirección IP asignada a través de DHCP de la red de invitados.
- **Puerta de enlace**: el componente del enrutador que enruta el tráfico entre la gred de invitados y las redes externas (por ejemplo, Internet).
- **Servidor DNS 1**: el servidor principal responsable de traducir 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.

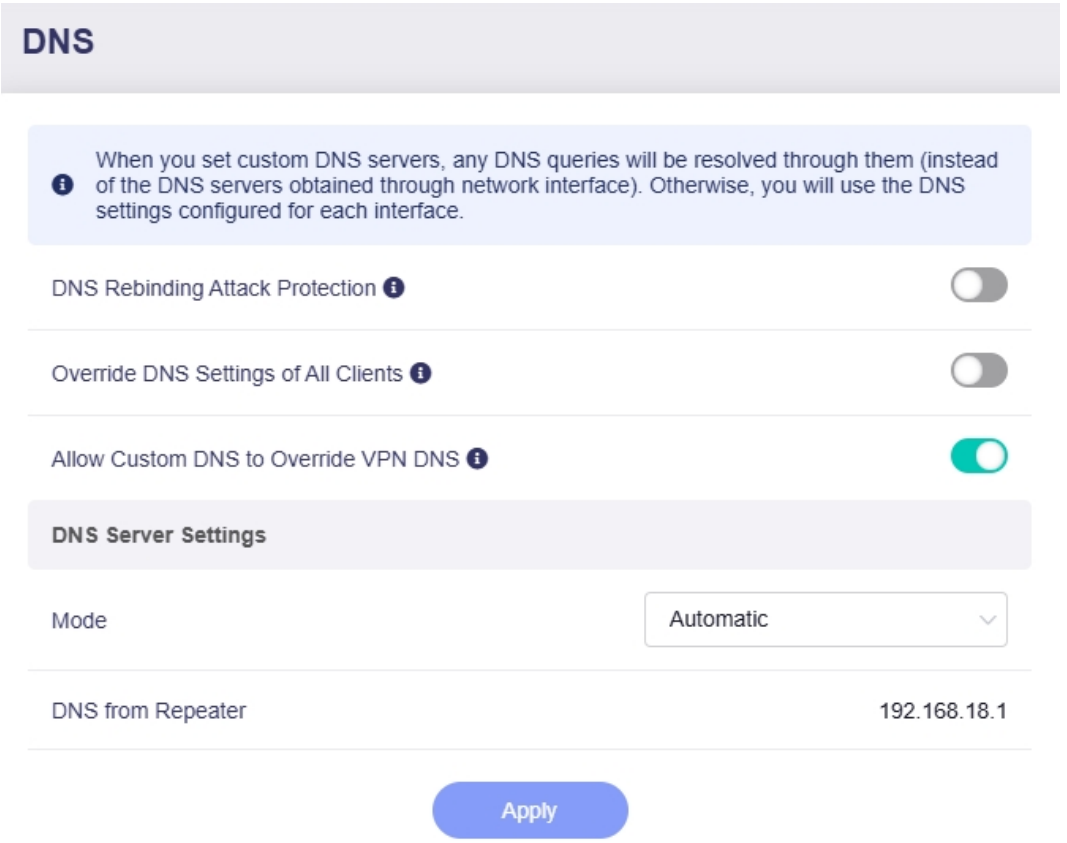
12.4 DNS

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

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

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

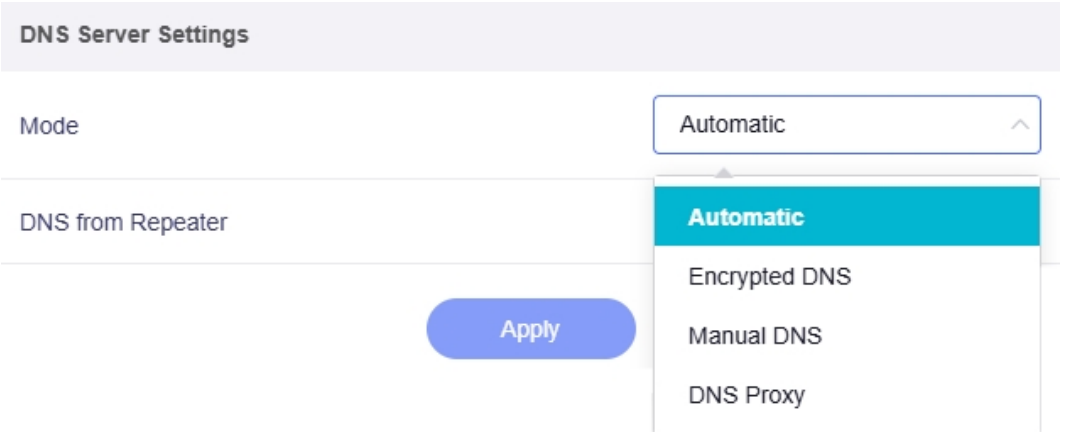
12.4.1 Configuración general



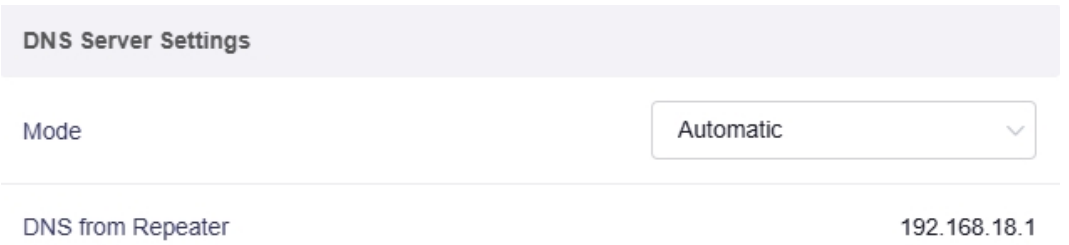
- **Protección contra ataques de revinculación de DNS**: protege contra ataques de revinculación de DNS bloqueando intentos maliciosos de resolución de DNS. Tenga en cuenta que habilitarlo puede causar fallas en la búsqueda de DNS privado; deshabilítelo si su red utiliza un portal cautivo (por ejemplo, páginas de inicio de sesión Wi-Fi públicas).
- **Anular la configuración DNS de todos los clientes**: Si está habilitado, todos los dispositivoss será forzado para usar 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.

12.4.2 Configuración del servidor DNS

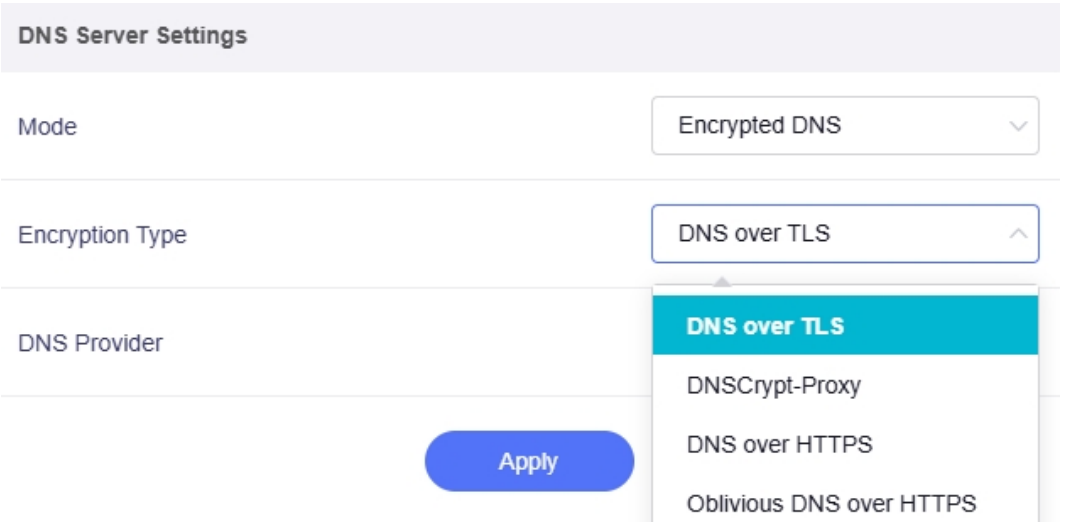
Hay cuatro modos para el servidor DNS: Automático, DNS cifrado, DNS manual y Proxy DNS.



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

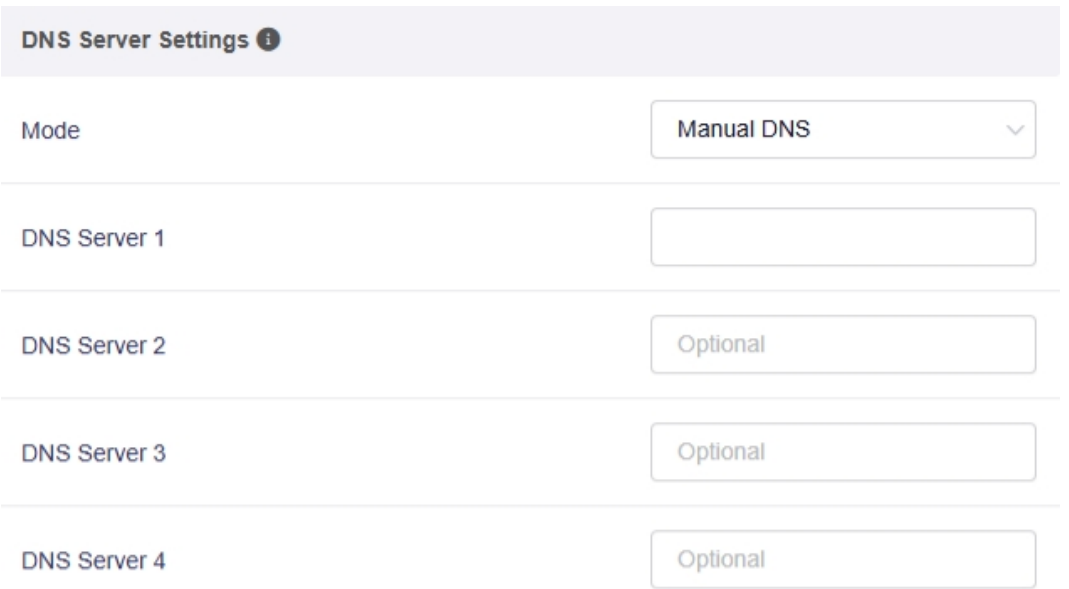


2. **DNS cifrado**: cuando se selecciona, el enrutador utilizará protocolos cifrados para procesar consultas DNS, protegiendo los datos de resolución contra escuchas o manipulación.
   Tiene cuatro tipos de cifrado: DNS sobre TLS, DNSCrypt-Proxy, DNS sobre HTTPS y DNS ajeno a través de HTTPS.



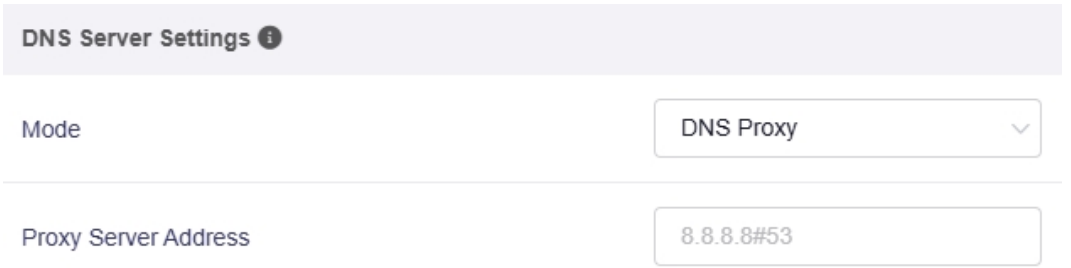
- Para DNS sobre TLS, seleccione un proveedor de DNS entre Control D, NextDNS y Cloudflare.
- Para los otros tres (es decir, DNSCrypt-Proxy, DNS sobre HTTPS y DNS ajeno a través de HTTPS), seleccione al menos un servidor DNS del repositorio. Se pueden seleccionar hasta 8 servidores. Cuando se seleccionan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

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



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

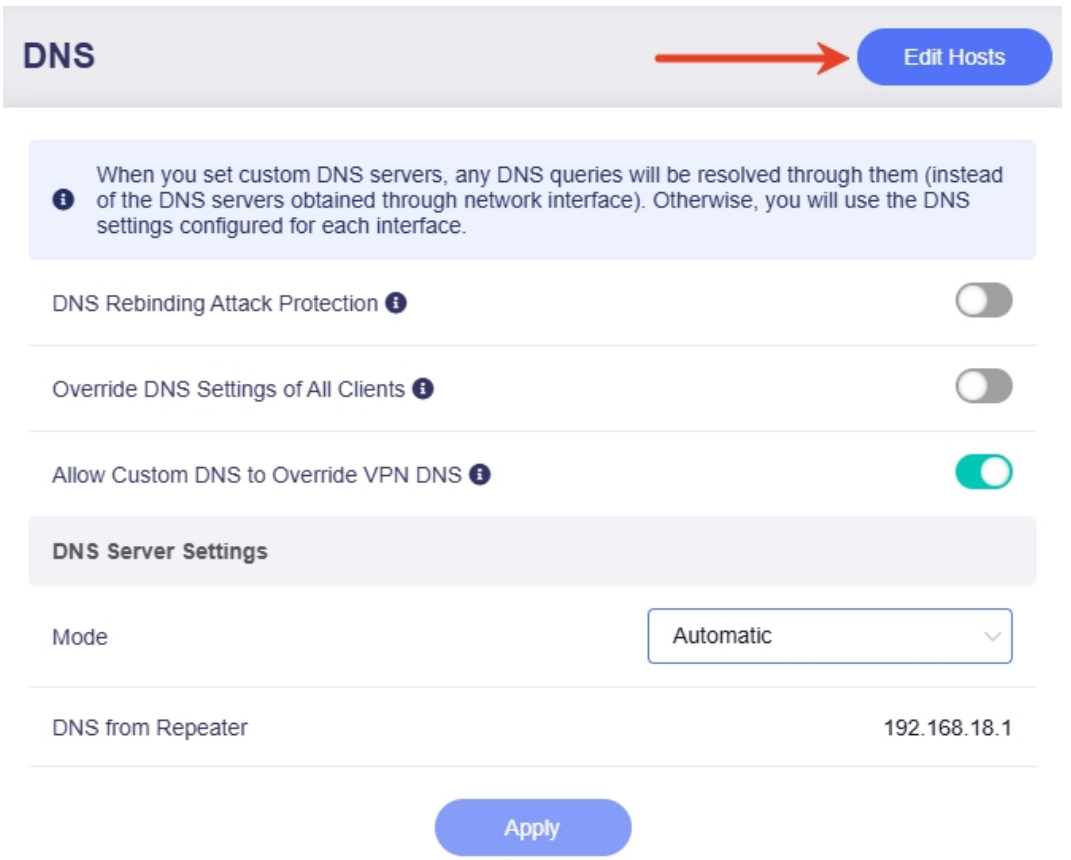
4. **Proxy DNS**: cuando se selecciona, el enrutador reenvía todas las consultas DNS a través de un servidor proxy, permiteresolución a través del entorno de red del proxy para necesidades de acceso específicas.



12.4.3 Editar hosts

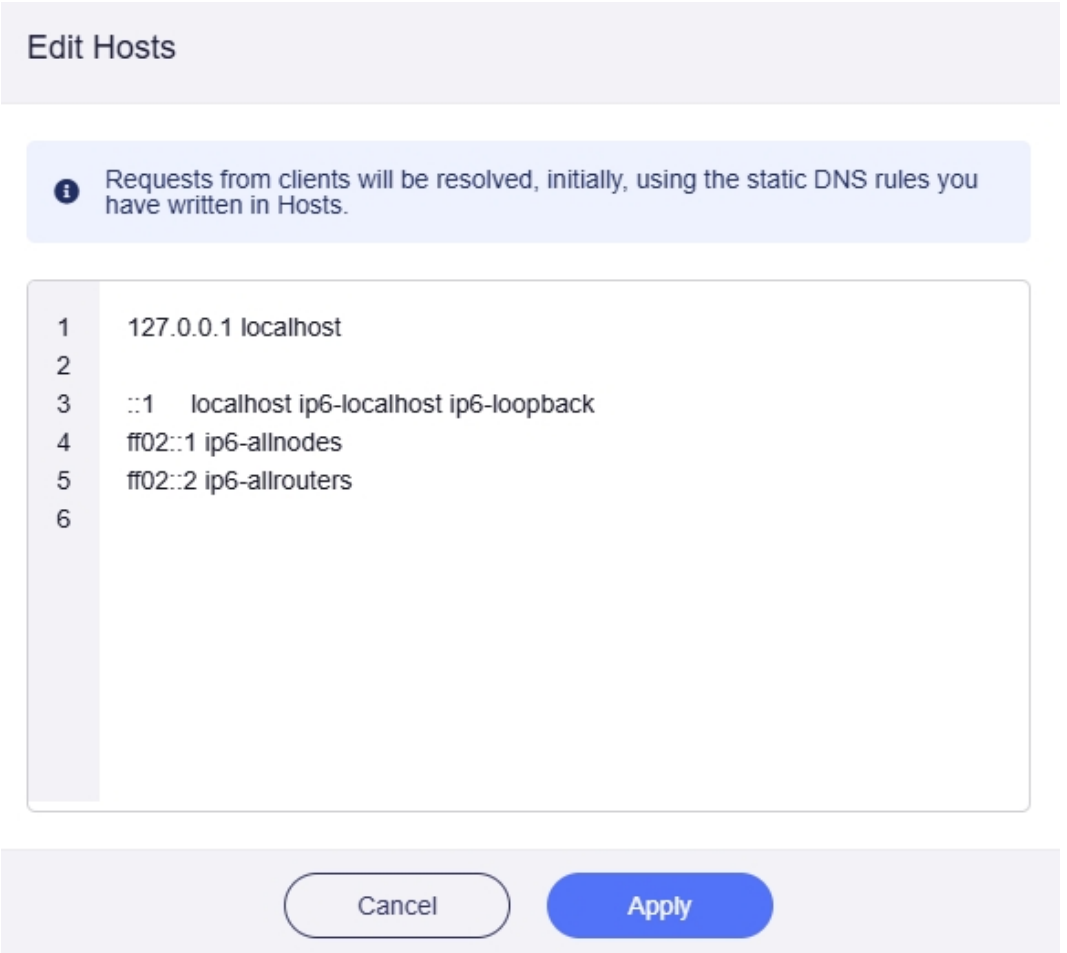
Puede definir reglas de resolución de DNS estáticas si es necesario.

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



Las solicitudes de los clientes se resolverán preferentemente utilizando las reglas DNS estáticas escritas aquí, lo que le permitirá asignar manualmente direcciones IP a nombres de

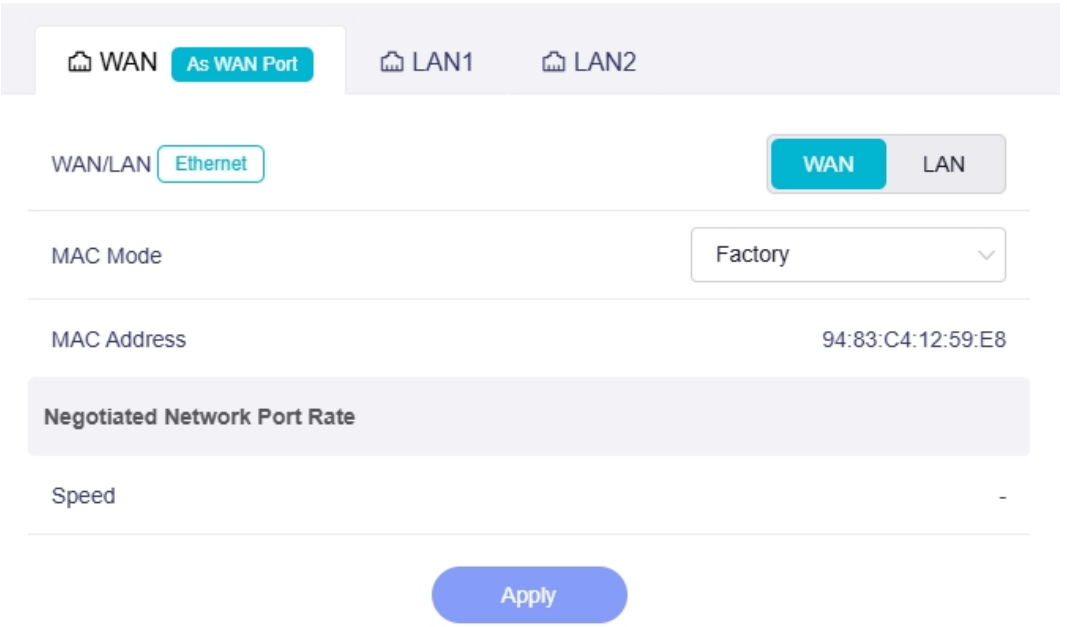
host (por ejemplo, las entradas predeterminadas como 127.0.0.1 localhost para loopback local) para un control personalizado de la resolución de nombres de dominio.



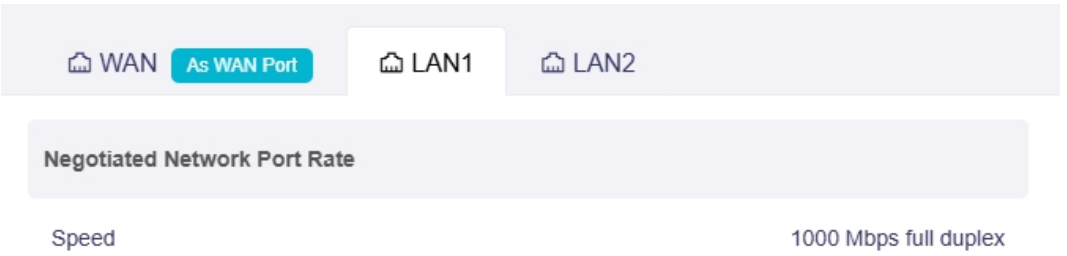
12.5 Puerto Ethernet

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'.

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



La sección **LAN** muestra la tarifa negociada del puerto LAN.



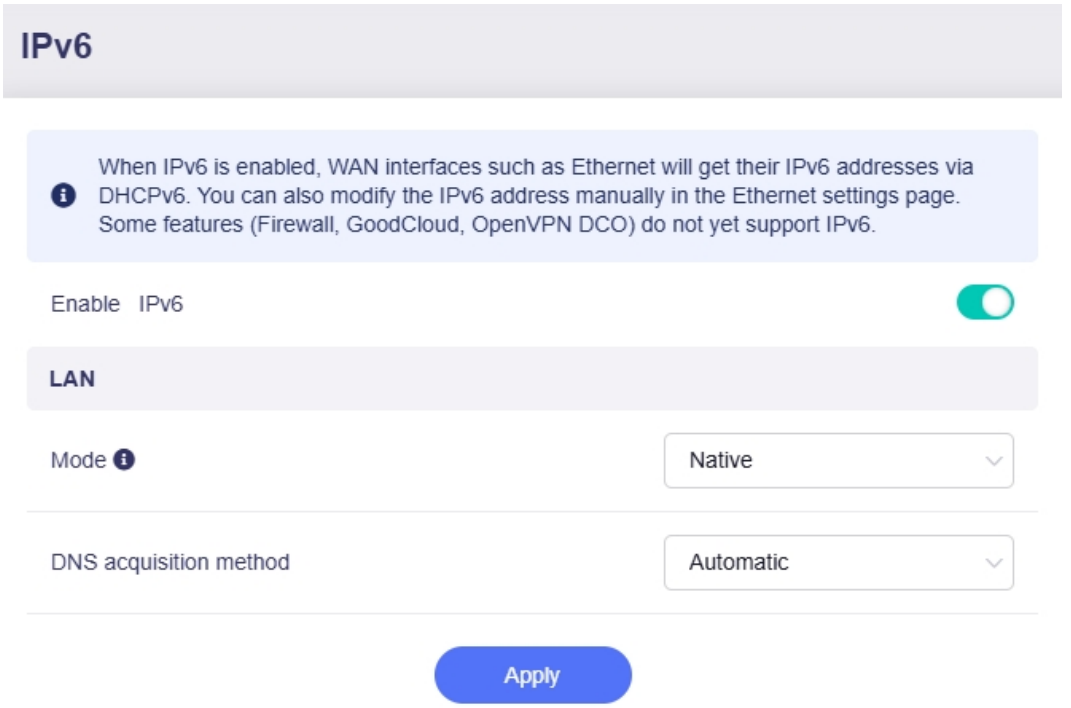
Nota: Solo se muestra la tarifa negociada para el puerto WAN y LAN cuando se conecta un cable Ethernet. Depende tanto del puerto Ethernet como del cable Ethernet.

12.6 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.

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



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

12.6.1 Modo IPv6

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

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

12.6.2 Método de obtención de DNS

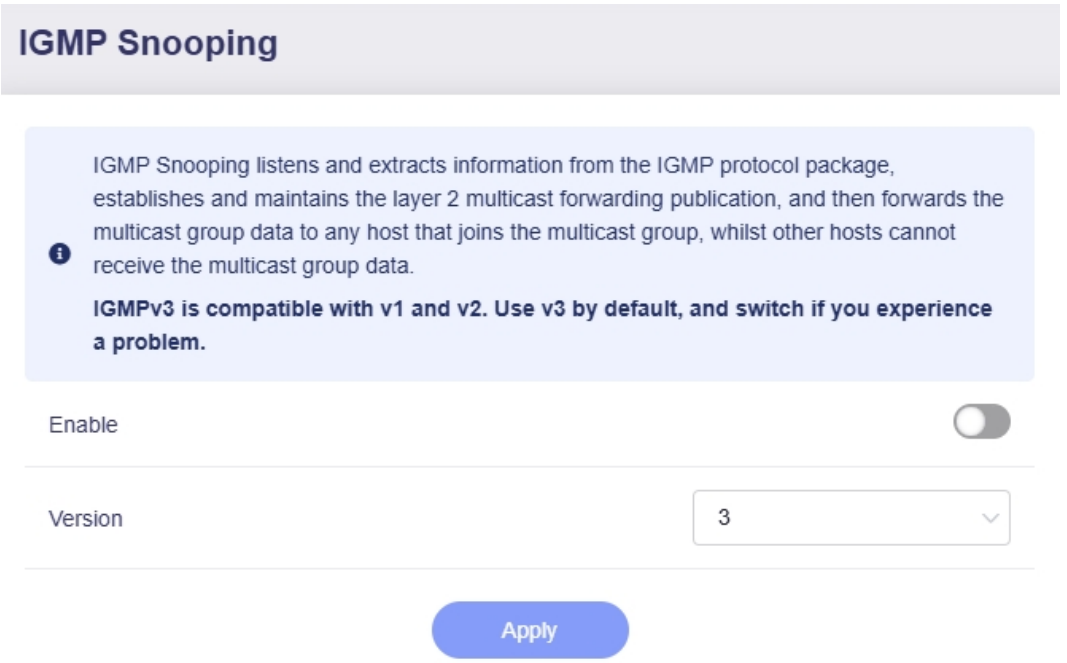
Determina cómo el enrutador obtiene las direcciones del servidor DNS IPv6. Hay dos opciones: Automático y Manual.

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

12.7 Inspección IGMP

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

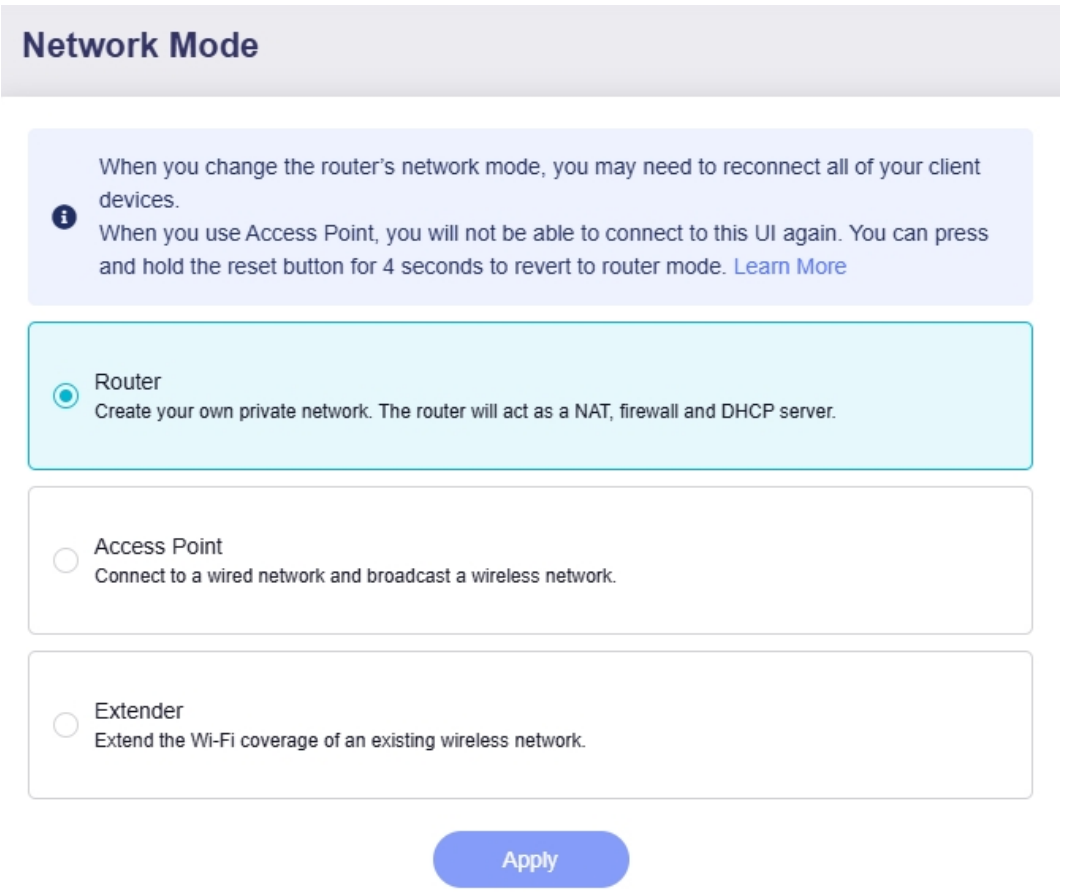
Inicie sesión en el panel de administración web de su enrutador' y navegue hasta **RED** > **Inspección IGMP**. Puede habilitar para usar la función de multidifusión en su enrutador si es necesario.



12.8 Modo de red

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

Inicie sesión en 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 exclusivamente como un transmisor y conmutador de señal inalámbrica en lugar de una puerta de enlace independiente.
- **Extensor**: este modo está diseñado para ampliar la cobertura Wi-Fi de una red inalámbrica existente y eliminar zonas muertas de señal en áreas con mala conectividad. Permite que el enrutador reciba señales del enrutador principal de forma inalámbrica, las amplifique y retransmita la señal potenciada. A diferencia del modo Punto de acceso, no requiere conexión por cable al enrutador principal, pero puede provocar que el ancho de banda se reduzca a la mitad, ya que el dispositivo tiene que manejar la recepción y transmisión de señales simultáneas.

Nota:

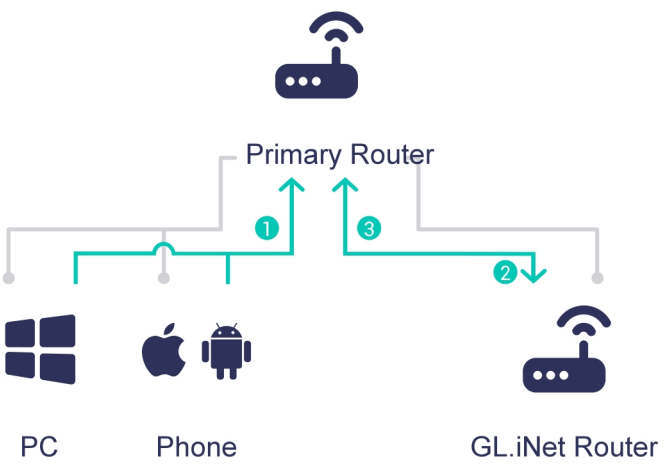
1. Cuando se cambia el modo de red, todos los dispositivos cliente se volverán a conectar al enrutador para una conectividad de red estable.
2. **En el modo de punto de acceso, no podrá acceder al administrador web panel usando la dirección IP original**. En su lugar, debe iniciar sesión en el enrutador ascendente para encontrar la dirección IP que ha asignado a este enrutador y luego usar esta dirección IP para acceder al panel de administración web. Si no tiene acceso al enrutador ascendente, presione y mantenga presionado el botón de reinicio durante 4 segundos para revertirlo al modo de enrutador predeterminado.
3. **En el modo Punto de acceso/Extensor, las siguientes funciones no estarán disponibles**: Control de acceso (lista de permitidos y lista 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, Puerta de enlace directa, Vigilancia IGMP, aceleración de red, configuración de NAT.

12.9 Puerta de enlace directa

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

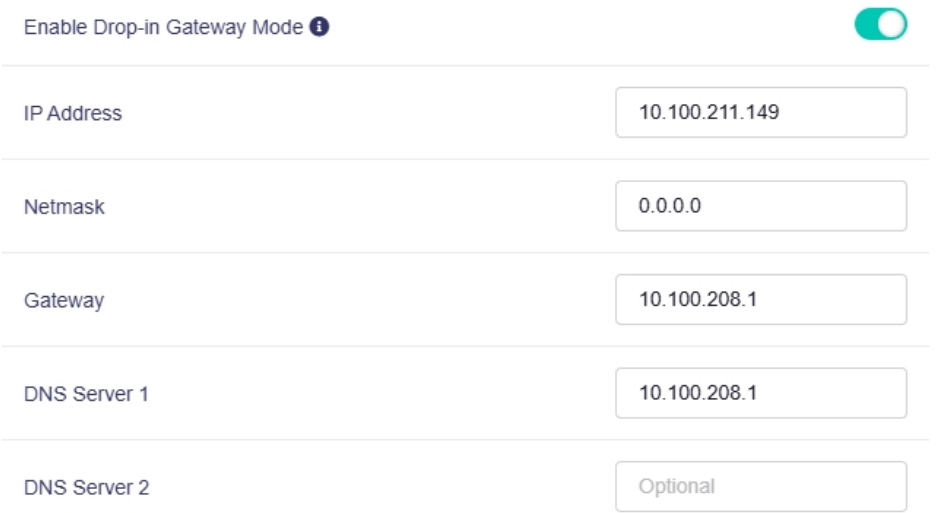
- **Gray lines** ilustran la topología de conexión física: dispositivos cliente (por ejemplo, computadora, computadora portátil) se conectan al enrutador principal, y el puerto LAN

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

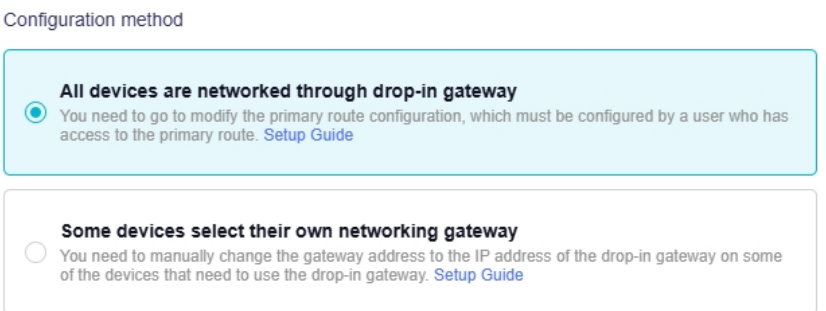
- **Glíneas verdes** representan la ruta de transmisión de datos secuencial cuando Drop-in Gateway está activo, con las flechas numeradas que indican el orden del flujo de tráfico:
  1. Tráfico desde dispositivos cliente se enruta primero al enrutador principal;
  2. El enrutador principal reenvía el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

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

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



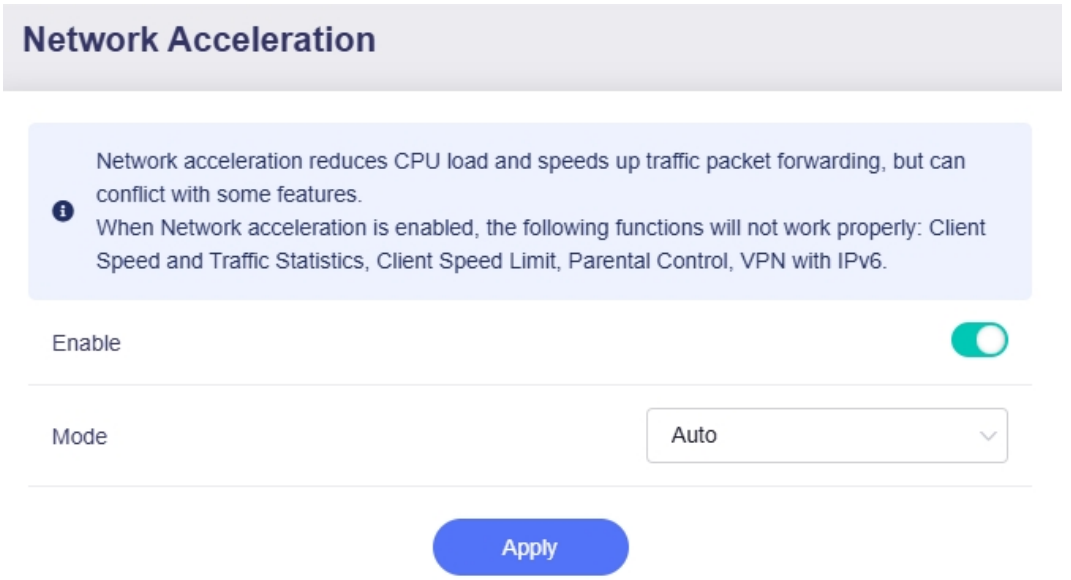
2. Seleccione el método de configuración, luego haga clic en **Aplicar**. Consulte este tutorial para detalless.



12.10 Aceleración de red

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

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



- **Auto**: cambia automáticamente entre los dos modos de aceleración según el uso real.
- **Aceleración de hardware**: Descarga Tareas de red de alta frecuencia (por ejemplo, NAT, reenvío de paquetes, verificación de suma de comprobación) a hardware dedicado como NPU o chips HWNAT. Funciona específicamente en conexiones Ethernet y repetidoras, sobresaliendo en estos escenarios con rutas fijas y reglas simples para ofrecer alto rendimiento, baja latencia y carga mínima de CPU para la transmisión de datos a velocidad de cable.
- **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

Seguridad

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

13.1 Reenvío de puertos

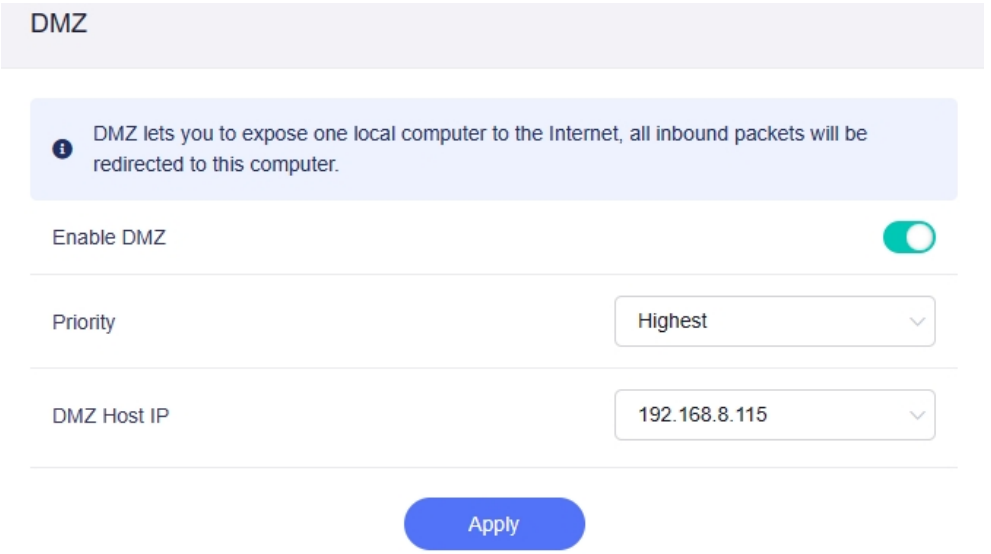
El reenvío de puertos es una característica de red que enruta solicitudes externas a dispositivos específicos en su red local. La página de reenvío de puertos incluye dos funciones clave: **DMZ** (para acceso completo directo a un único dispositivo) y **Reenvío de puertos** (para acceso dirigido a puertos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

13.1.1 DMZ

DMZ permitirle permite exponer una computadora a Internet, de modo que todos los paquetes entrantes se redireccionen 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. Activar **Activar DMZ**. Sseleccione la Prioridad y la IP del host DMZ de la lista desplegable y haga clic en **Aplicar**.



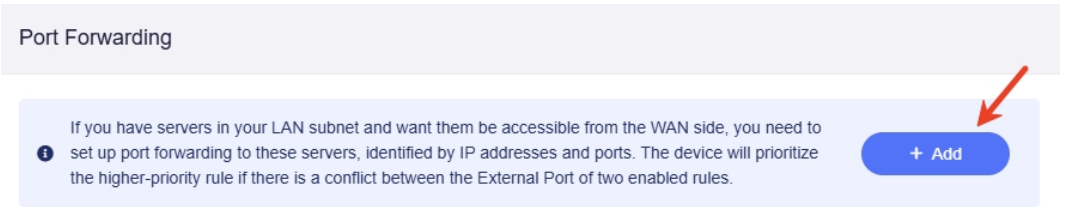
- **Prioridad**: configúrelo como Más alto o Más bajo. Si la prioridad de la DMZ es mayor que las reglas de reenvío de puertos, todas las reglas de reenvío de puertos quedarán invalidadas. De lo contrario, las solicitudes se reenviarán al dispositivo cliente DMZ solo si el puerto al que se accede no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

13.1.2 Reenvío de puertos

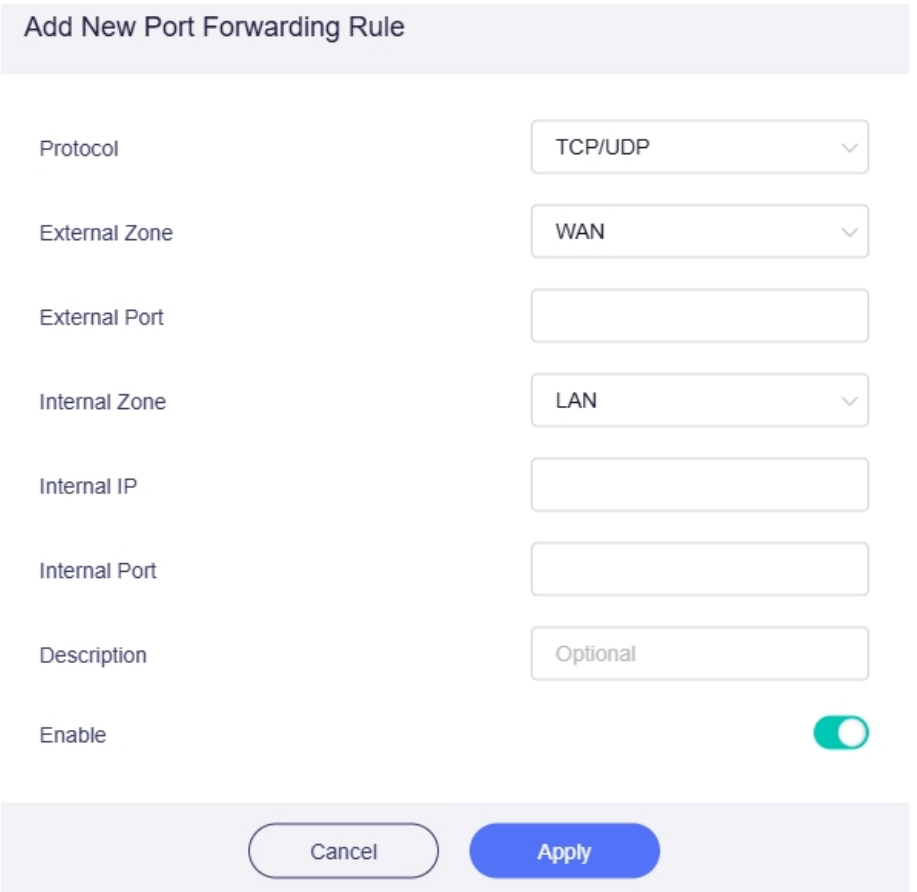
El reenvío de puertos permite que las computadoras remotas se conecten a una computadora o servidor local detrás del firewall de la LAN (por ejemplo, servidores web, servidores FTP).

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

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



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



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

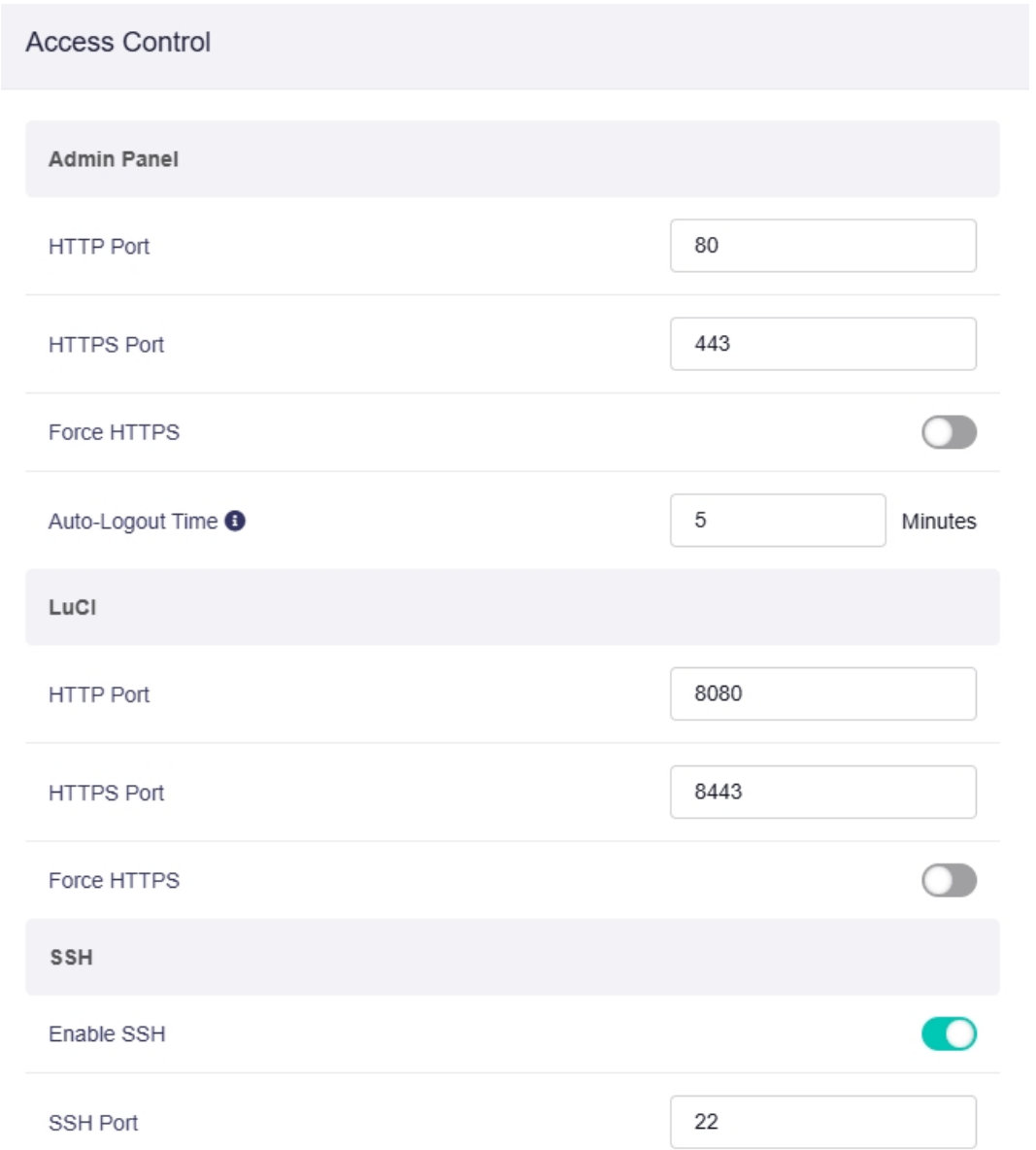
- **Zona externa**: las opciones disponibles son WAN, Cliente WireGuard, Servidor WireGuard, Cliente OpenVPN, Servidor OpenVPN, LAN e Invitado.
- **Puerto externo**: El número(s) de puertos externos. Introduzca aquí un número de puerto específico. El rango de puertos es 1–65535. Puede configurar un solo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

13.2 Control de gestión

Inicie sesión en el panel de administración web de su enrutador y navegue hasta **SEGURIDAD** > **Control de gestión**. Esta página contiene tres secciones: (Local) Acceso Control, Remoción Unacceso Control y aperturapen Ports en Rexterno.

13.2.1 Control de acceso

Esta sección administra el acceso a los múltiples enrutadores' interfaces (panel de administración web, 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.

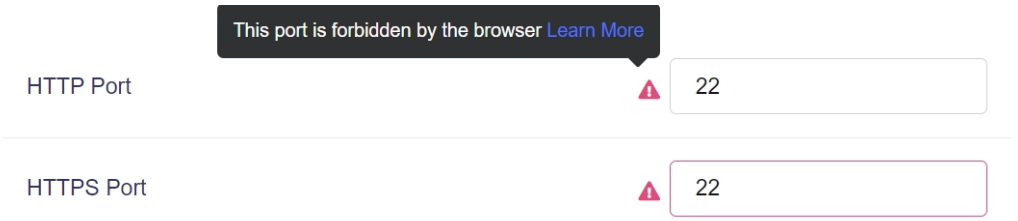
- **Puerto HTTP**: El valor predeterminado es 8080, para acceso HTTP sin cifrar a la interfaz LuCI.
- **Puerto HTTPS**: el valor predeterminado es 8443, para un acceso HTTPS seguro a la interfaz LuCI.
- **Forzar HTTPS**: cuando está habilitado, el acceso a la interfaz LuCI se exige para utilizar un HTTPS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

SSH

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

Nota:

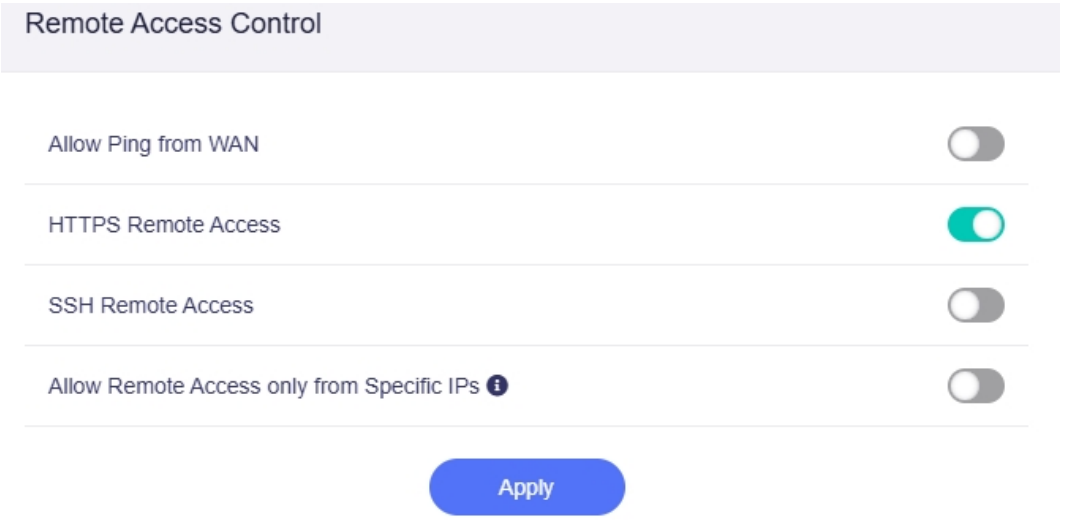
1. Si asigna un número de puerto que entra en conflicto con un puerto reservado (o uno reservado para servicios específicos por navegadores/convenciones de red), aparecerá un mensaje que indicará "Este puerto está prohibido por el navegador".



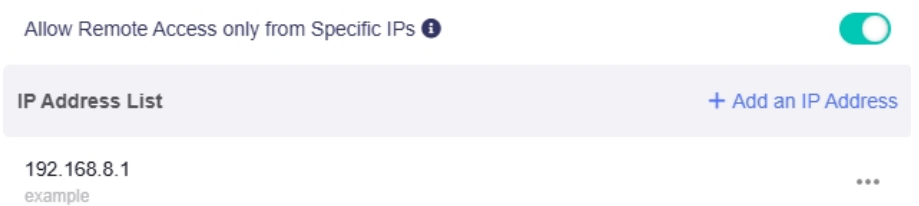
2. Si el número de puerto se modifica en el firmware, deberá ingresar el número de puerto correcto para acceder al panel de administración. Si olvidó el número de puerto, reinicie el enrutador para restaurar el número de puerto predeterminado.
3. La configuración de acceso a LuCI está disponible solo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

13.2.2 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.

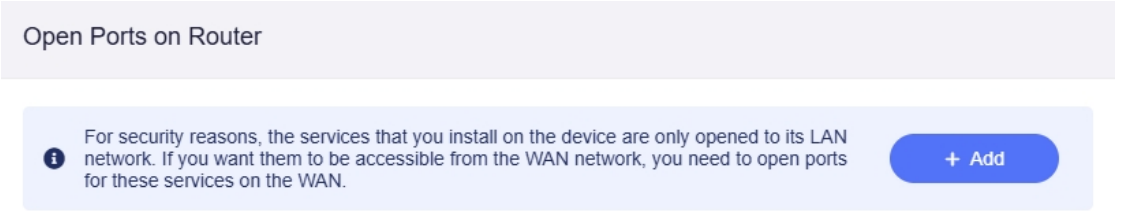


- **Permitir ping desde WAN**: Apermitir ping desde el lado WAN del enrutadorpuede ayudar a los usuarios a comprobar si se puede acceder al enrutador a través de la WAN wcuando hay un problema de red así como a determinar la latencia de la red y la pérdida de paquetes.
- **Acceso remoto HTTPS**: El acceso remoto HTTPS permite el acceso remoto seguro al panel de administración web del enrutador a través del protocolo HTTPS. Garantiza la transmisión de datos cifrados cuando se administra 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.

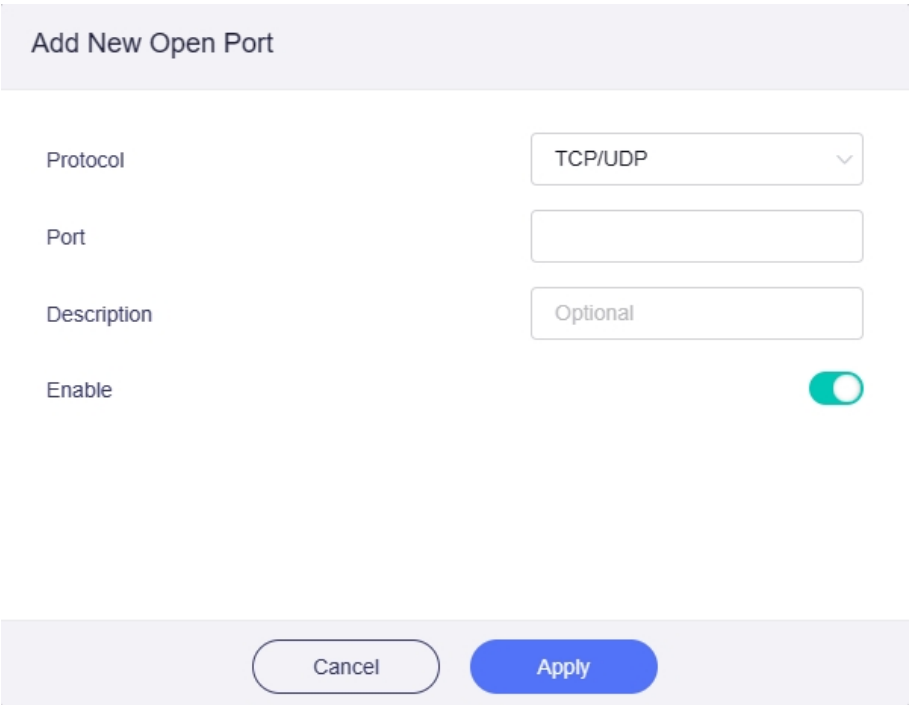


13.2.3 Abrir puertos en el enrutador

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.

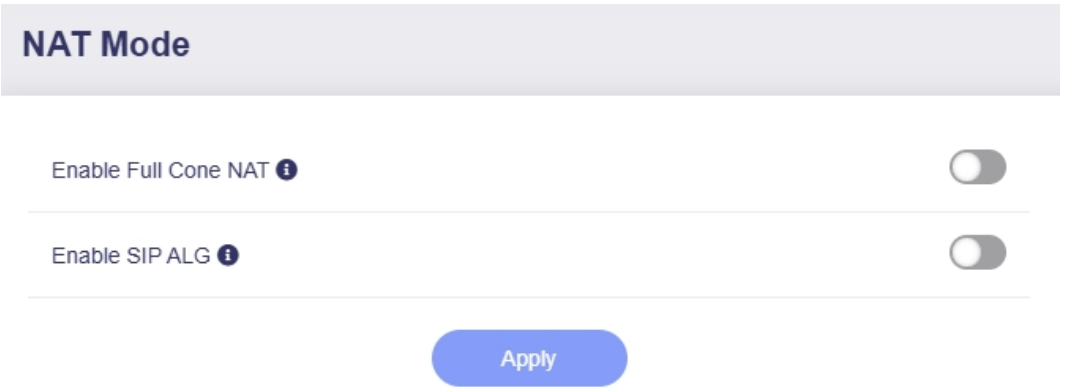


- **Protocolo**: seleccione el protocolo de red (TCP, UDP o TCP/UDP) para el puerto. Esto determina cómo se transmiten los datos para el servicio asociado con el puerto.
- **Puerto**: ingrese el número de puerto específico que desea abrir.

- **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.

13.3 Modo NAT

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

Capítulo 14

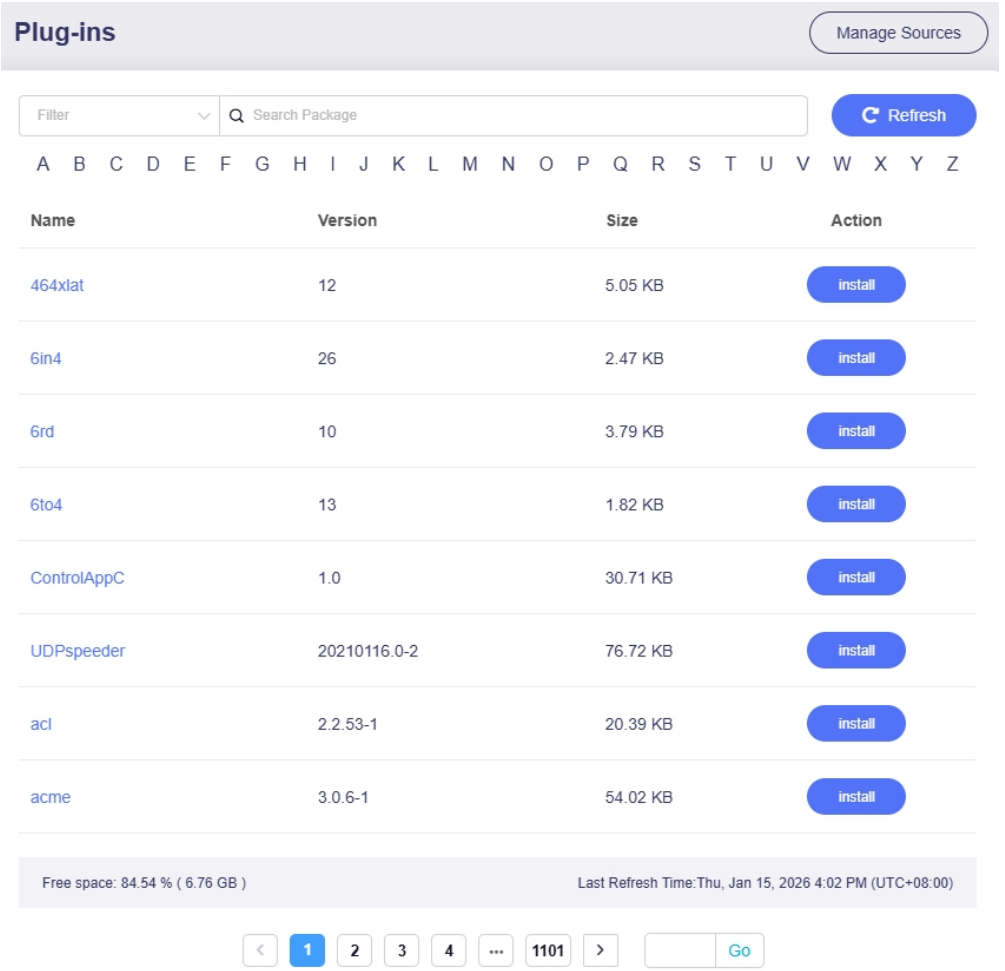
Aplicaciones

Este capítulo presenta algunas aplicaciones en los enrutadores GL.iNet, incluidas Complementos, DNS dinámico y almacenamiento de red.

14.1 Complementos

La página Complementos le permite administrar paquetes OpenWrt.

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



Nota:

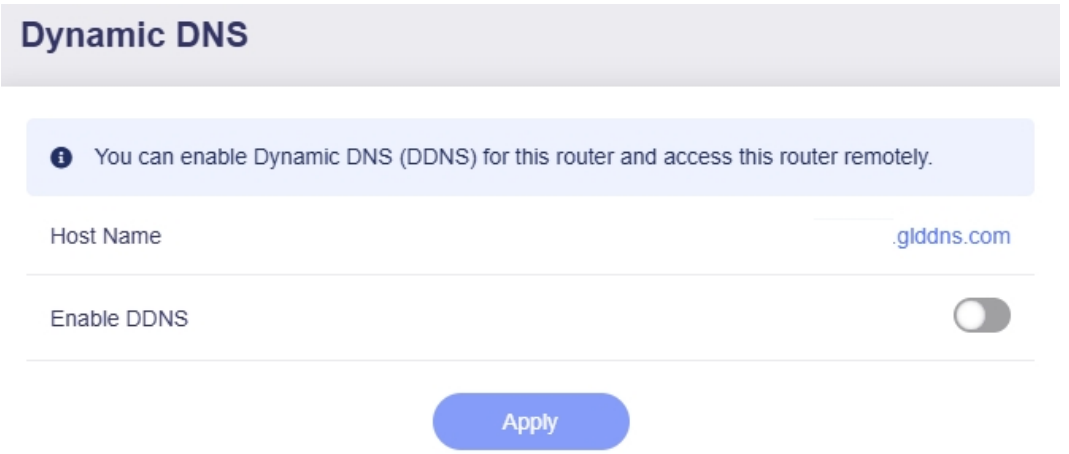
1. No se recomienda actualizar los complementos preinstalados en el firmware oficial de GL.iNet, como nginx, adguard home, tailscale, etc.
2. Los complementos de terceros instalados manualmente por los usuarios se pueden actualizar; sin embargo, GL.iNet no es responsable de ningún problema de seguridad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

14.2 DNS dinámico

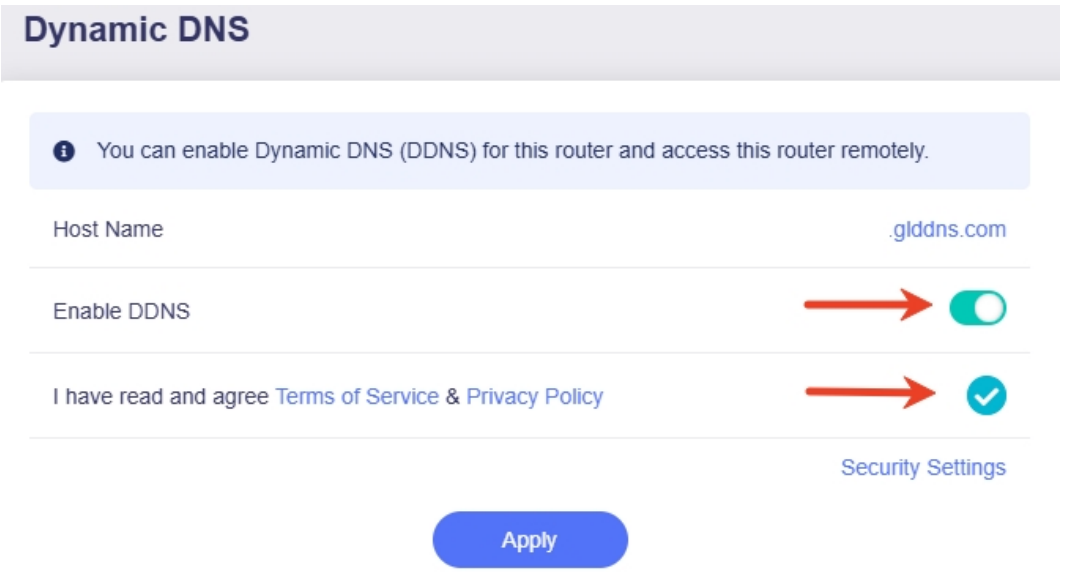
Dinámico El servicio de nombres de dominio (DDNS o DNS dinámico) es un servicio que se utiliza para asignar un nombre de dominio a la dirección IP dinámica de un dispositivo de red. Con DNS dinámico, puede acceder a su enrutador de forma remota. Se requiere una dirección IP pública para esta funcionalidad.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

14.2.1 Habilitar DDNS

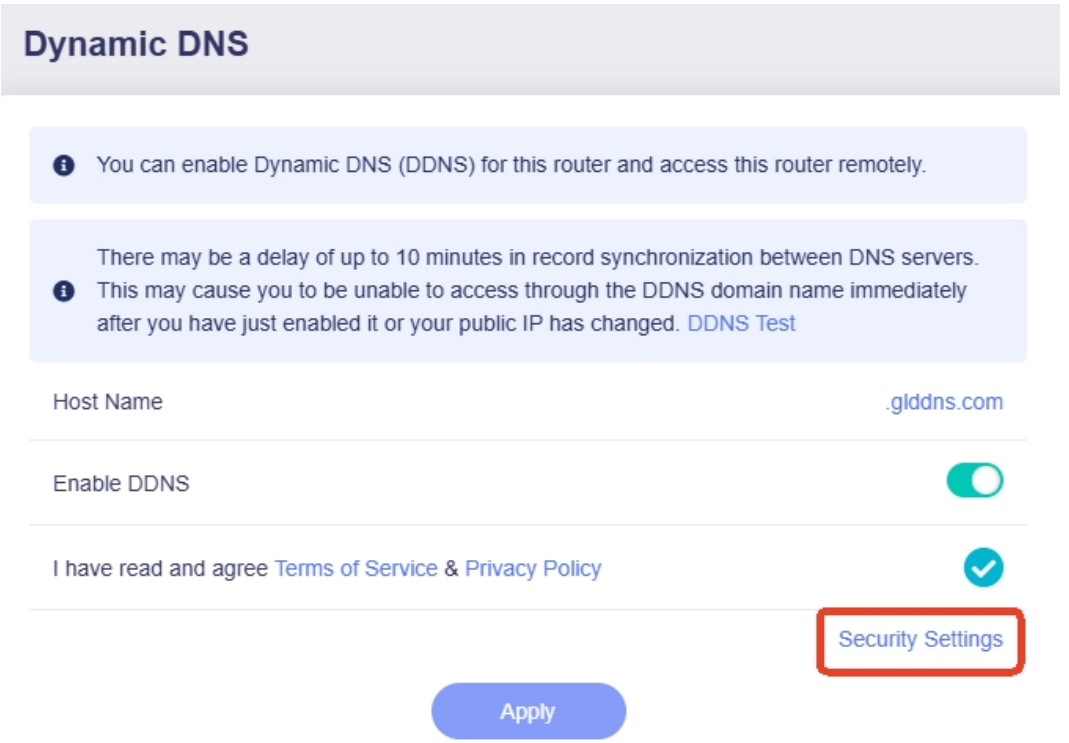
1. Inicie sesión en su enrutador's web admin panel, navegue hasta **APLICACIONES** > **DNS dinámico**, la página se muestra como a continuación.



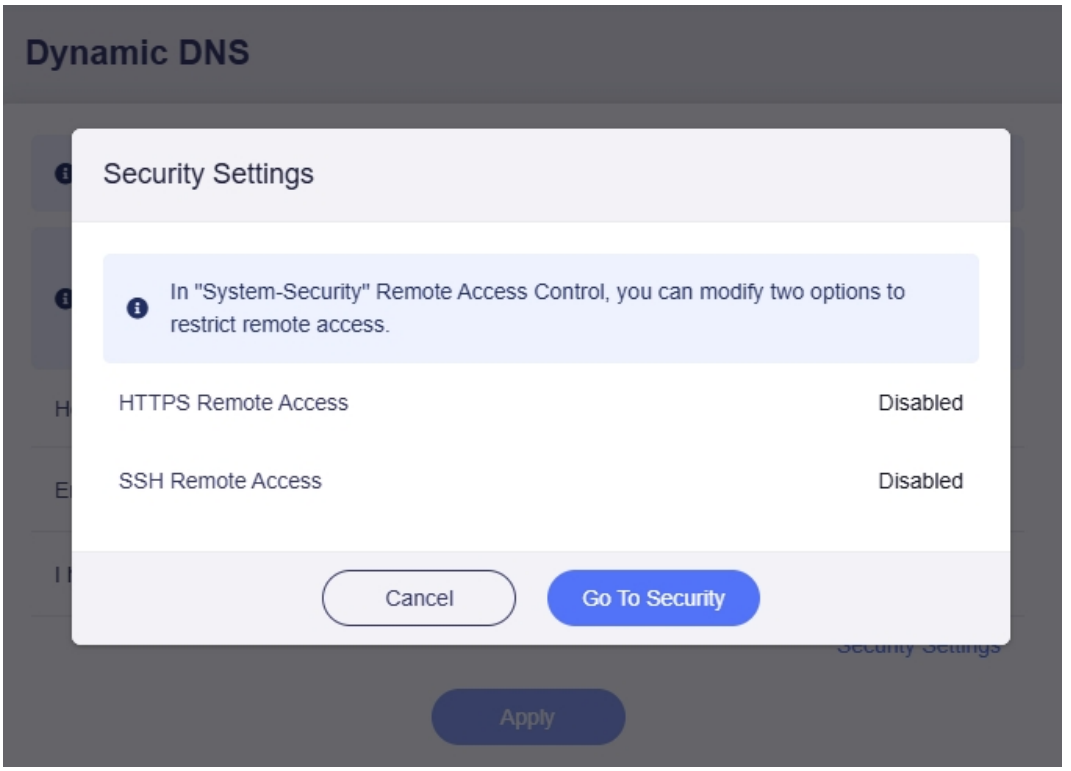
2. Active **Habilitar DDNS**, leer y aceptar los **Términos de servicios y política de privacidad**, luego haga clic en **Aplicar**.



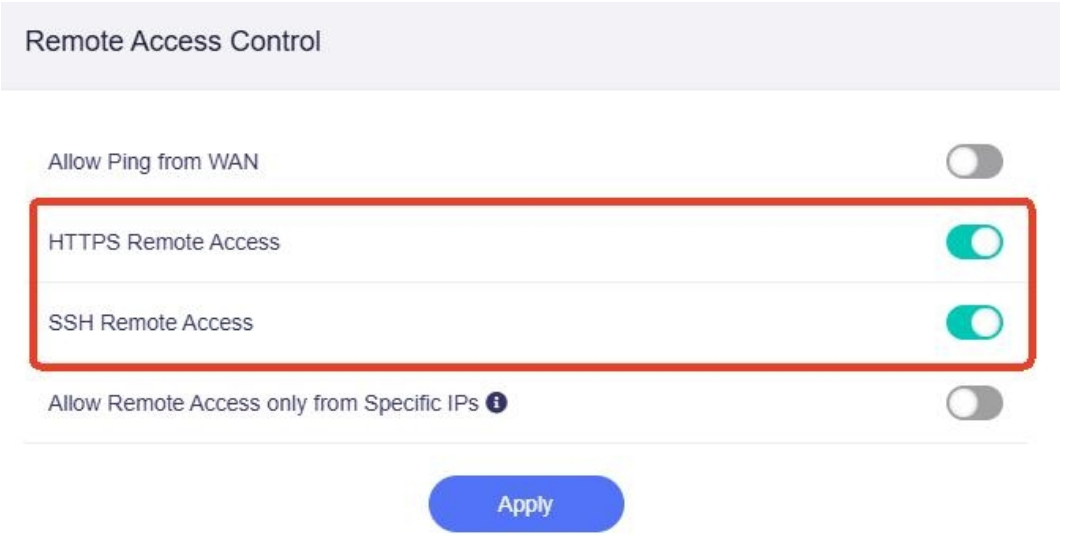
3. Haga clic **Configuración de seguridad** en la esquina inferior derecha.



4. En la ventana emergente, verifique si el acceso remoto que desea usar es habilitado.



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



Nota:

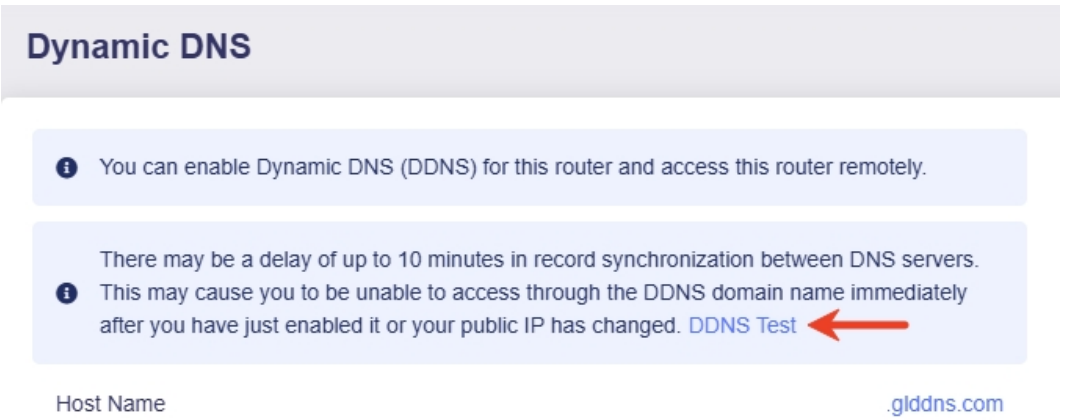
1. Puede haber un retraso de hasta 10 minutos en la sincronización de registros entre servidores DNS. Esto puede impedirle acceder a través del nombre de dominio DDNS inmediatamente después de habilitarlo o cuando cambie su IP pública.
2. Si habilita DDNS y el Cliente VPN al mismo tiempo, enseguro que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

14.2.2 Comprobar si DDNS funciona

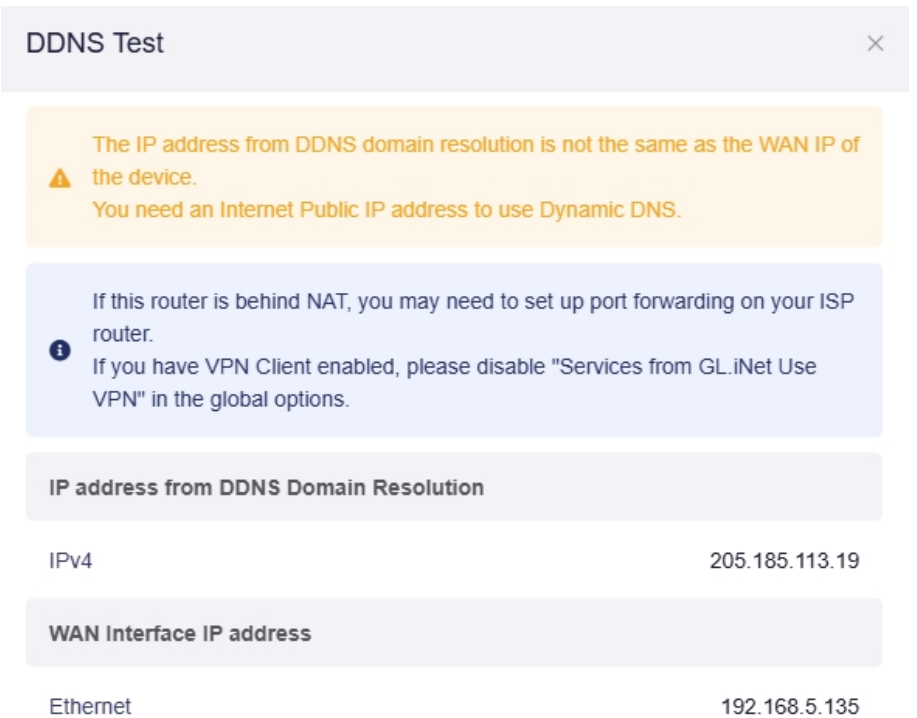
Puede comprobar si DDNS funciona utilizando la herramienta de prueba de DDNS o manualmente mediante comandos.

Método 1. Use Herramienta de prueba DDNS

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



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



Método 2. Usar comandos

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



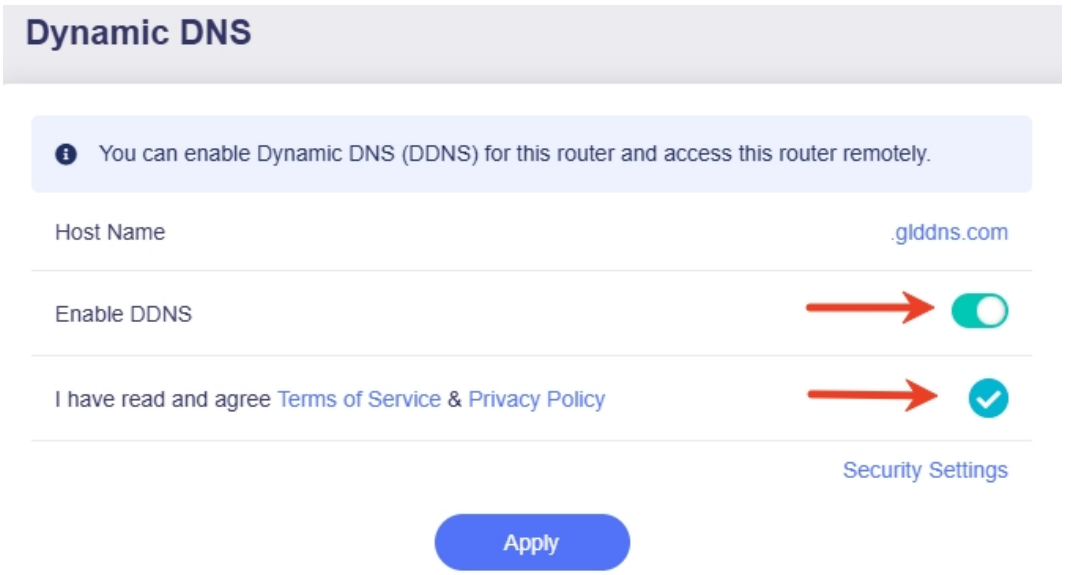
   - Reemplace “xxxxxxx.glddns.com” en la imagen de arriba con su nombre de host.
   - El “8.8.8.8” es el DNS de Google. Uconsúltelo o reemplácelo con otros, luego presione Entrar.
2. Si obtiene una dirección IP pública como “183.178.10.100” en la imagen de arriba, indica que su DDNS El dominio se ha asignado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

14.2.3 Acceso remoto HTTPS

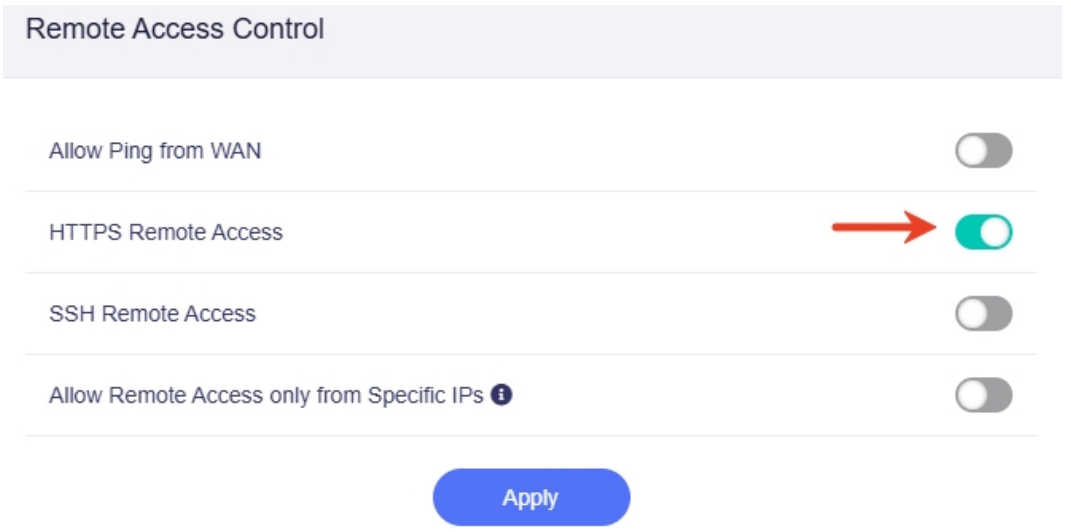
Se requiere una **Dirección IP pública** para el acceso remoto HTTPS.Consulte aquí parapara verificar si su ISP le asigna una dirección IP pública. Si su enrutador está detrás de NAT, configure el reenvío de puertos (**puerto 443**) en el enrutador ascendente para acceso HTTPS.

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

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

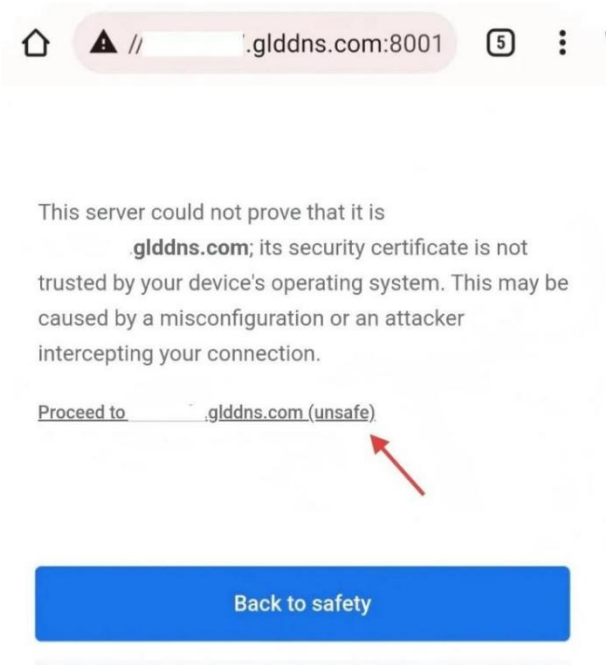


2. En el panel de administración web, vaya a **SISTEMA** > **Seguridad** > **Control de acceso remoto**. Habilite **Acceso remoto HTTPS** y haga clic en **Aplicar**.



3. Una vez habilitado, puede acceder al panel de administración del enrutador' 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.



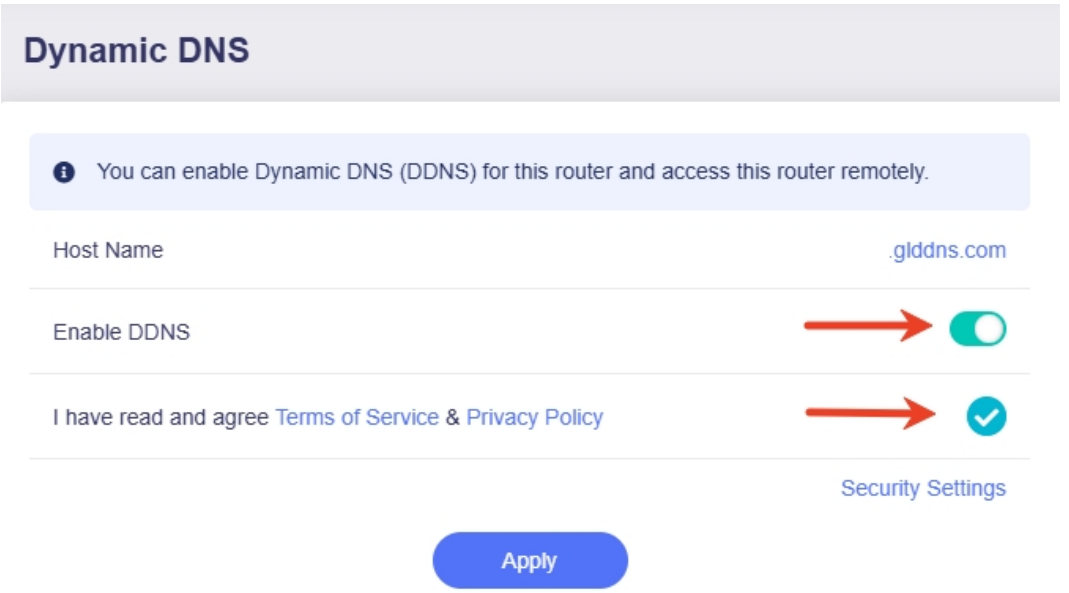
Luego podrá acceder al enrutador's panel de administración web usando el DDNS host nombre sobre **HTTPS**.

14.2.4 Acceso remoto SSH

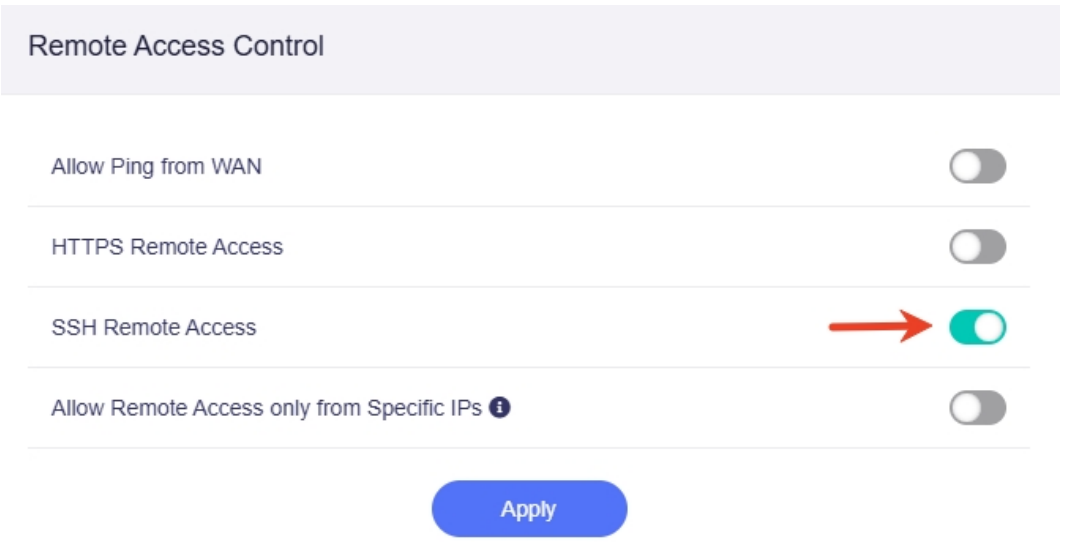
A **Dirección IP pública** es necesario para SSH acceso remoto. Consulte aquí tpara verificar si su ISP le asigna una dirección IP pública. Si su enrutador está detrás de NAT, configure el reenvío de puertos (**puerto 22**) en el enrutador ascendente para SSH acceso remoto.

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

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



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



Una vez habilitado, podrá acceder al enrutador’s panel de administración desde cualquier lugar usando 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).

14.3 Almacenamiento en red

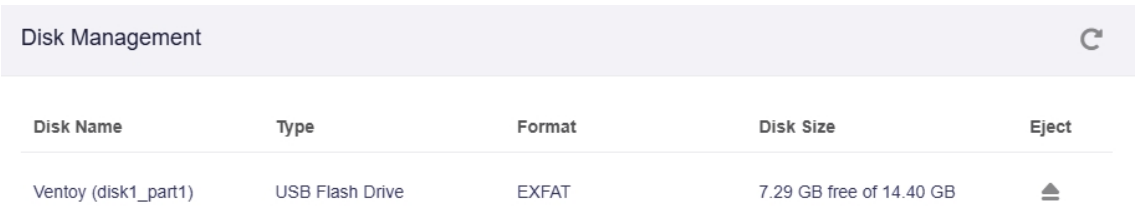
El almacenamiento en red permite compartir archivos de forma inalámbrica entre dispositivos conectando una unidad USB flash o una tarjeta SD a su enrutador. El enrutador convierte el medio de almacenamiento en una red compartido accesible a todos los dispositivos conectados a Wi-Fi-.

Opal está equipado con un puerto USB, compatible con unidades flash USB y discos duros externos portátiles. Puede configurar Samba para estos dispositivos de almacenamiento, que admiten 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.

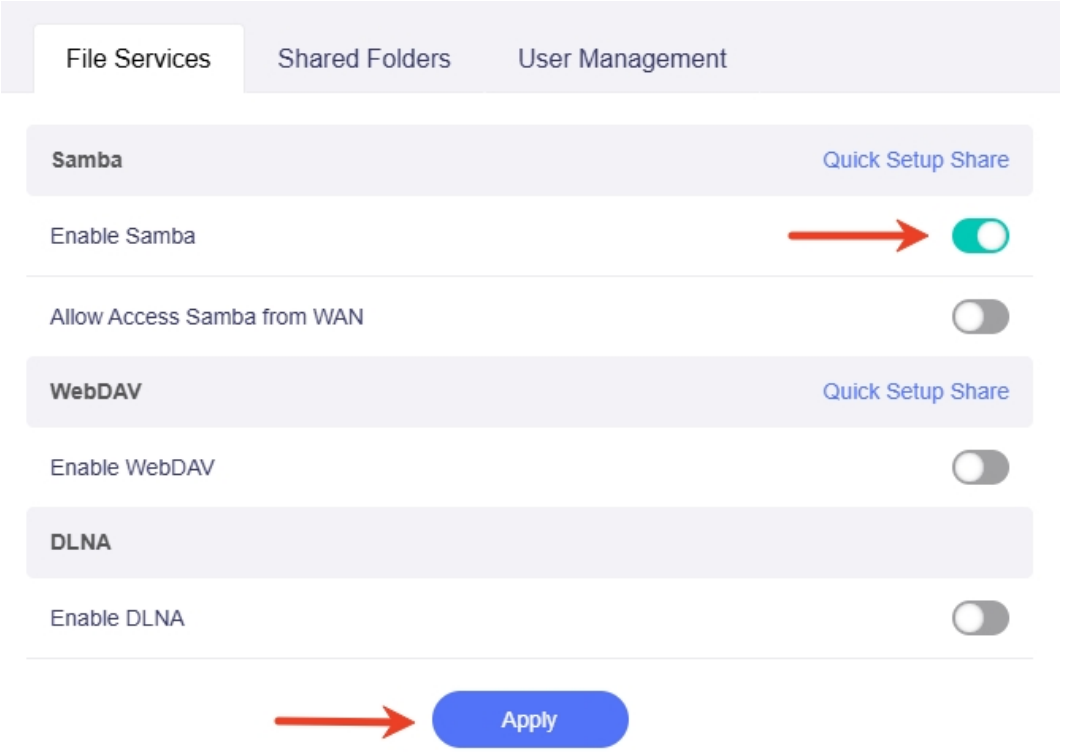
14.3.1 Conectar una unidad de almacenamiento

1. Conecte su dispositivo de almacenamiento al enrutador.
   - Para una unidad USB: conéctela directamente al puerto USB.
   - Para un disco duro externo: conéctelo a una fuente de alimentación separada (si es necesario) y luego conéctelo al enrutador.
2. Registro en a 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.



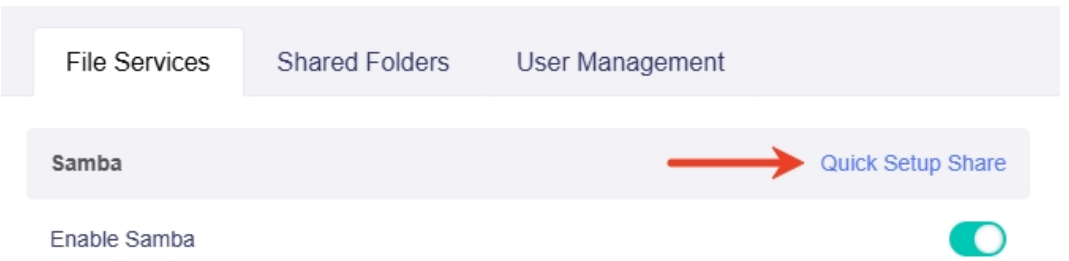
14.3.2 Configurar Samba

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

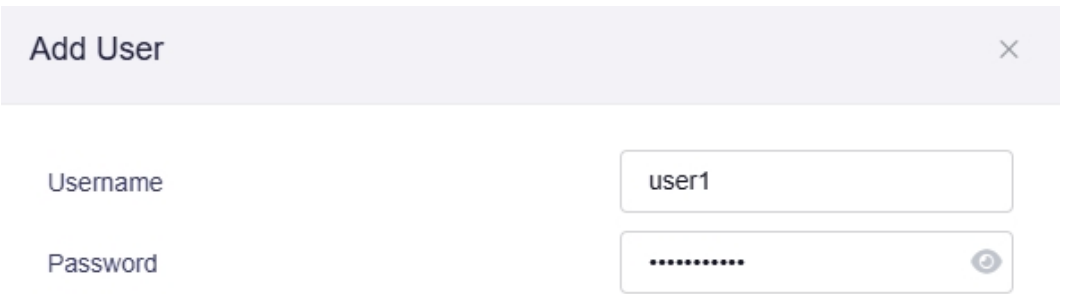


- **Permitir acceso a Samba desde WAN**: habilitar it si desea que los dispositivos ascendentes accedan al servicio Samba.

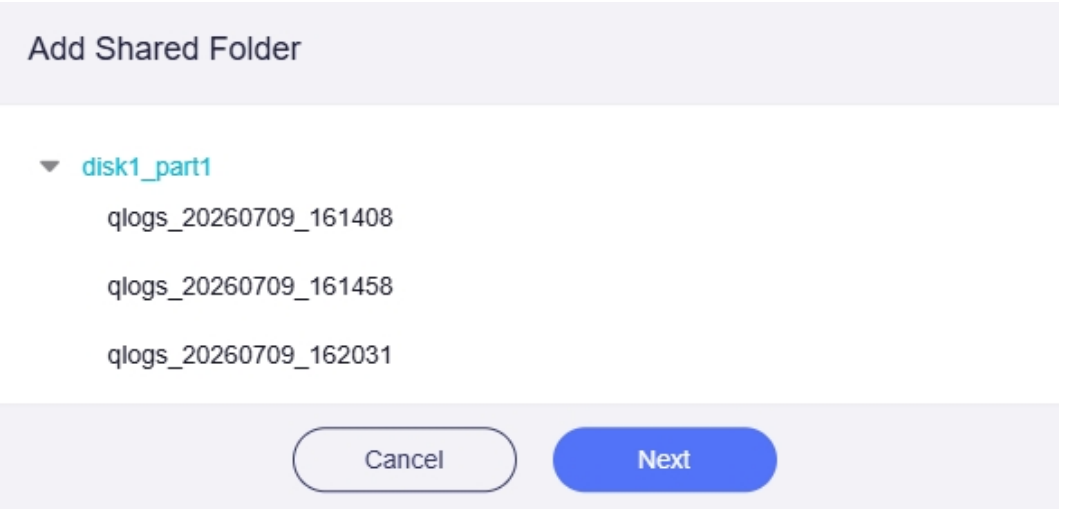
2. Haga clic en **Configuración rápida Compartir** para establecer enlace compartido.



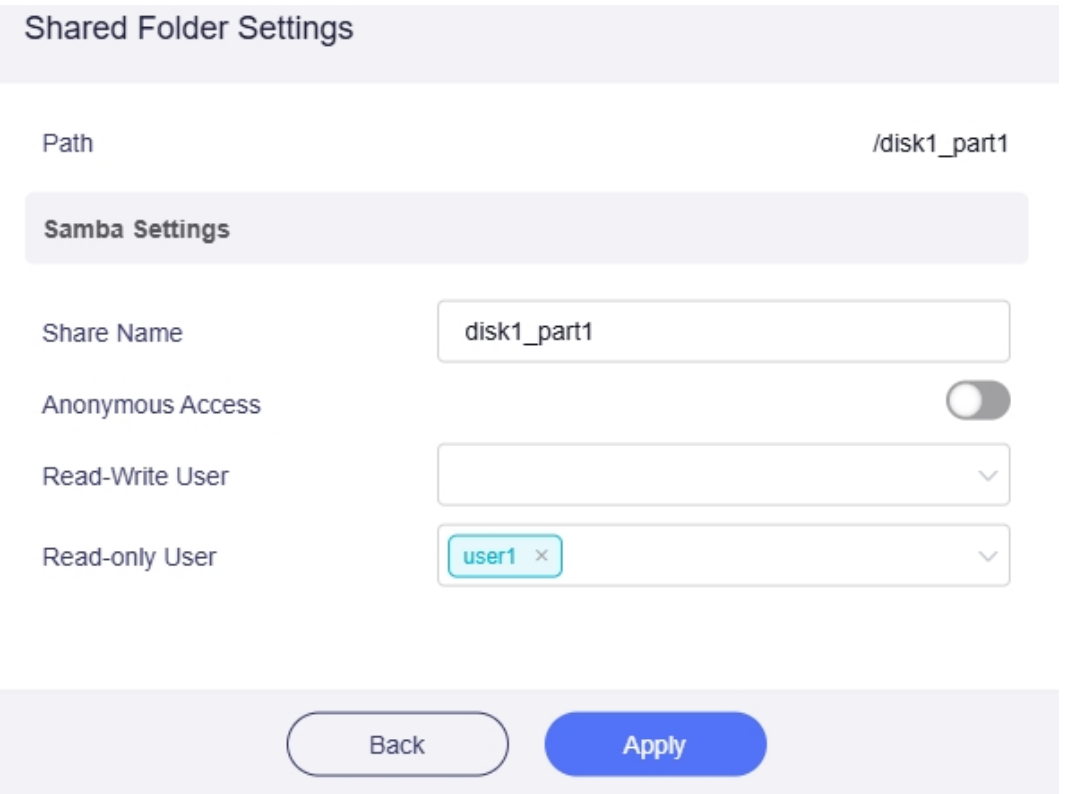
3. Agregue un usuario y haga clic en **Siguiente**. Este paso se omitirá si ya tiene una cuenta.



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

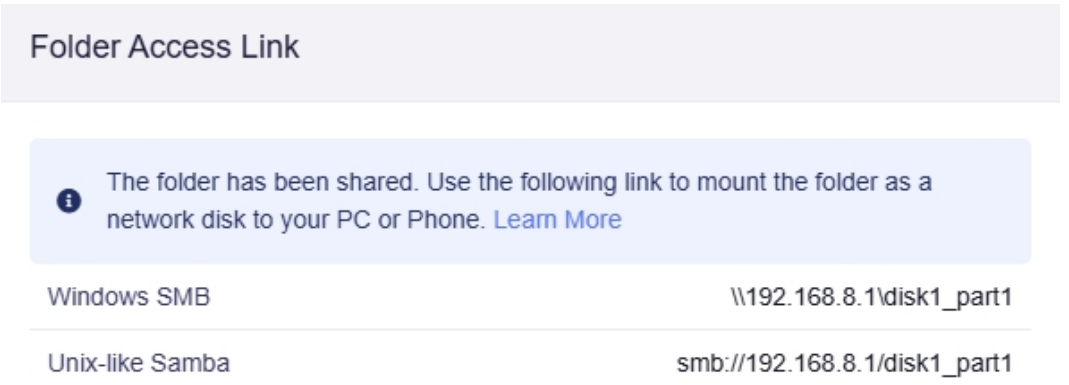


5. Configura la carpeta compartida.
   El usuario creado en el paso anterior se agregará a **Usuario de solo lectura** de forma predeterminada. Si desea que este usuario pueda escribir o eliminar archivos, eliminarlo desde Usuario de solo lectura y agréguelo a **Lectura-Escritura Usuario**, luegoluego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



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

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



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

Capítulo 15

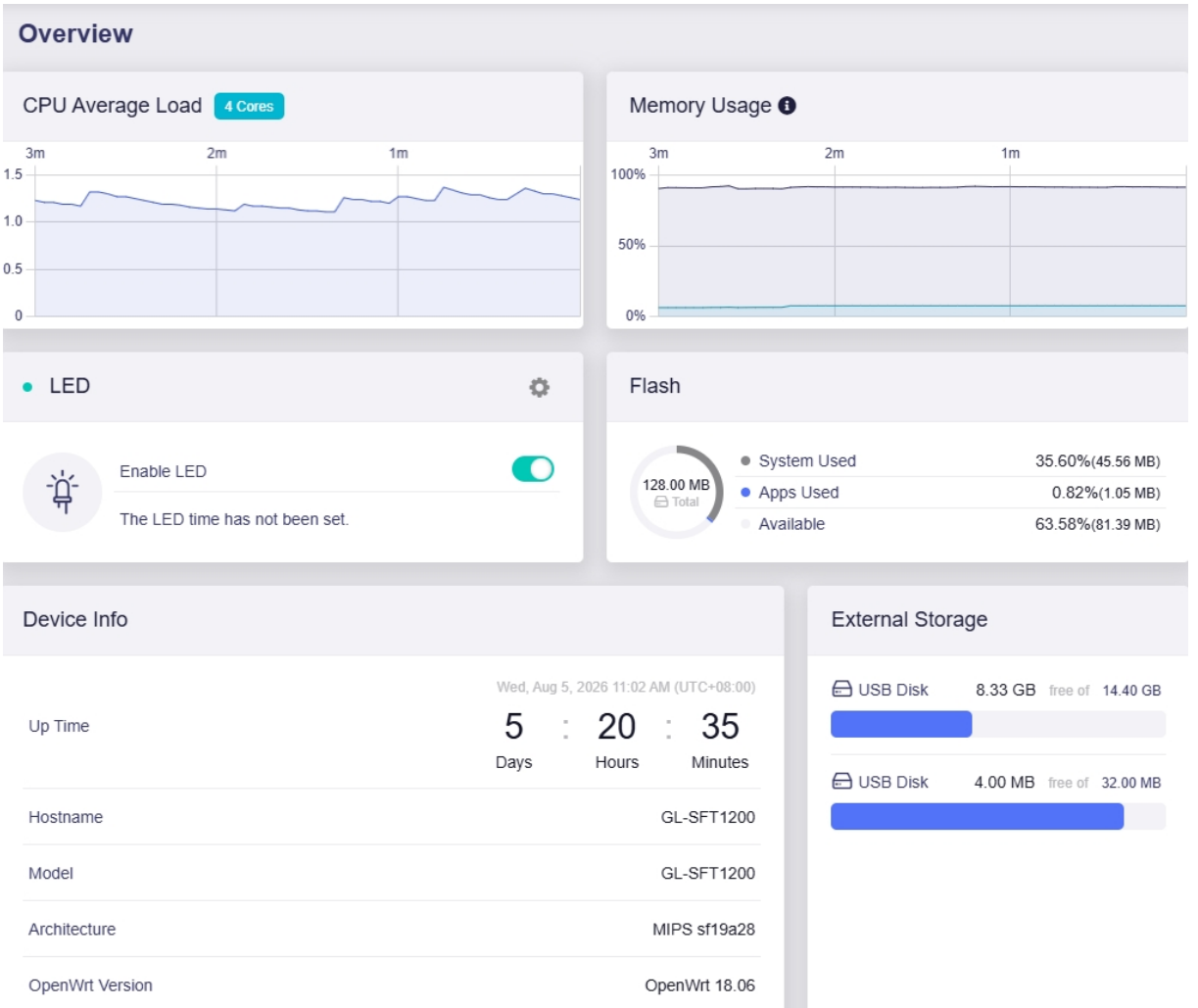
Sistema

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

15.1 Descripción general

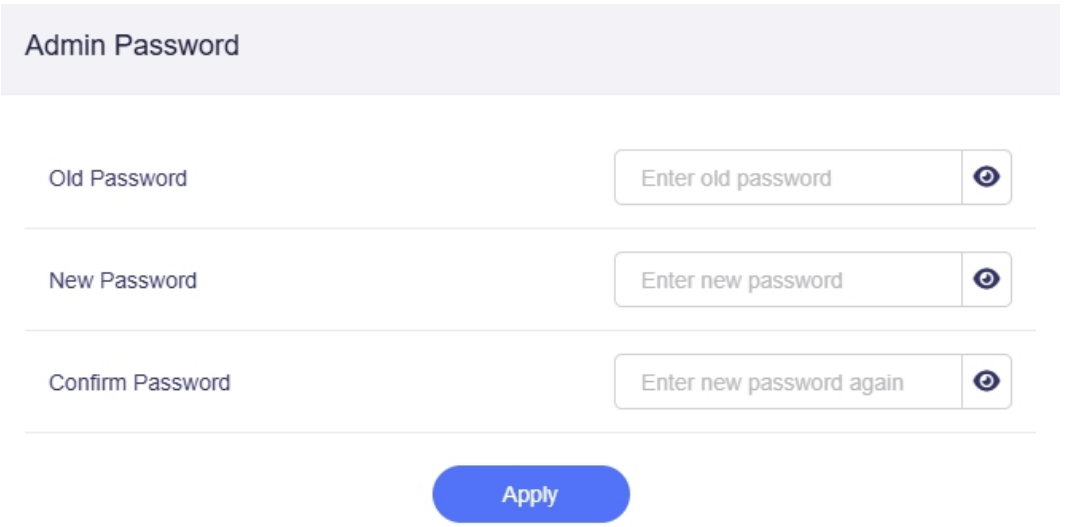
Inicie sesión en el panel de administración web de su enrutador' y navegue hasta **SISTEMA** > **Descripción general**. Esta página muestra estado del hardware y admite algunos controles simples, que incluyen:

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



15.2 Contraseña de administrador

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



Los requisitos para la contraseña de administrador son los siguientes:

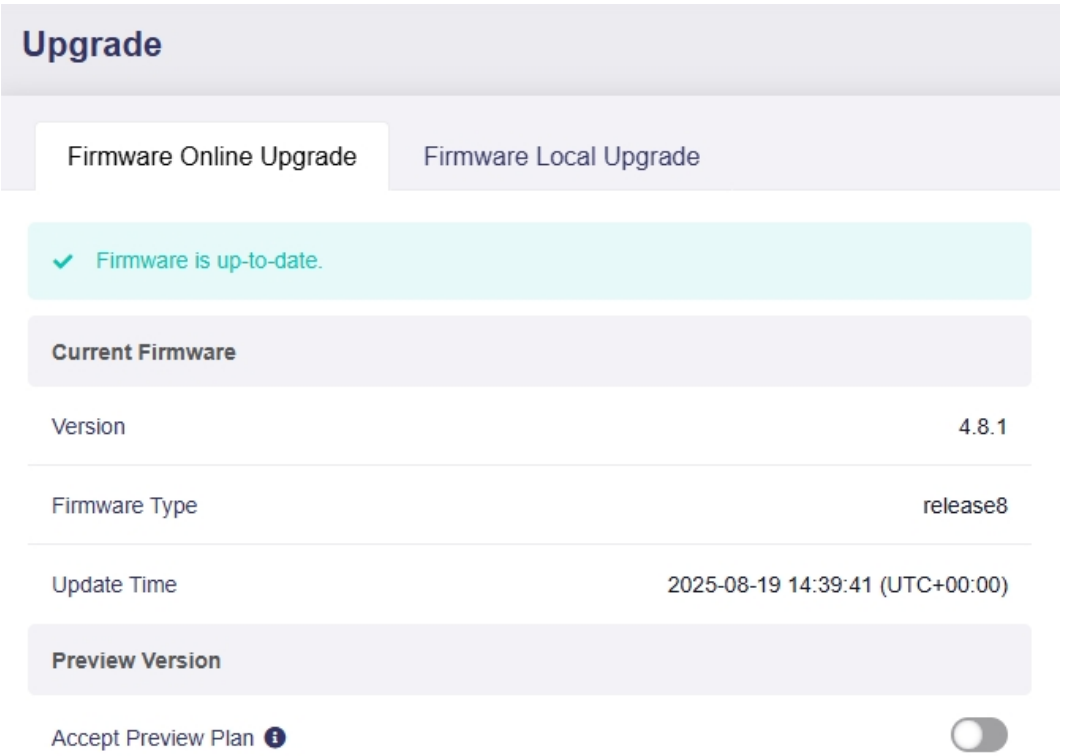
1. Mínimo 10 caracteres y máximo 63 caracteres de longitud.
2. Letras (distingue entre mayúsculas y minúsculas), números y símbolos (por ejemplo, ! @ # $ % ^ & * ( ) _ + - = , . > < | ? / \ [ ] { } : ; " ' ` ~) son necesarios.
3. Se requieren al menos dos tipos (letras mayúsculas, minúsculas, números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

15.3 Actualización

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

15.3.1 Actualización en línea

Puede encontrar el firmware actual detalles aquí, incluida la versión de firmware, el tipo de firmware (por ejemplo, versión, beta) y el tiempo de actualización. Si su enrutador está conectado a Internet, buscará la versión de firmware más reciente disponible para descargar.

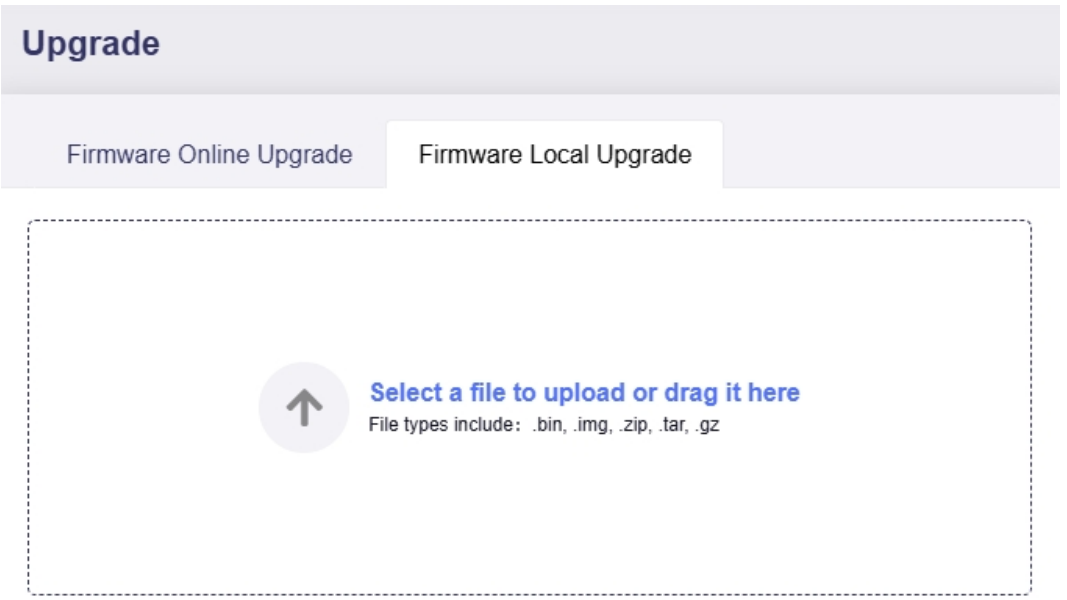


- **Aceptar plan de vista previa**: esta opción se muestra aleatoriamente según el modelo y el firmware. Si está habilitado, puede probar nuevas funciones antes de que se publique la versión final y enviarnos sus comentarios. Configúrelo una vez y permanecerá encendido. Tenga en cuenta que estas actualizaciones pueden no ser estables.

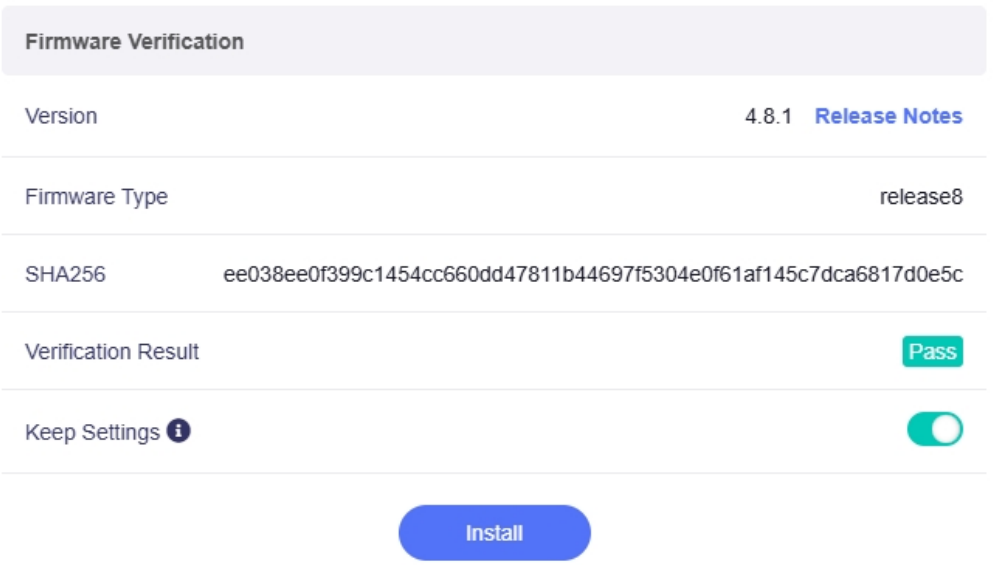
Consejo: Al intentar realizar una actualización en línea, si muestra **Descarga fallida**, navegue hasta **SISTEMA** -> **Zona horaria** y solucione el error de zona horaria (sincronización con el navegador).

15.3.2 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.

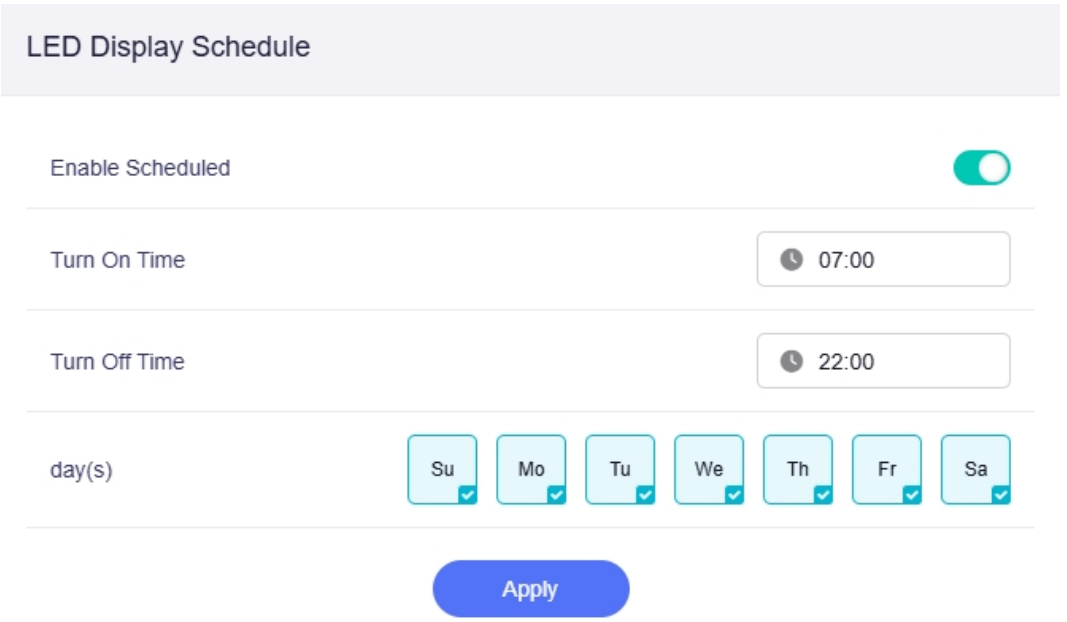
15.4 Tareas programadas

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

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

15.4.1 Programación de los indicadores LED

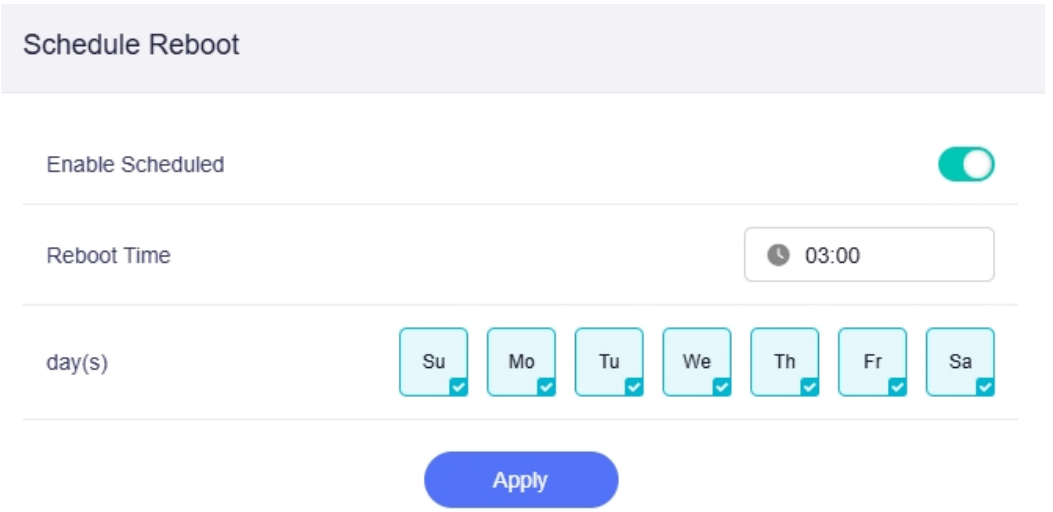
SEstablezca un programa para la luz LED de su enrutador si es necesario, luego haga clic **Aplicar**.



- **Habilitar programado**: cambie este interruptor a habilitar el LED programación de visualización.
- **hora de encendido**: establezca la hora (por ejemplo, 07:00) en la que se enciende el LED se encenderá.
- **Hora de apagado**: establezca la hora (por ejemplo, 22:00) en la que la luz LED se apagará.
- **día(s)**: Seleccione los días efectivos de la semana para estas configuraciones.

15.4.2 Programar reinicio

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



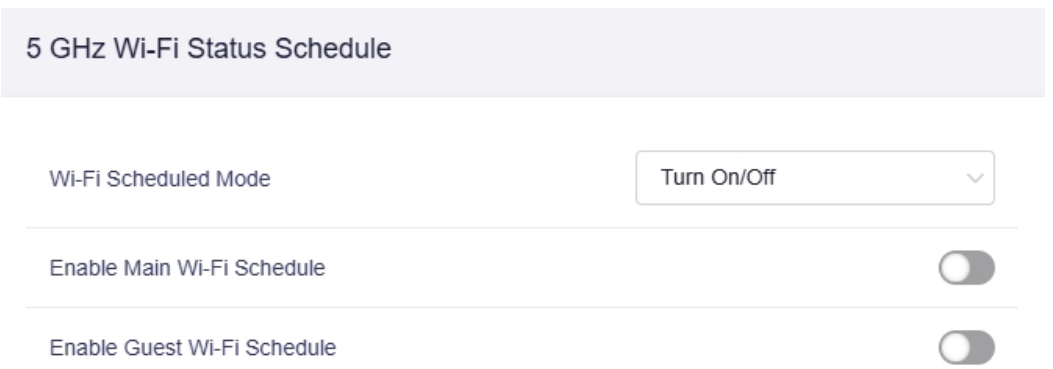
- **Habilitar programado**: active este interruptor para habilitar el reinicio programado.
- **Reiniciar Hora**: establezca la hora específica (por ejemplo, 03:00) en la que se reiniciará el enrutador.
- **día(s)**: Seleccione los días efectivos de la semana para esta configuración.

15.4.3 Programación de Wi-Fi de 5 GHz

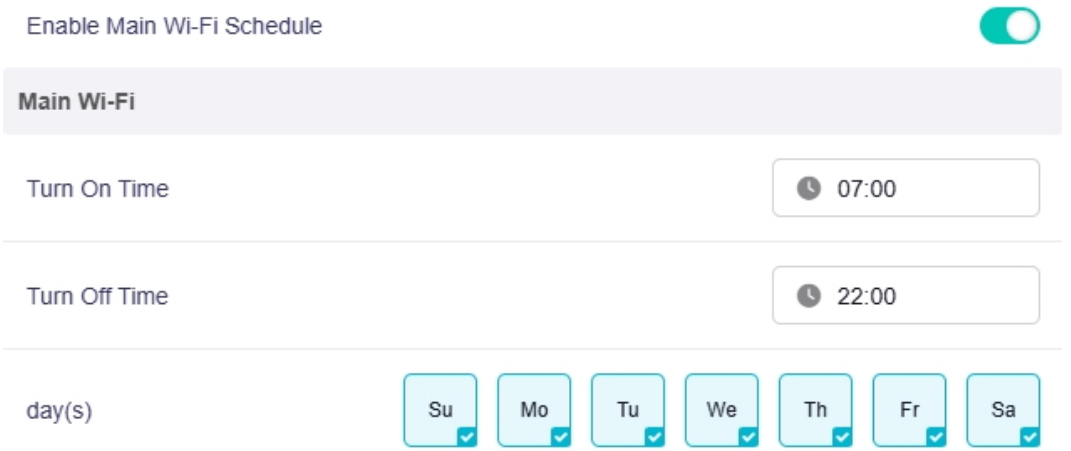
Esta función le permite establecer una programación para su Wi-Fi de 5 GHz. Hay dos modos: encender/apagar y cambiar la alimentación de TX.

Modo 1: Encender/apagar

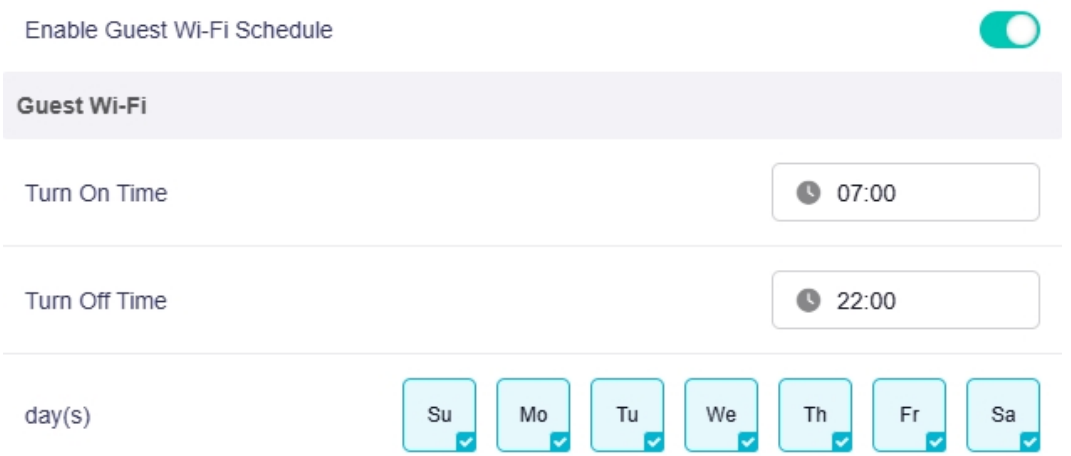
Puedes habilitar el horario de encendido/apagado tanto para Wi-Fi principal de 5 GHz como para Wi-Fi para invitados.



- **Programa de Wi-Fi principal**: Cuando esté habilitado, configura los horarios de encendido y apagado para tu Wi-Fi principal de 5 GHz y selecciona una fecha efectiva para la semana.

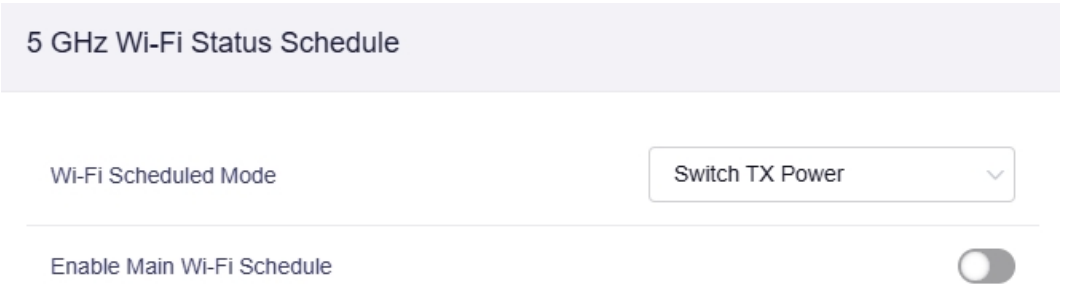


- **Programación de Wi-Fi para invitados**: cuando esté habilitado, configure los horarios de encendido y apagado de su Wi-Fi para invitados de 5 GHz y seleccione una fecha efectiva para la semana.

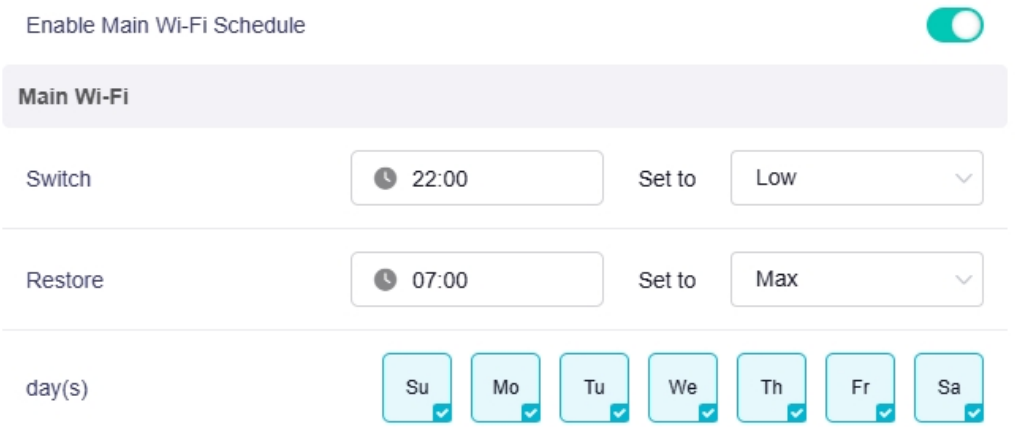


Modo 2: cambiar la alimentación de TX

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



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



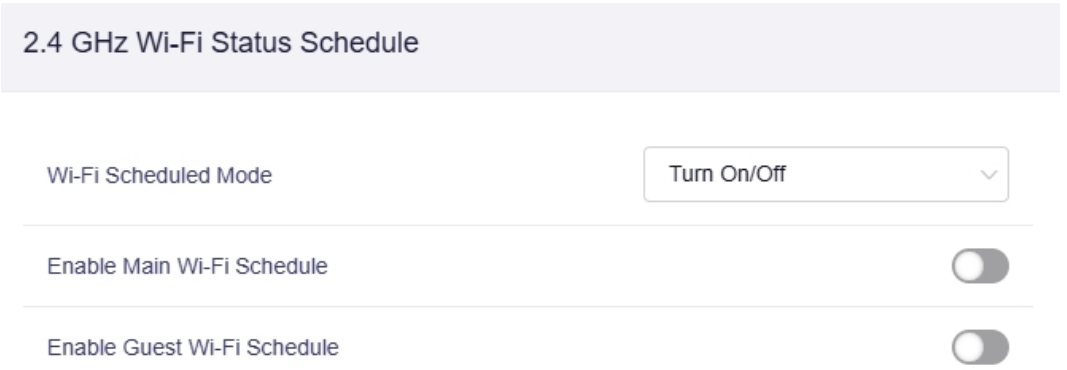
- **Cambiar**: Set TX Power a un cierto nivel (por ejemplo, bajo) aen un momento específico (por ejemplo, 22:00).
- **Restaurar**: Rrestaurar la energía de TX a unotro nivel (por ejemplo, máximo) unen otro momento (por ejemplo, 07:00).
- **días**: Seleccione los días efectivos de la semana para esta configuración.

15.4.4 Programación de Wi-Fi de 2,4 GHz

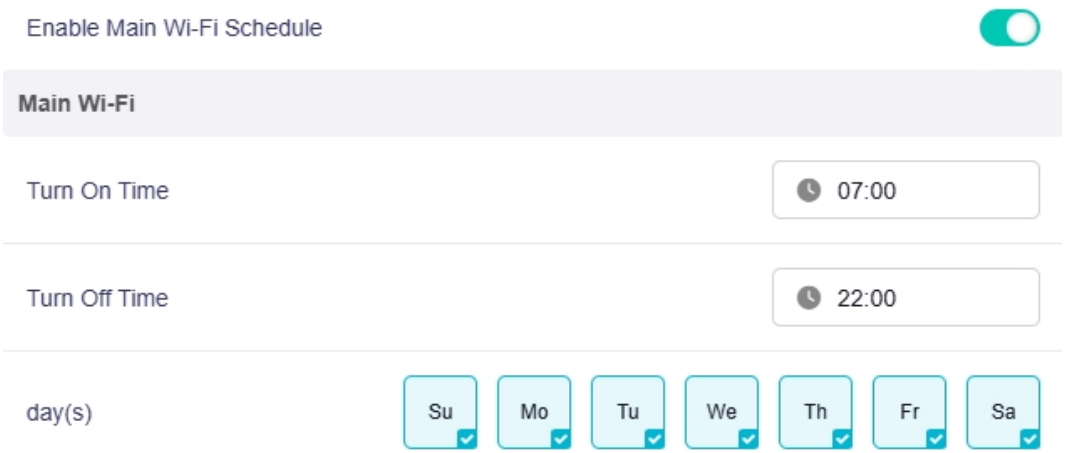
Esta función le permite establecer un horario para su Wi-Fi de 2,4 GHz. Hay dos modos: encender/apagar y cambiar la alimentación de TX.

Modo 1: Encender/apagar

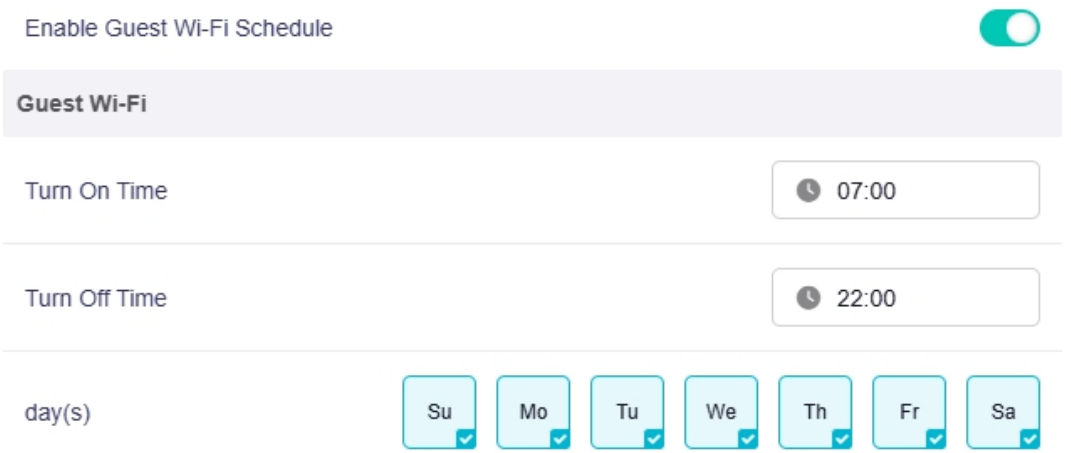
Puede habilitar el horario de encendido/apagado tanto para el Wi-Fi principal de 2,4 GHz como para el Wi-Fi para invitados.



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

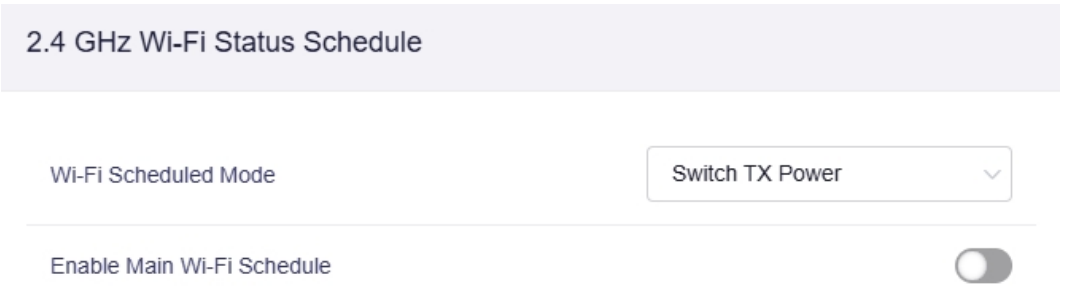


- **Programa de Wi-Fi para invitados**: cuando esté habilitado, configure los horarios de encendido y apagado para su Wi-Fi para invitados de 2,4 GHz y seleccione una fecha efectiva para el semana.

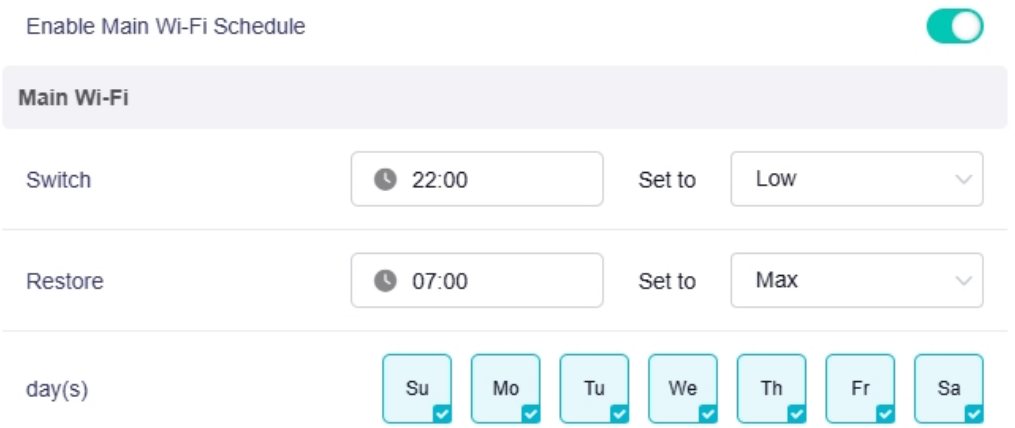


Modo 2: Cambiar alimentación de TX

Ypuede habilitar el cambio de alimentación de TX programación para el Wi-F principal de 2,4 GHzi.



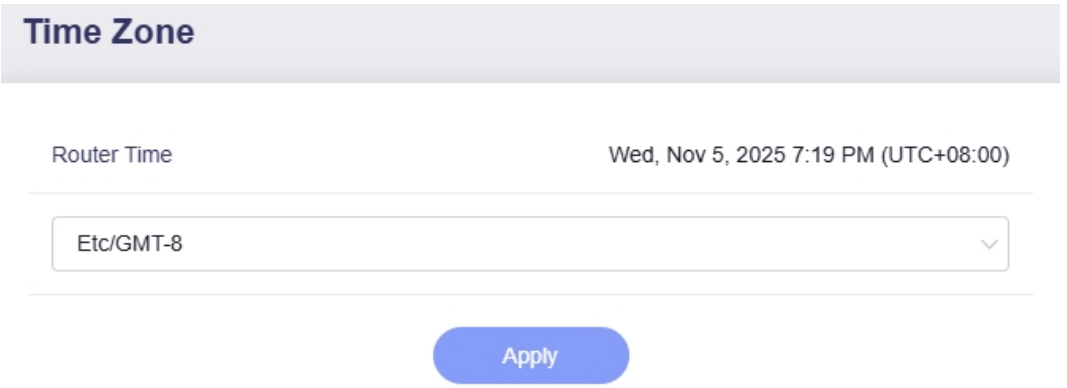
Cuando esté habilitado, configure dos acciones cronometradas para que su Wi-Fi principal de 2,4 GHz cambie la potencia de transmisión y seleccione una frecuencia efectiva. fecha de la semana.



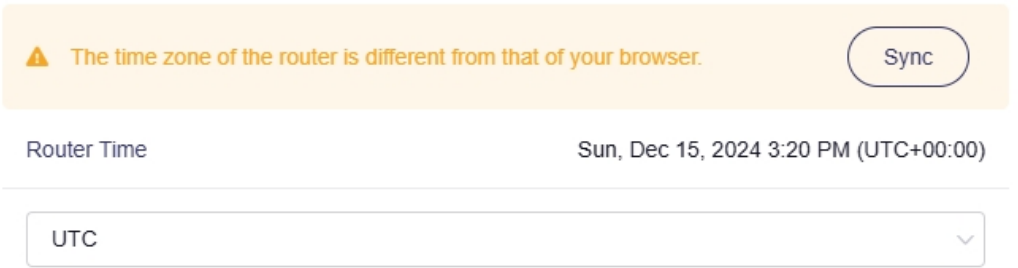
- **Cambiar**: Sajuste la potencia de TX a un cierto nivel (por ejemplo, bajo) enen un momento específico (p. ej., 22:00).
- **Restaurar**: Rrestaurar la energía de TX en unotro nivel (p. ej., Max) aen otro momento (por ejemplo, 07:00).
- **días**: Seleccione los días efectivos de la semana para esta configuración.

15.5 Zona horaria

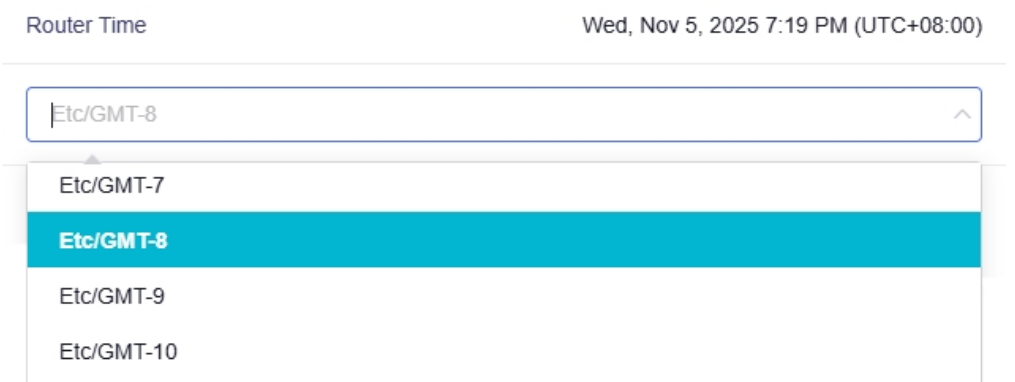
Inicie sesión en el panel de administración web de su enrutador y navegue hasta **SISTEMA** > **Zona horaria**. Esta página muestra la la hora del sistema, indicando la fecha, la hora y el desplazamiento de zona horaria correspondiente.



Algunas funciones dependen del tiempo del sistema del enrutador’para surtir efecto. 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 ’es diferente a la de su navegador, se mostrará un mensaje de la siguiente manera. Haga clic en **Sincronizar** para sincronizar la zona horaria.

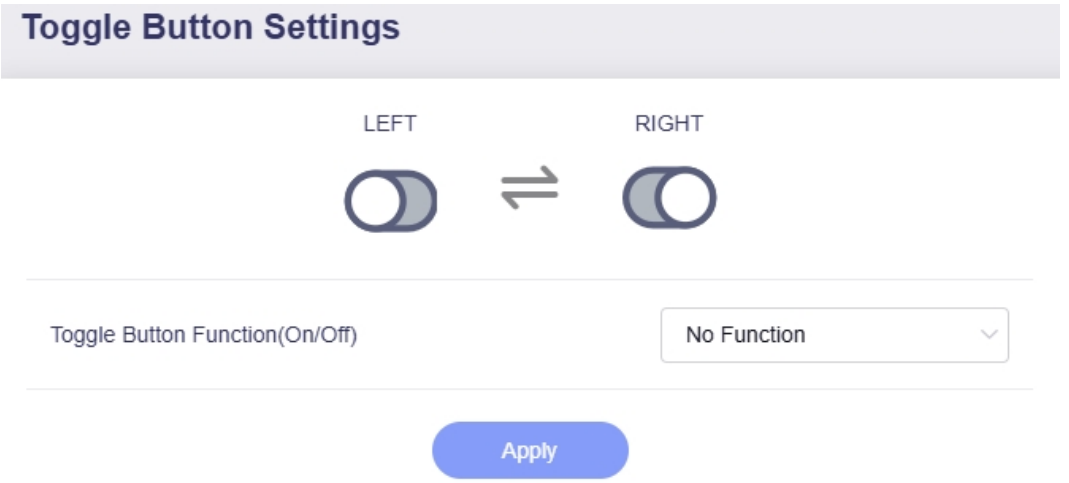


Para cambiar zona horaria, sseleccione la zona horaria apropiada de la lista para asegúrese de que la hora del sistema coincida con su hora local.

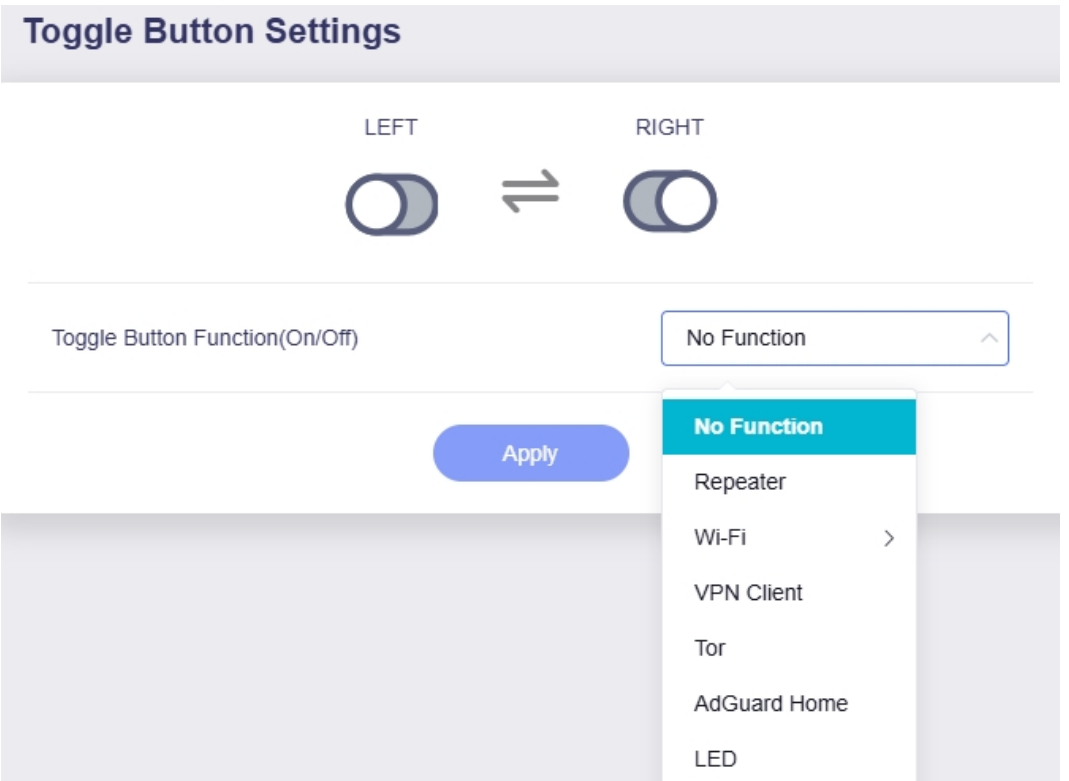


15.6 Configuración del botón de alternancia

Inicie sesión en el panel de administración web de su enrutador y navegue hasta **SISTEMA -> Configuración del botón de alternancia**. Esta página le permite personalizar la función de conmutación física del enrutador. interruptor (ubicado en el costado) para un uso más fácil.



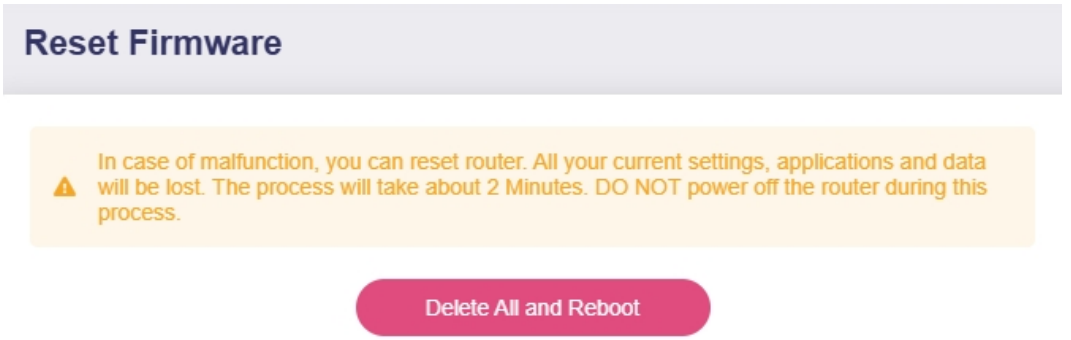
De forma predeterminada, al interruptor de palanca no se le asigna ninguna función. Puede personalizarlo si es necesario para activar o desactivar funciones específicas con un solo movimiento.



15.7 Restablecer firmware

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

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

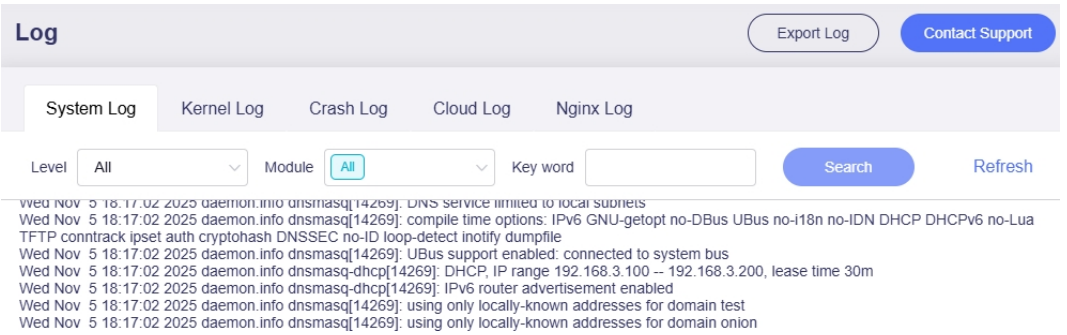


Nota: todas sus configuraciones, aplicaciones y datos actuales se borrado. El proceso durará unos 2 minutos. Nono apague el enrutador durante este proceso.

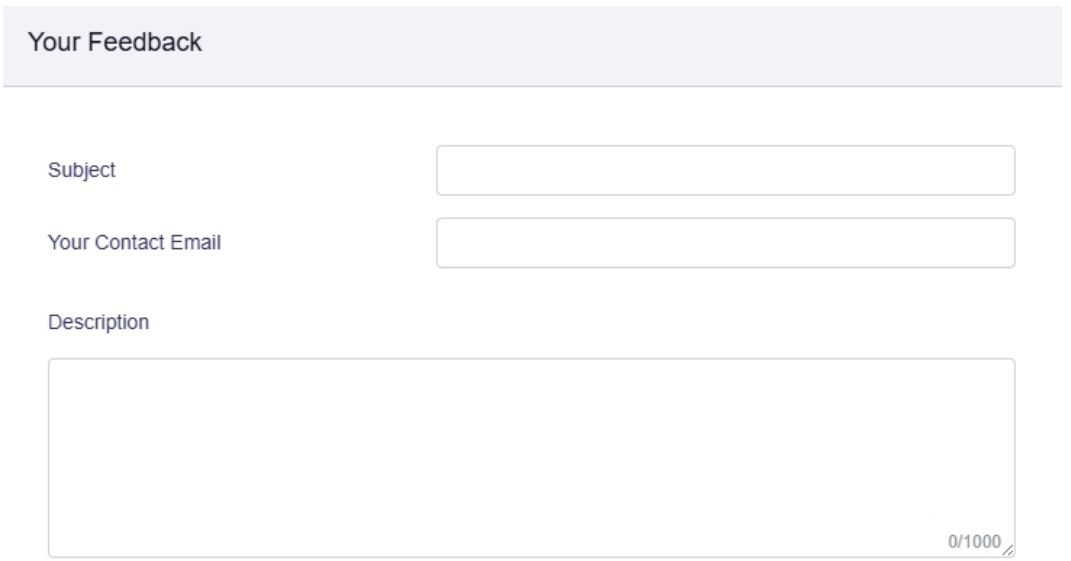
Si no puede acceder al panel de administración web del enrutador', intente restablecer su enrutador usando el botón de reinicio físico en el costado.

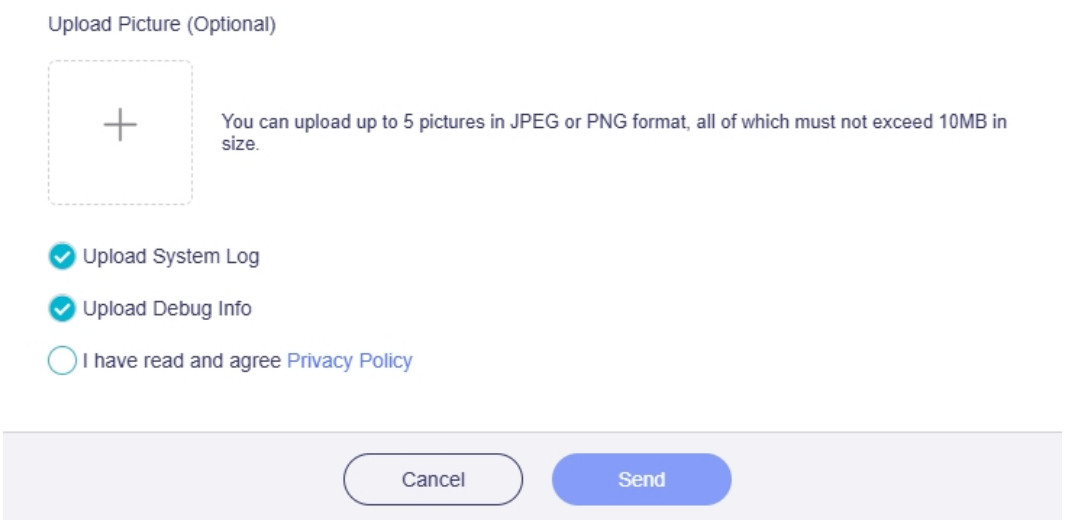
15.8 Registro

Inicie sesión en el panel de administración web de su enrutador y navegue hasta **SISTEMA** > **Registro**. Esta página le permite ver registros del sistema, kernel, bloqueo, nube y Nginx para análisis y solución de problemas.



- **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.



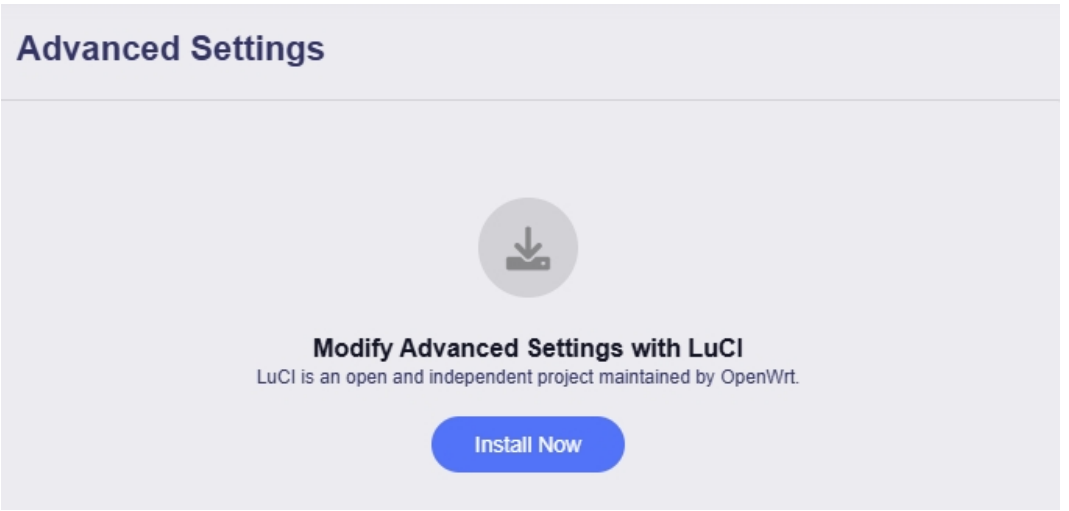

Upload Picture (Optional)
You can upload up to 5 pictures in JPEG or PNG format, all of which must not exceed 10MB in size.
Upload System Log
Upload Debug Info
I have read and agree Privacy Policy
Cancel
Send

15.9 Configuración avanzada

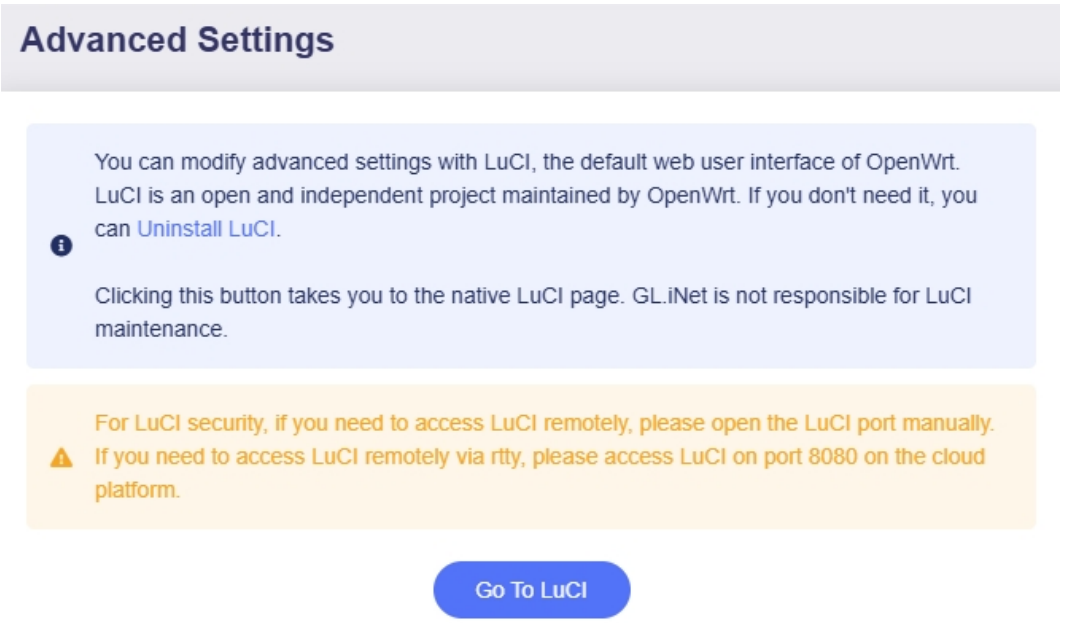
Inicie sesión en el panel de administración web de su enrutador y navegue hasta **SISTEMA** > **Configuración avanzada**. Esta página le permitemodificar la configuración avanzada modificar configuración avanzada en LuCI, que es la interfaz de usuario web predeterminada de OpenWrt. Como proyecto abierto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

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

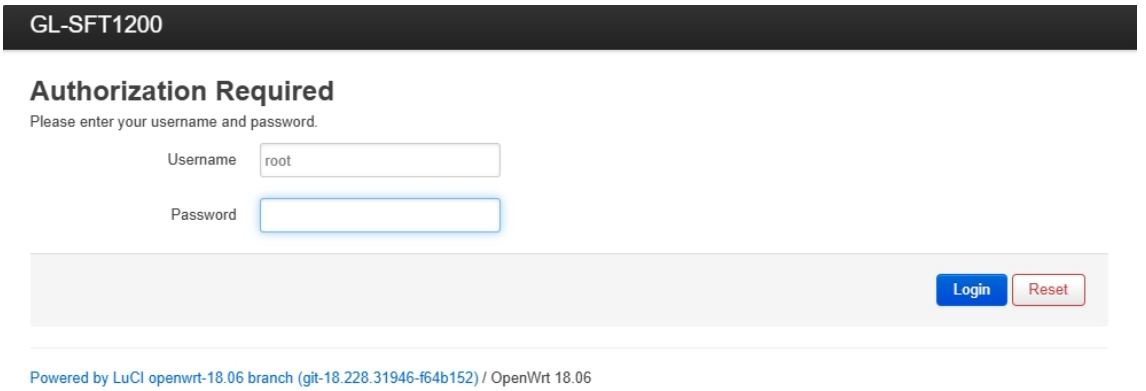
1. Haga clic en **Instalar ahora**, y se instalará la interfaz LuCI.



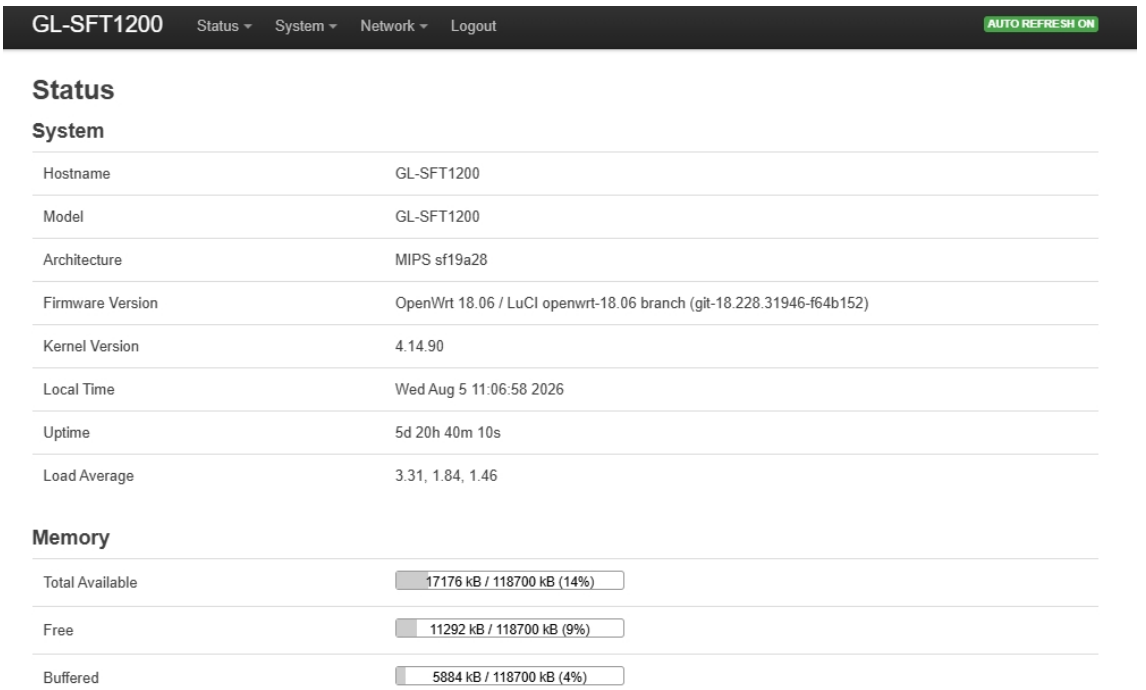
2. Click **Vaya a LuCI**, y será redirigido a la página de inicio de sesión de LuCI.



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



Ylo hará luego registrar en a la interfaz LuCI .



Declaración de Conformidad

Por la presente, GL TECHNOLOGIES (HONG KONG) LIMITED declara que el tipo de equipo de radio [AC1200 Wireless Travel Router, GL-SFT1200] cumple con 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/