GL·iNet



Manual de usuario

GL-AR300M16 / Shadow

Mini enrutador inalámbrico

Versión de firmware 4.3.27

Acerca de este manual

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

Con esta guía, podrá:

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

Convenciones de formato

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

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

Nota:

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

¿Necesita más ayuda o información?

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

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

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

Contenido

Capítulo 1 Conozca su enrutador 8

1.1 Descripción general del producto 9

1.1.1 Apariencia 9

1.1.2 Interfaz y botón 10

1.1.3 LED 11

1.2 Especificaciones 11

1.3 Contenido del paquete 12

Capítulo 2 Conexión de hardware 14

2.1 Elección de una ubicación 15

2.2 Conexión del enrutador 15

Capítulo 3 Iniciar sesión en el enrutador 17

Capítulo 4 Configurar la conexión a Internet 19

4.1 Conectarse a Internet mediante un cable Ethernet 21

4.1.1 Configuración básica 21

4.1.2 Protocolo 23

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

4.2.1 Configuración básica 26

4.2.2 Opciones de repetidor 29

4.3 Conectarse a Internet mediante conexión compartida por USB 30

4.3.1 Conexión compartida desde un iPhone 30

4.3.2 Conexión compartida desde Android 32

4.3.3 Solución de problemas 33

4.4 Conectarse a Internet mediante un módem USB 34

Capítulo 5 Red inalámbrica 36

Capítulo 6 Clientes 39

6.1 Detalles del dispositivo 41

6.2 Acción 43

6.3 Eliminar clientes 45

6.4 Ordenar 46

Capítulo 7 Conozca la VPN 47

7.1 Introducción 48

7.2 Escenarios de aplicación 49

Capítulo 8 Panel de VPN 51
8.1 Cliente VPN 52
8.1.1 Opciones del cliente 53
8.1.2 Modo de política 55
8.1.3 Opciones globales 56
8.2 Servidor VPN 59
8.2.1 Opciones del servidor 60
8.2.2 Regla de ruta del servidor 61
8.2.3 Opciones globales 62
Capítulo 9 Configurar el servidor VPN 63
9.1 Configurar el servidor OpenVPN 64
9.1.1 Preparación 64
9.1.2 Pasos de configuración 65
9.1.3 Solución de problemas 68
9.2 Configurar el servidor WireGuard 69
9.2.1 Preparación 69
9.2.2 Pasos de configuración 70
9.2.3 Solución de problemas 73
Capítulo 10 Configurar el cliente VPN 74
10.1 Configurar el cliente OpenVPN 75
10.1.1 Preparación 75
10.1.2 Configurar NordVPN 75
10.1.3 Configurar el cliente OpenVPN manualmente (para otros proveedores) 81
10.2 Configurar el cliente WireGuard 84
10.2.1 Preparación 84
10.2.2 Configurar AzireVPN 85
10.2.3 Configurar Mullvad 88
10.2.4 Configurar el cliente WireGuard manualmente (para otros proveedores) 92
Capítulo 11 Aplicaciones 96
11.1 Complementos 97
11.2 DNS dinámico 98
11.2.1 Habilitar DDNS 98
11.2.2 Comprobar si DDNS funciona 100
11.2.3 Acceso remoto HTTP 102

11.2.4 Acceso remoto HTTPS 104
11.2.5 Acceso remoto SSH 106
11.3 GoodCloud 107
11.3.1 Habilitar GoodCloud 108
11.3.2 Administrar el enrutador 112
11.3.3 Desvincular el dispositivo 117
Capítulo 12 Red 118
12.1 Cortafuegos 119
12.1.1 Reenvío de puertos 119
12.1.2 Abrir puertos en el enrutador 121
12.1.3 DMZ 122
12.2 Multi-WAN 123
12.2.1 Seguimiento del estado de la interfaz 123
12.2.2 Modo Multi-WAN 125
12.3 LAN 128
12.3.1 Red privada 128
12.3.2 Red de invitados 130
12.3.3 Reserva de direcciones 132
12.4 DNS 134
12.4.1 Configuración general 134
12.4.2 Configuración del servidor DNS 135
12.4.3 Editar hosts 137
12.5 Modo de red 139
12.6 IPv6 142
12.6.1 Modo IPv6 143
12.6.2 Método de obtención de DNS 143
12.7 Dirección MAC 144
12.8 Puerta de enlace directa 146
12.9 Inspección IGMP 148
Capítulo 13 Sistema 149
13.1 Descripción general 150
13.2 Actualización 151
13.2.1 Actualización en línea 151
13.2.2 Actualización local 152

13.3 Tareas programadas 154
13.3.1 Programación de los indicadores LED 154
13.3.2 Programar reinicio 155
13.3.3 Programación de Wi-Fi de 2,4 GHz 156
13.4 Contraseña de administrador 158
13.5 Zona horaria 159
13.6 Configuración del botón de alternancia 160
13.7 Registro 161
13.8 Restablecer firmware 162
13.9 Configuración avanzada 163

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

Shadow (GL-AR300M16) es un mini enrutador de bolsillo, diseñado para ser portátil y apto para viajes, que admite una velocidad de transmisión inalámbrica de hasta 300 Mbps. Shadow ofrece funciones de seguridad avanzadas, incluida la compatibilidad con OpenVPN, WireGuard® y un servidor DNS. No solo le permite convertir una red pública en una Wi-Fi privada para una navegación segura, sino que también le permite cargar archivos de configuración VPN de más de 30 proveedores de servicios VPN, configurarlo como cliente VPN, proporcionando una capa adicional de privacidad y seguridad para crear un tráfico cifrado entre su dispositivo y el servidor VPN.

1.1.1 Apariencia

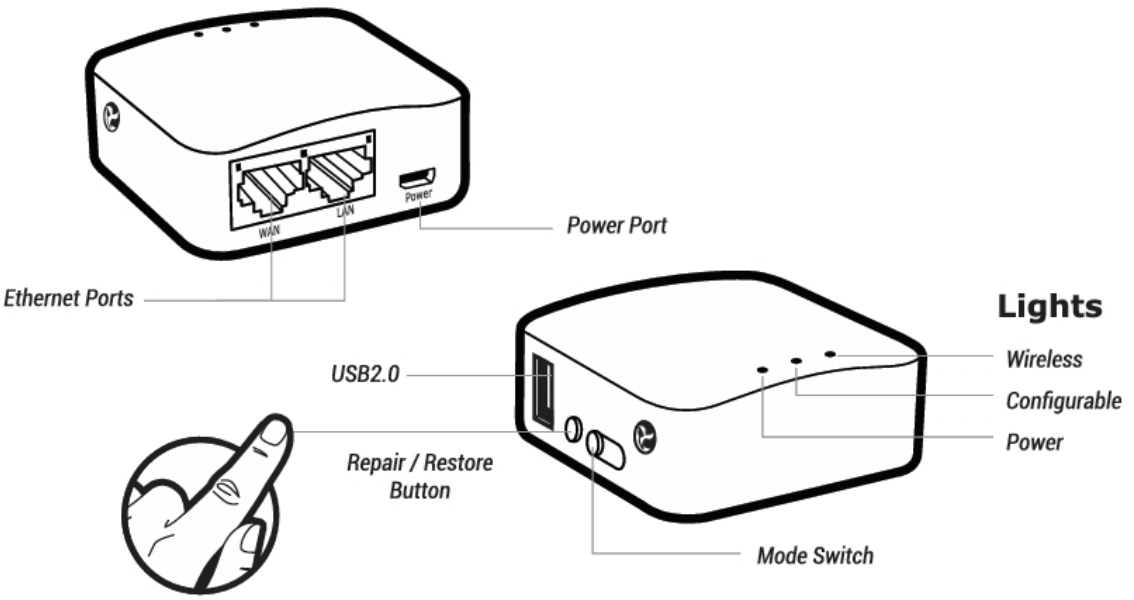








1.1.2 Interfaz y botón



Artículo	Descripción
Puerto de alimentación	Se conecta al adaptador de corriente.
Puerto Ethernet WAN	Se conecta a un módem o a una toma Ethernet para Internet.
Puerto Ethernet LAN	Se conecta a dispositivos cableados si es necesario.
USB 2.0	Para conectar unidades de almacenamiento USB, compartir la conexión a Internet de un teléfono por USB o utilizar módems USB móviles compatibles.
Cambio de modo	Interruptor físico que permite alternar los ajustes seleccionados del enrutador. Puede configurarlo en el panel de administración web para activar o desactivar funciones específicas con un solo movimiento.
Botón Reparar/Restaurar	Mantenga pulsado durante **4 segundos** para restablecer la conexión de red. Mantenga pulsado durante **10 segundos** y suéltelo para restablecer el enrutador a los valores de fábrica.

1.1.3 LED

Indicador LED	Indicación
LED de encendido	Encendido: Encendido Apagado: Apagado
LED central (configurable)	Encendido: el indicador LED está personalizado. Apagado: el indicador LED no está personalizado (modo predeterminado).
LED inalámbrico	Encendido: Wi-Fi 2.4G está conectado Apagado: Wi-Fi 2.4G está desconectado

1.2 Especificaciones

Interfaz	1 x puerto Ethernet WAN 1 x puerto LAN Ethernet 3 x LED 1 x puerto USB 2.0 1 x puerto de alimentación Micro USB 1 x botón Restablecer 1 x botón de alternancia
CPU	QCA9531, SoC de @650MHz
Memoria/Almacenamiento	DDR2 128MB / NOR Flash 16MB
Protocolo	IEEE 802.11/b/g/n
Velocidad de Wi-Fi	300Mbps (2,4GHz)
Velocidad de Ethernet	10/100Mbps
Entrada de energía	Micro USB, 5V/2A
LED	Alimentación/Wi-Fi
Consumo de energía	< 2W
Temperatura de funcionamiento	0 ~ 40°C (32 ~ 104°F)
Temperatura de almacenamiento	-20 ~ 70°C (-4 ~ 158°F)

Dimensión/Peso	58 x 58 x 25 mm / 40 g
Otras herramientas	Hoja de datos / Firmware / Aplicación

*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 Contenido del paquete

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

El paquete incluye:

- 1 x Shadow (GL-AR300M16)
- 1 manual de usuario
- 1 x Tarjeta de agradecimiento
- 1 cable Ethernet
- 1 cable USB



1 x User manual


1 x Shadow (GL-AR300M16)



1 x Thank you card


1 x Ethernet cable


1 x USB cable

(GL-AR300M16-Ext)



1 x User manual



1 x Shadow (GL-AR300M16)



1 x Thank you card



1 x Ethernet cable



1 x USB cable

(GL-AR300M16)

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 frescoing**: coloque el enrutador en un área fresca y bien- ventilada para obtener el calor adecuado. disipación.
- **Ubicación central**: coloque el enrutador en un lugar donde pueda conectarse fácilmente a la alimentación y a varios dispositivos (por ejemplo, la zona).
- **Cable de la sala de estar comodidad**: coloque los cables y el cable de alimentación de forma segura para evitar tropiezos.
- **Superficie estable**: coloque el enrutador en una superficie horizontal y plana (estante, escritorio) para estabilidad.
- **Evitación de EMI**: mantenga el enrutador alejado de fuentes de interferencia electromagnética (dispositivos Bluetooth, microondas) para minimizar la interferencia de la señal.

2.2 Conexión del enrutador

1. **Encendido**
   Junte el adaptador de corriente de dos piezas. Conéctelo al enrutador y conéctelo a una toma de corriente.
2. **Conectar 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’s etiqueta.
   - **Ethernet**: Conecte su. dispositivo al puerto LAN del enrutador’a través de un cable Ethernet.
3. **Inicie sesión en el enrutador**

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

Capítulo 3

Iniciar sesión en el enrutador

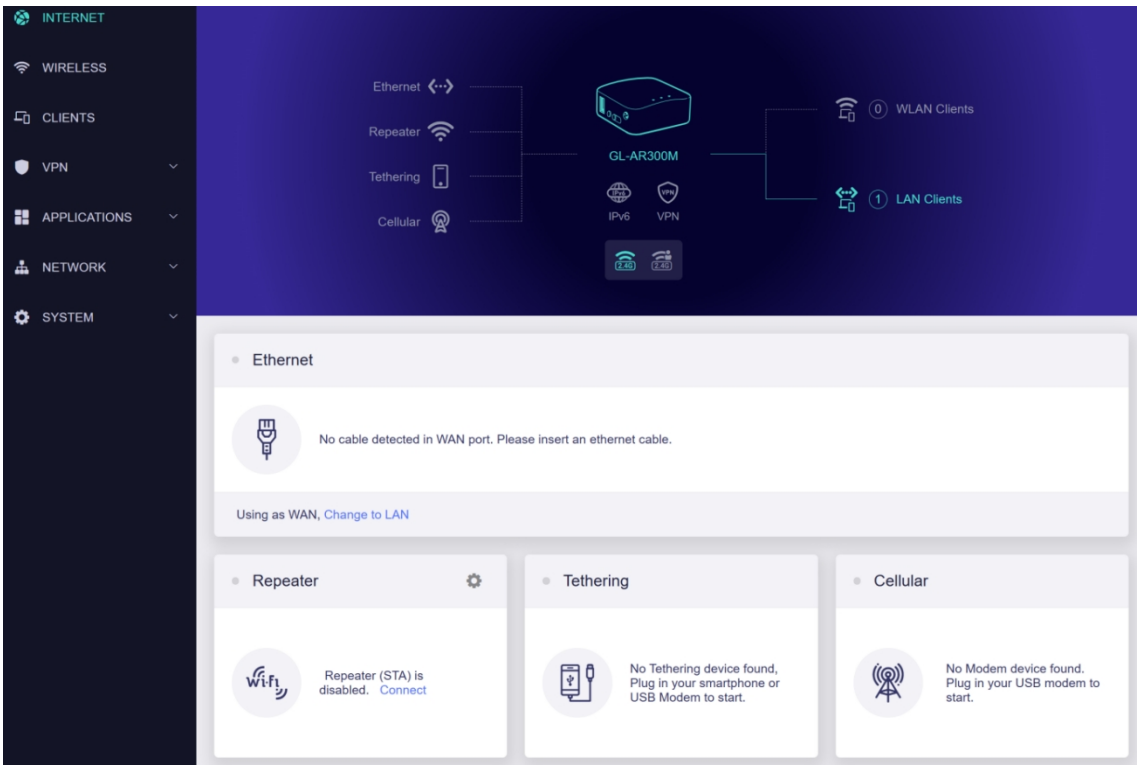
Este capítulo lo guía para iniciar sesión en su enrutador a través del panel de administración web

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

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

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

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



Capítulo 4

Configurar la conexión a Internet

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

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

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

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

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

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

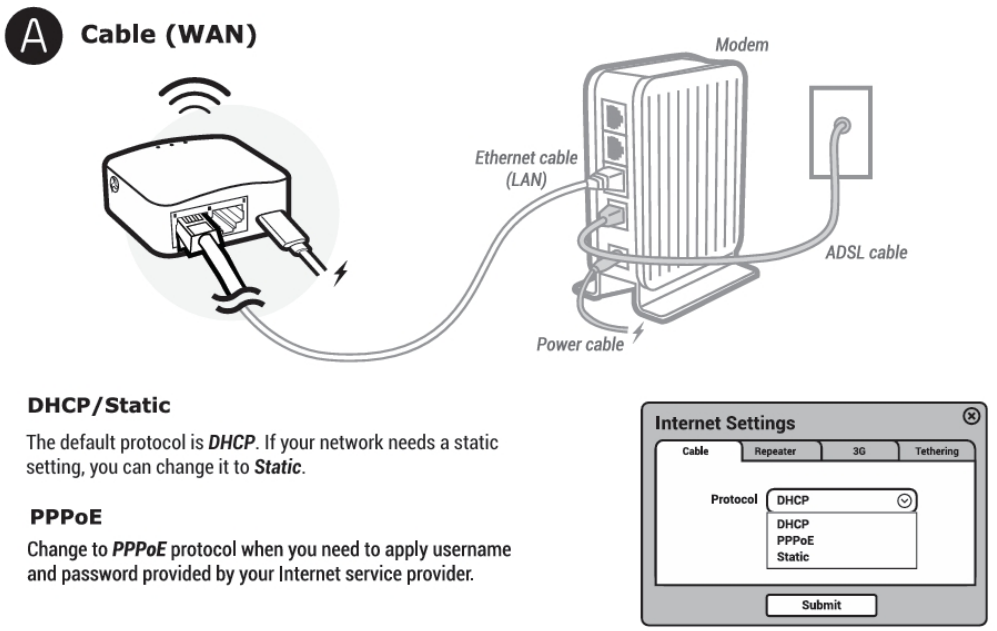
4.1 Conectarse a Internet mediante un cable Ethernet

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

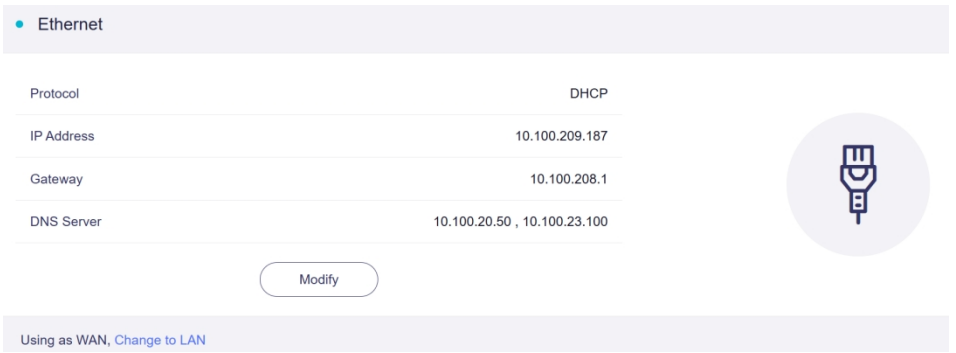
4.1.1 Configuración básica

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

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

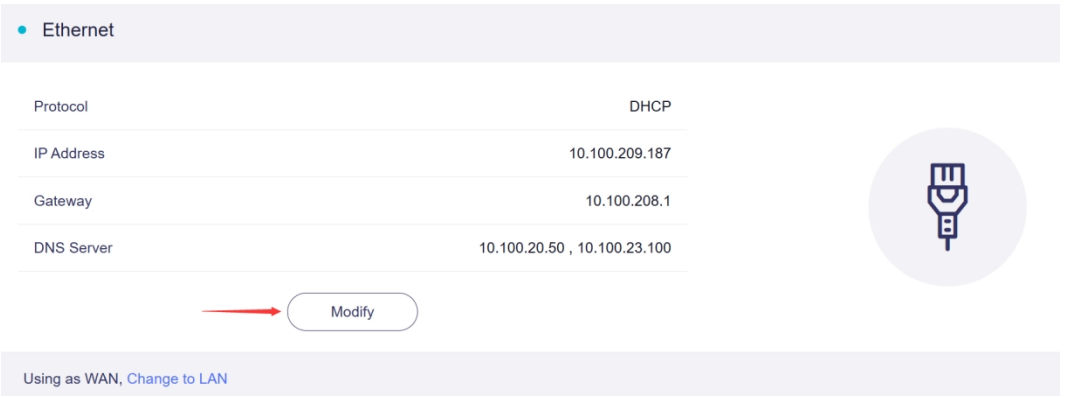


2. Inicie sesión en el el enrutador'panel de administración web y navegue a **INTERNET** > **Ethernet**. Si la conexión se realiza correctamente, la sección Ethernet mostrará red detalles, incluidos protocolo, dirección IP, puerta de enlace, y DNS Servidor.


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

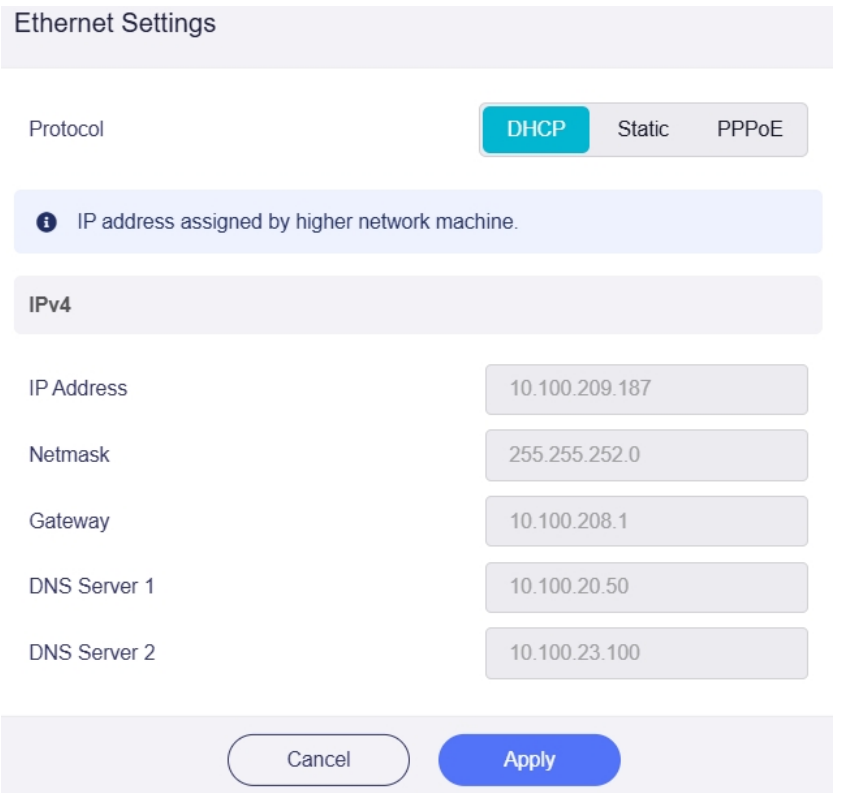
4.1.2 Protocolo

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



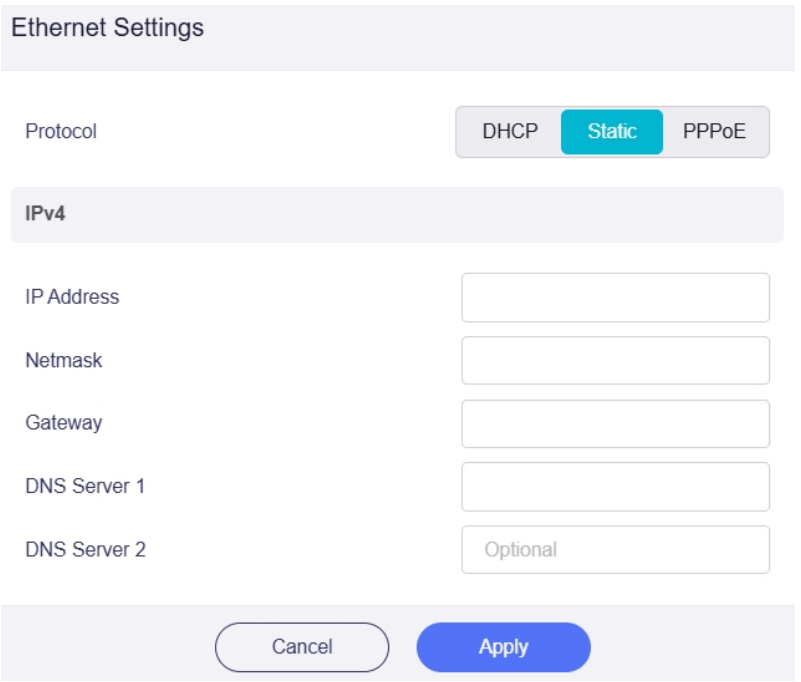
- **DHCP**

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



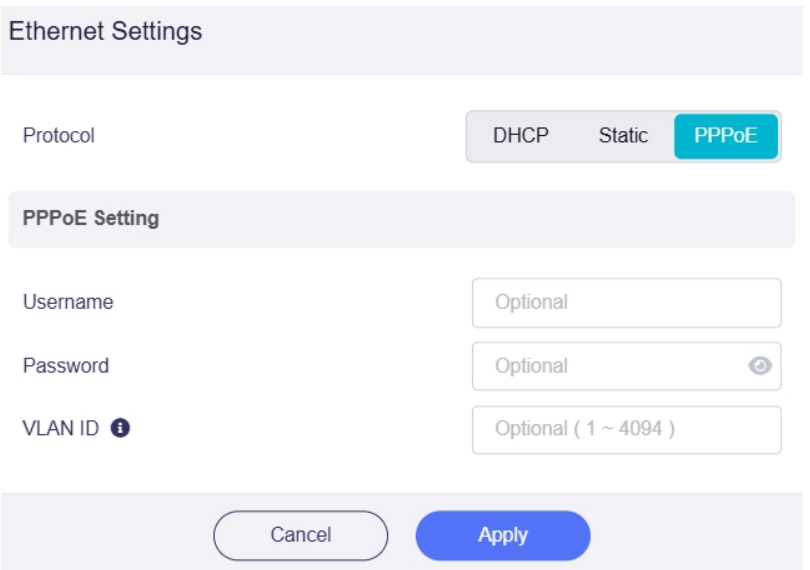
- **Estática**

  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, subred). máscara).



- **PPPoE**

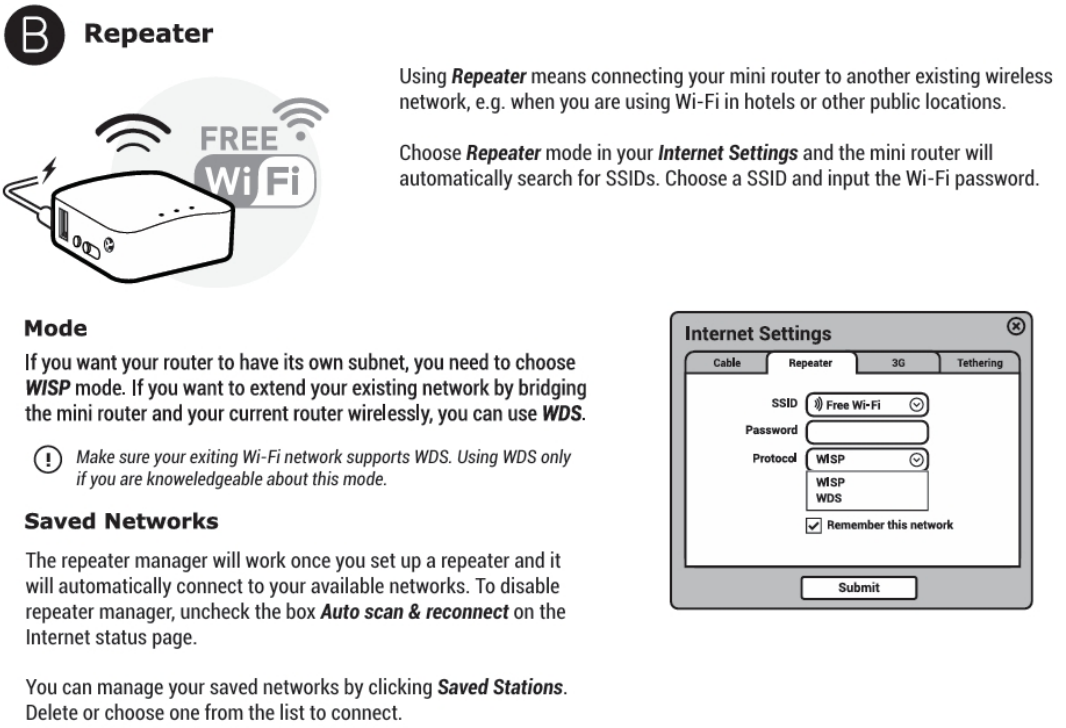
  PPPoE (Protocolo punto a punto sobre Ethernet) es un protocolo de red ampliamente utilizado por los ISP. Por lo general, proporcionarán un módem junto con un nombre de usuario y una contraseña únicos, que son necesarios para configurar una conexión a Internet.



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

4.2 Conectarse a Internet mediante una red Wi-Fi existente

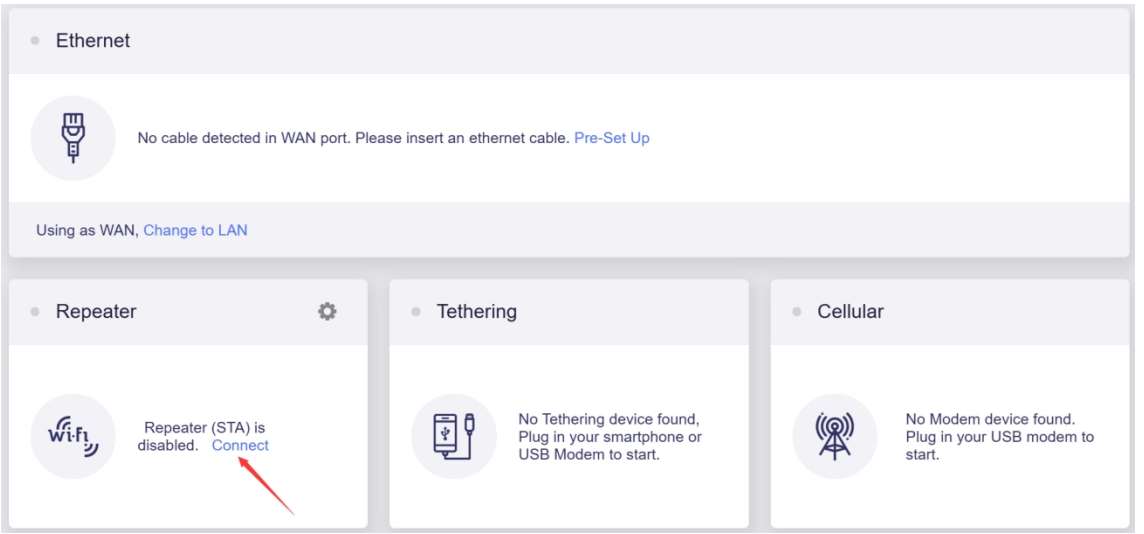
Conecte el enrutador como repetidor a la red inalámbrica existente para aumentar las señales Wi-Fi-Fi y crear una red local aislada de la red principal. Cuando en hoteles o cafeterías con puntos de acceso públicos gratuitos, el uso de un repetidor no solo fortaleces Wi-Fi, sino que también proporcionas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



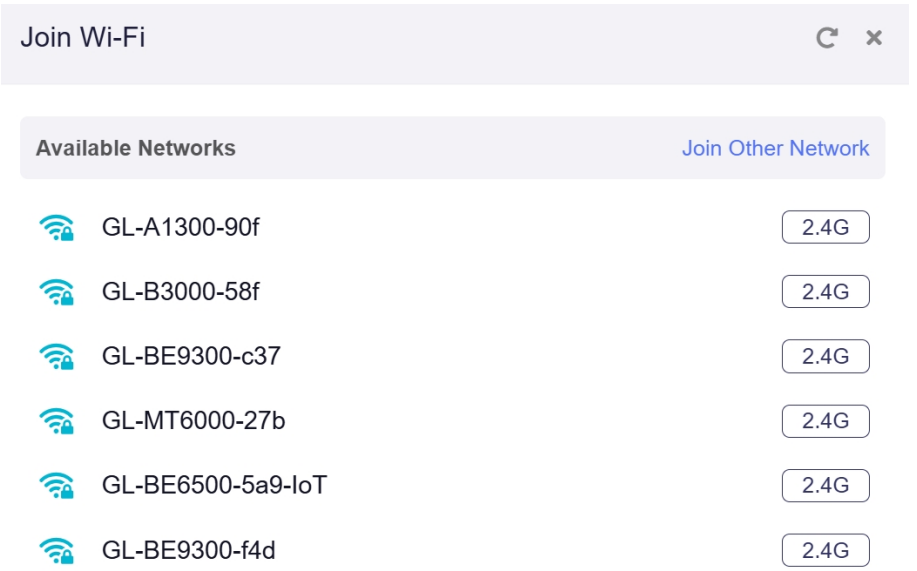
Repetidor GL.iNet Esta característica funciona en modo WISP (Proveedor de servicios de Internet inalámbrico) de forma predeterminada, lo que significa que el enrutador creará su propia subred y actuará como un firewall para protegerlo de la red pública.

4.2.1 Configuración básica

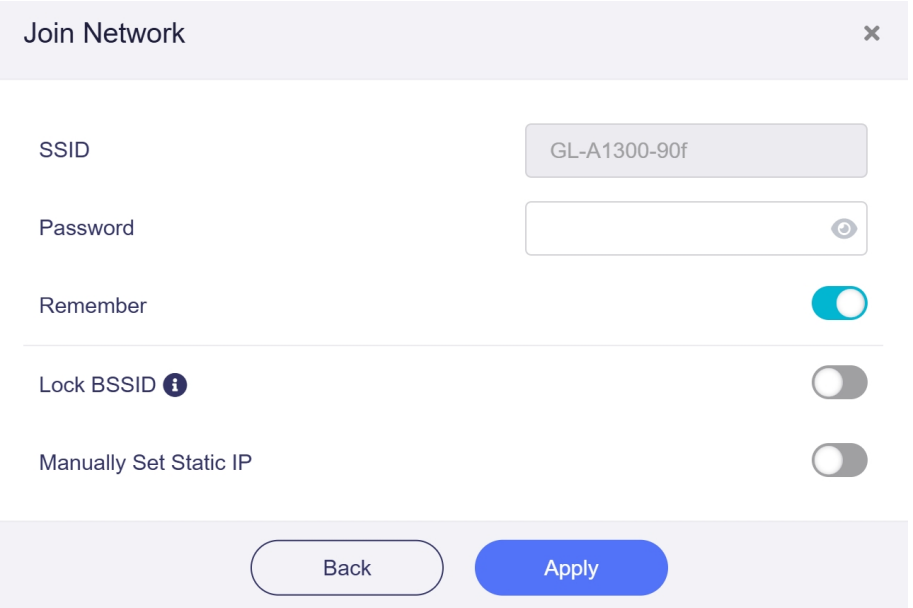
1. Registro acceda al del enrutador’panel de administración web y navegue a **INTERNET** > **Repetidor**. Haga clic en **Conectar**.



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

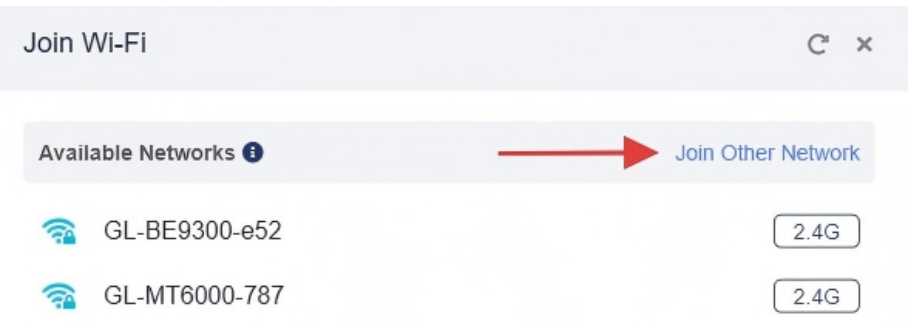


3. Eingrese la contraseña de Wi-Fi correcta y haga clic en **Aplicar**.

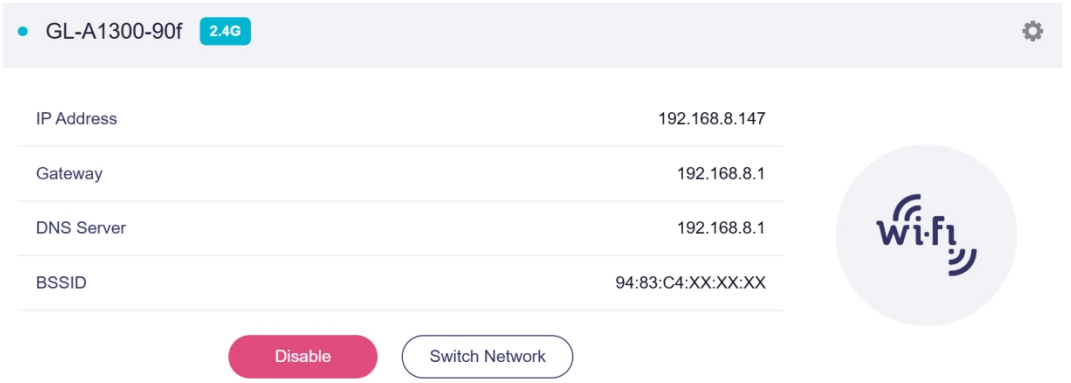


- **Recordar**: habilite esta opción para recordar la red Wi-Fi actual repetida.
- **Bloquear BSSID**: Cuando está habilitado, el enrutador se conectará solo al punto de acceso (AP) específico correspondiente al BSSID seleccionado, incluso cuando otros AP compartan el mismo SSID.
- **Manualmente Set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

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

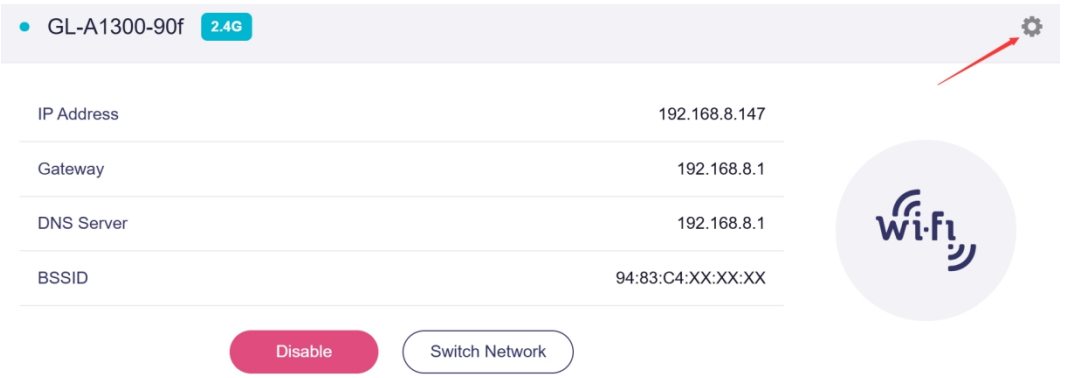


5. Espere un minuto hasta que el enrutador se conecte. Una vez conectado, la página se muestra a continuación.

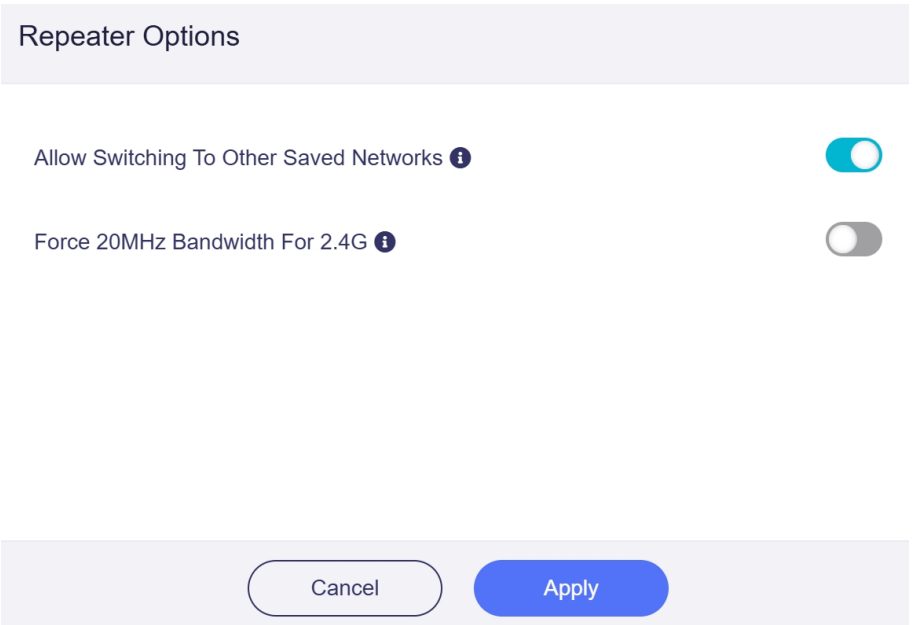

GL-A1300-90f
2.4G
IP Address
192.168.8.147
Gateway
192.168.8.1
DNS Server
192.168.8.1
BSSID
94:83:C4:XX:XX:XX
Disable
Switch Network

4.2.2 Opciones de repetidor

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



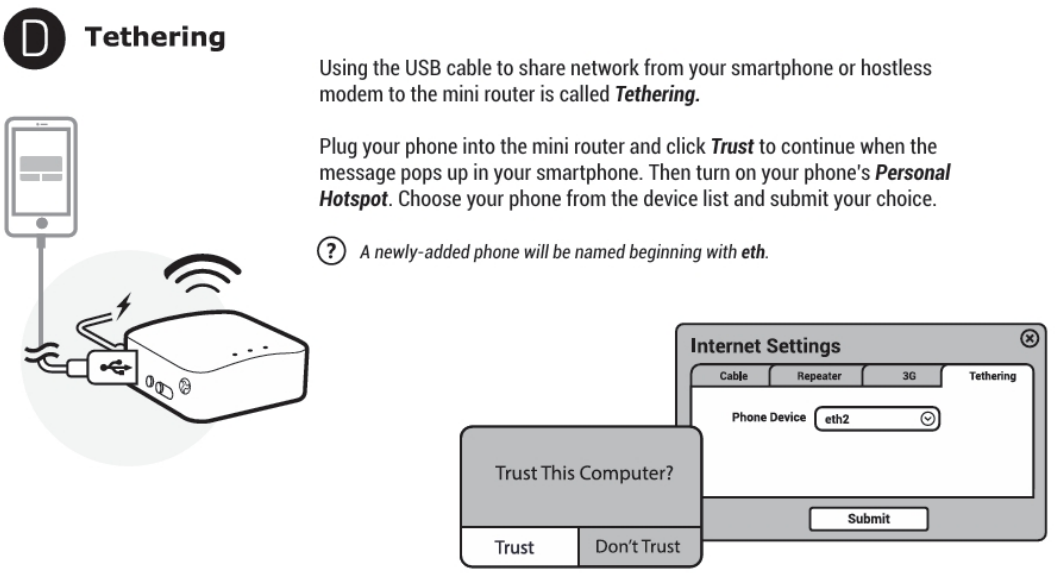
La página puede variar debido a las diferentes versiones de firmware.



- **Permitir cambiar a otras redes guardadas**: si la opción está habilitada, el enrutador se conectará automáticamente a otras redes guardadas cuando no pueda conectarse a la red Wi-Fi actual.
- **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.

4.3 Conectarse a Internet mediante conexión compartida por USB

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

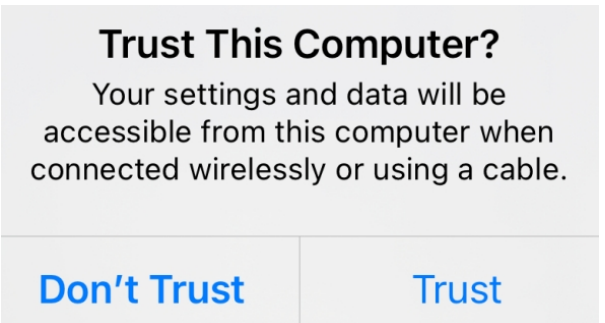


Sin host El módem también funciona en anclaje a red durante la configuración del módem.

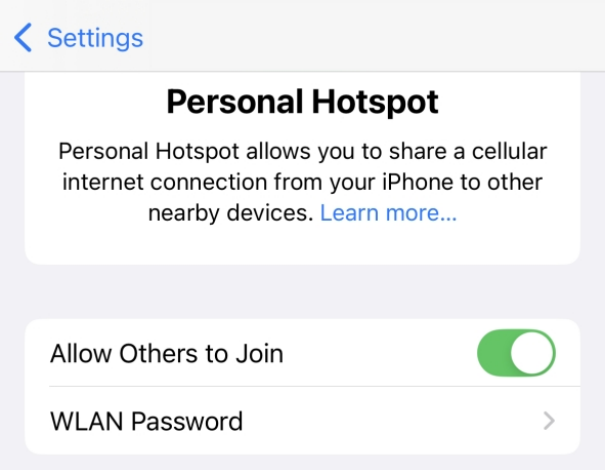
Nota: Algunos operadores de telefonía móvil limitan o cobran más por el anclaje a red. Recomendamos consultar con su operador.

4.3.1 Conexión compartida desde un iPhone

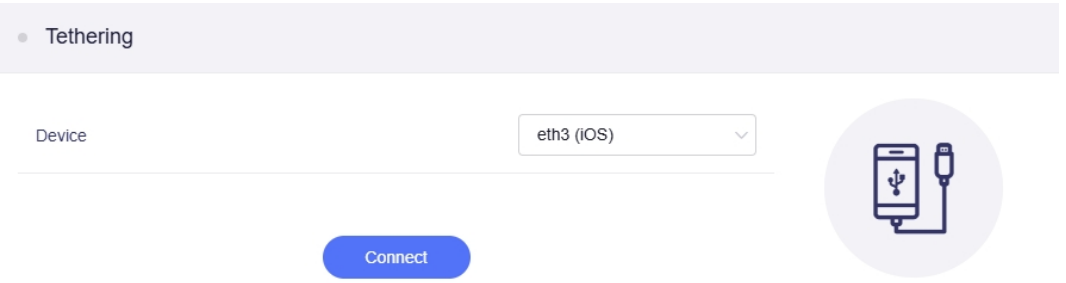
1. Conecte un iPhone al puerto USB del enrutador mediante un cable USB. Aparecerá un cuadro de diálogo del sistema preguntando si se debe confiar en el dispositivo. Toque **Confiar** para continuar.



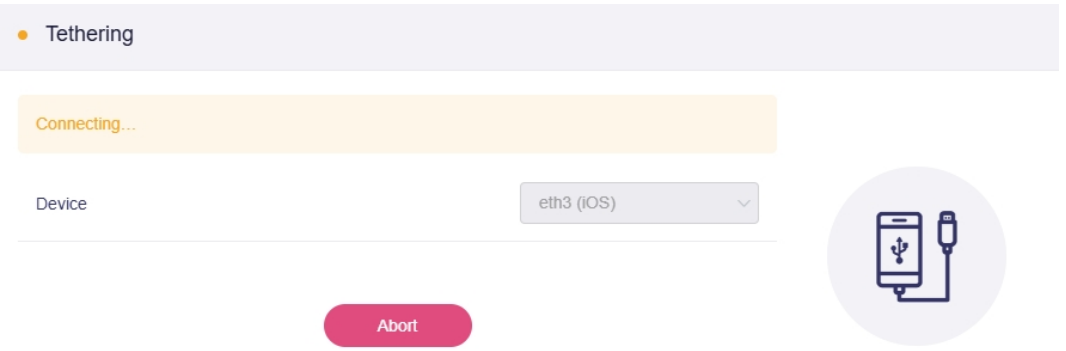
2. Ir a iPhone **Configuración** > **Punto de acceso personal**. Habilitar **Permitir que otros Unirse**.



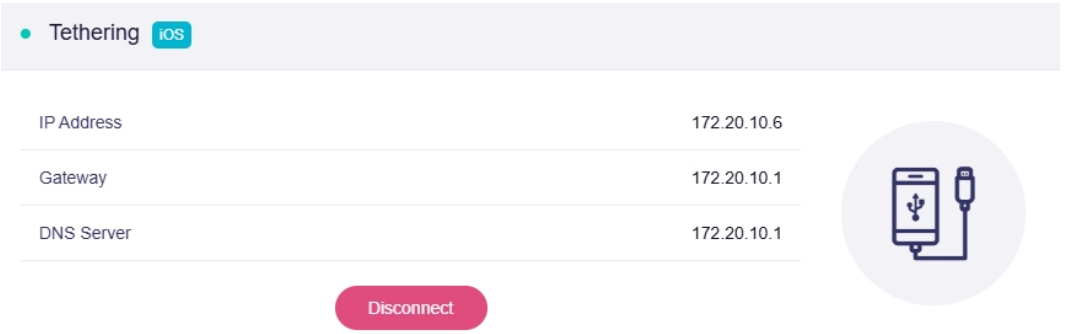
3. Conecte una computadora u otro teléfono al enrutador. Inicie sesión en el panel de administración web del enrutador y navegue hasta **INTERNET** > **Conexión**, luego haga clic en **Conectar**.



4. Comenzará a conectarse.

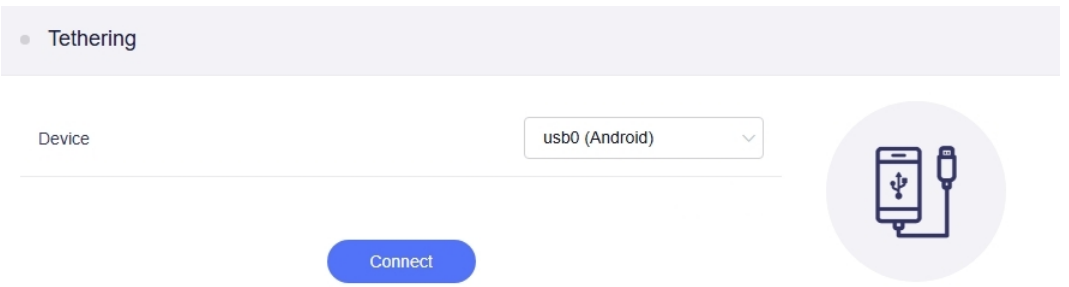


Una vez conectado, thesta página mostrará la conexión Tethering detalles.

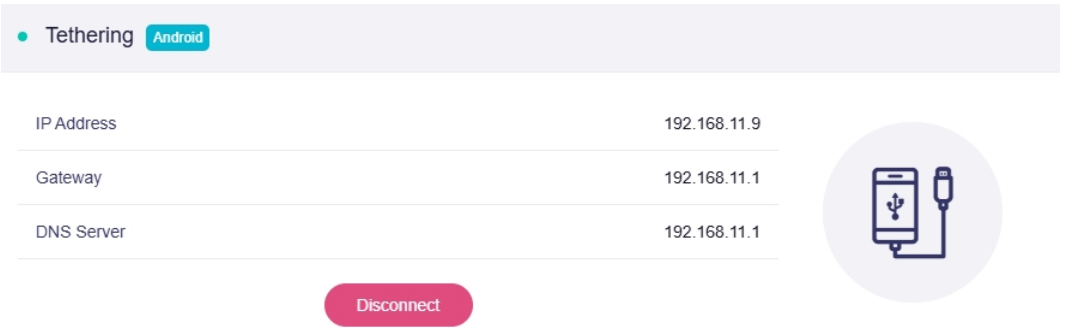


4.3.2 Conexión compartida desde Android

1. Conecte un teléfono Android al puerto USB del enrutador mediante un cable USB. Puede aparecer un cuadro de diálogo del sistema preguntando USB preferencias. Selecciona **Anclaje a red USB** o **Archivo Transferir** si se te solicita.
2. Vaya a la **Configuración** > **Red e Internet** > **Punto de acceso personal**. 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 fabricante soporte 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** > **Anclaje**. Click **Conectar**.



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



4.3.3 Solución de problemas

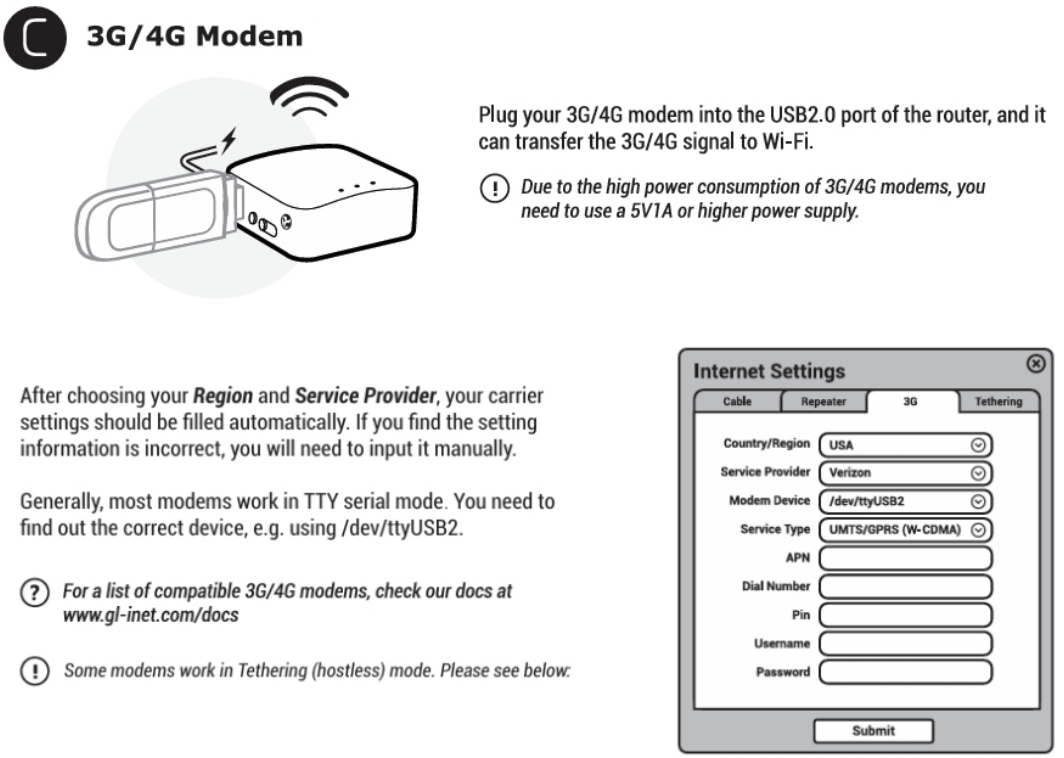
Si falla la conexión , intente estos pasos para solucionar el problema:

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

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

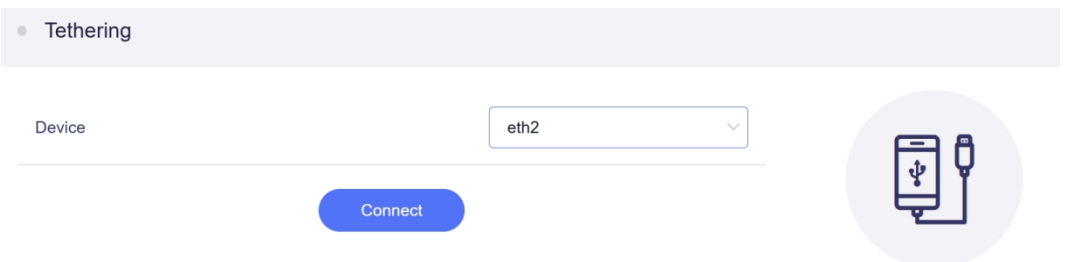
4.4 Conectarse a Internet mediante un módem USB

Conecte el enrutador a Internet insertando un módem USB con capacidad celular en su puerto USB. Esto permite que el enrutador se conecte a Internet a través de redes 3G/4G, brindando conectividad sin depender de la banda ancha de línea fija. Es adecuado para uso en vehículos o actividades al aire libre. Tenga en cuenta que esta conexión se implementa a través de la interfaz Tethering o Cellular del enrutador. 'Interfaz de anclaje a red o celular.

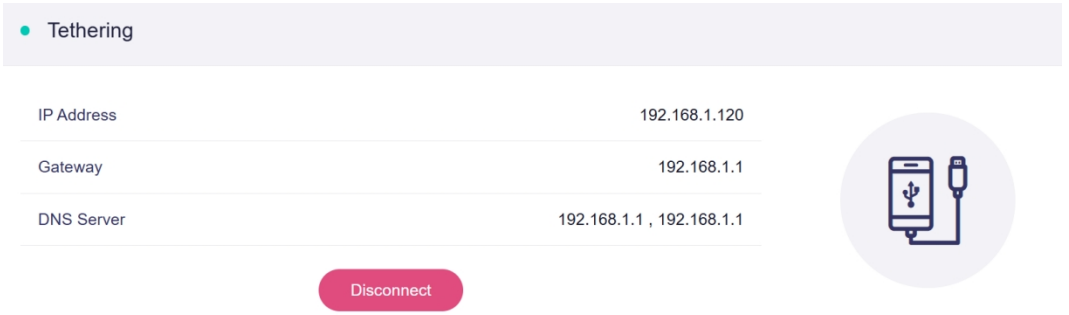


Siga los pasos siguientes para conectar su enrutador a Internet a través de un módem USB.

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



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



Consejo: Después de la configuración inicial, si reinicia el enrutador con el módem USB aún conectado, o re-inserte el módem en el enrutador, el USB módem será reconocido automáticamente , y una conexión de red establecerá sin volver a hacer clic en "Conectar".

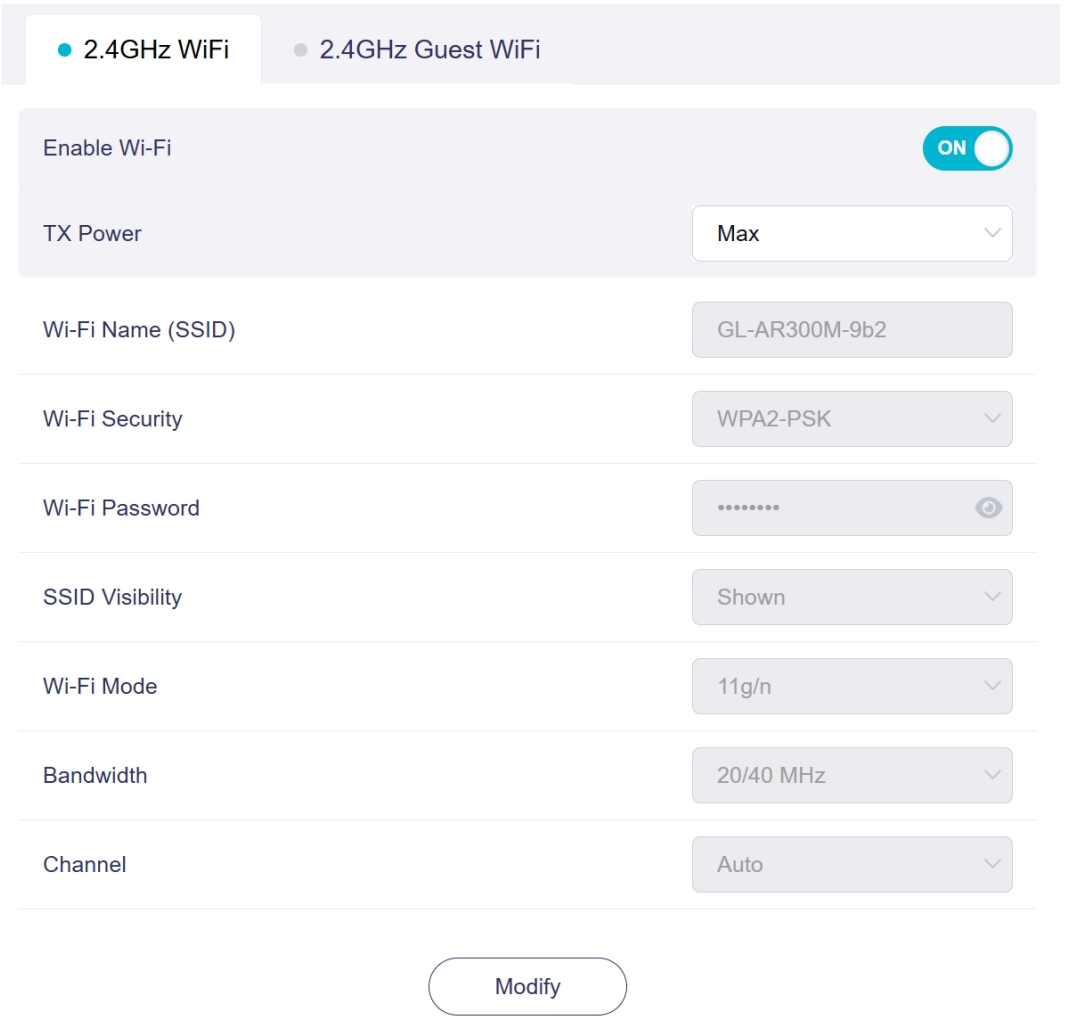
Capítulo 5

Red inalámbrica

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

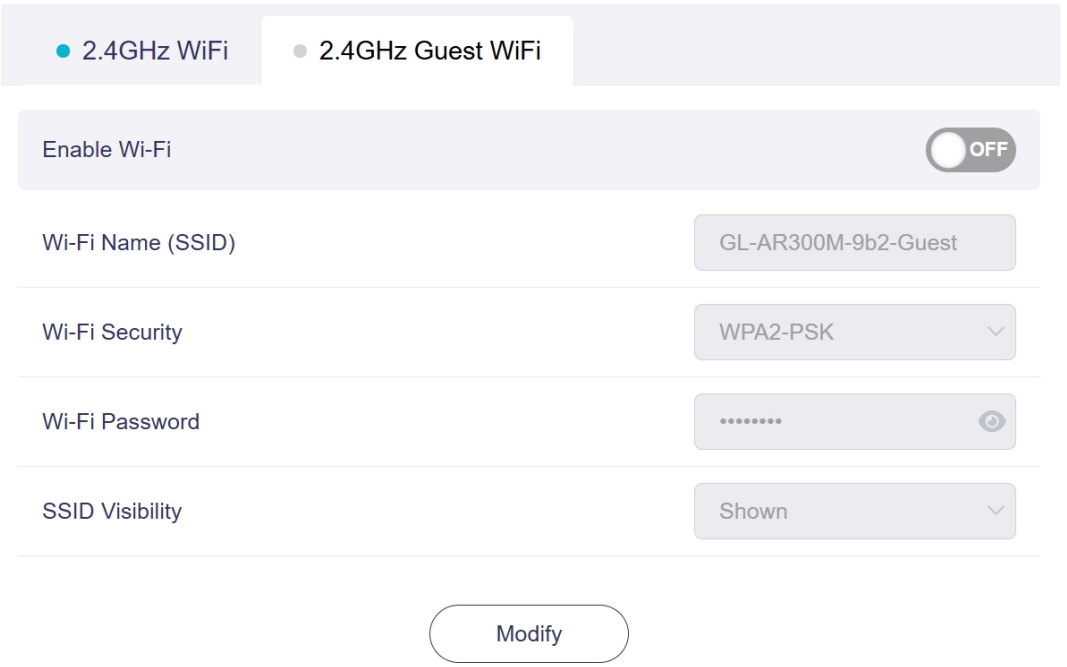
Inicie sesión en el panel de administración web del enrutador y navegue hasta **Inalámbrica**. La página inalámbrica muestra el enrutador’s Configuraciones de 2,4 GHz, con cada dividida en redes Wi-Fi principal-Fi y Wi-Fi para invitados-Fi para una administración flexible .

El 2.4 Wi-Fi principal de GHz le permite configurar múltiples ajustes, incluidos a 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.



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

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



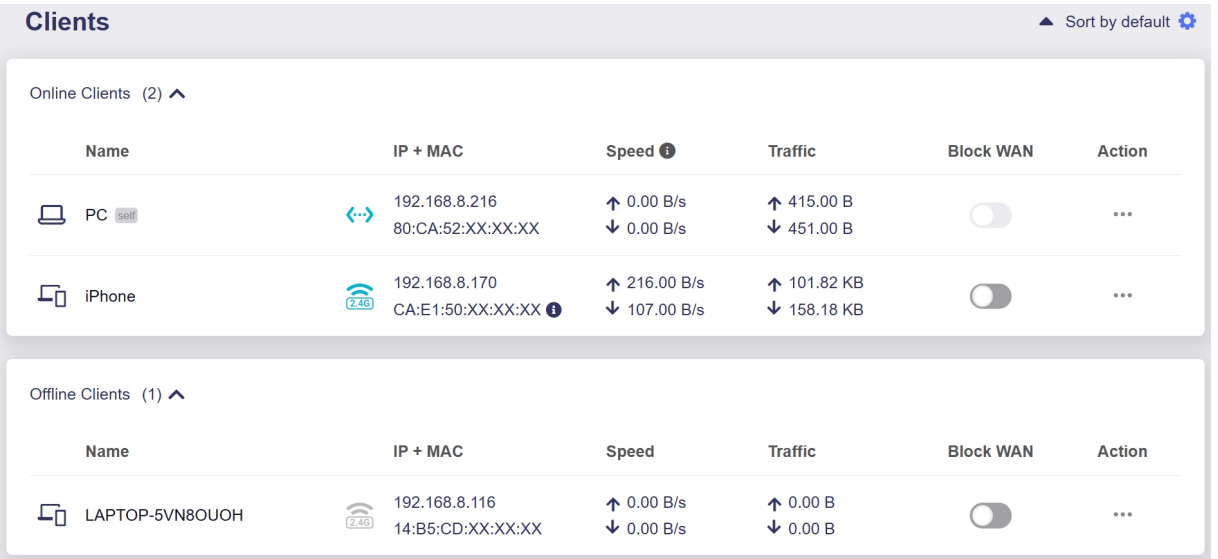
Capítulo 6

Clientes

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

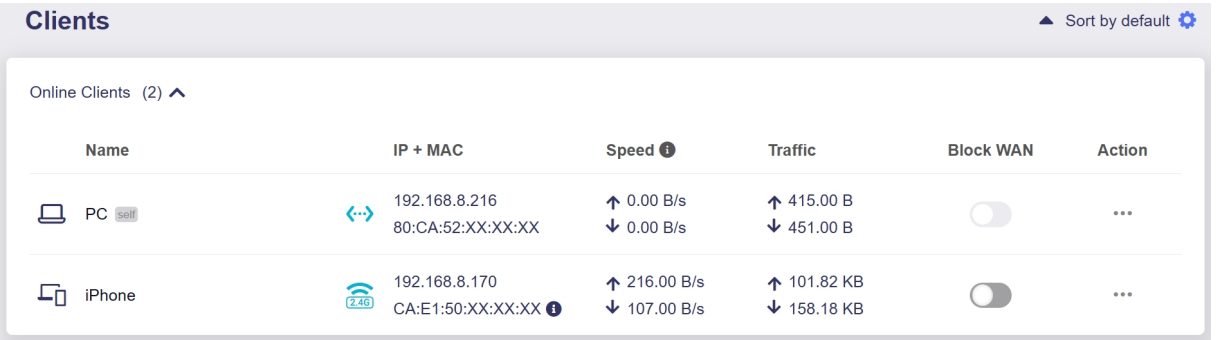
Inicie sesión en el enrutador’s web admin panel y navegue hasta **CLIENTES**.

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



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

6.1 Detalles del dispositivo



1. **Nombre del dispositivo**

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

2. **Dirección IP y MAC**

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



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

3. **Velocidad**

   La tercera columna muestra la velocidad de Internet de el dispositivo conectado. Estaes 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**: El la cuarta columna muestra el tráfico de Internet del dispositivo conectado.

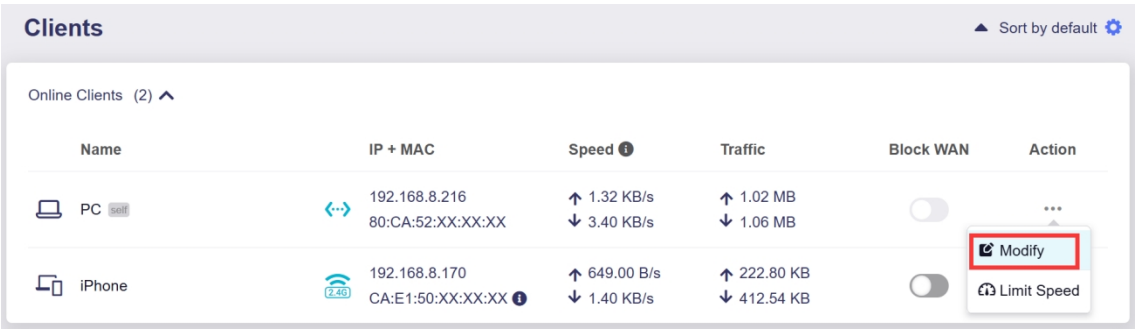
5. **Lista de bloqueo**

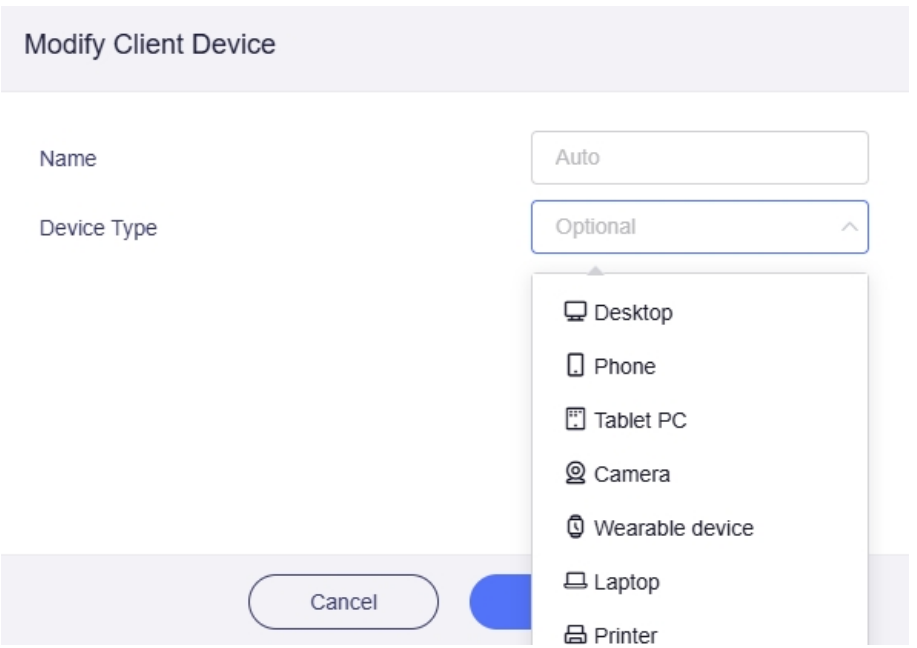
En la quintaésima columna, puede bloquear dispositivos conectados específicos con un clic. Si está habilitado, los dispositivos con direcciones MAC en la lista negrano están permitidos. para conectarse a este enrutador. Tenga en cuenta que el bloqueo del cliente se basa en la dirección MAC del dispositivo. Si el dispositivo bloqueado usa una dirección MAC diferente la próxima vez, aún podrá conectarse al enrutador.

6.2 Acción

1. **Modificar**

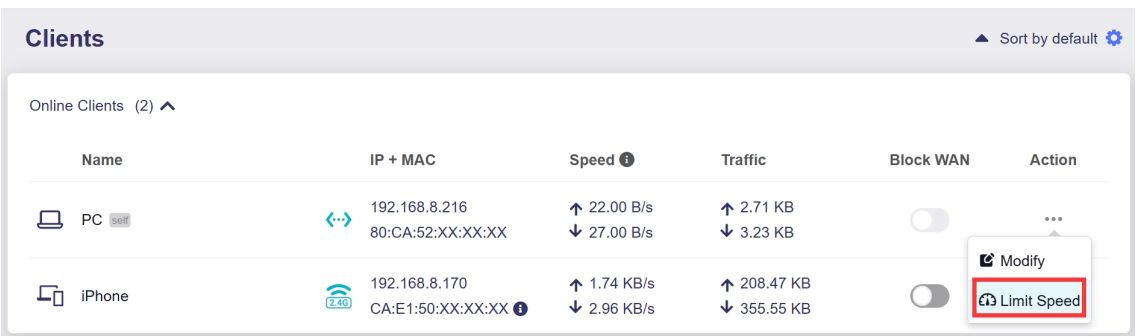
   Haga clic en el ícono de tres puntos en el **Acción** y haga clic en **Modificar** desde el menú desplegable menú para modificar el nombre y tipo del dispositivo.



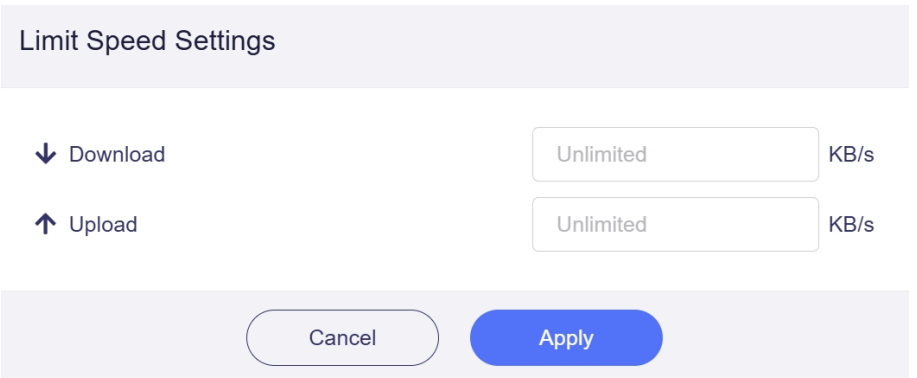


2. **Limitar velocidad**

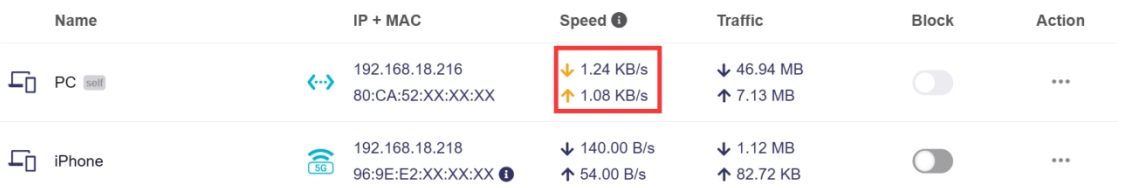
   Haga clic en el icono de tres puntos en la **Acción** columna y haga clic en **Limitar velocidad** en el menú desplegable.



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

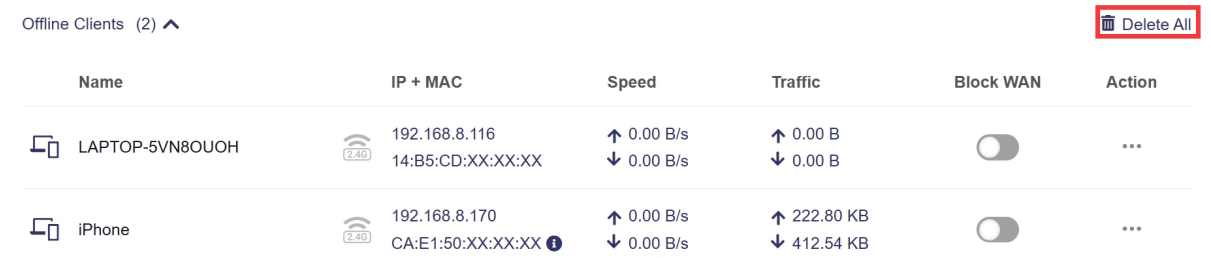


Si se ha aplicado una limitación de velocidad a un dispositivo, las flechas de velocidad de carga/descarga girarán amarillo.

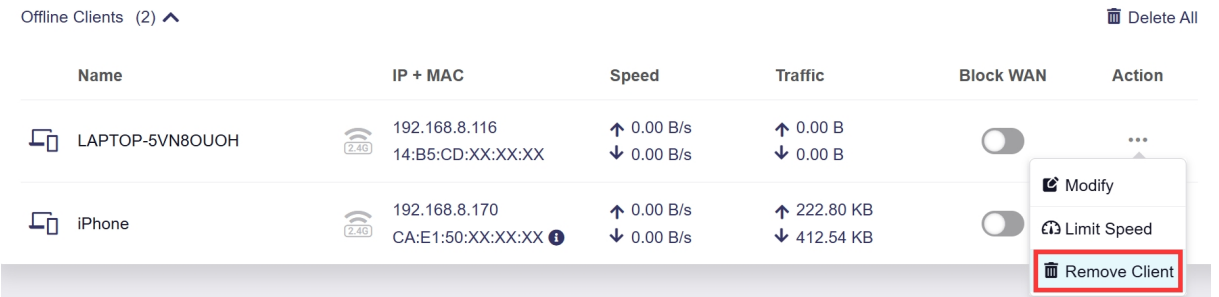


6.3 Eliminar clientes

En **Osin conexión Cclientes**, puede hacer clic en **Eliminar todo** en en la parte superior derecha esquina para eliminar todos los clientes fuera de línea.

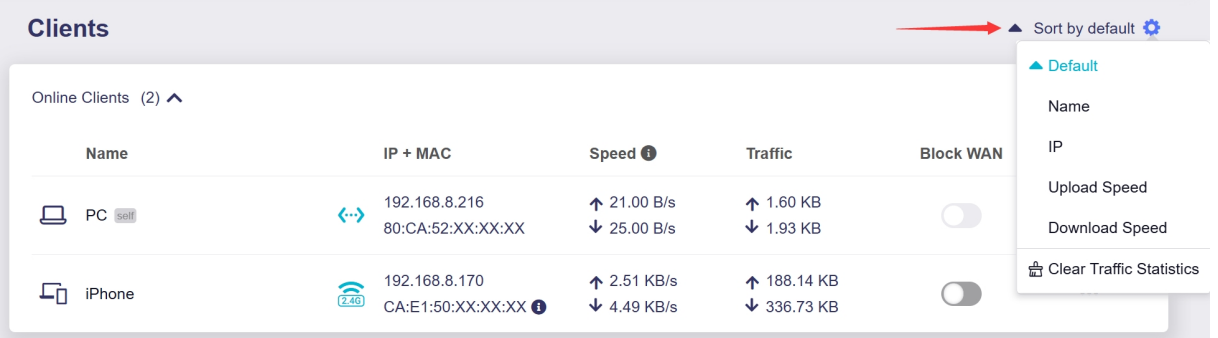


Si desea eliminar un cliente específico, haga clic en el icono de tres puntos en la **Acción** columna, luego haga clic en **Eliminar cliente** de el menú desplegable.



6.4 Ordenar

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



La clasificación predeterminadaing el pedido es de la siguiente manera:

- El propio-dispositivo (es decir, el dispositivo que está utilizando para acceder del enrutador'Panel de administración) siempre aparece en la parte superior.
- En el **Online Clients**, los dispositivos aparecen en una lista superior si se conectaron antes.
- En la sección **Fueralínea Cclientes** sección, los dispositivos aparecen en una lista superior si desconectado anteriormente.

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



Capítulo 7

Conozca la VPN

Este capítulo presenta VPN conceptos y escenarios de uso común .

7.1 Introducción

VPN

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

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

OpenVPN

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

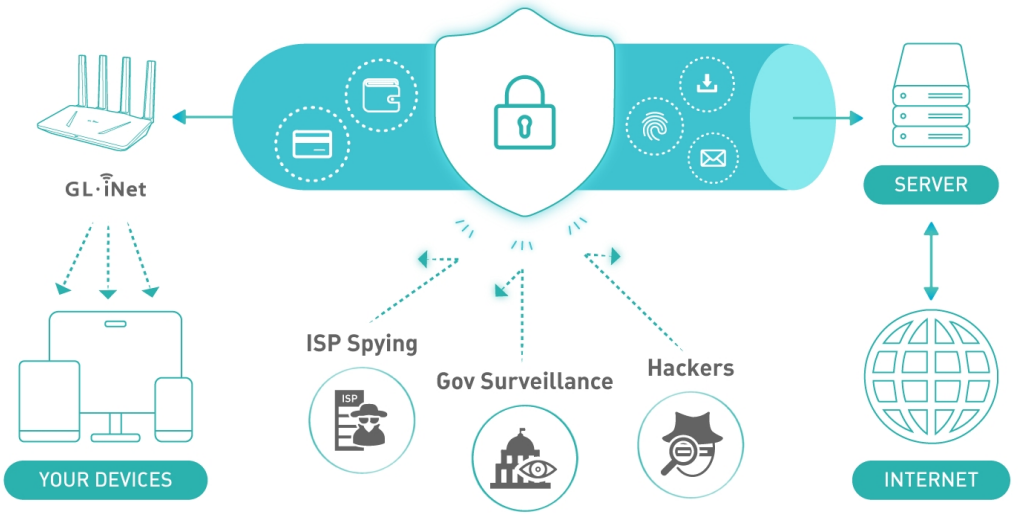
WireGuard

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

7.2 Escenarios de aplicación

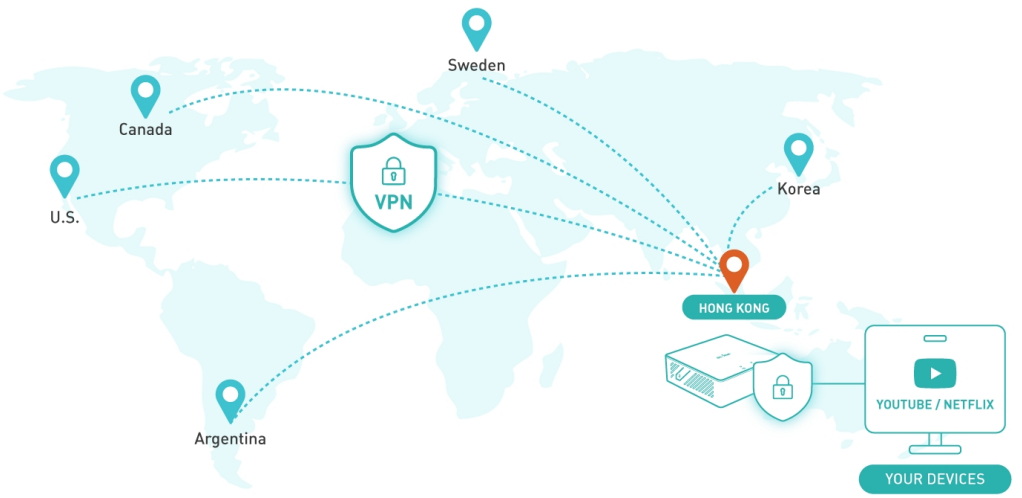
1. **Datos personales Privacidad**

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



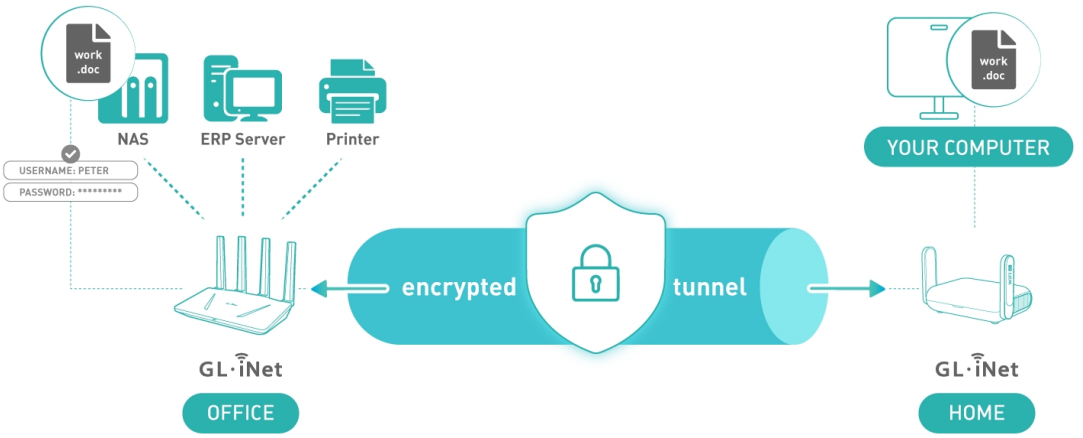
2. **Acceso sin restricciones en todo el mundo**

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



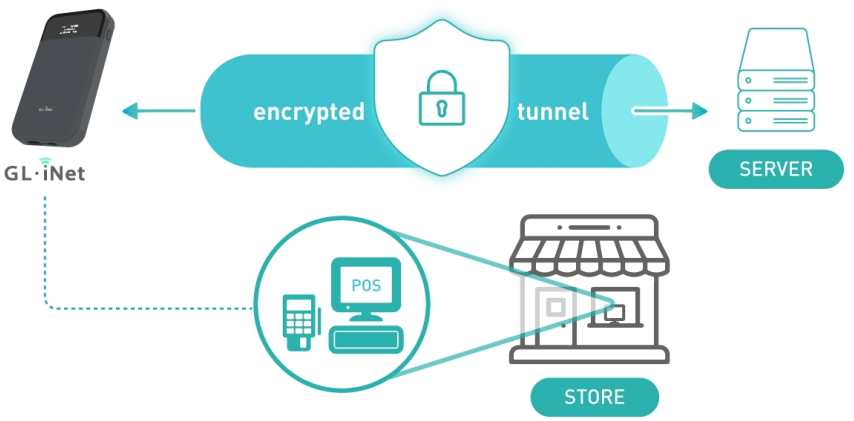
3. **Seguridad de datos para pequeñas empresas**

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



4. **Infraestructura de pago segura**

Los propietarios de pequeñas tiendas 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

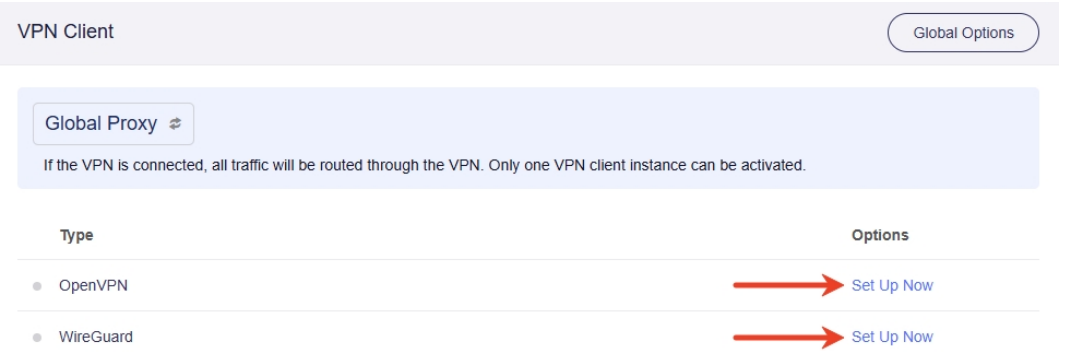
Este capítulo presenta cómo administrar las conexiones VPN a través del panel de administración web.

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

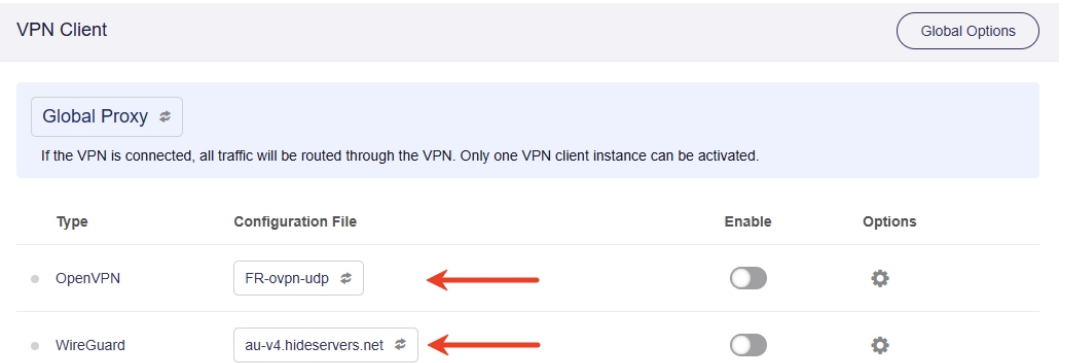
Cuando el enrutador está configurado como un cliente VPN activo, el panel de VPN muestra detalles de la conexión VPN, como la dirección del servidor, estadísticas de tráfico, IP virtual del cliente y registro de conexión. También le permite configurar ajustes avanzados como Bloquear tráfico que no sea 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 al **Cliente OpenVPN** o **Cliente WireGuard** página para cargar su archivo de configuración de VPNs.

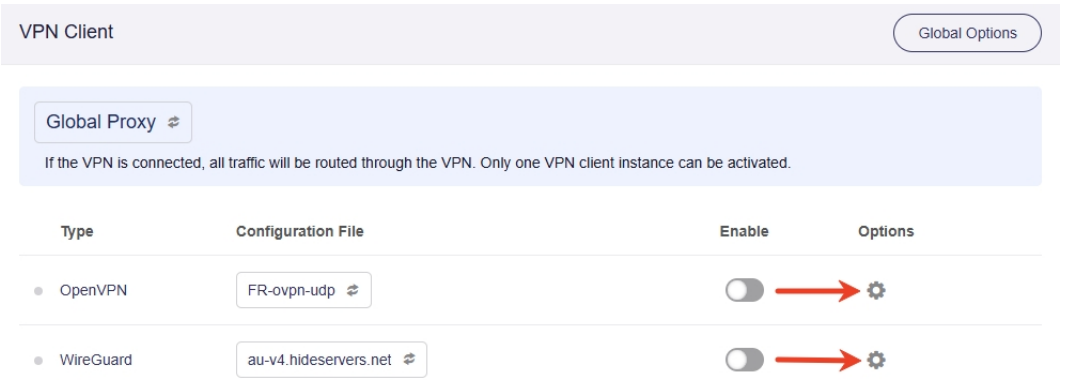


Una vez cargada, su configuración se mostrará en la columna **Archivo de configuración**. Si tiene varios archivos de configuración cargados, puede cambiar de archivo haciendo clic en el cuadro.

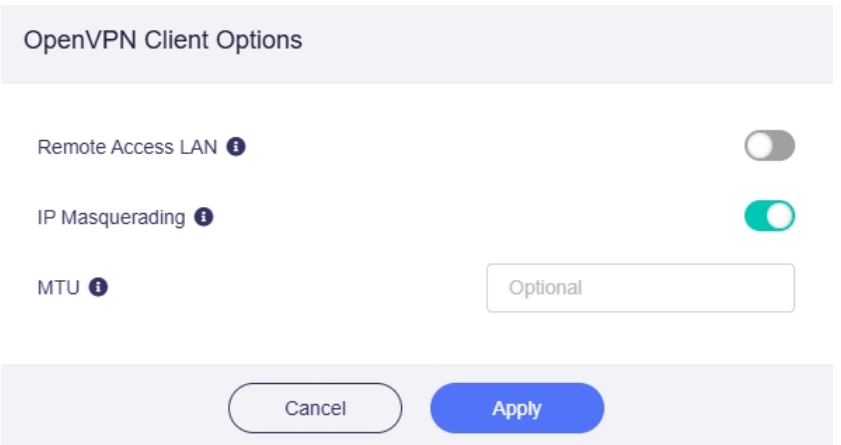


8.1.1 Opciones del cliente

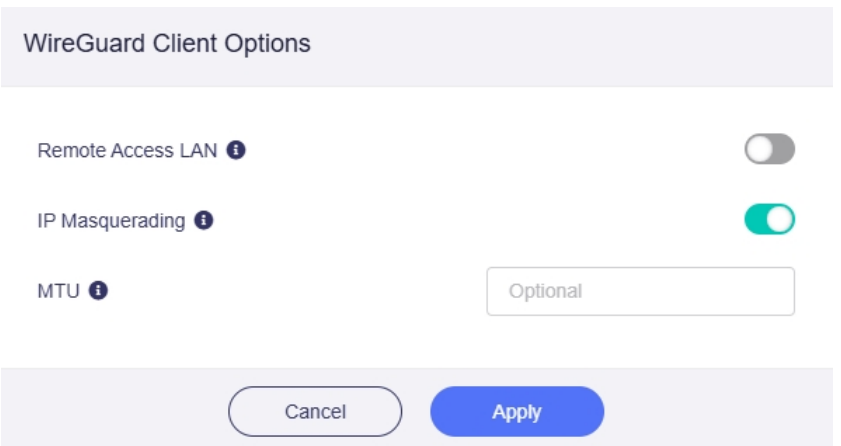
Haga clic en el ícono de ajustes a la derecha para acceder a las opciones del cliente OpenVPN o WireGuard.



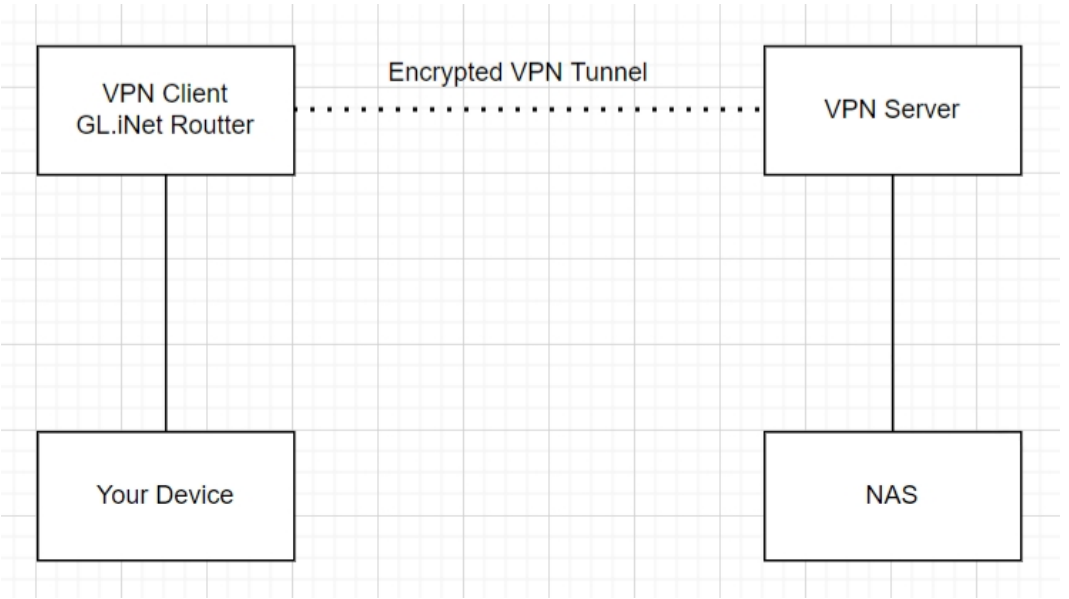
Las opciones del cliente OpenVPN se muestran de la siguiente manera.



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



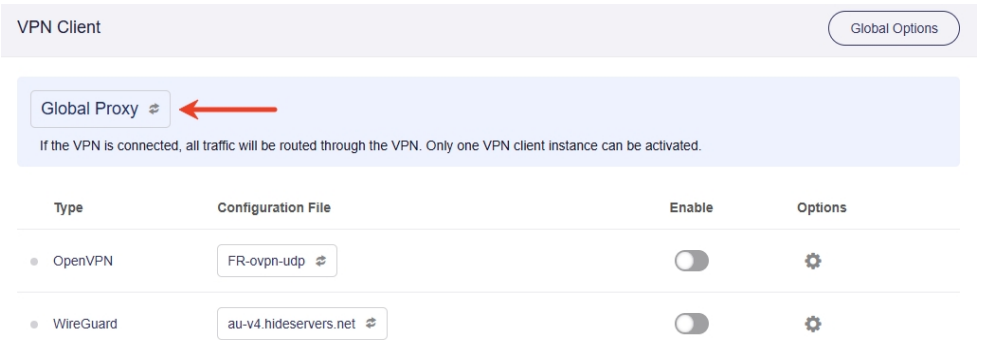
- **LAN de acceso remoto**: si está habilitado, acceso remoto a este enrutador y sus dispositivos LAN a través de VPN será permitido. El servidor VPN debe anunciar una ruta a la subred LAN de este enrutador.
  Por ejemplo, como se muestra en el siguiente diagrama, el enrutador GL.iNet se ejecuta como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



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

8.1.2 Modo de política

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



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

1. **Proxy global**

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

2. **Modo de política**

   Este modo se puede dividir en tres políticas.

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

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

   - **Según el dispositivo cliente.**

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

   - **Según la VLAN**.

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

3. **Modo de ruta**

   - **Detección automática**

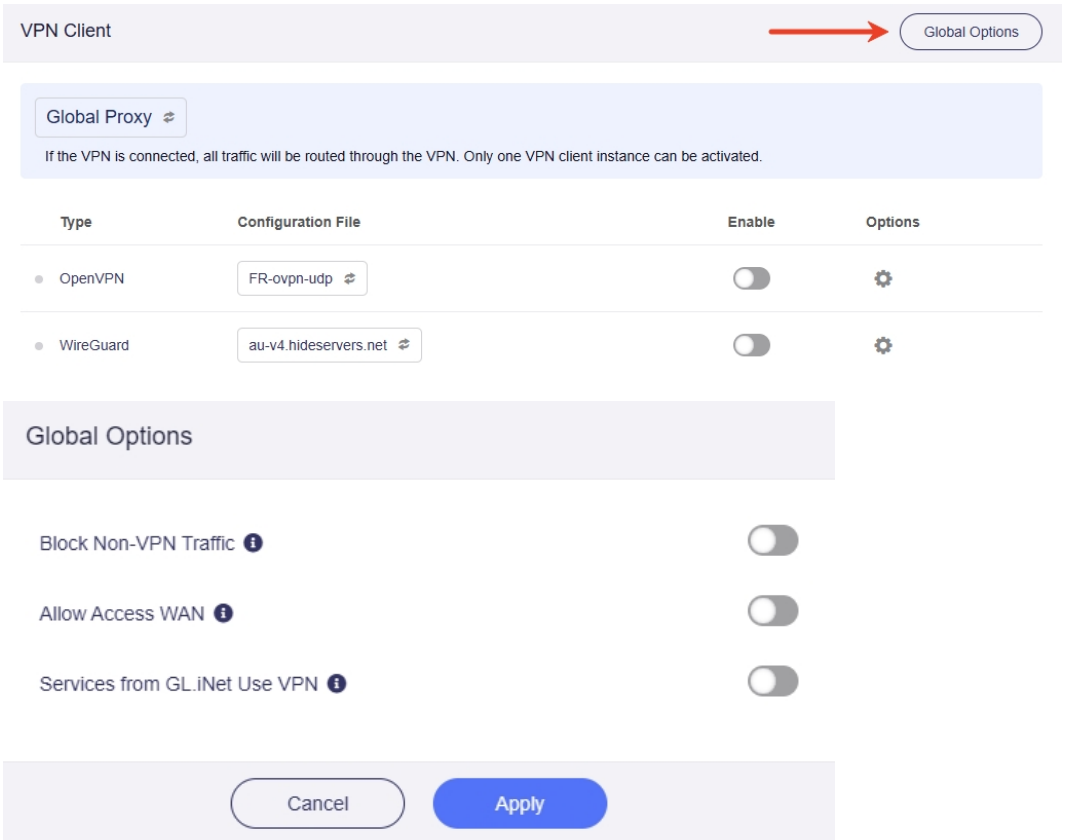
     Las reglas de enrutamiento definidas en cada archivo de configuración de cliente VPN o emitidas por el servidor VPN serán utilizado.

   - **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.



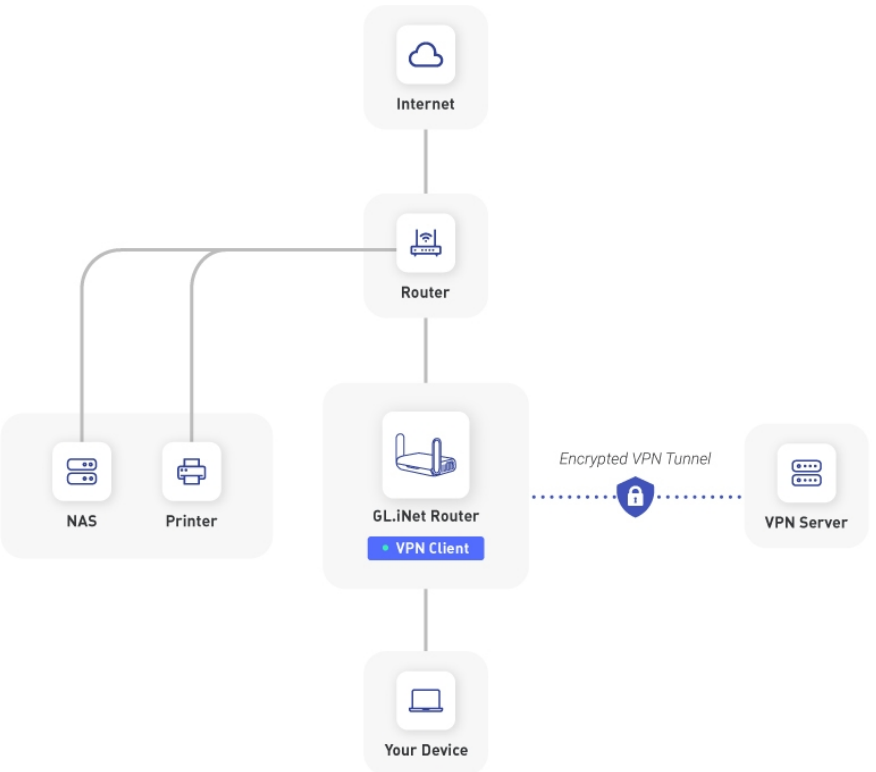
- **Bloquear tráfico que no sea VPN**: si está habilitado, todo el tráfico de Internet se fuerza a pasar exclusivamente a través del túnel VPN y no se puede enrutar a través de otras interfaces como la WAN del ISP local. Si la conexión VPN se cae inesperadamente, todo el tráfico de Internet se bloquea 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 la conexión VPN
e. Aplicaciones lanzadas antes del establecimiento de la VPN
f. Fugas de tráfico por aplicación

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



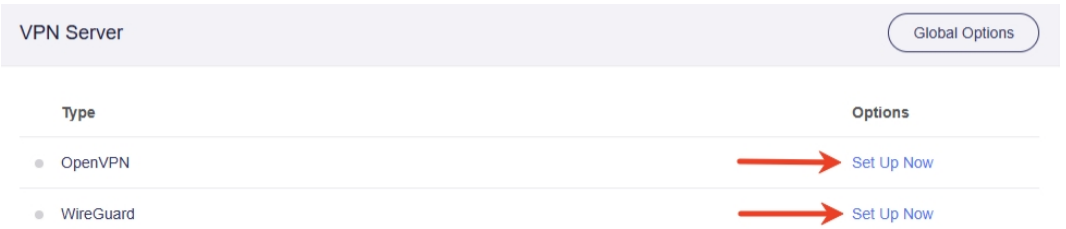
Como se muestra en el diagrama anterior, habilitar esta función permite que sus dispositivos locales lleguen a los hosts en la subred ascendente, como impresoras y NAS.

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

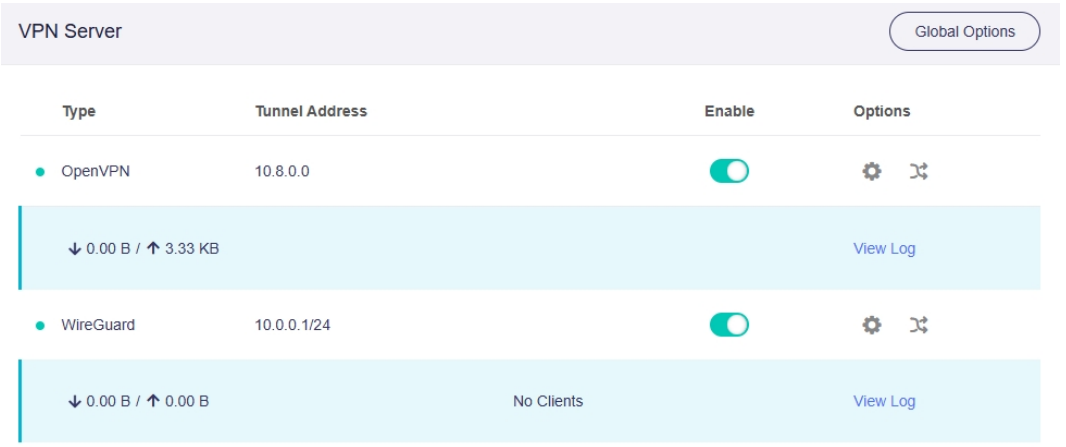
- **Servicios de GL.iNet usan VPN**: si están habilitados, los servicios GoodCloud, DDNS y rtty transmitirán paquetes a través de túneles VPN. Esta opción está deshabilitada de forma predeterminada, ya que estos servicios normalmente requieren la dirección IP real del dispositivo para funcionar correctamente.

8.2 Servidor VPN

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

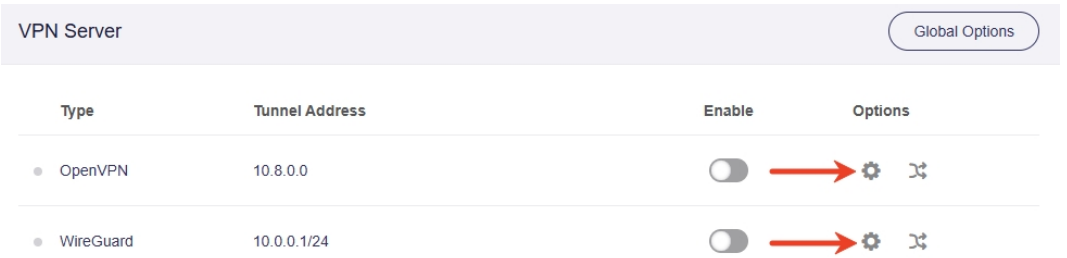


Después de habilitar el servidor OpenVPN o WireGuard, la página mostrará el estado del servidor de la siguiente manera.

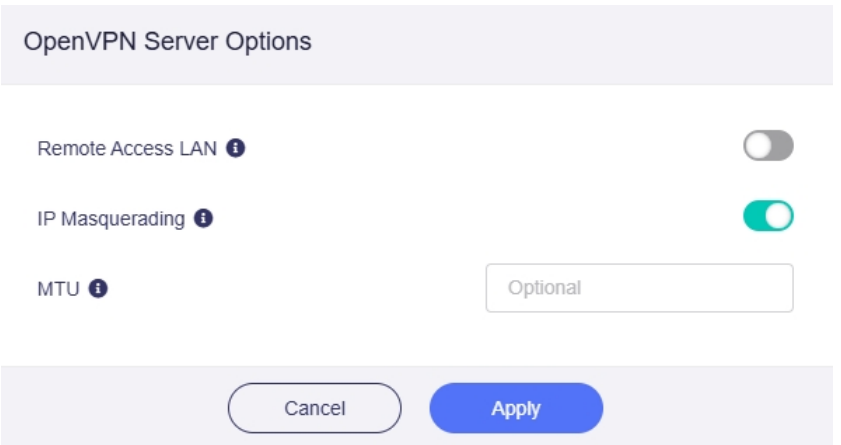


8.2.1 Opciones del servidor

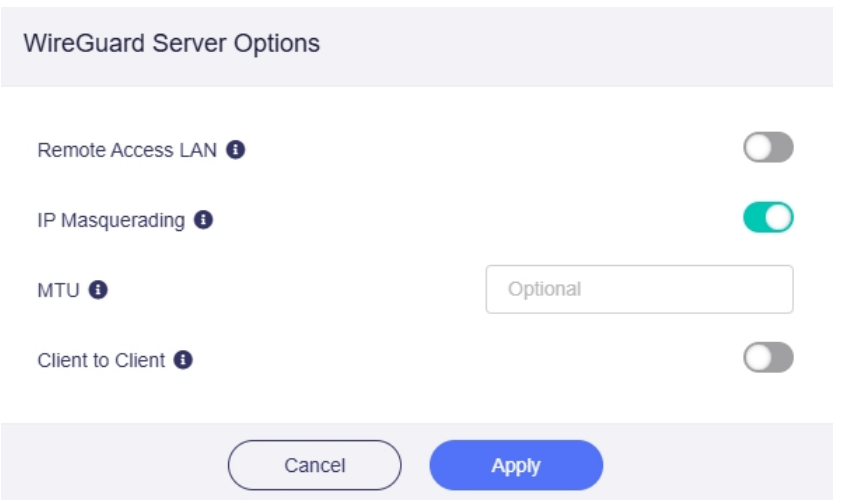
Haga clic en el ícono de ajustes a la derecha para acceder a las opciones del servidor OpenVPN o WireGuard.



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



Las opciones del servidor WireGuard se muestran como siguiente.

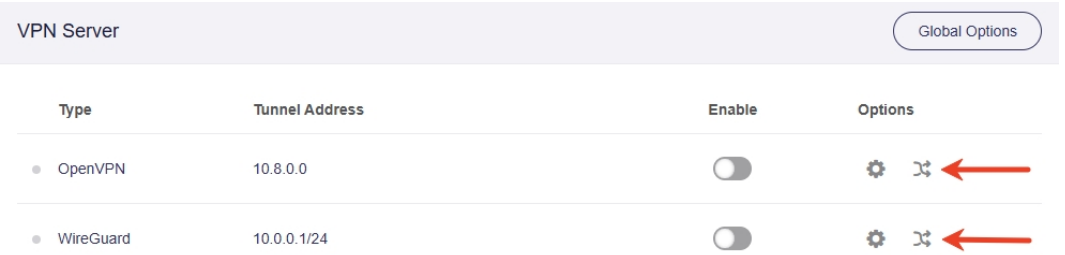


- **LAN de acceso remoto**: si está habilitado, se puede acceder a los recursos dentro de la subred LAN del servidor a través del túnel VPN.

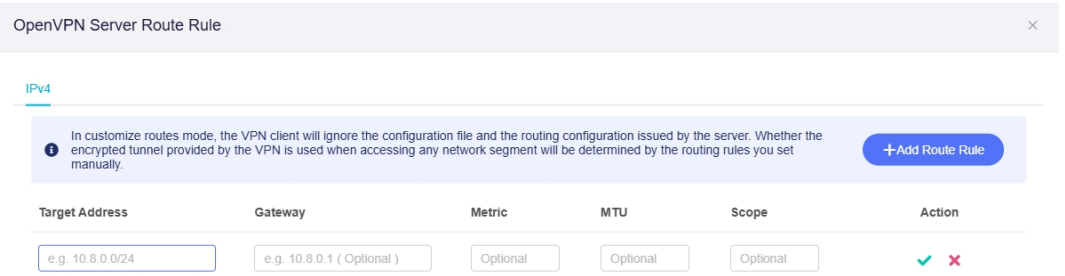
- **Enmascaramiento de IP**: Si está habilitado, las direcciones IP de origen de los clientes LAN se reescribirán en la IP del túnel VPN del enrutador. Deshabilite esto solo para configuraciones de sitio a sitio donde el par remoto conoce sus subredes LAN.
- **MTU**: abreviatura de Unidad de transmisión 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

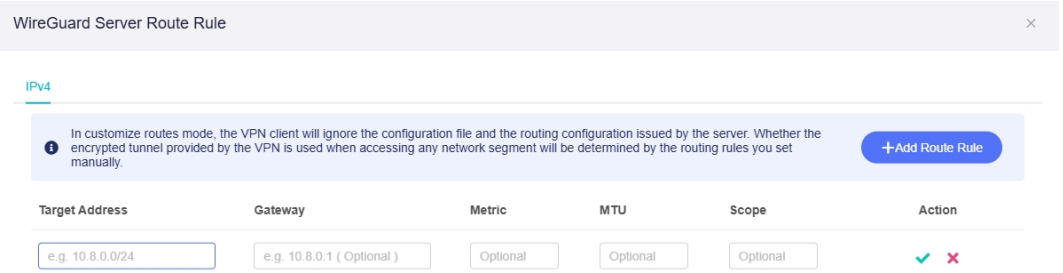
Haga clic en el icono de ruta a la derecha para personalizar las reglas de ruta OpenVPN o WireGuard como necesario.



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



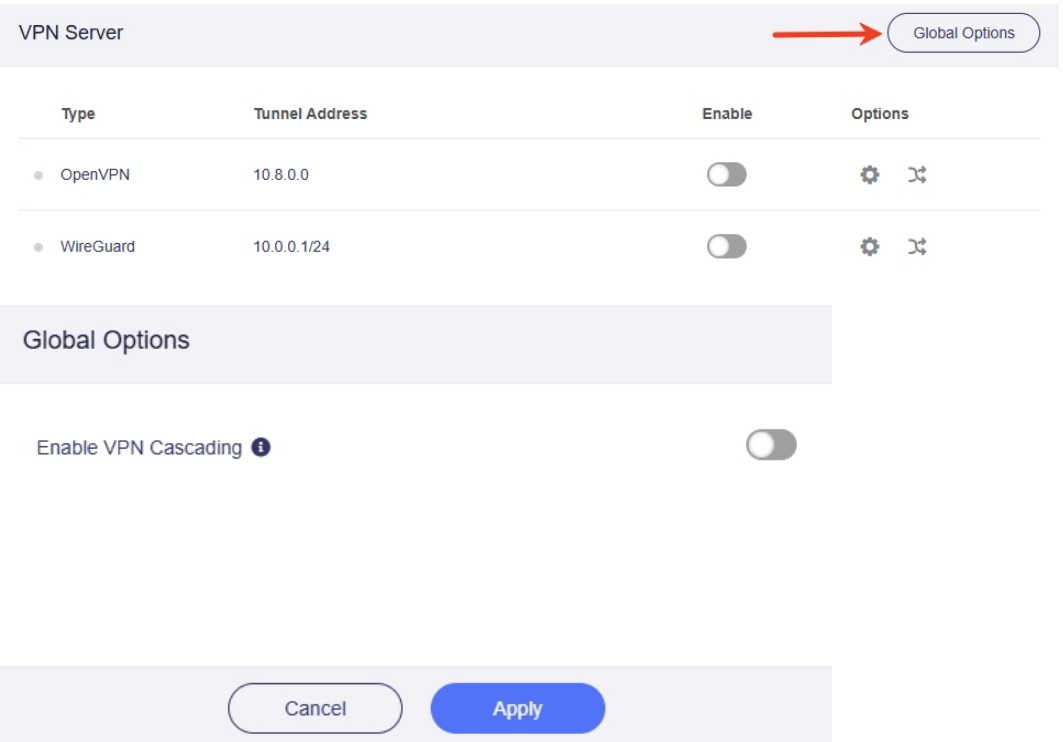
La regla de ruta del servidor WireGuard se muestra de la siguiente manera. Haga clic en **Agregar regla de ruta**, ingrese la **Dirección de destino** y **Puerta de enlace** y luego haga clic en el ícono de verificación verde para aplicar.



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

8.2.3 Opciones globales

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



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

Capítulo 9

Configurar el servidor VPN

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

9.1 Configurar el servidor OpenVPN

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

9.1.1 Preparación

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

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

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

   Métodos alternativos:

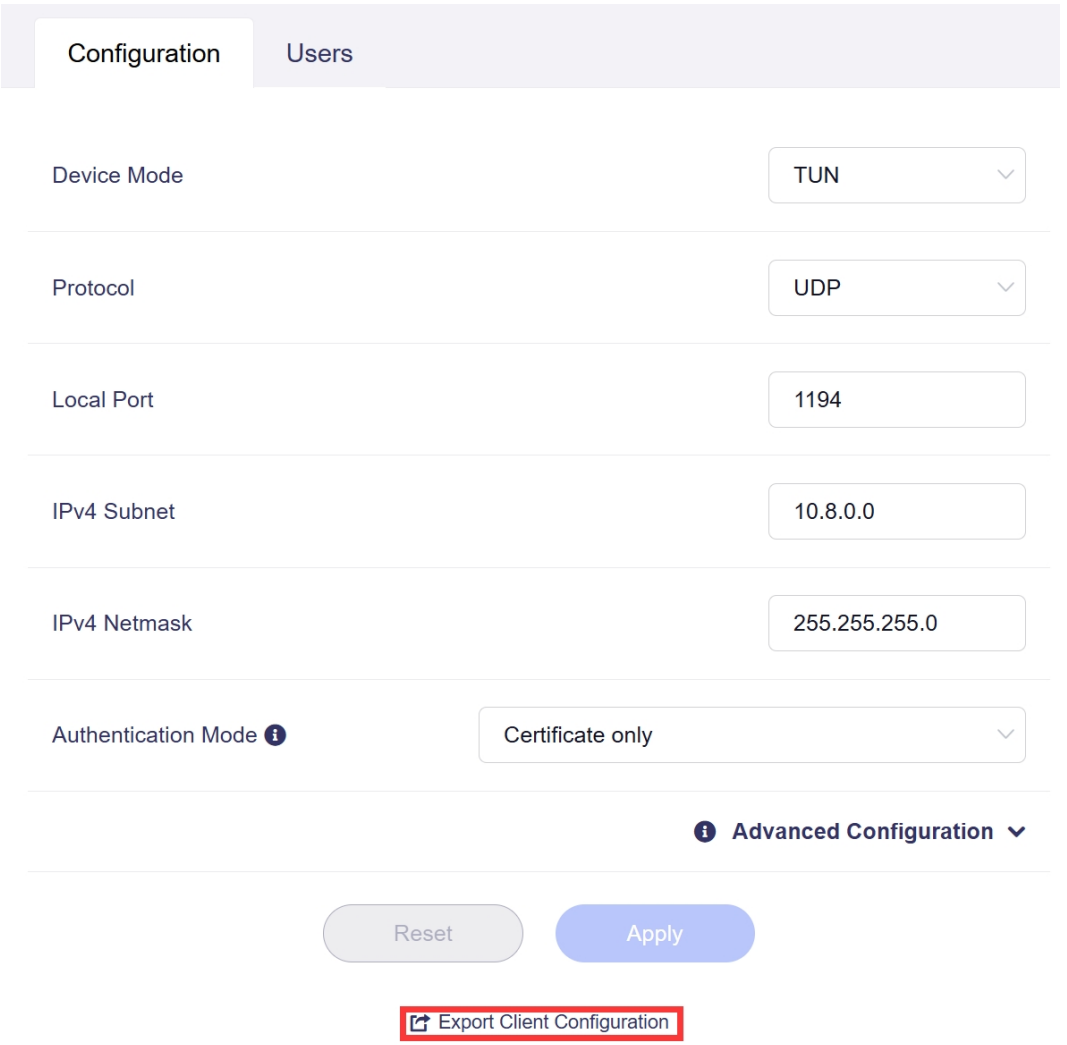
   - Si tiene un enrutador principal aguas arriba de su enrutador GL.iNet, inicie sesión en él y verifique que tenga una dirección IP pública asignada por su ISP.
   - Solicite a su ISP una dirección IP pública. Esto puede generar un cargo adicional.

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

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

9.1.2 Pasos de configuración

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



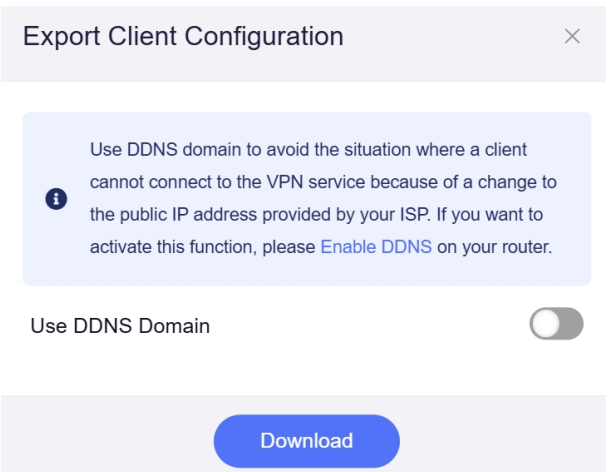
- **Modo de dispositivo**: TAP-S2S o Tun. Consulte aquí para las diferencias.
- **Protocolo**: UDP o TCP. Consulte aquí para las diferencias.
- **Modo de autenticación**: esto determina el método de autenticación utilizado cuando el cliente se conecta al servidor. Hay tres opciones:

- **Solo certificado**: si se selecciona, el enrutador generará automáticamente claves de certificado de servidor y cliente y las incrustará en el archivo de configuración. Cuando carga la configuración en el cliente, no se requieren credenciales adicionales.
- **Solo nombre de usuario/contraseña**: si se selecciona, el enrutador generará la configuración del cliente sin claves de certificado. Usted debe agregar primero un nombre de usuario y una 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**: Personalice más configuraciones del servidor si es necesario.

3. Exportar configuración del cliente.

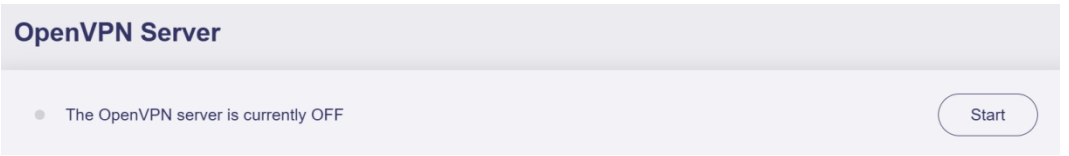
   Después de hacer clic **Exportar configuración del cliente** en la parte inferior de la pestaña Configuración (o aplicar la configuración modificada), aparecerá una ventana como la siguiente. Haga clic en **Descargar** para exportar la configuración.



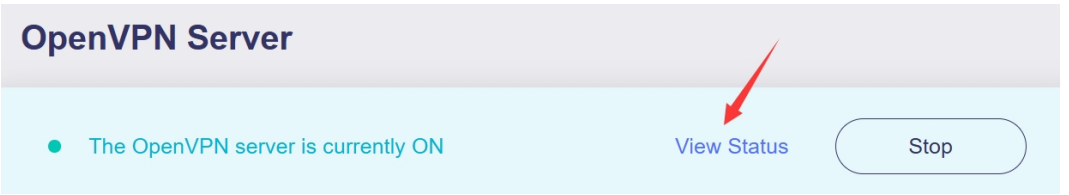
Consejo: Si su IP pública dirección cambia con frecuencia, vaya a **APLICACIONES** > **DNS dinámico** y habilitar DDNS. Luego puede usar el dominio DDNS como su dirección de servidor.

4. Inicie el servidor OpenVPN.

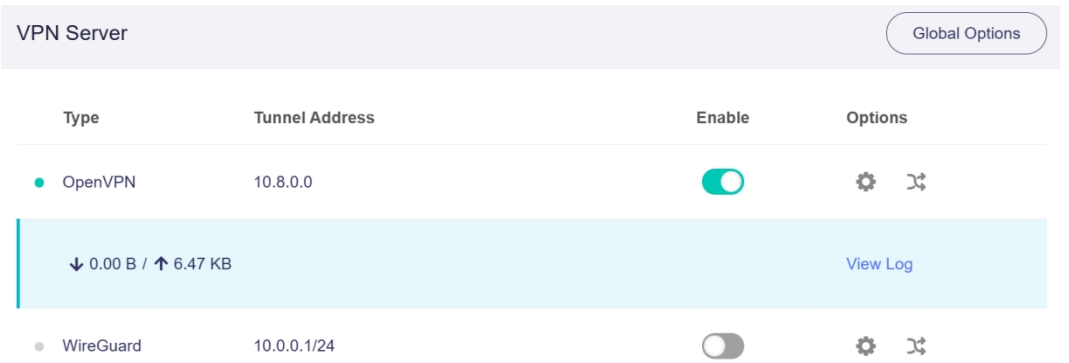
   En la página **Servidor OpenVPN**, haga clic en **Iniciar** en la esquina superior derecha para iniciar el servidor.



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



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



9.1.3 Solución de problemas

Si la conexión falla, existen varias razones comunes:

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

9.2 Configurar el servidor WireGuard

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

9.2.1 Preparación

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

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

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

   Métodos alternativos:

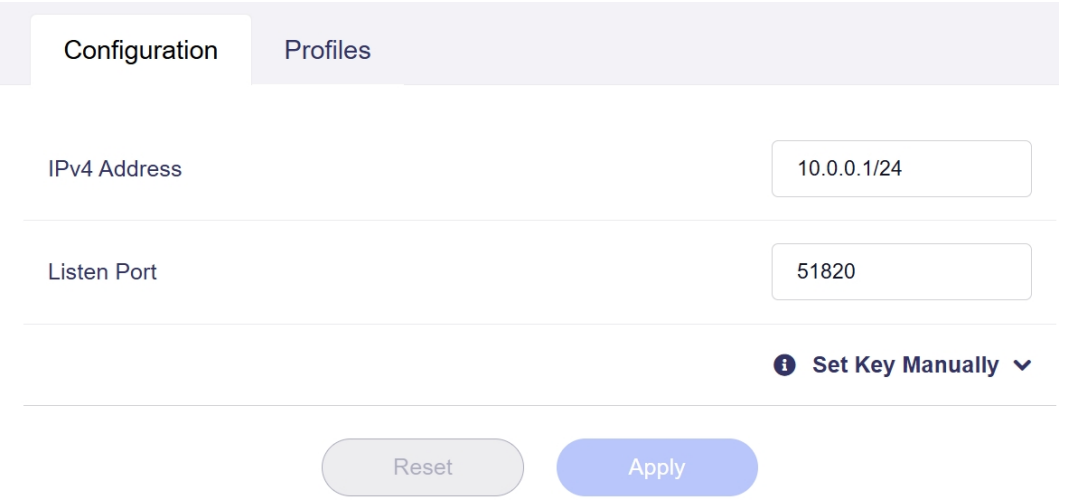
   - Si tiene un enrutador principal aguas arriba de su enrutador GL.iNet, inicie sesión en él y verifique que tenga una dirección IP pública asignada por su ISP.
   - Solicite a su ISP una dirección IP pública. Esto puede generar un cargo adicional.

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

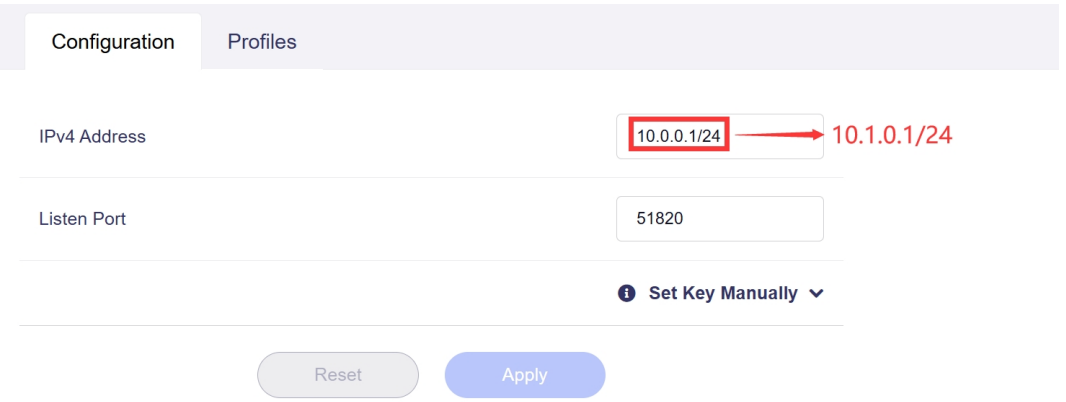
   - Si su enrutador GL.iNet es el enrutador principal de su red, no se requiere configuración de reenvío de puerto. Continúe con el siguiente paso.
   - Si ya hay un enrutador primario en uso y su enrutador GL.iNet está configurado como enrutador secundario, deberá configurar el reenvío de puertos en el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

9.2.2 Pasos de configuración

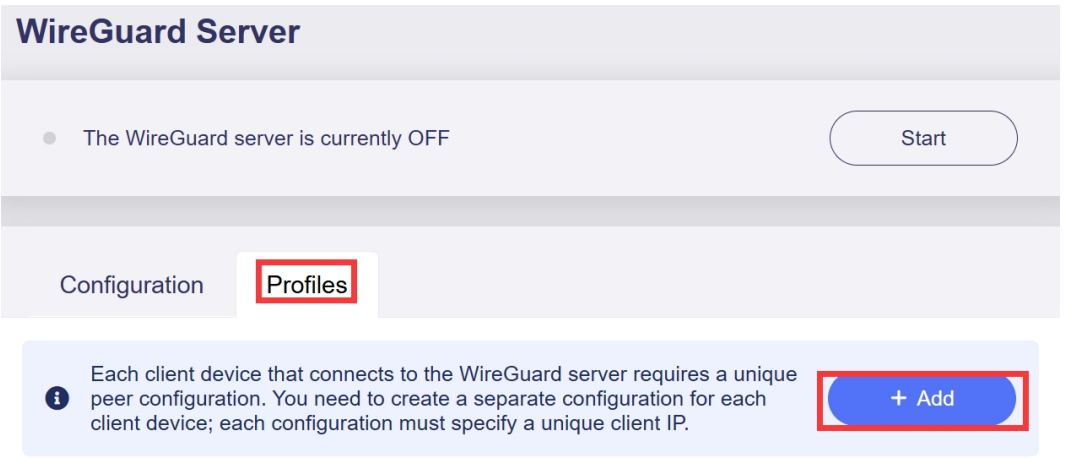
1. Inicie sesión en el panel de administración web del enrutador', navegue hasta **VPN** > **Servidor WireGuard** y luego haga clic en **Generar configuración** (solo para la configuración inicial del servidor VPN).
2. Aplicar la configuración.
   La configuración predeterminada funciona en la mayoría de los casos. No es necesario modificar la dirección IPv4 a menos que it conflictos con la puerta de enlace del enrutador ascendente.



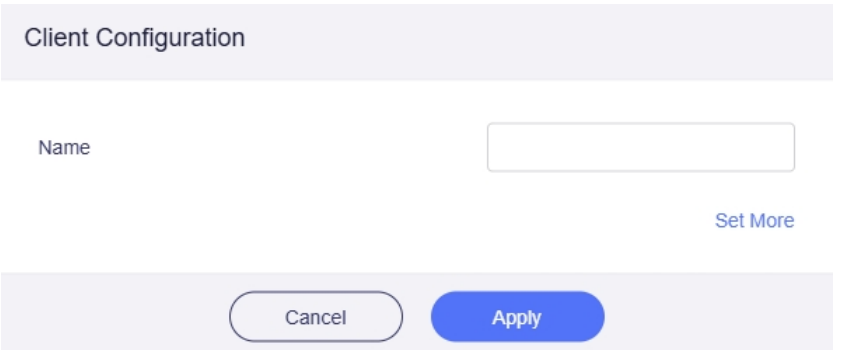
   Si el La dirección IPv4 entra en conflicto con la puerta de enlace de su enrutador ascendente, modifique la dirección IPv4 a otra una (por ejemplo, **10.1.0.1/24**) y haga clic en **Aplicar**. Asegúrese de que se incluya la notación CIDR "/24" para evitar problemas de conectividad.



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



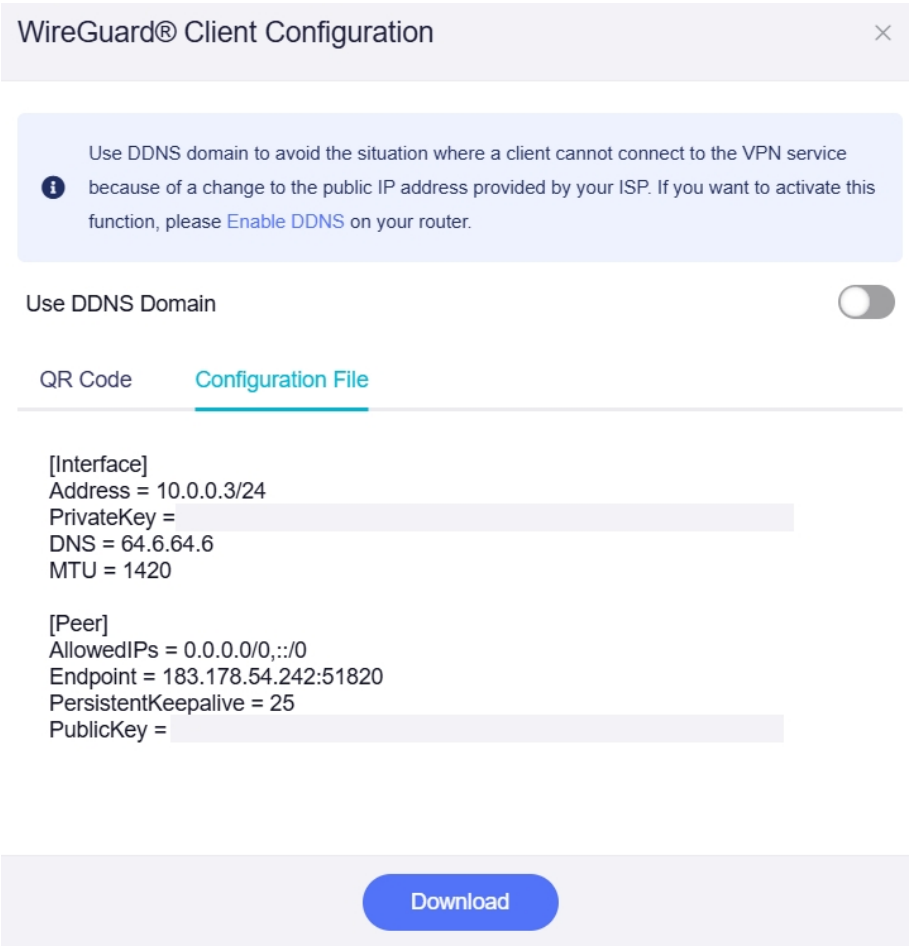
Establezca un nombre descriptivo y haga clic en **Aplicar** para continuar.



4. Descargar configuración.

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

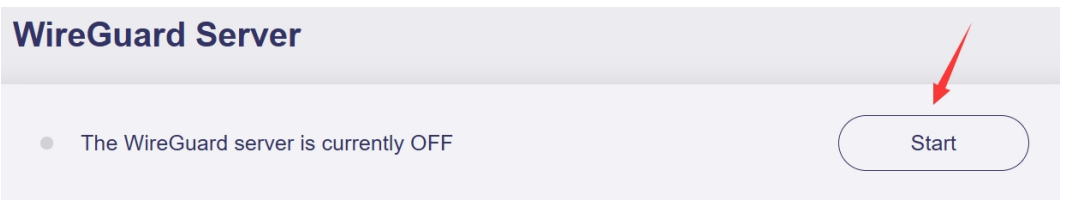
   - **Código QR**: Adecuado para dispositivos (por ejemplo, teléfonos inteligentes, tabletas, computadoras portátiles) con la aplicación WireGuard instalada. Si desea configurar un dispositivo específico como cliente WireGuard, simplemente abra la aplicación WireGuard y escanee el código QR para importar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



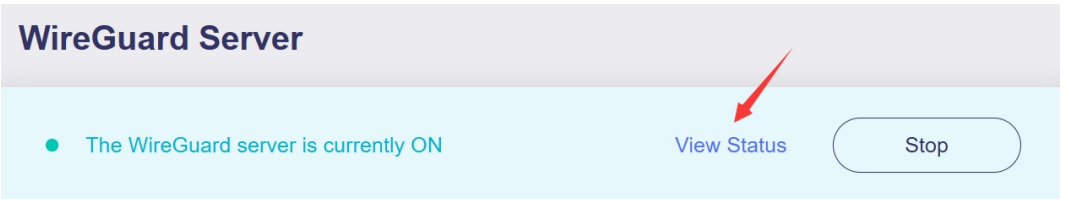
Consejo: Si su IP pública dirección cambia con frecuencia, vaya a **APLICACIONES** > **DNS dinámico** y habilite DDNS. Entonces puedes usar el dominio DDNS como su dirección de servidor.

5. Inicie el servidor WireGuard.

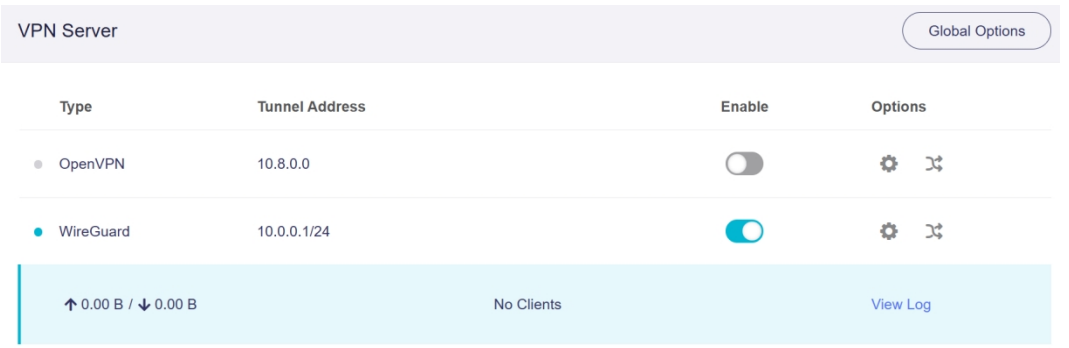
   En la página **Servidor WireGuard**, haga clic en **Iniciar** en la esquina superior derecha para iniciar el servidor.



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



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



9.2.3 Solución de problemas

Si la conexión falla, existen varias razones comunes:

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

Capítulo 10

Configurar el cliente VPN

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

10.1 Configurar el cliente OpenVPN

10.1.1 Preparación

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

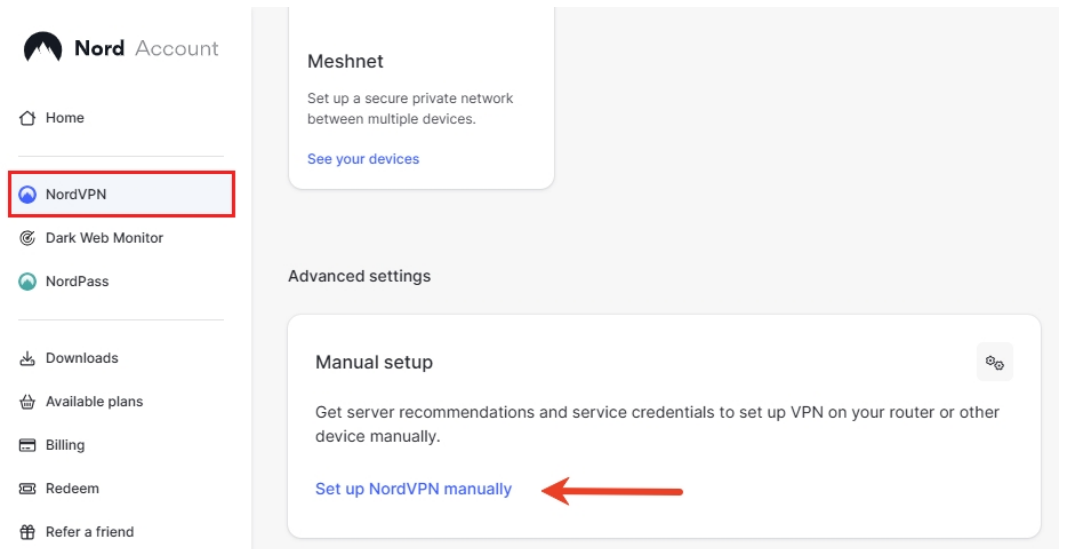
Siguiente, visite el sitio web oficial del proveedor de servicios VPN al que se suscribió y obtener las credenciales de servicio o el archivo de configuración. Si no sabe cómo obtener el archivo de configuración, consulte este enlace o póngase en contacto con su soporte.

10.1.2 Configurar NordVPN

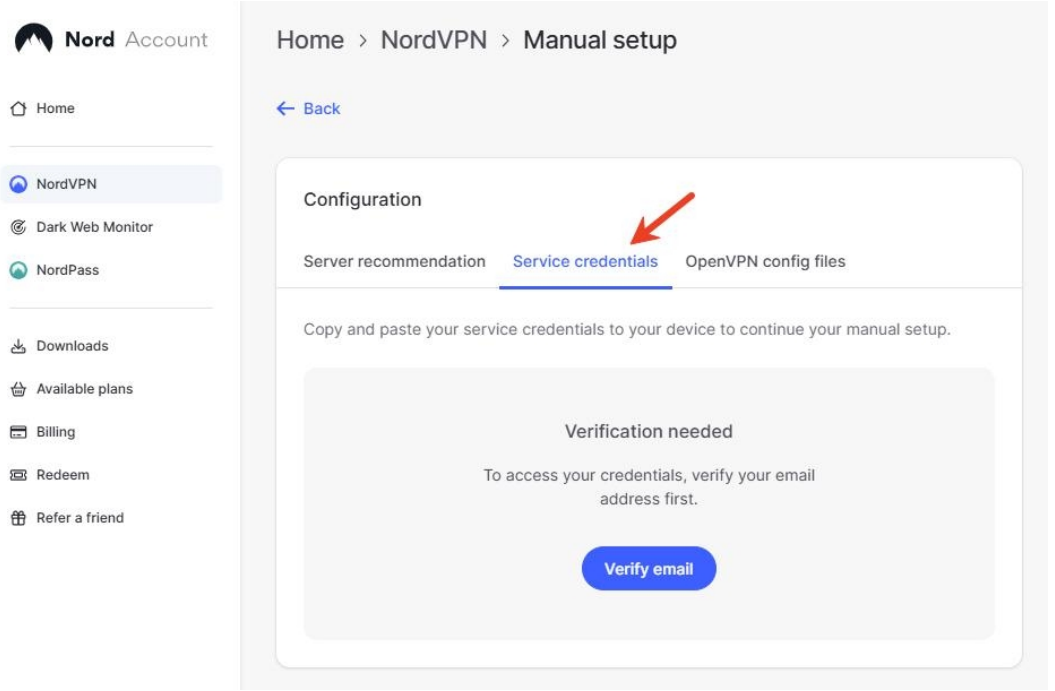
NordVPN está integrado en el panel de administración GL.iNet web . Puede adquirir archivos de configuración para todos los servidores NordVPN introduciendo las credenciales de su cuenta (obtenidas del Panel de NordVPN) en el panel de administración web del enrutador o en la aplicación móvil GL.iNet ,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

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

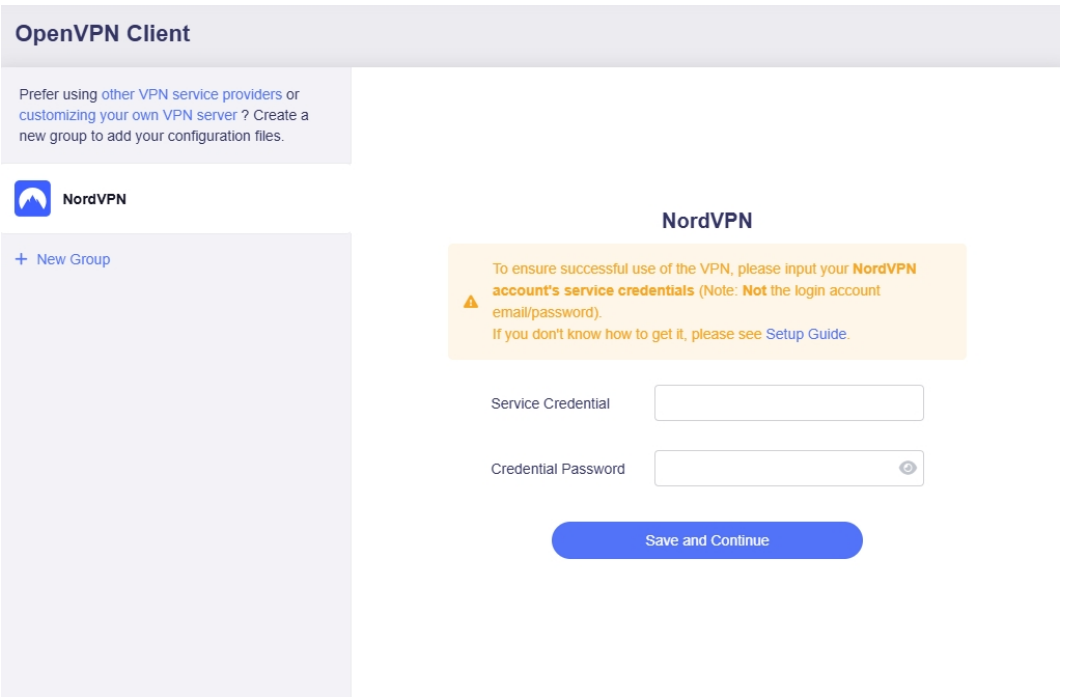
1. Inicie sesión en su cuenta web NordVPN aquí.
2. Oen el Nord Dashboard, haga clic en **NordVPN**, luego haga clic en **Configurar NordVPN manualmente**.



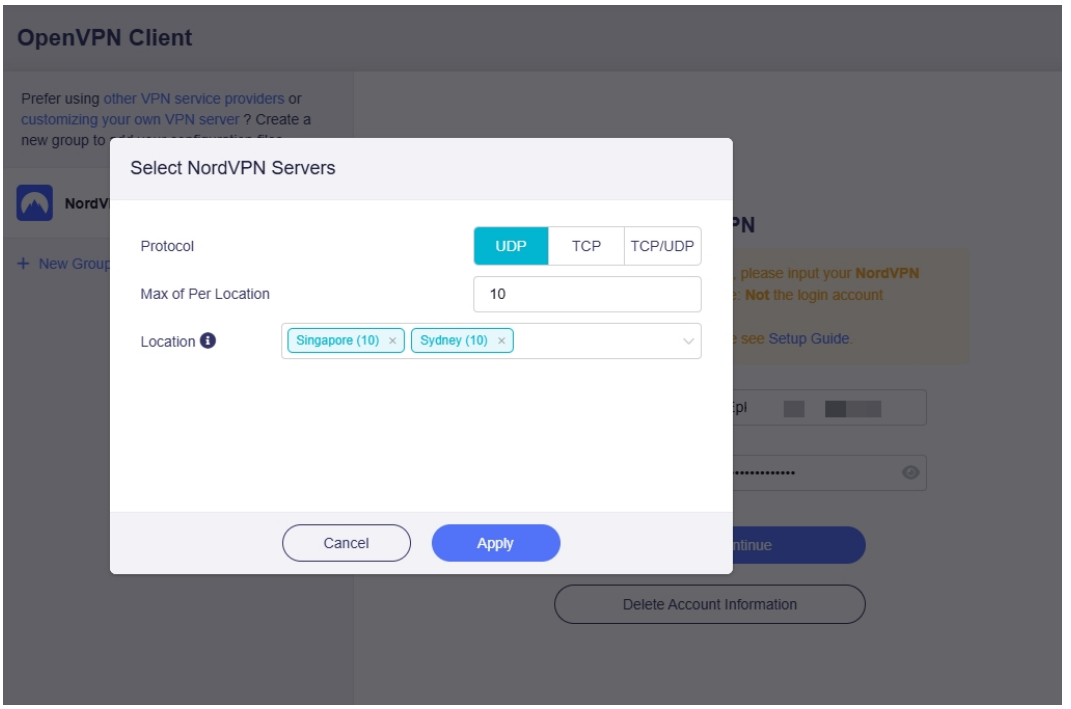
Encontrará el servicio **credenciales**. Cópielos para usarlos más adelante.



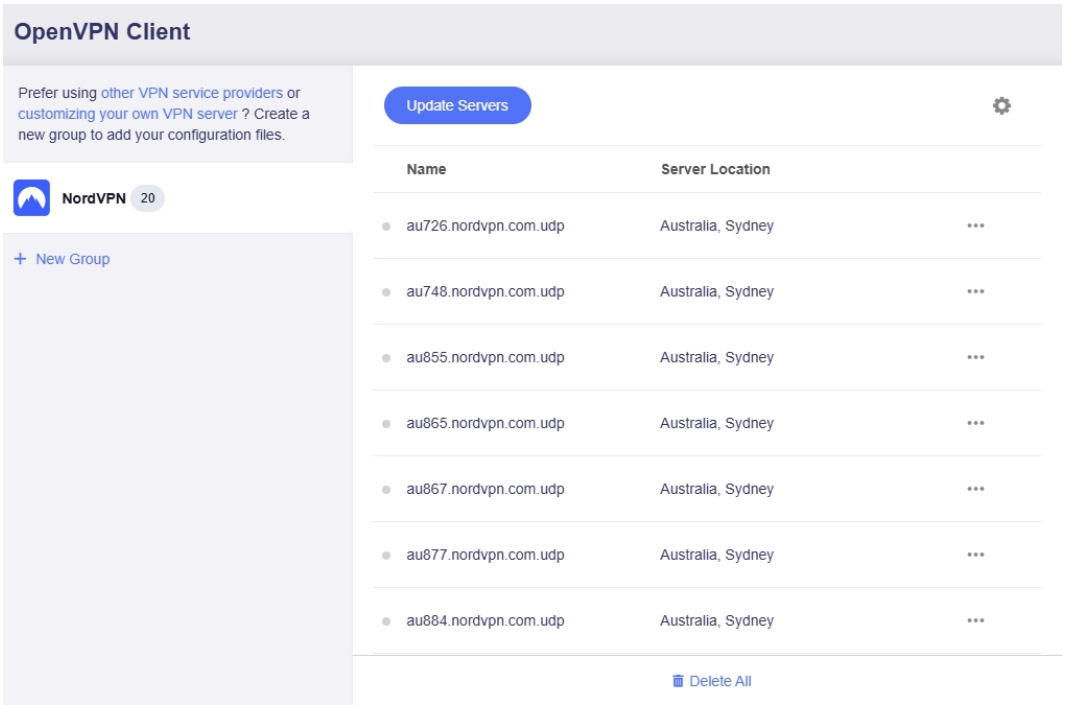
3. Inicie sesión en el panel de administración web de su enrutador y navegue a **VPN** > **Cliente OpenVPN** > **NordVPN**. Ingrese las credenciales de servicio (Nota: NO es el correo electrónico ni la contraseña de la cuenta de inicio de sesión), luego haga clic en **Guardar y continuar**.



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

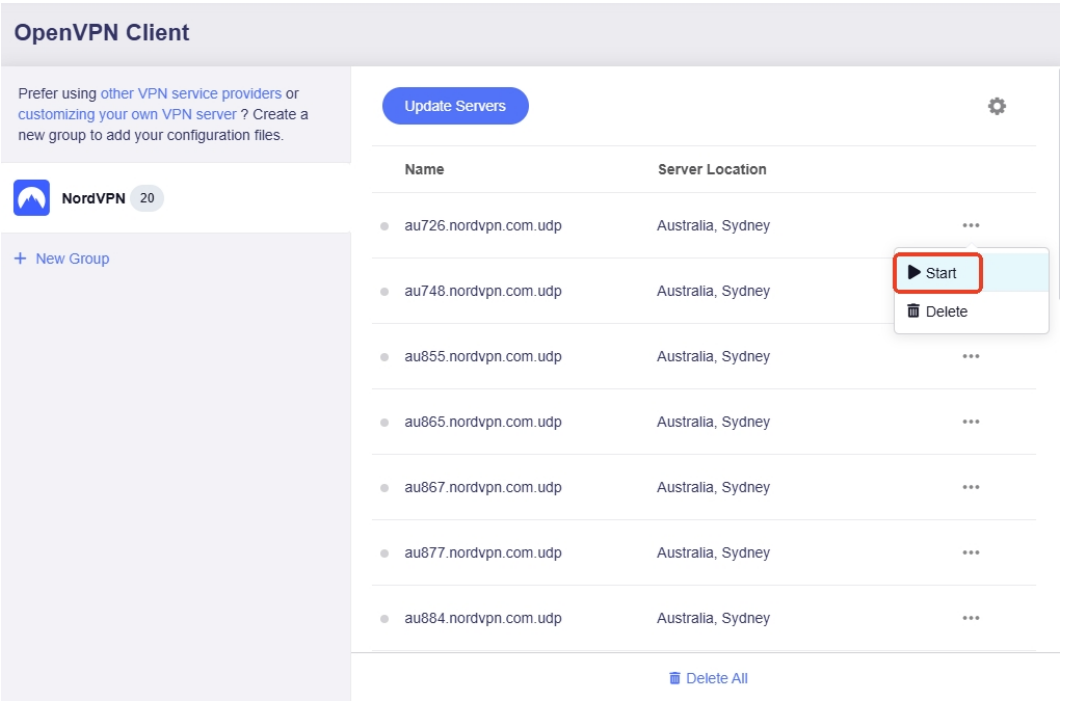


Descargará los archivos de configuración.

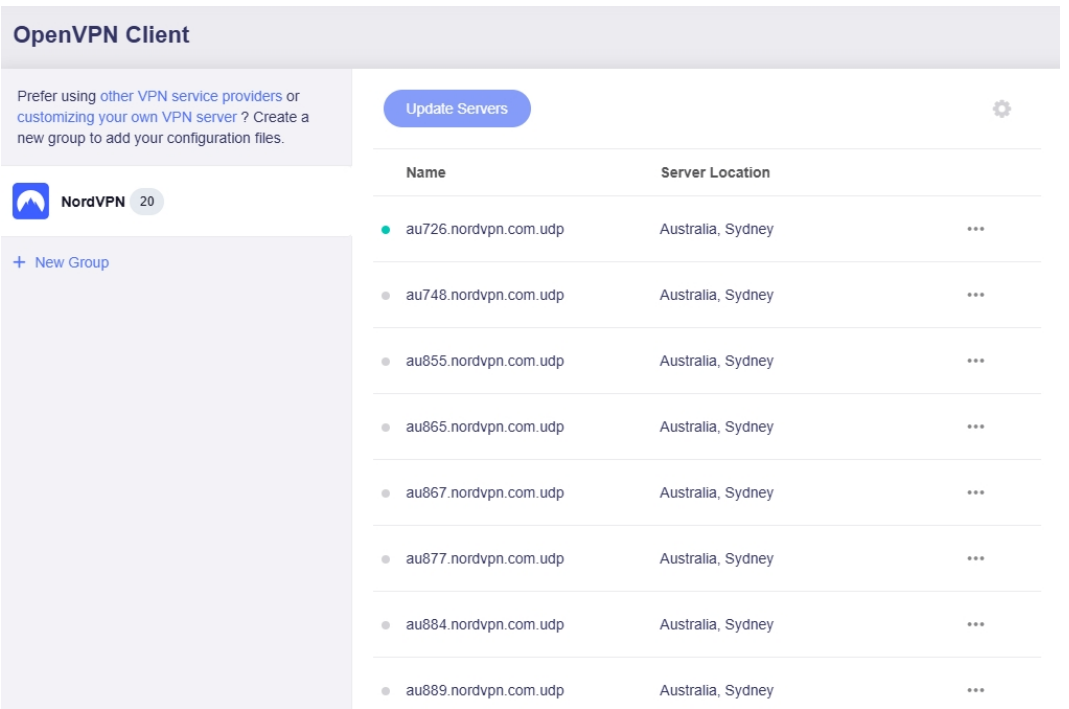


5. Iniciará una conexión.

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



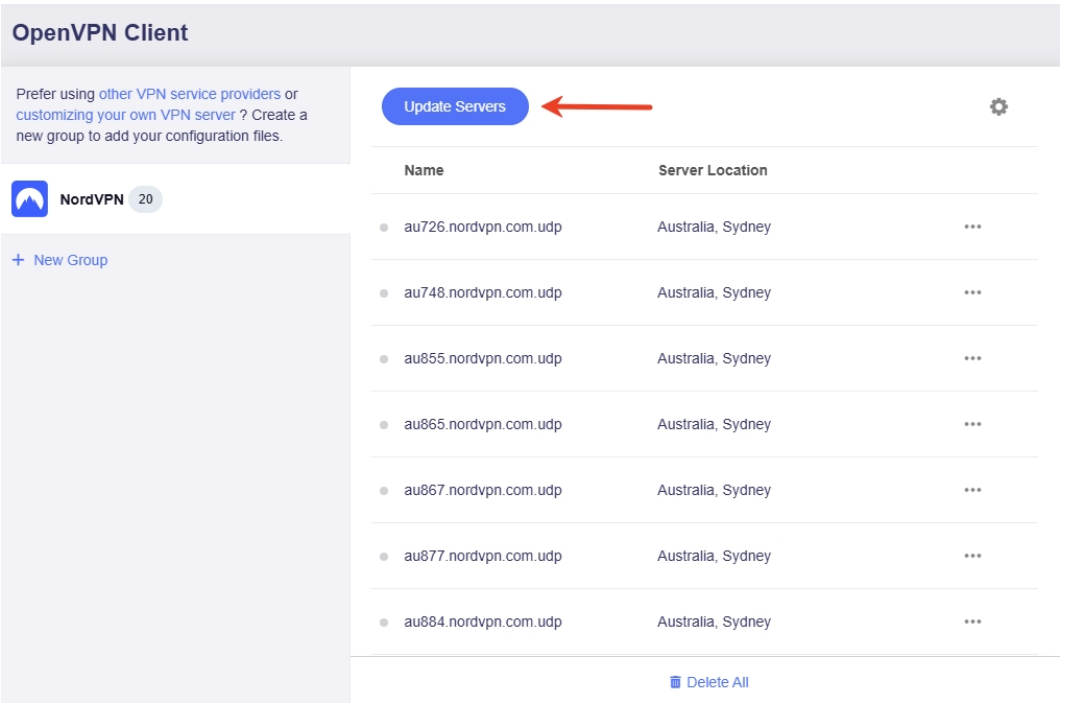
6. Una vez conectado, aparecerá un punto verde junto al archivo de configuración.



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

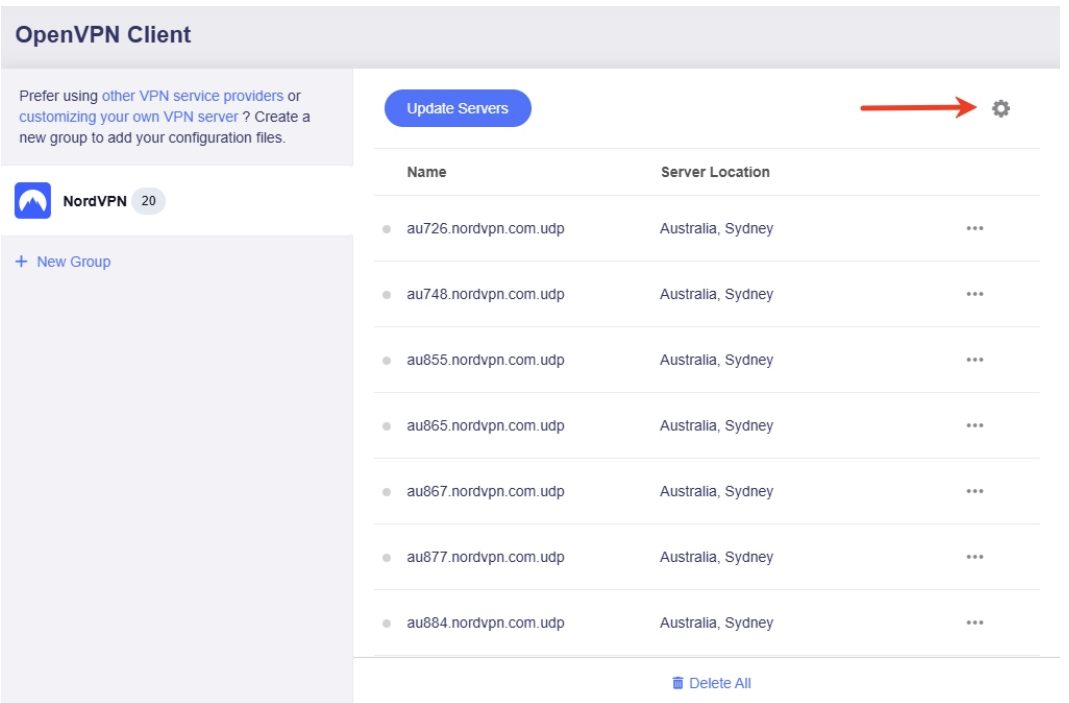
7. Actualizar servidores.

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



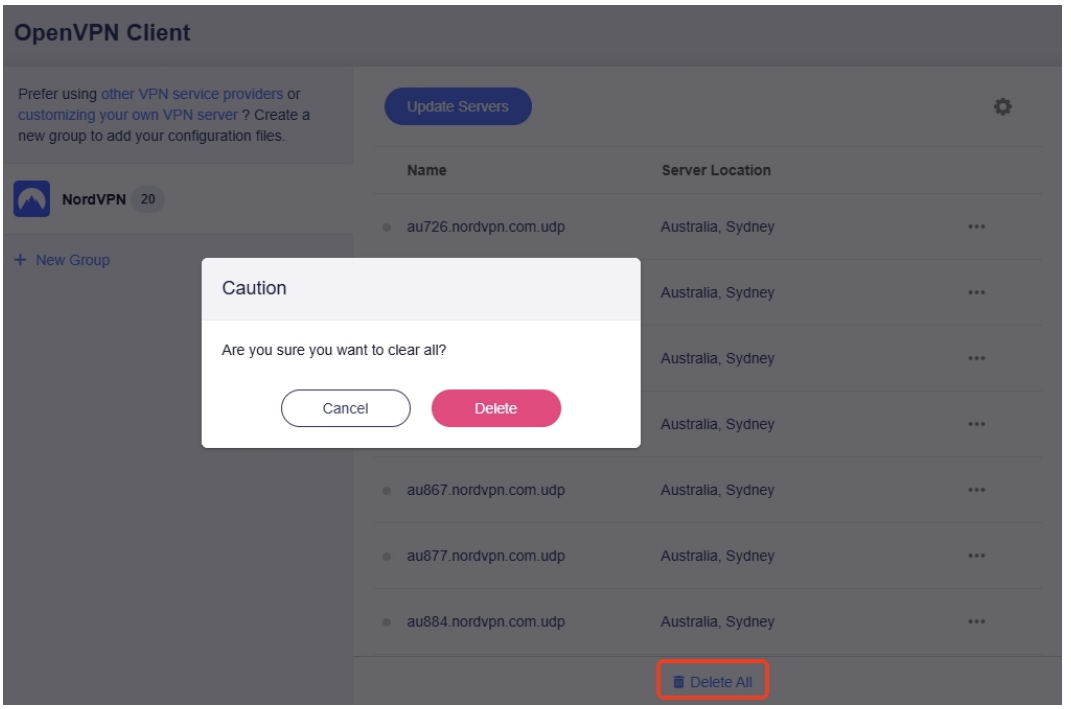
8. Editar credenciales.

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



9. Eliminar todos los archivos.

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

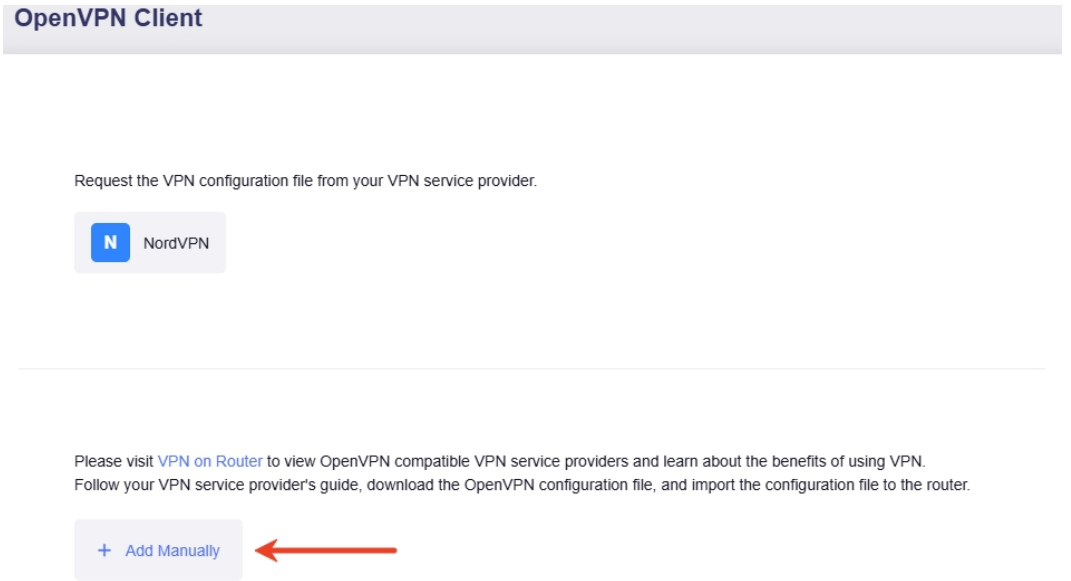


10.1.3 Configurar el cliente OpenVPN manualmente (para otros proveedores)

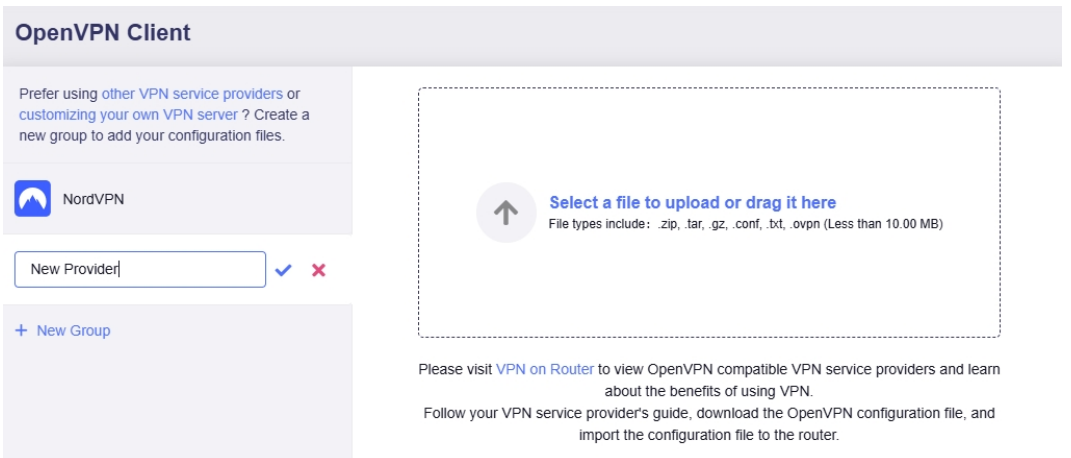
Si su proveedor de servicios OpenVPN no está integrado en nuestro panel de administración, primero visite el sitio web oficial de su proveedor de servicios suscrito para obtener el archivo de configuración. Luego cárguelo en el enrutador para configurar un cliente OpenVPN.

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

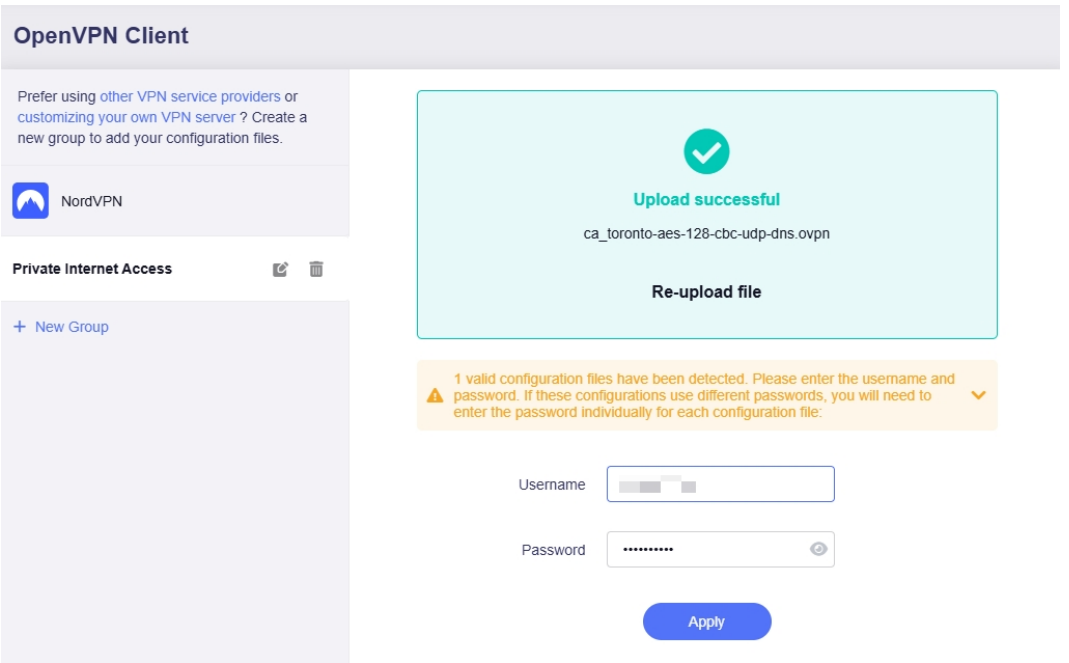
1. Descargue un archivo de configuración del sitio web oficial de Private Internet Access.
2. Inicie sesión en el panel de administración web de su enrutador, navegue hasta **VPN** > **Cliente OpenVPN** y haga clic en **Agregar. Manualmente**.



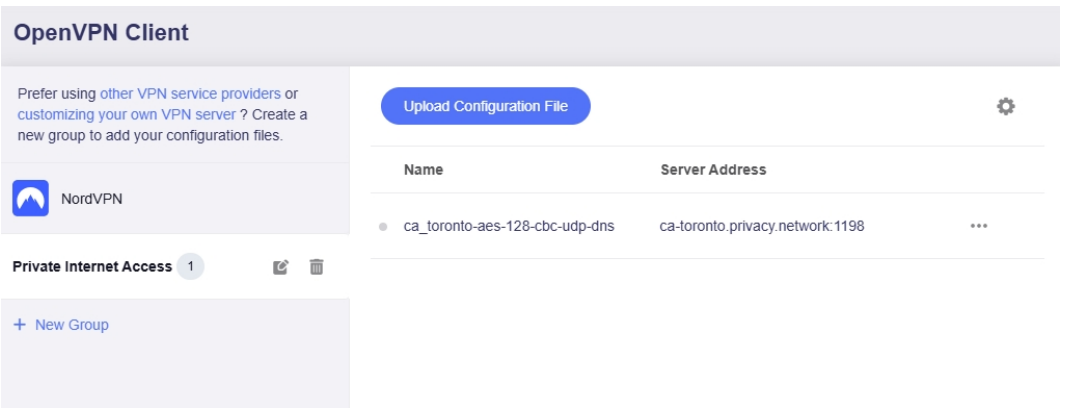
3. Creará un grupo en la barra lateral izquierda.Establezca un nombre descriptivo para el grupo.



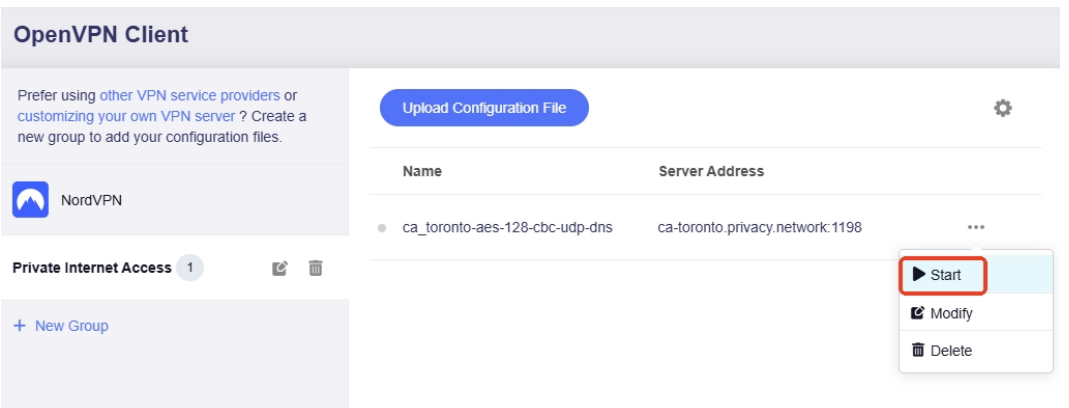
4. Cargue su archivo de configuración de OpenVPN. Ingrese las credenciales si es necesario, luego haga clic en **Aplicar**.



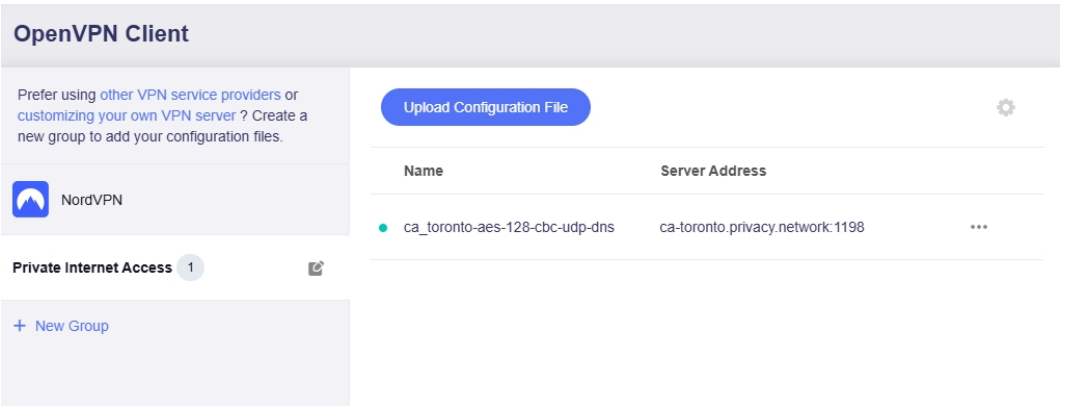
YVerá el archivo de configuración cargado.



5. Haga clic en el ícono de tres puntos en el derecho para iniciar una conexión.



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



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

10.2 Configurar el cliente WireGuard

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

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

10.2.1 Preparación

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

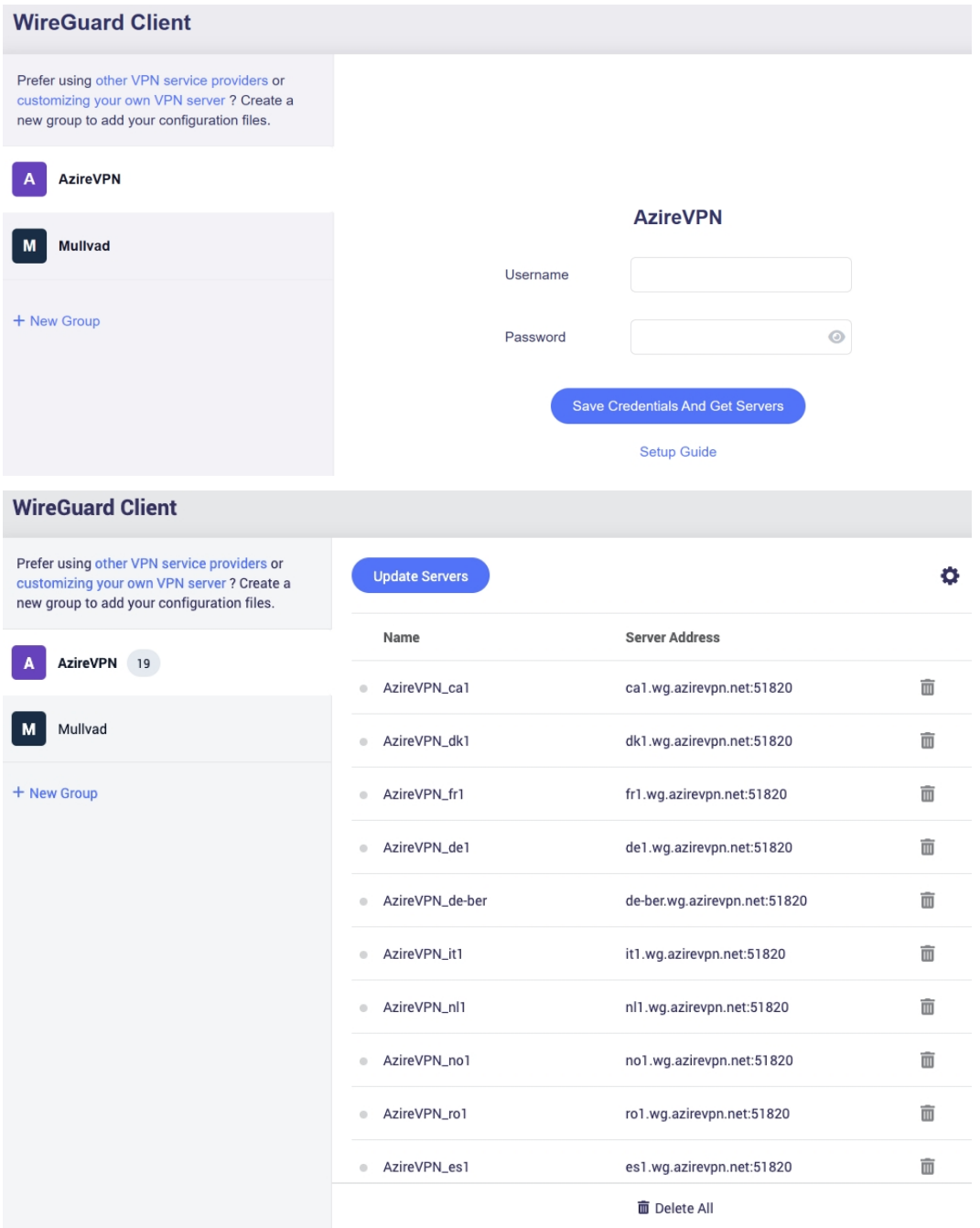
A continuación, sseleccione el proveedor de servicios WireGuard correspondiente a continuación para localizar rápidamente las instrucciones paso a paso.

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

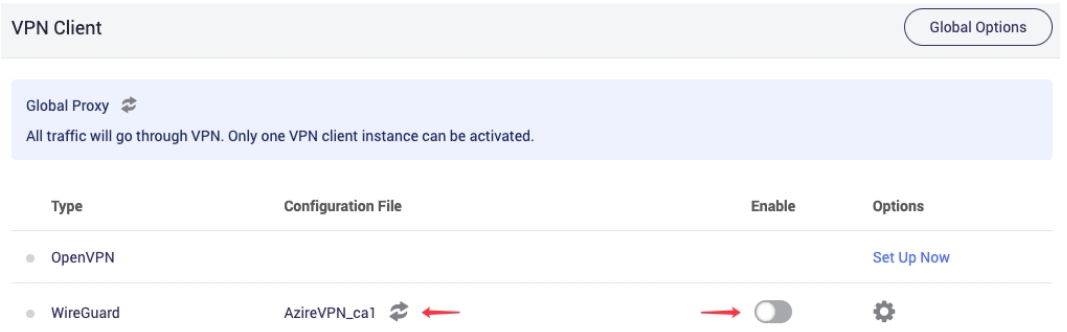
10.2.2 Configurar AzireVPN

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

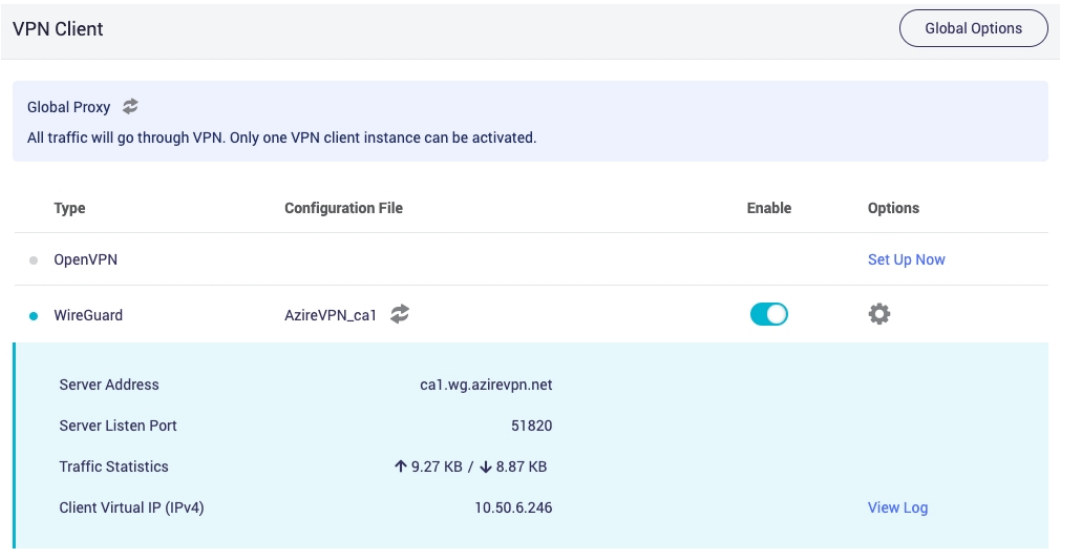
1. Inicie sesiónn en su enrutador’s web admin panel y vaya a **VPN** > **Cliente WireGuard** > **AzireVPN**.
2. Ingrese el nombre de usuario y la contraseña, luego haga clic en **Guardar credenciales y obtener servidores**. Generará archivos de configuración para cada servidor.



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

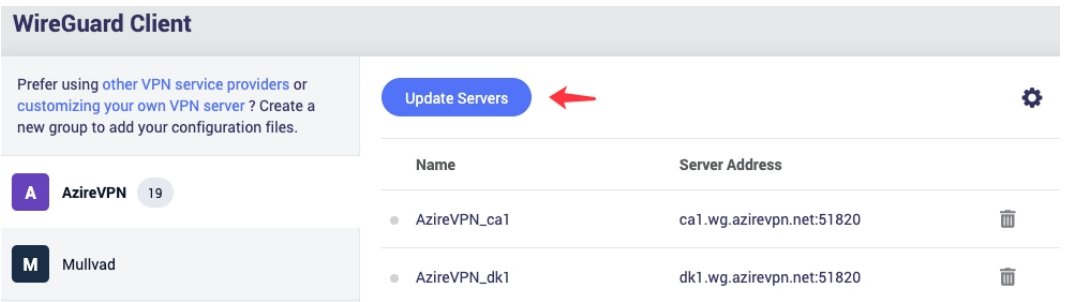


Una vez conectado, debería ver su dirección IP de usuario y la cantidad de bytes enviados/recibidos.



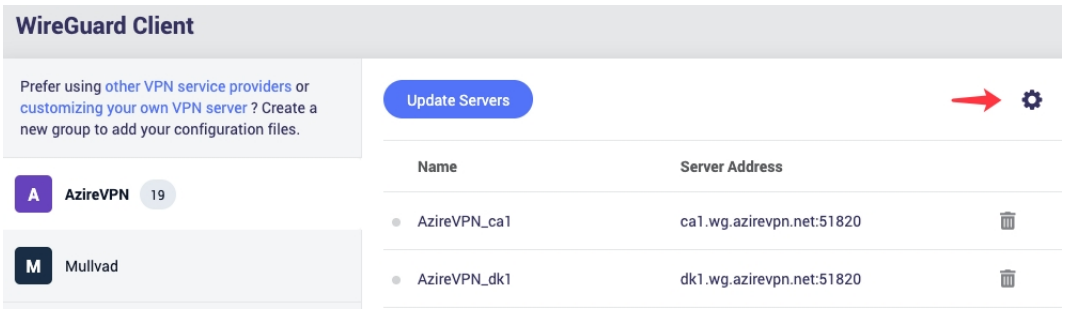
4. Actualizar servidores.

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



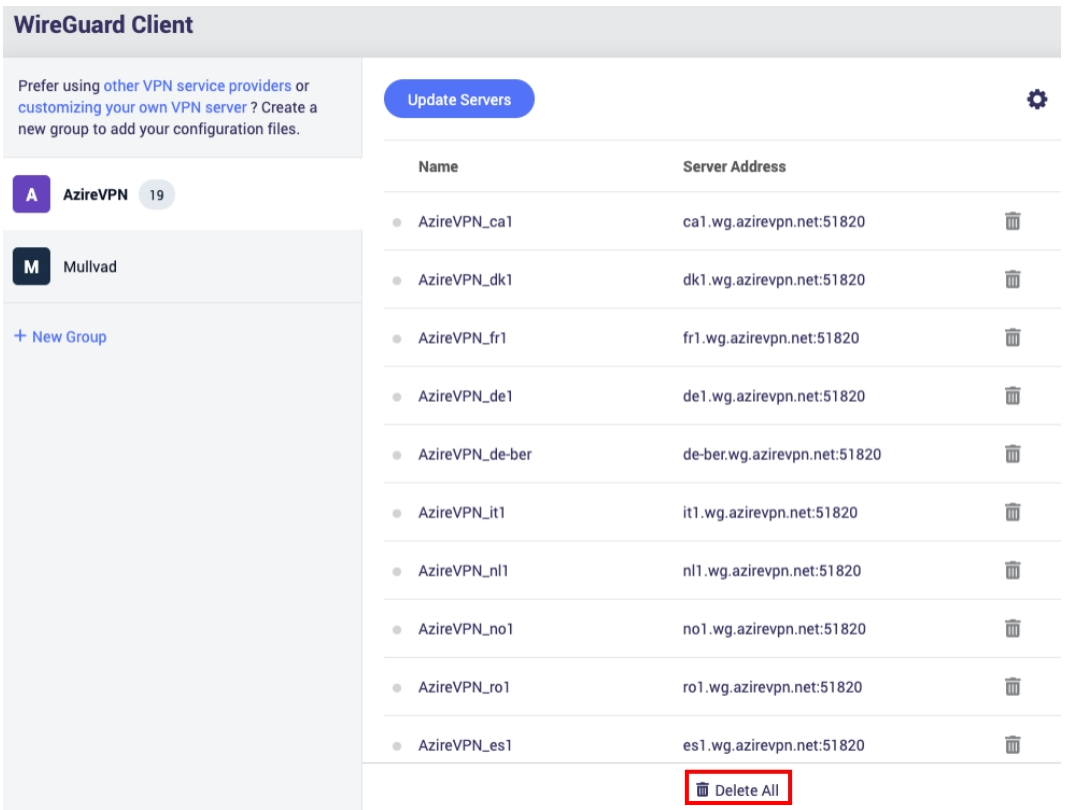
5. Editar credenciales.

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



6. Eliminar todos los archivos.

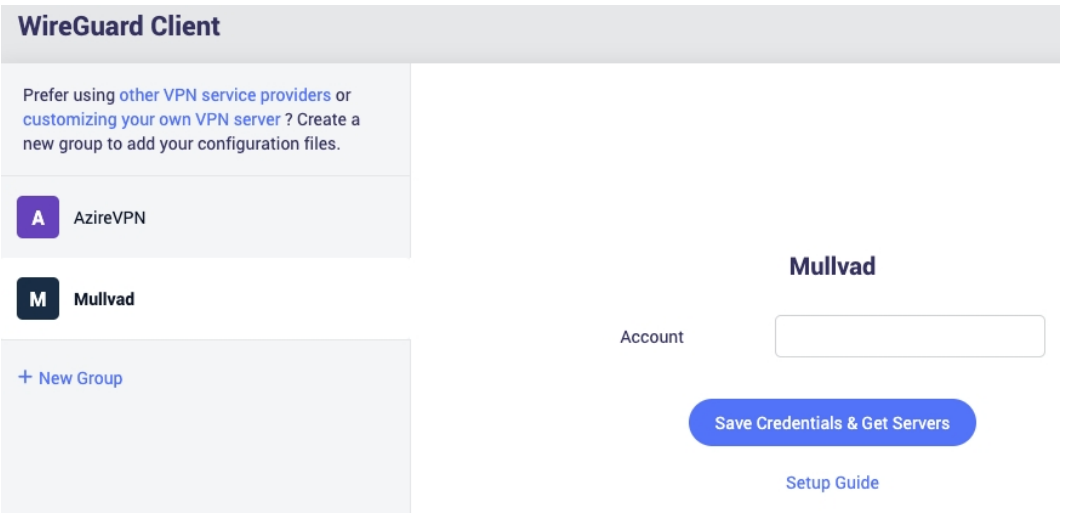
   Puede hacer clic en **Eliminar todo** para eliminar todos los archivos de configuración con un solo clic.



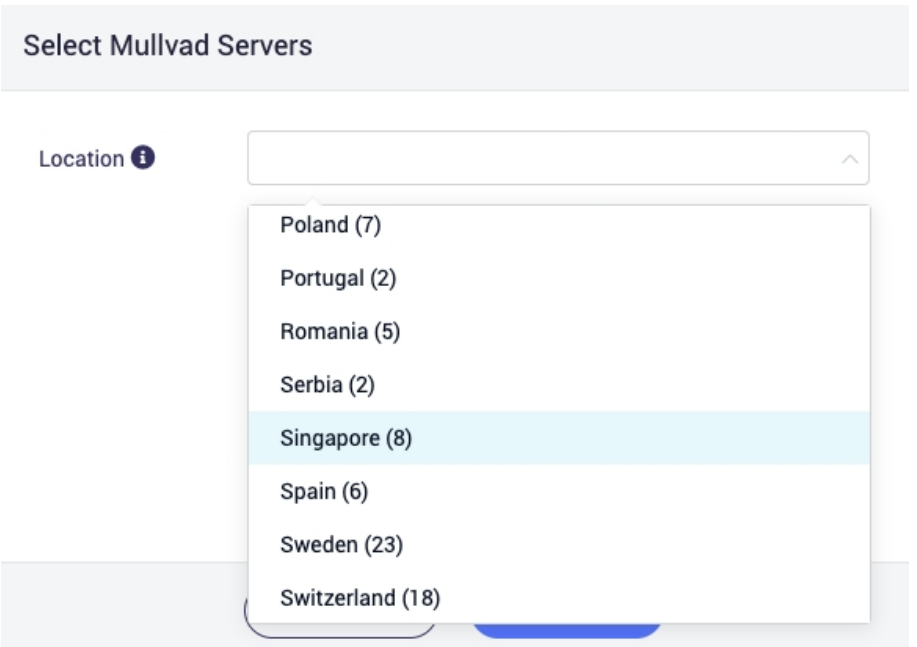
10.2.3 Configurar Mullvad

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

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

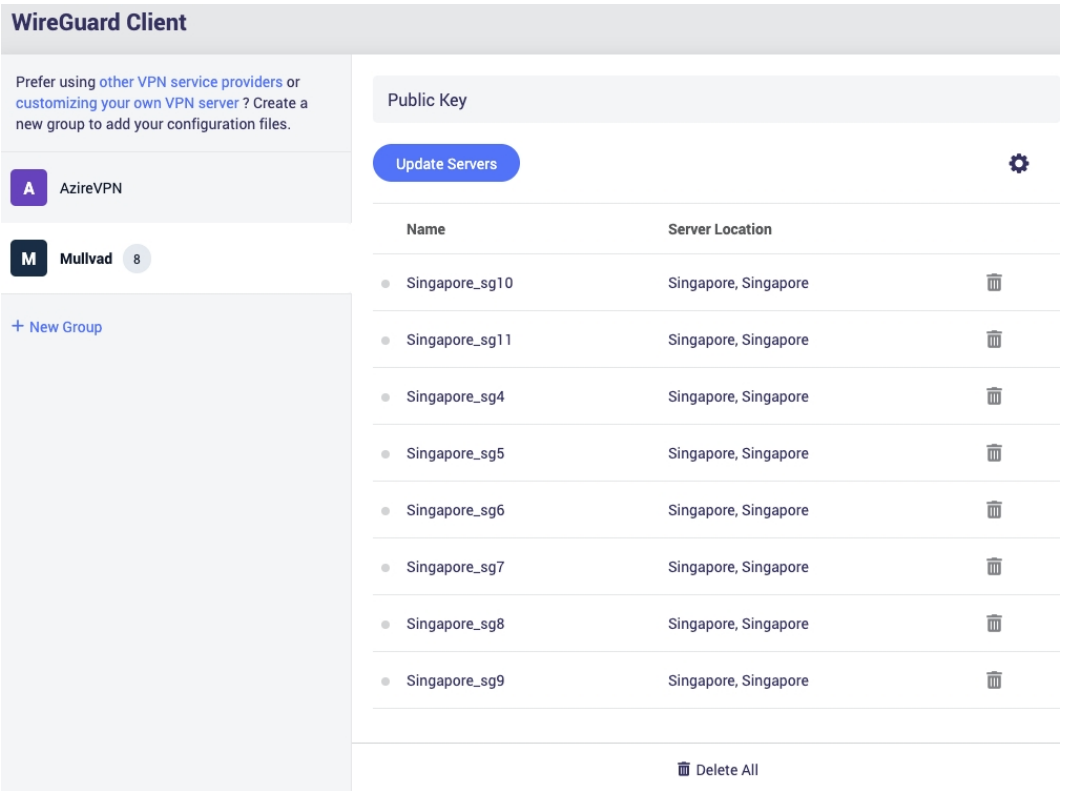


Aparecerá un cuadro de diálogo para seleccionar una ubicación.

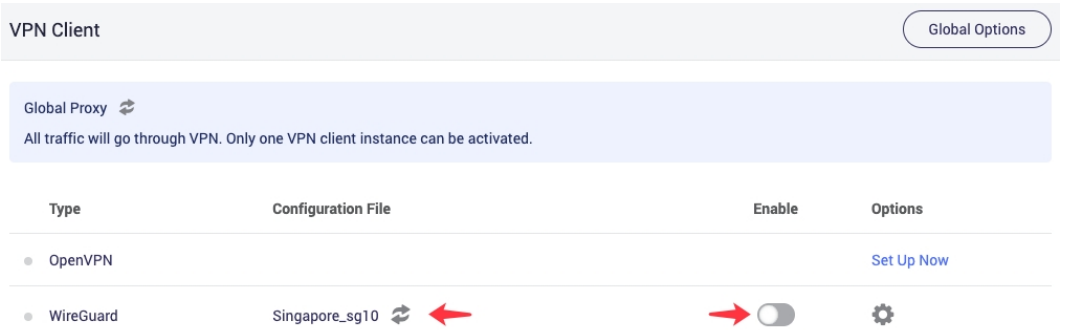


Luego generará los archivos de configuración del servidor de ubicación seleccionado.

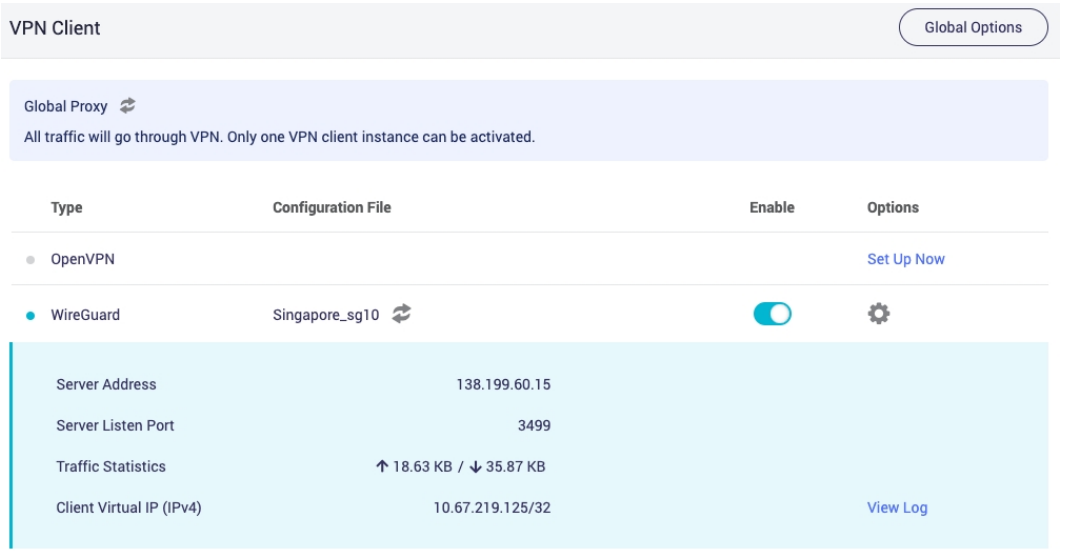
La **clave pública** es la clave pública de WireGuard para enviar al servidor Mullvad. Puede tener hasta cinco claves al mismo tiempoPuedes tener hasta cinco claves al mismo tiempo, y administrar claves WireGuard en su página de cuenta de Mullvad.



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

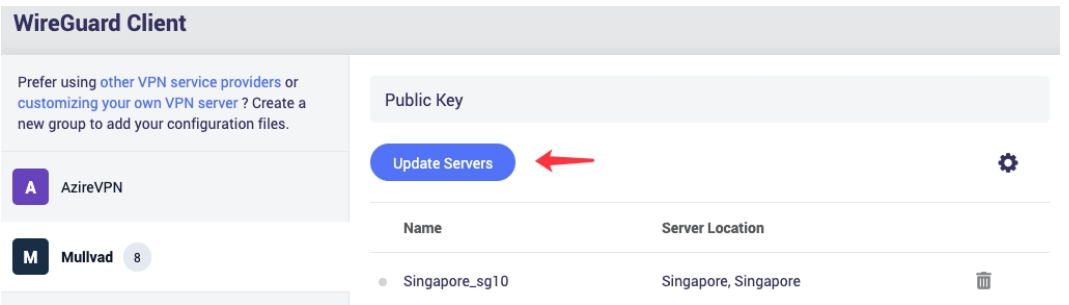


Una vez conectado, debería ver su dirección IP de usuario y la cantidad de bytes enviados/recibidos.



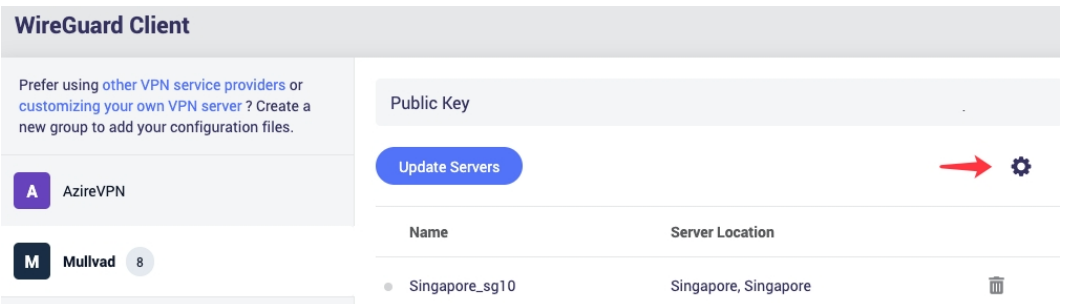
4. Actualizar servidores.

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



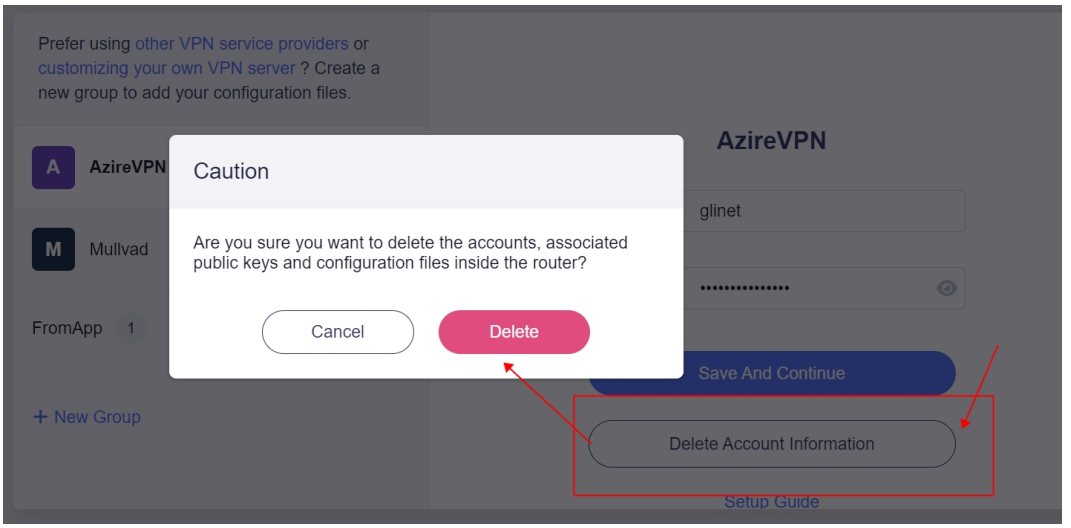
5. Editar credenciales

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



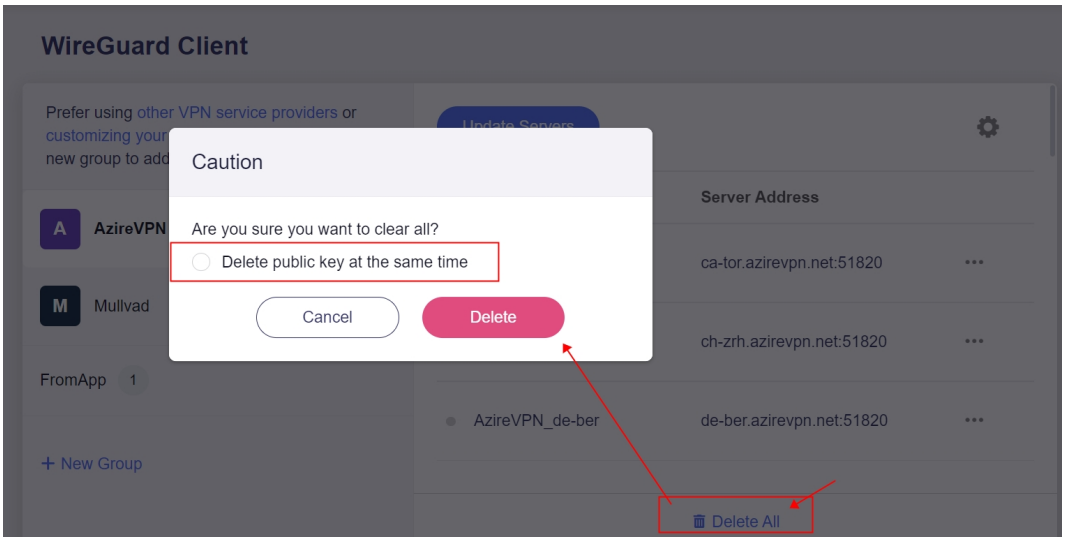
6. Eliminar información de la cuenta

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



7. Eliminar

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

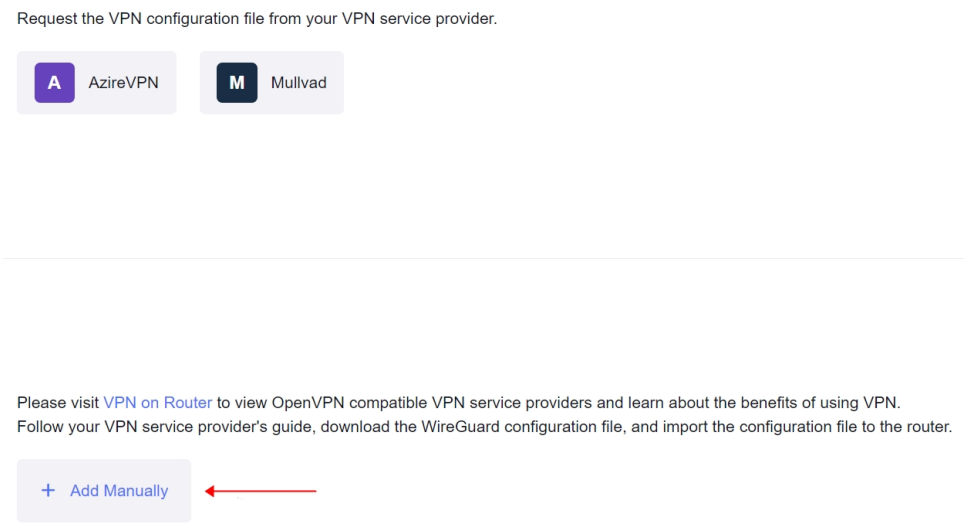


10.2.4 Configurar el cliente WireGuard manualmente (para otros proveedores)

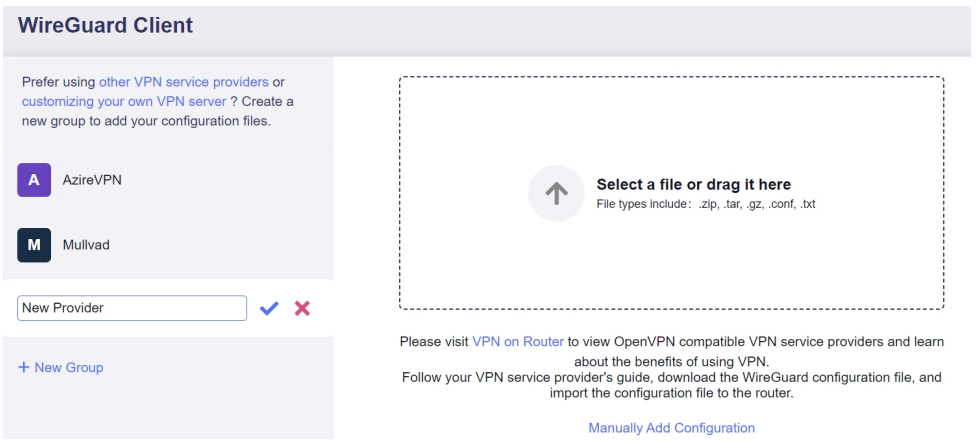
Si su proveedor de servicios WireGuard no está integrado en el panel de administración web, visite primero el sitio web oficial de su proveedor de servicios suscrito para obtener el archivo de configuración. Luego cárguelo en el enrutador para configurar un cliente WireGuard. Si no sabes cómo descargar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

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

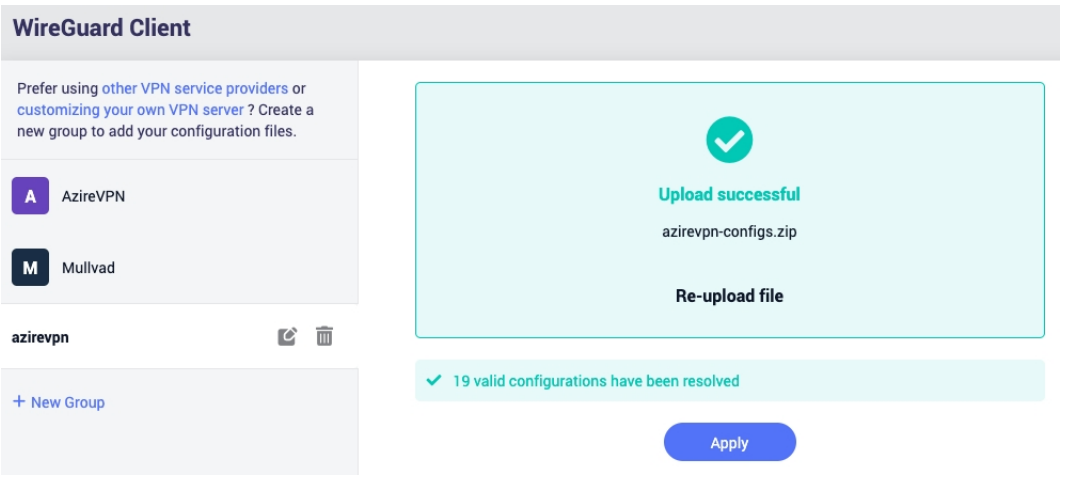
1. Iniciar sesiónn a su enrutador's web admin panel y navegue hasta **VPN** > **WireGuard Client** > **Agregar manualmente**.



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

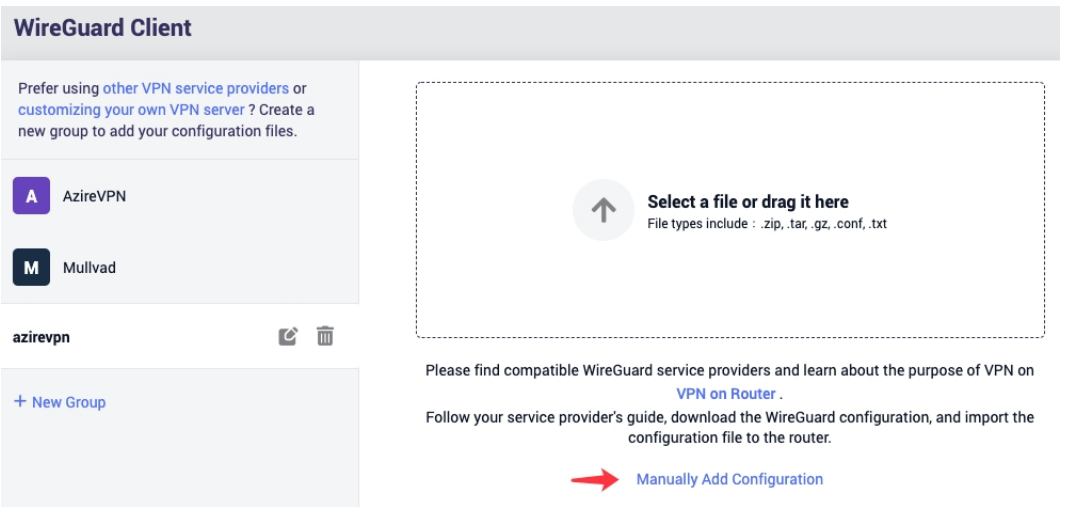


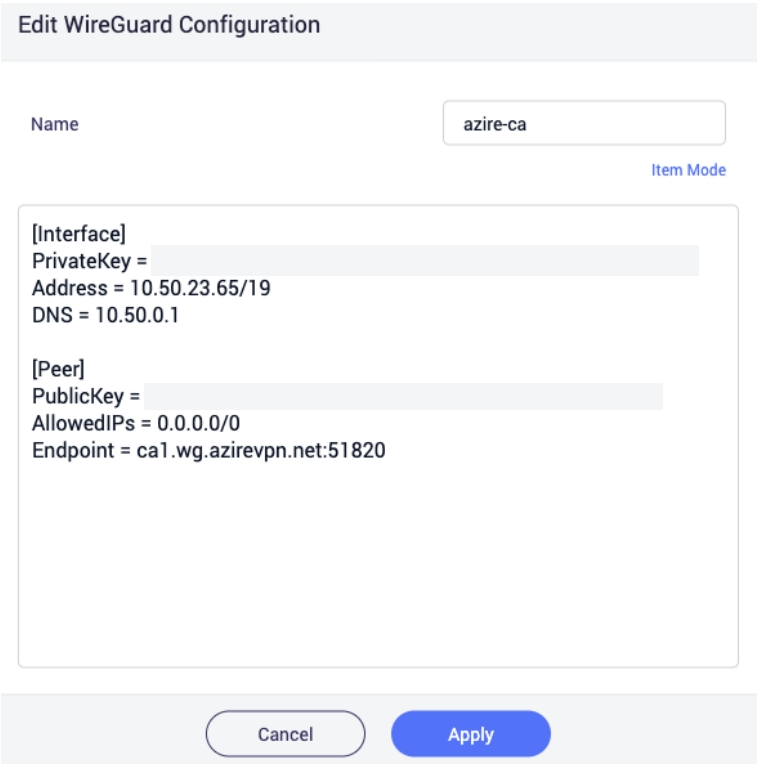
3. Chaz clic el área de carga para cargar su archivo de configuración de WireGuard (formatos admitidos: zip, tar, gz, conf, txt) y haga clic en **Aplicar**.



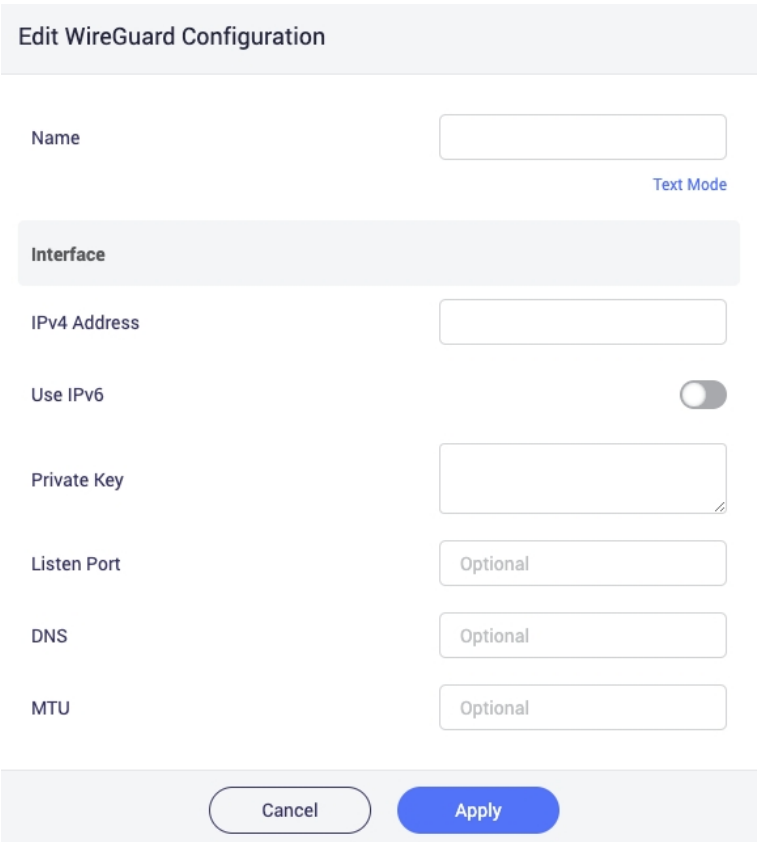
Si carga un archivo comprimido que contiene varios archivos de configuración, se descomprimirá automáticamente.

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

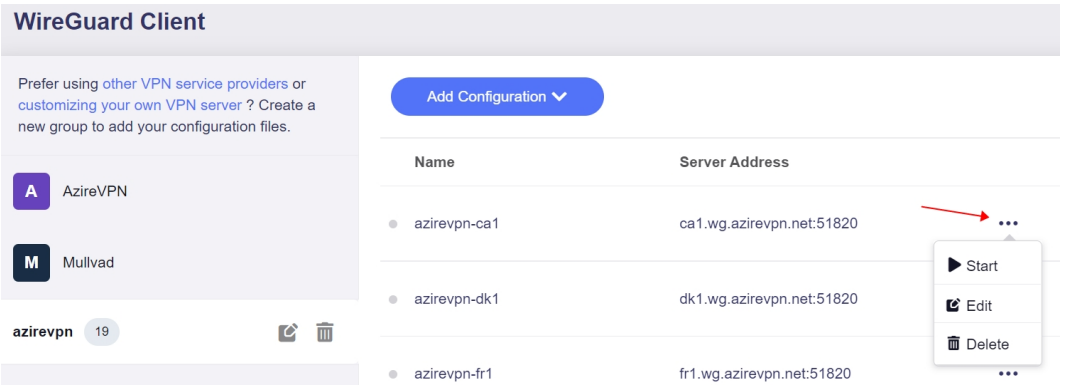




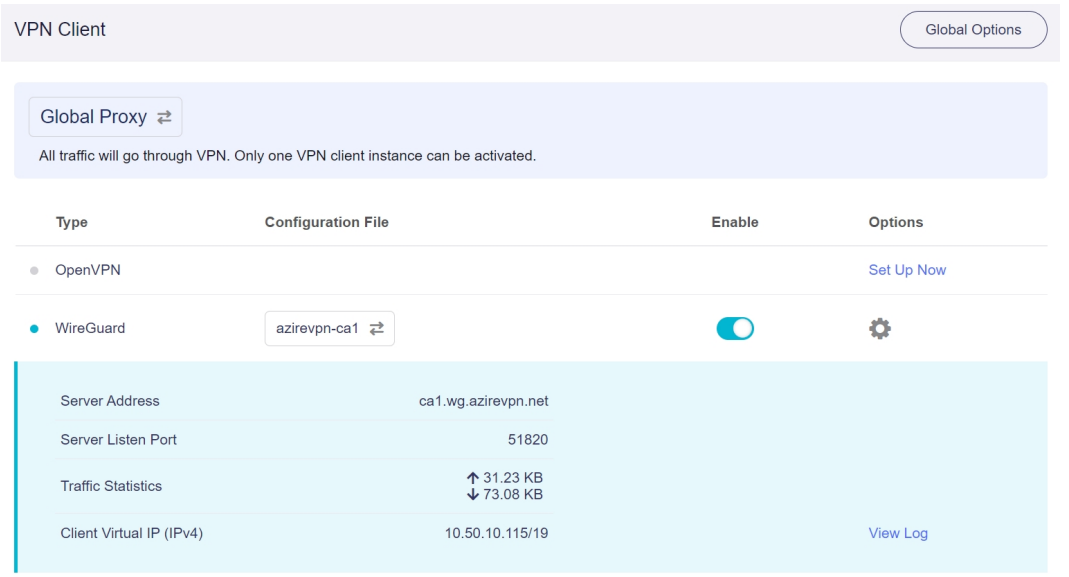
Si desea verificar cada elemento, puede cambiar al modo Elemento y verificar la configuraciónuración detalles, luegoluego haga clic en **Aplicar**.



4. Haga clic en los 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 conexión VPN en **Panel de VPN**.



Capítulo 11

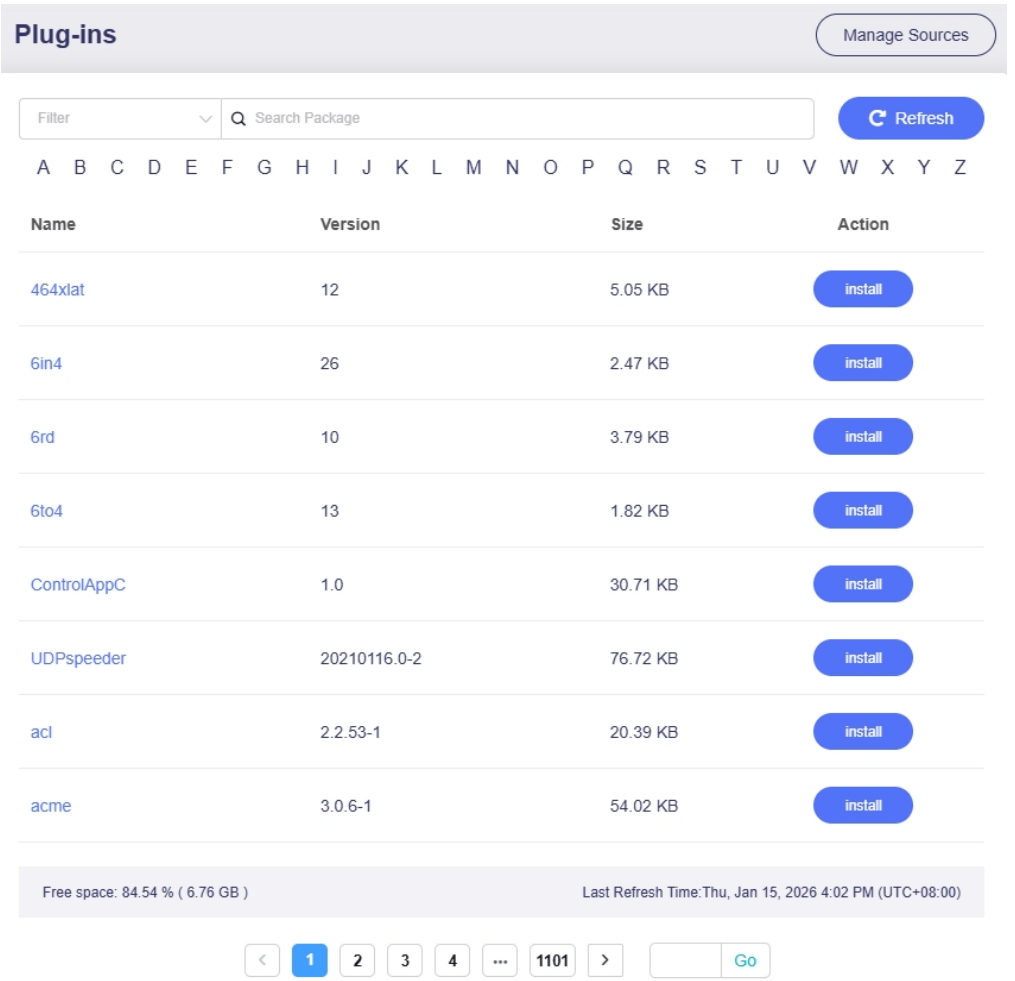
Aplicaciones

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

11.1 Complementos

La página Complementos le permite administrar paquetes OpenWrt.

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



Nota:

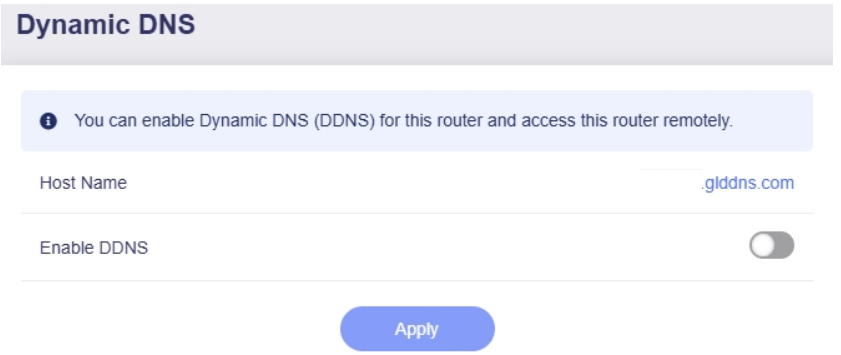
1. No se recomienda actualizar los complementos preinstalados en el firmware oficial de GL.iNet, como nginx, etc.
2. Los complementos de terceros instalados manualmente por los usuarios se pueden actualizar; sin embargo, GL.iNet no es responsable de ningún problema de seguridad causado por complementos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

11.2 DNS dinámico

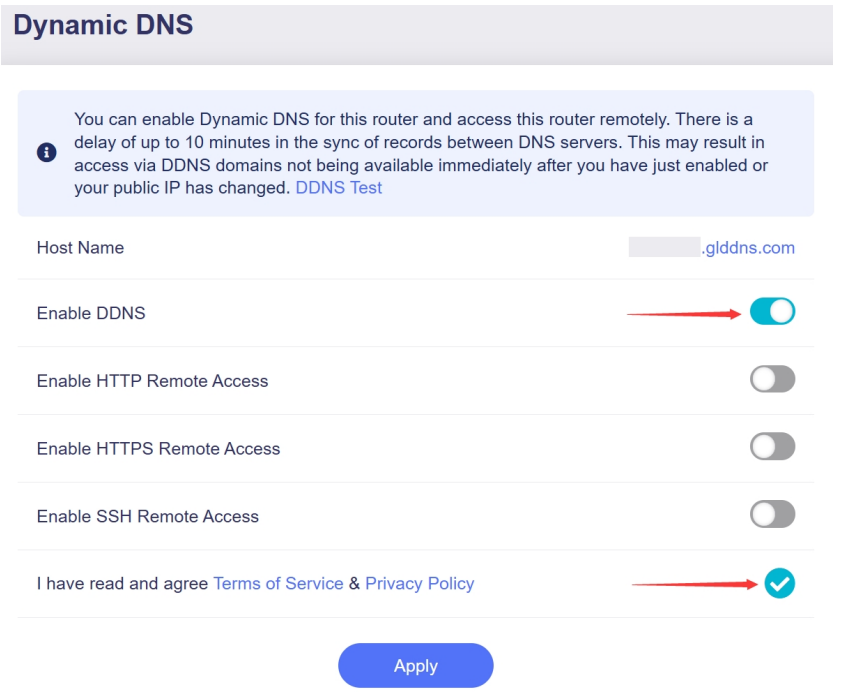
Dinámico El servicio de nombres de dominio (DDNS o DNS dinámico) es un servicio que se utiliza para asignar un nombre de dominio a la dirección IP dinámica de un dispositivo de red. Con DNS dinámico, puede acceder a su enrutador de forma remota. Se requiere una dirección IP pública para esta funcionalidad.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

11.2.1 Habilitar DDNS

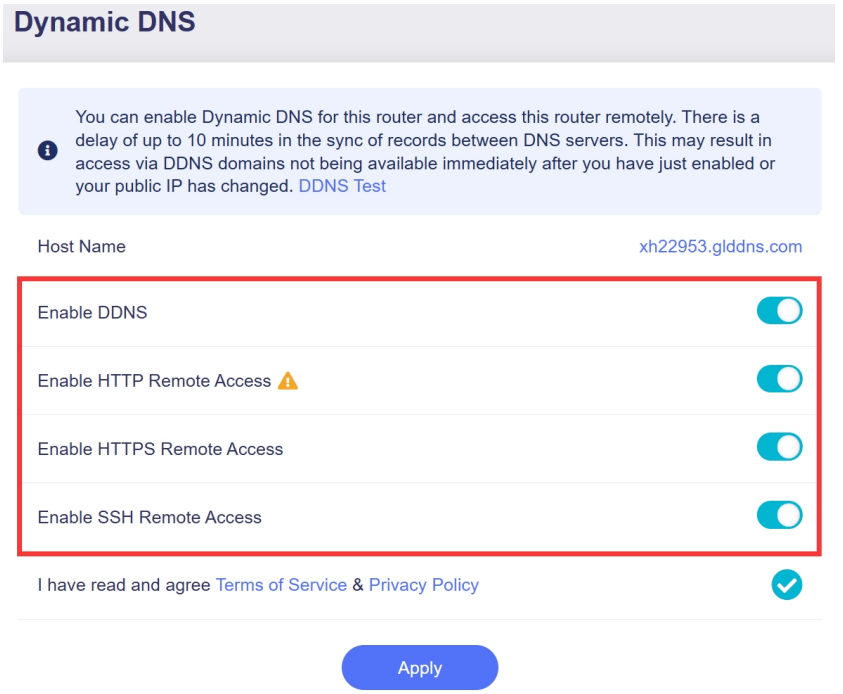
1. Inicie sesión en su enrutador's web admin panel, navegue hasta **APLICACIONES** > **DNS dinámico**, la página se muestra a continuación.



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



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



Nota:

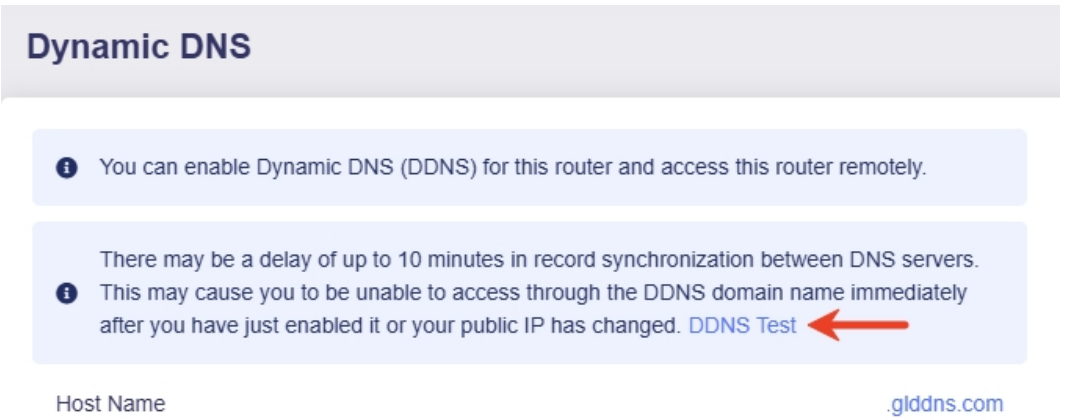
1. Puede haber un retraso de hasta 10 minutos en la sincronización de registros entre servidores DNS. Esto puede impedirle acceder a través del nombre de dominio DDNS inmediatamente después de habilitarlo o cuando cambie su IP pública.
2. Si habilita DDNS y el cliente VPN al mismo tiempo, enseguro de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

11.2.2 Comprobar si DDNS funciona

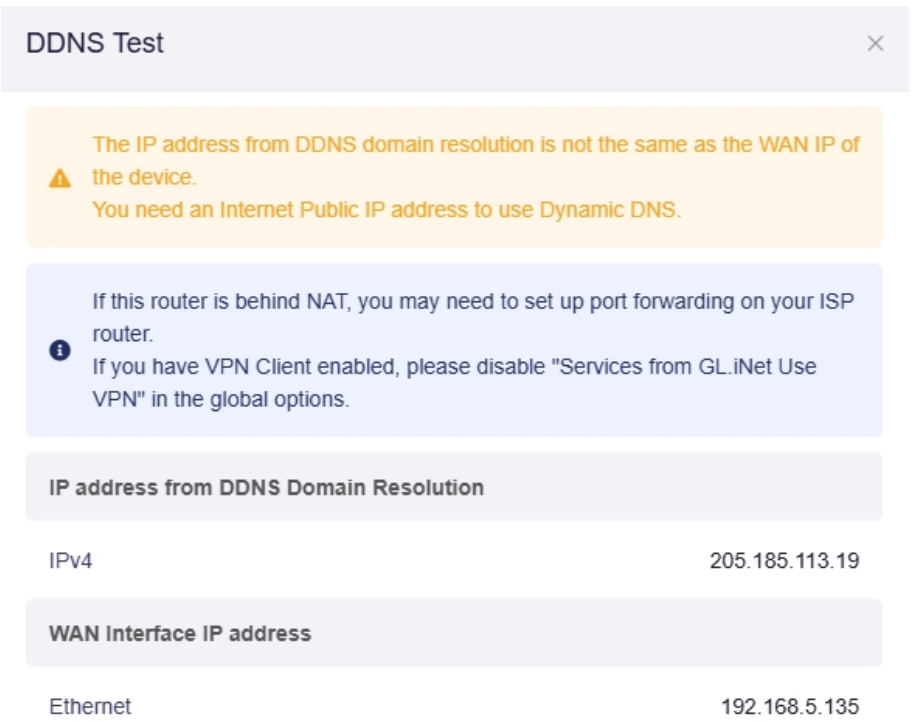
Puede comprobar si DDNS funciona utilizando la herramienta de prueba de DDNS o manualmente mediante comandos.

Método 1. Utilícese herramienta de prueba DDNS

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



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



Método 2. Usar comandos

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



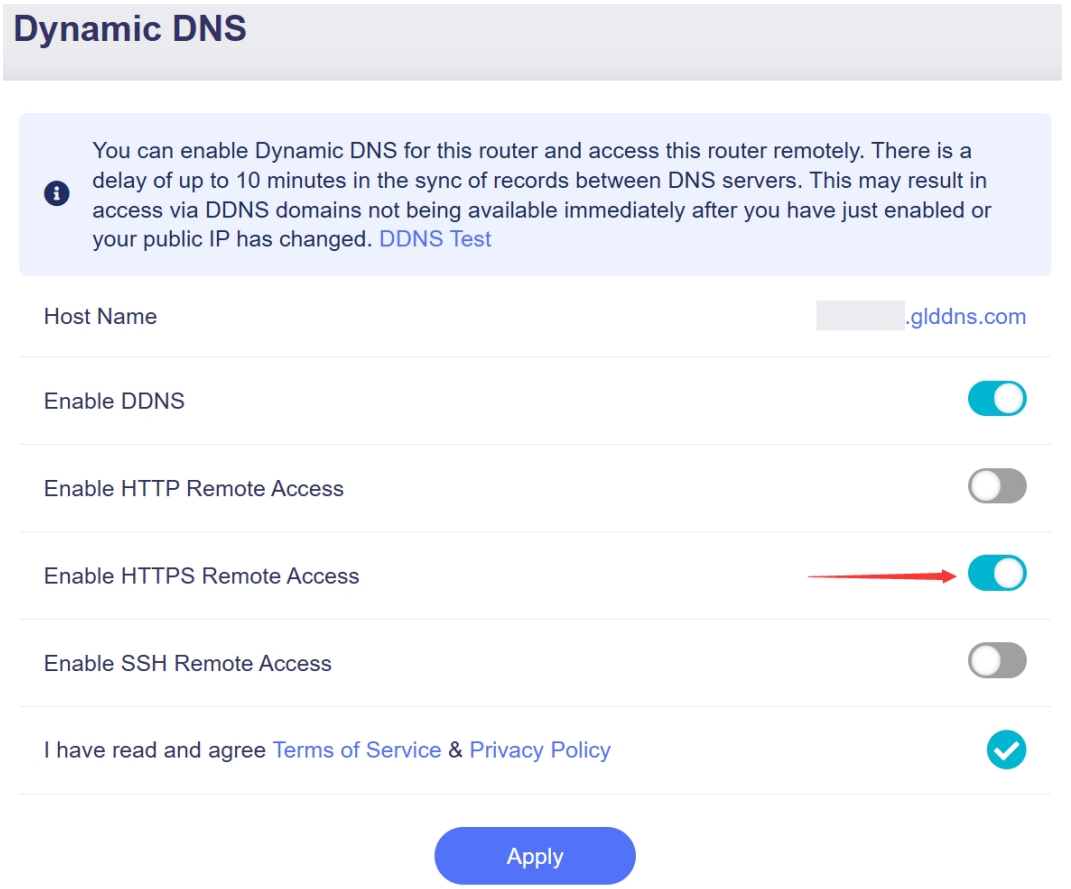
   - Reemplazar “xxxxxxx.glddns.com” en la imagen de arriba con su nombre de host.
   - El “8.8.8.8” es el DNS de Google. Úseloo reemplácelo con otrosy luego presione Entrar.
2. Si obtiene una dirección IP pública como “183.178.10.100” en la imagen de arriba, indica que su dominio DDNS se ha asignado correctamente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

11.2.3 Acceso remoto HTTP

Una **Dirección IP pública** es necesario 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 las **Términos de servicios y política de privacidad**, luego haga clic en **Aplicar**.



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

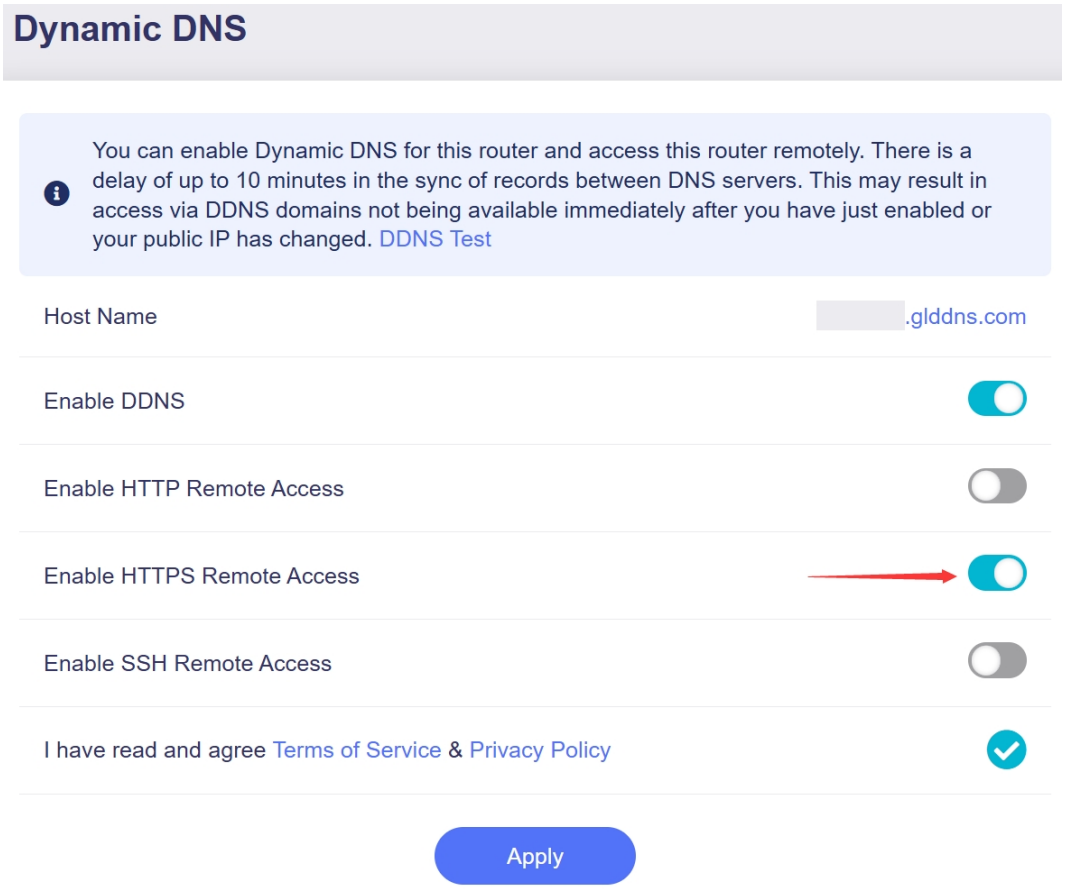
Nota: HTTP es un protocolo no cifrado. Todos los datos transmitidos, incluidas las credenciales de inicio de sesión, se envían en texto sin formato, lo que plantea riesgos de seguridad. Debe utilizar el acceso remoto HTTP con precaución.

11.2.4 Acceso remoto HTTPS

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

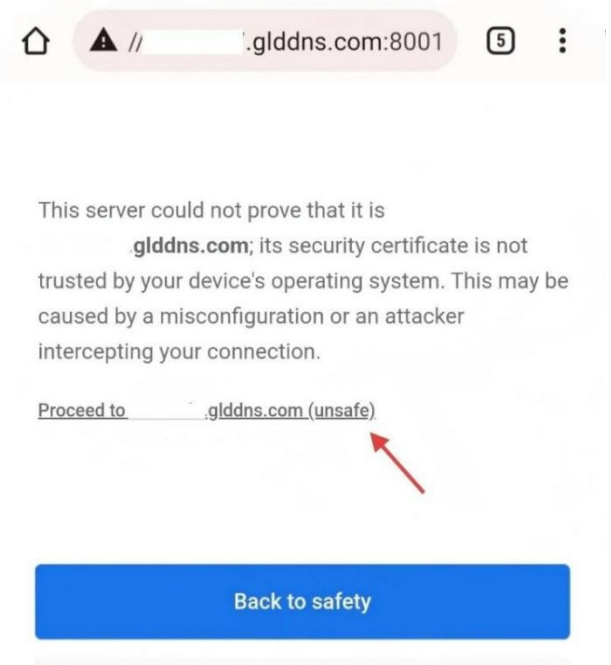
Siga los pasos a continuación para habilitar el acceso remoto HTTPS para su enrutador.

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



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

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



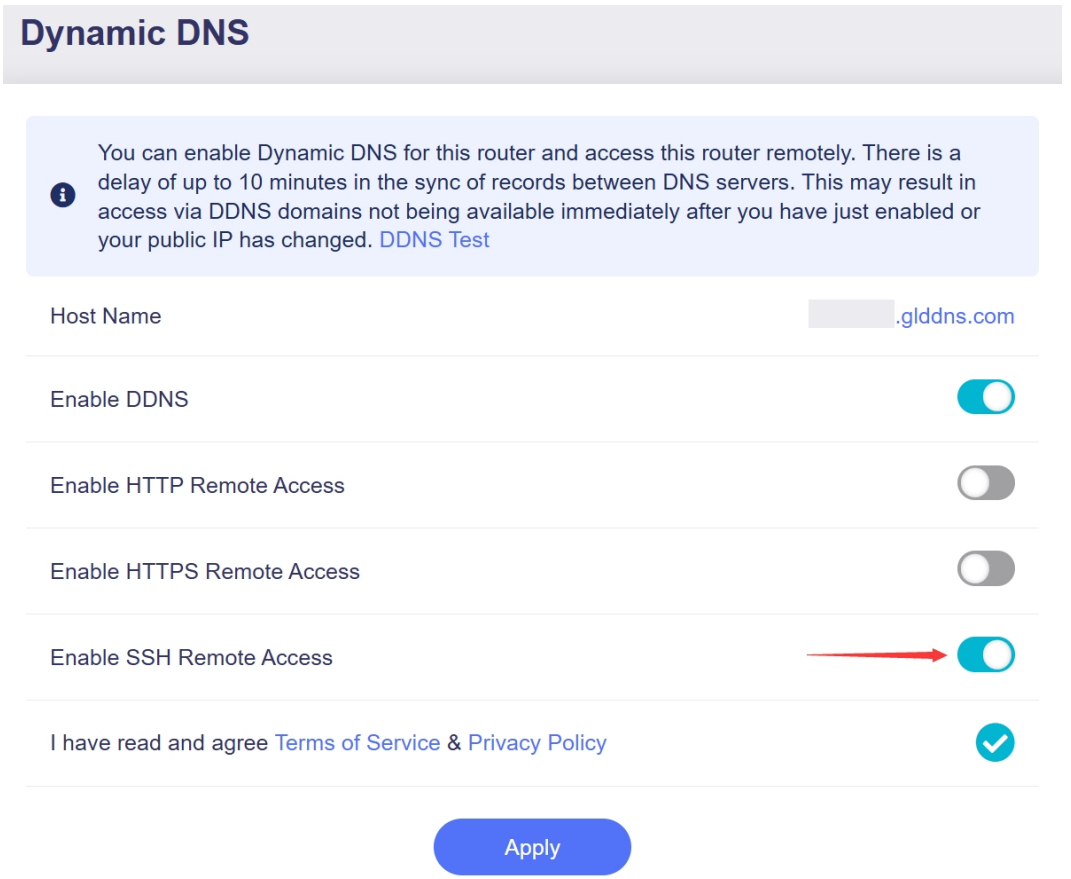
Luego podrá acceder a enrutador’s panel de administración web usando el DDNS host nombre sobre **HTTPS**.

11.2.5 Acceso remoto SSH

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

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

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



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

11.3 GoodCloud

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

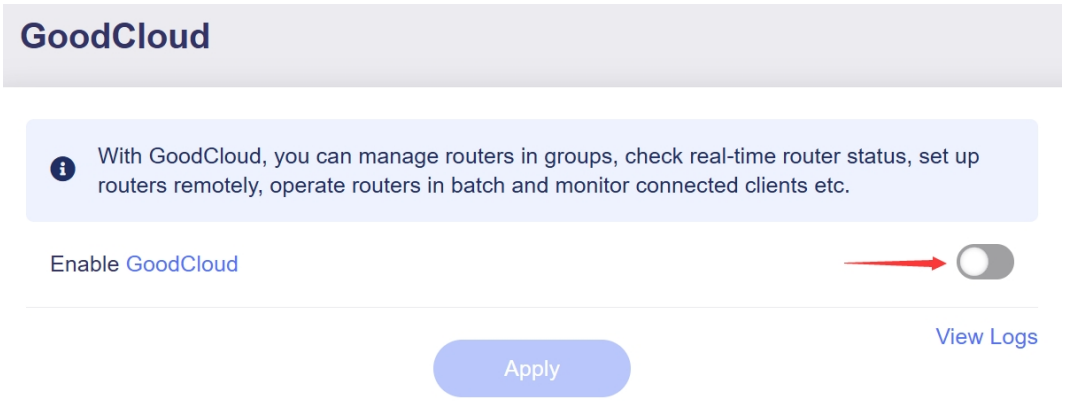
Con GoodCloud, puede:

- Compruebe el estado de su enrutador’en tiempo real
- Madministrar grupos de enrutadores
- Configurar enrutadores de forma remota
- Monitor conectado clientes
- Operar enrutadores en lote
- Establecer Sitio-al-Sitio conexión

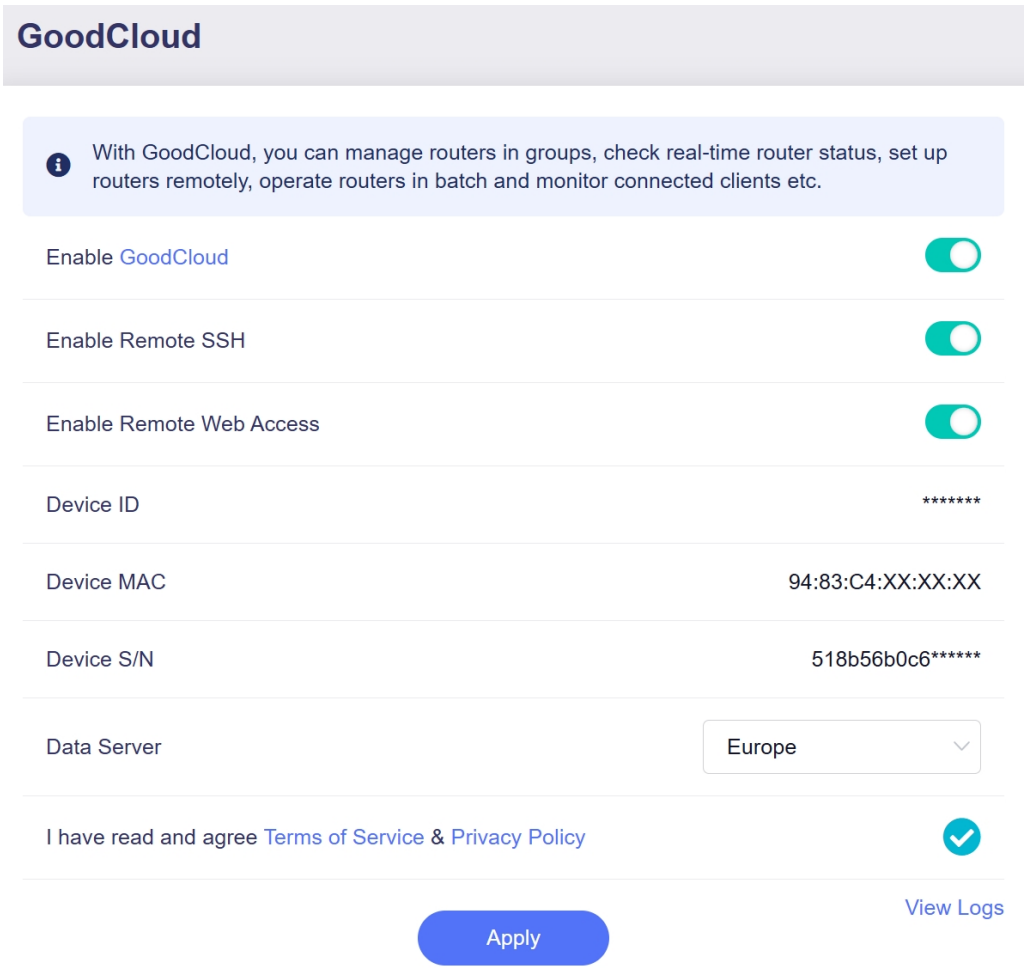
Algunas funciones están disponibles en el Plan Empresarial y en el Plan VAR (Revendedor de Valor Agregado). Consulte aquí para obtener más detalles.

11.3.1 Habilitar GoodCloud

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

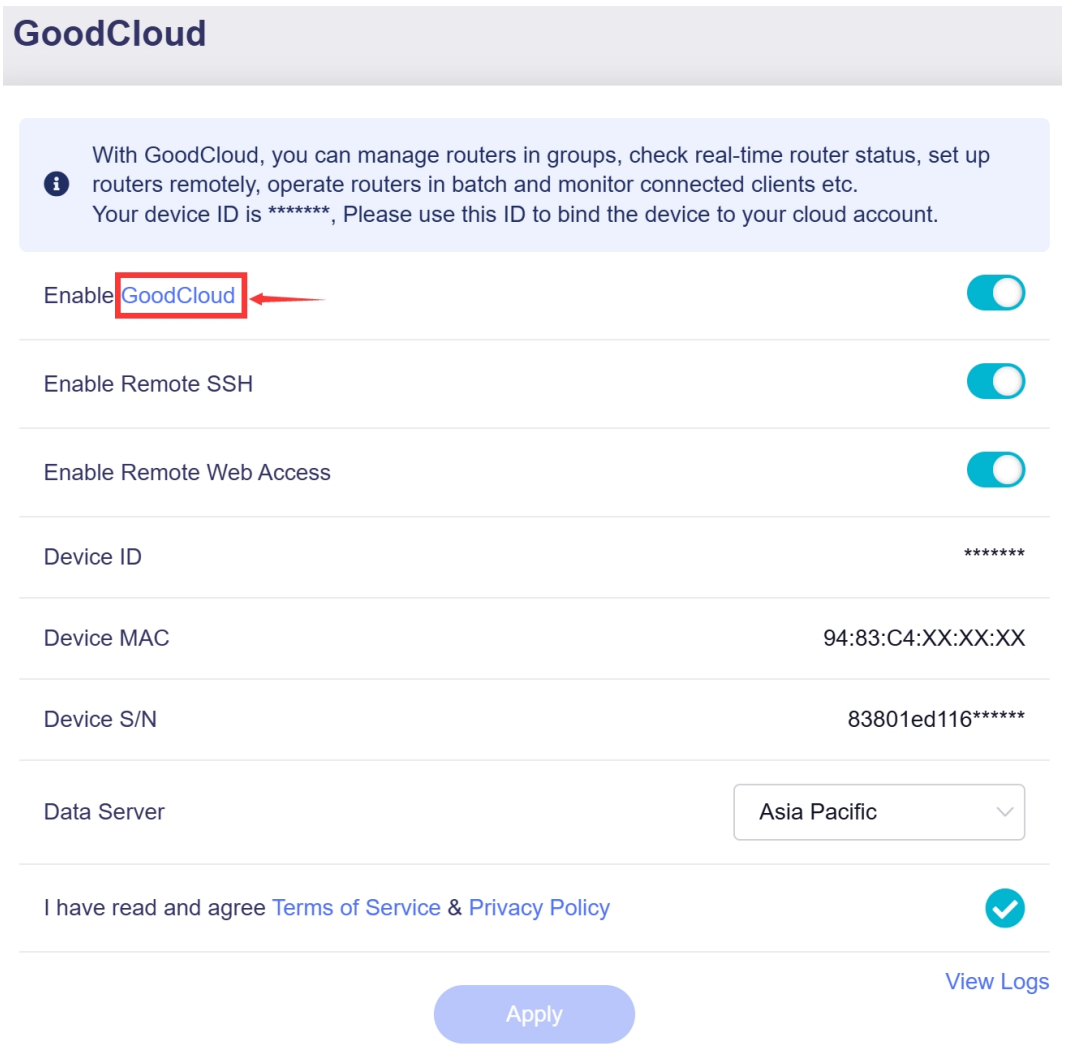


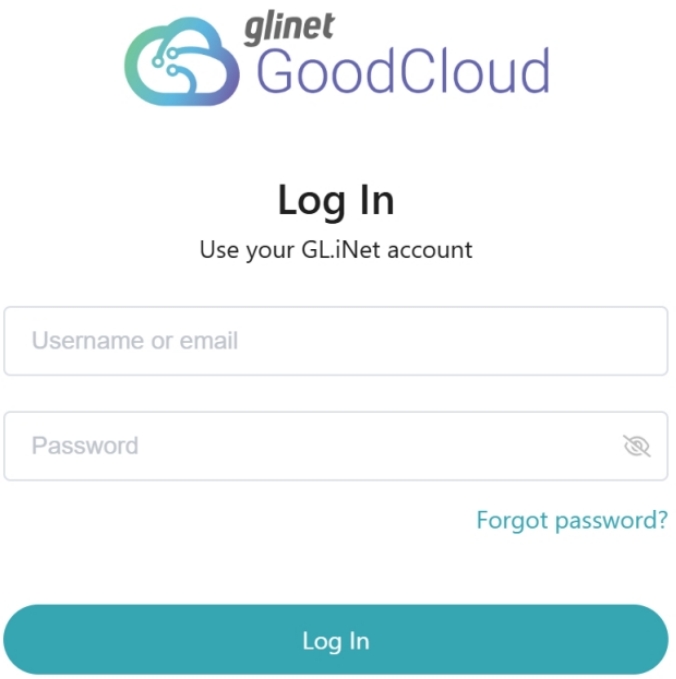
Habilite **Acceso remoto SSH** y **Acceso web remoto** si es necesario, seleccione el servidor más cercano, lea y acepte los **Términos de servicio y política de privacidad**, luego haga clic en **Aplicar**.



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

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

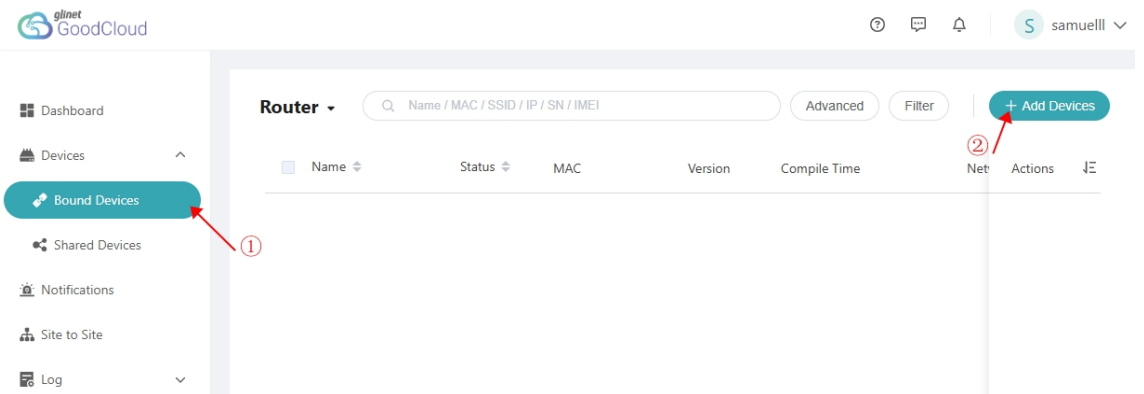




Consejos:

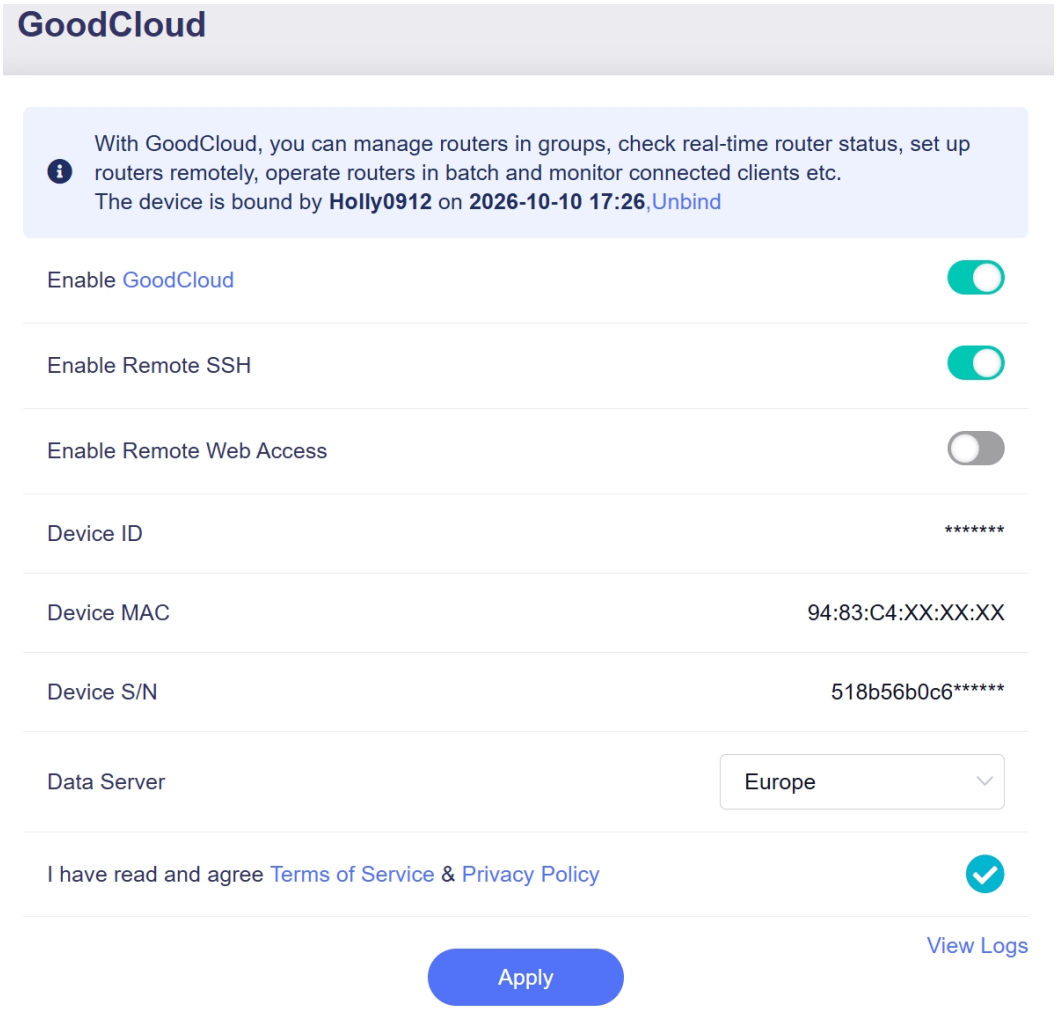
- Los pasos de vinculación de GoodCloud difieren según la versión del firmware.
- Si no recibe el correo electrónico de verificación, revise su carpeta de correo no deseado o inténtelo nuevamente más tarde. Para más ayuda, contáctenos en support@gl-inet.com.

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



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

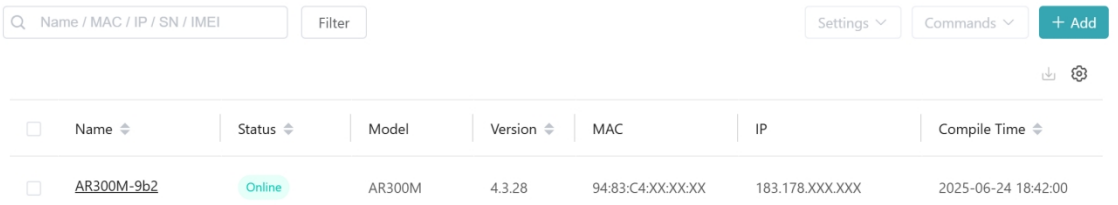
4. Después de la vinculación exitosa, regrese al Panel de administración web del enrutador y navegue hasta **APLICACIONES** > **GoodCloud**. Esta página muestra los detalles de vinculación, incluido el nombre de usuario y la hora de vinculación.



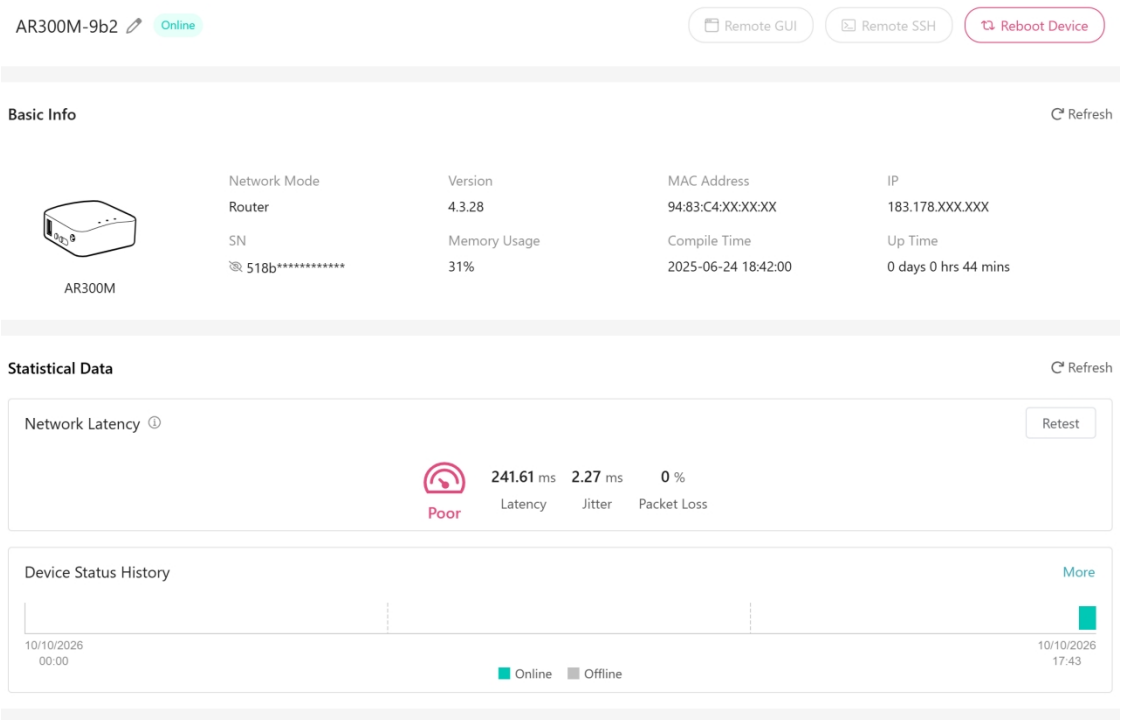
11.3.2 Administrar el enrutador

Consultar los detalles del dispositivo

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

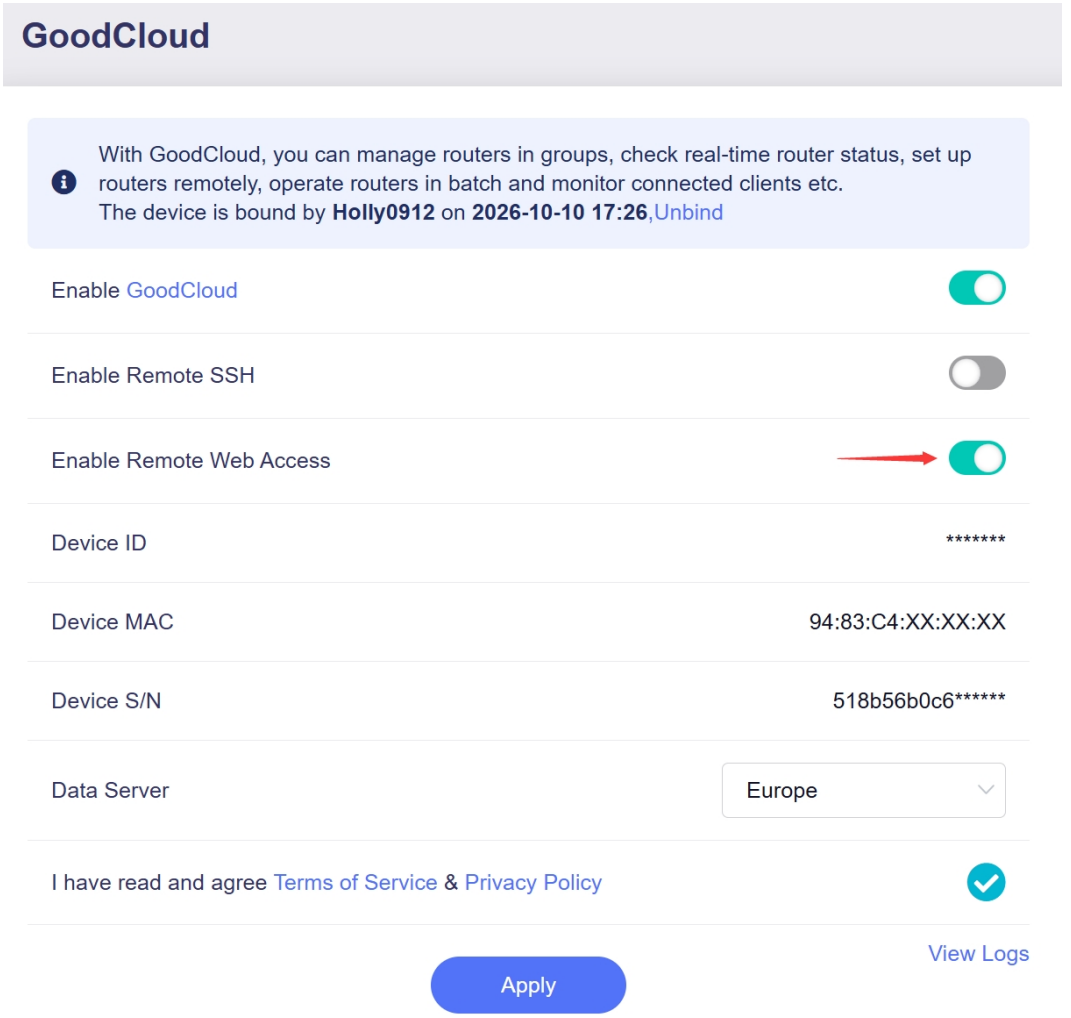


Haga clic en el nombre del dispositivo para ingrese a la página de detalles del dispositivo, que muestras información básica, datos estadísticos, descripción general de la red, lista de clientes y cronograma. También puede realizar operaciones avanzadas, como acceso remotolying al enrutador, y reiniciando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

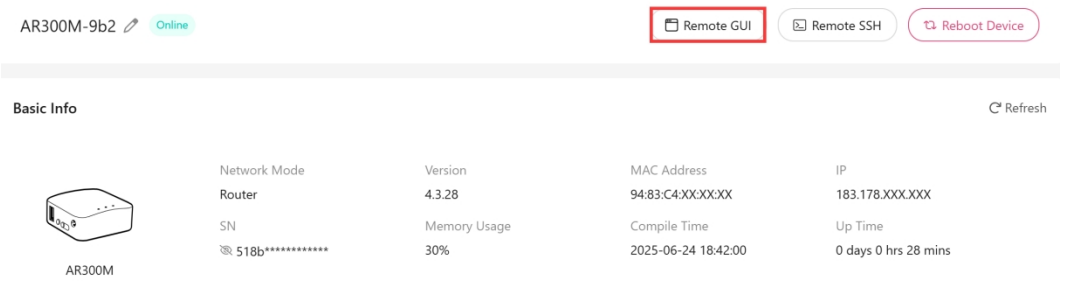


Acceso web remoto

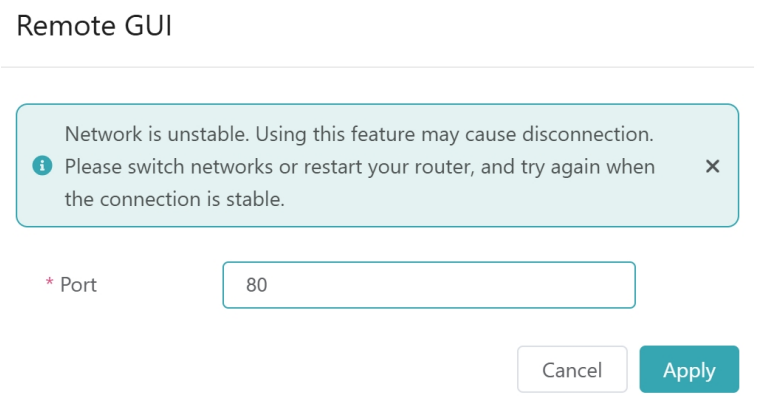
1. Inicie sesión en el panel de administración web del enrutador', navegue hasta **APLICACIONES** > **GoodCloud**, habilite **Acceso web remoto** y luego haga clic en **Aplicar**.



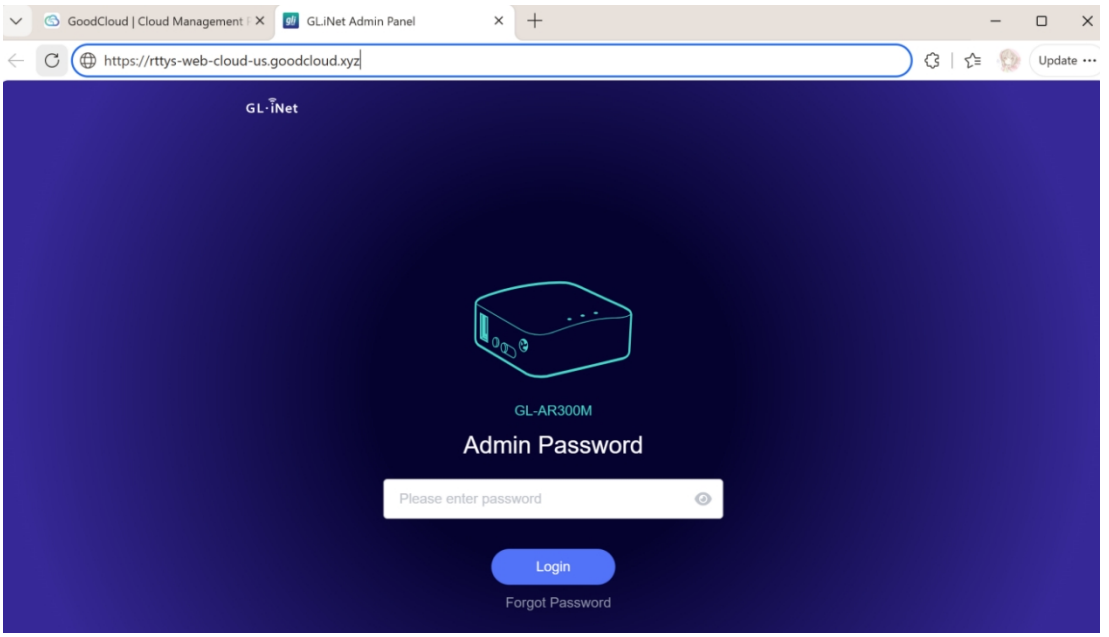
2. Inicie sesión en GoodCloud plataforma y navegue hasta **Dispositivos** > **Dispositivos vinculados**. Haga clic en el dispositivo al que desea acceder e ingresará el página de detalles del dispositivo.
3. En la página de detalles del dispositivo, haga clic en **GUI remota** en la esquina superior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



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

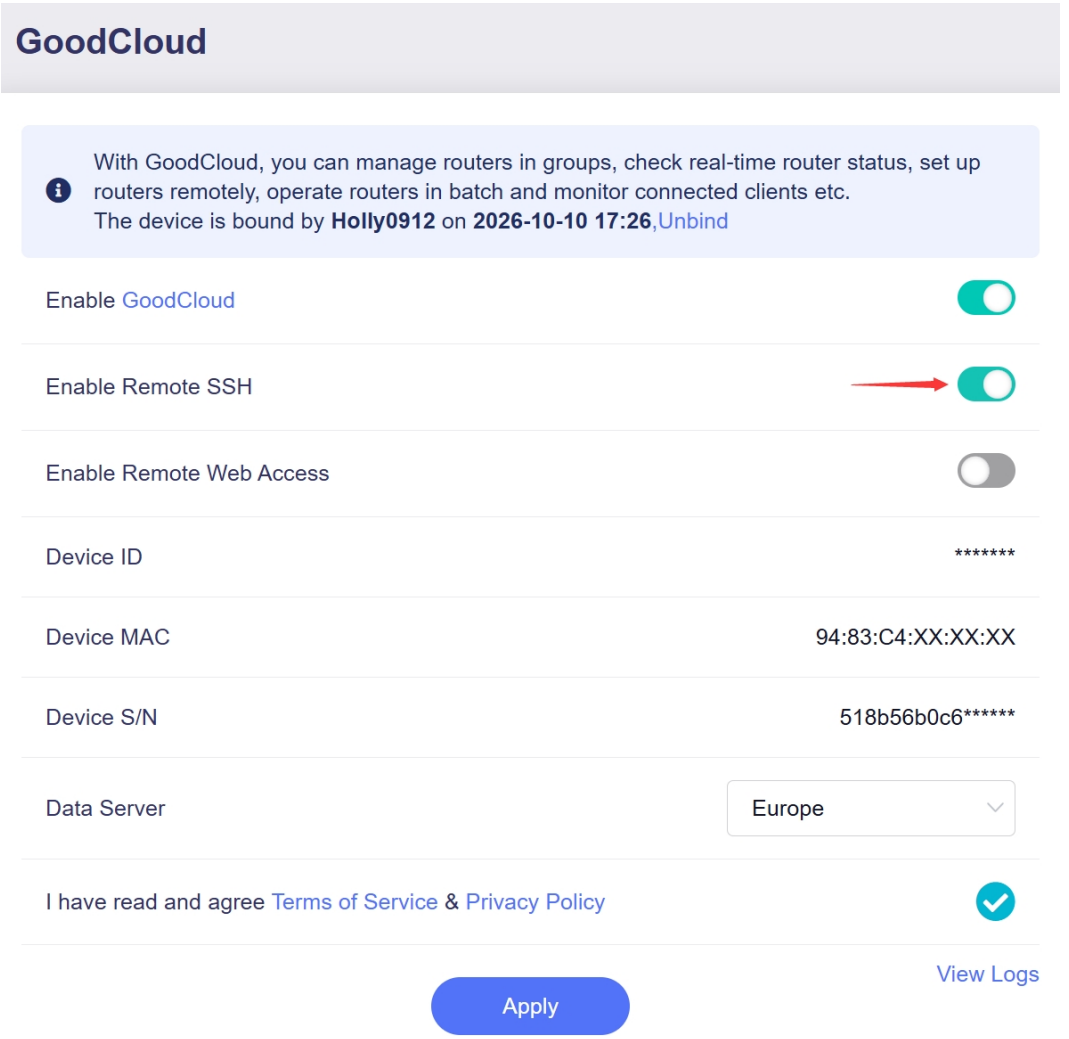


5. Será redirigido a la página de inicio de sesión del enrutador'. Ingrese la contraseña de administrador para acceder de forma remota al panel de administración web del enrutador'.

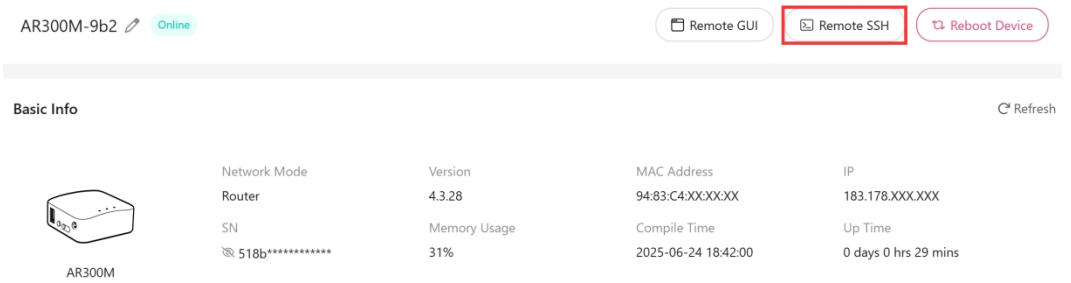


Acceso remoto SSH

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



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



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

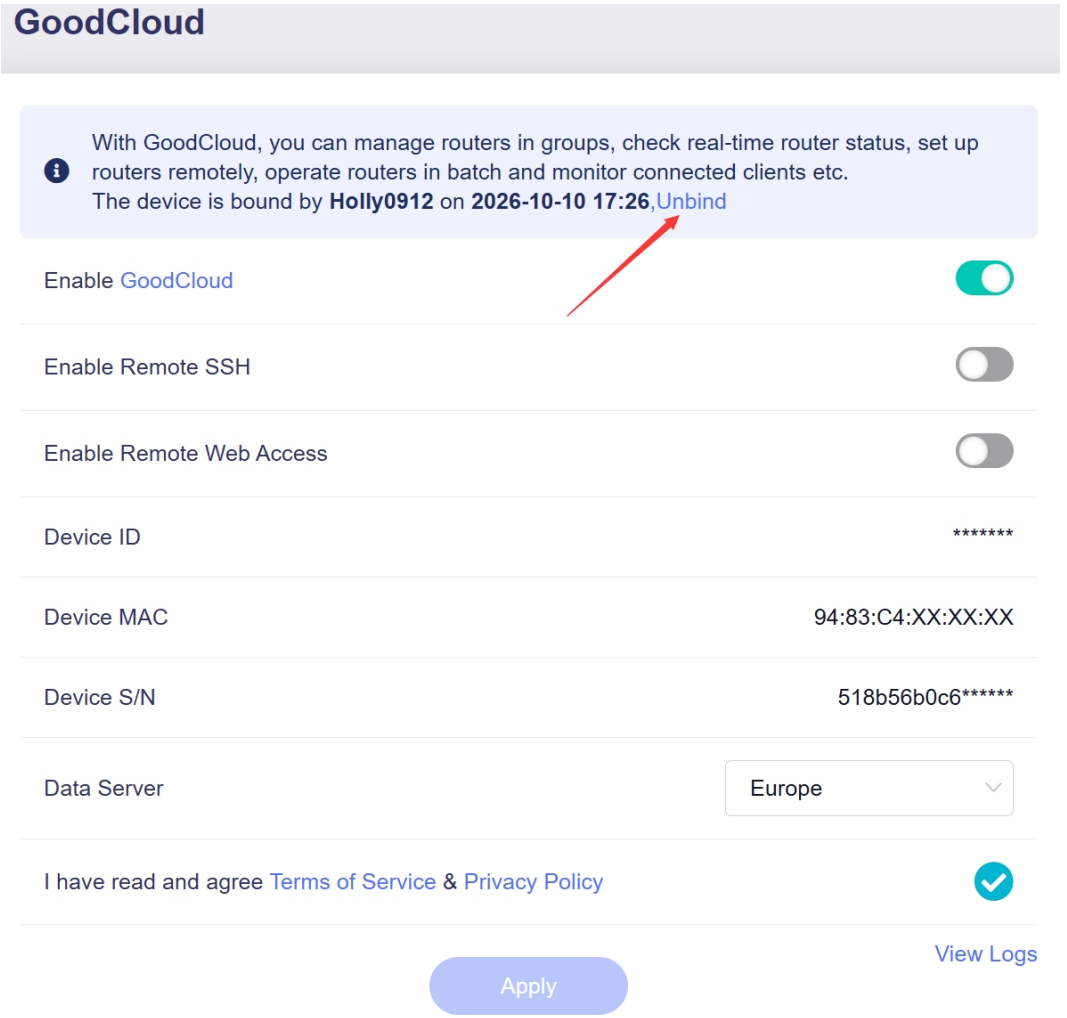
```
GL-AR300M login: root
Password:


BusyBox v1.35.0 (2023-04-09 12:27:46 UTC) built-in shell (ash)

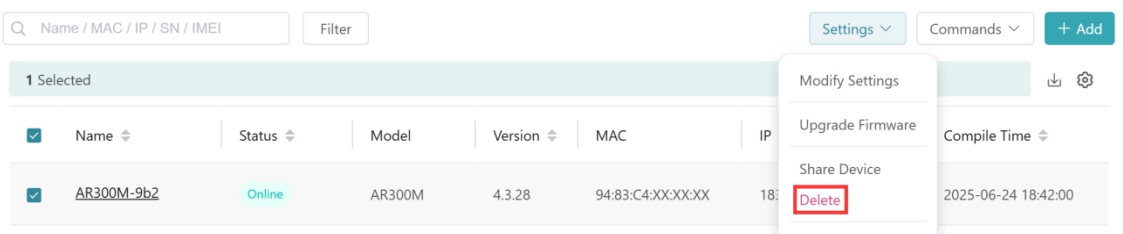
  _______                     ________        __
 |       |.-----.-----.-----.|  |  |  |.----.|  |_
 |   -   ||  _  |  -__|     ||  |  |  ||   _||   _|
 |_______||   __|_____|__|__||________||__|  |____|
          |__| W I R E L E S S   F R E E D O M
 -----------------------------------------------------
 OpenWrt 22.03.4, r20123-38ccc47687
 -----------------------------------------------------
root@GL-AR300M:~#
```

11.3.3 Desvincular el dispositivo

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



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



Capítulo 12

Red

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

12.1 Cortafuegos

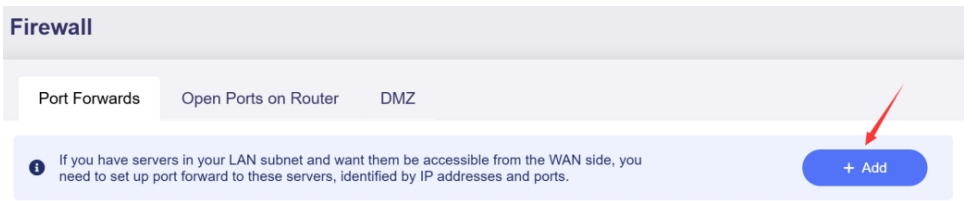
Firewall es una función de red que enruta solicitudes externas a dispositivos específicos en su red local. La página Firewall incluyetres funciones clave: **Reenvío de puertos** (para acceso dirigido a puertos específicos de dispositivos), **Abrir puertos en el enrutador** (para acceder a servicios que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

12.1.1 Reenvío de puertos

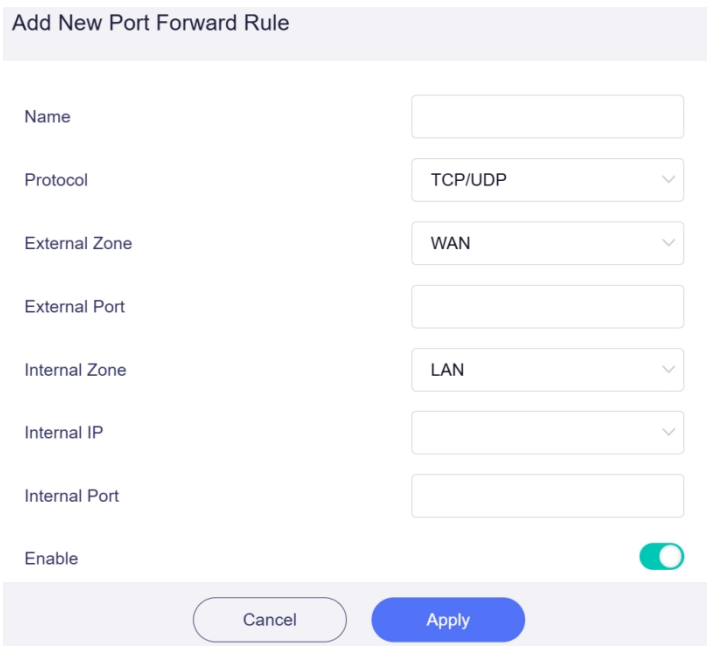
Puerto Reenviars permite que las computadoras remotas se conecten a una computadora o servidor local detrás del firewall LAN (por ejemplo, servidores web, servidores FTP).

Si necesitaconfigurar el puerto adelantes, 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 click **Agregar**.



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

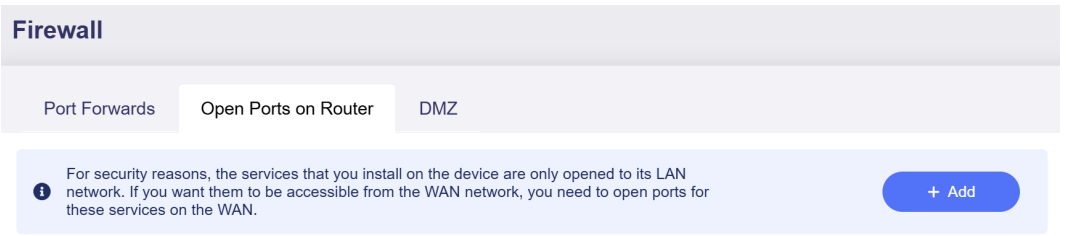


- **Nombre**: el nombre de la regla que puede especificar el usuario.
- **Protocolo**: el protocolo utilizado. Puede elegir TCP, UDP o TCP y UDP.
- **Zona externa**: las opciones disponibles son WAN, Cliente WireGuard, Servidor WireGuard, Cliente OpenVPN, Servidor OpenVPN, LAN e Invitado.
- **Puerto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

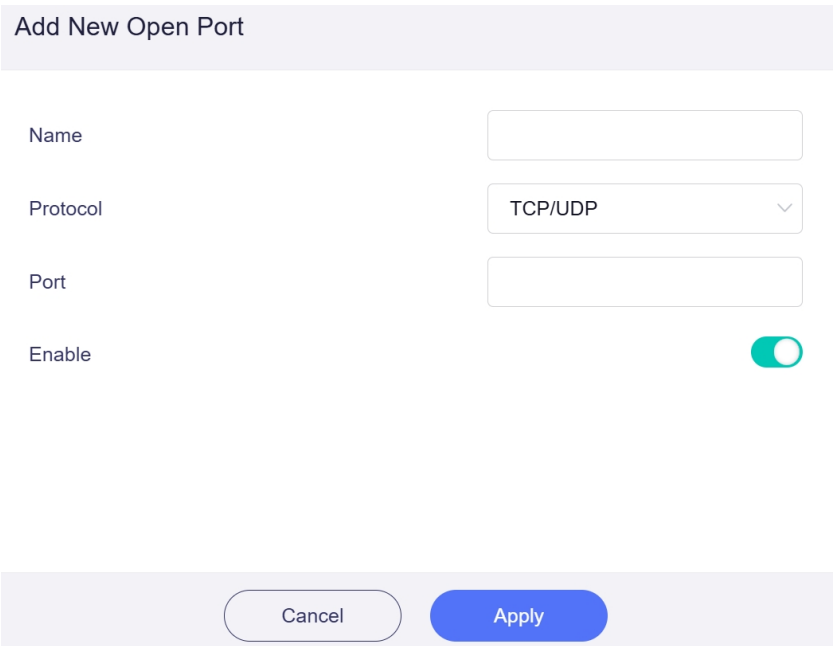
12.1.2 Abrir puertos en el enrutador

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

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



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



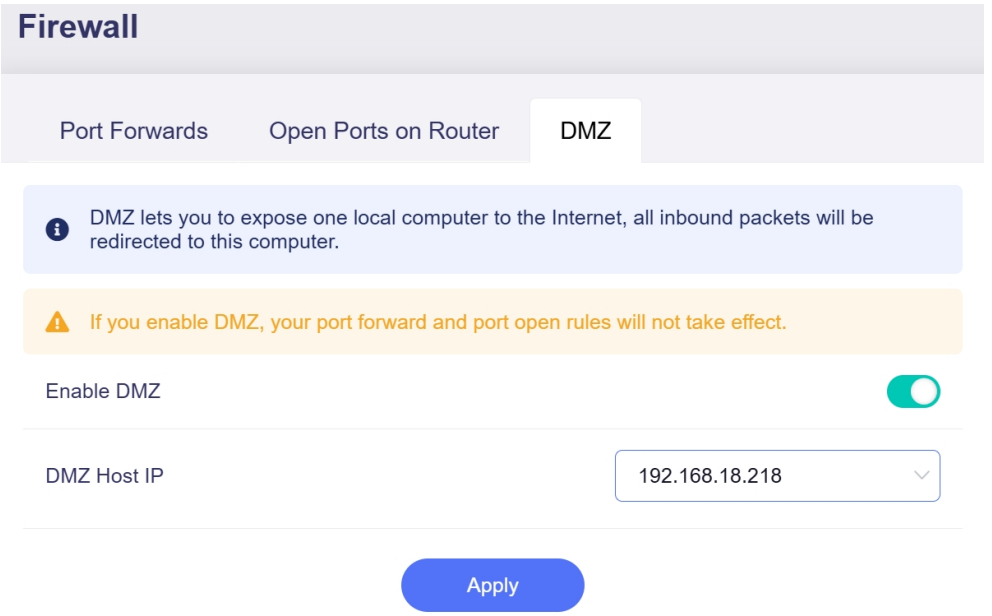
- **Nombre**: el nombre de la regla que puede especificar el usuario.
- **Protocolo**: El protocolo utilizado, puede elegir TCP, UDP o TCP y UDP.
- **Puerto**: el número de puerto que desea abrir.
- **Habilitar**: habilita o deshabilita esta regla.

12.1.3 DMZ

DMZ le permite exponer una computadora a Internet, por lo que todos los paquetes entrantes serán redirigidos a esta computadora.le permite exponer una computadora a Internet, de modo que todos los paquetes entrantes serán redirigidos 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.



12.2 Multi-WAN

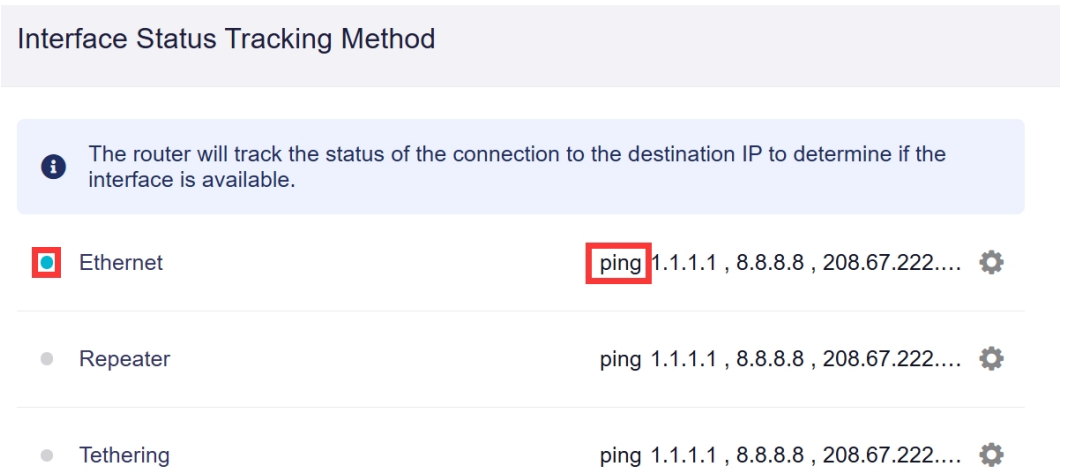
Multi-WAN permite el uso simultáneo de múltiples métodos de acceso a Internet, lo que permite la configuración de diversos opciones de conectividad en el enrutador. Ofrece dos modos de trabajo:

- **Conmutación por error**: cambia automáticamente a una conexión alternativa en poco tiempo si la conexión principal falla, lo que garantiza un acceso ininterrumpido a la red.
- **Equilibrio de carga**: distribuye 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.

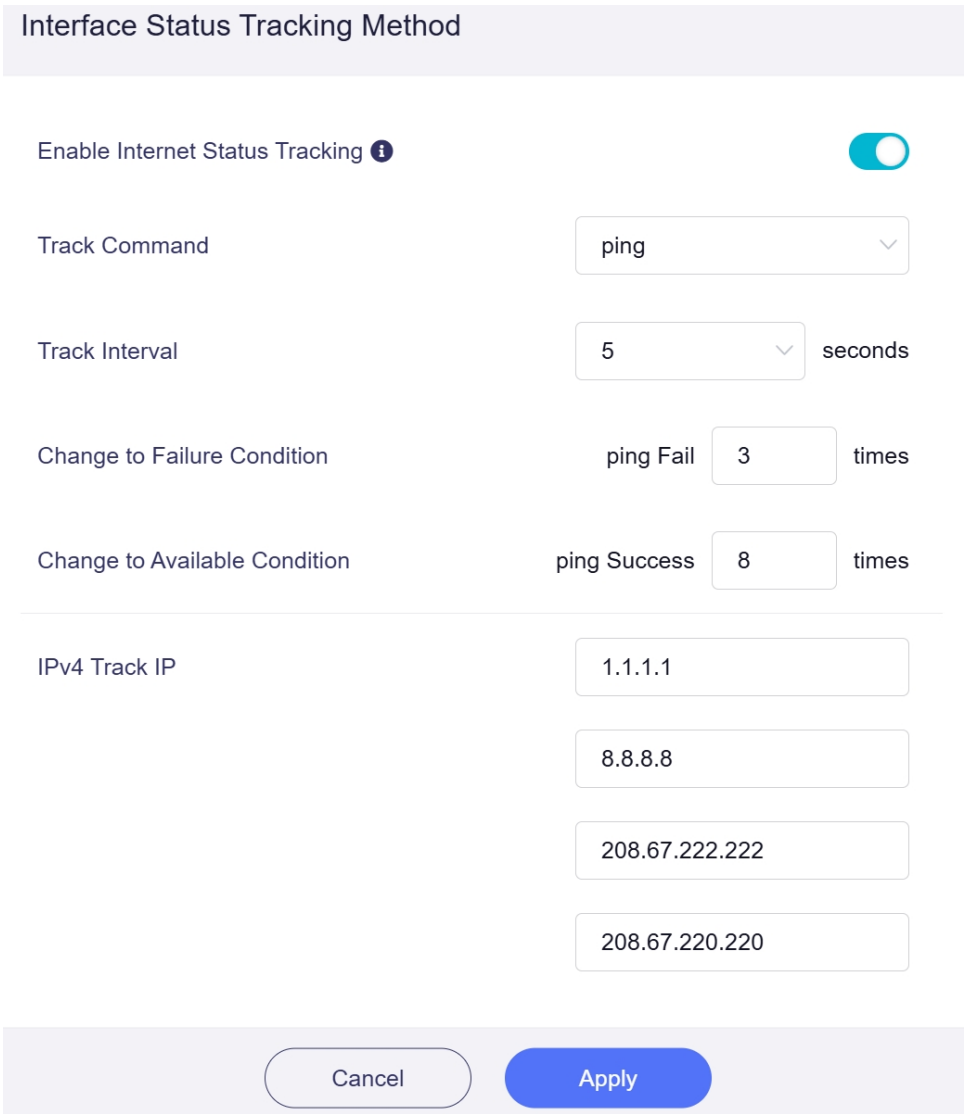
Inicie sesión en el panel de administración web de su enrutador' y navegue hasta **RED >Multi-WAN**. Esta página incluye dos secciones: Seguimiento del estado de la interfaz y modo Multi-WAN.

12.2.1 Seguimiento del estado de la interfaz

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



En el **Pista de estado de la interfaz** sección, chaga 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 el seguimiento de estadoing configuracións 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 Track**: el comando ping es se utiliza para monitorear el estado de la conexión a la IP de destino y verificar la disponibilidad de la interfaz.
- **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 se restaurará la interfaz al estado de conexión después del número especificado de ping exitosos consecutivos.
- **IPv4 Track IP**: Cpersonalice las direcciones IP de seguimiento IPv4 si necesario.

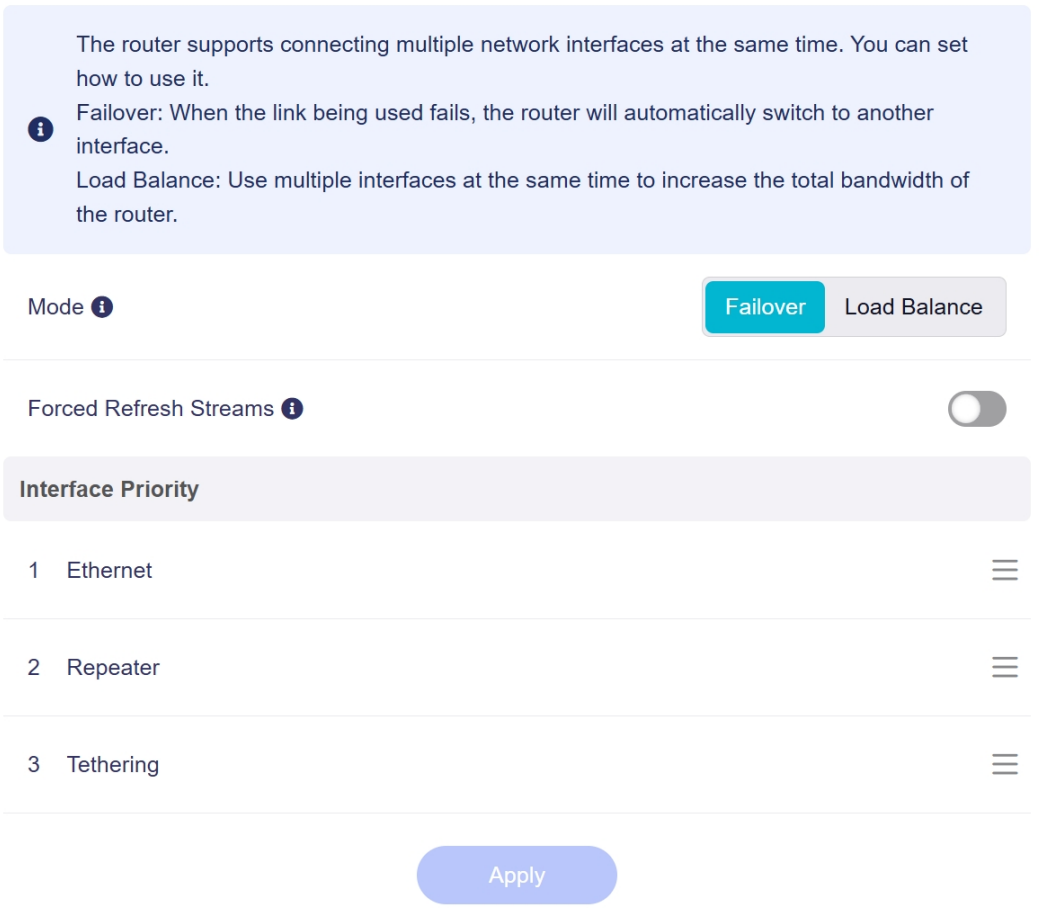
12.2.2 Modo Multi-WAN

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

Conmutación por error

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

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

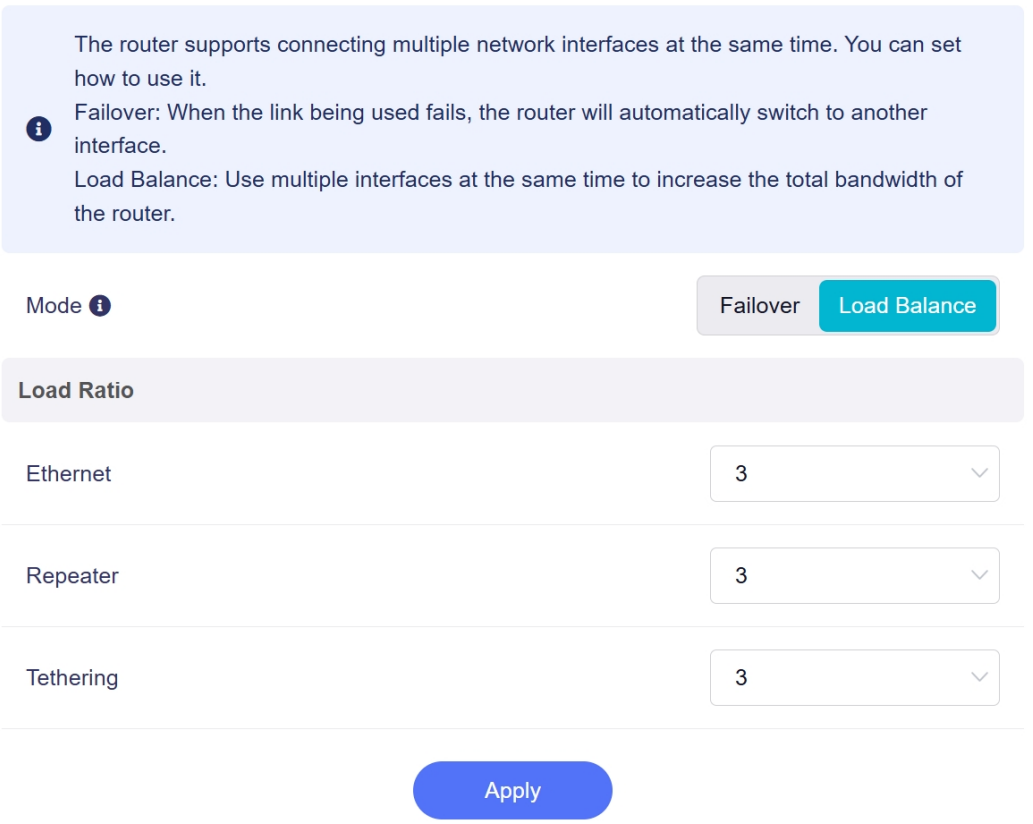


Equilibrio de carga

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

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

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



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

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

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

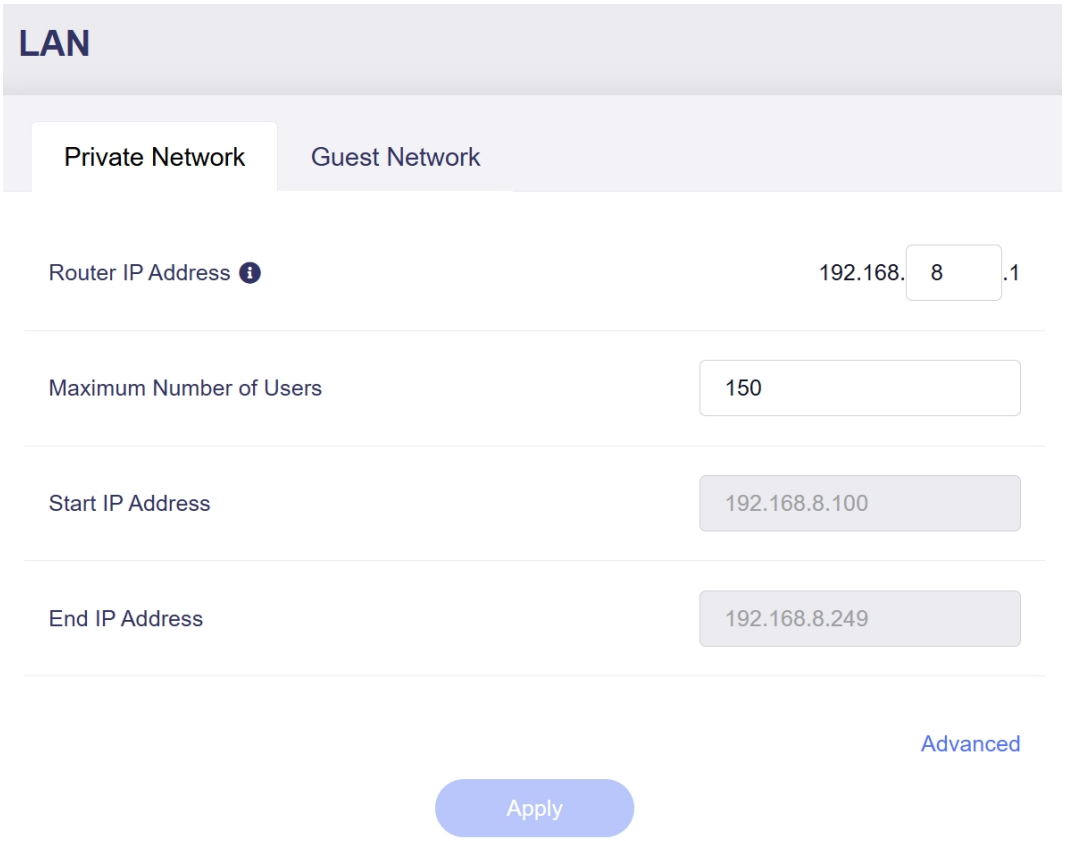
12.3 LAN

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

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

12.3.1 Red privada

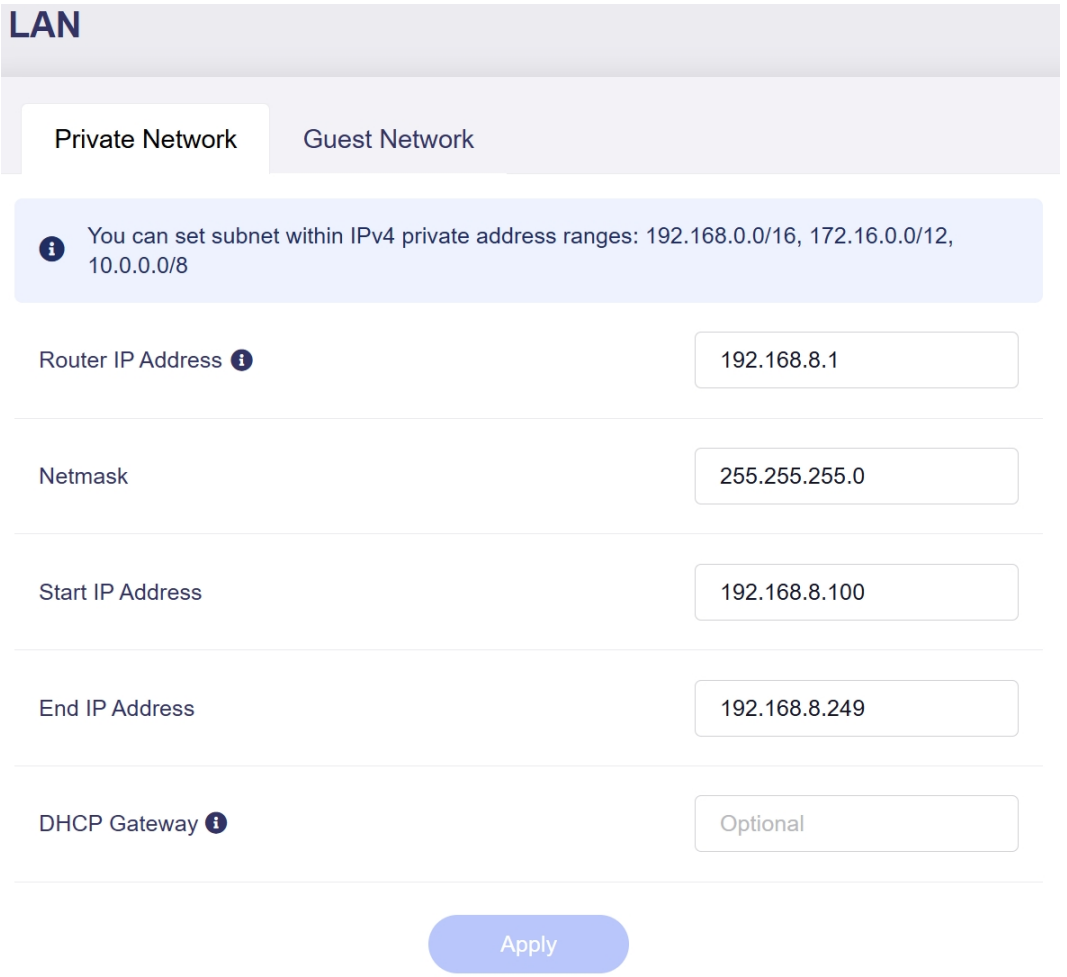
La red privada es la red local principal para sus dispositivos conectados. Puede configurar la dirección IP del enrutador, el rango de direcciones DHCP y el número máximo de clientes conectados.



- **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.'panel de administración. 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, la dirección IP inicial, la dirección IP final y la puerta de enlace DHCP.

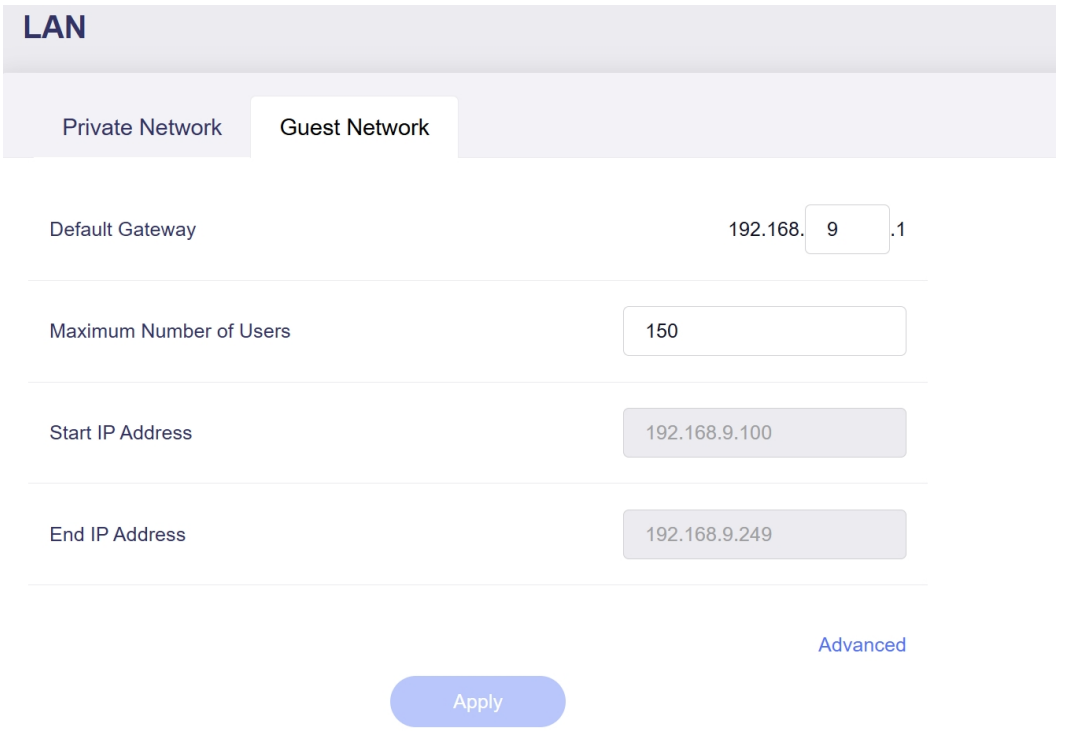


- **DHCP Puerta de enlace**: La dirección de puerta de enlace predeterminada asignada a los clientes por el servidor DHCP. Enruta el tráfico de la red local a redes externas, como Internet.
- **Máscara de red**: la máscara de subred para la red privada. El valor predeterminado es 255.255.255.0.

12.3.2 Red de invitados

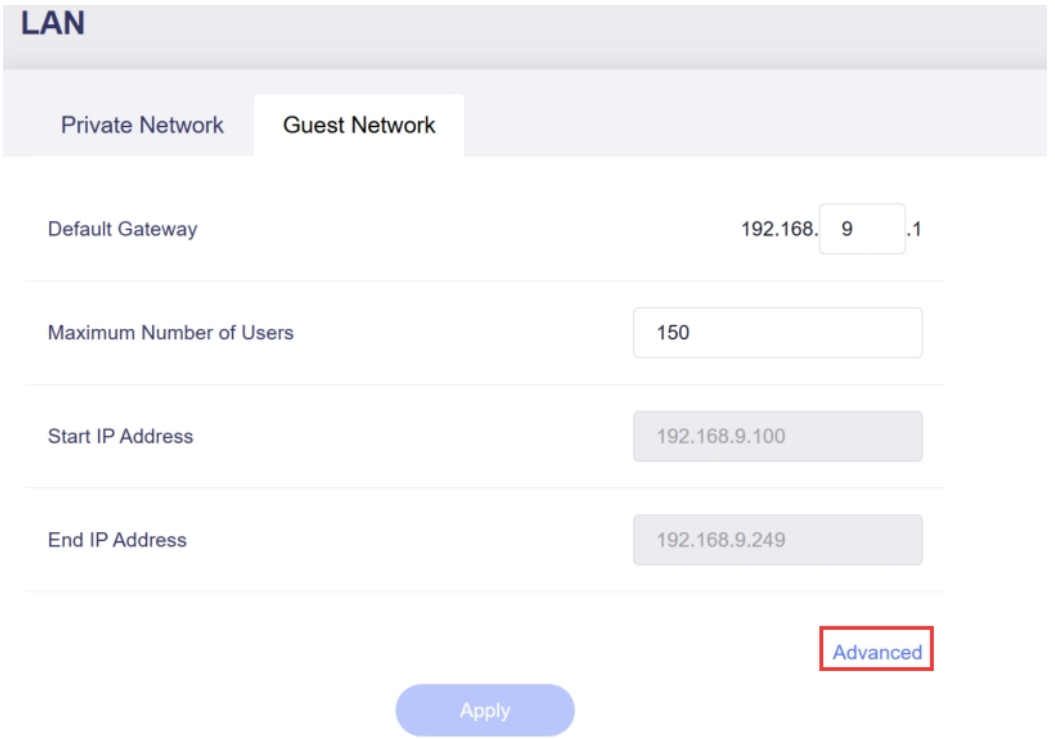
Red de invitados se refiere a una red dedicada a la que los visitantes se pueden conectar, aislando desde su LAN principal para proteger la seguridad de su red privada.

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.

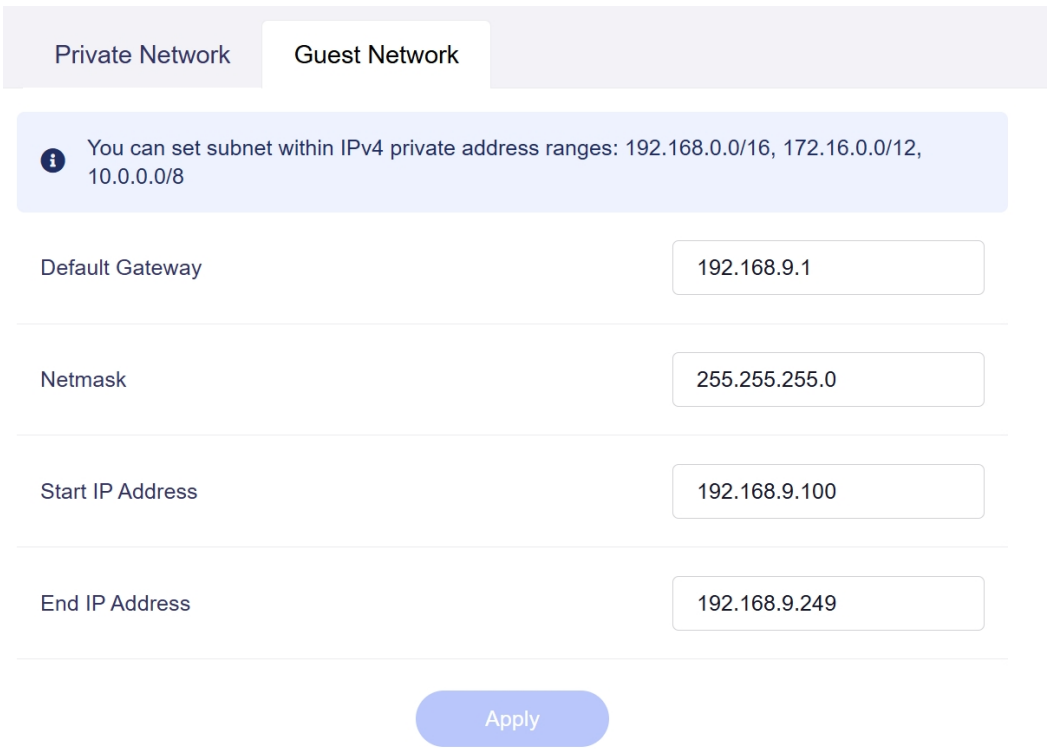


- **Puerta de enlace predeterminada**: Es 192.168.9.1 de forma predeterminada y se puede cambiar si es necesario, pero no debe entrar en conflicto con la puerta de enlace de la red principal.
- **Número máximo de usuarios**: Establezca el número máximo de clientes permitidos para conectarse a la red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

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



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



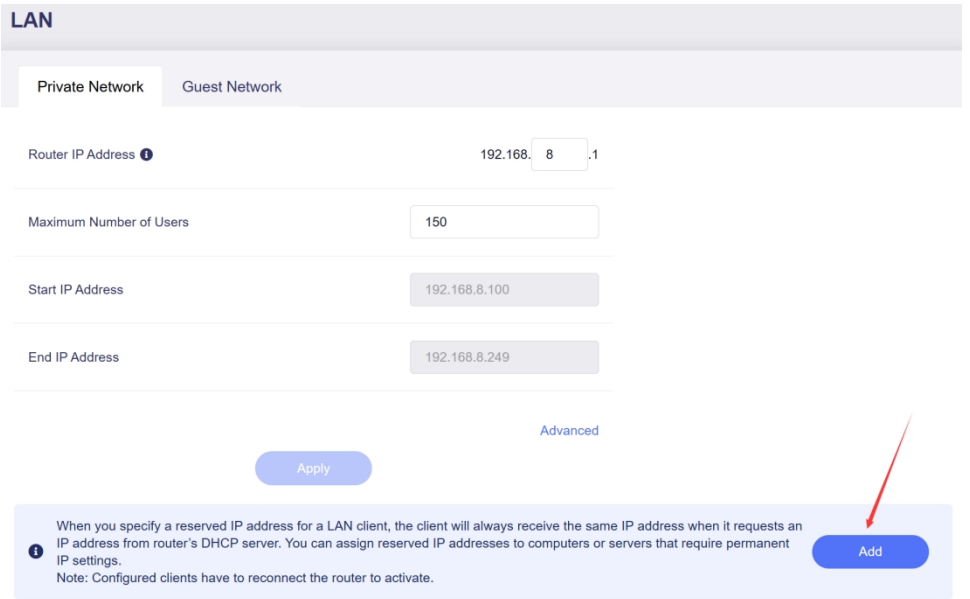
La **máscara de red** dpor defecto es 255.255.255.0. También puede seleccionar 255.255.0.0 si necesita una subred más grande con más direcciones IP.

12.3.3 Reserva de direcciones

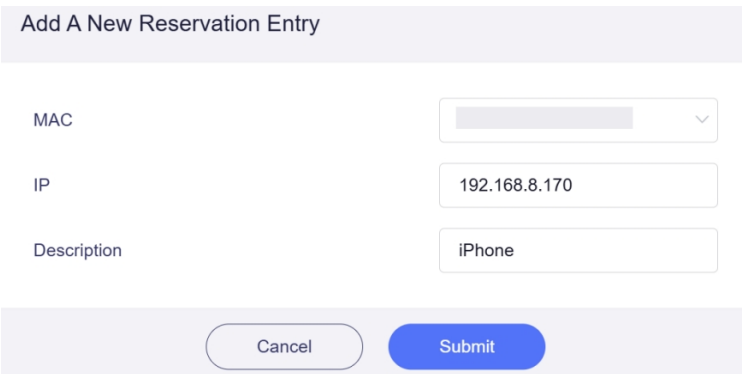
La reserva de dirección le permite especificar una dirección IP fija para un cliente LAN, de modo que el cliente siempre reciba la misma dirección IP cada vez que accede al servidor DHCP del enrutador. Puede asignar direcciones IP reservadas a computadoras o servidores que requieren una configuración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

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

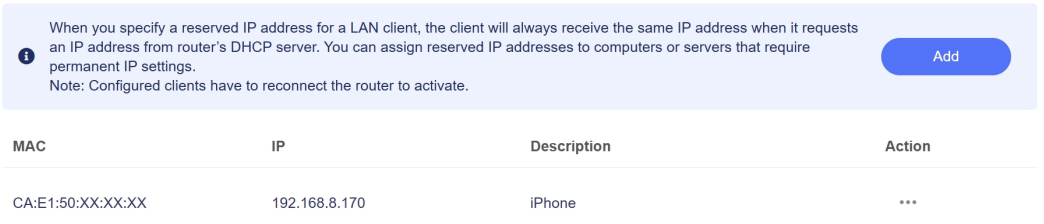
1. Inicie sesión en el panel de administración web de su enrutador', navegue hasta **RED** > **LAN** > **Reserva de direcciones** y haga clic en **Agregar**.



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



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



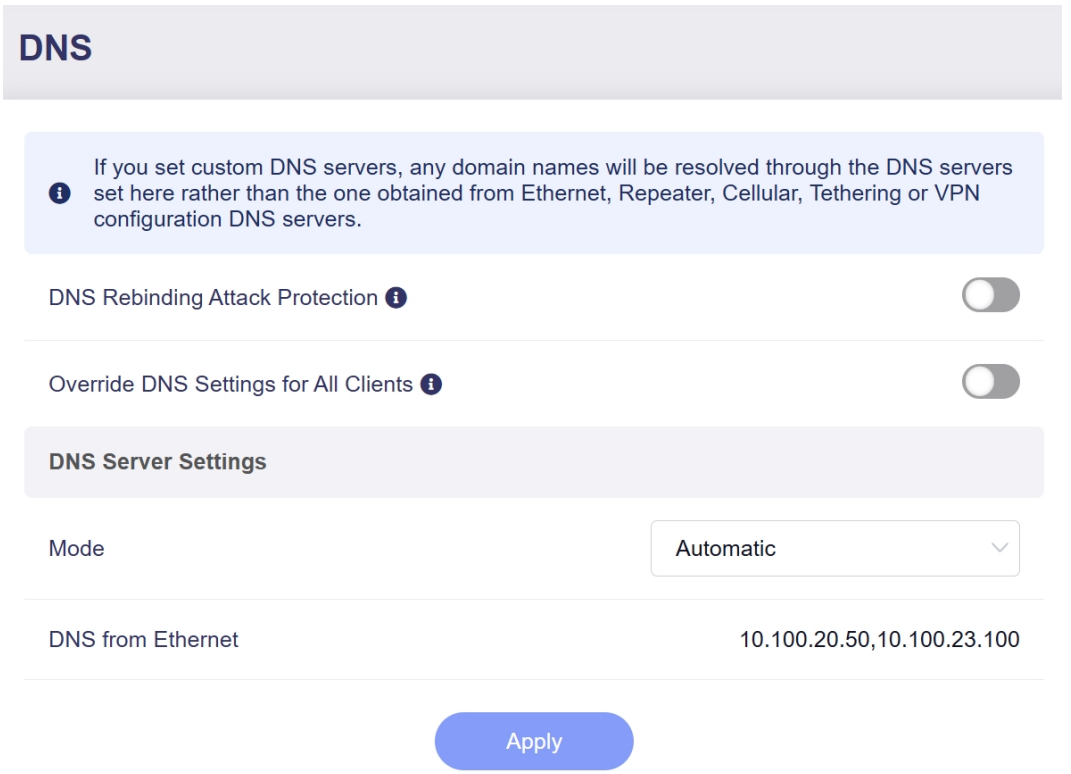
12.4 DNS

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

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

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

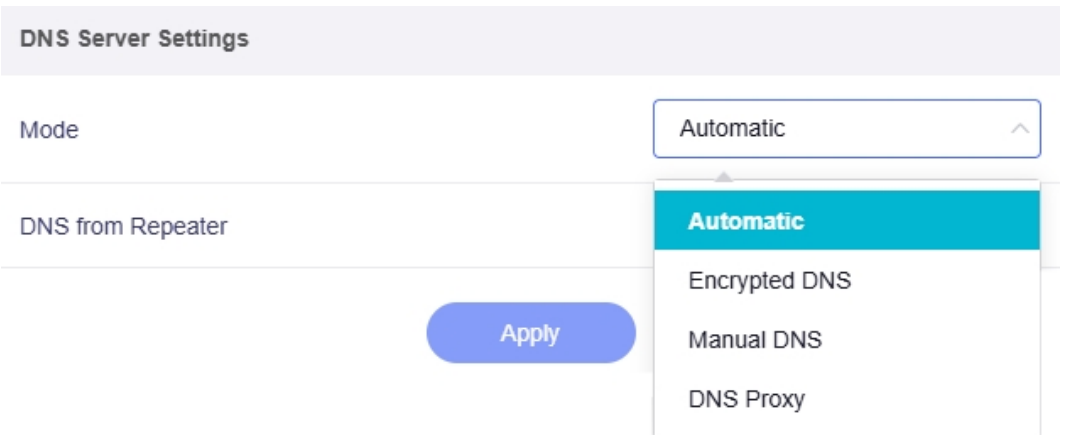
12.4.1 Configuración general



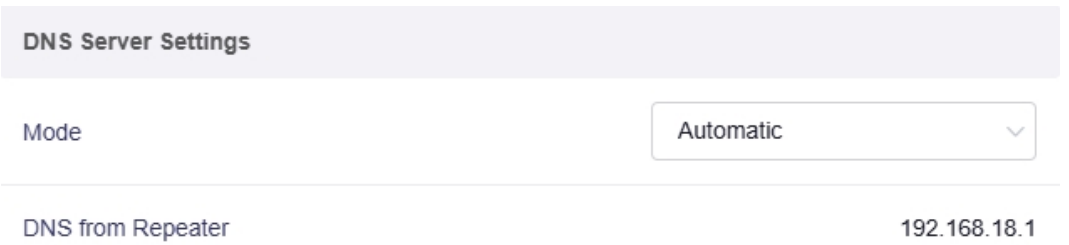
- **DNS Protección contra ataques de nueva vinculación**: protege contra ataques de nueva vinculación de DNS al bloquear intentos maliciosos de resolución de DNS. Tenga en cuenta que habilitarlo puede causar fallas en la búsqueda de DNS privado; deshabilítelo si su red utiliza un portal cautivo (por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

12.4.2 Configuración del servidor DNS

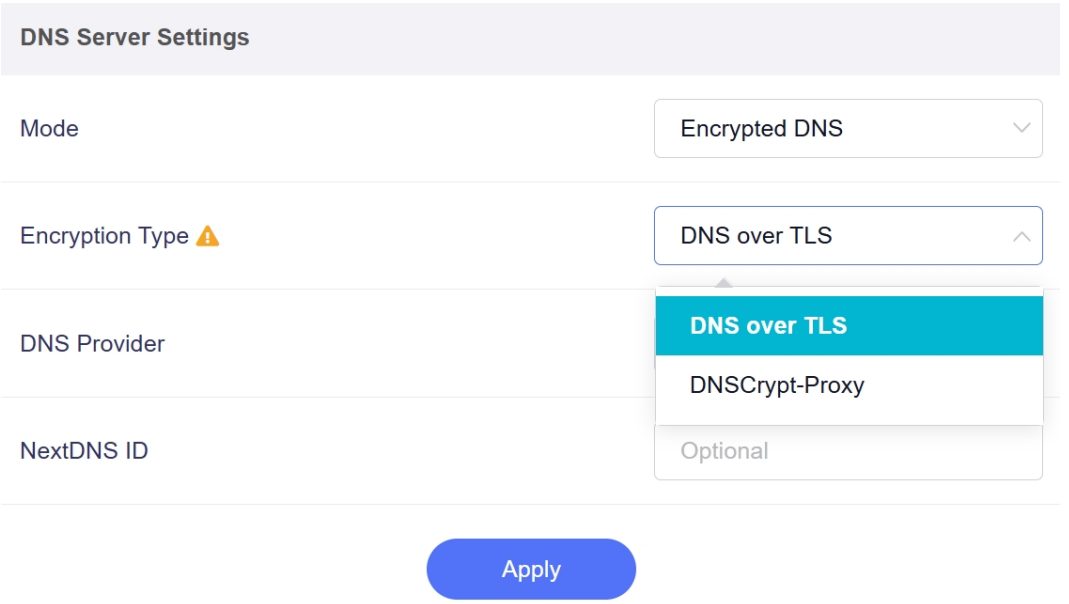
Hay cuatro modos para el servidor DNS: DNS automático, cifrado, DNS manual y proxy DNS.



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

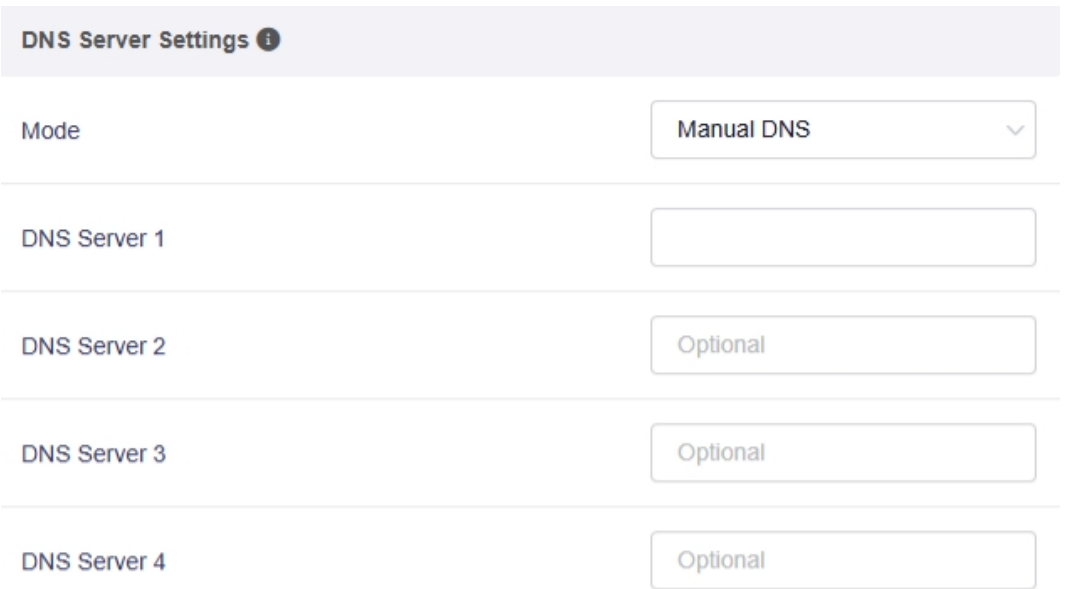


2. **Cifrado DNS**: cuando se selecciona, el enrutador utilizará protocolos cifrados para procesar consultas de DNS, protegiendo los datos de resolución contra escuchas o alteraciones.
   Tiene dos tipos de cifrado: DNS sobre TLS y DNSCrypt-Proxy.



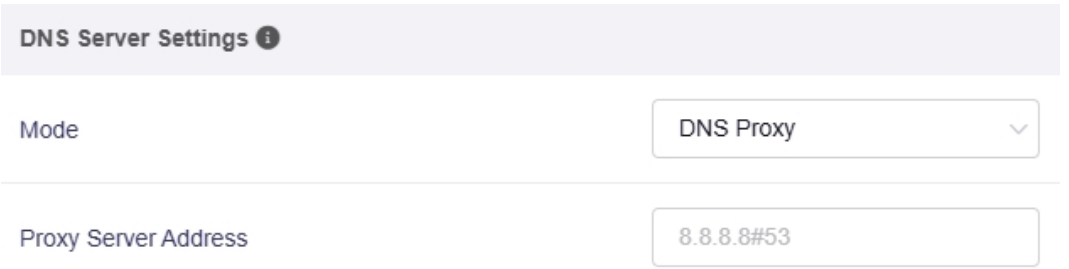
- Para DNS sobre TLS, seleccione un proveedor de DNS entre Control D, NextDNS y Cloudflare.
- Para DNSCrypt-Proxy, seleccione al menos un servidor DNS del repositorio. Se pueden seleccionar hasta 8 servidores. Cuando se seleccionan varios servidores, el enrutador utilizará el más rápido automáticamente.

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



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

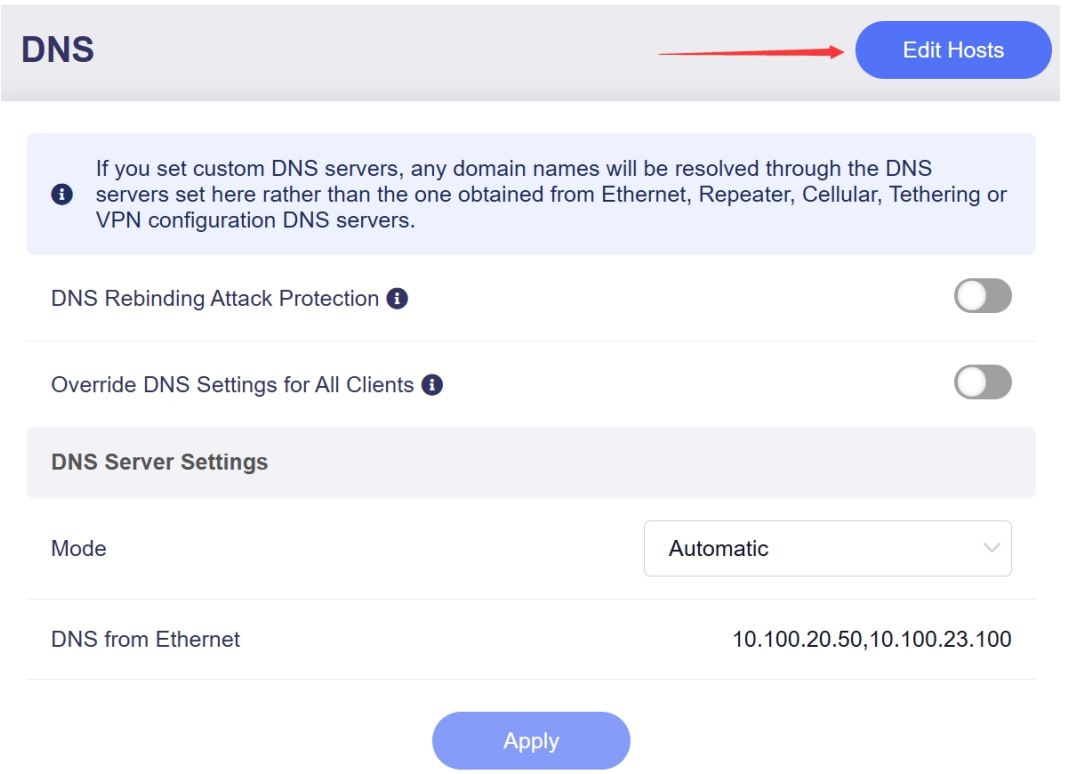
4. **Proxy DNS**: cuando se selecciona, el enrutador reenvía todas las consultas DNS a través de un servidor proxy, permitela resolución a través del proxy entorno de red para necesidades de acceso específicas.



12.4.3 Editar hosts

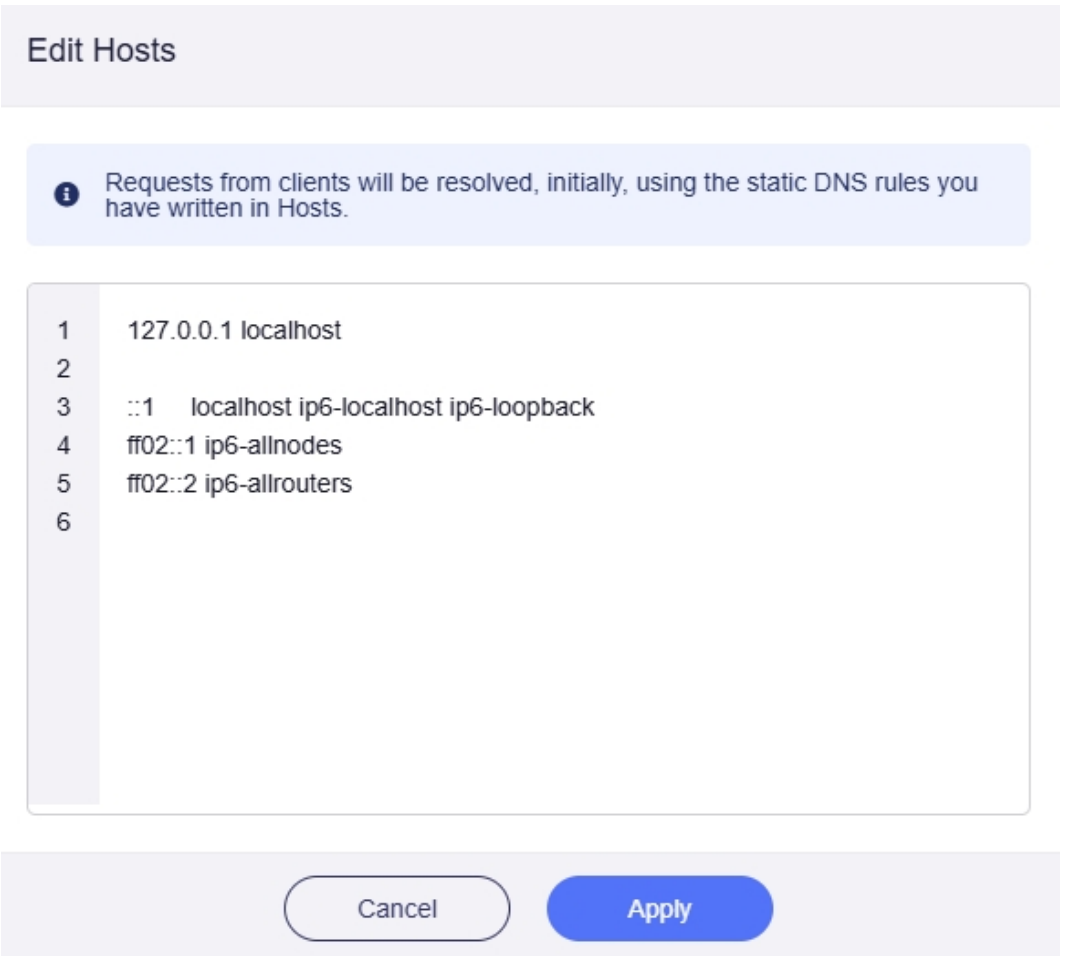
Puede definir reglas de resolución de DNS estáticas si es necesario.

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



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

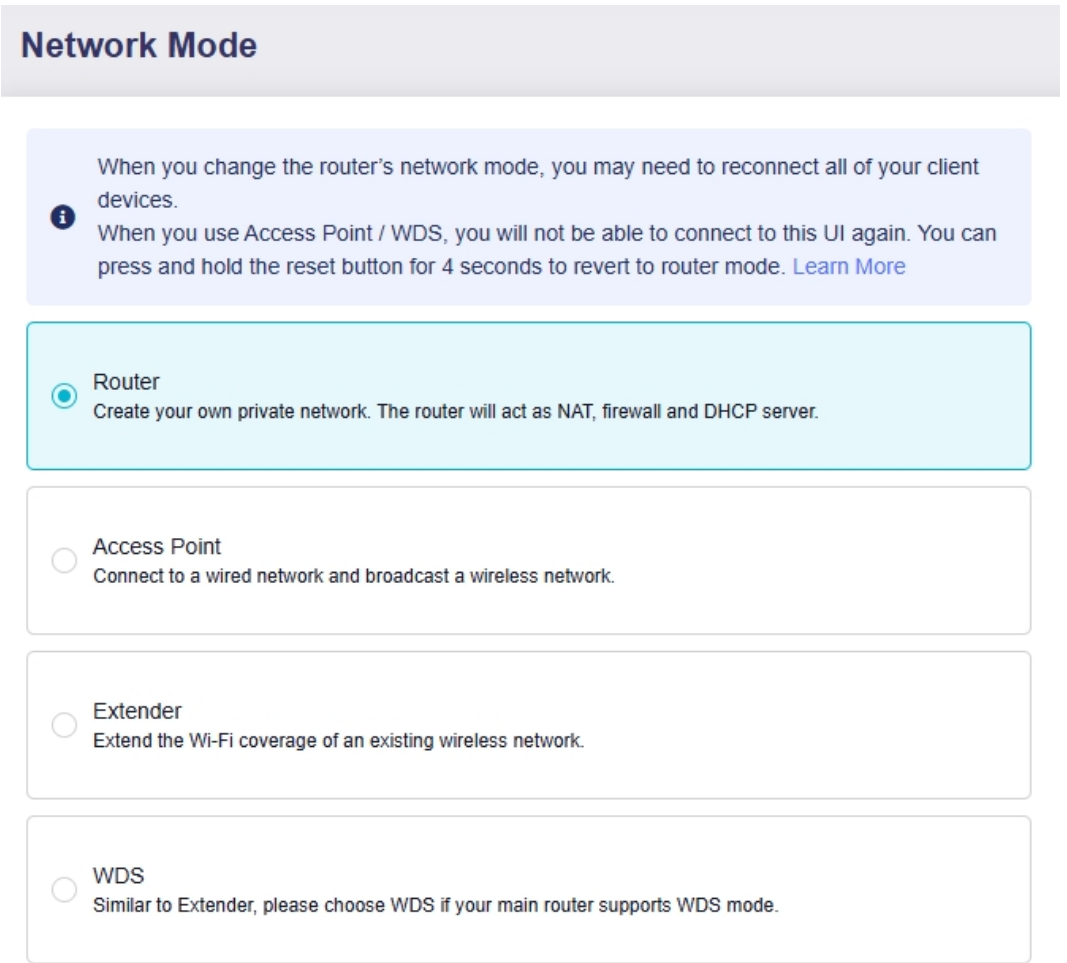
host (por ejemplo, las entradas predeterminadas). como 127.0.0.1 localhost para loopback local) para un control personalizado de la resolución de nombres de dominio.



12.5 Modo de red

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

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



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

- **Punto de acceso**: este modo permite que un enrutador se conecte a una red cableada a través de un cable LAN y transmita señales inalámbricas, ampliando la cobertura Wi-Fi en grandes espacios para permitir el acceso de más dispositivos. la red. En este modo, el enrutador desactiva sus funciones NAT y DHCP, funcionando exclusivamente 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 provocar que el ancho de banda se reduzca a la mitad, ya que el dispositivo tiene que manejar la recepción y transmisión de señales simultáneas.
- **WDS**: el modo Sistema de distribución inalámbrica (WDS) es similar al modo Extensor, ya que extiende la cobertura Wi-Fi de forma inalámbrica, pero admite puentes inalámbricos entre múltiples enrutadores compatibles. Se recomienda para la expansión de la red inalámbrica cuando el enrutador ascendente tiene funcionalidad WDS.
  Este modo es ideal para escenarios como cubrir edificios de varios pisos o campus de oficinas pequeñas donde varios enrutadores necesitan trabajar juntos para formar una red inalámbrica unificada. A diferencia del modo Extensor, que solo transmite señales desde un enrutador principal a un único extensor, el modo WDS permite que los enrutadores interconectados envíen y reciban señales, lo que permite una cobertura perfecta en áreas más grandes con múltiples nodos de señal.

Nota:

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

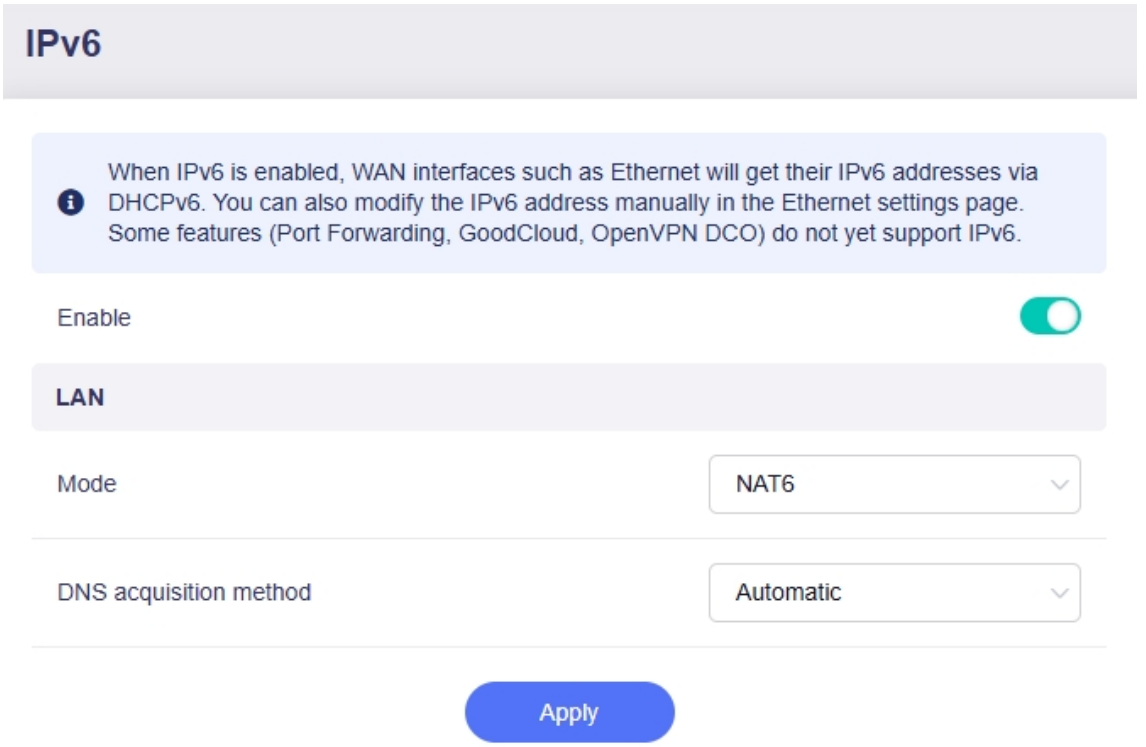
3. **En el modo Punto de acceso/Extensor/WDS, las siguientes funciones no estarán disponibles**: Control de acceso (lista de permitidos y de bloqueo), VPN, Firewall, Multi-WAN, servidor DHCP, reserva de dirección, red de invitados, DNS, IPv6, puerta de enlace directa, IGMP Espiando.

12.6 IPv6

IPv6 (Protocolo de Internet versión 6) es el último protocolo de Internet diseñado para reemplazar IPv4. Ofrece un grupo más grande de IP únicas, lo que resuelve el problema de agotamiento de direcciones de IPv4 y admite el creciente número de dispositivos conectados en todo el mundo.

Inicie sesión en el panel de administración web de su enrutador' y navegue hasta **RED** > **IPv6**. Estaesta página le permite habilitar y configurar IPv6 en su enrutador. Cuando IPv6 está habilitado, las interfaces WAN como Ethernet obtendrán sus direcciones IPv6 a través de DHCPv6.

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



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

12.6.1 Modo IPv6

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

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

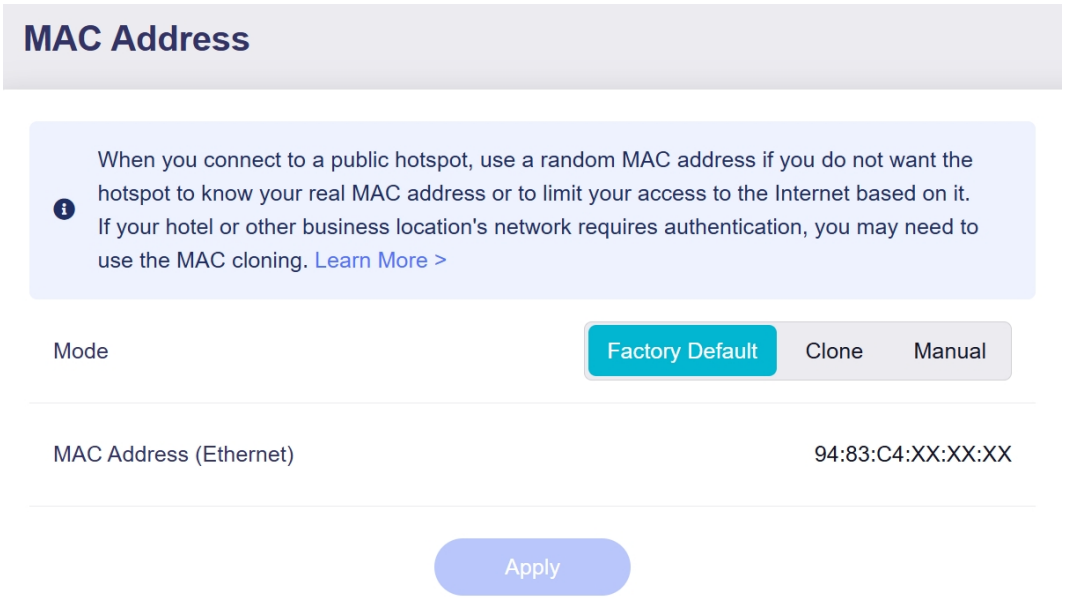
12.6.2 Método de obtención de DNS

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

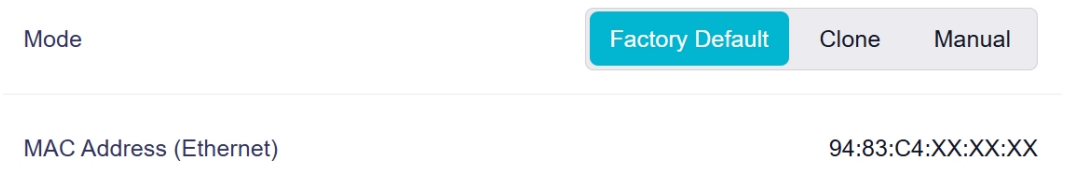
- **Automático**: el enrutador obtendrá direcciones de servidor DNS IPv6 de forma dinámica (por ejemplo, a través de DHCPv6).
- **Manual**: ingrese direcciones de servidor DNS IPv6 personalizadas. Sin embargo, dado que DNS se utiliza para resolver nombres de dominio en sus direcciones IP correspondientes,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

12.7 Dirección MAC

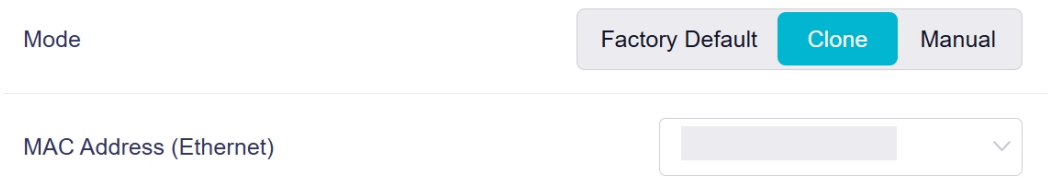
La Dirección MAC página mostrars la dirección MAC predeterminada del enrutador, clonar la dirección MAC de un cliente, ingresar una dirección MAC manualmente o generar una dirección MAC aleatoria. Si el dispositivo admite la configuración de varios puertos Ethernet para usarlos como puertos WAN, puede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



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



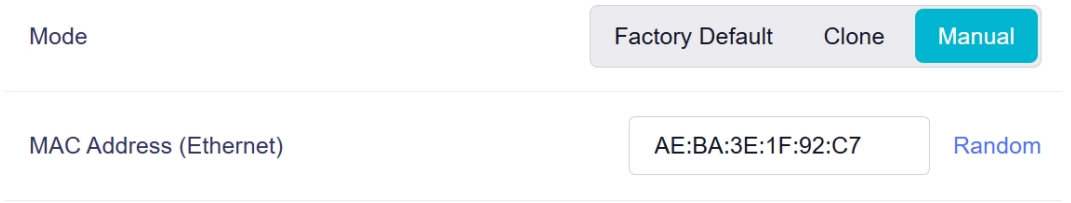
- **Clonar la dirección MAC de un cliente.**



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

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

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

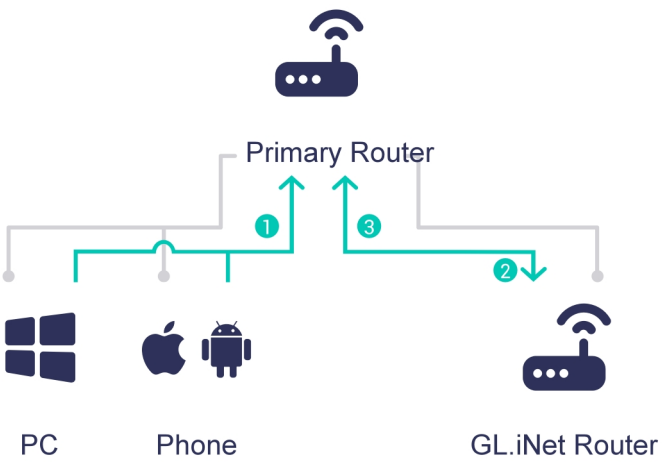


12.8 Puerta de enlace directa

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

- Habilitar cliente VPN
- Usar DNS cifrado

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



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

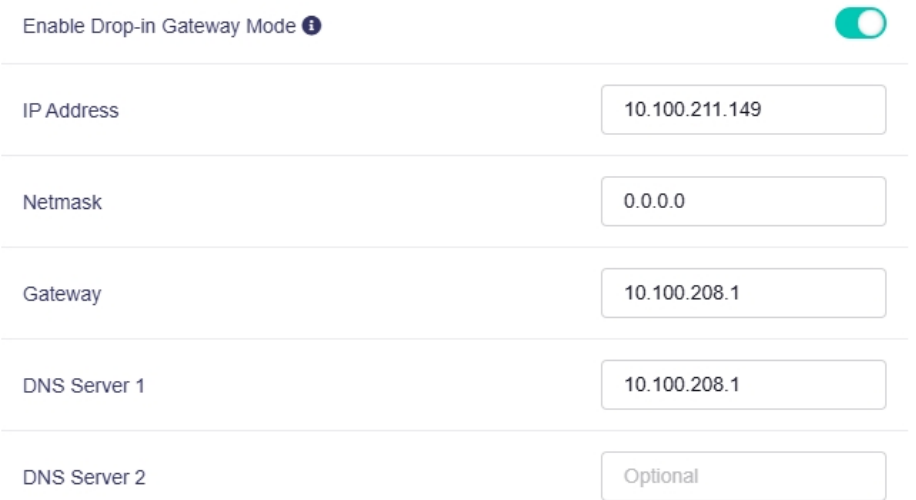
- **Grayo lines** ilustran la conexión física Topología: dispositivos cliente (por ejemplo, computadora, computadora portátil) se conectan al enrutador principal, y el puerto LAN

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

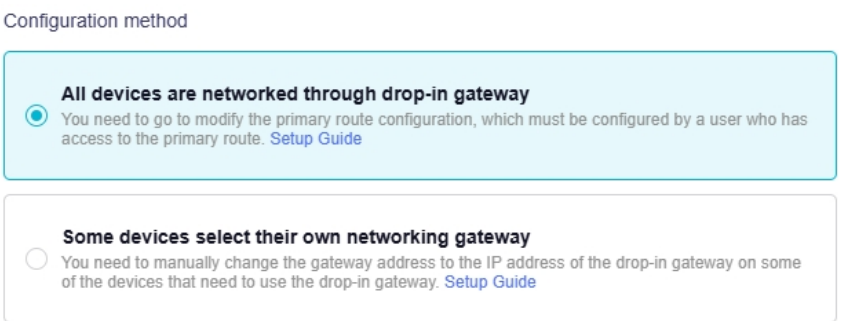
- **Glíneas verdes** representan la ruta de transmisión de datos secuencial cuando Drop-in Gateway está activo, con las flechas numeradas indicando el flujo de tráfico orden:
  1. El tráfico de los dispositivos cliente se enruta primero al enrutador principal;
  2. El enrutador principal reenvía el tráfico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

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

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



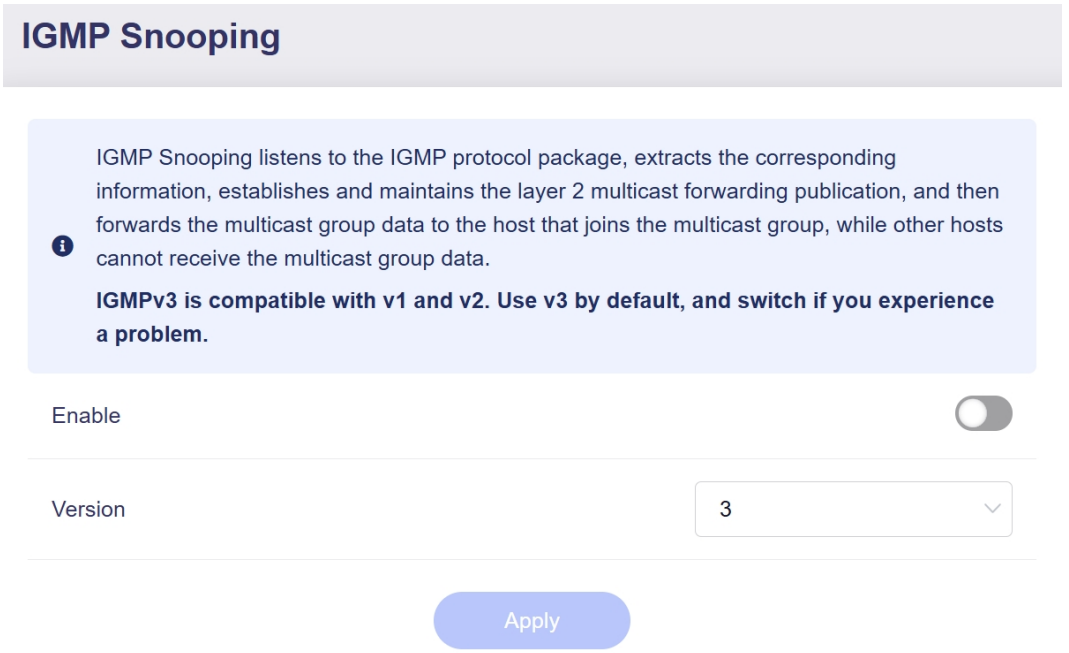
2. Seleccione el método de configuración y luego haga clic en **Aplicar**. Consulte este tutorial para detalless.



12.9 Inspección IGMP

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

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



Capítulo 13

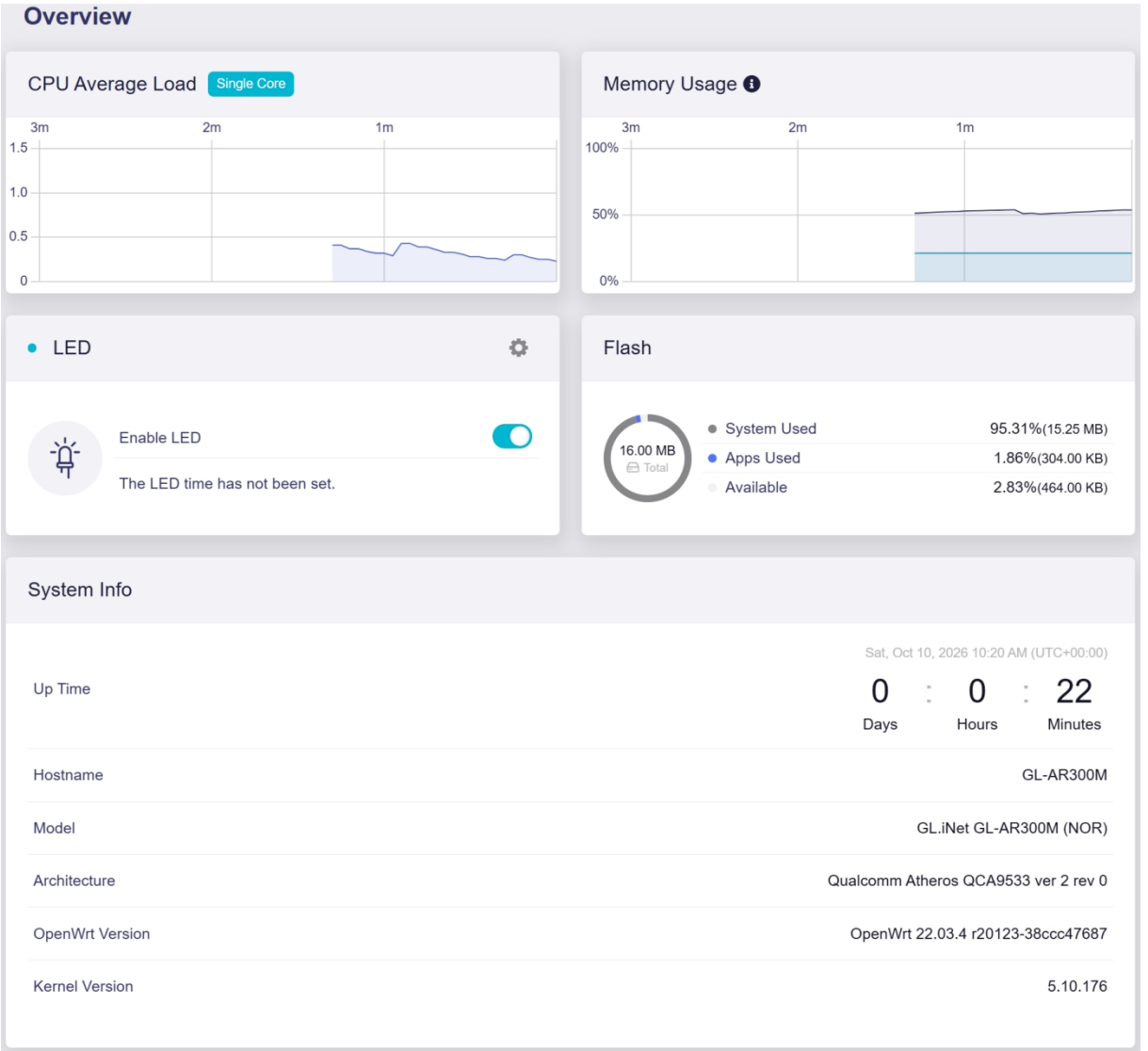
Sistema

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.

13.1 Descripción general

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

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

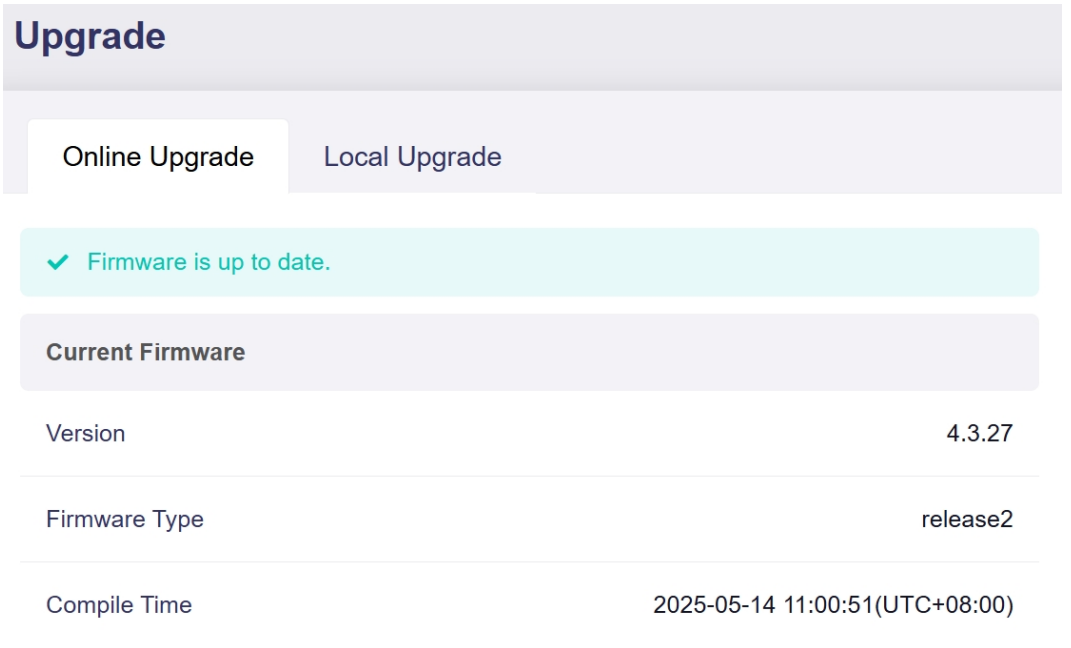


13.2 Actualización

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.

13.2.1 Actualización en línea

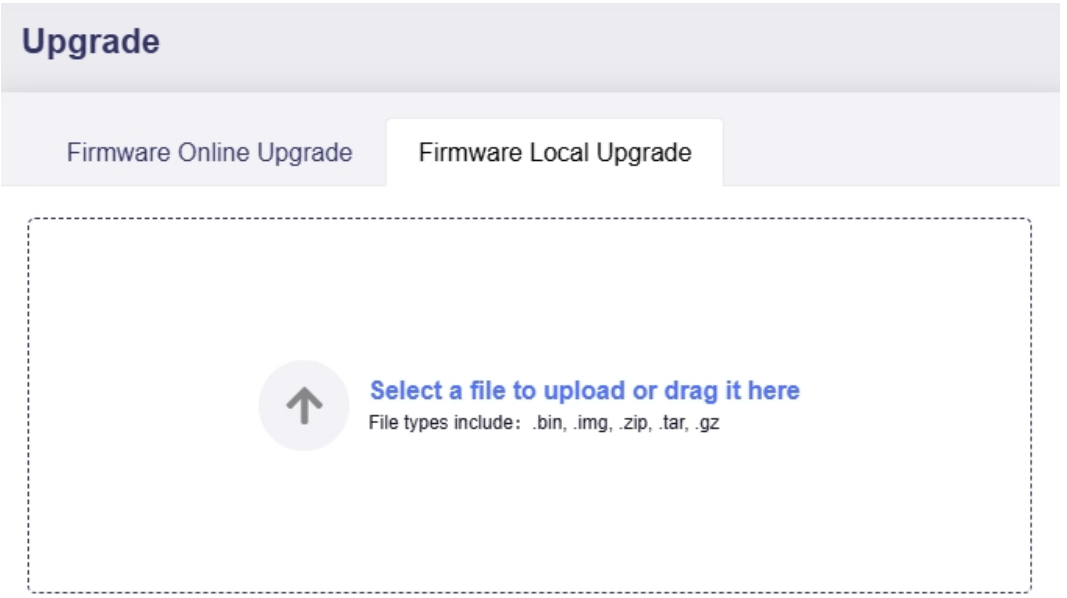
Puede buscar el firmware actual detalles aquí, incluida la versión del firmware, el tipo de firmware (por ejemplo, versión, beta) y el tiempo de actualización. Si su enrutador está conectado a Internet, buscará la versión de firmware más reciente disponible para descargar.



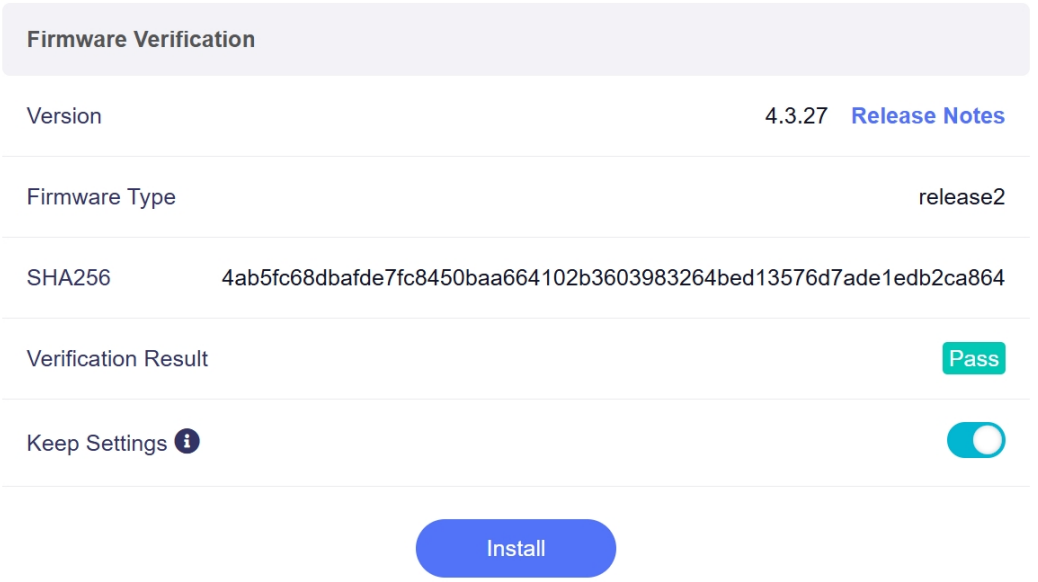
Consejo: Al intentar realizar una actualización en línea, si muestra **Descarga fallida**, navegue hasta **SISTEMA** > **Zona horaria** y corrija el error de zona horaria (sincronización con el navegador).

13.2.2 Actualización local

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



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



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

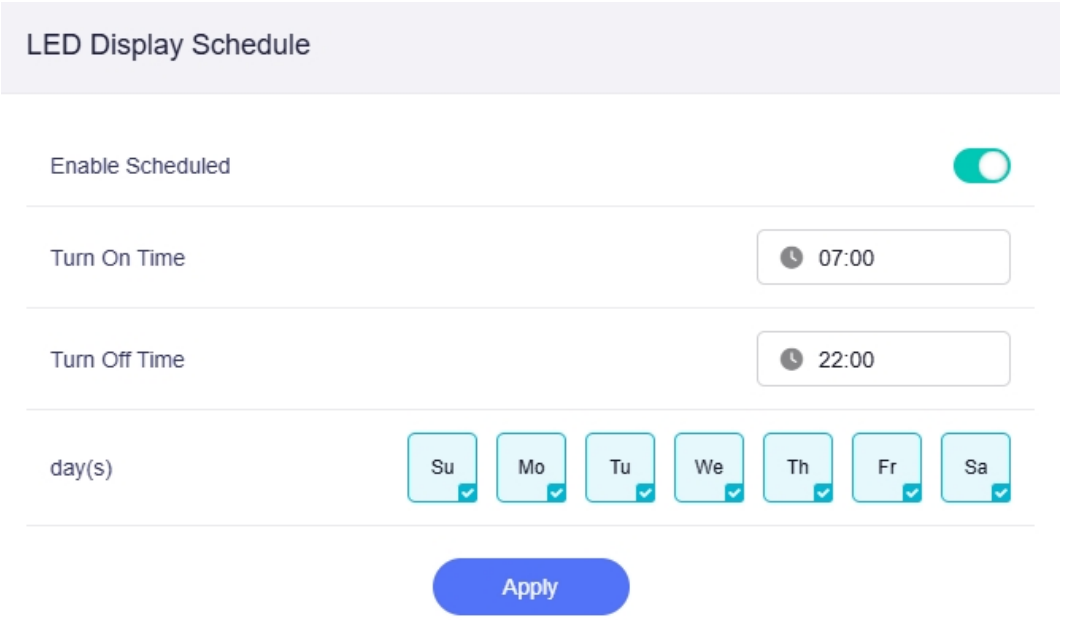
13.3 Tareas programadas

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

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

13.3.1 Programación de los indicadores LED

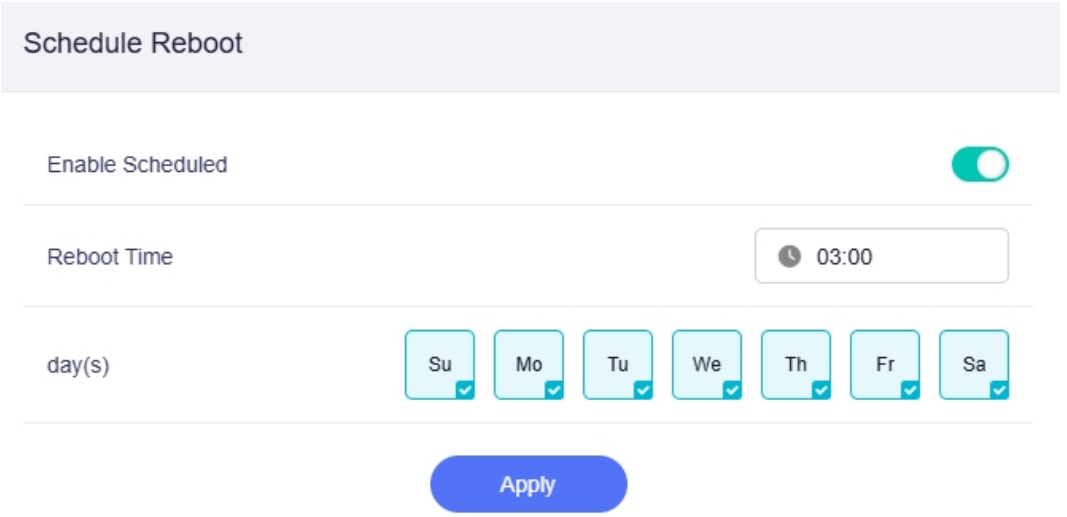
Sestablezca un programa para la luz LED de su enrutador si es necesario, luego haga clic **Aplicar**.



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

13.3.2 Programar reinicio

Set a programe el reinicio automático de su enrutador si es necesario, luego haga clic **Aplicar**.



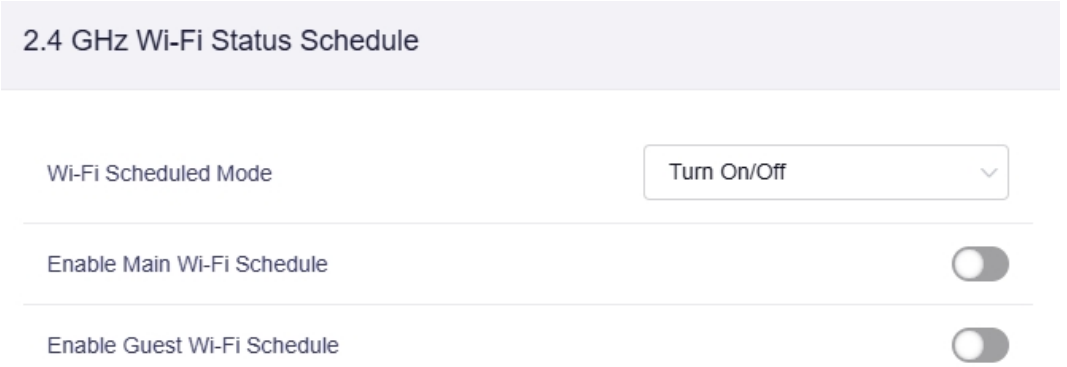
- **Activar programado**: active este interruptor para habilitar el reinicio programado.
- **Hora de reinicio**: establezca la hora específica (por ejemplo, 03:00) a la que se reiniciará el enrutador.
- **día(s)**: Seleccione los días efectivos de la semana para esta configuración.

13.3.3 Programación de Wi-Fi de 2,4 GHz

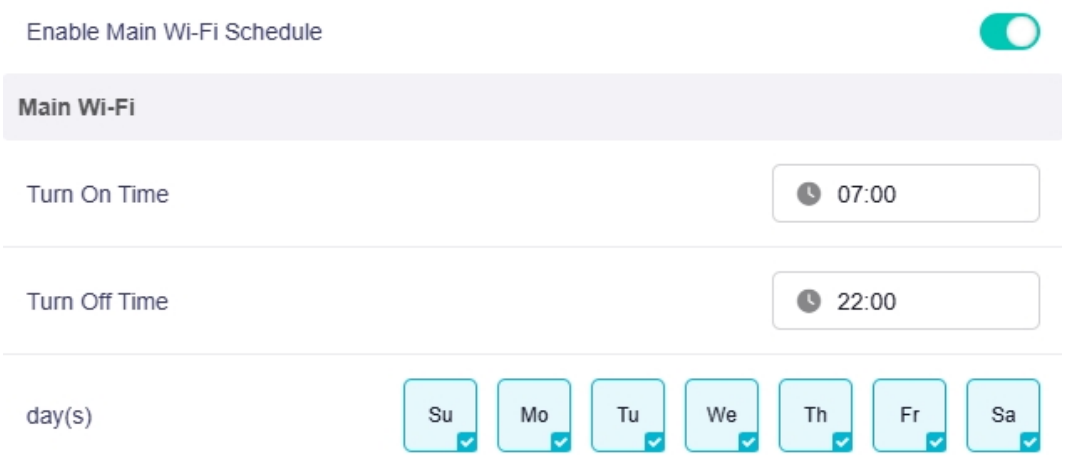
Esta función le permite establezca un horario para su Wi-Fi de 2,4 GHz. Hay dos modos: encender/apagar y cambiar la alimentación de TX.

Modo 1: Encender/apagar

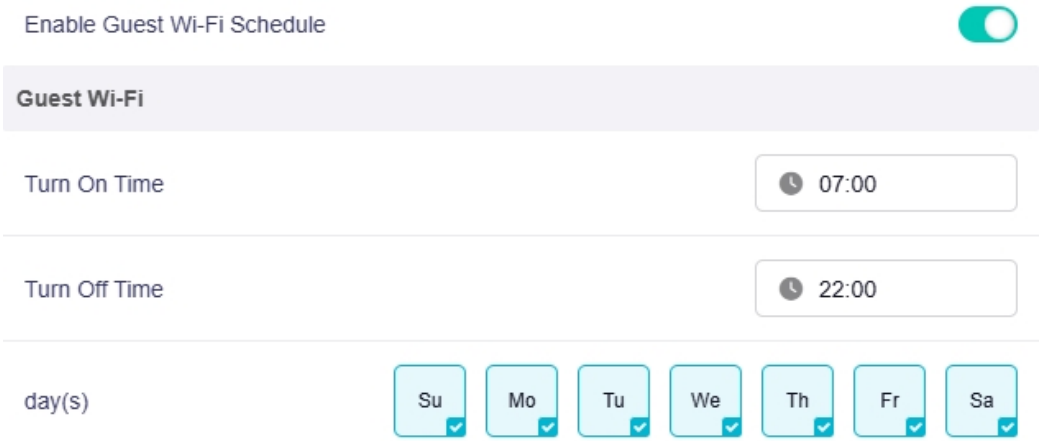
Puedes habilitar el horario de encendido/apagado tanto para el Wi-Fi principal de 2,4 GHz como para los invitados. Wi-Fi.



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

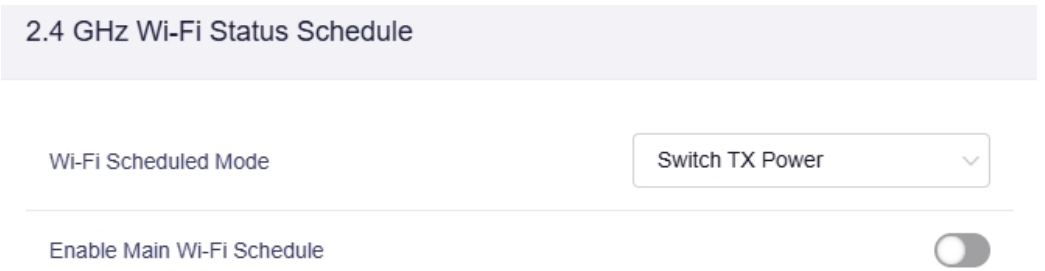


- **Wi-Fi para invitados Programación**: cuando esté habilitado, configure los horarios de encendido y apagado de su Wi-Fi para invitados de 2,4 GHz y seleccione una fecha efectiva para la semana.

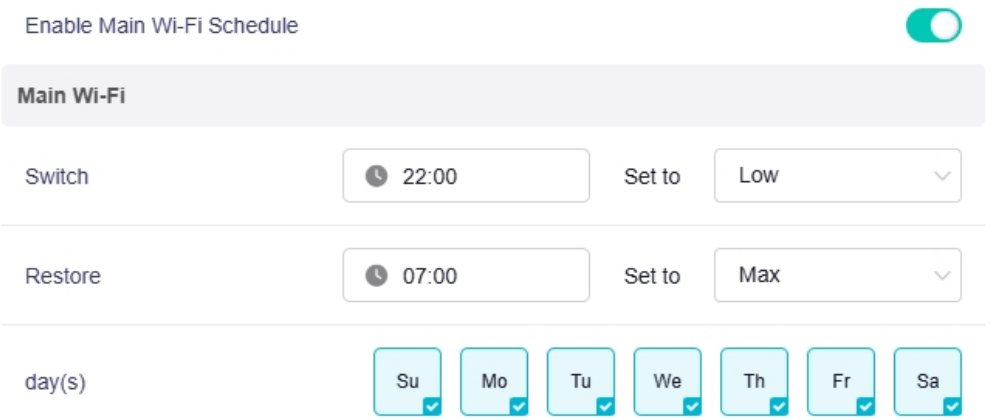


Modo 2: cambiar la alimentación de TX

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



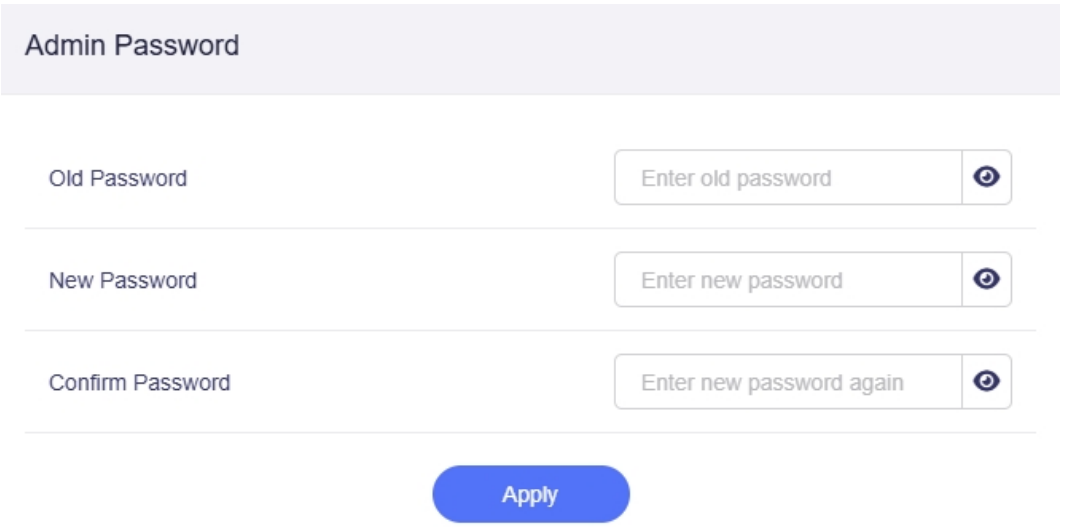
Cuando esté habilitado, configure dos acciones cronometradas para que su Wi-Fi principal de 2,4 GHz cambie la alimentación de TX y seleccione una fecha efectiva para la semana.



- **Cambiar**: Set TX Power a un cierto nivel (por ejemplo, bajo) at una hora específica (por ejemplo, 22:00).
- **Restaurar**: Restorar energía TX en unotro nivel (p. ej., máx.) aen otro momento (p. ej., 07:00).
- **días**: Seleccione los días efectivos de la semana para esta configuración.

13.4 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.

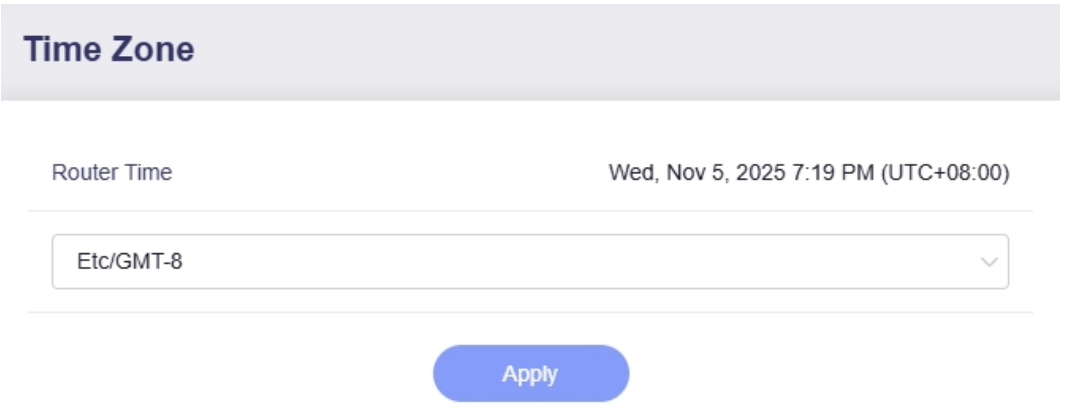


Los requisitos para la contraseña de administrador son los siguientes:

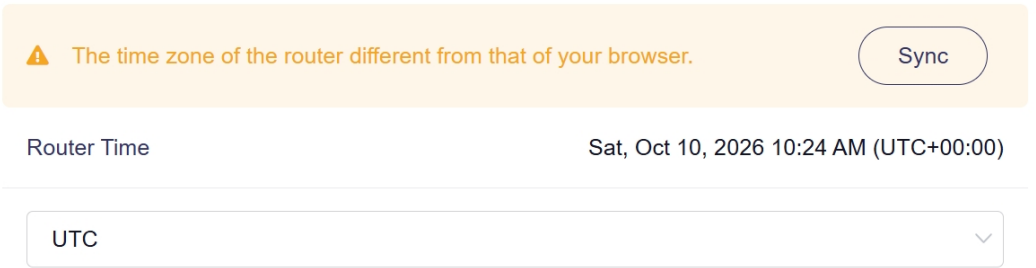
1. Mínimo 10 caracteres y máximo 63 caracteres de longitud.
2. Letras (distinguen entre mayúsculas y minúsculas), números y símbolos (por ejemplo, ! @ # $ % ^ & * ( ) _ + - = , . > < | ? / \ [ ] { } : ; " ' ` ~) son permitido.
3. Se requieren al menos dos tipos (letras mayúsculas, minúsculas, números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

13.5 Zona horaria

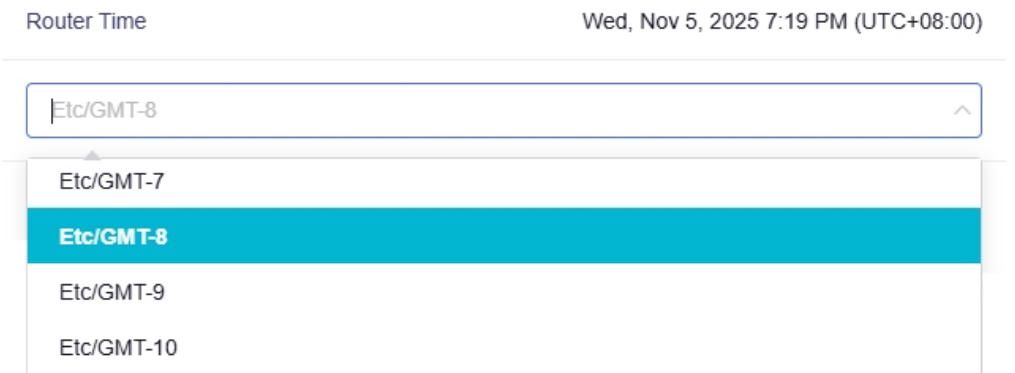
Inicie sesión en el administrador web de su enrutador panel y navegue hasta **SISTEMA** > **Zona horaria** Esta página muestra su. hora del sistema del enrutador, que indica la fecha, la hora y el desplazamiento de zona horaria correspondiente.



Algunas funciones dependen del sistema del enrutador' 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 **Sincronización** para sincronizar la zona horaria.

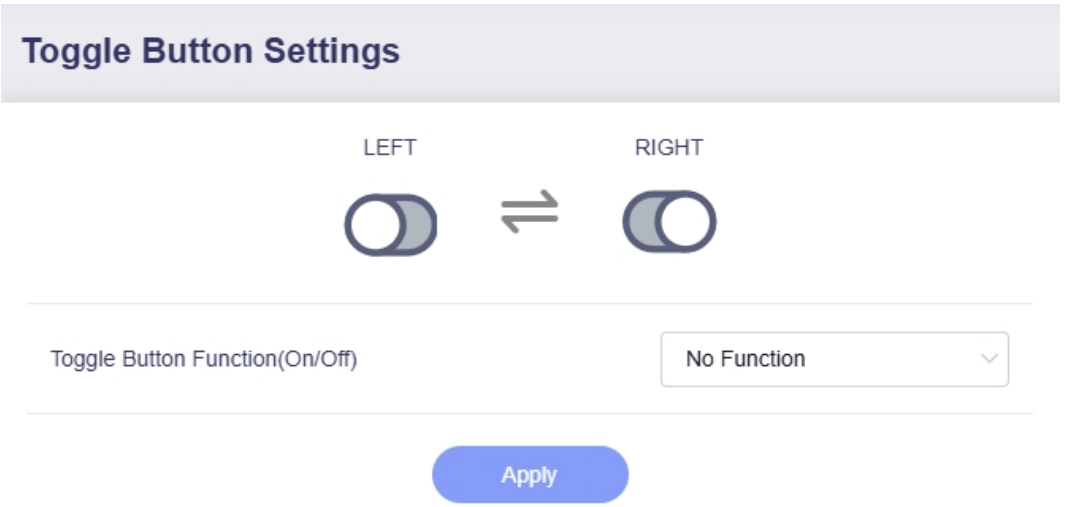


Para cambiar zona horaria, sseleccione la zona horaria apropiada de la lista para garantizar la del enrutador. La hora del sistema coincide con su hora local.

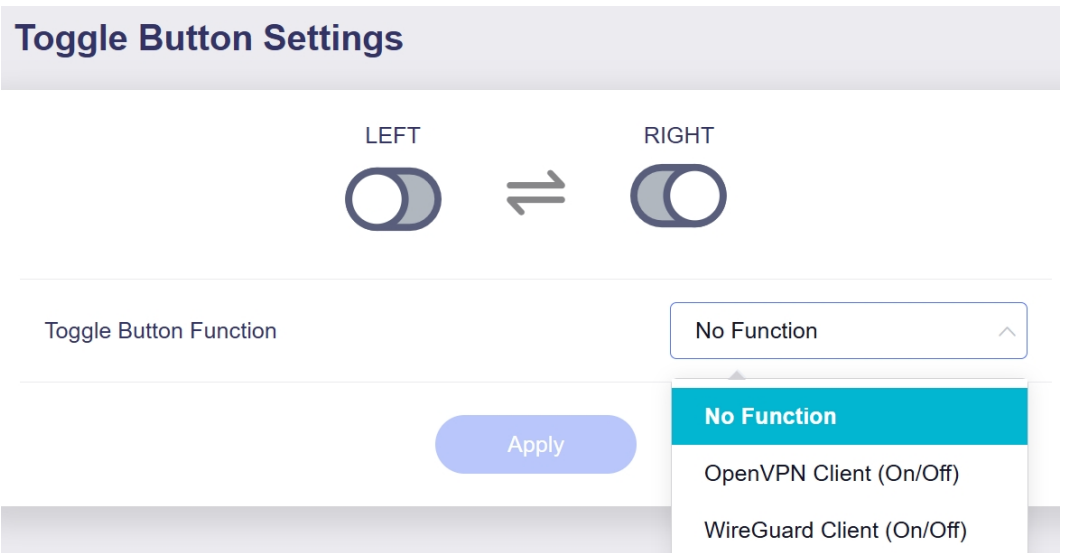


13.6 Configuración del botón de alternancia

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

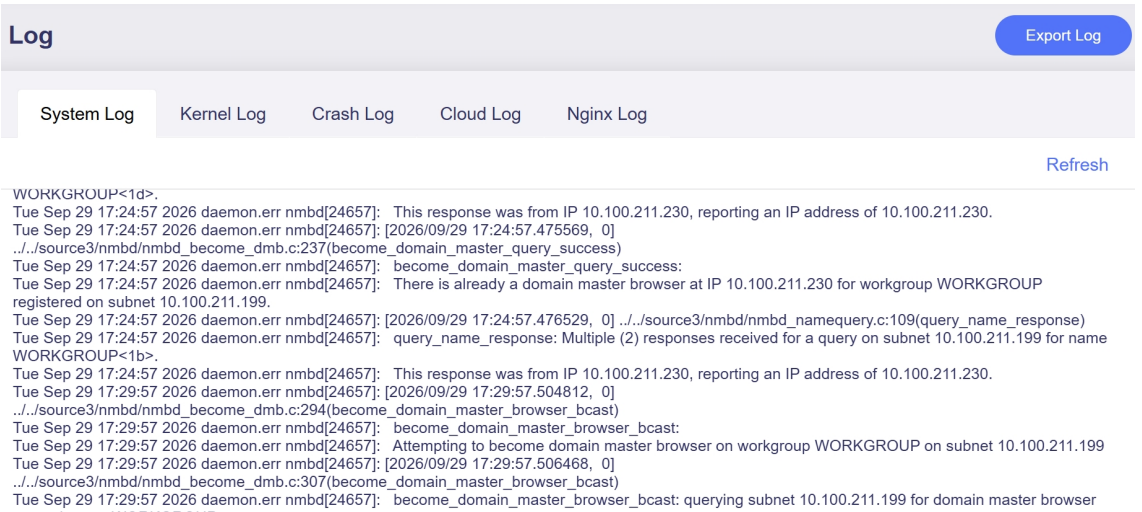


De forma predeterminada, el interruptor de palanca no tiene asignada ninguna función. personalícelo si es necesario para activar o desactivar funciones específicas con un solo giro.



13.7 Registro

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

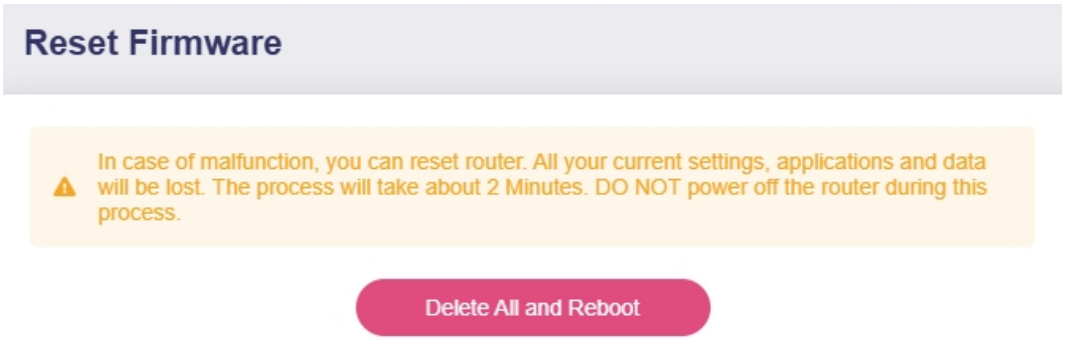


- **Actualizar**: Haga clic en este botón para actualizar registros.
- **Exportar registro**: Haga clic en este botón para exportar información de depuración junto con los registros.

13.8 Restablecer firmware

Si el enrutador no funciona correctamente, puede intentar resolving solucione el problema reiniciando 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 Reinicie** para restablecer el firmware si es necesario.



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

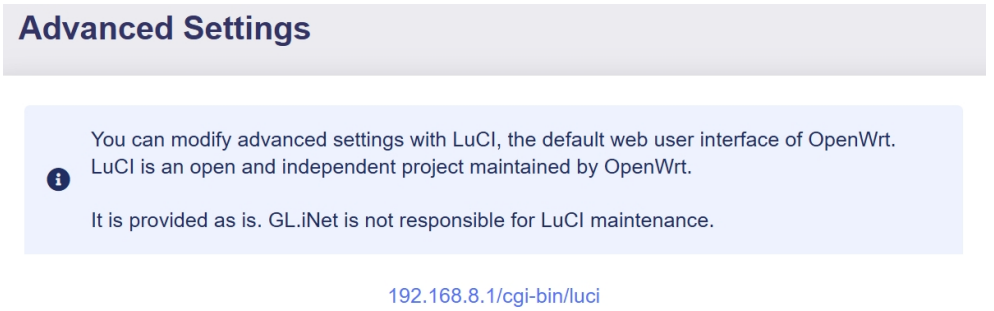
Si no puede acceder al panel de administración web del enrutador', intente restablecer su enrutador usando el botón de reinicio físico en el lado.

13.9 Configuración avanzada

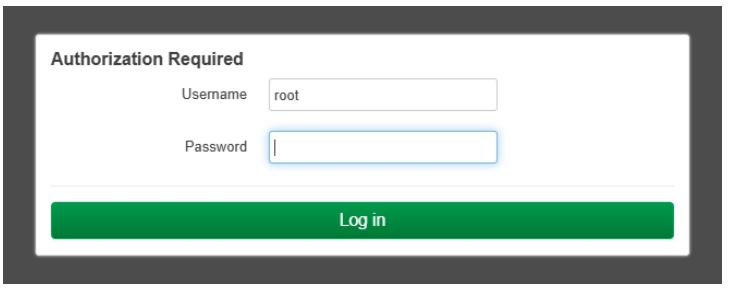
Inicie sesión en el panel de administración web de su enrutador y navegue hasta **SISTEMA** > **Configuración avanzada**. Esta página le permitemodificar la configuración avanzada a modificar configuración avanzada en LuCI, que es la interfaz de usuario web predeterminada de OpenWrt. Como proyecto abierto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

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

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



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



Yusted luego registrar en en el LuCI interfaz.

