

Manual de usuario

GL-MT5000 / Brume 3

Puerta de enlace de seguridad

Versión de firmware 4.9.0

Acerca de este manual

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

Con esta guía, podrá:

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

Convenciones de formato

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

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

Nota:

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

¿Necesita más ayuda o información?

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

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

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

Contenido

Capítulo 1 Conozca su enrutador 6
1.1 Descripción general del producto 7
1.1.1 Apariencia 7
1.1.2 Interfaz y botón 8
1.1.3 LED 9
1.2 Especificaciones 9
1.3 Contenido del paquete 10
Capítulo 2 Conexión de hardware 11
2.1 Elección de una ubicación 12
2.2 Conexión del enrutador 12
Capítulo 3 Iniciar sesión en el enrutador 13
Capítulo 4 Configurar la conexión a Internet 15
4.1 Usar el asistente de configuración rápida 16
4.2 Configurar manualmente la conexión a Internet 17
4.2.1 Conectarse a Internet mediante un cable Ethernet 18
4.2.2 Conectarse a Internet mediante conexión compartida por USB 22
4.2.3 Conectarse a Internet mediante un módem USB 27
Capítulo 5 Clientes 29
5.1 Detalles del dispositivo 31
5.2 Acción 33
5.3 Eliminar clientes 36
5.4 Ordenar 37
Capítulo 6 Servicios en la nube 38
6.1 GoodCloud 39
6.1.1 Habilitar GoodCloud 40
6.1.2 Administrar el enrutador 43
6.1.3 Desvincular el dispositivo 48
6.1.4 Desactivar GoodCloud 48
6.2 AstroWarp 49
6.2.1 Configuración rápida 49
6.2.2 Comprobar la conectividad 53
6.2.3 Plan de actualización 54

Capítulo 7 Conozca la VPN 55
7.1 Introducción 56
7.2 Escenarios de aplicación 57
Capítulo 8 Panel de VPN 59
8.1 Cargar perfil VPN 60
8.2 Agregar túnel VPN 63
8.2.1 Pasos generales 63
8.2.2 Referencia del caso 66
8.3 Bloqueo de tráfico sin VPN (Kill Switch) 82
8.4 Todo el resto del tráfico 83
8.5 Opciones de túnel 84
8.6 Prioridad del túnel 86
Capítulo 9 Configurar el servidor VPN 88
9.1 Configurar el servidor OpenVPN 89
9.1.1 Preparación 89
9.1.2 Pasos de configuración 90
9.1.3 Solución de problemas 92
9.2 Configurar el servidor WireGuard 94
9.2.1 Preparación 94
9.2.2 Pasos de configuración 95
9.2.3 Solución de problemas 98
Capítulo 10 Configurar el cliente VPN 100
10.1 Configurar el cliente OpenVPN 101
10.1.1 Preparación 101
10.1.2 Configurar NordVPN 101
10.1.3 Configurar el cliente OpenVPN manualmente (para otros proveedores) 107
10.2 Configurar el cliente WireGuard 110
10.2.1 Preparación 110
10.2.2 Configurar AzireVPN 111
10.2.3 Configurar Hide.me 115
10.2.4 Configurar IPVanish 118
10.2.5 Configurar Mullvad 122
10.2.6 Configurar NordVPN 126
10.2.7 Configurar PIA (Private Internet Access) 131

10.2.8 Configurar PureVPN 135
10.2.9 Configurar Surfshark 138
10.2.10 Configurar Windscribe 142
10.2.11 Configurar el cliente WireGuard manualmente (para otros proveedores) . 146
Capítulo 11 Red 151
11.1 Multi-WAN 152
11.1.1 Seguimiento del estado de la interfaz 152
11.1.2 Modo Multi-WAN 156
11.2 LAN 159
11.2.1 Configuración básica 159
11.2.2 Servidor DHCP 160
11.2.3 Reserva de direcciones 162
11.3 DNS 163
11.3.1 Configuración del servidor DNS 164
11.3.2 Editar hosts 168
11.4 Puerto Ethernet 169
11.5 IPv6 170
11.5.1 Modo IPv6 171
11.5.2 Método de obtención de DNS 171
11.6 Inspección IGMP 172
11.7 Modo de red 173
11.8 Puerta de enlace directa 175
11.9 Aceleración de red 177
Capítulo 12 Control de flujo 179
12.1 Motor DPI 180
12.2 Estadísticas de datos 182
12.2.1 Configuración rápida 182
12.2.2 Reglas de almacenamiento de datos 184
12.2.3 Cambiar el intervalo de tiempo 184
12.2.4 Borrar estadísticas 185
12.3 Filtro de contenido 186
12.4 Calidad de servicio (QoS) 188
12.5 Gestión inteligente de colas (SQM) 190
12.6 Control parental 192

Capítulo 13 Seguridad 198
13.1 Reenvío de puertos 199
13.1.1 DMZ 199
13.1.2 Reenvío de puertos 200
13.2 Lista de control de acceso (ACL) 202
13.3 Acceso de administrador 204
13.3.1 Control de acceso 204
13.3.2 Control de acceso remoto 207
13.3.3 Abrir puertos en el enrutador 208
13.4 Modo NAT 210
Capítulo 14 Aplicaciones 211
14.1 Complementos 212
14.2 DNS dinámico 213
14.2.1 Habilitar DDNS 213
14.2.2 Comprobar si DDNS funciona 216
14.2.3 Acceso remoto HTTPS 218
14.2.4 Acceso remoto SSH 220
14.3 Almacenamiento en red 222
14.3.1 Conectar una unidad de almacenamiento 222
14.3.2 Configurar Samba 223
14.3.3 Configurar WebDAV 226
14.3.4 Configurar DLNA 229
14.4 AdGuard Home 230
14.5 Tailscale 232
14.5.1 Configurar Tailscale 233
14.5.2 Anunciar subredes WAN 236
14.5.3 Anunciar subredes LAN 237
14.5.4 Nodos de salida personalizados 238
14.5.5 Activar el nodo de salida 239
14.6 ZeroTier 246
14.6.1 Configurar ZeroTier 247
14.6.2 Permitir el acceso remoto a la WAN 251
14.6.3 Permitir el acceso remoto a la LAN 252
14.7 Tor 253

Capítulo 15 Sistema 254
15.1 Descripción general 255
15.2 Contraseña de administrador 256
15.3 Actualización 257
15.3.1 Actualización en línea 257
15.3.2 Actualización local 258
15.4 Tareas programadas 260
15.4.1 Programación de los indicadores LED 260
15.4.2 Programar reinicio 261
15.5 Zona horaria 262
15.6 Restablecer firmware 263
15.7 Registro 264
15.8 Configuración avanzada 266

Capítulo 1

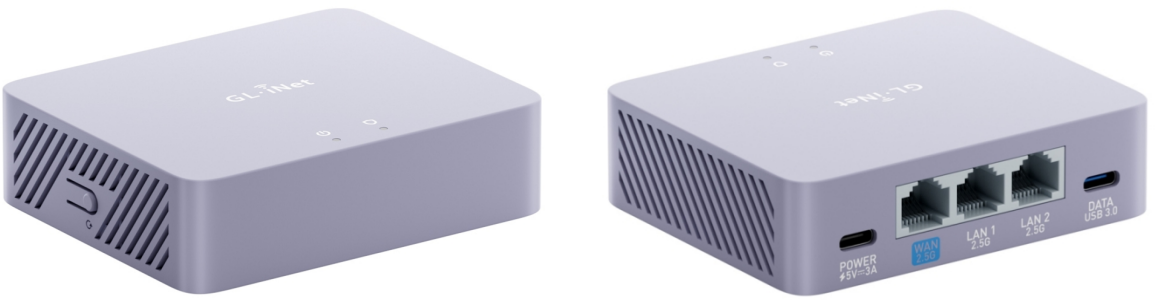
Conozca su enrutador

Este capítulo cubre la descripción general, las especificaciones y el contenido del paquete del enrutador.

1.1 Descripción general del producto

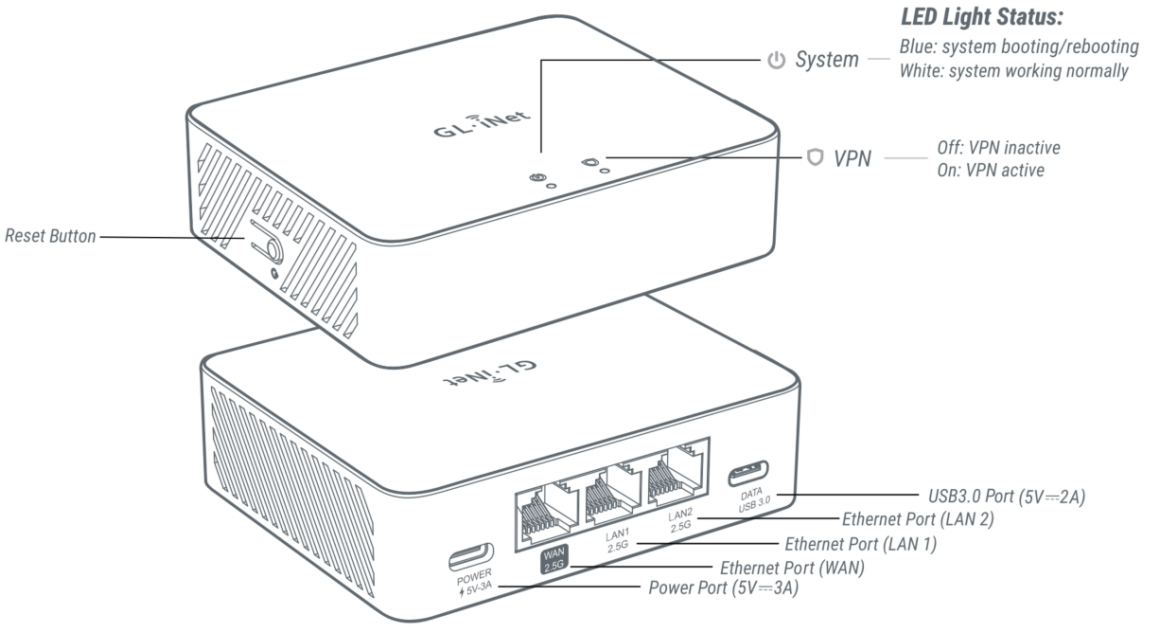
Brume 3 (GL-MT5000) es una puerta de enlace de seguridad de alto rendimiento, equipada con una CPU MediaTek Quad-core, 1 GB de RAM y 8 GB de almacenamiento eMMC. Presenta un diseño compacto, ideal para implementaciones con limitaciones de espacio y admite alojamiento VPN doméstico, así como más de 30 servicios VPN. Además, viene con la función DPI de GL.iNet, control parental y AdGuard Home, lo que satisface las diversas necesidades de los entusiastas de la tecnología y los usuarios empresariales.

1.1.1 Apariencia





1.1.2 Interfaz y botón



Artículo	Descripción
Puerto de alimentación	Se conecta al adaptador de corriente.
Puerto WAN 2.5G	Se conecta a un módem o a una toma Ethernet para Internet.
Puerto LAN 2.5G	Se conecta a dispositivos cableados si es necesario.
Puerto USB 3.0	Para dispositivos de almacenamiento USB, conexión USB de teléfono y dongles celulares compatibles.
Botón Restablecer	Presione y mantenga presionado durante **4 segundos** y luego suelte para reparar su red. El LED se volverá azul y parpadeará lentamente hasta que la red está restaurada.
	Presione y mantenga presionado durante **10 segundos** y luego suelte para restablecer enrutador a los valores predeterminados de fábrica. El LED se volverá azul y parpadeará rápidamente. Todos los datos se borrarán cuando el LED se vuelva fijo azul.

1.1.3 LED

LED	Estado
Sistema	Azul: Arranque del sistema
	Blanco: Conectado a Internet
VPN	Desactivado: VPN inactiva
	Activado: VPN activa

1.2 Especificaciones

Interfaz	1 puerto Ethernet WAN 2,5G 2 puertos Ethernet LAN 2.5G 1 x puerto USB 3.0 tipo C 1 x puerto de alimentación tipo C 1 x botón Restablecer
CPU	MediaTek, cuatro núcleos a 2,0 GHz
Memoria/Almacenamiento	DDR4 1GB / eMMC 8GB
Velocidad de Ethernet	10/100/1000/2500Mbps
Entrada de energía	Tipo C, 5V/3A
Consumo de energía	< 5W
Temperatura de funcionamiento	0 ~ 40°C (32 ~ 104°F)
Temperatura de almacenamiento	-20 ~ 70°C (-4 ~ 158°F)
Dimensión/Peso	75 x 92 x 25 mm/148 g
Otras herramientas	Hoja de datos / Firmware / Aplicación / Unboxing / Tutoriales

1.3 Contenido del paquete

El paquete incluye:

- 1 x Brume 3 (GL-MT5000)
- 1 x Manual del usuario (Guía de inicio rápido)
- 1 cable Ethernet
- 1 x Tarjeta de agradecimiento
- 1 x adaptador de corriente
- 1 x Convertidor (Dependiendo de su país de envío)



1 x User manual



1 x Thank you card



1 x Brume 3 (GL-MT5000)



1 x Ethernet cable



1 x Power adapter



Converters
(*Base on your shipping countries*)

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 refrigeración**: coloque el enrutador en un área fresca y bien- ventilada para una adecuada disipación del calor.
- **Central Ubicación**: coloque el enrutador en un lugar donde pueda conectarse fácilmente a la alimentación y a varios dispositivos (por ejemplo, la zona central de la sala de estar zona).
- **Cable conveniencia**: enrute los cables y el cable de alimentación de forma segura para evitar peligro de tropiezo.
- **Superficie estable**: coloque el enrutador en una superficie plana y horizontal (estante, escritorio) para mayor estabilidad.

2.2 Conexión del enrutador

1. **Encendido**

   Junte el adaptador de corriente de dos piezas. Conéctelo a su Brume 3 y enchúfelo a una toma de corriente. Se iniciará automáticamente.
2. **Conecte un dispositivo al enrutador**

   Conecte un dispositivo con cable (por ejemplo, una computadora o computadora portátil) al puerto LAN del Brume 3’con un cable Ethernet.
3. **Inicie sesión en el enrutador**

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

Capítulo 3

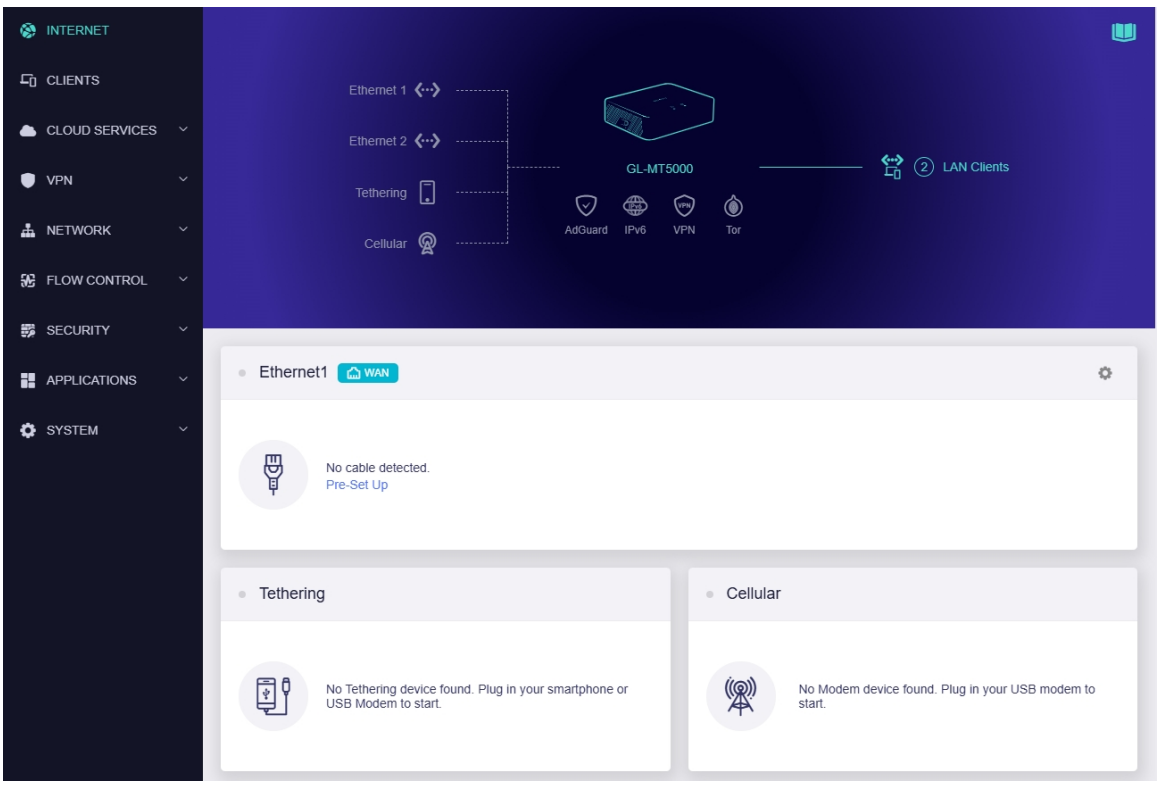
Iniciar sesión en el enrutador

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

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

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 puerto LAN del Brume 3’con un cable Ethernet.
2. Abra un navegador web (se recomienda Chrome y Edge) y visita http://192.168.8.1. You will be directed to the página de inicio de sesión de la web admin panel. Si no puede acceder a la web undmin panel, consulte aquí para solucionar problemas.
3. Sconfigure su contraseña de administrador. Se recomienda una contraseña segura por motivos de seguridad. Luego haga clic en **Siguiente** para continuar.
4. Yluego ingresará el Brume 3’s web admin panel.



Capítulo 4

Configurar la conexión a Internet

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

4.1 Usar el asistente de configuración rápida

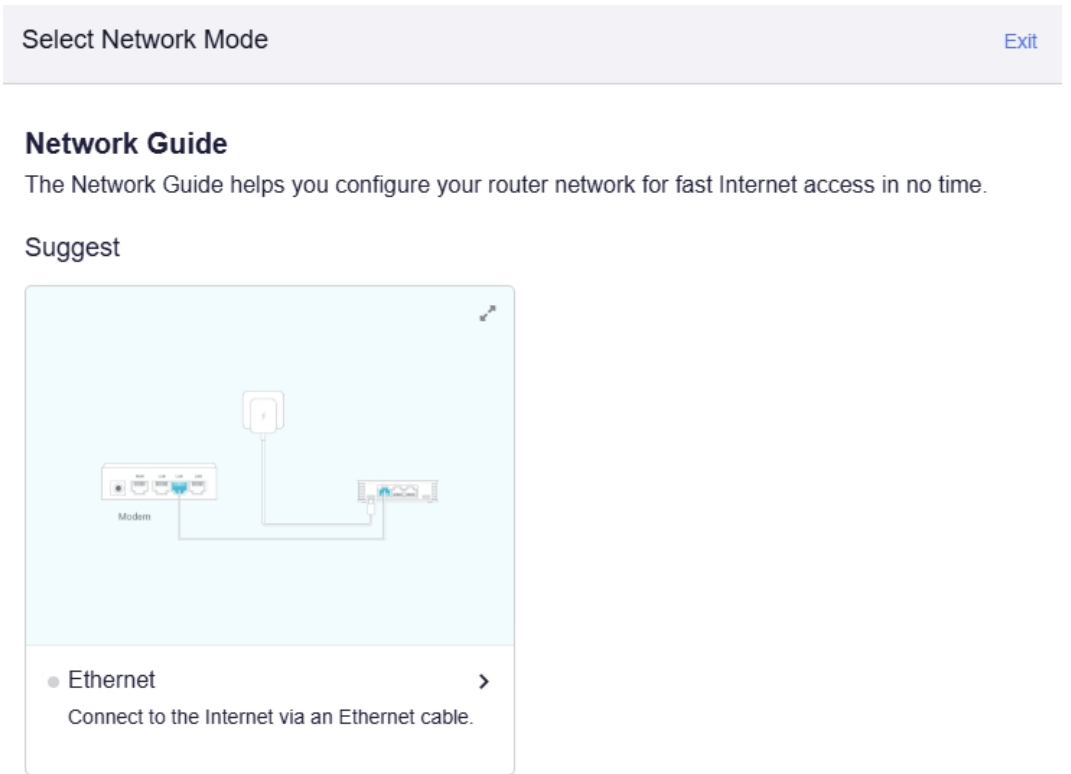
El asistente de configuración basado en web lo guiará a través de la configuración de la red del enrutador.

Siga los pasos a continuación para iniciar el asistente.

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



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



4.2 Configurar manualmente la conexión a Internet

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

Brume 3 admite tres métodos de conexión a Internet: Ethernet, Anclaje a red USB y módem/celular USB. Celija el método adecuado según sus necesidades de uso.

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

2. **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.

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

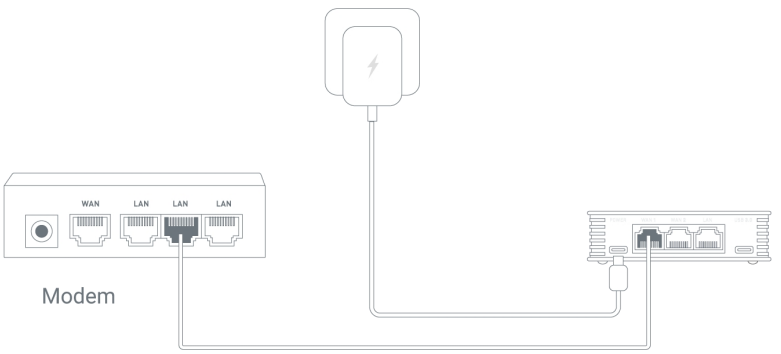
4.2.1 Conectarse a Internet mediante un cable Ethernet

Conecte el enrutador a una red de banda ancha usando 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.

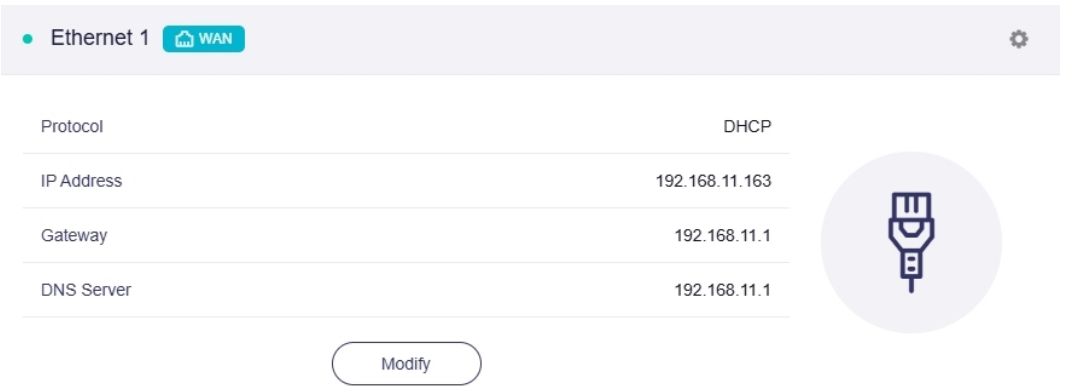
Configuración básica

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

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

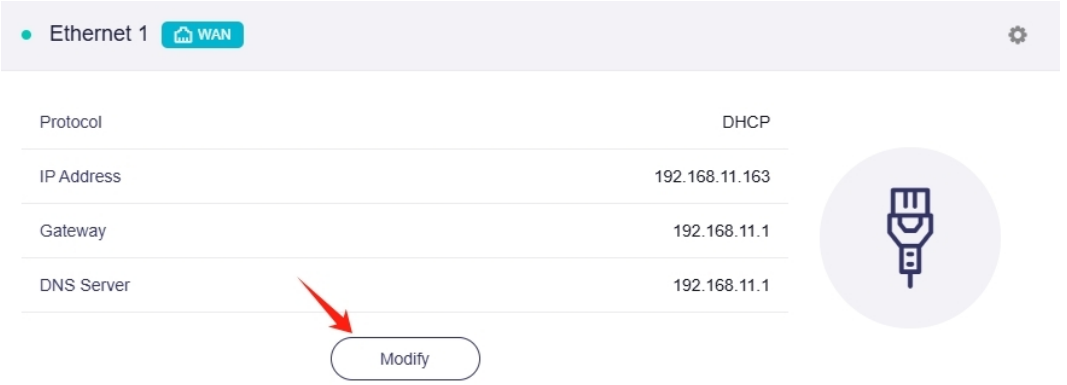


2. Inicie sesión en el panel de administración web del enrutador' y navegue a **INTERNET** > **Ethernet**. Si la conexión se realiza correctamente, la sección Ethernet mostrará red detalles, incluidos protocolo, dirección IP, puerta de enlace, y DNS servidor.



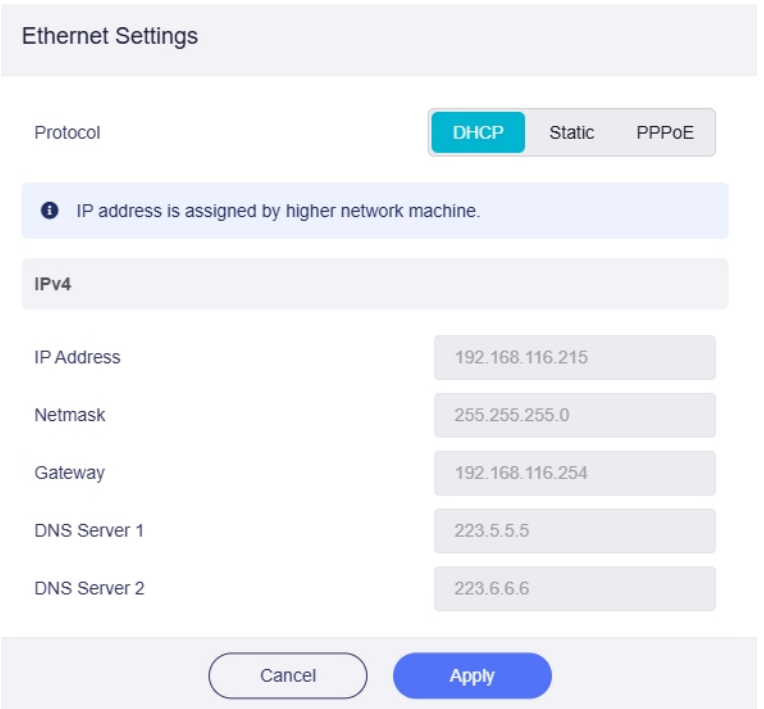
Protocolo

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



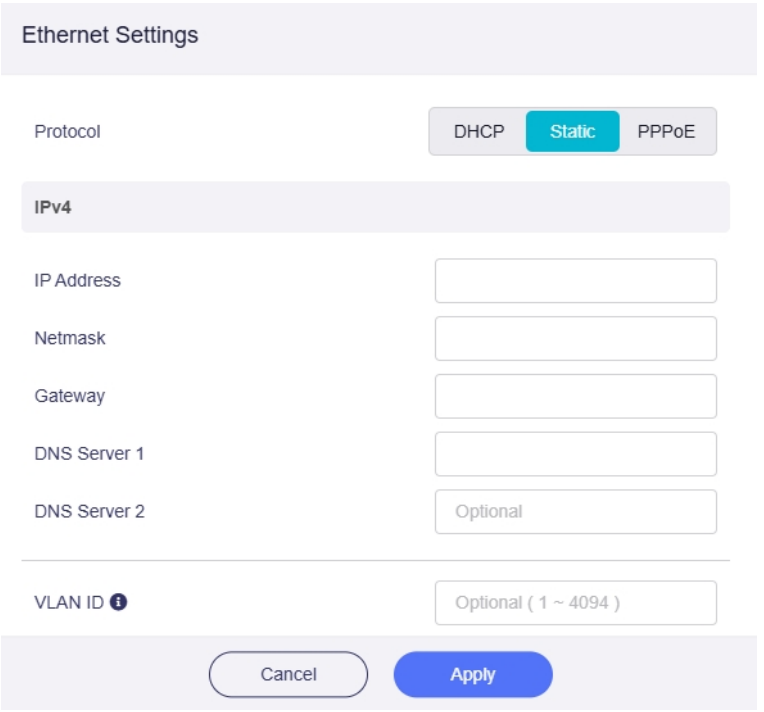
- **DHCP**

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



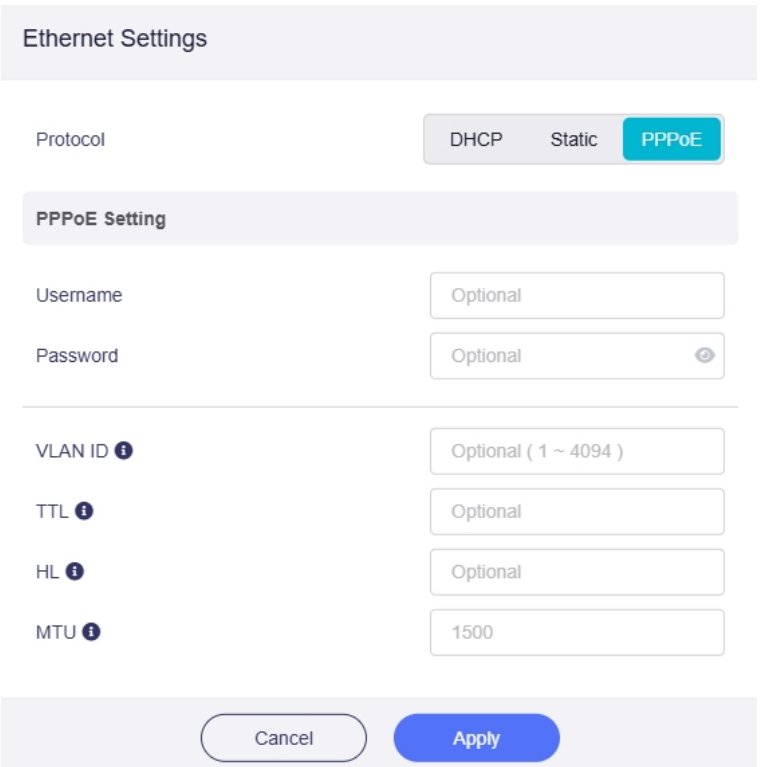
- **Estática**

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



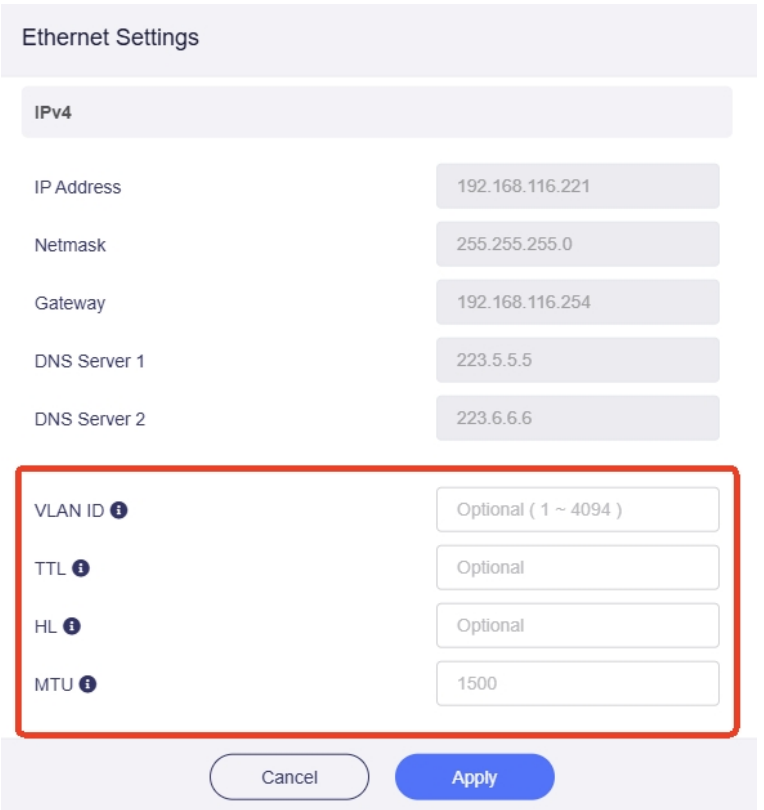
- **PPPoE**

  PPPoE (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 contraseña únicos, que son necesarios para configurar una conexión a Internet.



Configuración avanzada

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



- **ID de VLAN**

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

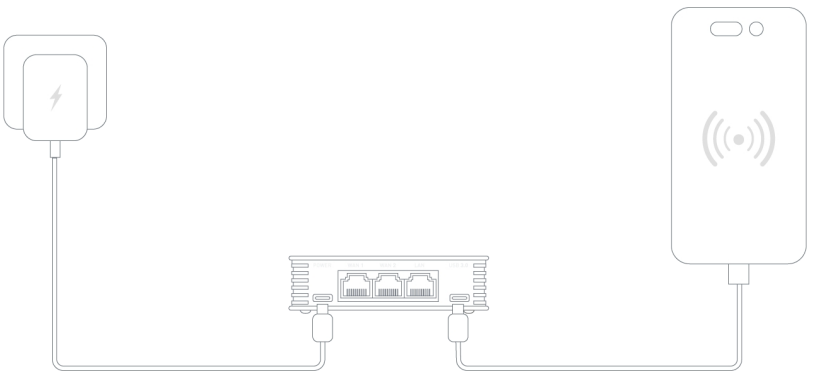
  TTL (Tiempo de vida) define el tiempo máximo que los paquetes pueden sobrevivir la red. De forma predeterminada, el enrutador disminuye en 1 el TTL de los paquetes entrantes de los dispositivos cliente antes de reenviarlos. Si necesita anularlo, puede establecer un valor fijo aquí. La configuración TTL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

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

  El valor de MTU predeterminado es 1500 bytes.

4.2.2 Conectarse a Internet mediante conexión compartida por USB

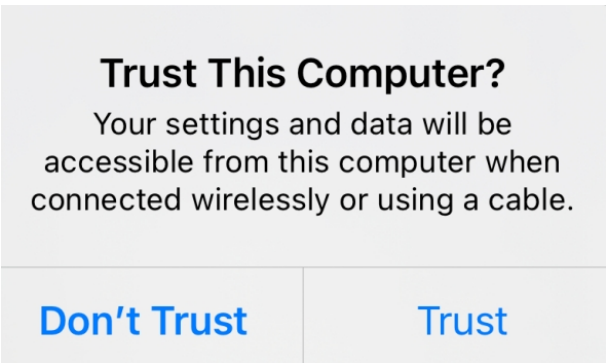
Cconexión de un inteligenteteléfono al enrutador a través de un cable USB se llama Tethering, que puede compartir la red de datos móviles del dispositivo (por ejemplo, 4G/5G) con el enrutador. Este es un método conveniente para el acceso temporal ia Internet, especialmente cuando al aire libre o en áreas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



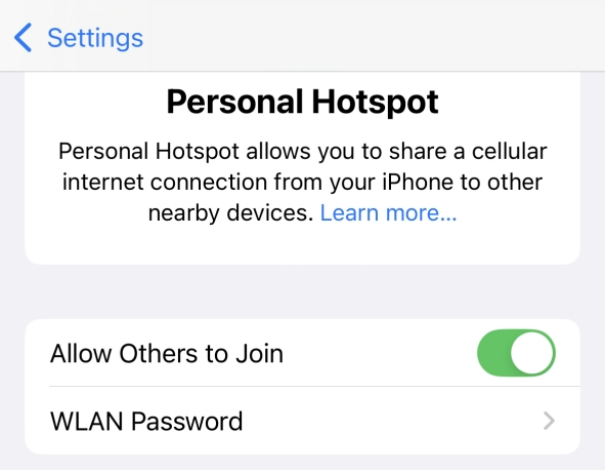
El módem sin host funciona en Tethering como bien durante la configuración del módem.
Nota: Algunos operadores de telefonía móvil limitan o cobran más por la conexión. Recomendamos consultar con su proveedor.

Conexión compartida desde un iPhone

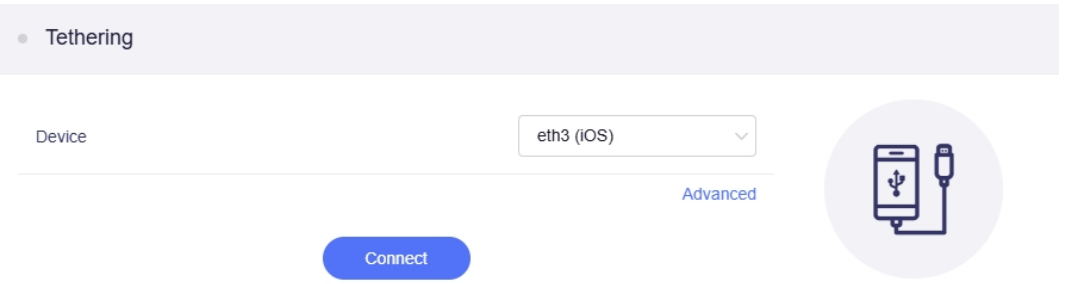
1. Conecte un iPhone al puerto USB del enrutador usando un cable USB. Aparecerá un cuadro de diálogo del sistema preguntando si se debe confiar en el dispositivo. Toque **Confiar** para continuar.



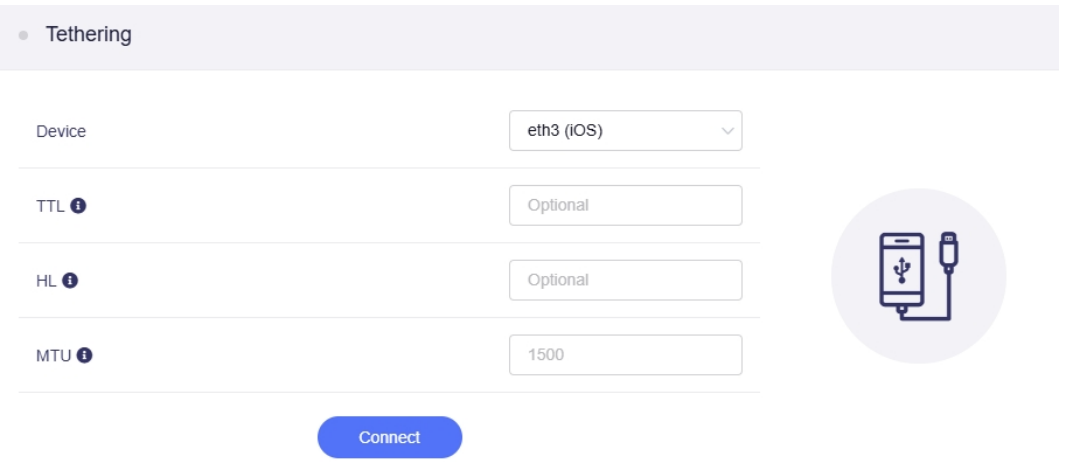
2. Ir a iPhone **Configuración** > **Punto de acceso personal**. Habilitar **Permitir que otros se unan**.



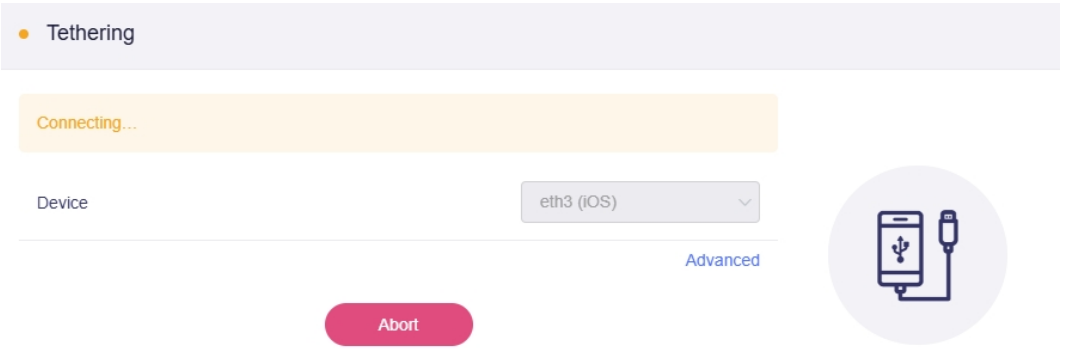
3. Conecte una computadora u otro teléfono al enrutador. Inicie sesión en el panel de administración web del enrutador y navegue hasta **INTERNET** > **Conexión**, luego haga clic en **Conectar**.



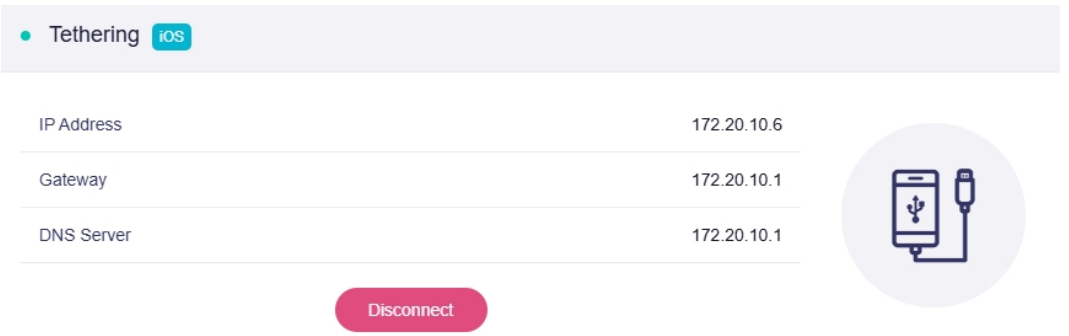
Si necesita establecer configuraciones avanzadas, como TTL, HL y MTU, haga clic **Avanzado** para personalizar estas configuraciones antes hacer clicing **Conectar**.



4. Comenzará a conectarse.

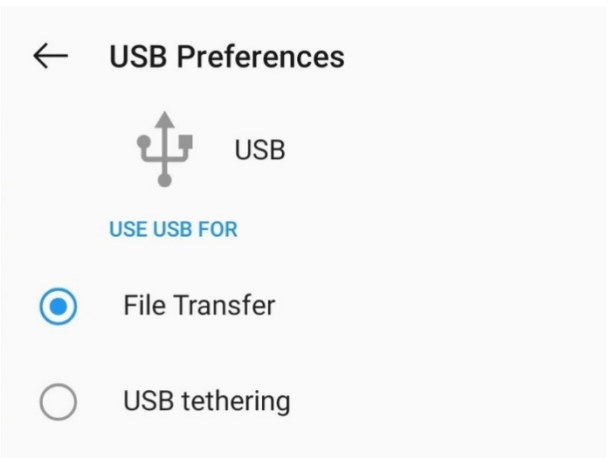


Una vez conectado, thes página mostrará los detalles.

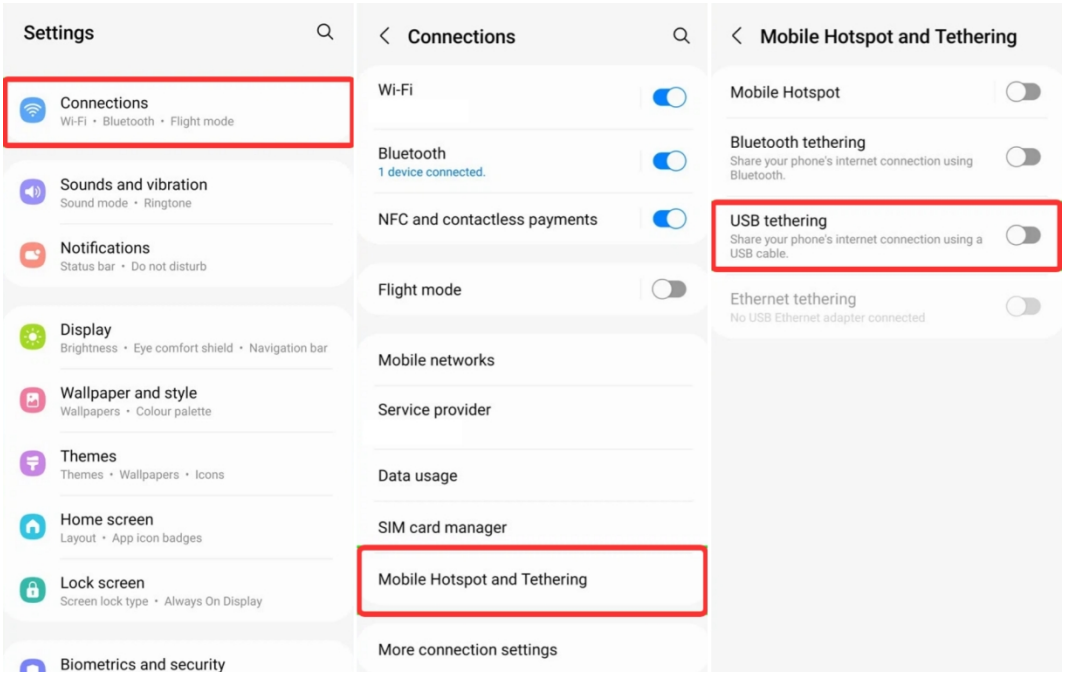


Conexión compartida desde Android

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.

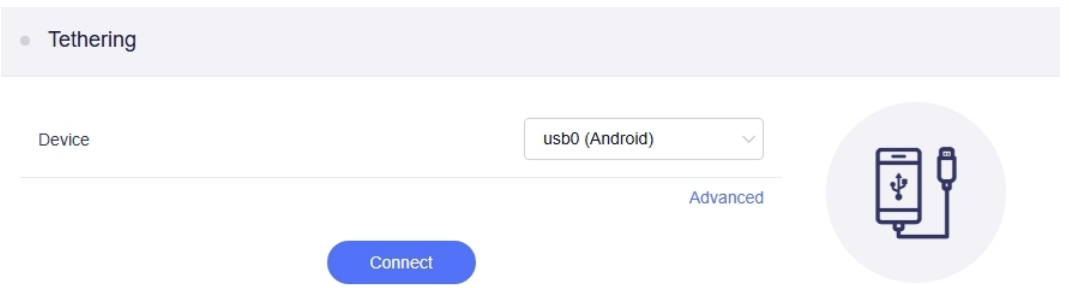


2. Vaya a la **Configuración** > **Red e Internet** > **Punto de acceso personal**. Activar **Personal Punto de acceso** o **Anclaje a red USB**.

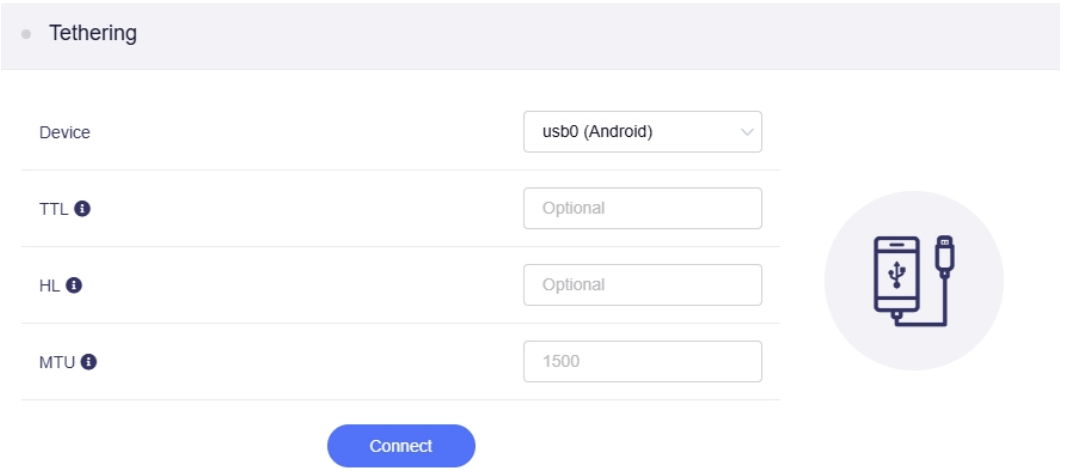


(Los pasos para habilitar el Anclaje a red USB varían según la marca. Verifique la configuración de su dispositivo para conocer la ubicación exacta y comuníquese con el soporte técnico del fabricante si es necesario).

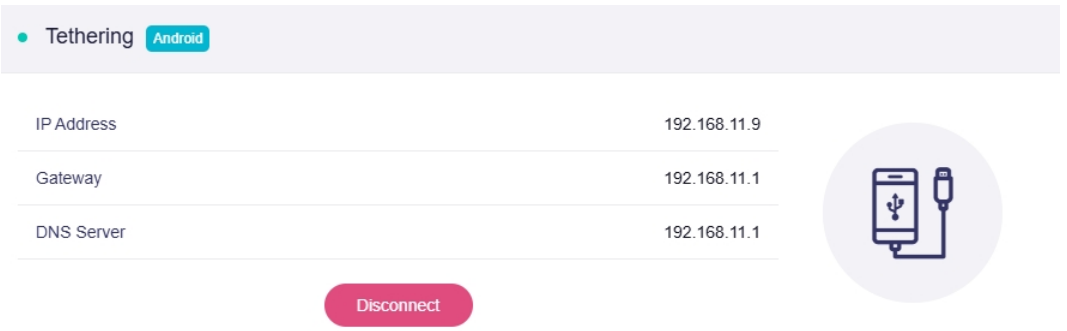
3. Conecte una computadora u otro teléfono al enrutador y luego inicie sesión. a el panel de administración web del enrutador, navegue a **INTERNET** > **Anclaje a red**. Click **Conectar**.



Si necesita establecer configuraciones avanzadas como TTL, HL y MTU, haga clic **Avanzado** para personaliza esta configuración antes de hacer clic **Conectar**.



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



Solución de problemas

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

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

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

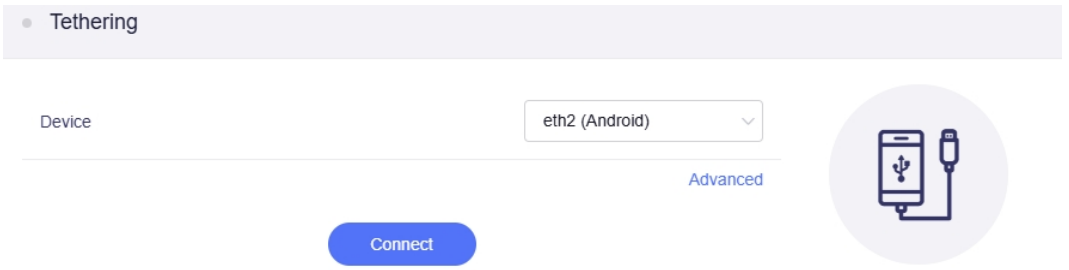
4.2.3 Conectarse a Internet mediante un módem USB

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

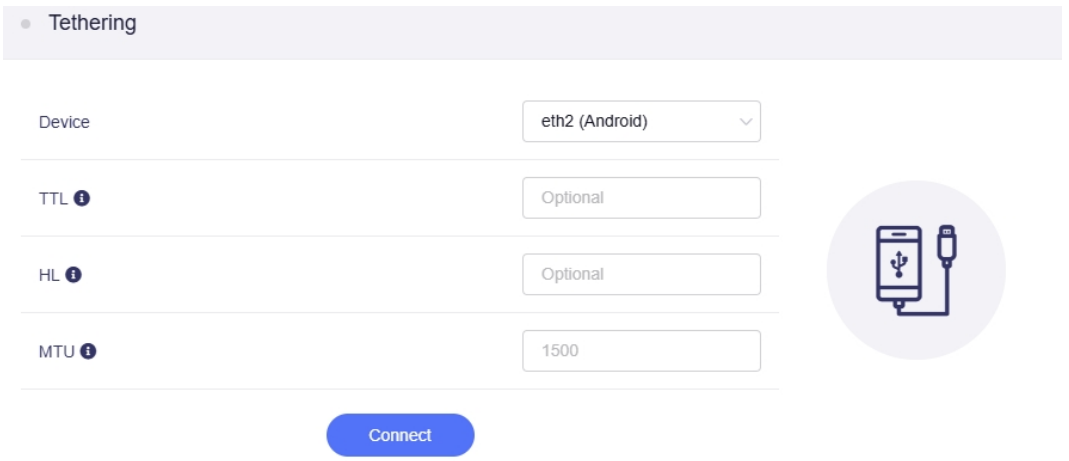
Para Brume 3, unse requiere un **adaptador USB-C a USB-A** adicional para conecte un módem USB.

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

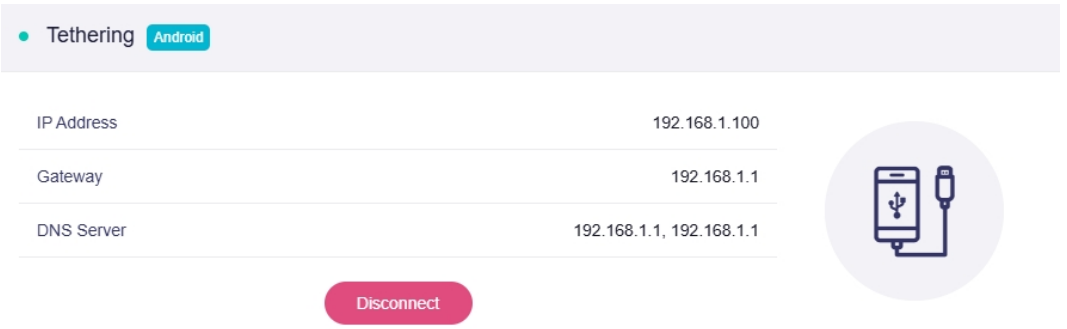
1. Pluego un módem USB con una tarjeta SIM preinstalada al puerto USB del enrutador' antes de encenderlo.
2. Inicie sesión en el enrutador's web admin panel, navegue hasta **INTERNET** > **Conexión** y luego haga clic en **Conectar**.



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

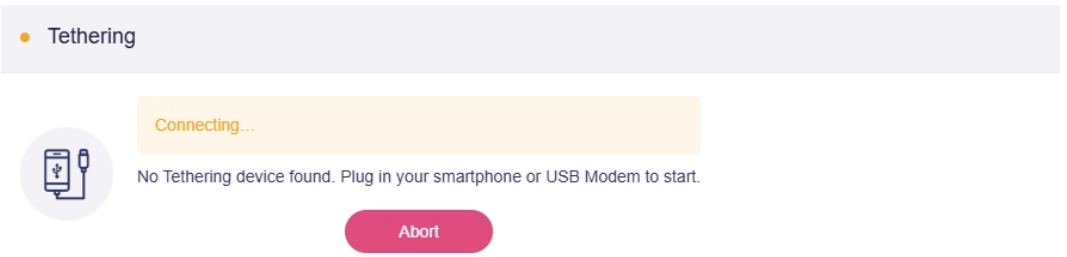


3. Comenzará a conectarse. Una vez conectado, esta página mostrará los red detalles.



Consejos:

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



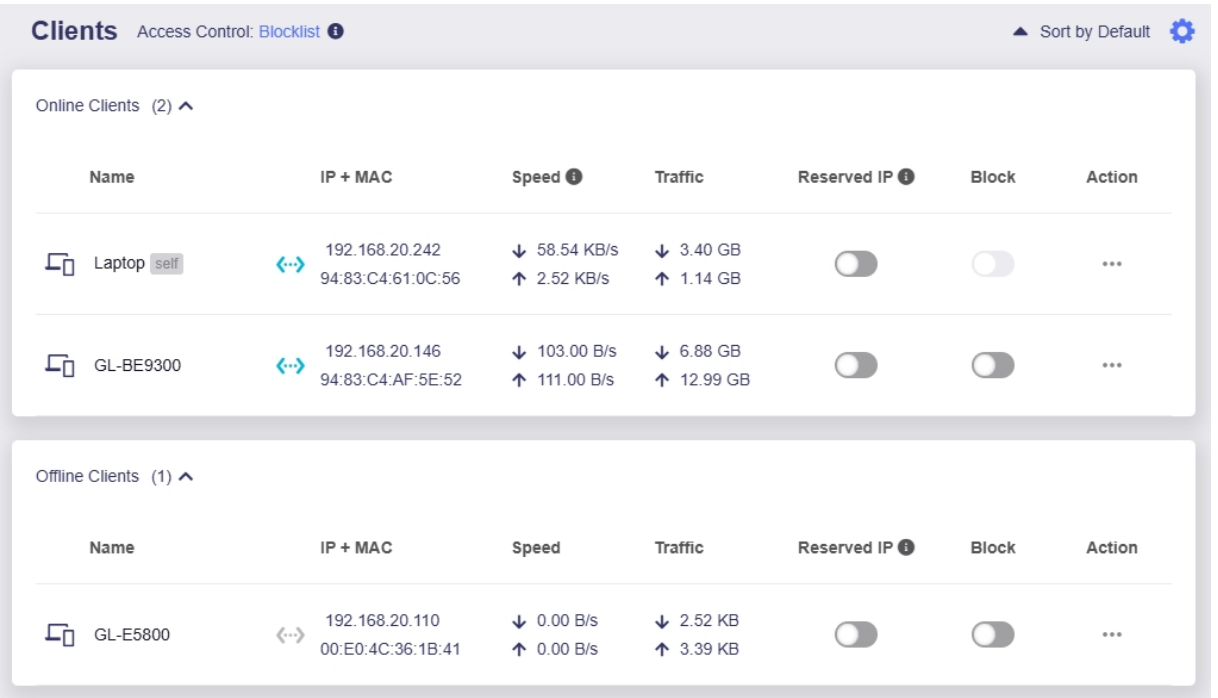
Capítulo 5

Clientes

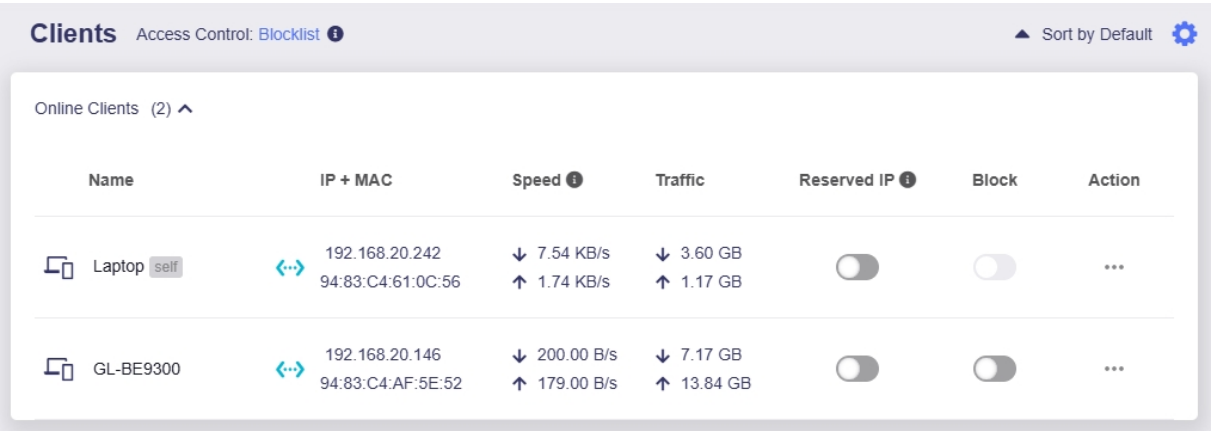
Este capítulo lo guía para ver los detalles de los dispositivos conectados y administrar sus conexiones.

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

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



5.1 Detalles del dispositivo



1. **Nombre del dispositivo**

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

2. **Dirección IP y MAC**

   La segunda columna enumera las direcciones IP y MAC de los dispositivos conectados. dispositivo.

3. **Velocidad**

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

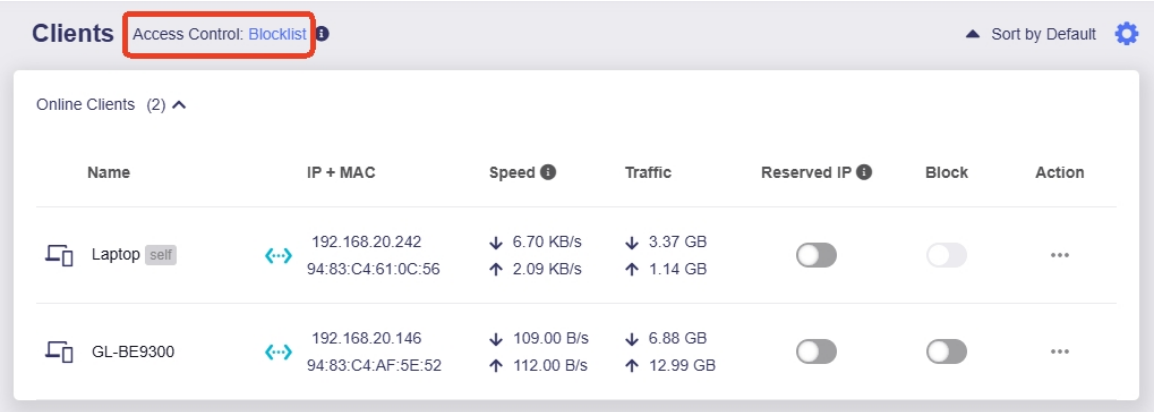
4. **Tráfico**: La cuarta columna muestra el tráfico de Internet del dispositivo conectado.

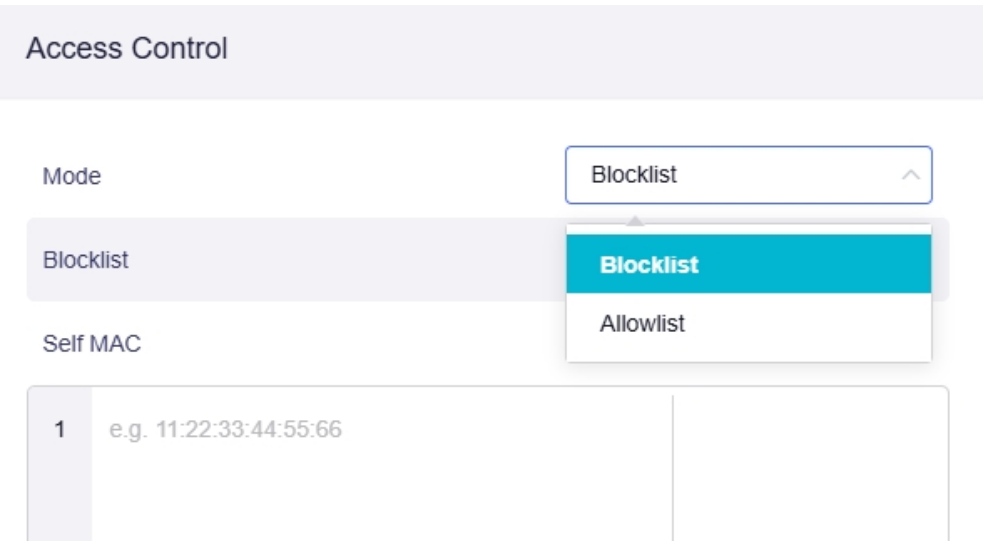
5. **Reservar IP**

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

6. **Lista de bloqueo**

   En la sexta columna, puede bloquear dispositivos conectados específicos con un clic. El Unala regla de control de Ces Lista de bloqueo de forma predeterminada y puede cambiarla a Lista de permitidos desde el top según necesario.



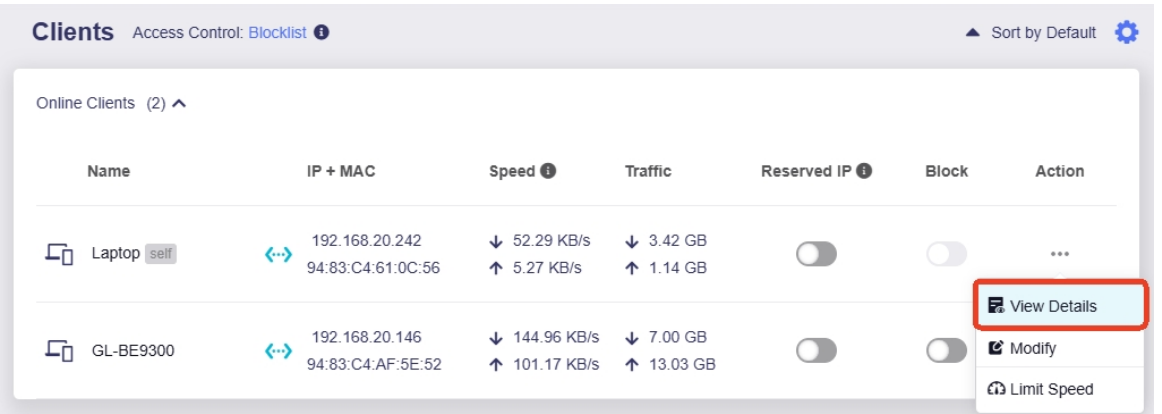


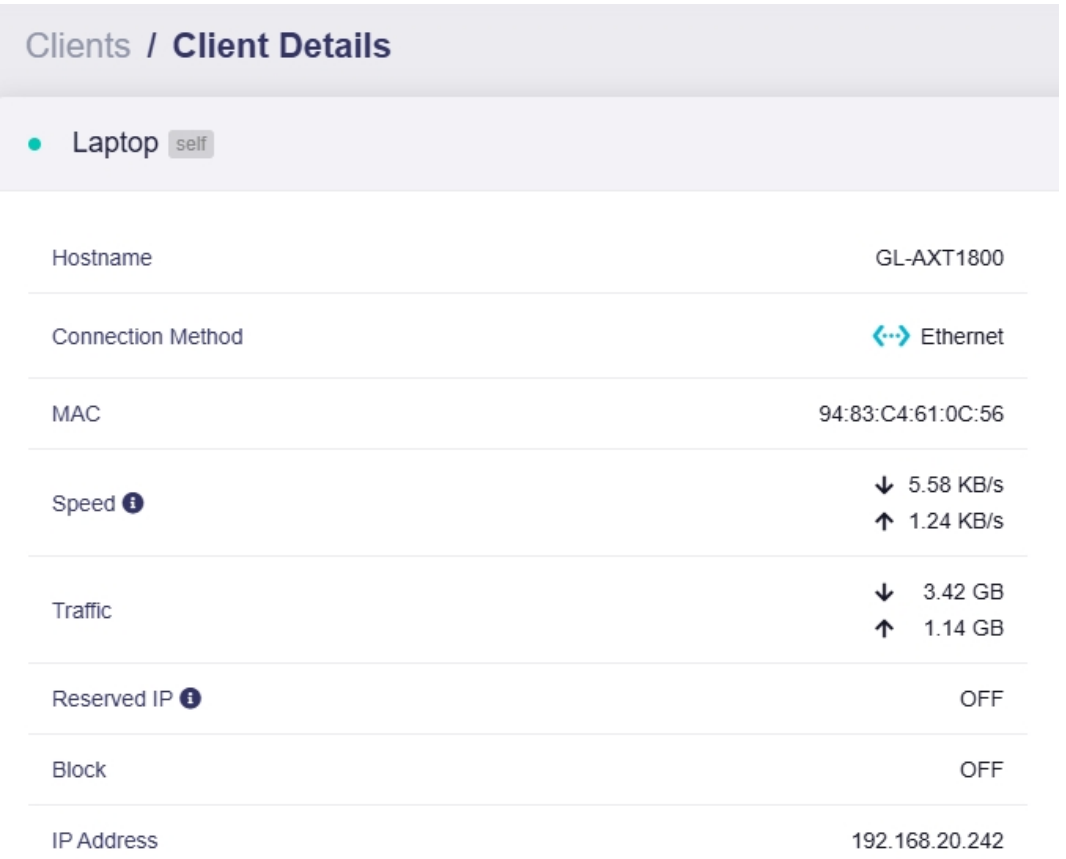
- **Lista negra**: dispositivos con direcciones MAC en el blacklist no pueden conectarse a este enrutador. Tenga en cuenta que el bloqueo del cliente se basa en la dirección MAC del dispositivo. Si el dispositivo bloqueado usa una dirección MAC diferente la próxima vez, aún podrá conectarse al enrutador.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

5.2 Acción

1. **Ver detalles**

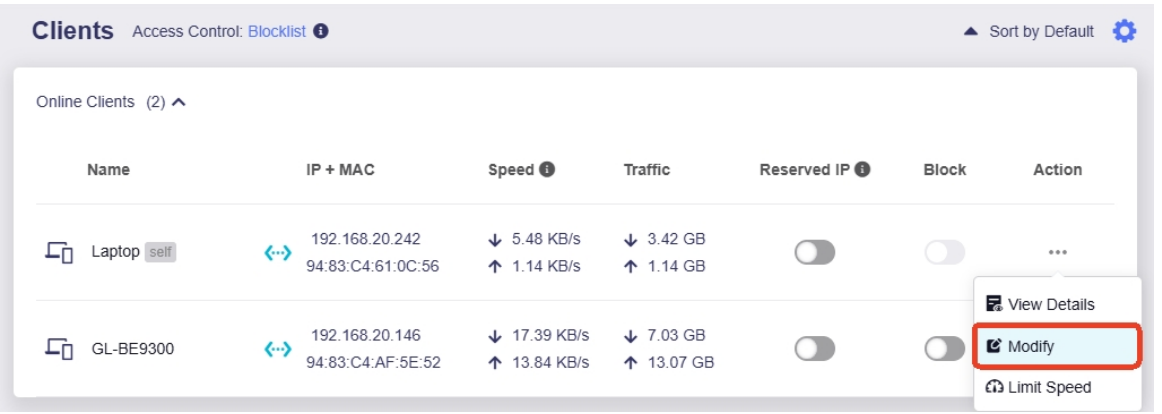
   Haga clic en el icono de tres puntos en la **Acción** columna y haga clic en **Ver detalles** en el menú desplegable para ver los detalles del dispositivo en una sola página.

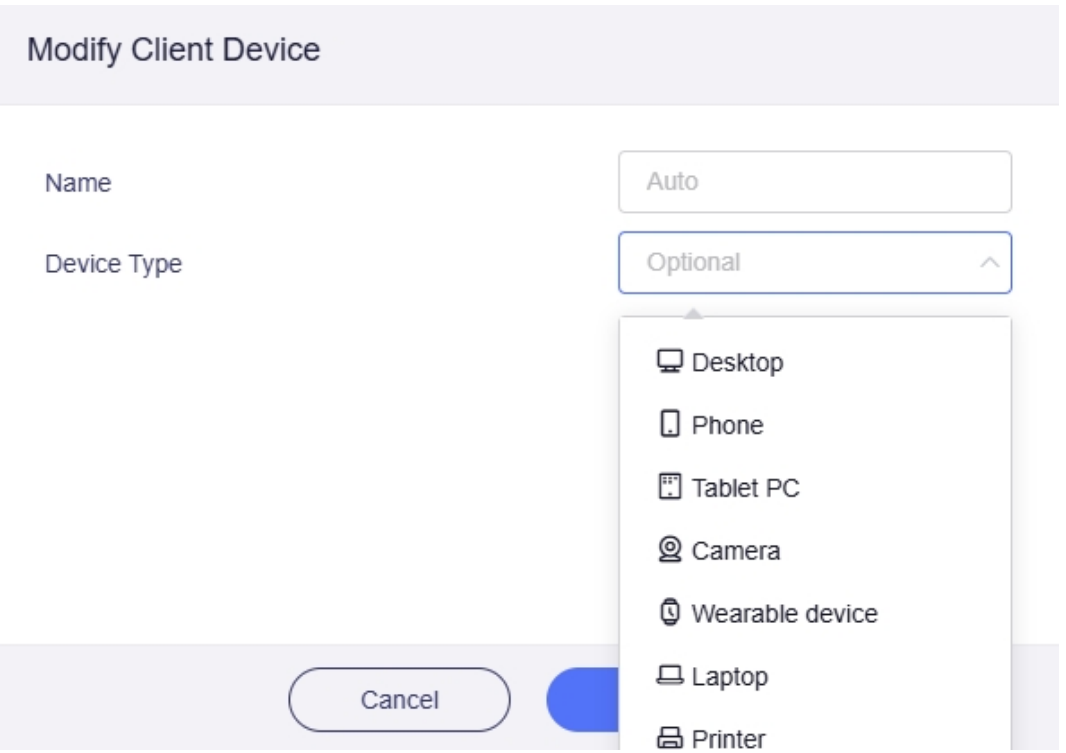




2. **Modificar**

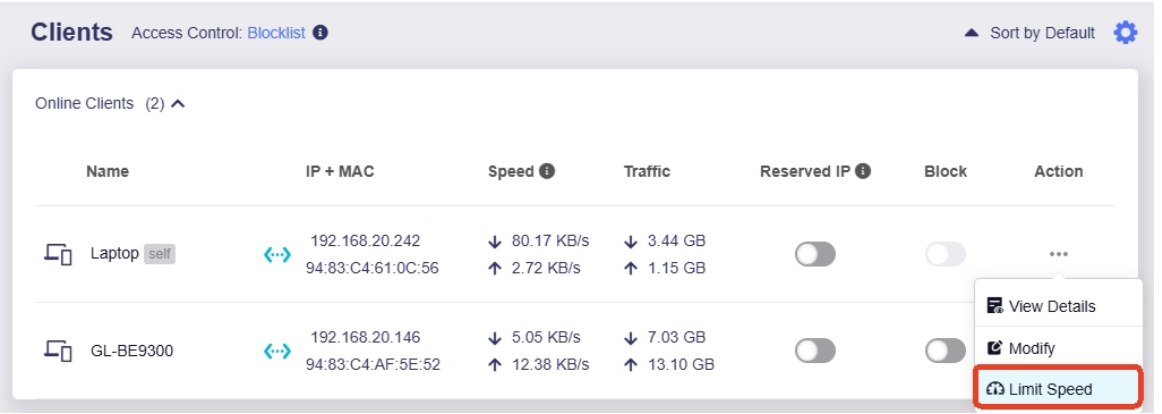
Haga clic en el icono de tres puntos en el **Acción** y haga clic en **Modificar** desde el menú desplegable menú para modificar el nombre y tipo del dispositivo.



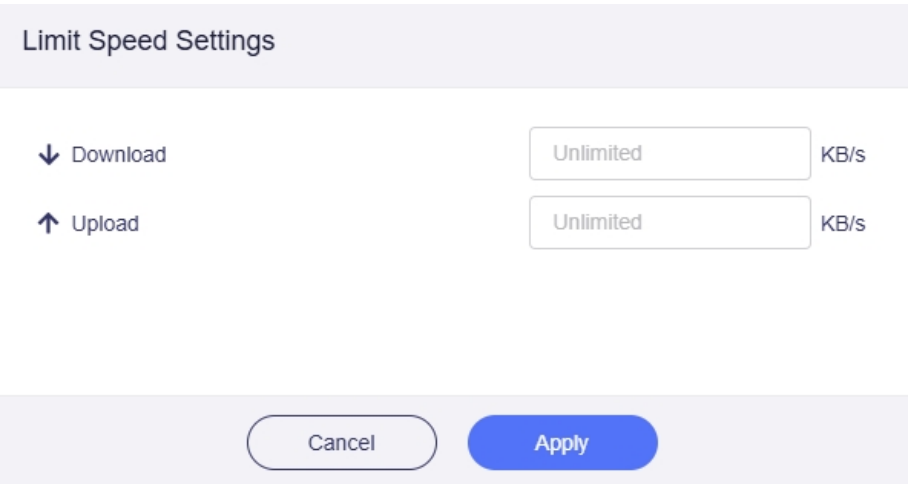


3. **Limitar velocidad**

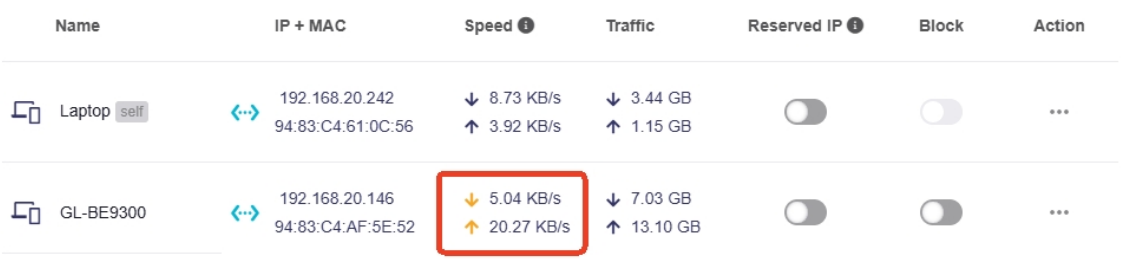
Haga clic en el icono de tres puntos en la **Acción** columna y haga clic en **Limitar velocidad** en el menú desplegable.



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



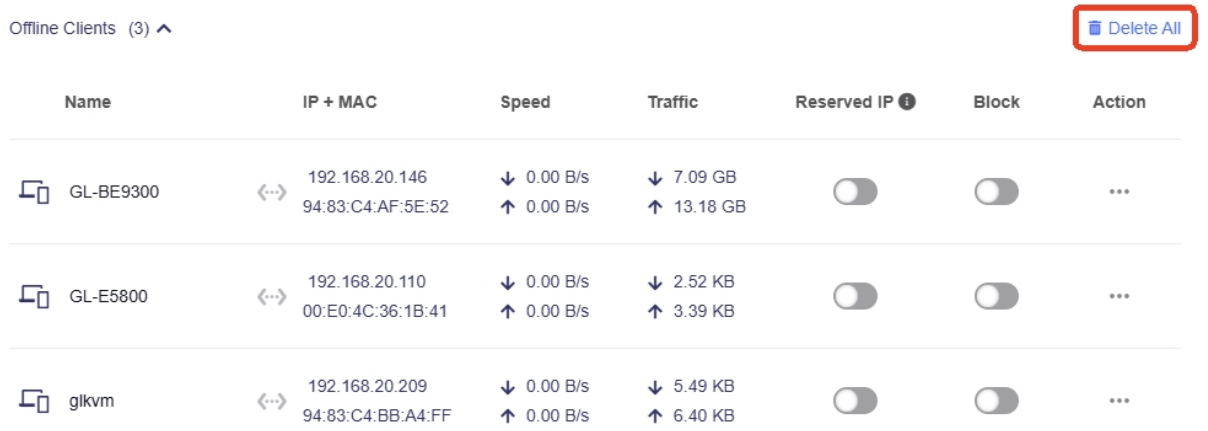
Si se ha aplicado una limitación de velocidad a un dispositivo, las flechas de velocidad de carga/descarga se volverán amarillas.



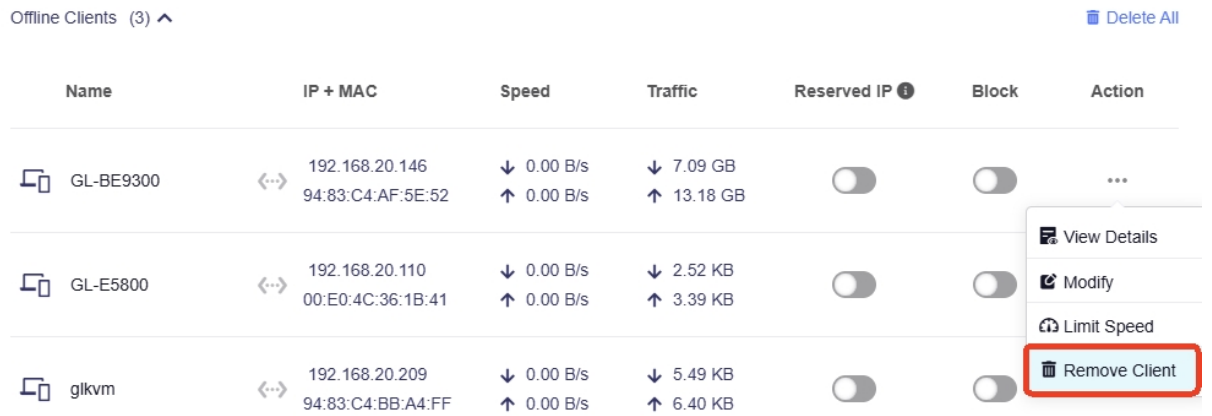
Consejo: Si la opción Limitar velocidad está activada no visible, vaya a **RED** > **Aceleración de red** y desactívela. La opción Limitar velocidad estará disponible.

5.3 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.

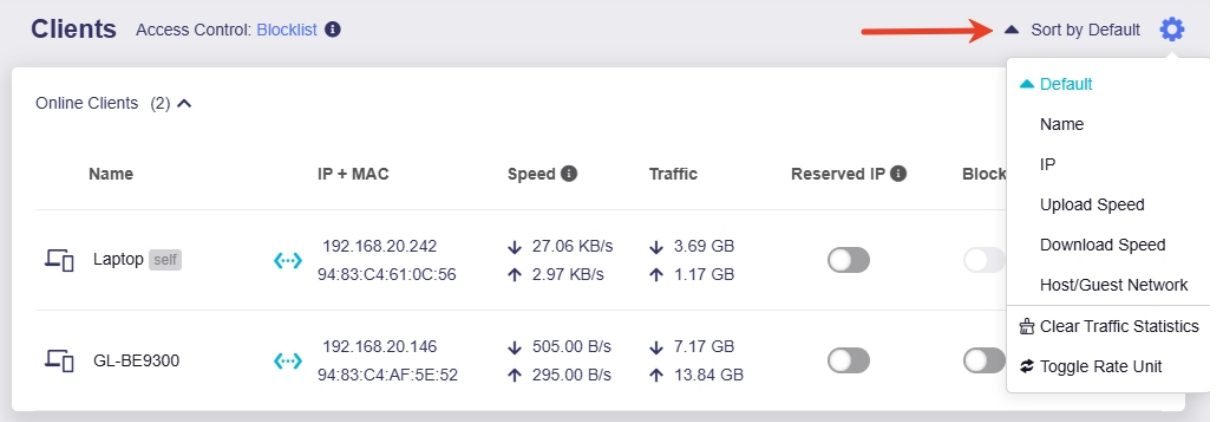


Si desea eliminar un cliente específico, haga clic en el ícono de tres puntos en **Acción** columna, luego haga clic en **Eliminar cliente** de menú desplegable.



5.4 Ordenar

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



La regla de clasificación predeterminadaing es la siguiente:

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

Capítulo 6

Servicios en la nube

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

6.1 GoodCloud

GL.iNet GoodCloud es una plataforma diseñada para simplificar la implementación y administración remota de dispositivos conectados. proporciona una fácil forma 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 realizar actualizaciones de software. También pueden acceder de forma remota al panel de administración web del enrutador o conectarse al terminal del enrutador a través de SSH, logrando una administración de dispositivos de red interregional y de extremo a extremo.

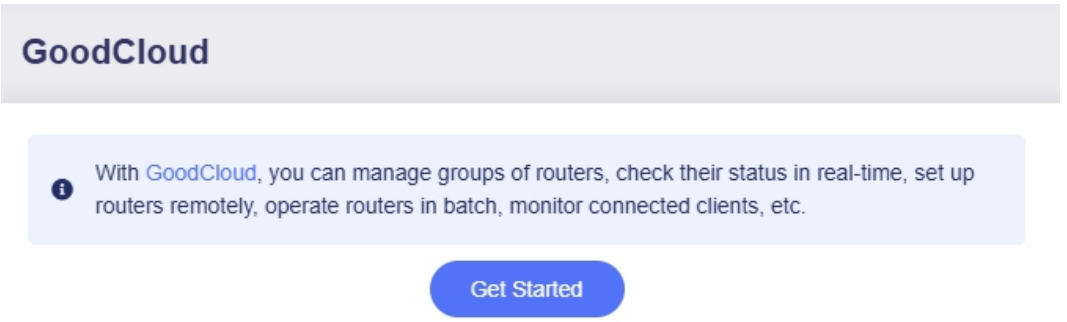
Con GoodCloud, puede:

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

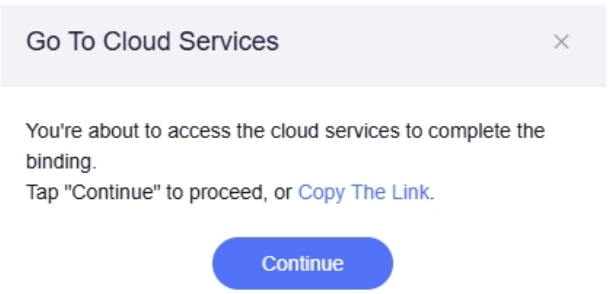
Algunas funciones están disponibles en el plan Enterprise y el plan VAR (revendedor de valor agregado). Consulte aquí para obtener más detalles.

6.1.1 Habilitar GoodCloud

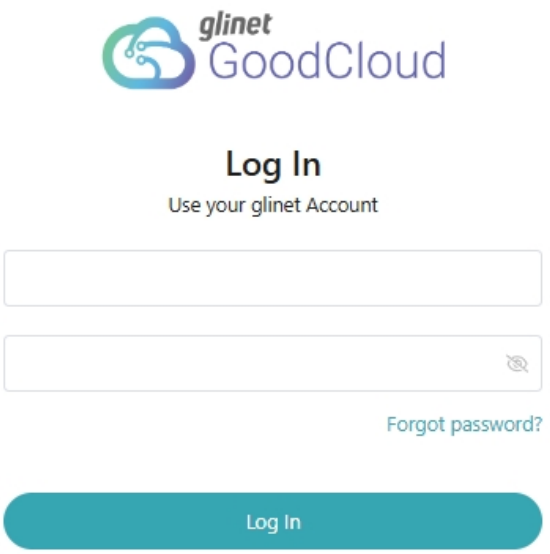
1. Inicie sesión en el panel de administración web de su enrutador', navegue hasta **SERVICIO EN LA NUBE** > **GoodCloud**, y click **Obtener Started.**



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



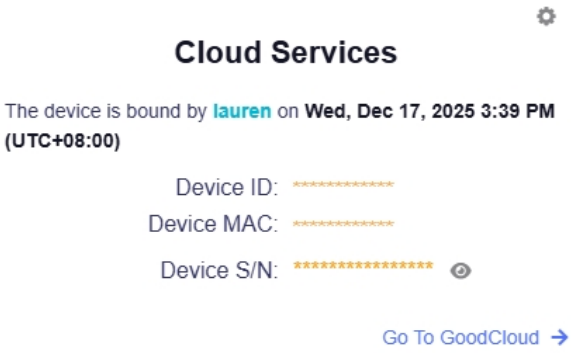
3. Será redirigido a la página de inicio de sesión de GoodCloud. Log en con su cuenta GL.iNet. Si'no tiene una cuenta, haga clic en **Registrarse** para registrarse e iniciar sesión. Una vez que haya iniciado sesión, confirme la información del dispositivo y vincúlela a su cuenta.



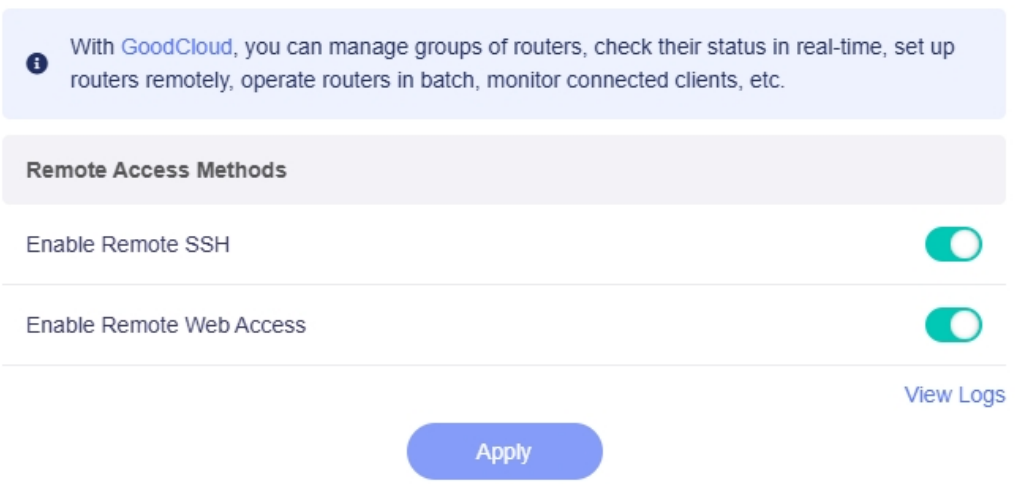
Consejos:

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

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



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

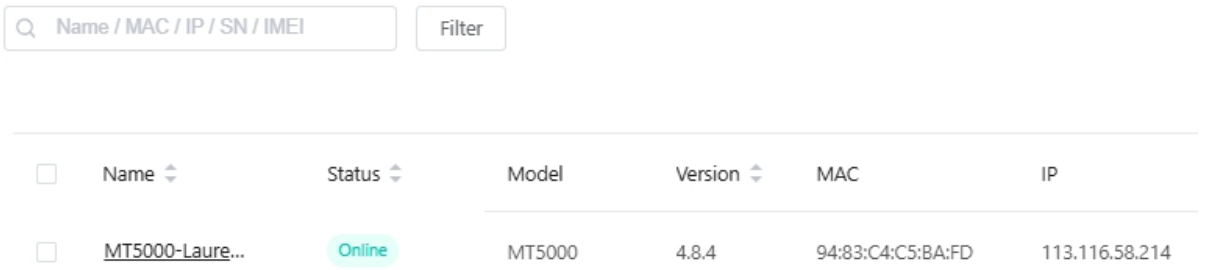


- **Acceso remoto SSH**: Accede de forma remota al terminal del router desde GoodCloud mediante SSH.
- **Acceso web remoto**: Remotely acceder a la web del admin panel desde GoodCloud a través de HTTP/HTTPS.
- **Ver registros**: Redireccionar a la página de registro y mostrar la nube log.

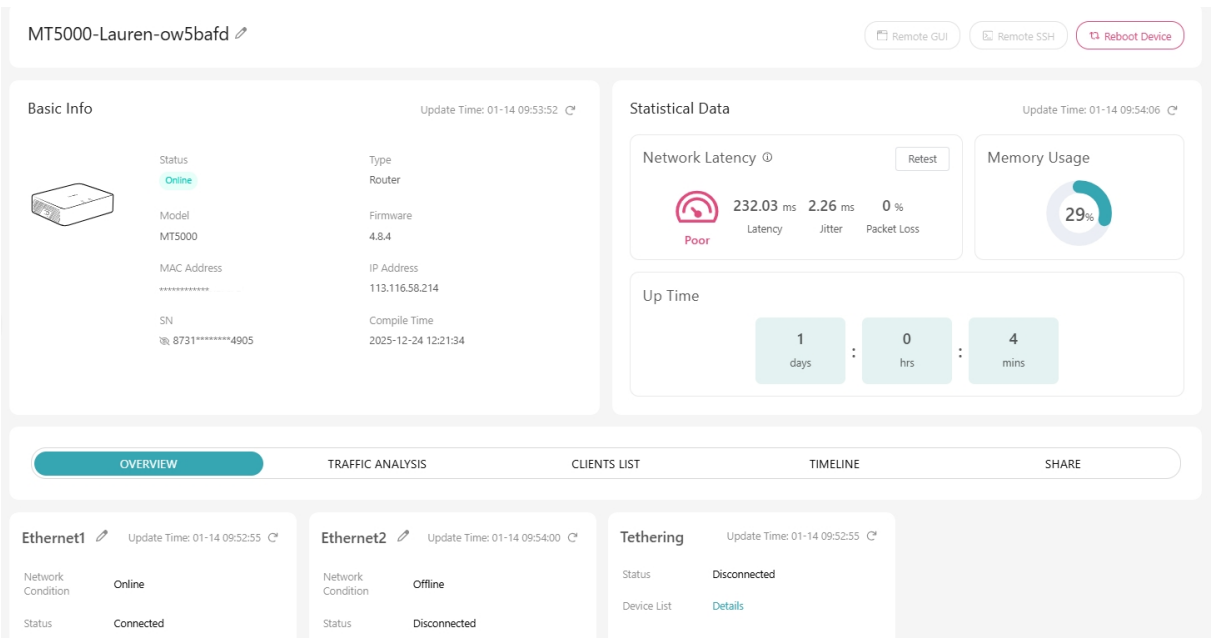
6.1.2 Administrar el enrutador

Consultar los detalles del dispositivo

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

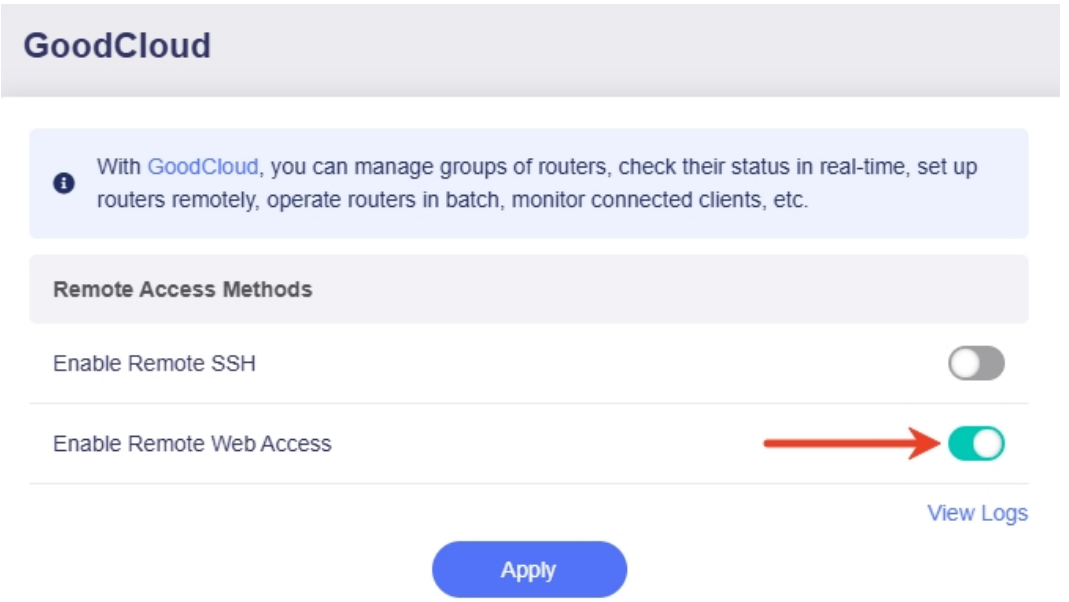


Haga clic en el nombre del dispositivo para ingrese a la página de detalles del dispositivo, que muestras información básica, datos estadísticos, descripción general de la red, lista de clientes y cronograma. También puede realizar operaciones avanzadas, como acceso remotolying al enrutador, y reiniciando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

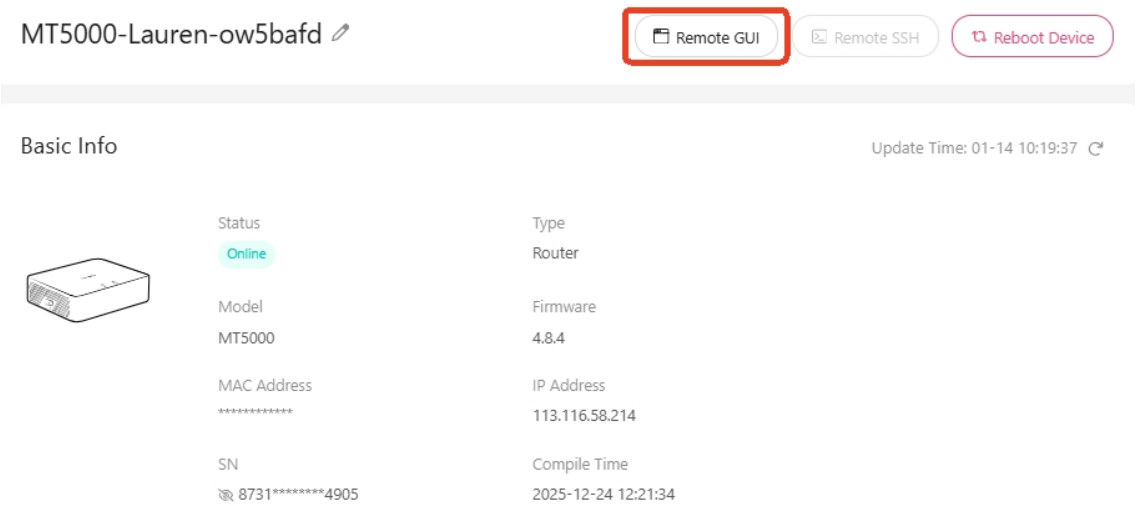


Acceso web remoto

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

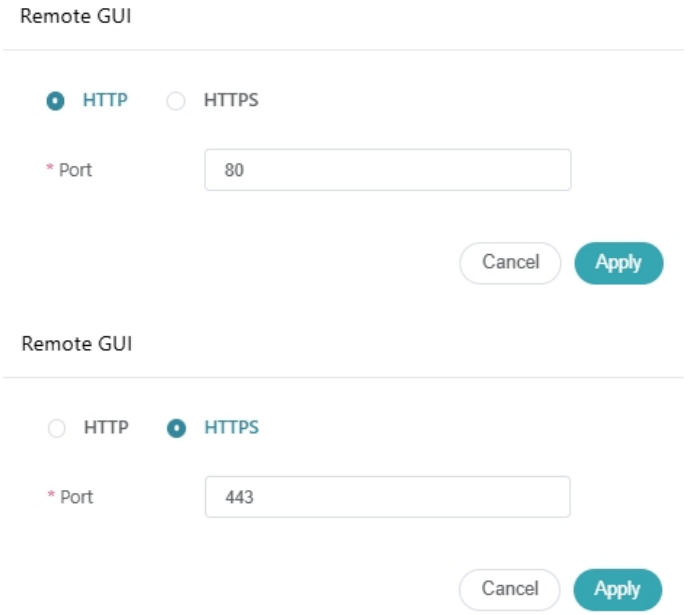


2. Inicie sesión en la plataforma GoodCloud y navegue a **Dispositivo** > **Dispositivos vinculados**. Haga clic en el dispositivo al que desea acceder e ingresará a la página de detalles del dispositivo.
3. En la página de detalles del dispositivo, haga clic en **Remoto GUI** botón en la esquina superior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

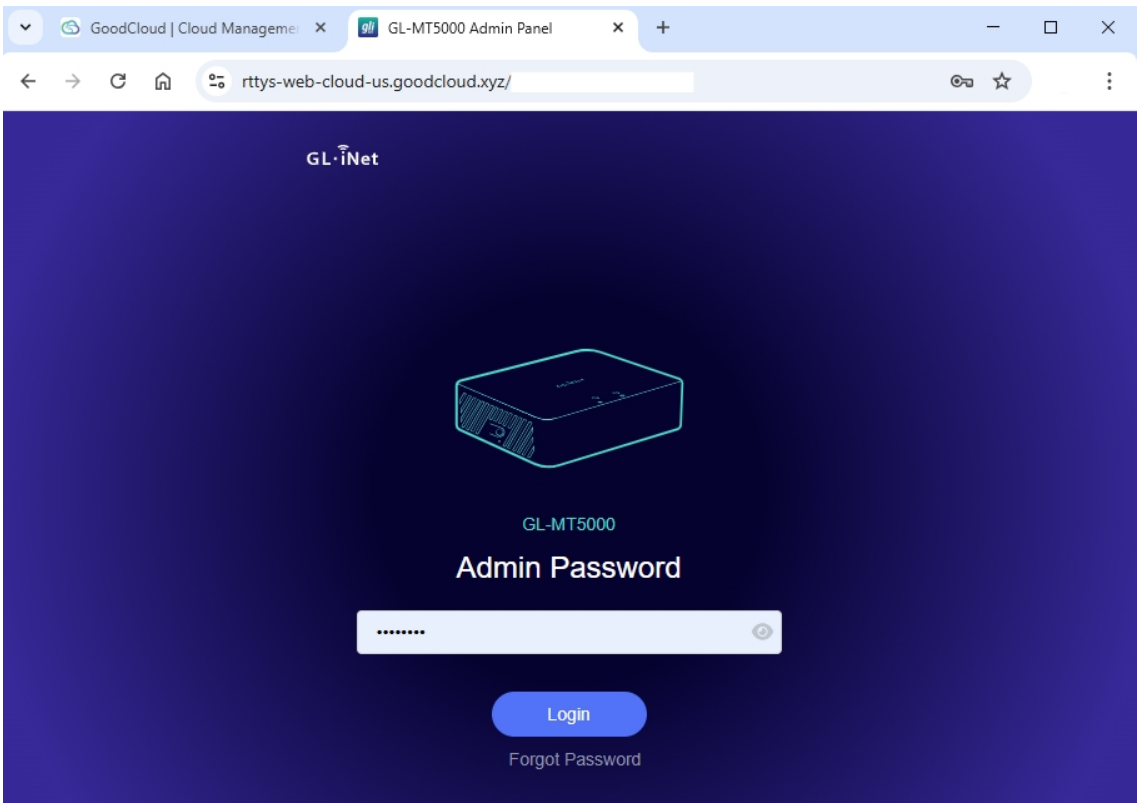


4. Seleccione el protocolo y el puerto de transferencia. Los valores predeterminados son **HTTP** y Puerto **80**. Puede cambiar el protocolo a HTTPSpuedes cambiar el protocolo a

HTTPS según sea necesario y el puerto cambiará automáticamente a 443. Luego haga clic en **Aplicar**.

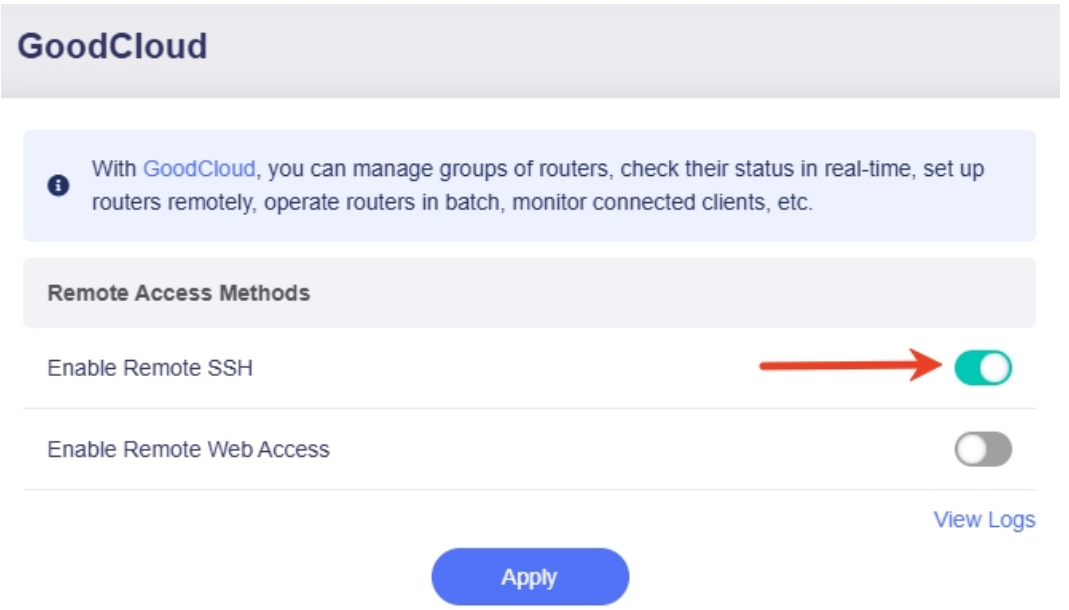


5. Será redirigido a la página de inicio de sesión del enrutador'. Ingrese la contraseña de administrador para acceder de forma remota al panel de administración web del enrutador'.

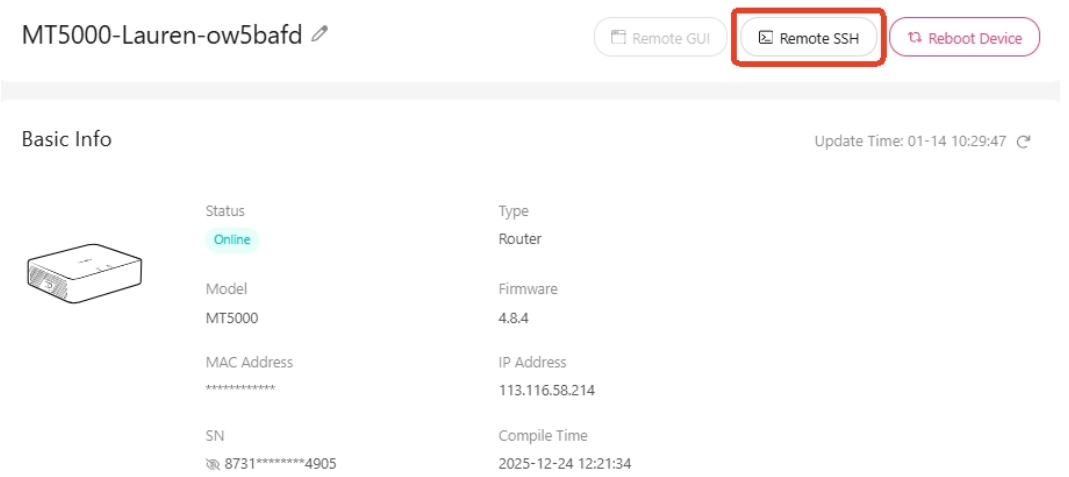


Acceso remoto al terminal

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



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

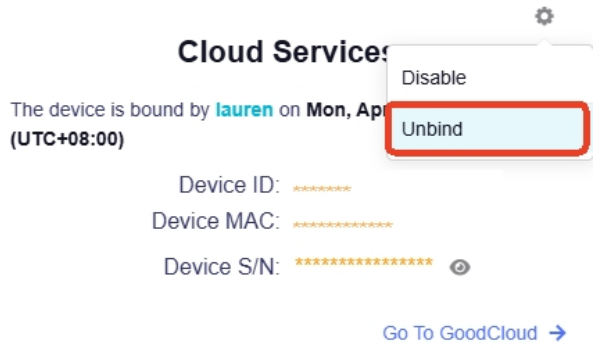


4. Inicie sesión como **root** e ingrese la contraseña para acceder al terminal de su enrutador.

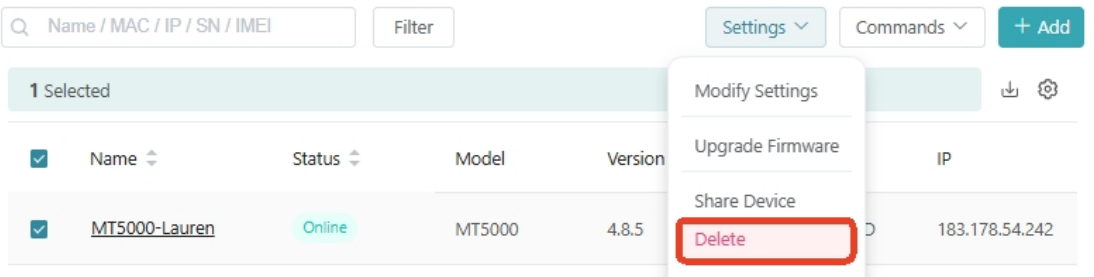

GL-MT5000 login: root
Password:
BusyBox v1.33.2 (2025-12-24 12:15:29 UTC) built-in shell (ash)
W I R E L E S S F R E E D O M
OpenWrt 21.02-SNAPSHOT,
root@GL-MT5000:~#

6.1.3 Desvincular el dispositivo

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

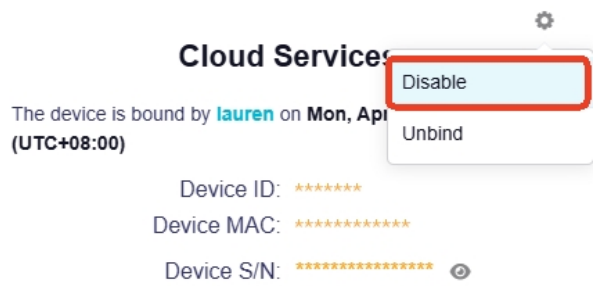


Como alternativa, inicie sesión en la plataforma en la nube y navegue hasta **Dispositivo** > **Dispositivos vinculados**. Select the device you want to unbind, click **Configuración** en la esquina superior derecha y luego seleccione **Eliminar**. Su dispositivo se desvinculará. su cuenta de GoodCloud.



6.1.4 Desactivar GoodCloud

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



6.2 AstroWarp

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

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

Nota:

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

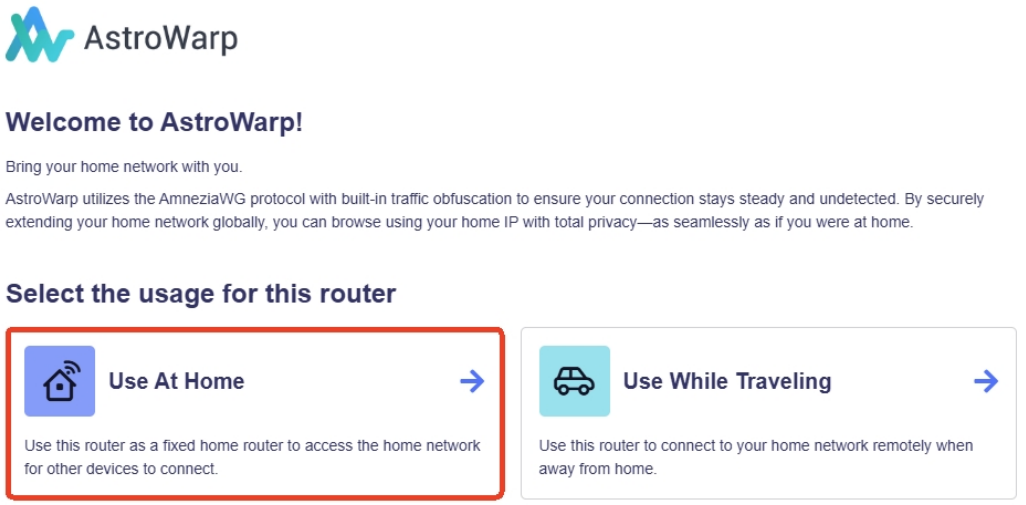
6.2.1 Configuración rápida

En el siguiente ejemplo, se utilizarán dos enrutadores para configurar una red AstroWarp: Brume 3 actuará como enrutador doméstico, mientras que un enrutador de viaje GL.iNet será ruta tráfico de red de regreso a Brume 3 para acceso a Internet. Sugerimos configurar la red AstroWarp antes de la salida.

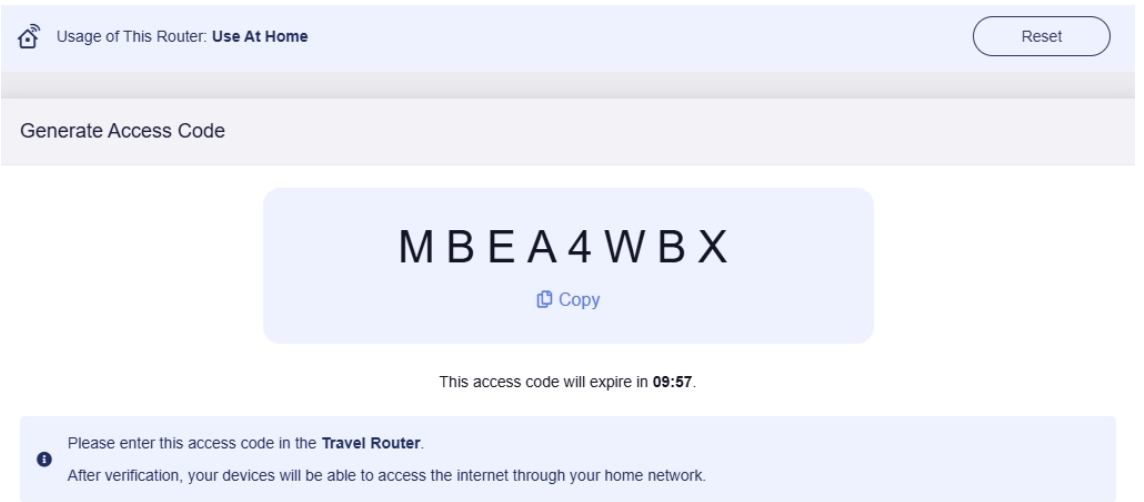
Consejo: Cada enrutador GL.iNet viene con **10 GB de datos gratuitos por mes** para redes AstroWarp. Los dispositivos en una red AstroWarp utilizarán los datos del enrutador doméstico para acceder a Internet. Puedes actualizar al plan AstroWarp+ para obtener datos ilimitados si es necesario.

1. Configurar Brume 3 para Internet.
   Inicia sesión en Brume 3panel de administración web y navegue hasta la página de INTERNET. Conéctelo a Internet usando uno de los métodos de conexión a Internet admitidos: Ethernet, Anclaje a red y celular.

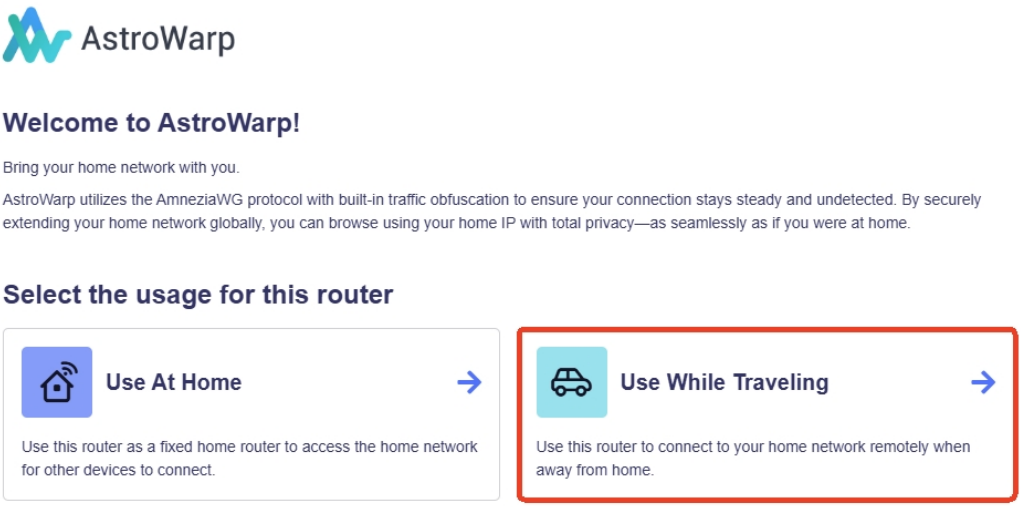
2. Estoyen el administrador web del Brume 3 panel, navegue hasta **SERVICIOS EN LA NUBE** > **AstroWarp**. Haga clic en **Usar en casa**.



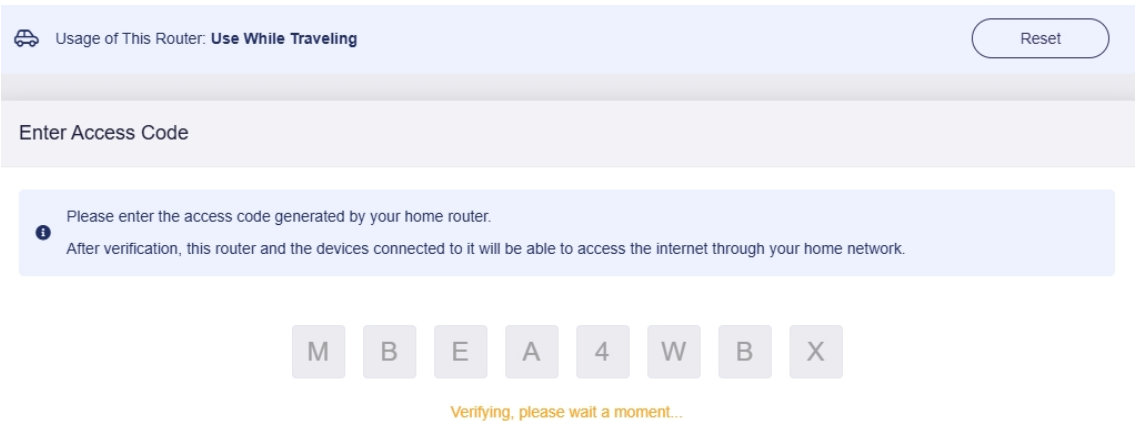
Se generará un **Código de acceso**. Copie este código para usarlo más adelante.



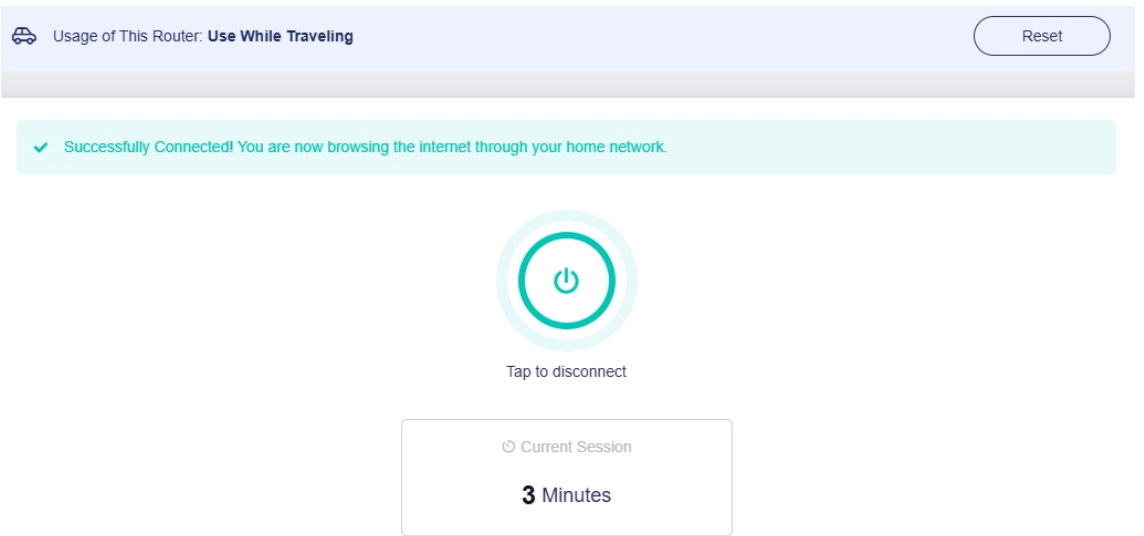
3. Configure el enrutador de viaje para Internet.
   Inicie sesión en el enrutador de viajepanel de administración web y navegue hasta la página de INTERNET. Conéctelo a Internet usando uno de los métodos de conexión a Internet admitidos: Ethernet, repetidor, anclaje a red y celular.
4. Ingrese el código de acceso.
   En el enrutador de viaje, navega hasta **SERVICIOS EN LA NUBE** > **AstroWarp**. Haga clic **Usar mientras viajaing**.



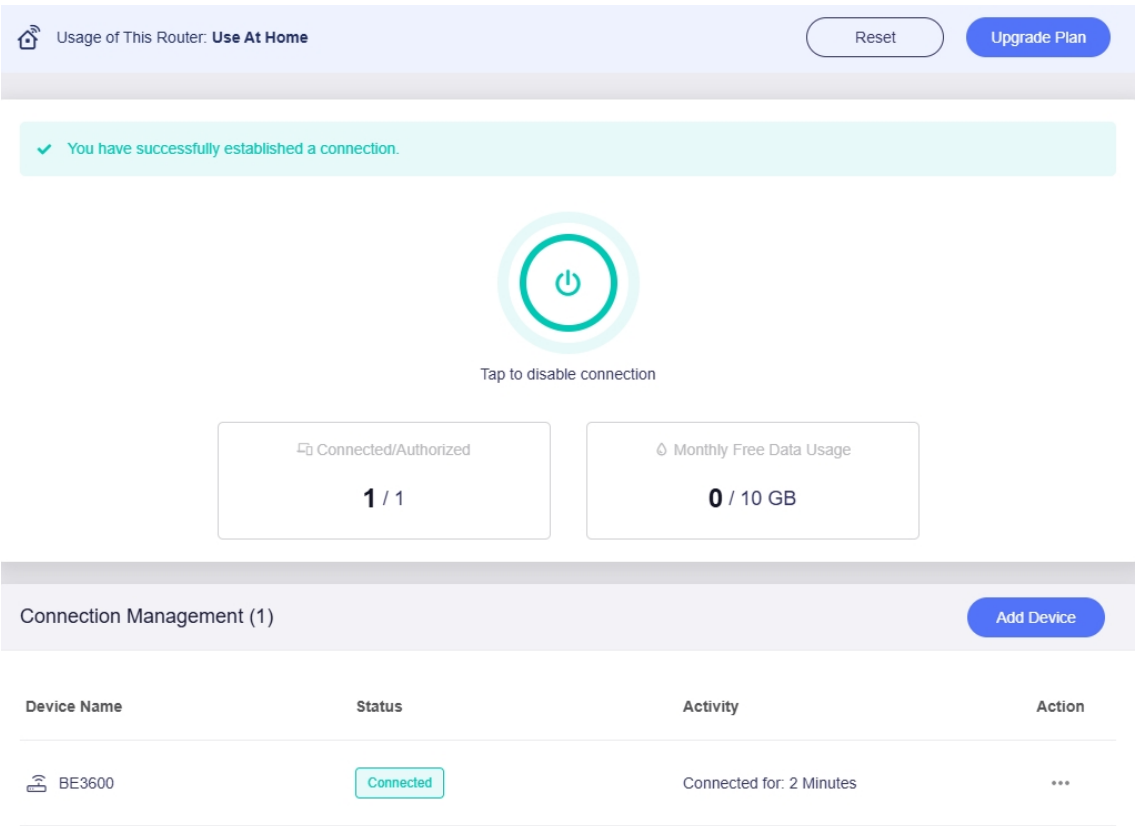
Ingrese el código de acceso obtenido en el paso 2 y espere a que se complete la verificación.espera a que se complete la verificación.



Luego se conectará a el Brume 3 con éxito. Ahora puede navegar por Internet a través de su red doméstica de forma segura.



5. Enen el panel de administración web del Brume 3, también muestra el estado de la conexión como sigue.



6.2.2 Comprobar la conectividad

1. Conecta una computadora portátil o un teléfono inteligente al enrutador de viaje’s Wi-Fi.
2. Abra un navegador y visite ipcheck.ing o cualquier otro sitio web de búsqueda de direcciones IP. Mostrará la dirección IP pública de Brume 3, lo que indica que el enrutador de viaje está accediendo a Internet a través el Brume 3.

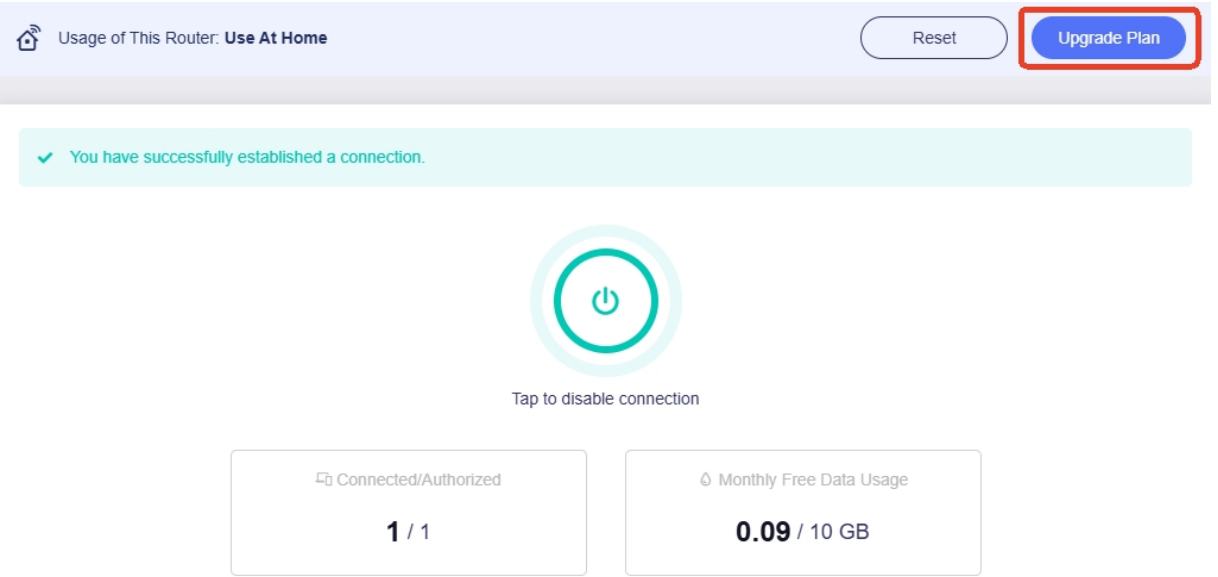


3. Desconecte la conexión AstroWarp en el enrutador de viaje, luego actualice la página web para volver a enviar la solicitud de consulta de IP. Mostrará la dirección IP pública local enrutador de viaje’, lo que indica que enrutador de viajeestá accediendo a Internet a través de su red local.



6.2.3 Plan de actualización

Cada enrutador GL.iNet viene con **10 GB de datos gratuitos por mes** para redes AstroWarp. Los dispositivos en una red AstroWarp utilizarán los datos del enrutador doméstico para acceder a Internet. Puedes actualizar al plan **AstroWarp+** para datos ilimitados si es necesario.



Haga clic aquí para ver más detalles y preguntas frecuentes sobre AstroWarp.

Capítulo 7

Conozca la VPN

Este capítulo presenta VPN conceptos y uso escenarios.

7.1 Introducción

VPN

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

Enrutador VPN

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

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

OpenVPN

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

WireGuard

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

7.2 Escenarios de aplicación

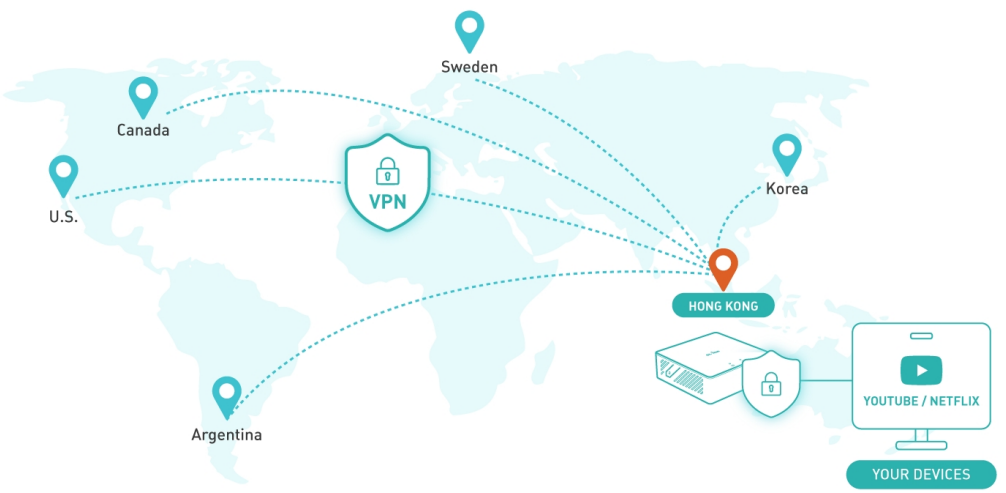
1. **Privacidad de datos personales**

   El servicio VPN de este enrutador funciona con una completa gama de dispositivos cableados, incluidos ordenadores de sobremesa, portátiles, consolas de juegos, televisores inteligentes y dispositivos de streaming. Todos sus datos transmitidos a través de conexiones por cable están protegidos por la VPN. También puede personalizar las políticas de VPN para permitir una protección flexible para dispositivos específicos.



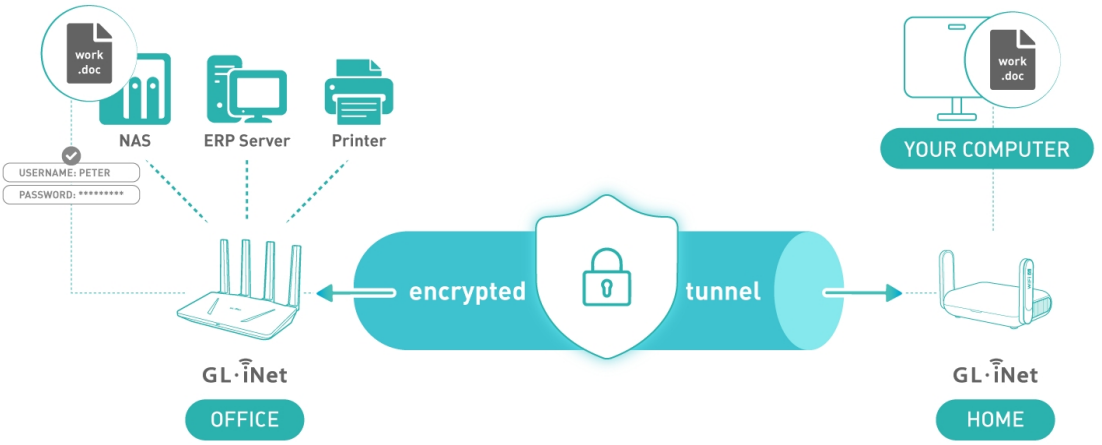
2. **Acceso sin restricciones en todo el mundo**

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



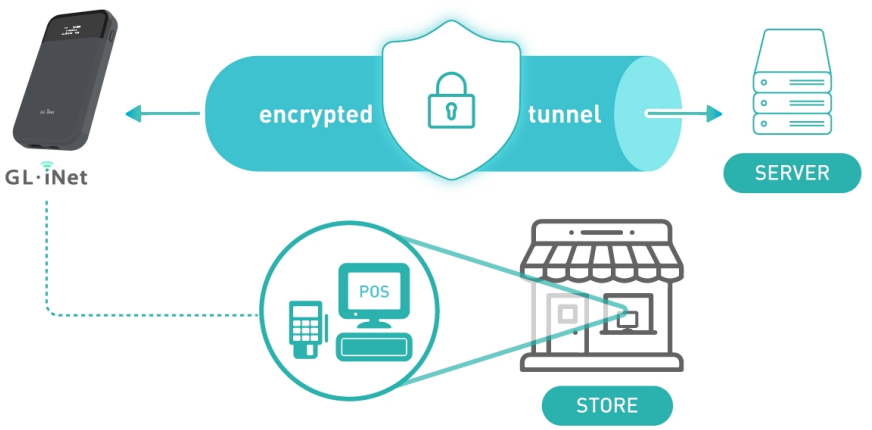
3. **Seguridad de datos para pequeñas empresas**

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



4. **Infraestructura de pago seguro**

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



Capítulo 8

Panel de VPN

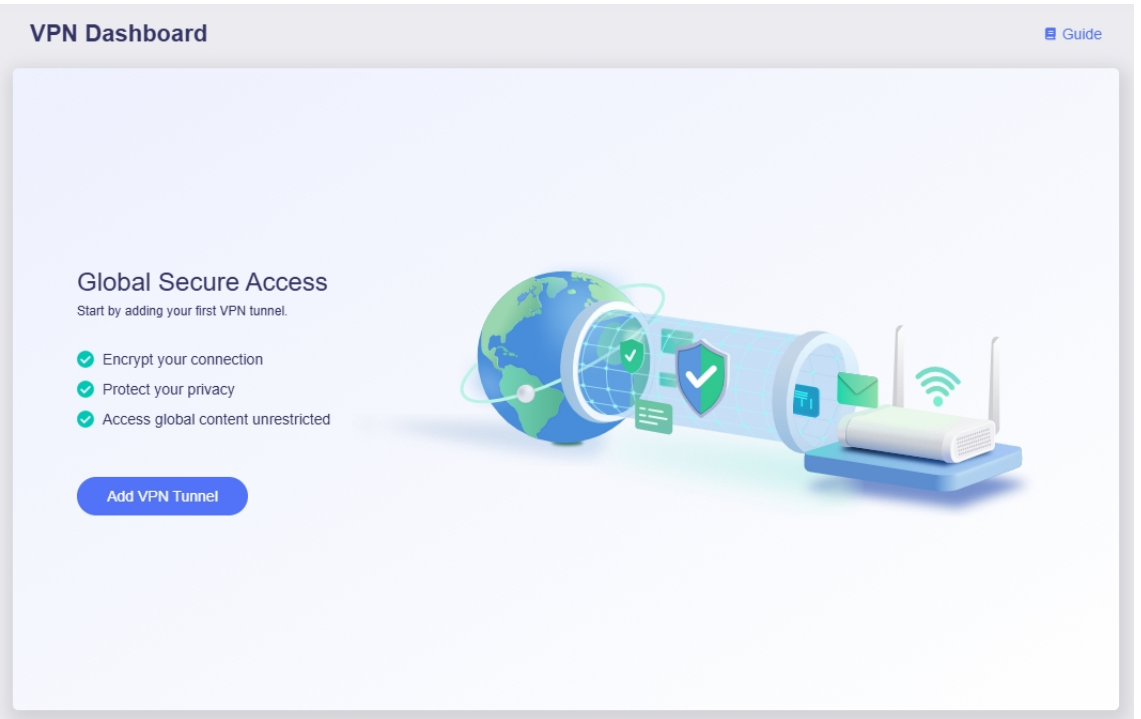
Este capítulo presenta cómo administrar conexiones VPN a través del panel de administración web.

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

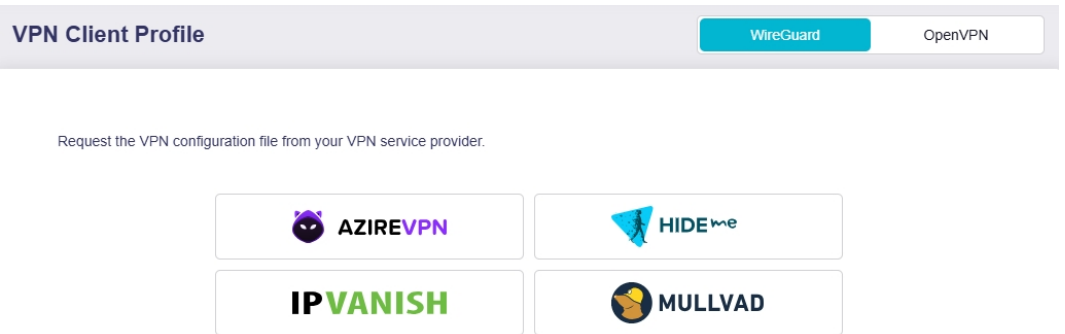
El El panel de VPN muestra detalles de la conexión VPN, como reglas de enrutamiento, servidor conectado, estadísticas de tráfico, IP virtual del cliente y registro de conexión, y permite a los usuarios configurar ajustes avanzados como VPN Kill Switch, enmascaramiento de IP y MTU.

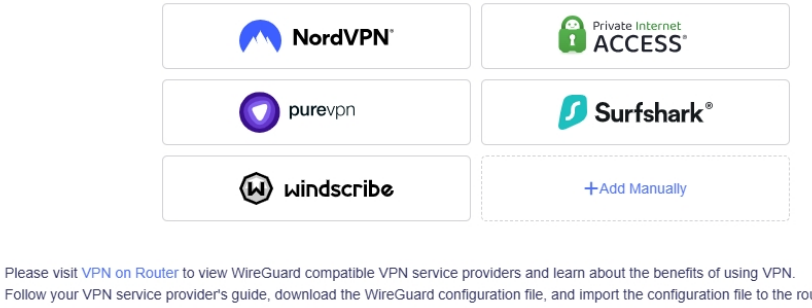
8.1 Cargar perfil VPN

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



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

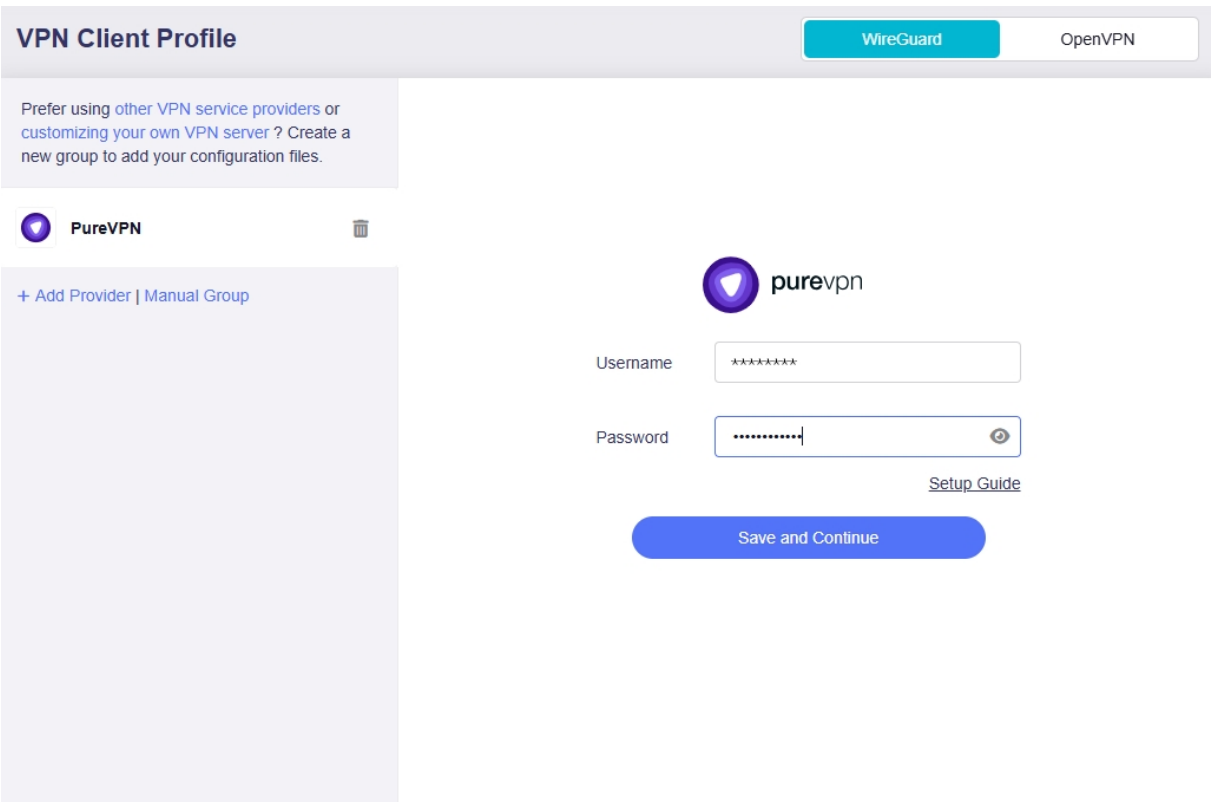




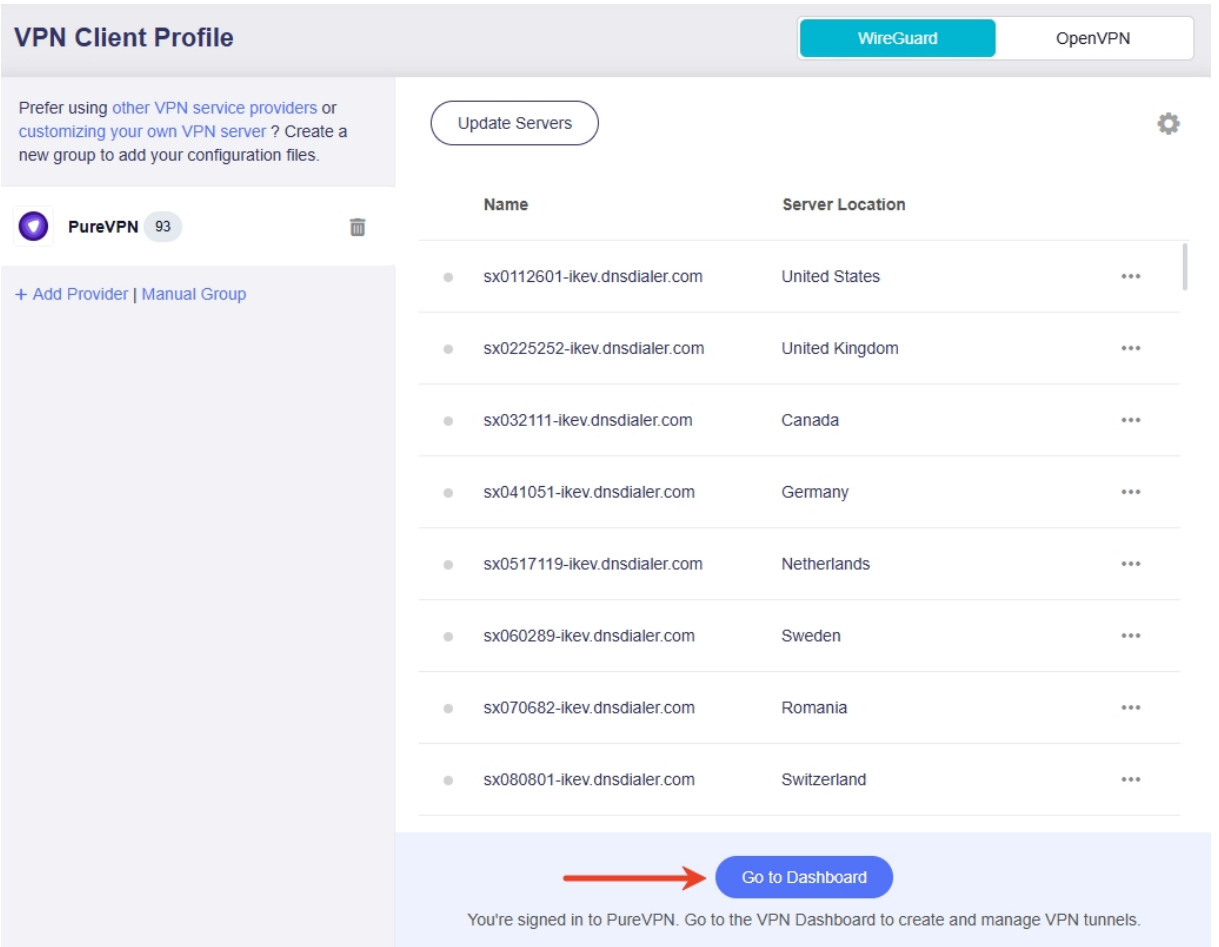
Consejos:

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

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



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



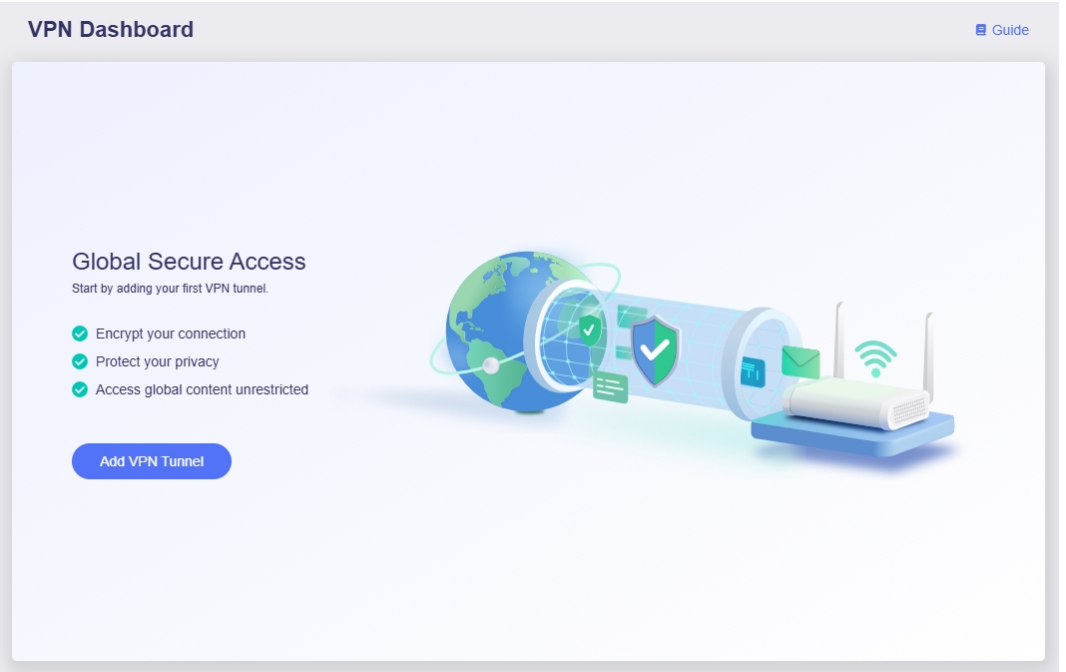
Consejo: Para algunos proveedores de servicios VPN, es posible que deba seleccionar un protocolo VPN o servidores/ciudades preferidos antes de que aparezca la lista de perfiles.

8.2 Agregar túnel VPN

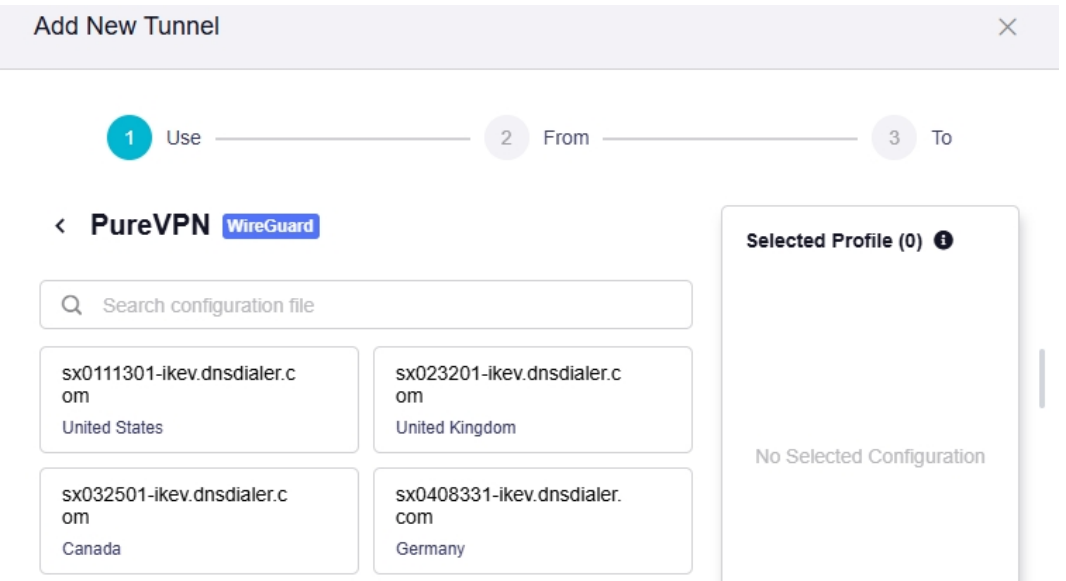
8.2.1 Pasos generales

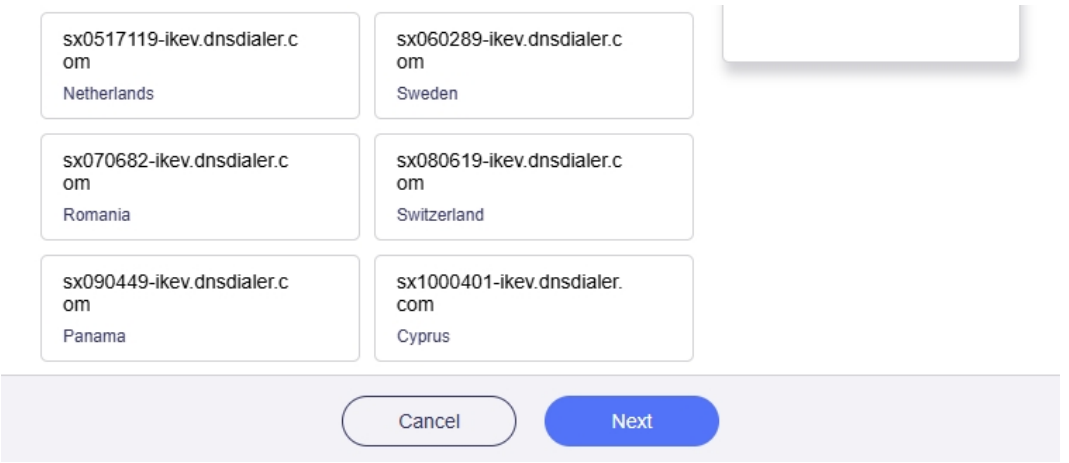
Siga los pasos a continuación para agregar su túnel VPN y configurar políticas VPN. Consulte Referencia del caso si es necesario.

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



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





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

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

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

8.2.2 Referencia del caso

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

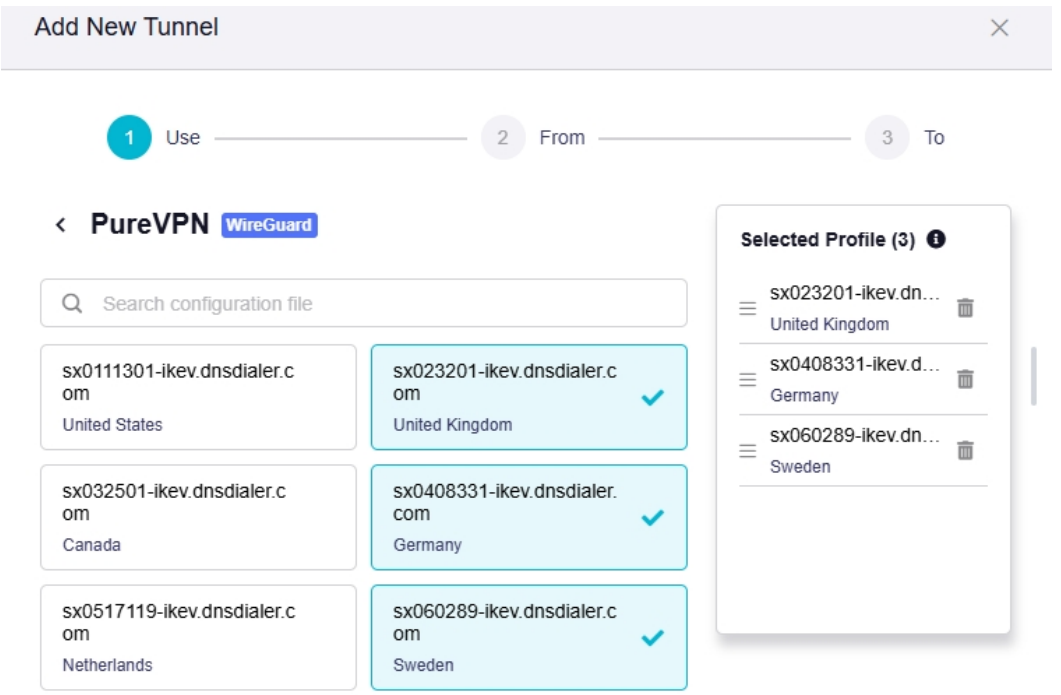
Caso 1: Enrutar solo dispositivos específicos a través de VPN

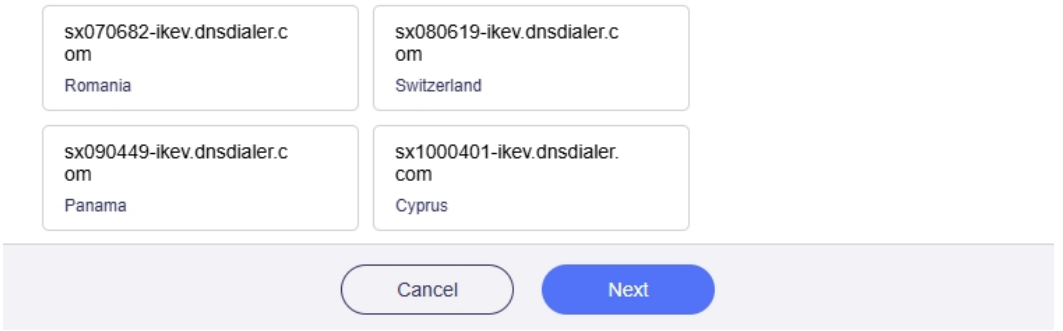
Requisitos:

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

Pasos de configuración:

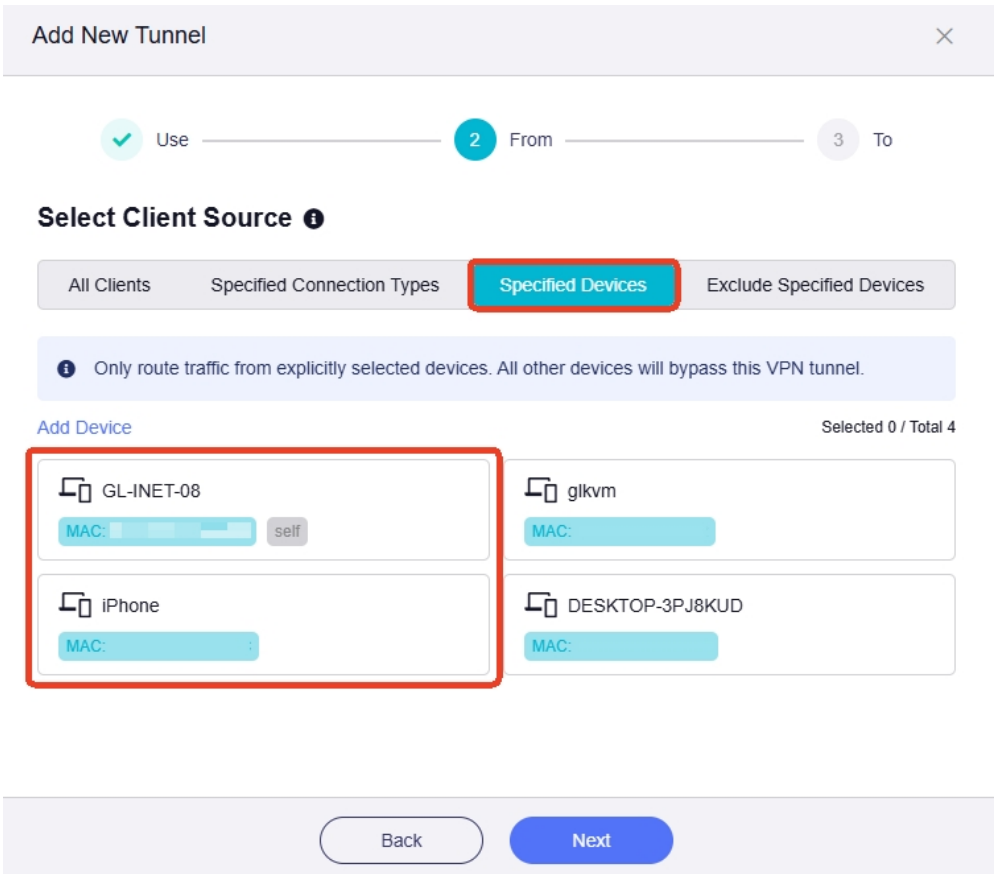
1. Seleccione el perfil de VPN.
   Si inició sesión con alguna credencial de servicio VPN integrada o cargó un archivo de configuración, los perfiles disponibles se enumerarán aquí. De lo contrario, vaya a **Perfil de cliente VPN** para iniciar sesión con sus credenciales o cargar un archivo de configuración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





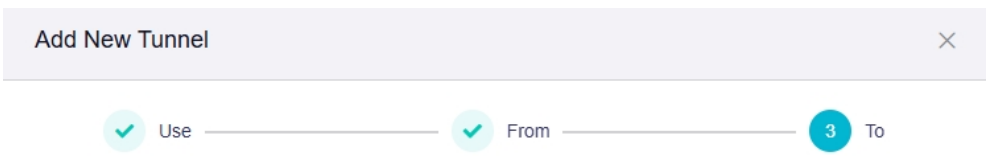
2. Seleccione la fuente del cliente.

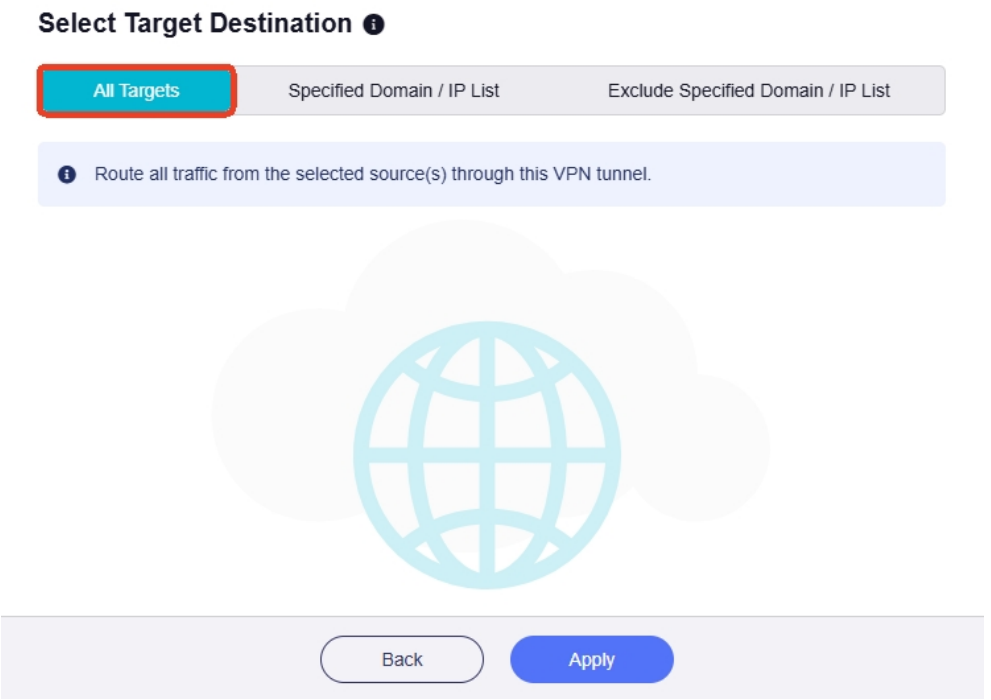
   Haga clic en la pestaña **Dispositivos especificados** , seleccione dispositivos que usarán la VPN y luego haga clic en **Siguiente**.



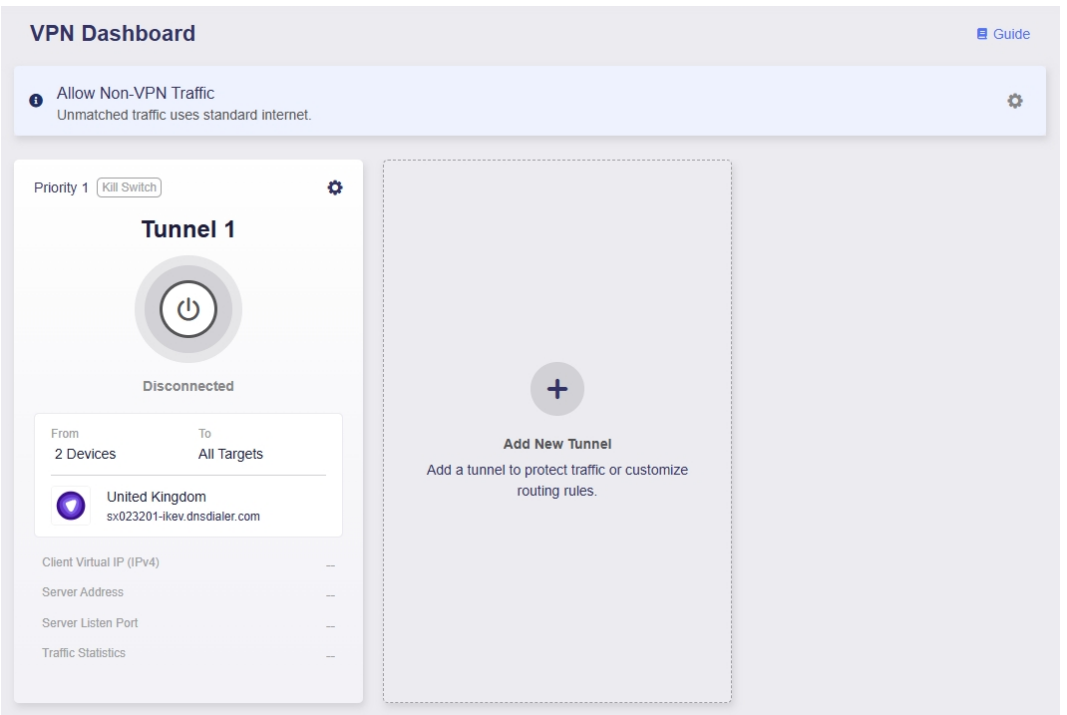
3. Seleccione el destino de destino.

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

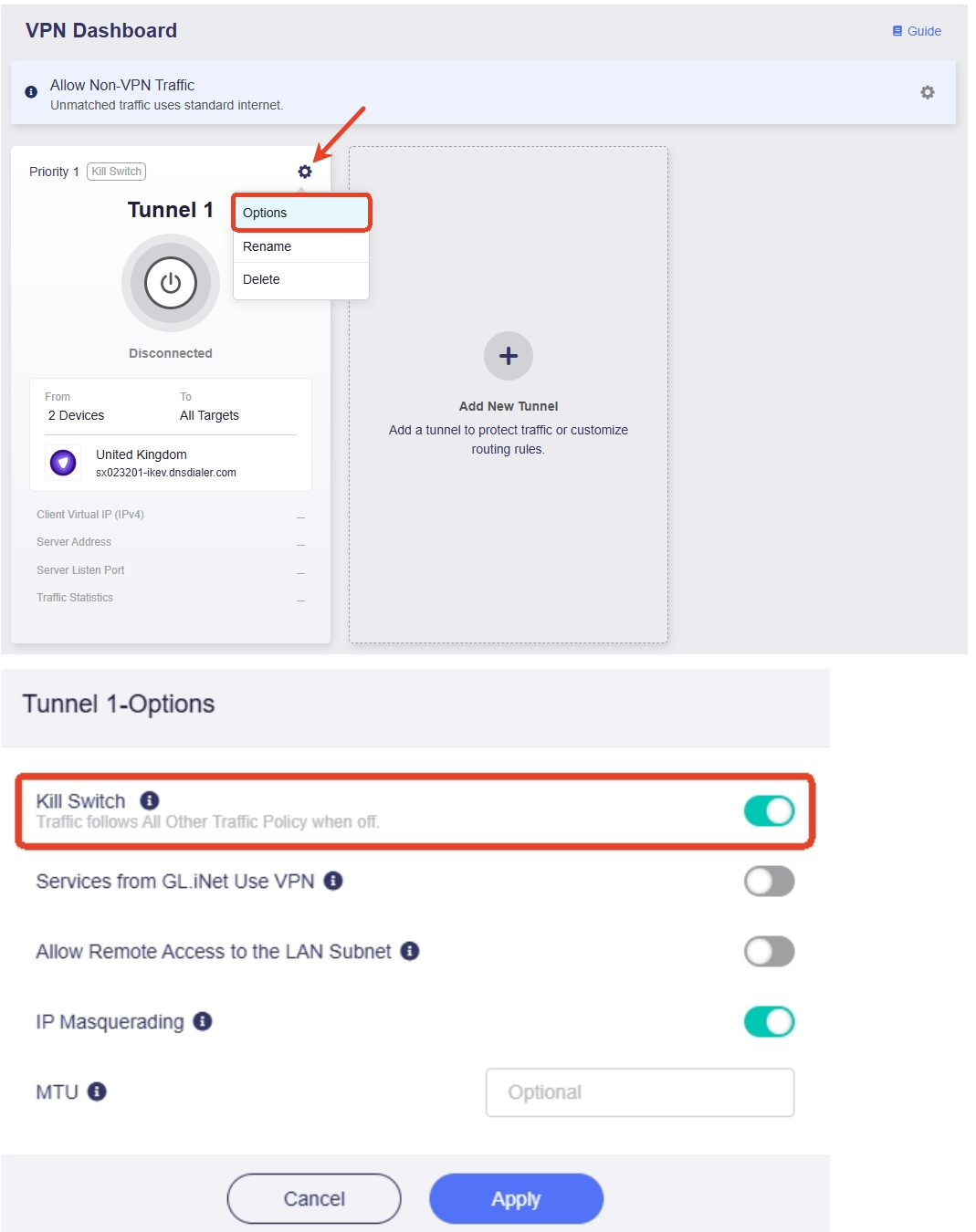




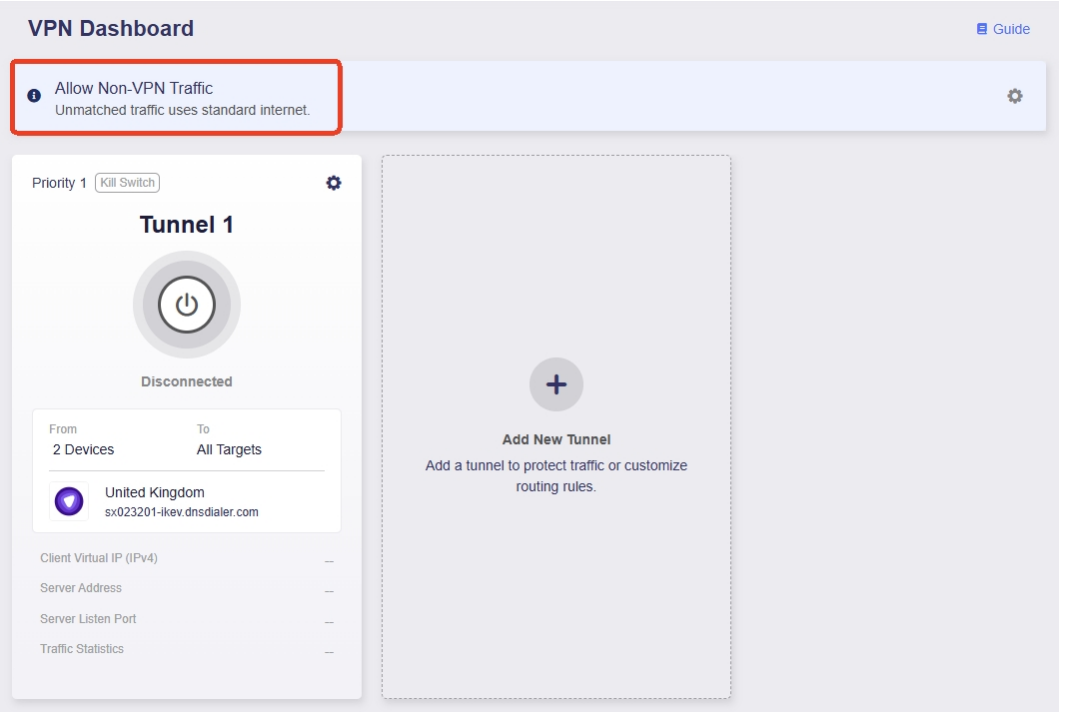
4. Usted será dirigido al Panel de VPN. Ahora se ha agregado correctamente un túnel VPN, como se muestra a continuación.



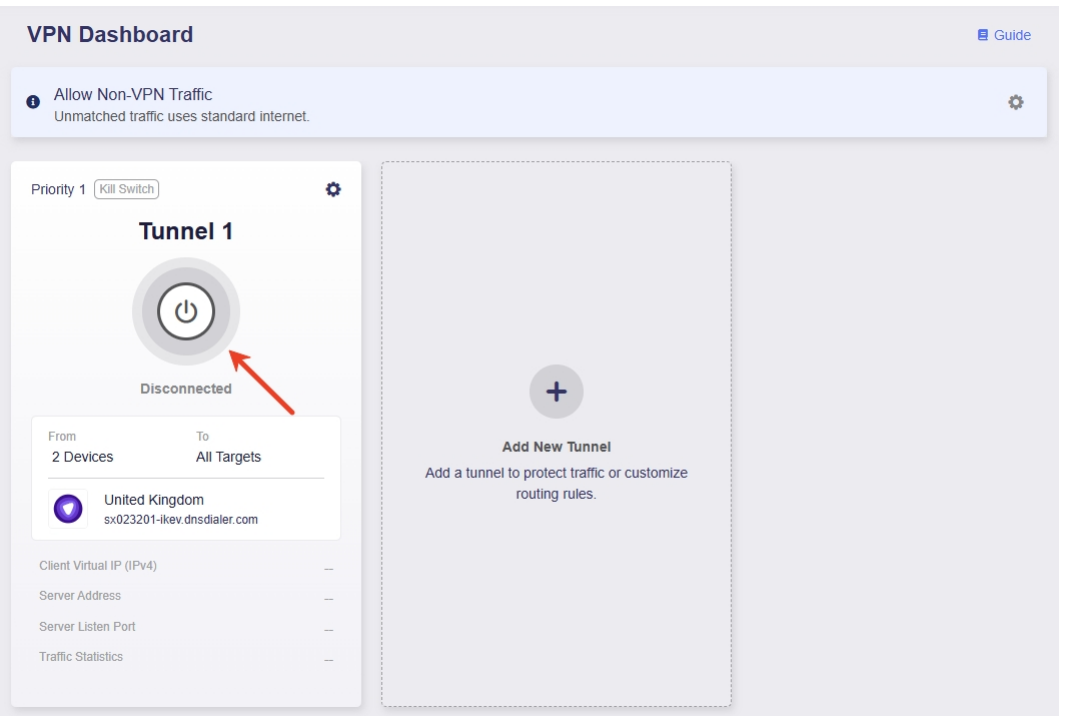
5. Asegúrese de que el **Bloqueo de tráfico sin VPN (Kill Switch)** para este túnel esté habilitado. Si la VPN se desconecta inesperadamente, se bloqueará el acceso a Internet para el tráfico que coincida con este túnel para evitar fugas de DNS y seguimiento de IP.



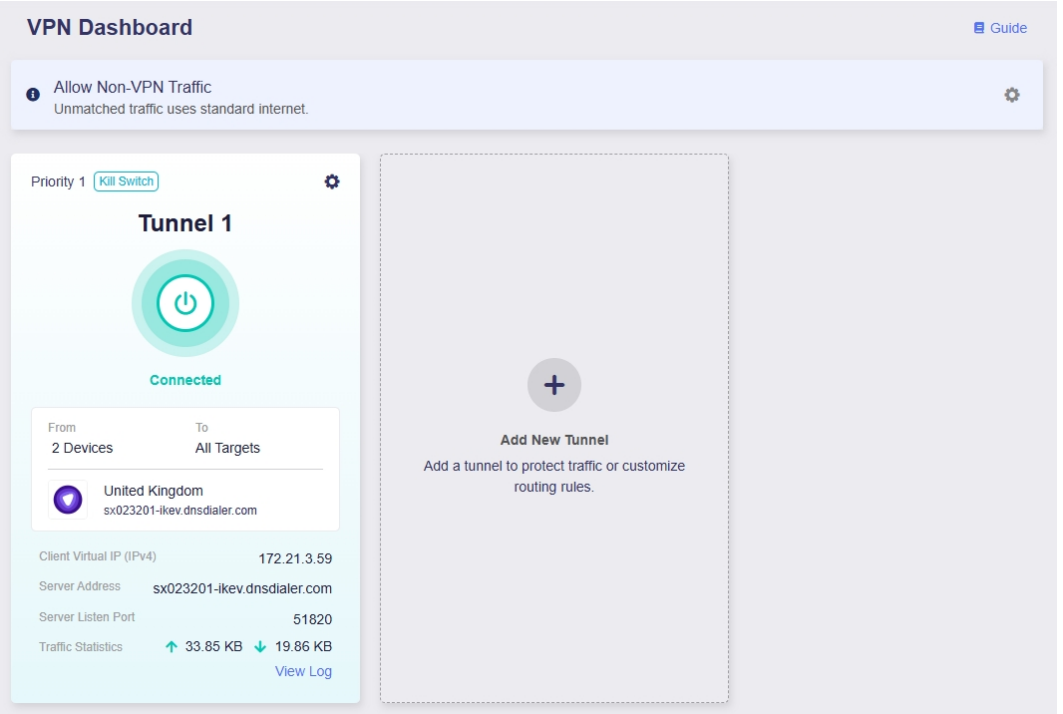
6. Asegúrese de que **Permitir tráfico que no sea de VPN** está habilitado. Esto está habilitado de forma predeterminada para garantizar que el tráfico que no coincida con el túnel VPN aún pueda acceder a Internet a través de la WAN local.



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



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



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

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

Requisitos:

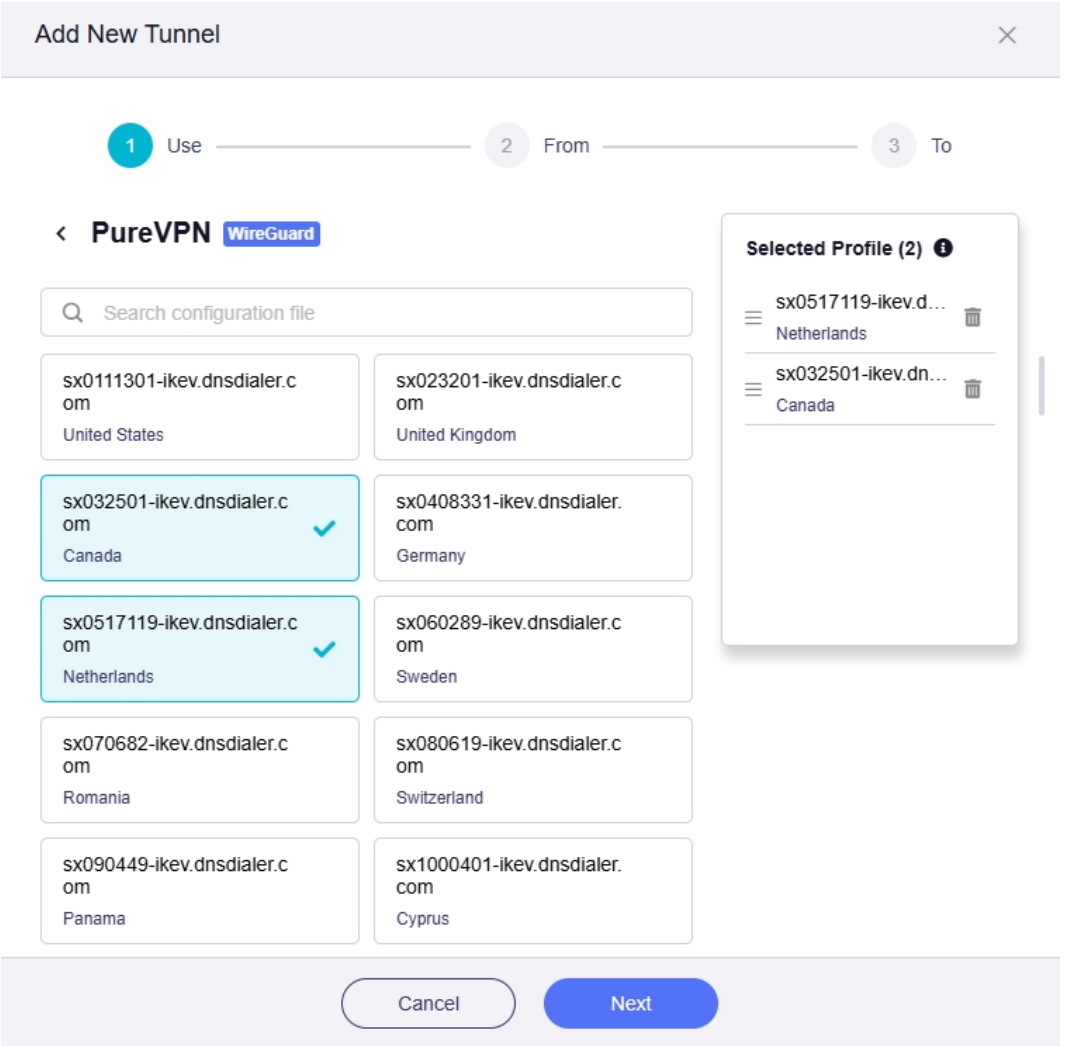
1. Todos los dispositivos utilizan VPN Tunnel 1 al acceder a dominios de redes sociales y servicios de streaming específicos, y utilice el túnel VPN 2 para todos los demás accesos a Internet.
2. Si los túneles VPN se desconectan inesperadamente, se bloqueará el acceso a Internet para todos los dispositivos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

Pasos de configuración:

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

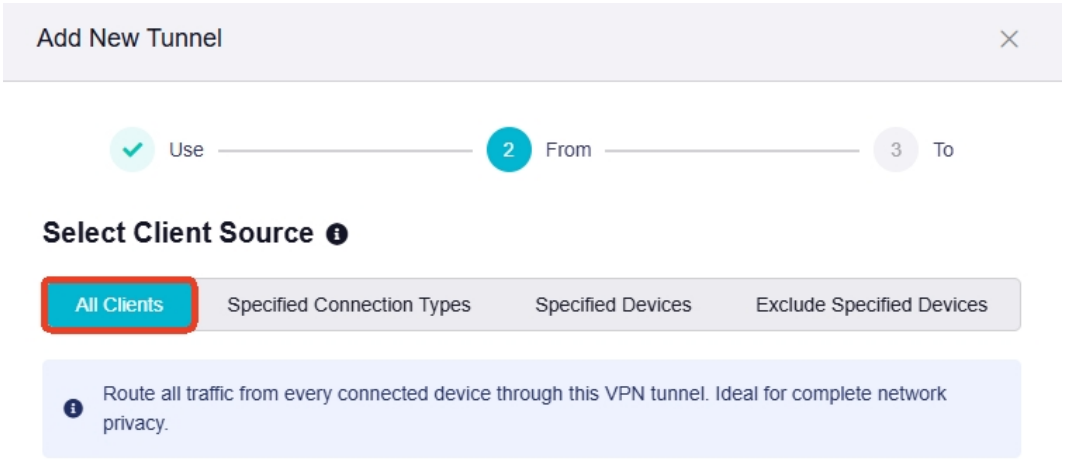
de cliente VPN para iniciar sesión con sus credenciales o cargar un archivo de configuración manualmente.

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

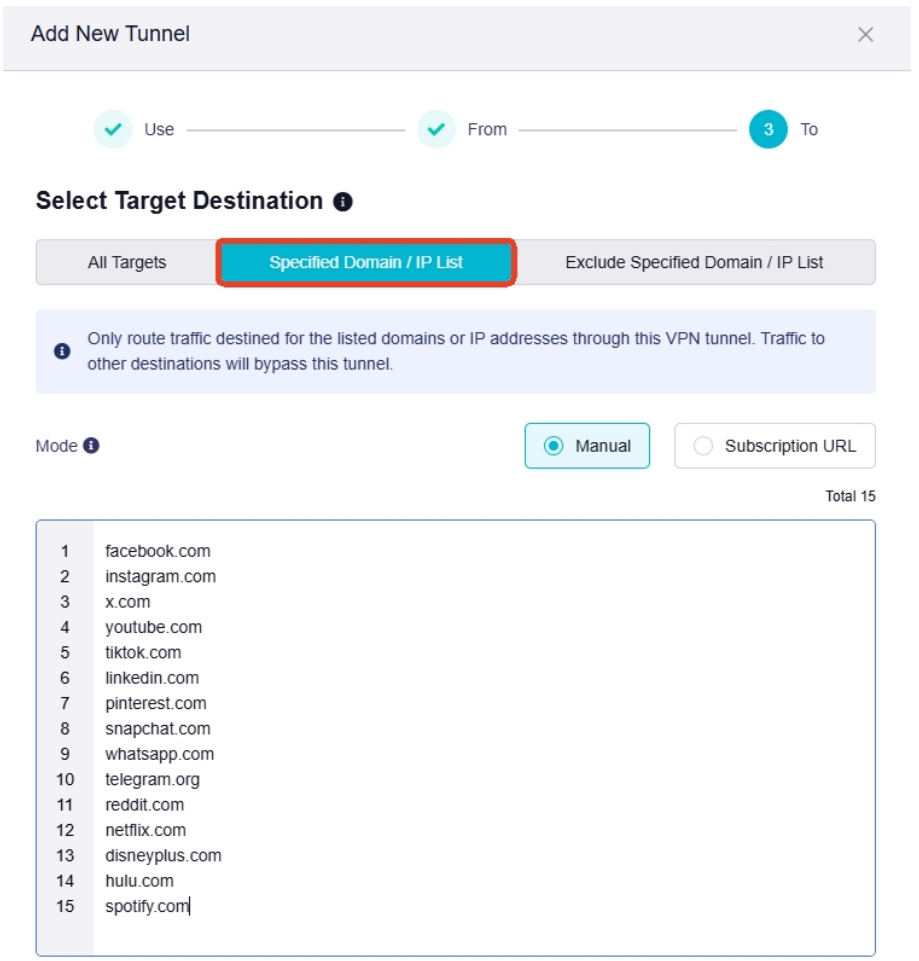


2. Seleccione la fuente del cliente.

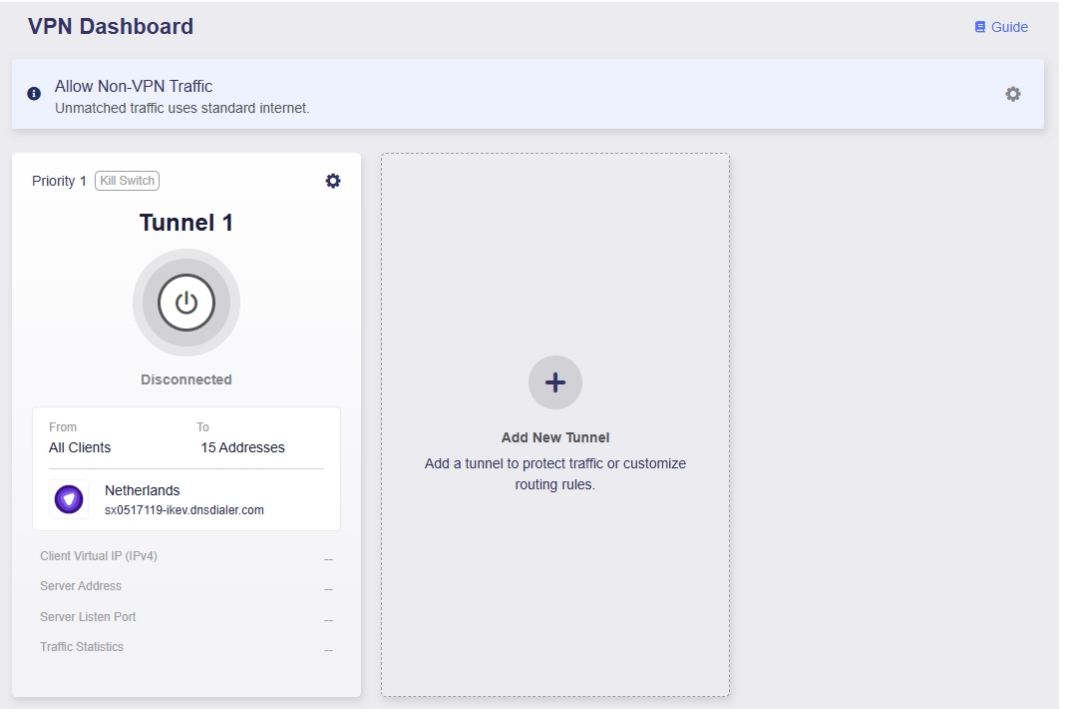
   Haga clic en la pestaña **Todos los clientes** , configúrela como origen del cliente para el Túnel 1, luego haga clic en **Siguiente**.



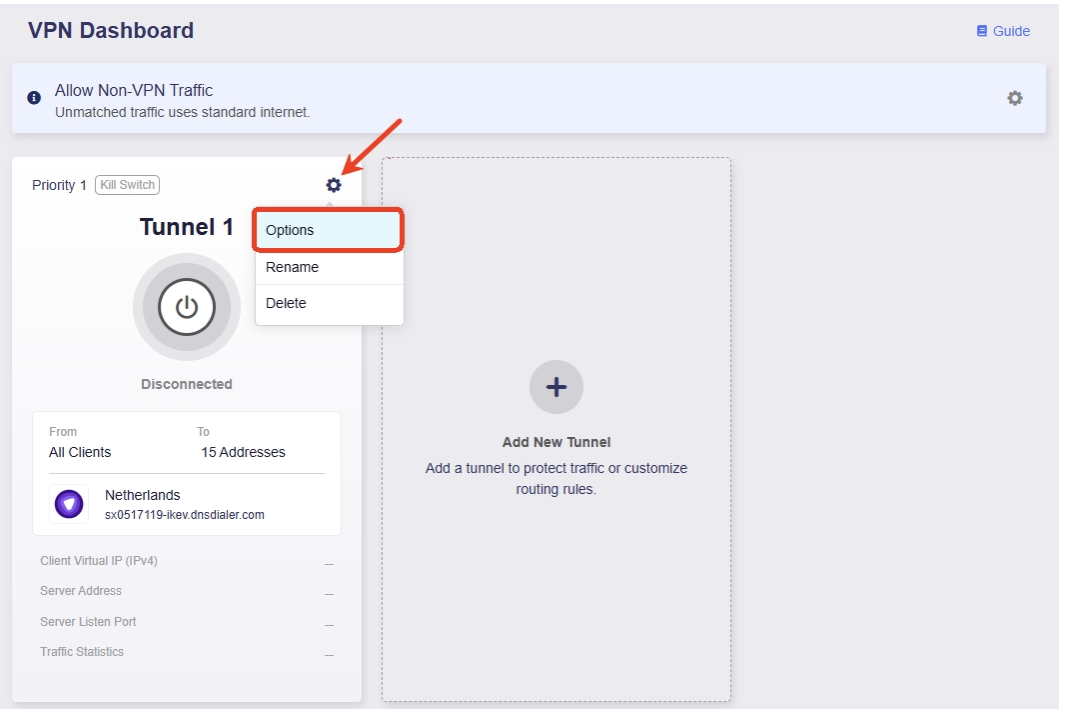
3. Seleccione el destino de destino.
   Haga clic en la pestaña **Dominio especificado/Lista de IP** e ingrese los dominios de algunos servicios de transmisión y redes sociales comunes, como se muestra a continuación, luego haga clic en **Aplicar**.

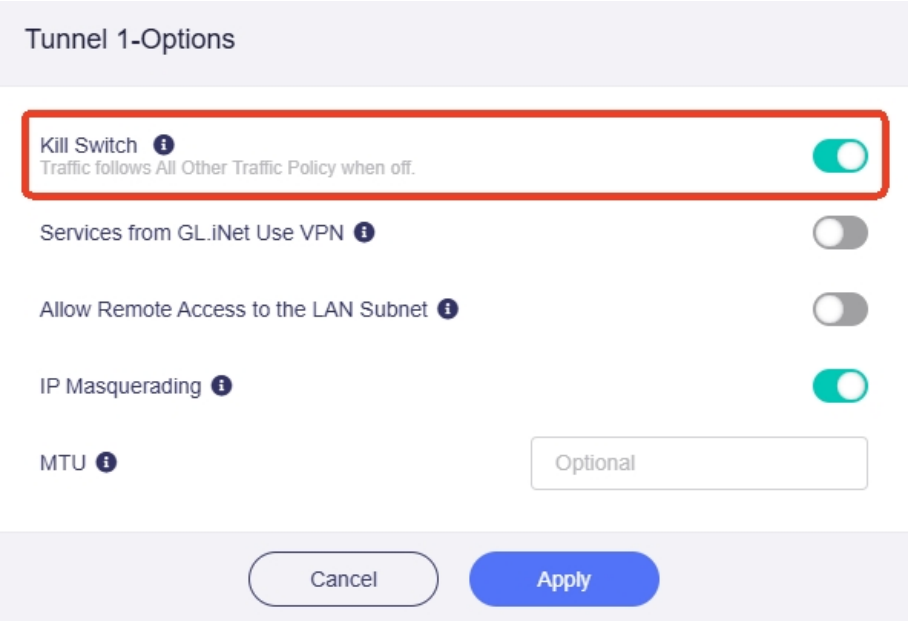


4. Se le dirigirá al panel de VPN. Ahora el túnel VPN 1 se ha agregado correctamente.

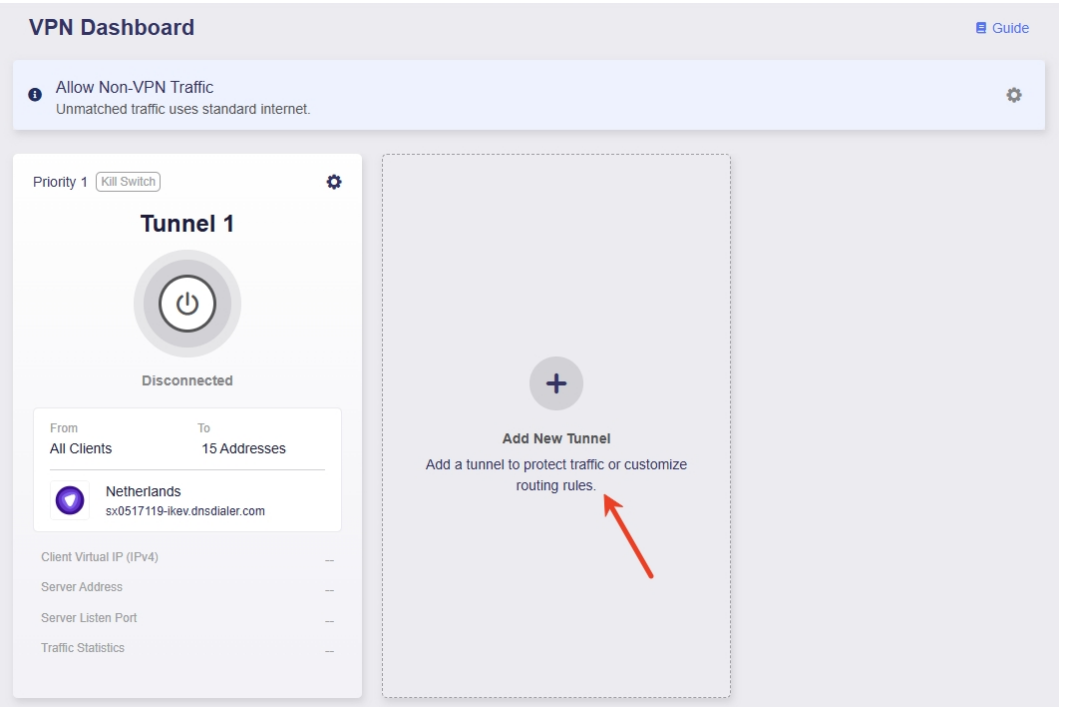


5. Asegúrese de que el **Bloqueo de tráfico sin VPN (Kill Switch)** para el túnel 1 esté habilitado. Si la VPN se desconecta inesperadamente, se bloqueará el acceso a Internet para el tráfico que coincida con este túnel para evitar fugas de DNS y seguimiento de IP.





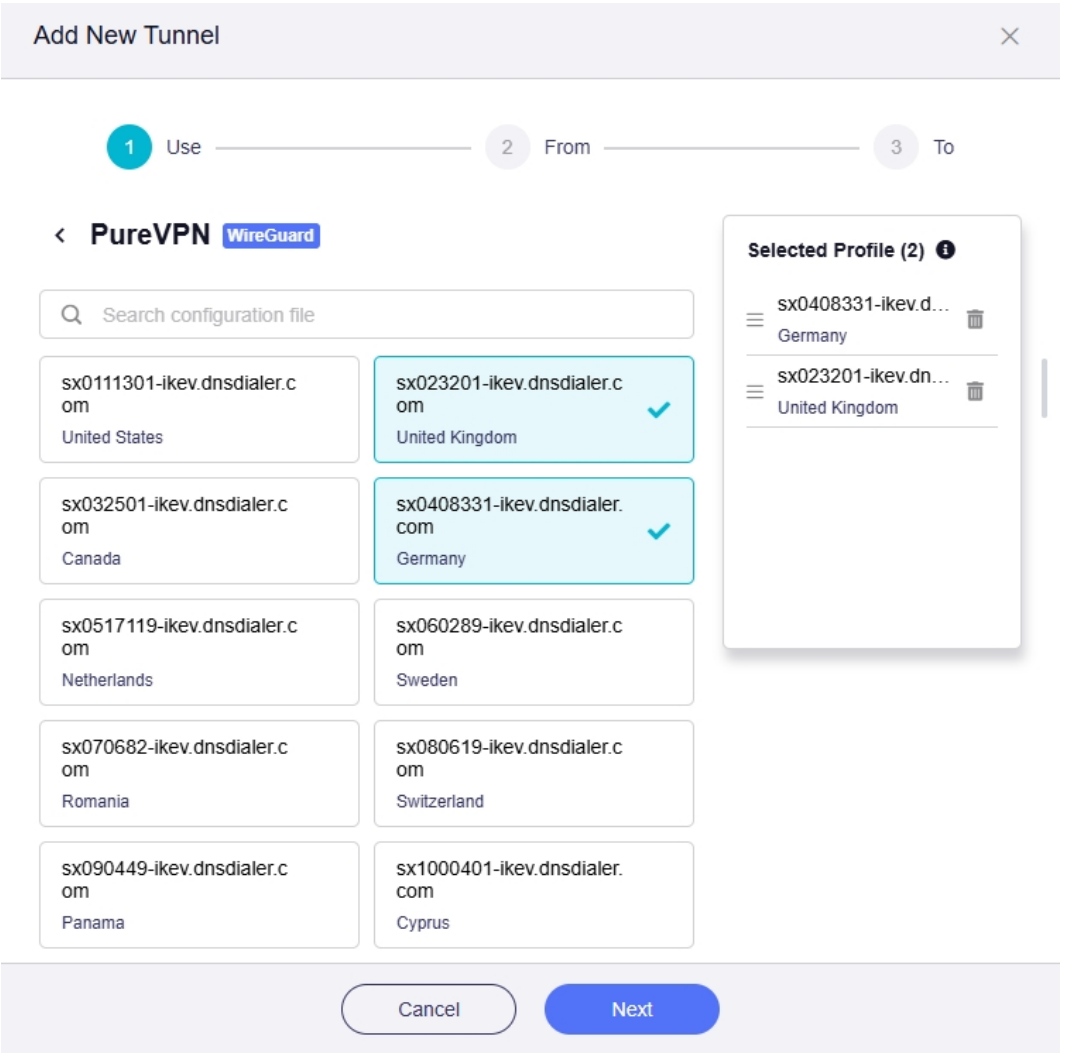
6. Haga clic en **Agregar nuevo túnel** para agregar el túnel 2.



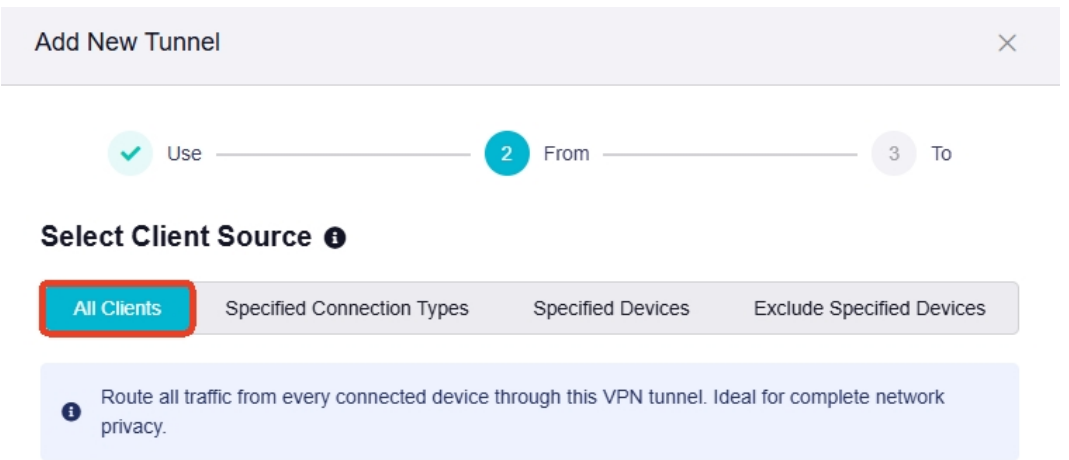
7. Seleccione el perfil de VPN para el túnel 2.

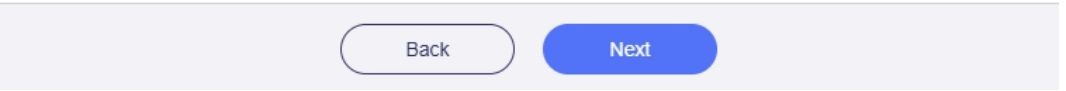
   Seleccione uno o varios perfiles y ajuste su prioridad a la derecha si es necesario.

   Tcuando haga clic **Siguiente**.



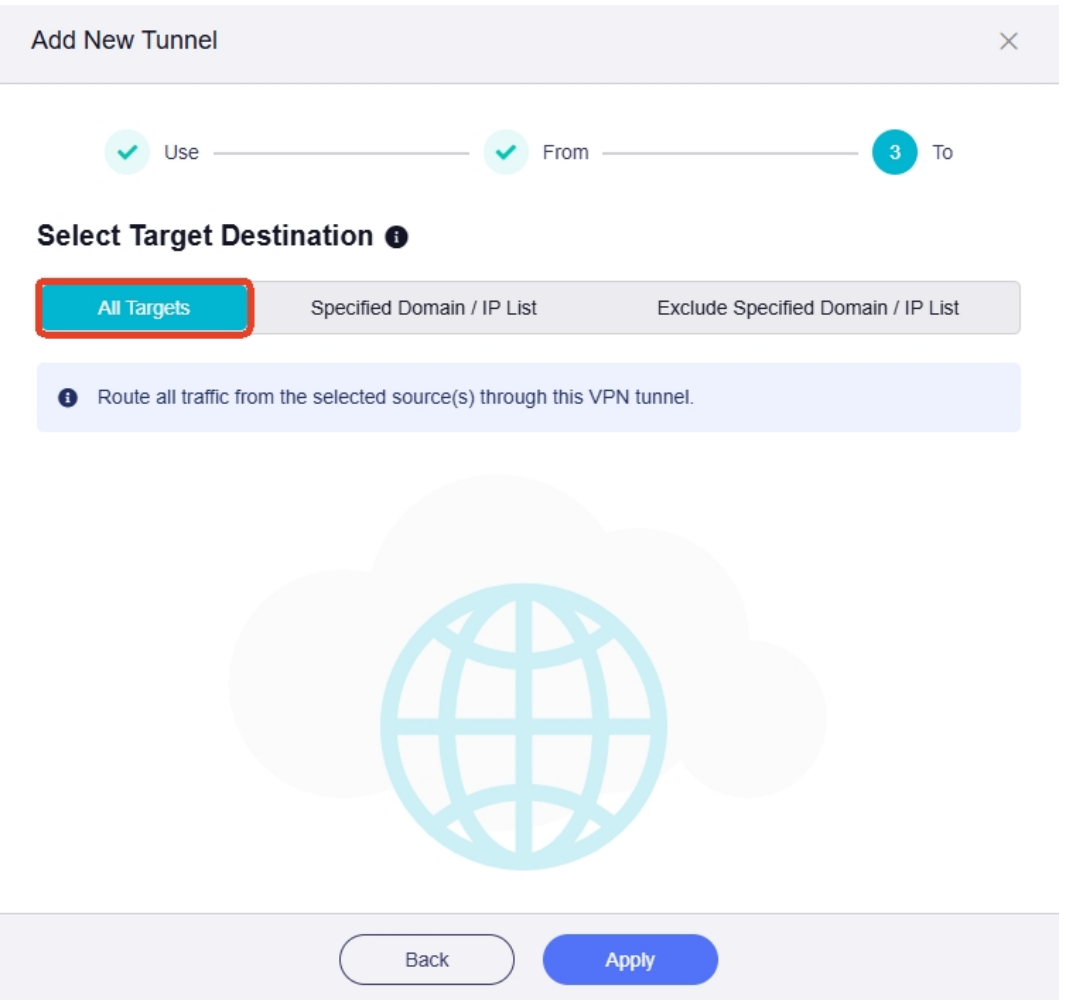
8. Seleccione la fuente del cliente.
   Haga clic en la pestaña Todos los clientes , configúrelo como origen del cliente para el túnel 2 y luego haga clic en Siguiente.



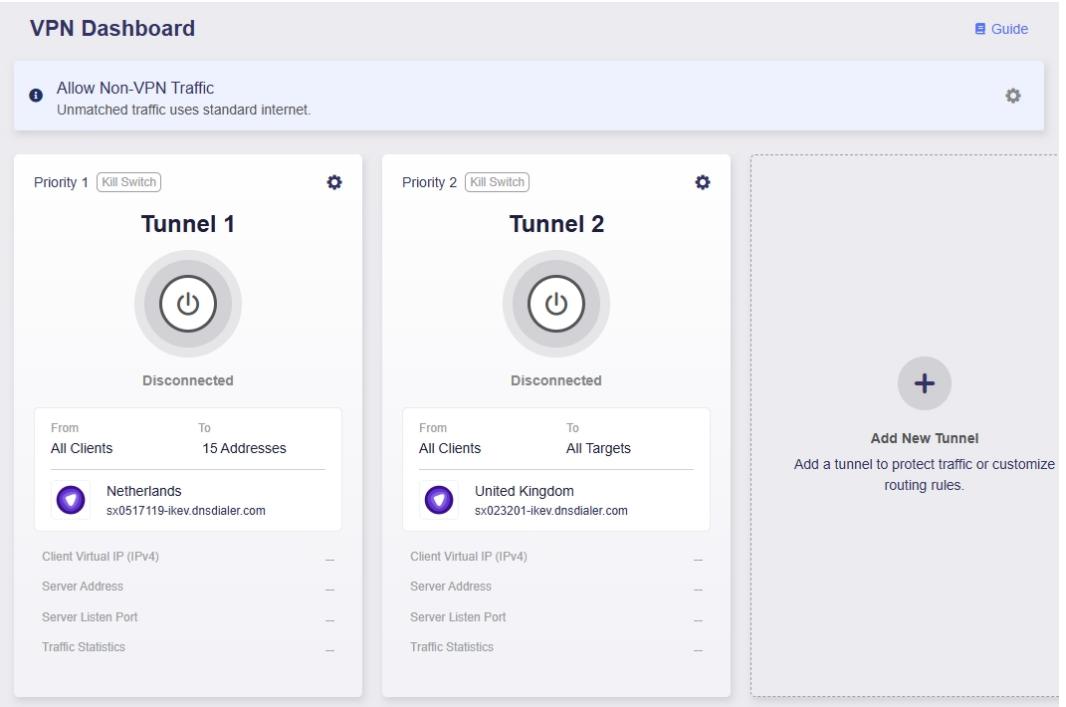


9. Seleccione el destino de destino.

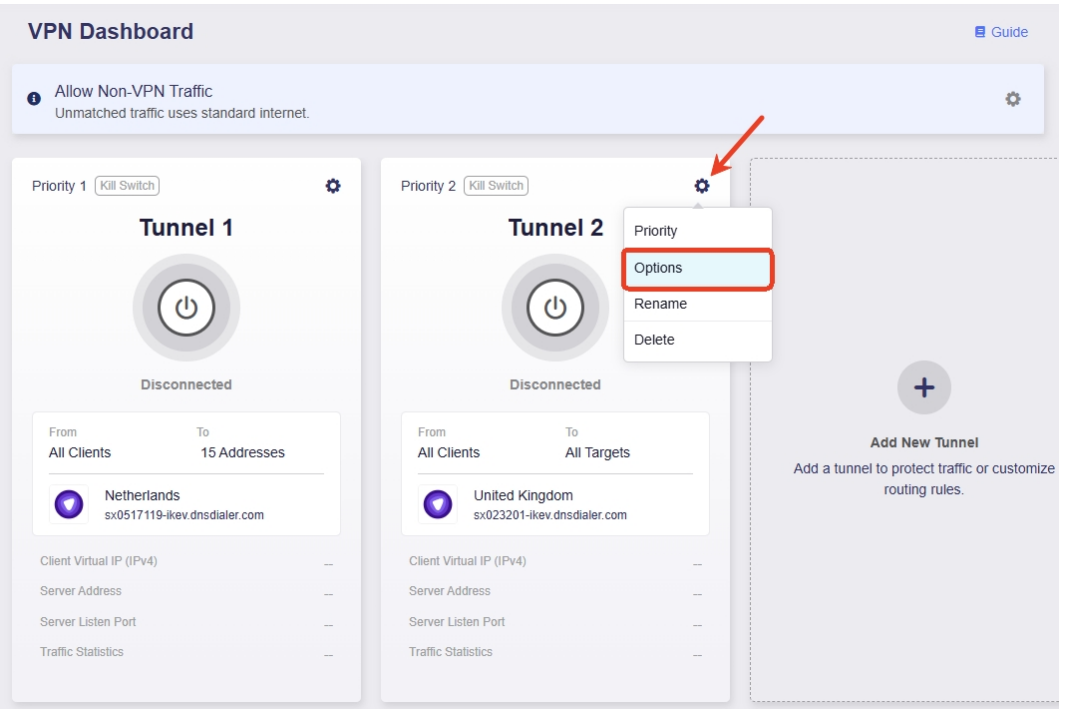
   Haga clic en la pestaña **Todos los objetivos** , configúrela como destino del tráfico para el túnel 2 y luego haga clic en **Aplicar**.

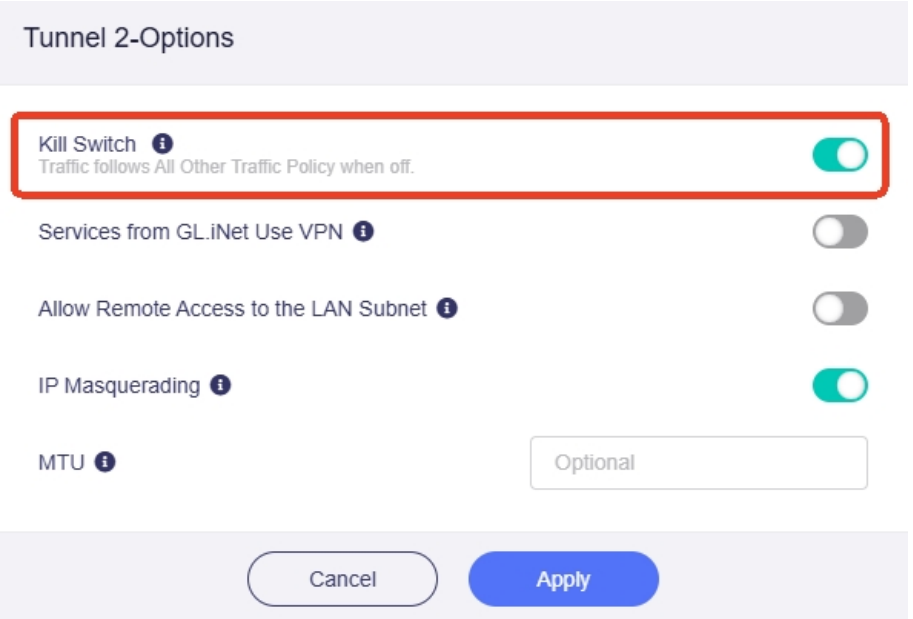


10. Se le dirigirá al panel de VPN. Ahora el túnel VPN 2 se ha agregado correctamente.

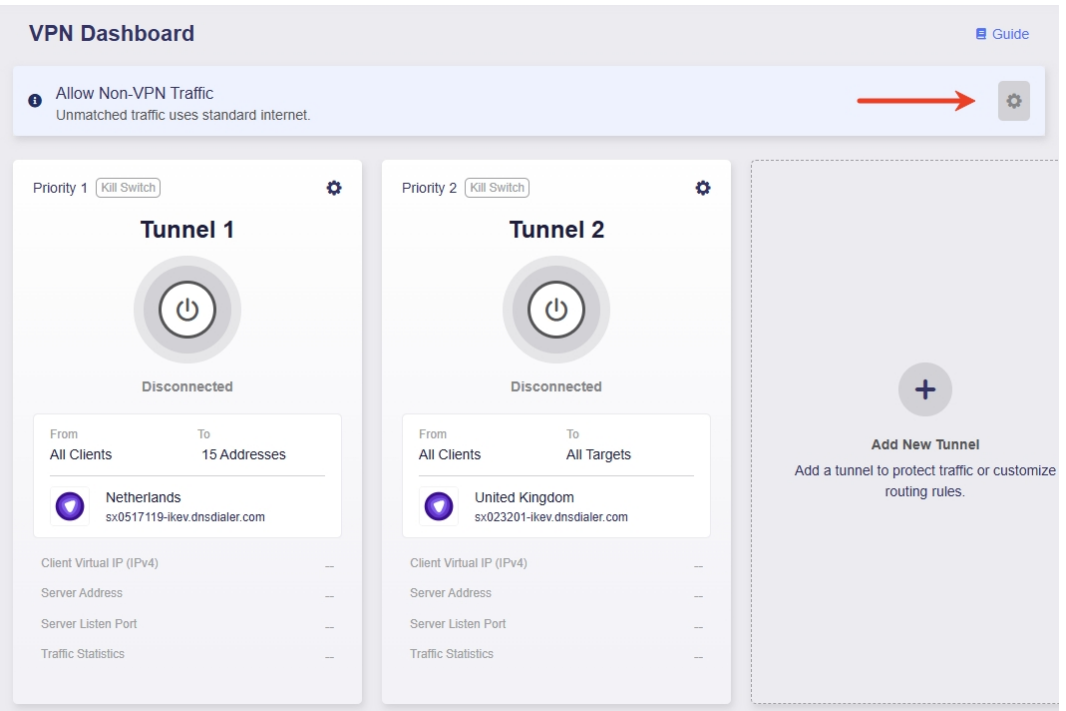


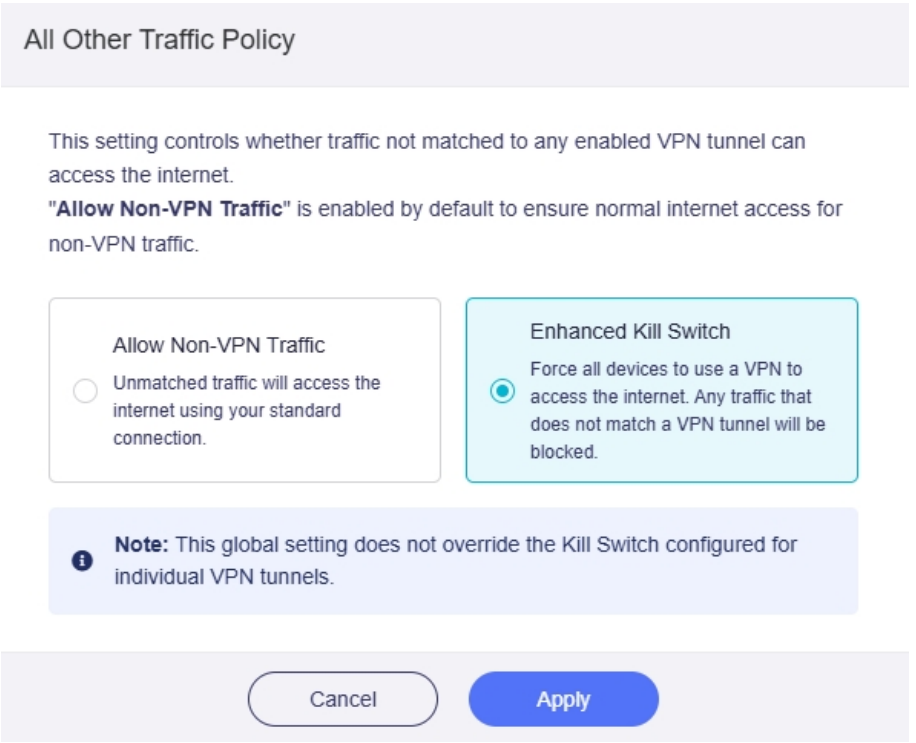
11. Asegúrese de que el **Bloqueo de tráfico sin VPN (Kill Switch)** para el túnel 2 esté habilitado. Si la VPN se desconecta inesperadamente, se bloqueará el acceso a Internet para el tráfico que coincida con este túnel para evitar fugas de DNS y seguimiento de IP.



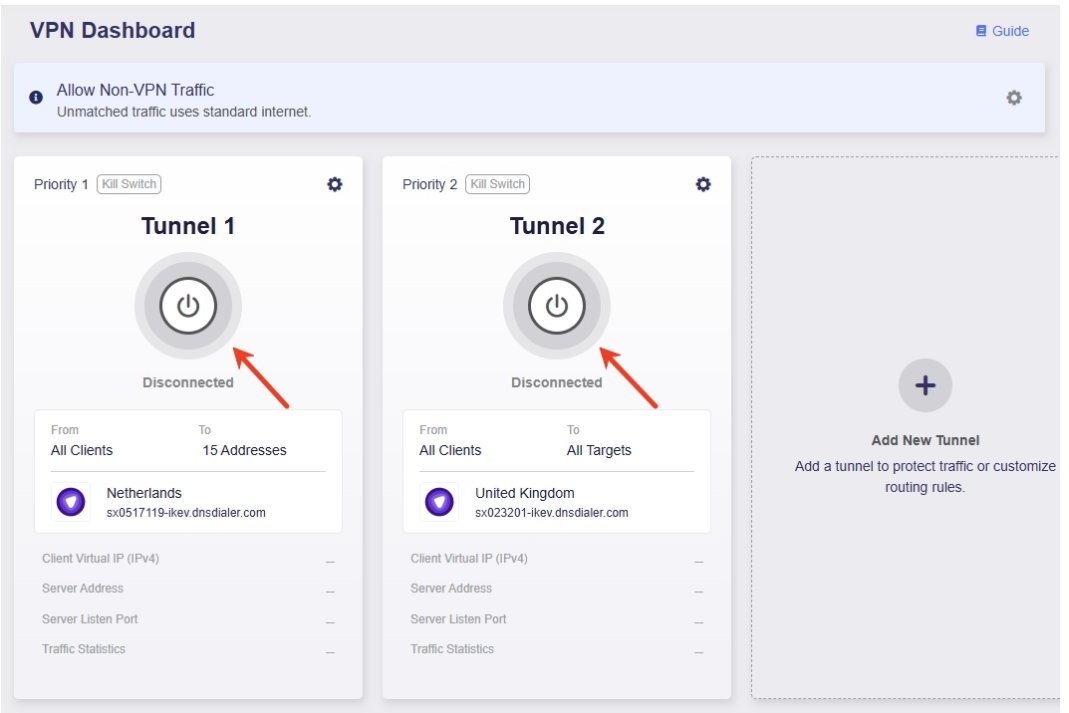


12. Haga clic en el ícono de ajustes en la parte superior derecha para habilitar **Interruptor de apagado mejorado**. Esto garantiza que todo el tráfico debe acceder a Internet a través de la VPN.

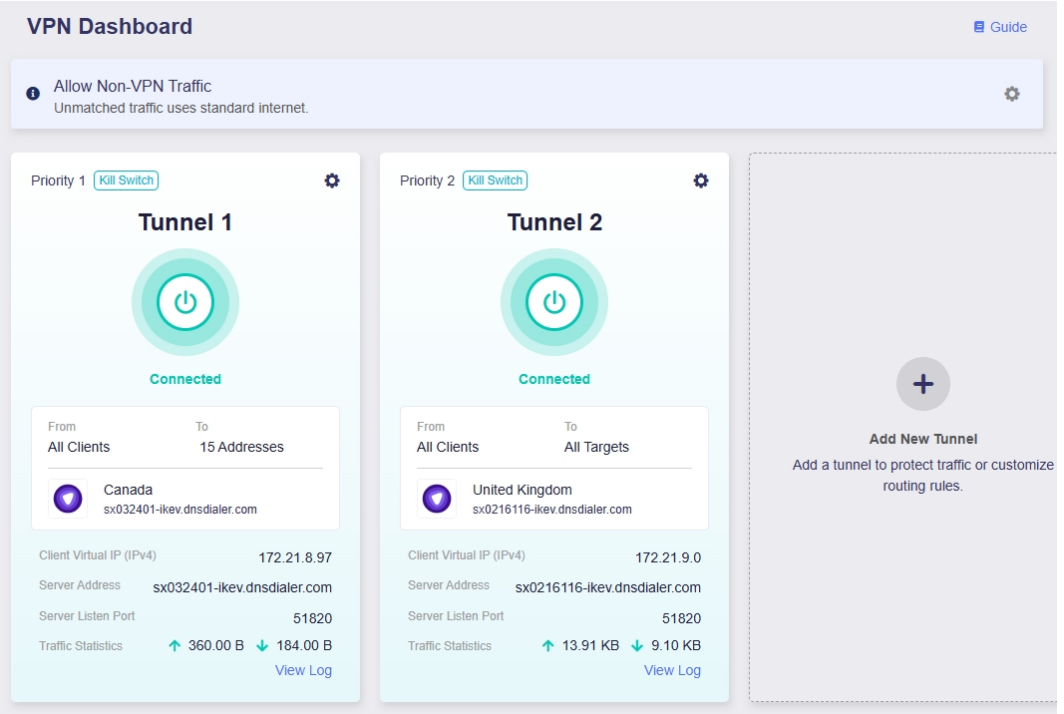




13. Haga clic en el botón central para activar el Túnel 1 y el Túnel 2.



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



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

8.3 Bloqueo de tráfico sin VPN (Kill Switch)

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

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

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

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

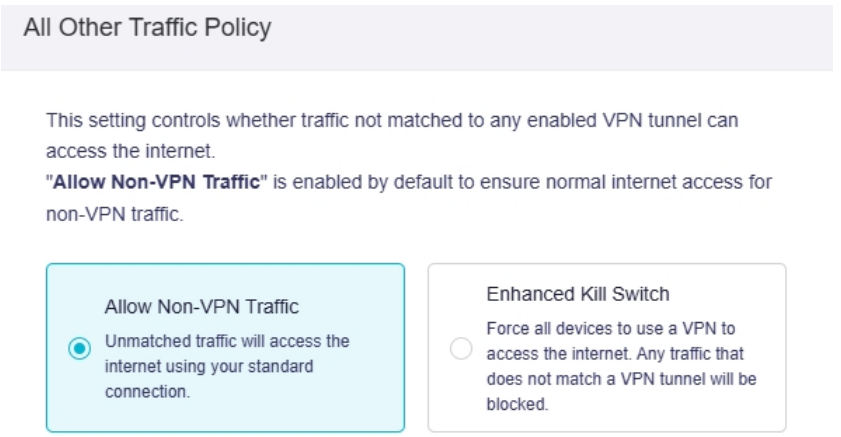
8.4 Todo el resto del tráfico

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

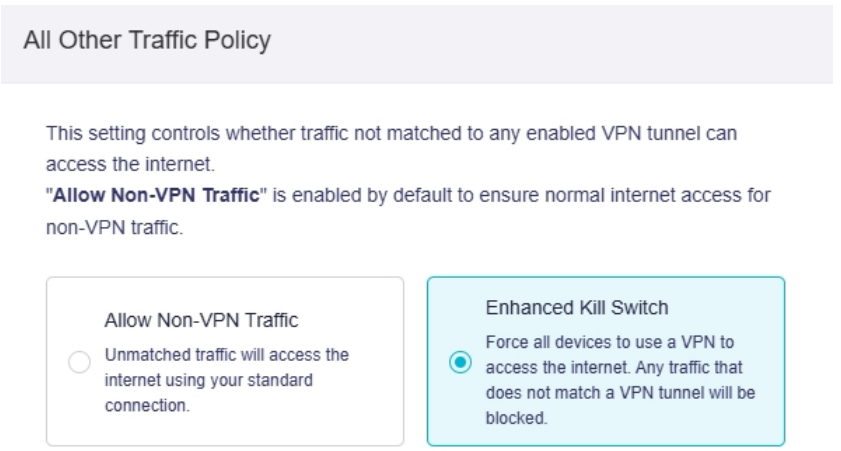


Esta política controla si el tráfico que no coincide con ninguno de sus grupos de túneles VPN puede acceder a Internet o no. Tiene dos opciones:

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



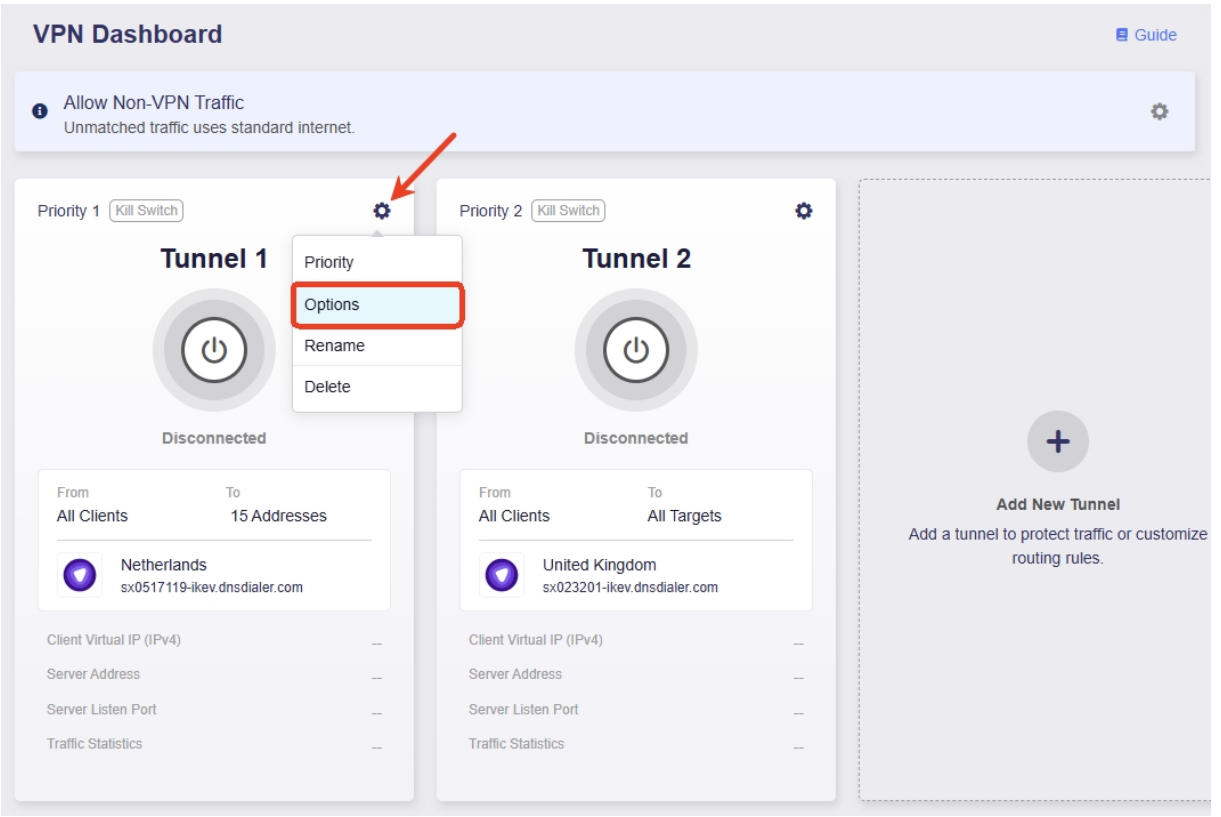
- **Interruptor de apagado mejorado**: Fuerza a todos los dispositivos a acceder a Internet a través de una VPN. Se bloqueará cualquier tráfico que no coincida con un túnel VPN. Esta configuración global no anula el interruptor de interrupción configurado para túneles VPN individuales.

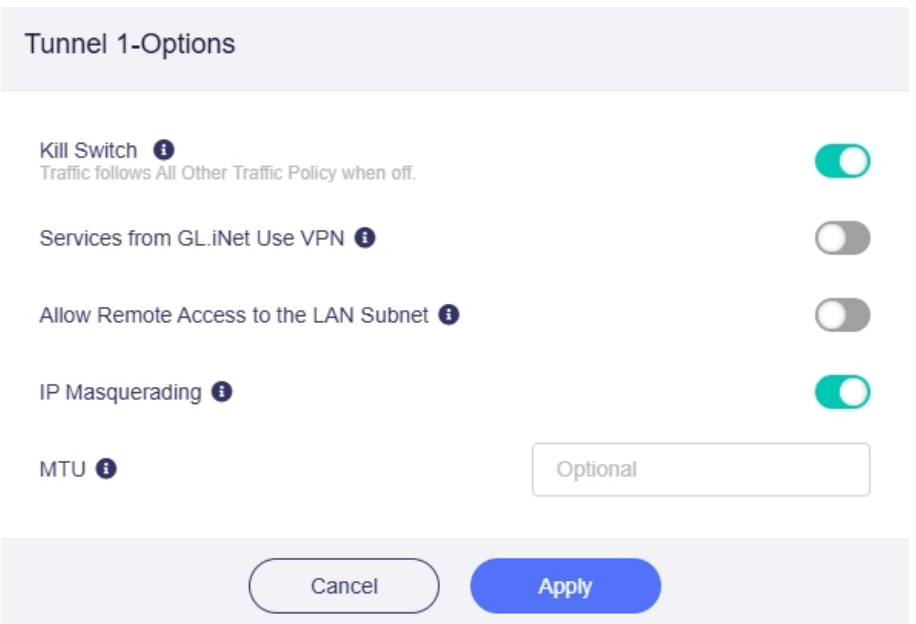


8.5 Opciones de túnel

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

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

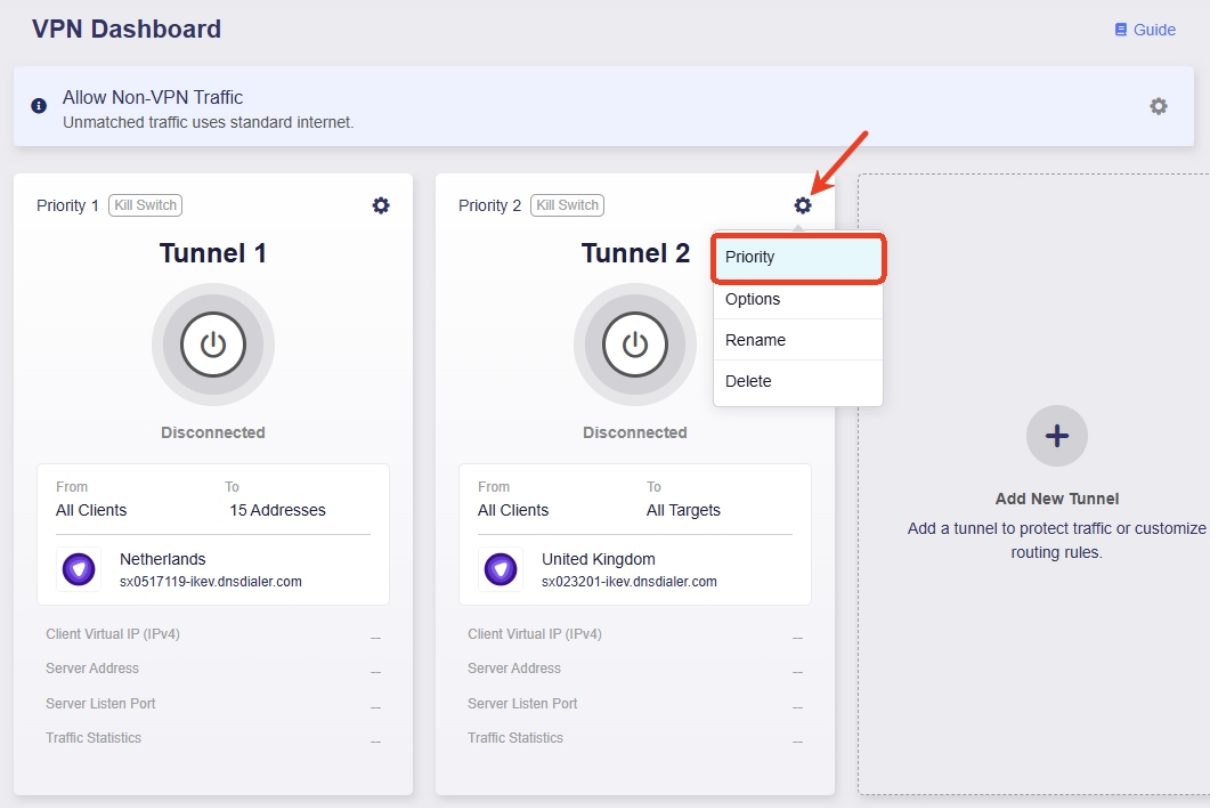




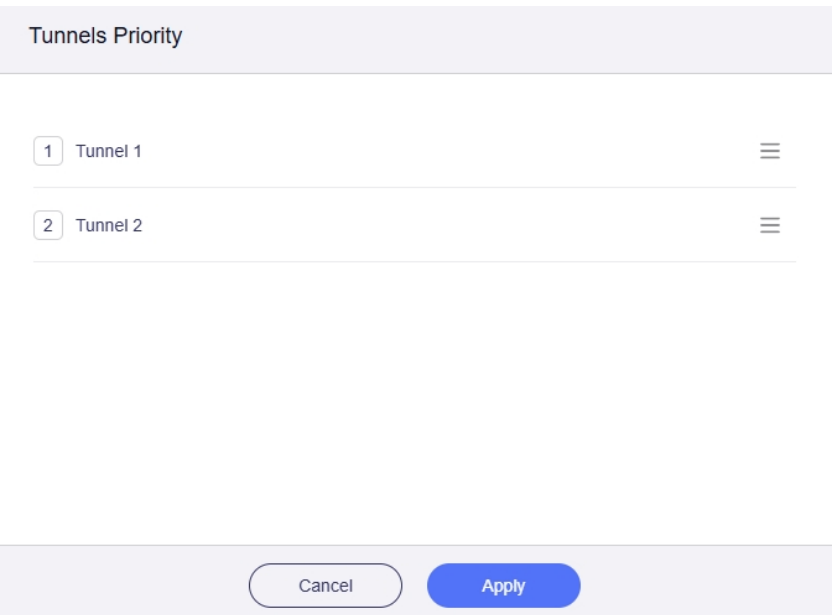
- **Bloqueo de tráfico sin VPN (Kill Switch)**: si está habilitado, el tráfico que coincida con este túnel VPN se bloqueará si la conexión VPN falla inesperadamente. Si está deshabilitado, dicho tráfico pasará por error al túnel Todo el resto del tráfico .
- **Los servicios de GL.iNet usan VPN**: si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

8.6 Prioridad del túnel

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



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



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

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

- **Interruptor de interrupción mejorado**: obliga a todos los dispositivos a acceder a Internet a través de una VPN. Se bloqueará cualquier tráfico que no coincida con un túnel VPN. Esta configuración global no anula el Kill Switch configurado para túneles VPN individuales. En resumen, fortalece el Kill Switch y bloquea el acceso regular a Internet para evitar fugas de IP.

Capítulo 9

Configurar el servidor VPN

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

9.1 Configurar el servidor OpenVPN

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

9.1.1 Preparación

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

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

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

   Métodos alternativos:

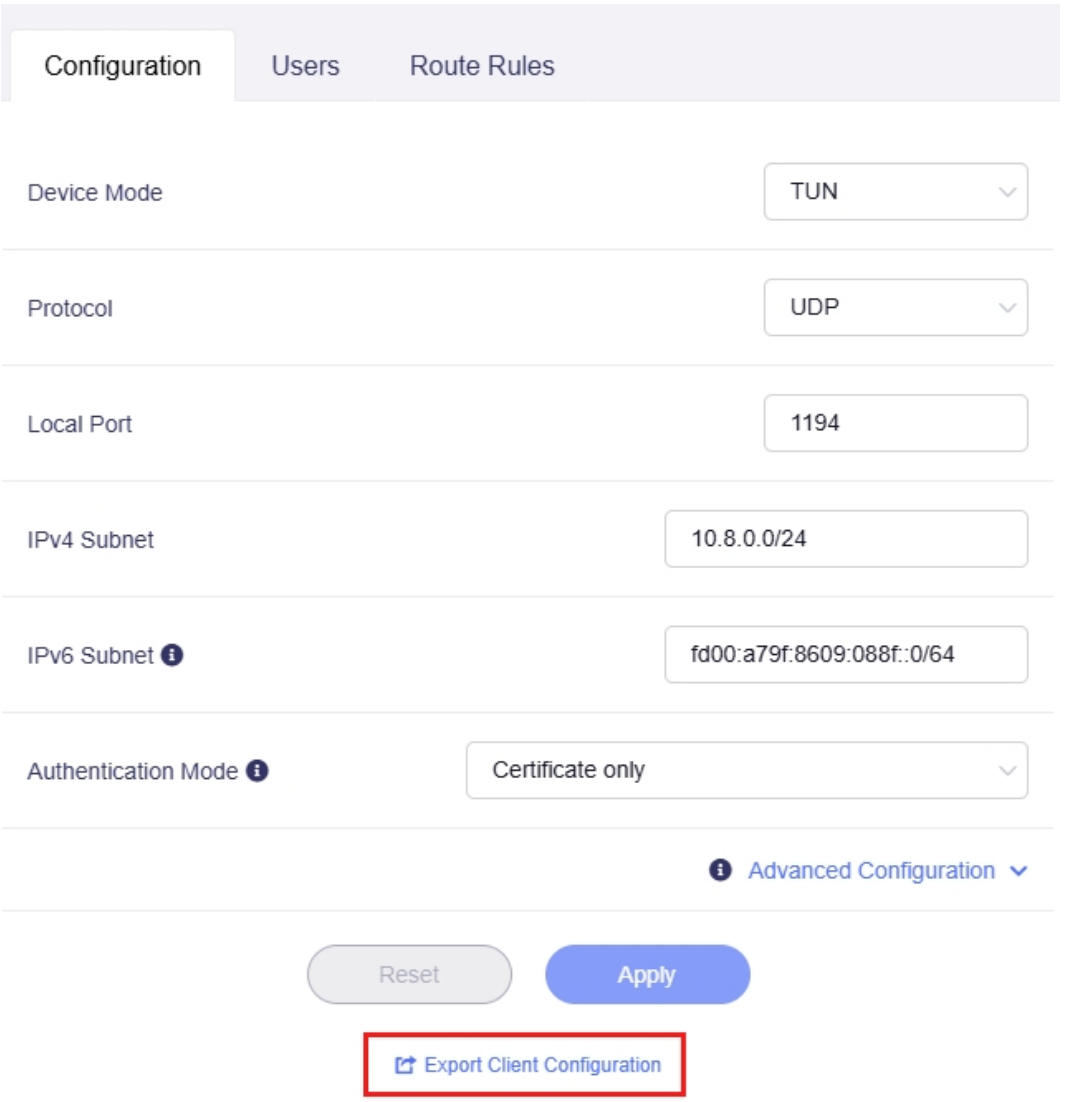
   - Si tiene un enrutador principal aguas arriba de su enrutador GL.iNet, inicie sesión en él y verifique que tenga una dirección IP pública asignada por su ISP.
   - Solicite a su ISP una dirección IP pública. Esto puede generar una tarifa adicional.
   - Si los dos métodos anteriores no funcionan (por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

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

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

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.

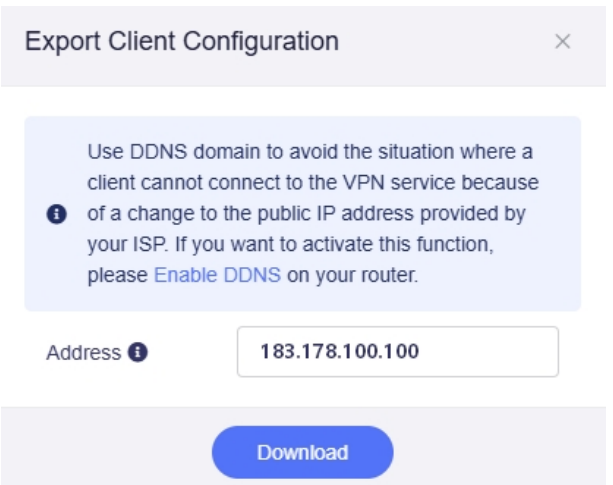


- **Dispositivo Modo**: TAP-S2S o Tun. Consulte aquí para las diferencias.
- **Protocolo**: UDP o TCP. Consulte aquí para las diferencias.

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

3. Exportar configuración del cliente.

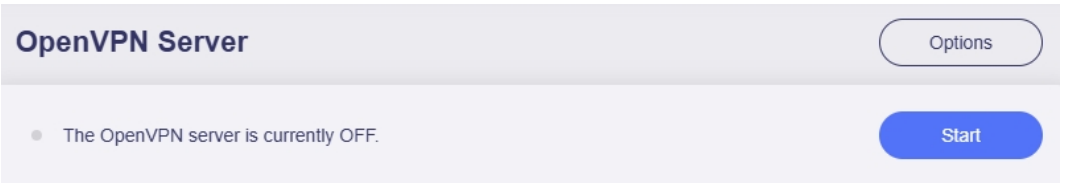
   Después de hacer clic **Exportar configuración del cliente** en la parte inferior de la pestaña Configuración (o aplicar la configuración modificada), aparecerá una ventana como la siguiente. Haga clic en **Descargar** para exportar la configuración.



Consejos:

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

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



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



9.1.3 Solución de problemas

Si la conexión falla, existen varias razones comunes:

- El servidor VPN no tiene una dirección IP pública. Consulte aquí para solucionar problemas.
- Es posible que deba configurar el reenvío de puertos. Consulte aquí para solucionar problemas.

- El puerto utilizado para el servidor OpenVPN está bloqueado por su proveedor de servicios de Internet. Cambie a otro puerto o comuníquese con su ISP para obtener ayuda.
- La conexión VPN puede estar bloqueada en ciertos países o regiones.

9.2 Configurar el servidor WireGuard

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

9.2.1 Preparación

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

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

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

   Alternativa métodos:

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

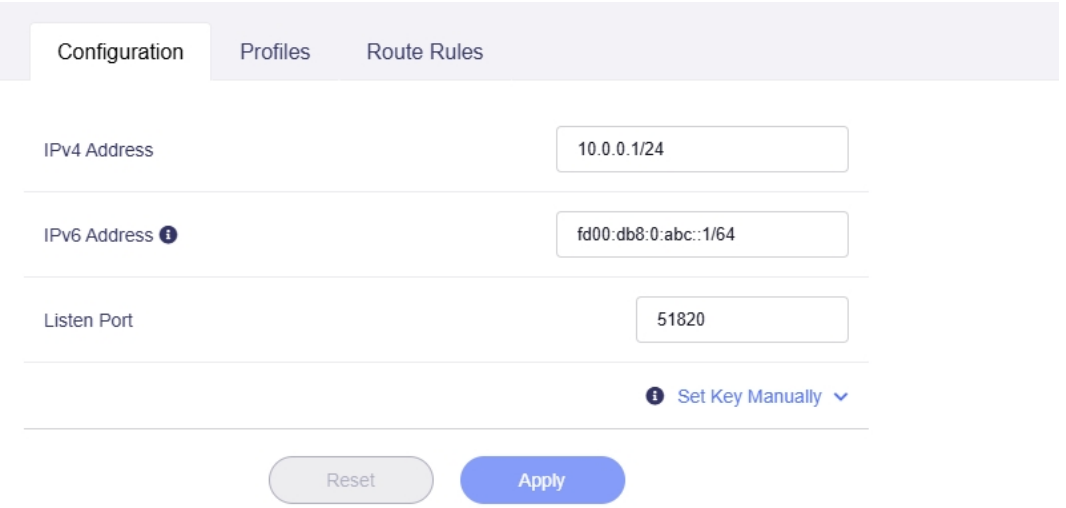
2. **Confirme si se requiere reenvío de puerto**

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

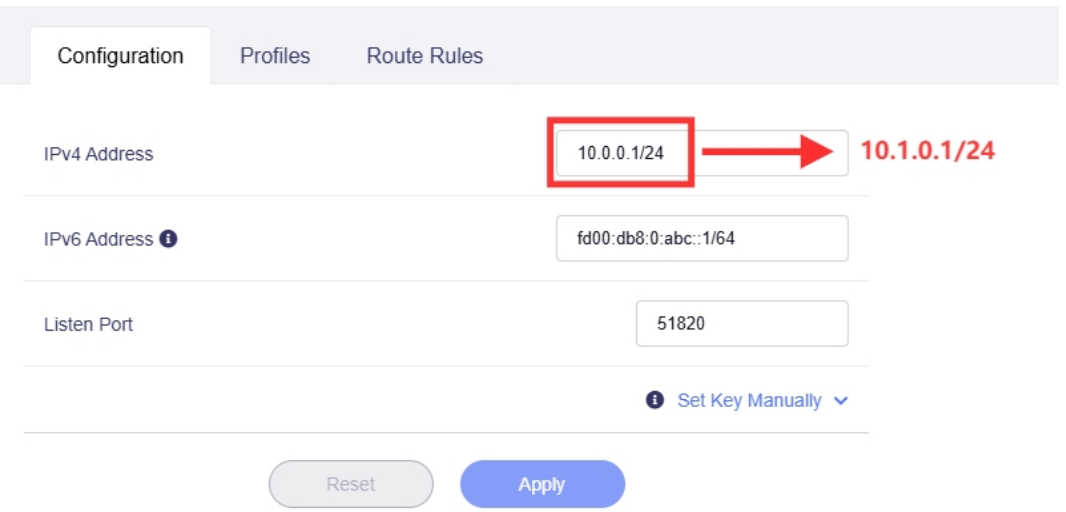
9.2.2 Pasos de configuración

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

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

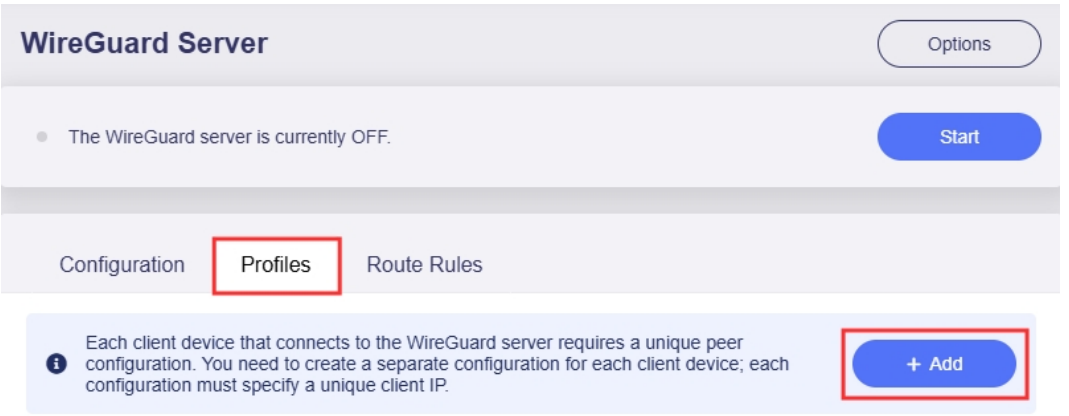


   Si la dirección IPv4 entra en conflicto con la puerta de enlace de su enrutador ascendente, modifique la dirección IPv4 a otra una (por ejemplo, **10.1.0.1/24**) y haga clic en **Aplicar**. Asegúrese de que se incluya la notación CIDR "/24" para evitar problemas de conectividad.

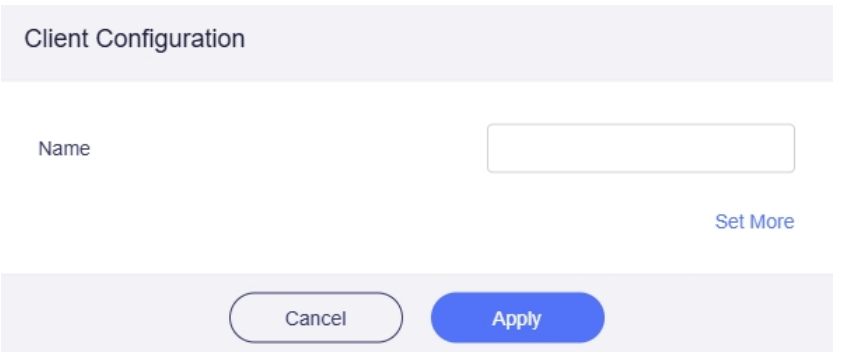


3. Agregue un perfil.

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



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



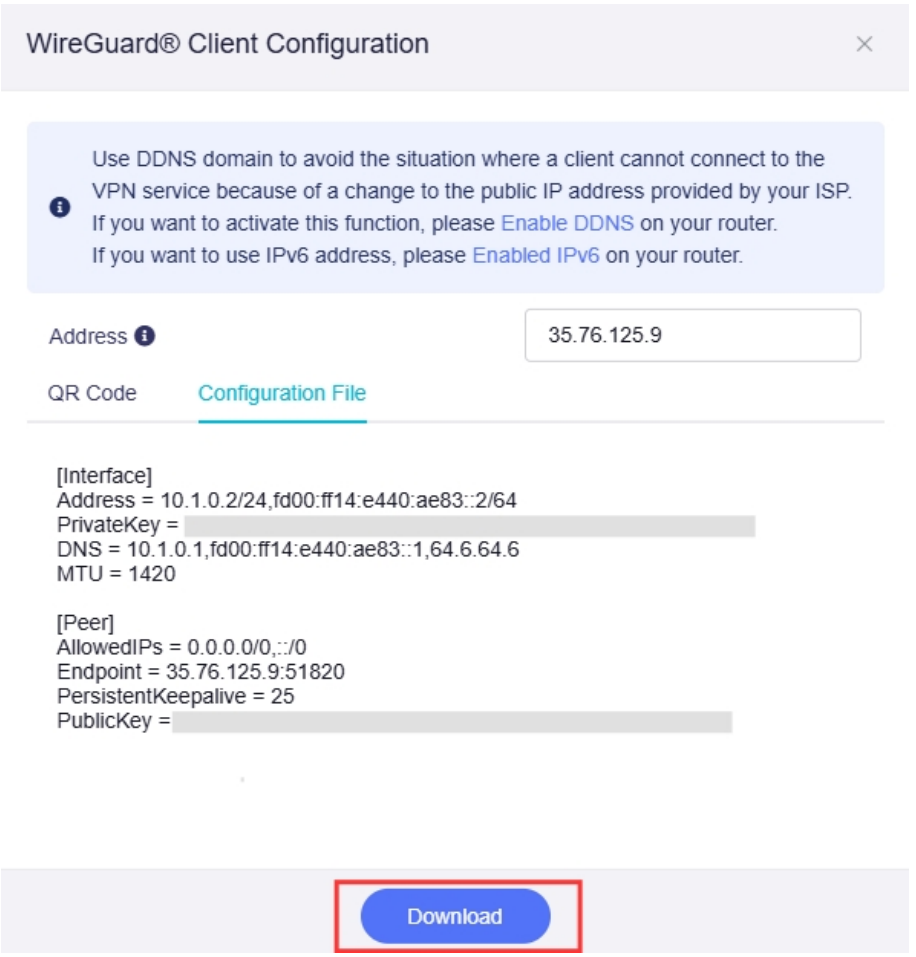
   Consejo: Si desea acceder a los dispositivos LAN del cliente WireGuard desde su servidor WireGuard , cambie a la pestaña **Reglas de ruta** para configurar reglas de ruta. Consulte aquí para detalless.

4. Descargar configuración.

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

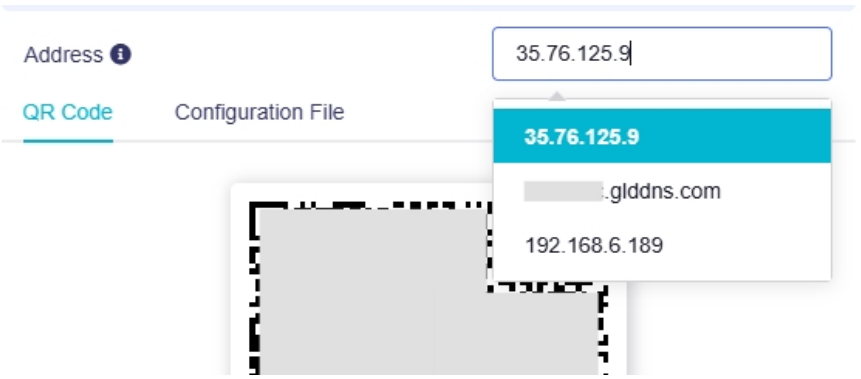
   - **Código QR**: Adecuado para dispositivos (por ejemplo, teléfonos inteligentes, tabletas, computadoras portátiles) con la aplicación WireGuard instalada. Si desea configurar un dispositivo específico como cliente WireGuard, simplemente abra la aplicación WireGuard y escanee el código QR para importar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

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

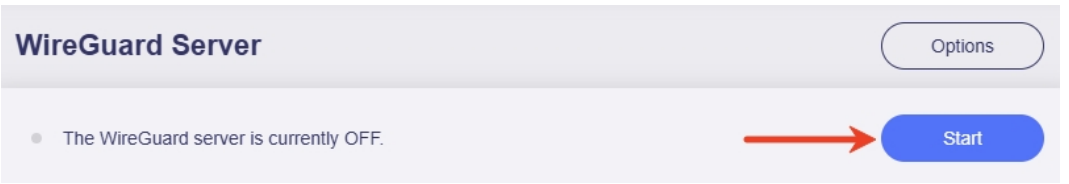


Consejos:

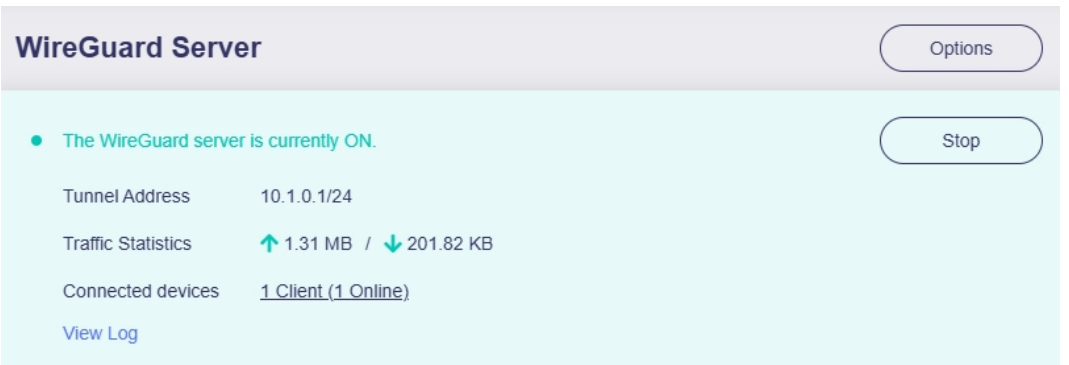
- Si su IP pública dirección cambia con frecuencia, vaya a **APLICACIONES** > **DNS dinámico** y habilite DDNS. Luego puede usar el dominio DDNS como su dirección de servidor.
- Desde firmware v4.8, puede seleccionar la dirección del servidor de una lista desplegable antes de exportar el archivo de configuración: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



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



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



9.2.3 Solución de problemas

Si la conexión falla, existen varias razones comunes:

- El servidor VPN no tiene una dirección IP pública. Consulta aquí para solucionar problemas.
- Es posible que tengas que configurar el reenvío de puertos. Consulta aquí para solucionar problemas.

- El puerto utilizado para el servidor WireGuard está bloqueado por su proveedor de servicios de Internet. Cambie a otro puerto o comuníquese con su ISP para obtener ayuda.
- La conexión VPN puede estar bloqueada en ciertos países o regiones.

Capítulo 10

Configurar el cliente VPN

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

10.1 Configurar el cliente OpenVPN

10.1.1 Preparación

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

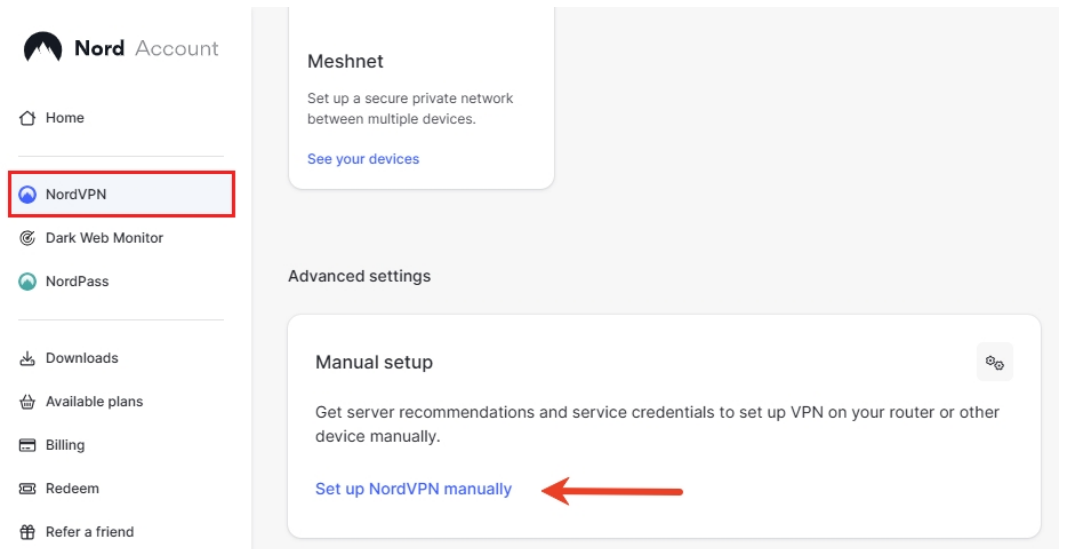
A continuación, visite el sitio web oficial del proveedor de servicios VPN al que se suscribió y obtenga las credenciales de servicio o el archivo de configuración. Si no sabe cómo obtener el archivo de configuración, consulte este enlace o póngase en contacto con su soporte.

10.1.2 Configurar NordVPN

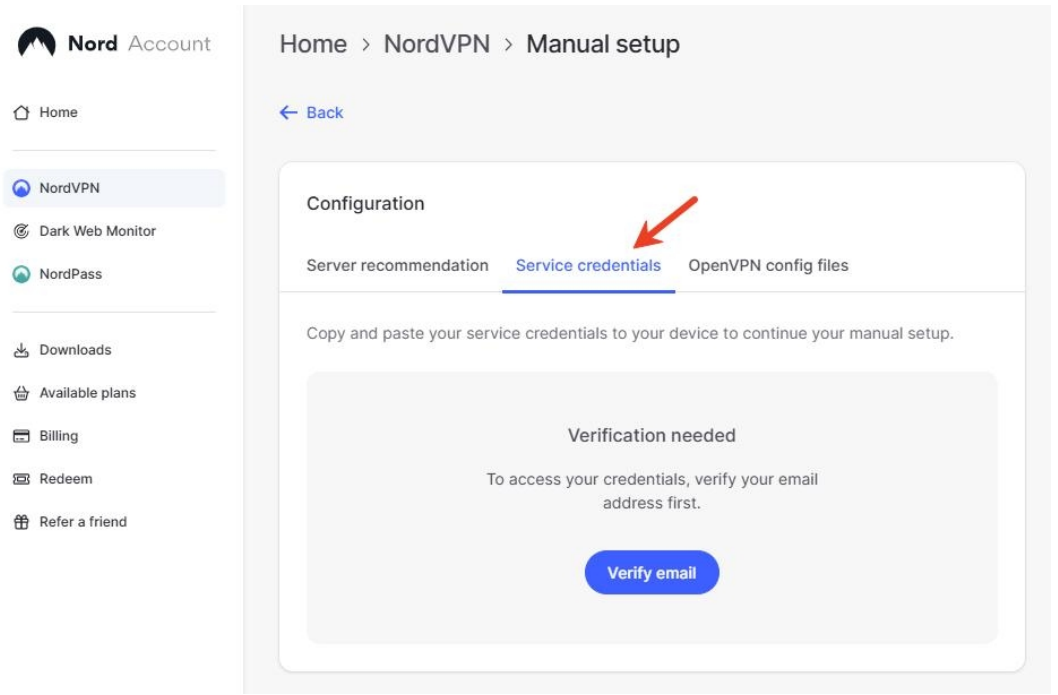
NordVPN está integrado en el panel de administración GL.iNet web . Puede adquirir archivos de configuración para todos los servidores NordVPN introduciendo las credenciales de su cuenta (obtenidas del Panel de NordVPN) en el panel de administración web del enrutador o en la aplicación móvil GL.iNet ,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

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

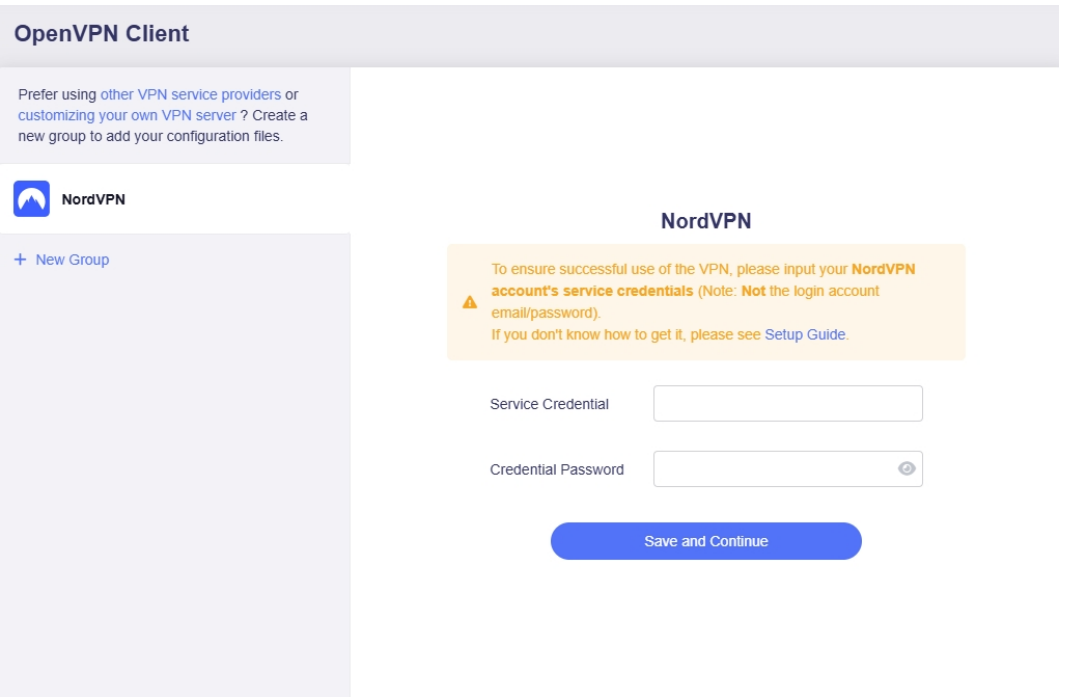
1. Inicie sesión en su cuenta web de NordVPN aquí.
2. Oen el Panel de control de Nord, haga clic en **NordVPN**, luego haga clic en **Configurar NordVPN manualmente**.



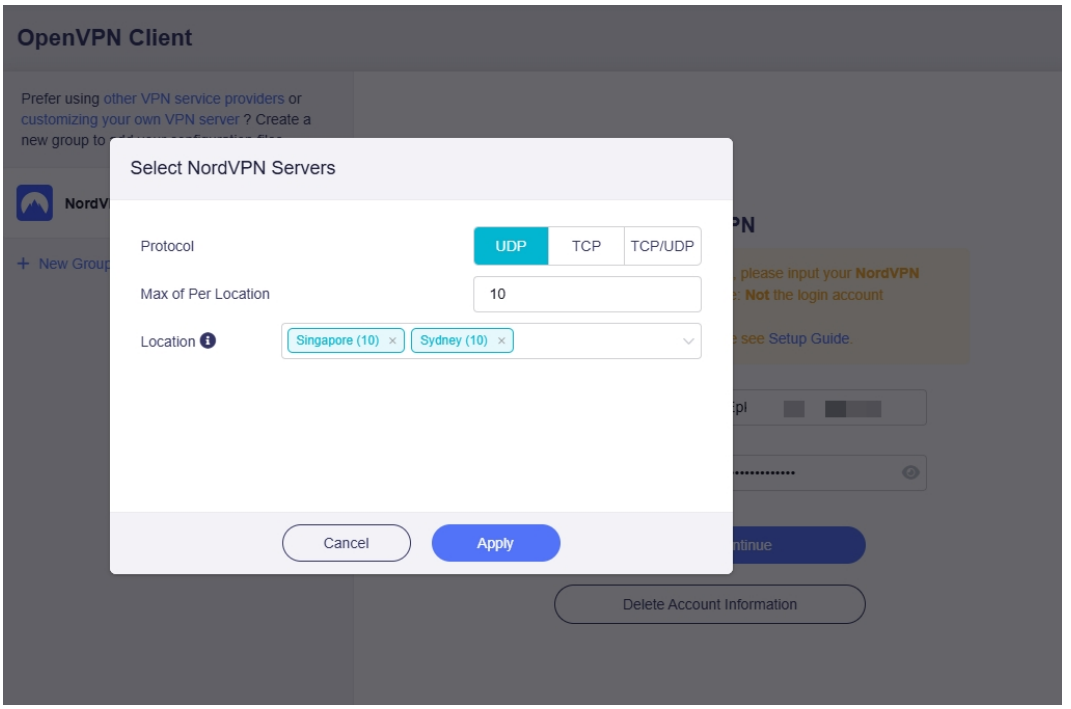
Encontrará el **credenciales de servicio**. Cópielos para usarlos más adelante.



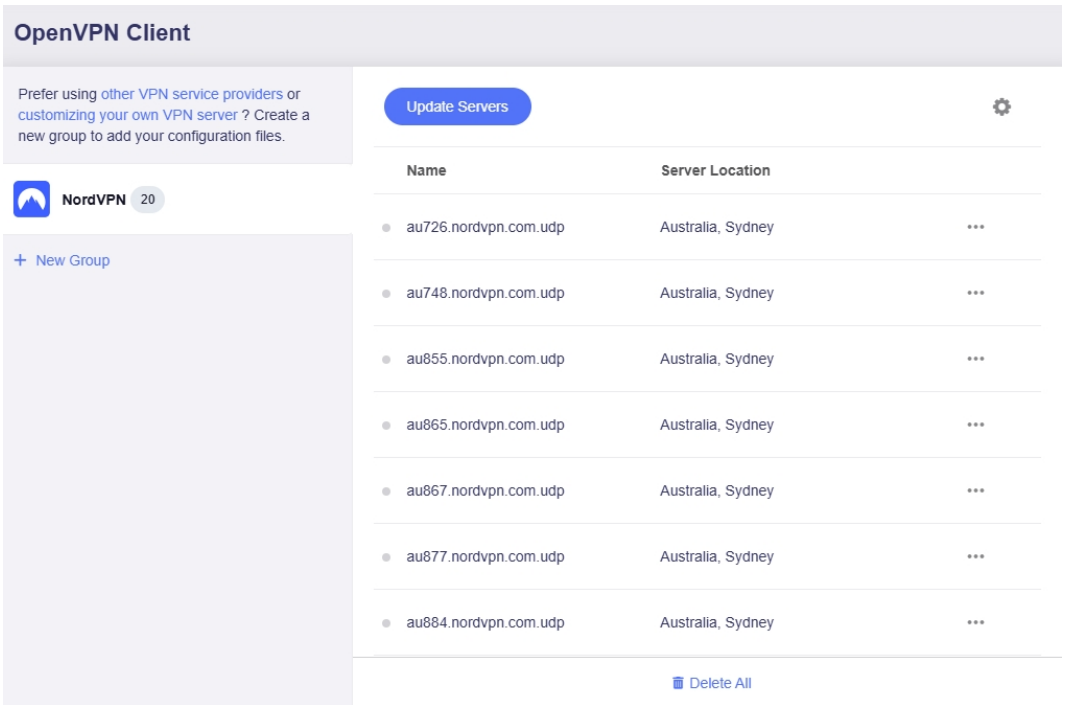
3. Inicie sesión en el panel de administración web de su enrutador y navegue hasta **VPN** > **Cliente OpenVPN** > **NordVPN**. Input the service credentials (Nota: NO es el correo electrónico ni la contraseña de la cuenta de inicio de sesión), luego haga clic en **Guardar y continuar**.



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

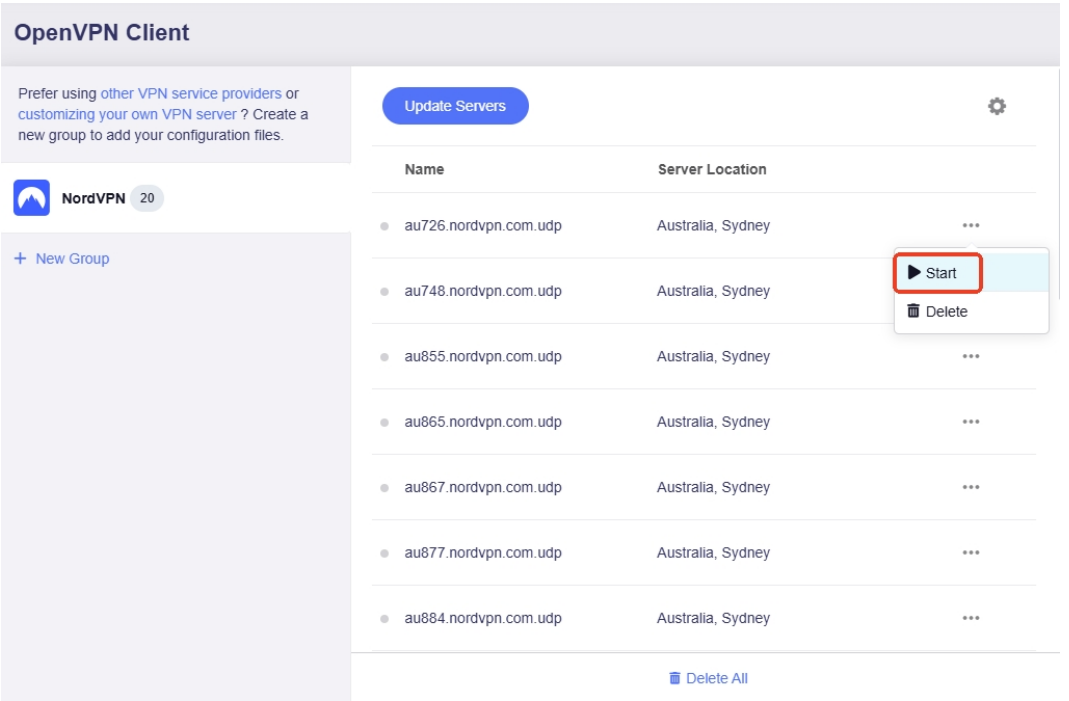


Descargará archivos de configuración.

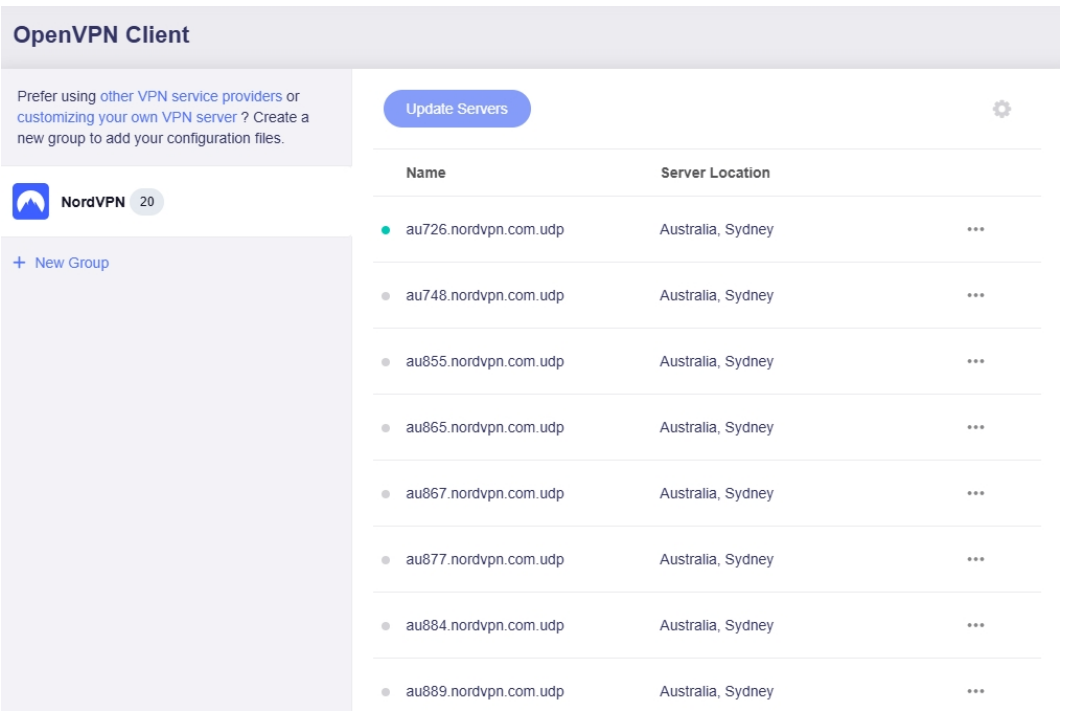


5. Iniciará una conexión.

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



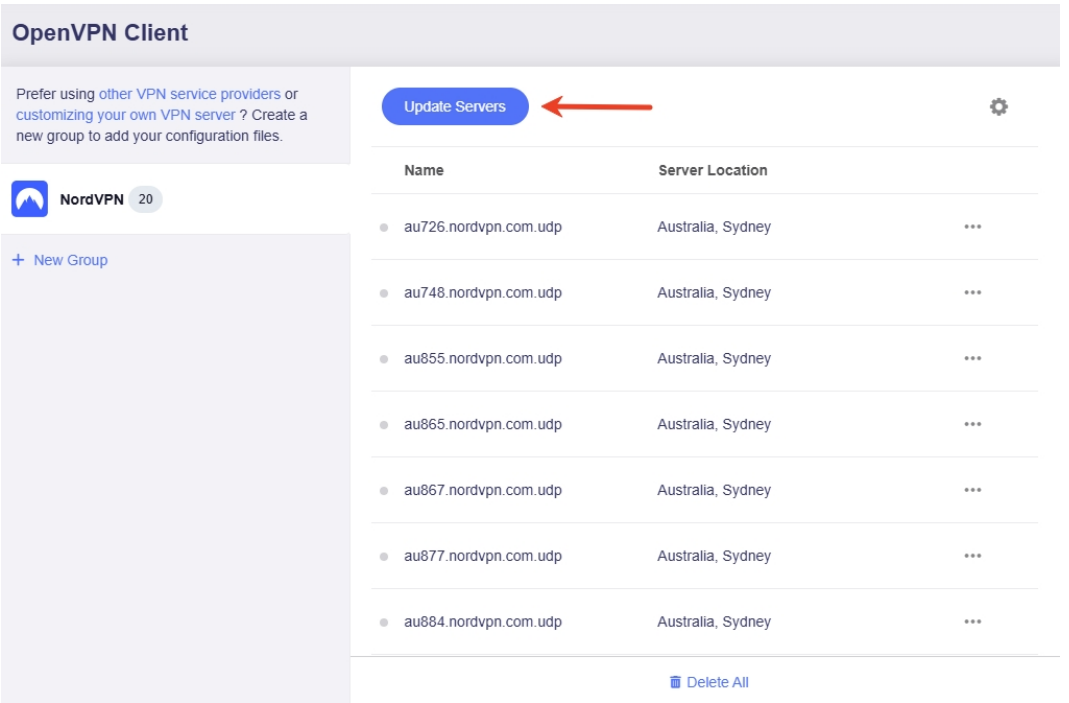
6. Una vez conectado, aparecerá un punto verde junto a el archivo de configuración.



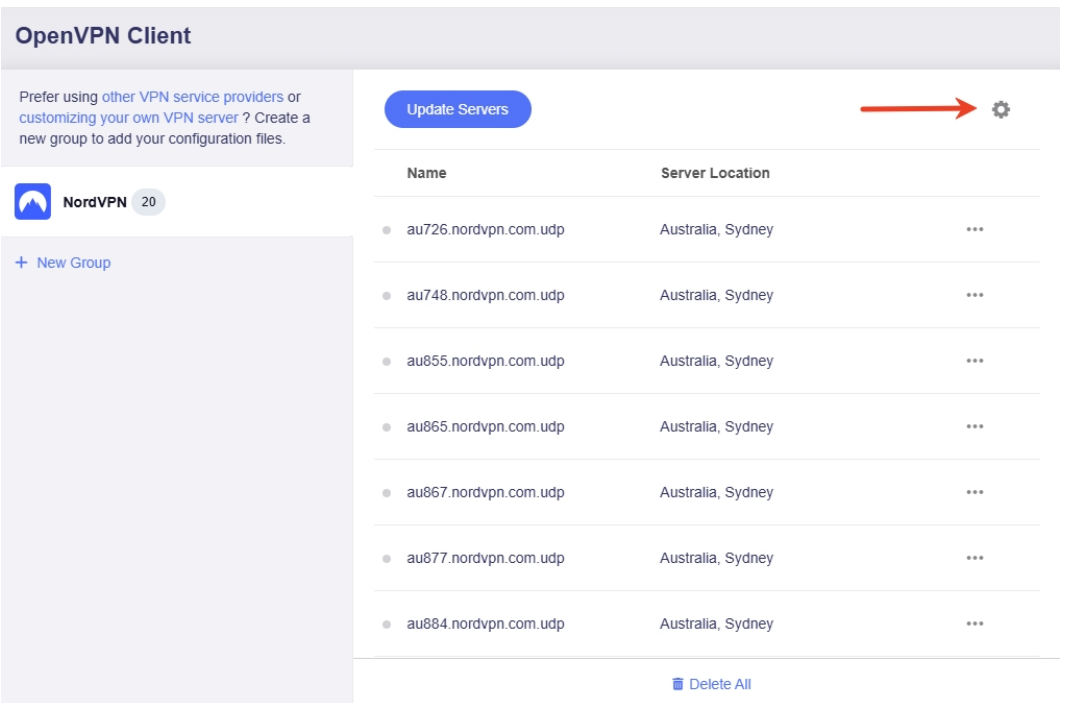
También puede consultar los detalles de la conexión VPN en el **Panel de VPN**.

7. Actualizar servidores.

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

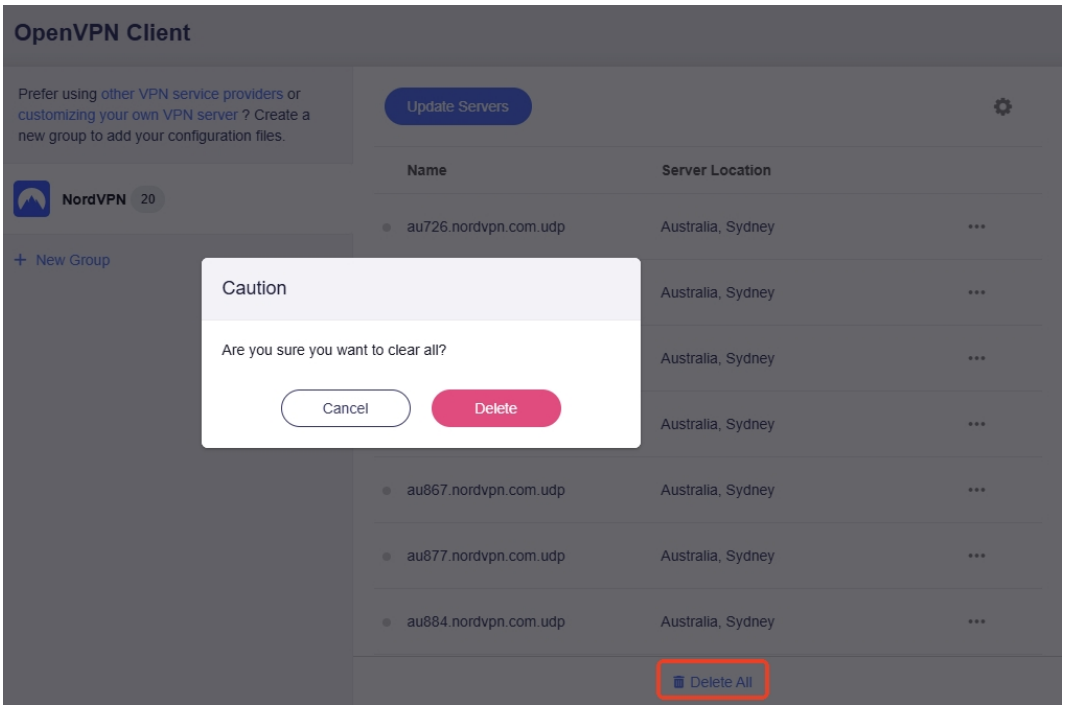


8. Editar credenciales.
   Haga clic en el ícono de ajustes para editar sus credenciales de inicio de sesión.



9. Eliminar todos los archivos.

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

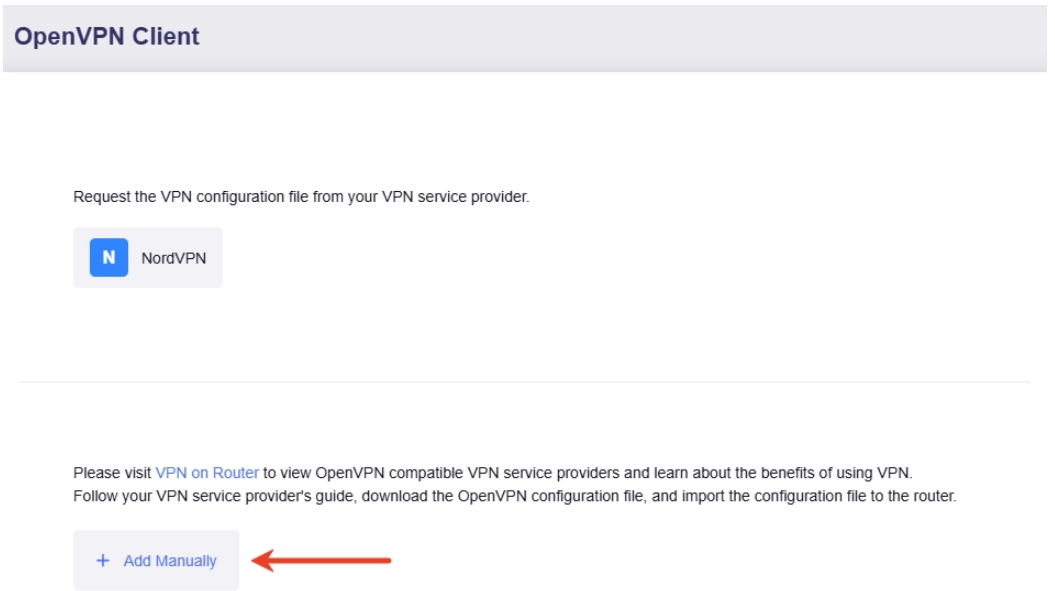


10.1.3 Configurar el cliente OpenVPN manualmente (para otros proveedores)

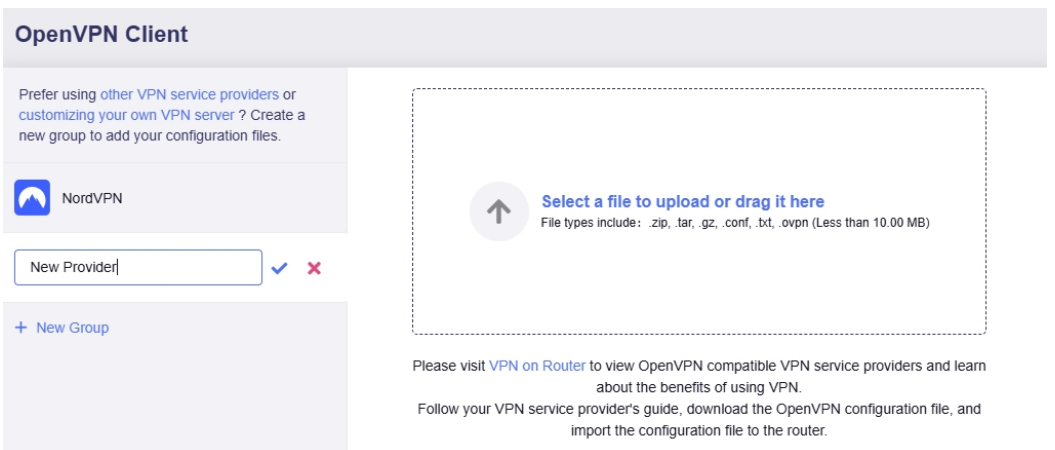
Si su proveedor de servicios OpenVPN no está integrado en nuestro panel de administración, primero visite el sitio web oficial de su proveedor de servicios suscrito para obtener el archivo de configuración. Luego cárguelo en el enrutador para configurar un cliente OpenVPN.

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

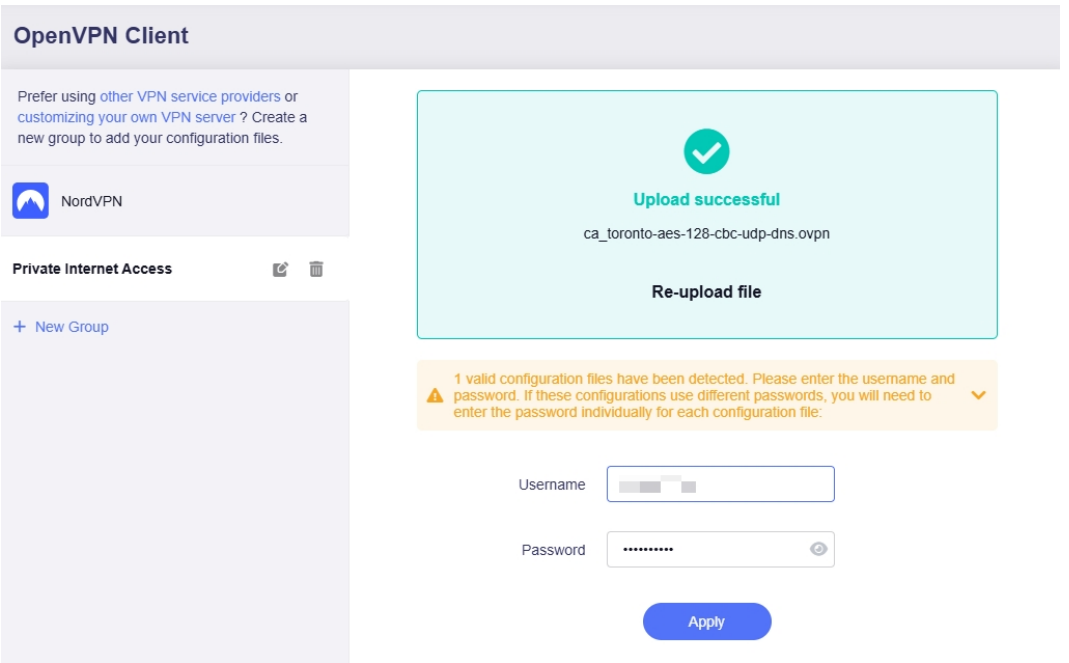
1. Descargue un archivo de configuración del sitio web oficial de Private Internet Access.
2. Inicie sesión en el panel de administración web de su enrutador, navegue hasta **VPN** > **Cliente OpenVPN** y haga clic en **Agregar manualmente**.



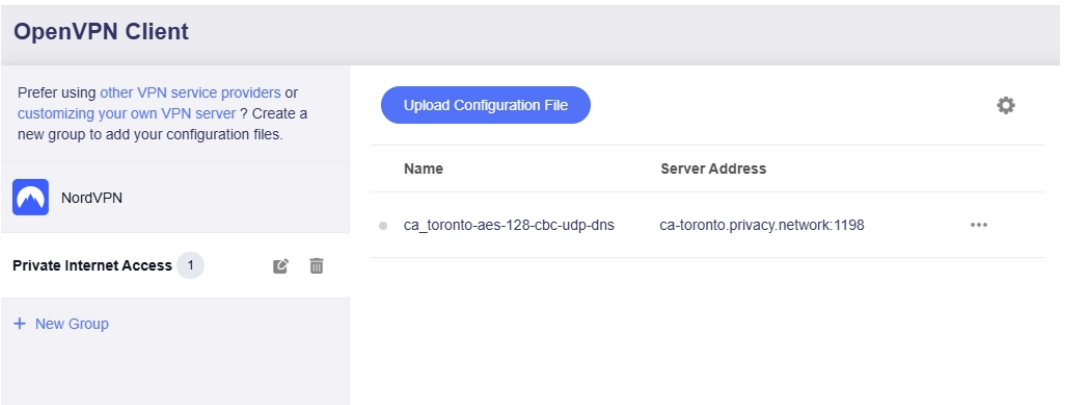
3. Se creará un grupo en la barra lateral izquierda.Establezca un nombre descriptivo para el grupo.



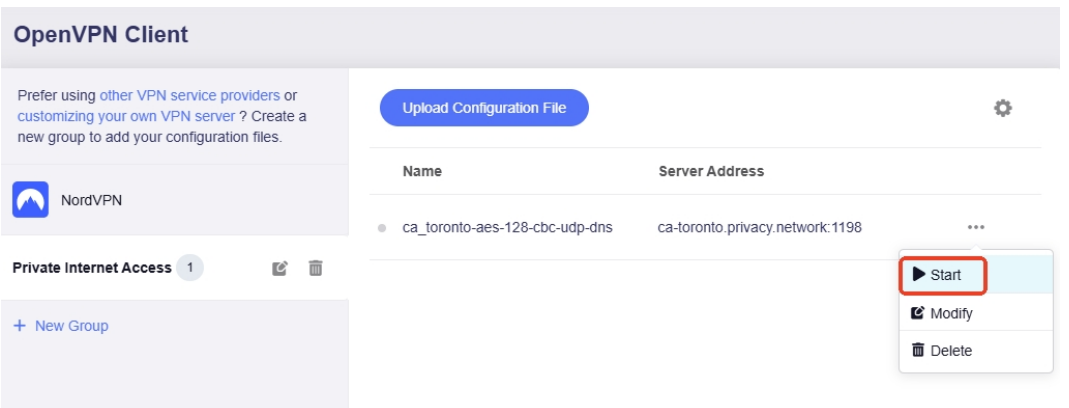
4. Cargue su archivo de configuración OpenVPN. Ingrese las credenciales si es necesario, luego haga clic en **Aplicar**.



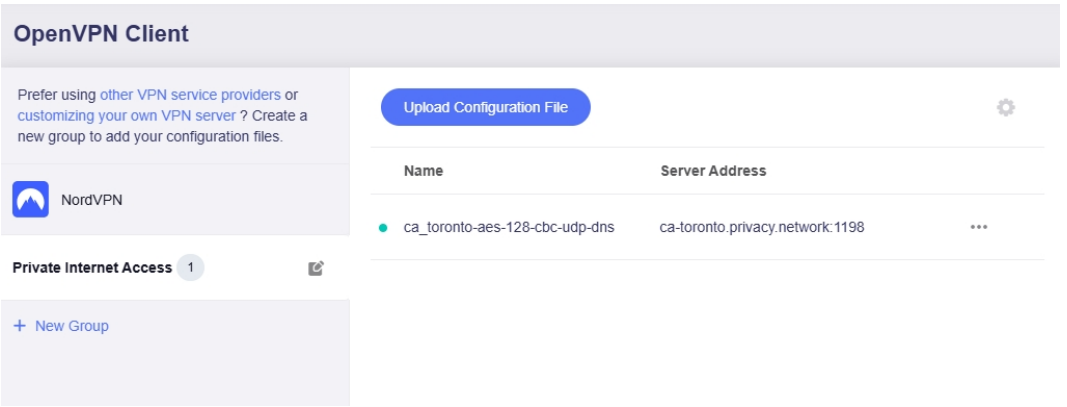
YVerá el archivo de configuración cargado.



5. Haga clic en el icono de tres puntos a la derecha para iniciar una conexión.



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



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

10.2 Configurar el cliente WireGuard

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

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

10.2.1 Preparación

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

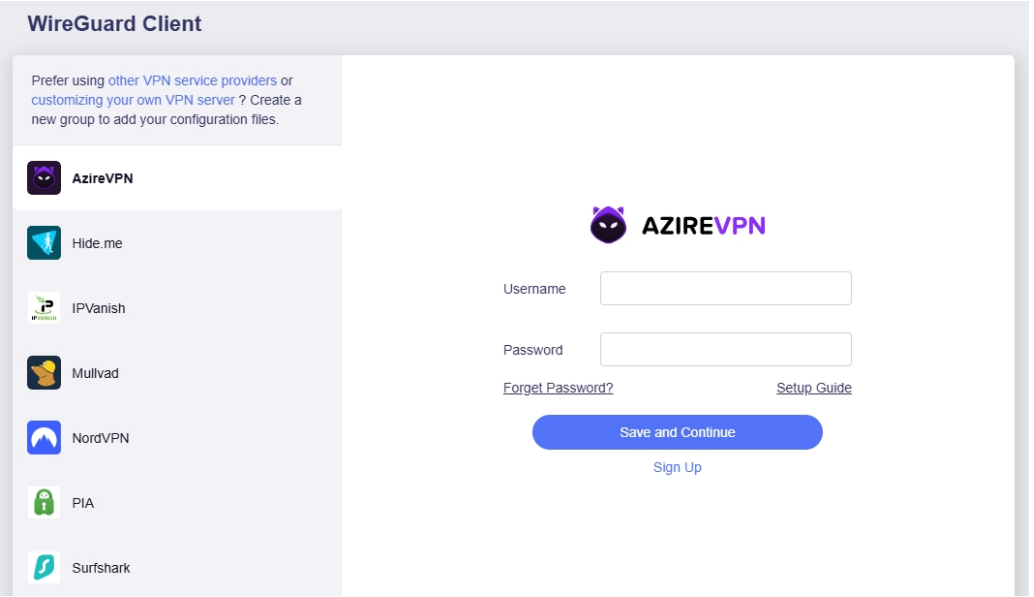
A continuación, sseleccione el proveedor de servicios WireGuard correspondiente a continuación para localizar rápidamente las instrucciones paso a paso.

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

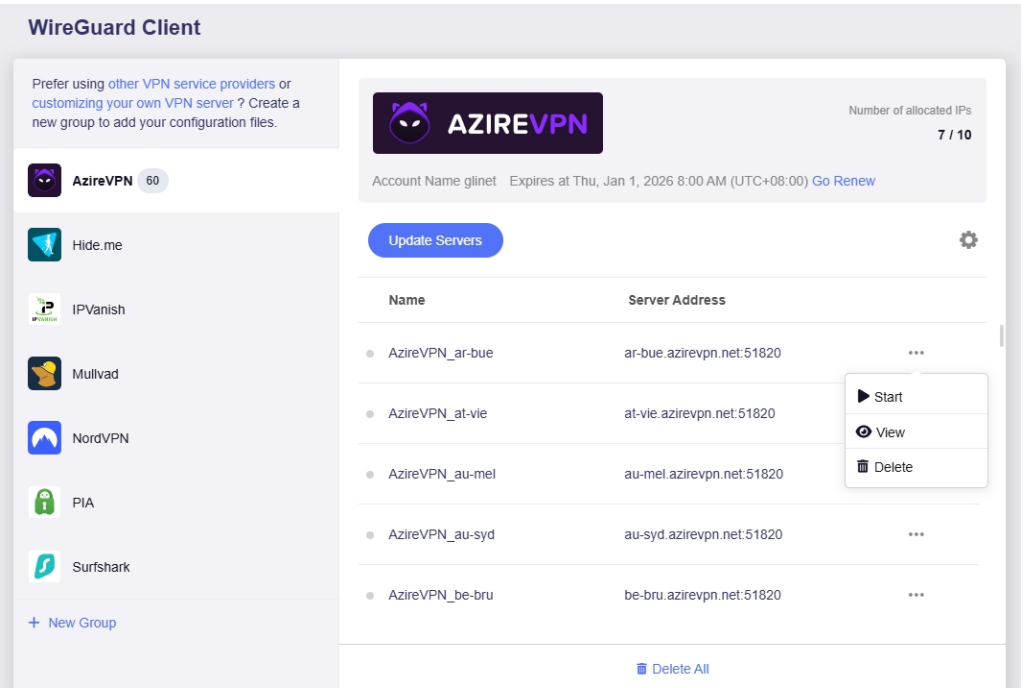
10.2.2 Configurar AzireVPN

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

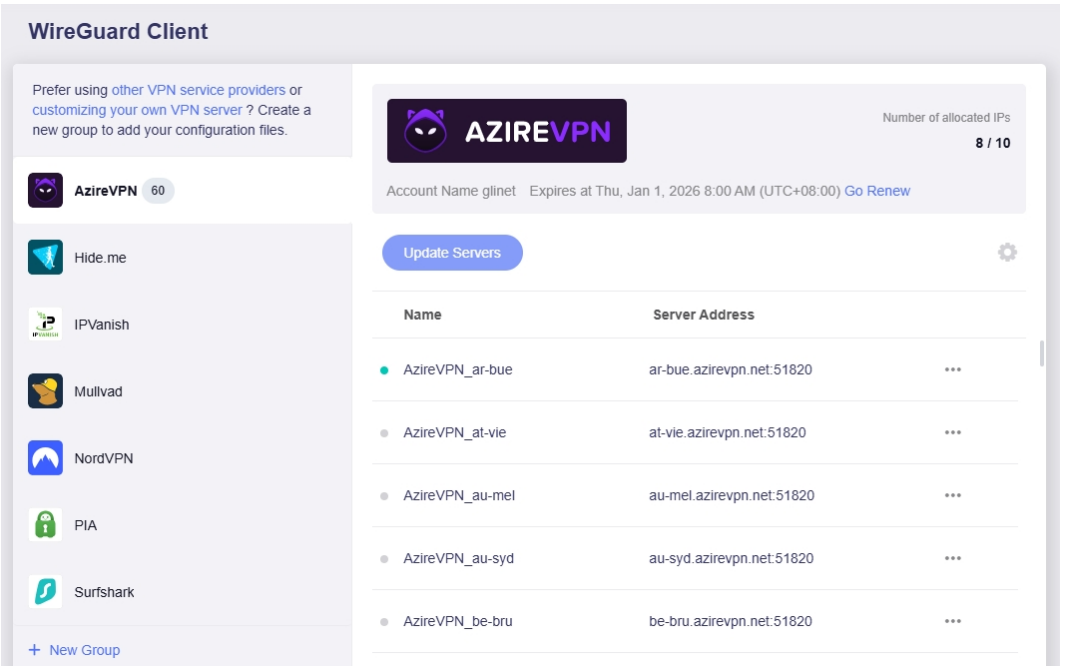
1. Inicie sesiónn en su enrutador’s web admin panel y vaya a **VPN** > **WireGuard Client** > **AzireVPN**.
2. Ingrese el nombre de usuario y la contraseña, luego haga clic en **Guardar y continuar**. Generará archivos de configuración para cada servidor.



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



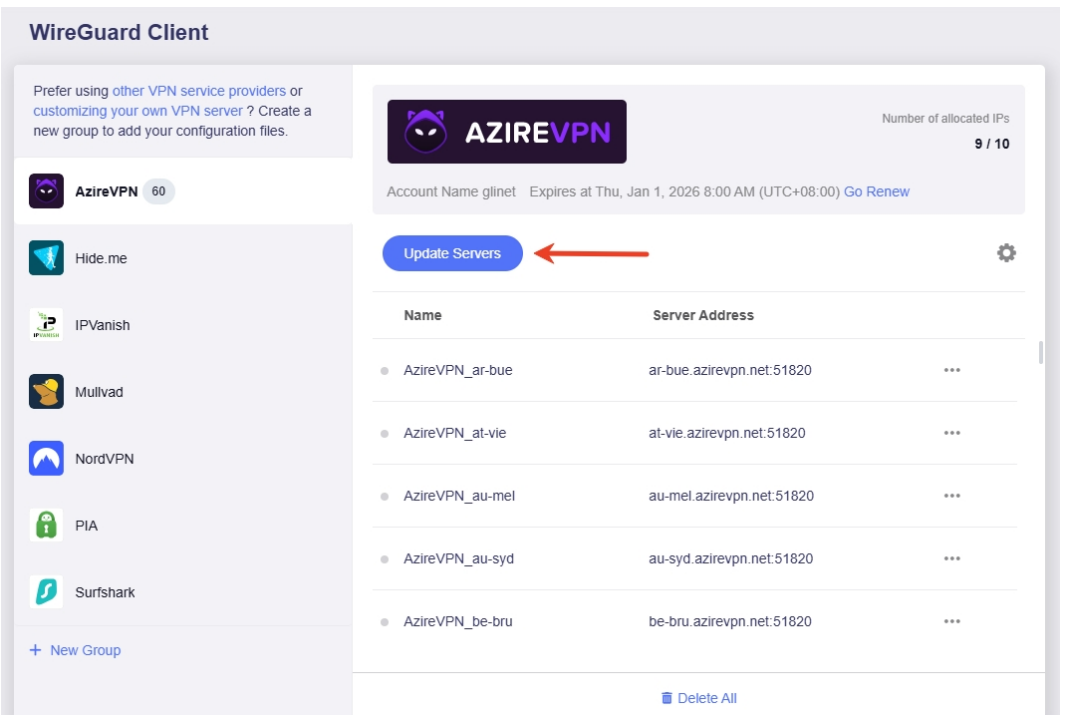
4. Una vez conectado, aparecerá un punto verde junto al archivo de configuración.



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

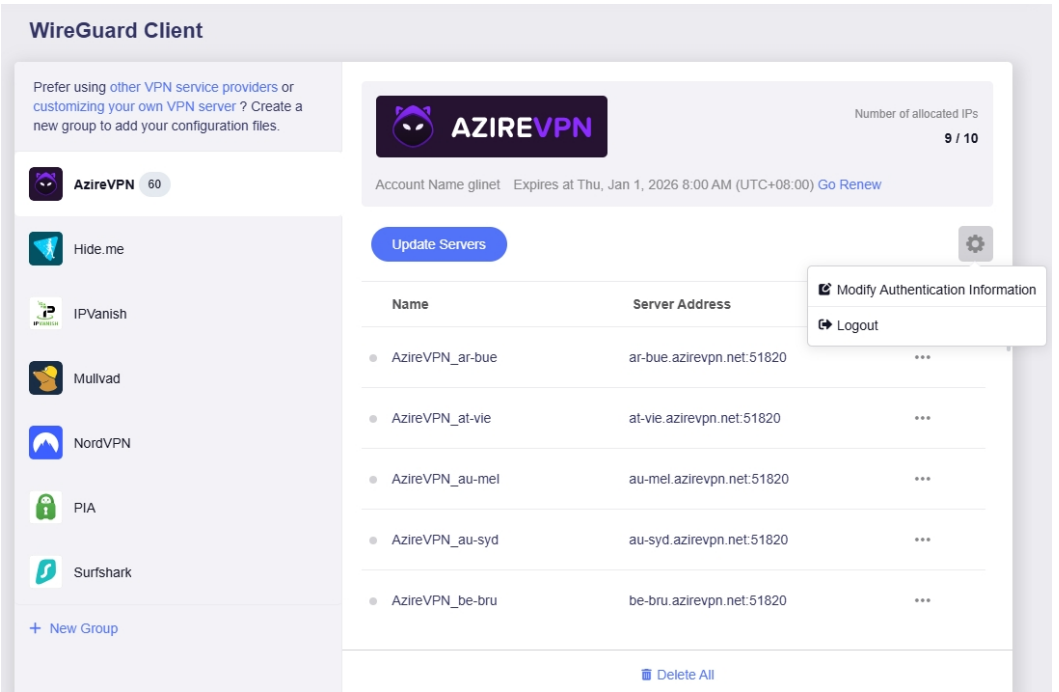
5. Actualizar servidores.

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



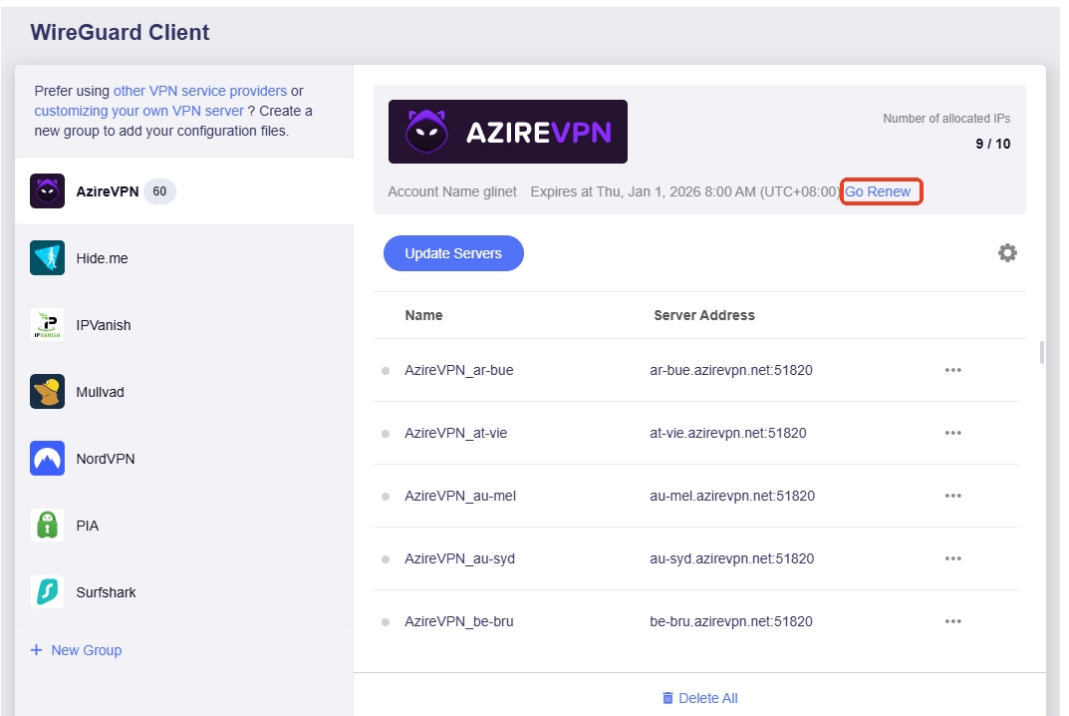
6. Editar credenciales o cerrar sesión.

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



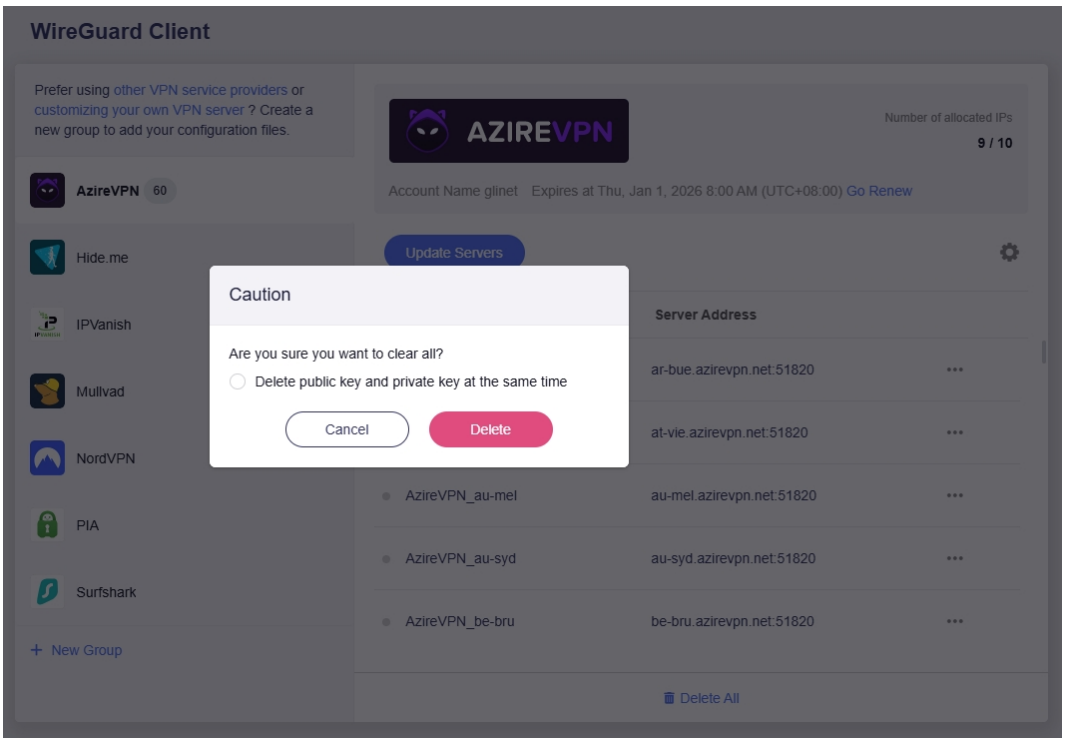
7. Ir a renovar.

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



8. Eliminar todos los archivos.

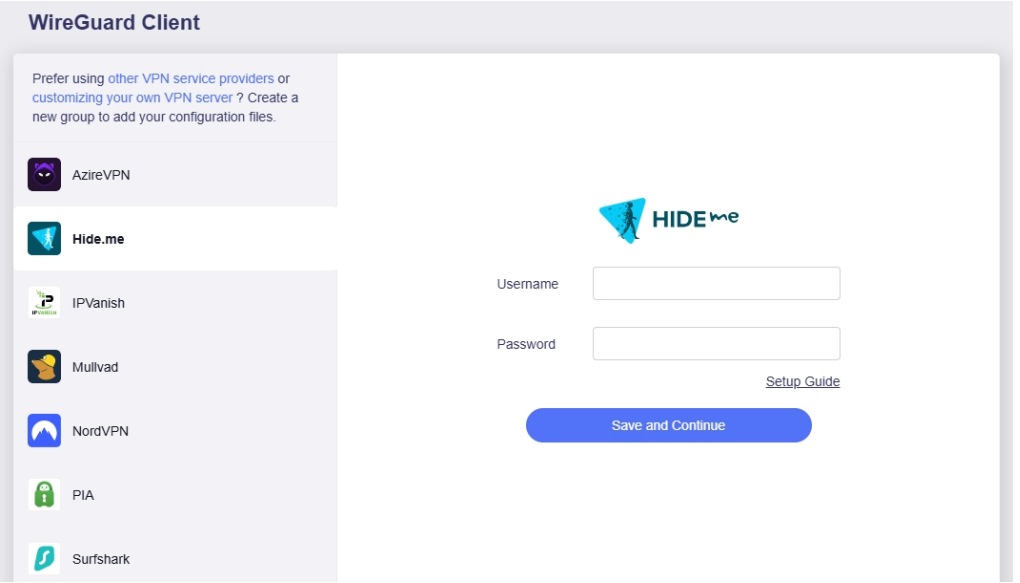
   Puedes hacer clic en **Eliminar todo** para eliminar todos los archivos de configuración con un solo clic y elegir si desea eliminar las claves públicas y privadas simultáneamente.



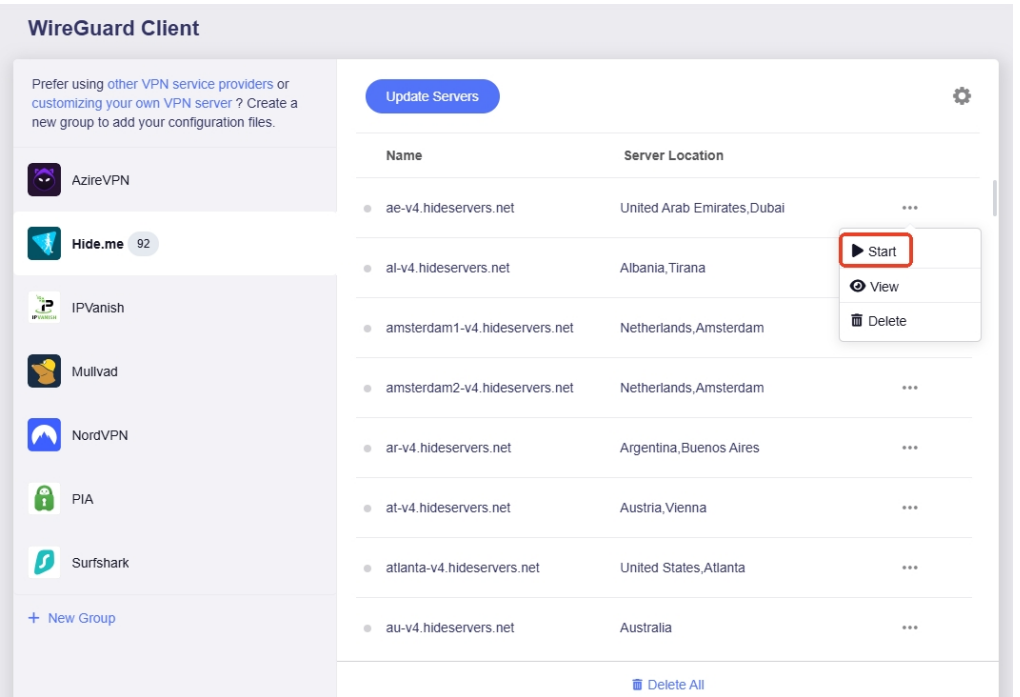
10.2.3 Configurar Hide.me

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

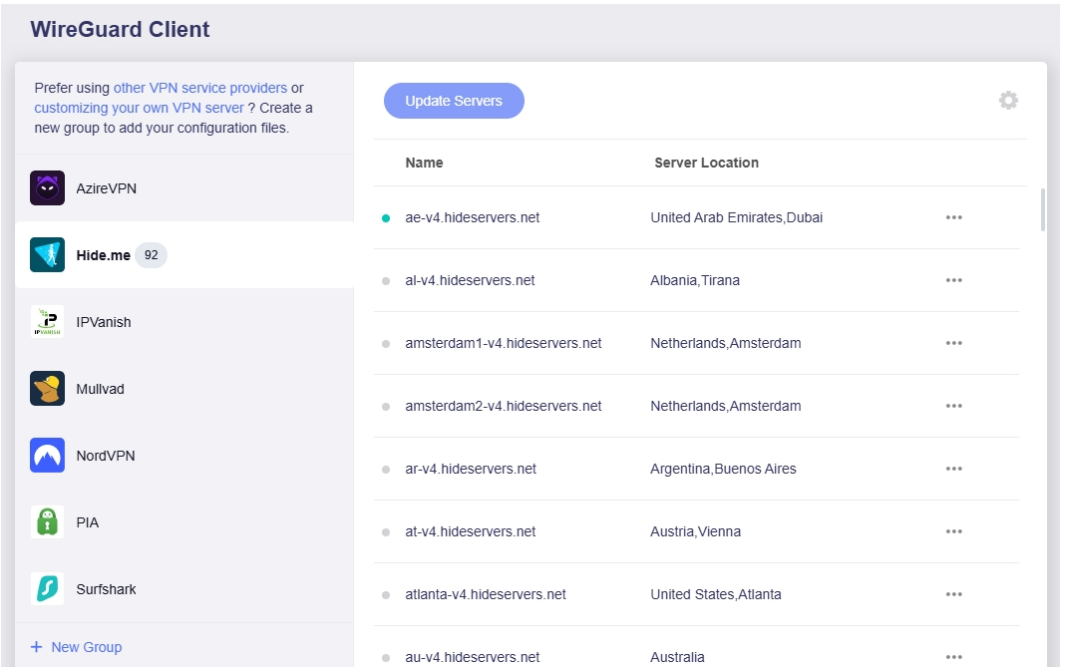
1. Inicie sesiónn en su enrutador’s web admin panel y vaya a **VPN** > **WireGuard Client** > **Hide.me**.
2. Ingrese nombre de usuario y contraseña, luego haga clic en **Guardar y continuar**. Generará archivos de configuración para cada servidor.



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



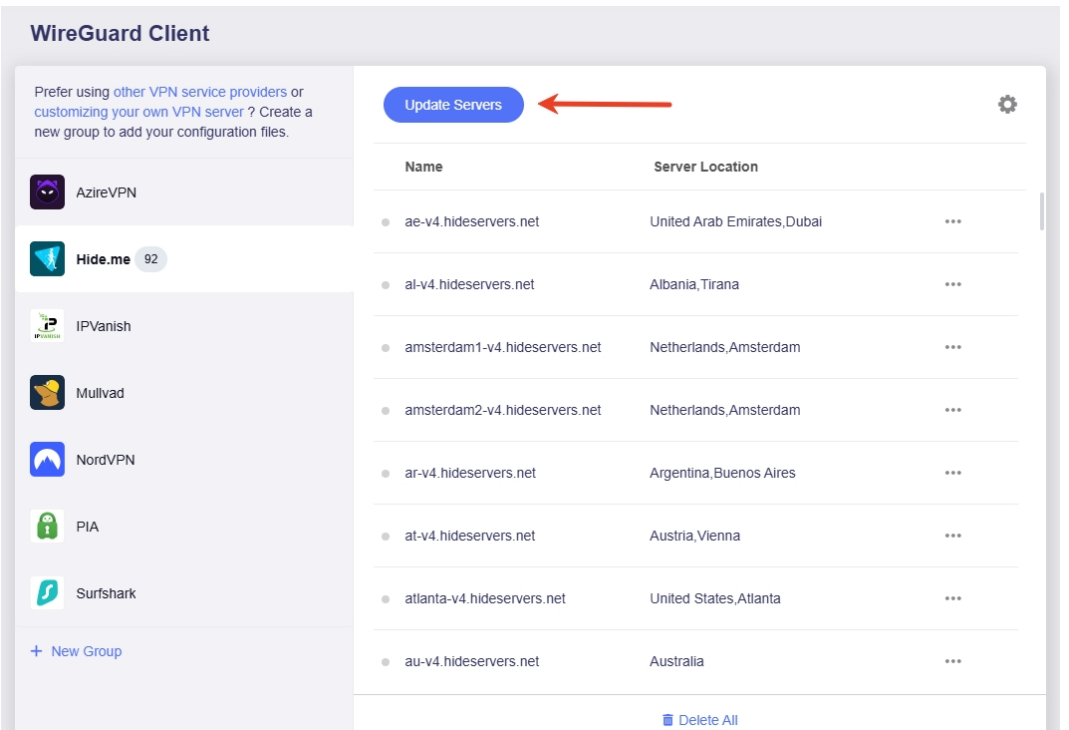
4. Una vez conectado, aparecerá un punto verde junto al archivo de configuración.



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

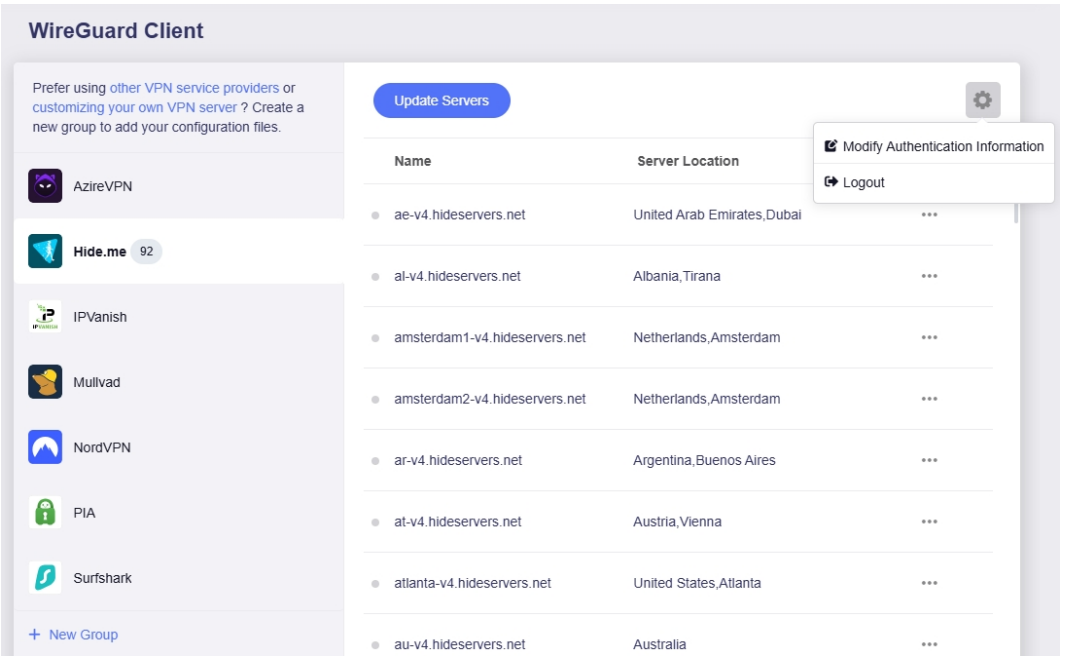
5. Actualizar servidores.

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



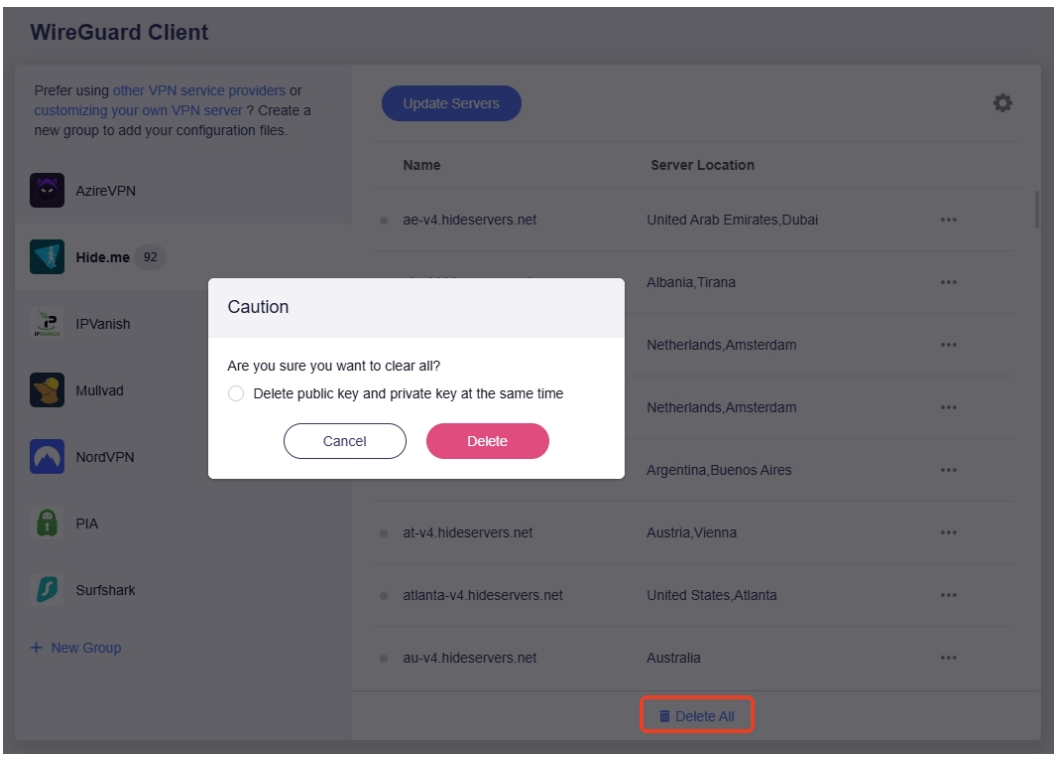
6. Edite las credenciales o cierre sesión.

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



7. Eliminar todos los archivos.

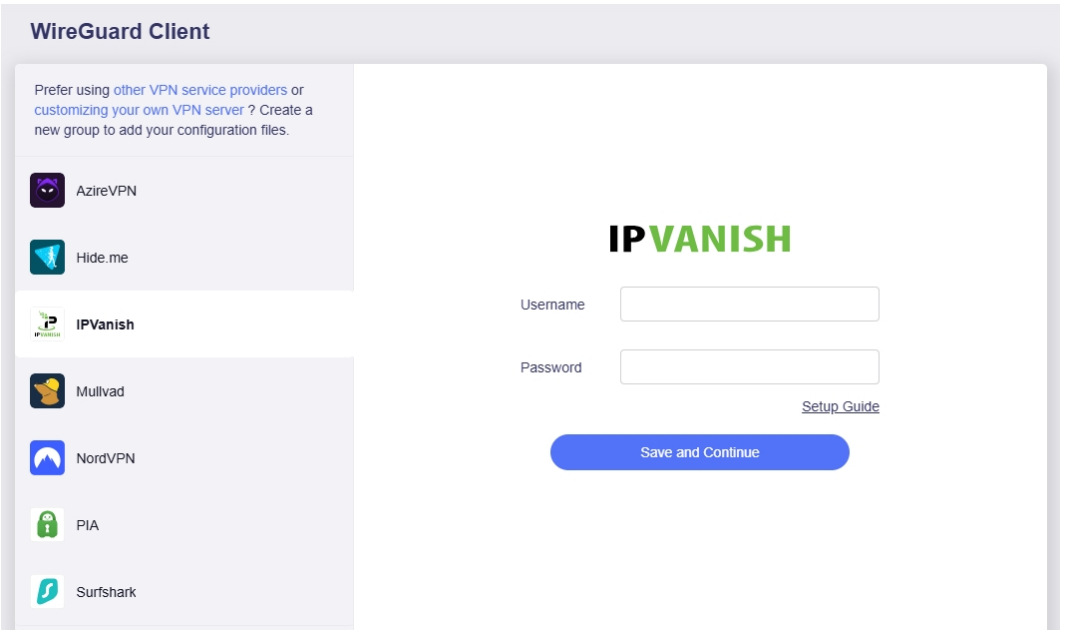
   Puede hacer clic en **Eliminar todo** para eliminar todos los archivos de configuración con un solo clic y elegir si desea eliminar las claves públicas y privadas simultáneamente.



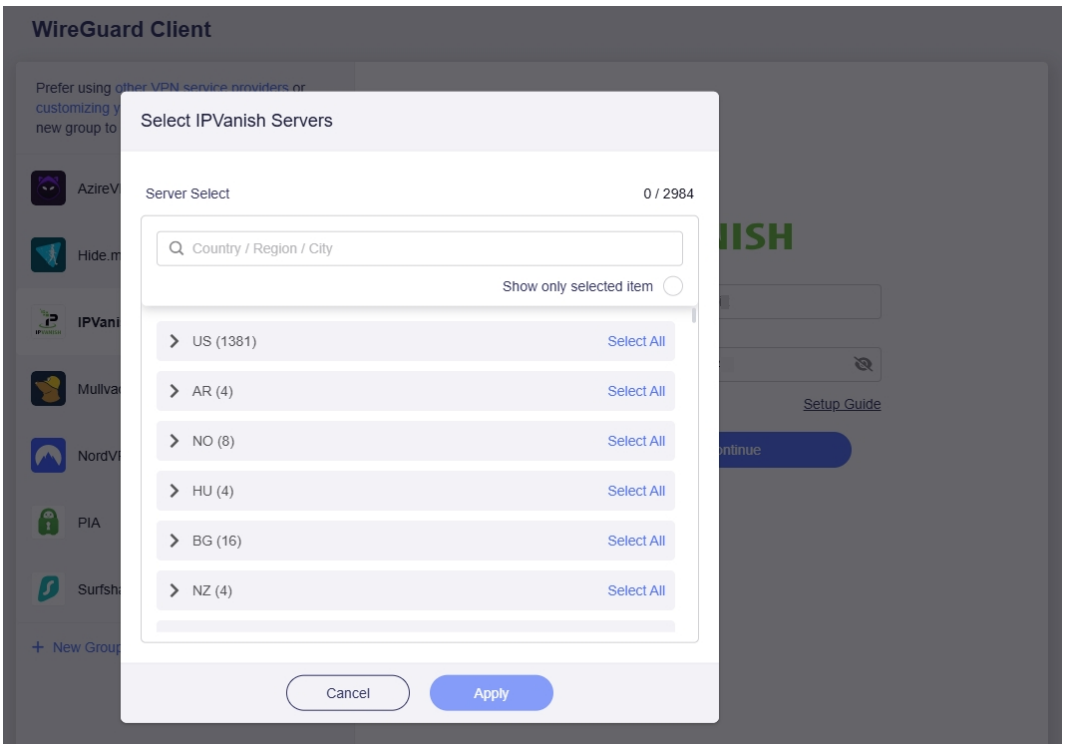
10.2.4 Configurar IPVanish

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

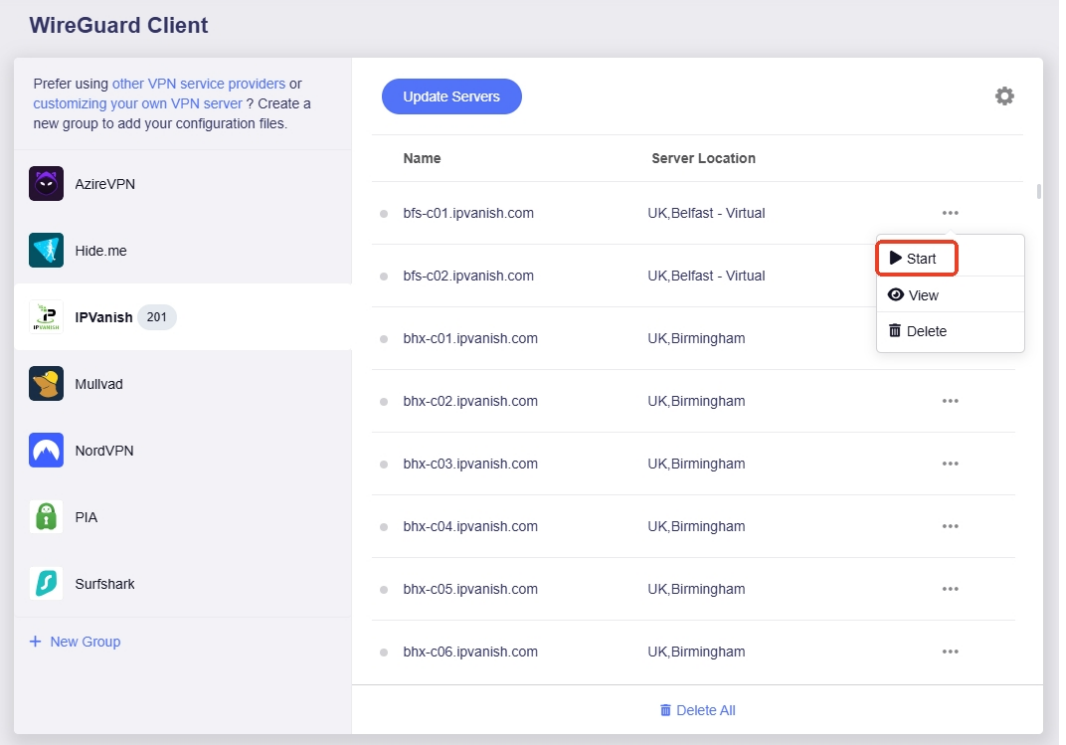
1. Iniciar sesiónn a su enrutador’s web admin panel y vaya a **VPN** > **WireGuard Client** > **IPVanish**.
2. Ingrese el nombre de usuario y la contraseña, luego haga clic en **Guardar y continuar**.



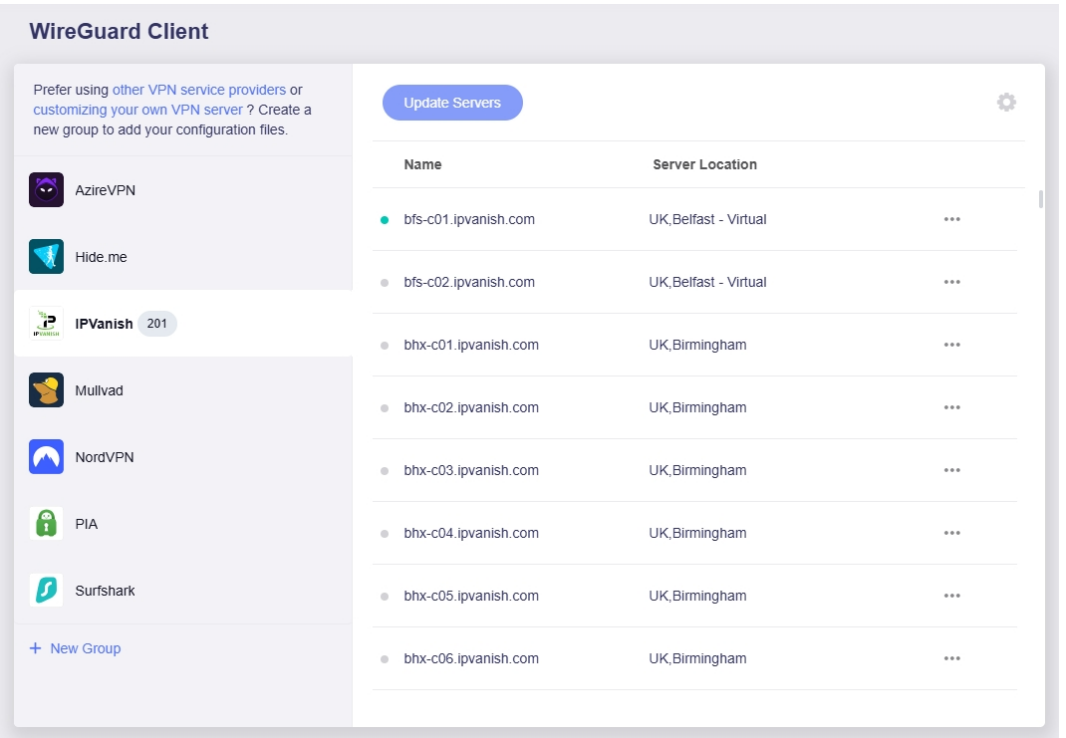
3. Seleccione los servidores a los que desea conectarse y haga clic en **Aplicar**.



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



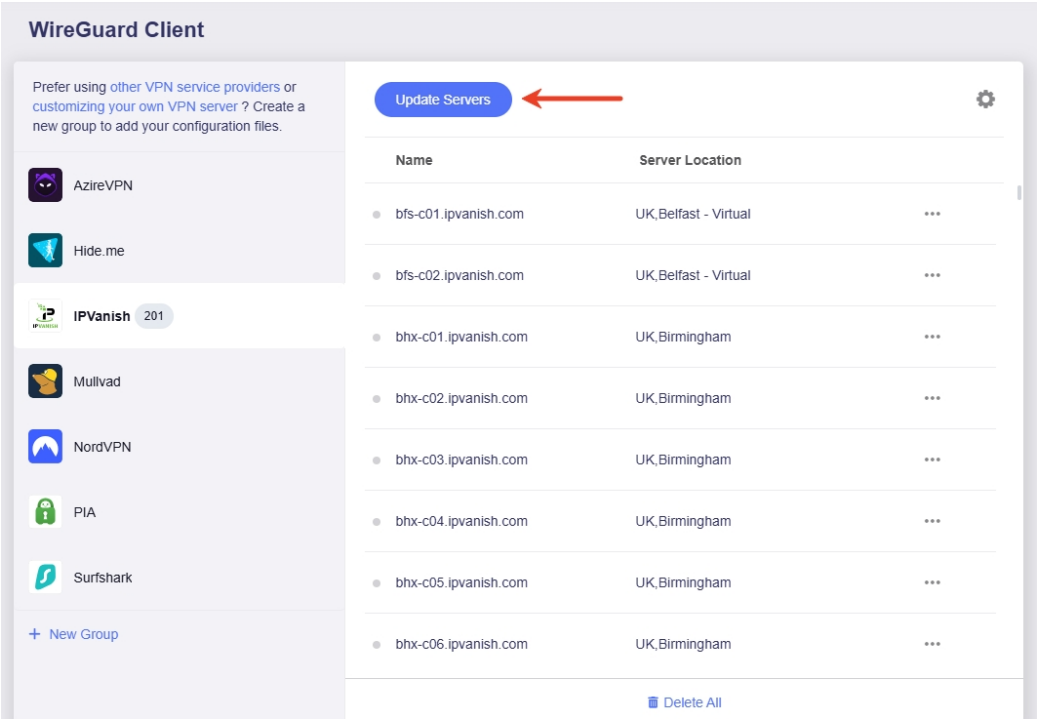
5. Una vez conectado, aparecerá un punto verde junto al archivo de configuración.



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

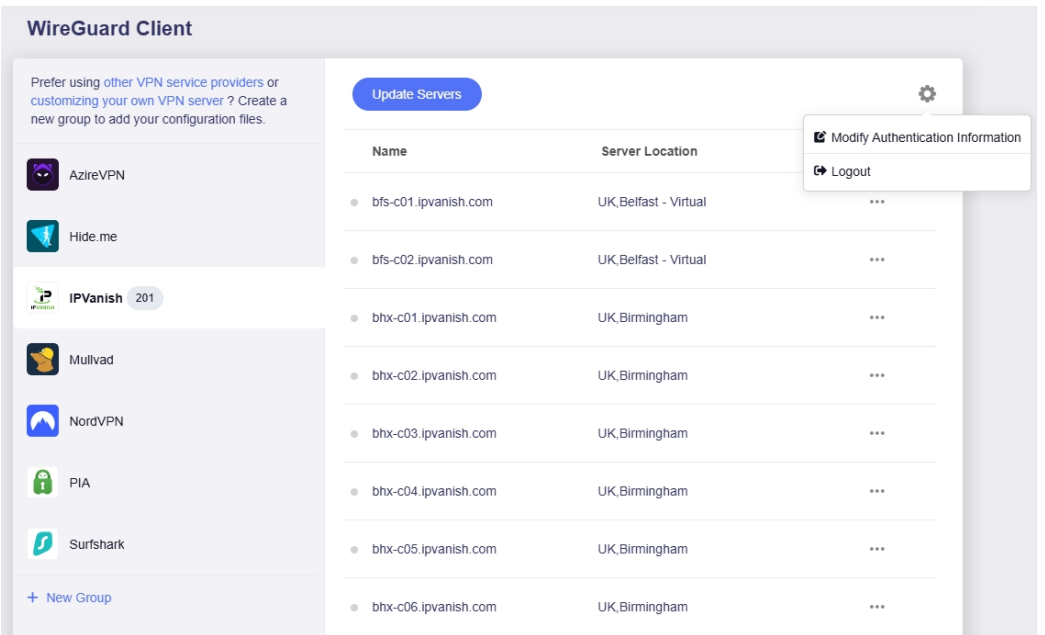
6. Actualizar servidores.

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



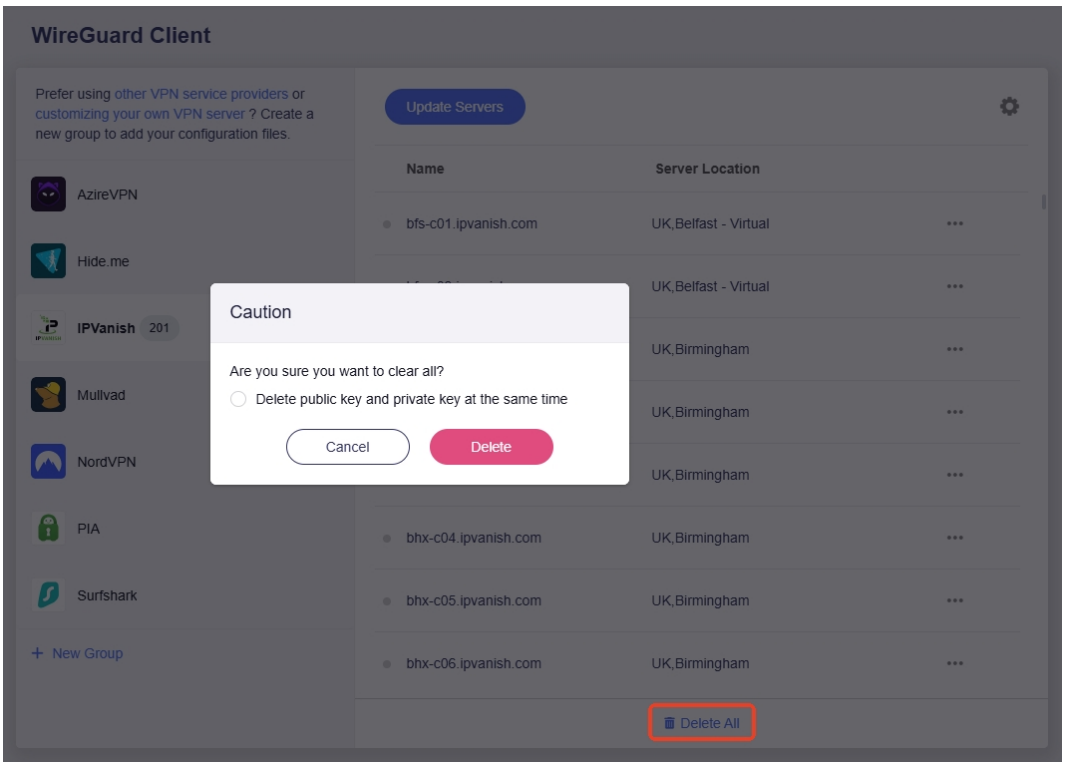
7. Edite las credenciales o cierre sesión.

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



8. Eliminar todos los archivos.

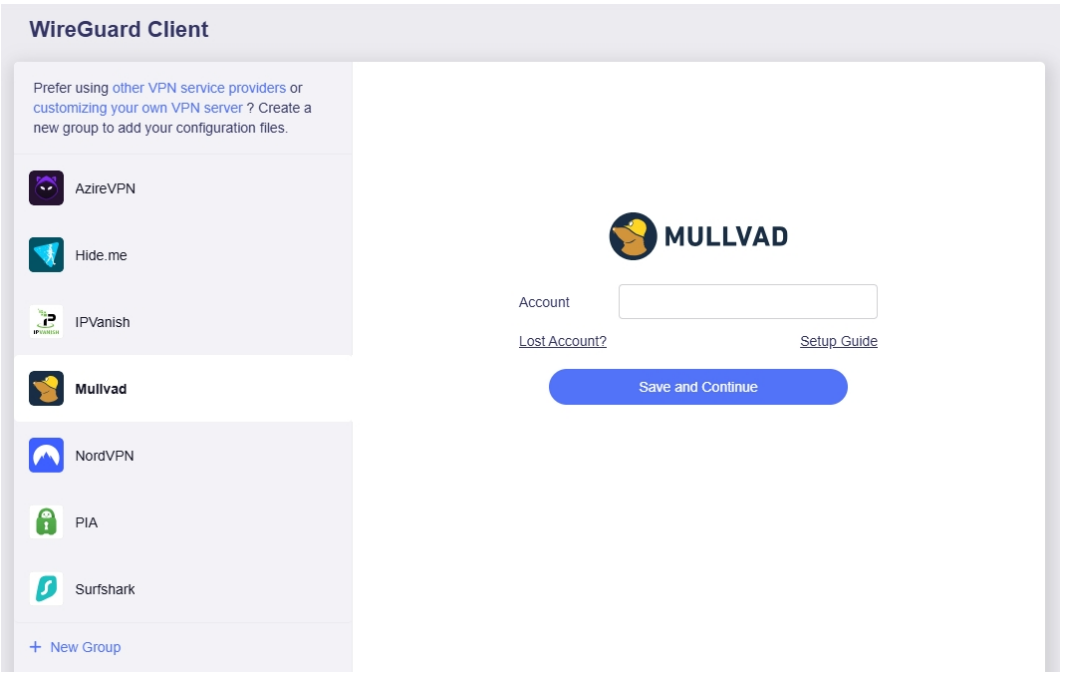
   Puede hacer clic en **Eliminar todo** para eliminar todos los archivos de configuración con un solo clic y elija si desea eliminar las claves pública y privada simultáneamente.



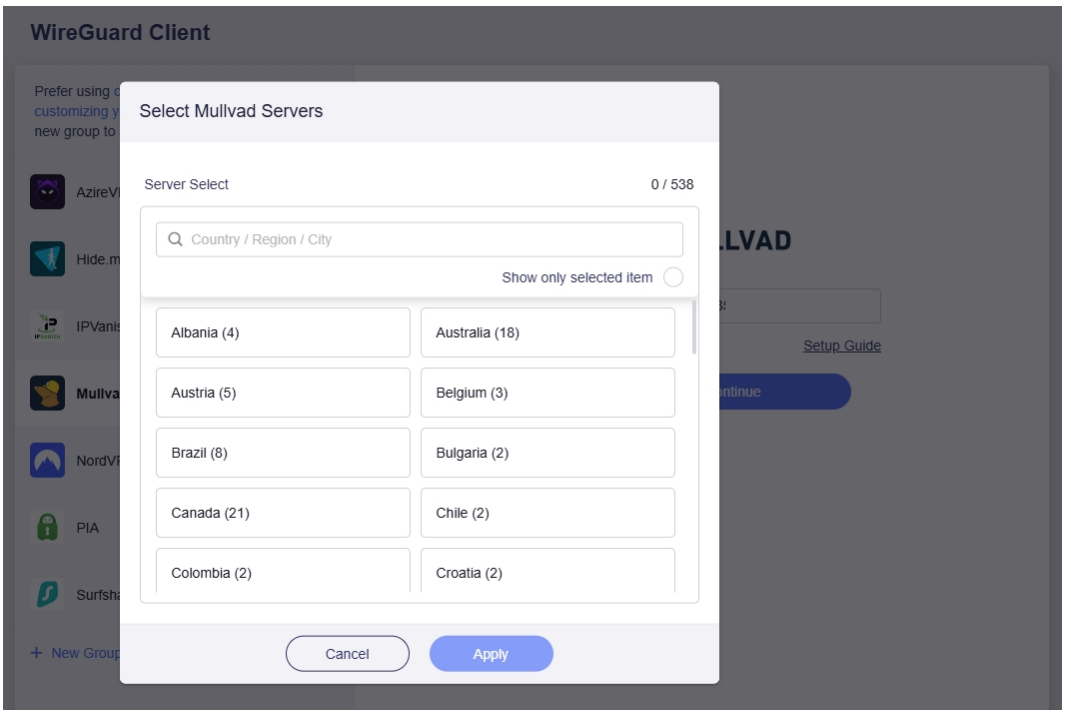
10.2.5 Configurar Mullvad

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

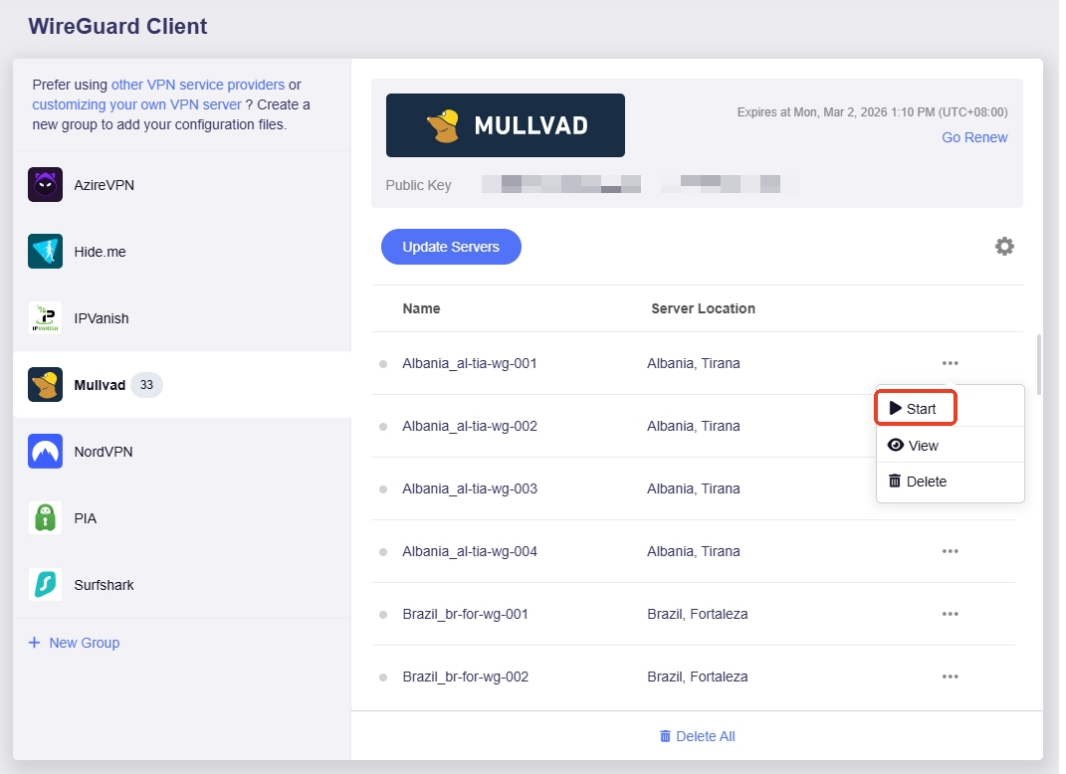
1. Inicie sesiónn en su enrutador’s web admin panel y vaya a **VPN** > **Cliente WireGuard** > **Mullvad**.
2. Ingrese nombre de usuario y contraseña, luego haga clic en **Guardar y continuar**.



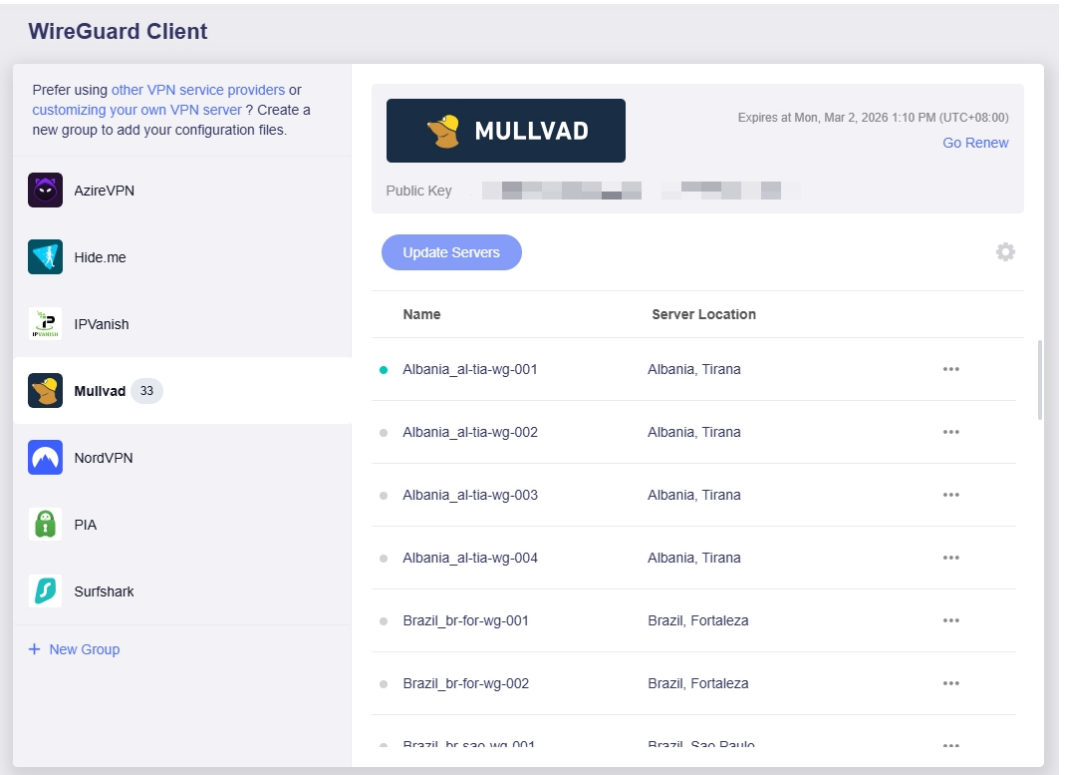
3. Seleccione los servidores a los que desea conectarse y haga clic en **Aplicar**.



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



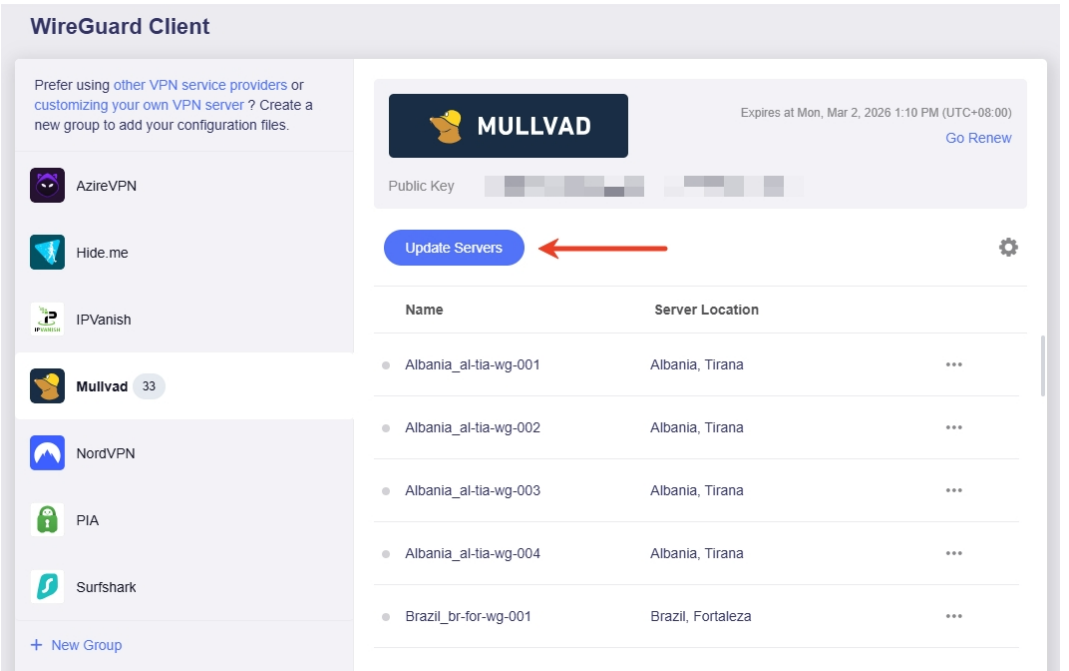
5. Una vez conectado, aparecerá un punto verde junto a la configuración archivo.



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

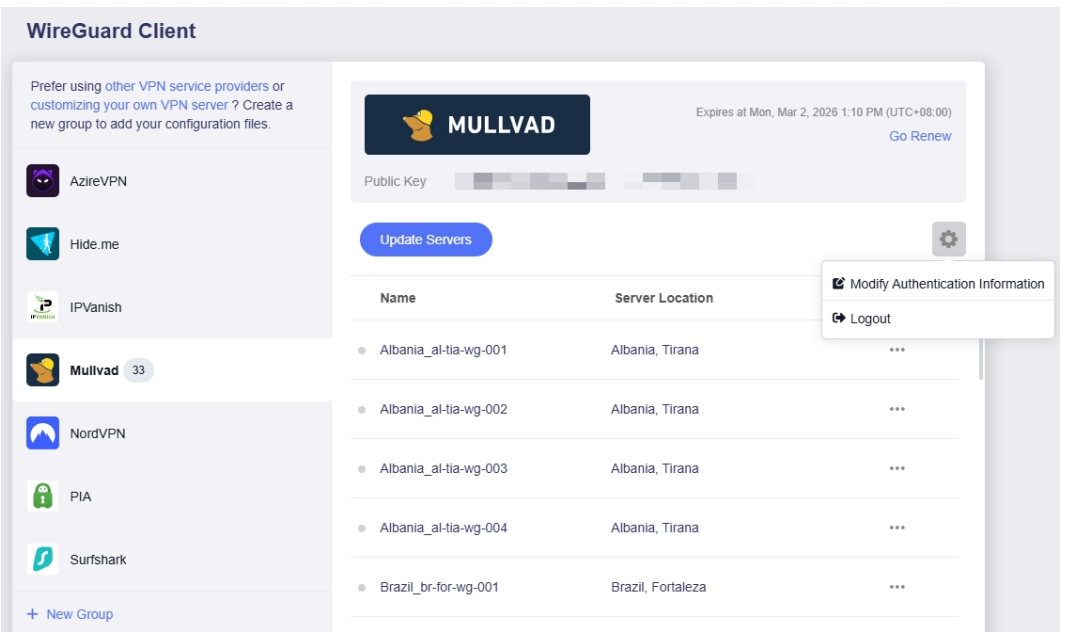
6. Actualizar servidores.

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



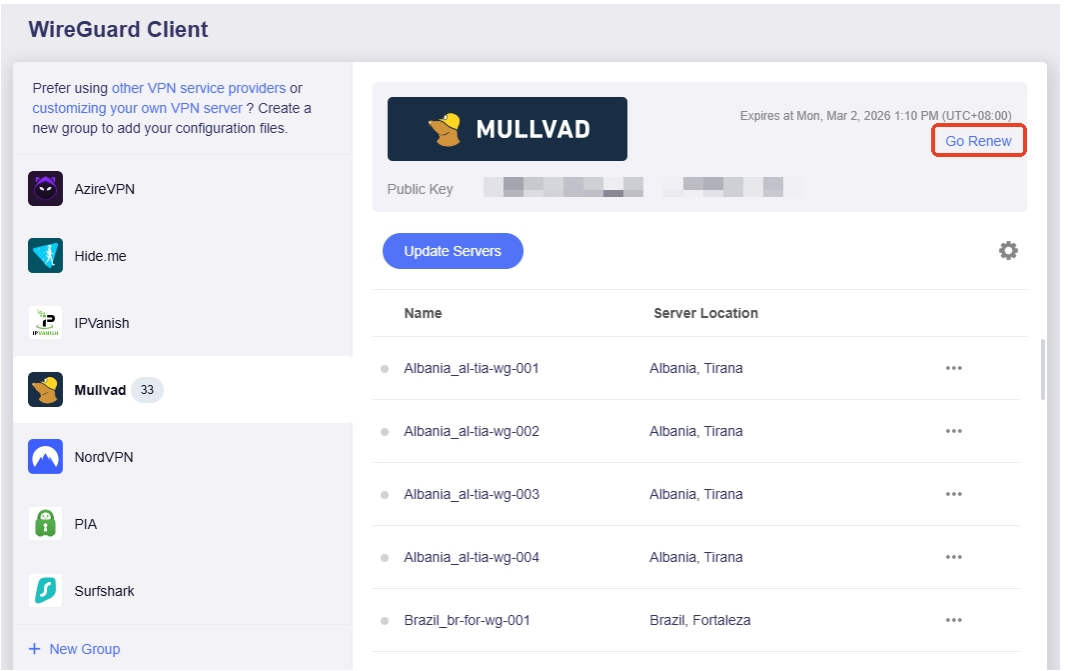
7. Edite las credenciales o cierre la sesión.

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



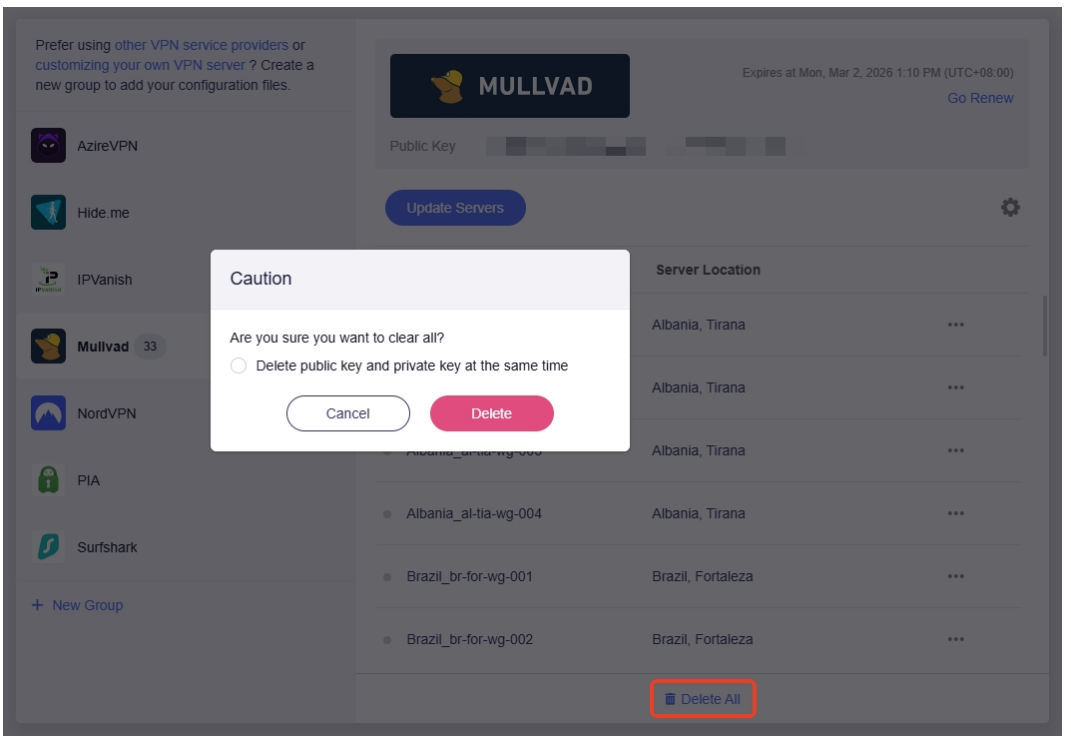
8. Vaya a renovar.

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



9. Eliminar todos los archivos.

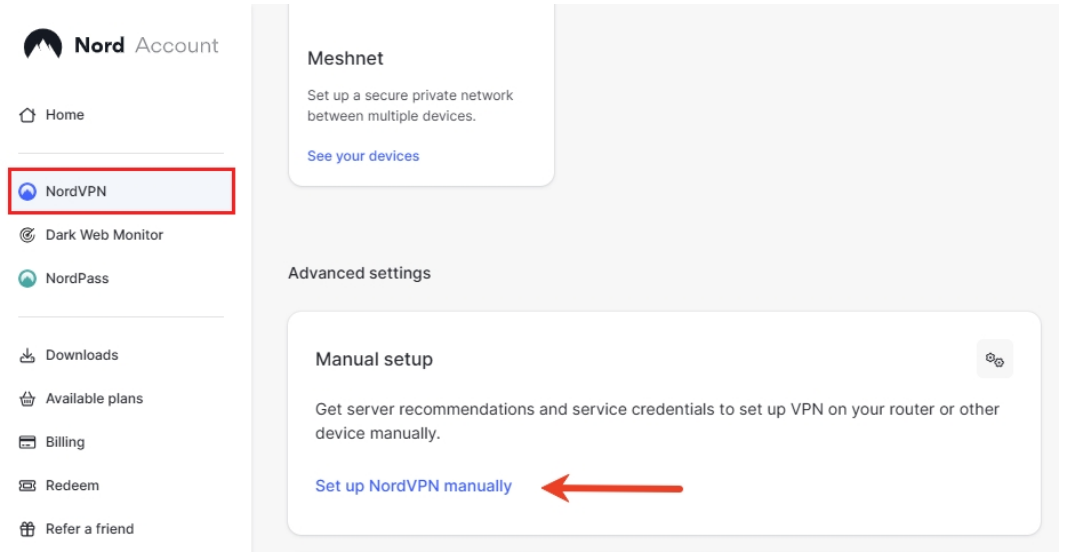
   Puede hacer clic en **Eliminar todo** para eliminar todos los archivos de configuración con un solo clic y elegir si desea eliminar las claves públicas y privadas simultáneamente.



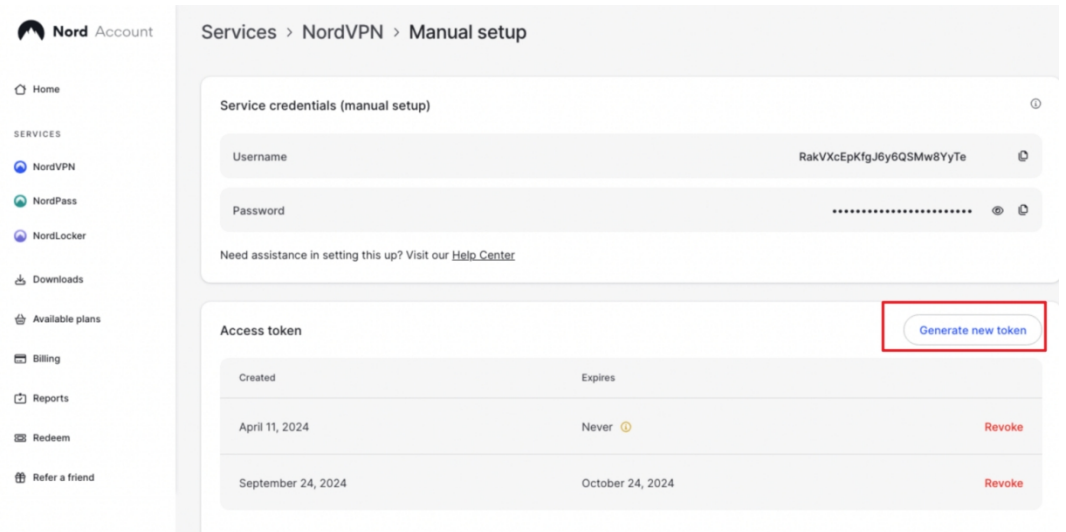
10.2.6 Configurar NordVPN

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

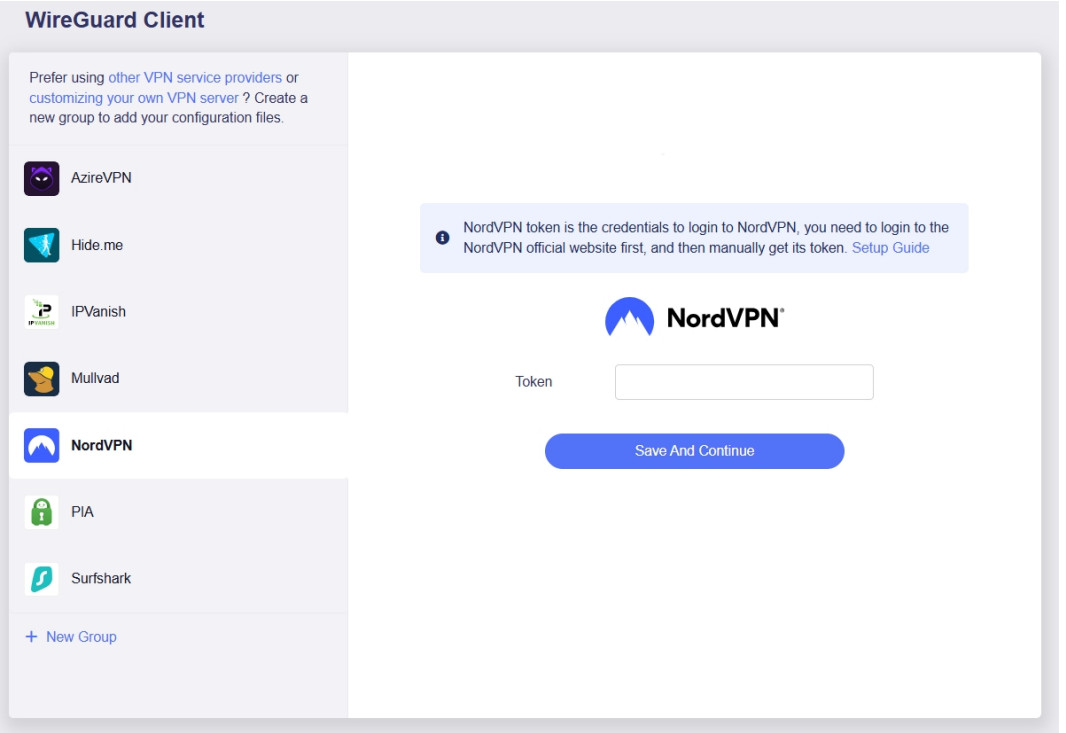
1. Inicie sesión en su cuenta web NordVPN aquí.
2. Oen el Nord Dashboard, haga clic en **NordVPN**, luego haga clic en **Configurar NordVPN manualmente**.



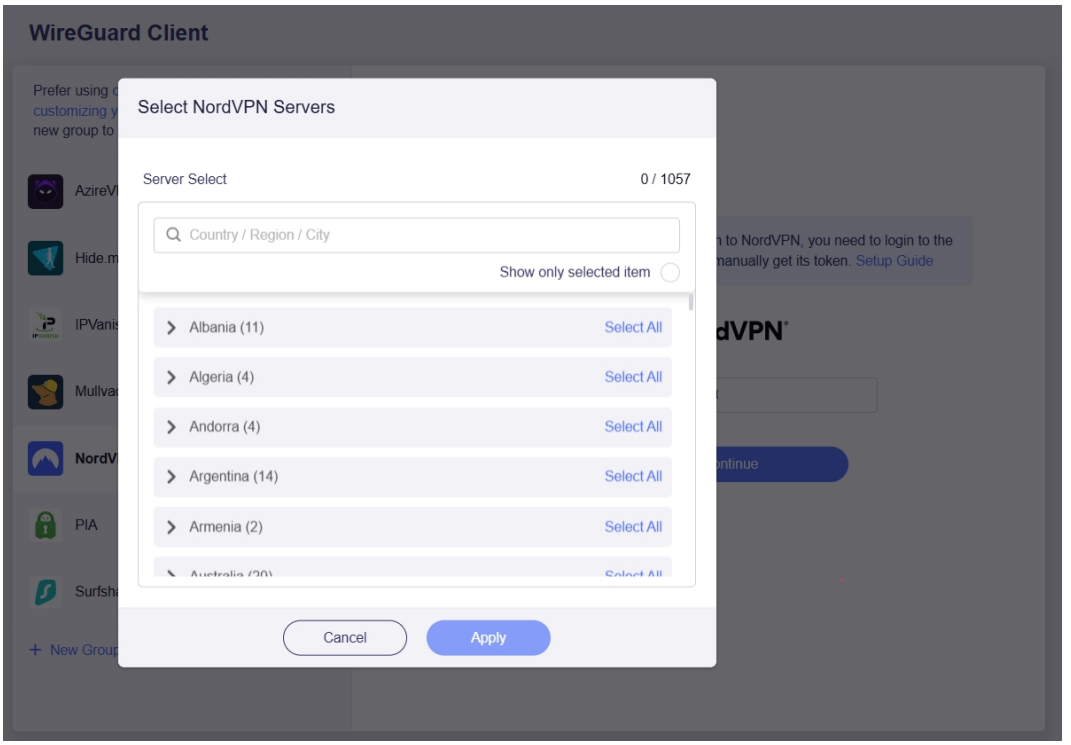
Encontrará el **Token de acceso**. Crear un token de acceso y ccopia para uso posterior.



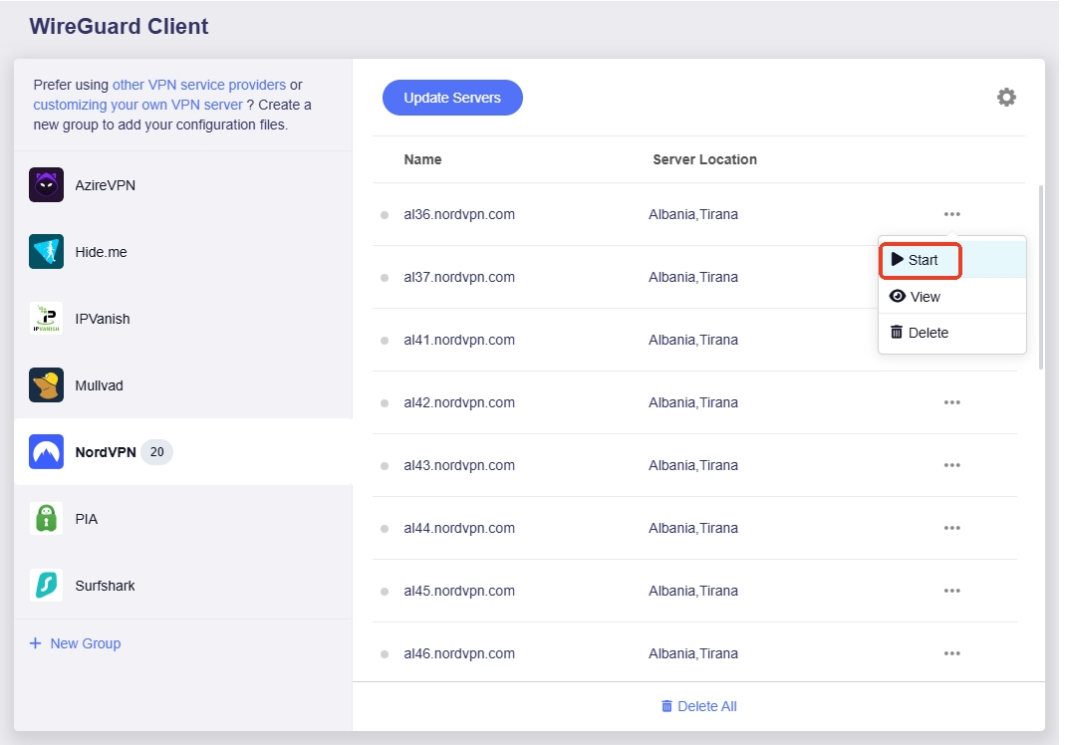
3. Inicie sesiónn en su enrutador's web admin panel y vaya a **VPN** > **Cliente WireGuard** > **NordVPN**.
4. Ingrese token, y haga clic en **Guardar y continuar**.



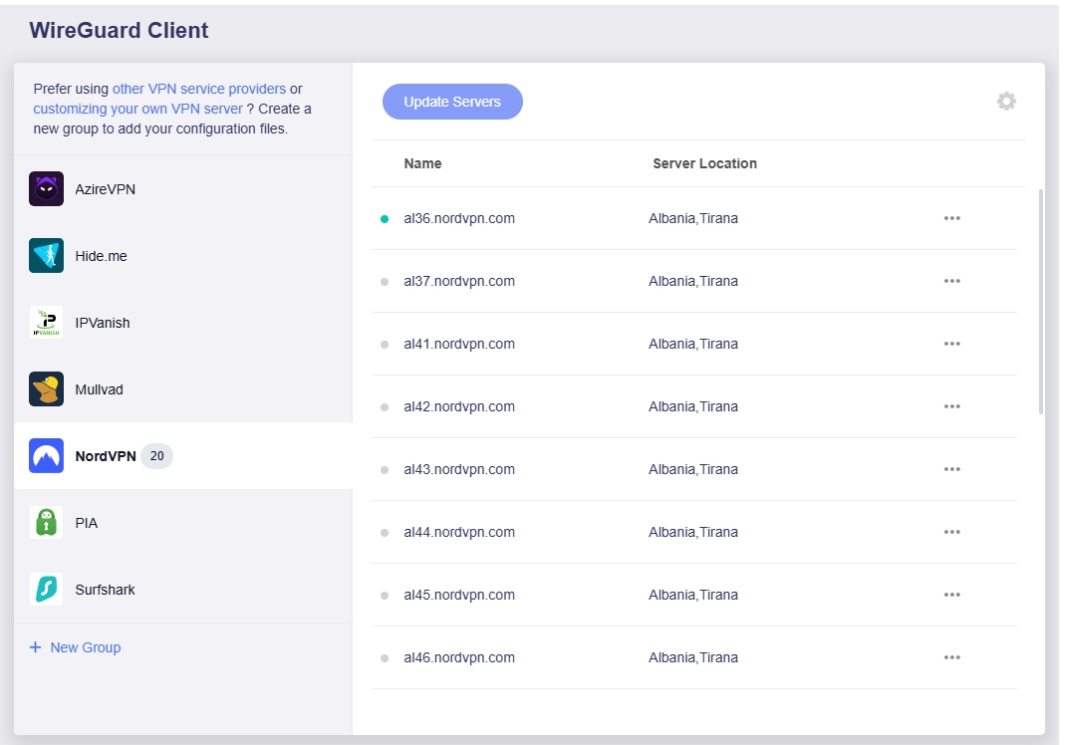
5. Seleccione los servidores a los que desea conectarse y haga clic en **Aplicar**.



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



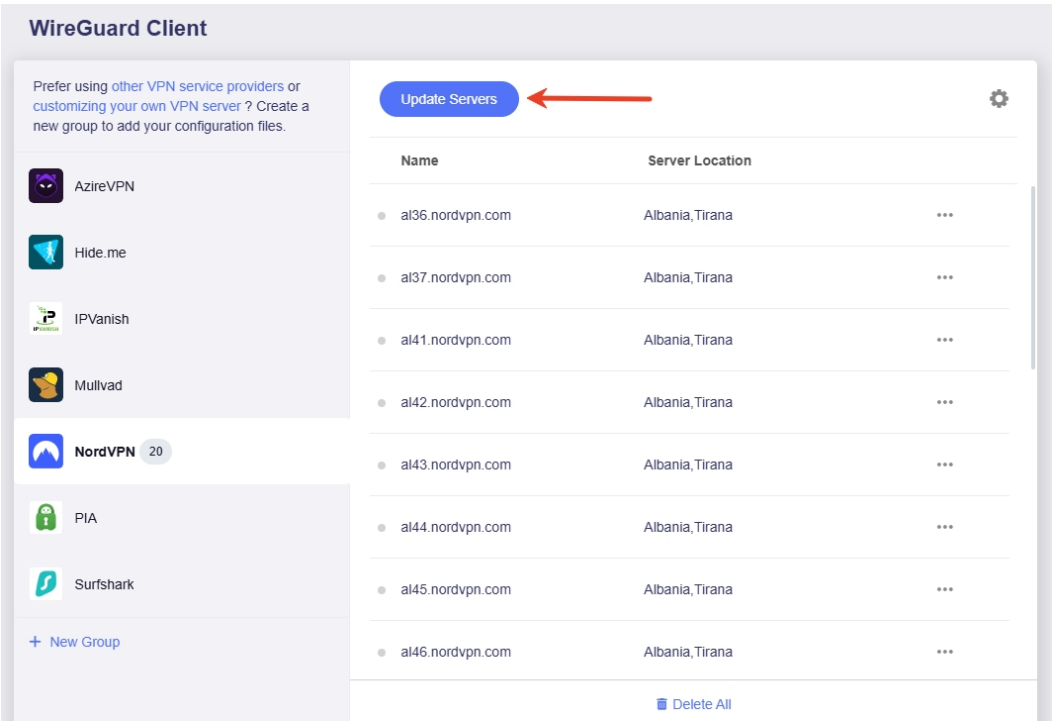
7. Una vez conectado, aparecerá un punto verde junto al archivo de configuración.



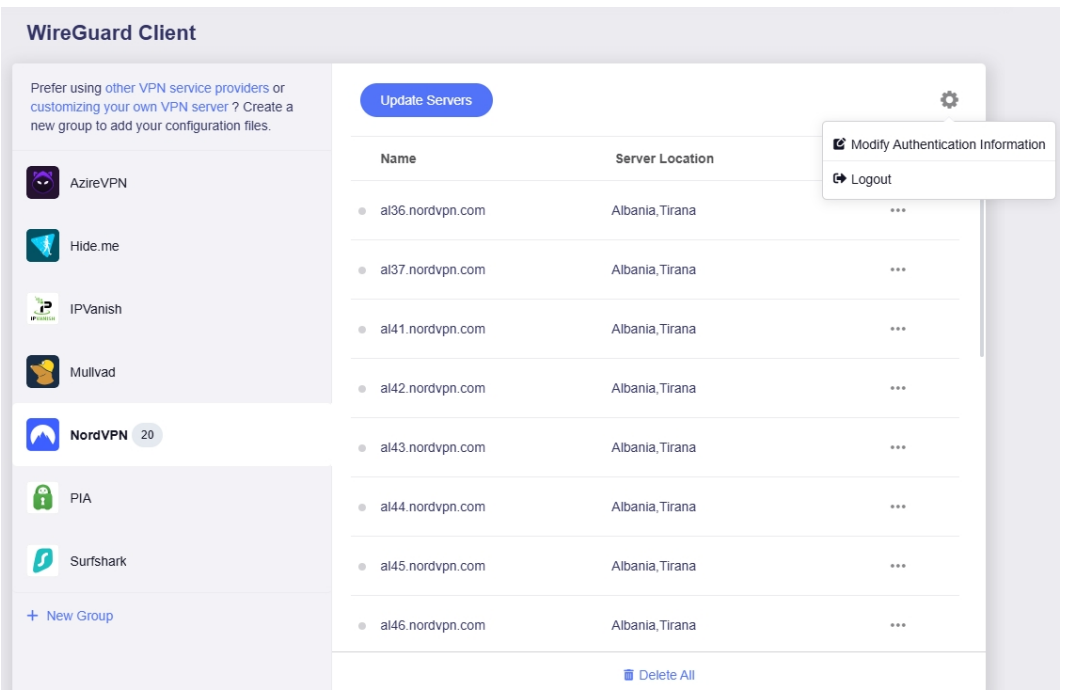
Usted puede también comprobar la conexión VPN detalles en **Panel de VPN**.

8. Actualizar servidores.

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

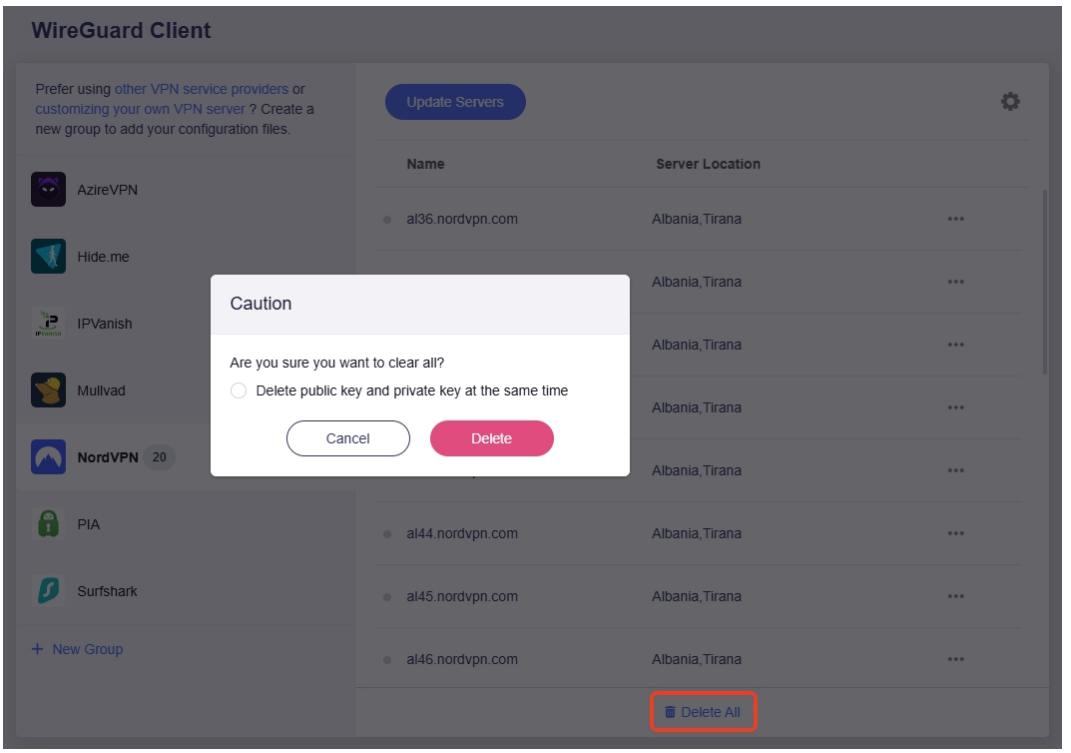


9. Edite las credenciales o cierre sesión.
   Haga clic en el ícono de ajustes para editar sus credenciales de inicio de sesión o cerrar sesión.



10. Eliminar todos los archivos.

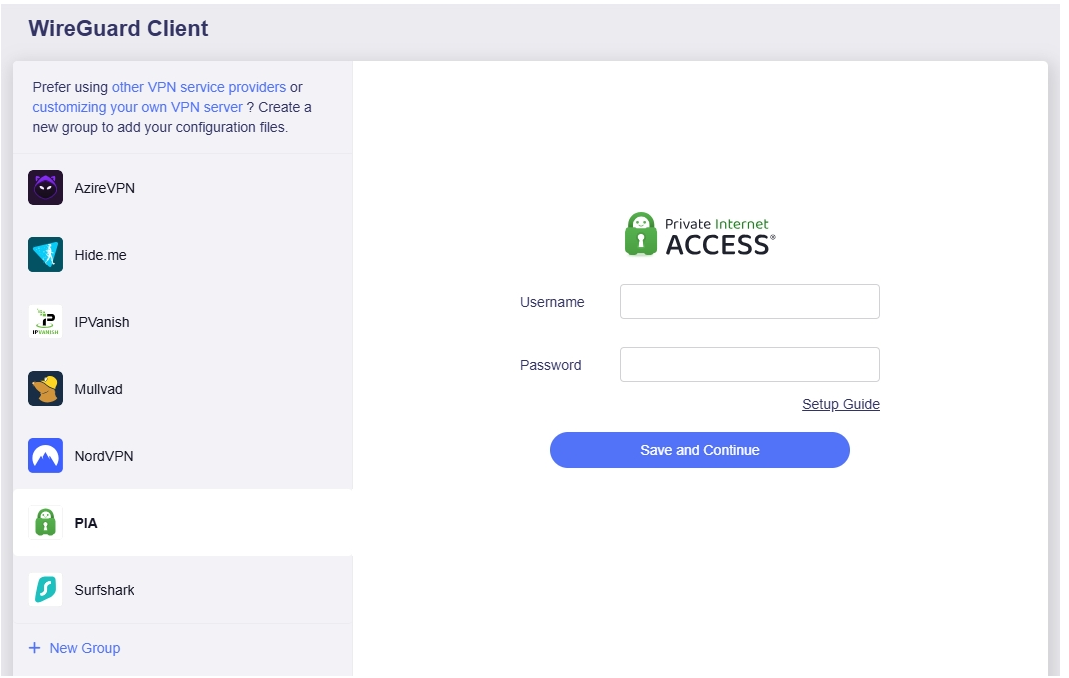
    Puedes hacer clic en **Eliminar todo** para eliminar todos los archivos de configuración con un solo clic y elija si desea eliminar las claves pública y privada simultáneamente.



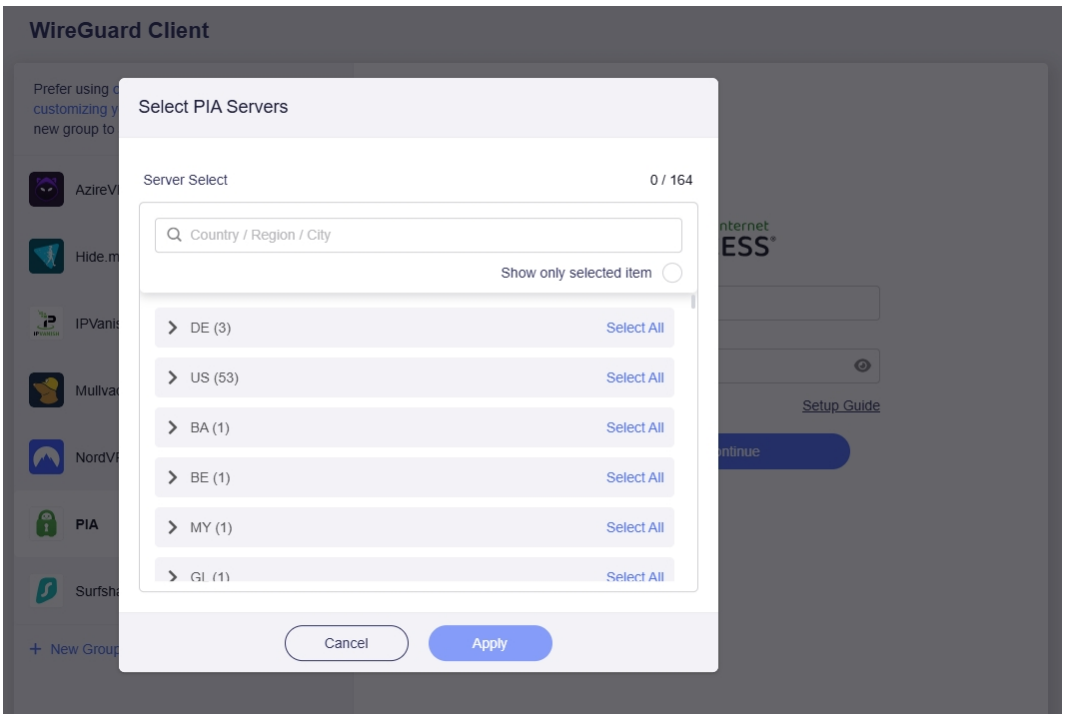
10.2.7 Configurar PIA (Private Internet Access)

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

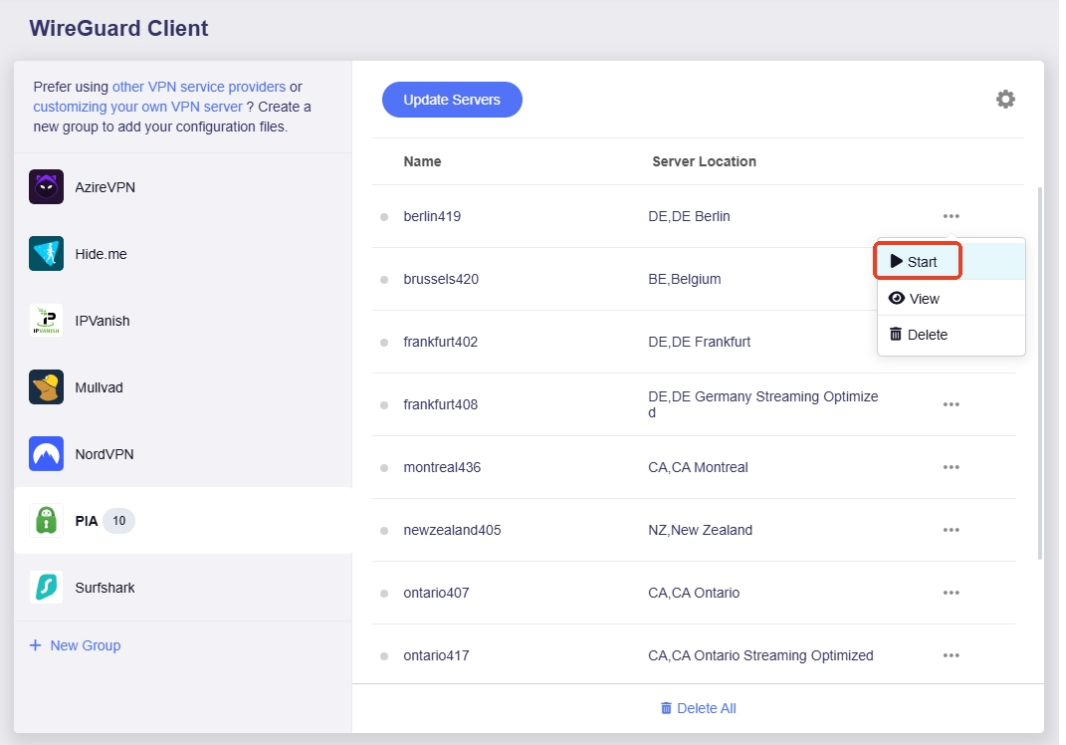
1. Iniciar sesión in a su enrutador’s web admin panel y vaya a **VPN** > **WireGuard Client** > **PIA**.
2. Ingrese el nombre de usuario y la contraseña, luego haga clic en **Guardar y continuar**.



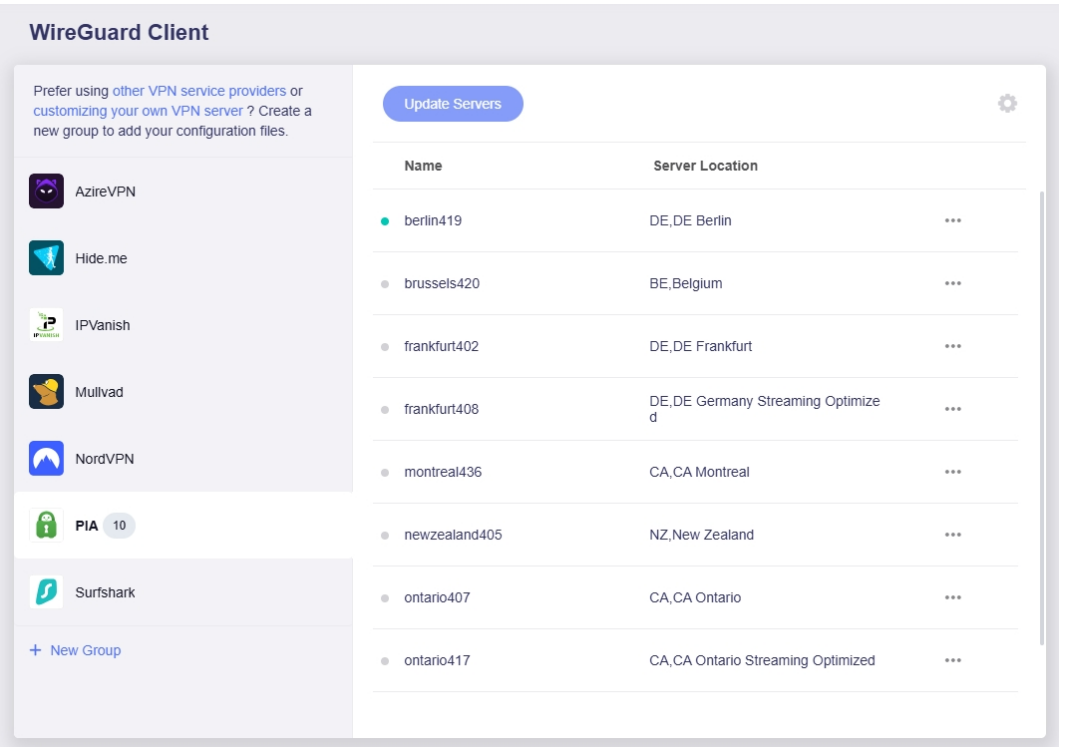
3. Seleccione los servidores a los que desea conectarse y haga clic en **Aplicar**.



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



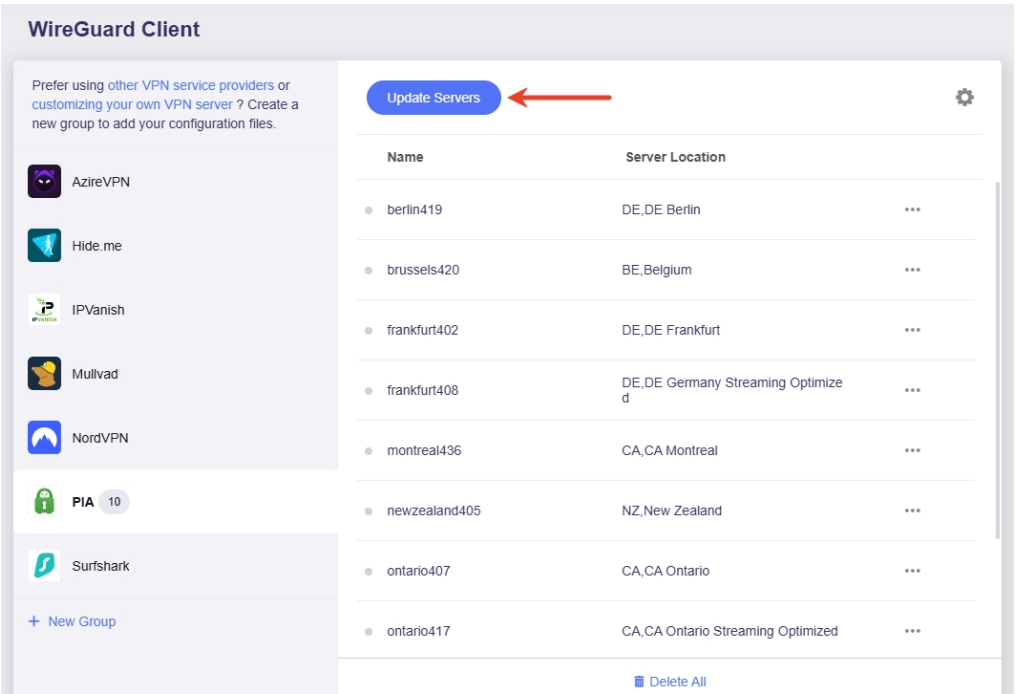
5. Una vez conectado, aparecerá un punto verde junto al archivo de configuración.



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

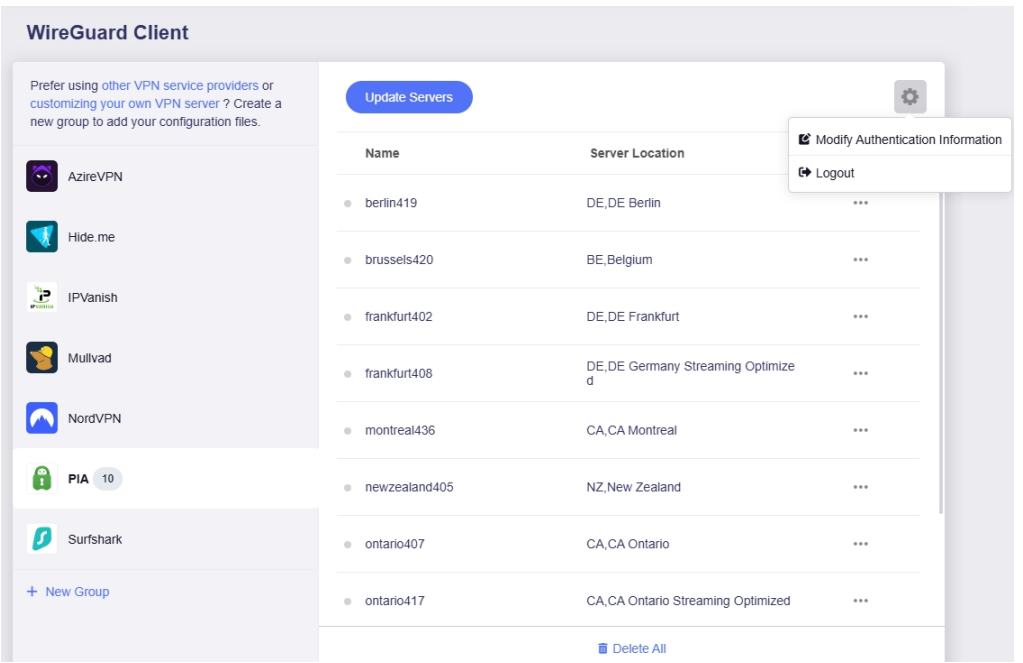
6. Actualizar servidores.

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



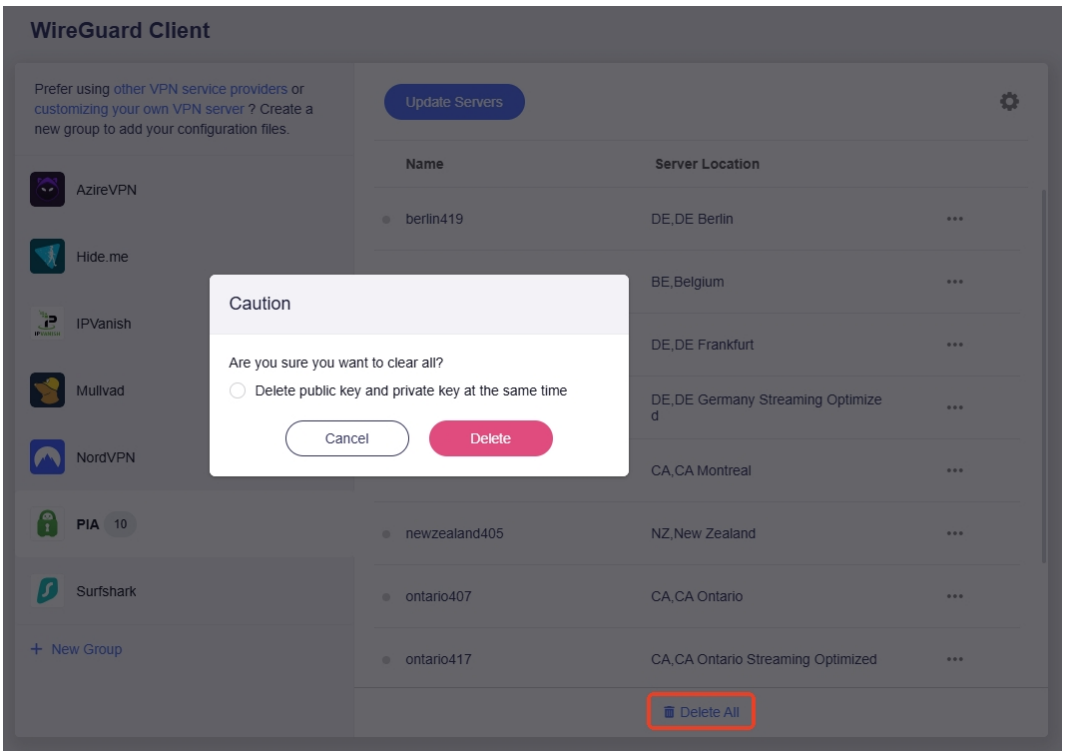
7. Edite las credenciales o cierre sesión.

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



8. Eliminar todos los archivos.

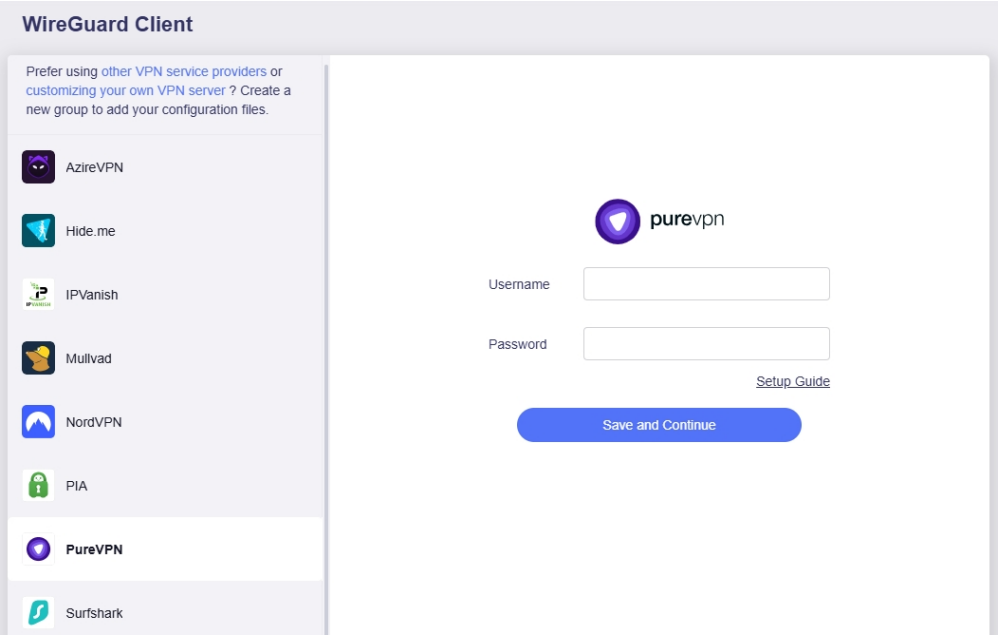
   Puede hacer clic en **Eliminar todo** para eliminar todos los archivos de configuración con un solo clic y elegir si desea eliminar los claves privadas y públicas simultáneamente.



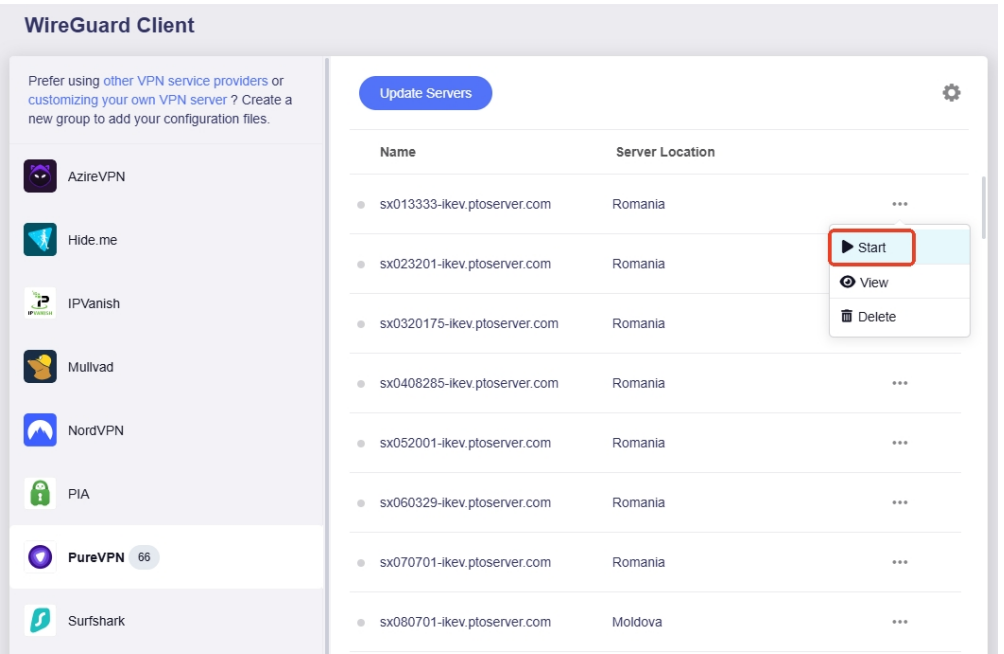
10.2.8 Configurar PureVPN

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

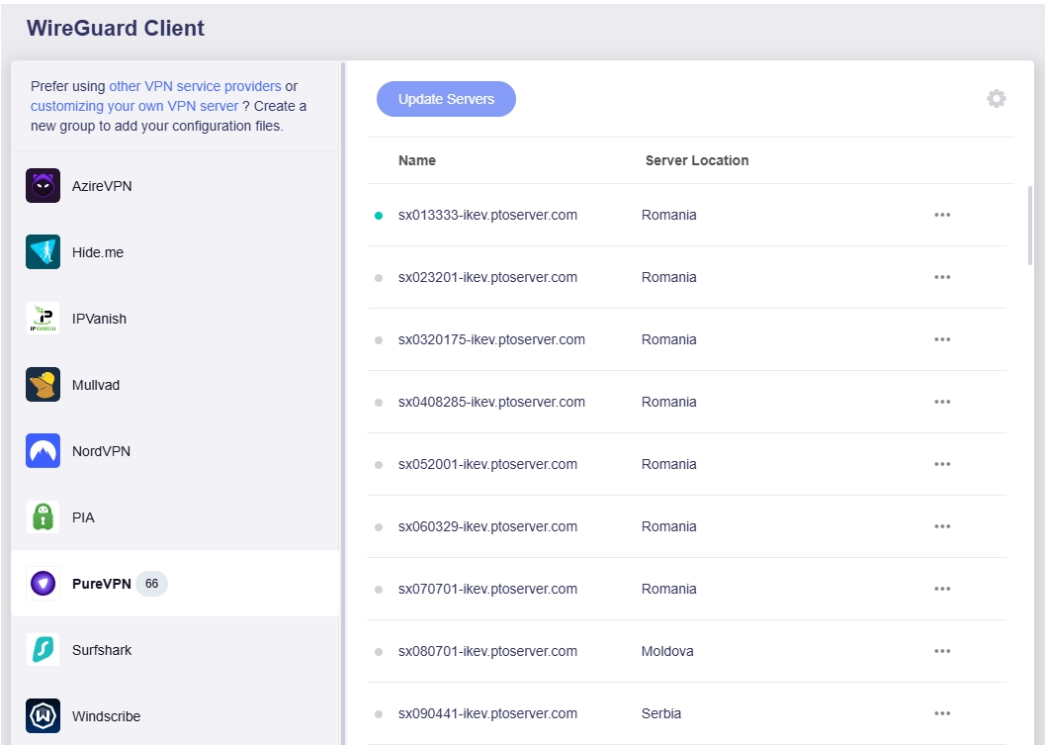
1. Inicie sesiónn a su enrutador’s web admin panel y vaya a **VPN** > **WireGuard Client** > **PureVPN**.
2. Ingrese nombre de usuario y contraseña, luego haga clic en **Guardar y continuar**. Generará archivos de configuración para cada servidor.



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



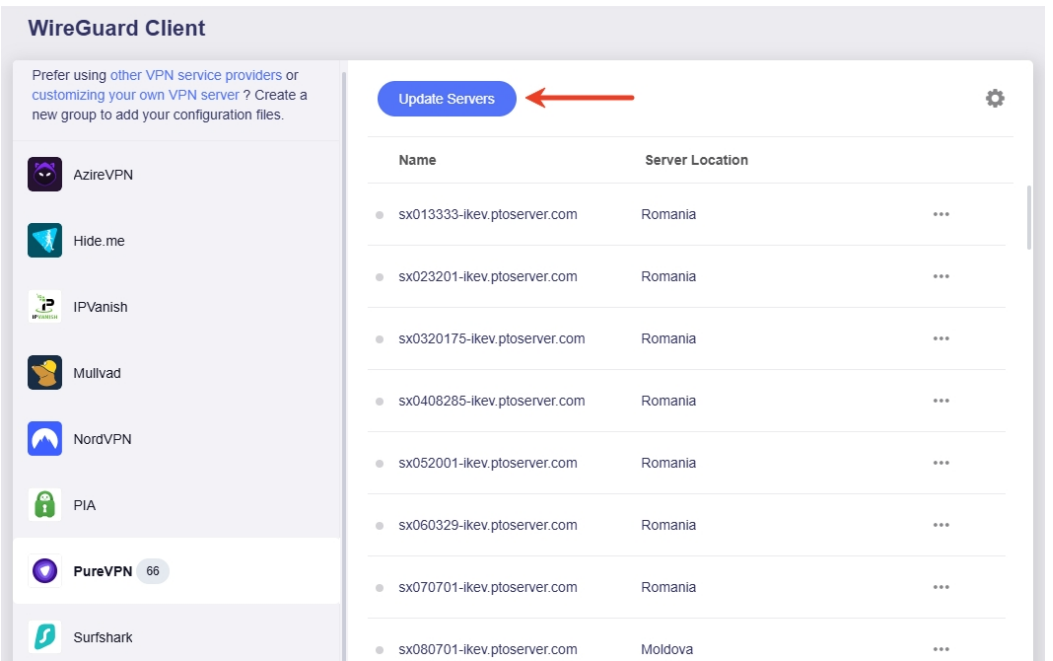
4. Una vez conectado, aparecerá un punto verde junto al archivo de configuración.



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

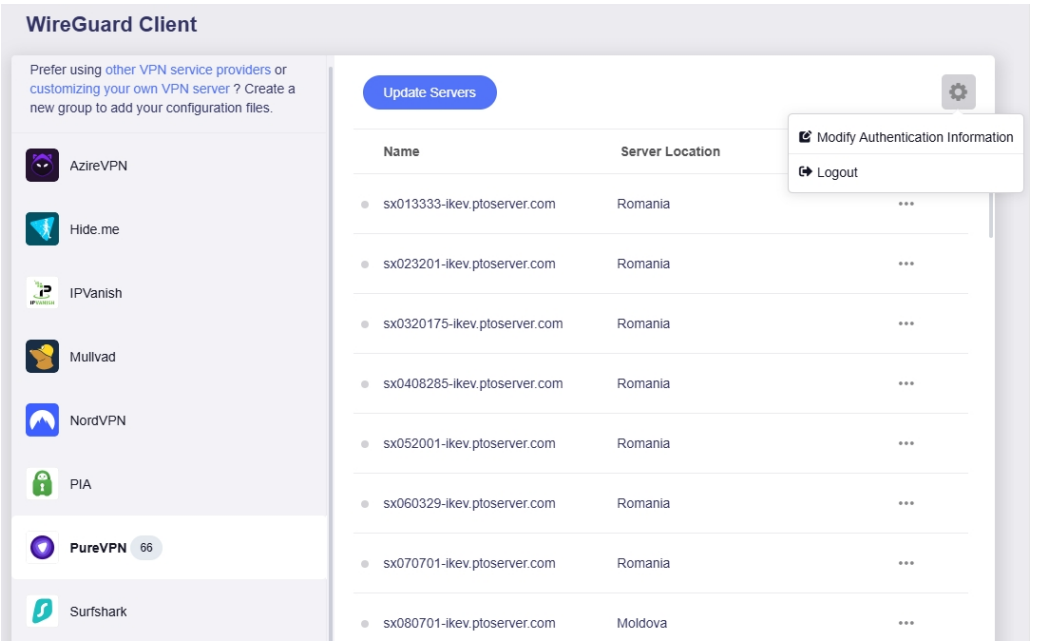
5. Actualizar servidores.

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



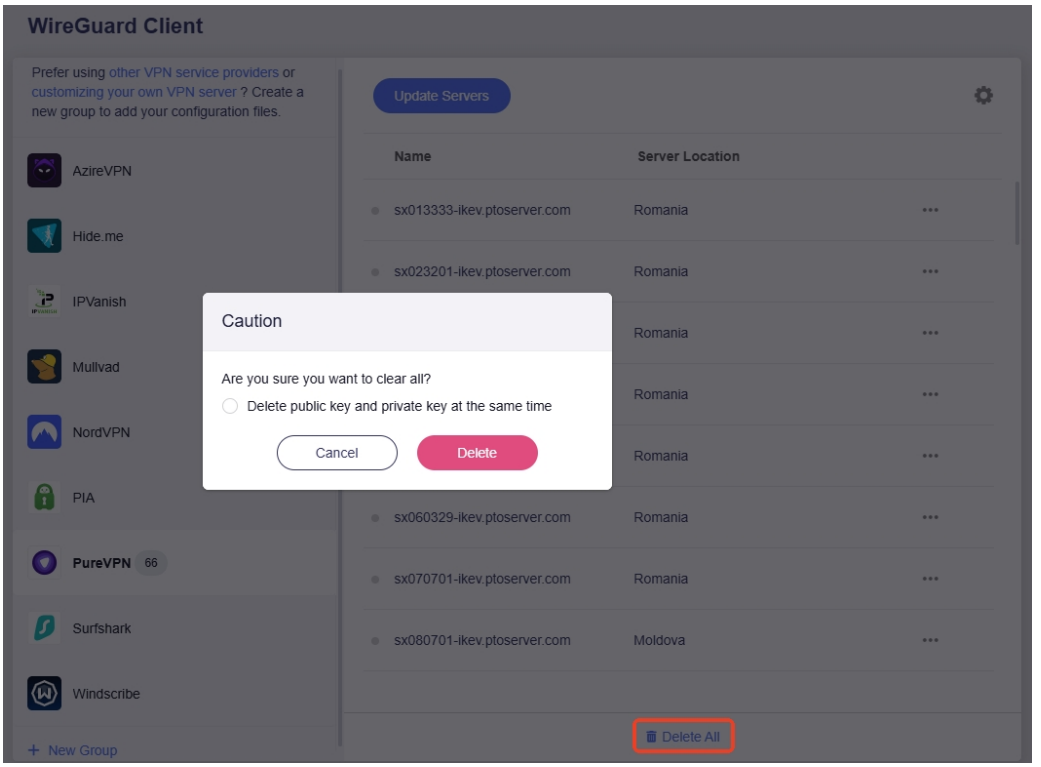
6. Editar credenciales o cerrar sesión.

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



7. Eliminar todos los archivos.

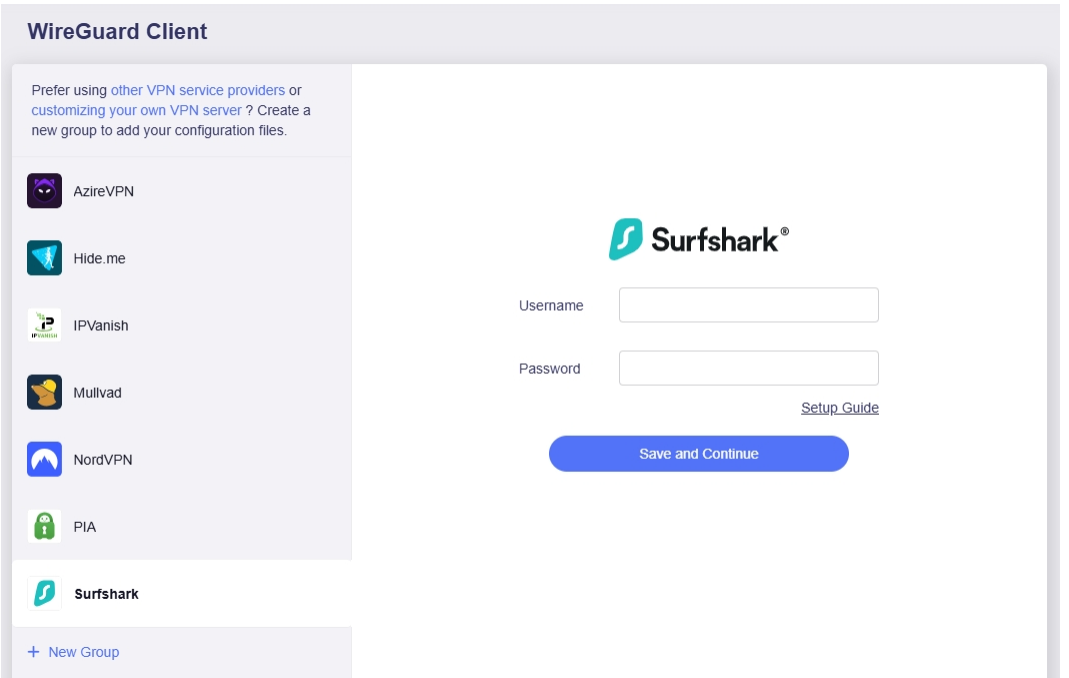
   Puede hacer clic en **Eliminar todo** para eliminar todos los archivos de configuración con un solo clic y elija si desea eliminar las claves pública y privada simultáneamente.



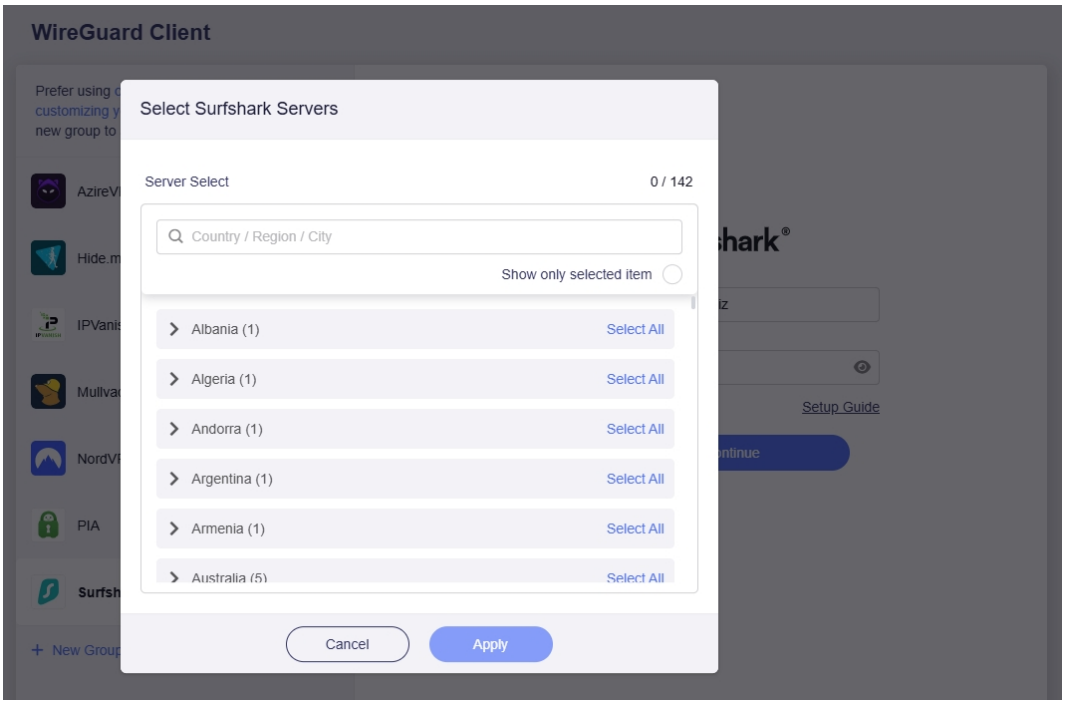
10.2.9 Configurar Surfshark

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

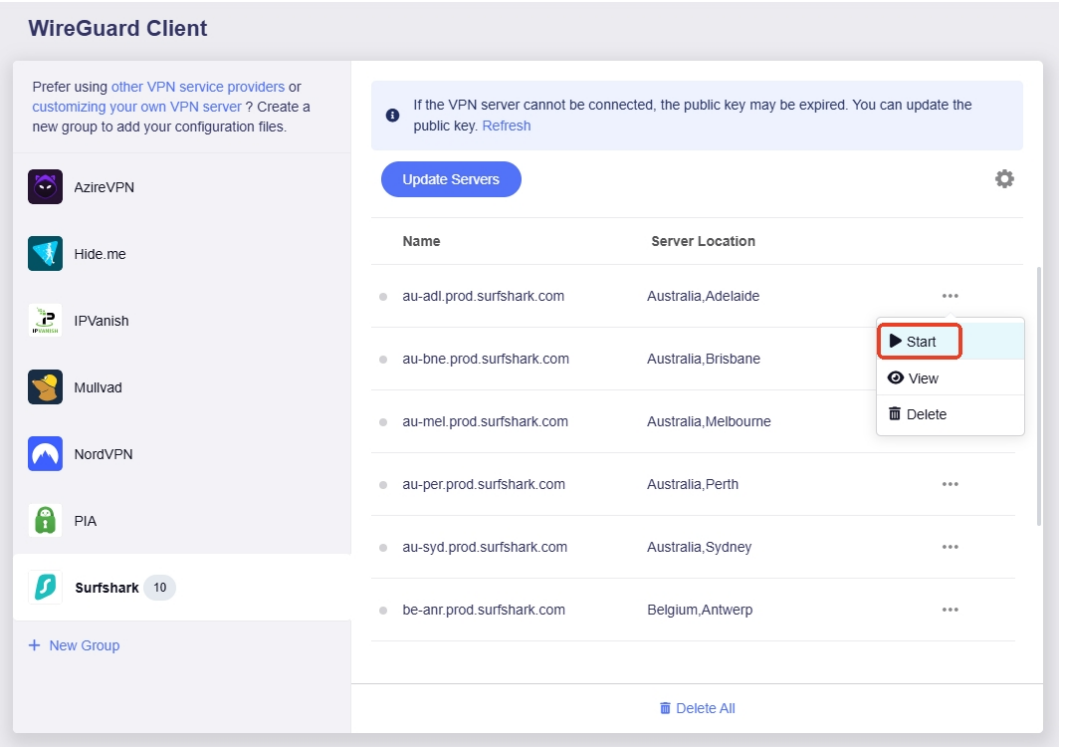
1. Inicie sesiónn en su enrutador’s web admin panel y vaya a **VPN** > **WireGuard Client** > **Surfshark**.
2. Ingrese nombre de usuario y contraseña, luego haga clic en **Guardar y continuar**.



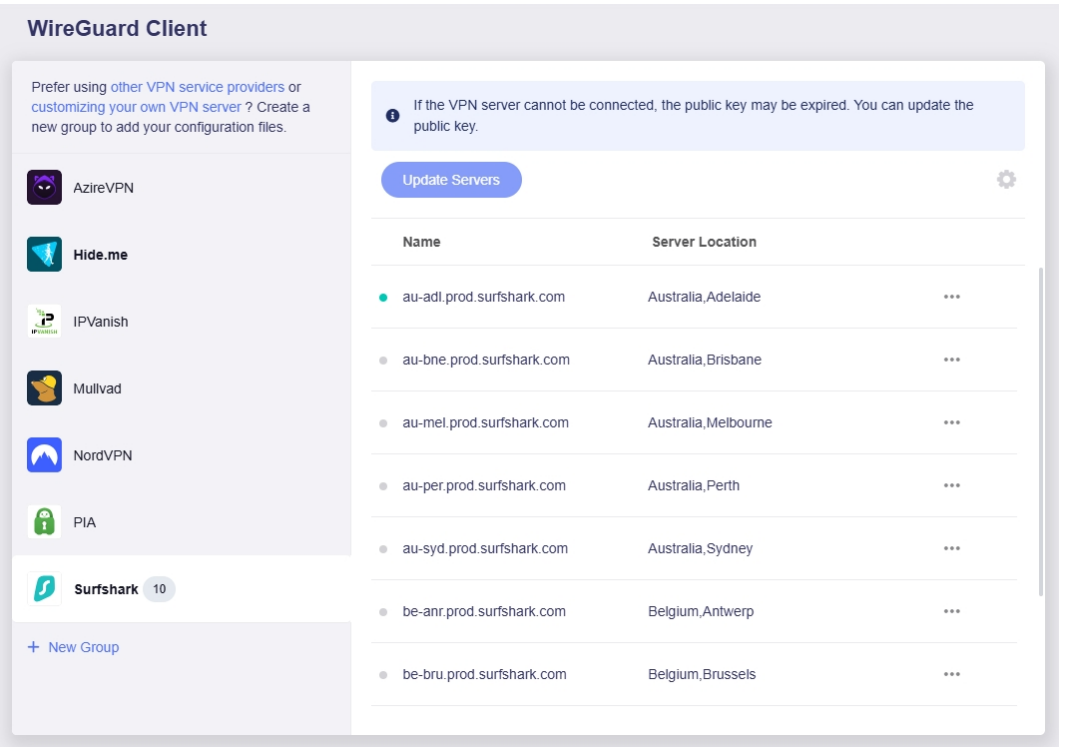
3. Seleccione los servidores a los que desea conectarse y haga clic en **Aplicar**.



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



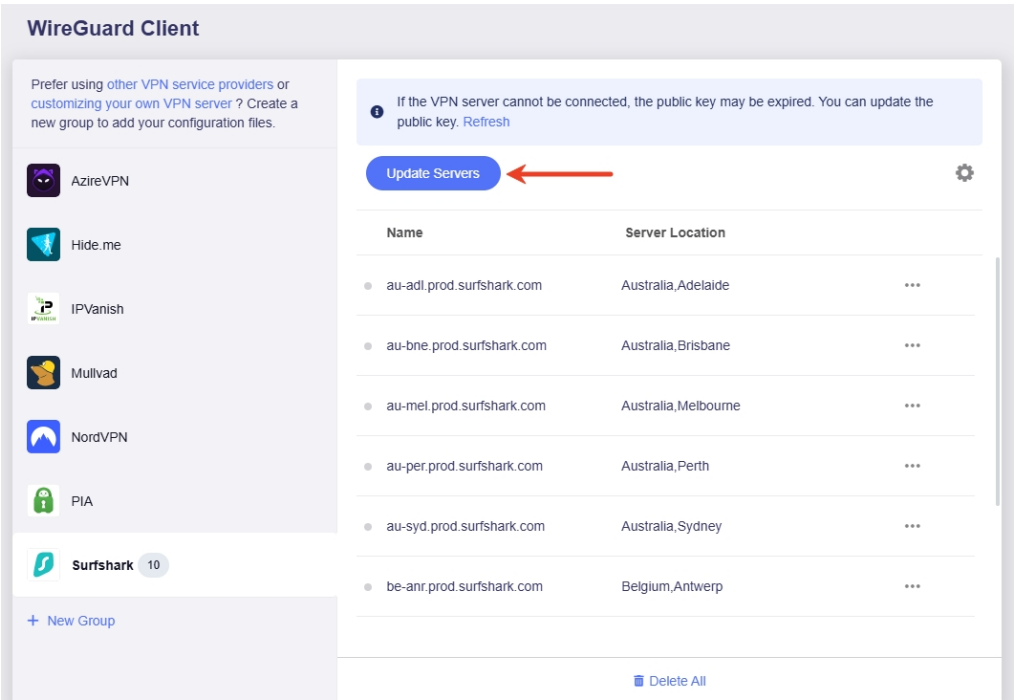
5. Una vez conectado, aparecerá un punto verde junto a la configuración. archivo.



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

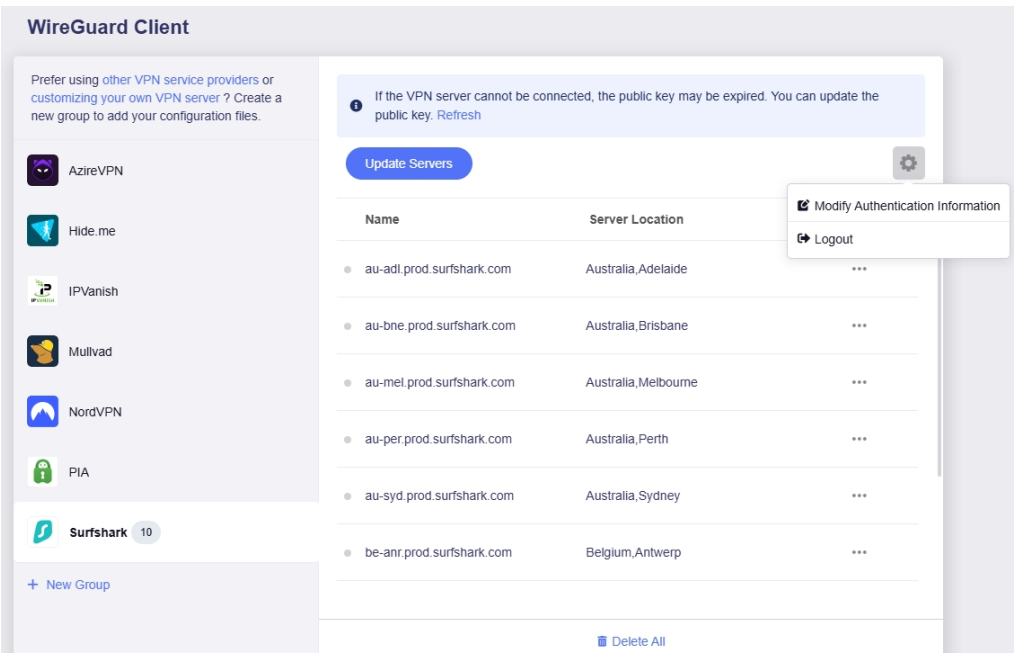
6. Actualizar servidores.

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



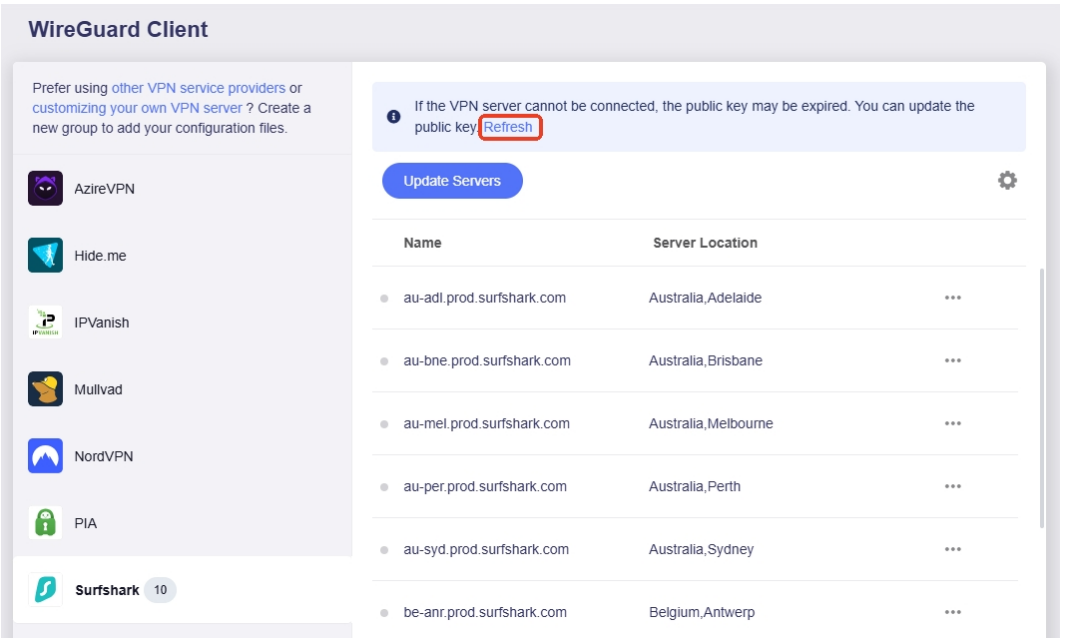
7. Edite las credenciales o cierre la sesión.

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



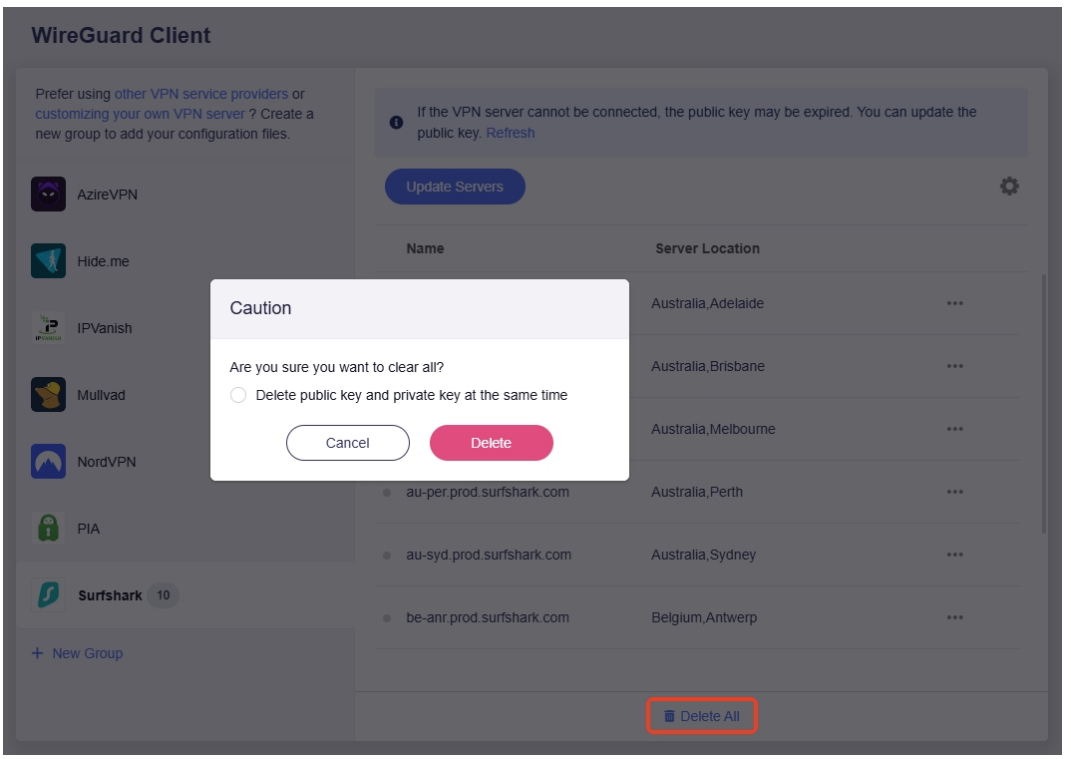
8. Actualizar.

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



9. Eliminar todos los archivos.

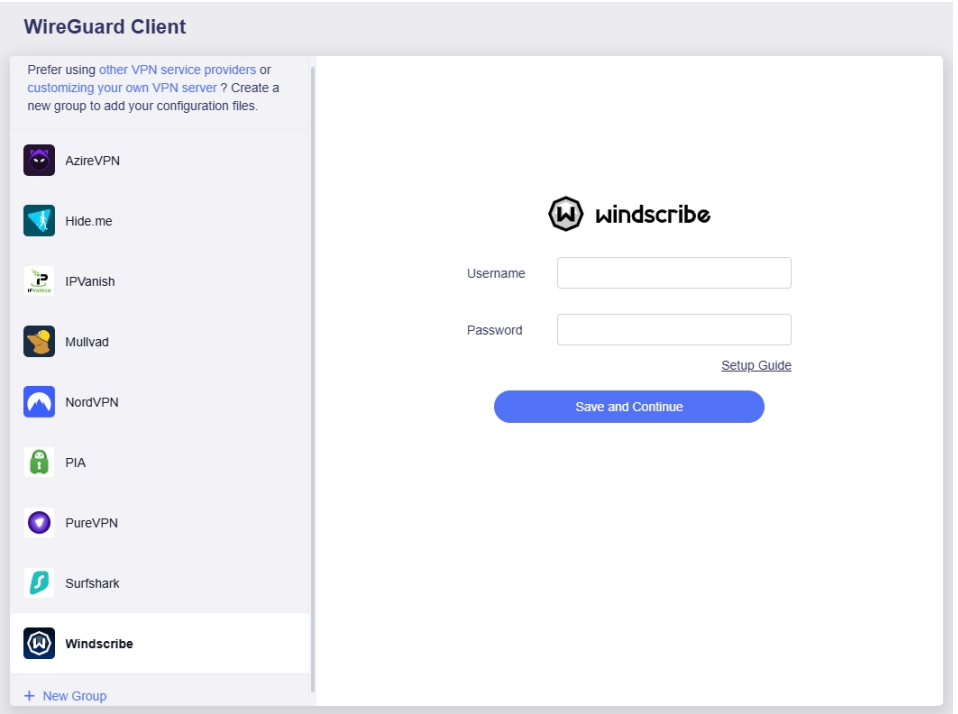
   Puede hacer clic en **Eliminar todo** para eliminar todos los archivos de configuración con un solo clic y elegir si desea eliminar las claves pública y privada simultáneamente.



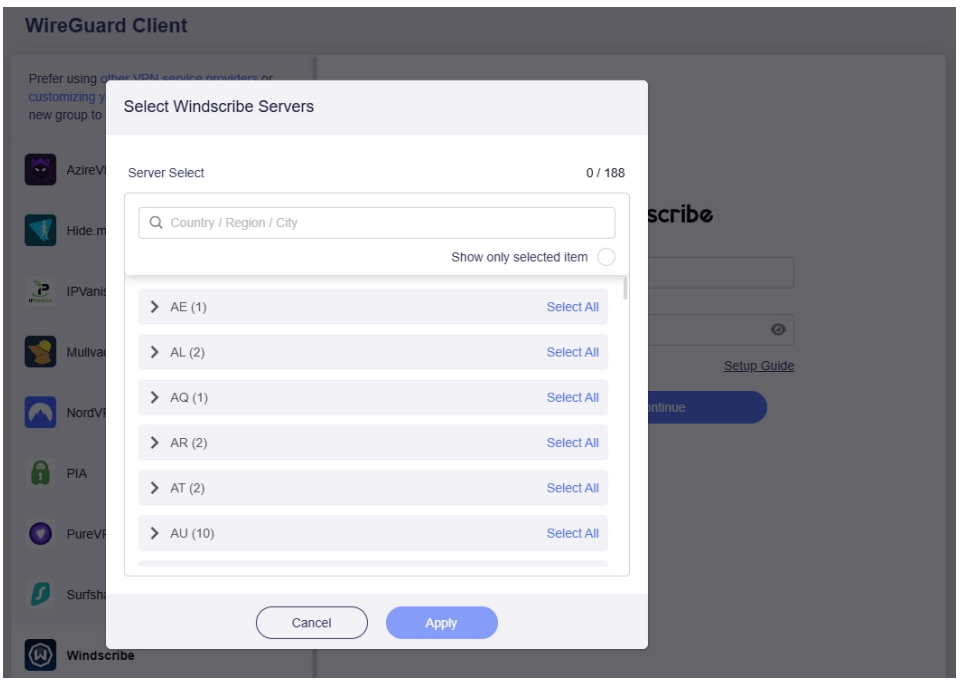
10.2.10 Configurar Windscribe

Siga las pasos a continuación para configurar su enrutador como cliente Windscribe.

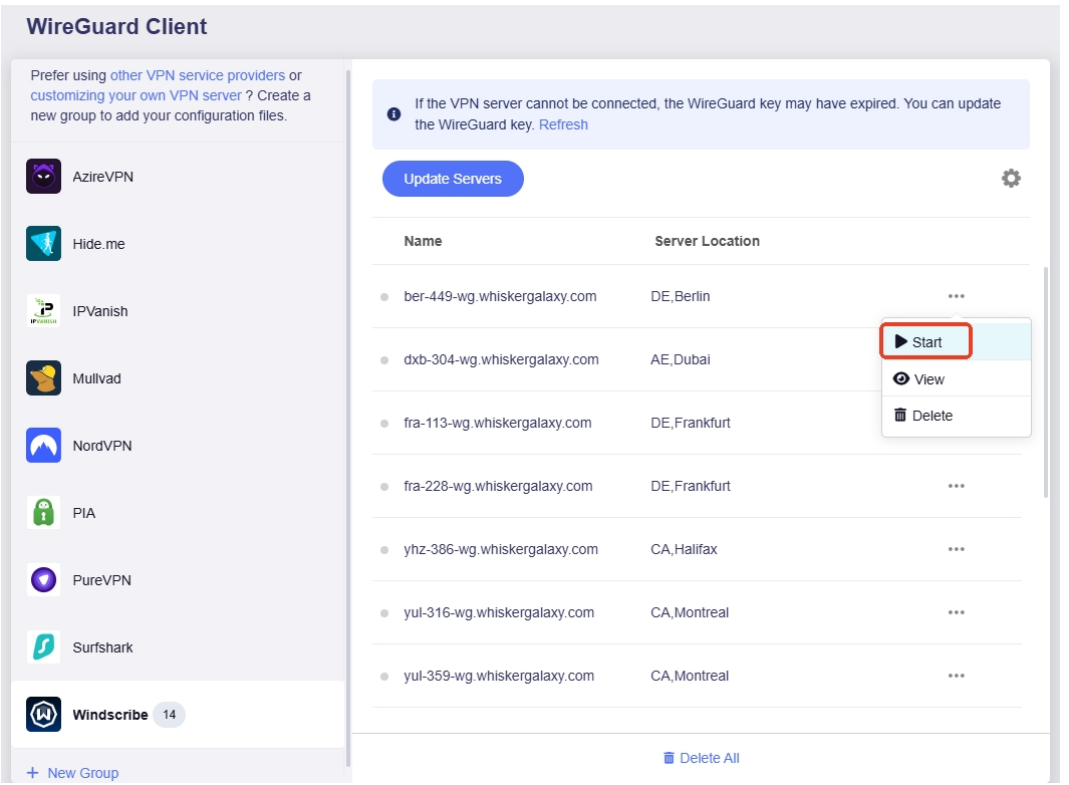
1. Inicie sesiónn en la web admin panel y vaya a **VPN** > **Cliente WireGuard** > **Windscribe**.
2. Ingrese nombre de usuario y contraseña, luego haga clic en **Guardar y continuar**. Se generarán archivos de configuración para cada servidor.



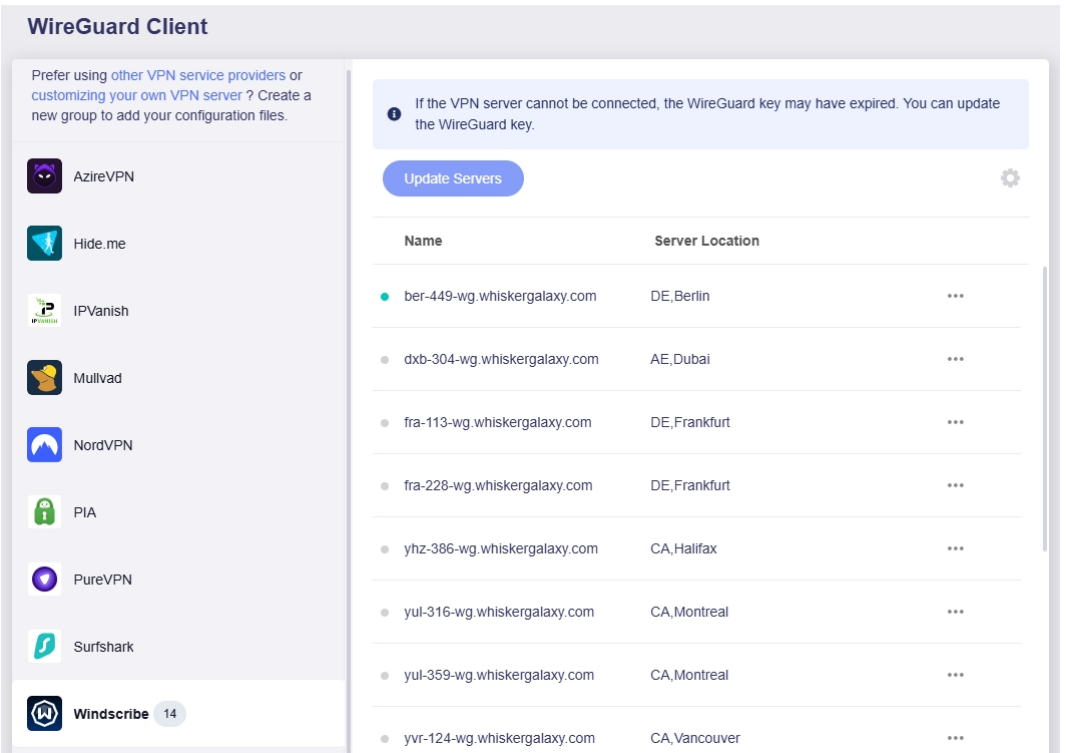
3. Seleccione los servidores que desea conéctese y haga clic en **Aplicar**.



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



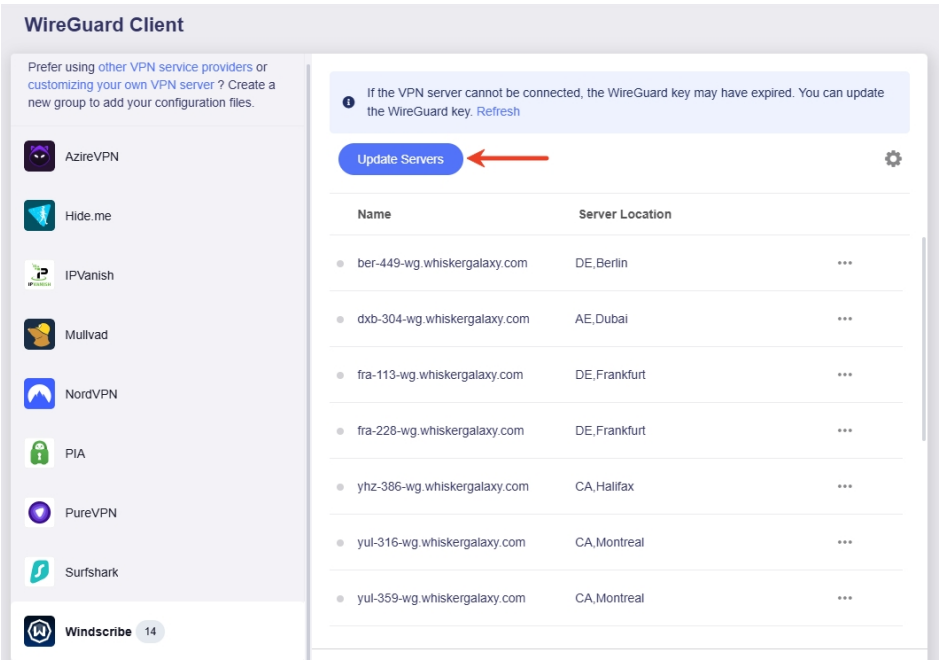
5. Una vez conectado, aparecerá un punto verde junto al archivo de configuración.



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

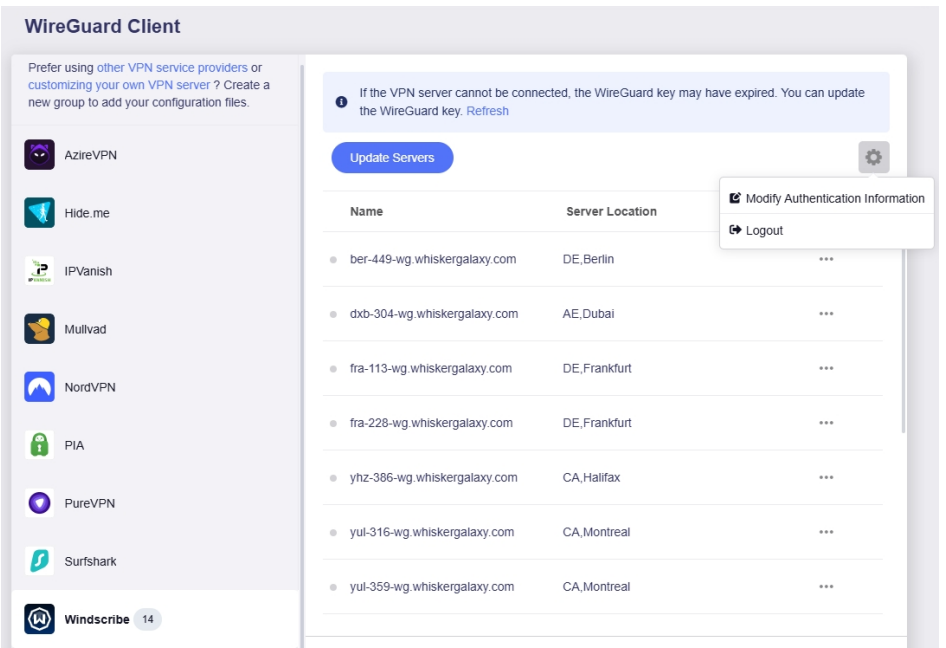
6. Actualizar servidores.

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



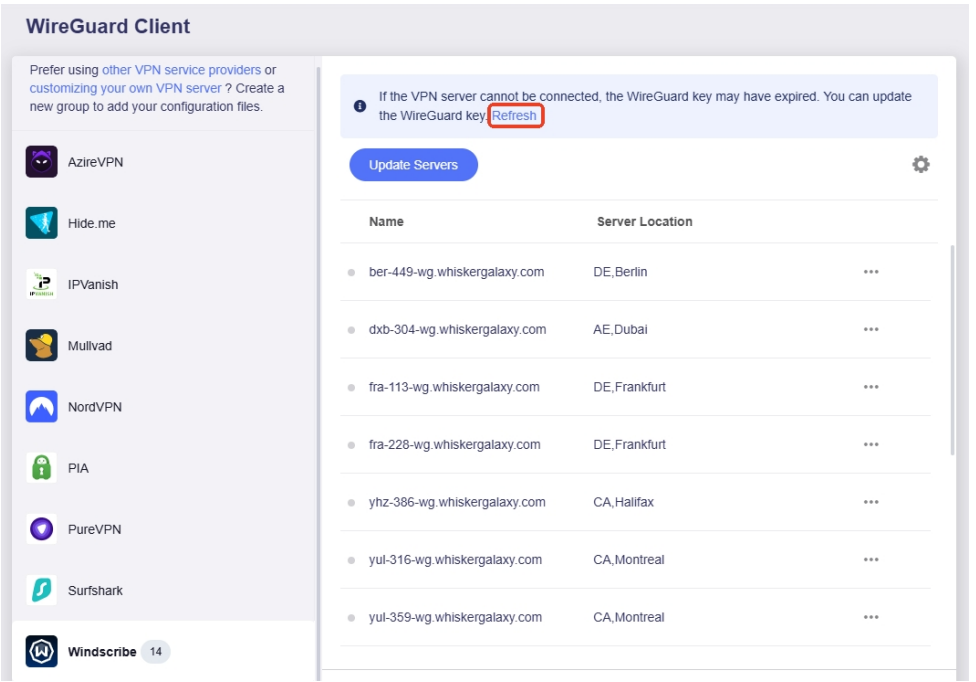
7. Edite las credenciales o cierre sesión.

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



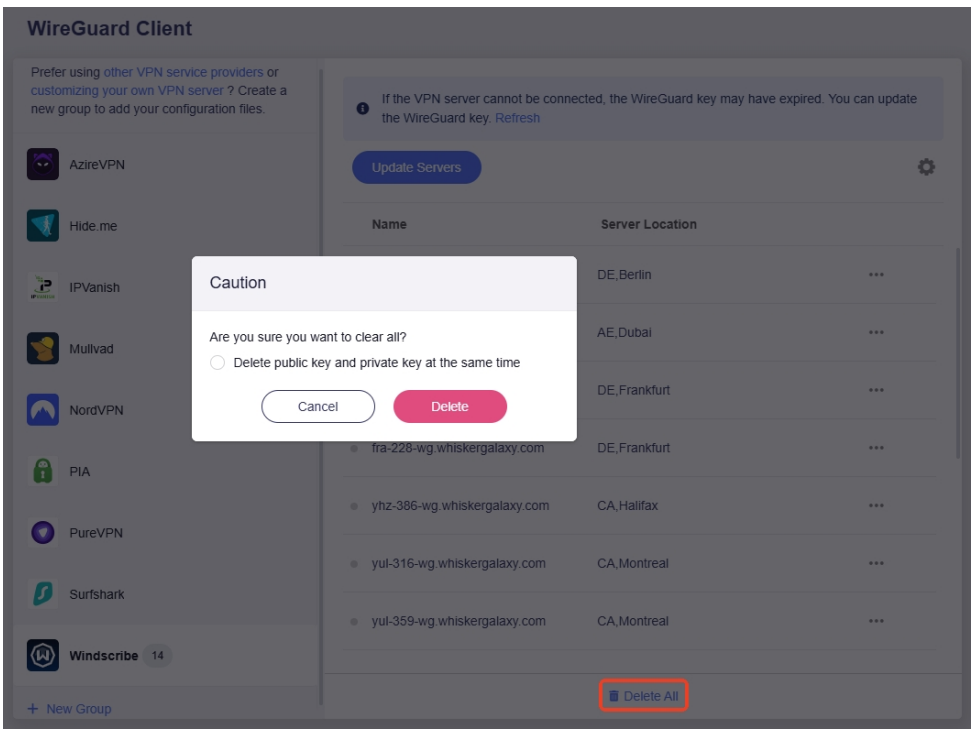
8. Actualizar.

   Puedes hacer clic en **Actualizar** para actualizar la clave pública cuando la VPN no se puede conectar.



9. Eliminar todos los archivos.

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

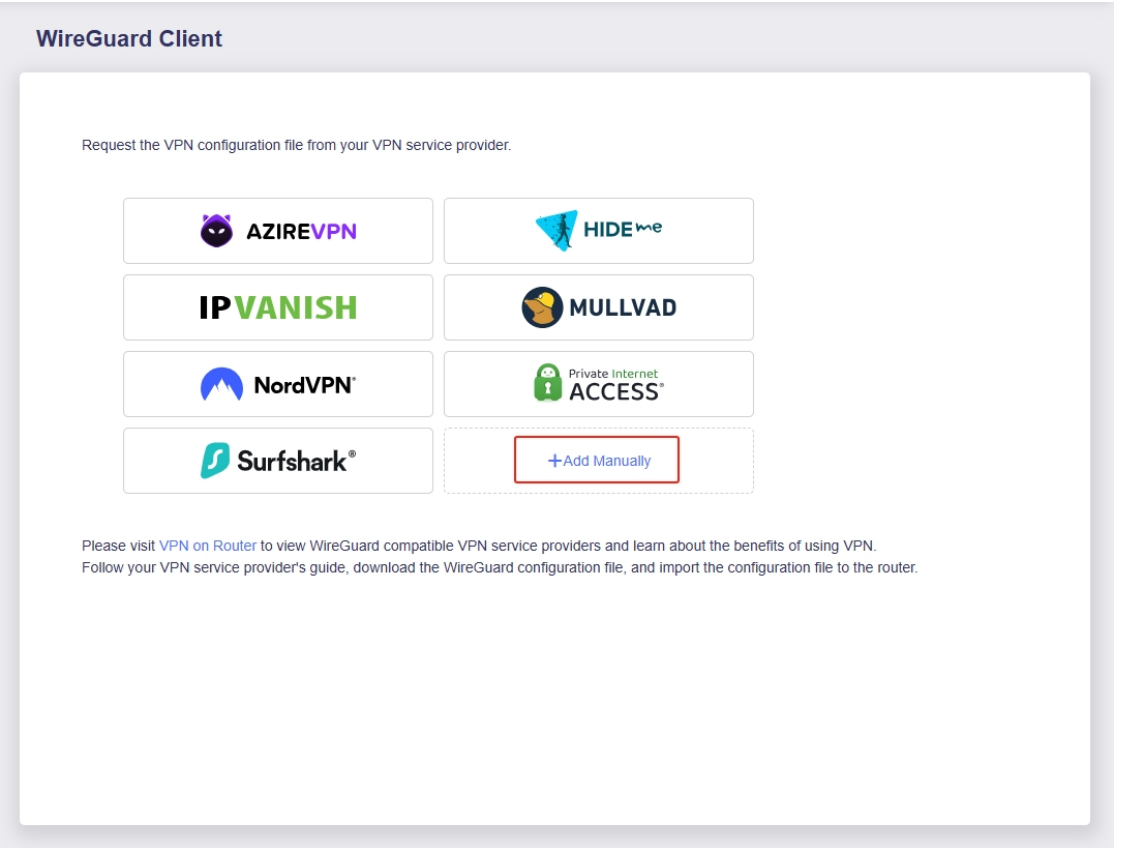


10.2.11 Configurar el cliente WireGuard manualmente (para otros proveedores)

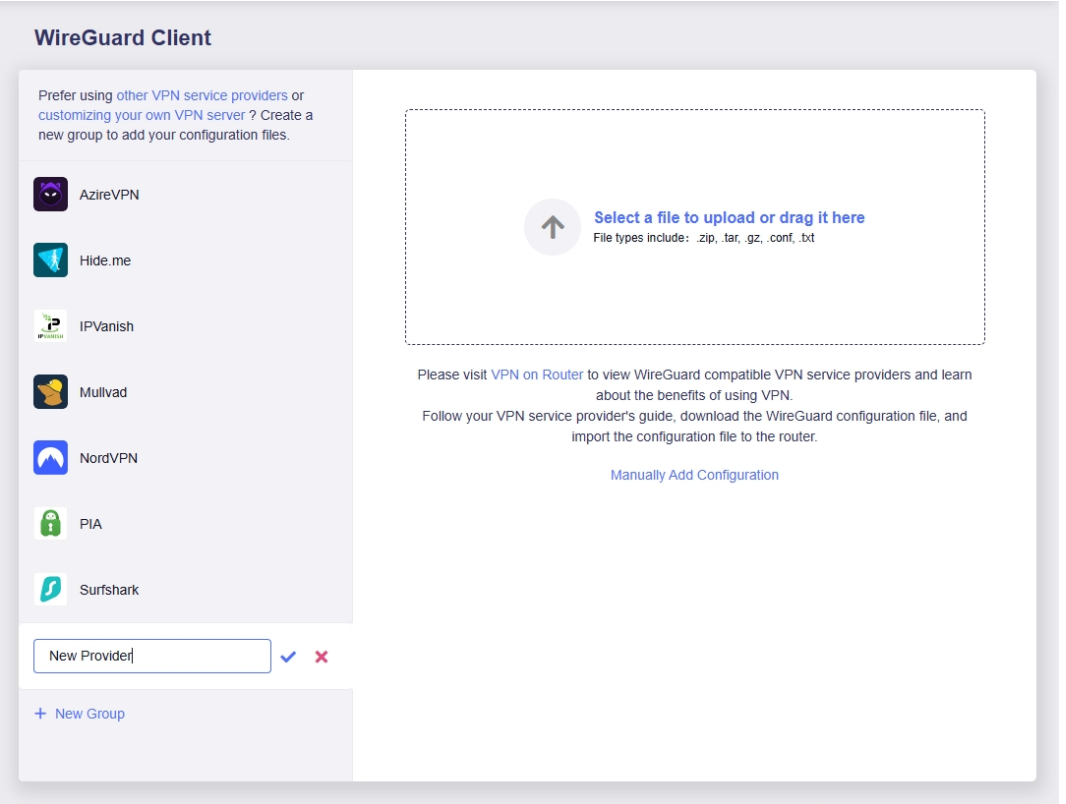
Si su proveedor de servicios WireGuard no está integrado en el panel de administración web, visite primero el sitio web oficial de su proveedor de servicios suscrito para obtener el archivo de configuración. Luego cárguelo en el enrutador para configurar un cliente WireGuard. Si no sabes cómo descargar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

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

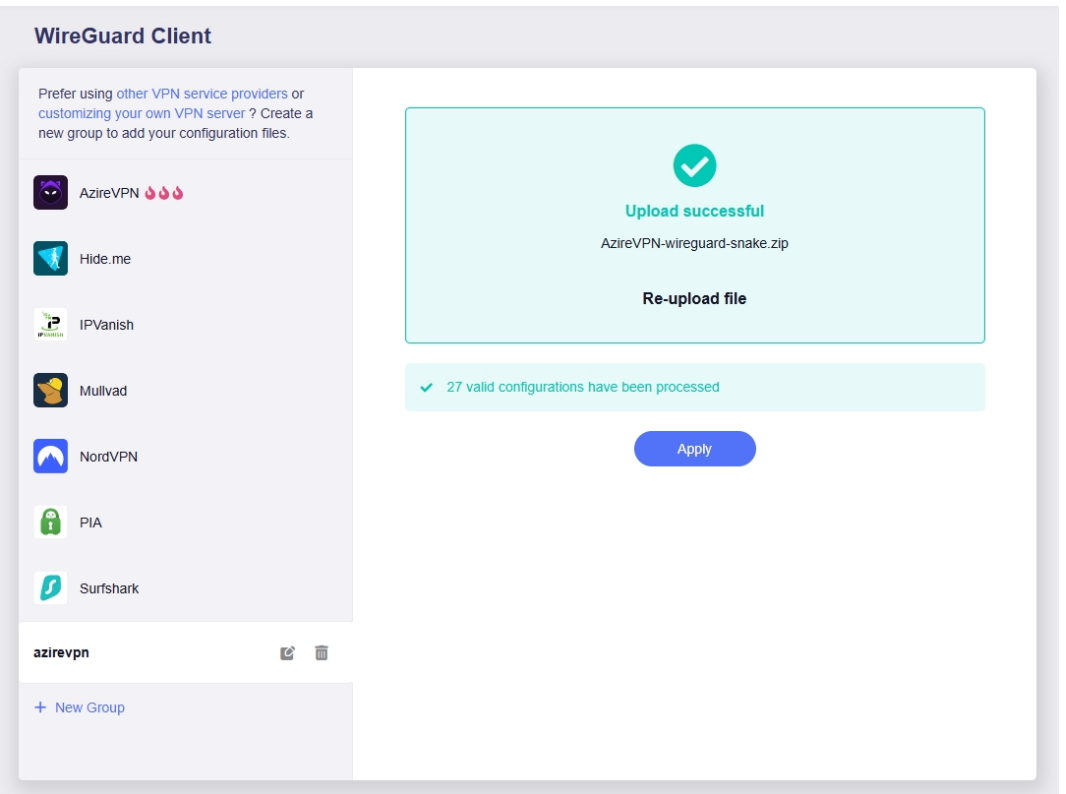
1. Inicie sesiónn en su enrutador's web admin panel y navegue hasta **VPN** > **Cliente WireGuard** > **Agregar manualmente**.



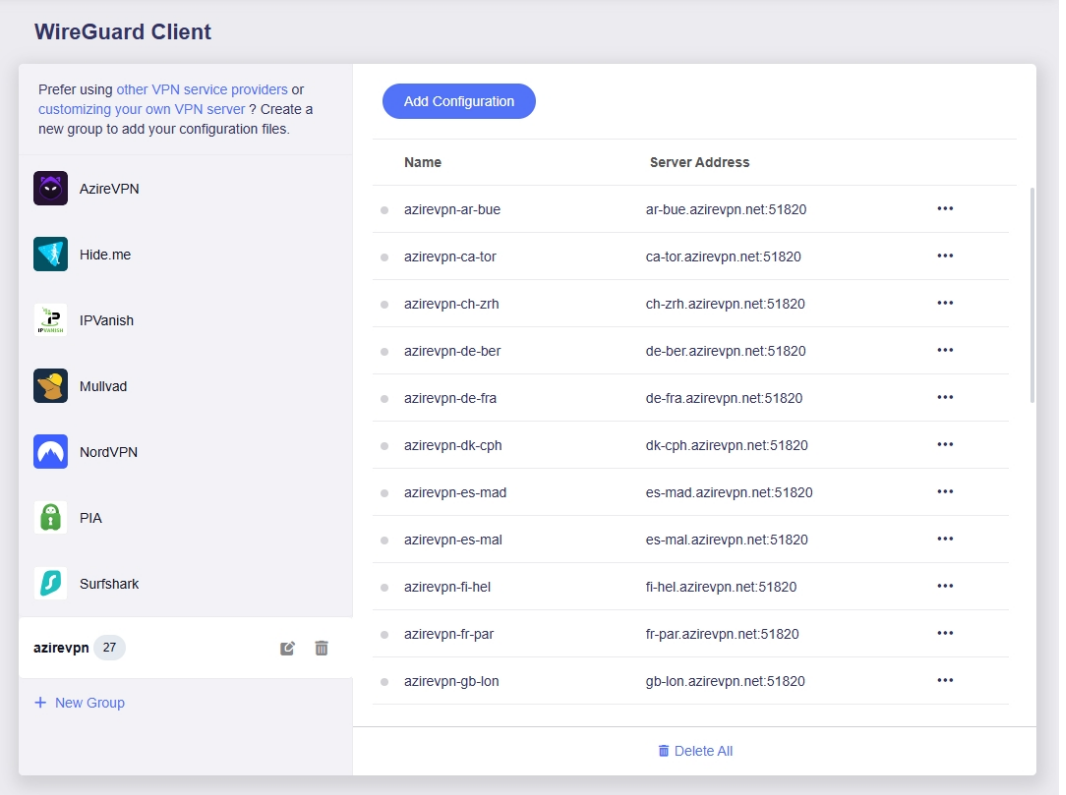
2. Se creará un grupo en la barra lateral izquierda. Establezca un nombre descriptivo para el grupo.



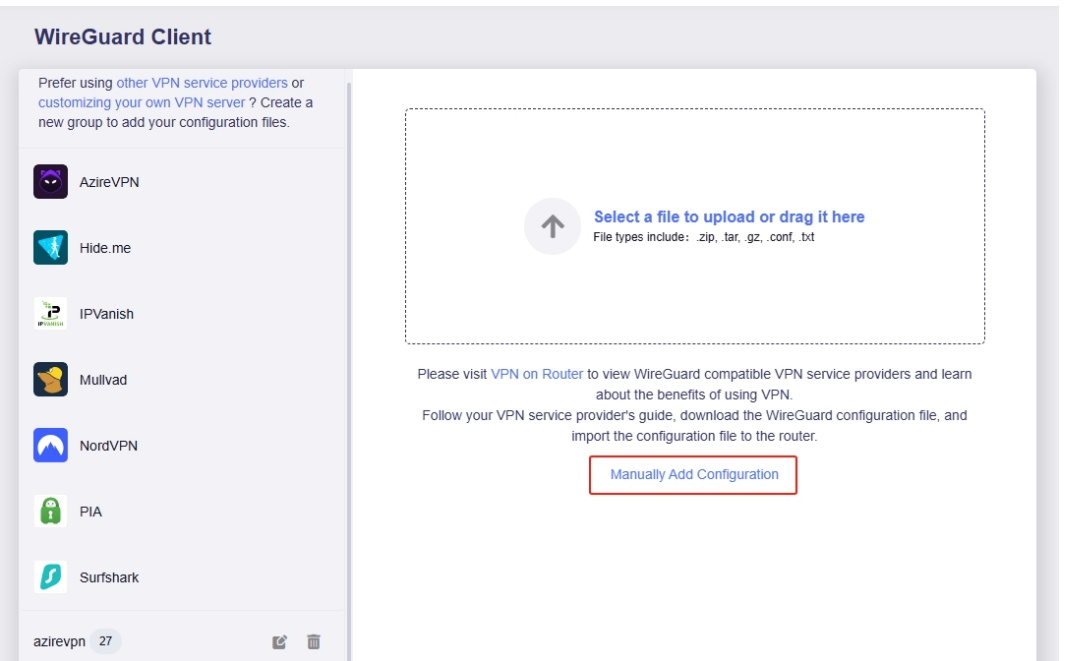
3. Click el área de carga para cargar su archivo de configuración de WireGuard (formatos admitidos: zip, tar, gz, conf, txt), y haga clic en **Aplicar**.

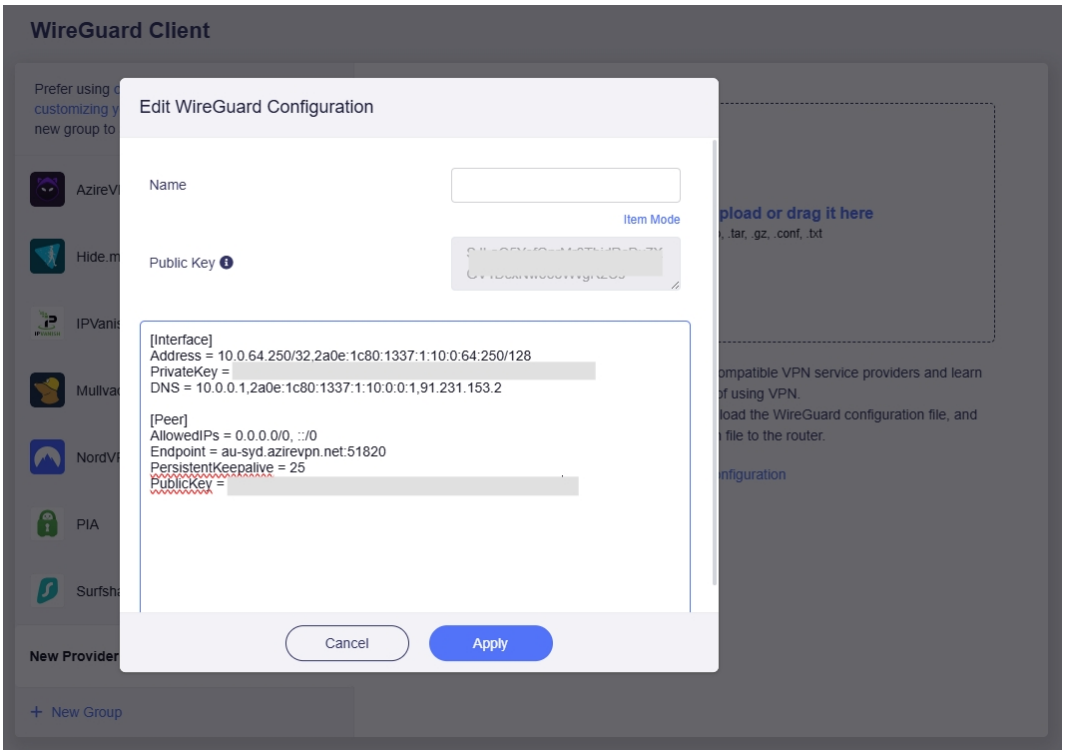


Si subes un archivo comprimido que contiene varios archivos de configuración, se descomprimirá automáticamente, como se muestra a continuación.

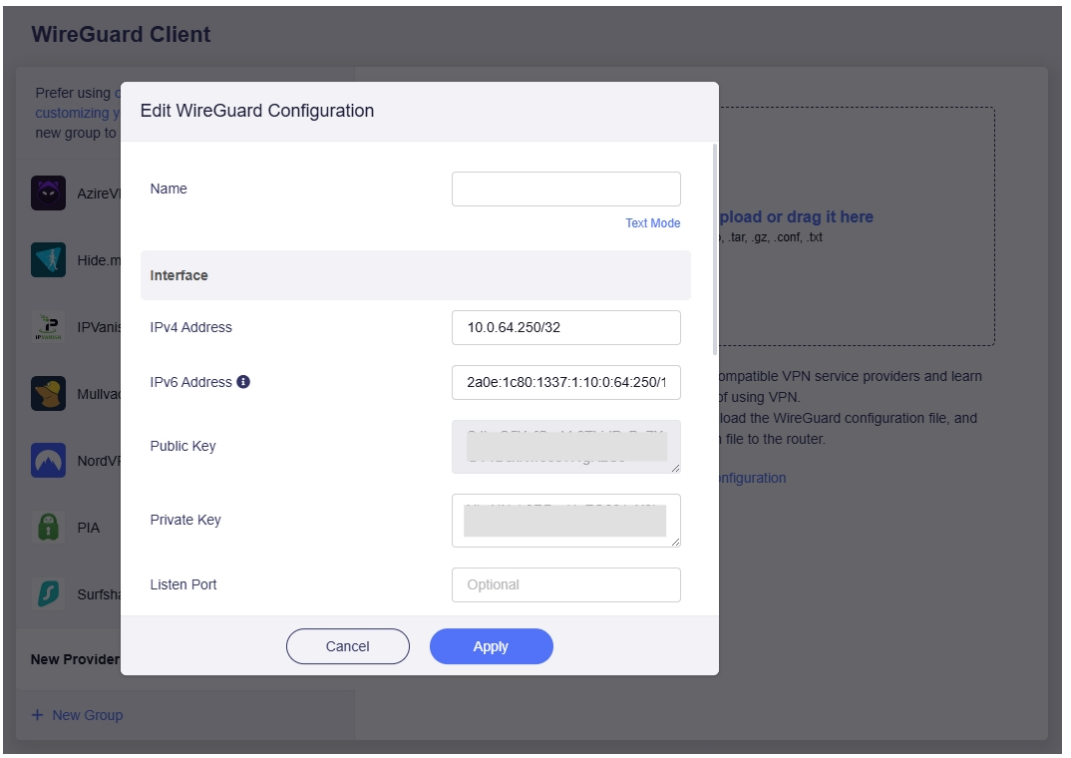


Como alternativa, puedes hacer clic en **Agregar configuración manualmente** en en la parte inferior del área de carga, agregue los detalles de configuración en forma de texto y haga clic en **Aplicar**.

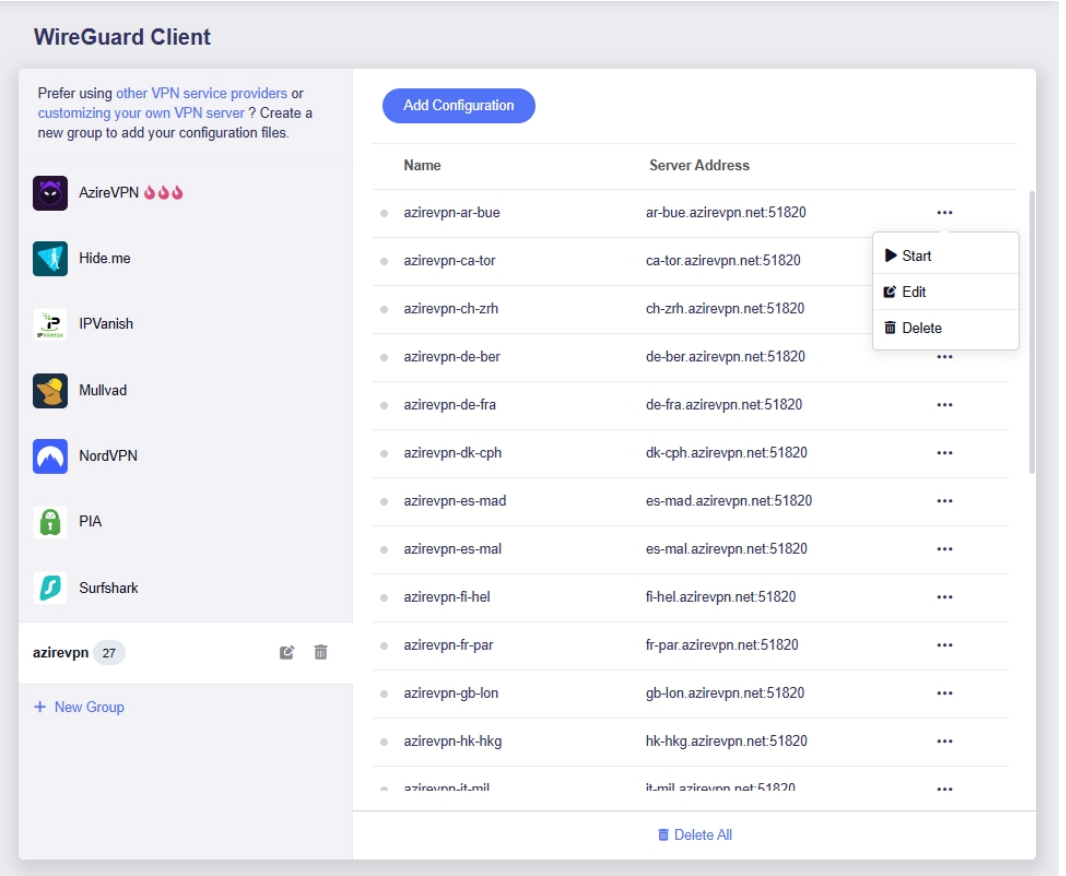




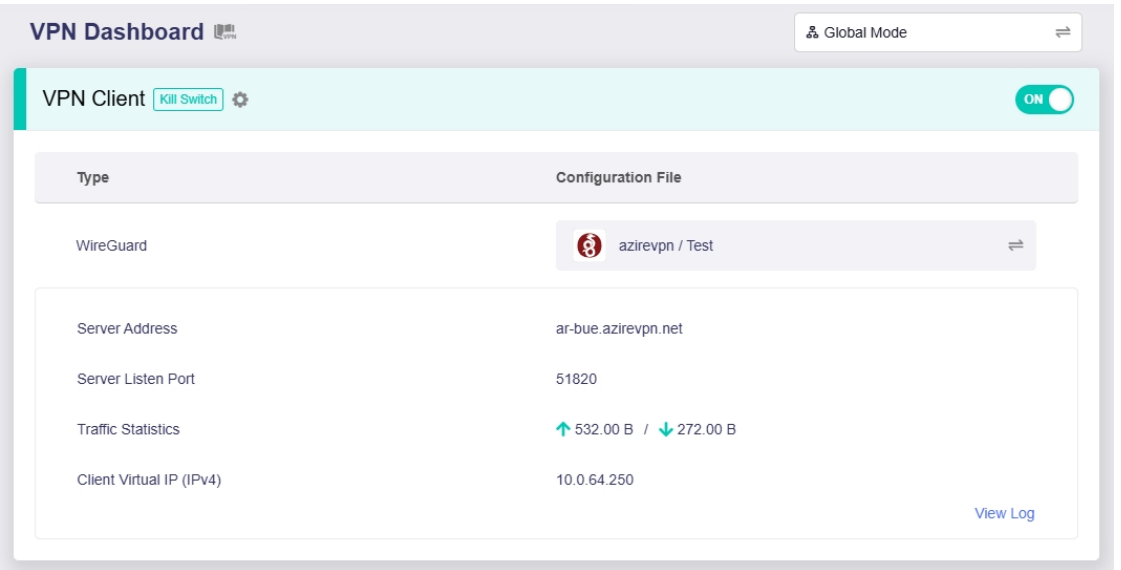
Si desea verificar cada elemento, puede cambiar al modo Elemento y verificar la configuraciónuración detalles, luegoluego haga clic en **Aplicar**.



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



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



Capítulo 11

Red

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

11.1 Multi-WAN

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

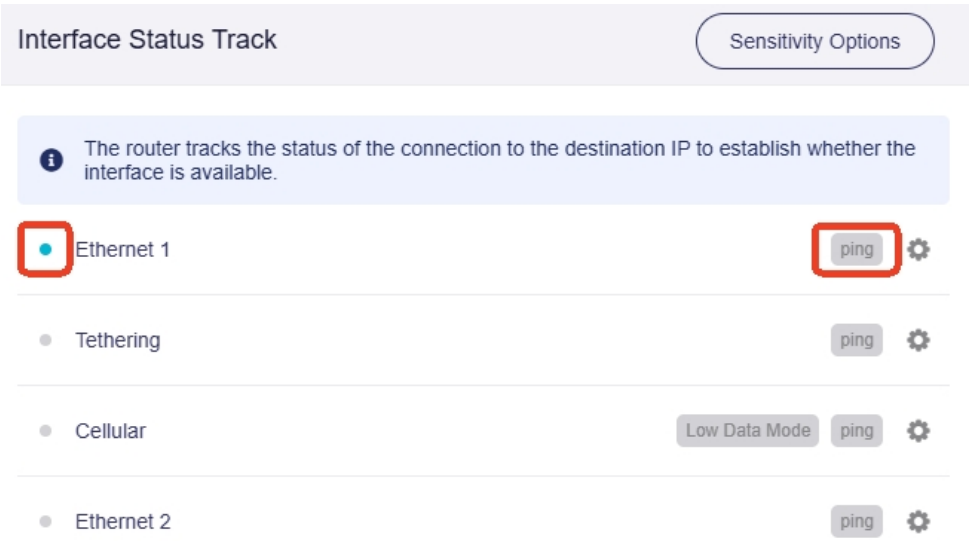
- **Conmutación por error**: cambia automáticamente a una conexión alternativa en poco tiempo si falla la conexión principal, lo que garantiza un acceso ininterrumpido a la red.
- **Equilibrio de carga**: distribuye el tráfico de red entre todas las conexiones disponibles en una proporción establecida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

Brume 3 admite tres tipos de conexión a Internet métodos, incluidos Ethernet, Anclaje a red y celular, cada uno de los cuales ofrece una función de red distinta en configuraciones definidas por software.

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.

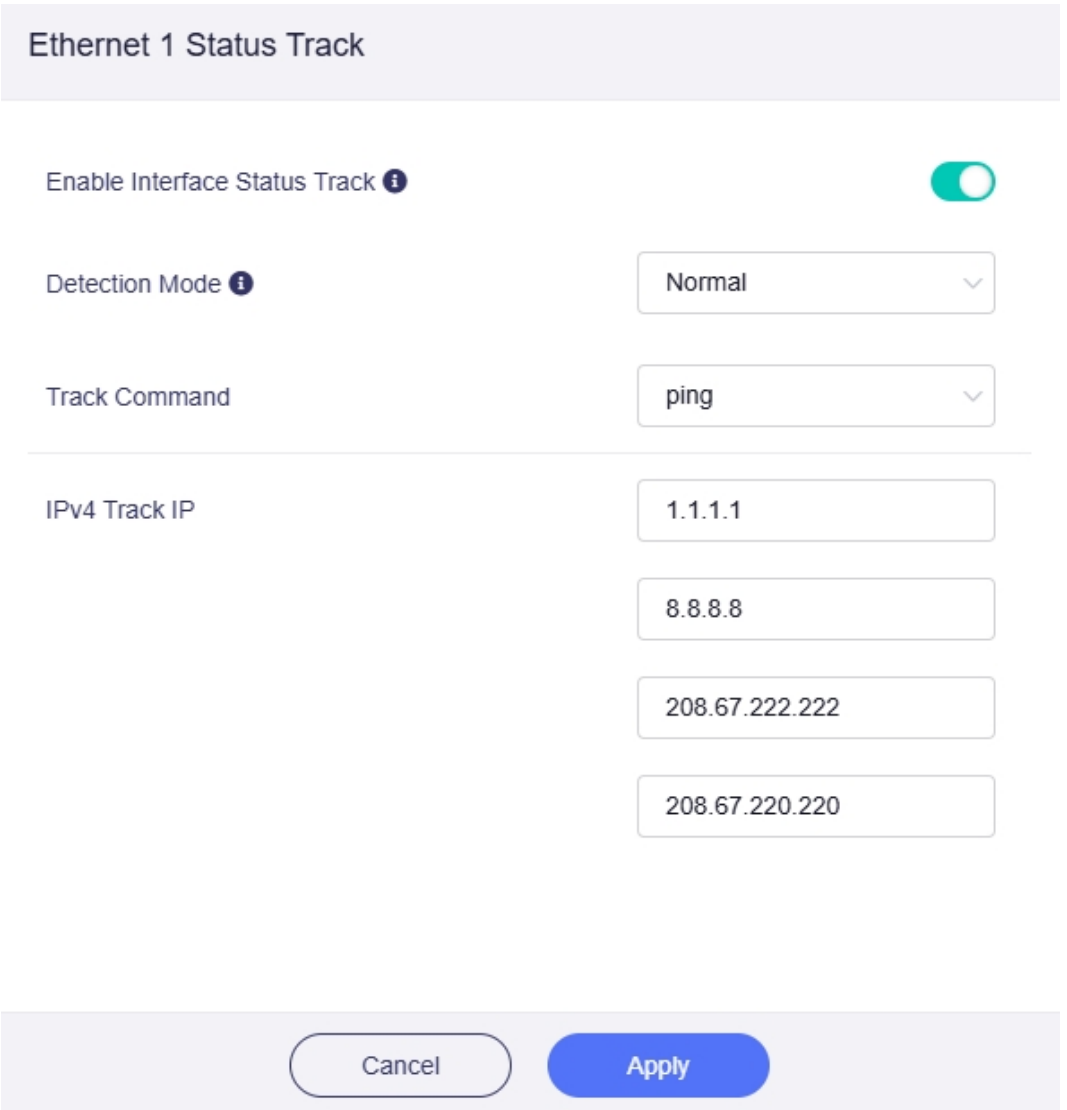
11.1.1 Seguimiento del estado de la interfaz

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



En la sección **Seguimiento del estado de la interfaz**, haga clicen el engranaje a la derecha para acceder a la configuración de seguimiento de estado para cada interfaz de red.

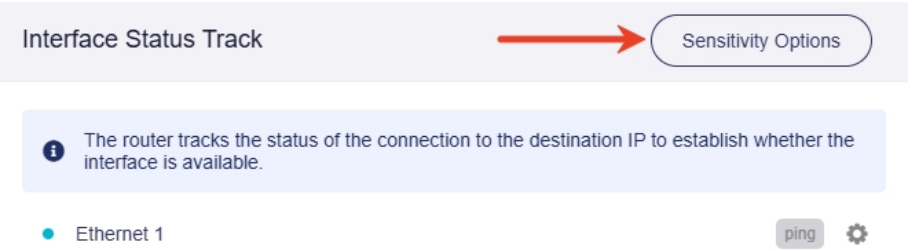
A continuación se muestran la configuración de seguimiento de estadoings para la interfaz Ethernet. La misma lógica de configuración se aplica a otras interfaces.



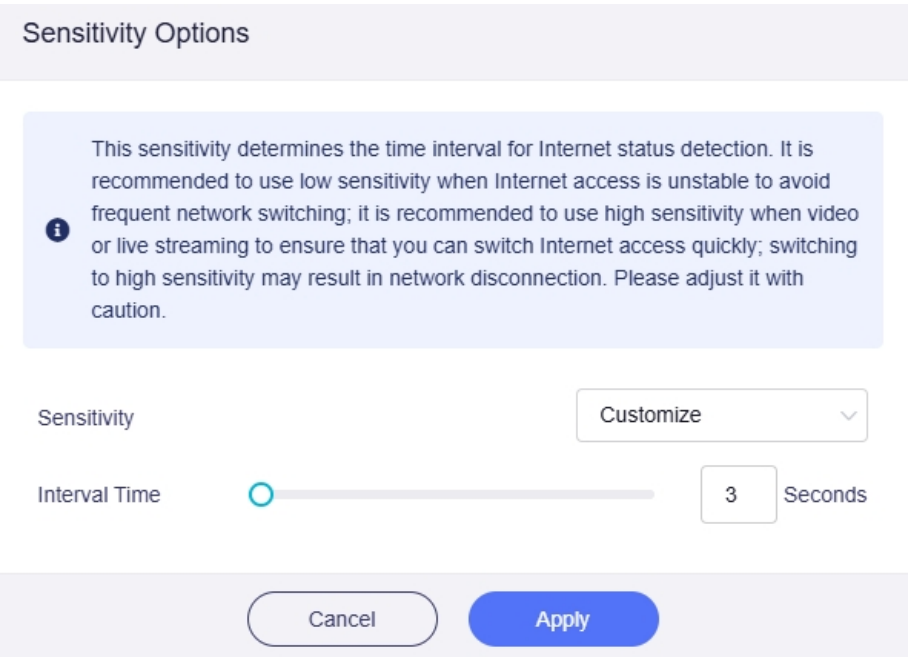
- **Habilitar seguimiento del estado de la interfaz**: Está habilitadode forma predeterminada. Si está deshabilitado, el enrutador determinará el estado de la interfaz según las condiciones (por ejemplo, si el cable Ethernet está enchufado).
- **Modo de detección**: esta característica se introdujo como modo de datos bajos en firmware v4.5, luego cambió el nombre a Modo de detección en firmware v4.7. Hay tres modos disponibles: Modo normal, Modo de datos bajos y Modo estricto.
    - **Normal Modo**: Es used de forma predeterminada.

    - **Datos bajos Modo**: Solo activa el seguimiento cuando se produce un error de red en la red interfaz. Utilice este modo si tiene un plan de datos limitado. Tenga en cuenta que la reconexión después de una desconexión puede ser un poco más lenta que en el modo normal y está habilitado de forma predeterminada solo para la interfaz celular.
    - **Estricto Modo**: Determina el estado de la interfaz exclusivamente en función de los resultados de un comando de detección enviado a una IP pública.
- **Comando Track**: El comando ping se utiliza para monitorear el estado de la conexión a la IP de destino y verificar la disponibilidad de la interfaz.
- **IPv4 Track IP**: Cpersonalizar IPv4 Track IP direcciones según sea necesario.

Haga clic en **Opciones de sensibilidad** en la esquina superior derecha.



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



Consejos: Si la red es estable, se recomienda una alta sensibilidad para un cambio rápido en caso de desconexión de la red. Esto es adecuado para escenarios como mirar videos, transmitir en vivo o jugar juegos. Si la red es inestable, se recomienda una sensibilidad baja para evitar cambios frecuentes de red y conexiones fallidas. Esto se aplica a escenarios como la descarga de archivos almacenados en caché.

Nota: Cambiar a alta sensibilidad puede provocar desconexiones ocasionales de la red durante el proceso. Ajústelo con precaución.

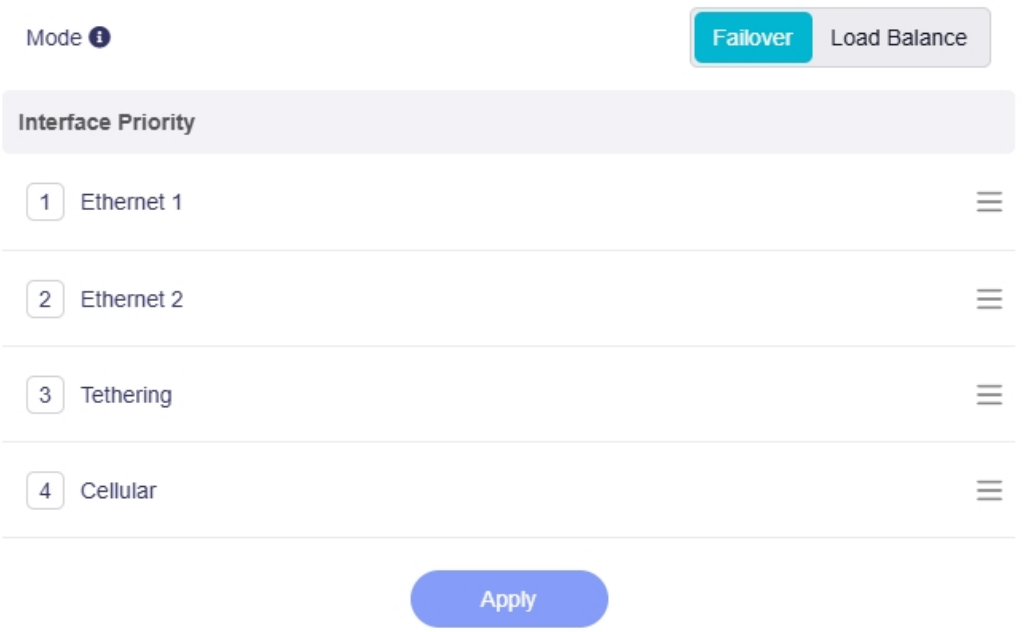
11.1.2 Modo Multi-WAN

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

Conmutación por error

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

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

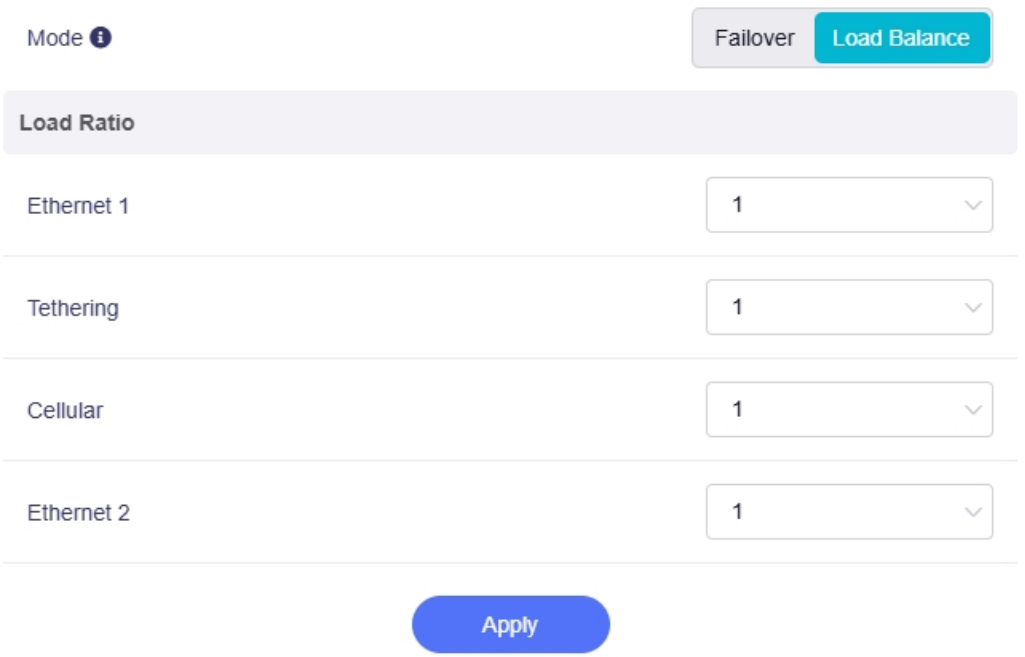


Equilibrio de carga

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

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

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



Personalice la relación de carga según sea necesario. Por ejemplo, si Ethernet 1 tiene un ancho de banda de 100 Mbps, Ethernet 2 tiene 200 Mbps y no hay conexiones Tethering o Cellular activas, establezca las relaciones de carga en 1 para Ethernet 1, 2 para Ethernet 2 y 0 para Tethering y Cellular. Luego, el sistema distribuirá nuevas conexiones a través de estas

interfaces de acuerdo con la proporción 1:2 configurada, lo que significa que Ethernet 1 manejará la mitad de conexiones que Ethernet 2. 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: Conexiones o tráfico existentes No se garantiza que se alineen con la relación de carga. La distribución real se acercará gradualmente a la proporción configurada con un uso prolongado.

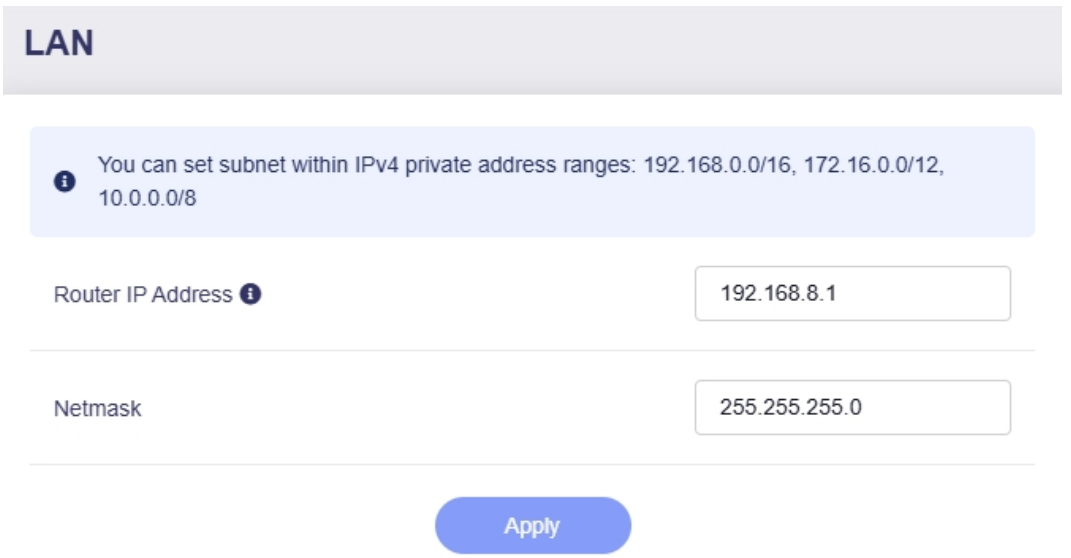
11.2 LAN

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

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

11.2.1 Configuración básica

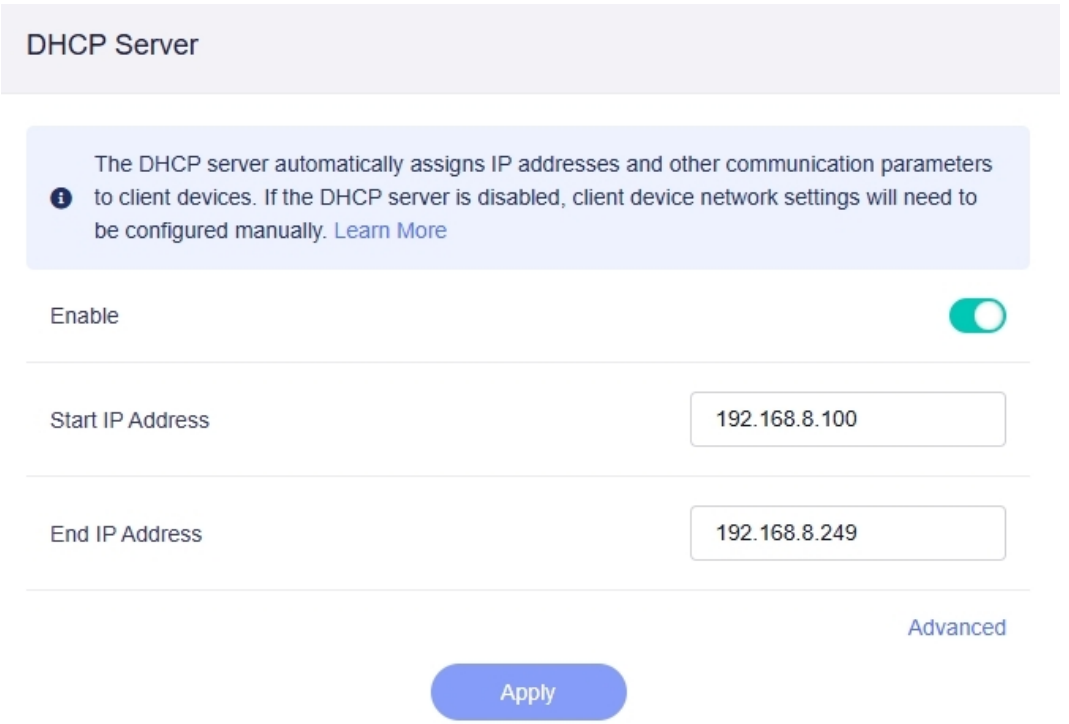
Los ajustes básicos incluyen la dirección IP del enrutador y Máscara de red. Puede configurar la subred dentro de rangos de direcciones privadas IPv4: 192.168.0.0/16, 172.16.0.0/12, 10.0.0.0/8



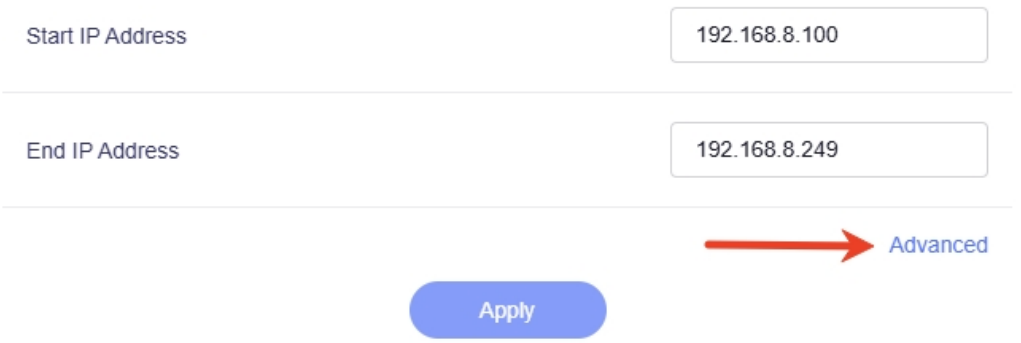
- **Dirección IP del enrutador**: esta es la dirección ingresada en la barra de direcciones de un navegador para acceder al panel de administración del enrutador. Es 192.168.8.1 de forma predeterminada y se puede cambiar si entra en conflicto con la red ascendente.'panel de administración. Es 192.168.8.1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

11.2.2 Servidor DHCP

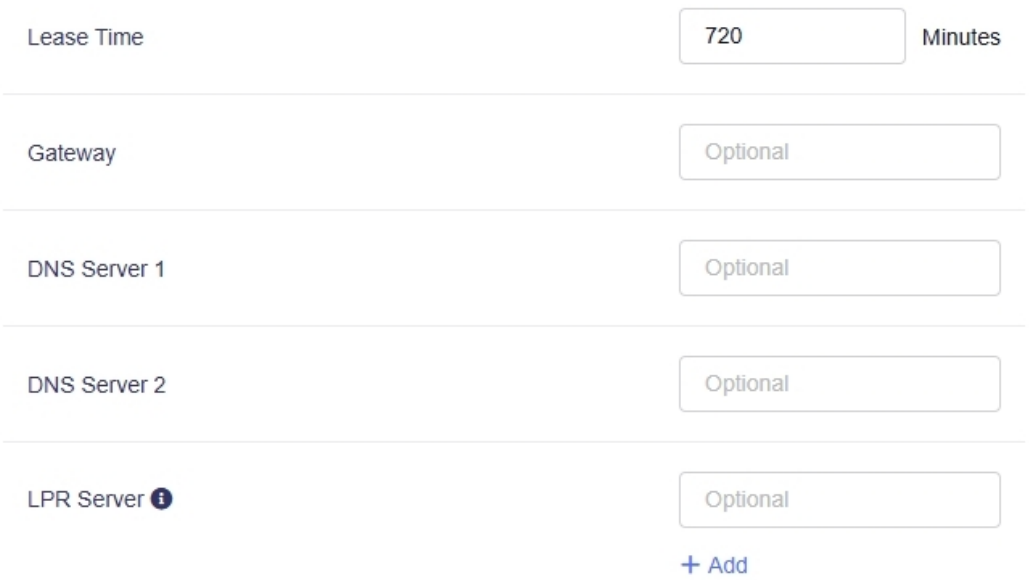
El servidor DHCP asigna automáticamente direcciones IP y otros parámetros de comunicación a cada cliente conectado. El servidor DHCP del enrutador GL.iNet está habilitado de forma predeterminada y el grupo de direcciones IP del servidor DHCP varía de 192.168.8.100 a 192.168.8.249. Puede personalizar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



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



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



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

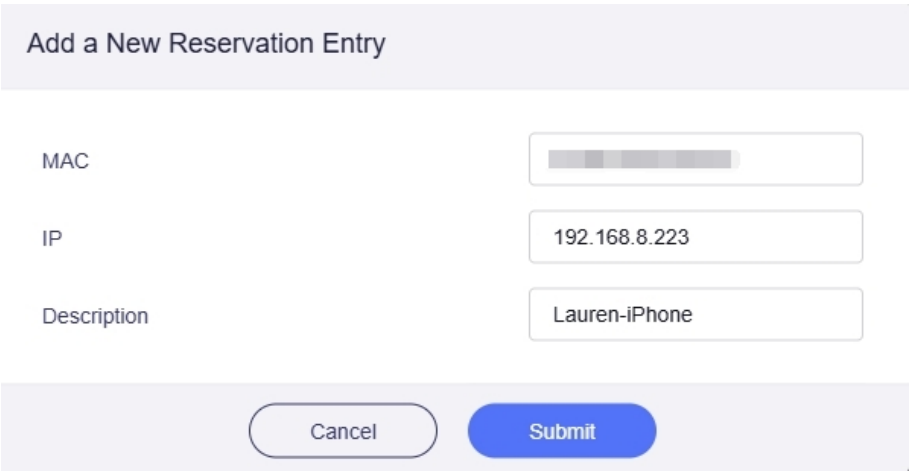
Nota: Si el servidor DHCP está deshabilitado, deberá configurar manualmente la IP estática y otros parámetros de comunicación para cada cliente. Consulte aquí para obtener más detalles.

11.2.3 Reserva de direcciones

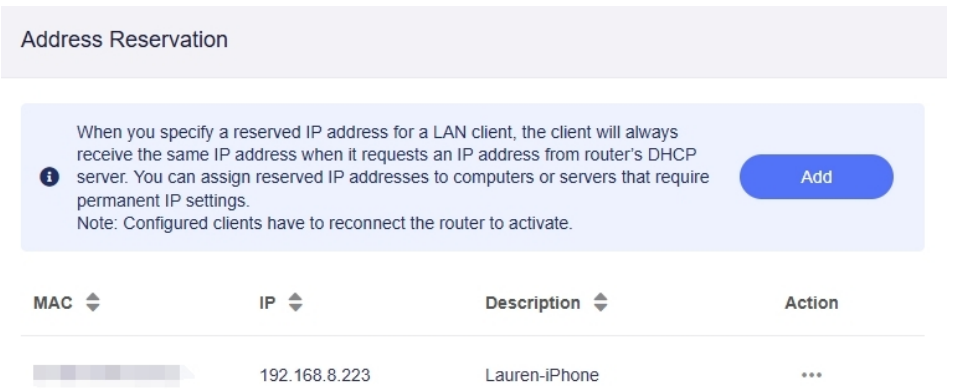
La reserva de dirección le permite especificar una dirección IP fija para un cliente LAN, de modo que el cliente siempre reciba la misma dirección IP cada vez que acceda al servidor DHCP del enrutador. Puede asignar direcciones IP reservadas a computadoras o servidores que requieren configuración IP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

Siga los pasos a continuación para configurar la reserva de dirección según sea necesario.

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



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

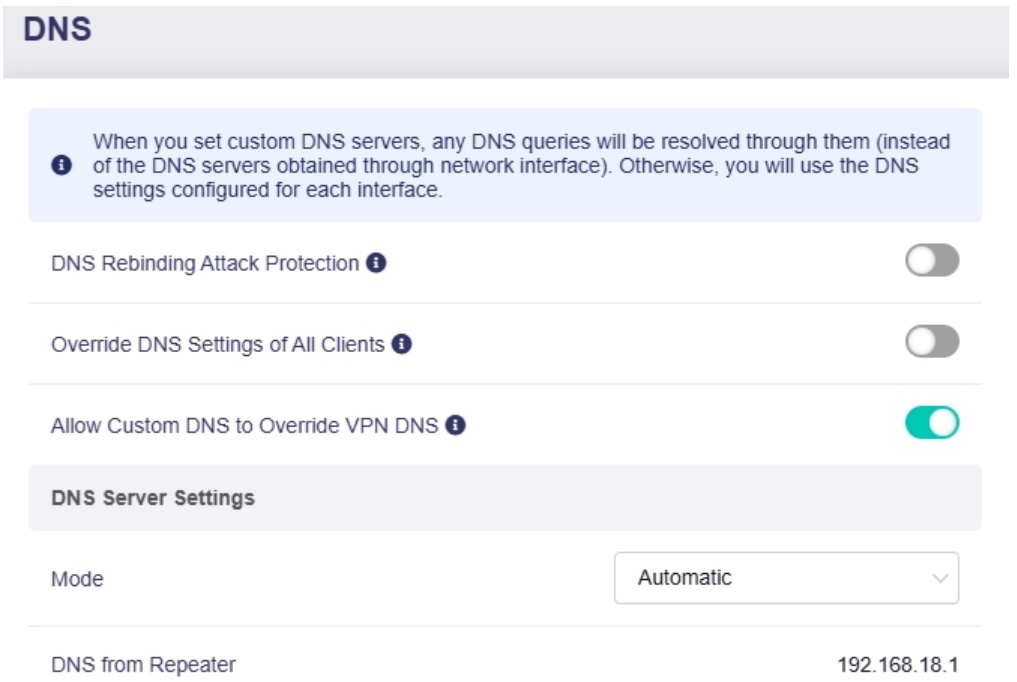


11.3 DNS

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

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

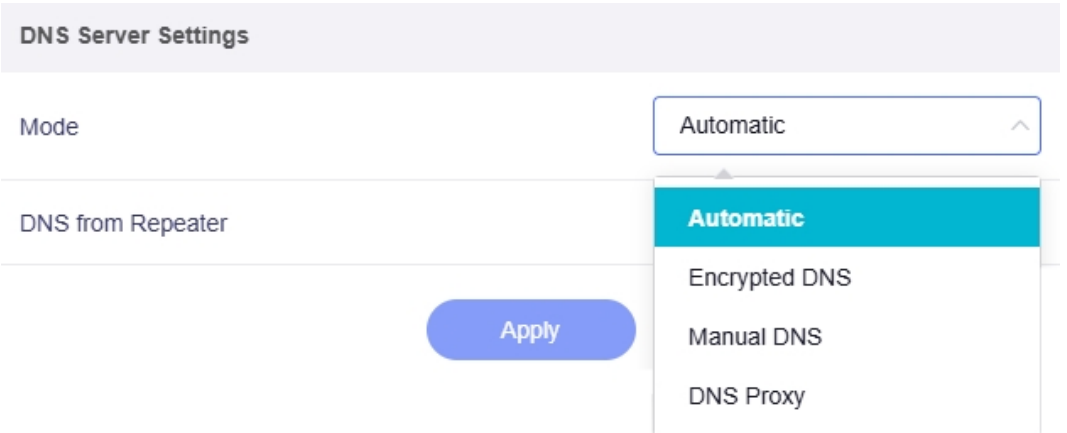
Inicie sesión en el panel de administración web de su enrutador y navegue hasta **RED** > **DNS**. Esta página le permite configurar ajustes relacionados con DNS, incluidas opciones de seguridad, modos de servidor y reglas de prioridad de DNS para diferentes escenarios de red.



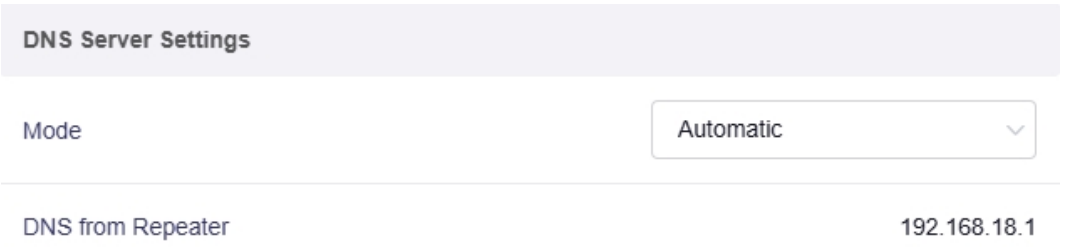
- **Protección contra ataques de vinculación de DNS**: Protege contra ataques de revinculación de DNS al bloquear intentos maliciosos de resolución de DNS. Tenga en cuenta que habilitarlo puede provocar un error en la búsqueda de DNS privada.
- **Anular la configuración de DNS de todos los clientes**: Si está habilitado, todos los dispositivoss será forzado a utilizar los servidores DNS configurados en el enrutador, ignorando su propia configuración DNS original. Permite la configuración de DNS unificada para todos los dispositivos.
- **Permitir que DNS personalizado anule el DNS de VPN**: Cuando está habilitado, si ha configurado DNS personalizado, los paquetes transmitidos a través del túnel VPN utilizarán el DNS personalizado para la resolución, en lugar de los servidores DNS de la conexión VPN. Esto garantiza que sus reglas de resolución DNS personalizadas se apliquen normalmente al usar VPN.

11.3.1 Configuración del servidor DNS

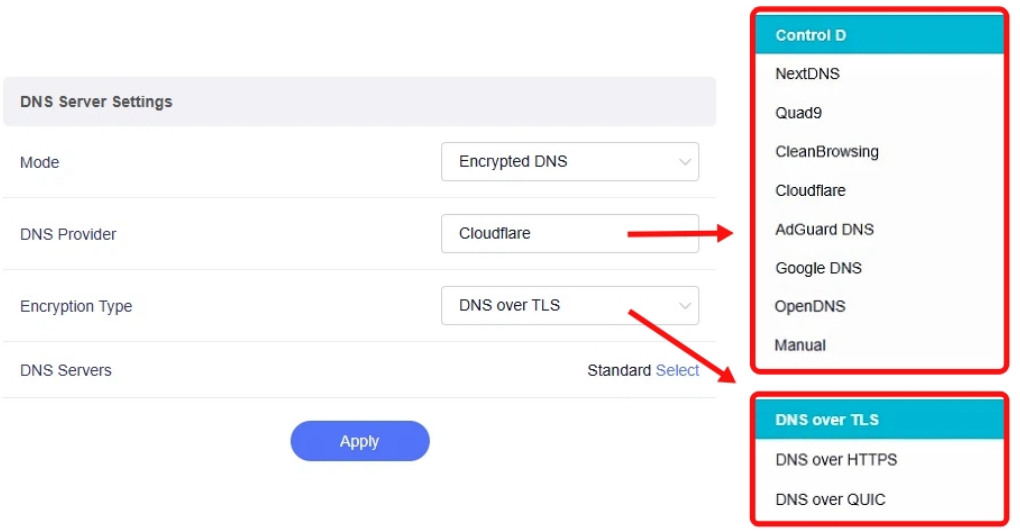
Hay cuatro modos para el servidor DNS: Automático, DNS cifrado, DNS manual y Proxy DNS.



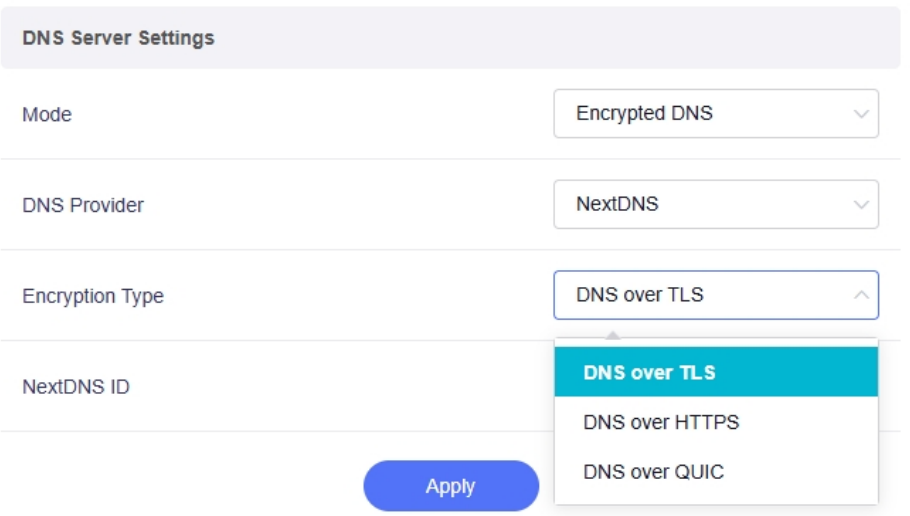
1. **Automático**: cuando se selecciona, el enrutador obtendrá automáticamente las direcciones del servidor DNS de la red ascendente y las aplicará a todos los dispositivos conectados.



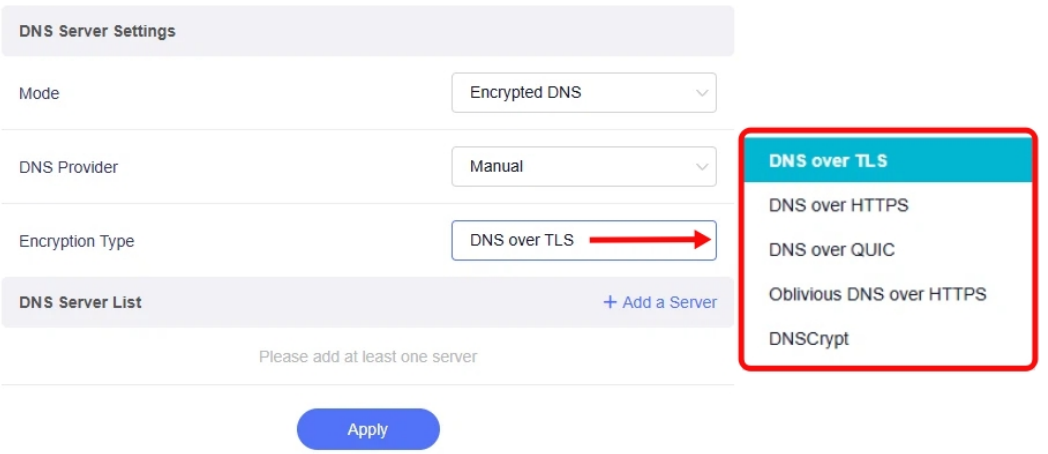
2. **DNS cifrado**: cuando se selecciona, el enrutador utilizará protocolos cifrados para procesar consultas DNS, protegiendo los datos de resolución contra escuchas o alteraciones.
   Admite múltiples proveedores de DNS para el modo DNS cifrado, incluidos Control D, NextDNS, Cloudflare,Quad9, CleanBrowsing,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



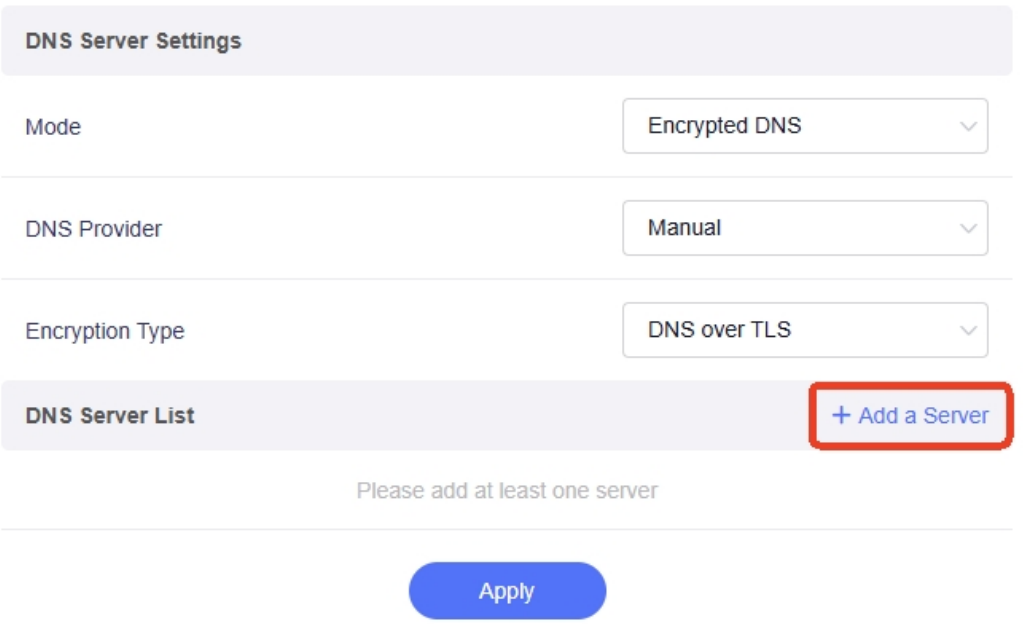
- Si selecciona un proveedor de DNS específico (por ejemplo, NextDNS), elija un tipo de cifrado entre DNS sobre TLS (DoT), DNS sobre HTTPS (DoH) y DNS sobre QUIC (DoQ). Tenga en cuenta que DNS sobre QUIC (DoQ) se introdujo en el firmware v4.9 y solo está disponible cuando se utiliza Control D, NextDNS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



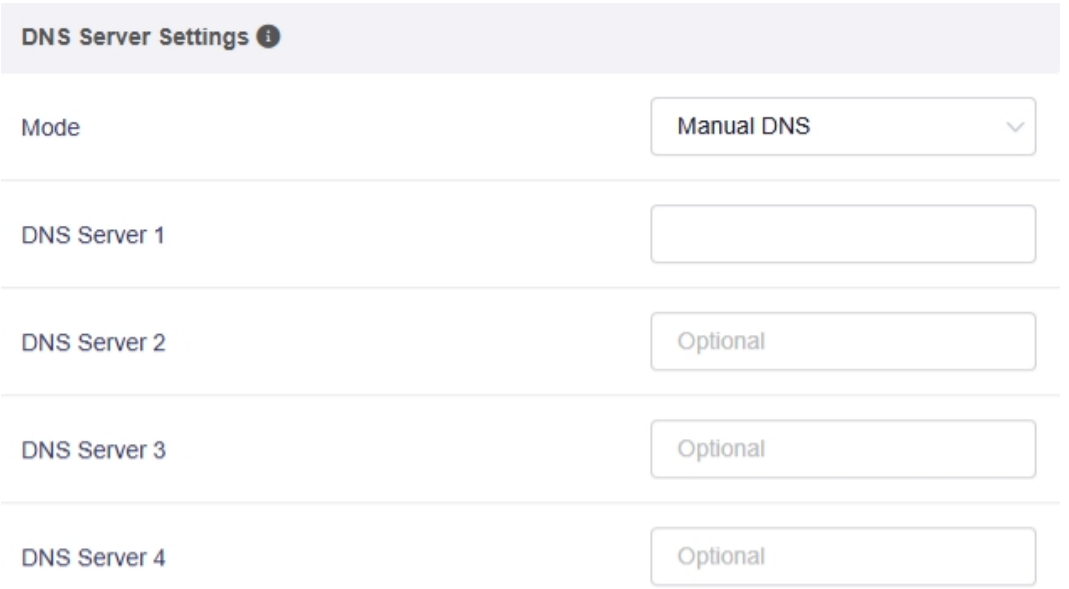
- Si selecciona Manual como proveedor de DNS, elija un tipo de cifrado entre DNS sobre TLS (DoT), DNS sobre HTTPS (DoH), DNS sobre QUIC (DoQ), DNS ajeno a HTTPS y DNSCrypt.



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

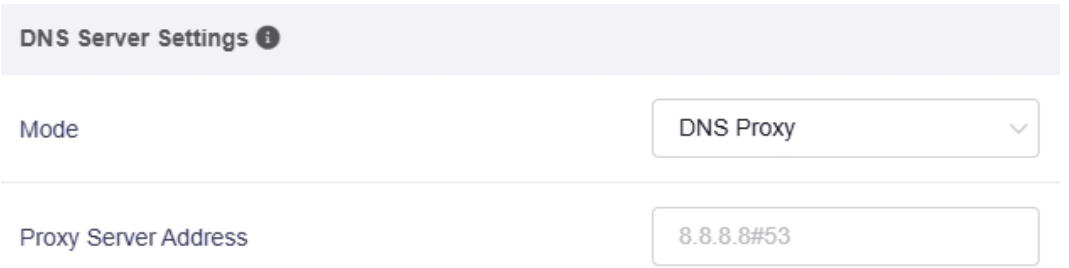


3. **DNS manual**: cuando se selecciona, puede personalizar los servidores DNS de su enrutador. Haga clic en Servidor DNS 1 y elija un servidor DNS de la lista desplegable. Los campos DNS restantes se actualizarán automáticamente.



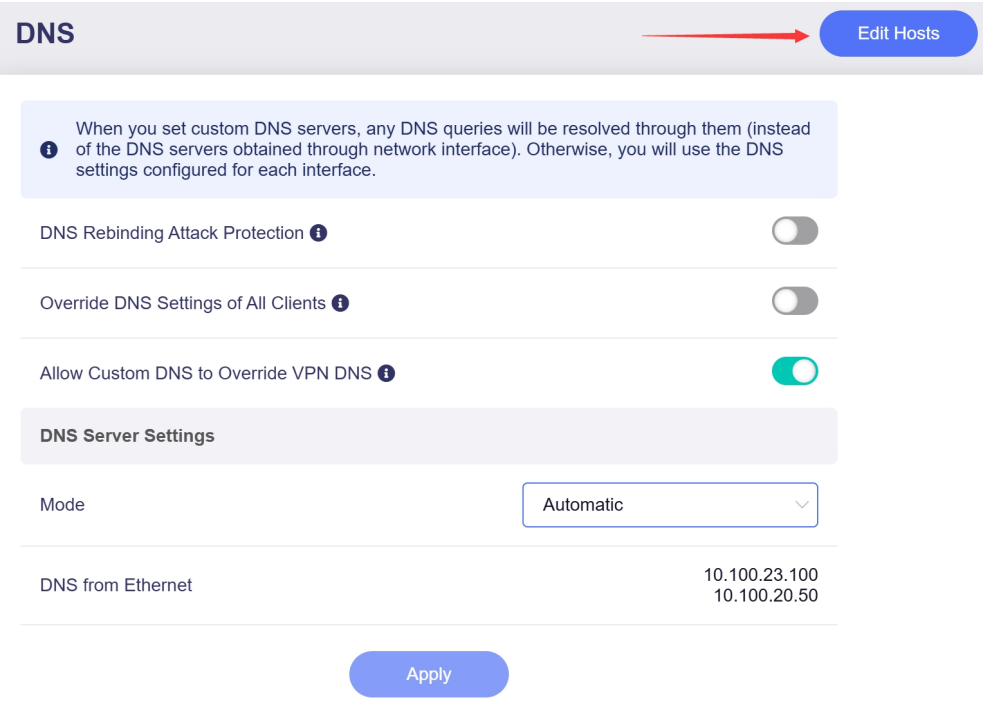
Nota: si necesita usar direcciones IPv6 para DNS manual, habilite IPv6 en su enrutador primero.

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

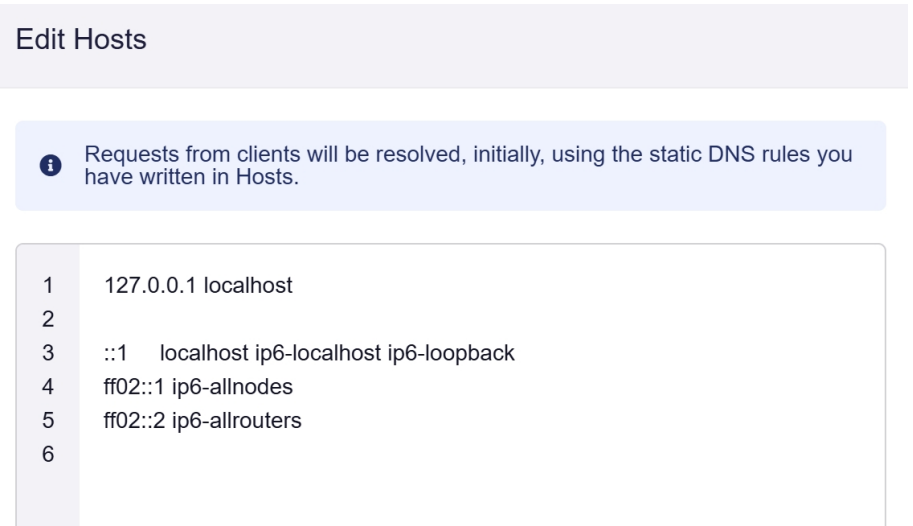


11.3.2 Editar hosts

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

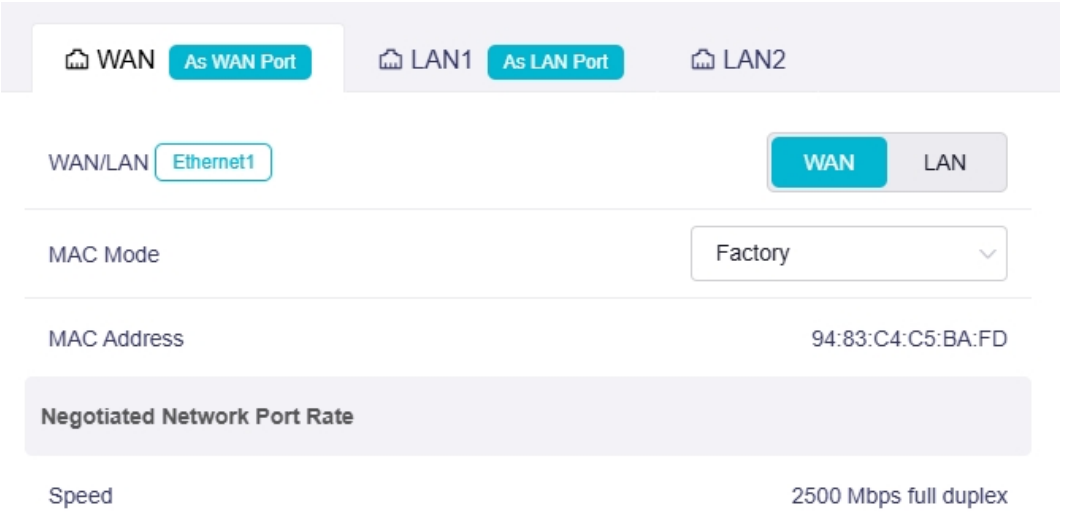


Las solicitudes de los clientes se resolverán preferentemente utilizando las reglas de DNS estáticas escritas aquí, lo que le permitirá asignar manualmente direcciones IP a nombres de host (por ejemplo, las entradas predeterminadas como 127.0.0.1 localhost para loopback local) para un control personalizado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

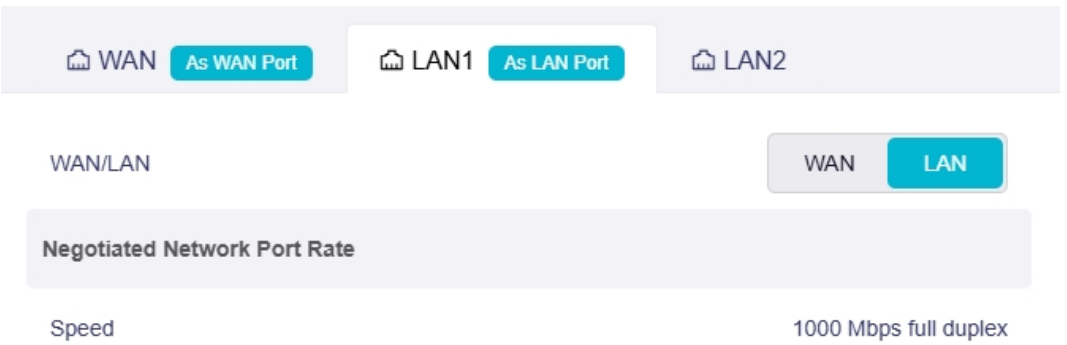


11.4 Puerto Ethernet

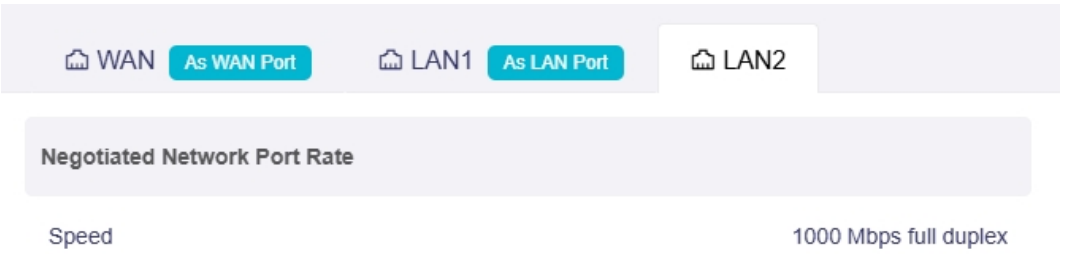
Inicie sesión en el panel de administración web de su enrutador' y navegue hasta **RED** > **Ethernet Puerto**. Esta página le permite administrar los puertos Ethernet del enrutador'. La sección **WAN** muestra la función del puerto (WAN o LAN), dirección MAC y tarifa negociada.



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



La sección **LAN 2** muestra la tarifa negociada del puerto LAN.



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

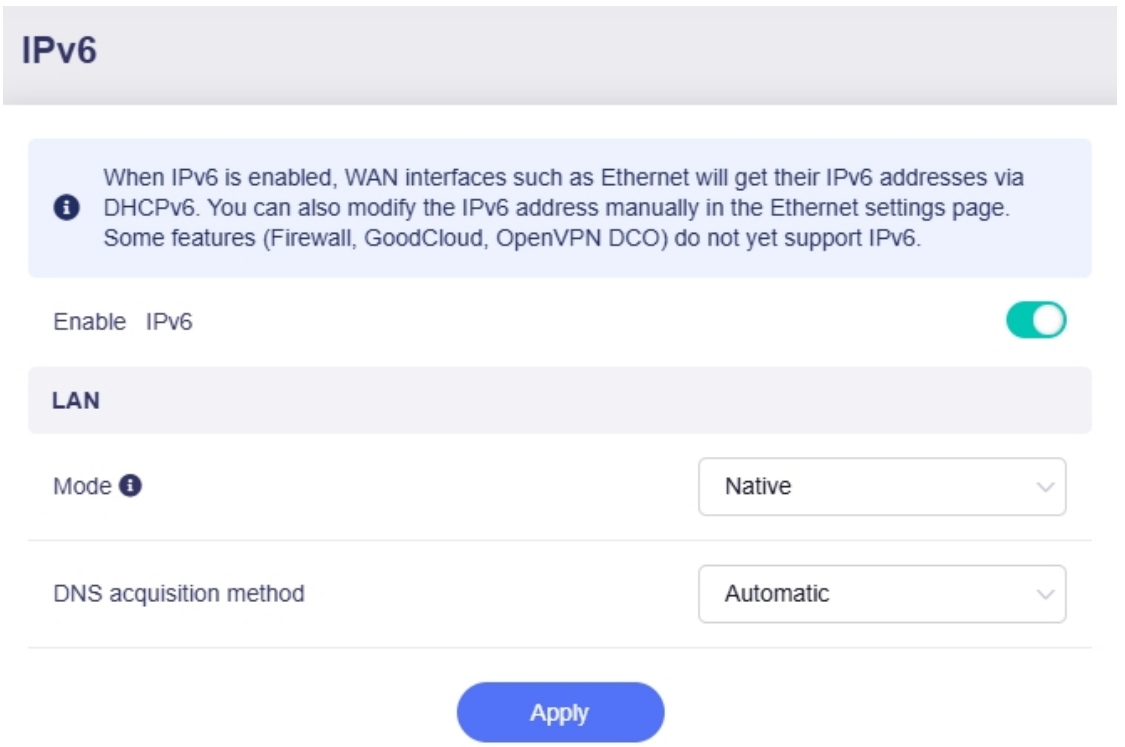
11.5 IPv6

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.

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

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



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

11.5.2 Método de obtención de DNS

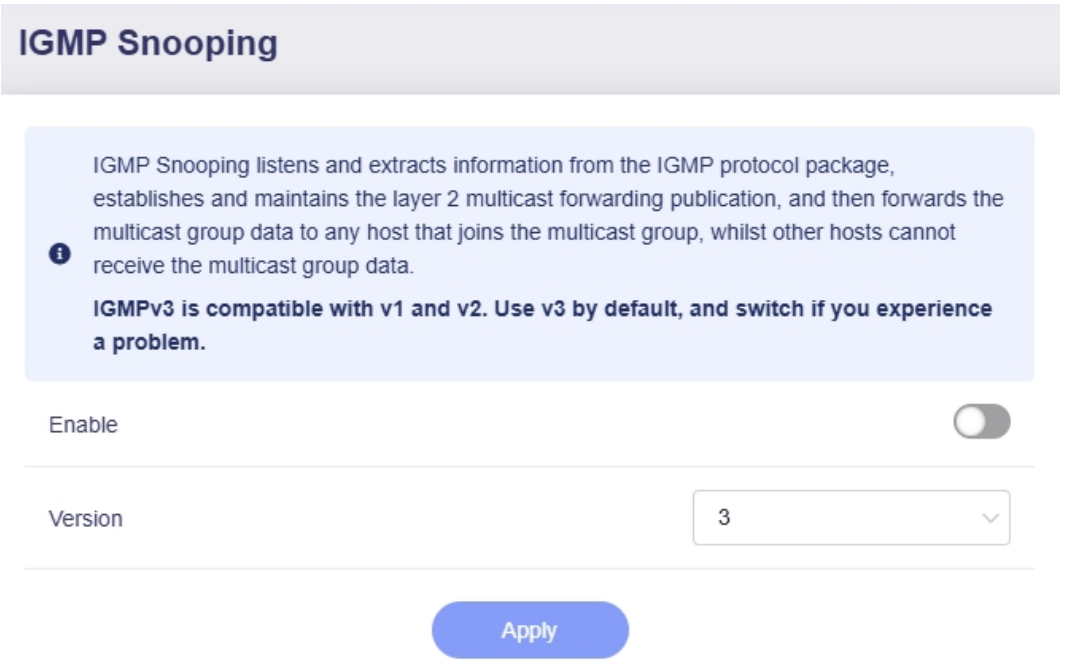
Determina cómo el enrutador obtiene las direcciones del servidor DNS IPv6. Hay dos opciones: Automático y Manual.

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

11.6 Inspección IGMP

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

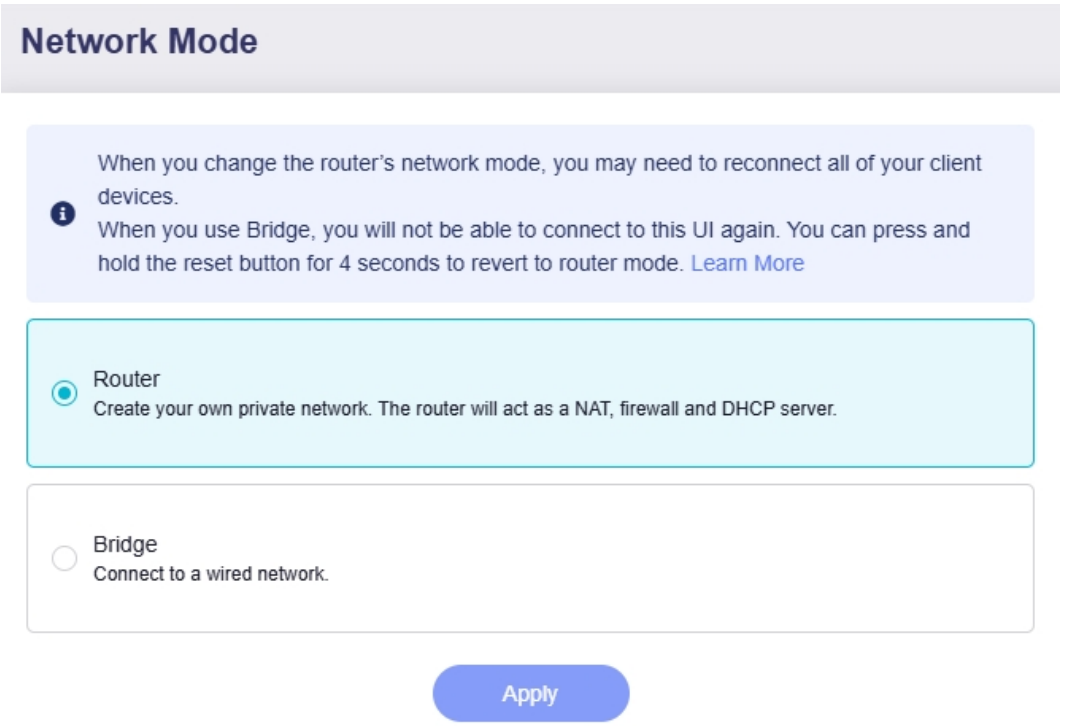
Inicie sesión en el panel de administración web de su enrutador' y navegue hasta **RED** > **Inspección IGMP**. Puede habilitar para usar la función de multidifusión en su enrutador según sea necesario.



11.7 Modo de red

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

Inicie sesión en su enrutador'panel de administración web y navegue hasta **RED** > **Modo de red**. Puede cambiar el modo de red de su enrutador. Brume 3 soportas dos modos: enrutador y modo puente.



- **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.
- **Puente**: permite que el enrutador se conecte a una red cableada y funcione como un puente entre dispositivos de red. En este modo, el enrutador funciona esencialmente como un conmutador, reenviando datos entre dispositivos conectados sin realizar

servicios NAT, firewall o DHCP. Esto permite una comunicación fluida entre dispositivos en la misma red al actuar como un simple punto de conexión en lugar de una puerta de enlace de red.

Nota:

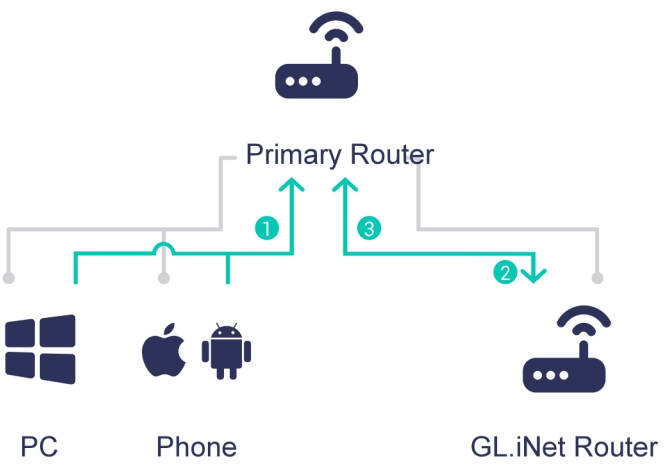
1. Cuando modo de red se cambia, dispositivos necesita volver a conectarse al enrutador para garantizar una estabilidad conexión.
2. **En modo puente, no podrá acceder al panel de administración web usando la dirección IP original**. En su lugar, debe iniciar sesión en el enrutador ascendente para encontrar la dirección IP que ha asignado a este enrutador y luego usar esta dirección IP para acceder al panel de administración web. Si no tiene acceso al enrutador ascendente, presione y mantenga presionado el botón de reinicio durante 4 segundos para revertirlo al modo de enrutador predeterminado.
3. **En el modo Puente, las siguientes funciones no estarán disponibles**: Control de acceso (lista de permitidos y lista de bloqueo), AstroWarp, VPN, AdGuard Home, control parental, ZeroTier, Tailscale, reenvío de puertos, Multi-WAN, servidor DHCP, reserva de direcciones, DNS, puerto Ethernet, IPv6, puerta de enlace directa, vigilancia IGMP, Aceleración de red, configuración de NAT.

11.8 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 reemplazar ni volver-configurarlo. Al conectar el enrutador GL.iNet al enrutador principal mediante un cable Ethernet, los usuarios pueden agregar funciones avanzadas a la infraestructura de red existente, por ejemplo:

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

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



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

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

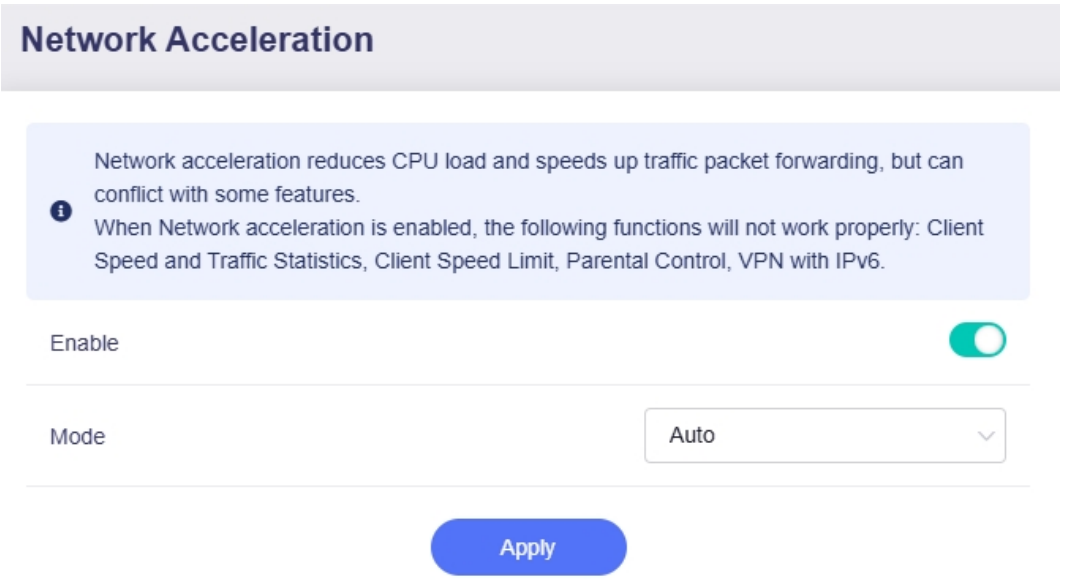
- **Glíneas verdes** representan la ruta de transmisión de datos secuencial cuando La puerta de enlace directa está activa y las flechas numeradas indican el orden del flujo de tráfico:
  1. El tráfico de los dispositivos cliente se enruta primero al enrutador principal;
  2. El enrutador principal reenvía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

Puede habilitar Dentrada Gpara todos o dispositivos específicos conectado a su enrutador principal. Consulte este enlace para obtener más instrucciones.

11.9 Aceleración de red

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

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



- **Auto**: cambia automáticamente entre los dos modos de aceleración según el uso real.
- **Aceleración de hardware**: este modo generalmente funciona en Ethernet y Repetidor (este último no está disponible en Brume 3). Descarga tareas de red de alta frecuencia (por ejemplo, NAT, reenvío de paquetes, verificación de suma de comprobación) a hardware dedicado como NPU o chips HWNAT. Funciona específicamente en conexiones Ethernet (WAN/LAN por cable) y repetidoras, sobresaliendo en estos escenarios con rutas fijas y reglas simples para ofrecer alto rendimiento, baja latencia y carga mínima de CPU para la transmisión de datos a velocidad de cable.
- **Aceleración de software**: este modo funciona en Celular. Se basa en la CPU general de un enrutador emparejada con núcleos o controladores optimizados (por ejemplo, SWNAT). Funciona con acceso celular (4G/5G), normalmente el escenario principal donde la aceleración de hardware no está disponible, y ofrece una gran compatibilidad y soporte para protocolos complejos. Si bien es flexible, puede afectar los cuellos de

botella de la CPU bajo cargas de gran ancho de banda, especialmente cuando se ejecutan funciones avanzadas como DPI, QoS o reenvío de puertos.

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

Capítulo 12

Control de flujo

Este capítulo presenta funciones de control de flujo y proporciona herramientas dedicadas para el tráfico de red y la gestión de contenido.

12.1 Motor DPI

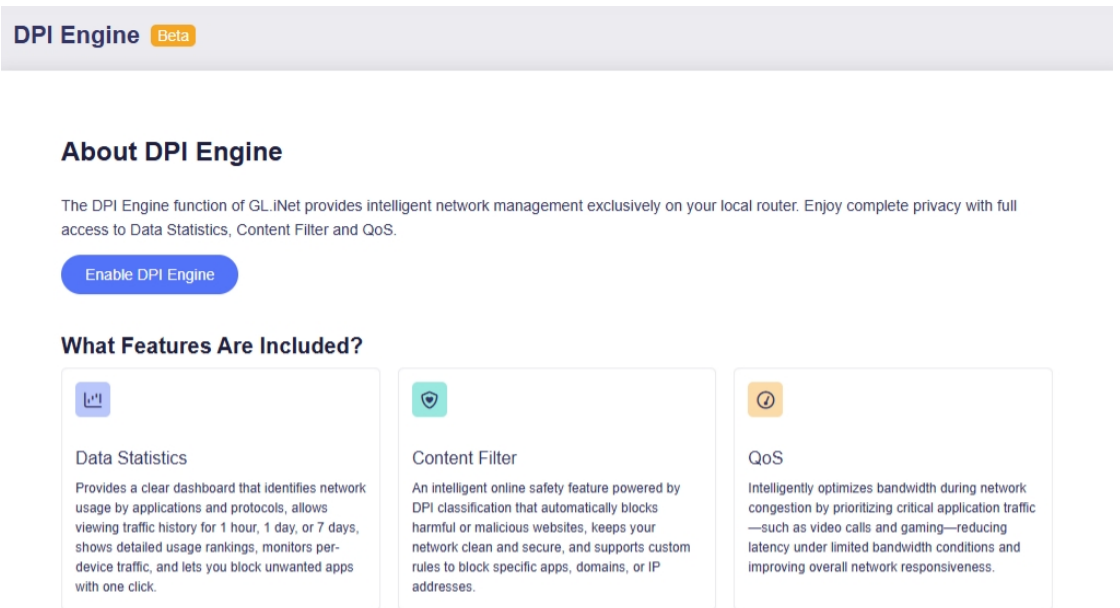
DPI (Inspección profunda de paquetes) es una tecnología central para la gestión inteligente de redes. A diferencia de los enrutadores tradicionales que solo identifican las direcciones de origen y destino, DPI realiza un análisis en profundidad de las cargas útiles de los paquetes e identifica con precisión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

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

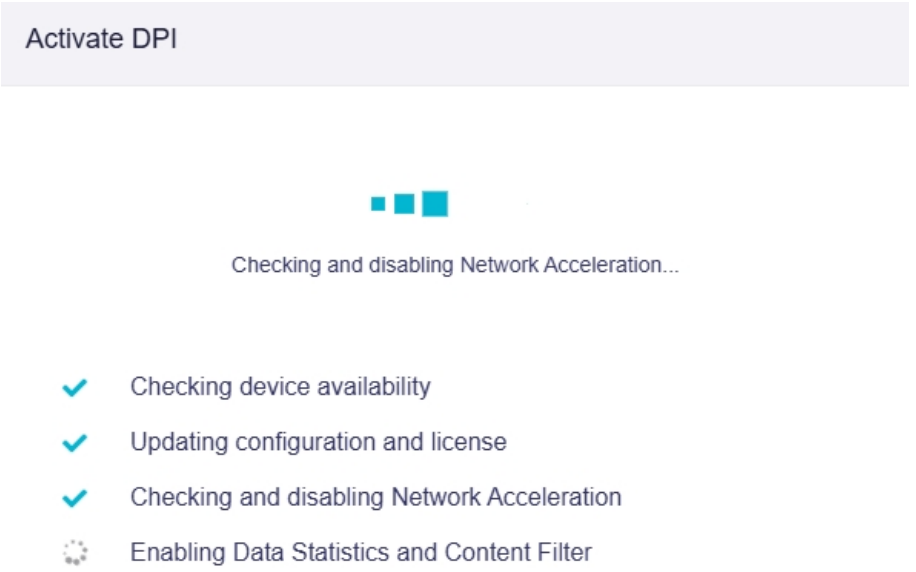
Nota:

1. Cuando el enrutador está en modo Drop-in Gateway, las funciones DPI (incluidas estadísticas de datos, Content Filter y QoS) y SQM no tendrán efecto.
2. Cuando DPI está habilitado, la aceleración de red se deshabilitará automáticamente para garantizar un rendimiento estable.

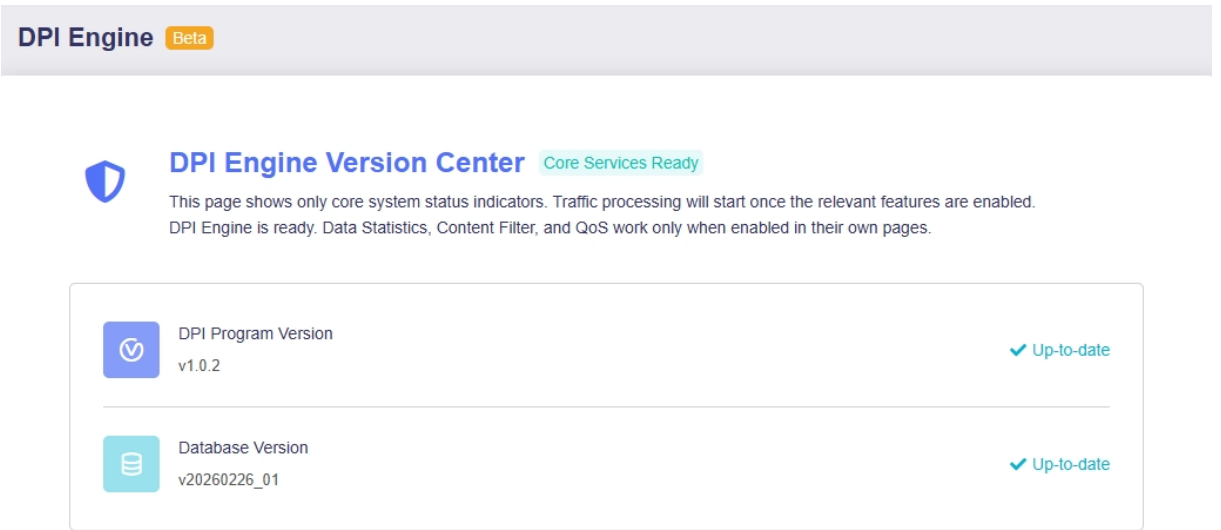
Inicie sesión en el panel de administración web del enrutador' y navegue hasta **FLOW. CONTROL** > **Motor DPI**. Haga clic en **Habilitar motor DPI**.



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



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



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

12.2 Estadísticas de datos

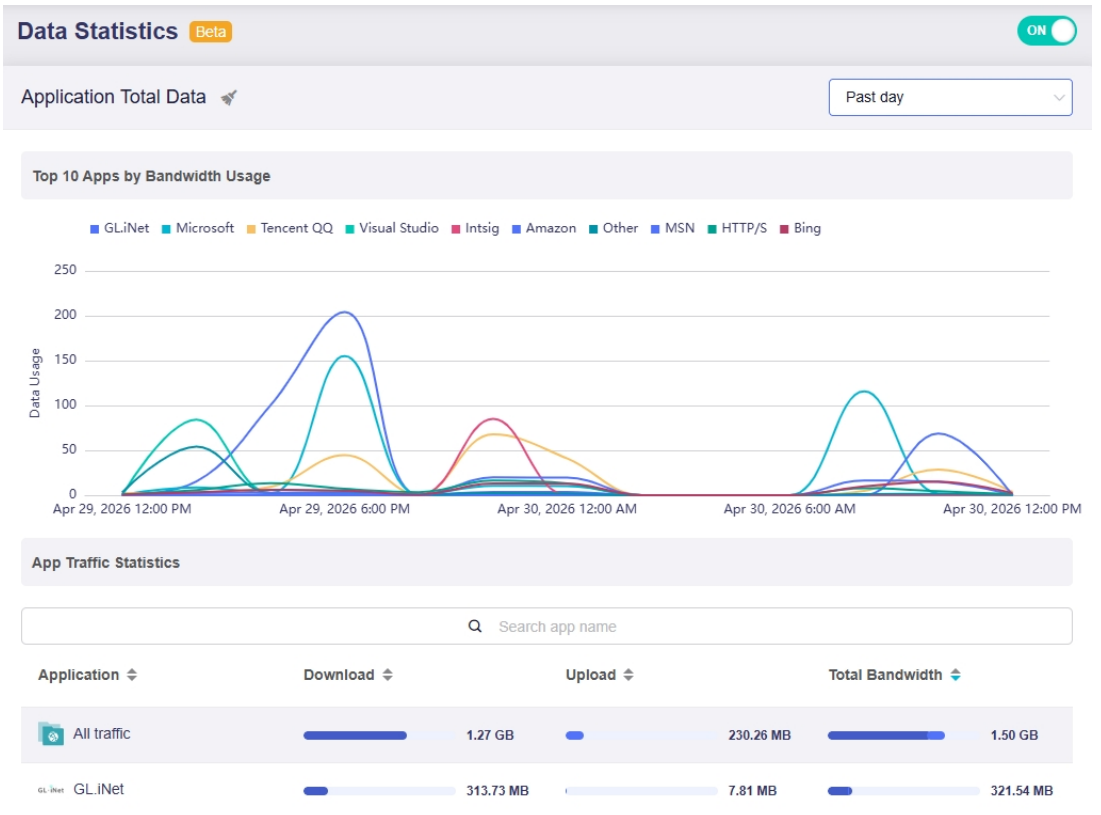
Las estadísticas de datos proporcionan un panel de tráfico intuitivo que identifica el uso de la red por aplicación y protocolo. Admite la visualización de tendencias históricas de 1-hora, 1-día y 7-día, muestra clasificaciones de uso, monitorea el tráfico por-dispositivo y permite bloquear con un solo-el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

Nota:

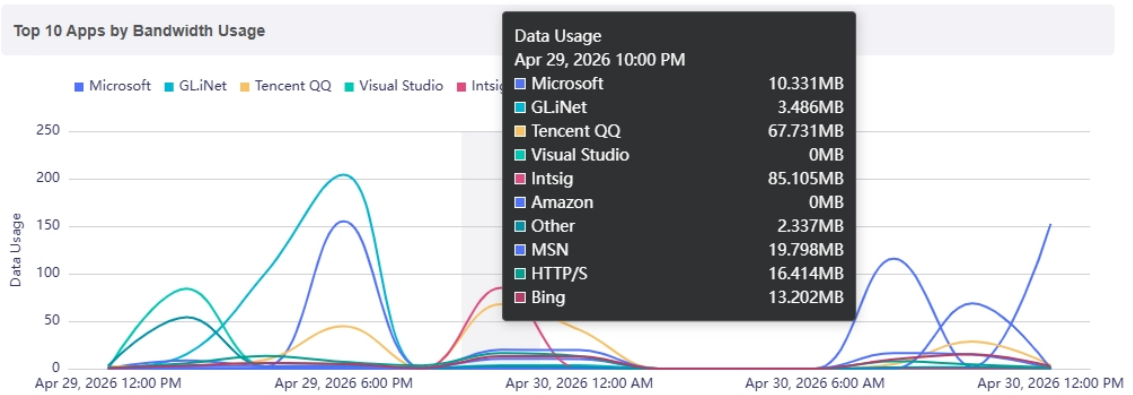
1. Las estadísticas de datos no tendrán efecto cuando el enrutador esté en modo de puerta de enlace directa.
2. Las estadísticas de datos no pueden funcionar con la aceleración de red. Al habilitar las estadísticas de datos, se deshabilitará automáticamente la aceleración de la red para garantizar un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

12.2.1 Configuración rápida

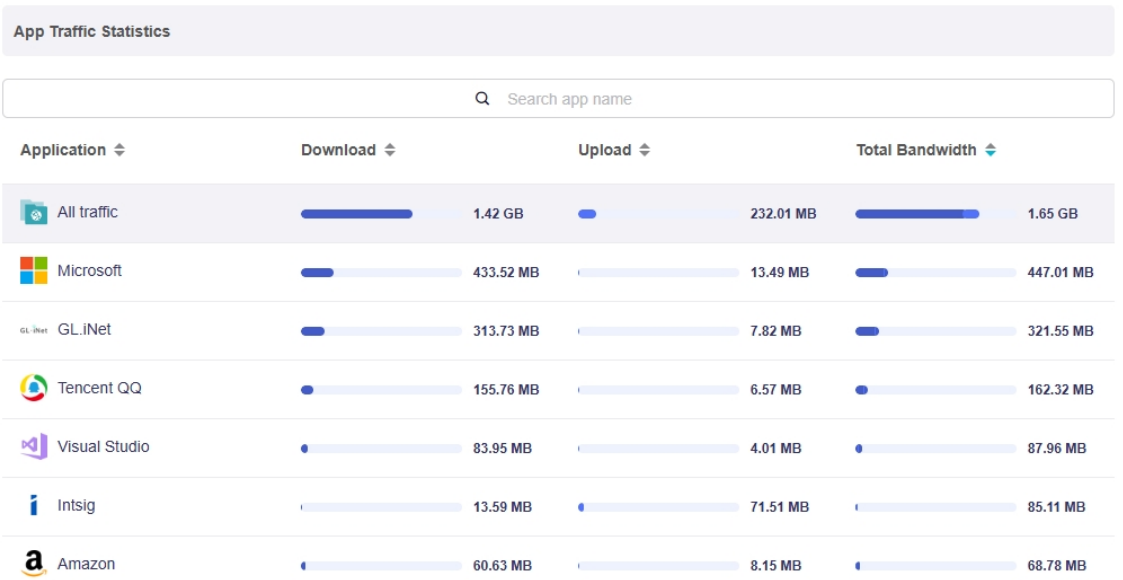
Inicie sesión en el enrutador'panel de administración web y navegue hasta **CONTROL DE FLUJO** > **Estadísticas de datos**. Mueva el interruptor en la esquina superior derecha para ver los **Datos totales de aplicaciones**.



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



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

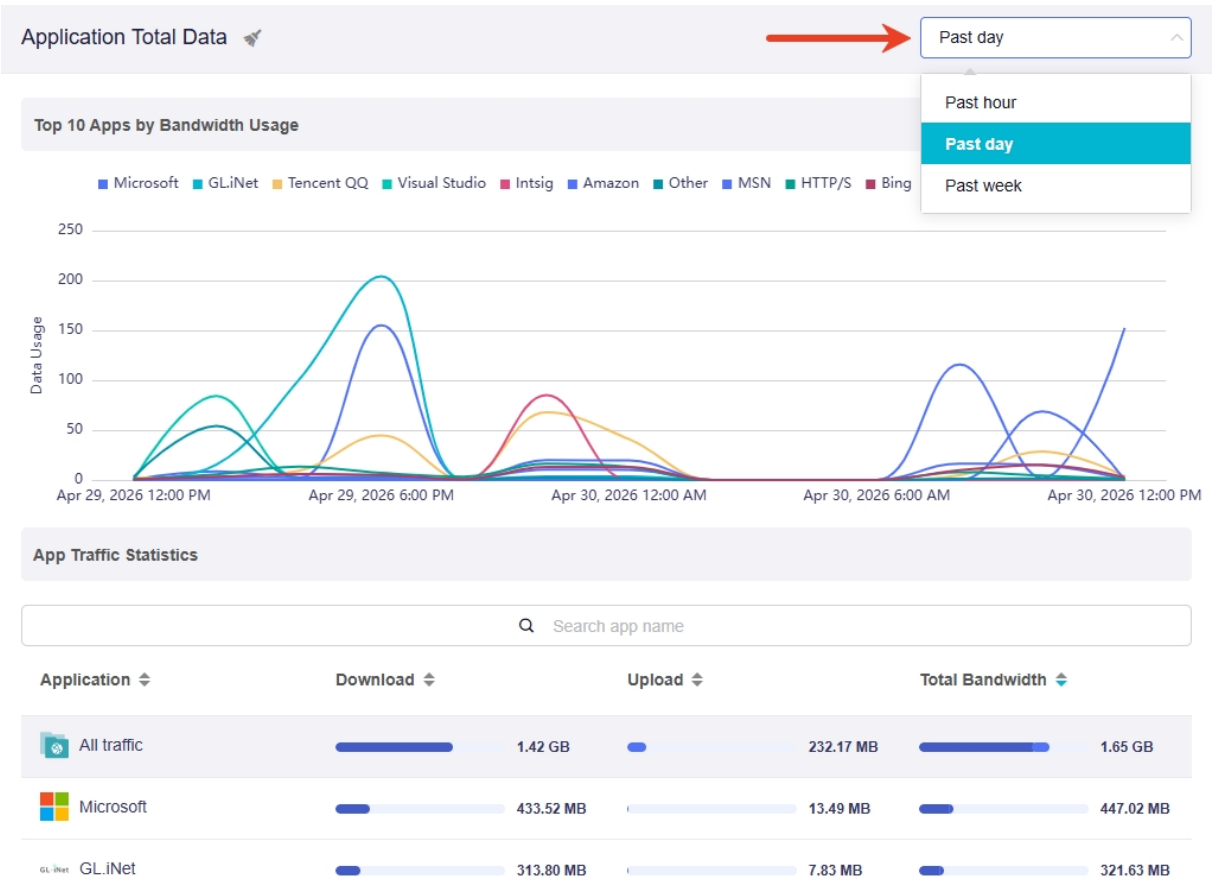


12.2.2 Reglas de almacenamiento de datos

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

12.2.3 Cambiar el intervalo de tiempo

Puede cambiar el rango de tiempo entre Hora pasada, Día pasado y Semana pasada si es necesario.

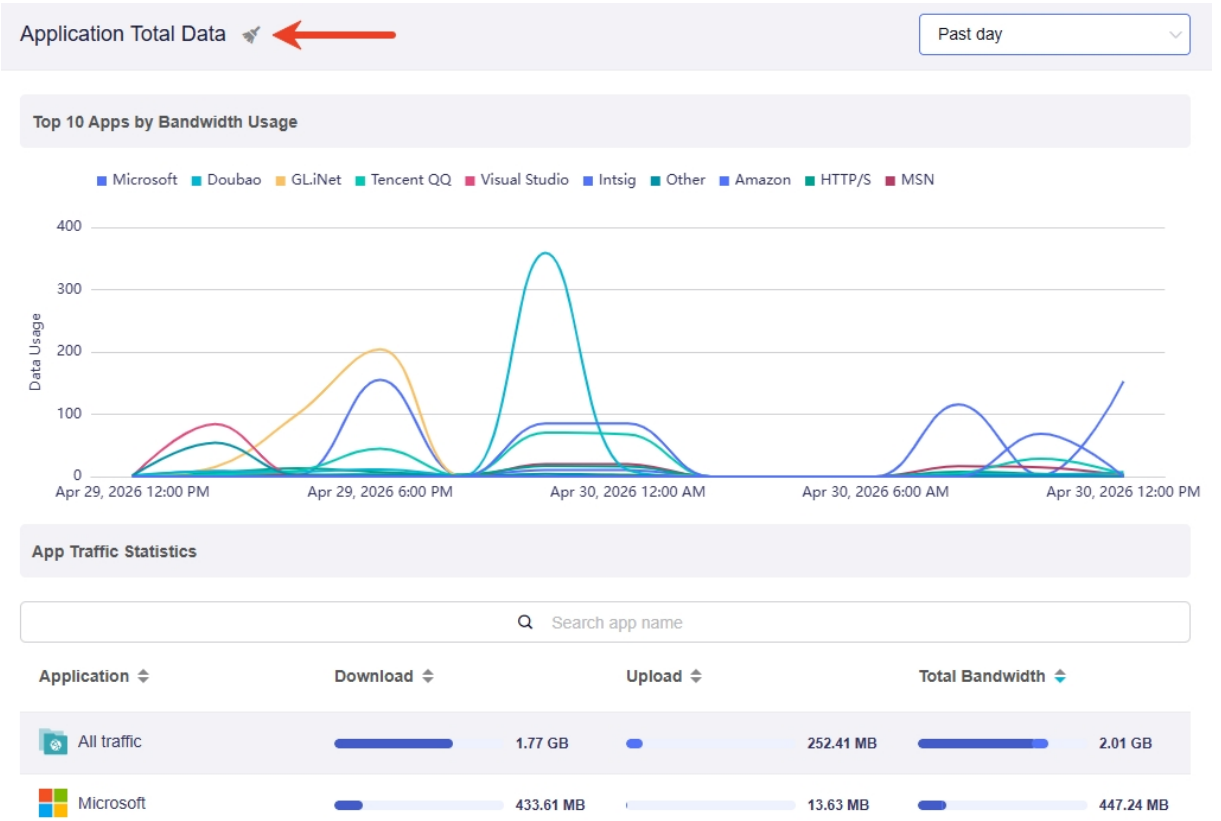


El rango de tiempo que elija determina cómo se muestran los datos:

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

12.2.4 Borrar estadísticas

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



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

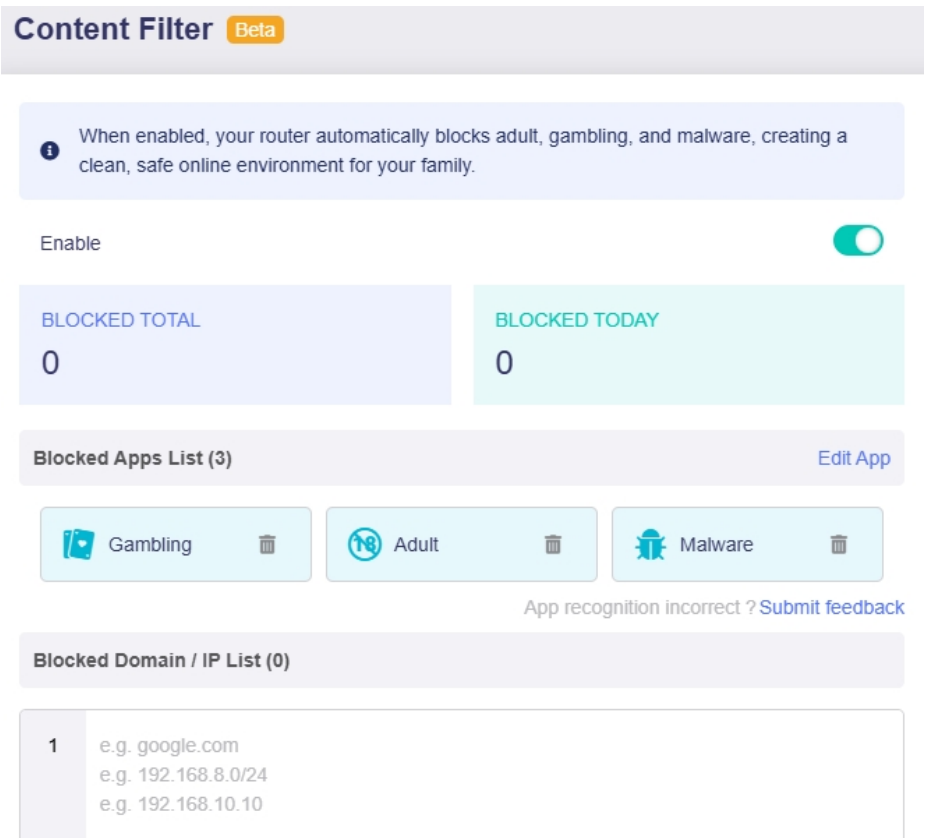
12.3 Filtro de contenido

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

Nota:

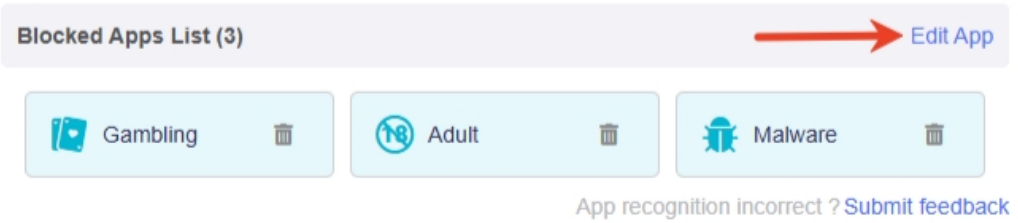
1. El filtro de contenido no tendrá efecto cuando el enrutador esté en modo Drop-in Gateway.
2. El filtro de contenido no puede funcionar con la aceleración de red. Al habilitar el filtro de contenido, se deshabilitará automáticamente la aceleración de red para garantizar un rendimiento estable.

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

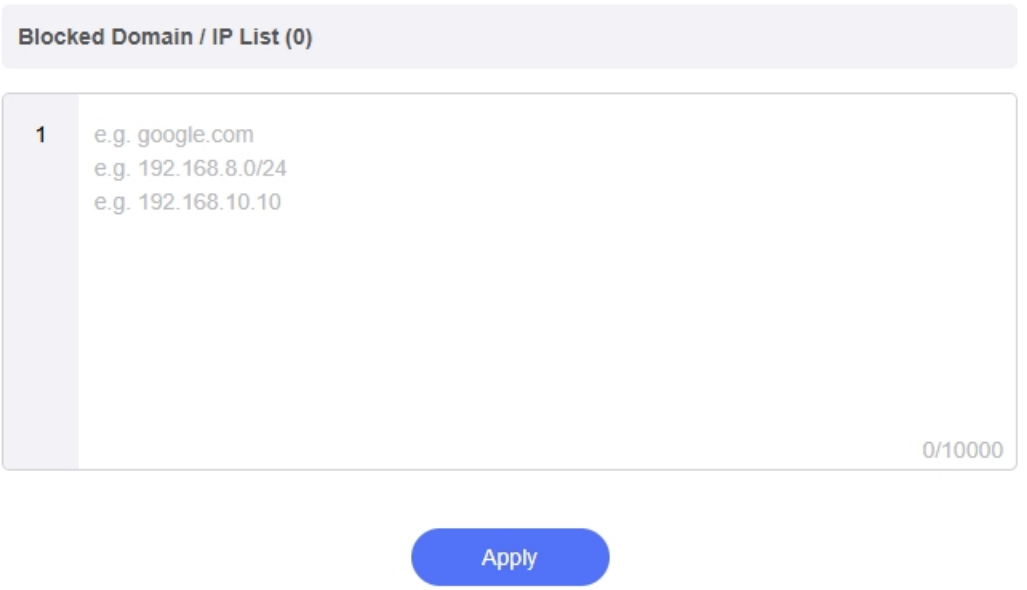


Esta página consta de dos partes:

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



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



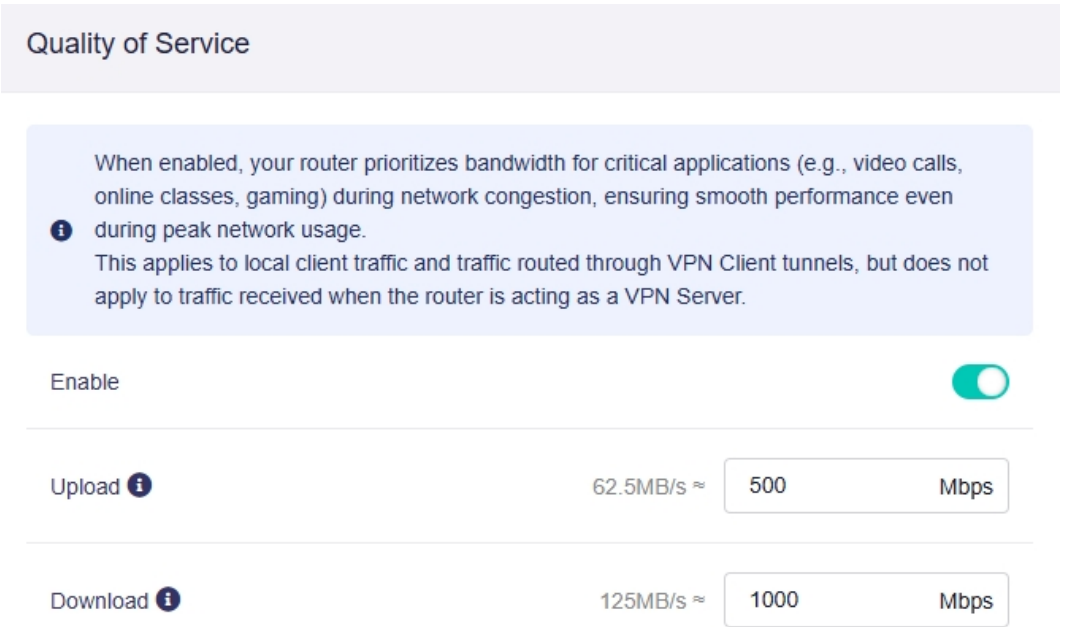
12.4 Calidad de servicio (QoS)

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

Nota:

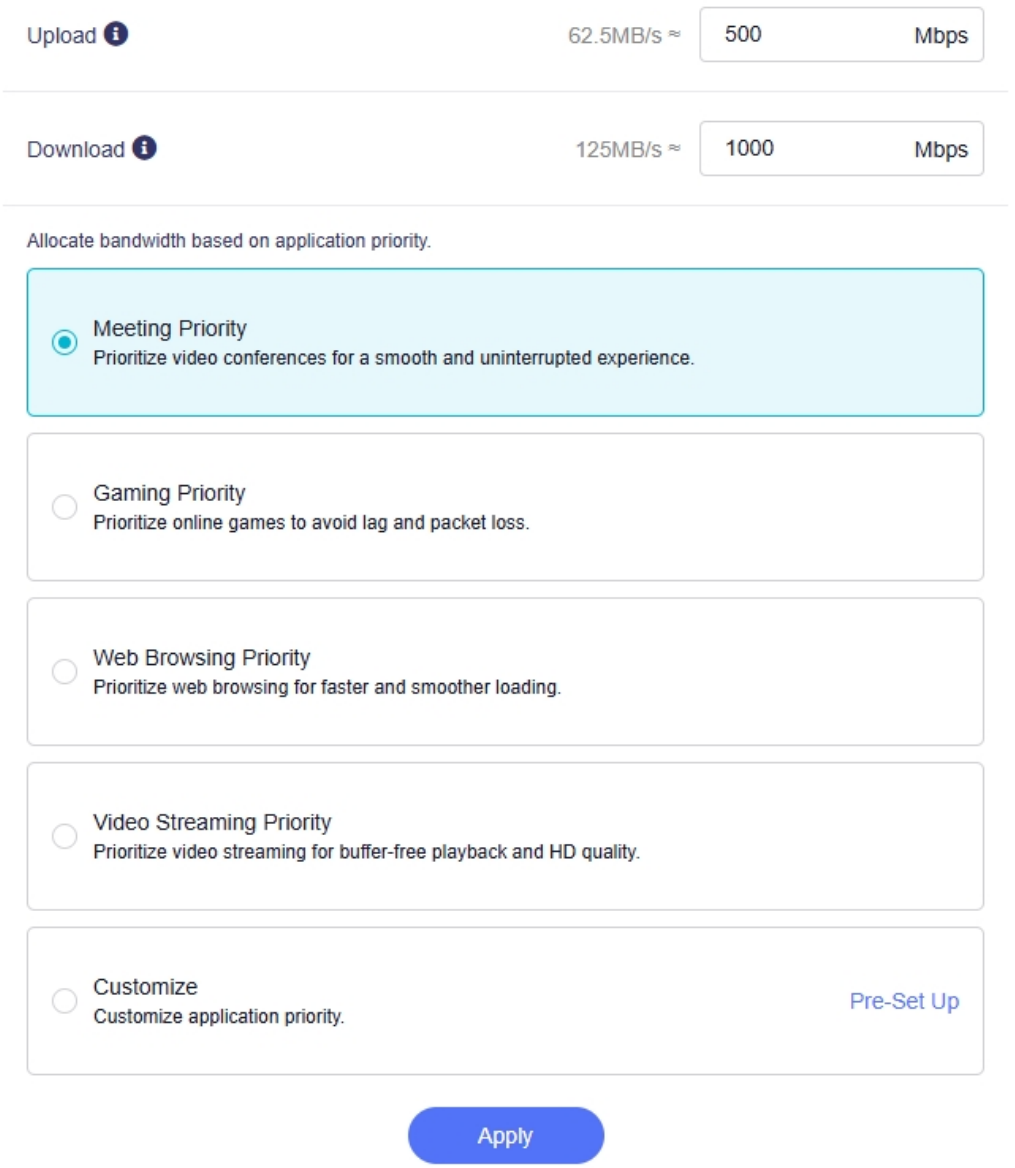
1. Esta característica solo afecta el tráfico que pasa a través del enrutador cuando funciona como puerta de enlace, incluido el tráfico de clientes locales y el tráfico de clientes VPN. No se aplica al tráfico entrante cuando el enrutador actúa como servidor VPN.
2. QoS no tendrá efecto cuando el enrutador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

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



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

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



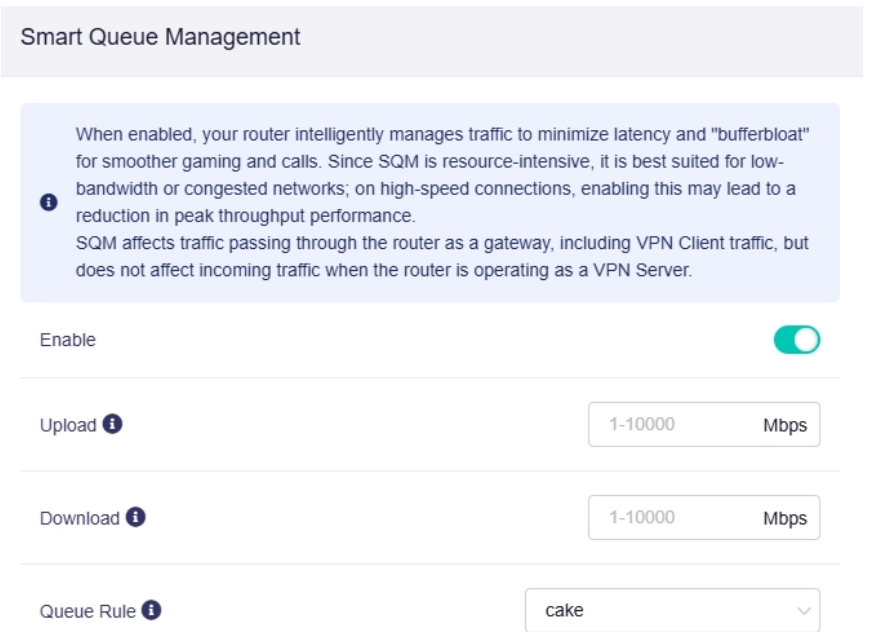
12.5 Gestión inteligente de colas (SQM)

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

Nota:

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

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



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

- **pastel**: configuración de tráfico inteligente y automática con control de latencia general superior (recomendado).
- **fq_codel**: cola justa, sencilla y eficiente con reducción de latencia básica.

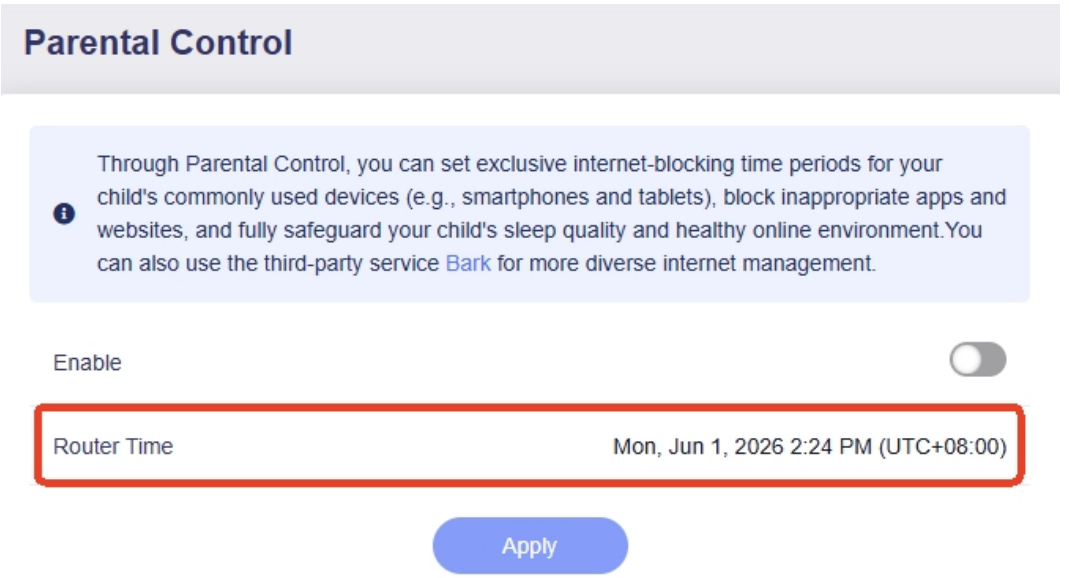
Consejo: una diferencia entre la configuración de QoS y SQM es que la QoS le permite establecer las prioridades de la aplicación, con el el enrutador asigna el ancho de banda en consecuencia; mientras que el SQM permite seleccionar una regla de cola.

12.6 Control parental

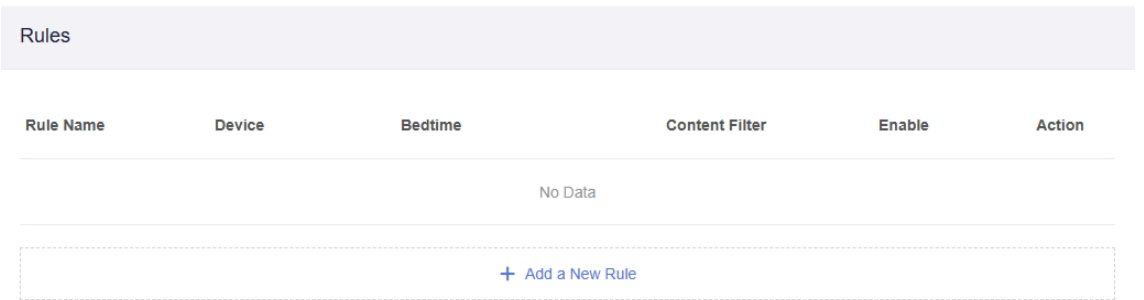
El control parental es una forma de mantener a los niños seguros en línea bloqueando sitios web inapropiados y limitando el tiempo que usan los dispositivos. Ayuda a prevenir el acceso a contenido dañino, administrar el tiempo de pantalla y garantizar que los niños usen Internet de manera responsable.

Siga los pasos a continuación para configurar su control parental.

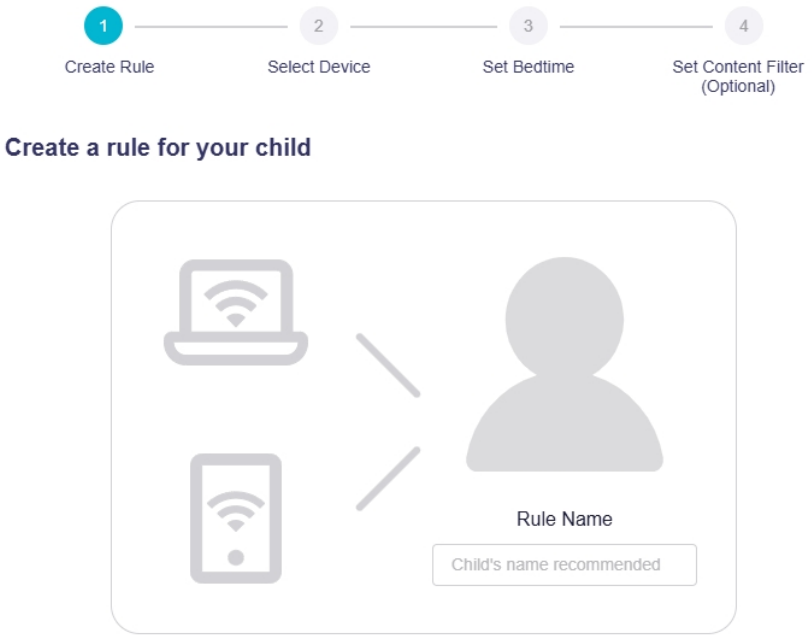
1. Inicie sesión en el panel de administración web del enrutador y vaya a **CONTROL DE FLUJO** -> **Control parental**. Asegúrese de que la hora del enrutador sea precisa.



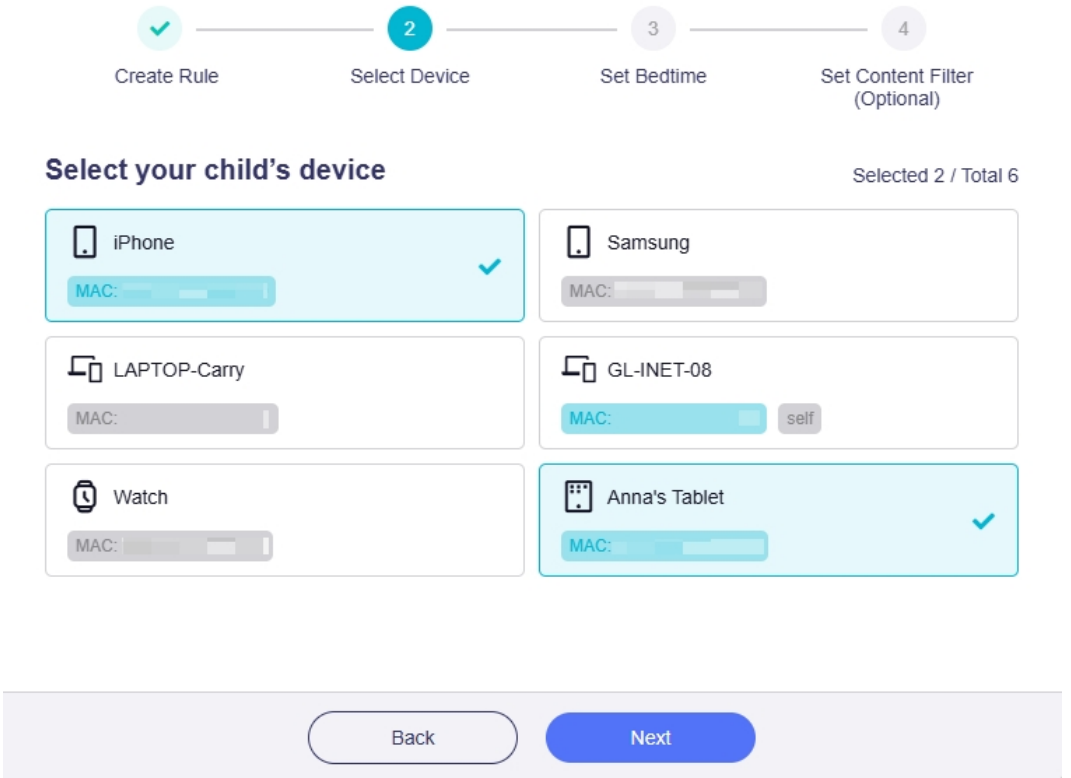
   Si no, ve a **SISTEMA** -> **Zona horaria** para sincronizarlo primero.
2. Habilita el control parental y haz clic en **Aplicar**.
3. Verá una lista de reglas como la siguiente. Haga clic en **Agregar una nueva regla**.



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

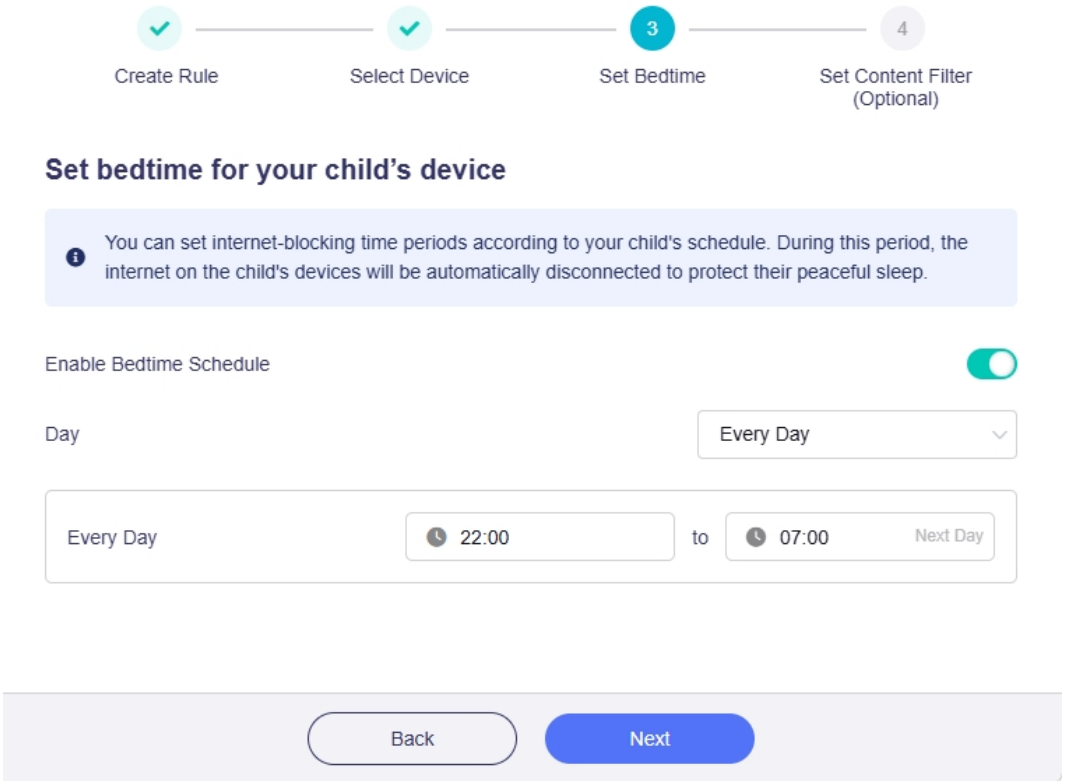


5. Seleccione el dispositivo de su hijo. Luegoluego haga clic en **Siguiente**.
   Del dispositivos solo aparecerá en esta página si están conectados al enrutador. El cian indica el estado en línea, mientras que el gris indica el estado fuera de línea.



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

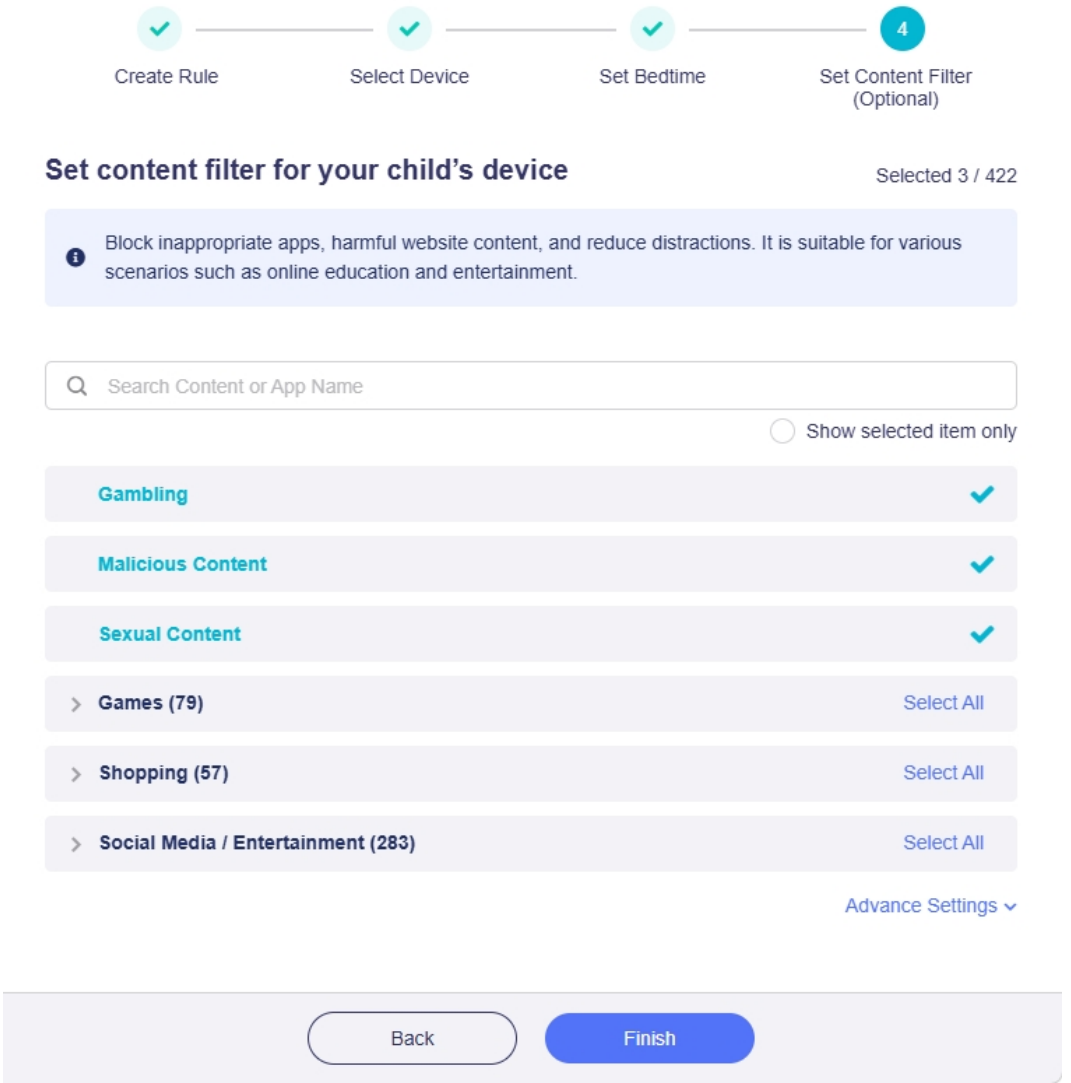
6. Establezca la hora de acostarse para el dispositivo de su hijo y luego haga clic en **Siguiente**. Internet en los dispositivos seleccionados no estará disponible durante este período. Lala hora de acostarse es la misma todos los días de forma predeterminada.



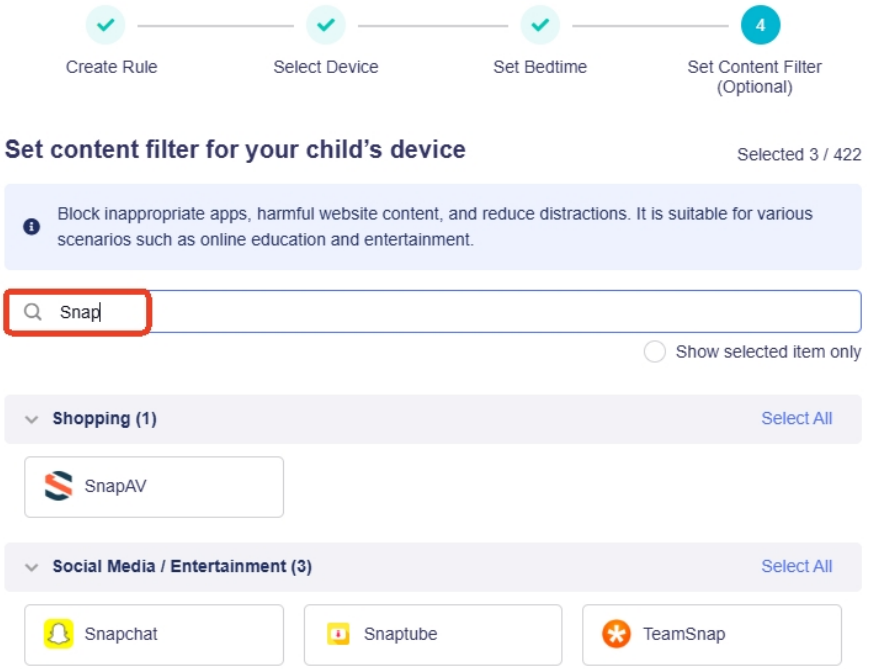
Si desea establecer diferentes horas de acostarse para cada día de la semana, seleccione **Personalizar días** y establezca diferentes horas de acostarse, luego haga clic en **Siguiente**.

7. Seleccionar filtro de contenido.

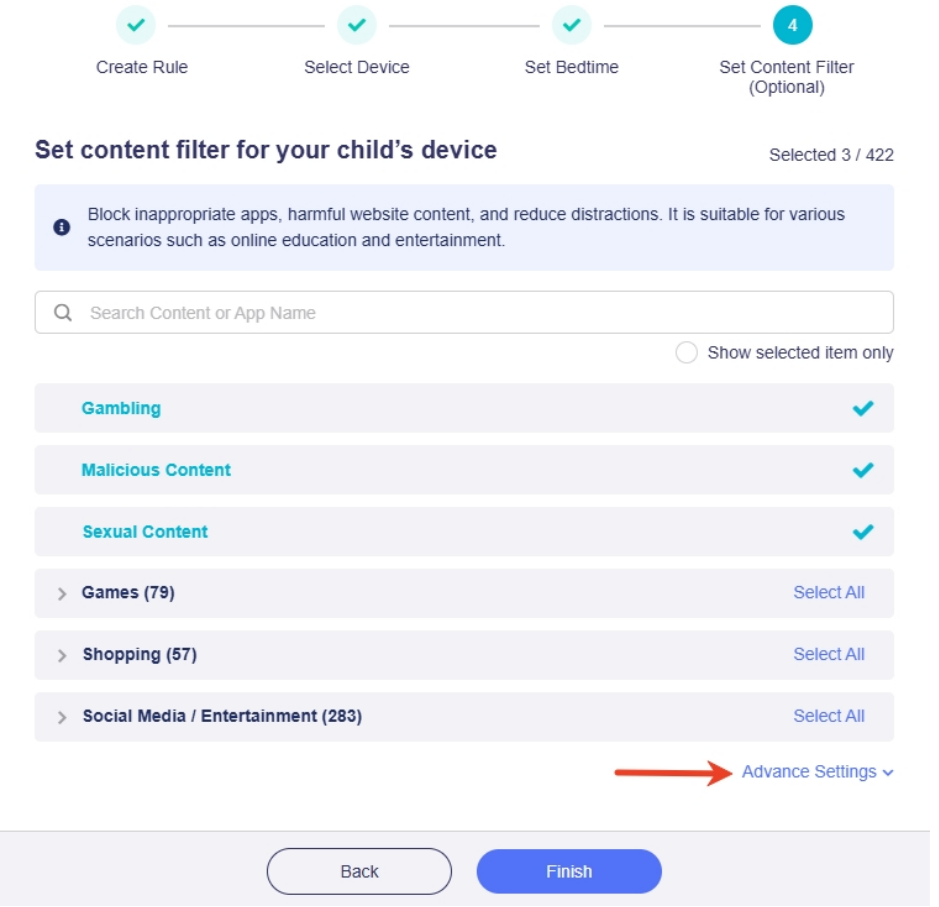
   Se han seleccionado tres categoríascted por predeterminado: **Apuestas**, **Contenido malicioso** y **Contenido sexual**. Puede seleccionar otras categorías si es necesario, como como **Juegos**, **Compras**, **Social Medios**, **Entretenimiento**, etc.



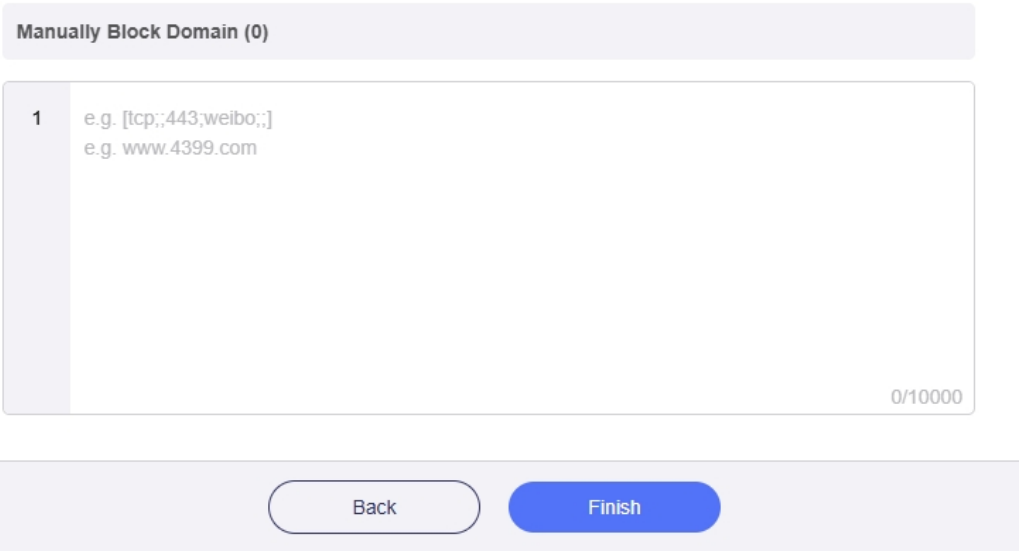
Si una determinada aplicación que deseas bloquear es difícil de encontrar, puedes buscarla en la parte superior.



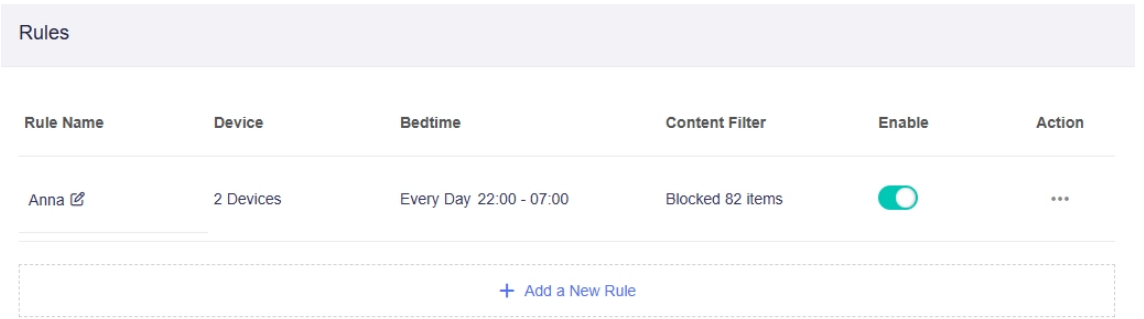
8. Si necesita bloquear ciertos dominios, haga clic en **Configuración avanzada** en la parte inferior derecha.



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



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



Capítulo 13

Seguridad

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

13.1 Reenvío de puertos

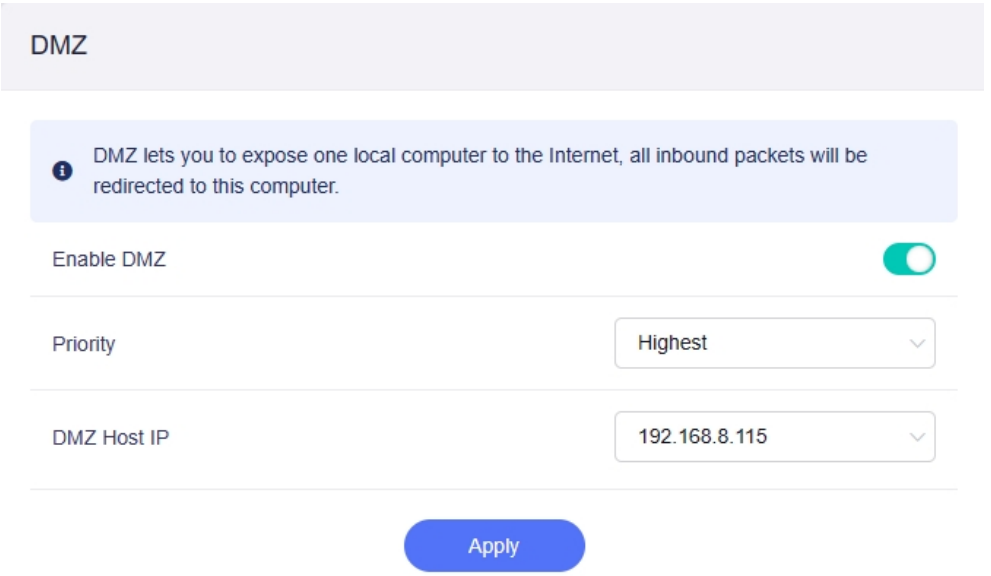
El reenvío de puertos es una función de red que enruta solicitudes externas a dispositivos específicos en su red local. La página de reenvío de puertos incluye dos funciones clave: **DMZ** (para acceso completo directo a un único dispositivo) y **Reenvío de puertos** (para acceso dirigido a puertos específicos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

13.1.1 DMZ

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

Siga los pasos a continuación para habilitar DMZ según sea necesario.

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



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

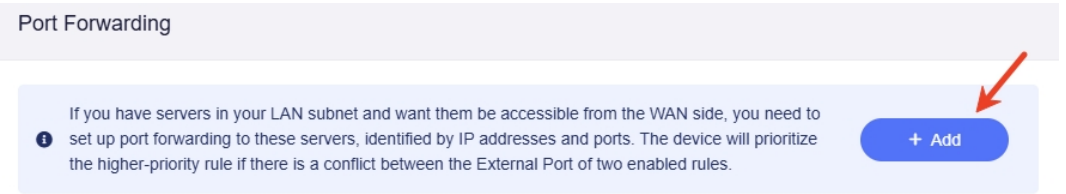
- **IP del host DMZ**: seleccione la dirección IP interna de el dispositivo que recibirá todos los paquetes entrantes.

13.1.2 Reenvío de puertos

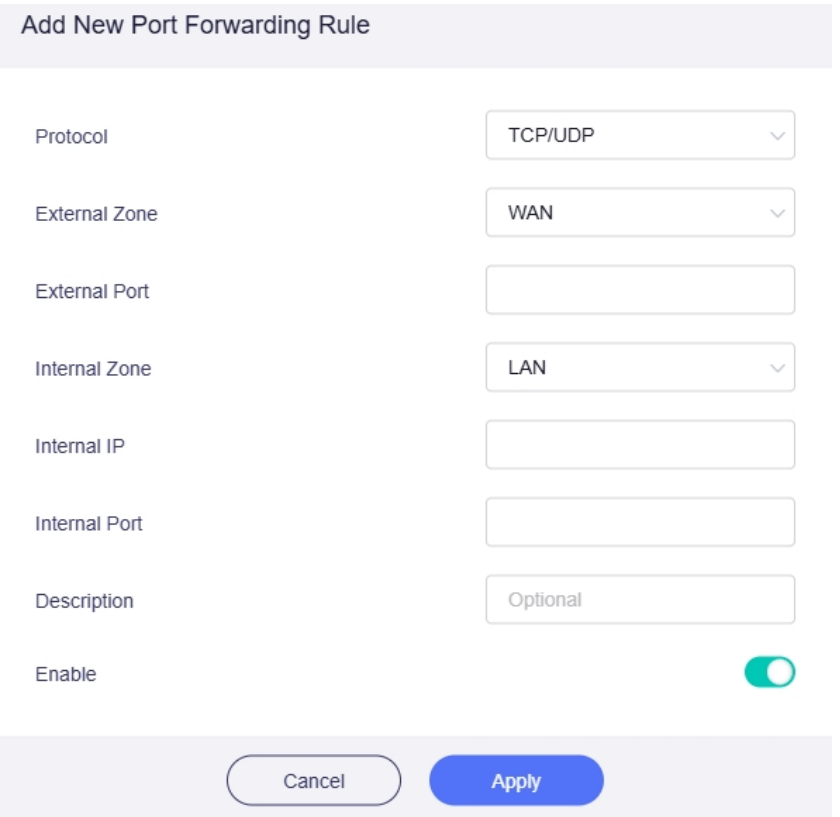
El reenvío de puertos permite que las computadoras remotas se conecten a una computadora o servidor local detrás del firewall de LAN (por ejemplo, servidores web, servidores FTP).

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

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



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



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

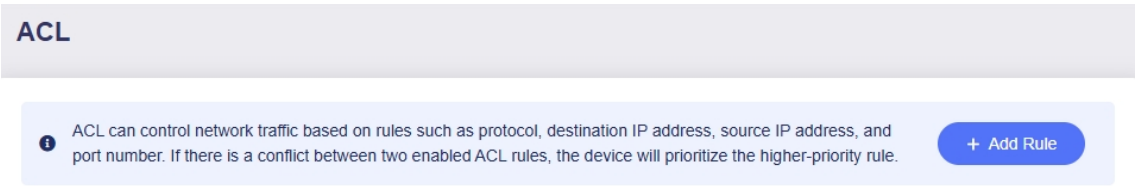
13.2 Lista de control de acceso (ACL)

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

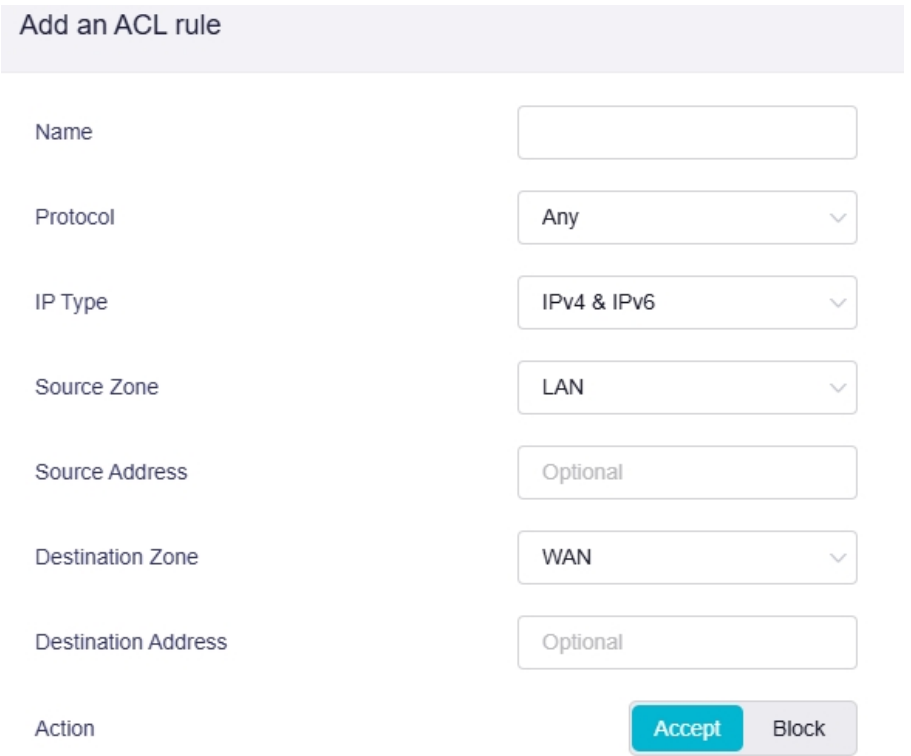
Ddiferente de Port Forwarding, ACL principalmente permite o bloquea el acceso a la red por motivos de seguridad, mientras que Port Forwarding redirige el tráfico externo a dispositivos específicos en su red local. para habilitar el acceso remoto a los servicios locales.

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

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



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





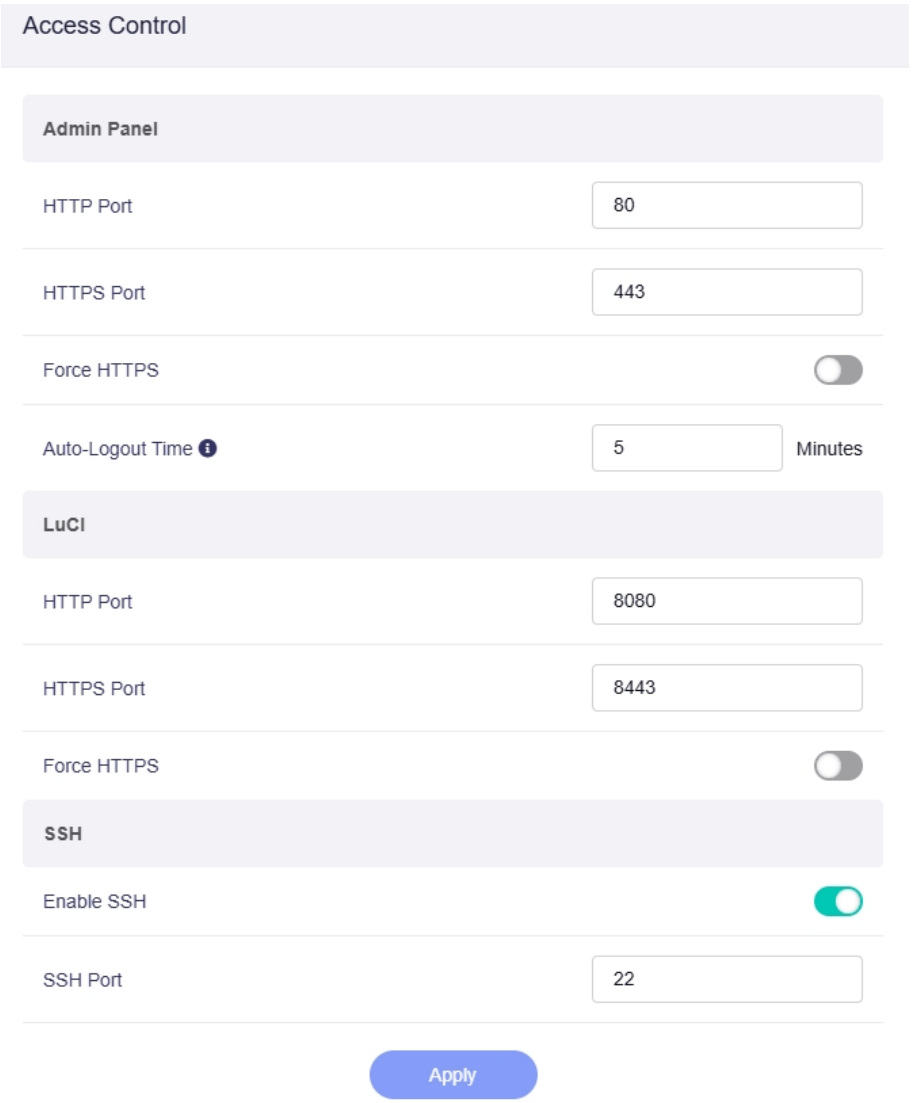
- **Nombre**: ingrese un nombre personalizado para la regla.
- **Protocolo**: especifique a qué tipo de tráfico de red se aplica la regla. Seleccione un protocolo de conexión entre Cualquiera, TCP, UDP, TCP+UDP e ICMP.
- **Tipo de IP**: defina el formato de dirección IP para el tráfico de red. Seleccione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

13.3 Acceso de administrador

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

13.3.1 Control de acceso

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



Panel de administración

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

LuCI

Nota: instale LuCI en la Configuración avanzada antes de realizar la configuración. el control de acceso.

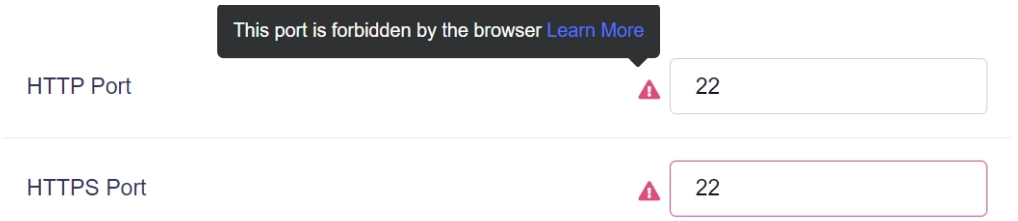
- **Puerto HTTP**: El valor predeterminado es 8080, para acceso HTTP sin cifrar a la interfaz LuCI.
- **Puerto HTTPS**: El valor predeterminado es 8443, para un acceso HTTPS seguro al mismo. Interfaz LuCI.
- **Forzar HTTPS**: cuando está habilitado, se exige el acceso a la interfaz LuCI para utilizar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

SSH

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

Nota:

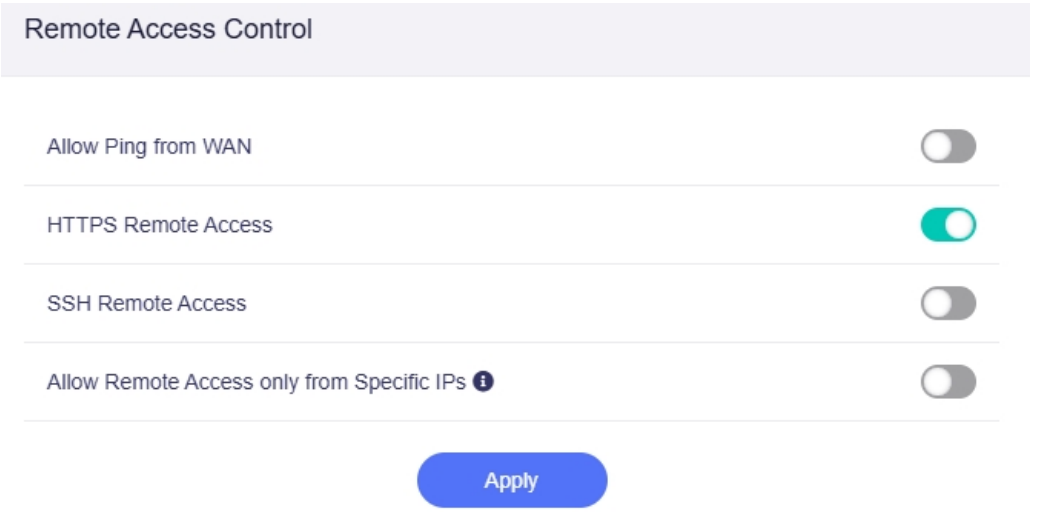
1. Si asigna un número de puerto que entra en conflicto con un puerto reservado (o uno reservado para servicios específicos por navegadores/convenciones de red), aparecerá un mensaje que indicará "Este puerto está prohibido por el navegador".



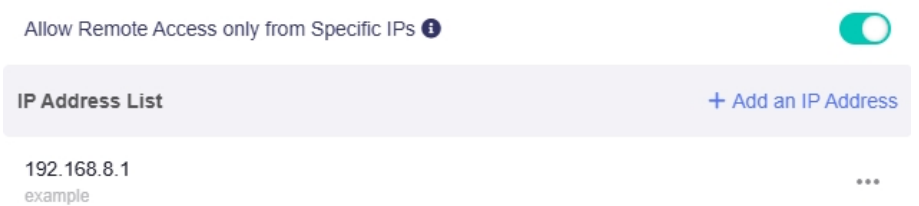
2. Si el número de puerto se modifica en el firmware, deberá ingresar el número de puerto correcto para acceder al panel de administración. Si olvidó el número de puerto, reinicie el enrutador para restaurar el número de puerto predeterminado.

13.3.2 Control de acceso remoto

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

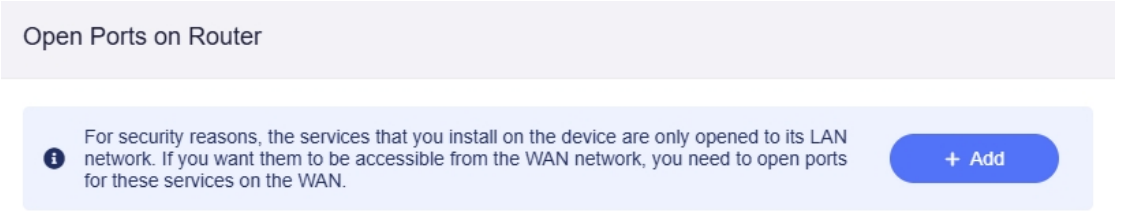


- **Permitir ping desde WAN**: Apermitir ping desde el lado WAN del enrutadorpuede ayudar a los usuarios a verificar si se puede acceder al enrutador a través de la WAN wcuando hay un problema de red, así como a determinar la latencia de la red y la pérdida de paquetes.
- **Acceso remoto HTTPS**: El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

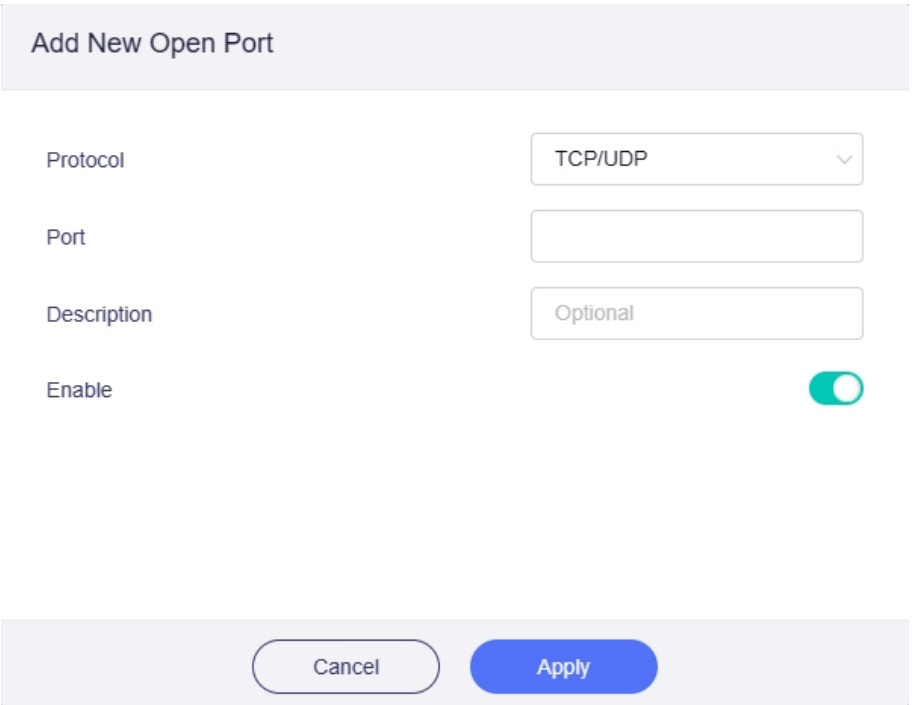


13.3.3 Abrir puertos en el enrutador

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



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

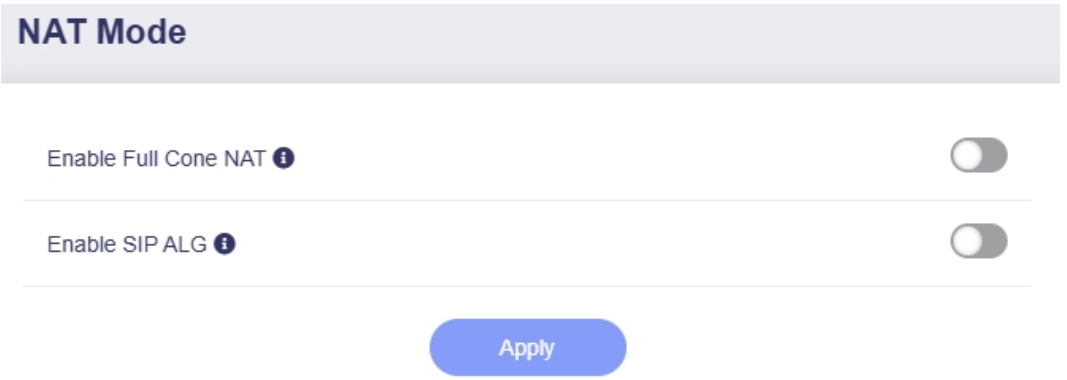


- **Protocolo**: seleccione el protocolo de red (TCP, UDP o TCP/UDP) para el puerto. Esto determina cómo se transmiten los datos para el servicio asociado con el puerto.
- **Puerto**: ingrese el número de puerto específico que desea abrir.

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

13.4 Modo NAT

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



- **NAT de cono completo**: se puede utilizar para reducir la latencia del juego, mejorando la capacidad de respuesta de los juegos en línea. Sin embargo, habilitar Full Cone NAT puede ser menos seguro ya que permite conexiones entrantes sin restricciones.
- **ALG SIP**: Su objetivo es mitigar los efectos de múltiples NAT en el tráfico SIP (Protocolo de inicio de sesión) . Sin embargo, en la mayoría de los casos, no ayudará e incluso puede afectar las llamadas VoIP, causando problemas como audio unidireccional, teléfonos que no suenan, caídas inesperadas de llamadas o llamadas que van directamente al correo de voz.

Capítulo 14

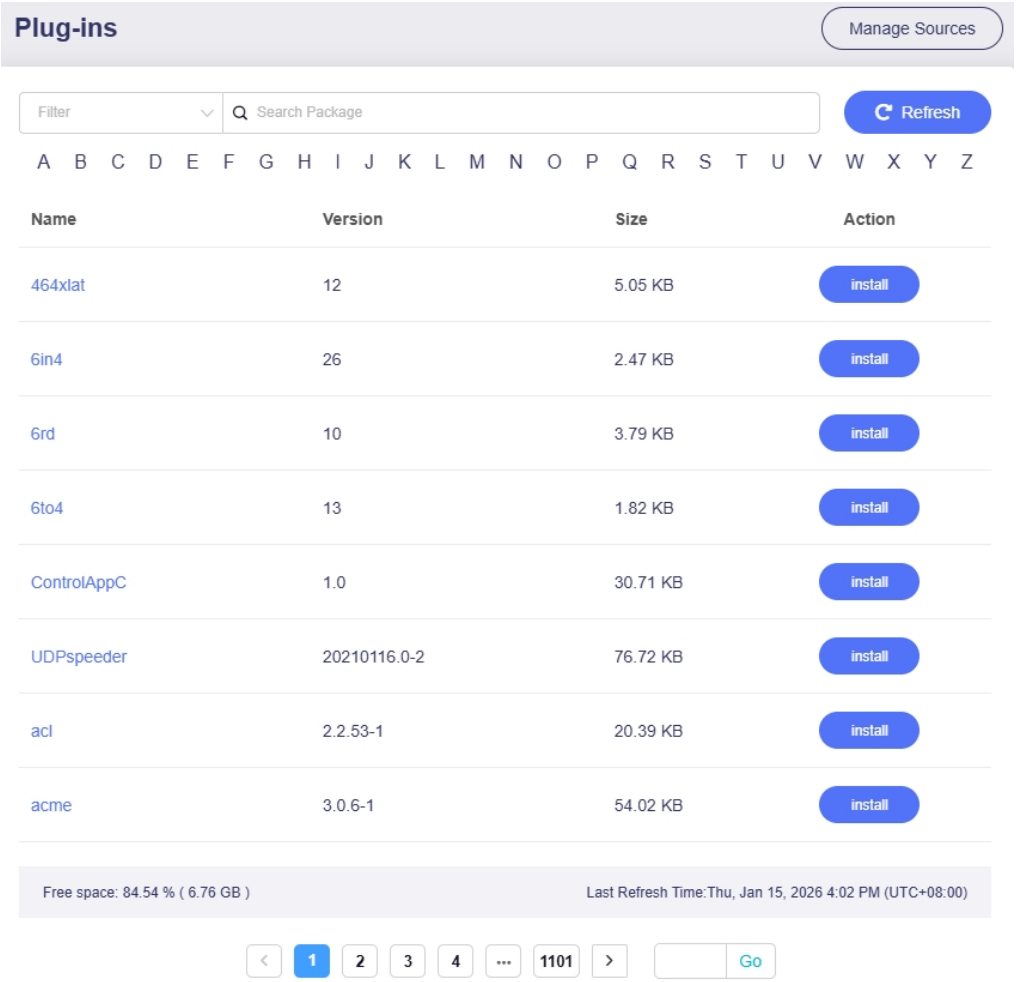
Aplicaciones

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

14.1 Complementos

La Página de complementos le permite administrar paquetes OpenWrt.

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



Nota:

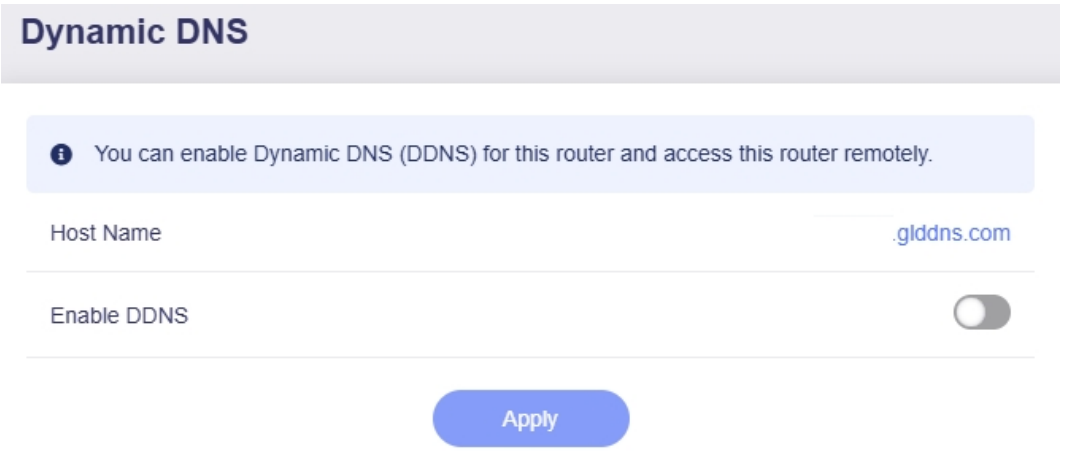
1. No se recomienda actualizar los complementos preinstalados en el firmware oficial de GL.iNet, como nginx, adguard home, tailscale, etc.
2. Los complementos de terceros instalados manualmente por los usuarios se pueden actualizar; sin embargo, GL.iNet no es responsable de ningún problema de seguridad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

14.2 DNS dinámico

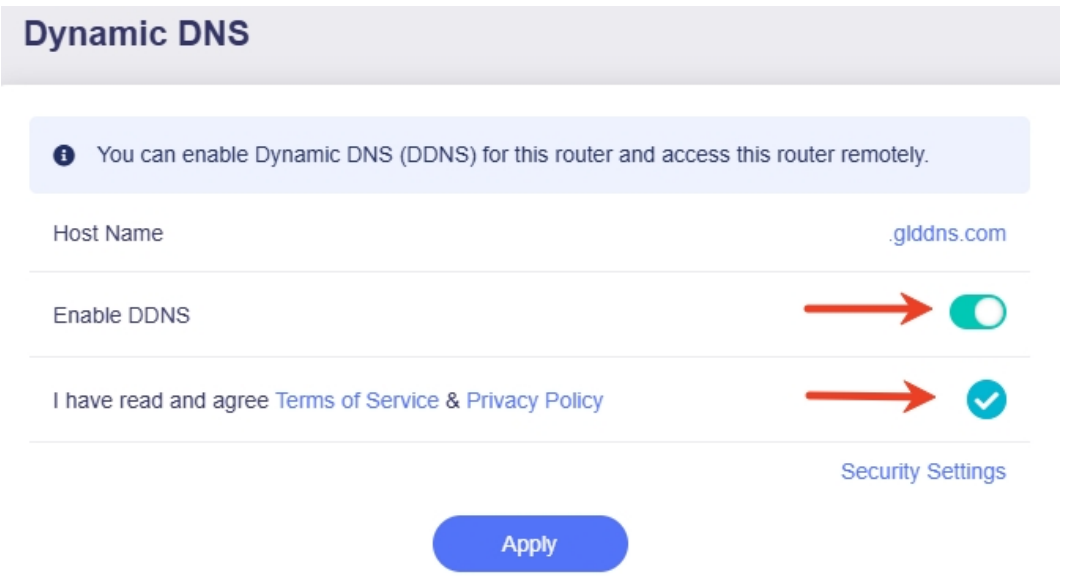
Dinámico El servicio de nombres de dominio (DDNS o DNS dinámico) es un servicio que se utiliza para asignar un nombre de dominio a la dirección IP dinámica de un dispositivo de red. Con DNS dinámico, puede acceder a su enrutador de forma remota. Se requiere una dirección IP pública para esta funcionalidad.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

14.2.1 Habilitar DDNS

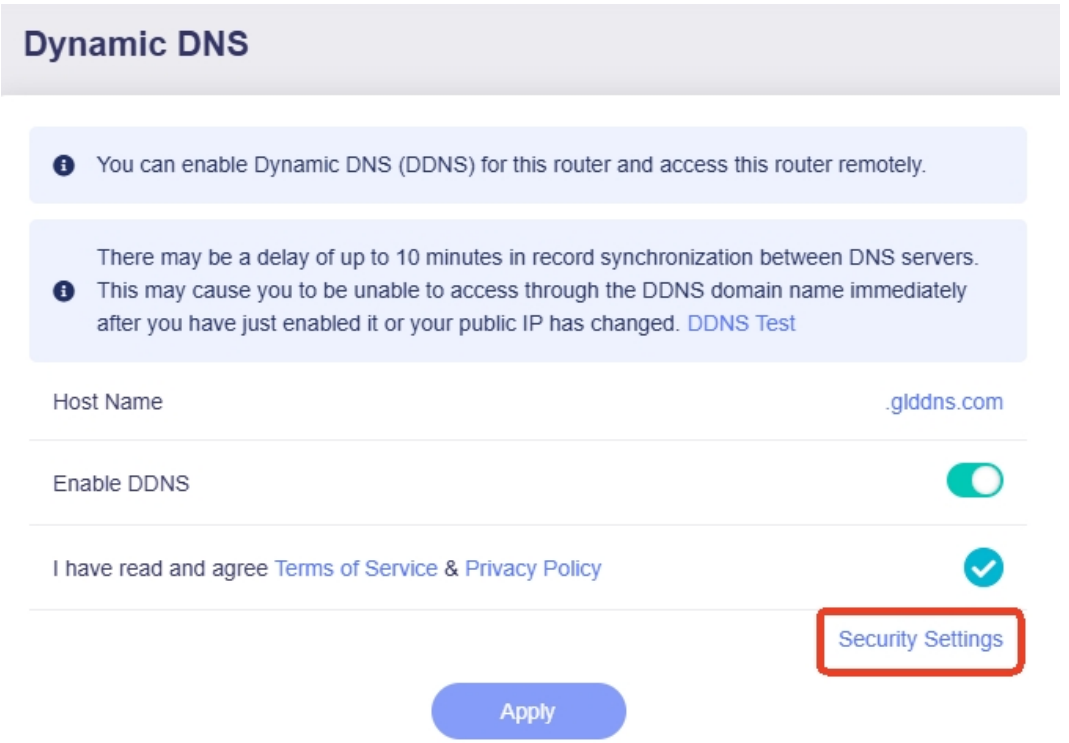
1. Inicie sesión en su enrutador's web admin panel, navegue hasta **APLICACIONES** > **DNS dinámico**, la página se muestra como a continuación.



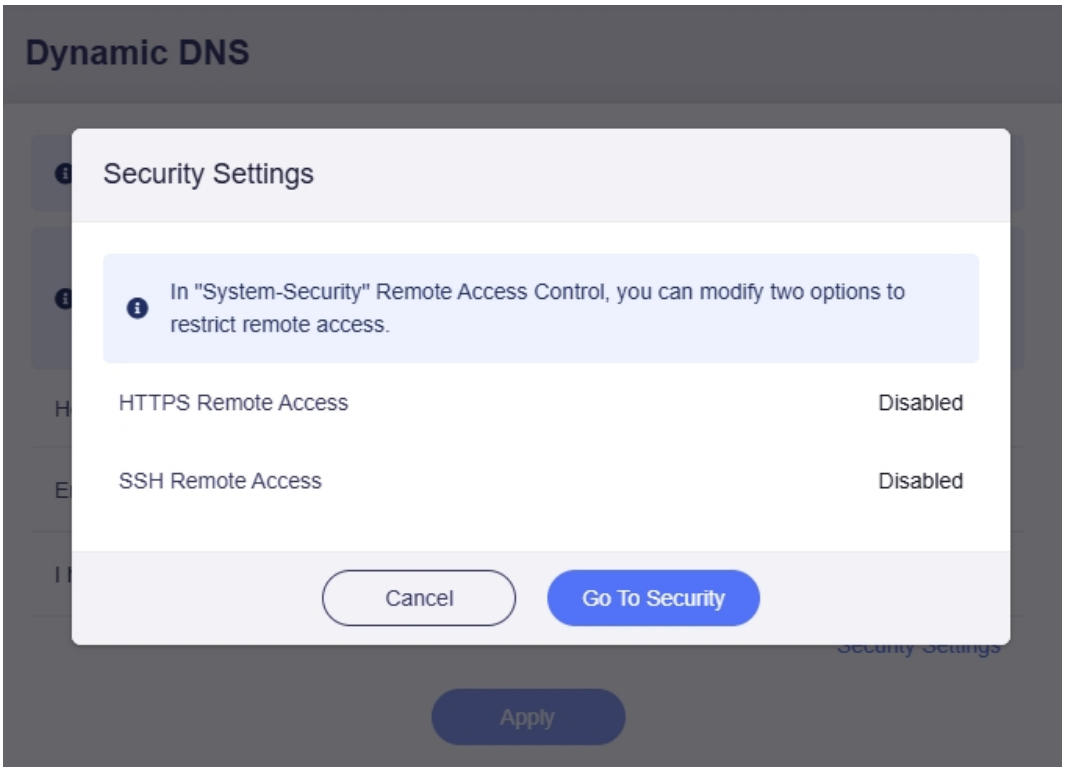
2. Active **Habilitar DDNS**, lectura y acepta los los **Términos de servicios y política de privacidad** y luego haz clic en **Aplicar**.



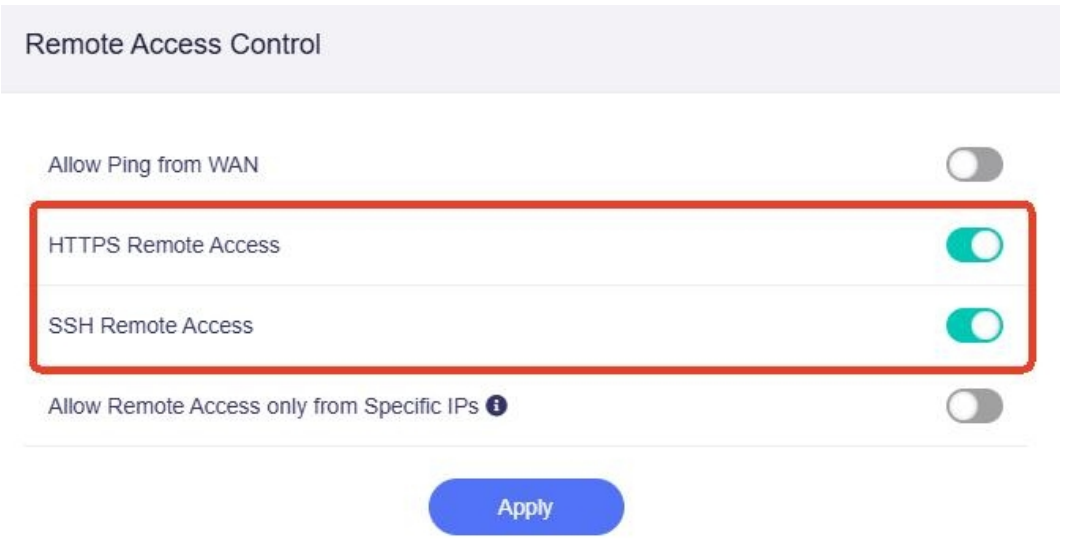
3. Haga clic en **Configuración de seguridad** en la esquina inferior derecha.



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



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



Nota:

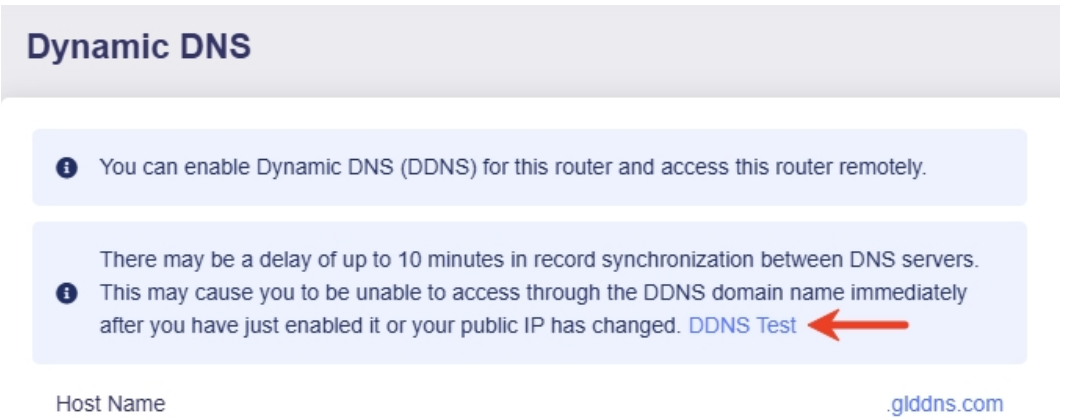
1. Puede haber un retraso de hasta 10 minutos en la sincronización de registros entre servidores DNS. Esto puede impedirle acceder a través del nombre de dominio DDNS inmediatamente después de habilitarlo o cuando cambie su IP pública.
2. Si habilita DDNS y el Cliente VPN al mismo tiempo, enseguro que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

14.2.2 Comprobar si DDNS funciona

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

Método 1. Use Herramienta de prueba DDNS

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



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



Método 2. Usar comandos

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



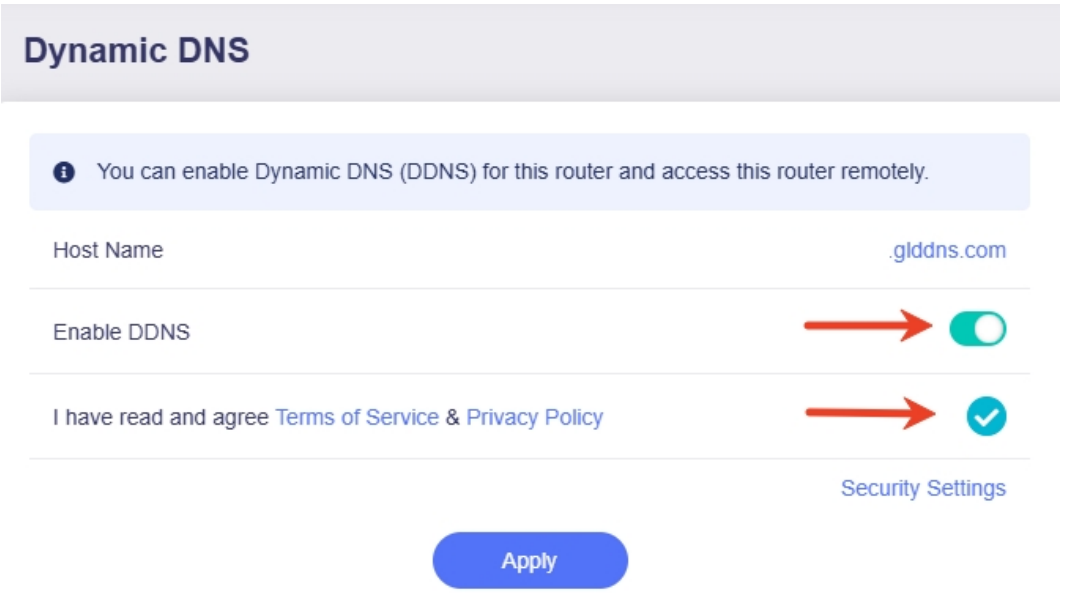
   - Reemplace “xxxxxxx.glddns.com” en la imagen de arriba con su Nombre del host.
   - El “8.8.8.8” es el DNS de Google. Úseloúselo o reemplácelo por otros, luego presione Entrar.
2. Si obtiene una dirección IP pública como “183.178.10.100” en la imagen de arriba, indica que su dominio DDNS se ha asignado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

14.2.3 Acceso remoto HTTPS

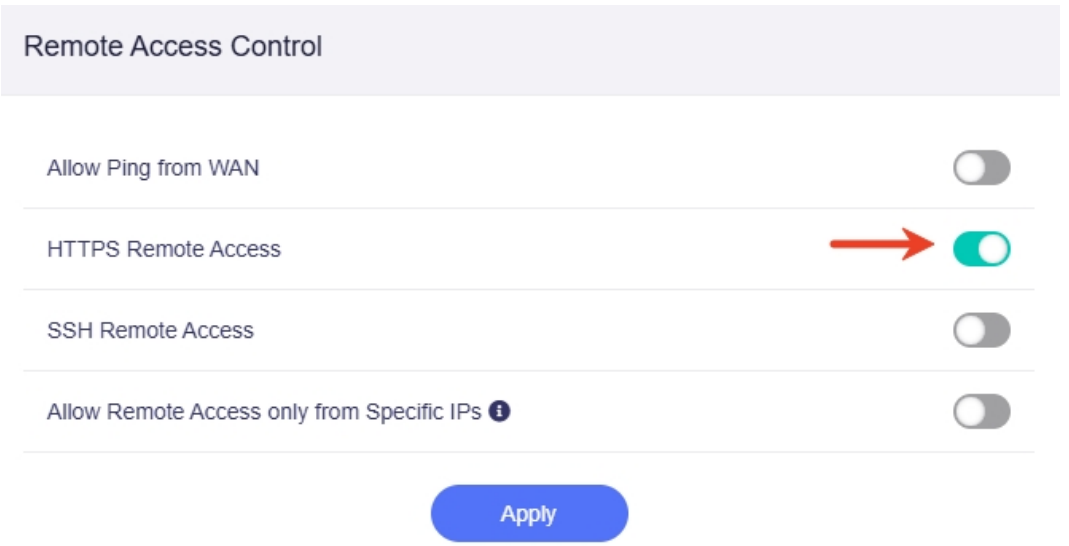
Se requiere una **Dirección IP pública** para el acceso remoto HTTPS. Ver aquí tpara verificar si su ISP le asigna una dirección IP pública. Si su enrutador está detrás de NAT, configure el reenvío de puertos (**puerto 443**) en el enrutador ascendente para acceso HTTPS.

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

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

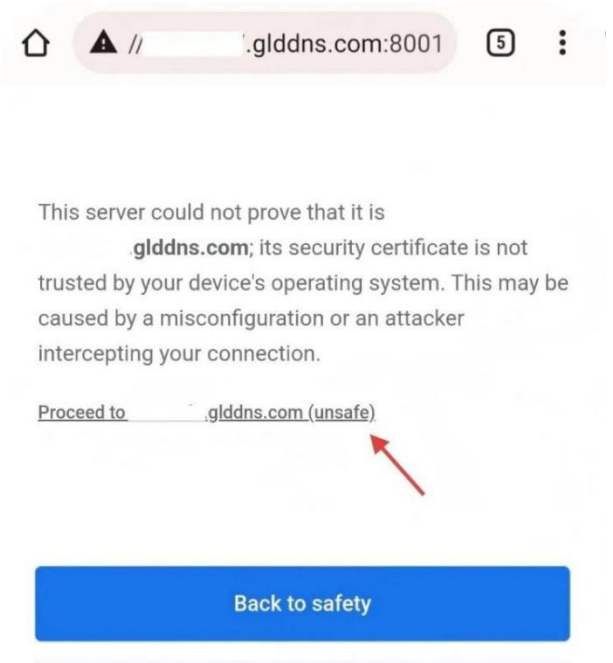


2. En el panel de administración web, vaya a **SECURITY** > **Acceso de administrador** > **Control de acceso remoto**. Habilitar **Acceso remoto HTTPS** y haga clic en **Aplicar**.



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

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



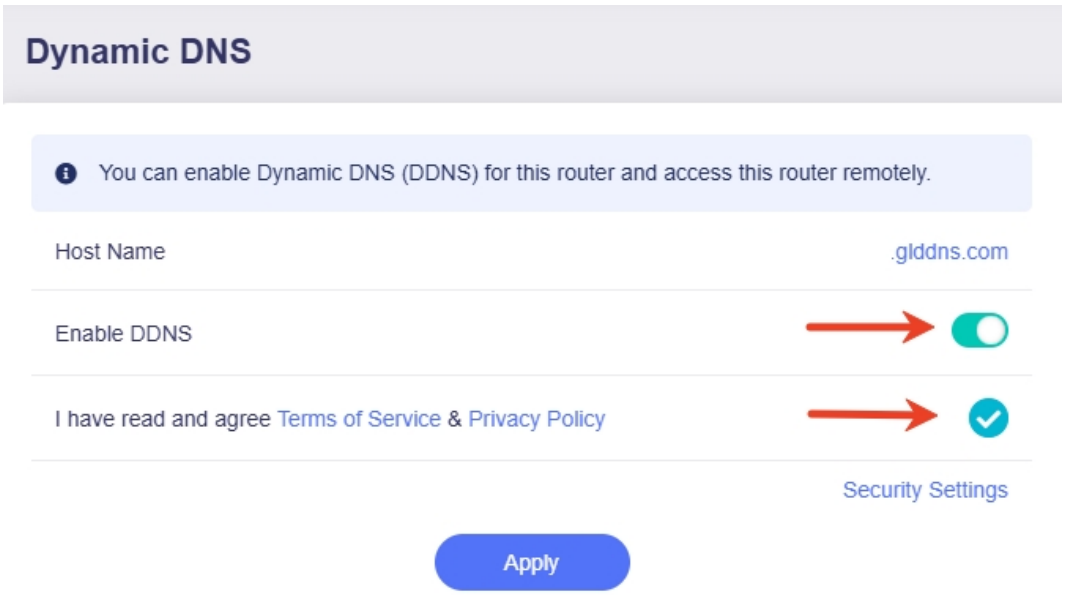
Luego podrá acceder al enrutador's panel de administración web usando DDNS host nombre sobre **HTTPS**.

14.2.4 Acceso remoto SSH

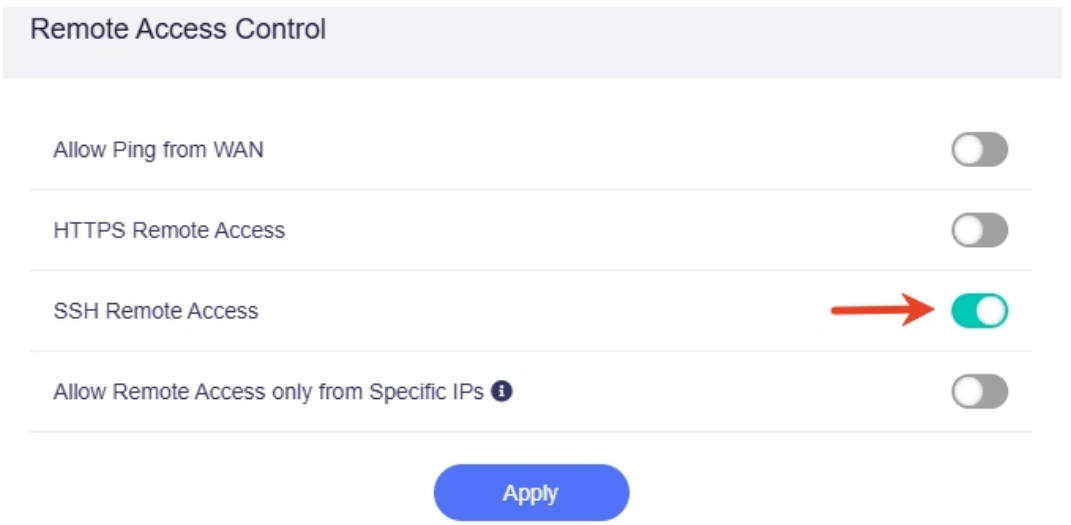
Se requiere una **Dirección IP pública** para el acceso remoto SSH.Consulte aquí tpara verificar si su ISP le asigna una dirección IP pública. Si su enrutador está detrás de NAT, configure el reenvío de puertos (**puerto 22**) en el enrutador ascendente para SSH remoto acceso.

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

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



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



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

14.3 Almacenamiento en red

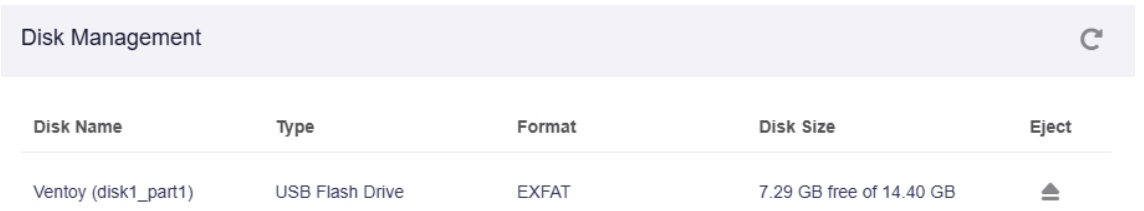
El almacenamiento en red permite compartir archivos entre dispositivos conectando una unidad USB o una tarjeta SD a su enrutador. El enrutador convierte el dispositivo de almacenamiento en una unidad de red compartida, accesible para todos dispositivos conectados.

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

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

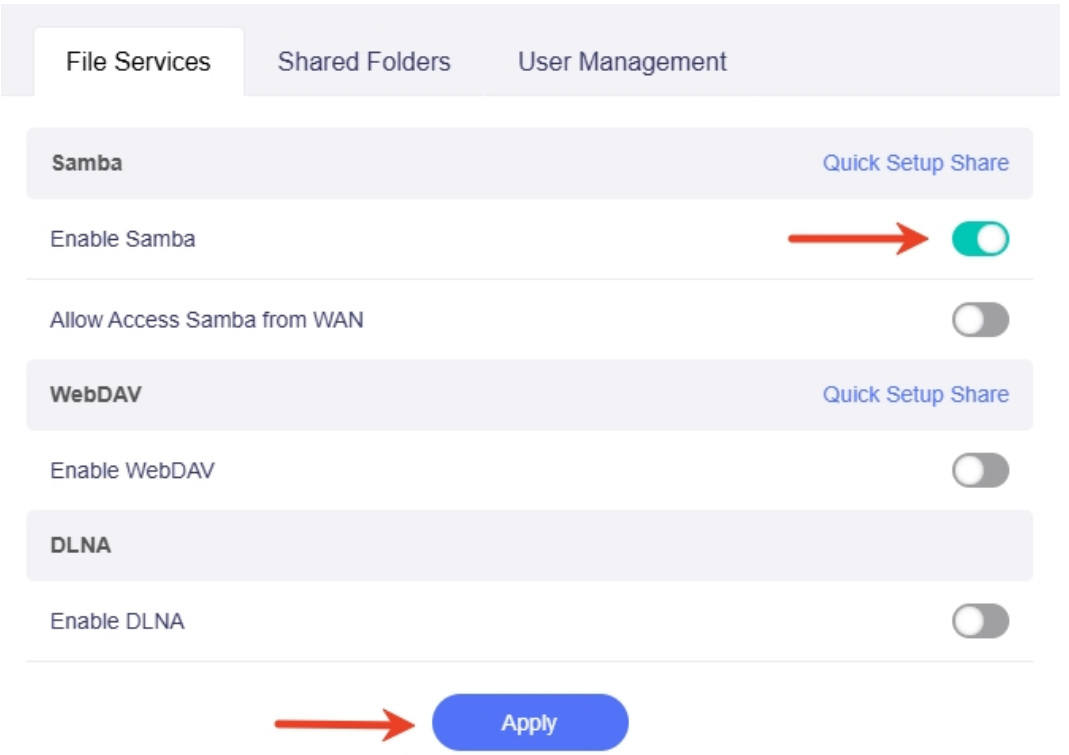
14.3.1 Conectar una unidad de almacenamiento

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



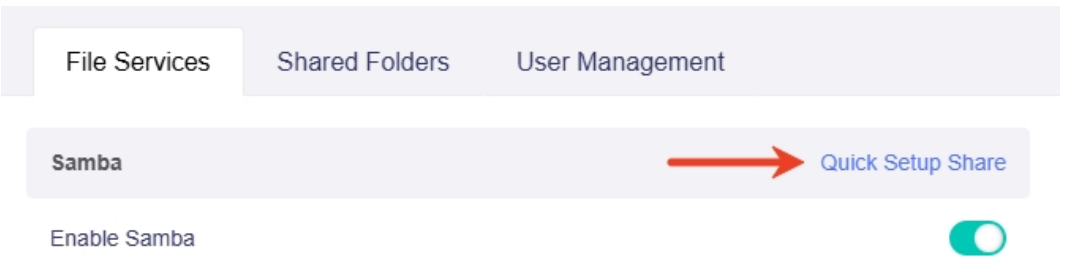
14.3.2 Configurar Samba

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

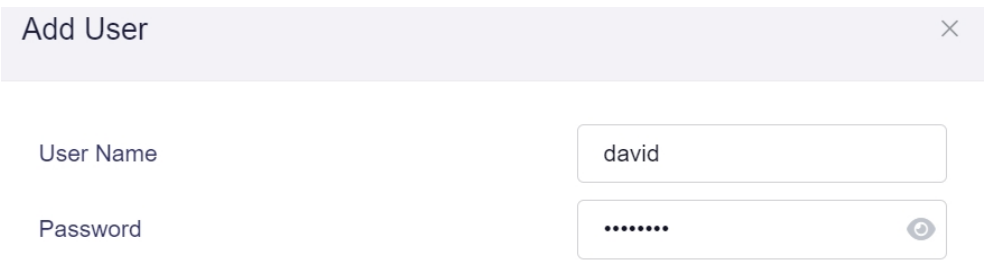


- **Permitir acceso a Samba desde WAN**: habilitar it si desea que los dispositivos ascendentes accedan al servicio Samba.

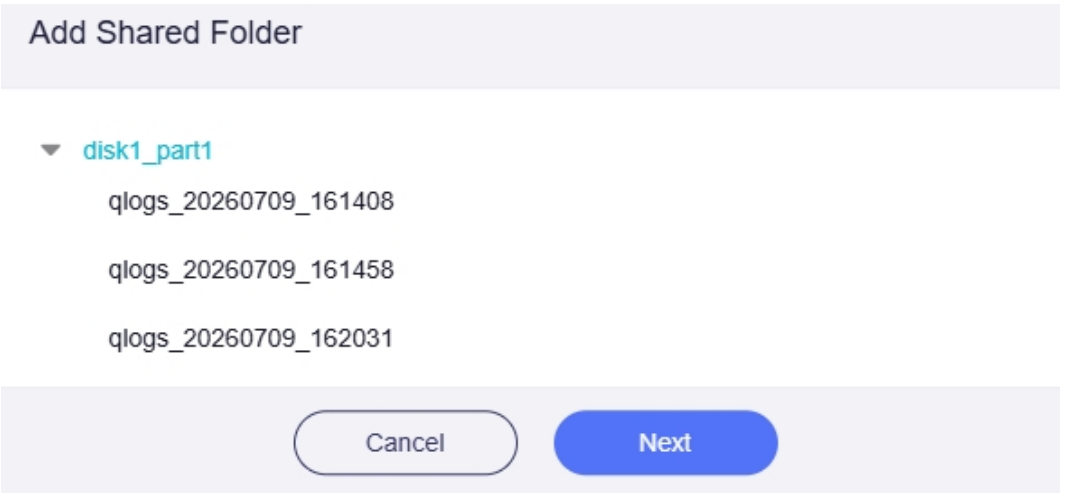
2. Haga clic en **Configuración rápida Compartir** a establezca el enlace compartido.



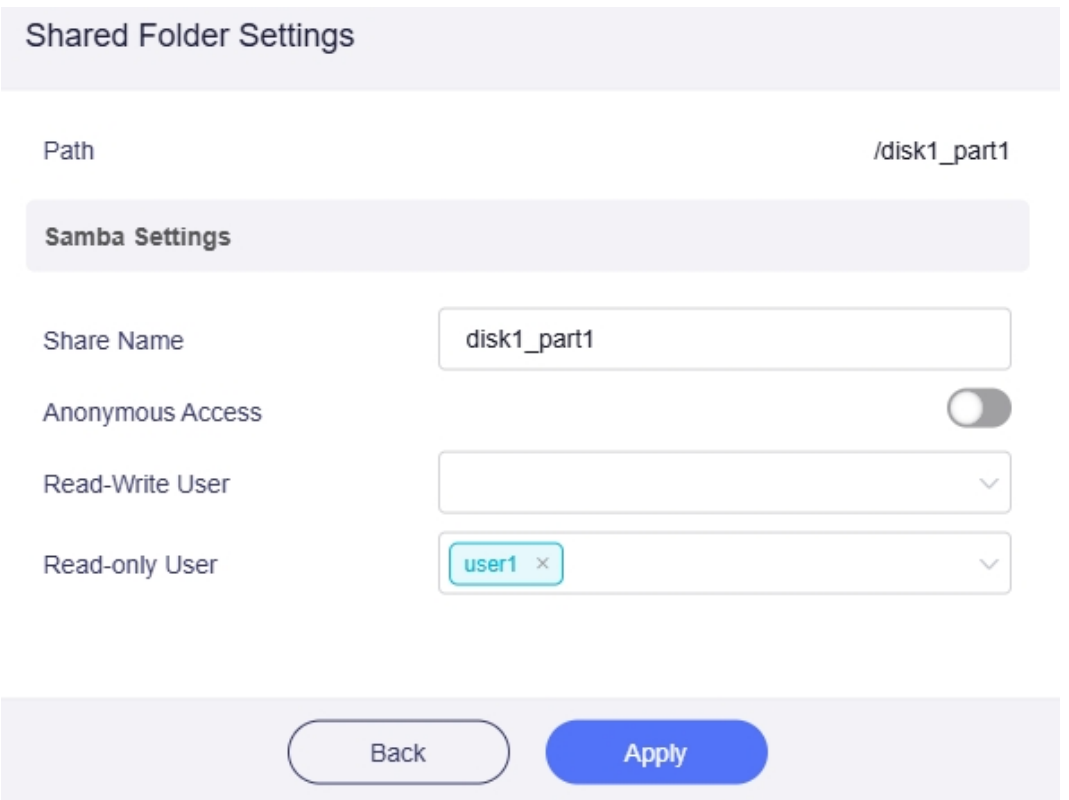
3. Agregue un usuario y haga clic en **Siguiente**. Este paso se omitirá si ya tiene una cuenta.



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

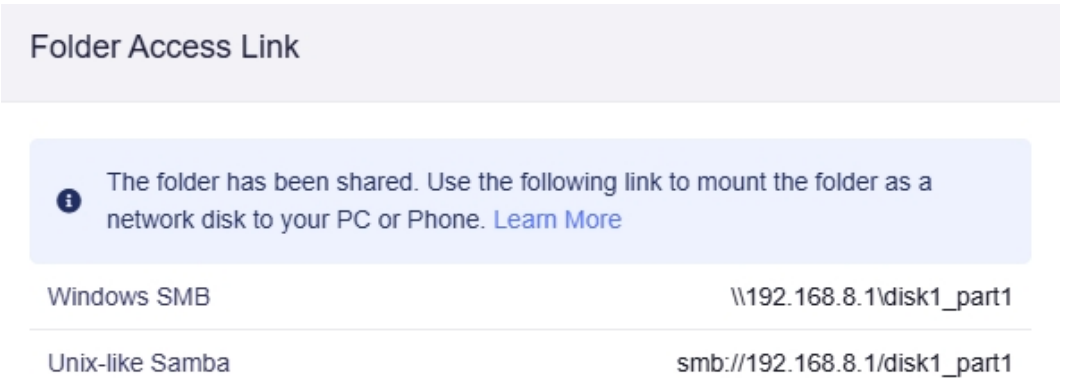


5. Configura lacarpeta compartida.
   Tel usuario creado en el paso anterior se agregará a **Usuario de solo lectura** de forma predeterminada. Si desea que este usuario pueda escribir o eliminar archivos, eliminarlo de Usuario de solo lectura y agregarlo a **Lectura-Escritura Usuario**, then haga clic en **Aplicar**.



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

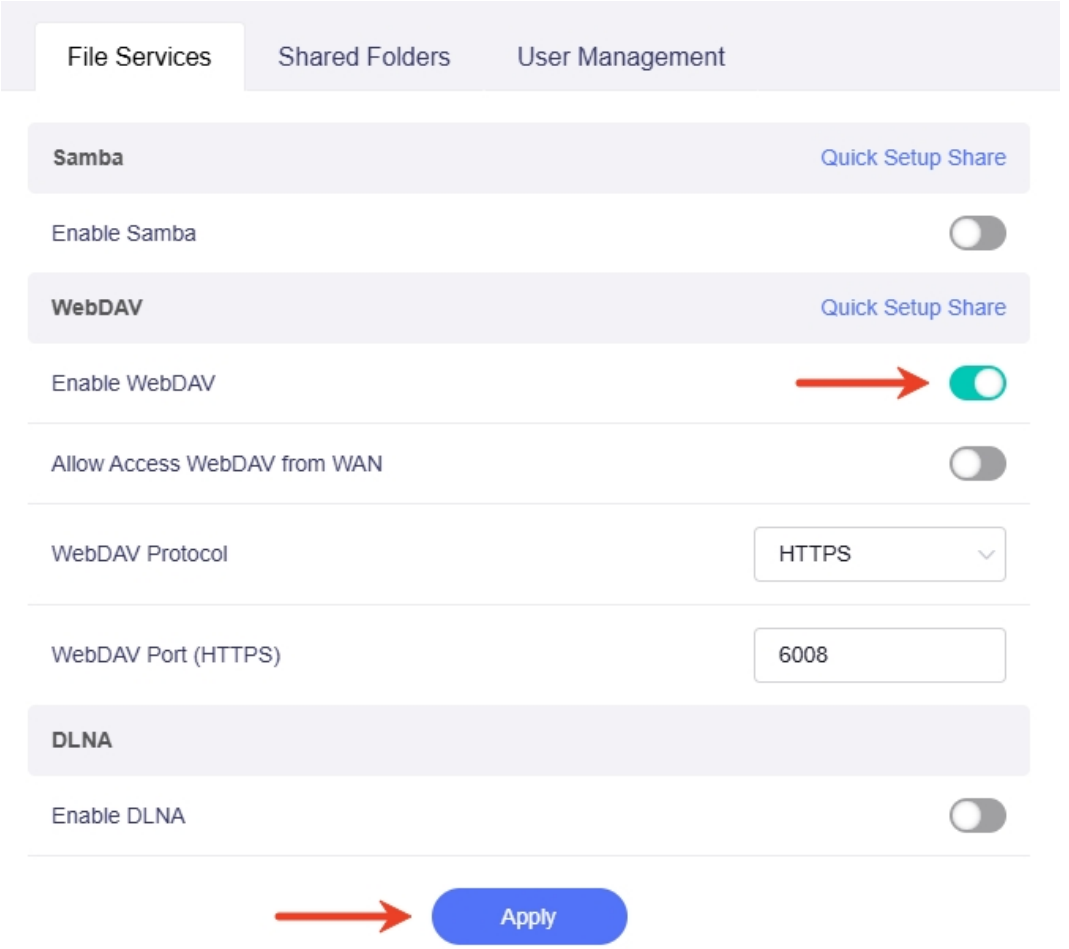
6. Obtenga el enlace de acceso a la carpeta .
   La página mostrará el enlaces para Windows y sistemas operativos tipo Unix. El sistema tipo Unix incluyes Android, iOS, macOS, Ubuntu, etc. Ahora puedes acceder su carpeta compartida a través del servicio Samba a través de estos enlaces.



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

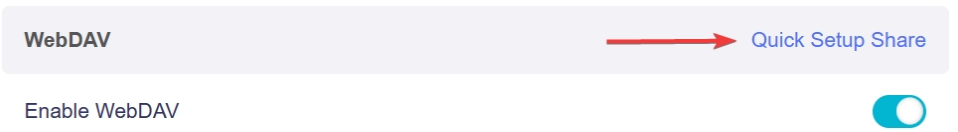
14.3.3 Configurar WebDAV

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

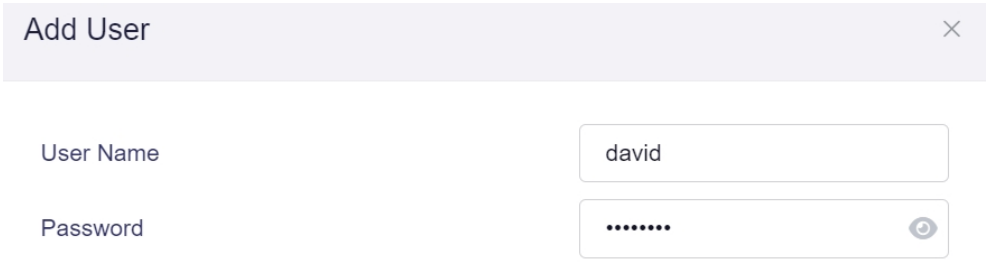


- **Permitir acceso a WebDAV desde WAN**: habilítelo si desea el dispositivos ascendentes para acceder al servicio WebDAV.
- **Protocolo WebDAV**: HTTP es sin cifrar; úselo bajo su propia responsabilidad. HTTPS está cifrado y it utiliza certificado autofirmado.
- **Puerto WebDAV**: no es necesario modificar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

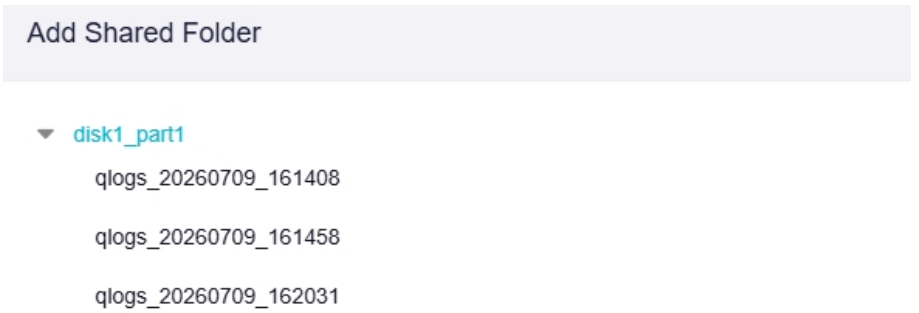
2. Haga clic en **Configuración rápida Compartir** para sestablezca el enlace compartido.



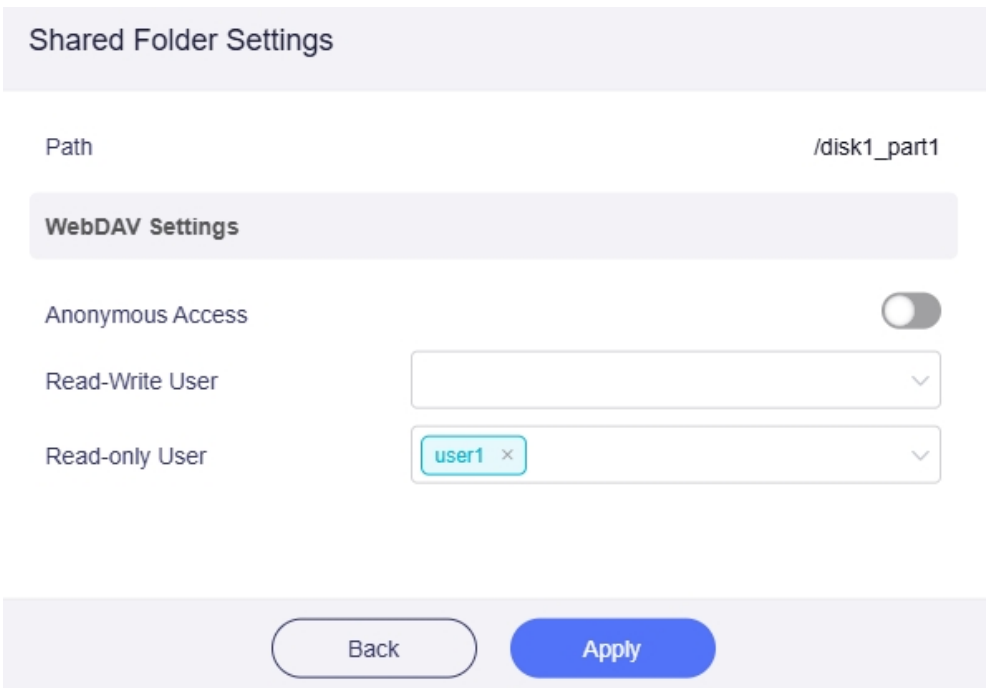
3. Agregue un usuario y haga clic en **Siguiente**. Este paso se omitirá si ya tiene una cuenta.



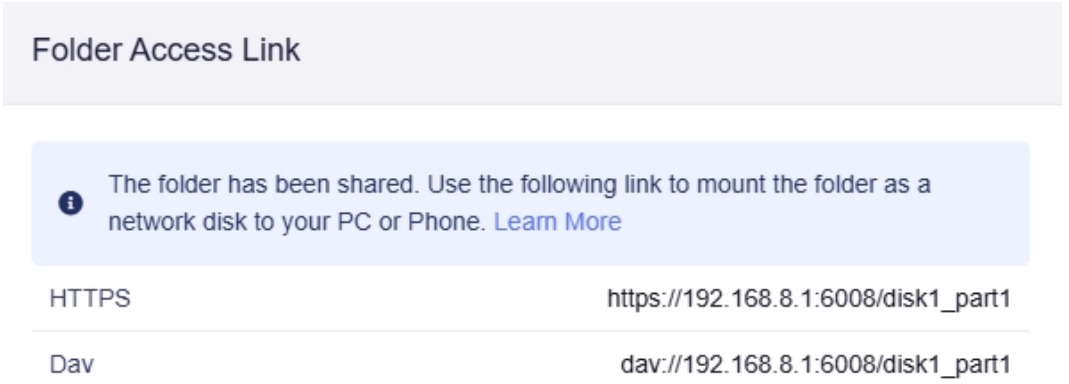
4. Haga clic en el ícono del triángulo para mostrar todas las carpetas. Sseleccione una carpeta para compartir. Sisi desea compartir el completo disco, haga clic en el nombre del disco (por ejemplo, disk1_part1).



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



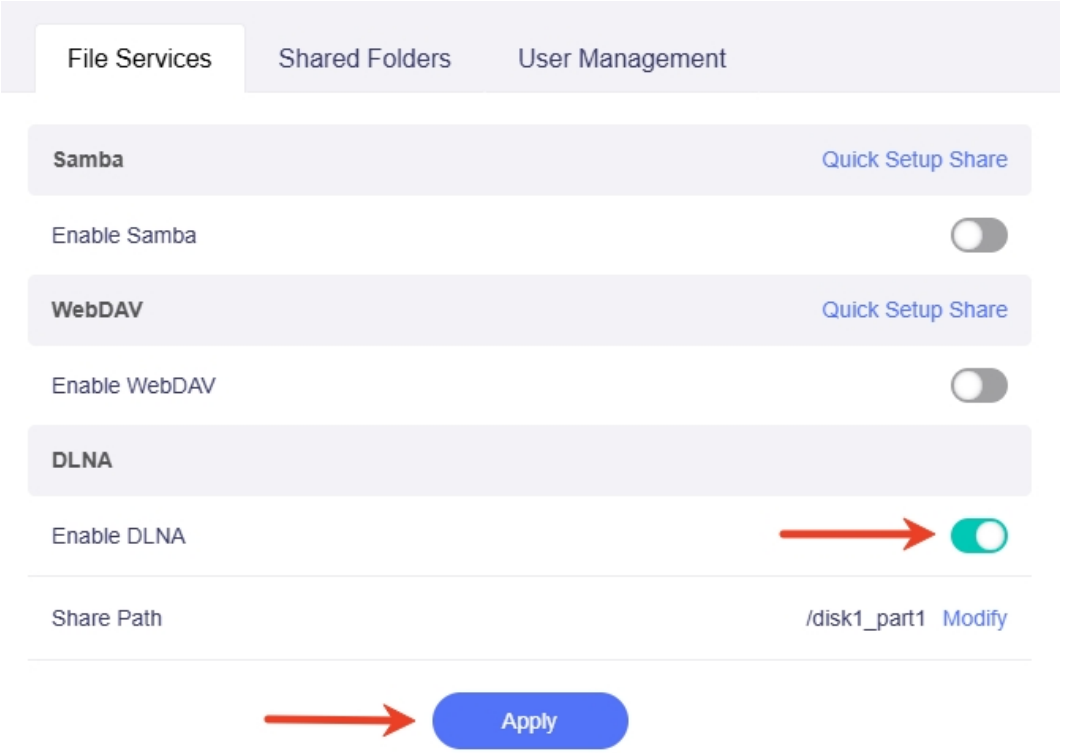
6. Obtener el enlace de acceso a la carpeta.
   La página mostrará el enlaces para Windows y sistemas operativos tipo Unix. Los sistemas tipo Unix incluyens Android, iOS, macOS, Ubuntu, etc. Ahora puede acceder a su carpeta compartida a través del servicio WebDAV a través de estos enlaces.



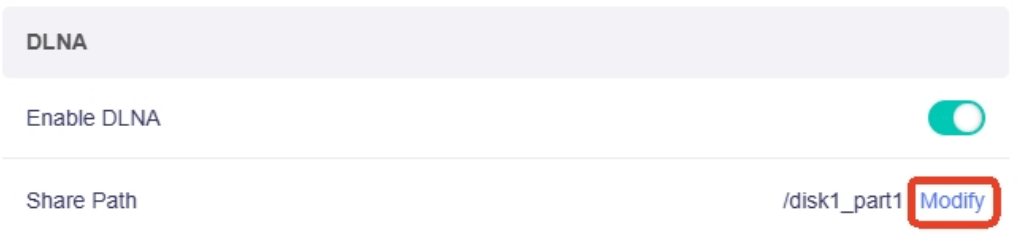
Nota: si habilita **Permitir acceso WebDAV desde WAN** y acceda la carpeta compartida de red ascendente, reemplace la IP del enrutador (predeterminada: 192.168.8.1) en el enlace de acceso con tu enrutador’s WAN IP, que se puede encontrar en la página INTERNET del panel de administración web.

14.3.4 Configurar DLNA

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



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



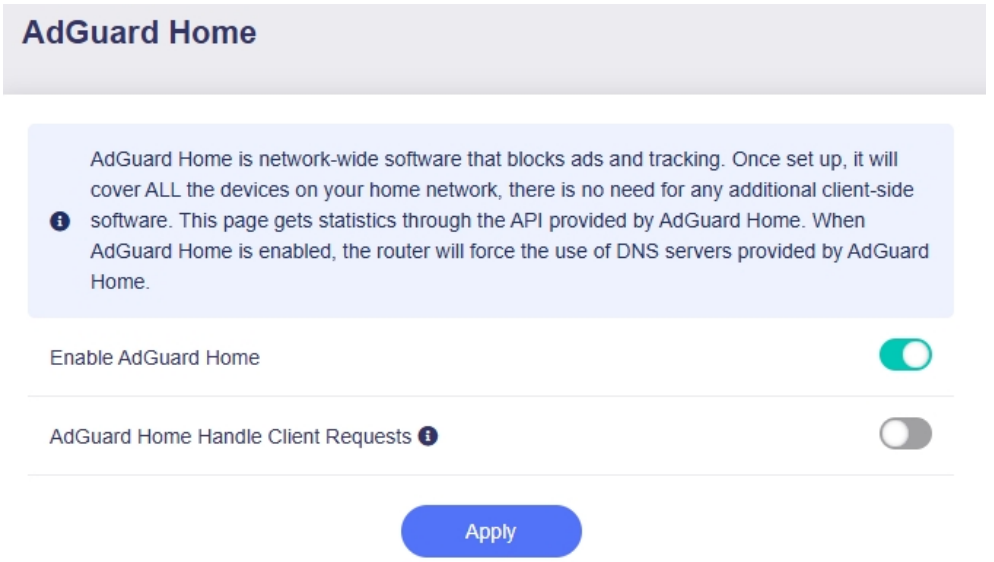
3. Conecte su televisor inteligente al enrutador. encontrará el DLNA sservidor automáticamente.

14.4 AdGuard Home

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

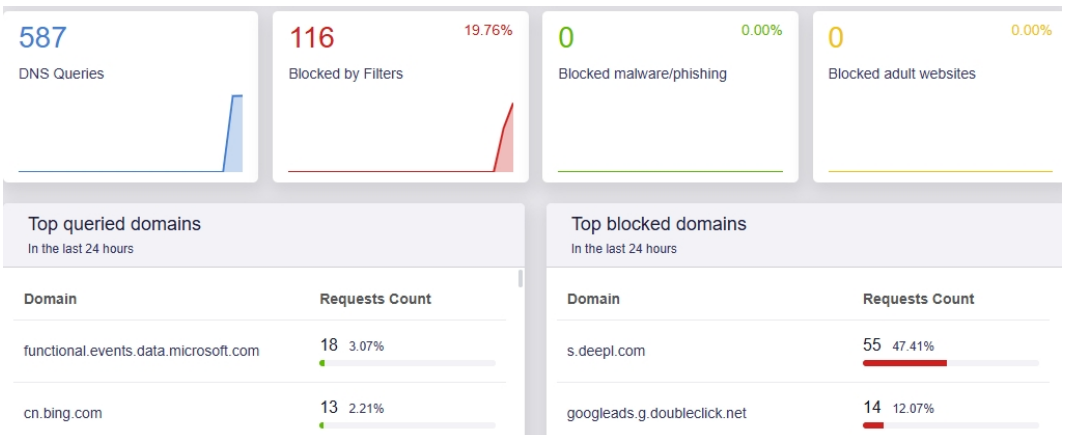
Siga estos pasos para configurar AdGuard Home.

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

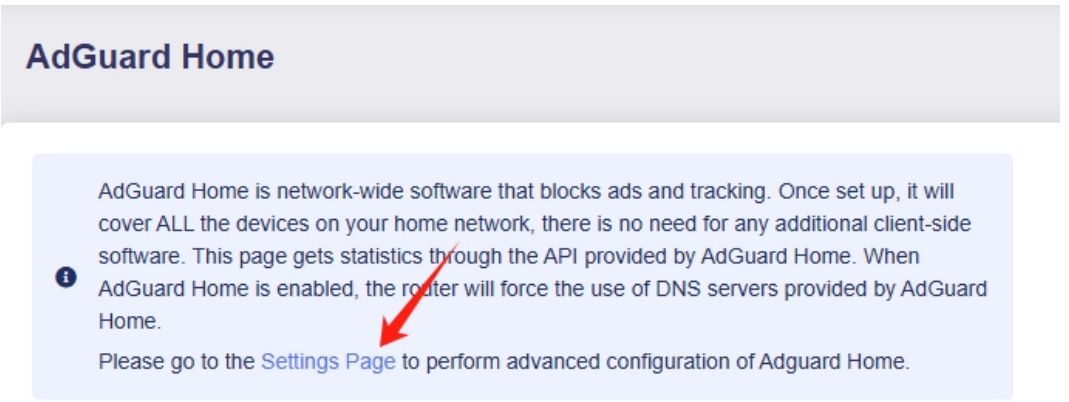


- **Inicio de AdGuard Gestionars solicitudes de clientes**: si está habilitado, las consultas de DNS de los dispositivos cliente serán manejadas directamente por AdGuard Home, pero esto hará que las políticas de VPN basadas en dominios fallen.

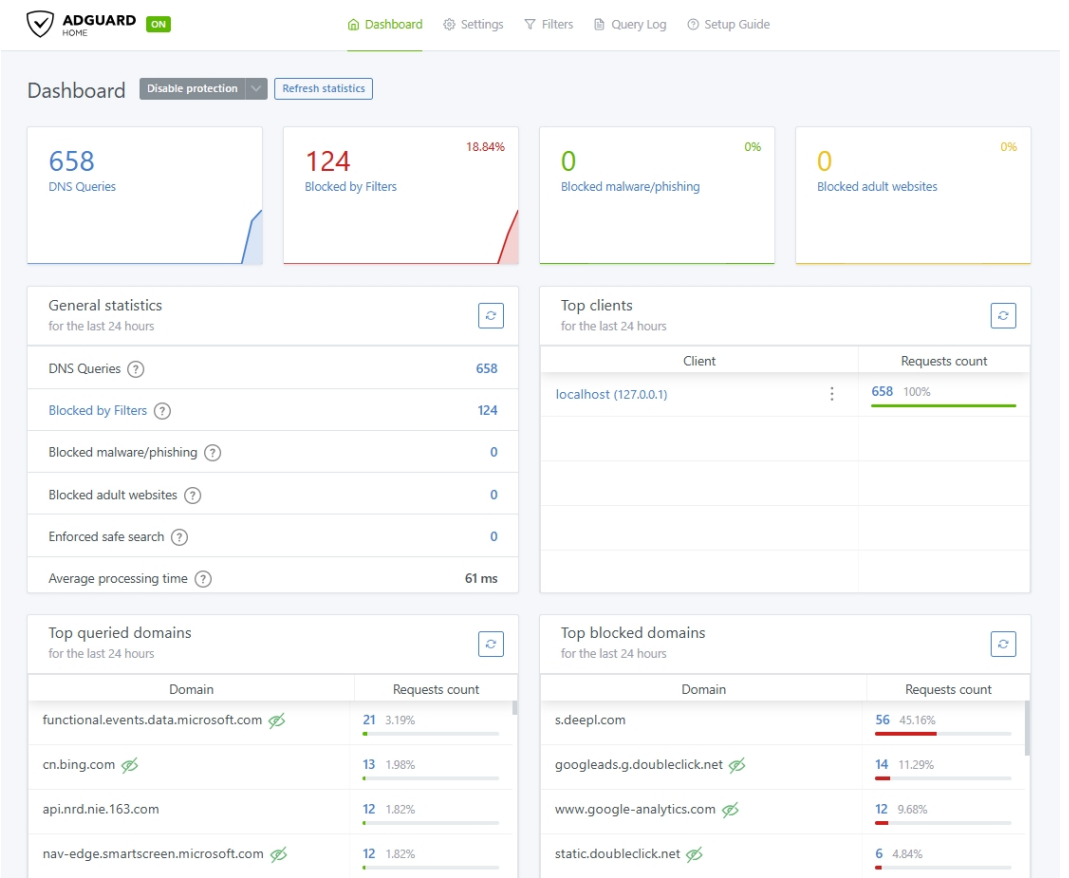
2. La página cargará automáticamente estadísticas de DNS (consultas, bloqueadas) dominios, etc.) a través de la API proporcionada por AdGuard Home.



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



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



14.5 Tailscale

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

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

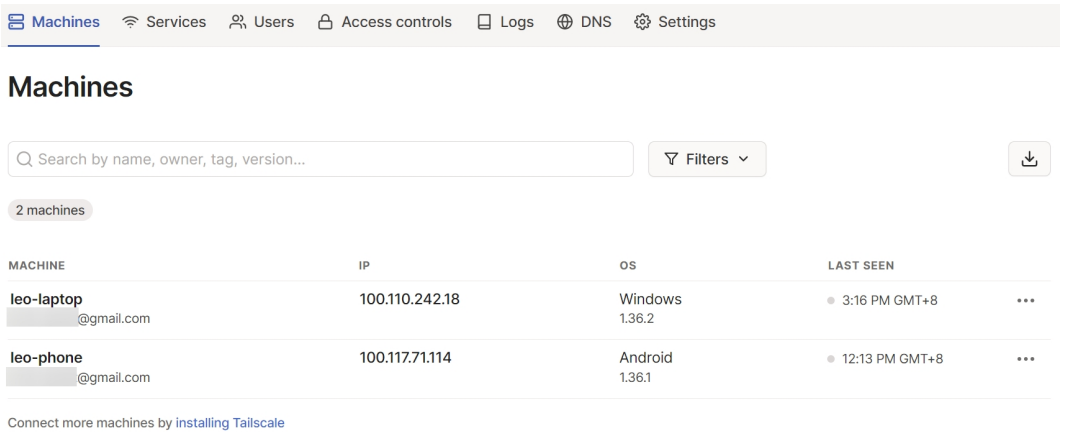
Nota:

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

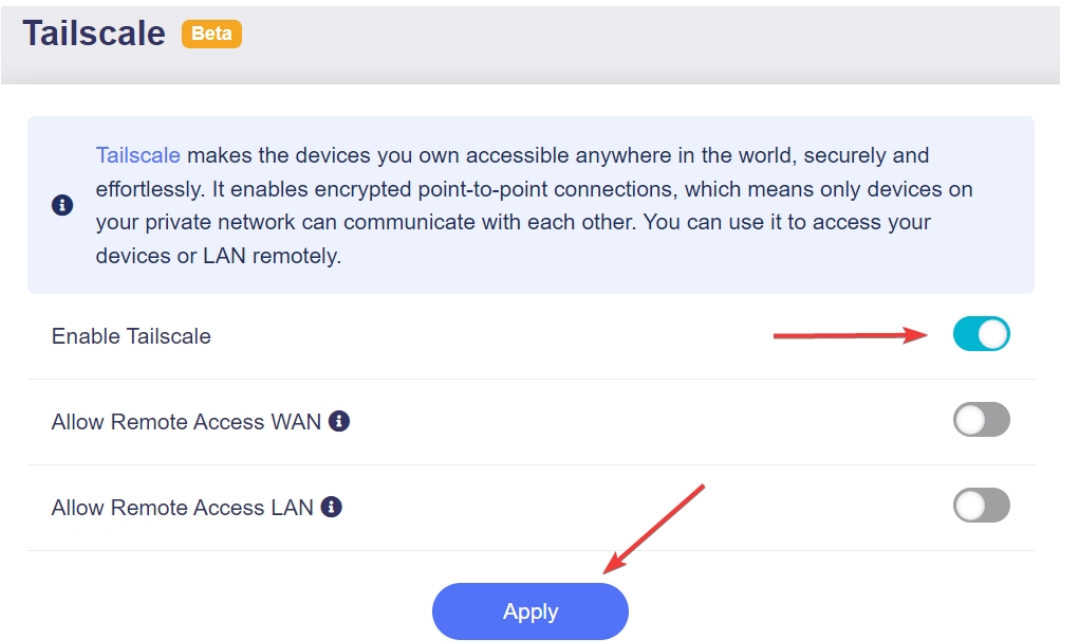
14.5.1 Configurar Tailscale

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

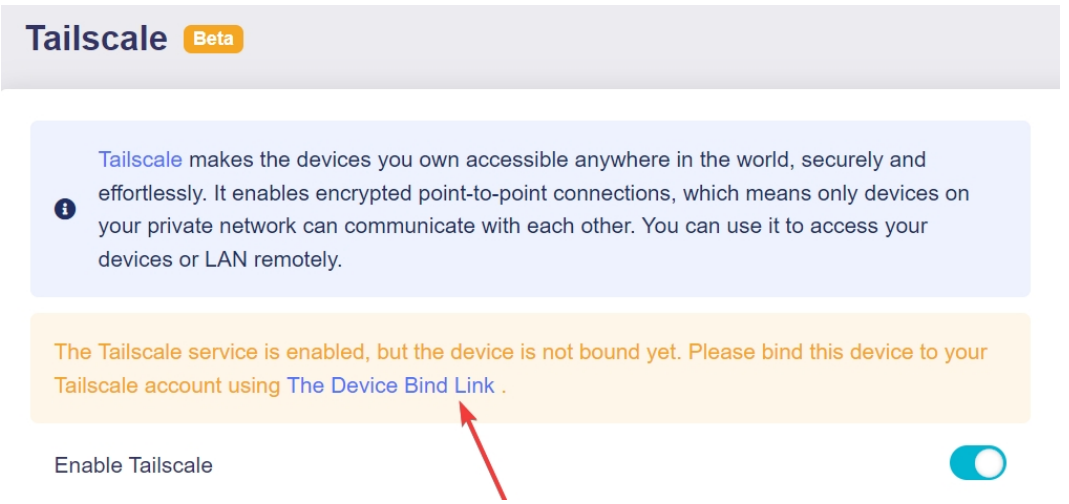
1. Rregistre primero una cuenta de Tailscale y vincule uno o dos dispositivos a su cuenta de Tailscale parao con fines de prueba. Después de vincular, verá sus dispositivos en Tailscale Console.



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



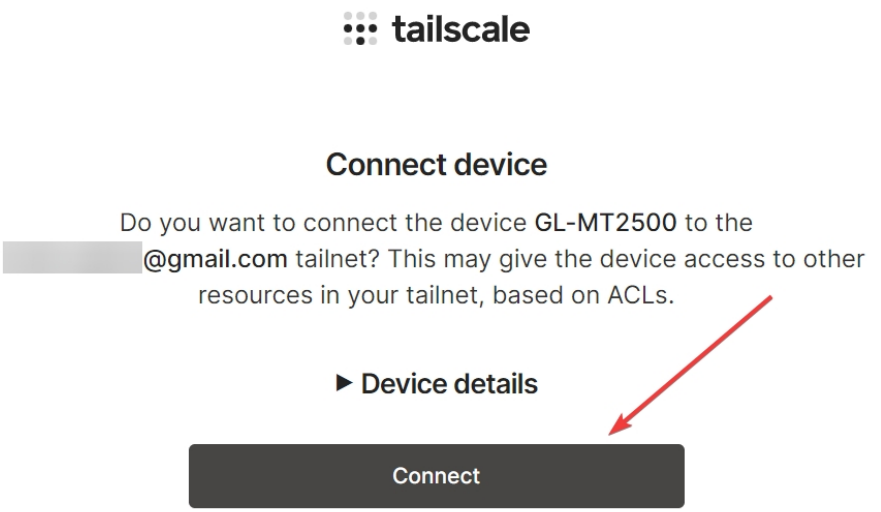
3. La página le pedirá que vincule el dispositivo. Haga clic **Enlace de enlace de dispositivo**.



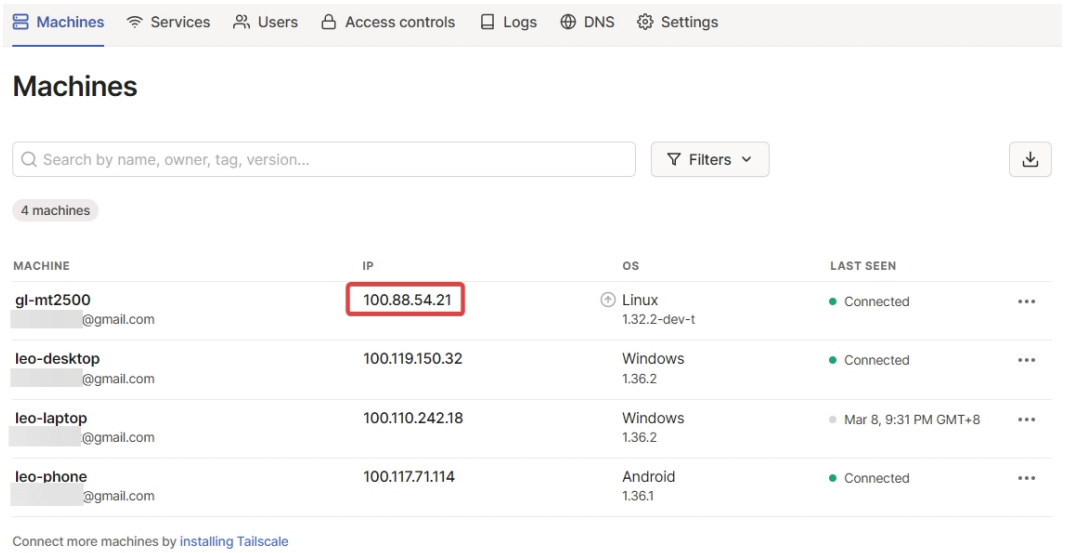
4. En la ventana emergente, haga clic en el enlace e inicie sesión con su cuenta de Tailscale.



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



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

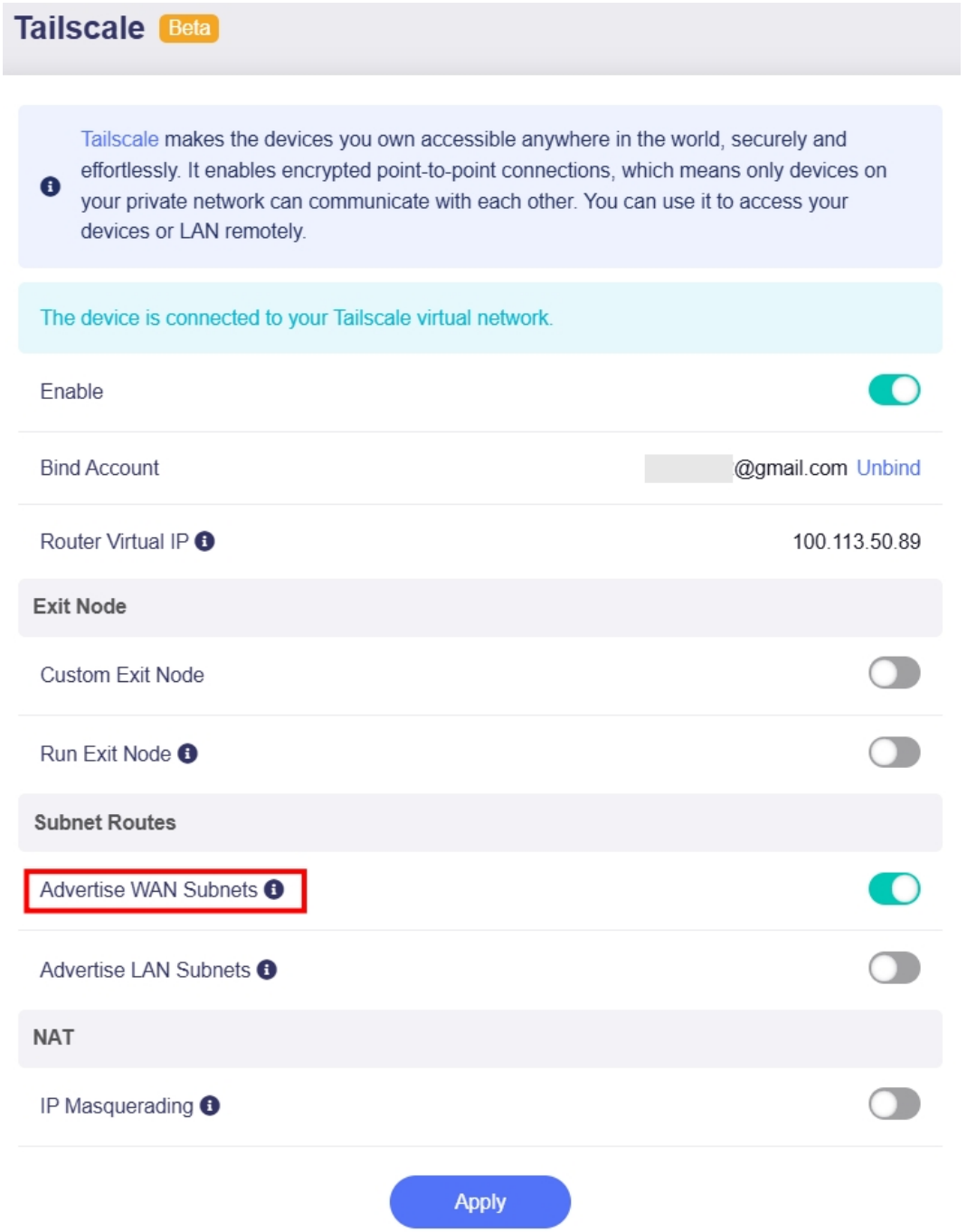


7. Pruebe la conectividad.

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

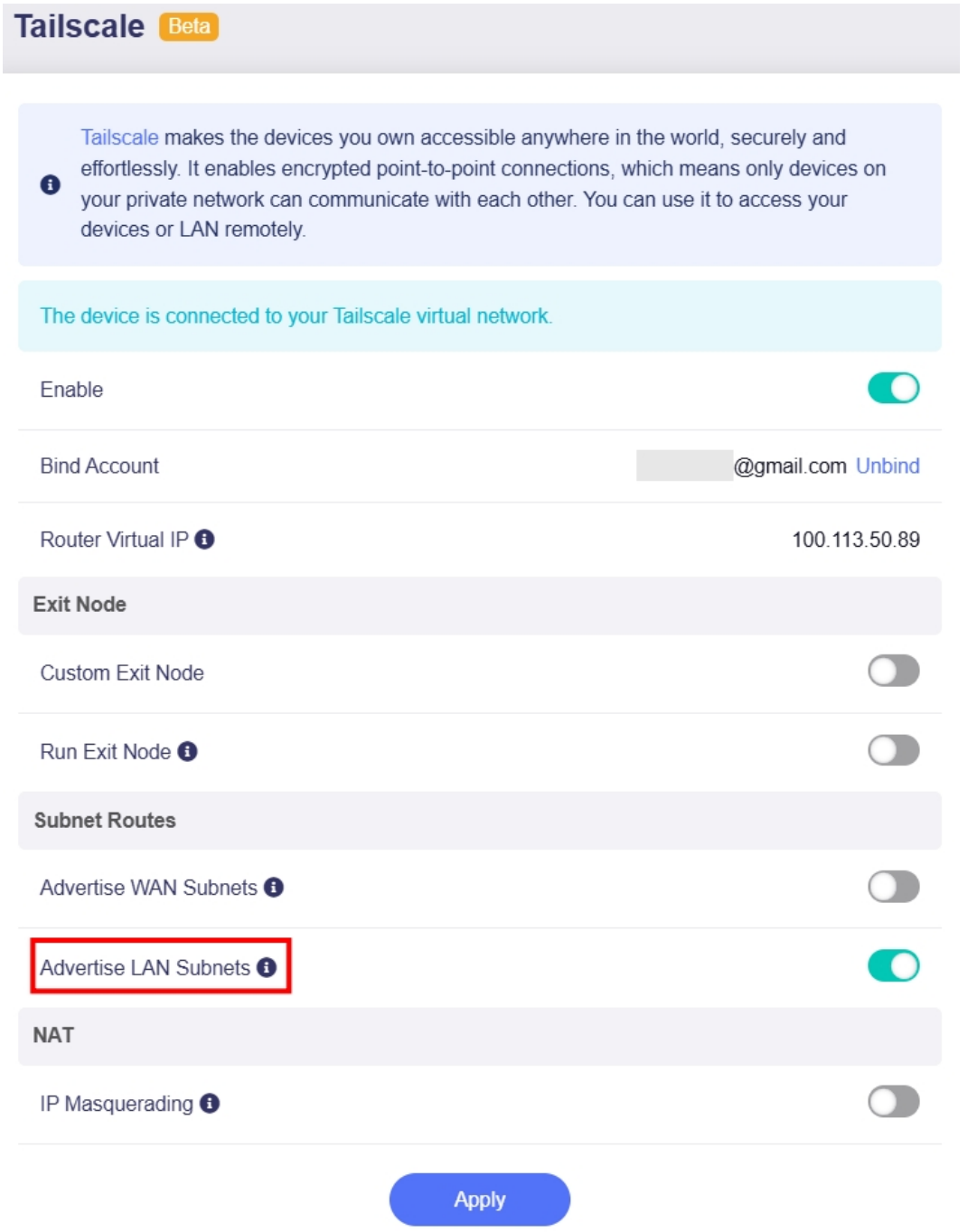
14.5.2 Anunciar subredes WAN

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



14.5.3 Anunciar subredes LAN

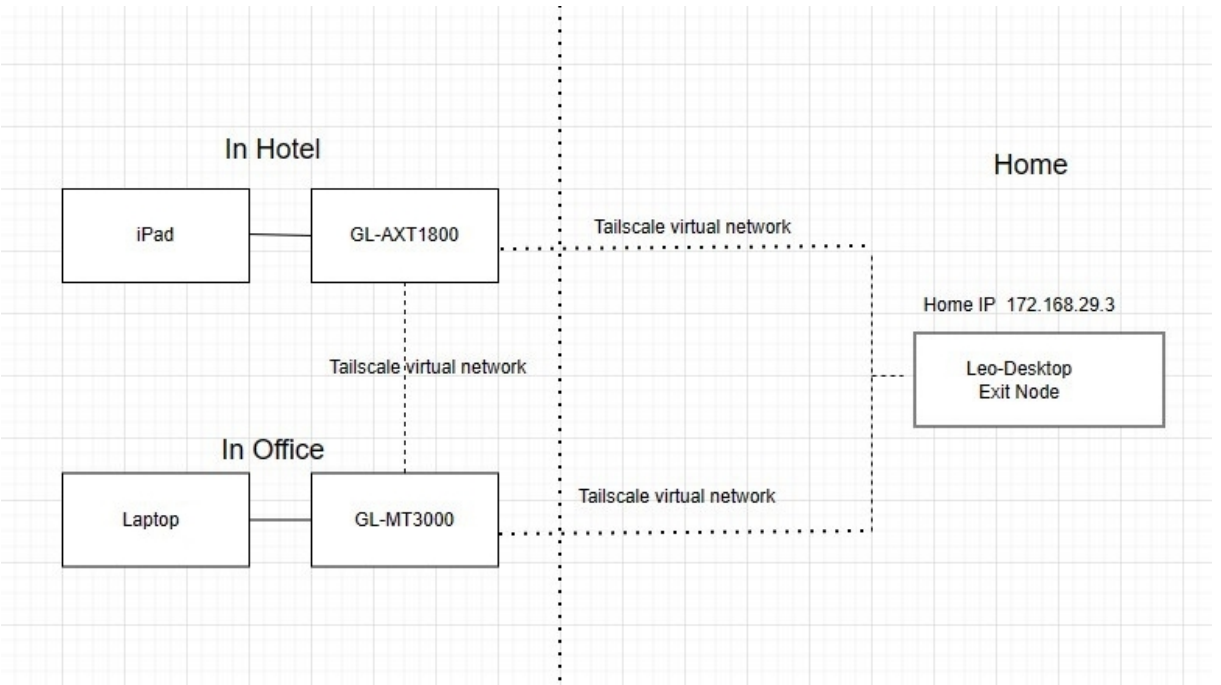
Si esta opción está habilitada, se puede acceder a los recursos en el lado LAN del dispositivo a través de la red virtual Tailscale. Consulte aquí para obtener más detalles.



14.5.4 Nodos de salida personalizados

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

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



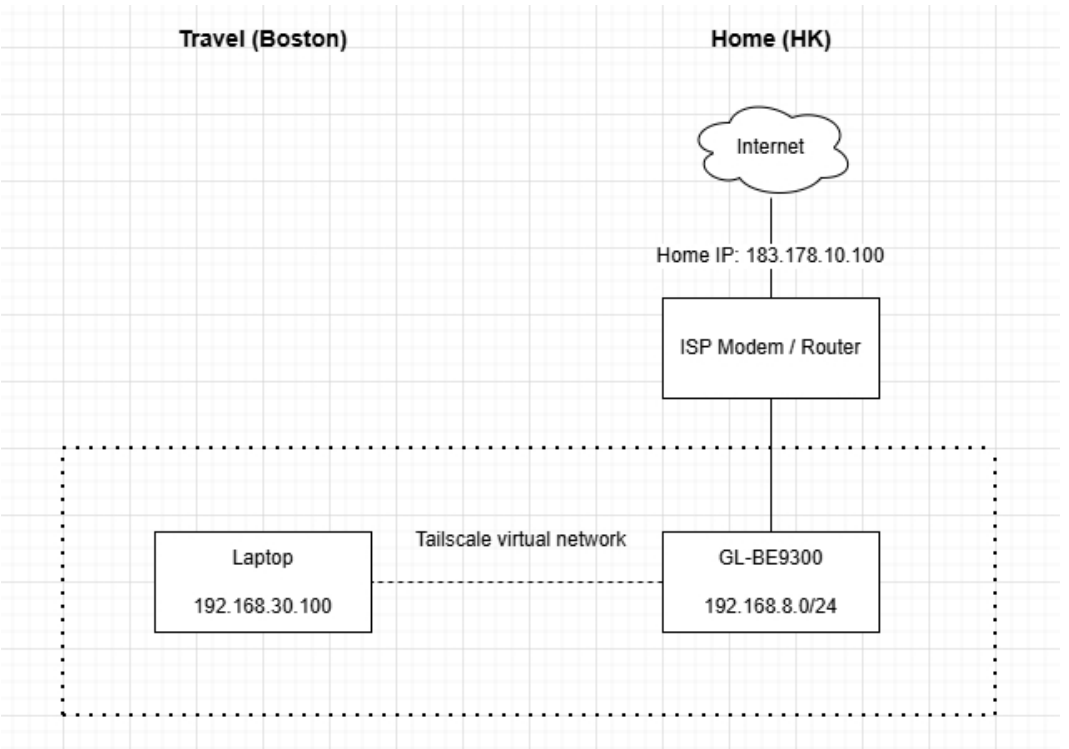
En resumen, un nodo de salida enruta el tráfico de Internet saliente desde sus dispositivos Tailnet, actuando efectivamente como servidores VPN. Cuando se conecta a un nodo de salida, todo su tráfico de Internet que no es de Tailscale parece originarse desde su ubicación, lo que le ayuda a acceder a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

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

14.5.5 Activar el nodo de salida

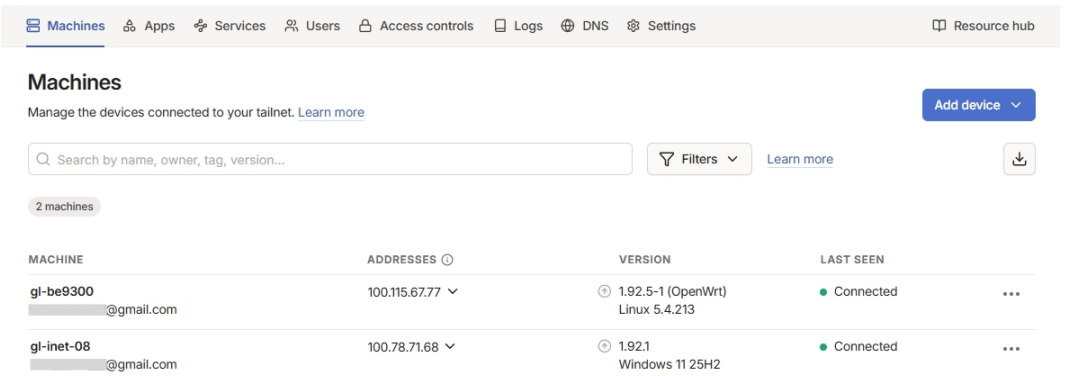
La ejecución de un nodo de salida en su enrutador permite que otros dispositivos dentro de su tailnet enruten todo el tráfico de Internet saliente a través de la IP pública de este enrutador.

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

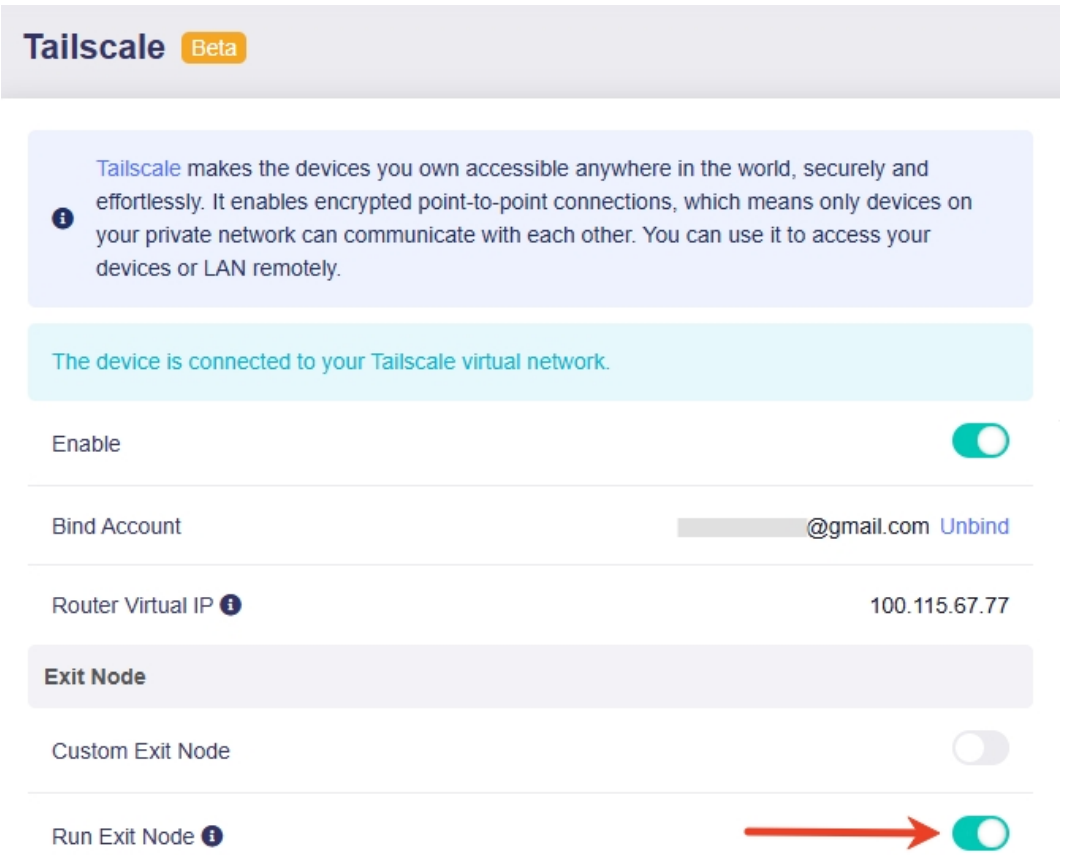


Aquí se muestra un ejemplo de configuración de un enrutador GL-BE9300 como nodo de salida.

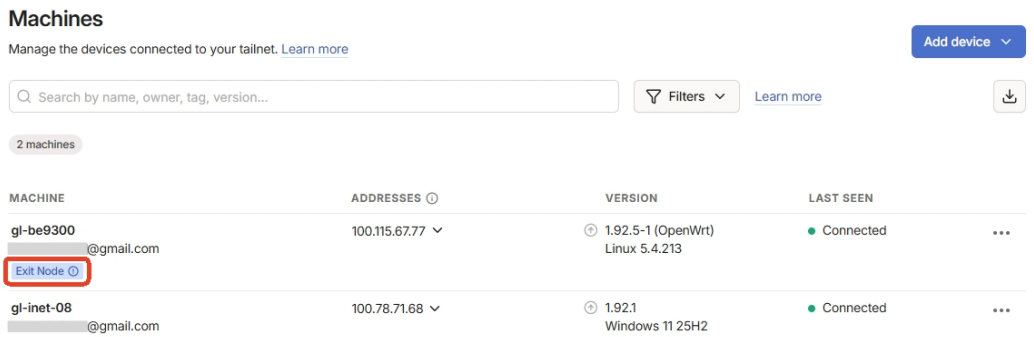
1. Inscriba ambos GL-BE9300 y computadora portátil de viaje a la misma red trasera de Tailscale.



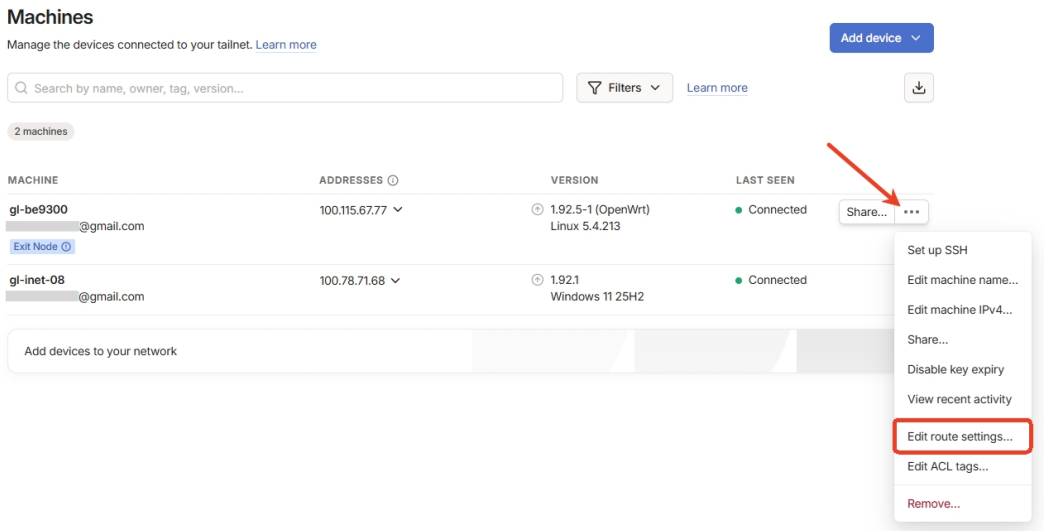
2. En el panel de administración web GL-BE9300, vaya a APLICACIONES > Tailscale. habilite **Activar el nodo de salida** y haga clic en **Aplicar**.



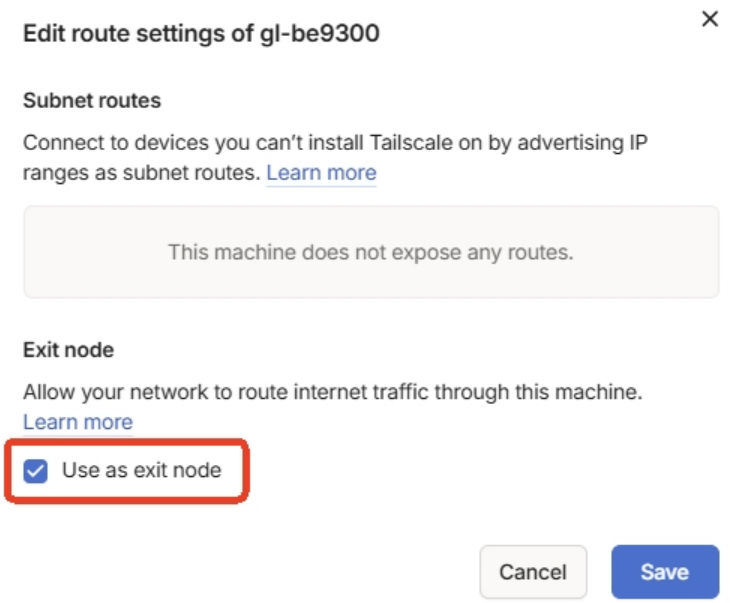
3. Vaya a la consola de administración de Tailscale y verá una etiqueta "Nodo de salida" debajo del GL-BE9300.



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



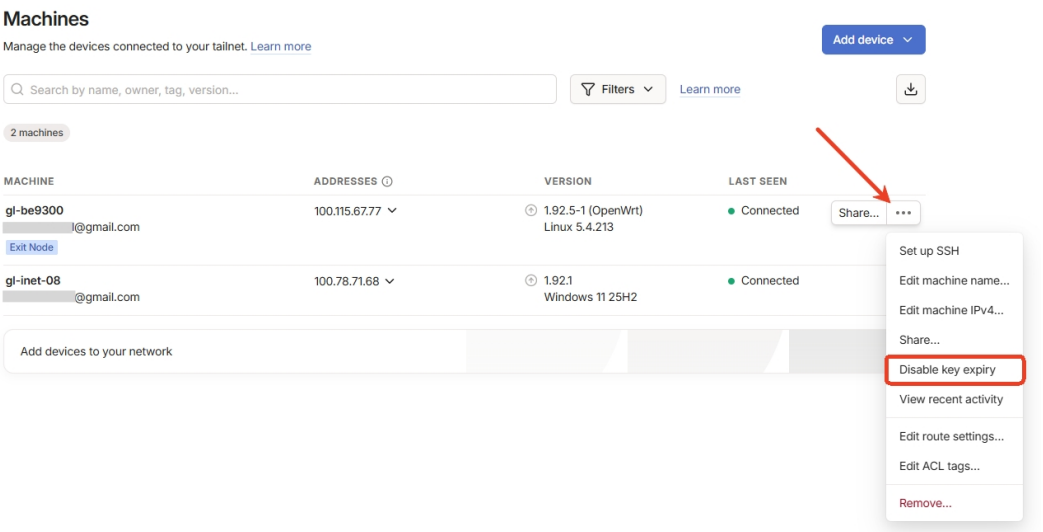
5. En la ventana emergente, marque **Usar como nodo de salida** y haga clic en **Guardar**.



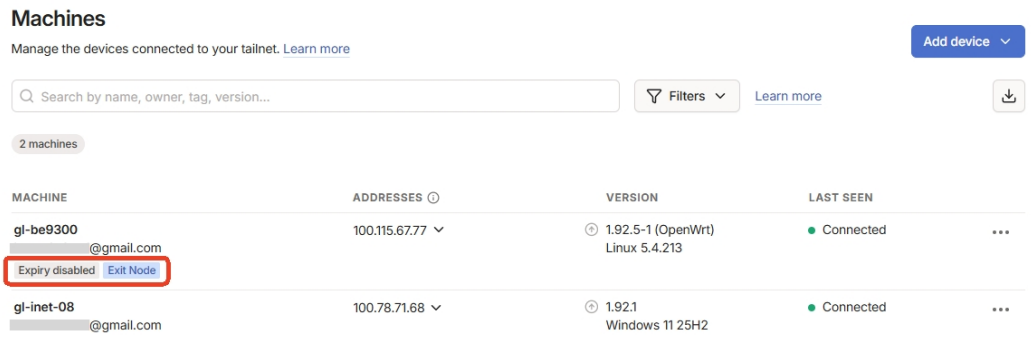
6. Desactivar la caducidad de la clave.

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

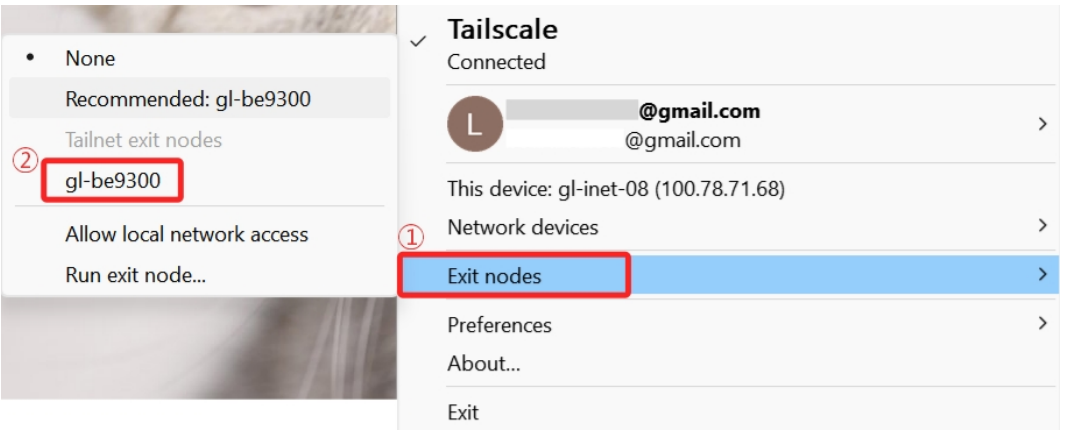
   Haga clic en el icono de tres puntos a la derecha del GL-BE9300 y seleccione Desactivar caducidad de la clave.



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



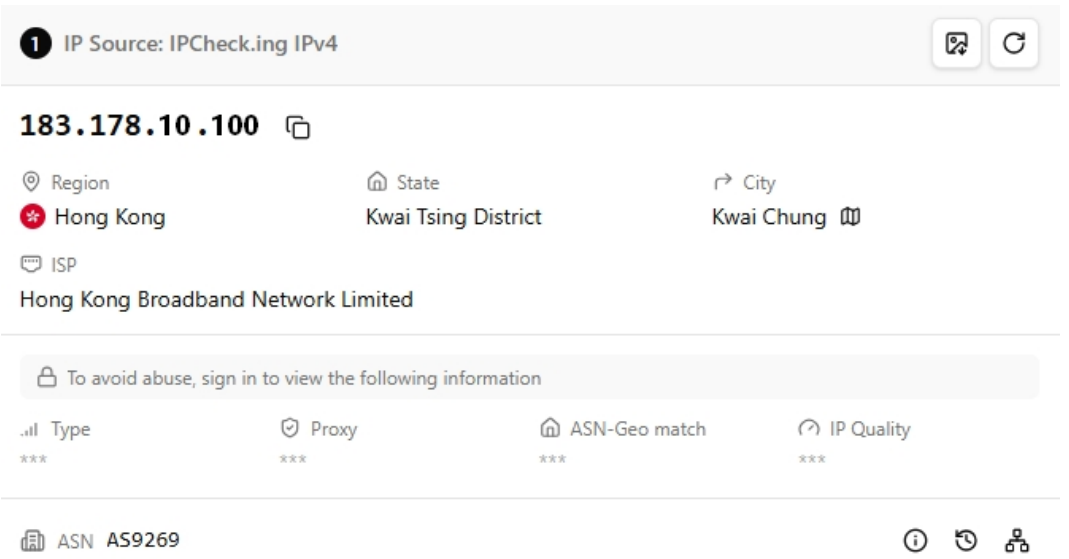
7. Ejecute Tailscale en su computadora portátil de viaje. El icono de Tailscale aparecerá en la bandeja del sistema en la esquina inferior derecha. Haga clic con el botón derecho en el icono, haga clic en **Salir de nodos** y seleccione **gl-be9300**.



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

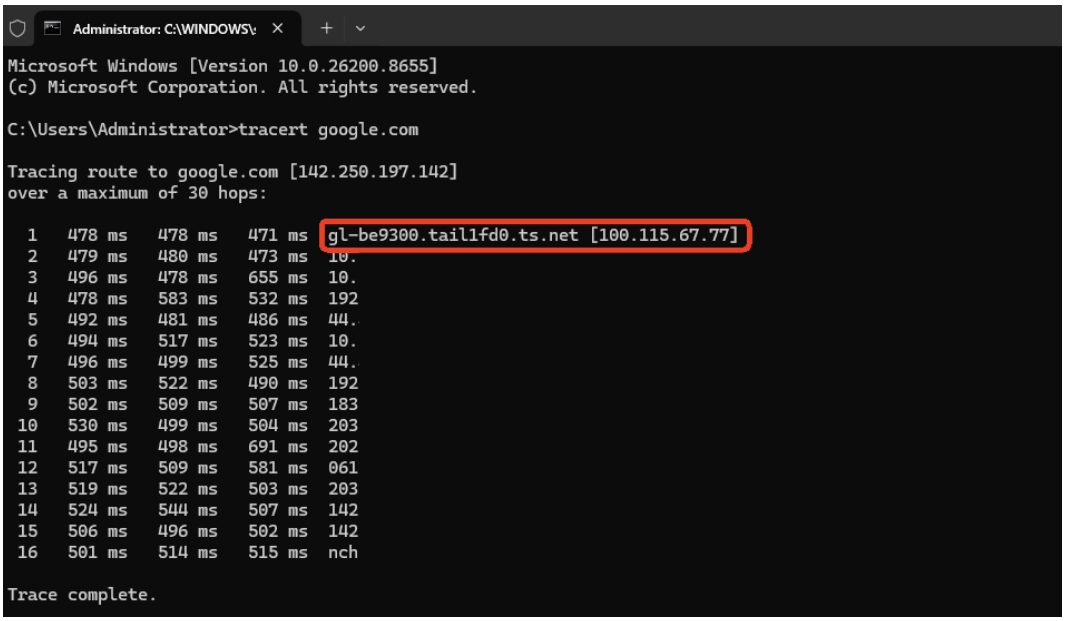
8. Pruebe la conectividad.

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

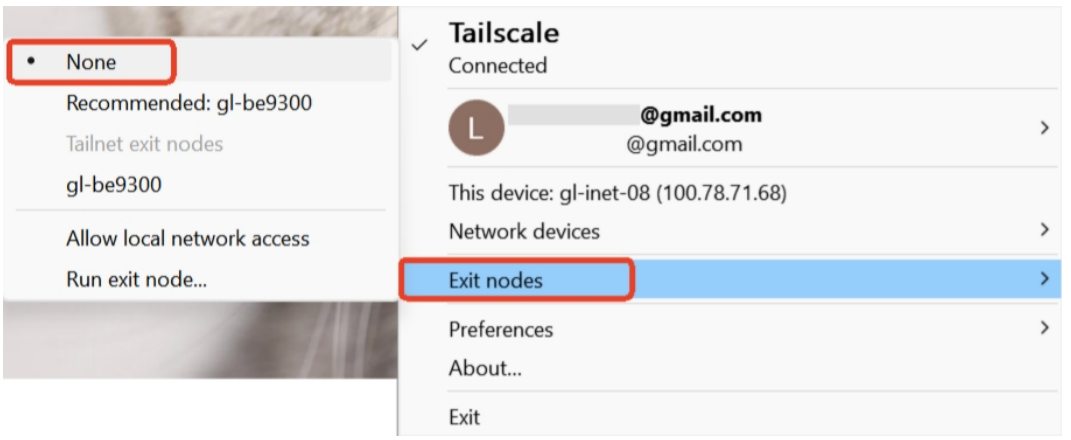


(2) Presione *Win+R*, escriba *cmd* para iniciar el símbolo del sistema y luego ejecute *tracert google.com* para rastrear las rutas de tráfico saliente. El resultado del comando enumera todos los saltos de enrutamiento para su tráfico de Internet. Si se configura correctamente, el primer salto externo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

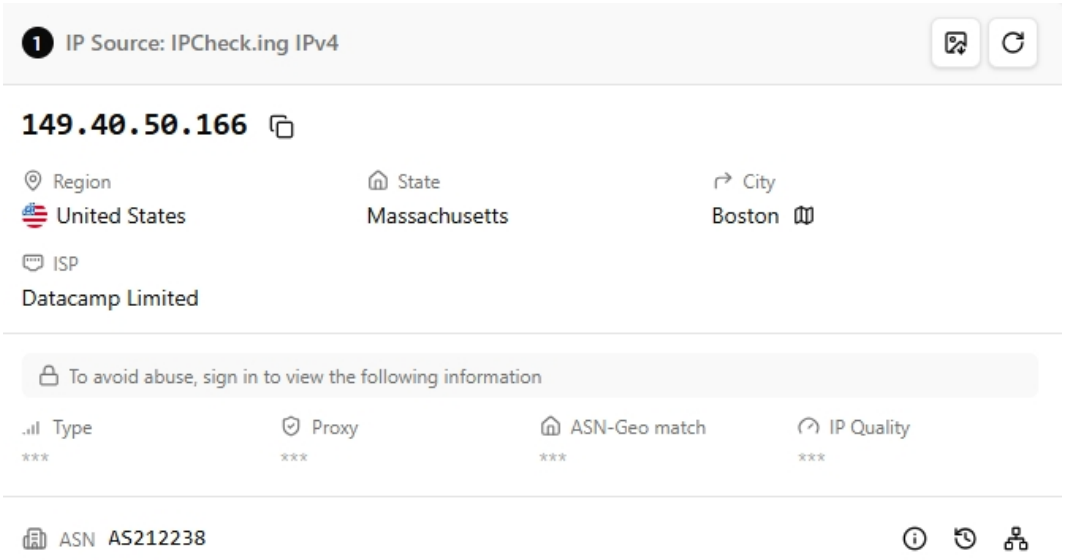
como se muestra a continuación, verificando todas las salidas del tráfico de Internet saliente a través de este enrutador.



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



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


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

14.6 ZeroTier

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

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

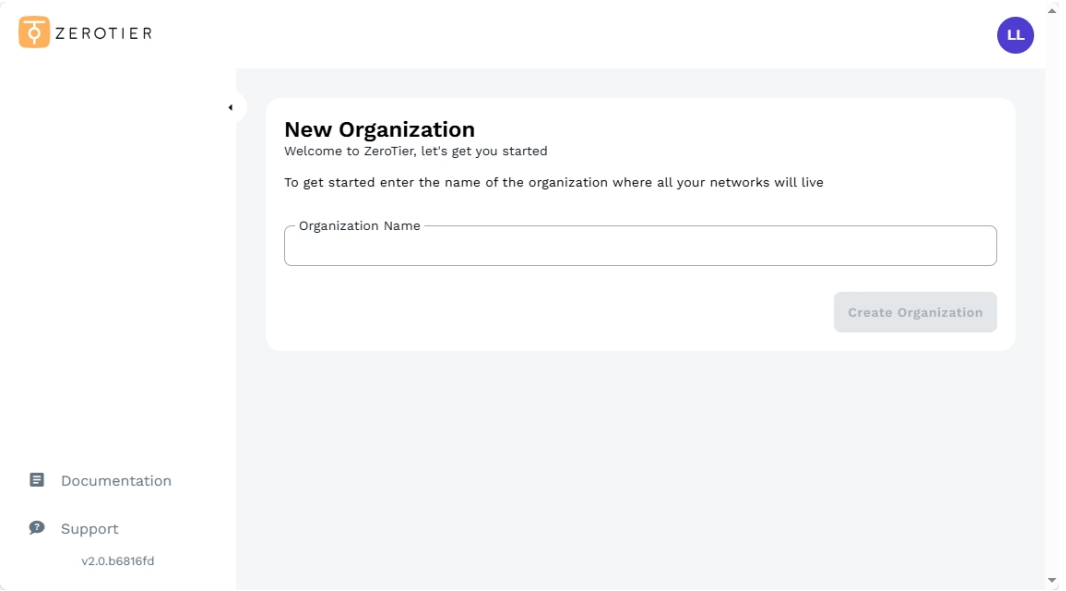
Nota:

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

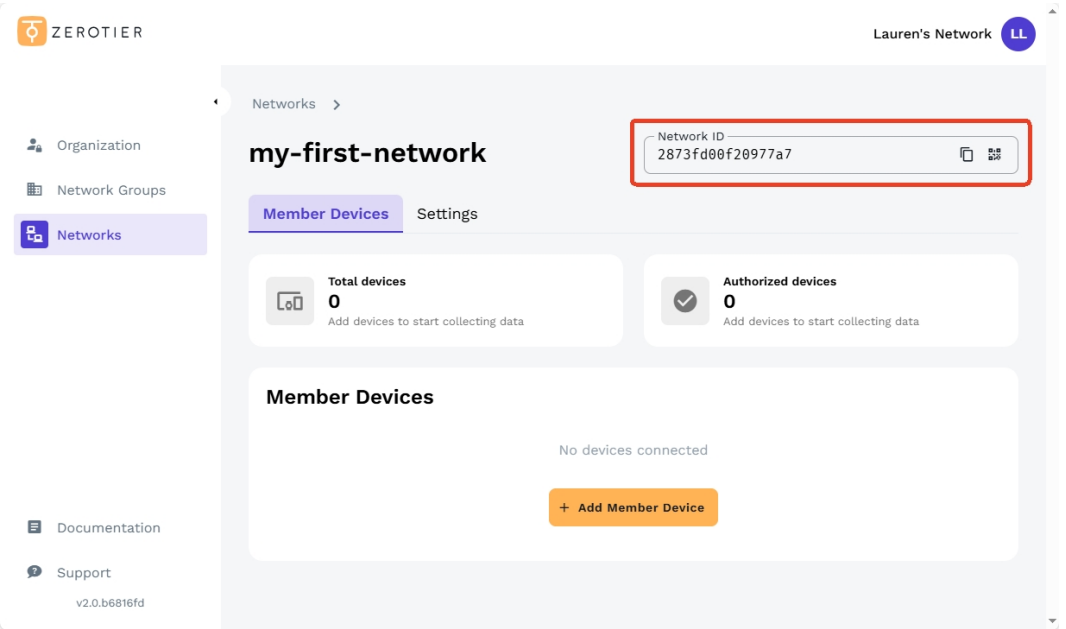
14.6.1 Configurar ZeroTier

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

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

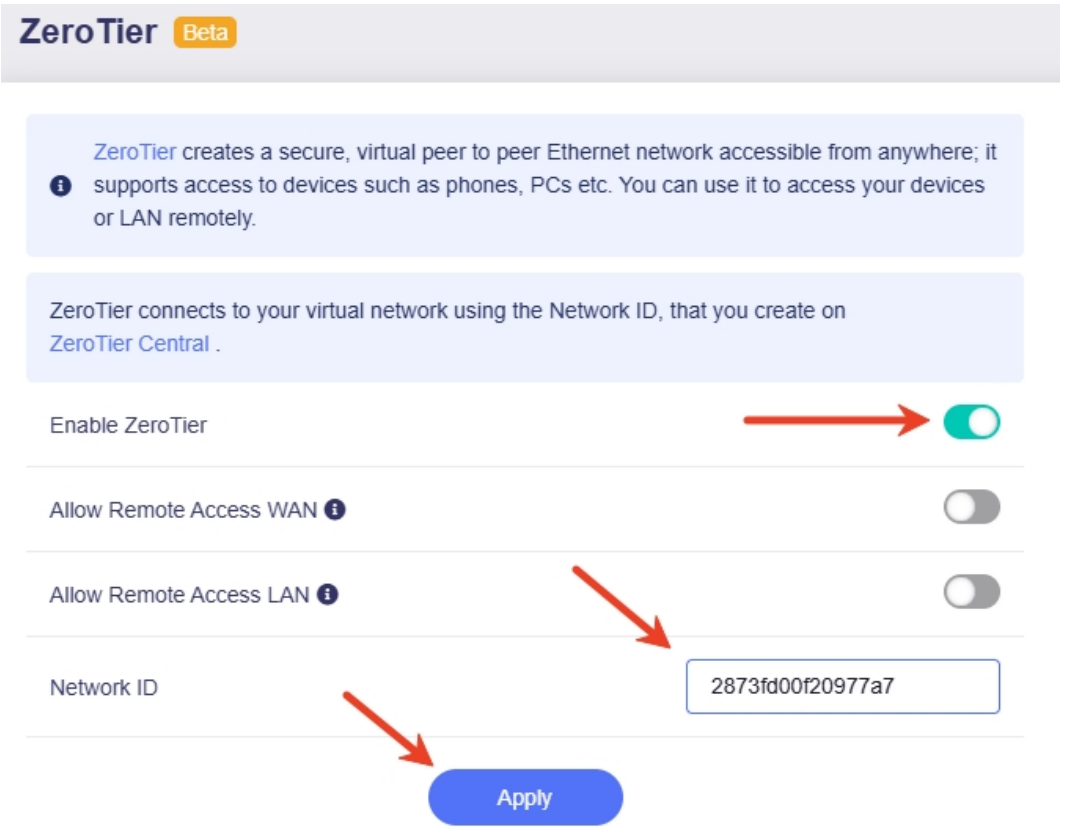


3. Seleccione un plan. Aquí elegimos **plan personal** como ejemplo, que incluye 10 dispositivos, 1 administrador de red y 1 red. Si necesita crear más redes, agregar más dispositivos o agregar rutas y DNS personalizados, elija otro plan pago.
4. Ahora se ha creado su red ZeroTier.

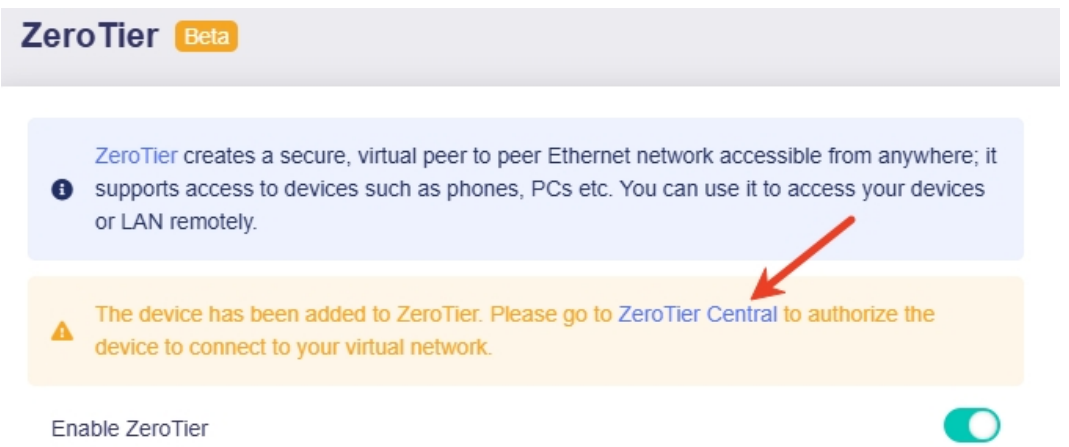


Tome nota del **ID de red**, que es una combinación alfanumérica de 16 caracteres en la esquina superior derecha, ya que será necesaria cuando conecte otros dispositivos más adelante.

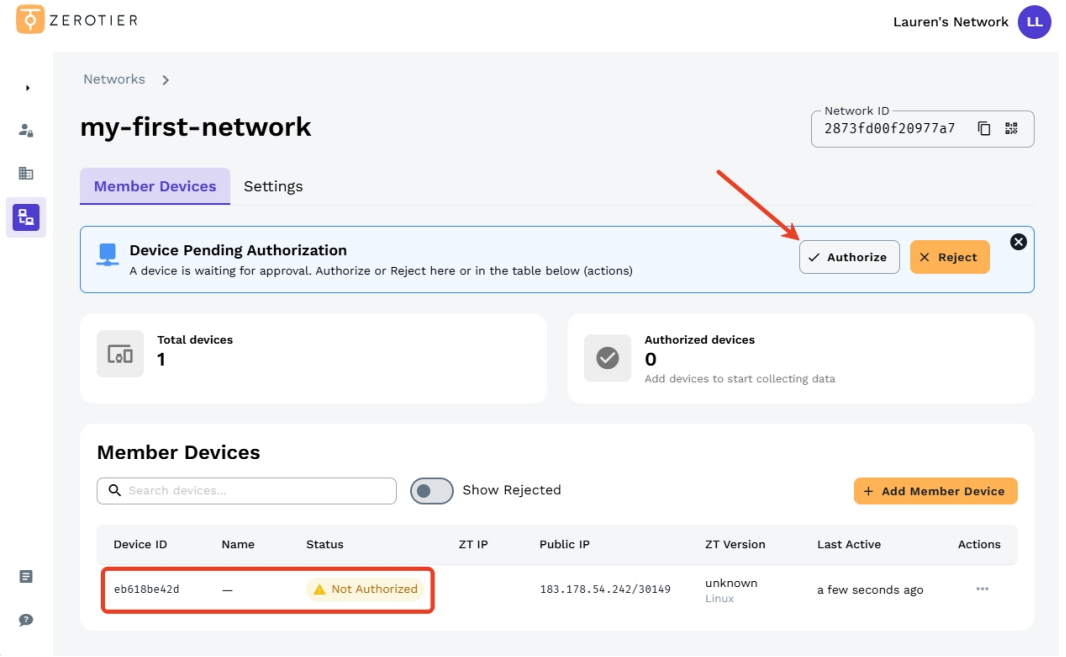
5. Inicie sesión en la web de su enrutador Panel de administración y navegue hasta **APLICACIONES** -> **ZeroTier**. Habilite ZeroTier, ingrese el **ID de red**, luego haga clic en **Aplicar**.



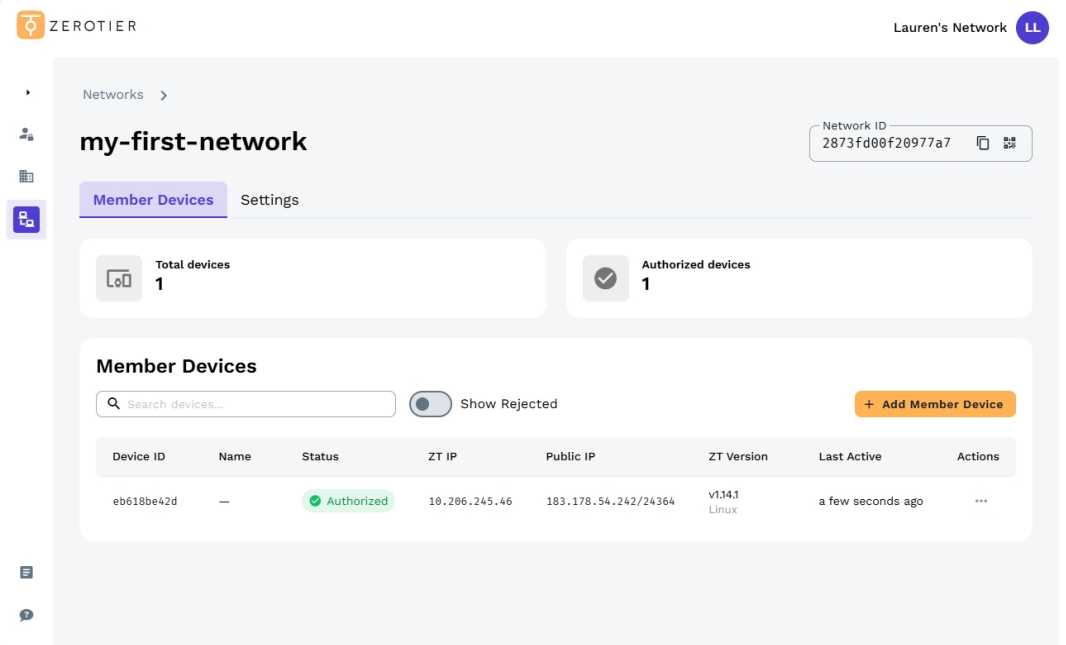
Después de un momento, la página indicará que se requiere autorización. Haga clic en el **ZeroTier Central** hipervínculo para redirigir a ZeroTier Central.



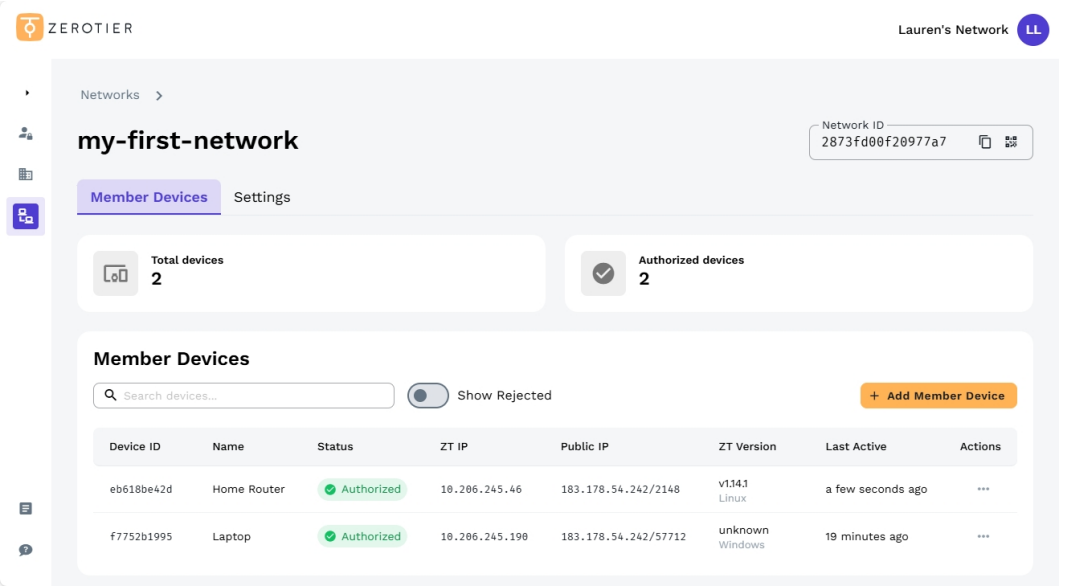
6. En ZeroTier Central, localice el dispositivo pendiente y autorícelo.



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

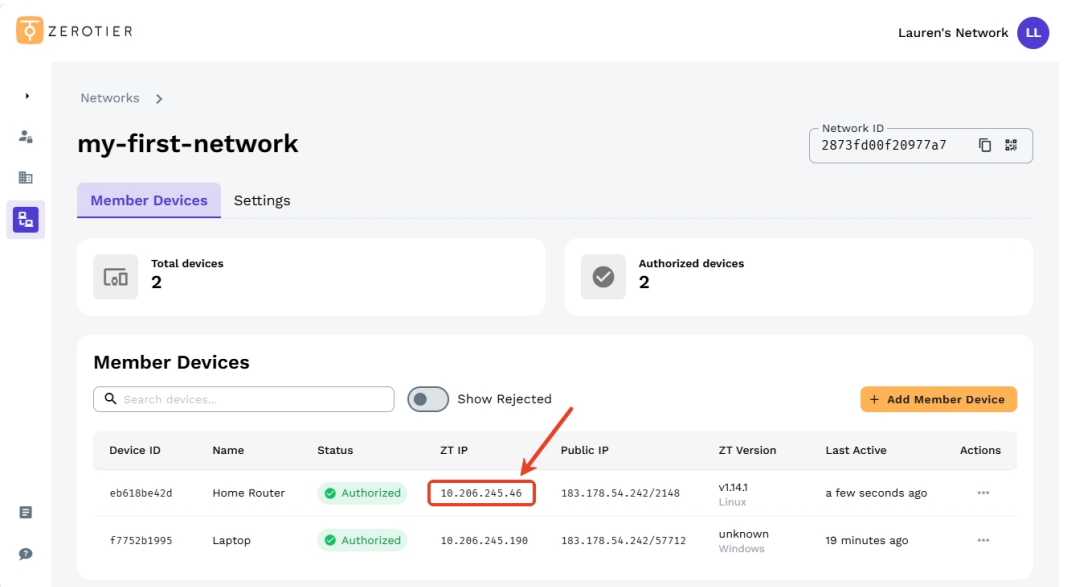


7. Agregue otro dispositivo (como una computadora o un teléfono inteligente) a la misma red ZeroTier siguiendo esta guía. Una vez agregado correctamente, se muestra la página como sigue. Verá los detalles de los dispositivos miembros, como **ID del dispositivo**, **Nombre**, **Estado**, **IP administrada**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



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

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



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

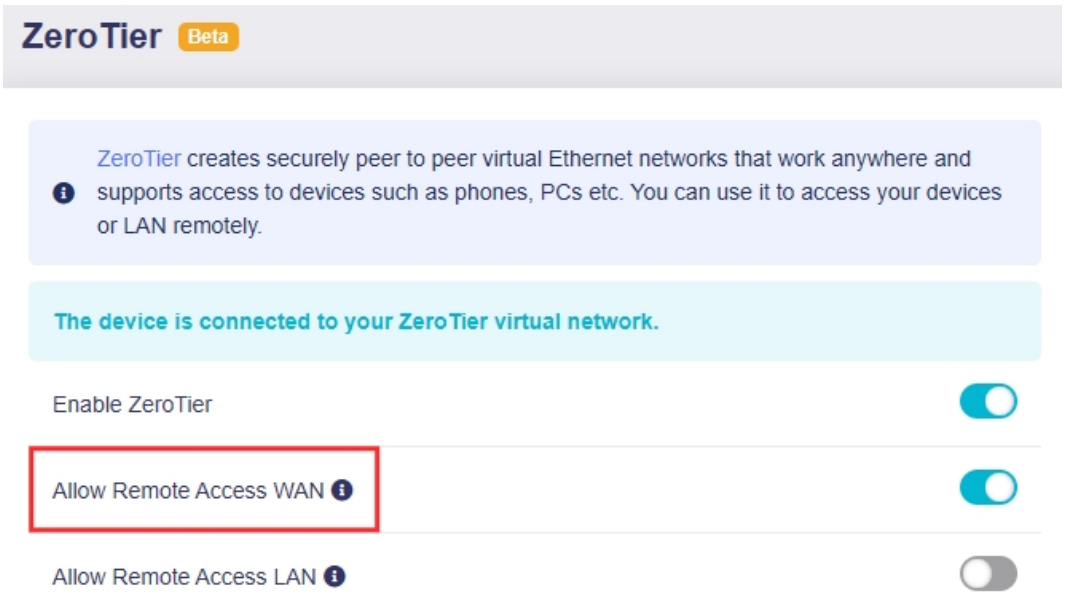
9. Pruebe la conectividad.

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

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

14.6.2 Permitir el acceso remoto a la WAN

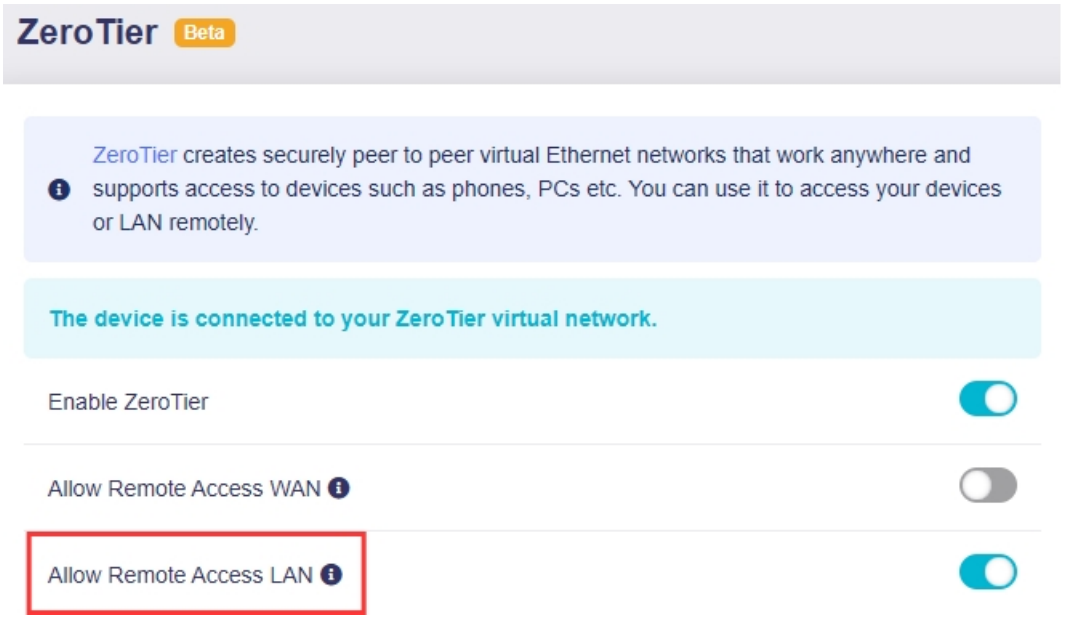
Si esta opción está habilitada, se puede acceder a los recursos en el lado WAN del dispositivo a través de la red virtual ZeroTier. Consulte aquí para obtener más detalles.



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

14.6.3 Permitir el acceso remoto a la LAN

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



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

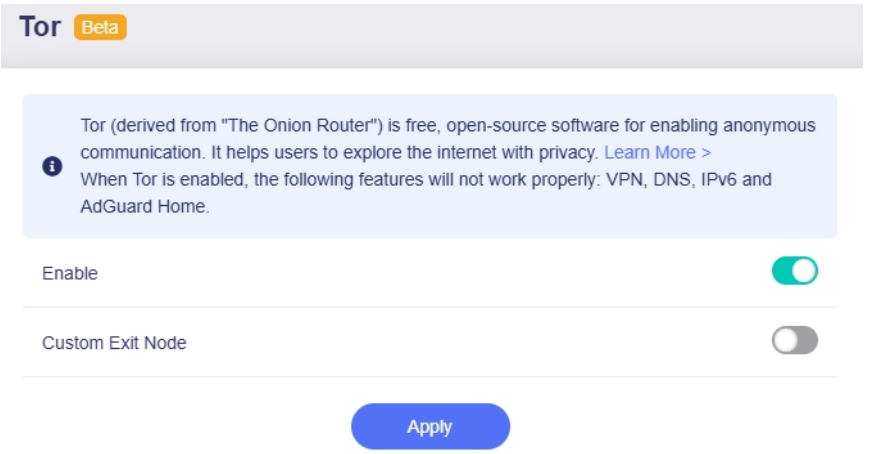
14.7 Tor

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

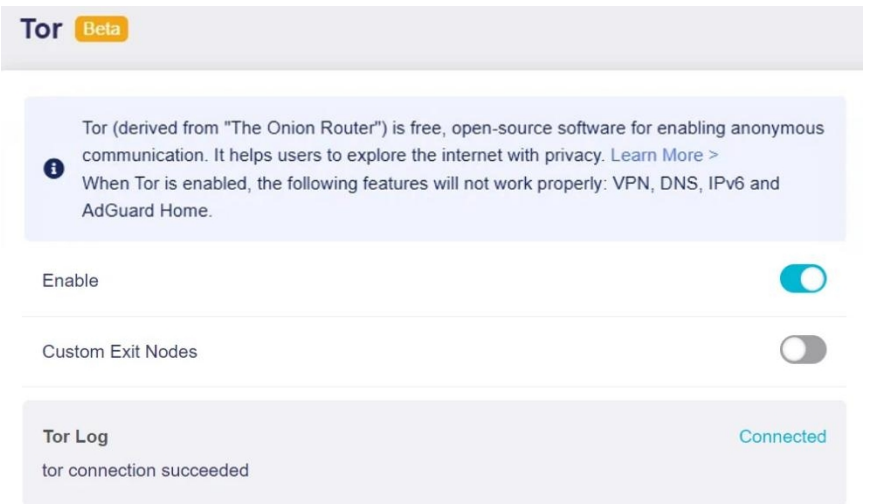
cuando Tor habilitado, laslas siguientes características no funcionarán correctamente: VPN, DNS, IPv6, y AdGuard Home.

Siga los pasos a continuación para configurar Tor según sea necesario.

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



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



Capítulo 15

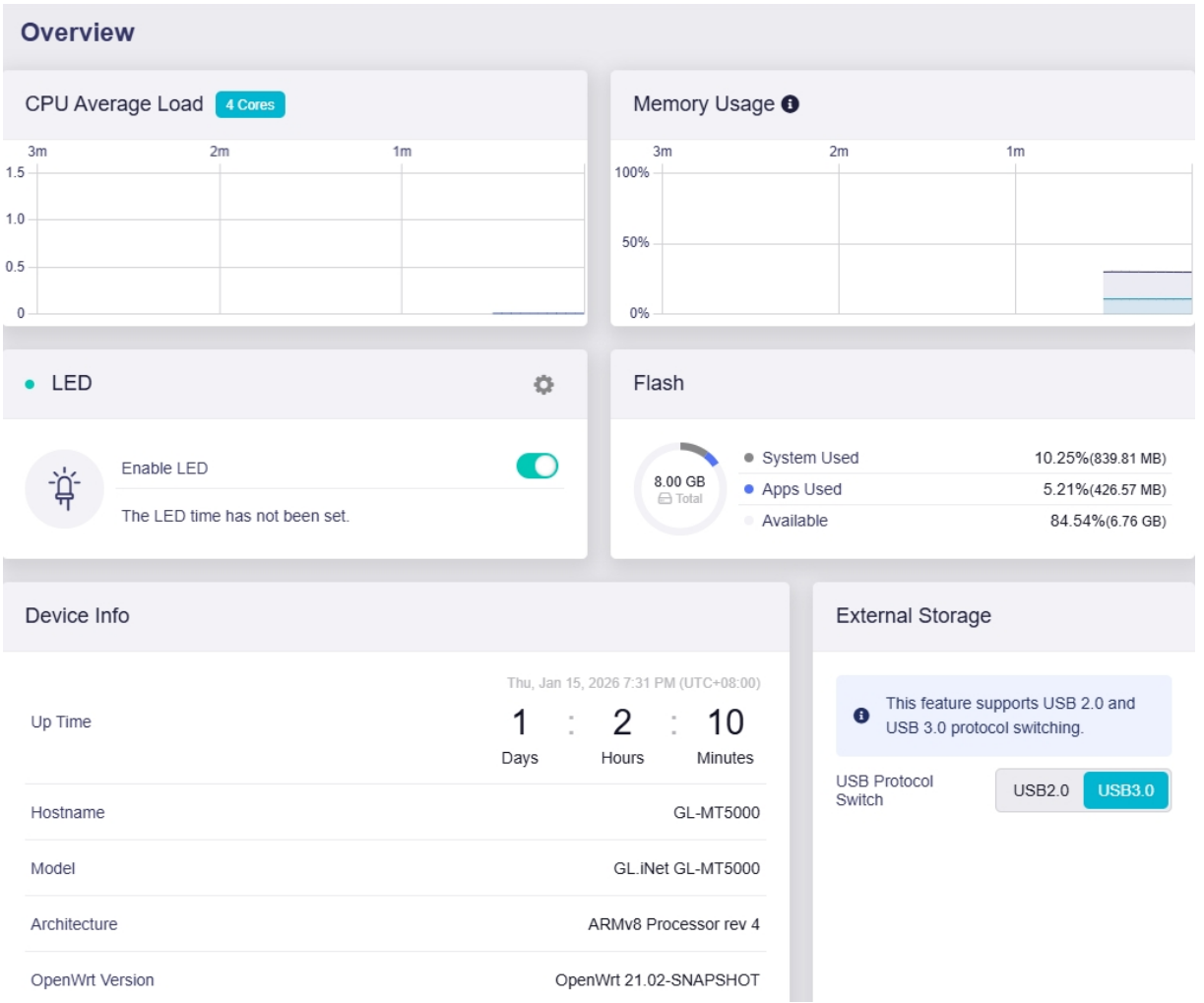
Sistema

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

15.1 Descripción general

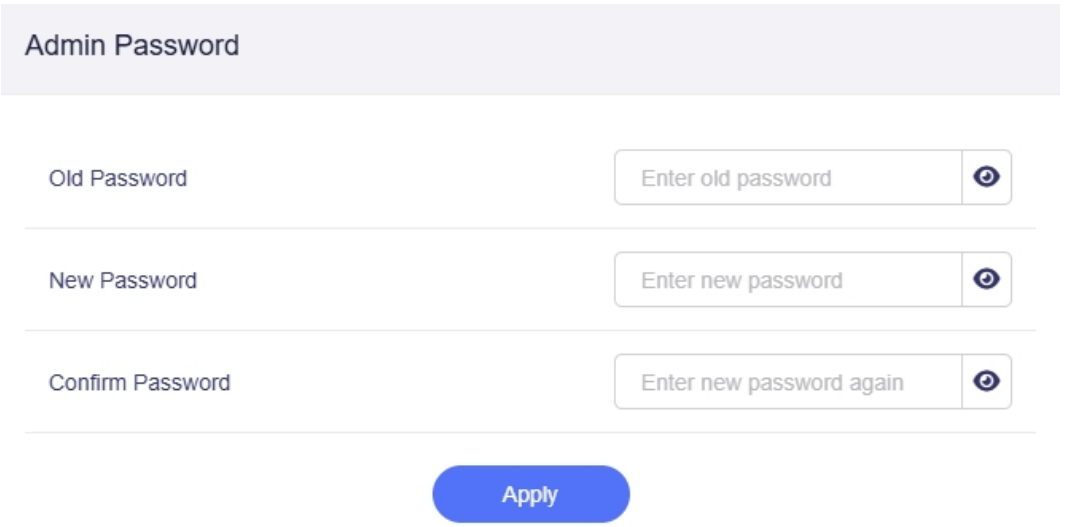
Inicie sesión en el panel de administración web de su enrutador' y navegue hasta **SISTEMA** > **Descripción general**. Esta página muestra estado del hardware y admite algunos controles simples, que incluyen:

- CPU Estado, memoria, flash y dispositivos de almacenamiento externo
- LED Control
- Información del dispositivo



15.2 Contraseña de administrador

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



Los requisitos para la contraseña de administrador son los siguientes:

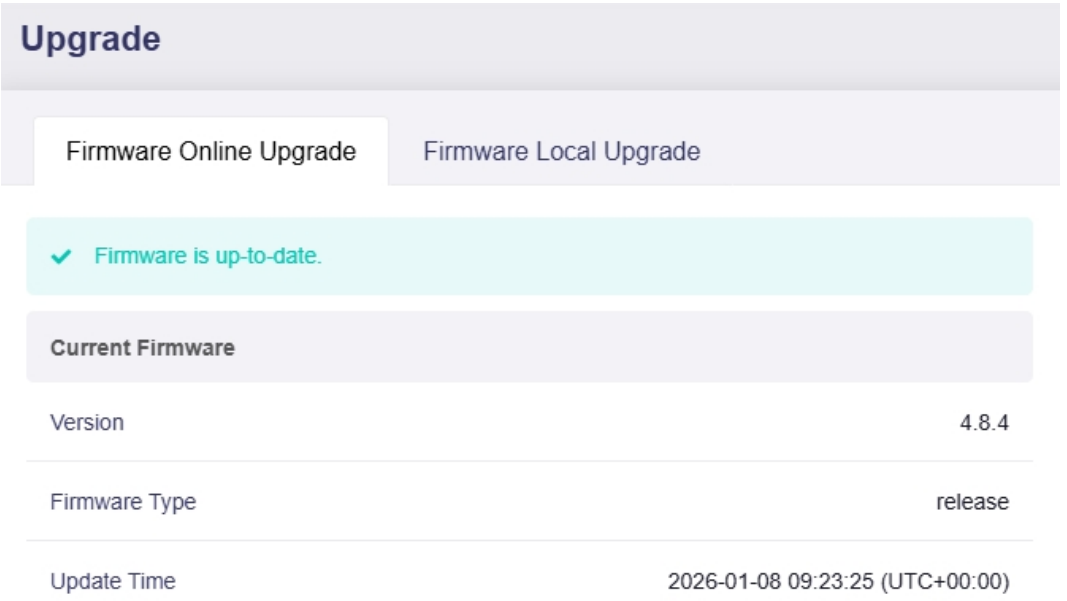
1. Mínimo 10 caracteres y máximo 63 caracteres de longitud.
2. Se permiten letras (distingue entre mayúsculas y minúsculas), números y símbolos (por ejemplo, ! @ # $ % ^ & * ( ) _ + - = , . > < | ? / \ [ ] { } : ; " ' ` ~).
3. Se requieren al menos dos tipos (letras mayúsculas, minúsculas, números y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

15.3 Actualización

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

15.3.1 Actualización en línea

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



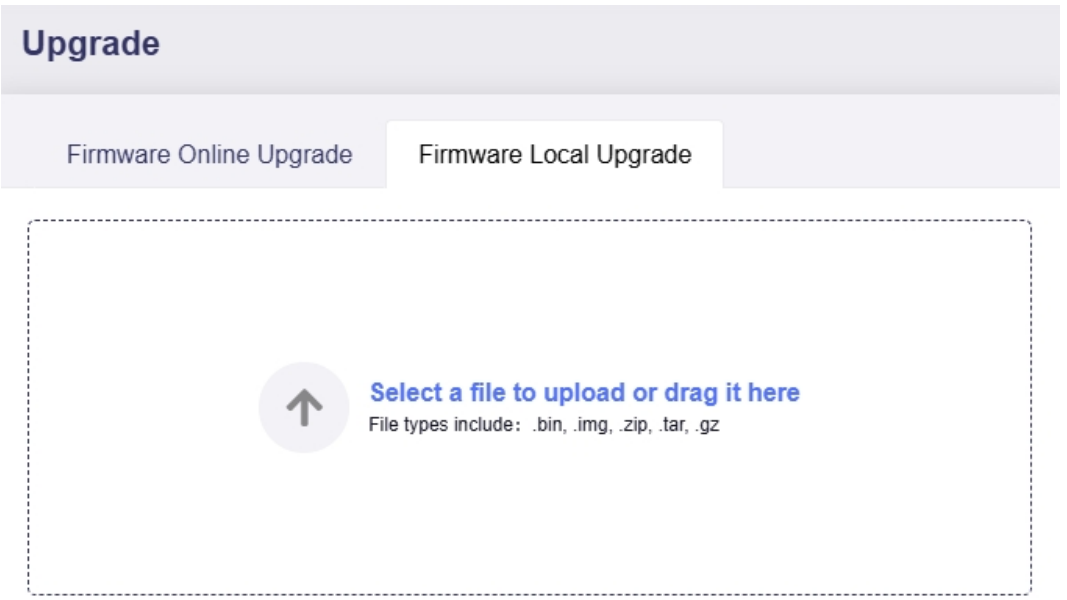
Si su enrutador está conectado a Internet, buscará la versión de firmware más reciente disponible para descargar.

Consejos: Cuando intente realizar una actualización en línea, si muestra **Descarga fallida**, por favor navegue hasta **SISTEMA** -> **Zona horaria** y solucione el error de zona horaria (sincronización con el navegador).

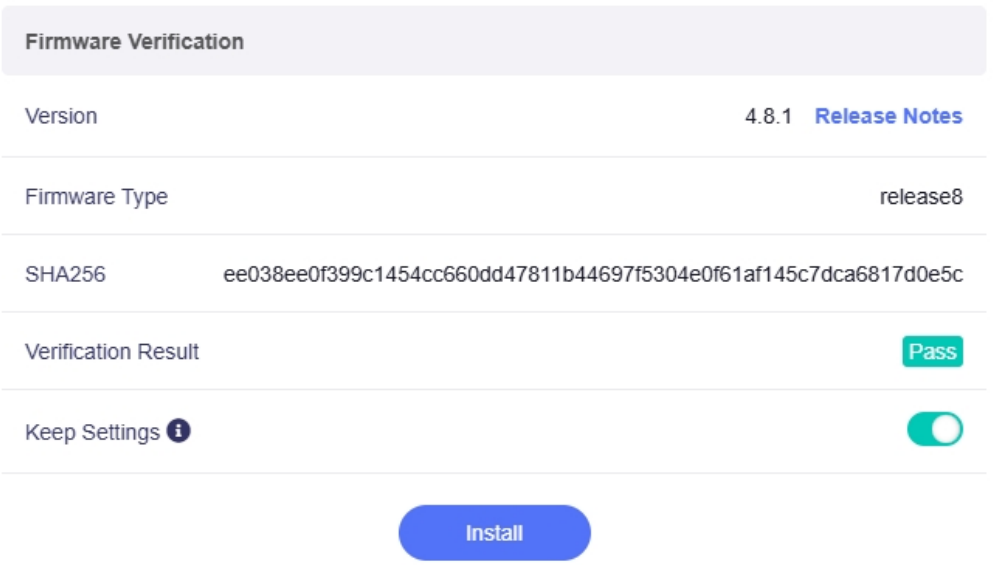
15.3.2 Actualización local

Este método no depende de una conexión a Internet para el enrutador.

Descargue el paquete de firmware correcto (que coincida con el modelo de su enrutador) desde el Centro de descargas oficial a su dispositivo local. Luego inicie sesión en el's panel de administración web del enrutador, navegue hasta **SISTEMA** > **Actualización** > **Actualización local** y cargue el paquete de firmware.



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



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

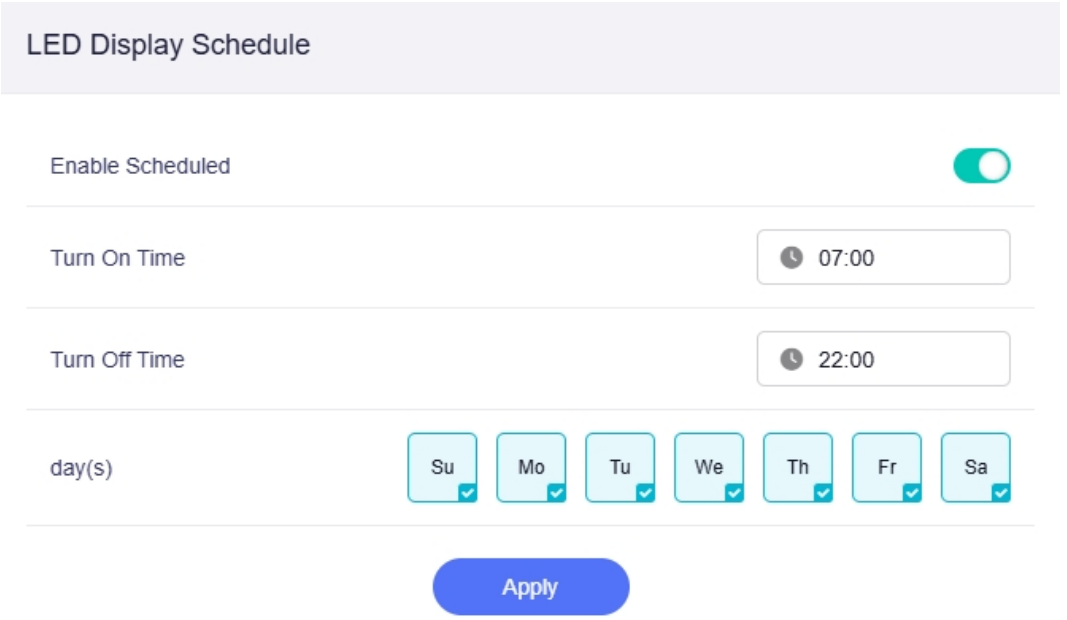
15.4 Tareas programadas

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

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

15.4.1 Programación de los indicadores LED

Esta función le permite configurar un programa para la luz LED de su enrutador.

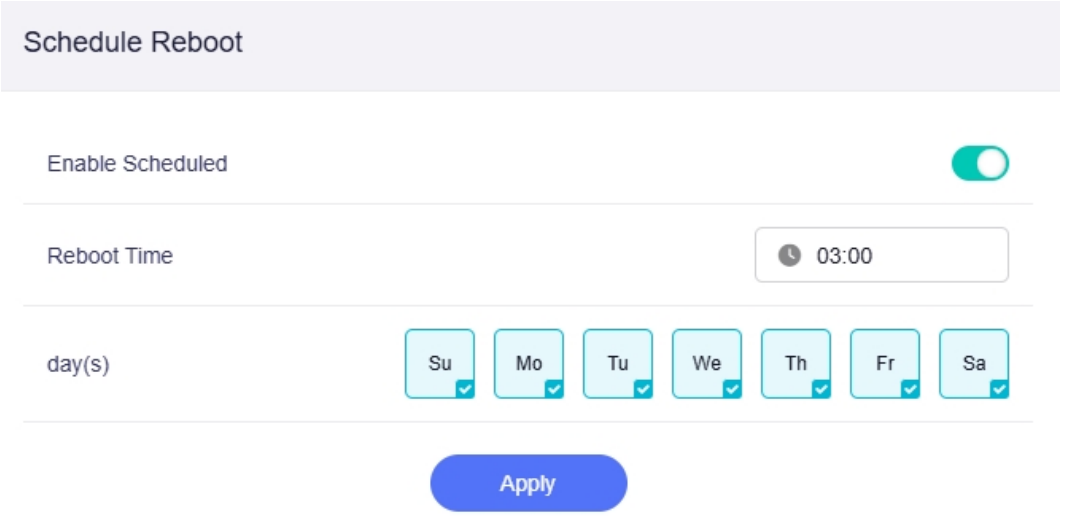


- **Habilitar programación**: cambie este interruptor para habilitar el LED mostrar programación.
- **Activar Hora**: establezca la hora (p. ej., 07:00) en la que se encenderá la luz LED .
- **Hora de apagado**: establezca la hora (p. ej., 22:00) en la que se encenderá la luz LED la luz se apagará.
- **día(s)**: Seleccione los días efectivos de la semana para esta configuración.

Después de configurar, hacer clic **Aplicar** para guardar su configuración.

15.4.2 Programar reinicio

Esta función le permite configurar un programa para reiniciar automáticamente su enrutador.

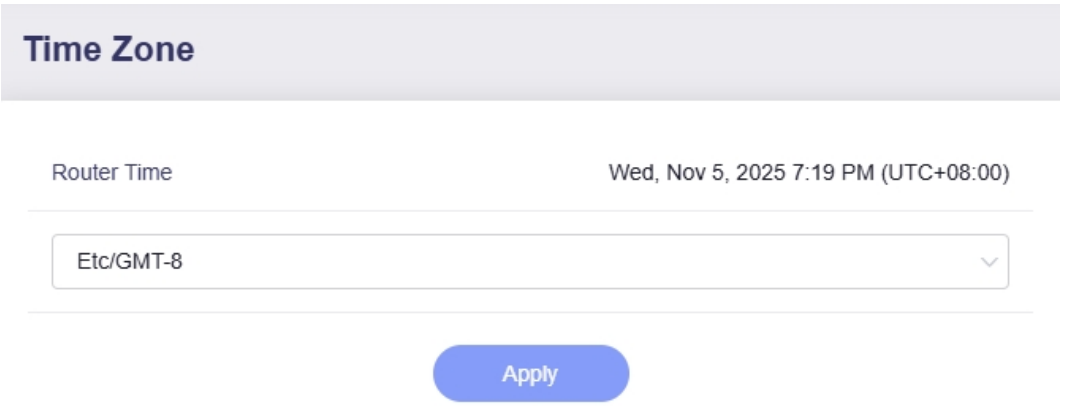


- **Habilitar programado**: active este interruptor para habilitar el reinicio programado.
- **Reiniciar Hora**: establezca la hora específica (por ejemplo, 03:00) en la que se reiniciará el enrutador.
- **día(s)**: Seleccione los días efectivos de la semana para esta configuración.

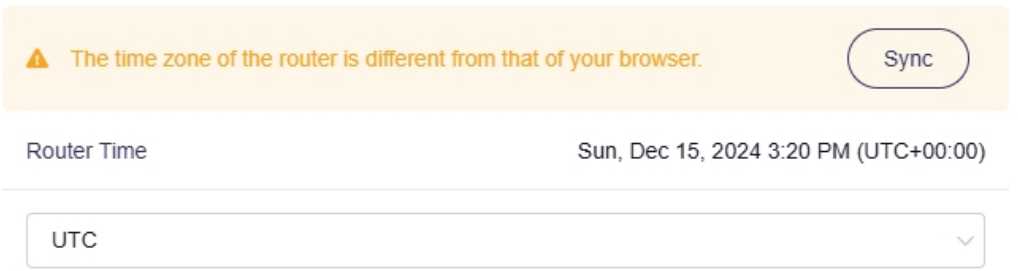
Después de la configuración, haga clic en **Aplicar** para guardar su configuración.

15.5 Zona horaria

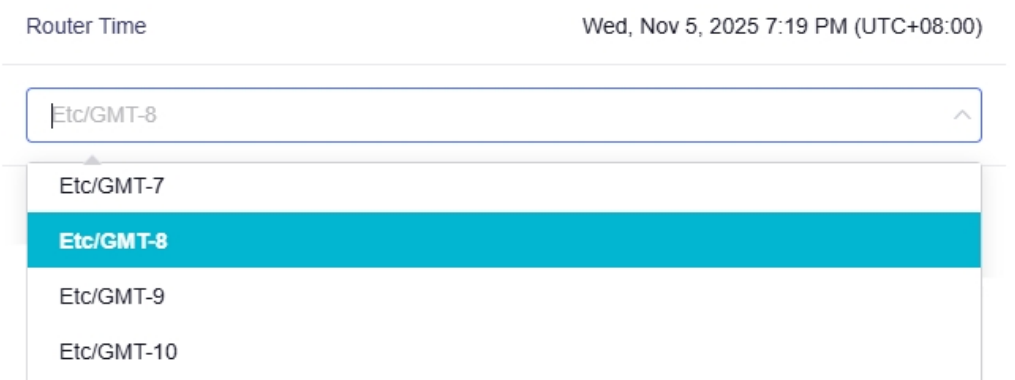
Inicie sesión en el panel de administración web de su enrutador y navegue hasta **SISTEMA** > **Zona horaria**. Esta página muestra la la hora del sistema, indicando la fecha, la hora y el desplazamiento de zona horaria correspondiente.



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



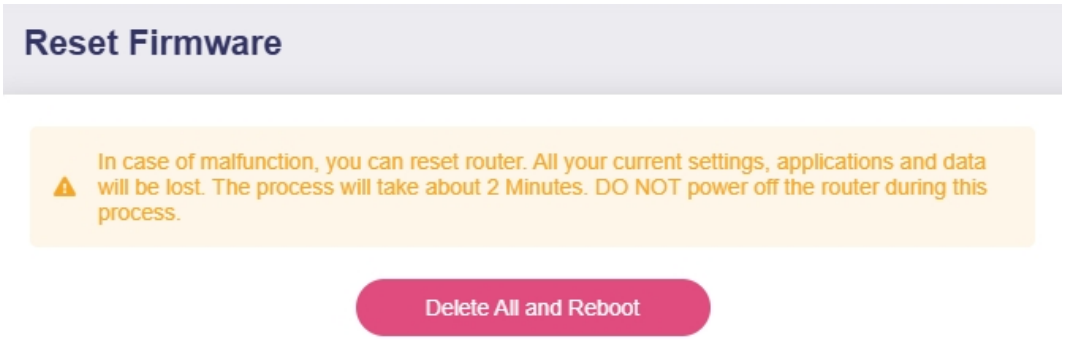
Para cambiar la zona horaria, sseleccione la zona horaria apropiada de la lista para garantizar que la hora del sistema coincida con su hora local.



15.6 Restablecer firmware

Inicie sesión en el panel de administración web de su enrutador y navegue hasta **SISTEMA** > **Restablecer firmware**. Si el enrutador no funciona correctamente, puede intentar resolver el problema restableciendo el firmware.

Haga clic en el botón **Eliminar todo y reiniciar** para restablecer el firmware según sea necesario.

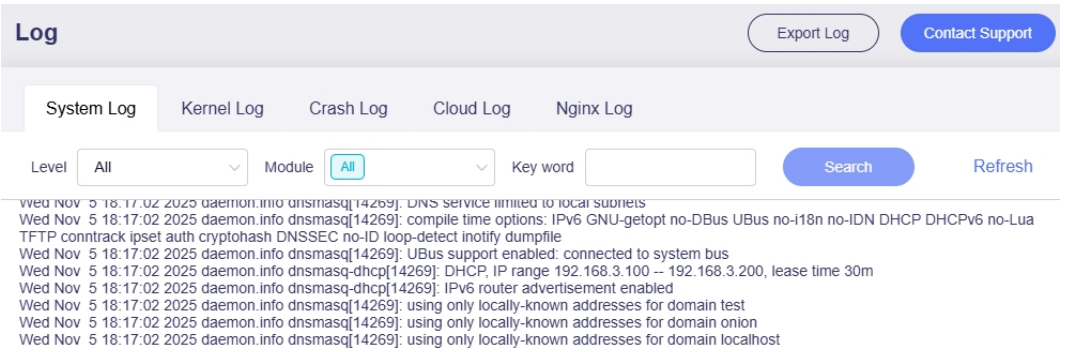


Nota: Todas sus configuraciones, aplicaciones y datos actuales serán borrados. El proceso durará unos 2 minutos. Nono apague el enrutador durante este proceso.

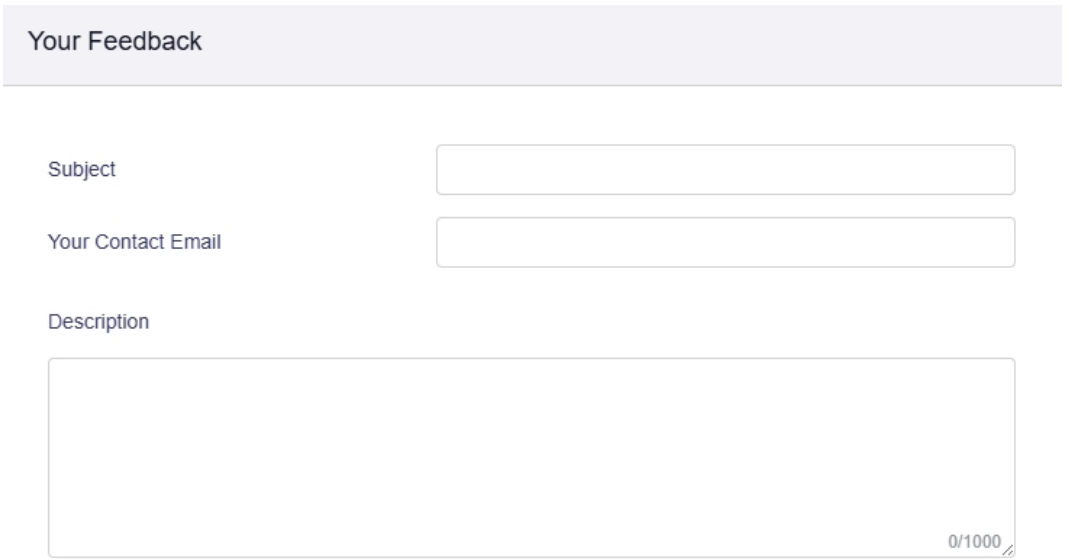
Si no puede acceder al panel de administración web del enrutador', intente restablecer su enrutador usando el botón de reinicio físico en el costado.

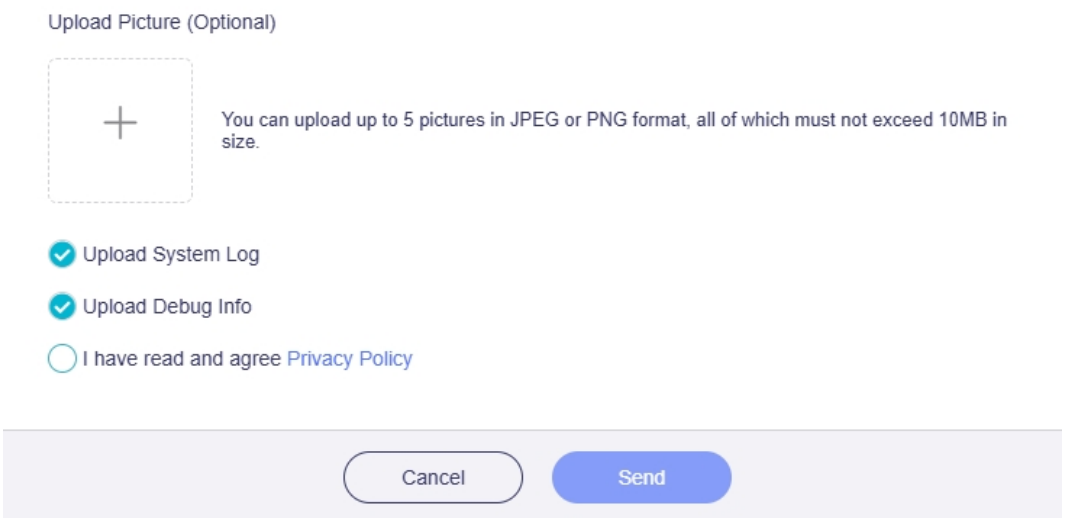
15.7 Registro

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



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

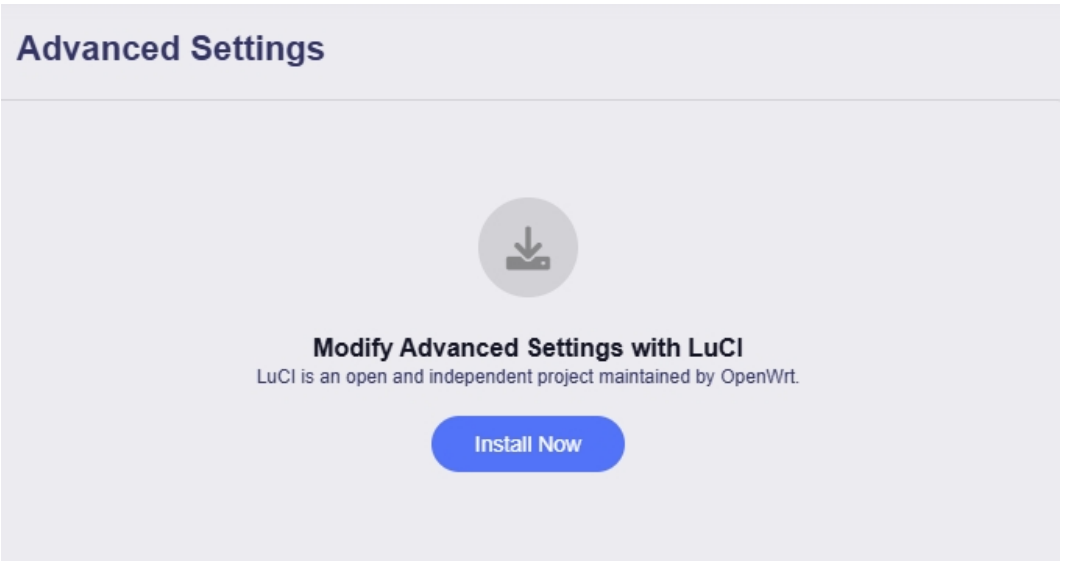



Upload Picture (Optional)
You can upload up to 5 pictures in JPEG or PNG format, all of which must not exceed 10MB in size.
Upload System Log
Upload Debug Info
I have read and agree Privacy Policy
Cancel
Send

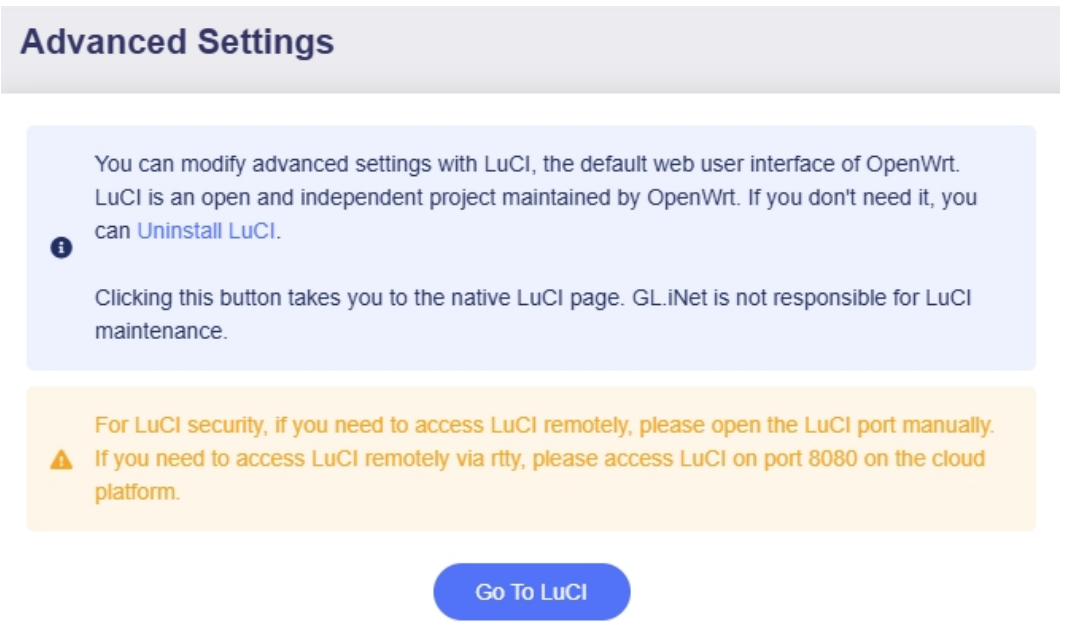
15.8 Configuración avanzada

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

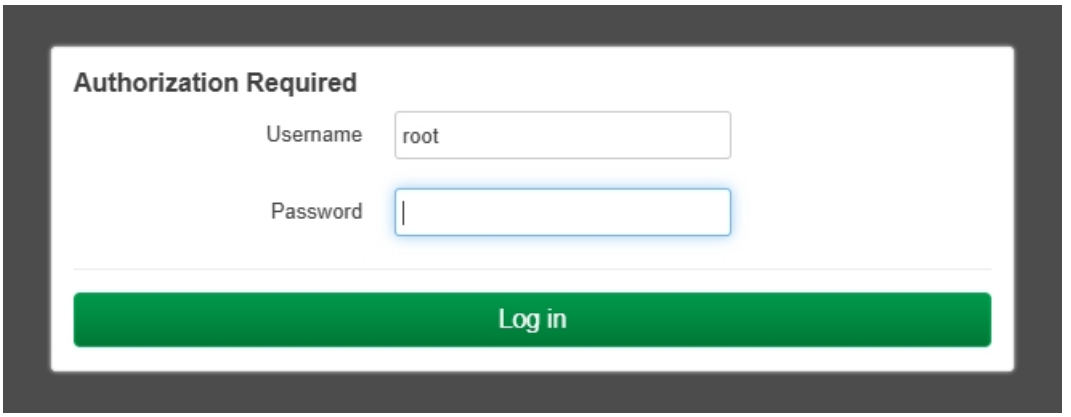
Haga clic en el botón **Instalar ahora** y se instalará la interfaz LuCI.



Haga clic en el **Ir a LuCI** botón, y será redirigido a la página de inicio de sesión de LuCI.



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



Luego iniciará sesión en la página de LuCI.

