GL·iNet



Manual de usuario

GL-E750/GL-E750V2 Mudi

Enrutador de viaje 4G LTE

Versión de firmware 4.3.26

Acerca de este manual

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

Con esta guía, podrá:

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

Convenciones de formato

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

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

Nota:

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

¿Necesita más ayuda o información?

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

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

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

Contenido

Capítulo 1 Conozca su enrutador 8

1.1 Descripción general del producto 9

1.1.1 Apariencia 9

1.1.2 Interfaz y botón 10

1.2 Especificaciones 12

1.3 Bandas de frecuencia 13

1.4 Contenido del paquete 14

Capítulo 2 Conexión de hardware 15

2.1 Elección de una ubicación 16

2.2 Conexión del enrutador 16

Capítulo 3 Iniciar sesión en el enrutador 18

Capítulo 4 Configurar la conexión a Internet 20

4.1 Conectarse a Internet mediante la red móvil 22

4.1.1 Configuración básica 23

4.1.2 Configuración manual 25

4.1.3 Configuración del módem 28

4.2 Conectarse a Internet mediante un cable Ethernet 30

4.2.1 Configuración básica 30

4.2.2 Protocolo 32

4.3 Conectarse a Internet mediante una red Wi-Fi existente 34

4.3.1 Configuración básica 35

4.3.2 Opciones de repetidor 38

4.4 Conectarse a Internet mediante conexión compartida por USB 39

4.4.1 Conexión compartida desde un iPhone 39

4.4.2 Conexión compartida desde Android 41

4.4.3 Solución de problemas 42

Capítulo 5 Red inalámbrica 43

5.1 Wi-Fi de 5 GHz 44

5.2 Wi-Fi de 2,4 GHz 46

Capítulo 6 Clientes 48

6.1 Detalles del dispositivo 50

6.2 Acción 52

6.3 Eliminar clientes 54
6.4 Ordenar 55
Capítulo 7 Conozca la VPN 56
7.1 Introducción 57
7.2 Escenarios de aplicación 58
Capítulo 8 Panel de VPN 60
8.1 Cliente VPN 61
8.1.1 Opciones del cliente 62
8.1.2 Modo de política 64
8.1.3 Opciones globales 66
8.2 Servidor VPN 69
8.2.1 Opciones del servidor 70
8.2.2 Regla de ruta del servidor 71
8.2.3 Opciones globales 73
Capítulo 9 Configurar el servidor VPN 74
9.1 Configurar el servidor OpenVPN 75
9.1.1 Preparación 75
9.1.2 Pasos de configuración 76
9.1.3 Solución de problemas 78
9.2 Configurar el servidor WireGuard 80
9.2.1 Preparación 80
9.2.2 Pasos de configuración 81
9.2.3 Solución de problemas 84
Capítulo 10 Configurar el cliente VPN 85
10.1 Configurar el cliente OpenVPN 86
10.1.1 Preparación 86
10.1.2 Configurar NordVPN 86
10.1.3 Configurar el cliente OpenVPN manualmente (para otros proveedores) 92
10.2 Configurar el cliente WireGuard 95
10.2.1 Preparación 95
10.2.2 Configurar AzireVPN 96
10.2.3 Configurar Mullvad 99
10.2.4 Configurar el cliente WireGuard manualmente (para otros proveedores) ... 103
Capítulo 11 Tor 107

Capítulo 12 Aplicaciones 109
12.1 Complementos 110
12.2 DNS dinámico 111
12.2.1 Habilitar DDNS 111
12.2.2 Comprobar si DDNS funciona 113
12.2.3 Acceso remoto HTTP 115
12.2.4 Acceso remoto HTTPS 116
12.2.5 Acceso remoto SSH 118
12.3 GoodCloud 119
12.3.1 Habilitar GoodCloud 119
12.3.2 Administrar el enrutador 124
12.3.3 Desvincular el dispositivo 129
Capítulo 13 Red 130
13.1 Cortafuegos 131
13.1.1 Reenvío de puertos 131
13.1.2 Abrir puertos en el enrutador 133
13.1.3 DMZ 134
13.2 Multi-WAN 135
13.2.1 Seguimiento del estado de la interfaz 135
13.2.2 Modo Multi-WAN 138
13.3 LAN 141
13.3.1 Red privada 141
13.3.2 Red de invitados 143
13.3.3 Reserva de direcciones 145
13.4 DNS 147
13.4.1 Configuración general 147
13.4.2 Configuración del servidor DNS 148
13.4.3 Editar hosts 150
13.5 Modo de red 152
13.6 IPv6 155
13.6.1 Modo IPv6 156
13.6.2 Método de obtención de DNS 156
13.7 Dirección MAC 157
13.8 Inspección IGMP 159

Capítulo 14 Sistema 160
14.1 Descripción general 161
14.2 Actualización 162
14.2.1 Actualización en línea 162
14.2.2 Actualización local 163
14.3 Configuración de pantalla OLED 165
14.4 Tareas programadas 166
14.4.1 Programación de los indicadores LED 166
14.4.2 Programar reinicio 167
14.4.3 Programación de Wi-Fi de 5 GHz 168
14.4.4 Programación de Wi-Fi de 2,4 GHz 171
14.5 Contraseña de administrador 174
14.6 Zona horaria 175
14.7 Configuración del botón de alternancia 176
14.8 Registro 177
14.9 Restablecer firmware 178
14.10 Configuración avanzada 179

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

Mudi V2 (GL-E750V2) es un enrutador de viaje portátil 4G LTE compatible con operadores globales. Se ejecuta de código completamente abierto en OpenWrt y el SDK 4.0 de GL.iNet, lo que proporciona capacidades de personalización y un conjunto de funciones. Mudi V2 (GL-E750V2) admite velocidades Wi-Fi de 300 Mbps (2,4 GHz) y 433 Mbps (5 GHz) y una tarjeta MicroSD de hasta 1 TB. Tiene una batería incorporada de 7000 mAh. También admite múltiples WAN (conmutación por error y equilibrio de carga) para garantizar una conexión fluida para todos sus dispositivos.

1.1.1 Apariencia

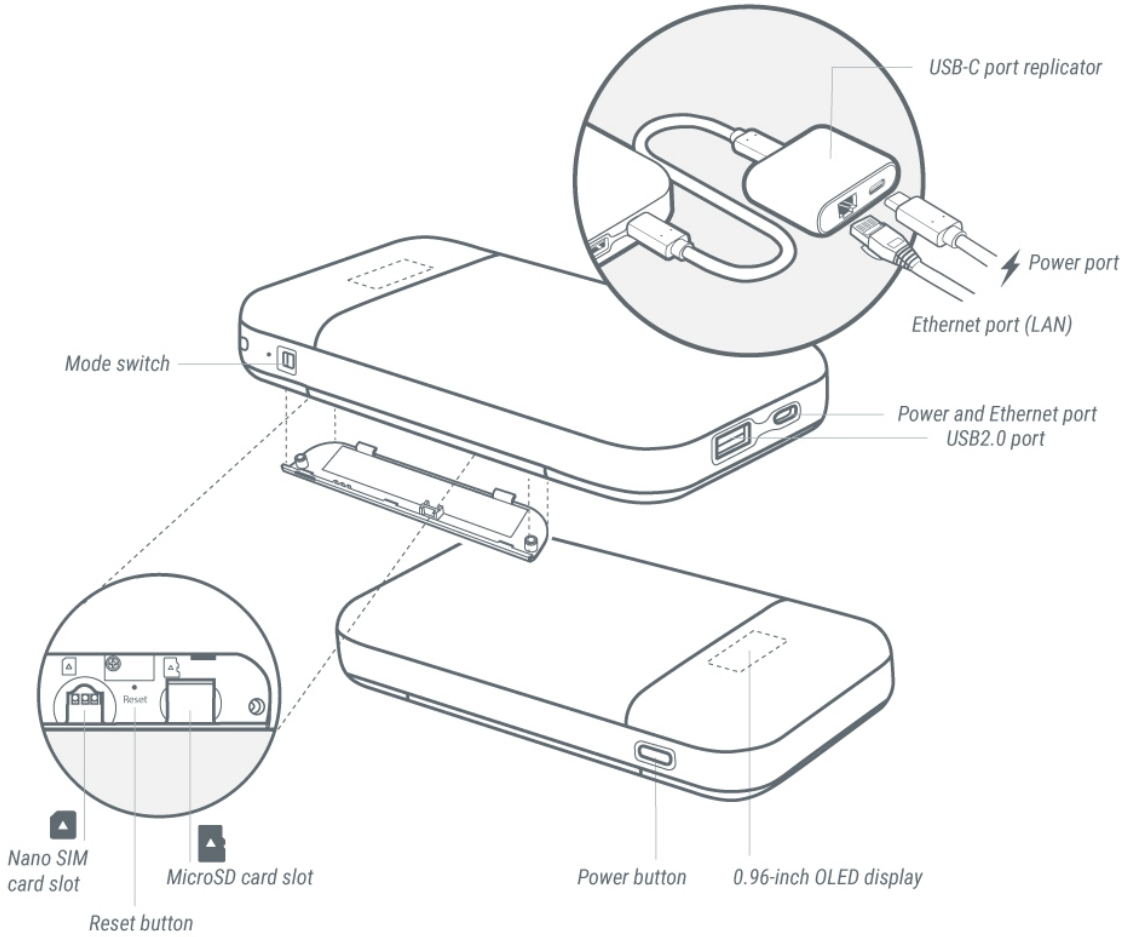








1.1.2 Interfaz y botón



Artículo	Descripción
Puerto de alimentación y Ethernet	Se conecta al adaptador de corriente.
Botón de encendido	Presione el botón de encendido durante 3 segundos: enciende el dispositivo.
	Presione el botón de encendido durante 3-5 segundos: ingrese al modo de espera.
	Presione el botón de encendido durante más de 5 segundos: apague el dispositivo.
Cambio de modo	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.

Puerto USB 2.0	Para dispositivos de almacenamiento USB, conexión USB de teléfono y dongles celulares compatibles.
Pantalla ANTIGUA de 0,96 pulgadas	Para verificaciones de estado en tiempo real y control funcional extenso.
Ranura para tarjeta Nano SIM	Para insertar una tarjeta Nano-SIM para proporcionar acceso a Internet celular a través de una red móvil 3G/4G.
Ranura para tarjeta MicroSD	Para insertar una tarjeta MicroSD para proporcionar almacenamiento expandible para acceder a archivos y guardar datos.
Botón Restablecer	Mantenga presionado durante **4 segundos** para reparar su red; Mantenga presionado durante **10 segundos** y luego suelte para restablecer el enrutador a los valores predeterminados de fábrica.

1.2 Especificaciones

Interfaz	1 x puerto USB 2.0 1 x ranura para tarjeta Nano SIM 1 x ranura para tarjeta MicroSD (hasta 1 TB) 1 x botón de alternancia 1 x botón de encendido
CPU	QCA9531, SoC de @650MHz
Memoria/Almacenamiento	DDR2 128 MB / NOR Flash 16 MB + NAND Flash 128 MB
Módem 3G/4G	Módulo CAT4 (DL/UL 150/50Mbps) o Módulo CAT6 (DL/UL 300/50Mbps)
Protocolo	IEEE 802.11/b/g/n/ac
Velocidad de Wi-Fi	300Mbps (2,4 GHz), 433 Mbps (5 GHz)
Antena LTE	2 x antenas internas de frecuencia completa (700M~2.7GHz)
Puerto Ethernet	1 x puerto FE (compatible con la estación de acoplamiento)
Entrada de energía	Tipo C, 5V/2A
Batería	Batería recargable de 7000 mAh
LED	Pantalla OLED de 0,96 pulgadas
Temperatura de funcionamiento	0 ~ 35°C (32 ~ 95°F)
Temperatura de almacenamiento	-20 ~ 45°C (-4 ~ 113°F)
Dimensión/Peso	145 x 77,5 x 23,5 mm/285 g
Otras herramientas	Hoja de datos / Firmware / Aplicación / Unboxing

*La velocidad y el alcance inalámbricos reales pueden variar según los obstáculos ambientales, la congestión de la red y las capacidades del dispositivo cliente.

1.3 Bandas de frecuencia

Bandas de frecuencia LTE Cat 6（Módulo: EM060K-G）

Modo de red	Bandas admitidas y combinaciones de CA
LTE-FDD	B1/B2/B3/B4/B5/B7/B8/B12/B13/B14/B17/B18/B19/B20/B25/B26/B28/B29②/B30/B32①/B66/B71
LTE-TDD	B34/B38/B39/B40/B41/B42/B43/B46① (LAA)/B48 (CBRS)
Hasta 2 ×CA	B2+B2/5/12/13/29③;B4+B4/5/12/13/29③; B5+B5/7/25/30/66; B7+B7/12/26;B12+B12/25/30/66; B13+B66; B25+B25/26; B30+B29; B66+B29/66; B41+B41;
WCDMA	B1/2/3/4/5/6/8/19

Nota:

①: B32 es solo para el soporte del componente secundario, B46 es solo para el soporte del componente secundario.

②: B29 es solo para portador de componentes secundarios.

③: significa que LTE-FDD B29 solo admite recepción y es solo para portador de componentes secundarios en 2×CA.

Bandas de frecuencia LTE Cat 4（Módulo: EM05-G）

Modo de red	Bandas compatibles
LTE	1/2/3/4/5/7/8/12/13/14/18/19/20/25/26/28/66/71/38/39/40/41
WCDMA	B1/2/3/4/5/6/8/19

1.4 Contenido del paquete

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

El paquete incluye:

- 1 enrutador 4G LTE portátil Mudi V2 (GL-E750V2)
- 1 x adaptador de corriente
- 4 x convertidores (enchufes de EE. UU., UE, Reino Unido y Australia)
- 1 X Manual de usuario
- 1 x Tarjeta de garantía
- 1 cable Ethernet
- 1 x replicador de puerto USB-C
- 1 cable USB-C a USB-C
- 1 cable USB-A a USB-C
- 1 x bolsa
- 1 x tarjeta de agradecimiento



Capítulo 2

Conexión de hardware

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

2.1 Elección de una ubicación

Siga estos consejos para elegir 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 cooling**: coloque el enrutador en un área fresca y bien- ventilada para una adecuada disipación del calor.
- **Ubicación central**: coloque el enrutador en un lugar donde pueda conectarse fácilmente a la alimentación y a varios dispositivos (por ejemplo, en la zona central de la sala de estar zona).
- **Cable conveniencia**: enrute los cables y el cable de alimentación de forma segura para evitar tropiezos peligros.
- **Superficie estable**: coloque el enrutador en una superficie plana y horizontal (estante, escritorio) para mayor estabilidad.
- **Evitación de EMI**: mantenga el enrutador alejado de fuentes de interferencias electromagnéticass (dispositivos Bluetooth, microondas) para minimizar la señal interferencias.

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

Capítulo 3

Iniciar sesión en el enrutador

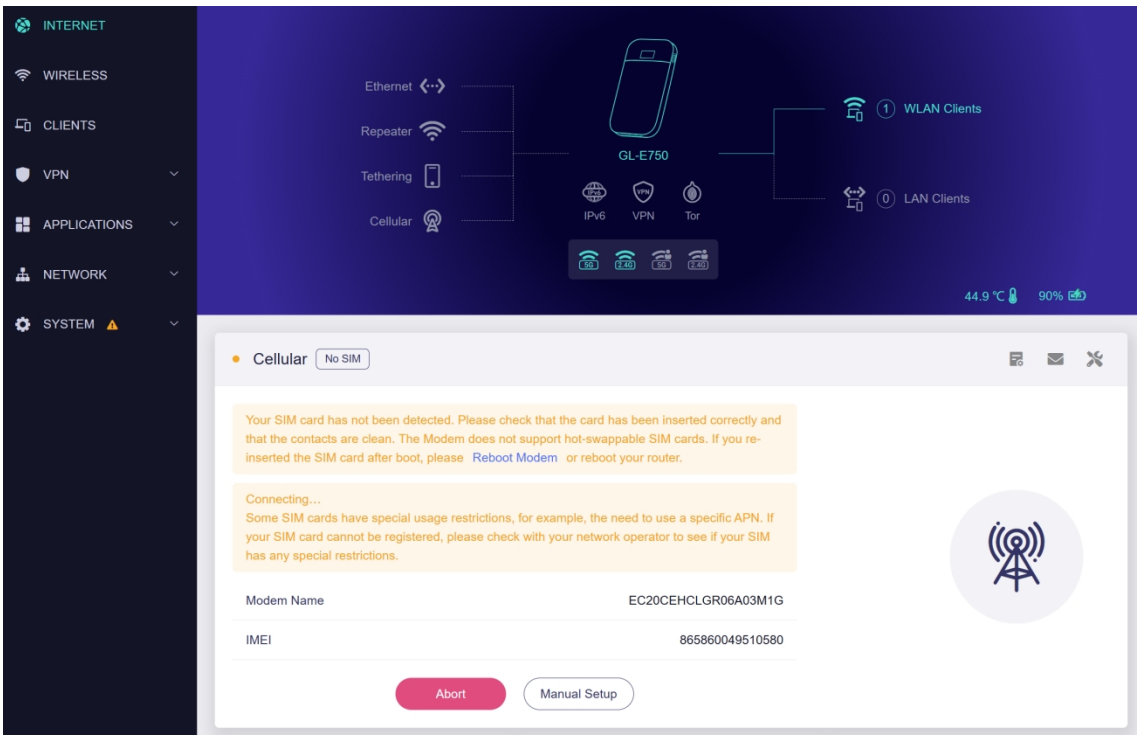
Este capítulo lo guía para iniciar sesión en su enrutador a través del panel de administración web.

Configure y administre su enrutador a través de una interfaz de administración basada en webement, a la que se puede acceder desde cualquier sistema operativo Windows, Mac OS 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 indicaciones en pantalla.

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

1. Conecte un dispositivo (por ejemplo, una computadora o computadora portátil) al enrutador mediante Wi-Fi o un cable Ethernet.
2. Abra un navegador web (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 accede a la web undmin panel, consulte aquí para solucionar problemas.
3. Sconfigure su contraseña de administrador. Se recomienda una contraseña segura por motivos de seguridad. Luego haga clic en **Siguiente** para continuar.
4. Ylo luego ingrese al router's web admin panel.



Capítulo 4

Configurar la conexión a Internet

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

Mudi V2 admite cuatro métodos de conexión a Internet: Ethernet, Repetidor, Anclaje a red USB y módem USB. Elija el método adecuado según sus necesidades de usoelija el método apropiado según su.

1. **Celular (Cellular)**: inserte una tarjeta SIM en el enrutador o habilite la eSIM integrada. Luego, el enrutador se conectará a Internet a través de una red celular 3G o 4G, según la red de su proveedor y las bandas de frecuencia admitidas. Este método ofrece una gran flexibilidad y es ideal para escenarios como el uso en vehículos o actividades al aire libre.

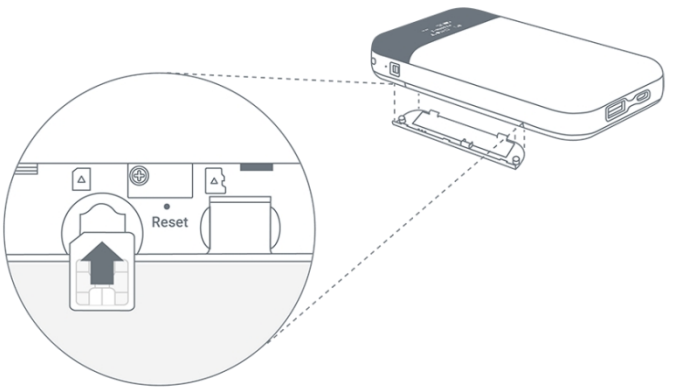
2. **Ethernet (RJ45)**: conecte el enrutador a una red de banda ancha usando unn cable Ethernet conectado al puerto WAN. El enrutador normalmente obtiene una dirección IP automáticamente a través de DHCP. Los usuarios pueden también manualmente configurar una IP estática o configuración PPPoE. Este método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

3. **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.

4. **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, 3G/4G) con el enrutador. Esta es una solución conveniente para el acceso temporal a Internet, especialmente al aire libre o en áreas sin banda ancha fija.

4.1 Conectarse a Internet mediante la red móvil

Conecte el enrutador a Internet insertando una tarjeta SIM en la ranura SIM. El enrutador puede acceder a Internet a través de redes 3G/4G sin depender de la banda ancha de línea fija. Es ideal para uso en vehículos o actividades al aire libre y comparte la red SIM con todos los dispositivos conectados. Esta conexión se implementa a través del módem celular del enrutador'.



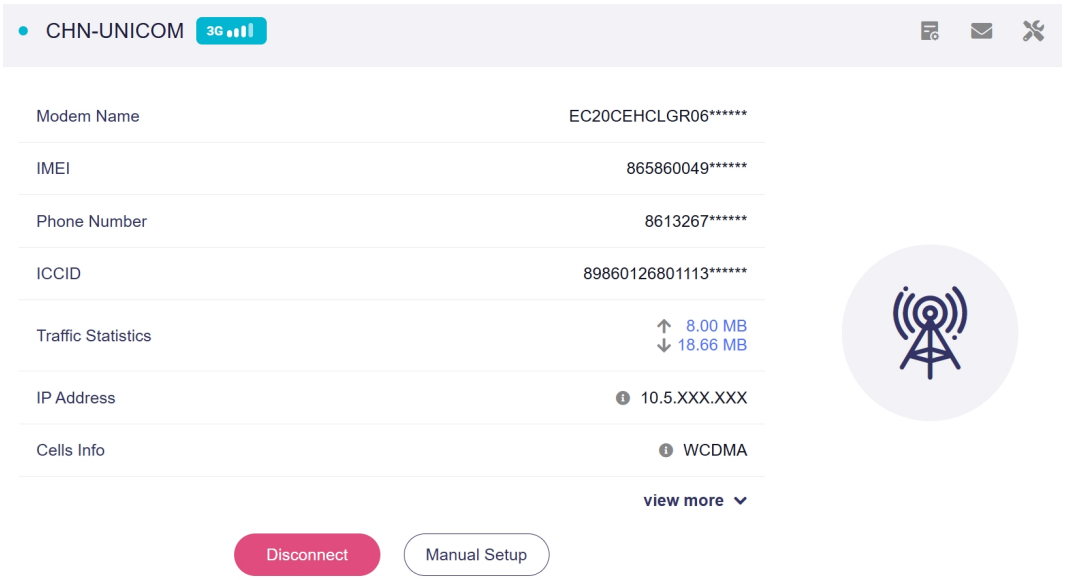
Nota:

1. GL-E750V2 admite tarjetas eSIM físicas. Tenga en cuenta que GL-E750V2 vSIM no admite tarjetas físicas eSIMs. Para obtener más información, consulte cómo utilizar la tarjeta física eSIM en el enrutador GL.iNet.
2. La ranura para tarjeta MicroSD es solo para almacenamiento y no es necesaria para el acceso a Internet celular.

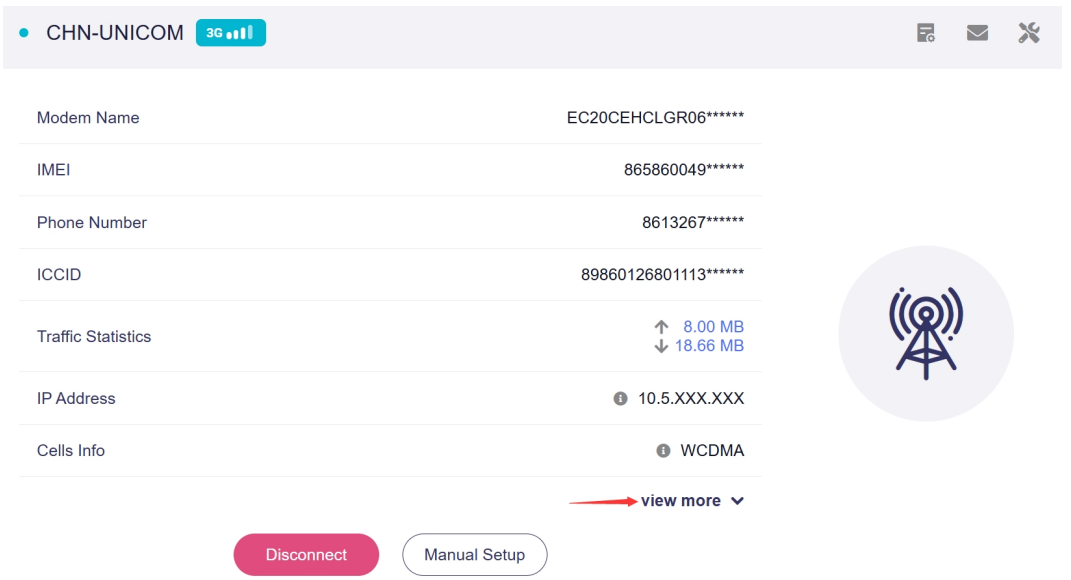
4.1.1 Configuración básica

Siga los pasos a continuación para conectar su enrutador a Internet a través de Celular.

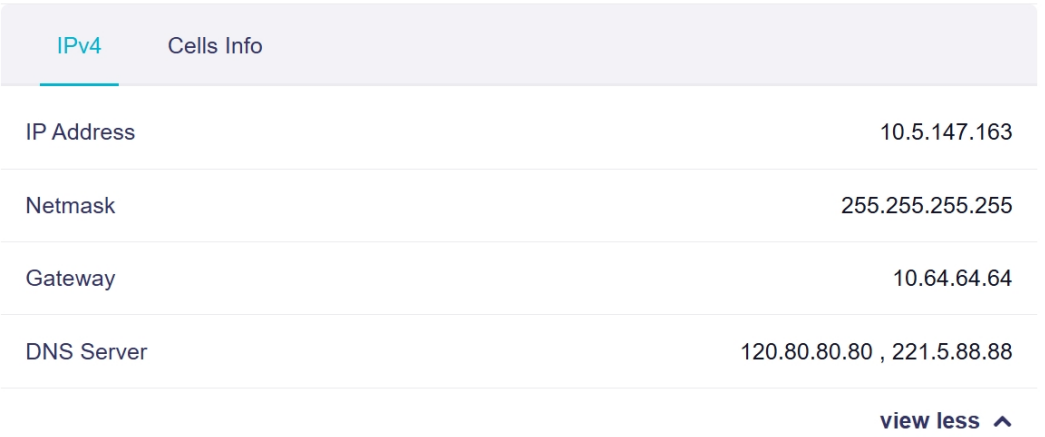
1. Inserte una tarjeta SIM en el enrutador, lala conexión a Internet se establecerá automáticamente.
2. Inicie sesión en el enrutador’s web admin panel, navega hasta **INTERNET** > **Celula**r. Deberías ver el nombre de tu operador SIM y un punto verde en la sección Celular. De lo contrario, apaga el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



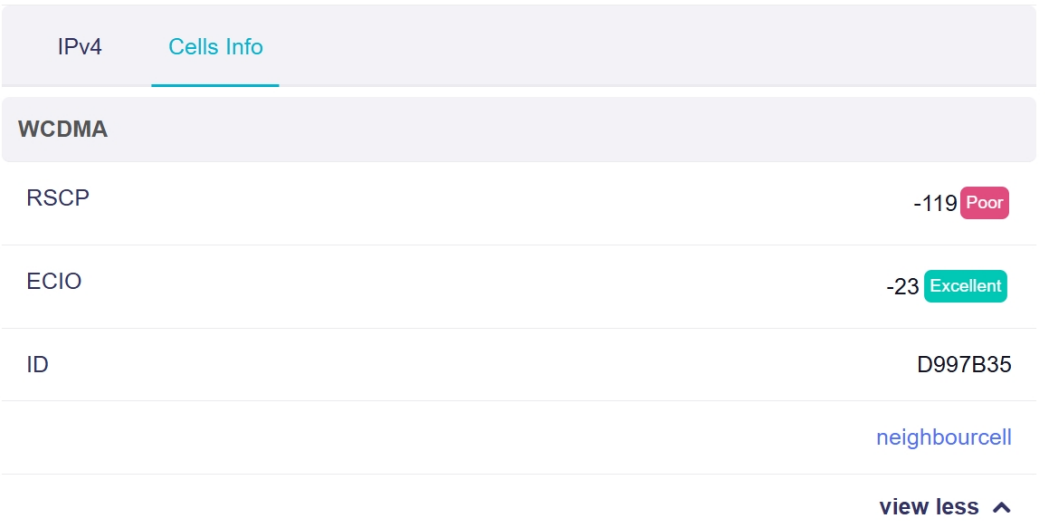
3. Haz clic en **Ver más** para ver más información celular, incluidos detalles del módem, detalles de la tarjeta SIM, detalles de Internet y señal celular.



Puede ver detalles de WAN.



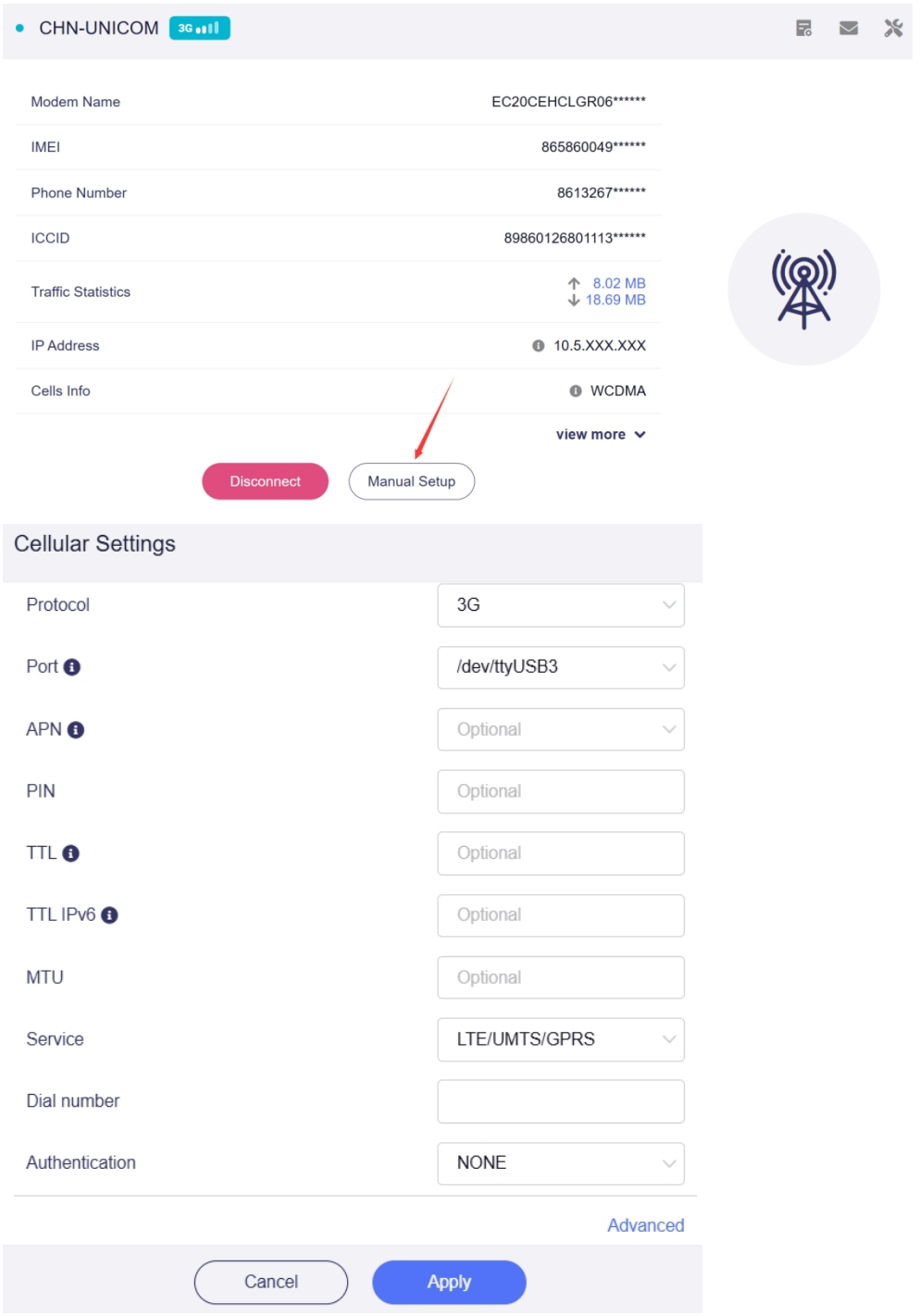
Haga clic en **Información de celdas** para ver los detalles celulares si necesario.



Si encuentra algún problema, consulte la Guía de solución de problemas de red celular.

4.1.2 Configuración manual

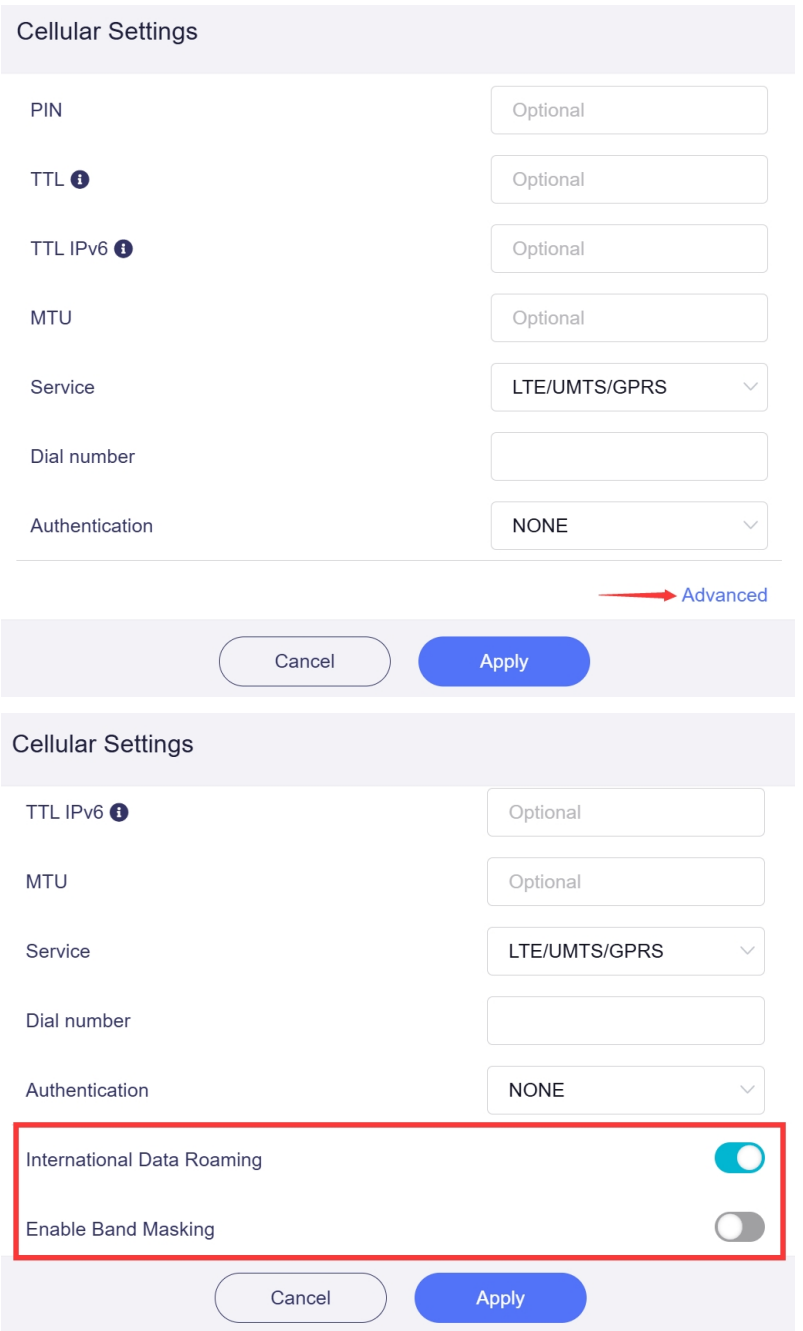
El enrutador proporciona configuraciones avanzadas opcionales para conexiones celulares. Haga clic en **Configuración manual** para configurarlos.



- **Protocolo**: seleccione el protocolo de comunicación para el módulo celular, incluidos 3G, QMI y QCM.

- **Puerto**: El puerto serie utilizado para comunicarse con el módem celular. Esto suele detectarse automáticamente y no requiere ajuste manual.
- **APN**: algunas tarjetas SIM requieren un APN específico. Si no conoce el APN correcto, consulte a su operador de red.
- **PIN**: ingrese el PIN de la tarjeta SIM si la protección mediante PIN está habilitada.
- **TTL**: TTL (tiempo de vida) define el tiempo máximo que los paquetes pueden sobrevivir en la red. De forma predeterminada, el enrutador reduce en 1 el TTL de los paquetes entrantes de los dispositivos cliente antes de reenviarlos. Si necesita anular/falsificar el TTL, ingrese el TTL efectivo deseado más 1 para compensar la disminución automática. TTL es válido solo para IPv4.
- **TTL IPv6**: Equivale a TTL en IPv4, lo que limita el recuento máximo de saltos de los paquetes de datos IPv6.
- **MTU**: El valor predeterminado es 1500.
- **Servicios**: seleccione el tipo de servicio de red celular, incluidos LTE/UMTS/GPRS y CDMA/EVDO.
- **Marcar número**: ingrese el número de acceso telefónico proporcionado por su operador, déjelo en blanco si no es necesario.
- **Autenticación**: elija el método de autenticación requerido por su proveedor (por ejemplo, NINGUNO, PAP, CHAP). Por lo general, esto se establece en NINGUNO si no se necesitan credenciales.

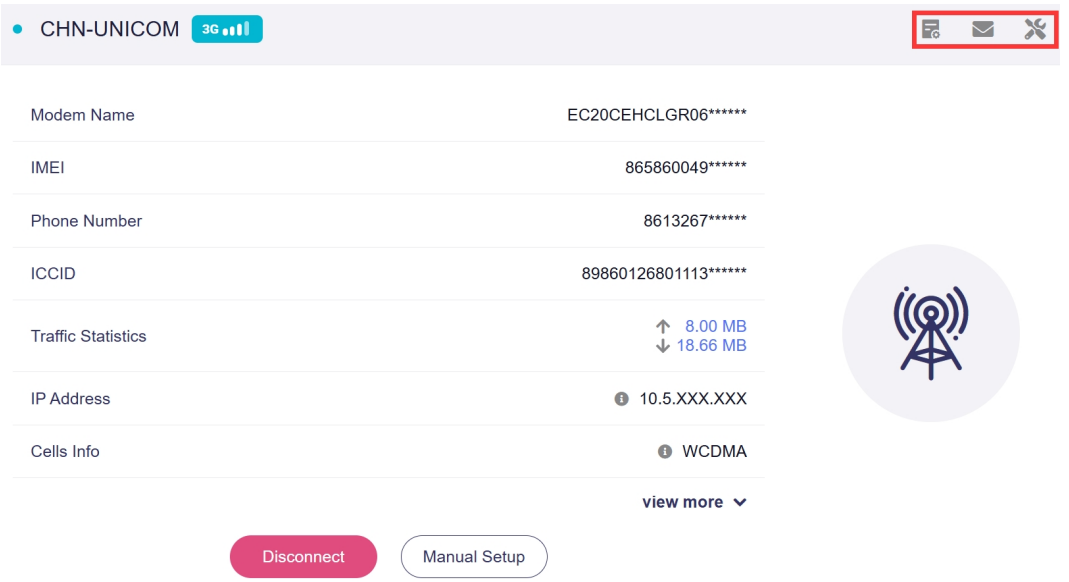
Haga clic **Avanzado** para habilitar roaming de datos internacional o enmascaramiento de banda si es necesario.



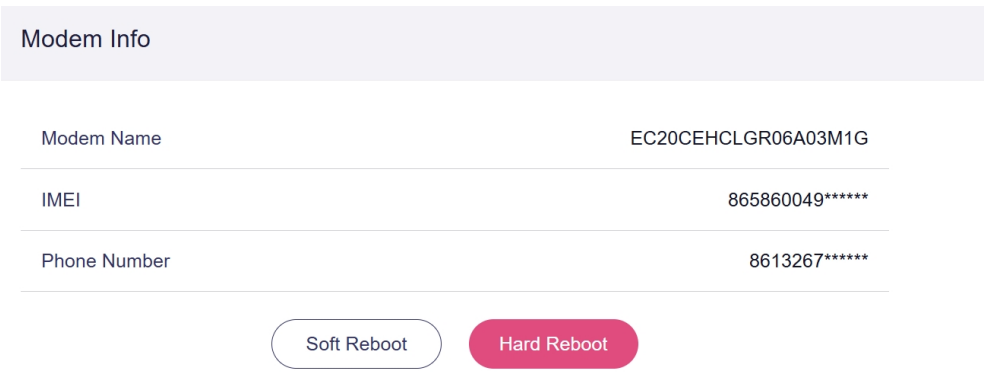
- **roaming de datos internacional**: si esta opción está habilitada, la tarjeta SIM puede usar datos móviles mientras está en roaming en el extranjero. Es posible que se apliquen cargos de roaming adicionales. Esta opción está habilitada de forma predeterminada.
- **Habilitar enmascaramiento de banda**: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

4.1.3 Configuración del módem

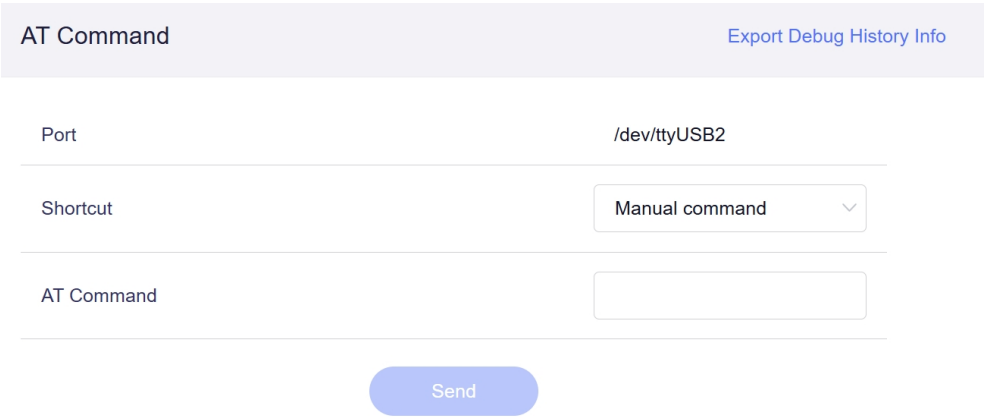
Además de las configuraciones celulares básicas, usted puede habilitar funciones avanzadas para administrar perfiles celulares, mensajes SMS y modem management.



- **Administrar perfiles**: cree y administre perfiles celulares para cambiar rápidamente APN y otras configuraciones celulares.
- **SMS**: envíe, reciba y vea mensajes SMS a través del módem celular integrado.
- **Administración de módem**: vea información del módem y ejecute comandos AT para depurarlo.
  - **Información del módem**: visualización básica información del módem y realice un reinicio suave/hard del módem.



  - **Comando AT**: envíe comandos AT para verificar el estado y depurar el módem celular.


AT Command
Export Debug History Info
Port
/dev/ttyUSB2
Shortcut
Manual command
AT Command
Send

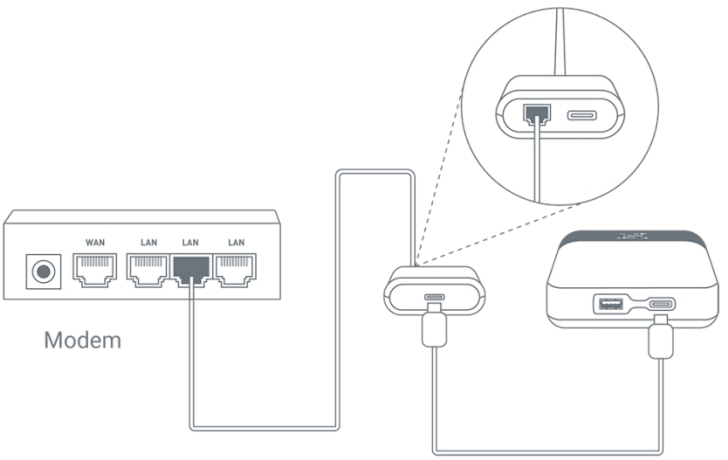
4.2 Conectarse a Internet mediante un cable Ethernet

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

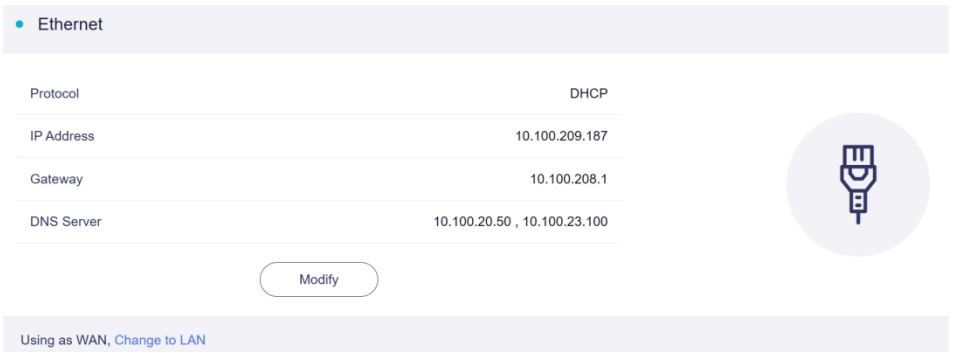
4.2.1 Configuración básica

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

1. Primero, verifique si el puerto del replicador de puertos USB-C está configurado como puerto WAN. De lo contrario, inicie sesión en el panel de administración web del enrutador y navegue hasta **INTERNET** > **Ethernet** para configurarlo en **WAN**.
2. Conecte el **WAN** puerto de su enrutador al el dispositivo ascendente (por ejemplo, un Módem ISP, enrutador principal, conmutador de red o conector Ethernet) a través de un Ethernet cable.

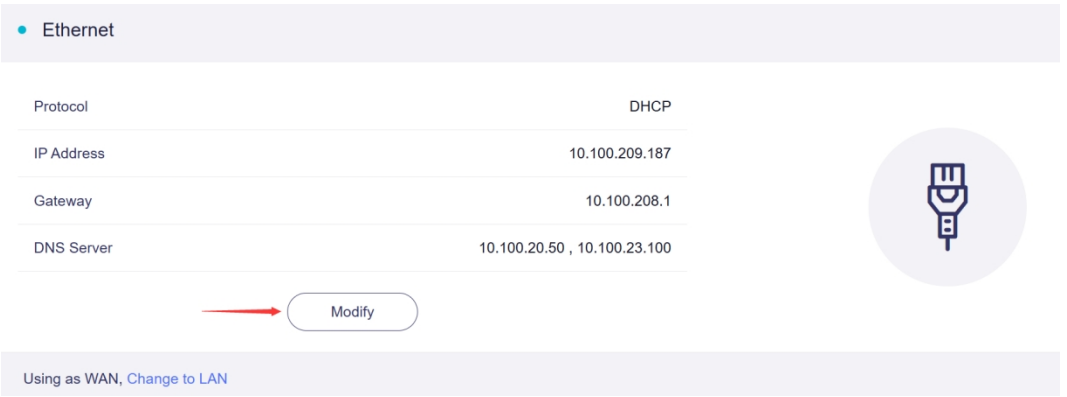


3. Inicie sesión en el enrutador’panel de administración web y navegue a **INTERNET** > **Ethernet**. Si la conexión se realiza correctamente, la sección Ethernet mostrará los detalles de la red, incluidos el protocolo, la dirección IP, la puerta de enlace y el servidor DNS.


Ethernet
Protocol
DHCP
IP Address
10.100.209.187
Gateway
10.100.208.1
DNS Server
10.100.20.50 , 10.100.23.100
Modify
Using as WAN, Change to LAN

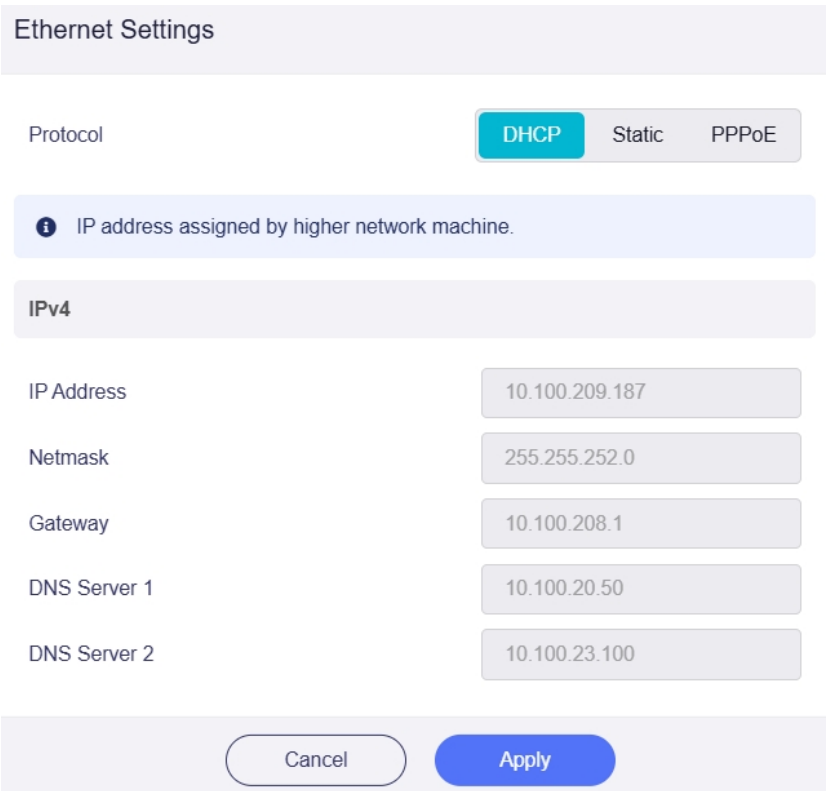
4.2.2 Protocolo

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



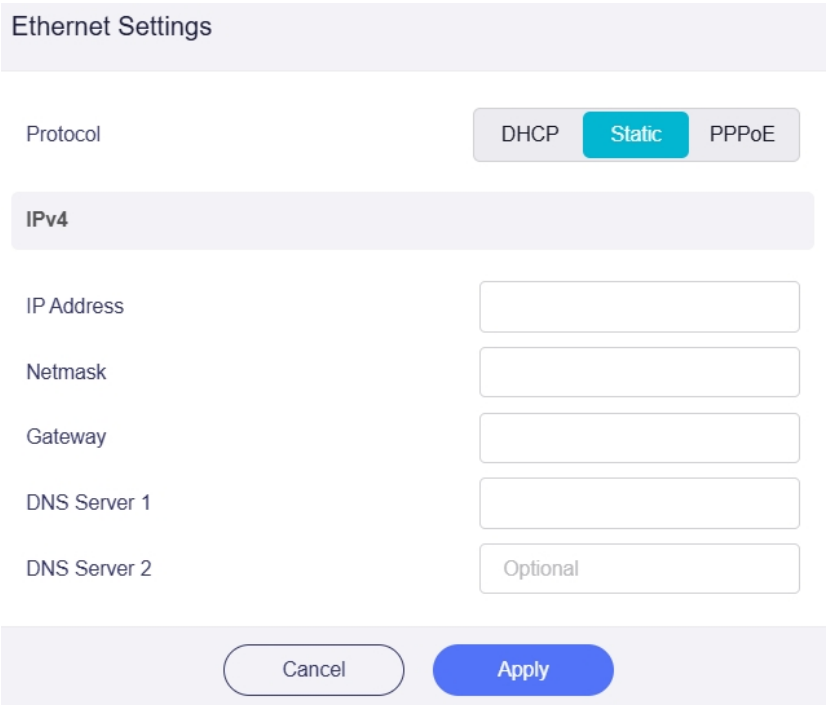
- **DHCP**

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



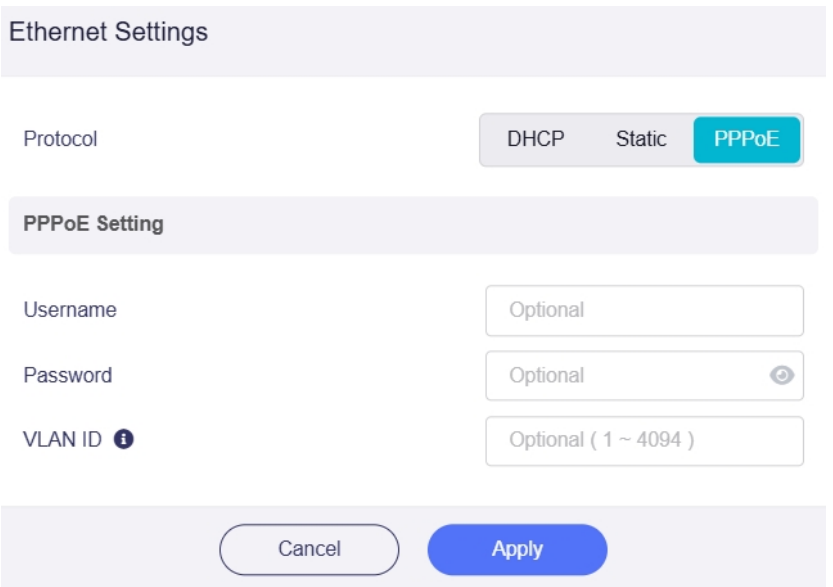
- **Estática**

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



- **PPPoE**

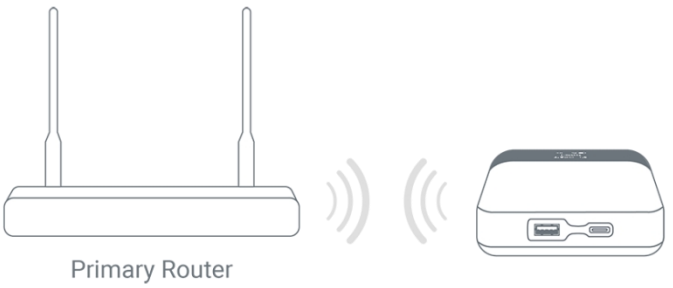
  PPPoE (punto a punto) Protocolo sobre Ethernet) es un protocolo de red ampliamente utilizado por los ISP. Por lo general, proporcionarán un módem junto con un nombre de usuario y una contraseña únicos, que son necesarios para configurar una conexión a Internet.



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

4.3 Conectarse a Internet mediante una red Wi-Fi existente

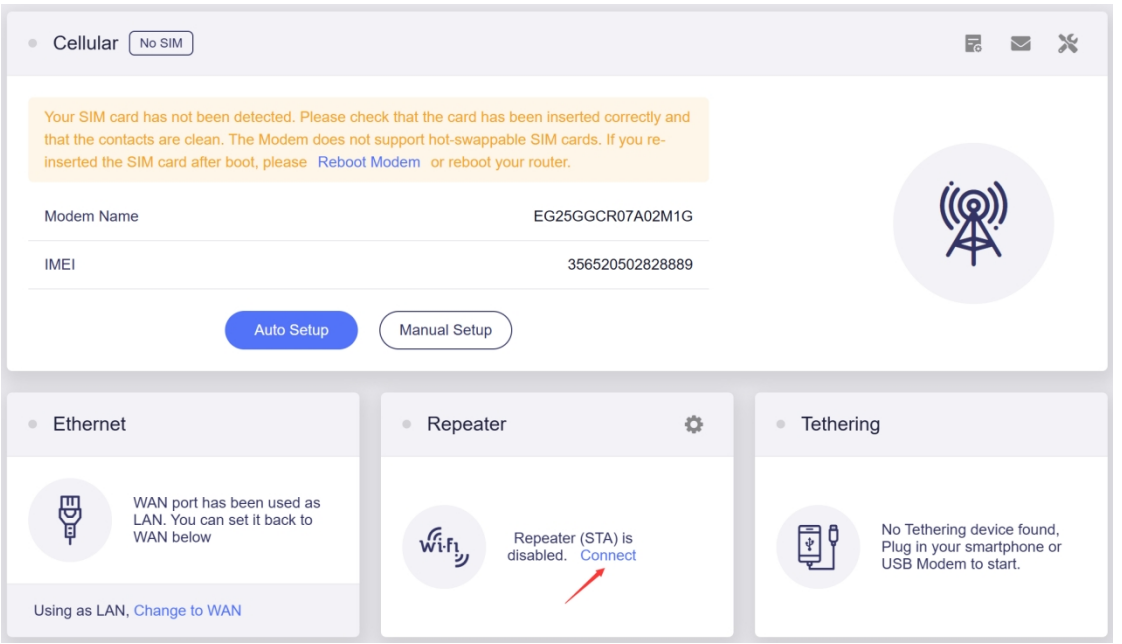
Conecte el enrutador como repetidor a la red inalámbrica existente para aumentar las señales Wi-Fi-Fi y crear una red local aislada de la red principal. cuando en hoteles o cafeterías con puntos de acceso públicos gratuitos, el uso de un repetidor no solo fortaleces Wi-señales de Fi, sino que también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



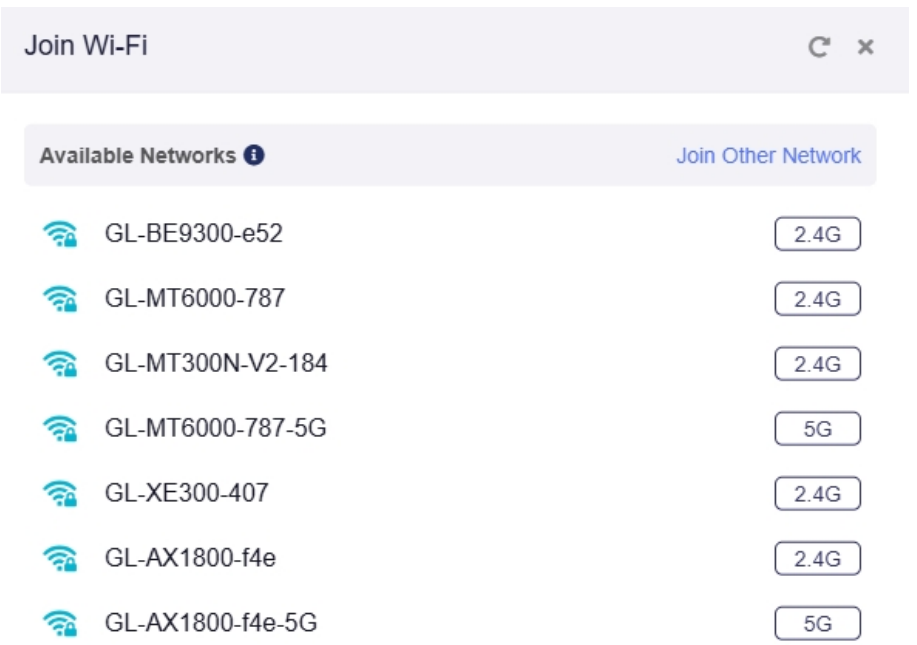
Función de repetidor GL.iNet funciona en modo WISP (Proveedor de servicios de Internet inalámbrico) de forma predeterminada, lo que significa que el enrutador creará su propia subred y actuará como un firewall para protegerlo de la red pública.

4.3.1 Configuración básica

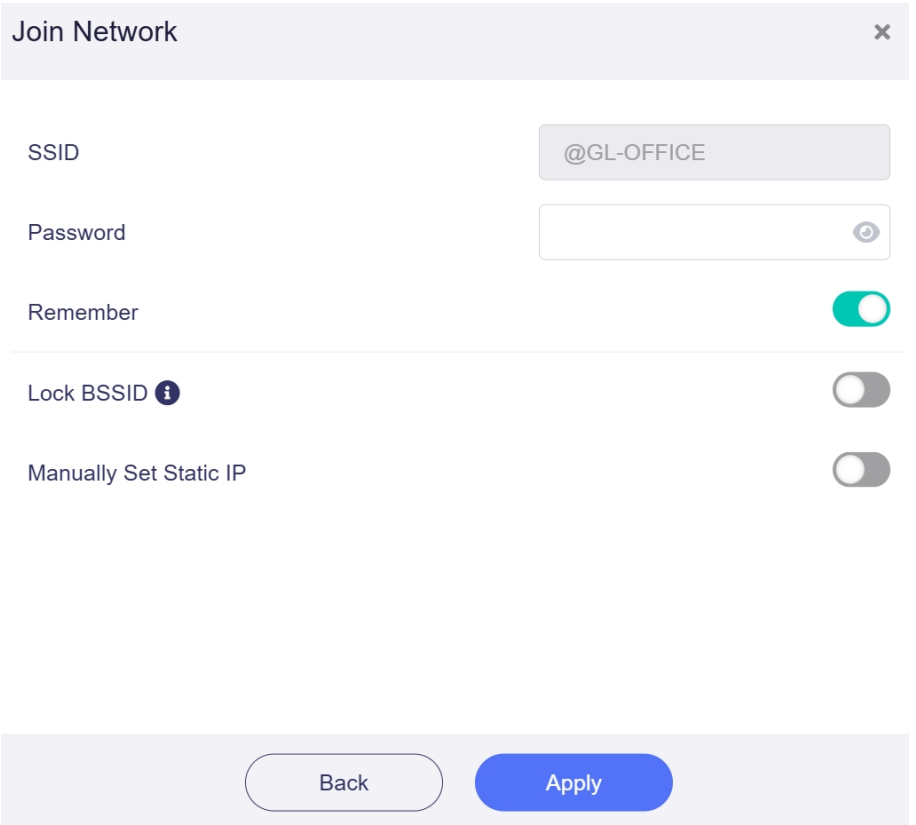
1. Inicie sesión en enrutador'panel de administración web y navegue a **INTERNET** > **Repetidor**. Haga clic en **Conectar**.



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

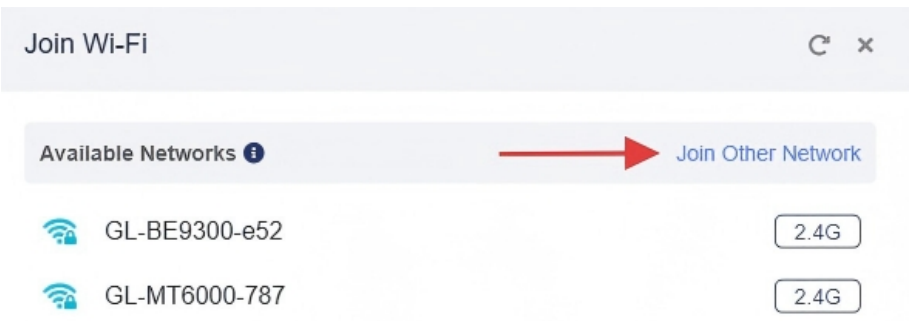


3. Eingrese la contraseña de Wi-Fi correcta y haga clic en **Aplicar**.

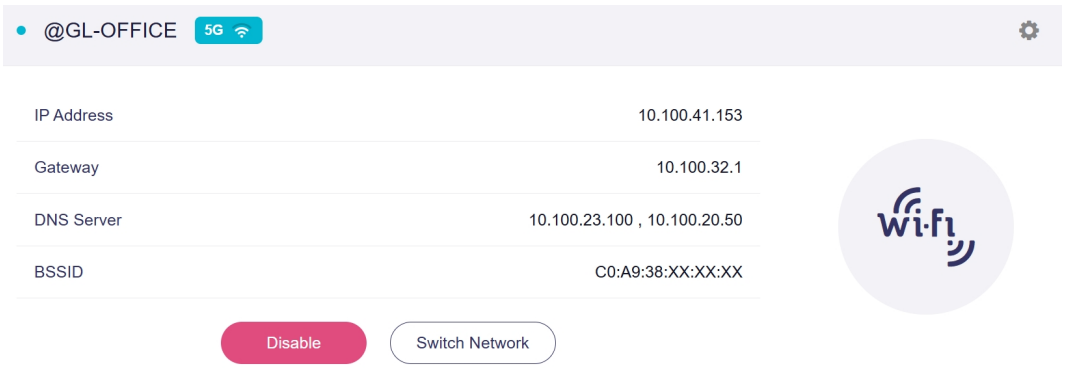


- **Recordar**: habilite esta opción para recordar la red Wi-Fi actual repetida.
- **Bloquear BSSID**: Cuando está habilitado, el enrutador se conectará solo al punto de acceso (AP) específico correspondiente al BSSID seleccionado, incluso cuando otros AP compartan el mismo SSID.
- **Manualmente Set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

4. Si el SSID de Wi-Fi de destino no está en en la lista Red disponible, 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**.

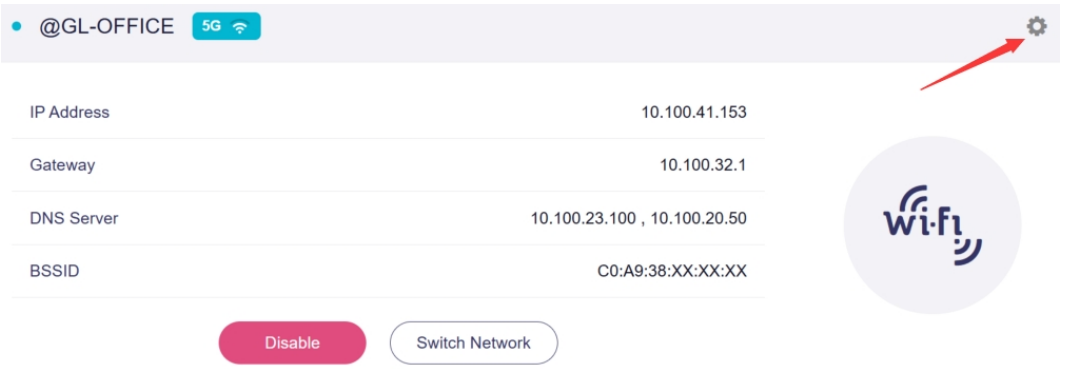


5. Espere un minuto hasta que el enrutador conectar. Una vez conectado, la página se muestra a continuación.

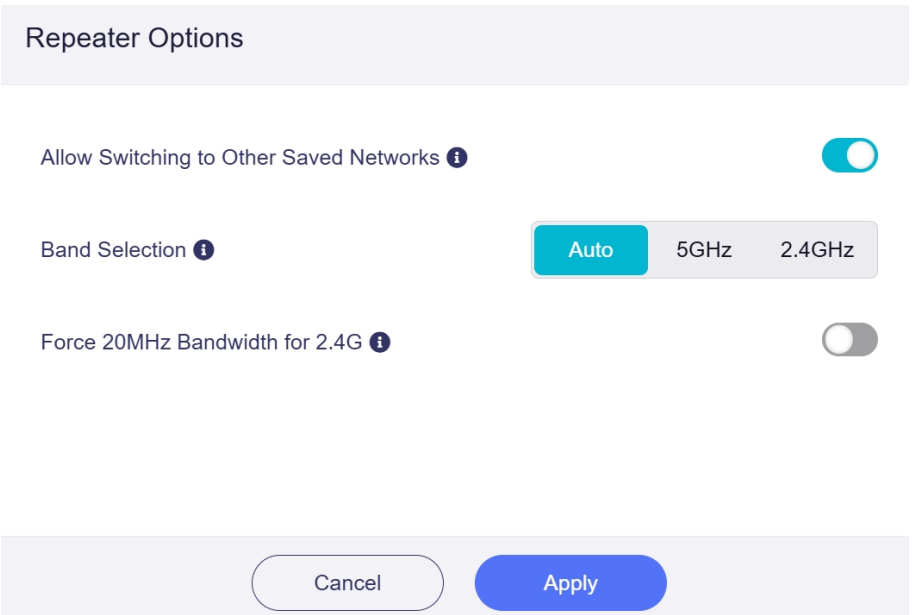


4.3.2 Opciones de repetidor

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



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



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

4.4 Conectarse a Internet mediante conexión compartida por USB

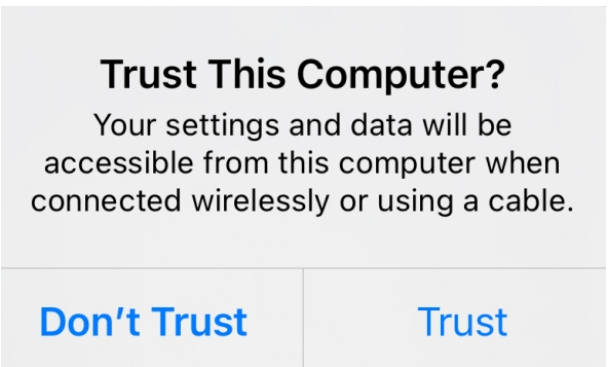
Cla conexión de un inteligenteteléfono al enrutador a través de un cable USB se llama Anclaje a red, que puede compartir la red de datos móviles del dispositivo (por ejemplo, 4G/5G) con el enrutador. Este es un método conveniente para el acceso temporal ia Internet, especialmente cuando al aire libre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



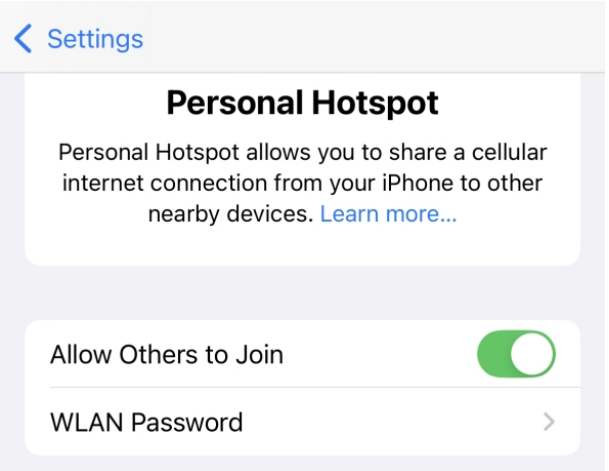
El módem sin host también funciona en anclaje a red durante la configuración del módem.
Nota: Algunos operadores de telefonía móvil limitan o cobran más por el anclaje a red. Recomendamos consultar con su operador.

4.4.1 Conexión compartida desde un iPhone

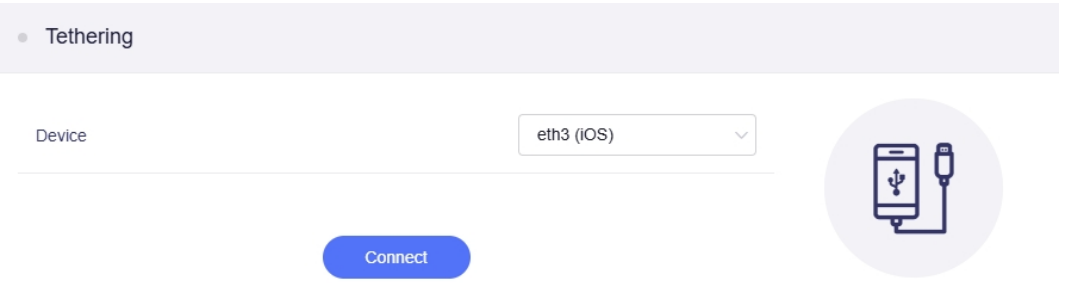
1. Conecte un iPhone al puerto USB del enrutador usando un cable USB. Aparecerá un cuadro de diálogo del sistema preguntando si se debe confiar en el dispositivo. Toque **Confiar** para continuar.



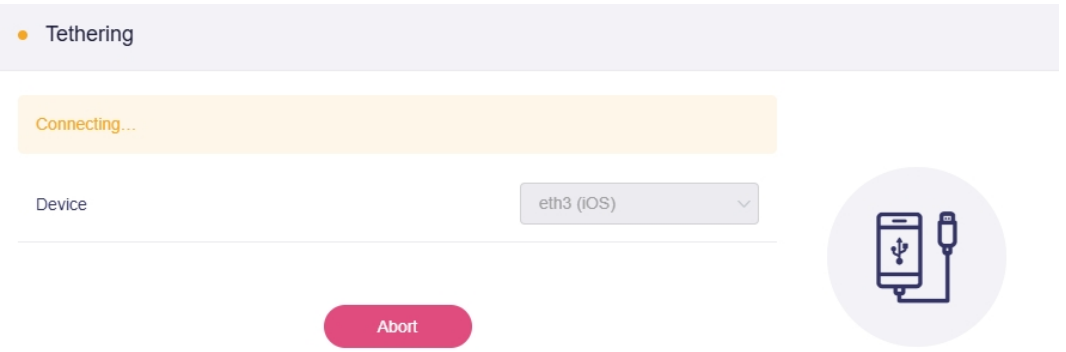
2. Ir a iPhone **Configuración** > **Punto de acceso personal**. Activar **Permitir que otros se unan**.



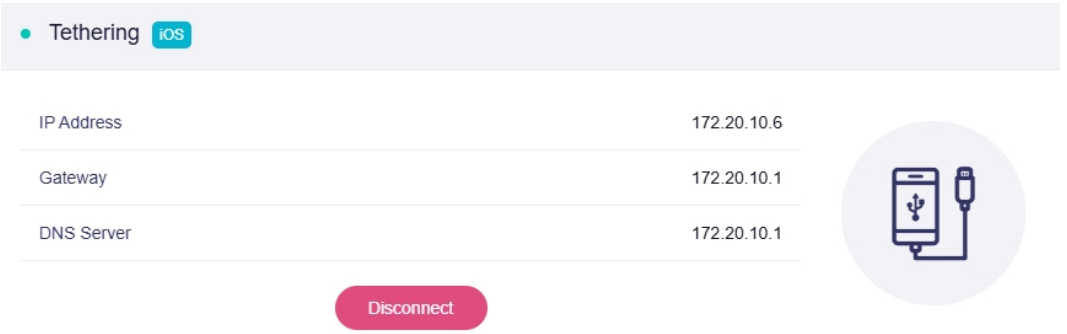
3. Conecte una computadora u otro teléfono al enrutador. Inicie sesión en el panel de administración web del enrutador y navegue hasta **INTERNET** > **Conexión**, luego haga clic en **Conectar**.



4. Comenzará a conectarse.

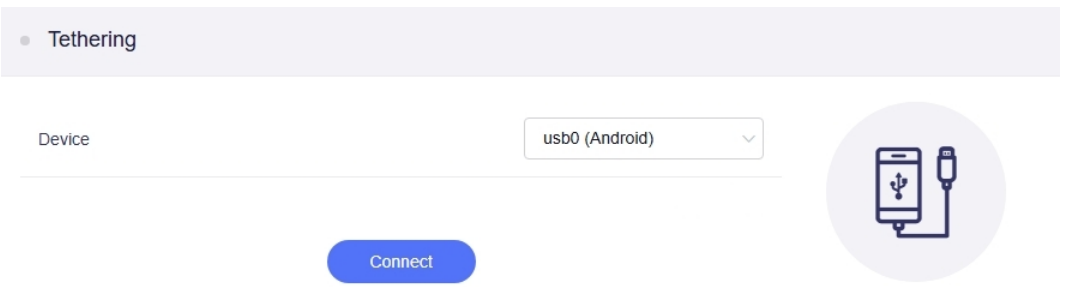


Una vez conectado, thesta página muestra la conexión de anclaje a red detalles.

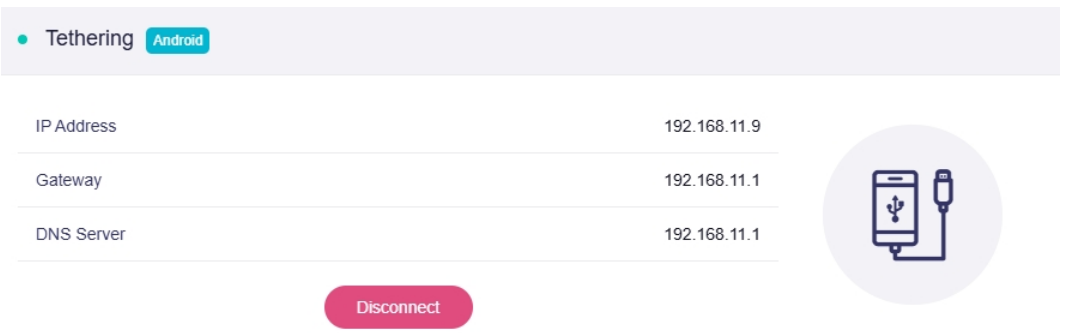


4.4.2 Conexión compartida desde Android

1. Conecta un teléfono Android al puerto USB del enrutador mediante un USB cable. 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**.



4. Una vez conectado, Estaes página mostrará el Estado de conexión .



4.4.3 Solución de problemas

Si el La conexión falla. intente estos pasos para solucionar el problema:

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

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

Capítulo 5

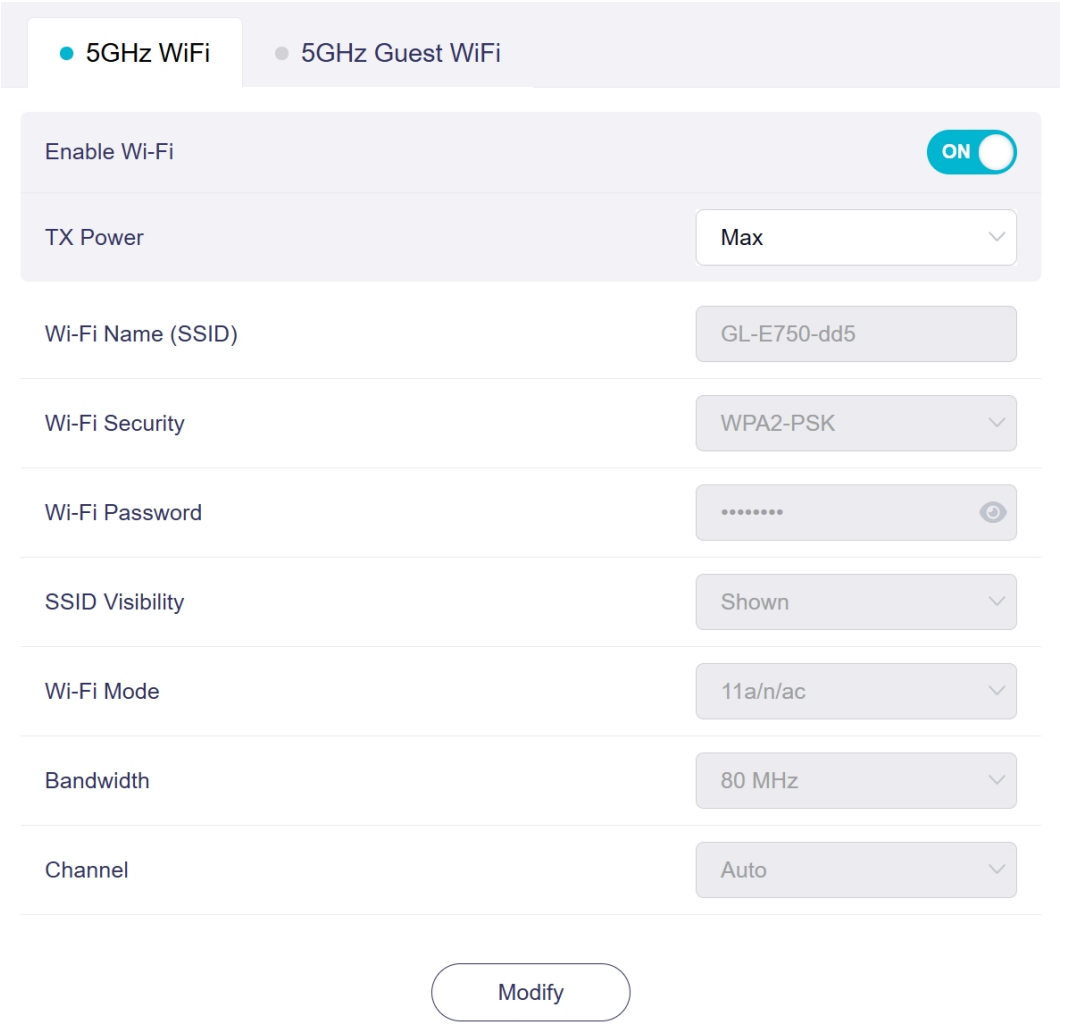
Red inalámbrica

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

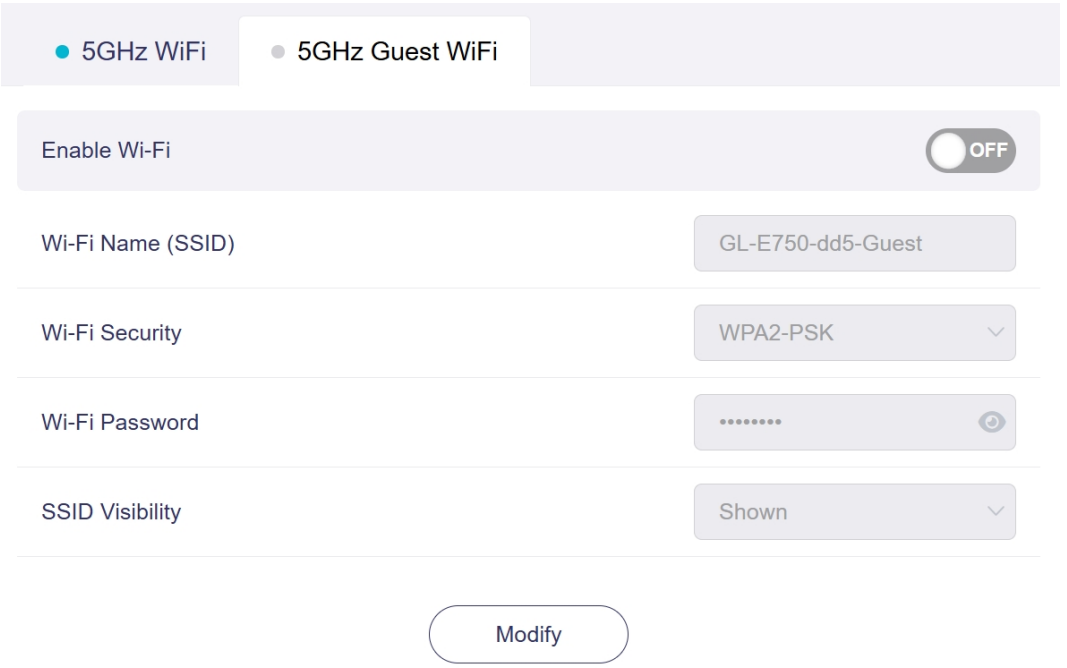
Inicie sesión en el panel de administración web del enrutador y navegue hasta **Inalámbrica**. La página inalámbrica muestra el enrutador’s 5 GHz y Configuraciones de 2,4 GHz, con cada dividida en redes Wi-Fi principal y Wi-Fi para invitados-Fi para una administración flexible .

5.1 Wi-Fi de 5 GHz

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



El 5 GHz Invitado Wi-Fi le permite configurar ajustes simplificados, incluyendo habilitar/deshabilitar Wi-Fi, configurar el nombre de Wi-Fi (SSID), la seguridad, la contraseña y la visibilidad del SSID.

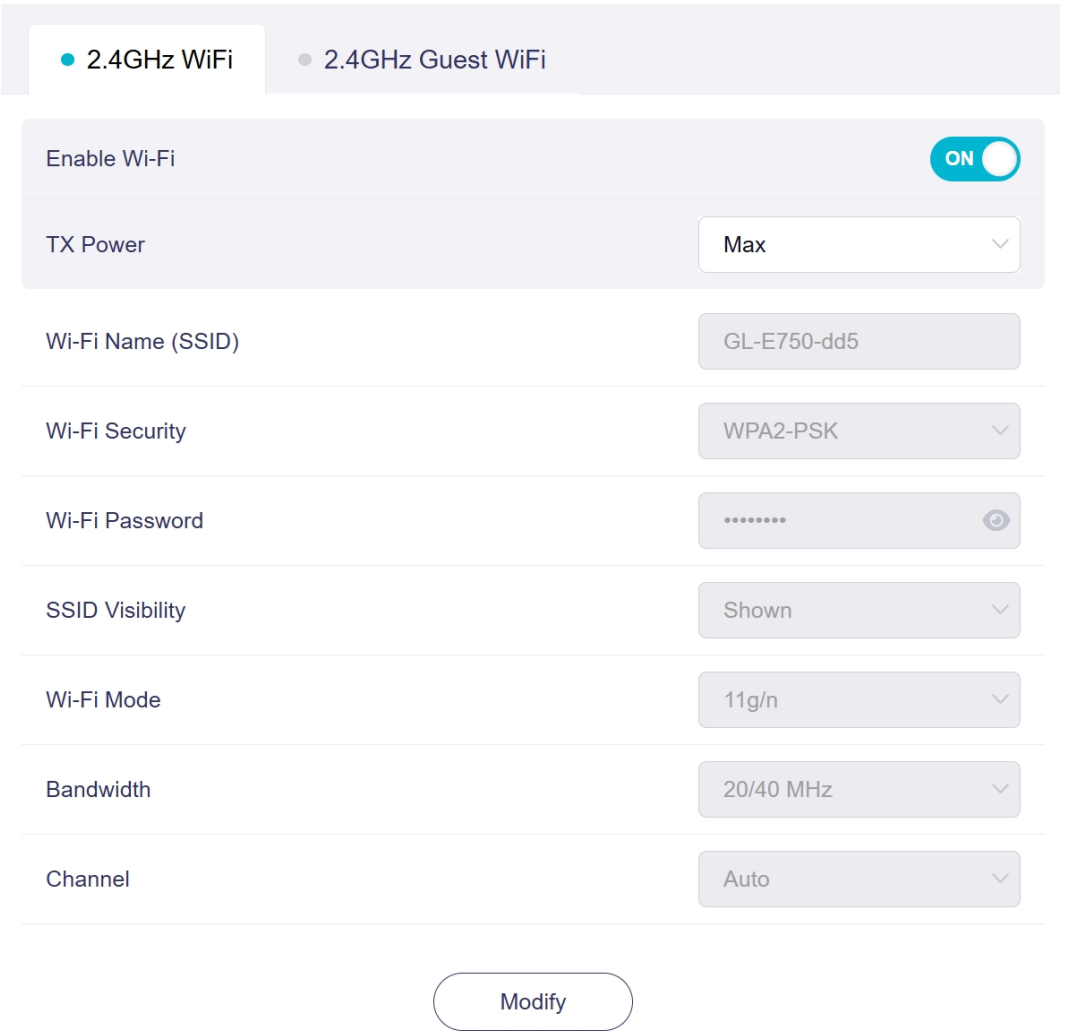


Nota:

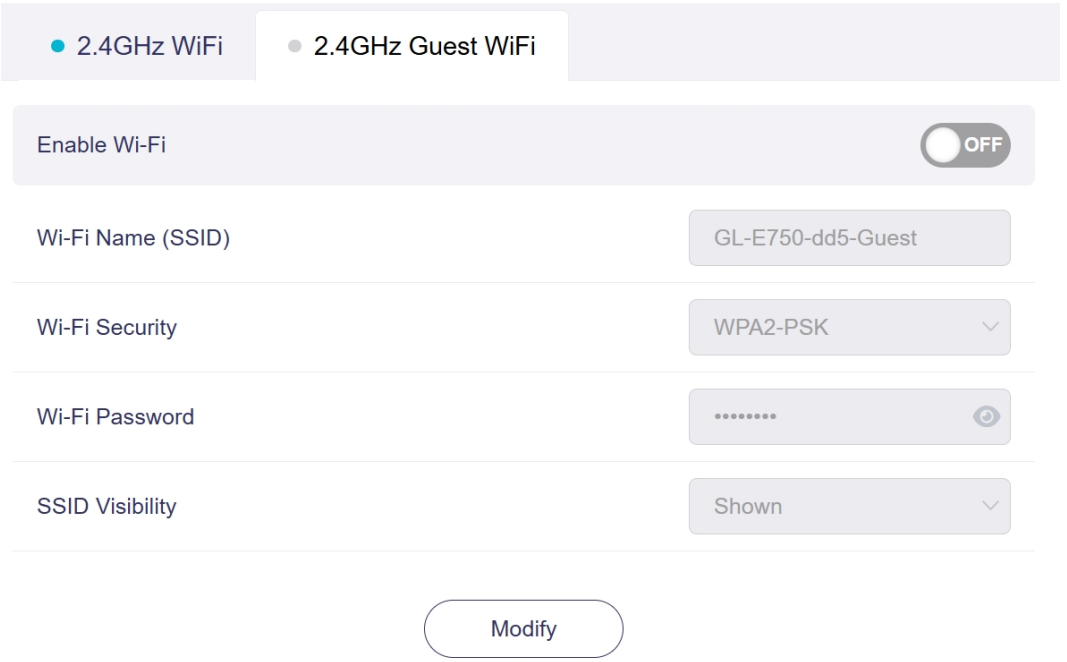
1. El **Ancho de banda** y **Canal** nono se puede modificar cuando el enrutador está configurado como a repetidor, ya que siguen el de la red repetida.
2. Cuando **Canal** está establecido a **Auto**, el enrutador's Wi-Fi no cambiará automáticamente al canal DFS.

5.2 Wi-Fi de 2,4 GHz

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



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



Nota: El **Ancho de banda** y **Canal** no puedenno modificarse cuando el enrutador está configurado como a repeater, ya que siguen el de la red repetida.

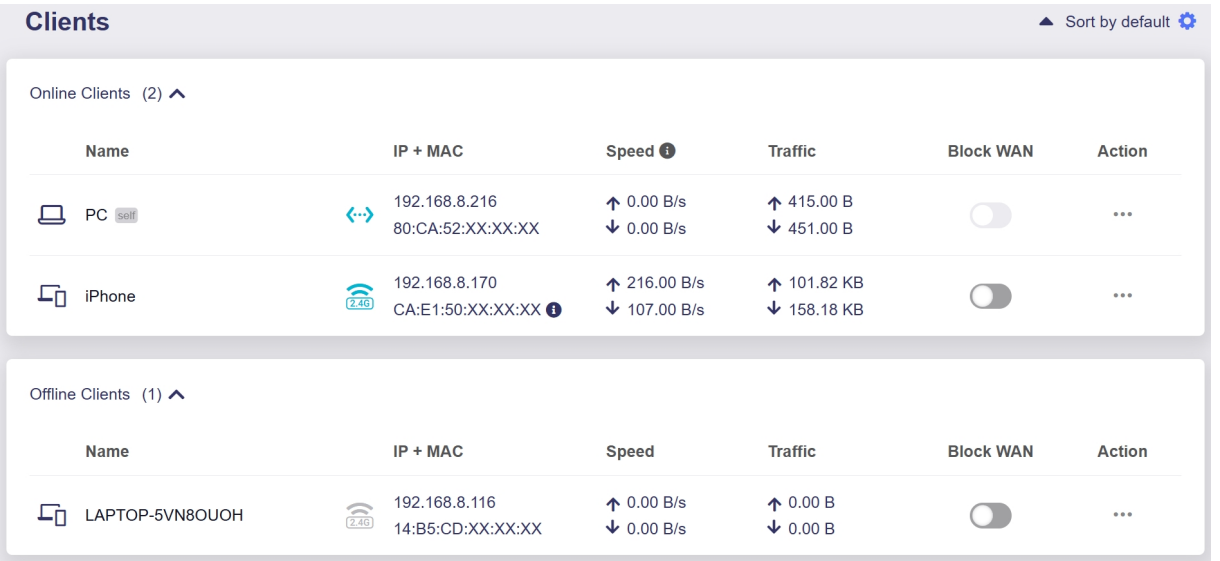
Capítulo 6

Clientes

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

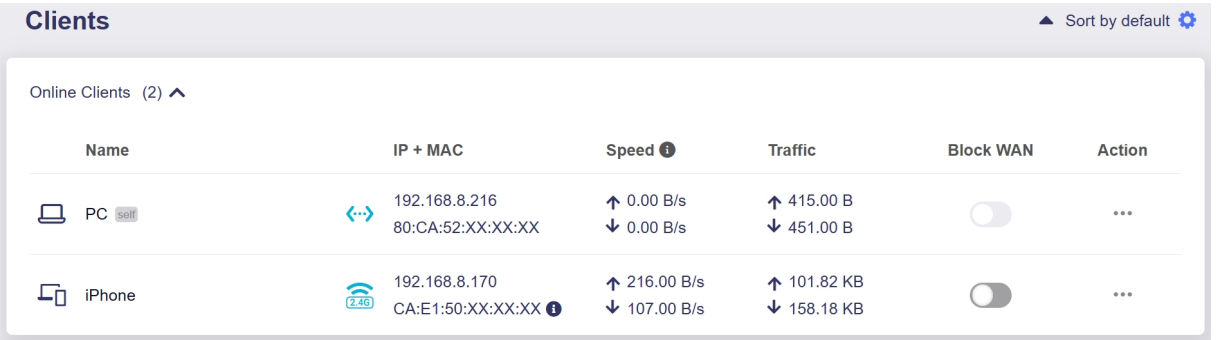
Inicie sesión en el enrutador’s web admin panel y navegue hasta **CLIENTES**.

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



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

6.1 Detalles del dispositivo



1. **Nombre del dispositivo**

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

2. **Dirección IP y MAC**

   La segunda columna enumera las direcciones IP y MAC del dispositivo conectado. Si los dispositivos conectados utilizan direcciones MAC aleatorias, aparecerá un mensaje, lo que indica 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 la tercera columna muestra la velocidad de Internet del dispositivo conectado. Laes velocidad representa la velocidad promedio durante el pasado 3 minutos. El sistema comienza a calcular la velocidad promedio cuando se abre esta página (por ejemplo, si la página solo ha estado abierta durante 10 segundos, la velocidad promedio se basará en solo 10 segundos de datos).

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

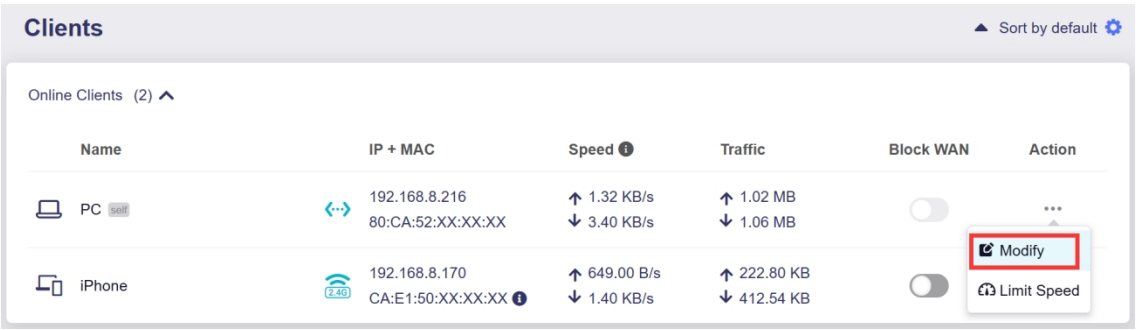
5. **Lista de bloqueo**

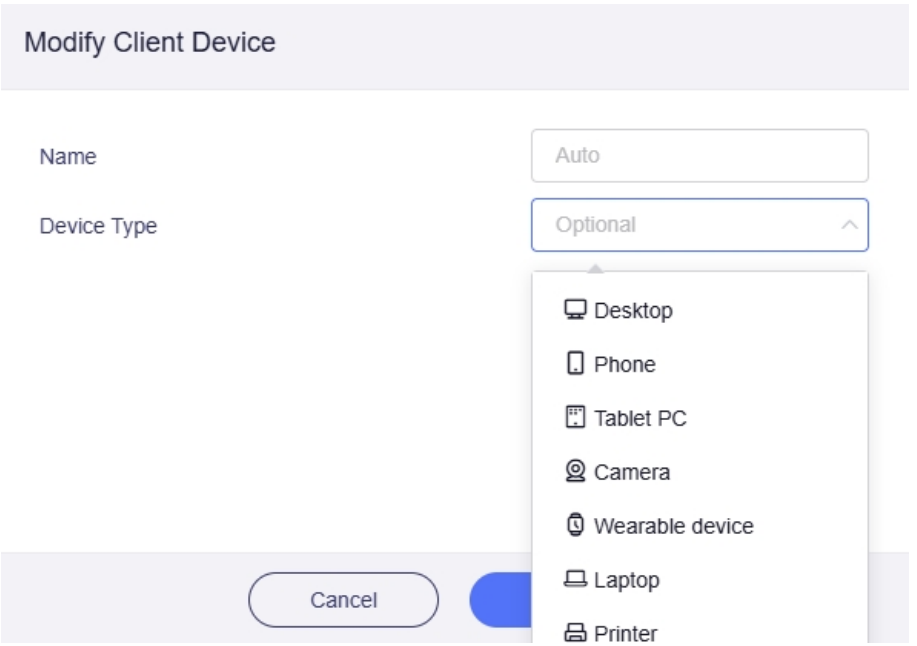
En la quintaésima columna, puede bloquear dispositivos conectados específicos con un clic. Si está habilitado, los dispositivos con direcciones MAC en el negrolist no puede conectarse a este enrutador. Tenga en cuenta que el bloqueo del cliente se basa en la dirección MAC del dispositivo. Si el dispositivo bloqueado usa una dirección MAC diferente la próxima vez, aún podrá conectarse al enrutador.

6.2 Acción

1. **Modificar**

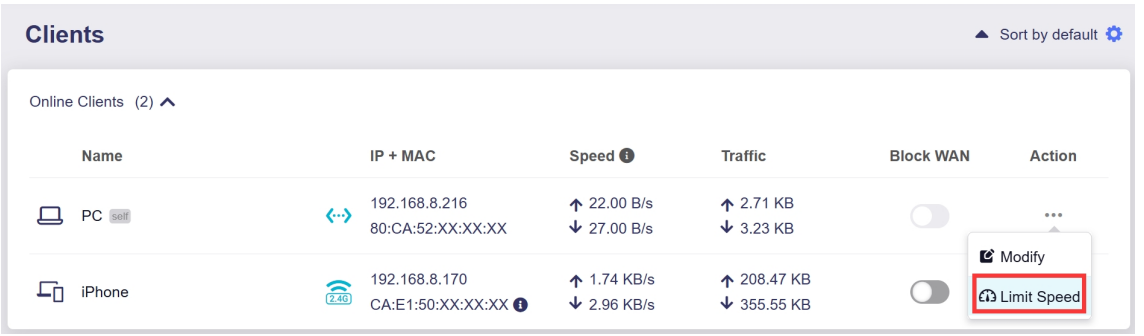
   Haga clic en el ícono de tres puntos en la **Acción** columna y haga clic en **Modificar** de el menú desplegable a modifique el nombre y tipo del dispositivo.



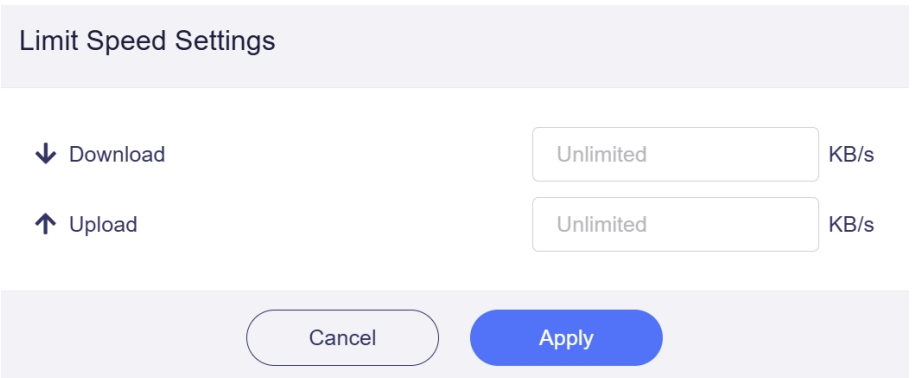


2. **Limitar velocidad**

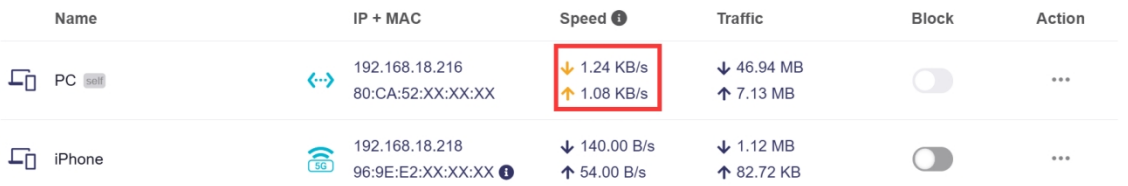
Haga clic en el icono de tres puntos en la **Acción** columna y haga clic en **Limitar velocidad** en el menú desplegable.



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

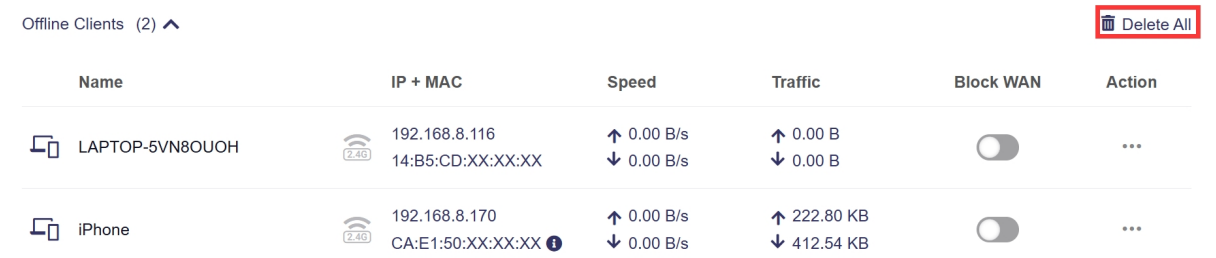


Si se ha aplicado una limitación de velocidad a un dispositivo, las flechas de velocidad de carga/descarga se volverán amarillas.

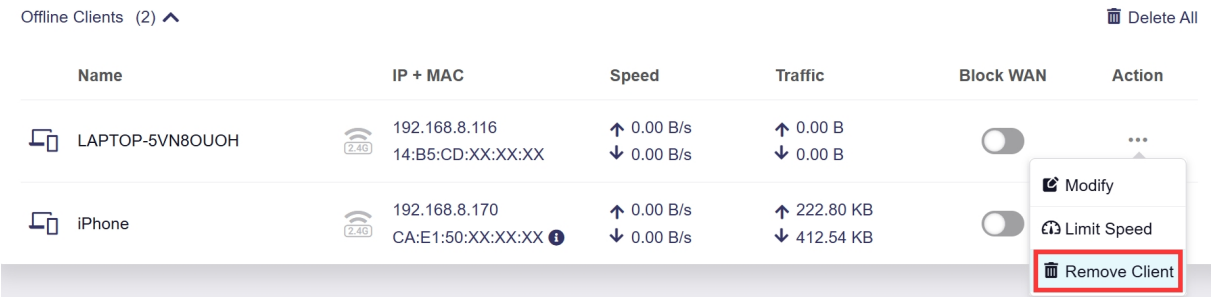


6.3 Eliminar clientes

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

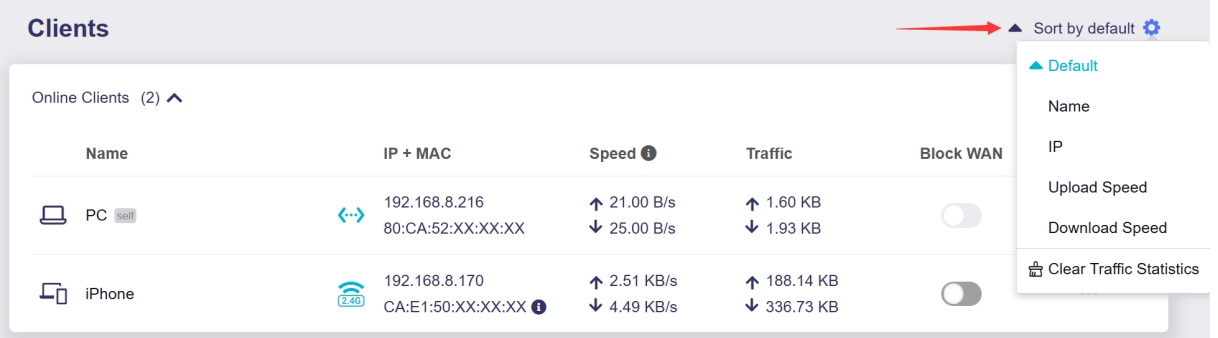


Si desea eliminar a cliente específico, haga clic en el ícono de tres puntos en la columna **Acción**, luego haga clic en **Quitar Cliente** desde el menú desplegable.



6.4 Ordenar

Puede configurar la clasificación del dispositivo regla para el Cliente página en la superior esquina derecha.



La clasificación predeterminadaing el orden es el siguiente:

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

Además de las reglas de clasificación, el menú desplegable también proporciona la **Borrar estadísticas de tráfico** función. Sese borra estadísticas de tráfico para todos los clientes en línea con un solo clic. Una vez aplicada, la columna de estadísticas de tráfico se restablecerá a cero y luego se reiniciarán las estadísticas.



Capítulo 7

Conozca la VPN

Este capítulo presenta VPN conceptos y uso escenarios.

7.1 Introducción

VPN

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

Enrutador VPN

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

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

OpenVPN

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

WireGuard

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

7.2 Escenarios de aplicación

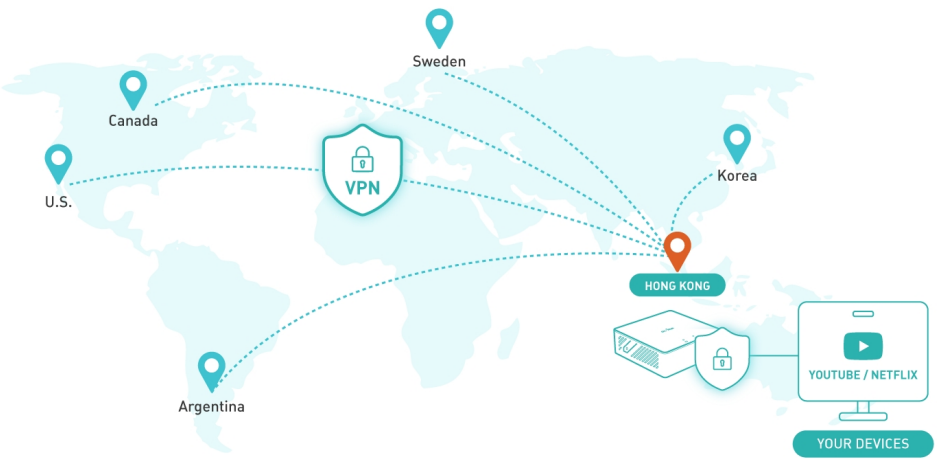
1. **Privacidad de datos personales**

   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 VPN para lograr una protección flexible para ciertos dispositivos.



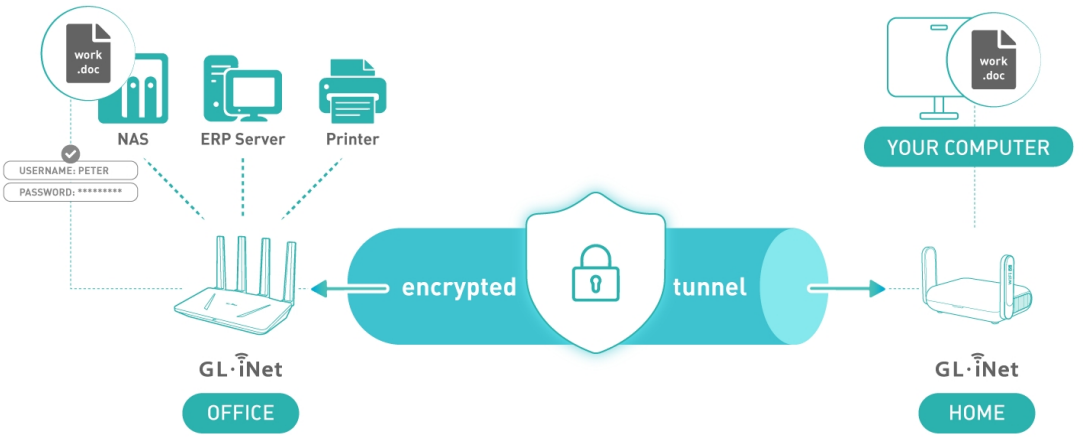
2. **Acceso sin restricciones en todo el mundo**

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



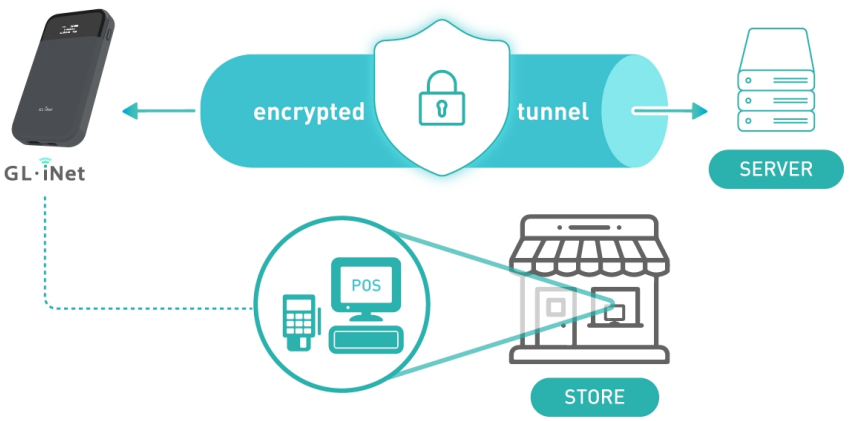
3. **Seguridad de datos para pequeñas empresas**

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



4. **Infraestructura de pago 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 La máquinas puede cargar información de la tarjeta de crédito a través de una VPN cifrada tunnel para garantizar la seguridad del pago.



Capítulo 8

Panel de VPN

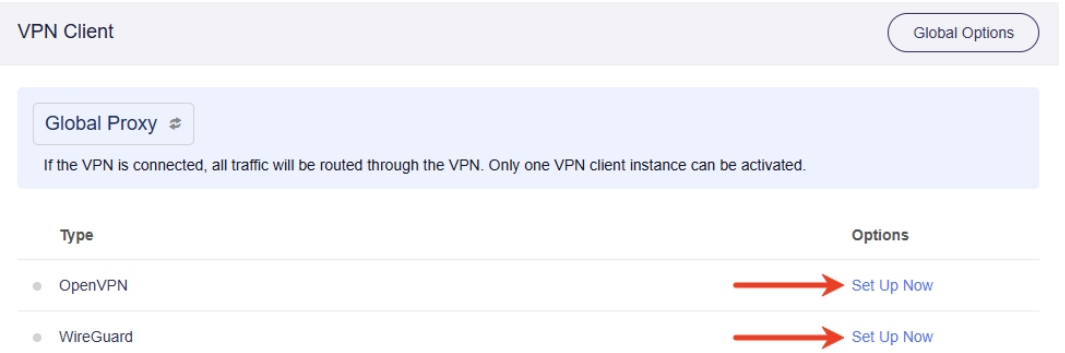
Este capítulo presenta cómo administrar conexiones VPN a través del panel de administración web.

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

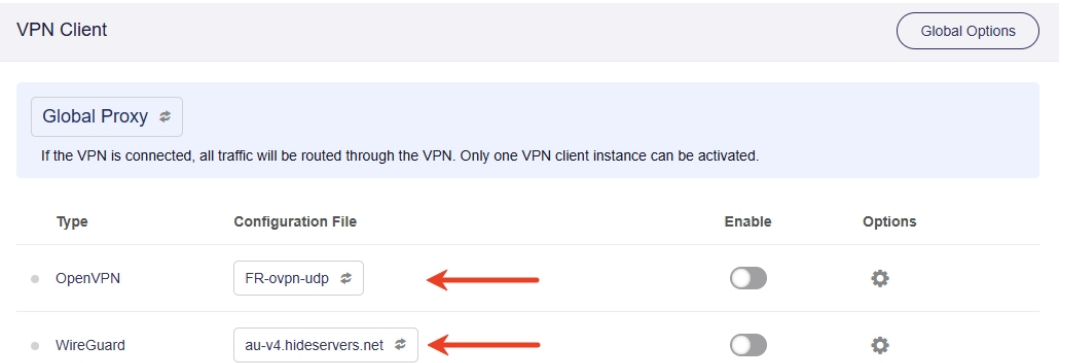
Cuando el enrutador está configurado como un cliente VPN activo, el panel de VPN muestra detalles de la conexión VPN, como la dirección del servidor, estadísticas de tráfico, IP virtual del cliente y registro de conexión. También le permite configurar ajustes avanzados como Bloquear tráfico que no sea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

8.1 Cliente VPN

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

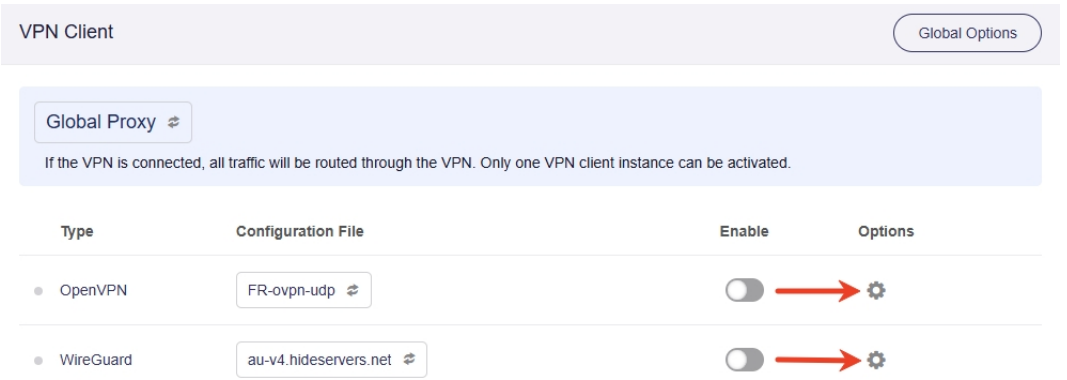


Una vez cargado, su configuración se mostrará en el **Archivo de configuración** columna. Si tiene varios archivos de configuración cargados, puede cambiar de archivo haciendo clic en el cuadro.

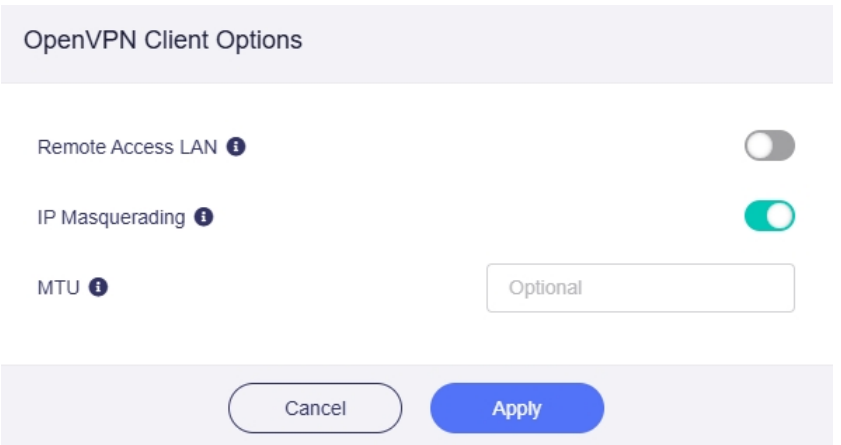


8.1.1 Opciones del cliente

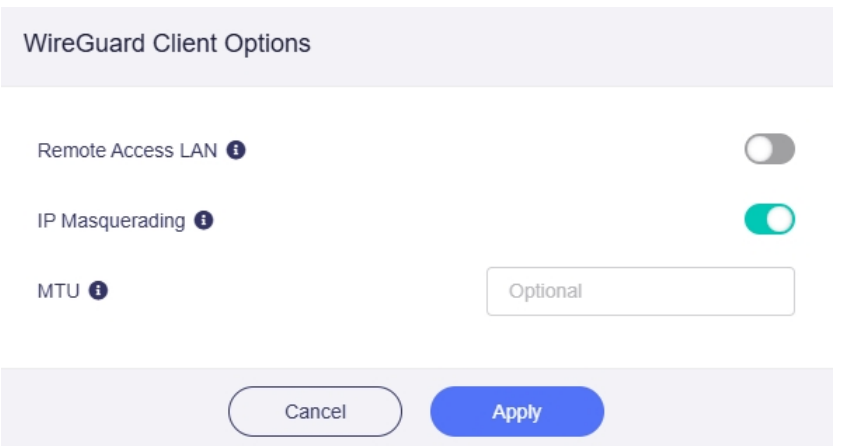
Haga clic en el ícono de ajustes a la derecha para acceder a las opciones del cliente OpenVPN o WireGuard.



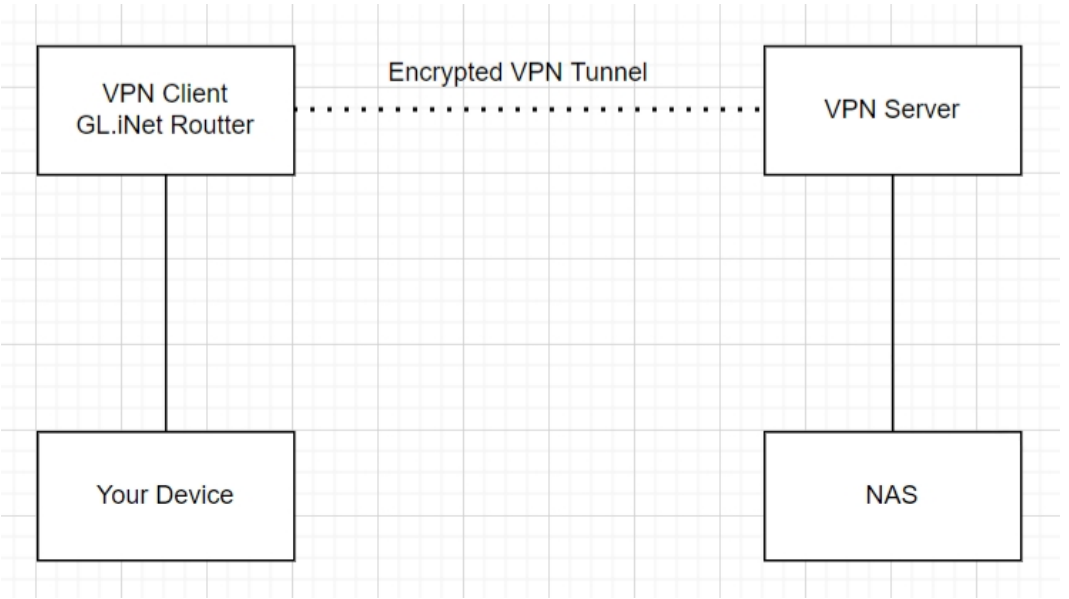
Las Opciones del cliente OpenVPN se muestran de la siguiente manera.



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



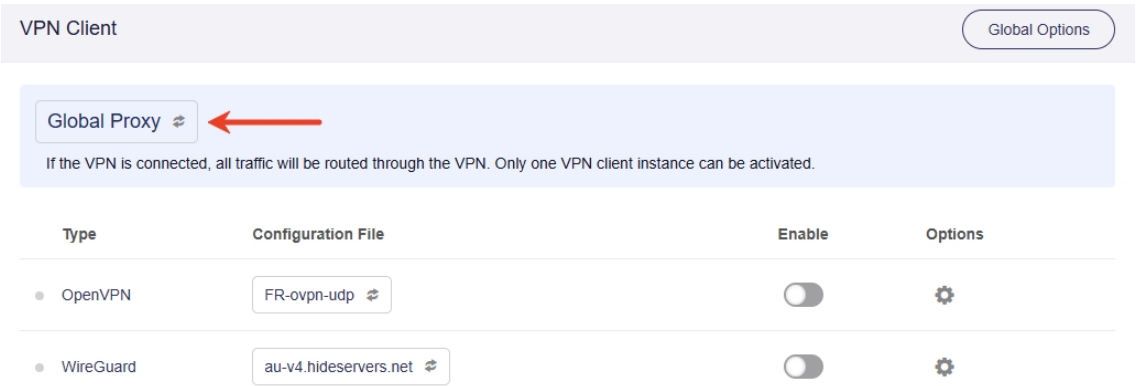
- **LAN de acceso remoto**: si está habilitado, se permitirá el acceso remoto a este enrutador y sus dispositivos LAN a través de VPN. El servidor VPN debe anunciar una ruta a la subred LAN de este enrutador.
  Por ejemplo, como se muestra en el siguiente diagrama, el enrutador GL.iNet se ejecuta como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



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

8.1.2 Modo de política

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



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

1. **Proxy global**

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

2. **Modo de política**

   Este modo se puede dividir en tres políticas.

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

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

   - **Según el dispositivo cliente**

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

   - **Según la VLAN**

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

3. **Modo de ruta**

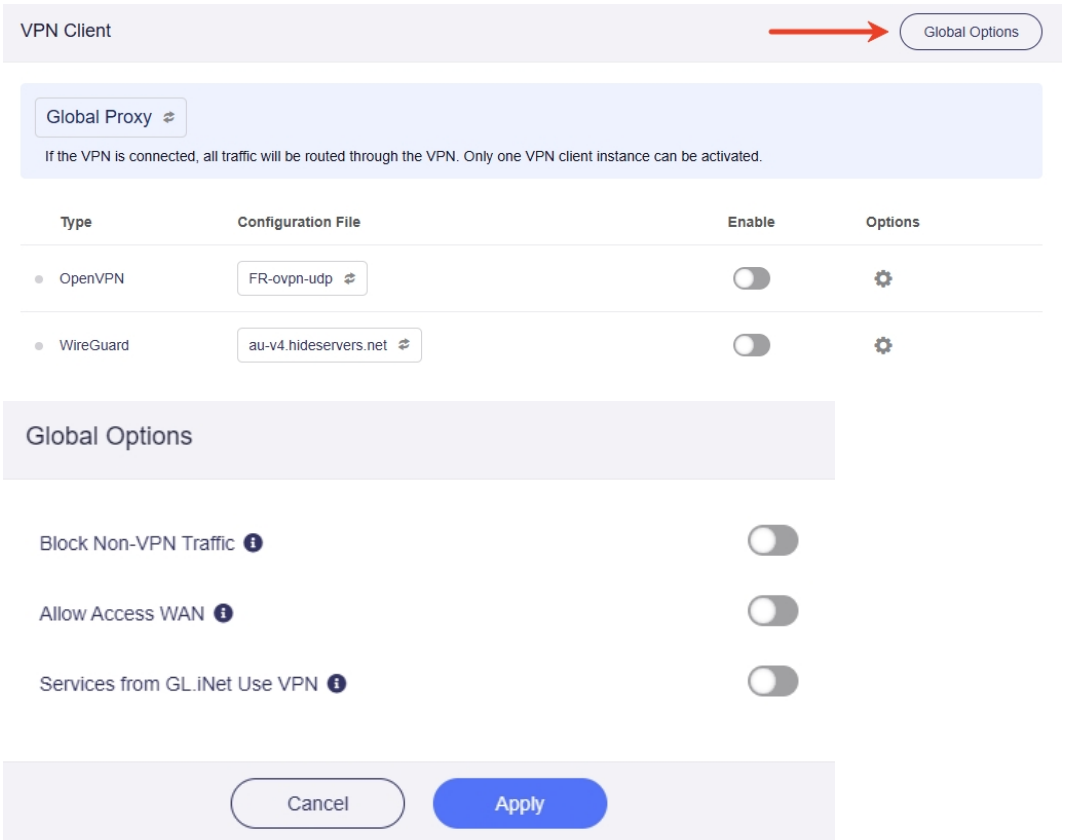
   - **Detección automática**

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

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

8.1.3 Opciones globales

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



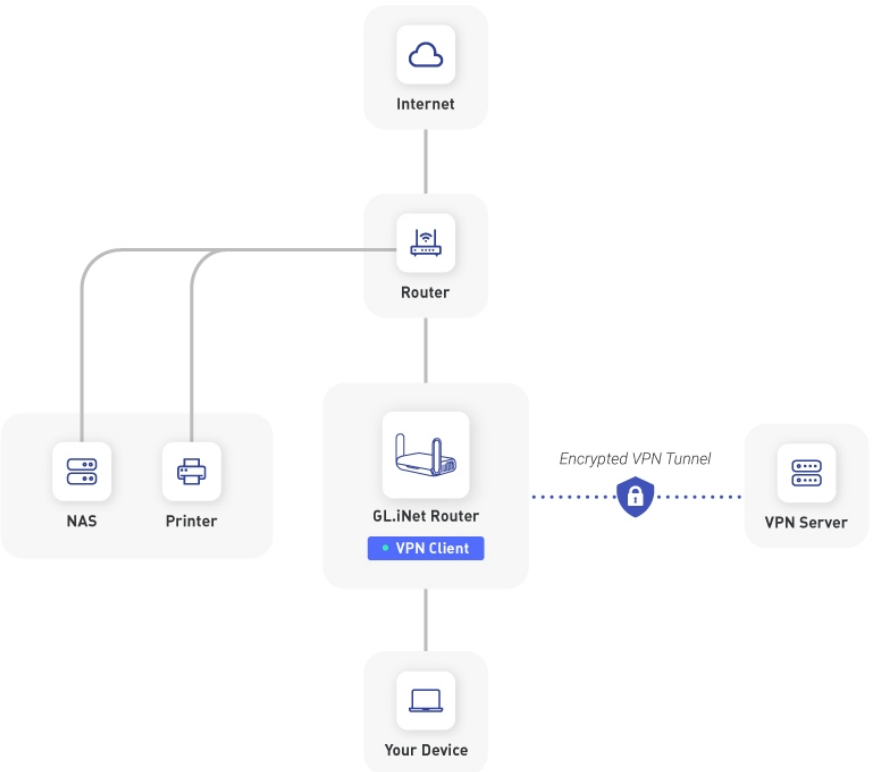
- **Bloquear tráfico que no sea VPN**: si está habilitado, todo el tráfico de Internet se fuerza a pasar exclusivamente a través del túnel VPN y no se puede enrutar a través de otras interfaces como la WAN del ISP local. Si la conexión VPN se cae inesperadamente, todo el tráfico de Internet se bloquea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

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

  a. Fuga de DNS
  b. Fuga de IPv6

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

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



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

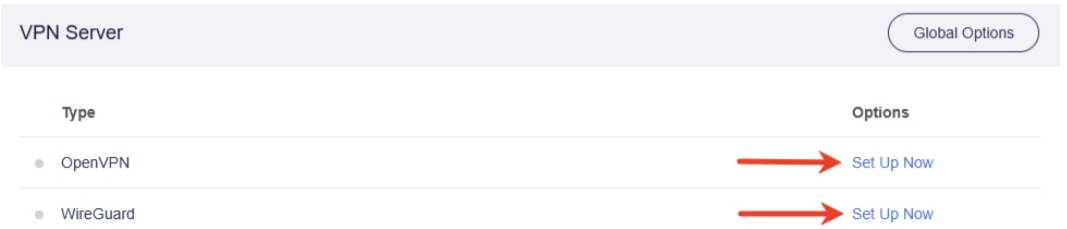
Esta opción está diseñada principalmente para permitir que los clientes accedan a dispositivos dentro de la subred ascendente. Sin embargo, el enrutador no puede distinguir el tráfico de subred ascendente del tráfico normal de Internet. Si los dispositivos cliente acceden a los recursos directamente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

tráfico que no sea VPN son mutuamente excluyentes y no se pueden habilitar simultáneamente.

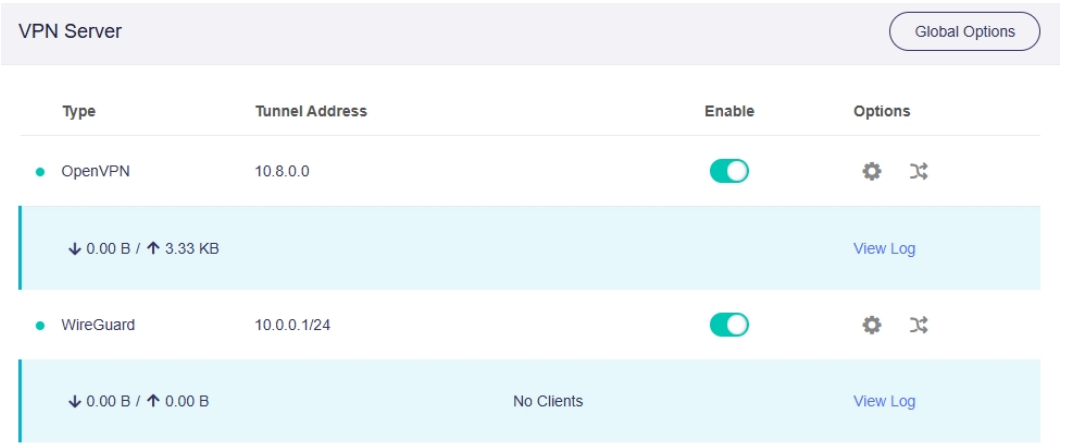
- **Servicios de GL.iNet usan VPN**: si están habilitados, los servicios GoodCloud, DDNS y rtty transmitirán paquetes a través de túneles VPN. Esta opción está deshabilitada de forma predeterminada, ya que estos servicios normalmente requieren la dirección IP real del dispositivo para funcionar correctamente.

8.2 Servidor VPN

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

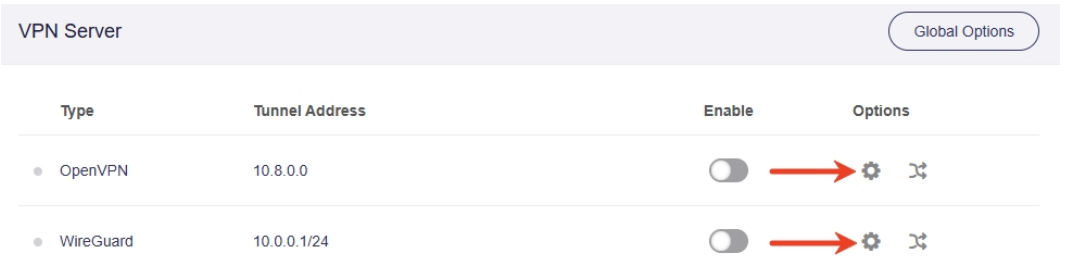


Después de habilitar el servidor OpenVPN o el servidor WireGuard, la página mostrará el estado del servidor de la siguiente manera.

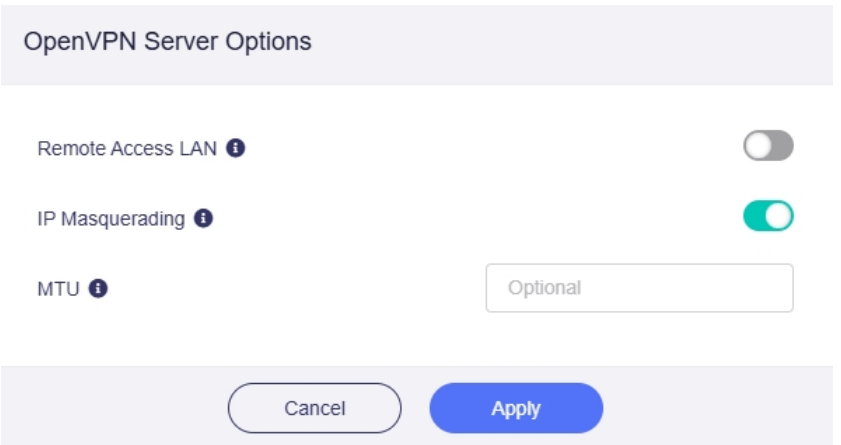


8.2.1 Opciones del servidor

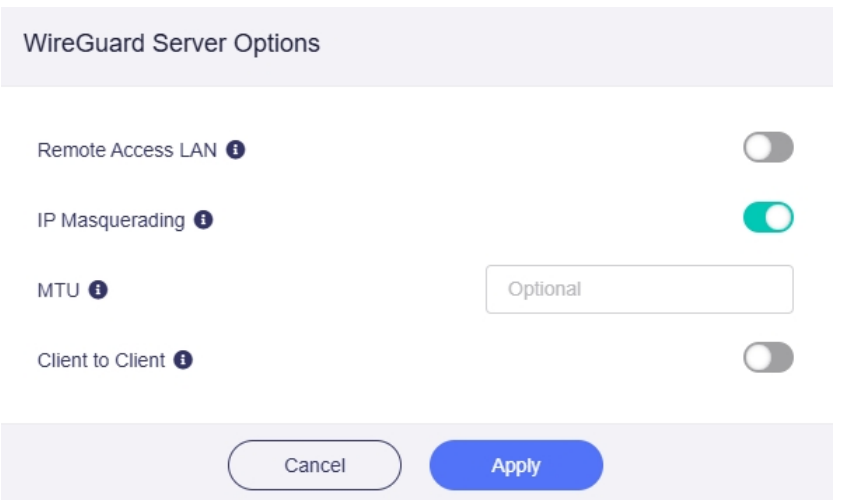
Haga clic en el ícono de ajustes a la derecha para acceder Opciones de servidor OpenVPN o WireGuard.



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



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

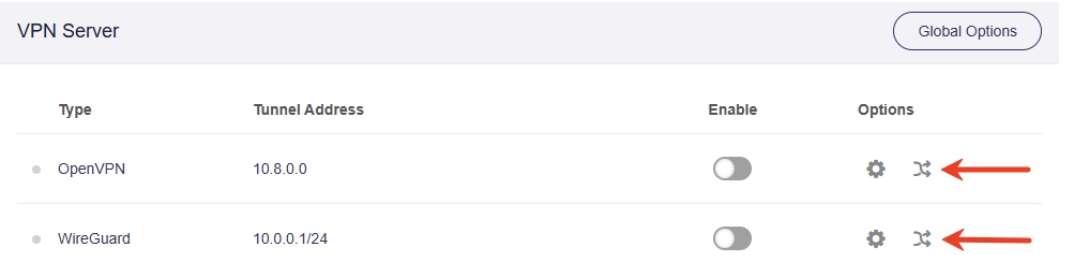


- **LAN de acceso remoto**: Si está habilitado, se puede acceder a los recursos dentro de la subred LAN del servidor a través de la VPN túnel.

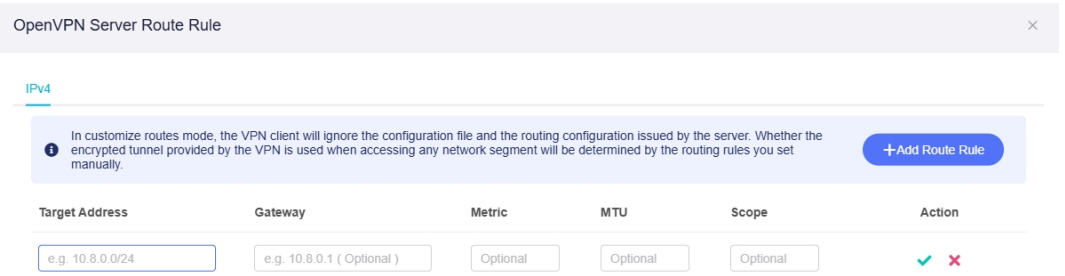
- **Enmascaramiento de IP**: si está habilitado, las direcciones IP de origen de los clientes LAN se reescribirán en la IP del túnel VPN del enrutador. Deshabilite esto solo para configuraciones de sitio a sitio donde el par remoto conoce sus subredes LAN.
- **MTU**: abreviatura de Unidad de transmisión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

8.2.2 Regla de ruta del servidor

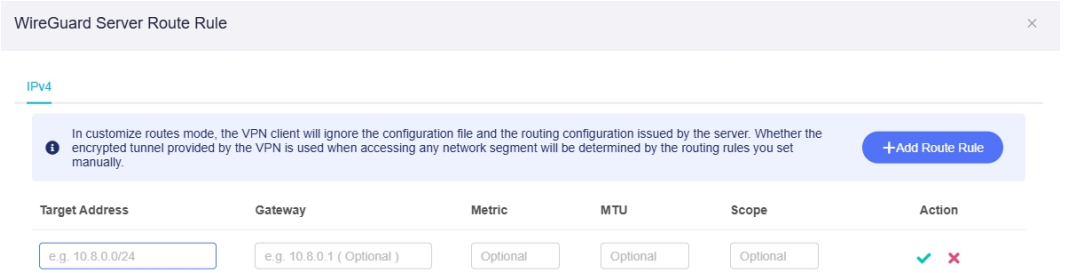
Haga clic en el icono de ruta a la derecha para personalizar las reglas de ruta OpenVPN o WireGuard según sea necesario.



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



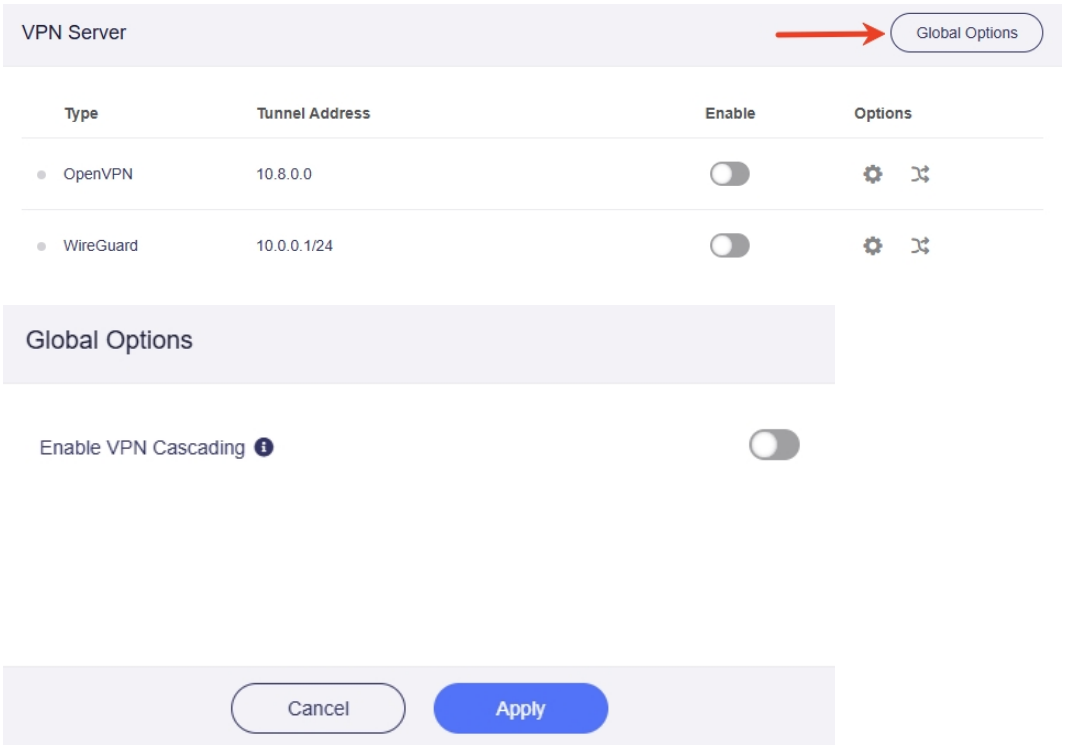
La regla de ruta del servidor WireGuard se muestra de la siguiente manera. Haga clic en **Agregar regla de ruta**, ingrese la **Dirección de destino** y **puerta de enlace**, luego haga clic en el ícono de verificación verde para aplicar.



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

8.2.3 Opciones globales

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



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

Capítulo 9

Configurar el servidor VPN

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

9.1 Configurar el servidor OpenVPN

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

9.1.1 Preparación

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

   Haz clic aquí para verificar si tu proveedor de servicios de Internet (ISP) te asigna una dirección IP pública. De lo contrario, su enrutador no se puede configurar como servidor OpenVPN.

   Métodos alternativos:

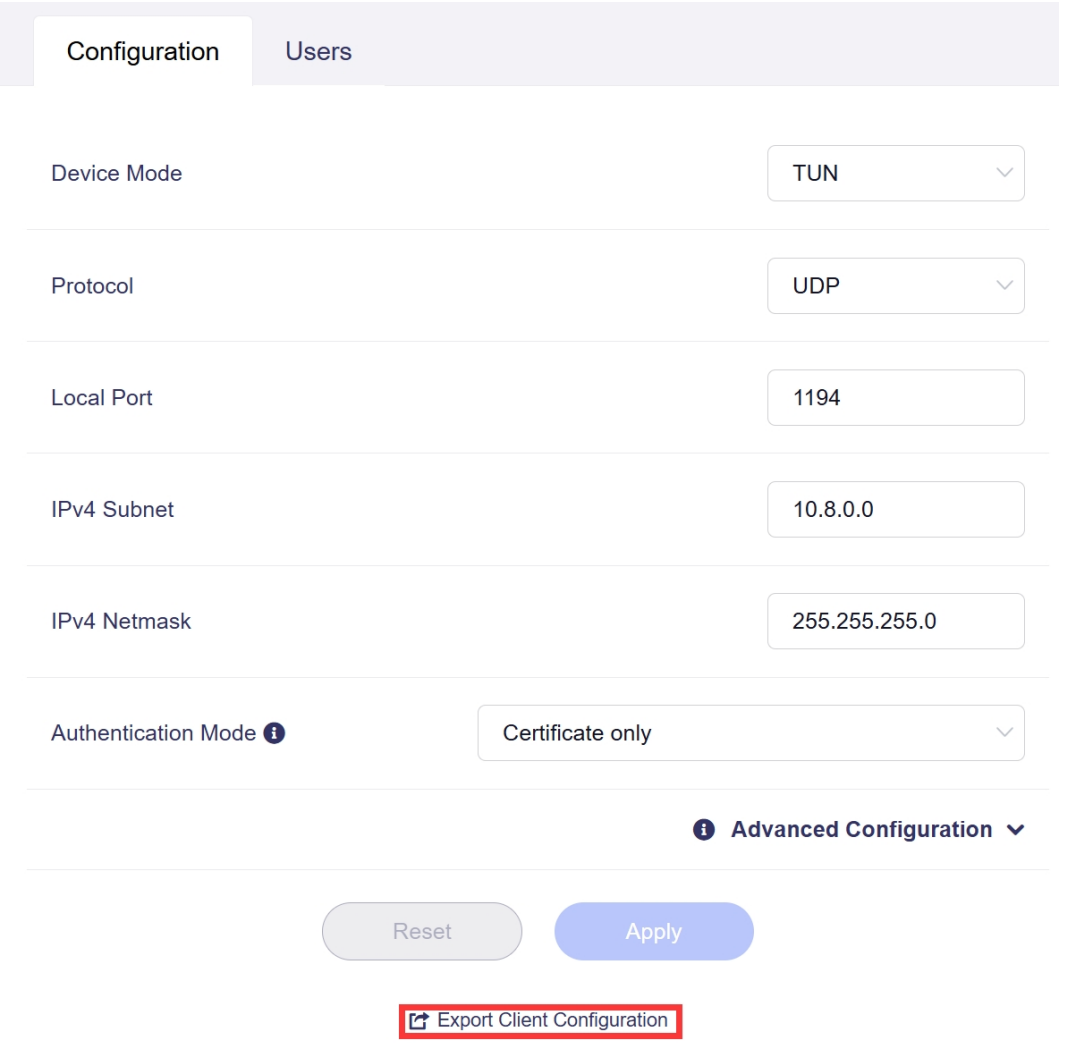
   - Si tiene un enrutador principal ascendente de su enrutador GL.iNet, inicie sesión en él y verifique que tenga una dirección IP pública asignada por su ISP.
   - Solicite a su ISP una dirección IP pública. Esto puede generar un cargo adicional.

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

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

9.1.2 Pasos de configuración

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



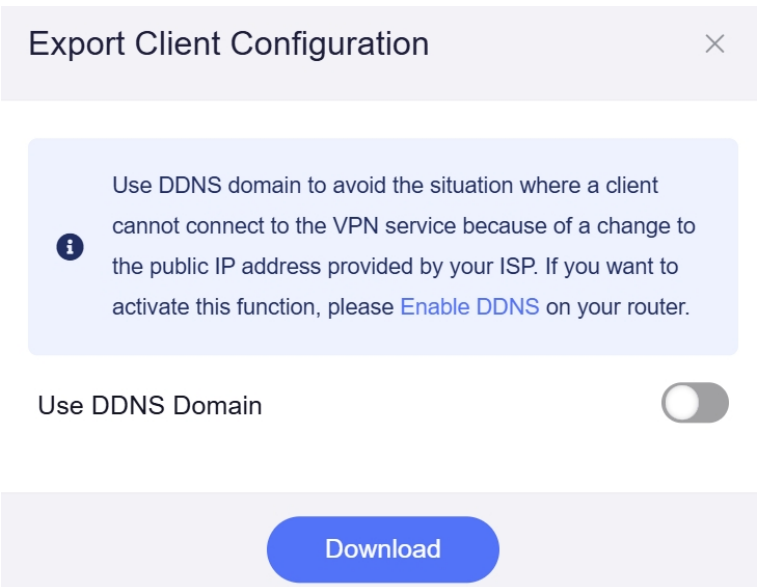
- **Dispositivo Modo**: TAP-S2S o Tun. Consulte aquí para las diferencias.
- **Protocolo**: UDP o TCP. Consulte aquí para las diferencias.
- **Modo de autenticación**: Esto determina el método de autenticación utilizado cuando el cliente se conecta al servidor. Hay tres opciones:

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

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

3. Exportar configuración del cliente.

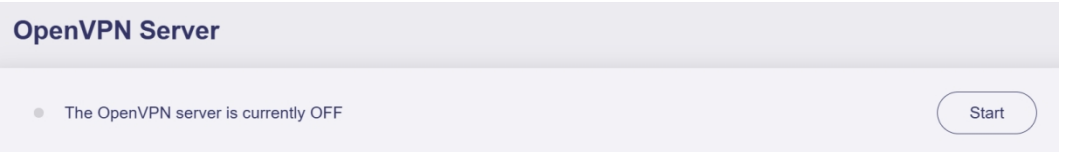
   Después de hacer clic **Exportar configuración del cliente** en la parte inferior de la pestaña Configuración (o aplicar la configuración modificada), aparecerá una ventana como la siguiente. Haga clic en **Descargar** para exportar la configuración.



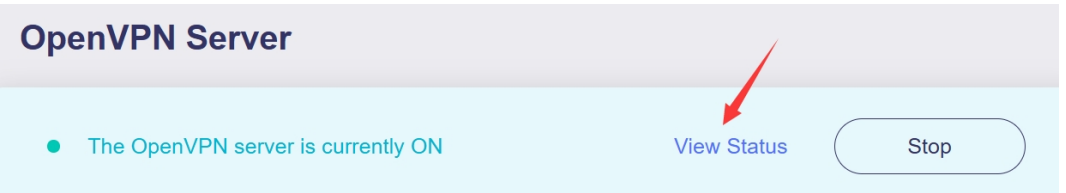
Consejo: Si su IP pública dirección cambia con frecuencia, vaya a **APLICACIONES** > **DNS dinámico** y habilitar DDNS. Luego puede usar el dominio DDNS como su dirección de servidor.

4. Inicie OpenVPN servidor.

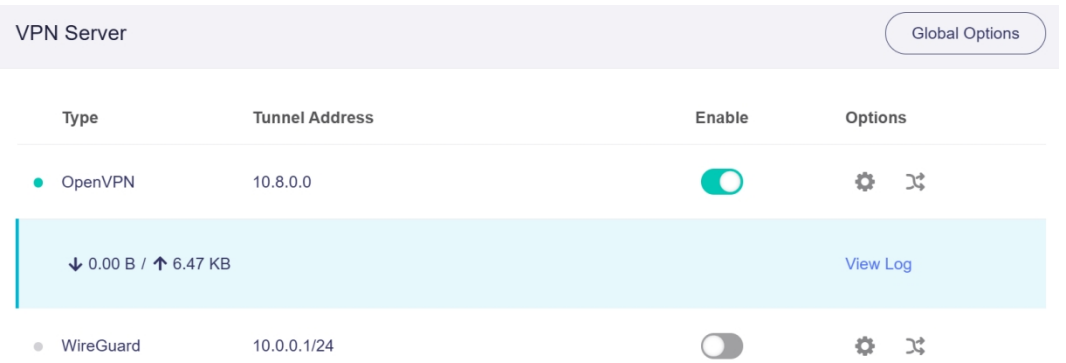
   En la página **Servidor OpenVPN**, haga clic en **Iniciar** en la esquina superior derecha para iniciar el servidor.



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



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



9.1.3 Solución de problemas

Si la conexión falla, existen varias razones comunes:

- El servidor VPN no tiene una dirección IP pública. 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.

9.2 Configurar el servidor WireGuard

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

9.2.1 Preparación

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

   Haga clic aquí para verificar si su proveedor de servicios de Internet le asigna una dirección IP pública. De lo contrario, su enrutador no se puede configurar como servidor WireGuard.

   Alternativa métodos:

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

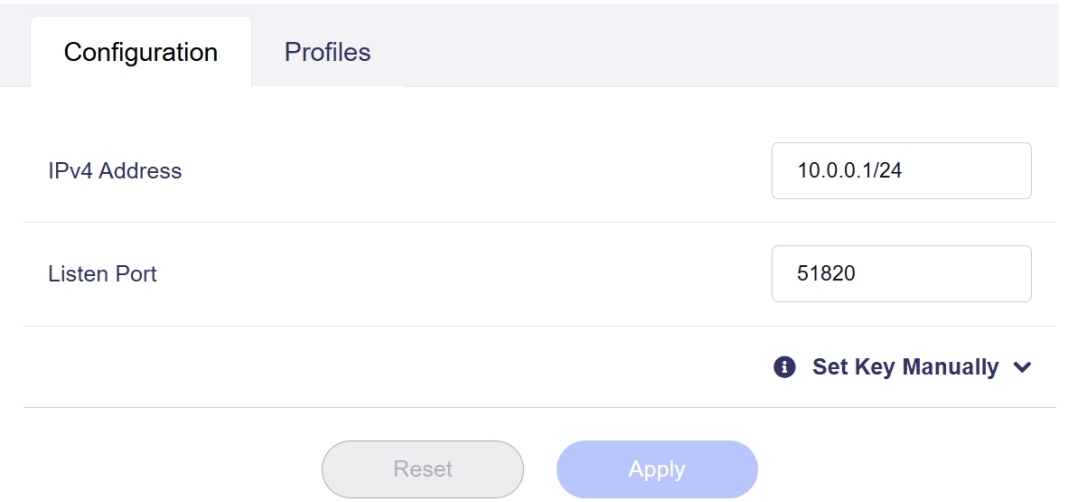
2. **Confirme si se requiere reenvío de puertos**

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

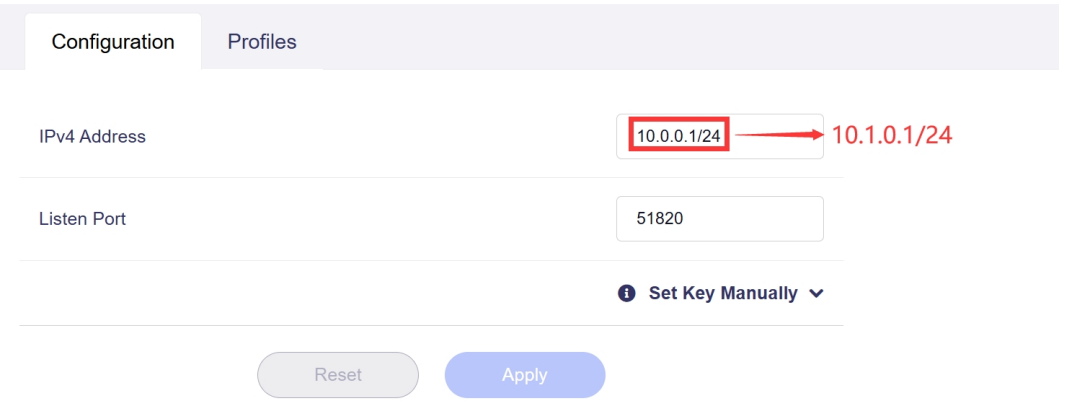
9.2.2 Pasos de configuración

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

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

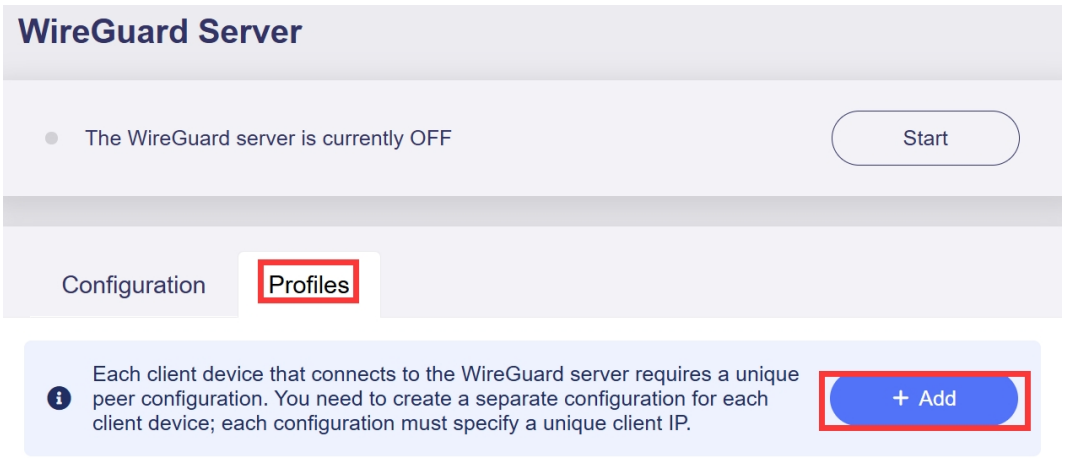


   Si la dirección IPv4 entra en conflicto con la puerta de enlace de su enrutador ascendente, modifique la dirección IPv4 a otra una (por ejemplo, **10.1.0.1/24**) y haga clic en **Aplicar**. Asegúrese de que se incluya la notación CIDR "/24" para evitar problemas de conectividad.

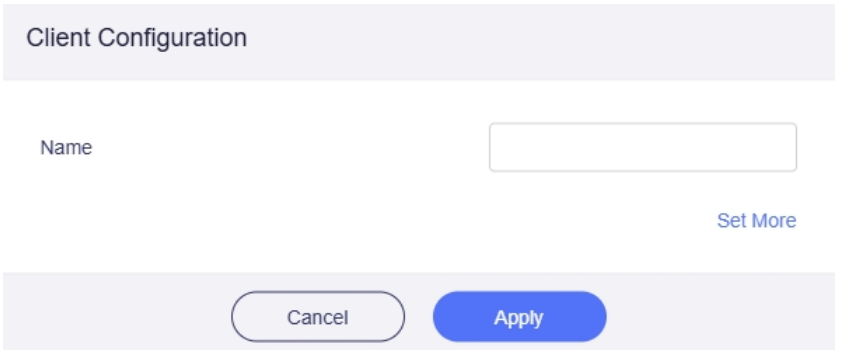


3. Agregue un perfil.

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



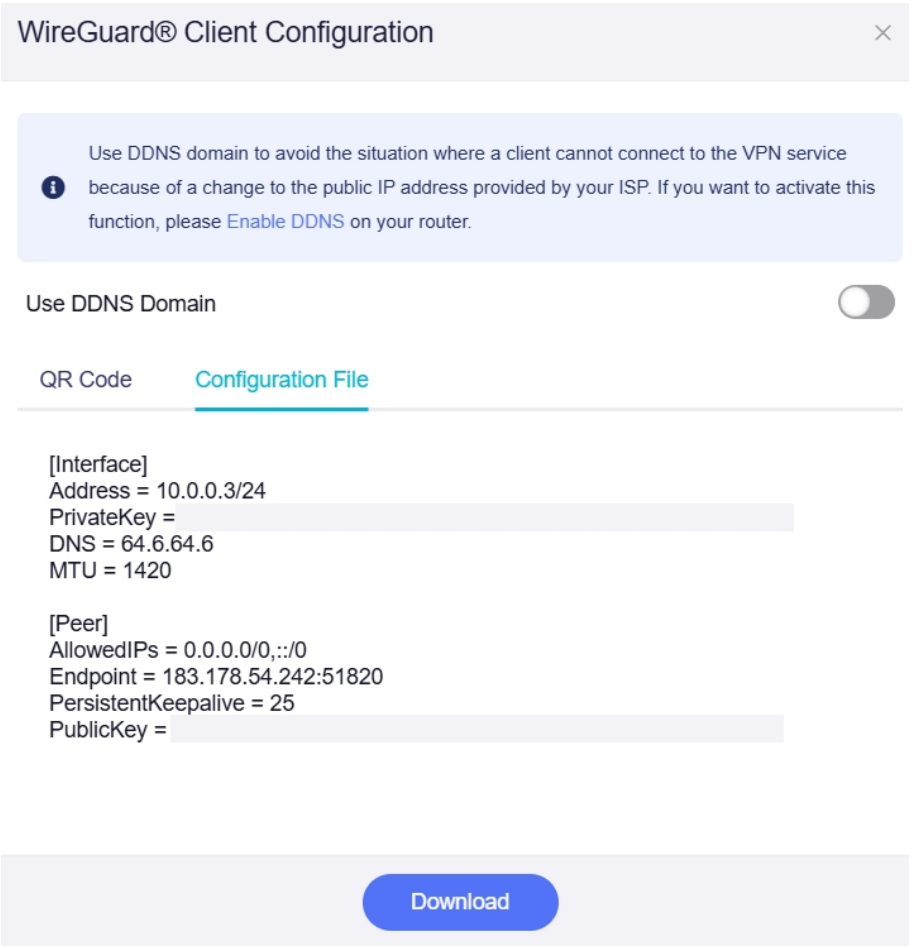
Establezca un nombre descriptivo y haga clic en **Aplicar** para continuar.



4. Descargar configuración.

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

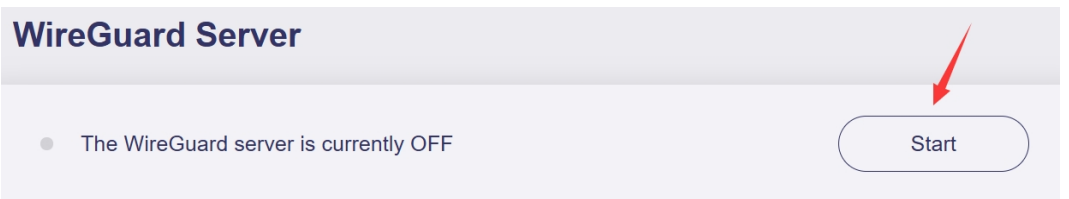
   - **Código QR**: Adecuado para dispositivos (por ejemplo, teléfonos inteligentes, tabletas, computadoras portátiles) con la aplicación WireGuard instalada. Si desea configurar un dispositivo específico como cliente WireGuard, simplemente abra la aplicación WireGuard y escanee el código QR para importar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



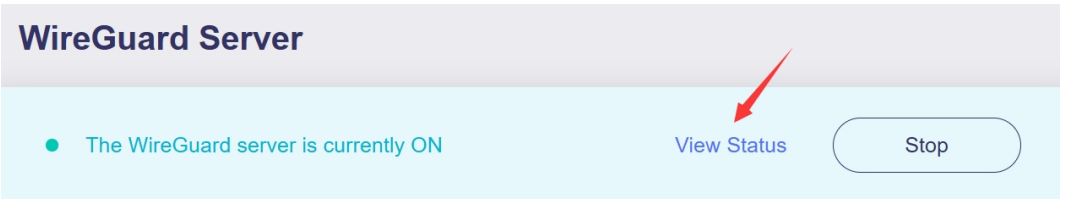
Consejo: Si su IP pública dirección cambia con frecuencia, vaya a **APLICACIONES** > **DNS dinámico** y habilite DDNS. Entonces puedes usar el dominio DDNS como su dirección de servidor.

5. Inicie WireGuard servidor.

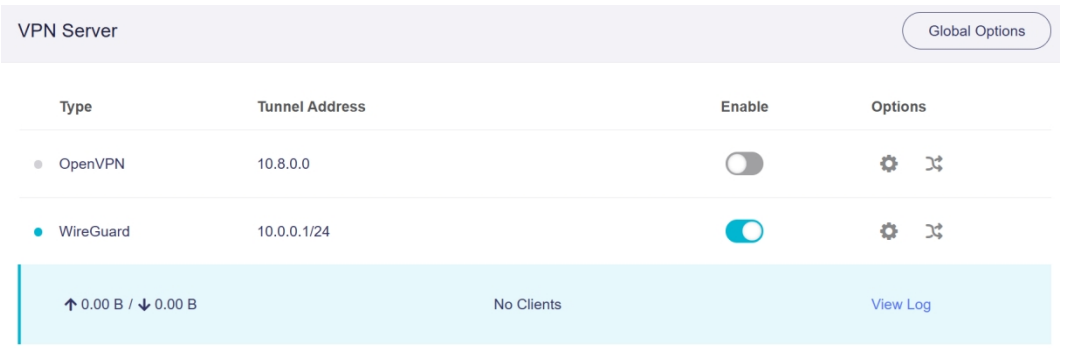
   En la página **Servidor WireGuard**, haga clic en el botón **Iniciar** en la esquina superior derecha para iniciar el servidor.



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



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



9.2.3 Solución de problemas

Si la conexión falla, existen varias razones comunes:

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

Capítulo 10

Configurar el cliente VPN

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

10.1 Configurar el cliente OpenVPN

10.1.1 Preparación

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

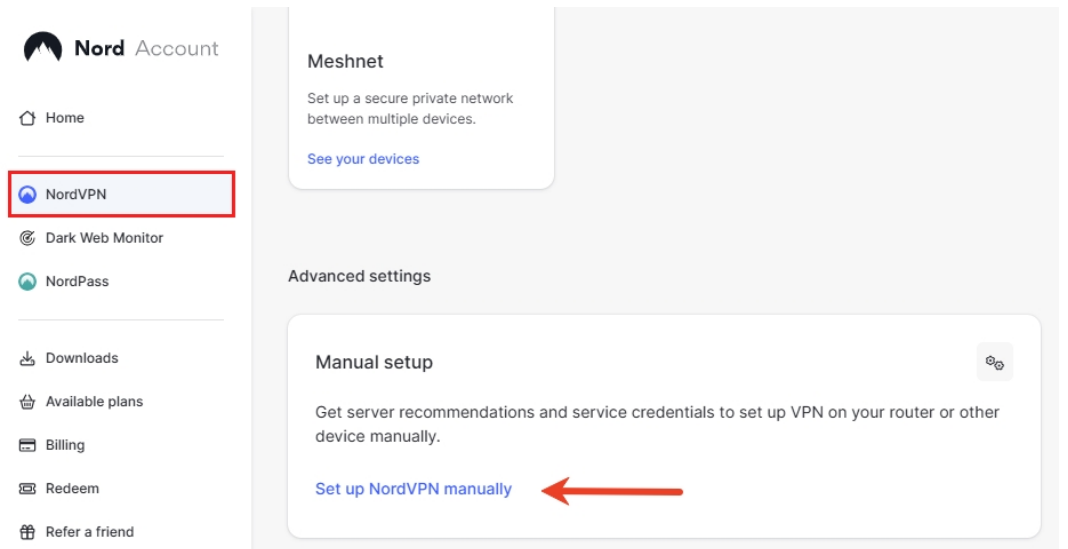
Siguiente, visite el sitio web oficial del proveedor de servicios VPN al que se suscribió y obtenga las credenciales del servicio o el archivo de configuración. Si no sabe cómo obtener el archivo de configuración, consulte este enlace o póngase en contacto con su soporte.

10.1.2 Configurar NordVPN

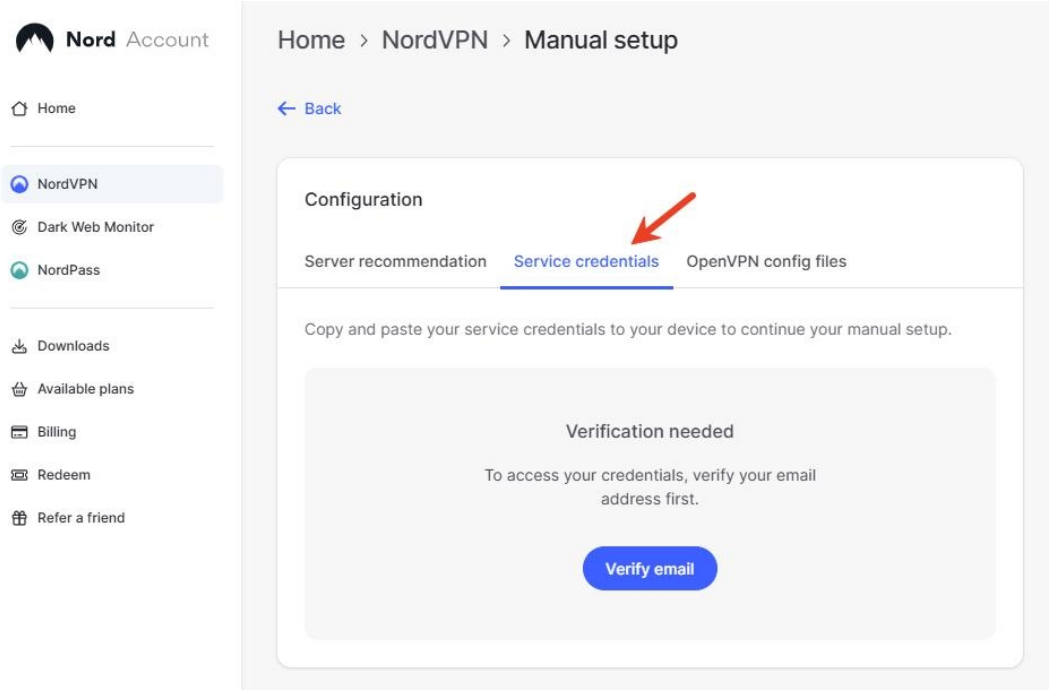
NordVPN está integrado en el panel de administración GL.iNet web . Puede adquirir archivos de configuración para todos los servidores NordVPN introduciendo las credenciales de su cuenta (obtenidas del Panel de NordVPN) en el panel de administración web del enrutador o en la aplicación móvil GL.iNet ,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

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

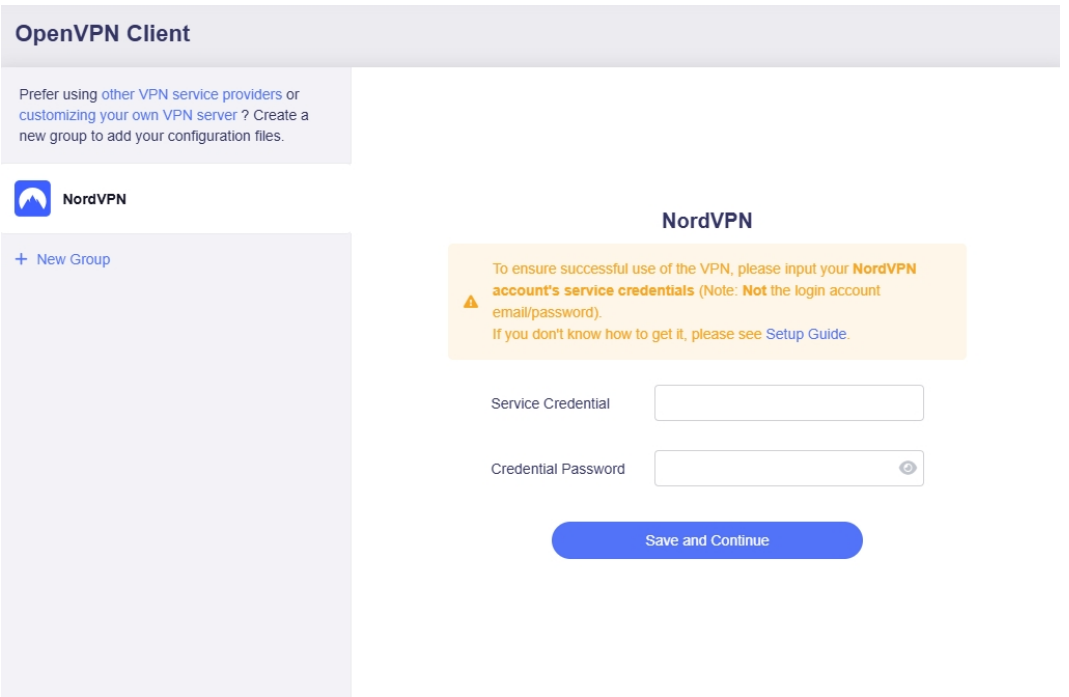
1. Inicie sesión en su cuenta web de NordVPN aquí.
2. Oen el Panel de control de Nord, haga clic en **NordVPN**, luego haga clic en **Configurar NordVPN manualmente**.



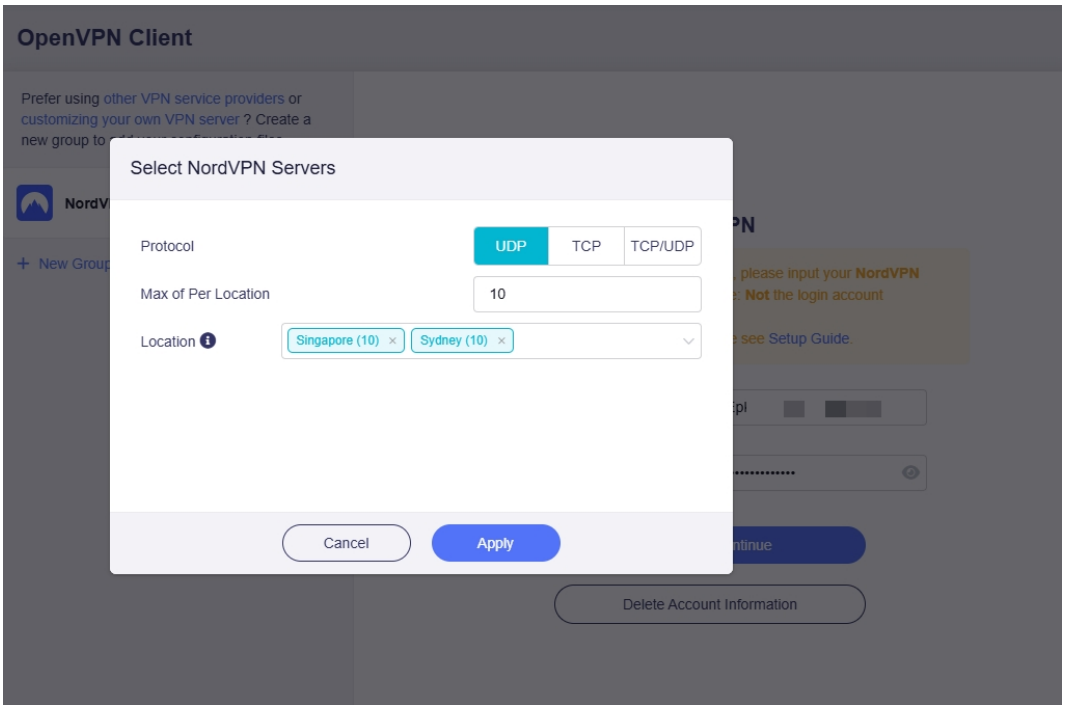
Encontrará las **credenciales de servicio**. Cópialos para usarlos más adelante.



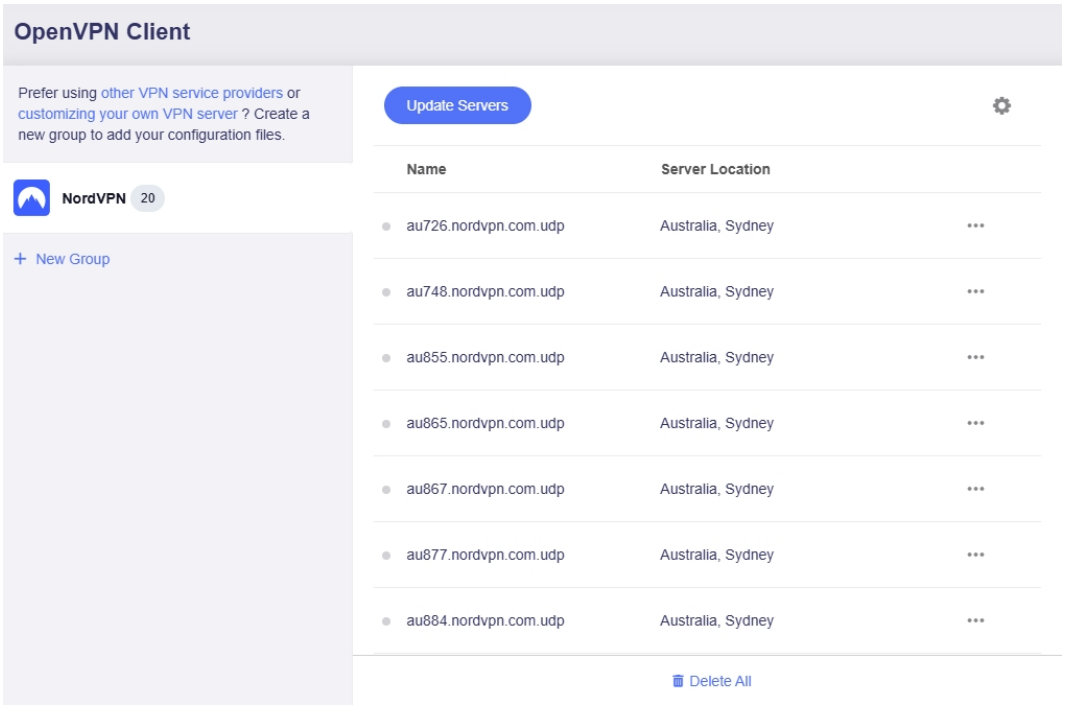
3. Inicie sesión en el panel de administración web de su enrutador y navegue hasta **VPN** > **Cliente OpenVPN** > **NordVPN**. Introduzca las credenciales del servicio (Nota: NO es el correo electrónico ni la contraseña de la cuenta de inicio de sesión), luego haga clic en **Guardar y continuar**.



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

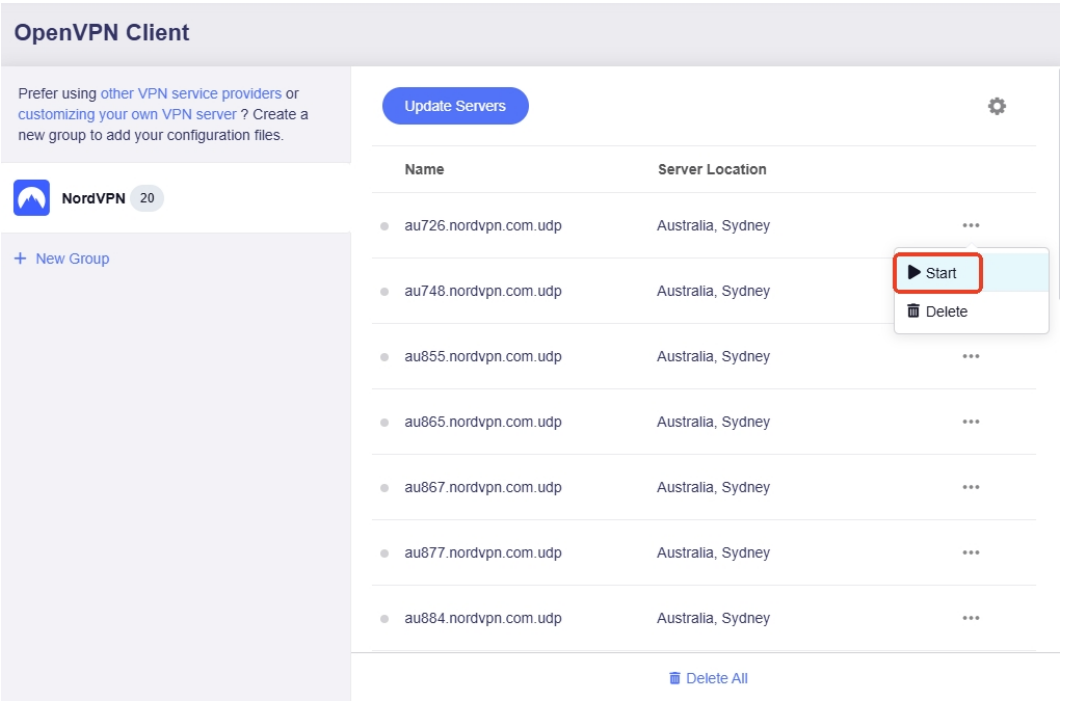


Descargará archivos de configuración.

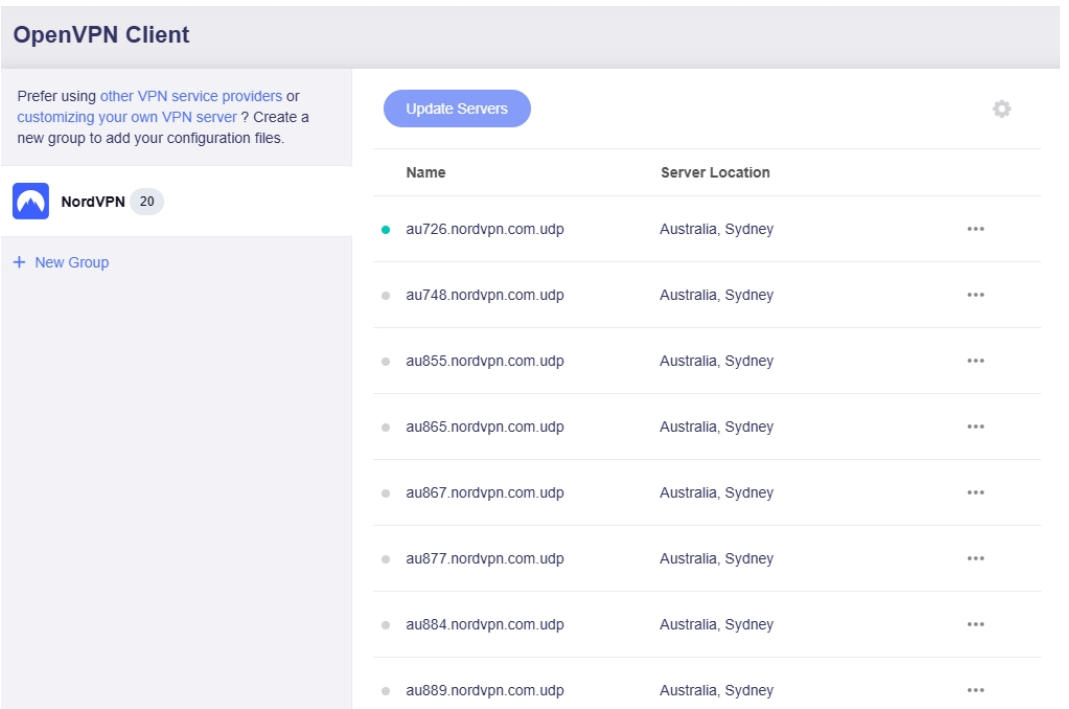


5. Iniciará una conexión.

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



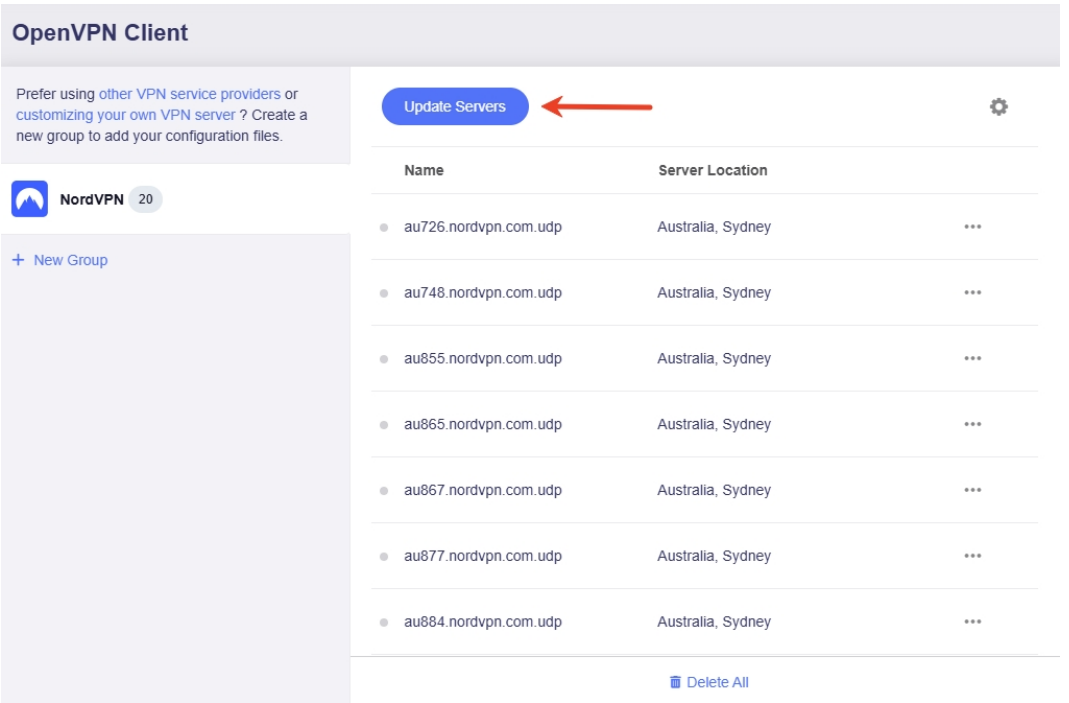
6. Una vez conectado, aparecerá un punto verde junto a el archivo de configuración.



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

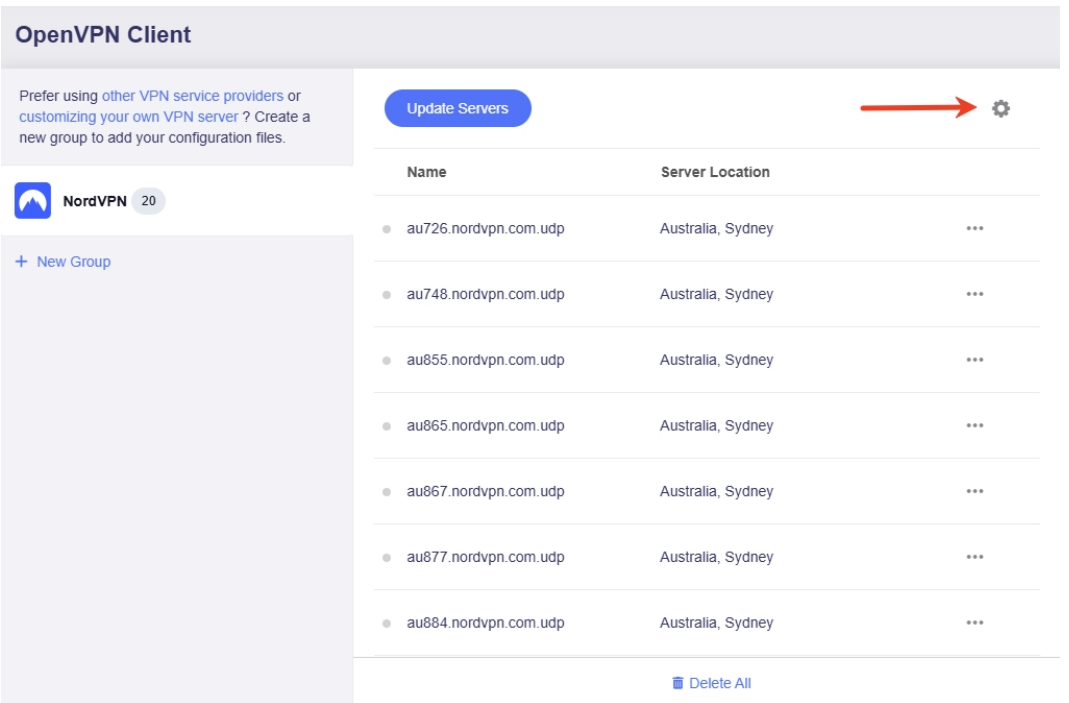
7. Actualizar servidores.

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



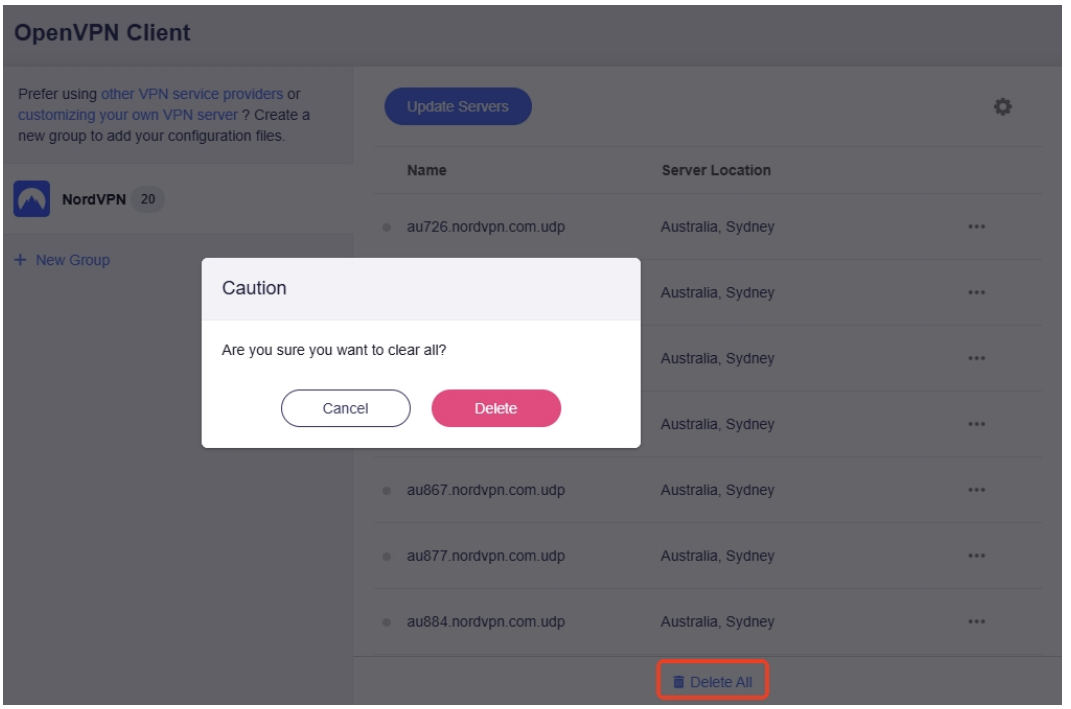
8. Editar credenciales.

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



9. Eliminar todos los archivos.

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

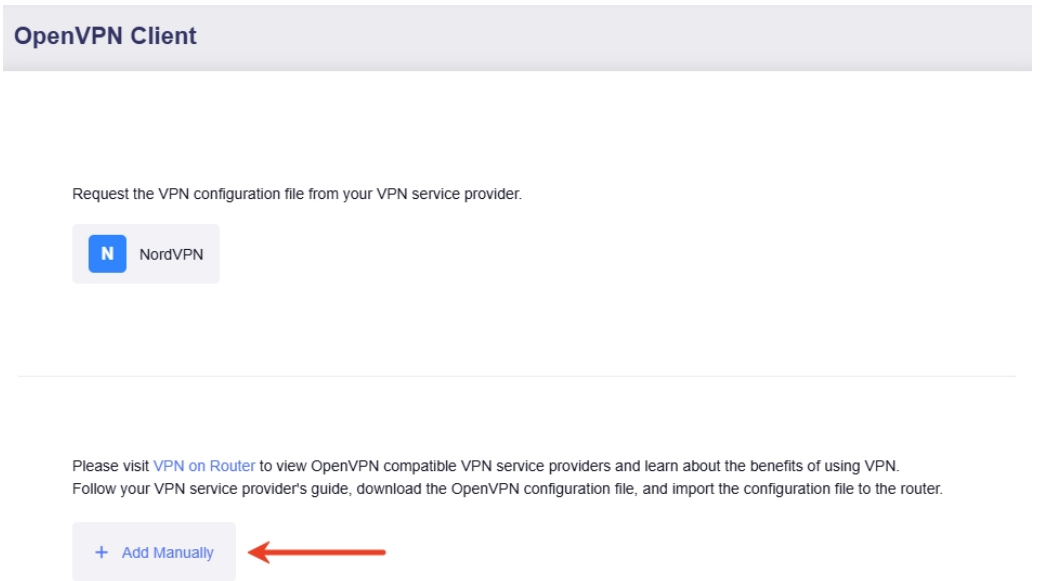


10.1.3 Configurar el cliente OpenVPN manualmente (para otros proveedores)

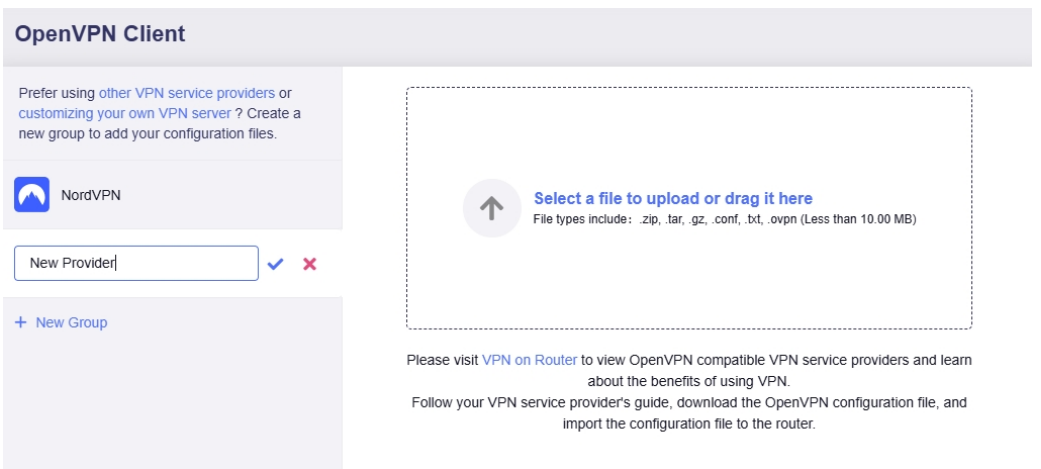
Si su proveedor de servicios OpenVPN no está integrado en nuestro panel de administración, primero visite el sitio web oficial de su proveedor de servicios suscrito para obtener el archivo de configuración. Luego cárguelo en el enrutador para configurar un cliente OpenVPN.

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

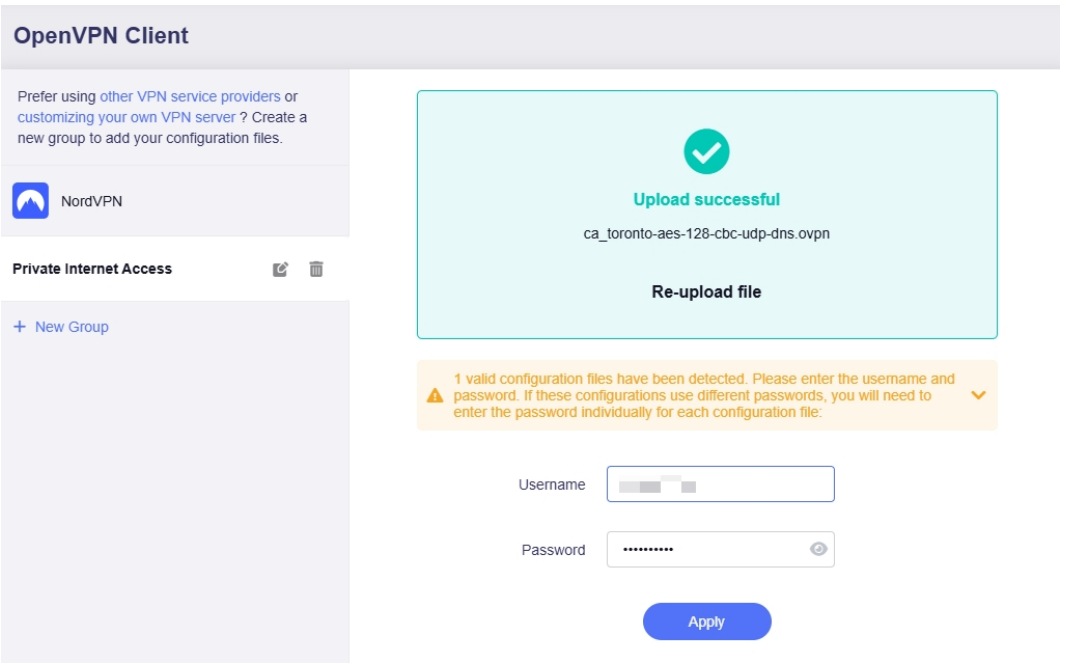
1. Descargue un archivo de configuración del sitio web oficial de Private Internet Access.
2. Inicie sesión en el panel de administración web de su enrutador, navegue hasta **VPN** > **Cliente OpenVPN** y haga clic en **Agregar manualmente**.



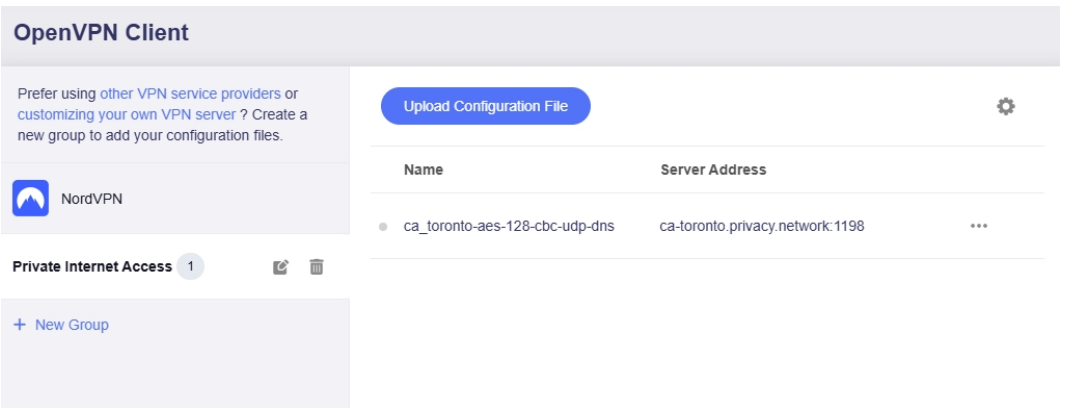
3. Se creará un grupo en la barra lateral izquierda.Establezca un nombre descriptivo para el grupo.



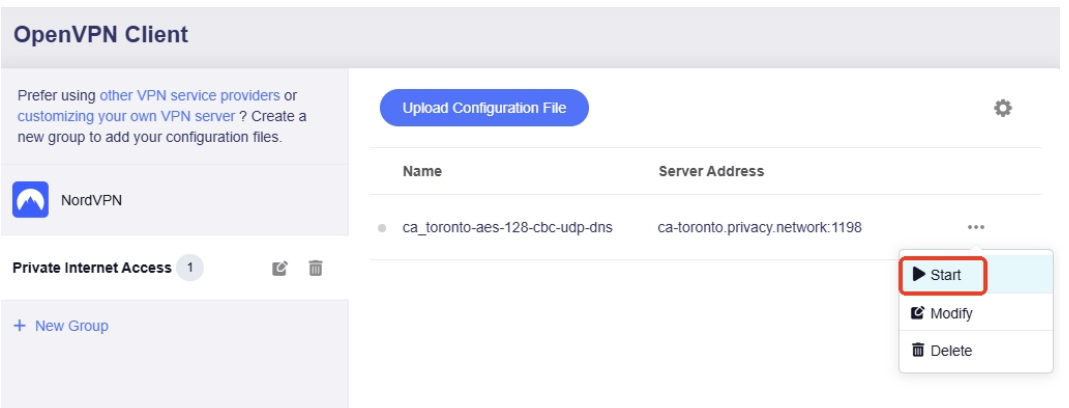
4. Cargue su archivo de configuración OpenVPN. Ingrese las credenciales si es necesario, luego haga clic en **Aplicar**.



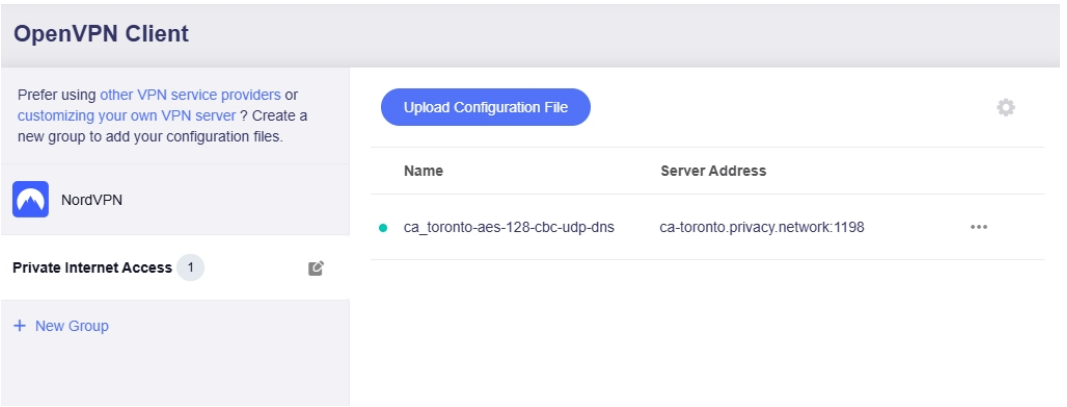
YVerá el archivo de configuración cargado.



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**.

10.2 Configurar el cliente WireGuard

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

- La aplicación móvil integra algunos 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.

10.2.1 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.

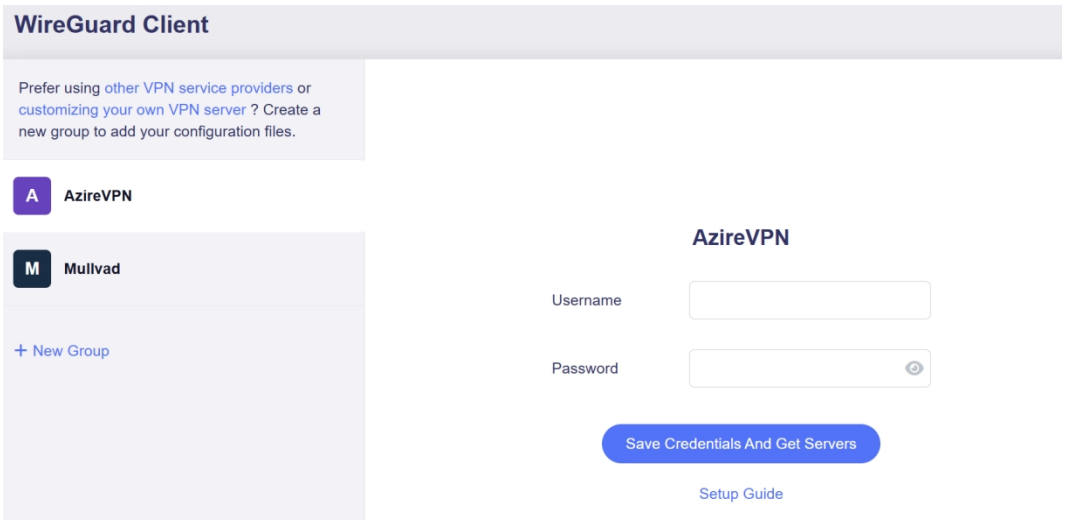
A continuación, sseleccione el proveedor de servicios WireGuard correspondiente a continuación para localizar rápidamente las instrucciones paso a paso.

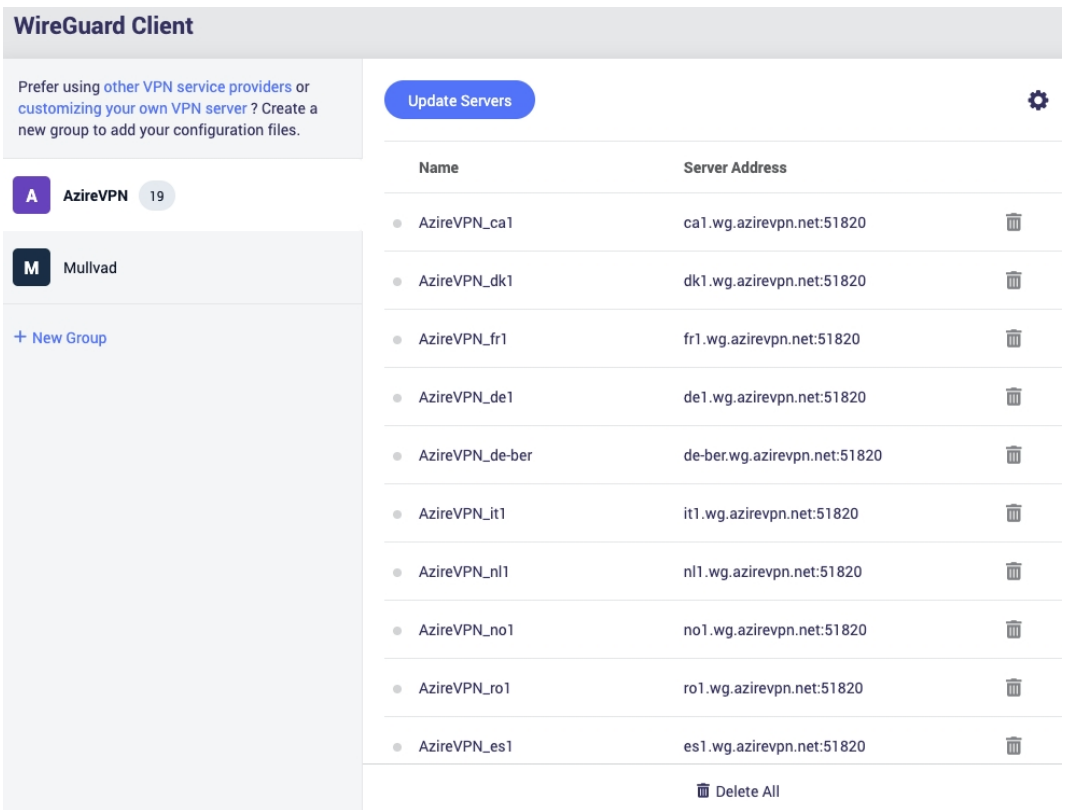
- Configurar AzireVPN
- Configurar Mullvad
- Configurar el cliente WireGuard manualmente (para otros proveedores)

10.2.2 Configurar AzireVPN

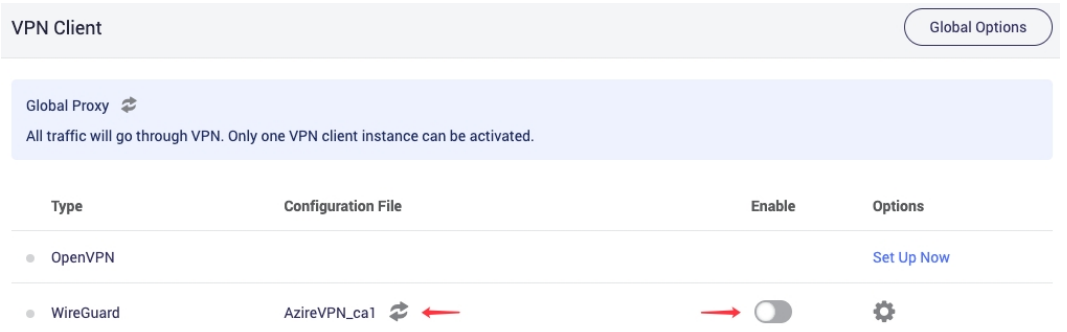
Siga los pasos a continuación para configurar su enrutador como AzireVPN client.

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

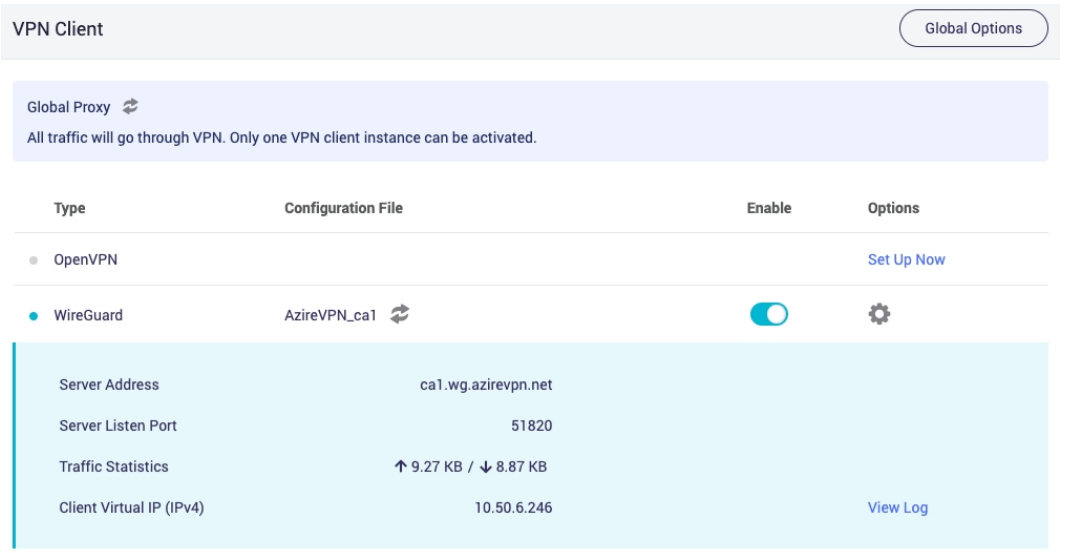




3. Vaya al Panel de VPN para habilitar la conexión.

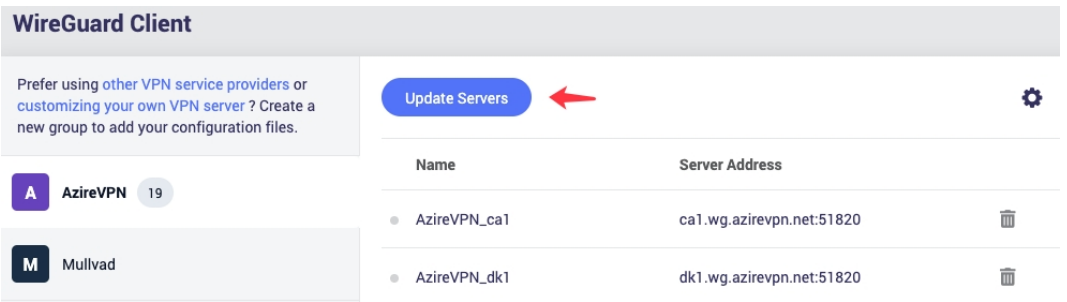


Una vez conectado, debería ver su dirección IP de usuario y la cantidad de bytes enviados/recibidos.



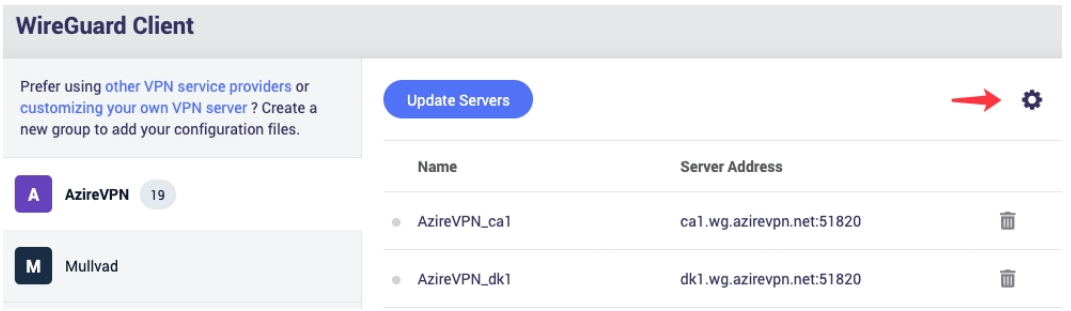
4. Actualice los servidores.

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



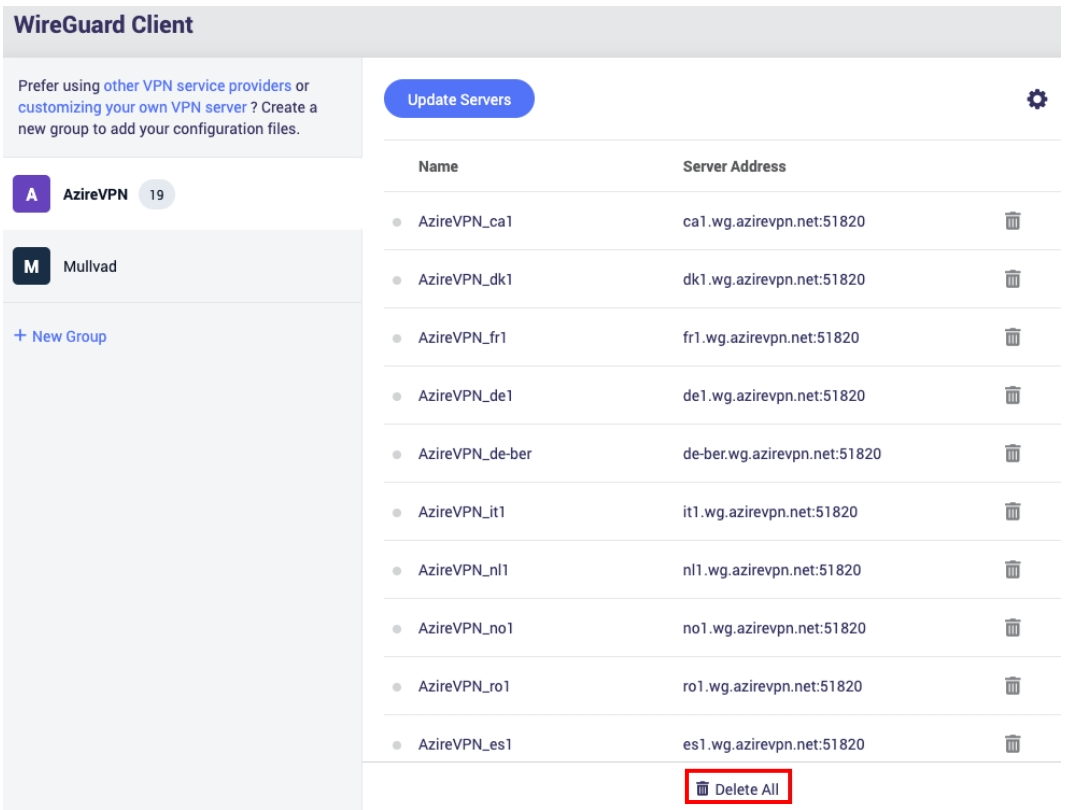
5. Editar credenciales.

   Haga clic el icono de engranaje para editar la credencial.



6. Eliminar todos los archivos.

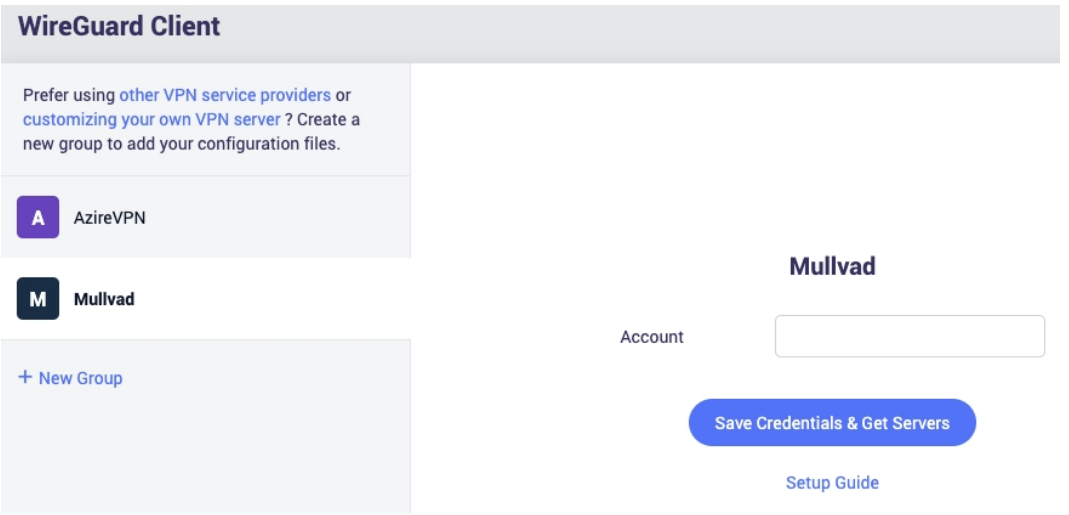
Puede hacer clic en **Eliminar todo** para eliminar todos los archivos de configuración con un solo clic.



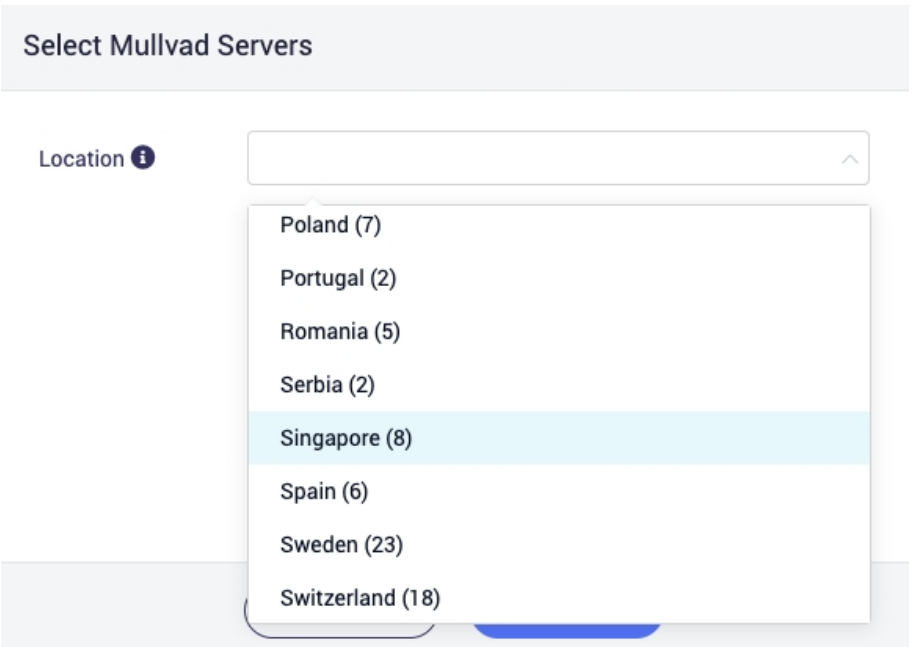
10.2.3 Configurar Mullvad

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

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

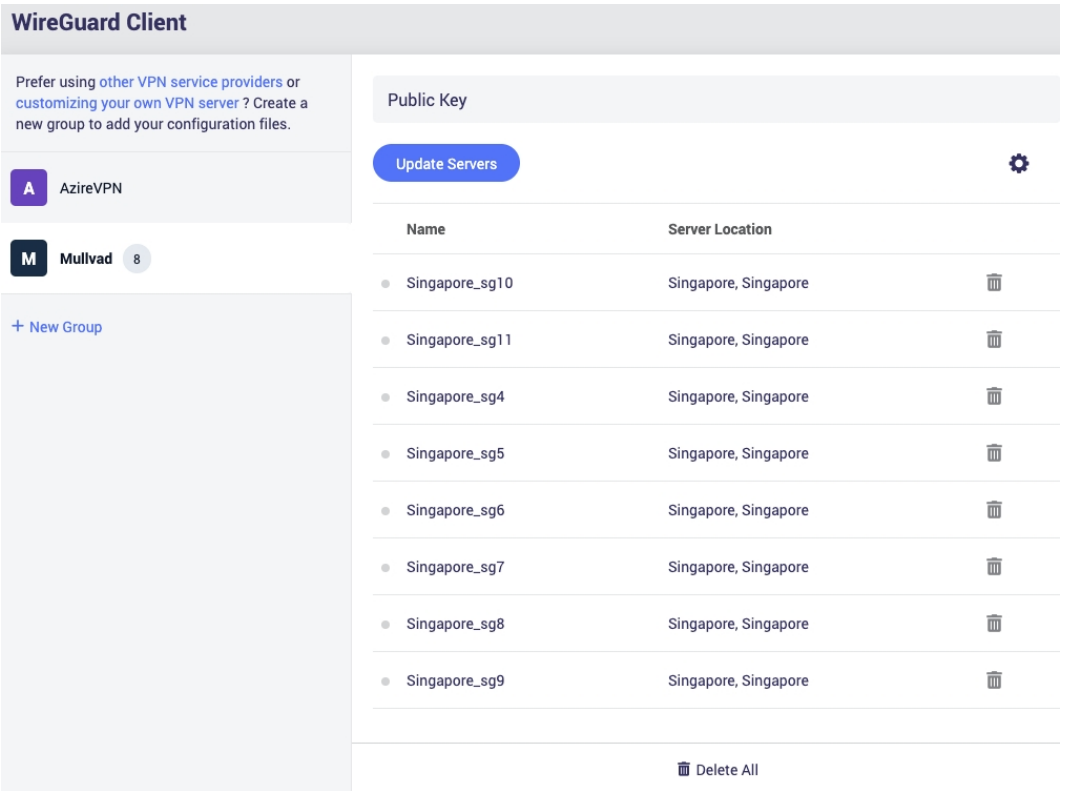


Aparecerá un cuadro de diálogo para seleccionar una ubicación.

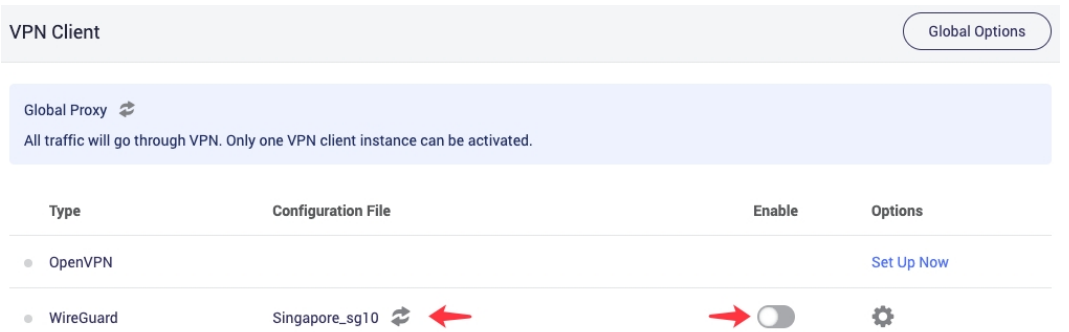


Luego generará los archivos de configuración del servidor de ubicación seleccionado.

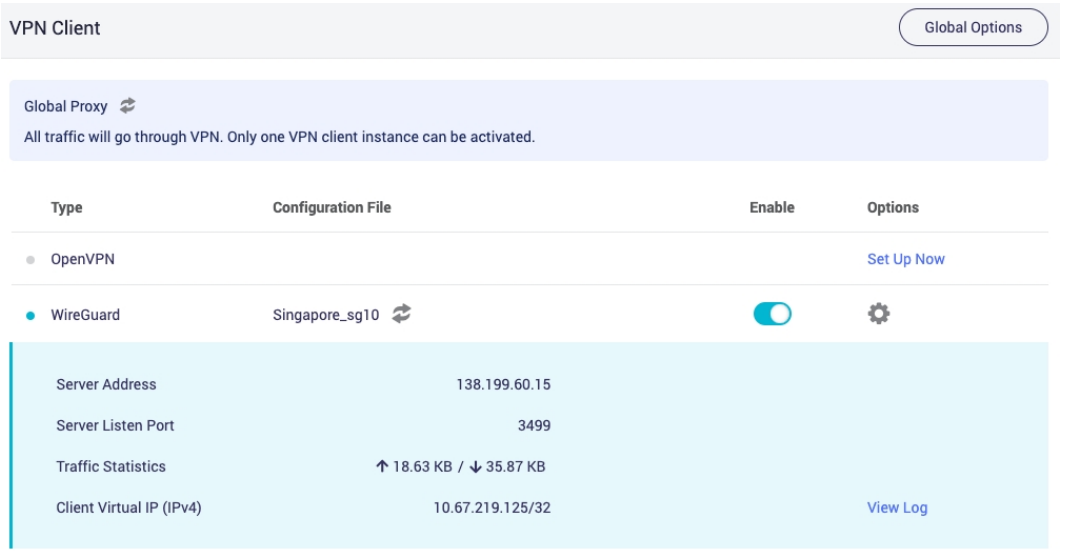
El **Clave pública** es la clave pública de WireGuard para enviar al servidor Mullvad. Puede tener hasta cinco claves al mismo tiempoPuedes tener hasta cinco claves al mismo tiempo, y administrar claves WireGuard en su página de cuenta de Mullvad.



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

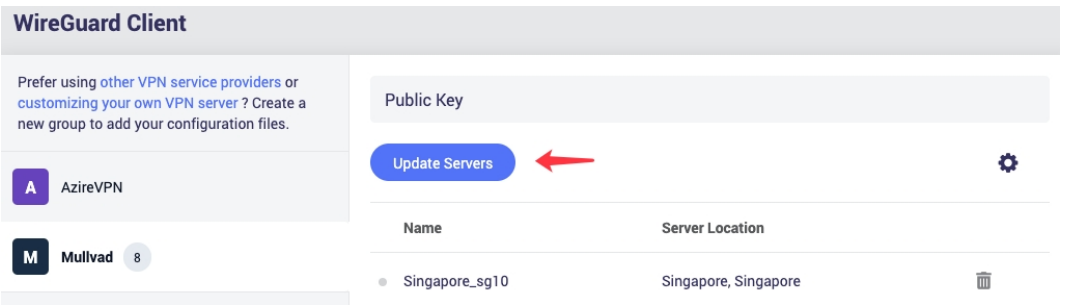


Una vez conectado, debería ver su dirección IP de usuario y la cantidad de bytes enviados/recibidos.



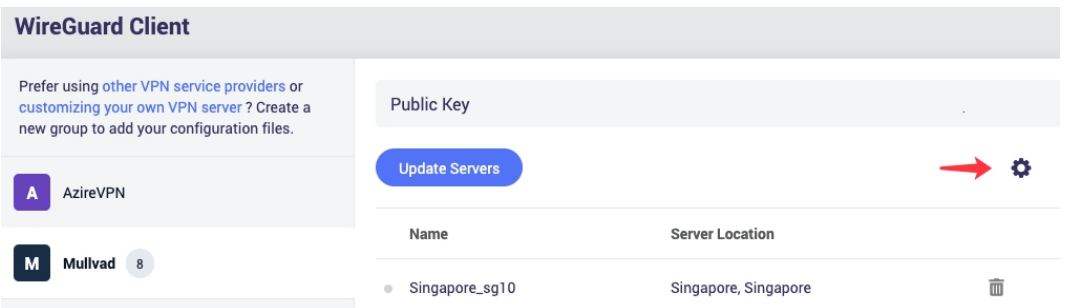
4. Actualice los servidores.

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



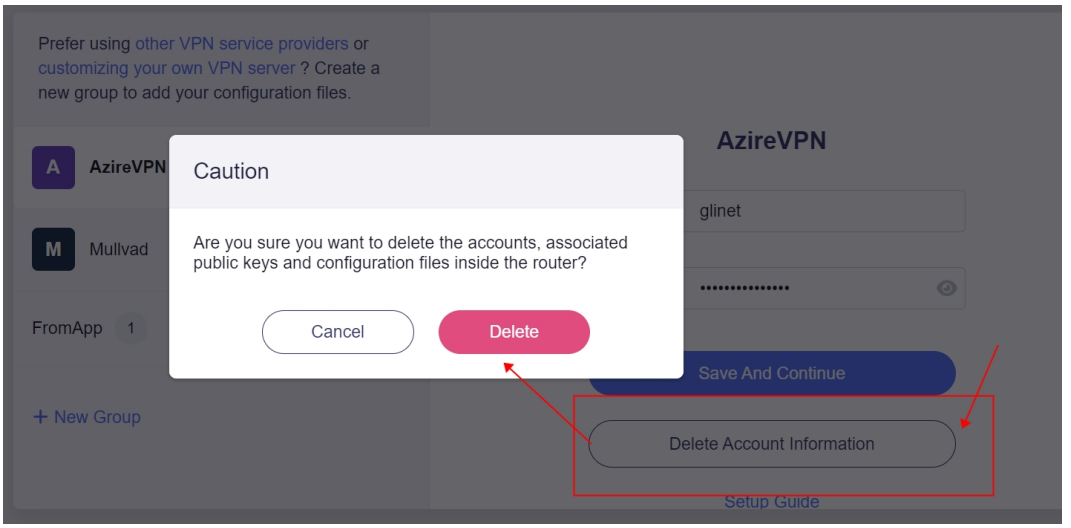
5. Editar credenciales

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



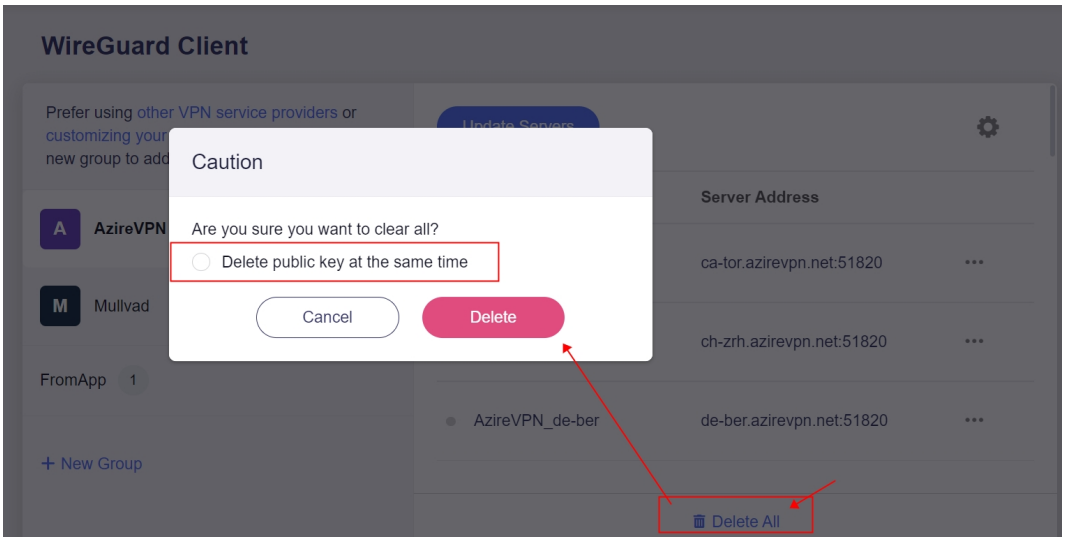
6. Eliminar información de cuenta

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



7. Eliminar

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

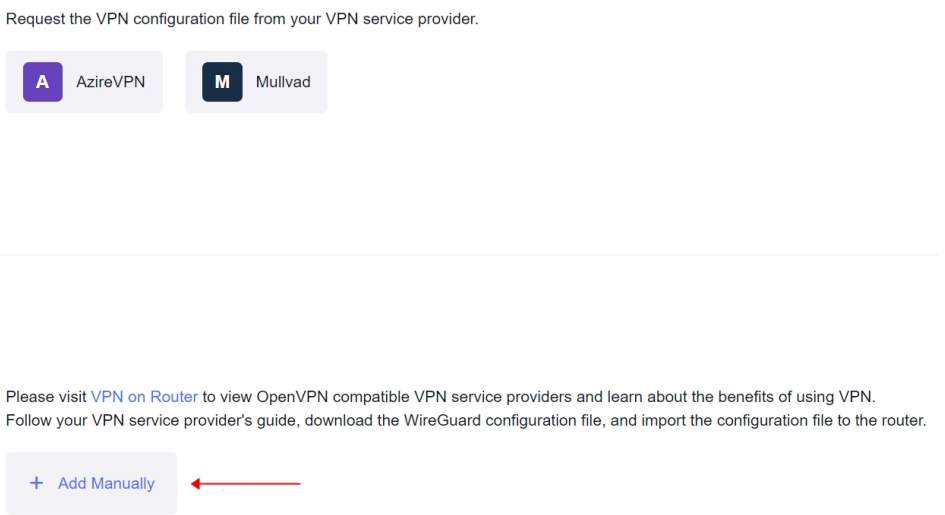


10.2.4 Configurar el cliente WireGuard manualmente (para otros proveedores)

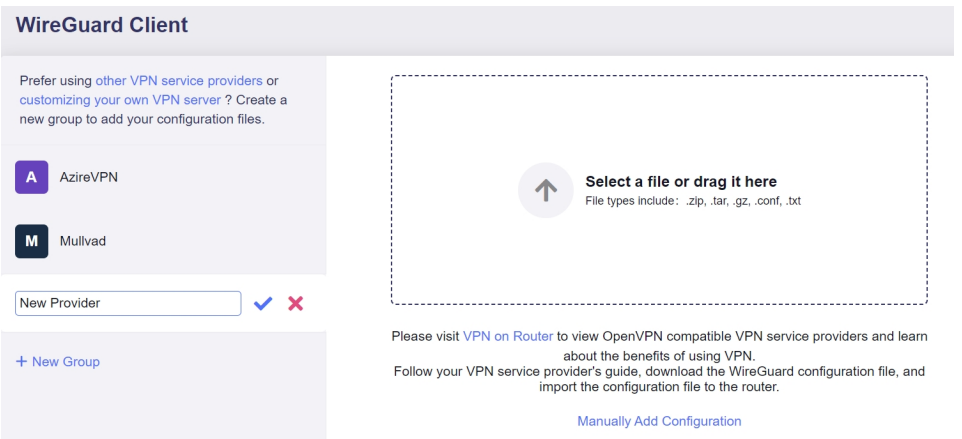
Si su proveedor de servicios WireGuard no está integrado en el panel de administración web, visite primero el sitio web oficial de su proveedor de servicios suscrito para obtener el archivo de configuración. Luego cárguelo en el enrutador para configurar un cliente WireGuard. Si no sabes cómo descargar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

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

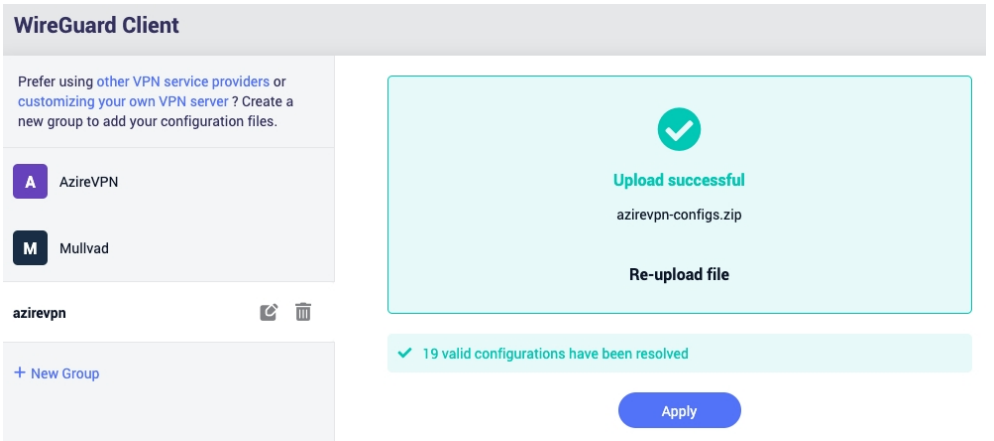
1. Inicie sesiónn en su enrutador's web admin panel y navegue hasta **VPN** > **Cliente WireGuard** > **Agregar manualmente**.



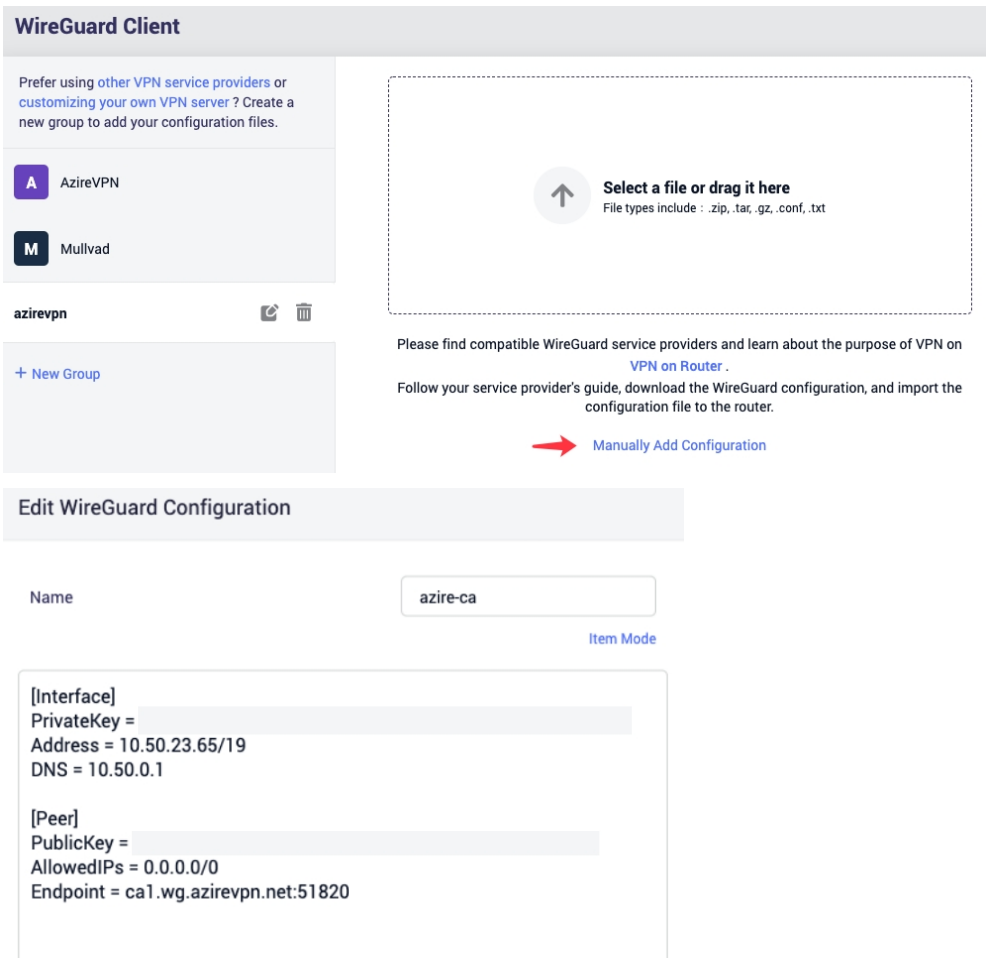
2. Se creará un grupo en la barra lateral izquierda. Establezca un nombre descriptivo para el grupo.



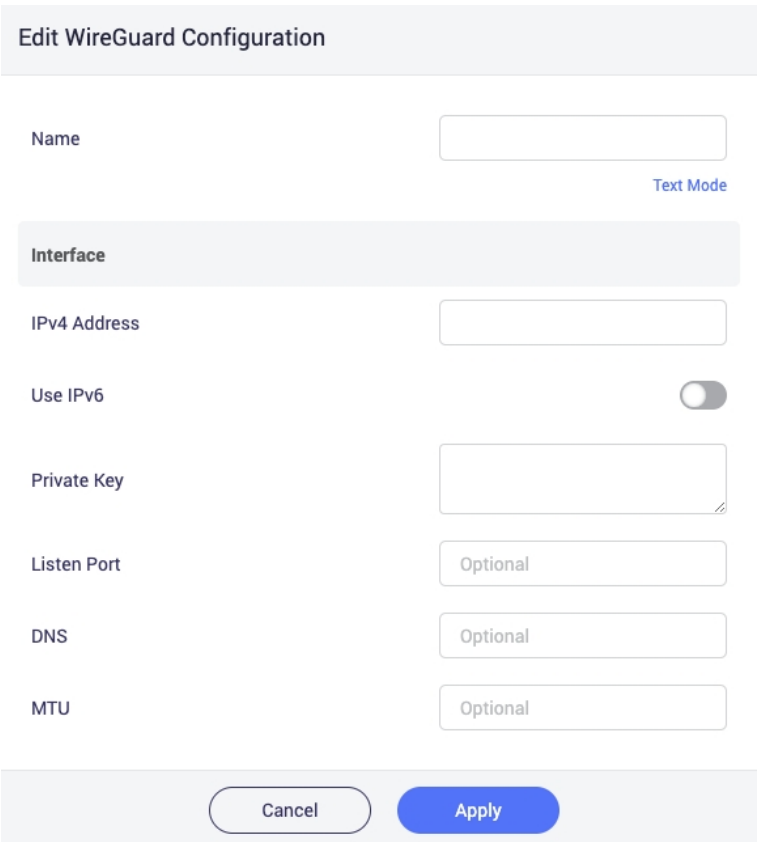
3. Click el área de carga para cargar su archivo de configuración WireGuard (formatos admitidos: zip, tar, gz, conf, txt), y haga clic en **Aplicar**. Si carga un archivo comprimido que contiene varios archivos de configuración, se descomprimirá automáticamente.



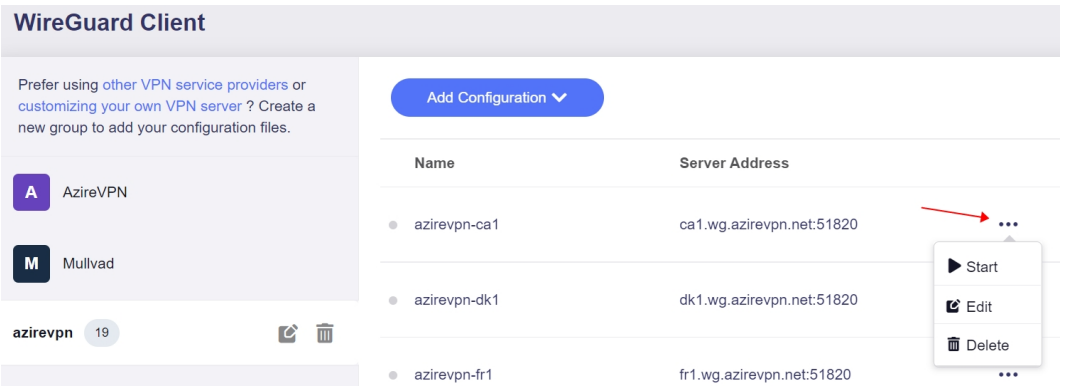
Como alternativa, puede hacer clic en **Agregar configuración manualmente** en la parte inferior del área de carga, agregar detalles de configuración en forma de texto y haga clic en **Aplicar**.



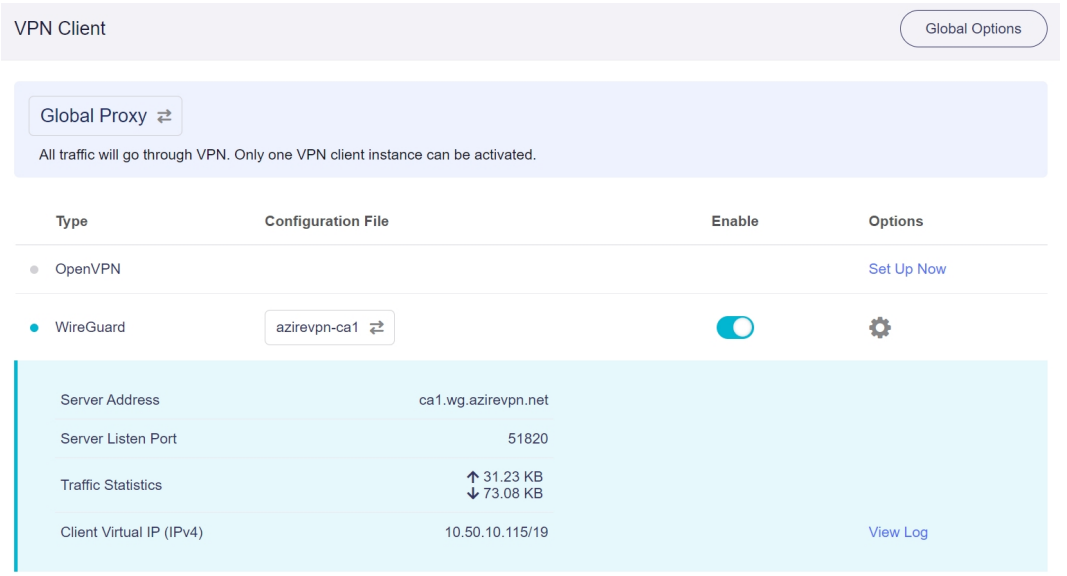
Si desea verificar cada elemento, puede cambiar al modo Elemento y verificar los detalles de configuraciónuración, luegoluego haga clic en **Aplicar**.



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



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


VPN Client
Global Options
Global Proxy
All traffic will go through VPN. Only one VPN client instance can be activated.
Type
Configuration File
Enable
Options
OpenVPN
Set Up Now
WireGuard
azirevpn-ca1
Server Address
ca1.wg.azirevpn.net
Server Listen Port
51820
Traffic Statistics
31.23 KB
73.08 KB
Client Virtual IP (IPv4)
10.50.10.115/19
View Log

Capítulo 11

Tor

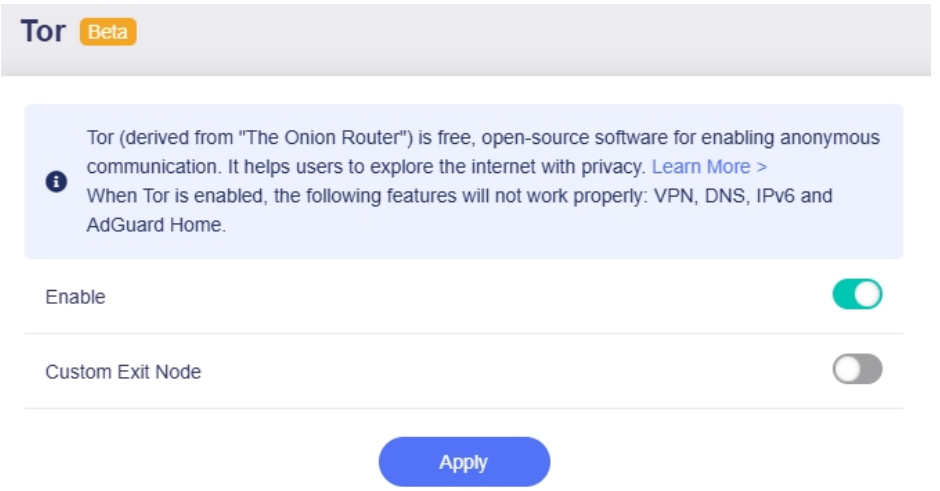
Este capítulo proporciona una breve introducción a Tor (The Onion Router), un software gratuito y de código abierto para permitir la comunicación anónima.

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

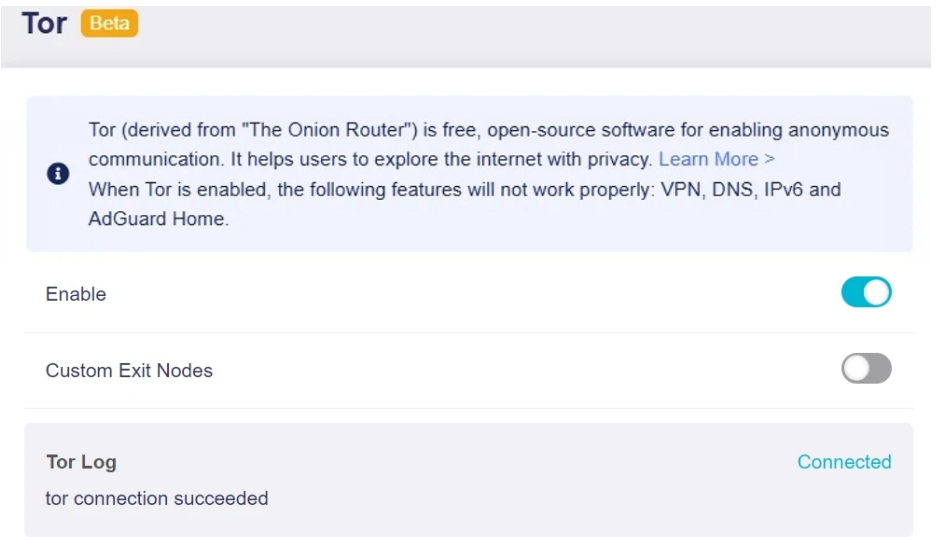
cuando Tor habilitado, laslas siguientes funciones no funcionarán correctamente: VPN, DNS, IPv6, y AdGuard Home.

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

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



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



Capítulo 12

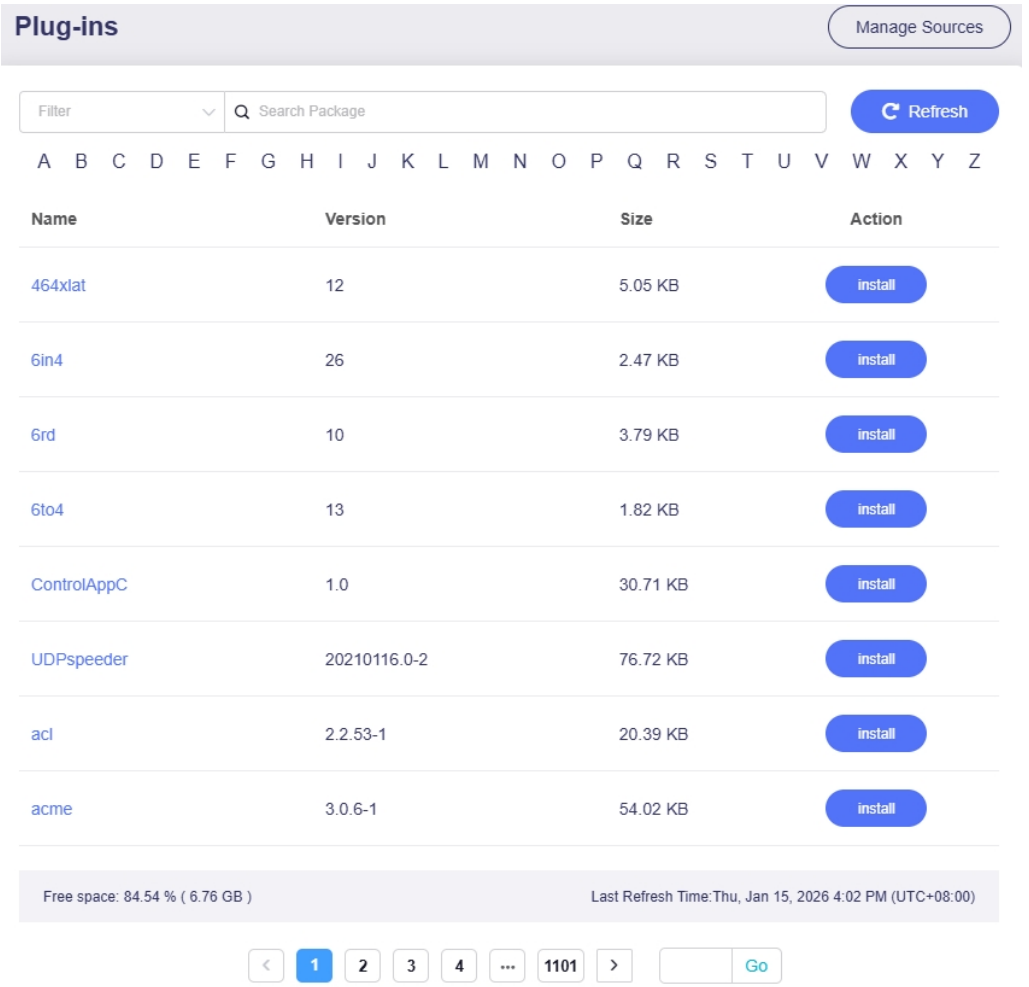
Aplicaciones

Este capítulo presenta algunas aplicaciones en enrutadores GL.iNet, por ejemplo, Complementos, DNS dinámico y GoodCloud.

12.1 Complementos

La Complementos página le permite administrar paquetes OpenWrt.

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



Nota:

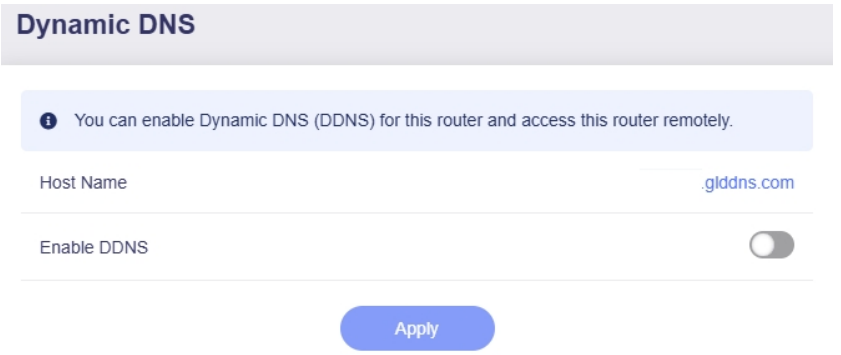
1. No se recomienda actualizar los complementos preinstalados en el firmware oficial de GL.iNet, como nginx, etc.
2. Los complementos de terceros instalados manualmente por los usuarios se pueden actualizar; sin embargo, GL.iNet no es responsable de ningún problema de seguridad causado por complementos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

12.2 DNS dinámico

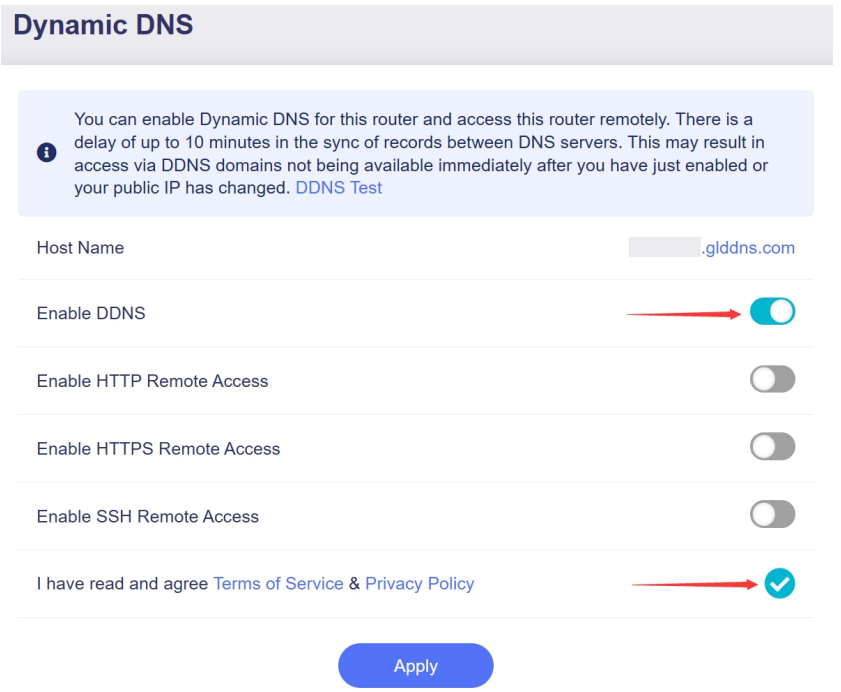
Dinámico Servicio de nombres de dominio (DDNS o DNS dinámico) es un servicio que se utiliza para asignar un nombre de dominio a la dirección IP dinámica de un dispositivo de red. Con DNS dinámico, puede acceder a su enrutador de forma remota. Se requiere una dirección IP pública para esta funcionalidad.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

12.2.1 Habilitar DDNS

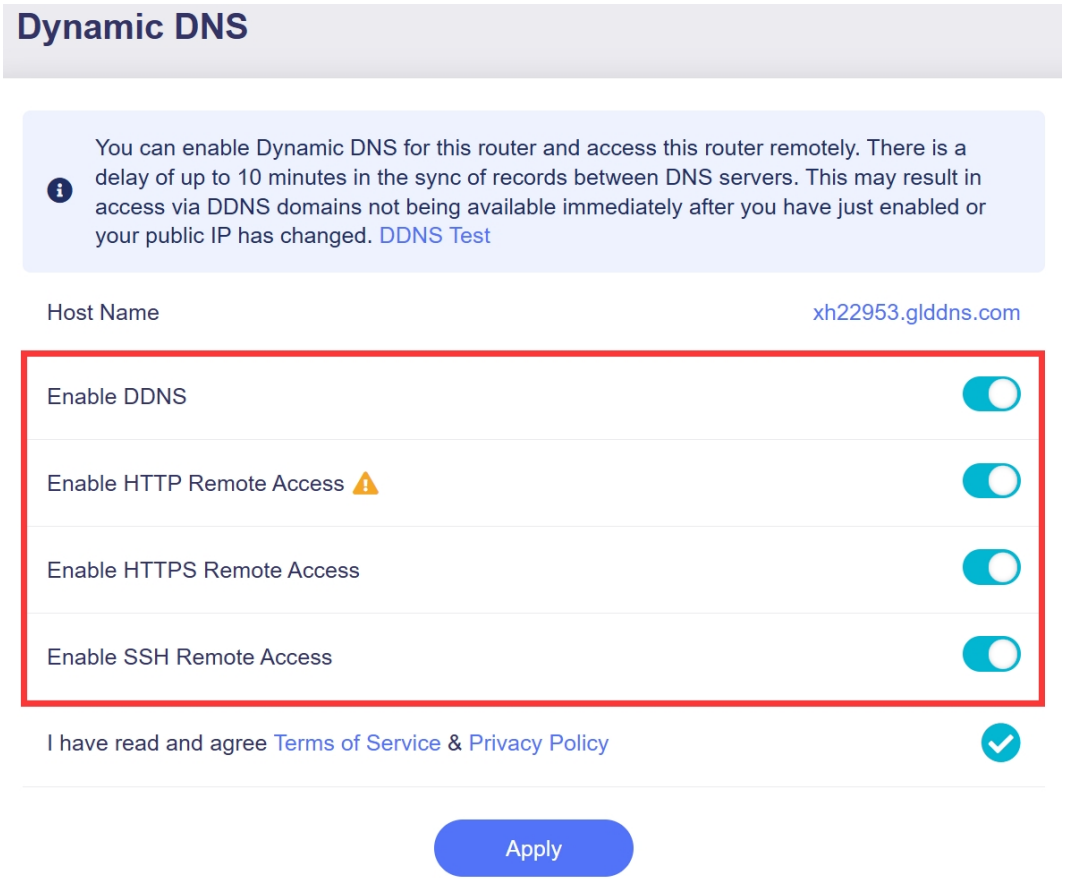
1. Inicie sesión en su enrutador's web admin panel, navegue hasta **APLICACIONES** > **DNS dinámico**, la página se muestra como a continuación.



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



3. Si necesita acceso remoto, habilite los servicios requeridos en esta página. incluyendo **HTTP**, **HTTPS** y **SSH**.



Nota:

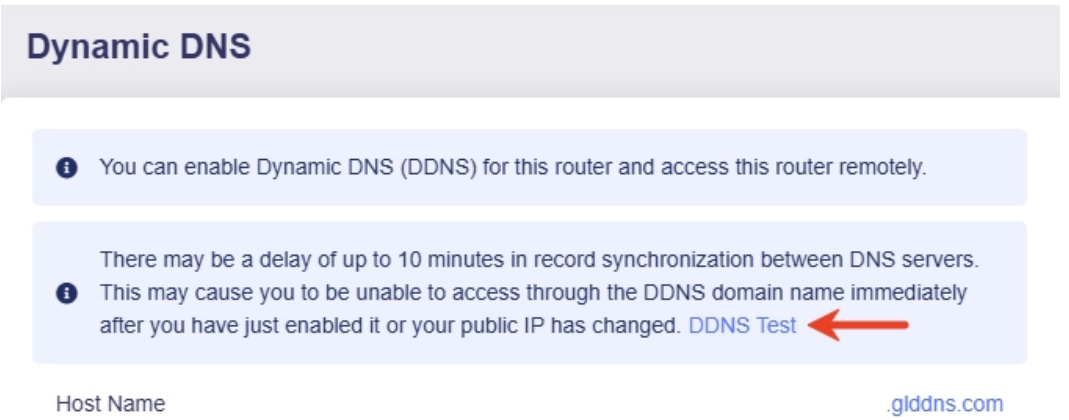
1. Puede haber un retraso de hasta 10 minutos en la sincronización de registros entre servidores DNS. Esto puede impedirle acceder a través del nombre de dominio DDNS inmediatamente después de habilitarlo o cuando cambie su IP pública.
2. Si habilita DDNS y el Cliente VPN al mismo tiempo, enseguro que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

12.2.2 Comprobar si DDNS funciona

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

Método 1. Use Herramienta de prueba DDNS

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



2. Asegúrese de que la dirección IP de la resolución del dominio DDNS coincida con la IP WAN del enrutador. 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.



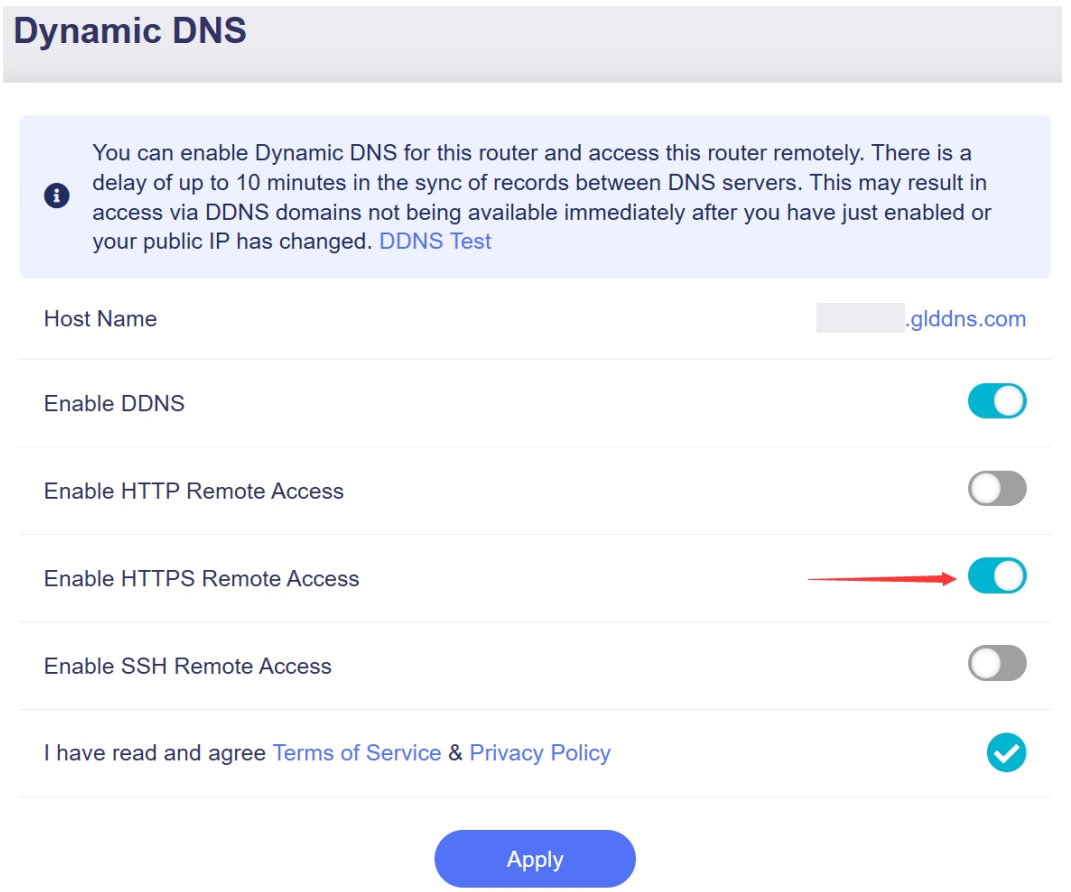
   - Reemplace “xxxxxxx.glddns.com” en la imagen de arriba con su nombre de host.
   - El “8.8.8.8” es el DNS de Google. Úselo o reemplácelo con otros, luego presione Entrar.
2. Si obtiene una dirección IP pública como “183.178.10.100” en la imagen de arriba, indica que su DDNS El dominio se ha asignado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

12.2.3 Acceso remoto HTTP

Se requiere una **Dirección IP pública** para el acceso remoto HTTP.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 80**) en el enrutador ascendente para acceso HTTP.

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

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



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

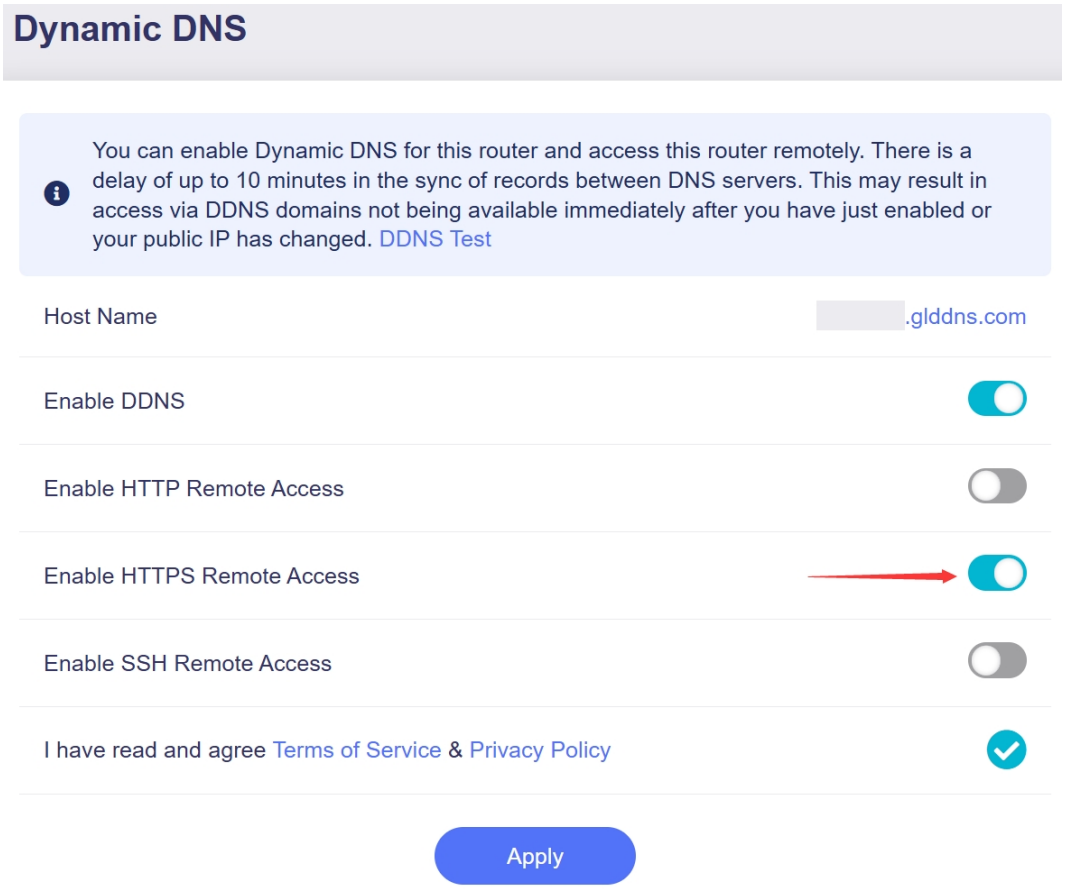
Nota: HTTP es un protocolo no cifrado. Todos los datos transmitidos, incluidas las credenciales de inicio de sesión, se envían en texto sin formato, lo que plantea riesgos de seguridad. Debe utilizar el acceso remoto HTTP con precaución.

12.2.4 Acceso remoto HTTPS

Se requiere una **Dirección IP pública** para el acceso remoto HTTPS. 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 443**) en el enrutador ascendente para HTTPS acceso.

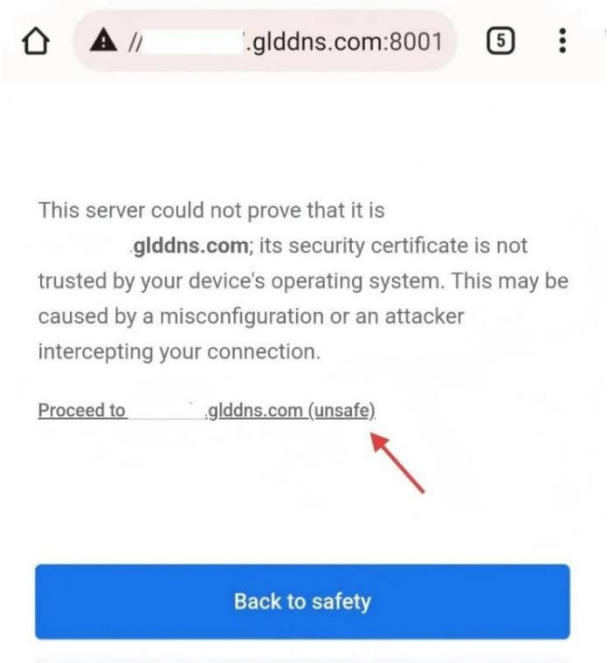
Siga los pasos siguientes para habilitar el acceso remoto HTTPS para su enrutador.

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



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

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



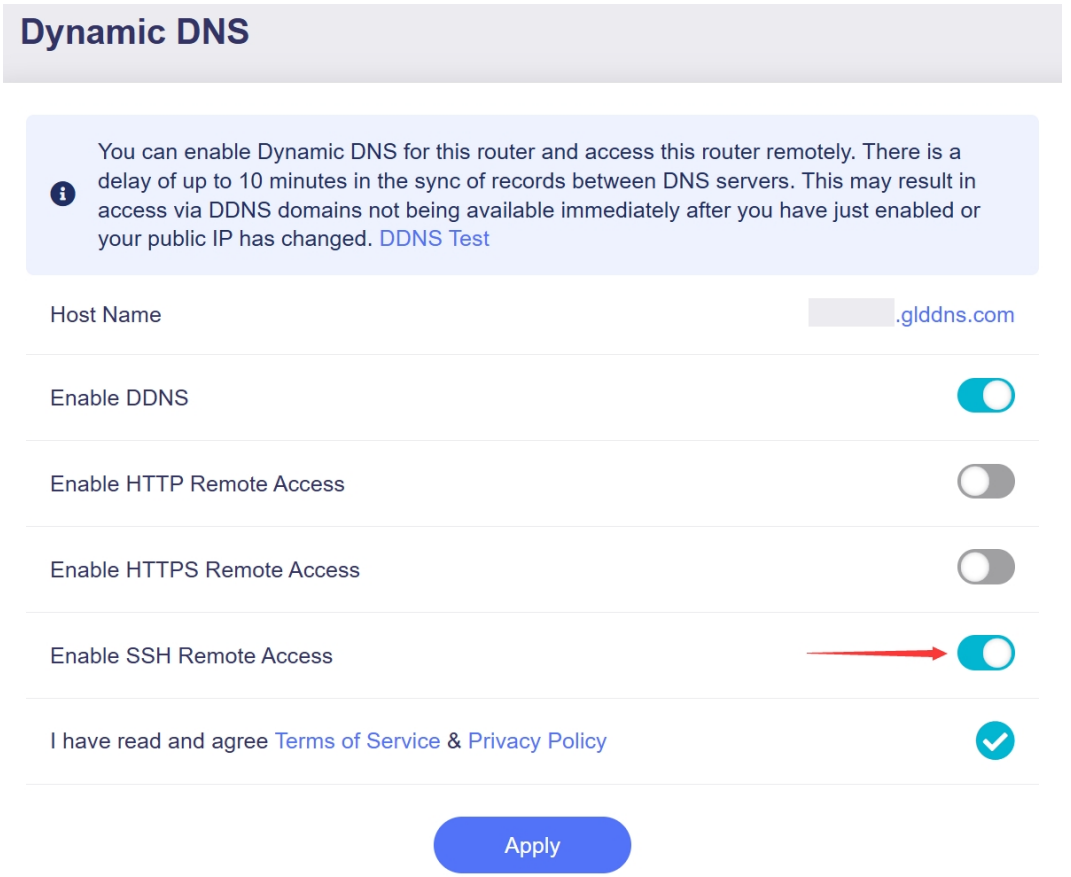
Luego podrá acceder al enrutador’s panel de administración web usando el DDNS host nombre sobre **HTTPS**.

12.2.5 Acceso remoto SSH

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

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

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



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

12.3 GoodCloud

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

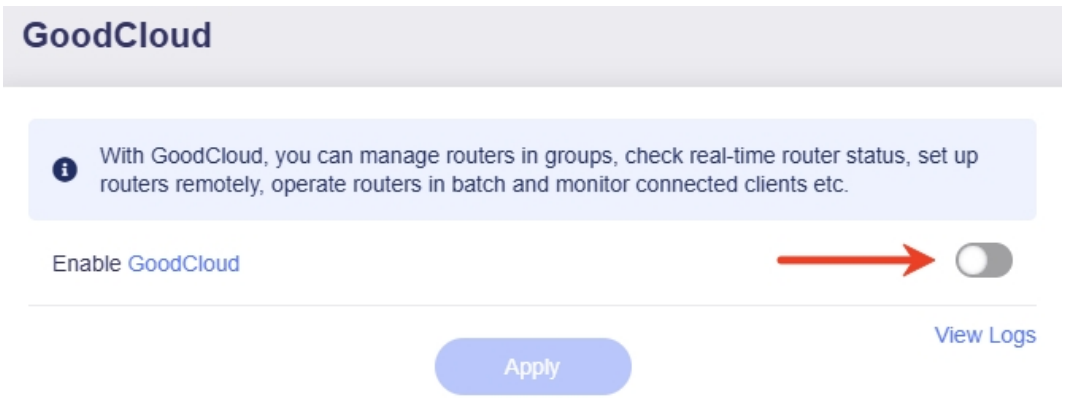
Con GoodCloud, puede:

- Verificar estado de su enrutador’en tiempo real
- Madministrar grupos de enrutadores
- Configurar enrutadores de forma remota
- Monitor clientes conectados
- Operar enrutadores en lote
- Establecer Sitio-con-Sitio conexión

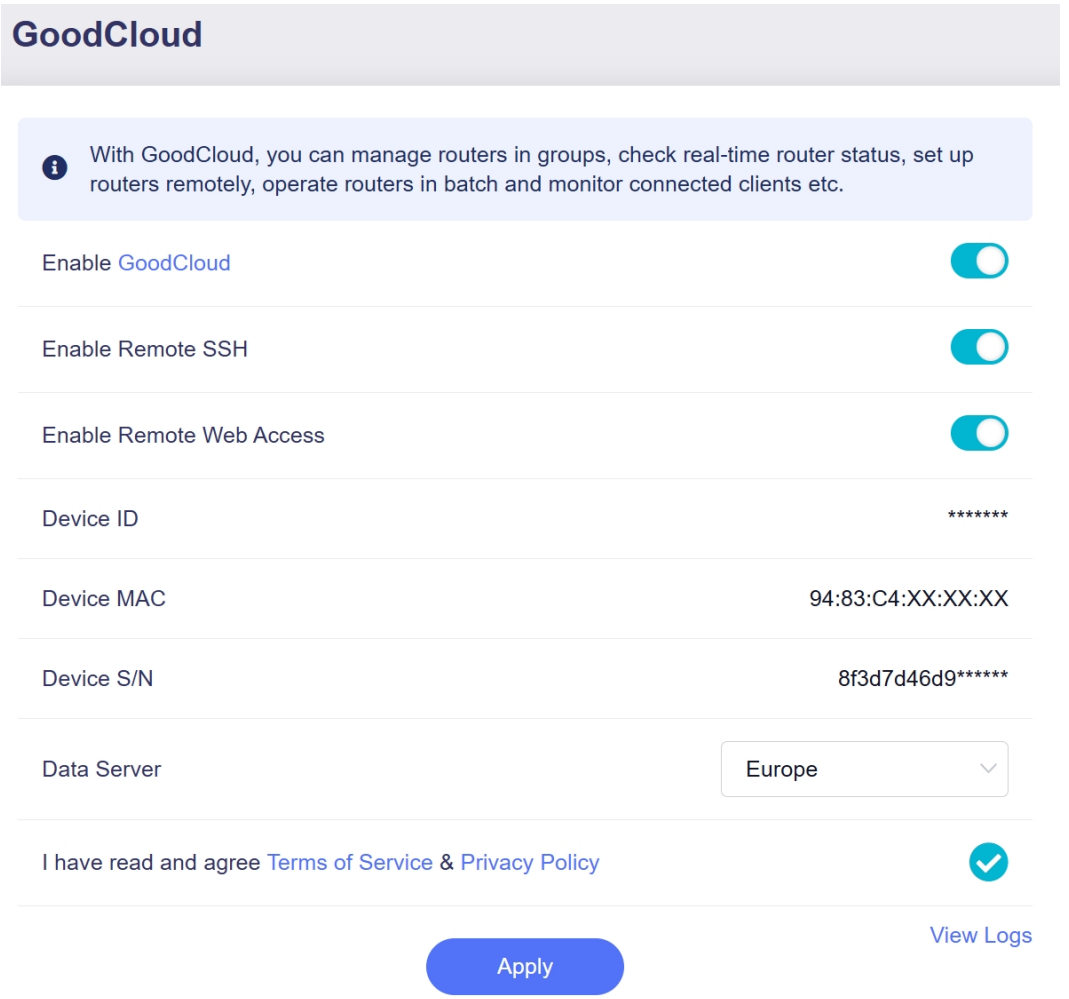
Algunas funciones están disponibles en el plan Enterprise y el plan VAR (revendedor de valor agregado). Consulte aquí para obtener más detalles.

12.3.1 Habilitar GoodCloud

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

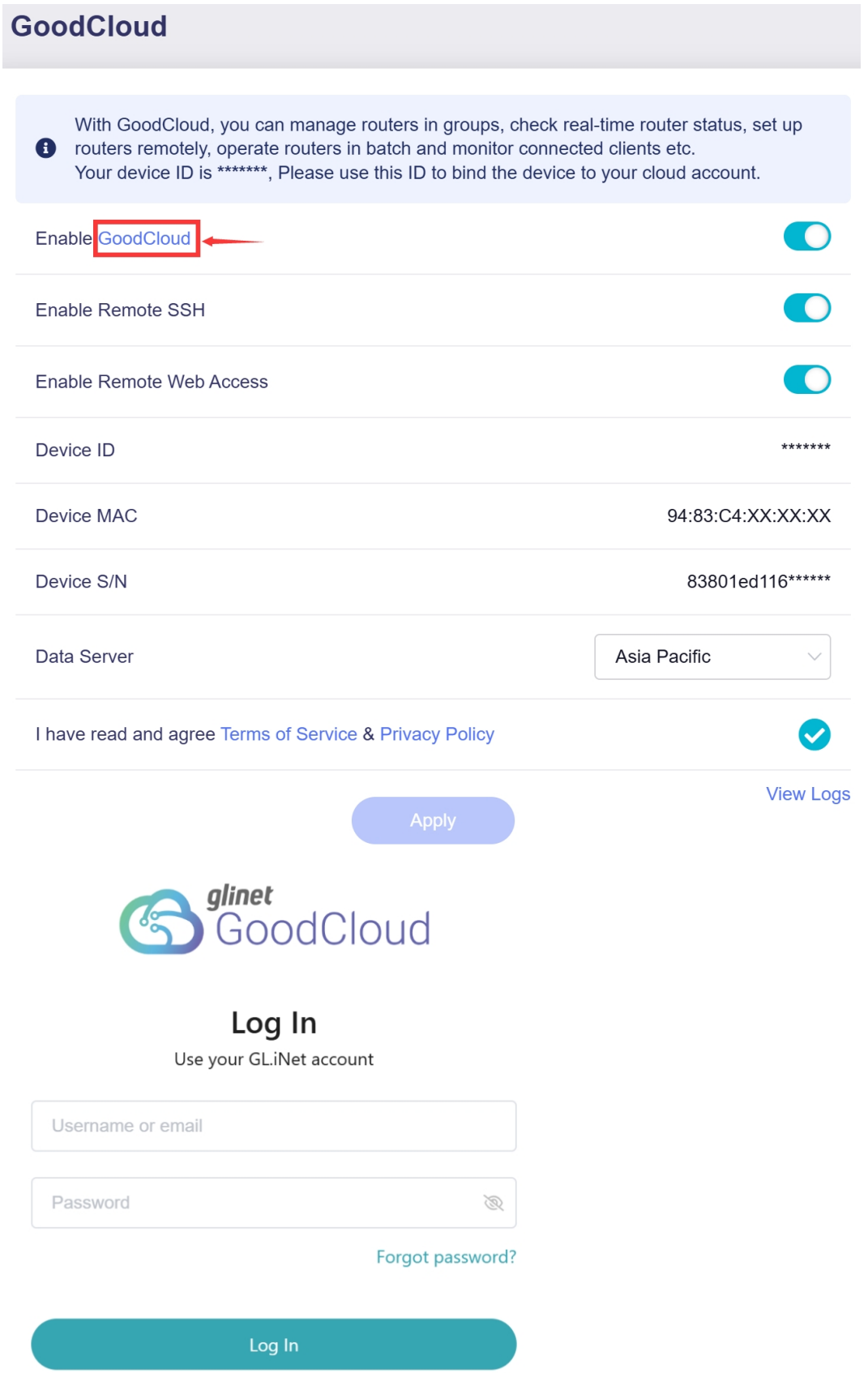


Habilite **Acceso remoto SSH** y **Acceso web remoto** si es necesario, seleccione el servidor más cercano, lea y acepte las **Términos de servicio y política de privacidad**, luego haga clic en **Aplicar**.



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

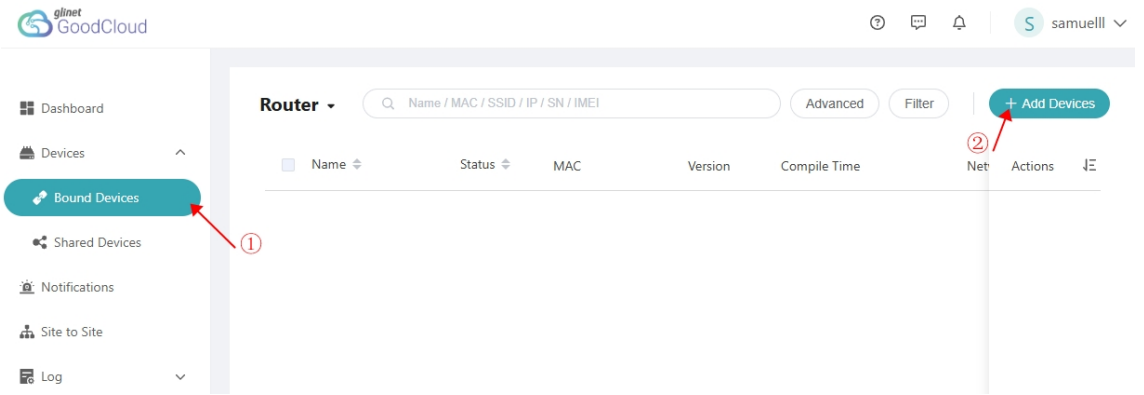
2. Haga clic en GoodCloud para ir a la página de inicio de sesión e inicie sesión con su cuenta GL.iNet Cloud. Si no'no tiene una cuenta, regístrese para obtener una e inicie sesión. Una vez haya iniciado sesión, el enrutador estará vinculado a su cuenta automáticamente.


GoodCloud
With GoodCloud, you can manage routers in groups, check real-time router status, set up routers remotely, operate routers in batch and monitor connected clients etc.
Your device ID is *******, Please use this ID to bind the device to your cloud account.
Enable GoodCloud
Enable Remote SSH
Enable Remote Web Access
Device ID
****
Device MAC
94:83:C4:XX:XX:XX
Device S/N
83801ed116******
Data Server
Asia Pacific
I have read and agree Terms of Service & Privacy Policy
View Logs
Apply
glinet
GoodCloud
Log In
Use your GL.iNet account
Username or email
Password
Forgot password?
Log In

Consejos:

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

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



Hay tres métodos para vincular un dispositivo a su cuenta de GoodCloud: descubrimiento automático, agregar manualmente y de forma masiva. Importar. Haga clic aquí para obtener más detalles.

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

GoodCloud

With GoodCloud, you can manage routers in groups, check real-time router status, set up routers remotely, operate routers in batch and monitor connected clients etc.
The device is bound by **Holly0912** on **2026-10-08 17:03**,Unbind

Enable GoodCloud	
Enable Remote SSH	
Enable Remote Web Access	
Device ID	*******
Device MAC	94:83:C4:XX:XX:XX
Device S/N	8f3d7d46d******
Data Server	Europe
I have read and agree Terms of Service & Privacy Policy	

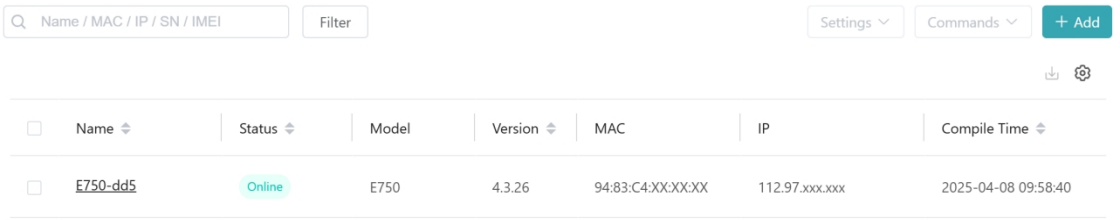
View Logs

Apply

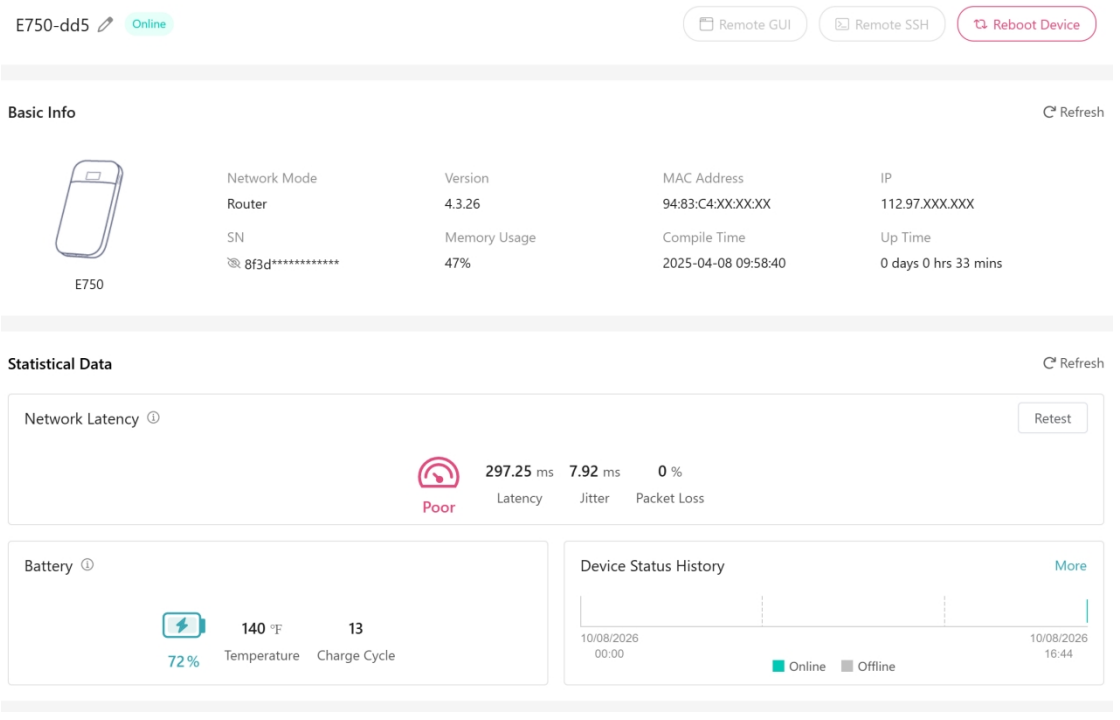
12.3.2 Administrar el enrutador

Consultar los detalles del dispositivo

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

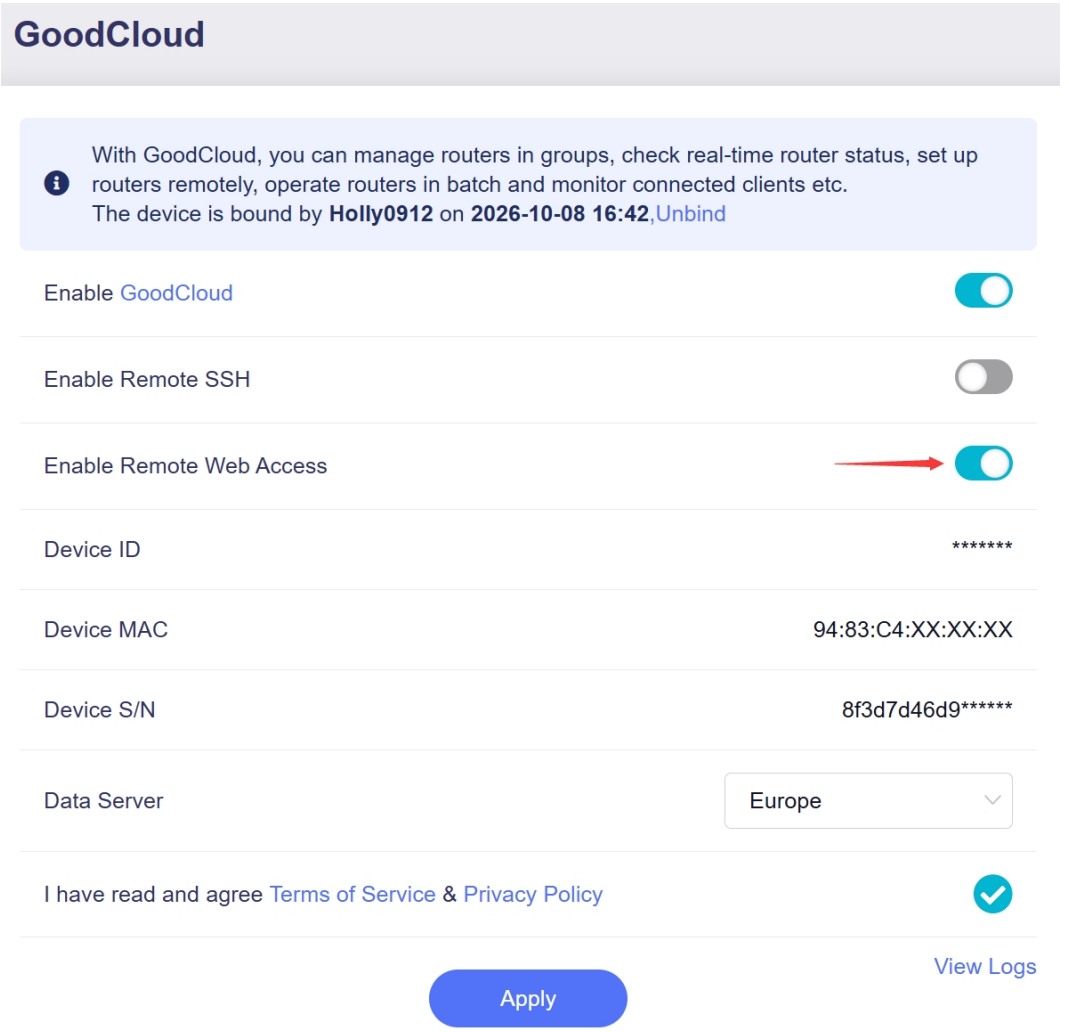


Haga clic en el nombre del dispositivo para ingresar a la página de detalles del dispositivo, que muestras información básica, datos estadísticos, descripción general de la red, lista de clientes y cronograma. También puede realizar operaciones avanzadas, como acceso remotolying al enrutador, y reiniciando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

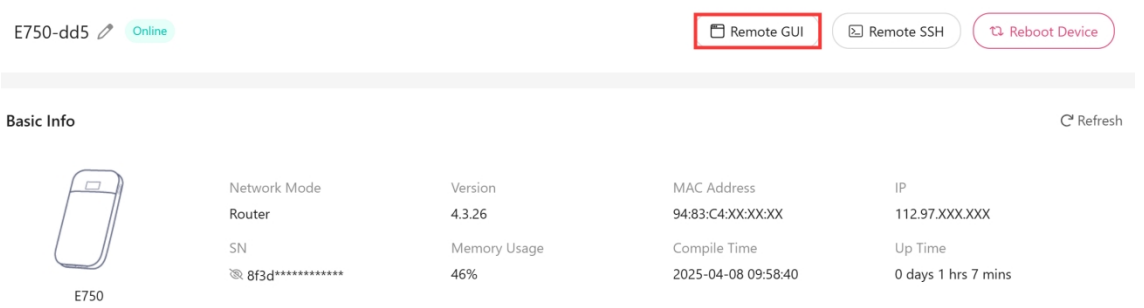


Acceso web remoto

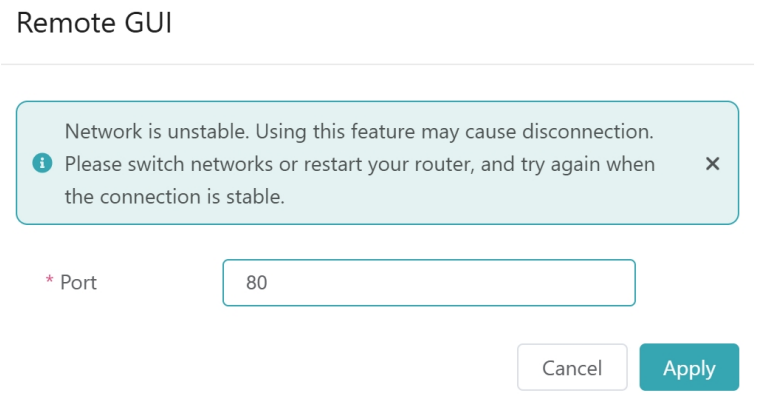
1. Inicie sesión en el panel de administración web del del enrutador', navegue hasta **APLICACIONES** > **GoodCloud**, habilite **Acceso web remoto** y luego haga clic en **Aplicar**.



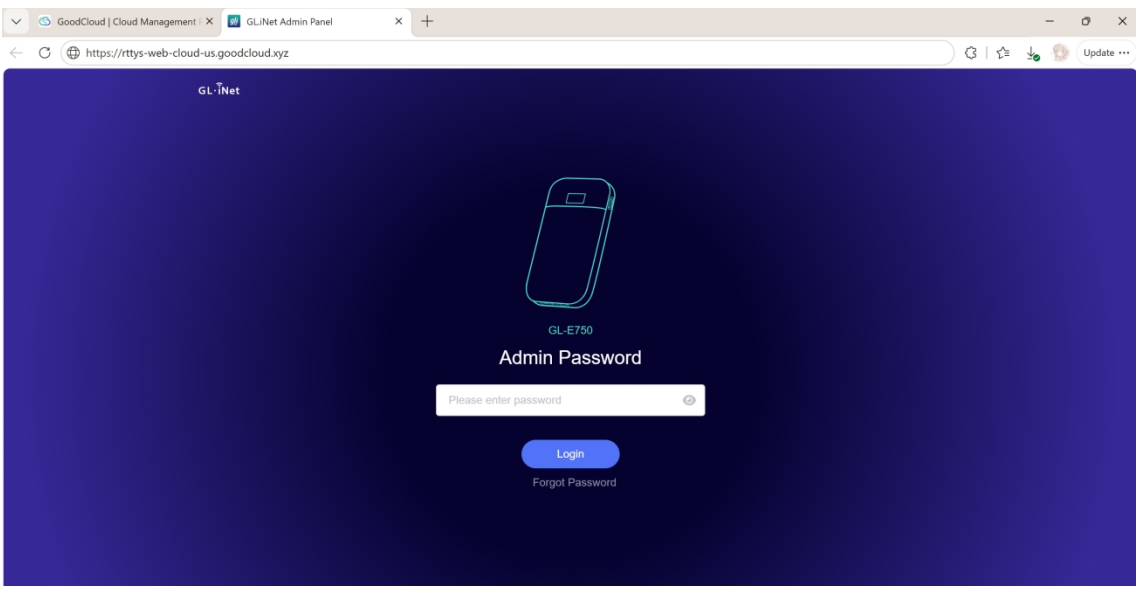
2. Inicie sesión en la plataforma GoodCloud y navegue hasta **Dispositivos** > **Dispositivos vinculados**. Haga clic en el dispositivo al que desea acceder e ingresará a la página de detalles del dispositivo.
3. En la página de detalles del dispositivo, haga clic en **Remoto GUI** botón en la esquina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



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

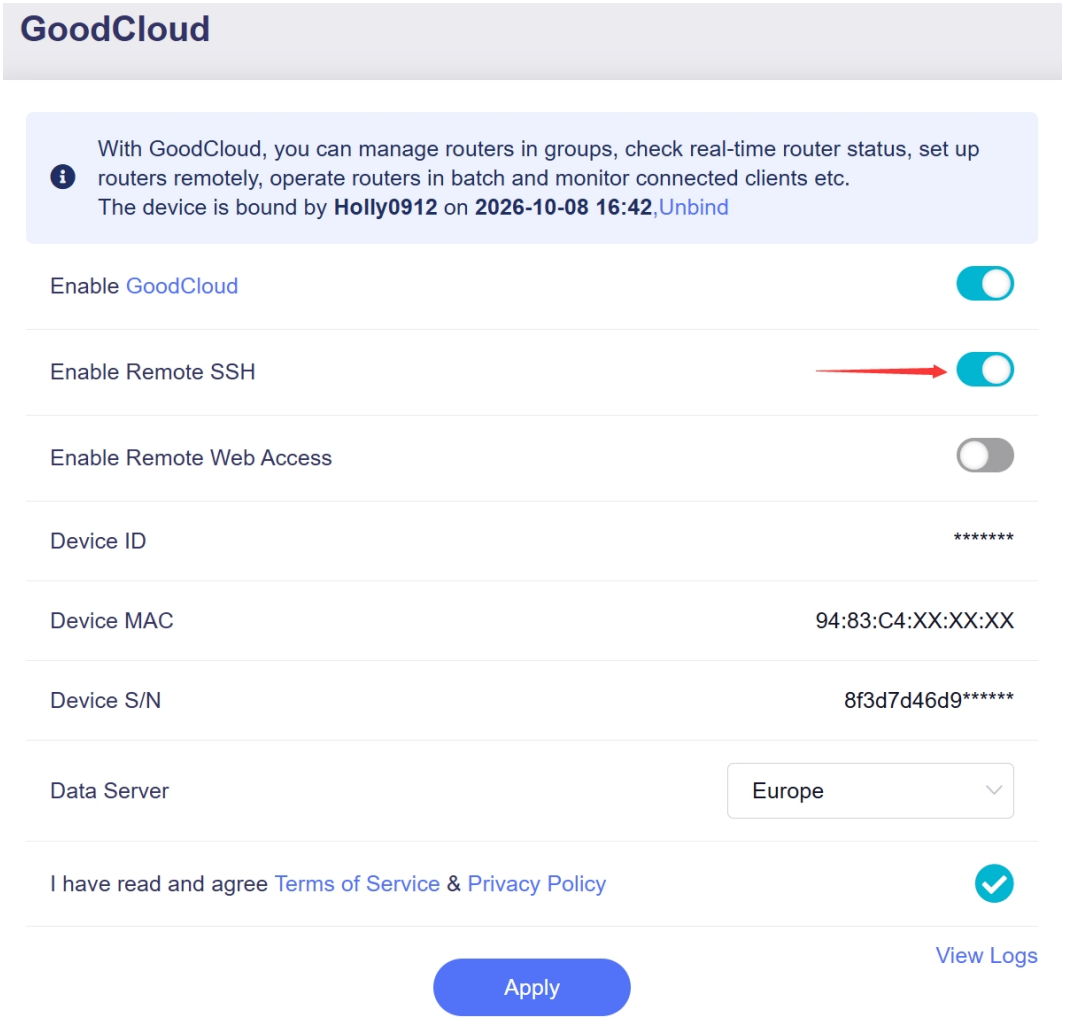


5. Será redirigido a la página de inicio de sesión del enrutador'. Ingrese la contraseña de administrador para acceder de forma remota al panel de administración web del enrutador'.

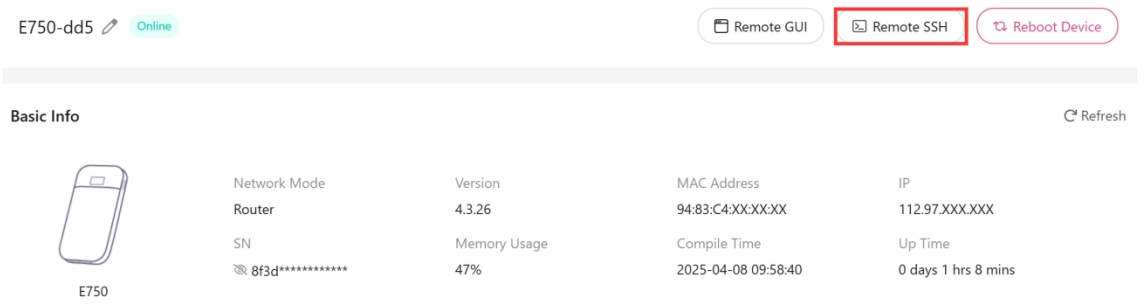


Acceso remoto SSH

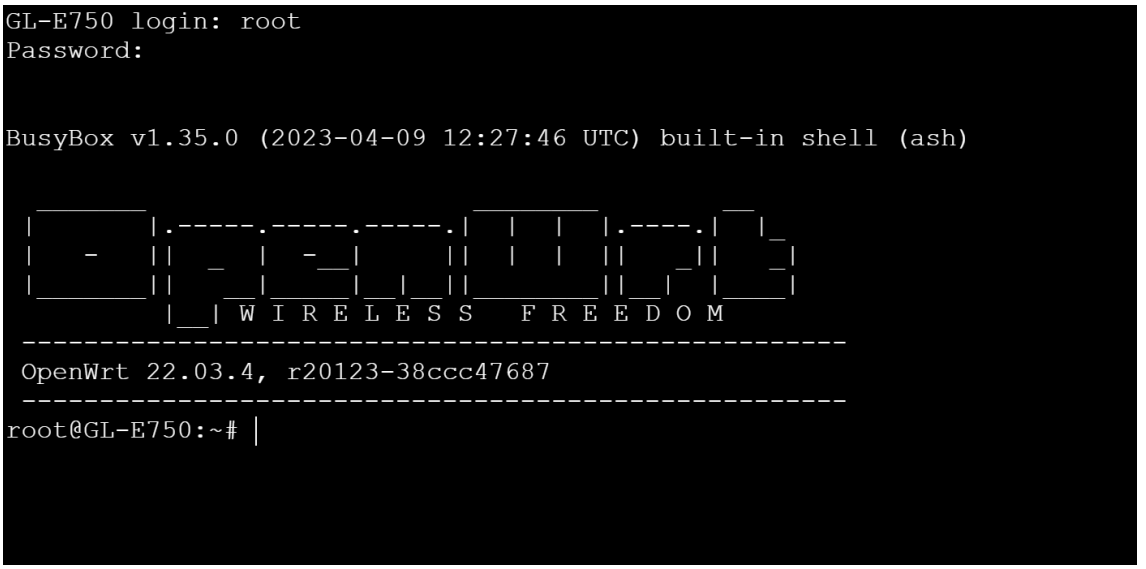
1. Inicie sesión en el enrutador'panel de administración web, navegue hasta **APLICACIONES** > **GoodCloud**, habilite **Acceso remoto SSH** y luego haga clic en **Aplicar**.



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

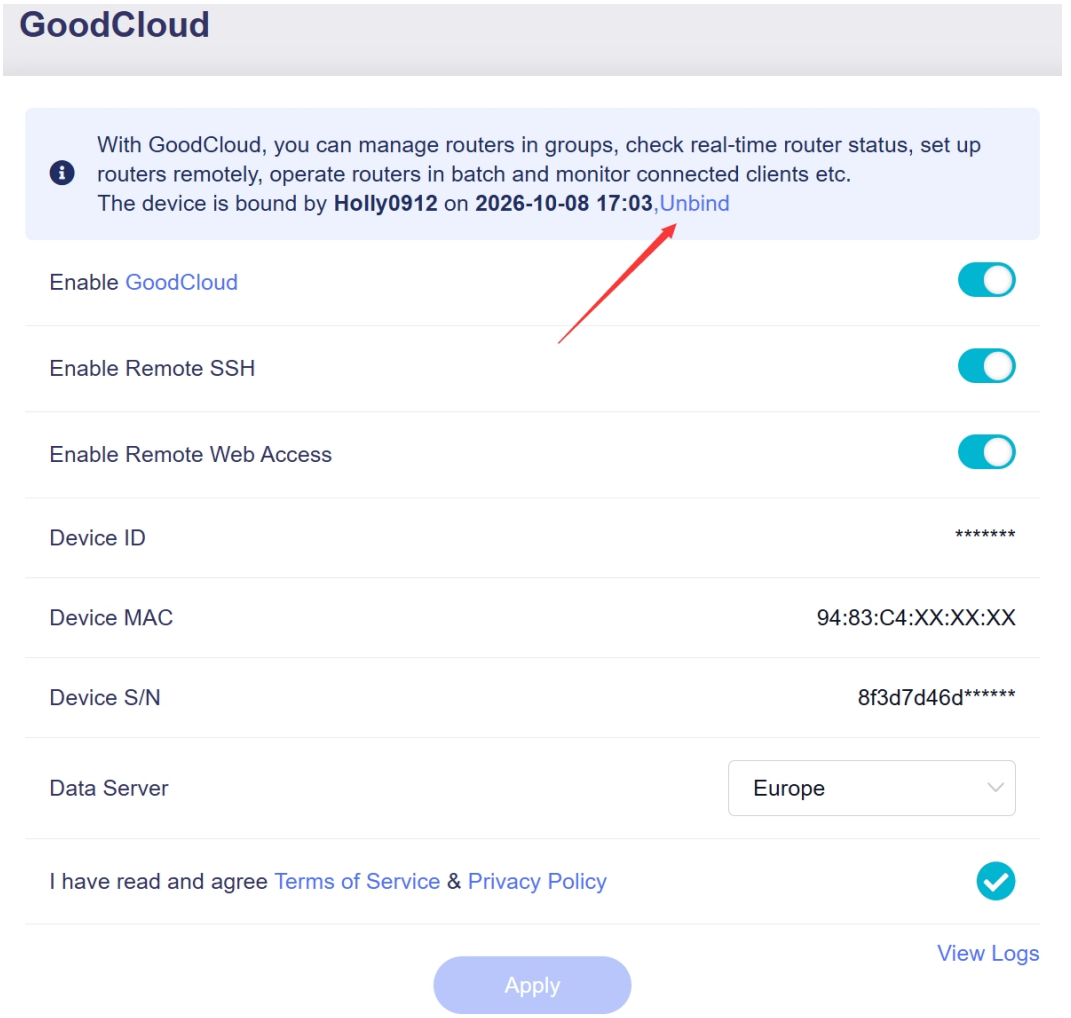


4. Inicie sesión como **root** e ingrese la contraseña para acceder al terminal de su enrutador.

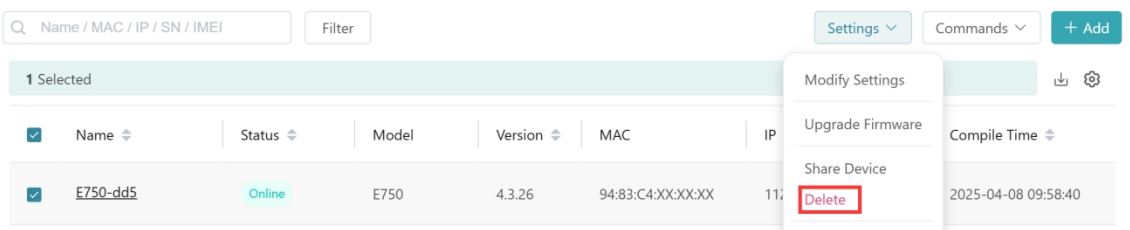


12.3.3 Desvincular el dispositivo

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



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



Capítulo 13

Red

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

13.1 Cortafuegos

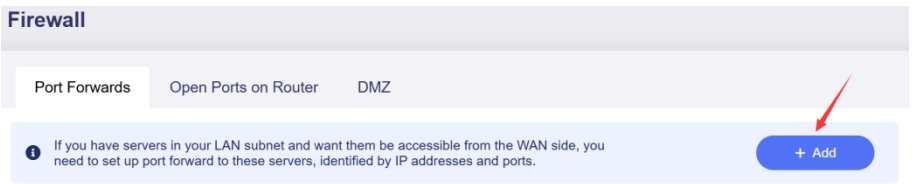
Firewall es una función de red que enruta solicitudes externas a dispositivos específicos en su red local. La página Firewall incluyetres funciones clave: **Reenvío de puertos** (para acceso dirigido a puertos específicos de dispositivos), **Abrir puertos en el enrutador** (para acceso a servicios que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

13.1.1 Reenvío de puertos

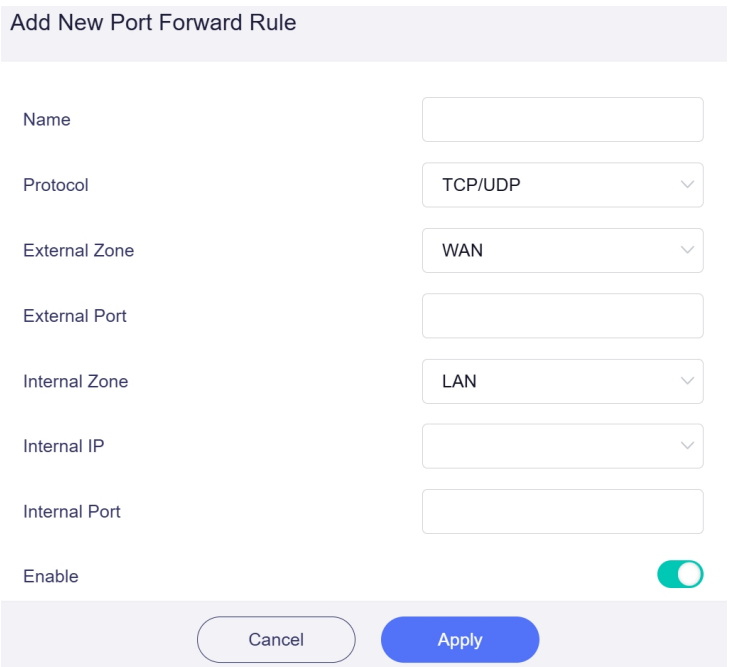
Reenvío de puertos permite que las computadoras remotas se conecten a una computadora o servidor local detrás del firewall de la LAN (por ejemplo, servidores web, servidores FTP).

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

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



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

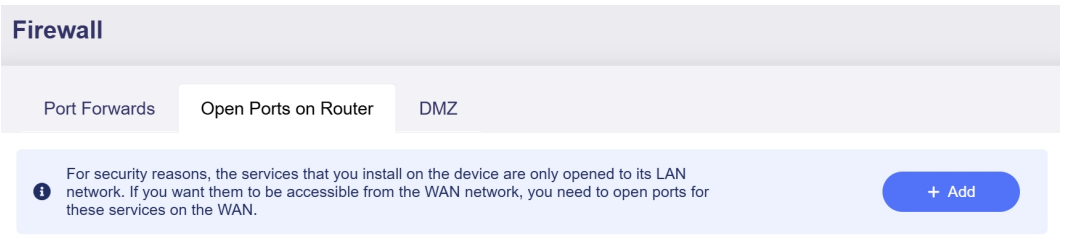


- **Nombre**: el nombre de la regla que puede especificar el usuario.
- **Protocolo**: el protocolo utilizado. Puede elegir TCP, UDP o TCP y UDP.
- **Zona externa**: las opciones disponibles son WAN, Cliente WireGuard, Servidor WireGuard, Cliente OpenVPN, Servidor OpenVPN, LAN e Invitado.
- **Puerto externo**: El número(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.
- **Habilitar**: habilite o deshabilite esta regla.

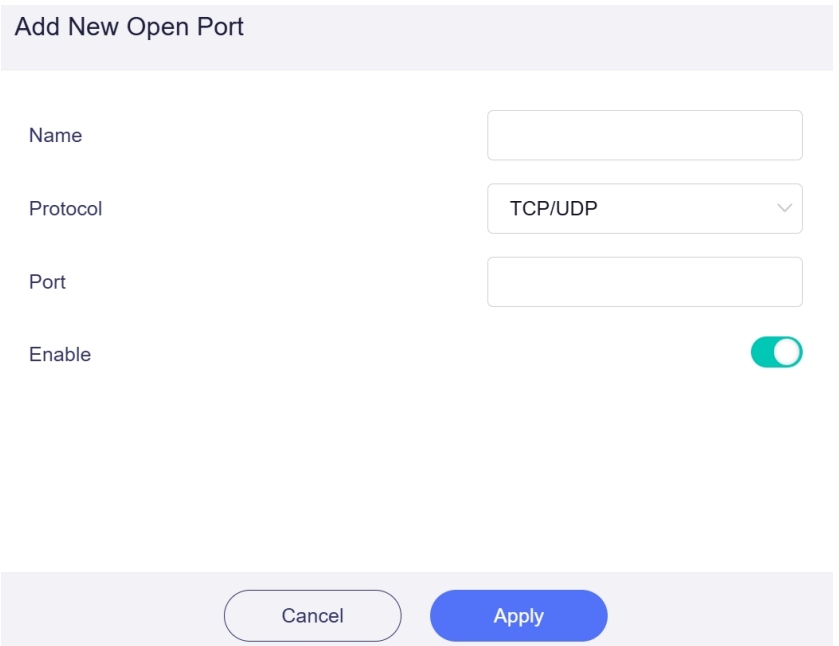
13.1.2 Abrir puertos en el enrutador

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

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



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



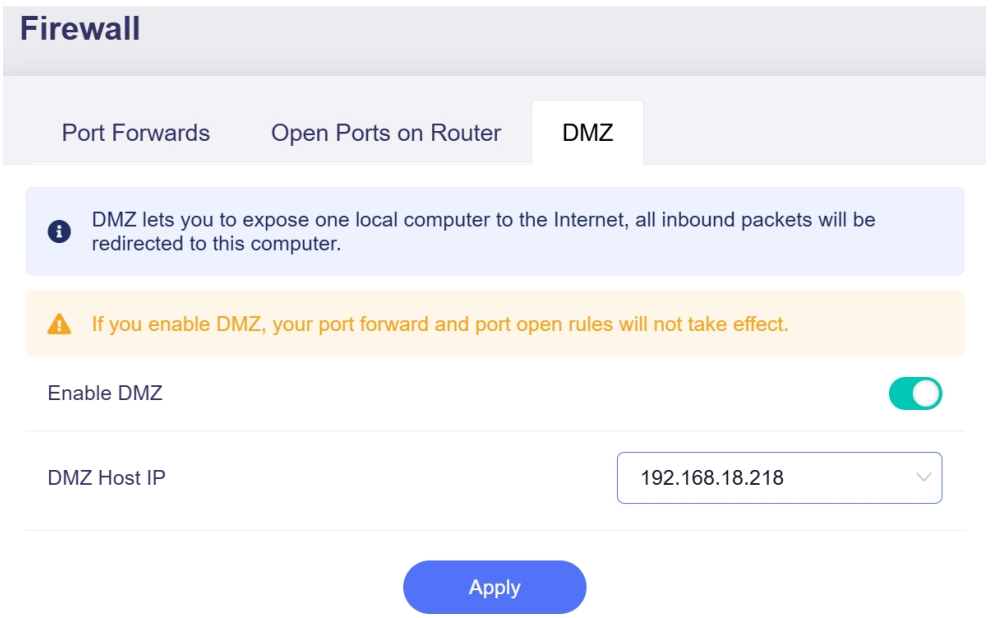
- **Nombre**: el nombre de la regla que puede especificar el usuario.
- **Protocolo**: El protocolo utilizado, puede elegir TCP, UDP o TCP y UDP.
- **Puerto**: El número de puerto que desea abrir.
- **Activar**: activa o desactiva esta regla.

13.1.3 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 **RED** > **Cortafuegos** > **DMZ** sección.
2. Tactivar **Habilite DMZ**, luego seleccione lae **IP del host DMZ** de la lista desplegable. El dispositivo seleccionado recibe todos los paquetes entrantes. Haga clic en **Aplicar** para guardar la configuración.



13.2 Multi-WAN

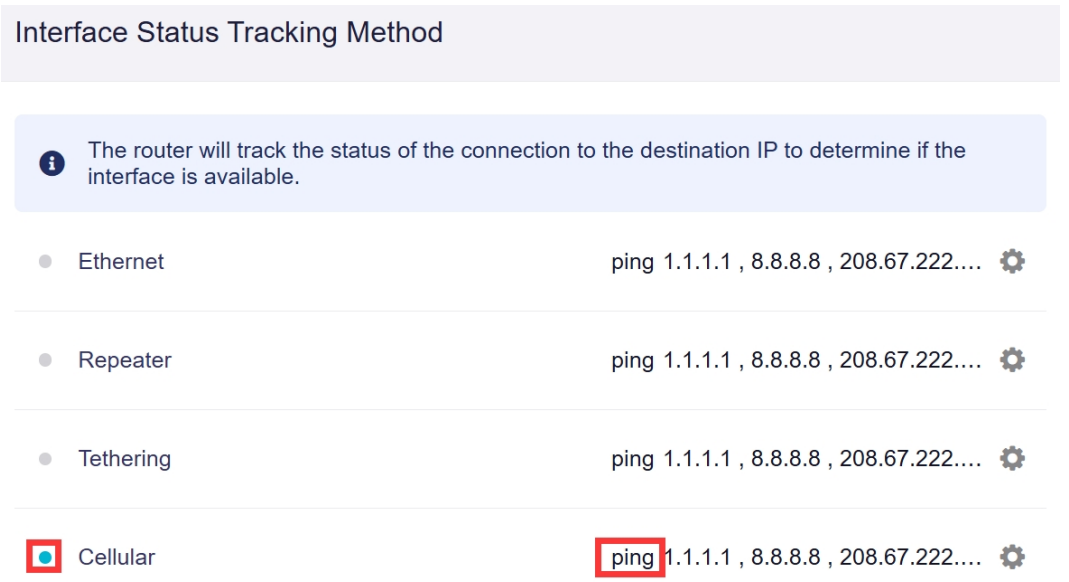
Multi-WAN permite el uso simultáneo de múltiples métodos de acceso a Internet, lo que permite la configuración de diversas opciones de conectividad en el enrutador. Ofrece dos modos de trabajo:

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

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

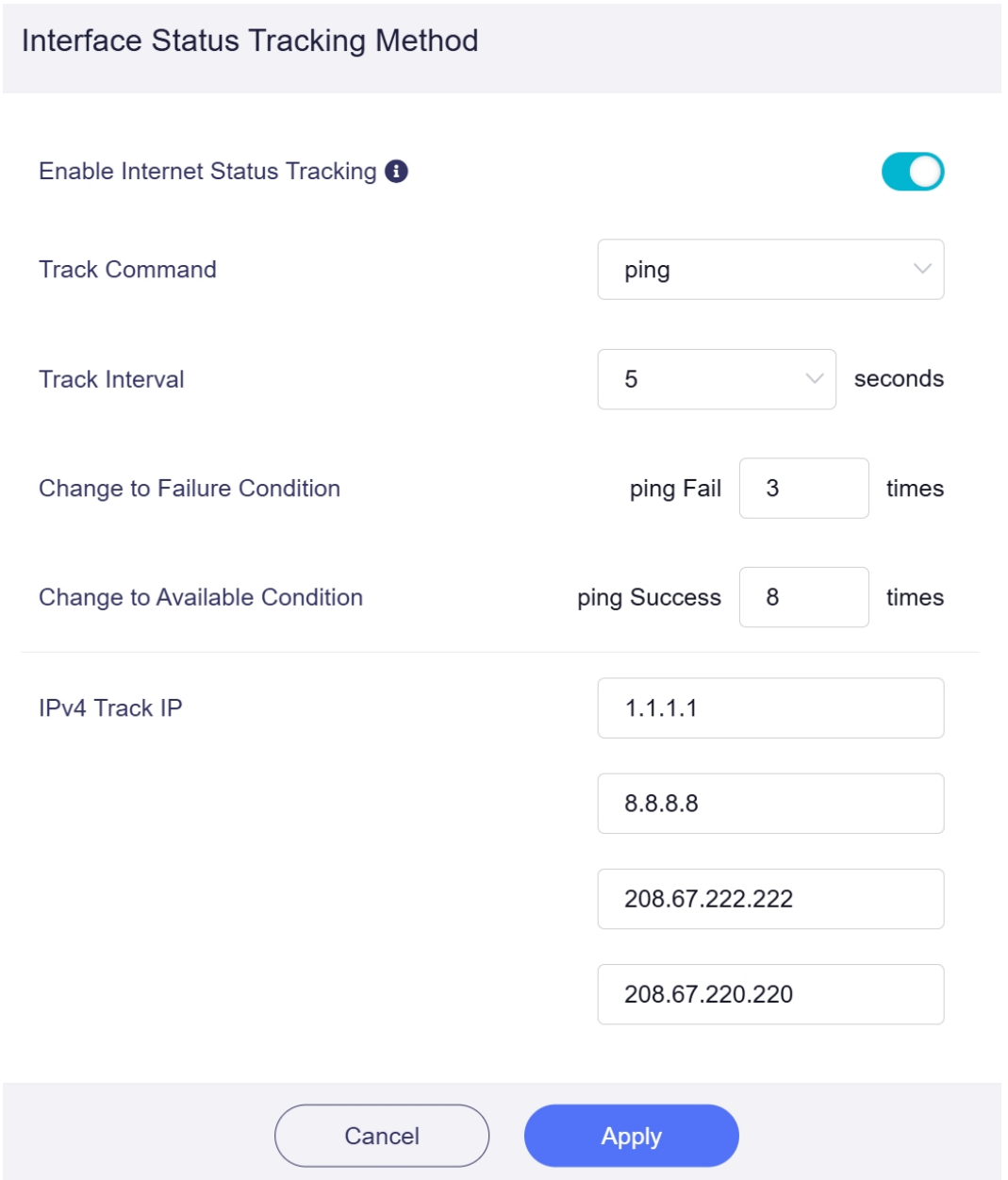
13.2.1 Seguimiento del estado de la interfaz

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



En la sección **Seguimiento del estado de la interfaz**, Haga clic en el icono de engranaje a la derecha para acceder a la configuración de seguimiento de estado para cada interfaz de

red.haga clic en el ícono de ajustes a la derecha para acceder a la configuración de seguimiento de estado para cada interfaz de red. A continuación se muestran la configuración de seguimiento de estadoings para la interfaz Ethernet. La misma lógica de configuración se aplica a otras interfaces.



- **Habilitar seguimiento del estado de la interfaz**: Está habilitadode forma predeterminada. Si está deshabilitado, el enrutador determinará el estado de la interfaz según las condiciones (por ejemplo, si el cable Ethernet está enchufado).

- **Comando de seguimiento**: el comando ping se utiliza para monitorear el estado de la conexión a la IP de destino y verificar la interfaz. disponibilidad.
- **Intervalo de seguimiento**: establezca la frecuencia con la que el enrutador ejecuta el comando de seguimiento. La unidad es segundos.
- **Cambiar a condición de falla**: el enrutador marcará esta interfaz como desconectada después del número especificado de fallas de ping consecutivas.
- **Cambiar a condición disponible**: el enrutador restaurará la interfaz al estado de conectada después de la cantidad especificada de períodos consecutivos ping exitoso.
- **IPv4 Track IP**: Cpersonalice las direcciones IP de seguimiento IPv4 si es necesario.

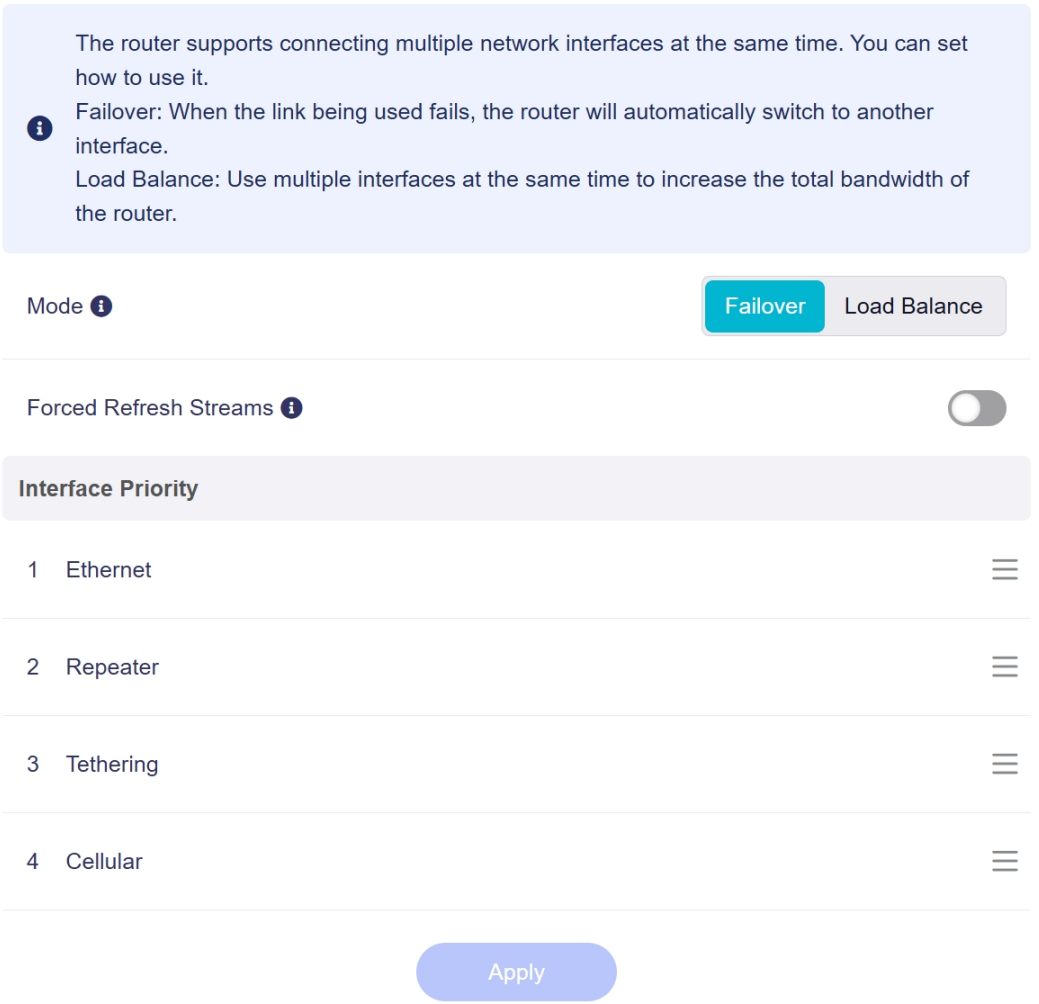
13.2.2 Modo Multi-WAN

Tdos 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.

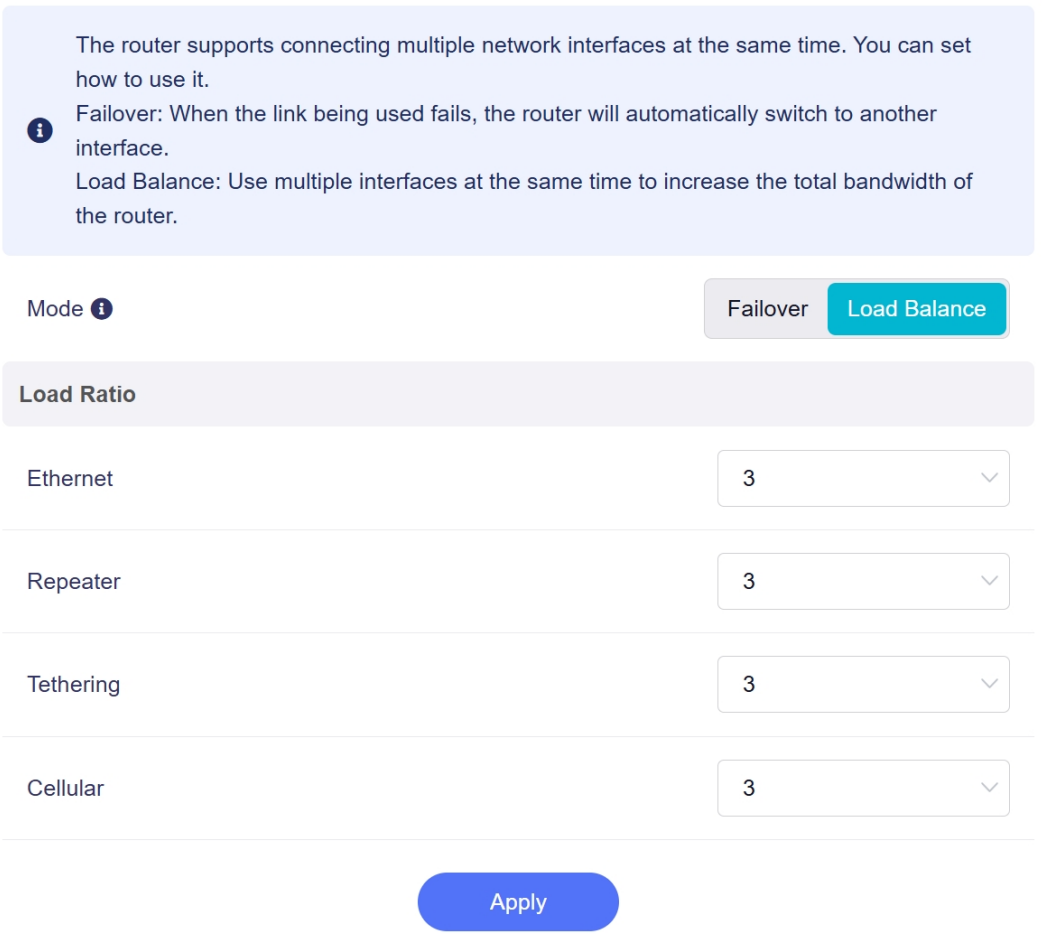
Puede establecer niveles de prioridad para cada interfaz: cuando la interfaz utilizada actualmente falla, el enrutador cambia a la siguiente interfaz disponible con la mayor prioridad. Una vez que se restablece una conexión de mayor prioridad, el enrutador volverá automáticamente a su modo.



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 redes (por ejemplo, Ethernet , Repetidor, Anclaje a red, y Celular) simultáneamente y todas las 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 interfaces de acuerdo con la relación de carga 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 otras conexiones están 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.

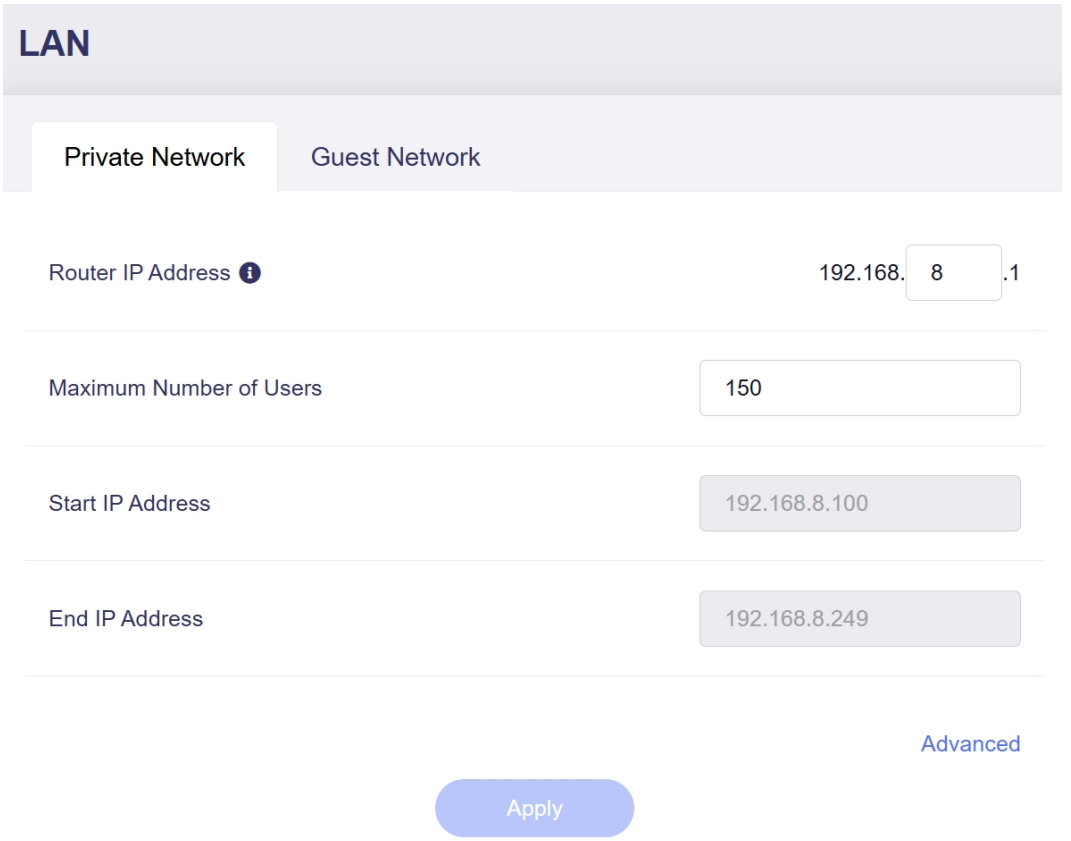
13.3 LAN

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

Inicie sesión en el panel de administración web de su enrutador'y navegue a **RED** > **LAN** . Aquí puede configurar los ajustes de LAN, incluida la red privada y la red de invitados.

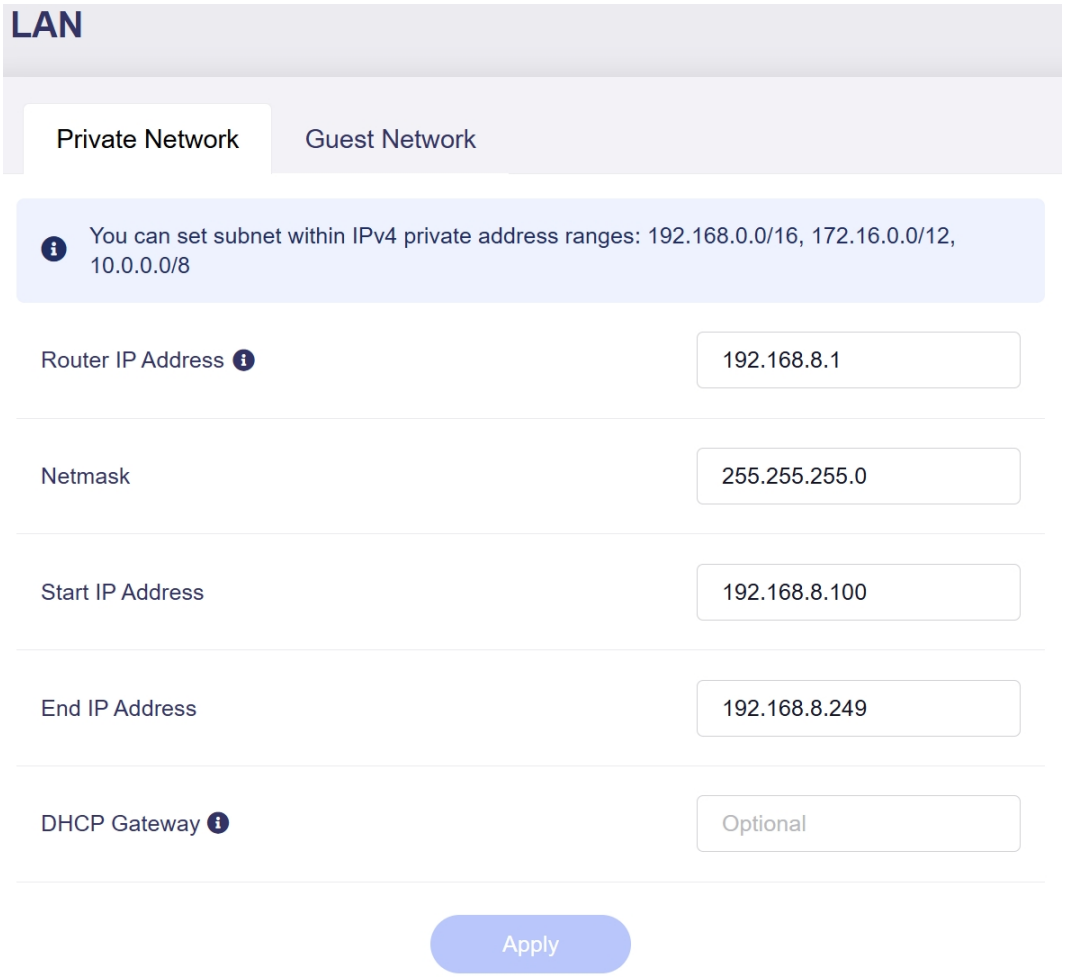
13.3.1 Red privada

La red privada es la red local principal para sus dispositivos conectados. Puede configurar la dirección IP del enrutador, el rango de direcciones DHCP y el número máximo de clientes conectados.



- **Dirección IP del enrutador**: esta es la dirección ingresada en la barra de direcciones del navegador para acceder al panel de administración del enrutador'. Es 192.168.8.1 de forma predeterminada y se puede cambiar si entra en conflicto con la red ascendente.
- **Número máximo de usuarios**: Establezca el número máximo de clientes permitidos para conectarse a la red de invitados.

Haga clic en **Avanzado** para modificar la configuración avanzada, incluida la puerta de enlace predeterminada, la máscara de red y la IP de inicio. Dirección, dirección IP final y puerta de enlace DHCP.

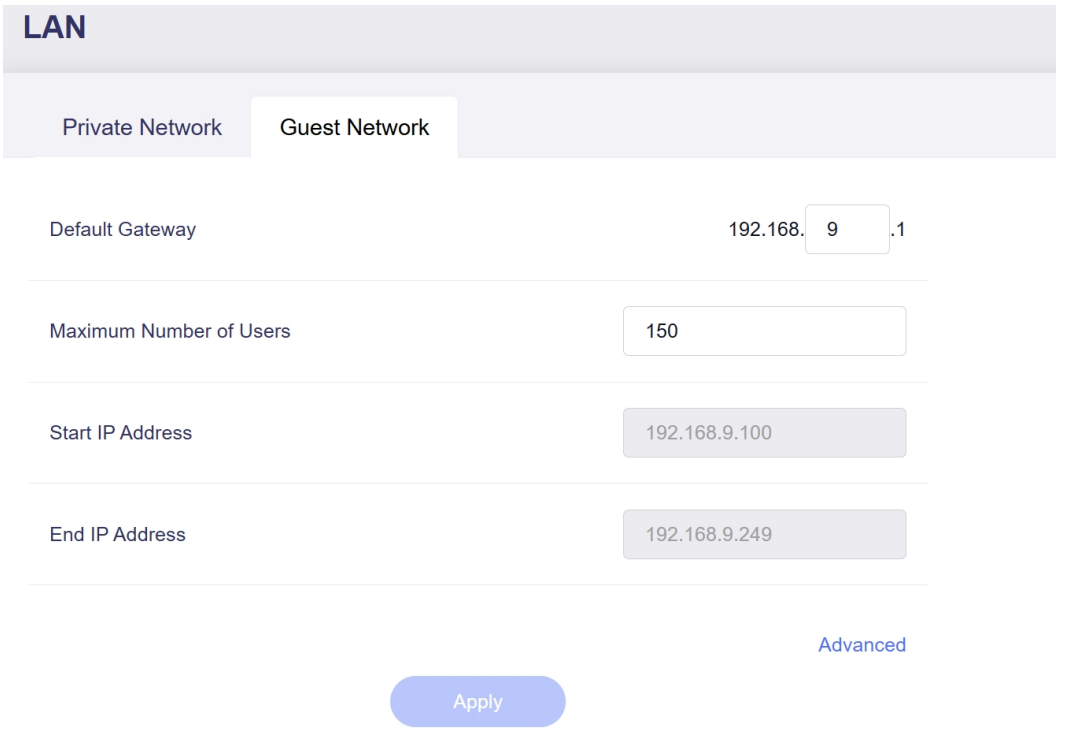


- **DHCP Puerta de enlace**: La dirección de puerta de enlace predeterminada asignada a los clientes por el servidor DHCP. Enruta el tráfico de la red local a redes externas, como Internet.
- **Máscara de red**: la máscara de subred para la red privada. El valor predeterminado es 255.255.255.0.

13.3.2 Red de invitados

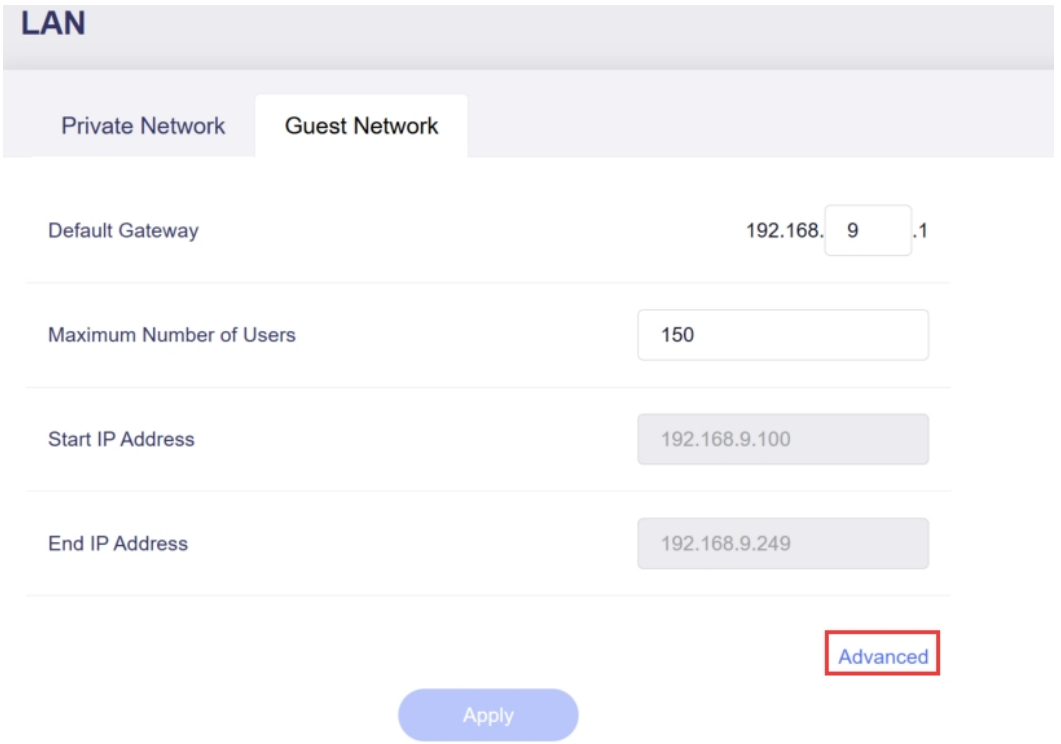
Red de invitados se refiere a una red dedicada a la que los visitantes pueden conectarse, aislándolos de su LAN principal para proteger la seguridad de su red privada.

Inicie sesión en el panel de administración web de su enrutador y vaya a **RED** > **LAN** > **Red de invitados**. Esta página le permite configurar los ajustes de la red de invitados.

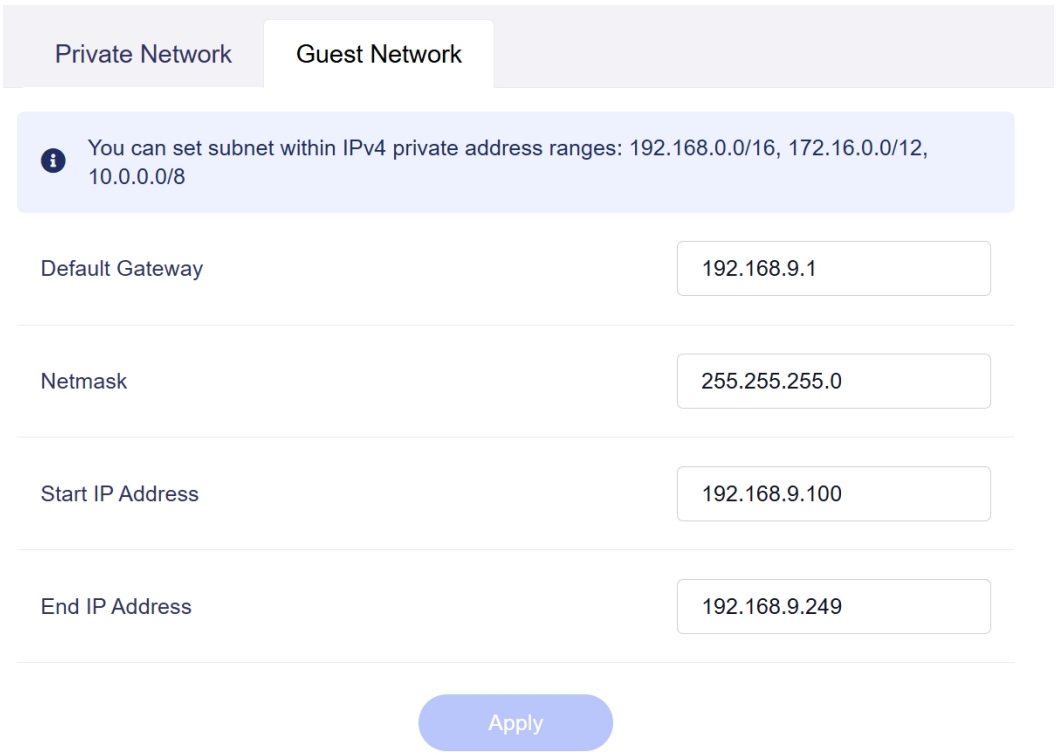


- **Puerta de enlace predeterminada**: Es 192.168.9.1 de forma predeterminada y se puede cambiar si es necesario, pero no debe entrar en conflicto con la puerta de enlace de la red principal.
- **Número máximo de usuarios**: Establezca el número máximo de clientes permitidos para conectarse a la red de invitados.

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



Podrá configurar ajustes avanzados, incluyendo puerta de enlace predeterminada, máscara de red, dirección IP inicial y dirección IP final.



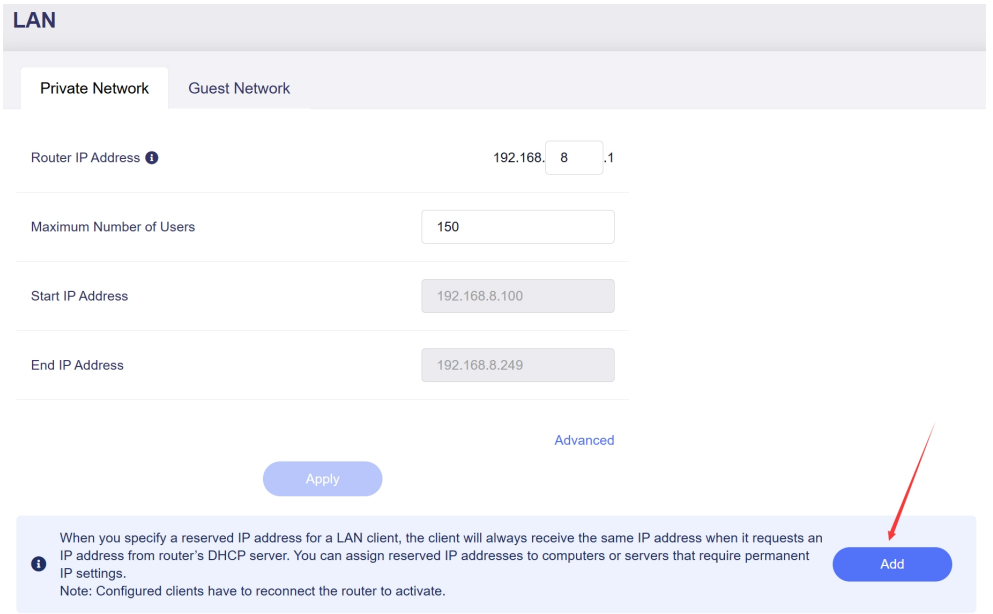
La **máscara de red** del valor predeterminado es 255.255.255.0. También puede seleccionar 255.255.0.0 si necesita una subred más grande con más direcciones IP.

13.3.3 Reserva de direcciones

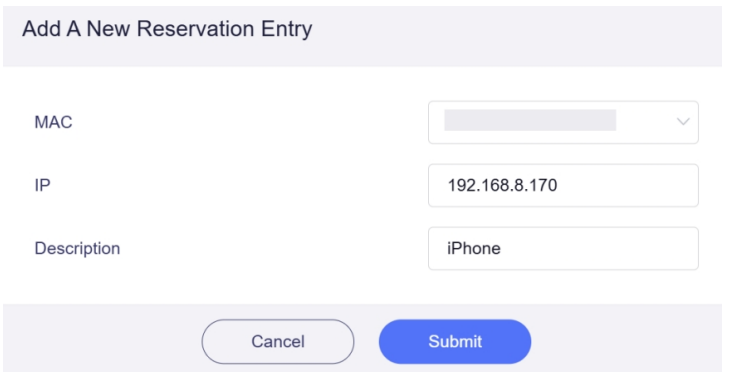
La reserva de dirección le permite especificar una dirección IP fija para un cliente LAN, de modo que el cliente siempre reciba la misma dirección IP cada vez que acceda al servidor DHCP del enrutador. Puede asignar direcciones IP reservadas a computadoras o servidores que requieren una configuración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

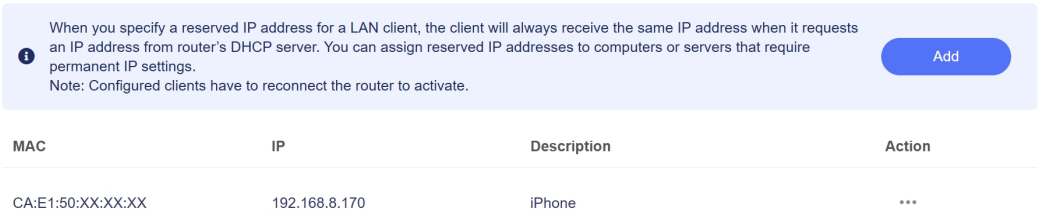
1. Registro en tu enrutador', navegue hasta **RED** > **LAN** > **Reserva de direcciones** y haga clic en **Agregar**.



2. En la ventana emergente, seleccione la dirección MAC de la lista desplegable, luego lala correspondiente IP dirección para la MAC seleccionada se completará automáticamente. Introduzca un nombre descriptivo y haga clic en **Enviar**.



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



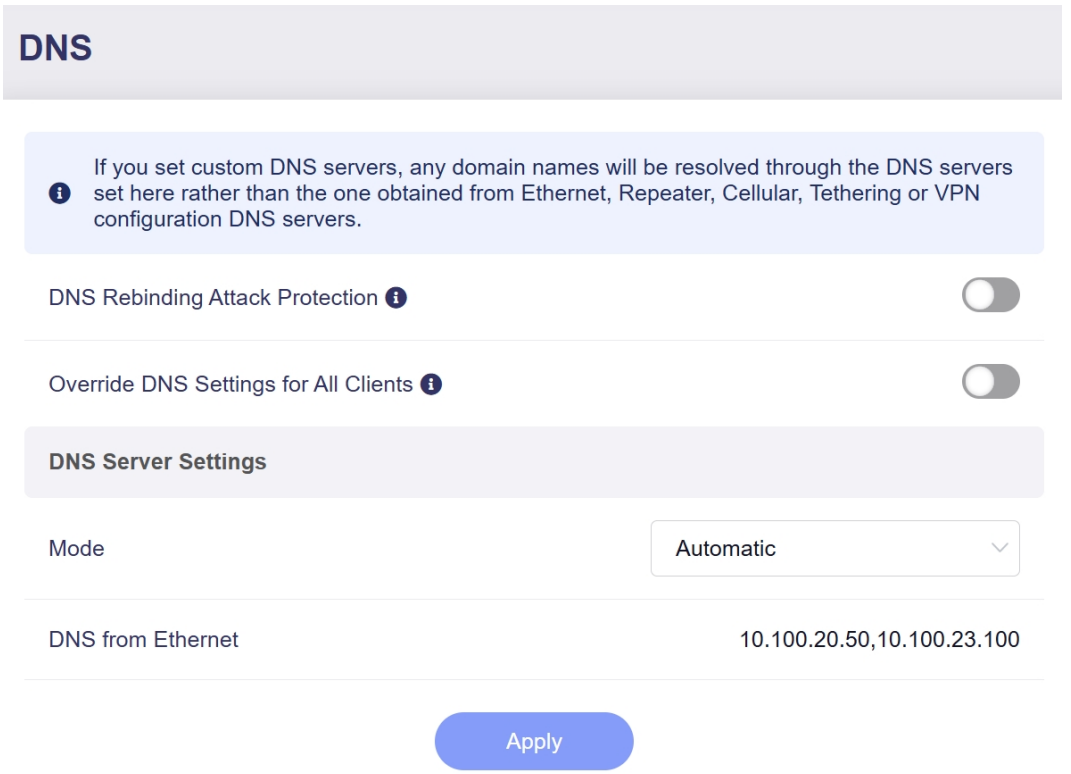
13.4 DNS

DNS (Sistema de nombres de dominio) es un servicio 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.

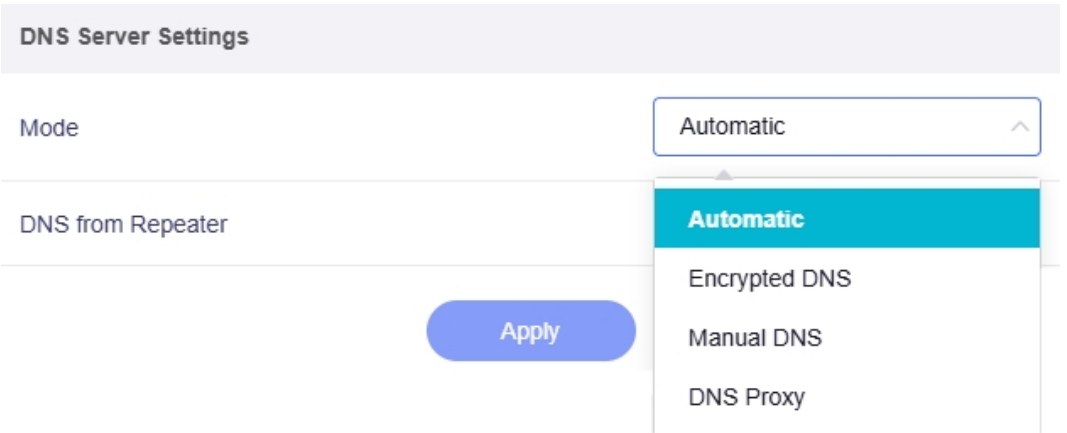
13.4.1 Configuración general



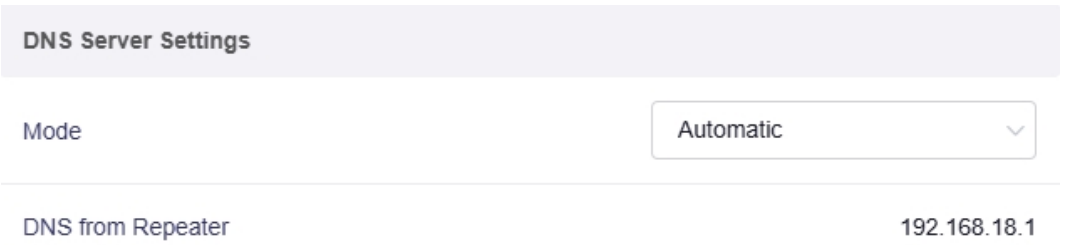
- **Protección contra ataques de revinculación de DNS**: protege contra ataques de revinculación de DNS bloqueando intentos maliciosos de resolución de DNS. Tenga en cuenta que habilitarlo puede causar fallas en la búsqueda de DNS privado; deshabilítelo si su red utiliza un portal cautivo (por ejemplo, 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.

13.4.2 Configuración del servidor DNS

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

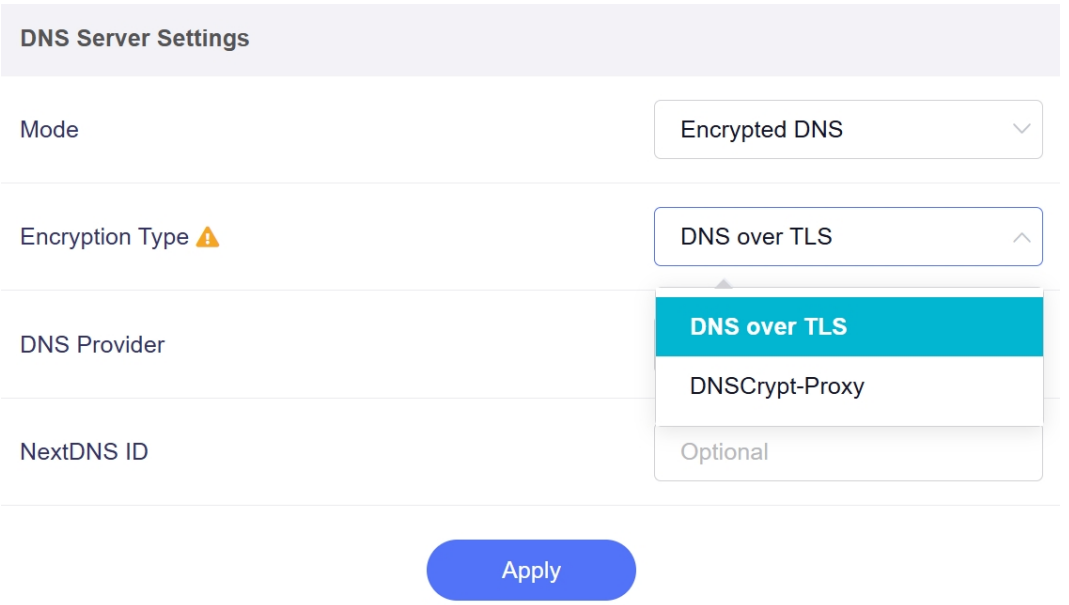


1. **Automático**: cuando se selecciona, el enrutador obtendrá automáticamente las direcciones del servidor DNS de la red ascendente y las aplicará a todos los dispositivos conectados.



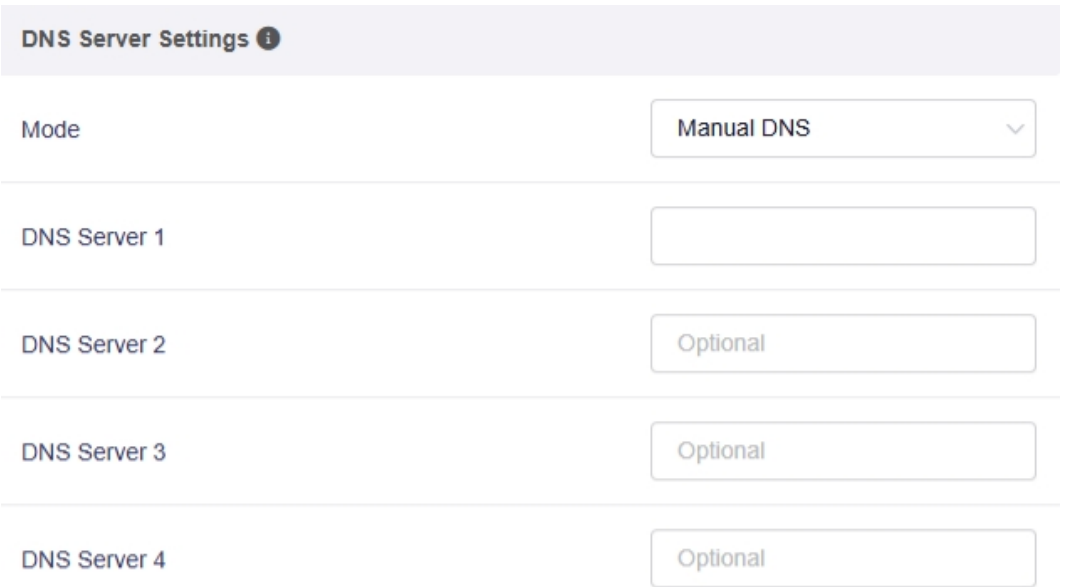
2. **DNS cifrado**: cuando se selecciona, el enrutador utilizará protocolos cifrados para procesar consultas DNS, protegiendo los datos de resolución contra escuchas o manipulación.

Tiene dos tipos de cifrado: DNS sobre TLS y DNSCrypt-Proxy.



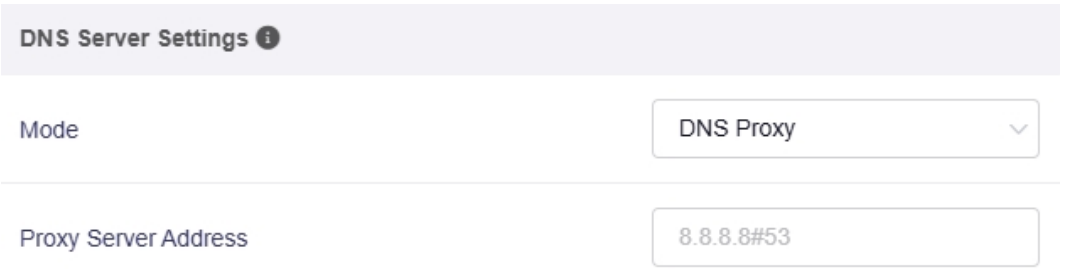
- Para DNS sobre TLS, seleccione un proveedor de DNS entre Control D, NextDNS y Cloudflare.
- Para DNSCrypt-Proxy, seleccione al menos un servidor DNS del repositorio. Se pueden seleccionar hasta 8 servidores. Cuando se seleccionan varios servidores, el enrutador utilizará el más rápido automáticamente.

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.

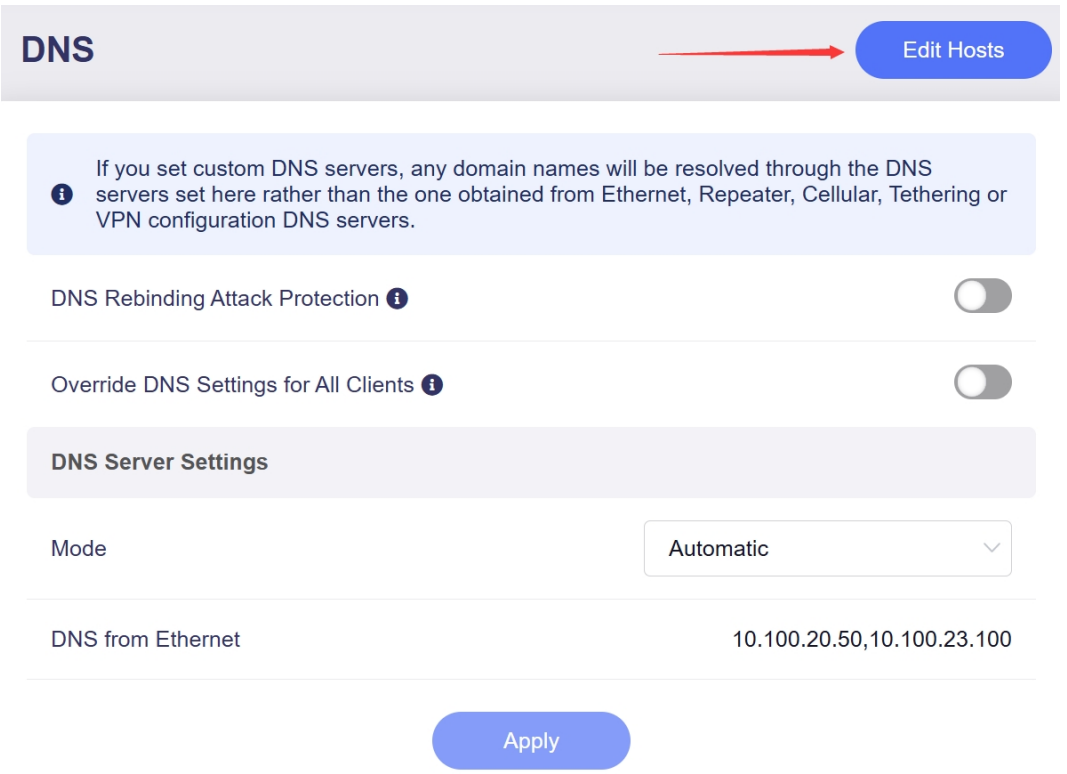
4. **Proxy DNS**: cuando se selecciona, el enrutador reenvía todas las consultas DNS a través de un servidor proxy, permiteresolución a través del entorno de red del proxy para necesidades de acceso específicas.



13.4.3 Editar hosts

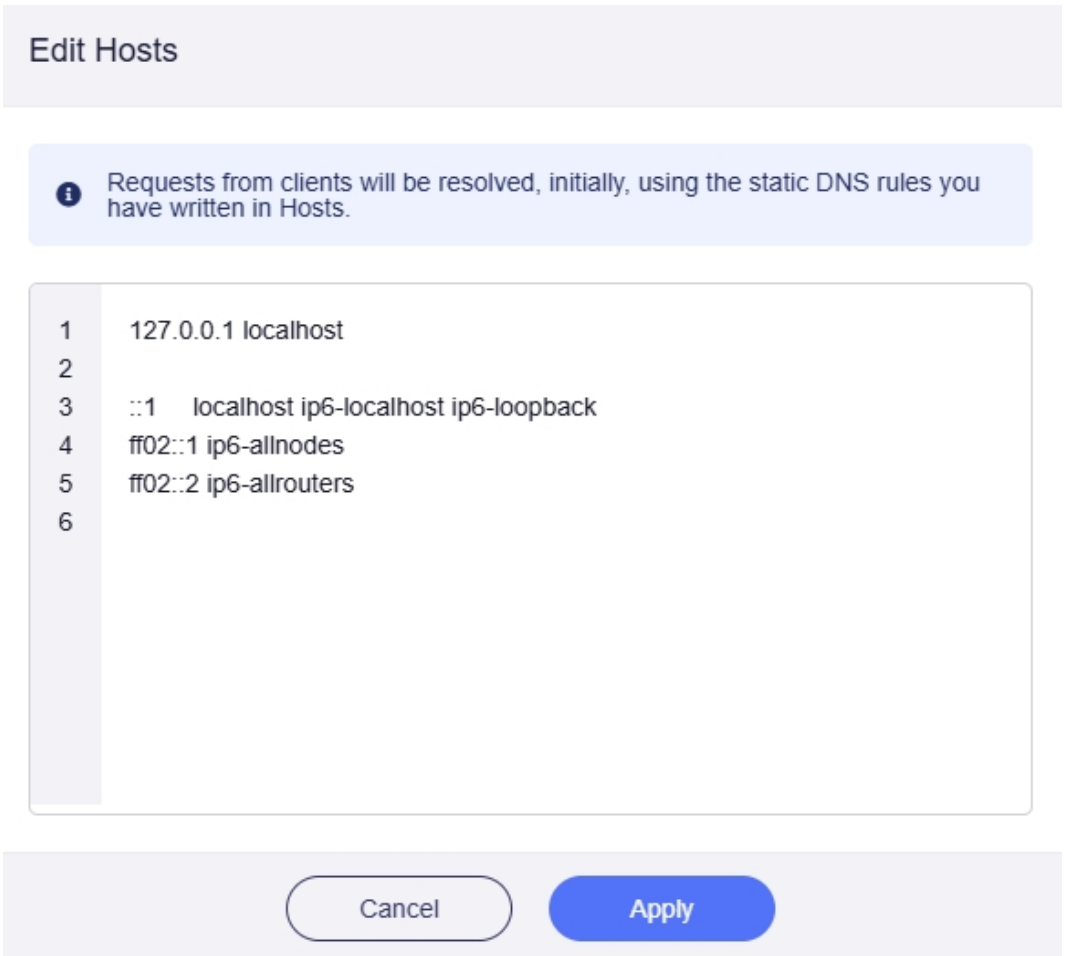
Puede definir reglas de resolución de DNS estáticas si es necesario.

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 de DNS estáticas escritas aquí, lo que le permitirá asignar manualmente direcciones IP a nombres de

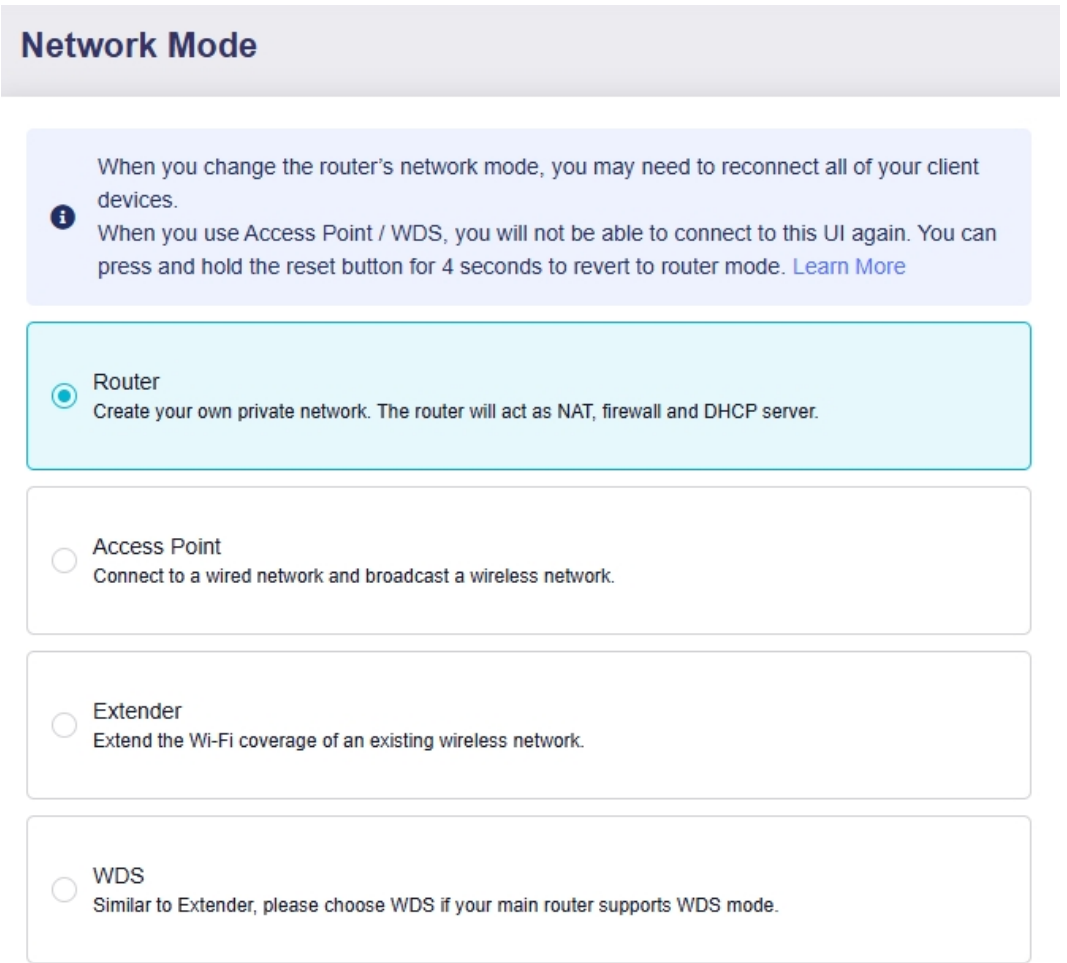
host (por ejemplo, las entradas predeterminadas como 127.0.0.1 localhost para loopback local) para un control personalizado de la resolución de nombres de dominio.



13.5 Modo de red

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

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



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

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

Nota:

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

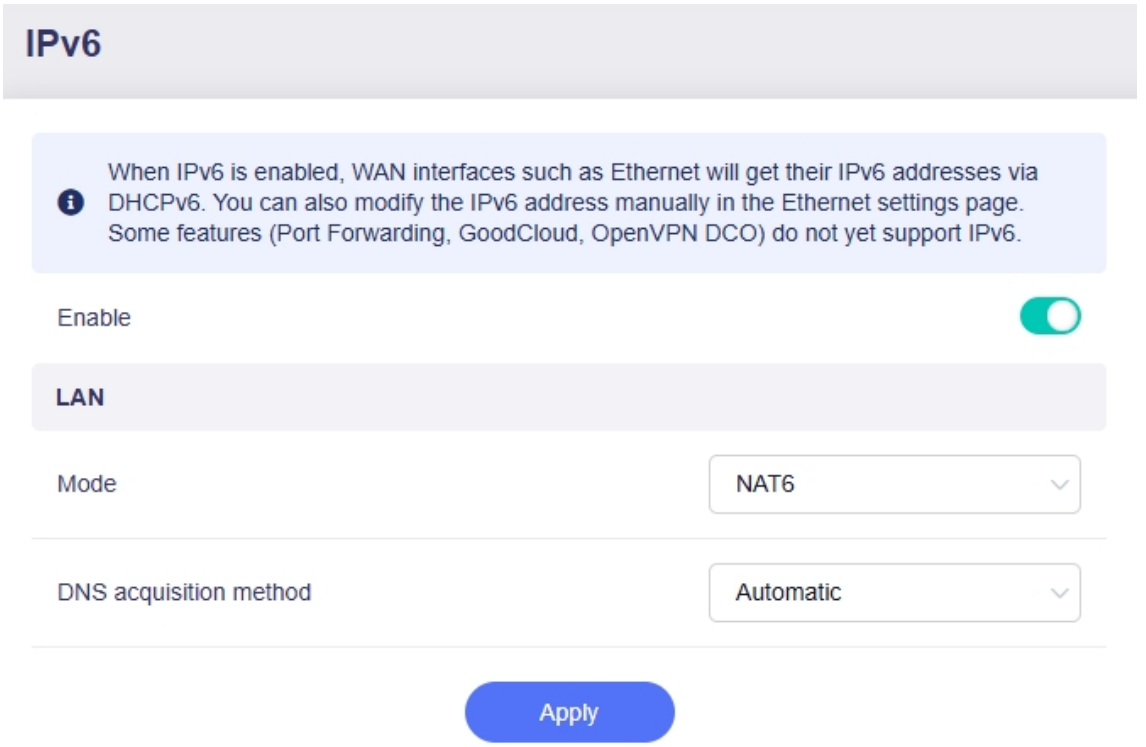
3. **En el modo Punto de acceso/Extensor/WDS, las siguientes funciones no estarán disponibles**: Control de acceso (lista de permitidos y de bloqueo), VPN, Firewall, Multi-WAN, servidor DHCP, reserva de direcciones, red de invitados, DNS, IPv6, vigilancia IGMP.

13.6 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.

Alternar en **Enable**, 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) aún no son compatibles con IPv6. Si habilita estas funciones e IPv6 al mismo tiempo, es probable que cause problemas de conectividad .

13.6.1 Modo IPv6

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

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

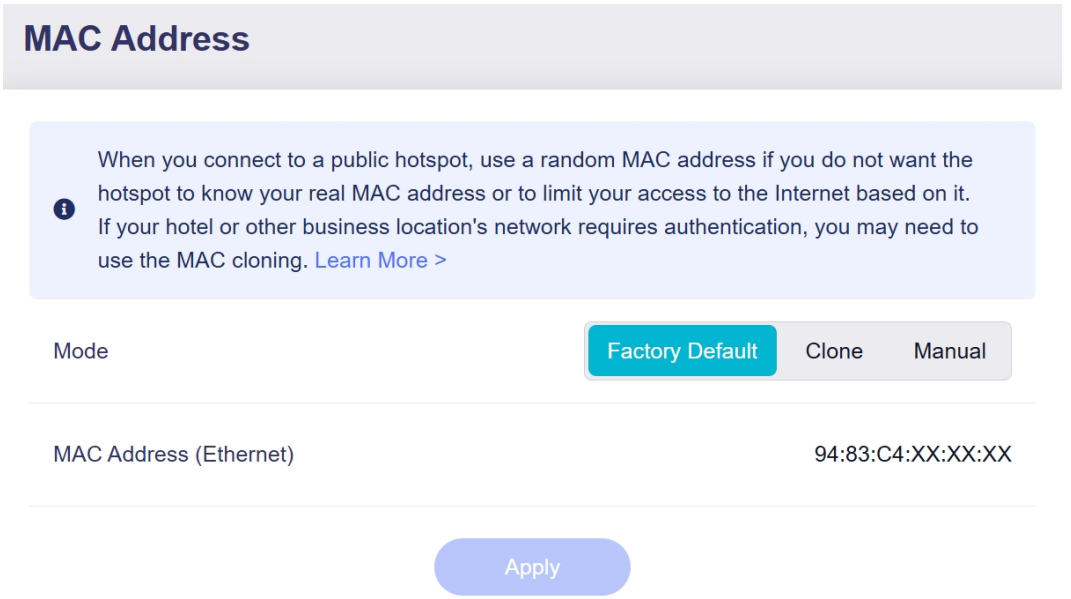
13.6.2 Método de obtención de DNS

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

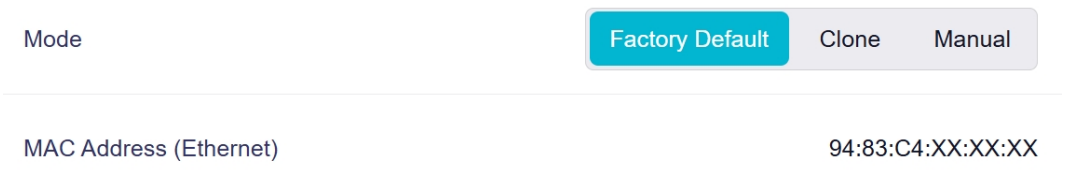
- **Automático**: el enrutador obtendrá direcciones de servidor DNS IPv6 dinámicamente (por ejemplo, a través de DHCPv6).
- **Manual**: ingrese direcciones de servidor DNS IPv6 personalizadas. Sin embargo, dado que DNS se utiliza para resolver nombres de dominio en sus direcciones IP correspondientes,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

13.7 Dirección MAC

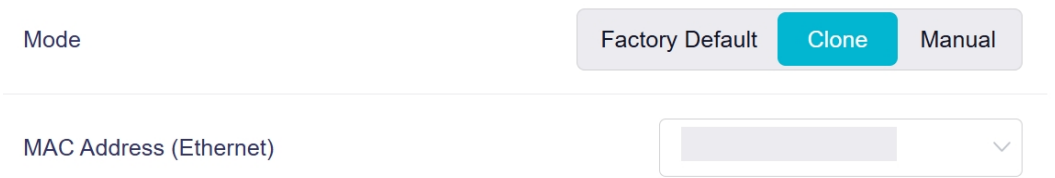
La Dirección MAC página pantallas la dirección MAC predeterminada del enrutador, clonar la dirección MAC de un cliente, ingresar una dirección MAC manualmente o generar una dirección MAC aleatoria. Si el dispositivo admite la configuración de varios puertos Ethernet para usarlos como puertos WAN, puede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



- La dirección MAC predeterminada de fábrica.



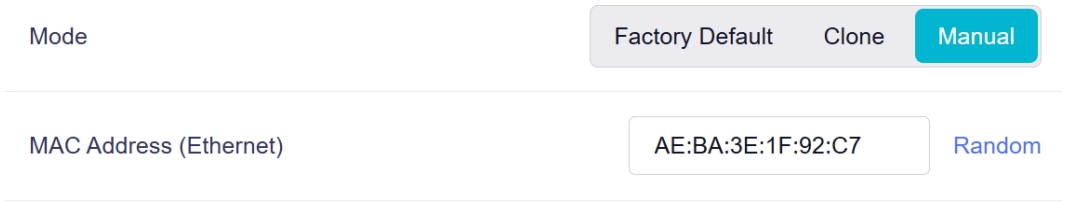
- Clonar la dirección MAC de un cliente.



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

puede denominarse dirección Wi-Fi privada o dirección de hardware aleatoria en diferentes dispositivos.

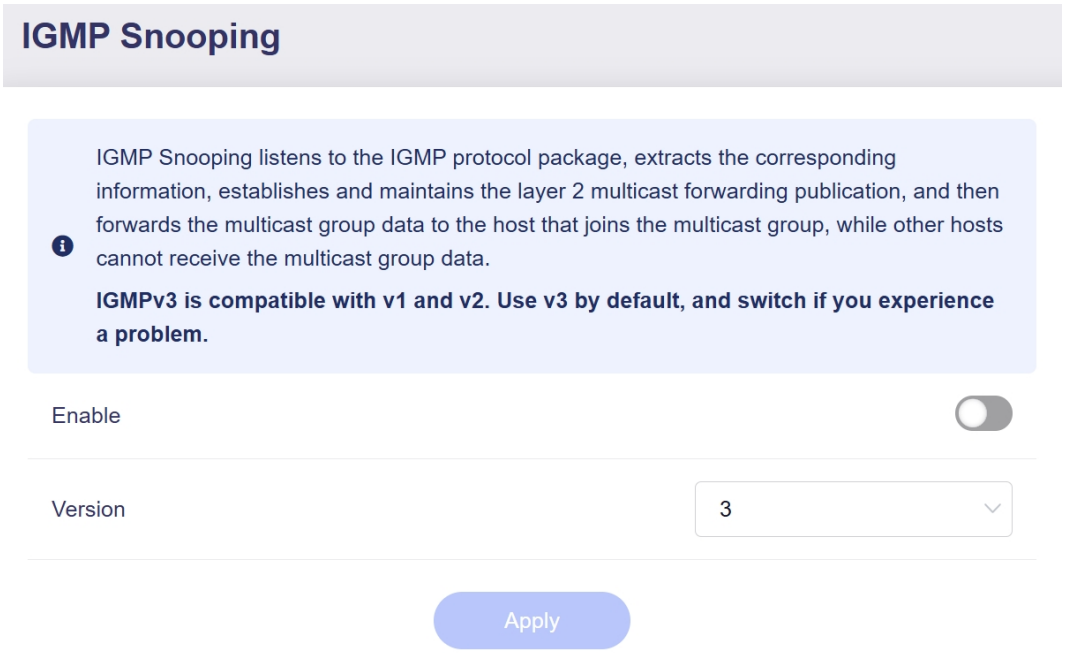
- Ingrese manualmente o genere una dirección MAC aleatoria.



13.8 Inspección IGMP

IGMP Snooping escucha el paquete de protocolo IGMP, extrae la información correspondiente, establece y mantiene el 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**. Puedes habilitar para usar la función de multidifusión en tu enrutador si necesario.



Capítulo 14

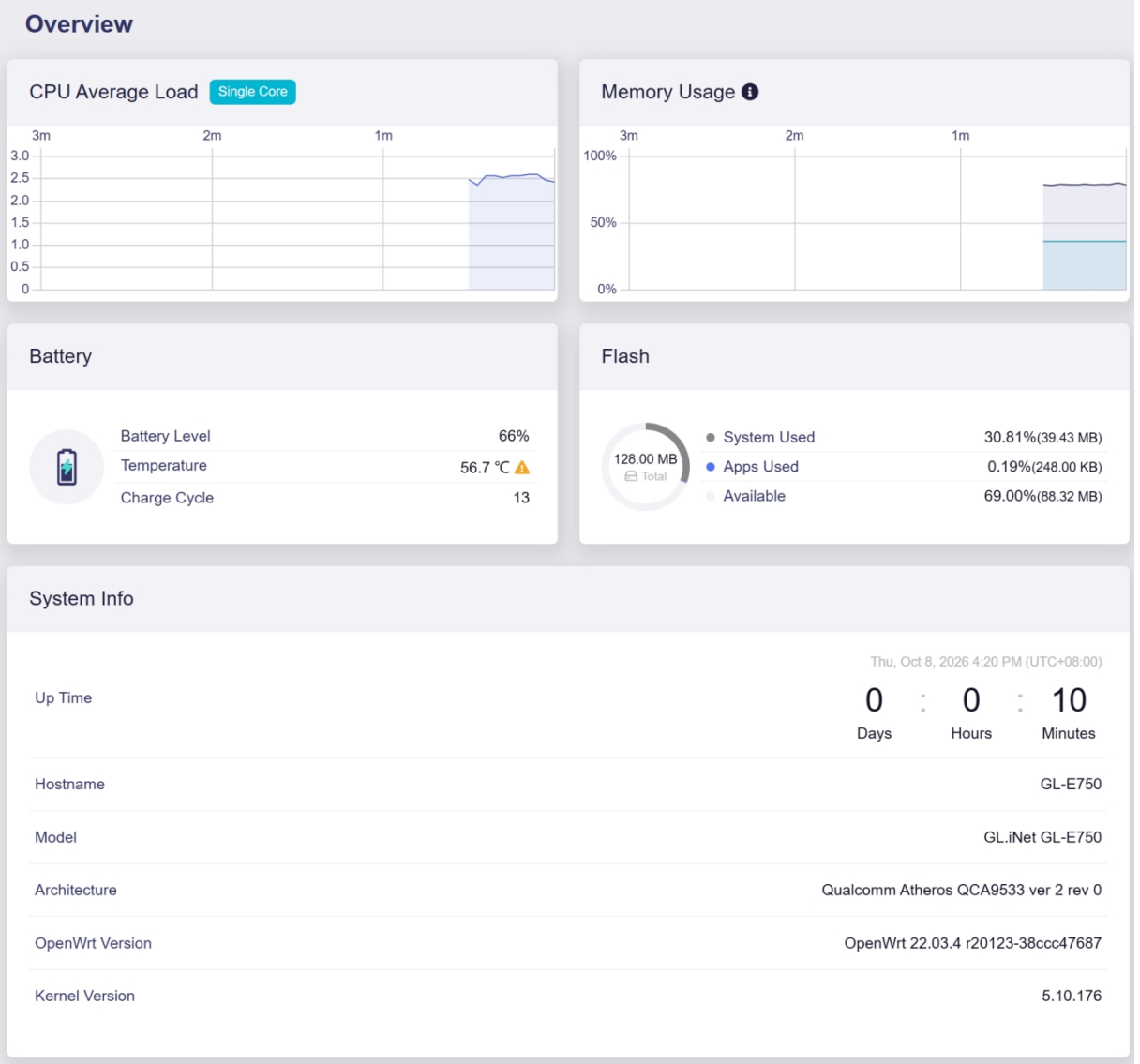
Sistema

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

14.1 Descripción general

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

- CPU, memoria, y Flash Estado
- Estado de la batería
- Dispositivo IInformación

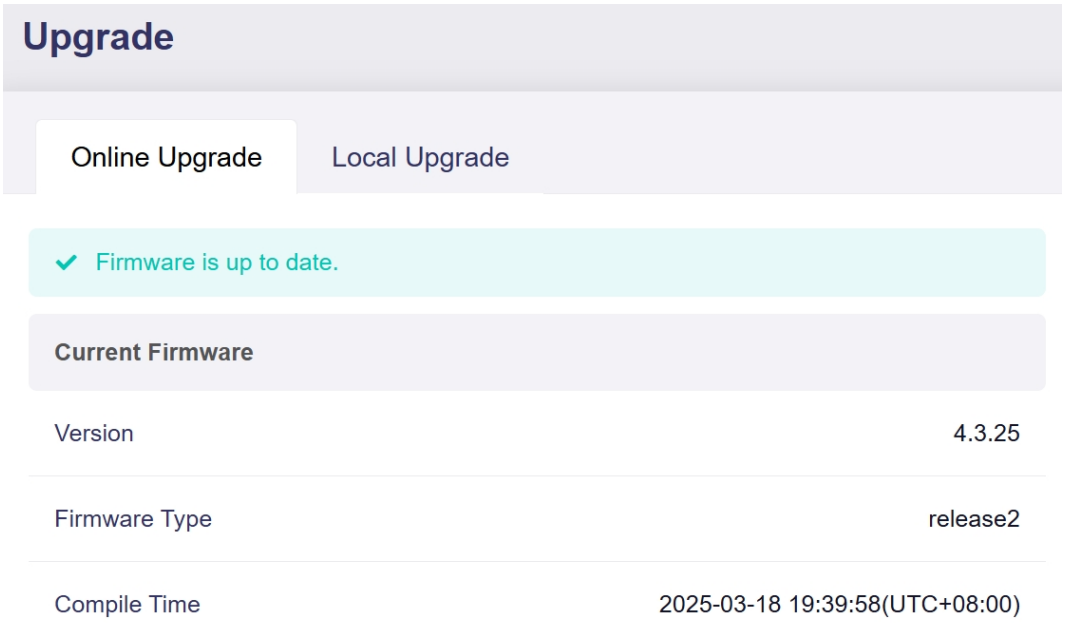


14.2 Actualización

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

14.2.1 Actualización en línea

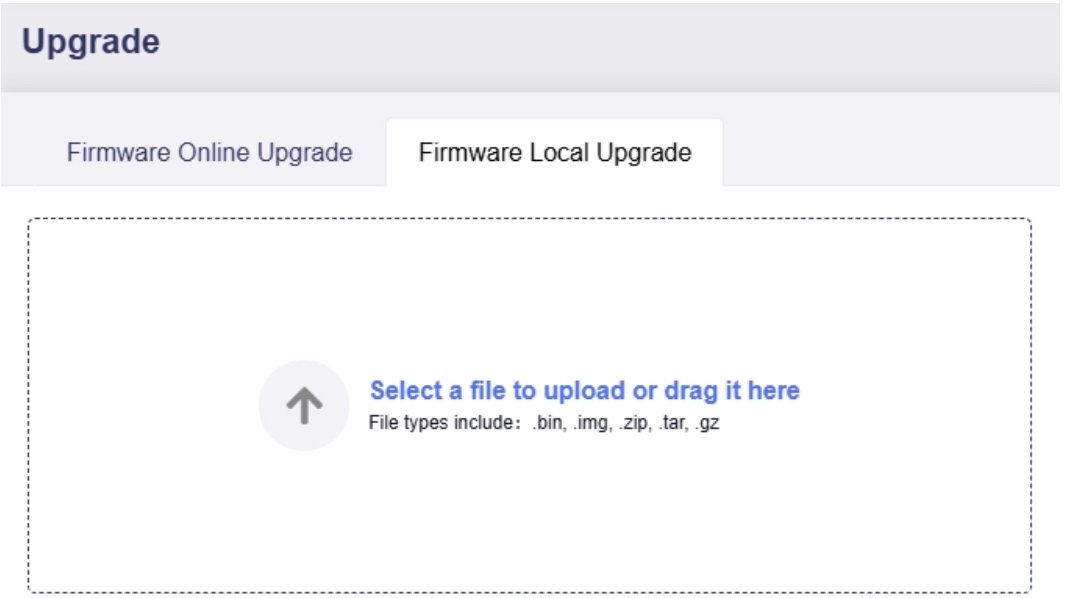
Puede buscar el firmware actual detalles aquí, incluida la versión del firmware, el tipo de firmware (por ejemplo, versión, beta) y el tiempo de actualización. Si su enrutador está conectado a Internet, buscará la versión de firmware más reciente disponible para descargar.



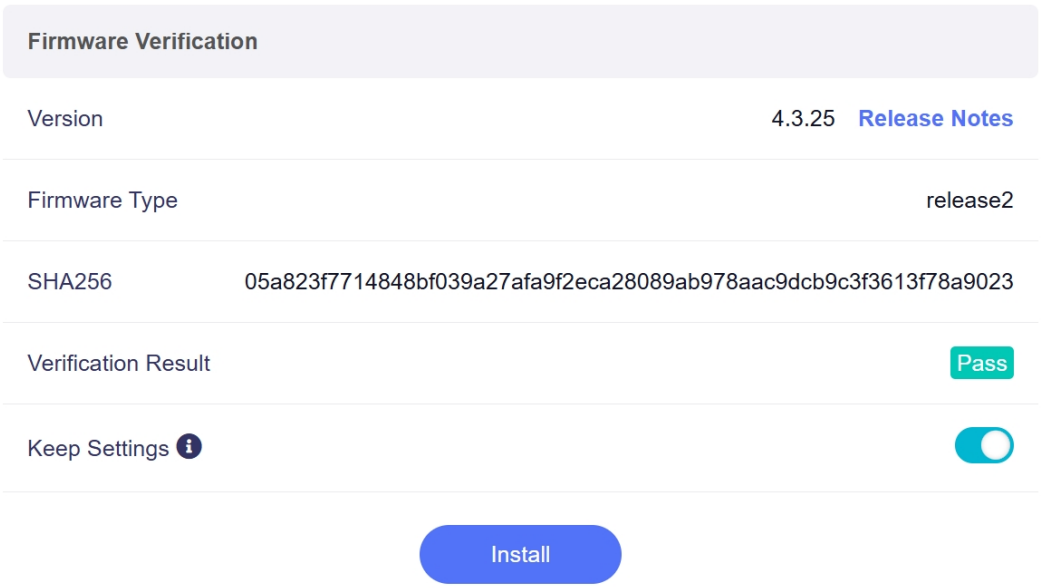
Consejo: Al intentar realizar una actualización en línea, si muestra **Descarga fallida**, navegue hasta **SISTEMA** > **Zona horaria** y solucione el error de zona horaria (sincronización con el navegador).

14.2.2 Actualización local

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



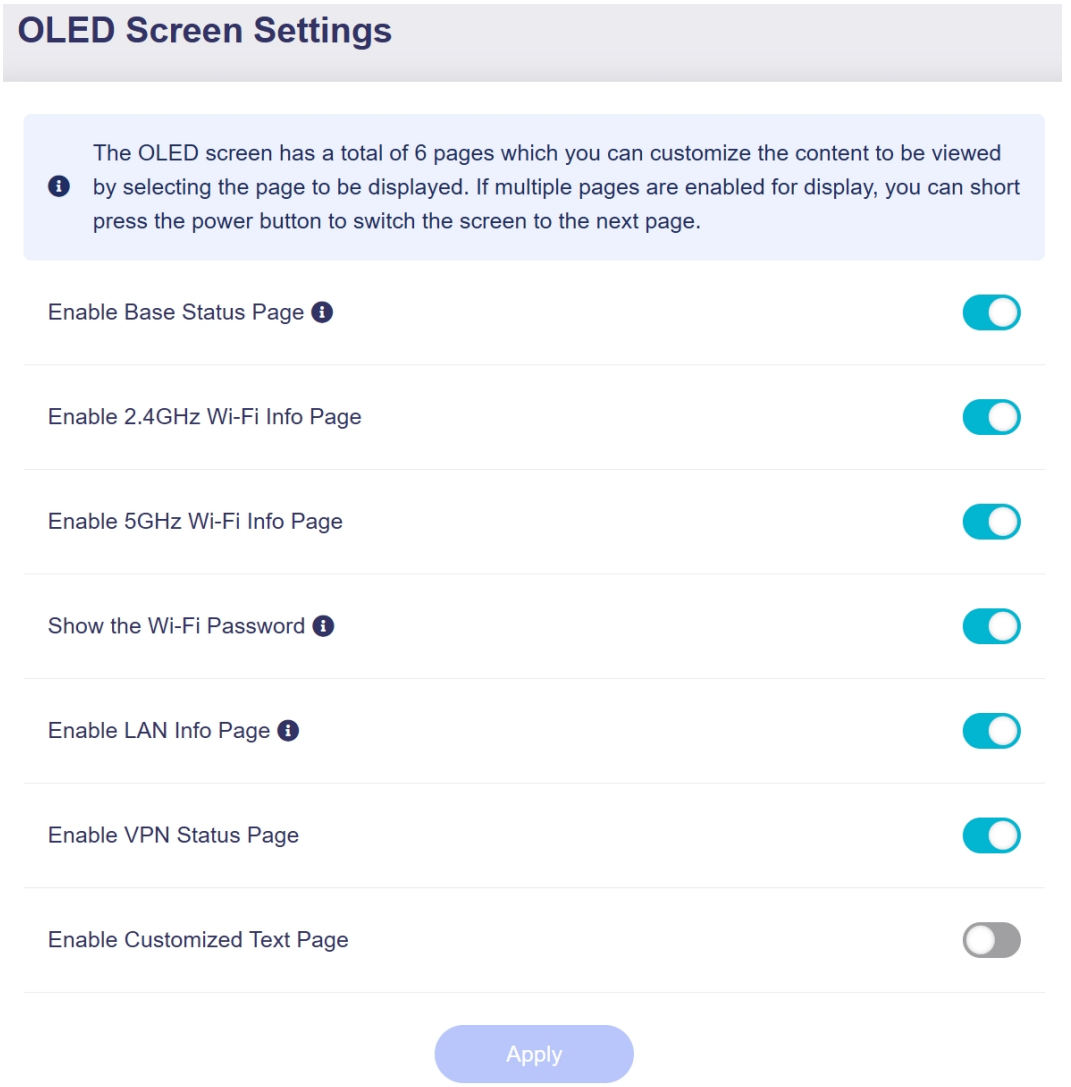
Ta página mostrará los detalles del firmware. Verifique estos detalles antes de hacer clic **Instalar**.



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

14.3 Configuración de pantalla OLED

El enrutador está equipado con una pantalla OLED que contiene 6 páginas de visualización. Puede personalizar el contenido mostrado habilitando o deshabilitando páginas individuales. Cuando varias páginas están habilitadas para su visualización, puedes presionar brevemente el botón de encendido para pasar a la siguiente página de la pantalla.



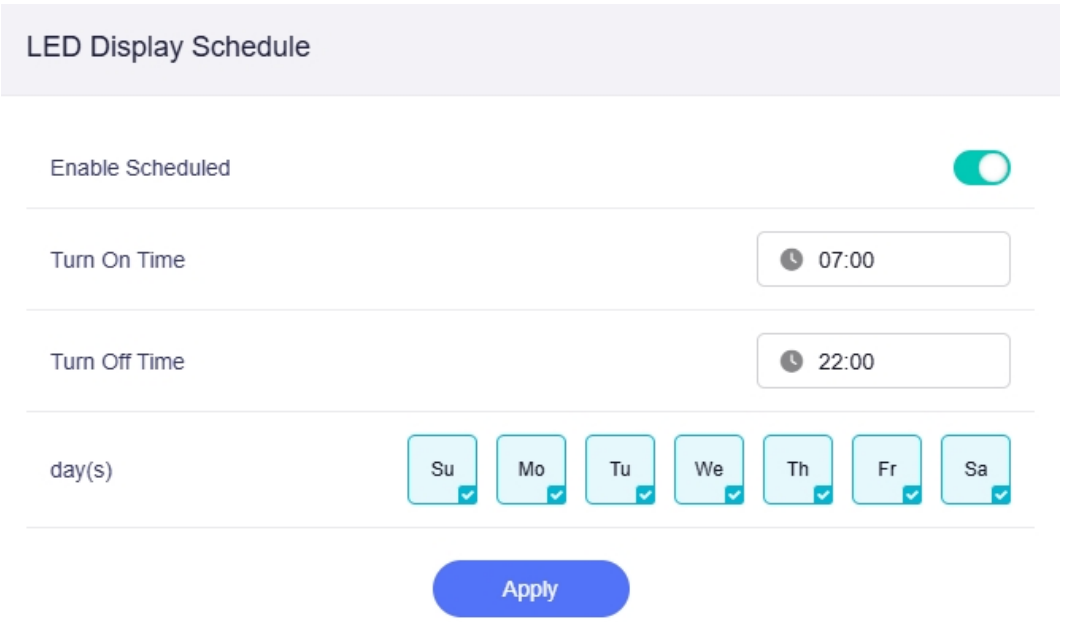
14.4 Tareas programadas

Inicia sesión en el panel de administración web de tu 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 el reinicio del enrutador.

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

14.4.1 Programación de los indicadores LED

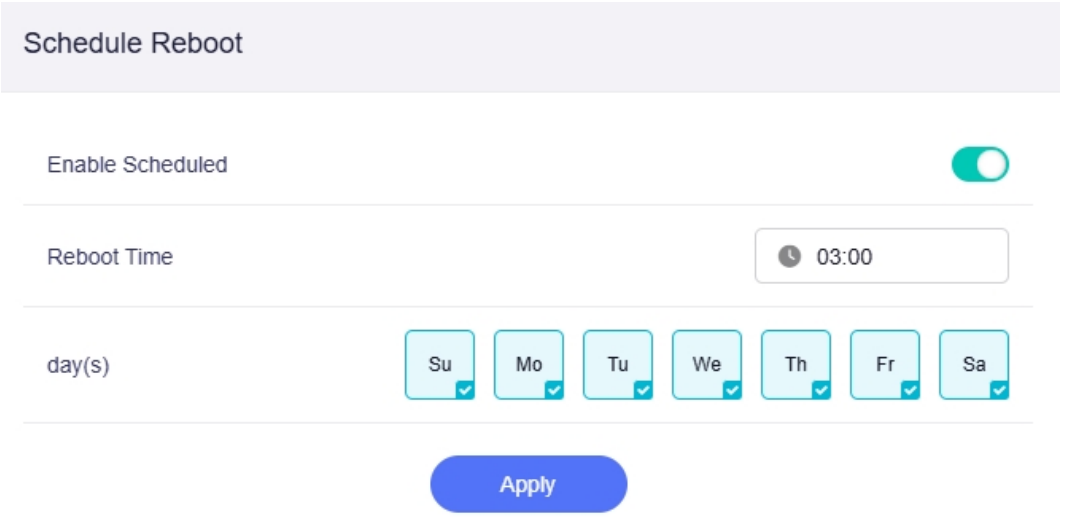
SEstablezca un programa para la luz LED de su enrutador si es necesario, luego haga clic **Aplicar**.



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

14.4.2 Programar reinicio

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



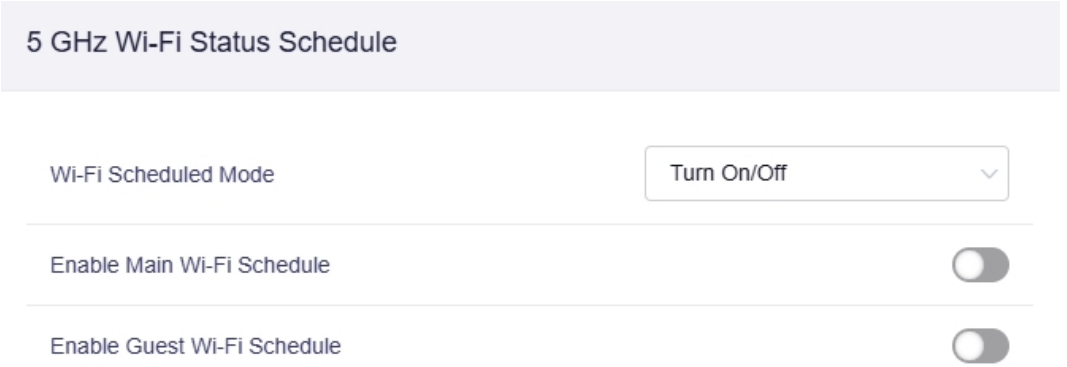
- **Habilitar Programado**: active este interruptor para habilitar el reinicio programado.
- **Hora de reinicio**: establezca la hora específica (por ejemplo, 03:00) en que se reiniciará el enrutador.
- **día(s)**: Seleccione los días efectivos de la semana para estas configuraciones.

14.4.3 Programación de Wi-Fi de 5 GHz

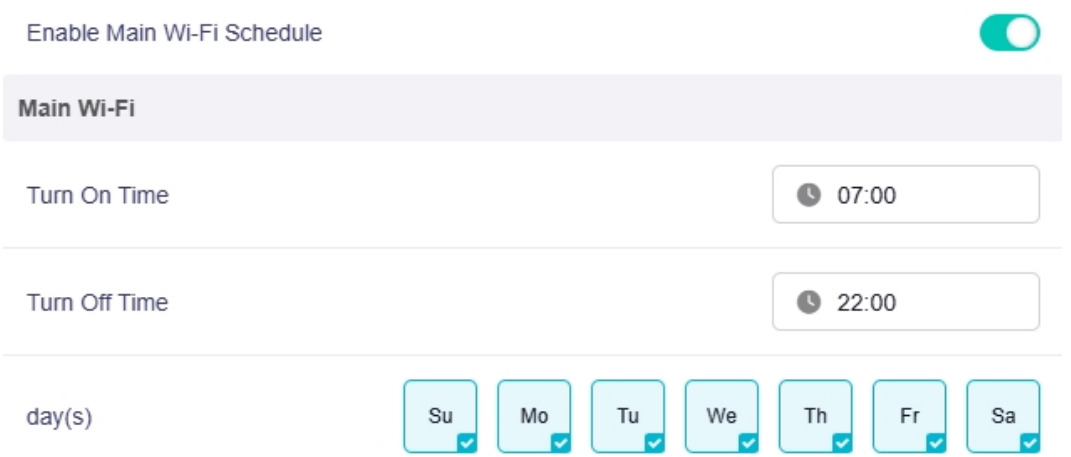
Esta función le permite establecer una programación para su Wi-Fi de 5 GHz. Hay dos modos: encender/apagar y cambiar la alimentación de TX.

Modo 1: Encender/apagar

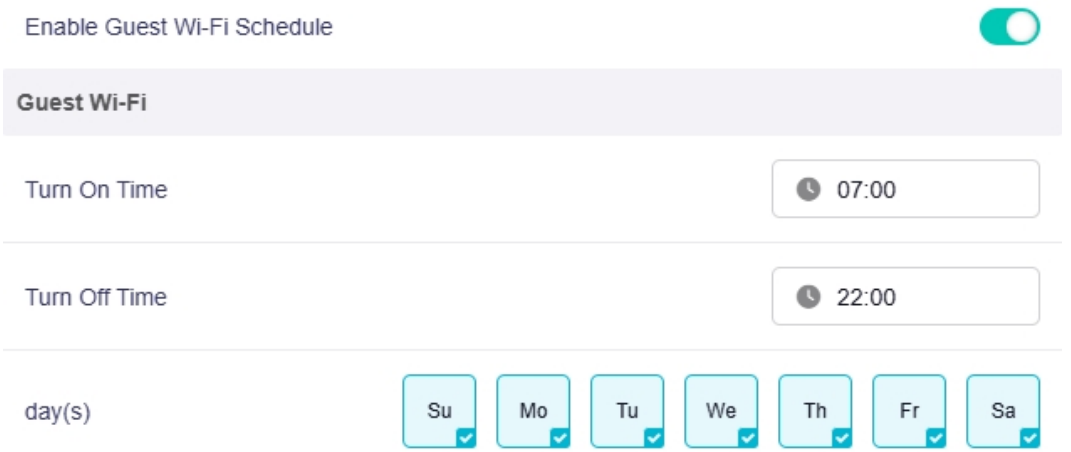
Puede habilitar el horario de encendido/apagado tanto para el Wi-Fi principal de 5 GHz como para el Wi-Fi para invitados.



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

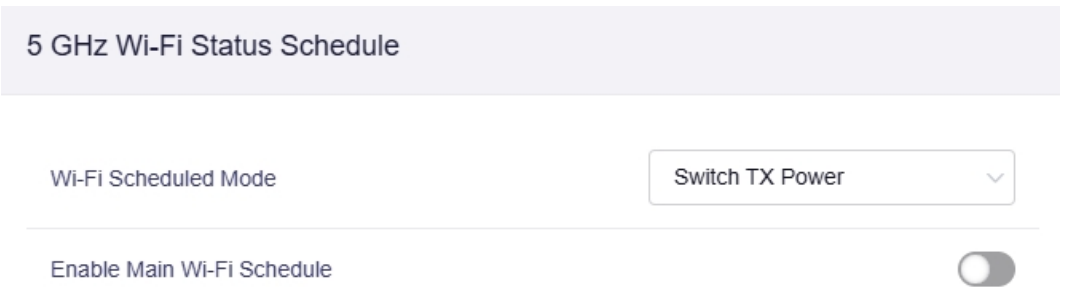


- **Programación de Wi-Fi para invitados**: cuando esté habilitado, configure los horarios de encendido y apagado de su Wi-Fi para invitados de 5 GHz y seleccione una fecha efectiva para la semana.

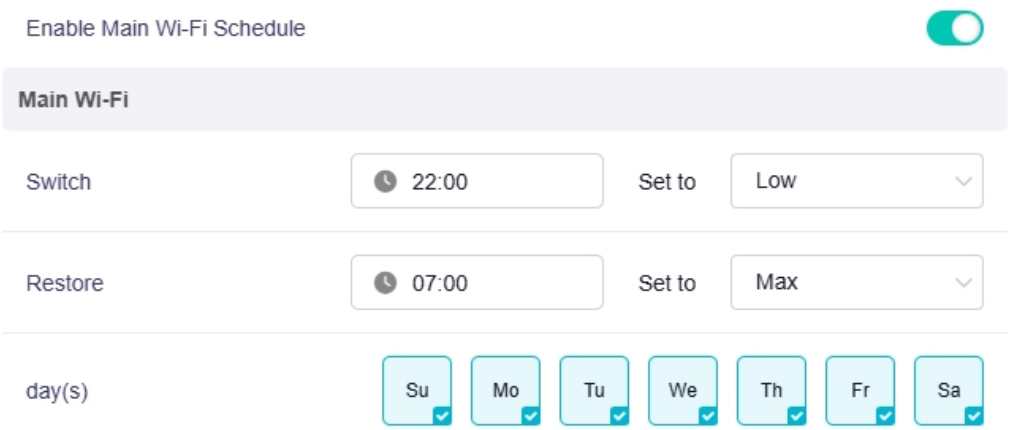


Modo 2: cambiar la alimentación de TX

YPuede habilitar el Conmutación de alimentación TX programación para los 5 GHz Principal Wi-Fi.



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



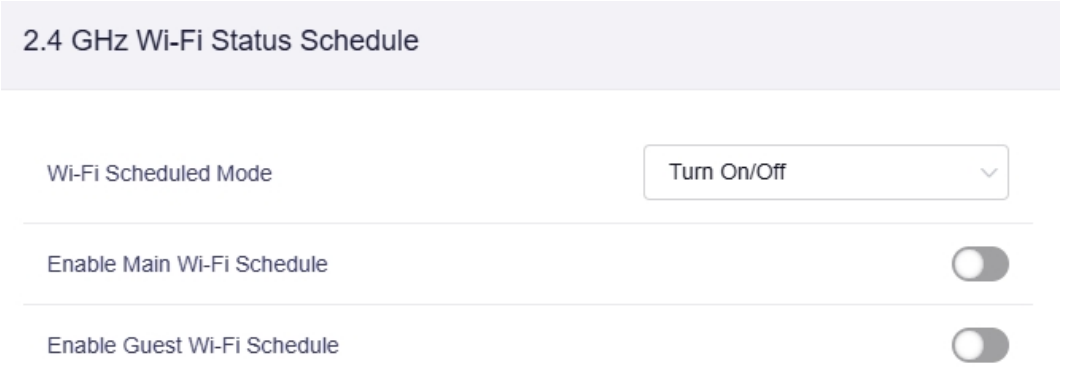
- **Cambiar**: Sestablece la potencia de TX a un cierto nivel (por ejemplo, bajo) at un hora (por ejemplo, 22:00).
- **Restaurar**: Rrestaurar la energía de TX a unotro nivel (por ejemplo, Max) aen otro momento (por ejemplo, 07:00).
- **días**: Seleccione los días efectivos de la semana para esta configuración.

14.4.4 Programación de Wi-Fi de 2,4 GHz

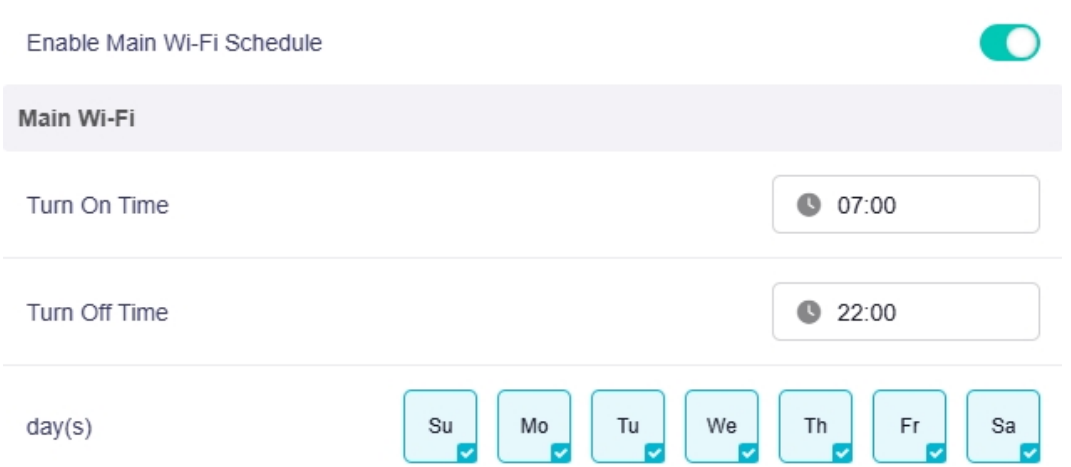
Esta función le permite establecer un horario para su Wi-Fi de 2,4 GHz. Hay dos modos: encender/apagar y cambiar la alimentación de TX.

Modo 1: Encender/apagar

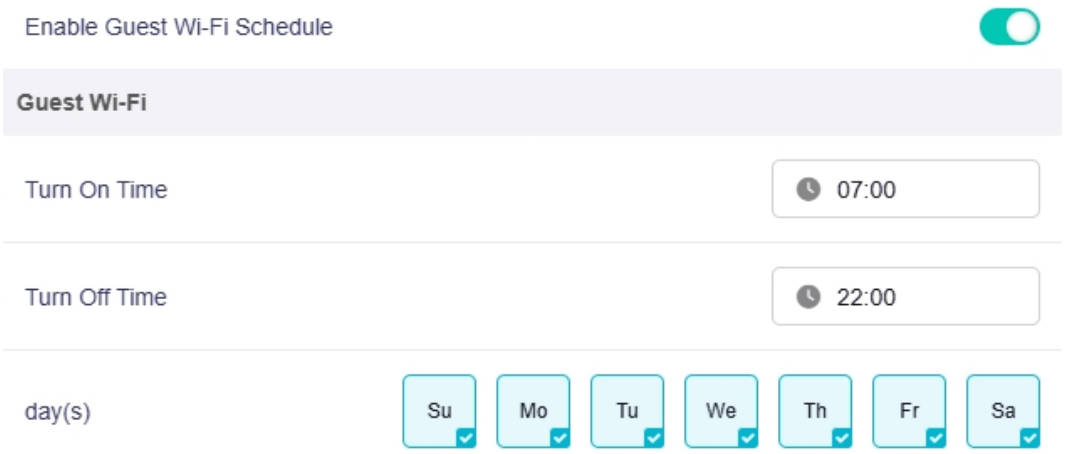
Puede habilitar el horario de encendido/apagado tanto para el Wi-Fi principal de 2,4 GHz como para el Wi-Fi para invitados.



- **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.

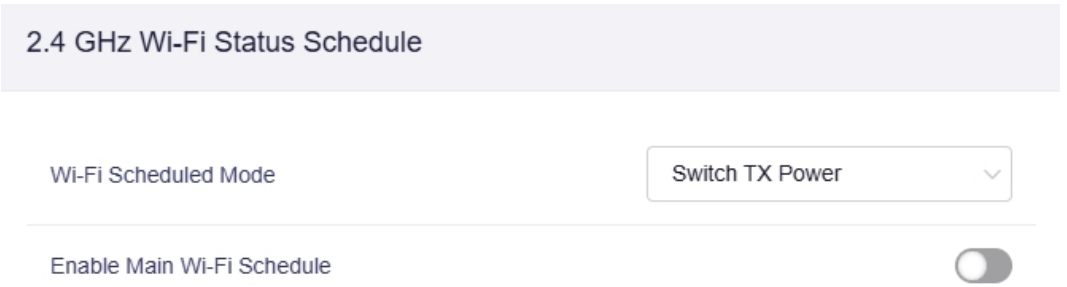


- **Programa de Wi-Fi para invitados**: cuando esté habilitado, configure los horarios de encendido y apagado para su Wi-Fi para invitados de 2,4 GHz y seleccione una fecha efectiva para el semana.

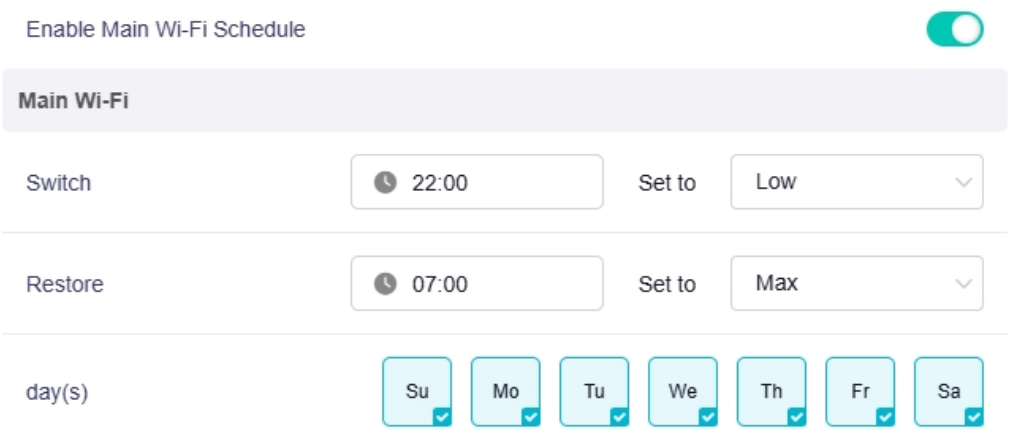


Modo 2: Cambiar alimentación de TX

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.

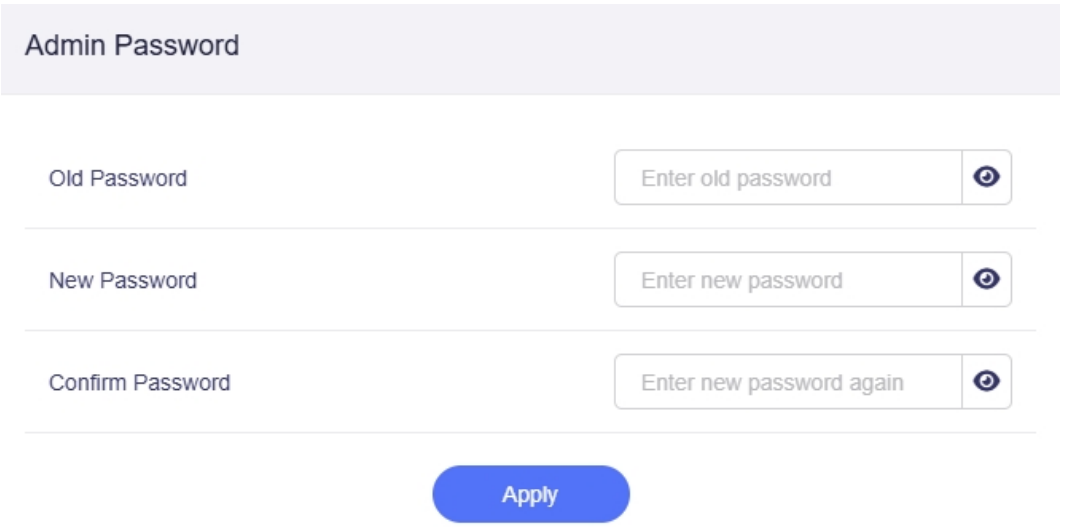


- **Cambiar**: Sajuste la potencia de TX a un cierto nivel (por ejemplo, bajo) enen un momento específico (p. ej., 22:00).

- **Restaurar**: Rrestaurar la energía de TX aotro nivel (p. ej., Max) aen otro momento (por ejemplo, 07:00).
- **días**: Seleccione los días efectivos de la semana para esta configuración.

14.5 Contraseña de administrador

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

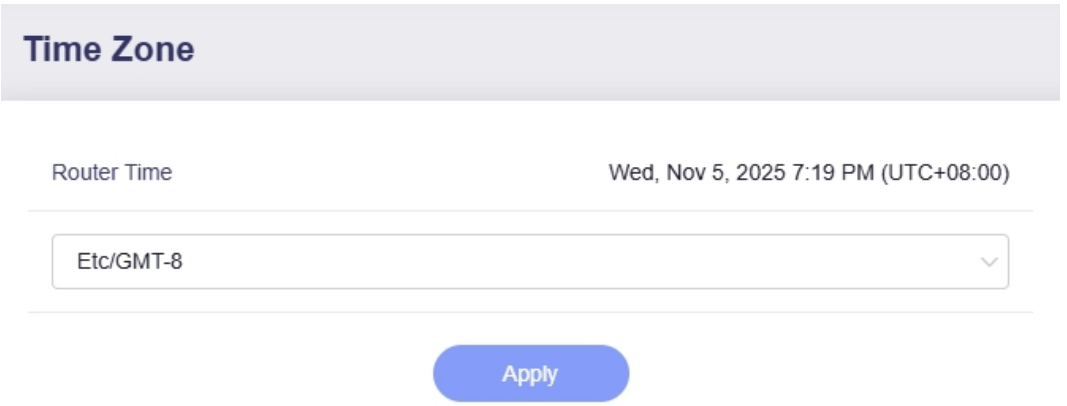


Los requisitos para la contraseña de administrador son los siguientes:

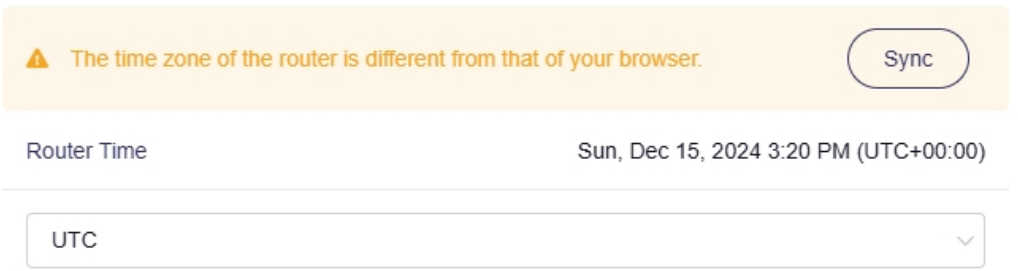
1. Mínimo 10 caracteres y máximo 63 caracteres en longitud.
2. Se permiten letras (distingue entre mayúsculas y minúsculas), números y símbolos (p. ej., ! @ # $ % ^ & * ( ) _ + - = , . > < | ? / \ [ ] { } : ; " ' ` ~).
3. Al menos dos tipos (letras mayúsculas, letras minúsculas, números y símbolos) están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

14.6 Zona horaria

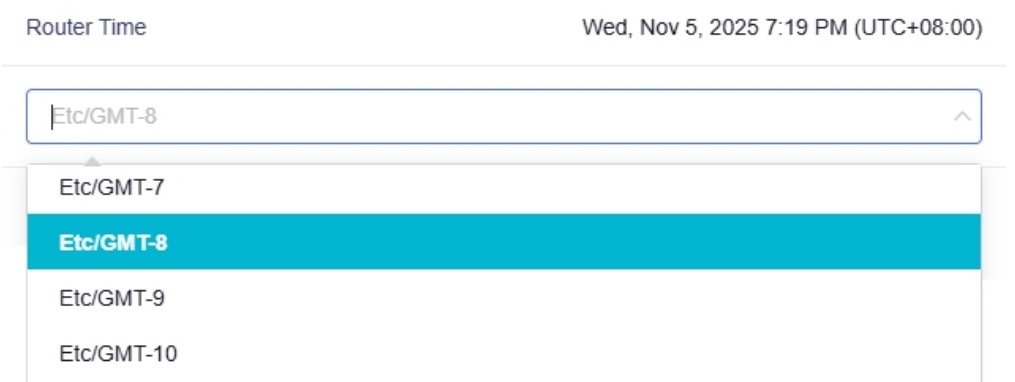
Inicie sesión en el panel de administración web de su enrutador y navegue hasta **SISTEMA** > **Zona horaria**. Esta página muestra la la hora del sistema, indicando la fecha, la hora y el desplazamiento de zona horaria correspondiente.



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 el botón **Sincronizar** para sincronizar la zona horaria.

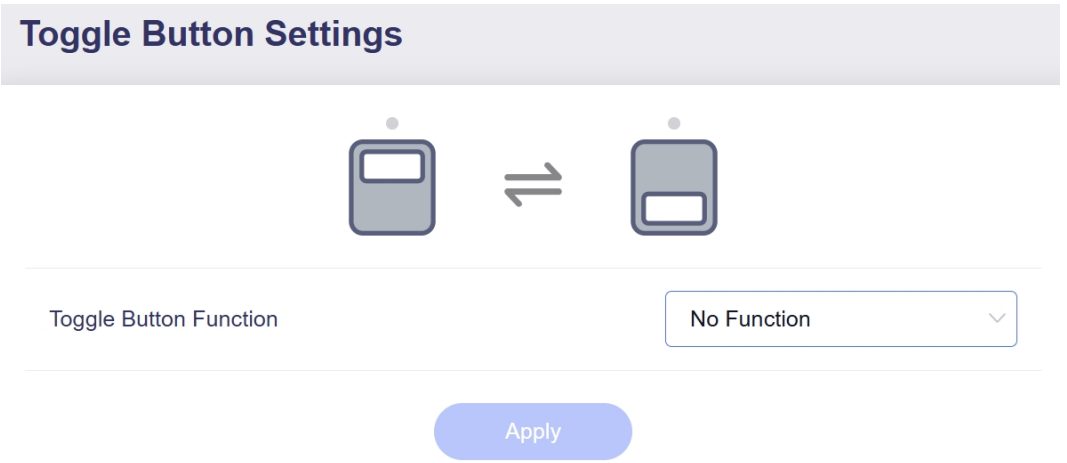


Para cambiar la zona horaria, sseleccione la zona horaria apropiada de la lista para garantizar que la hora del sistema coincida con su hora local.

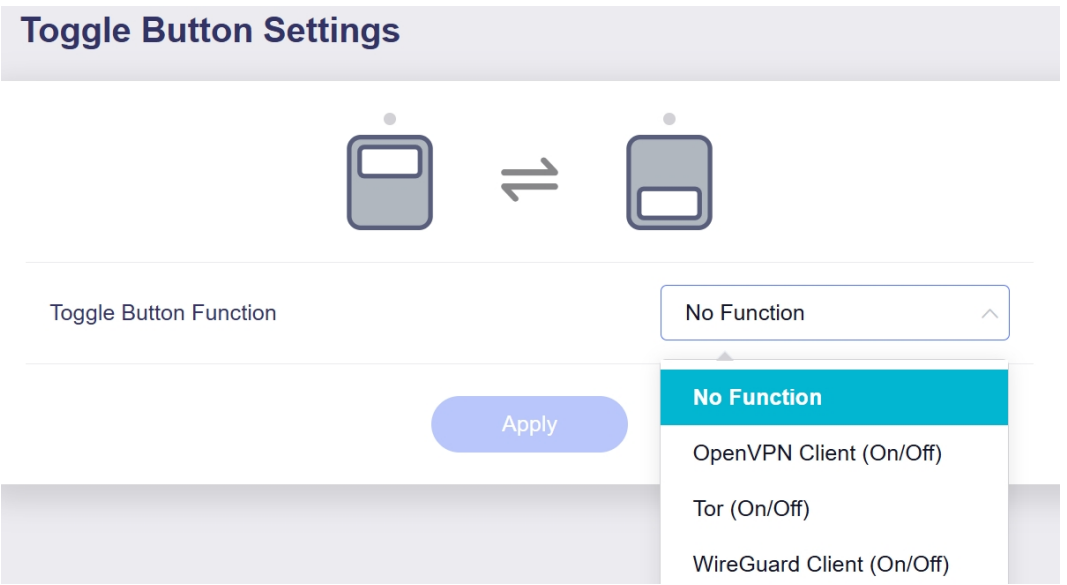


14.7 Configuración del botón de alternancia

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

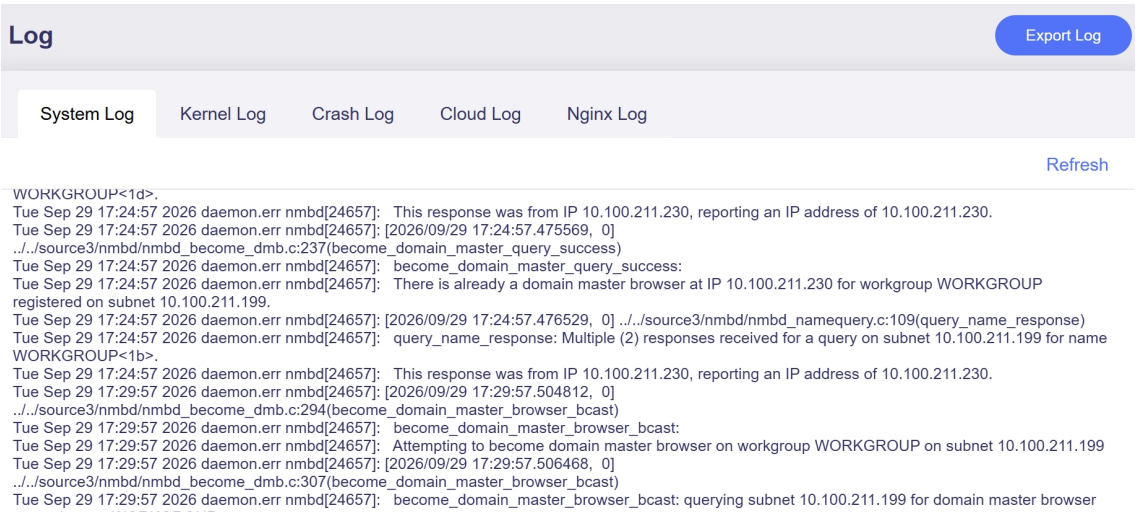


De forma predeterminada, al interruptor de palanca no se le asigna ninguna función. Puede personalizarlo si es necesario para activar o desactivar funciones específicas con un solo giro.



14.8 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.

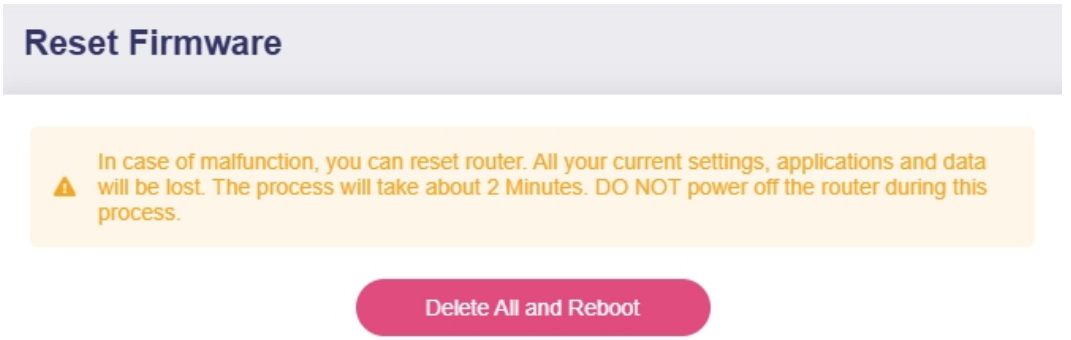


- **Actualizar**: Haga clic en este botón para actualizar logs.
- **Exportar registro**: Haga clic en este botón para exportar información de depuración junto con los registros.

14.9 Restablecer firmware

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

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



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

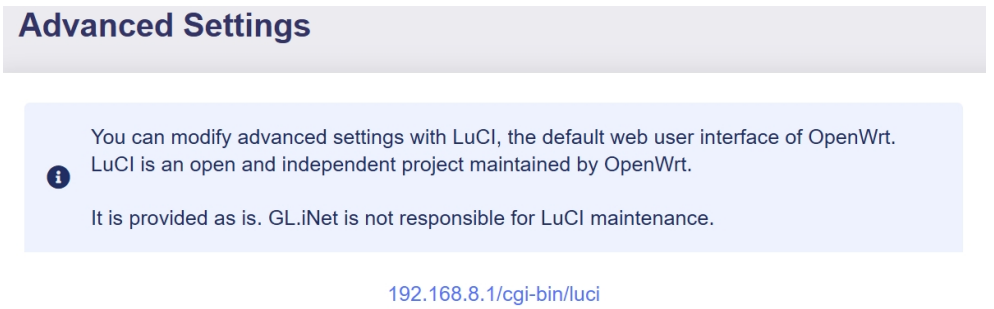
Si no puede acceder al panel de administración web del enrutador', intente restablecer su enrutador usando el botón de reinicio físico en el costado.

14.10 Configuración avanzada

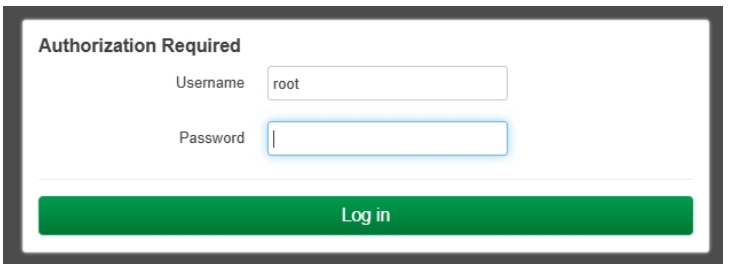
Inicie sesión en el panel de administración web de su enrutador y navegue hasta **SISTEMA** > **Configuración avanzada**. Esta página le permitemodificar la configuración avanzada a modificar configuración avanzada en LuCI, que es la interfaz de usuario web predeterminada de OpenWrt. Como proyecto abierto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

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

1. Haga clic en el enlace de acceso y será redirigido a la página de inicio de sesión de LuCI.



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



Ylo hará luego registrar en en la interfaz.

