GL·iNet



Instrukcja obsługi

GL-MG1300 / Mango 2

Dwupasmowy miniaturowy router podróżny

Wersja oprogramowania sprzętowego 4.10.0

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 9

1.1 Opis produktu 10

1.1.1 Wygląd 10

1.1.2 Złącza i przyciski 11

1.1.3 Dioda LED 12

1.2 Dane techniczne 12

1.3 Zawartość opakowania 13

Rozdział 2 Podłączanie sprzętu 14

2.1 Wybór miejsca 15

2.2 Podłączanie routera 15

Rozdział 3 Logowanie do routera 16

Rozdział 4 Konfiguracja połączenia z Internetem 18

4.1 Kreator szybkiej konfiguracji 19

4.2 Ręczna konfiguracja połączenia z Internetem 20

4.2.1 Połączenie z Internetem przez kabel Ethernet 21

4.2.2 Połączenie z Internetem przez istniejącą sieć Wi-Fi 26

4.2.3 Połączenie z Internetem przez tethering USB 33

4.2.4 Połączenie z Internetem przez modem USB 38

Rozdział 5 Sieć bezprzewodowa 41

5.1 Wyświetlanie stanu Wi-Fi 42

WLAN5.2 Ustawienia sieci bezprzewodowej 43

5.2.1 Sieć główna 43

5.2.2 Sieć gościnna 44

5.2.3 Sieć IoT 46

Rozdział 6 Urządzenia klienckie 48

6.1 Szczegóły urządzenia 50

6.2 Działania 52

6.3 Usuwanie urządzeń klienckich 55

6.4 Sortowanie 56

Rozdział 7 Usługi w chmurze 57

7.1 Konto GL.iNet 58

7.1.1 Włączanie konta GL.iNet 58
7.1.2 Usuwanie powiązania z kontem GL.iNet 60
7.2 GoodCloud 61
7.2.1 Włączanie GoodCloud 61
7.2.2 Zarządzanie routerem 64
7.2.3 Usuwanie powiązania urządzenia 68
7.3 GoodPAS 69
7.3.1 Szybka konfiguracja 69
7.3.2 Testowanie łączności 73
7.3.3 Zmiana planu na wyższy 74
Rozdział 8 Poznaj VPN 75
8.1 Wprowadzenie 76
8.2 Przykłady zastosowań 77
Rozdział 9 Panel VPN 80
9.1 Przesyłanie profilu VPN 81
9.2 Dodawanie tunelu VPN 85
9.2.1 Czynności ogólne 85
9.2.2 Przykłady konfiguracji 87
9.3 Kill Switch 105
9.4 Cały pozostały ruch 106
9.5 Opcje tunelu 107
9.6 Priorytet tuneli 109
Rozdział 10 Konfiguracja serwera VPN 111
10.1 Konfiguracja serwera OpenVPN 112
10.1.1 Przygotowanie 112
10.1.2 Etapy konfiguracji 113
10.1.3 Rozwiązywanie problemów 115
10.2 Konfiguracja serwera WireGuard 116
10.2.1 Przygotowanie 116
10.2.2 Etapy konfiguracji 117
10.2.3 Rozwiązywanie problemów 120
Rozdział 11 Konfiguracja klienta VPN 121
11.1 Konfiguracja klienta OpenVPN 122
11.1.1 Przygotowanie 122

11.1.2 Konfiguracja NordVPN 122
11.1.3 Ręczna konfiguracja klienta OpenVPN (inni dostawcy) 128
11.2 Konfiguracja klienta WireGuard 131
11.2.1 Przygotowanie 131
11.2.2 Konfiguracja AzireVPN 132
11.2.3 Konfiguracja Hide.me 137
11.2.4 Konfiguracja IPVanish 140
11.2.5 Konfiguracja Mullvad 145
11.2.6 Konfiguracja NordVPN 150
11.2.7 Konfiguracja PIA (Private Internet Access) 155
11.2.8 Konfiguracja Surfshark 160
11.2.9 Ręczna konfiguracja klienta WireGuard (inni dostawcy) 165
Rozdział 12 Sieć 170
12.1 Multi-WAN 171
12.1.1 Monitorowanie stanu interfejsów 171
12.1.2 Tryb Multi-WAN 174
12.2 Podsieci 177
12.2.1 Sieć główna 177
12.2.2 Sieć gościnna 183
12.2.3 Sieć IoT 187
12.2.4 Sieci VLAN 191
12.3 Port Ethernet 194
12.3.1 WAN 195
12.3.2 LAN 196
12.3.3 Dwa łącza Ethernet WAN 198
12.4 DNS 200
12.4.1 Ustawienia serwera DNS 201
12.4.2 Edycja pliku hosts 205
12.5 IPv6 207
12.5.1 Tryb IPv6 208
12.5.2 Sposób uzyskiwania DNS 208
12.6 IGMP Snooping 209
12.7 Tryb sieciowy 210
12.8 Przyspieszanie sieci 212

Rozdział 13 Kontrola ruchu 213
13.1 Kontrola rodzicielska 214
Rozdział 14 Bezpieczeństwo 220
14.1 Przekierowanie portów 221
14.1.1 DMZ 221
14.1.2 Przekierowanie portów 222
14.2 Dostęp administratora 224
14.2.1 Kontrola dostępu 224
14.2.2 Kontrola dostępu zdalnego 227
14.2.3 Otwieranie portów routera 228
14.3 Tryb NAT 229
Rozdział 15 Aplikacje 230
15.1 Wtyczki 231
15.2 Dynamiczny DNS 232
15.2.1 Włączanie DDNS 232
15.2.2 Sprawdzanie działania DDNS 235
15.2.3 Zdalny dostęp przez HTTPS 237
15.2.4 Zdalny dostęp przez SSH 239
15.3 Pamięć sieciowa 241
15.3.1 Podłączanie pamięci 241
15.3.2 Konfiguracja usługi Samba 242
15.4 Tailscale 245
15.4.1 Konfiguracja Tailscale 246
15.4.2 Rozgłaszanie podsieci WAN 249
15.4.3 Rozgłaszanie podsieci LAN 250
15.4.4 Niestandardowe węzły wyjściowe 251
15.4.5 Uruchamianie węzła wyjściowego 252
Rozdział 16 System 259
16.1 Przegląd 260
16.2 Hasło administratora 261
16.3 Aktualizacja 262
16.3.1 Aktualizacja online 262
16.3.2 Aktualizacja lokalna 263
16.4 Zadania zaplanowane 264

16.4.1 Harmonogram diody LED 264
16.4.2 Harmonogram ponownego uruchamiania 265
16.4.3 Harmonogram Wi-Fi 5 GHz 265
16.4.4 Harmonogram Wi-Fi 2,4 GHz 267
16.5 Strefa czasowa 270
16.6 Ustawienia przełącznika 271
16.7 Resetowanie oprogramowania 273
16.8 Dziennik 274
16.9 Ustawienia zaawansowane 276
Oświadczenia dotyczące zgodności z przepisami 278

Rozdział 1

Poznaj swój router

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

1.1 Opis produktu

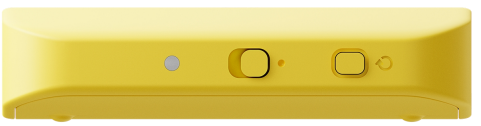
Mango 2 to pierwszy dwupasmowy miniaturowy router podróżny Wi-Fi 5 firmy GL.iNet, wyróżniający się wyjątkowo smukłą, przenośną konstrukcją. Zapewnia teoretyczne prędkości 400 Mb/s (2,4 GHz) i 866 Mb/s (5 GHz) w konfiguracji 2×2 MIMO. Ma fabrycznie zainstalowane OpenVPN i WireGuard, obsługuje ponad 30 usług VPN i automatycznie szyfruje cały ruch sieciowy. Umożliwia też zdalne zarządzanie przez GoodCloud, łącząc wydajność, praktyczność i bezpieczeństwo.

1.1.1 Wygląd

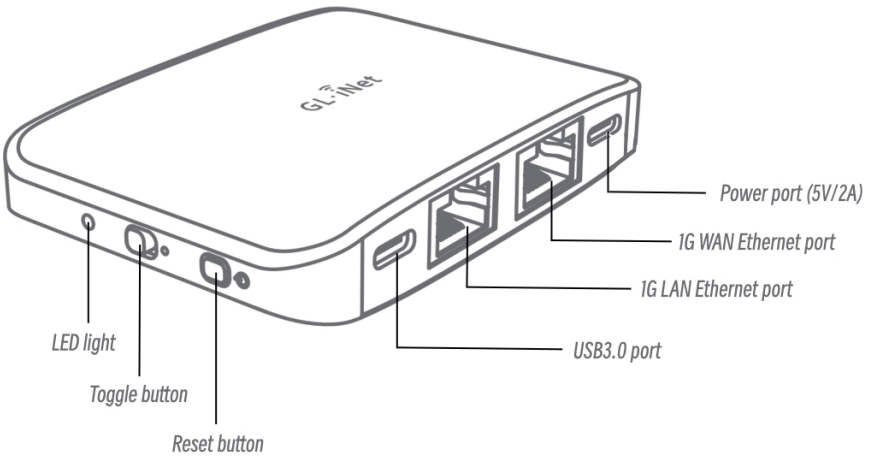








1.1.2 Złącza i przyciski



Element	Opis
Złącze zasilania	Służy do podłączenia zasilacza.
Port WAN 1G	Służy do połączenia z modemem lub gniazdem Ethernet zapewniającym dostęp do Internetu.
Port LAN 1G	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 **3 sekundy**, a następnie zwolnij, aby naprawić połączenie sieciowe.
	Naciśnij i przytrzymaj przez **8 sekund**, a następnie zwolnij, aby przywrócić ustawienia fabryczne routera.
Przełącznik	Fizyczny przełącznik umożliwiający zmianę wybranych ustawień routera jednym ruchem. W panelu administracyjnym można go skonfigurować, aby jednym ruchem włączać lub wyłączać określone funkcje.

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 1G 1 port Ethernet LAN 1G 1 × port USB 3.0 1 × złącze zasilania USB-C 1 × przycisk resetowania 1 × przełącznik
Procesor	MediaTek, dwurdzeniowy, 880 MHz
Pamięć RAM / pamięć masowa	DDR3 128 MB / NOR 2 MB + NAND 128 MB
Protokół	IEEE 802.11a/b/g/n/ac
Prędkość Wi-Fi	400 Mb/s (2,4 GHz), 866 Mb/s (5 GHz)
Anteny	2 wewnętrzne anteny Wi-Fi
Prędkość Ethernet	10/100/1000 Mb/s
Zasilanie	USB-C, 5 V / 2 A
Pobór mocy	<5 W (bez obciążenia USB)
Temperatura pracy	0 ~ 40°C (32 ~ 104°F)
Temperatura przechowywania	-20 ~ 70°C (-4 ~ 158°F)

Wymiary / masa	89 × 63 × 15 mm / 100 g
Inne materiały i narzędzia	Karta katalogowa / Oprogramowanie sprzętowe / Aplikacja / Poradniki / Rozpakowanie

*Prędkości transmisji bezprzewodowej opierają się na standardach IEEE 802.11 (np. 802.11ac dla Wi-Fi 5). Rzeczywista przepustowość i zasięg mogą być niższe ze względu na przeszkody w otoczeniu (ściany, metal), obciążenie sieci lub możliwości urządzeń klienckich. *Korzystanie z Wi-Fi 5 (802.11ac) i jego funkcji (DL MU-MIMO, 256-QAM) wymaga urządzeń klienckich obsługujących odpowiednie technologie.

1.3 Zawartość opakowania

Opakowanie zawiera:

- 1 × Mango 2 (GL-MG1300)
- 1 × kabel zasilający USB-C–USB-C
- 1 × instrukcja obsługi
- 1 × karta z podziękowaniem



1 x User manual



1 x Mango 2 (GL-MG1300)



1 x Thank You Card



1 x Power cable

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

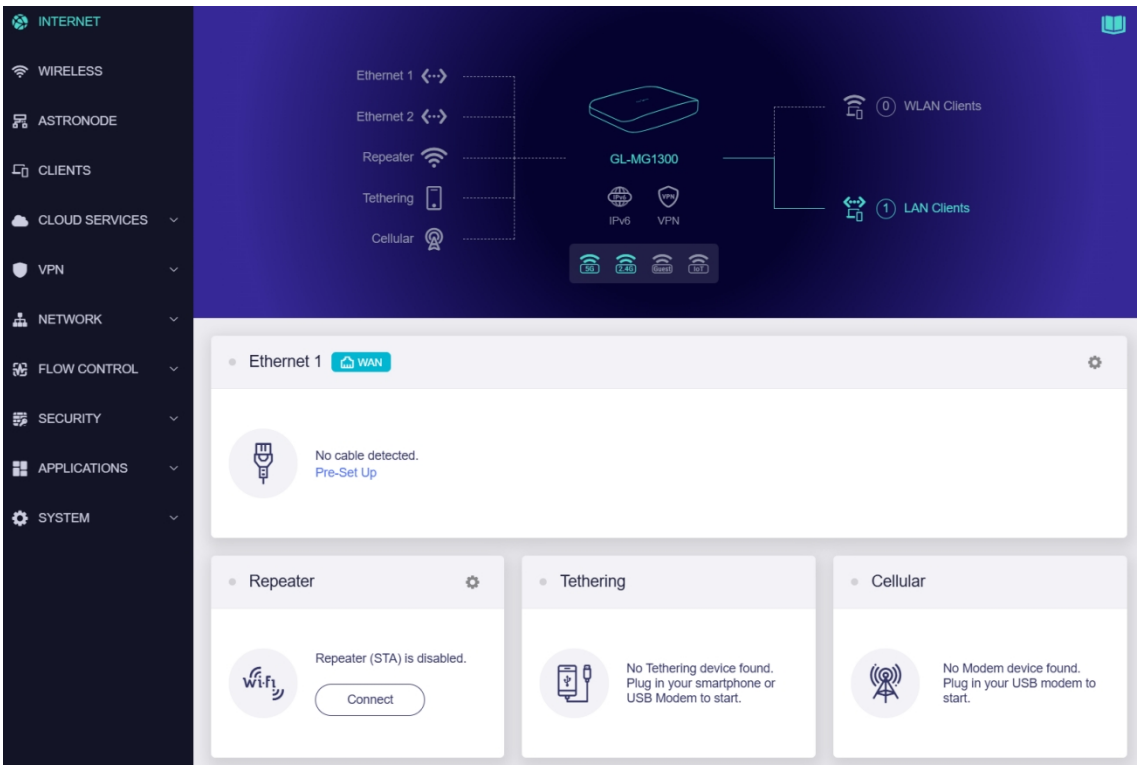
W tym rozdziale opisano logowanie do routera przez panel administracyjny w przeglądarce.

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.

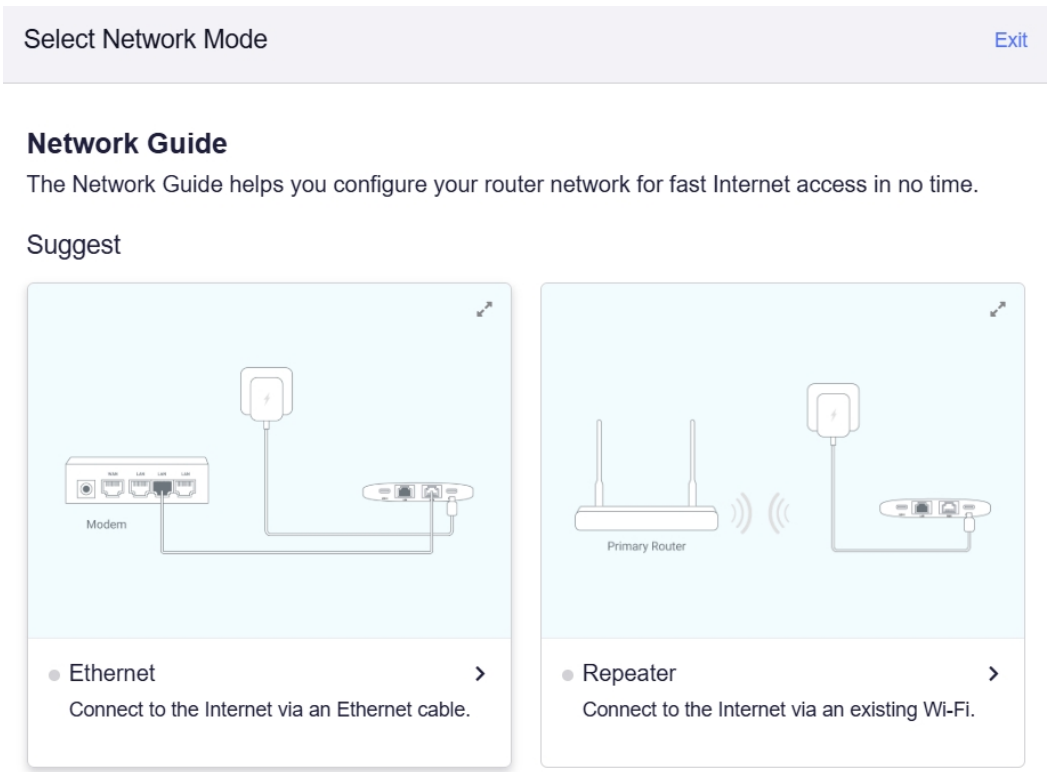
4.1 Kreator szybkiej konfiguracji

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.

Mango 2 obsługuje cztery sposoby łączenia z Internetem: Ethernet, Repeater, udostępnianie połączenia przez USB i modem USB. Wybierz sposób odpowiedni 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.

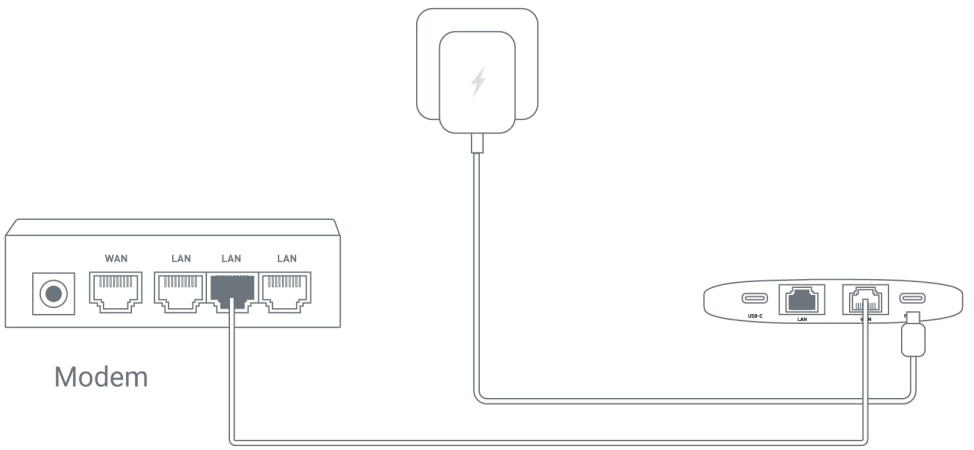
4.2.1 Połączenie z Internetem przez kabel Ethernet

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.

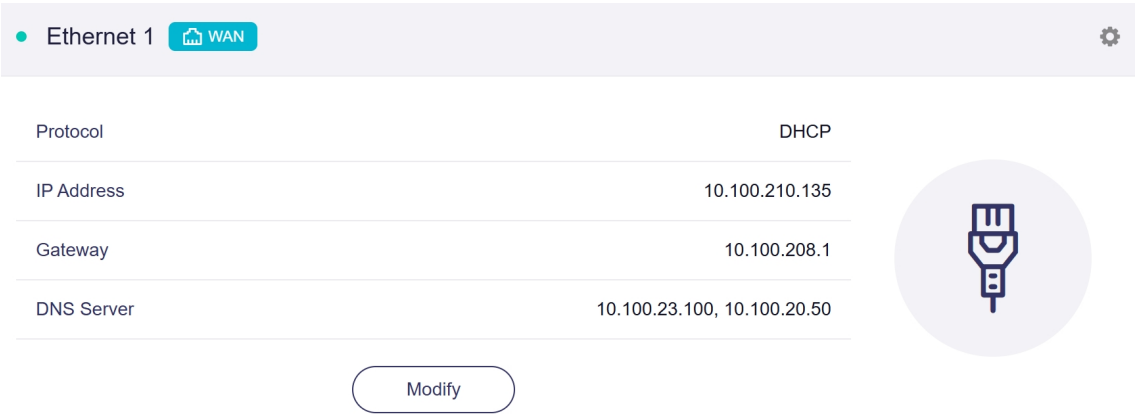
Podstawowa konfiguracja

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.

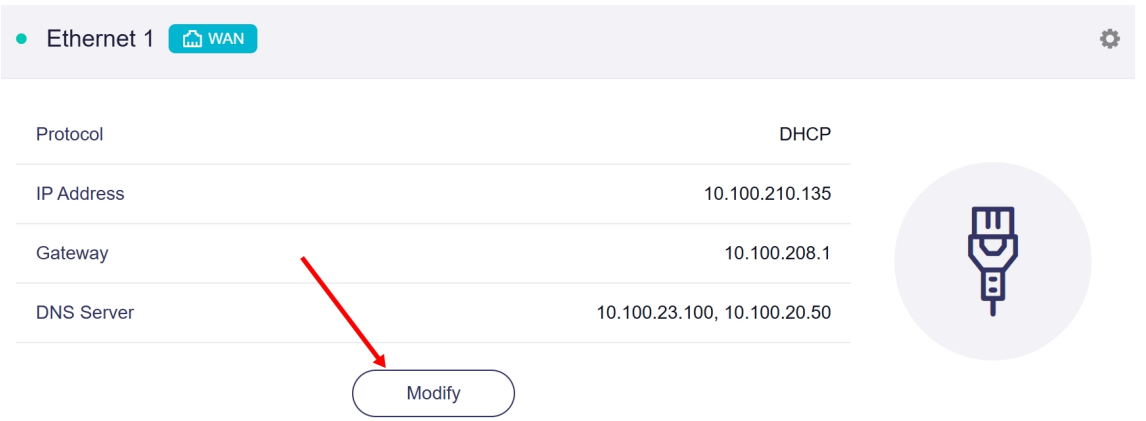


2. Zaloguj się do panelu administracyjnego routera i przejdź do **INTERNET** > **Ethernet**. Po pomyślnym nawiązaniu połączenia w sekcji Ethernet pojawią się szczegóły sieci, w tym protokół, adres IP, brama i serwer DNS.



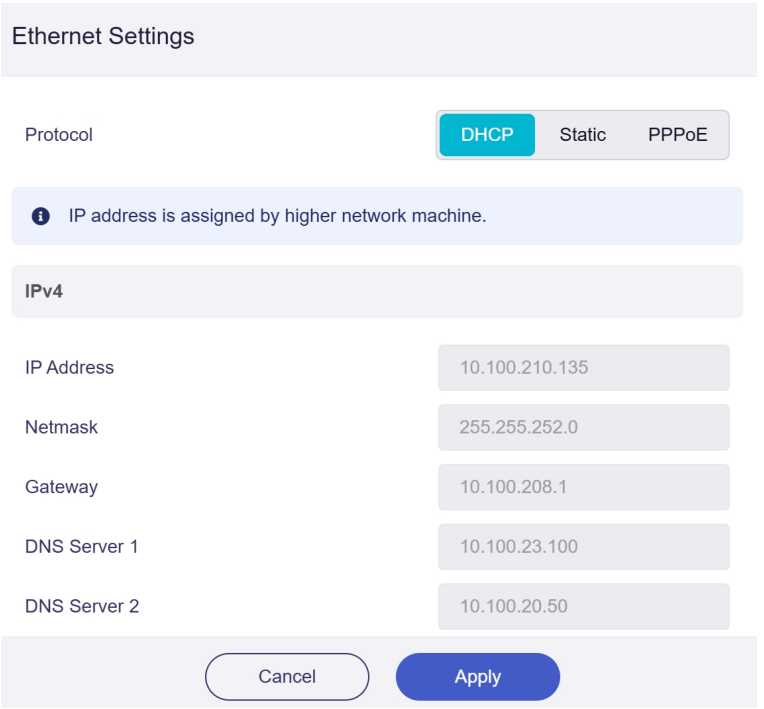
Protokół

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



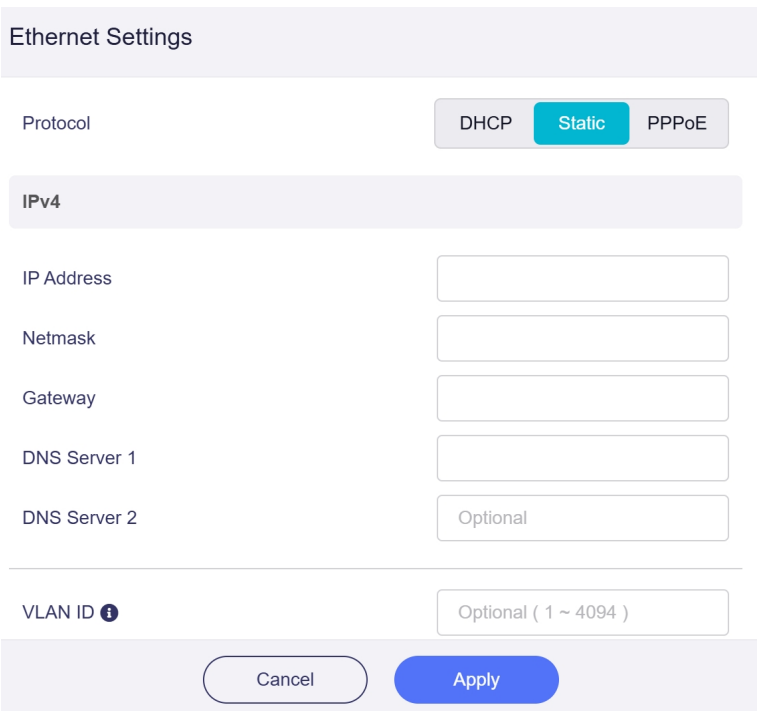
- **DHCP**

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



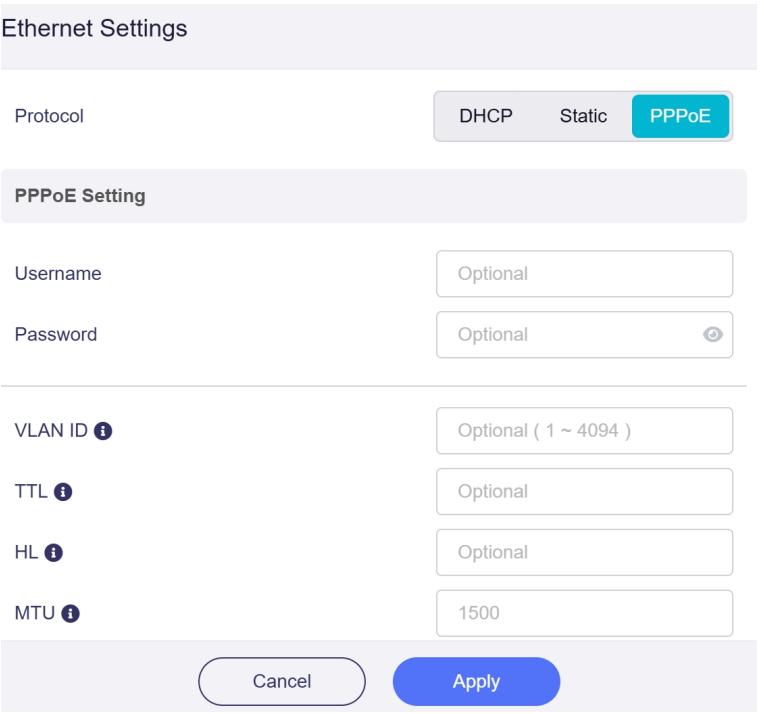
- **Statyczny adres IP**

  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.



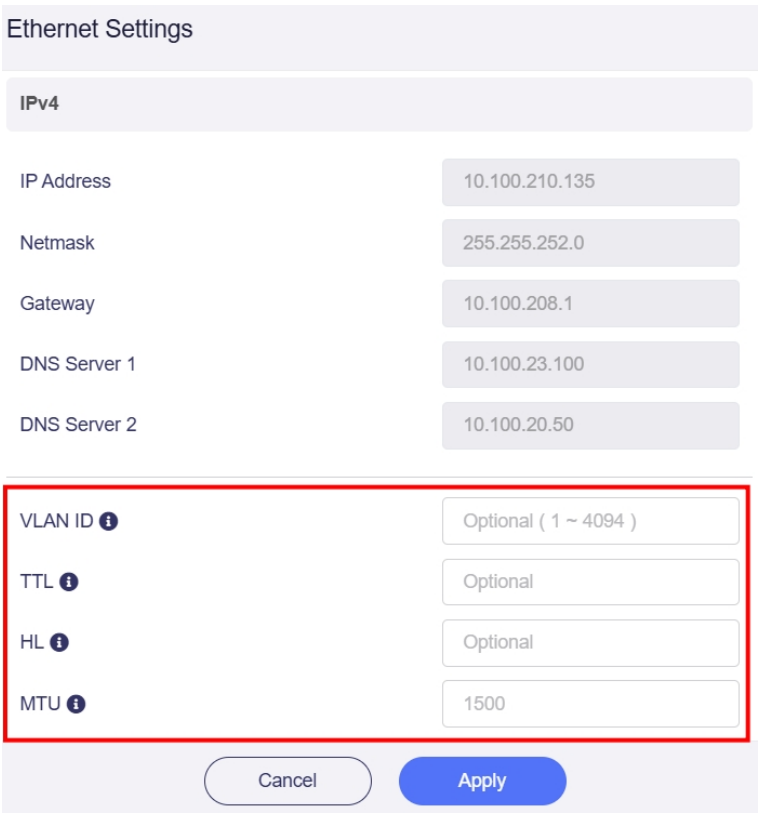
- **PPPoE**

  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**

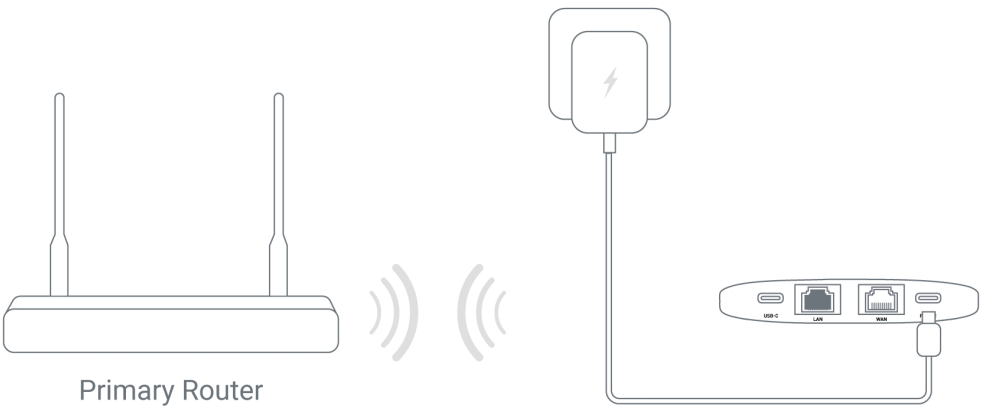
  W IPv6 pole HL (Hop Limit) ogranicza liczbę przeskoków pakietów danych w sieci i jest odpowiednikiem TTL w IPv4.

- **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.

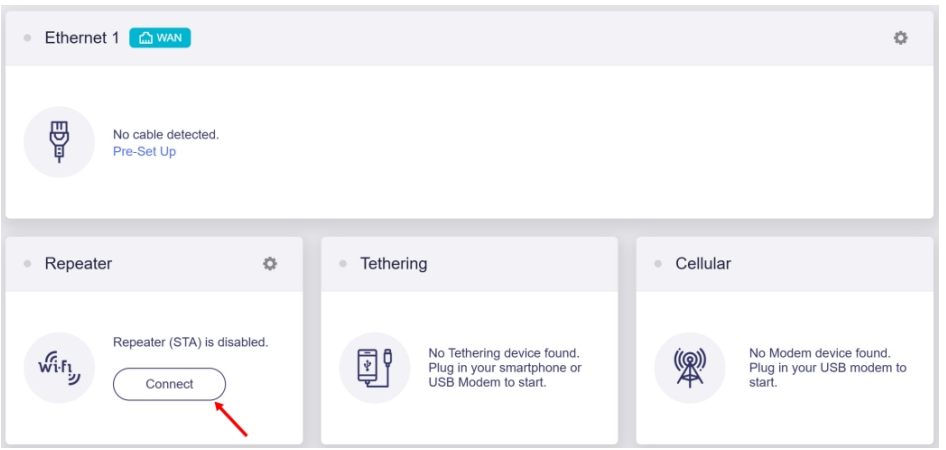


Funkcja wzmacniacza GL.iNet domyślnie działa w trybie WISP (Wireless Internet Service Provider). Oznacza to, że router tworzy własną podsieć i działa jako zapora, chroniąc przed zagrożeniami z sieci publicznej.

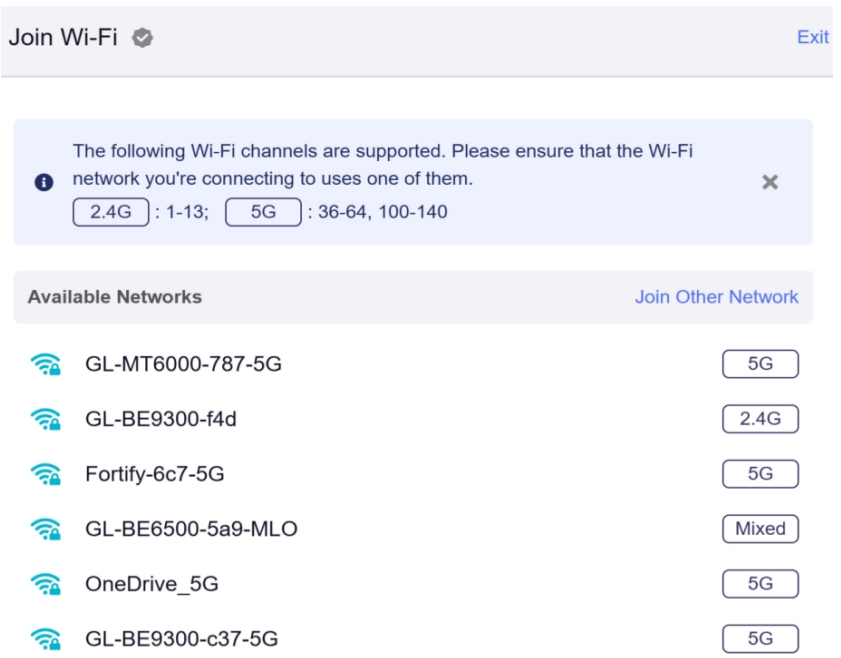
Podstawowa konfiguracja

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

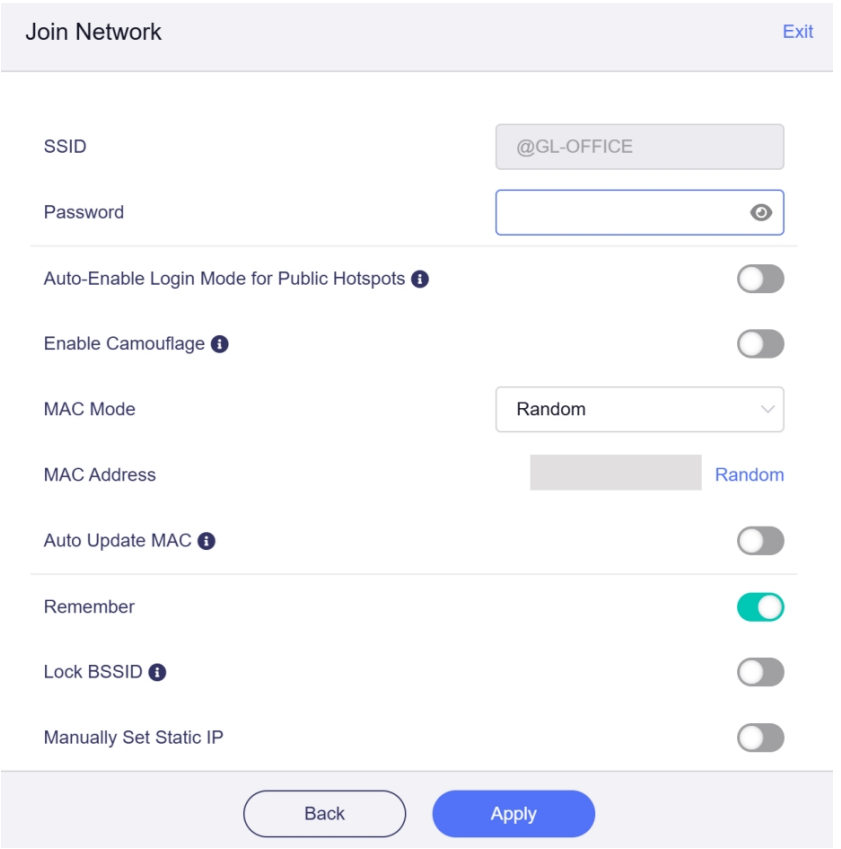
1. Zaloguj się do panelu administracyjnego routera i przejdź do **INTERNET** > **Repeater**. Kliknij **Connect**.



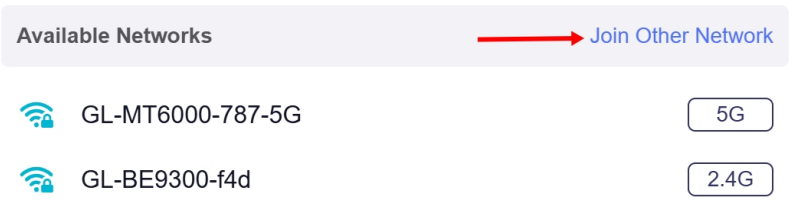
2. W wyświetlonym oknie wybierz z listy dostępnych sieci sieć Wi-Fi, z którą chcesz się połączyć.



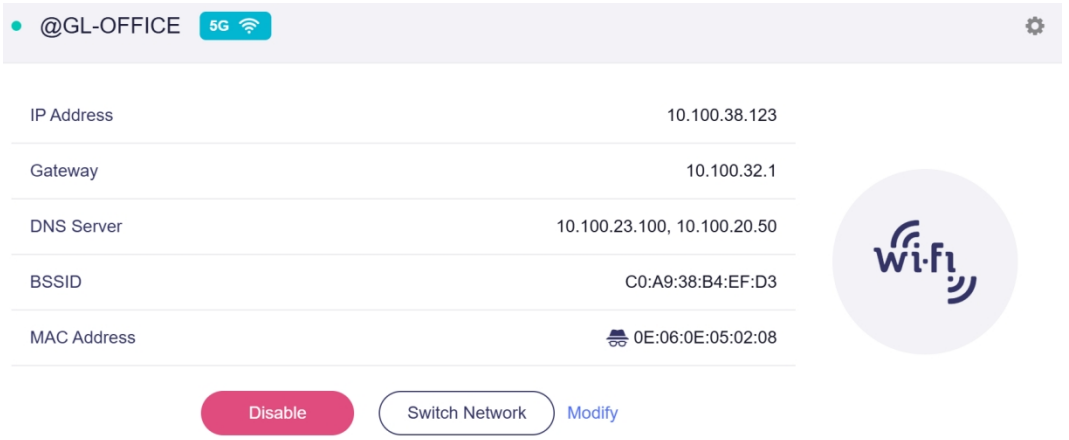
3. Wprowadź prawidłowe hasło Wi-Fi i kliknij **Apply**.



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**.

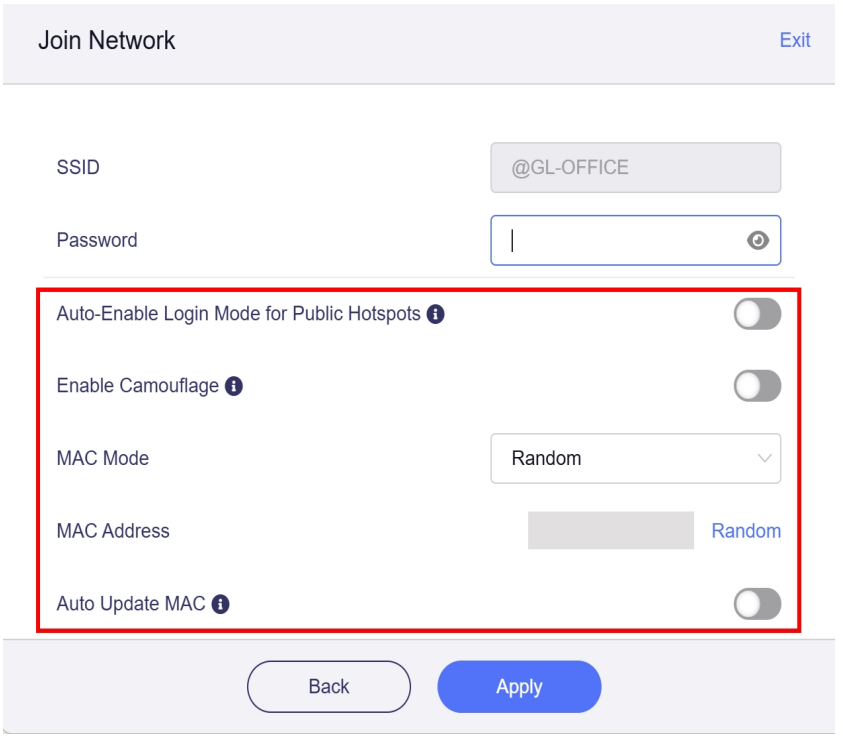


4. Poczekaj chwilę na połączenie routera. Po połączeniu strona będzie wyglądać jak poniżej.

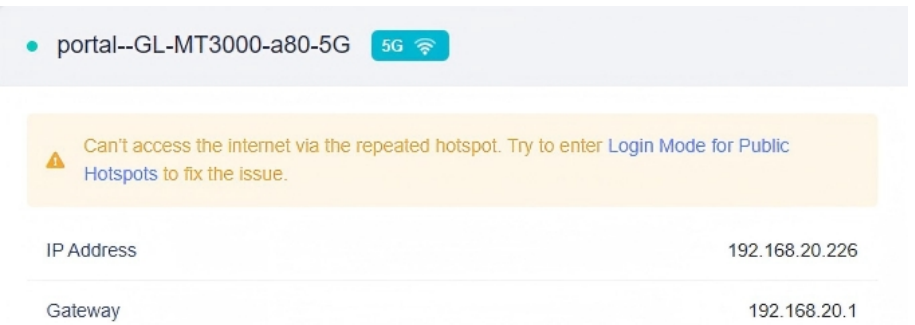

@GL-OFFICE
5G
IP Address
10.100.38.123
Gateway
10.100.32.1
DNS Server
10.100.23.100, 10.100.20.50
BSSID
C0:A9:38:B4:EF:D3
MAC Address
0E:06:0E:05:02:08
Disable
Switch Network
Modify

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.

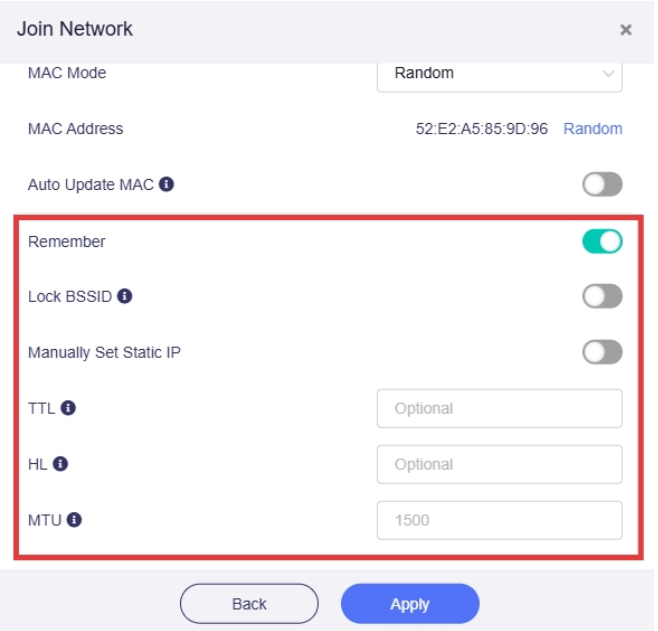


- **Włączanie kamuflażu**
  Po włączeniu tej opcji router podszywa się pod urządzenie klienckie używane do otwierania panelu administracyjnego, naśladując jego adres MAC.
- **Tryb MAC**
  Wybierz adres MAC, którego router ma używać do łączenia się z publicznym hotspotem.
  Factory: używa oryginalnego 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

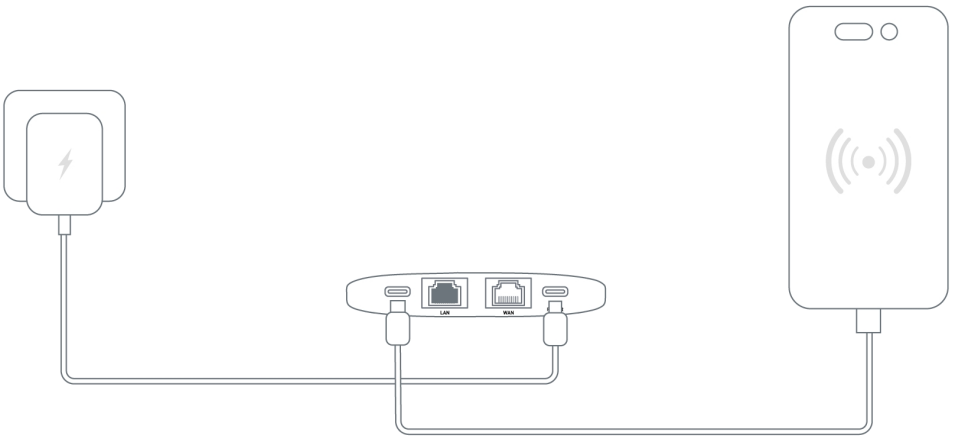
Podczas dołączania do sieci dostępne są opcjonalne ustawienia zaawansowane.



- **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

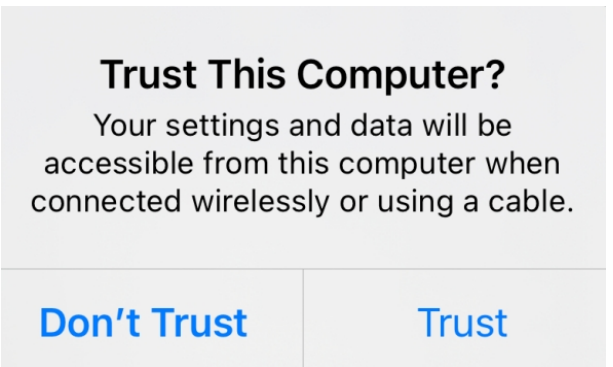
Podłączenie smartfona do routera kablem USB w celu udostępnienia routerowi komórkowej transmisji danych (np. 4G/5G) nazywa się tetheringiem. To wygodny sposób uzyskania tymczasowego dostępu do Internetu, szczególnie w terenie lub w miejscach bez stałego łącza szerokopasmowego.



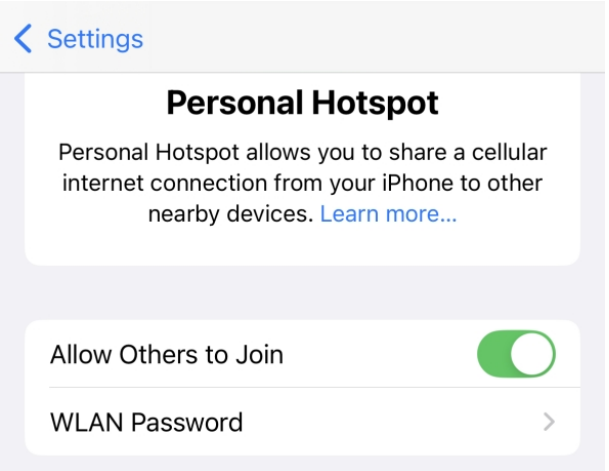
Modem typu hostless również korzysta z interfejsu Tethering podczas konfiguracji modemu.
Uwaga: niektórzy operatorzy komórkowi ograniczają tethering lub pobierają za niego dodatkowe opłaty. Zalecamy sprawdzenie warunków u operatora.

Tethering z iPhone’a

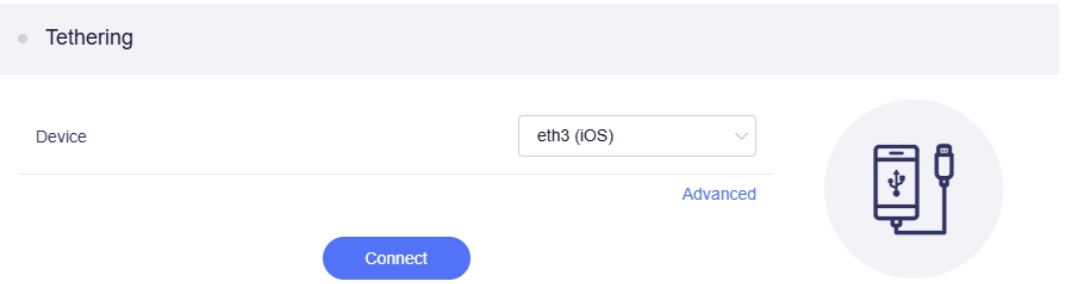
1. Podłącz iPhone'a do portu USB routera za pomocą kabla USB. Pojawi się komunikat systemowy z pytaniem, czy zaufać urządzeniu. Stuknij **Trust**, aby kontynuować.



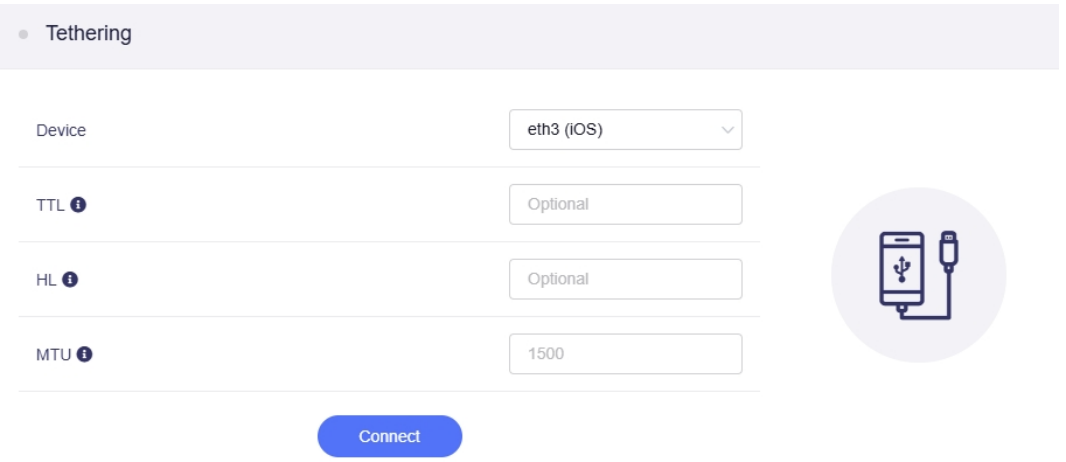
2. Na iPhonie przejdź do **Settings** > **Personal Hotspot**. Włącz **Allow Others to Join**.



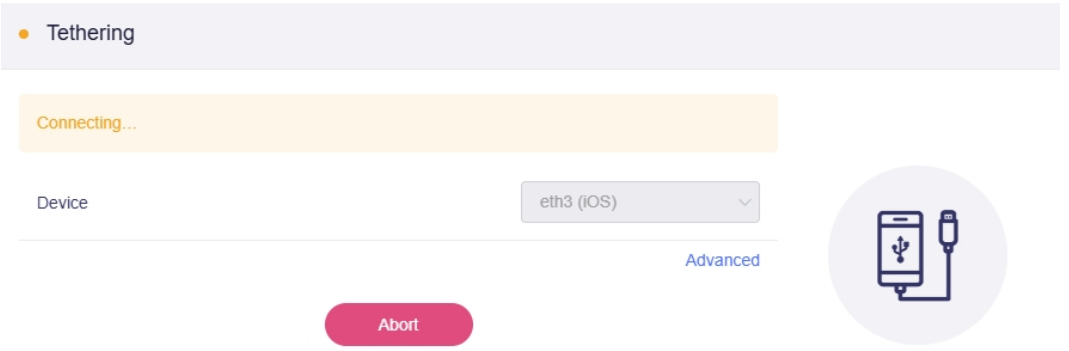
3. Podłącz komputer lub inny telefon do routera. Zaloguj się do panelu administracyjnego routera i przejdź do **INTERNET** > **Tethering**, a następnie kliknij **Connect**.



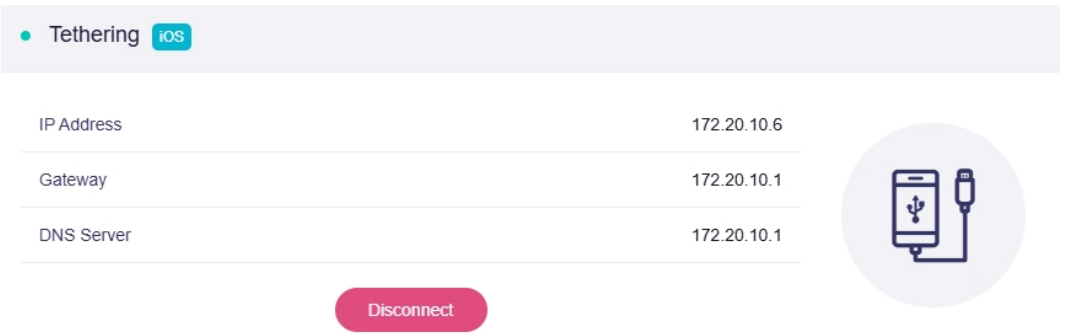
Aby dostosować ustawienia zaawansowane, takie jak TTL, HL i MTU, kliknij **Advanced** i zmień te ustawienia przed kliknięciem **Connect**.



4. Rozpocznie się nawiązywanie połączenia.

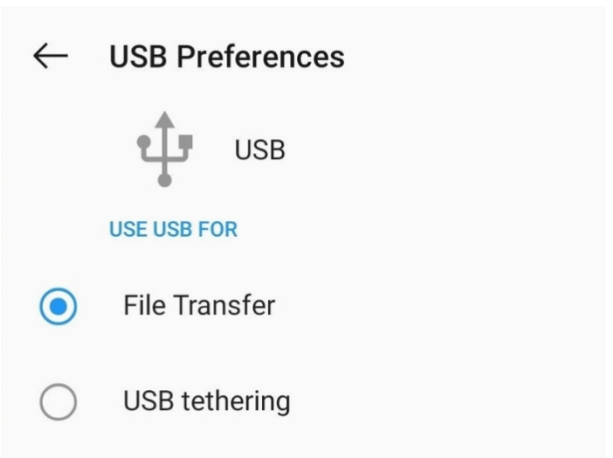


Po połączeniu na tej stronie pojawią się szczegóły połączenia tethering.

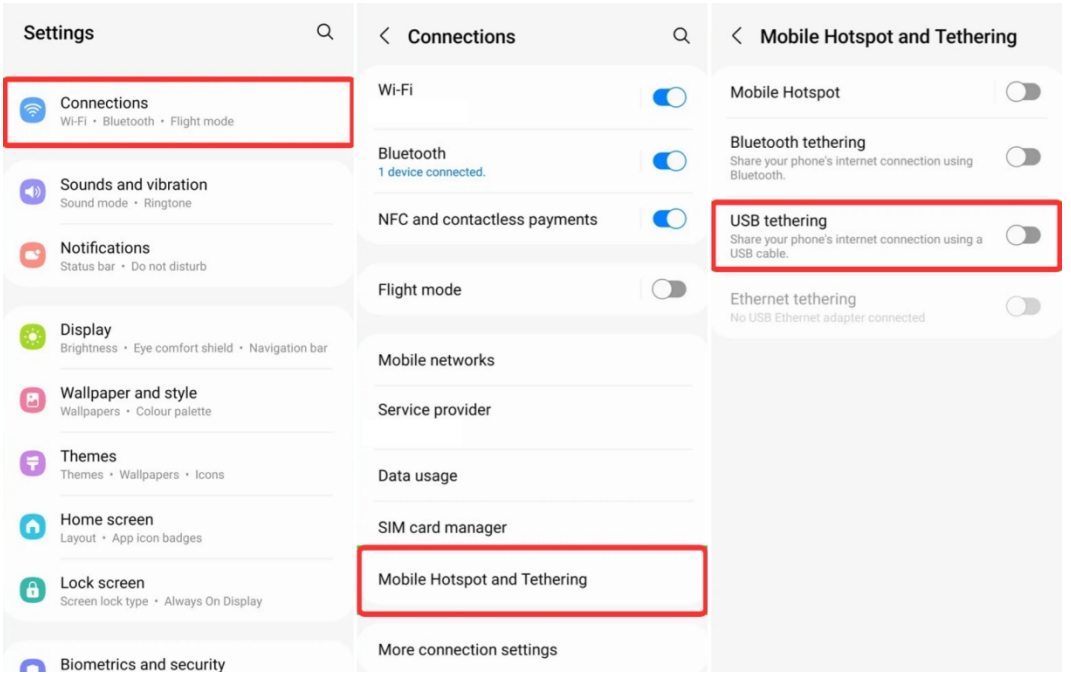


Tethering z telefonem z systemem Android

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**.

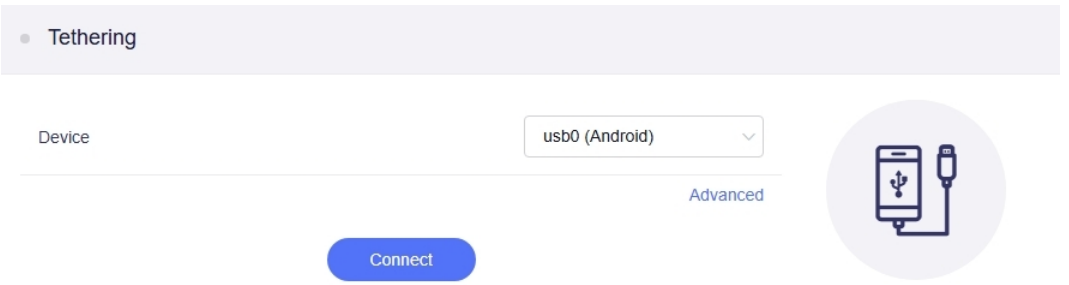


2. W telefonie przejdź do **Settings** > **Network & Internet** > **Personal Hotspot**. Włącz **Personal Hotspot** lub **USB Tethering**.

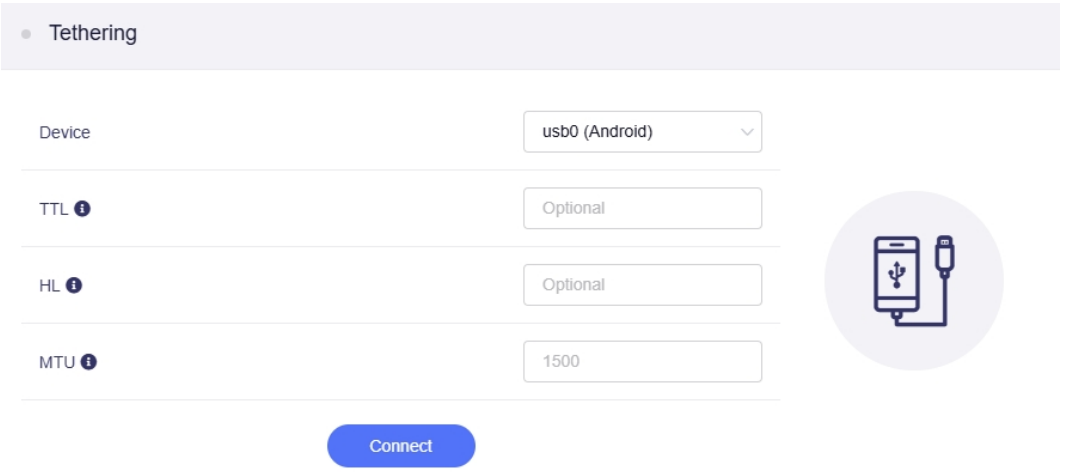


(Sposób włączania tetheringu USB zależy od producenta. Dokładną lokalizację opcji sprawdź w ustawieniach urządzenia, a w razie potrzeby skontaktuj się z pomocą techniczną producenta.)

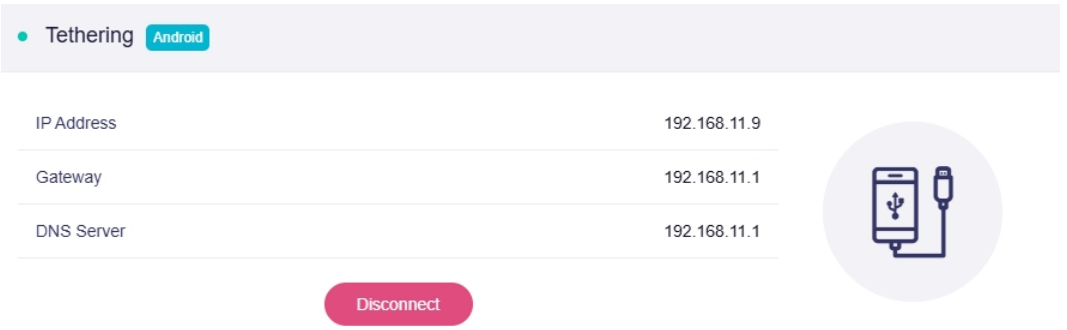
3. Podłącz komputer lub inny telefon do routera, a następnie zaloguj się do panelu administracyjnego routera i przejdź do **INTERNET** > **Tethering**. Kliknij **Connect**.



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:

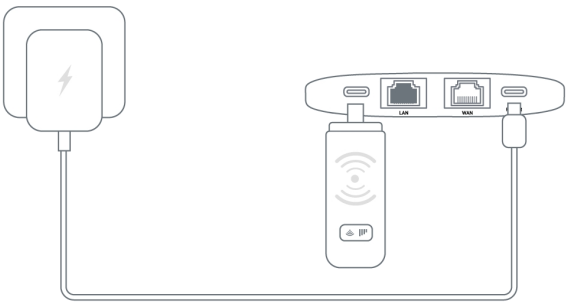
- Użyj oryginalnego zasilacza routera.
- Odłącz i ponownie podłącz kabel USB.
- Użyj innego kabla USB. Upewnij się, że obsługuje transmisję danych, a nie tylko ładowanie.
- Kilkakrotnie wyłącz i włącz opcję „USB Tethering” (na telefonie z systemem Android).
- Kilkakrotnie wyłącz i włącz opcję „Allow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

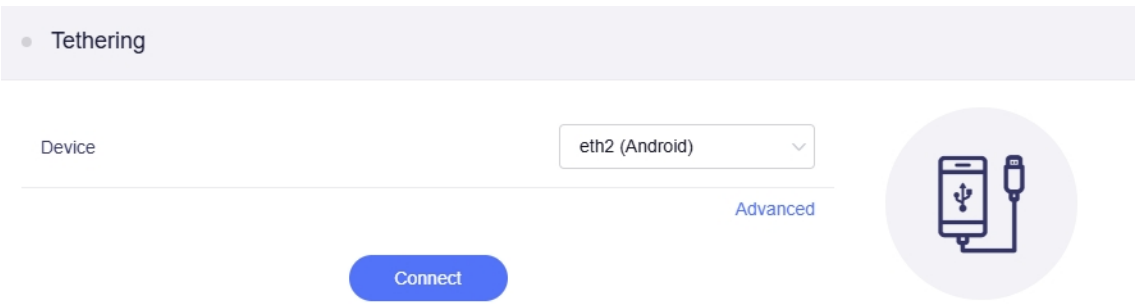
Aby połączyć router z Internetem, podłącz komórkowy modem USB do jego portu USB. Umożliwia to korzystanie z Internetu przez sieci 4G/5G bez stałego łącza szerokopasmowego. Rozwiązanie sprawdza się w pojazdach lub podczas aktywności w terenie. Połączenie jest realizowane za pośrednictwem interfejsu Tethering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

Do Mango 2 możesz podłączyć modem USB-C bezpośrednio lub użyć przejściówki USB-C–USB-A, aby podłączyć modem USB-A.

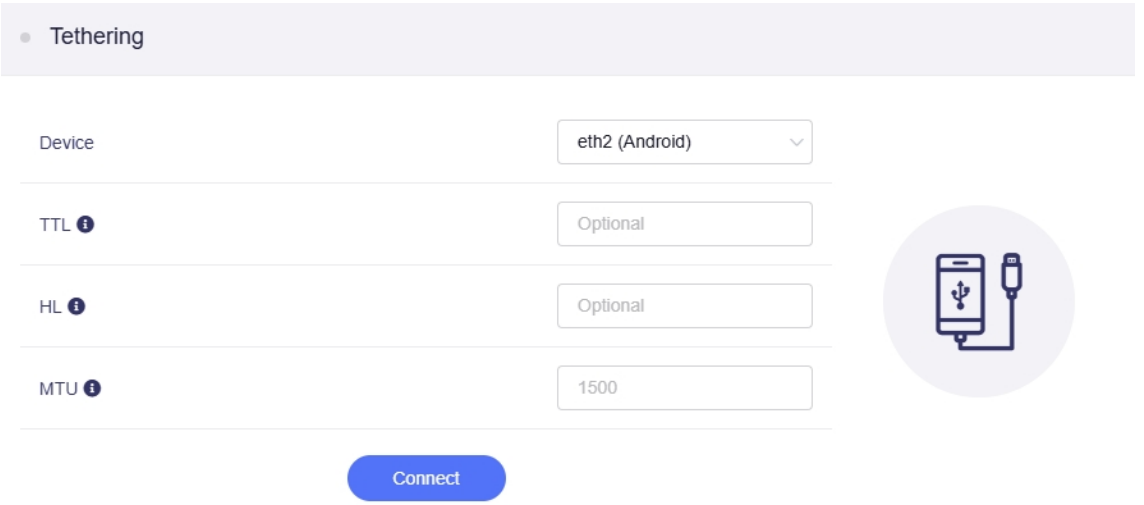


Aby połączyć router z Internetem przez modem USB, wykonaj poniższe czynności.

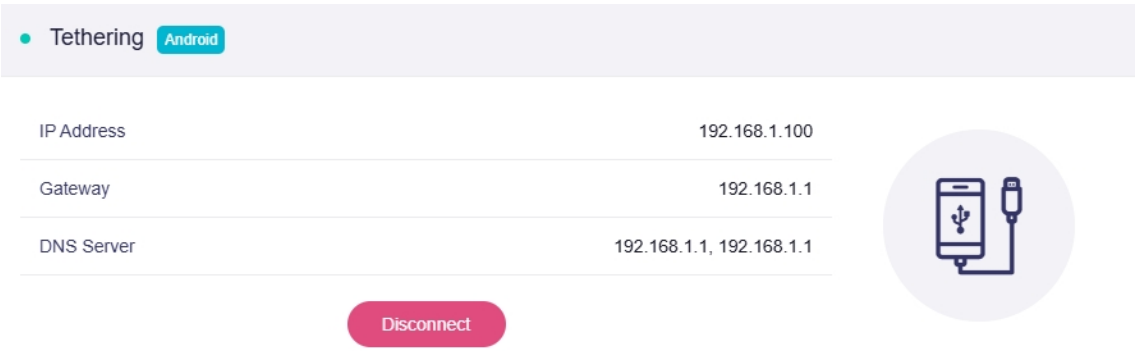
1. Przed włączeniem routera podłącz do jego portu USB modem USB z wcześniej włożoną kartą SIM.
2. Zaloguj się do panelu administracyjnego routera, przejdź do **INTERNET** > **Tethering**, a następnie kliknij **Connect**.



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

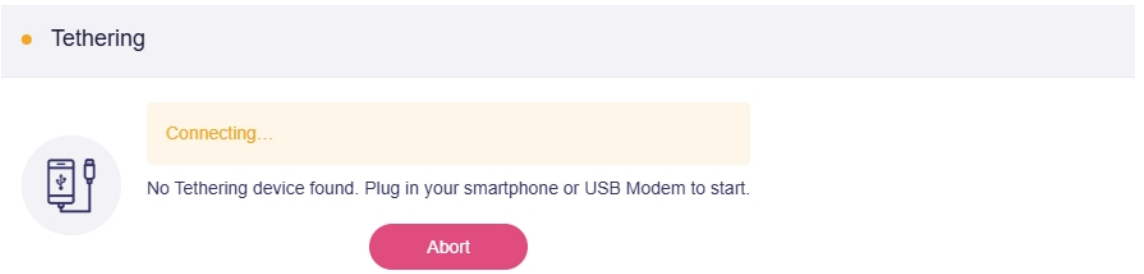


3. Rozpocznie się nawiązywanie połączenia. Po połączeniu na tej stronie pojawią się szczegóły sieci.



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

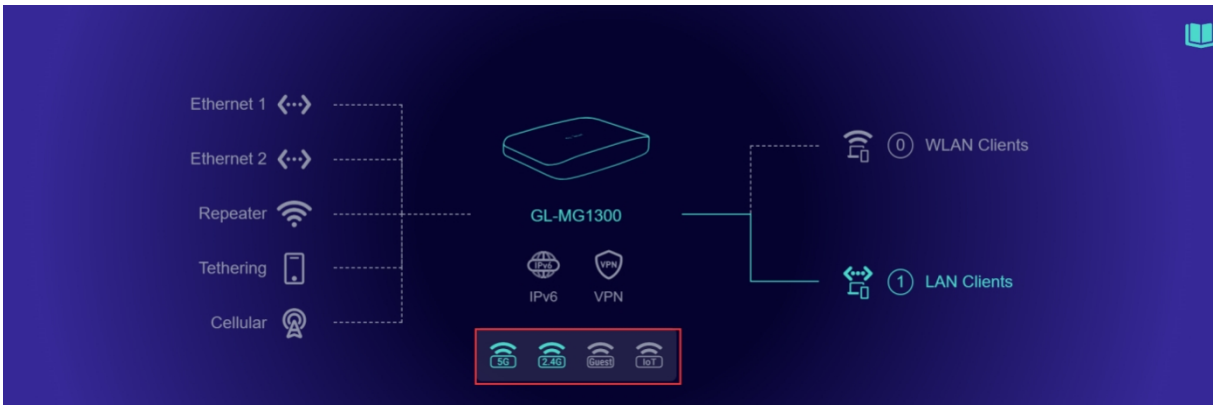
Rozdział 5

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.



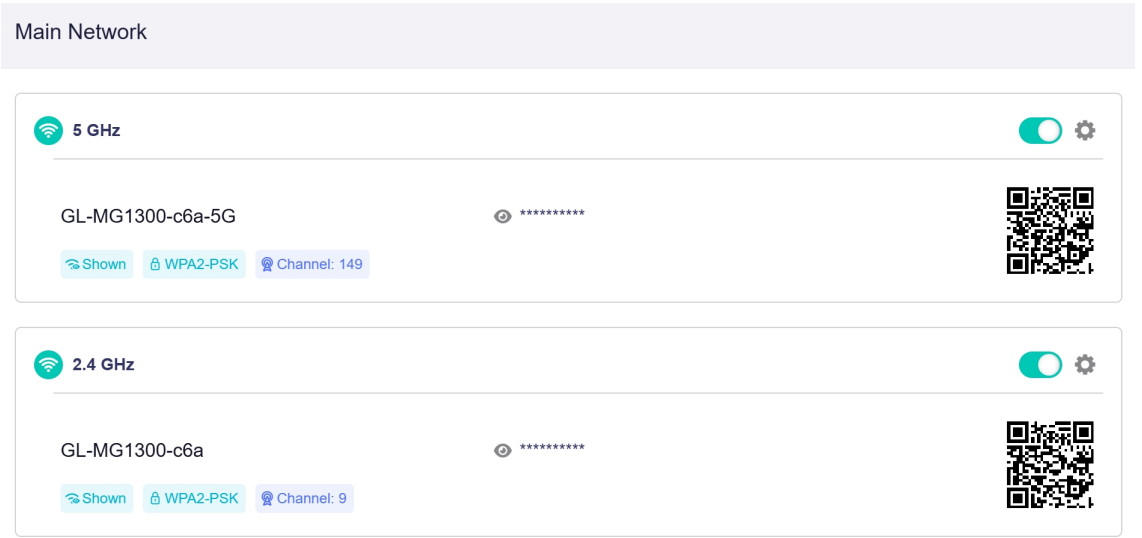
WLAN5.2 Ustawienia sieci bezprzewodowej

Zaloguj się do panelu administracyjnego routera i przejdź do **WIRELESS**.
Strona Wireless umożliwia konfigurację różnych sieci Wi-Fi, w tym sieci głównej, gościnnej i IoT. Obsługiwane pasma Wi-Fi zależą od modelu.

5.2.1 Sieć główna

Main Network to podstawowa sieć Wi-Fi, która obsługuje jednoczesne nadawanie w różnych pasmach radiowych. Wszystkie pasma są domyślnie włączone.

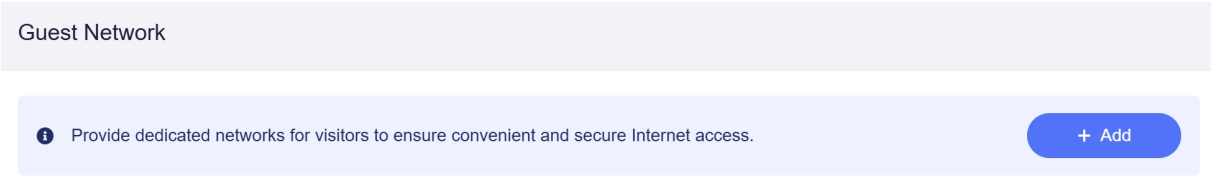
Kliknij ikonę koła zębatego po prawej stronie, aby wyświetlić lub zmienić ustawienia Wi-Fi dla każdego pasma, takie jak SSID, zabezpieczenia, hasło, losowy BSSID, moc nadawania, szerokość pasma i kanał Wi-Fi.
Uwaga: dostępne pasma Wi-Fi zależą od modelu.



5.2.2 Sieć gościnna

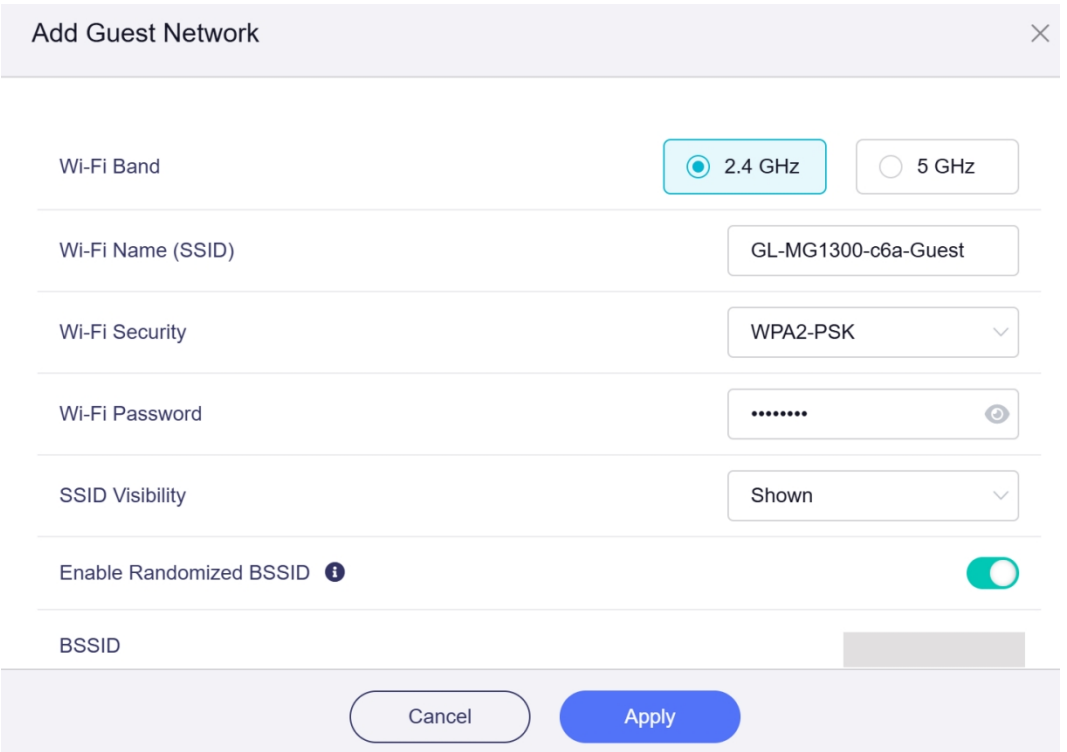
Guest Network to oddzielna sieć Wi-Fi dla gości. Wszystkie pasma są domyślnie wyłączone. Możesz włączyć poszczególne pasma i skonfigurować ich podstawowe ustawienia, takie jak SSID, tryb zabezpieczeń, hasło i losowy BSSID.

Aby utworzyć sieć Wi-Fi dla gości, kliknij przycisk **Add** po prawej stronie.

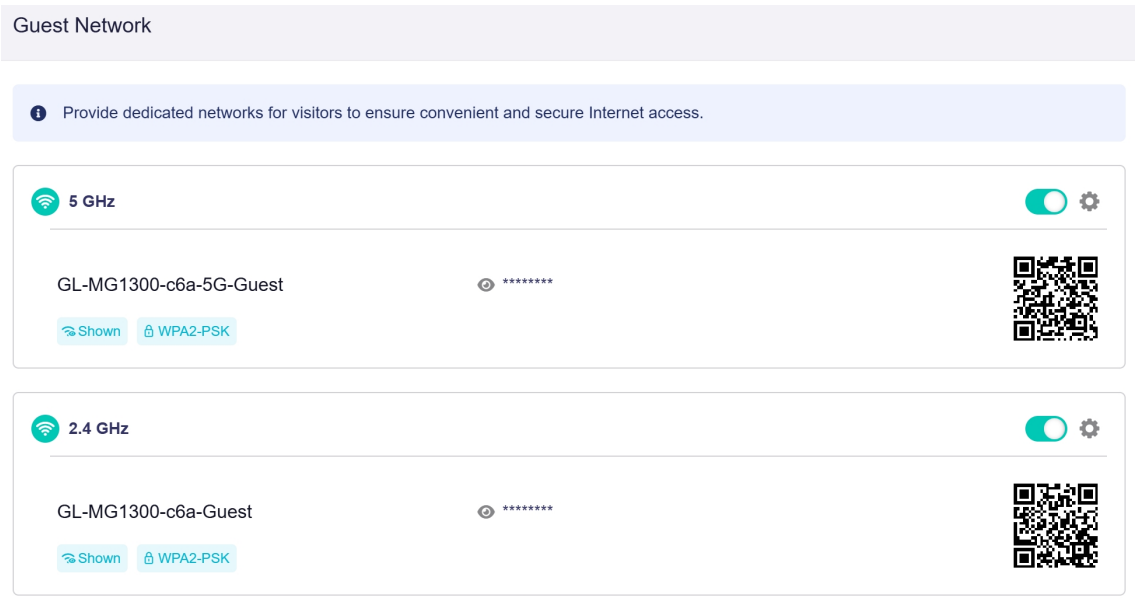


Wybierz pasmo Wi-Fi, skonfiguruj szczegóły sieci, a następnie kliknij **Apply**.

Uwaga: dostępne pasma Wi-Fi zależą od modelu.



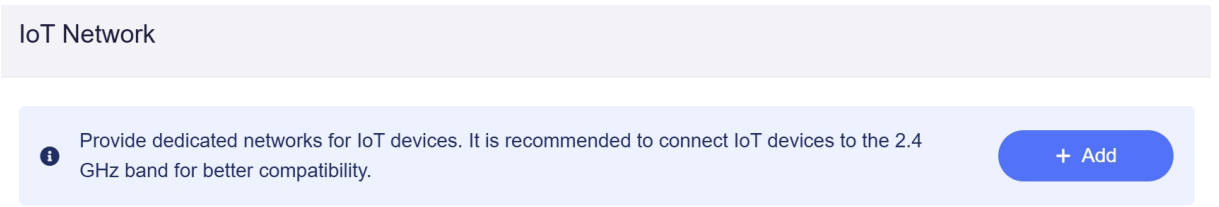
Po włączeniu strona wygląda jak na poniższej ilustracji.


Guest Network
Provide dedicated networks for visitors to ensure convenient and secure Internet access.
5 GHz
GL-MG1300-c6a-5G-Guest
****
Shown
WPA2-PSK
2.4 GHz
GL-MG1300-c6a-Guest
****
Shown
WPA2-PSK

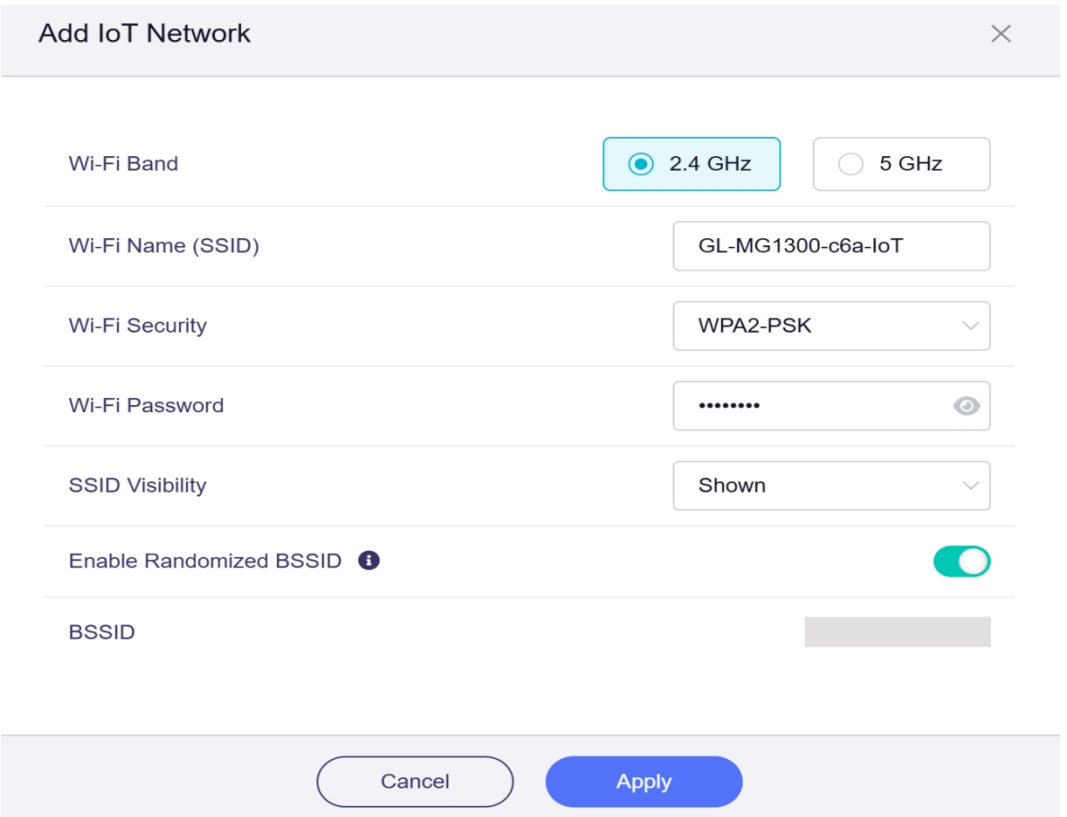
5.2.3 Sieć IoT

IoT Network to oddzielna sieć Wi-Fi dla urządzeń inteligentnych. Wszystkie pasma są domyślnie wyłączone. Możesz włączyć poszczególne pasma i skonfigurować ich podstawowe ustawienia, takie jak SSID, tryb zabezpieczeń, hasło i losowy BSSID.

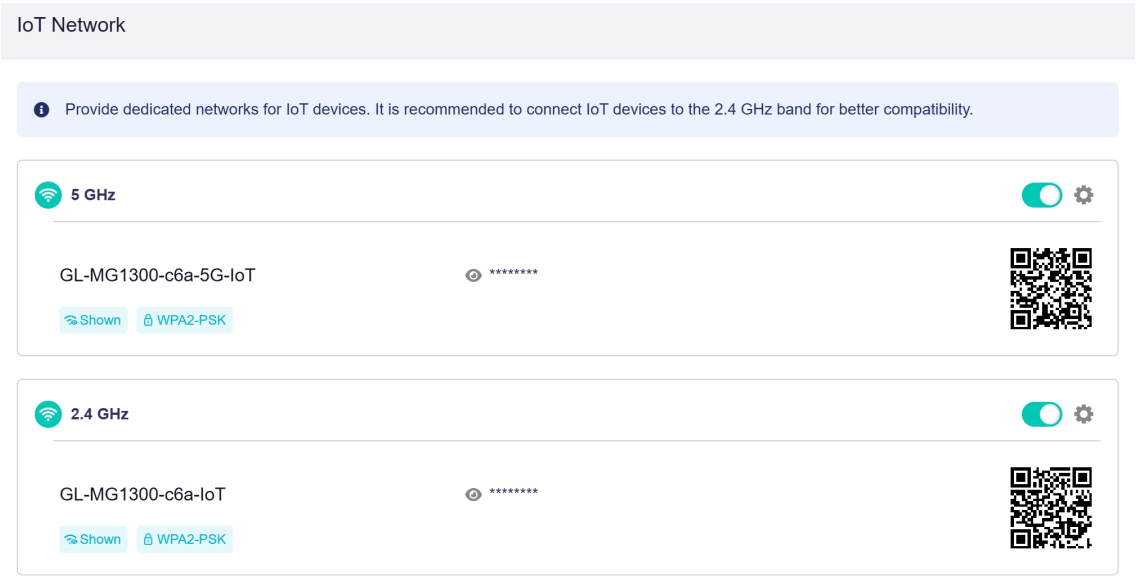
Aby utworzyć sieć Wi-Fi IoT, kliknij przycisk **Add** po prawej stronie.



Wybierz pasmo Wi-Fi, skonfiguruj szczegóły sieci, a następnie kliknij **Apply**.



Po włączeniu strona wygląda jak na poniższej ilustracji.


IoT Network
Provide dedicated networks for IoT devices. It is recommended to connect IoT devices to the 2.4 GHz band for better compatibility.
5 GHz
GL-MG1300-c6a-5G-IoT
****
Shown
WPA2-PSK
2.4 GHz
GL-MG1300-c6a-IoT
****
Shown
WPA2-PSK

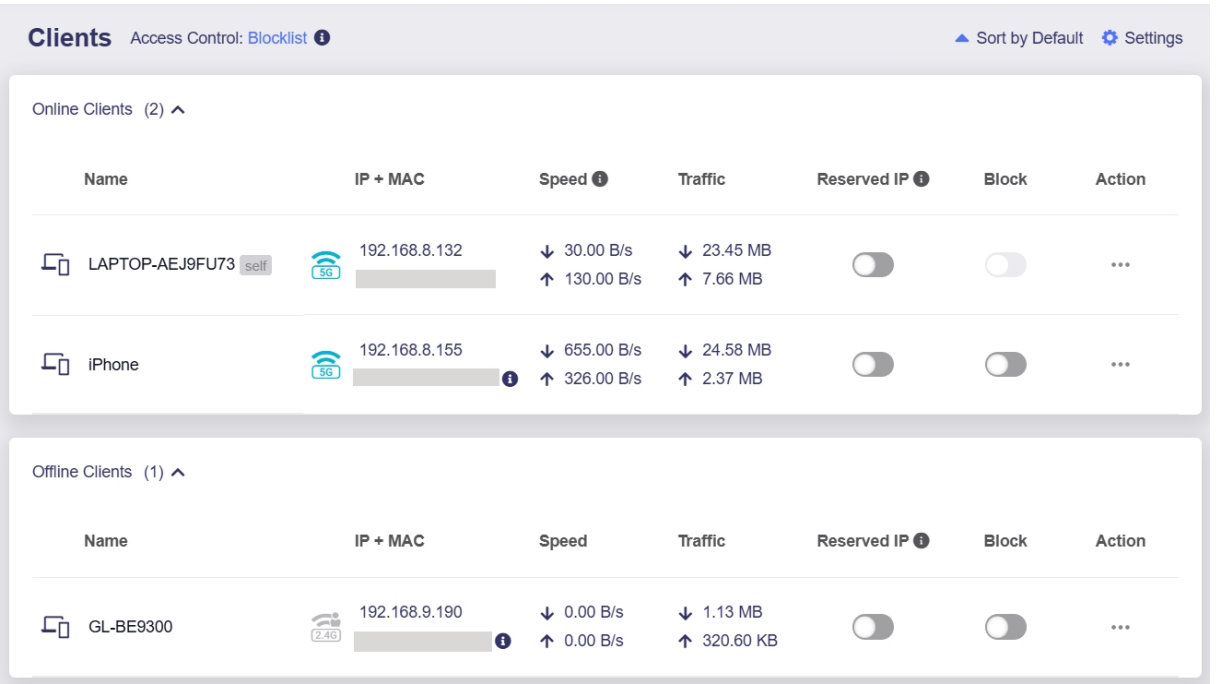
Rozdział 6

Urządzenia klienckie

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

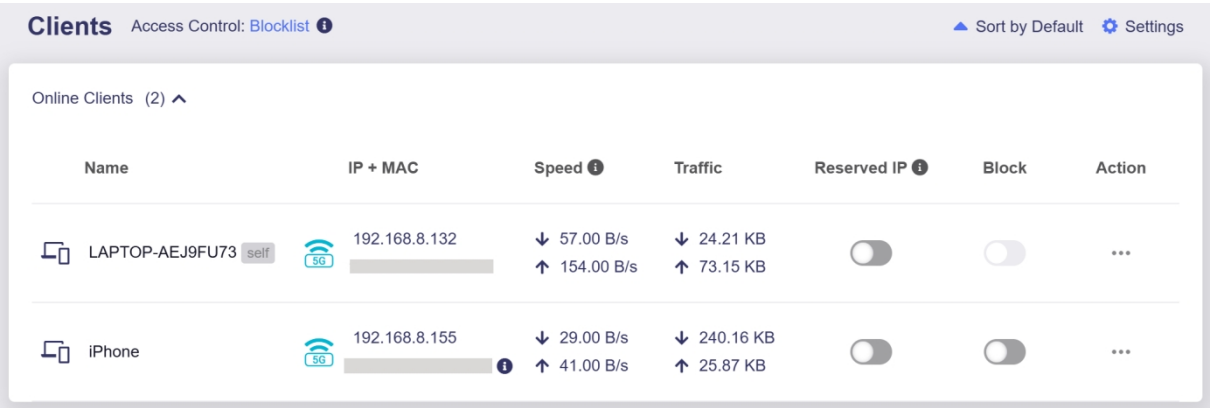
Zaloguj się do panelu administracyjnego routera i przejdź do **CLIENTS**.

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.

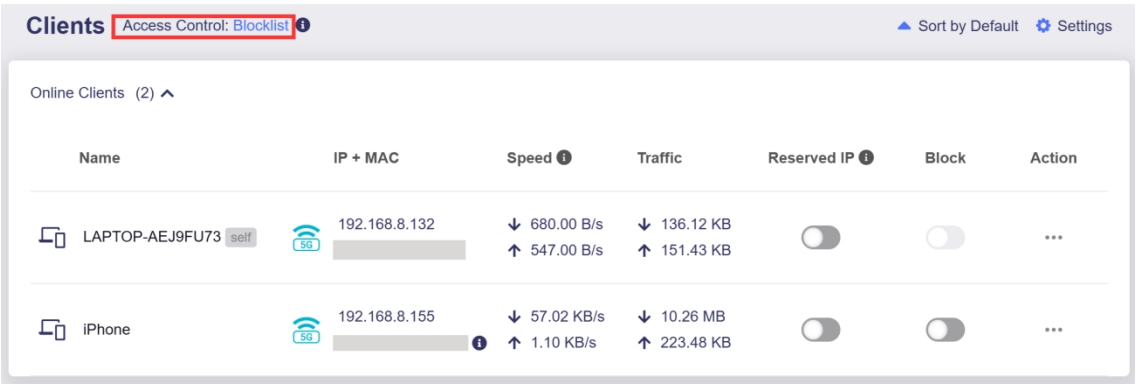
5. **Rezerwacja adresu IP**

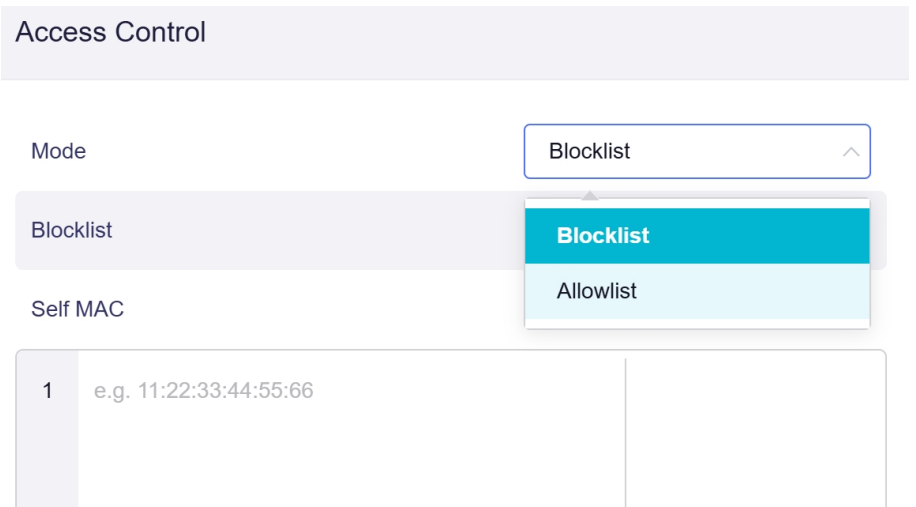
   W piątej kolumnie możesz jednym kliknięciem zarezerwować adres IP dla podłączonego urządzenia. Po przypisaniu klientowi w sieci lokalnej zarezerwowanego adresu IP będzie on otrzymywał ten sam adres przy każdym połączeniu z routerem.

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.



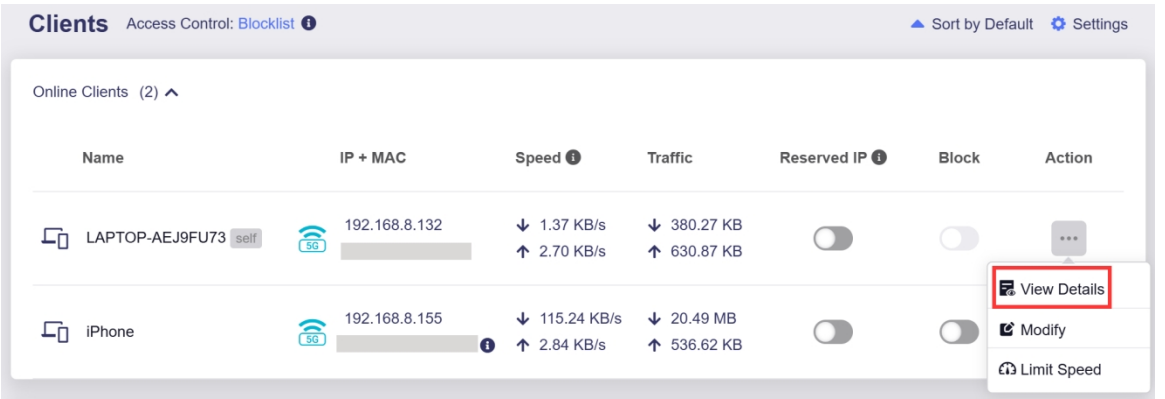


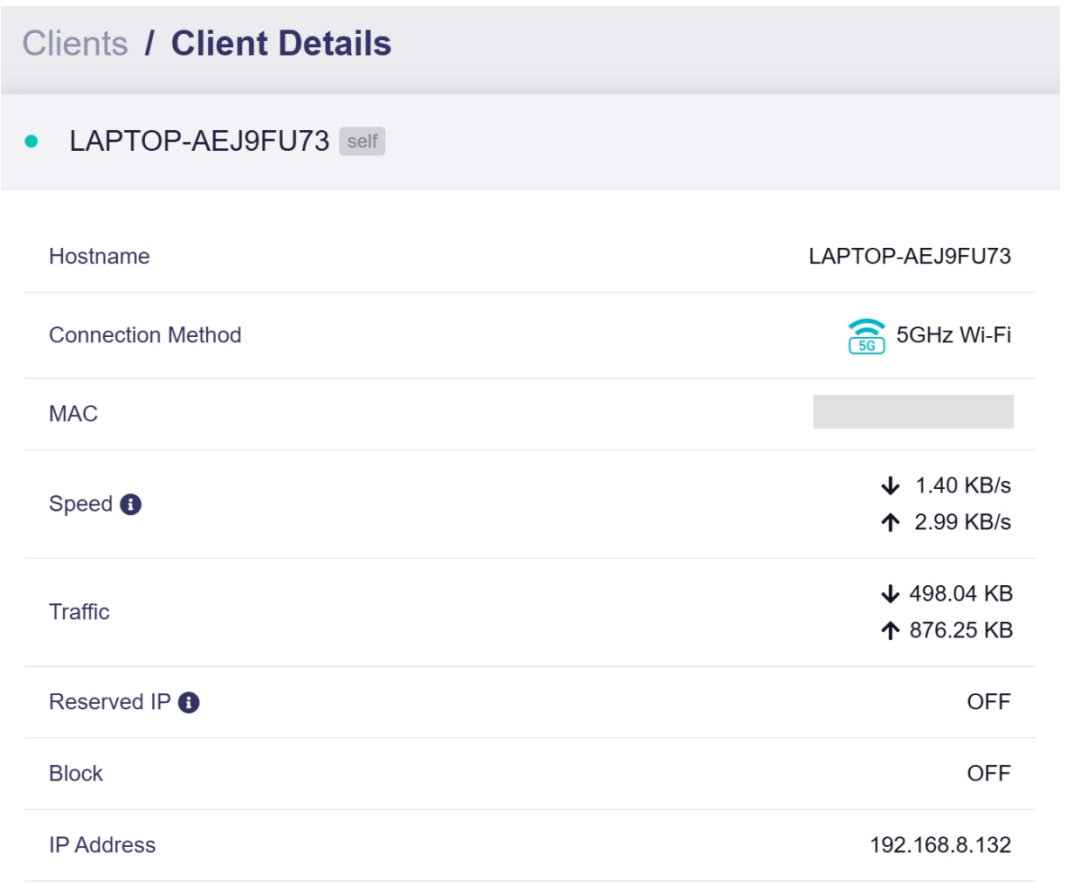
- **Blacklist**: urządzenia o adresach MAC znajdujących się na liście blokowanych nie mogą łączyć się z tym routerem. Blokowanie klienta opiera się na adresie MAC urządzenia. Jeśli zablokowane urządzenie następnym razem użyje innego adresu MAC, nadal będzie mogło połączyć się z routerem.
- **Allowlist**: 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**

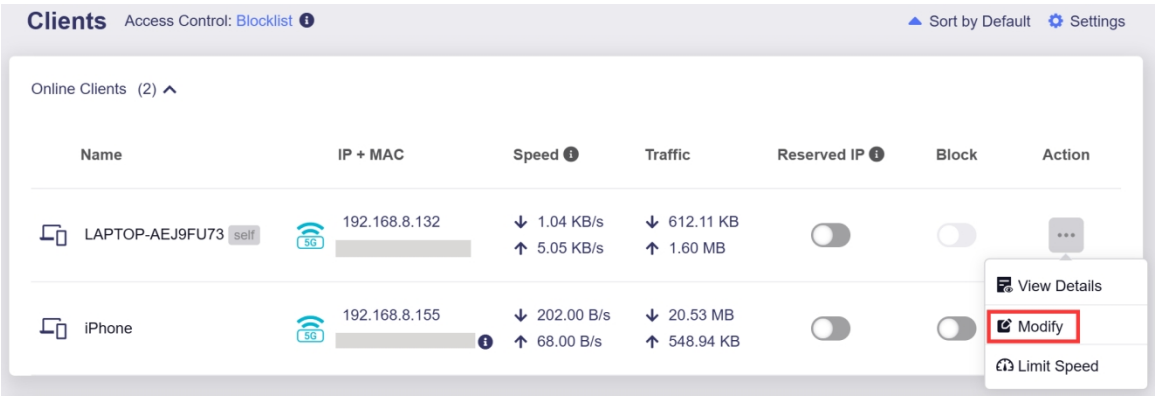
   Kliknij ikonę trzech kropek w kolumnie **Action**, a następnie wybierz **View Details** z menu, aby wyświetlić szczegóły urządzenia na jednej stronie.

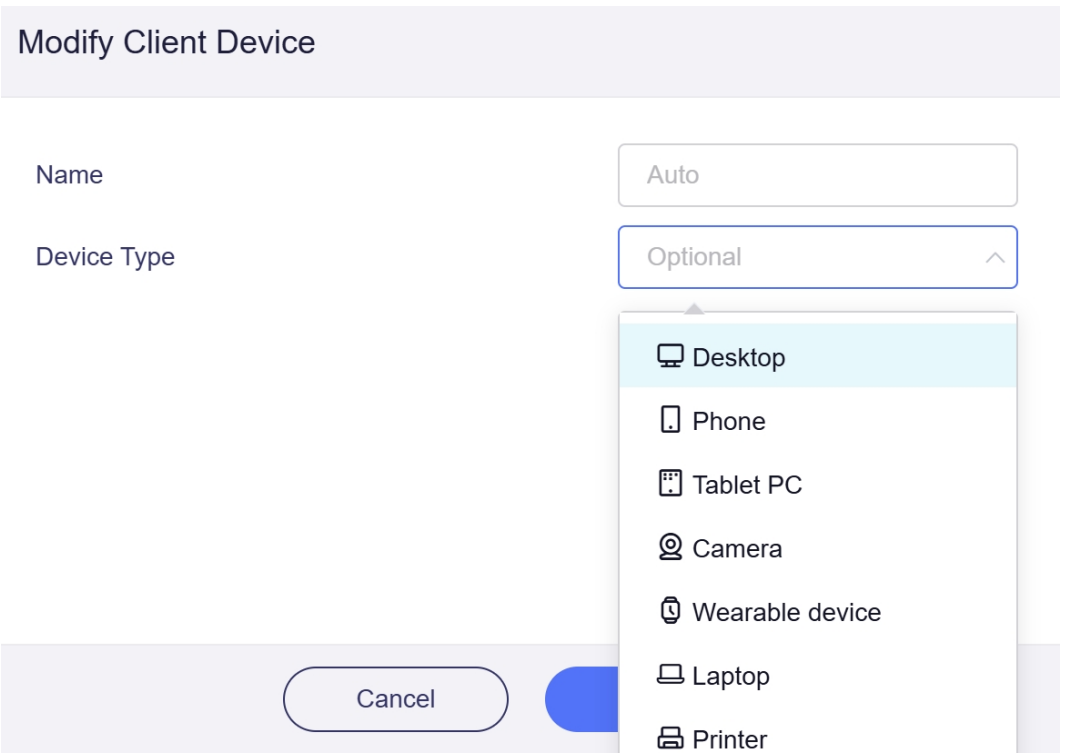




2. **Modyfikowanie**

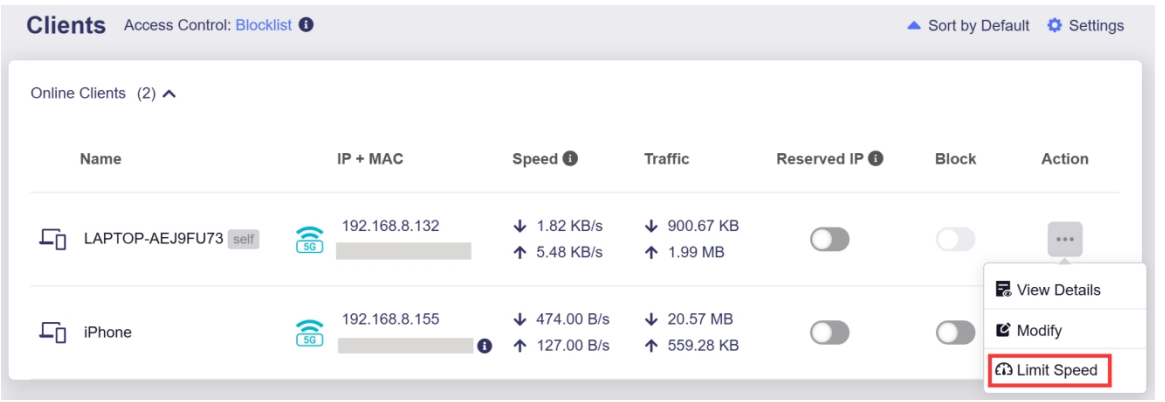
Kliknij ikonę trzech kropek w kolumnie **Action**, a następnie wybierz **Modify** z menu, aby zmienić nazwę i typ urządzenia.

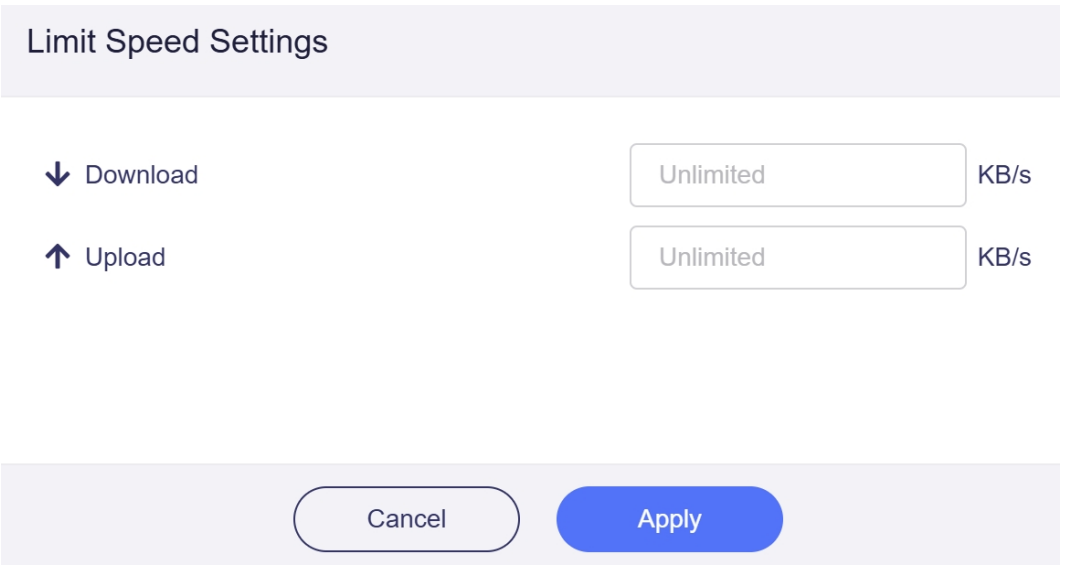




3. **Ograniczanie prędkości**

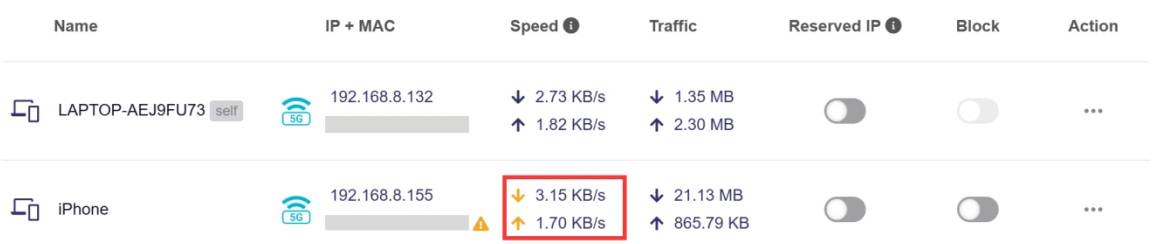
Kliknij ikonę trzech kropek w kolumnie **Action**, a następnie wybierz **Limit Speed** z menu.





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

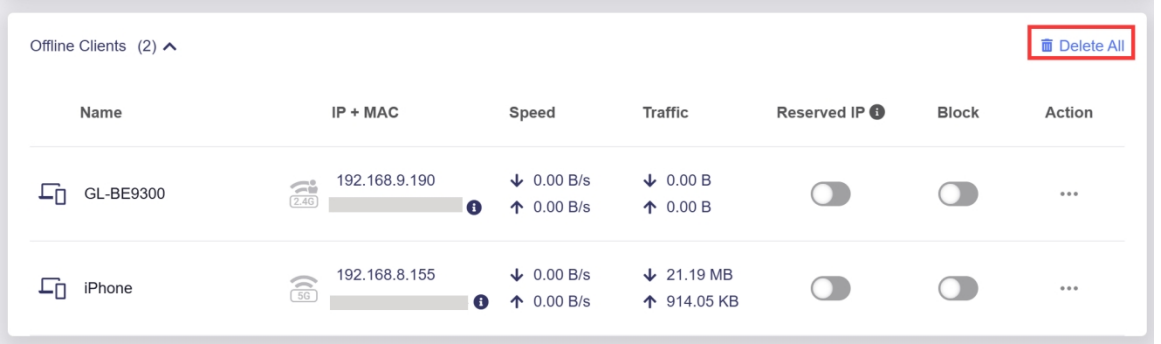
Jeśli dla urządzenia ustawiono ograniczenie prędkości, strzałki prędkości wysyłania i pobierania zmienią kolor na żółty.



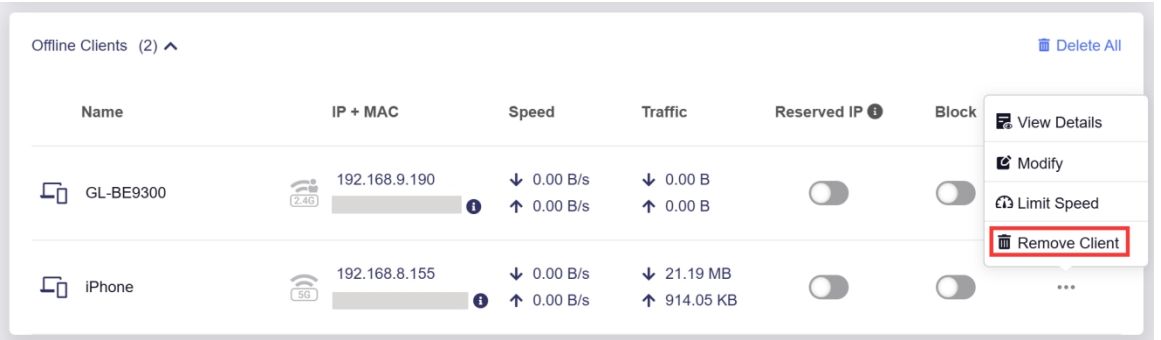
Wskazówka: jeśli opcja Limit Speed nie jest widoczna, przejdź do **NETWORK** > **Network Acceleration** i wyłącz przyspieszanie sieci. Opcja Limit Speed stanie się wtedy dostępna.

6.3 Usuwanie urządzeń klienckich

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

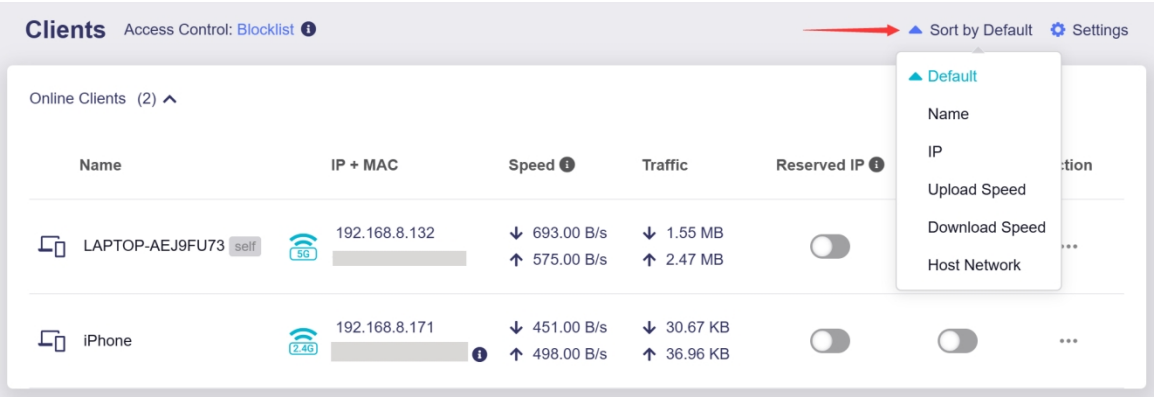


Aby usunąć określone urządzenie klienckie, kliknij ikonę trzech kropek w kolumnie **Action**, a następnie wybierz **Remove Client** z menu.



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

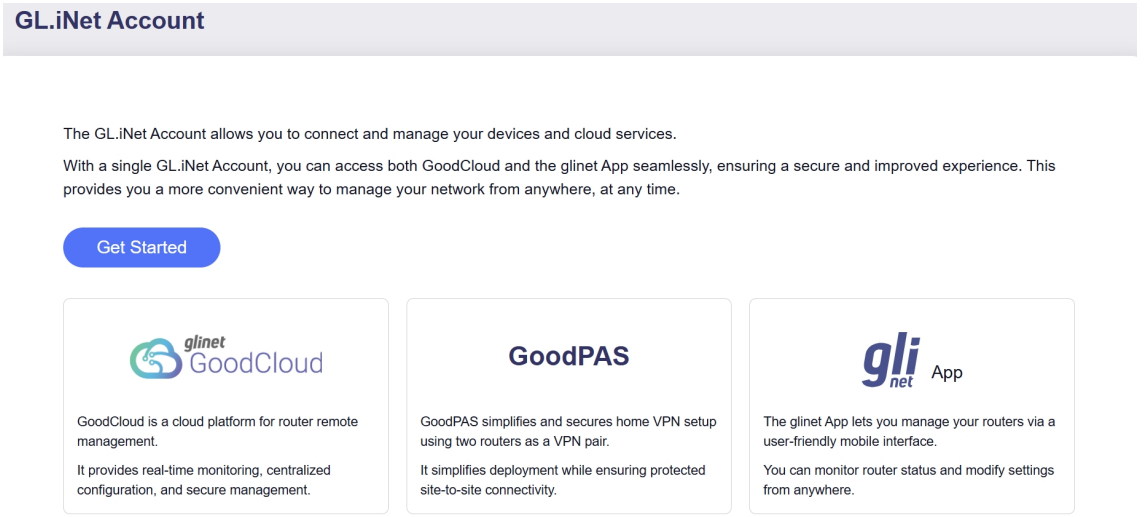
W tym rozdziale opisano trzy usługi chmurowe: GL.iNet Account, GoodCloud i GoodPAS.

7.1 Konto GL.iNet

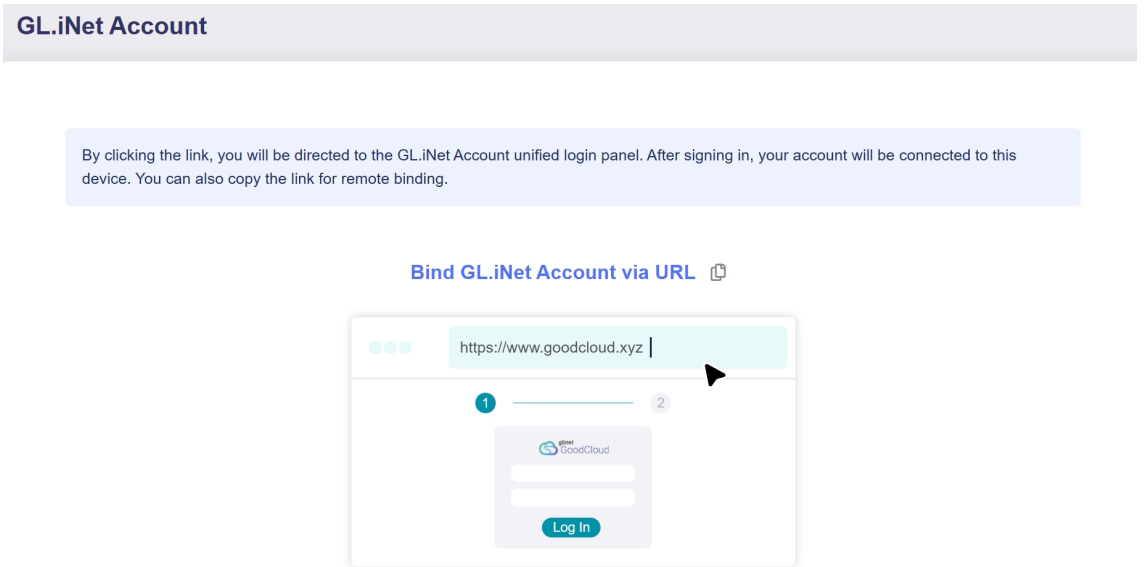
Konto GL.iNet umożliwia łączenie urządzeń i usług chmurowych oraz zarządzanie nimi. Zapewnia dostęp do funkcji i usług chmurowych, w tym GoodCloud, GoodPAS i aplikacji glinet.

7.1.1 Włączanie konta GL.iNet

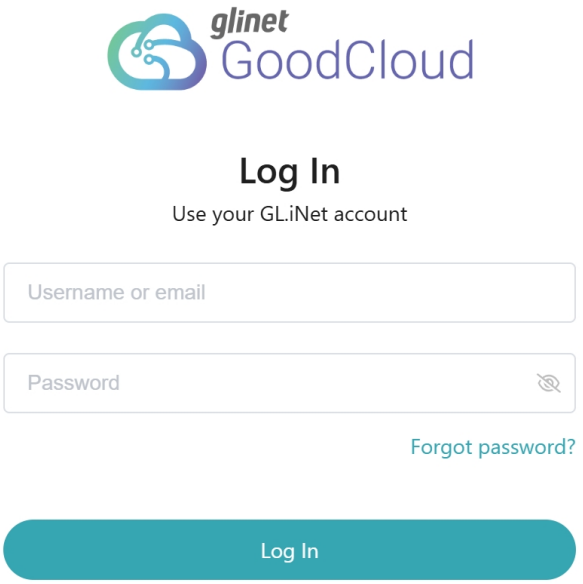
1. Zaloguj się do panelu administracyjnego routera, przejdź do **CLOUD SERVICE** > **GL.iNet Account** i kliknij **Get Started.**



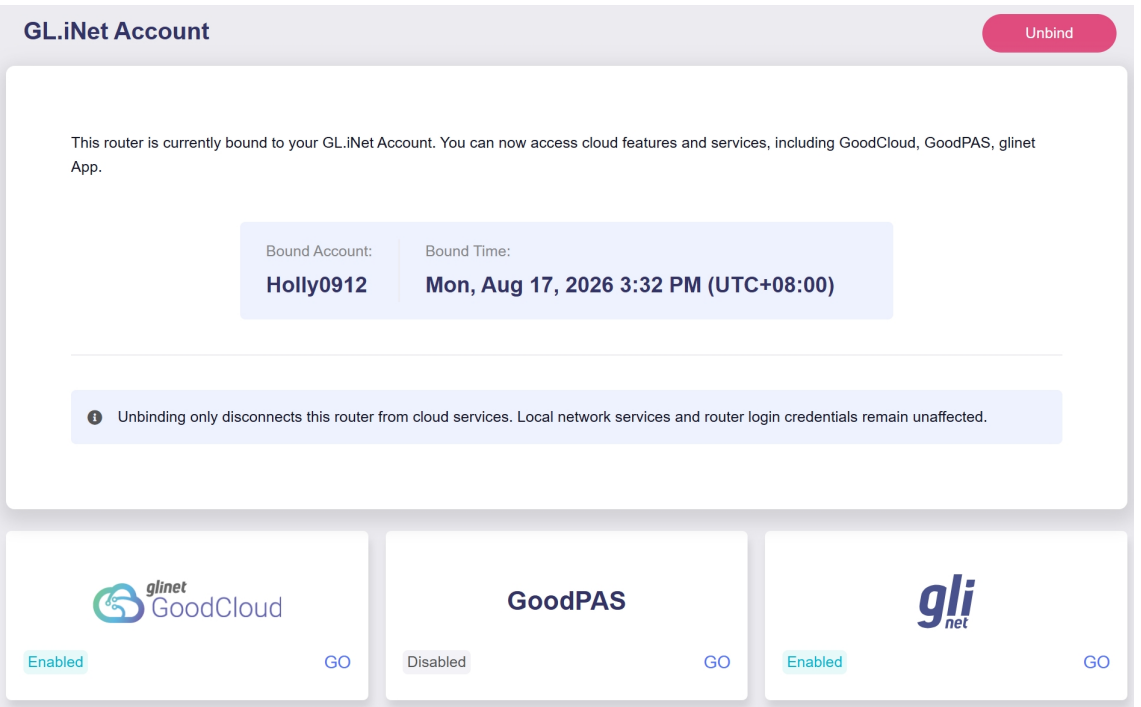
2. Na stronie pojawi się adres URL. Kliknij **łącze**, aby zalogować się na stronie konta GL.iNet, lub skopiuj je w celu zdalnego powiązania.



3. Zaloguj się na konto GL.iNet. Jeśli nie masz konta, zarejestruj się i zaloguj.



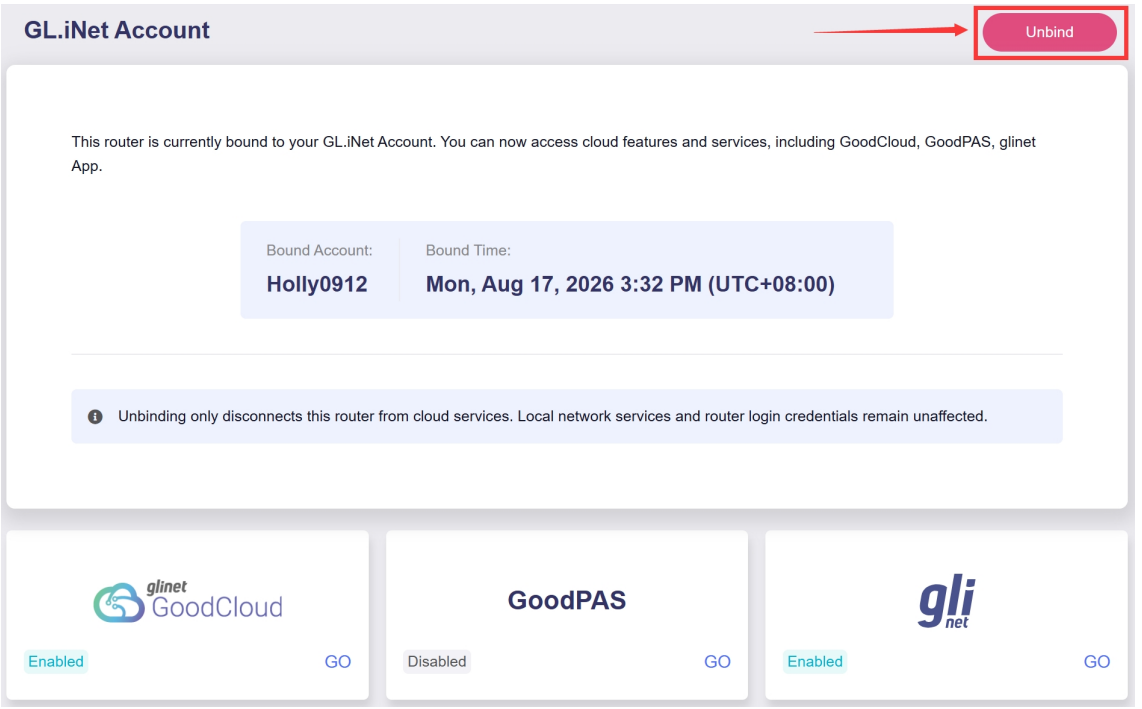
4. Po zalogowaniu strona wyświetla powiązane konto (Bound Account) i czas powiązania (Bound Time). Możesz tu zarządzać powiązaniem routera z kontem GL.iNet. Etykieta Enabled/Disabled w lewym dolnym rogu każdej usługi chmurowej wskazuje jej stan. Kliknij **GO** obok usługi, aby otworzyć stronę jej funkcji.



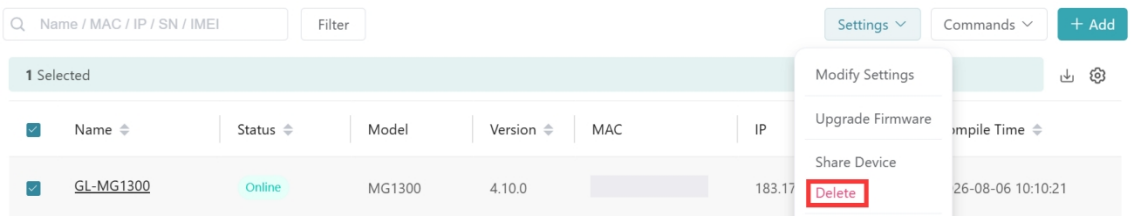
5. GoodPAS jest domyślnie wyłączony. Instrukcje włączania znajdziesz w rozdziale 7.3 GoodPAS.

7.1.2 Usuwanie powiązania z kontem GL.iNet

W panelu administracyjnym routera przejdź do **CLOUD SERVICES** > **GL.iNet Account** i kliknij **Unbind**. Powiązanie urządzenia z kontem GoodCloud zostanie usunięte.



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.



7.2 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.

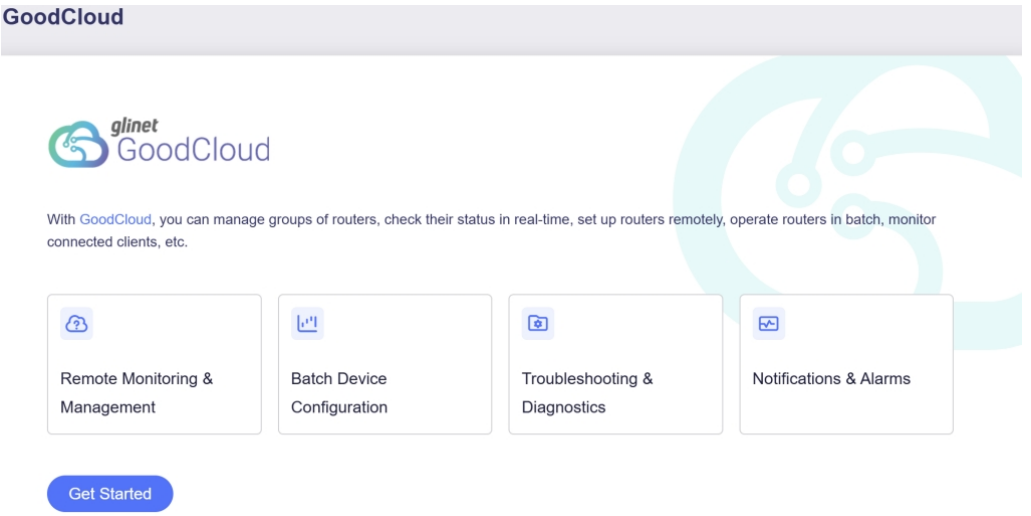
Dzięki GoodCloud możesz:

- 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

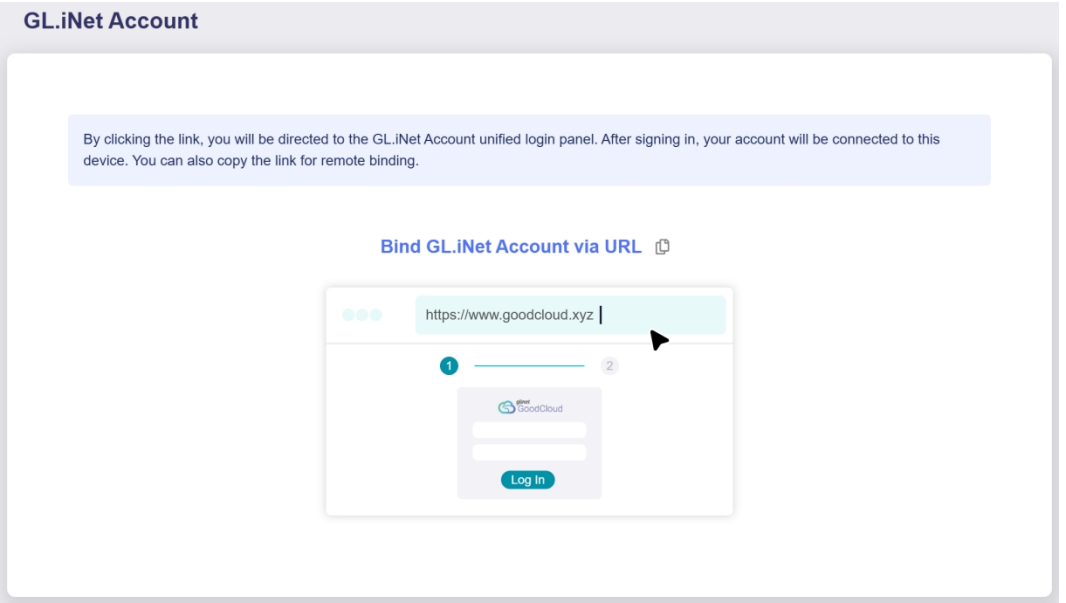
Niektóre funkcje są dostępne w planach Enterprise i VAR (Value Added Reseller). Szczegóły znajdziesz tutaj.

7.2.1 Włączanie GoodCloud

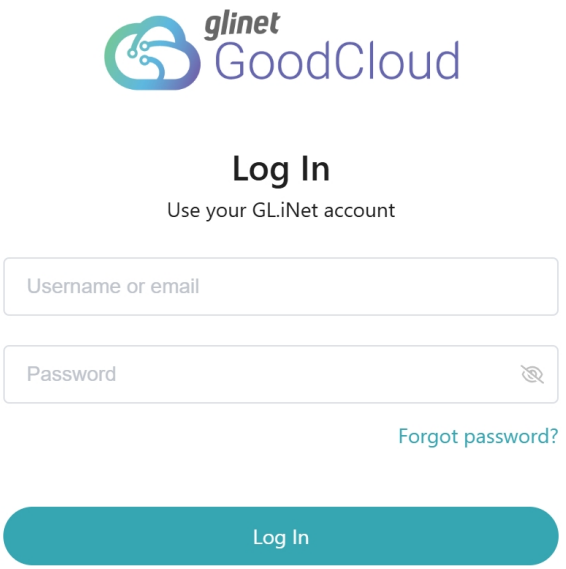
1. Zaloguj się do panelu administracyjnego routera, przejdź do **CLOUD SERVICE** > **GoodCloud** i kliknij **Get Started.**



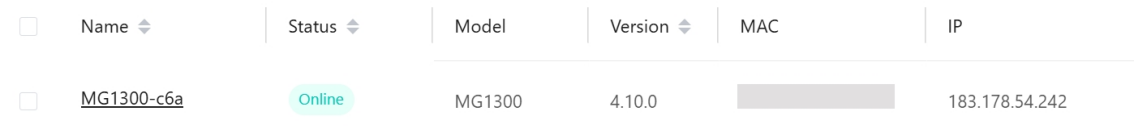
2. Na stronie pojawi się adres URL. Kliknij **łącze**, aby zalogować się na stronie konta GL.iNet, lub skopiuj je w celu zdalnego powiązania.



3. Zaloguj się na konto GL.iNet. Jeśli nie masz konta, zarejestruj się i zaloguj.



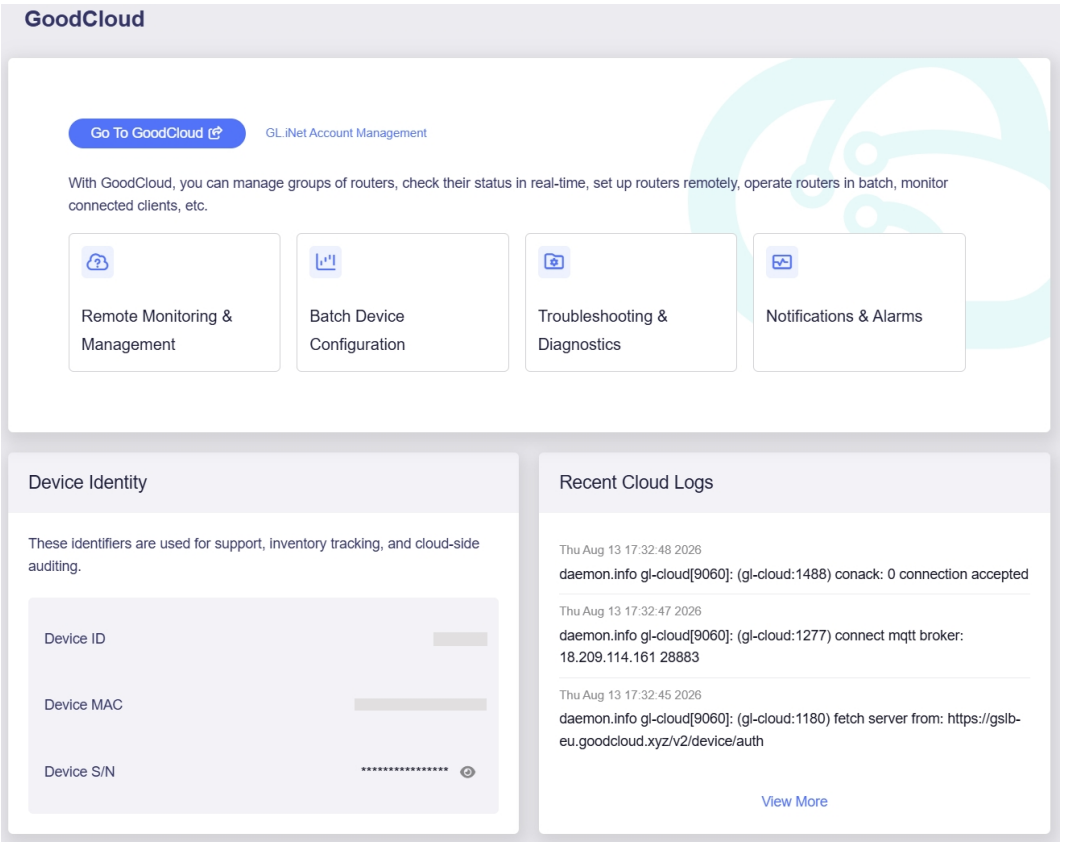
4. W następnym kroku potwierdź dane konta i urządzenia, a następnie kliknij **Bind**. Nastąpi przekierowanie do platformy GoodCloud, na której możesz sprawdzić, czy router został powiązany z kontem.



Wskazówki:

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

5. Po pomyślnym powiązaniu wróć do strony usługi chmurowej w panelu administracyjnym. Zobaczysz tożsamość powiązanego urządzenia i ostatnie dzienniki chmurowe, w tym identyfikator urządzenia, jego adres MAC i numer seryjny.



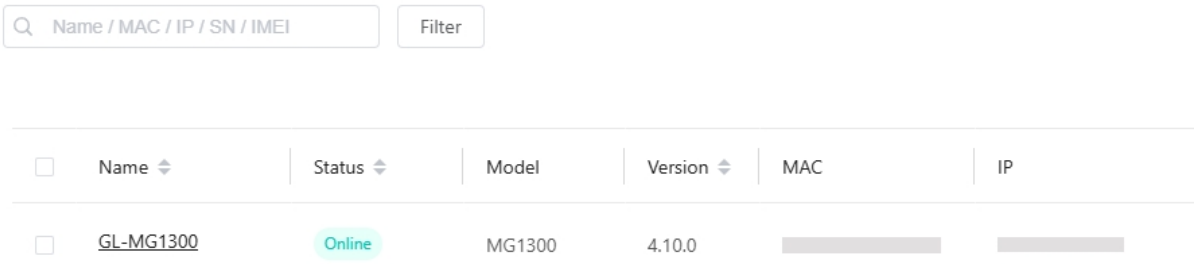
6. Po zalogowaniu do GoodCloud domyślnie włączane są także Remote Web Access i Remote SSH. Jest to szczególnie przydatne przy zdalnym zarządzaniu i rozwiązywaniu problemów.

- **Remote Web Access**: umożliwia zdalny dostęp do panelu administracyjnego routera z GoodCloud przez HTTP/HTTPS.
- **Remote SSH**: umożliwia zdalny dostęp do terminala routera z GoodCloud przez SSH.

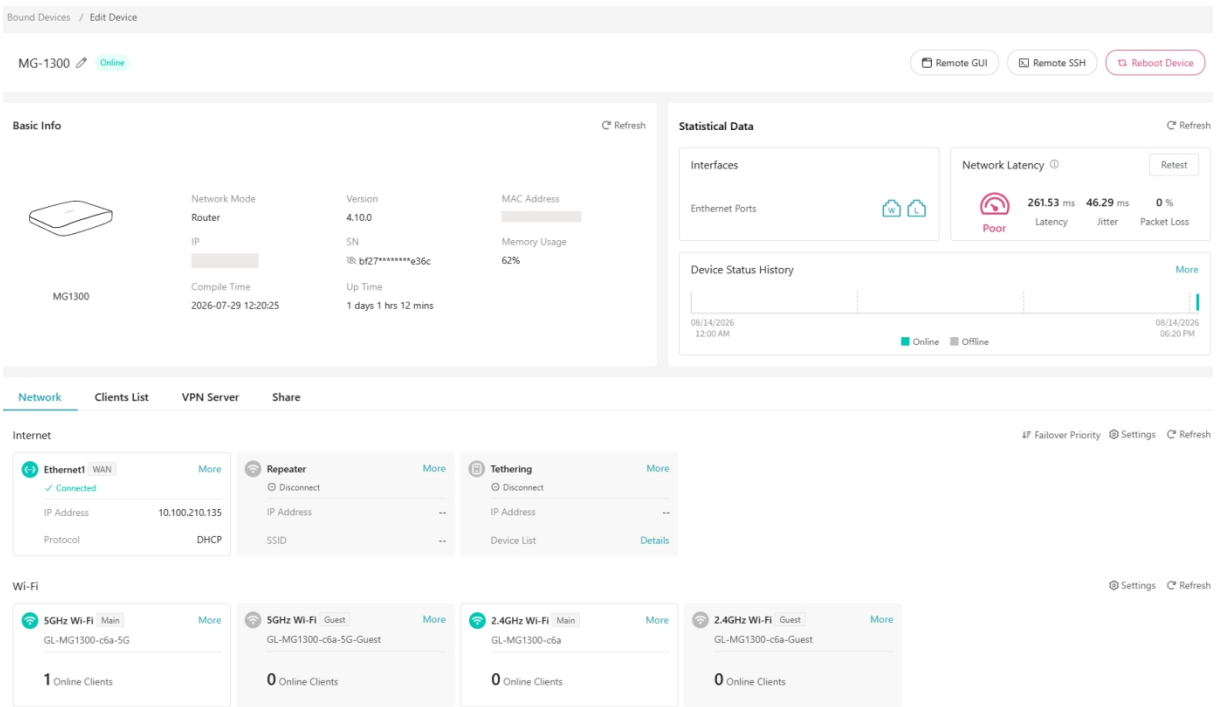
7.2.2 Zarządzanie routerem

Sprawdzanie szczegółów urządzenia

Zaloguj się na platformie GoodCloud i przejdź do **Devices** > **Bound Devices**. Możesz sprawdzić podstawowe informacje o urządzeniu, takie jak nazwa hosta, stan (online/offline), model, wersja oprogramowania i adres MAC.

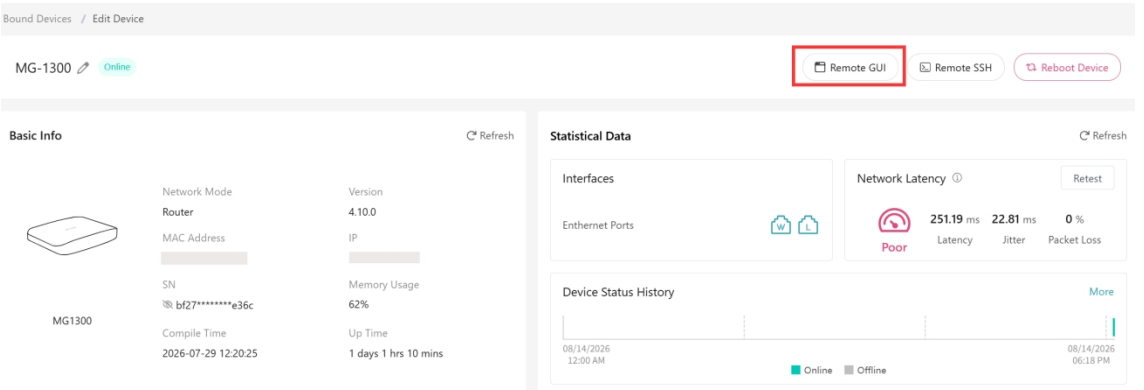


Kliknij nazwę urządzenia, aby otworzyć stronę szczegółów zawierającą podstawowe informacje, statystyki, przegląd sieci, listę klientów i oś czasu. Możesz też wykonywać zaawansowane działania, np. zdalnie uzyskiwać dostęp do routera i uruchamiać go ponownie.

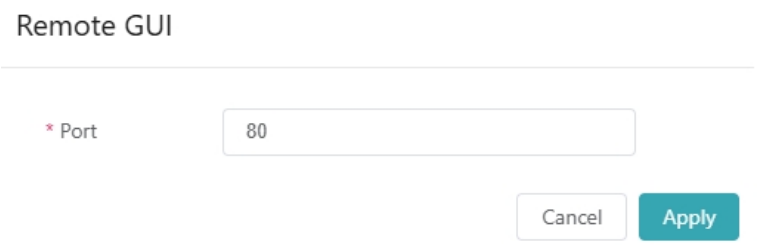


Zdalny dostęp przez przeglądarkę

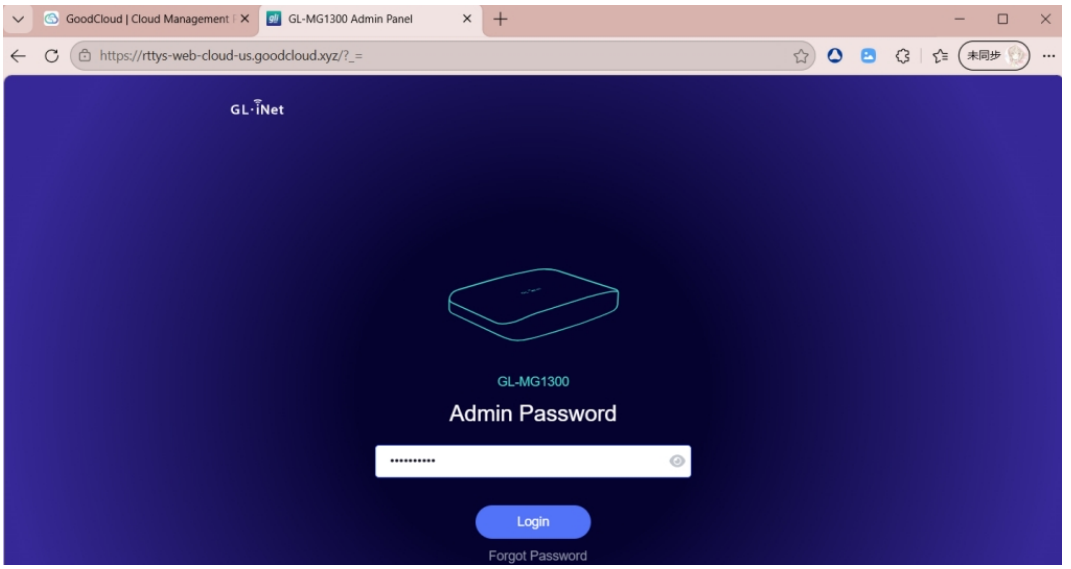
1. Zaloguj się na platformie GoodCloud i przejdź do **Devices** > **Bound Devices**. Kliknij urządzenie, do którego chcesz uzyskać dostęp, aby otworzyć stronę jego szczegółów. Na tej stronie kliknij przycisk **Remote GUI** w prawym górnym rogu.



2. 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**.

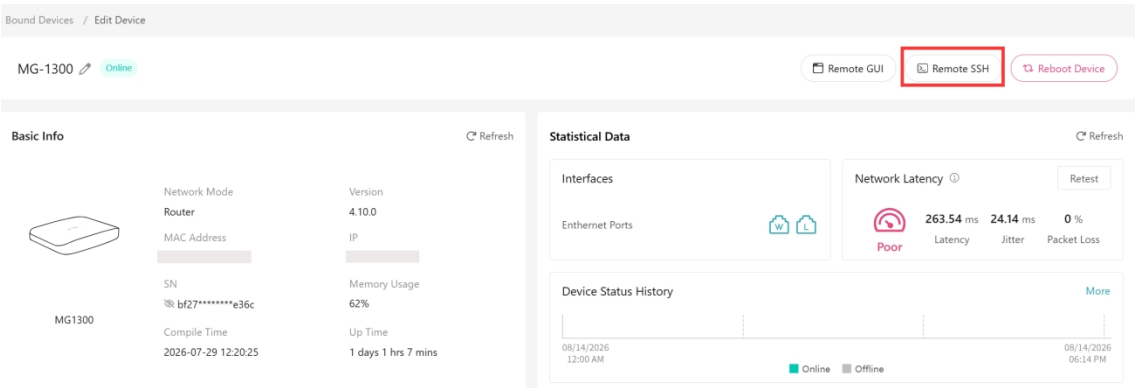


3. Otworzy się strona logowania routera. Wprowadź hasło administratora, aby uzyskać zdalny dostęp do panelu administracyjnego routera.



Zdalny dostęp do terminala

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

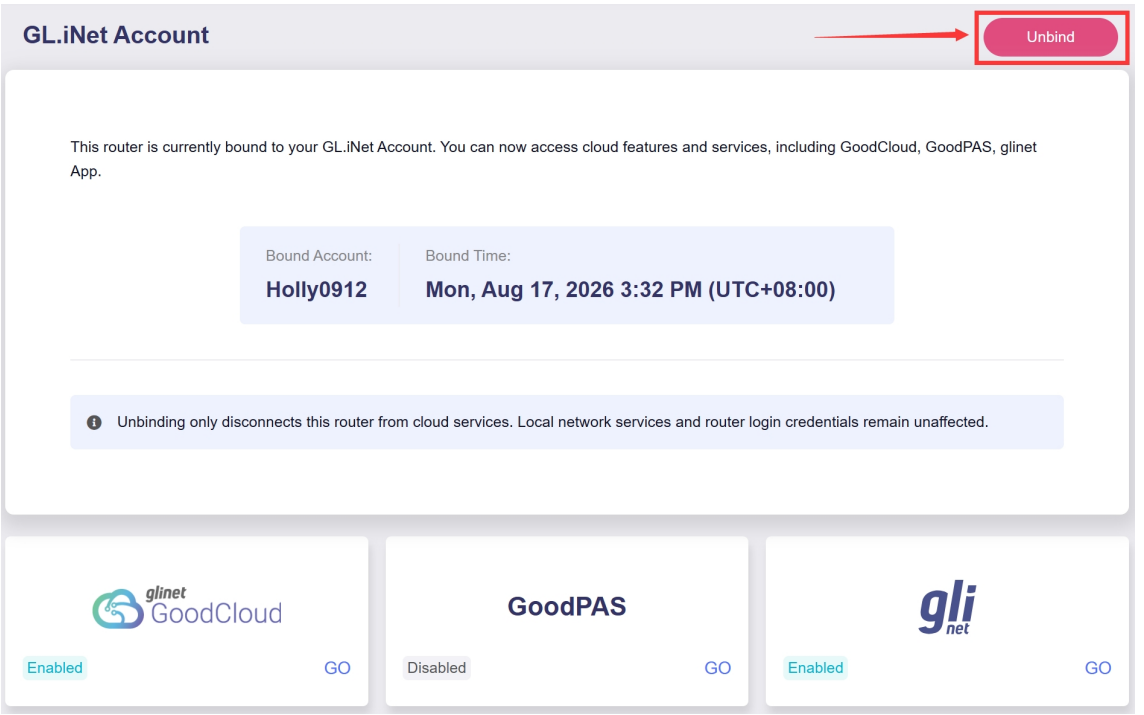


3. Zaloguj się jako **root** i wprowadź hasło, aby uzyskać dostęp do terminala routera.

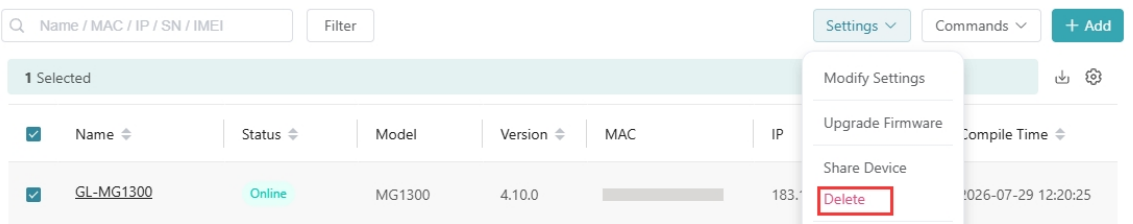

GL-MG1300 login: root
Password:
BusyBox v1.35.0 (2023-04-09 12:27:46 UTC) built-in shell (ash)
W I R E L E S S F R E E D O M
OpenWrt 22.03.4, r20123-38ccc47687
root@GL-MG1300:~#

7.2.3 Usuwanie powiązania urządzenia

W panelu administracyjnym routera przejdź do **CLOUD SERVICES** > **GL.iNet Account** i kliknij **Unbind**. Powiązanie urządzenia z kontem GoodCloud zostanie usunięte.



Możesz też zalogować się na platformie chmurowej i przejść do **Devices** > **Bound Devices**. Wybierz urządzenie, którego powiązanie chcesz usunąć, kliknij **Settings** w prawym górnym rogu, a następnie wybierz **Delete**. Powiązanie urządzenia z kontem GoodCloud zostanie usunięte.



7.3 GoodPAS

GoodPAS to zaawansowana funkcja sieciowa routerów GL.iNet zapewniająca wygodny zdalny dostęp i zarządzanie urządzeniami. Jest zintegrowana z pakietem SDK routerów GL.iNet i korzysta z protokołu AmneziaWG z wbudowanym maskowaniem ruchu, zapewniając stabilne, bezpieczne połączenia i niezawodny zdalny dostęp w dowolnym miejscu i czasie.

Funkcja umożliwia wygodny zdalny dostęp do sieci domowej. Urządzenia można skonfigurować i sparować bezpośrednio w internetowym panelu administracyjnym za pomocą dynamicznego kodu dostępu. Bezpieczne połączenie między routerem podróżnym a siecią domową powstaje w kilka sekund, bez rejestracji i logowania.

Uwaga:

1. Nie zaleca się jednoczesnego korzystania z GoodPAS i następujących funkcji, ponieważ może to powodować konflikty trasowania: GoodCloud Site to Site, ZeroTier, Tailscale, Tor.
2. Gdy GoodPAS jest włączony, nie można korzystać z funkcji Network Mode.

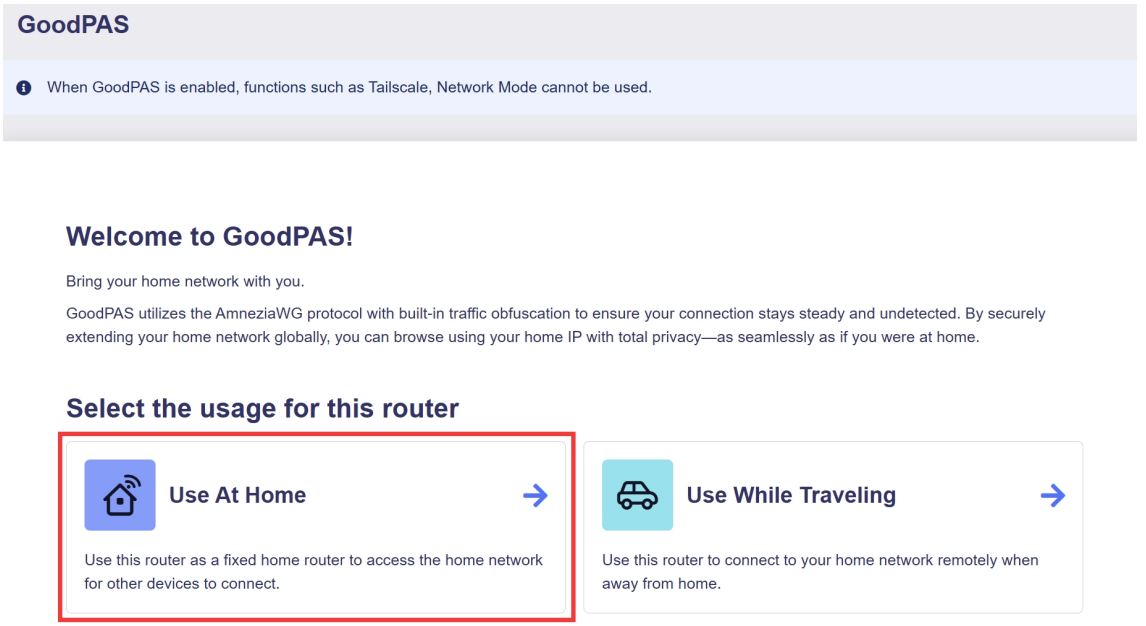
7.3.1 Szybka konfiguracja

Poniżej przedstawiono przykład konfiguracji sieci GoodPAS za pomocą Mango 2 (GL-MG1300) i Flint 3 (GL-BE9300). Flint 3 pełni rolę routera domowego, a Mango 2 jest routerem podróżnym, który kieruje ruch sieciowy z powrotem do Flint 3, aby uzyskać dostęp do Internetu.

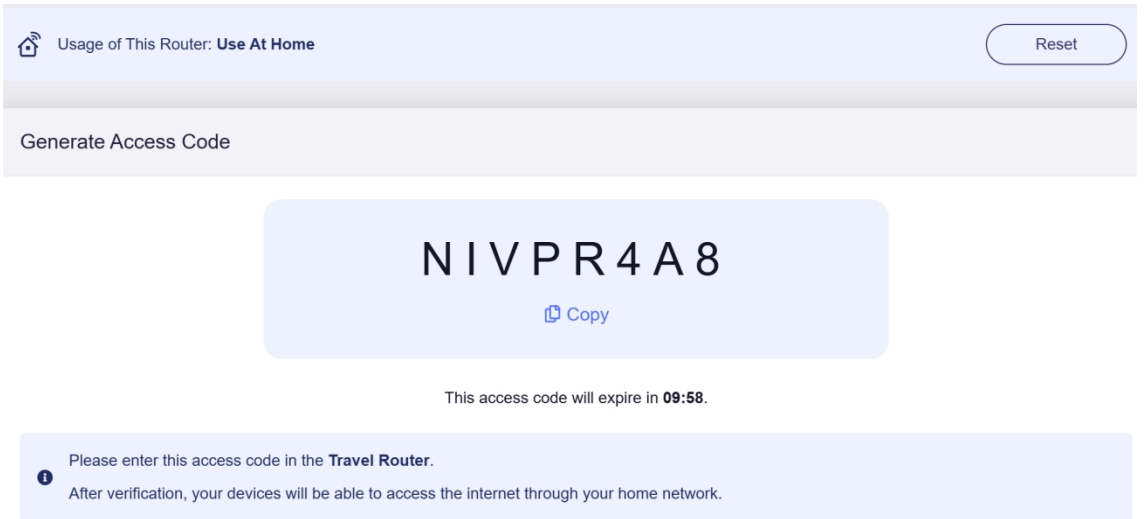
Wskazówka: Każdy router GL.iNet otrzymuje **10 GB bezpłatnego transferu miesięcznie** na potrzeby sieci GoodPAS. Urządzenia w sieci GoodPAS korzystają z pakietu danych routera domowego do uzyskiwania dostępu do Internetu. W razie potrzeby możesz przejść na plan GoodPAS+ z nielimitowanym transferem.

1. Skonfiguruj dostęp do Internetu na Flint 3.
   Zaloguj się do internetowego panelu administracyjnego Flint 3 i przejdź na stronę INTERNET. Połącz router z Internetem jedną z obsługiwanych metod: Ethernet, Repeater, Tethering lub Cellular.

2. W panelu administracyjnym Flint 3 przejdź do **CLOUD SERVICES** > **GoodPAS**. Kliknij **Use At Home**.

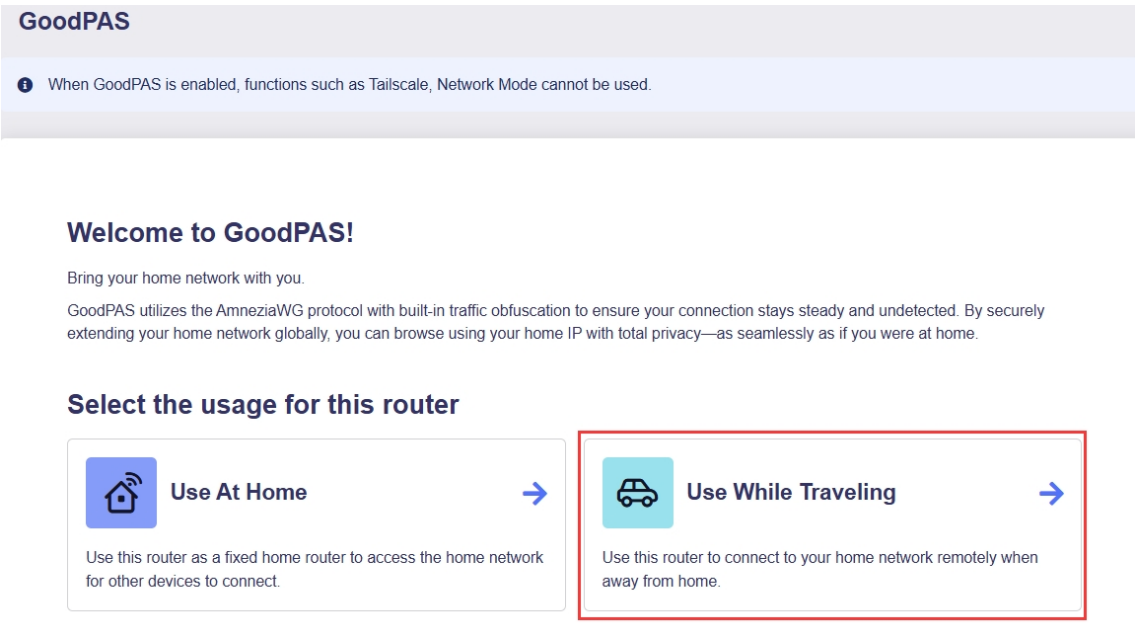


Zostanie wygenerowany kod **Access Code**. Skopiuj go do późniejszego użycia.

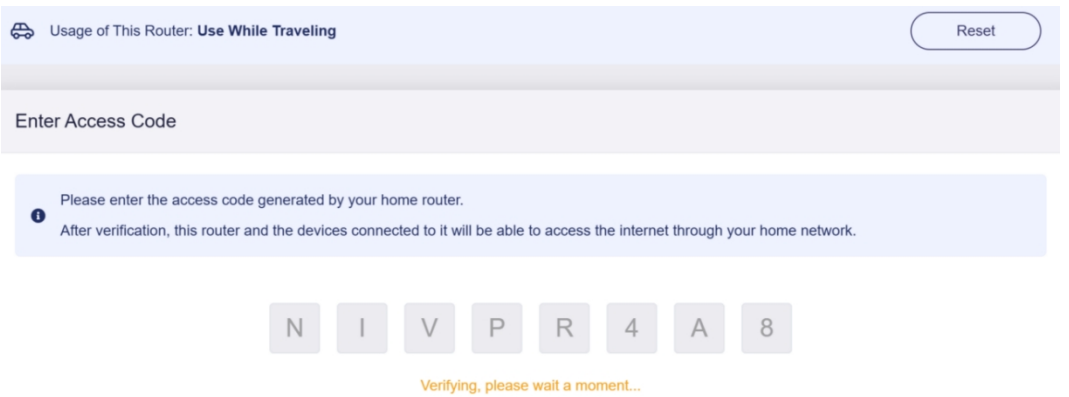


3. Skonfiguruj połączenie Mango 2 z Internetem.
   Zaloguj się do panelu administracyjnego Mango 2 i przejdź do strony INTERNET. Połącz router z Internetem jednym z obsługiwanych sposobów: Ethernet, Repeater, Tethering lub Cellular.
4. Wprowadź kod dostępu.

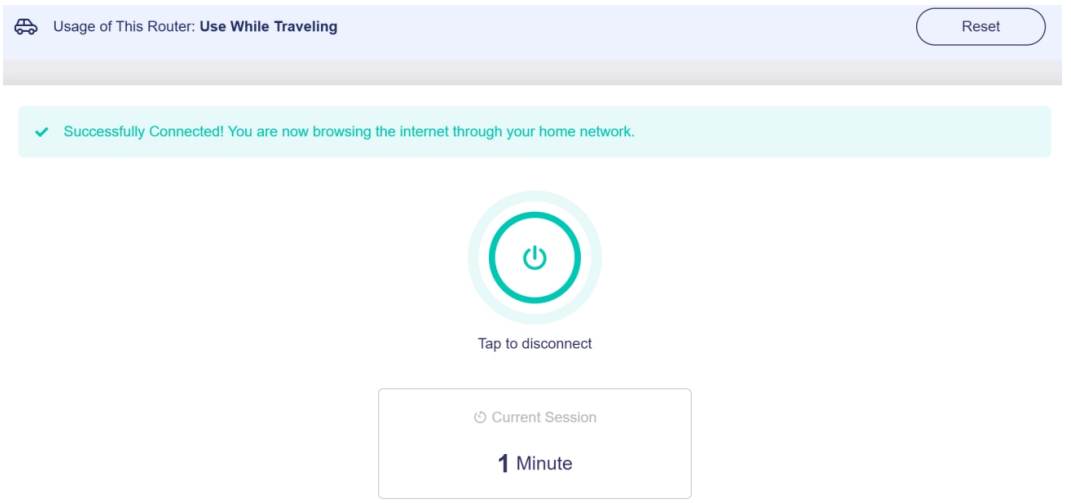
W panelu administracyjnym Mango 2 przejdź do **CLOUD SERVICES** > **GoodPAS**. Kliknij **Use While Traveling**.



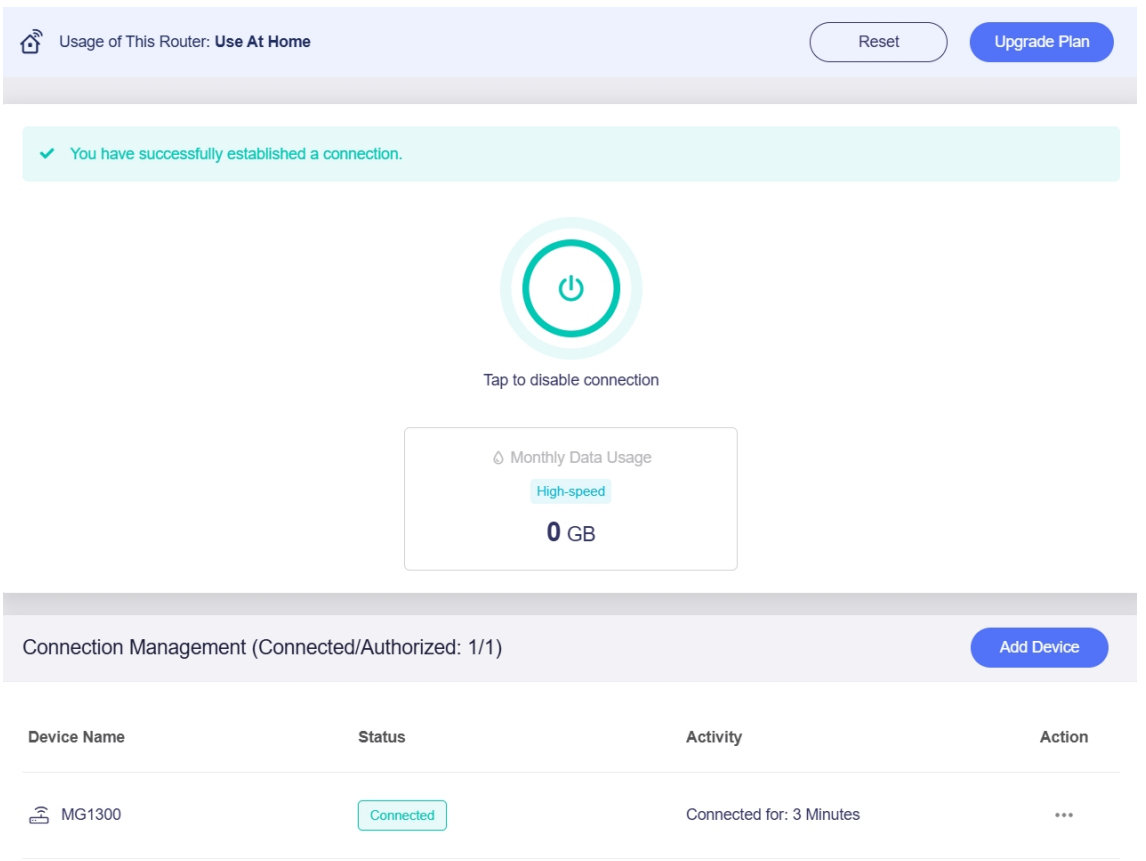
Wprowadź kod Access Code uzyskany w kroku 2 i poczekaj na zakończenie weryfikacji.



Połączenie z domowym routerem Flint 3 zostanie nawiązane. Teraz możesz bezpiecznie korzystać z Internetu przez swoją sieć domową.

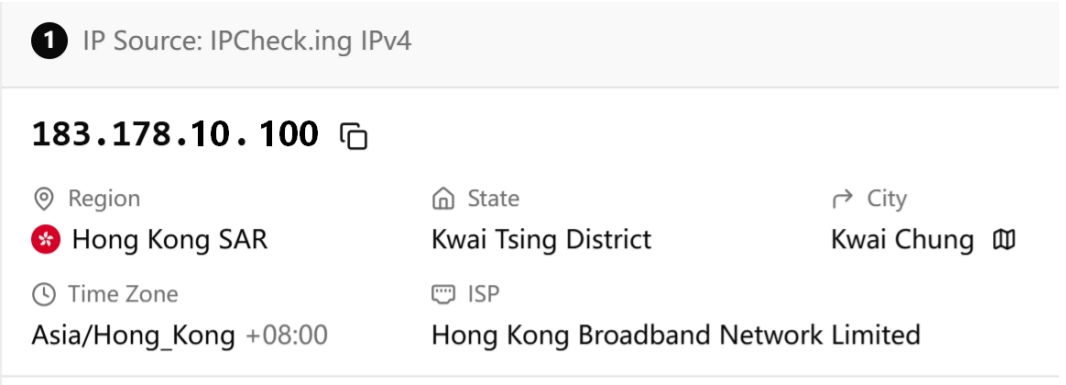


5. Internetowy panel administracyjny Flint 3 również wyświetla stan połączenia, jak pokazano poniżej.

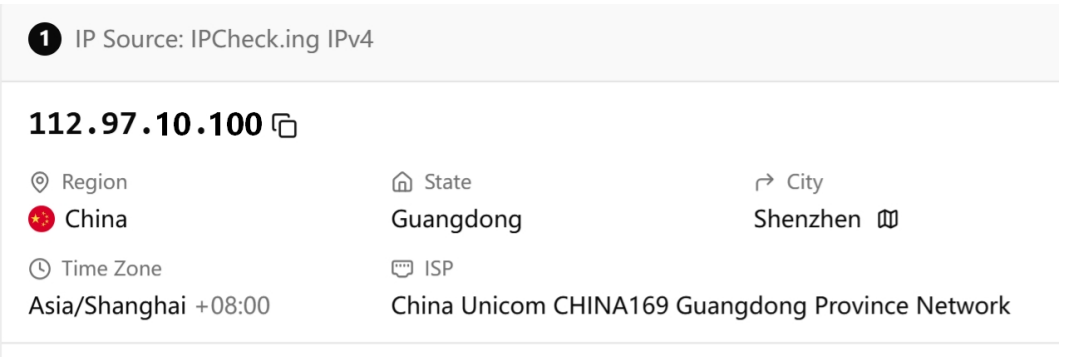


7.3.2 Testowanie łączności

1. Podłącz laptop lub smartfon do sieci Wi-Fi routera podróżnego Mango 2.
2. Otwórz przeglądarkę i odwiedź ipcheck.ing lub inną stronę sprawdzającą adres IP. Wyświetlony zostanie publiczny adres IP Flint 3, co oznacza, że Mango 2 uzyskuje dostęp do Internetu przez domowy router Flint 3.

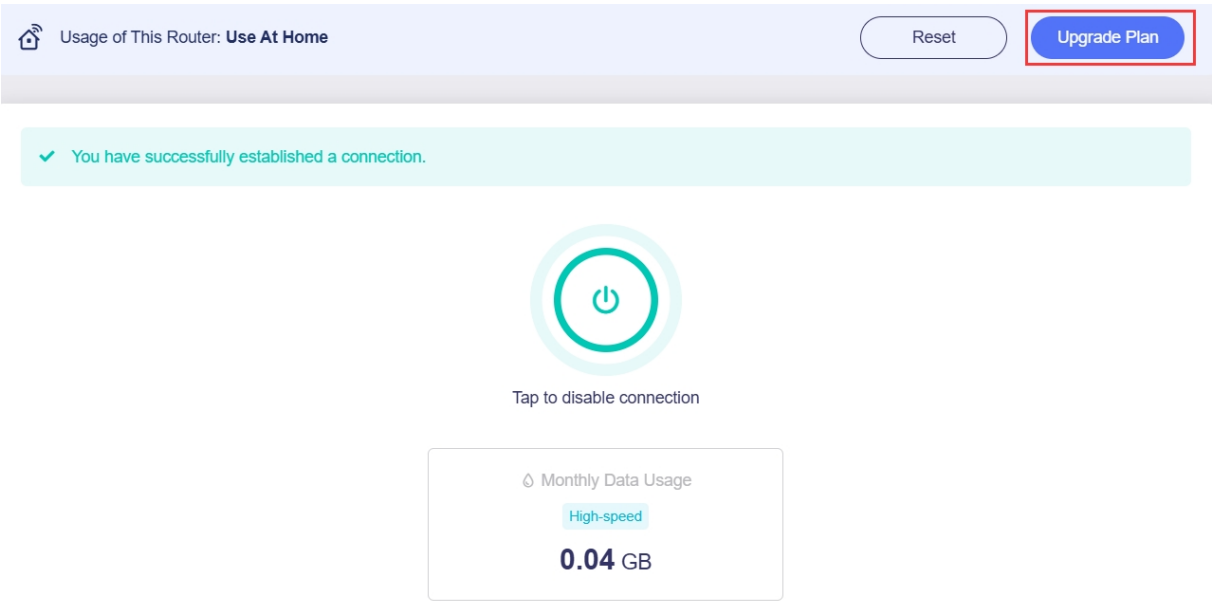


3. Rozłącz połączenie GoodPAS na Mango 2, a następnie odśwież stronę, aby ponownie sprawdzić adres IP. Pojawi się publiczny adres IP Mango 2, co oznacza, że router uzyskuje dostęp do Internetu przez swoją sieć lokalną.



7.3.3 Zmiana planu na wyższy

Każdy router GL.iNet otrzymuje **10 GB bezpłatnego transferu miesięcznie** na potrzeby sieci GoodPAS. Urządzenia w tej sieci korzystają z pakietu danych routera domowego do uzyskiwania dostępu do Internetu. W razie potrzeby możesz przejść na plan **GoodPAS+** z nielimitowanym transferem.



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

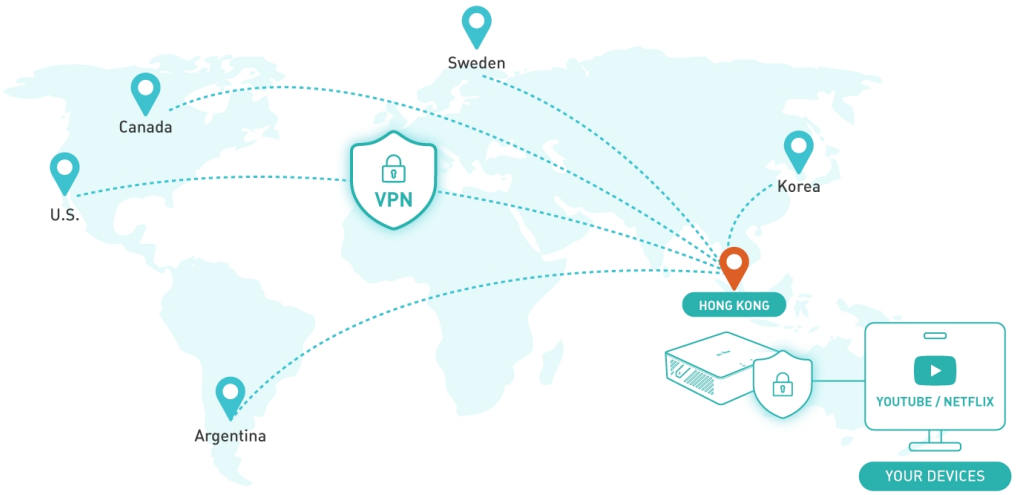
1. **Prywatność danych osobowych**

   Za pośrednictwem naszego routera usługa VPN współpracuje z wieloma urządzeniami: laptopami, telefonami i tabletami, a także konsolami do gier, telewizorami i urządzeniami do strumieniowania. Dane są chronione zarówno przy połączeniu bezprzewodowym, jak i przewodowym. Możesz również dostosować reguły VPN, aby elastycznie chronić wybrane urządzenia.



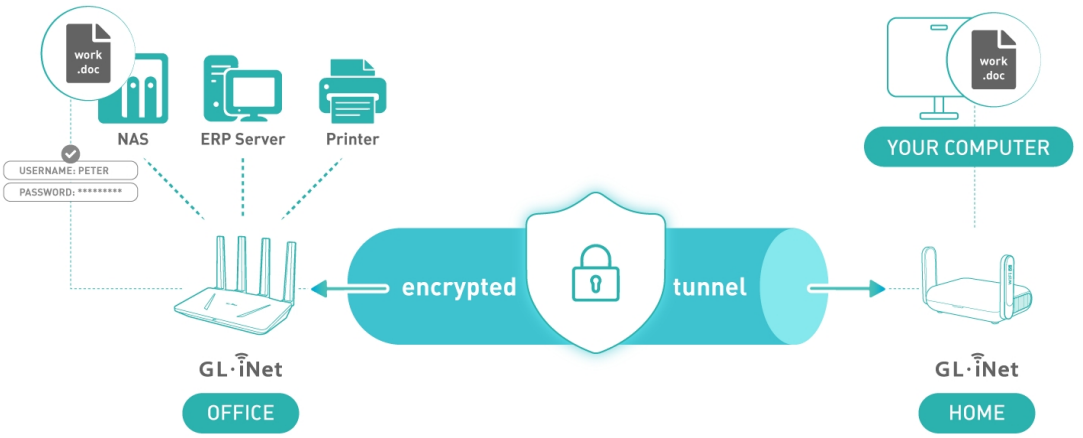
2. **Dostęp bez ograniczeń na całym świecie**

   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

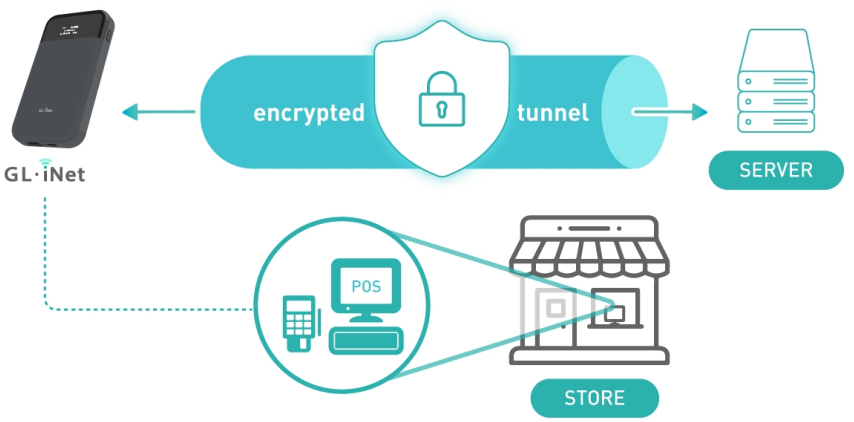
3. **Bezpieczeństwo danych małych firm**

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

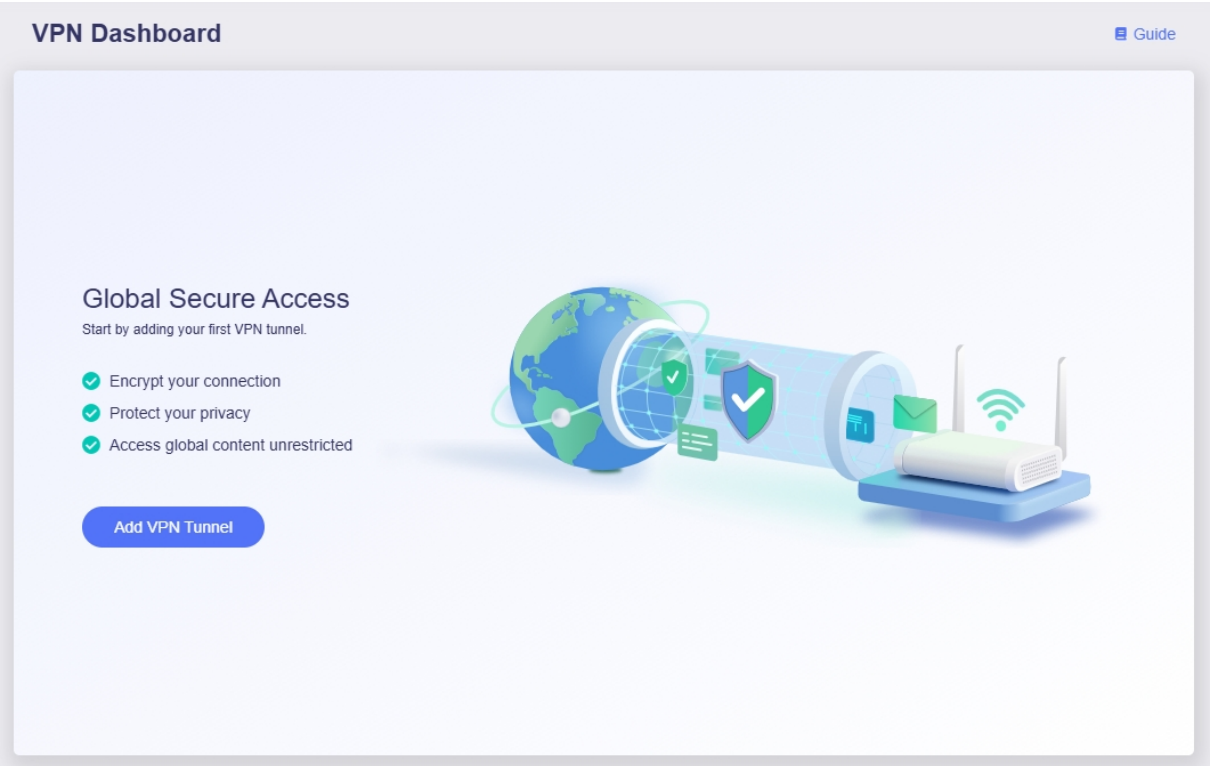
W tym rozdziale opisano zarządzanie połączeniami VPN w panelu administracyjnym.

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

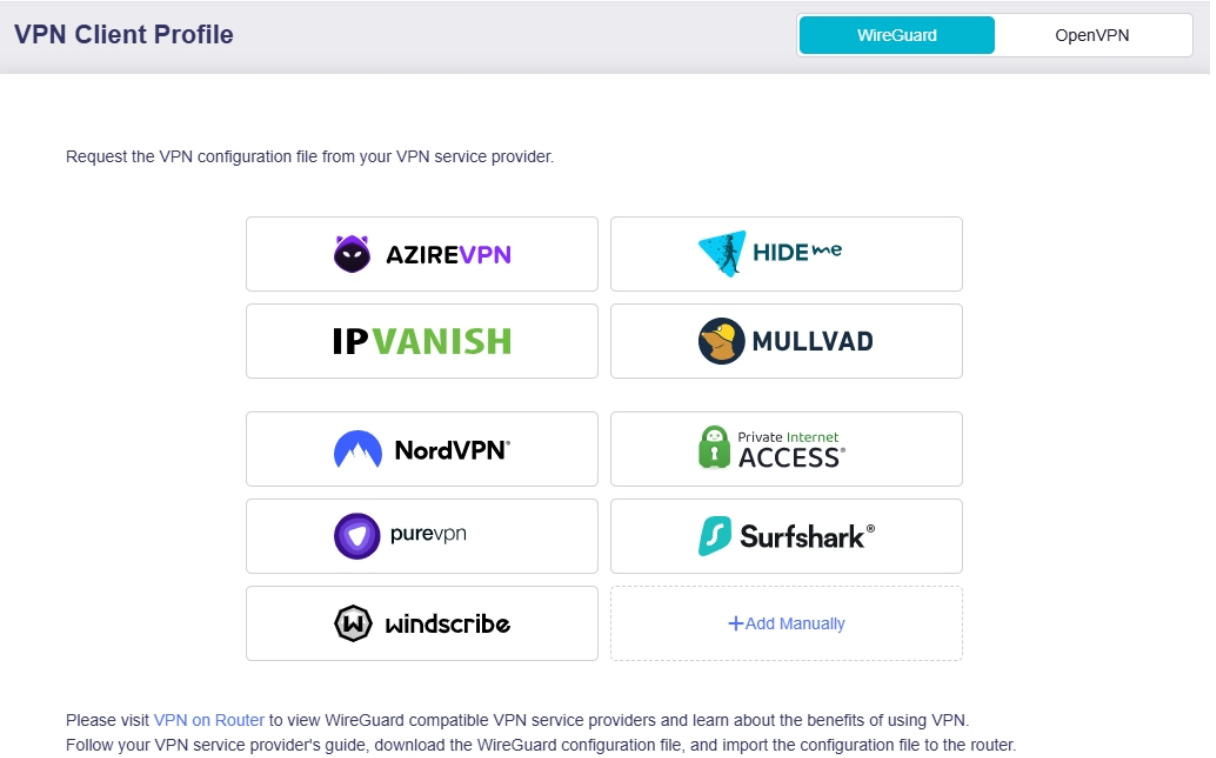
Panel VPN wyświetla szczegóły połączenia VPN, takie jak reguły routingu, połączony serwer, statystyki ruchu, wirtualny adres IP klienta i dziennik połączenia. Umożliwia też konfigurowanie ustawień zaawansowanych, takich jak Kill Switch, maskarada adresów IP i MTU.

9.1 Przesyłanie profilu VPN

Przy pierwszym otwarciu tej strony, jeśli nie utworzono jeszcze tuneli, pojawi się poniższy widok. Kliknij **Add VPN Tunnel,** aby rozpocząć.



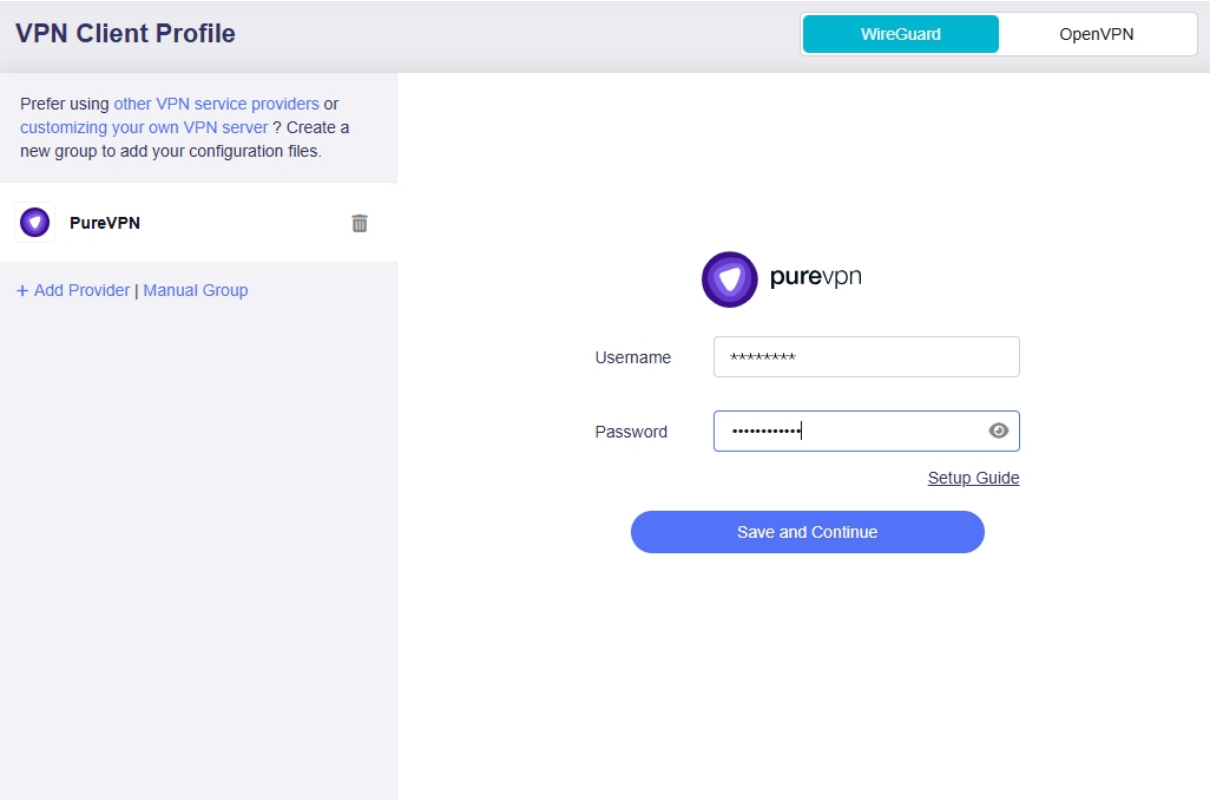
Nastąpi przekierowanie na **stronę VPN Client** Profile. Wybierz dostawcę VPN i zaloguj się.



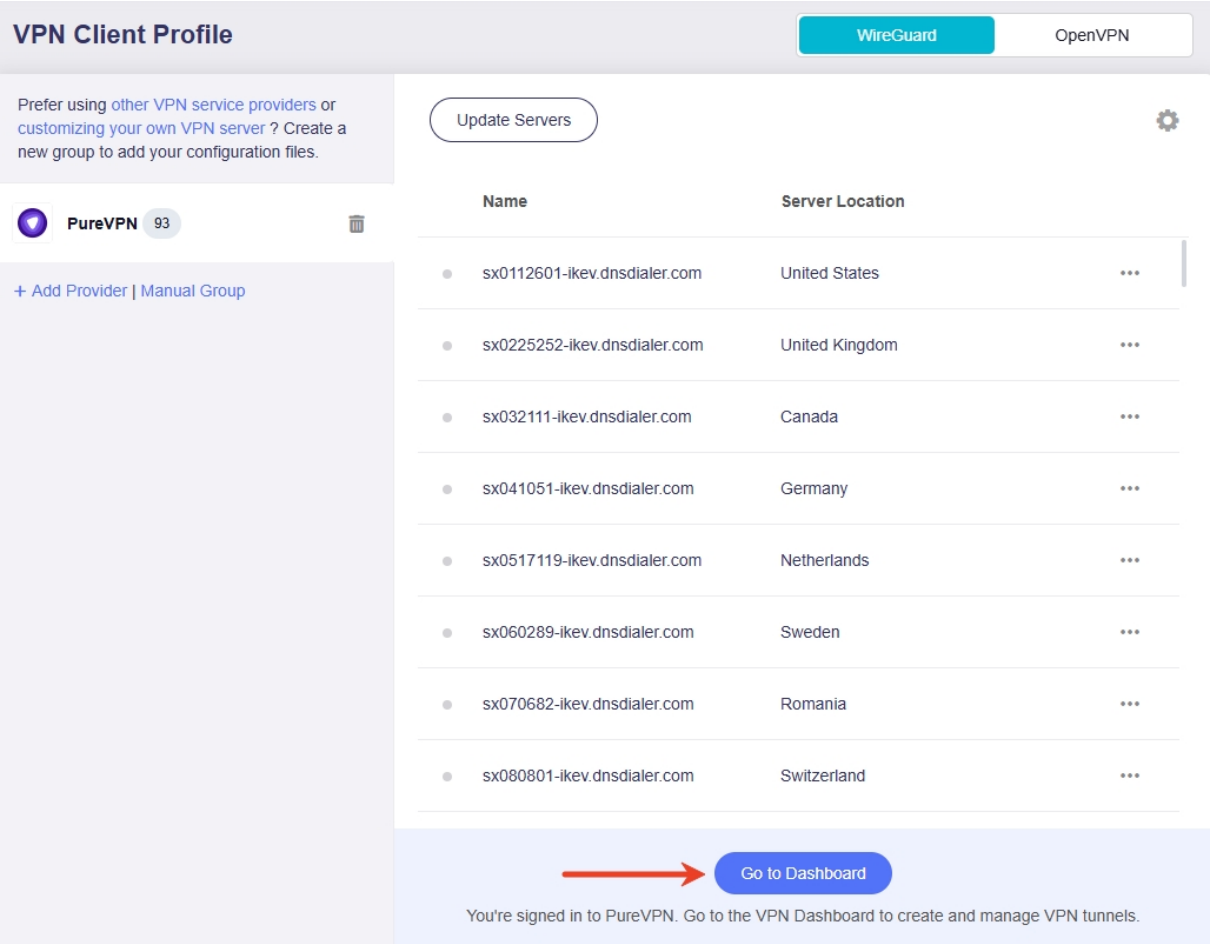
Wskazówki:

1. Wymienieni dostawcy VPN są zintegrowani z internetowym panelem administracyjnym routera GL.iNet. Jeśli masz aktywną subskrypcję, wystarczy podać dane logowania, aby natychmiast się zalogować i pobrać pliki konfiguracyjne połączeń VPN.
2. Jeśli korzystasz z subskrypcji innego dostawcy VPN lub chcesz przesłać własną konfigurację VPN, kliknij **Add** Manually i prześlij konfigurację.

Jako przykład posłuży PureVPN. Kliknij PureVPN i zaloguj się przy użyciu prawidłowych danych.



Pojawi się lista profili VPN, jak pokazano poniżej. **Kliknij Go to** Dashboard u dołu strony, aby przejść do panelu VPN i skonfigurować tunel oraz zasady VPN.



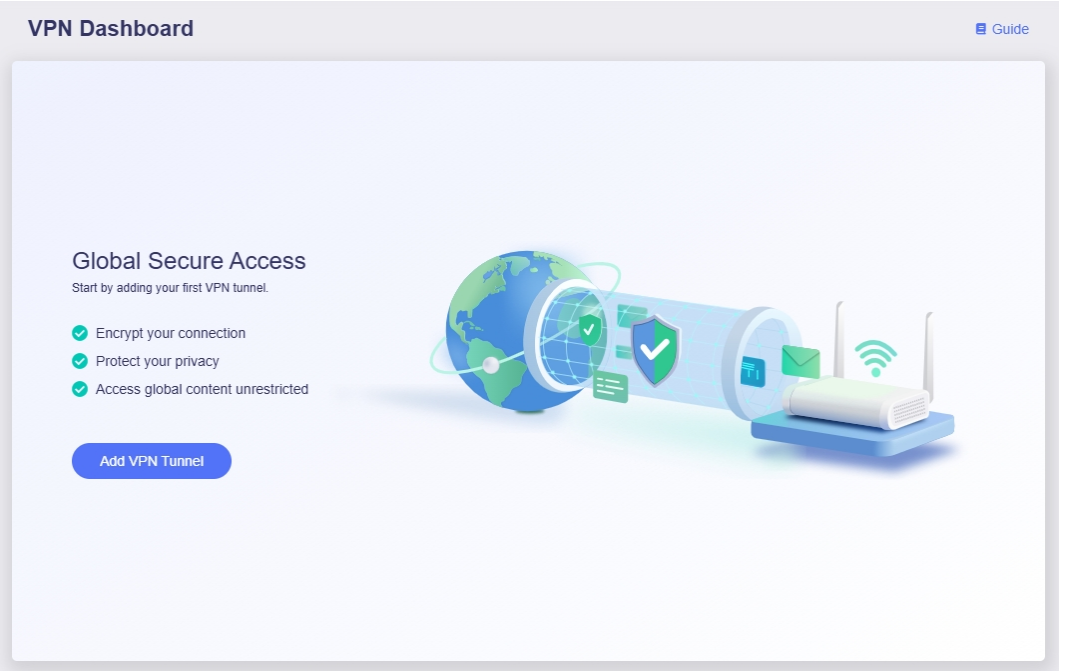
Wskazówka: w przypadku niektórych dostawców VPN przed wyświetleniem listy profili trzeba wybrać protokół VPN lub preferowane serwery/miasta.

9.2 Dodawanie tunelu VPN

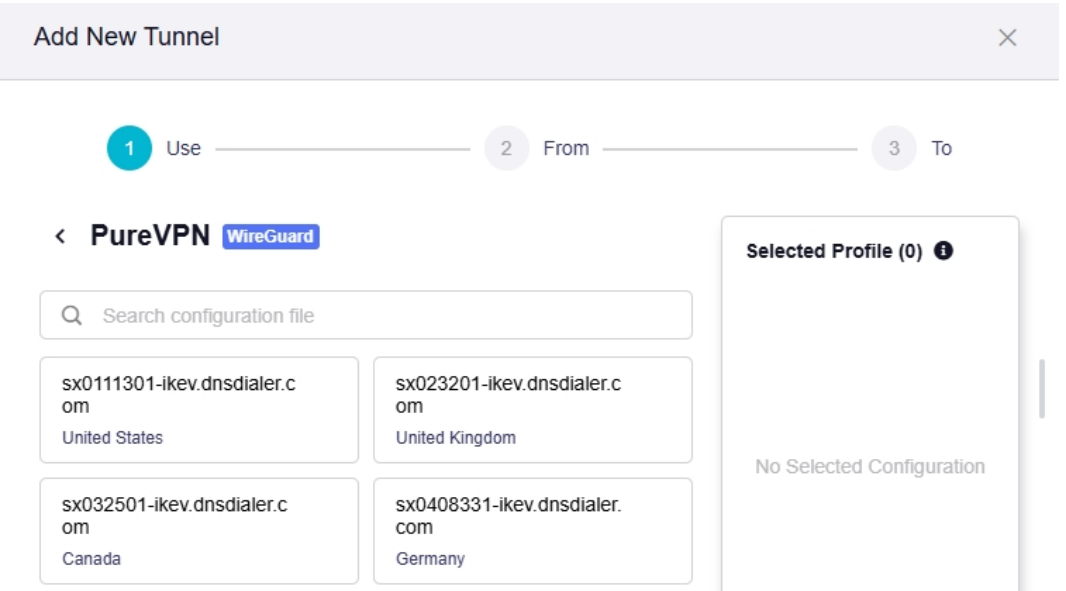
9.2.1 Czynności ogólne

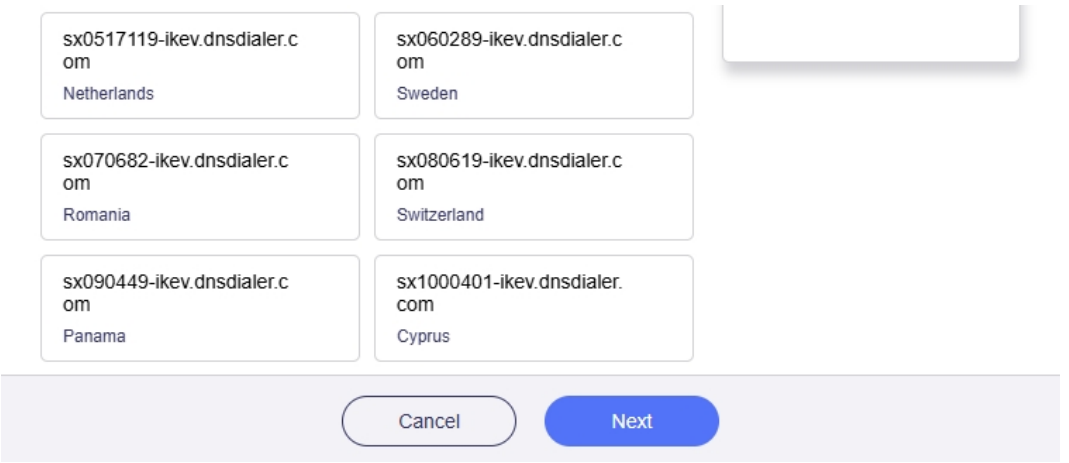
Wykonaj poniższe czynności, aby dodać tunel VPN i skonfigurować zasady VPN. W razie potrzeby zobacz Przykłady konfiguracji.

1. W panelu VPN kliknij Add VPN **Tunnel. Po prawej** stronie pojawi się kreator konfiguracji.



2. Wybierz co najmniej jeden profil i w razie potrzeby dostosuj priorytety po prawej stronie, a następnie kliknij **Next**.





Uwaga: jeśli wybrano wiele profili, tunel będzie próbował nawiązać połączenie za pomocą kolejnych profili według priorytetu, aż połączenie się powiedzie. Jeśli żaden profil w tunelu nie nawiąże połączenia, system zdecyduje, czy przełączyć się na lokalną sieć routera (WAN), na podstawie stanu Kill Switch w ustawieniach Opcje tunelu i Cały pozostały ruch.

3. Wybierz źródło klientów, a następnie **kliknij** Next. Dostępne są cztery opcje:
   - **All Clients**: ruch ze wszystkich urządzeń będzie pasował do tej reguły.
   - **Specified Connection** Types: ruch z określonych typów połączeń (np. podsieci LAN, Drop-in Gateway, Guest Network) będzie pasował do tej reguły.
   - **Specified Devices:** ruch z określonych urządzeń (identyfikowanych na podstawie adresu MAC) będzie pasował do tej reguły.
   - **Exclude Specified Devices:** ruch z określonych urządzeń (identyfikowanych na podstawie adresu MAC) nie będzie pasował do tej reguły.
4. Wybierz miejsce docelowe, a następnie **kliknij** Apply. Dostępne są trzy opcje:
   - **All Targets:** ruch pasujący do tej reguły będzie kierowany do wszystkich celów.
   - **Specified Domain / IP** List: ruch pasujący do tej reguły będzie kierowany do określonych domen lub adresów IP. Należy wprowadzić je ręcznie.
   - **Exclude specified Domain / IP** List: ruch pasujący do tej reguły nie będzie kierowany do określonych domen lub adresów IP. Należy wprowadzić je ręcznie.
5. Tunel VPN został dodany. Nastąpi przekierowanie do panelu VPN. W razie potrzeby dodaj **kolejne tunele. Ze** względów bezpieczeństwa przed włączeniem tunelu VPN sprawdź stan Kill Switch w sekcjach Cały pozostały ruch i Opcje tunelu.

9.2.2 Przykłady konfiguracji

Poniżej przedstawiono dwa typowe przykłady konfiguracji zasad VPN wraz z instrukcjami krok po kroku.

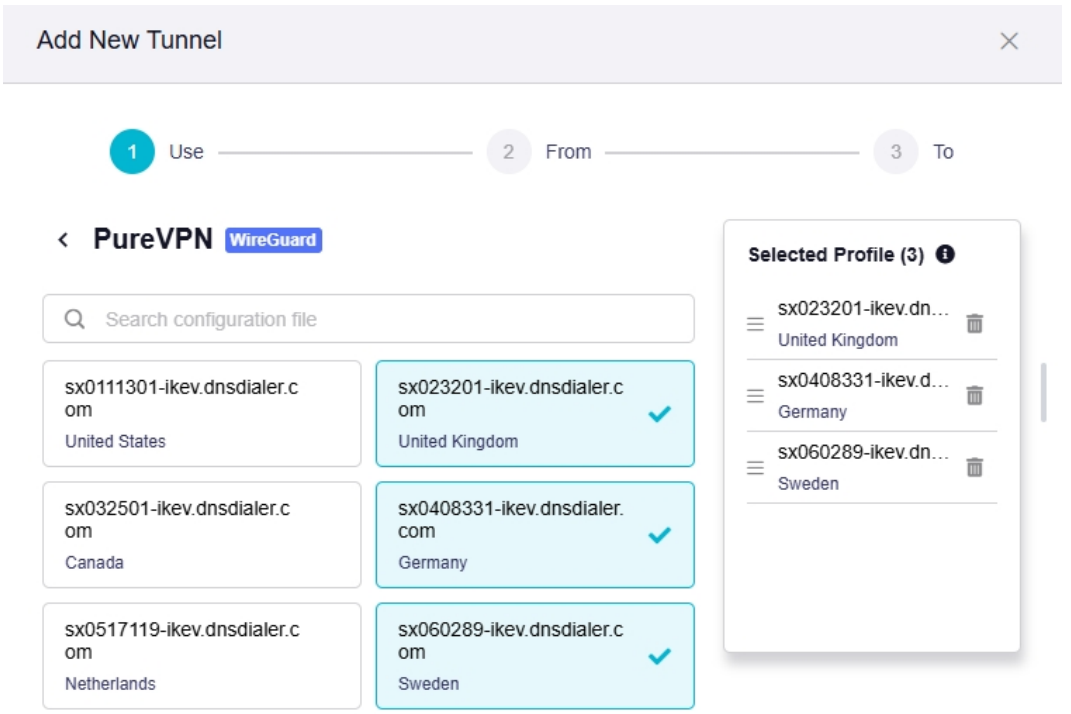
Przykład 1: kierowanie przez VPN tylko określonych urządzeń

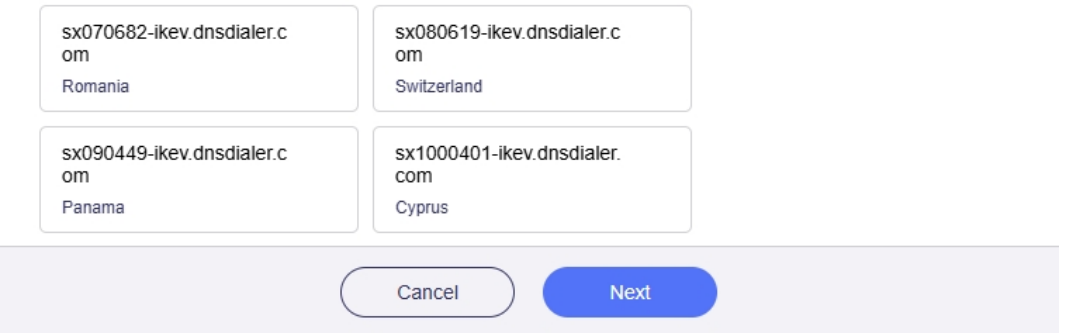
Wymagania:

1. Tylko określone urządzenia podłączone do tego routera łączą się z Internetem przez VPN. Wszystkie pozostałe urządzenia korzystają z lokalnego łącza WAN.
2. Wybrane urządzenia muszą korzystać wyłącznie z połączenia VPN. Jeśli VPN niespodziewanie się rozłączy, dostęp tych urządzeń do Internetu zostanie zablokowany, aby zapobiec wyciekom DNS i śledzeniu adresu IP.

Czynności konfiguracyjne:

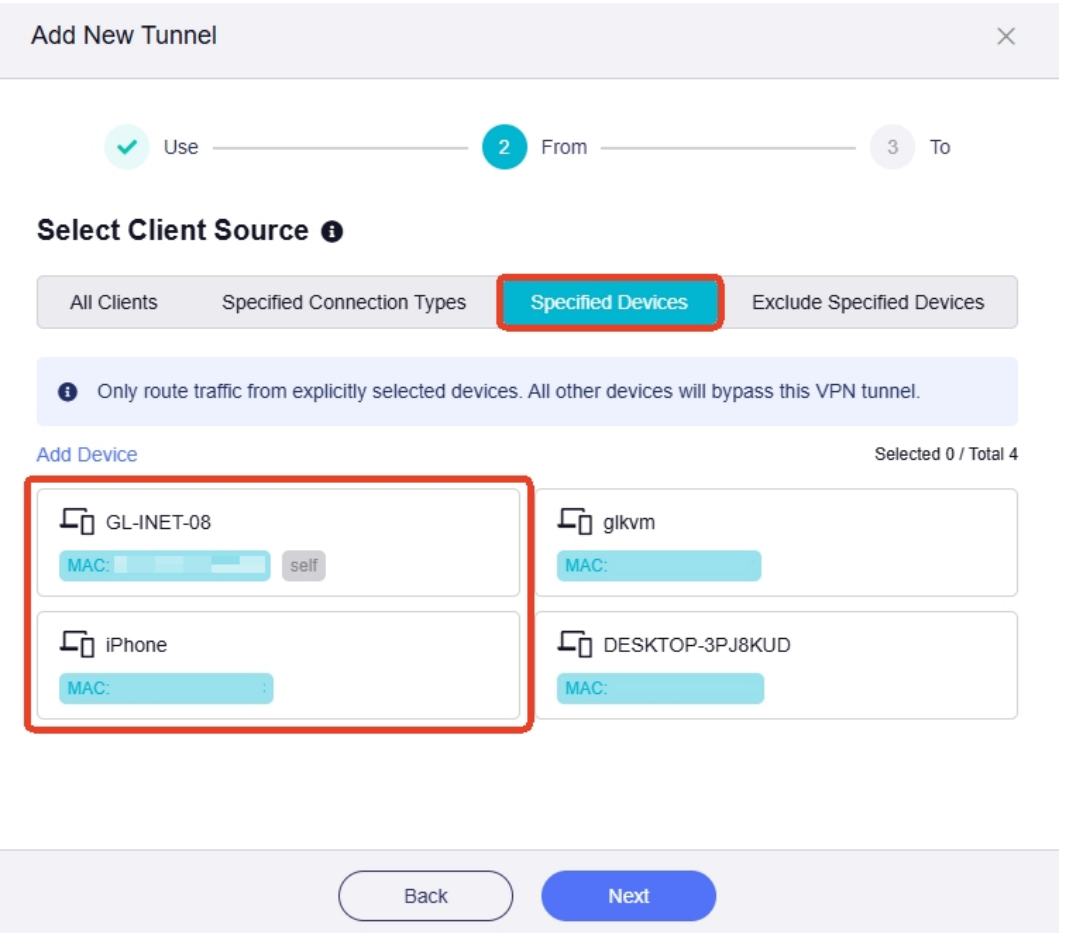
1. Wybierz profil VPN.
   Jeśli zalogowano się już przy użyciu danych zintegrowanej usługi VPN lub przesłano plik konfiguracyjny, dostępne profile zostaną wymienione tutaj. W przeciwnym razie przejdź do **VPN Client Profile**, aby się zalogować lub ręcznie przesłać plik konfiguracyjny.
   Jako przykład posłuży PureVPN. Wybierz co najmniej jeden profil i w razie potrzeby dostosuj priorytety po prawej stronie.





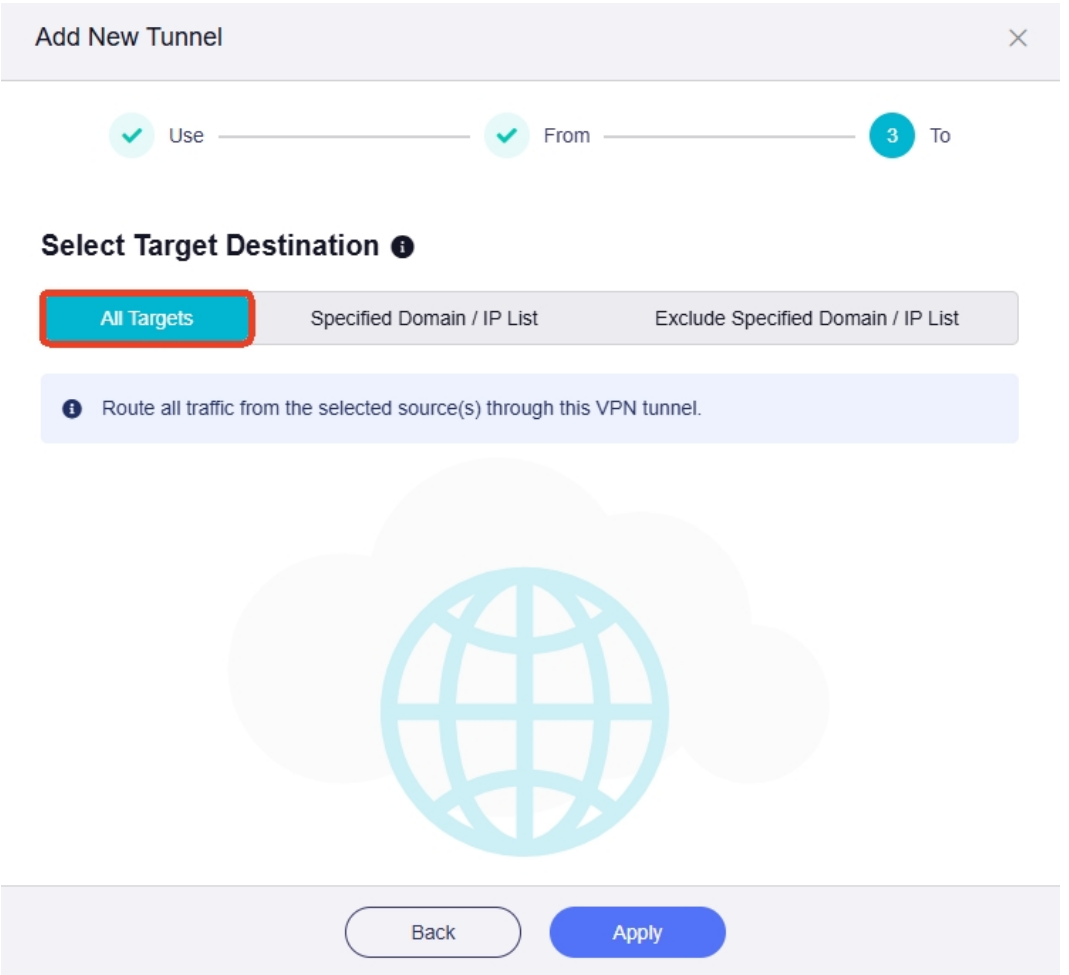
2. Wybierz źródło klientów.

   Kliknij kartę **Specified Devices**, wybierz urządzenia, które mają korzystać z VPN, a następnie kliknij **Next**.

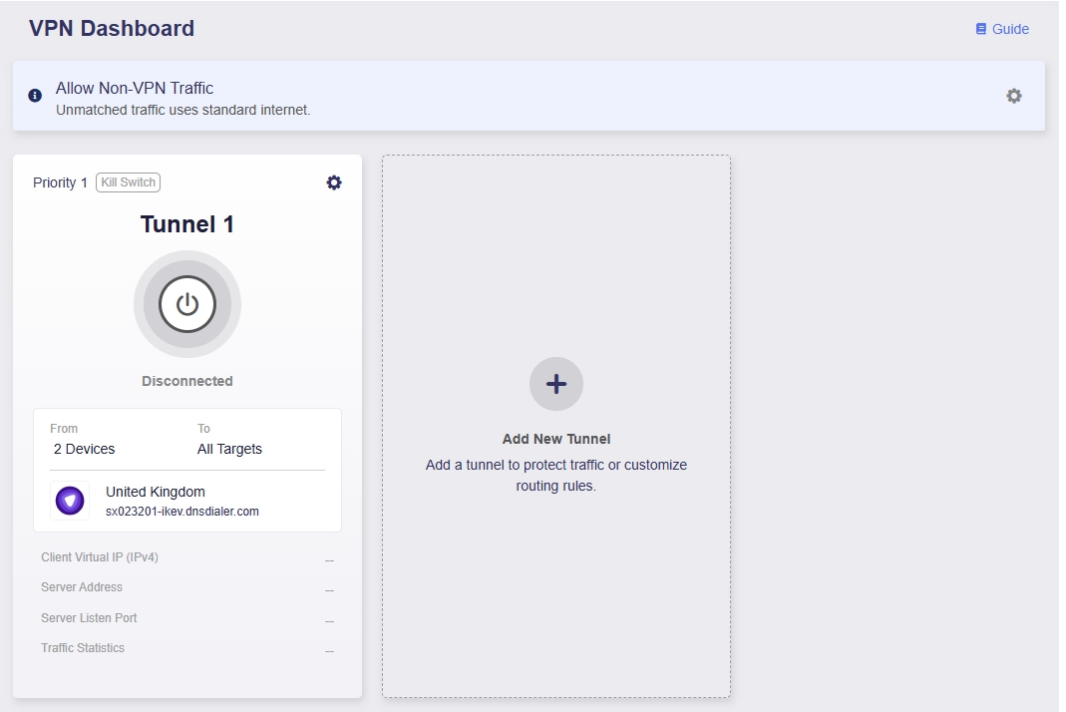


3. Wybierz miejsce docelowe.

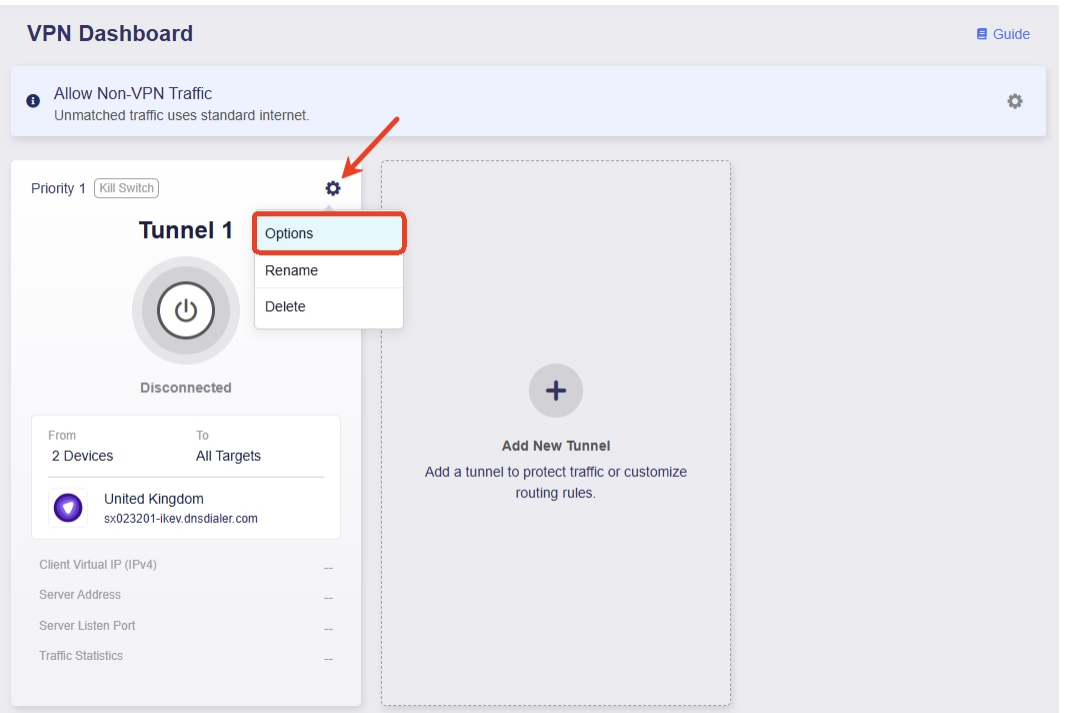
   Kliknij kartę **All Targets**, ustaw ją jako miejsce docelowe ruchu, a następnie kliknij **Apply**.

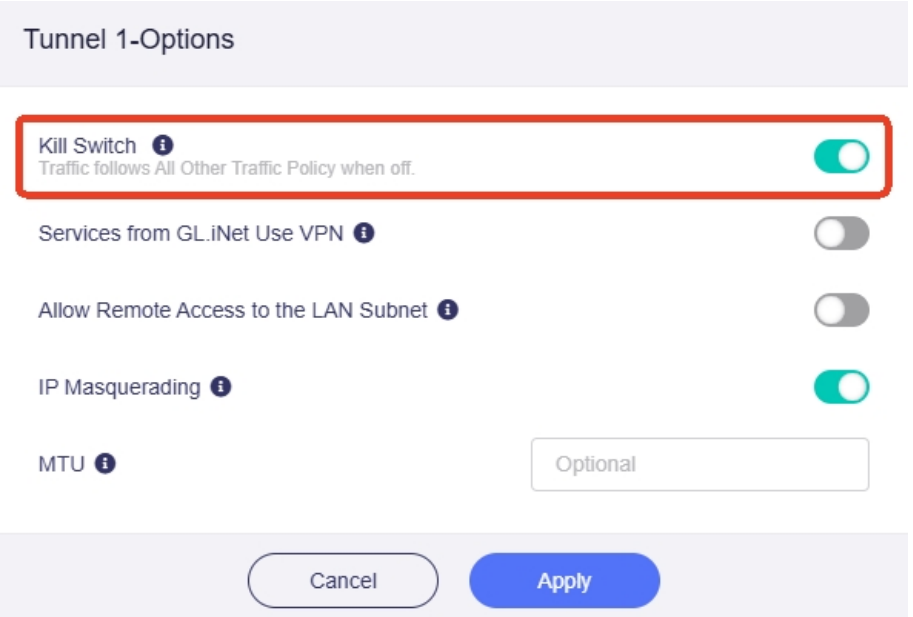


4. Nastąpi przekierowanie do panelu VPN. Tunel VPN został dodany, jak pokazano poniżej.

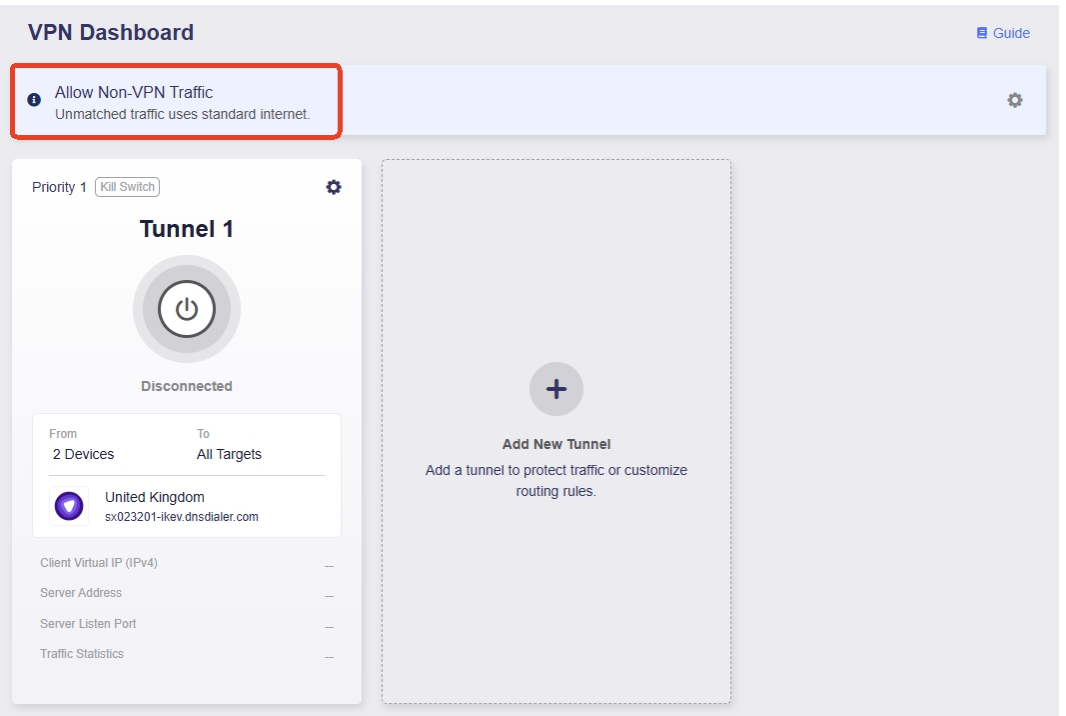


5. Upewnij się, że **Kill Switch** dla tego tunelu jest włączony. Jeśli VPN niespodziewanie się rozłączy, dostęp do Internetu dla ruchu pasującego do tunelu zostanie zablokowany, aby zapobiec wyciekom DNS i śledzeniu adresu IP.

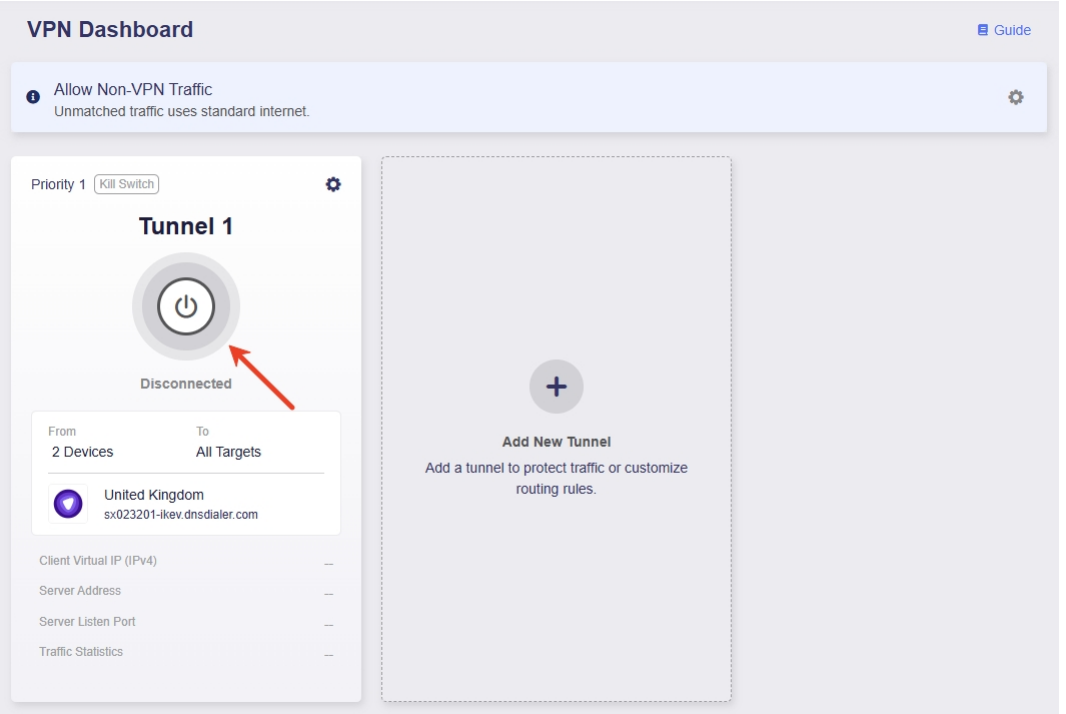




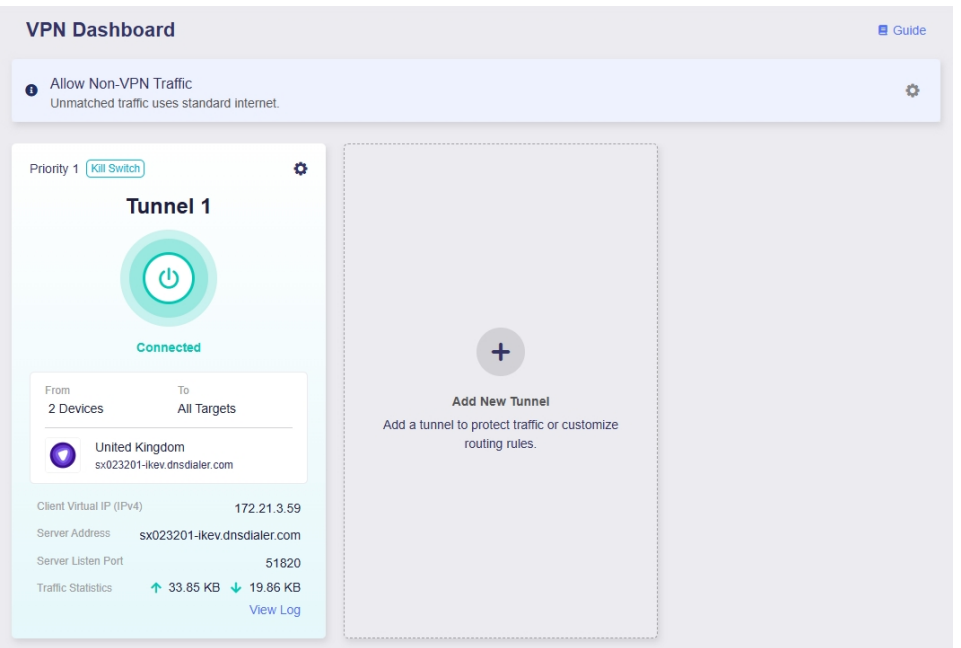
6. Upewnij się, że **Allow Non-VPN Traffic** jest włączone. Domyślnie ta opcja jest włączona, aby ruch niepasujący do tunelu VPN mógł nadal korzystać z Internetu przez lokalne łącze WAN.



7. Kliknij środkowy przycisk, aby aktywować ten tunel.



8. Po nawiązaniu połączenia strona wyświetli szczegóły połączenia VPN, w tym zasady VPN, statystyki ruchu, adres serwera, port nasłuchiwania i wirtualny adres IP.



Teraz tylko dwa określone urządzenia łączą się z Internetem przez VPN. Jeśli VPN niespodziewanie się rozłączy, dostęp tych urządzeń do Internetu zostanie zablokowany, aby zapobiec wyciekom DNS i śledzeniu adresu IP. Pozostałe urządzenia będą korzystać z lokalnego łącza WAN.

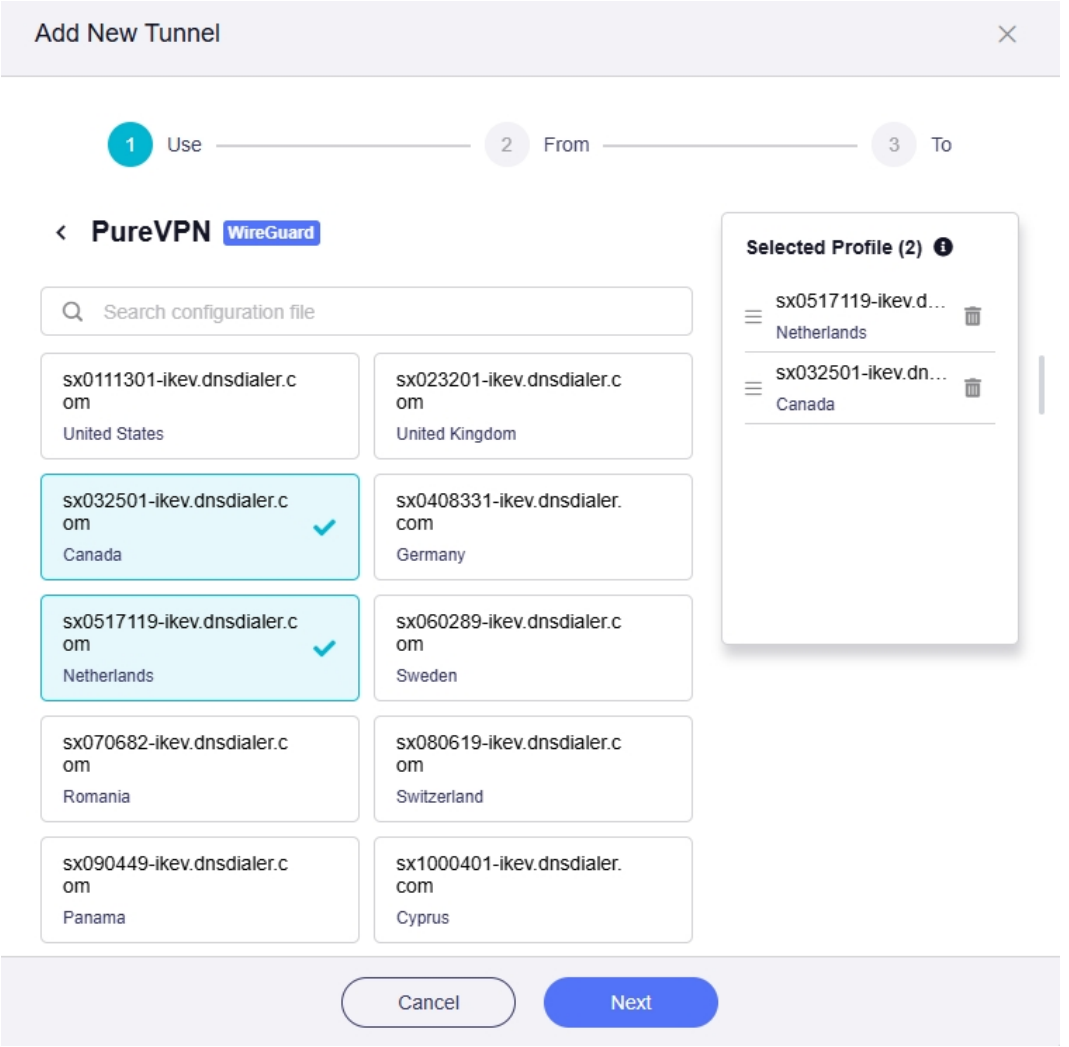
Przykład 2: kierowanie wszystkich urządzeń przez VPN 1 dla określonych witryn, a całego pozostałego ruchu przez VPN 2

Wymagania:

1. Wszystkie urządzenia korzystają z VPN Tunnel 1 podczas odwiedzania domen określonych serwisów społecznościowych i streamingowych, a z VPN Tunnel 2 przy pozostałym dostępie do Internetu.
2. Jeśli tunele VPN niespodziewanie się rozłączą, dostęp wszystkich urządzeń do Internetu zostanie zablokowany, aby zapobiec wyciekom DNS i śledzeniu adresu IP.

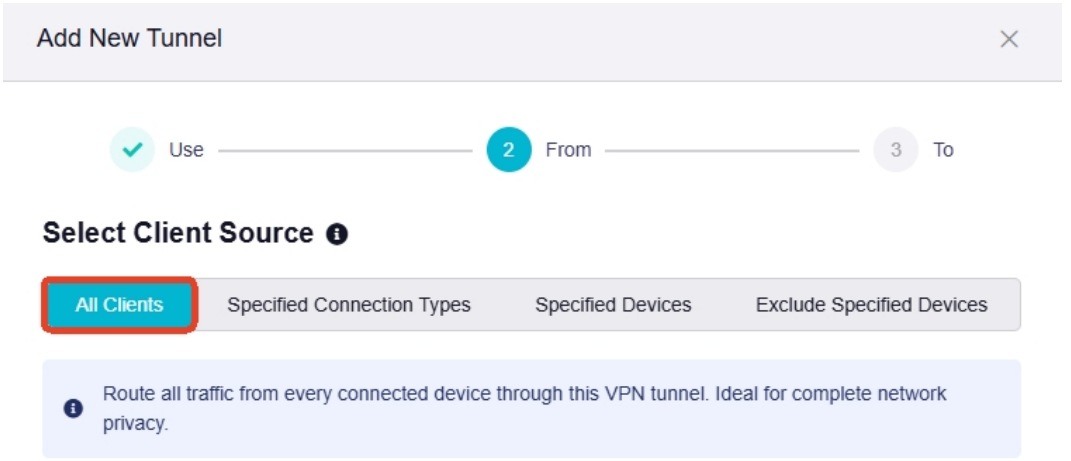
Czynności konfiguracyjne:

1. Wybierz profil VPN dla tunelu 1.
   Jeśli zalogowano się już przy użyciu danych zintegrowanej usługi VPN lub przesłano plik konfiguracyjny, dostępne profile zostaną wymienione tutaj. W przeciwnym razie przejdź do **VPN Client Profile**, aby się zalogować lub ręcznie przesłać plik konfiguracyjny.
   Jako przykład posłuży PureVPN. Wybierz co najmniej jeden profil i w razie potrzeby dostosuj priorytety po prawej stronie, a następnie kliknij **Next**.

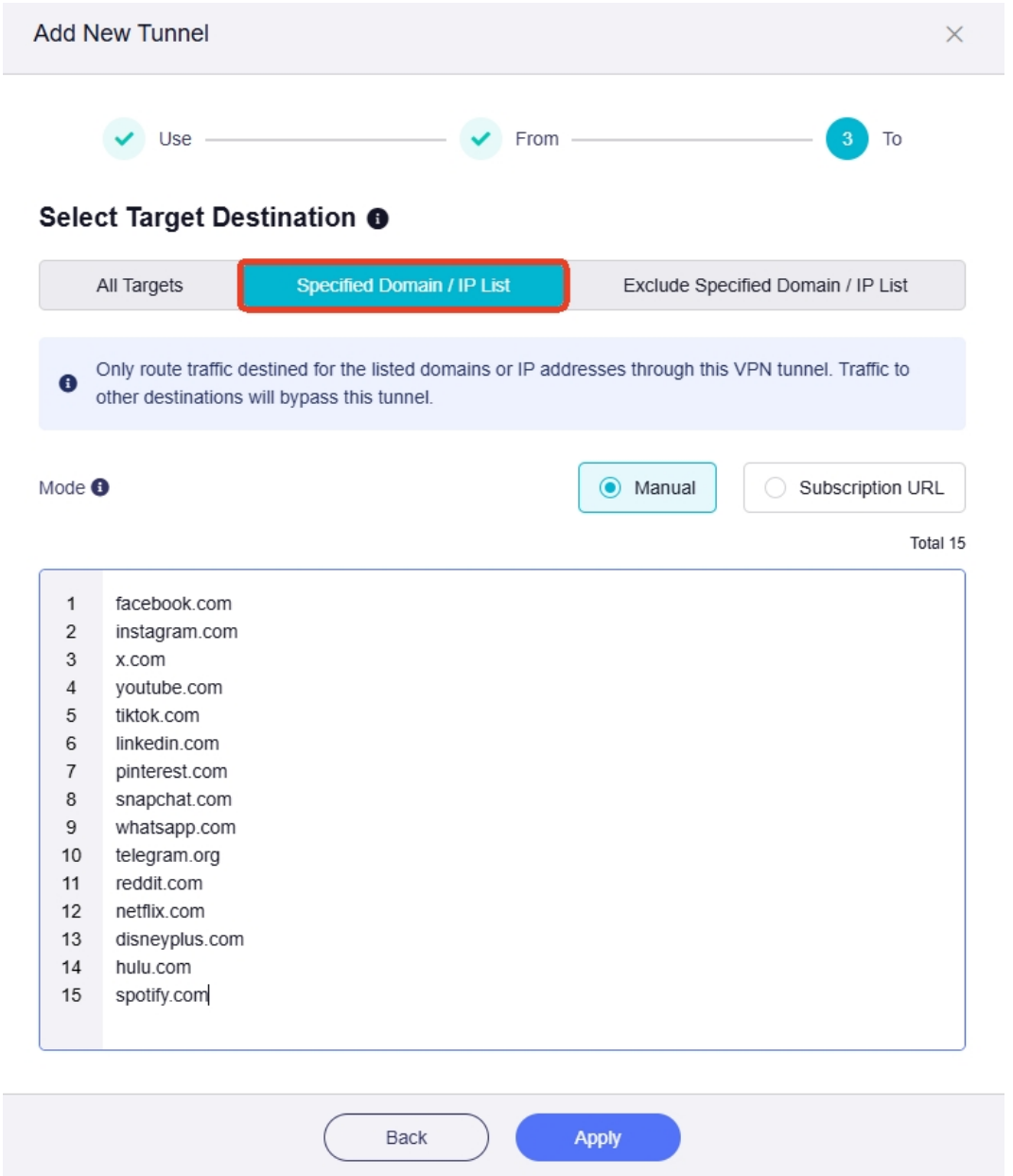


2. Wybierz źródło klientów.

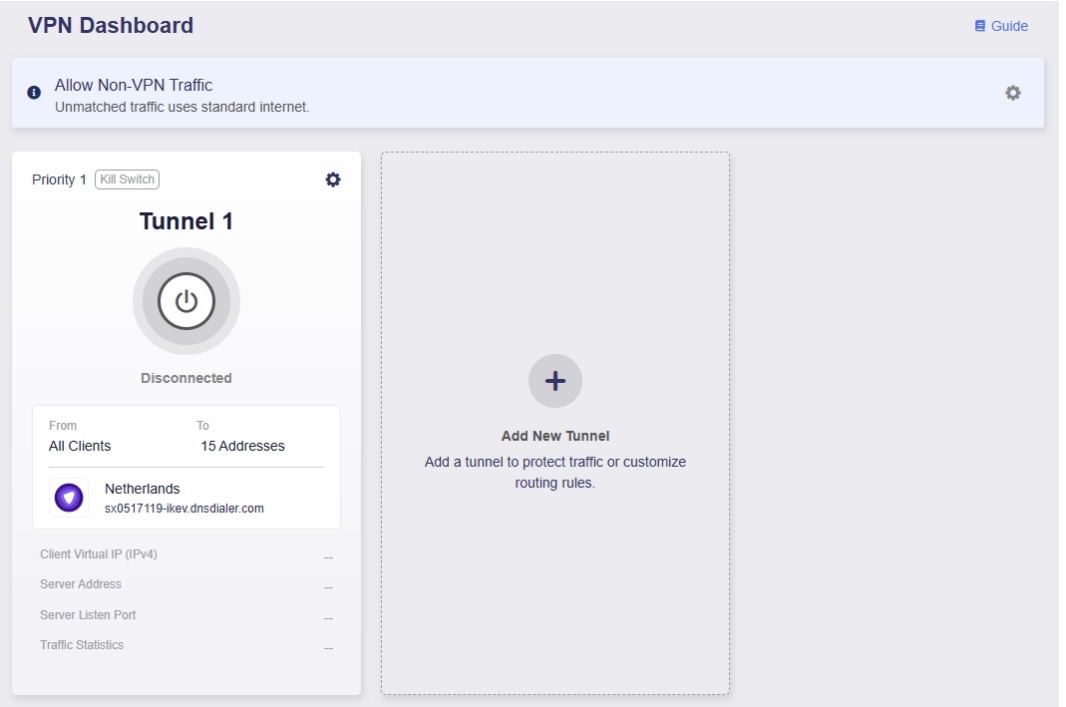
   Kliknij kartę **All Clients**, ustaw ją jako źródło klientów dla tunelu 1, a następnie kliknij **Next**.



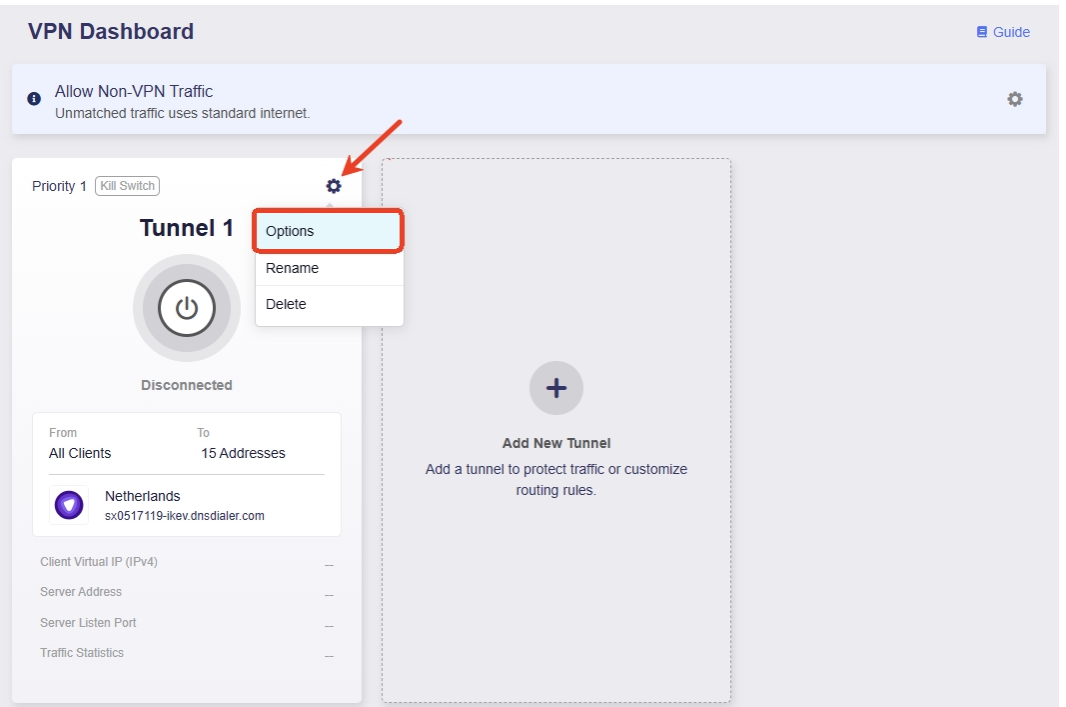
3. Wybierz miejsce docelowe.
   Kliknij kartę **Specified Domain / IP List**, wprowadź domeny popularnych serwisów społecznościowych i streamingowych, jak pokazano poniżej, a następnie kliknij **Apply**.

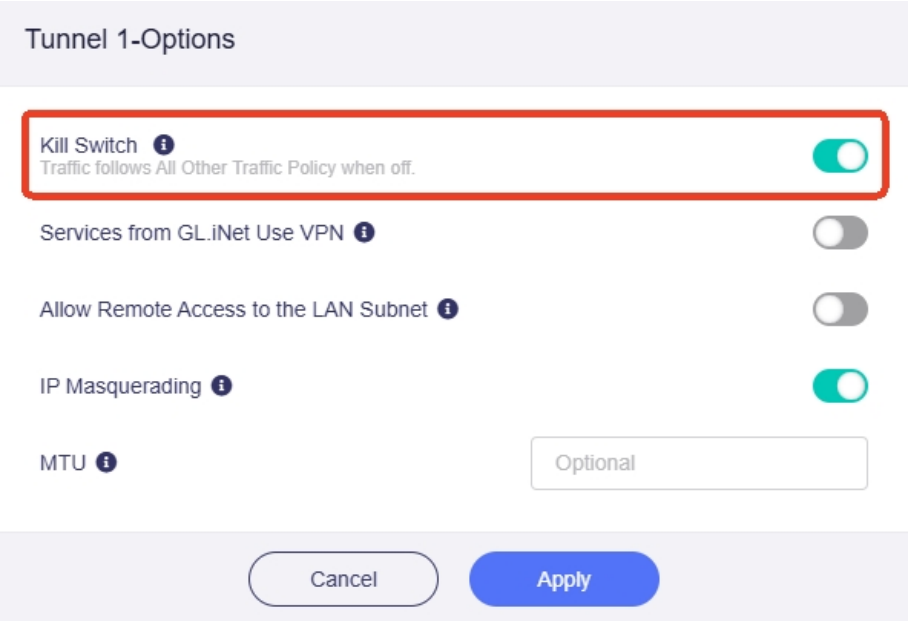


4. Nastąpi przekierowanie do panelu VPN. Tunel VPN 1 został dodany.

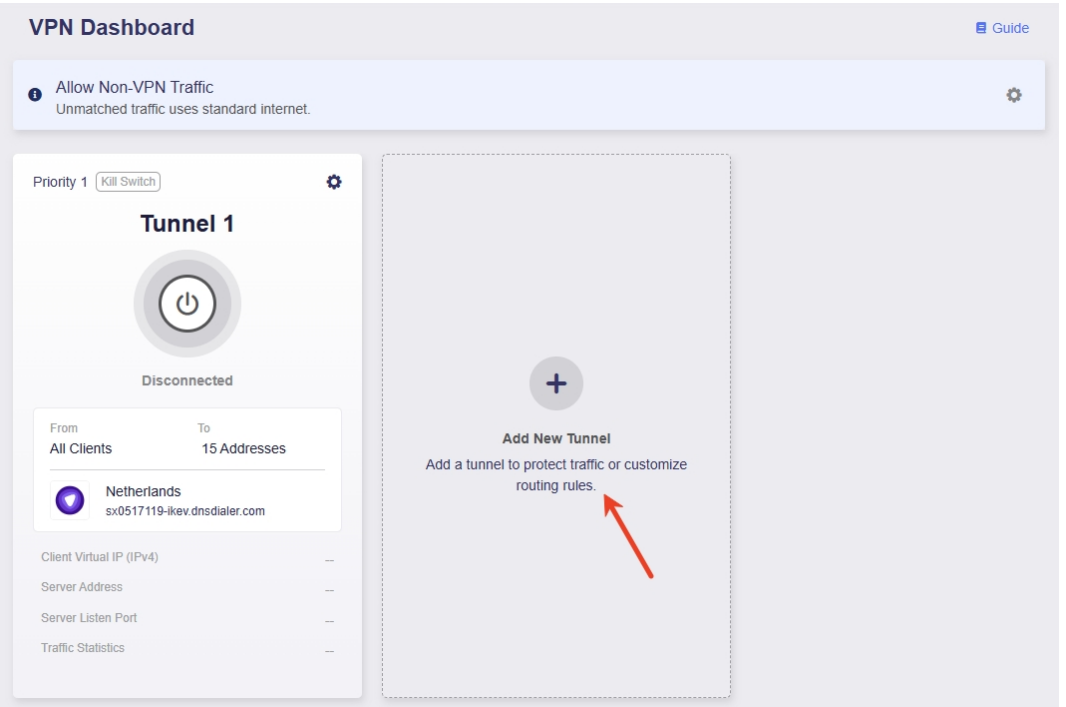


5. Upewnij się, że **Kill Switch** dla tunelu 1 jest włączony. Jeśli VPN niespodziewanie się rozłączy, dostęp do Internetu dla ruchu pasującego do tunelu zostanie zablokowany, aby zapobiec wyciekom DNS i śledzeniu adresu IP.





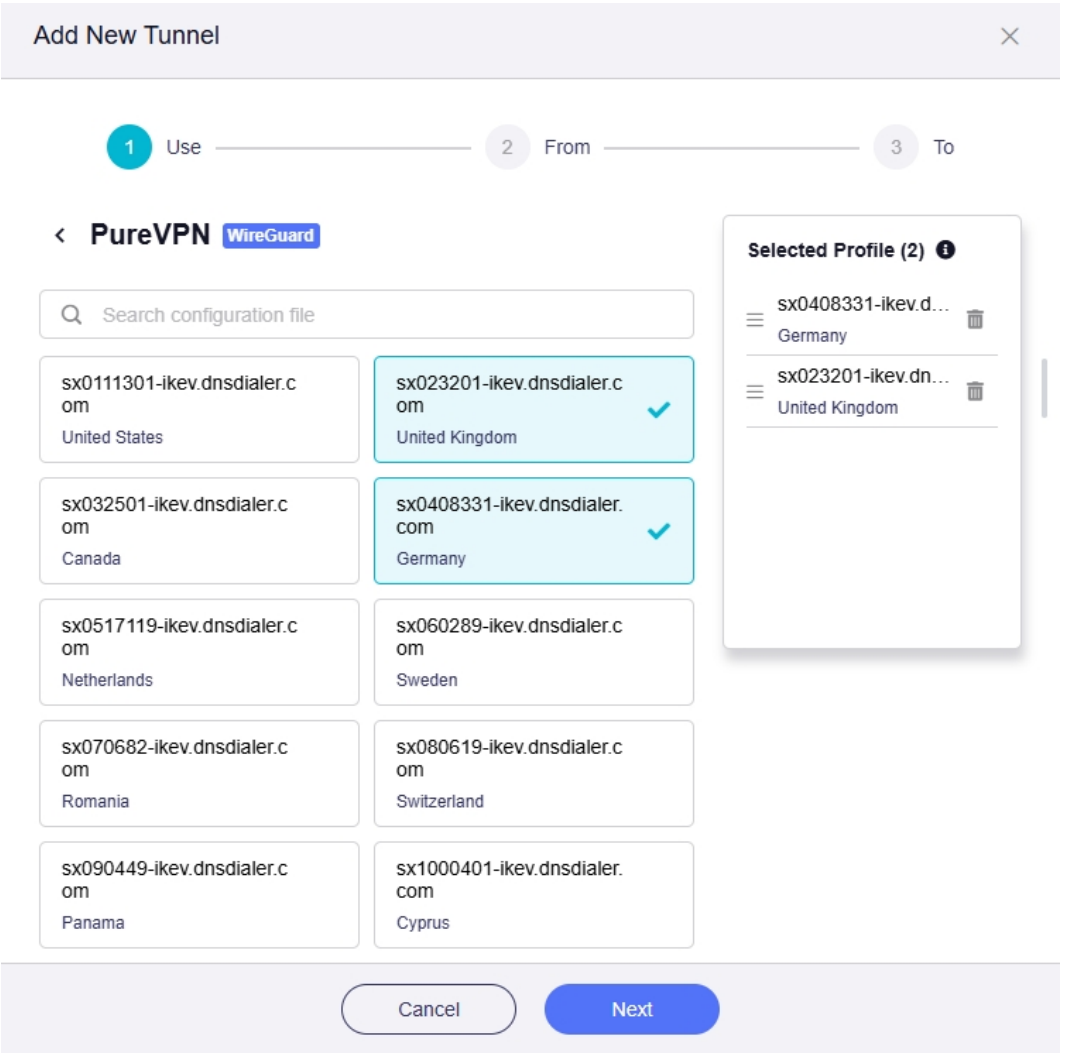
6. Kliknij **Add New Tunnel**, aby dodać tunel 2.



7. Wybierz profil VPN dla tunelu 2.

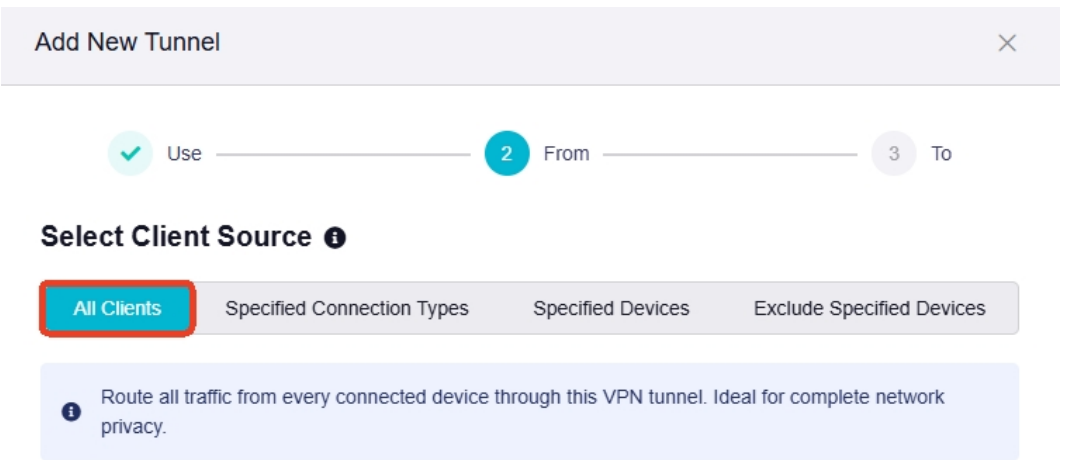
   Wybierz co najmniej jeden profil i w razie potrzeby dostosuj priorytety po prawej stronie.

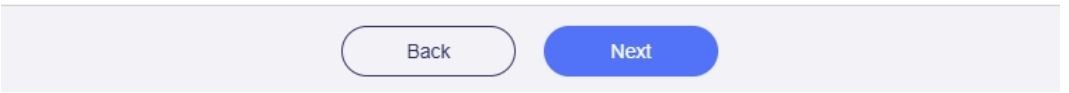
   Następnie kliknij **Next**.



8. Wybierz źródło klientów.

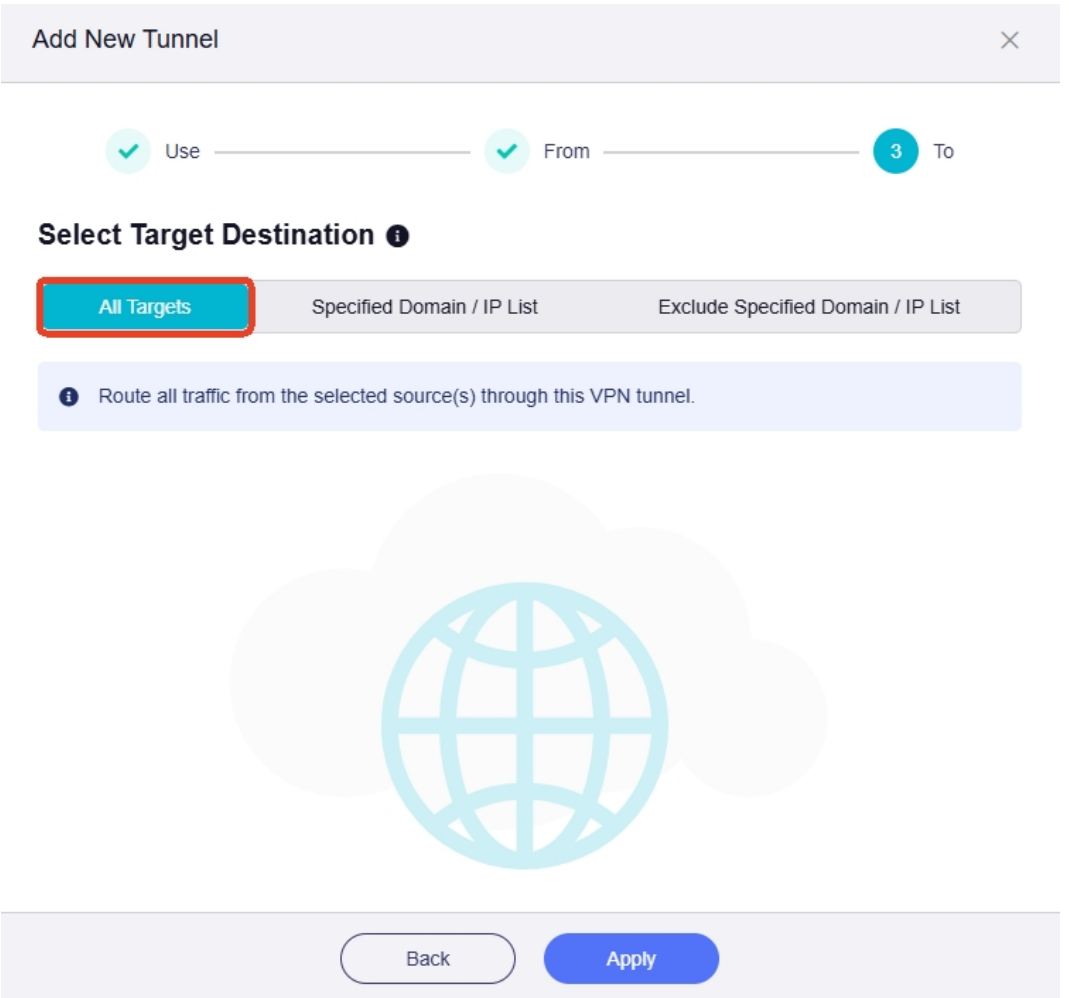
Kliknij kartę **All Clients**, ustaw ją jako źródło klientów dla tunelu 2, a następnie kliknij **Next**.



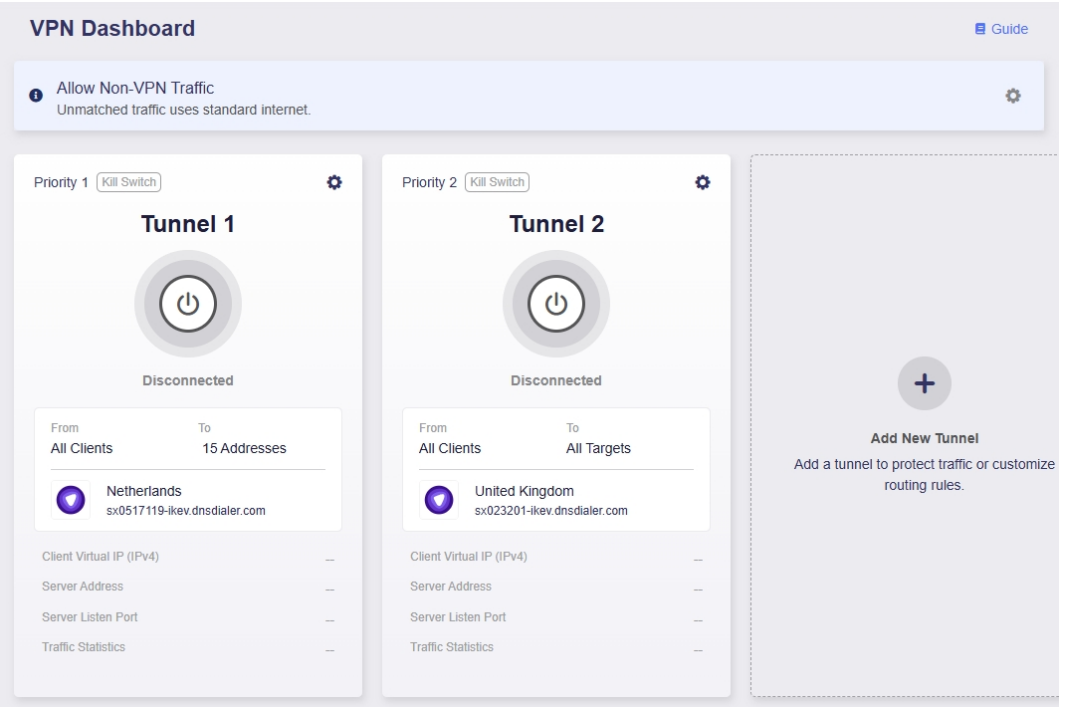


9. Wybierz miejsce docelowe.

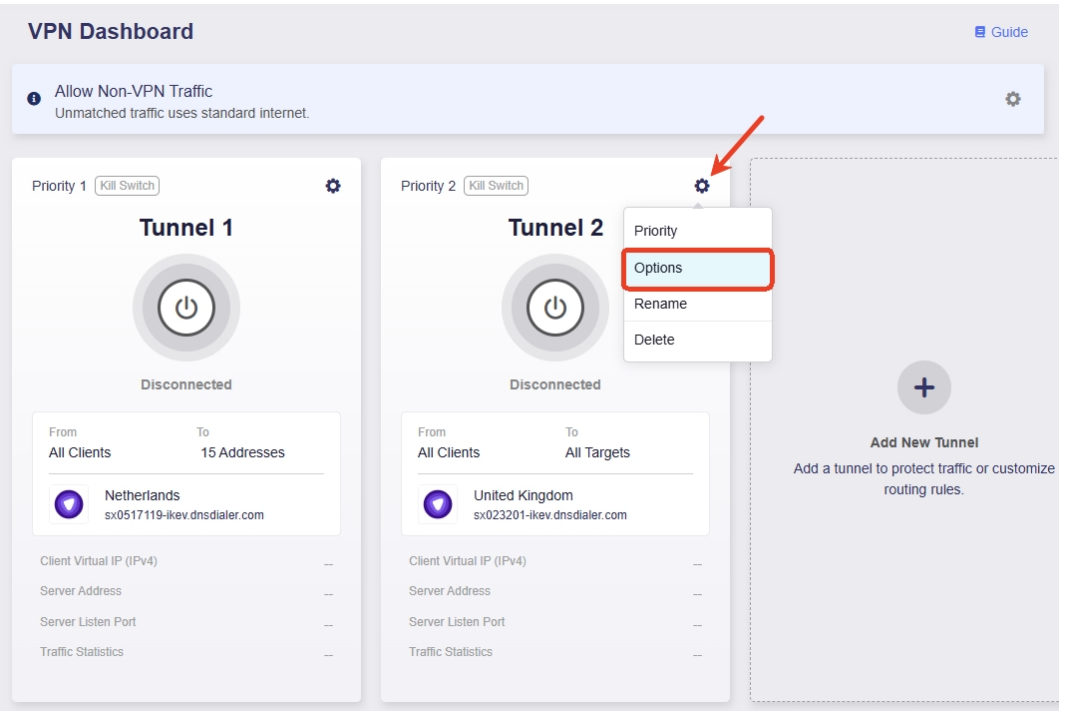
Kliknij kartę **All Targets**, ustaw ją jako miejsce docelowe ruchu dla tunelu 2, a następnie kliknij **Apply**.

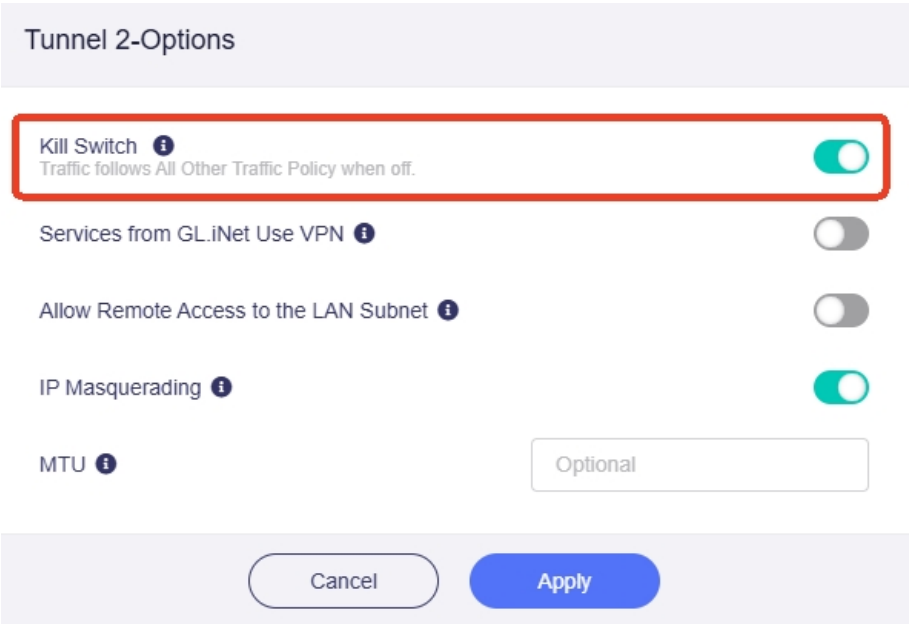


10. Nastąpi przekierowanie do panelu VPN. Tunel VPN 2 został dodany.

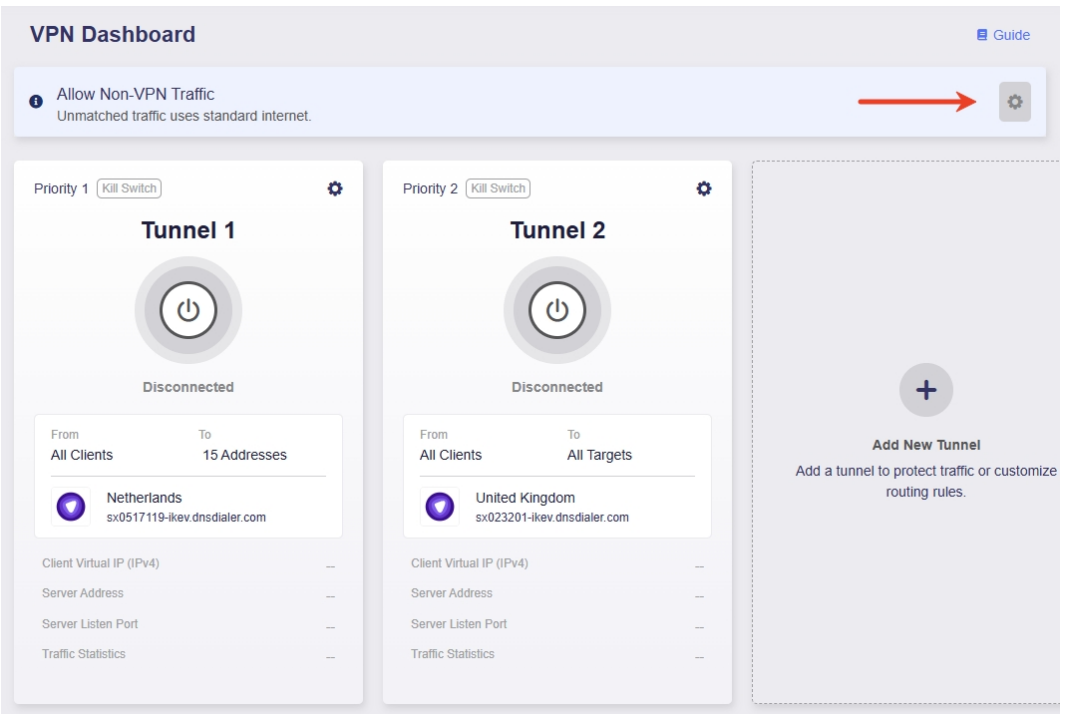


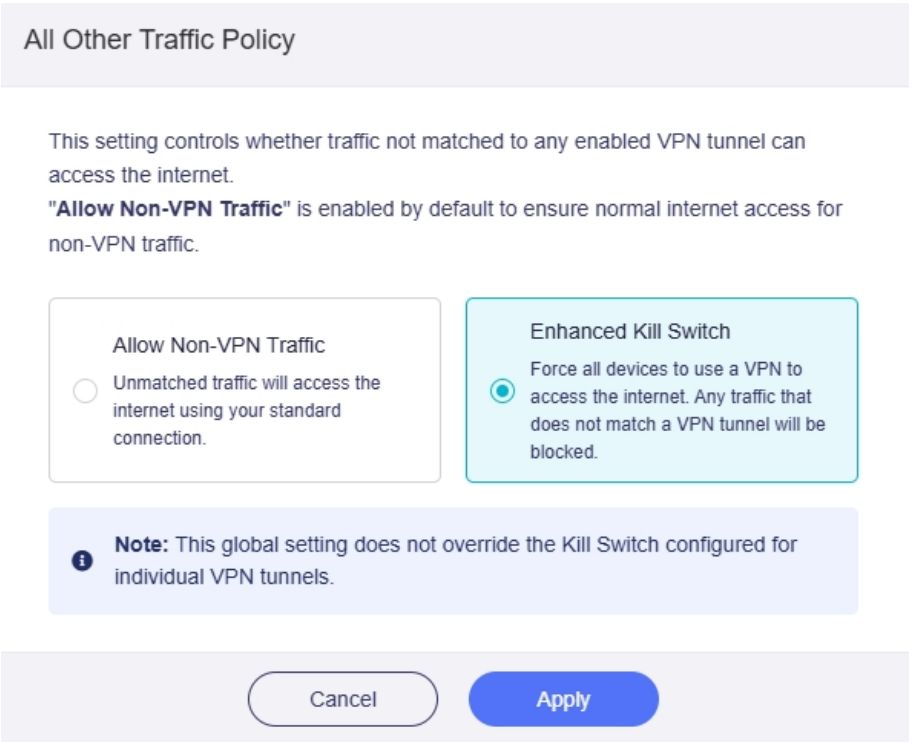
11. Upewnij się, że **Kill Switch** dla tunelu 2 jest włączony. Jeśli VPN niespodziewanie się rozłączy, dostęp do Internetu dla ruchu pasującego do tunelu zostanie zablokowany, aby zapobiec wyciekom DNS i śledzeniu adresu IP.



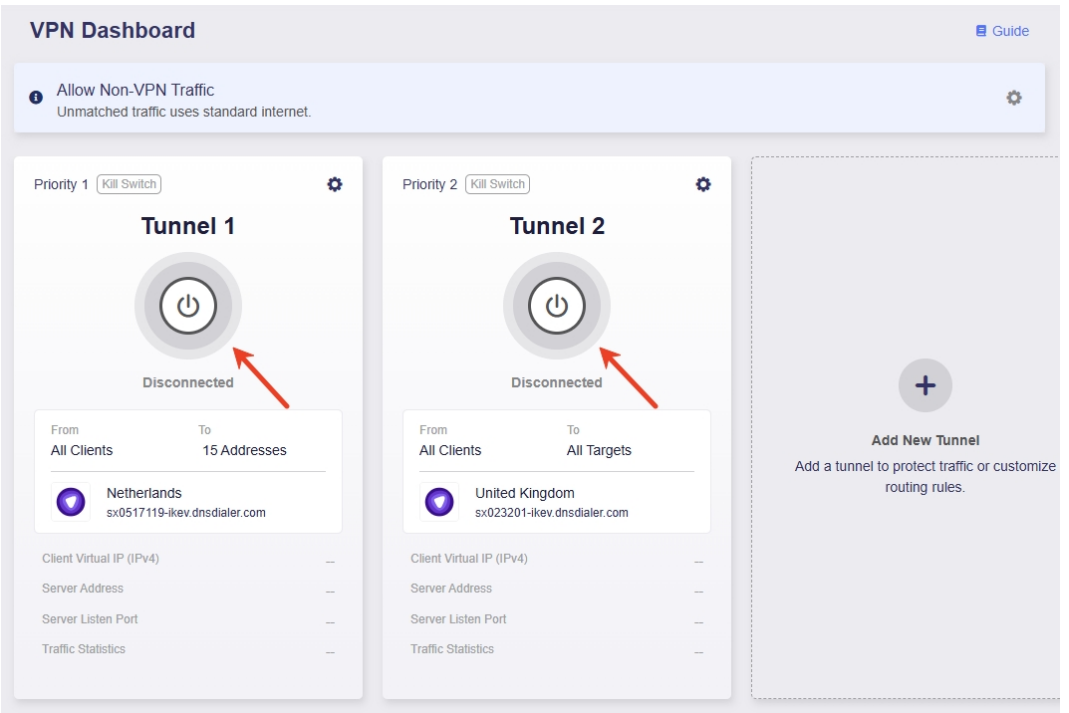


12. Kliknij ikonę koła zębatego w prawym górnym rogu, aby włączyć **Enhanced Kill Switch**. Zapewnia to dostęp do Internetu wyłącznie przez VPN dla całego ruchu.

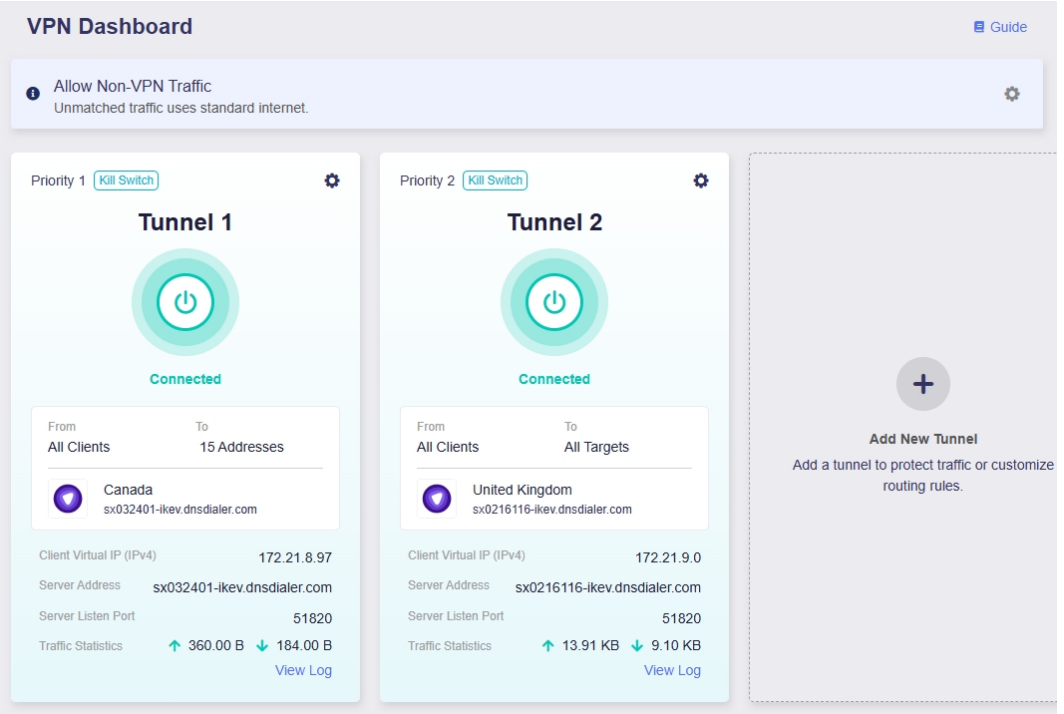




13. Kliknij środkowy przycisk, aby aktywować tunel 1 i tunel 2.



14. Po nawiązaniu połączenia strona wyświetli szczegóły połączenia VPN, w tym zasady VPN, statystyki ruchu, adres serwera, port nasłuchiwania i wirtualny adres IP.



Teraz wszystkie urządzenia będą korzystać z VPN Tunnel 1 podczas odwiedzania określonych domen, a z VPN Tunnel 2 przy pozostałym dostępie do Internetu. Jeśli tunele VPN niespodziewanie się rozłączą, dostęp wszystkich urządzeń do Internetu zostanie zablokowany, aby zapobiec wyciekom DNS i śledzeniu adresu IP.

9.3 Kill Switch

Kill Switch to zabezpieczenie połączeń VPN. W razie niespodziewanego zerwania połączenia VPN automatycznie odcina dostęp do Internetu w sieci lokalnej, zapobiegając ujawnieniu rzeczywistego adresu IP i danych przesyłanych w sieci oraz zapewniając ciągłą ochronę prywatności i bezpieczeństwa. Funkcja jest szczególnie przydatna, gdy wymagany jest bezpieczny, anonimowy dostęp do Internetu, np. w sieciach publicznych, podczas przetwarzania poufnych danych lub ukrywania rzeczywistego adresu IP.

Po włączeniu blokuje ruch klientów próbujący ominąć tunel VPN. Skutecznie zapobiega to wyciekom z VPN spowodowanym błędami konfiguracji DNS, niespodziewanymi rozłączeniami, bezpośrednimi żądaniami do adresów IP i podobnymi sytuacjami.

Od wersji oprogramowania sprzętowego v4.8 routery GL.iNet umożliwiają konfigurowanie Kill Switch zarówno dla globalnego połączenia VPN, jak i dla każdego tunelu VPN osobno.

- Aby skonfigurować Kill Switch dla globalnego połączenia VPN, zobacz Cały pozostały ruch.
- Aby skonfigurować Kill Switch dla każdego tunelu VPN osobno, zobacz Opcje tunelu.

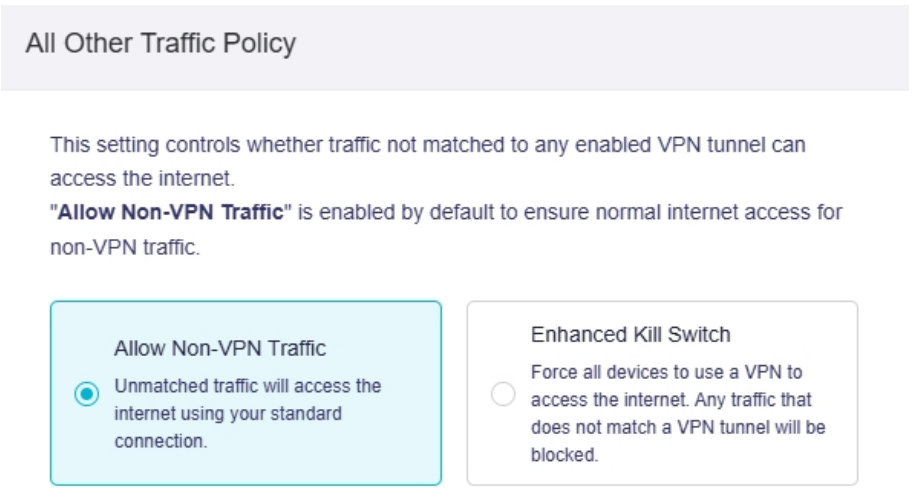
9.4 Cały pozostały ruch

Kliknij ikonę koła zębatego w prawym górnym rogu, aby ustawić zasady dla ruchu niepasującego do tunelu VPN.

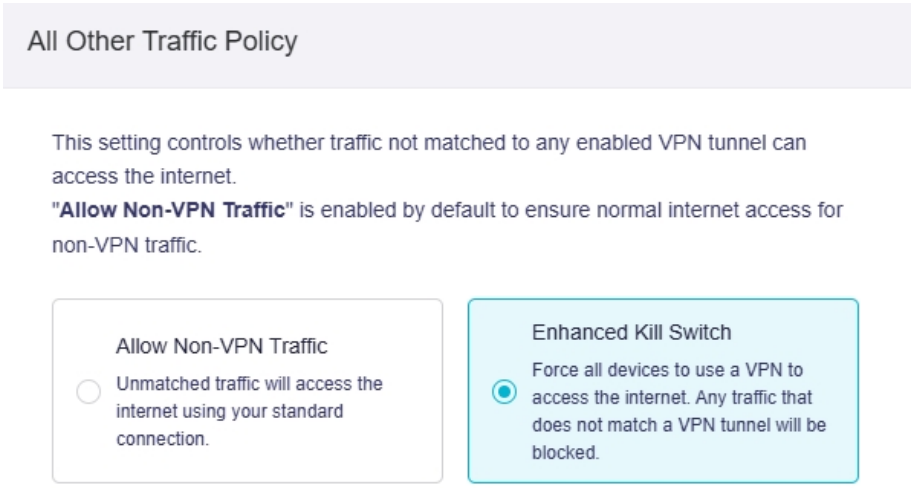


Ta zasada określa, czy ruch niepasujący do żadnej grupy tuneli VPN może uzyskiwać dostęp do Internetu. Dostępne są dwie opcje:

- **Allow Non-VPN Traffic**: domyślnie włączone, aby zapewnić zwykły dostęp do Internetu dla ruchu poza VPN.



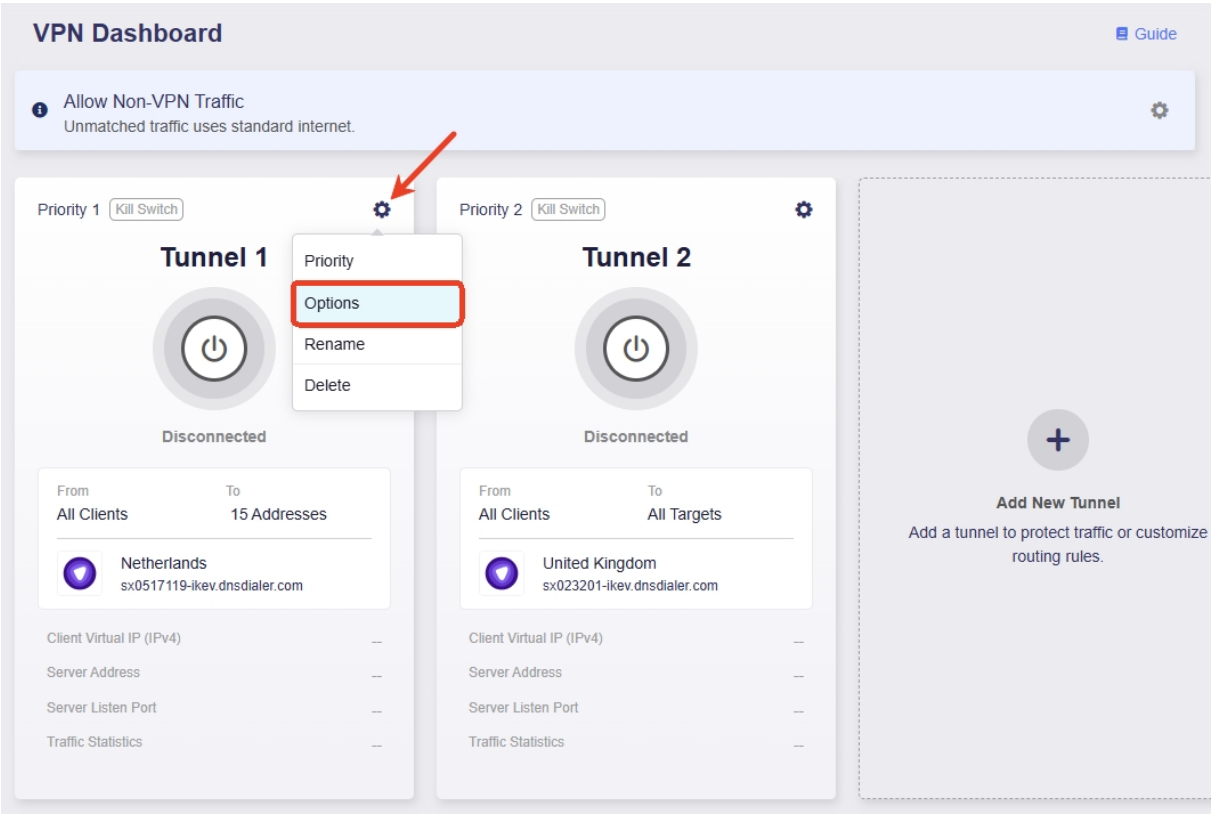
- **Enhanced Kill Switch**: wymusza dostęp do Internetu przez VPN na wszystkich urządzeniach. Ruch niepasujący do tunelu VPN zostanie zablokowany. To ustawienie globalne nie zastępuje ustawień Kill Switch poszczególnych tuneli VPN.

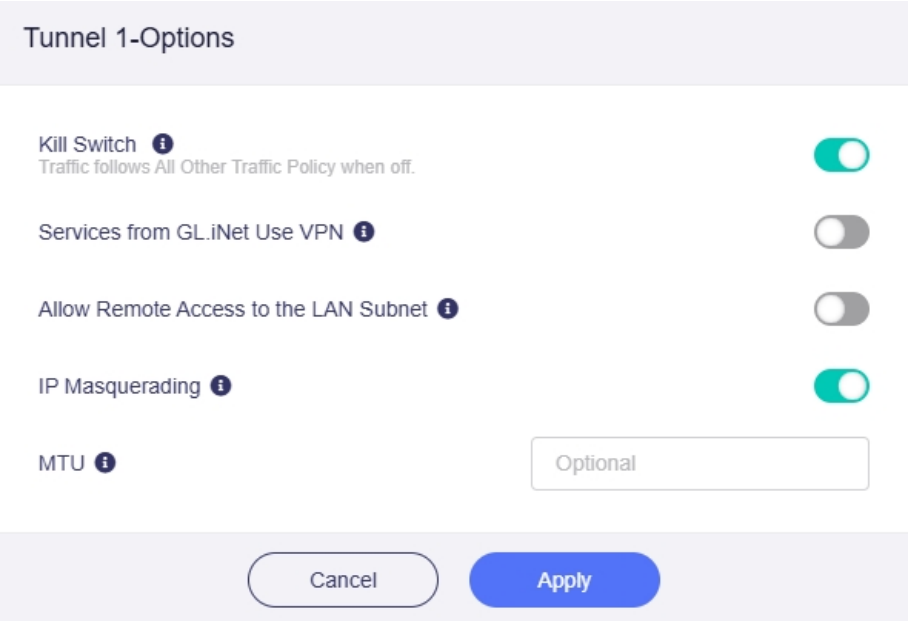


9.5 Opcje tunelu

Możesz skonfigurować zaawansowane ustawienia każdego tunelu VPN, takie jak Kill Switch, maskarada adresów IP i MTU.

Kliknij ikonę koła zębatego w grupie tuneli i wybierz **Options**.

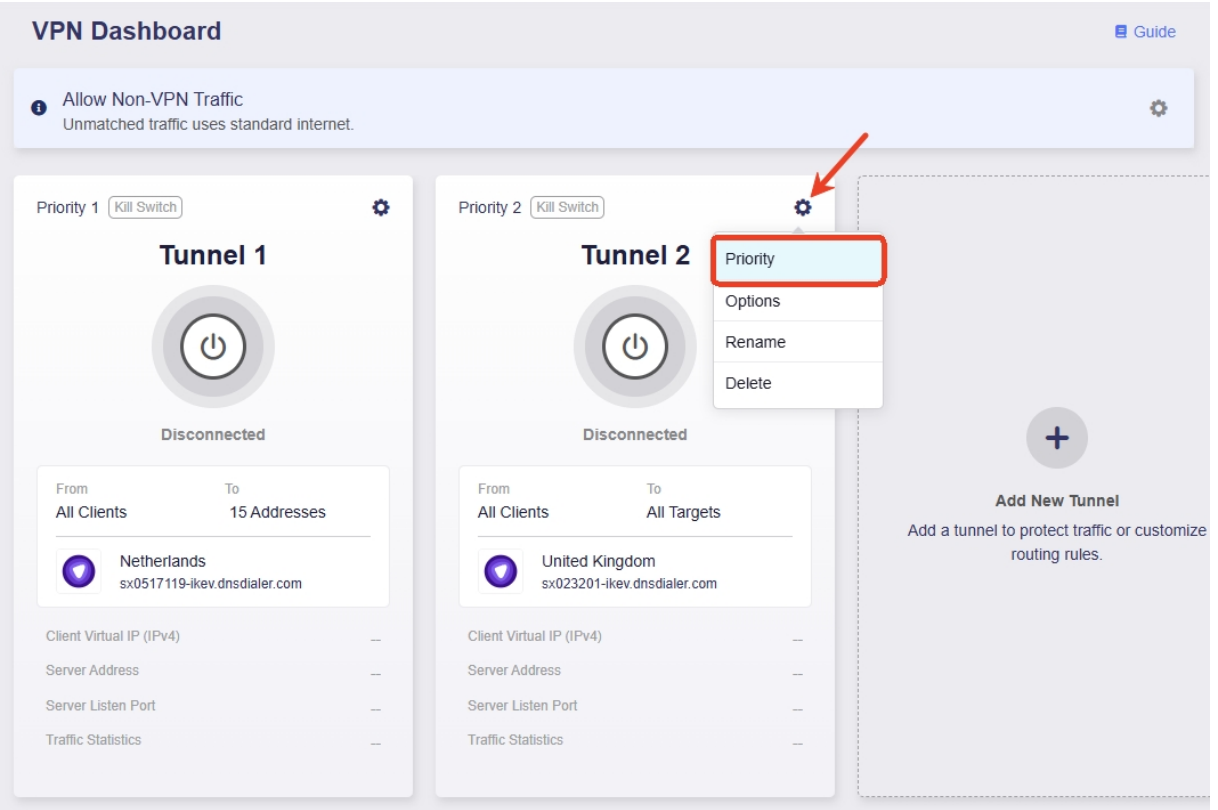




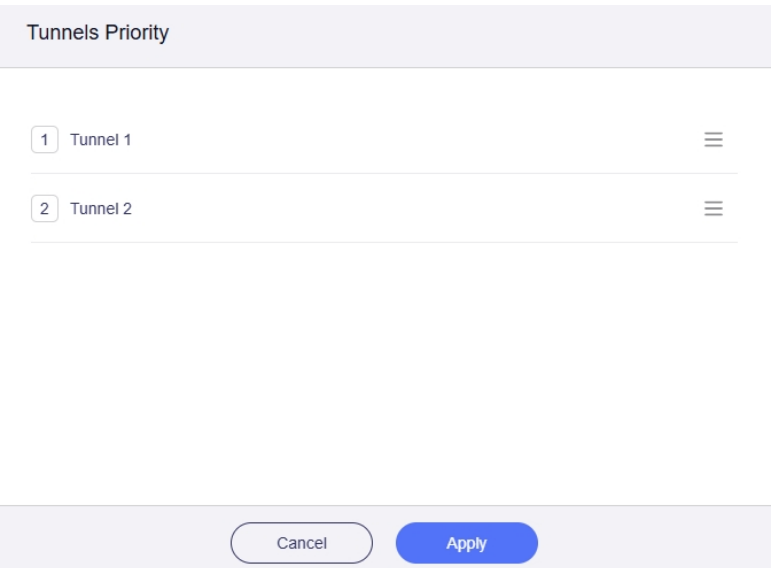
- **Kill Switch**: po włączeniu ruch pasujący do tego tunelu VPN zostanie zablokowany w razie niespodziewanej awarii połączenia VPN. Po wyłączeniu taki ruch zostanie przełączony do tunelu All Other Traffic.
- **Services from GL.iNet Use VPN**: po włączeniu usługi GoodCloud, DDNS i rtty przesyłają pakiety przez tunele VPN. Ta opcja jest domyślnie wyłączona, ponieważ usługi te zwykle wymagają rzeczywistego adresu IP urządzenia do poprawnego działania.
- **Allow Remote Access to the LAN Subnet**: po włączeniu dozwolony jest zdalny dostęp do tego routera i urządzeń w jego sieci LAN przez VPN. Serwer VPN musi rozgłaszać trasę powrotną do swojej podsieci LAN.
- **IP Masquerading**: po włączeniu źródłowe adresy IP klientów LAN są zastępowane adresem IP tunelu VPN routera. Wyłączaj tę opcję tylko w konfiguracjach sieć–sieć, w których zdalny węzeł zna Twoje podsieci LAN.
- **MTU**: wartość MTU ustawiona dla tunelu zastępuje ustawienia MTU w pliku konfiguracyjnym.

9.6 Priorytet tuneli

Aby dostosować priorytet tuneli, kliknij ikonę koła zębatego w grupie tuneli i wybierz **Priority**.



Kliknij i przytrzymaj ikonę z trzema liniami po prawej stronie, zmień kolejność tuneli, a następnie kliknij **Apply**.



Jeśli włączono wiele tuneli, router kieruje ruch według następujących reguł:

1. Najpierw sprawdza, czy ruch pasuje do reguły tunelu o najwyższym priorytecie. Jeśli tak, kieruje go przez ten tunel; w przeciwnym razie sprawdza tunel o kolejnym priorytecie itd.
2. Każda grupa tuneli działa niezależnie. Gdy ruch pasuje do reguły tunelu, jest kierowany przez ten tunel i nie jest przełączany między grupami tuneli.
3. W każdej grupie tuneli można wybrać wiele profili, aby umożliwić przełączanie awaryjne wewnątrz tunelu. Gdy profil o najwyższym priorytecie w grupie przestanie działać, tunel automatycznie połączy się za pomocą profilu o drugim najwyższym priorytecie itd.
4. Jeśli tunel VPN niespodziewanie się rozłączy, system zdecyduje, czy przełączyć ruch do tunelu All Other Traffic, zależnie od tego, czy **Kill Switch** tego tunelu jest włączony.
    - Jeśli Kill Switch jest włączony, ruch zostanie zablokowany i nie będzie przełączany do tunelu All Other Traffic.
    - Jeśli Kill Switch jest wyłączony, ruch zostanie przełączony do tunelu All Other Traffic.
5. W tunelu **All Other Traffic** poszczególne tryby określają, czy ruch niepasujący do tunelu VPN może uzyskiwać dostęp do Internetu.
    - **Allow Non-VPN Traffic**: domyślnie włączone, aby ruch niepasujący do tuneli VPN mógł nadal łączyć się z Internetem przez lokalne łącze WAN.
    - **Enhanced Kill Switch**: wymusza dostęp do Internetu przez VPN na wszystkich urządzeniach. Ruch niepasujący do tunelu VPN zostanie zablokowany. To ustawienie globalne nie zastępuje ustawień Kill Switch poszczególnych tuneli VPN. Wzmacnia więc działanie Kill Switch i blokuje zwykły dostęp do Internetu, zapobiegając wyciekom adresu IP.

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:

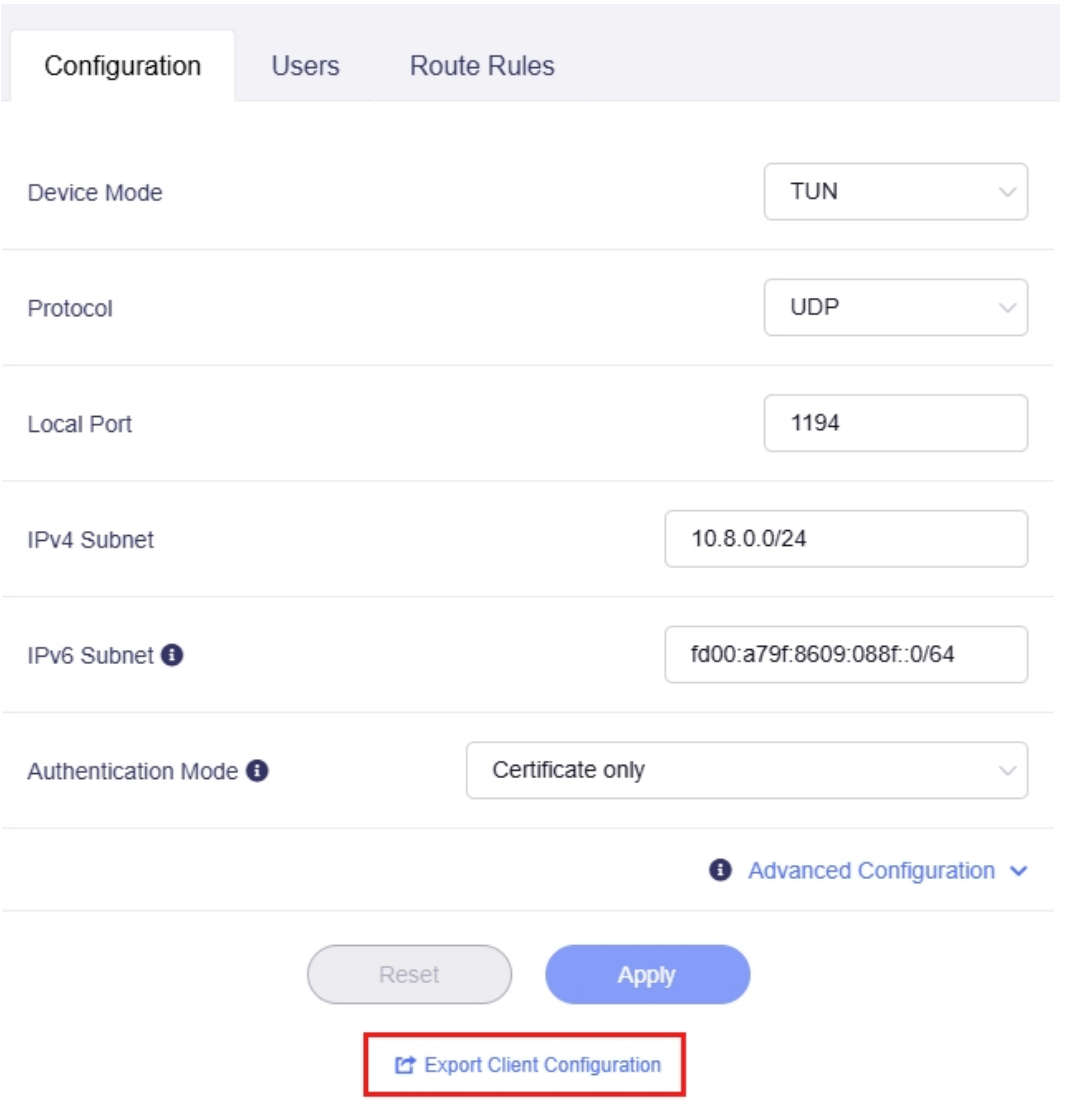
   - Jeśli przed routerem GL.iNet znajduje się główny router, zaloguj się do niego i sprawdź, czy ma publiczny adres IP przydzielony przez dostawcę Internetu.
   - Poproś dostawcę Internetu o publiczny adres IP. Może to wiązać się z dodatkową opłatą.
   - Jeśli powyższe dwie metody nie działają (np. sieć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

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

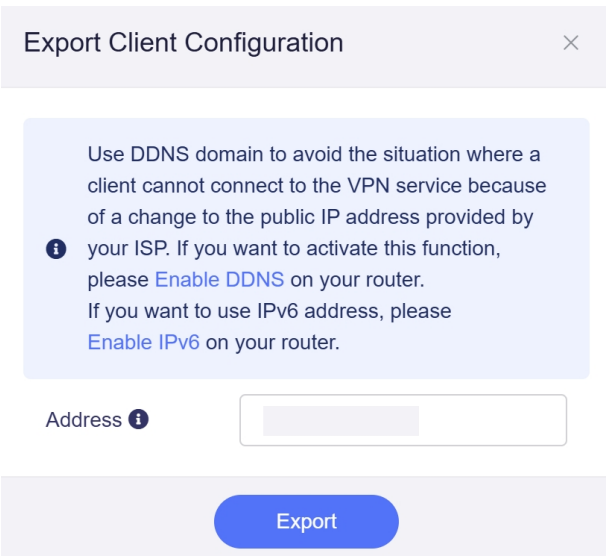
1. Zaloguj się do panelu administracyjnego routera, przejdź do **VPN** > **OpenVPN Server**, a następnie kliknij **Generate Configuration** (tylko przy pierwszej konfiguracji serwera VPN).
2. Zastosuj konfigurację.
   Domyślna konfiguracja sprawdza się w większości przypadków. Kliknij **Export Client 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.

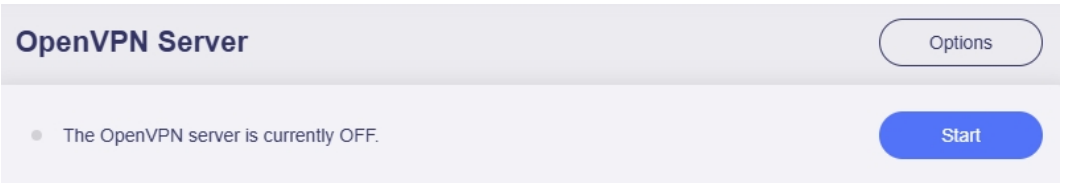


Wskazówki:

- Jeśli Twój publiczny adres IP często się zmienia, przejdź do **APPLICATIONS** > **Dynamic DNS** i włącz DDNS. Możesz wtedy używać domeny DDNS jako adresu serwera.
- Przed wyeksportowaniem pliku konfiguracji możesz wybrać z listy rozwijanej adres serwera: publiczny adres IP, domenę DDNS lub bieżący adres IP WAN. Adres serwera w pliku konfiguracji zostanie automatycznie zaktualizowany. Jeśli zmienisz ten adres, pobierz plik konfiguracji ponownie.

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:

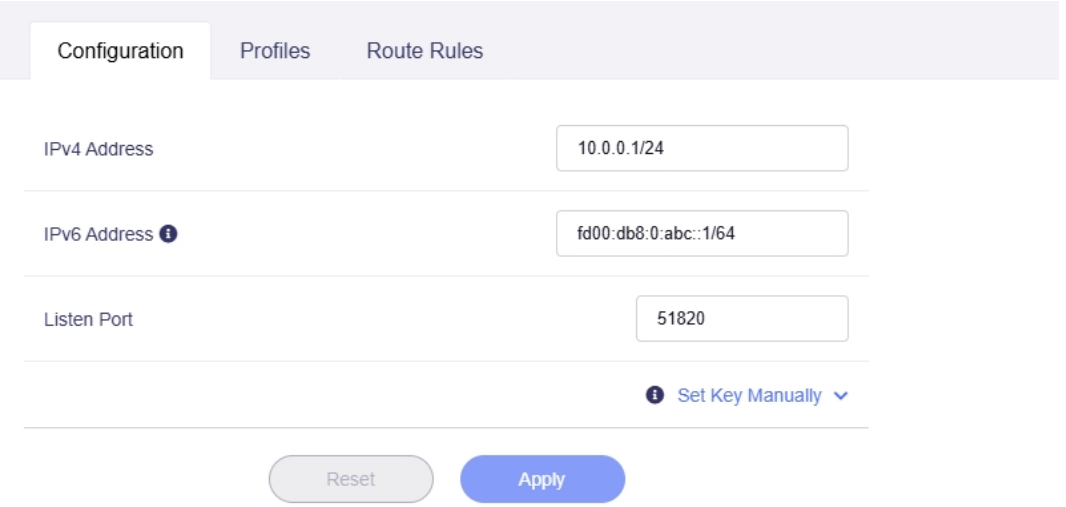
   - Jeśli przed routerem GL.iNet znajduje się główny router, zaloguj się do niego i sprawdź, czy ma publiczny adres IP przydzielony przez dostawcę Internetu.
   - Poproś dostawcę Internetu o publiczny adres IP. Może to wiązać się z dodatkową opłatą.
   - Jeśli powyższe dwie metody nie działają (np. sieć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

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

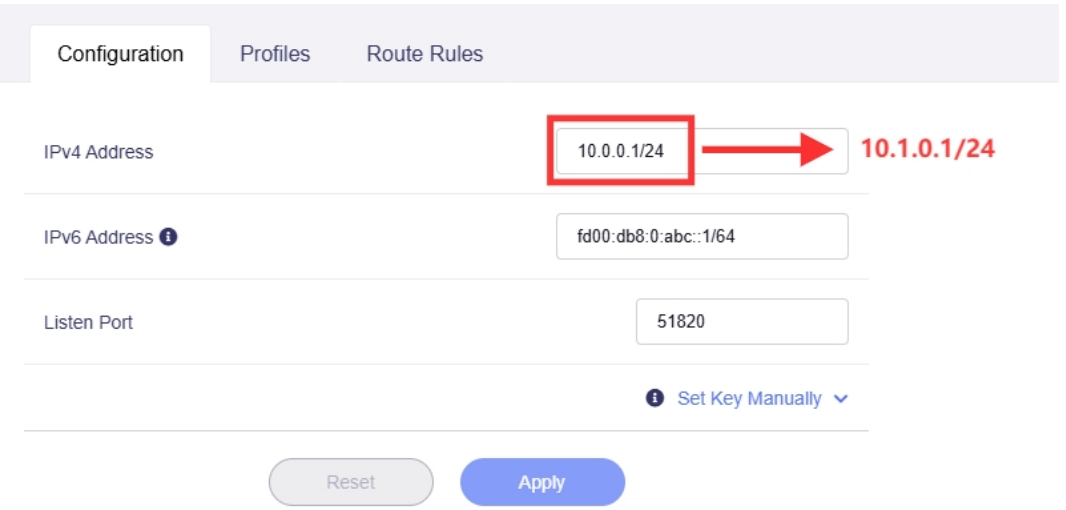
   - Jeśli router GL.iNet jest głównym routerem w sieci, konfiguracja przekierowania portów nie jest wymagana. Przejdź do następnego kroku.
   - Jeśli korzystasz już z głównego routera, a router GL.iNet działa jako router dodatkowy, trzeba skonfigurować przekierowanie portów na głównym routerze.
   - Jeśli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

10.2.2 Etapy konfiguracji

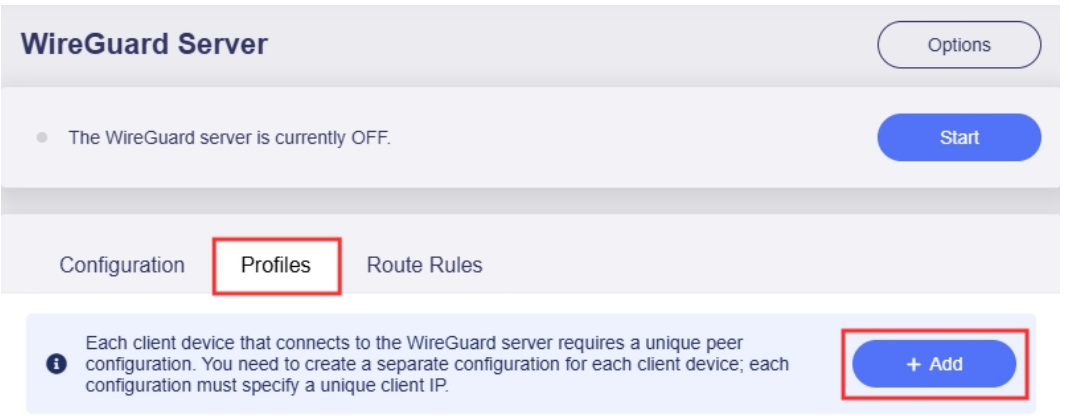
1. Zaloguj się do panelu administracyjnego routera, przejdź do **VPN** > **WireGuard Server**, a następnie kliknij **Generate Configuration** (tylko przy pierwszej konfiguracji serwera VPN).
2. Zastosuj konfigurację.
   Domyślna konfiguracja sprawdza się w większości przypadków. Nie trzeba zmieniać adresu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



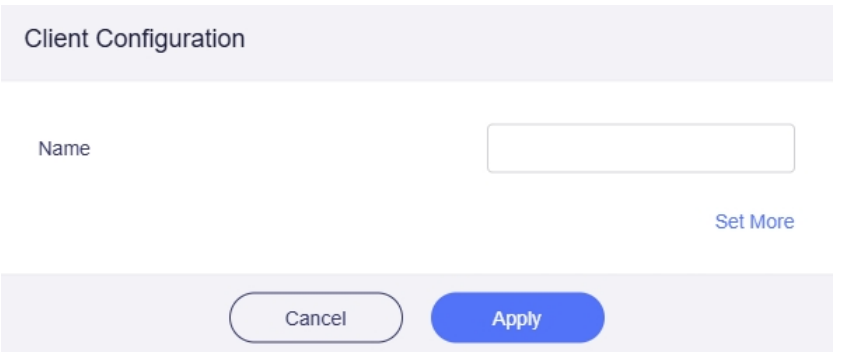
   Jeśli adres IPv4 koliduje z adresem bramy routera nadrzędnego, zmień go na inny (np. **10.1.0.1/24**) i kliknij **Apply**. Aby uniknąć problemów z łącznością, koniecznie zachowaj zapis CIDR „/24”.



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

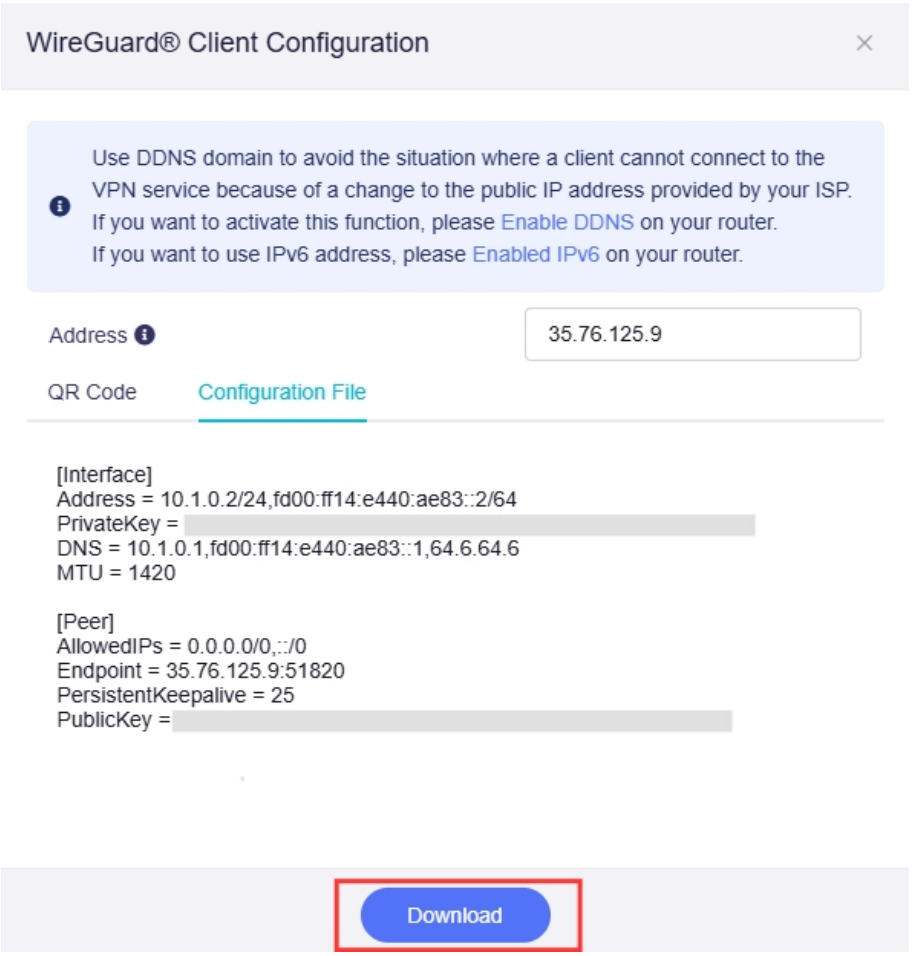


Nadaj opisową nazwę i kliknij **Apply**, aby kontynuować.



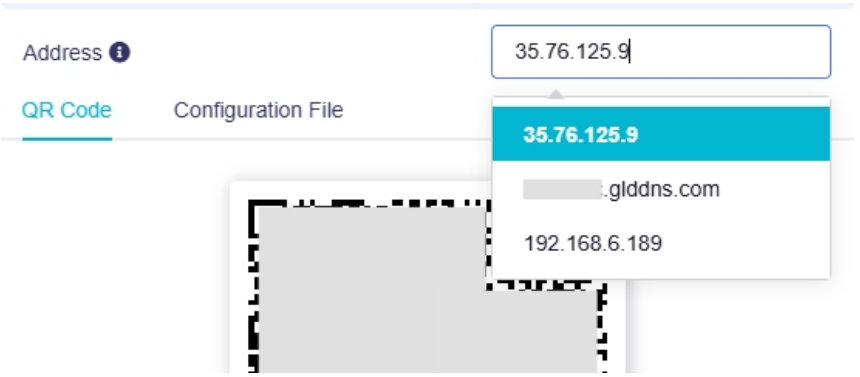
Wskazówka: aby z serwera WireGuard uzyskać dostęp do urządzeń LAN klienta WireGuard, przejdź na kartę **Route Rules** i skonfiguruj reguły routingu. Szczegóły znajdziesz tutaj.

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.

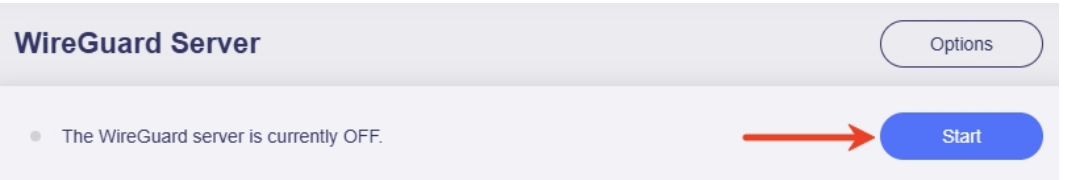


Wskazówki:

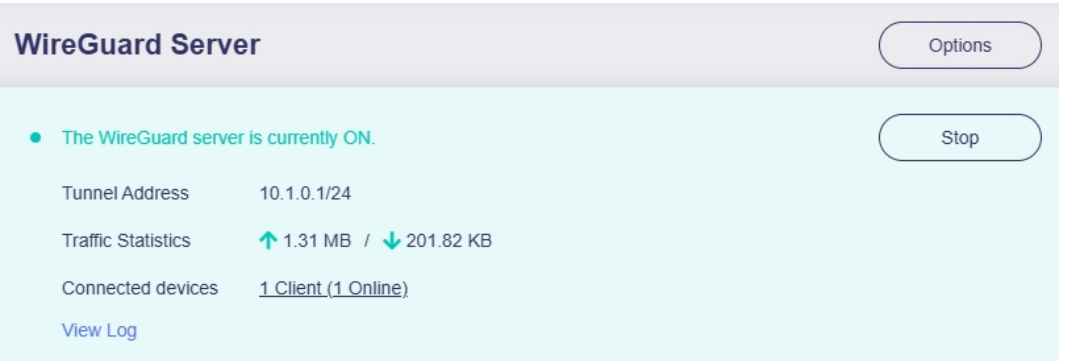
- Jeśli Twój publiczny adres IP często się zmienia, przejdź do **APPLICATIONS** > **Dynamic DNS** i włącz DDNS. Możesz wtedy używać domeny DDNS jako adresu serwera.
- Od wersji oprogramowania 4.8 przed wyeksportowaniem pliku konfiguracyjnego można wybrać adres serwera z listy: publiczny adres IP, domenę 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.

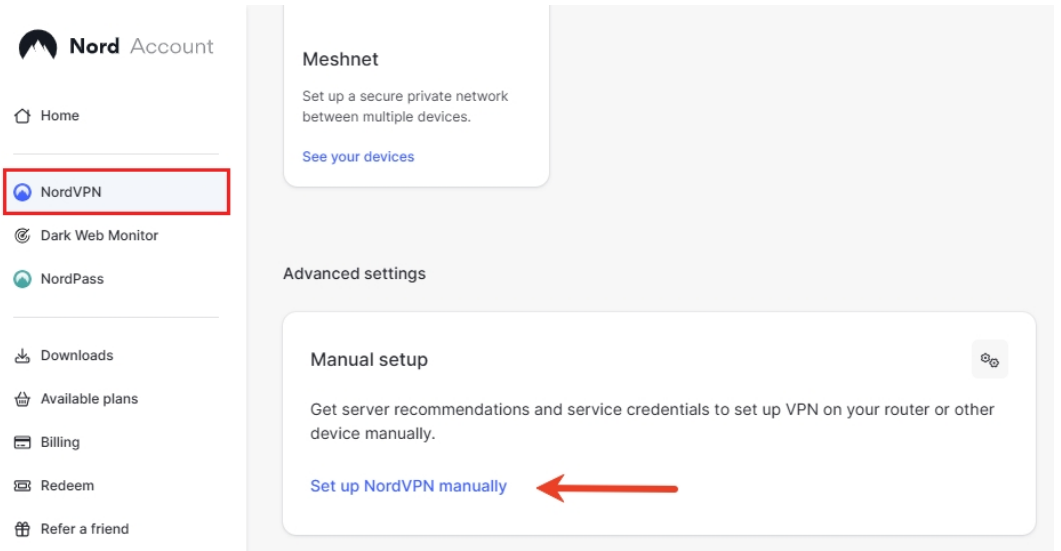
Następnie odwiedź oficjalną witrynę dostawcy VPN, którego usługę subskrybujesz, i uzyskaj dane dostępowe usługi lub plik konfiguracyjny. Jeśli nie wiesz, jak uzyskać plik konfiguracyjny, skorzystaj z tego łącza lub skontaktuj się z pomocą techniczną dostawcy.

11.1.2 Konfiguracja NordVPN

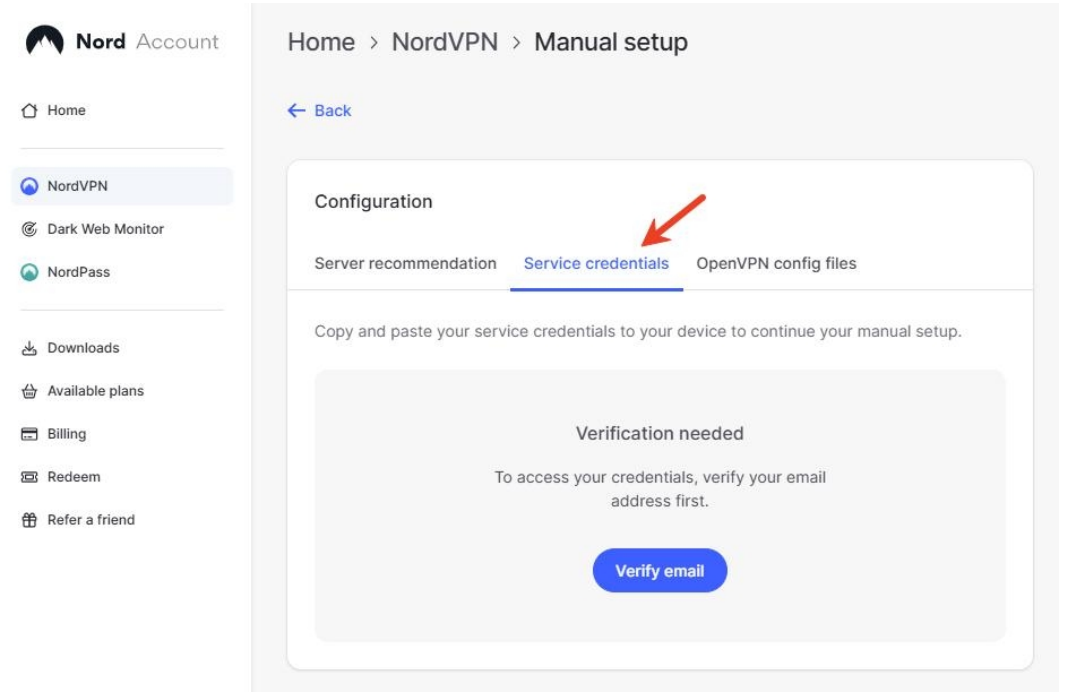
NordVPN jest zintegrowany z panelem administracyjnym GL.iNet. Pliki konfiguracyjne wszystkich serwerów NordVPN można uzyskać, wprowadzając dane dostępowe konta (z panelu NordVPN) w panelu administracyjnym routera lub aplikacji mobilnej GL.iNet. Eliminuje to potrzebę ręcznego przesyłania plików.

Aby skonfigurować router jako klienta NordVPN, wykonaj poniższe czynności.

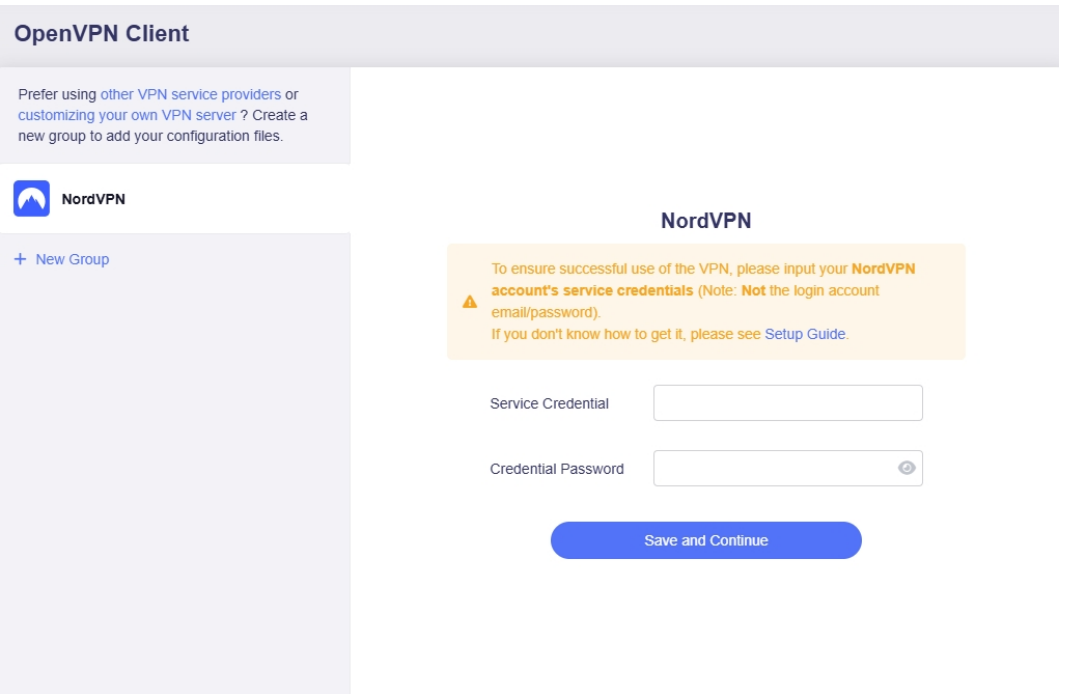
1. Zaloguj się na swoje konto internetowe NordVPN tutaj.
2. W panelu Nord kliknij **NordVPN**, a następnie **Set up NordVPN manually**.



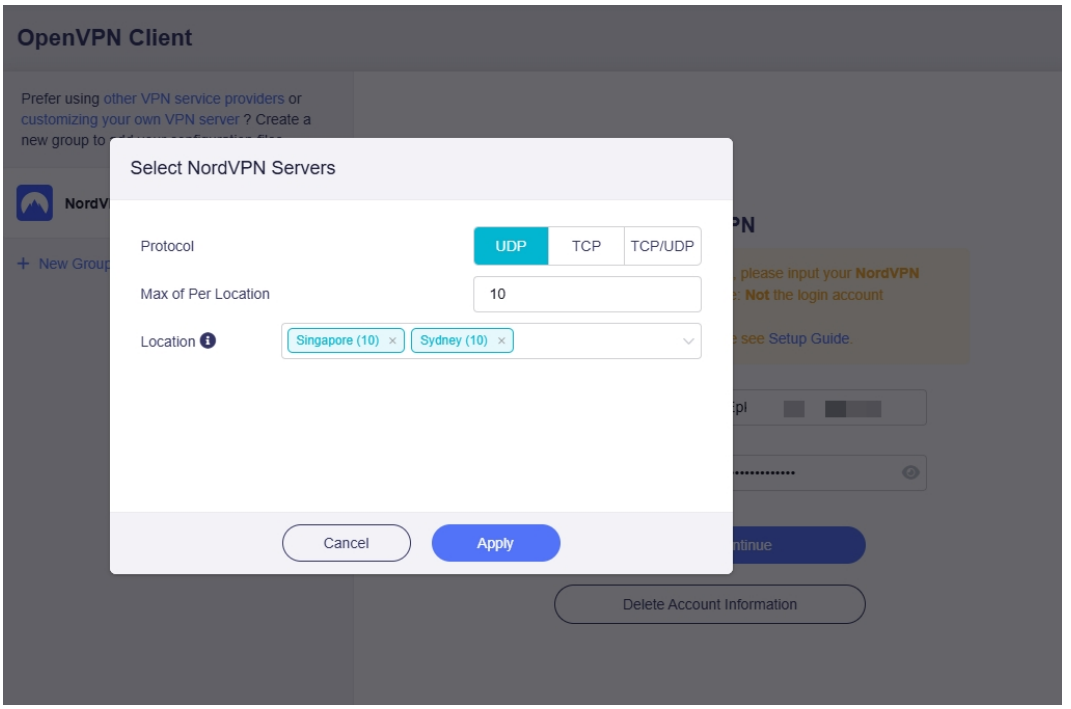
Znajdziesz tam **dane dostępowe usługi**. Skopiuj je do późniejszego użycia.



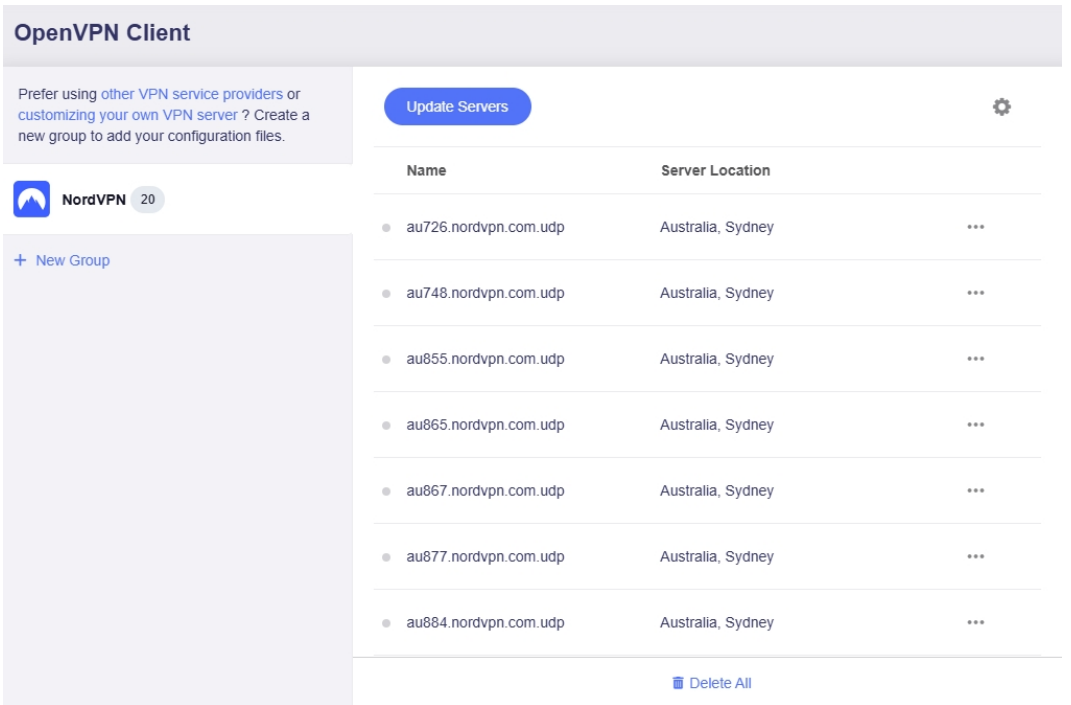
3. Zaloguj się do panelu administracyjnego routera i przejdź do **VPN** > **OpenVPN Client** > **NordVPN**. Wprowadź dane dostępowe usługi (uwaga: NIE jest to adres e-mail ani hasło do logowania na konto), a następnie kliknij **Save and Continue**.



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

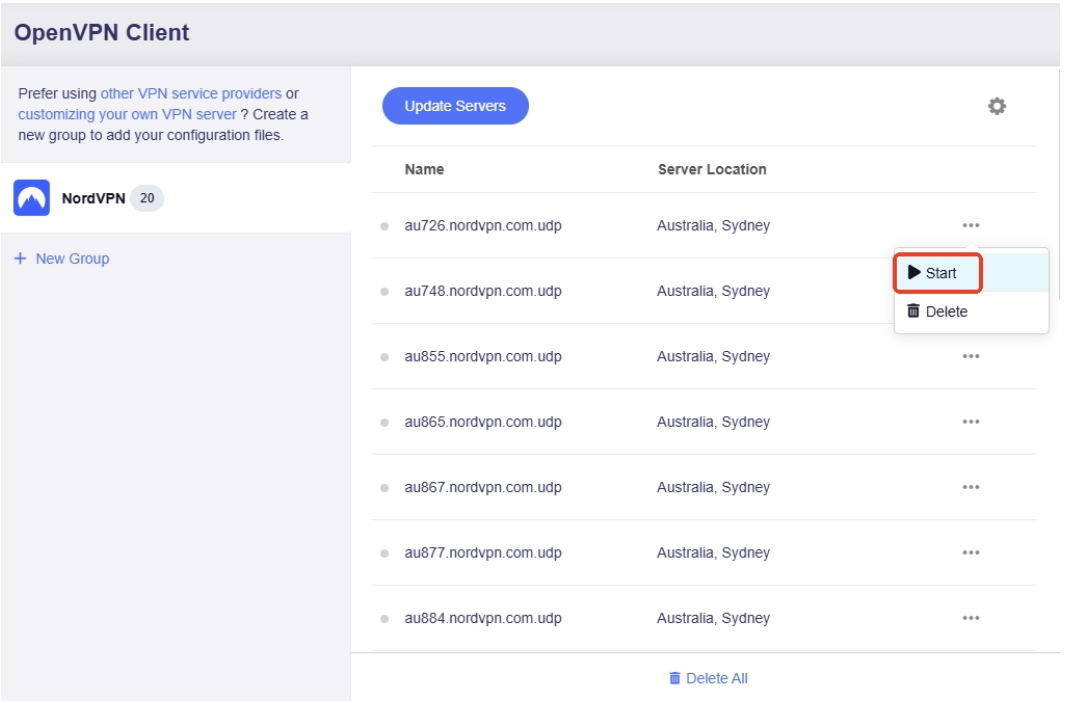


Rozpocznie się pobieranie plików konfiguracyjnych.

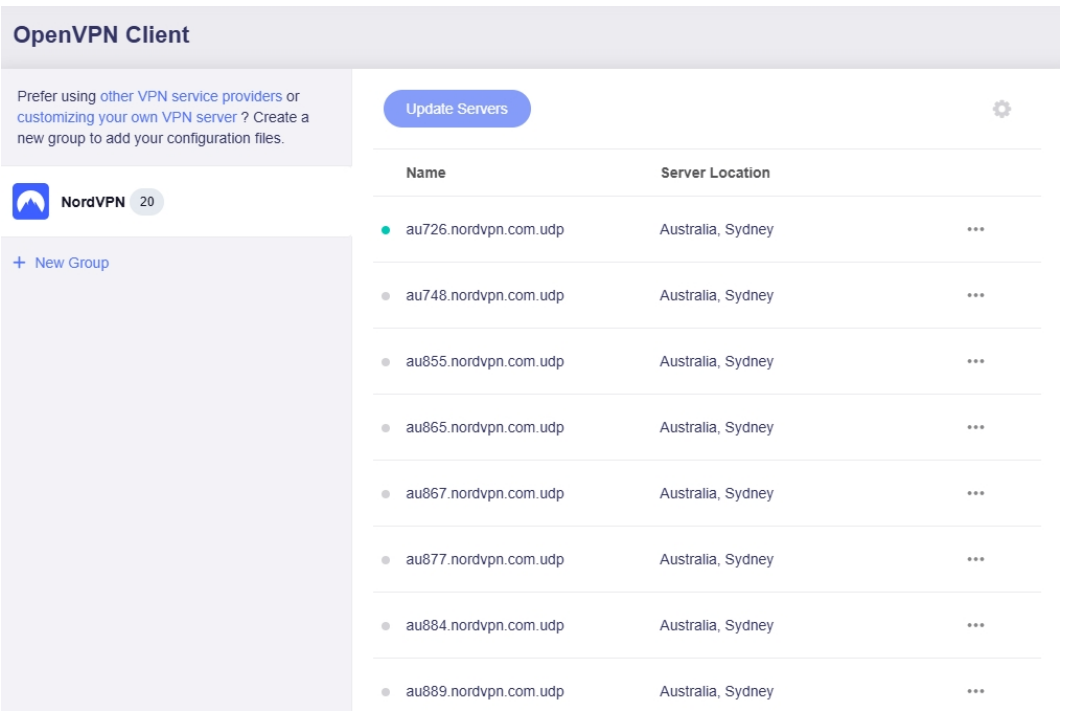


5. Nawiąż połączenie.

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



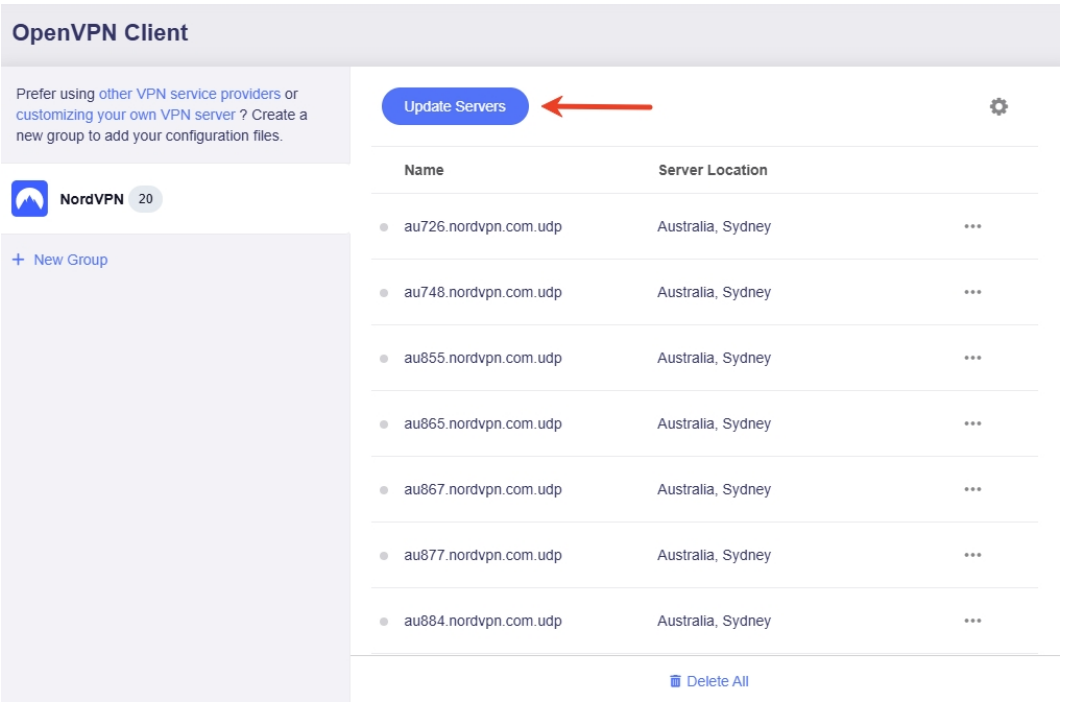
6. Po połączeniu obok pliku konfiguracyjnego pojawi się zielona kropka.



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

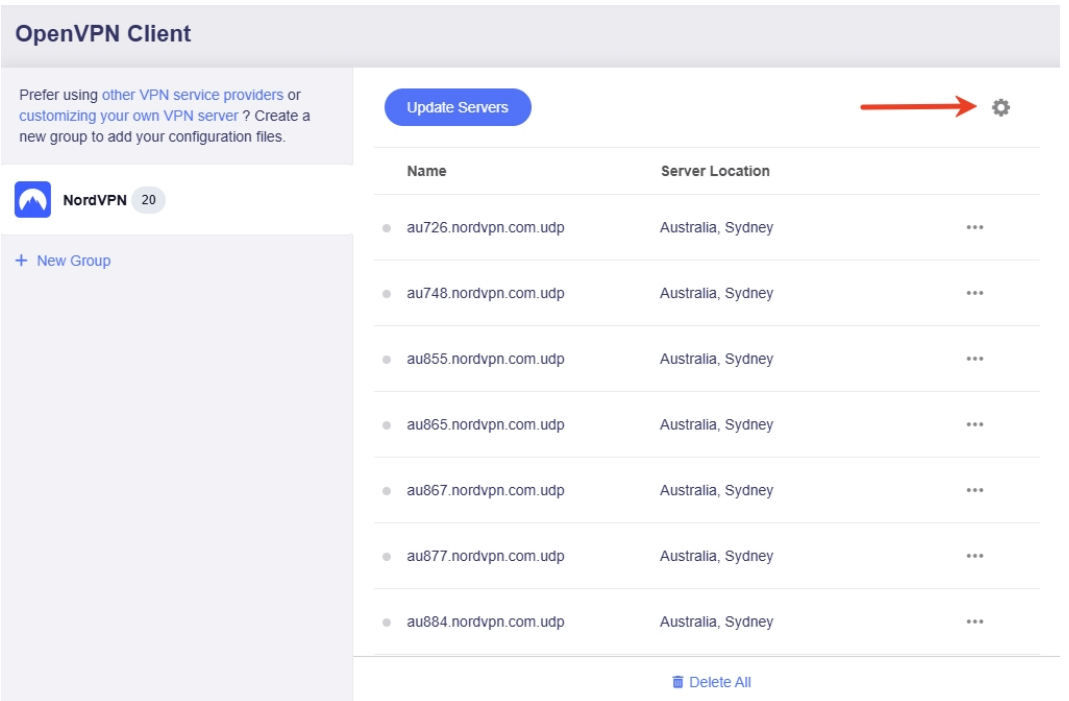
7. Zaktualizuj serwery.

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



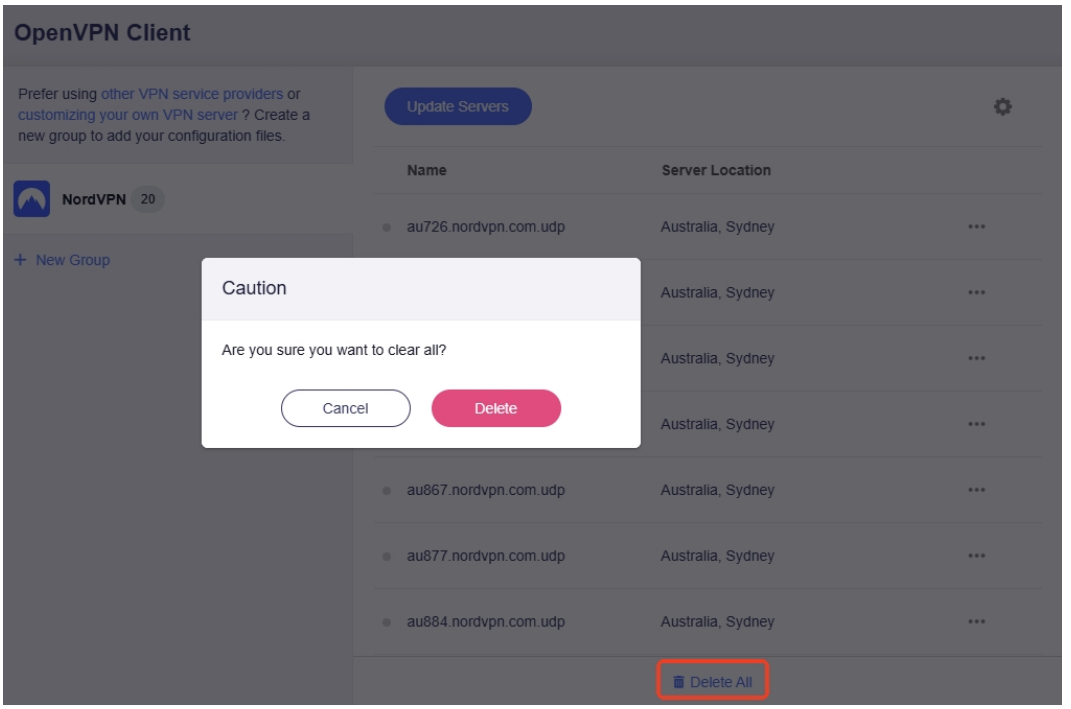
8. Zmień dane dostępowe.

   Kliknij ikonę koła zębatego, aby zmienić dane logowania.



9. Usuń wszystkie pliki.

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

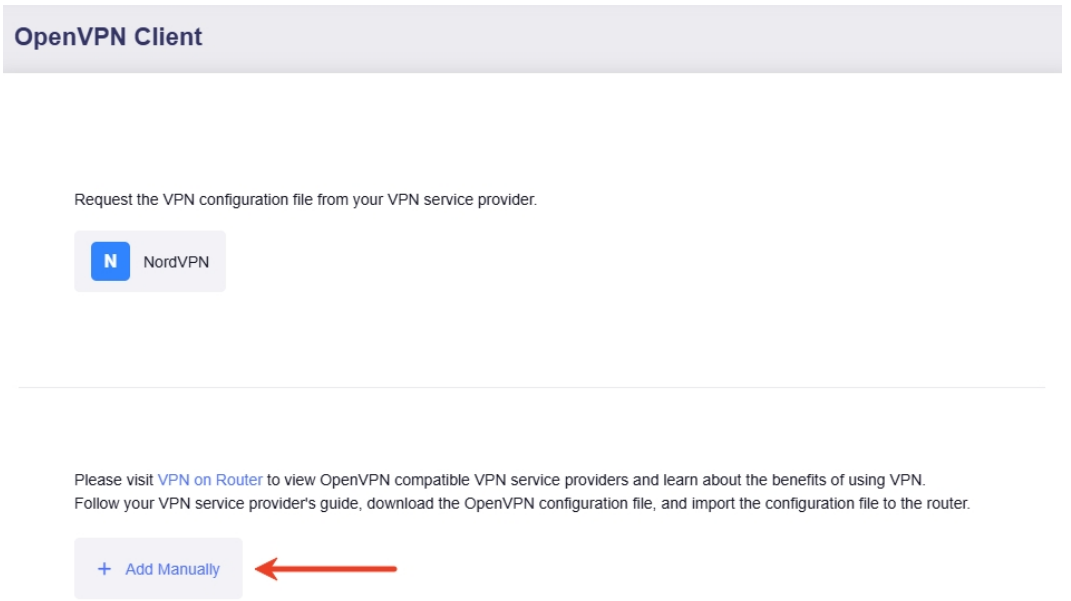


11.1.3 Ręczna konfiguracja klienta OpenVPN (inni dostawcy)

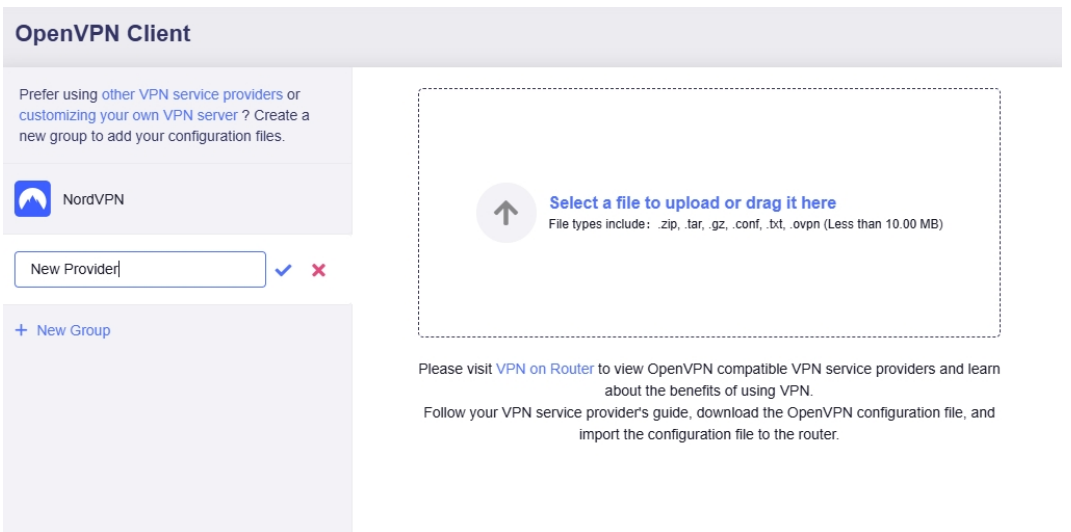
Jeśli Twój dostawca OpenVPN nie jest zintegrowany z panelem administracyjnym, najpierw odwiedź jego oficjalną witrynę i pobierz plik konfiguracyjny. Następnie prześlij go do routera, aby skonfigurować klienta OpenVPN.

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

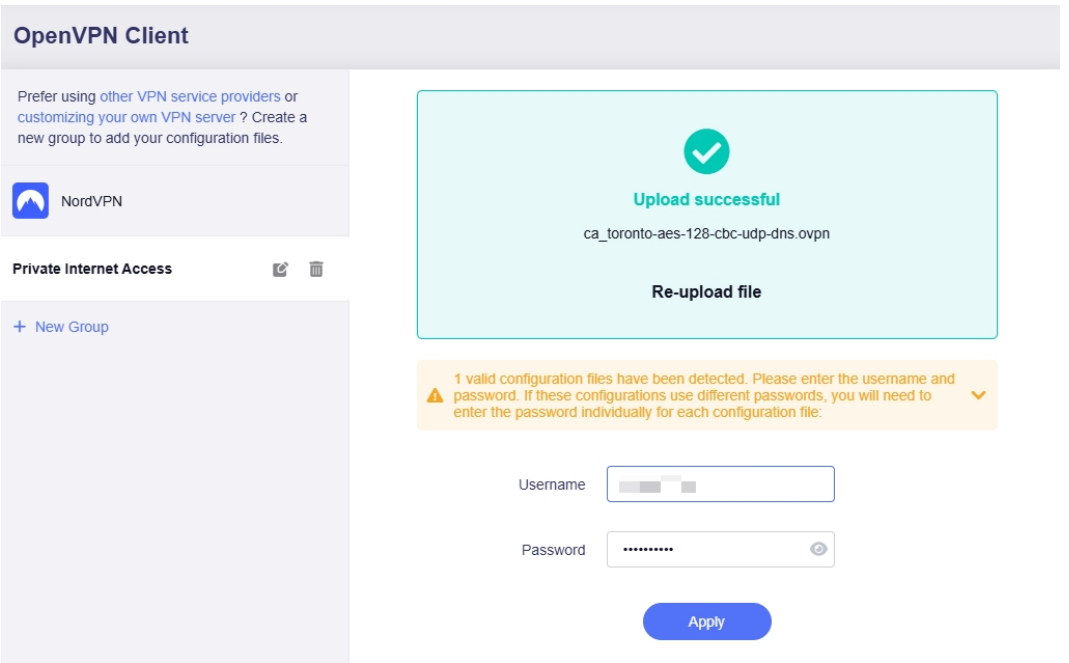
1. Pobierz plik konfiguracyjny z oficjalnej witryny Private Internet Access.
2. Zaloguj się do panelu administracyjnego routera, przejdź do **VPN** > **OpenVPN Client** i kliknij **Add Manually**.



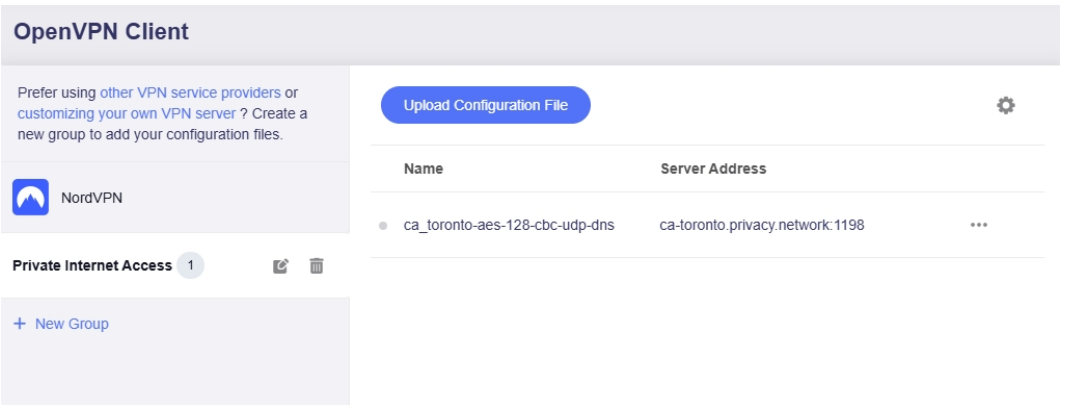
3. Na lewym pasku bocznym powstanie grupa. Nadaj jej opisową nazwę.



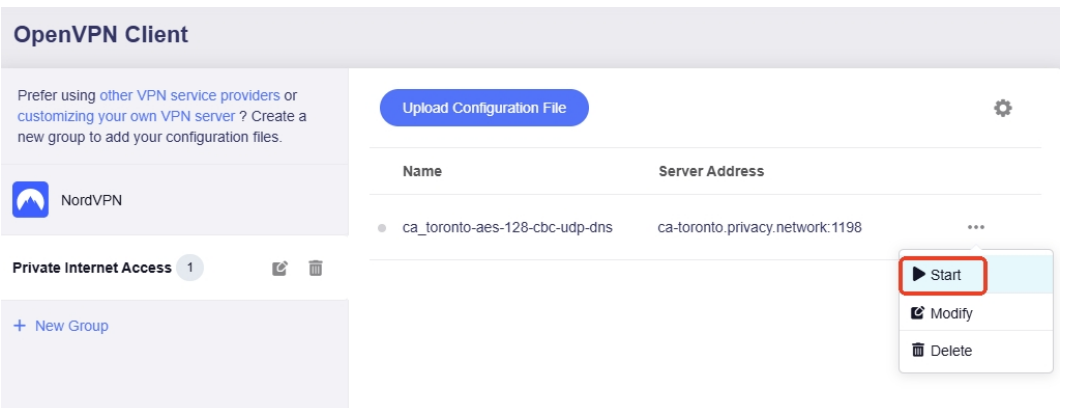
4. Prześlij plik konfiguracyjny OpenVPN. Jeśli jest to wymagane, wprowadź dane dostępowe, a następnie kliknij **Apply**.



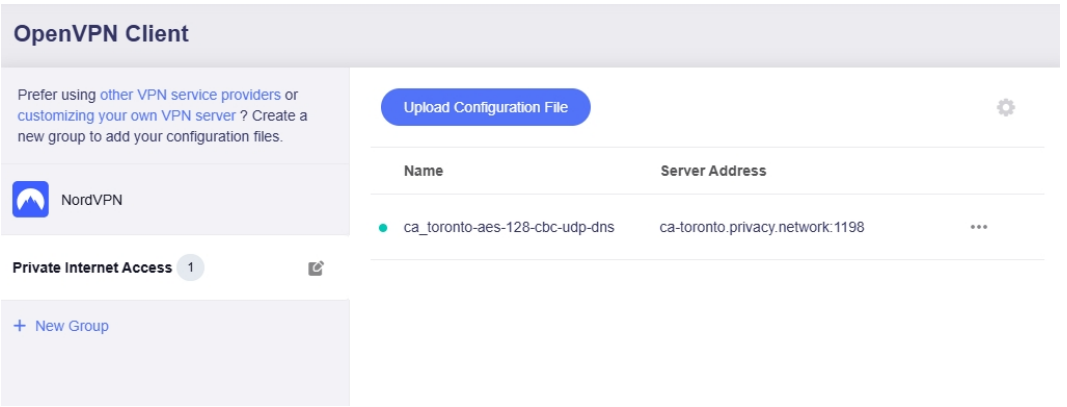
Pojawi się przesłany plik konfiguracyjny.



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.

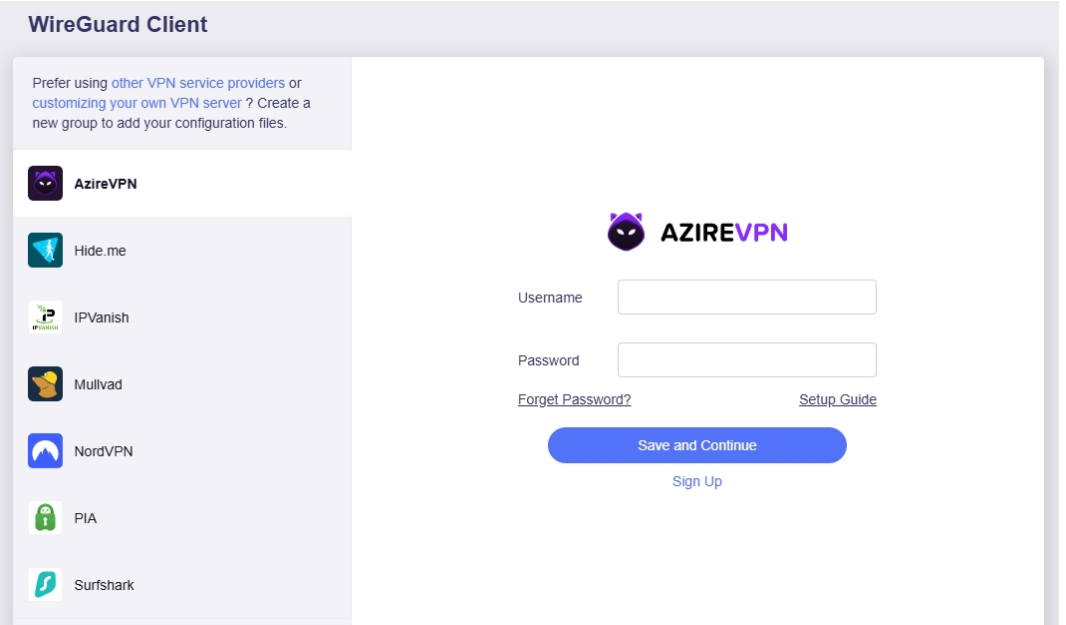
Następnie wybierz poniżej odpowiedniego dostawcę WireGuard, aby szybko przejść do instrukcji krok po kroku.

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

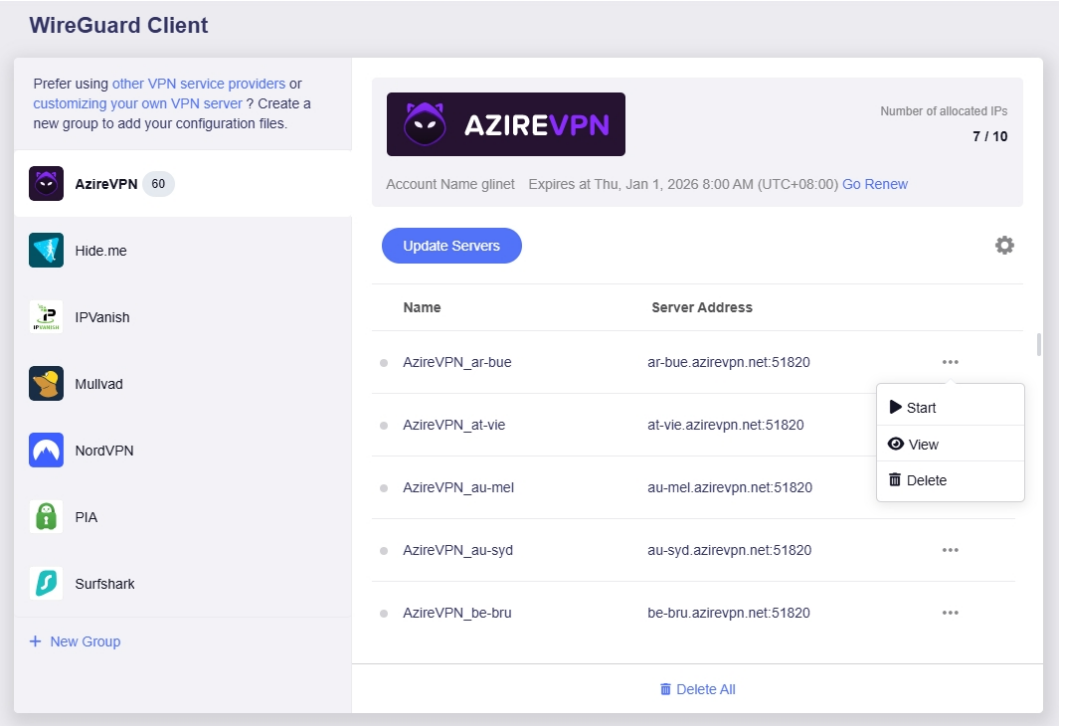
11.2.2 Konfiguracja AzireVPN

Aby skonfigurować router jako klienta AzireVPN, wykonaj poniższe czynności.

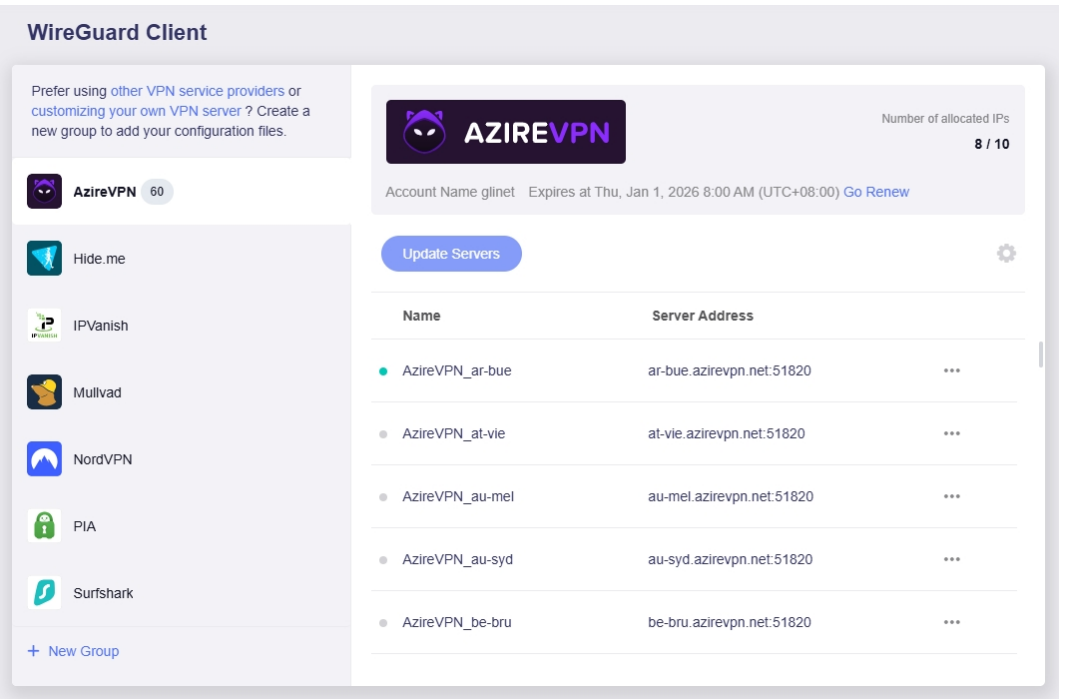
1. Zaloguj się do panelu administracyjnego routera i przejdź do **VPN** > **WireGuard Client** > **AzireVPN**.
2. Wprowadź nazwę użytkownika i hasło, a następnie kliknij **Save and Continue**. Zostaną wygenerowane pliki konfiguracyjne dla każdego serwera.



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



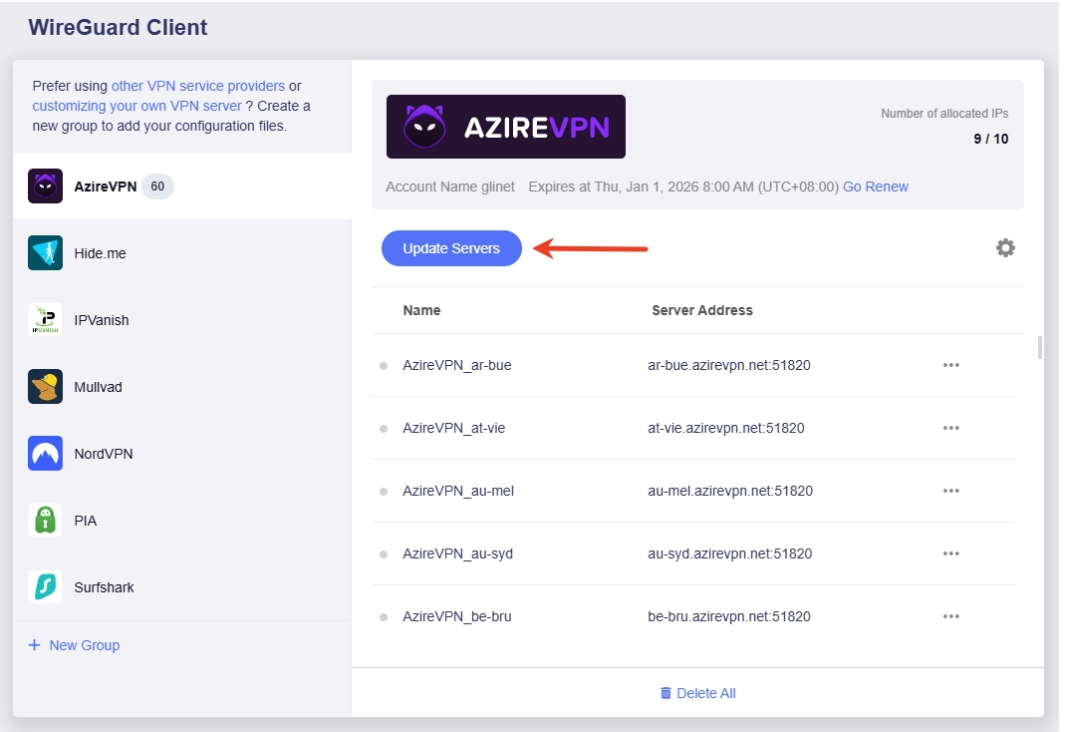
4. Po połączeniu obok pliku konfiguracyjnego pojawi się zielona kropka.



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

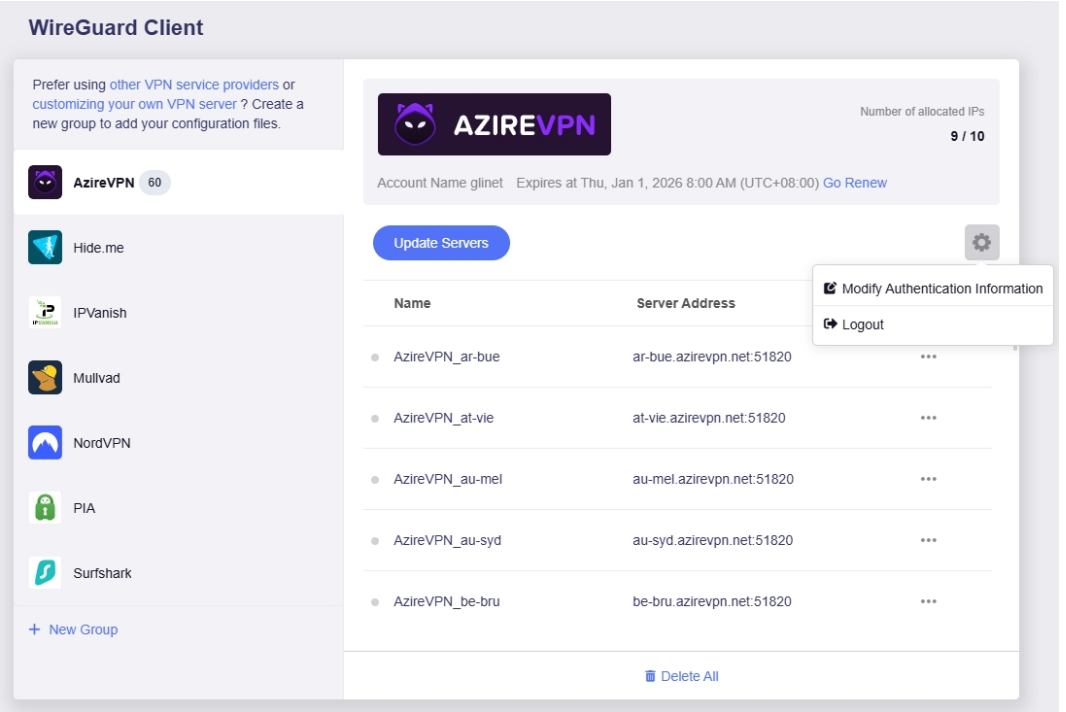
5. Zaktualizuj serwery.

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



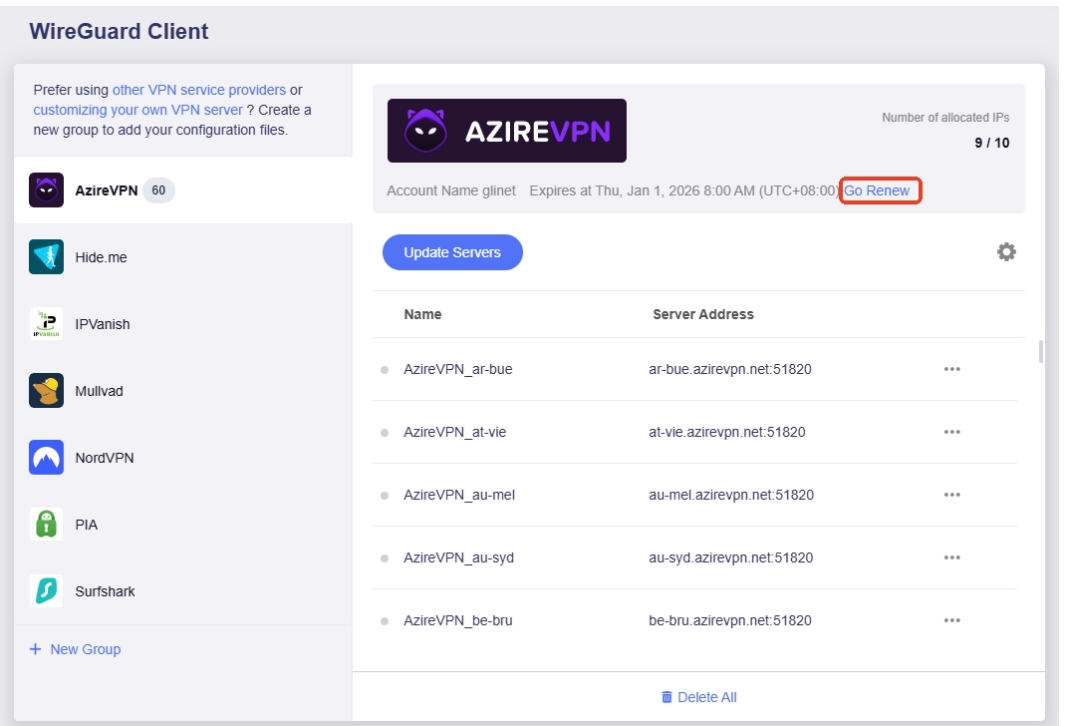
6. Zmiana danych logowania lub wylogowanie.

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



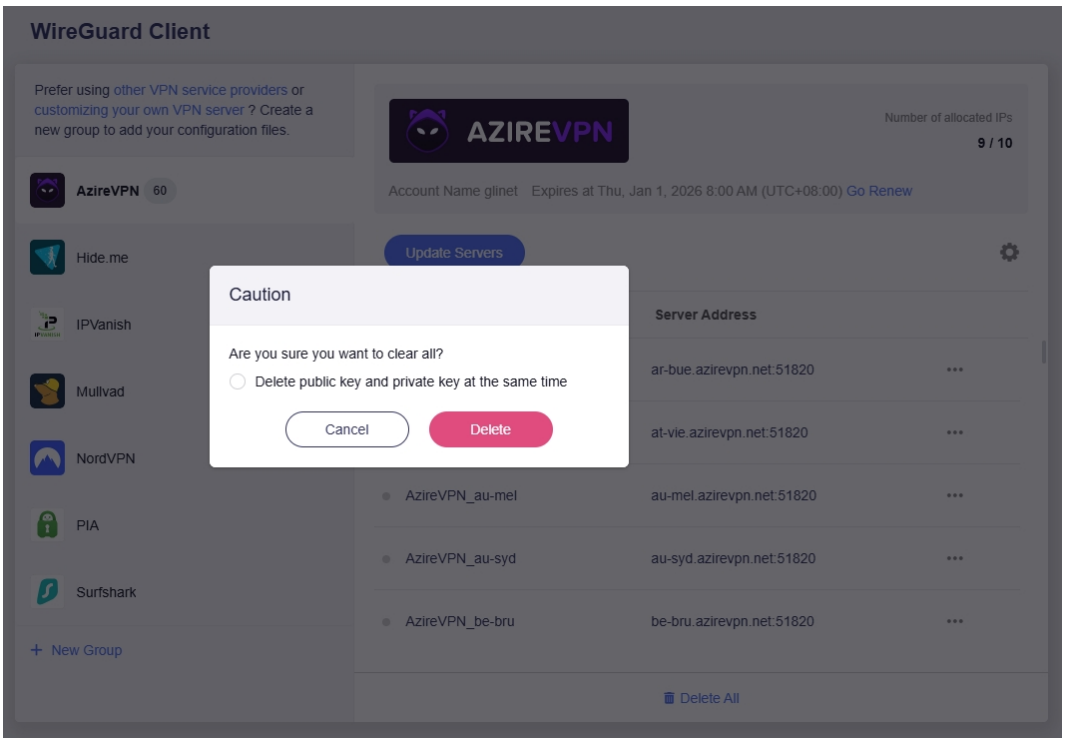
7. Odnowienie subskrypcji.

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



8. Usuń wszystkie pliki.

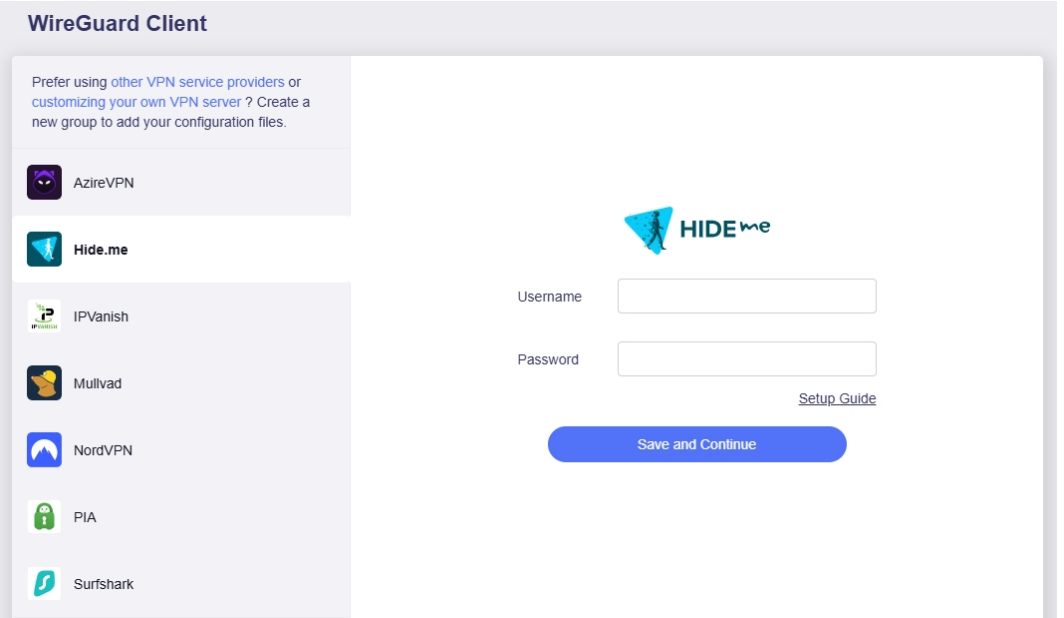
   Możesz kliknąć **Delete All**, aby jednym kliknięciem usunąć wszystkie pliki konfiguracyjne, oraz wybrać, czy jednocześnie usunąć klucze prywatny i publiczny.



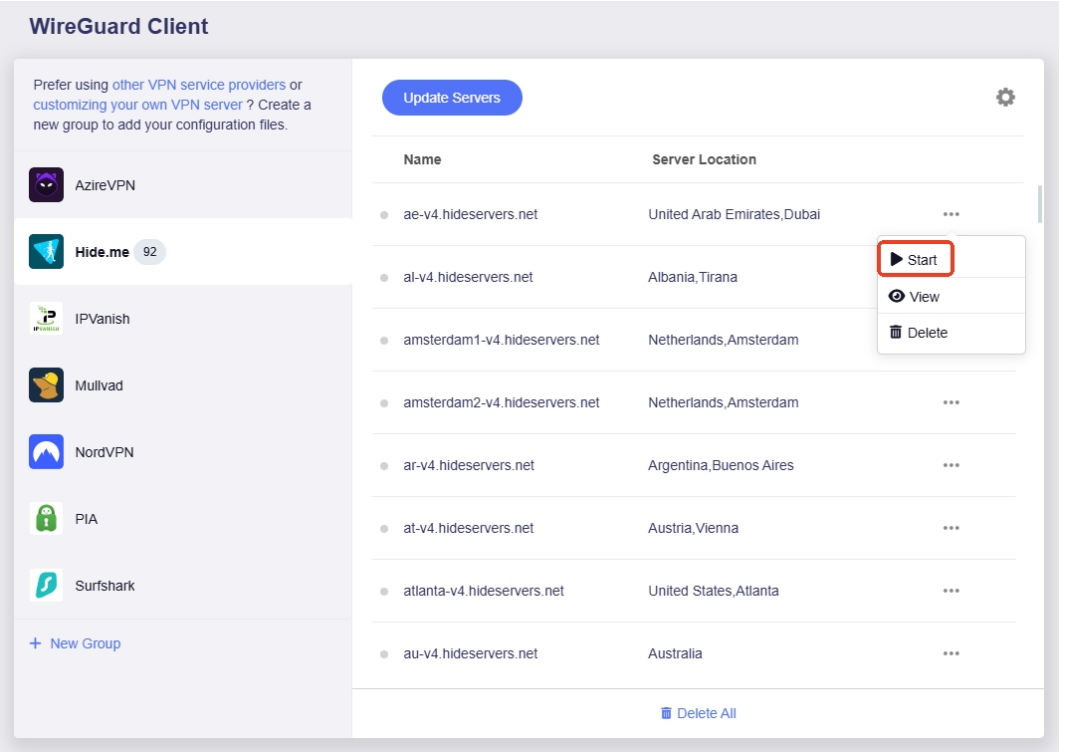
11.2.3 Konfiguracja Hide.me

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

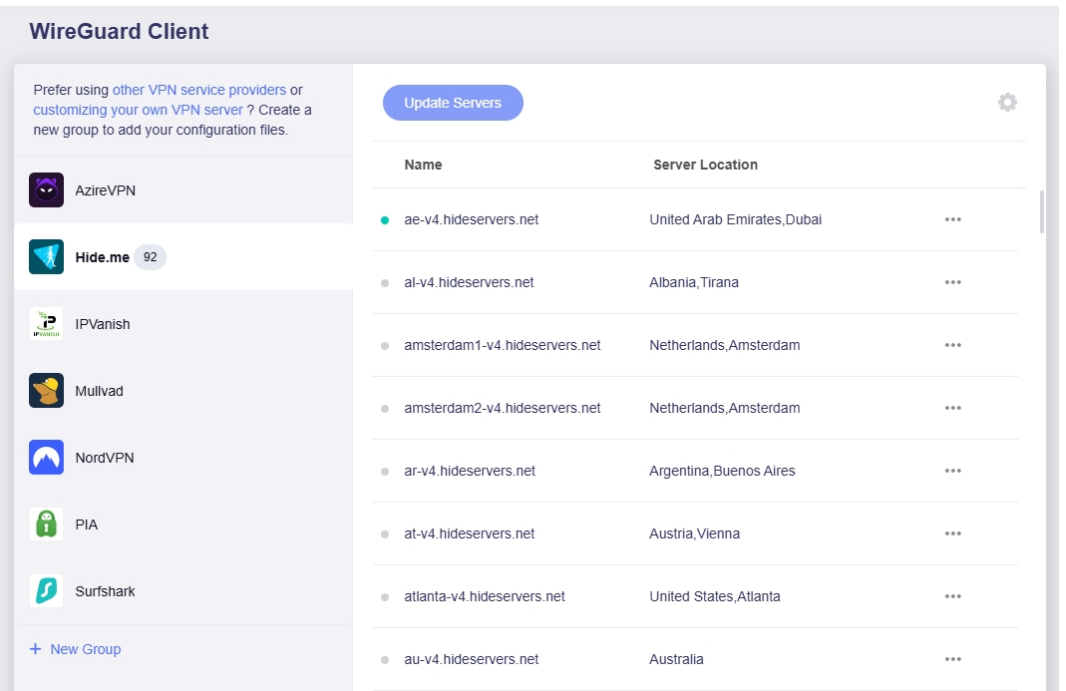
1. Zaloguj się do panelu administracyjnego routera i przejdź do **VPN** > **WireGuard Client** > **Hide.me**.
2. Wprowadź nazwę użytkownika i hasło, a następnie kliknij **Save and Continue**. Zostaną wygenerowane pliki konfiguracyjne dla każdego serwera.



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



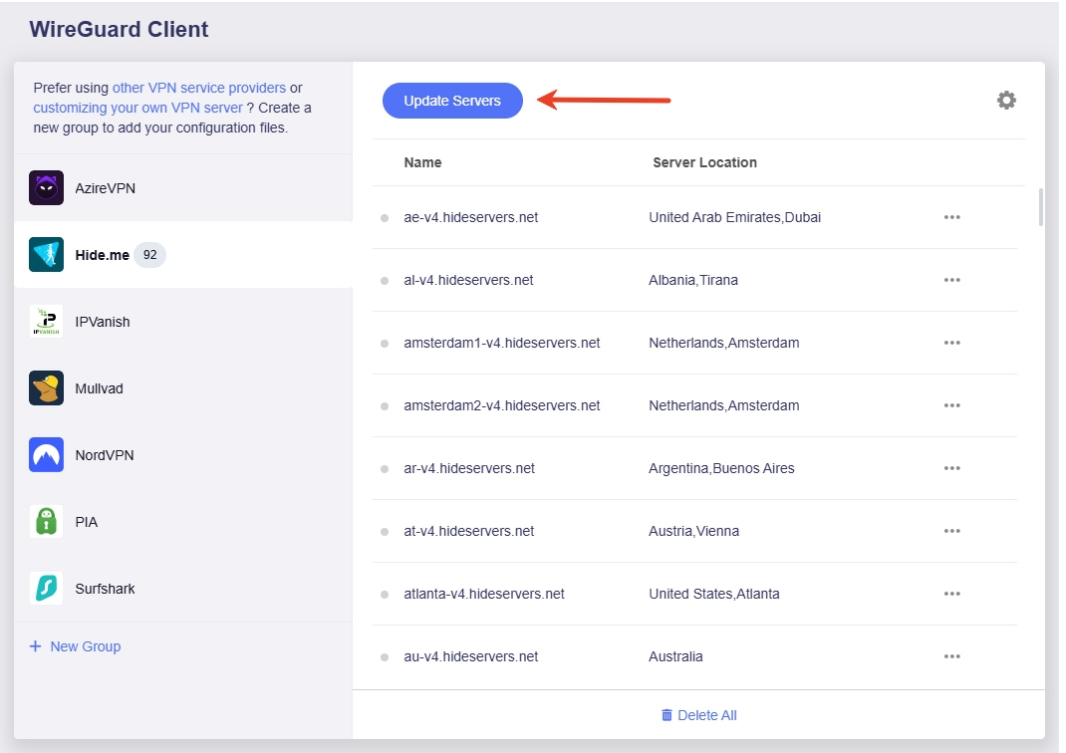
4. Po połączeniu obok pliku konfiguracyjnego pojawi się zielona kropka.



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

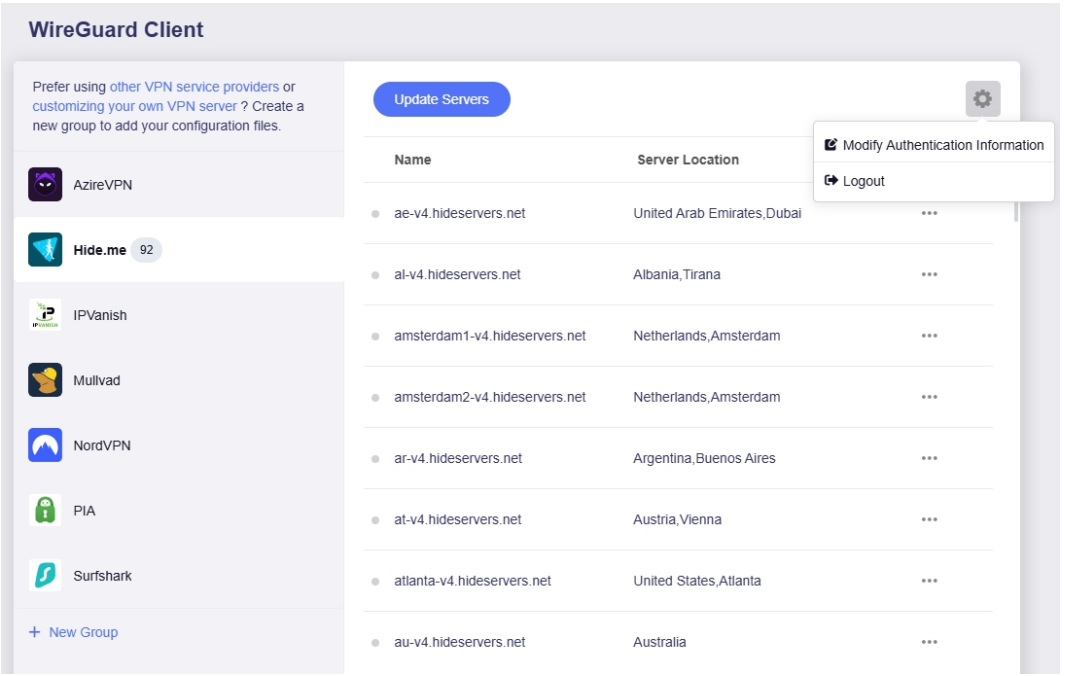
5. Zaktualizuj serwery.

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



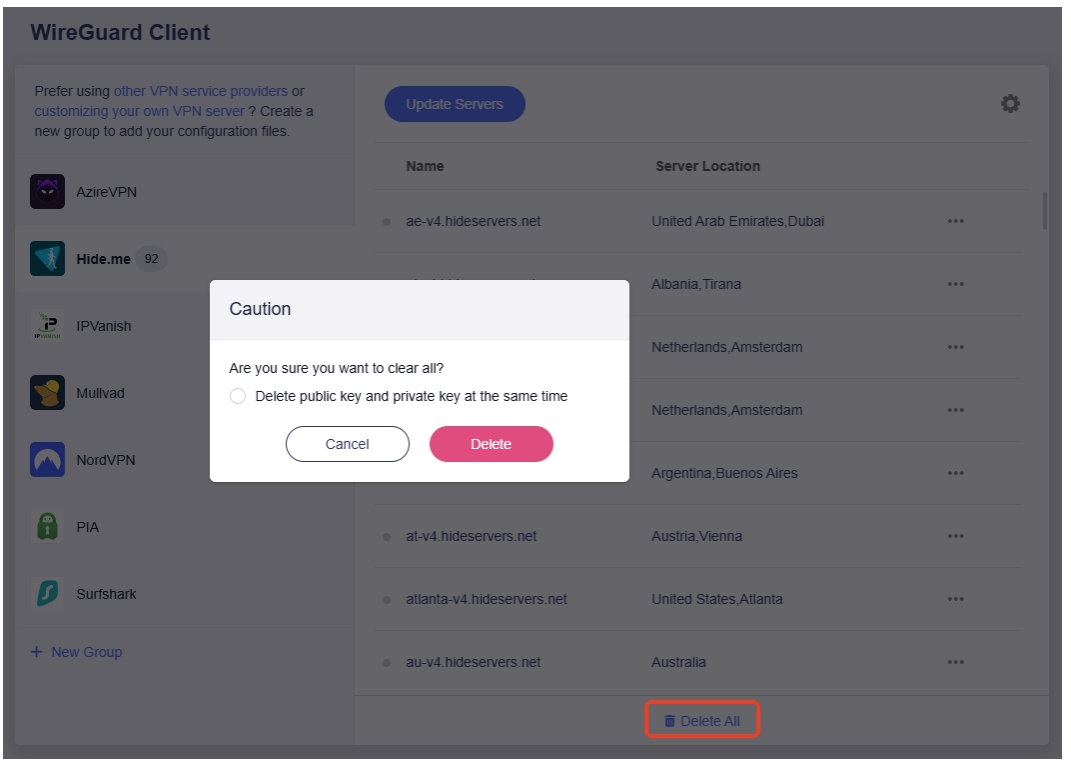
6. Zmiana danych logowania lub wylogowanie.

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



7. Usuń wszystkie pliki.

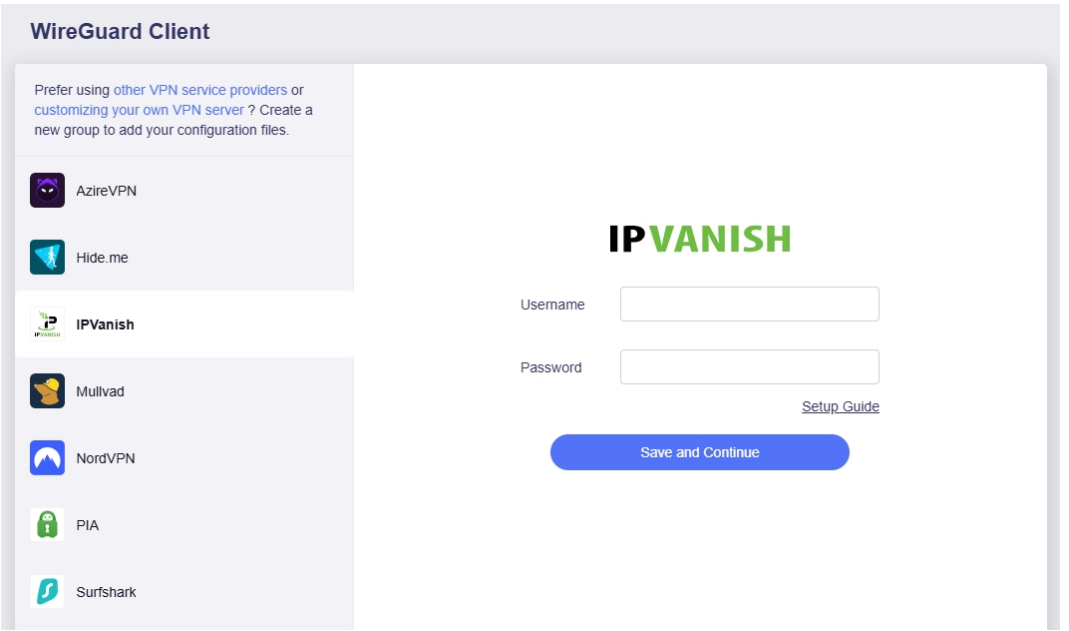
   Możesz kliknąć **Delete All**, aby jednym kliknięciem usunąć wszystkie pliki konfiguracyjne, oraz wybrać, czy jednocześnie usunąć klucze prywatny i publiczny.



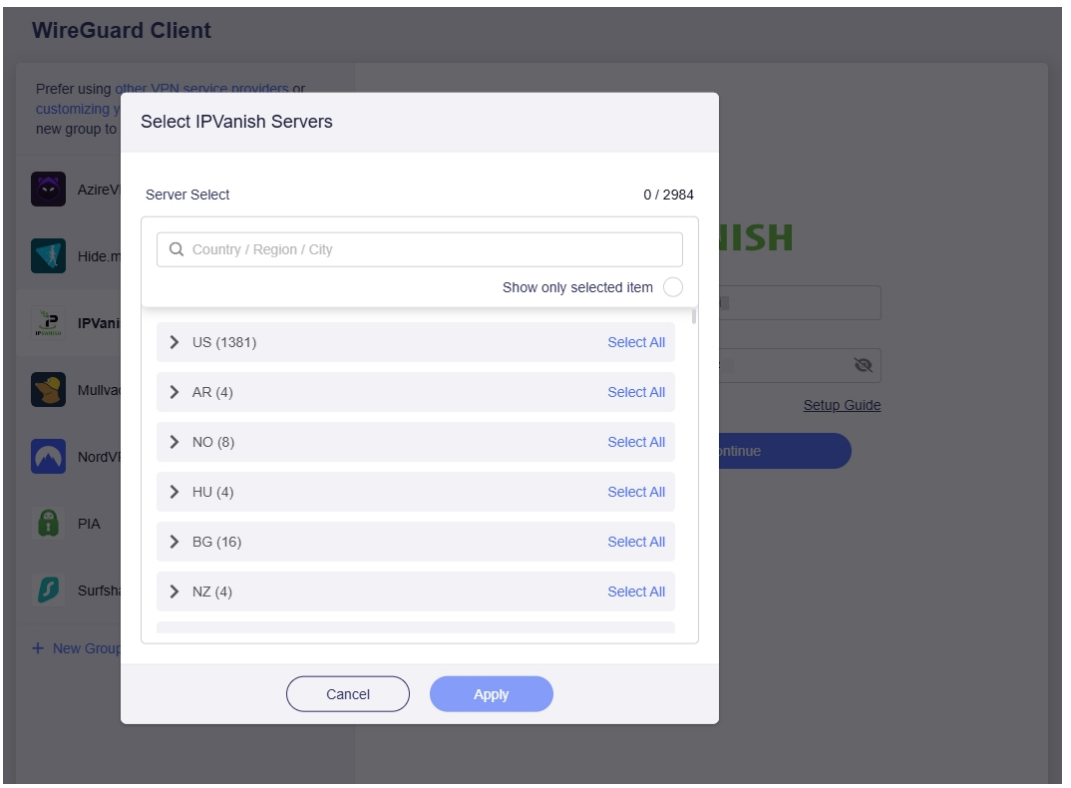
11.2.4 Konfiguracja IPVanish

Aby skonfigurować router jako klienta IPVanish, wykonaj poniższe czynności.

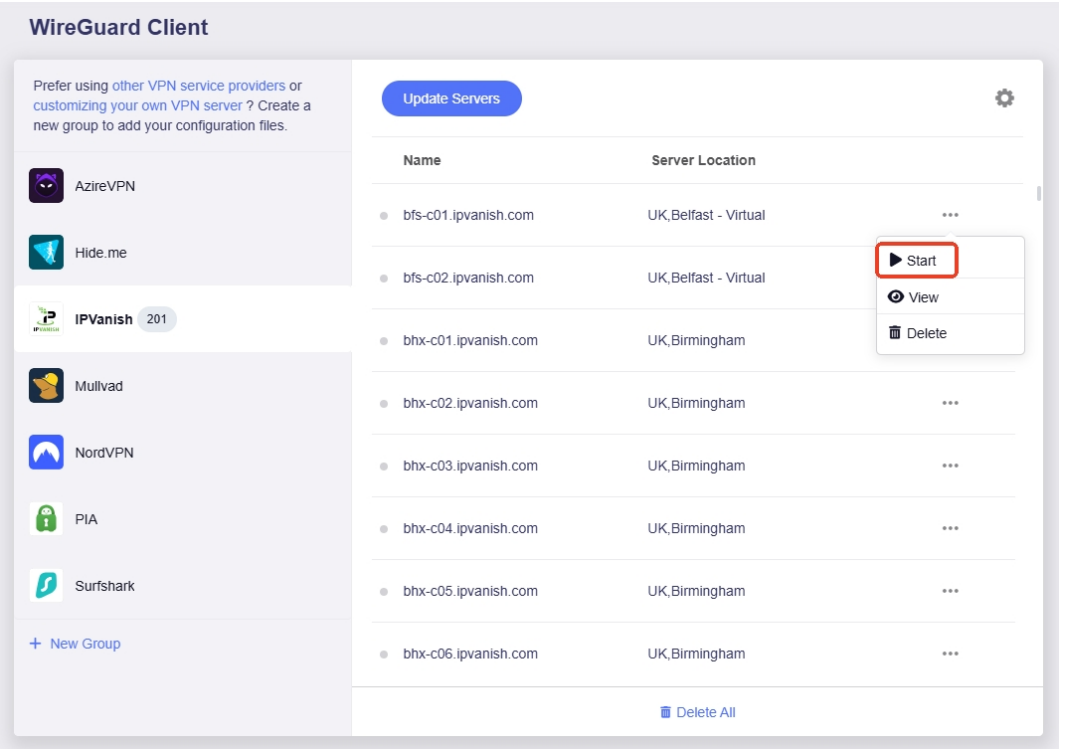
1. Zaloguj się do panelu administracyjnego routera i przejdź do **VPN** > **WireGuard Client** > **IPVanish**.
2. Wprowadź nazwę użytkownika i hasło, a następnie kliknij **Save and Continue**.



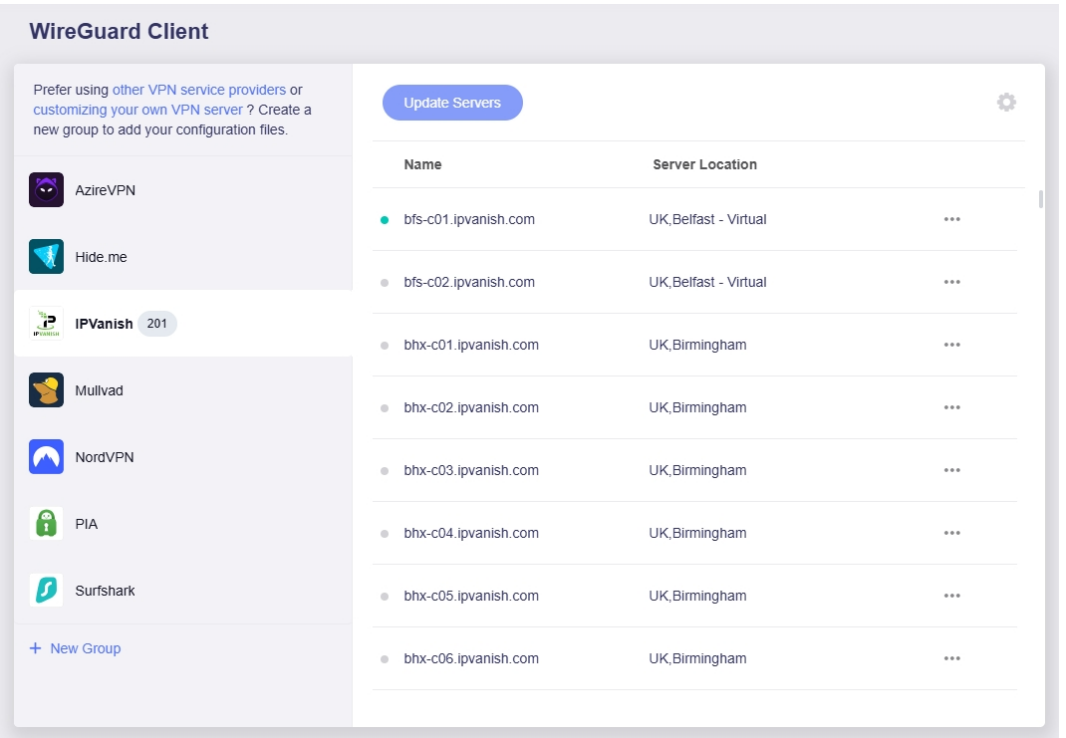
3. Wybierz serwery, z którymi chcesz się połączyć, i kliknij **Apply**.



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



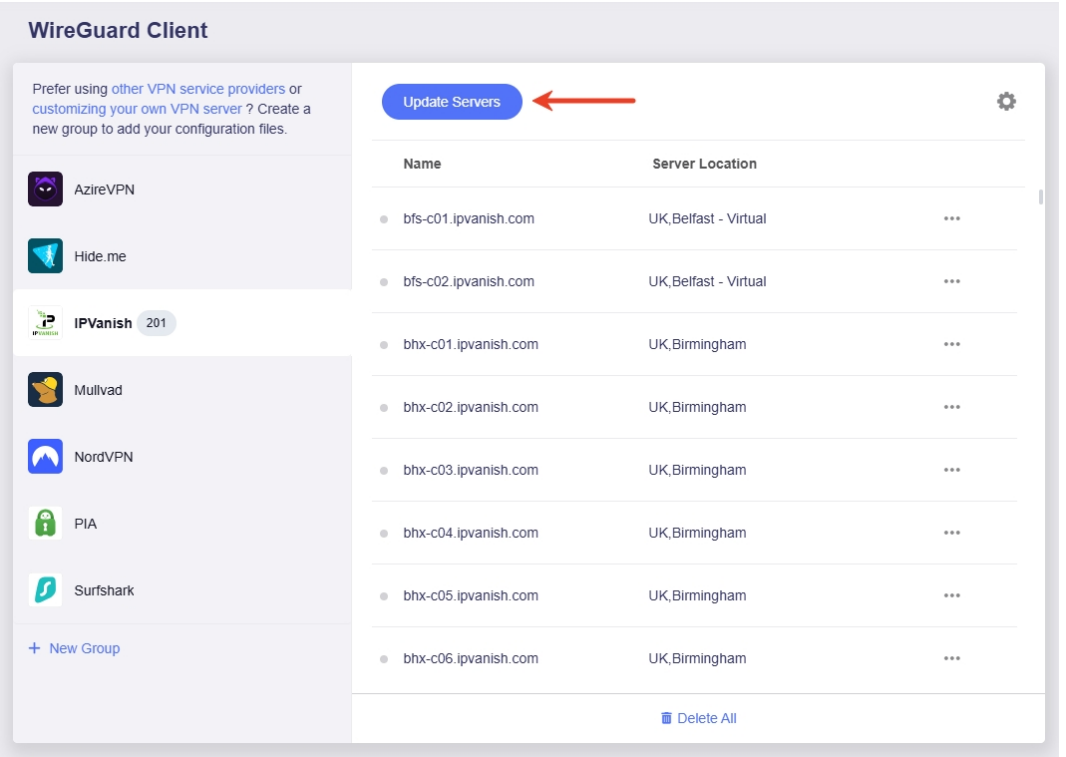
5. Po połączeniu obok pliku konfiguracyjnego pojawi się zielona kropka.



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

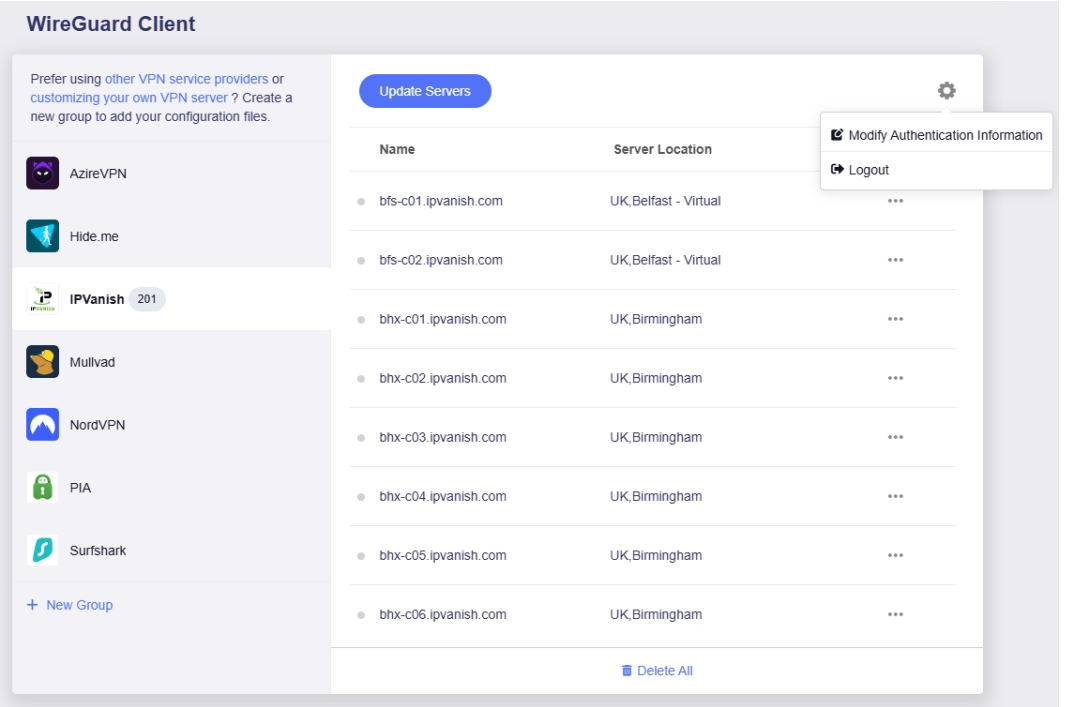
6. Zaktualizuj serwery.

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



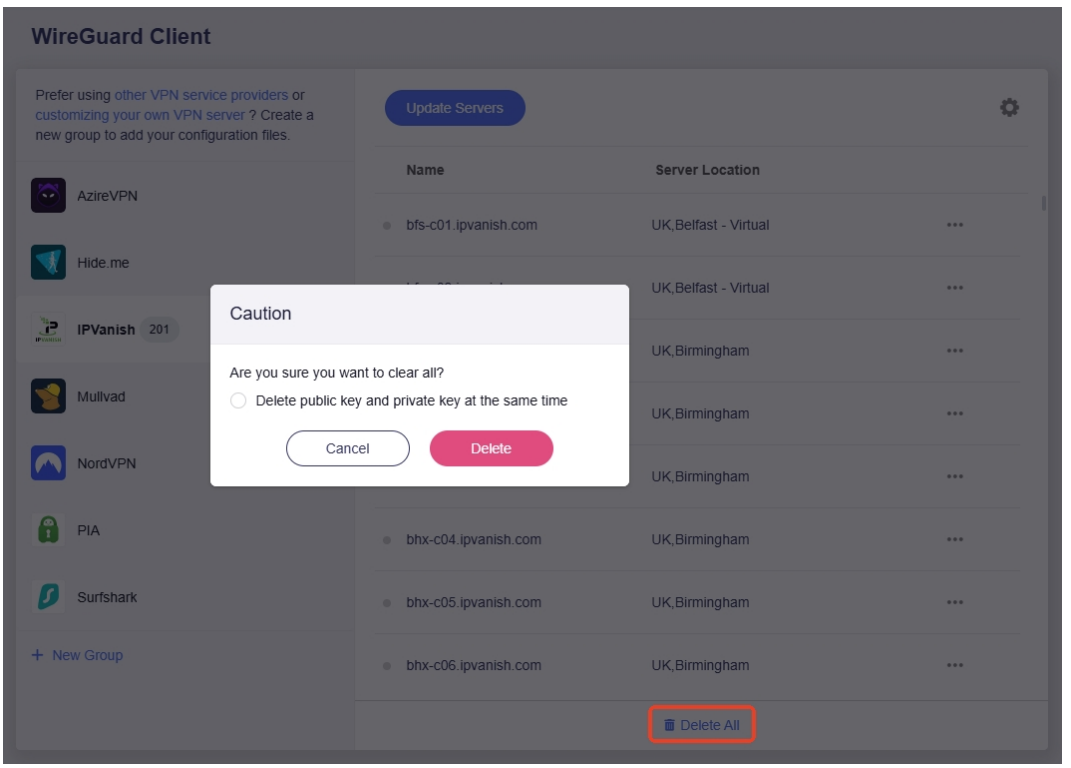
7. Zmiana danych logowania lub wylogowanie.

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



8. Usuń wszystkie pliki.

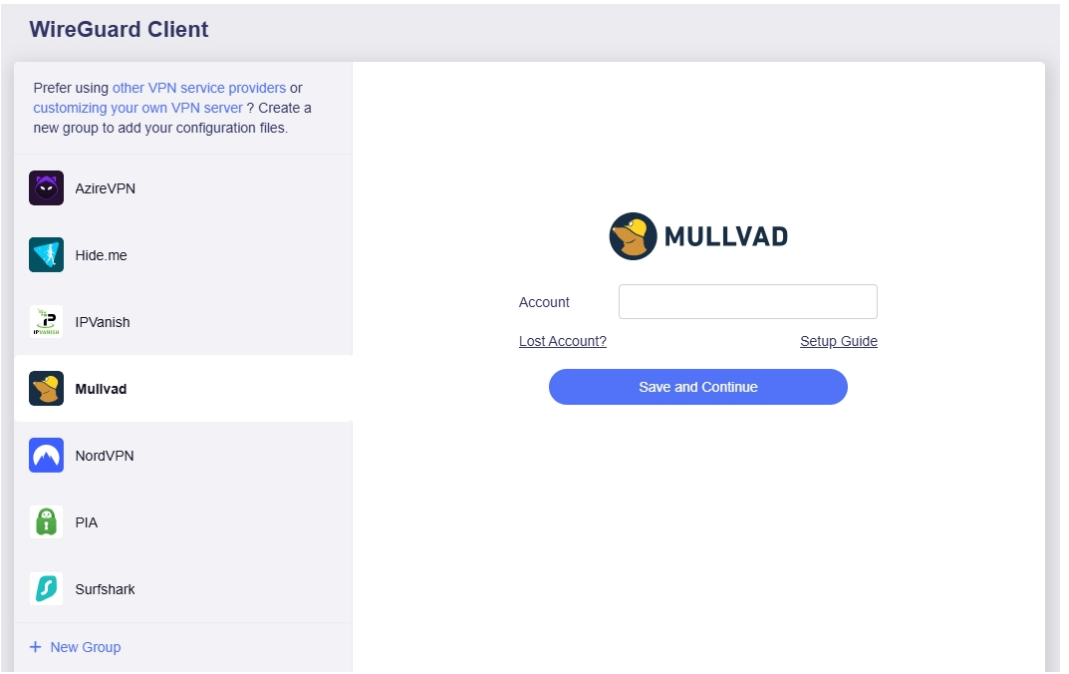
   Możesz kliknąć **Delete All**, aby jednym kliknięciem usunąć wszystkie pliki konfiguracyjne, oraz wybrać, czy jednocześnie usunąć klucze prywatny i publiczny.



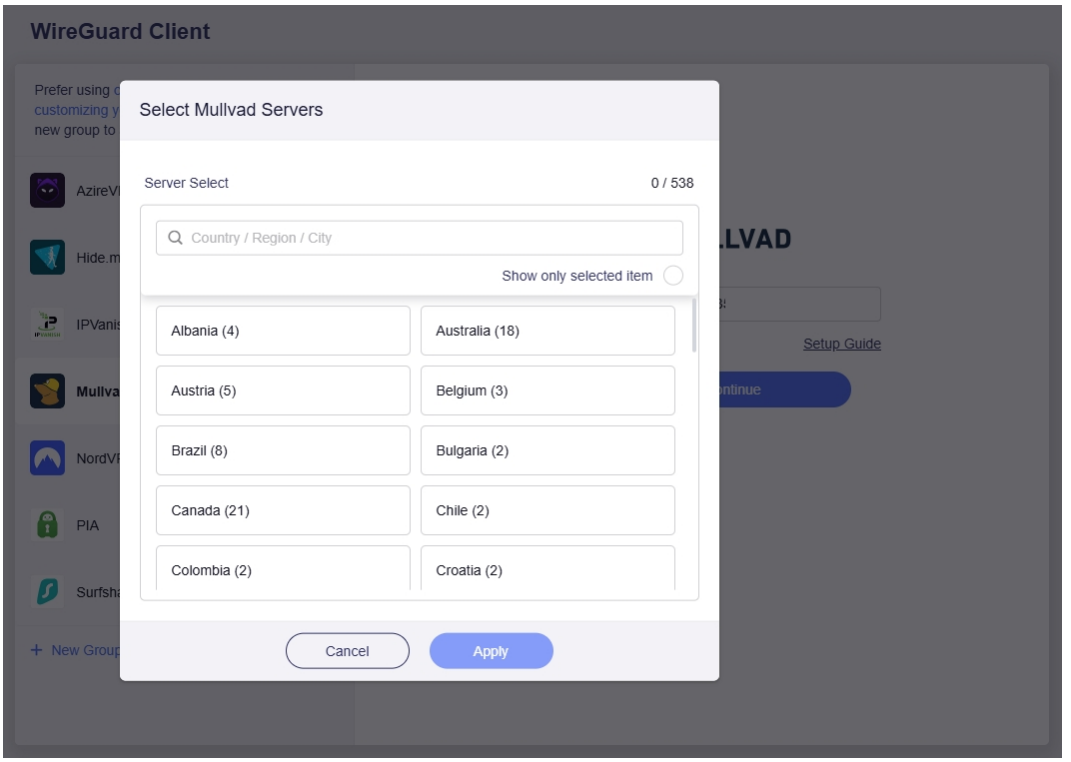
11.2.5 Konfiguracja Mullvad

Aby skonfigurować router jako klienta Mullvad, wykonaj poniższe czynności.

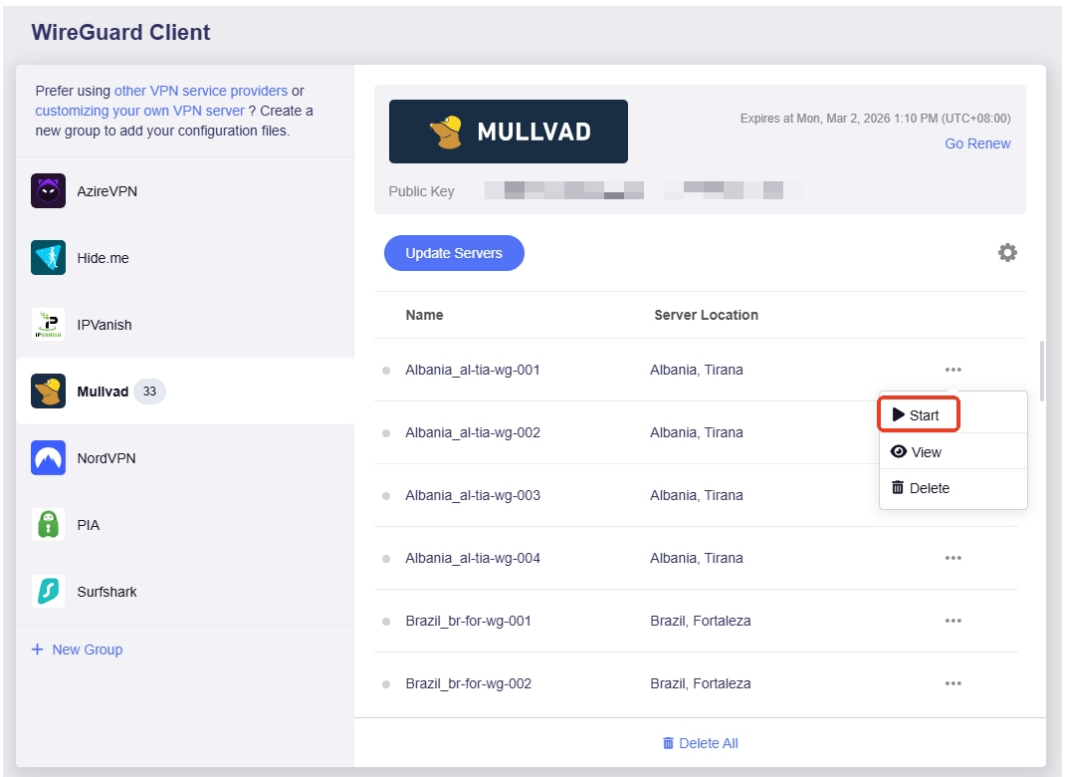
1. Zaloguj się do panelu administracyjnego routera i przejdź do **VPN** > **WireGuard Client** > **Mullvad**.
2. Wprowadź nazwę użytkownika i hasło, a następnie kliknij **Save and Continue**.



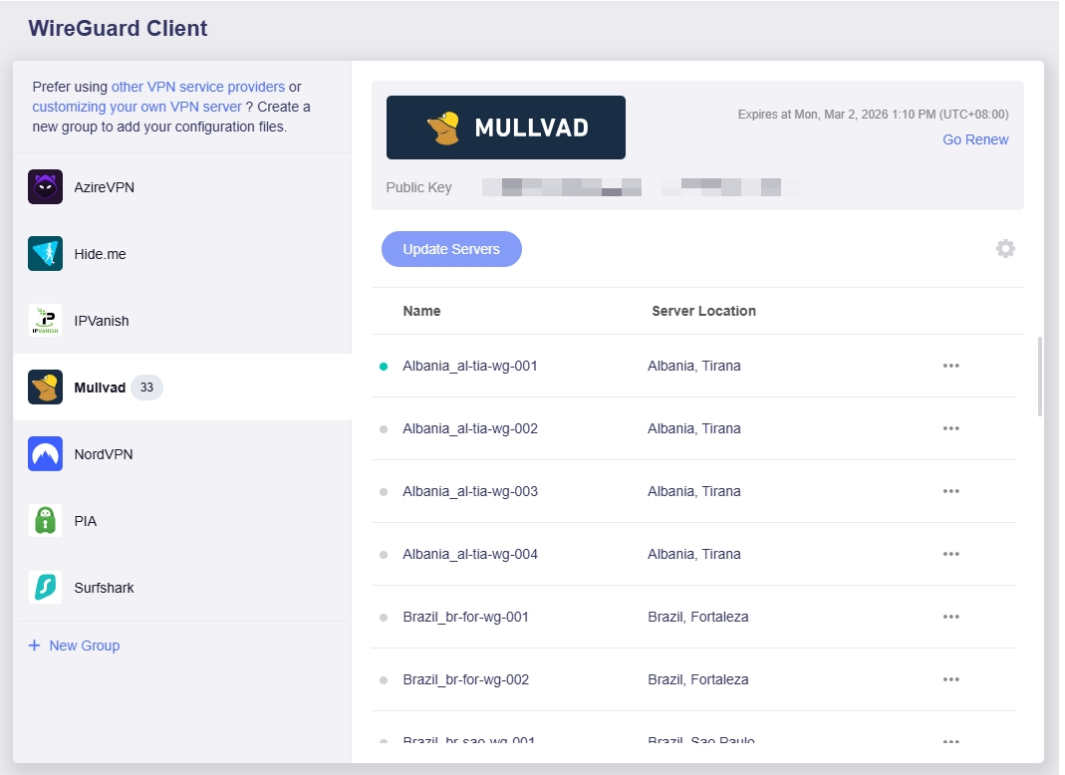
3. Wybierz serwery, z którymi chcesz się połączyć, i kliknij **Apply**.



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



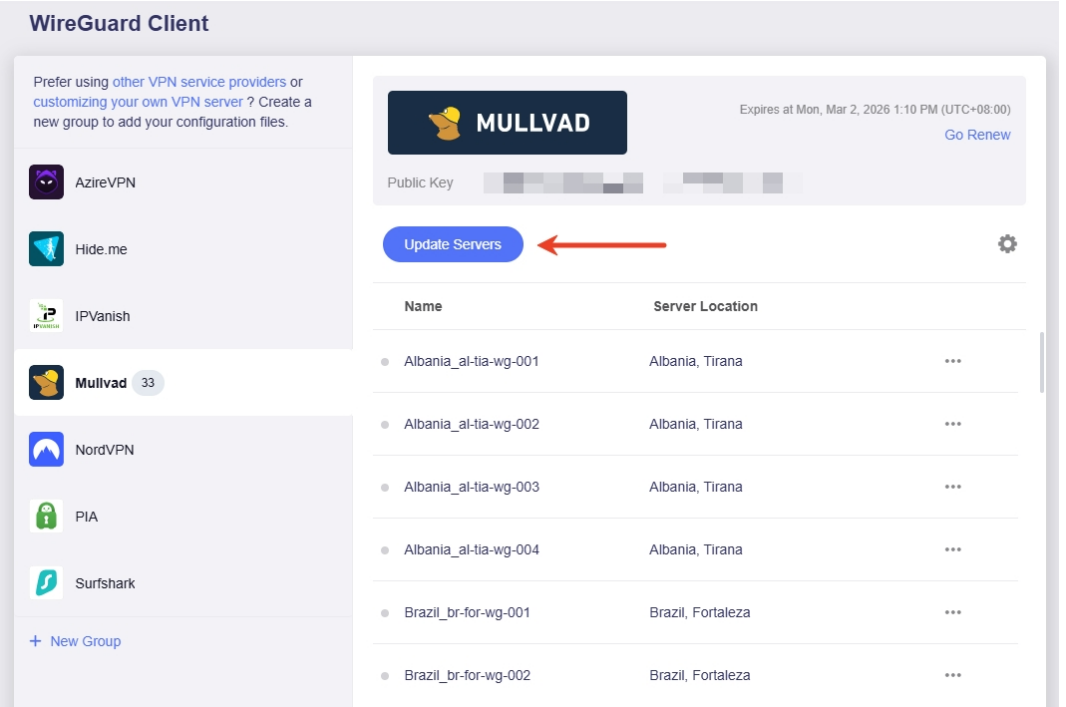
5. Po połączeniu obok pliku konfiguracyjnego pojawi się zielona kropka.



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

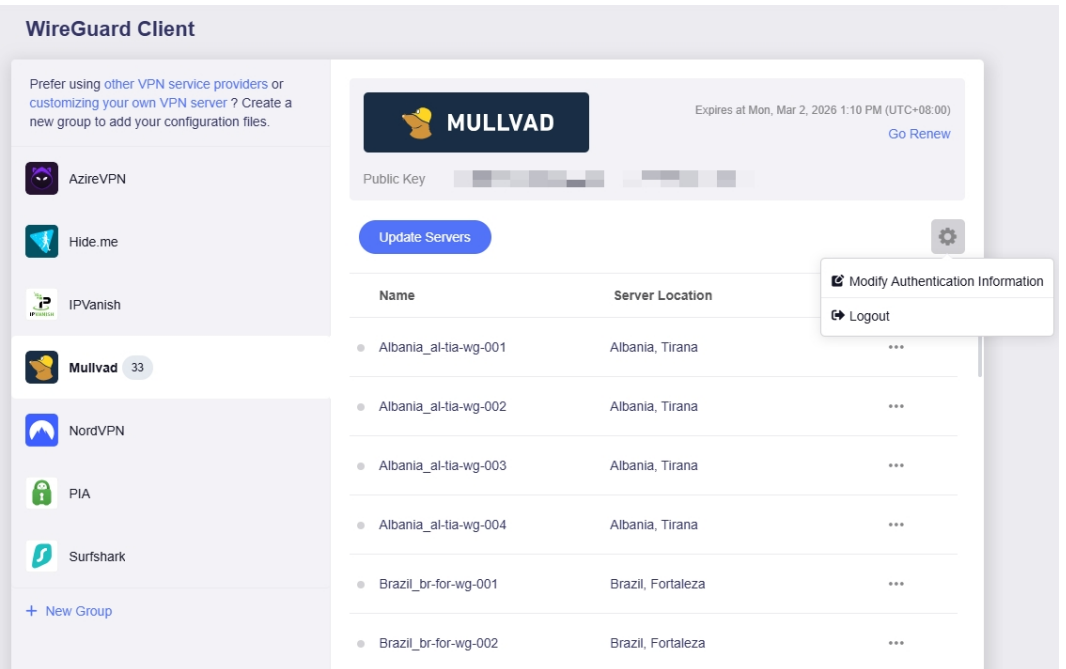
6. Zaktualizuj serwery.

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



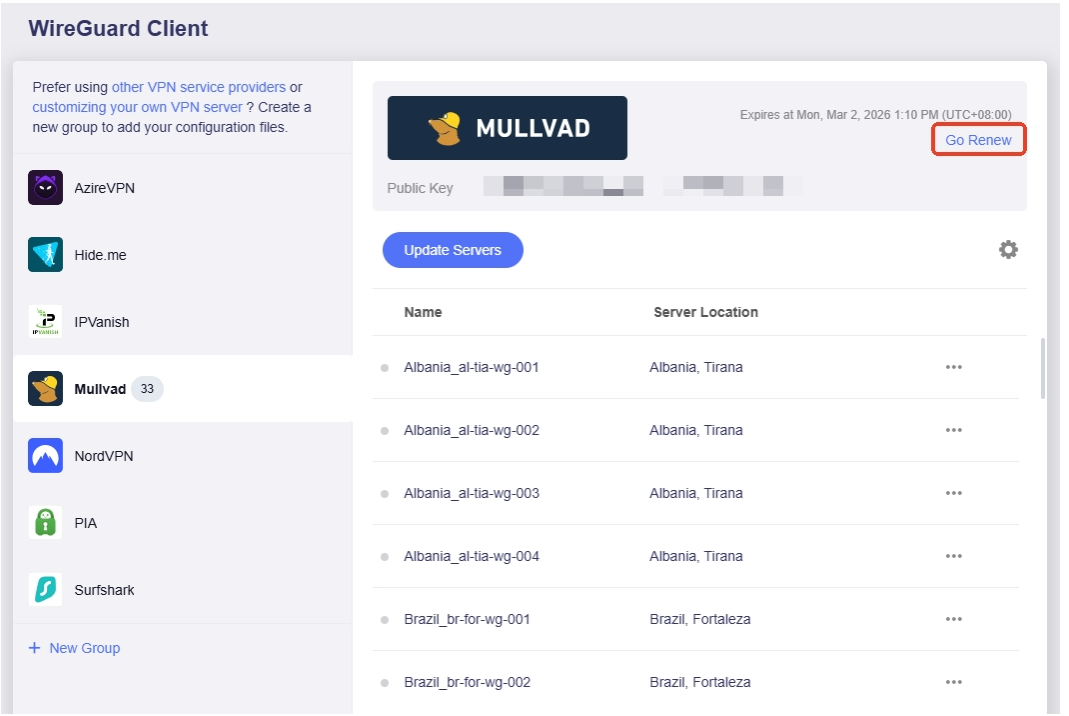
7. Zmiana danych logowania lub wylogowanie.

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



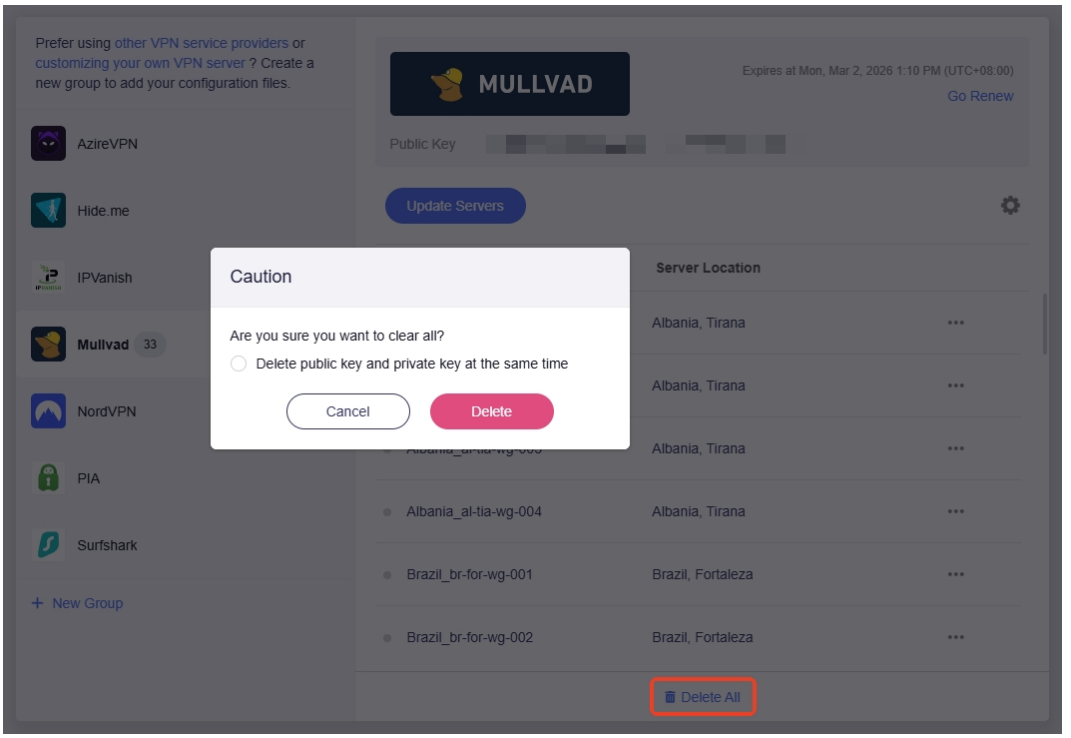
8. Odnowienie subskrypcji.

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



9. Usuń wszystkie pliki.

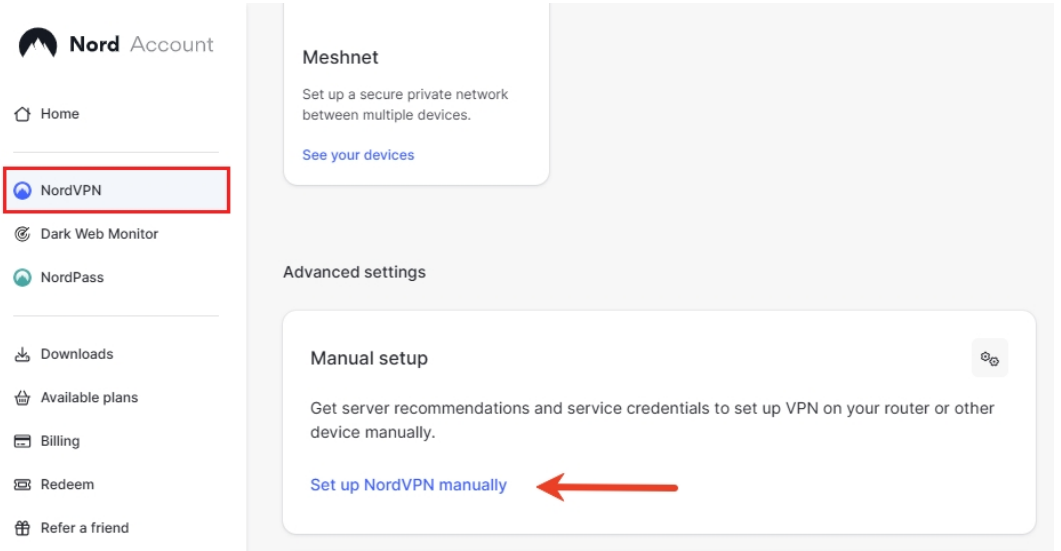
   Możesz kliknąć **Delete All**, aby jednym kliknięciem usunąć wszystkie pliki konfiguracyjne, oraz wybrać, czy jednocześnie usunąć klucze prywatny i publiczny.



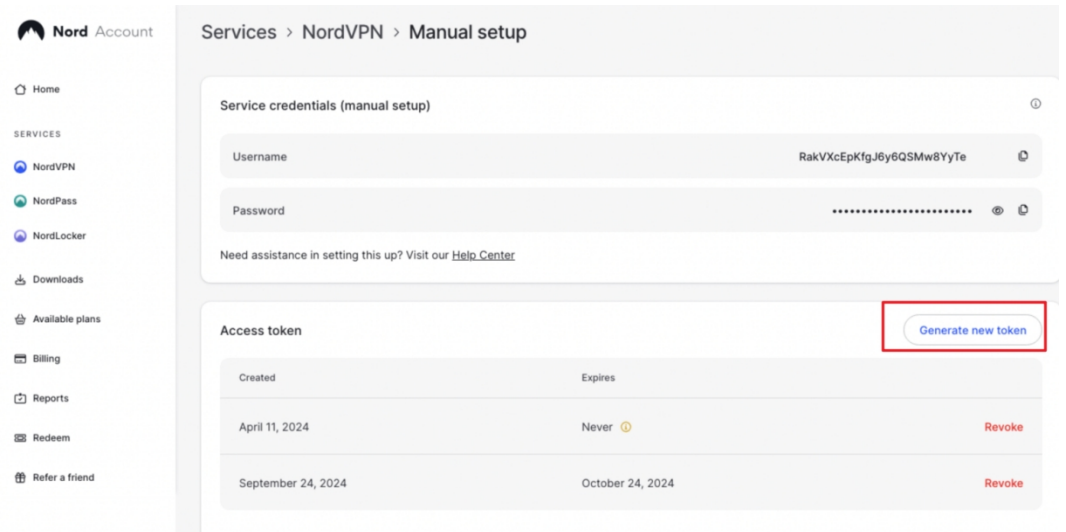
11.2.6 Konfiguracja NordVPN

Aby skonfigurować router jako klienta NordVPN, wykonaj poniższe czynności.

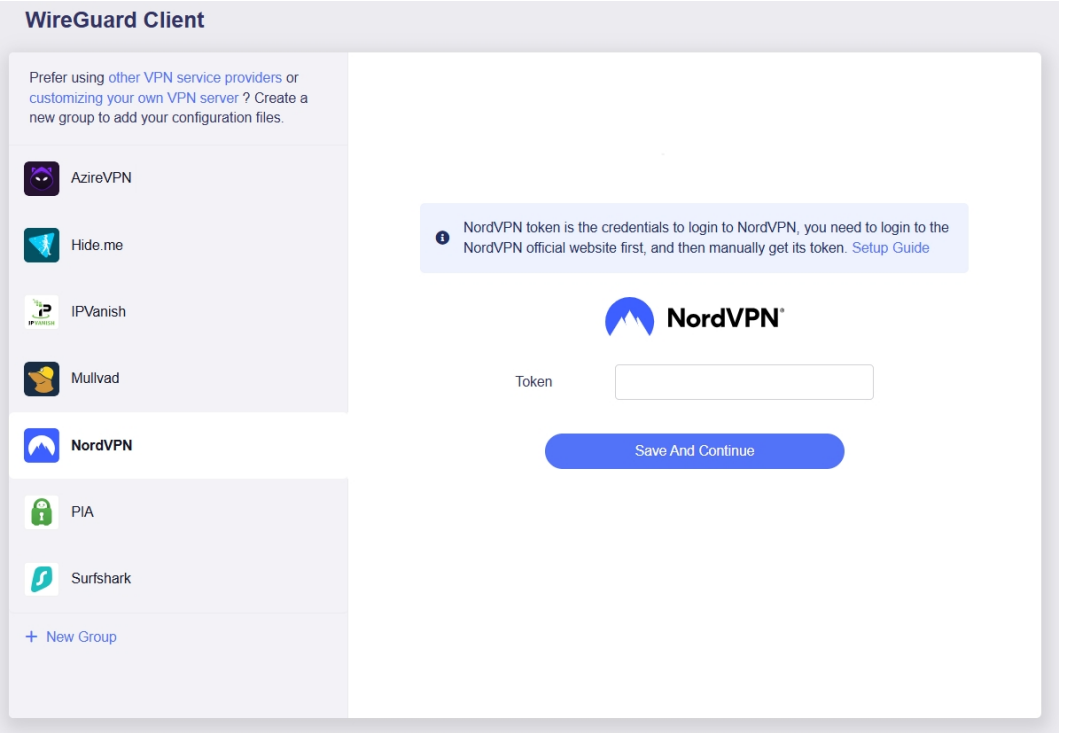
1. Zaloguj się na swoje konto internetowe NordVPN tutaj.
2. W panelu Nord kliknij **NordVPN**, a następnie **Set up NordVPN manually**.



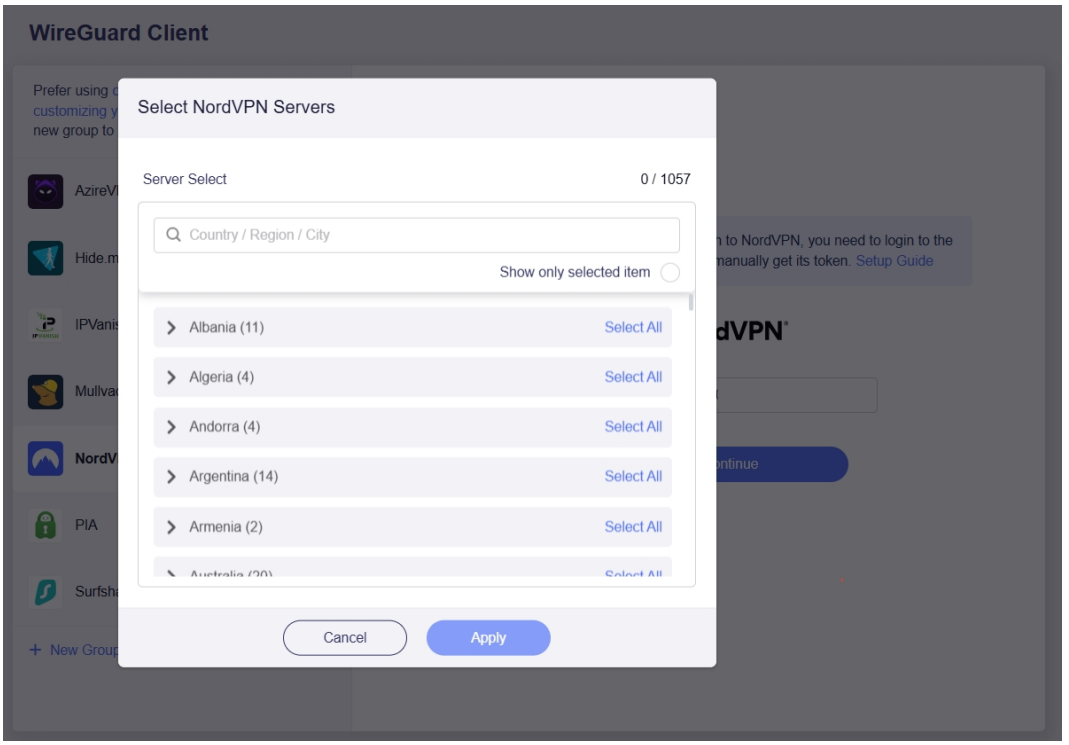
Znajdziesz tam **Access Token**. Utwórz token dostępu i skopiuj go do późniejszego użycia.



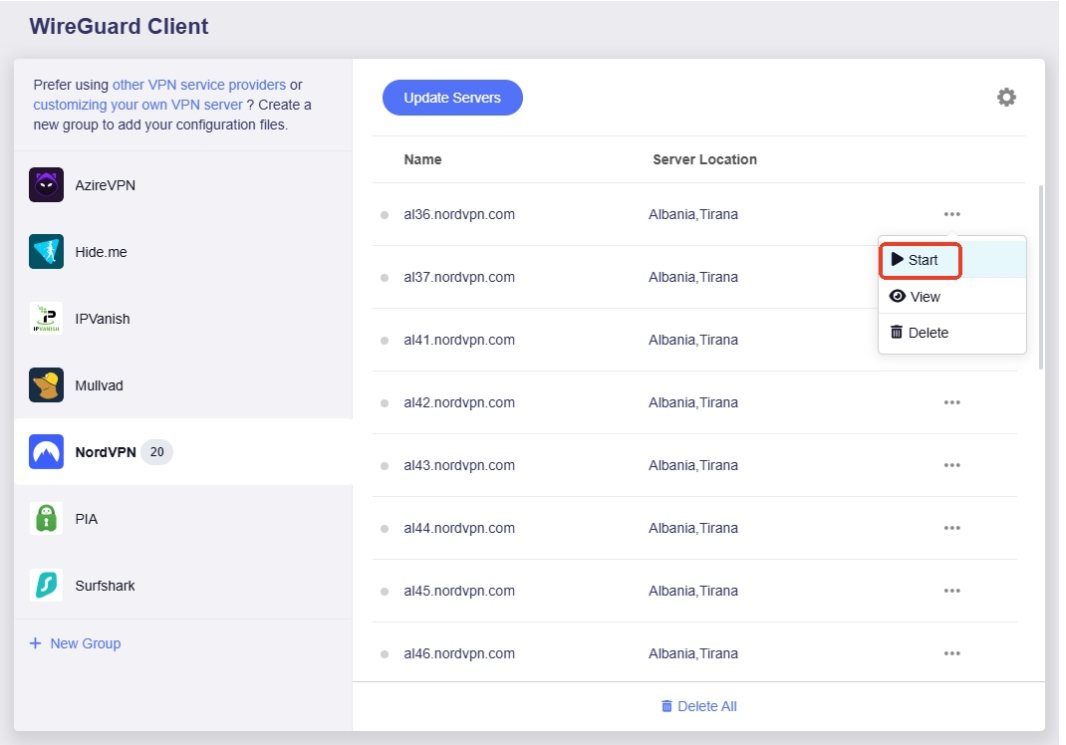
3. Zaloguj się do panelu administracyjnego routera i przejdź do **VPN** > **WireGuard Client** > **NordVPN**.
4. Wprowadź token i kliknij **Save and Continue**.



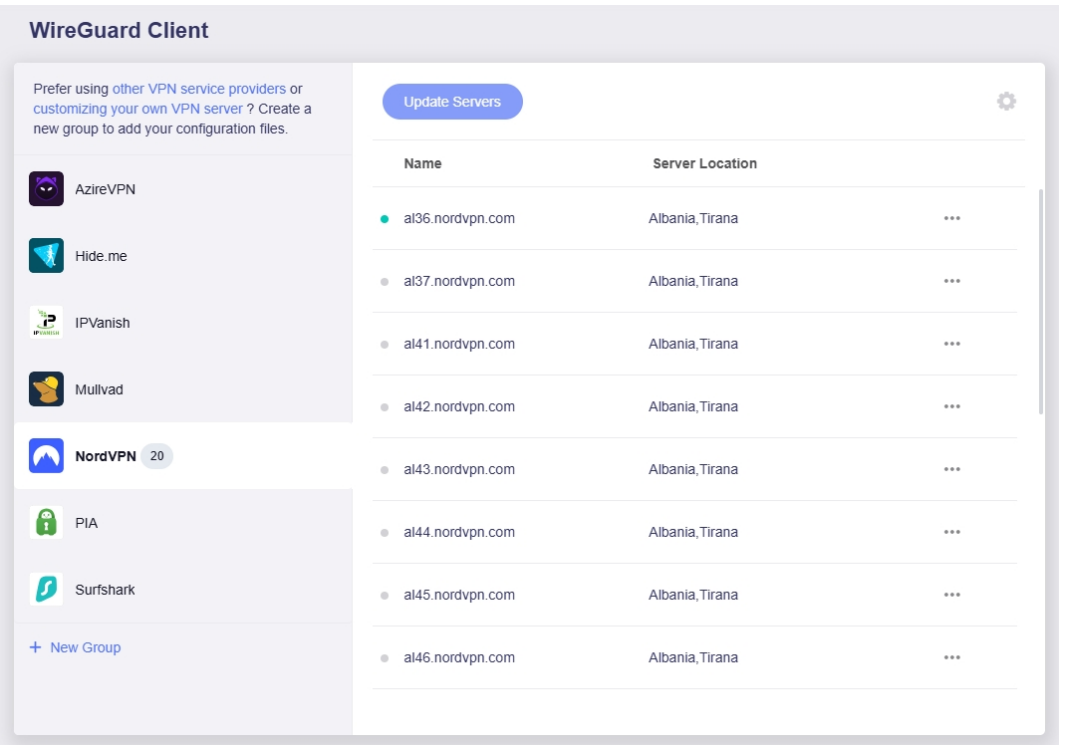
5. Wybierz serwery, z którymi chcesz się połączyć, i kliknij **Apply**.



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



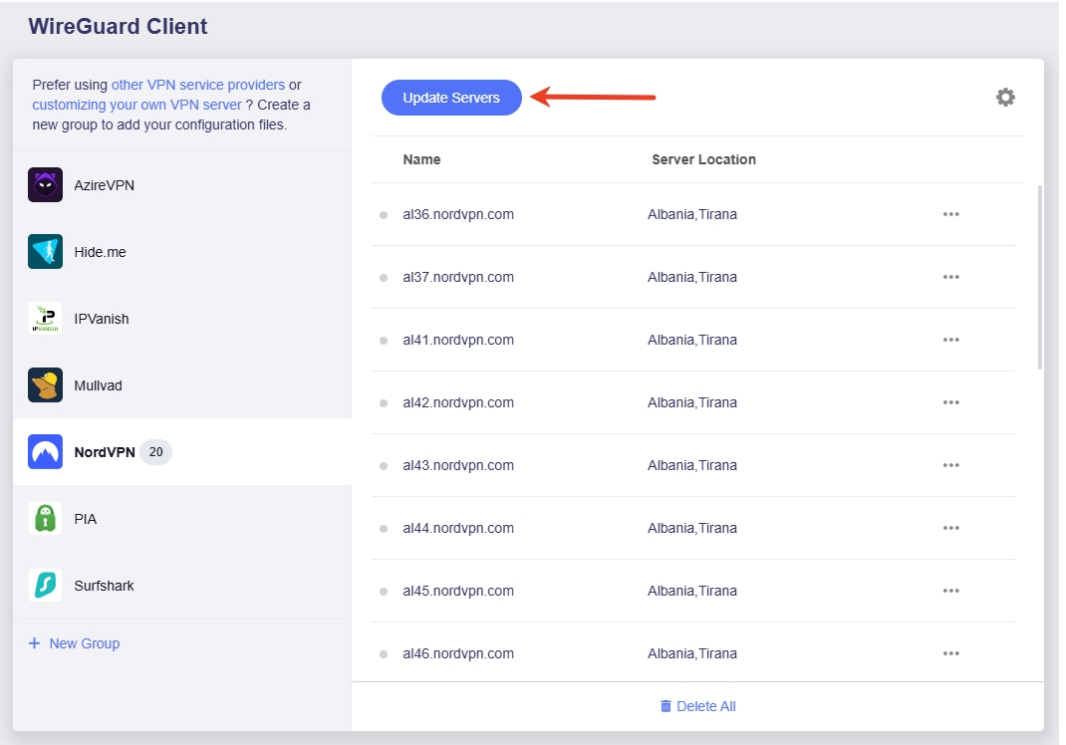
7. Po połączeniu obok pliku konfiguracyjnego pojawi się zielona kropka.



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

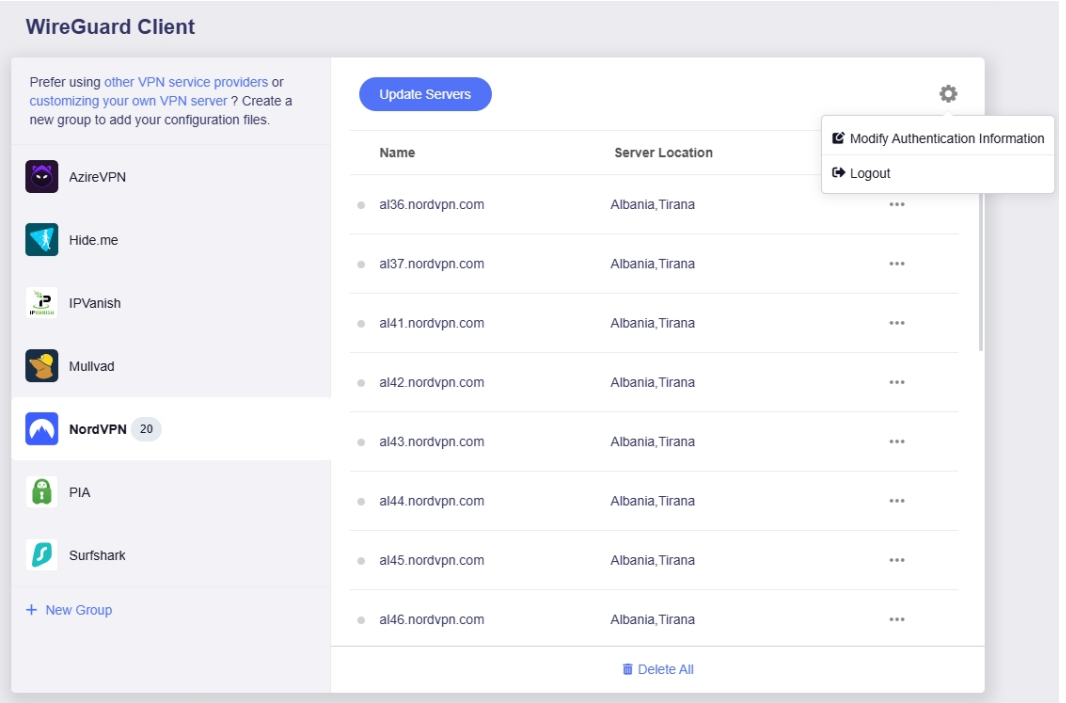
8. Zaktualizuj serwery.

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



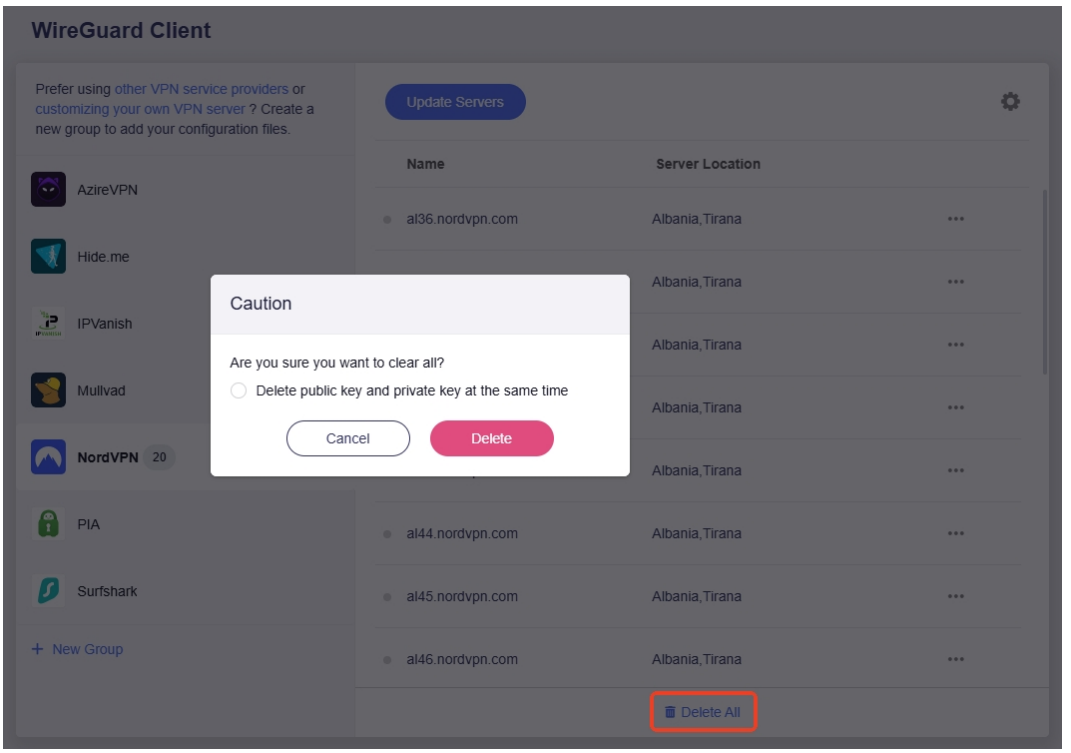
9. Zmiana danych logowania lub wylogowanie.

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



10. Usuń wszystkie pliki.

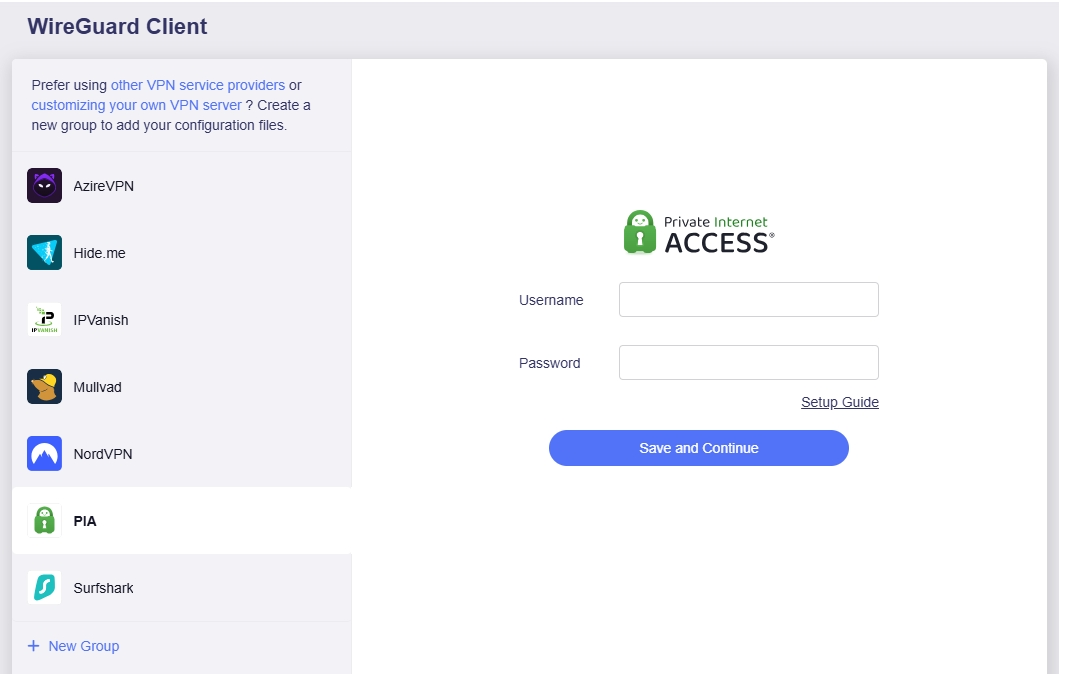
    Możesz kliknąć **Delete All**, aby jednym kliknięciem usunąć wszystkie pliki konfiguracyjne, oraz wybrać, czy jednocześnie usunąć klucze prywatny i publiczny.



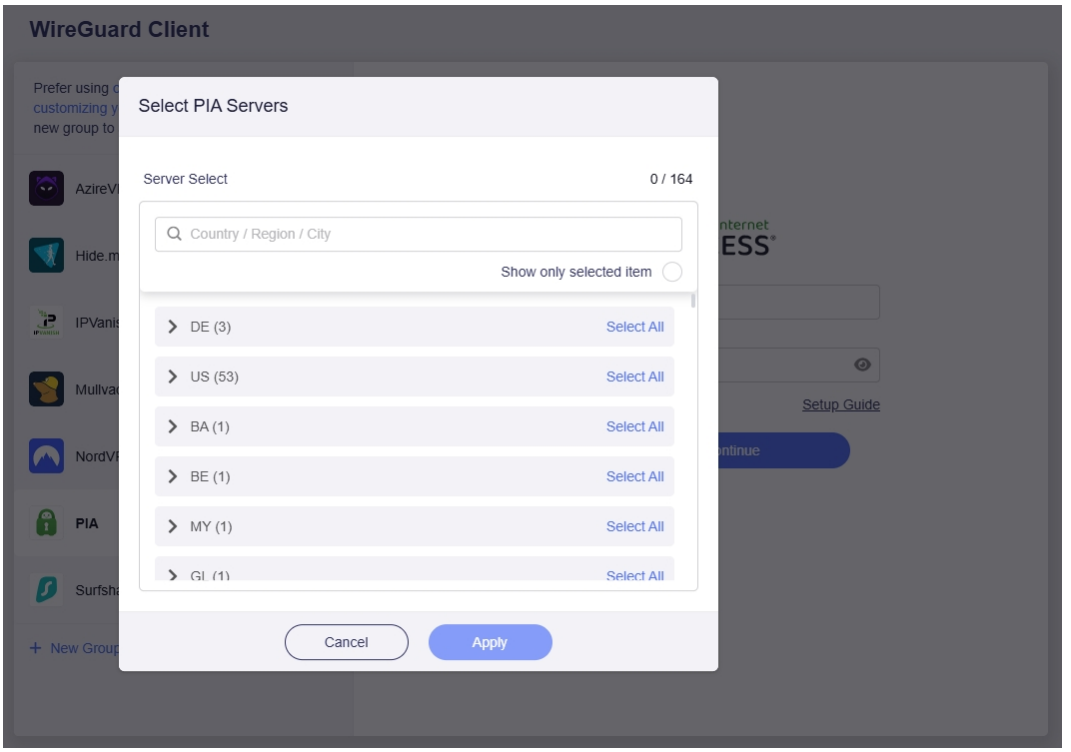
11.2.7 Konfiguracja PIA (Private Internet Access)

Aby skonfigurować router jako klienta PIA, wykonaj poniższe czynności.

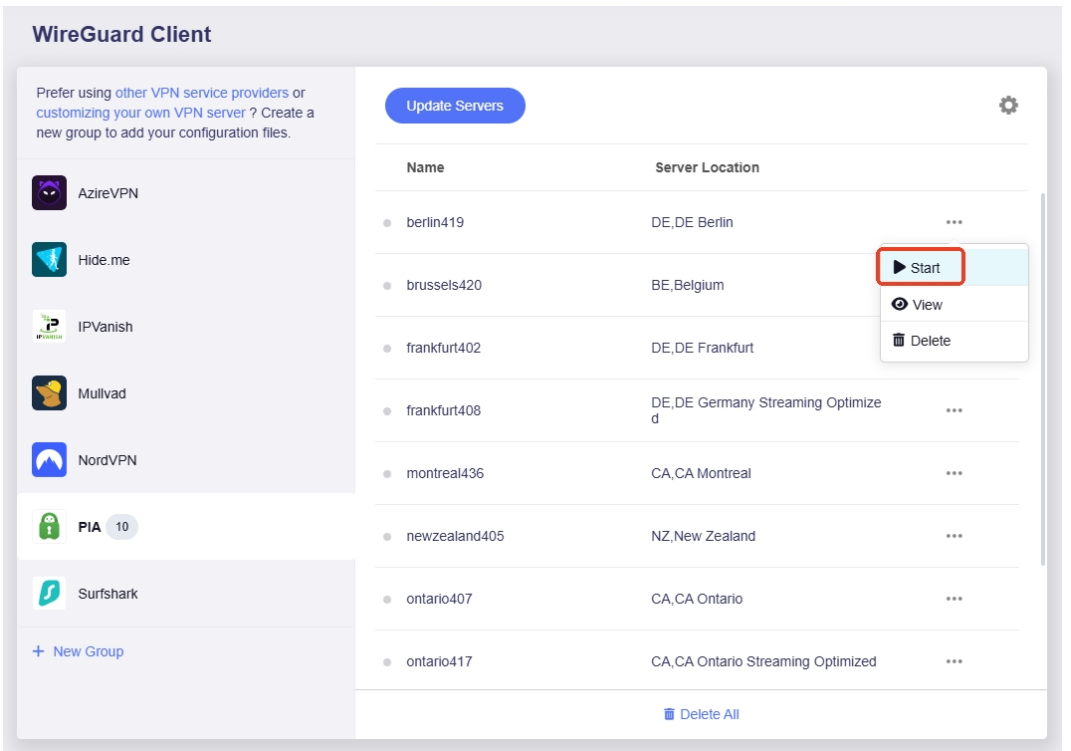
1. Zaloguj się do panelu administracyjnego routera i przejdź do **VPN** > **WireGuard Client** > **PIA**.
2. Wprowadź nazwę użytkownika i hasło, a następnie kliknij **Save and Continue**.



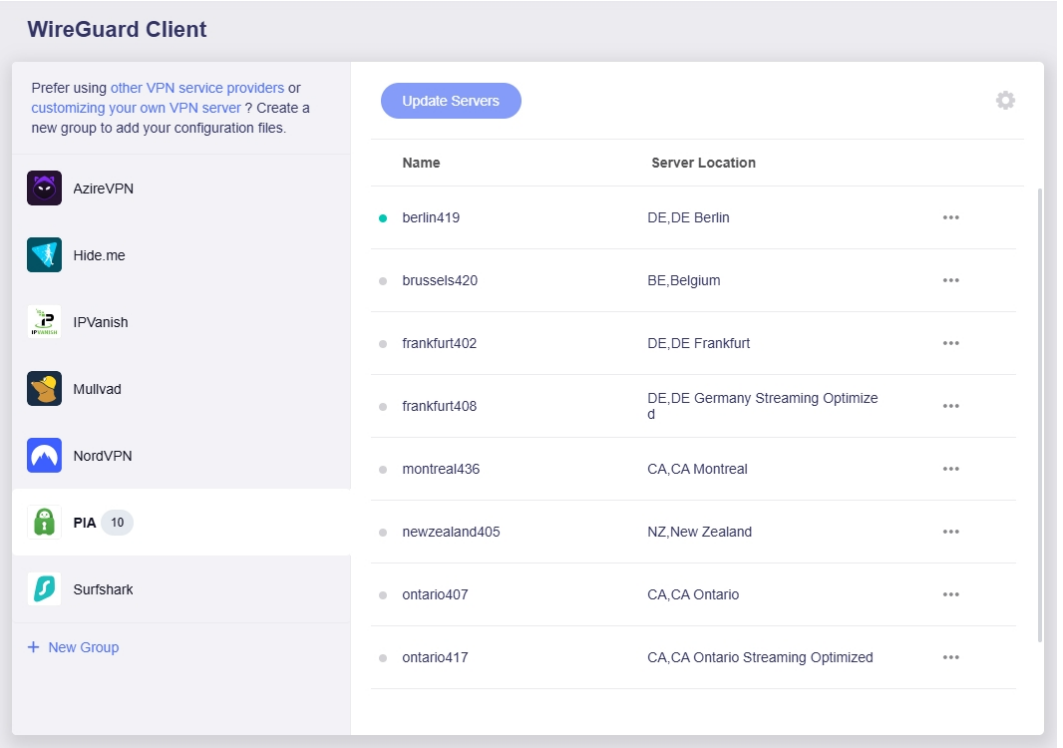
3. Wybierz serwery, z którymi chcesz się połączyć, i kliknij **Apply**.



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



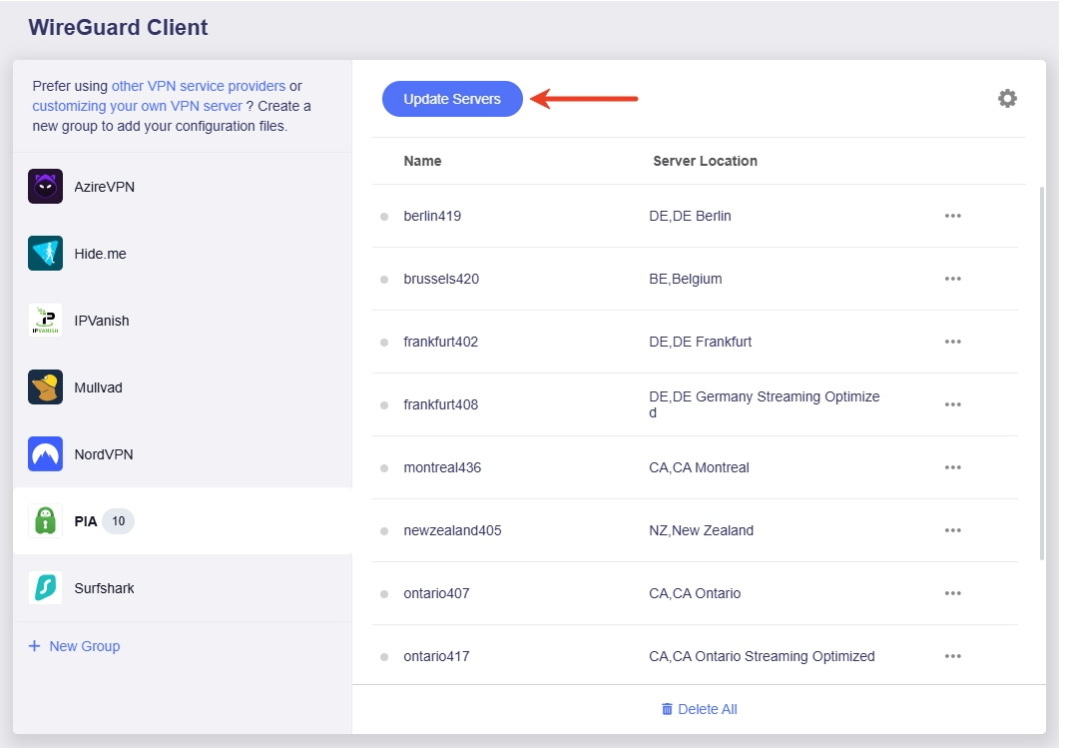
5. Po połączeniu obok pliku konfiguracyjnego pojawi się zielona kropka.



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

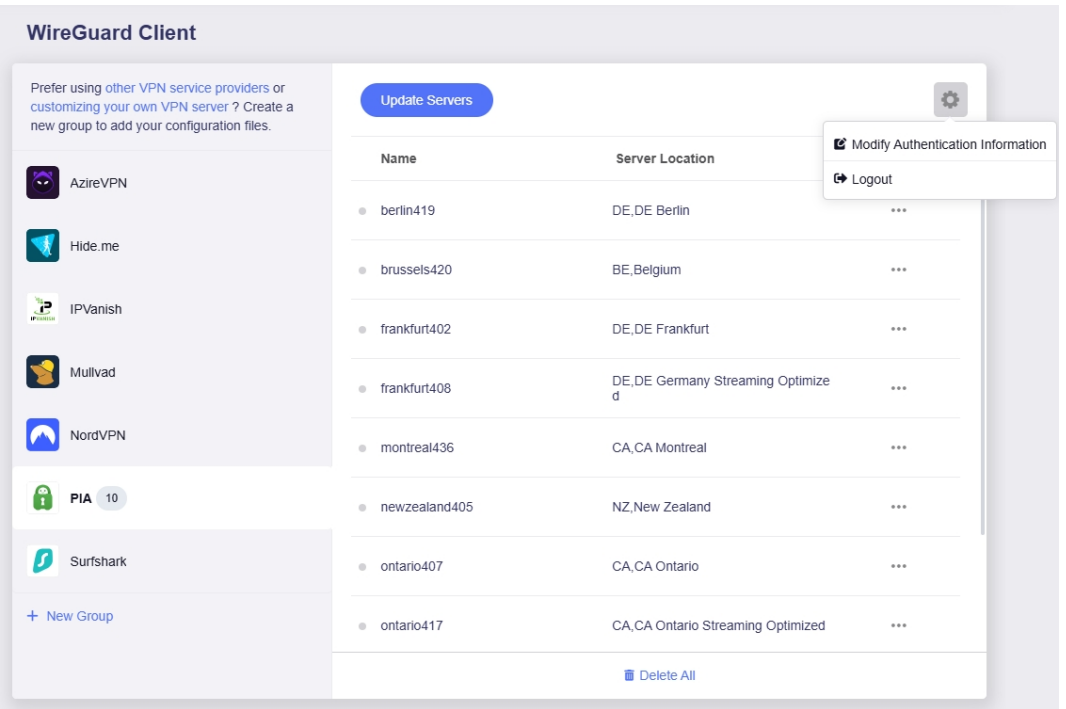
6. Zaktualizuj serwery.

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



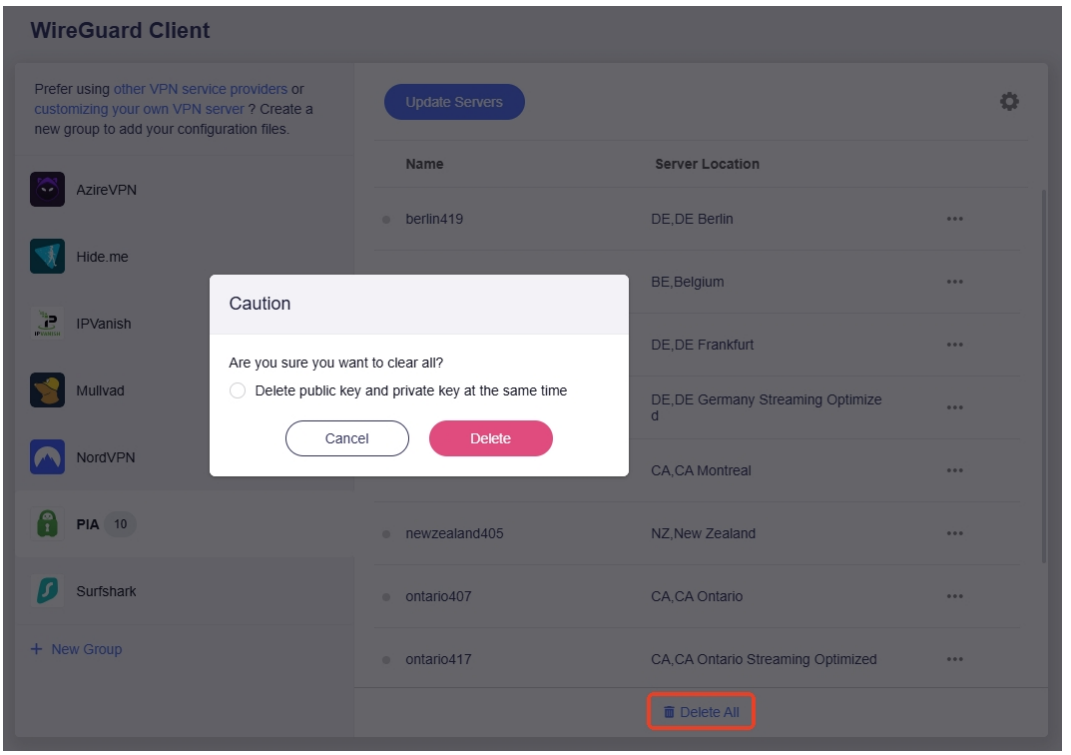
7. Zmiana danych logowania lub wylogowanie.

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



8. Usuń wszystkie pliki.

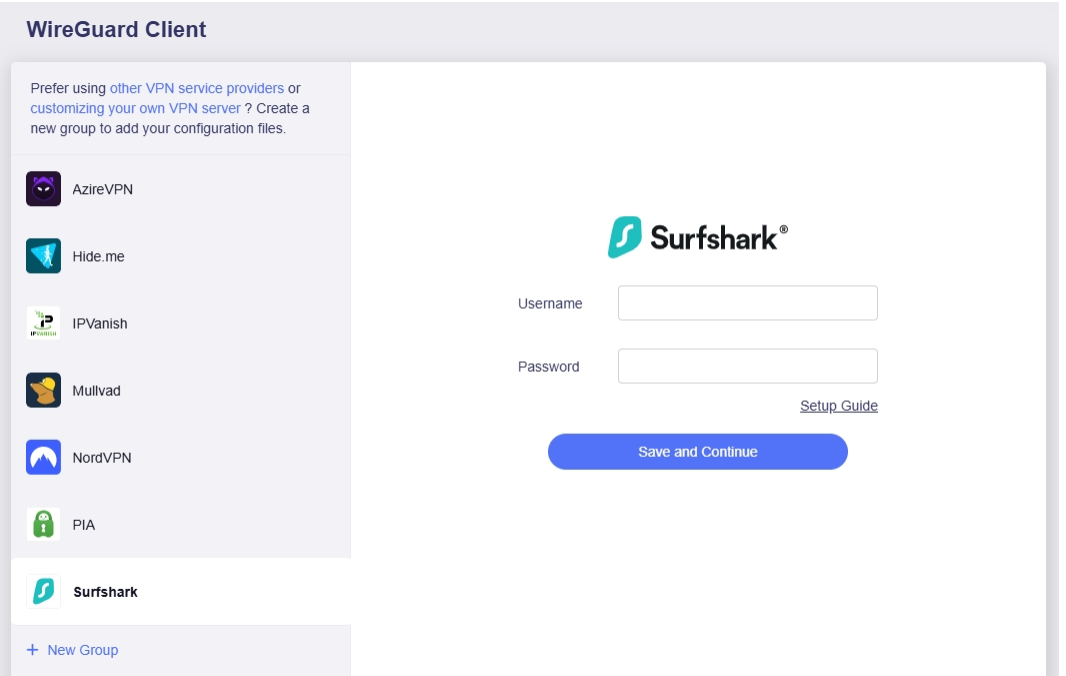
   Możesz kliknąć **Delete All**, aby jednym kliknięciem usunąć wszystkie pliki konfiguracyjne, oraz wybrać, czy jednocześnie usunąć klucze prywatny i publiczny.



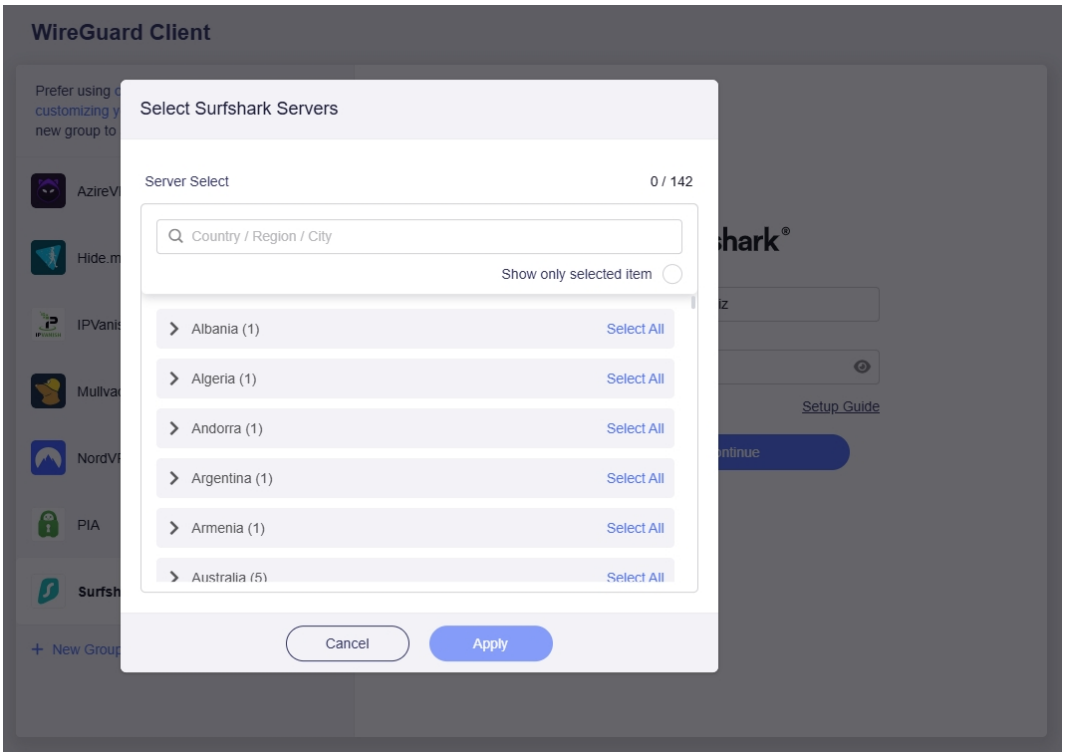
11.2.8 Konfiguracja Surfshark

Aby skonfigurować router jako klienta Surfshark, wykonaj poniższe czynności.

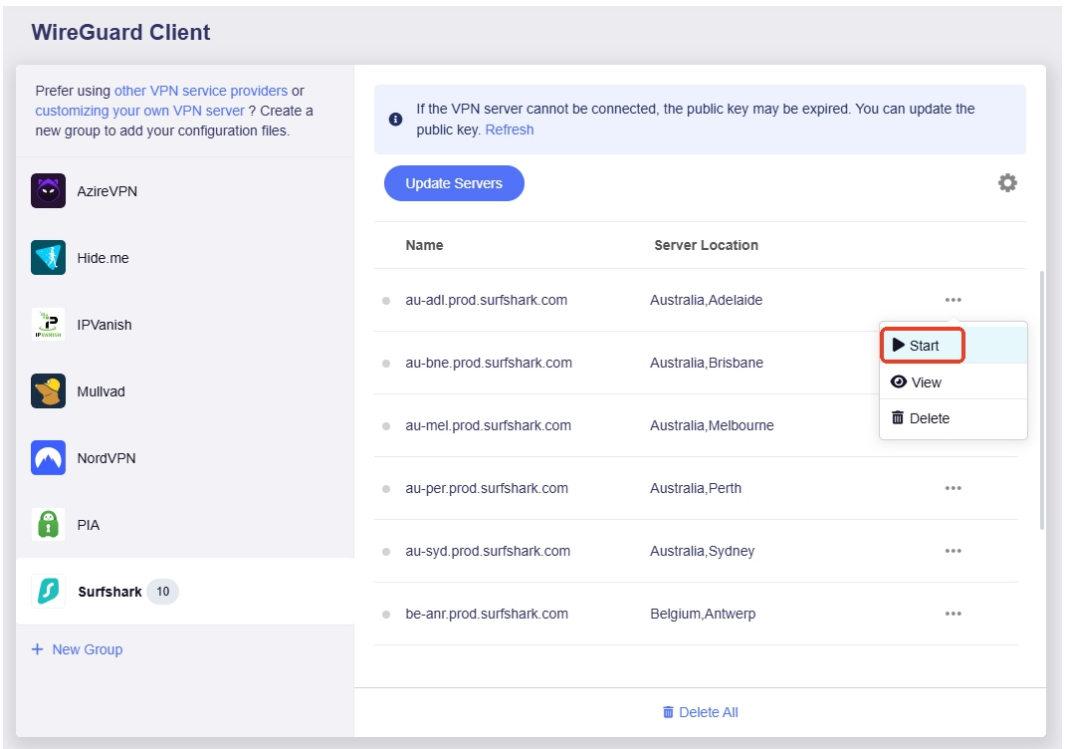
1. Zaloguj się do panelu administracyjnego routera i przejdź do **VPN** > **WireGuard Client** > **Surfshark**.
2. Wprowadź nazwę użytkownika i hasło, a następnie kliknij **Save and Continue**.



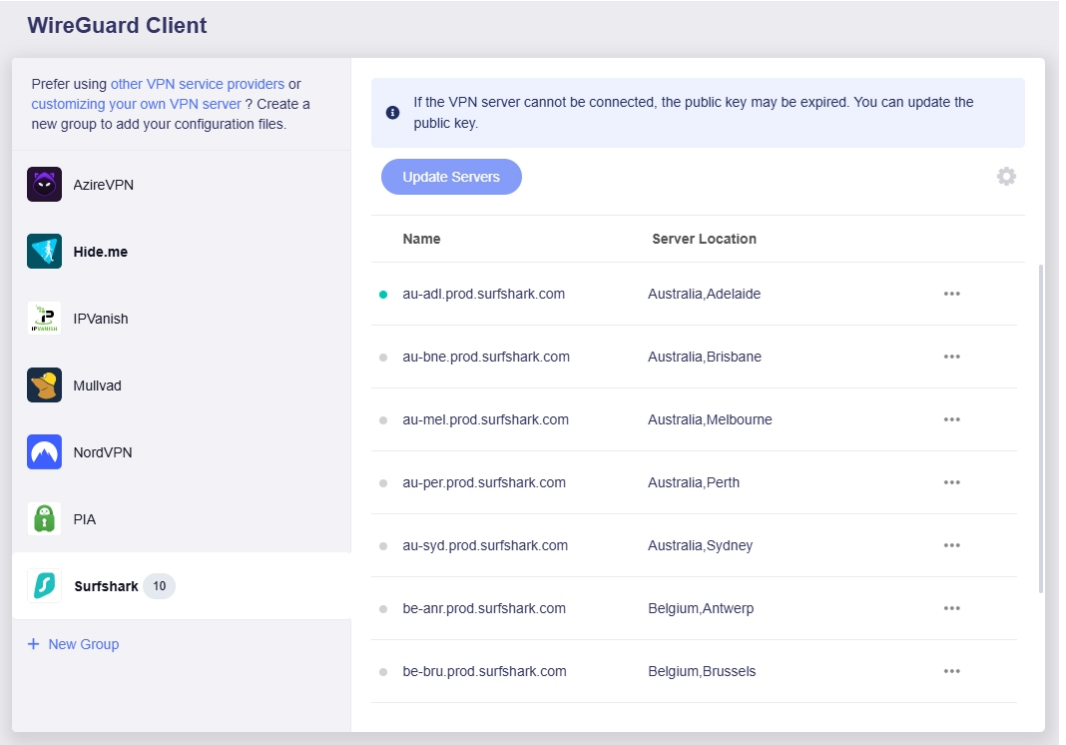
3. Wybierz serwery, z którymi chcesz się połączyć, i kliknij **Apply**.



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

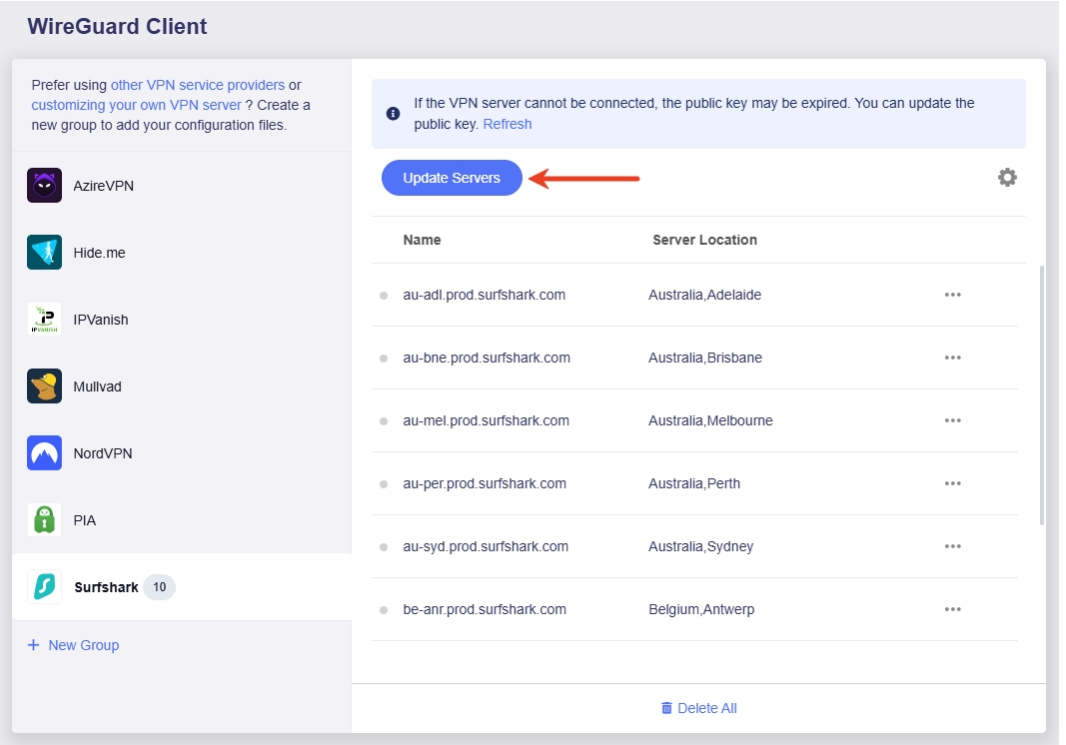


5. Po połączeniu obok pliku konfiguracyjnego pojawi się zielona kropka.



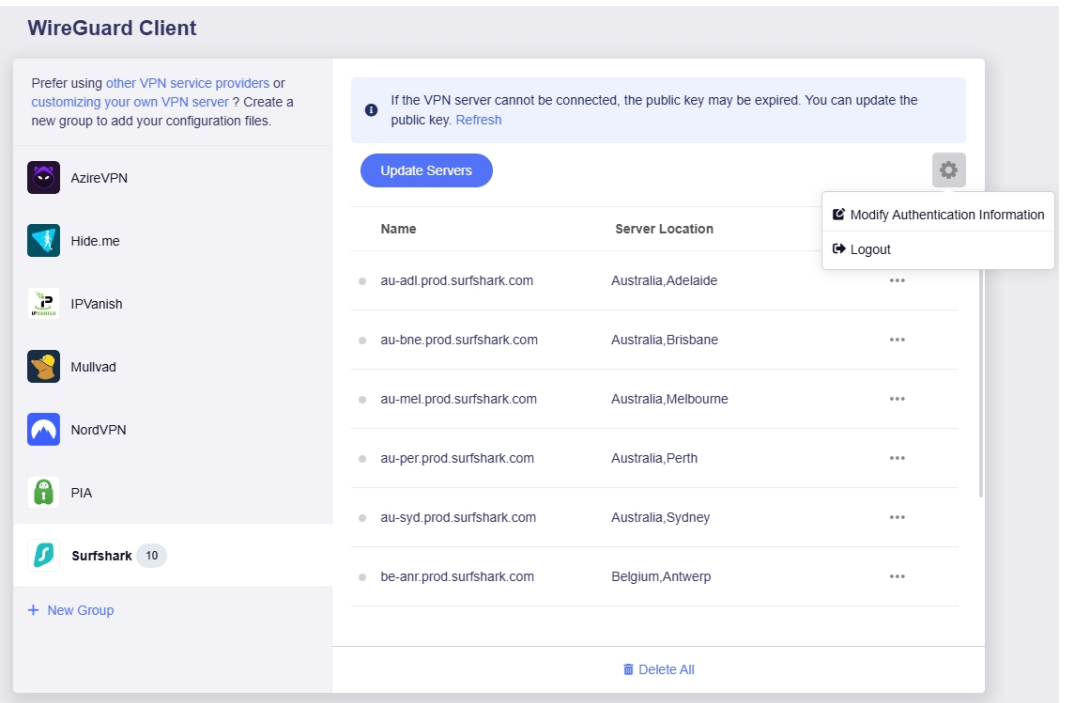
Szczegóły połączenia VPN możesz również sprawdzić w **VPN Dashboard**.

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



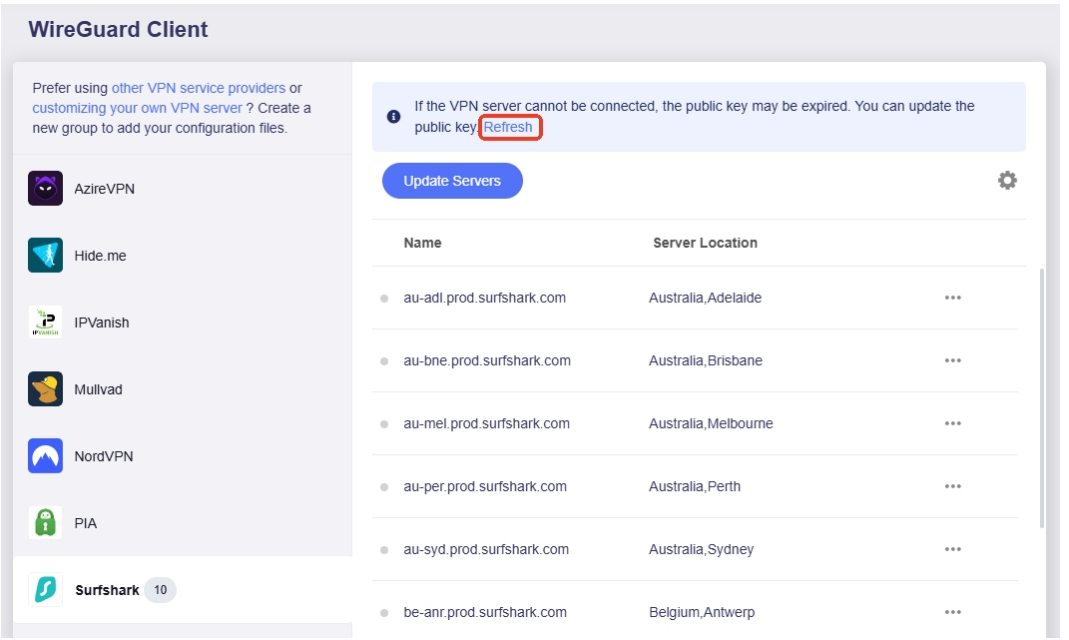
7. Zmiana danych logowania lub wylogowanie.

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



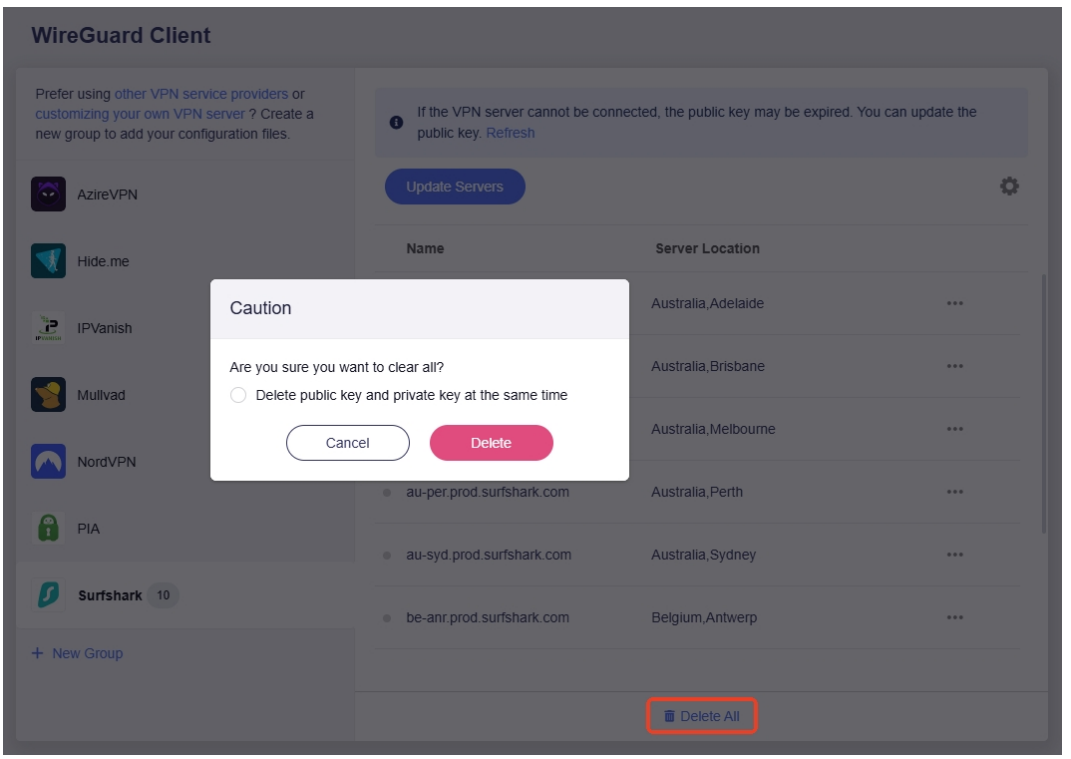
8. Odświeżanie.

   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.

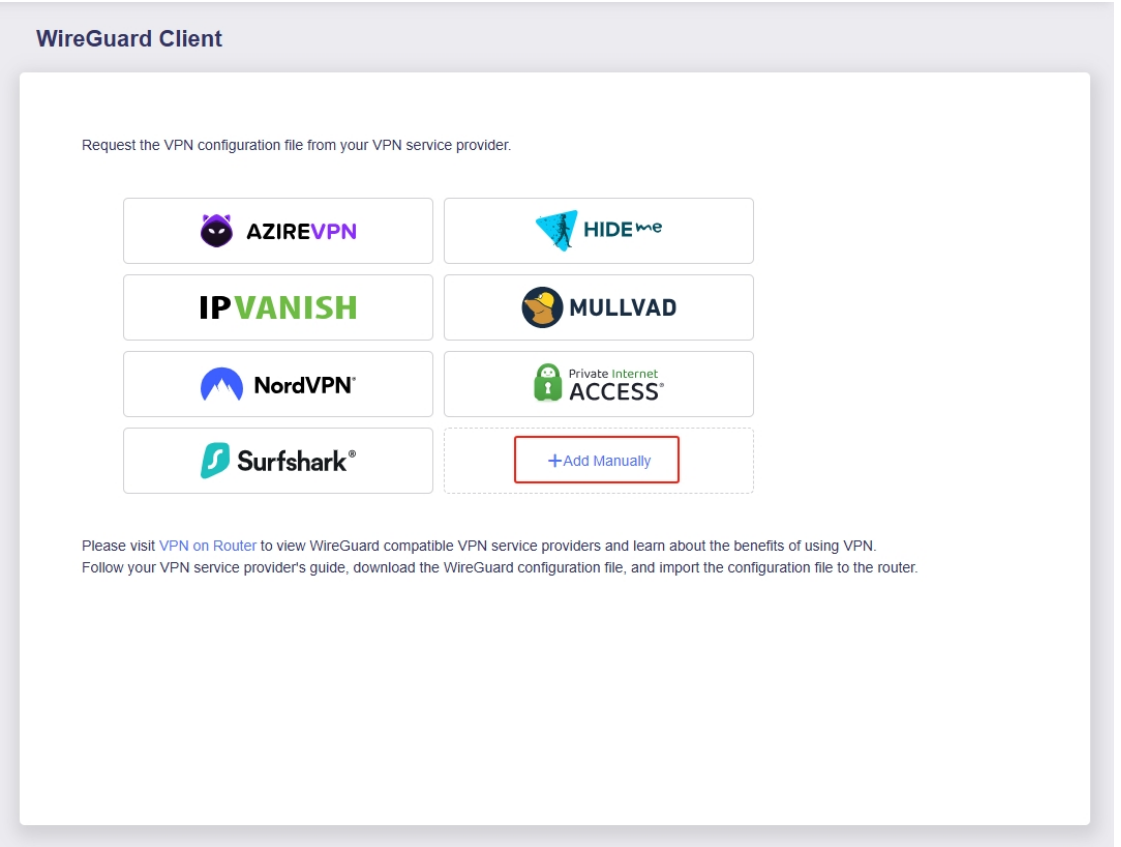


11.2.9 Ręczna konfiguracja klienta WireGuard (inni dostawcy)

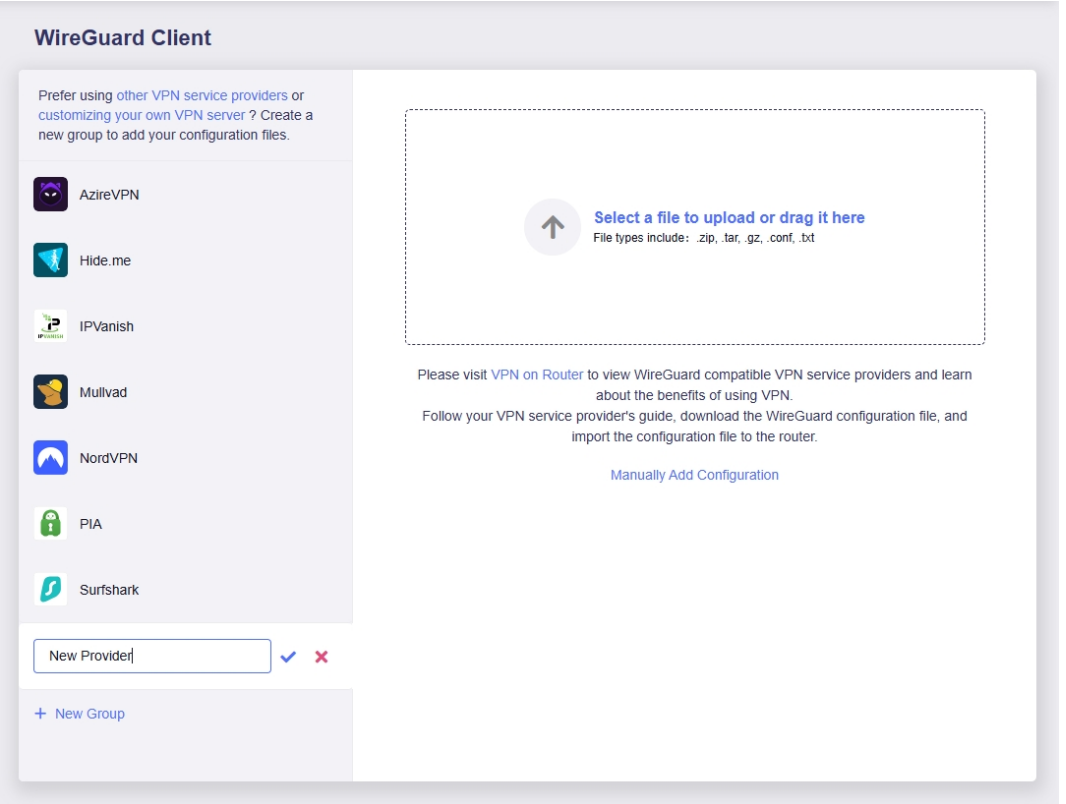
Jeśli Twój dostawca WireGuard nie jest zintegrowany z panelem administracyjnym, najpierw odwiedź jego oficjalną witrynę i pobierz plik konfiguracyjny. Następnie prześlij go do routera, aby skonfigurować klienta WireGuard. Jeśli nie wiesz, jak pobrać pliki konfiguracyjne, skorzystaj z tego poradnika lub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

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

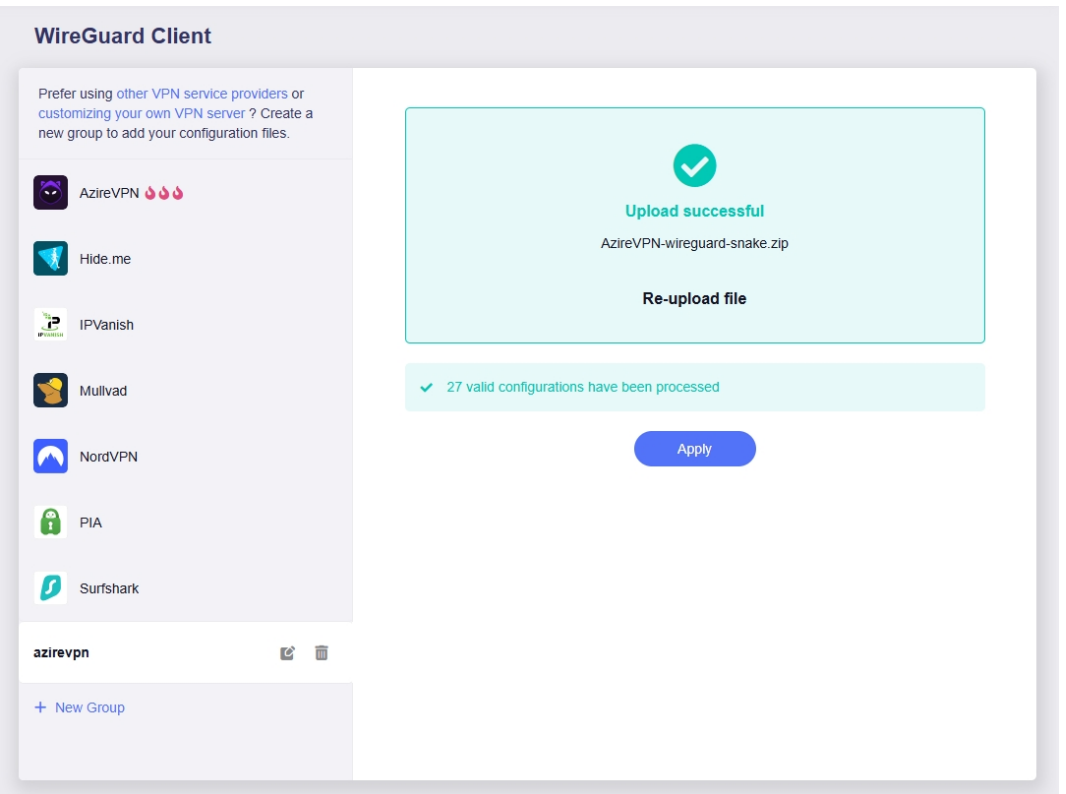
1. Zaloguj się do panelu administracyjnego routera i przejdź do **VPN** > **WireGuard Client** > **Add Manually**.



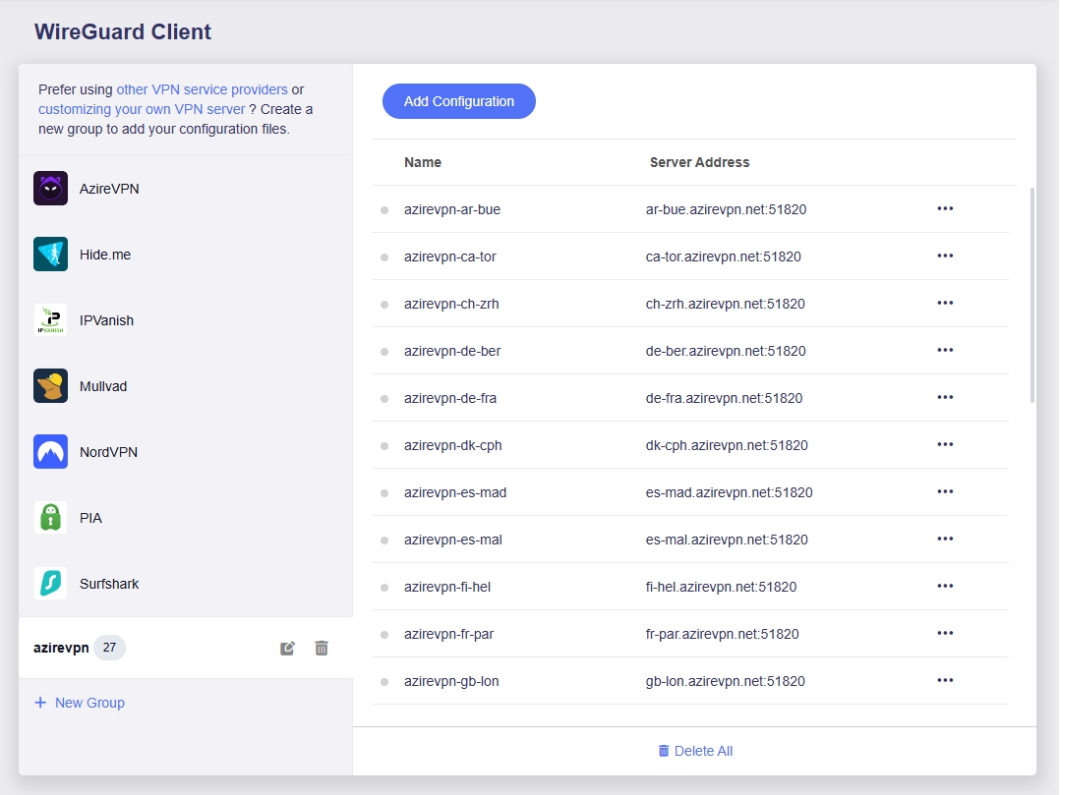
2. Na lewym pasku bocznym powstanie grupa. Nadaj jej opisową nazwę.



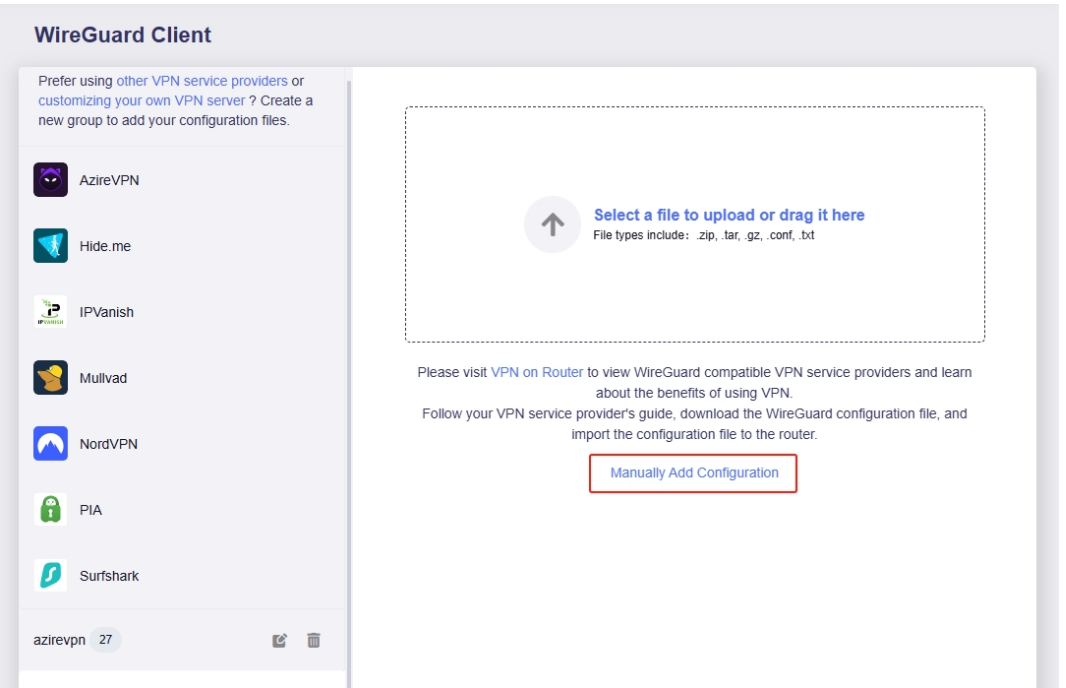
3. Kliknij obszar przesyłania, aby przesłać plik konfiguracyjny WireGuard (obsługiwane formaty: zip, tar, gz, conf, txt), i kliknij **Apply**.

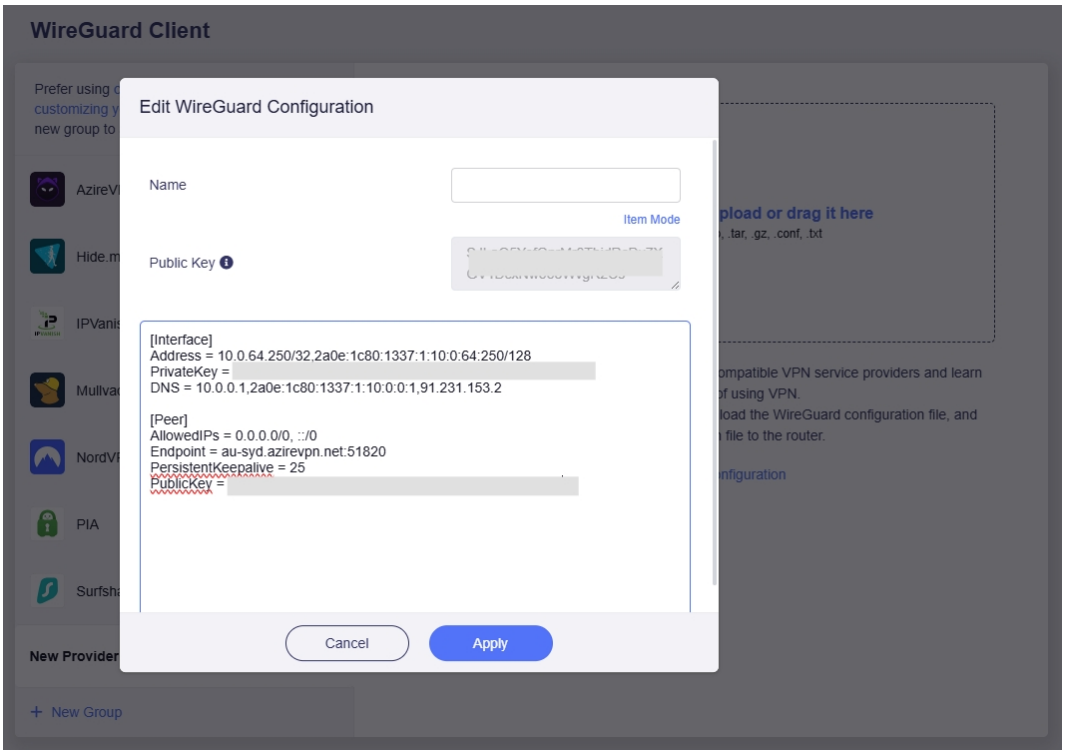


Po przesłaniu skompresowanego pliku zawierającego wiele plików konfiguracyjnych zostanie on automatycznie rozpakowany, jak pokazano poniżej.

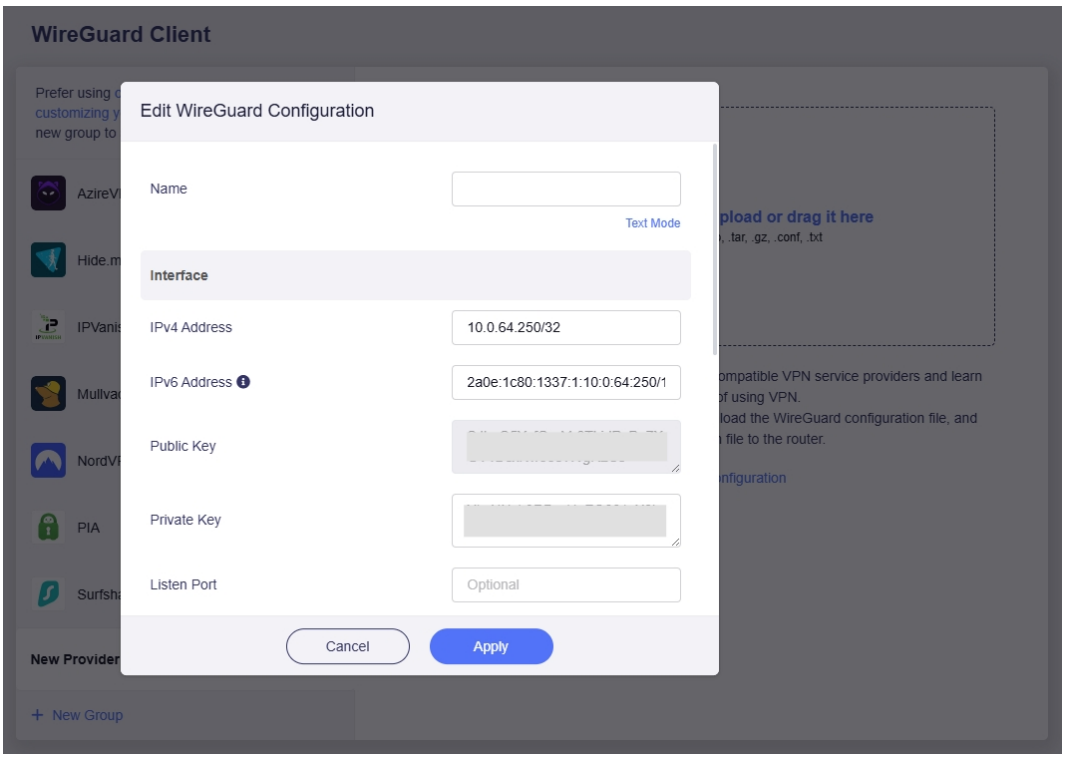


Możesz też kliknąć **Manually Add Configuration** u dołu obszaru przesyłania, dodać konfigurację w postaci tekstu i kliknąć **Apply**.

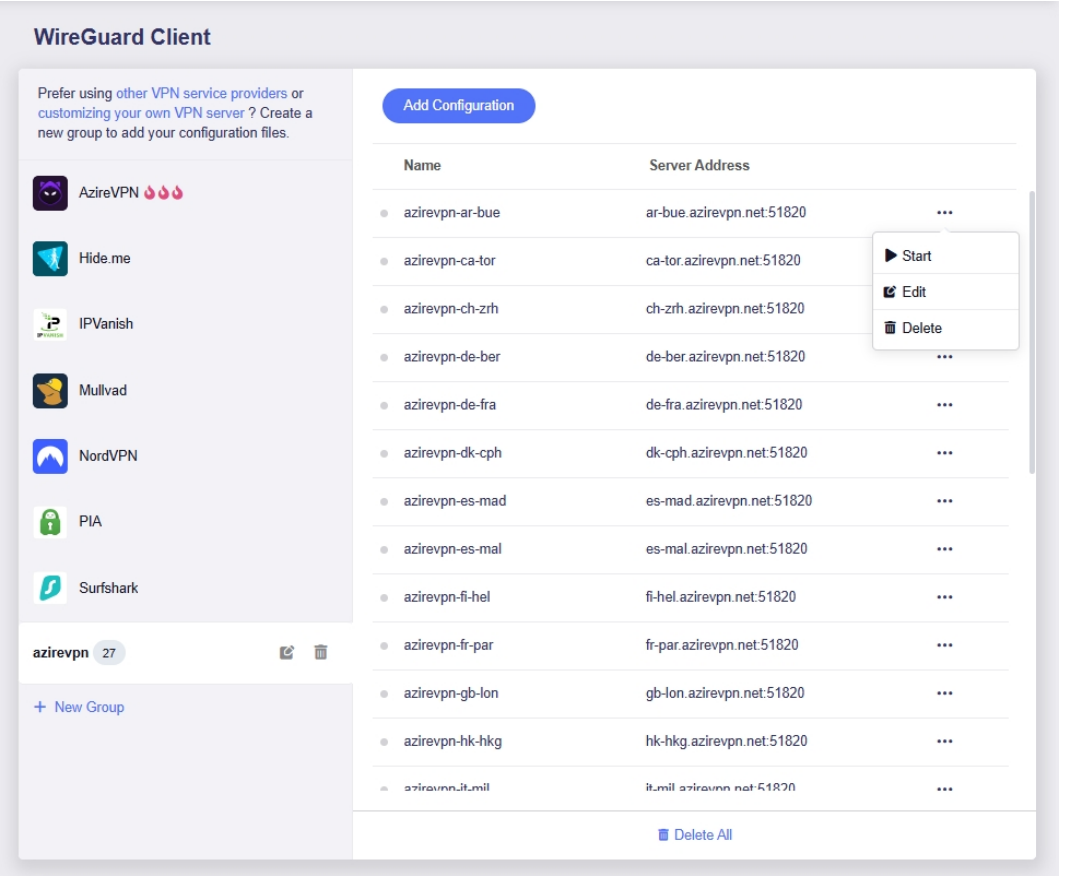




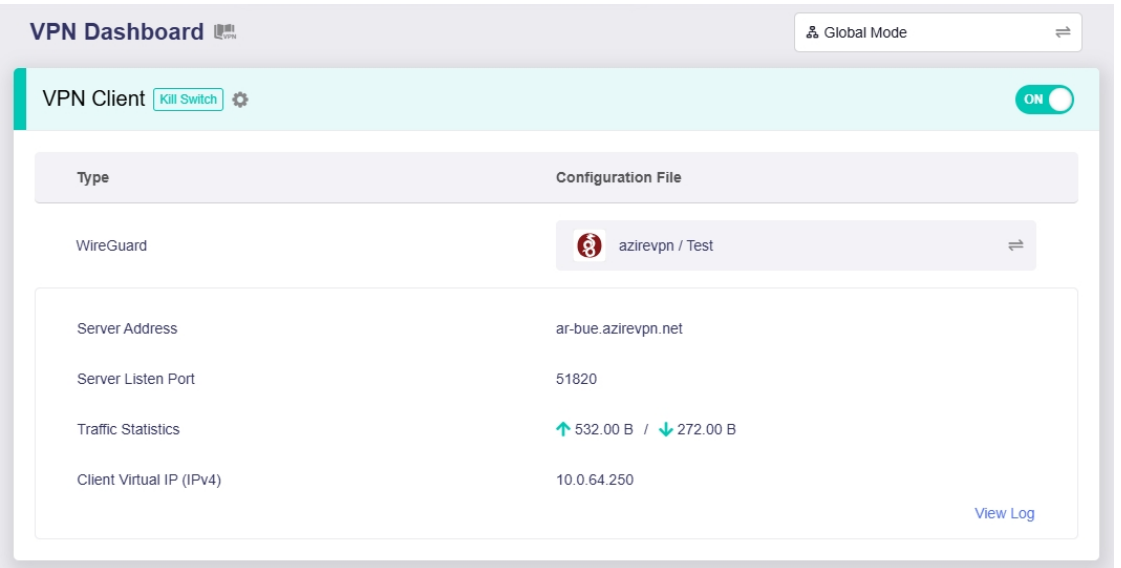
Aby sprawdzić poszczególne elementy, przełącz się do trybu Item, sprawdź szczegóły konfiguracji, a następnie kliknij **Apply**.



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

Sieć

W tym rozdziale przedstawiono ustawienia związane z konfiguracją i zarządzaniem siecią, takie jak podsieci, DNS i IPv6.

12.1 Multi-WAN

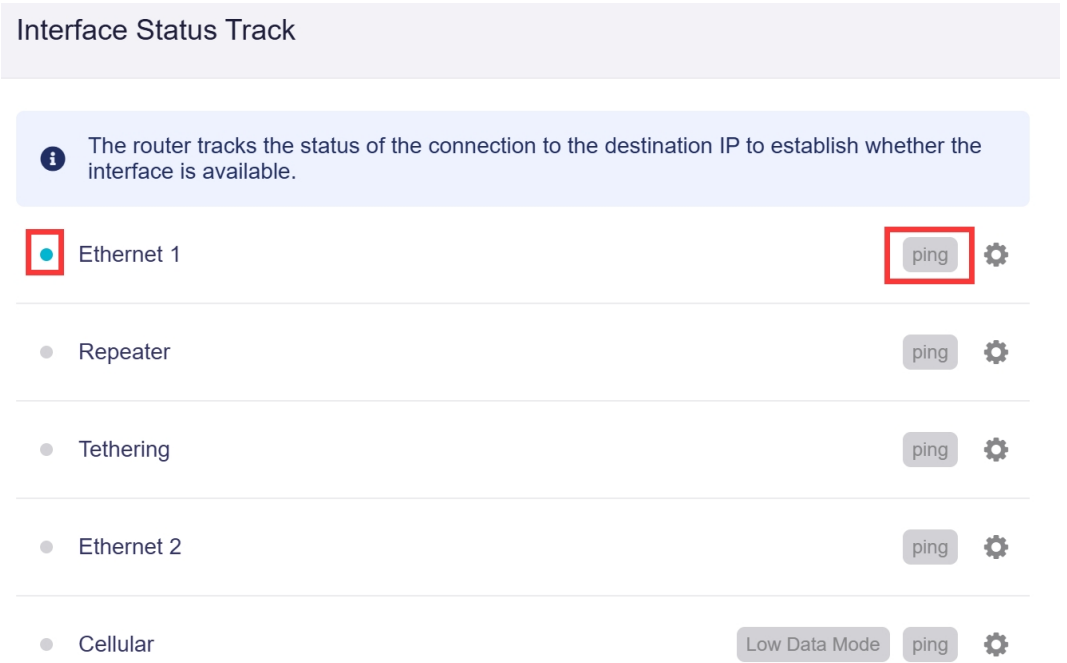
Multi-WAN umożliwia jednoczesne korzystanie z wielu sposobów dostępu do Internetu i konfigurowanie różnych połączeń na routerze. Oferuje dwa tryby pracy:

- **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.

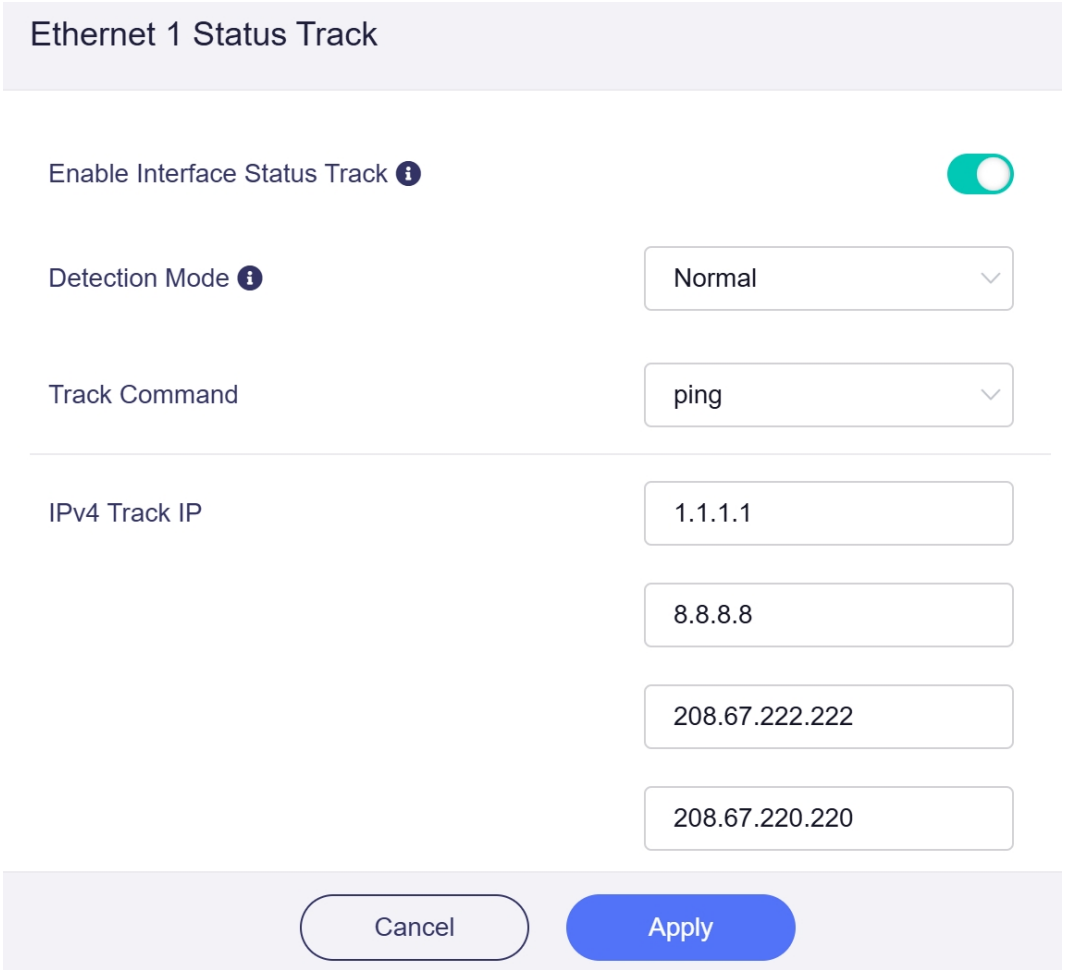
Zaloguj się do panelu administracyjnego routera i przejdź do **NETWORK** > **Multi-WAN**. Strona obejmuje dwie sekcje: Interface Status Track i Multi-WAN Mode.

12.1.1 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.



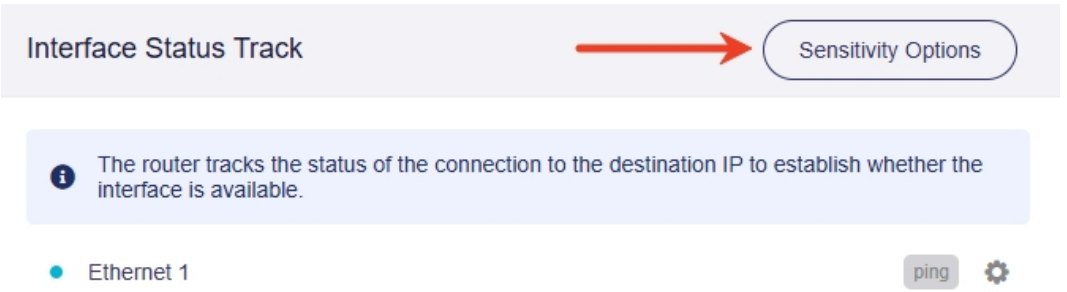
W sekcji **Interface Status Track** kliknij ikonę koła zębatego po prawej stronie, aby otworzyć ustawienia monitorowania poszczególnych interfejsów sieciowych. Poniżej pokazano ustawienia interfejsu Ethernet. Pozostałe interfejsy konfiguruje się według tych samych zasad.



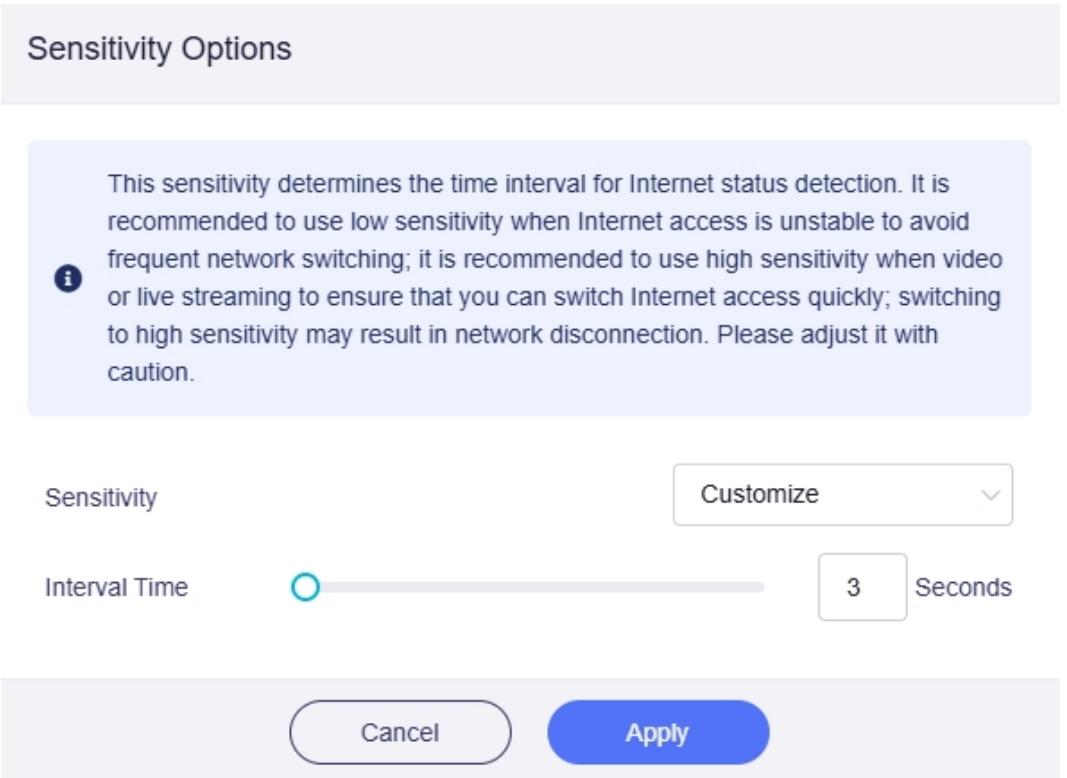
- **Enable Interface Status Track**: opcja jest domyślnie włączona. Po wyłączeniu router określa stan interfejsu na podstawie warunków fizycznych (np. podłączenia kabla Ethernet).
- **Detection Mode**: tę funkcję wprowadzono w wersji oprogramowania 4.5 jako Low Data Mode, a w wersji 4.7 zmieniono nazwę 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.



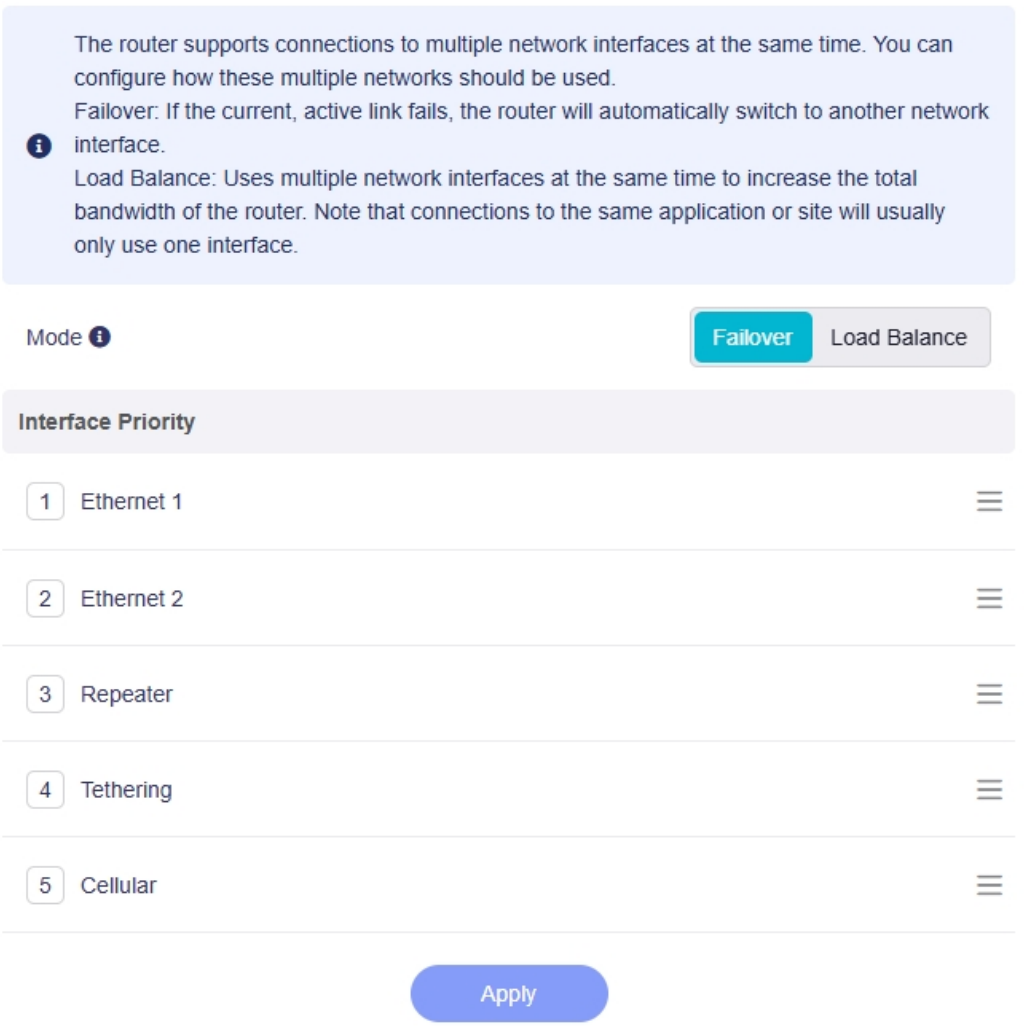
12.1.2 Tryb Multi-WAN

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.

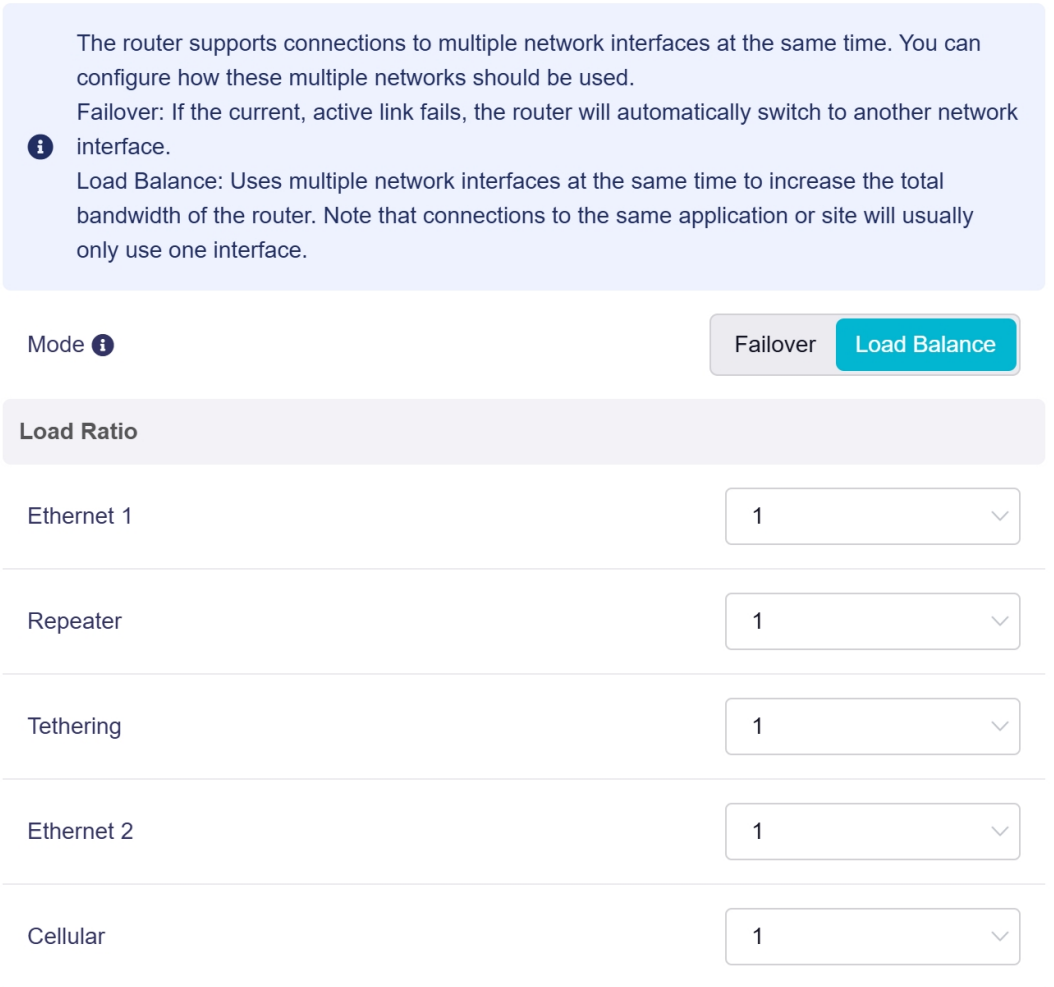
Możesz ustawić priorytety interfejsów. Po awarii używanego interfejsu router przełącza się na dostępny interfejs o najwyższym priorytecie. Gdy połączenie o wyższym priorytecie zostanie przywrócone, router automatycznie do niego wróci.



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. Jeśli na przykład Ethernet 1 ma przepustowość 100 Mb/s, Repeater 200 Mb/s, a inne połączenia są nieaktywne, ustaw proporcje na 1 dla Ethernet 1, 2 dla Repeater oraz 0 dla Tethering, Cellular i Ethernet 2. System będzie rozdzielać nowe połączenia między interfejsy w proporcji 1:2, więc Ethernet 1 obsłuży o połowę mniej połączeń niż Repeater. Ten tryb optymalizuje ogólną przepustowość przez równoważenie ruchu między wszystkimi dostępnymi interfejsami, inaczej niż tryb Failover.

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

12.2 Podsieci

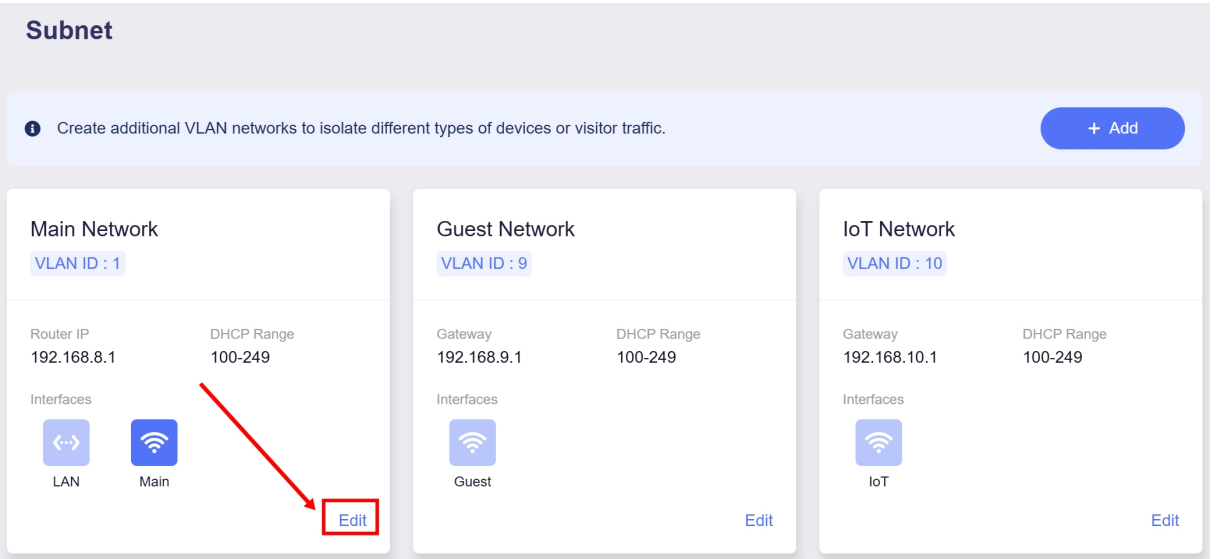
Podsieć to logicznie wydzielona część sieci, która służy do organizowania i izolowania urządzeń w różnych segmentach sieci.

Zaloguj się do internetowego panelu administracyjnego routera i przejdź do **NETWORK** > **Subnet**. Tutaj możesz skonfigurować Main Network, Guest Network, IoT Network i własne sieci VLAN.

12.2.1 Sieć główna

Main Network to połączenie przez główną sieć Wi-Fi lub Ethernet. Wyświetla stan wszystkich interfejsów, identyfikator VLAN, adres IP routera i zakres DHCP.

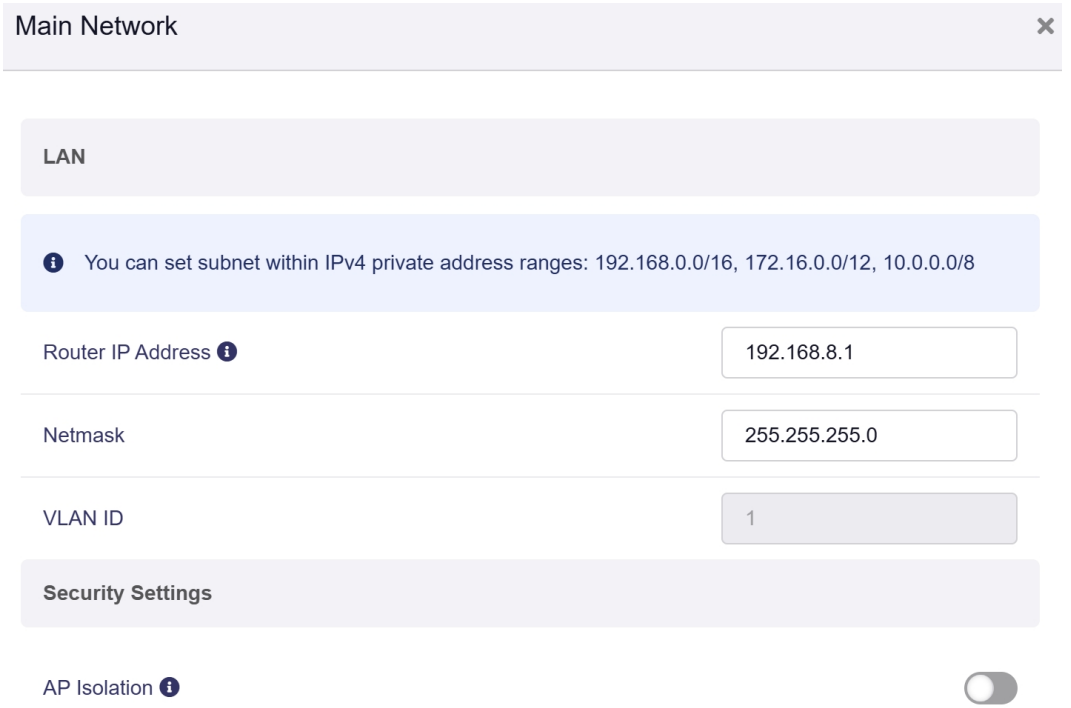
Kliknij **Edit** w prawym dolnym rogu, aby skonfigurować sieć główną.



Strona konfiguracji obejmuje ustawienia podstawowe, ustawienia serwera DHCP i rezerwację adresów.

Ustawienia podstawowe

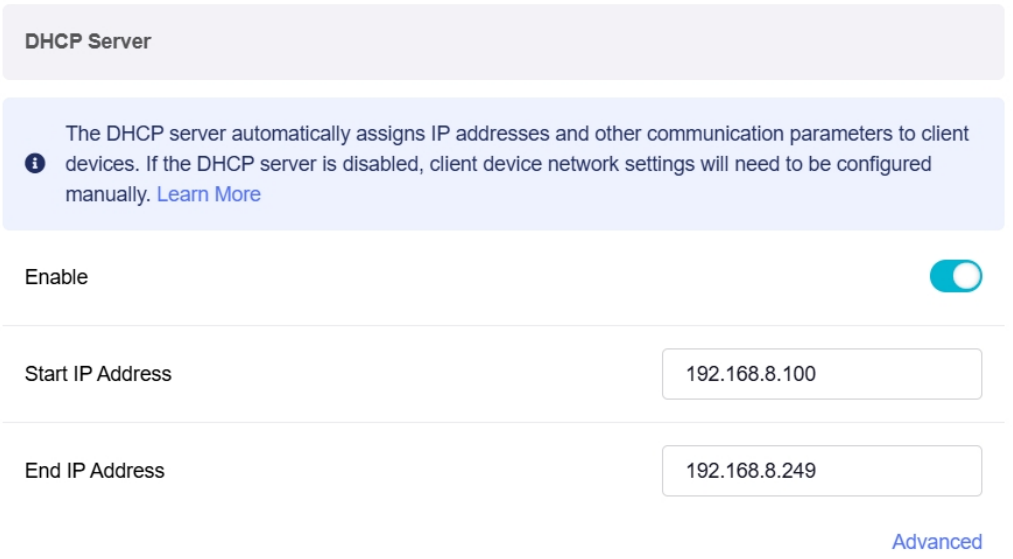
Ustawienia podstawowe obejmują adres IP routera, maskę podsieci i identyfikator VLAN. Podsieć można ustawić w prywatnych zakresach adresów IPv4: 192.168.0.0/16, 172.16.0.0/12 i 10.0.0.0/8.



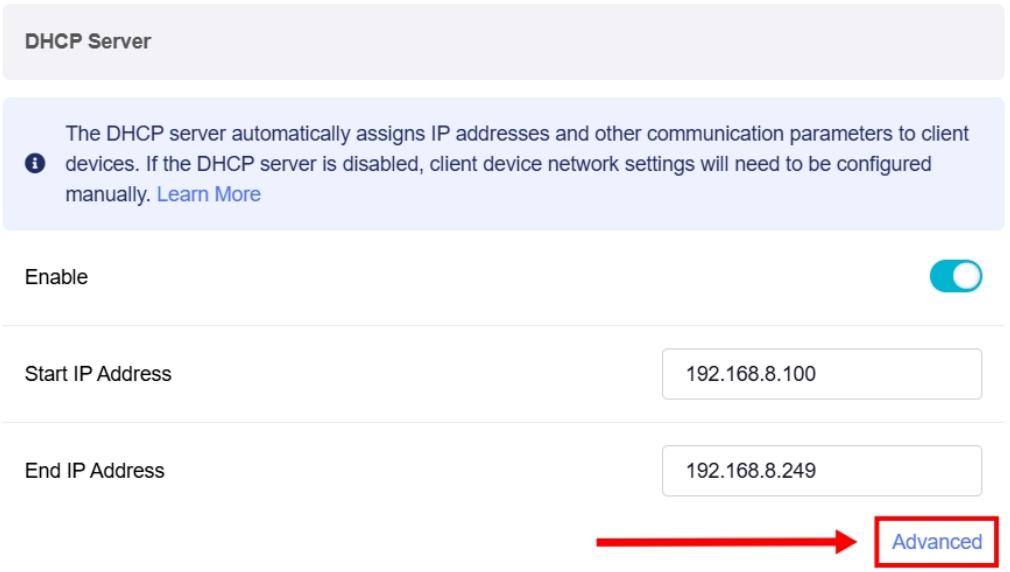
- **Router IP Address**: adres wpisywany w pasku adresu przeglądarki w celu otwarcia panelu administracyjnego routera. Domyślnie jest to 192.168.8.1. Można go zmienić, jeśli koliduje z siecią nadrzędną.
- **Netmask**: dostępne są dwie opcje: 255.255.255.0 i 255.255.0.0.
- **VLAN ID**: domyślny identyfikator VLAN sieci głównej to 1. Nie można go zmienić.
- **AP Isolation**: pozwala odizolować urządzenia klienckie w oddzielnym segmencie sieci. Urządzenia te nie będą mogły komunikować się z innymi urządzeniami w tej samej sieci.

Serwer DHCP

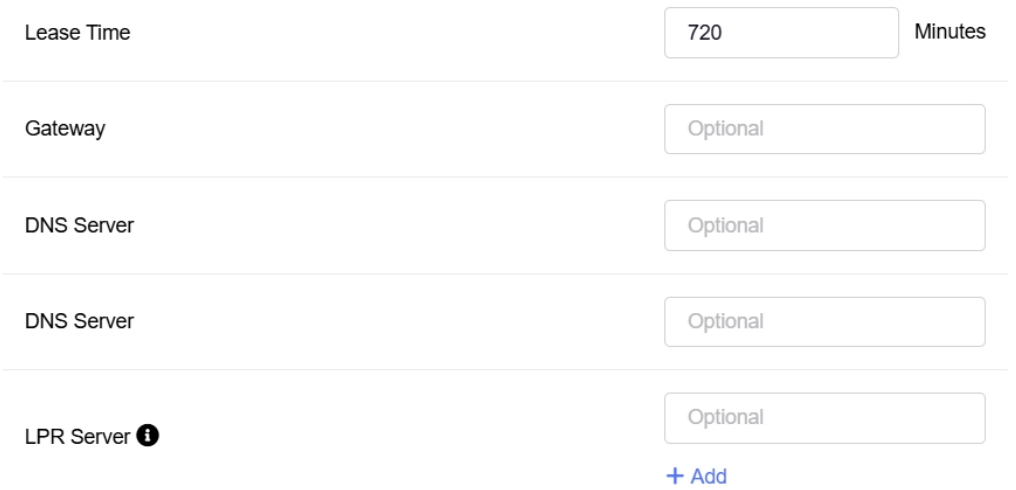
Serwer DHCP automatycznie przydziela adresy IP i inne parametry komunikacji każdemu podłączonemu klientowi. W routerze GL.iNet jest domyślnie włączony, a jego pula adresów IP obejmuje zakres od 192.168.8.100 do 192.168.8.249. W razie potrzeby można zmienić ten zakres.



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** : dwa pola serwerów DNS umożliwiają skonfigurowanie podstawowego i zapasowego serwera rozpoznającego nazwy. Podstawowy DNS wpisuje się w górnym polu, a zapasowy w dolnym. Gdy serwer podstawowy jest niedostępny, urządzenia klienckie automatycznie przełączają się na zapasowy, zapewniając ciągłość rozpoznawania nazw domen.
- **LPR Server** (Line Printer Remote Server): usługa zarządzająca zadaniami drukowania, która umożliwia urządzeniom sieciowym wysyłanie żądań drukowania do zdalnych drukarek. Można skonfigurować wiele portów LPR dla drukarek.

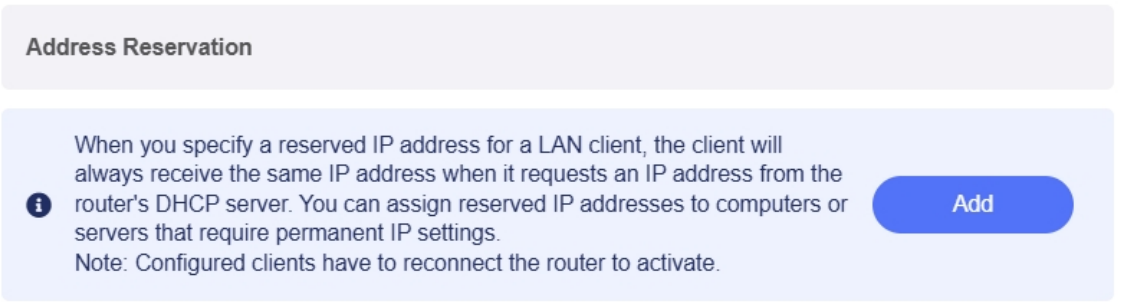
Uwaga: po wyłączeniu serwera DHCP trzeba ręcznie skonfigurować statyczny adres IP i inne parametry komunikacji na każdym urządzeniu klienckim. Szczegóły znajdziesz tutaj.

Rezerwacja adresów

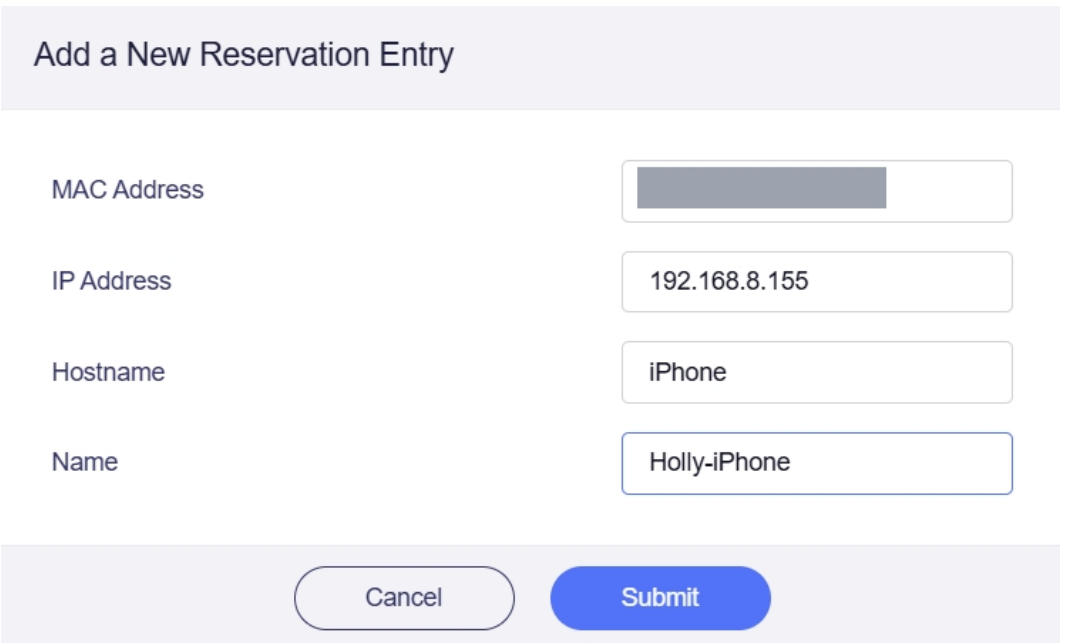
Rezerwacja adresów umożliwia przypisanie stałego adresu IP klientowi LAN, dzięki czemu przy każdym kontakcie z serwerem DHCP routera otrzymuje on ten sam adres. Zarezerwowane adresy można przypisywać komputerom lub serwerom wymagającym stałych ustawień IP. Aby ustawienie zaczęło działać, urządzenia z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

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

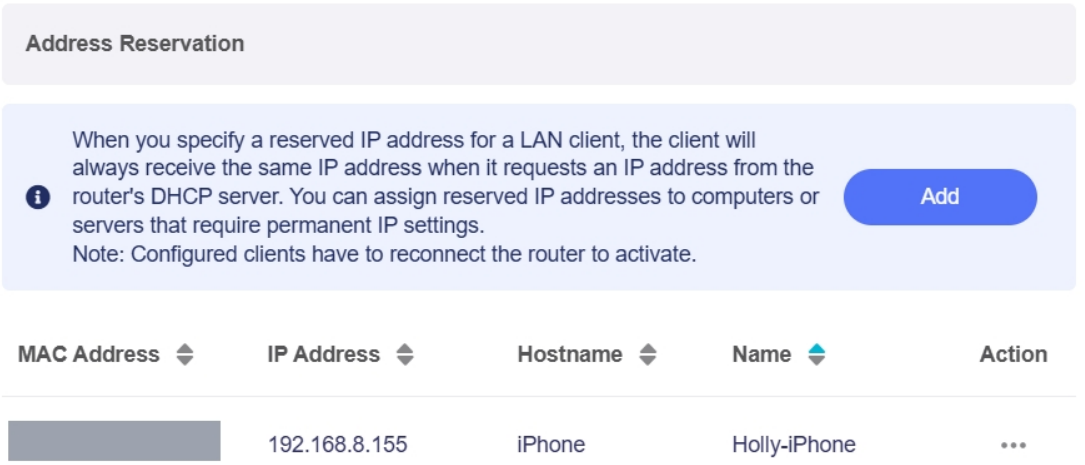
1. Zaloguj się do internetowego panelu administracyjnego routera, przejdź do **Subnet** > **Main Network** > **Address Reservation** i kliknij **Add**.



2. W wyświetlonym oknie wybierz adres MAC z listy rozwijanej. Odpowiadający mu adres IP zostanie uzupełniony automatycznie. Wprowadź nazwę hosta (Hostname) i własną nazwę (Name), aby ułatwić identyfikację. Następnie kliknij **Submit**.



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

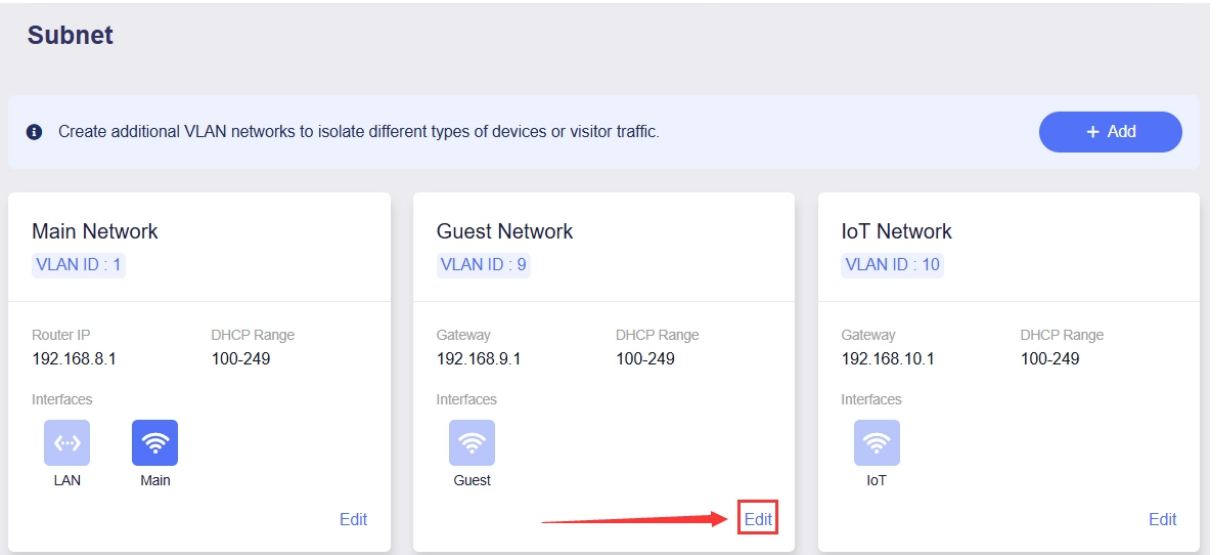


12.2.2 Sieć gościnna

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

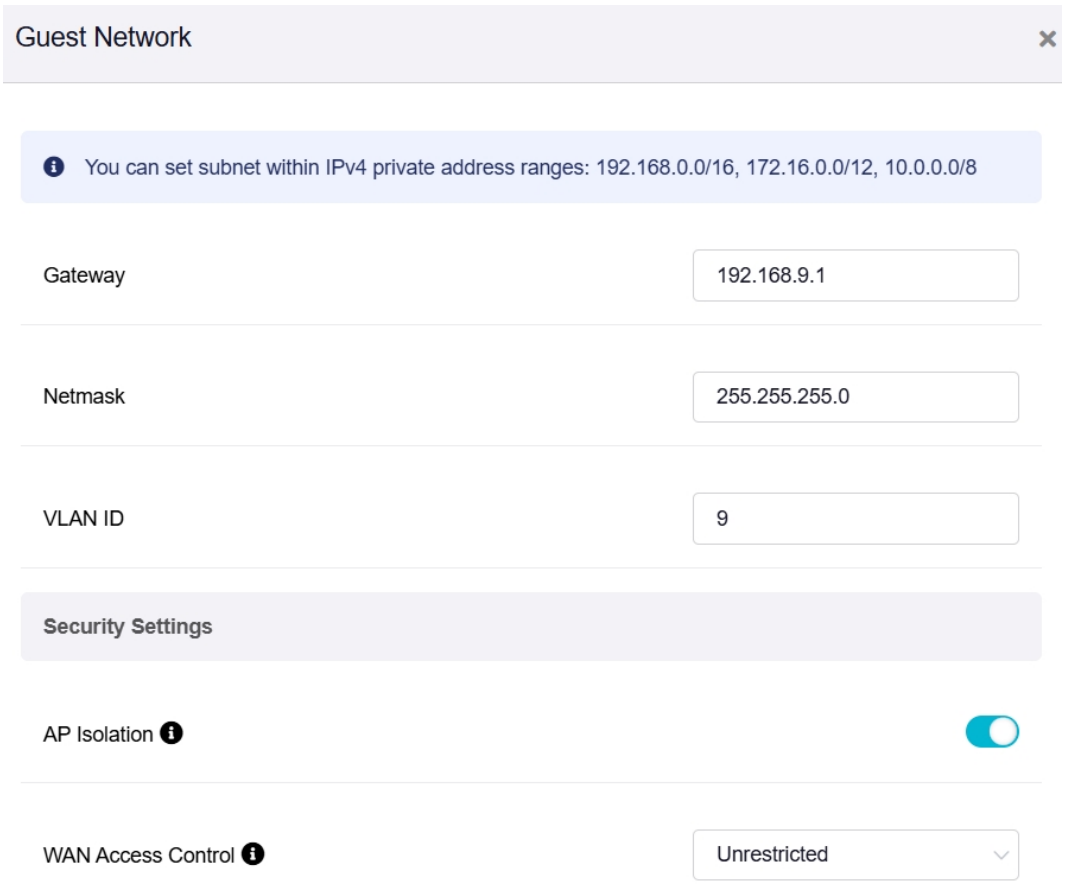
Zaloguj się do internetowego panelu administracyjnego routera i przejdź do **NETWORK** > **Subnet** > **Guest Network**. Na tej stronie możesz skonfigurować ustawienia sieci gościnnej, w tym ustawienia podstawowe i serwer DHCP.

Kliknij **Edit** w prawym dolnym rogu, aby skonfigurować sieć gościnną.



Ustawienia podstawowe

Ustawienia podstawowe obejmują Gateway, Netmask, AP Isolation, VLAN ID i WAN Access Control.

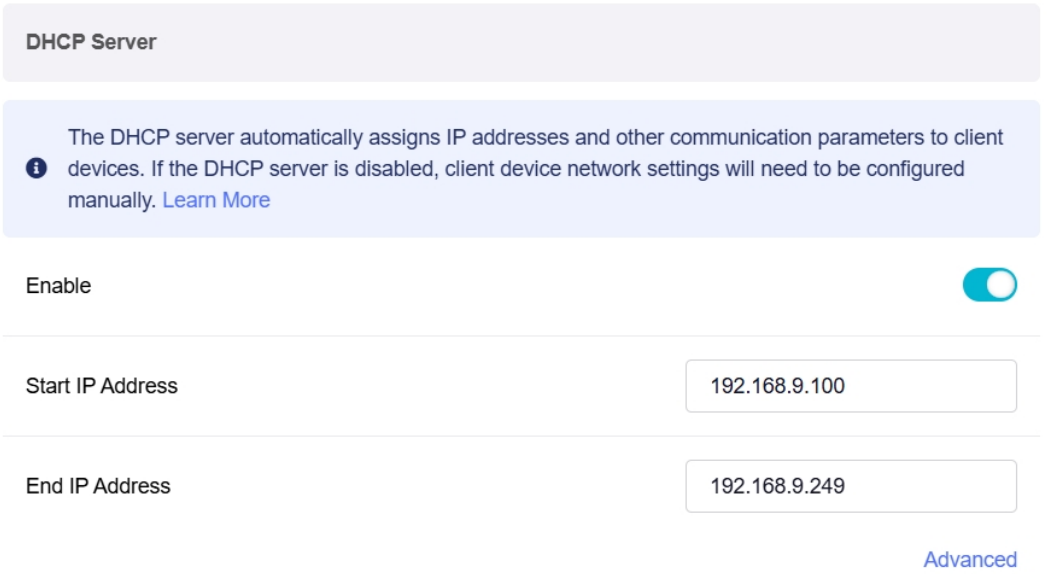


- **Gateway**: domyślny adres to 192.168.9.1. Można go zmienić, ale nie może kolidować z adresem bramy sieci głównej.
- **Netmask**: dostępne są dwie opcje: 255.255.255.0 i 255.255.0.0.
- **VAN ID**: domyślny identyfikator VLAN sieci gościnnej to 9. Można go zmienić w razie potrzeby.
- **AP Isolation**: izoluje klientów sieci gościnnej w oddzielnych segmentach, aby nie mogli komunikować się z innymi urządzeniami w tej samej sieci.
- **WAN Access Control**: zarządza dostępem lokalnej podsieci do sieci po stronie WAN, w tym do Internetu i innych podsieci WAN.
  Dostępne są trzy tryby kontroli dostępu do WAN:
  - **Unrestricted**: umożliwia tej podsieci nieograniczony dostęp do Internetu i innych podsieci po stronie WAN.
  - **Block WAN Subnet**: blokuje dostęp do innych podsieci po stronie WAN. Dostęp do Internetu pozostaje dostępny.
  - **Block Internet Access**: blokuje cały dostęp wychodzący, w tym do Internetu i podsieci po stronie WAN.

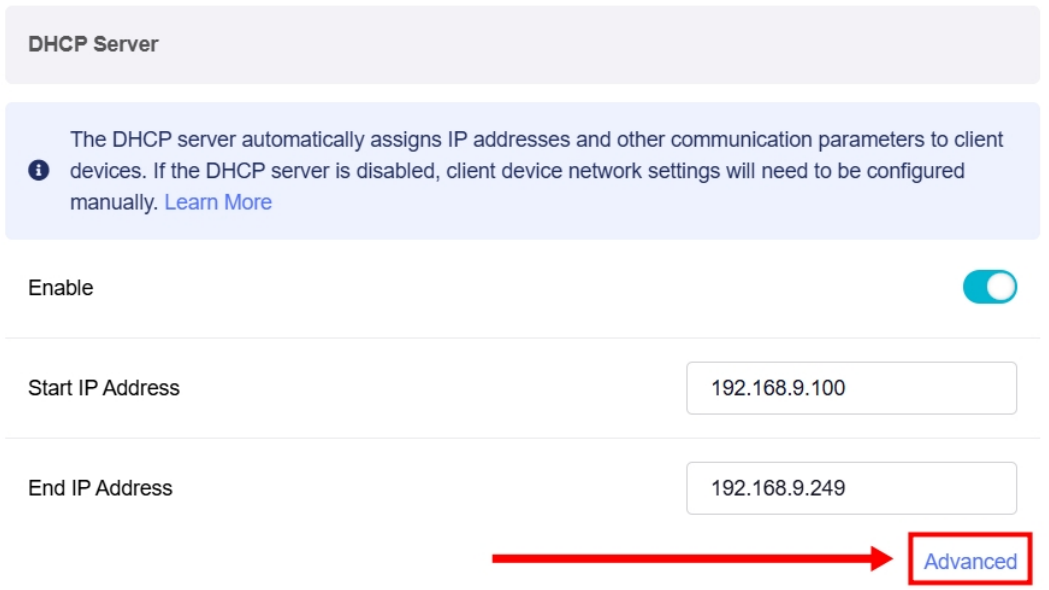
Serwer DHCP

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

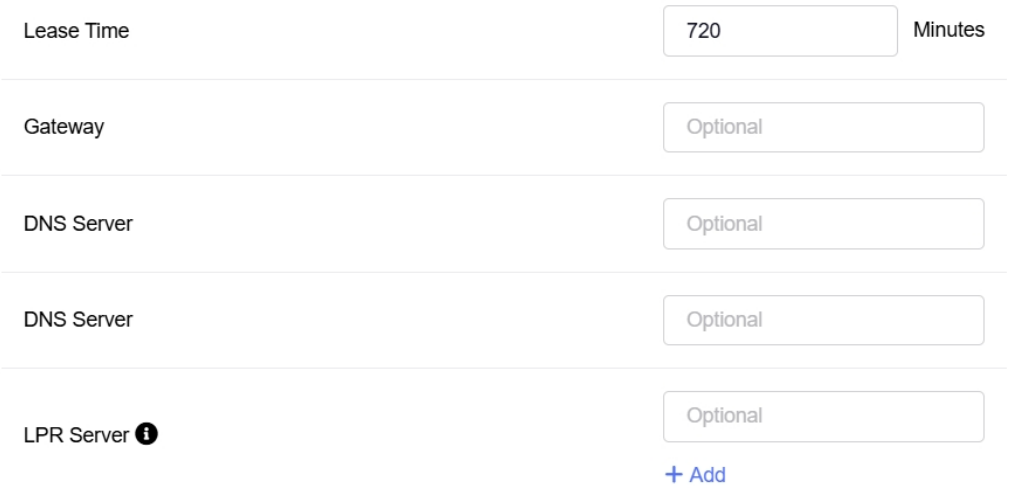
Po włączeniu serwer DHCP automatycznie przydziela adresy IP i inne parametry komunikacji każdemu podłączonemu klientowi. Pula adresów IP sieci gościnnej obejmuje zakres od 192.168.9.100 do 192.168.9.249. W razie potrzeby można go zmienić.



Kliknij **Advanced** w prawym dolnym rogu.



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



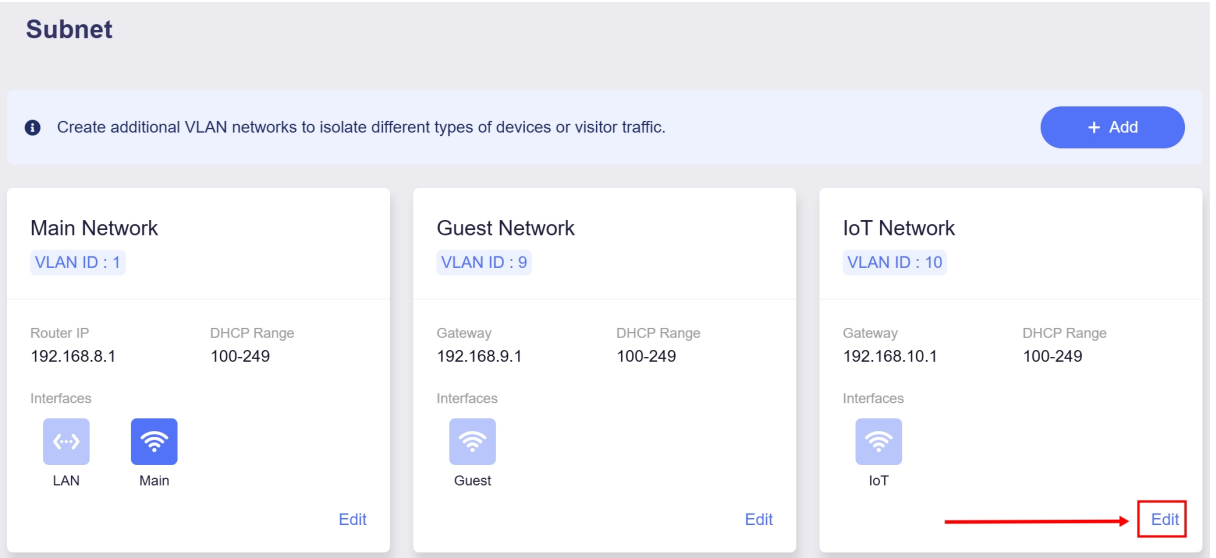
- **Lease Time**: czas, przez który urządzenie może korzystać z adresu IP przydzielonego przez DHCP sieci gościnnej.
- **Gateway**: element routera kierujący ruch między siecią gościnną a sieciami zewnętrznymi (np. Internetem).
- **DNS Server** : dwa pola serwerów DNS umożliwiają skonfigurowanie podstawowego i zapasowego serwera rozpoznającego nazwy. Podstawowy DNS wpisuje się w górnym polu, a zapasowy w dolnym. Gdy serwer podstawowy jest niedostępny, urządzenia klienckie automatycznie przełączają się na zapasowy, zapewniając ciągłość rozpoznawania nazw domen.
- **LPR Server** (Line Printer Remote Server): usługa zarządzająca zadaniami drukowania, która umożliwia urządzeniom sieciowym wysyłanie żądań drukowania do zdalnych drukarek. Można skonfigurować wiele portów LPR dla drukarek.

12.2.3 Sieć IoT

IoT Network tworzy oddzielną sieć Wi-Fi dla urządzeń IoT. Izolacja od sieci głównej zapewnia lepszą zgodność i większe bezpieczeństwo. Możesz bezpośrednio sprawdzić stan interfejsu, identyfikator VLAN, bramę i zakres DHCP.

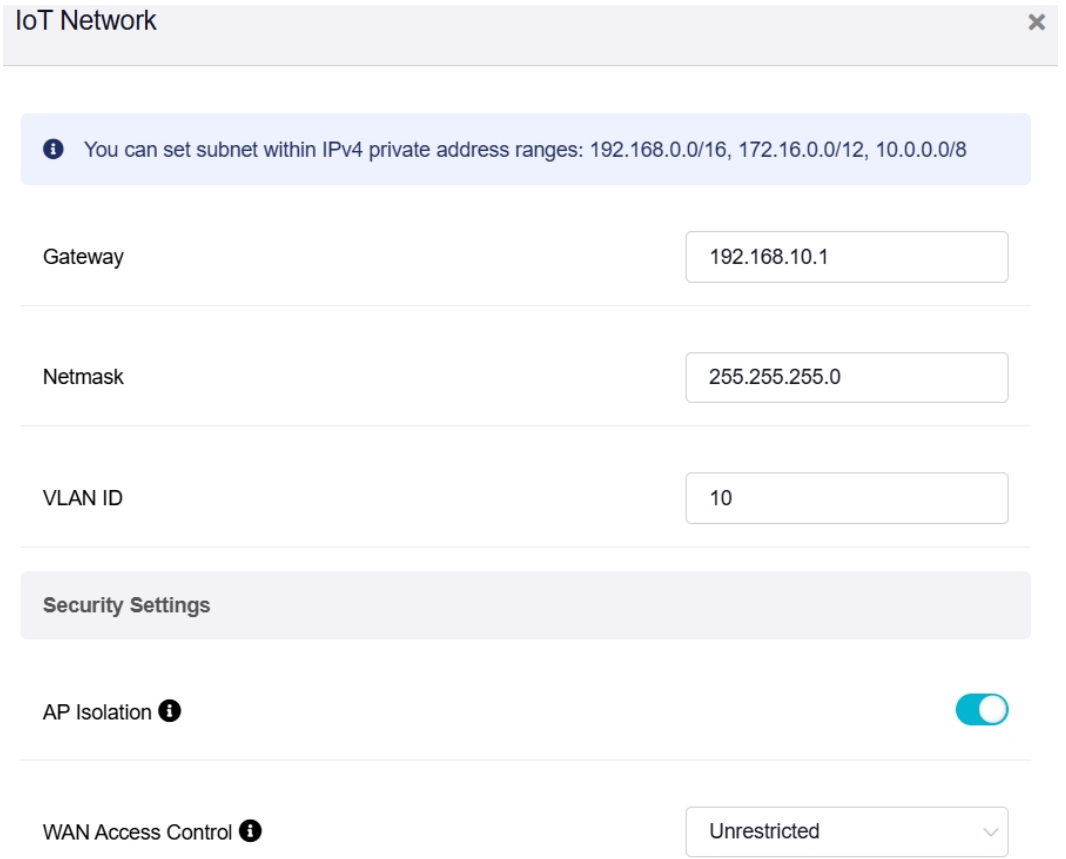
Zaloguj się do internetowego panelu administracyjnego routera i przejdź do **NETWORK** > **Subnet** > **IoT Network**. Na tej stronie możesz skonfigurować ustawienia sieci IoT, w tym ustawienia podstawowe i serwer DHCP.

Kliknij **Edit** w prawym dolnym rogu, aby skonfigurować sieć gościnną.



Ustawienia podstawowe

Ustawienia podstawowe obejmują Gateway, Netmask, AP Isolation, VLAN ID i WAN Access Control.

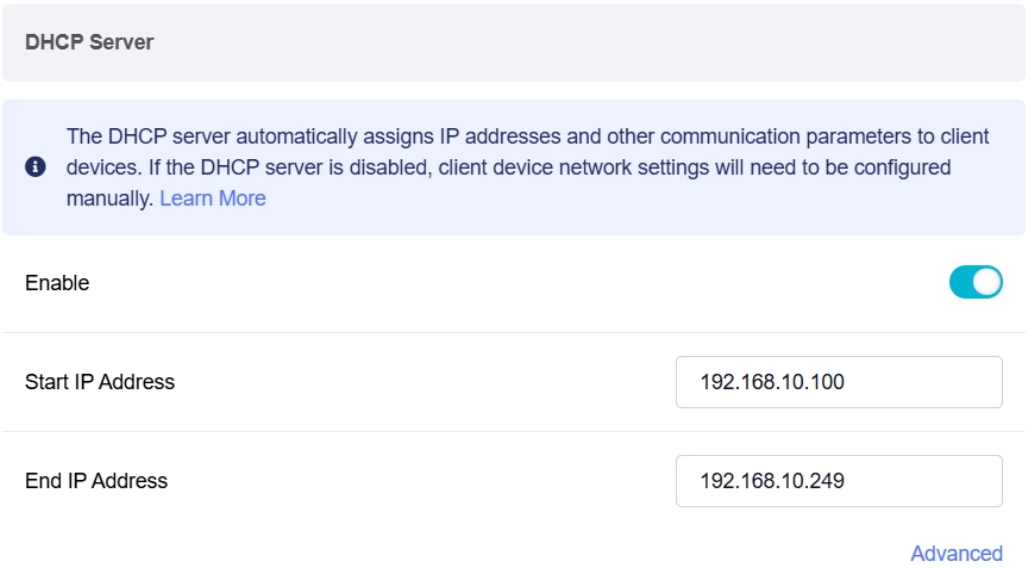


- **Gateway**: domyślny adres to 192.168.10.1. Można go zmienić, ale nie może kolidować z adresem bramy sieci głównej.
- **Netmask**: dostępne są dwie opcje: 255.255.255.0 i 255.255.0.0.
- **VAN ID**: domyślny identyfikator VLAN sieci gościnnej to 10. Można go zmienić w razie potrzeby.
- **AP Isolation**: izoluje klientów sieci gościnnej w oddzielnych segmentach, aby nie mogli komunikować się z innymi urządzeniami w tej samej sieci.
- **WAN Access Control**: zarządza dostępem lokalnej podsieci do sieci po stronie WAN, w tym do Internetu i innych podsieci WAN.
  Dostępne są trzy tryby kontroli dostępu do WAN:
  - **Unrestricted**: umożliwia tej podsieci nieograniczony dostęp do Internetu i innych podsieci po stronie WAN.
  - **Block WAN Subnet**: blokuje dostęp do innych podsieci po stronie WAN. Dostęp do Internetu pozostaje dostępny.
  - **Block Internet Access**: blokuje cały dostęp wychodzący, w tym do Internetu i podsieci po stronie WAN.

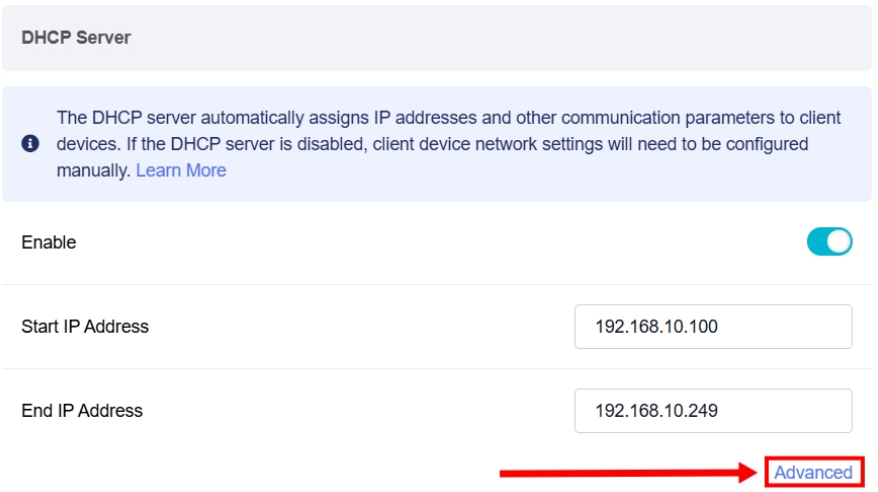
Serwer DHCP

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

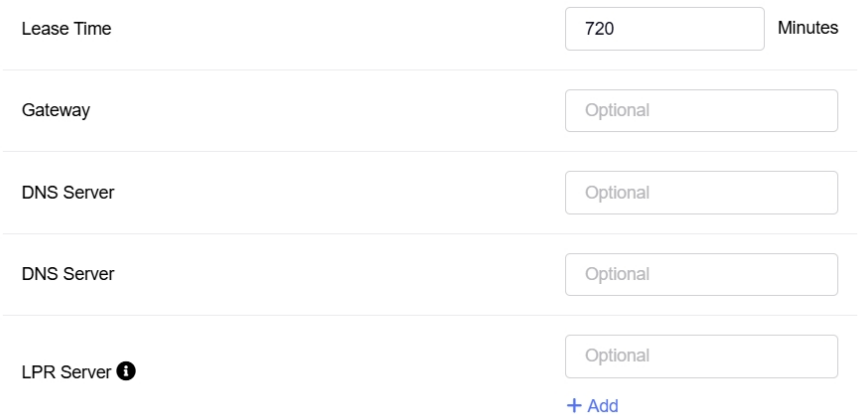
Po włączeniu serwer DHCP automatycznie przypisuje adresy IP i inne parametry komunikacji każdemu podłączonemu klientowi. Pula adresów IP serwera DHCP dla sieci IoT obejmuje zakres od 192.168.10.100 do 192.168.10.249. W razie potrzeby możesz go dostosować.



Kliknij **Advanced** w prawym dolnym rogu.



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

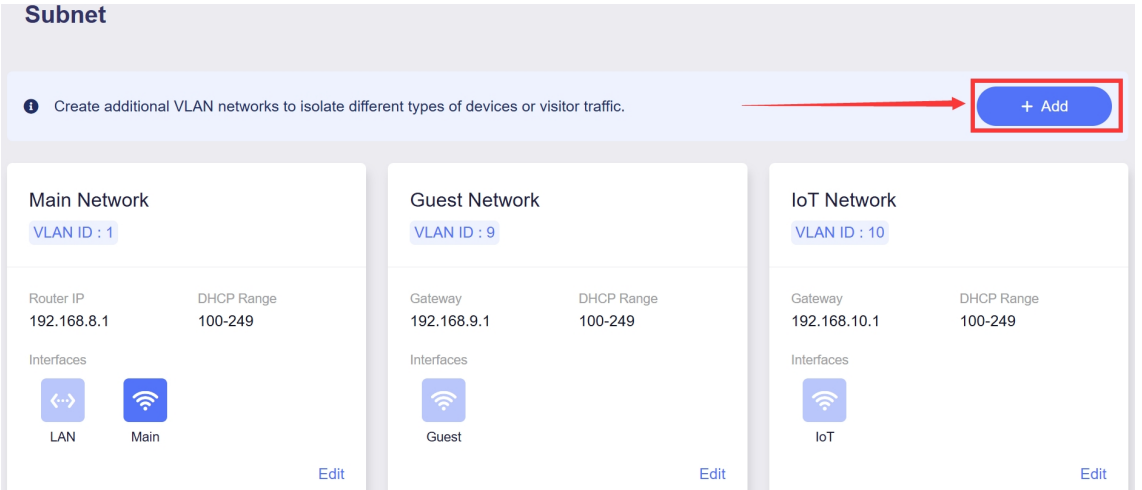


- **Lease Time**: czas, przez który urządzenie może korzystać z adresu IP przydzielonego przez DHCP sieci gościnnej.
- **Gateway**: element routera kierujący ruch między siecią gościnną a sieciami zewnętrznymi (np. Internetem).
- **DNS Server** : dwa pola serwerów DNS umożliwiają skonfigurowanie podstawowego i zapasowego serwera rozpoznającego nazwy. Podstawowy DNS wpisuje się w górnym polu, a zapasowy w dolnym. Gdy serwer podstawowy jest niedostępny, urządzenia klienckie automatycznie przełączają się na zapasowy, zapewniając ciągłość rozpoznawania nazw domen.
- **LPR Server** (Line Printer Remote Server): usługa zarządzająca zadaniami drukowania, która umożliwia urządzeniom sieciowym wysyłanie żądań drukowania do zdalnych drukarek. Można skonfigurować wiele portów LPR dla drukarek.

12.2.4 Sieci VLAN

VLAN Networks umożliwia tworzenie dodatkowych sieci VLAN w celu oddzielenia różnych typów urządzeń lub ruchu gości zależnie od potrzeb.

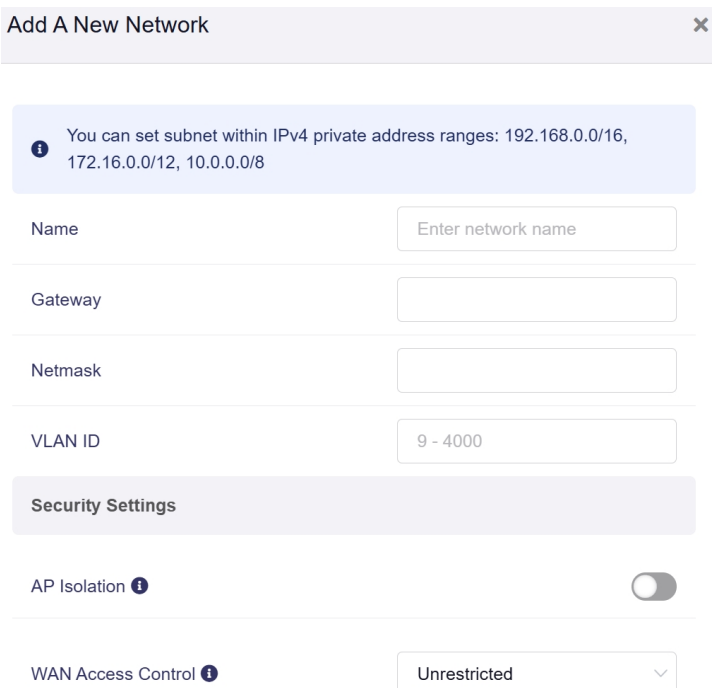
Kliknij przycisk **+ Add** po prawej stronie, aby skonfigurować nową sieć.



Na tej stronie możesz skonfigurować ustawienia sieci VLAN, w tym ustawienia podstawowe i serwer DHCP.

Ustawienia podstawowe

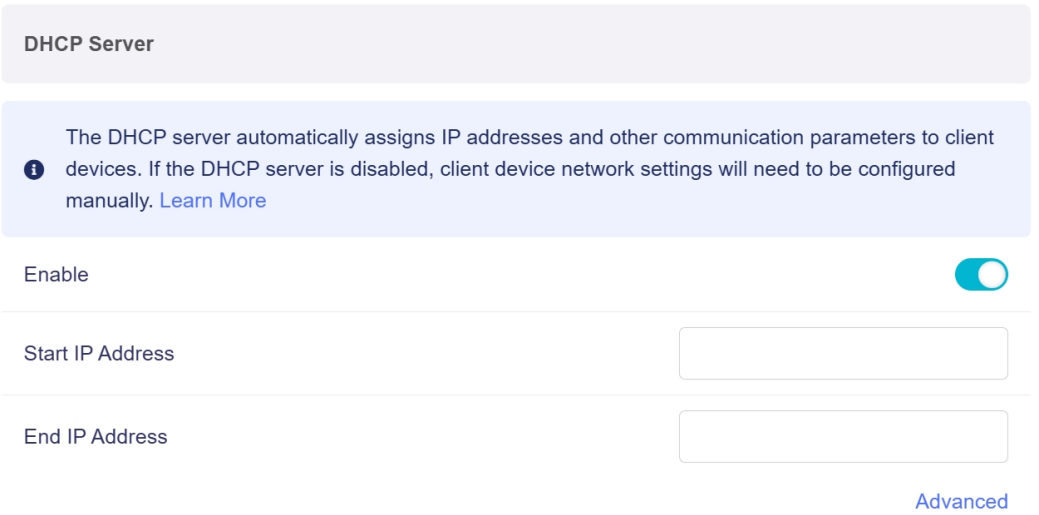
Na tej stronie możesz skonfigurować podstawowe informacje o sieciach VLAN.



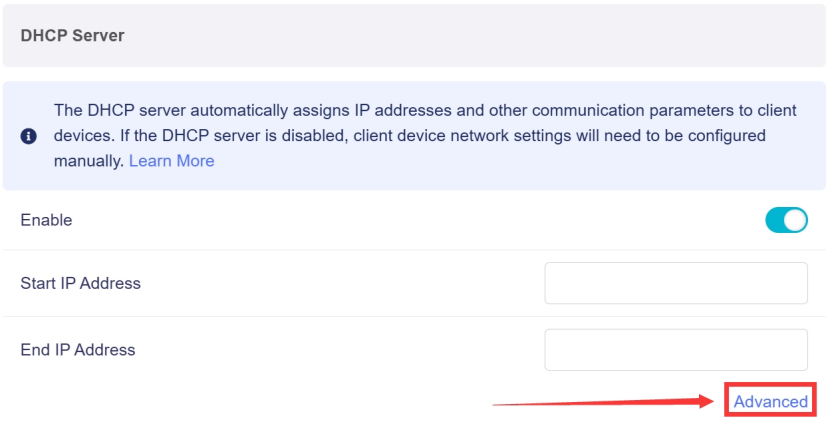
- **Name**: nadaj nowo utworzonej podsieci własną nazwę, aby ułatwić jej identyfikację.
- **Gateway**: domyślny adres to 192.168.10.1. Można go zmienić, ale nie może kolidować z adresem bramy sieci głównej.
- **Netmask**: dostępne są dwie opcje: 255.255.255.0 i 255.255.0.0.
- **VAN ID**: podczas tworzenia podsieci należy przypisać identyfikator VLAN z zakresu od 9 do 4000. Nie używaj zajętego identyfikatora VLAN, aby uniknąć konfliktów sieciowych.
- **AP Isolation**: izoluje klientów sieci gościnnej w oddzielnych segmentach, aby nie mogli komunikować się z innymi urządzeniami w tej samej sieci.
- **WAN Access Control**: zarządza dostępem lokalnej podsieci do sieci po stronie WAN, w tym do Internetu i innych podsieci WAN.
  Dostępne są trzy tryby kontroli dostępu do WAN:
  - **Unrestricted**: umożliwia tej podsieci nieograniczony dostęp do Internetu i innych podsieci po stronie WAN.
  - **Block WAN Subnet**: blokuje dostęp do innych podsieci po stronie WAN. Dostęp do Internetu pozostaje dostępny.
  - **Block Internet Access**: blokuje cały dostęp wychodzący, w tym do Internetu i podsieci po stronie WAN.

Serwer DHCP

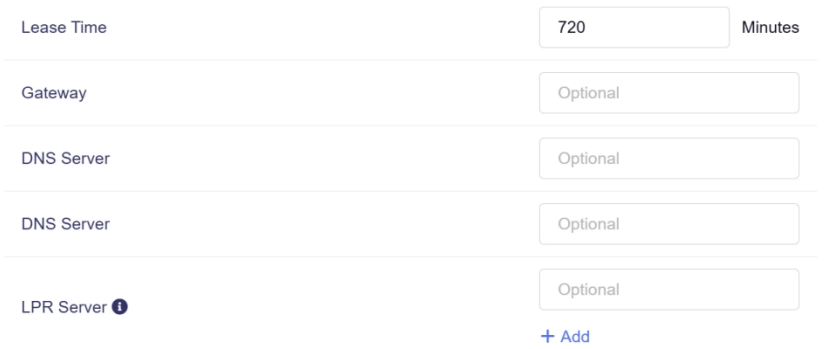
Po włączeniu serwer DHCP automatycznie przypisuje adresy IP i inne parametry komunikacji każdemu podłączonemu klientowi. W razie potrzeby możesz dostosować zakres adresów.



W razie potrzeby kliknij **Advanced**, aby przejść do dalszej konfiguracji.



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



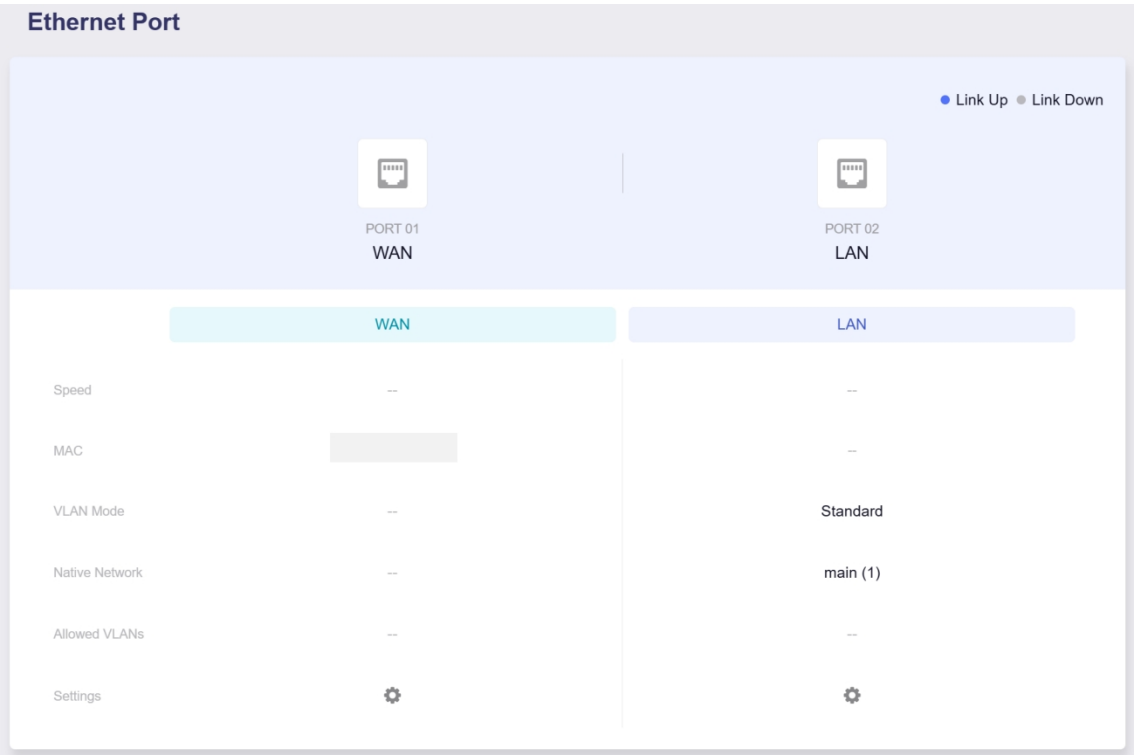
- **Lease Time**: czas, przez który urządzenie może korzystać z adresu IP przydzielonego przez DHCP sieci gościnnej.
- **Gateway**: element routera kierujący ruch między siecią gościnną a sieciami zewnętrznymi (np. Internetem).
- **DNS Server** : dwa pola serwerów DNS umożliwiają skonfigurowanie podstawowego i zapasowego serwera rozpoznającego nazwy. Podstawowy DNS wpisuje się w górnym polu, a zapasowy w dolnym. Gdy serwer podstawowy jest niedostępny, urządzenia klienckie automatycznie przełączają się na zapasowy, zapewniając ciągłość rozpoznawania nazw domen.
- **LPR Server** (Line Printer Remote Server): usługa zarządzająca zadaniami drukowania, która umożliwia urządzeniom sieciowym wysyłanie żądań drukowania do zdalnych drukarek. Można skonfigurować wiele portów LPR dla drukarek.

Po skonfigurowaniu nowa sieć VLAN pojawi się na bieżącej stronie wraz z informacjami o podsieci.

12.3 Port Ethernet

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

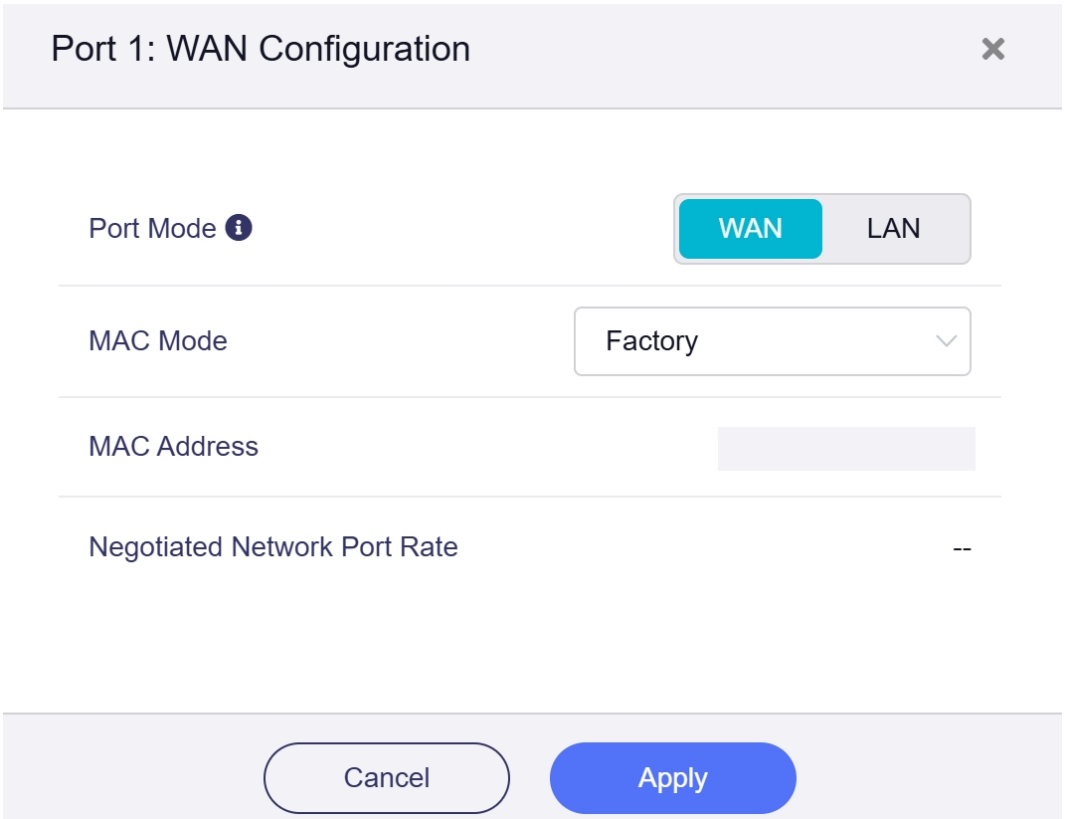
Strona Ethernet Port wyświetla wszystkie interfejsy routera. Możesz sprawdzić stan połączenia każdego interfejsu, zarządzać rolami portów Ethernet (WAN lub LAN) i wyświetlać szczegóły portów, takie jak adres MAC, wynegocjowana szybkość i bieżący stan łącza. Możesz też przypisywać interfejsy fizyczne do utworzonych podsieci.



- **Link up**: niebieska ikona portu oznacza aktywne łącze fizyczne.
- **Link Down**: szara ikona portu oznacza nieaktywne łącze fizyczne.
- **Speed**: wynegocjowana szybkość transmisji portu Ethernet.
- **MAC**: adres MAC portu.
- **VLAN ID**: porty LAN mogą działać w trybie Standard lub Multiple VLANs.
- **Native Network**: domyślna nieoznaczona podsieć przypisana do portu LAN.
- **Allowed VLANs**: określa oznaczone sieci VLAN, które mogą przechodzić przez ten port w trybie Multiple VLANs.
- **Settings**: kliknij, aby otworzyć stronę konfiguracji danego portu.

12.3.1 WAN

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



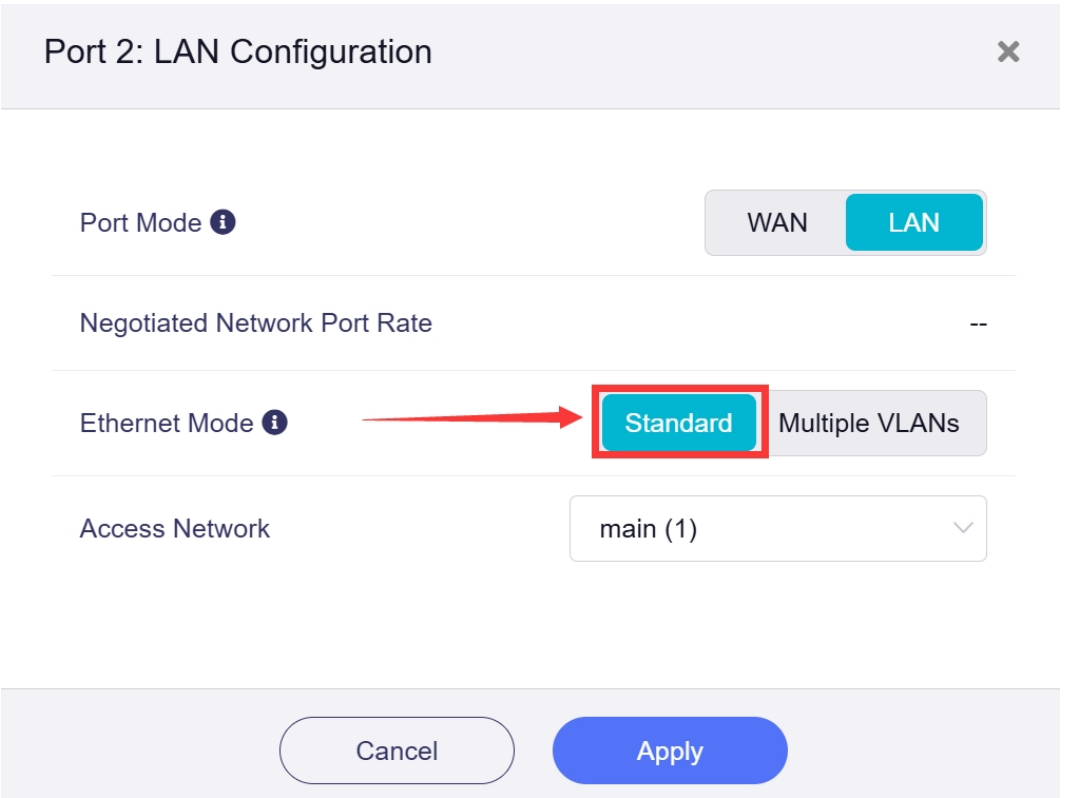
- **Port Mode**: bieżący tryb pracy fizycznego portu WAN. W razie potrzeby możesz ustawić go jako LAN.
- **MAC Mode:** domyślnie Factory Mode. Możesz przełączyć na Clone Mode lub Random Mode.
- **MAC Address**: adres MAC interfejsu WAN.
- **Negotiated Network Port Rate:** wynegocjowana szybkość łącza interfejsu WAN. Jest wyświetlana tylko po wykryciu prawidłowego łącza.

12.3.2 LAN

Sekcja **LAN** wyświetla konfigurację portu LAN. Możesz zmieniać rolę portu między **LAN** a **WAN**, wybierać tryb Ethernet portu LAN (Standard lub Multiple VLANs) i sprawdzać wynegocjowaną prędkość łącza.

1. Tryb Standard

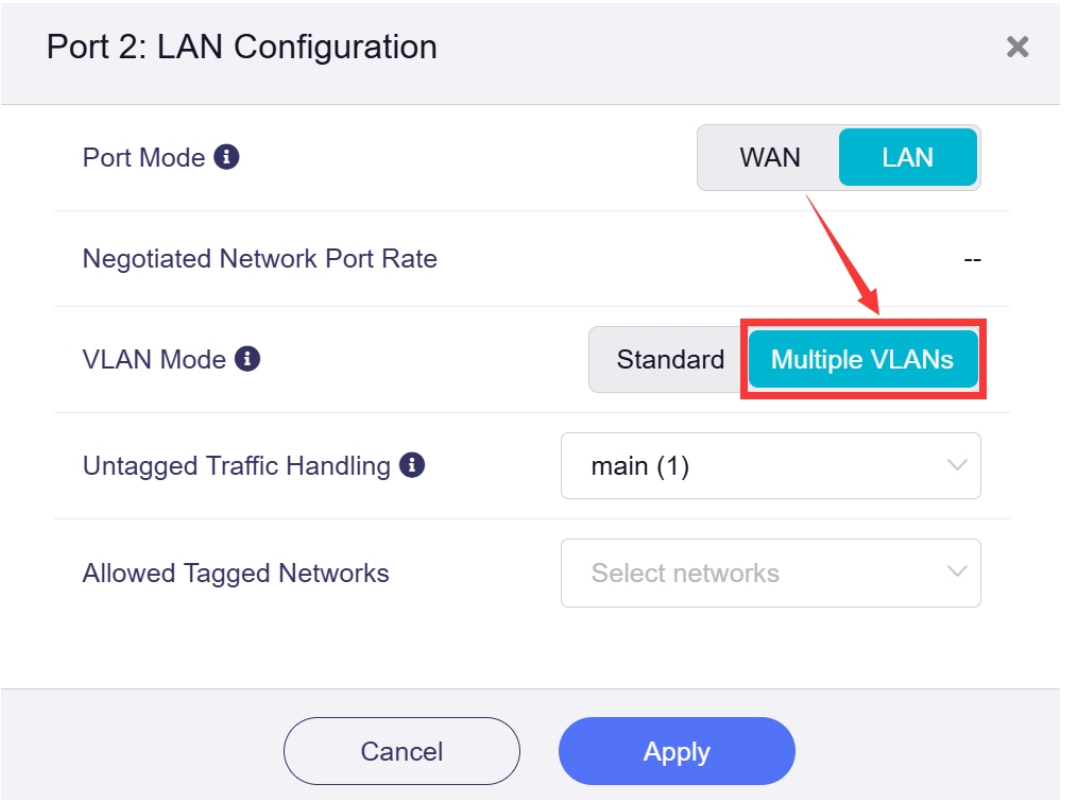
   Tryb Standard pozwala korzystać tylko z jednej sieci VLAN (bez oznaczenia) i służy do podłączania urządzeń końcowych.



- **Negotiated Network Port Rate**: wynegocjowana szybkość łącza interfejsu LAN. Jest wyświetlana tylko po wykryciu prawidłowego łącza.
- **Ethernet Mode**: domyślnie Standard Mode.
- **Access Network**: umożliwia izolowanie sieci przez przypisywanie portów LAN do różnych podsieci.

2. Tryb Multiple VLANs

   Tryb Multiple VLANs umożliwia korzystanie z wielu oznaczonych sieci VLAN na jednym porcie. Zwykle służy do podłączania punktów dostępowych lub innych przełączników.



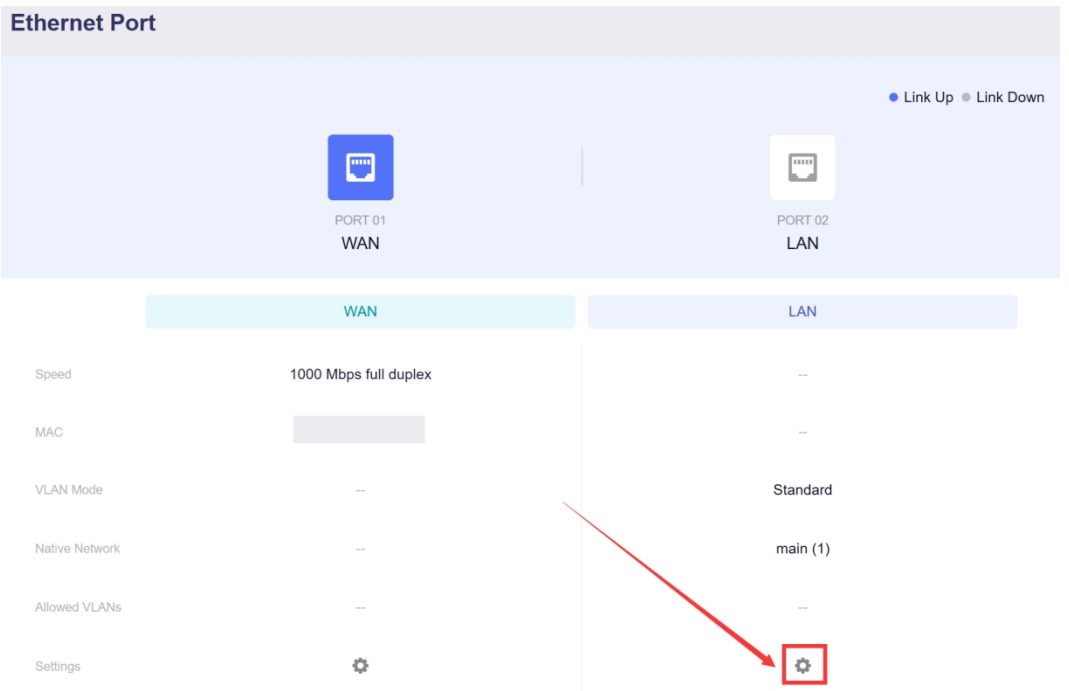
- **Negotiated Network Port Rate**: wynegocjowana szybkość łącza interfejsu LAN. Jest wyświetlana tylko po wykryciu prawidłowego łącza.
- **VLAN Mode**: aby przełączyć na tryb wielu sieci VLAN, kliknij kartę Multiple VLANs.
- **Untagged Traffic Handling**: konfiguruje obsługę nieoznaczonych pakietów na porcie. Możesz odrzucać je bezpośrednio lub przekazywać do innej podsieci jako natywnej sieci PVID.
- **Allowed Tagged Networks**: określa sieci VLAN, które mogą przechodzić przez port z oznaczeniem. Możesz wybrać sieci VLAN z listy. Przekazywany będzie tylko pasujący ruch.

Uwaga: wynegocjowana prędkość portów WAN i LAN jest wyświetlana tylko po podłączeniu kabla
Ethernet. Zależy ona zarówno od portu Ethernet, jak i od kabla Ethernet.

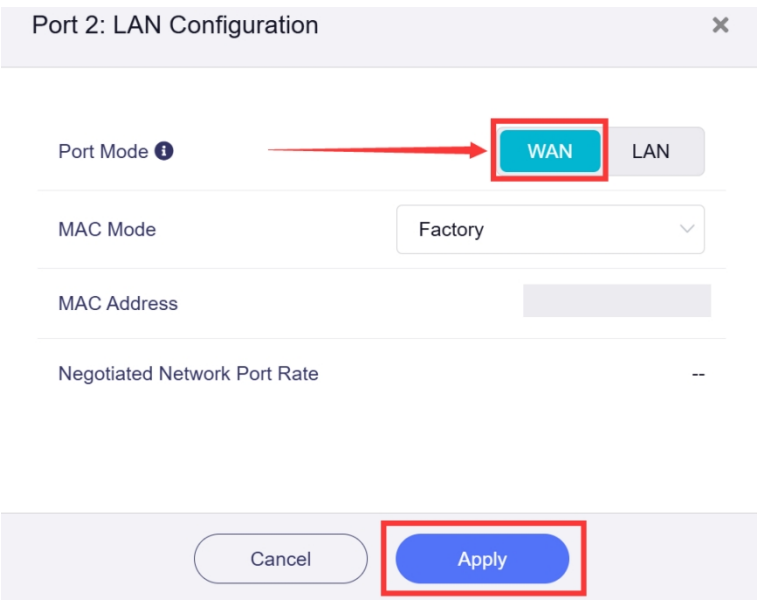
12.3.3 Dwa łącza Ethernet WAN

Funkcja Dual-Ethernet WAN umożliwia przekształcenie domyślnego portu Ethernet LAN w dodatkowy port WAN, aby korzystać z dwóch przewodowych łączy internetowych. Pozwala też jednocześnie łączyć się z dwiema niezależnymi sieciami (np. służbową i prywatną), zwiększając elastyczność bez dodatkowego sprzętu.

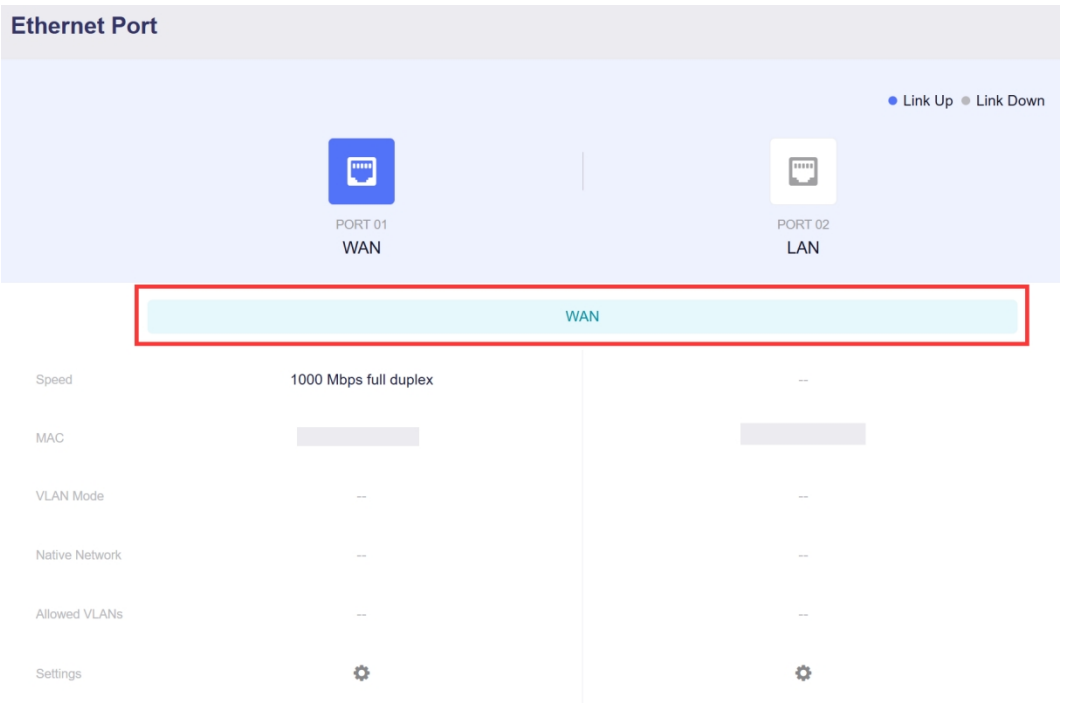
1. Na stronie Ethernet Port kliknij ustawienie LAN, aby otworzyć stronę Configuration.



2. Zmień rolę portu na WAN i kliknij **Apply**.



3. Wróć do strony Ethernet Port, aby sprawdzić, czy rola portu zmieniła się na WAN. Port LAN będzie wtedy działać jako port WAN.

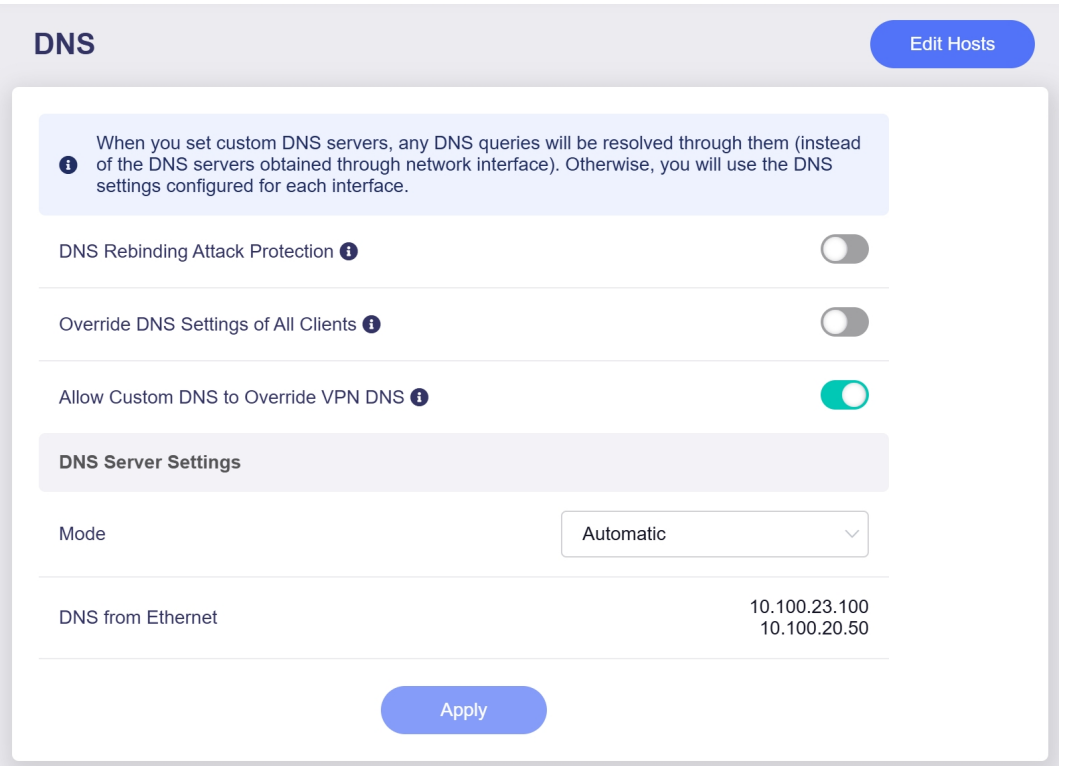


12.4 DNS

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.

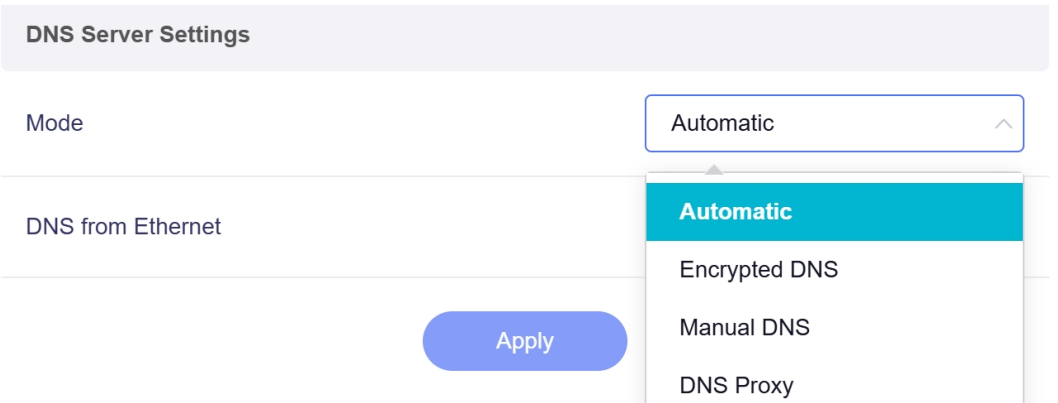
Zaloguj się do panelu administracyjnego routera i przejdź do **NETWORK** > **DNS**. Ta strona umożliwia konfigurację ustawień DNS, w tym opcji bezpieczeństwa, trybów serwera i reguł priorytetów DNS w różnych scenariuszach sieciowych.



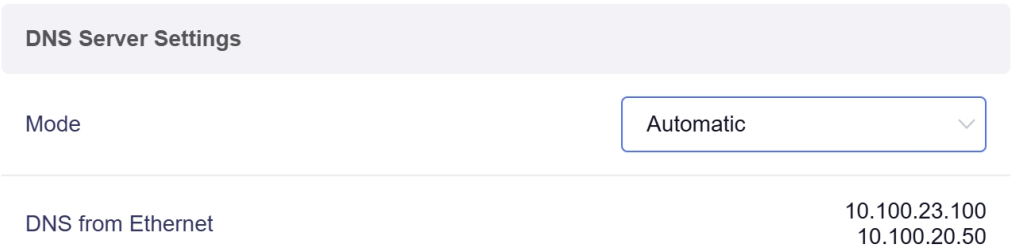
- **DNS Rebinding Attack Protection**: chroni przed atakami DNS rebinding przez blokowanie złośliwych prób rozwiązywania nazw DNS. Włączenie może spowodować problemy z prywatnymi zapytaniami DNS. Wyłącz tę opcję, jeśli sieć korzysta z portalu logowania (np. strony logowania do publicznego Wi-Fi).
- **Override 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.

12.4.1 Ustawienia serwera DNS

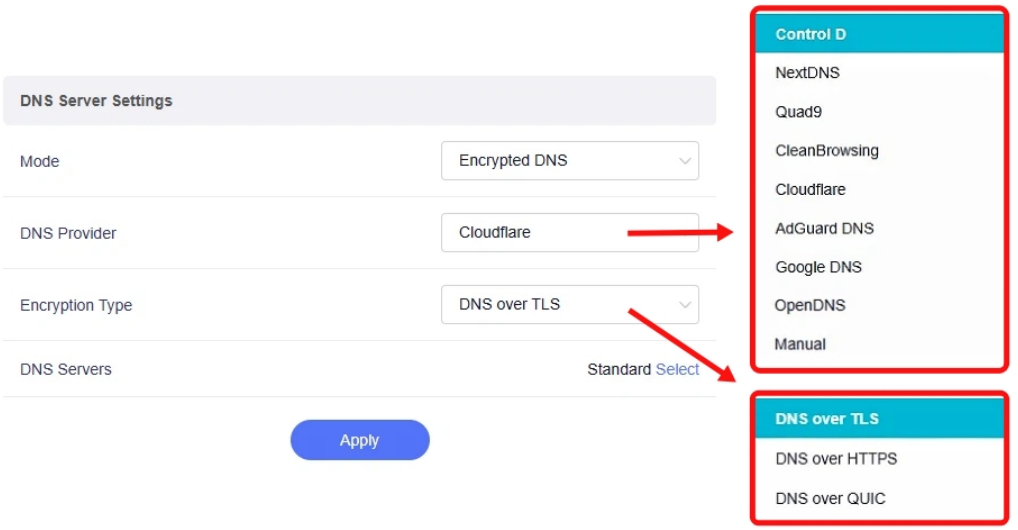
Dostępne są cztery tryby serwera DNS: Automatic, Encrypted DNS, Manual DNS i DNS Proxy.



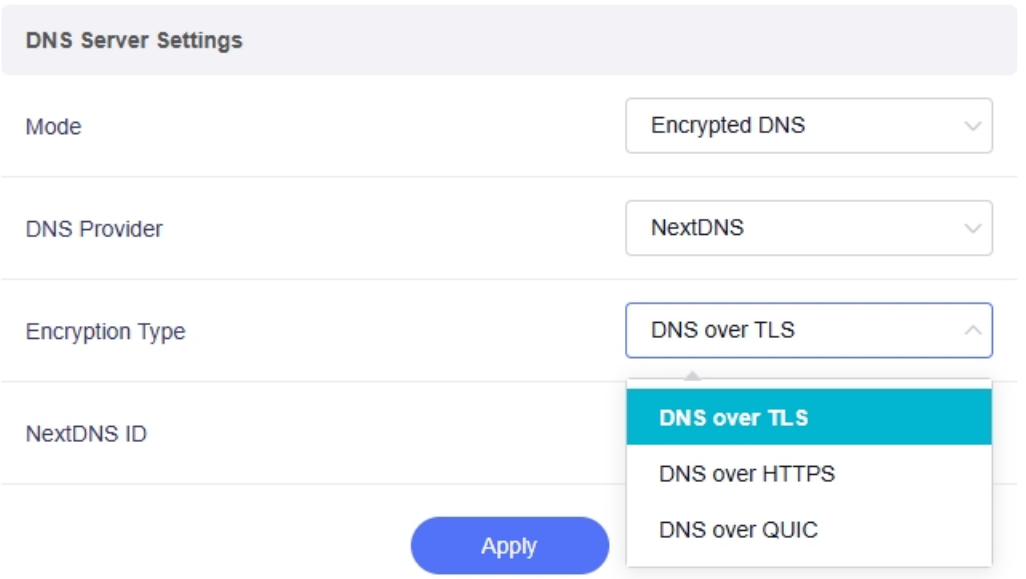
1. **Automatic**: router automatycznie pobiera adresy serwerów DNS z sieci nadrzędnej i stosuje je do wszystkich podłączonych urządzeń.



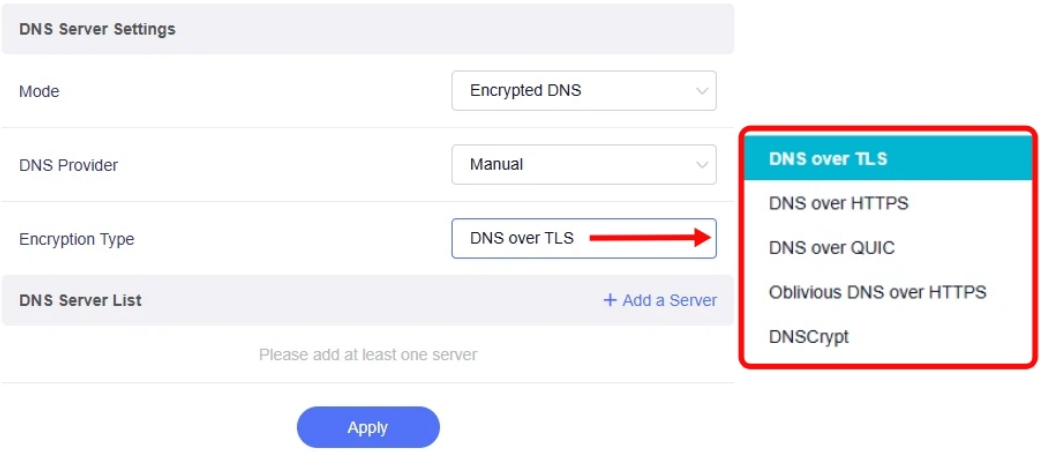
2. **Encrypted DNS**: router używa szyfrowanych protokołów do obsługi zapytań DNS, chroniąc dane rozwiązywania nazw przed podsłuchiwaniem i modyfikacją.
   Tryb Encrypted DNS obsługuje wielu dostawców DNS: Control D, NextDNS, Cloudflare, Quad9, CleanBrowsing, AdGuard DNS, Google DNS i OpenDNS.
   Najpierw wybierz dostawcę DNS. Pozostałe opcje zmienią się zależnie od wyboru.



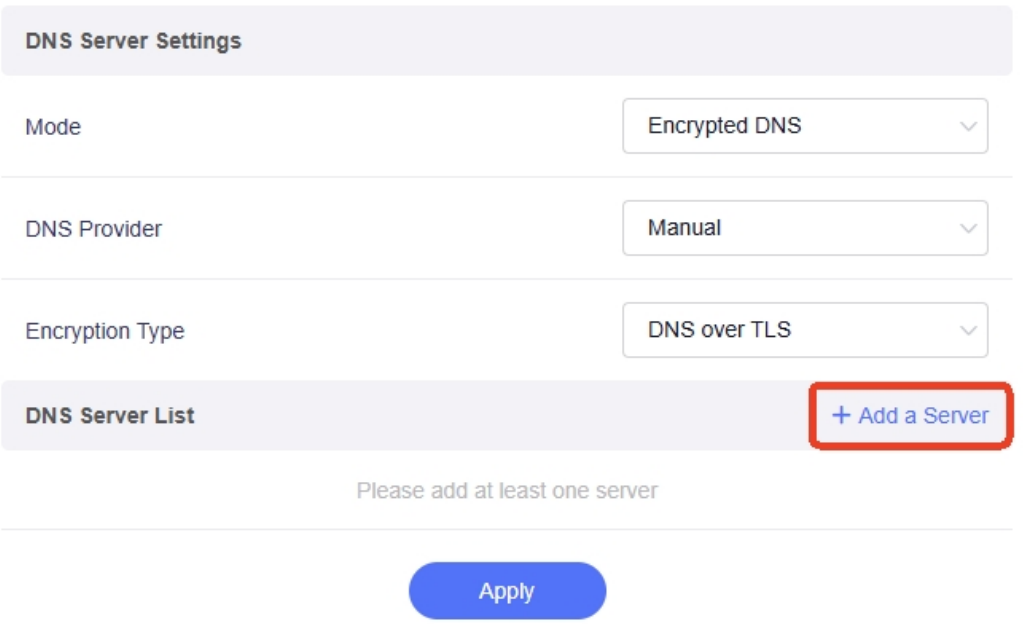
- Jeśli wybierzesz konkretnego dostawcę DNS (np. NextDNS), wybierz typ szyfrowania: DNS over TLS (DoT), DNS over HTTPS (DoH) lub DNS over QUIC (DoQ). DNS over QUIC (DoQ) wprowadzono w oprogramowaniu sprzętowym v4.9. Jest dostępny tylko dla dostawców Control D, NextDNS i AdGuard DNS.



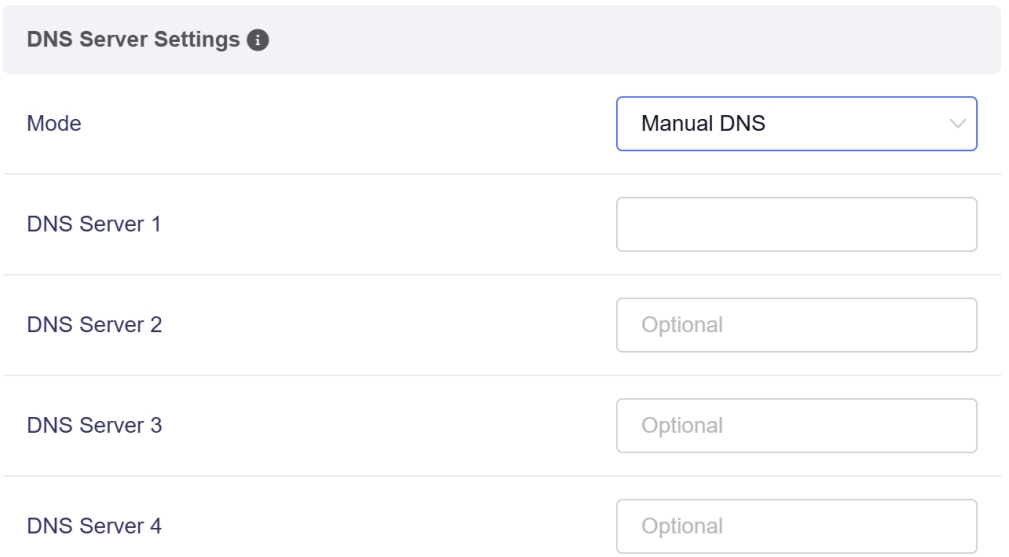
- Jeśli jako dostawcę DNS wybierzesz Manual, wybierz typ szyfrowania: DNS over TLS (DoT), DNS over HTTPS (DoH), DNS over QUIC (DoQ), Oblivious DNS over HTTPS lub DNSCrypt.



Następnie **kliknij Add a** Server, aby dodać co najmniej jeden serwer DNS. Możesz bezpośrednio wprowadzić adres URL lub zaszyfrowany DNS w formacie stamp. Listę serwerów publicznych znajdziesz na stronie https://dnscrypt.info/public-servers.

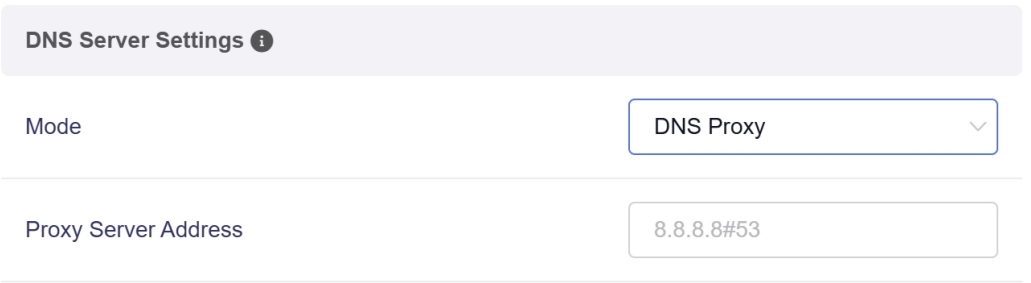


3. **Manual DNS**: umożliwia samodzielne ustawienie serwerów DNS routera. Kliknij DNS Server 1 i wybierz serwer z listy. Pozostałe pola DNS zaktualizują się automatycznie.



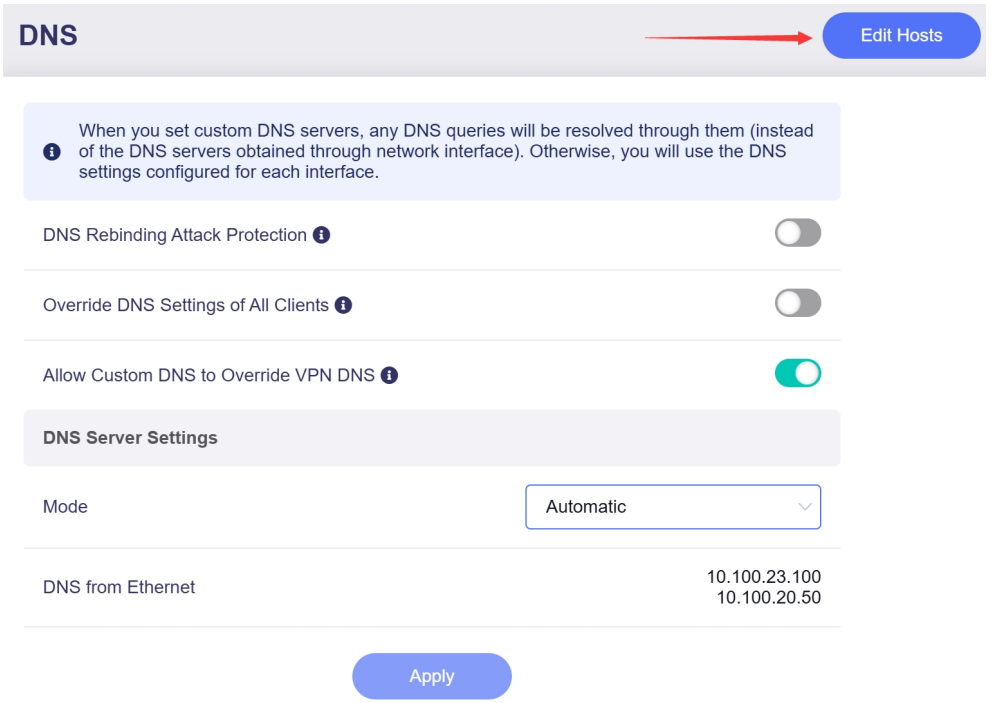
Uwaga: aby używać adresów IPv6 w ręcznej konfiguracji DNS, najpierw włącz IPv6 na routerze.

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

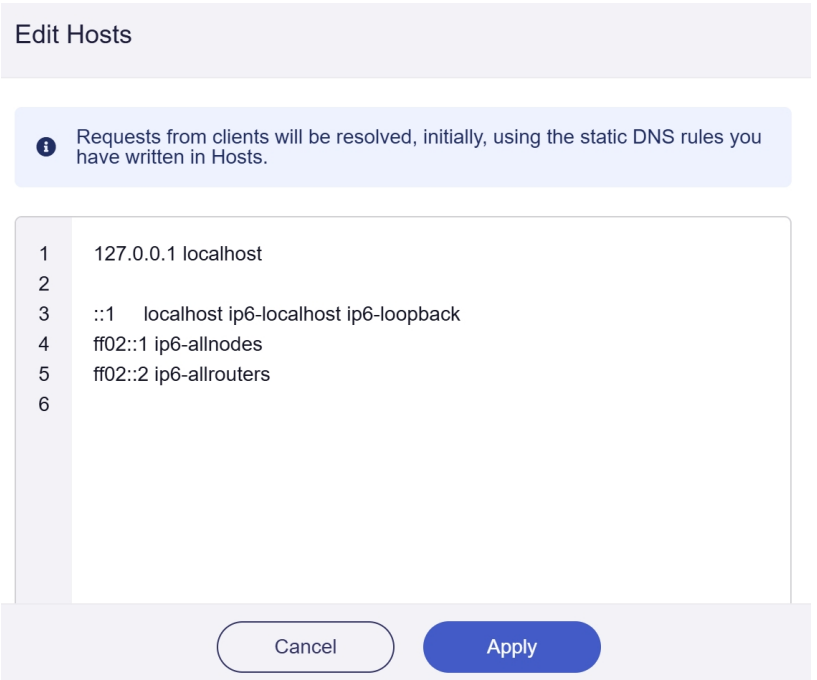


12.4.2 Edycja pliku hosts

W razie potrzeby możesz zdefiniować statyczne reguły rozpoznawania 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.

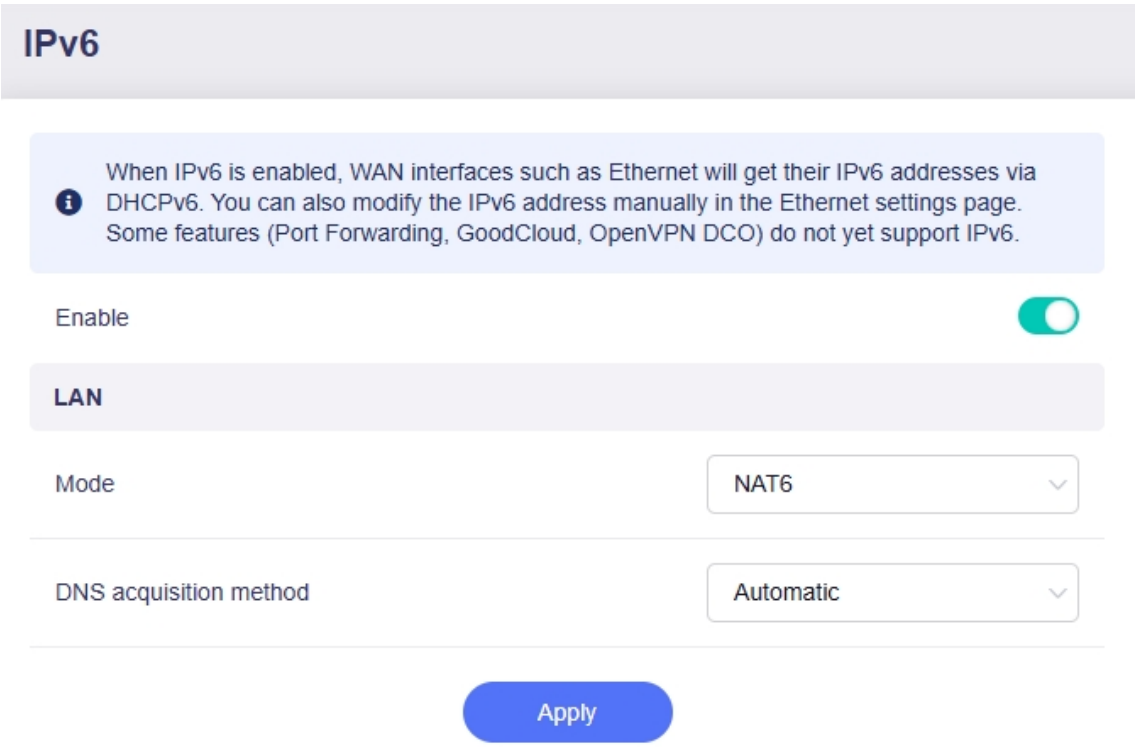

Edit Hosts
Requests from clients will be resolved, initially, using the static DNS rules you have written in Hosts.
1 127.0.0.1 localhost
2
3 ::1 localhost ip6-localhost ip6-loopback
4 ff02::1 ip6-allnodes
5 ff02::2 ip6-allrouters
6
Cancel
Apply

12.5 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.

12.5.1 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.

12.5.2 Sposób uzyskiwania DNS

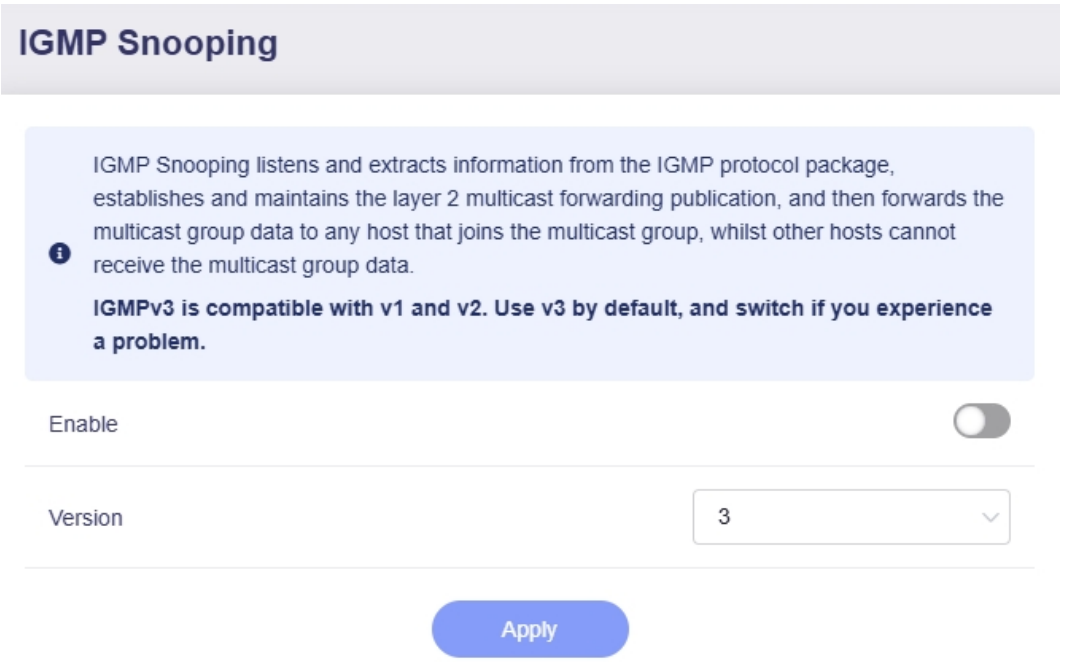
Określa sposób uzyskiwania przez router adresów serwerów DNS IPv6. Dostępne są dwie opcje: Automatic i Manual.

- **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.

12.6 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.

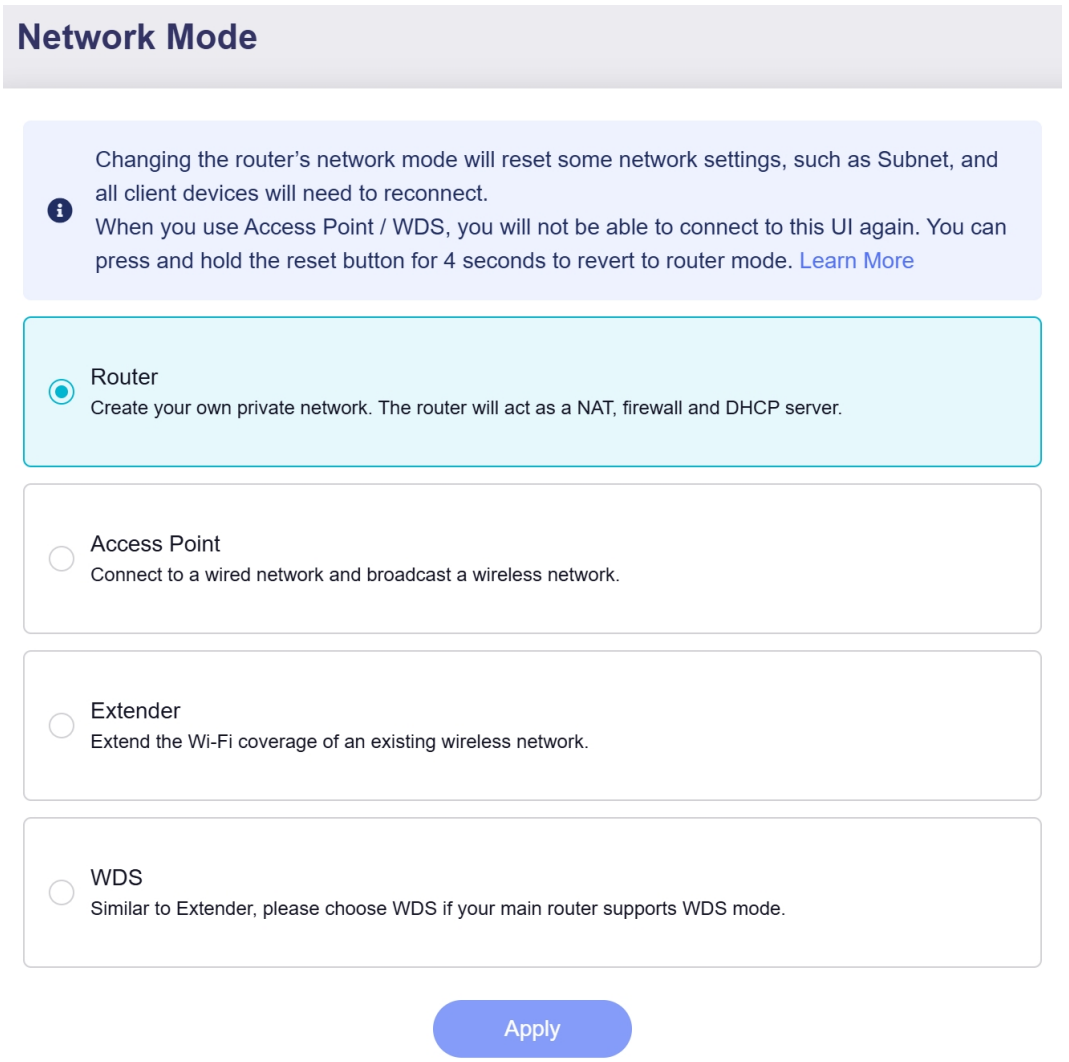
Zaloguj się do panelu administracyjnego routera i przejdź do **NETWORK** > **IGMP Snooping**. W razie potrzeby włącz tę opcję, aby korzystać z multicastu na routerze.



12.7 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.

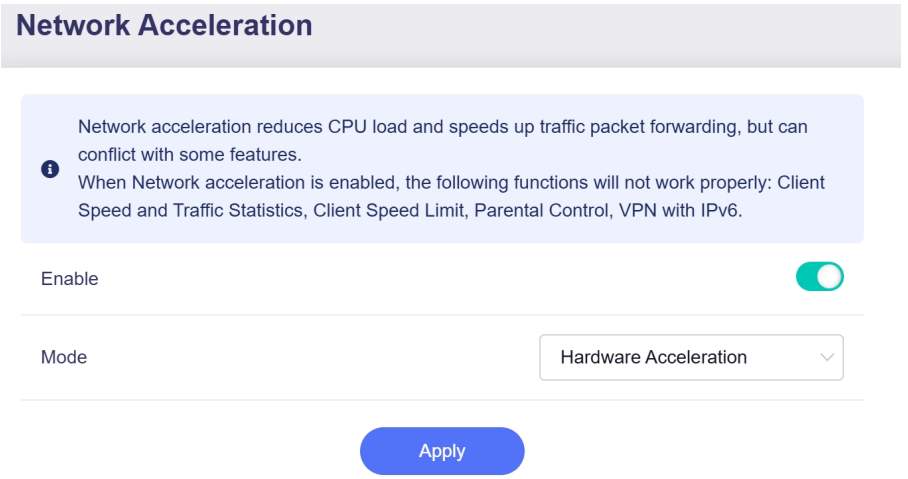
Uwaga:

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**: Access Control (Allowlist i Blocklist), GoodPAS, VPN, AdGuard Home, Parental Control, ZeroTier, Tailscale, Port Forwarding, Multi-WAN, DHCP Server, Address Reservation, Guest Network, DNS, Ethernet Port, IPv6, Drop-in Gateway, IGMP Snooping, Network Acceleration, NAT Settings.

12.8 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 Hardware Acceleration lub Software Acceleration.



- **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.

Rozdział 13

Kontrola ruchu

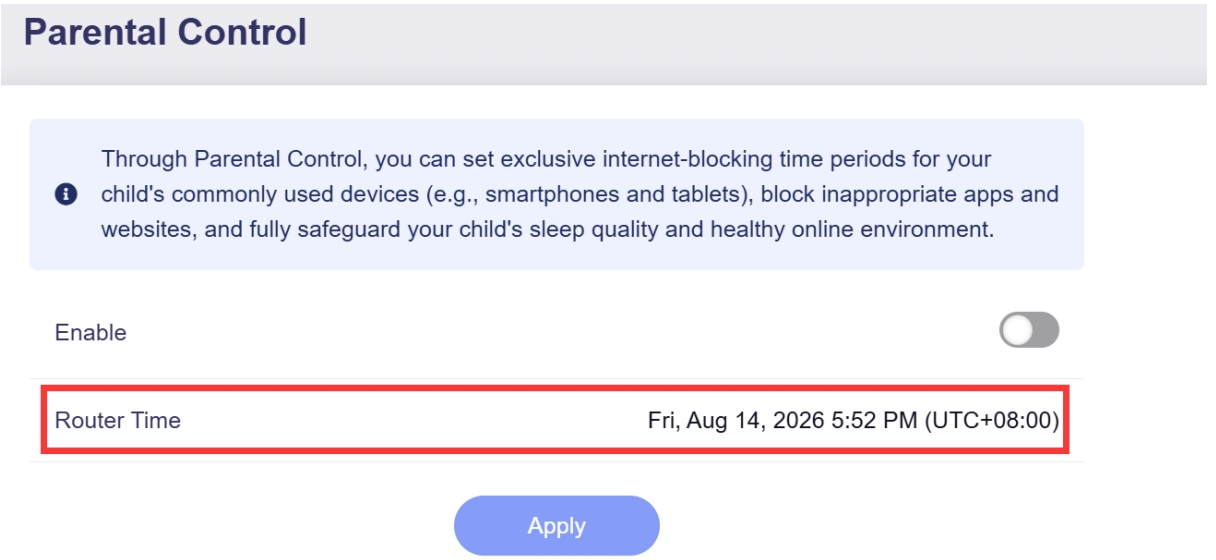
W tym rozdziale przedstawiono kontrolę rodzicielską, czyli narzędzie do filtrowania witryn i ustawiania limitów korzystania.

13.1 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.

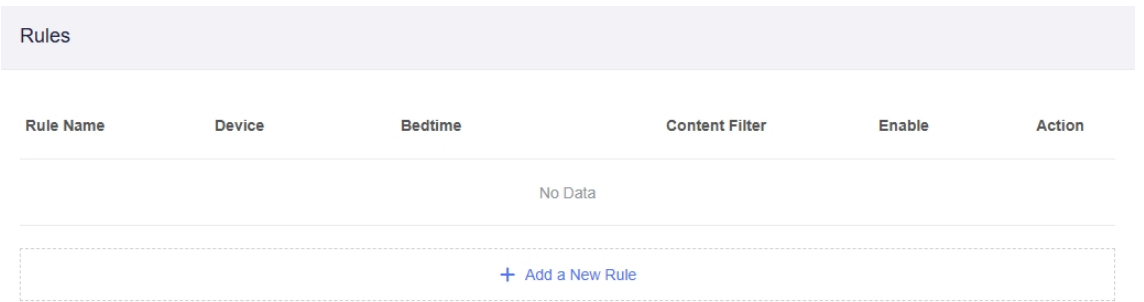
Aby skonfigurować kontrolę rodzicielską, wykonaj poniższe czynności.

1. Zaloguj się do panelu administracyjnego routera i przejdź **do FLOW CONTROL** > **Parental Control.** Upewnij się, że czas routera jest prawidłowy.

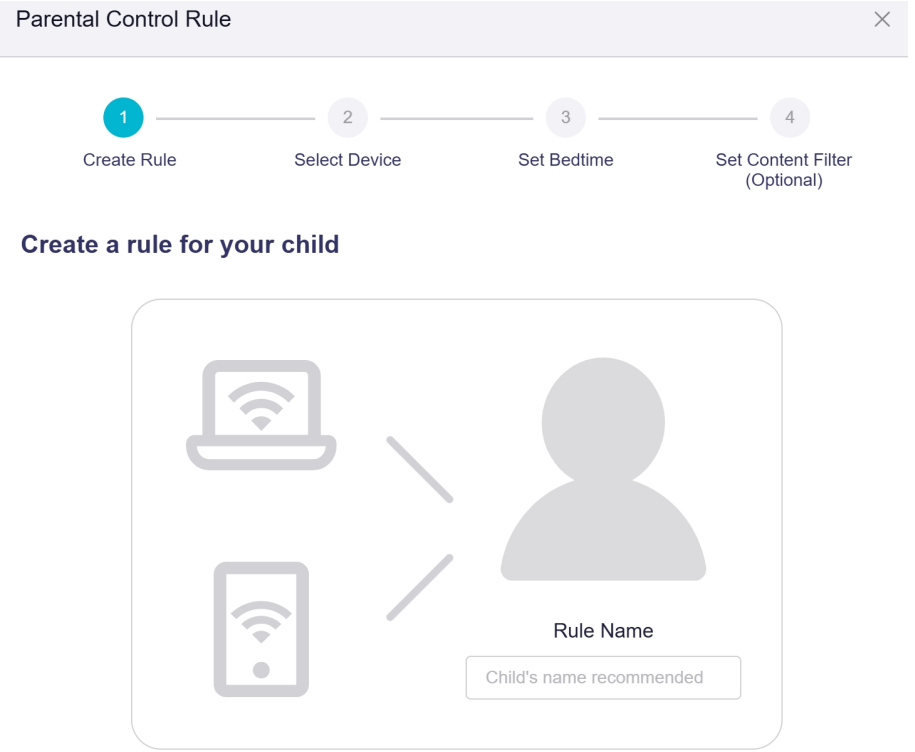


   Jeśli nie, najpierw **przejdź do SYSTEM >** Time Zone i zsynchronizuj czas.

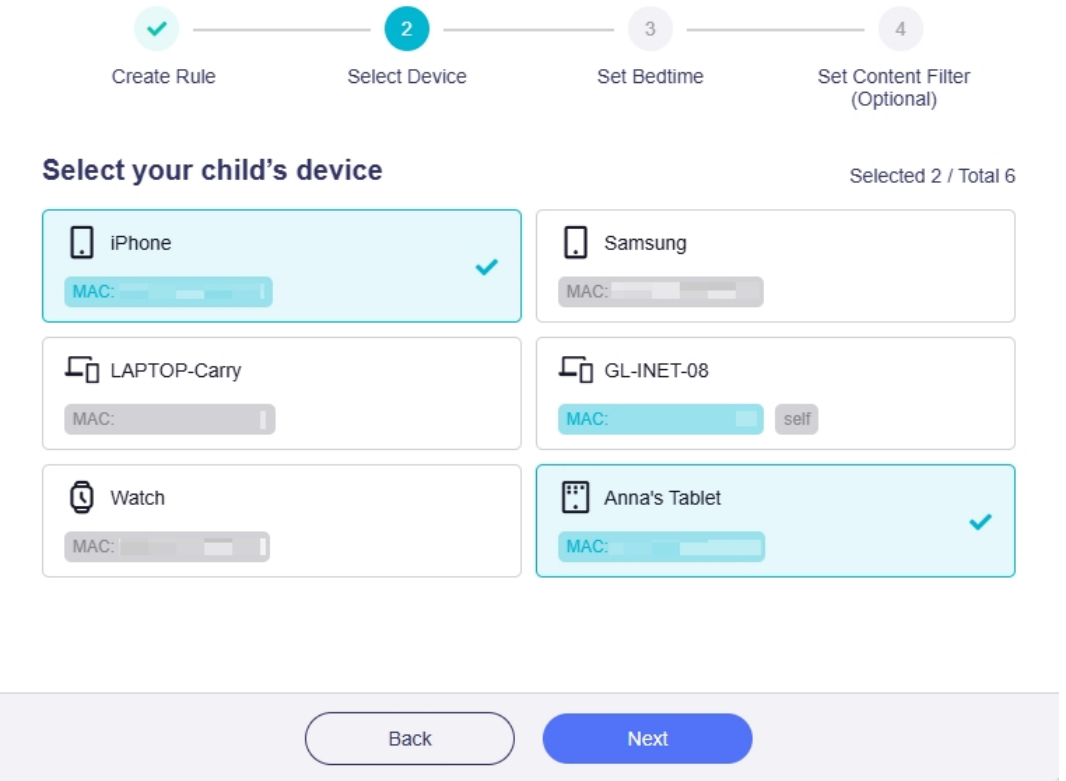
2. Włącz kontrolę rodzicielską i kliknij **Apply**.
3. Pojawi się poniższa lista reguł. Kliknij **Add a New Rule**.



4. W wyświetlonym oknie utwórz regułę, nadaj jej własną nazwę i kliknij **Next**.

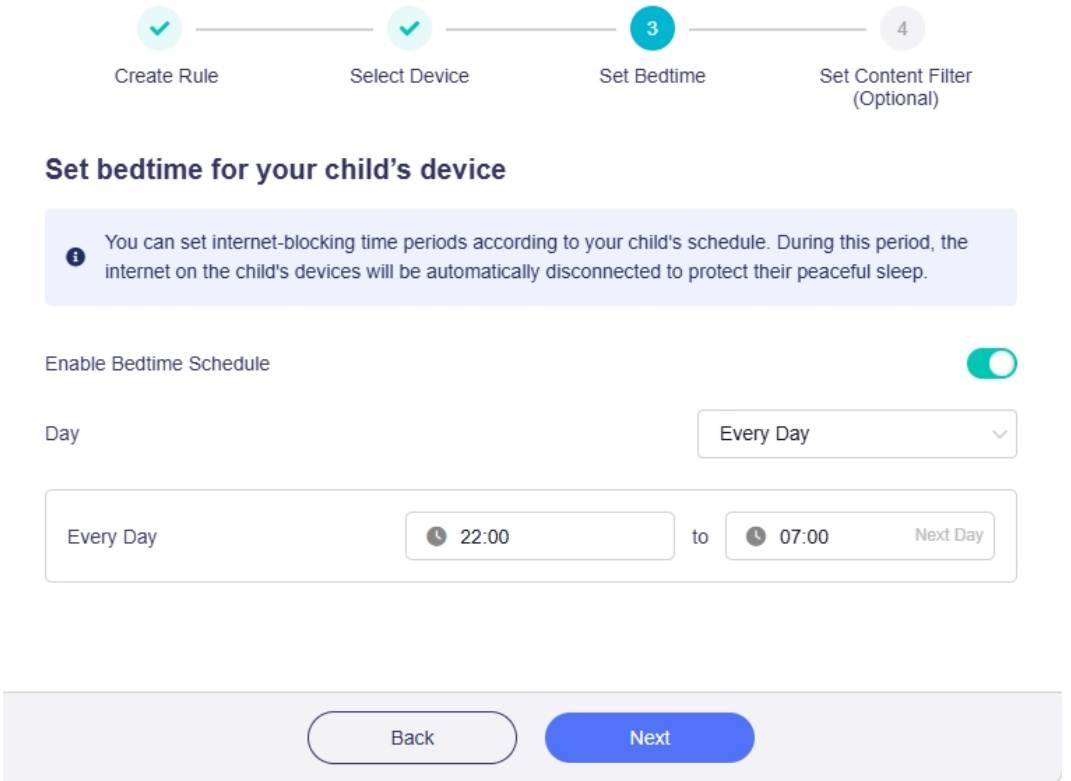


5. Wybierz urządzenie dziecka i kliknij **Next**.
   Urządzenia pojawią się na tej stronie tylko wtedy, gdy są podłączone do routera przez Wi-Fi lub Ethernet. Kolor turkusowy oznacza urządzenie online, a szary — offline.



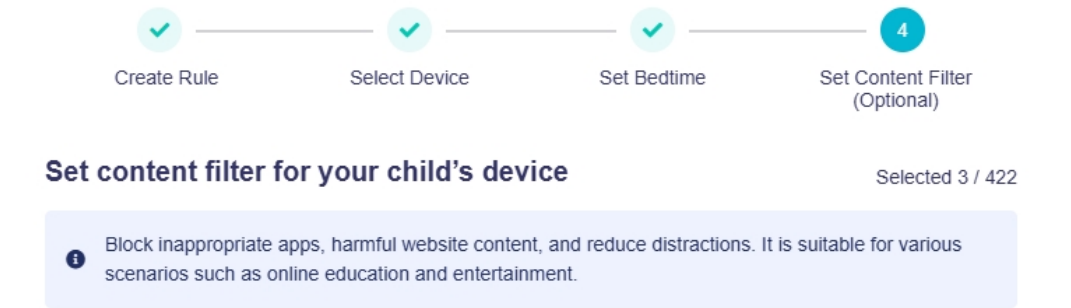
Wskazówka: aby łatwiej rozróżniać podłączone urządzenia, przejdź **na stronę** CLIENTS i nadaj im własne nazwy.

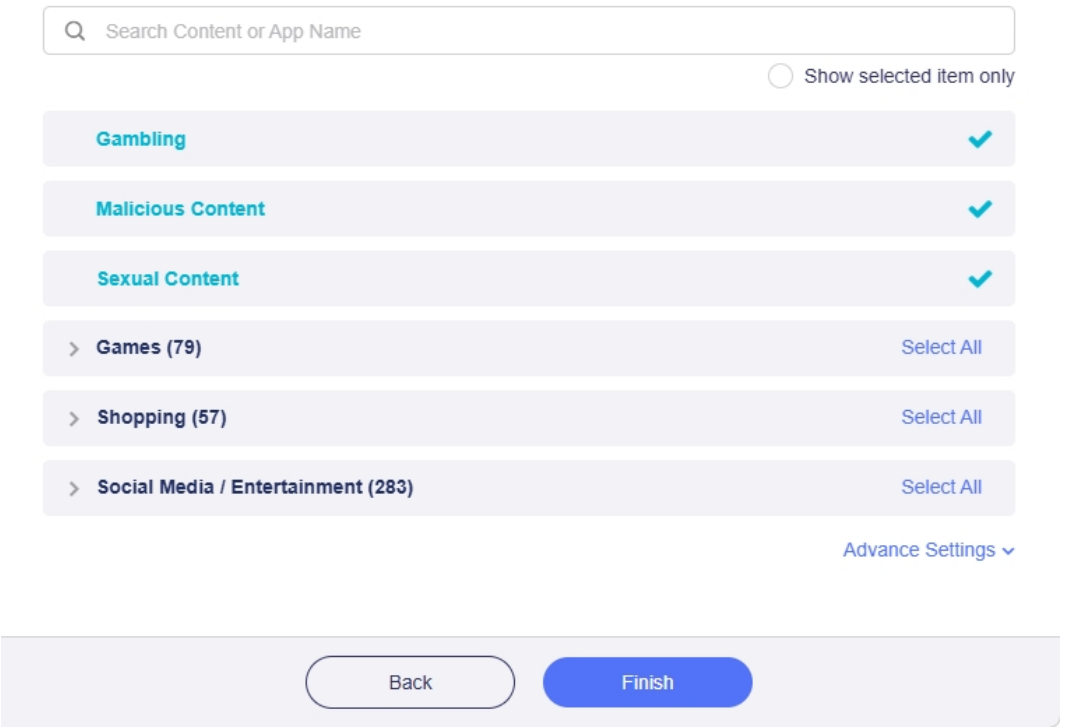
6. Ustaw porę snu dla urządzenia dziecka i kliknij Next. W tym czasie wybrane urządzenia nie będą miały dostępu do Internetu. Domyślnie pora snu jest taka sama każdego dnia.



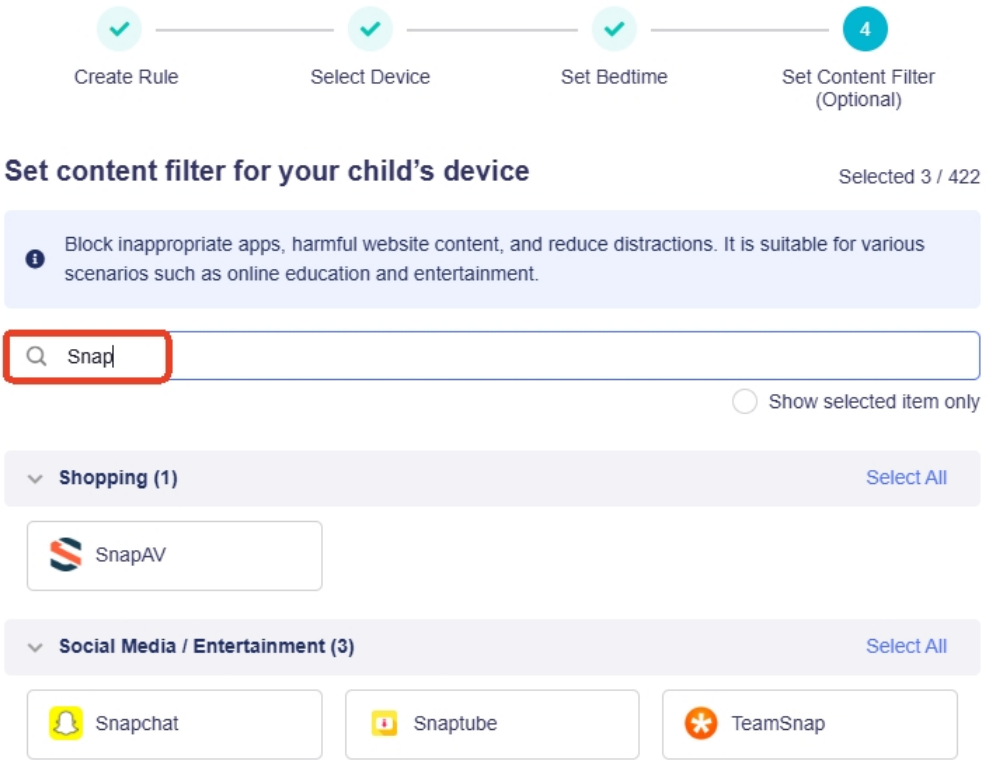
Aby ustawić różne pory snu w poszczególne dni tygodnia, wybierz **Customize Days,** ustaw odpowiednie godziny i kliknij **Next**.

7. Wybierz filtr treści.
   Domyślnie wybrano trzy kategorie: Gambling (hazard), **Malicious Content (szkodliwe** treści) i **Sexual Content (**treści seksualne). W razie potrzeby możesz wybrać inne kategorie, np. **Games, Shopping, Social Media lub** Entertainment.

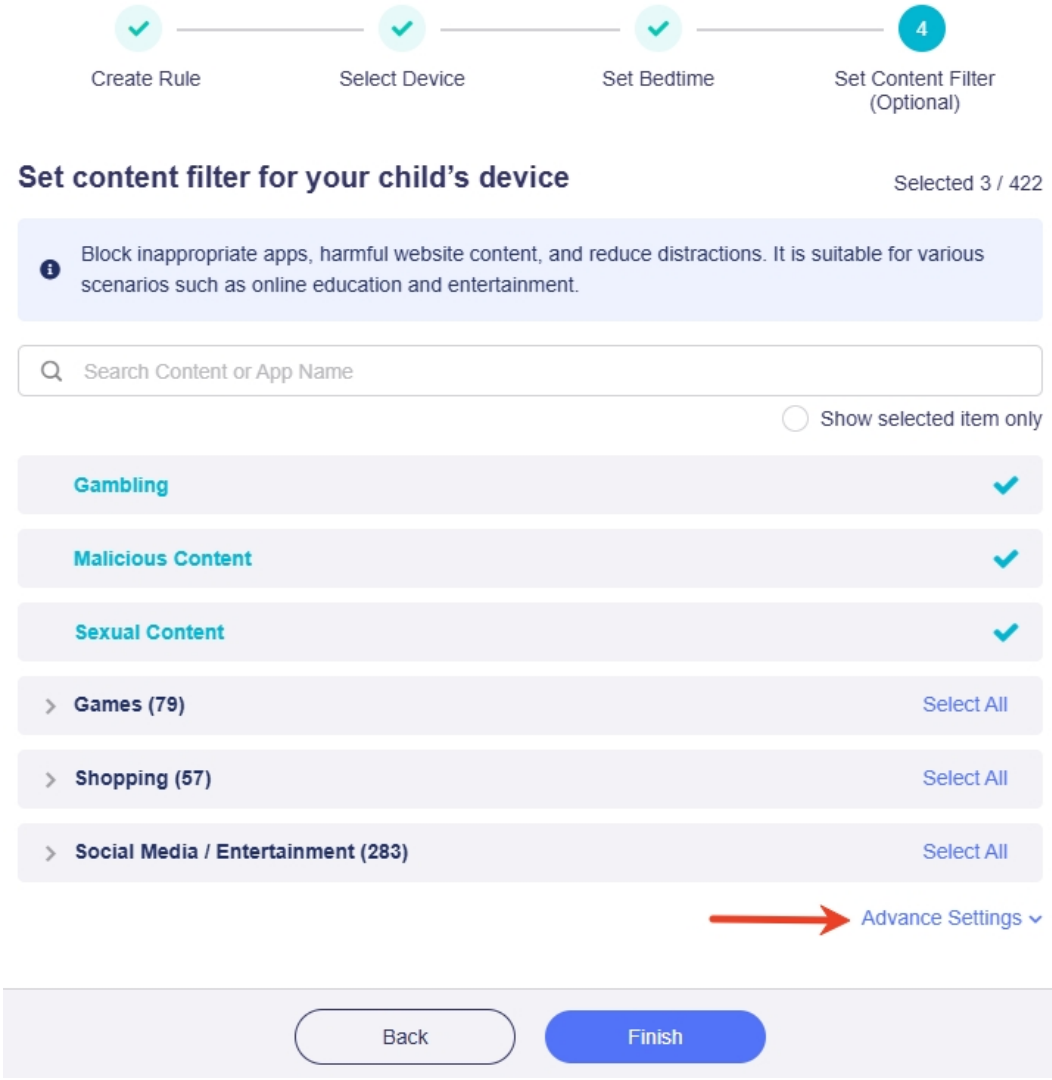




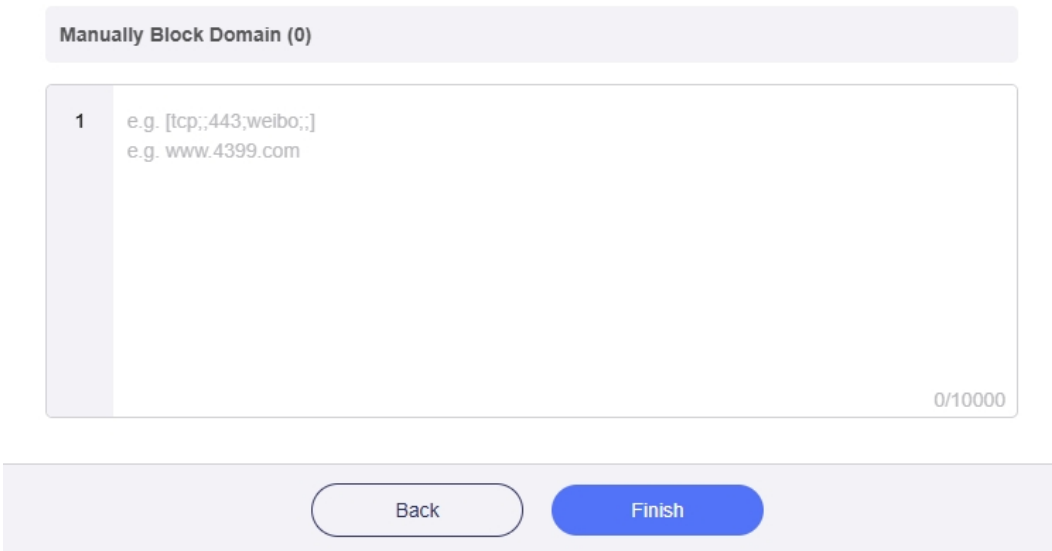
Jeśli trudno znaleźć aplikację, którą chcesz zablokować, możesz wyszukać ją u góry strony.



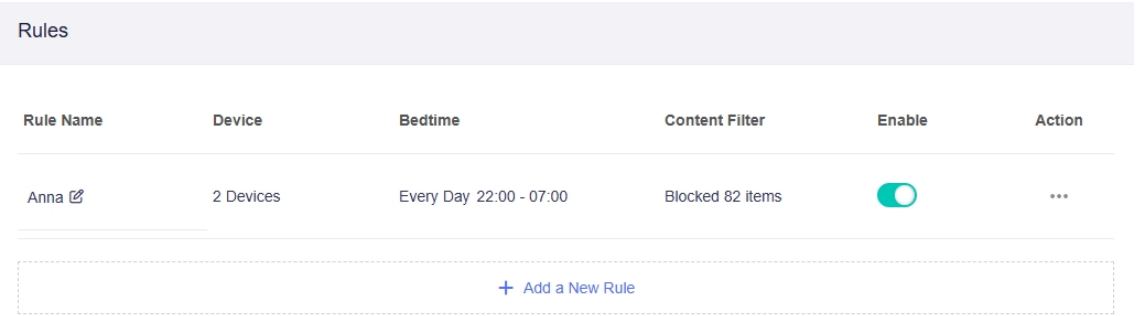
8. Aby zablokować określone domeny, kliknij **Advanced Settings w** prawym dolnym rogu.



Wprowadź domeny ręcznie i kliknij **Finish**.



9. Reguła została dodana. Lista wyświetla nazwę reguły, liczbę podłączonych urządzeń, harmonogram pory snu, filtrowane treści i stan reguły (włączona/wyłączona).



Rozdział 14

Bezpieczeństwo

W tym rozdziale opisano zarządzanie bezpieczeństwem sieci, w tym przekierowanie portów, ustawienia dostępu administratora i tryb NAT.

14.1 Przekierowanie portów

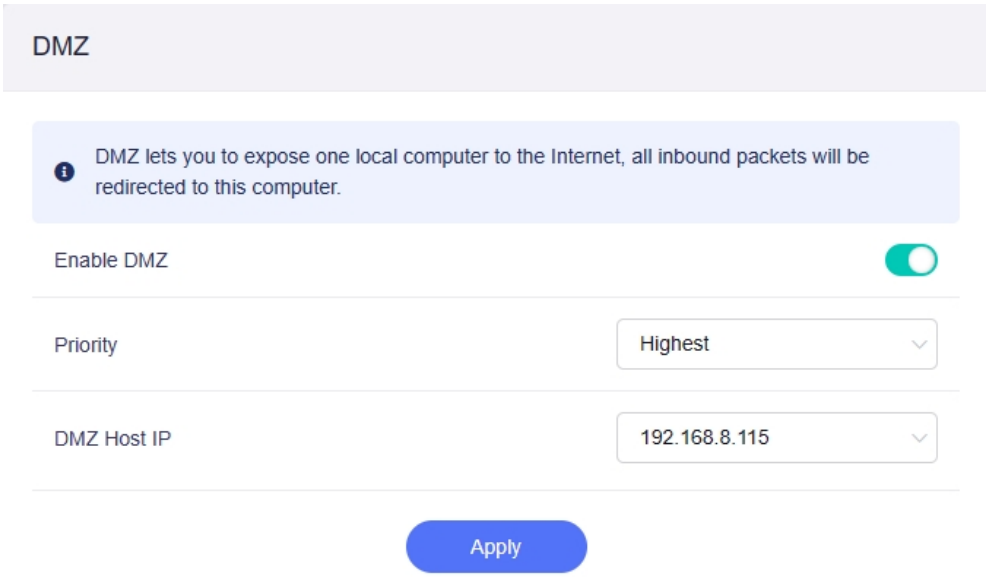
Przekierowanie portów to funkcja sieciowa kierująca żądania zewnętrzne do określonych urządzeń w sieci lokalnej. Strona Port Forwarding zawiera dwie główne funkcje: **DMZ** (bezpośredni pełny dostęp do jednego urządzenia) i **Port Forwarding** (dostęp do określonych portów urządzeń).

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 **SECURITY** > **Port Forwarding** > **DMZ**.
2. Włącz **Enable DMZ**. Wybierz Priority i DMZ Host IP z list, a następnie kliknij **Apply**.



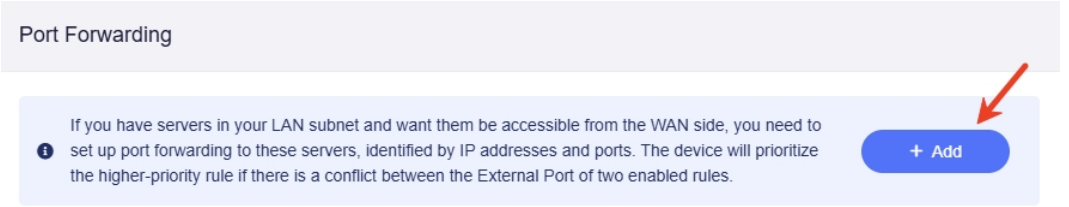
- **Priority**: ustaw Highest lub Lowest. Jeśli DMZ ma wyższy priorytet niż reguły przekierowania portów, wszystkie te reguły przestają obowiązywać. W przeciwnym razie żądania są przekazywane do urządzenia klienckiego DMZ tylko wtedy, gdy dla danego portu nie ma reguły przekierowania.
- **DMZ Host IP**: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

14.1.2 Przekierowanie portów

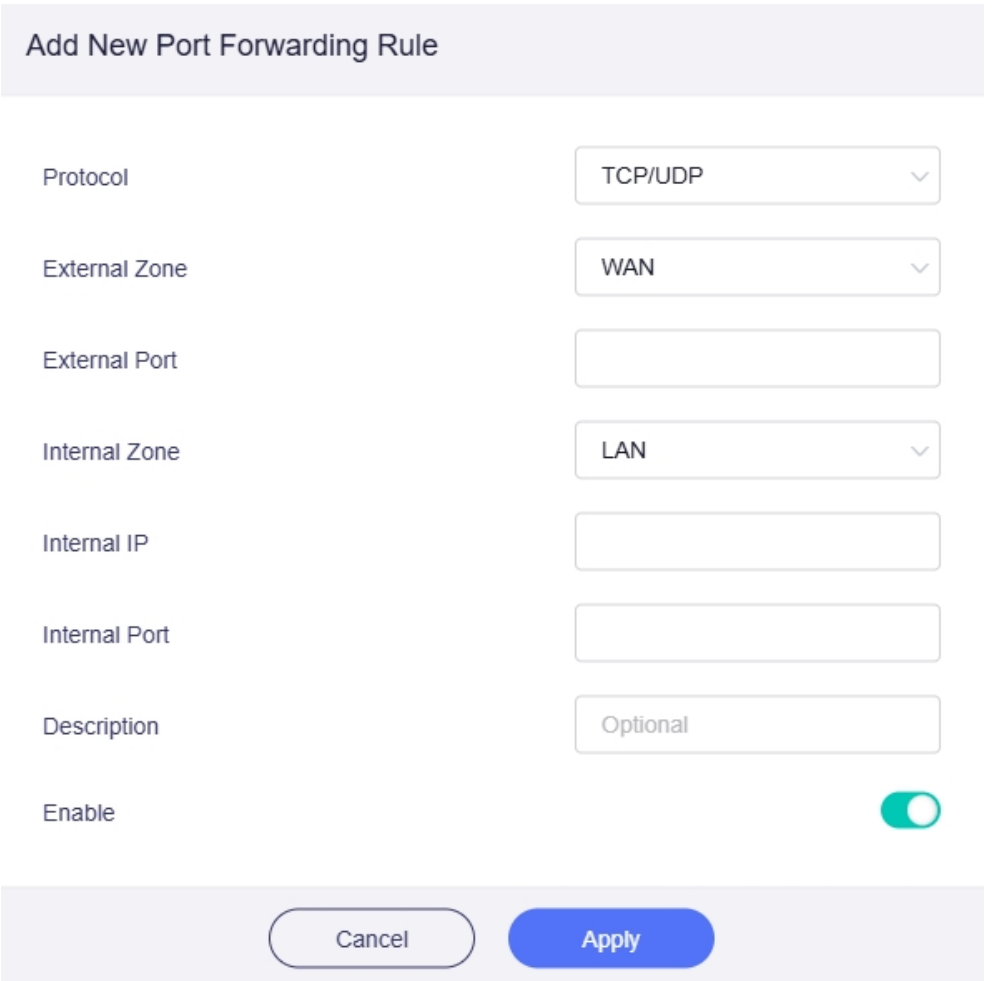
Przekierowanie portów umożliwia komputerom zdalnym łączenie się z komputerem lokalnym lub serwerem za zaporą LAN (np. serwerem WWW lub FTP).

Aby skonfigurować przekierowanie portów, w razie potrzeby wykonaj poniższe czynności.

1. Zaloguj się do panelu administracyjnego routera, przejdź do sekcji **SECURITY** > **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**.



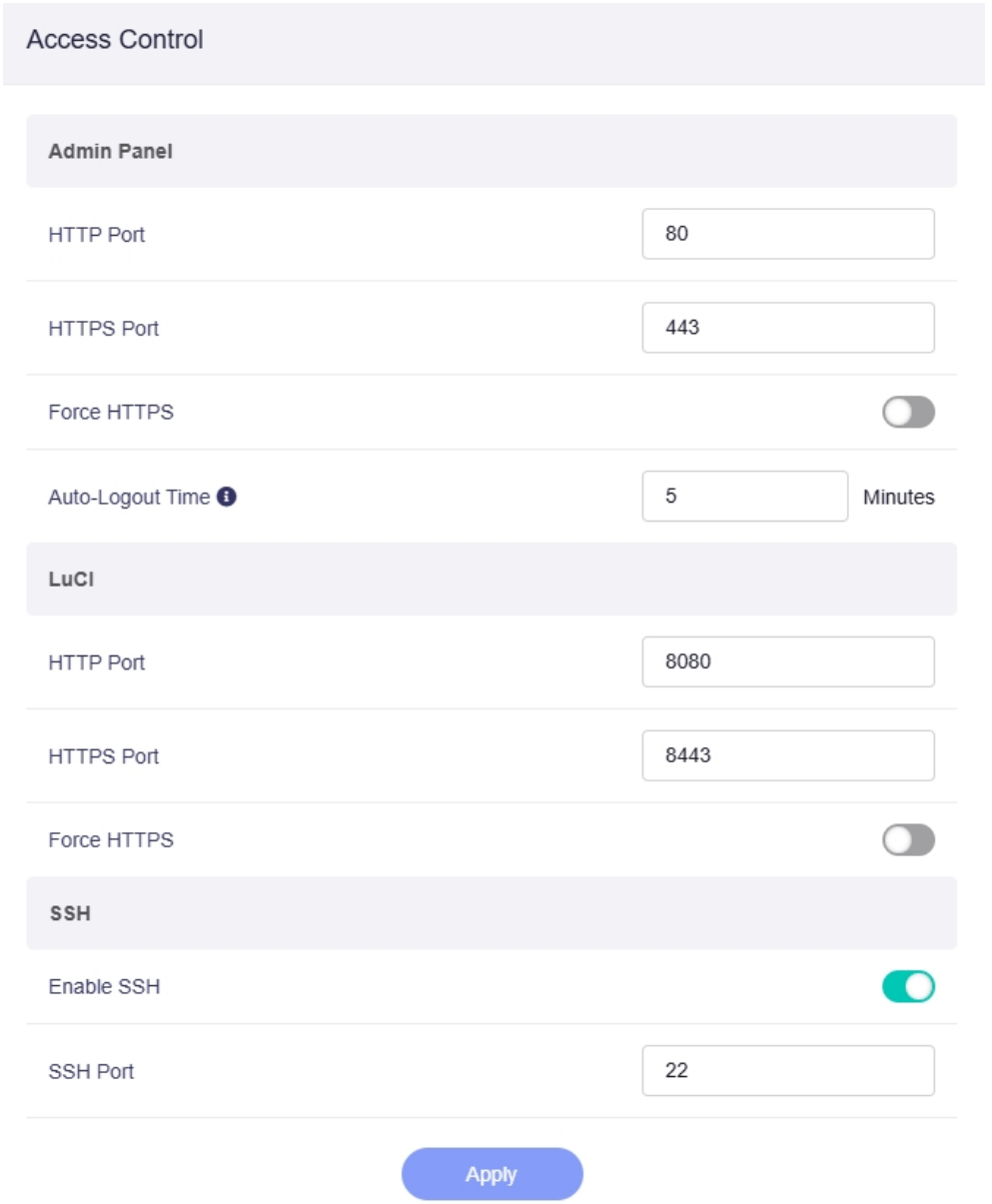
- **Protocol**: używany protokół. Możesz wybrać TCP, UDP lub oba protokoły.
- **External Zone**: dostępne opcje to WAN, WireGuard Client, WireGuard Server, OpenVPN Client, OpenVPN Server i LAN.
- **External Port**: numer lub numery portów zewnętrznych. Wprowadź określony numer portu z zakresu 1–65535. Możesz ustawić pojedynczy port lub zakres, łącząc pierwszy i ostatni numer łącznikiem (np. 501-510).
- **Internal Zone**: dostępne opcje to LAN, 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 Dostęp administratora

Zaloguj się do panelu administracyjnego routera i przejdź do **SECURITY** > **Admin Access**. Na tej stronie możesz skonfigurować lokalny dostęp do routera i zdalny dostęp przez HTTPS/SSH oraz zarządzać otwartymi portami routera, aby chronić router i sieć przed nieuprawnionym dostępem.

14.2.1 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

Przed skonfigurowaniem kontroli dostępu do LuCI zainstaluj go w Advanced Settings.

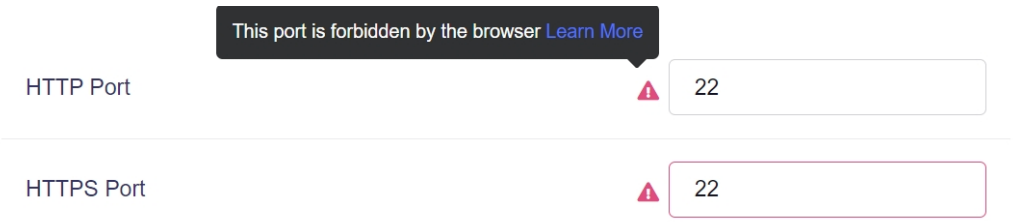
- **HTTP Port**: domyślnie 8080; służy do nieszyfrowanego dostępu HTTP do interfejsu LuCI.
- **HTTPS Port**: domyślnie 8443; służy do bezpiecznego dostępu HTTPS do interfejsu LuCI.
- **Force HTTPS**: po włączeniu wymusza bezpieczne połączenie HTTPS z interfejsem LuCI.

SSH

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

Uwaga:

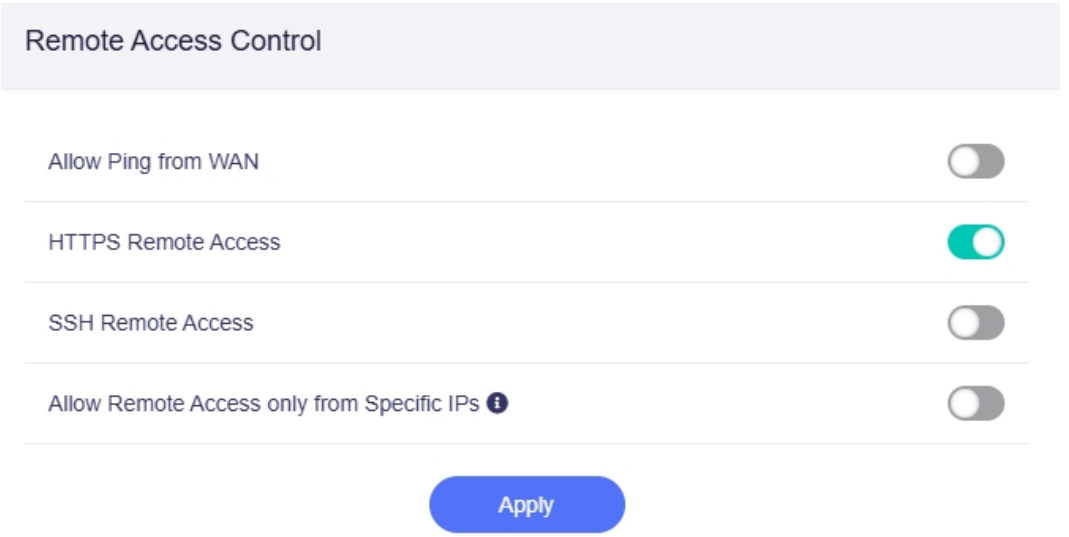
1. Jeśli przypiszesz numer kolidujący z portem zastrzeżonym (lub zarezerwowanym dla określonych usług przez przeglądarki albo konwencje sieciowe), pojawi się komunikat „This port is forbidden by the browser”.



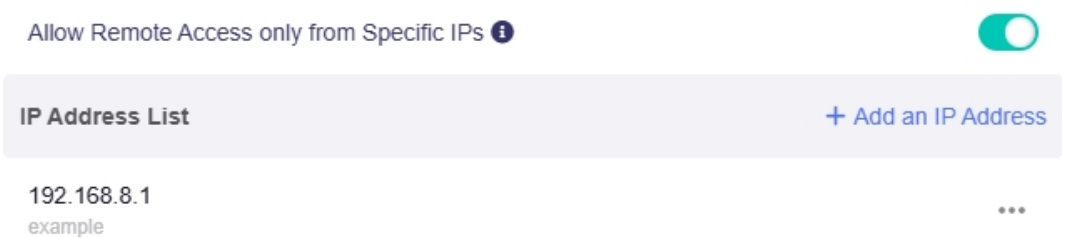
2. Po zmianie numeru portu w oprogramowaniu trzeba podawać prawidłowy numer, aby otworzyć panel administracyjny. Jeśli zapomnisz numeru, zresetuj router, aby przywrócić port domyślny.

14.2.2 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.

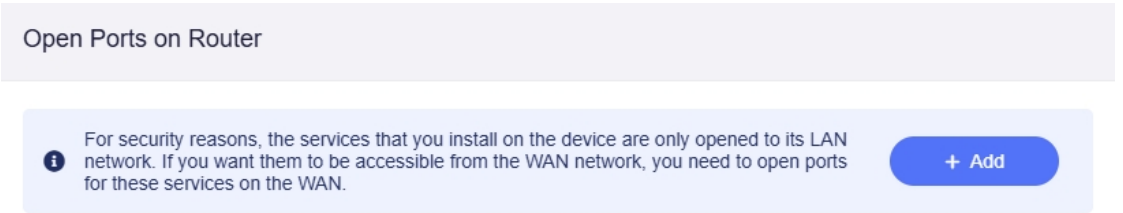


- **Allow Ping from WAN**: zezwolenie na ping od strony WAN pomaga sprawdzić dostępność routera przez WAN w razie problemów z siecią oraz określić opóźnienie i utratę pakietów.
- **HTTPS Remote Access**: umożliwia bezpieczny zdalny dostęp do panelu administracyjnego przez HTTPS. Zapewnia szyfrowaną transmisję 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.

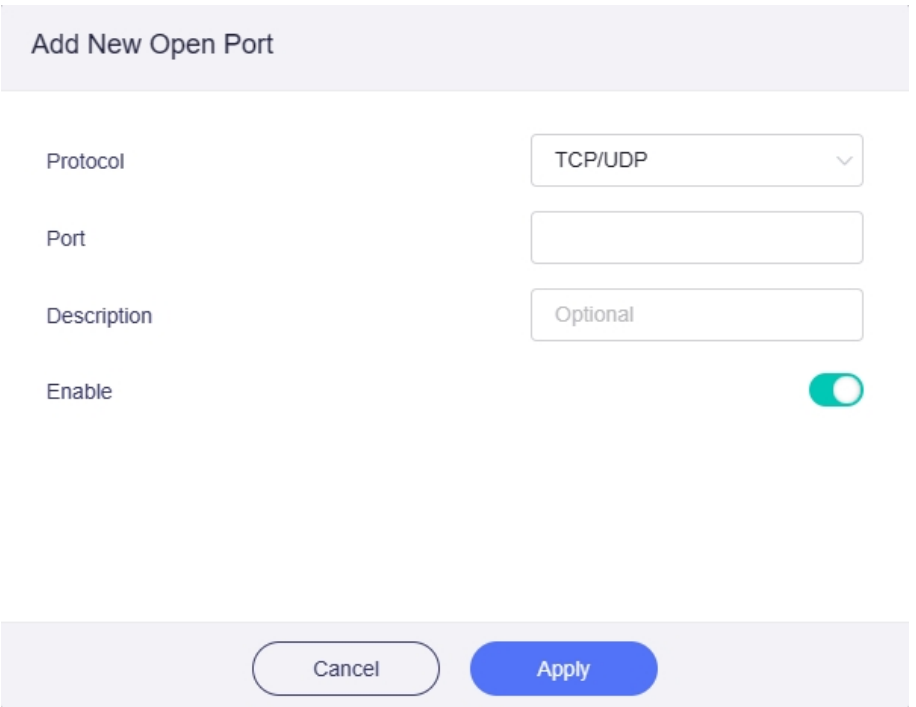


14.2.3 Otwieranie portów routera

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.



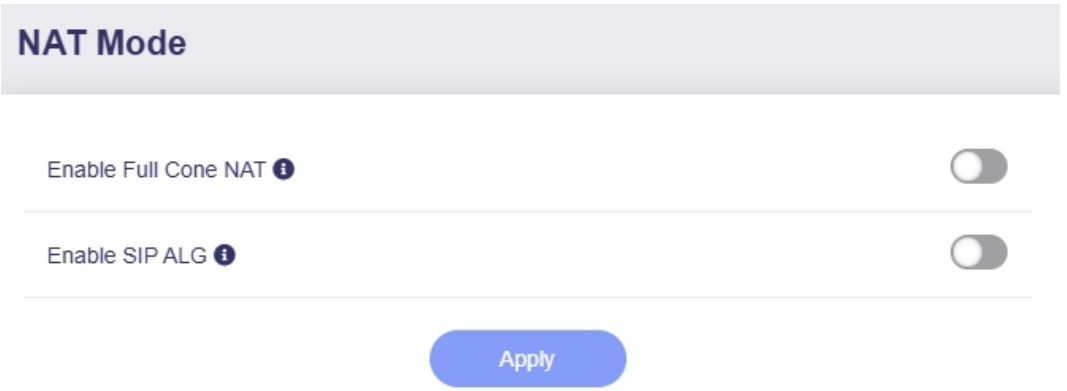
Aby otworzyć port, kliknij **Add** i wprowadź wymagane informacje w wyskakującym oknie.



- **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.

14.3 Tryb NAT

Zaloguj się do panelu administracyjnego routera i przejdź do **SECURITY** > **NAT Mode**. Ta strona umożliwia konfigurację dwóch głównych funkcji związanych z 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

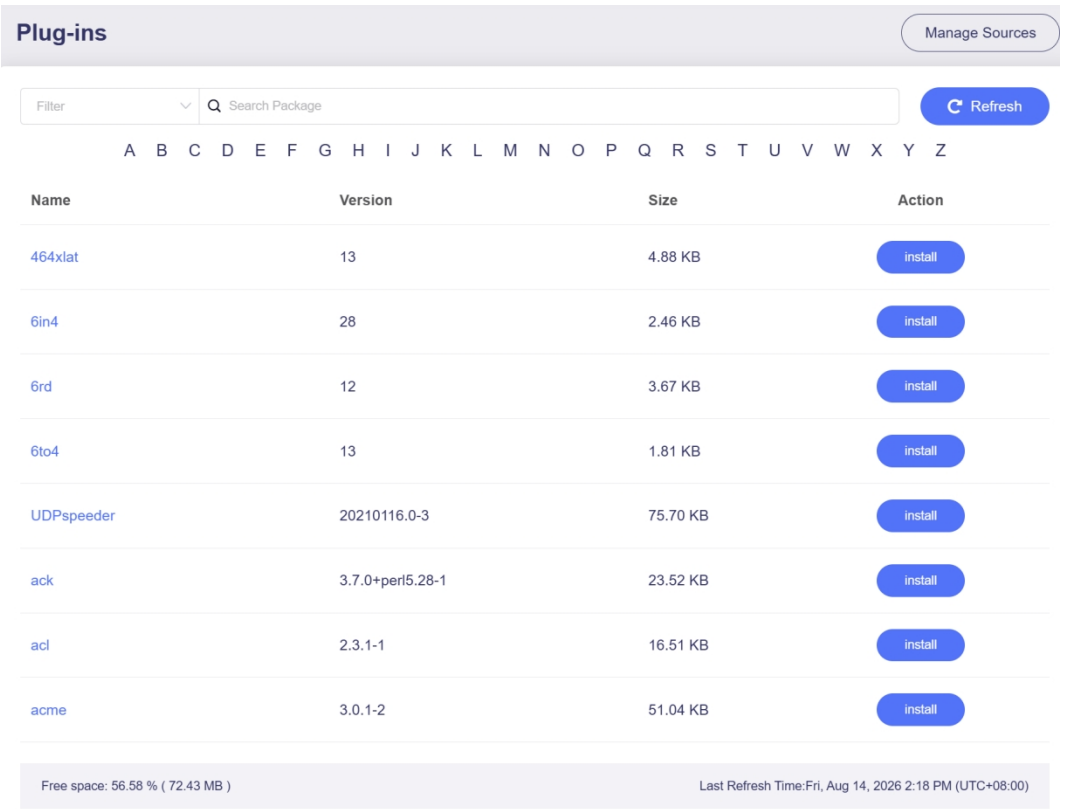
Aplikacje

W tym rozdziale opisano wybrane aplikacje routerów GL.iNet, takie jak wtyczki, dynamiczny DNS, pamięć sieciowa i Tailscale.

15.1 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:

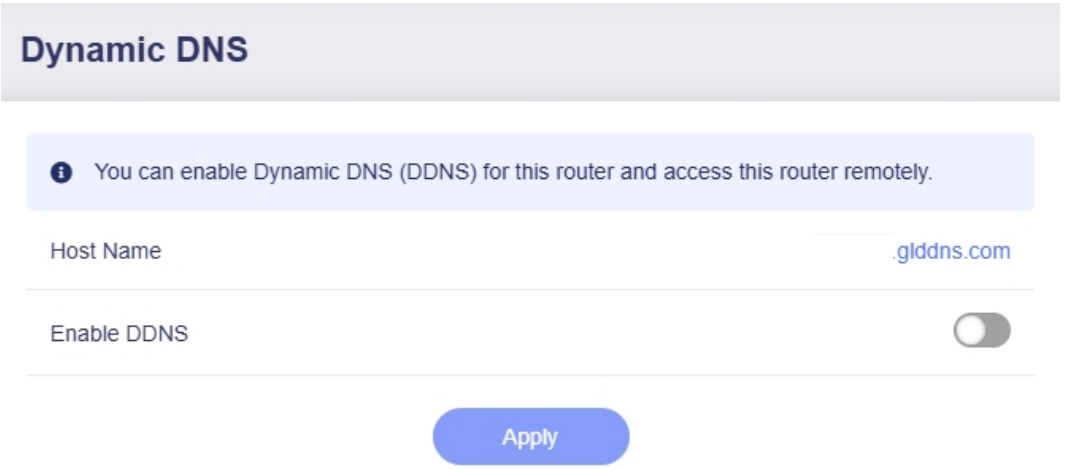
1. Nie zaleca się aktualizowania wtyczek zainstalowanych fabrycznie w oficjalnym oprogramowaniu GL.iNet, takich jak nginx, adguard home, tailscale itp.
2. Wtyczki zewnętrzne zainstalowane ręcznie przez użytkownika można aktualizować, jednak GL.iNet nie odpowiada za związane z nimi problemy z bezpieczeństwem.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

15.2 Dynamiczny DNS

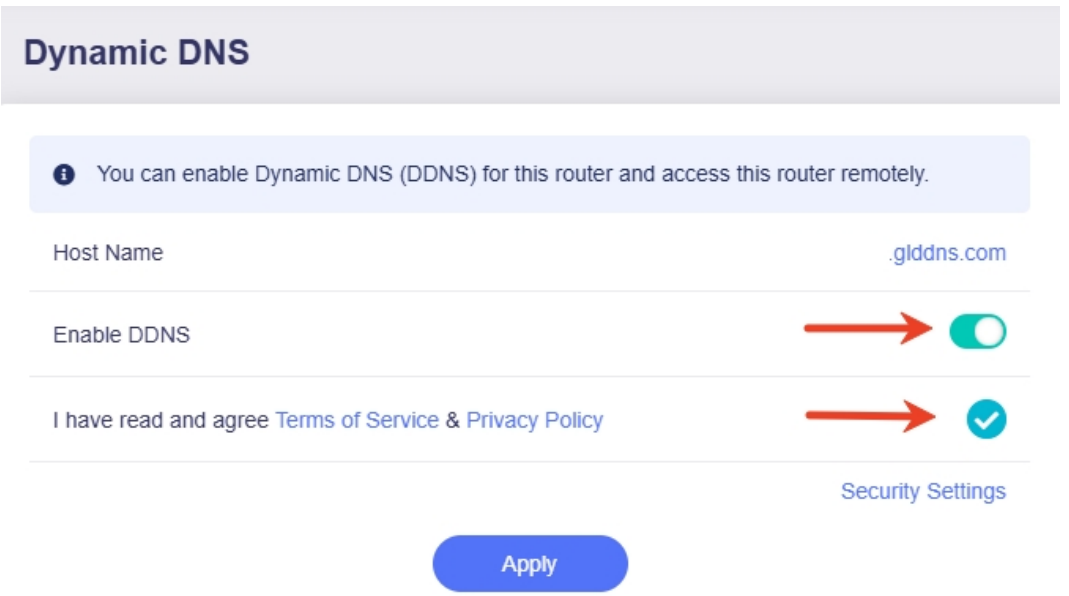
Dynamic Domain Name Service (DDNS, czyli dynamiczny DNS) to usługa mapująca nazwę domeny na dynamiczny adres IP urządzenia sieciowego. Dzięki niej można zdalnie uzyskiwać dostęp do routera. Ta funkcja wymaga publicznego adresu IP.

15.2.1 Włączanie DDNS

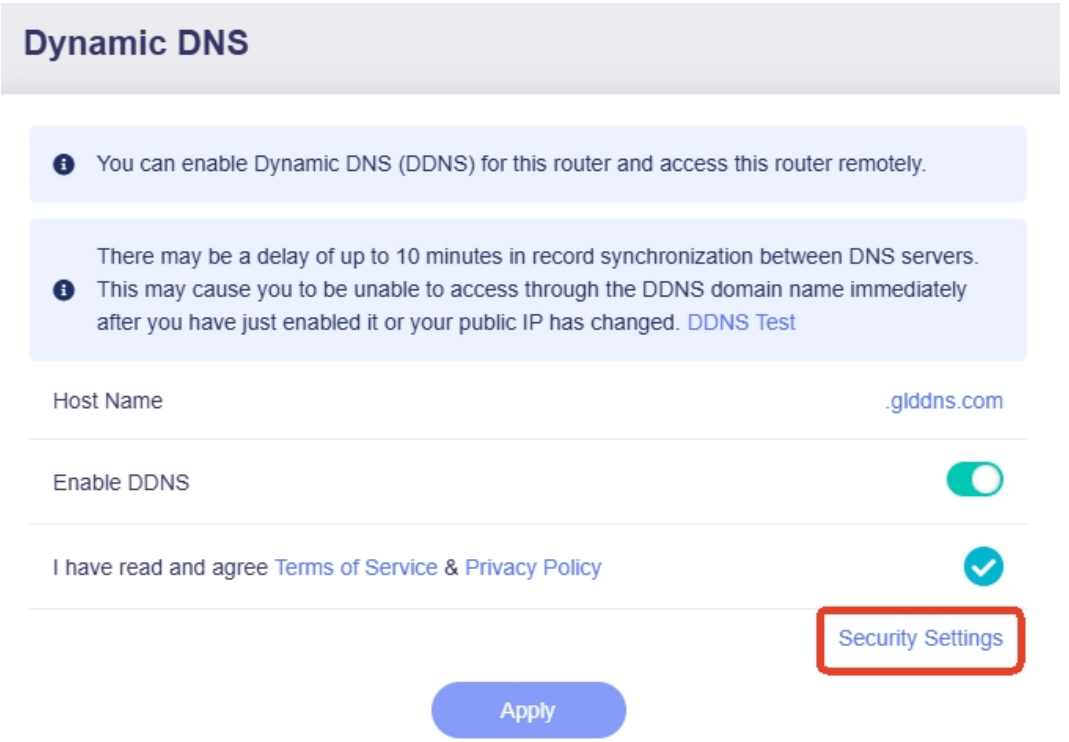
1. Zaloguj się do panelu administracyjnego routera i przejdź do **APPLICATIONS** > **Dynamic DNS**. Strona wygląda jak poniżej.



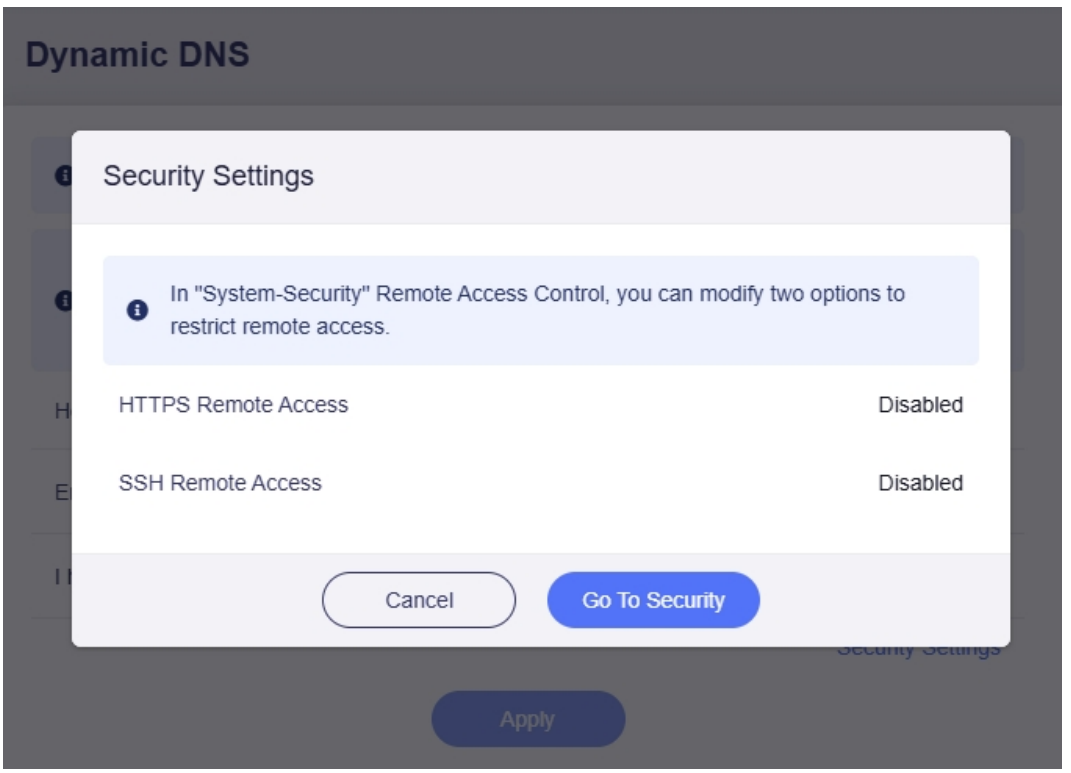
2. Włącz **Enable DDNS**, przeczytaj i zaakceptuj **Terms of Services & Privacy Policy**, a następnie kliknij **Apply**.



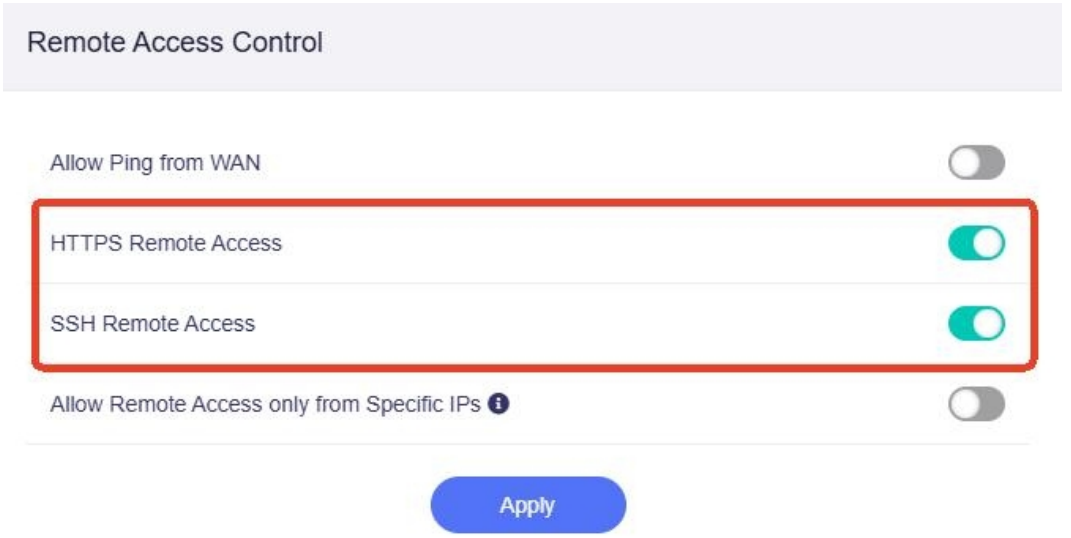
3. Kliknij **Security Settings** w prawym dolnym rogu.



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



Jeśli nie, przejdź do **SECURITY** > **Admin Access** > **Remote Access Control**, włącz tę funkcję i kliknij **Apply**.



Uwaga:

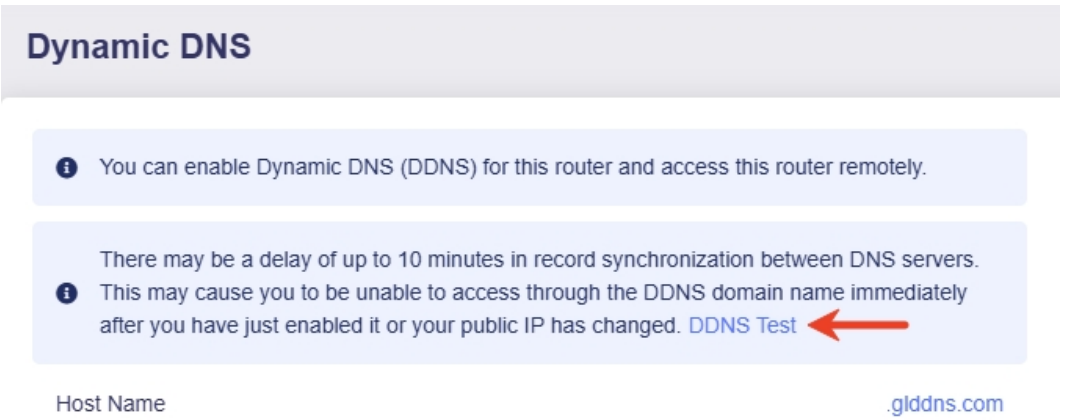
1. Synchronizacja rekordów między serwerami DNS może trwać do 10 minut. Może to uniemożliwić dostęp przez nazwę domeny DDNS bezpośrednio po włączeniu funkcji lub zmianie publicznego adresu IP.
2. Jeśli jednocześnie włączysz DDNS i klienta VPN, upewnij się, że opcja Services From GL.iNet Use VPN jest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

15.2.2 Sprawdzanie działania DDNS

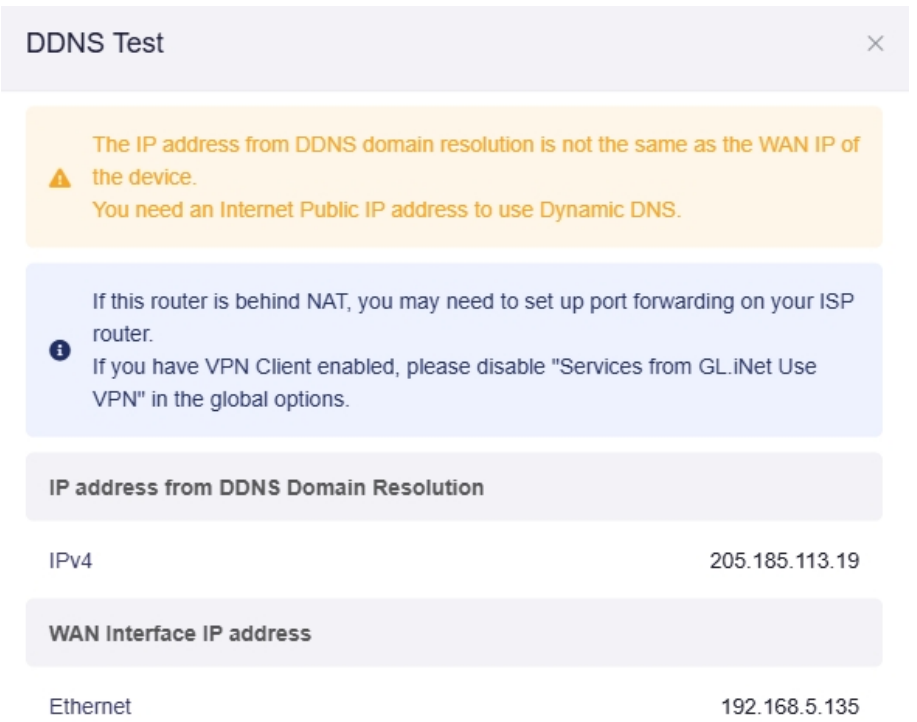
Działanie DDNS można sprawdzić za pomocą narzędzia testowego DDNS lub ręcznie, przy użyciu poleceń.

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.



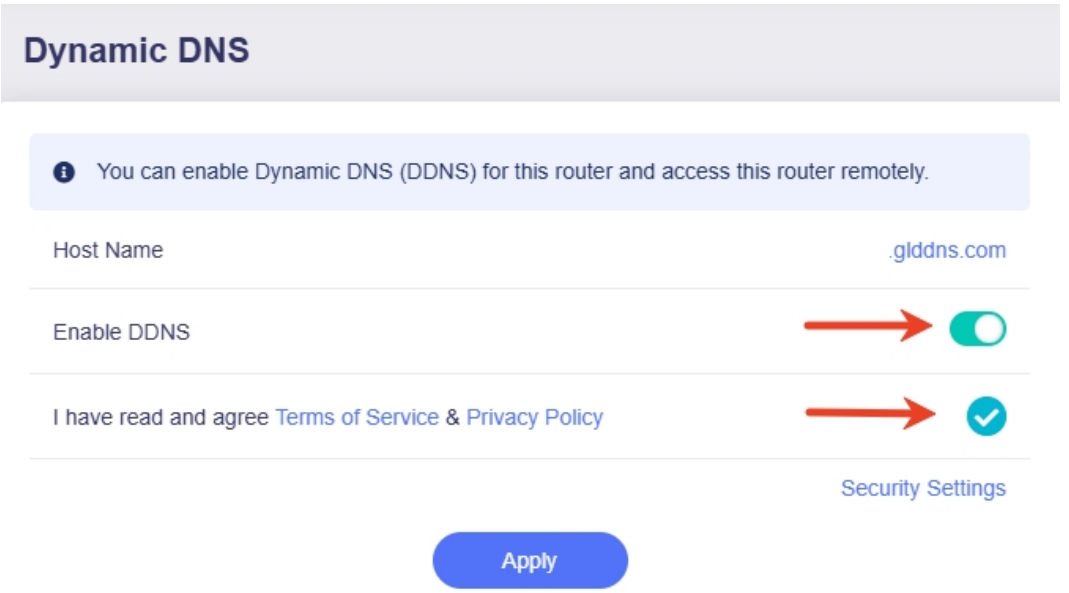
   - Zastąp „xxxxxxx.glddns.com” na powyższej ilustracji własną nazwą hosta.
   - „8.8.8.8” to serwer DNS Google. Użyj go lub zastąp innym adresem, a następnie naciśnij Enter.
2. Jeśli otrzymasz publiczny adres IP, taki jak „183.178.10.100” na powyższej ilustracji, domena DDNS została prawidłowo powiązana 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.

15.2.3 Zdalny dostęp przez HTTPS

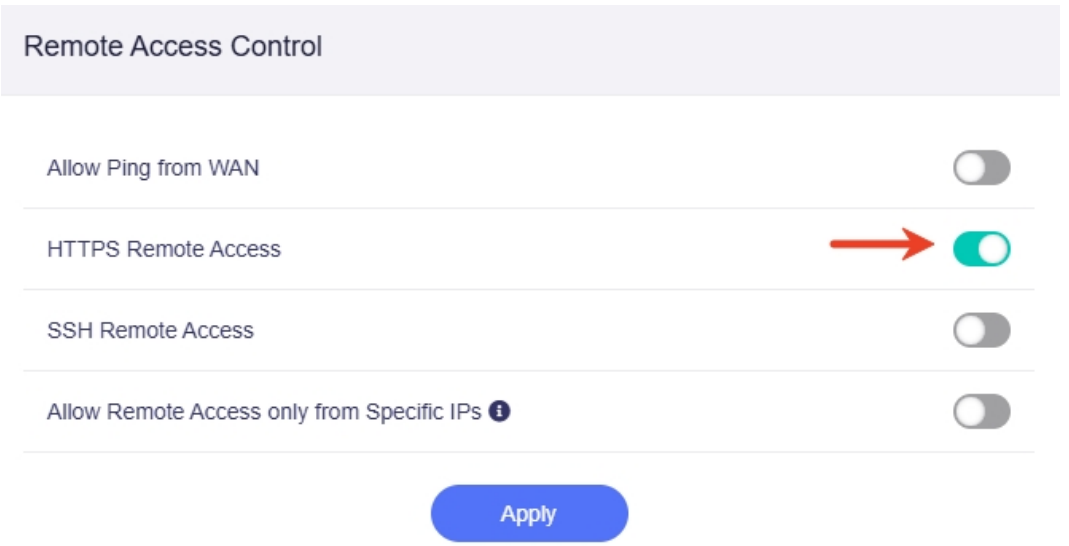
Do zdalnego dostępu przez HTTPS wymagany jest **publiczny adres IP**. Kliknij tutaj, aby sprawdzić, czy dostawca Internetu przydziela taki adres. Jeśli router znajduje się za NAT, skonfiguruj przekierowanie portów (**port 443**) na routerze nadrzędnym dla dostępu HTTPS.

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**.

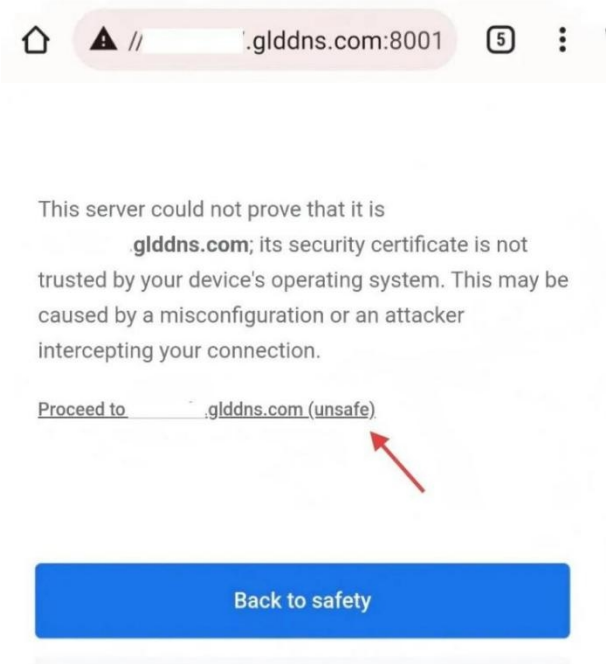


2. W panelu administracyjnym przejdź do **SECURITY** > **Admin Access** > **Remote Access Control**. Włącz **HTTPS Remote Access** i kliknij **Apply**.



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** .



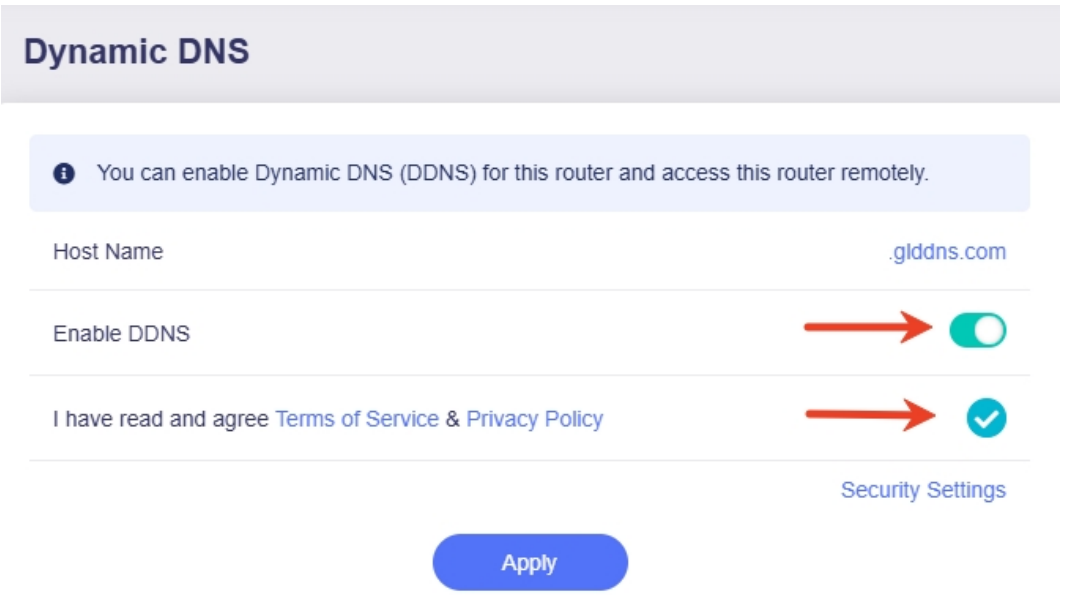
Możesz teraz uzyskiwać dostęp do panelu administracyjnego routera za pomocą nazwy hosta DDNS przez **HTTPS**.

15.2.4 Zdalny dostęp przez SSH

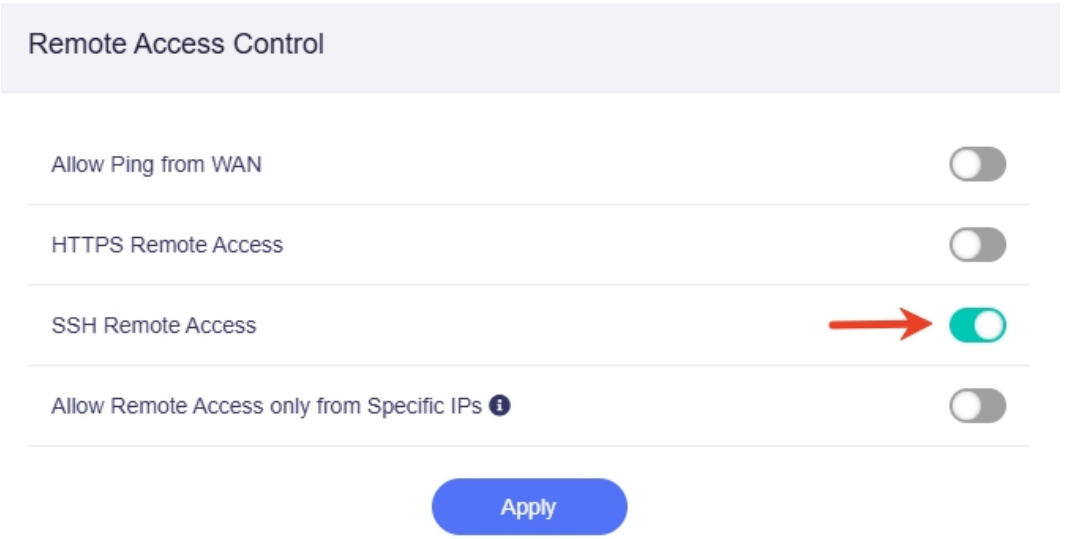
Do zdalnego dostępu przez SSH wymagany jest **publiczny adres IP**. Kliknij tutaj, aby sprawdzić, czy dostawca Internetu przydziela taki adres. Jeśli router znajduje się za NAT, skonfiguruj przekierowanie portów (**port 22**) na routerze nadrzędnym dla zdalnego dostępu SSH.

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 **SECURITY** > **Admin Access** > **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).

15.3 Pamięć sieciowa

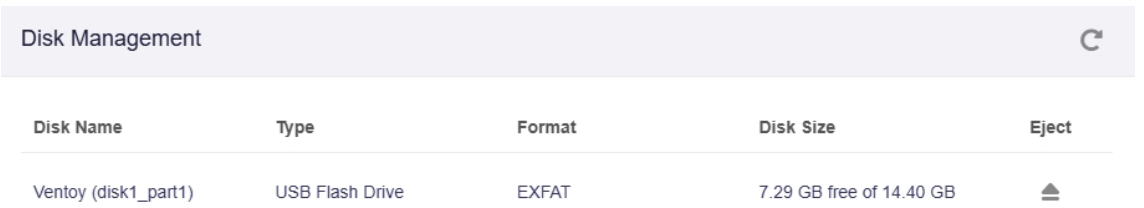
Pamięć sieciowa umożliwia bezprzewodowe udostępnianie plików między urządzeniami po podłączeniu nośnika USB lub karty SD do routera. Router przekształca nośnik w udostępniony dysk sieciowy, dostępny dla wszystkich urządzeń połączonych przez Wi-Fi.

Mango 2 ma port USB zgodny z pamięciami flash USB i przenośnymi zewnętrznymi dyskami twardymi. Dla tych nośników możesz skonfigurować Sambę z obsługą popularnych formatów, takich jak NTFS, FAT32 i EXT4.

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

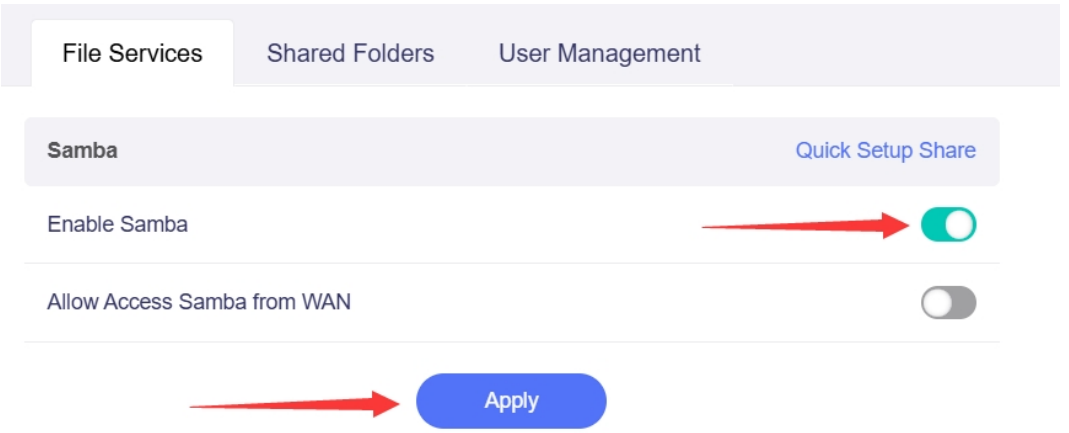
15.3.1 Podłączanie pamięci

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.



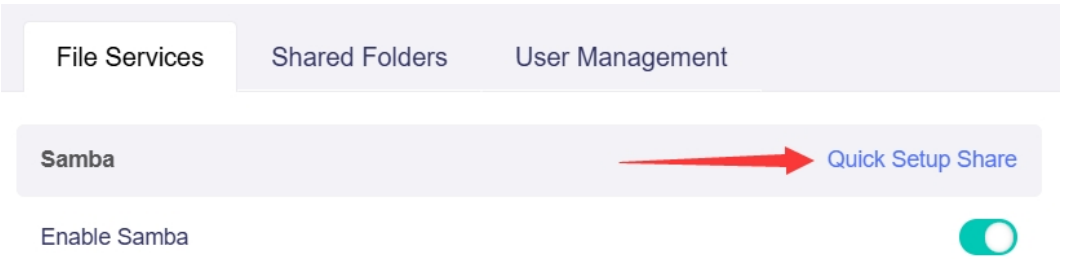
15.3.2 Konfiguracja usługi Samba

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

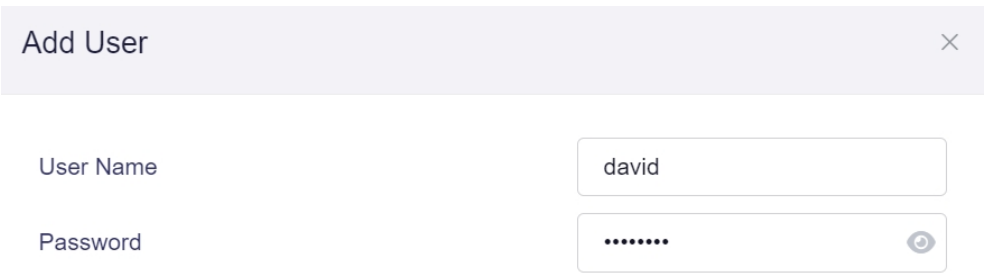


   - **Allow Access Samba from WAN**: włącz tę opcję, jeśli urządzenia w sieci nadrzędnej mają uzyskiwać dostęp do usługi Samba.

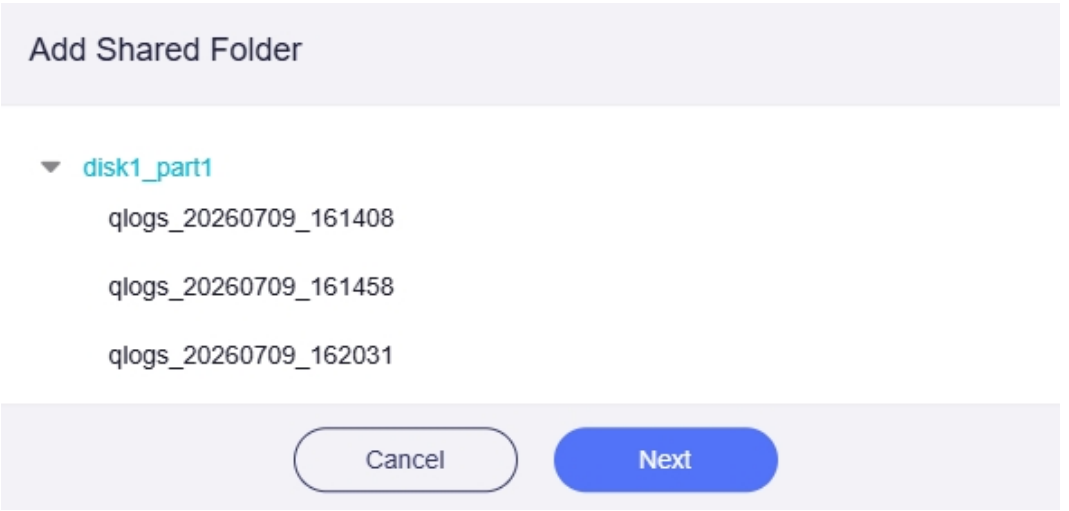
2. Kliknij **Quick Setup Share**, aby skonfigurować łącze do udostępnionego zasobu.



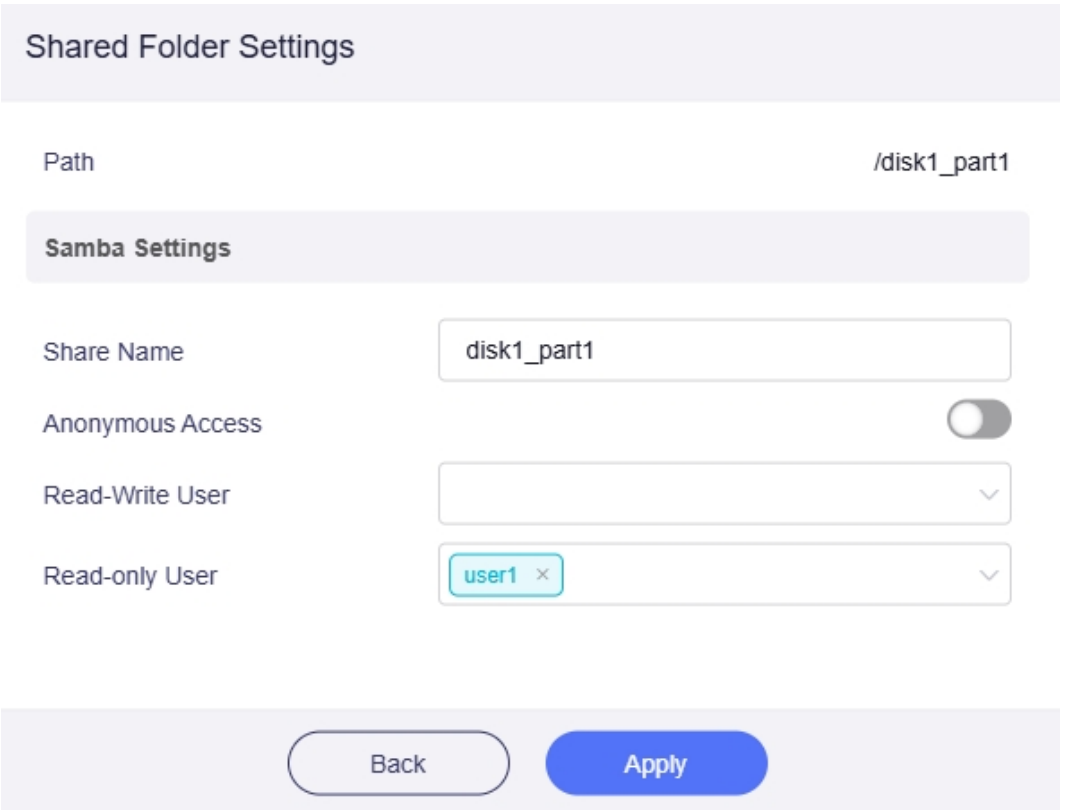
3. Dodaj użytkownika i kliknij **Next**. Jeśli konto już istnieje, ten krok zostanie pominięty.



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).



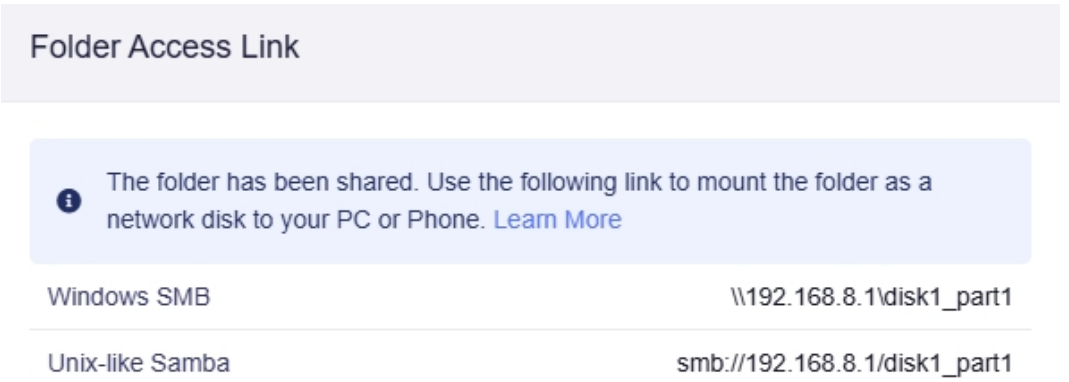
5. Skonfiguruj folder udostępniony.
   Użytkownik utworzony w poprzednim kroku jest domyślnie dodawany do **Read-Only User**. Aby mógł zapisywać lub usuwać pliki, usuń go z Read-Only User i dodaj do **Read-Write User**, a następnie kliknij **Apply**.



   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.

15.4 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 opiera się na WireGuard, nie zaleca się jednoczesnego korzystania z Tailscale i następujących funkcji lub usług, gdyż może to powodować konflikty trasowania: OpenVPN Client, WireGuard Client, GoodCloud Site to Site, ZeroTier, GoodPAS.
2. Ta funkcja jest obecnie w fazie beta i może zawierać błędy.

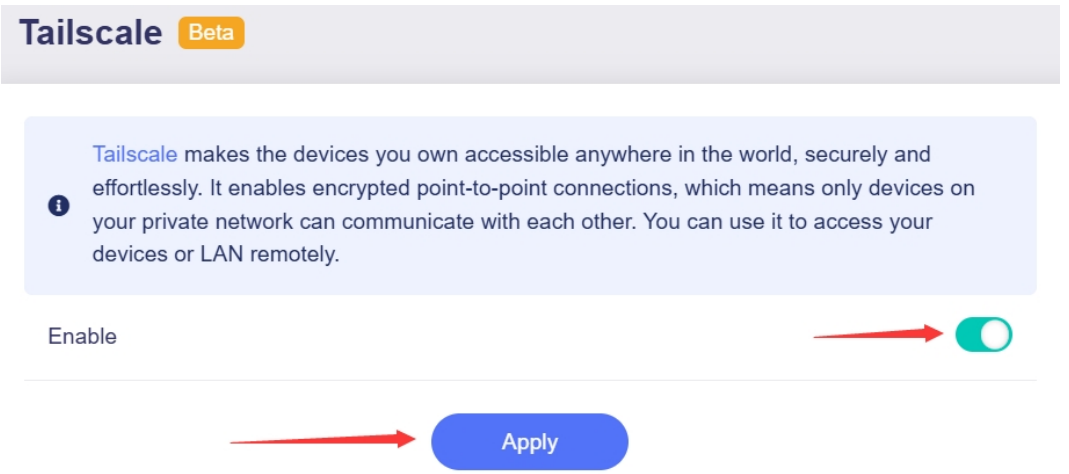
15.4.1 Konfiguracja Tailscale

Poniżej przedstawiono przykład konfiguracji sieci Tailscale za pomocą GL-MG1300.

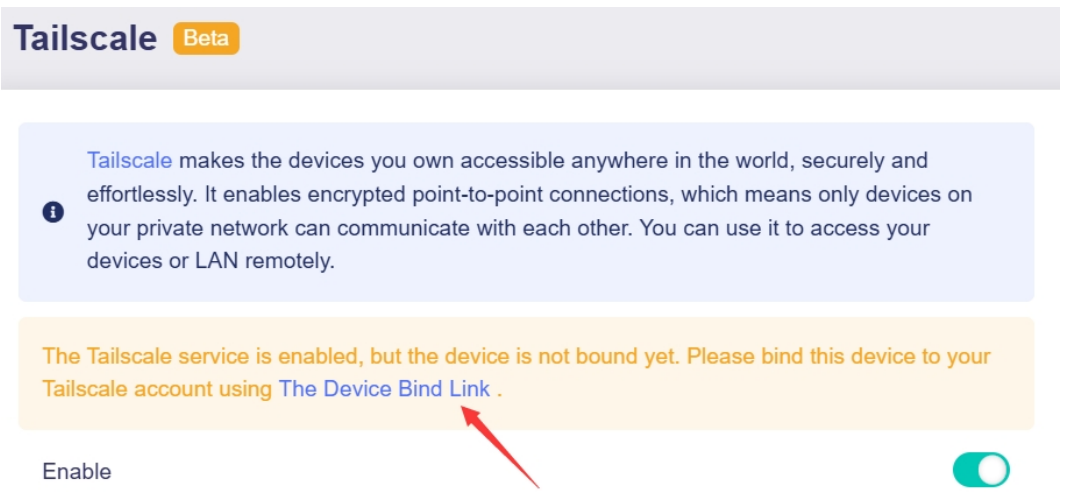
1. Najpierw zarejestruj konto Tailscale i powiąż z nim jedno lub dwa urządzenia do testów. Po powiązaniu zobaczysz je w konsoli Tailscale.



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



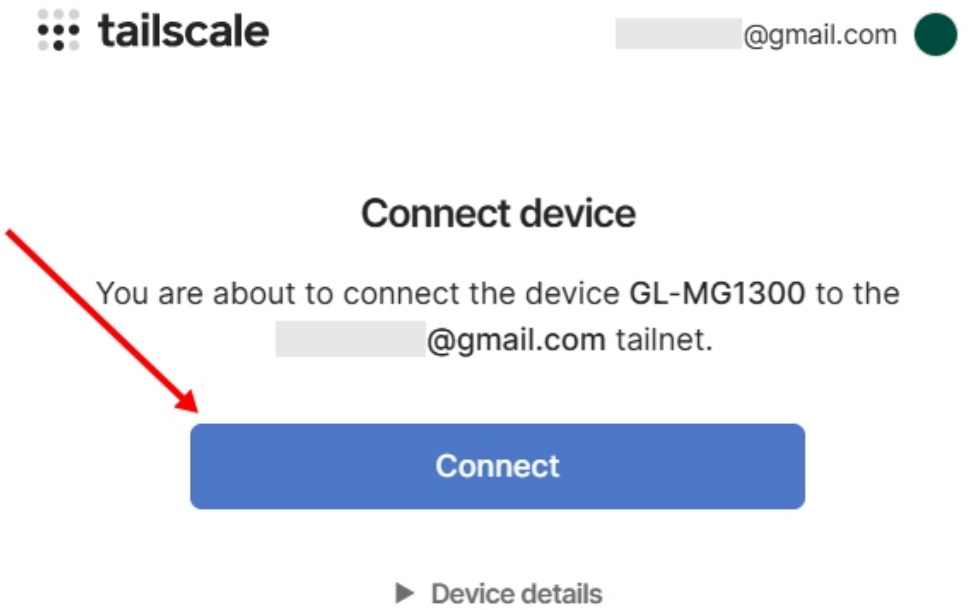
3. Strona poprosi o powiązanie urządzenia. Kliknij **Device Bind Link**.



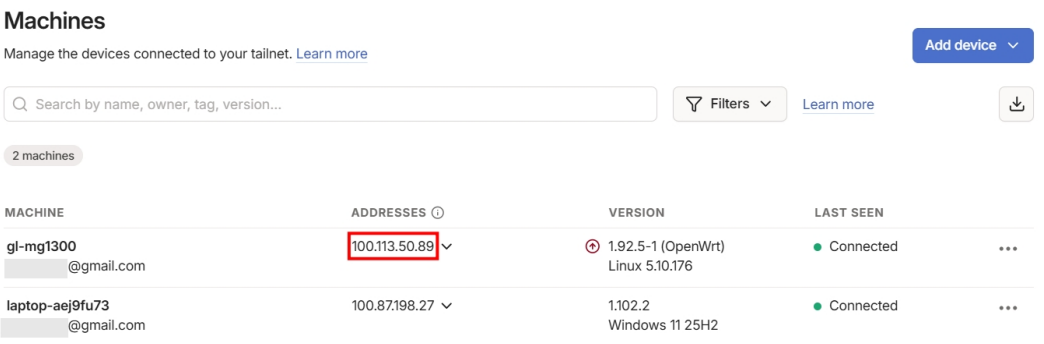
4. W wyświetlonym oknie kliknij łącze i zaloguj się na konto Tailscale.



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



6. Nastąpi przekierowanie do konsoli administracyjnej Tailscale. Router został dodany do wirtualnej sieci Tailscale i jest dostępny zdalnie pod wirtualnym adresem IP Tailscale 100.113.50.89.

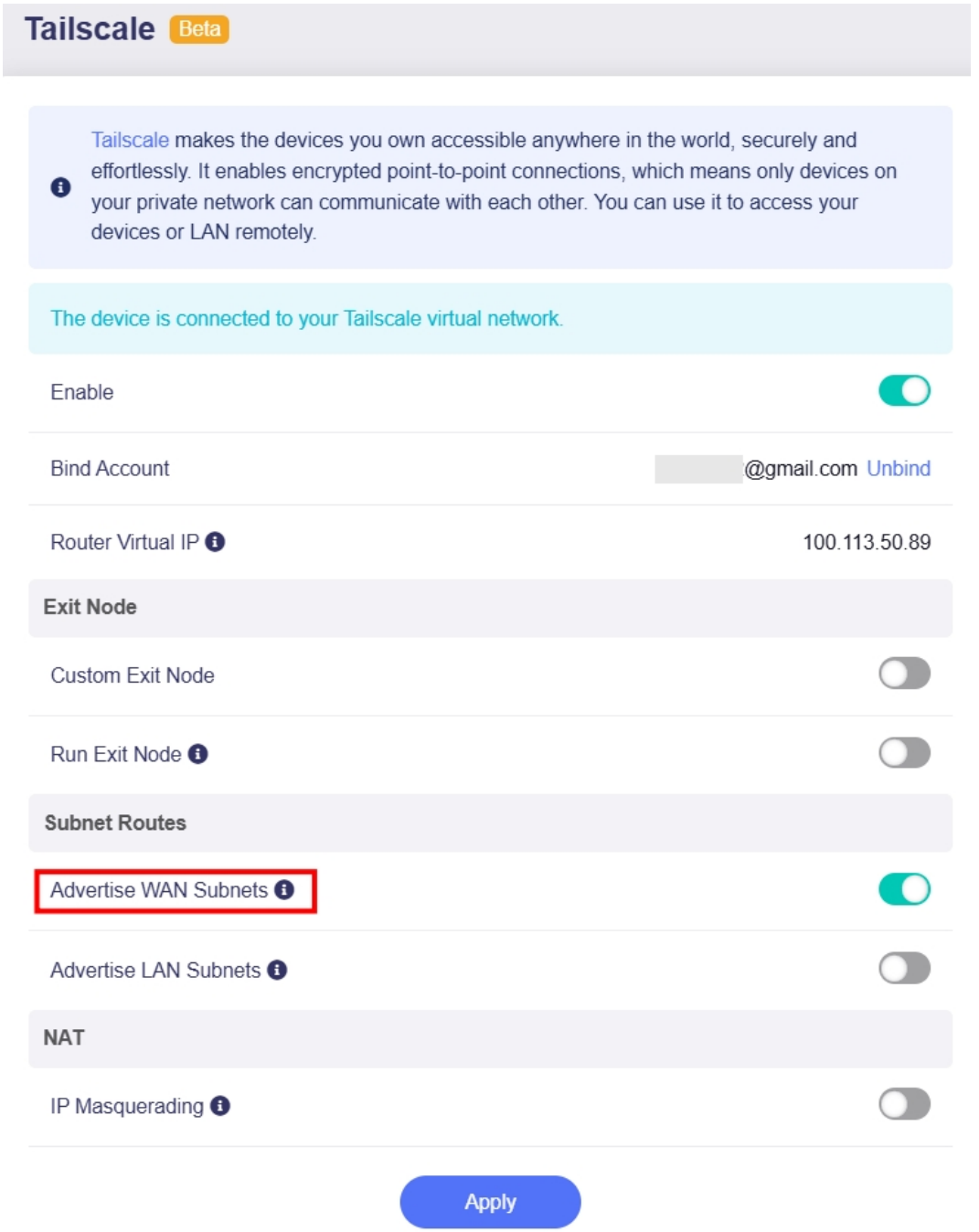


7. Sprawdź łączność.

   Na innym urządzeniu połączonym z tą samą siecią Tailscale otwórz przeglądarkę i wpisz wirtualny adres IP routera w pasku adresu. Jeśli otworzy się panel administracyjny routera, Tailscale działa poprawnie. Aby sprawdzić łączność, możesz też użyć polecenia ping lub zalogować się przez SSH do terminala routera za pomocą jego wirtualnego adresu IP.

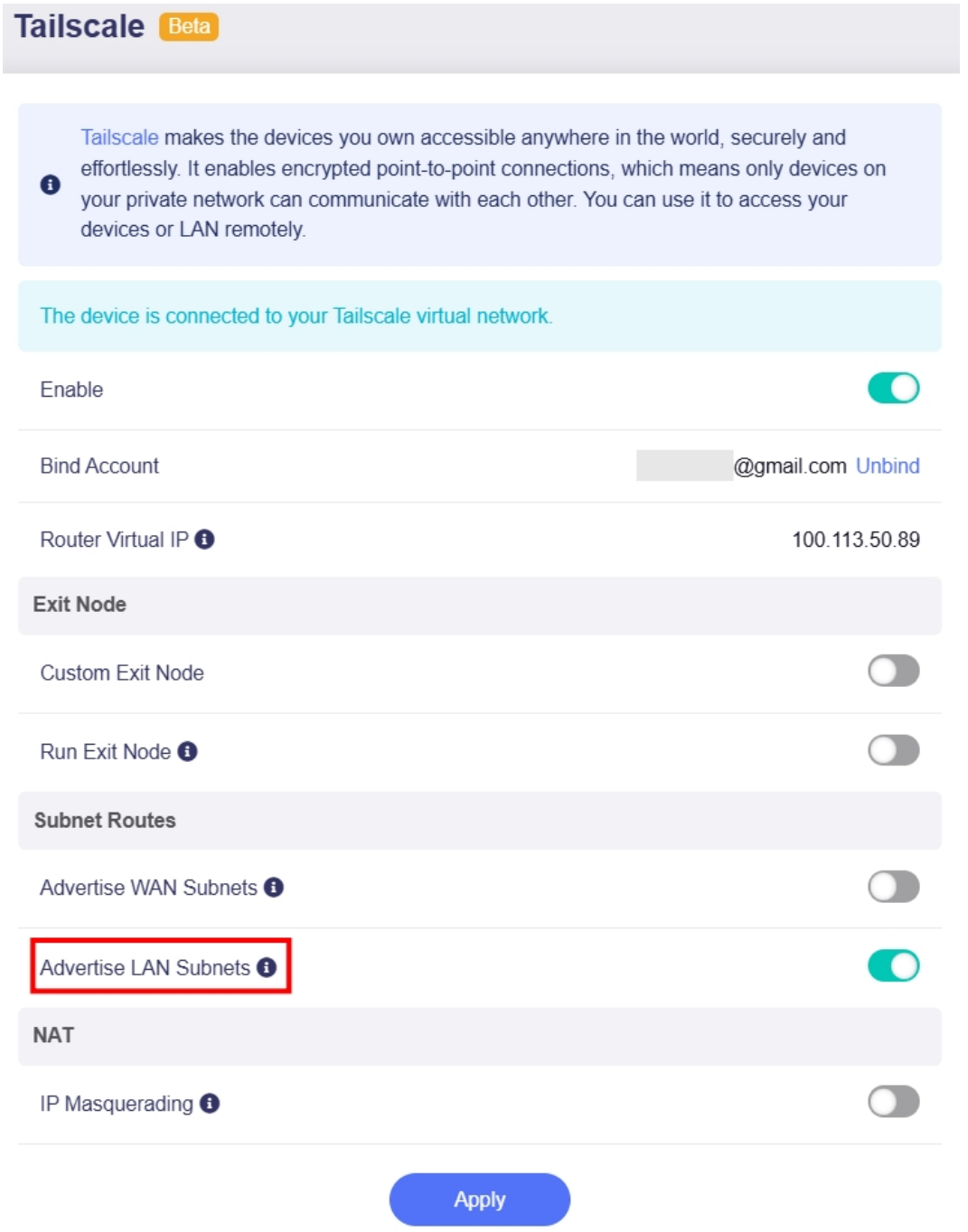
15.4.2 Rozgłaszanie podsieci WAN

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



15.4.3 Rozgłaszanie podsieci LAN

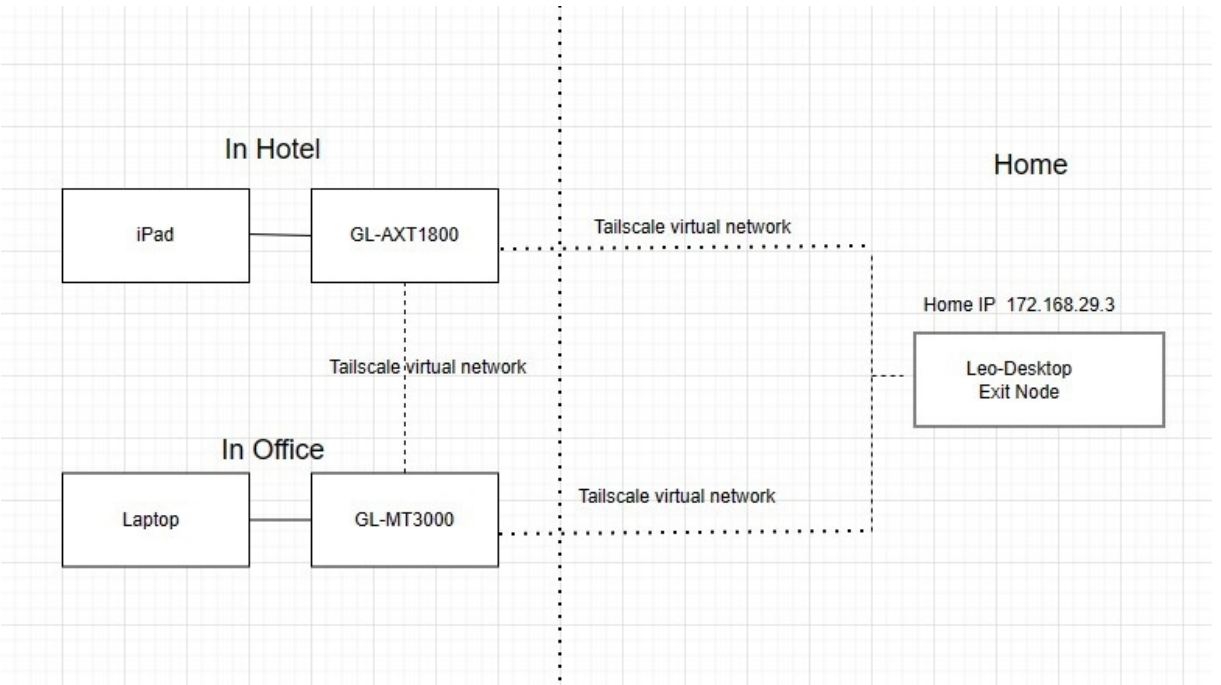
Po włączeniu tej opcji zasoby po stronie LAN urządzenia są dostępne przez wirtualną sieć Tailscale. Więcej informacji znajdziesz tutaj.



15.4.4 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.



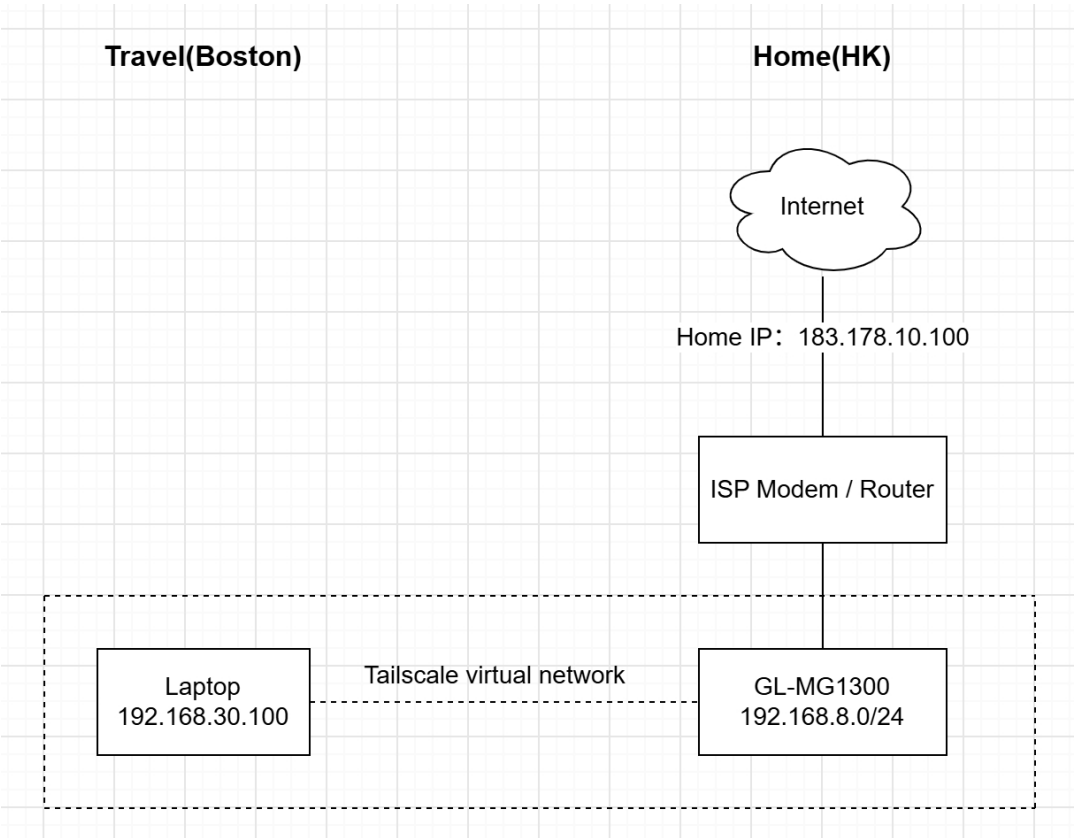
Węzeł wyjściowy kieruje wychodzący ruch internetowy urządzeń Tailnet, pełniąc w praktyce funkcję serwera VPN. Po połączeniu z takim węzłem cały ruch internetowy niezwiązany z Tailscale jest widziany jako pochodzący z jego lokalizacji. Pomaga to uzyskiwać dostęp do treści z ograniczeniami geograficznymi 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).

15.4.5 Uruchamianie węzła wyjściowego

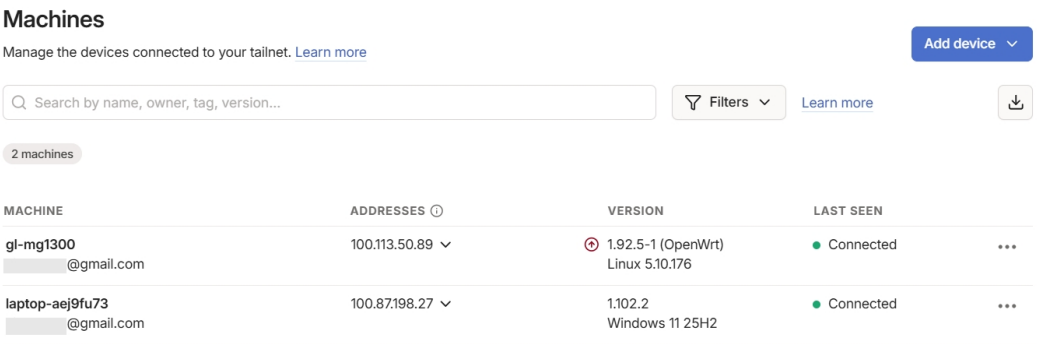
Uruchomienie węzła wyjściowego na routerze umożliwia innym urządzeniom w sieci tailnet kierowanie całego wychodzącego ruchu internetowego przez publiczny adres IP tego routera.

Na poniższym schemacie laptop znajduje się w Bostonie, a router GL-MG1300 w Hongkongu. Oba urządzenia dodano do tej samej sieci Tailscale. Jeśli ustawisz GL-MG1300 jako węzeł wyjściowy, cały ruch wychodzący z laptopa będzie przechodzić przez ten router do Internetu, a publiczny adres IP laptopa będzie wskazywać Hongkong zamiast Bostonu.

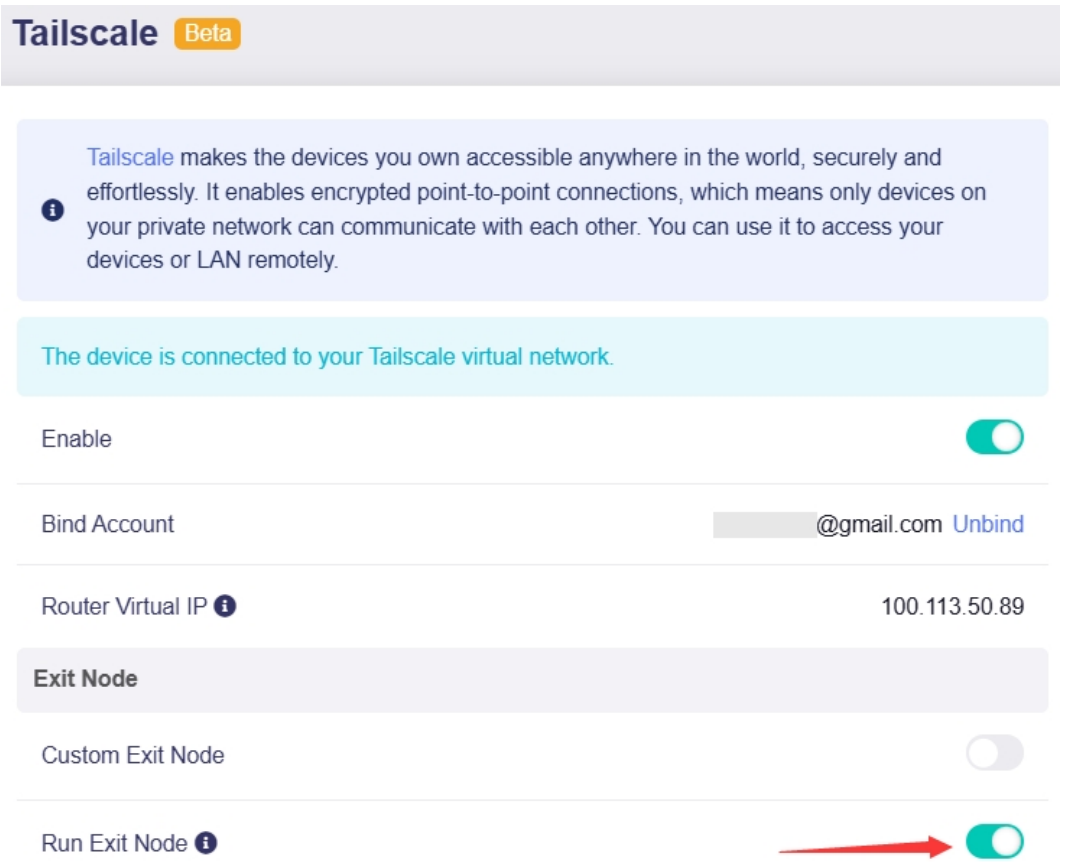


Aby ustawić GL-MG1300 jako węzeł wyjściowy, wykonaj poniższe czynności.

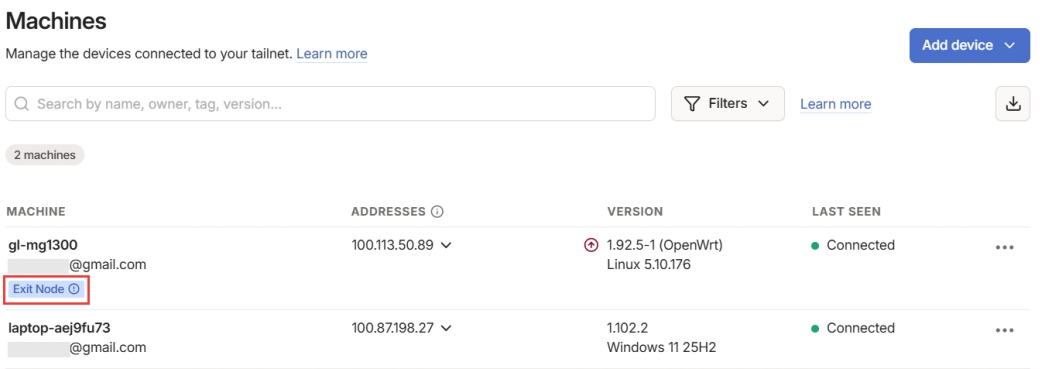
1. Dodaj router GL-MG1300 i laptop podróżny do tej samej sieci tailnet Tailscale.



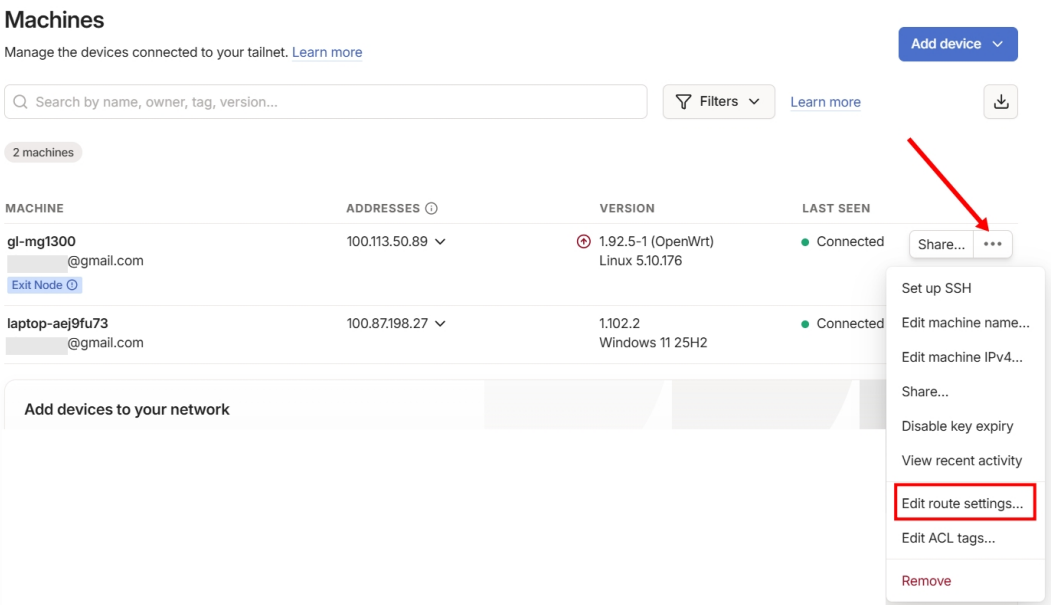
2. W panelu administracyjnym GL-MG1300 przejdź do **APPLICATIONS** > **Tailscale**. Włącz **Run Exit Node** i kliknij **Apply**.



3. Przejdź do konsoli administracyjnej Tailscale. Pod GL-MG1300 pojawi się etykieta „Exit Node”.



4. Kliknij ikonę trzech kropek po prawej stronie GL-MG1300 i wybierz **Edit route settings**.



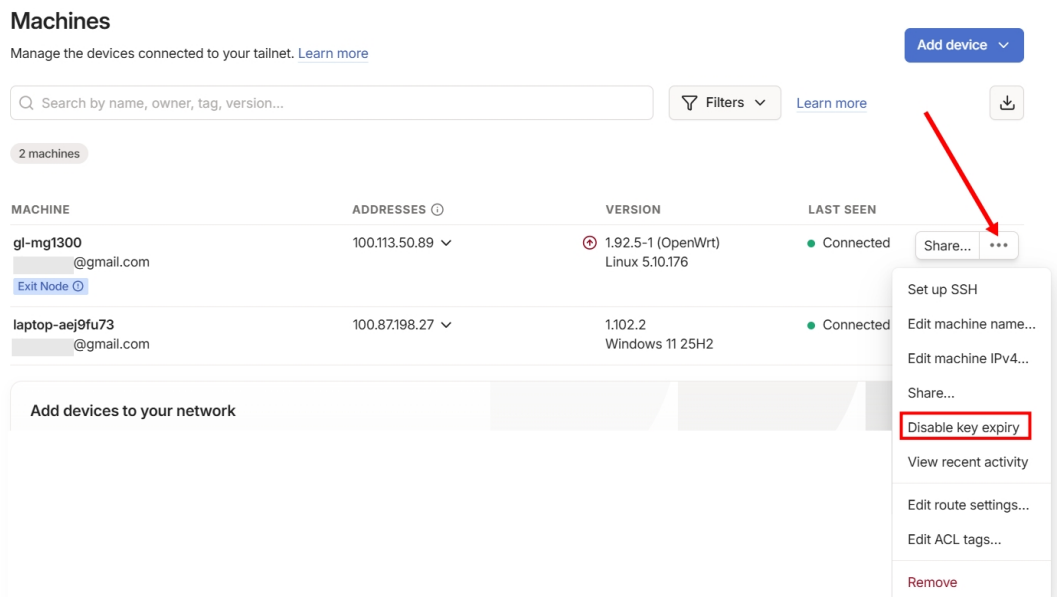
5. W wyświetlonym oknie zaznacz **Use as exit node** i kliknij **Save**.



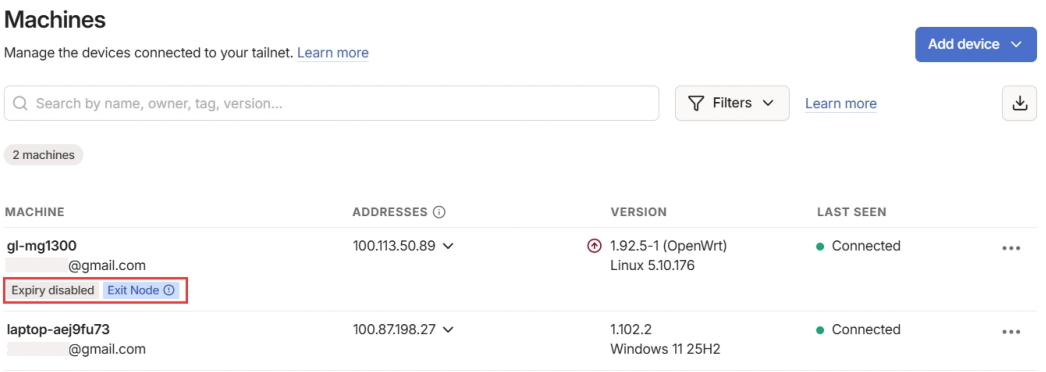
6. Wyłącz wygasanie klucza.

   Ze względów bezpieczeństwa użytkownicy muszą okresowo ponownie uwierzytelniać każde urządzenie. Aby uniknąć rozłączeń po wygaśnięciu klucza uwierzytelniającego węzła wyjściowego, zalecamy wyłączenie wygasania klucza dla tego węzła. Kliknij tutaj, aby dowiedzieć się więcej o wygasaniu kluczy.

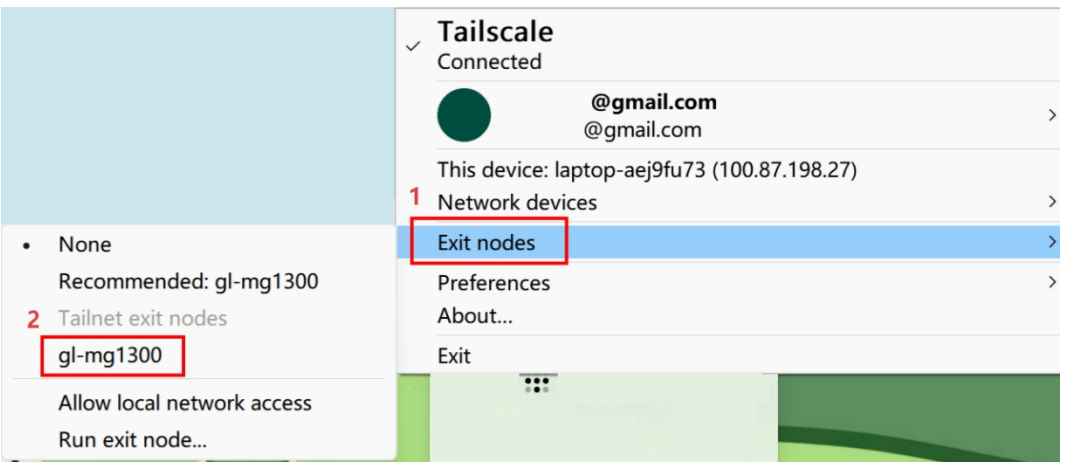
   Kliknij ikonę trzech kropek po prawej stronie GL-MG1300 i wybierz Disable key expiry.



   Po zastosowaniu ustawienia pod GL-MG1300 pojawi się etykieta „Expiry disabled”.



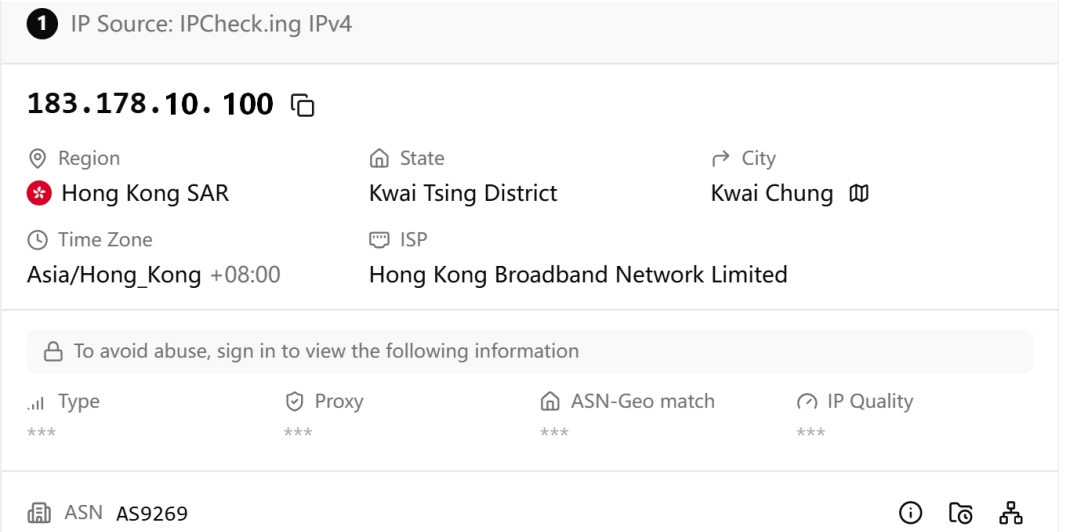
7. Uruchom Tailscale na laptopie podróżnym. Ikona Tailscale pojawi się w zasobniku systemowym w prawym dolnym rogu. Kliknij ją prawym przyciskiem myszy, wybierz **Exit nodes**, a następnie **gl-mg1300**.



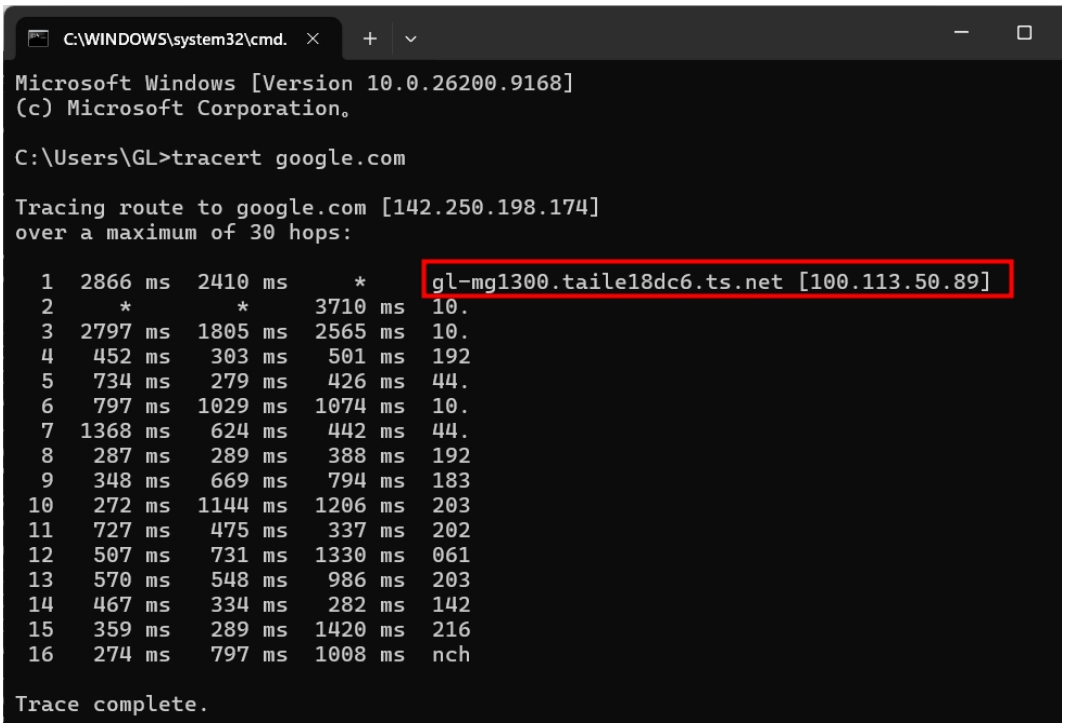
Cały ruch wychodzący z tego laptopa podróżnego będzie teraz przechodzić przez GL-BMG1300 do Internetu.

8. Sprawdź łączność.

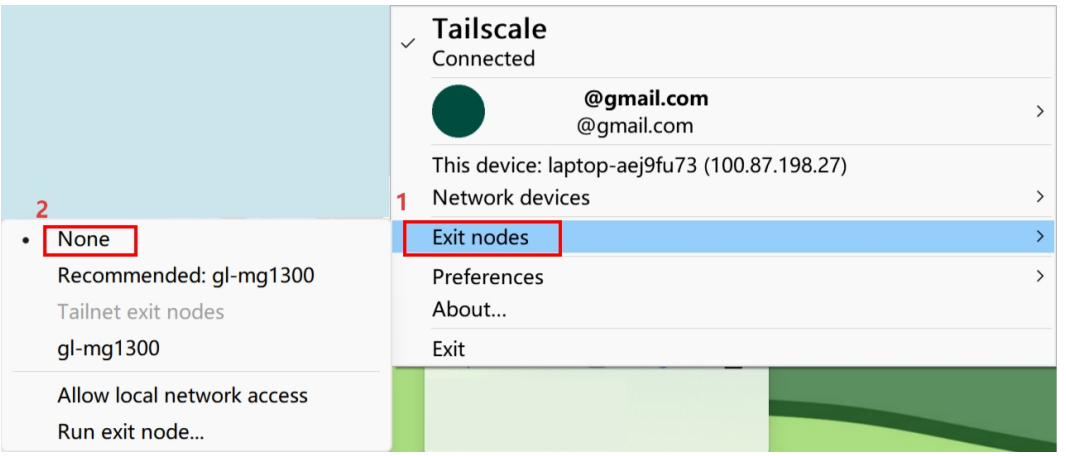
(1) Na laptopie podróżnym otwórz przeglądarkę i odwiedź ipcheck.ing lub inną stronę sprawdzającą adres IP. Strona wyświetli publiczny adres IP węzła wyjściowego Tailscale, potwierdzając, że laptop łączy się z Internetem przez ten węzeł (w tym przykładzie GL-MG1300 znajdujący się w Hongkongu).



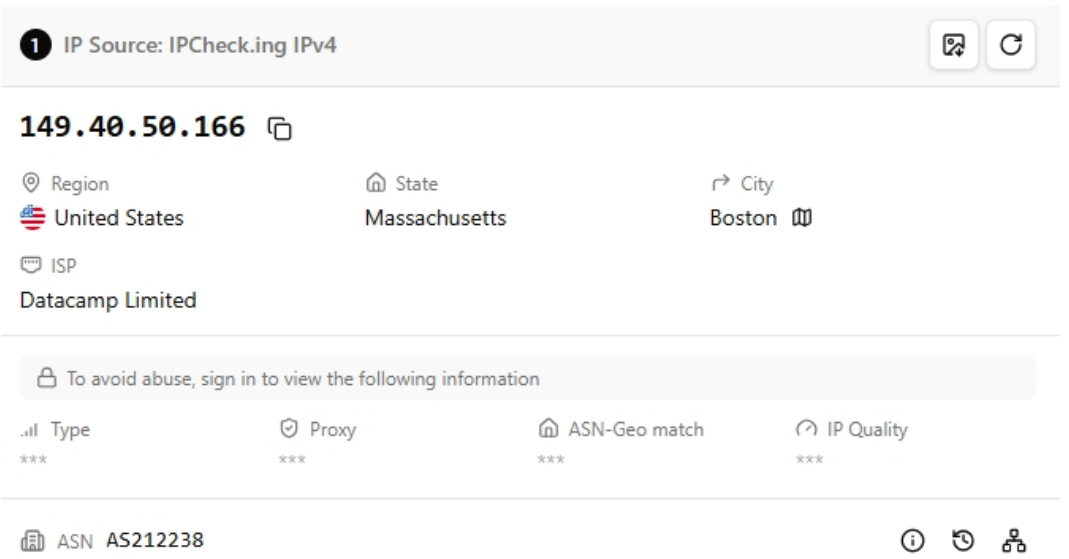
(2) Naciśnij *Win+R*, wpisz *cmd*, aby uruchomić wiersz polecenia, a następnie wykonaj *tracert google.com*, aby prześledzić trasy ruchu wychodzącego. Wynik polecenia zawiera wszystkie przeskoki routingu ruchu internetowego. Przy poprawnej konfiguracji pierwszy przeskok zewnętrzny prowadzi przez węzeł wyjściowy, jak pokazano poniżej. Potwierdza to, że cały ruch wychodzący do Internetu opuszcza sieć przez ten router.



(3) Rozłącz węzeł wyjściowy, aby wykonać test porównawczy. Kliknij prawym przyciskiem ikonę Tailscale w zasobniku systemowym w prawym dolnym rogu, kliknij **Exit nodes** i wybierz **None**, aby przestać korzystać z węzła wyjściowego.



(4) Otwórz nową kartę przeglądarki i odwiedź ipcheck.ing lub inną usługę sprawdzania adresu IP. Teraz pojawi się własny publiczny adres IP laptopa, co potwierdzi, że urządzenie korzysta z lokalnego łącza internetowego (w tym przykładzie w Bostonie).



Rozdział 16

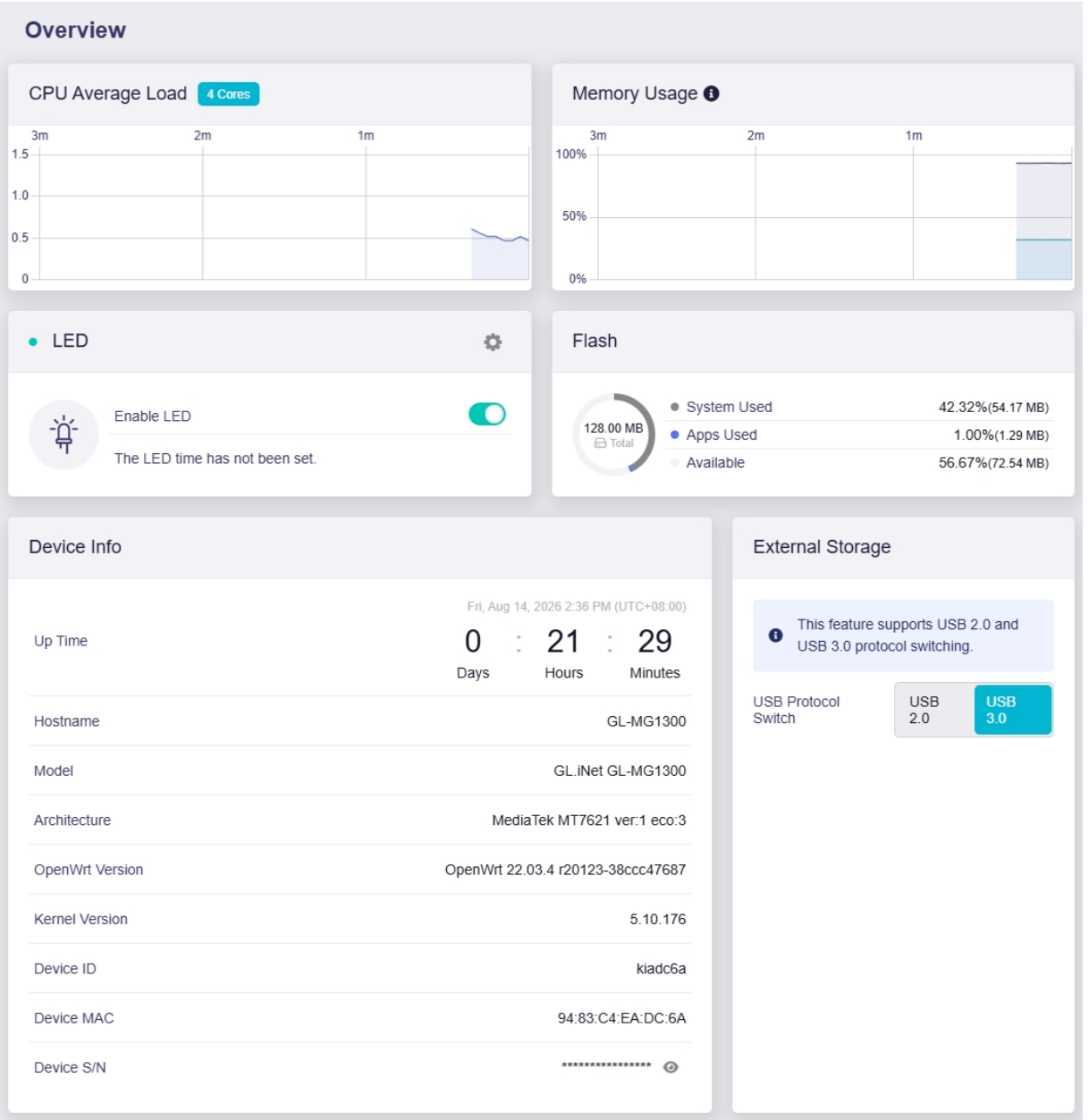
System

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

16.1 Przegląd

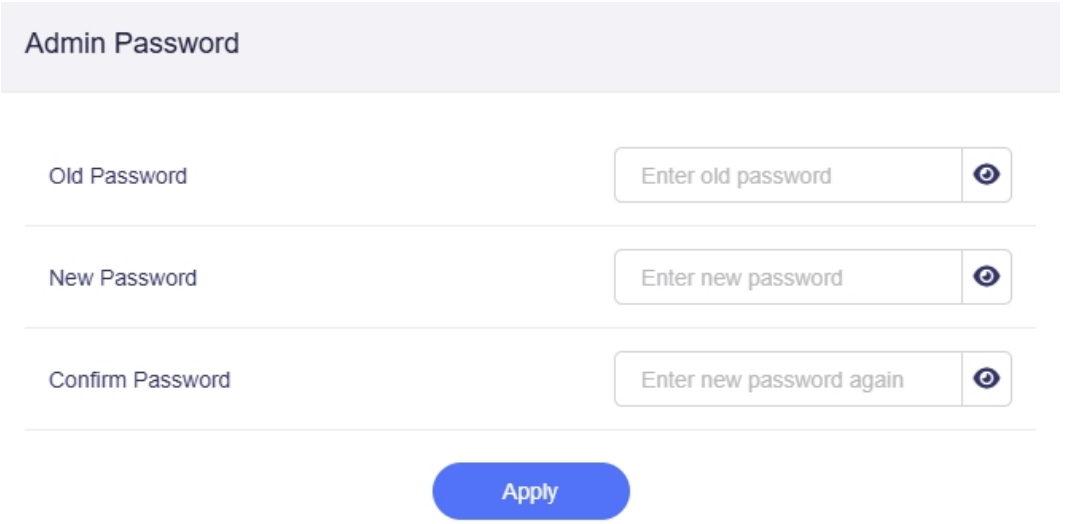
Zaloguj się do panelu administracyjnego routera i przejdź do **SYSTEM** > **Overview**. Strona wyświetla stan sprzętu i udostępnia proste funkcje sterowania, w tym:

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



16.2 Hasło administratora

Zaloguj się do panelu administracyjnego routera i przejdź do **SYSTEM** > **Admin Password**. Tutaj możesz zmienić hasło logowania do panelu administracyjnego.



Wymagania dotyczące hasła administratora:

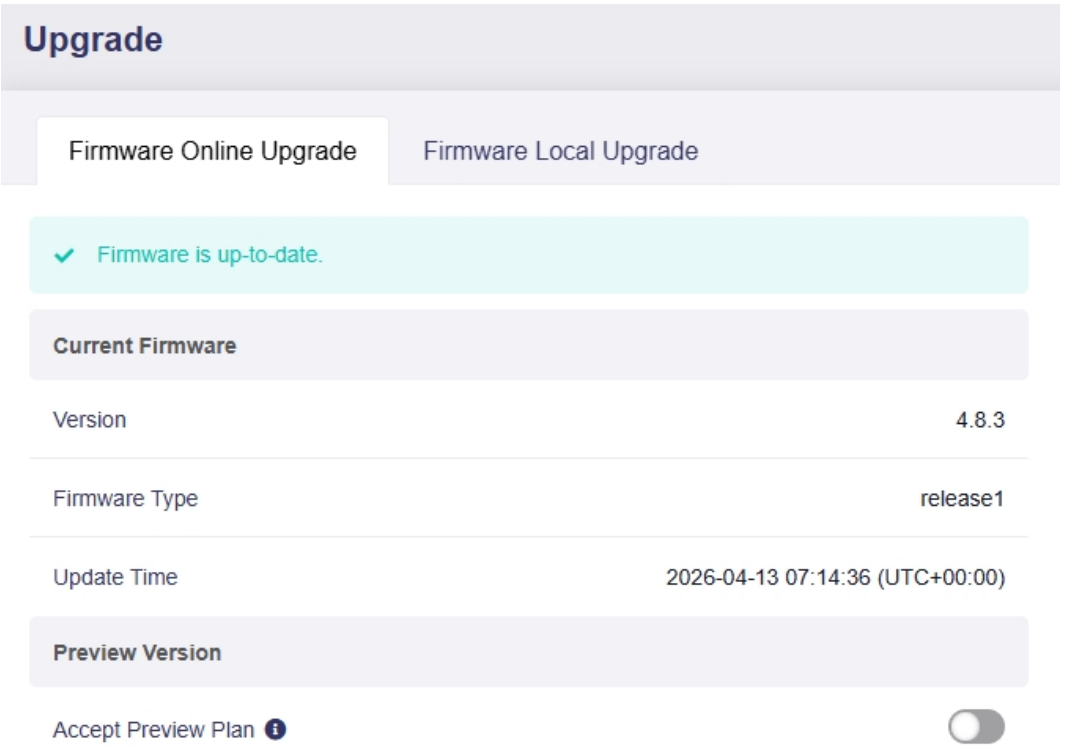
1. Długość od 10 do 63 znaków.
2. Dozwolone są litery (z rozróżnianiem wielkości), cyfry i symbole (np. ! @ # $ % ^ & * ( ) _ + - = , . > < | ? / \ [ ] { } : ; " ' ` ~).
3. Wymagane są co najmniej dwa rodzaje znaków spośród: wielkie litery, małe litery, cyfry i symbole.

16.3 Aktualizacja

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

16.3.1 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.

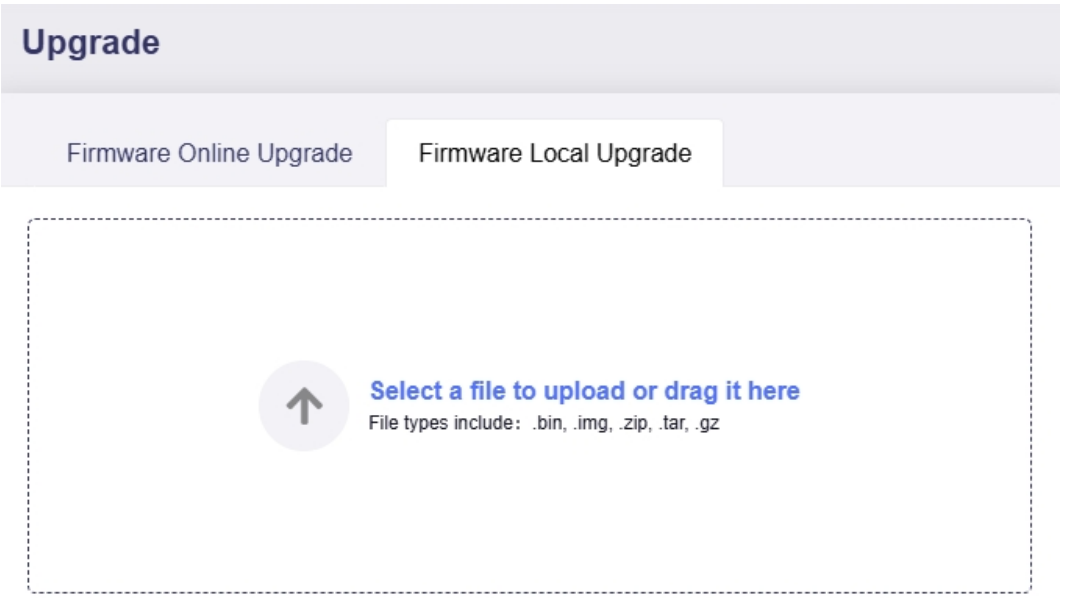
Jeśli router ma połączenie z Internetem, sprawdzi dostępność nowszej wersji oprogramowania do pobrania.

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

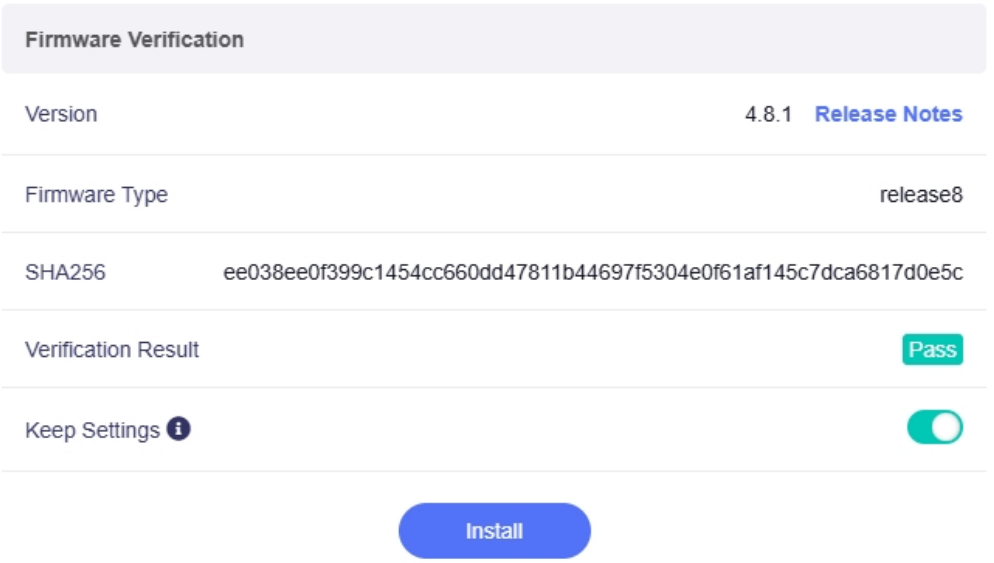
16.3.2 Aktualizacja lokalna

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.

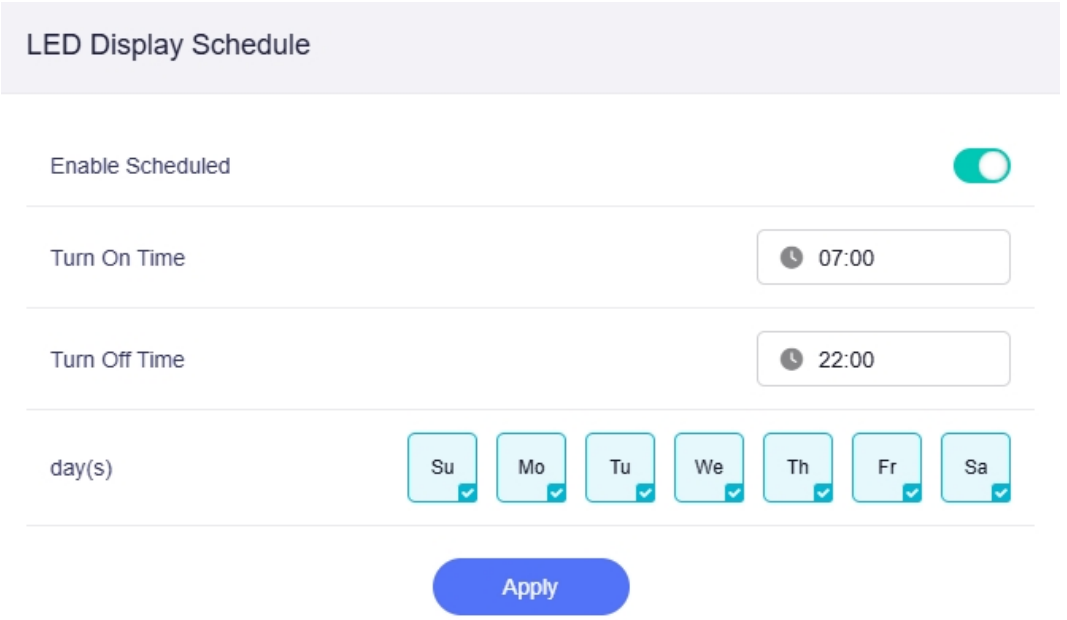
16.4 Zadania zaplanowane

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.

16.4.1 Harmonogram diody LED

W razie potrzeby ustaw harmonogram diody LED routera.

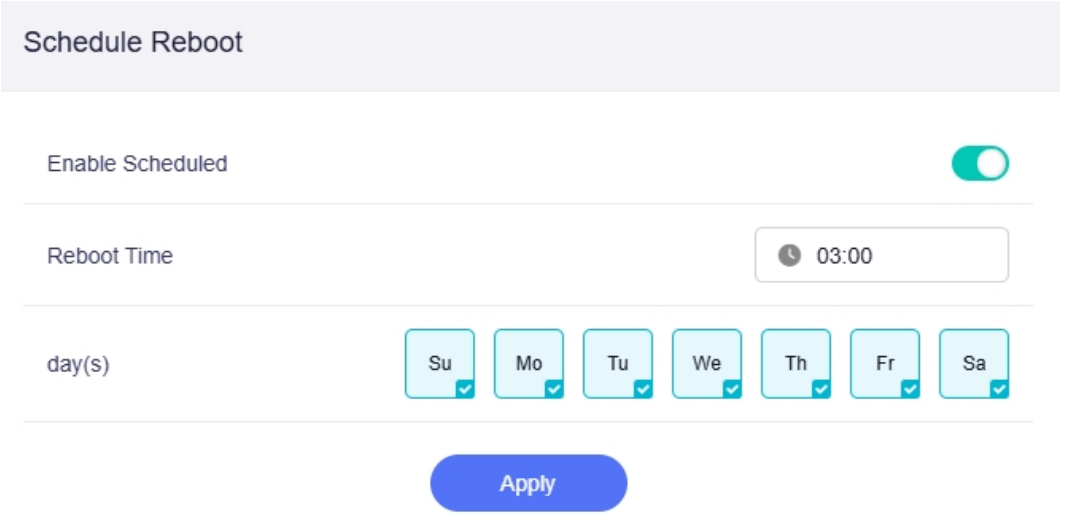


- **Enable Scheduled**: włącz ten przełącznik, aby uruchomić harmonogram diody LED.
- **Turn On Time**: ustaw godzinę włączenia diody LED (np. 07:00).
- **Turn Off Time**: ustaw godzinę wyłączenia diody LED (np. 22:00).
- **day(s)**: wybierz dni tygodnia, w których te ustawienia mają obowiązywać.

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

16.4.2 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 te ustawienia mają obowiązywać.

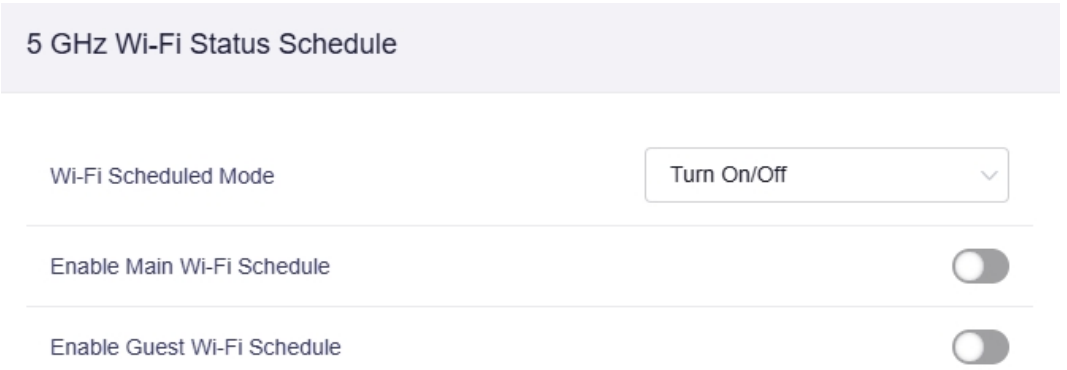
Po skonfigurowaniu kliknij **Apply**, aby zapisać ustawienia.

16.4.3 Harmonogram Wi-Fi 5 GHz

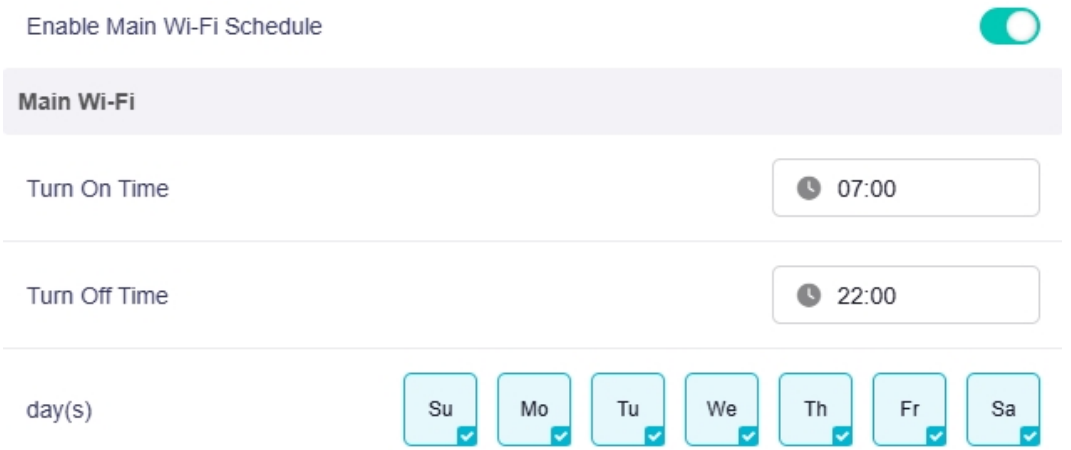
Ta funkcja umożliwia ustawienie harmonogramu Wi-Fi 5 GHz. Dostępne są dwa tryby: Turn On/Off i Switch TX Power.

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

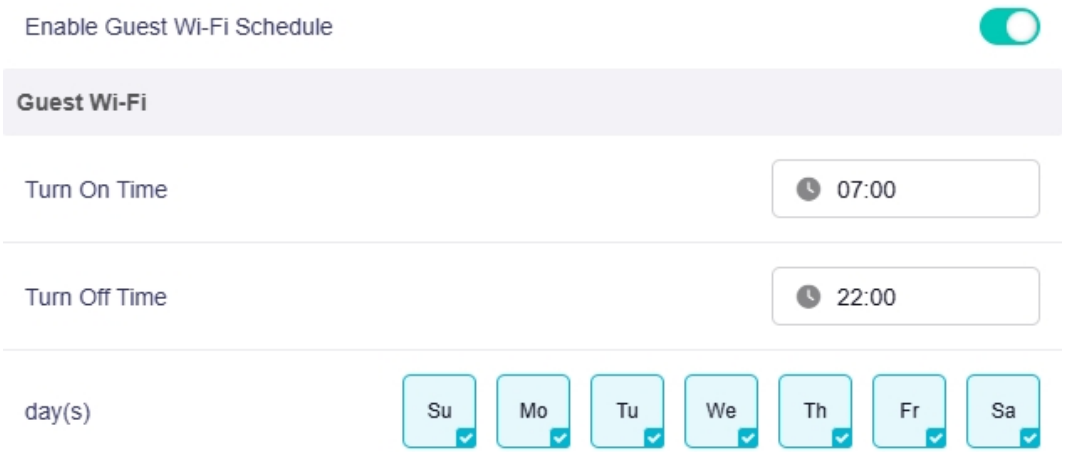
Możesz włączyć harmonogram włączania i wyłączania głównej oraz gościnnej sieci Wi-Fi 5 GHz.



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



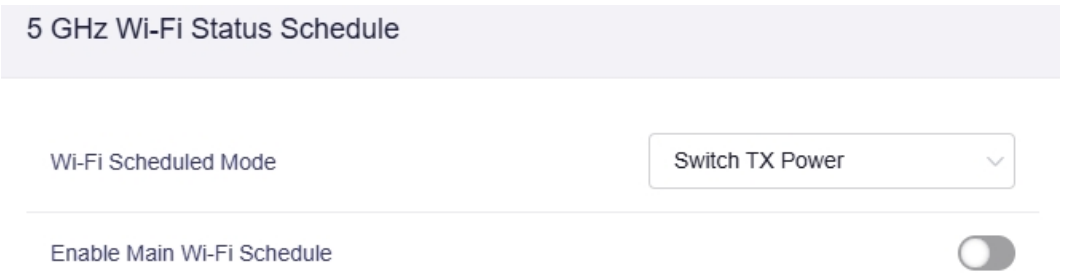
- **Guest Wi-Fi Schedule**: po włączeniu ustaw godziny włączania i wyłączania gościnnej sieci Wi-Fi 5 GHz oraz wybierz dni tygodnia, w których harmonogram obowiązuje.



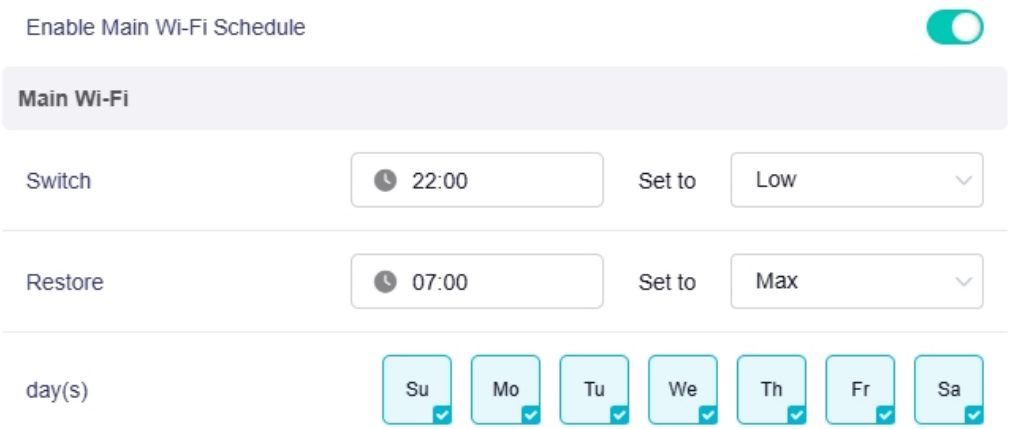
Po skonfigurowaniu kliknij **Apply**, aby zapisać ustawienia.

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 czynności zmiany mocy nadawania głównej sieci Wi-Fi 5 GHz oraz wybierz dni tygodnia, w których obowiązują.



- **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.

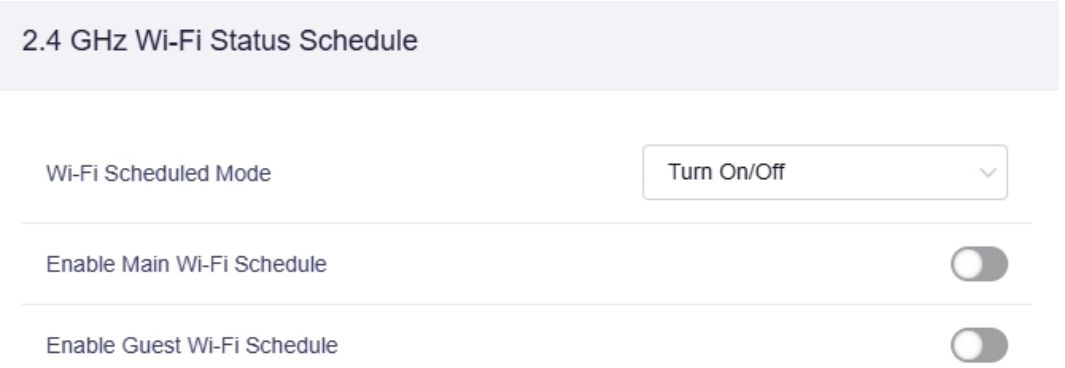
Po skonfigurowaniu kliknij **Apply**, aby zapisać ustawienia.

16.4.4 Harmonogram Wi-Fi 2,4 GHz

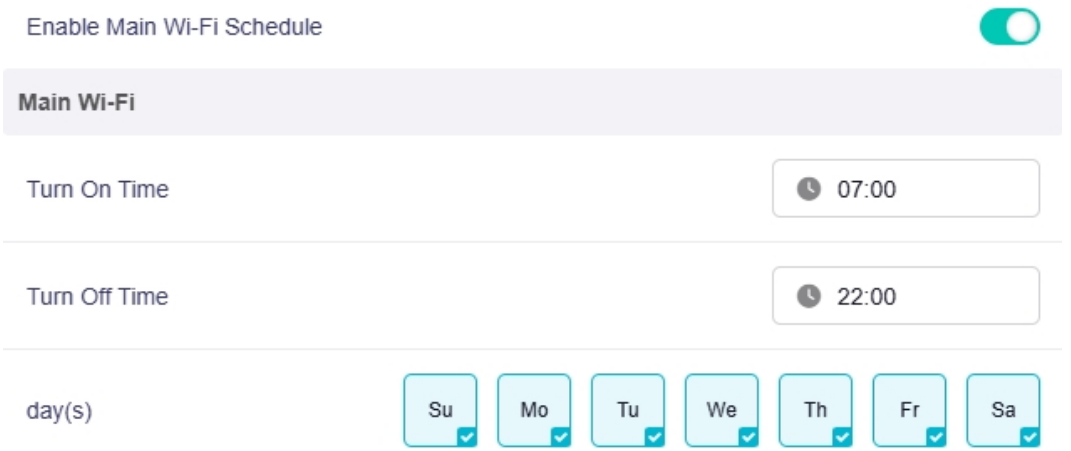
Ta funkcja umożliwia ustawienie harmonogramu Wi-Fi 2,4 GHz. Dostępne są dwa tryby: Turn On/Off i Switch TX Power.

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

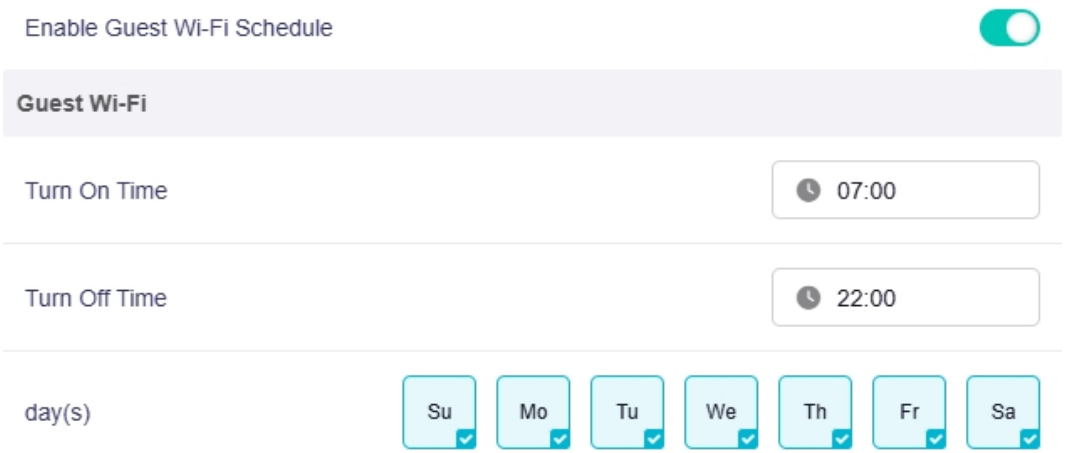
Możesz włączyć harmonogram włączania i wyłączania głównej oraz gościnnej sieci Wi-Fi 2,4 GHz.



- **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 obowiązuje.



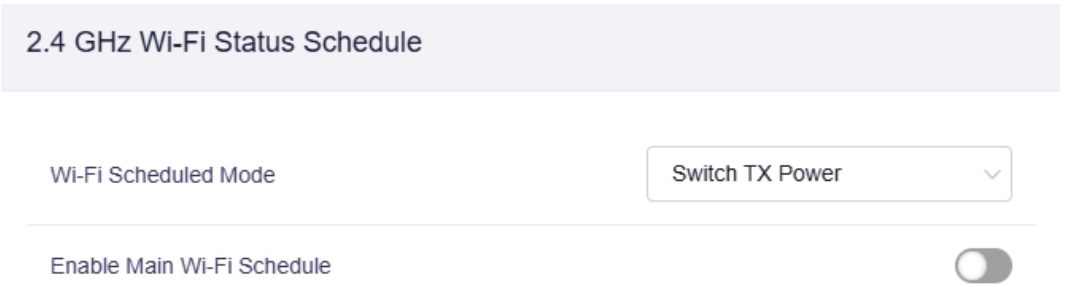
- **Guest Wi-Fi Schedule**: po włączeniu ustaw godziny włączania i wyłączania gościnnej sieci Wi-Fi 2,4 GHz oraz wybierz dni tygodnia, w których harmonogram obowiązuje.



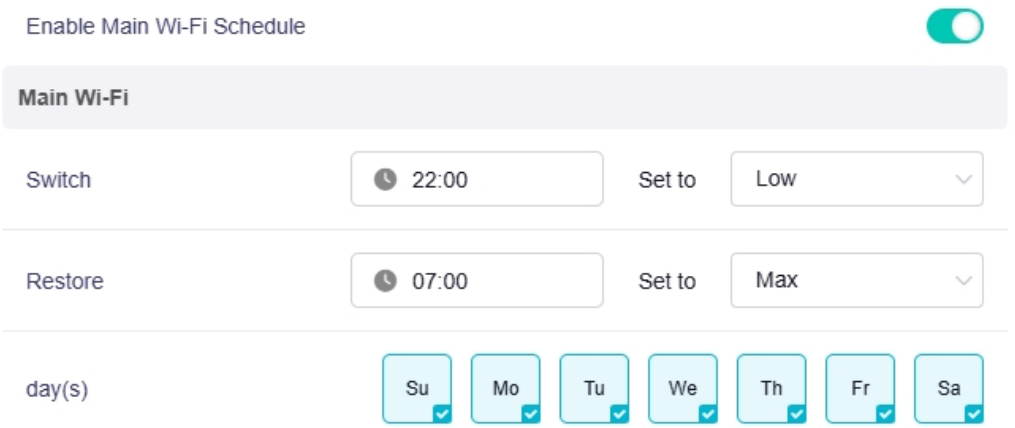
Po skonfigurowaniu kliknij **Apply**, aby zapisać ustawienia.

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 czynności zmiany mocy nadawania głównej sieci Wi-Fi 2,4 GHz oraz wybierz dni tygodnia, w których obowiązują.

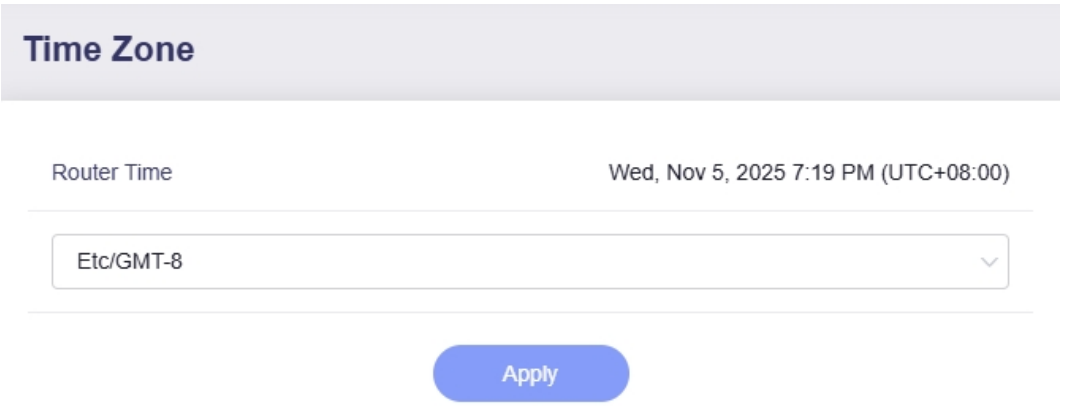


- **Switch**: o wybranej porze (np. 22:00) ustawia moc nadawania (np. Low).
- **Restore**: przywraca inny poziom mocy nadawania (np. Max) o innej godzinie (np. 07:00).
- **days**: wybierz dni tygodnia, w których te ustawienia mają obowiązywać.

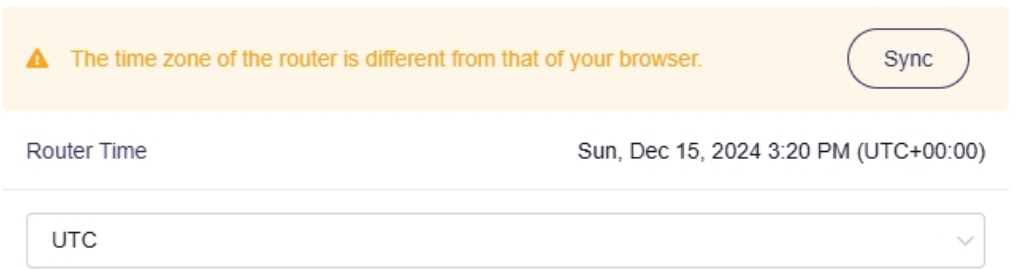
Po skonfigurowaniu kliknij **Apply**, aby zapisać ustawienia.

16.5 Strefa czasowa

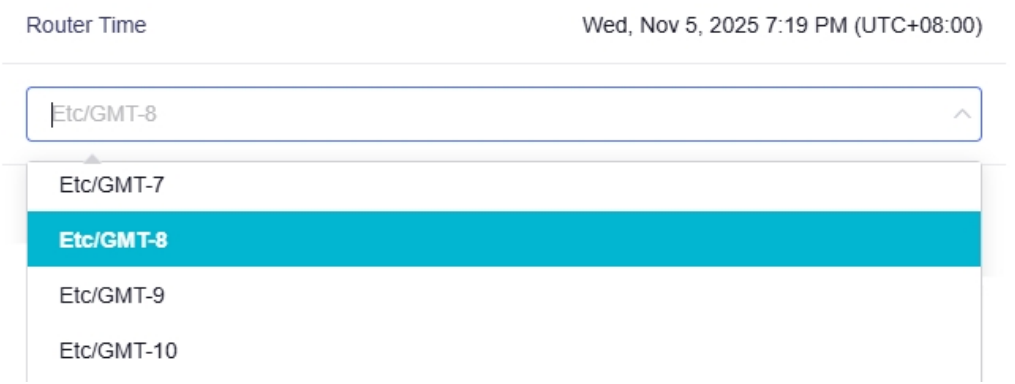
Zaloguj się do panelu administracyjnego routera i przejdź do **SYSTEM** > **Time Zone**. Strona wyświetla czas systemowy routera: datę, godzinę i odpowiadające im przesunięcie strefy czasowej.



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.



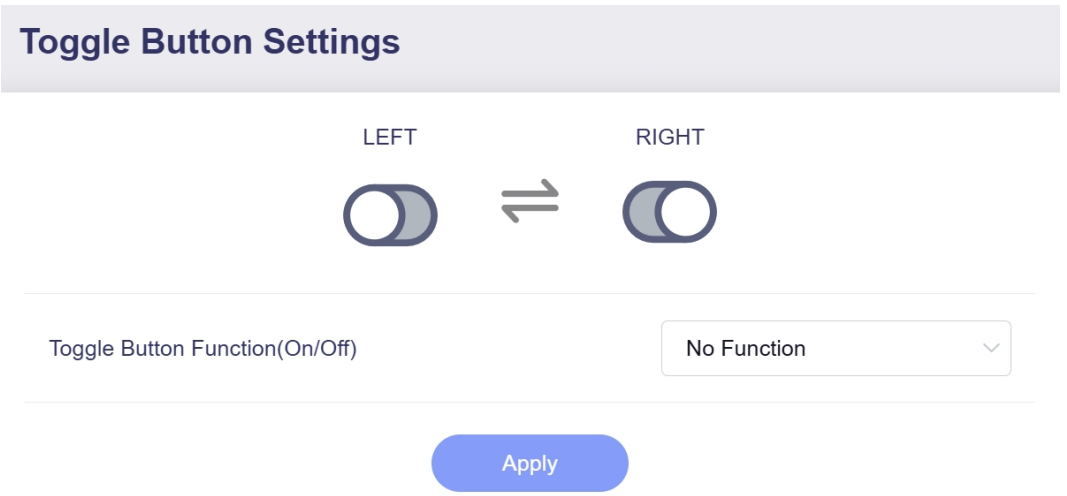
Aby zmienić strefę czasową, wybierz odpowiednią pozycję z listy, tak aby czas systemowy routera odpowiadał czasowi lokalnemu.



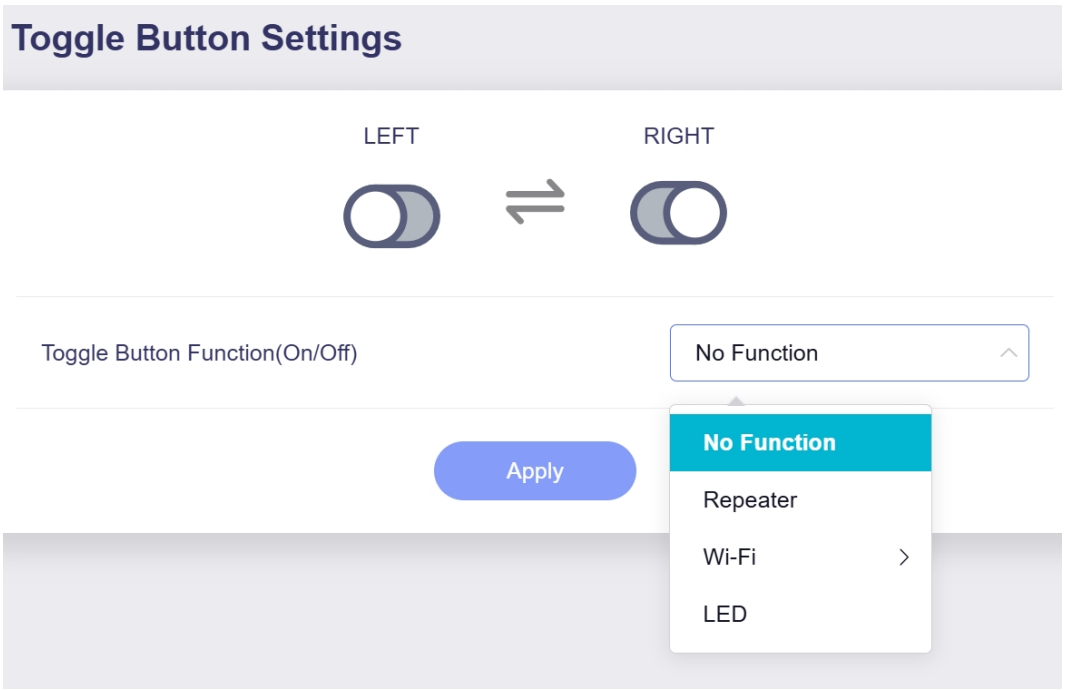
16.6 Ustawienia przełącznika

Zaloguj się do panelu administracyjnego routera i przejdź do **SYSTEM** > **Toggle Button Settings**.

Na tej stronie możesz dostosować funkcję fizycznego przełącznika routera (umieszczonego z boku), aby ułatwić jego obsługę.



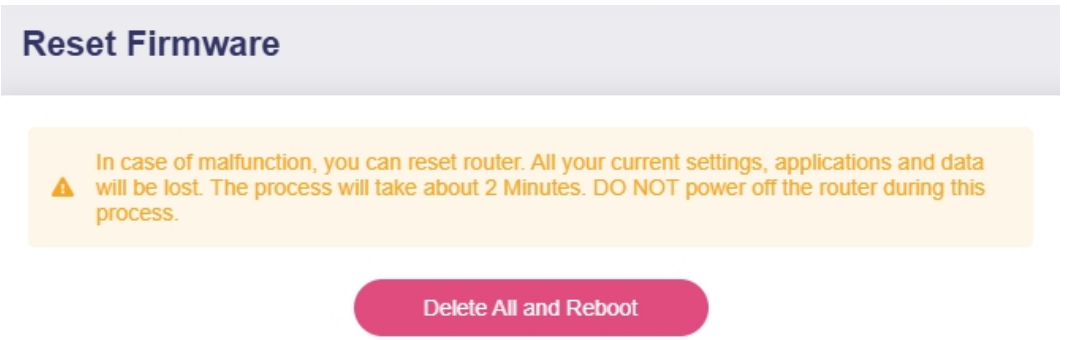
Domyślnie przełącznik nie ma przypisanej funkcji. W razie potrzeby możesz go skonfigurować, aby
jednym ruchem włączać lub wyłączać wybrane funkcje.


Toggle Button Settings
LEFT
RIGHT
Toggle Button Function(On/Off)
No Function
Apply
No Function
Repeater
Wi-Fi
LED

16.7 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.

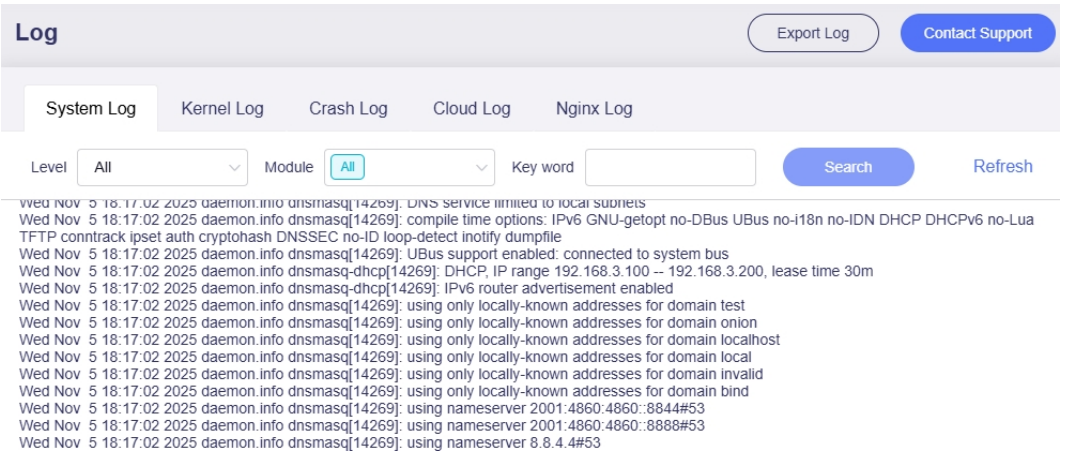


Uwaga: wszystkie bieżące ustawienia, aplikacje i dane zostaną usunięte. Proces trwa około 2 minut. W tym czasie nie wyłączaj zasilania routera.

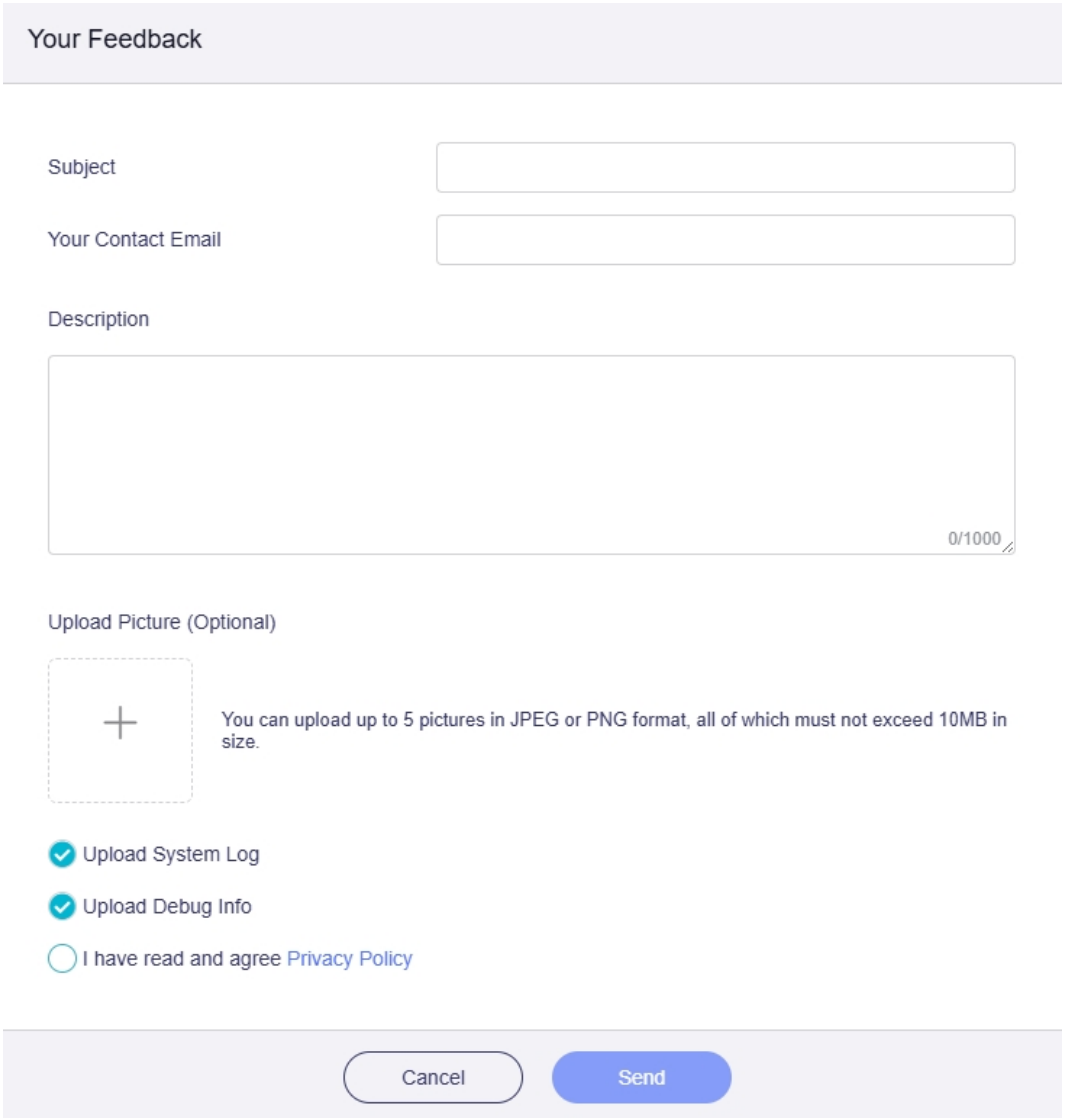
Jeśli panel administracyjny routera jest niedostępny, spróbuj zresetować router za pomocą fizycznego przycisku resetowania z boku urządzenia.

16.8 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.

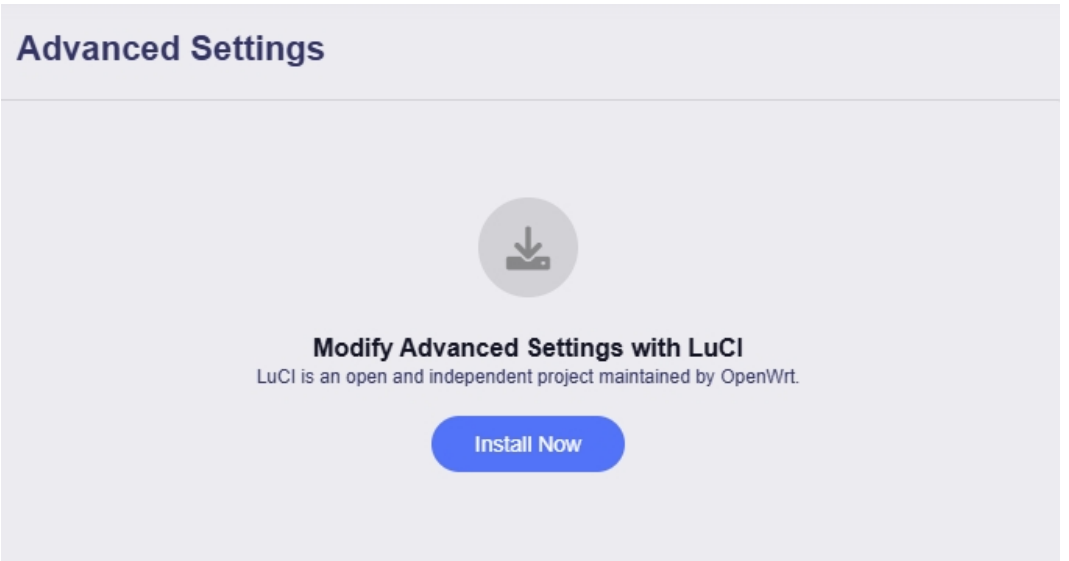

Your Feedback
Subject
Your Contact Email
Description
0/1000
Upload Picture (Optional)
You can upload up to 5 pictures in JPEG or PNG format, all of which must not exceed 10MB in size.
Upload System Log
Upload Debug Info
I have read and agree Privacy Policy
Cancel
Send

16.9 Ustawienia zaawansowane

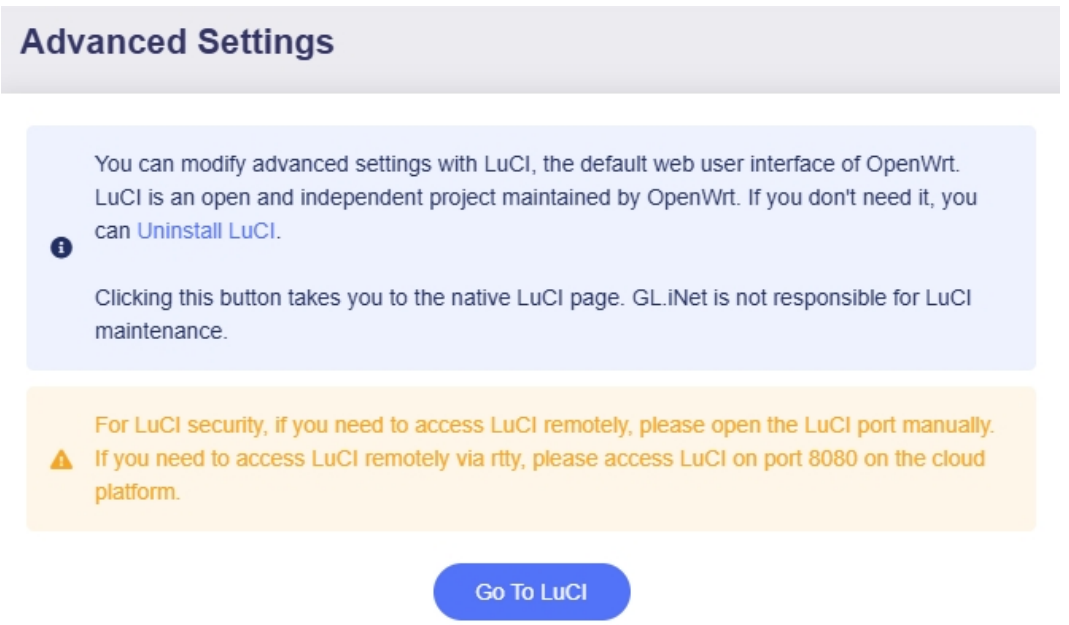
Zaloguj się do panelu administracyjnego routera i przejdź do **SYSTEM** > **Advanced Settings**. Tutaj możesz zmieniać ustawienia zaawansowane w LuCI, domyślnym interfejsie internetowym OpenWrt. LuCI to otwarty, niezależny projekt utrzymywany przez OpenWrt, udostępniany w obecnej postaci. GL.iNet nie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

Aby zalogować się do interfejsu LuCI, wykonaj poniższe czynności.

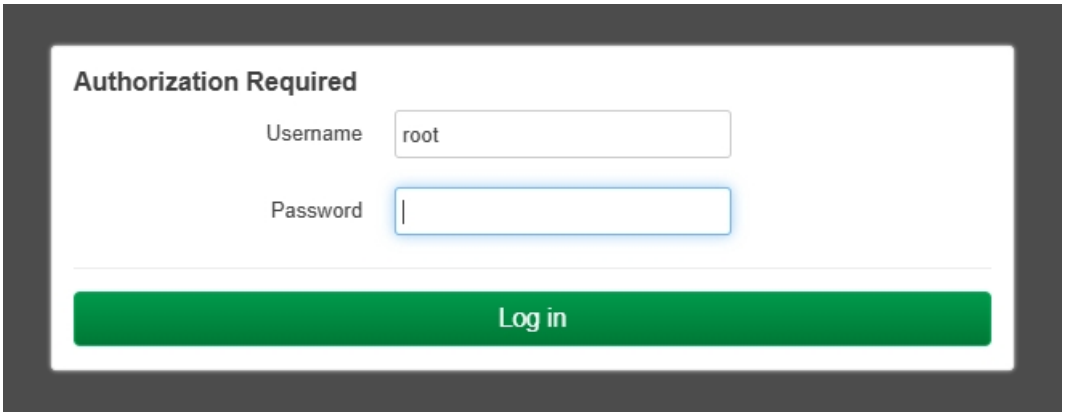
1. Kliknij **Install Now**, aby rozpocząć instalację interfejsu LuCI.



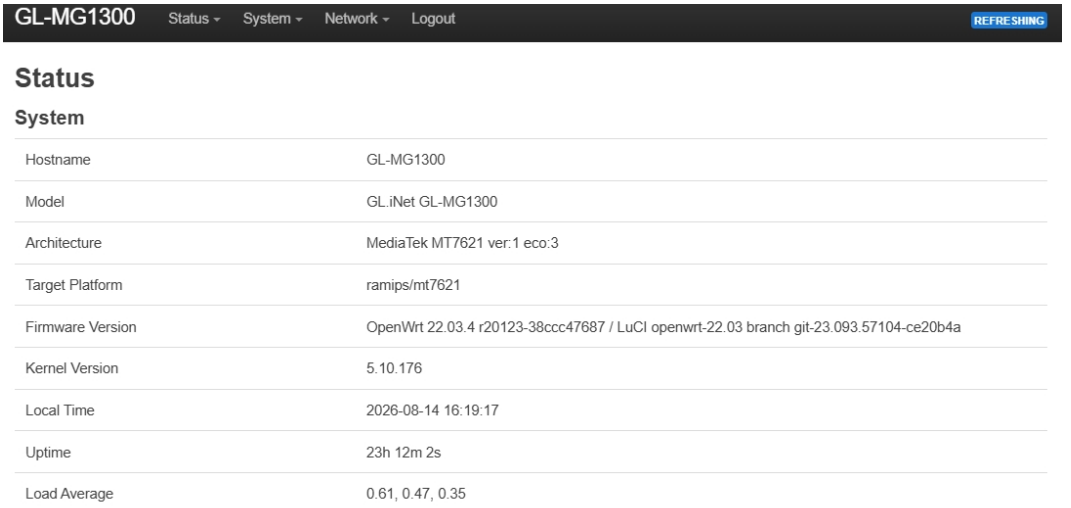
2. Kliknij **Go To LuCI**, aby przejść do strony logowania LuCI.



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



Otworzy się interfejs LuCI.



Oświadczenia dotyczące zgodności z przepisami

To urządzenie zawiera nadajniki/odbiorniki niewymagające zezwolenia, zgodne z normami RSS organizacji Innovation, Science and Economic Development Canada dotyczącymi urządzeń niewymagających zezwolenia. Użytkowanie 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.
Działanie podlega następującym dwóm warunkom:
(1) Urządzenie nie może powodować zakłóceń.
(2) Urządzenie musi przyjmować wszelkie zakłócenia radioelektryczne, nawet jeśli mogą one zakłócać jego działanie.

To urządzenie spełnia limity narażenia na promieniowanie IC RSS-102 określone dla środowiska niekontrolowanego.
Urządzenie należy instalować i użytkować z zachowaniem odległości co najmniej 20 cm między elementem promieniującym a ciałem.

Urządzenie spełnia limity narażenia na promieniowanie IC CNR-102 określone dla środowiska niekontrolowanego.
Urządzenie należy instalować i użytkować z zachowaniem odległości co najmniej 20 cm między elementem promieniującym a ciałem użytkownika.

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 działające w paśmie 5150–5250 MHz jest przeznaczone wyłącznie do użytku wewnątrz pomieszczeń w celu ograniczenia ryzyka szkodliwych zakłóceń mobilnych systemów satelitarnych korzystających z tego samego kanału.

Funkcje bezprzewodowych systemów dostępu, w tym radiowych sieci lokalnych (WAS/R-LAN), działające w tym urządzeniu w paśmie 5150–5350 MHz, są ograniczone do użytku wewnątrz pomieszczeń we wszystkich krajach Unii Europejskiej.

Deklaracja zgodności
Niniejszym GL TECHNOLOGIES (HONG KONG) LIMITED oświadcza, że urządzenie radiowe typu [dwupasmowy miniaturowy router podróżny, GL-MG1300] spełnia zasadnicze wymagania i pozostałe odpowiednie postanowienia dyrektywy 2014/53/UE. Pełny tekst deklaracji zgodności UE jest dostępny pod adresem https://www.gl-inet.com/products/certificate.

DLA UE:
Maksymalna moc wyjściowa
CE: ≤20 dBm EIRP (2,412–2,472 GHz); ≤23 dBm EIRP (5,15–5,35 GHz); s30 dBm EIRP (5,47–5,725 GHz); ≤13,98 dBm (5,725–5,85 GHz)