

Instrukcja obsługi

GL-BE6500 / Flint 3e

Dwupasmowy domowy router Wi-Fi 7

Wersja oprogramowania sprzętowego 4.8.8

O tej instrukcji

Ta instrukcja pomoże rozpocząć korzystanie z urządzenia. Zawiera podstawowe informacje o produkcie, opis podłączania sprzętu, logowania do interfejsu zarządzania w przeglądarce i konfiguracji początkowej, a także szczegółowe instrukcje dotyczące wszystkich funkcji oprogramowania w panelu administracyjnym.

Z tej instrukcji dowiesz się, jak:

- Poznać najważniejsze informacje o produkcie
- Wybrać odpowiednie miejsce dla urządzenia
- Podłączyć sprzęt zgodnie z instrukcjami krok po kroku
- Łatwo zalogować się do interfejsu zarządzania w przeglądarce
- Skonfigurować ustawienia początkowe i korzystać ze wszystkich funkcji oprogramowania w panelu administracyjnym

Konwencje formatowania

Poniższe symbole i kolory ułatwiają wykonywanie opisanych czynności.

Konwencja	Znaczenie
Podkreślony tekst w kolorze turkusowym	Łącze otwierające stronę internetową lub określoną sekcję
Tekst pogrubiony	Wyróżnia lub oznacza istotne informacje w tym dokumencie, takie jak tytuły, hiperłącza oraz dokładne nazwy menu i elementów w interfejsie internetowym urządzenia
>	Ścieżka do odpowiedniej strony (np. System > Firmware)
Uwaga	Ważne informacje dotyczące konfiguracji, obsługi i bezpieczeństwa. Ich zignorowanie może skutkować niepowodzeniem konfiguracji, nieprawidłowym działaniem lub uszkodzeniem urządzenia
Wskazówki	Porady ułatwiające korzystanie z urządzenia

Uwaga:

- Funkcje urządzenia mogą się różnić w zależności od modelu i wersji oprogramowania.
- Dostępność produktu zależy od regionu lub specyfikacji dostawcy usług internetowych.
- Wszystkie ilustracje, procedury i opisy w tej instrukcji mają charakter poglądowy i mogą różnić się od rzeczywistego sposobu korzystania z urządzenia.

Potrzebujesz pomocy lub dodatkowych informacji?

- Aktualizacja oprogramowania: Centrum pobierania oprogramowania GL.iNet | Router
- Społeczność: porozmawiaj o naszych produktach i wymieniaj się doświadczeniami na forum społeczności GL.iNet
- Pomoc techniczna: skontaktuj się z naszym zespołem pomocy technicznej na stronie kontaktowej

Prawa autorskie © 2026 GL.iNet Technology (HK) Ltd. Wszelkie prawa zastrzeżone.
Żadna część tej instrukcji nie może być powielana, przepisywana, tłumaczona ani rozpowszechniana w jakiejkolwiek formie i w jakikolwiek sposób bez uprzedniej pisemnej zgody GL.iNet Technology (HK) Ltd. GL.iNet jest zastrzeżonym znakiem towarowym GL.iNet Technology (Hong Kong) Ltd. w Chinach oraz innych krajach i regionach. Wszystkie pozostałe wymienione nazwy marek i produktów są znakami towarowymi lub zastrzeżonymi znakami towarowymi ich właścicieli.
Treść tego dokumentu może ulec zmianie bez powiadomienia w związku z aktualizacją wersji produktu lub z innych przyczyn. O ile nie uzgodniono inaczej, dokument służy wyłącznie celom informacyjnym, a żadne zawarte w nim stwierdzenia, informacje i zalecenia nie stanowią jakiejkolwiek gwarancji.

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

Spis treści

Rozdział 1 Poznaj swój router 6

1.1 Opis produktu 7

1.1.1 Wygląd 7

1.1.2 Złącza i przyciski 8

1.1.3 Dioda LED 9

1.2 Dane techniczne 9

1.3 Zawartość opakowania 10

Rozdział 2 Podłączanie sprzętu 12

2.1 Wybór miejsca 13

2.2 Podłączanie routera 13

Rozdział 3 Logowanie do routera 14

Rozdział 4 Konfiguracja połączenia z Internetem 16

4.1 Kreator szybkiej konfiguracji 17

4.2 Ręczna konfiguracja połączenia z Internetem 18

4.2.1 Połączenie z Internetem przez kabel Ethernet 19

4.2.2 Połączenie z Internetem przez istniejącą sieć Wi-Fi 25

4.2.3 Połączenie z Internetem przez tethering USB 32

4.2.4 Połączenie z Internetem przez modem USB 37

Rozdział 5 Sieć bezprzewodowa 40

5.1 Wyświetlanie stanu Wi-Fi 41

5.2 Ustawienia sieci bezprzewodowej 42

5.2.1 MLO Wi-Fi 42

5.2.2 Wi-Fi 5 GHz 44

5.2.3 Wi-Fi 2,4 GHz 46

5.2.4 Losowy BSSID 48

Rozdział 6 Urządzenia klienckie 50

6.1 Szczegóły urządzenia 52

6.2 Działania 54

6.3 Usuwanie urządzeń klienckich 57

6.4 Sortowanie 58

Rozdział 7 Usługi w chmurze 59

7.1 GoodCloud 60
7.1.1 Włączanie GoodCloud 61
7.1.2 Zarządzanie routerem 63
7.1.3 Usuwanie powiązania urządzenia 68
7.1.4 Wyłączanie GoodCloud 68
7.2 AstroWarp 69
Rozdział 8 Poznaj VPN 70
8.1 Wprowadzenie 71
8.2 Przykłady zastosowań 72
Rozdział 9 Panel VPN 75
9.1 Kreator konfiguracji VPN 76
9.2 Tryb VPN 80
9.2.1 Tryb globalny 81
9.2.2 Tryb reguł 82
Rozdział 10 Konfiguracja serwera VPN 92
10.1 Konfiguracja serwera OpenVPN 93
10.1.1 Przygotowanie 93
10.1.2 Etapy konfiguracji 94
10.1.3 Rozwiązywanie problemów 96
10.2 Konfiguracja serwera WireGuard 97
10.2.1 Przygotowanie 97
10.2.2 Etapy konfiguracji 98
10.2.3 Rozwiązywanie problemów 101
Rozdział 11 Konfiguracja klienta VPN 102
11.1 Konfiguracja klienta OpenVPN 103
11.1.1 Przygotowanie 103
11.1.2 Konfiguracja NordVPN 103
11.1.3 Ręczna konfiguracja klienta OpenVPN (inni dostawcy) 109
11.2 Konfiguracja klienta WireGuard 112
11.2.1 Przygotowanie 112
11.2.2 Konfiguracja AzireVPN 113
11.2.3 Konfiguracja Hide.me 118
11.2.4 Konfiguracja IPVanish 121
11.2.5 Konfiguracja Mullvad 126

11.2.6 Konfiguracja NordVPN 131
11.2.7 Konfiguracja PIA (Private Internet Access) 136
11.2.8 Konfiguracja Surfshark 141
11.2.9 Ręczna konfiguracja klienta WireGuard (inni dostawcy) 146
Rozdział 12 Tor 151
Rozdział 13 Aplikacje 154
13.1 Wtyczki 155
13.2 Dynamiczny DNS 156
13.2.1 Włączanie DDNS 156
13.2.2 Sprawdzanie działania DDNS 159
13.2.3 Zdalny dostęp przez HTTPS 161
13.2.4 Zdalny dostęp przez SSH 163
13.3 Pamięć sieciowa 165
13.3.1 Podłączanie pamięci 165
13.3.2 Konfiguracja usługi Samba 166
13.3.3 Konfiguracja WebDAV 169
13.3.4 Konfiguracja DLNA 172
13.4 AdGuard Home 173
13.5 Kontrola rodzicielska 176
13.5.1 Szybka konfiguracja 176
13.5.2 Rozwiązywanie problemów 185
13.6 Tailscale 186
13.6.1 Konfiguracja Tailscale 187
13.6.2 Zdalny dostęp do WAN 190
13.6.3 Zdalny dostęp do LAN 190
13.6.4 Niestandardowe węzły wyjściowe 191
13.7 ZeroTier 192
13.7.1 Konfiguracja ZeroTier 193
13.7.2 Zdalny dostęp do WAN 197
13.7.3 Zdalny dostęp do LAN 198
Rozdział 14 Sieć 199
14.1 Przekierowanie portów 200
14.1.1 DMZ 200
14.1.2 Przekierowanie portów 201

14.2 Multi-WAN 203
14.2.1 Monitorowanie stanu interfejsów 203
14.2.2 Tryb Multi-WAN 206
14.3 LAN 209
14.3.1 Ustawienia podstawowe 209
14.3.2 Serwer DHCP 210
14.3.3 Rezerwacja adresów 212
14.4 Sieć gościnna 213
14.4.1 Ustawienia podstawowe 213
14.4.2 Serwer DHCP 214
14.5 DNS 216
14.5.1 Ustawienia serwera DNS 217
14.5.2 Edycja pliku hosts 219
14.6 Port Ethernet 222
14.7 Tryb sieciowy 223
14.8 IPv6 225
14.8.1 Tryb IPv6 226
14.8.2 Sposób uzyskiwania DNS 226
14.9 Drop-in Gateway 227
14.10 IGMP Snooping 229
14.11 Przyspieszanie sieci 230
14.12 Ustawienia NAT 231
Rozdział 15 System 232
15.1 Przegląd 233
15.2 Aktualizacja 234
15.2.1 Aktualizacja online 234
15.2.2 Aktualizacja lokalna 235
15.3 Zadania zaplanowane 236
15.3.1 Harmonogram diody LED 236
15.3.2 Harmonogram ponownego uruchamiania 237
15.3.3 Harmonogram MLO Wi-Fi 237
15.3.4 Harmonogram Wi-Fi 5 GHz 238
15.3.5 Harmonogram Wi-Fi 2,4 GHz 240
15.4 Strefa czasowa 243

15.5 Dziennik 245
15.6 Bezpieczeństwo 247
15.6.1 Hasło administratora 247
15.6.2 Kontrola dostępu 248
15.6.3 Kontrola dostępu zdalnego 250
15.6.4 Otwieranie portów routera 251
15.7 Resetowanie oprogramowania 252
15.8 Ustawienia zaawansowane 253
Oświadczenia dotyczące zgodności z przepisami 255

Rozdział 1

Poznaj swój router

W tym rozdziale przedstawiono ogólne informacje o routerze, dane techniczne i zawartość opakowania.

1.1 Opis produktu

Flint 3e (GL-BE6500) to dwupasmowy stacjonarny router Wi-Fi 7 przeznaczony do domu i małego biura. Ma pięć portów 2,5GbE zapewniających szybkie połączenia przewodowe, zaawansowane funkcje VPN, wbudowany AdGuard Home, kontrolę rodzicielską i AstroWarp. Zapewnia płynną pracę sieci w inteligentnym domu, biurze i środowiskach z wieloma użytkownikami.

1.1.1 Wygląd

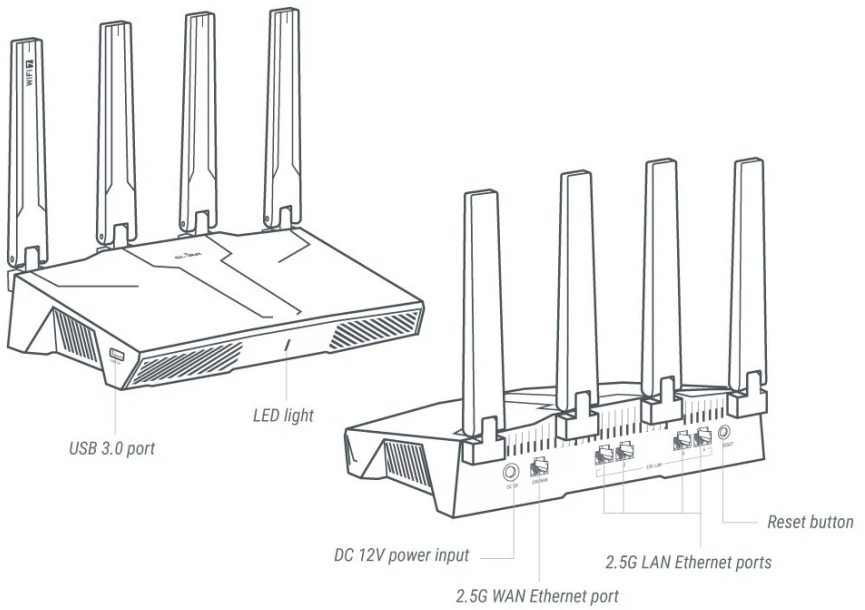








1.1.2 Złącza i przyciski



Uwaga: różnica w wyglądzie modeli Flint 3e i Flint 3 dotyczy nadruku: nadruk na Flint 3e jest niebieski, a na Flint 3 — biały.

Element	**Opis**
Złącze zasilania	Służy do podłączenia zasilacza.
Port WAN 2,5G	Służy do połączenia z modemem lub gniazdem Ethernet zapewniającym dostęp do Internetu.
Port LAN 2,5G	W razie potrzeby służy do podłączenia urządzeń przewodowych.
Port USB 3.0	Do podłączania nośników USB, udostępniania Internetu przez USB z telefonu oraz zgodnych modemów komórkowych USB.
Przycisk resetowania	Naciśnij i przytrzymaj przez **4 sekundy**, a następnie zwolnij, aby naprawić połączenie sieciowe.
	Naciśnij i przytrzymaj przez **10 sekund**, a następnie zwolnij, aby przywrócić ustawienia fabryczne routera.

1.1.3 Dioda LED

Stan	Znaczenie
Świeci na niebiesko	Uruchamianie
Powoli pulsuje na niebiesko	Uruchomiony, brak połączenia z Internetem
Świeci na biało	Połączony z Internetem
Szybko miga na niebiesko	Resetowanie

1.2 Dane techniczne

Złącza	1 × port Ethernet WAN 2,5G 1 × port Ethernet WAN/LAN 2,5G 3 × port Ethernet LAN 2,5G 1 × port USB 3.0 1 × przycisk resetowania
Procesor	Czterordzeniowy Qualcomm, 1,5 GHz
Pamięć RAM / pamięć masowa	DDR4 1 GB / NAND 512 MB
Protokół	IEEE 802.11a/b/g/n/ac/ax/be
Prędkość Wi-Fi	688 Mb/s (2,4 GHz), 5764 Mb/s (5 GHz)
Anteny	4 × składana zewnętrzna antena Wi-Fi
Prędkość Ethernet	10/100/1000/2500 Mb/s
Zasilanie	DC5521, 12 V/3 A (5,5 × 2,1 mm)
Pobór mocy	Bez obciążenia USB: <25 W Z obciążeniem USB: <37,2 W
Temperatura pracy	0 ~ 40°C (32 ~ 104°F)
Temperatura przechowywania	-20 ~ 70°C (-4 ~ 158°F)

Wymiary / masa	240 × 157 × 74 mm / 848 g
Inne materiały i narzędzia	Karta katalogowa / Oprogramowanie / Aplikacja / Rozpakowanie / Poradniki

*Prędkości sieci bezprzewodowej określono na podstawie standardów IEEE 802.11 (np. 802.11be dla Wi-Fi 7). Rzeczywista przepustowość i zasięg mogą być mniejsze ze względu na przeszkody w otoczeniu (ściany, metal), przeciążenie sieci lub możliwości urządzeń klienckich.

*Korzystanie z Wi-Fi 7 (802.11be) i jego funkcji (OFDMA, MU-MIMO, 4096-QAM, MLO) wymaga obsługi odpowiednich technologii przez urządzenia klienckie.

1.3 Zawartość opakowania

Opakowanie zawiera:

- 1 × Flint 3e (GL-BE6500)
- 1 × instrukcja obsługi (skrócona instrukcja)
- 1 × kabel Ethernet
- 1 × karta z podziękowaniem
- 1 × zasilacz
- 1 × adapter wtyczki (w zależności od kraju dostawy)



1 x User manual



1 x Flint 3e (GL-BE6500)



1 x Thank you card



1 x Ethernet cable



1 x Power adapter



Converter
(Base on your shipping countries)

Rozdział 2

Podłączanie sprzętu

W tym rozdziale opisano wybór miejsca ustawienia routera i czynności związane z jego podłączaniem.

2.1 Wybór miejsca

Aby uzyskać najlepszą wydajność, wybierz miejsce zgodnie z poniższymi wskazówkami.

- **Unikaj wilgoci i gorąca**: nie umieszczaj routera w miejscach narażonych na wodę, wilgoć lub wysoką temperaturę (np. przy zlewach lub grzejnikach).
- **Wentylacja i chłodzenie**: ustaw router w chłodnym, dobrze wentylowanym miejscu, aby zapewnić prawidłowe odprowadzanie ciepła.
- **Centralne położenie**: ustaw router w miejscu, w którym łatwo podłączyć zasilanie i wiele urządzeń (np. w centralnej części salonu).
- **Ułożenie przewodów**: poprowadź kable i przewód zasilający bezpiecznie, aby uniknąć ryzyka potknięcia.
- **Stabilna powierzchnia**: ustaw router na poziomej, płaskiej powierzchni (półce lub biurku), aby zapewnić stabilność.
- **Unikanie zakłóceń elektromagnetycznych**: umieść router z dala od źródeł zakłóceń elektromagnetycznych (urządzeń Bluetooth, kuchenek mikrofalowych), aby ograniczyć zakłócenia sygnału.

2.2 Podłączanie routera

1. **Włącz zasilanie**

   Połącz obie części zasilacza. Podłącz go do routera i do gniazdka elektrycznego. Router uruchomi się automatycznie.

2. **Podłącz urządzenie do routera**

   Podłącz urządzenie (np. laptop lub smartfon) do routera przez Wi-Fi lub za pomocą kabla Ethernet.

   - **Wi-Fi**: na swoim urządzeniu przejdź do Ustawienia -> WLAN, znajdź nazwę sieci Wi-Fi routera na liście dostępnych sieci i wprowadź hasło. Domyślna nazwa sieci i hasło znajdują się na etykiecie routera.
   - **Ethernet**: podłącz urządzenie do portu LAN routera za pomocą kabla Ethernet.

3. **Zaloguj się do routera**

   Przy pierwszym połączeniu z routerem Internet jest niedostępny. Przed uzyskaniem dostępu do Internetu zaloguj się do routera zgodnie z opisem w rozdziale 3 i wykonaj konfigurację początkową.

Rozdział 3

Logowanie do routera

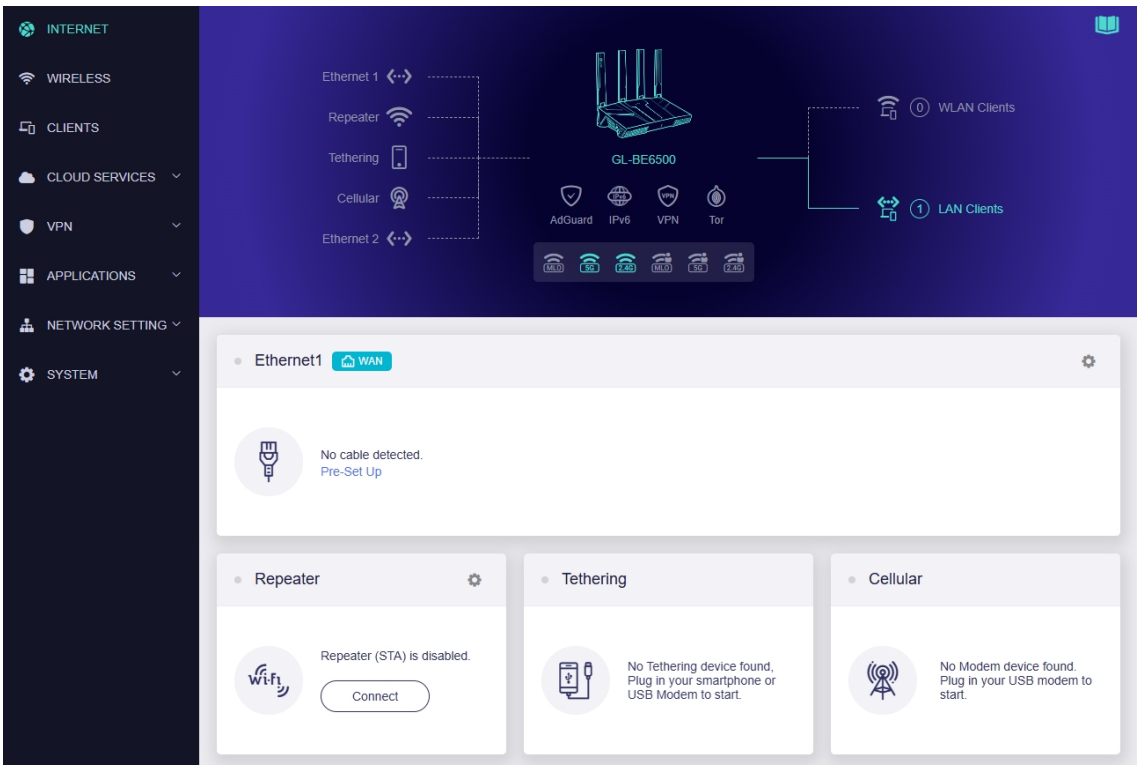
W tym rozdziale opisano logowanie do routera przez panel administracyjny w przeglądarce.

Router można konfigurować i zarządzać nim za pomocą interfejsu w przeglądarce internetowej. Jest on dostępny w systemach Windows, Mac OS i Linux za pośrednictwem przeglądarki, takiej jak Microsoft Edge, Google Chrome, Mozilla Firefox lub Apple Safari.

Uwaga: jeśli wolisz korzystać z aplikacji GL.iNet zamiast panelu administracyjnego, pobierz aplikację i postępuj zgodnie z instrukcjami na ekranie.

Aby zalogować się do routera przez panel administracyjny, wykonaj poniższe czynności.

1. Podłącz urządzenie (np. komputer stacjonarny lub laptop) do routera przez Wi-Fi lub za pomocą kabla Ethernet.
2. Otwórz przeglądarkę internetową (zalecane są Chrome i Edge) i przejdź pod adres http://192.168.8.1. Otworzy się strona logowania do panelu administracyjnego. Jeśli nie możesz uzyskać do niego dostępu, wskazówki dotyczące rozwiązywania problemów znajdziesz tutaj.
3. Ustaw hasło administratora. Ze względów bezpieczeństwa zaleca się użycie silnego hasła. Następnie kliknij **Next**, aby kontynuować.
4. Otworzy się panel administracyjny routera.



Rozdział 4

Konfiguracja połączenia z Internetem

W tym rozdziale przedstawiono różne sposoby łączenia routera z Internetem, dostosowane do różnych środowisk sieciowych.

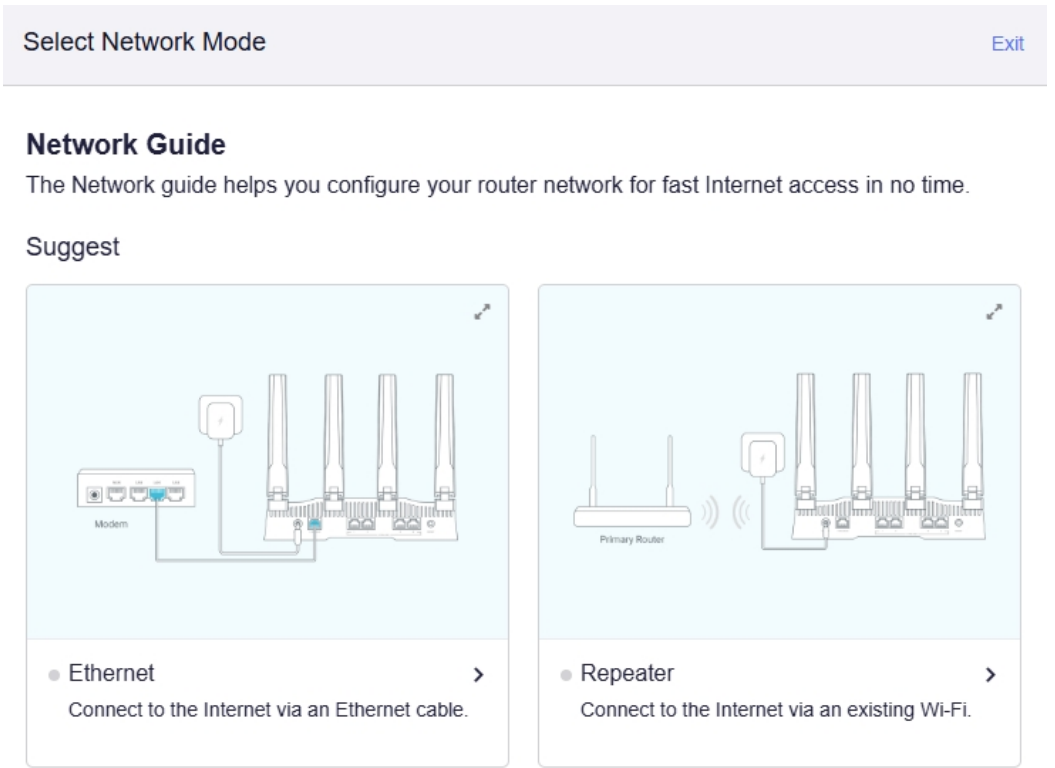
4.1 Kreator szybkiej konfiguracji

Kreator konfiguracji w przeglądarce przeprowadzi Cię przez konfigurację sieci routera. Aby uruchomić kreator, wykonaj poniższe czynności.

1. Zaloguj się do panelu administracyjnego routera zgodnie z opisem w rozdziale 3.
2. Na stronie głównej kliknij ikonę książki w prawym górnym rogu.



3. Postępuj zgodnie z instrukcjami kreatora konfiguracji, aby skonfigurować router i nawiązać połączenie z Internetem.



Jeśli korzystasz z aplikacji GL.iNet, skonfiguruj dostęp do Internetu zgodnie z instrukcjami na ekranie.

4.2 Ręczna konfiguracja połączenia z Internetem

Kreator konfiguracji ułatwia szybkie skonfigurowanie sieci, natomiast konfiguracja ręczna pozwala dostosować zaawansowane ustawienia sieciowe do konkretnych wymagań oraz w razie potrzeby sprawdzić lub zmienić istniejące połączenia.

Flint 3e obsługuje cztery metody połączenia z Internetem: Ethernet, Repeater, USB Tethering i USB Modem. Wybierz metodę odpowiednią do swoich potrzeb.

1. **Ethernet**: podłącz router do sieci szerokopasmowej za pomocą kabla Ethernet wpiętego do portu WAN. Router zazwyczaj uzyskuje adres IP automatycznie przez DHCP. Można też ręcznie skonfigurować statyczny adres IP lub ustawienia PPPoE. Ten sposób zapewnia dużą stabilność i szybkość, dlatego sprawdza się w domu i biurze ze stałym łączem szerokopasmowym.

2. **Wzmacniacz sygnału**: w tym trybie router łączy się z istniejącą siecią Wi-Fi, rozszerza jej zasięg i tworzy odrębną, bezpieczną sieć lokalną. Prędkość transmisji może się nieco zmniejszyć. Ten tryb sprawdza się w miejscach bez zasięgu Wi-Fi wymagających rozszerzenia sygnału oraz w miejscach publicznych, w których potrzebna jest większa ochrona sieci.

3. **Tethering USB**: podłącz smartfon lub inne zgodne urządzenie do routera kablem USB, aby udostępnić routerowi komórkowe połączenie transmisji danych tego urządzenia (np. 4G/5G). To wygodne rozwiązanie zapewniające tymczasowy dostęp do Internetu, szczególnie w terenie lub w miejscach bez stałego łącza szerokopasmowego.

4. **Modem USB**: podłącz do routera komórkowy modem USB z wcześniej włożoną kartą SIM. Router połączy się z Internetem przez sieć komórkową 4G/5G, niezależnie od stałego łącza szerokopasmowego. Ten sposób zapewnia dużą mobilność i sprawdza się np. w pojazdach oraz podczas aktywności w terenie.

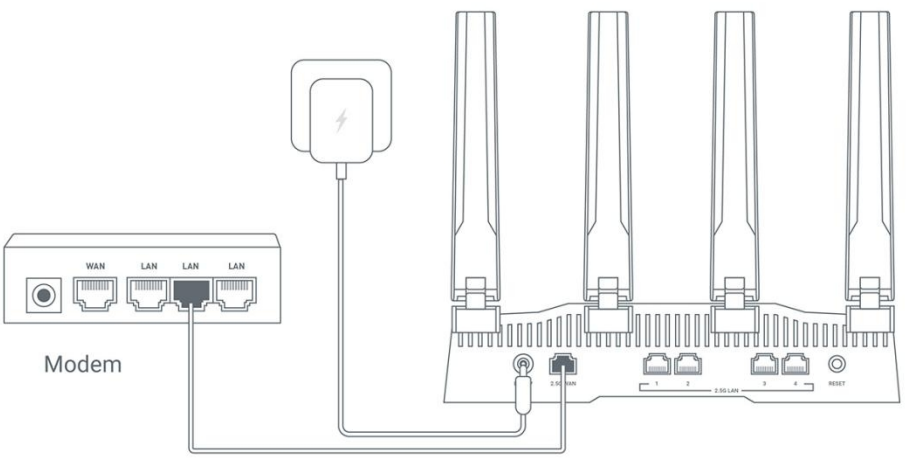
4.2.1 Połączenie z Internetem przez kabel Ethernet

Podłącz router do sieci szerokopasmowej za pomocą kabla Ethernet wpiętego do portu WAN. Router zazwyczaj uzyskuje adres IP automatycznie przez DHCP. Można też ręcznie skonfigurować statyczny adres IP lub ustawienia PPPoE. Ten sposób zapewnia dużą stabilność i szybkość, dlatego sprawdza się w domu i biurze ze stałym łączem szerokopasmowym.

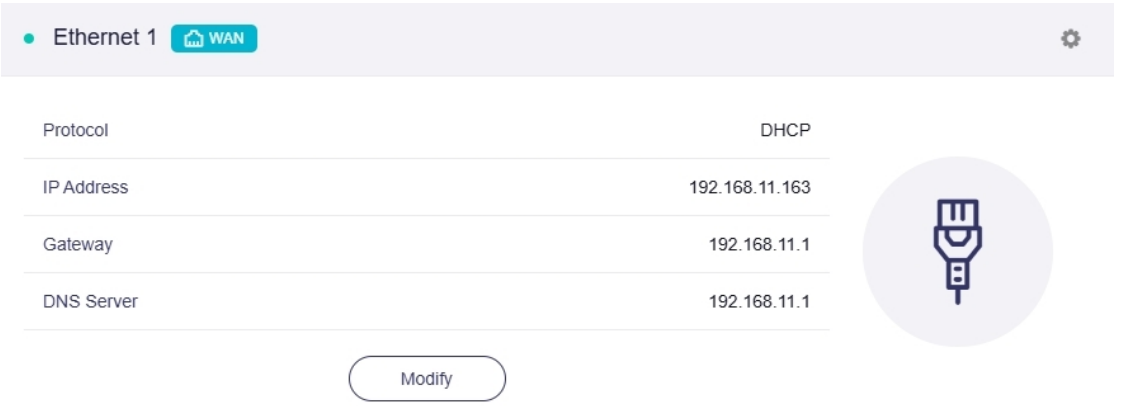
Podstawowa konfiguracja

Aby połączyć router z Internetem za pomocą kabla Ethernet, wykonaj poniższe czynności.

1. Połącz port **WAN** routera z urządzeniem nadrzędnym (np. modemem dostawcy Internetu, głównym routerem, przełącznikiem sieciowym lub gniazdem Ethernet) za pomocą kabla Ethernet.

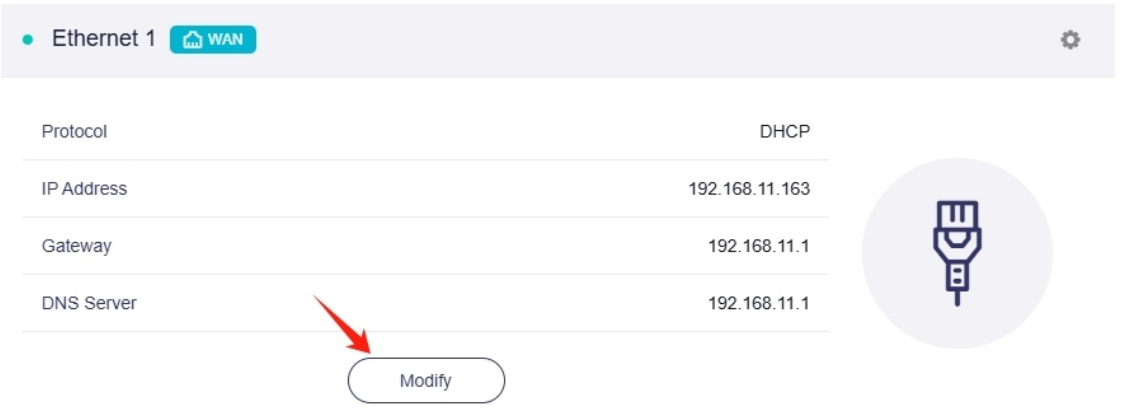


2. Zaloguj się do panelu administracyjnego routera i przejdź do **INTERNET** > **Ethernet**. Po pomyślnym nawiązaniu połączenia w sekcji Ethernet pojawią się szczegóły sieci, w tym protokół, adres IP, brama i serwer DNS.


Ethernet 1
WAN
Protocol
DHCP
IP Address
192.168.11.163
Gateway
192.168.11.1
DNS Server
192.168.11.1
Modify

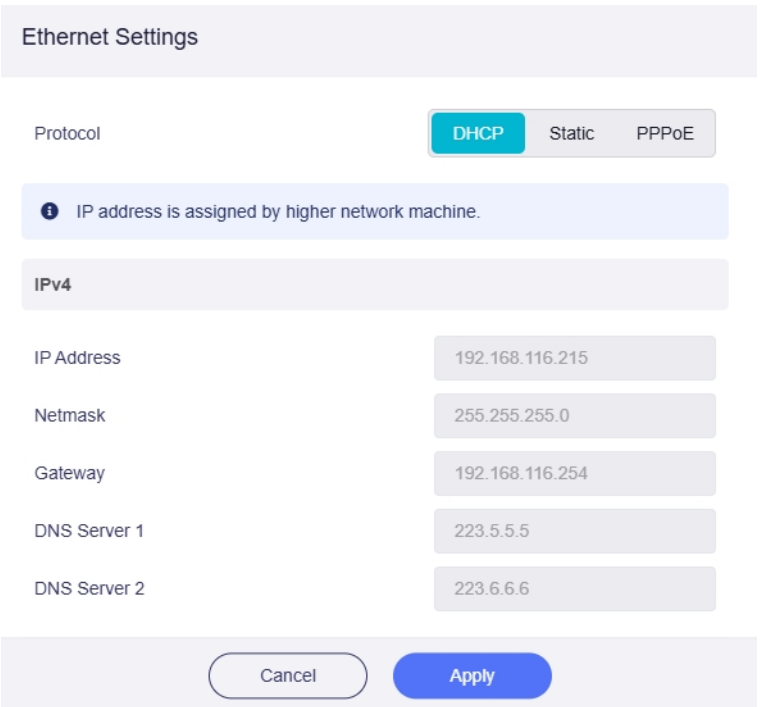
Protokół

Dostępne są trzy rodzaje protokołu: DHCP, Static i PPPoE. Kliknij **Modify**, aby zmienić protokół.



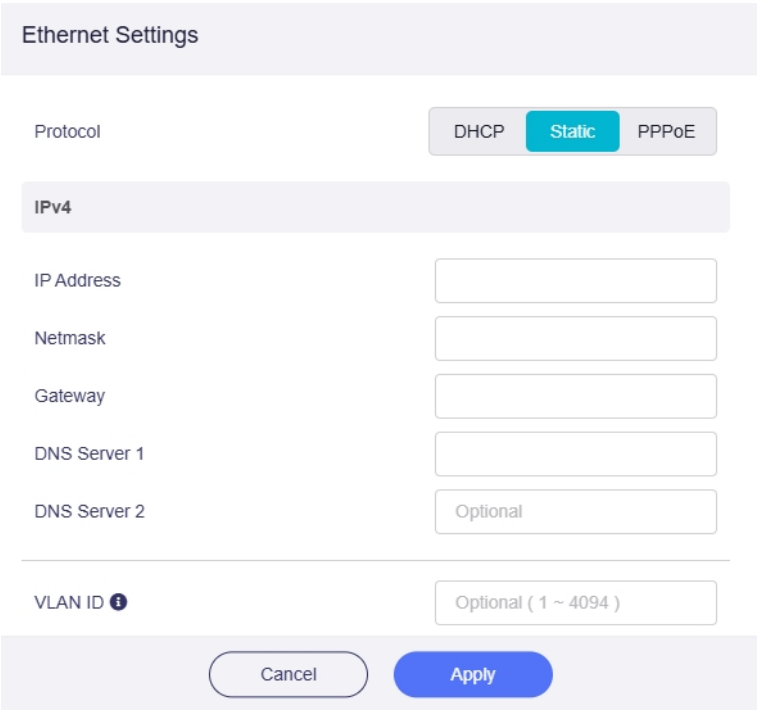
- **DHCP**

  DHCP to domyślny i najczęściej używany protokół sieciowy. Automatycznie przydziela adresy IP i inne parametry konfiguracji urządzeniom w sieci IP w modelu klient–serwer.



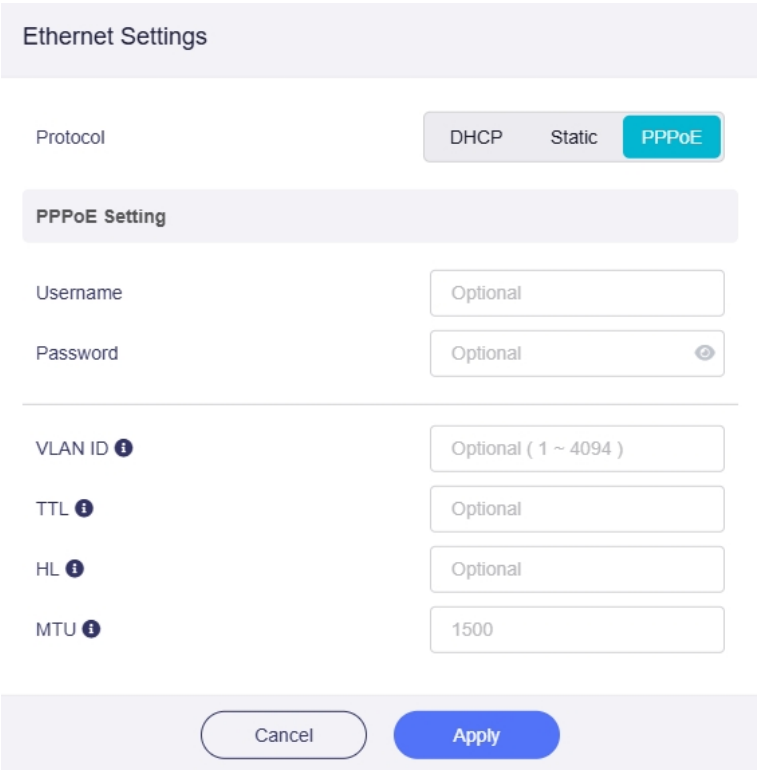
- **Statyczny adres IP**

  Statyczny adres IP jest wymagany, gdy dostawca usług internetowych przydziela stały publiczny adres IP lub gdy parametry sieci (np. adres IP, bramę, maskę podsieci) trzeba skonfigurować ręcznie.



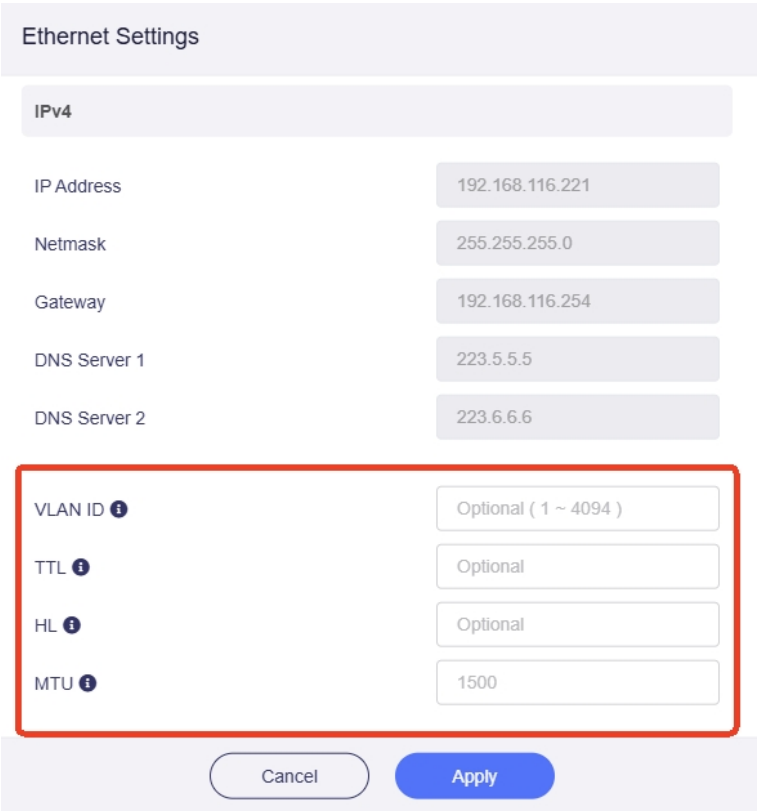
- **PPPoE**

  PPPoE (Point-to-Point Protocol over Ethernet) to protokół sieciowy powszechnie stosowany przez dostawców Internetu. Dostawca zazwyczaj udostępnia modem oraz indywidualną nazwę użytkownika i hasło wymagane do skonfigurowania połączenia z Internetem.



Ustawienia zaawansowane

Oprócz ustawień podstawowych dostępne są także opcjonalne ustawienia zaawansowane dla trzech powyższych protokołów.



- **VLAN ID**

  To ustawienie jest potrzebne tylko wtedy, gdy serwer dostawcy wymaga używania przez interfejs konkretnego identyfikatora tagowanej sieci VLAN.
- **TTL**

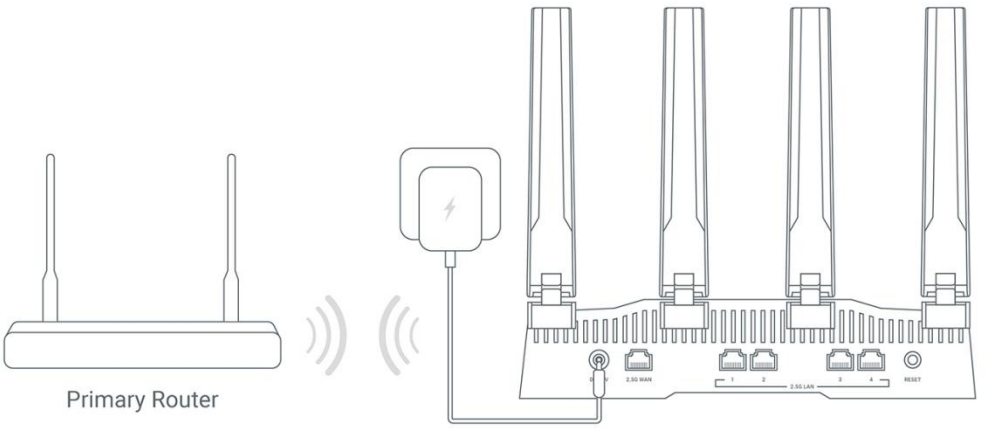
  TTL (Time To Live) określa maksymalny czas istnienia pakietów w sieci. Domyślnie router zmniejsza o 1 wartość TTL pakietów odebranych od urządzeń klienckich przed ich przekazaniem dalej. Jeśli chcesz zastąpić tę wartość, możesz ustawić tutaj stałą wartość. Ustawienie TTL dotyczy wyłącznie IPv4.
- **HL**

  W IPv6 pole HL (Hop Limit) ogranicza liczbę przeskoków pakietów danych w sieci i jest odpowiednikiem TTL w IPv4.
- **MTU**

  Domyślna wartość MTU wynosi 1500 bajtów.

4.2.2 Połączenie z Internetem przez istniejącą sieć Wi-Fi

Podłącz router jako wzmacniacz do istniejącej sieci bezprzewodowej, aby wzmocnić sygnał Wi-Fi i utworzyć sieć lokalną odizolowaną od sieci głównej. W hotelach i kawiarniach oferujących bezpłatne publiczne hotspoty wzmacniacz zwiększa zasięg Wi-Fi, zapewnia przewodowy i bezprzewodowy dostęp wielu urządzeniom oraz chroni bezpieczeństwo sieci.

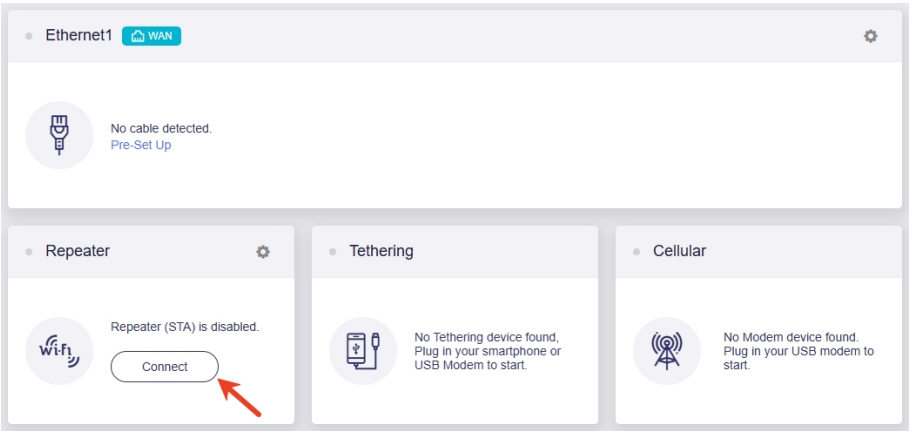


Funkcja wzmacniacza GL.iNet domyślnie działa w trybie WISP (Wireless Internet Service Provider). Oznacza to, że router tworzy własną podsieć i działa jako zapora, chroniąc przed zagrożeniami z sieci publicznej.

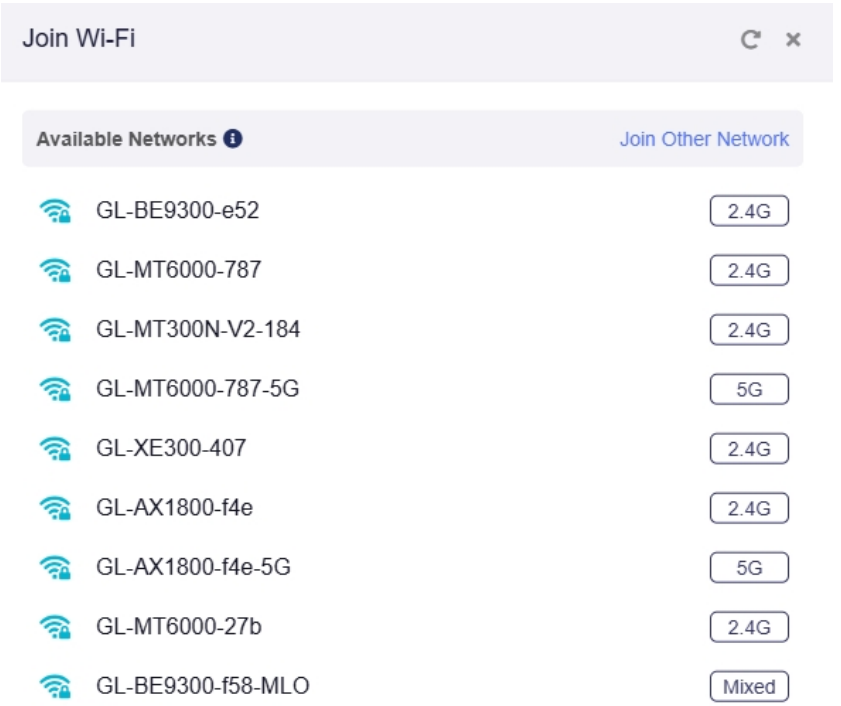
Podstawowa konfiguracja

Aby połączyć router z istniejącą siecią Wi-Fi w trybie wzmacniacza sygnału, wykonaj poniższe czynności.

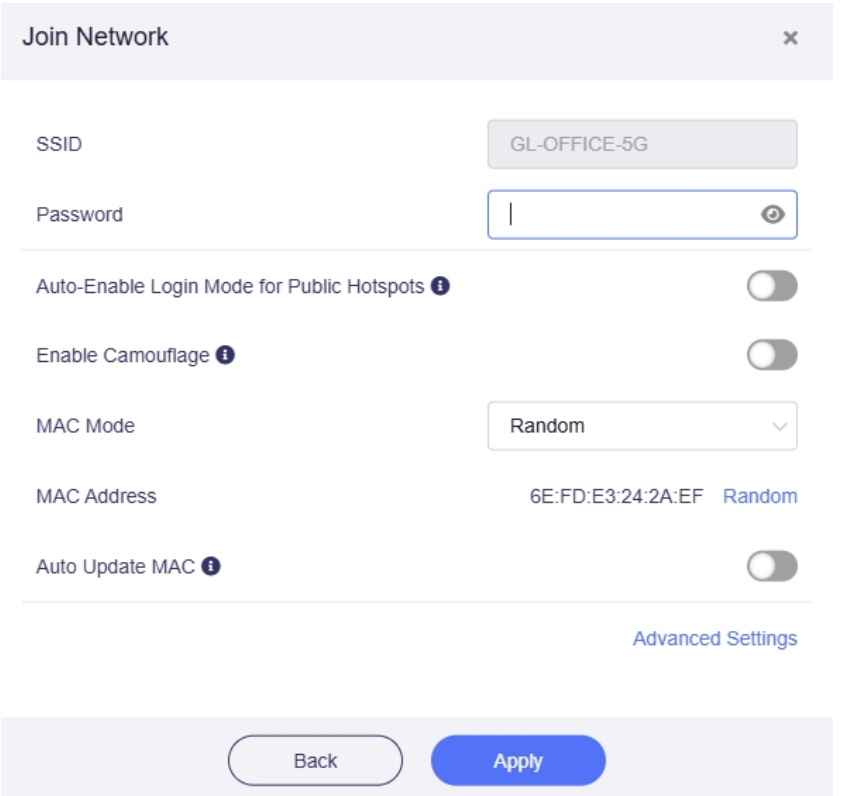
1. Zaloguj się do panelu administracyjnego routera i przejdź do **INTERNET** -> **Repeater**. Kliknij **Connect**.



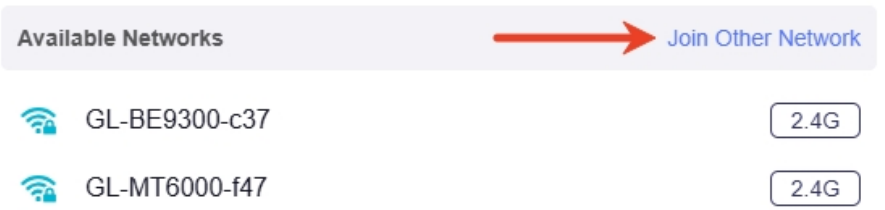
2. W wyświetlonym oknie wybierz z listy dostępnych sieci sieć Wi-Fi, z którą chcesz się połączyć.



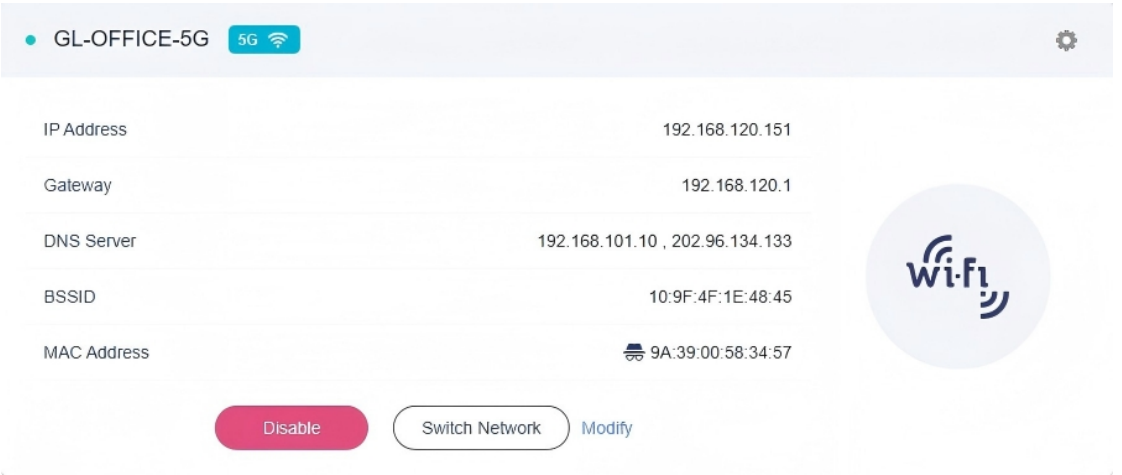
3. Wprowadź prawidłowe hasło Wi-Fi i kliknij **Apply**.



Jeśli identyfikatora SSID docelowej sieci Wi-Fi nie ma na liście dostępnych sieci, kliknij **Join Other Network** w prawym górnym rogu, ręcznie wprowadź SSID i pozostałe wymagane informacje, a następnie kliknij **Apply**.

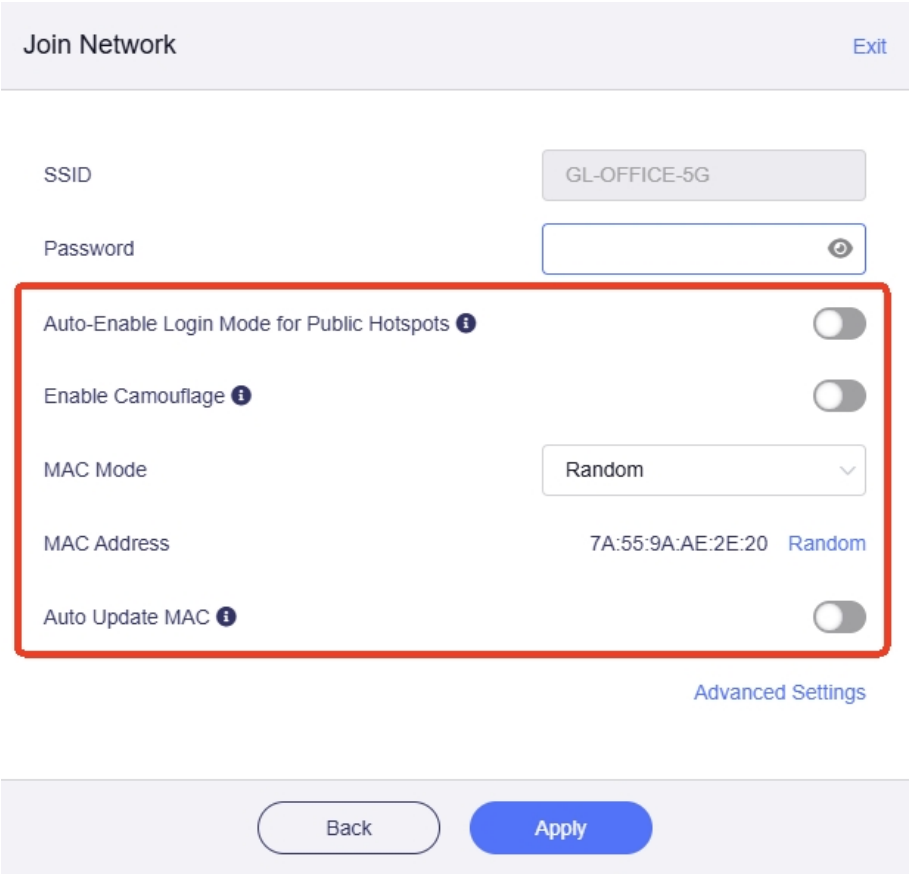


4. Poczekaj chwilę na połączenie routera. Po połączeniu strona będzie wyglądać jak poniżej.

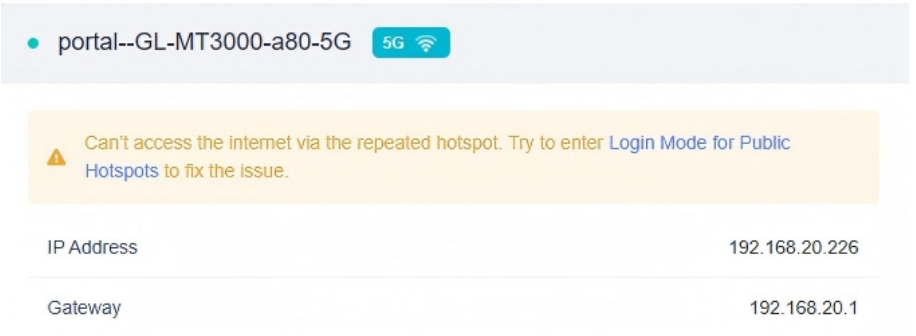

GL-OFFICE-5G
5G
IP Address
192.168.120.151
Gateway
192.168.120.1
DNS Server
192.168.101.10 , 202.96.134.133
BSSID
10:9F:4F:1E:48:45
MAC Address
9A:39:00:58:34:57
Disable
Switch Network
Modify

Ustawienia publicznego hotspotu

Podczas łączenia routera z publicznym hotspotem z portalem logowania zaleca się włączenie poniższych funkcji, aby zwiększyć szansę pomyślnego połączenia.



- **Automatyczne włączanie trybu logowania do publicznych hotspotów**
  Po włączeniu tej opcji router automatycznie przechodzi w tryb Public Hotspot Login Mode, gdy jest połączony z hotspotem, ale nie ma dostępu do Internetu. W tym trybie niektóre usługi zostają wstrzymane, a tryb DNS zmienia się na automatyczny, co może ujawnić Twoją aktywność sieciową dostawcy sieci (np. hotelowi lub centrum handlowemu). Nawet po wyłączeniu tej opcji router zaproponuje przejście do tego trybu, jeśli wykryje portal logowania hotspotu lub logowanie się nie powiedzie.

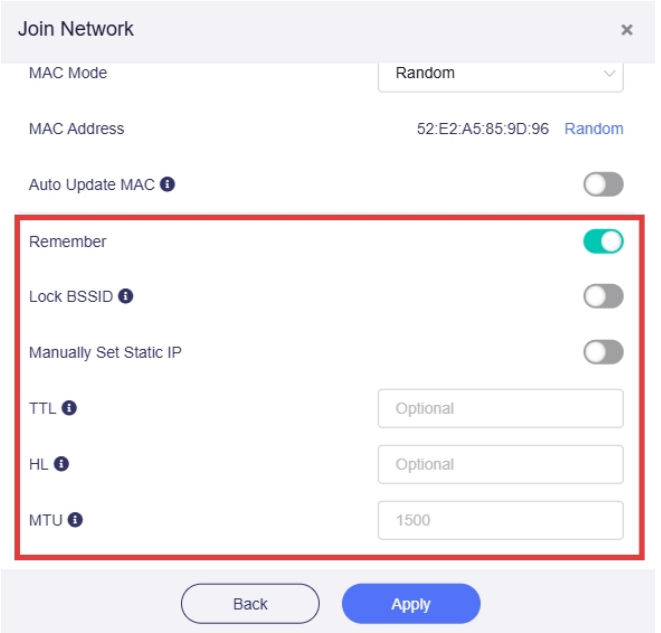


- **Włączanie kamuflażu**
  Po włączeniu tej opcji router podszywa się pod urządzenie klienckie używane do otwierania panelu administracyjnego, naśladując jego adres MAC.
- **Tryb MAC**
  Wybierz adres MAC, którego router ma używać do łączenia się z publicznym hotspotem.
  Factory: używa oryginalnego adresu MAC przypisanego fabrycznie do urządzenia.
  Clone: klonuje adres MAC urządzenia klienckiego na potrzeby połączenia.
  Jeśli żądanego adresu MAC nie ma na liście, wprowadź go ręcznie, aby go sklonować.
  Uwaga: wiele urządzeń używa losowych adresów MAC (często określanych jako prywatny adres Wi-Fi lub losowy adres sprzętowy) podczas łączenia się z sieciami Wi-Fi. Dlatego wyświetlany tutaj adres MAC może różnić się od rzeczywistego fizycznego adresu MAC urządzenia.
  Random: automatycznie generuje losowy adres MAC na potrzeby połączenia.
- **Automatyczna aktualizacja adresu MAC**
  Po włączeniu tej opcji adres MAC jest aktualizowany automatycznie.

Podczas zapisywania konfiguracji sieci tryb MAC, w tym sklonowany lub losowy adres MAC, zostaje powiązany z zapisywanym identyfikatorem SSID. Ustawienia te można w każdej chwili ręcznie zmienić dla poszczególnych identyfikatorów SSID.

Ustawienia zaawansowane

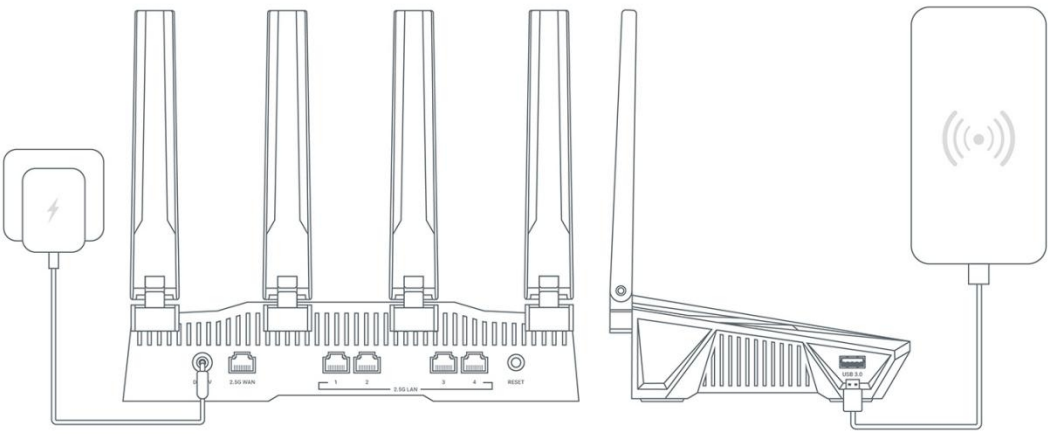
Podczas dołączania do sieci dostępne są opcjonalne ustawienia zaawansowane.



- **Remember**: włącz tę opcję, aby zapamiętać bieżącą sieć Wi-Fi, której sygnał jest wzmacniany.
- **Lock BSSID**: po włączeniu router będzie łączyć się wyłącznie z konkretnym punktem dostępu (AP) odpowiadającym wybranemu BSSID, nawet jeśli inne punkty dostępu mają taki sam identyfikator SSID.
- **Manually Set Static IP**: po włączeniu tej opcji możesz ręcznie skonfigurować stały adres IPv4, maskę sieci, bramę i serwery DNS dla połączenia routera w trybie wzmacniacza sygnału zamiast uzyskiwać te ustawienia automatycznie.
- **TTL**: TTL (Time To Live) określa maksymalny czas istnienia pakietów w sieci. Domyślnie router zmniejsza o 1 wartość TTL pakietów odebranych od urządzeń klienckich przed ich przekazaniem dalej. Aby zastąpić lub zmodyfikować TTL, wprowadź żądaną wartość efektywną powiększoną o 1, co skompensuje automatyczne zmniejszenie. TTL dotyczy wyłącznie IPv4.
- **HL**: w IPv6 pole HL (Hop Limit) ogranicza liczbę przeskoków pakietów danych w sieci i jest odpowiednikiem TTL w IPv4.
- **MTU**: wartość domyślna wynosi 1500.

4.2.3 Połączenie z Internetem przez tethering USB

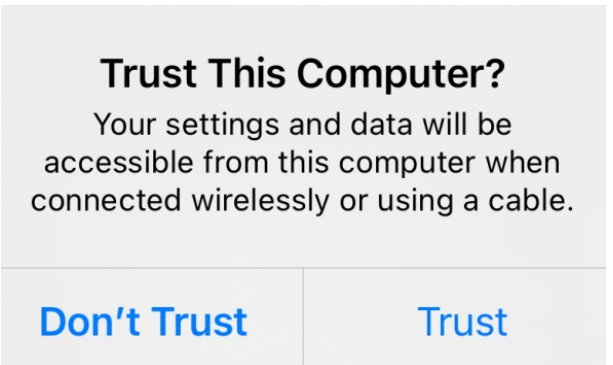
Podłączenie smartfona do routera kablem USB w celu udostępnienia routerowi komórkowej transmisji danych (np. 4G/5G) nazywa się tetheringiem. To wygodny sposób uzyskania tymczasowego dostępu do Internetu, szczególnie w terenie lub w miejscach bez stałego łącza szerokopasmowego.



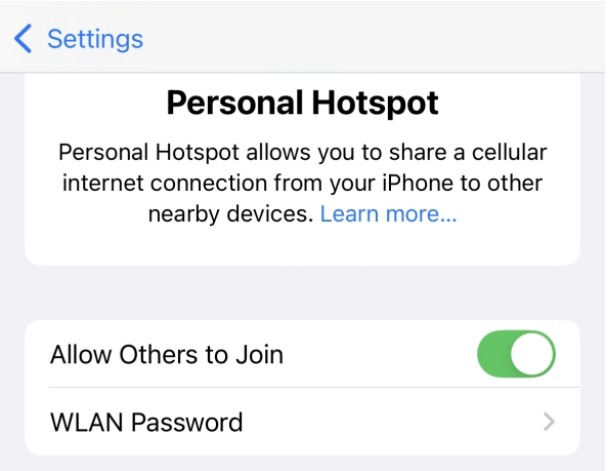
Modem typu hostless również korzysta z interfejsu Tethering podczas konfiguracji modemu.
Uwaga: niektórzy operatorzy komórkowi ograniczają tethering lub pobierają za niego dodatkowe opłaty. Zalecamy sprawdzenie warunków u operatora.

Tethering z iPhone’a

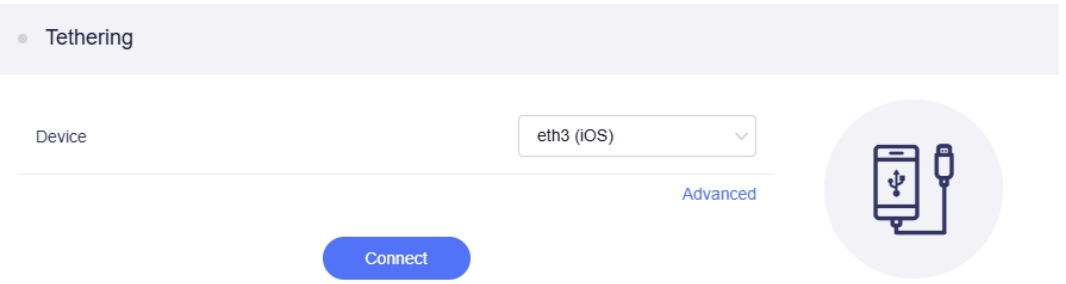
1. Podłącz iPhone'a do portu USB routera za pomocą kabla USB. Pojawi się komunikat systemowy z pytaniem, czy zaufać urządzeniu. Stuknij **Trust**, aby kontynuować.



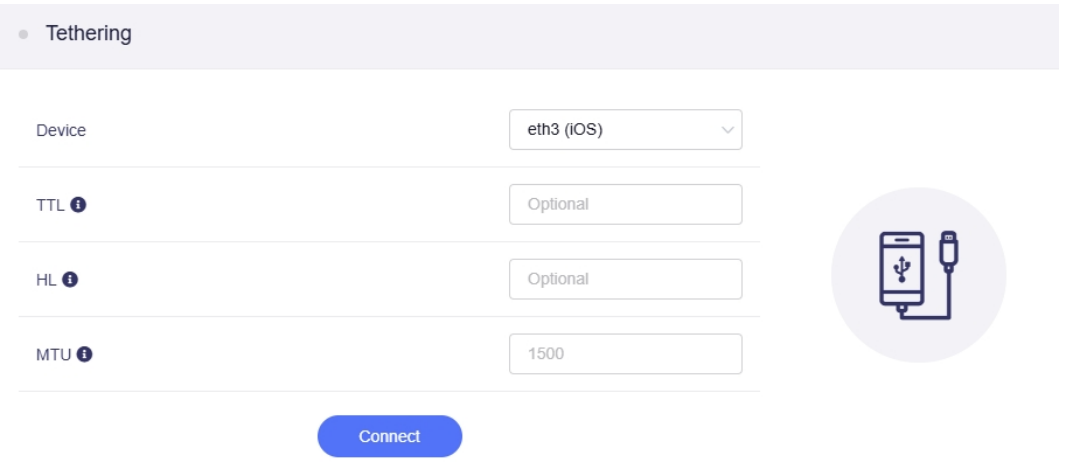
2. Na iPhonie przejdź do **Settings** > **Personal Hotspot**. Włącz **Allow Others to Join**.



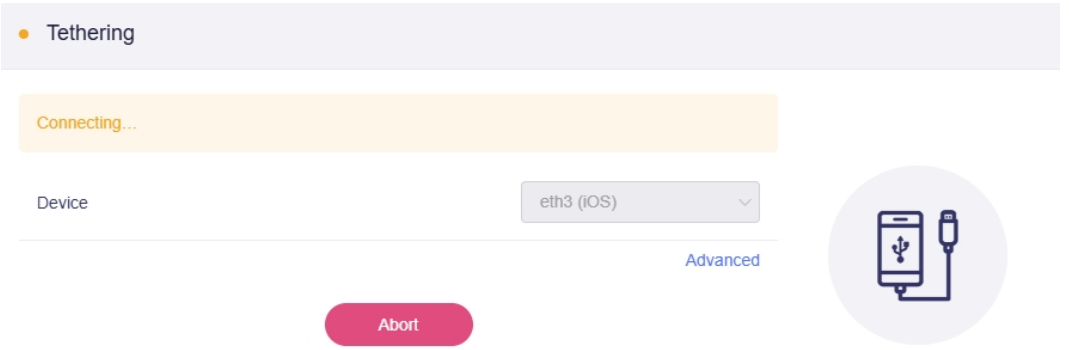
3. Podłącz komputer lub inny telefon do routera. Zaloguj się do panelu administracyjnego routera i przejdź do **INTERNET** > **Tethering**, a następnie kliknij **Connect**.



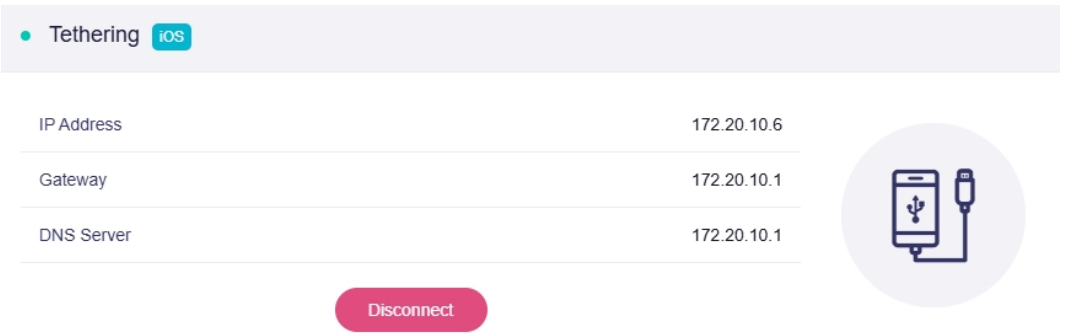
Aby dostosować ustawienia zaawansowane, takie jak TTL, HL i MTU, kliknij **Advanced** i zmień te ustawienia przed kliknięciem **Connect**.



4. Rozpocznie się nawiązywanie połączenia.

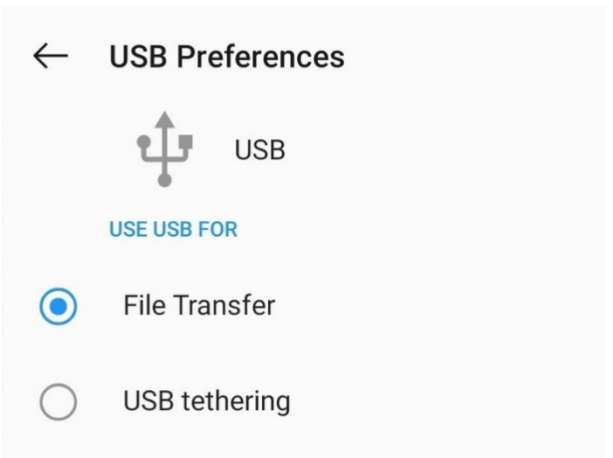


Po połączeniu na tej stronie pojawią się szczegóły połączenia tethering.

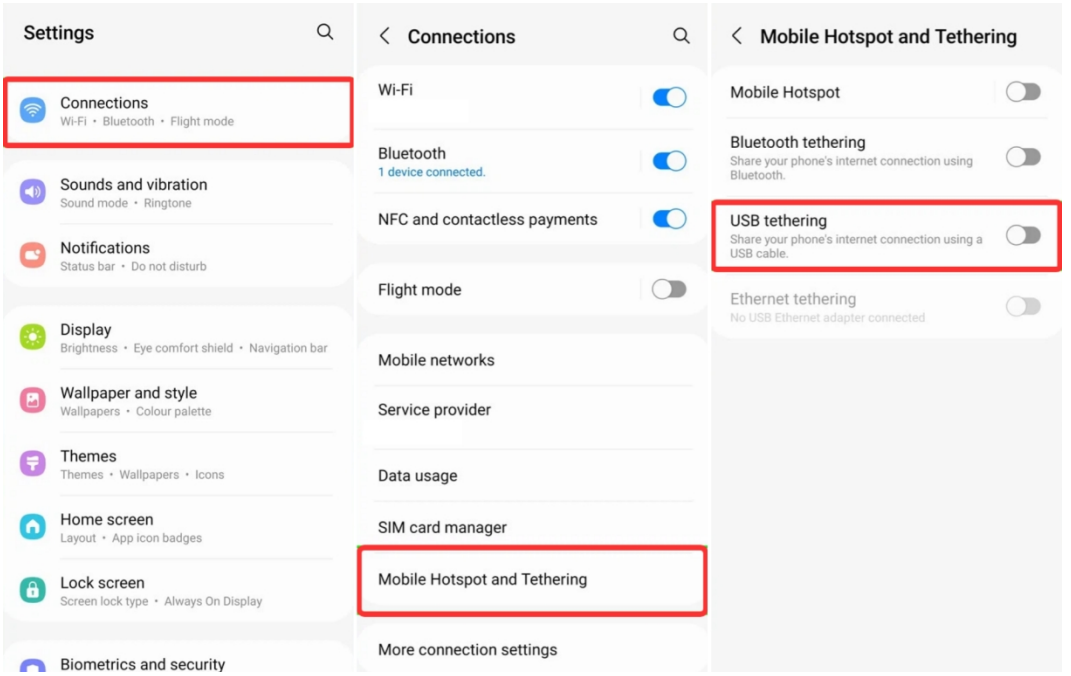


Tethering z telefonem z systemem Android

1. Podłącz telefon z systemem Android do portu USB routera za pomocą kabla USB. Może pojawić się okno systemowe z pytaniem o preferencje USB. Jeśli zostanie wyświetlone, wybierz **USB Tethering** lub **File Transfer**.

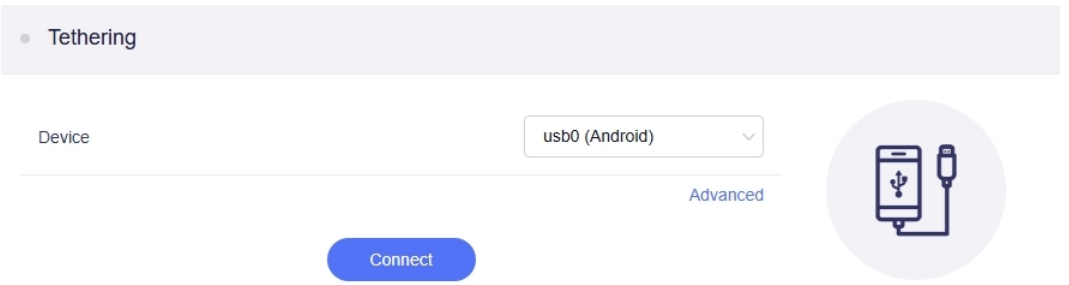


2. W telefonie przejdź do **Settings** > **Network & Internet** > **Personal Hotspot**. Włącz **Personal Hotspot** lub **USB Tethering**.

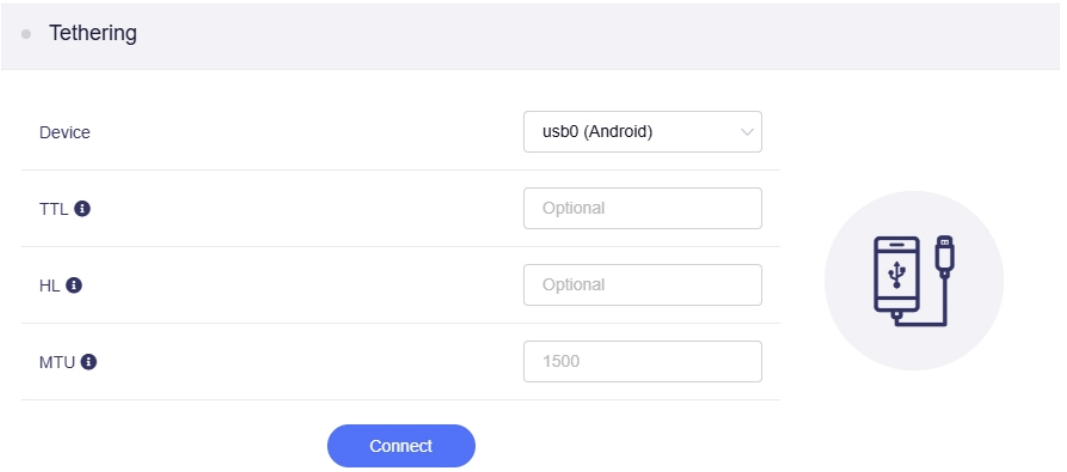


(Sposób włączania tetheringu USB zależy od producenta. Dokładną lokalizację opcji sprawdź w ustawieniach urządzenia, a w razie potrzeby skontaktuj się z pomocą techniczną producenta.)

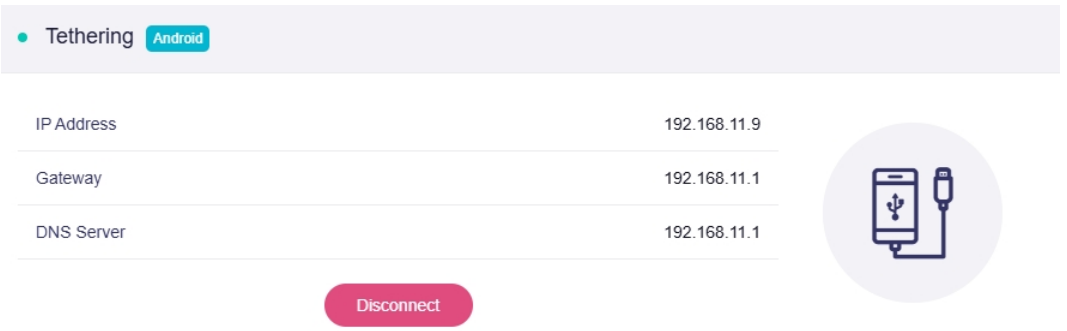
3. Podłącz komputer lub inny telefon do routera, a następnie zaloguj się do panelu administracyjnego routera i przejdź do **INTERNET** > **Tethering**. Kliknij **Connect**.



Aby dostosować ustawienia zaawansowane, takie jak TTL, HL i MTU, kliknij **Advanced** i zmień te ustawienia przed kliknięciem **Connect**.



4. Rozpocznie się nawiązywanie połączenia. Po połączeniu na tej stronie pojawi się stan połączenia tethering.



Rozwiązywanie problemów

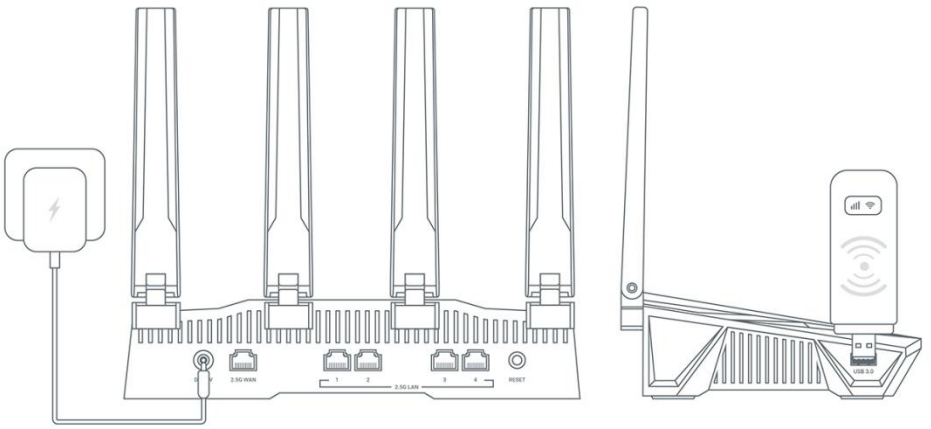
Jeśli nie uda się nawiązać połączenia tethering, wykonaj poniższe czynności:

- Użyj oryginalnego zasilacza routera.
- Odłącz i ponownie podłącz kabel USB.
- Użyj innego kabla USB. Upewnij się, że obsługuje transmisję danych, a nie tylko ładowanie.
- Kilkakrotnie wyłącz i włącz opcję „USB Tethering” (na telefonie z systemem Android).
- Kilkakrotnie wyłącz i włącz opcję „Allow Others to Join” (na iPhonie).
- Uruchom ponownie smartfon i spróbuj jeszcze raz.

Jeśli problem nadal występuje, skontaktuj się z naszą pomocą techniczną: support@gl-inet.com.

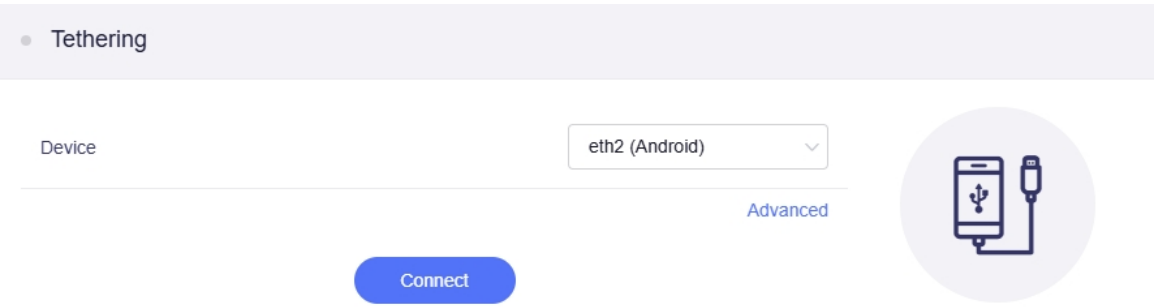
4.2.4 Połączenie z Internetem przez modem USB

Aby połączyć router z Internetem, podłącz komórkowy modem USB do jego portu USB. Umożliwia to korzystanie z Internetu przez sieci 4G/5G bez stałego łącza szerokopasmowego. Rozwiązanie sprawdza się w pojazdach lub podczas aktywności w terenie. Połączenie jest realizowane za pośrednictwem interfejsu Tethering lub Cellular routera.

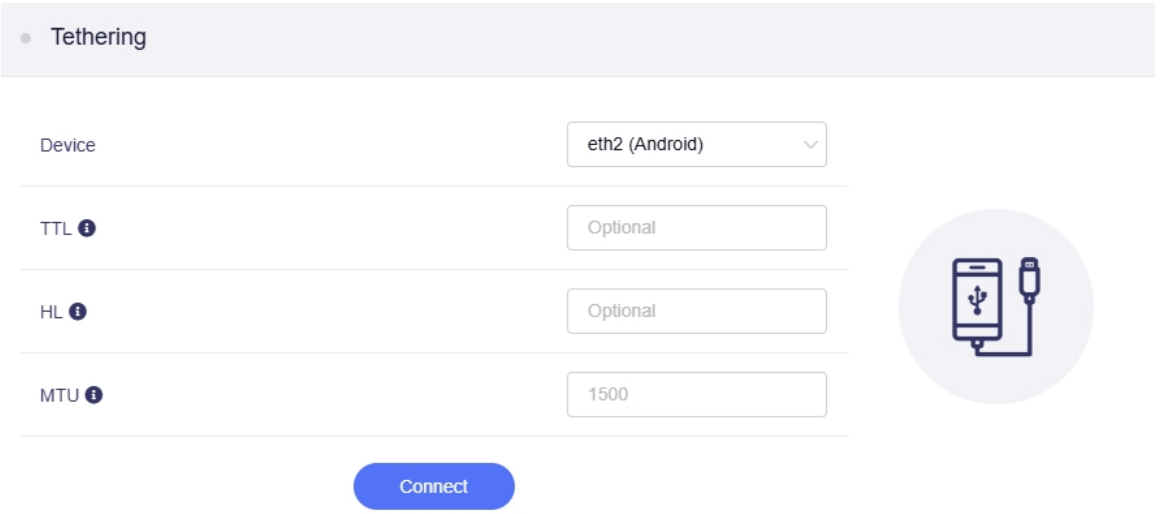


Aby połączyć router z Internetem przez modem USB, wykonaj poniższe czynności.

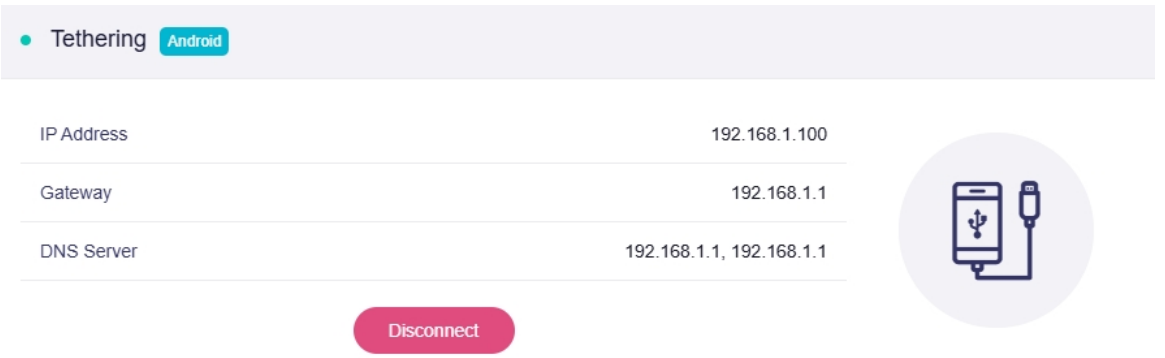
1. Przed włączeniem routera podłącz do jego portu USB modem USB z wcześniej włożoną kartą SIM.
2. Zaloguj się do panelu administracyjnego routera, przejdź do **INTERNET** > **Tethering**, a następnie kliknij **Connect**.



Aby dostosować ustawienia zaawansowane, takie jak TTL, HL i MTU, kliknij **Advanced**, zmień te ustawienia, a następnie kliknij **Connect**.

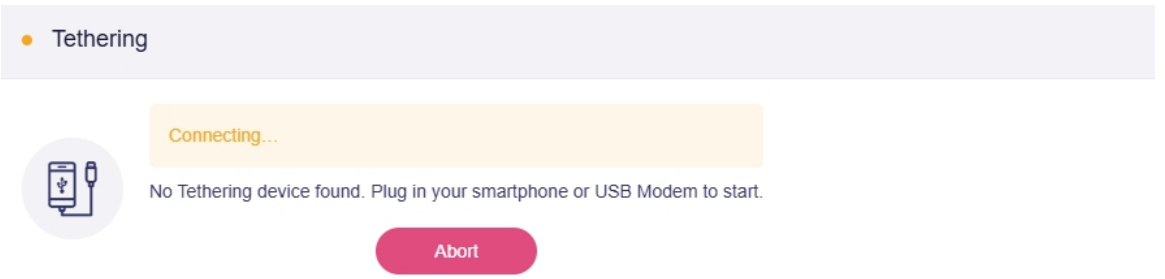


3. Rozpocznie się nawiązywanie połączenia. Po połączeniu na tej stronie pojawią się szczegóły sieci.



Wskazówki:

1. Po wstępnej konfiguracji, jeśli uruchomisz ponownie router z podłączonym modemem USB lub ponownie włożysz modem do routera, modem zostanie automatycznie rozpoznany i połączenie sieciowe zostanie nawiązane bez ponownego klikania „Connect”.
2. Po odłączeniu modemu USB strona pokaże przedstawiony poniżej stan z komunikatem „No Tethering device found”, natomiast interfejs Tethering pozostanie w stanie „Connecting”.


Tethering
Connecting...
No Tethering device found. Plug in your smartphone or USB Modem to start.
Abort

Rozdział 5

Sieć bezprzewodowa

W tym rozdziale opisano sprawdzanie stanu Wi-Fi i konfigurowanie ustawień sieci bezprzewodowej.

5.1 Wyświetlanie stanu Wi-Fi

Sieci Wi-Fi routera są domyślnie włączone, a odpowiadające im ikony Wi-Fi świecą pod ilustracją modelu urządzenia na stronie INTERNET.



Po najechaniu kursorem na ikonę włączonej sieci Wi-Fi pojawi się kod QR Wi-Fi, jak pokazano poniżej. Możesz zeskanować kod QR, aby szybko połączyć się z odpowiednią siecią Wi-Fi.



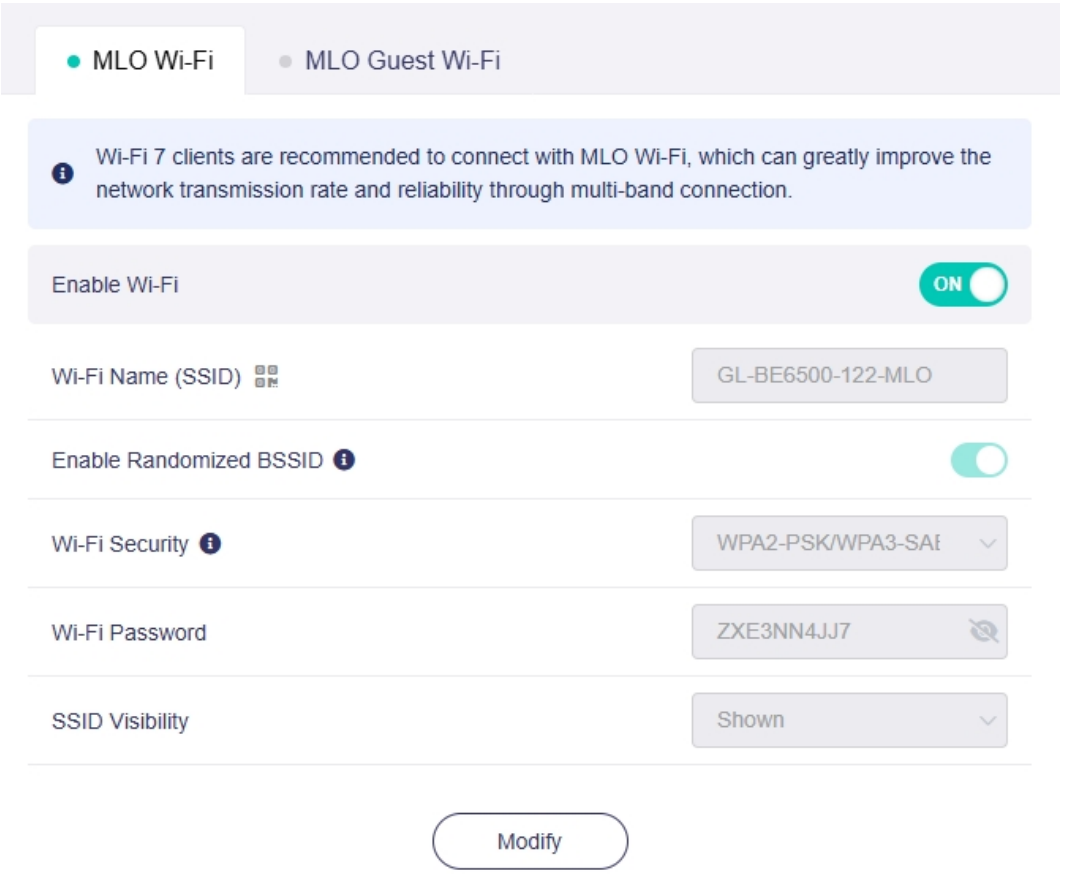
5.2 Ustawienia sieci bezprzewodowej

Zaloguj się do panelu administracyjnego routera i przejdź do **WIRELESS**.
Strona ustawień bezprzewodowych wyświetla ustawienia sieci Wi-Fi 2,4 GHz, 5 GHz i MLO routera. Każda z nich jest podzielona na sieć główną i gościnną, co zapewnia elastyczne zarządzanie.

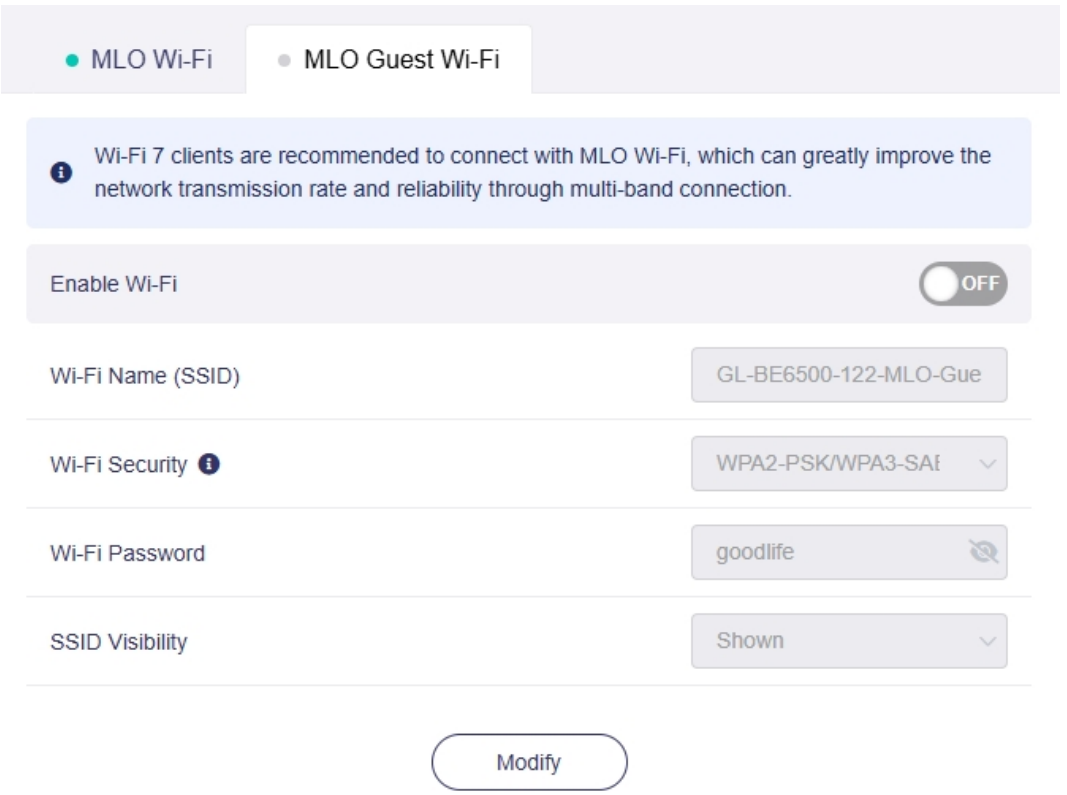
5.2.1 MLO Wi-Fi

MLO (Multi-Link Operation) to jedna z podstawowych funkcji Wi-Fi 7 (802.11be). Poprawia wydajność sieci, znacznie zmniejsza opóźnienia i zwiększa stabilność połączenia dzięki jednoczesnemu wykorzystaniu wielu pasm częstotliwości.

W głównej sieci Wi-Fi MLO można skonfigurować wiele ustawień: włączać i wyłączać Wi-Fi oraz losowy BSSID, ustawiać nazwę sieci (SSID), zabezpieczenia, hasło i widoczność SSID.

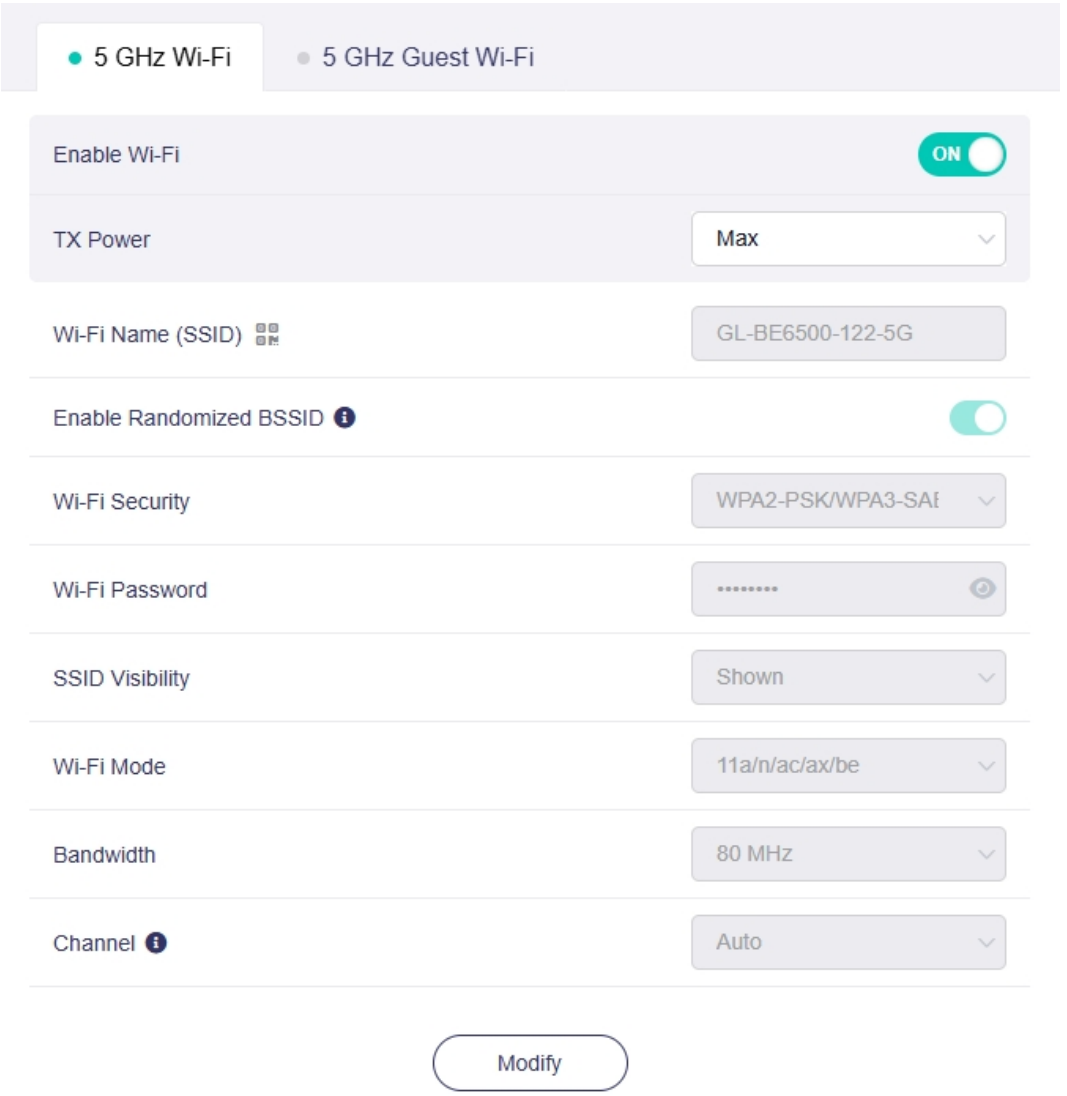


Gościnna sieć Wi-Fi MLO udostępnia uproszczone ustawienia: włączanie i wyłączanie Wi-Fi, nazwę sieci (SSID), zabezpieczenia, hasło i widoczność SSID.



5.2.2 Wi-Fi 5 GHz

W głównej sieci Wi-Fi 5 GHz można skonfigurować wiele ustawień: włączanie i wyłączanie Wi-Fi, moc nadawania, włączanie i wyłączanie losowego BSSID, nazwę sieci Wi-Fi (SSID), zabezpieczenia, hasło, widoczność SSID, tryb, szerokość kanału i kanał.

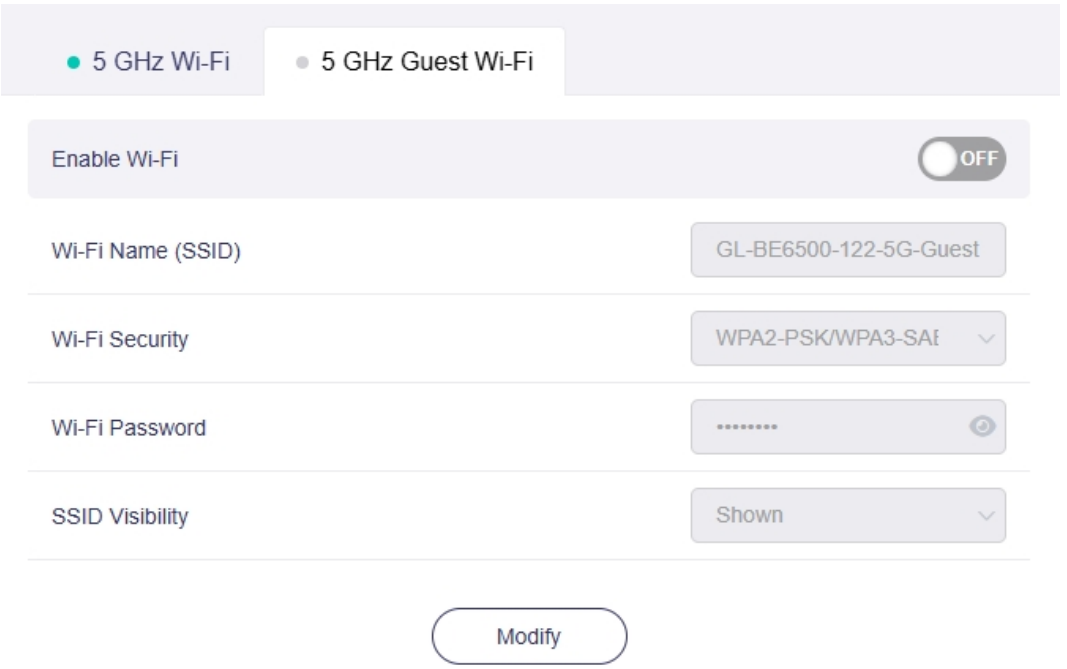


Uwaga:

1. **Randomized BSSID** jest domyślnie włączone. Pomaga zapobiegać śledzeniu routera za pomocą stałego BSSID, ponieważ urządzenia klienckie mogą przesyłać pobliskie identyfikatory BSSID i własne dane lokalizacyjne producentom systemów operacyjnych lub urządzeń, którzy tworzą z nich bazę powiązań BSSID z lokalizacją. Po włączeniu tej opcji router używa losowo generowanego BSSID i odnawia go przy każdym uruchomieniu, dzięki czemu nie można powiązać BSSID ze stałą lokalizacją.

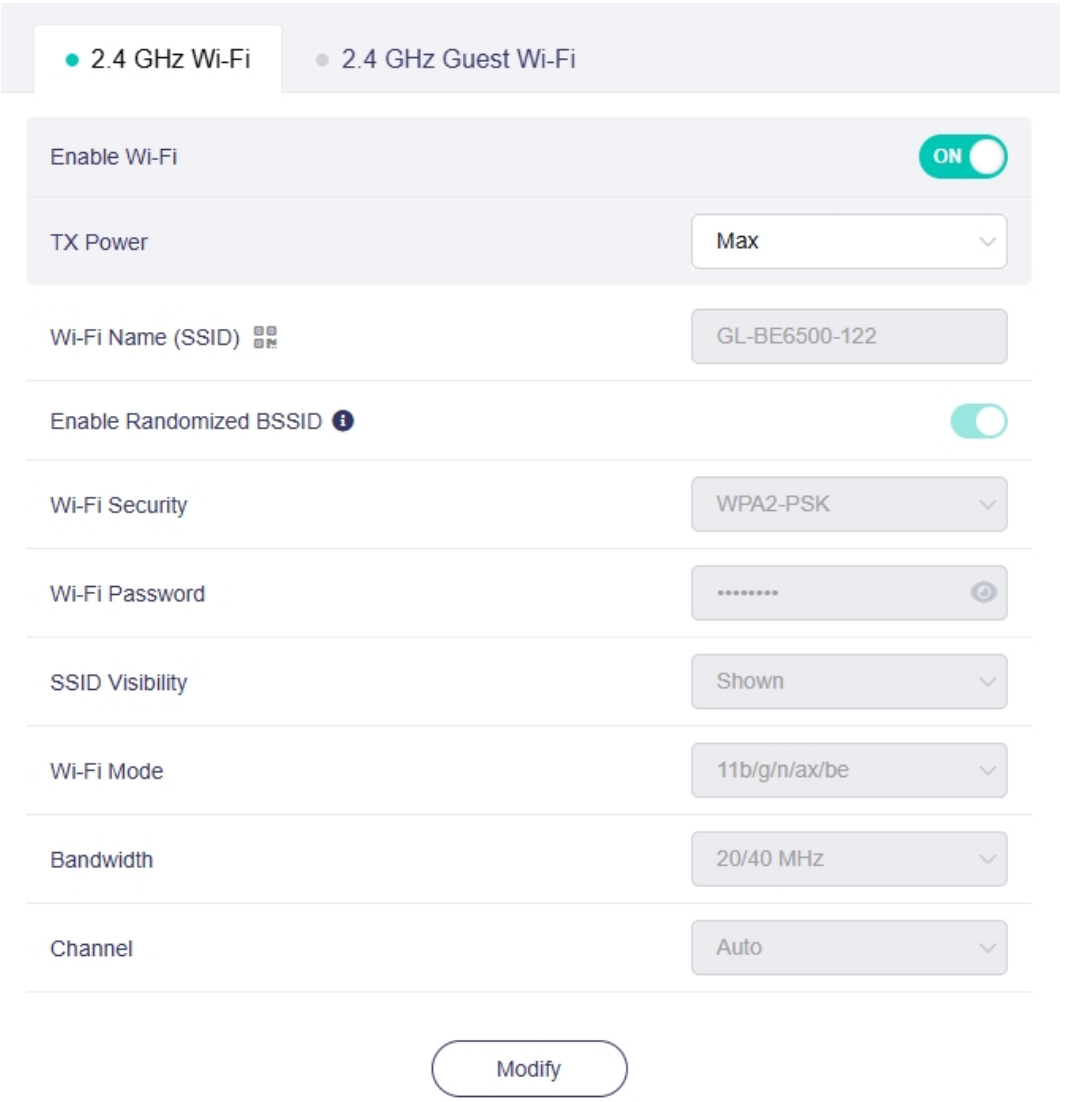
2. Ustawień **Bandwidth** i **Channel** nie można zmieniać, gdy router działa jako wzmacniacz sygnału, ponieważ są one przejmowane z sieci, której sygnał jest wzmacniany.
3. Gdy opcja **Channel** jest ustawiona na **Auto**, sieć Wi-Fi routera nie przełącza się automatycznie na kanał DFS.
4. Gdy opcja **Bandwidth** jest ustawiona na **160 MHz** (dostępne tylko w wybranych modelach), sieć Wi-Fi zawsze korzysta z kanału DFS, nawet jeśli wybierzesz kanał spoza DFS lub ustawienie Auto.

W gościnnej sieci Wi-Fi 5 GHz dostępny jest uproszczony zestaw ustawień: włączanie i wyłączanie Wi-Fi, nazwa sieci Wi-Fi (SSID), zabezpieczenia, hasło i widoczność SSID.



5.2.3 Wi-Fi 2,4 GHz

W głównej sieci Wi-Fi 2,4 GHz można skonfigurować wiele ustawień: włączanie i wyłączanie Wi-Fi, moc nadawania, włączanie i wyłączanie losowego BSSID, nazwę sieci Wi-Fi (SSID), zabezpieczenia, hasło, widoczność SSID, tryb, szerokość kanału i kanał.

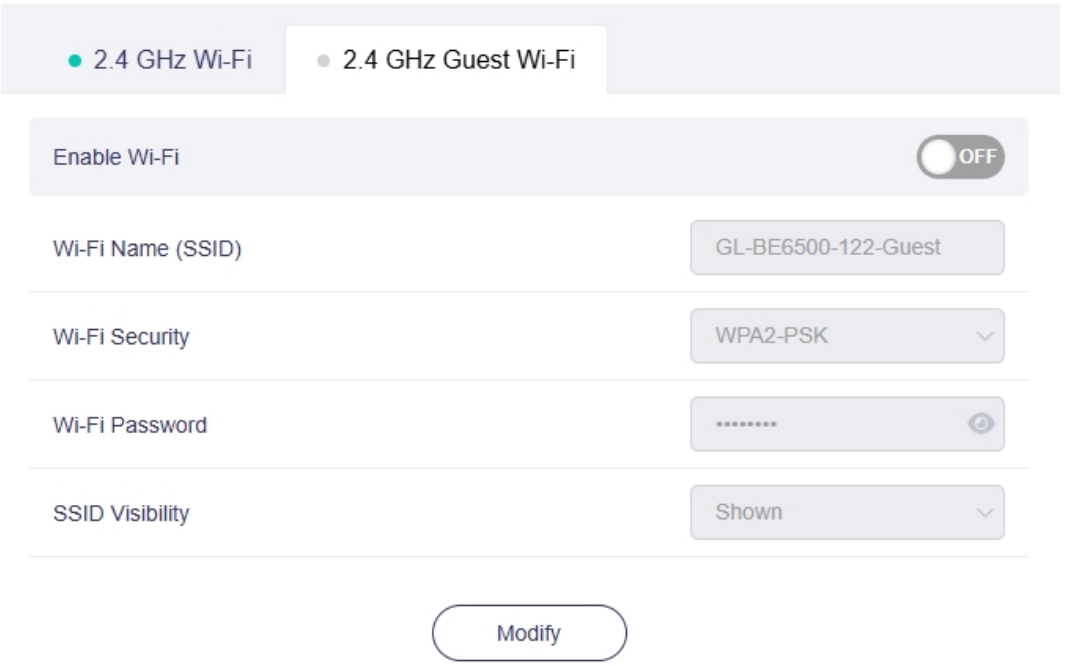


Uwaga:

1. **Randomized BSSID** jest domyślnie włączone. Pomaga zapobiegać śledzeniu routera za pomocą stałego BSSID, ponieważ urządzenia klienckie mogą przesyłać pobliskie identyfikatory BSSID i własne dane lokalizacyjne producentom systemów operacyjnych lub urządzeń, którzy tworzą z nich bazę powiązań BSSID z lokalizacją. Po włączeniu tej opcji router używa losowo generowanego BSSID i odnawia go przy każdym uruchomieniu, dzięki czemu nie można powiązać BSSID ze stałą lokalizacją.

2. Ustawień **Bandwidth** i **Channel** nie można zmieniać, gdy router działa jako wzmacniacz sygnału, ponieważ są one przejmowane z sieci, której sygnał jest wzmacniany.

W gościnnej sieci Wi-Fi 2,4 GHz dostępny jest uproszczony zestaw ustawień: włączanie i wyłączanie Wi-Fi, nazwa sieci Wi-Fi (SSID), zabezpieczenia, hasło i widoczność SSID.



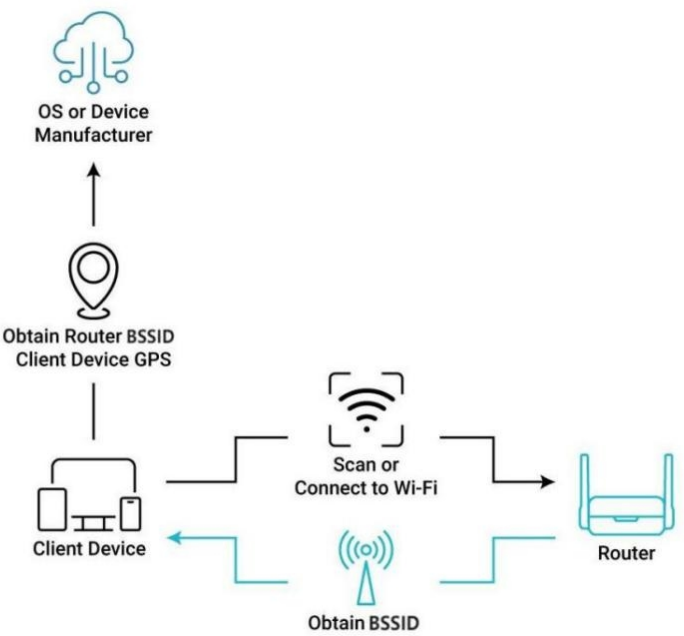
5.2.4 Losowy BSSID

Losowy BSSID to funkcja ochrony prywatności dostępna od wersji oprogramowania 4.6 i domyślnie włączona. Zapobiega ustalaniu lokalizacji i śledzeniu routera za pomocą stałego BSSID sieci Wi-Fi (adresu MAC interfejsu bezprzewodowego routera).

Dlaczego stały BSSID zagraża prywatności?

Mobilne systemy operacyjne (np. Android i iOS) korzystają ze zbiorowo gromadzonych danych o położeniu sieci Wi-Fi, aby świadczyć usługi lokalizacyjne:

1. Urządzenia klienckie (telefony, laptopy) okresowo przesyłają widoczne dla nich identyfikatory BSSID wraz z własną lokalizacją uzyskaną z GPS na serwer producenta systemu operacyjnego lub urządzenia.
2. Producenci łączą te dane w globalną bazę powiązań BSSID z lokalizacją.
3. Każde urządzenie z włączonym Wi-Fi, nawet bez GPS, może wysłać zapytanie do tej bazy, aby oszacować swoje położenie na podstawie pobliskich identyfikatorów BSSID.
4. W efekcie router ze stałym BSSID działa jak nieruchomy znacznik lokalizacji: można zdalnie ustalić jego położenie i z czasem śledzić jego przemieszczanie (np. podczas podróży). Atakujący również mogą korzystać z takich baz, aby lokalizować routery lub je identyfikować na podstawie informacji o producencie zawartej w BSSID (OUI).



Jak losowy BSSID chroni Twoją prywatność

Po włączeniu tej funkcji router generuje losowy BSSID i odnawia go przy każdym uruchomieniu. Ponieważ BSSID stale się zmienia, nie można już powiązać go ze stałą lokalizacją w bazach producentów, co zrywa używane do śledzenia powiązanie BSSID z lokalizacją.

Stan	Działanie
Włączone (domyślnie)	Przy każdym uruchomieniu generowany i odnawiany jest losowy BSSID
Wyłączone	Router używa swojego rzeczywistego fabrycznego adresu MAC jako BSSID

Uwagi:

1. BSSID zmienia się tylko po ponownym uruchomieniu routera; podczas jego pracy pozostaje taki sam.
2. W gościnnej sieci Wi-Fi BSSID pozostaje zgodny z BSSID głównej sieci Wi-Fi w tym samym paśmie częstotliwości.
3. Losowy BSSID blokuje śledzenie za pomocą BSSID routera, ale nie zapobiega przesyłaniu przez urządzenia klienckie własnej lokalizacji i nie zapewnia pełnej ochrony prywatności: nadal można obserwować SSID, kanał oraz charakterystykę sygnału.

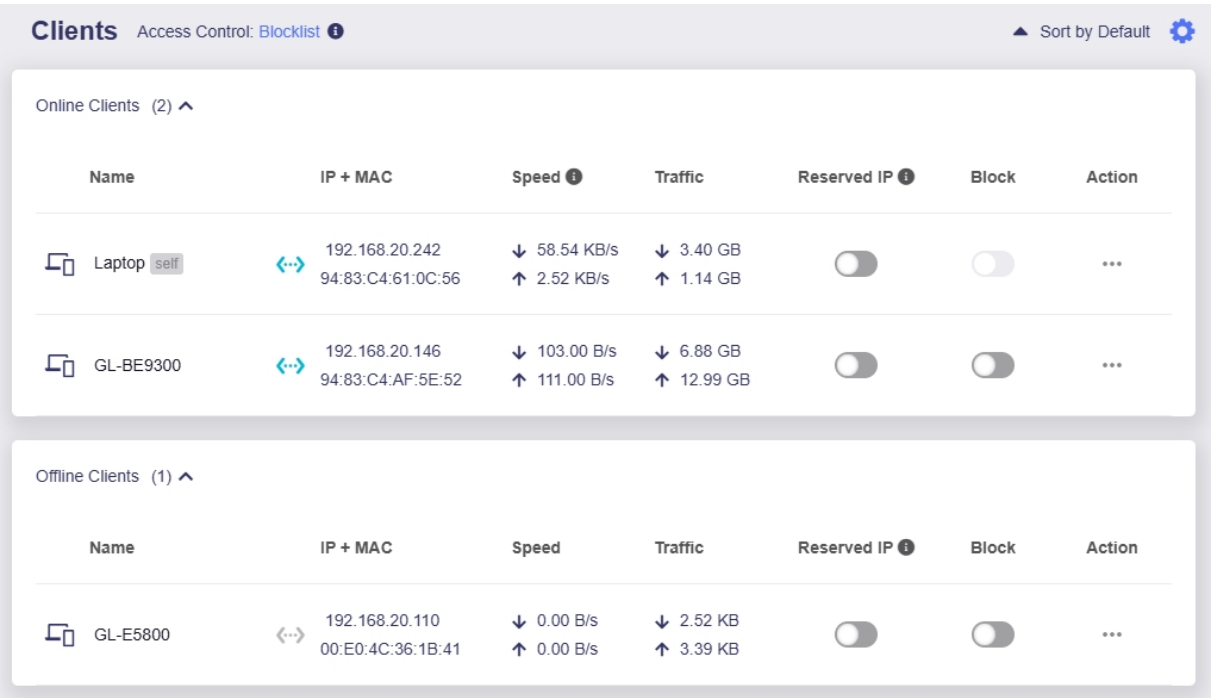
Rozdział 6

Urządzenia klienckie

W tym rozdziale opisano wyświetlanie szczegółów podłączonych urządzeń i zarządzanie ich połączeniami.

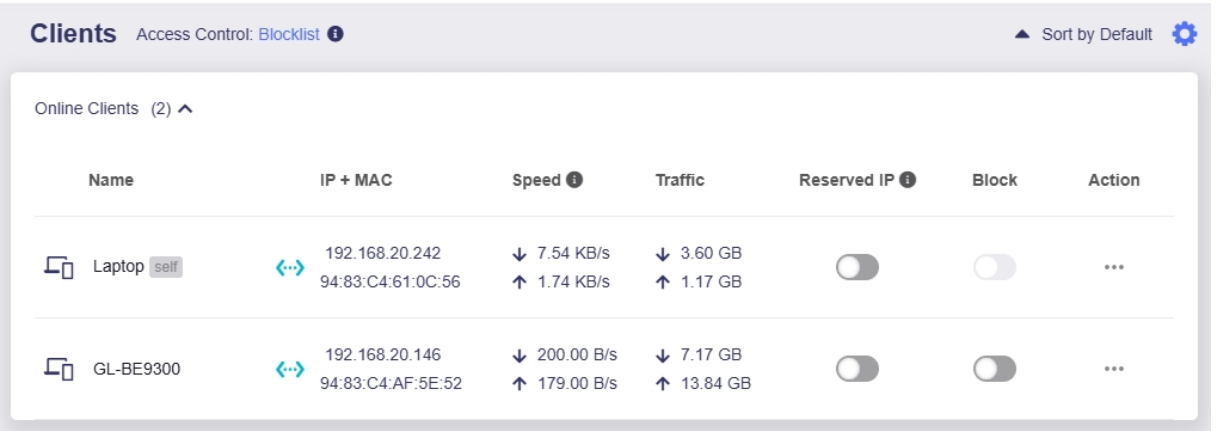
Zaloguj się do panelu administracyjnego routera i przejdź do **CLIENTS**.

Strona urządzeń klienckich przedstawia informacje o podłączonych urządzeniach, kolejno od lewej: nazwę urządzenia, rodzaj połączenia, adres IP i MAC, prędkość oraz transfer danych. Umożliwia też szybkie rezerwowanie adresu IP, blokowanie klienta i wykonywanie innych działań.



- **Online Clients**: urządzenia obecnie podłączone do sieci routera.
- **Offline Clients**: urządzenia, które wcześniej łączyły się z routerem, ale obecnie są odłączone od sieci.

6.1 Szczegóły urządzenia



1. **Nazwa urządzenia**

   Pierwsza kolumna zawiera nazwę i typ urządzenia, zależne od nazwy hosta ustawionej przez jego użytkownika. Niebieska ikona obok nazwy oznacza sposób połączenia i wskazuje, że urządzenie jest podłączone do routera kablem Ethernet.

2. **Adres IP i MAC**

   Druga kolumna zawiera adresy IP i MAC podłączonego urządzenia. Jeśli podłączone urządzenie używa losowego adresu MAC, pojawi się odpowiedni komunikat.



   Jeśli drugim znakiem adresu MAC jest 2, 6, A lub E (bez rozróżniania wielkości liter), adres jest uznawany za losowy. Niektóre urządzenia mogą jednak generować losowe adresy MAC według innej reguły, dlatego ten sposób wykrywania nie zawsze jest dokładny.

3. **Prędkość**

   Trzecia kolumna przedstawia prędkość połączenia internetowego podłączonego urządzenia. Jest to średnia z ostatnich 3 minut. System zaczyna obliczać średnią po otwarciu tej strony (np. jeśli strona jest otwarta od 10 sekund, średnia będzie oparta tylko na danych z tych 10 sekund).

4. **Transfer danych**: czwarta kolumna przedstawia transfer internetowy podłączonego urządzenia.

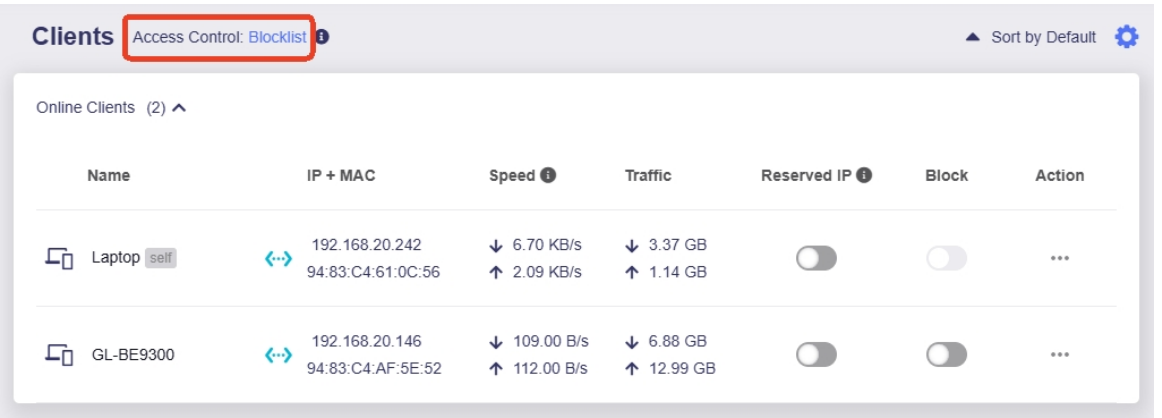
5. **Rezerwacja adresu IP**

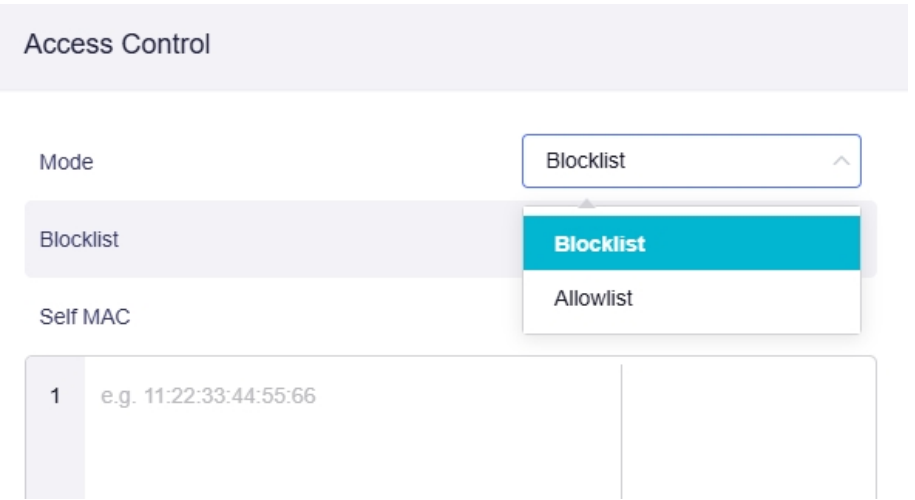
   W piątej kolumnie możesz jednym kliknięciem zarezerwować adres IP dla podłączonego urządzenia. Po przypisaniu klientowi w sieci lokalnej zarezerwowanego adresu IP będzie on otrzymywał ten sam adres przy każdym połączeniu z routerem.

6. **Lista blokowanych urządzeń**

   W szóstej kolumnie możesz jednym kliknięciem zablokować wybrane podłączone urządzenia.

   Domyślną regułą kontroli dostępu jest Blocklist. W razie potrzeby możesz przełączyć ją u góry na Allowlist.



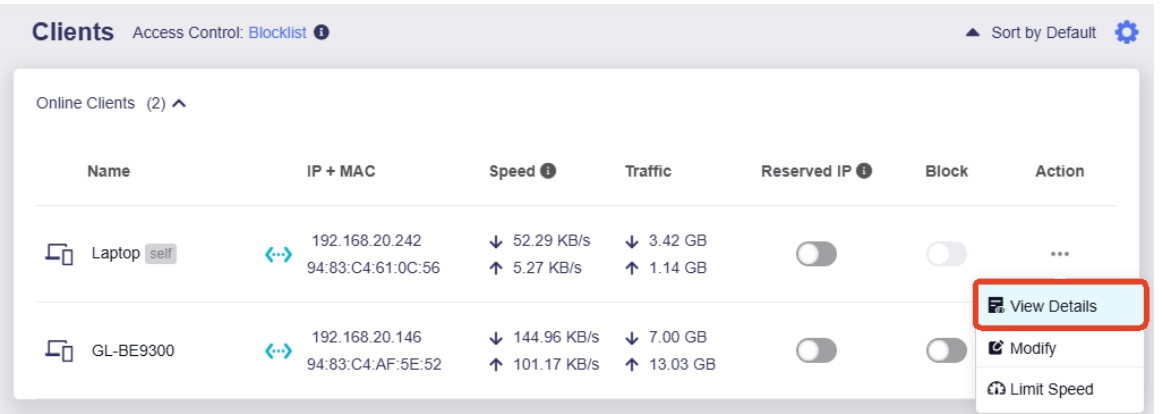


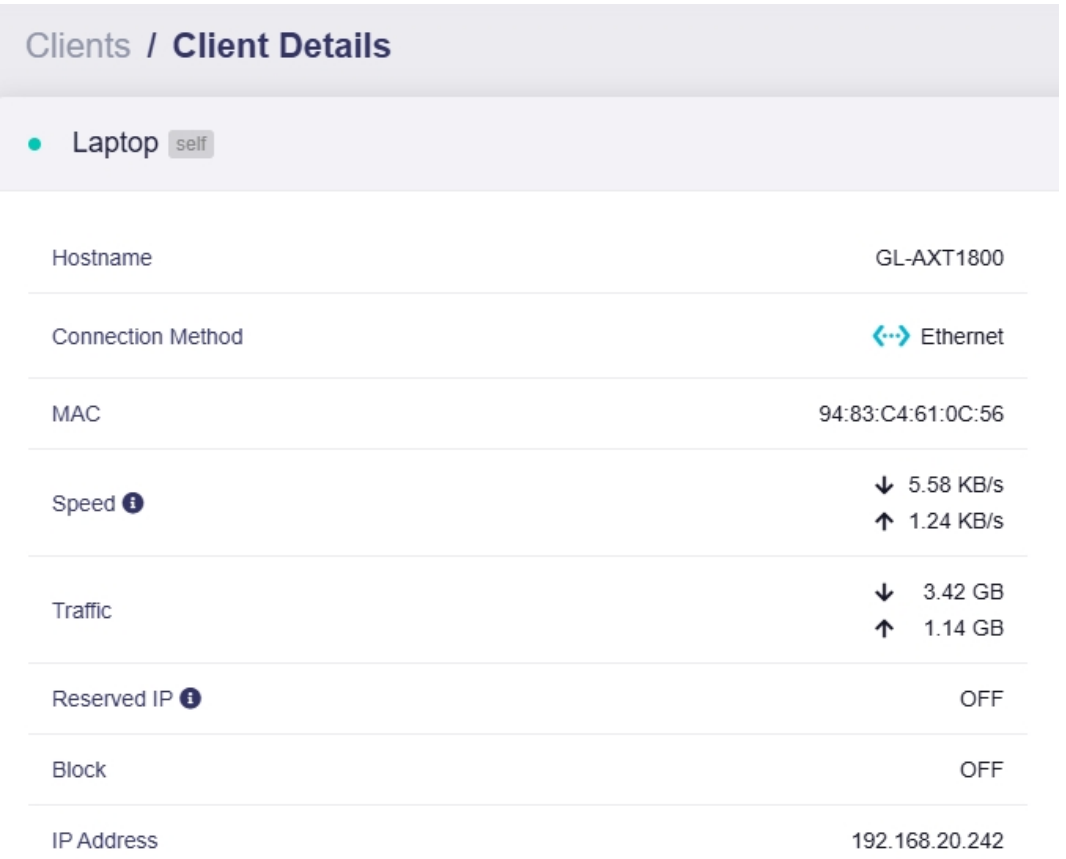
- **Blacklist**: urządzenia o adresach MAC znajdujących się na liście blokowanych nie mogą łączyć się z tym routerem. Blokowanie klienta opiera się na adresie MAC urządzenia. Jeśli zablokowane urządzenie następnym razem użyje innego adresu MAC, nadal będzie mogło połączyć się z routerem.
- **Allowlist**: z routerem mogą łączyć się tylko urządzenia o określonych adresach MAC. Ta opcja jest przydatna dla urządzeń IoT i przy zarządzaniu siecią firmową.

6.2 Działania

1. **Wyświetlanie szczegółów**

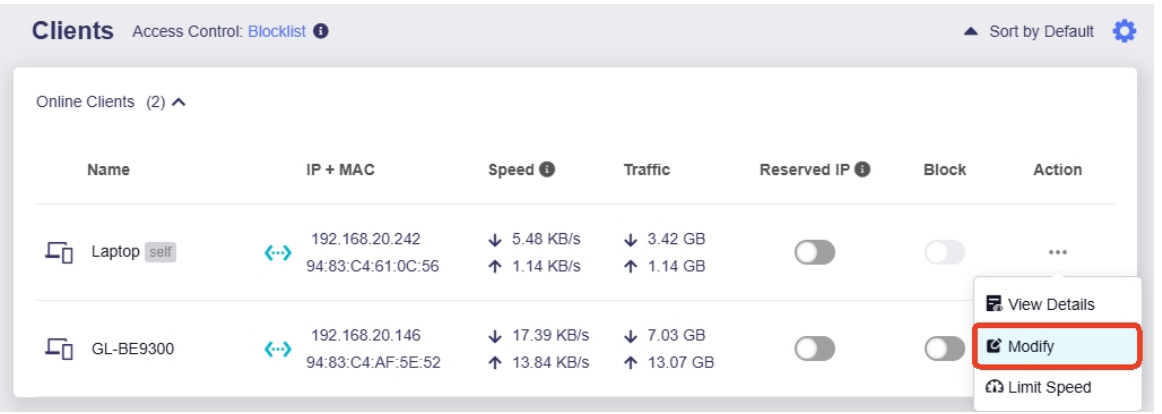
   Kliknij ikonę trzech kropek w kolumnie **Action**, a następnie wybierz **View Details** z menu, aby wyświetlić szczegóły urządzenia na jednej stronie.

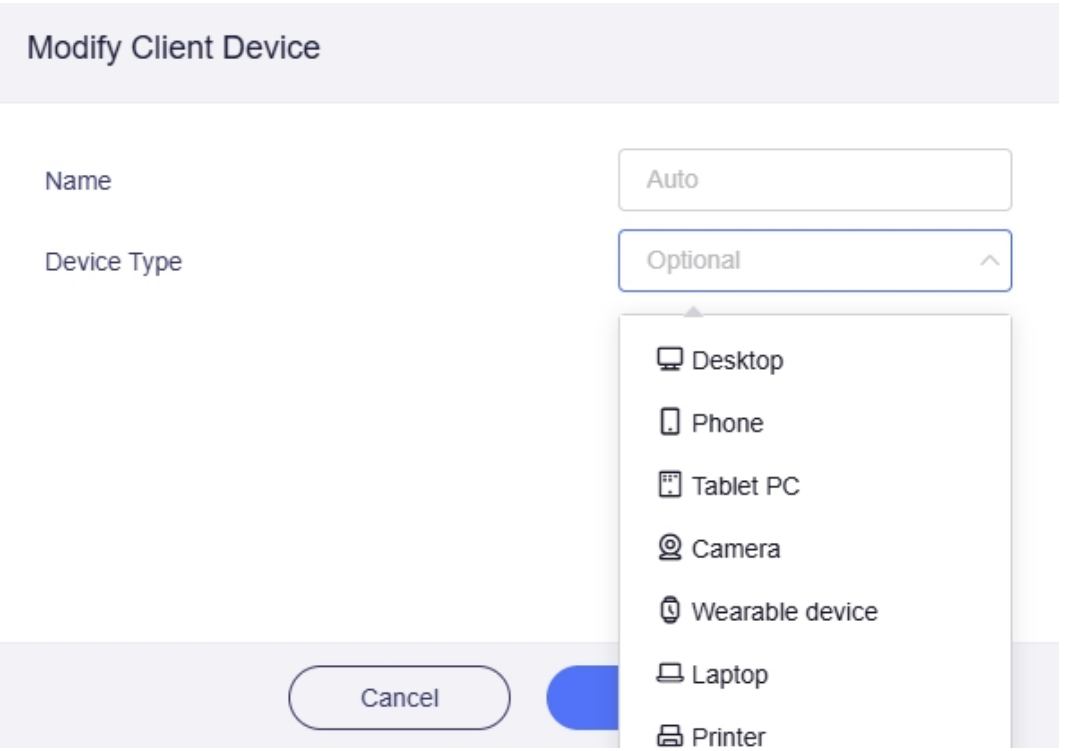




2. **Modyfikowanie**

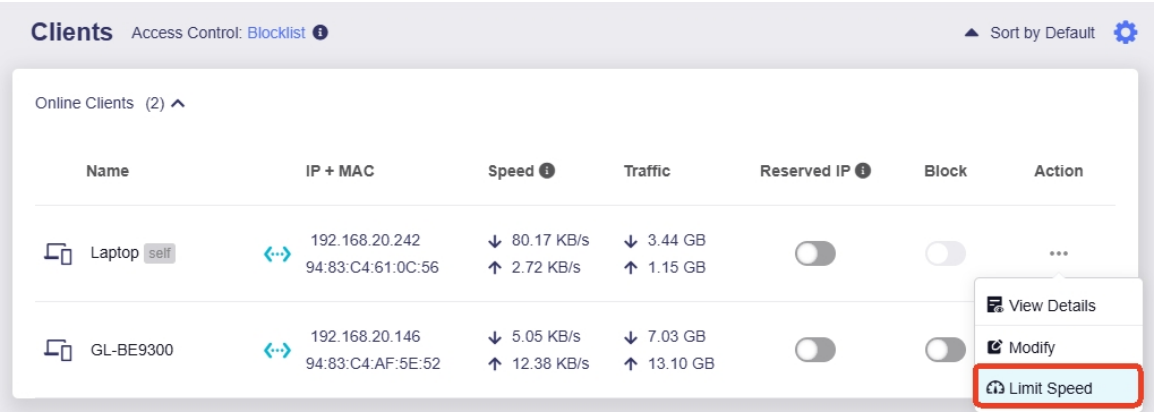
Kliknij ikonę trzech kropek w kolumnie **Action**, a następnie wybierz **Modify** z menu, aby zmienić nazwę i typ urządzenia.



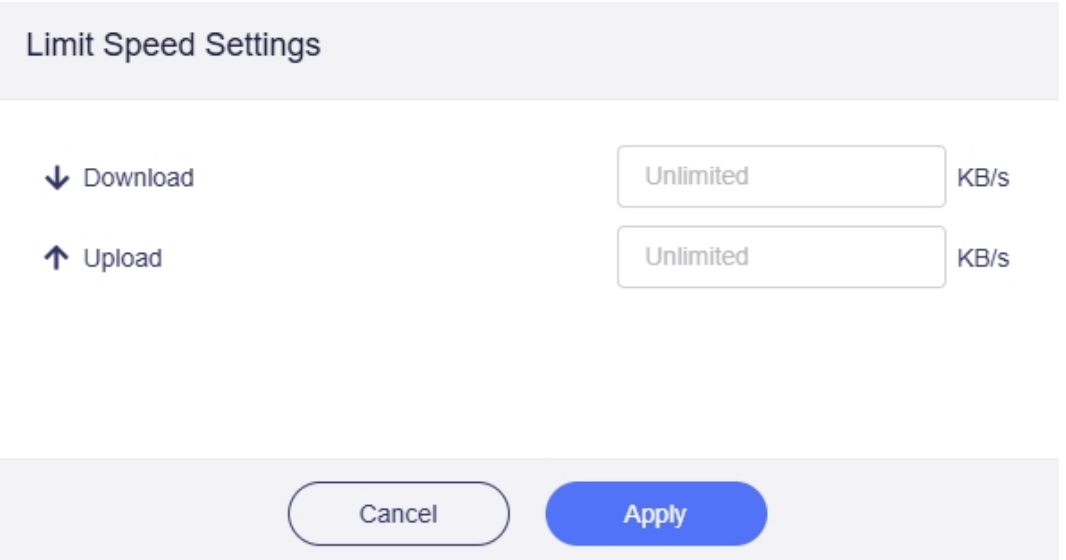


3. **Ograniczanie prędkości**

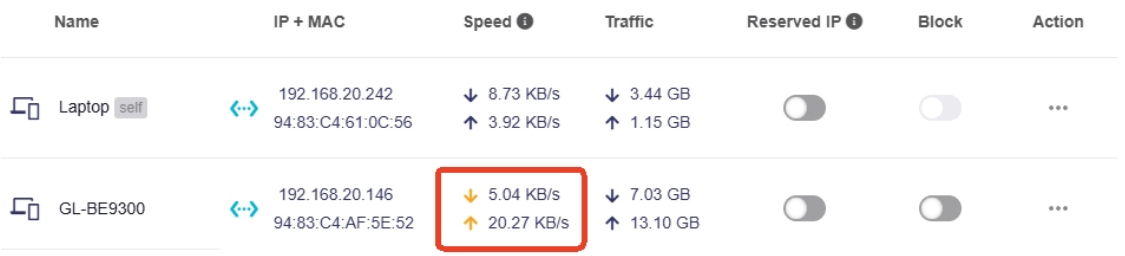
Kliknij ikonę trzech kropek w kolumnie **Action**, a następnie wybierz **Limit Speed** z menu.



Możesz ograniczyć prędkość podłączonego urządzenia, podając wartość w KB/s.



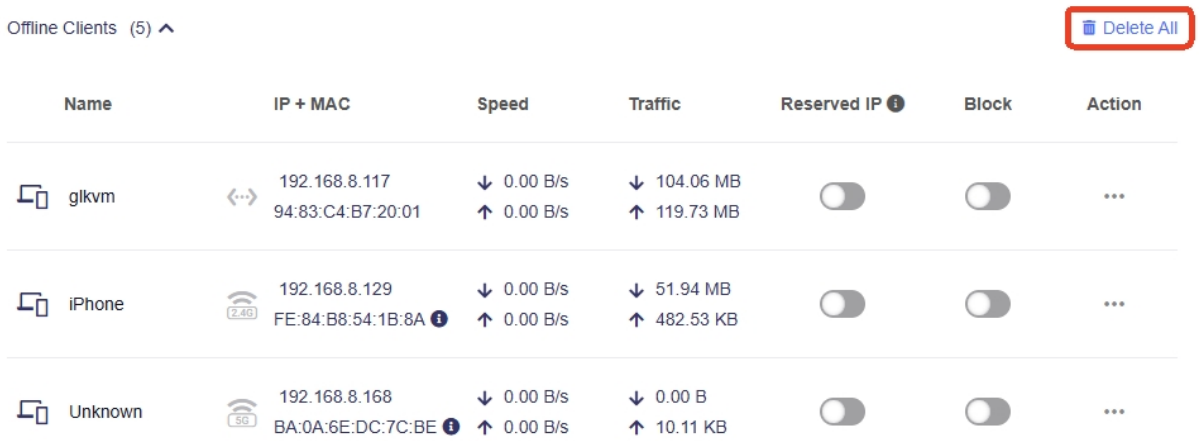
Jeśli dla urządzenia ustawiono ograniczenie prędkości, strzałki prędkości wysyłania i pobierania zmienią kolor na żółty.



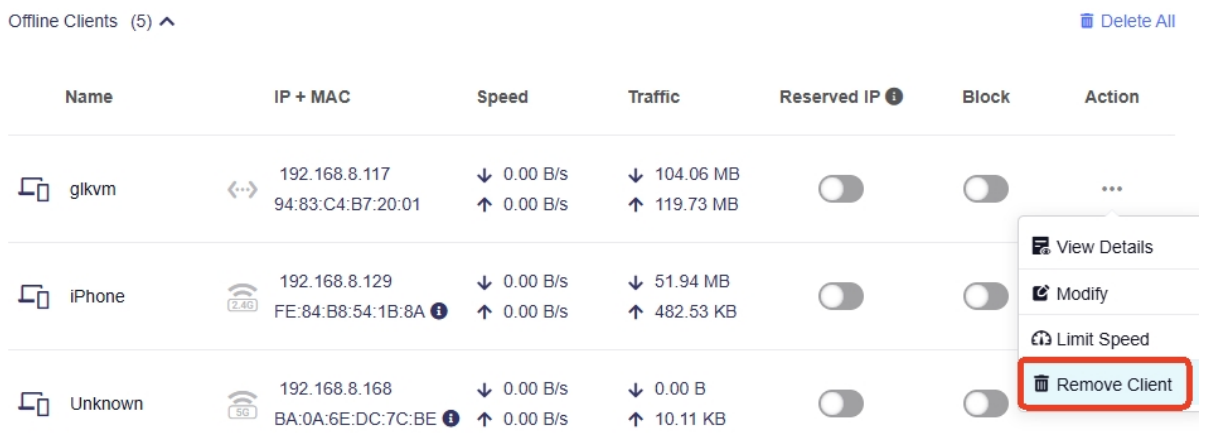
Wskazówka: jeśli opcja Limit Speed nie jest widoczna, przejdź do **NETWORK** > **Network Acceleration** i wyłącz przyspieszanie sieci. Opcja Limit Speed stanie się wtedy dostępna.

6.3 Usuwanie urządzeń klienckich

W sekcji **Offline Clients** możesz kliknąć **Delete All** w prawym górnym rogu, aby usunąć wszystkie niepodłączone urządzenia klienckie.

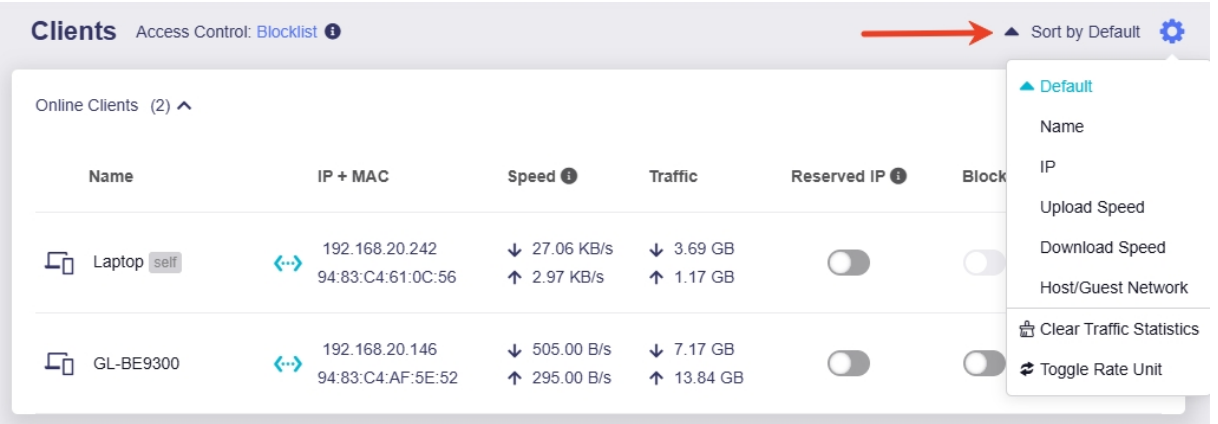


Aby usunąć określone urządzenie klienckie, kliknij ikonę trzech kropek w kolumnie **Action**, a następnie wybierz **Remove Client** z menu.



6.4 Sortowanie

Regułę sortowania urządzeń na stronie klientów możesz ustawić w prawym górnym rogu.



Domyślne reguły sortowania są następujące:

- Urządzenie, z którego korzystasz do otwierania panelu administracyjnego routera, jest zawsze wyświetlane jako pierwsze.
- W sekcji **Online Clients** urządzenia, które połączyły się wcześniej, są wyświetlane wyżej.
- W sekcji **Offline Clients** urządzenia, które rozłączyły się wcześniej, są wyświetlane wyżej.

Rozdział 7

Usługi w chmurze

W tym rozdziale przedstawiono dwie usługi w chmurze: GoodCloud i AstroWarp.

7.1 GoodCloud

GL.iNet GoodCloud to platforma ułatwiająca zdalne wdrażanie podłączonych urządzeń i zarządzanie nimi. Zapewnia prosty sposób zdalnego dostępu do routerów GL.iNet oraz ich obsługi. Centralizacja urządzeń sieciowych w chmurze pozwala sprawnie wykonywać działania zbiorcze, takie jak wdrażanie konfiguracji sieciowych i aktualizowanie oprogramowania. Użytkownicy mogą też zdalnie otwierać panel administracyjny routera lub łączyć się z jego terminalem przez SSH, zarządzając urządzeniami sieciowymi w różnych regionach od końca do końca.

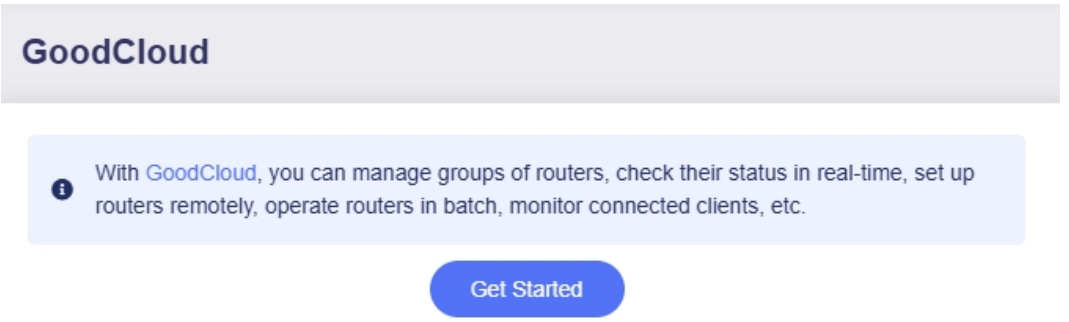
Dzięki GoodCloud możesz:

- Sprawdzać stan routera w czasie rzeczywistym
- Zarządzać grupami routerów
- Zdalnie konfigurować routery
- Monitorować podłączone urządzenia klienckie
- Wykonywać działania zbiorcze na routerach
- Tworzyć połączenia sieć–sieć

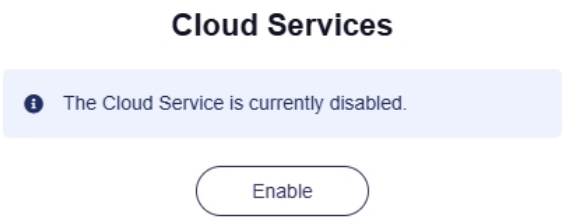
Niektóre funkcje są dostępne w planach Enterprise i VAR (Value Added Reseller). Szczegóły znajdziesz tutaj.

7.1.1 Włączanie GoodCloud

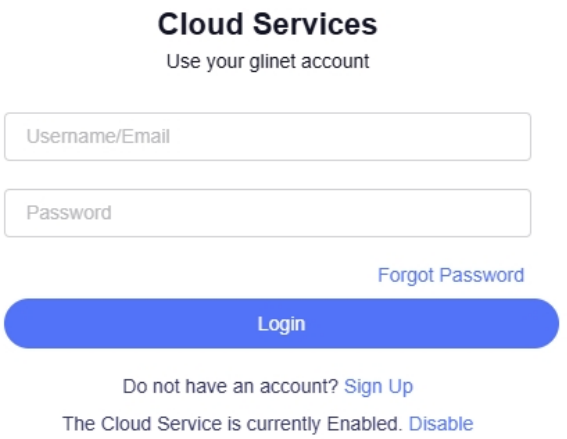
1. Zaloguj się do panelu administracyjnego routera, przejdź do **CLOUD SERVICE** > **GoodCloud** i kliknij **Get Started.**



2. W prawym górnym rogu pojawi się rozwijane okno. Kliknij **Enable**.



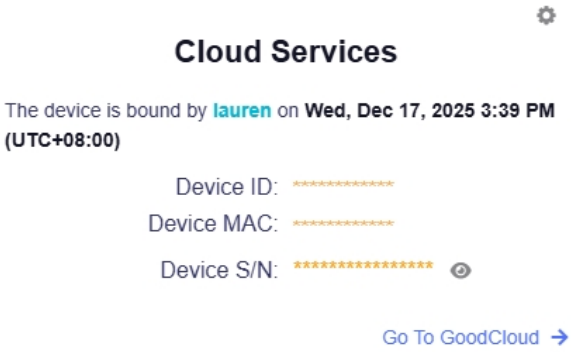
3. Zaloguj się na swoje konto GL.iNet Cloud. Jeśli nie masz konta, zarejestruj je i zaloguj się. Po zalogowaniu router zostanie automatycznie powiązany z Twoim kontem.



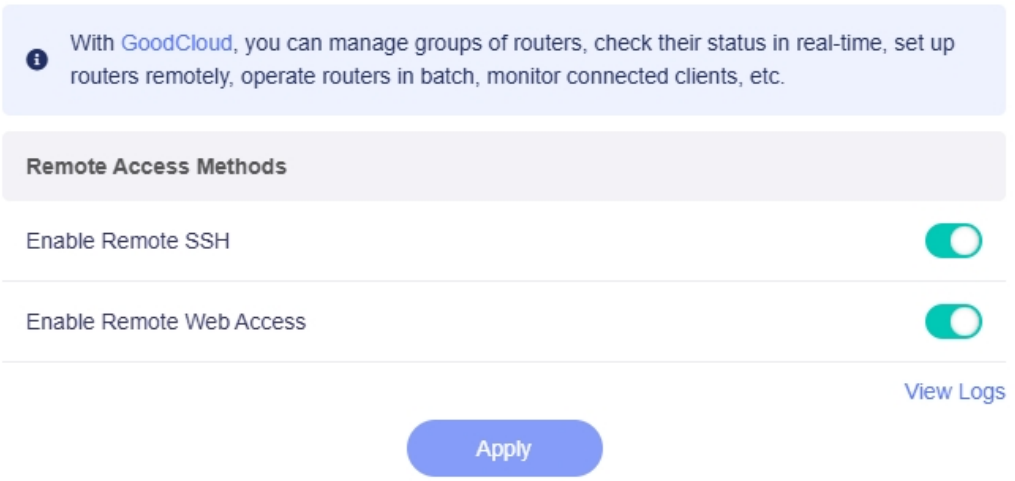
Wskazówki:

- Sposób powiązania z GoodCloud zależy od wersji oprogramowania.
- Jeśli nie otrzymasz wiadomości weryfikacyjnej, sprawdź folder spamu lub spróbuj później. Aby uzyskać dodatkową pomoc, napisz na support@gl-inet.com.

4. Po pomyślnym powiązaniu kliknij **ikonę chmury** w prawym górnym rogu panelu administracyjnego. Wyświetlą się szczegóły powiązanego urządzenia: powiązane konto, data powiązania, Device ID, Device MAC i Device S/N.



5. Przejdź do **CLOUD SERVICES** > **GoodCloud** i włącz dostęp zdalny. GoodCloud zapewnia zdalny dostęp do panelu administracyjnego i terminala powiązanego routera. Jest to szczególnie przydatne przy zdalnym zarządzaniu, konfiguracji sieci i rozwiązywaniu problemów. Tutaj możesz włączyć lub wyłączyć dostęp zdalny do routera.

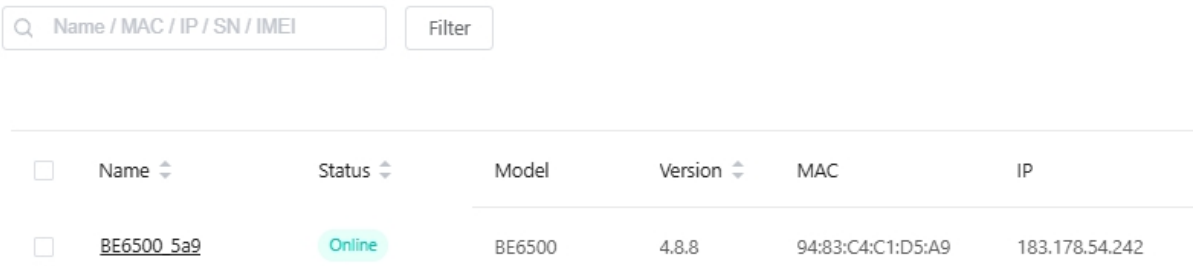


- **Remote SSH**: umożliwia zdalny dostęp do terminala routera z GoodCloud przez SSH.
- **Remote Web Access**: umożliwia zdalny dostęp do panelu administracyjnego routera z GoodCloud przez HTTP/HTTPS.
- **View Logs**: otwiera stronę dziennika i wyświetla dziennik chmury.

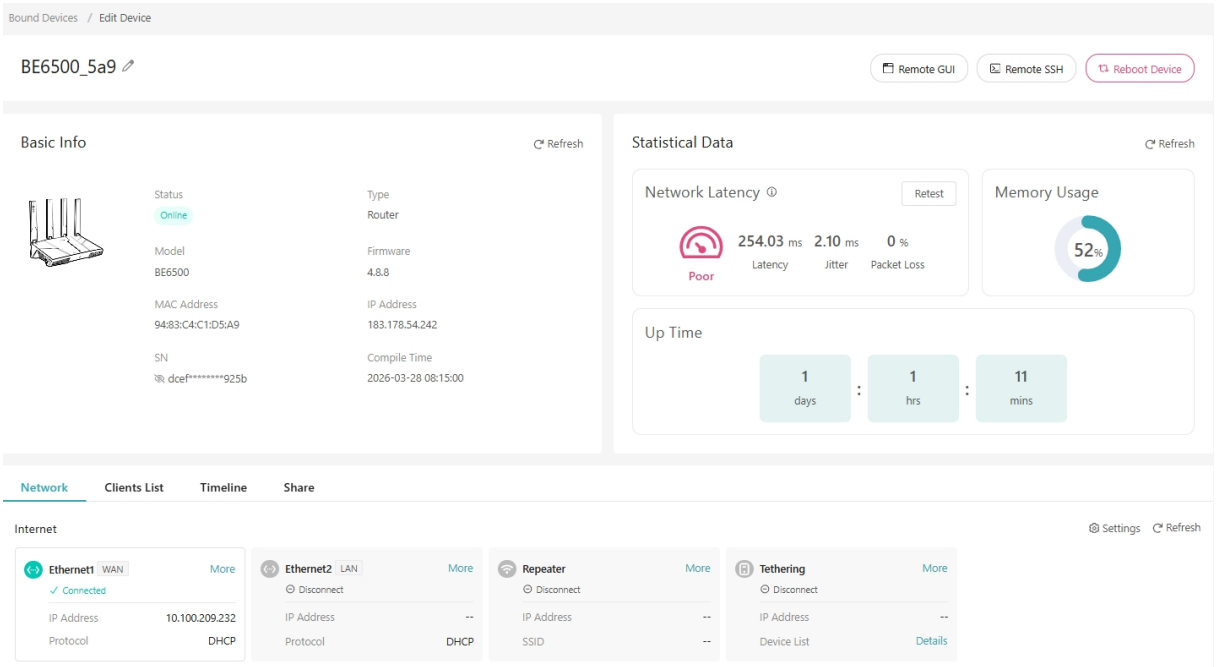
7.1.2 Zarządzanie routerem

Sprawdzanie szczegółów urządzenia

Zaloguj się na platformie GoodCloud i przejdź do **Device** > **Bound Devices**. Możesz sprawdzić podstawowe informacje o urządzeniu: nazwę hosta, stan (online/offline), model, wersję oprogramowania i adres MAC.

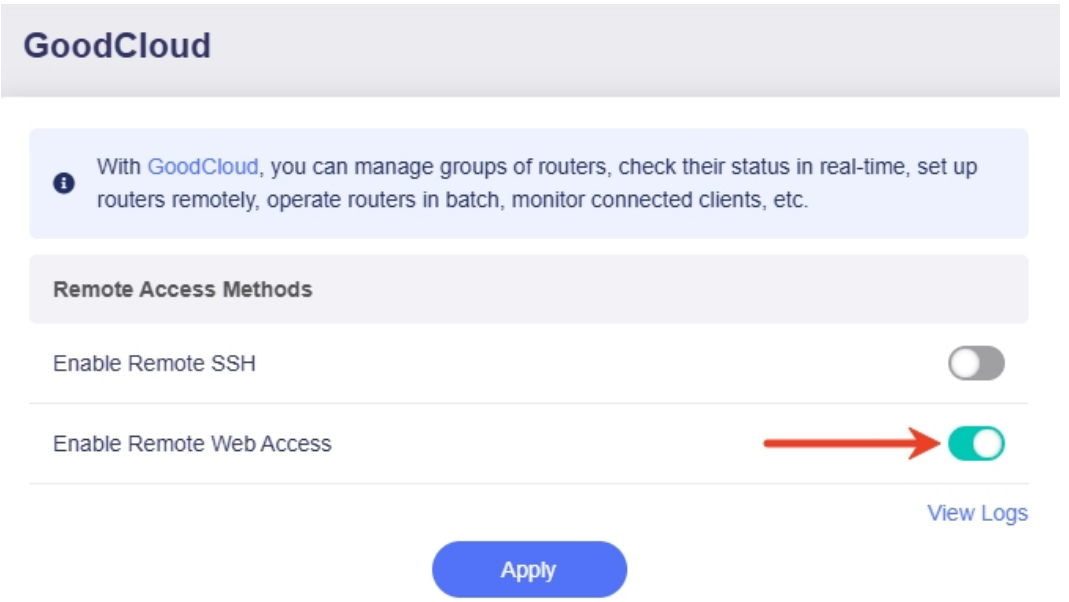


Kliknij nazwę urządzenia, aby otworzyć stronę szczegółów zawierającą podstawowe informacje, statystyki, przegląd sieci, listę klientów i oś czasu. Możesz też wykonywać zaawansowane działania, np. zdalnie uzyskiwać dostęp do routera i uruchamiać go ponownie.

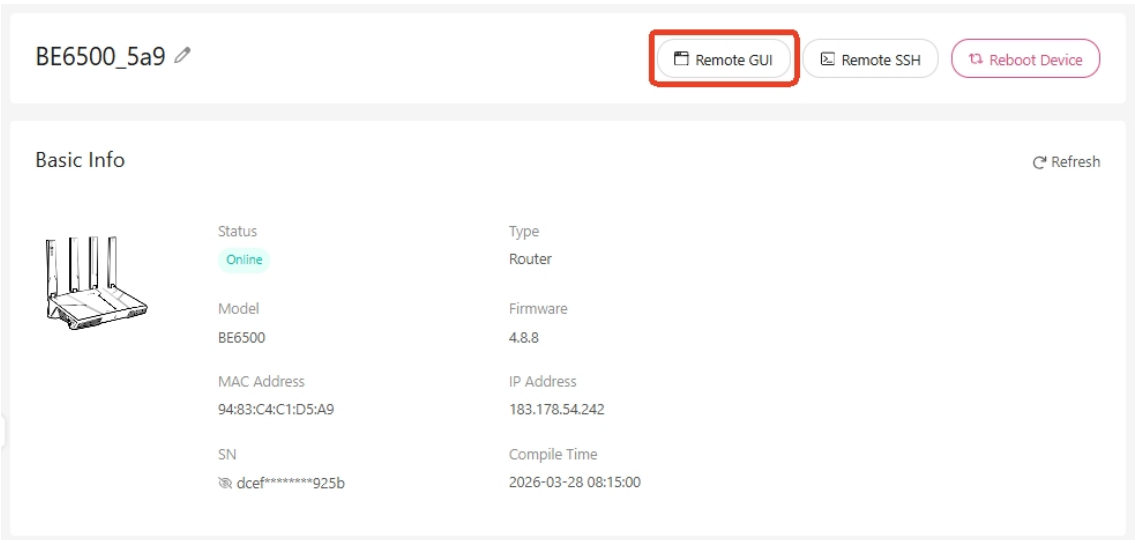


Zdalny dostęp przez przeglądarkę

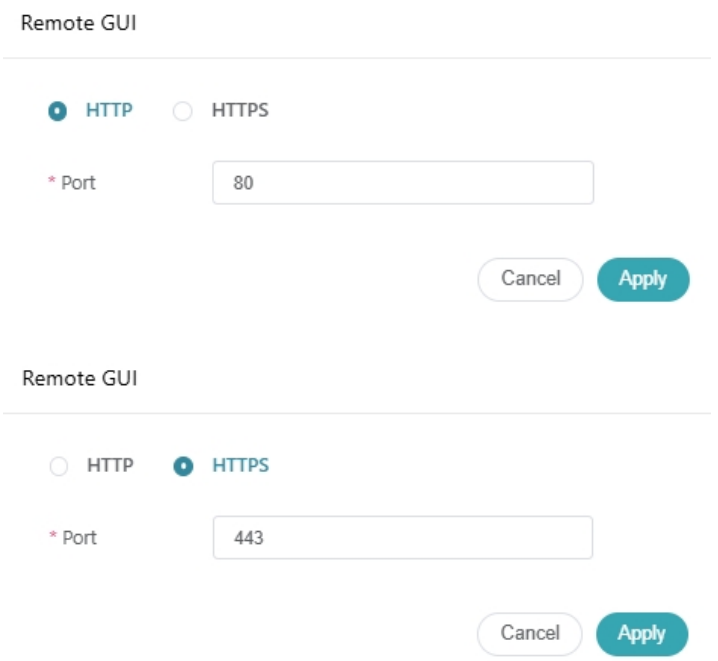
1. Zaloguj się do panelu administracyjnego routera, przejdź do **CLOUD SERVICES** > **GoodCloud**, włącz **Remote Web Access**, a następnie kliknij **Apply**.



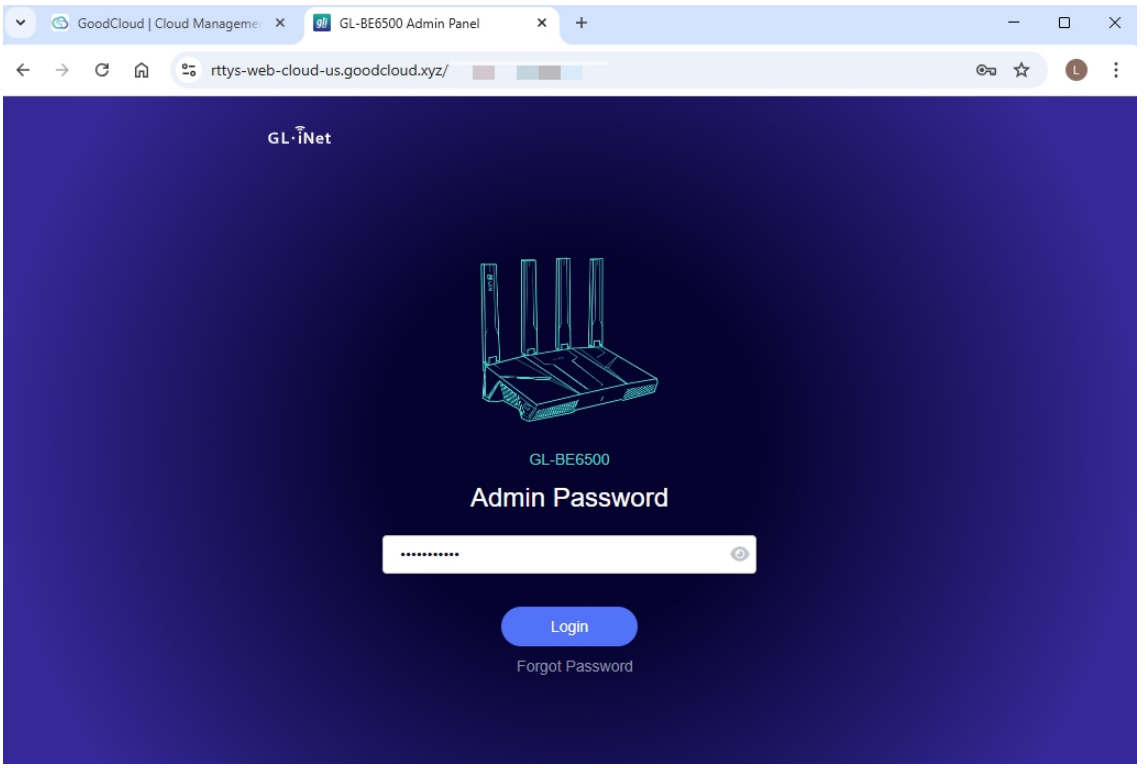
2. Zaloguj się na platformie GoodCloud i przejdź do **Device** > **Bound Devices**. Kliknij urządzenie, do którego chcesz uzyskać dostęp, aby otworzyć stronę jego szczegółów.
3. Na stronie szczegółów urządzenia kliknij przycisk **Remote GUI** w prawym górnym rogu.



4. Wybierz protokół transmisji i port. Domyślne wartości to **HTTP** i port **80**. W razie potrzeby możesz wybrać HTTPS; port automatycznie zmieni się na 443. Następnie kliknij **Apply**.

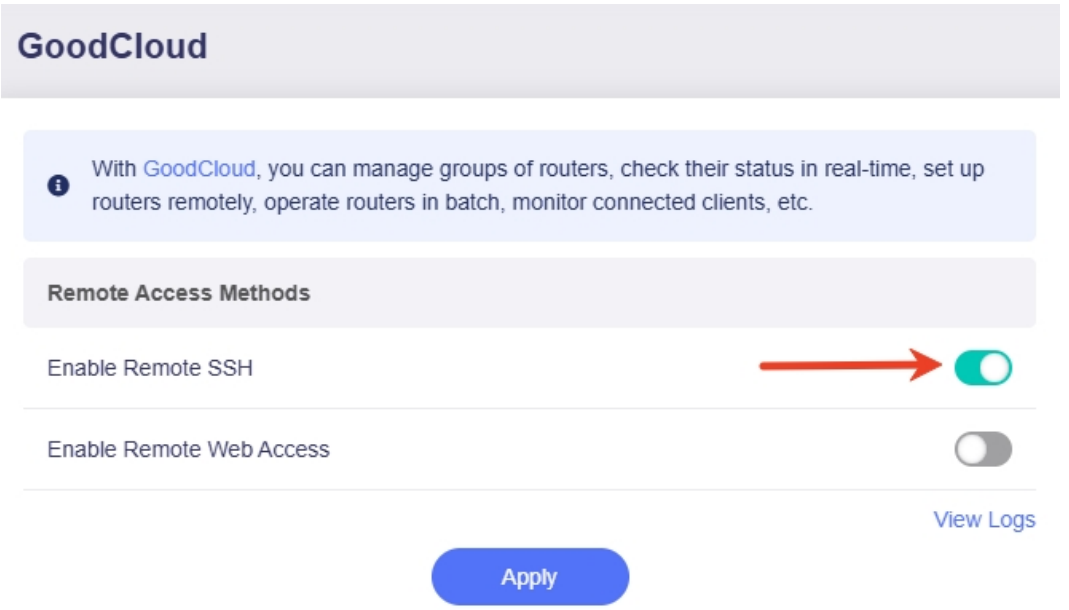


5. Otworzy się strona logowania routera. Wprowadź hasło administratora, aby uzyskać zdalny dostęp do panelu administracyjnego routera.

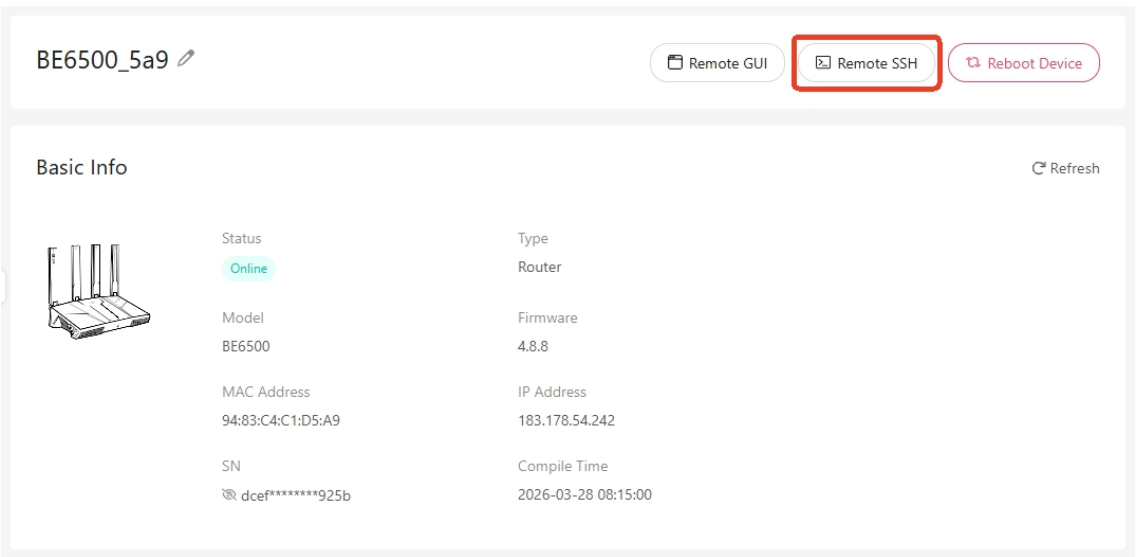


Zdalny dostęp do terminala

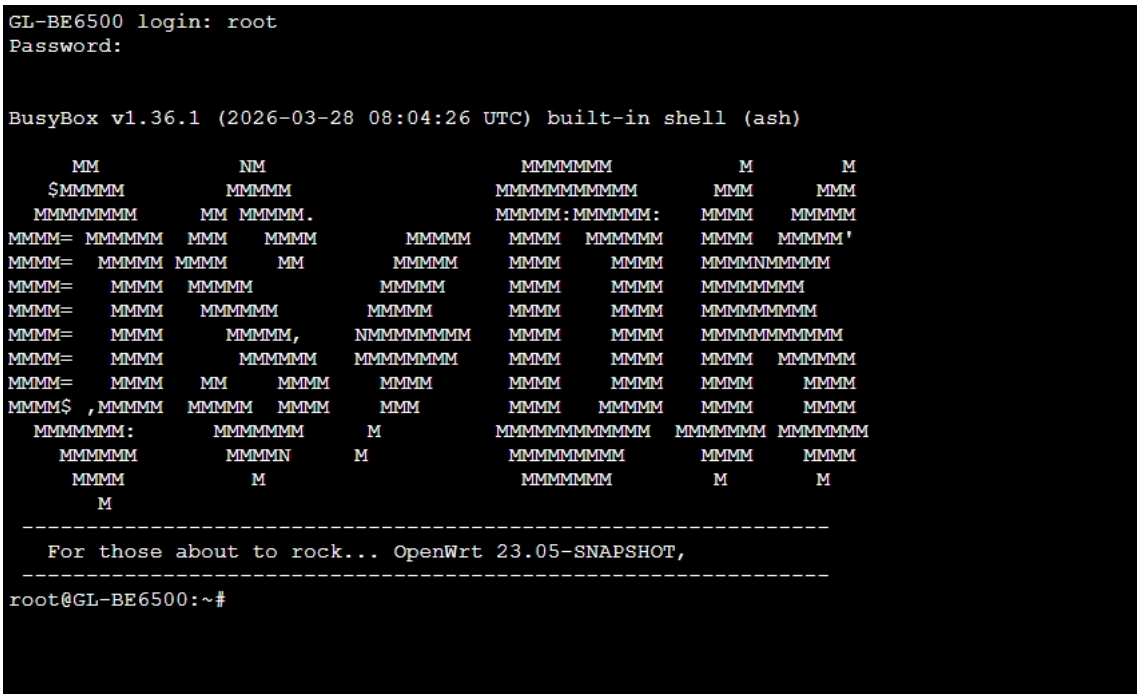
1. Zaloguj się do panelu administracyjnego routera, przejdź do **CLOUD SERVICES** > **GoodCloud**, włącz **Remote SSH**, a następnie kliknij **Apply**.



2. Zaloguj się na platformie GoodCloud i przejdź do **Device** > **Bound Devices**. Kliknij urządzenie, do którego chcesz uzyskać dostęp, aby otworzyć stronę jego szczegółów.
3. Na stronie szczegółów urządzenia kliknij przycisk **Remote SSH** w prawym górnym rogu.

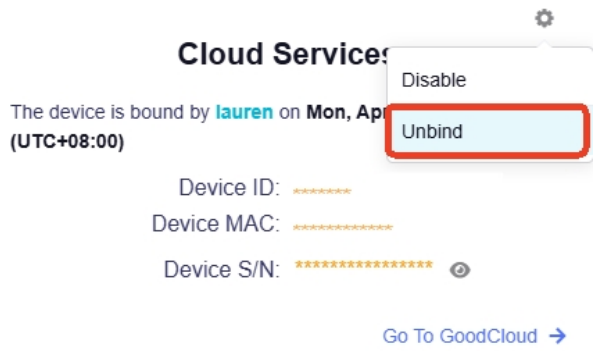


4. Zaloguj się jako **root** i wprowadź hasło, aby uzyskać dostęp do terminala routera.

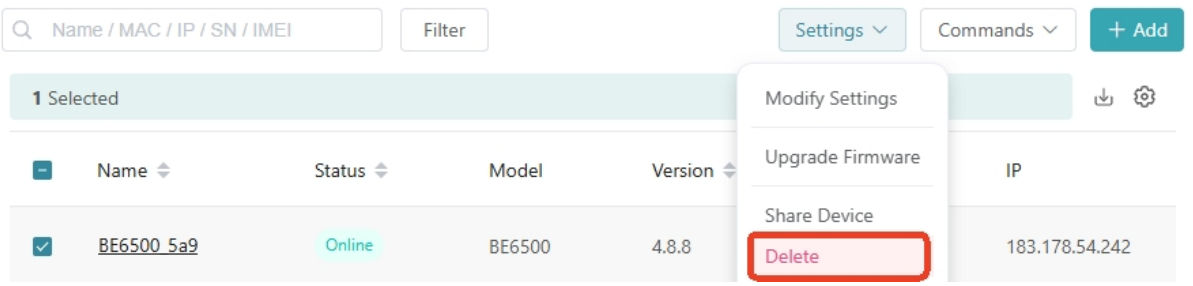

GL-BE6500 login: root
Password:
BusyBox v1.36.1 (2026-03-28 08:04:26 UTC) built-in shell (ash)
For those about to rock... OpenWrt 23.05-SNAPSHOT,
root@GL-BE6500:~#

7.1.3 Usuwanie powiązania urządzenia

W panelu administracyjnym routera kliknij ikonę chmury w prawym górnym rogu. W rozwijanym menu kliknij ikonę koła zębatego i wybierz **Unbind**. Urządzenie zostanie odłączone od konta GoodCloud.

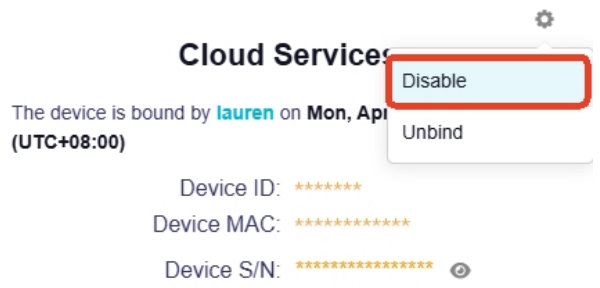


Możesz też zalogować się na platformie chmurowej i przejść do **Device** > **Bound Devices**. Wybierz urządzenie do odłączenia, kliknij **Settings** w prawym górnym rogu, a następnie wybierz **Delete**. Urządzenie zostanie odłączone od konta GoodCloud.



7.1.4 Wyłączanie GoodCloud

Jeśli nie chcesz już łączyć urządzenia z chmurą, kliknij ikonę chmury w prawym górnym rogu. W rozwijanym menu kliknij ikonę koła zębatego i wybierz **Disable**.



Usługa chmurowa zostanie wyłączona.

7.2 AstroWarp

AstroWarp to zaawansowana platforma sieciowa zaprojektowana z myślą o sprawnym tworzeniu połączeń zdalnych i zdalnym zarządzaniu urządzeniami.

AstroWarp, stworzony specjalnie do integracji z routerami GL.iNet, umożliwia kompleksowe zarządzanie urządzeniami w całych sieciach, w tym sterowanie urządzeniami nadrzędnymi i podrzędnymi.

Dzięki zarządzaniu całą siecią i planowanej obsłudze sterowania na poziomie sprzętu AstroWarp oferuje solidne i niezawodne rozwiązanie do zarządzania urządzeniami oraz utrzymywania bezpiecznych, stabilnych sieci.

Więcej informacji znajdziesz na astrowarp.net.

Rozdział 8

Poznaj VPN

W tym rozdziale przedstawiono pojęcia związane z VPN i typowe zastosowania.

8.1 Wprowadzenie

VPN

VPN, czyli wirtualna sieć prywatna (Virtual Private Network), tworzy zaszyfrowany, prywatny tunel między urządzeniem a zdalnym serwerem, chroniąc transmisję danych i umożliwiając bezpieczny dostęp do sieci prywatnych lub o ograniczonym dostępie.

Router VPN

Router VPN ma fabrycznie zainstalowane funkcje VPN, które chronią wszystkie podłączone urządzenia. Skonfigurowanie routera jako klienta VPN kieruje cały ruch przez zaszyfrowany tunel i nie wymaga oddzielnej konfiguracji na każdym urządzeniu. Chroni to jednocześnie wiele urządzeń, oszczędza czas i zapewnia spójne ustawienia VPN, ograniczając ryzyko wynikające z nieprawidłowej konfiguracji poszczególnych urządzeń.

Routery GL.iNet obsługują ponad 30 popularnych komercyjnych usług VPN OpenVPN i WireGuard. Prześlij pliki konfiguracyjne VPN, aby uruchomić połączenie VPN i bezpiecznie korzystać z sieci. Pełną listę zewnętrznych dostawców VPN znajdziesz tutaj.

OpenVPN

OpenVPN to protokół VPN o otwartym kodzie źródłowym, wykorzystujący zabezpieczenia SSL/TLS w połączeniach urządzenie–sieć lub sieć–sieć. Obsługuje różne metody szyfrowania, TCP/UDP i ułatwia pokonywanie ograniczeń zapór oraz NAT.

WireGuard

WireGuard to lekki, szybki protokół VPN, prostszy i wydajniejszy od OpenVPN. Wykorzystuje nowoczesną kryptografię zapewniającą wydajność, niewielką bazę kodu ułatwiającą audyty i zwiększającą bezpieczeństwo oraz zaawansowane algorytmy ChaCha20/Poly1305 do szyfrowania i zapewniania integralności danych.

8.2 Przykłady zastosowań

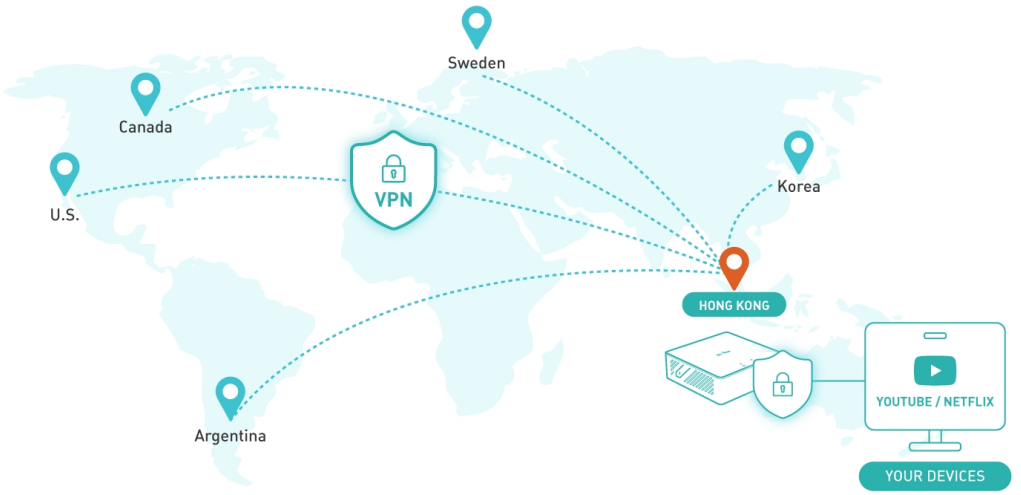
1. **Prywatność danych osobowych**

   Usługa VPN tego routera obsługuje szeroką gamę urządzeń przewodowych i bezprzewodowych, w tym laptopy, tablety, smartfony, konsole do gier i telewizory Smart TV. VPN chroni wszystkie dane przesyłane zarówno przez połączenia przewodowe, jak i Wi-Fi. Możesz też dostosować zasady VPN, aby elastycznie chronić wybrane urządzenia.



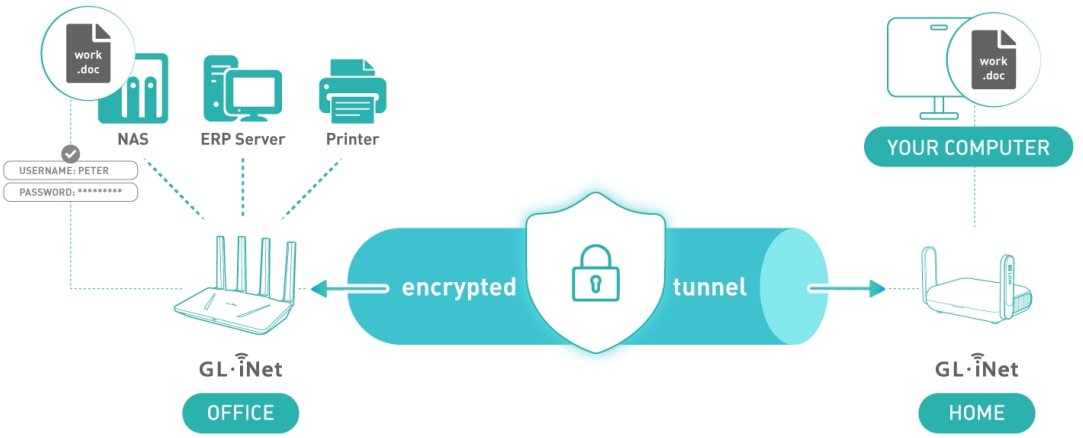
2. **Dostęp bez ograniczeń na całym świecie**

   Dostęp do niektórych witryn może zależeć od lokalizacji. Po włączeniu VPN możesz w razie potrzeby odblokować witryny. Łącząc się z różnymi serwerami zewnętrznymi, otrzymujesz różne adresy IP do przeglądania stron lub uzyskiwania dostępu do witryn objętych blokadą regionalną.


Sweden
Canada
U.S.
VPN
Korea
HONG KONG
Argentina
YOUTUBE / NETFLIX
YOUR DEVICES

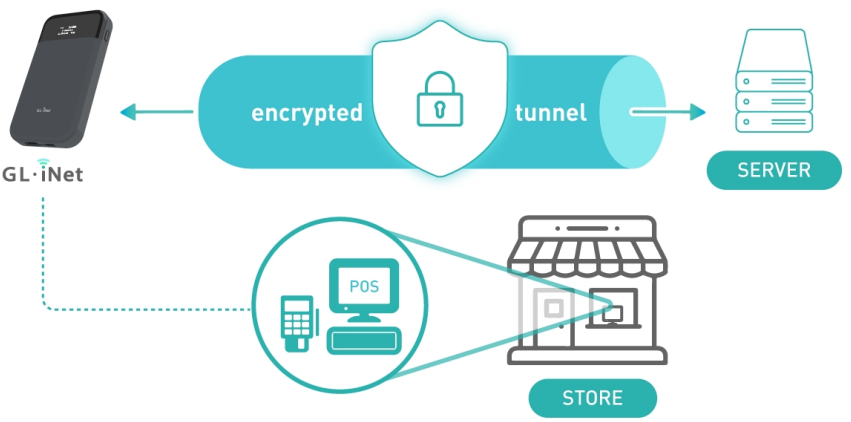
3. **Bezpieczeństwo danych małych firm**

Wiele osób pracuje w przestrzeniach coworkingowych lub kawiarniach i korzysta z bezpłatnych publicznych sieci Wi-Fi. Takie sieci są podatne na ataki cyberprzestępców. Skonfigurowanie routera podróżnego jako klienta VPN zapewnia bezpieczne połączenie podczas pracy w dowolnym miejscu.



4. **Bezpieczna infrastruktura płatnicza**

Właściciele małych sklepów przetwarzają dane płatnicze klientów podczas sprzedaży na miejscu. Dzięki routerowi VPN terminale POS mogą przesyłać dane kart kredytowych przez zaszyfrowany tunel VPN, zapewniając bezpieczeństwo płatności.



Rozdział 9

Panel VPN

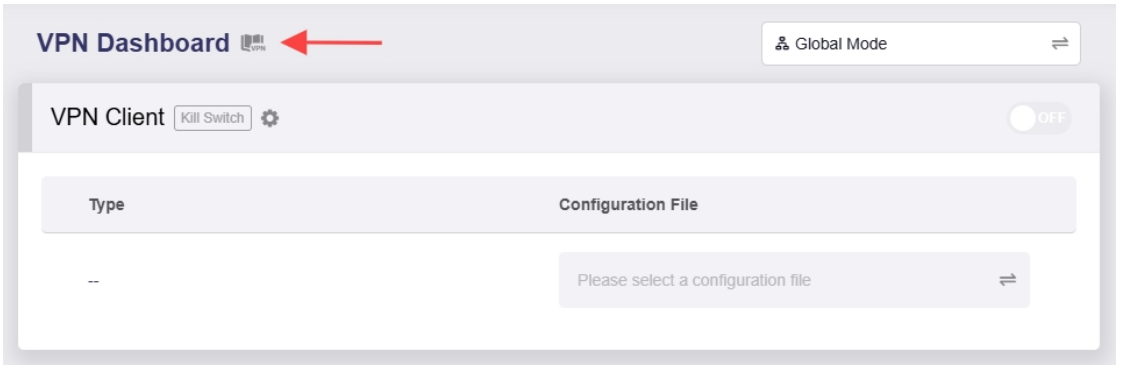
W tym rozdziale opisano zarządzanie połączeniami VPN w panelu administracyjnym.

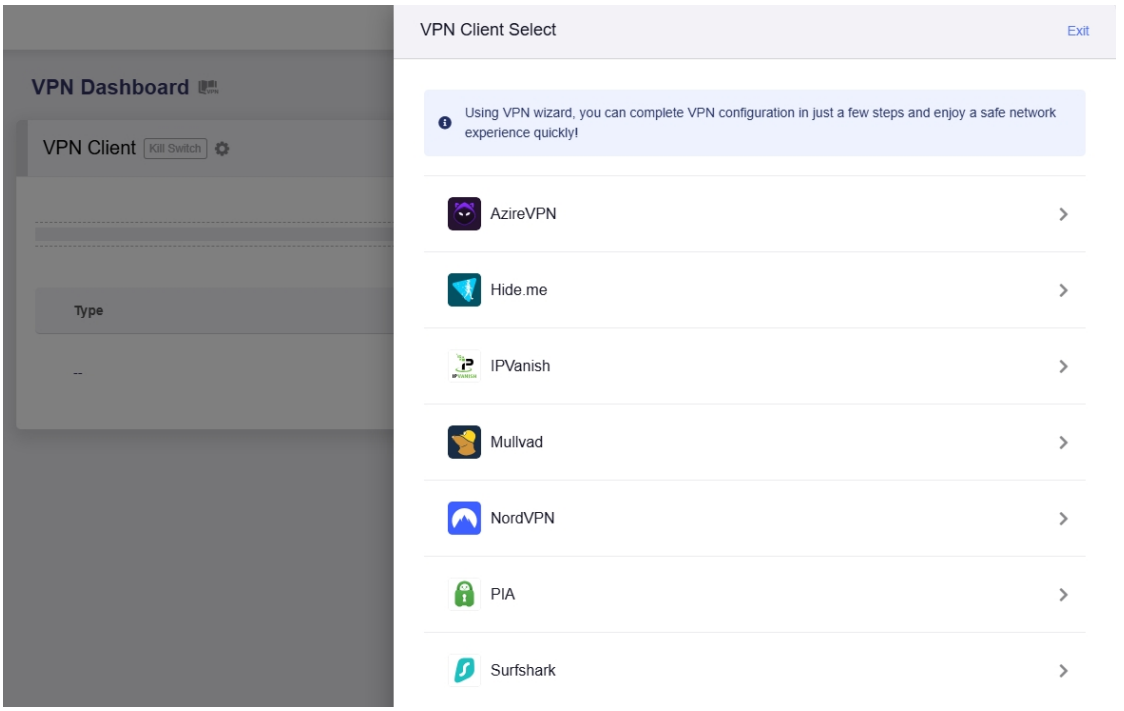
Zaloguj się do panelu administracyjnego routera i przejdź do **VPN** > **VPN Dashboard**.

Panel VPN wyświetla szczegóły połączenia VPN, takie jak reguły tunelu, adres serwera, statystyki transferu, wirtualny adres IP klienta i dziennik połączenia, oraz umożliwia konfigurację ustawień zaawansowanych, takich jak VPN Kill Switch, IP Masquerading i MTU. Możesz też włączyć wiele połączeń VPN w konfiguracjach z wieloma tunelami.

9.1 Kreator konfiguracji VPN

Aby rozpocząć, kliknij ikonę książki w lewym górnym rogu i skorzystaj z kreatora konfiguracji VPN, aby szybko skonfigurować VPN.



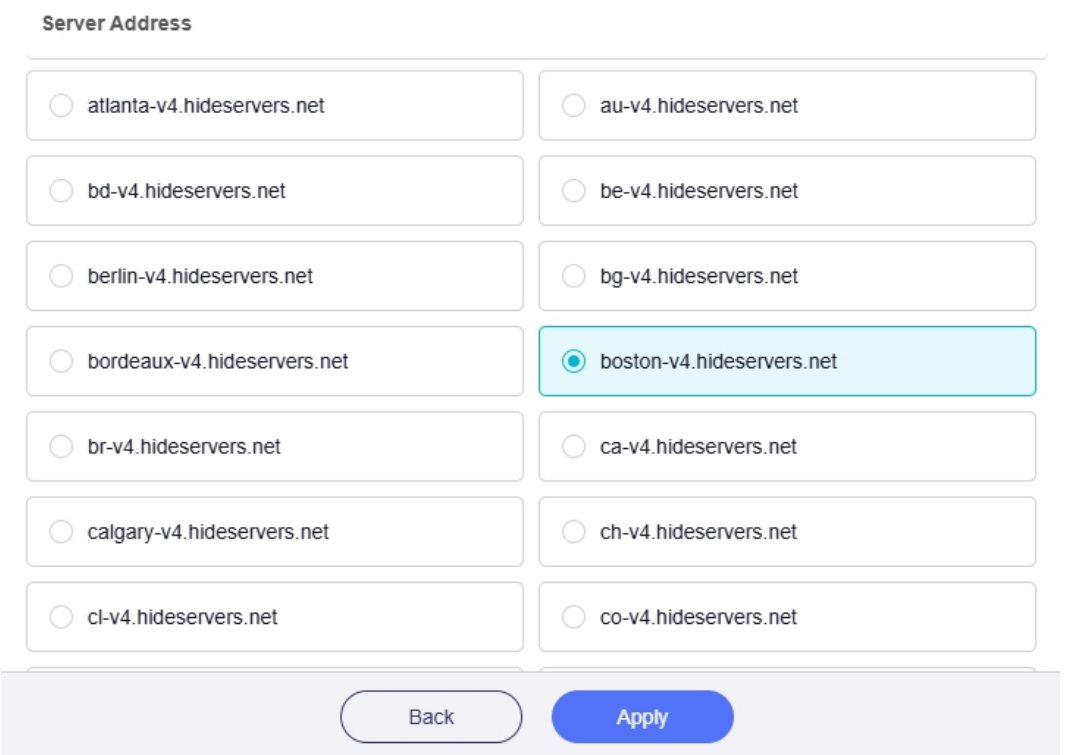


Uwaga: kreator konfiguracji VPN jest przeznaczony wyłącznie do zintegrowanych usług VPN, takich jak AzireVPN, Hide.me, IPVanish, Mullvad, NordVPN, PIA i Surfshark. W przypadku innych dostawców pomiń kreator i przejdź do **VPN** > **OpenVPN Client** lub **WireGuard Client**, aby ręcznie skonfigurować VPN.

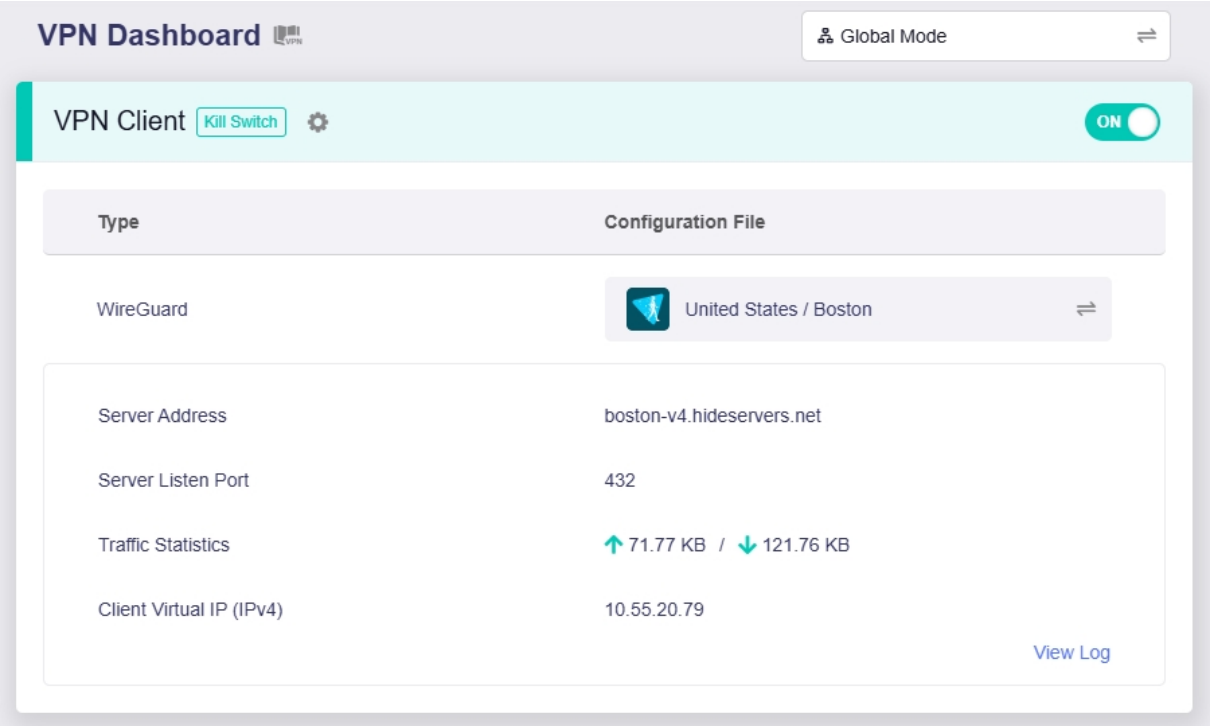
Poniżej przedstawiono przykład dla **Hide.me**. Zaloguj się, podając dane logowania Hide.me.



Wybierz serwer VPN i kliknij **Apply**. Z tym serwerem zostanie nawiązane połączenie, a Twój publiczny adres IP będzie wskazywać lokalizację wybranego serwera.

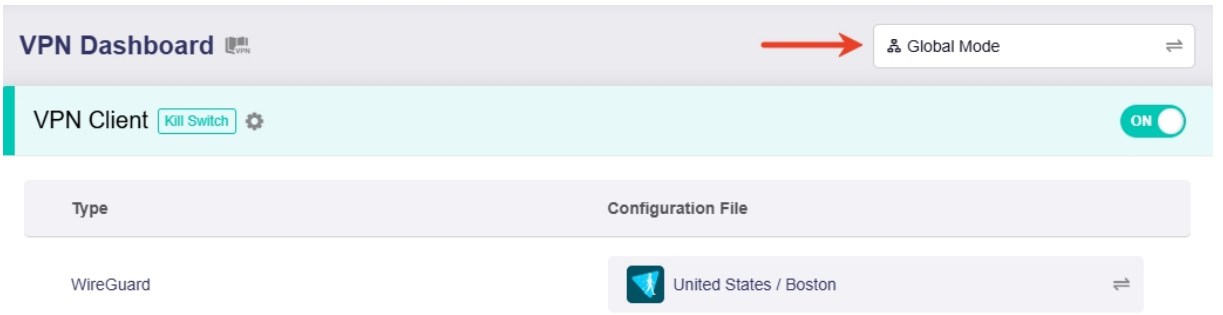


Połączenie zostanie nawiązane automatycznie. Po połączeniu przejdź do **VPN Dashboard**. Zobaczysz włączony tunel VPN wraz ze szczegółami: protokołem VPN (np. WireGuard), plikiem konfiguracyjnym, adresem serwera, portem nasłuchiwania serwera, statystykami transferu i wirtualnym adresem IP klienta. W prawym dolnym rogu możesz też przeglądać dzienniki połączenia.

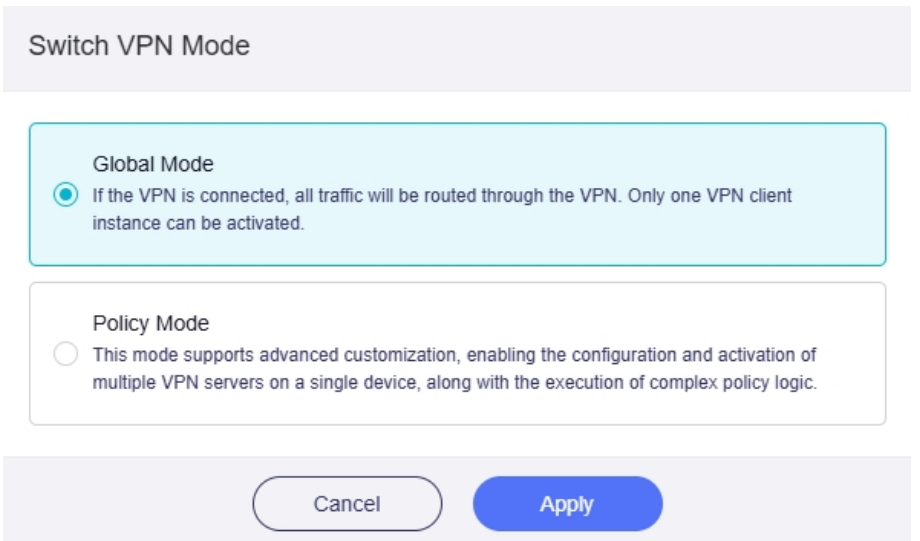

VPN Dashboard
Global Mode
VPN Client
Kill Switch
ON
Type
Configuration File
WireGuard
United States / Boston
Server Address
boston-v4.hideservers.net
Server Listen Port
432
Traffic Statistics
71.77 KB / 121.76 KB
Client Virtual IP (IPv4)
10.55.20.79
View Log

9.2 Tryb VPN

W razie potrzeby kliknij przycisk w prawym górnym rogu panelu VPN, aby przełączyć tryb VPN.



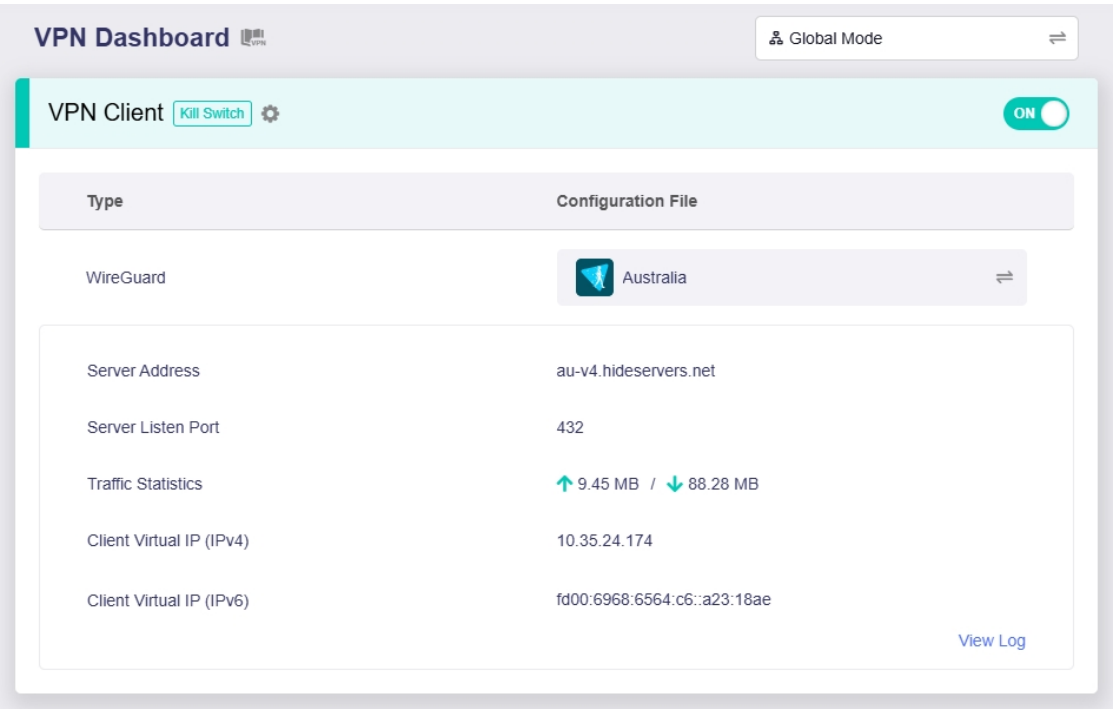
Dostępne są dwa tryby: **Global Mode** i **Policy Mode**.



9.2.1 Tryb globalny

W tym trybie cały ruch jest kierowany przez tunel VPN i można włączyć tylko jedną instancję klienta VPN. Sprawdza się on, gdy ruch wszystkich urządzeń ma przechodzić przez jeden serwer VPN, np. w celu zapewnienia jednolitej ochrony sieci lub dostępu do treści przeznaczonych dla określonego regionu.

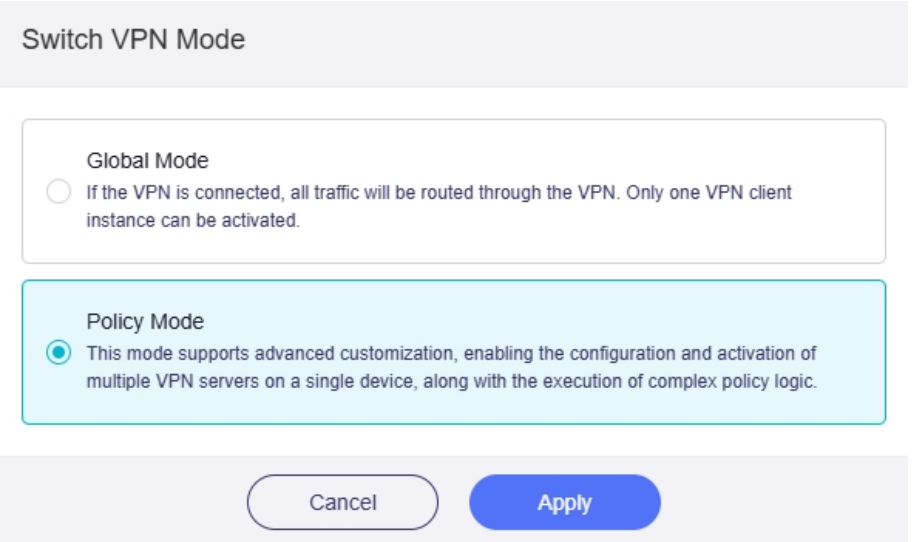
W poniższym przykładzie router łączy się z serwerem w Australii za pomocą protokołu WireGuard. Cały ruch podłączonych klientów będzie kierowany przez ten tunel VPN.



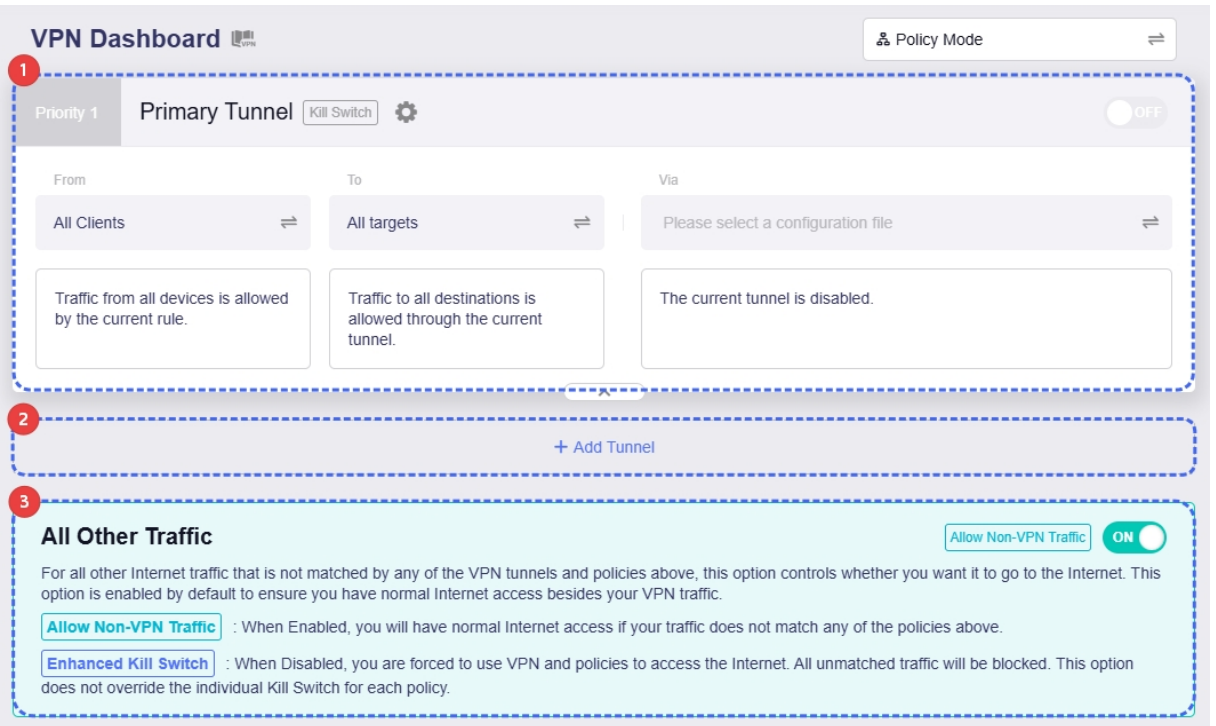
9.2.2 Tryb reguł

W tym trybie możesz połączyć jeden router z wieloma serwerami VPN i dostosować reguły VPN. Sprawdza się on, gdy potrzebne jest elastyczne zarządzanie ruchem, np. kierowanie różnych rodzajów ruchu do różnych miejsc docelowych przez wiele serwerów VPN.

Zmień tryb VPN na **Policy Mode** i kliknij **Apply**.



Po zmianie trybu, jeśli VPN nie jest włączony, strona wygląda jak poniżej i zawiera trzy sekcje: **Primary Tunnel**, **Add Tunnel** i **All Other Traffic**.

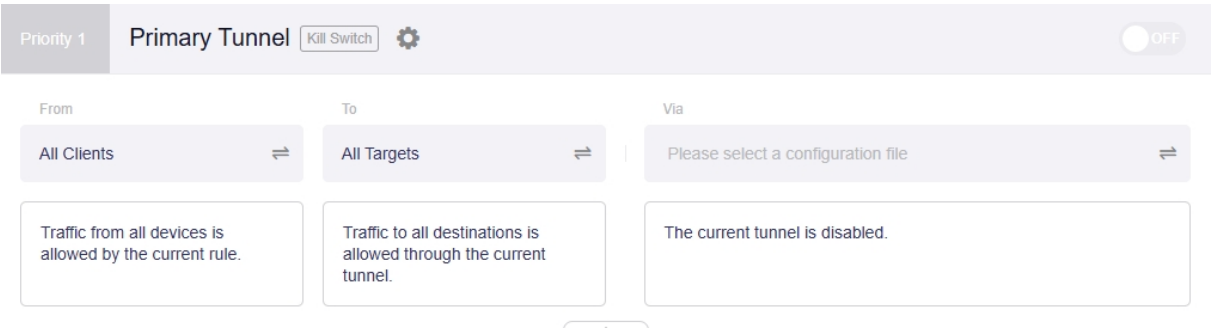


Tunel główny

Tunel główny jest wstępnie zdefiniowanym tunelem w trybie reguł. Domyślnie ma najwyższy priorytet; po skonfigurowaniu wielu tuneli można zmienić jego priorytet.

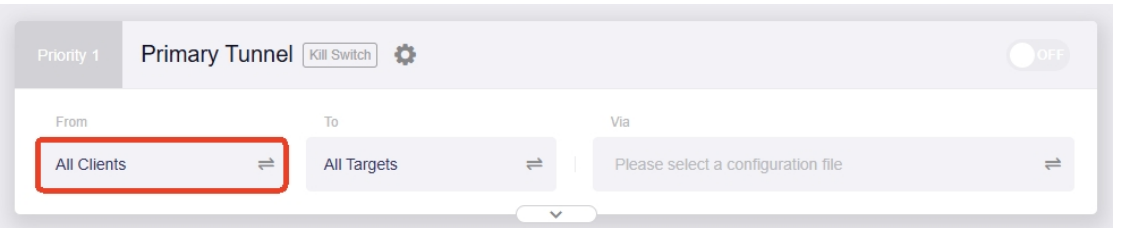
W tym tunelu możesz dostosować regułę tunelu, ustawiając trzy parametry:

- **From**: źródło ruchu, czyli ruch, który ma być kierowany przez ten tunel.
- **To**: miejsce docelowe, do którego ruch jest kierowany przez ten tunel.
- **Via**: sposób kierowania ruchu, czyli określenie, czy ma być używany VPN.

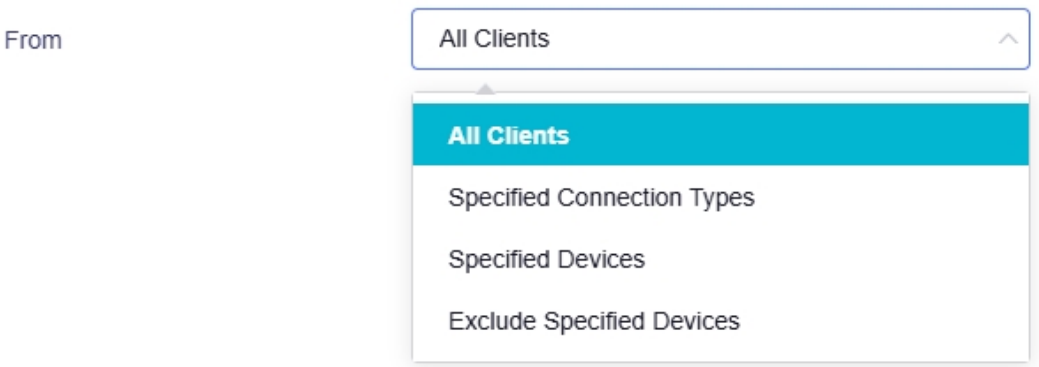


Aby skonfigurować regułę tunelu, wykonaj poniższe czynności.

1. Kliknij szare pole po lewej stronie.



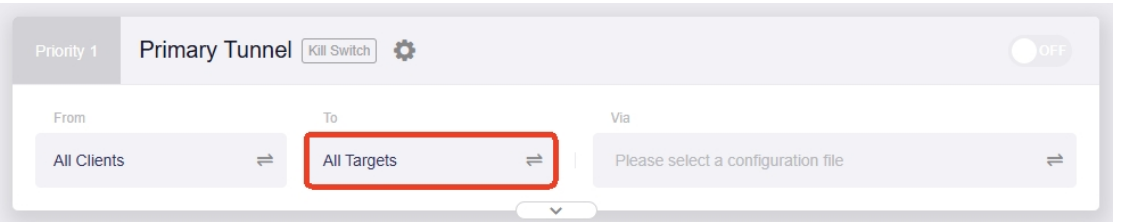
2. Wybierz urządzenie, które ma odpowiadać tej regule, i kliknij **Apply**.



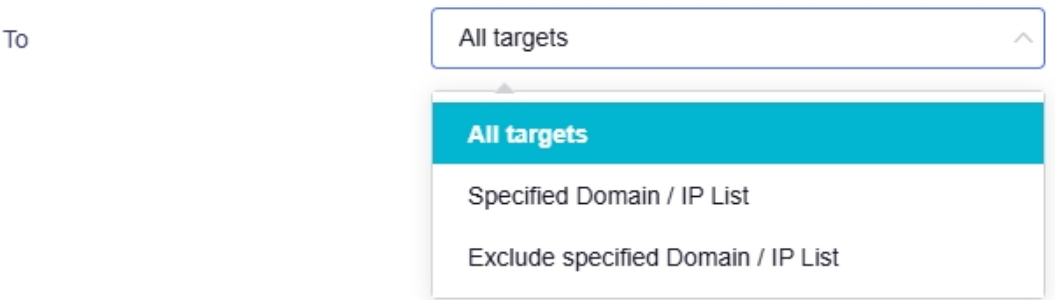
- **All Clients**: ruch ze wszystkich urządzeń będzie odpowiadać tej regule.

- **Specified Connection Types**: ruch z określonych typów połączeń (np. podsieci LAN, Drop-in Gateway, sieci gościnnej) będzie odpowiadać tej regule.
- **Specified Devices**: ruch z określonych urządzeń (identyfikowanych według adresu MAC) będzie odpowiadać tej regule.
- **Exclude Specified Devices**: ruch z określonych urządzeń (identyfikowanych według adresu MAC) **NIE** będzie odpowiadać tej regule.

3. Kliknij szare pole pośrodku.



4. Wybierz miejsce docelowe, do którego ruch ma być kierowany przez ten tunel, i kliknij **Apply**.

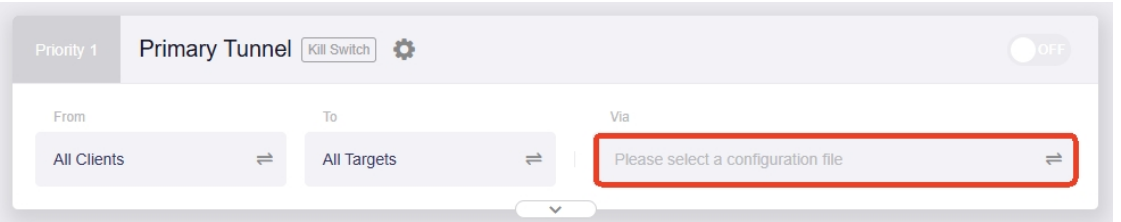


- **All Targets**: ruch odpowiadający tej regule będzie kierowany do wszystkich miejsc docelowych.
- **Specified Domain / IP List**: ruch odpowiadający tej regule będzie kierowany do określonych domen lub adresów IP. Wprowadź je ręcznie lub podaj adres URL subskrypcji. Wskazanie domeny głównej obejmuje wszystkie jej subdomeny.
- **Exclude specified Domain / IP List**: ruch odpowiadający tej regule **NIE** będzie kierowany do określonych domen lub adresów IP. Wprowadź je ręcznie lub podaj adres URL subskrypcji. Wskazanie domeny głównej obejmuje wszystkie jej subdomeny.

Uwaga: po wybraniu Subscribe URL nazwy domen lub adresy IP dostępne pod tym adresem URL będą automatycznie aktualizowane codziennie. Wprowadź poprawny

adres URL. Sprawdzanie adresu URL zweryfikuje poprawność nazwy domeny lub adresu IP.

5. Kliknij szare pole po prawej stronie.

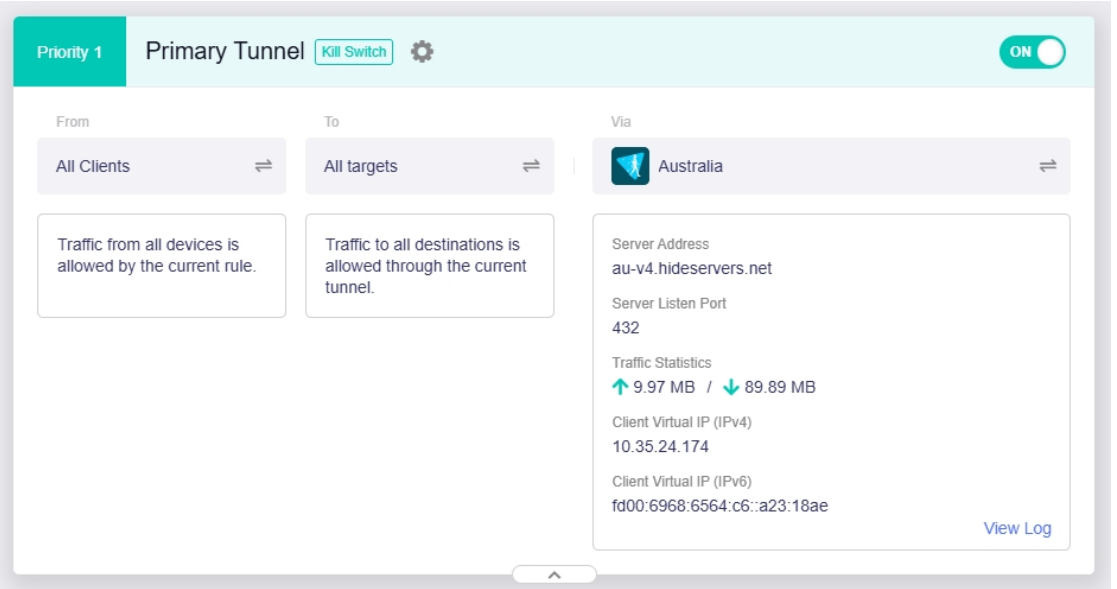


6. Wybierz sposób kierowania ruchu dla tego tunelu: **Use VPN** lub **Not Use VPN**.



- **Use VPN**: ruch odpowiadający tej regule będzie kierowany do wybranych miejsc docelowych przez tunel VPN. Dla tej reguły należy wybrać plik konfiguracyjny VPN.
- **Not Use VPN**: ruch odpowiadający tej regule będzie kierowany do wybranych miejsc docelowych przez lokalną sieć WAN zamiast przez VPN.

7. Po skonfigurowaniu źródła ruchu, miejsca docelowego i sposobu kierowania ruchu konfiguracja reguły tunelu głównego jest zakończona. W poniższym przykładzie reguła tunelu jest następująca: wszyscy klienci podłączeni do tego routera będą korzystać z Internetu przez VPN; ich ruch zostanie skierowany tym tunelem VPN do serwera w Australii, a następnie przez ten serwer do Internetu.

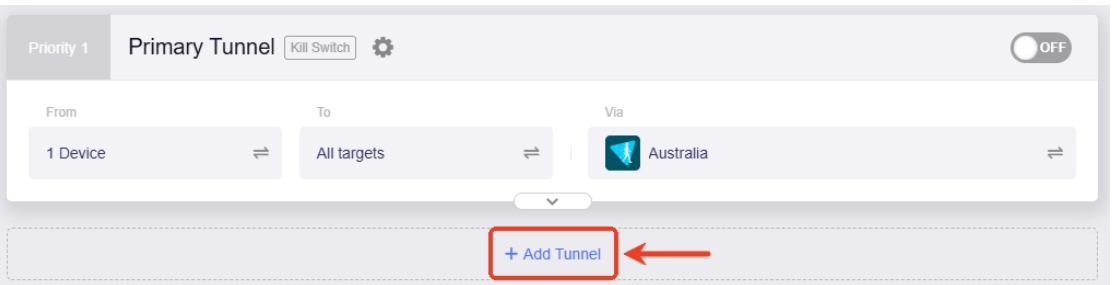


Uwaga: ze względów bezpieczeństwa przed włączeniem tego tunelu przejdź do All Other Traffic i Tunnel Options, aby sprawdzić pozostałe ustawienia.

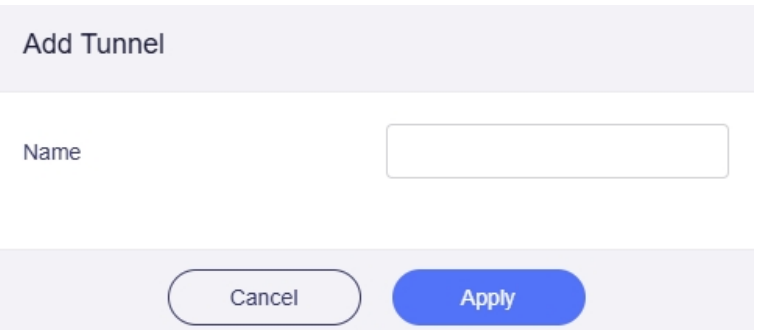
Dodawanie tunelu

Dodaj tunele, jeśli chcesz kierować ruch z różnych urządzeń do różnych miejsc docelowych. Aby dodać tunel, wykonaj poniższe czynności.

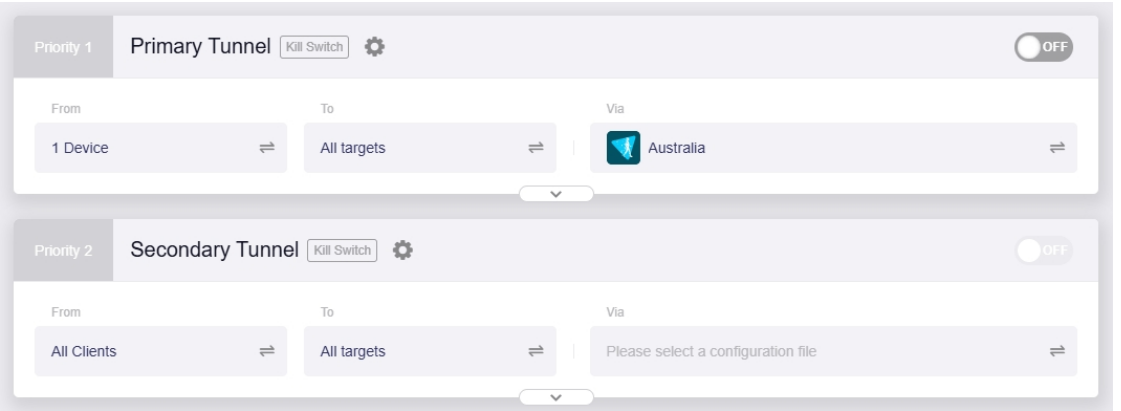
1. Kliknij **Add Tunnel** pod tunelem głównym.



2. Nadaj tunelowi nazwę.



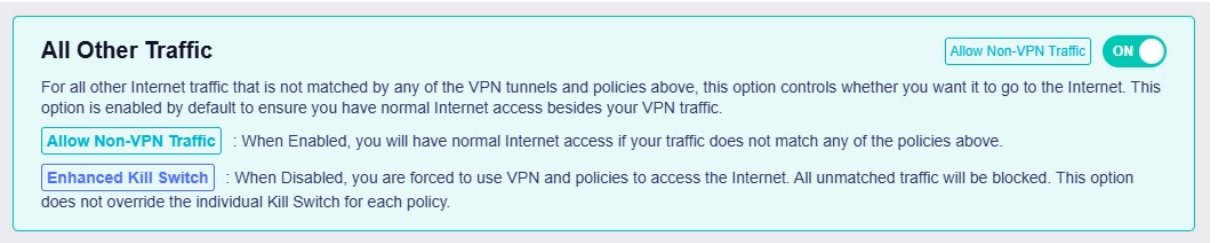
3. Na stronie VPN Dashboard pojawi się kolejny tunel. Można utworzyć maksymalnie 5 tuneli, łącznie ze wstępnie zdefiniowanym tunelem głównym.



4. Skonfiguruj reguły tunelu, ustawiając źródło ruchu, miejsca docelowe i sposób kierowania ruchu. Po zakończeniu ze względów bezpieczeństwa sprawdź pozostałe ustawienia w All Other Traffic i Tunnel Options przed włączeniem tuneli.

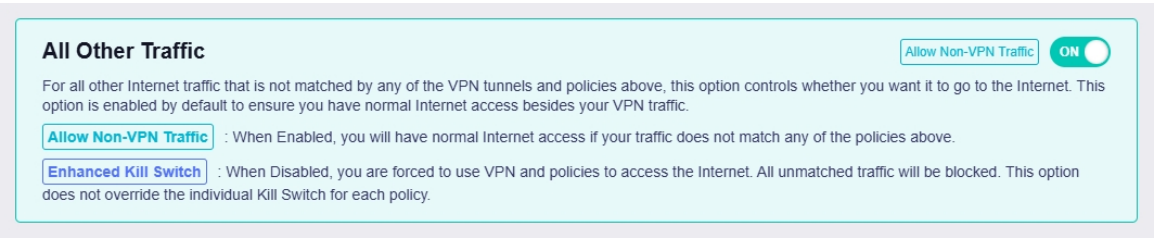
Cały pozostały ruch

W trybie reguł na dole strony VPN Dashboard widoczny jest domyślny tunel, który jest już włączony.

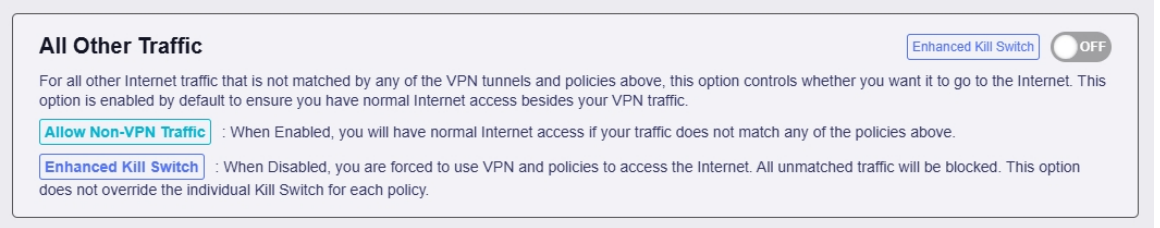


Ten tunel określa, czy ruch niepasujący do żadnej z powyższych grup tuneli VPN może uzyskiwać dostęp do Internetu. Jest domyślnie włączony, aby zapewnić normalny dostęp do Internetu dla ruchu niekierowanego przez VPN.

- Po włączeniu ruch niepasujący do reguł nadal może uzyskiwać dostęp do Internetu.



- Po wyłączeniu tylko ruch kierowany przez VPN może uzyskiwać dostęp do Internetu. Cały ruch poza VPN oraz ruch przełączany awaryjnie z połączeń VPN zostaje zablokowany. Ta opcja nie zastępuje indywidualnego ustawienia Kill Switch dla każdego tunelu VPN.

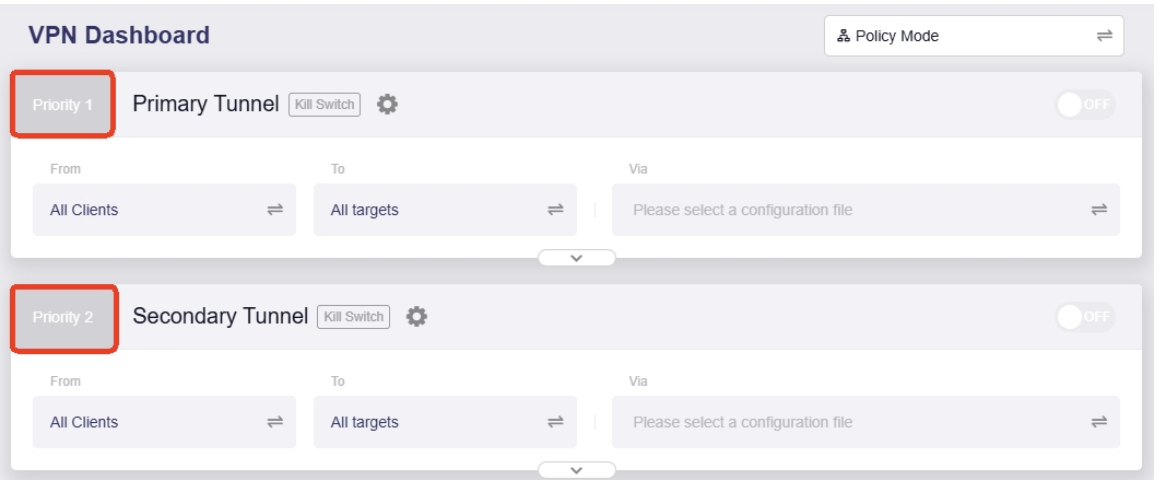


Priorytet tunelu

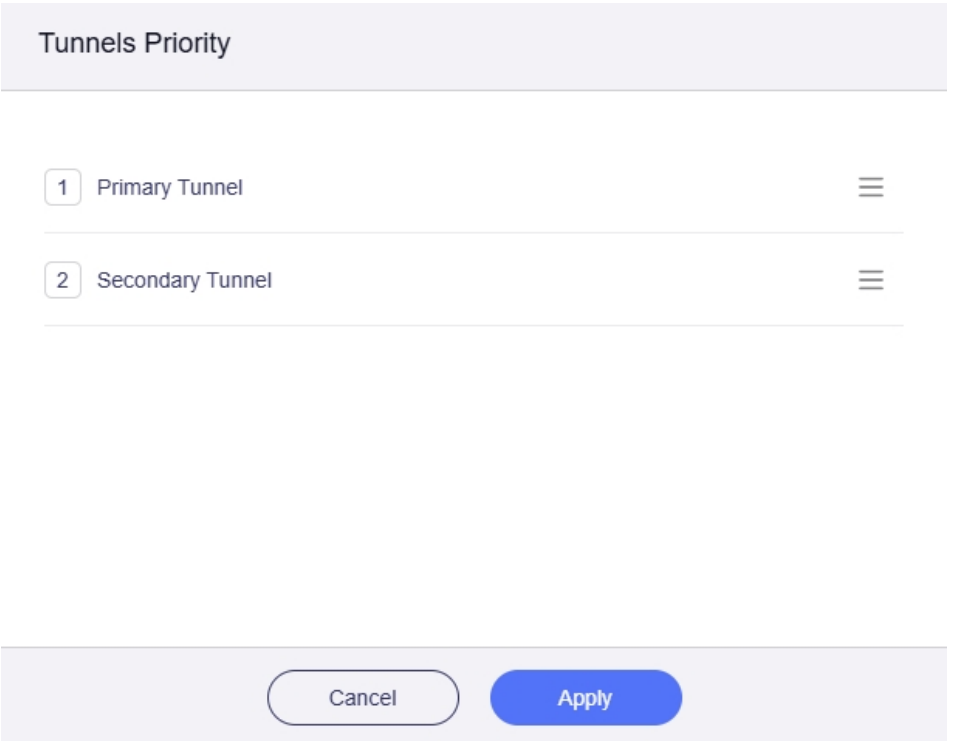
Domyślnie wstępnie zdefiniowany tunel Primary Tunnel ma najwyższy priorytet, po nim następują ręcznie dodane tunele (jeśli istnieją), a następnie tunel All Other Traffic, który zapewnia łączność przez lokalną sieć dostawcy Internetu (WAN).

Aby zmienić priorytet tuneli, wykonaj poniższe czynności.

1. Kliknij etykietę priorytetu w lewym górnym rogu dowolnego tunelu (np. Priority 1 / Priority 2).



2. W wyskakującym oknie kliknij i przytrzymaj ikonę trzech linii po prawej stronie, zmień kolejność tuneli, a następnie kliknij **Apply**.

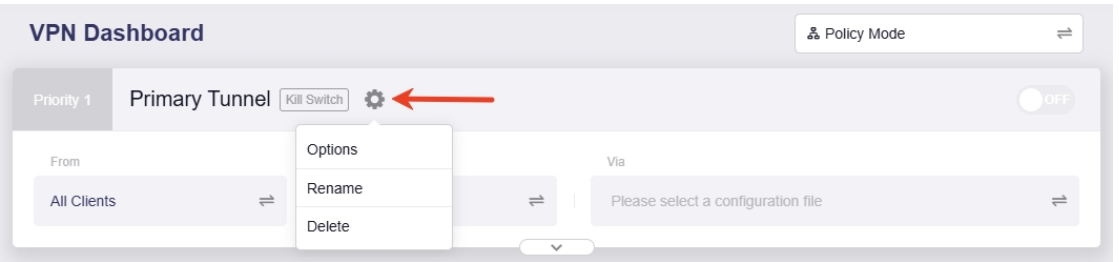


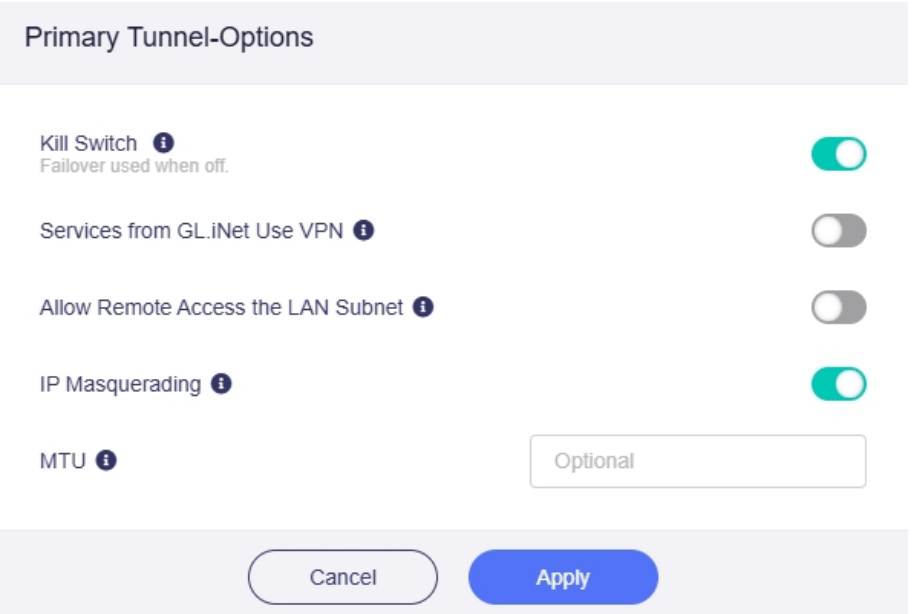
Gdy włączonych jest wiele tuneli, router kieruje ruch w następującej kolejności:

1. Najpierw sprawdza dopasowanie ruchu do reguły tunelu o najwyższym priorytecie. Jeśli ruch pasuje, kieruje go przez ten tunel; w przeciwnym razie sprawdza kolejny tunel, aż do dopasowania tunelu „All Other Traffic”.
2. Jeśli tunel VPN niespodziewanie się rozłączy, system zdecyduje o przełączeniu ruchu do tunelu o kolejnym priorytecie na podstawie tego, czy w tym tunelu włączono **Kill Switch**.
   - Gdy Kill Switch jest włączony, ruch zostaje zablokowany i nie jest przełączany do tunelu o kolejnym priorytecie.
   - Gdy Kill Switch jest wyłączony, ruch jest przełączany do tunelu o kolejnym priorytecie i sprawdzany pod kątem dopasowania do jego reguł.
3. Tunel **All Other Traffic** jest domyślnie włączony, aby ruch niepasujący do tuneli VPN nadal mógł uzyskiwać dostęp do Internetu.
   - Po włączeniu kieruje niedopasowany lub przełączony awaryjnie ruch przez lokalną sieć WAN.
   - Po wyłączeniu wzmacnia działanie Kill Switch i blokuje zwykły dostęp do Internetu, aby zapobiec ujawnieniu adresu IP.

Opcje tunelu

Dla każdego tunelu VPN możesz skonfigurować ustawienia zaawansowane, takie jak VPN Kill Switch, IP Masquerading i MTU. Kliknij ikonę koła zębatego obok nazwy tunelu.





- **Kill Switch**: po włączeniu ruch pasujący do tego tunelu VPN zostanie zablokowany, jeśli połączenie niespodziewanie się zerwie; w przeciwnym razie zostanie przełączony do tuneli o kolejnym priorytecie lub sieci WAN.
- **Services from GL.iNet Use VPN**: po włączeniu usługi GoodCloud, DDNS i rtty przesyłają pakiety przez tunele VPN. Ta opcja jest domyślnie wyłączona, ponieważ usługi te zwykle wymagają rzeczywistego adresu IP urządzenia do poprawnego działania.
- **Allow Remote Access the LAN Subnet**: po włączeniu dozwolony jest zdalny dostęp przez VPN do tego routera (adresu IP tunelu) i urządzeń LAN. Serwer VPN musi rozgłaszać trasę powrotną do podsieci LAN tego routera.
- **IP Masquerading**: po włączeniu źródłowe adresy IP klientów LAN są zastępowane adresem IP tunelu VPN routera. Wyłączaj tylko w konfiguracjach sieć–sieć, gdy zdalny węzeł zna Twoje podsieci LAN.
- **MTU**: wartość ustawiona dla tunelu zastępuje wartość MTU w pliku konfiguracyjnym.

Rozdział 10

Konfiguracja serwera VPN

W tym rozdziale opisano konfigurację routera GL.iNet jako serwera OpenVPN lub WireGuard.

10.1 Konfiguracja serwera OpenVPN

OpenVPN to protokół VPN o otwartym kodzie źródłowym, wykorzystujący szyfrowanie SSL/TLS do bezpiecznych połączeń punkt–punkt i sieć–sieć. Aby skonfigurować serwer OpenVPN na routerze GL.iNet, obejrzyj ten film lub wykonaj poniższe czynności.

10.1.1 Przygotowanie

1. **Upewnij się, że masz publiczny adres IP**

   Kliknij tutaj, aby sprawdzić, czy dostawca usług internetowych (ISP) przydziela Ci publiczny adres IP.

   Jeśli nie, nie można skonfigurować routera jako serwera OpenVPN.

   Rozwiązania alternatywne:

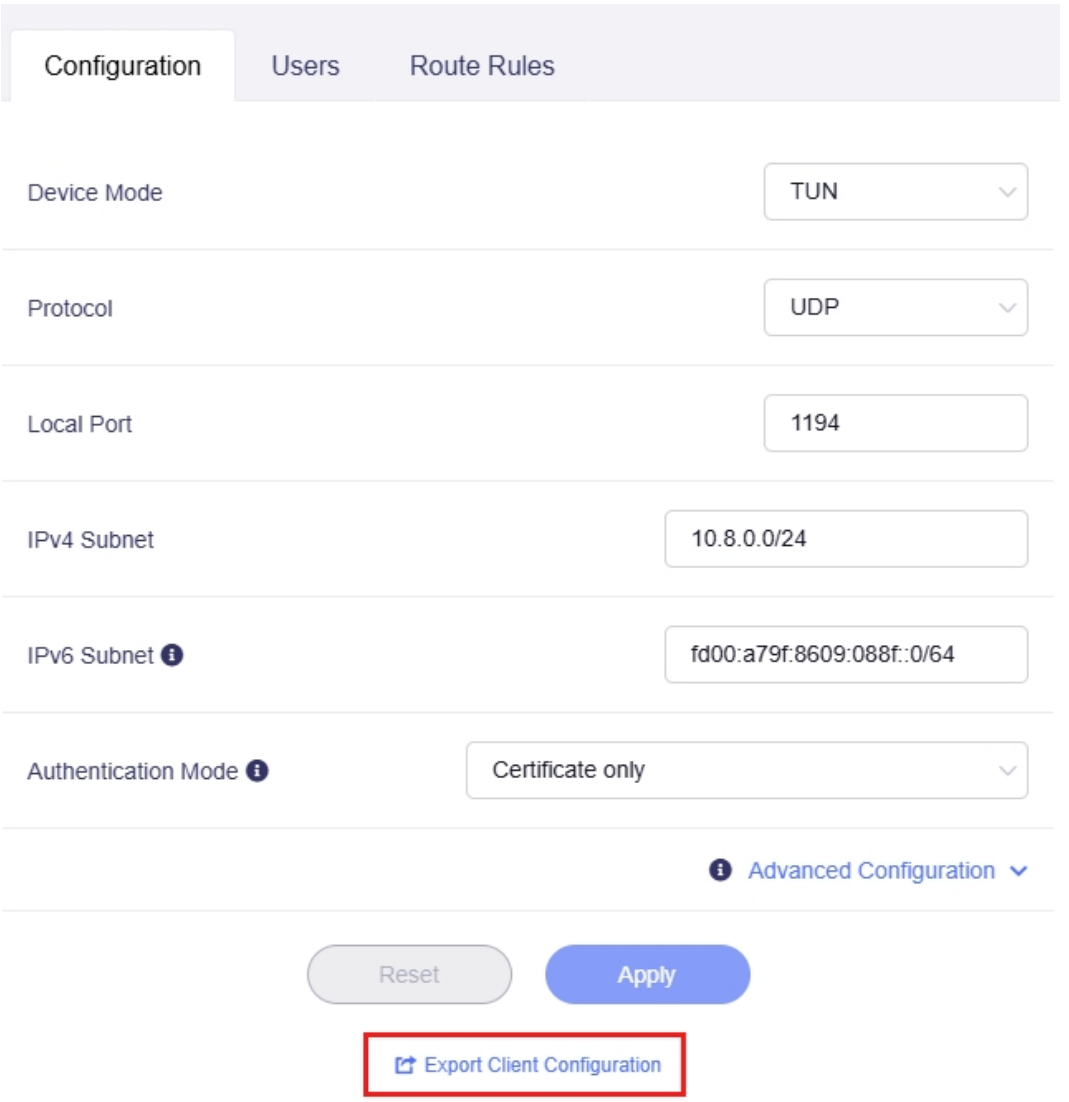
   - Jeśli przed routerem GL.iNet znajduje się główny router, zaloguj się do niego i sprawdź, czy ma publiczny adres IP przydzielony przez dostawcę Internetu.
   - Poproś dostawcę Internetu o publiczny adres IP. Może to wiązać się z dodatkową opłatą.
   - Jeśli dwie powyższe metody nie działają (np. gdy sieć znajduje się za CGNAT), możesz wypróbować nasze rozwiązanie SD-WAN AstroWarp.

2. **Sprawdź, czy wymagane jest przekierowanie portów**

   - Jeśli router GL.iNet jest głównym routerem w sieci, konfiguracja przekierowania portów nie jest wymagana. Przejdź do następnego kroku.
   - Jeśli korzystasz już z głównego routera, a router GL.iNet działa jako router dodatkowy, trzeba skonfigurować przekierowanie portów na głównym routerze.
   - Jeśli router GL.iNet znajduje się kilka poziomów za głównym routerem, skonfiguruj przekierowanie portów na każdym urządzeniu pośrednim.

10.1.2 Etapy konfiguracji

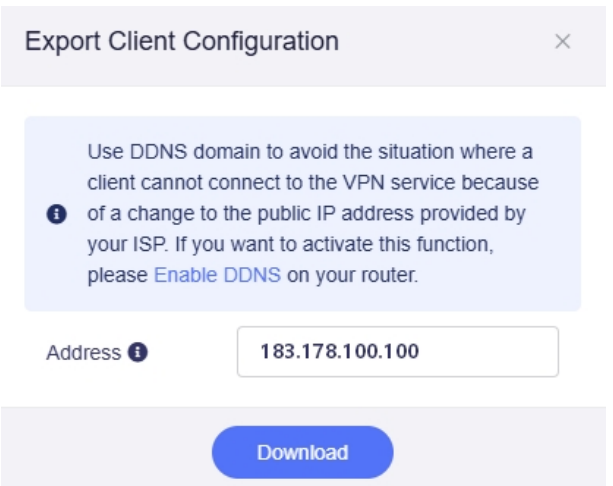
1. Zaloguj się do panelu administracyjnego routera, przejdź do **VPN** > **OpenVPN Server**, a następnie kliknij **Generate Configuration** (tylko przy pierwszej konfiguracji serwera VPN).
2. Zastosuj konfigurację.
   Domyślna konfiguracja sprawdza się w większości przypadków. Kliknij **Export Client Configuration** u dołu i przejdź do kroku 3. Jeśli konfiguracja została zmieniona, przed eksportem kliknij **Apply**.



- **Device Mode**: TAP-S2S lub Tun. Różnice opisano tutaj.
- **Protocol**: UDP lub TCP. Różnice opisano tutaj.

- **Authentication Mode**: określa metodę uwierzytelniania klienta podczas łączenia z serwerem. Dostępne są trzy opcje:
  - **Certificate Only**: router automatycznie generuje certyfikaty i klucze serwera oraz klienta, a następnie umieszcza je w pliku konfiguracyjnym. Po przesłaniu konfiguracji do klienta nie są wymagane dodatkowe dane logowania.
  - **Username/Password Only**: router generuje konfigurację klienta bez kluczy certyfikatów. Przed eksportem konfiguracji klienta trzeba dodać nazwę użytkownika i hasło na karcie **Users**. Podczas przesyłania konfiguracji do klienta wprowadź te dane w celu uwierzytelnienia.
  - **Username/Password and Certificate**: przed eksportem konfiguracji klienta trzeba najpierw dodać nazwę użytkownika i hasło na karcie **Users**. Następnie router automatycznie generuje certyfikaty i klucze serwera oraz klienta i umieszcza je w pliku konfiguracyjnym. Podczas przesyłania konfiguracji do klienta najpierw sprawdzany jest certyfikat i klucz, a potem nazwa użytkownika i hasło, co zapewnia uwierzytelnianie dwuskładnikowe.
- **Advanced Configuration**: w razie potrzeby dostosuj dodatkowe ustawienia serwera.

3. Wyeksportuj konfigurację klienta.
   Po kliknięciu **Export Client Configuration** u dołu karty Configuration (lub zastosowaniu zmienionej konfiguracji) pojawi się poniższe okno. Kliknij **Download**, aby wyeksportować konfigurację.



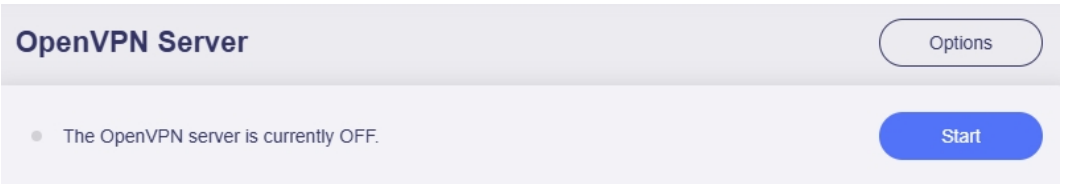
Wskazówki:

- Jeśli Twój publiczny adres IP często się zmienia, przejdź do **APPLICATIONS** > **Dynamic DNS** i włącz DDNS. Możesz wtedy używać domeny DDNS jako adresu serwera.

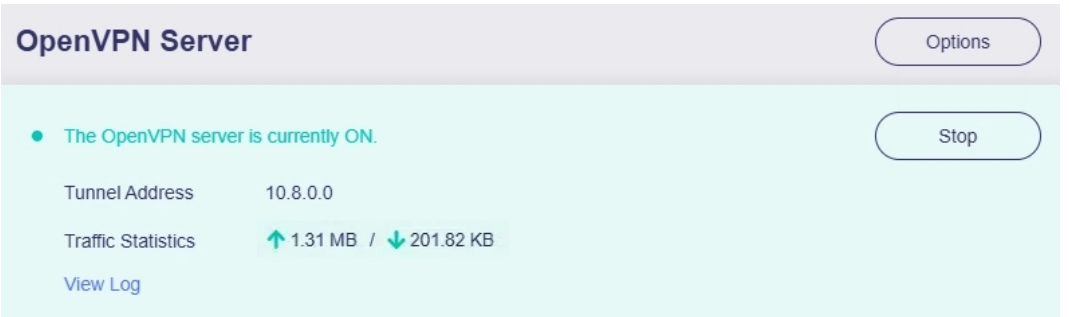
- Od wersji oprogramowania 4.8 przed wyeksportowaniem pliku konfiguracyjnego można wybrać adres serwera z listy: publiczny adres IP, domenę DDNS lub bieżący adres IP WAN. Po wybraniu adres serwera w pliku konfiguracyjnym zostanie automatycznie zaktualizowany. Pobierz plik konfiguracyjny ponownie, jeśli adres serwera ulegnie zmianie.

4. Uruchom serwer OpenVPN.

   Na stronie **OpenVPN Server** kliknij przycisk **Start** w prawym górnym rogu, aby uruchomić serwer.



   Stan połączenia serwera jest wyświetlany u góry. Jeśli widoczne są statystyki wysyłania i pobierania, serwer OpenVPN działa.



10.1.3 Rozwiązywanie problemów

Jeśli połączenie się nie powiedzie, przyczyną może być jeden z typowych problemów:

- Serwer VPN nie ma publicznego adresu IP. Pomoc znajdziesz tutaj.
- Może być wymagane przekierowanie portów. Pomoc znajdziesz tutaj.
- Port używany przez serwer OpenVPN jest blokowany przez dostawcę Internetu. Zmień port lub skontaktuj się z dostawcą w celu uzyskania pomocy.
- Połączenie VPN może być blokowane w niektórych krajach lub regionach.

10.2 Konfiguracja serwera WireGuard

WireGuard® to prosty, szybki i nowoczesny VPN wykorzystujący najnowsze rozwiązania kryptograficzne. Ma być szybszy, prostszy i bardziej użyteczny niż IPSec, bez związanych z nim komplikacji. Jego celem jest również znacznie wyższa wydajność niż OpenVPN. Aby skonfigurować serwer WireGuard na routerze GL.iNet, obejrzyj ten film lub wykonaj poniższe czynności.

10.2.1 Przygotowanie

1. **Upewnij się, że masz publiczny adres IP**

   Kliknij tutaj, aby sprawdzić, czy dostawca Internetu przydziela Ci publiczny adres IP. Jeśli nie, nie można skonfigurować routera jako serwera WireGuard.

   Rozwiązania alternatywne:

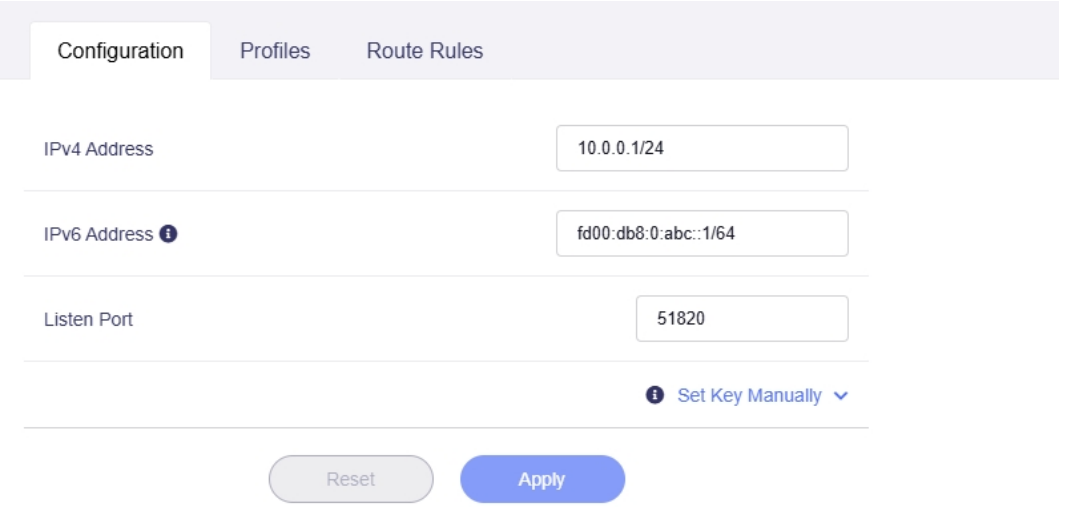
   - Jeśli przed routerem GL.iNet znajduje się główny router, zaloguj się do niego i sprawdź, czy ma publiczny adres IP przydzielony przez dostawcę Internetu.
   - Poproś dostawcę Internetu o publiczny adres IP. Może to wiązać się z dodatkową opłatą.
   - Jeśli dwie powyższe metody nie działają (np. gdy sieć znajduje się za CGNAT), możesz wypróbować nasze rozwiązanie SD-WAN AstroWarp.

2. **Sprawdź, czy wymagane jest przekierowanie portów**

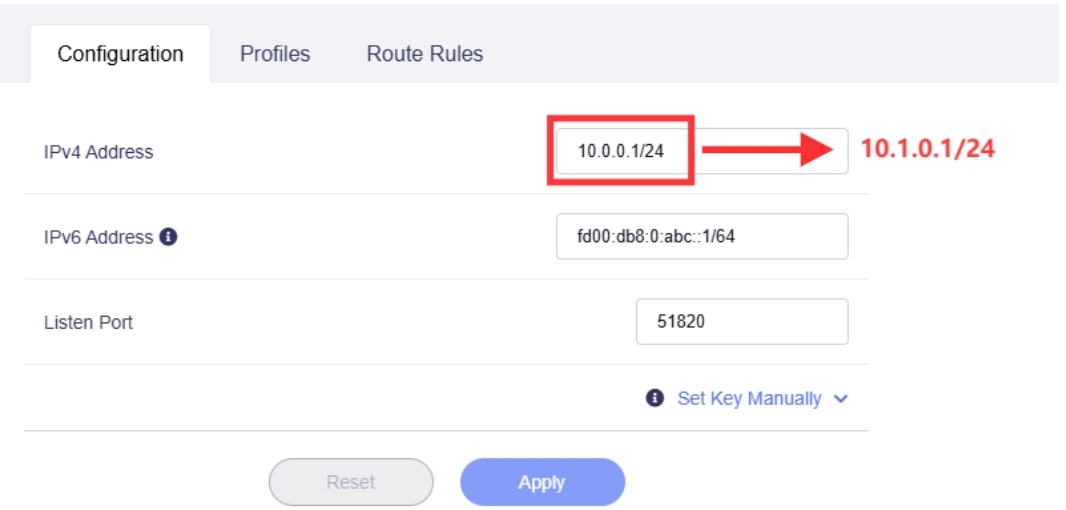
   - Jeśli router GL.iNet jest głównym routerem w sieci, konfiguracja przekierowania portów nie jest wymagana. Przejdź do następnego kroku.
   - Jeśli korzystasz już z głównego routera, a router GL.iNet działa jako router dodatkowy, trzeba skonfigurować przekierowanie portów na głównym routerze.
   - Jeśli router GL.iNet znajduje się kilka poziomów za głównym routerem, skonfiguruj przekierowanie portów na każdym urządzeniu pośrednim.

10.2.2 Etapy konfiguracji

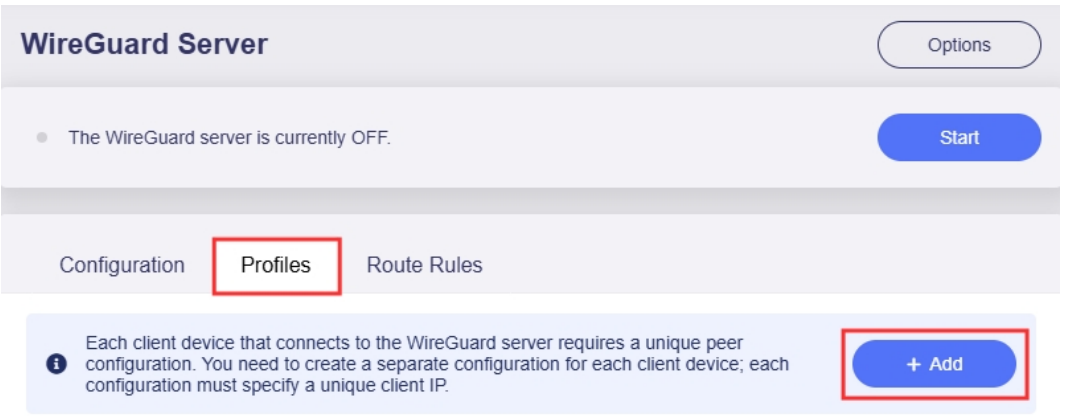
1. Zaloguj się do panelu administracyjnego routera, przejdź do **VPN** > **WireGuard Server**, a następnie kliknij **Generate Configuration** (tylko przy pierwszej konfiguracji serwera VPN).
2. Zastosuj konfigurację.
   Domyślna konfiguracja sprawdza się w większości przypadków. Nie trzeba zmieniać adresu IPv4, chyba że koliduje z adresem bramy routera nadrzędnego.



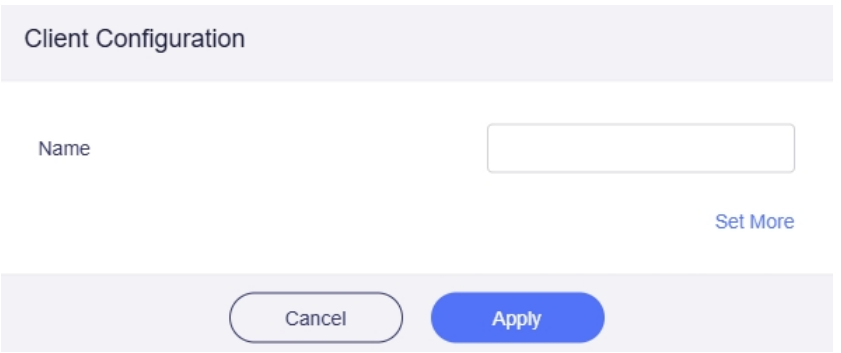
   Jeśli adres IPv4 koliduje z adresem bramy routera nadrzędnego, zmień go na inny (np. **10.1.0.1/24**) i kliknij **Apply**. Aby uniknąć problemów z łącznością, koniecznie zachowaj zapis CIDR „/24”.



3. Dodaj profil.
   Przejdź na kartę **Profiles** i kliknij przycisk **Add**, aby wygenerować profil dla urządzenia.



Nadaj opisową nazwę i kliknij **Apply**, aby kontynuować.

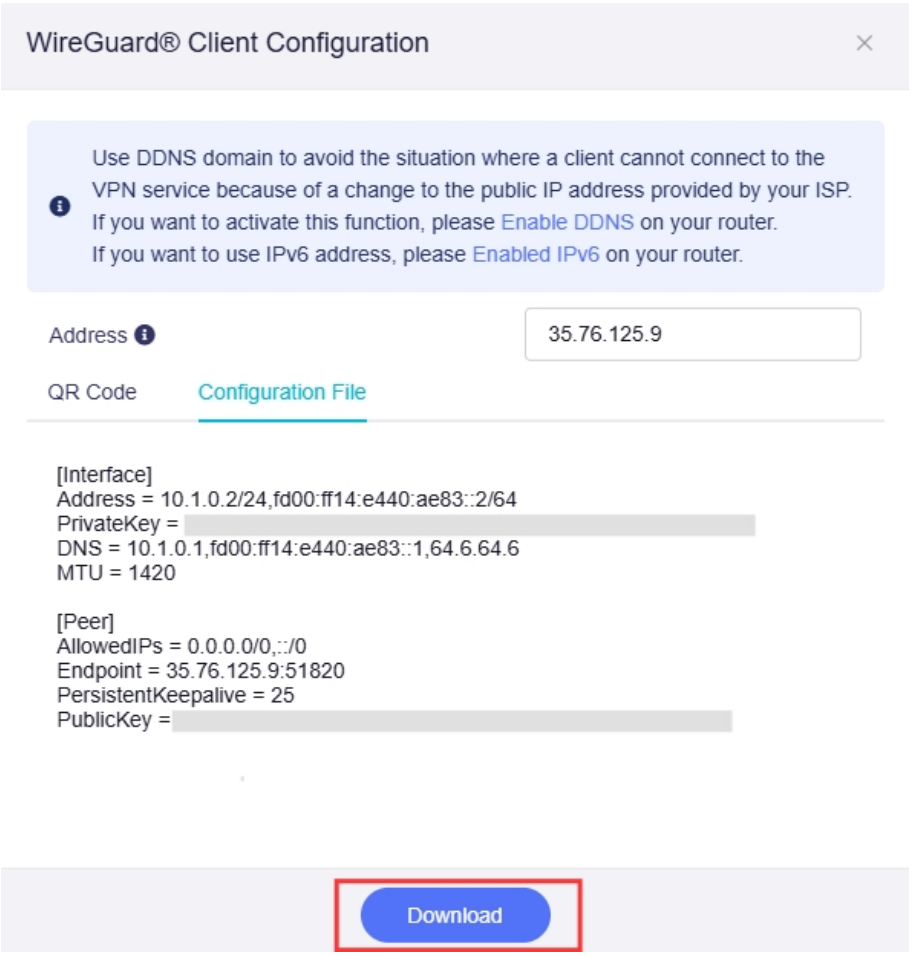


Wskazówka: aby z serwera WireGuard uzyskać dostęp do urządzeń LAN klienta WireGuard, przejdź na kartę **Route Rules** i skonfiguruj reguły routingu. Szczegóły znajdziesz tutaj.

4. Pobierz konfigurację.

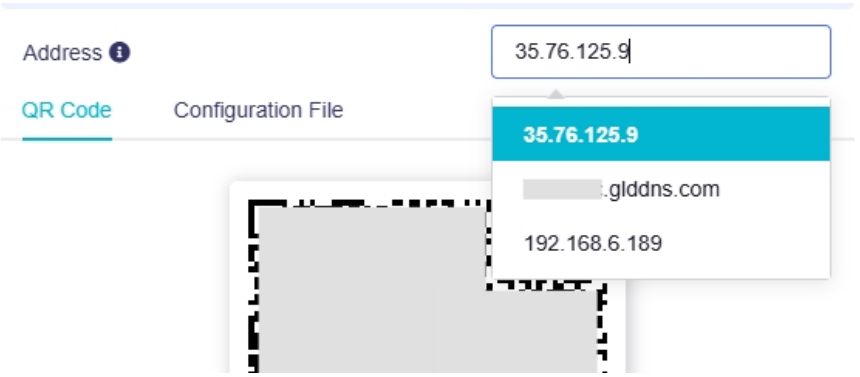
   Po dodaniu profilu router generuje plik konfiguracyjny w trzech postaciach: kodu QR, zwykłego tekstu i pliku .conf. Wybierz preferowany sposób uzyskania konfiguracji.

   - **Kod QR**: odpowiedni dla urządzeń (np. smartfonów, tabletów, laptopów) z zainstalowaną aplikacją WireGuard. Aby skonfigurować urządzenie jako klienta WireGuard, otwórz aplikację WireGuard i zeskanuj kod QR w celu zaimportowania pliku konfiguracyjnego.
   - **Zwykły tekst**: umożliwia sprawdzenie szczegółów konfiguracji oraz wygodne skopiowanie i wklejenie ich w innym miejscu do ręcznej konfiguracji, np. w aplikacji WireGuard lub na routerze GL.iNet.
   - **Plik .conf**: kliknij przycisk **Download**, aby zapisać plik .conf na urządzeniu lokalnym. Można go następnie bezpośrednio przesłać do aplikacji WireGuard lub routera GL.iNet.

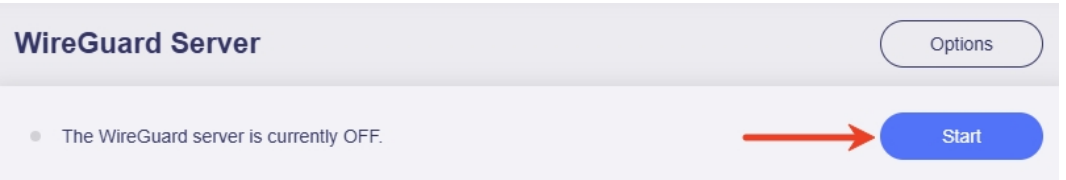


Wskazówki:

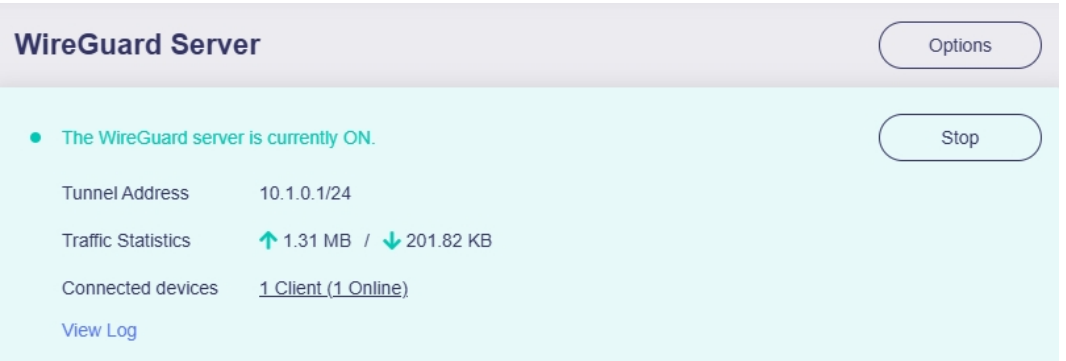
- Jeśli Twój publiczny adres IP często się zmienia, przejdź do **APPLICATIONS** > **Dynamic DNS** i włącz DDNS. Możesz wtedy używać domeny DDNS jako adresu serwera.
- Od wersji oprogramowania 4.8 przed wyeksportowaniem pliku konfiguracyjnego można wybrać adres serwera z listy: publiczny adres IP, domenę DDNS lub bieżący adres IP WAN. Po wybraniu adres serwera w pliku konfiguracyjnym zostanie automatycznie zaktualizowany. Pobierz plik konfiguracyjny ponownie, jeśli adres serwera ulegnie zmianie.



5. Uruchom serwer WireGuard.
   Na stronie **WireGuard Server** kliknij przycisk **Start** w prawym górnym rogu, aby uruchomić serwer.



   Stan połączenia serwera jest wyświetlany u góry. Jeśli widoczne są statystyki wysyłania i pobierania oraz podłączone urządzenia online, serwer WireGuard działa.



10.2.3 Rozwiązywanie problemów

Jeśli połączenie się nie powiedzie, przyczyną może być jeden z typowych problemów:

- Serwer VPN nie ma publicznego adresu IP. Pomoc znajdziesz tutaj.
- Może być wymagane przekierowanie portów. Pomoc znajdziesz tutaj.
- Port używany przez serwer WireGuard jest blokowany przez dostawcę Internetu. Zmień port lub skontaktuj się z dostawcą w celu uzyskania pomocy.
- Połączenie VPN może być blokowane w niektórych krajach lub regionach.

Rozdział 11

Konfiguracja klienta VPN

W tym rozdziale opisano konfigurację routera GL.iNet jako klienta OpenVPN lub WireGuard.

11.1 Konfiguracja klienta OpenVPN

11.1.1 Przygotowanie

Najpierw upewnij się, że masz aktywną subskrypcję u dostawcy VPN obsługującego ręczną konfigurację OpenVPN. Listę dostawców OpenVPN zgodnych z GL.iNet znajdziesz tutaj.

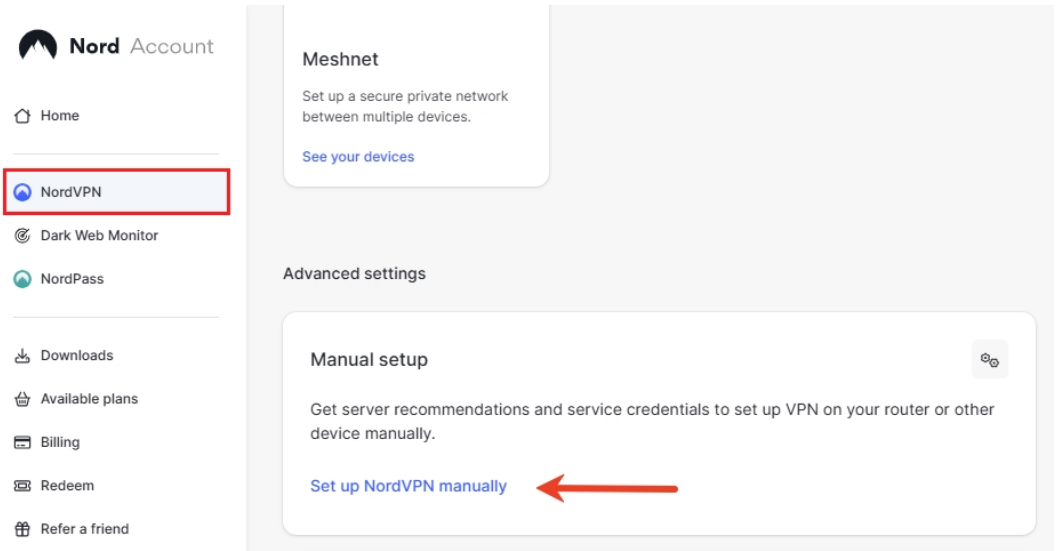
Następnie odwiedź oficjalną witrynę dostawcy VPN, którego usługę subskrybujesz, i uzyskaj dane dostępowe usługi lub plik konfiguracyjny. Jeśli nie wiesz, jak uzyskać plik konfiguracyjny, skorzystaj z tego łącza lub skontaktuj się z pomocą techniczną dostawcy.

11.1.2 Konfiguracja NordVPN

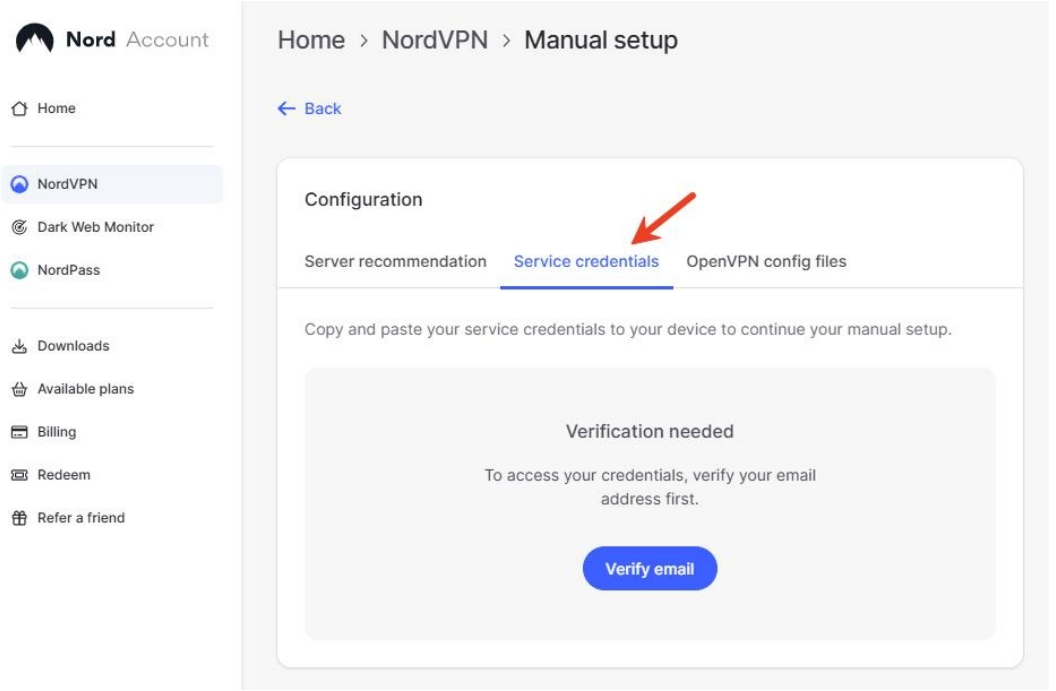
NordVPN jest zintegrowany z panelem administracyjnym GL.iNet. Pliki konfiguracyjne wszystkich serwerów NordVPN można uzyskać, wprowadzając dane dostępowe konta (z panelu NordVPN) w panelu administracyjnym routera lub aplikacji mobilnej GL.iNet. Eliminuje to potrzebę ręcznego przesyłania plików.

Aby skonfigurować router jako klienta NordVPN, wykonaj poniższe czynności.

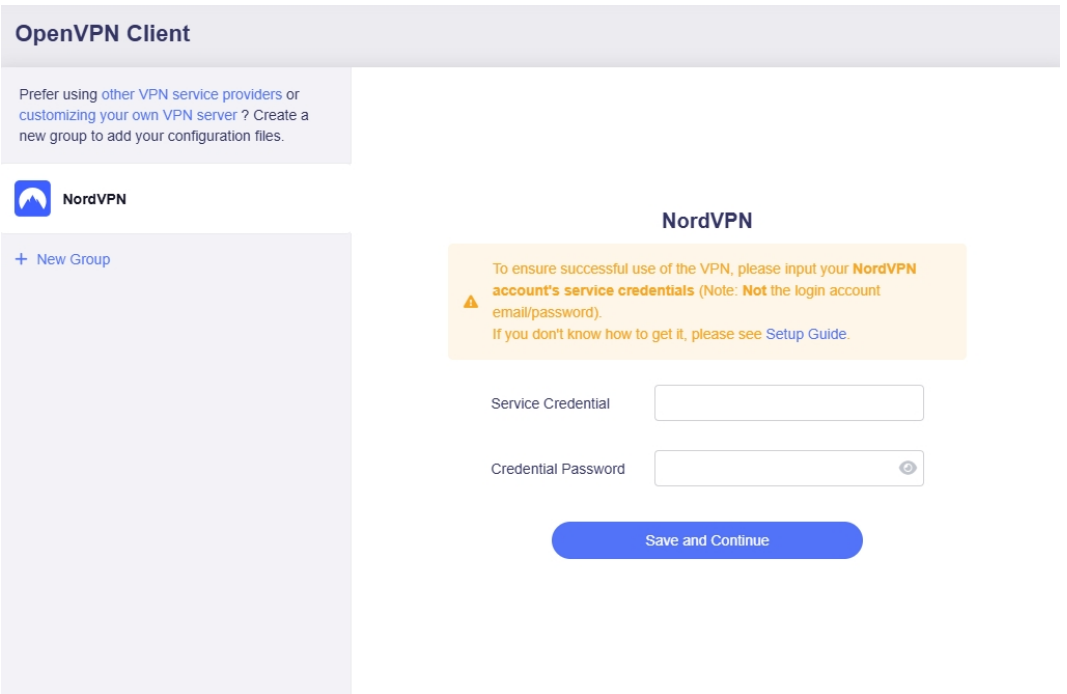
1. Zaloguj się na swoje konto internetowe NordVPN tutaj.
2. W panelu Nord kliknij **NordVPN**, a następnie **Set up NordVPN manually**.



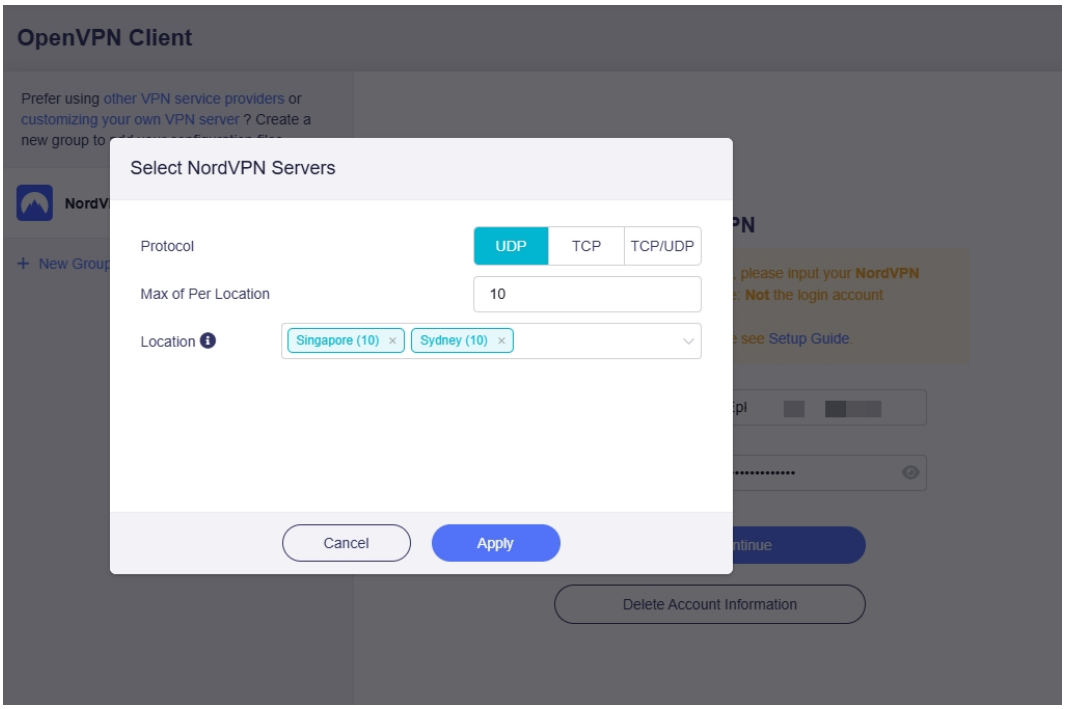
Znajdziesz tam **dane dostępowe usługi**. Skopiuj je do późniejszego użycia.



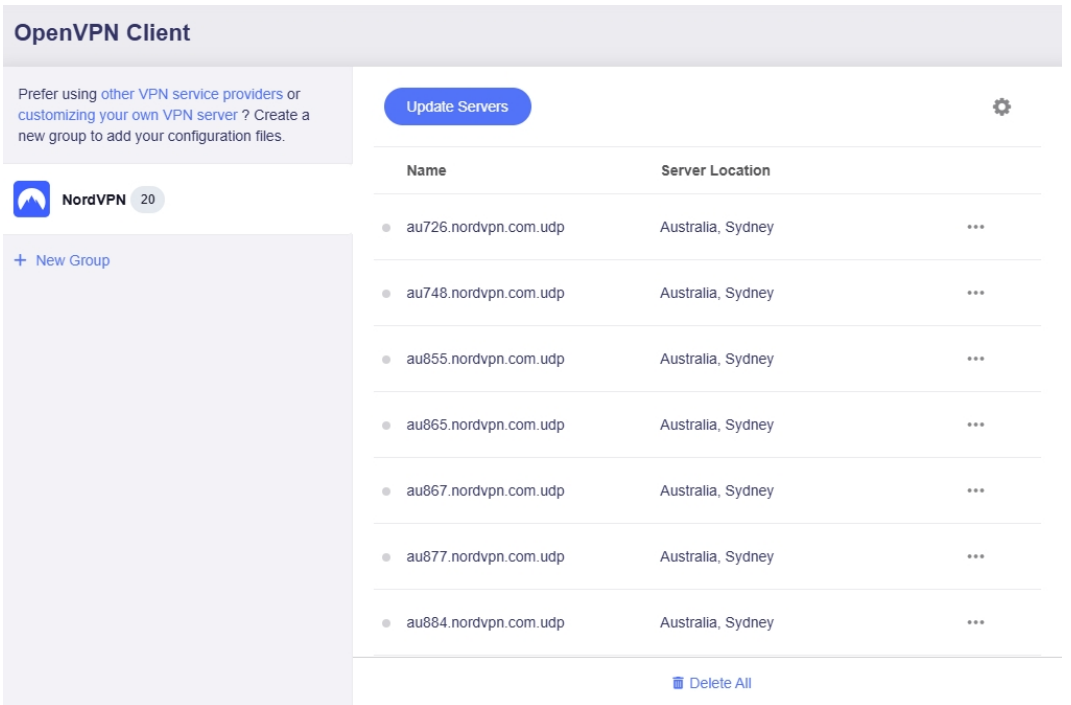
3. Zaloguj się do panelu administracyjnego routera i przejdź do **VPN** > **OpenVPN Client** > **NordVPN**. Wprowadź dane dostępowe usługi (uwaga: NIE jest to adres e-mail ani hasło do logowania na konto), a następnie kliknij **Save and Continue**.



4. Wybierz protokół, maksymalną liczbę serwerów dla każdej lokalizacji oraz lokalizacje, a następnie kliknij **Apply**.

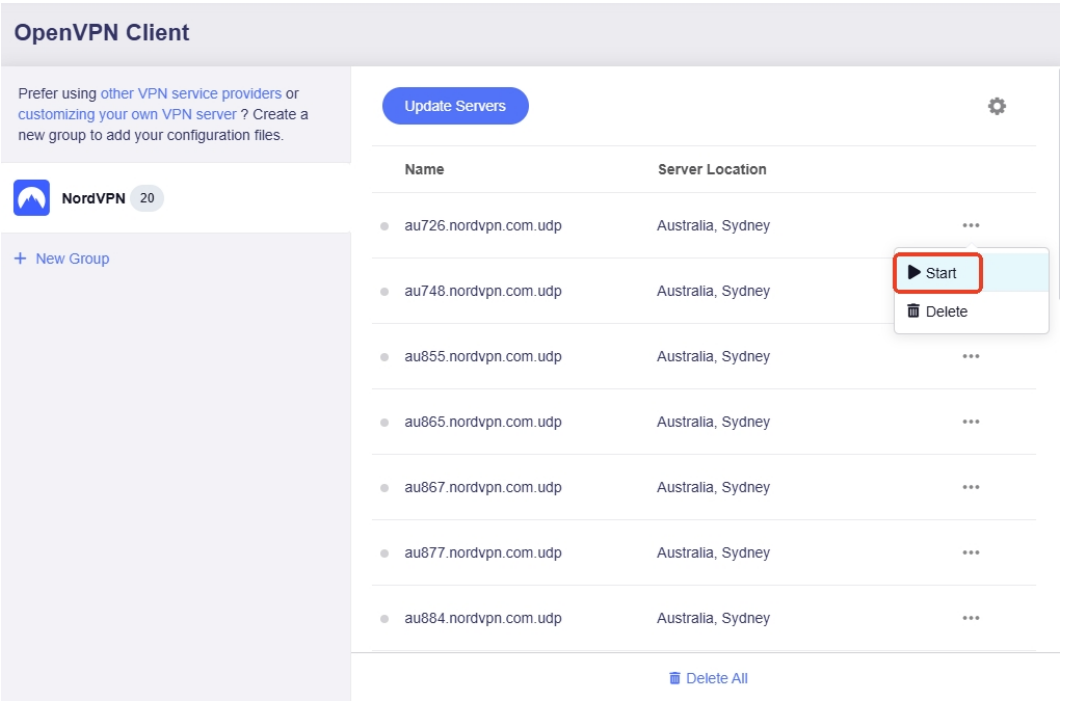


Rozpocznie się pobieranie plików konfiguracyjnych.

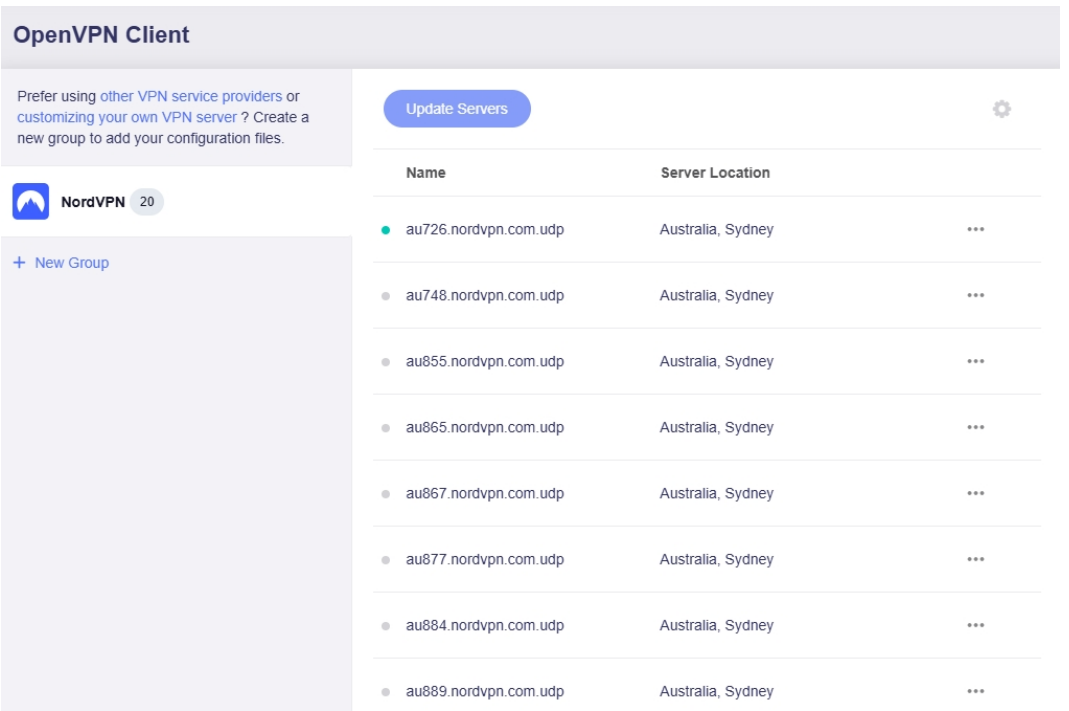


5. Nawiąż połączenie.

   Wybierz serwer i kliknij ikonę trzech kropek po prawej stronie, aby nawiązać połączenie.



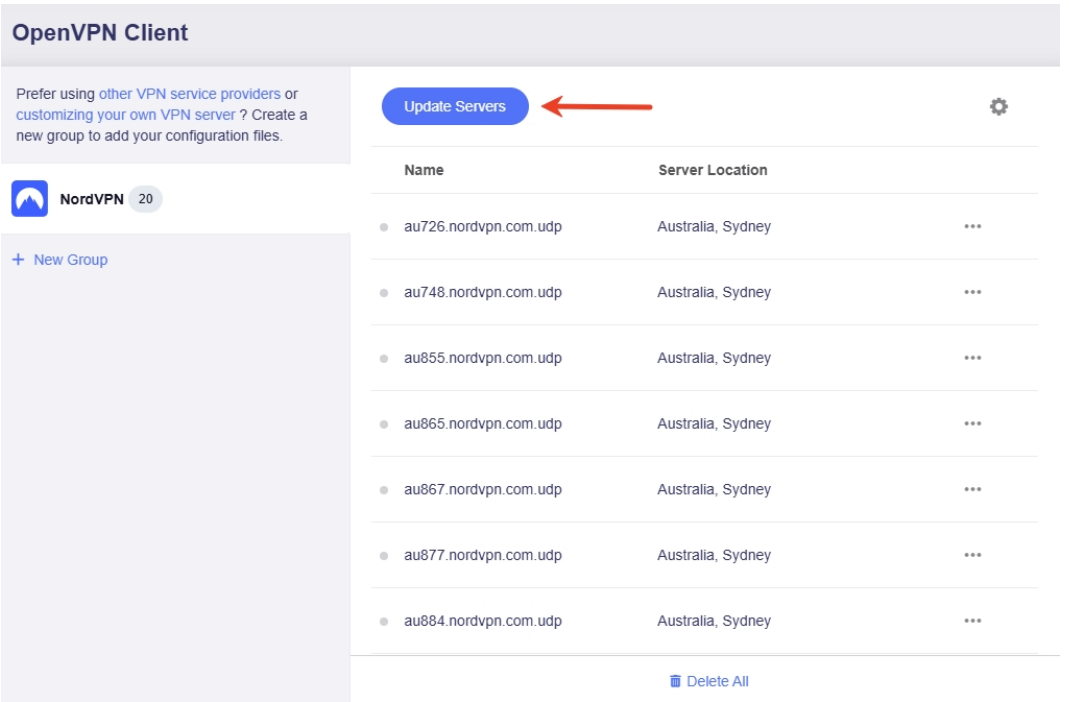
6. Po połączeniu obok pliku konfiguracyjnego pojawi się zielona kropka.



Szczegóły połączenia VPN możesz również sprawdzić w **VPN Dashboard**.

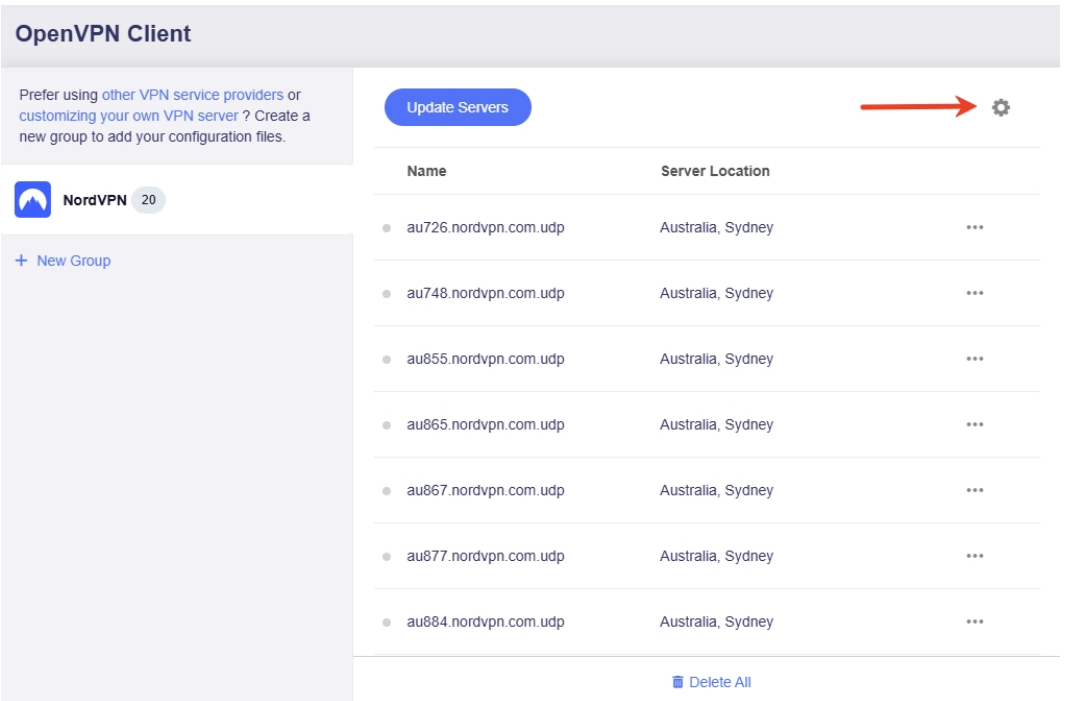
7. Zaktualizuj serwery.

   Możesz kliknąć **Update Servers**, aby pobrać aktualną listę dostępnych serwerów i uniknąć problemów z połączeniem spowodowanych konserwacją lub wyłączeniem serwerów.



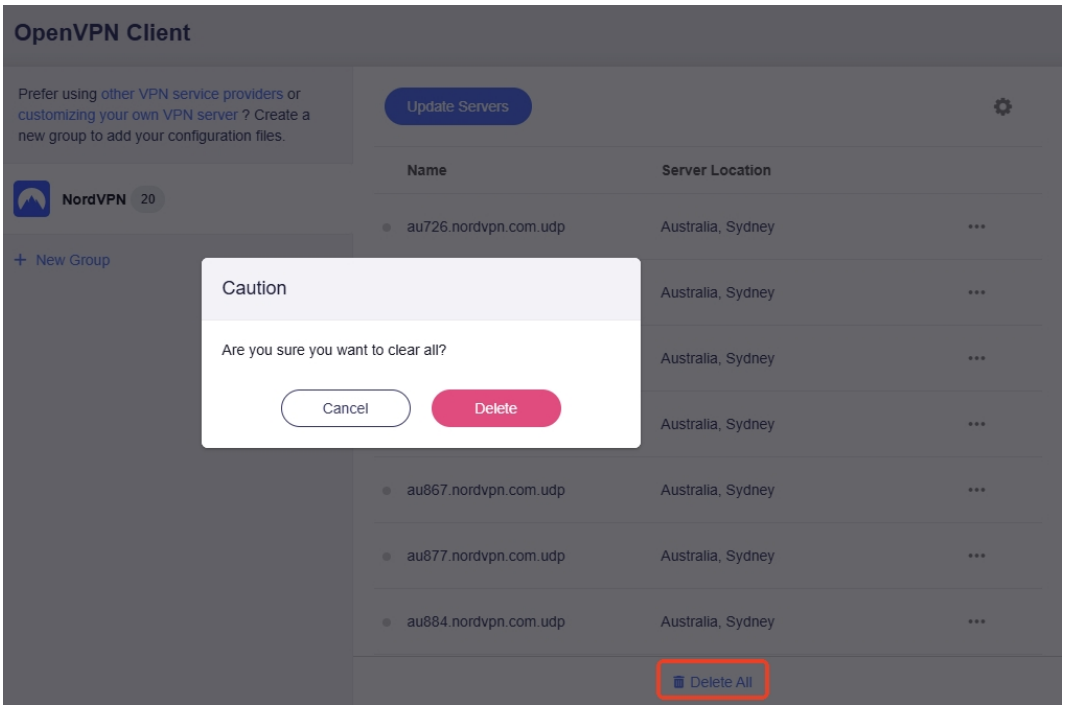
8. Zmień dane dostępowe.

   Kliknij ikonę koła zębatego, aby zmienić dane logowania.



9. Usuń wszystkie pliki.

   Możesz kliknąć **Delete All**, aby jednym kliknięciem usunąć wszystkie pliki konfiguracyjne.

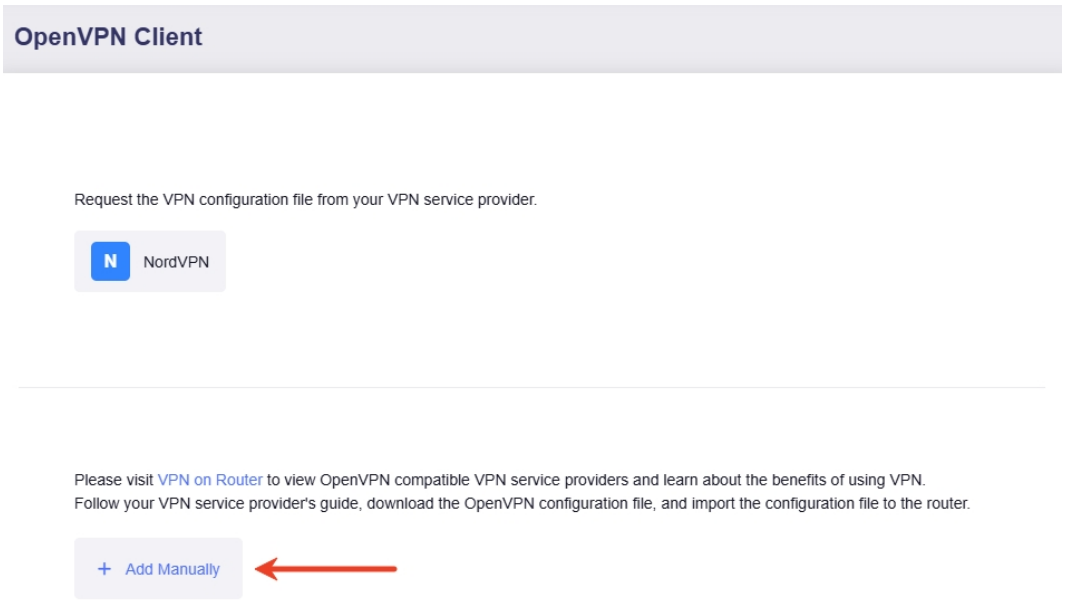


11.1.3 Ręczna konfiguracja klienta OpenVPN (inni dostawcy)

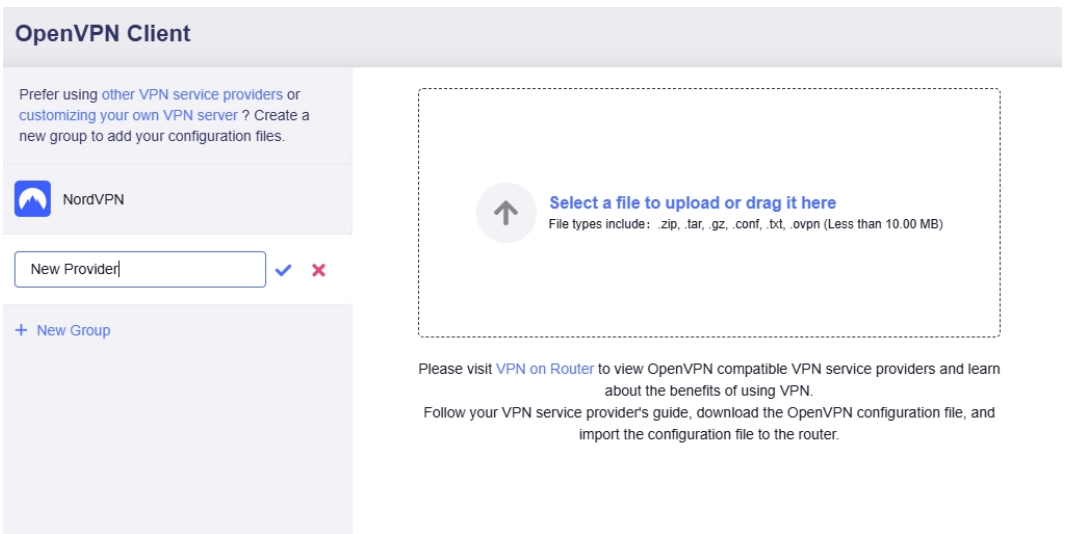
Jeśli Twój dostawca OpenVPN nie jest zintegrowany z panelem administracyjnym, najpierw odwiedź jego oficjalną witrynę i pobierz plik konfiguracyjny. Następnie prześlij go do routera, aby skonfigurować klienta OpenVPN.

W poniższych krokach jako przykład wykorzystano PIA (Private Internet Access).

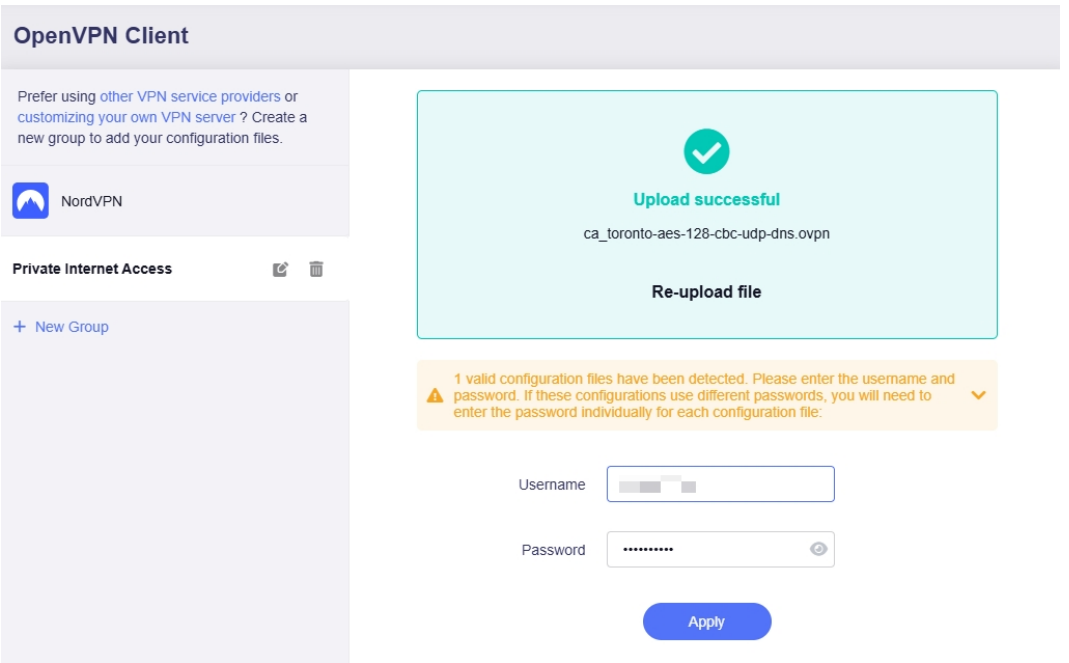
1. Pobierz plik konfiguracyjny z oficjalnej witryny Private Internet Access.
2. Zaloguj się do panelu administracyjnego routera, przejdź do **VPN** > **OpenVPN Client** i kliknij **Add Manually**.



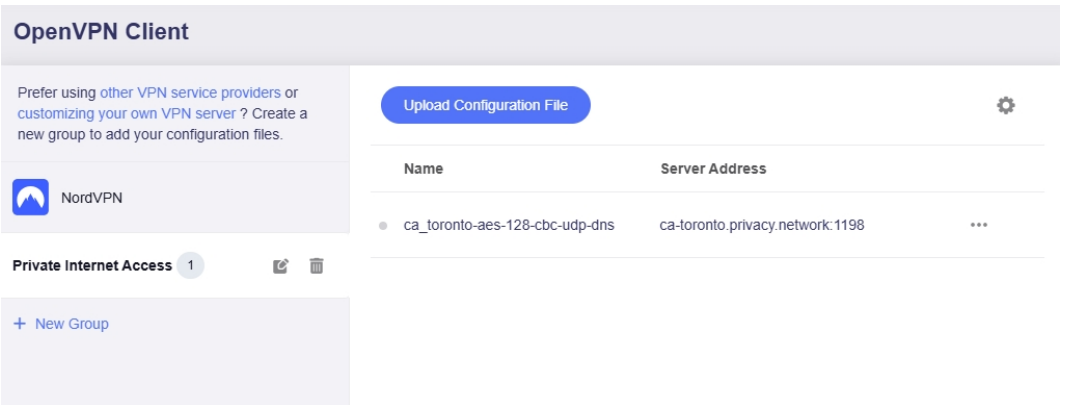
3. Na lewym pasku bocznym powstanie grupa. Nadaj jej opisową nazwę.



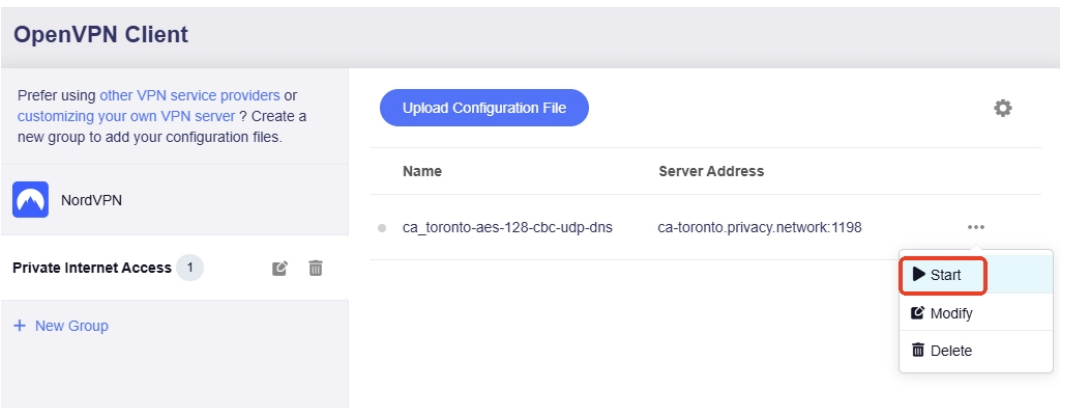
4. Prześlij plik konfiguracyjny OpenVPN. Jeśli jest to wymagane, wprowadź dane dostępowe, a następnie kliknij **Apply**.



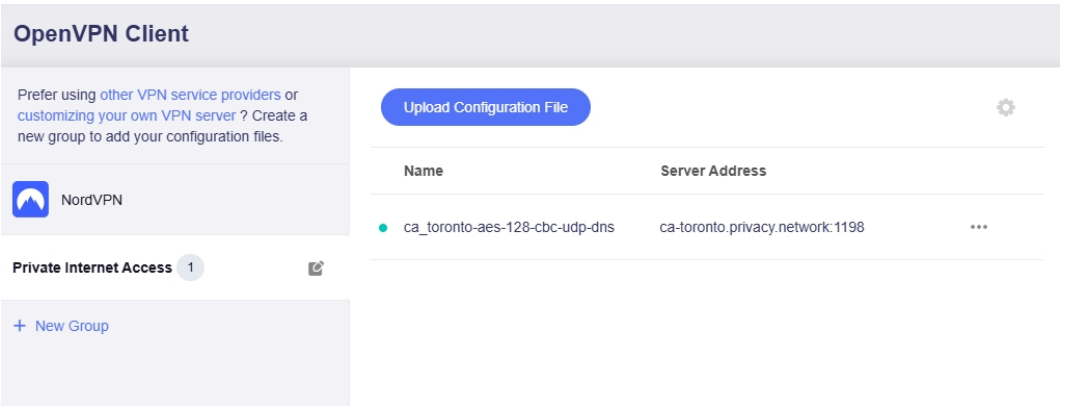
Pojawi się przesłany plik konfiguracyjny.



5. Kliknij ikonę trzech kropek po prawej stronie, aby nawiązać połączenie.



6. Po połączeniu obok pliku konfiguracyjnego pojawi się zielona kropka.



Szczegóły połączenia VPN możesz również sprawdzić w **VPN Dashboard**.

11.2 Konfiguracja klienta WireGuard

Klienta WireGuard można skonfigurować za pomocą aplikacji mobilnej GL.iNet lub panelu administracyjnego w przeglądarce.

- Aplikacja mobilna integruje niektórych dostawców usług WireGuard, takich jak AzireVPN, Mullvad VPN, OVPN, StrongVPN i PIA VPN. Wystarczy wprowadzić dane logowania do subskrybowanej usługi WireGuard. Otwórz aplikację i postępuj zgodnie z instrukcjami na ekranie, aby wykonać konfigurację.
- Panel administracyjny integruje niektórych dostawców usług WireGuard i umożliwia również ręczną konfigurację. Możesz wprowadzić dane dostępowe subskrybowanej usługi WireGuard w celu szybkiej konfiguracji lub ręcznie przesłać plik konfiguracyjny.

11.2.1 Przygotowanie

Najpierw upewnij się, że masz aktywną subskrypcję u dostawcy VPN obsługującego ręczną konfigurację WireGuard. Listę dostawców WireGuard zgodnych z GL.iNet znajdziesz tutaj.

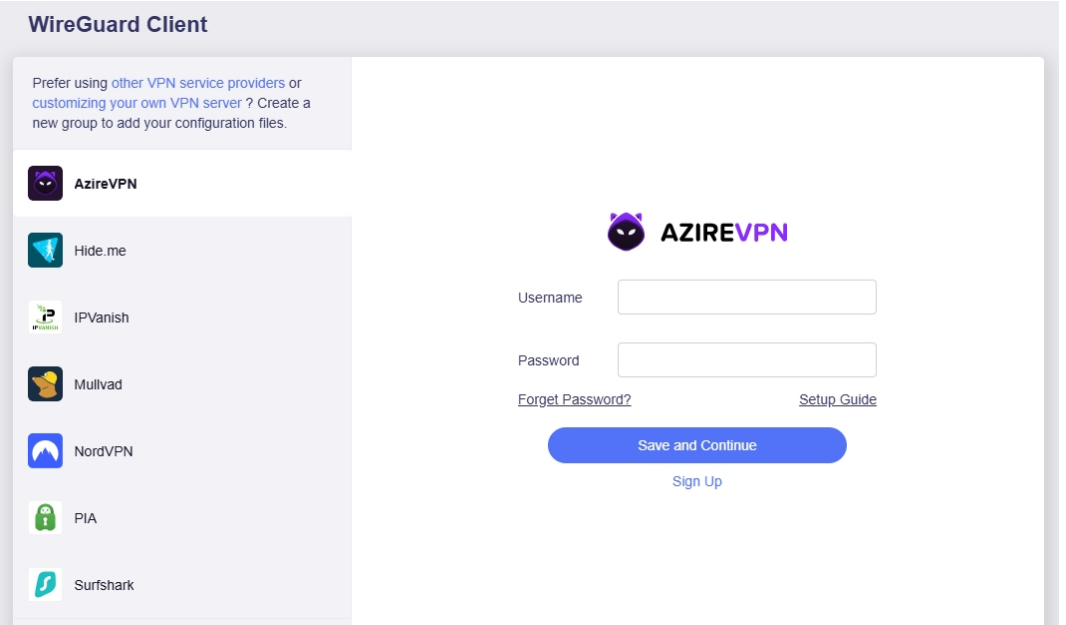
Następnie wybierz poniżej odpowiedniego dostawcę WireGuard, aby szybko przejść do instrukcji krok po kroku.

- Konfiguracja AzireVPN
- Konfiguracja Hide.me
- Konfiguracja IPVanish
- Konfiguracja Mullvad
- Konfiguracja NordVPN
- Konfiguracja PIA (Private Internet Access)
- Konfiguracja Surfshark
- Ręczna konfiguracja klienta WireGuard (inni dostawcy)

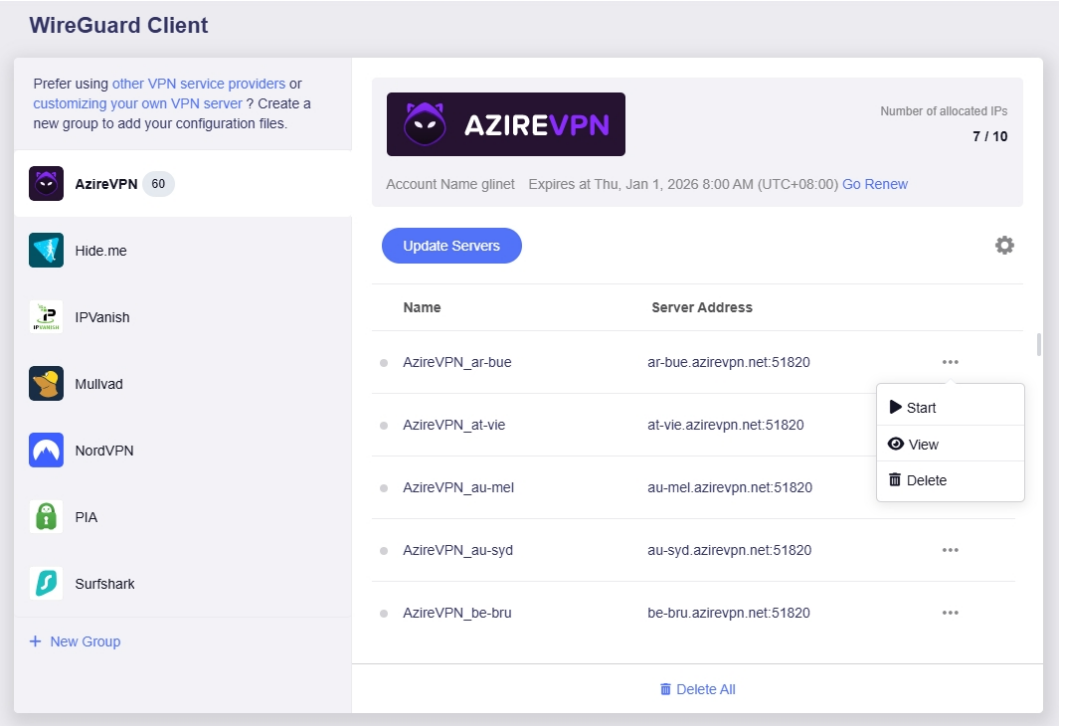
11.2.2 Konfiguracja AzireVPN

Aby skonfigurować router jako klienta AzireVPN, wykonaj poniższe czynności.

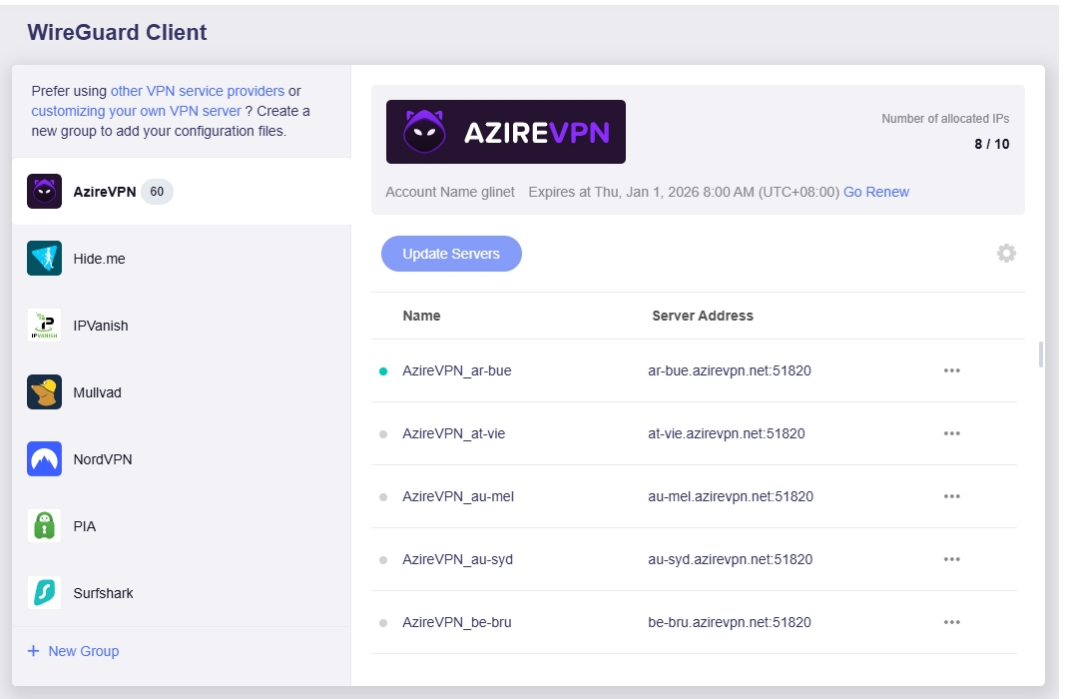
1. Zaloguj się do panelu administracyjnego routera i przejdź do **VPN** > **WireGuard Client** > **AzireVPN**.
2. Wprowadź nazwę użytkownika i hasło, a następnie kliknij **Save and Continue**. Zostaną wygenerowane pliki konfiguracyjne dla każdego serwera.



3. Wybierz preferowany serwer i kliknij ikonę trzech kropek po prawej stronie, aby nawiązać połączenie.



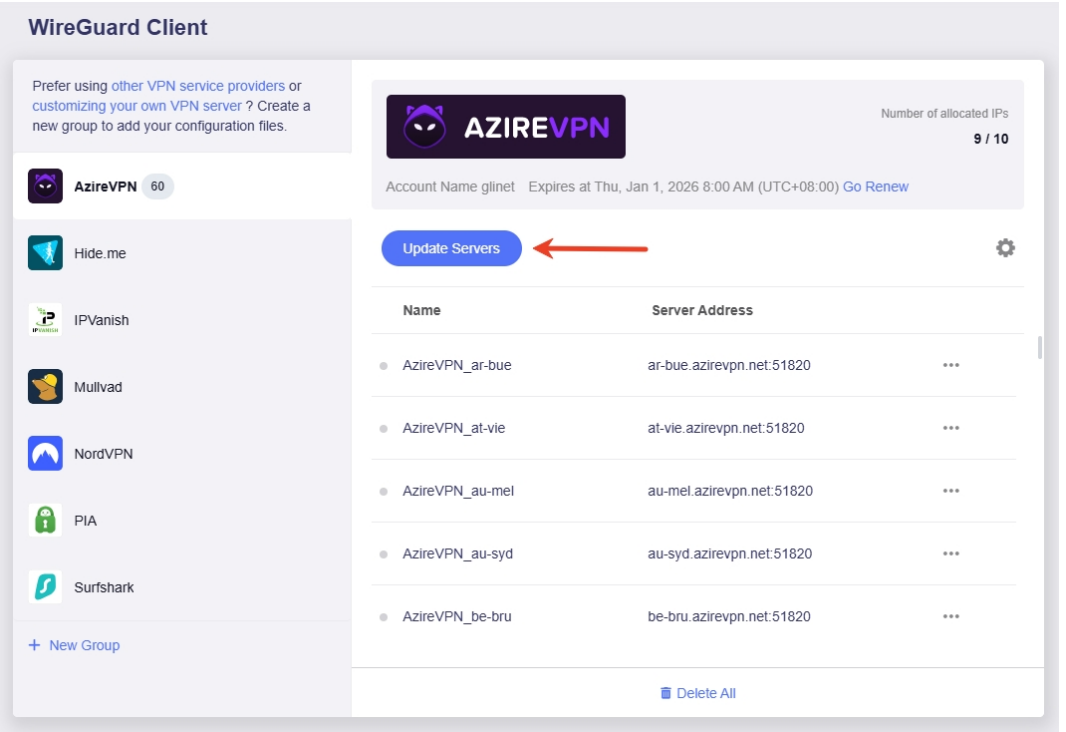
4. Po połączeniu obok pliku konfiguracyjnego pojawi się zielona kropka.



Szczegóły połączenia VPN możesz również sprawdzić w **VPN Dashboard**.

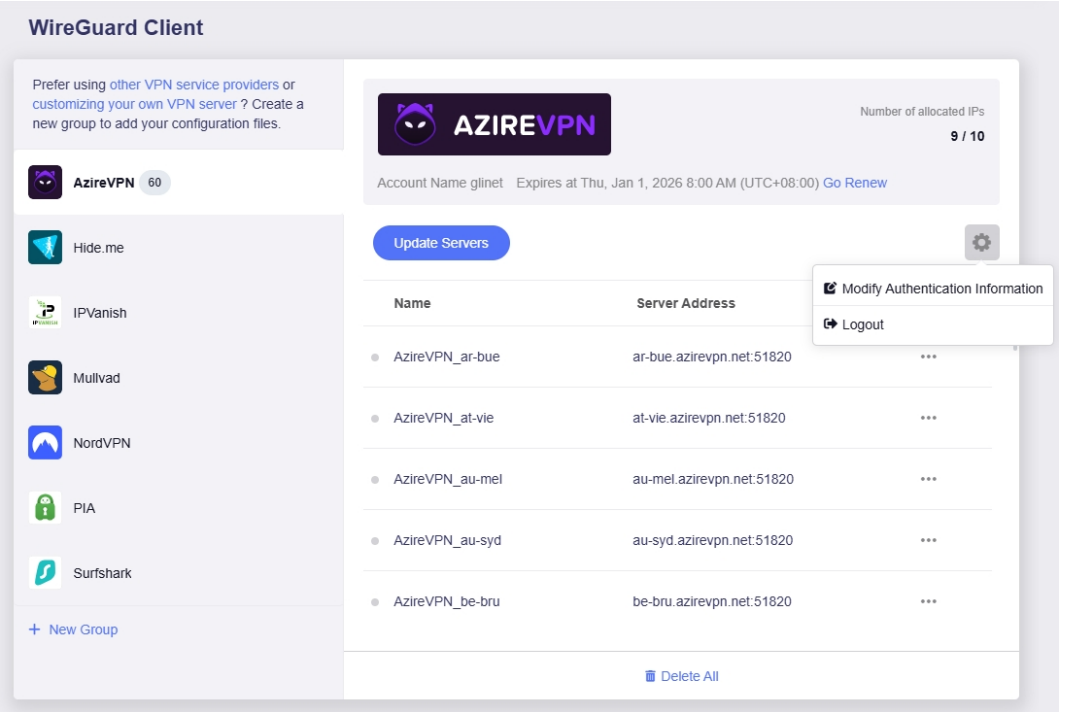
5. Zaktualizuj serwery.

   Możesz kliknąć **Update Servers**, aby pobrać aktualną listę dostępnych serwerów i uniknąć problemów z połączeniem spowodowanych konserwacją lub wyłączeniem serwerów.



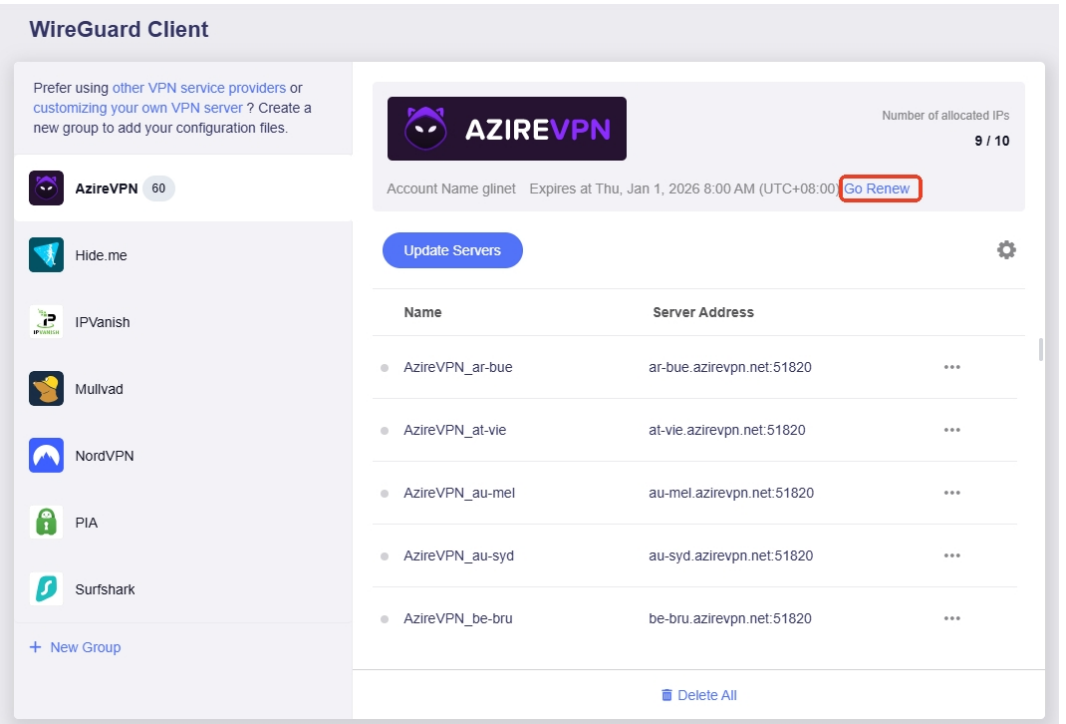
6. Zmiana danych logowania lub wylogowanie.

   Kliknij ikonę koła zębatego, aby zmienić dane logowania lub się wylogować.



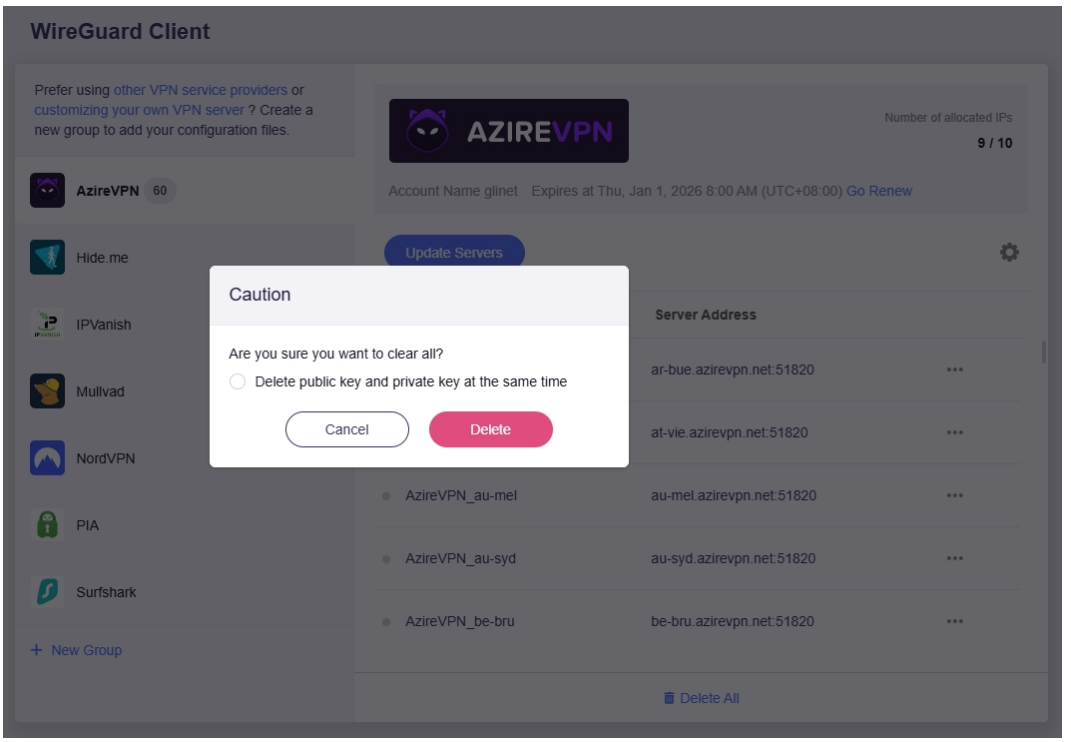
7. Odnowienie subskrypcji.

   Po kliknięciu **Go Renew** nastąpi przekierowanie na oficjalną stronę w celu odnowienia subskrypcji.



8. Usuń wszystkie pliki.

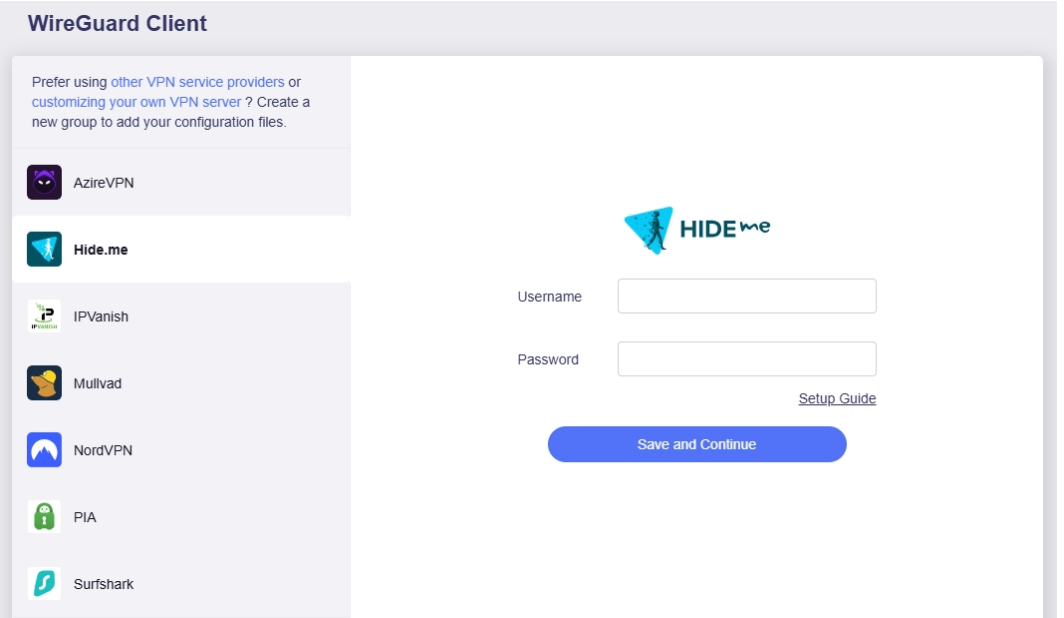
   Możesz kliknąć **Delete All**, aby jednym kliknięciem usunąć wszystkie pliki konfiguracyjne, oraz wybrać, czy jednocześnie usunąć klucze prywatny i publiczny.



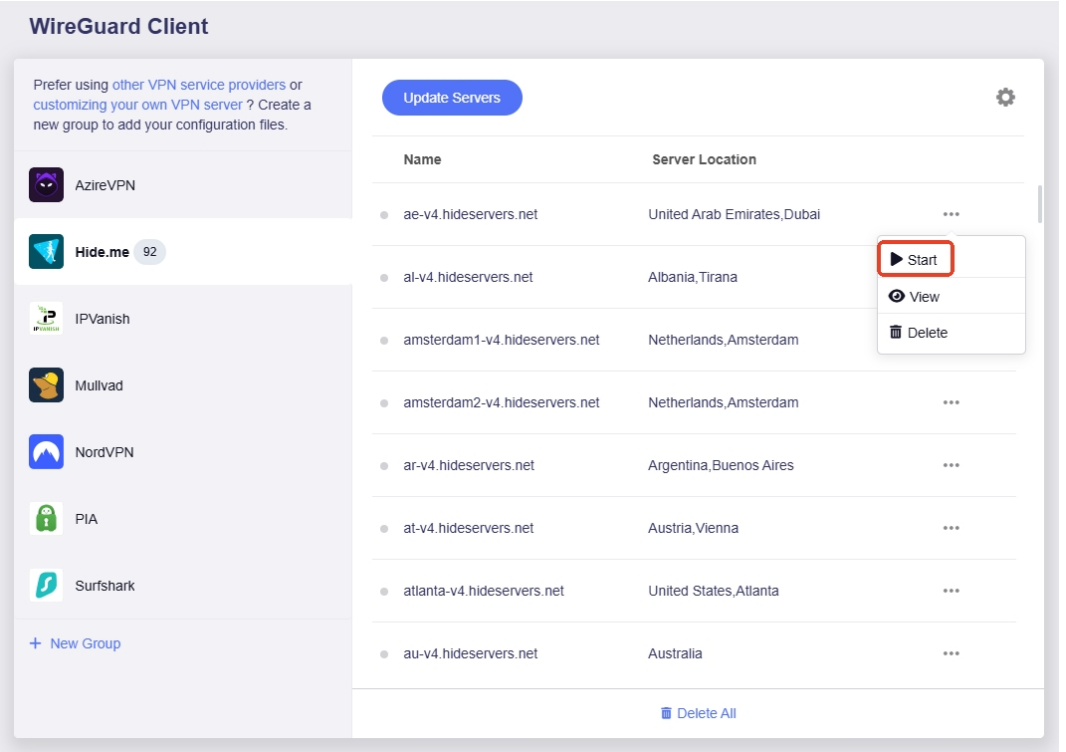
11.2.3 Konfiguracja Hide.me

Aby skonfigurować router jako klienta Hide.me, wykonaj poniższe czynności.

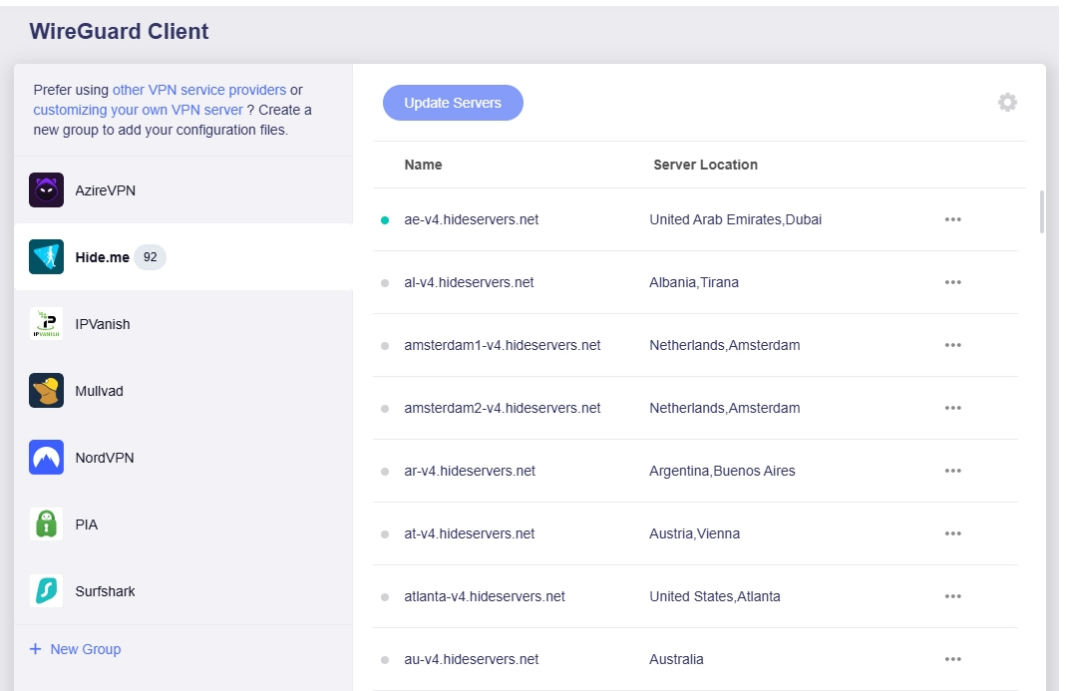
1. Zaloguj się do panelu administracyjnego routera i przejdź do **VPN** > **WireGuard Client** > **Hide.me**.
2. Wprowadź nazwę użytkownika i hasło, a następnie kliknij **Save and Continue**. Zostaną wygenerowane pliki konfiguracyjne dla każdego serwera.



3. Wybierz preferowany serwer i kliknij ikonę trzech kropek po prawej stronie, aby nawiązać połączenie.



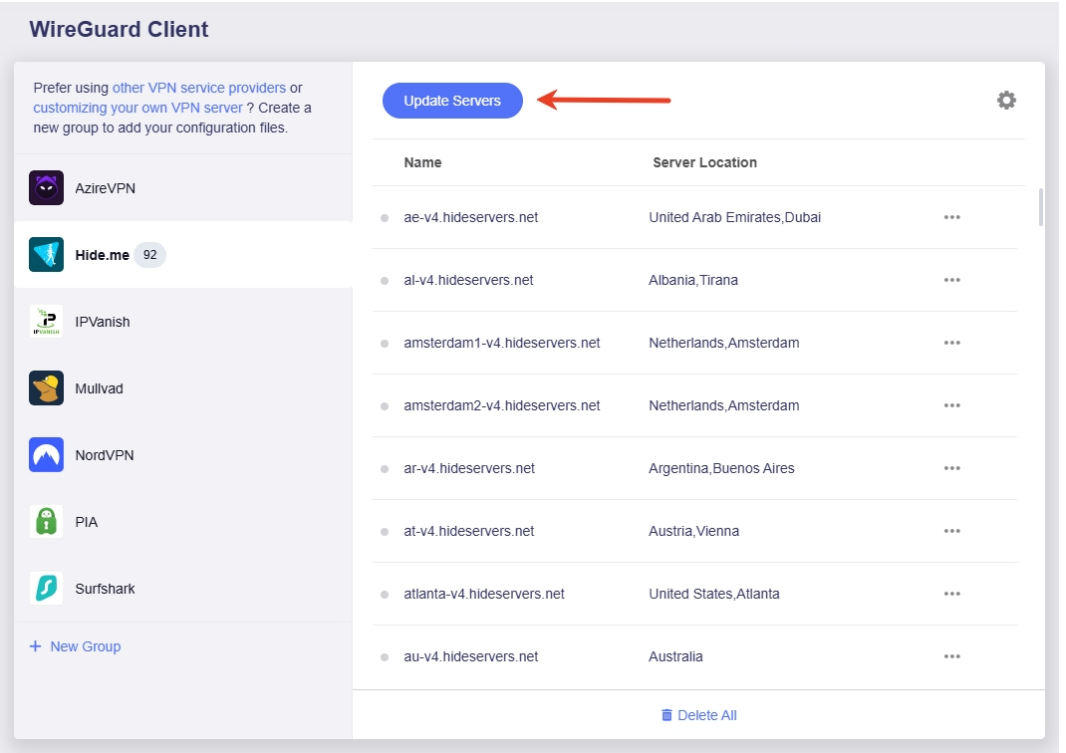
4. Po połączeniu obok pliku konfiguracyjnego pojawi się zielona kropka.



Szczegóły połączenia VPN możesz również sprawdzić w **VPN Dashboard**.

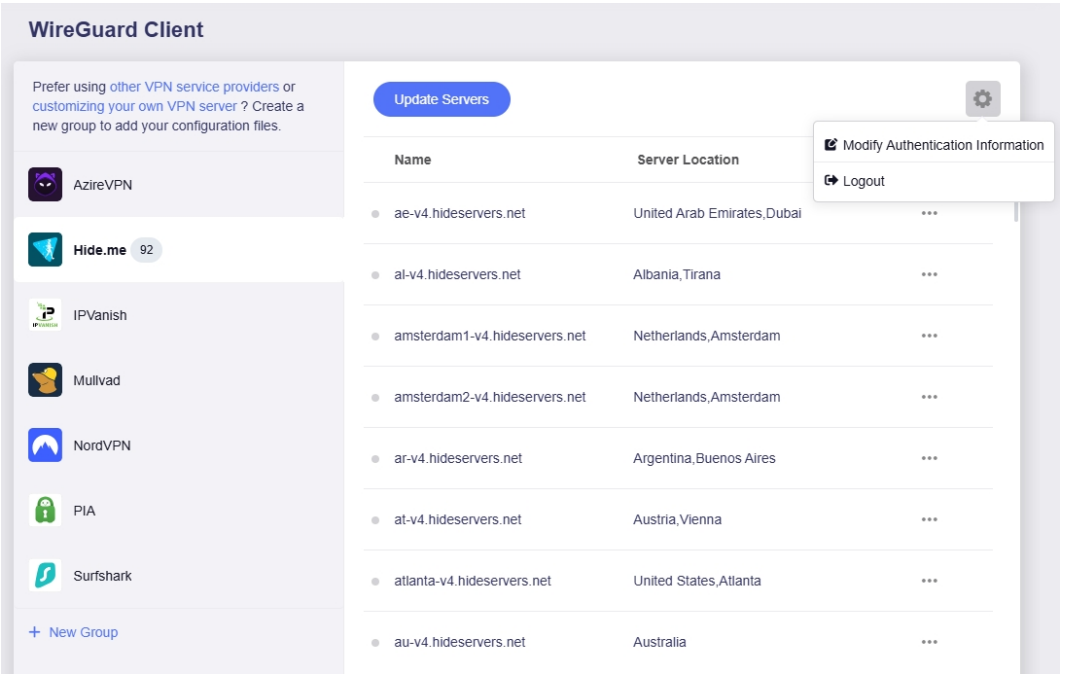
5. Zaktualizuj serwery.

   Możesz kliknąć **Update Servers**, aby pobrać aktualną listę dostępnych serwerów i uniknąć problemów z połączeniem spowodowanych konserwacją lub wyłączeniem serwerów.



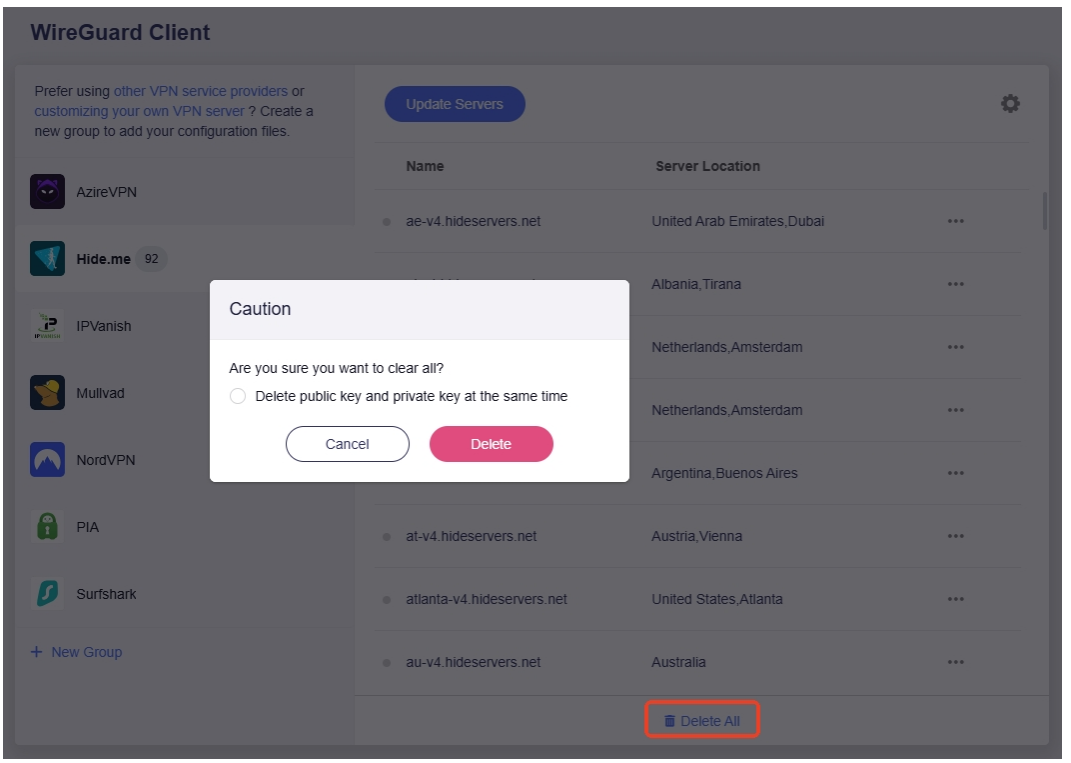
6. Zmiana danych logowania lub wylogowanie.

   Kliknij ikonę koła zębatego, aby zmienić dane logowania lub się wylogować.



7. Usuń wszystkie pliki.

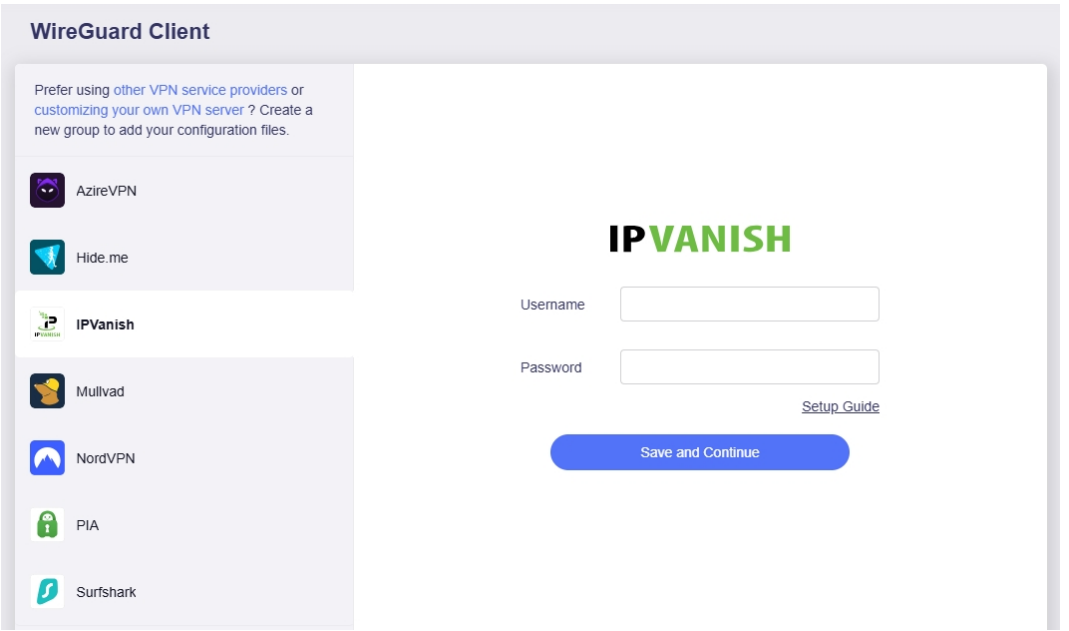
   Możesz kliknąć **Delete All**, aby jednym kliknięciem usunąć wszystkie pliki konfiguracyjne, oraz wybrać, czy jednocześnie usunąć klucze prywatny i publiczny.



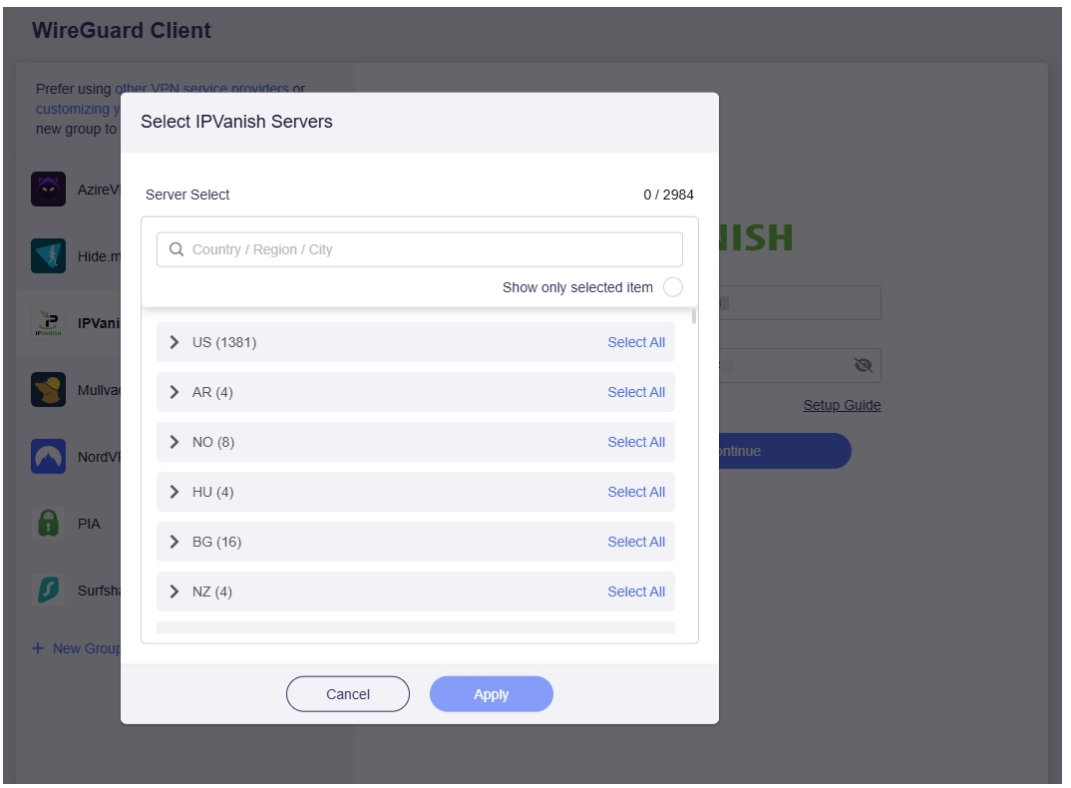
11.2.4 Konfiguracja IPVanish

Aby skonfigurować router jako klienta IPVanish, wykonaj poniższe czynności.

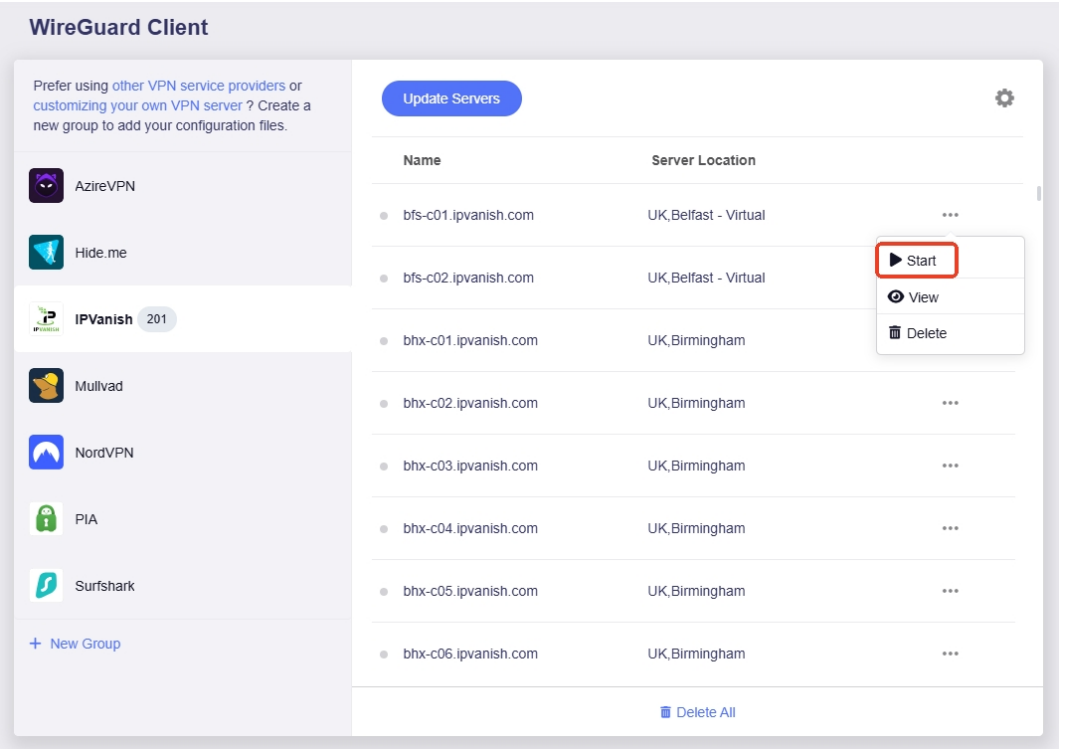
1. Zaloguj się do panelu administracyjnego routera i przejdź do **VPN** > **WireGuard Client** > **IPVanish**.
2. Wprowadź nazwę użytkownika i hasło, a następnie kliknij **Save and Continue**.



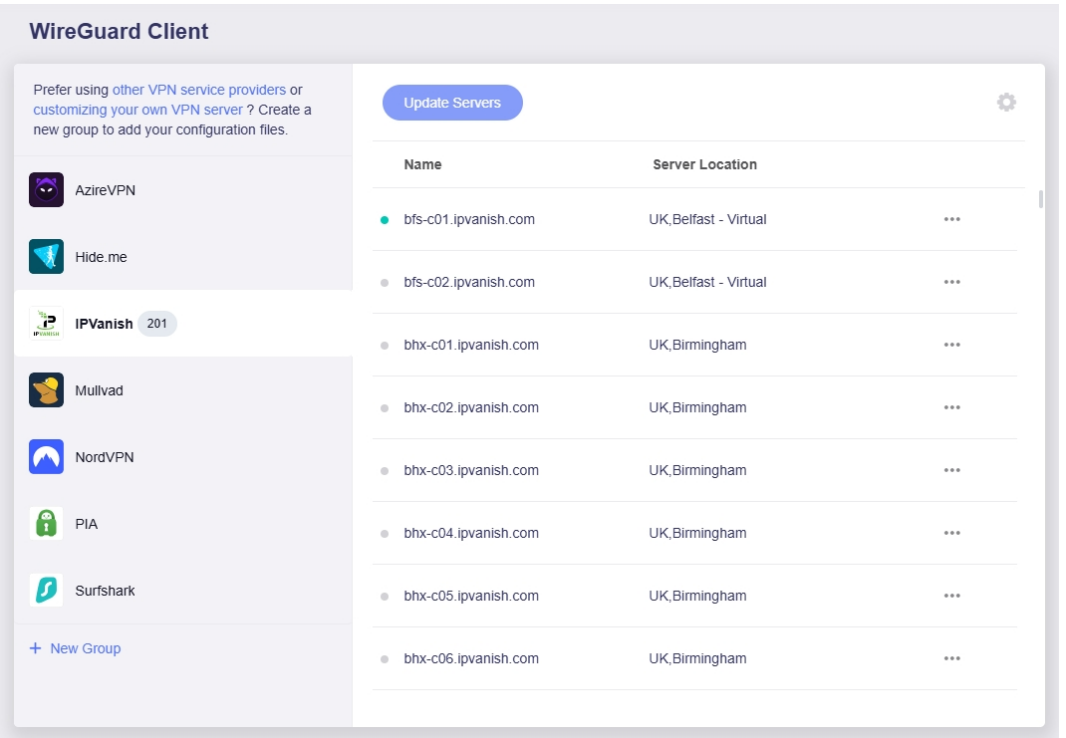
3. Wybierz serwery, z którymi chcesz się połączyć, i kliknij **Apply**.



4. Wybierz preferowany serwer i kliknij ikonę trzech kropek po prawej stronie, aby nawiązać połączenie.



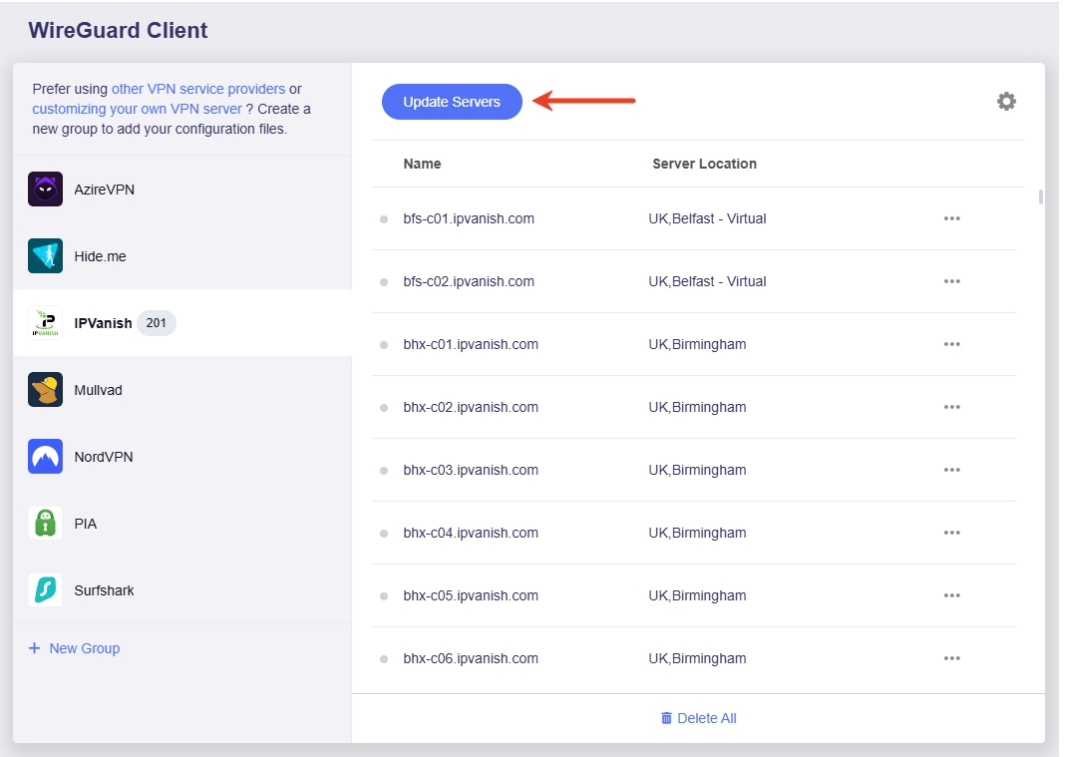
5. Po połączeniu obok pliku konfiguracyjnego pojawi się zielona kropka.



Szczegóły połączenia VPN możesz również sprawdzić w **VPN Dashboard**.

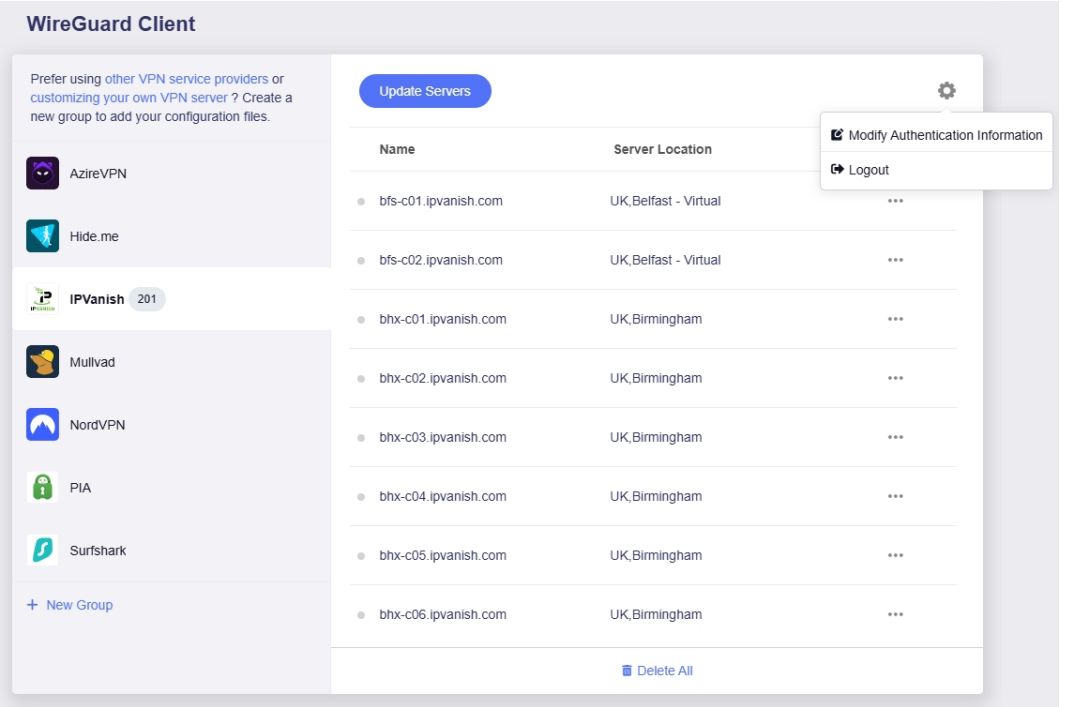
6. Zaktualizuj serwery.

   Możesz kliknąć **Update Servers**, aby pobrać aktualną listę dostępnych serwerów i uniknąć problemów z połączeniem spowodowanych konserwacją lub wyłączeniem serwerów.



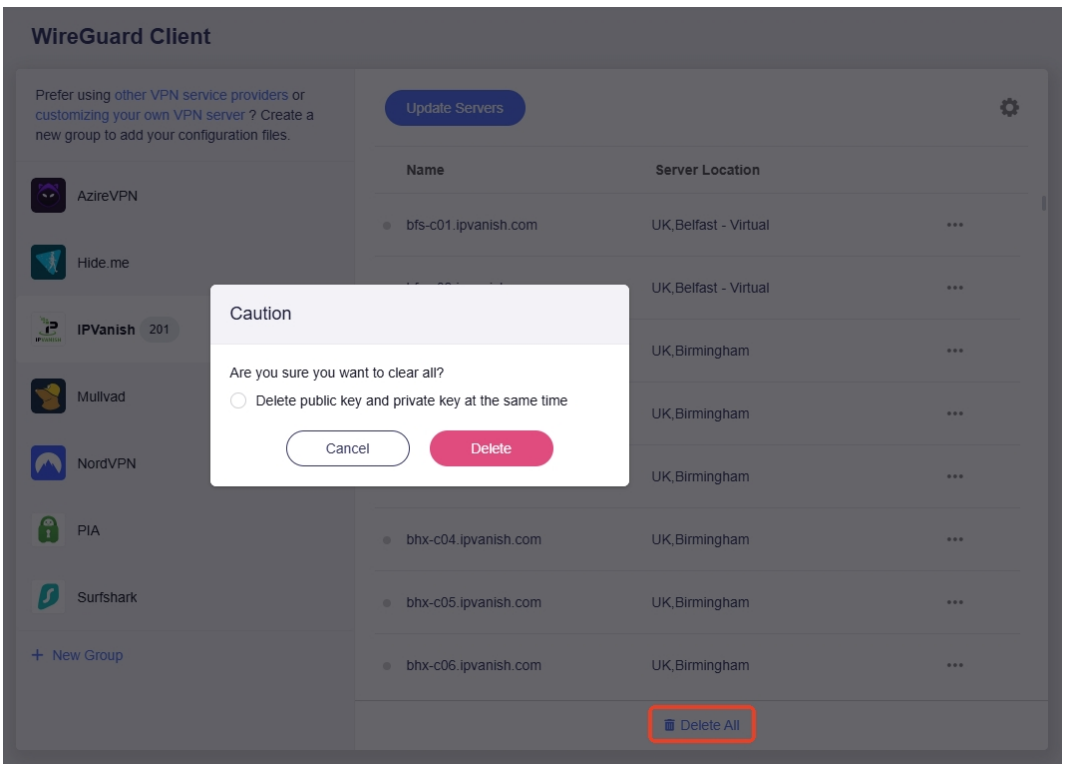
7. Zmiana danych logowania lub wylogowanie.

   Kliknij ikonę koła zębatego, aby zmienić dane logowania lub się wylogować.



8. Usuń wszystkie pliki.

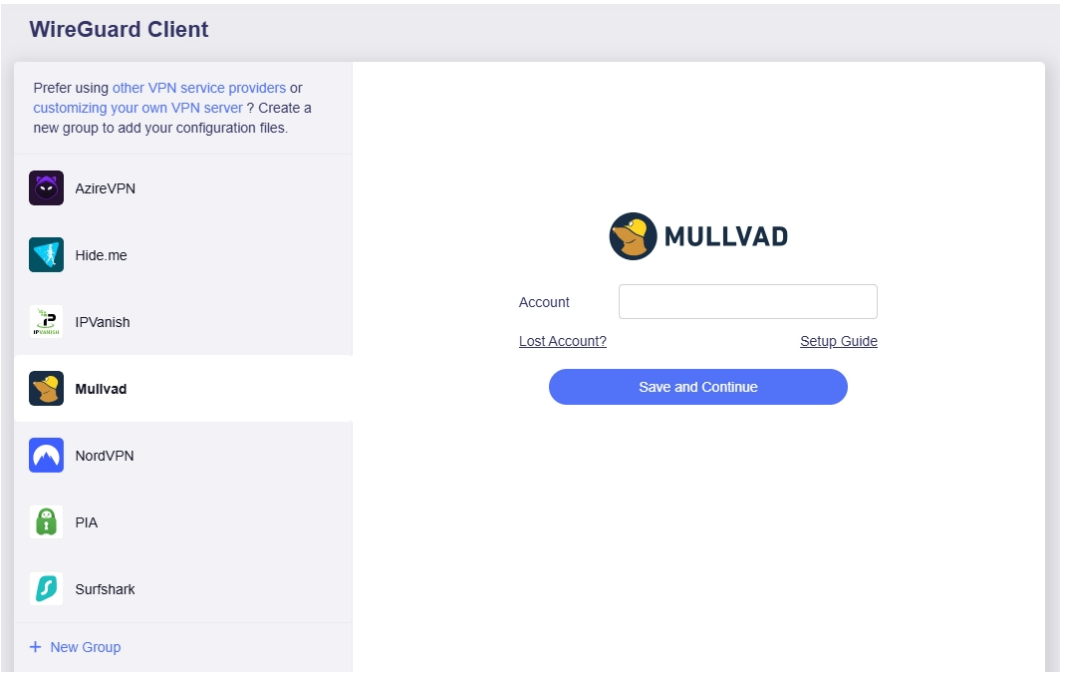
   Możesz kliknąć **Delete All**, aby jednym kliknięciem usunąć wszystkie pliki konfiguracyjne, oraz wybrać, czy jednocześnie usunąć klucze prywatny i publiczny.



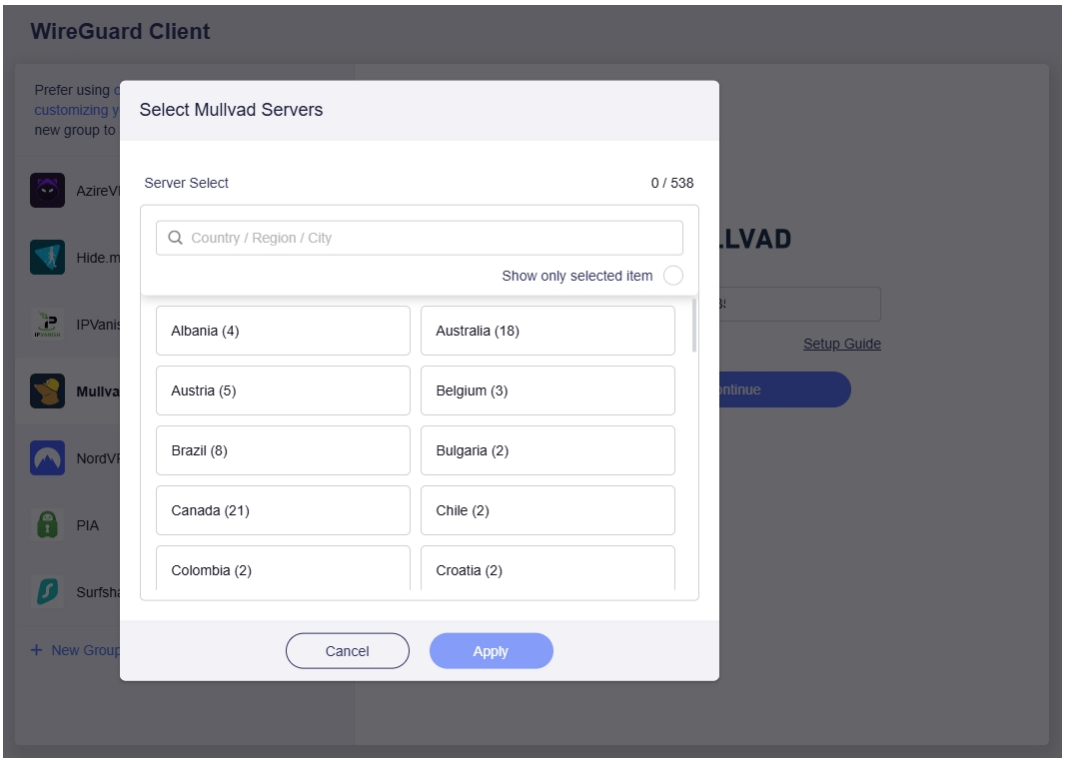
11.2.5 Konfiguracja Mullvad

Aby skonfigurować router jako klienta Mullvad, wykonaj poniższe czynności.

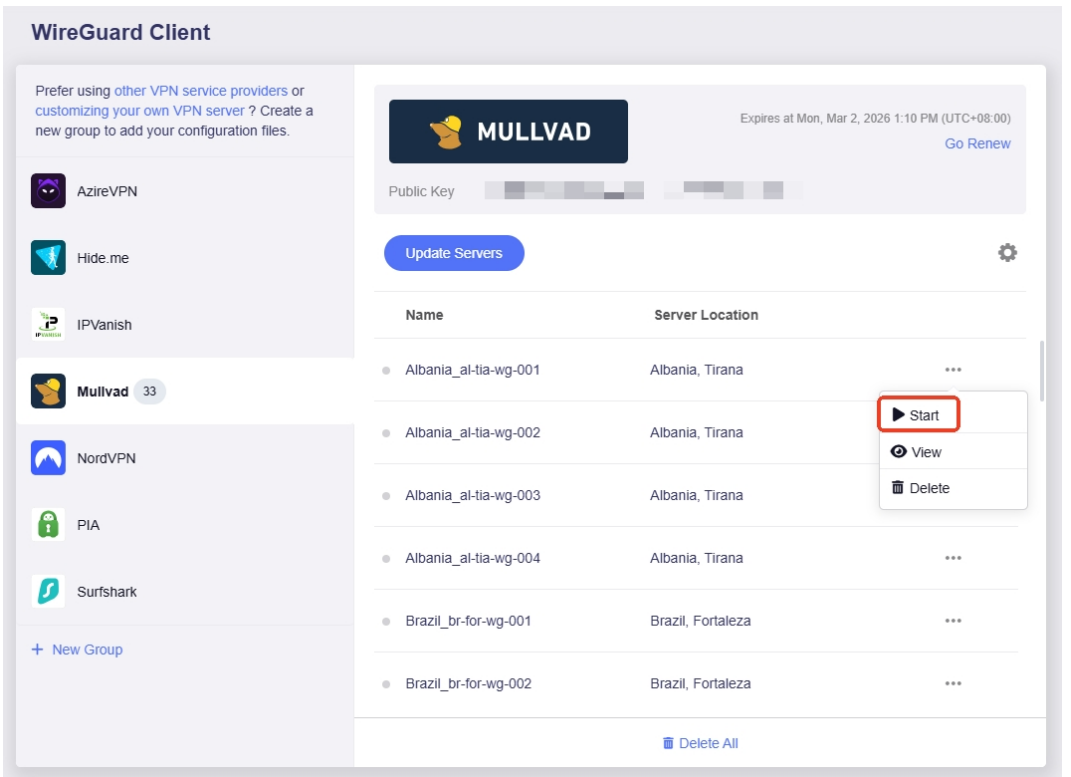
1. Zaloguj się do panelu administracyjnego routera i przejdź do **VPN** > **WireGuard Client** > **Mullvad**.
2. Wprowadź nazwę użytkownika i hasło, a następnie kliknij **Save and Continue**.



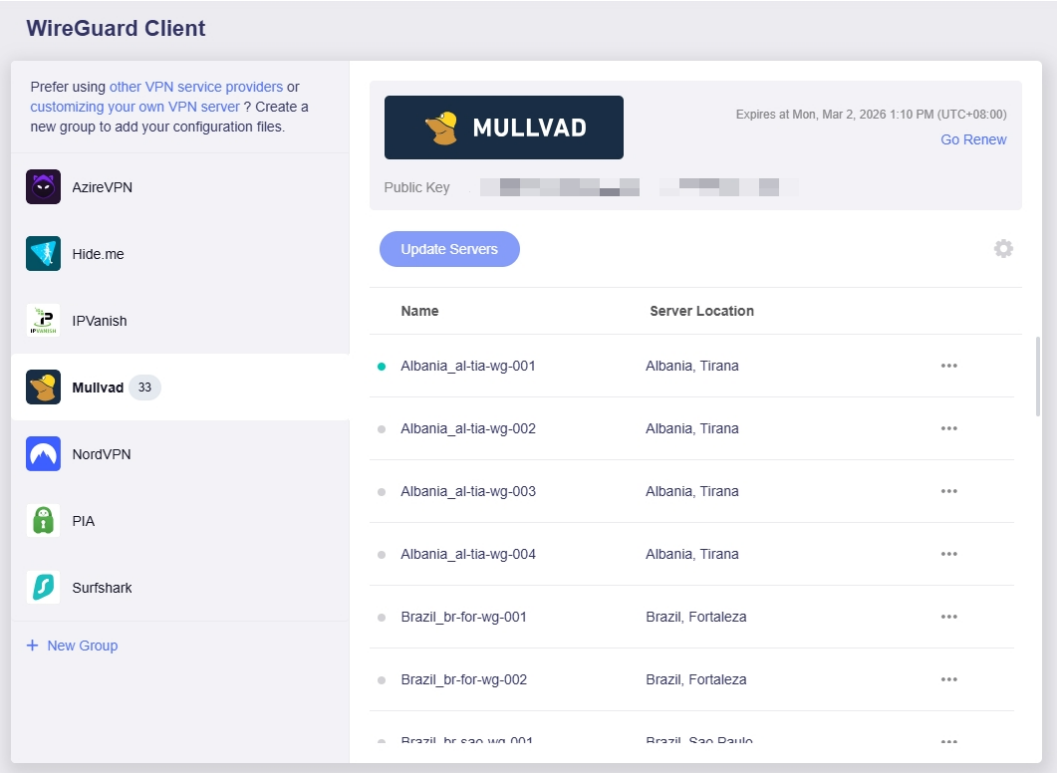
3. Wybierz serwery, z którymi chcesz się połączyć, i kliknij **Apply**.



4. Wybierz preferowany serwer i kliknij ikonę trzech kropek po prawej stronie, aby nawiązać połączenie.



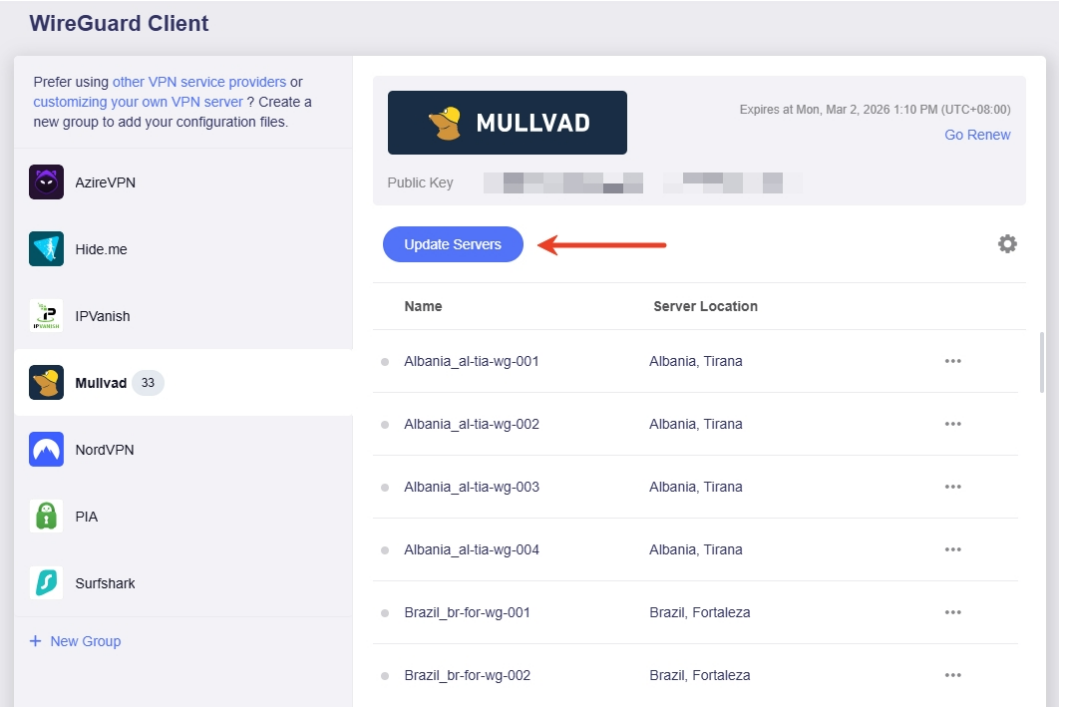
5. Po połączeniu obok pliku konfiguracyjnego pojawi się zielona kropka.



Szczegóły połączenia VPN możesz również sprawdzić w **VPN Dashboard**.

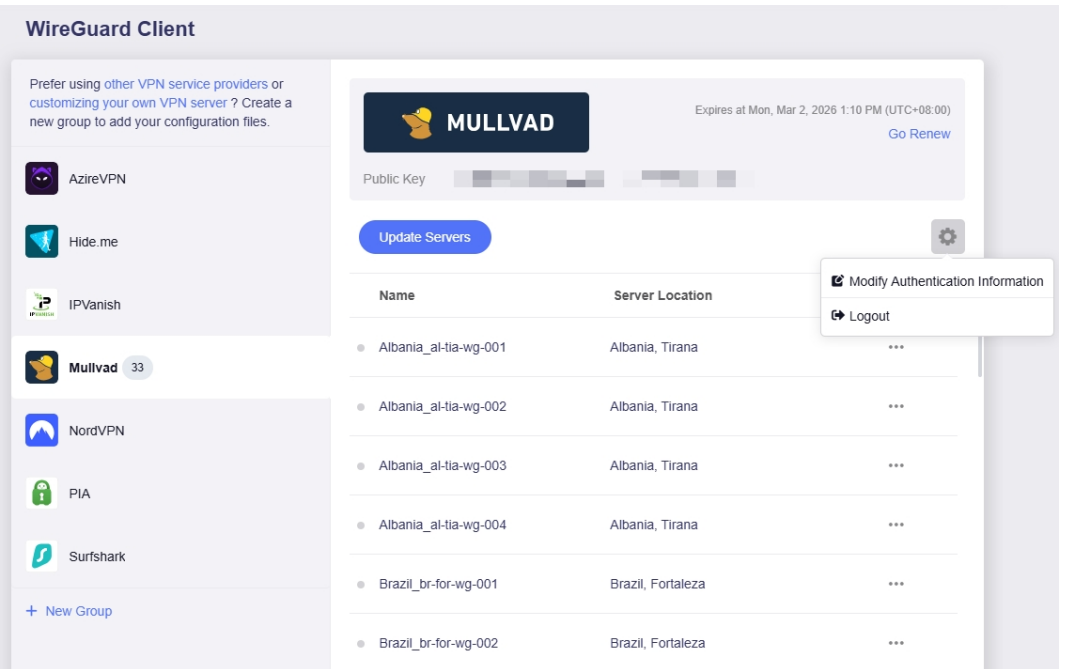
6. Zaktualizuj serwery.

   Możesz kliknąć **Update Servers**, aby pobrać aktualną listę dostępnych serwerów i uniknąć problemów z połączeniem spowodowanych konserwacją lub wyłączeniem serwerów.



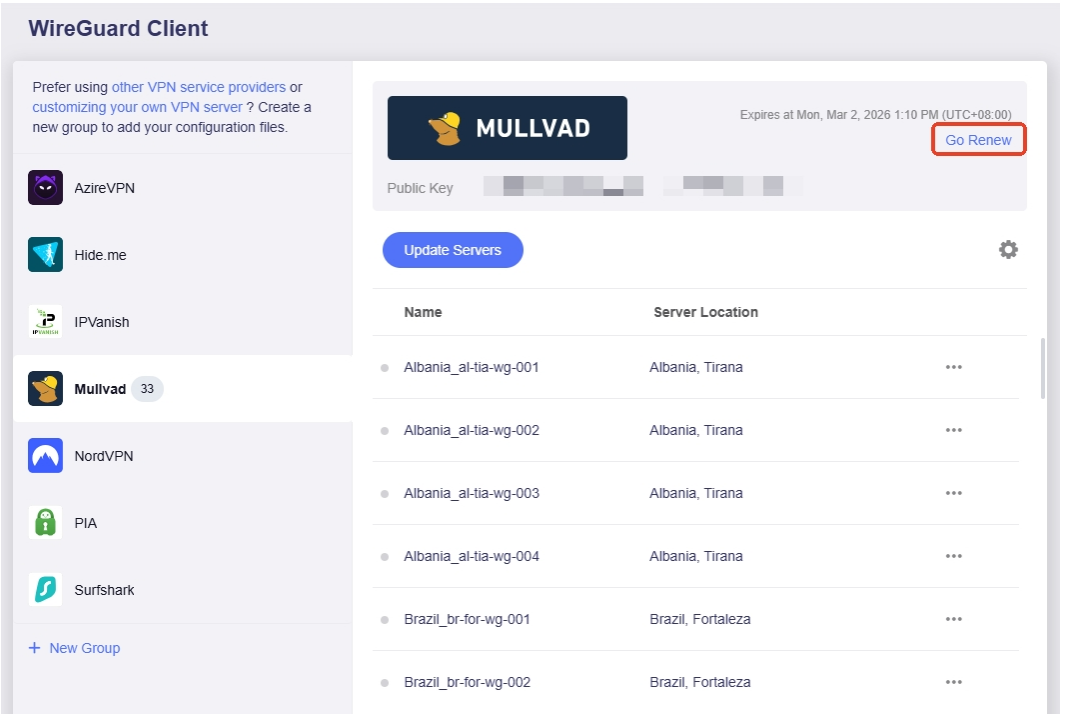
7. Zmiana danych logowania lub wylogowanie.

   Kliknij ikonę koła zębatego, aby zmienić dane logowania lub się wylogować.



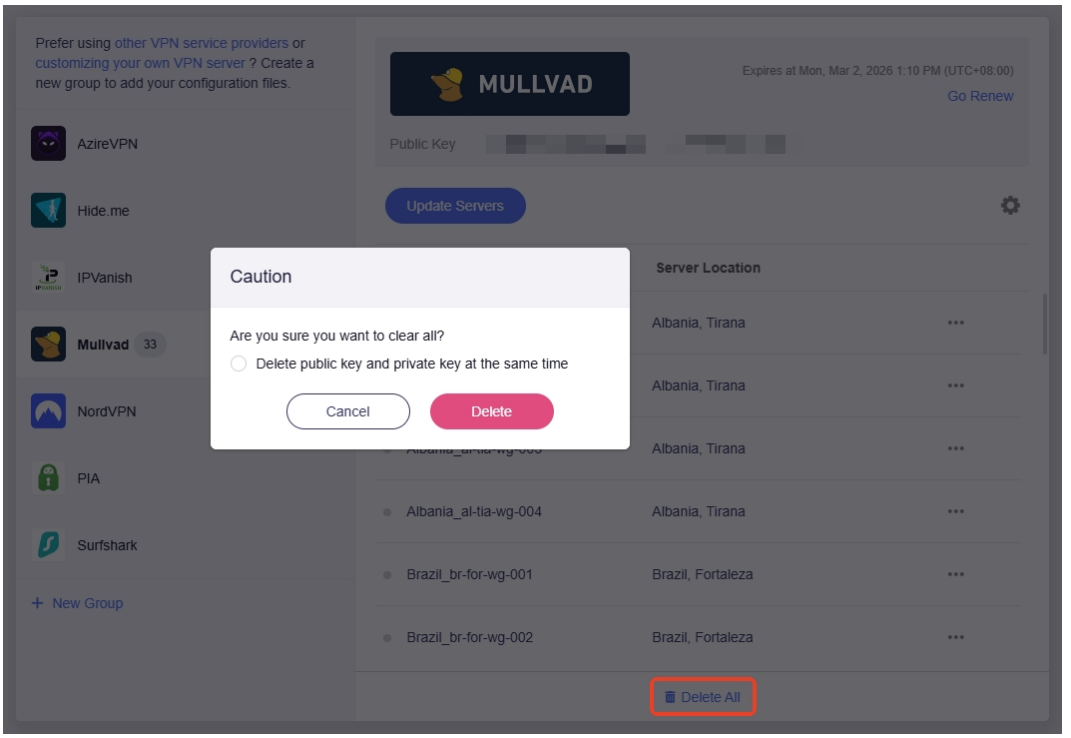
8. Odnowienie subskrypcji.

   Po kliknięciu **Go Renew** nastąpi przekierowanie na oficjalną stronę w celu odnowienia subskrypcji.



9. Usuń wszystkie pliki.

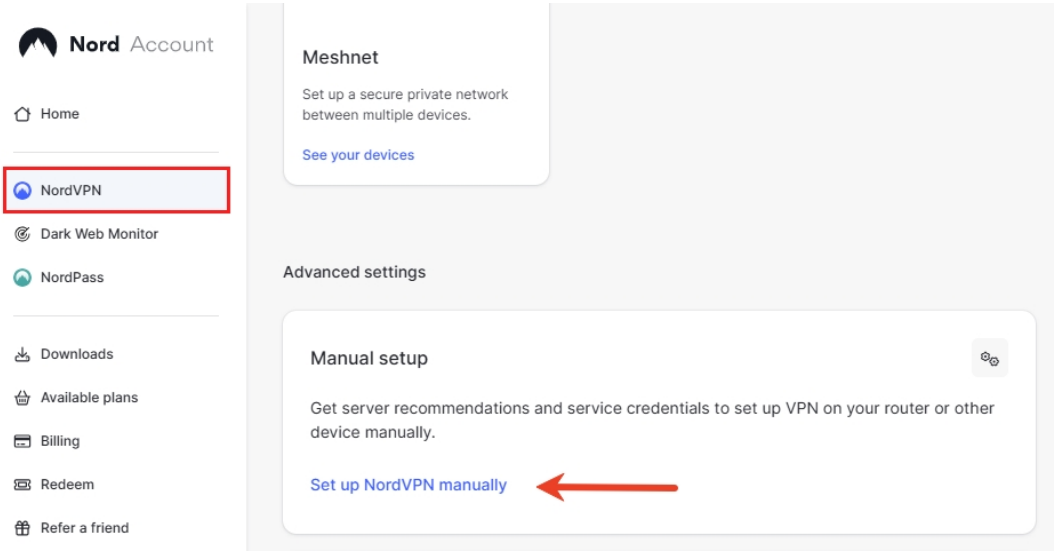
   Możesz kliknąć **Delete All**, aby jednym kliknięciem usunąć wszystkie pliki konfiguracyjne, oraz wybrać, czy jednocześnie usunąć klucze prywatny i publiczny.



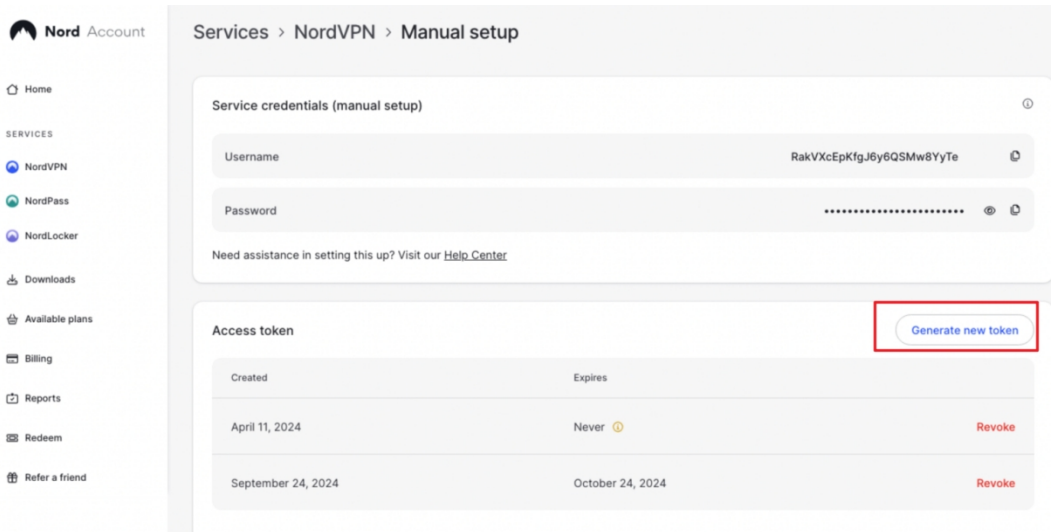
11.2.6 Konfiguracja NordVPN

Aby skonfigurować router jako klienta NordVPN, wykonaj poniższe czynności.

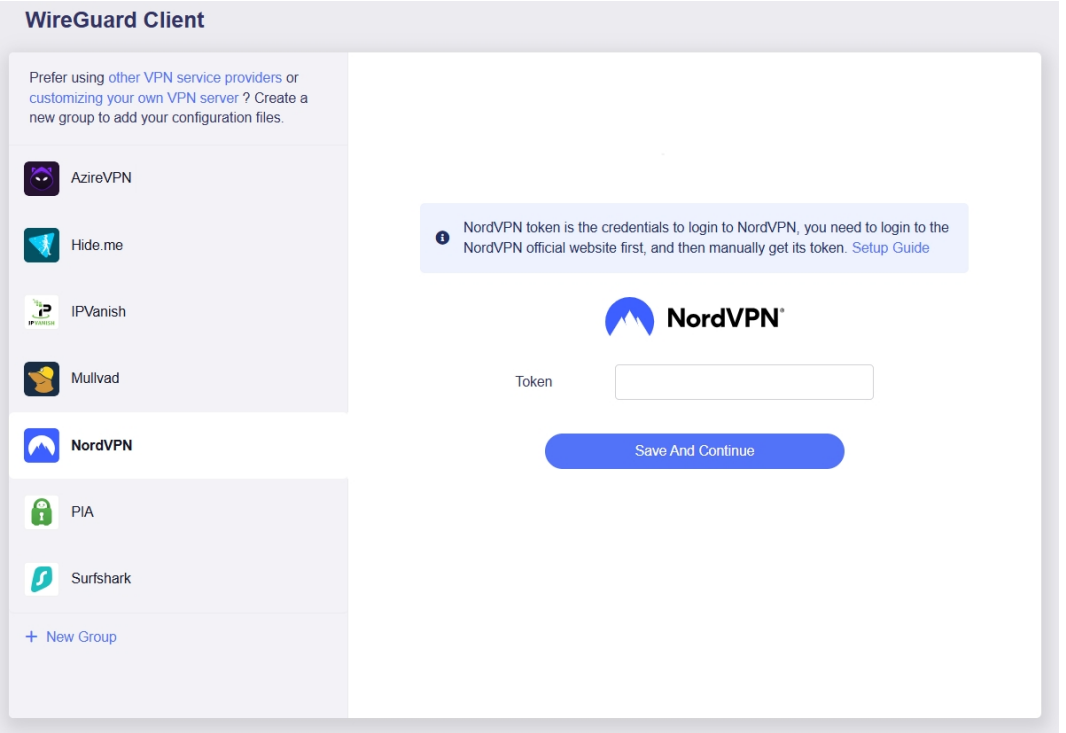
1. Zaloguj się na swoje konto internetowe NordVPN tutaj.
2. W panelu Nord kliknij **NordVPN**, a następnie **Set up NordVPN manually**.



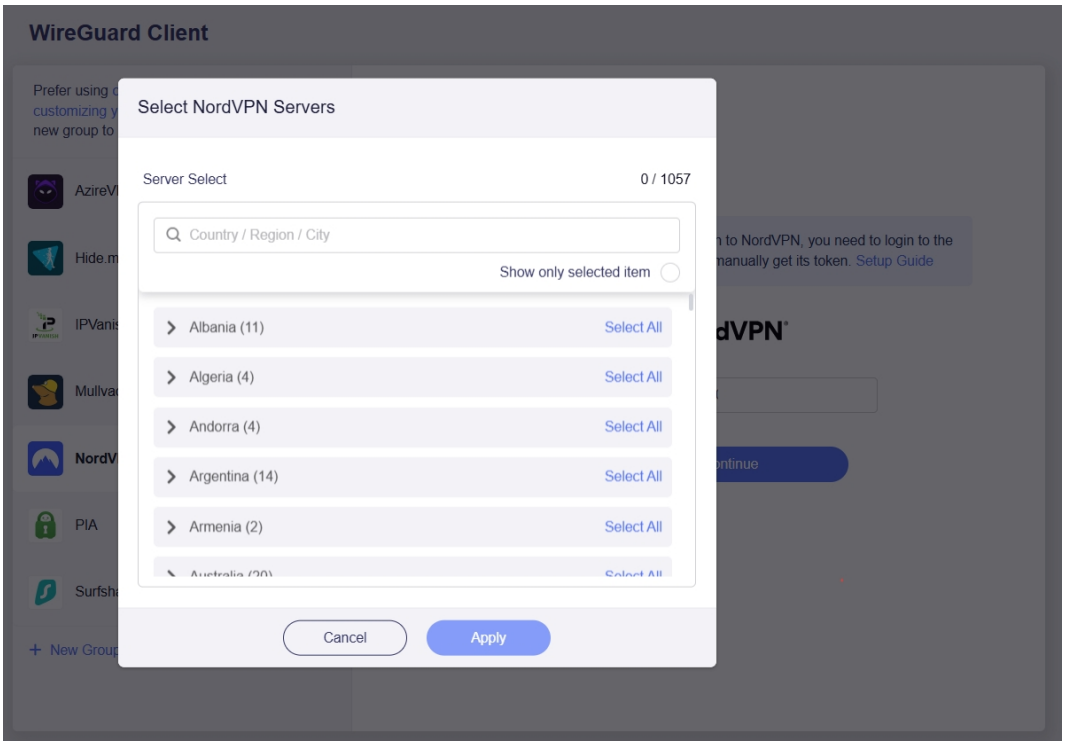
Znajdziesz tam **Access Token**. Utwórz token dostępu i skopiuj go do późniejszego użycia.



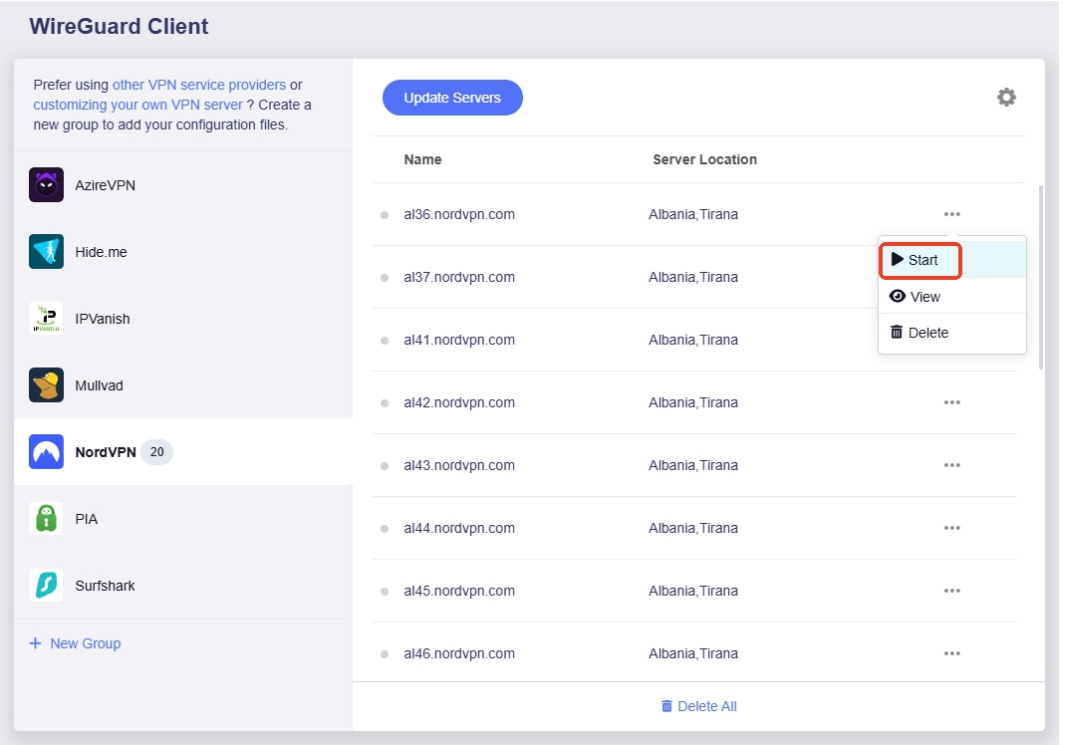
3. Zaloguj się do panelu administracyjnego routera i przejdź do **VPN** > **WireGuard Client** > **NordVPN**.
4. Wprowadź token i kliknij **Save and Continue**.



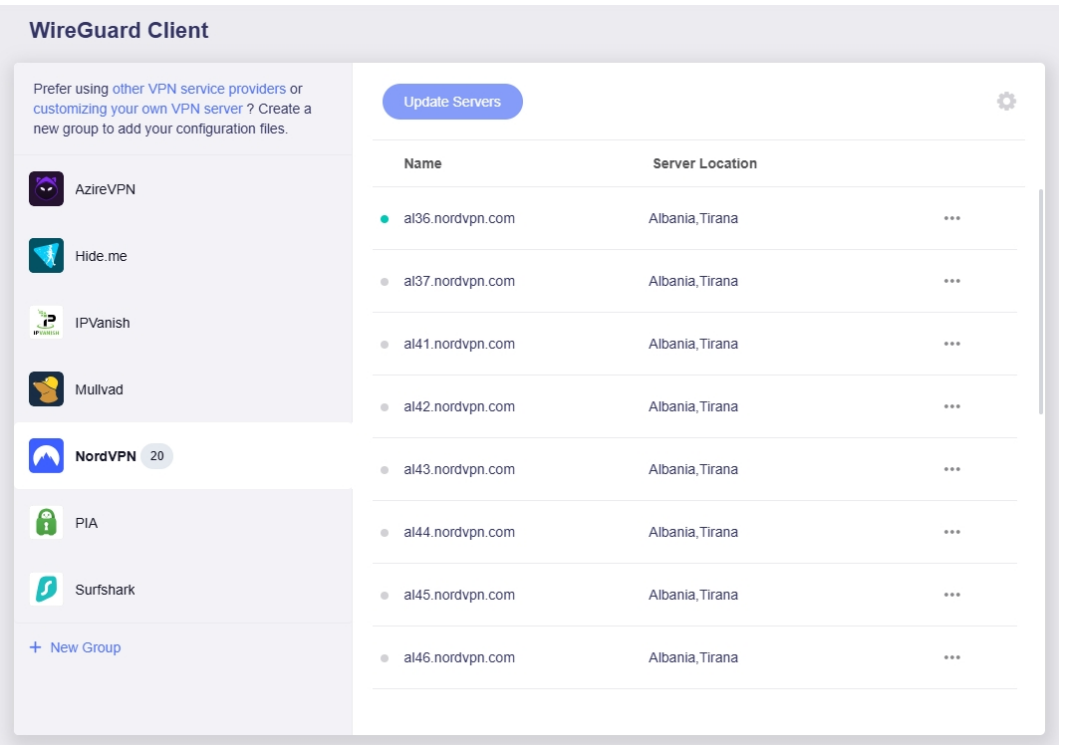
5. Wybierz serwery, z którymi chcesz się połączyć, i kliknij **Apply**.



6. Wybierz preferowany serwer i kliknij ikonę trzech kropek po prawej stronie, aby nawiązać połączenie.



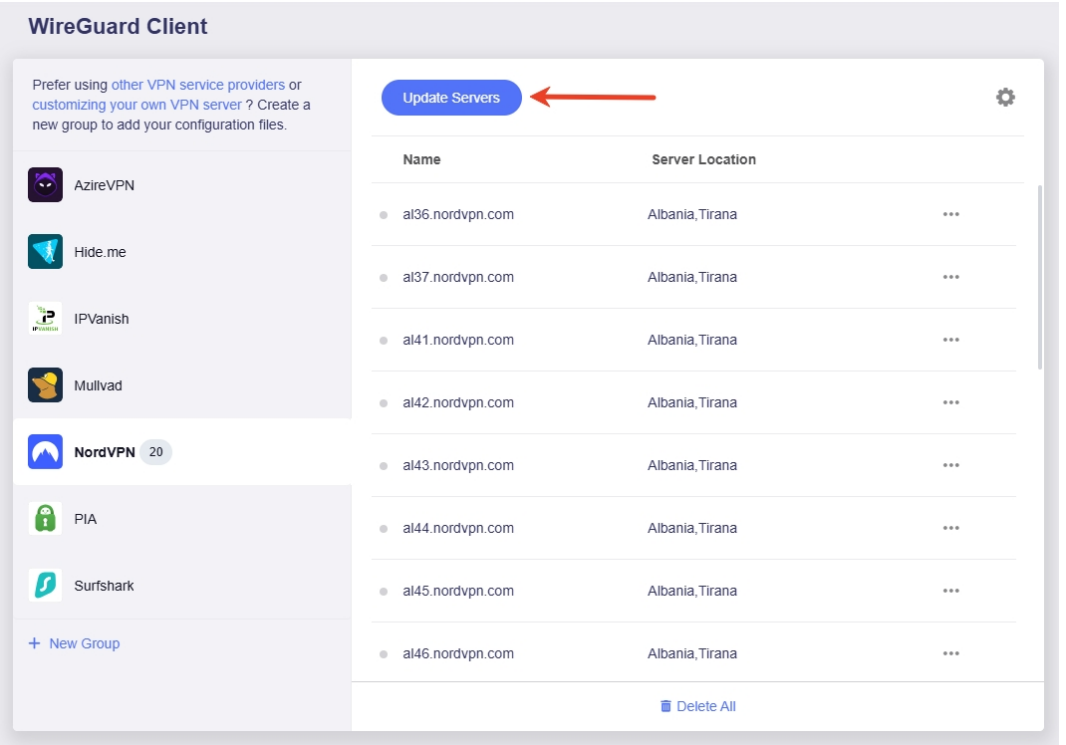
7. Po połączeniu obok pliku konfiguracyjnego pojawi się zielona kropka.



Szczegóły połączenia VPN możesz również sprawdzić w **VPN Dashboard**.

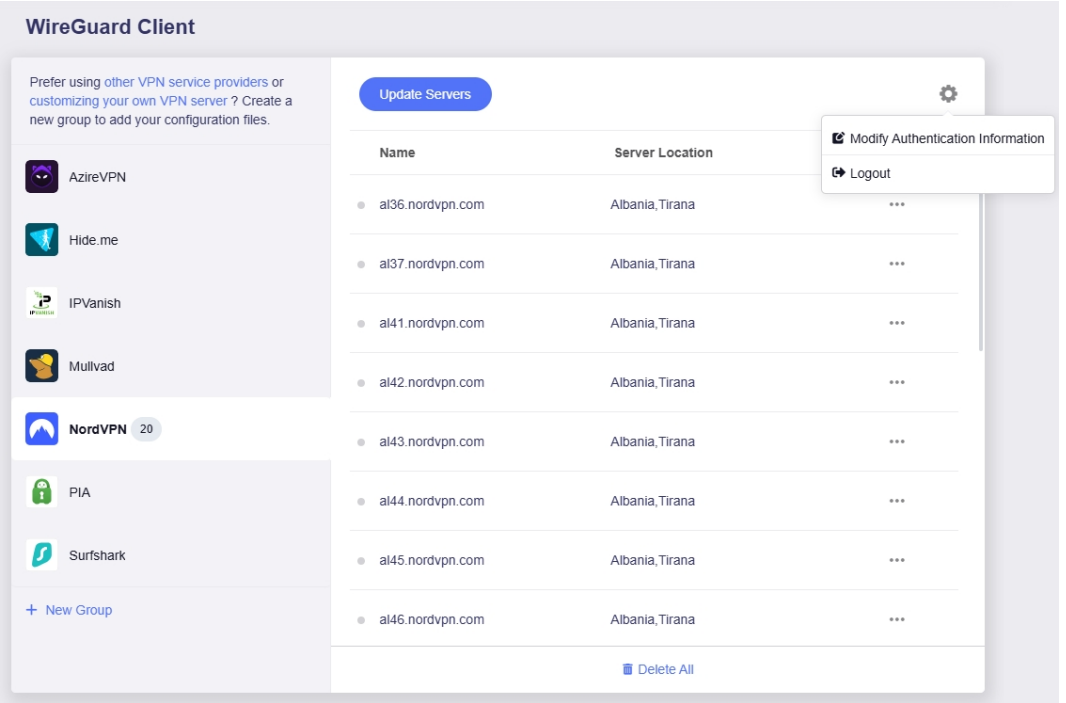
8. Zaktualizuj serwery.

   Możesz kliknąć **Update Servers**, aby pobrać aktualną listę dostępnych serwerów i uniknąć problemów z połączeniem spowodowanych konserwacją lub wyłączeniem serwerów.



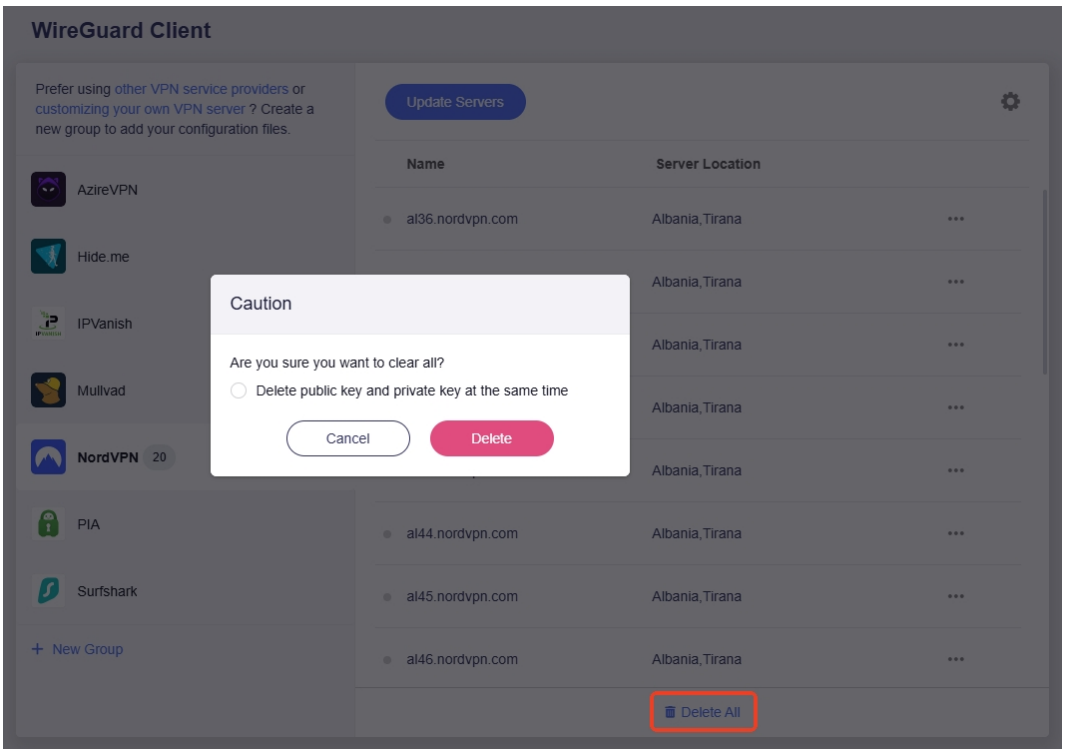
9. Zmiana danych logowania lub wylogowanie.

   Kliknij ikonę koła zębatego, aby zmienić dane logowania lub się wylogować.



10. Usuń wszystkie pliki.

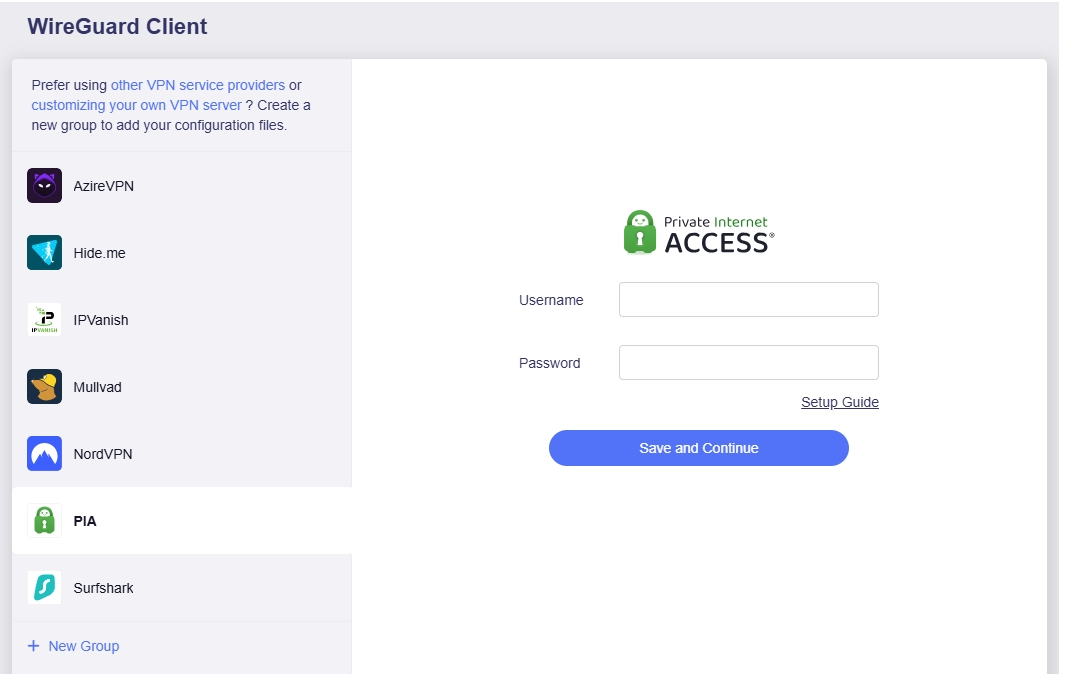
    Możesz kliknąć **Delete All**, aby jednym kliknięciem usunąć wszystkie pliki konfiguracyjne, oraz wybrać, czy jednocześnie usunąć klucze prywatny i publiczny.



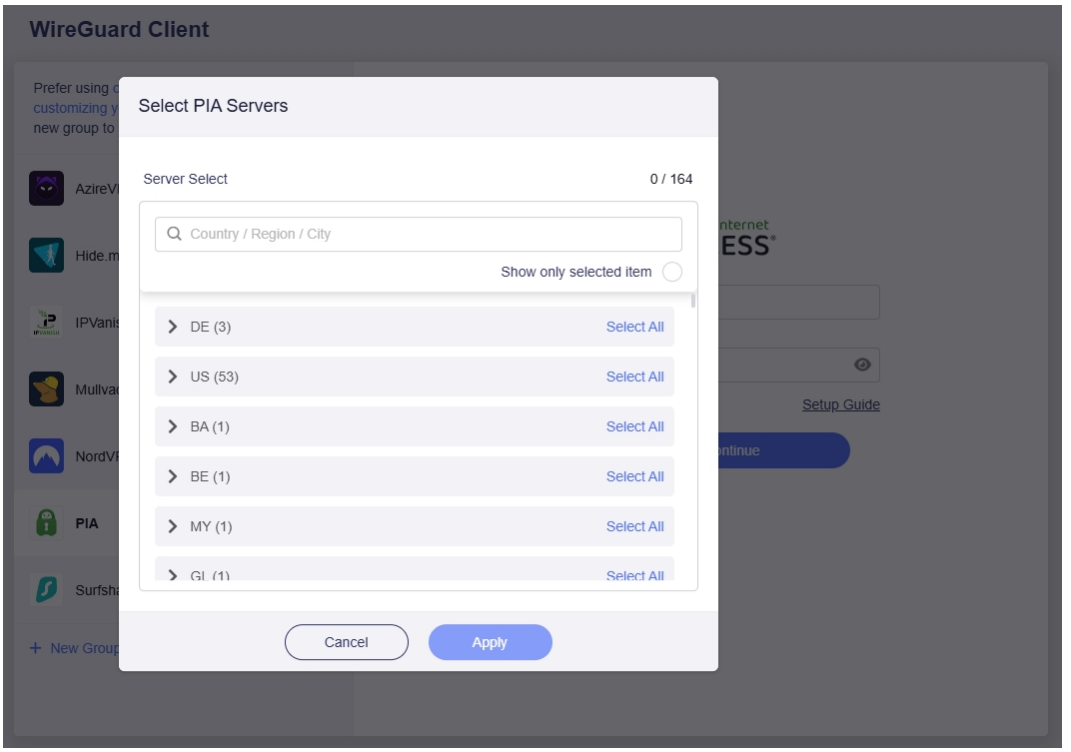
11.2.7 Konfiguracja PIA (Private Internet Access)

Aby skonfigurować router jako klienta PIA, wykonaj poniższe czynności.

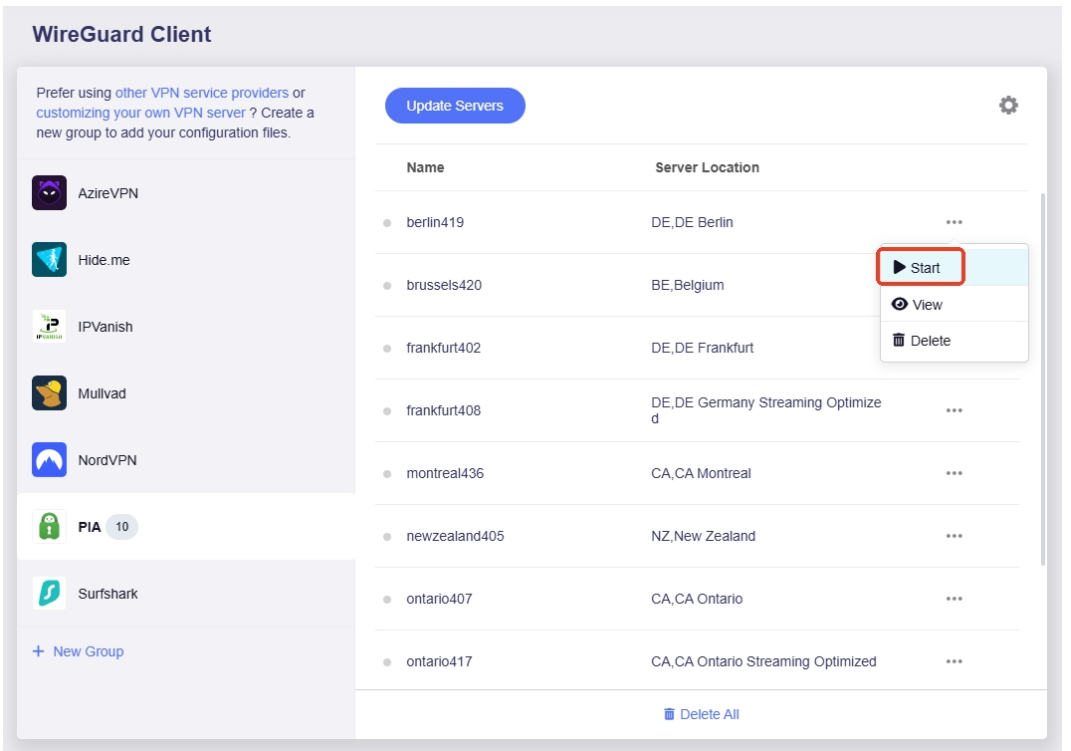
1. Zaloguj się do panelu administracyjnego routera i przejdź do **VPN** > **WireGuard Client** > **PIA**.
2. Wprowadź nazwę użytkownika i hasło, a następnie kliknij **Save and Continue**.



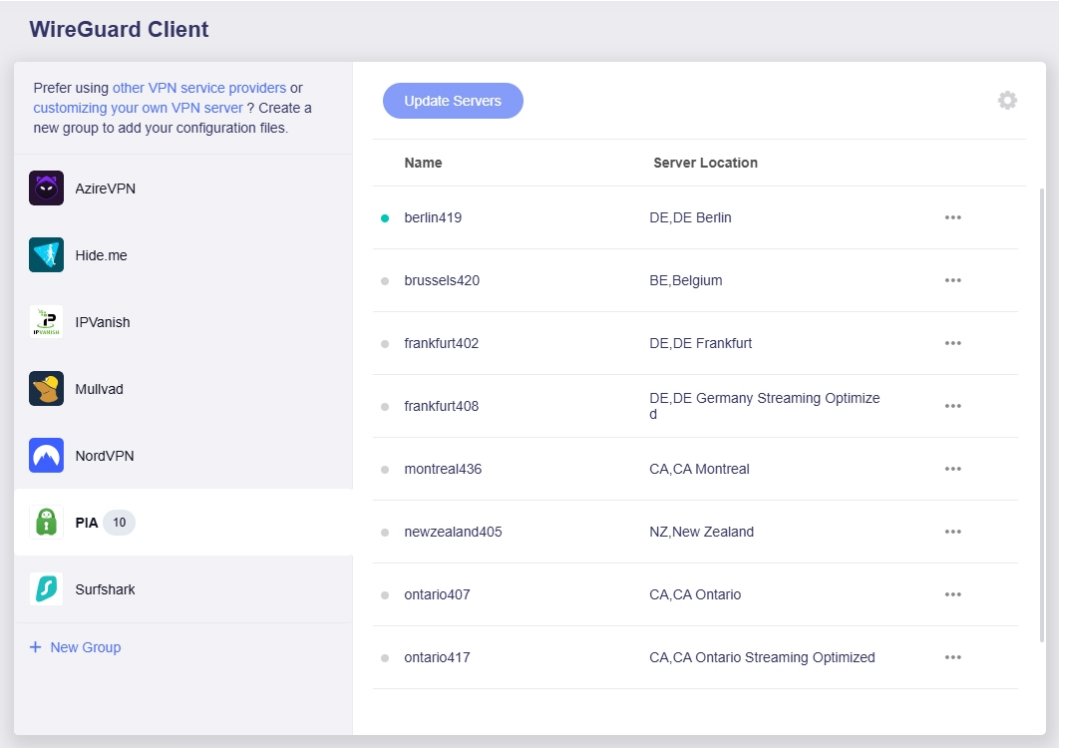
3. Wybierz serwery, z którymi chcesz się połączyć, i kliknij **Apply**.



4. Wybierz preferowany serwer i kliknij ikonę trzech kropek po prawej stronie, aby nawiązać połączenie.



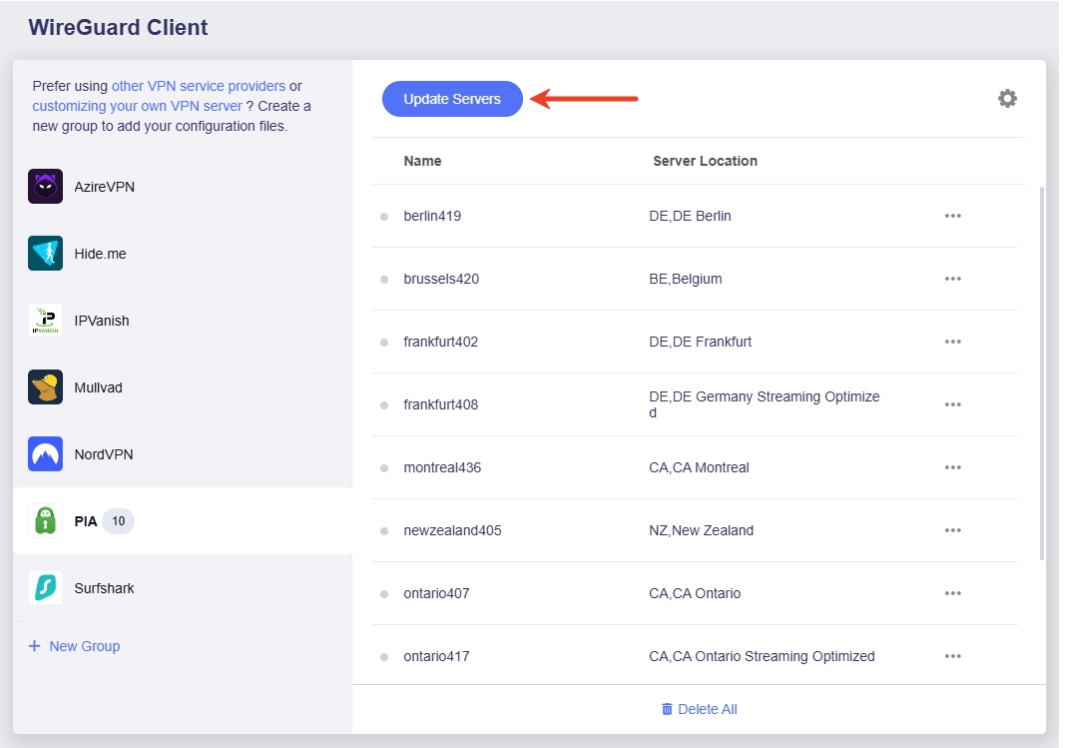
5. Po połączeniu obok pliku konfiguracyjnego pojawi się zielona kropka.



Szczegóły połączenia VPN możesz również sprawdzić w **VPN Dashboard**.

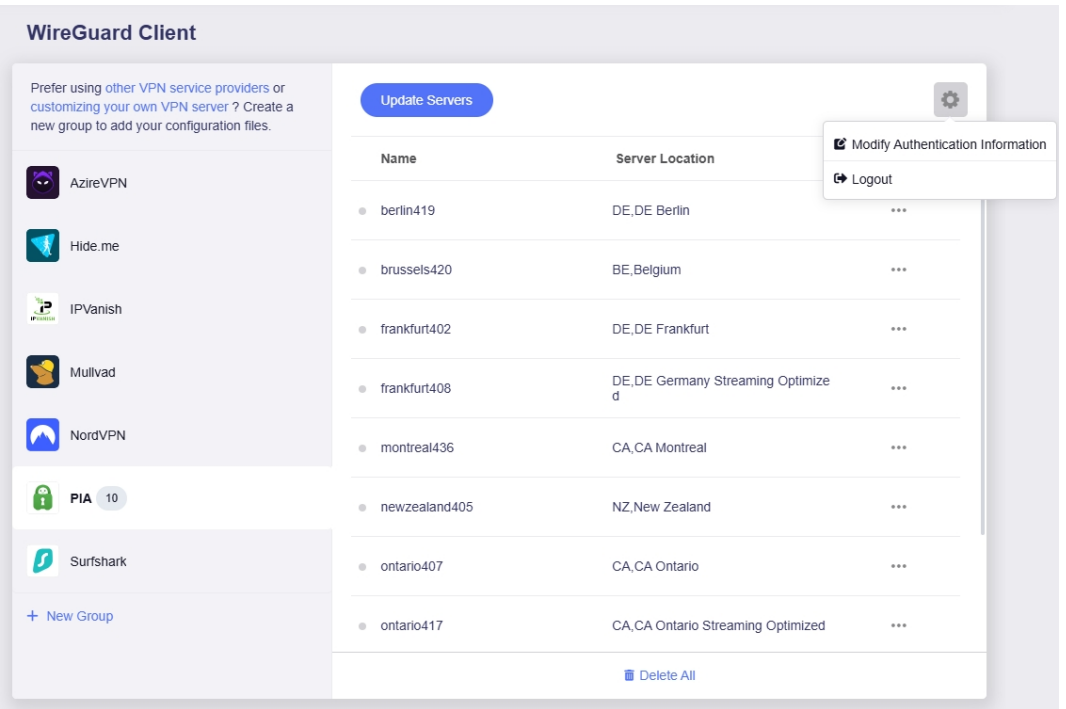
6. Zaktualizuj serwery.

   Możesz kliknąć **Update Servers**, aby pobrać aktualną listę dostępnych serwerów i uniknąć problemów z połączeniem spowodowanych konserwacją lub wyłączeniem serwerów.



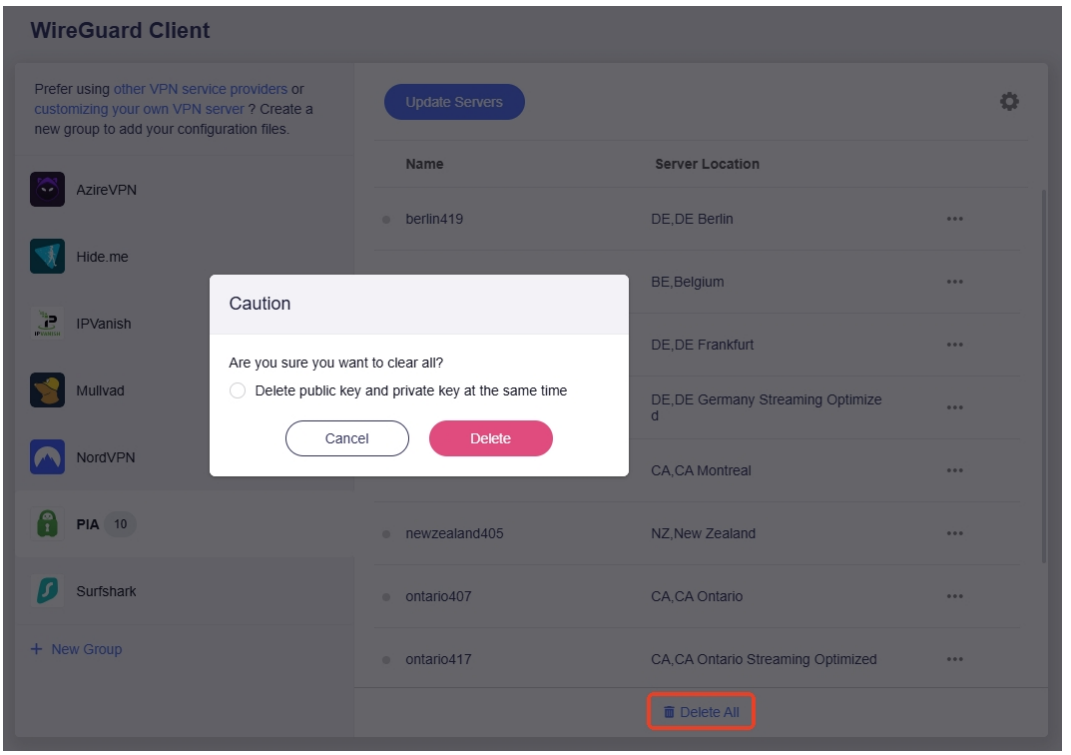
7. Zmiana danych logowania lub wylogowanie.

   Kliknij ikonę koła zębatego, aby zmienić dane logowania lub się wylogować.



8. Usuń wszystkie pliki.

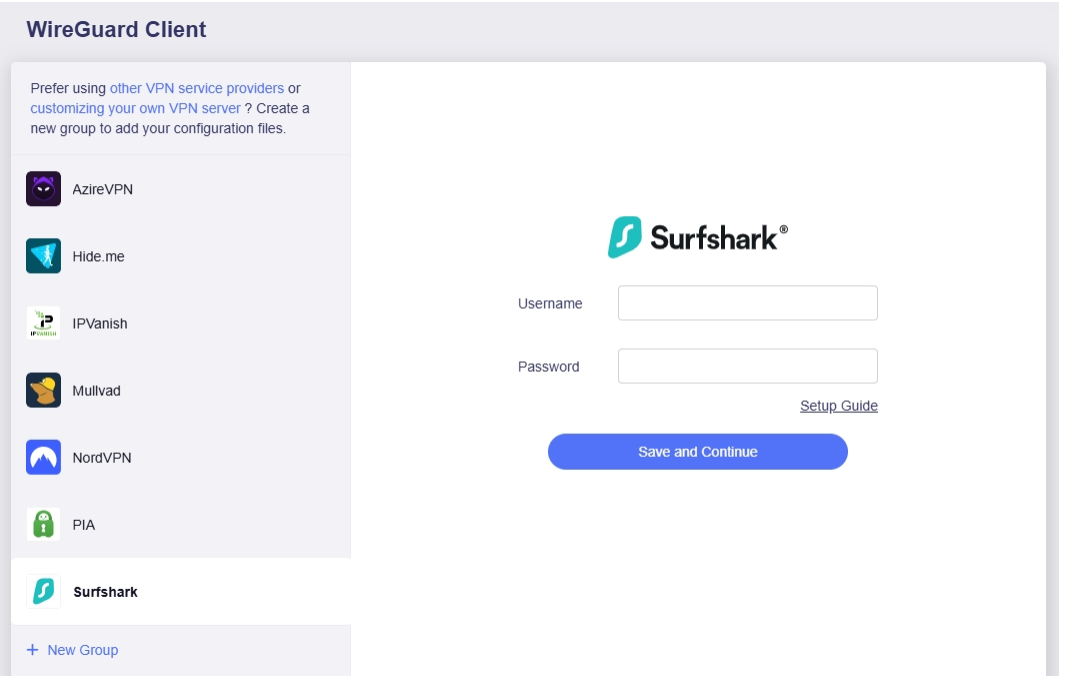
   Możesz kliknąć **Delete All**, aby jednym kliknięciem usunąć wszystkie pliki konfiguracyjne, oraz wybrać, czy jednocześnie usunąć klucze prywatny i publiczny.



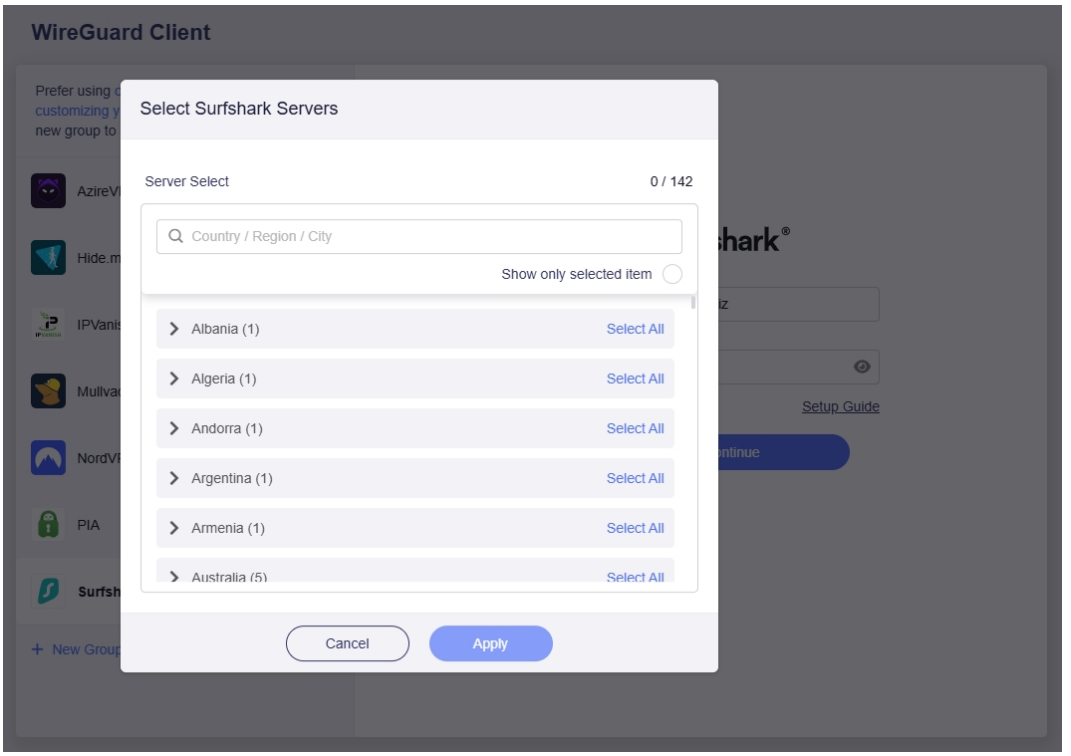
11.2.8 Konfiguracja Surfshark

Aby skonfigurować router jako klienta Surfshark, wykonaj poniższe czynności.

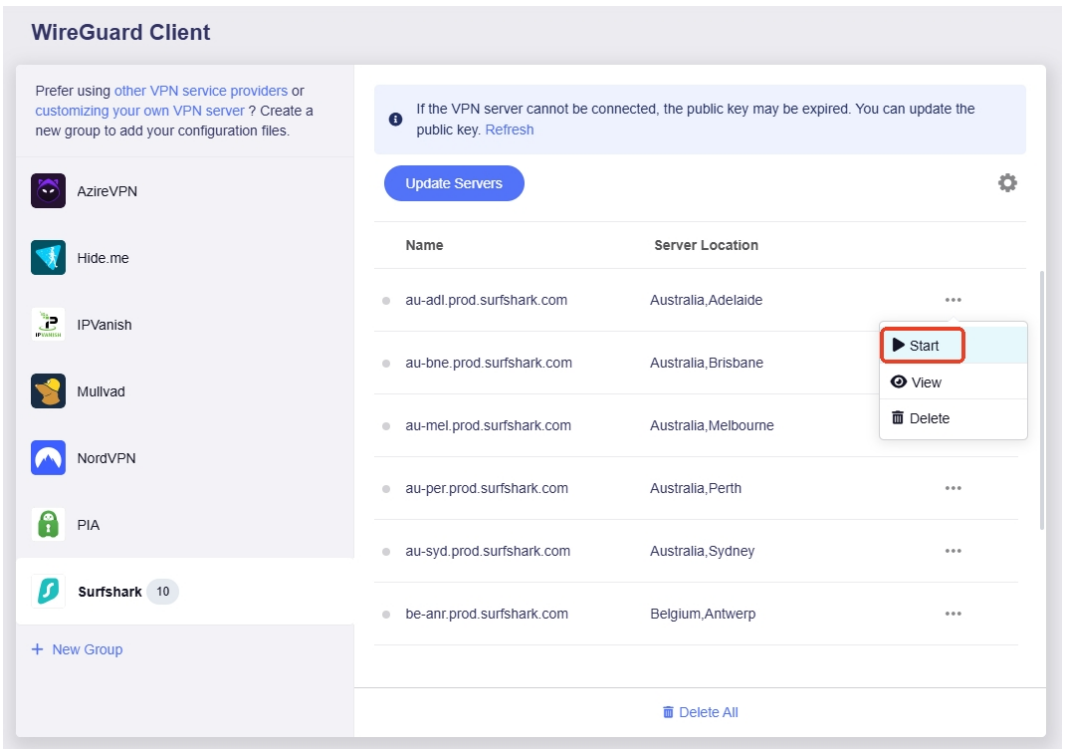
1. Zaloguj się do panelu administracyjnego routera i przejdź do **VPN** > **WireGuard Client** > **Surfshark**.
2. Wprowadź nazwę użytkownika i hasło, a następnie kliknij **Save and Continue**.



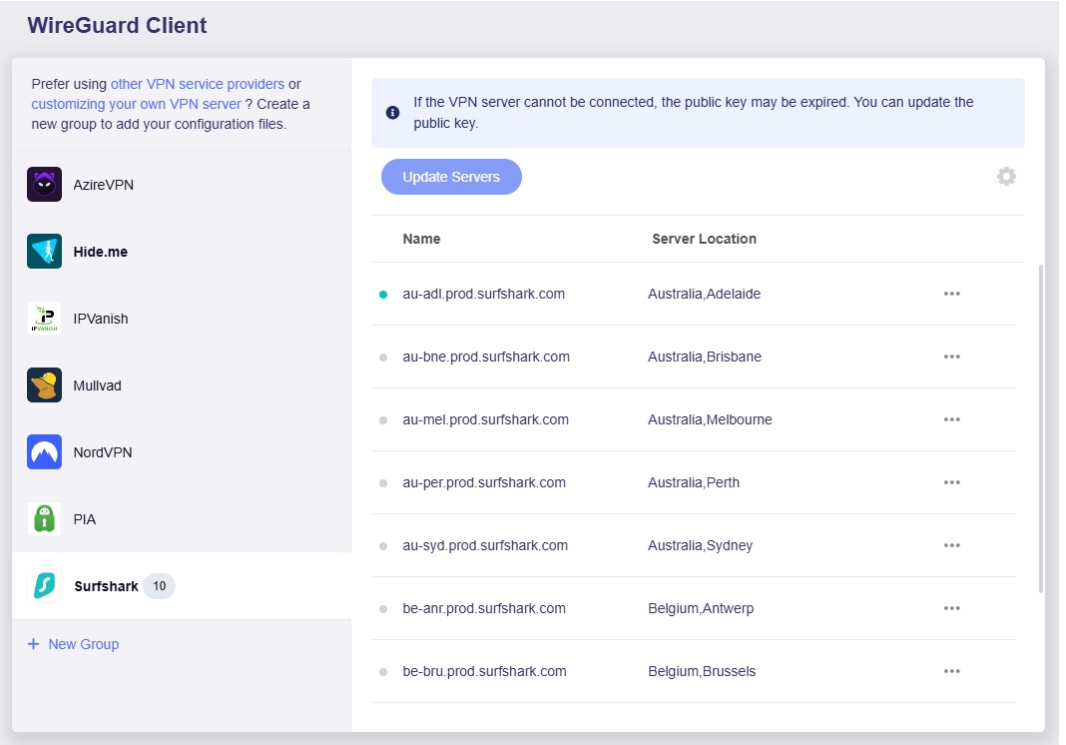
3. Wybierz serwery, z którymi chcesz się połączyć, i kliknij **Apply**.



4. Wybierz preferowany serwer i kliknij ikonę trzech kropek po prawej stronie, aby nawiązać połączenie.

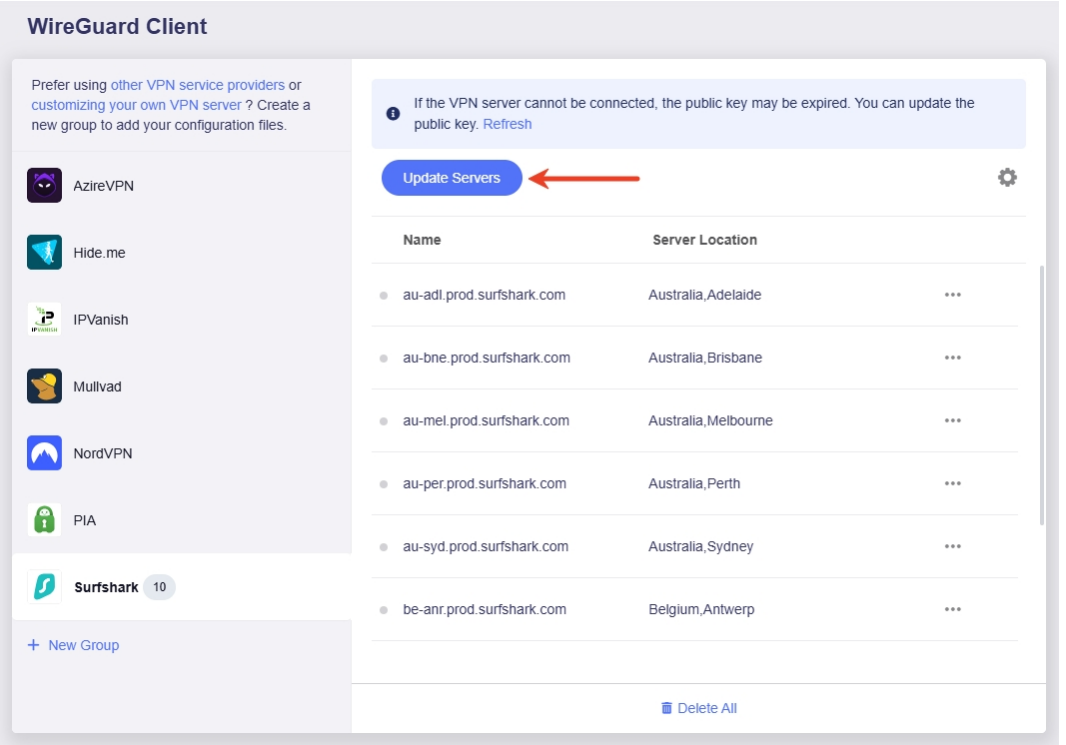


5. Po połączeniu obok pliku konfiguracyjnego pojawi się zielona kropka.



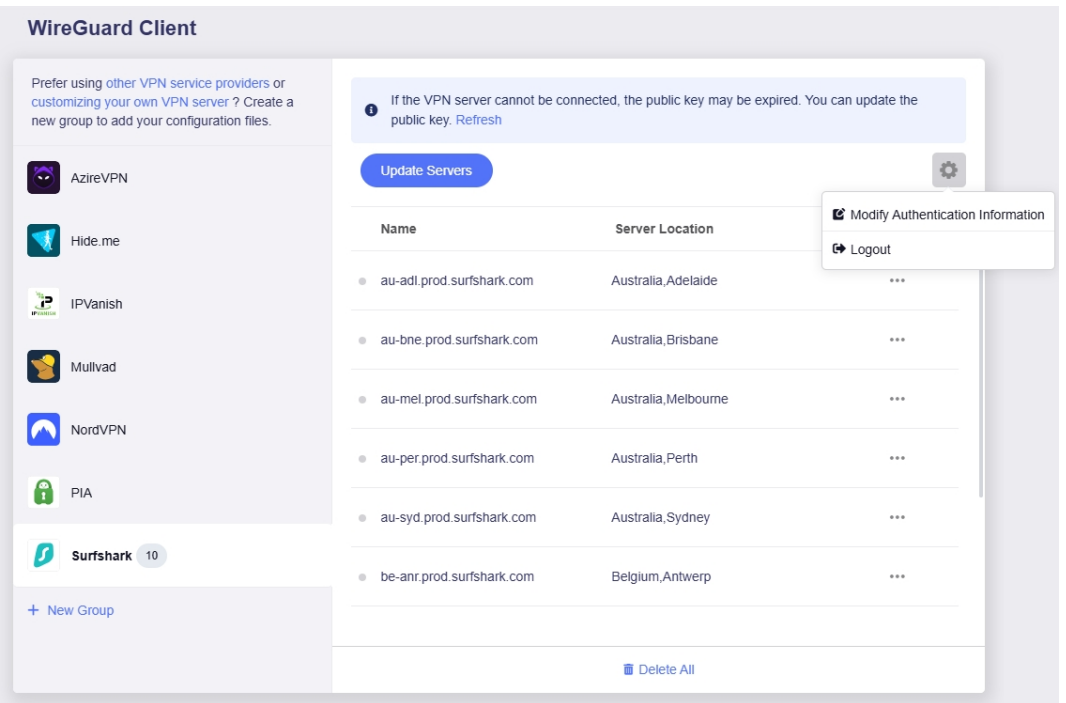
Szczegóły połączenia VPN możesz również sprawdzić w **VPN Dashboard**.

6. Zaktualizuj serwery.
   Możesz kliknąć **Update Servers**, aby pobrać aktualną listę dostępnych serwerów i uniknąć problemów z połączeniem spowodowanych konserwacją lub wyłączeniem serwerów.



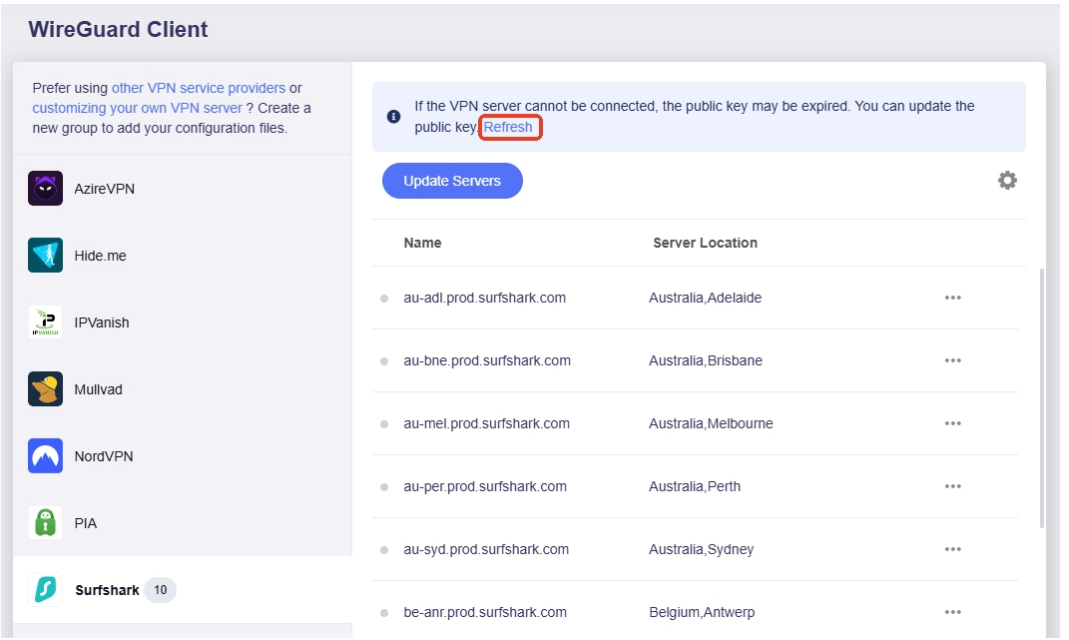
7. Zmiana danych logowania lub wylogowanie.

   Kliknij ikonę koła zębatego, aby zmienić dane logowania lub się wylogować.



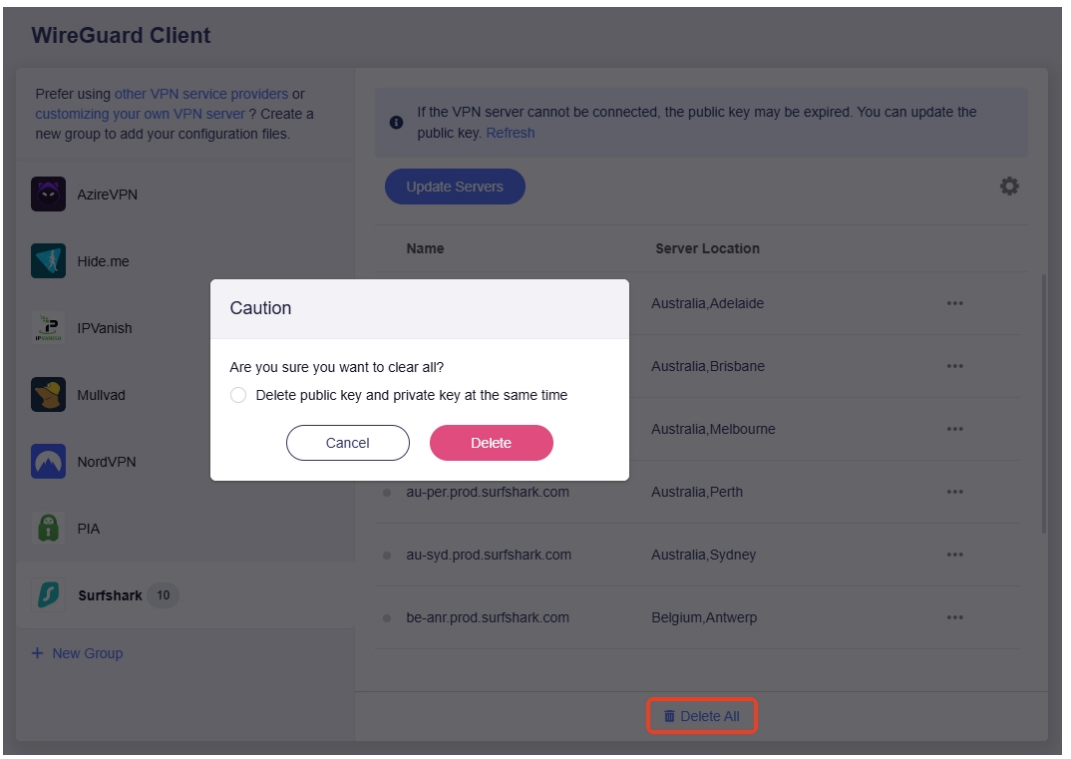
8. Odświeżanie.

   Możesz kliknąć **Refresh**, aby zaktualizować klucz publiczny, gdy nie można połączyć się z serwerem VPN.



9. Usuń wszystkie pliki.

   Możesz kliknąć **Delete All**, aby jednym kliknięciem usunąć wszystkie pliki konfiguracyjne, oraz wybrać, czy jednocześnie usunąć klucze prywatny i publiczny.

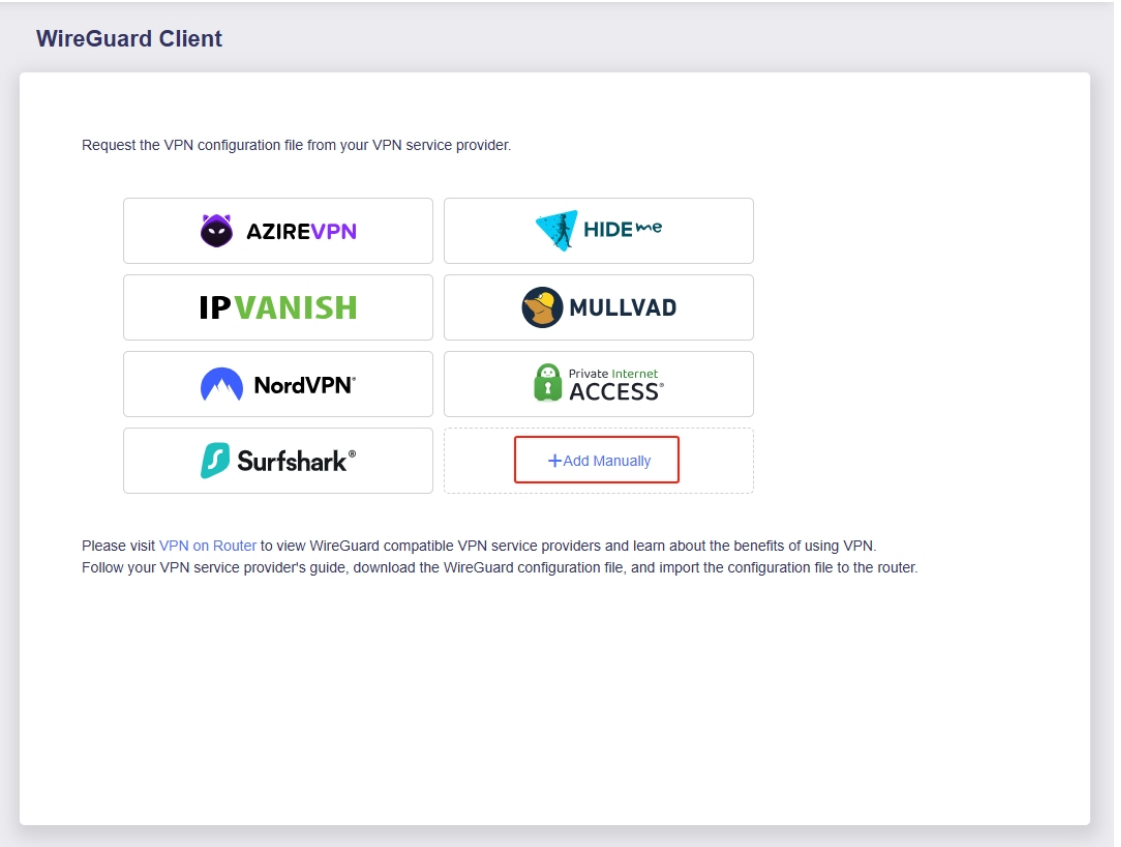


11.2.9 Ręczna konfiguracja klienta WireGuard (inni dostawcy)

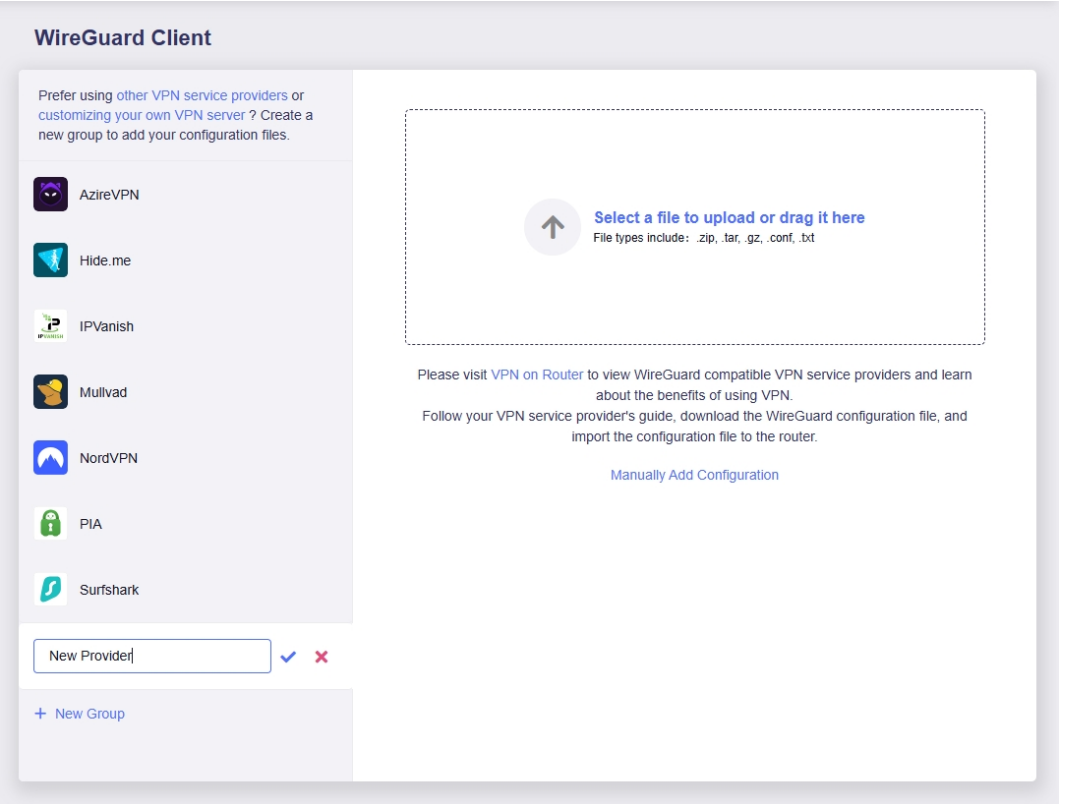
Jeśli Twój dostawca WireGuard nie jest zintegrowany z panelem administracyjnym, najpierw odwiedź jego oficjalną witrynę i pobierz plik konfiguracyjny. Następnie prześlij go do routera, aby skonfigurować klienta WireGuard. Jeśli nie wiesz, jak pobrać pliki konfiguracyjne, skorzystaj z tego poradnika lub skontaktuj się z pomocą techniczną dostawcy.

Poniżej opisano przesyłanie pliku konfiguracyjnego do routera w celu skonfigurowania klienta WireGuard.

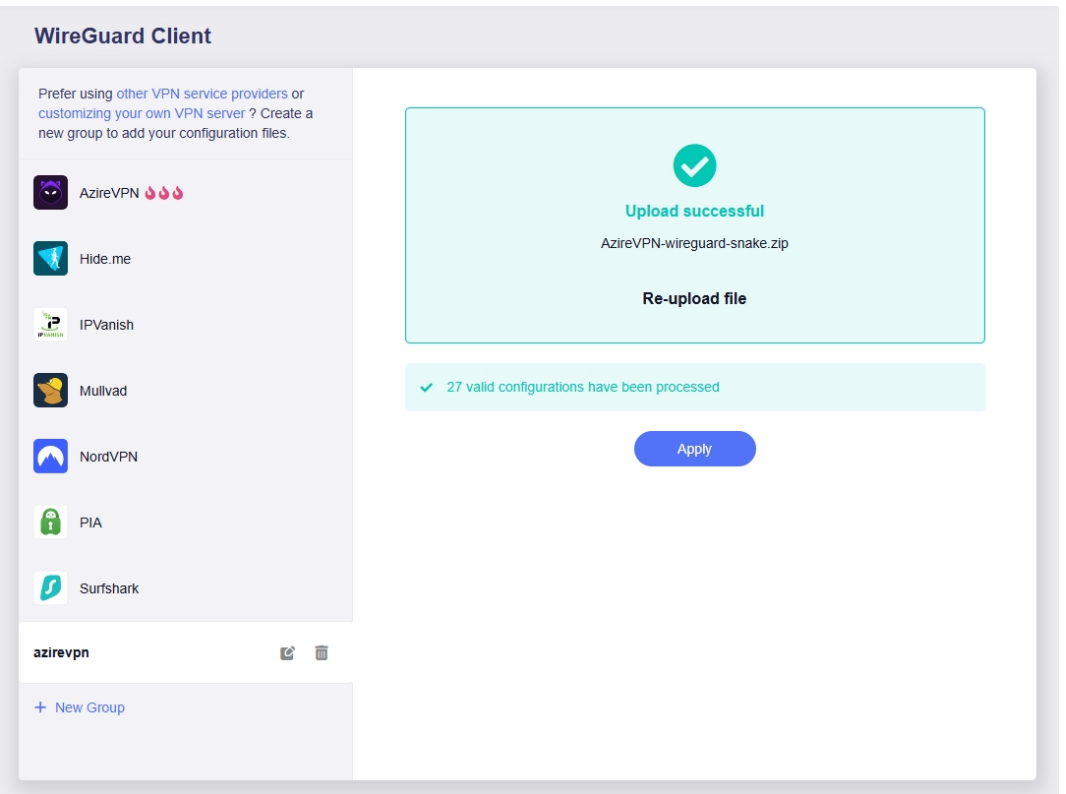
1. Zaloguj się do panelu administracyjnego routera i przejdź do **VPN** > **WireGuard Client** > **Add Manually**.



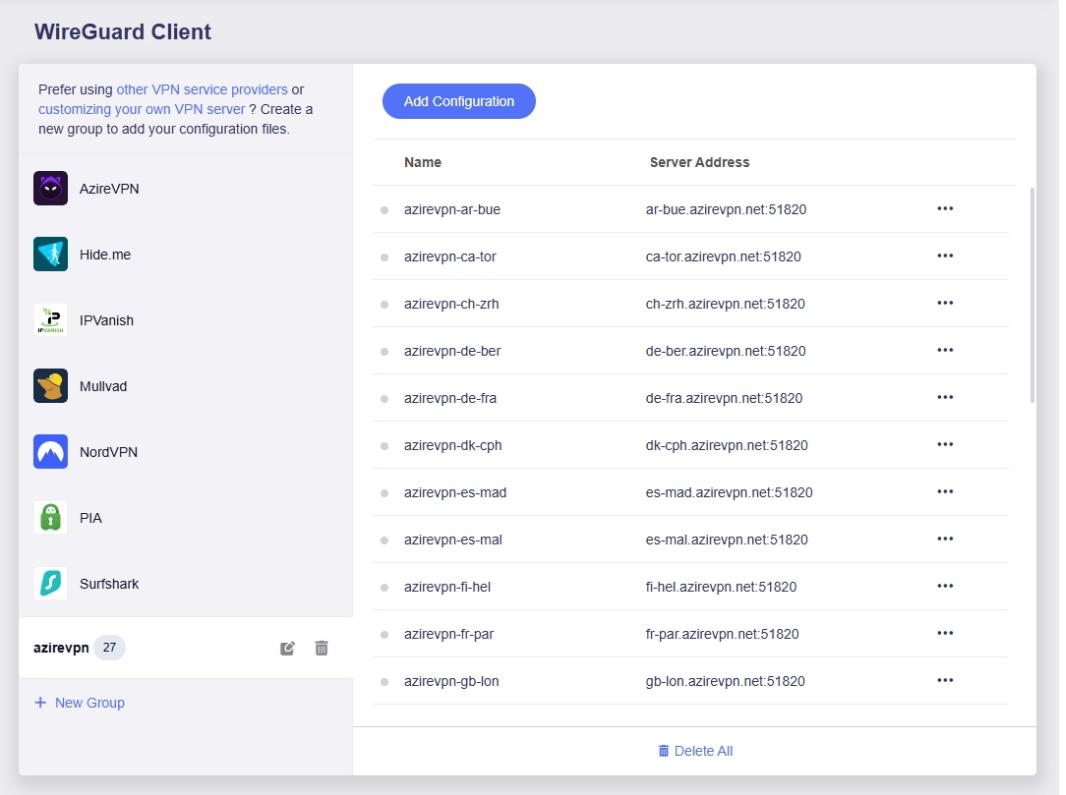
2. Na lewym pasku bocznym powstanie grupa. Nadaj jej opisową nazwę.



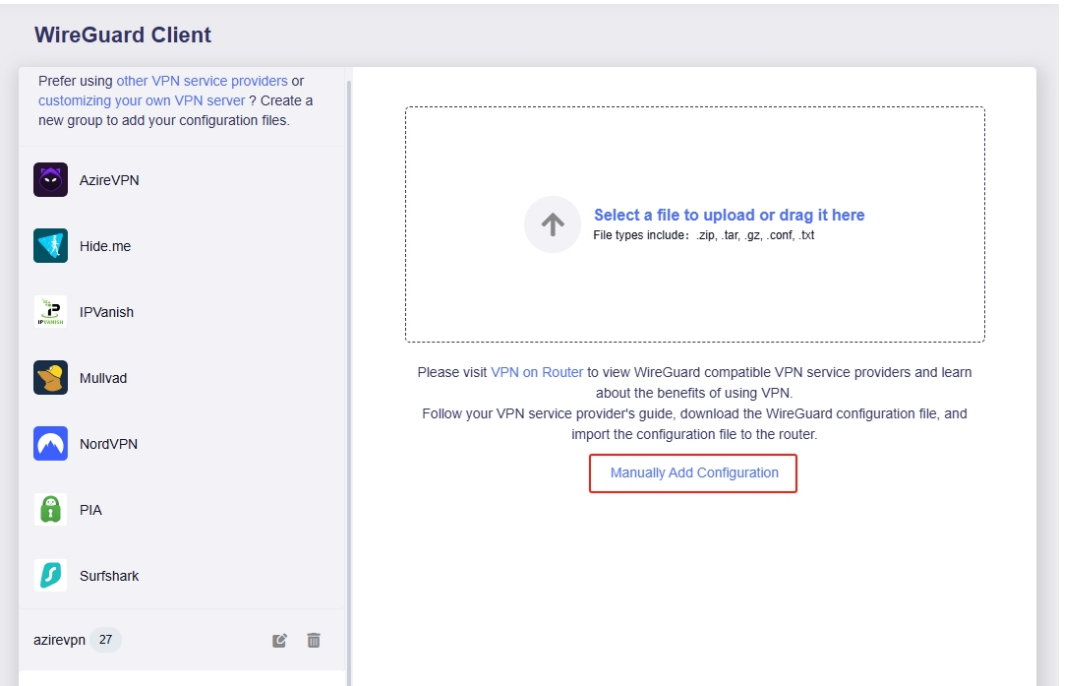
3. Kliknij obszar przesyłania, aby przesłać plik konfiguracyjny WireGuard (obsługiwane formaty: zip, tar, gz, conf, txt), i kliknij **Apply**.

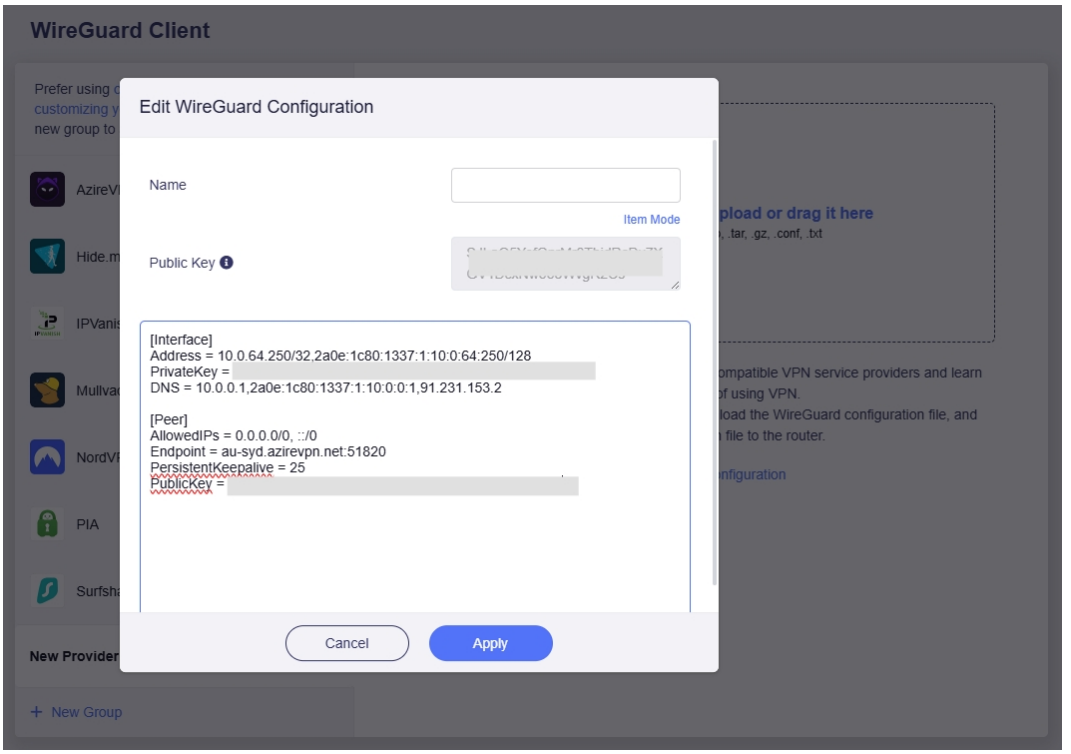


Po przesłaniu skompresowanego pliku zawierającego wiele plików konfiguracyjnych zostanie on automatycznie rozpakowany, jak pokazano poniżej.

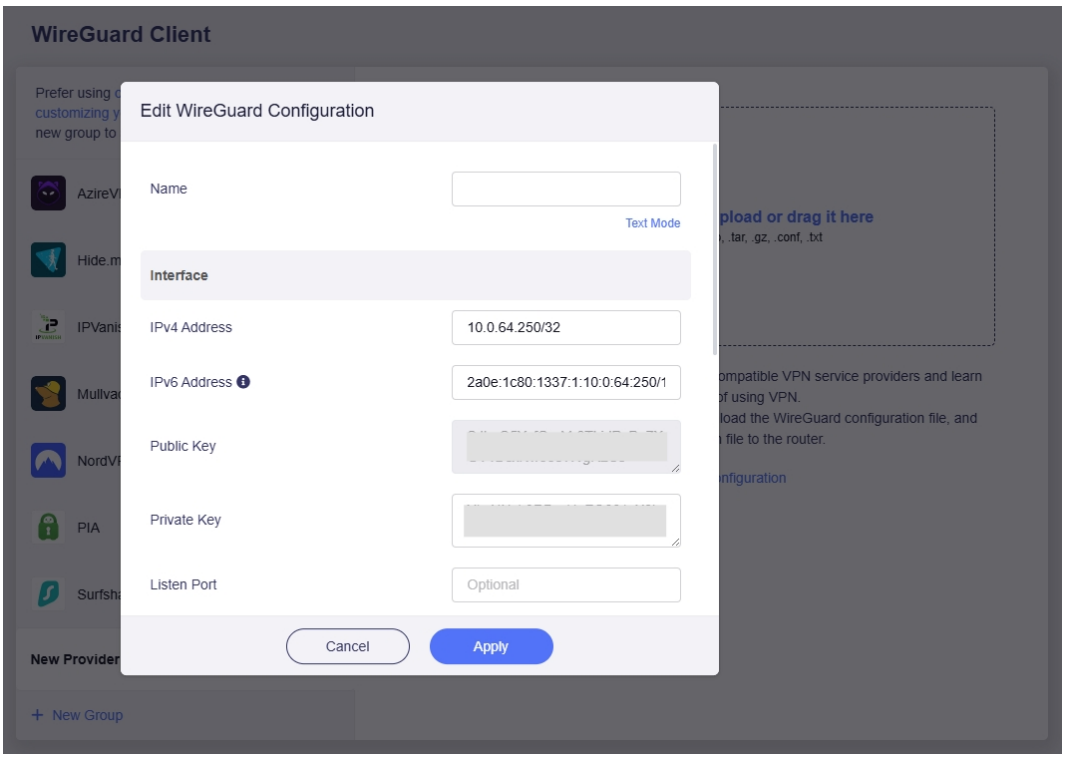


Możesz też kliknąć **Manually Add Configuration** u dołu obszaru przesyłania, dodać konfigurację w postaci tekstu i kliknąć **Apply**.

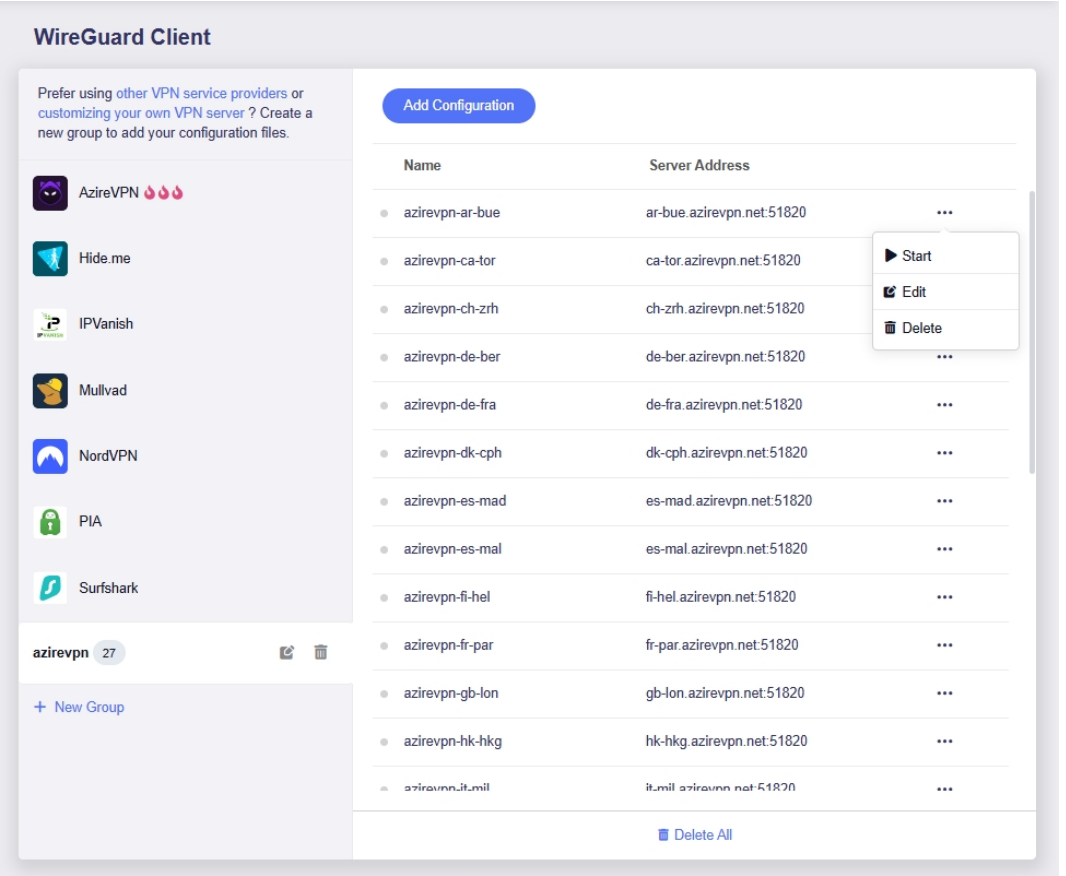




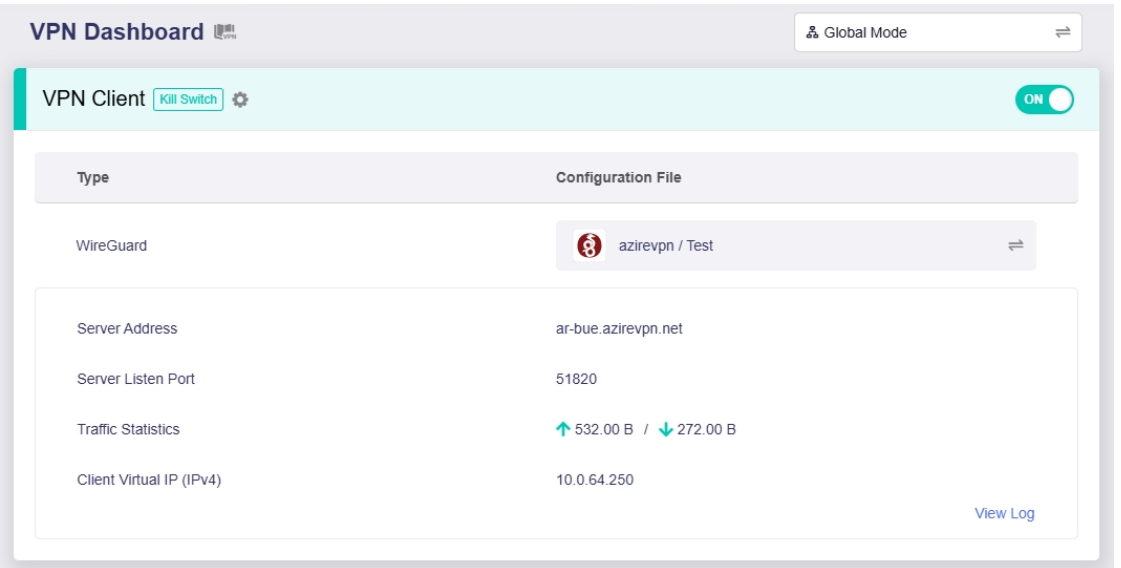
Aby sprawdzić poszczególne elementy, przełącz się do trybu Item, sprawdź szczegóły konfiguracji, a następnie kliknij **Apply**.



4. Kliknij ikonę trzech kropek po prawej stronie, aby nawiązać połączenie.



5. Po połączeniu obok pliku konfiguracyjnego pojawi się zielona kropka. Szczegóły połączenia VPN możesz sprawdzić w **VPN Dashboard**.



Rozdział 12

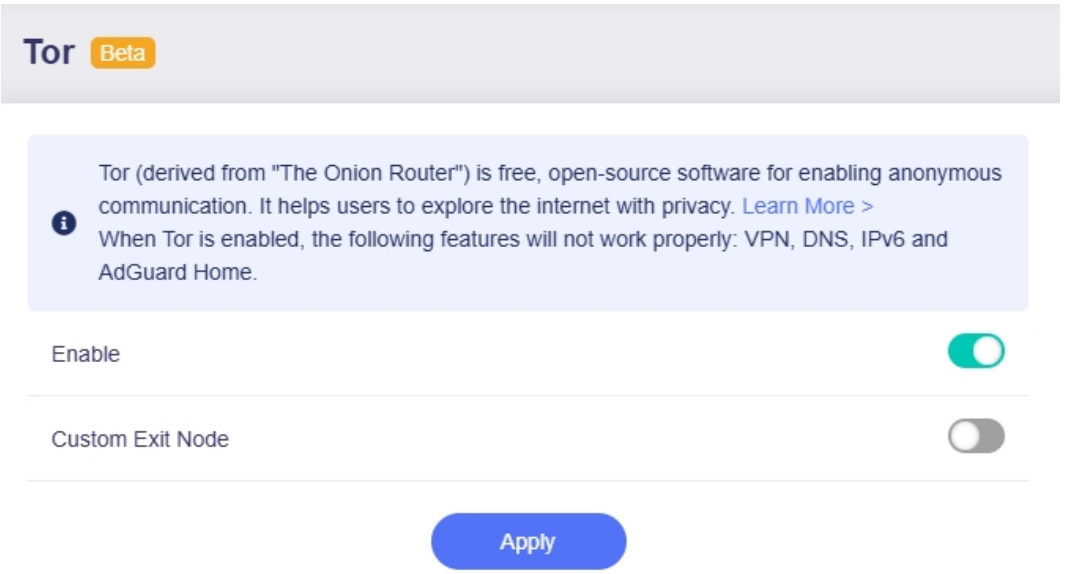
Tor

W tym rozdziale krótko przedstawiono Tor (The Onion Router), bezpłatne oprogramowanie o otwartym kodzie źródłowym umożliwiające anonimową komunikację.

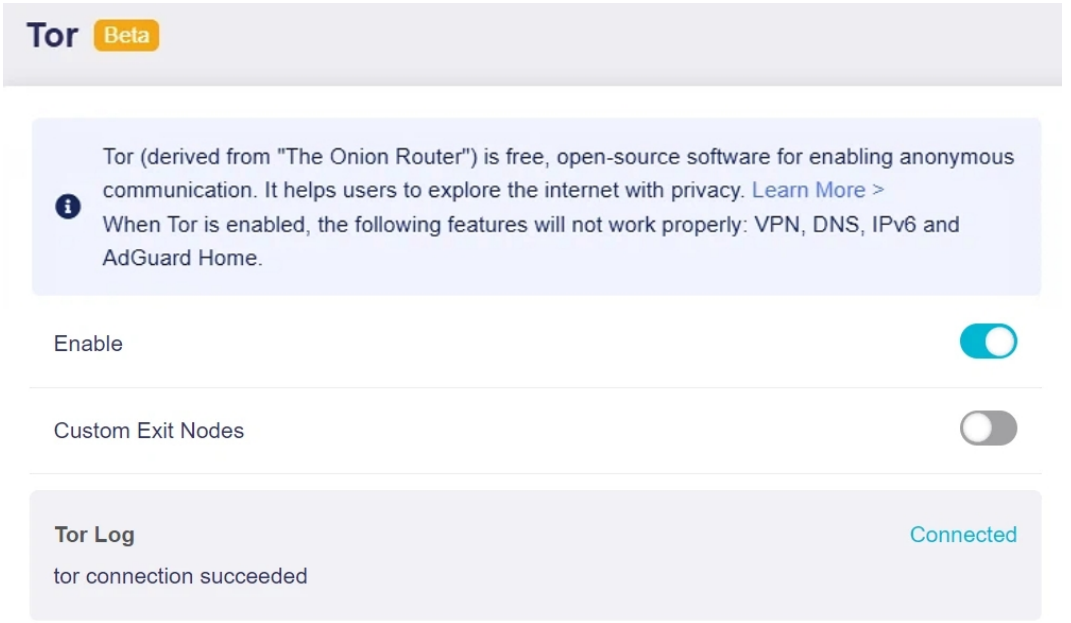
Tor (nazwa pochodzi od **The Onion Router**) to bezpłatne oprogramowanie o otwartym kodzie źródłowym umożliwiające anonimową komunikację. Pomaga przeglądać Internet z zachowaniem prywatności. Ta funkcja jest obecnie w wersji beta i może zawierać błędy. Po włączeniu Tor następujące funkcje nie będą działać poprawnie: VPN, DNS, IPv6 i AdGuard Home.

Aby w razie potrzeby skonfigurować Tor, wykonaj poniższe czynności.

1. Zaloguj się do panelu administracyjnego routera i przejdź do **VPN** > **Tor**. Włącz funkcję przełącznikiem, w razie potrzeby włącz Custom Exit Nodes i kliknij **Apply**.



2. Rozpocznie się nawiązywanie połączenia. Jeśli sieć spełnia wymagania, pojawi się stan połączenia.


Tor
Beta
Tor (derived from "The Onion Router") is free, open-source software for enabling anonymous communication. It helps users to explore the internet with privacy. Learn More >
When Tor is enabled, the following features will not work properly: VPN, DNS, IPv6 and AdGuard Home.
Enable
Custom Exit Nodes
Tor Log
Connected
tor connection succeeded

Rozdział 13

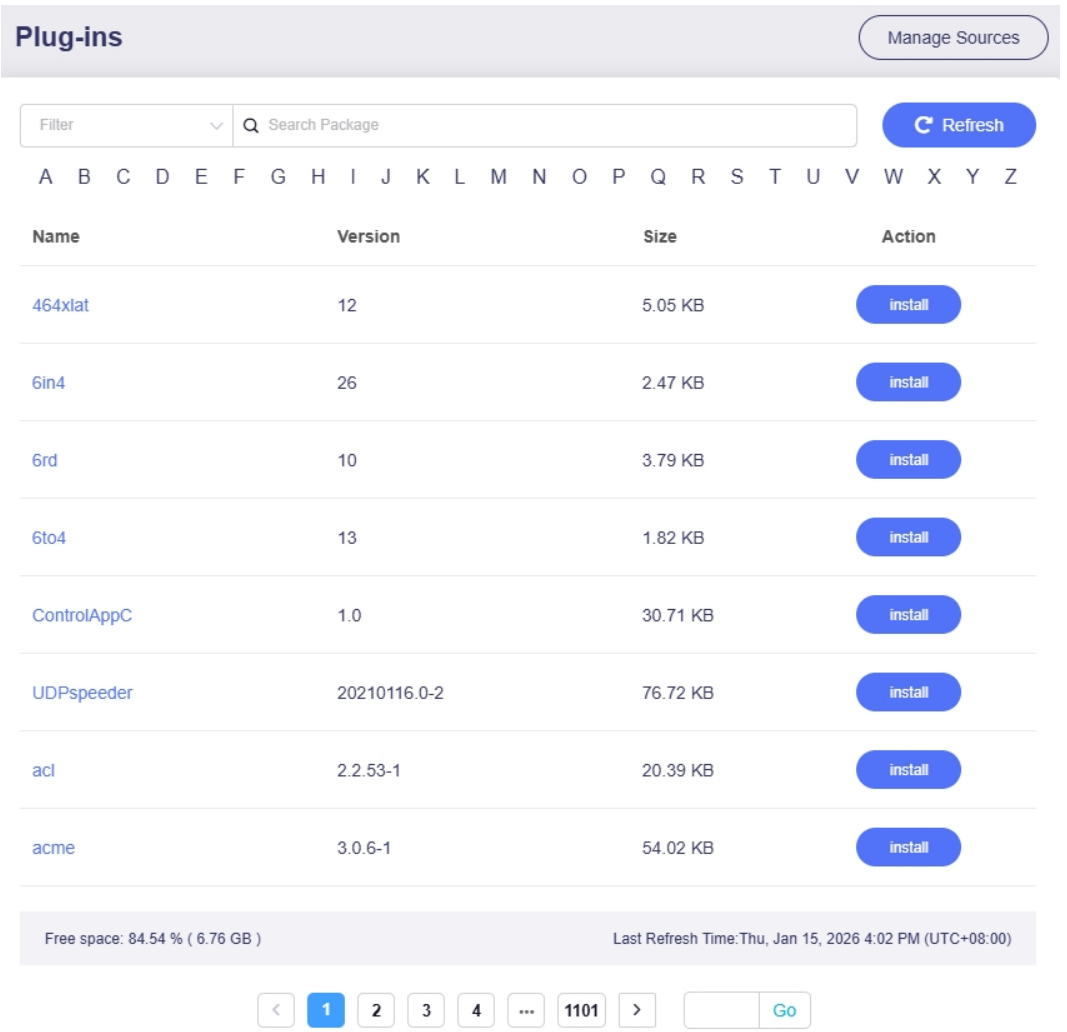
Aplikacje

W tym rozdziale przedstawiono aplikacje dostępne w routerach GL.iNet: wtyczki, Dynamic DNS, pamięć sieciową, AdGuard Home, ZeroTier i Tailscale.

13.1 Wtyczki

Strona Plug-ins umożliwia zarządzanie pakietami OpenWrt.

Zaloguj się do panelu administracyjnego routera i przejdź do **APPLICATIONS** > **Plug-ins.** Możesz instalować lub usuwać dowolne pakiety dostępne w repozytorium. Przed instalacją wtyczek kliknij przycisk **Refresh**, aby zaktualizować listę pakietów.



Uwaga:

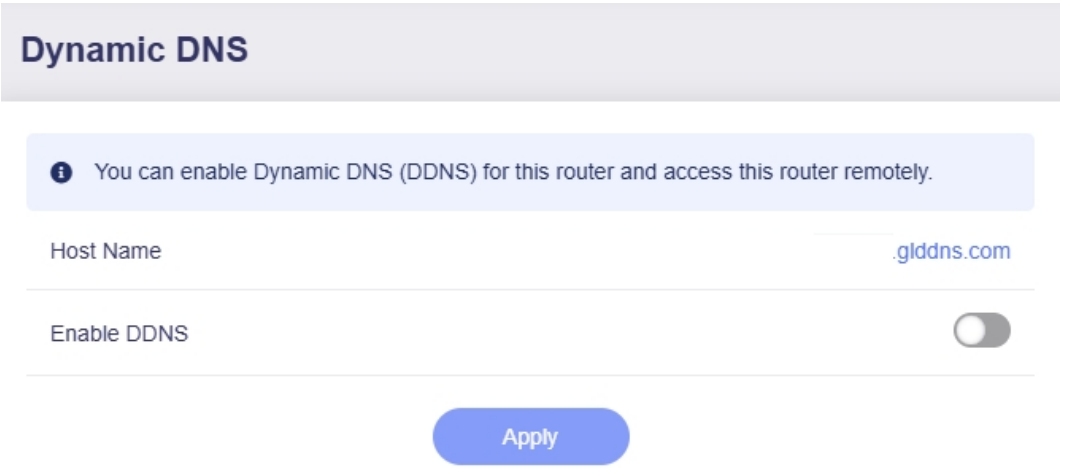
1. Nie zaleca się aktualizowania wtyczek zainstalowanych fabrycznie w oficjalnym oprogramowaniu GL.iNet, takich jak nginx, adguard home, tailscale itp.
2. Wtyczki zewnętrzne zainstalowane ręcznie przez użytkownika można aktualizować, jednak GL.iNet nie odpowiada za związane z nimi problemy z bezpieczeństwem. Pytania należy kierować do autorów odpowiednich wtyczek.

13.2 Dynamiczny DNS

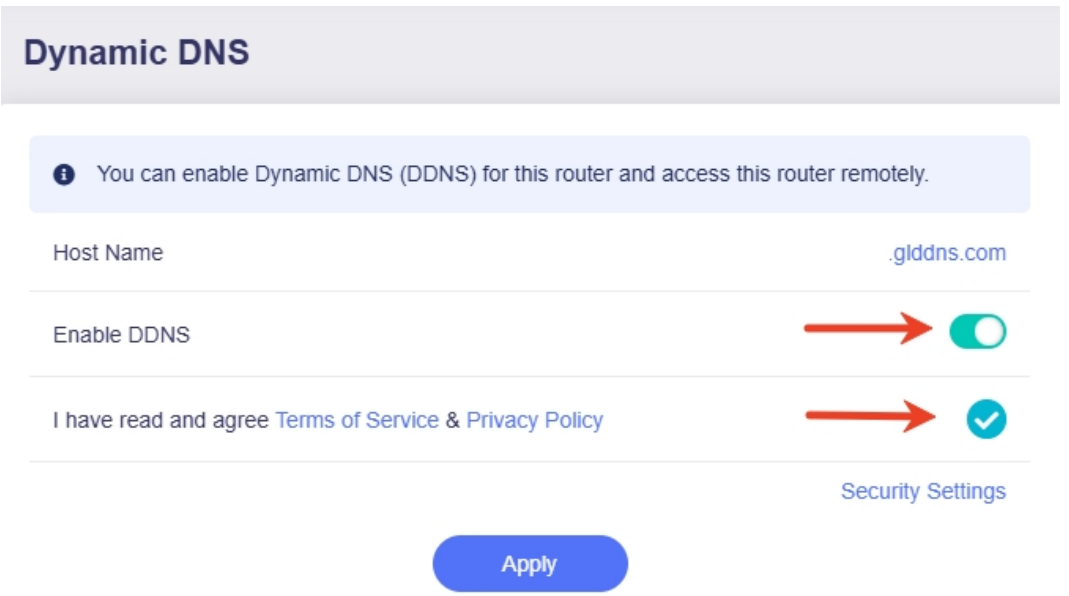
Dynamic Domain Name Service (DDNS, czyli dynamiczny DNS) to usługa mapująca nazwę domeny na dynamiczny adres IP urządzenia sieciowego. Dzięki niej można zdalnie uzyskiwać dostęp do routera. Ta funkcja wymaga publicznego adresu IP.

13.2.1 Włączanie DDNS

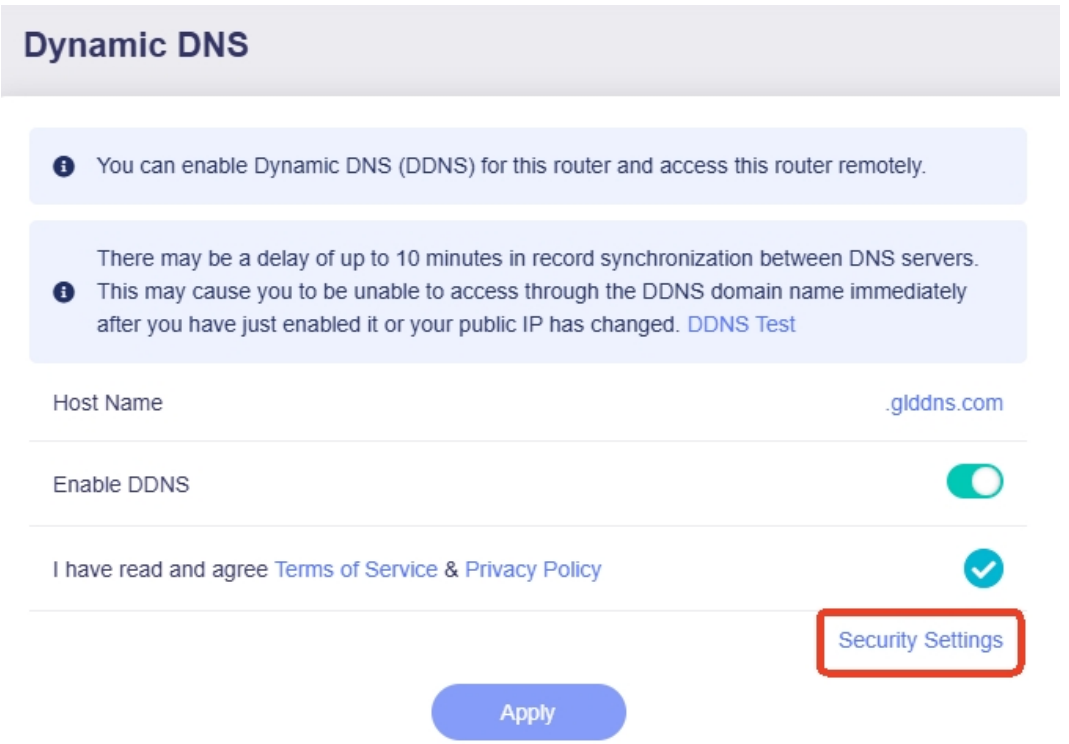
1. Zaloguj się do panelu administracyjnego routera i przejdź do **APPLICATIONS** > **Dynamic DNS**. Strona wygląda jak poniżej.



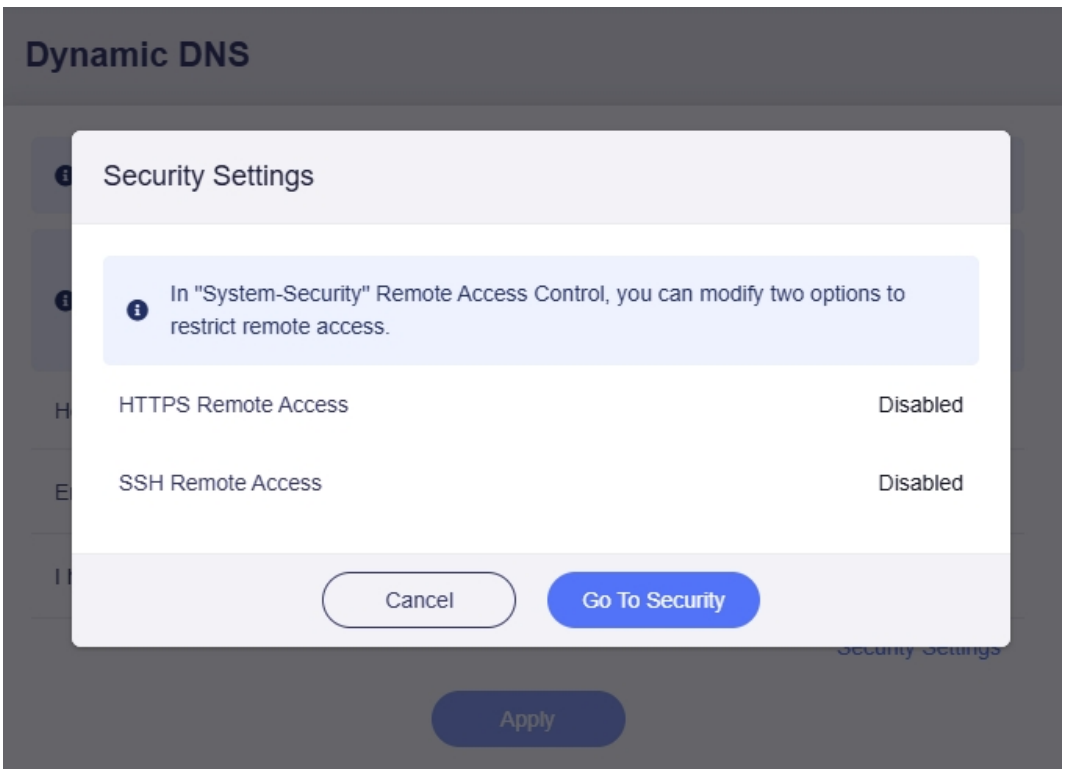
2. Włącz **Enable DDNS**, przeczytaj i zaakceptuj **Terms of Services & Privacy Policy**, a następnie kliknij **Apply**.



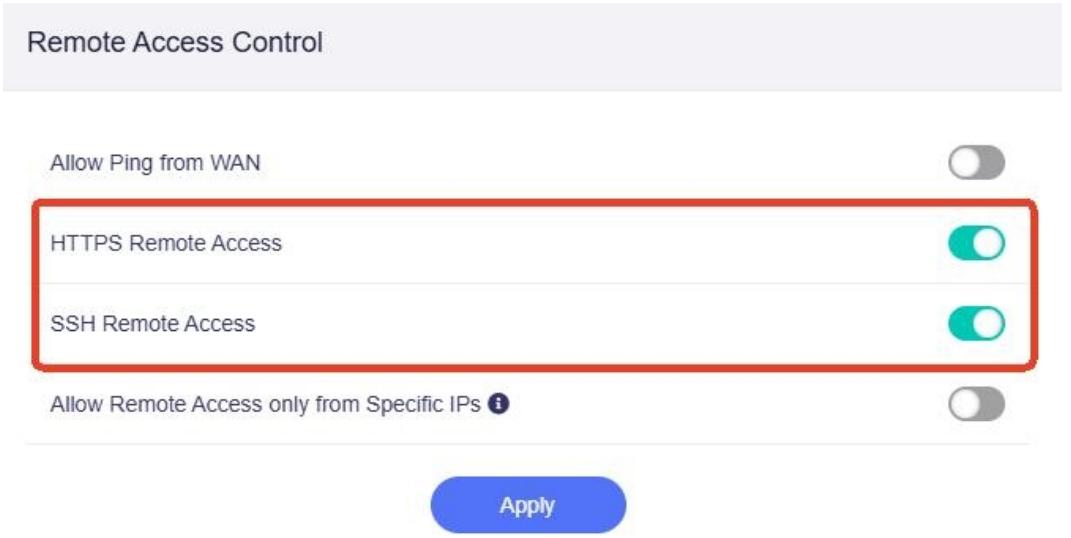
3. Kliknij **Security Settings** w prawym dolnym rogu.



4. W wyświetlonym oknie sprawdź, czy wybrany rodzaj dostępu zdalnego jest włączony.



Jeśli nie, przejdź do **SYSTEM** > **Security** > **Remote Access Control**, aby włączyć tę funkcję, a następnie kliknij **Apply**.



Uwaga:

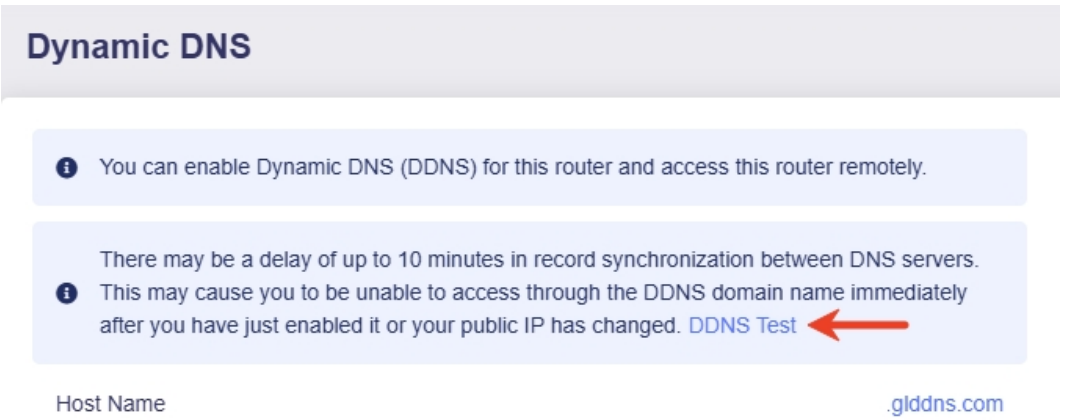
1. Synchronizacja rekordów między serwerami DNS może trwać do 10 minut. Może to uniemożliwić dostęp przez nazwę domeny DDNS bezpośrednio po włączeniu funkcji lub zmianie publicznego adresu IP.
2. Jeśli jednocześnie włączysz DDNS i klienta VPN, upewnij się, że opcja Services From GL.iNet Use VPN jest wyłączona.

13.2.2 Sprawdzanie działania DDNS

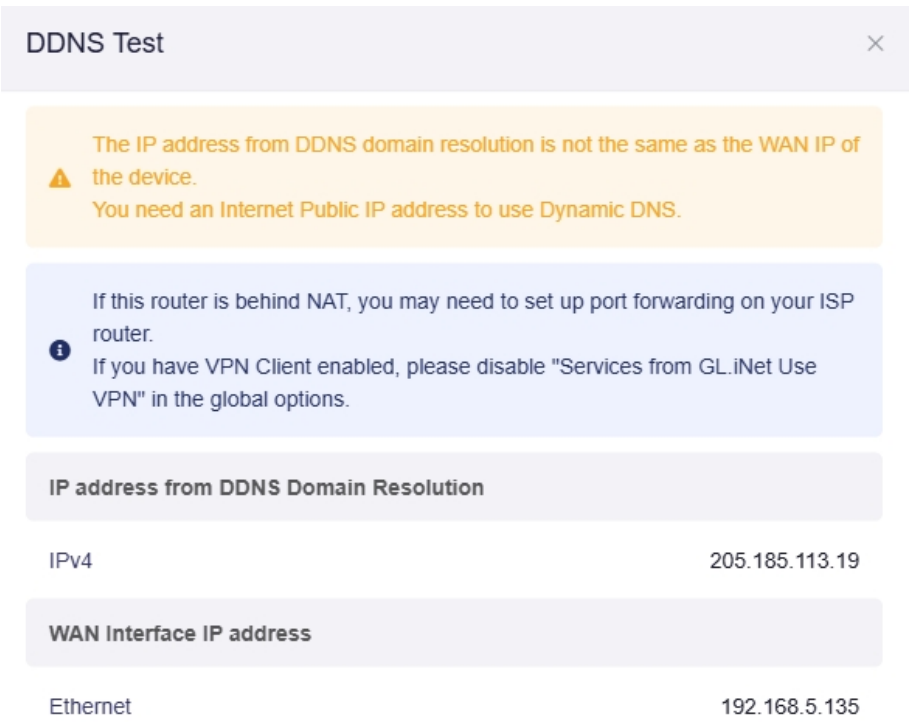
Działanie DDNS można sprawdzić za pomocą narzędzia testowego DDNS lub ręcznie, przy użyciu poleceń.

Metoda 1. Narzędzie DDNS Test

1. Na stronie Dynamic DNS kliknij **DDNS Test**.



2. Upewnij się, że adres IP uzyskany z rozwiązania nazwy domeny DDNS odpowiada adresowi WAN routera. W przeciwnym razie u góry pojawi się żółty komunikat wskazujący, że router może znajdować się za NAT i trzeba skonfigurować przekierowanie portów na routerze nadrzędnym.



Metoda 2. Polecenia

1. Użyj polecenia nslookup *nslookup xxxxxxx.glddns.com 8.8.8.8* , aby sprawdzić powiązanie nazwy domeny z adresem IP. Poniżej przedstawiono przykład dla Beryl AX GL-MT3000.



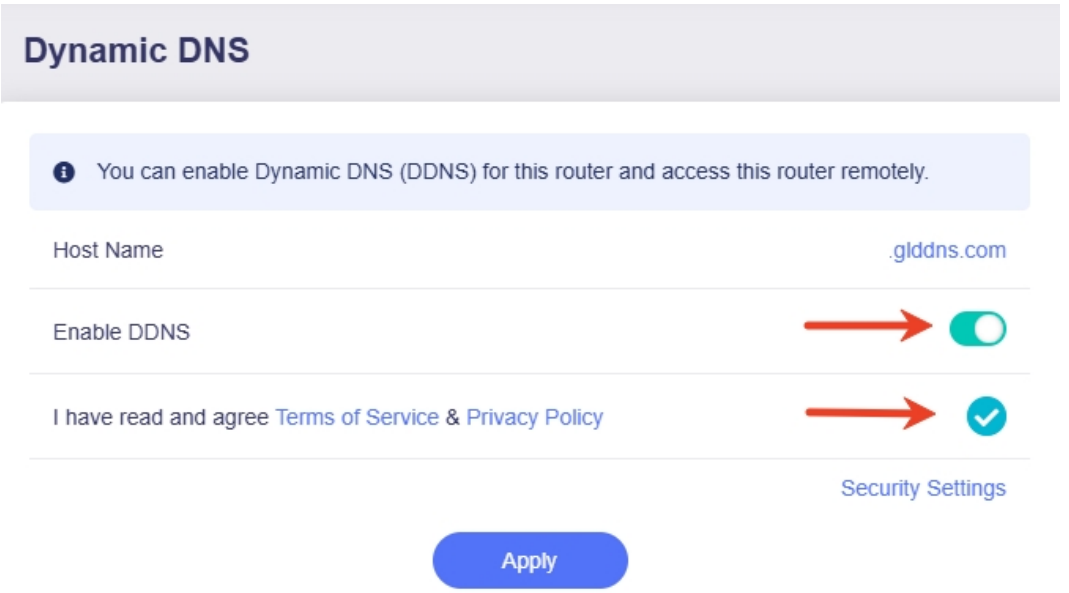
   - Zastąp „xxxxxxx.glddns.com” na powyższej ilustracji własną nazwą hosta.
   - „8.8.8.8” to serwer DNS Google. Użyj go lub zastąp innym adresem, a następnie naciśnij Enter.
2. Jeśli otrzymasz publiczny adres IP, taki jak „183.178.10.100” na powyższej ilustracji, domena DDNS została prawidłowo powiązana z publicznym adresem IP. Komunikat w rodzaju „server can’t find xxxxxxx.glddns.com” może oznaczać, że rozwiązanie nazwy domeny nie powiodło się i domena DDNS nie została prawidłowo powiązana z publicznym adresem IP. Przejdź do następnego kroku, aby to sprawdzić.
3. Zaloguj się do panelu administracyjnego routera i przejdź do **INTERNET**. Znajdź adres IP WAN routera w aktualnie aktywnym interfejsie. Porównaj go z uzyskanym wyżej publicznym adresem IP. Jeśli są takie same, DDNS działa; w przeciwnym razie nie działa.

13.2.3 Zdalny dostęp przez HTTPS

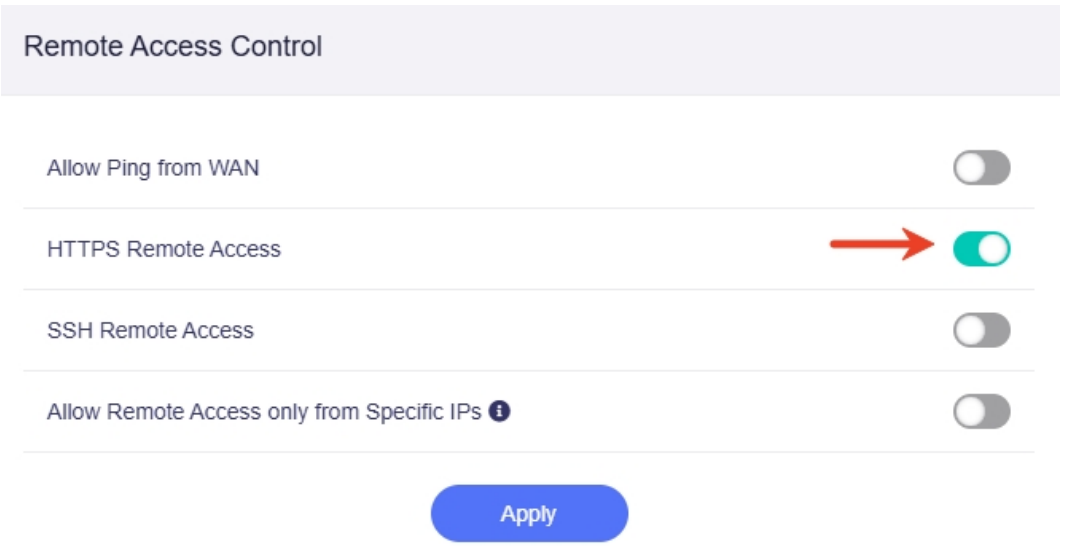
Do zdalnego dostępu przez HTTPS wymagany jest **publiczny adres IP**. Kliknij tutaj, aby sprawdzić, czy dostawca Internetu przydziela taki adres. Jeśli router znajduje się za NAT, skonfiguruj przekierowanie portów (**port 443**) na routerze nadrzędnym dla dostępu HTTPS.

Aby włączyć zdalny dostęp do routera przez HTTPS, wykonaj poniższe czynności.

1. Na stronie Dynamic DNS włącz **Enable DDNS**, zaakceptuj **Terms of Services & Privacy Policy**, a następnie kliknij **Apply**.

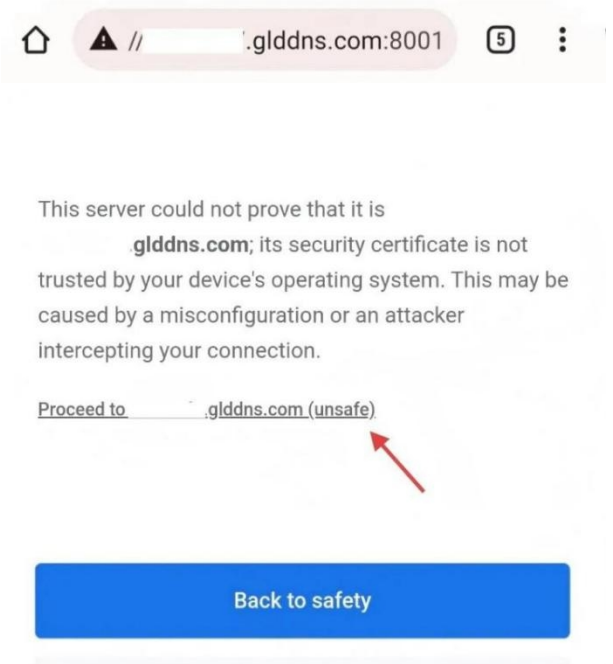


2. W panelu administracyjnym przejdź do **SYSTEM** > **Security** > **Remote Access Control**. Włącz **HTTPS Remote Access** i kliknij **Apply**.



Po włączeniu możesz z dowolnego miejsca uzyskiwać dostęp do panelu administracyjnego przez HTTPS, używając nazwy hosta DDNS, np. **https://xxxxxxx.glddns.com**. Jeśli skonfigurowano przekierowanie portów, użyj adresu **https://xxxxxxx.glddns.com:external_port** (zastąp external_port rzeczywistym numerem portu).

Uwaga: ta funkcja używa certyfikatów z podpisem własnym, dlatego przy dostępie do panelu administracyjnego przez HTTPS z nazwą hosta DDNS przeglądarka wyświetla komunikat „Your connection is not private”. Aby kontynuować dostęp zdalny HTTPS, kliknij **Advanced** u dołu, a następnie **Proceed to xxxxxxx.glddns.com** .



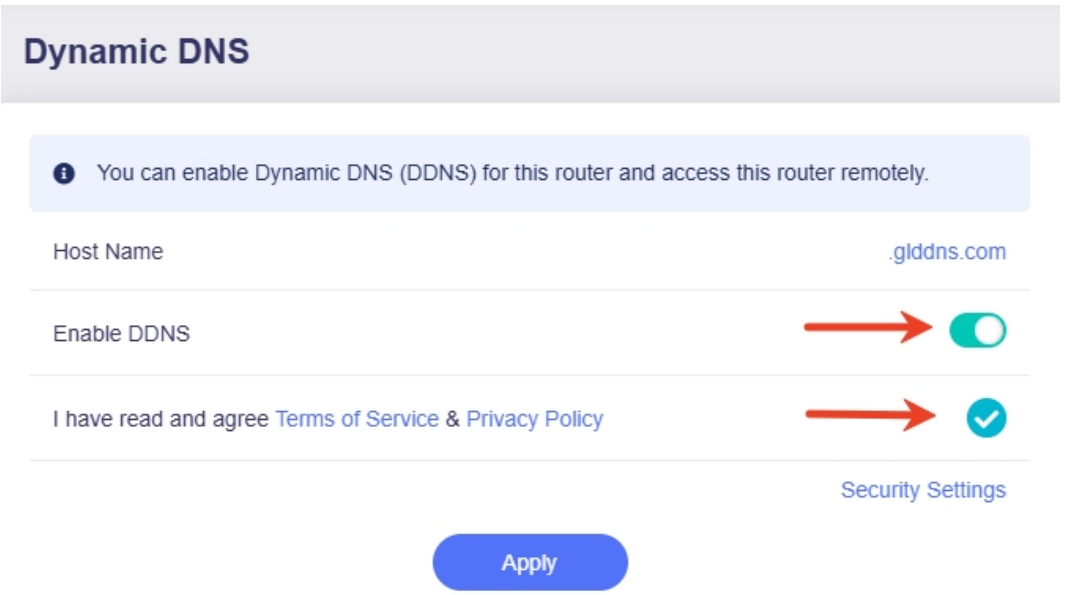
Możesz teraz uzyskiwać dostęp do panelu administracyjnego routera za pomocą nazwy hosta DDNS przez **HTTPS**.

13.2.4 Zdalny dostęp przez SSH

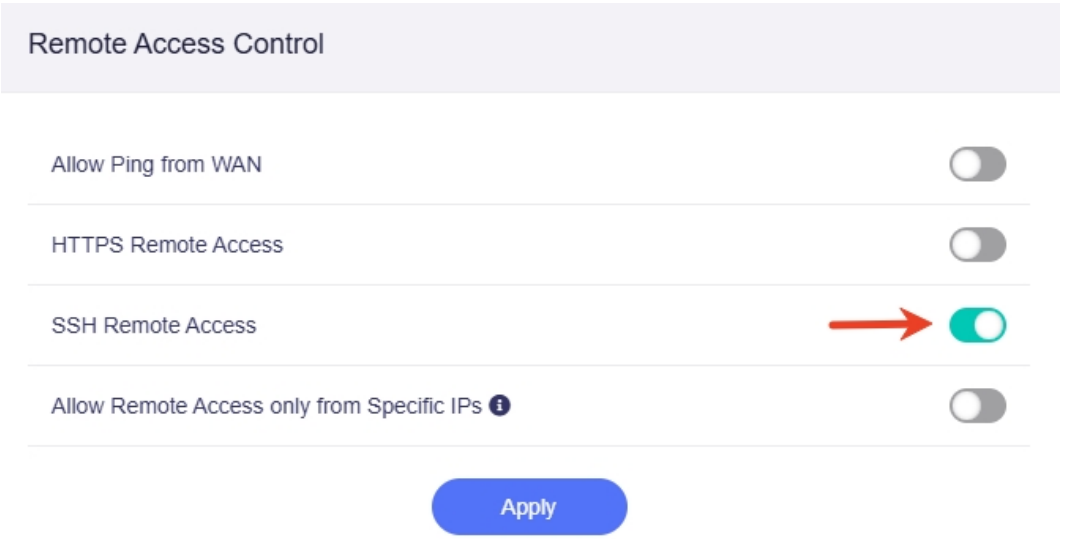
Do zdalnego dostępu przez SSH wymagany jest **publiczny adres IP**. Kliknij tutaj, aby sprawdzić, czy dostawca Internetu przydziela taki adres. Jeśli router znajduje się za NAT, skonfiguruj przekierowanie portów (**port 22**) na routerze nadrzędnym dla zdalnego dostępu SSH.

Aby włączyć zdalny dostęp do routera przez SSH, wykonaj poniższe czynności.

1. Na stronie Dynamic DNS włącz **Enable DDNS**, zaakceptuj **Terms of Services & Privacy Policy**, a następnie kliknij **Apply**.



2. W panelu administracyjnym przejdź do **SYSTEM** > **Security** > **Remote Access Control**. Włącz **SSH Remote Access** i kliknij **Apply**.



Po włączeniu możesz z dowolnego miejsca uzyskiwać dostęp do panelu administracyjnego przez SSH, używając nazwy hosta DDNS, np. **ssh root@xxxxxxx.glddns.com**. Jeśli skonfigurowano przekierowanie portów, użyj **ssh root@xxxxxxx.glddns.com:external_port** (zastąp external_port rzeczywistym numerem portu).

13.3 Pamięć sieciowa

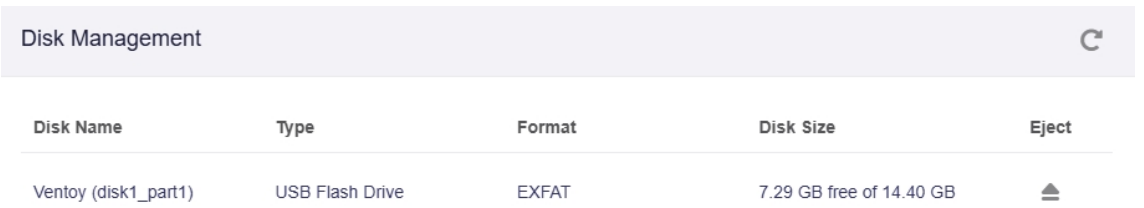
Pamięć sieciowa umożliwia bezprzewodowe udostępnianie plików między urządzeniami po podłączeniu nośnika USB lub karty SD do routera. Router przekształca nośnik w udostępniony dysk sieciowy, dostępny dla wszystkich urządzeń połączonych przez Wi-Fi.

Flint 3e jest wyposażony w port USB zgodny z pamięciami flash USB i przenośnymi zewnętrznymi dyskami twardymi. Dla tych nośników można skonfigurować Samba, WebDAV lub DLNA. Obsługiwane są popularne formaty, takie jak NTFS, FAT32 i EXT4.

Uwaga: dysk twardy USB pobiera stosunkowo dużo energii. Używaj zewnętrznego zasilacza, w przeciwnym razie mogą wystąpić nieprawidłowości w działaniu.

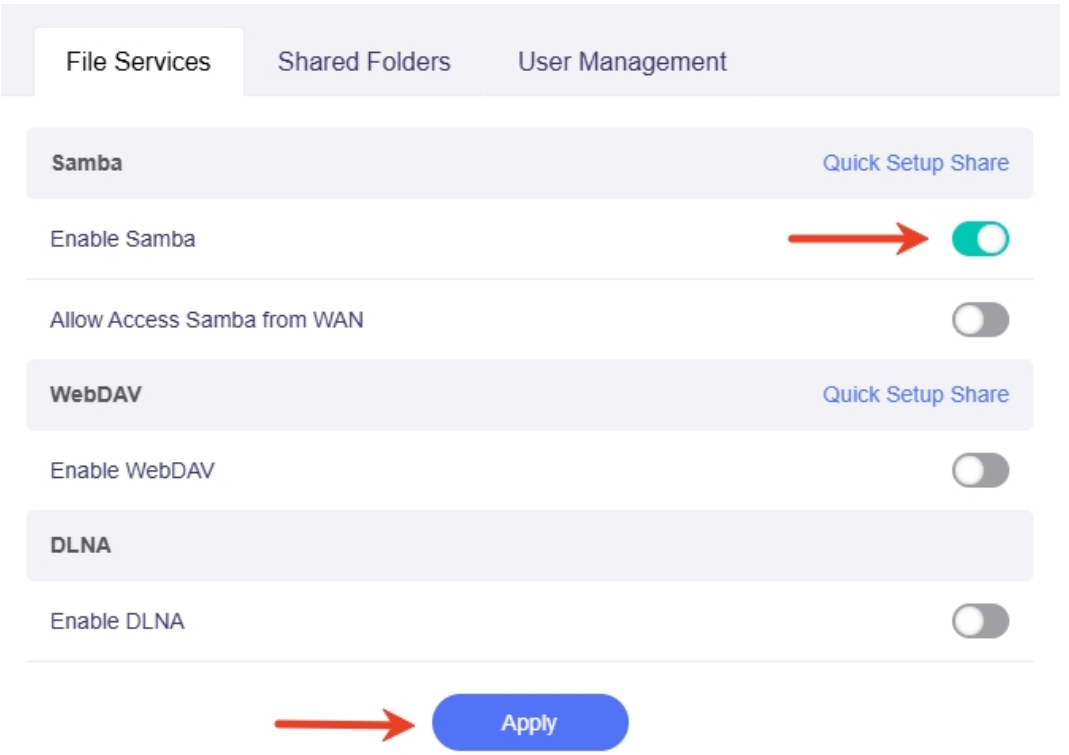
13.3.1 Podłączanie pamięci

1. Podłącz nośnik danych do routera.
   - Pamięć USB: podłącz ją bezpośrednio do portu USB.
   - Zewnętrzny dysk twardy: podłącz go do oddzielnego zasilacza (jeśli jest wymagany), a następnie do routera.
2. Zaloguj się do panelu administracyjnego routera i przejdź do **APPLICATIONS** > **Network Storage**. Tutaj możesz włączać usługi przesyłania plików i zarządzać folderem udostępnionym.
3. Po wykryciu nośnika danych sekcja **Disk Management** będzie wyglądać jak poniżej.



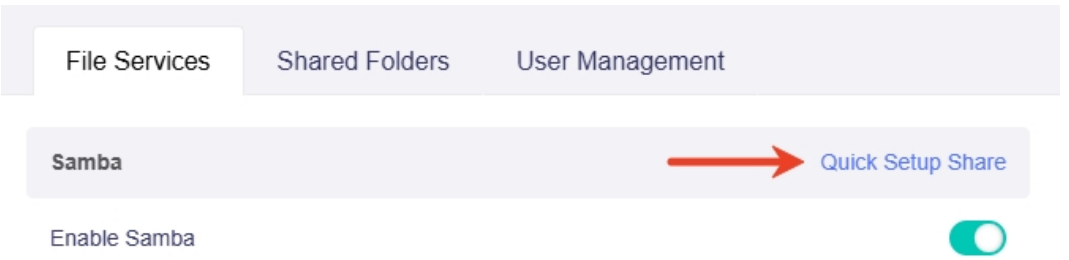
13.3.2 Konfiguracja usługi Samba

1. W sekcji **File Services** włącz **Enable Samba** i kliknij **Apply**.

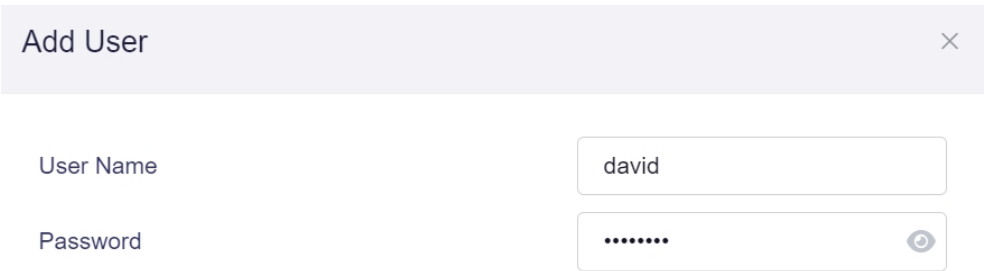


   - **Allow Access Samba from WAN**: włącz tę opcję, jeśli urządzenia w sieci nadrzędnej mają uzyskiwać dostęp do usługi Samba.

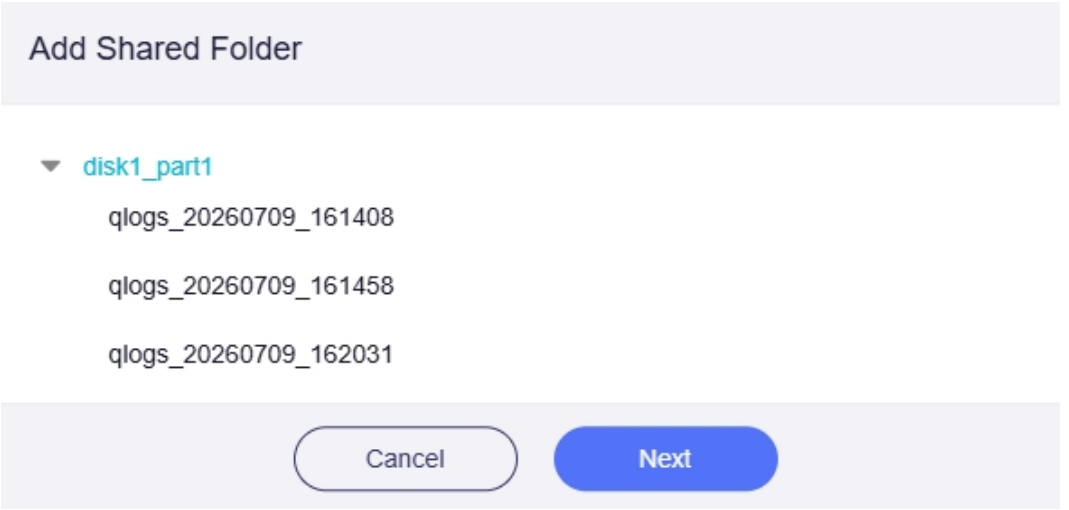
2. Kliknij **Quick Setup Share**, aby skonfigurować łącze do udostępnionego zasobu.



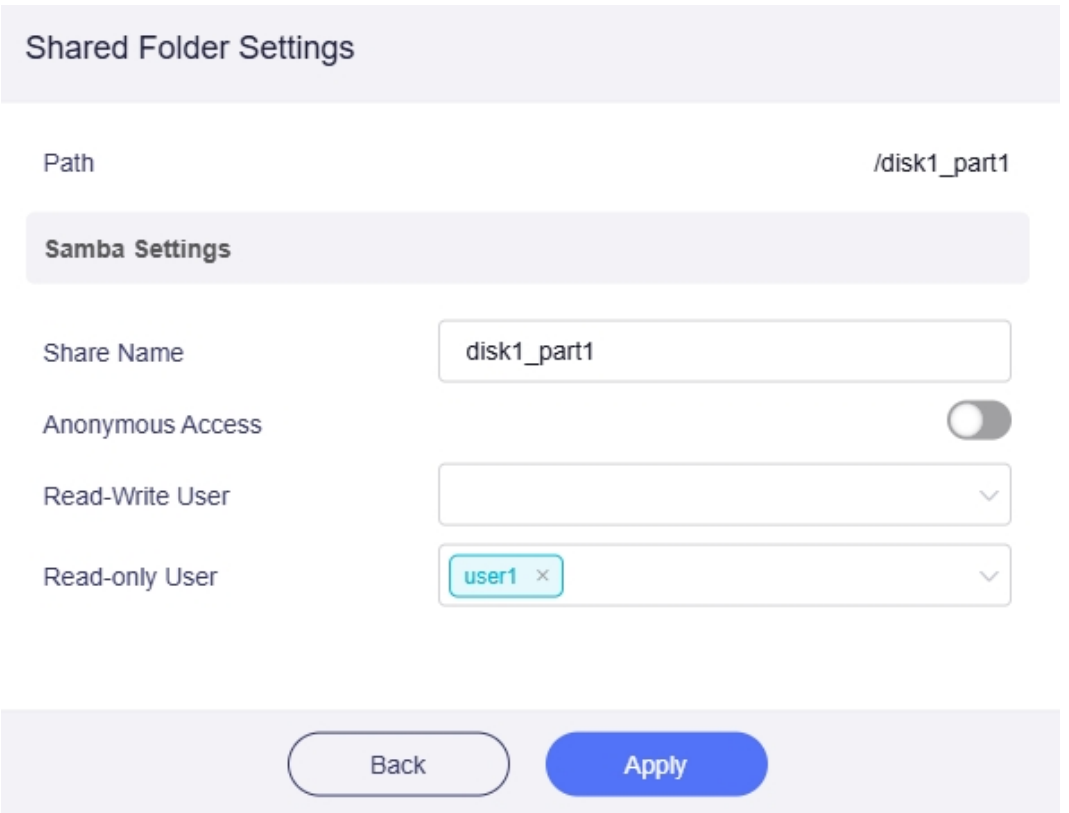
3. Dodaj użytkownika i kliknij **Next**. Jeśli konto już istnieje, ten krok zostanie pominięty.



4. Kliknij ikonę trójkąta, aby wyświetlić wszystkie foldery. Wybierz folder do udostępnienia i kliknij **Next**. Aby udostępnić cały dysk, kliknij jego nazwę (np. disk1_part1).

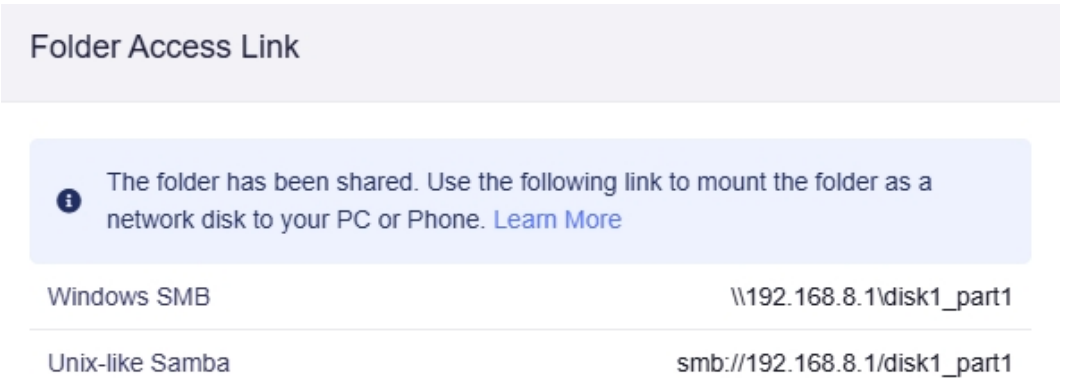


5. Skonfiguruj folder udostępniony.
   Użytkownik utworzony w poprzednim kroku jest domyślnie dodawany do **Read-Only User**. Aby mógł zapisywać lub usuwać pliki, usuń go z Read-Only User i dodaj do **Read-Write User**, a następnie kliknij **Apply**.



Wskazówka: ze względów bezpieczeństwa nie zaleca się włączania Anonymous Access.

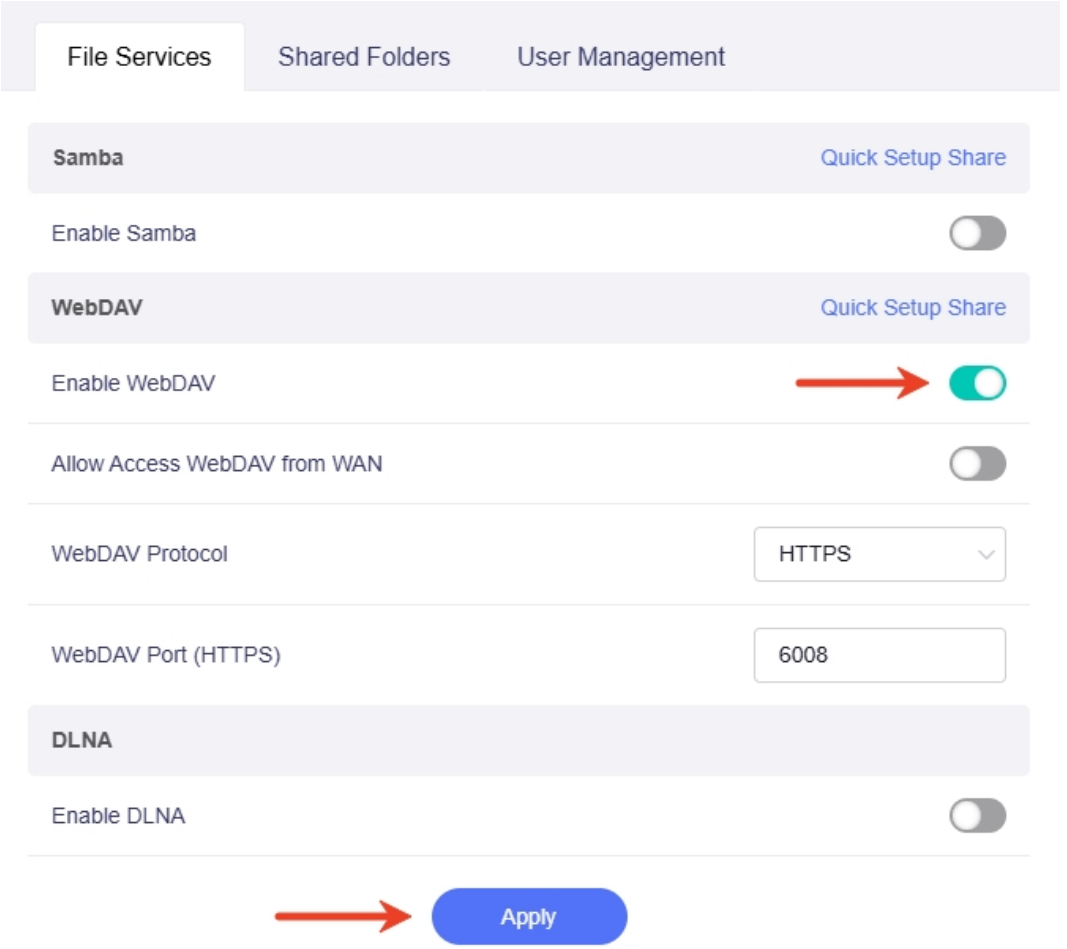
6. Uzyskaj łącze dostępu do folderu.
   Na stronie pojawią się łącza dla systemu Windows i systemów uniksopodobnych, takich jak Android, iOS, macOS, Ubuntu itp. Za ich pomocą można uzyskać dostęp do folderu udostępnionego przez usługę Samba.



Uwaga: jeśli włączysz **Allow Access Samba from WAN** i uzyskujesz dostęp do folderu z sieci nadrzędnej, zastąp adres IP routera w łączu (domyślnie 192.168.8.1) jego adresem IP WAN. Znajdziesz go na stronie INTERNET w panelu administracyjnym.

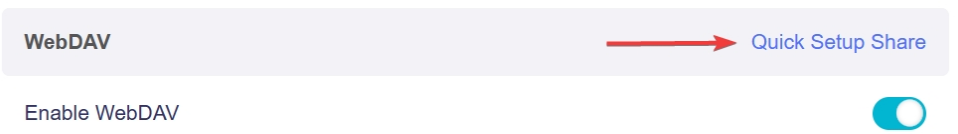
13.3.3 Konfiguracja WebDAV

1. W sekcji **File Services** włącz **Enable WebDAV** i kliknij **Apply**.

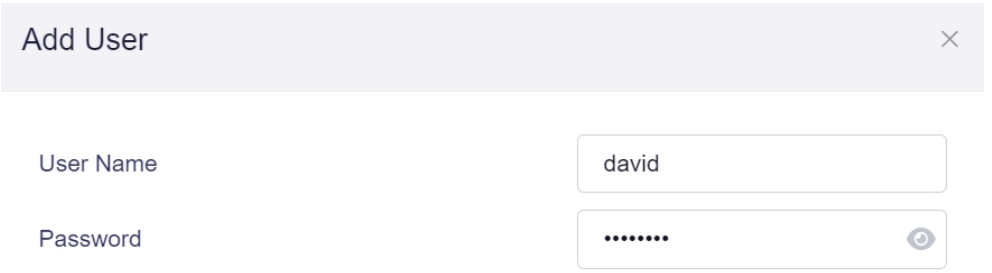


- **Allow Access WebDAV from WAN**: włącz tę opcję, jeśli urządzenia w sieci nadrzędnej mają uzyskiwać dostęp do usługi WebDAV.
- **WebDAV Protocol**: HTTP nie jest szyfrowany; korzystasz z niego na własne ryzyko. HTTPS jest szyfrowany i używa certyfikatu z podpisem własnym.
- **WebDAV Port**: nie trzeba zmieniać numeru portu, chyba że występuje konflikt. Zalecany zakres numerów portów to 1024–65535.

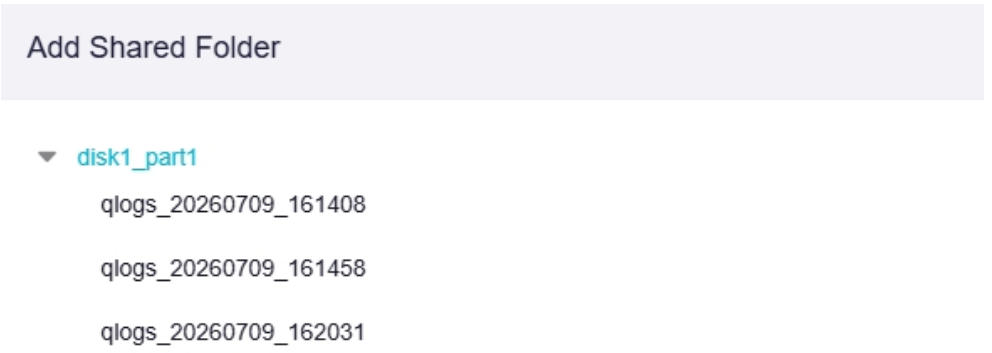
2. Kliknij **Quick Setup Share**, aby skonfigurować łącze do udostępnionego zasobu.



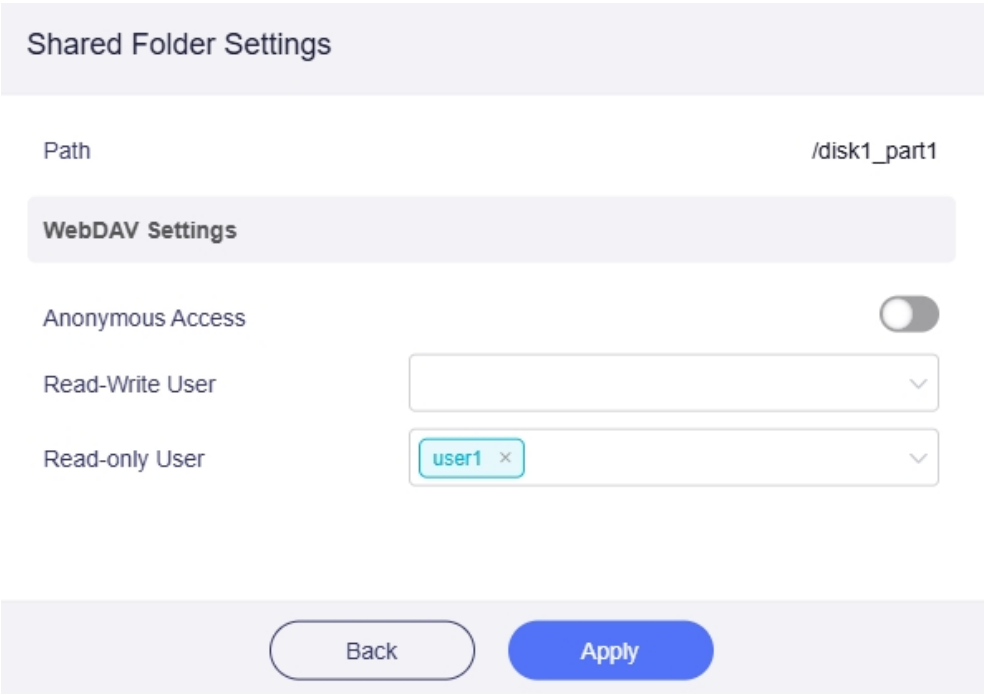
3. Dodaj użytkownika i kliknij **Next**. Jeśli konto już istnieje, ten krok zostanie pominięty.



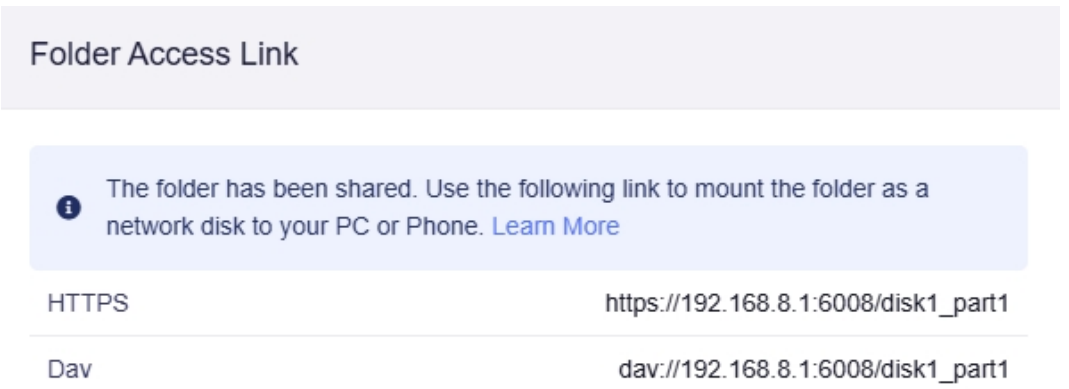
4. Kliknij ikonę trójkąta, aby wyświetlić wszystkie foldery. Wybierz folder do udostępnienia. Aby udostępnić cały dysk, kliknij jego nazwę (np. disk1_part1).



5. Skonfiguruj folder udostępniony.
   Użytkownik utworzony w poprzednim kroku jest domyślnie dodawany do **Read-Only User**.
   Aby użytkownik mógł zapisywać lub usuwać pliki, usuń go z Read-Only User i dodaj do **Read-Write User**, a następnie kliknij **Apply**.



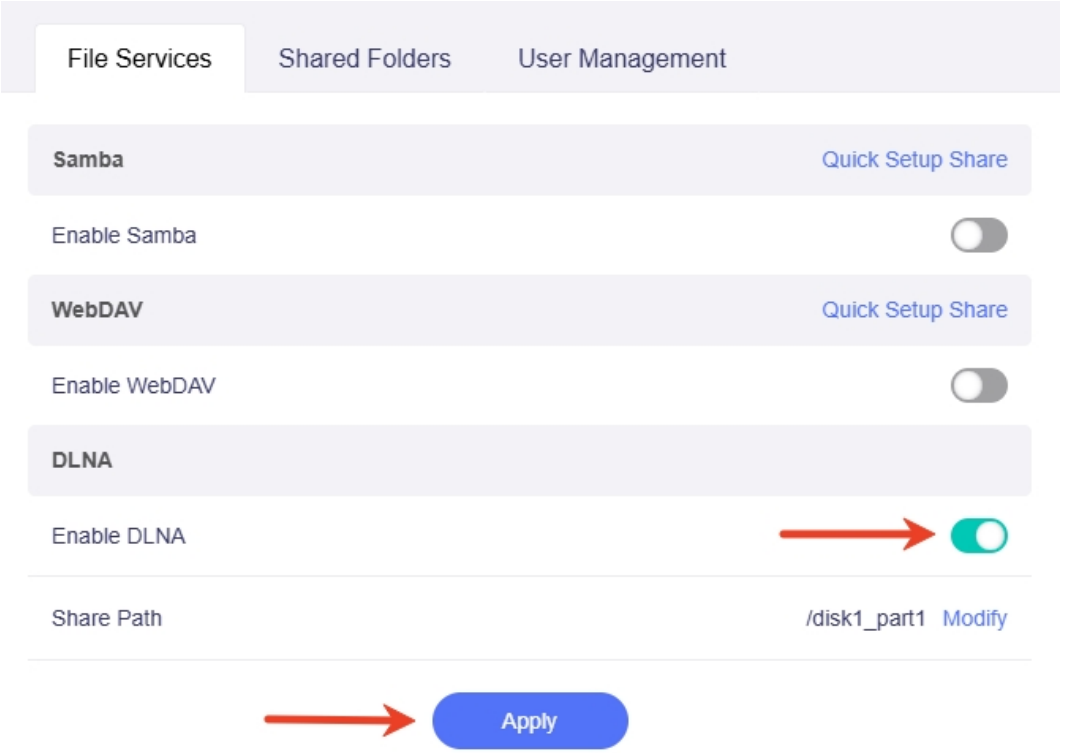
6. Uzyskaj łącze dostępu do folderu.
   Na stronie pojawią się łącza dla systemu Windows i systemów uniksopodobnych, takich jak Android, iOS, macOS, Ubuntu itp. Za ich pomocą można uzyskać dostęp do folderu udostępnionego przez usługę WebDAV.



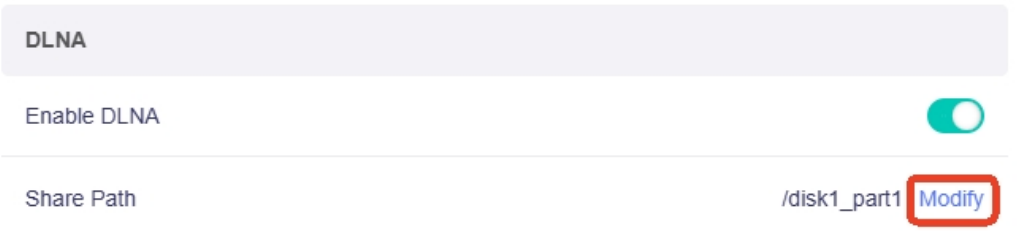
Uwaga: jeśli włączysz **Allow Access WebDAV from WAN** i uzyskujesz dostęp do folderu z sieci nadrzędnej, zastąp adres IP routera w łączu (domyślnie 192.168.8.1) jego adresem IP WAN. Znajdziesz go na stronie INTERNET w panelu administracyjnym.

13.3.4 Konfiguracja DLNA

1. W sekcji **File Services** włącz **Enable DLNA** i kliknij **Apply**.



2. W razie potrzeby zmień Share Path po prawej stronie.



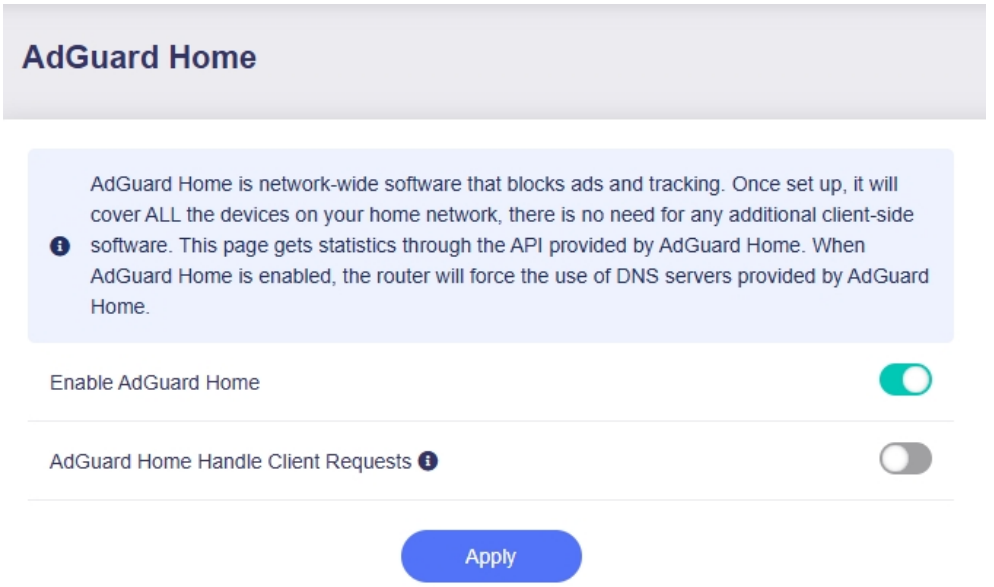
Podłącz telewizor Smart TV do routera. Automatycznie wykryje serwer DLNA.

13.4 AdGuard Home

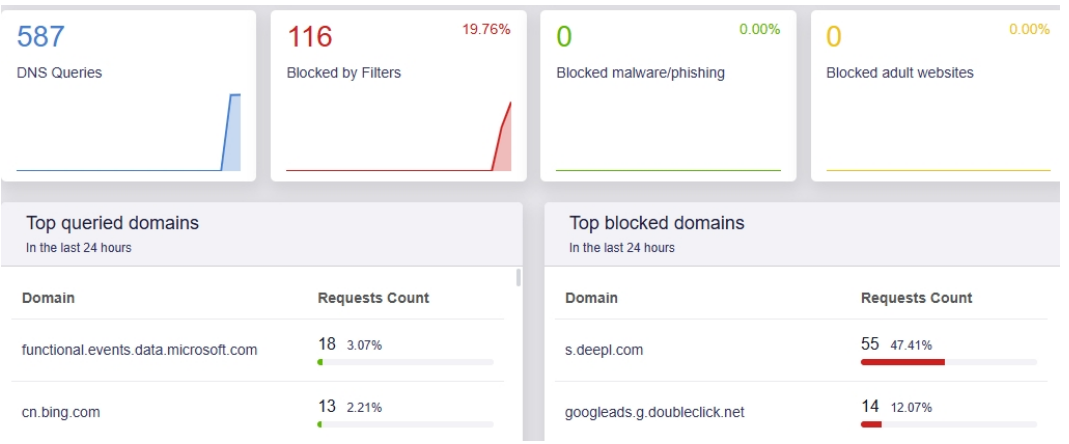
AdGuard Home to oprogramowanie blokujące reklamy i śledzenie w całej sieci. Po konfiguracji obejmuje wszystkie urządzenia klienckie bez konieczności instalowania na nich dodatkowego oprogramowania.

Aby skonfigurować AdGuard Home, wykonaj poniższe czynności.

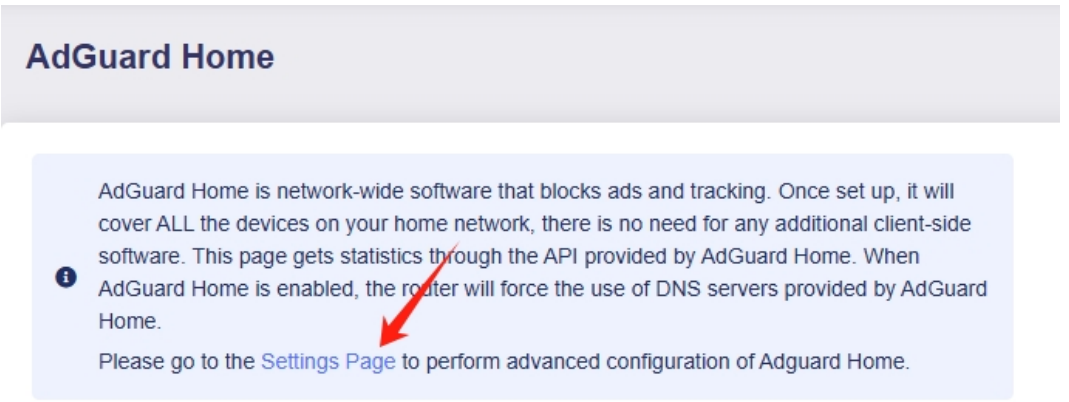
1. Zaloguj się do panelu administracyjnego routera i przejdź do **APPLICATIONS** > **AdGuard Home**. Włącz **Enable AdGuard Home** i kliknij **Apply**.



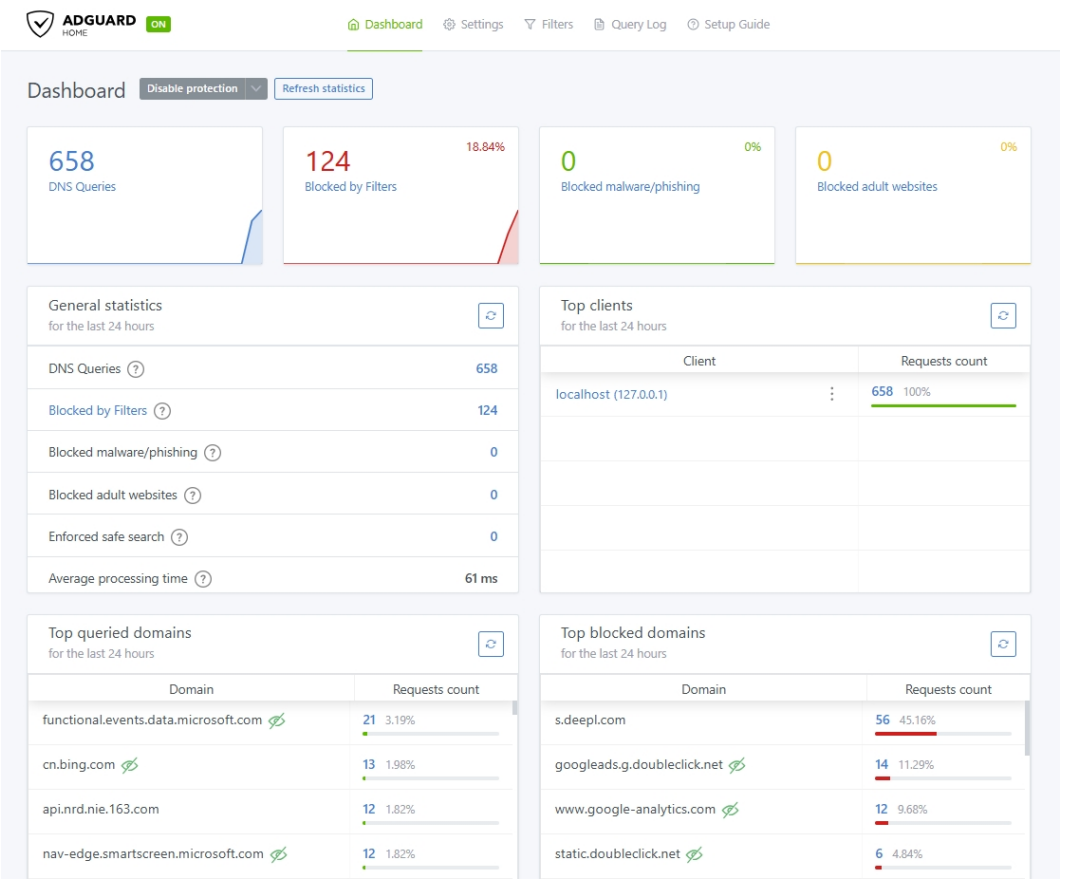
   - **AdGuard Home Handles Client Requests**: po włączeniu zapytania DNS urządzeń klienckich są obsługiwane bezpośrednio przez AdGuard Home, ale powoduje to niedziałanie reguł VPN opartych na domenach.
2. Strona automatycznie pobiera statystyki DNS (zapytania, zablokowane domeny itp.) przez API udostępniane przez AdGuard Home.



3. Kliknij **Settings Page**, aby skonfigurować zaawansowane ustawienia AdGuard Home.



4. Otworzy się strona ustawień AdGuard Home. Aby uzyskać pomoc, odwiedź [Centrum pomocy AdGuard Home].


ADGUARD HOME
ON
Dashboard
Settings
Filters
Query Log
Setup Guide
Dashboard
Disable protection
Refresh statistics
658
DNS Queries
124
18.84%
Blocked by Filters
0
0%
Blocked malware/phishing
0
0%
Blocked adult websites
General statistics
for the last 24 hours
DNS Queries 658
Blocked by Filters 124
Blocked malware/phishing 0
Blocked adult websites 0
Enforced safe search 0
Average processing time 61 ms
Top clients
for the last 24 hours
Client
Requests count
localhost (127.0.0.1) 658 100%
Top queried domains
for the last 24 hours
Domain
Requests count
functional.events.data.microsoft.com 21 3.19%
cn.bing.com 13 1.98%
api.nrd.nie.163.com 12 1.82%
nav-edge.smartscreen.microsoft.com 12 1.82%
Top blocked domains
for the last 24 hours
Domain
Requests count
s.deepl.com 56 45.16%
googleads.g.doubleclick.net 14 11.29%
www.google-analytics.com 12 9.68%
static.doubleclick.net 6 4.84%

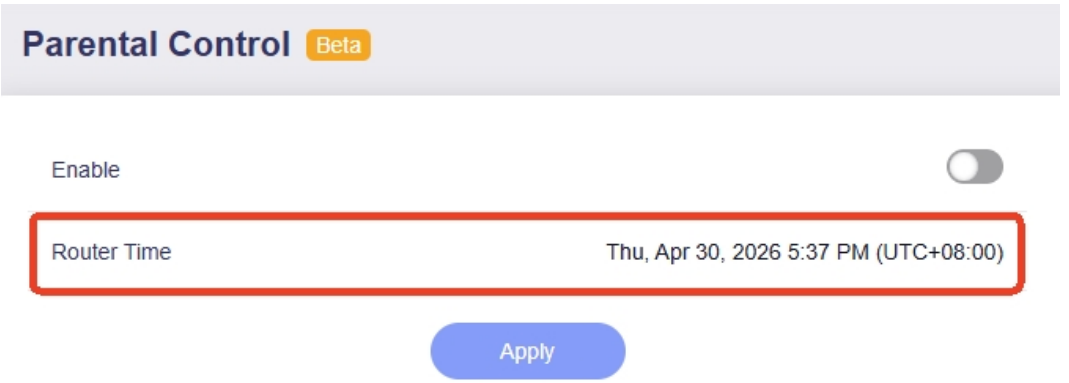
13.5 Kontrola rodzicielska

Kontrola rodzicielska pomaga chronić dzieci w Internecie przez blokowanie nieodpowiednich witryn i ograniczanie czasu korzystania z urządzeń. Zapobiega dostępowi do szkodliwych treści, ułatwia zarządzanie czasem przed ekranem i pomaga dzieciom odpowiedzialnie korzystać z Internetu.

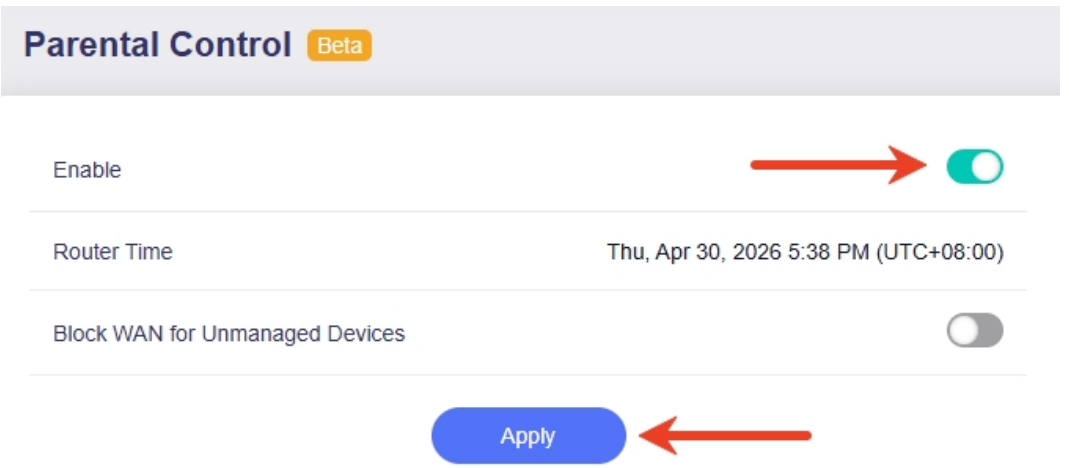
13.5.1 Szybka konfiguracja

Aby skonfigurować kontrolę rodzicielską na routerach GL.iNet, wykonaj poniższe czynności.

1. Zaloguj się do panelu administracyjnego routera i przejdź do **APPLICATIONS** > **Parental Control.** Upewnij się, że czas routera jest prawidłowy. Jeśli nie, najpierw przejdź do **SYSTEM** > **Time Zone**, aby go zsynchronizować.



2. Włącz kontrolę rodzicielską i kliknij **Apply**. Następnie skonfiguruj ją zgodnie z kreatorem. Film instruktażowy znajdziesz również tutaj.



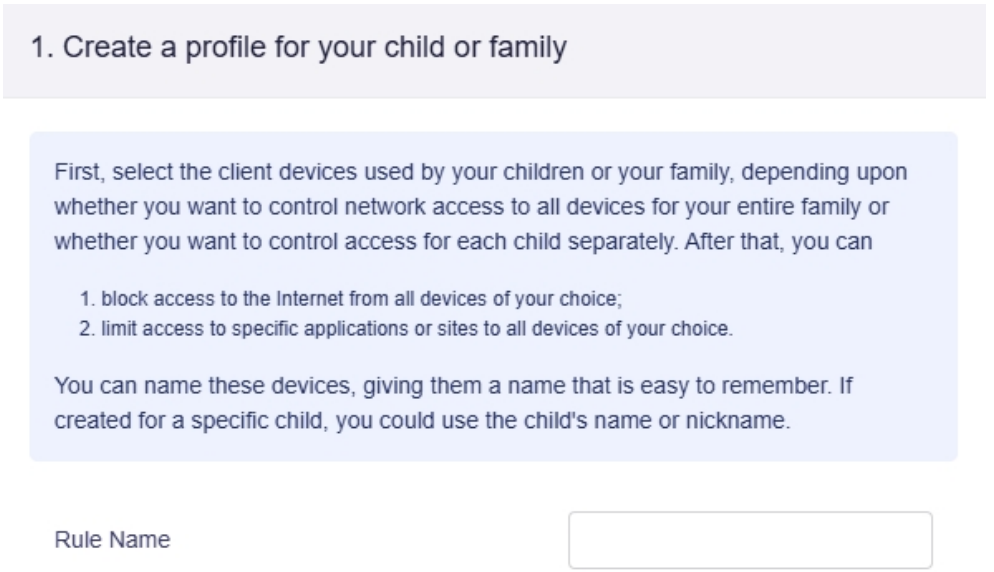
- **Block WAN for Unmanaged Devices**: blokuje dostęp do Internetu wszystkim urządzeniom, których nie ma na liście kontroli rodzicielskiej.

Poniżej przedstawiono przykładowe zastosowanie.

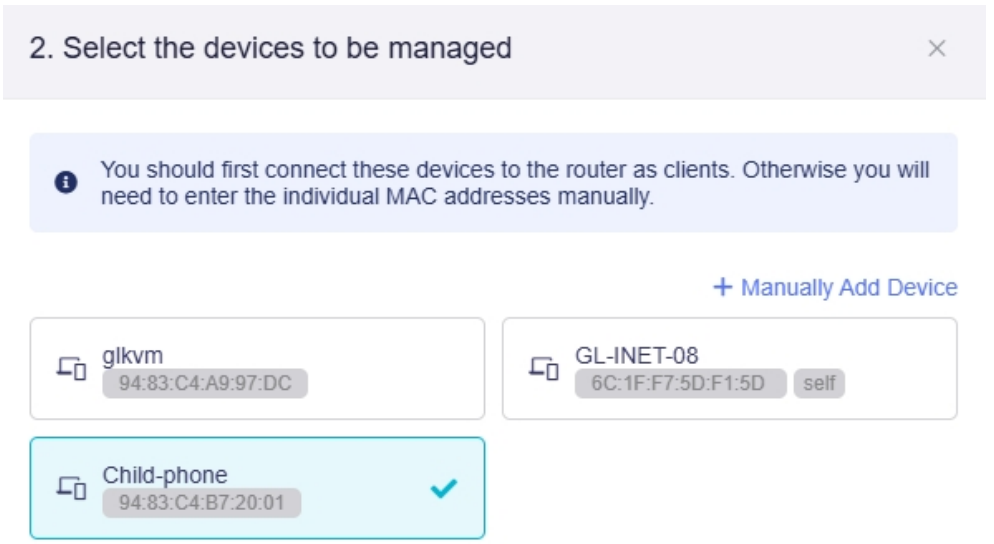
Scenariusz: urządzenia w tym profilu mogą korzystać z Internetu wyłącznie do nauki od 8:00 do 11:00 w dni robocze i do grania od 18:00 do 20:00 w weekendy. W pozostałych godzinach dostęp do Internetu jest domyślnie zablokowany.

Etapy konfiguracji:

1. Utwórz profil i nadaj mu nazwę.

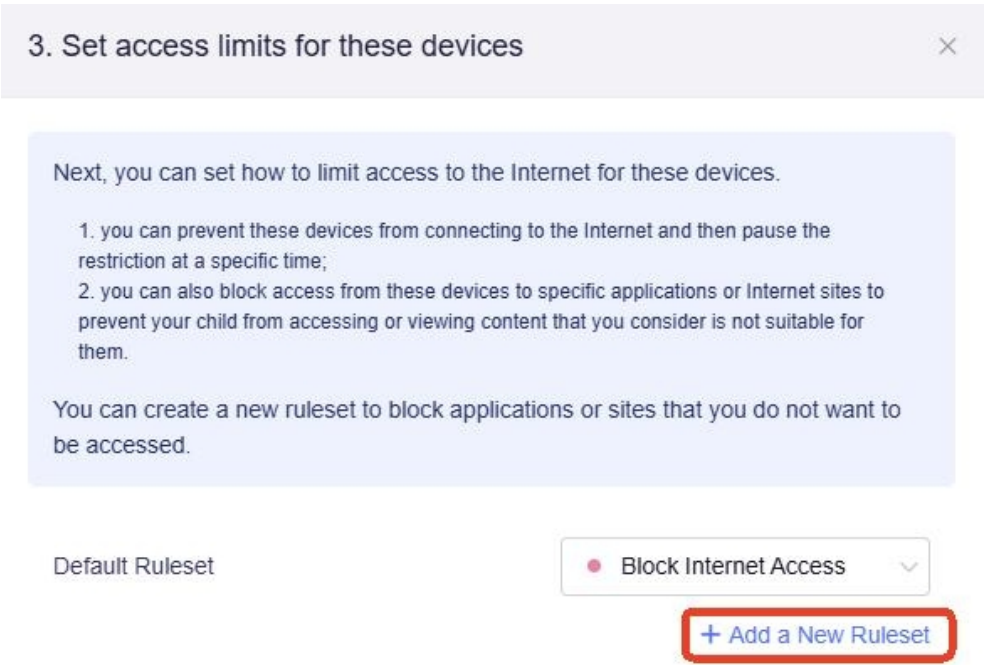


2. Wybierz urządzenia, którymi chcesz zarządzać. Najpierw podłącz je do routera. Jeśli nie były jeszcze podłączane, dodaj je ręcznie, wprowadzając ich adresy MAC.

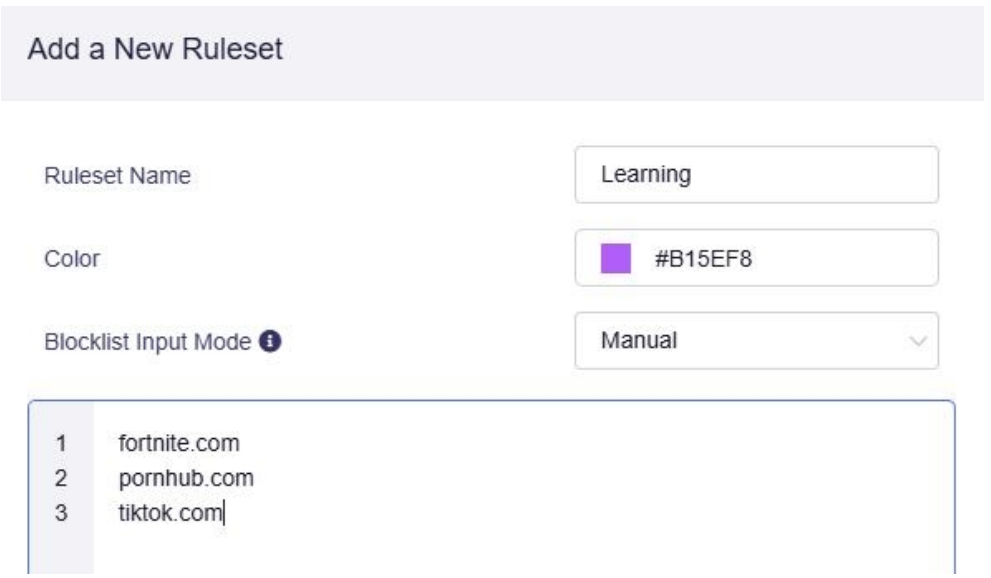


3. Ustaw ograniczenia dostępu.

Dostępne są dwa domyślne zestawy reguł: **Block Internet Access** i **No Limit**.
Kliknij **Add a New Ruleset**, aby utworzyć dwa dodatkowe zestawy reguł do późniejszego użycia: **Learning** i **Play**.

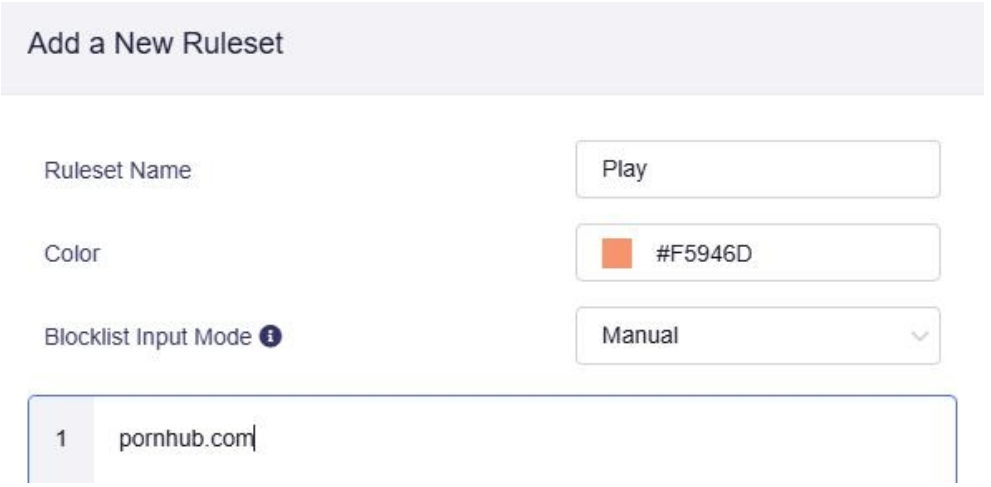


Określ nazwę zestawu reguł (np. Learning) i kolor, wprowadź witryny do zablokowania, a następnie kliknij **Apply**.

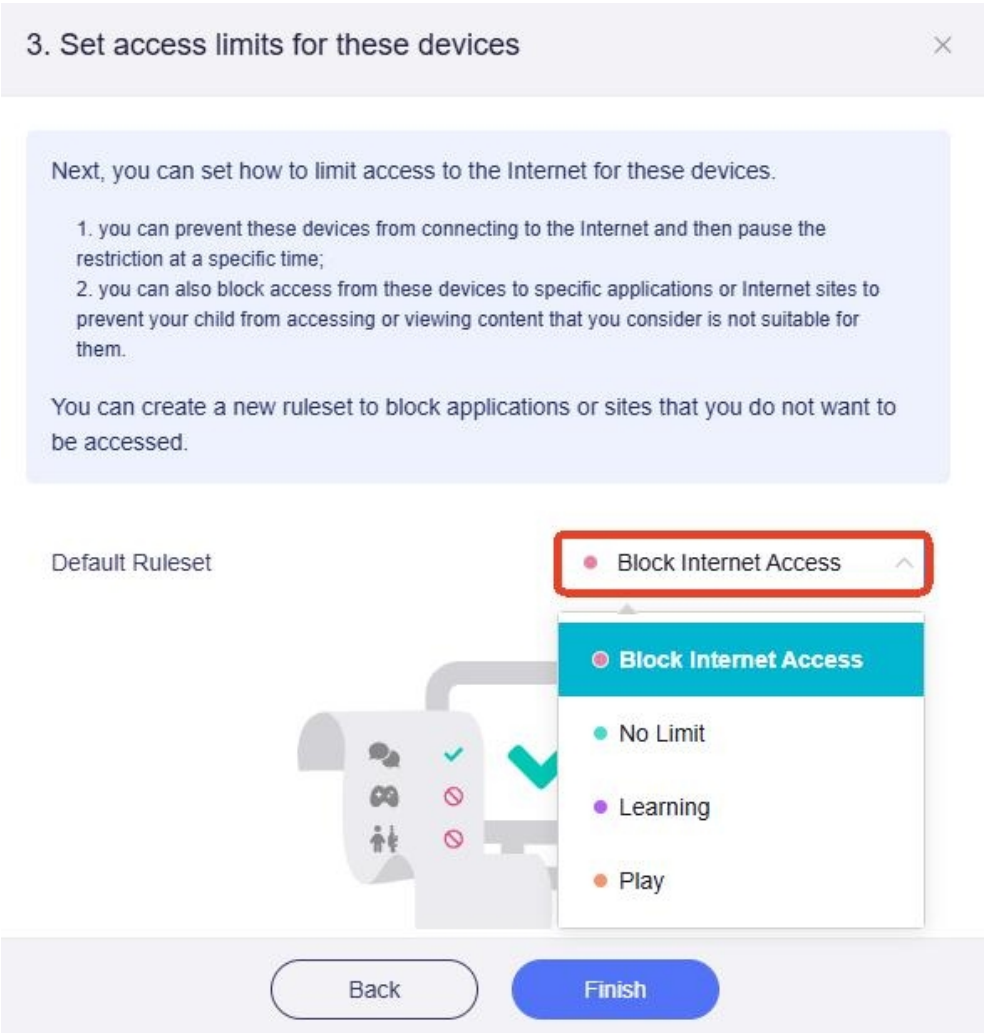


Uwaga: nazwy domen dodane do listy blokowanych obejmują również ich subdomeny. Na przykład wpis „example.com” obejmuje także każdą subdomenę, np. „subdomain.example.com”.

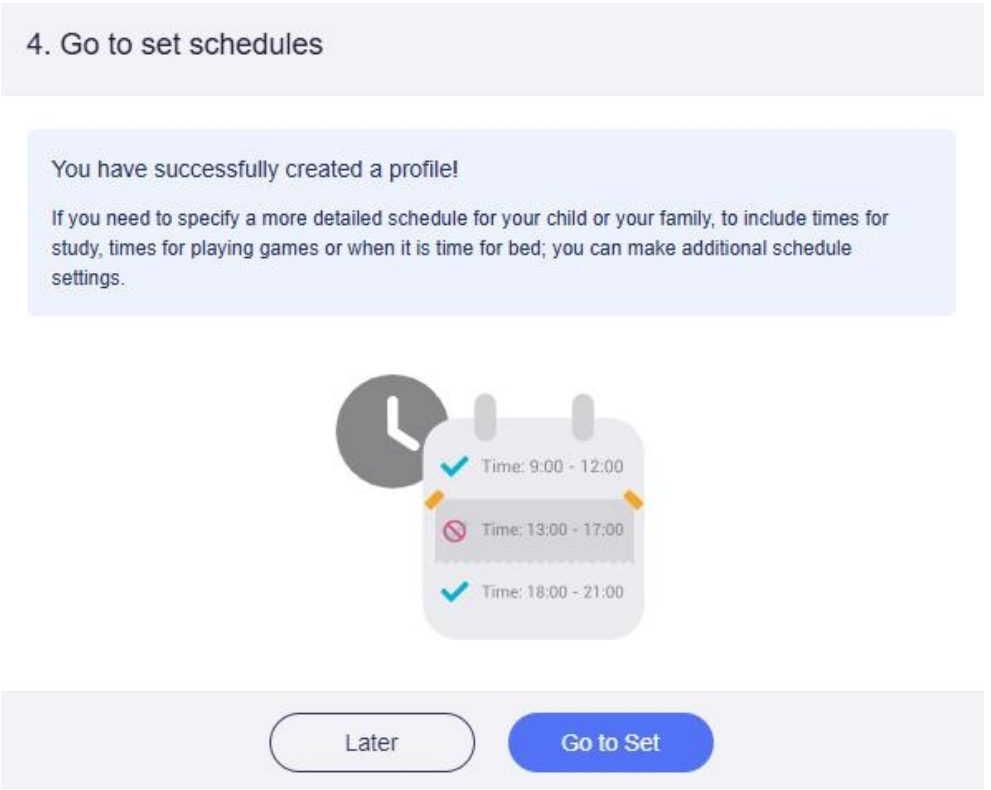
Podobnie utwórz drugi zestaw reguł. Określ jego nazwę (np. Play) i kolor, wprowadź witryny do zablokowania, a następnie kliknij **Apply**.



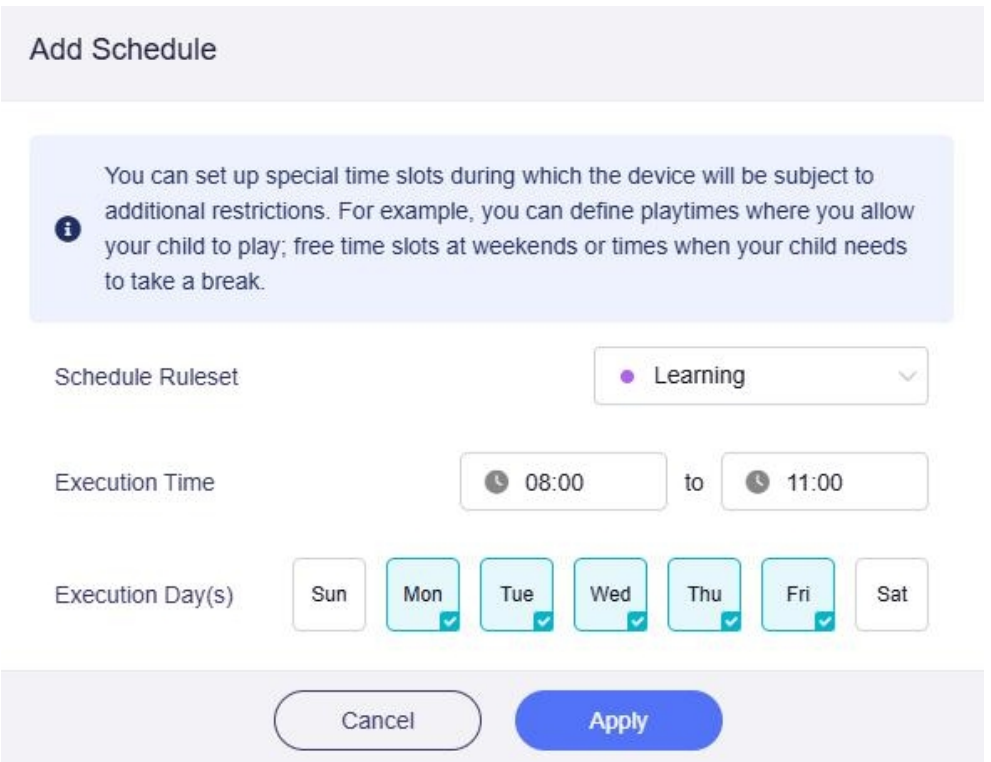
Po zastosowaniu ustawień dostępne będą cztery zestawy reguł. Wybierz **Block Internet Access** jako **Default Ruleset** i kliknij **Finish**.



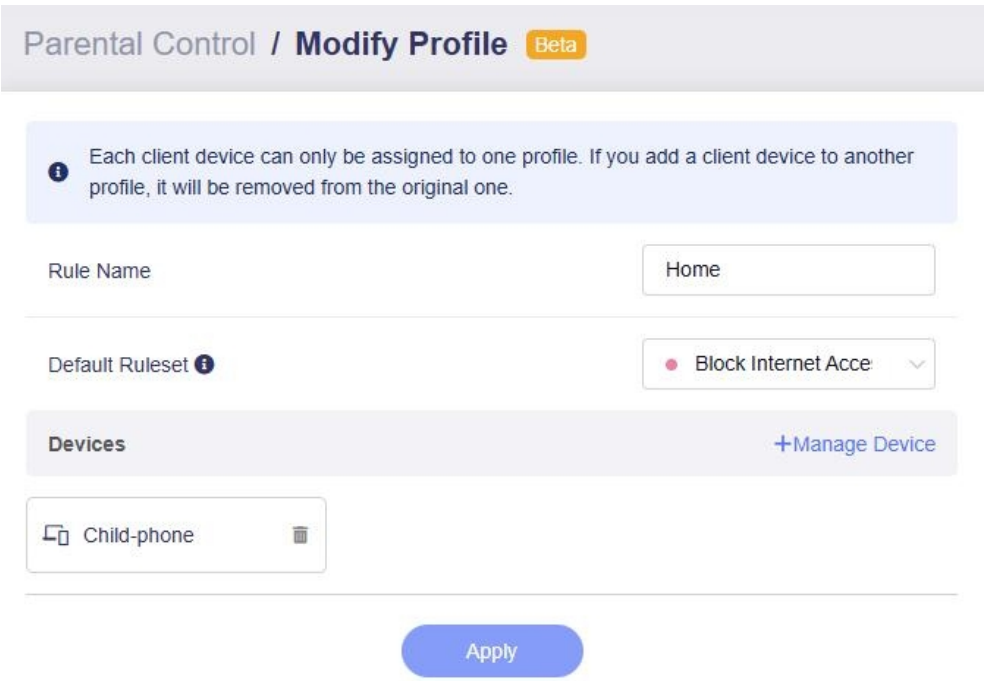
4. Następnie ustaw harmonogram profilu. Kliknij **Go to Set**.



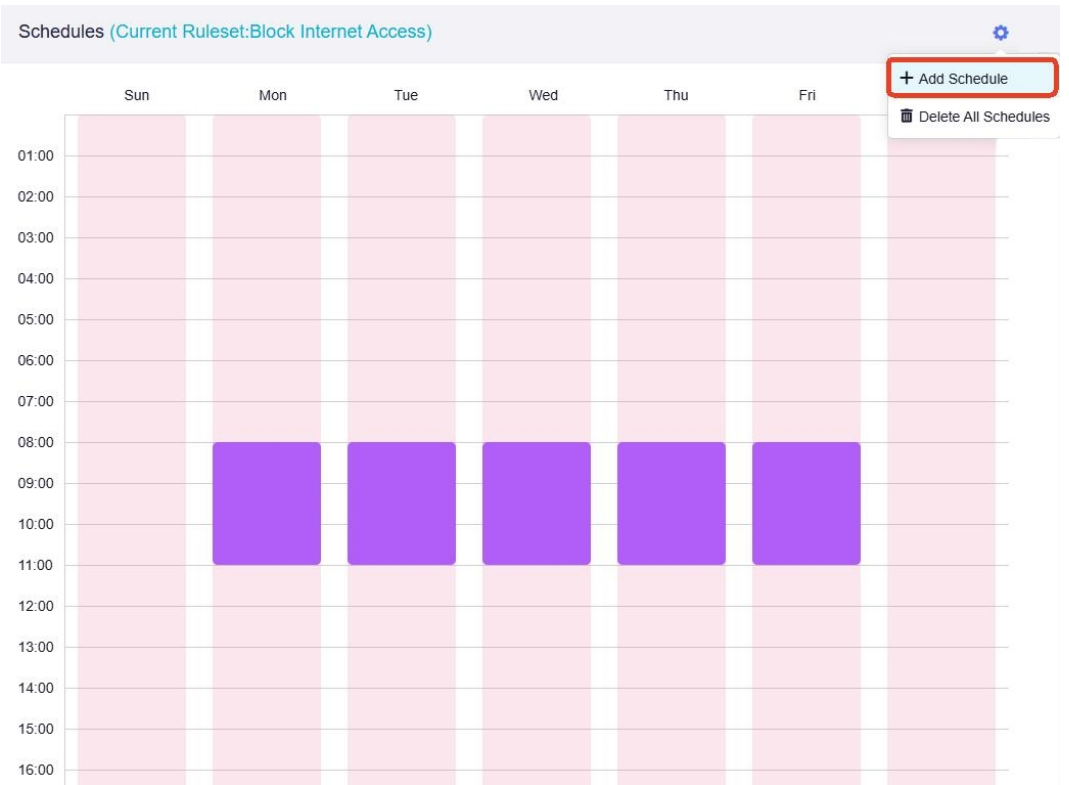
Dodaj zestaw reguł **Learning** do harmonogramu. Ustaw **Execution Time** od 8:00 do 11:00 w dni robocze, a następnie kliknij **Apply**.



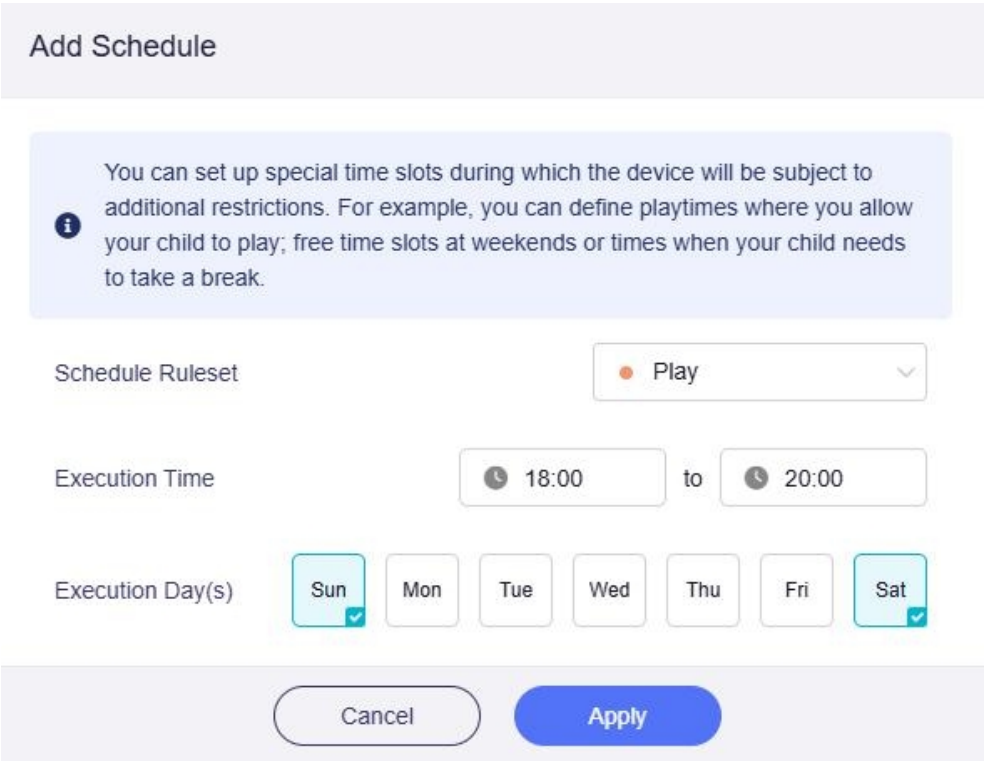
5. Otworzy się strona edycji utworzonego profilu.



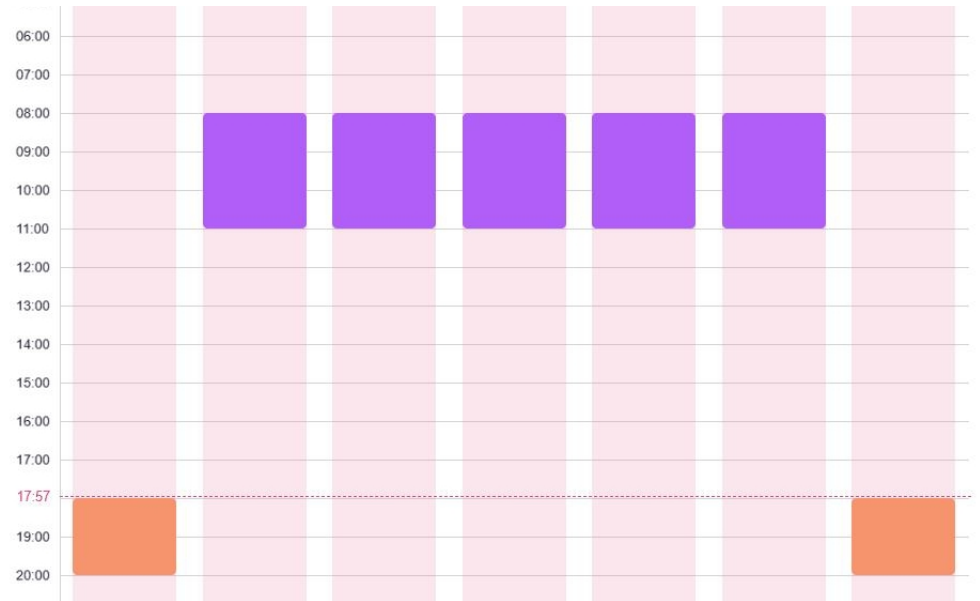
Przewiń w dół, aby zobaczyć utworzony harmonogram. Kliknij ikonę koła zębatego w prawym górnym rogu i wybierz **Add Schedule**.



6. Dodaj do harmonogramu drugi zestaw reguł, **Play**. Ustaw **Execution Time** od 18:00 do 20:00 w weekendy, a następnie kliknij **Apply**.



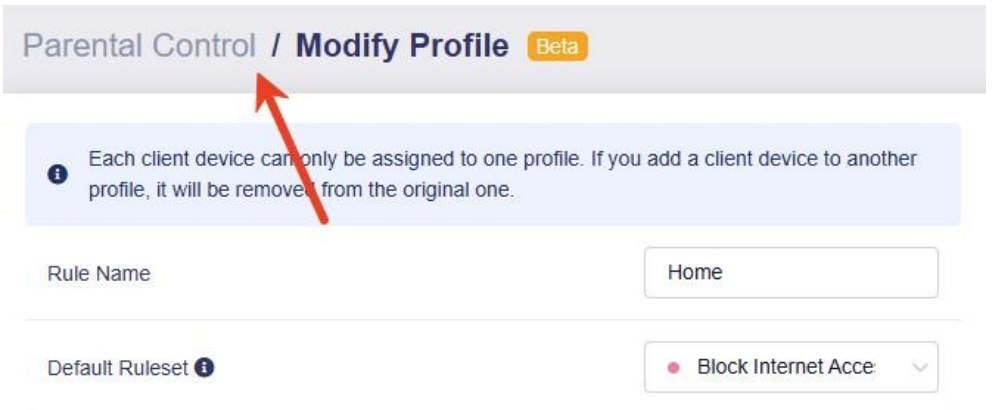
Zestaw reguł Play zostanie dodany do harmonogramu.



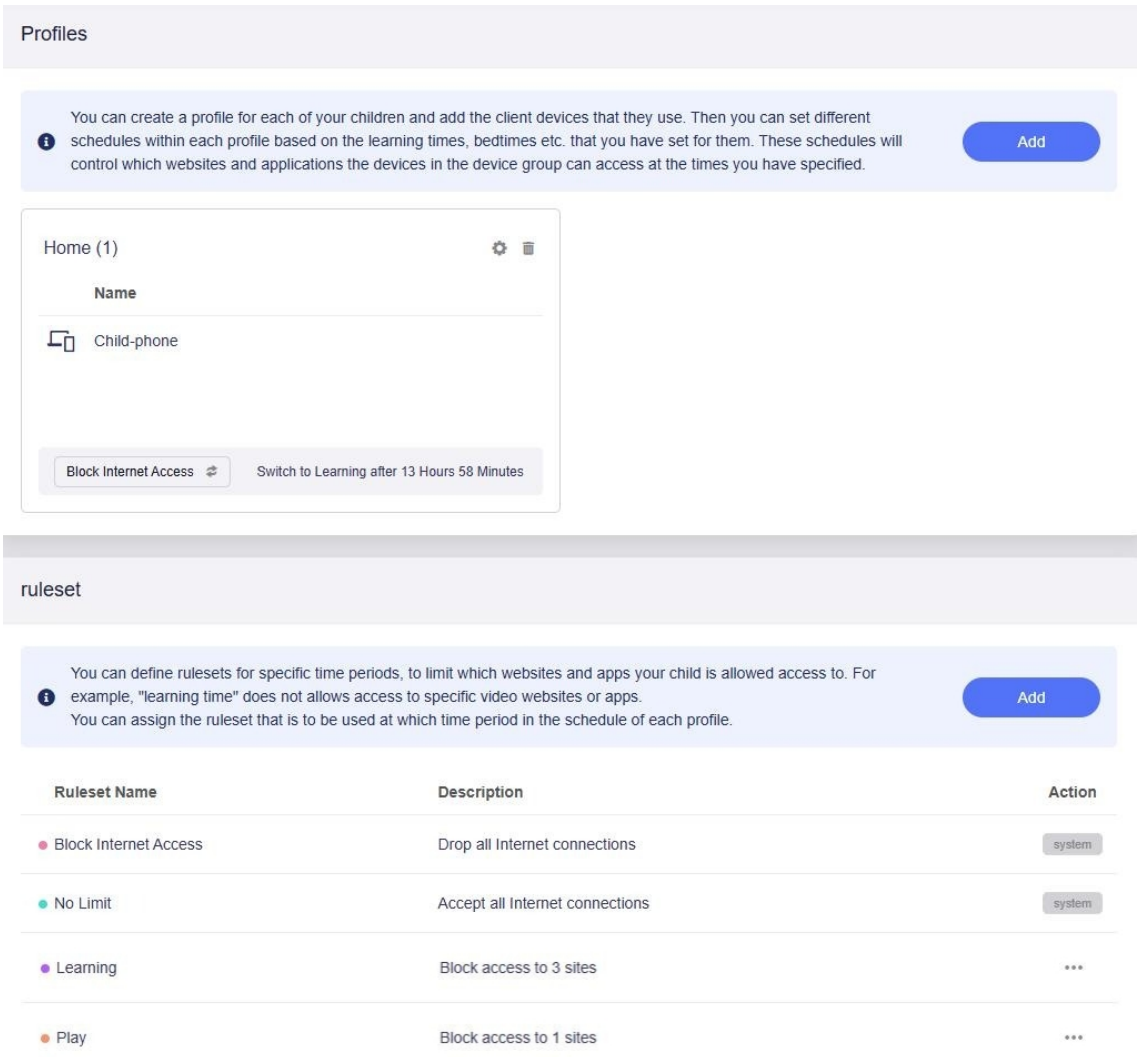
Wskazówki:

- Czerwona linia przerywana wskazuje bieżący czas.
- Aby zmienić czas obowiązywania, kliknij odpowiedni zestaw reguł w harmonogramie.

7. Kliknij **Parental Control** u góry, aby wrócić do strony kontroli rodzicielskiej.



Pojawi się końcowa konfiguracja. Kontrola rodzicielska działa teraz zgodnie z harmonogramem. W razie potrzeby możesz zmieniać istniejące profile i zestawy reguł lub dodawać nowe.



13.5.2 Rozwiązywanie problemów

Jeśli skonfigurowane ustawienia nie działają, sprawdź poniższe możliwe przyczyny.

1. Problem z pamięcią podręczną DNS.
   Przeglądarki i systemy operacyjne przechowują pamięć podręczną DNS, co może opóźniać zastosowanie zmian konfiguracji. Wyczyść ją, aby natychmiast zastosować zmiany.
2. Harmonogram profilu jeszcze się nie rozpoczął.
3. Wprowadzona nazwa domeny może być nieprawidłowa.
   Publiczną domenę witryny łatwo znaleźć, ale domeny API używane przez aplikacje często nie są publicznie udostępniane. Aby znaleźć właściwą domenę, użyj narzędzia do przechwytywania pakietów, np. Wireshark, lub wyszukaj odpowiednie informacje o domenie.
   Na przykład przy blokowaniu „www.google.com” wpisanie „google.com” daje lepsze wyniki niż „www.google.com”.
4. Urządzenie docelowe używa losowego adresu MAC przy każdym połączeniu z siecią, co uniemożliwia działanie reguł dostępu. Wyłącz losowanie adresu MAC na tym urządzeniu, a następnie ponownie dodaj je do profilu.

13.6 Tailscale

Tailscale to usługa VPN zapewniająca bezpieczny i łatwy dostęp do osobistych urządzeń i aplikacji z dowolnego miejsca na świecie. Szczegóły znajdziesz tutaj.

Funkcja Tailscale w routerach GL.iNet pozwala dołączyć router do wirtualnej sieci Tailscale, umożliwiając zdalny dostęp do routera oraz zasobów po jego stronie WAN i LAN.

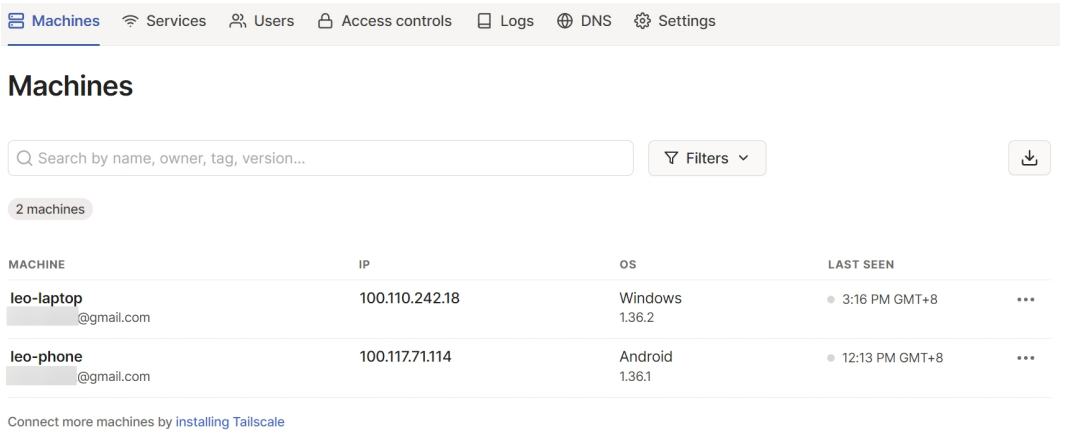
Uwaga:

1. Ponieważ Tailscale bazuje na WireGuard, nie zaleca się używania go jednocześnie z następującymi funkcjami lub usługami ze względu na możliwość konfliktów routingu: OpenVPN Client, WireGuard Client, GoodCloud Site to Site, ZeroTier i AstroWarp.
2. Ta funkcja jest obecnie w fazie beta i może zawierać błędy.
3. Routerów GL.iNet nie można jeszcze używać jako węzłów wyjściowych.

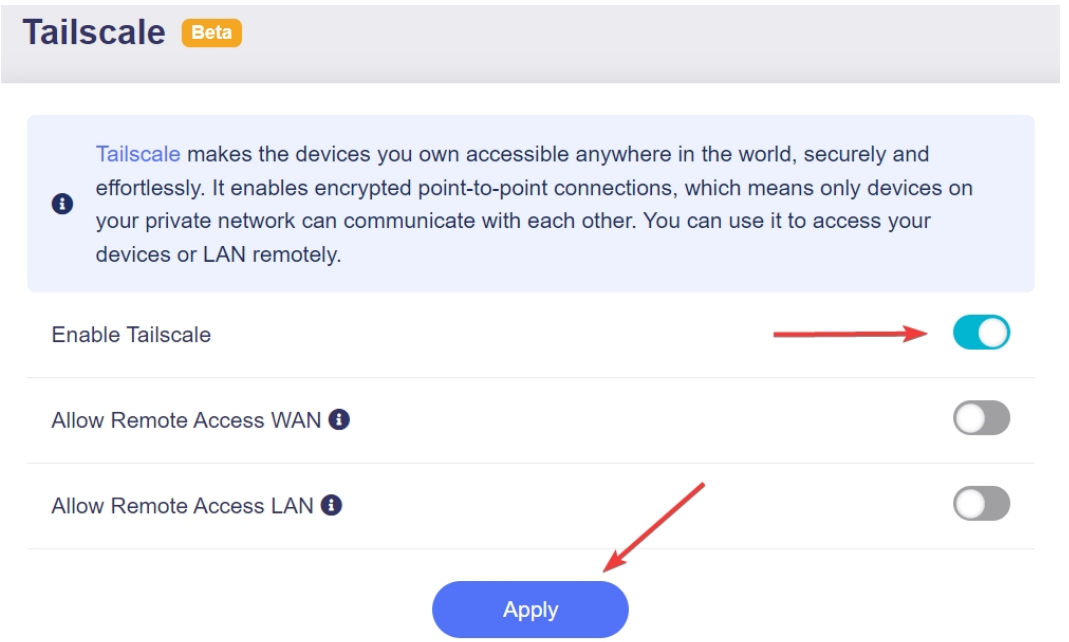
13.6.1 Konfiguracja Tailscale

Poniżej przedstawiono przykład konfiguracji sieci Tailscale na GL-MT2500.

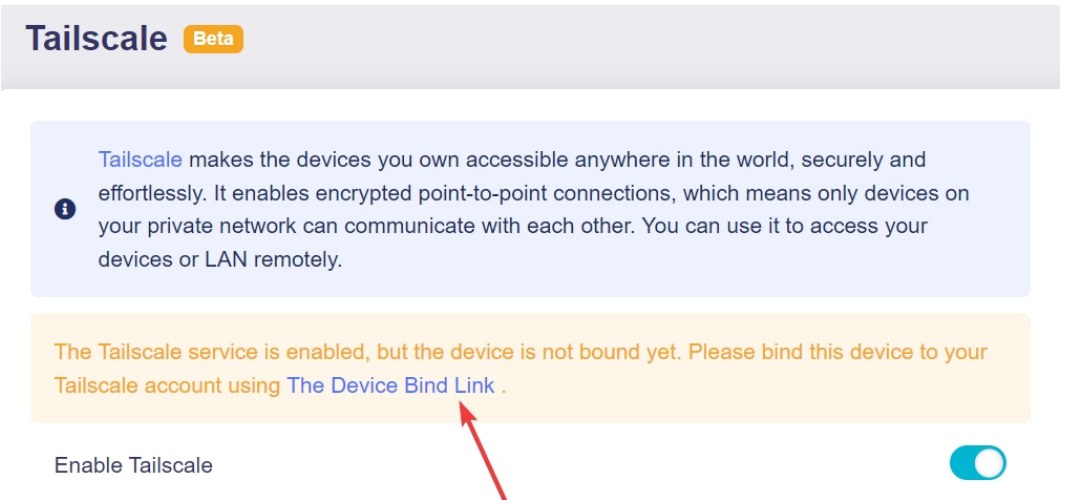
1. Najpierw zarejestruj konto Tailscale i powiąż z nim jedno lub dwa urządzenia do testów. Po powiązaniu zobaczysz je w konsoli Tailscale.



2. Zaloguj się do panelu administracyjnego routera i przejdź do **APPLICATIONS** > **Tailscale**. Włącz **Enable Tailscale** i kliknij **Apply**.



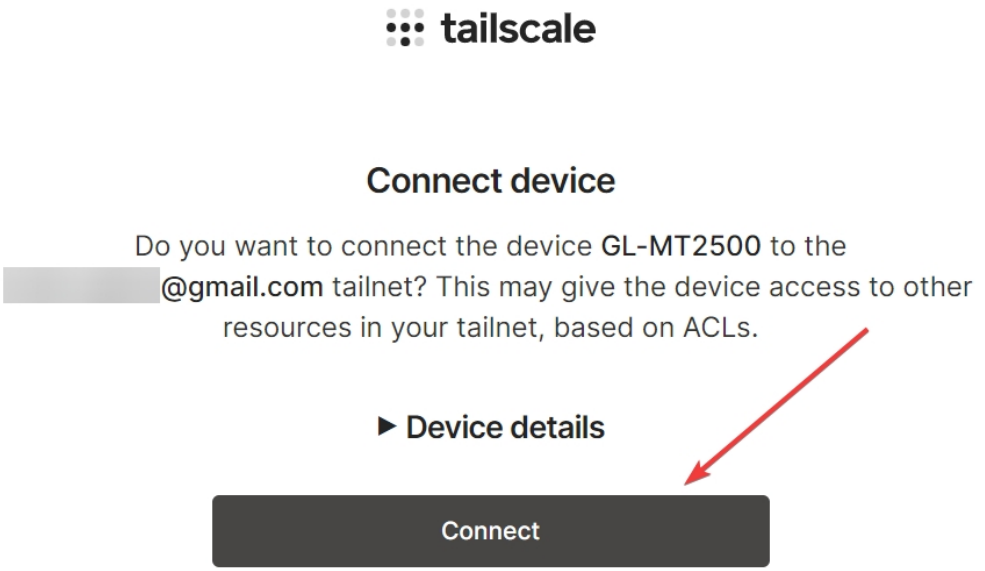
3. Strona poprosi o powiązanie urządzenia. Kliknij **Device Bind Link**.



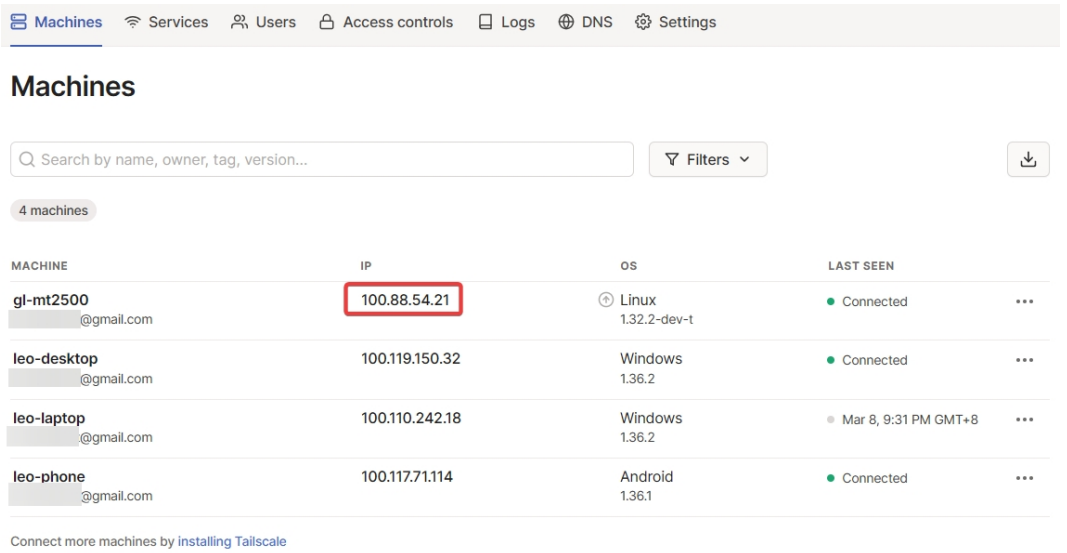
4. W wyświetlonym oknie kliknij łącze i zaloguj się na konto Tailscale.



5. Po zalogowaniu pojawi się prośba o potwierdzenie urządzenia. Kliknij **Connect**.



6. Nastąpi przekierowanie do konsoli administracyjnej Tailscale. Router został dodany do sieci wirtualnej Tailscale i można uzyskać do niego zdalny dostęp przez wirtualny adres IP Tailscale 100.88.54.21.

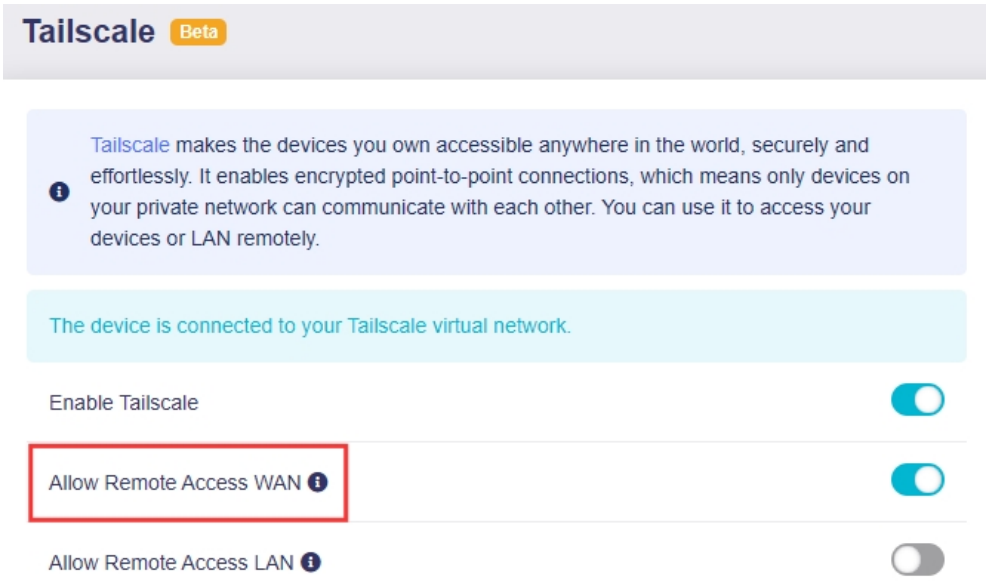


7. Sprawdź łączność.

   Na innym urządzeniu w tej samej sieci Tailscale otwórz przeglądarkę i wprowadź wirtualny adres IP routera w pasku adresu. Jeśli panel administracyjny jest dostępny, Tailscale działa prawidłowo. Aby sprawdzić łączność, możesz też użyć polecenia ping lub zalogować się przez SSH do terminala routera, korzystając z jego wirtualnego adresu IP.

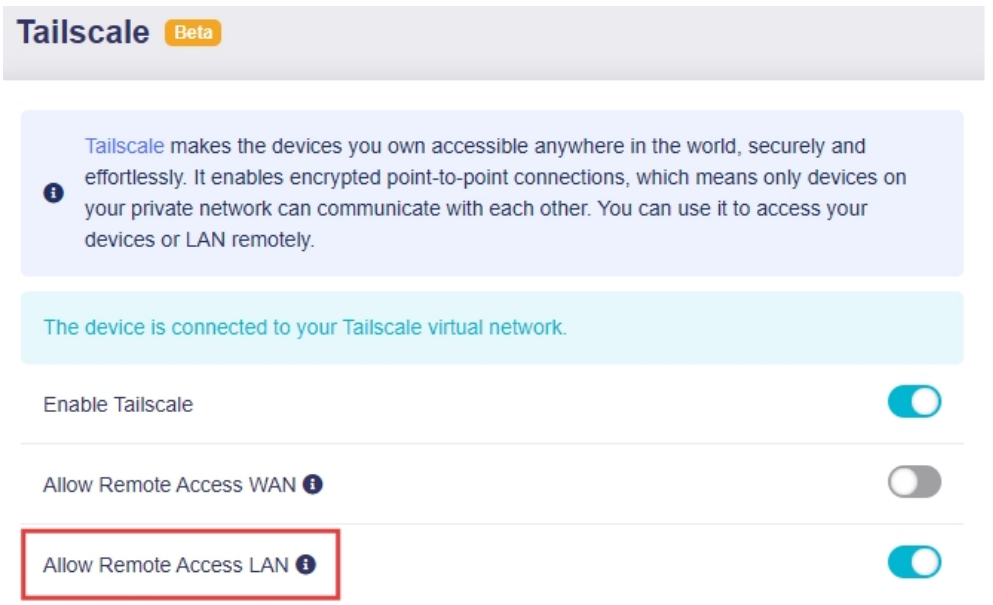
13.6.2 Zdalny dostęp do WAN

Po włączeniu tej opcji zasoby po stronie WAN urządzenia są dostępne przez wirtualną sieć Tailscale. Więcej informacji znajdziesz tutaj.



13.6.3 Zdalny dostęp do LAN

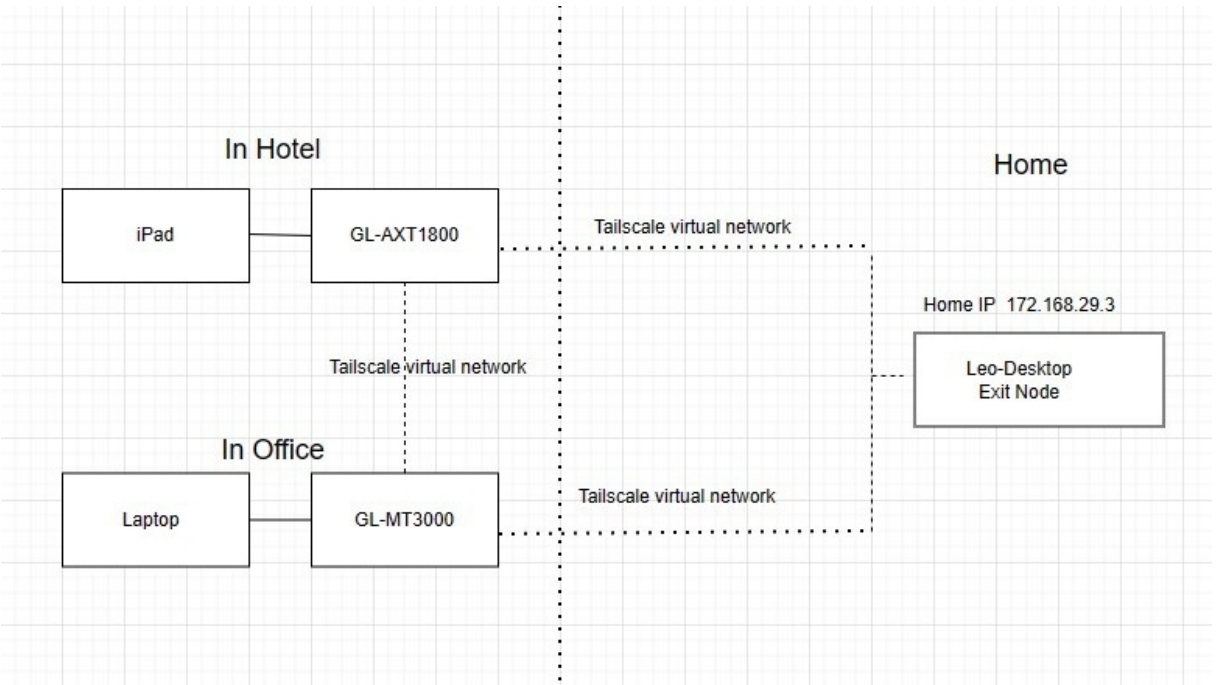
Po włączeniu tej opcji zasoby po stronie LAN urządzenia są dostępne przez wirtualną sieć Tailscale. Więcej informacji znajdziesz tutaj.



13.6.4 Niestandardowe węzły wyjściowe

Domyślnie Tailscale działa jako sieć nakładkowa: kieruje wyłącznie ruch między urządzeniami z Tailscale i nie obsługuje ruchu do publicznego Internetu, np. podczas przeglądania witryn takich jak Google.

Czasami jednak potrzebne jest kierowanie przez Tailscale ruchu do publicznego Internetu. Na przykład podczas pobytu poza domem lub podróży zagranicznej możesz potrzebować usług internetowych, np. bankowości, dostępnych tylko w kraju zamieszkania. W takim przypadku skonfiguruj domowy komputer z publicznym adresem IP jako węzeł wyjściowy i ustaw inne urządzenia w tej samej sieci Tailnet, np. GL-AXT1800 i GL-MT3000 na poniższej ilustracji, aby przesyłały ruch przez ten węzeł. Umożliwia to przekazywanie całego ruchu do publicznego Internetu przez węzeł wyjściowy.



Węzeł wyjściowy kieruje wychodzący ruch internetowy urządzeń Tailnet, pełniąc w praktyce funkcję serwera VPN. Po połączeniu z takim węzłem cały ruch internetowy niezwiązany z Tailscale jest widziany jako pochodzący z jego lokalizacji. Pomaga to uzyskiwać dostęp do treści z ograniczeniami geograficznymi i zwiększać prywatność w sieci. Urządzenie przekazujące ten ruch jest nazywane „węzłem wyjściowym”. Szczegóły znajdziesz tutaj.

Uwaga: jeśli serwer DNS routera ma prywatny adres IP dostępny wyłącznie w sieci lokalnej, po uruchomieniu węzłów wyjściowych możesz utracić dostęp do Internetu. Aby temu zapobiec, ręcznie ustaw na routerze publiczny serwer DNS (np. 8.8.8.8).

13.7 ZeroTier

ZeroTier to programowa wirtualna sieć prywatna (VPN) umożliwiająca bezpieczną, szyfrowaną komunikację między urządzeniami przez Internet. Tworzy prywatną sieć wirtualną, w której urządzenia komunikują się tak, jakby znajdowały się w tej samej sieci lokalnej, niezależnie od fizycznej lokalizacji i topologii sieci. ZeroTier zaprojektowano z myślą o łatwej konfiguracji i obsłudze. Oferuje szyfrowanie od końca do końca, segmentację sieci i tworzenie mostów sieciowych.

Funkcja ZeroTier w routerach GL.iNet pozwala dołączyć router do wirtualnej sieci ZeroTier, umożliwiając zdalny dostęp do routera oraz zasobów po jego stronie WAN i LAN.

Uwaga:

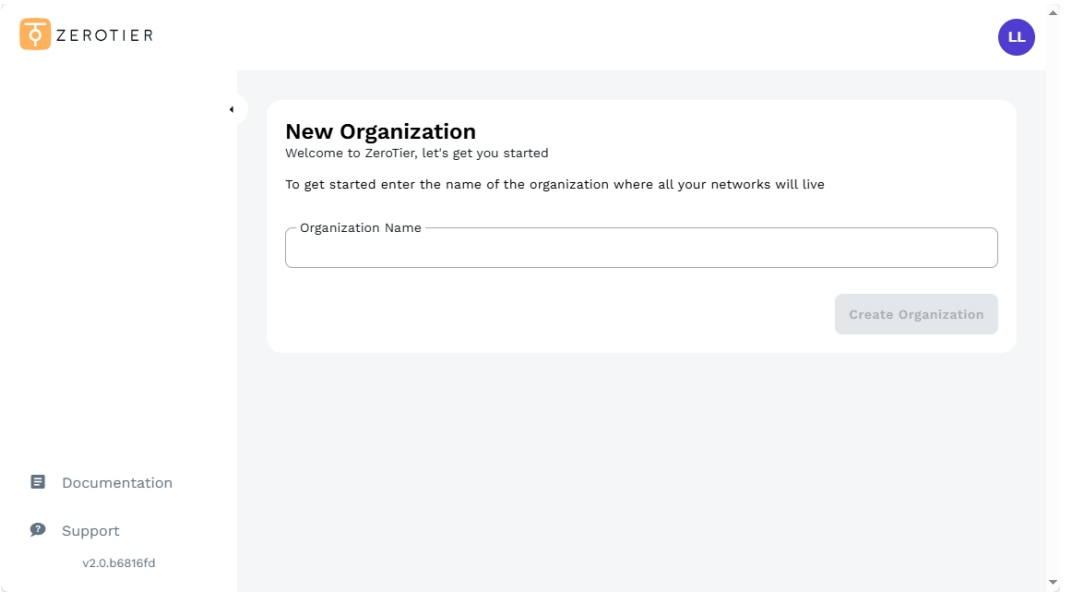
1. Nie zaleca się używania ZeroTier jednocześnie z następującymi funkcjami lub usługami ze względu na możliwość konfliktów routingu: OpenVPN Client, WireGuard Client, GoodCloud Site to Site, Tailscale i AstroWarp.
2. Ta funkcja jest obecnie w fazie beta i może zawierać błędy.

13.7.1 Konfiguracja ZeroTier

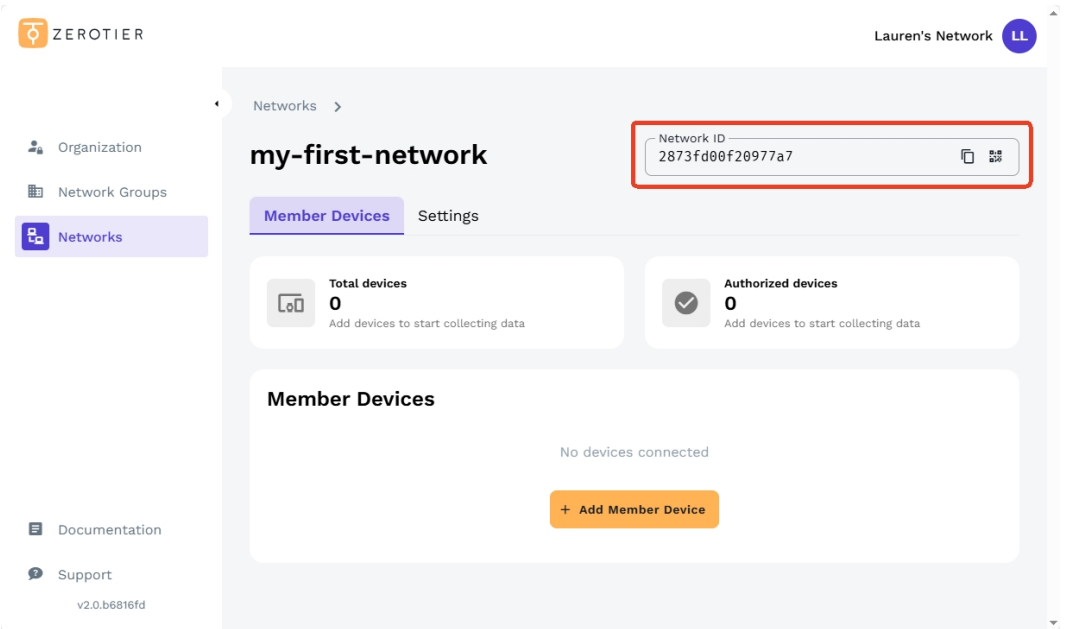
Dostępne są dwie wersje ZeroTier Central: New Central i Legacy Central.

W poniższych krokach jako przykład wykorzystano New Central.

1. Odwiedź oficjalną witrynę ZeroTier i zaloguj się na swoje konto.
2. Utwórz organizację.

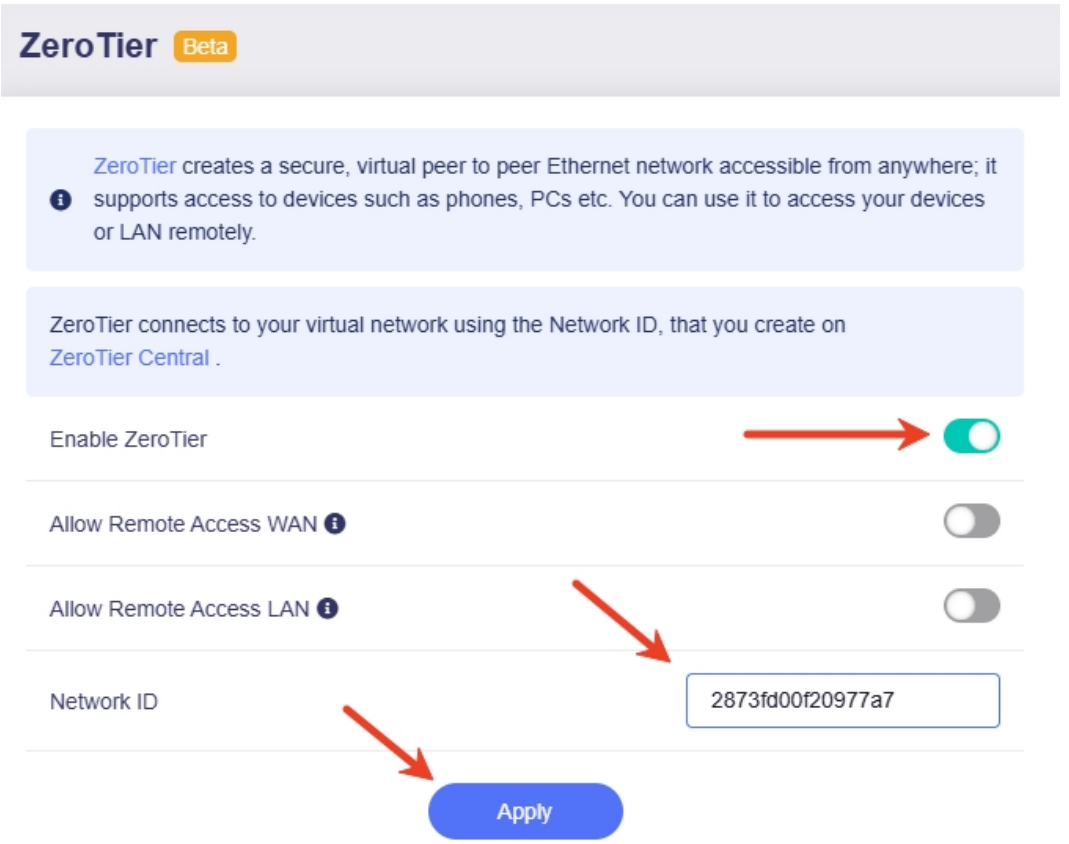


3. Wybierz plan. W tym przykładzie wybieramy **Personal plan**, obejmujący 10 urządzeń, 1 administratora sieci i 1 sieć. Aby tworzyć więcej sieci, dodawać więcej urządzeń lub niestandardowe trasy i DNS, wybierz inny płatny plan.
4. Sieć ZeroTier została utworzona.

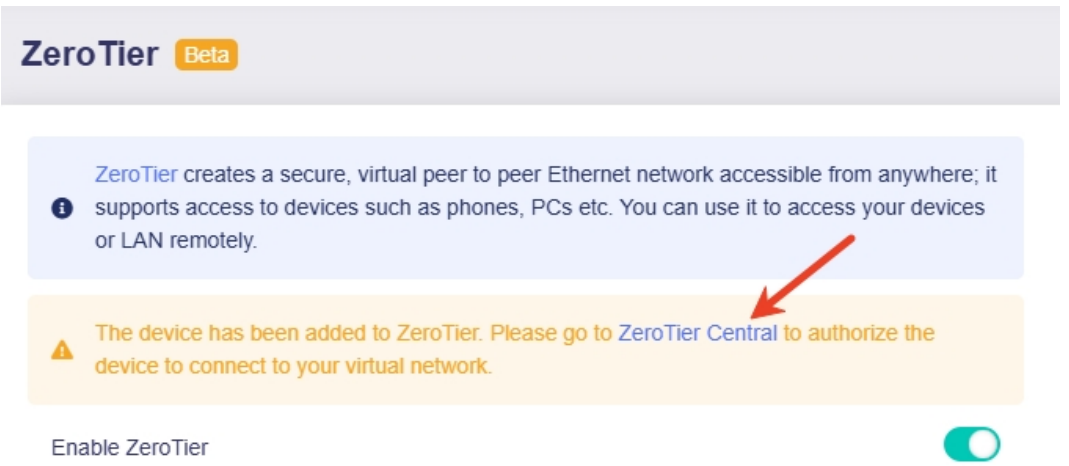


Zapisz **Network ID**, czyli 16-znakową kombinację liter i cyfr w prawym górnym rogu. Będzie potrzebna do późniejszego podłączania innych urządzeń.

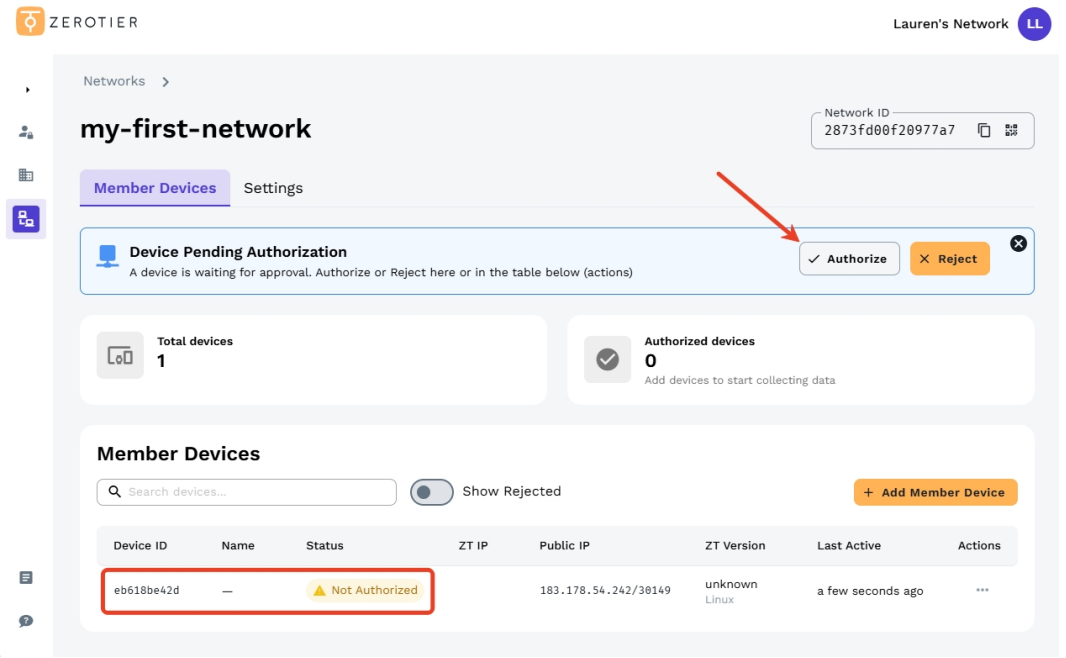
5. Zaloguj się do panelu administracyjnego routera i przejdź do **APPLICATIONS** -> **ZeroTier**. Włącz ZeroTier, wprowadź **Network ID** i kliknij **Apply**.



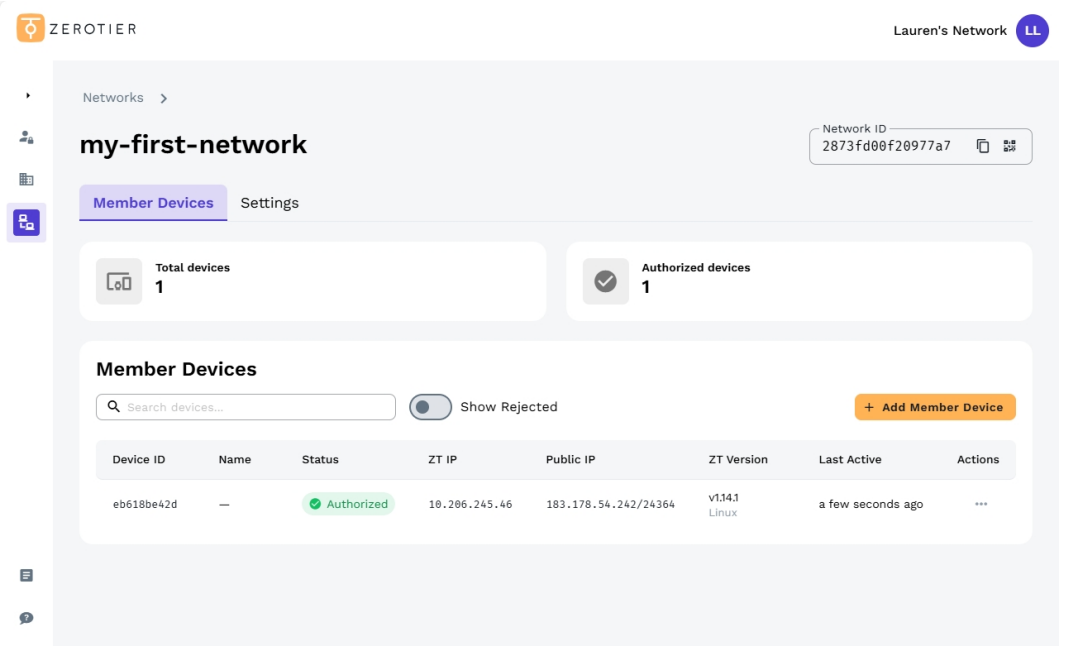
Po chwili na stronie pojawi się informacja o wymaganej autoryzacji. Kliknij hiperłącze **ZeroTier Central**, aby otworzyć ZeroTier Central.



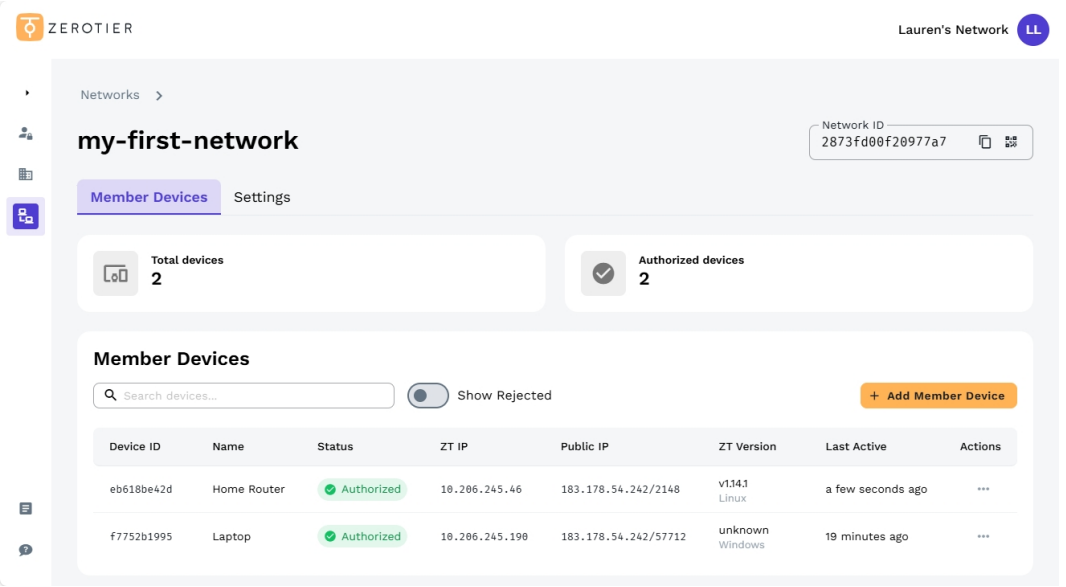
6. W ZeroTier Central znajdź oczekujące urządzenie i autoryzuj je.



Po autoryzacji strona będzie wyglądać jak poniżej.

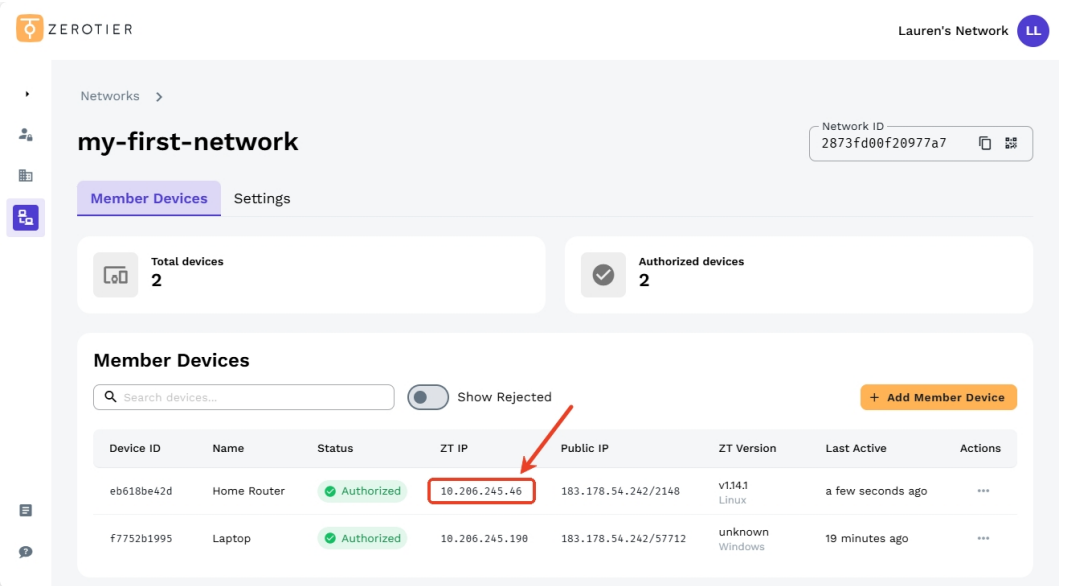


7. Dodaj kolejne urządzenie (np. komputer lub smartfon) do tej samej sieci ZeroTier zgodnie z tym poradnikiem. Po pomyślnym dodaniu strona będzie wyglądać jak poniżej. Pojawią się szczegóły urządzeń w sieci, takie **jak Device** ID**,** Name**,** Status, **Managed** IP i **Public IP**.



Wskazówka: kliknij ikonę trzech kropek po prawej stronie, aby zmienić ustawienia urządzenia w sieci, w tym nazwę, adresy Managed IP i ustawienia zaawansowane.

8. Kliknij adres Managed IP **routera,** aby go skopiować.



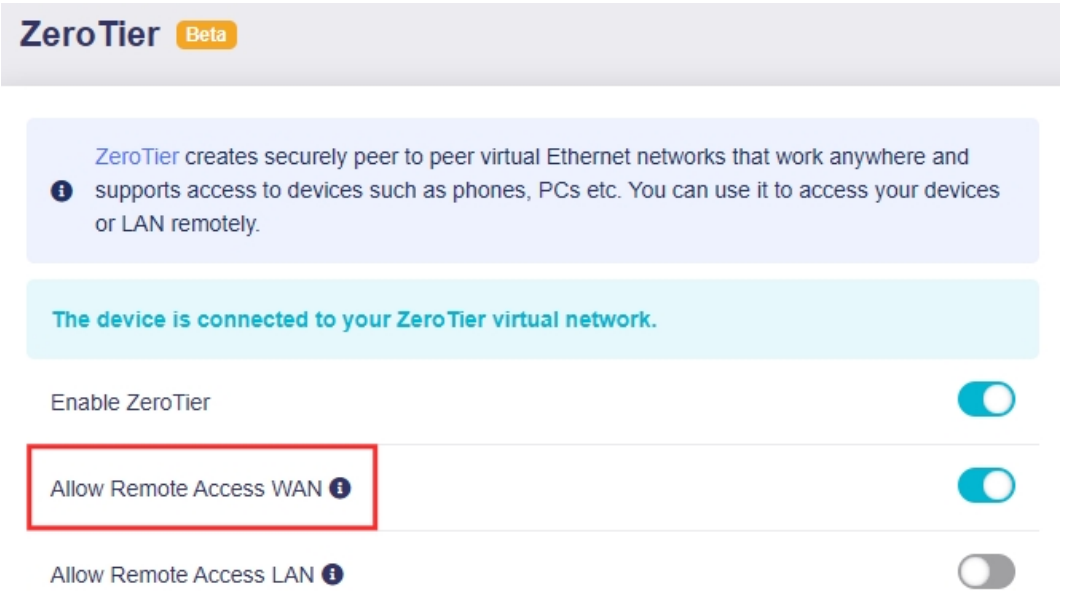
Możesz go następnie użyć do uzyskania dostępu do routera z laptopa w tej samej sieci ZeroTier.

9. Sprawdź łączność.

   Na laptopie podłączonym do tej samej sieci ZeroTier otwórz przeglądarkę i wprowadź adres Managed IP routera uzyskany w poprzednim kroku. Jeśli panel administracyjny routera jest dostępny, połączenie ZeroTier działa prawidłowo.

13.7.2 Zdalny dostęp do WAN

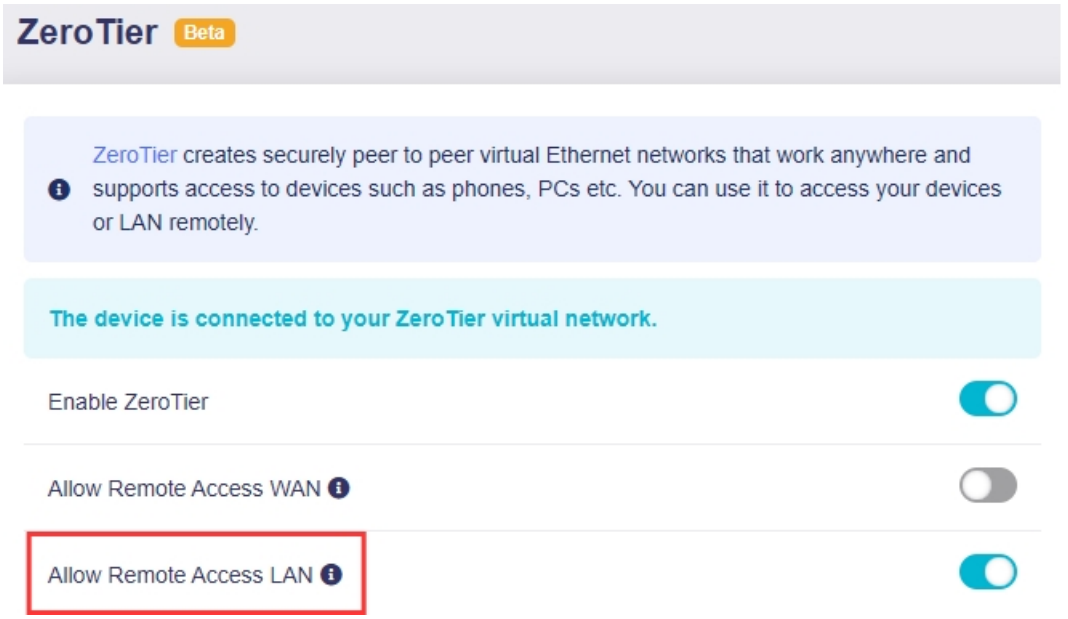
Po włączeniu tej opcji zasoby po stronie WAN urządzenia są dostępne przez wirtualną sieć ZeroTier. Więcej informacji znajdziesz tutaj.



Uwaga: aby ta funkcja działała, trzeba dodać reguły routingu do sieci ZeroTier. W Legacy Central można bezpłatnie dodać jedną niestandardową trasę, natomiast w New Central konfigurowanie takich tras jest dostępne dopiero w planie Essential lub wyższym. Szczegóły cenowe znajdziesz tutaj.

13.7.3 Zdalny dostęp do LAN

Po włączeniu tej opcji zasoby po stronie LAN urządzenia są dostępne przez wirtualną sieć ZeroTier. Więcej informacji znajdziesz tutaj.



Uwaga: aby ta funkcja działała, trzeba dodać reguły routingu do sieci ZeroTier. W Legacy Central można bezpłatnie dodać jedną niestandardową trasę, natomiast w New Central konfigurowanie takich tras jest dostępne dopiero w planie Essential lub wyższym. Szczegóły cenowe znajdziesz tutaj.

Rozdział 14

Sieć

W tym rozdziale przedstawiono ustawienia konfiguracji i zarządzania siecią, takie jak LAN, DNS i IPv6.

14.1 Przekierowanie portów

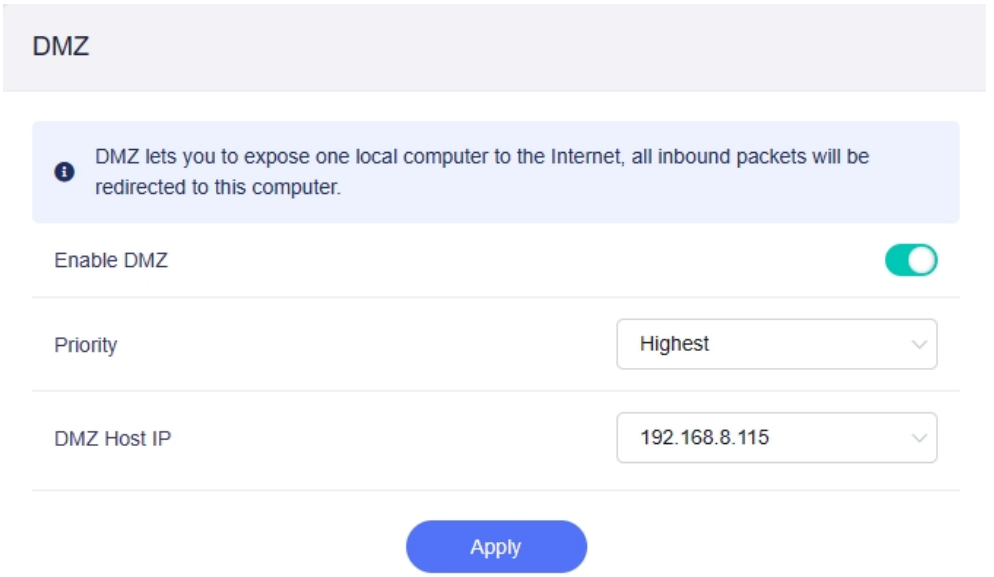
Przekierowanie portów to funkcja sieciowa kierująca żądania zewnętrzne do określonych urządzeń w sieci lokalnej. Strona Port Forwarding zawiera dwie główne funkcje: **DMZ** (bezpośredni pełny dostęp do jednego urządzenia) i **Port Forwarding** (dostęp do określonych portów urządzeń).

14.1.1 DMZ

DMZ umożliwia wystawienie jednego komputera do Internetu. Wszystkie pakiety przychodzące będą przekierowywane do tego komputera.

Aby w razie potrzeby włączyć DMZ, wykonaj poniższe czynności.

1. Zaloguj się do panelu administracyjnego routera i przejdź do sekcji **NETWORK** > **Port Forwarding** > **DMZ**.
2. Włącz **Enable DMZ**. Wybierz Priority i DMZ Host IP z list, a następnie kliknij **Apply**.



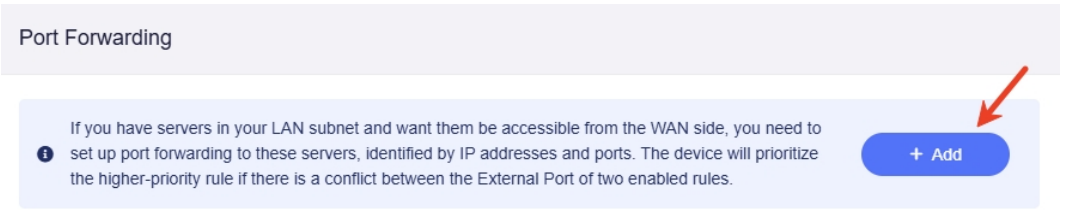
- **Priority**: ustaw Highest lub Lowest. Jeśli DMZ ma wyższy priorytet niż reguły przekierowania portów, wszystkie te reguły przestają obowiązywać. W przeciwnym razie żądania są przekazywane do urządzenia klienckiego DMZ tylko wtedy, gdy dla danego portu nie ma reguły przekierowania.
- **DMZ Host IP**: wybierz wewnętrzny adres IP urządzenia, które ma otrzymywać wszystkie pakiety przychodzące.

14.1.2 Przekierowanie portów

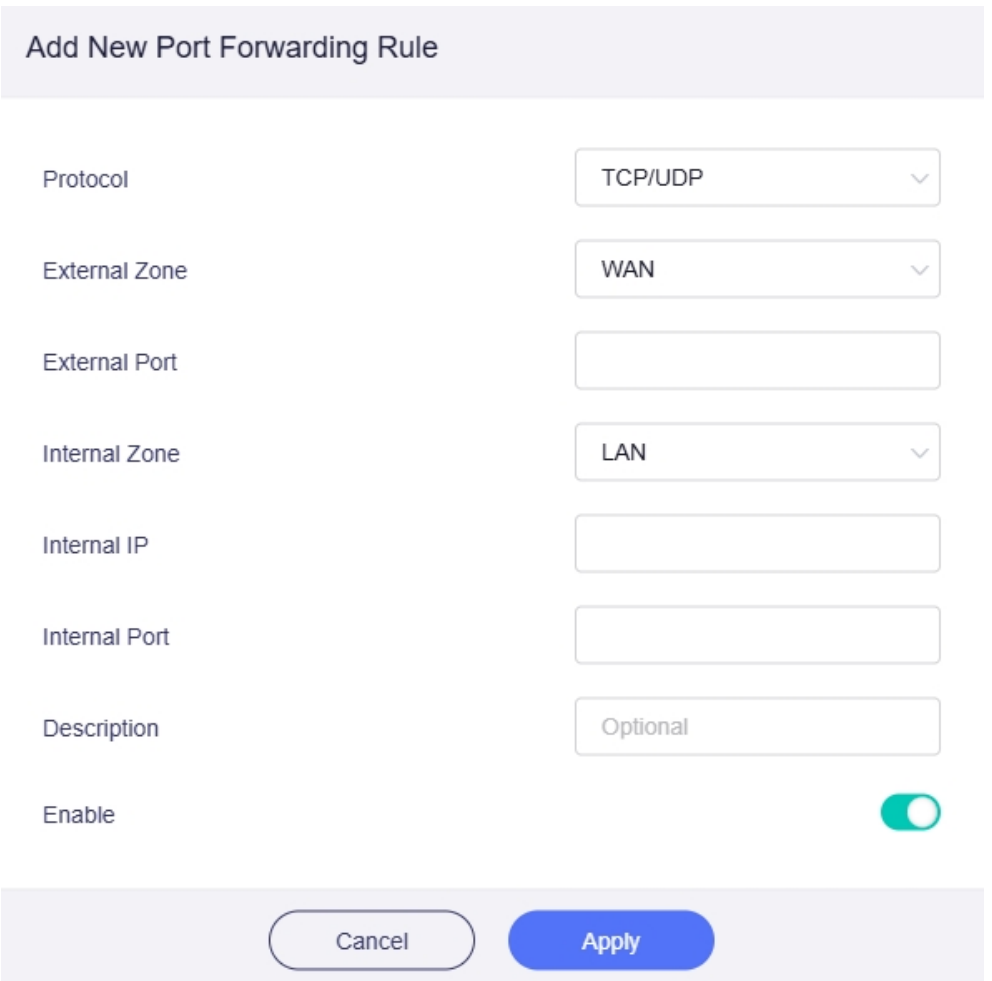
Przekierowanie portów umożliwia komputerom zdalnym łączenie się z komputerem lokalnym lub serwerem za zaporą LAN (np. serwerem WWW lub FTP).

Aby skonfigurować przekierowanie portów, wykonaj poniższe czynności.

1. Zaloguj się do panelu administracyjnego routera, przejdź do sekcji **NETWORK** > **Port Forwarding** > **Port Forwarding** i kliknij **Add**.



2. W wyskakującym oknie wprowadź wymagane parametry lub wybierz je z list, aby dodać regułę przekierowania portów, a następnie kliknij **Apply**.



- **Protocol**: używany protokół. Możesz wybrać TCP, UDP lub oba protokoły.
- **External Zone**: dostępne opcje to WAN, WireGuard Client, WireGuard Server, OpenVPN Client, OpenVPN Server, LAN i Guest.
- **External Port**: numer lub numery portów zewnętrznych. Wprowadź określony numer portu z zakresu 1–65535. Możesz ustawić pojedynczy port lub zakres, łącząc pierwszy i ostatni numer łącznikiem (np. 501-510).
- **Internal Zone**: dostępne opcje to LAN, Guest, WireGuard Client, WireGuard Server, OpenVPN Client, OpenVPN Server i WAN.
- **Internal IP**: adres IP przydzielony przez router urządzeniu wymagającemu zdalnego dostępu. Jeśli w External Port ustawiono pojedynczy port, tutaj również ustaw pojedynczy port. Jeśli w External Port ustawiono zakres portów, tutaj ustaw odpowiadający mu zakres.
- **Internal Port**: numer portu wewnętrznego urządzenia. Wprowadź określony numer portu. Pozostaw pole puste, jeśli jest taki sam jak port zewnętrzny.
- **Description**: nadaj nazwę lub dodaj opis reguły przekierowania portów (opcjonalnie).
- **Enable**: włącza lub wyłącza tę regułę.

14.2 Multi-WAN

Multi-WAN umożliwia jednoczesne korzystanie z wielu sposobów dostępu do Internetu i konfigurowanie różnych połączeń na routerze. Oferuje dwa tryby pracy:

- **Failover**: po awarii połączenia głównego automatycznie przełącza na połączenie zapasowe w krótkim czasie, zapewniając ciągły dostęp do sieci.
- **Load Balance**: rozdziela ruch między wszystkie dostępne połączenia w ustalonych proporcjach, umożliwiając ich równoczesne wykorzystanie i optymalizując użycie pasma.

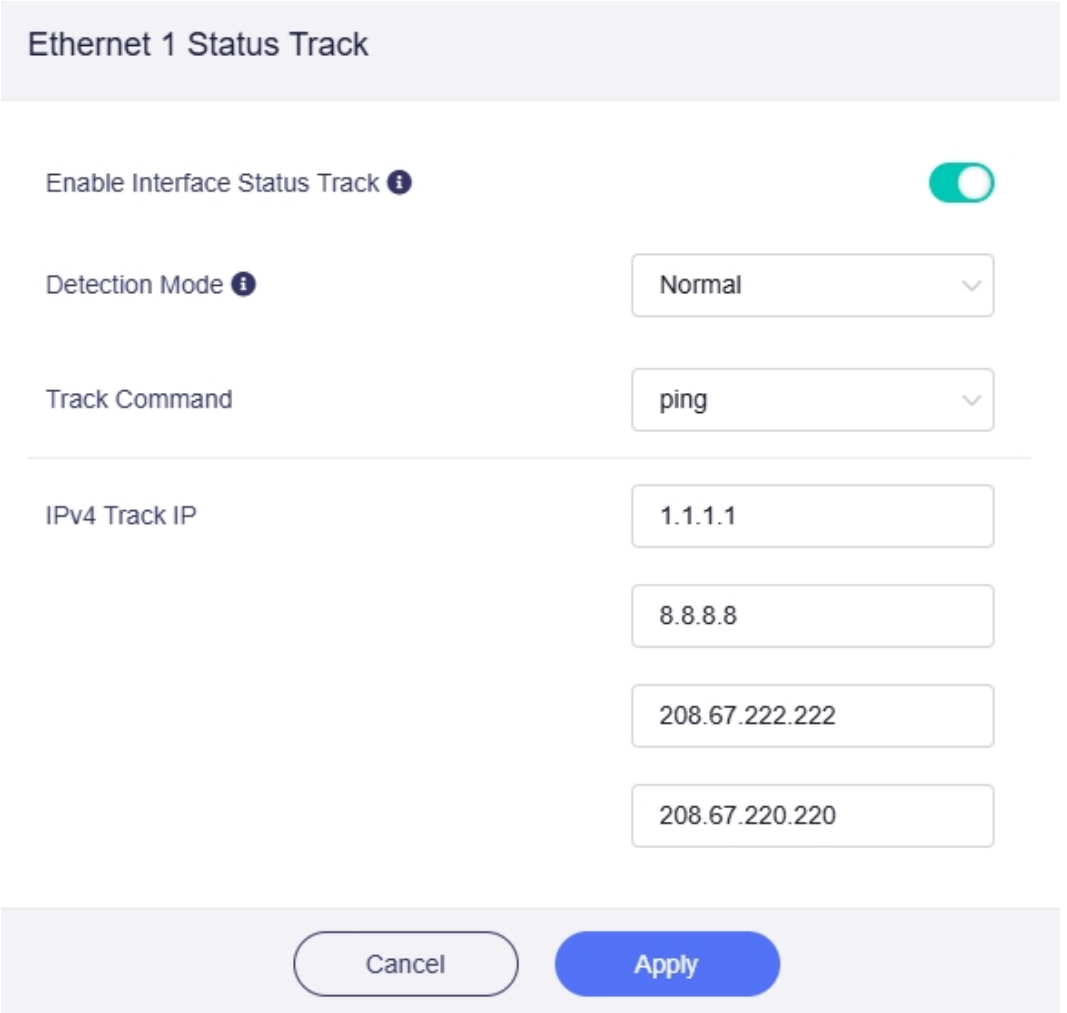
Zaloguj się do panelu administracyjnego routera i przejdź do **NETWORK** > **Multi-WAN**. Strona obejmuje dwie sekcje: Interface Status Track i Multi-WAN Mode.

14.2.1 Monitorowanie stanu interfejsów

Routery GL.iNet używają polecenia **ping**, aby monitorować połączenie z docelowym adresem IP i określać dostępność interfejsu. Jeśli interfejs jest dostępny, po lewej pojawia się zielona kropka; w przeciwnym razie jest szara.



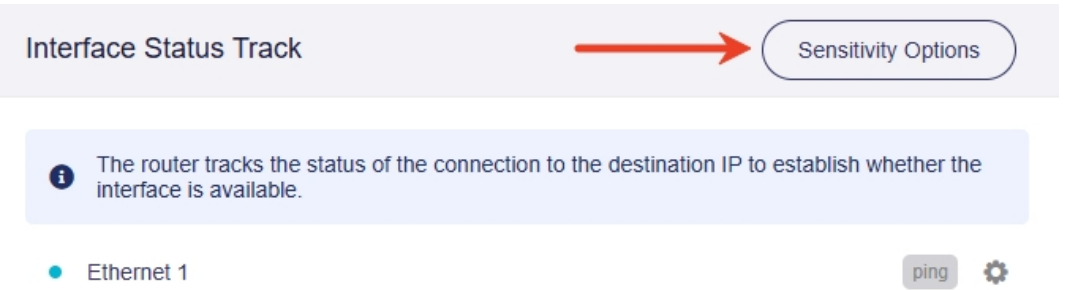
W sekcji **Interface Status Track** kliknij ikonę koła zębatego po prawej stronie, aby otworzyć ustawienia monitorowania poszczególnych interfejsów sieciowych. Poniżej pokazano ustawienia interfejsu Ethernet. Pozostałe interfejsy konfiguruje się według tych samych zasad.



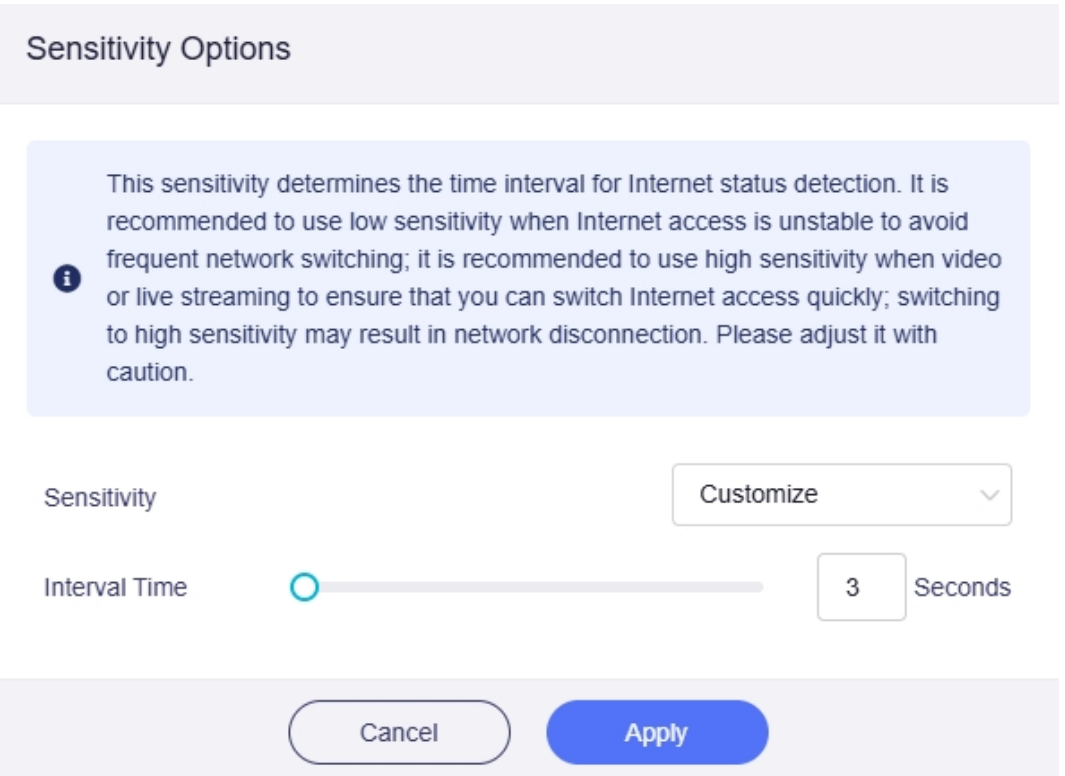
- **Enable Interface Status Track**: opcja jest domyślnie włączona. Po wyłączeniu router określa stan interfejsu na podstawie warunków fizycznych (np. podłączenia kabla Ethernet).
- **Detection Mode**: tę funkcję wprowadzono w wersji oprogramowania 4.5 jako Low Data Mode, a w wersji 4.7 zmieniono nazwę na Detection Mode. Dostępne są trzy tryby: Normal Mode, Low Data Mode i Strict Mode.
  - **Normal Mode**: używany domyślnie.
  - **Low Data Mode**: uruchamia monitorowanie tylko wtedy, gdy na interfejsie sieciowym wystąpi błąd sieci. Używaj tego trybu przy ograniczonym pakiecie danych. Ponowne nawiązanie zerwanego połączenia może być nieco wolniejsze niż w Normal Mode. Ten tryb jest domyślnie włączony tylko dla interfejsu komórkowego.
  - **Strict Mode**: określa stan interfejsu wyłącznie na podstawie wyników polecenia sprawdzającego wysyłanego na publiczny adres IP.

- **Track Command**: polecenie ping służy do monitorowania połączenia z docelowym adresem IP i sprawdzania dostępności interfejsu.
- **IPv4 Track IP**: w razie potrzeby dostosuj adresy IPv4 używane do monitorowania.

Kliknij **Sensitivity Options** w prawym górnym rogu.



Możesz ustawić częstotliwość sprawdzania dostępu do Internetu na Low, Medium lub High albo określić własny odstęp. Dostępny zakres wynosi od 0,5 do 90 sekund.



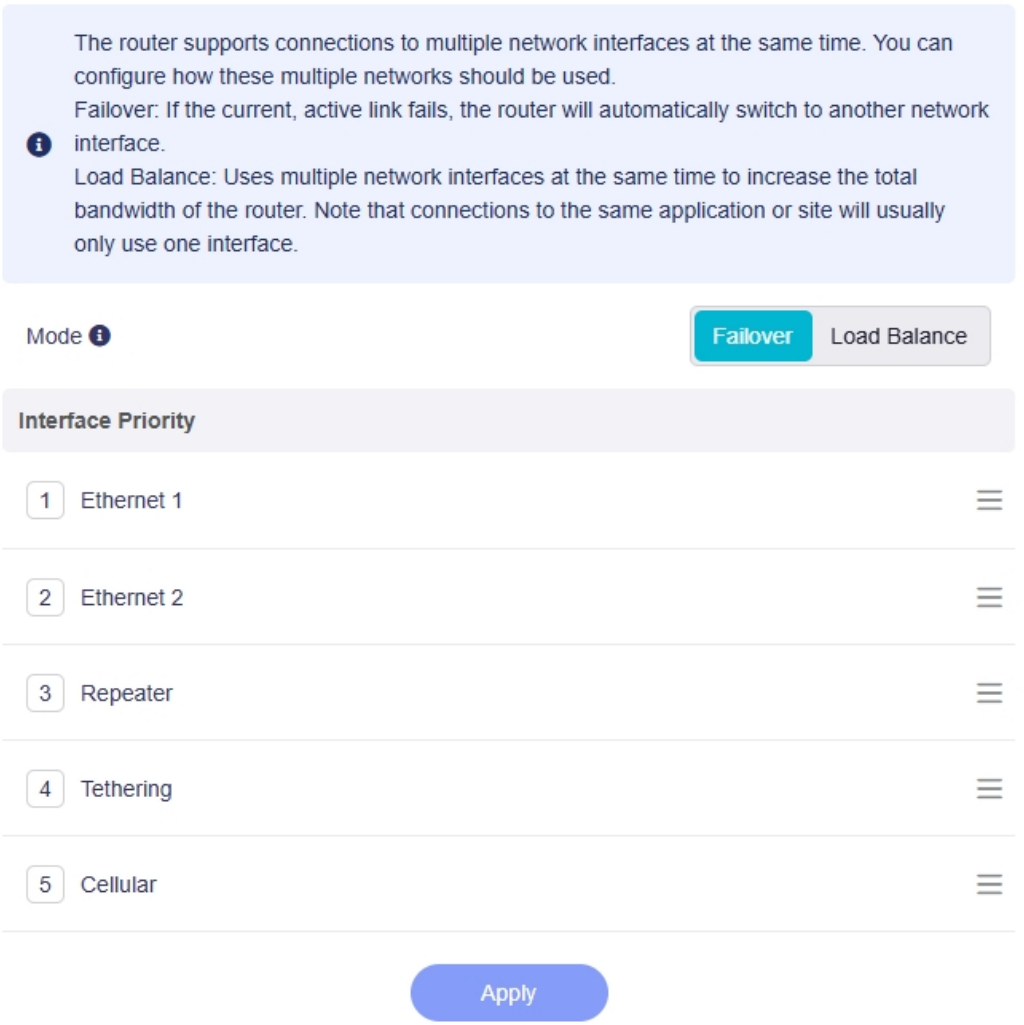
14.2.2 Tryb Multi-WAN

Multi-WAN oferuje dwa tryby: **Failover** i **Load Balance**. Tryby te wzajemnie się wykluczają.

Przełączanie awaryjne (Failover)

Failover jest trybem domyślnym po skonfigurowaniu wielu połączeń. Jeśli aktywne łącze ulegnie awarii, router automatycznie przełącza się na inny interfejs sieciowy zapewniający dostęp do Internetu.

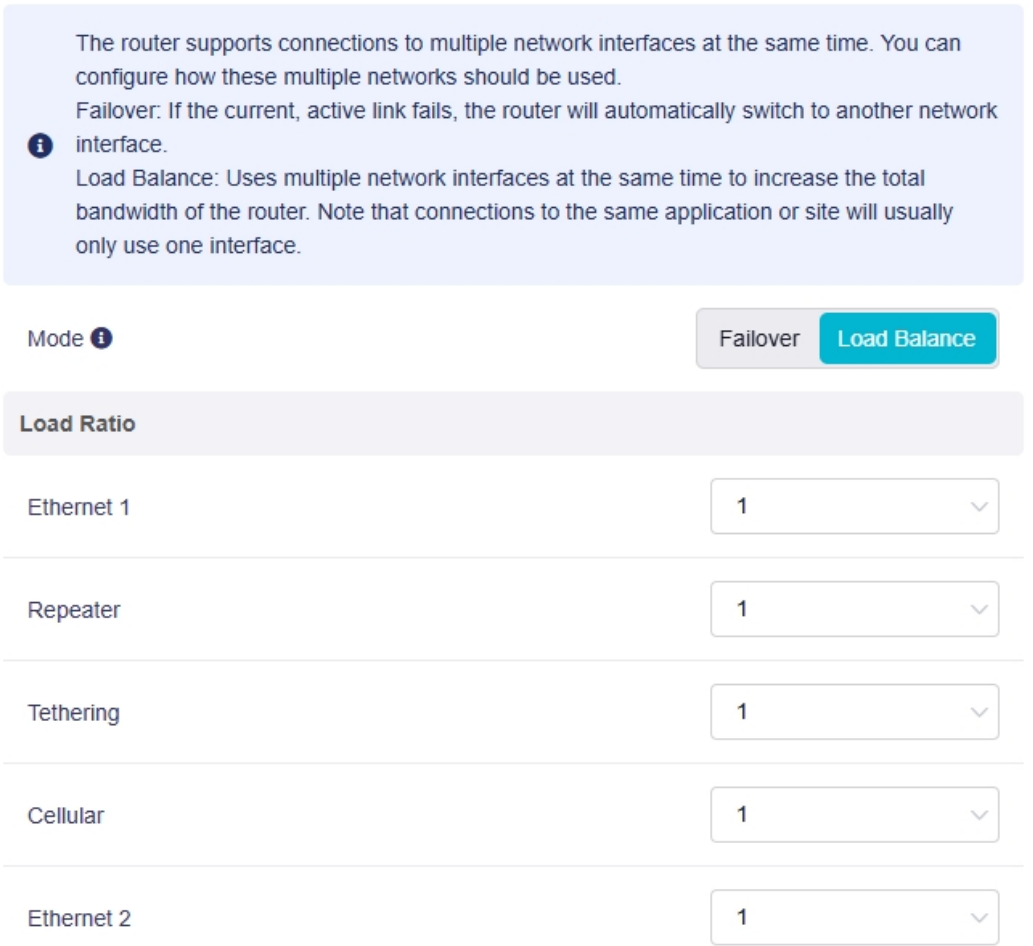
Możesz ustawić priorytety interfejsów. Po awarii używanego interfejsu router przełącza się na dostępny interfejs o najwyższym priorytecie. Gdy połączenie o wyższym priorytecie zostanie przywrócone, router automatycznie do niego wróci.



Równoważenie obciążenia (Load Balance)

Tryb Load Balance korzysta jednocześnie z wielu interfejsów sieciowych, zwiększając łączną przepustowość routera. System rozdziela nowe połączenia między interfejsy zgodnie z ustawionymi proporcjami obciążenia. Połączenia z tą samą aplikacją lub witryną zazwyczaj korzystają jednak tylko z jednego interfejsu.

Proporcje obciążenia określają udział poszczególnych interfejsów sieciowych. System przydziela interfejsy do obsługi nowych połączeń zgodnie z ustawionymi proporcjami. Na przykład jeśli router jest jednocześnie połączony z pięcioma sieciami (np. Ethernet 1, Repeater, Tethering, Cellular i Ethernet 2), a wszystkie interfejsy mają dostęp do Internetu, włączenie Load Balance i ustawienie proporcji 1:1:1:1:1 oznacza równy podział pasma między pięć interfejsów. System rozdziela nowe połączenia między te interfejsy zgodnie z ustawionymi proporcjami obciążenia.



W razie potrzeby możesz dostosować proporcje obciążenia. Na przykład jeśli Ethernet 1 ma przepustowość 100 Mb/s, Repeater 200 Mb/s, a pozostałe połączenia są nieaktywne, ustaw proporcje na 1 dla Ethernet 1, 2 dla Repeater oraz 0 dla Tethering, Cellular i Ethernet 2. System rozdzieli nowe połączenia między te interfejsy w proporcji 1:2, więc Ethernet 1 będzie obsługiwać o połowę mniej połączeń niż Repeater. W odróżnieniu od trybu Failover ten tryb optymalizuje łączną przepustowość przez równoważenie ruchu na wszystkich dostępnych interfejsach.

Uwaga: nie ma gwarancji, że istniejące połączenia lub ruch będą odpowiadać ustawionym proporcjom. Przy dłuższym korzystaniu rzeczywisty rozkład stopniowo się do nich zbliży.

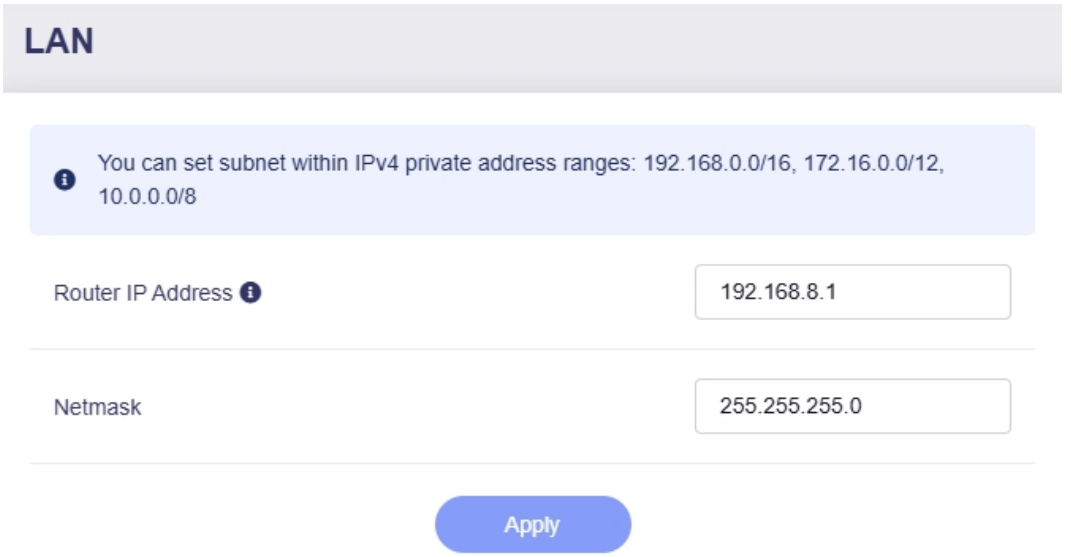
14.3 LAN

LAN (Local Area Network) to prywatna sieć lokalna, do której urządzenia łączą się za pomocą kabli Ethernet.

Zaloguj się do panelu administracyjnego routera i przejdź do **NETWORK** > **LAN**. Tutaj możesz konfigurować ustawienia LAN: ustawienia podstawowe, serwer DHCP i rezerwację adresów.

14.3.1 Ustawienia podstawowe

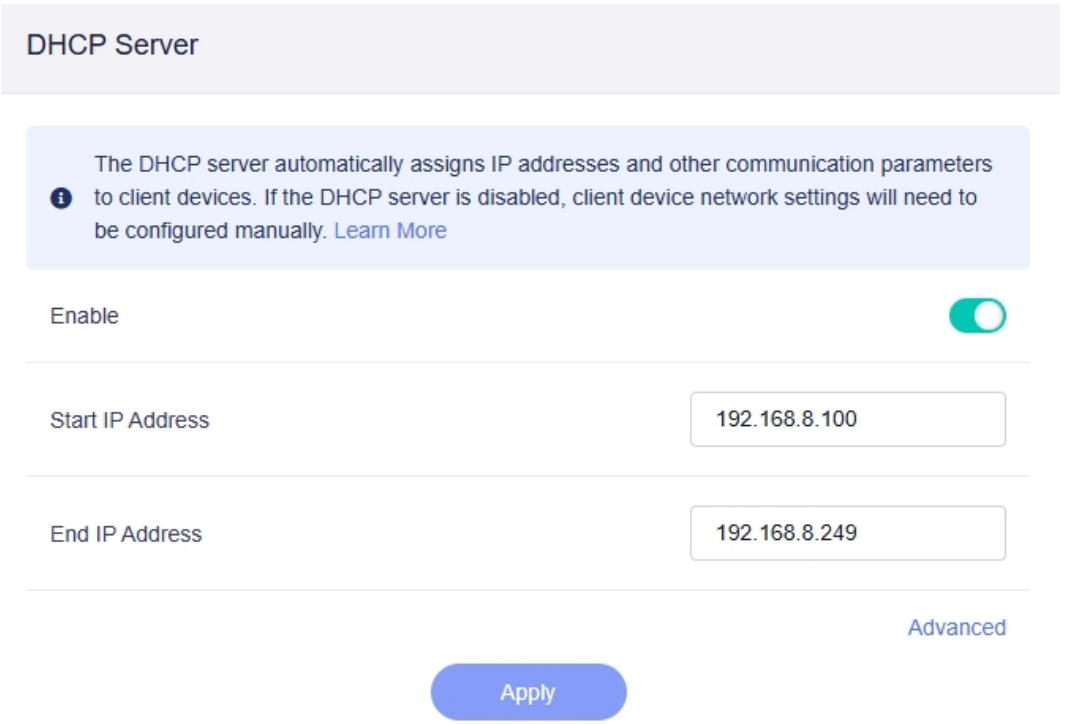
Ustawienia podstawowe obejmują adres IP routera i maskę sieci. Podsieć można ustawić w prywatnych zakresach adresów IPv4: 192.168.0.0/16, 172.16.0.0/12, 10.0.0.0/8.



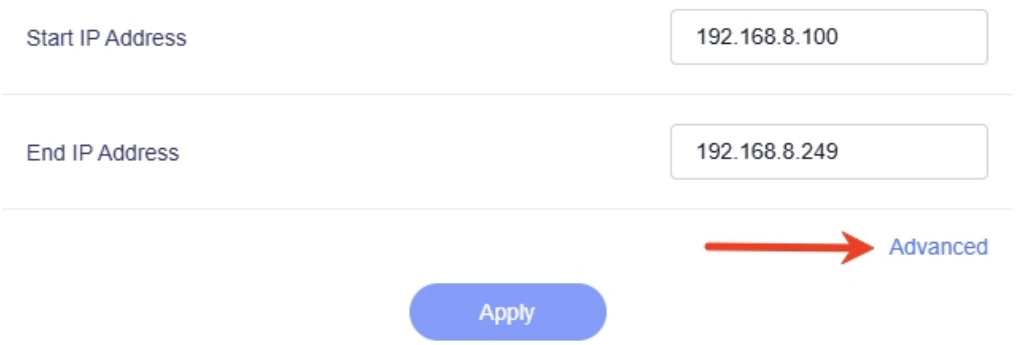
- **Router IP Address**: adres wpisywany w pasku adresu przeglądarki w celu otwarcia panelu administracyjnego routera. Domyślnie jest to 192.168.8.1. Można go zmienić, jeśli koliduje z siecią nadrzędną.
- **Netmask**: dostępne są dwie opcje: 255.255.255.0 i 255.255.0.0.

14.3.2 Serwer DHCP

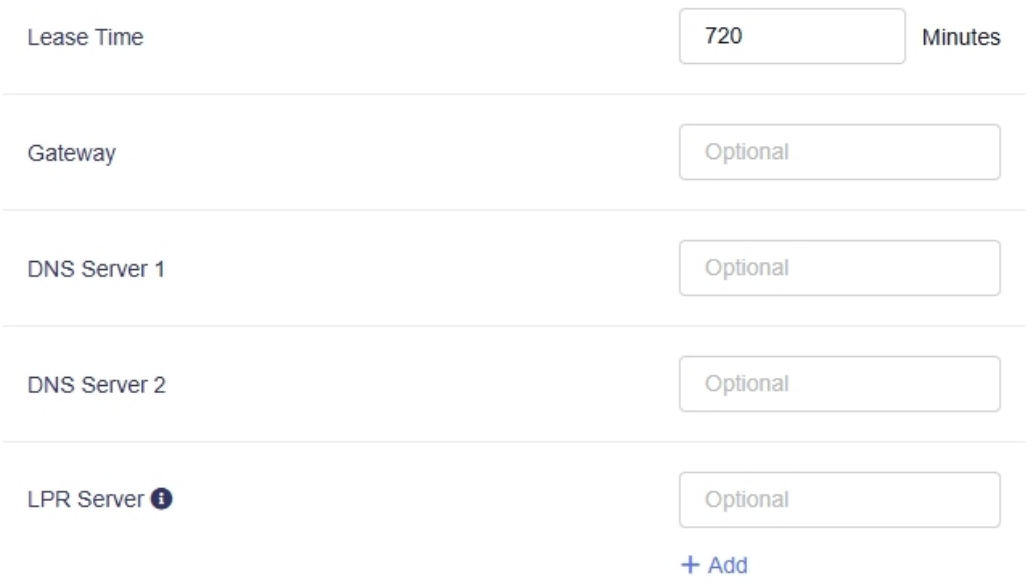
Serwer DHCP automatycznie przydziela adresy IP i inne parametry komunikacji każdemu podłączonemu klientowi. W routerze GL.iNet jest domyślnie włączony, a jego pula adresów IP obejmuje zakres od 192.168.8.100 do 192.168.8.249. W razie potrzeby można zmienić ten zakres.



Kliknij **Advanced** w prawym dolnym rogu.



Możesz skonfigurować ustawienia zaawansowane: czas dzierżawy, bramę, serwery DNS i serwer LPR.



- **Lease Time**: czas, przez który urządzenie może korzystać z adresu IP przydzielonego przez DHCP.
- **Gateway**: element routera kierujący ruch między siecią lokalną a sieciami zewnętrznymi (np. Internetem).
- **DNS Server 1**: serwer główny odpowiedzialny za tłumaczenie nazw domen na adresy IP.
- **DNS Server 2**: serwer zapasowy używany do rozwiązywania nazw domen w razie awarii głównego serwera DNS.
- **LPR Server**: (Line Printer Remote Server) usługa zarządzająca zadaniami drukowania i umożliwiająca urządzeniom sieciowym wysyłanie żądań do zdalnych drukarek. Można skonfigurować wiele portów LPR dla drukarek.

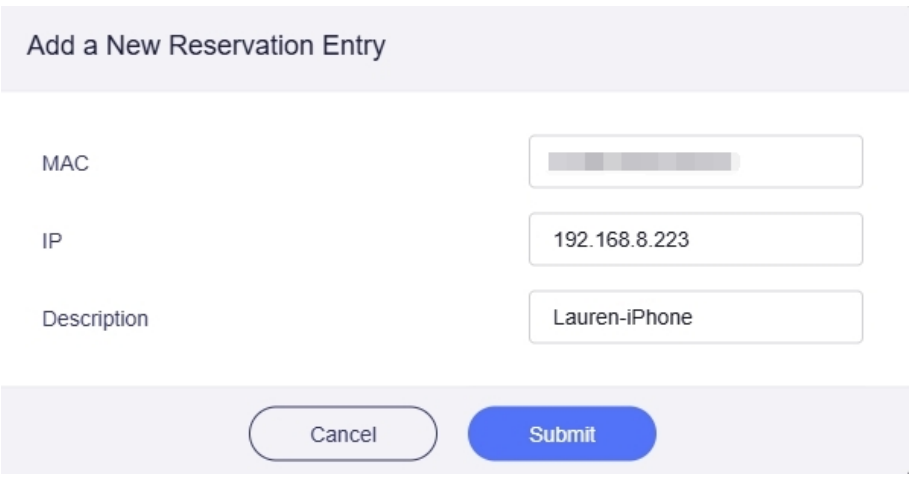
Uwaga: po wyłączeniu serwera DHCP trzeba ręcznie skonfigurować statyczny adres IP i inne parametry komunikacji na każdym urządzeniu klienckim. Szczegóły znajdziesz tutaj.

14.3.3 Rezerwacja adresów

Rezerwacja adresów umożliwia przypisanie stałego adresu IP klientowi LAN, dzięki czemu przy każdym kontakcie z serwerem DHCP routera otrzymuje on ten sam adres. Zarezerwowane adresy można przypisywać komputerom lub serwerom wymagającym stałych ustawień IP. Aby ustawienie zaczęło działać, urządzenia z rezerwacją adresu muszą ponownie połączyć się z routerem.

Aby w razie potrzeby skonfigurować rezerwację adresów, wykonaj poniższe czynności.

1. Zaloguj się do panelu administracyjnego routera, przejdź do **NETWORK** > **LAN** > **Address Reservation** i kliknij **Add**.
2. W wyświetlonym oknie wybierz adres MAC z listy. Odpowiadający mu adres IP zostanie uzupełniony automatycznie. Wprowadź opisową nazwę i kliknij **Submit**.



3. Po dodaniu rezerwacji adresu IP na stronie pojawi się odpowiedni wpis, jak pokazano poniżej.



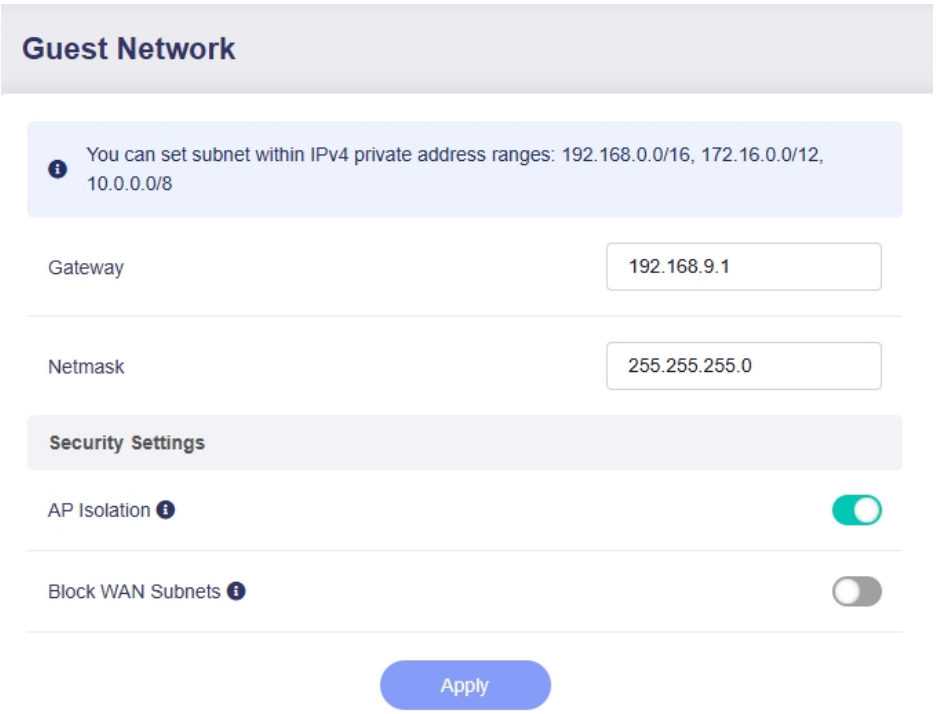
14.4 Sieć gościnna

Sieć gościnna to oddzielna sieć dla gości, odizolowana od głównej sieci LAN w celu ochrony bezpieczeństwa sieci prywatnej.

Zaloguj się do panelu administracyjnego routera i przejdź do **NETWORK** -> **Guest Network**. Tutaj możesz skonfigurować ustawienia sieci gościnnej, w tym ustawienia podstawowe i serwer DHCP.

14.4.1 Ustawienia podstawowe

Podstawowe ustawienia obejmują Gateway, Netmask, AP Isolation i Block WAN Subnets.

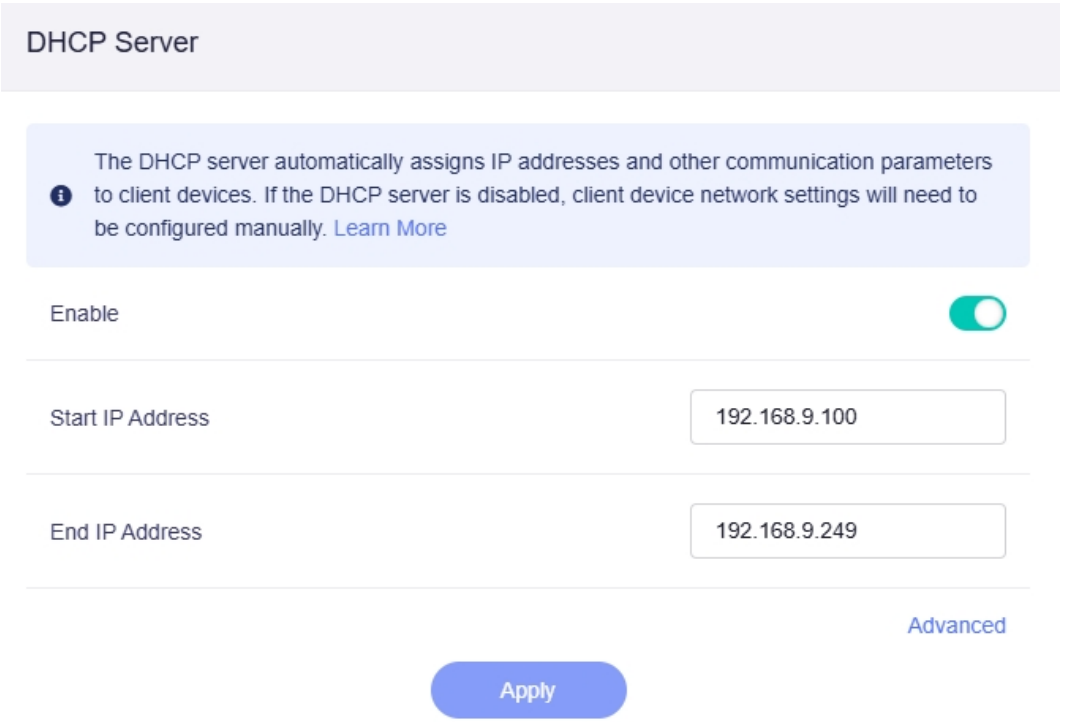


- **Gateway**: domyślny adres to 192.168.9.1. Można go zmienić, ale nie może kolidować z adresem bramy sieci głównej.
- **Netmask**: dostępne są dwie opcje: 255.255.255.0 i 255.255.0.0.
- **AP Isolation**: izoluje klientów sieci gościnnej w oddzielnych segmentach, aby nie mogli komunikować się z innymi urządzeniami w tej samej sieci.
- **Block WAN Subnets**: po włączeniu sieć gościnna nie może uzyskiwać dostępu do sieci nadrzędnej ani odpowiadającego jej segmentu sieci.

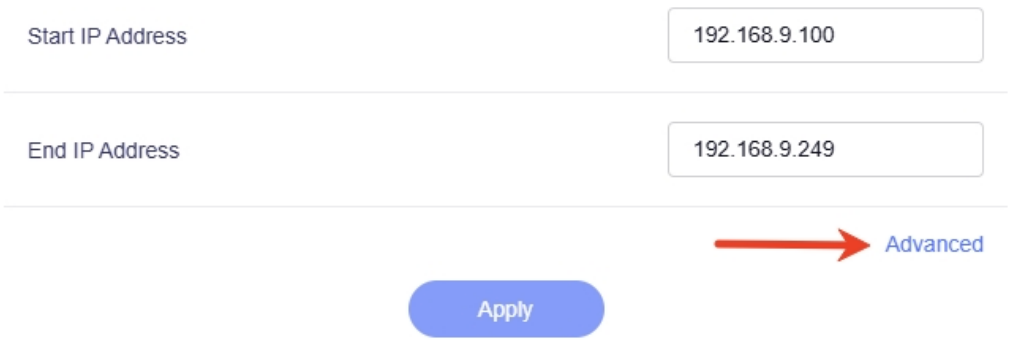
14.4.2 Serwer DHCP

Ponieważ sieć gościnna jest domyślnie wyłączona, jej serwer DHCP również jest wyłączony i ukryty do czasu ręcznego włączenia sieci.

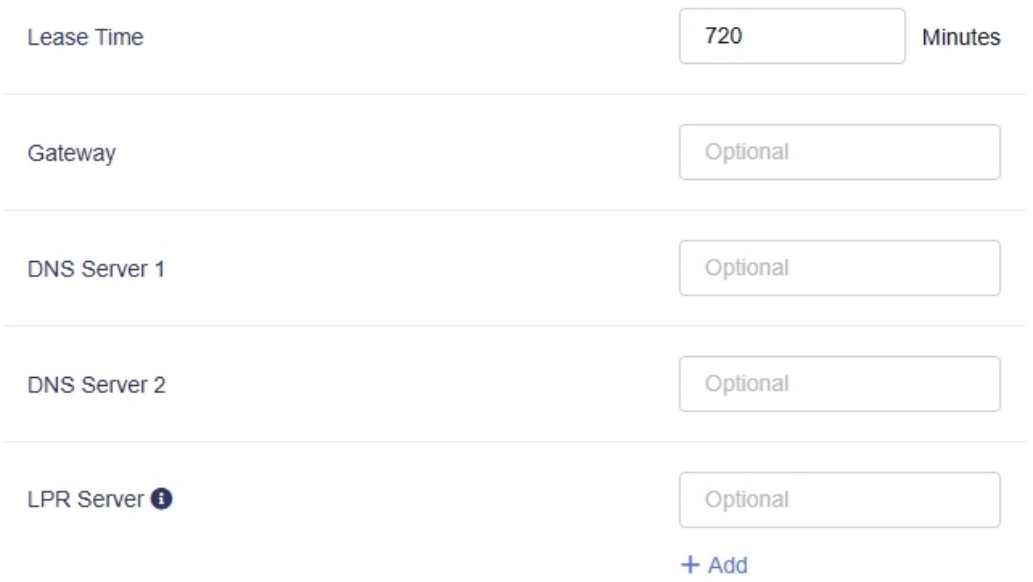
Po włączeniu serwer DHCP automatycznie przydziela adresy IP i inne parametry komunikacji każdemu podłączonemu klientowi. Pula adresów IP sieci gościnnej obejmuje zakres od 192.168.9.100 do 192.168.9.249. W razie potrzeby można go zmienić.



Kliknij **Advanced** w prawym dolnym rogu.



Możesz skonfigurować ustawienia zaawansowane: czas dzierżawy, bramę, serwery DNS i serwer LPR.



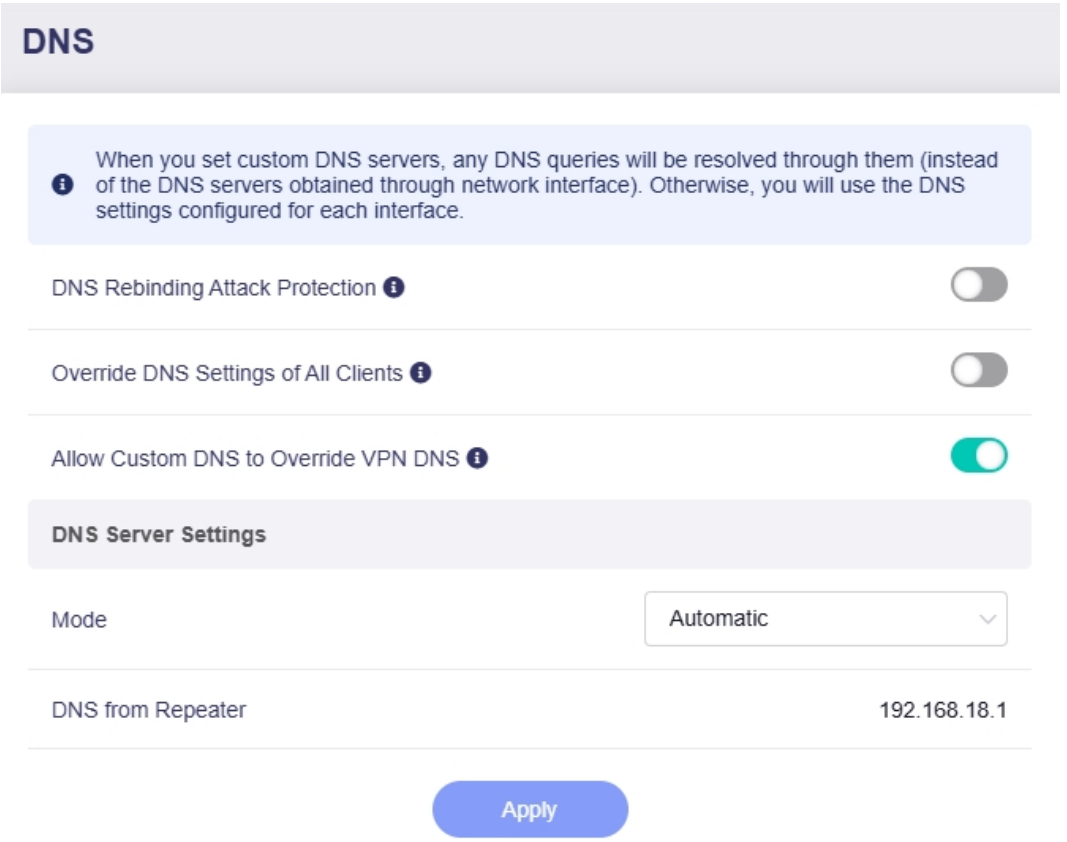
- **Lease Time**: czas, przez który urządzenie może korzystać z adresu IP przydzielonego przez DHCP sieci gościnnej.
- **Gateway**: element routera kierujący ruch między siecią gościnną a sieciami zewnętrznymi (np. Internetem).
- **DNS Server 1**: serwer główny odpowiedzialny za tłumaczenie nazw domen na adresy IP.
- **DNS Server 2**: serwer zapasowy używany do rozwiązywania nazw domen w razie awarii głównego serwera DNS.
- **LPR Server**: (Line Printer Remote Server) usługa zarządzająca zadaniami drukowania i umożliwiająca urządzeniom sieciowym wysyłanie żądań do zdalnych drukarek. Można skonfigurować wiele portów LPR dla drukarek.

14.5 DNS

DNS (Domain Name System) to usługa sieciowa, która przekształca czytelne dla ludzi nazwy domen (np. www.google.com) na rozpoznawane przez komputery adresy IP (np. 142.250.185.142), umożliwiając urządzeniom łączenie się z docelowymi witrynami lub usługami.

Serwer DNS routera to wbudowana w router usługa DNS, która przekształca nazwy domen na adresy IP dla wszystkich podłączonych urządzeń. Zwykle działa na dwa sposoby: automatycznie pobiera adresy DNS z sieci nadrzędnej, zapewniając domyślne rozwiązywanie nazw, lub pozwala ręcznie skonfigurować własne publiczne adresy DNS (np. 8.8.8.8) w panelu administracyjnym w celu optymalizacji dostępu do sieci lub zwiększenia bezpieczeństwa. Po konfiguracji wszystkie podłączone urządzenia domyślnie korzystają z tego wspólnego serwera DNS, bez potrzeby oddzielnej konfiguracji DNS na każdym urządzeniu.

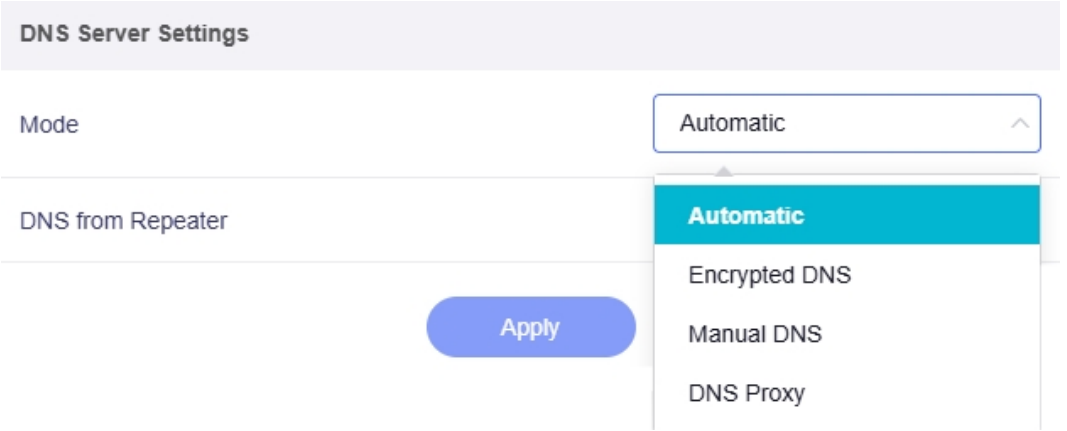
Zaloguj się do panelu administracyjnego routera i przejdź do **NETWORK** > **DNS**. Ta strona umożliwia konfigurację ustawień DNS, w tym opcji bezpieczeństwa, trybów serwera i reguł priorytetów DNS w różnych scenariuszach sieciowych.



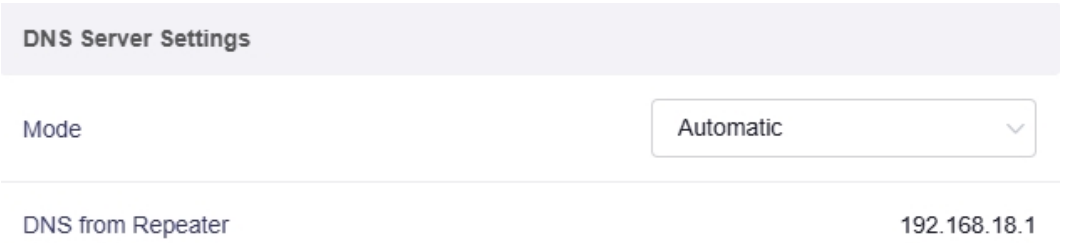
- **DNS Rebinding Attack Protection**: chroni przed atakami DNS rebinding przez blokowanie złośliwych prób rozwiązywania nazw DNS. Włączenie może spowodować problemy z prywatnymi zapytaniami DNS. Wyłącz tę opcję, jeśli sieć korzysta z portalu logowania (np. strony logowania do publicznego Wi-Fi).
- **Override DNS Settings of All Clients**: po włączeniu wszystkie podłączone urządzenia muszą korzystać z serwerów DNS skonfigurowanych na routerze, niezależnie od własnych ustawień DNS. Zapewnia to jednolitą konfigurację DNS dla wszystkich urządzeń.
- **Allow Custom DNS to Override VPN DNS**: po włączeniu, jeśli skonfigurowano własny DNS, pakiety przesyłane przez tunel VPN będą używać go do rozwiązywania nazw zamiast serwerów DNS połączenia VPN. Zapewnia to normalne stosowanie własnych reguł DNS podczas korzystania z VPN.

14.5.1 Ustawienia serwera DNS

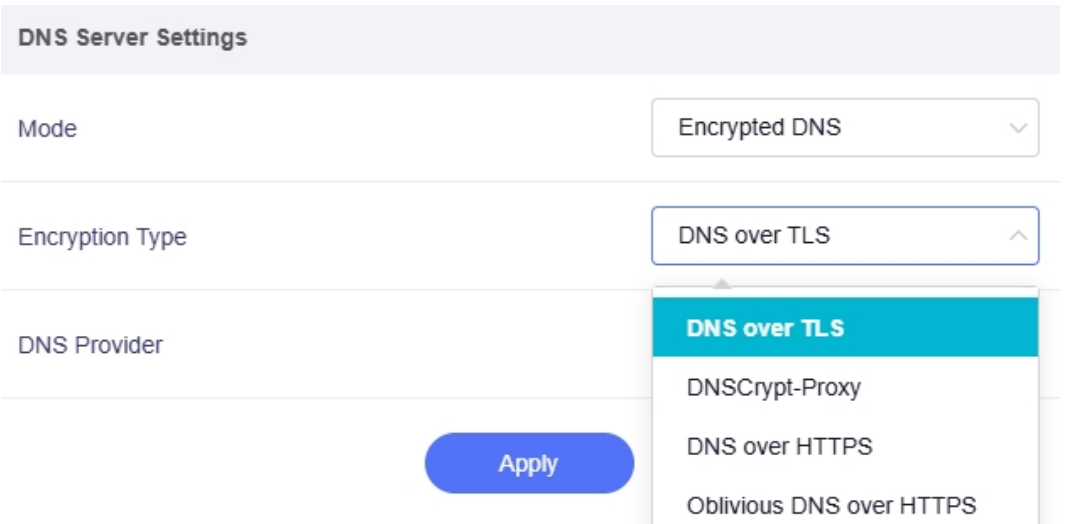
Dostępne są cztery tryby serwera DNS: Automatic, Encrypted DNS, Manual DNS i DNS Proxy.



1. **Automatic**: router automatycznie pobiera adresy serwerów DNS z sieci nadrzędnej i stosuje je do wszystkich podłączonych urządzeń.



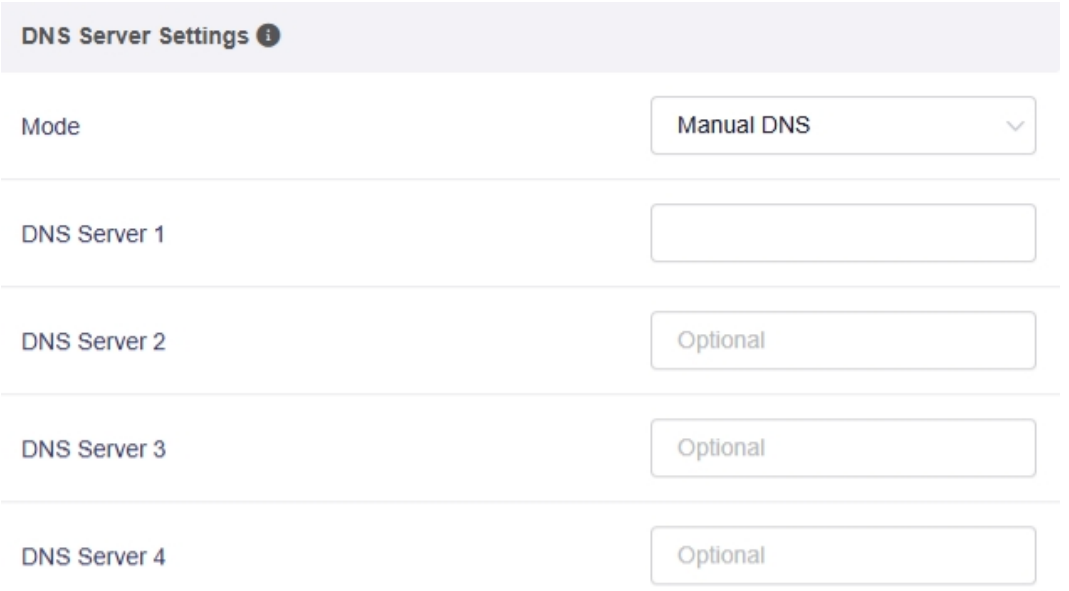
2. **Encrypted DNS**: router używa szyfrowanych protokołów do obsługi zapytań DNS, chroniąc dane rozwiązywania nazw przed podsłuchiwaniem i modyfikacją. Dostępne są cztery rodzaje szyfrowania: DNS over TLS, DNSCrypt-Proxy, DNS over HTTPS i Oblivious DNS over HTTPS.



- Dla DNS over TLS wybierz dostawcę DNS spośród Control D, NextDNS i Cloudflare.
- Dla pozostałych trzech opcji (DNSCrypt-Proxy, DNS over HTTPS i Oblivious DNS over HTTPS) wybierz z repozytorium co najmniej jeden serwer DNS. Można wybrać

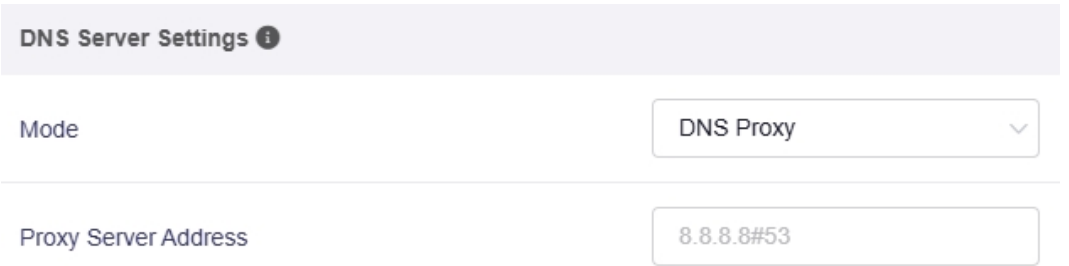
maksymalnie 8 serwerów. Przy wielu serwerach router automatycznie używa najszybszego.

3. **Manual DNS**: umożliwia samodzielne ustawienie serwerów DNS routera. Kliknij DNS Server 1 i wybierz serwer z listy. Pozostałe pola DNS zaktualizują się automatycznie.



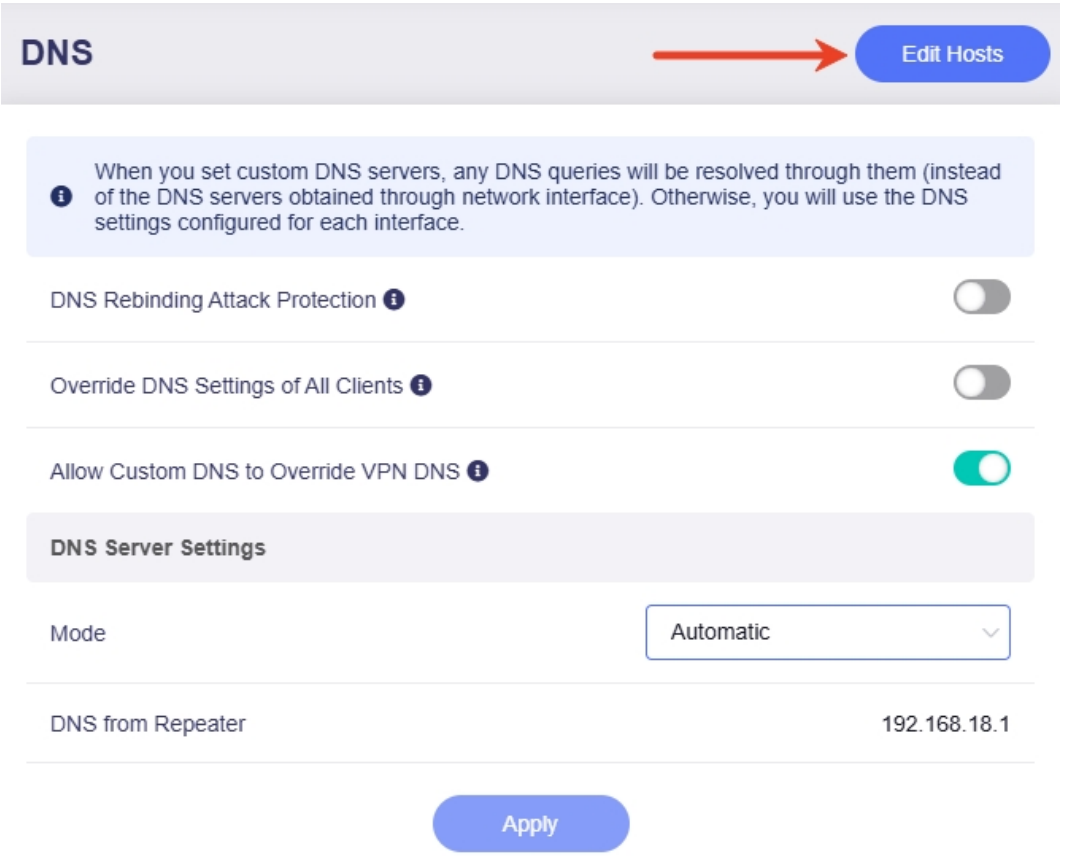
Uwaga: aby używać adresów IPv6 w ręcznej konfiguracji DNS, najpierw włącz IPv6 na routerze.

4. **DNS Proxy**: router przekazuje wszystkie zapytania DNS przez serwer proxy, umożliwiając rozwiązywanie nazw w środowisku sieciowym tego serwera na potrzeby określonego dostępu.

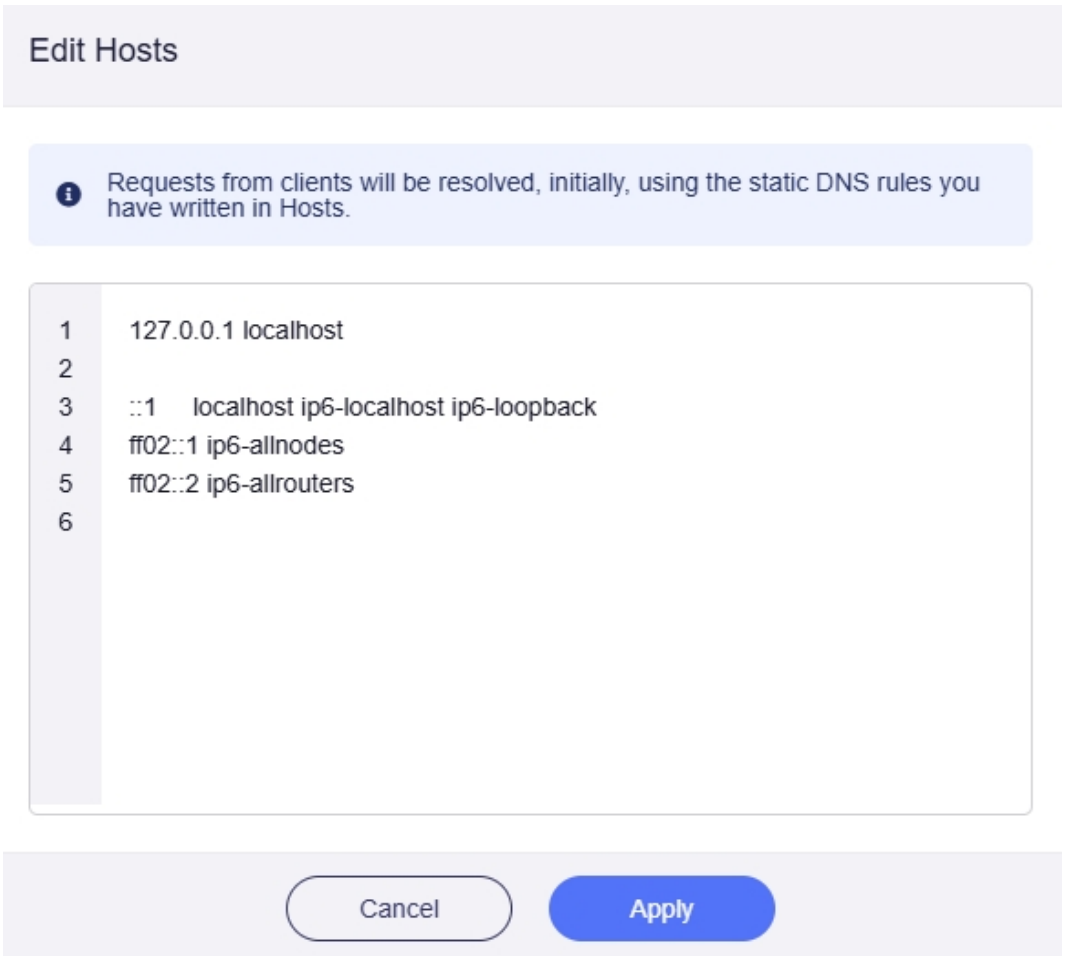


14.5.2 Edycja pliku hosts

W razie potrzeby możesz zdefiniować statyczne reguły rozwiązywania nazw DNS.
Na stronie DNS kliknij **Edit Hosts** w prawym górnym rogu.



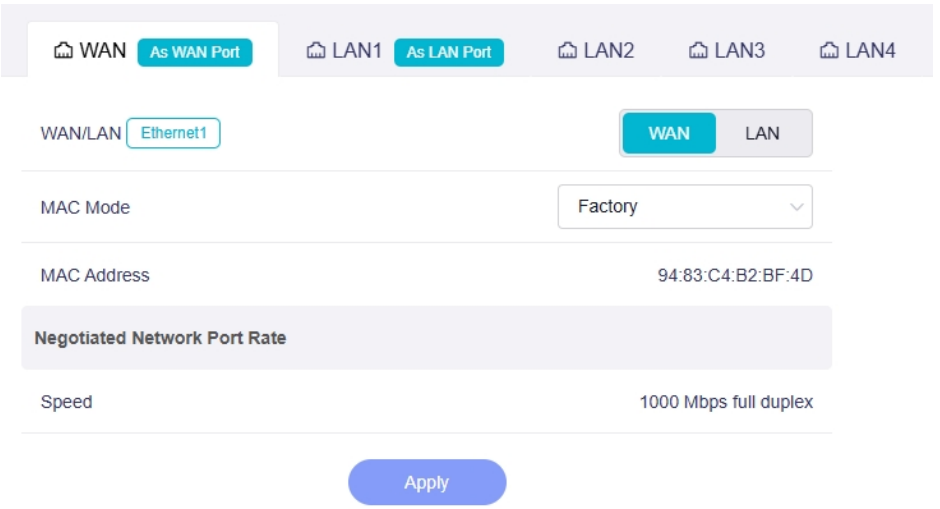
Żądania klientów są rozwiązywane w pierwszej kolejności według wpisanych tutaj statycznych reguł DNS. Pozwala to ręcznie mapować adresy IP na nazwy hostów (np. domyślny wpis 127.0.0.1 localhost dla lokalnej pętli zwrotnej) i samodzielnie kontrolować rozwiązywanie nazw domen.


Edit Hosts
Requests from clients will be resolved, initially, using the static DNS rules you have written in Hosts.
1 127.0.0.1 localhost
2
3 ::1 localhost ip6-localhost ip6-loopback
4 ff02::1 ip6-allnodes
5 ff02::2 ip6-allrouters
6
Cancel
Apply

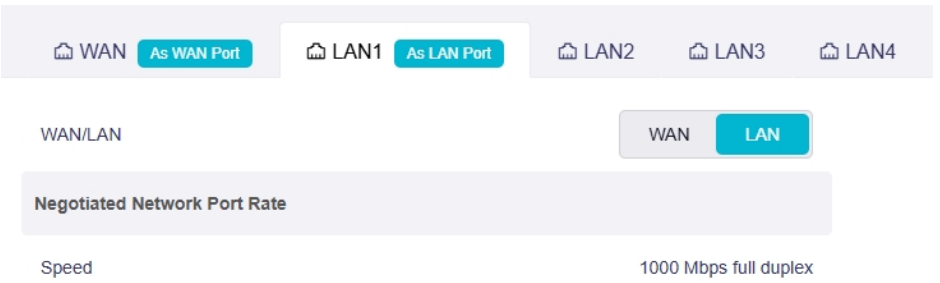
14.6 Port Ethernet

Zaloguj się do panelu administracyjnego routera i przejdź do **NETWORK** > **Ethernet Port**. Ta strona umożliwia zarządzanie portami Ethernet routera.

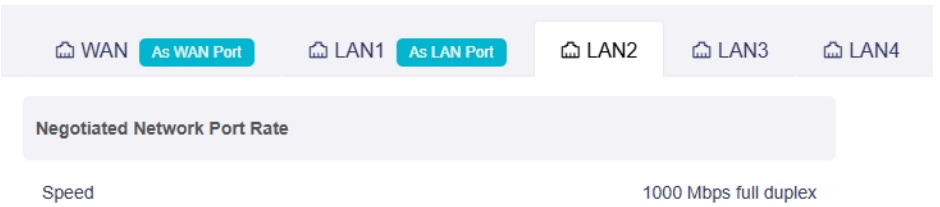
Sekcja **WAN** wyświetla rolę portu (WAN lub LAN), adres MAC i wynegocjowaną prędkość.



Sekcja **LAN 1** umożliwia zmianę portu LAN 1 na WAN. Tutaj możesz zmienić rolę portu i sprawdzić wynegocjowaną szybkość.



Pozostałe sekcje **LAN** wyświetlają wynegocjowaną szybkość odpowiednich portów LAN.



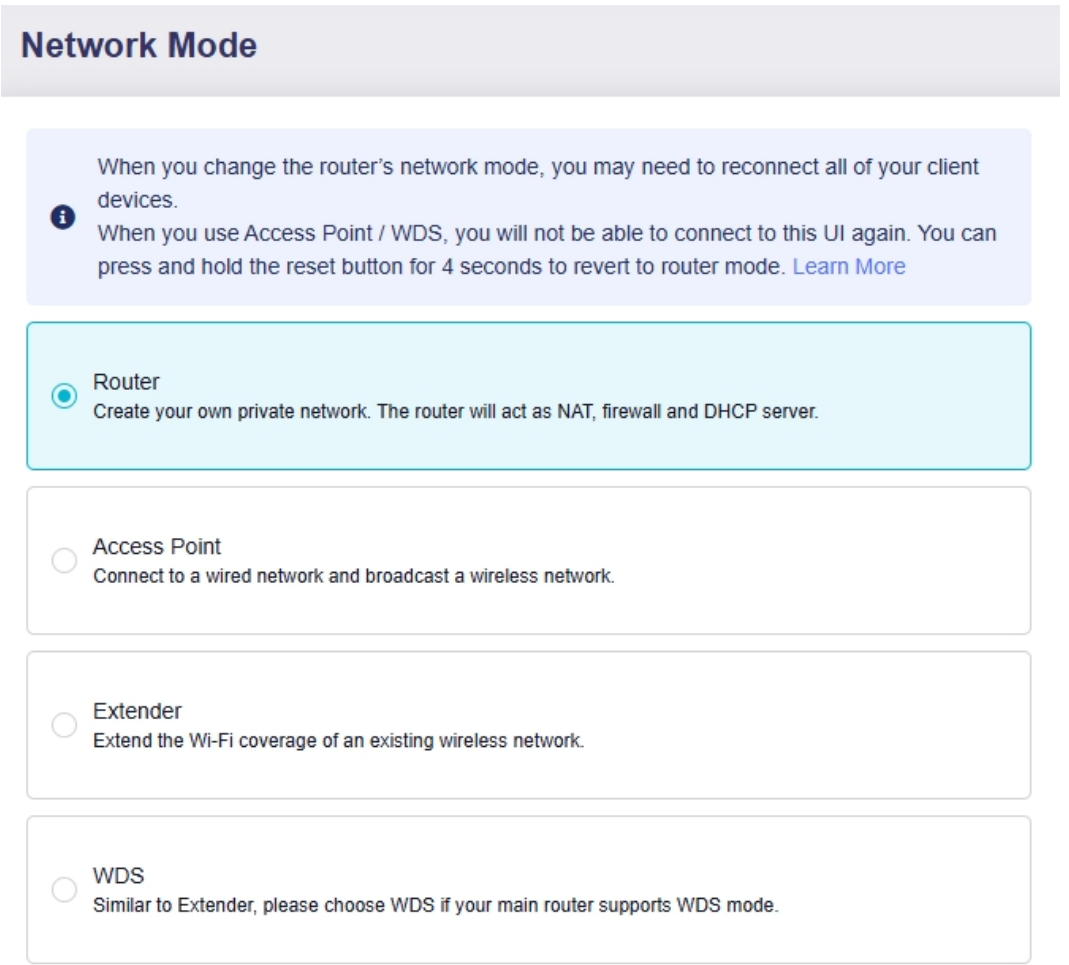
Uwaga: wynegocjowana szybkość portów WAN i LAN jest wyświetlana tylko po podłączeniu kabla

Ethernet. Zależy ona zarówno od portu Ethernet, jak i od kabla Ethernet.

14.7 Tryb sieciowy

Tryb sieciowy określa rolę i funkcje routera, dostosowane do różnych sposobów wdrażania sieci.

Zaloguj się do panelu administracyjnego routera i przejdź do **NETWORK** > **Network Mode**. Tutaj możesz zmienić tryb sieciowy routera.



- **Router**: domyślny tryb większości routerów domowych i małych biur. Tworzy prywatną sieć lokalną (LAN) i pełni funkcję bramy między publicznym Internetem a podłączonymi urządzeniami. W tym trybie działają podstawowe funkcje: NAT, DHCP i wbudowana zapora. Router łączy się z łączem nadrzędnym, np. światłowodowym, automatycznie przydziela prywatne adresy IP podłączonym urządzeniom i chroni całą sieć prywatną.
- **Access Point**: w tym trybie router łączy się z siecią przewodową kablem LAN i nadaje sygnał bezprzewodowy, rozszerzając zasięg Wi-Fi w dużych przestrzeniach i

zapewniając dostęp większej liczbie urządzeń. NAT i DHCP są wyłączone, a router działa wyłącznie jako nadajnik bezprzewodowy i przełącznik, bez funkcji samodzielnej bramy.

- **Extender**: ten tryb rozszerza zasięg istniejącej sieci Wi-Fi i eliminuje martwe strefy o słabej łączności. Router bezprzewodowo odbiera sygnał z głównego routera, wzmacnia go i nadaje ponownie. W odróżnieniu od trybu Access Point nie wymaga połączenia przewodowego z głównym routerem. Może jednak zmniejszyć przepustowość o połowę, ponieważ urządzenie jednocześnie odbiera i nadaje sygnał.
- **WDS**: tryb Wireless Distribution System (WDS), podobnie jak Extender, bezprzewodowo rozszerza zasięg Wi-Fi, ale obsługuje mosty bezprzewodowe między wieloma zgodnymi routerami. Jest zalecany do rozbudowy sieci bezprzewodowej, gdy router nadrzędny obsługuje WDS.

  Ten tryb sprawdza się np. w budynkach wielopiętrowych lub małych kompleksach biurowych, w których wiele routerów musi współpracować w ramach jednej sieci bezprzewodowej. W odróżnieniu od trybu Extender, przesyłającego sygnał z jednego głównego routera do jednego wzmacniacza, WDS pozwala połączonym routerom zarówno nadawać, jak i odbierać sygnały, zapewniając płynny zasięg na większych obszarach z wieloma węzłami.

Uwaga:

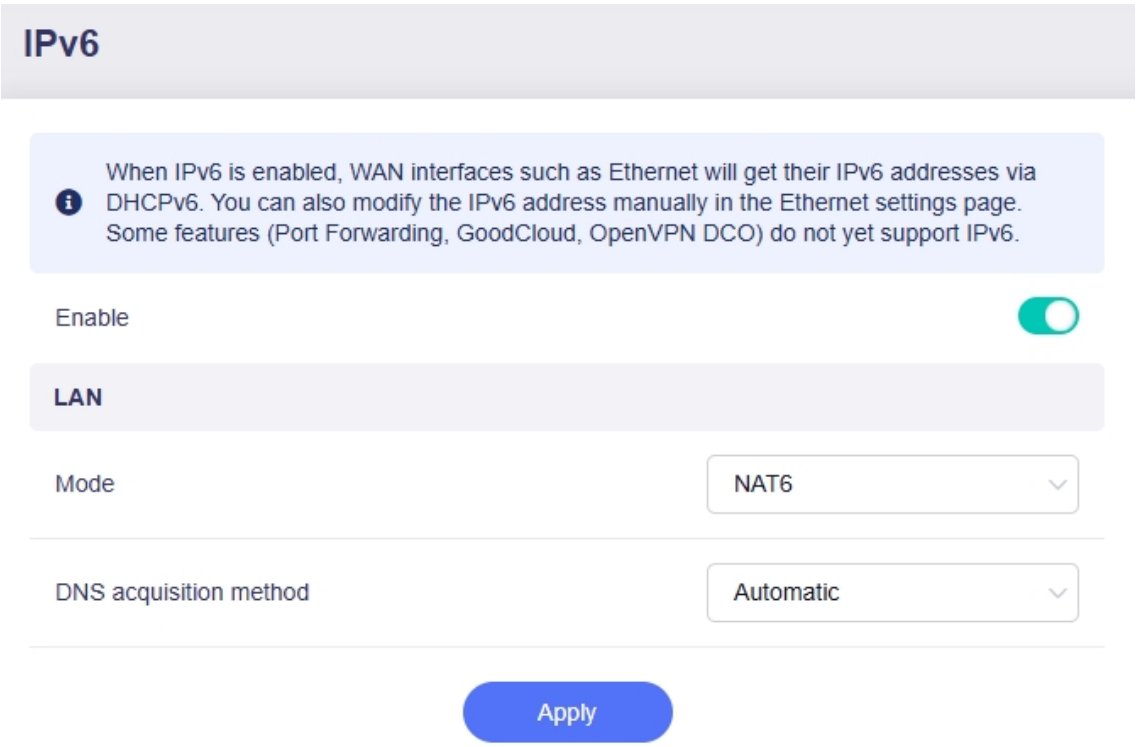
1. Po zmianie trybu sieciowego wszystkie urządzenia klienckie powinny ponownie połączyć się z routerem, aby zapewnić stabilną łączność.
2. **W trybie Access Point / WDS panel administracyjny nie jest dostępny pod pierwotnym adresem IP**. Zaloguj się do routera nadrzędnego, znajdź adres IP przydzielony temu routerowi i użyj go do otwarcia panelu administracyjnego. Jeśli nie masz dostępu do routera nadrzędnego, naciśnij i przytrzymaj przycisk resetowania przez 4 sekundy, aby przywrócić domyślny tryb Router.
3. **W trybach Access Point / Extender / WDS niedostępne są następujące funkcje**: kontrola dostępu (Allowlist i Blocklist), AstroWarp, VPN, AdGuard Home, kontrola rodzicielska, ZeroTier, Tailscale, przekierowanie portów, Multi-WAN, serwer DHCP, rezerwacja adresów, sieć gościnna, DNS, Ethernet Port, IPv6, Drop-in Gateway, IGMP Snooping, przyspieszanie sieci i ustawienia NAT.

14.8 IPv6

IPv6 (Internet Protocol version 6) to najnowsza wersja protokołu internetowego, zaprojektowana jako następca IPv4. Zapewnia większą pulę unikalnych adresów IP, rozwiązując problem wyczerpywania adresów IPv4 i obsługując rosnącą liczbę podłączonych urządzeń na świecie.

Zaloguj się do panelu administracyjnego routera i przejdź do **NETWORK** > **IPv6**. Tutaj możesz włączyć i skonfigurować IPv6. Po włączeniu interfejsy WAN, np. Ethernet, uzyskują adresy IPv6 przez DHCPv6.

Włącz **Enable**, wybierz tryb sieci głównej i sposób uzyskiwania DNS, a następnie kliknij **Apply.**



Uwaga: niektóre funkcje (np. zapora, GoodCloud, OpenVPN DCO) nie obsługują jeszcze IPv6. Ich jednoczesne włączenie z IPv6 może powodować problemy z połączeniem.

14.8.1 Tryb IPv6

Dostępne są cztery tryby: Native, Passthrough, NAT6 i Static IPv6.

- **Native**: odpowiedni, gdy router bezpośrednio uzyskuje publiczny adres IPv6 i automatycznie przydziela adresy IPv6 podłączonym urządzeniom. Spełnia potrzeby większości użytkowników korzystających z IPv6.
- **Passthrough**: odpowiedni, gdy pakiety IPv6 mają być przekazywane bezpośrednio, bez przetwarzania ani konwersji. Niektóre aplikacje lub usługi mogą wymagać zachowania pełnej zawartości pakietów IPv6 do dalszego przetwarzania lub analizy. Ten tryb jest używany przez specjalistów do diagnostyki sieci i analizy bezpieczeństwa.
- **NAT6**: odpowiedni, gdy router działa jako brama przydzielająca każdemu urządzeniu w sieci dynamiczny wewnętrzny adres IPv6. W tym trybie urządzenia końcowe łączą się przez terminal sieci optycznej i uzyskują adres IPv6 sieci lokalnej.
- **Static IPv6**: odpowiedni dla urządzeń i usług wymagających stałego adresu IPv6, np. serwerów lub drukarek sieciowych. Urządzenie zawsze używa tego samego adresu IPv6, co ułatwia zarządzanie i dostęp.

14.8.2 Sposób uzyskiwania DNS

Określa sposób uzyskiwania przez router adresów serwerów DNS IPv6. Dostępne są dwie opcje: Automatic i Manual.

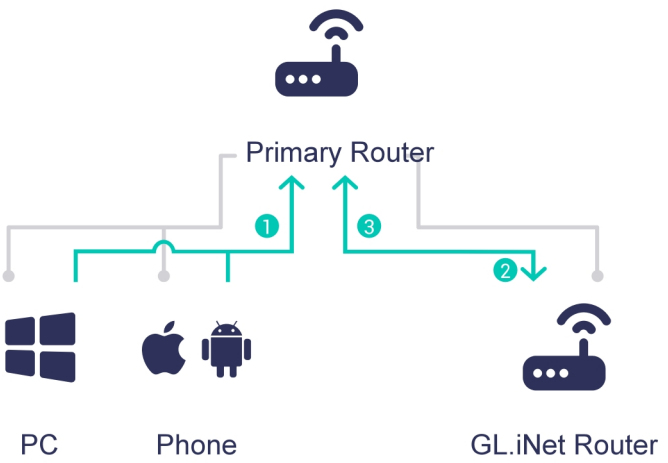
- **Automatic**: router dynamicznie uzyskuje adresy serwerów DNS IPv6 (np. przez DHCPv6).
- **Manual**: wprowadź własne adresy serwerów DNS IPv6. Ponieważ DNS służy do tłumaczenia nazw domen na odpowiadające im adresy IP, ręczna konfiguracja serwera DNS może powodować błędy rozwiązywania nazw. Używaj jej ostrożnie.

14.9 Drop-in Gateway

Drop-in Gateway rozszerza możliwości istniejącego głównego routera bez jego wymiany ani ponownej konfiguracji. Po podłączeniu routera GL.iNet do głównego routera kablem Ethernet można dodać do istniejącej infrastruktury zaawansowane funkcje, na przykład:

- Filtrowanie reklam przez AdGuard Home
- Włączenie klienta VPN
- Korzystanie z szyfrowanego DNS

Drop-in Gateway działa jako pośredni system sieciowy: kieruje ruch urządzeń klienckich przez router GL.iNet w celu przetworzenia, zanim zostanie on przesłany przez główny router. Zachowuje istniejące ustawienia sieci, zapewniając ciągłość połączeń wszystkich urządzeń, a w razie potrzeby umożliwia też zarządzanie ruchem wszystkich lub wybranych klientów.



Powyższy schemat zawiera dwa rodzaje linii: szare oraz zielone z trzema strzałkami oznaczonymi numerami.

- **Szare linie** przedstawiają fizyczną topologię połączeń: urządzenia klienckie (np. komputer stacjonarny i laptop) łączą się z głównym routerem, a jego port LAN jest połączony kablem Ethernet z portem WAN routera GL.iNet z włączonym Drop-in Gateway.
- **Zielone linie** przedstawiają kolejne etapy transmisji danych przy aktywnym Drop-in Gateway. Ponumerowane strzałki wskazują kolejność przepływu ruchu:

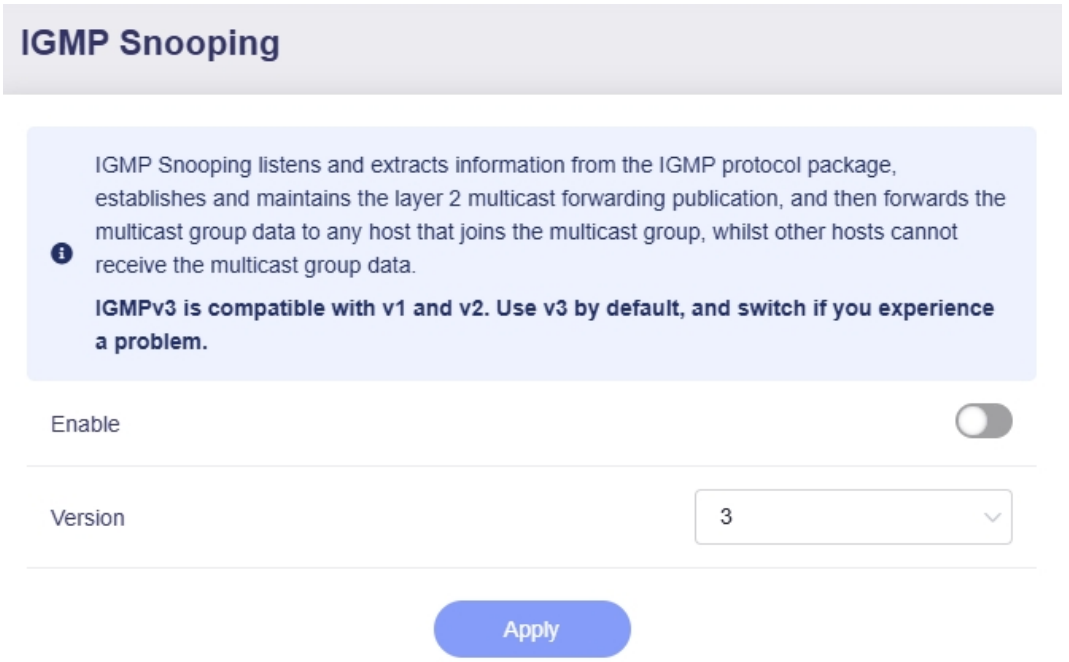
1. Ruch urządzeń klienckich jest najpierw kierowany do głównego routera;
2. Główny router przekazuje ruch do routera GL.iNet w celu przetworzenia (np. filtrowania reklam, szyfrowania VPN);
3. Po przetworzeniu ruch wraca do głównego routera, który dostarcza dane do pierwotnych urządzeń klienckich lub kieruje je do Internetu.

Możesz włączyć Drop-in Gateway dla wszystkich lub wybranych urządzeń podłączonych do głównego routera. Szczegóły znajdziesz pod tym łączem.

14.10 IGMP Snooping

IGMP Snooping nasłuchuje pakietów protokołu IGMP, wyodrębnia odpowiednie informacje oraz tworzy i utrzymuje tablicę przekazywania ruchu multicast w warstwie 2. Następnie przekazuje dane grupy multicast do hostów należących do tej grupy. Pozostałe hosty nie otrzymują tych danych.

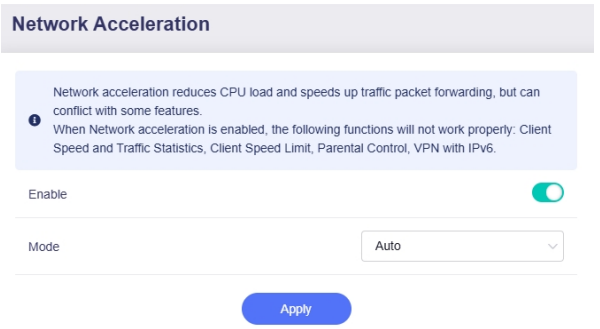
Zaloguj się do panelu administracyjnego routera i przejdź do **NETWORK** > **IGMP Snooping**. W razie potrzeby włącz tę opcję, aby korzystać z multicastu na routerze.



14.11 Przyspieszanie sieci

Przyspieszanie sieci zmniejsza obciążenie procesora i przyspiesza przekazywanie pakietów, ale może kolidować z niektórymi funkcjami.

Zaloguj się do panelu administracyjnego routera i przejdź do **NETWORK** > **Network Acceleration**. Na tej stronie możesz włączyć przyspieszanie sieci i wybrać tryb Auto, Hardware Acceleration lub Software Acceleration.

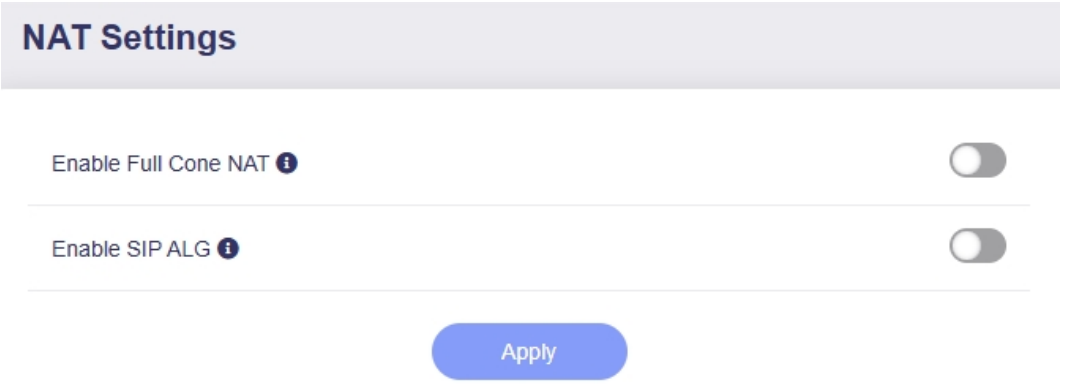


- **Auto**: automatycznie przełącza między dwoma trybami przyspieszania w zależności od sposobu użytkowania.
- **Hardware Acceleration**: przenosi często wykonywane zadania sieciowe (np. NAT, przekazywanie pakietów i weryfikację sum kontrolnych) do wyspecjalizowanego sprzętu, takiego jak procesory NPU lub układy HWNAT. Działa w połączeniach Ethernet i Repeater. W takich zastosowaniach, ze stałymi ścieżkami i prostymi regułami, zapewnia wysoką przepustowość, małe opóźnienia i minimalne obciążenie procesora przy transmisji z pełną prędkością łącza.
- **Software Acceleration**: wykorzystuje ogólny procesor routera wraz ze zoptymalizowanym jądrem lub sterownikami (np. SWNAT). Działa przy dostępie komórkowym (4G/5G), który jest typowym zastosowaniem bez dostępnego przyspieszania sprzętowego. Zapewnia szeroką zgodność i obsługę złożonych protokołów. Jest elastyczny, ale przy dużej przepustowości, szczególnie z włączonymi funkcjami zaawansowanymi, wydajność procesora może ograniczać szybkość transmisji.

Uwaga: po włączeniu przyspieszania sieci następujące funkcje nie działają prawidłowo: statystyki prędkości klientów, statystyki ruchu, ograniczanie prędkości, kontrola rodzicielska i VPN z IPv6.

14.12 Ustawienia NAT

Zaloguj się do panelu administracyjnego routera i przejdź do **NETWORK** > **NAT Settings**. Tutaj możesz skonfigurować dwie główne funkcje NAT: Full Cone NAT i SIP ALG.



- **Full Cone NAT**: może zmniejszać opóźnienia i poprawiać szybkość reakcji w grach sieciowych. Włączenie może jednak obniżyć bezpieczeństwo, ponieważ zezwala na nieograniczone połączenia przychodzące.
- **SIP ALG**: ma ograniczać wpływ wielu translacji NAT na ruch SIP (Session Initiation Protocol). W większości przypadków nie pomaga, a może nawet zakłócać połączenia VoIP, powodując jednostronny dźwięk, brak dzwonka telefonu, nieoczekiwane rozłączenia lub przekierowanie połączeń bezpośrednio do poczty głosowej.

Rozdział 15

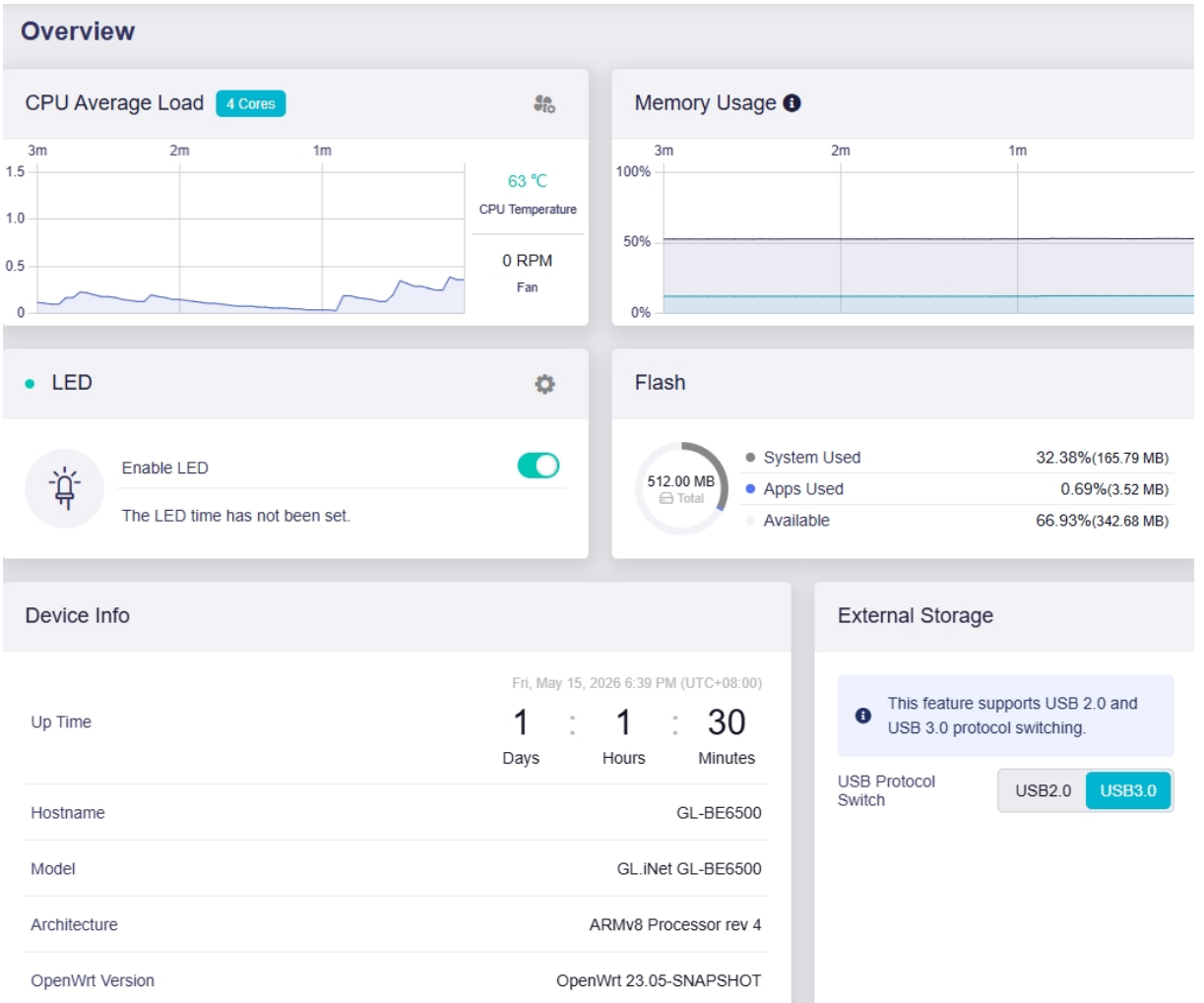
System

W tym rozdziale opisano narzędzia zarządzania urządzeniem: przegląd systemu, aktualizacje, zadania zaplanowane, strefę czasową, dziennik, resetowanie oprogramowania i ustawienia zaawansowane.

15.1 Przegląd

Zaloguj się do panelu administracyjnego routera i przejdź do **SYSTEM** > **Overview**. Strona wyświetla stan sprzętu i udostępnia proste funkcje sterowania, w tym:

- Stan procesora, pamięci RAM i pamięci flash
- Sterowanie diodą LED
- Informacje o urządzeniu
- Przełączanie protokołu pamięci zewnętrznej

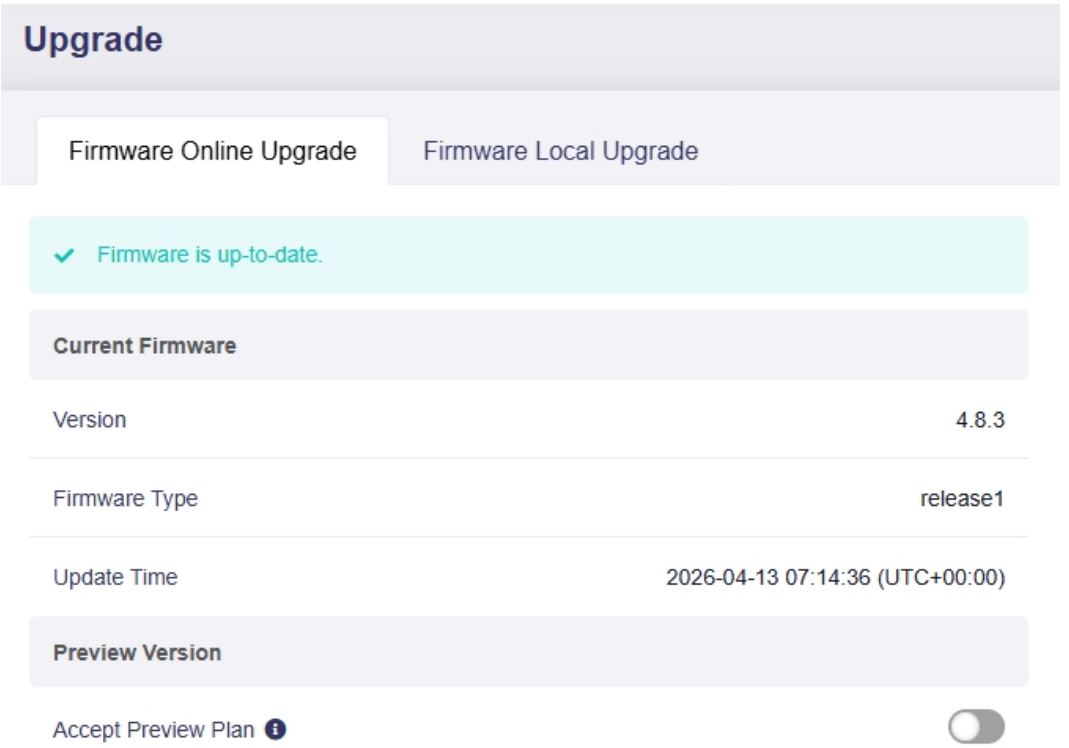


15.2 Aktualizacja

Zaloguj się do panelu administracyjnego routera i przejdź do **SYSTEM** > **Upgrade**. Oprogramowanie routera można aktualizować online lub lokalnie.

15.2.1 Aktualizacja online

Tutaj znajdziesz szczegóły bieżącego oprogramowania, w tym wersję, typ (np. wydanie stabilne, beta) i czas aktualizacji.



- **Accept Preview Plan**: po włączeniu tej opcji możesz testować nowe funkcje przed wydaniem wersji końcowej i przesyłać nam opinie. Wystarczy włączyć ją raz, aby pozostała aktywna. Te aktualizacje mogą być niestabilne.

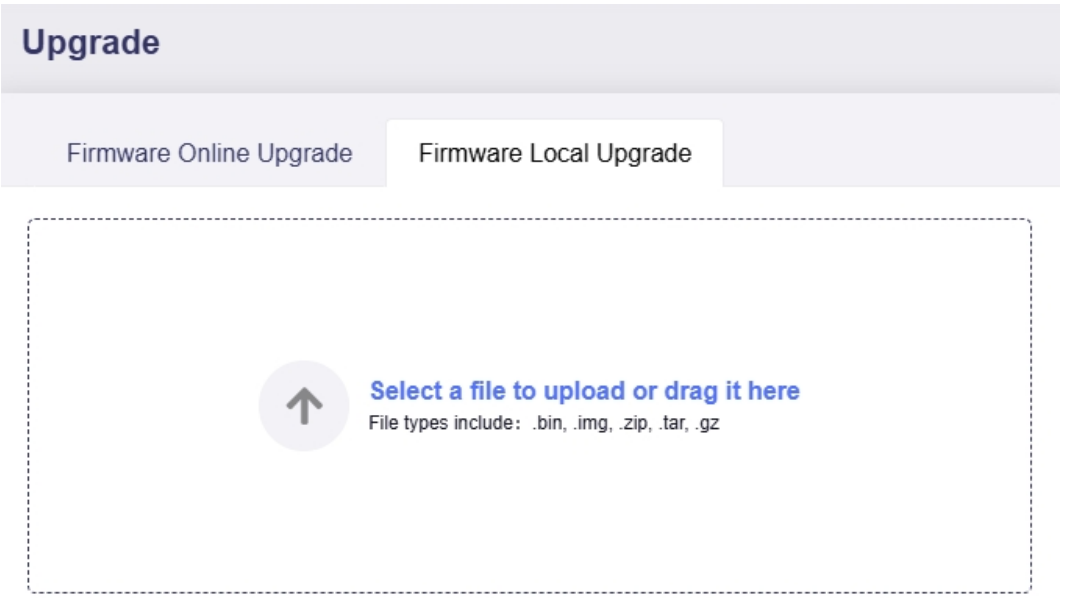
Jeśli router ma połączenie z Internetem, sprawdzi dostępność nowszej wersji oprogramowania do pobrania.

Wskazówka: jeśli podczas aktualizacji online pojawi się komunikat **Download Failed**, przejdź do **SYSTEM** -> **Time Zone** i popraw błąd strefy czasowej (zsynchronizuj z przeglądarką).

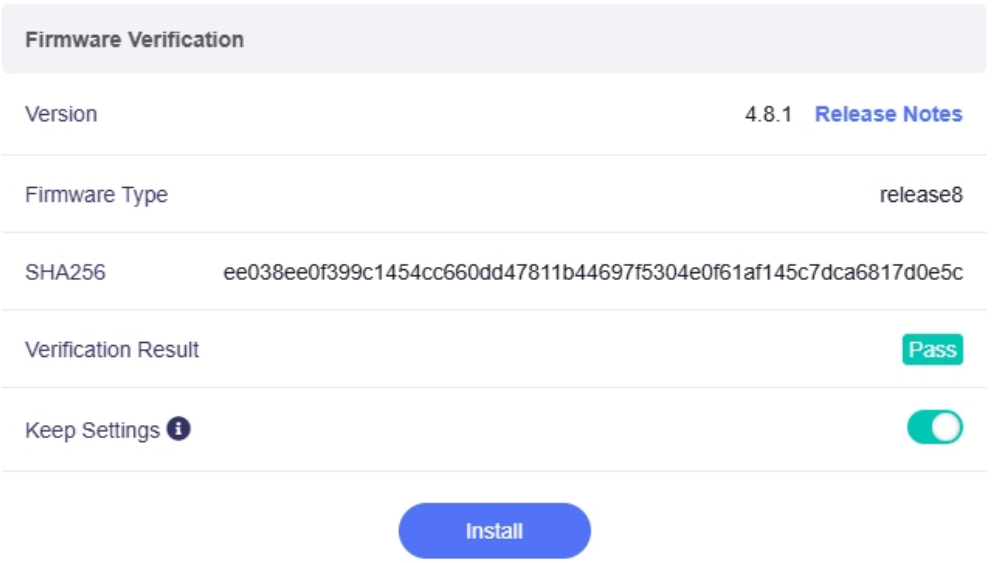
15.2.2 Aktualizacja lokalna

Aktualizacja lokalna nie wymaga połączenia routera z Internetem.

Pobierz właściwy pakiet oprogramowania dla swojego modelu routera z oficjalnego Centrum pobierania na urządzenie lokalne. Następnie zaloguj się do panelu administracyjnego routera, przejdź do sekcji **SYSTEM** > **Upgrade** > **Local Upgrade** i prześlij pakiet oprogramowania.



Na stronie pojawią się szczegóły oprogramowania. Sprawdź je przed kliknięciem **Install**.



- **Keep Settings**: po włączeniu bieżące ustawienia zostają zachowane. Pakiety zainstalowane ręcznie trzeba jednak zainstalować ponownie po zakończeniu aktualizacji. Nie włączaj tej opcji podczas instalowania starszej wersji oprogramowania.

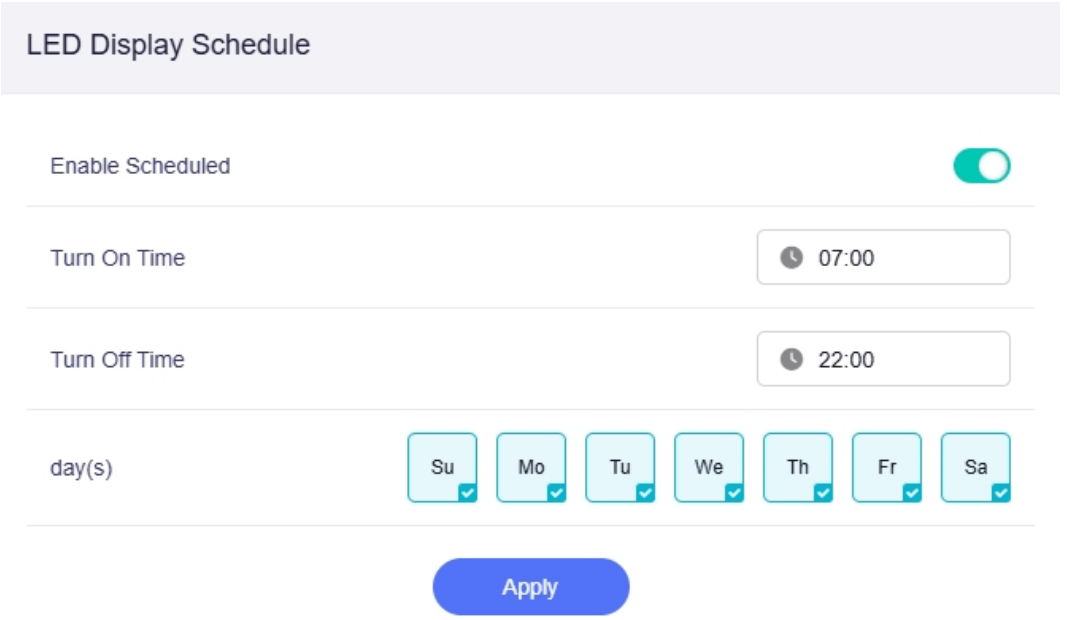
15.3 Zadania zaplanowane

Zaloguj się do panelu administracyjnego routera i przejdź do **SYSTEM** > **Scheduled Tasks**. Tutaj możesz ustawić codzienny harmonogram podstawowych czynności, takich jak włączanie i wyłączanie diody LED oraz ponowne uruchamianie routera.

Uwaga: przed użyciem tej funkcji zsynchronizuj czas w Time Zone. Jeśli urządzenie będzie wyłączone w zaplanowanym terminie, zadanie nie zostanie wykonane.

15.3.1 Harmonogram diody LED

W razie potrzeby ustaw harmonogram diody LED routera.

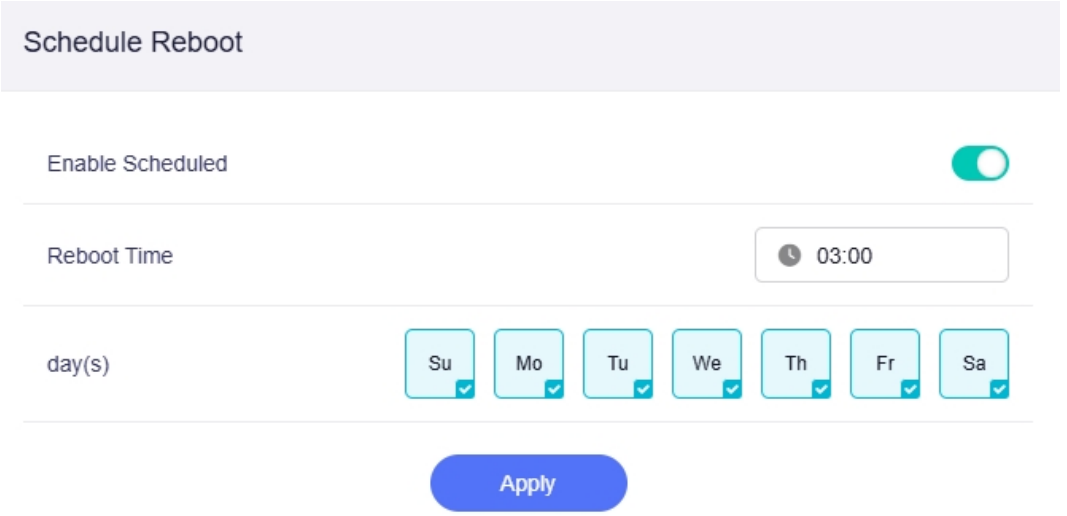


- **Enable Scheduled**: włącz ten przełącznik, aby uruchomić harmonogram diody LED.
- **Turn On Time**: ustaw godzinę włączenia diody LED (np. 07:00).
- **Turn Off Time**: ustaw godzinę wyłączenia diody LED (np. 22:00).
- **day(s)**: wybierz dni tygodnia, w których te ustawienia mają obowiązywać.

Po skonfigurowaniu kliknij **Apply**, aby zapisać ustawienia.

15.3.2 Harmonogram ponownego uruchamiania

W razie potrzeby ustaw harmonogram automatycznego ponownego uruchamiania routera.

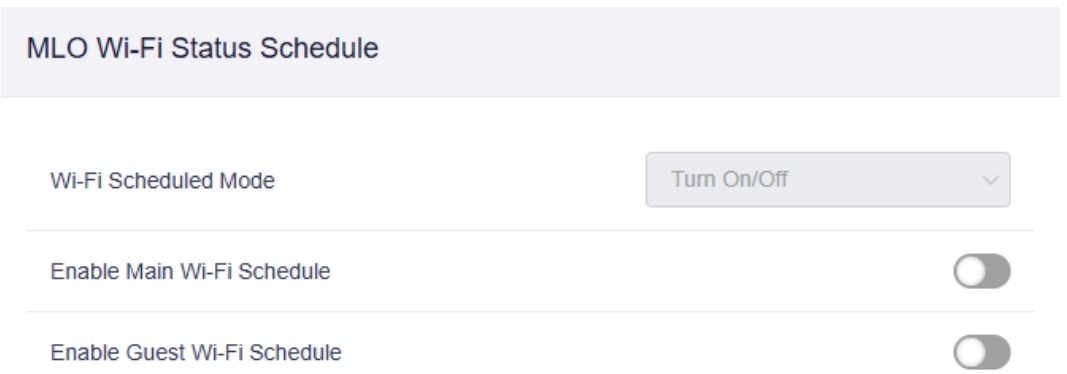


- **Enable Scheduled**: włącz ten przełącznik, aby uruchomić harmonogram ponownego uruchamiania.
- **Reboot Time**: ustaw konkretną godzinę ponownego uruchomienia routera (np. 03:00).
- **day(s)**: wybierz dni tygodnia, w których harmonogram ma obowiązywać.

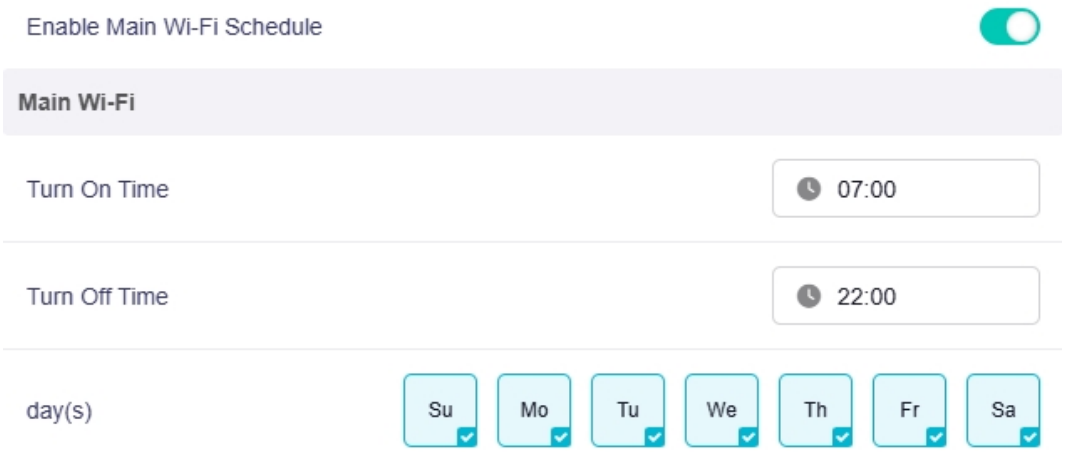
Po skonfigurowaniu kliknij **Apply**, aby zapisać ustawienia.

15.3.3 Harmonogram MLO Wi-Fi

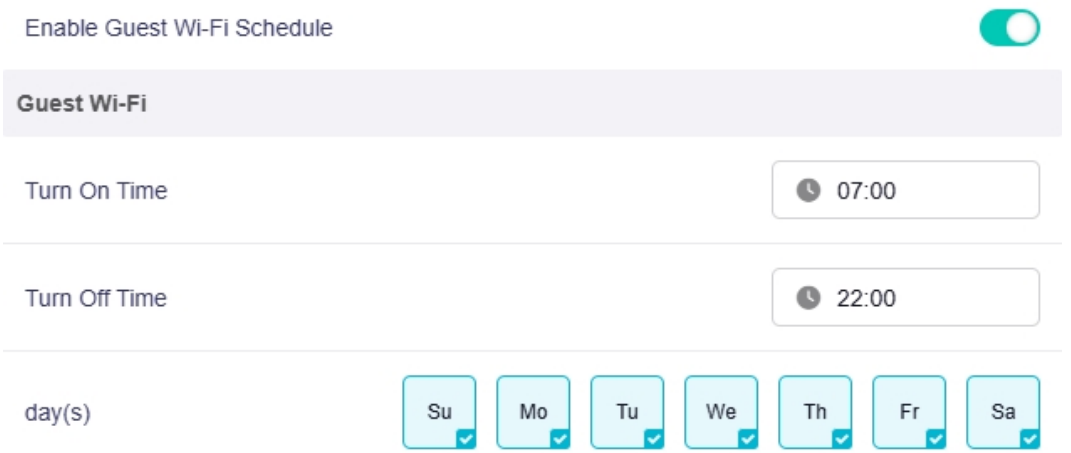
W razie potrzeby ustaw harmonogram sieci Wi-Fi MLO. Możesz włączyć harmonogram włączania i wyłączania głównej oraz gościnnej sieci Wi-Fi MLO.



- **Main Wi-Fi Schedule**: po włączeniu ustaw godziny włączania i wyłączania głównej sieci Wi-Fi MLO oraz wybierz dni tygodnia, w których harmonogram ma obowiązywać.



- **Guest Wi-Fi Schedule**: po włączeniu ustaw godziny włączania i wyłączania gościnnej sieci Wi-Fi MLO oraz wybierz dni tygodnia, w których harmonogram ma obowiązywać.



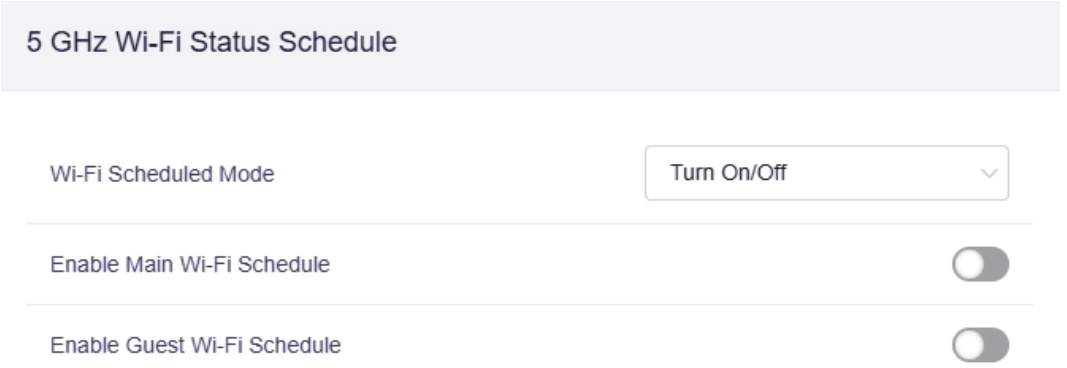
Po skonfigurowaniu kliknij **Apply**, aby zapisać ustawienia.

15.3.4 Harmonogram Wi-Fi 5 GHz

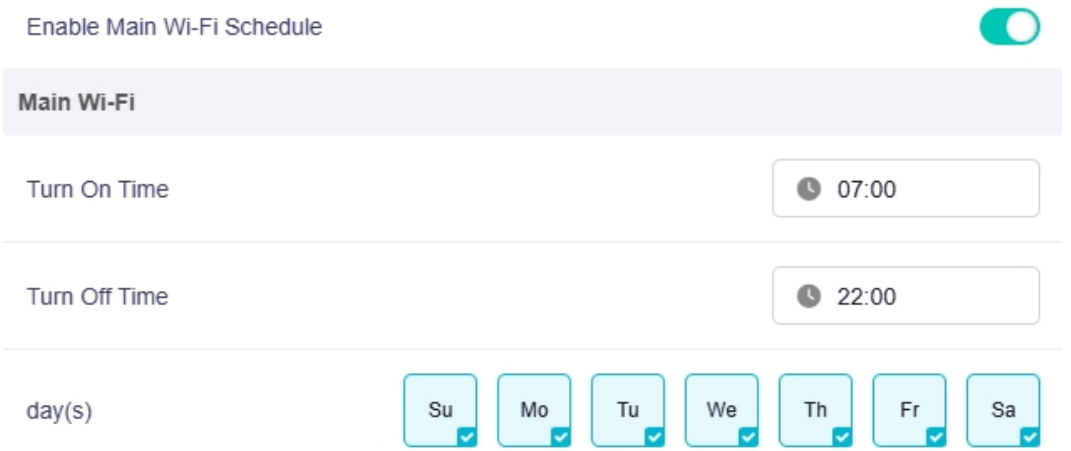
Ta funkcja umożliwia ustawienie harmonogramu Wi-Fi 5 GHz. Dostępne są dwa tryby: Turn On/Off i Switch TX Power.

Tryb 1: włączanie i wyłączanie (Turn On/Off)

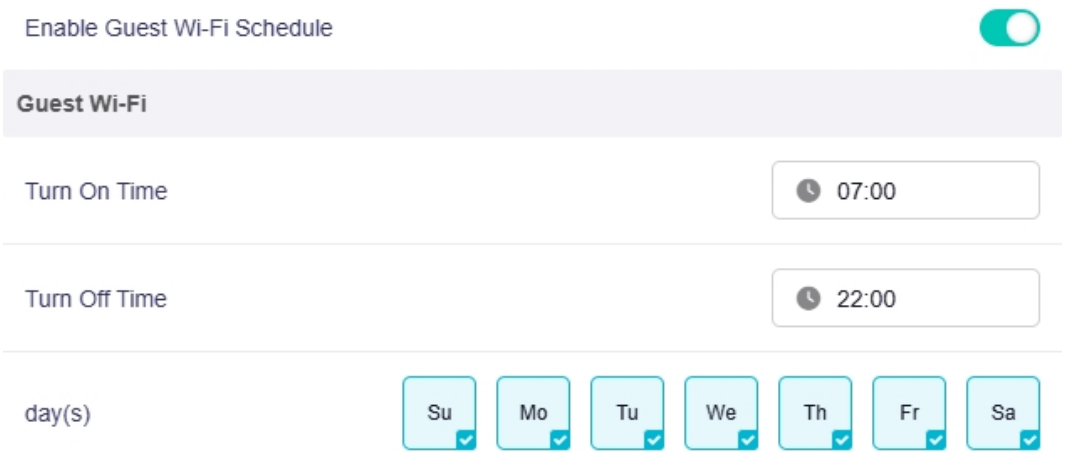
Możesz włączyć harmonogram włączania i wyłączania głównej oraz gościnnej sieci Wi-Fi 5 GHz.



- **Main Wi-Fi Schedule**: po włączeniu ustaw godziny włączania i wyłączania głównej sieci Wi-Fi 5 GHz oraz wybierz dni tygodnia, w których harmonogram ma obowiązywać.



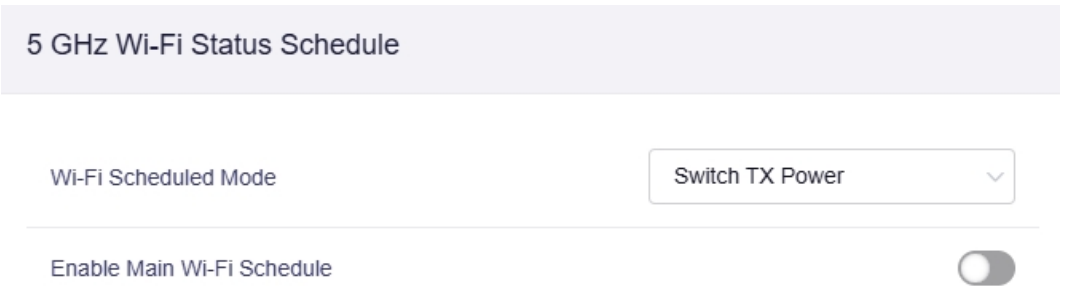
- **Guest Wi-Fi Schedule**: po włączeniu ustaw godziny włączania i wyłączania gościnnej sieci Wi-Fi 5 GHz oraz wybierz dni tygodnia, w których harmonogram ma obowiązywać.



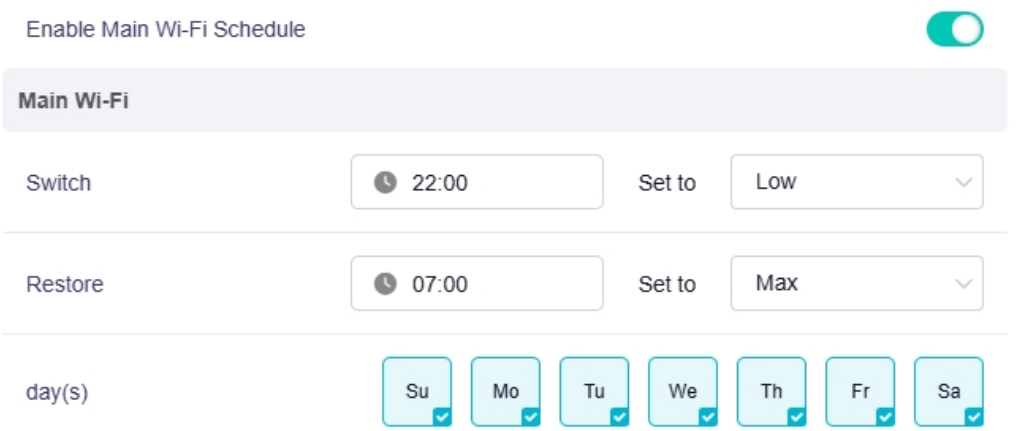
Po skonfigurowaniu kliknij **Apply**, aby zapisać ustawienia.

Tryb 2: przełączanie mocy nadawania (Switch TX Power)

Możesz włączyć harmonogram przełączania mocy nadawania głównej sieci Wi-Fi 5 GHz.



Po włączeniu ustaw dwie zaplanowane zmiany mocy nadawania i wybierz dni tygodnia, w których harmonogram ma obowiązywać.



- **Switch**: o wybranej porze (np. 22:00) ustawia moc nadawania (np. Low).
- **Restore**: przywraca inny poziom mocy nadawania (np. Max) o innej godzinie (np. 07:00).
- **days**: wybierz dni tygodnia, w których harmonogram ma obowiązywać.

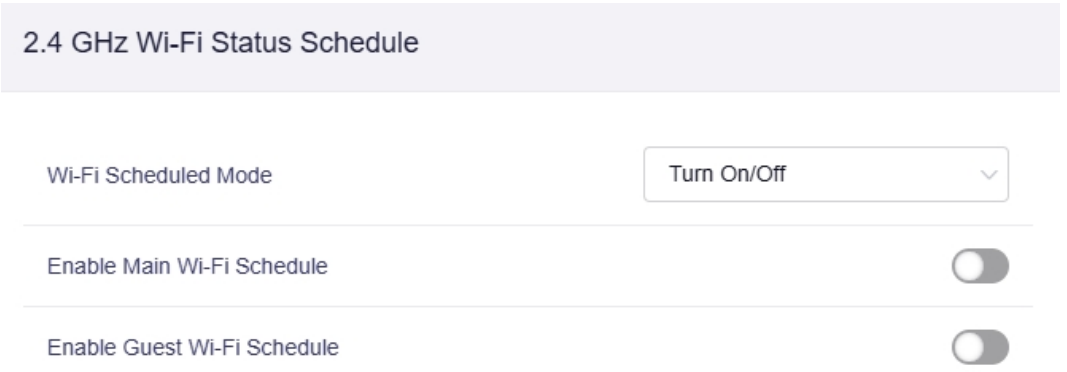
Po skonfigurowaniu kliknij **Apply**, aby zapisać ustawienia.

15.3.5 Harmonogram Wi-Fi 2,4 GHz

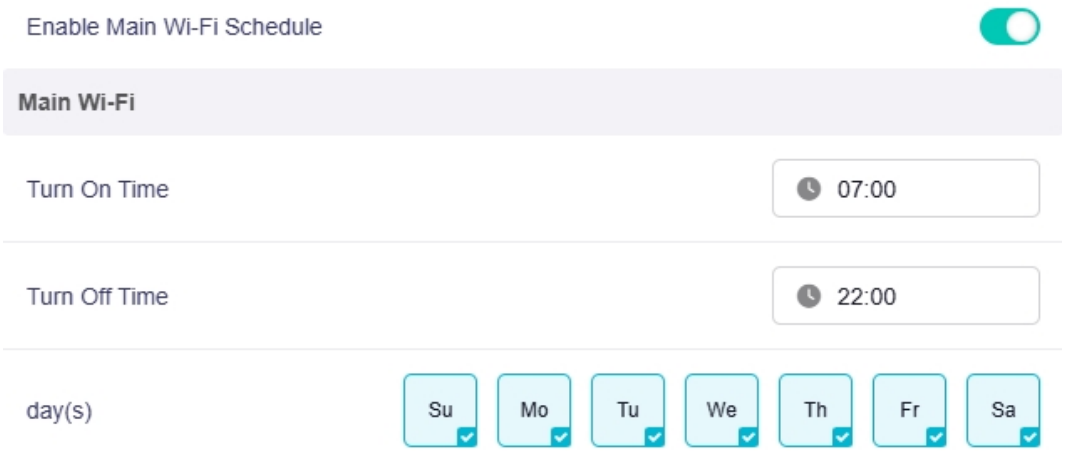
Ta funkcja umożliwia ustawienie harmonogramu Wi-Fi 2,4 GHz. Dostępne są dwa tryby: Turn On/Off i Switch TX Power.

Tryb 1: włączanie i wyłączanie (Turn On/Off)

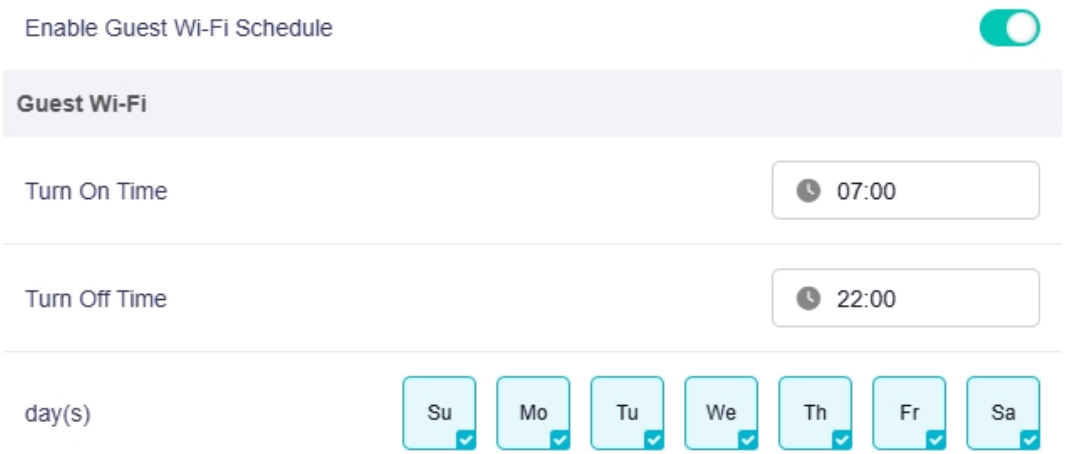
Możesz włączyć harmonogram włączania i wyłączania głównej oraz gościnnej sieci Wi-Fi 2,4 GHz.



- **Main Wi-Fi Schedule**: po włączeniu ustaw godziny włączania i wyłączania głównej sieci Wi-Fi 2,4 GHz oraz wybierz dni tygodnia, w których harmonogram ma obowiązywać.



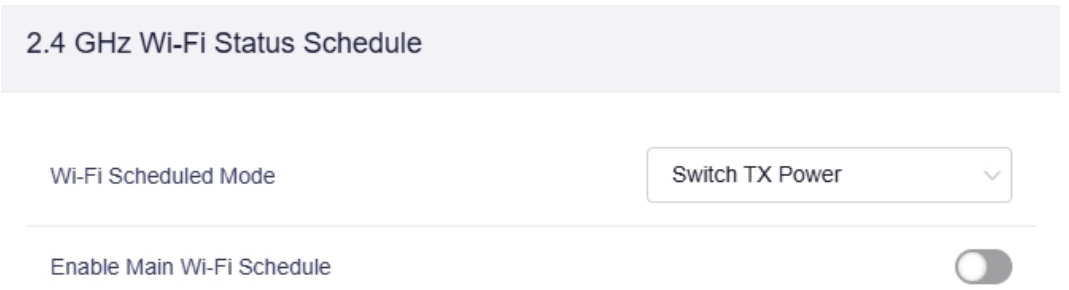
- **Guest Wi-Fi Schedule**: po włączeniu ustaw godziny włączania i wyłączania gościnnej sieci Wi-Fi 2,4 GHz oraz wybierz dni tygodnia, w których harmonogram ma obowiązywać.



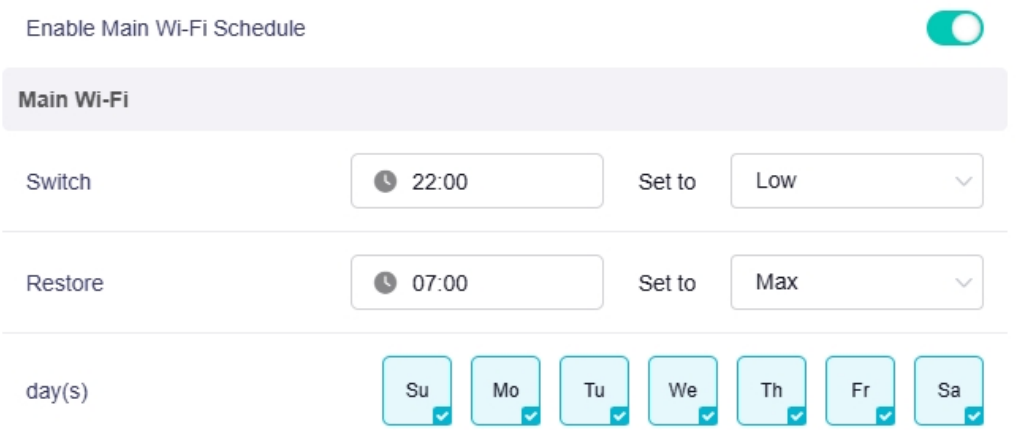
Po skonfigurowaniu kliknij **Apply**, aby zapisać ustawienia.

Tryb 2: przełączanie mocy nadawania (Switch TX Power)

Możesz włączyć harmonogram przełączania mocy nadawania głównej sieci Wi-Fi 2,4 GHz.



Po włączeniu ustaw dwie zaplanowane zmiany mocy nadawania i wybierz dni tygodnia, w których harmonogram ma obowiązywać.

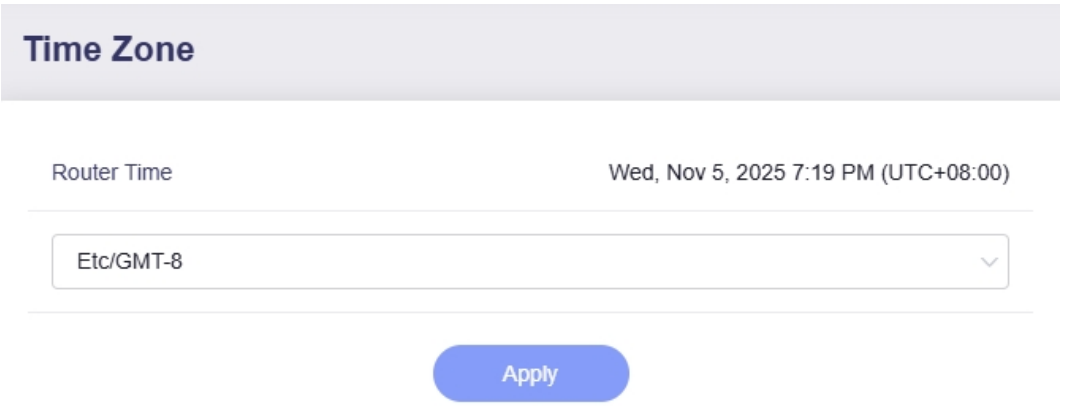


- **Switch**: o wybranej porze (np. 22:00) ustawia moc nadawania (np. Low).
- **Restore**: przywraca inny poziom mocy nadawania (np. Max) o innej godzinie (np. 07:00).
- **days**: wybierz dni tygodnia, w których te ustawienia mają obowiązywać.

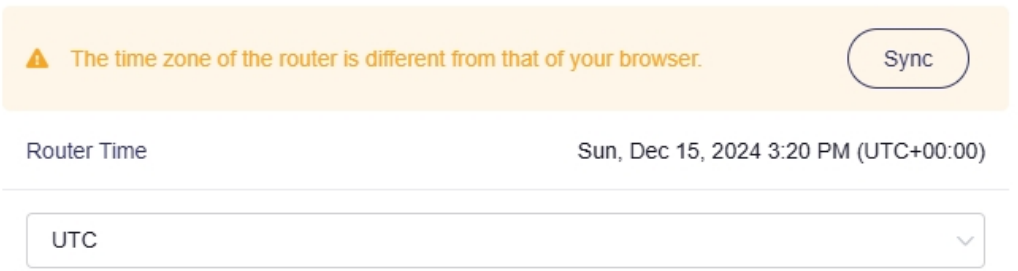
Po skonfigurowaniu kliknij **Apply**, aby zapisać ustawienia.

15.4 Strefa czasowa

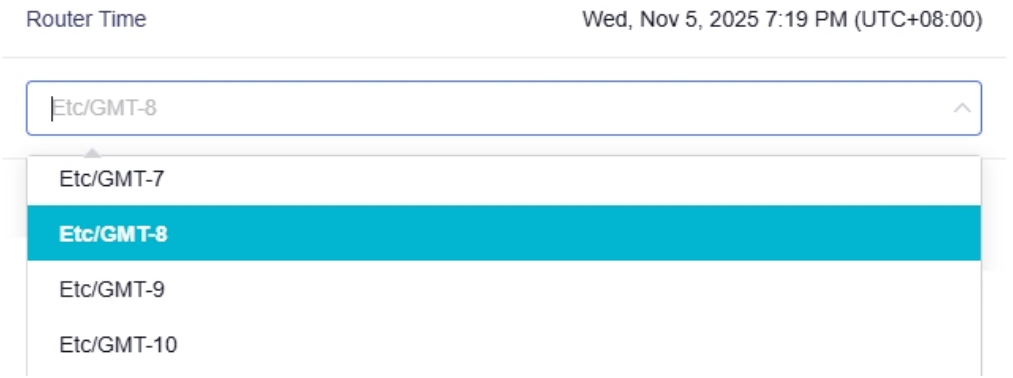
Zaloguj się do panelu administracyjnego routera i przejdź do **SYSTEM** > **Time Zone**. Strona wyświetla czas systemowy routera: datę, godzinę i odpowiadające im przesunięcie strefy czasowej.



Niektóre funkcje zależą od czasu systemowego routera. Upewnij się, że właściwa strefa czasowa jest prawidłowo zsynchronizowana. Jeśli strefa routera różni się od strefy przeglądarki, pojawi się poniższy komunikat. Kliknij przycisk **Sync**, aby zsynchronizować strefę czasową.

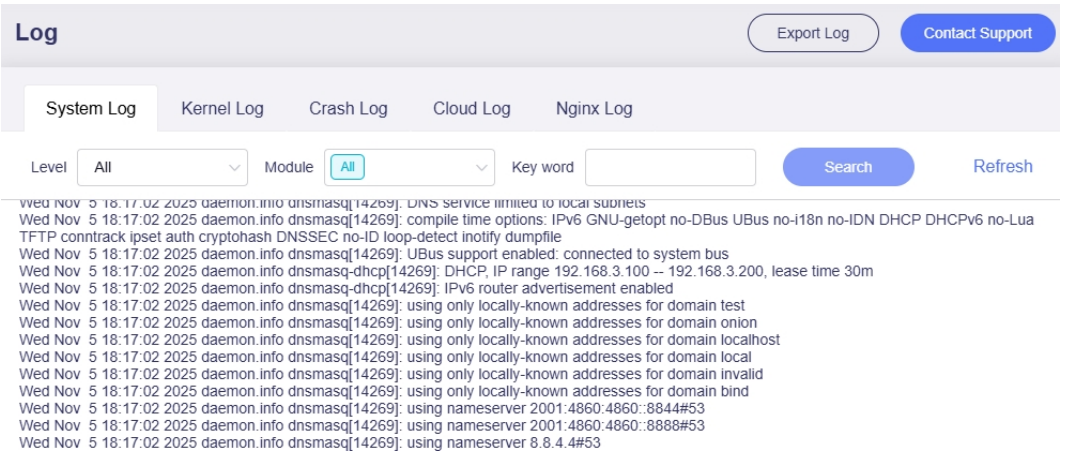


Aby zmienić strefę czasową, wybierz odpowiednią pozycję z listy, tak aby czas systemowy routera odpowiadał czasowi lokalnemu.

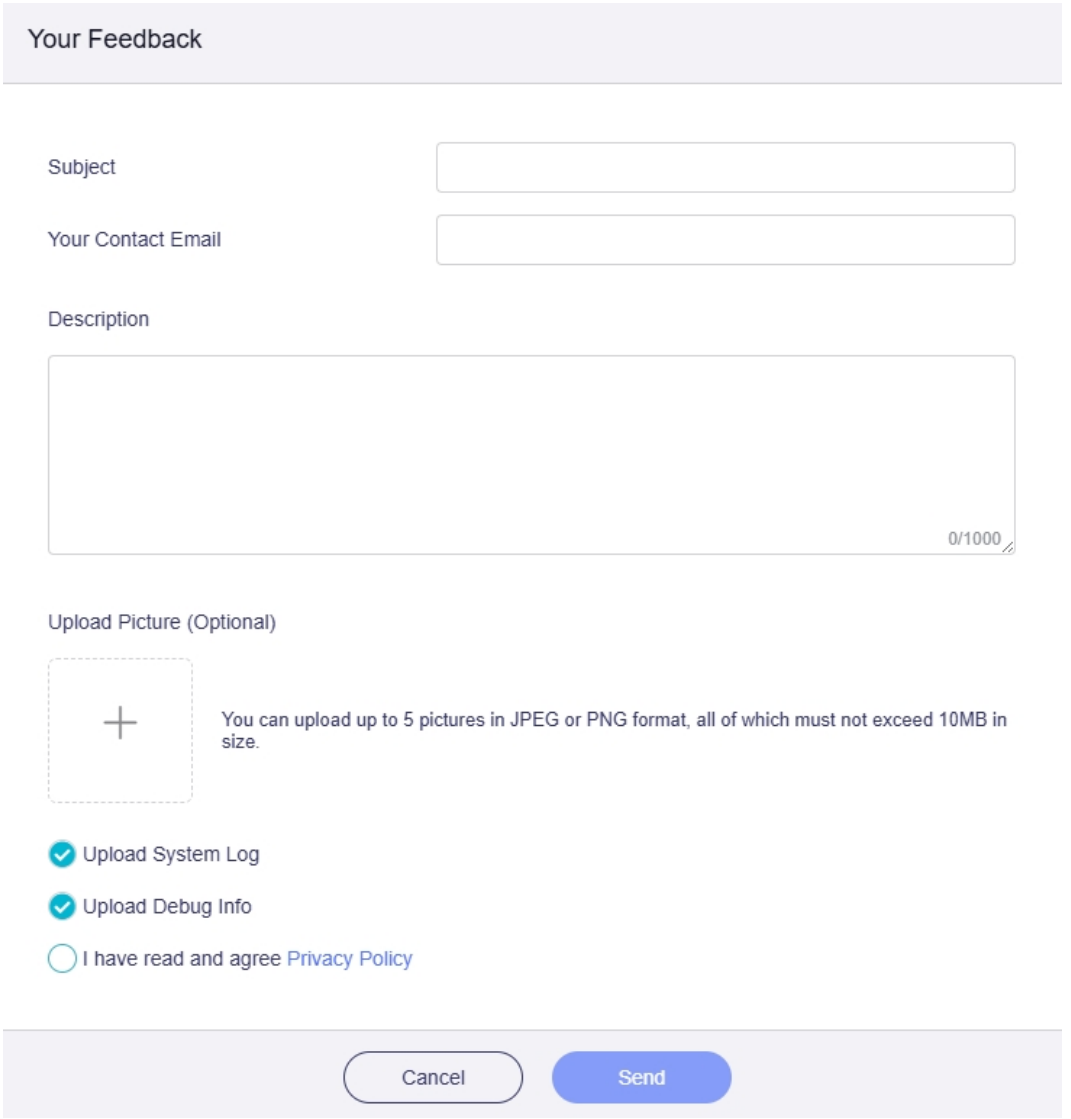

Router Time
Wed, Nov 5, 2025 7:19 PM (UTC+08:00)
Etc/GMT-8
Etc/GMT-7
Etc/GMT-8
Etc/GMT-9
Etc/GMT-10

15.5 Dziennik

Zaloguj się do panelu administracyjnego routera i przejdź do **SYSTEM** > **Log**. Tutaj możesz przeglądać dzienniki System, Kernel, Crash, Cloud i Nginx do analizy i rozwiązywania problemów. Ponadto niektóre modele komórkowe z obsługą eSIM udostępniają dziennik eSIM.



- **Search**: strona dziennika systemowego umożliwia filtrowanie w celu szybkiego wyszukiwania. Możesz wybrać z listy poziom dziennika (np. all, info, error) lub moduł (np. IPv6, Tethering, Cellular) albo wprowadzić słowa kluczowe, aby szybko przeszukać dzienniki.
- **Refresh**: kliknij ten przycisk, aby odświeżyć dzienniki.
- **Export Log**: kliknij ten przycisk, aby wyeksportować informacje diagnostyczne wraz z dziennikami.
- **Contact Support**: kliknij ten przycisk, wypełnij szczegółowe informacje w wyskakującym oknie po prawej stronie, a następnie kliknij **Send**. Twoja wiadomość zostanie wysłana bezpośrednio do pomocy technicznej GL.iNet.


Your Feedback
Subject
Your Contact Email
Description
0/1000
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

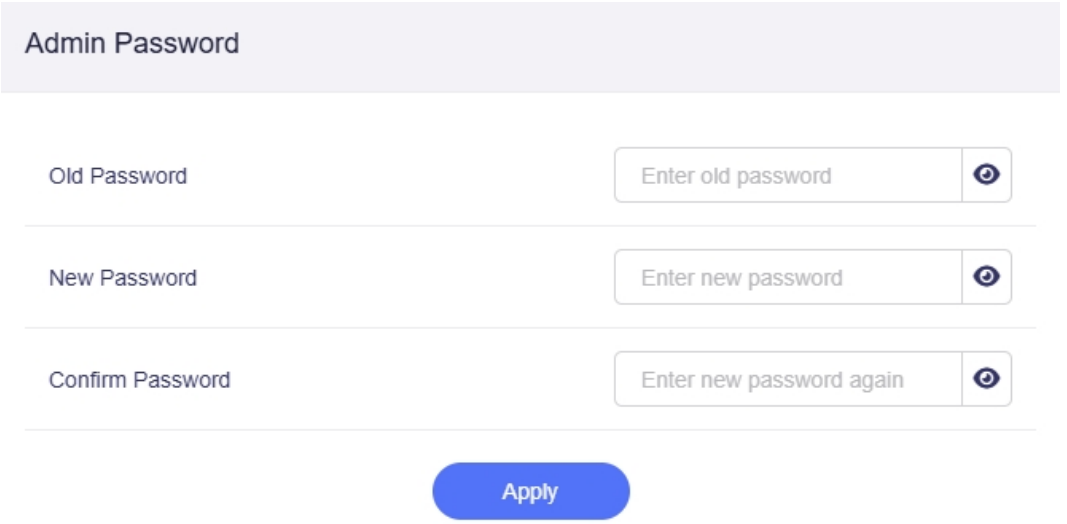
15.6 Bezpieczeństwo

Zaloguj się do panelu administracyjnego routera i przejdź do **SYSTEM** > **Security**. Strona zawiera opcje konfiguracji zarządzania lokalnego i zdalnego, w tym:

- Hasło administratora
- Lokalny dostęp do panelu administracyjnego, LuCI i SSH
- Zdalny dostęp przez HTTPS/SSH
- Zarządzanie otwartymi portami routera

15.6.1 Hasło administratora

W tej sekcji możesz zmienić hasło logowania do panelu administracyjnego.

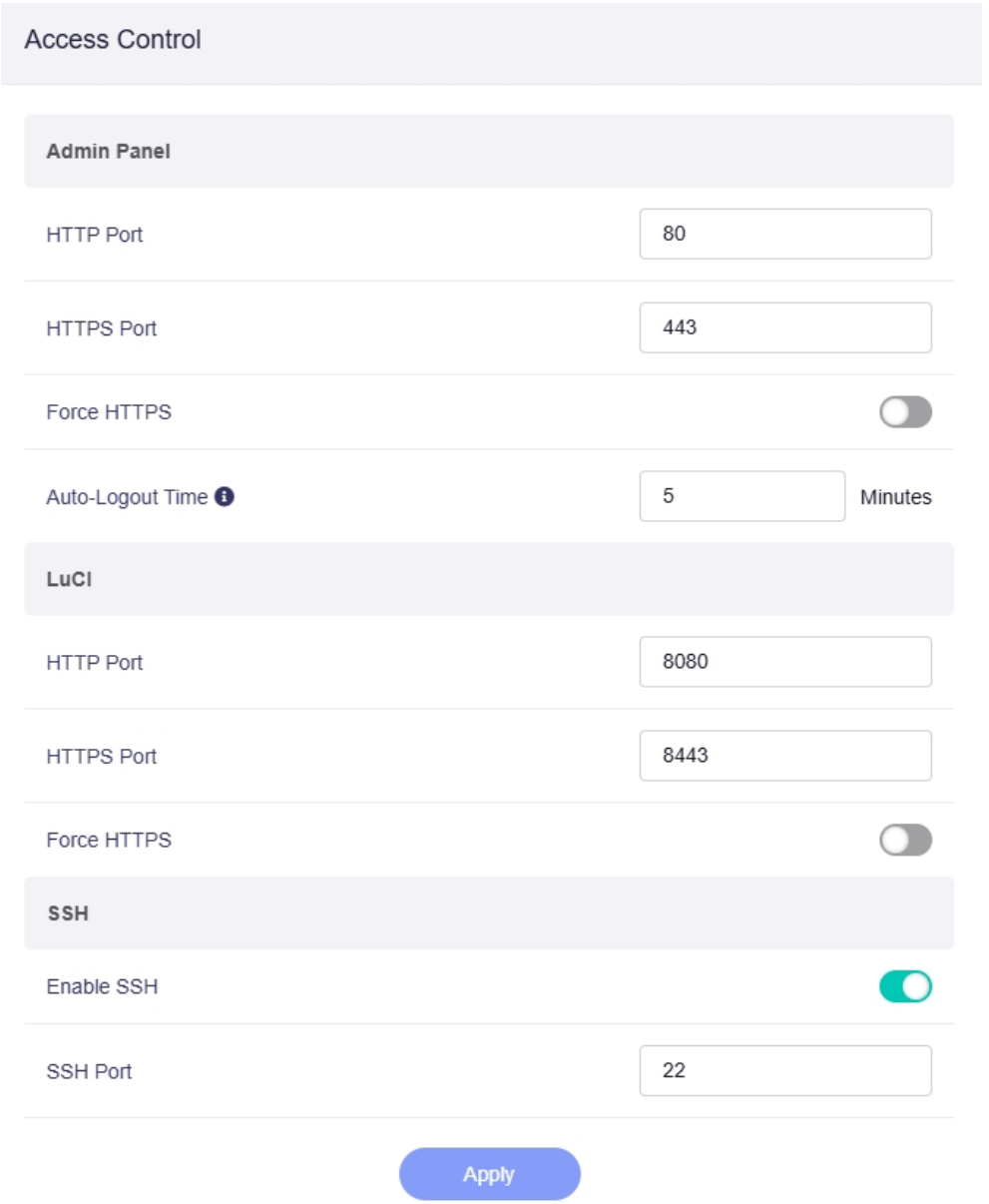


Wymagania dotyczące hasła administratora:

1. Długość od 10 do 63 znaków.
2. Dozwolone są litery (z rozróżnianiem wielkości), cyfry i symbole (np. ! @ # $ % ^ & * ( ) _ + - = , . > < | ? / \ [ ] { } : ; " ' ` ~).
3. Wymagane są co najmniej dwa rodzaje znaków spośród: wielkie litery, małe litery, cyfry i symbole.

15.6.2 Kontrola dostępu

Ta sekcja zarządza dostępem do różnych interfejsów routera (panel administracyjny, LuCI i SSH). Pozwala zapobiegać skanowaniu i próbom włamania na domyślnym porcie oraz unikać problemów sieciowych spowodowanych konfliktami portów.



Panel administracyjny

- **HTTP Port**: domyślnie 80; służy do nieszyfrowanego dostępu HTTP do panelu administracyjnego.
- **HTTPS Port**: domyślnie 443; służy do bezpiecznego dostępu HTTPS do panelu administracyjnego.

- **Force HTTPS**: po włączeniu wymusza używanie bezpiecznego połączenia HTTPS przy dostępie do panelu administracyjnego.
- **Auto-Logout Time**: domyślnie 5 minut. Ze względów bezpieczeństwa po tym czasie bezczynne sesje administratora są automatycznie wylogowywane. Możesz ustawić czas od 1 minuty do 3 godzin.

LuCI

Uwaga: przed skonfigurowaniem kontroli dostępu do LuCI zainstaluj go w Advanced Settings.

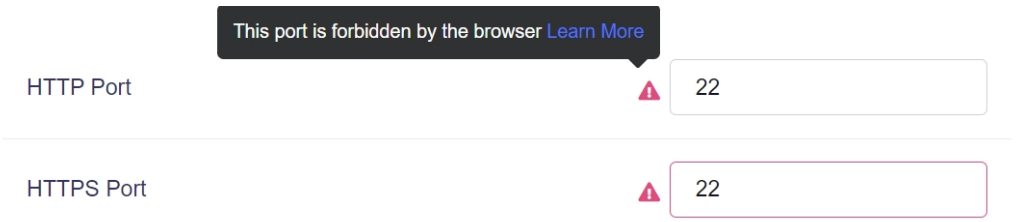
- **HTTP Port**: domyślnie 8080; służy do nieszyfrowanego dostępu HTTP do interfejsu LuCI.
- **HTTPS Port**: domyślnie 8443; służy do bezpiecznego dostępu HTTPS do interfejsu LuCI.
- **Force HTTPS**: po włączeniu wymusza bezpieczne połączenie HTTPS z interfejsem LuCI.

SSH

- **Enable SSH**: domyślnie włączone; określa, czy dozwolony jest dostęp do routera przez SSH.
- **SSH Port**: domyślnie 22; port dostępu SSH do routera.

Uwaga:

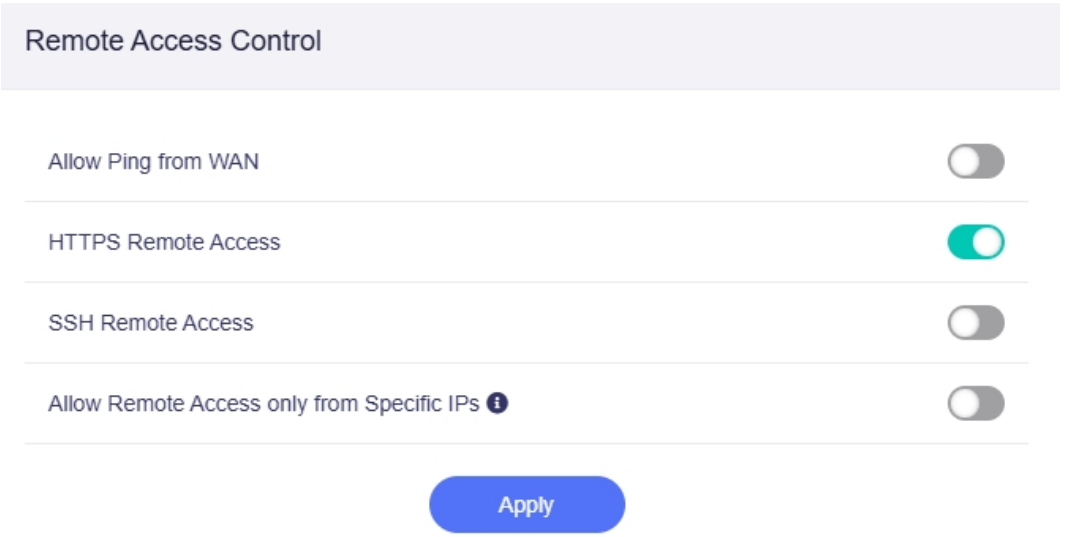
1. Jeśli przypiszesz numer kolidujący z portem zastrzeżonym (lub zarezerwowanym dla określonych usług przez przeglądarki albo konwencje sieciowe), pojawi się komunikat „This port is forbidden by the browser”.



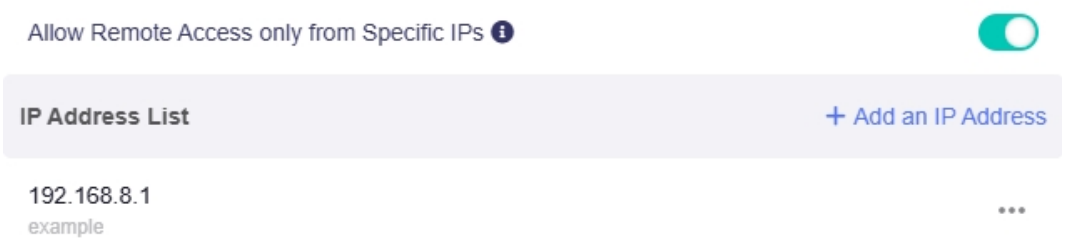
2. Po zmianie numeru portu w oprogramowaniu trzeba podawać prawidłowy numer, aby otworzyć panel administracyjny. Jeśli zapomnisz numeru, zresetuj router, aby przywrócić port domyślny.
3. Ustawienia dostępu do LuCI są dostępne dopiero po jego zainstalowaniu. Jeśli ich nie widać, przejdź do **SYSTEM** > **Advanced Settings**, aby zainstalować LuCI.

15.6.3 Kontrola dostępu zdalnego

Ta sekcja zarządza zdalnym dostępem do interfejsów routera, w tym HTTPS, SSH i ping od strony WAN. Pozwala też ograniczyć dostęp do określonych adresów IP, zachowując równowagę między dostępnością zdalną a bezpieczeństwem sieci.

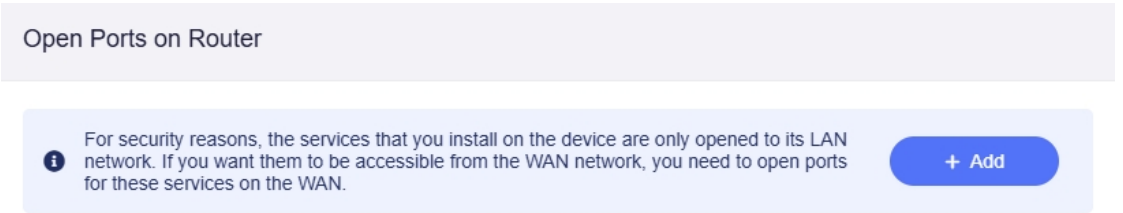


- **Allow Ping from WAN**: zezwolenie na ping od strony WAN pomaga sprawdzić dostępność routera przez WAN w razie problemów z siecią oraz określić opóźnienie i utratę pakietów.
- **HTTPS Remote Access**: umożliwia bezpieczny zdalny dostęp do panelu administracyjnego przez HTTPS. Zapewnia szyfrowaną transmisję danych podczas zdalnego zarządzania routerem w przeglądarce.
- **SSH Remote Access**: umożliwia bezpieczny dostęp do terminala routera. Pozwala zdalnie zarządzać routerem przez SSH za pomocą zaszyfrowanego tunelu.
- **Allow Remote Access from Specific IPs**: funkcja jest dostępna tylko po włączeniu co najmniej jednej z powyższych trzech opcji. Możesz dodać wiele określonych adresów IP, aby zdalnie zarządzać routerem wyłącznie z urządzeń o tych adresach.

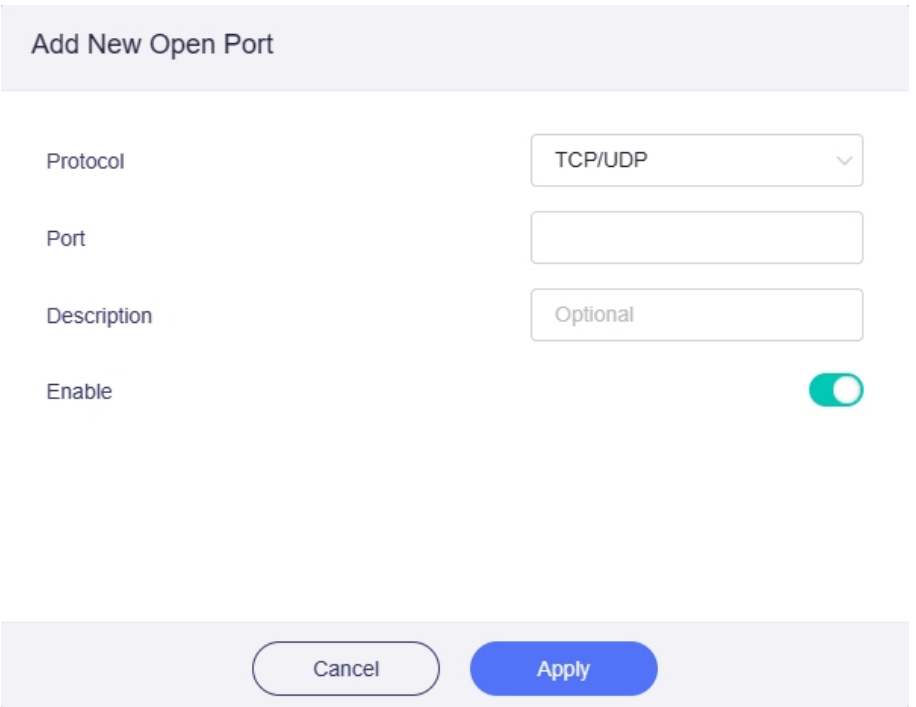


15.6.4 Otwieranie portów routera

Ta sekcja zarządza przekierowaniem portów dla usług routera. Niektóre usługi, np. WWW i FTP, wymagają otwarcia odpowiednich portów routera, aby były publicznie dostępne z sieci WAN. Ze względów bezpieczeństwa usługi zainstalowane na urządzeniu są domyślnie dostępne tylko w sieci LAN. Jeśli potrzebujesz dostępu z WAN, możesz otworzyć tutaj określone porty.



Aby otworzyć port, kliknij **Add** i wprowadź wymagane informacje w wyskakującym oknie.

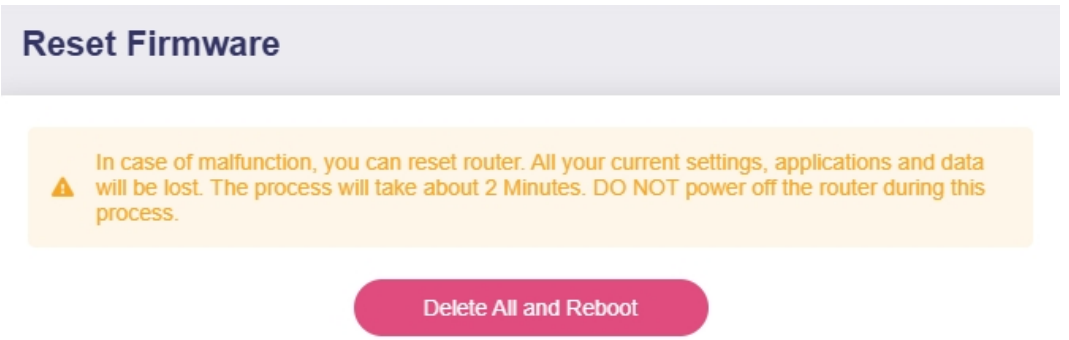


- **Protocol**: wybierz protokół sieciowy portu (TCP, UDP lub TCP/UDP). Określa on sposób przesyłania danych dla usługi powiązanej z portem.
- **Port**: wprowadź numer portu, który chcesz otworzyć.
- **Description** (opcjonalnie): dodaj krótką informację opisującą przeznaczenie otwartego portu (np. „Serwer WWW” lub „Usługa FTP”), aby ułatwić zarządzanie.
- **Enable**: użyj tego przełącznika, aby włączyć lub wyłączyć regułę przekierowania portów.

15.7 Resetowanie oprogramowania

Jeśli router działa nieprawidłowo, możesz spróbować rozwiązać problem przez zresetowanie oprogramowania.

Zaloguj się do panelu administracyjnego routera i przejdź do **SYSTEM** > **Reset Firmware**. W razie potrzeby kliknij **Delete All and Reboot**, aby zresetować oprogramowanie.



Uwaga: wszystkie bieżące ustawienia, aplikacje i dane zostaną usunięte. Proces trwa około 2 minut. W tym czasie nie wyłączaj zasilania routera.

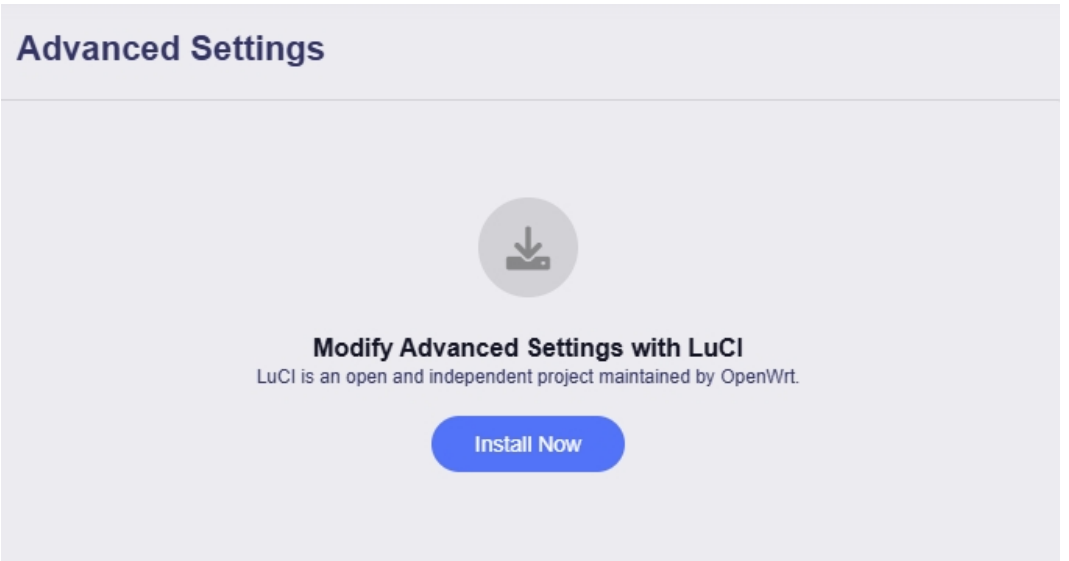
Jeśli panel administracyjny routera jest niedostępny, spróbuj zresetować router za pomocą fizycznego przycisku resetowania z boku urządzenia.

15.8 Ustawienia zaawansowane

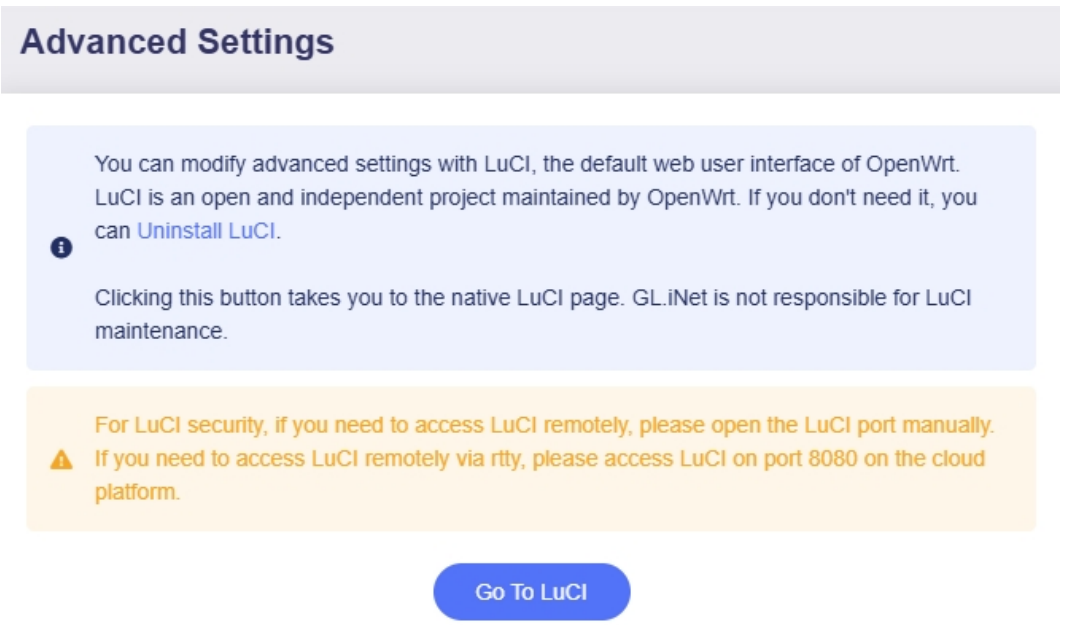
Zaloguj się do panelu administracyjnego routera i przejdź do **SYSTEM** > **Advanced Settings**. Tutaj możesz zmieniać ustawienia zaawansowane w LuCI, domyślnym interfejsie internetowym OpenWrt. LuCI to otwarty, niezależny projekt utrzymywany przez OpenWrt, udostępniany w obecnej postaci. GL.iNet nie odpowiada za jego utrzymanie.

Aby zalogować się do interfejsu LuCI, wykonaj poniższe czynności.

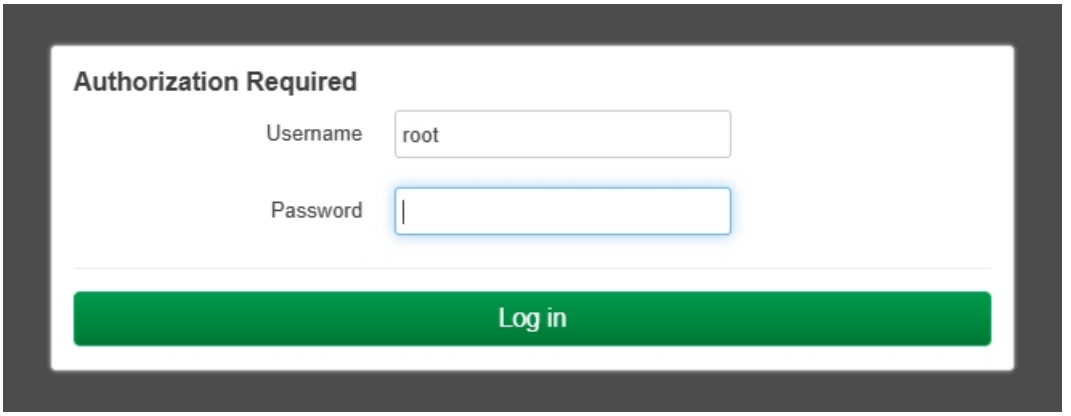
1. Kliknij **Install Now**, aby rozpocząć instalację interfejsu LuCI.



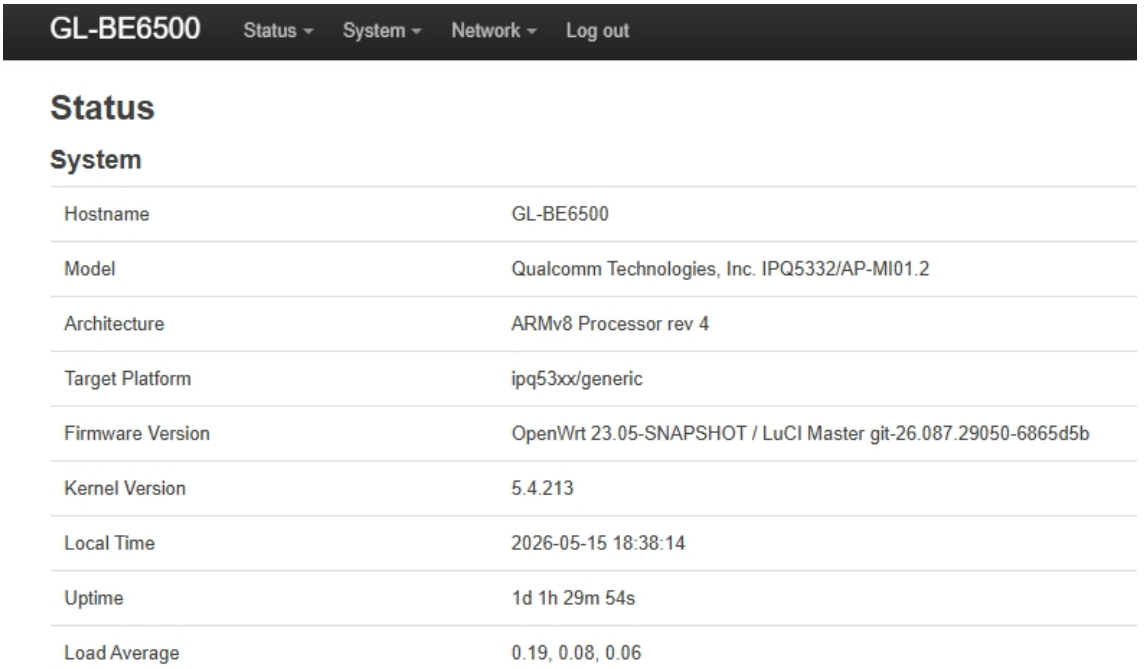
2. Kliknij **Go To LuCI**, aby przejść do strony logowania LuCI.



3. Wprowadź hasło logowania, takie samo jak do panelu administracyjnego.



Otworzy się interfejs LuCI.



Oświadczenia dotyczące zgodności z przepisami

FCC ID: 2AFIW-BE6500

To urządzenie jest zgodne z częścią 15 przepisów FCC. Jego działanie podlega następującym dwóm warunkom:

(1) Urządzenie nie może powodować szkodliwych zakłóceń oraz

(2) Urządzenie musi przyjmować wszelkie odbierane zakłócenia, w tym zakłócenia mogące powodować niepożądane działanie.

Zmiany lub modyfikacje, które nie zostały wyraźnie zatwierdzone przez stronę odpowiedzialną za zgodność, mogą spowodować utratę uprawnień użytkownika do obsługi urządzenia.

Uwaga: urządzenie zostało przetestowane i uznane za zgodne z limitami dla urządzeń cyfrowych klasy B zgodnie z częścią 15 przepisów FCC. Limity te mają zapewniać odpowiednią ochronę przed szkodliwymi zakłóceniami w instalacjach domowych. Urządzenie generuje, wykorzystuje i może emitować energię o częstotliwości radiowej, a jeśli nie zostanie zainstalowane i nie będzie używane zgodnie z instrukcjami, może powodować szkodliwe zakłócenia łączności radiowej. Nie ma jednak gwarancji, że zakłócenia nie wystąpią w konkretnej instalacji. Jeśli urządzenie powoduje szkodliwe zakłócenia odbioru radiowego lub telewizyjnego, co można sprawdzić przez jego wyłączenie i ponowne włączenie, zaleca się podjęcie jednej lub kilku z poniższych czynności w celu usunięcia zakłóceń:

- Zmień kierunek lub położenie anteny odbiorczej.
- Zwiększ odległość między urządzeniem a odbiornikiem.
- Podłącz urządzenie do gniazda w obwodzie innym niż ten, do którego podłączony jest odbiornik.
- Skontaktuj się ze sprzedawcą lub doświadczonym technikiem radiowo-telewizyjnym w celu uzyskania pomocy. Ważna informacja.

Oświadczenie FCC dotyczące narażenia na promieniowanie

Urządzenie spełnia limity narażenia na promieniowanie FCC określone dla środowiska niekontrolowanego. Należy je instalować i użytkować z zachowaniem minimalnej odległości 20 cm między elementem promieniującym a ciałem. Nadajnik nie może być umieszczany w tym samym miejscu ani działać razem z inną anteną lub nadajnikiem.

Oświadczenie o zgodności z przepisami kanadyjskimi

Urządzenie zawiera nadajniki lub odbiorniki niewymagające licencji, zgodne z normami RSS kanadyjskiego Ministerstwa Innowacji, Nauki i Rozwoju Gospodarczego dotyczącymi urządzeń niewymagających licencji.
Działanie podlega następującym dwóm warunkom:
(1) Urządzenie nie może powodować zakłóceń.
(2) Urządzenie musi przyjmować wszelkie zakłócenia, w tym zakłócenia mogące powodować jego niepożądane działanie.
Nadajnik lub odbiornik niewymagający licencji, zawarty w tym urządzeniu, jest zgodny z normami CNR kanadyjskiego Ministerstwa Innowacji, Nauki i Rozwoju Gospodarczego dotyczącymi urządzeń radiowych niewymagających licencji. Użytkowanie jest dozwolone pod następującymi dwoma warunkami:
(1) Urządzenie nie może powodować zakłóceń.
(2) Urządzenie musi przyjmować wszelkie zakłócenia radioelektryczne, nawet jeśli mogą one zakłócać jego działanie.

Urządzenie spełnia limity narażenia na promieniowanie IC RSS-102 określone dla środowiska niekontrolowanego. Należy je instalować i użytkować z zachowaniem minimalnej odległości 20 cm między elementem promieniującym a ciałem.
Urządzenie spełnia limity narażenia na promieniowanie IC CNR-102 określone dla środowiska niekontrolowanego. Należy je instalować i użytkować z zachowaniem minimalnej odległości 20 cm między elementem promieniującym a ciałem.

Instrukcja obsługi urządzeń LE-LAN powinna zawierać wskazówki dotyczące ograniczeń wymienionych w powyższych punktach, a mianowicie:
i. Urządzenie działające w paśmie 5150–5250 MHz jest przeznaczone wyłącznie do użytku w pomieszczeniach, aby ograniczyć ryzyko szkodliwych zakłóceń systemów mobilnej łączności satelitarnej korzystających z tego samego kanału.

i. Urządzenie używane w paśmie 5150–5250 MHz jest przeznaczone wyłącznie do użytku w pomieszczeniach, aby ograniczyć ryzyko szkodliwych zakłóceń systemów mobilnej łączności satelitarnej korzystających z tego samego kanału.

GL TECHNOLOGIES (HONG KONG) LIMITED niniejszym oświadcza, że urządzenie radiowe typu [router Wi-Fi 7 BE6500, GL-BE6500] jest zgodne z zasadniczymi wymaganiami i innymi stosownymi postanowieniami dyrektywy 2014/53/UE. Pełny tekst deklaracji zgodności UE jest dostępny na stronie https://www.gl-inet.com/products/certificate.
Maksymalna moc wyjściowa:
CE: ≤20 dBm EIRP (2,412 GHz~2,472 GHz); ≤23 dBm EIRP (5,15 GHz~5,35 GHz); ≤30 dBm EIRP (5,47 GHz~5,725 GHz); ≤13,98 dBm (5,725 GHz~5,85 GHz).