GL·iNet



Instrukcja obsługi

GL-B3000 / Marble

Dwupasmowy router domowy Wi-Fi 6

Wersja oprogramowania 4.5.22

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 8

1.1 Opis produktu 9

1.1.1 Wygląd 9

1.1.2 Złącza i przyciski 10

1.1.3 Dioda LED 11

1.2 Dane techniczne 11

1.3 Zawartość opakowania 12

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 19

4.1 Połączenie z Internetem przez kabel Ethernet 21

4.1.1 Podstawowa konfiguracja 21

4.1.2 Protokół 23

4.2 Połączenie z Internetem przez istniejącą sieć Wi-Fi 26

4.2.1 Podstawowa konfiguracja 26

4.2.2 Opcje wzmacniacza sygnału 29

Rozdział 5 Sieć bezprzewodowa 30

5.1 Wi-Fi 5 GHz 31

5.2 Wi-Fi 2,4 GHz 33

Rozdział 6 Urządzenia klienckie 35

6.1 Szczegóły urządzenia 37

6.2 Działania 39

6.3 Usuwanie urządzeń klienckich 41

6.4 Sortowanie 42

Rozdział 7 Poznaj VPN 43

7.1 Wprowadzenie 44

7.2 Przykłady zastosowań 45

Rozdział 8 Panel VPN 48

8.1 Klient VPN 49

8.1.1 Opcje klienta 50
8.1.2 Tryb reguł 52
8.1.3 Opcje globalne 53
8.2 Serwer VPN 56
8.2.1 Opcje serwera 57
8.2.2 Reguły tras serwera 58
8.2.3 Opcje globalne 60
Rozdział 9 Konfiguracja serwera VPN 61
9.1 Konfiguracja serwera OpenVPN 62
9.1.1 Przygotowanie 62
9.1.2 Etapy konfiguracji 63
9.1.3 Rozwiązywanie problemów 65
9.2 Konfiguracja serwera WireGuard 66
9.2.1 Przygotowanie 66
9.2.2 Etapy konfiguracji 67
9.2.3 Rozwiązywanie problemów 70
Rozdział 10 Konfiguracja klienta VPN 71
10.1 Konfiguracja klienta OpenVPN 72
10.1.1 Przygotowanie 72
10.1.2 Konfiguracja NordVPN 72
10.1.3 Ręczna konfiguracja klienta OpenVPN (inni dostawcy) 78
10.2 Konfiguracja klienta WireGuard 81
10.2.1 Przygotowanie 81
10.2.2 Konfiguracja AzireVPN 82
10.2.3 Konfiguracja Mullvad 85
10.2.4 Ręczna konfiguracja klienta WireGuard (inni dostawcy) 89
Rozdział 11 Tor 93
Rozdział 12 Aplikacje 96
12.1 Wtyczki 97
12.2 Dynamiczny DNS 98
12.2.1 Włączanie DDNS 98
12.2.2 Sprawdzanie działania DDNS 101
12.2.3 Zdalny dostęp przez HTTPS 103
12.2.4 Zdalny dostęp przez SSH 105

12.3 GoodCloud 107
12.3.1 Włączanie GoodCloud 108
12.3.2 Zarządzanie routerem 112
12.3.3 Usuwanie powiązania urządzenia 118
12.4 AdGuard Home 119
12.5 Kontrola rodzicielska 122
12.5.1 Szybka konfiguracja 122
12.6.2 Rozwiązywanie problemów 131
12.7 ZeroTier 132
12.7.1 Konfiguracja ZeroTier 133
12.7.2 Zdalny dostęp do WAN 137
12.7.3 Zdalny dostęp do LAN 138
12.8 Tailscale 139
12.8.1 Konfiguracja Tailscale 140
12.8.2 Zdalny dostęp do WAN 143
12.8.3 Zdalny dostęp do LAN 144
12.8.4 Niestandardowe węzły wyjściowe 145
Rozdział 13 Sieć 147
13.1 Zapora sieciowa 148
13.1.1 Przekierowanie portów 148
13.1.2 Otwieranie portów routera 150
13.1.3 DMZ 151
13.2 Multi-WAN 152
13.2.1 Monitorowanie stanu interfejsów 152
13.2.2 Tryb Multi-WAN 155
13.3 LAN 158
13.3.1 Ustawienia podstawowe 158
13.3.2 Serwer DHCP 159
13.3.3 Rezerwacja adresów 161
13.4 Sieć gościnna 162
13.4.1 Ustawienia podstawowe 162
13.4.2 Serwer DHCP 163
13.5 DNS 165
13.5.1 Ustawienia ogólne 165

13.5.2 Ustawienia serwera DNS 166
13.5.3 Edycja pliku hosts 168
13.6 Tryb sieciowy 170
13.7 IPv6 172
13.7.1 Tryb IPv6 172
13.7.2 Sposób uzyskiwania DNS 173
13.8 Adres MAC 174
13.9 Drop-in Gateway 176
13.10 IGMP Snooping 178
13.11 Przyspieszanie sieci 179
13.12 Ustawienia NAT 180
Rozdział 14 System 181
14.1 Przegląd 182
14.2 Aktualizacja 183
14.2.1 Aktualizacja online 183
14.2.2 Aktualizacja lokalna 184
14.3 Zadania zaplanowane 185
14.3.1 Harmonogram diody LED 185
14.3.2 Harmonogram ponownego uruchamiania 186
14.3.3 Harmonogram Wi-Fi 5 GHz 187
14.3.4 Harmonogram Wi-Fi 2,4 GHz 189
14.4 Strefa czasowa 191
14.5 Dziennik 193
14.6 Bezpieczeństwo 194
14.6.1 Hasło administratora 194
14.6.2 Kontrola dostępu lokalnego 195
14.6.3 Kontrola dostępu zdalnego 197
14.7 Resetowanie oprogramowania 198
14.8 Ustawienia zaawansowane 199

Rozdział 1

Poznaj swój router

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

1.1 Opis produktu

Router Marble (GL-B3000) sam w sobie jest dziełem sztuki: pomysłowo ukryty w ramce na zdjęcia, pozwala wyeksponować ulubiony obraz i wzbogacić wystrój wnętrza. Oprócz atrakcyjnego wyglądu router Marble (GL-B3000) zapewnia wysoką wydajność dzięki technologii Wi-Fi 6 i obsłudze VPN.

1.1.1 Wygląd

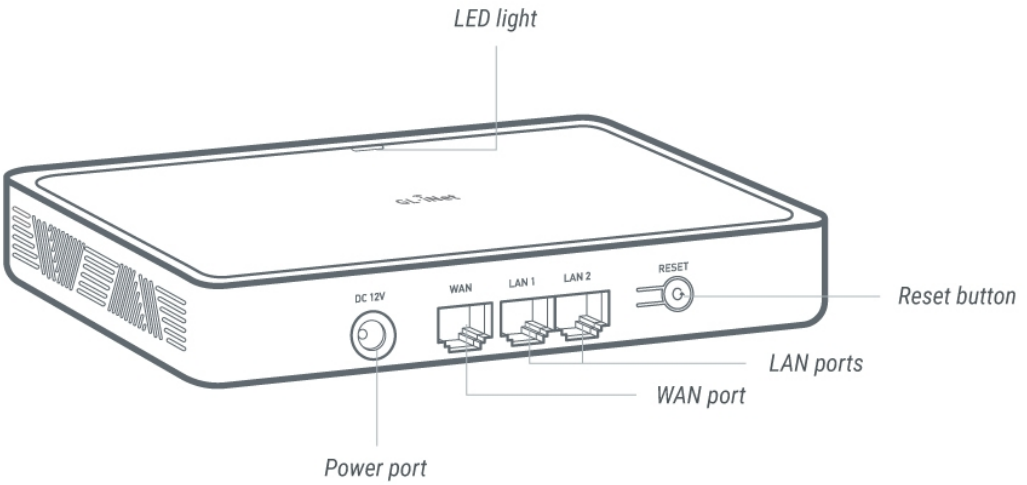








1.1.2 Złącza i przyciski



Element	Opis
Złącze zasilania	Służy do podłączenia zasilacza.
Port WAN	Służy do połączenia z modemem lub gniazdem Ethernet zapewniającym dostęp do Internetu.
Port LAN	W razie potrzeby służy do podłączenia urządzeń przewodowych.
Przycisk resetowania	Naciśnij i przytrzymaj przez **4 sekundy**, aby naprawić połączenie sieciowe; Naciśnij i przytrzymaj przez **10 sekund**, a następnie zwolnij, aby przywrócić ustawienia fabryczne routera.

1.1.3 Dioda LED

Stan	Znaczenie
Świeci na niebiesko	Uruchamianie systemu
Powoli miga na niebiesko	Wyszukiwanie sieci
Szybko miga na niebiesko	Aktualizacja oprogramowania
Świeci na biało	Normalna praca

1.2 Dane techniczne

Złącza	1 × port Ethernet WAN 2 × port Ethernet LAN 1 × wejście zasilania DC 12 V / 1,5 A 1 × przycisk resetowania
Procesor	Dwurdzeniowy procesor Qualcomm, 1 GHz
Pamięć RAM / pamięć masowa	DDR3L 512 MB / NAND Flash 128 MB
Protokół	IEEE 802.11a/b/g/n/ac/ax
Prędkość Wi-Fi	574 Mb/s (2,4 GHz), 2402 Mb/s (5 GHz)
Anteny	4 × antena wewnętrzna
Prędkość Ethernet	10/100/1000 Mb/s
Zasilanie	DC5521, 12 V / 1,5 A (5,5 × 2,1 mm)
Pobór mocy	< 13W
Temperatura pracy	0 ~ 40°C (32 ~ 104°F)
Temperatura przechowywania	-20 ~ 70°C (-4 ~ 158°F)

Wymiary / masa	Router: 155 × 120 × 23 mm / 275 g Ramka na zdjęcia: 235 × 197 × 32 mm (mieści zdjęcie 8-calowe)
Inne materiały i narzędzia	Karta katalogowa / Oprogramowanie / Aplikacja / Rozpakowanie / Poradniki

*Prędkości sieci bezprzewodowej określono na podstawie standardów IEEE 802.11 (np. 802.11ax dla Wi-Fi 6). Rzeczywista przepustowość i zasięg mogą być mniejsze ze względu na przeszkody w otoczeniu (ściany, metal), przeciążenie sieci lub możliwości urządzeń klienckich.

*Korzystanie z Wi-Fi 6 (802.11ax) i jego funkcji (OFDMA, MU-MIMO, 1024-QAM, HT160) wymaga obsługi odpowiednich technologii przez urządzenia klienckie.

1.3 Zawartość opakowania

Zasilacz dołączony do opakowania zależy od kraju dostawy.

Opakowanie zawiera:

- 1 × Marble (GL-B3000)
- 1 × instrukcja obsługi
- 1 × karta z podziękowaniem
- 1 × kabel Ethernet
- 1 × zestaw do montażu na ścianie
- 1 × podkładka samoprzylepna
- 1 × podstawka routera
- 1 × ramka na zdjęcia (opcjonalnie)
- 1 × zasilacz
- 1 × adapter wtyczki (zależnie od kraju dostawy)

User manual



Marble (GL-B3000)



Photo frame (Optional)



Thank you card



Adhesive pad

Router stand



Ethernet cable



Power adapter



Converters

(Base on your shipping countries)



Wall mount



Screws



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.
- **Ustawienie**: ustaw router na płaskiej, stabilnej powierzchni (półce, biurku) lub zamontuj go na ścianie, korzystając z dołączonego zestawu montażowego.
- **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

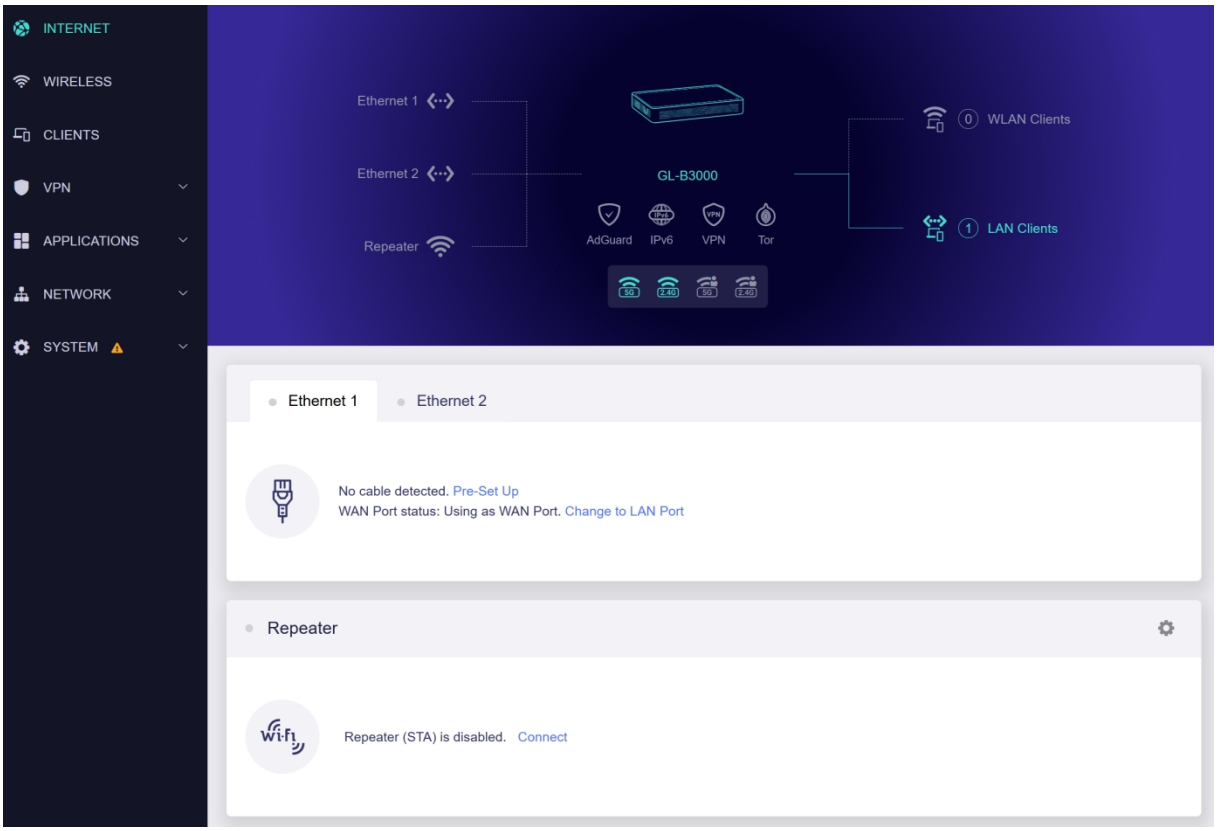
W tym rozdziale opisano logowanie do routera przez panel administracyjny w przeglądarce.

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.


INTERNET
WIRELESS
CLIENTS
VPN
APPLICATIONS
NETWORK
SYSTEM
Ethernet 1
Ethernet 2
Repeater
GL-B3000
AdGuard
IPv6
VPN
Tor
0 WLAN Clients
1 LAN Clients
Ethernet 1
Ethernet 2
No cable detected. Pre-Set Up
WAN Port status: Using as WAN Port. Change to LAN Port
Repeater
Repeater (STA) is disabled. Connect

Rozdział 4

Konfiguracja połączenia z Internetem

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

Marble obsługuje dwa sposoby połączenia z Internetem: Ethernet i Repeater. Wybierz odpowiedni sposób zgodnie ze swoimi potrzebami.

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.

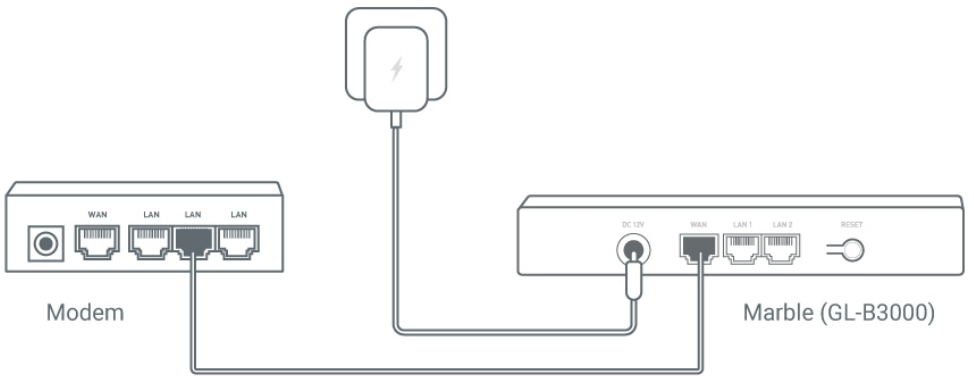
4.1 Połączenie z Internetem przez kabel Ethernet

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.

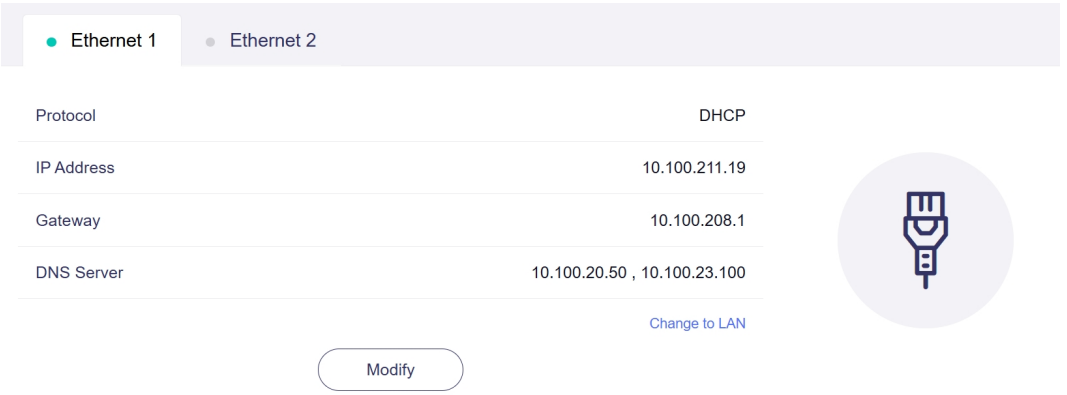
4.1.1 Podstawowa konfiguracja

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

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

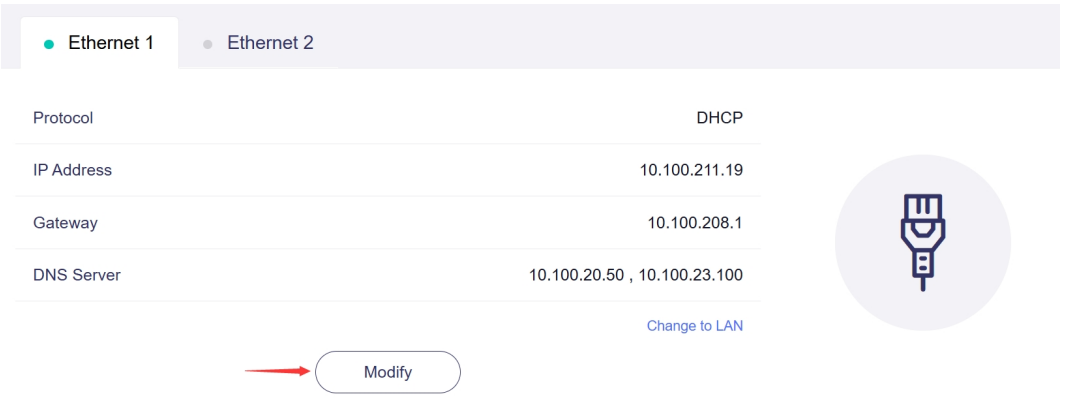


2. Zaloguj się do panelu administracyjnego routera i przejdź do **INTERNET** > **Ethernet**. Po pomyślnym nawiązaniu połączenia w sekcji Ethernet pojawią się szczegóły sieci, w tym protokół, adres IP, brama i serwer DNS.


Ethernet 1
Ethernet 2
Protocol
DHCP
IP Address
10.100.211.19
Gateway
10.100.208.1
DNS Server
10.100.20.50 , 10.100.23.100
Change to LAN
Modify

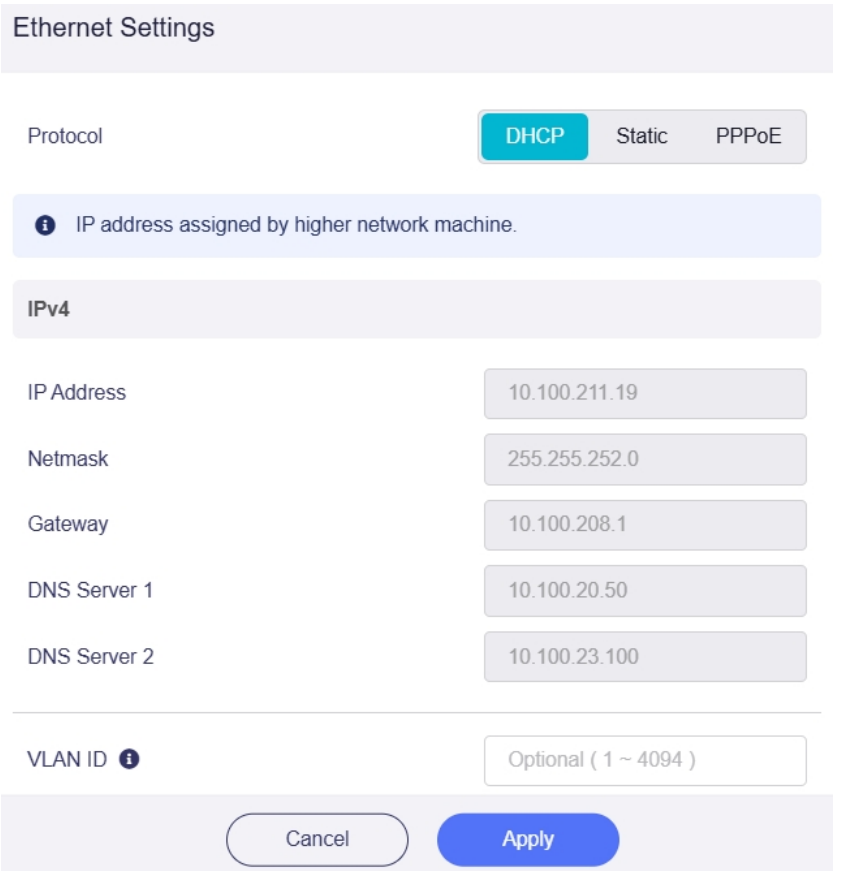
4.1.2 Protokół

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



- **DHCP**

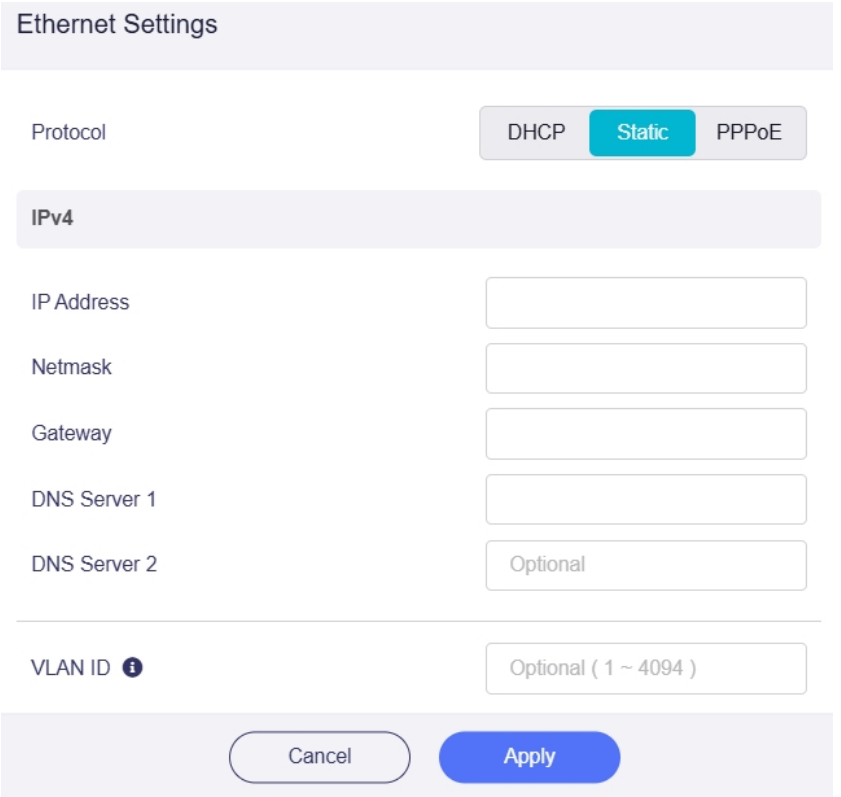
  DHCP to domyślny i najczęściej używany protokół sieciowy. Automatycznie przydziela adresy IP i inne parametry konfiguracji urządzeniom w sieci IP w modelu klient–serwer.



  Możesz skonfigurować **VLAN ID**, jeśli dostawca usług wymaga używania przez interfejs określonego identyfikatora tagowanej sieci VLAN.

- **Statyczny adres IP**

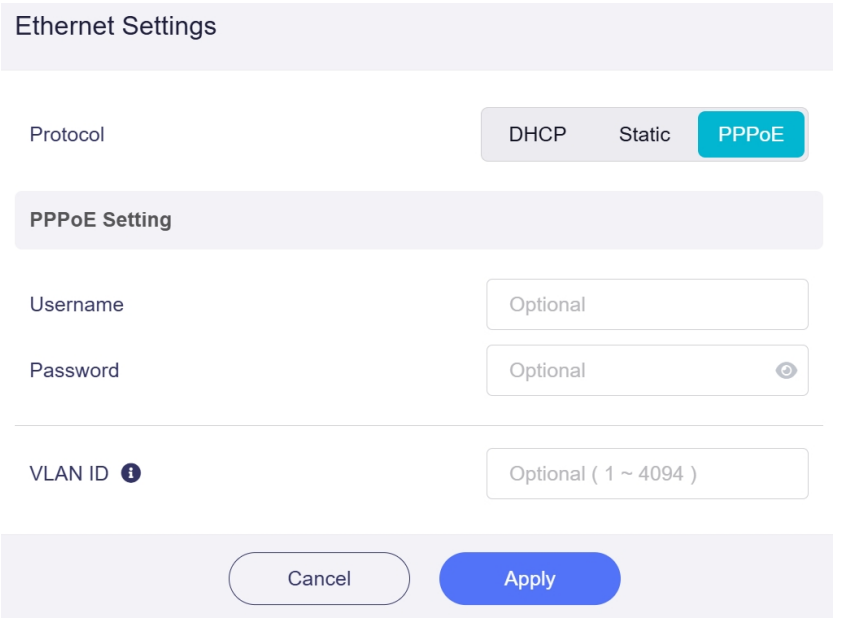
  Statyczny adres IP jest wymagany, gdy dostawca usług internetowych przydziela stały publiczny adres IP lub gdy parametry sieci (np. adres IP, bramę, maskę podsieci) trzeba skonfigurować ręcznie.



  Możesz skonfigurować **VLAN ID**, jeśli dostawca usług wymaga używania przez interfejs określonego identyfikatora tagowanej sieci VLAN.

- **PPPoE**

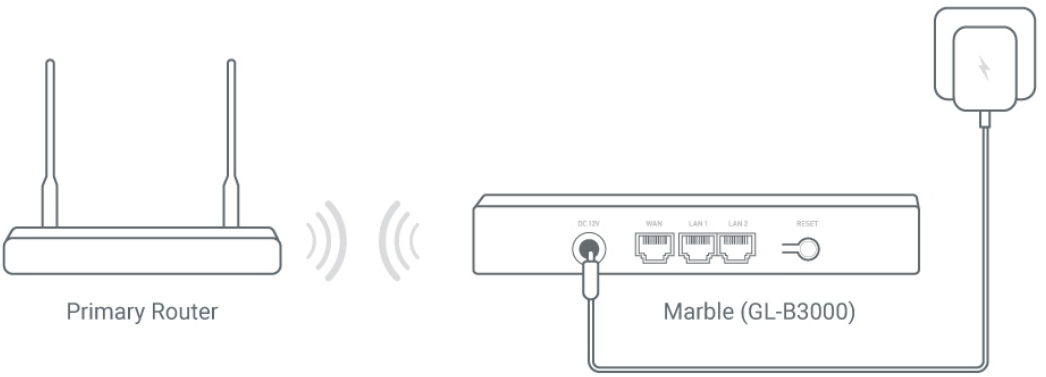
  PPPoE (Point-to-Point Protocol over Ethernet) to protokół sieciowy powszechnie stosowany przez dostawców Internetu. Dostawca zazwyczaj udostępnia modem oraz indywidualną nazwę użytkownika i hasło wymagane do skonfigurowania połączenia z Internetem.



Możesz skonfigurować **VLAN ID**, jeśli dostawca usług wymaga używania przez interfejs określonego identyfikatora tagowanej sieci VLAN.

4.2 Połączenie z Internetem przez istniejącą sieć Wi-Fi

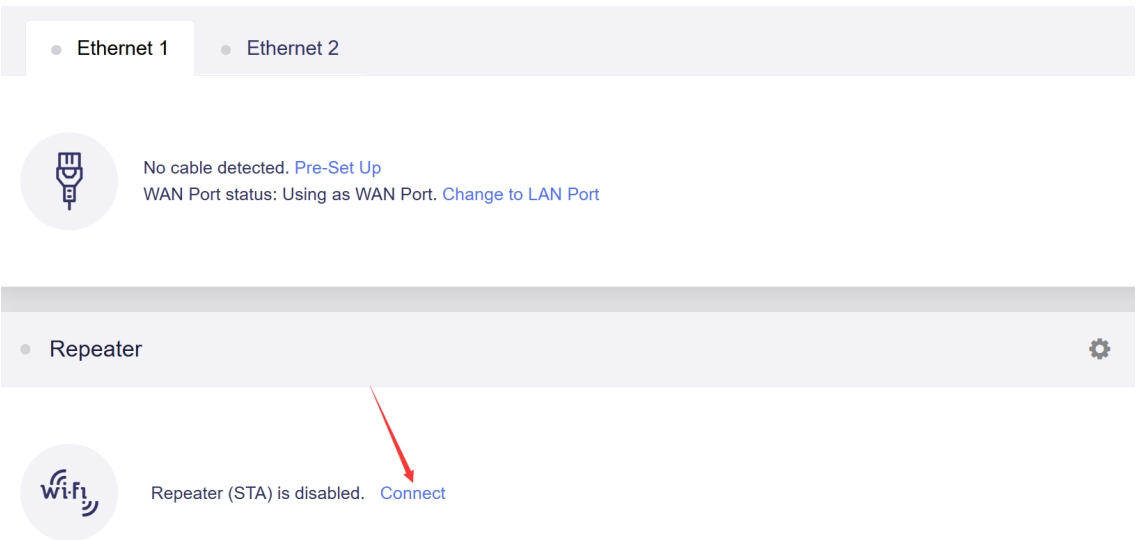
Podłącz router jako wzmacniacz do istniejącej sieci bezprzewodowej, aby wzmocnić sygnał Wi-Fi i utworzyć sieć lokalną odizolowaną od sieci głównej. W hotelach i kawiarniach oferujących bezpłatne publiczne hotspoty wzmacniacz zwiększa zasięg Wi-Fi, zapewnia przewodowy i bezprzewodowy dostęp wielu urządzeniom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



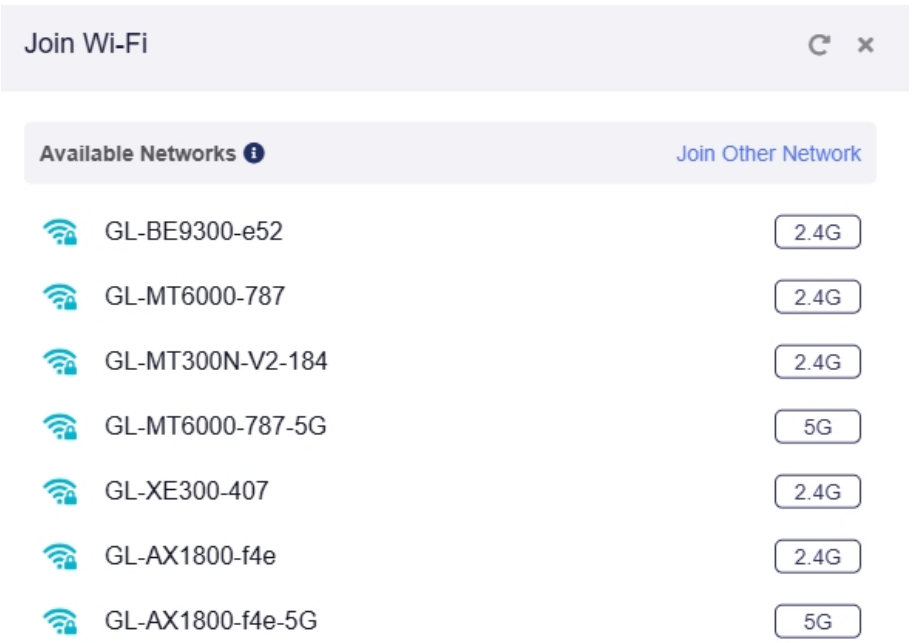
Funkcja wzmacniacza GL.iNet domyślnie działa w trybie WISP (Wireless Internet Service Provider). Oznacza to, że router tworzy własną podsieć i działa jako zapora, chroniąc przed zagrożeniami z sieci publicznej.

4.2.1 Podstawowa konfiguracja

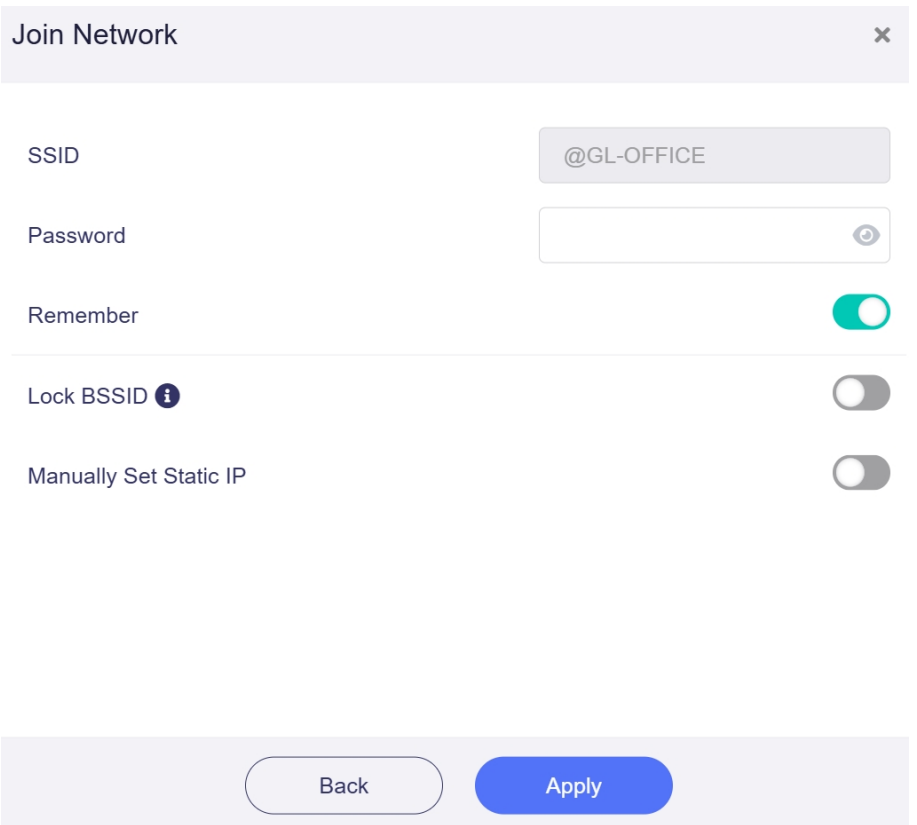
1. Zaloguj się do panelu administracyjnego routera i przejdź do **INTERNET** > **Repeater**. Kliknij **Connect**.



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

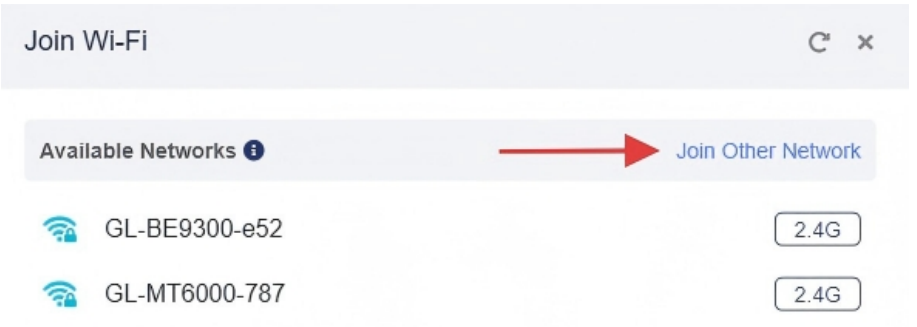


3. Wprowadź prawidłowe hasło Wi-Fi i kliknij **Apply**.

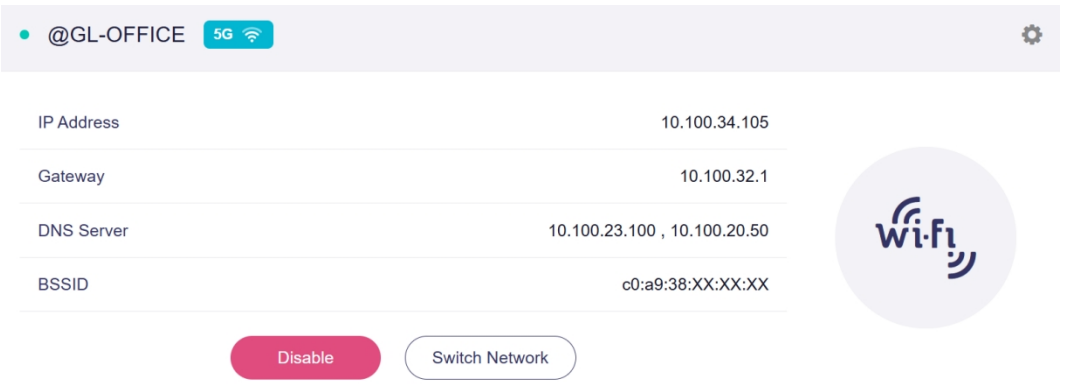


- **Remember**: włącz tę opcję, aby zapamiętać bieżącą sieć Wi-Fi, której sygnał jest wzmacniany.
- **Lock BSSID**: po włączeniu router będzie łączyć się wyłącznie z konkretnym punktem dostępu (AP) odpowiadającym wybranemu BSSID, nawet jeśli inne punkty dostępu mają taki sam identyfikator SSID.
- **Manually Set Static IP**: po włączeniu możesz ręcznie skonfigurować adres IP, maskę podsieci, bramę i serwery DNS zamiast uzyskiwać ustawienia IP automatycznie przez DHCP.

4. 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**.

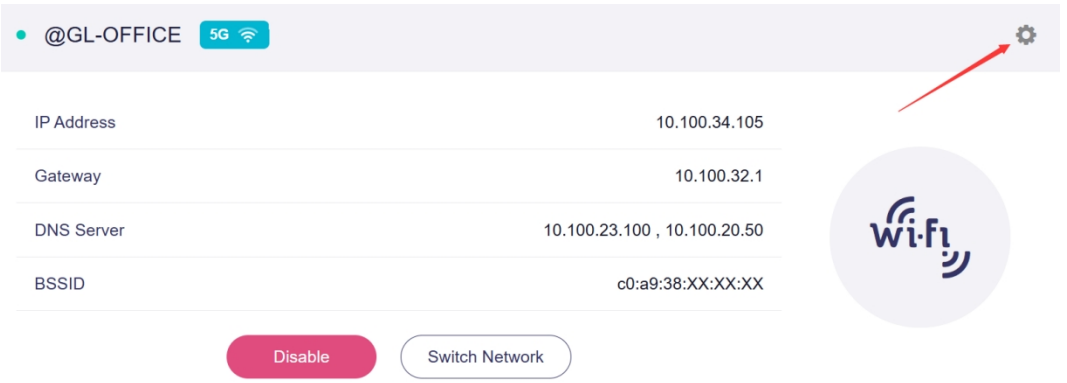


5. Poczekaj chwilę na połączenie routera. Po połączeniu strona będzie wyglądać jak poniżej.

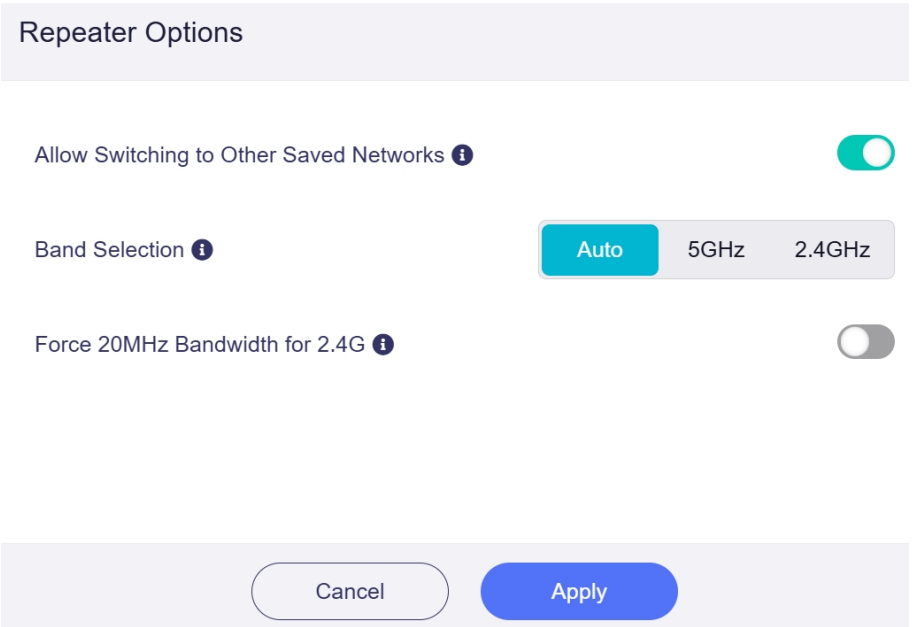


4.2.2 Opcje wzmacniacza sygnału

Kliknij ikonę koła zębatego w prawym górnym rogu, aby skonfigurować opcje wzmacniacza.



Wygląd strony może się różnić w zależności od wersji oprogramowania.



- **Allow Switching to Other Saved Networks**: po włączeniu tej opcji router automatycznie połączy się z innymi zapisanymi sieciami, gdy nie będzie mógł połączyć się z bieżącą siecią Wi-Fi.
- **Band Selection**: jeśli ręcznie wybierzesz pasmo, router nie będzie wyszukiwać sieci Wi-Fi w innym paśmie ani łączyć się z nimi.
- **Force 20MHz Bandwidth for 2.4G**: po włączeniu tej opcji urządzenie poprawia stabilność połączenia przez zmniejszenie prędkości transmisji.
  Uwaga: działa tylko podczas wzmacniania sygnału sieci Wi-Fi 2,4 GHz.

Rozdział 5

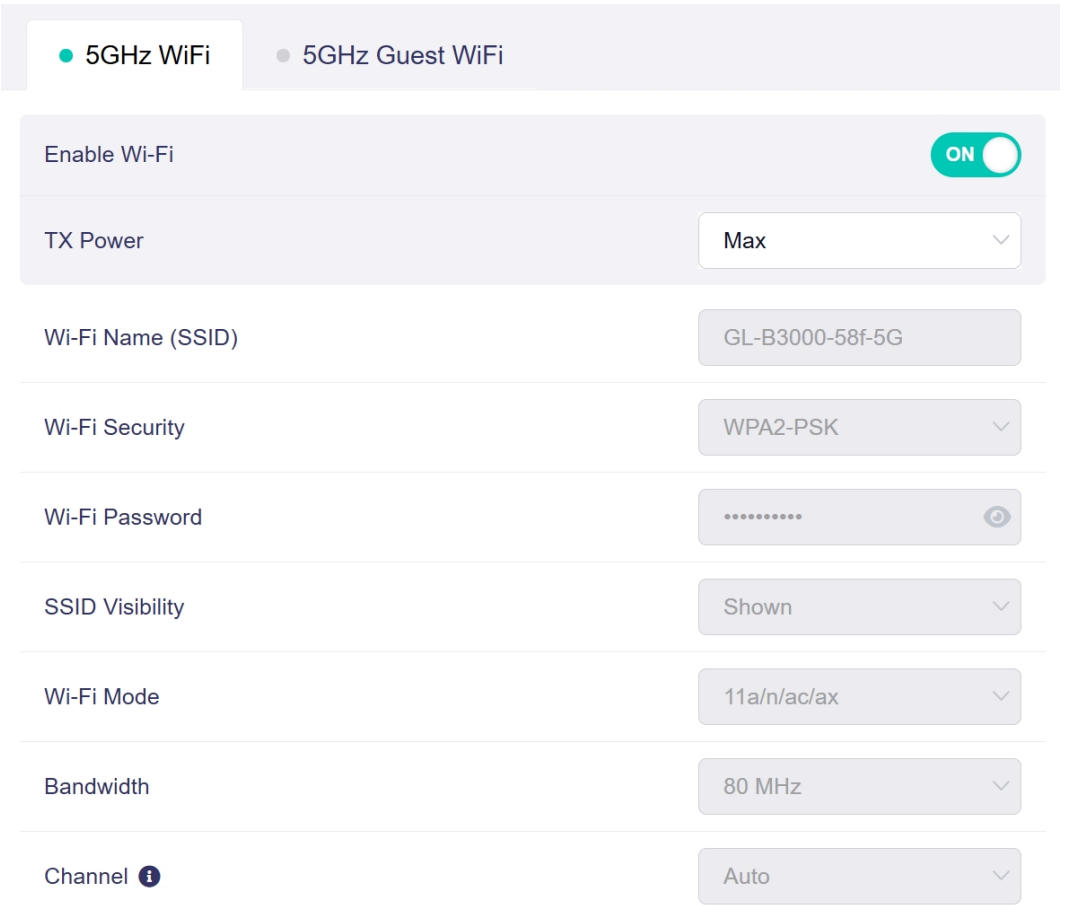
Sieć bezprzewodowa

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

Zaloguj się do panelu administracyjnego routera i przejdź do **WIRELESS**.
Strona ustawień bezprzewodowych wyświetla ustawienia Wi-Fi routera w pasmach 5 GHz i 2,4 GHz. Każde pasmo ma oddzielną sieć główną i gościnną, co zapewnia elastyczne zarządzanie.

5.1 Wi-Fi 5 GHz

W głównej sieci Wi-Fi 5 GHz można włączać i wyłączać Wi-Fi oraz ustawiać moc nadawania, nazwę sieci (SSID), zabezpieczenia, hasło, widoczność SSID, tryb, szerokość kanału i kanał.

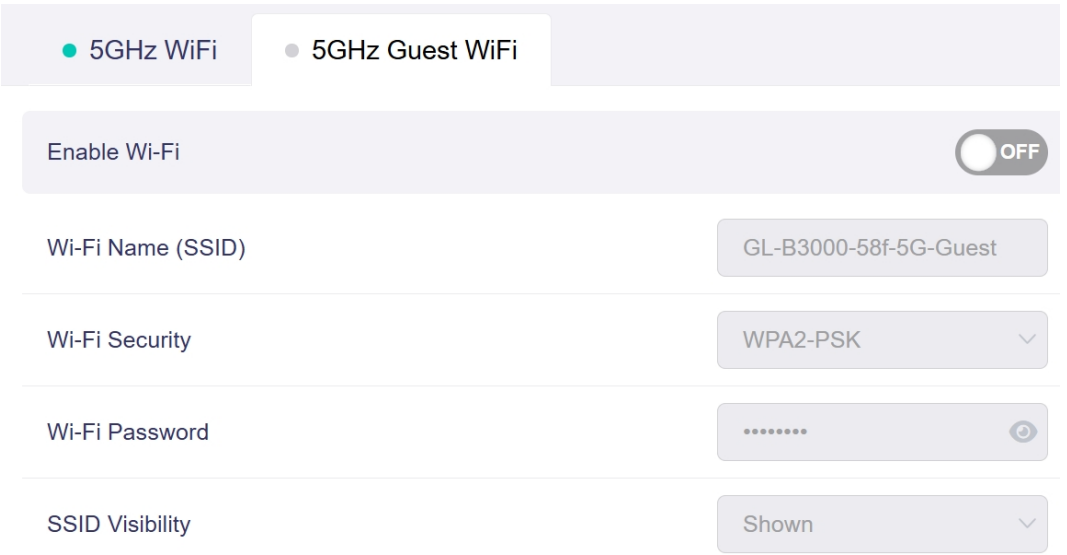


Uwaga:

1. Ustawień **Bandwidth** i **Channel** nie można zmieniać, gdy router działa jako wzmacniacz sygnału, ponieważ są one przejmowane z sieci, której sygnał jest wzmacniany.
2. Gdy opcja **Channel** jest ustawiona na **Auto**, sieć Wi-Fi routera nie przełącza się automatycznie na kanał DFS.

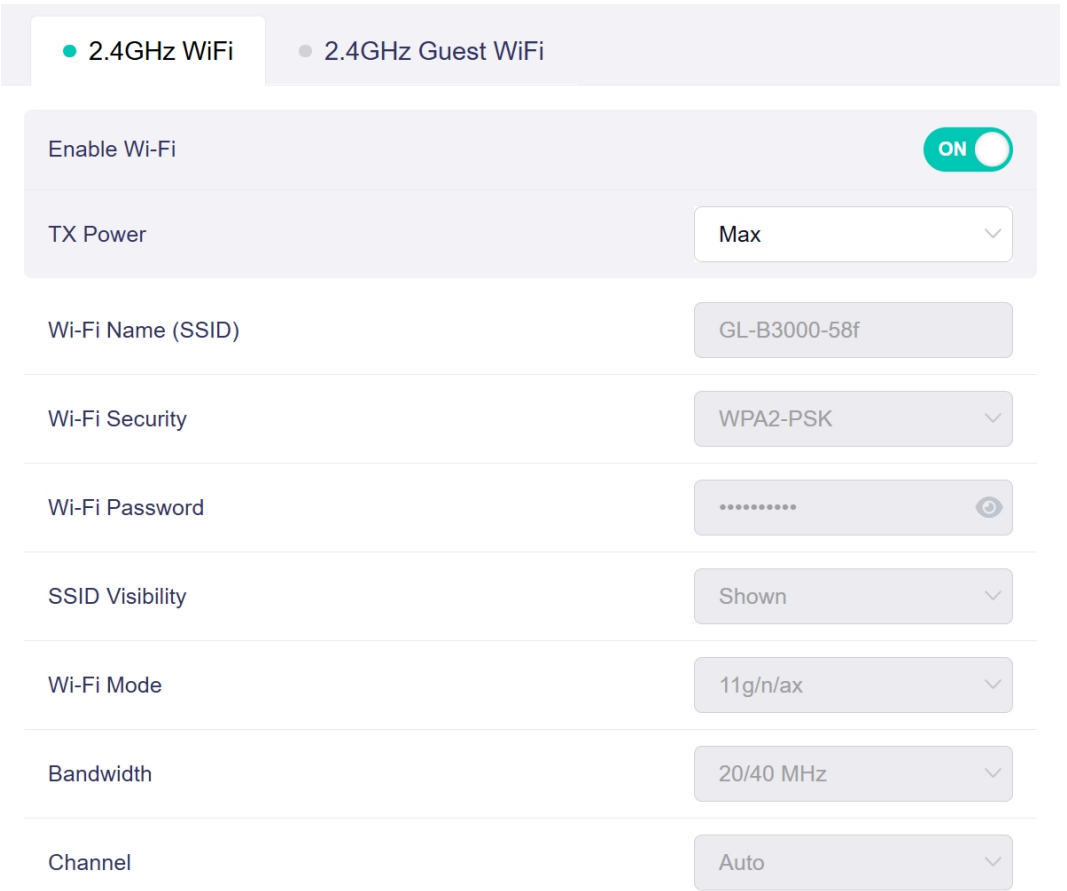
3. Gdy parametr **Bandwidth** jest ustawiony na **160 MHz** (opcja dostępna tylko w niektórych modelach), sieć Wi-Fi zawsze korzysta z kanału DFS, nawet jeśli wybierzesz kanał bez DFS lub ustawienie Auto.

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



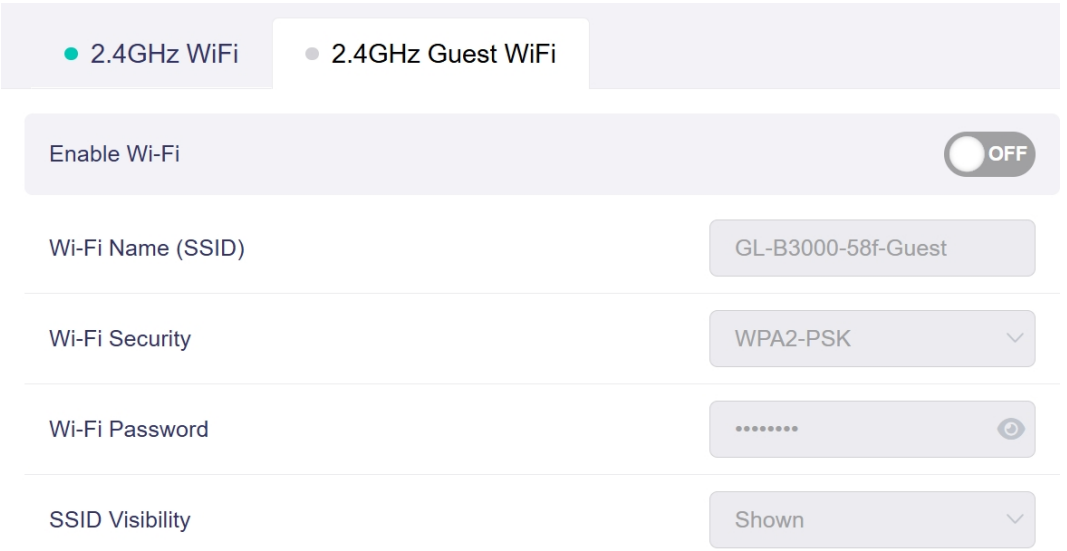
5.2 Wi-Fi 2,4 GHz

W głównej sieci Wi-Fi 2,4 GHz można włączać i wyłączać Wi-Fi oraz ustawiać moc nadawania, nazwę sieci (SSID), zabezpieczenia, hasło, widoczność SSID, tryb, szerokość kanału i kanał.



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

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


2.4GHz WiFi
2.4GHz Guest WiFi
Enable Wi-Fi
OFF
Wi-Fi Name (SSID)
GL-B3000-58f-Guest
Wi-Fi Security
WPA2-PSK
Wi-Fi Password
••••••••
SSID Visibility
Shown

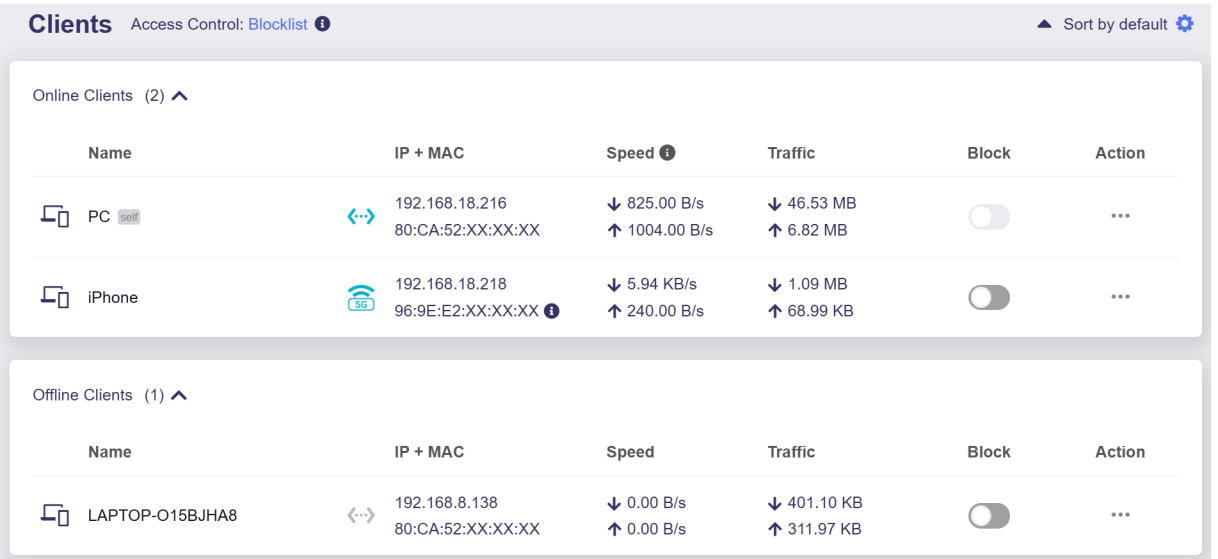
Rozdział 6

Urządzenia klienckie

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

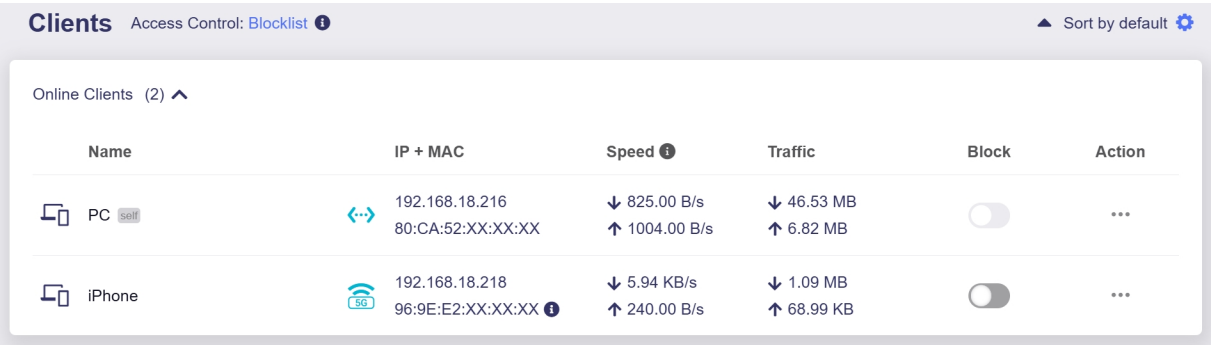
Zaloguj się do panelu administracyjnego routera i przejdź do **CLIENTS**.

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**

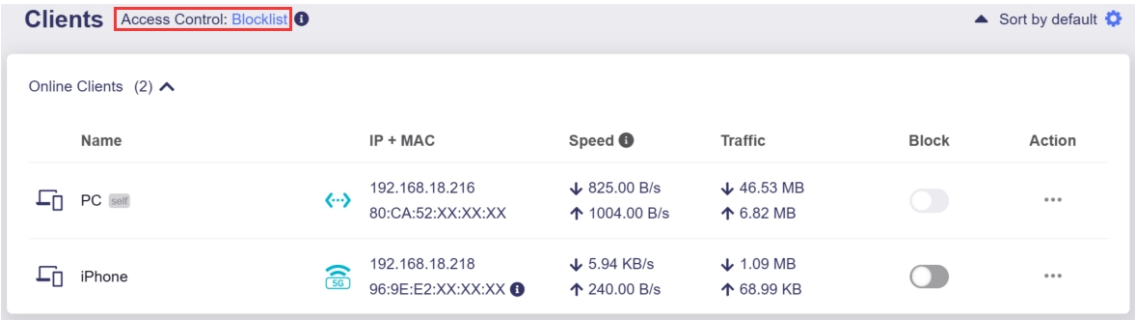
   Trzecia kolumna przedstawia prędkość połączenia internetowego podłączonego urządzenia. Jest to średnia z ostatnich 3 minut. System zaczyna obliczać średnią po otwarciu tej strony (np. jeśli strona jest otwarta od 10 sekund, średnia będzie oparta tylko na danych z tych 10 sekund).

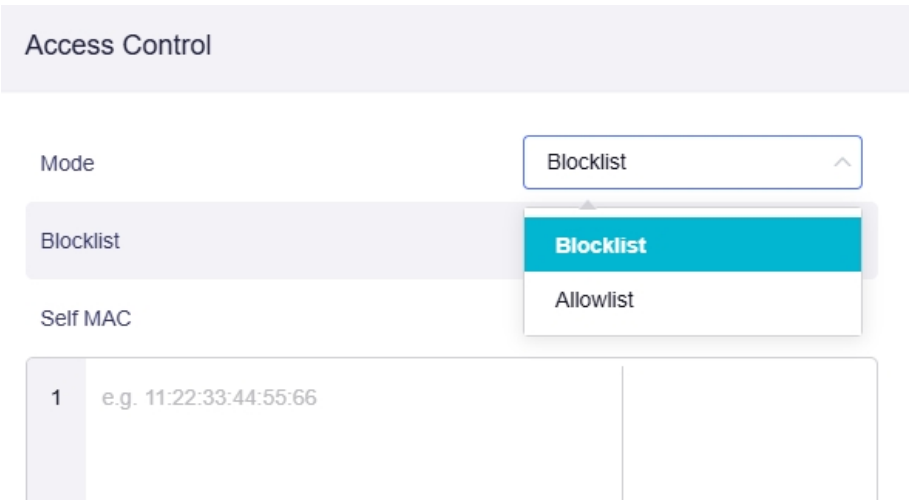
4. **Transfer danych**: czwarta kolumna przedstawia transfer internetowy podłączonego urządzenia.

5. **Lista blokowanych urządzeń**

   W piątej kolumnie możesz jednym kliknięciem zablokować wybrane podłączone urządzenie.

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



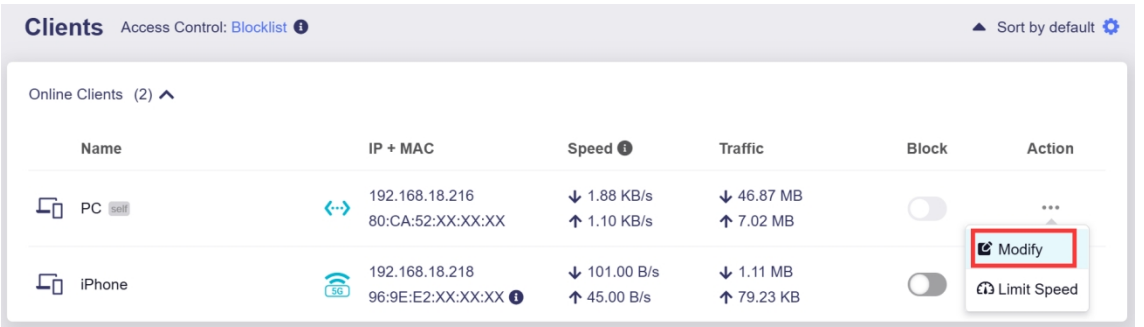


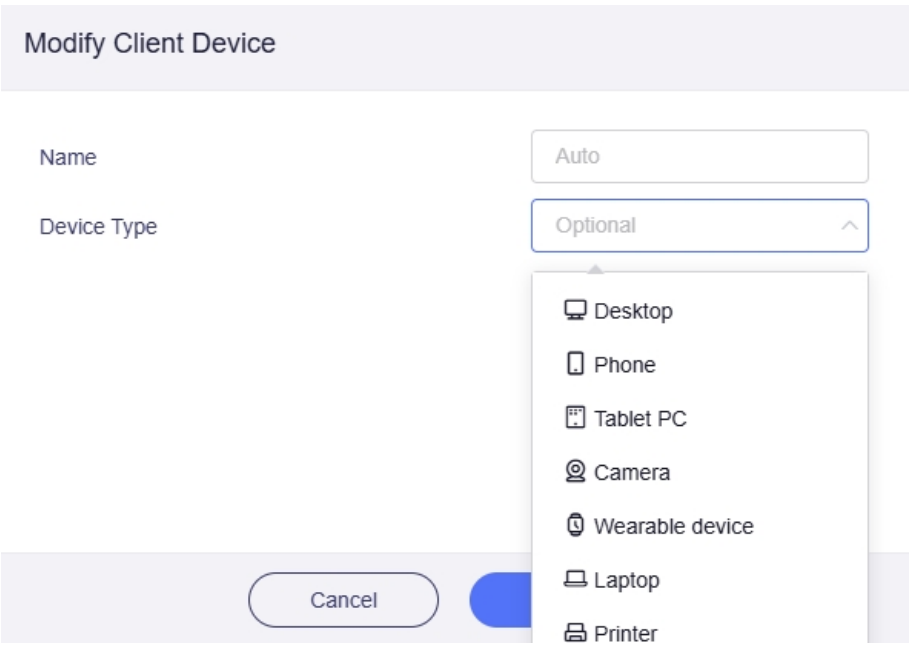
- **Blacklist**: urządzenia o adresach MAC znajdujących się na liście blokowanych nie mogą łączyć się z tym routerem. Blokowanie klienta opiera się na adresie MAC urządzenia. Jeśli zablokowane urządzenie następnym razem użyje innego adresu MAC, nadal będzie mogło połączyć się z routerem.
- **Allowlist**: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

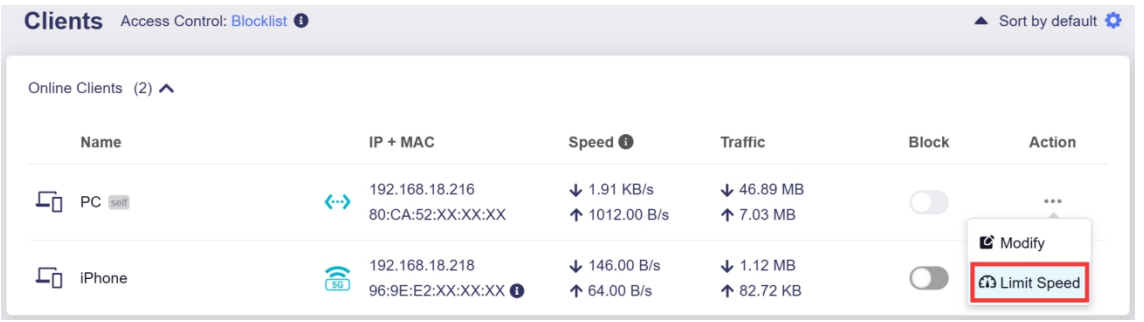
   Kliknij ikonę trzech kropek w kolumnie **Action**, a następnie wybierz **Modify** z menu, aby zmienić nazwę i typ urządzenia.



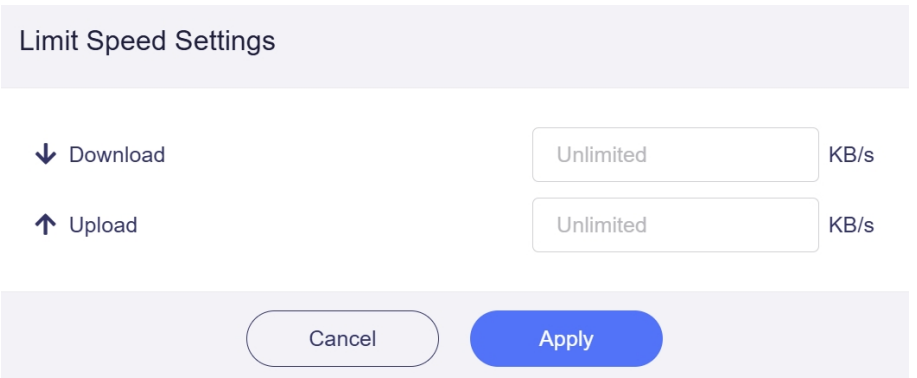


2. **Ograniczanie prędkości**

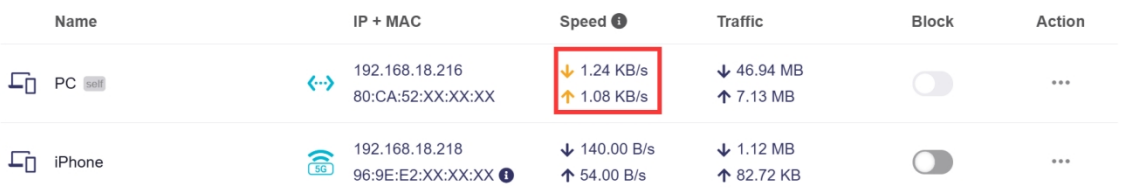
Kliknij ikonę trzech kropek w kolumnie **Action**, a następnie wybierz **Limit Speed** z menu.



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

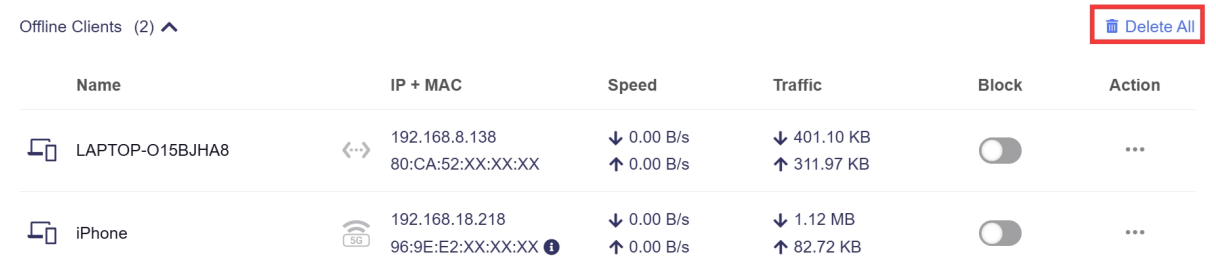


Jeśli dla urządzenia ustawiono ograniczenie prędkości, strzałki prędkości wysyłania i pobierania zmienią kolor na żółty.

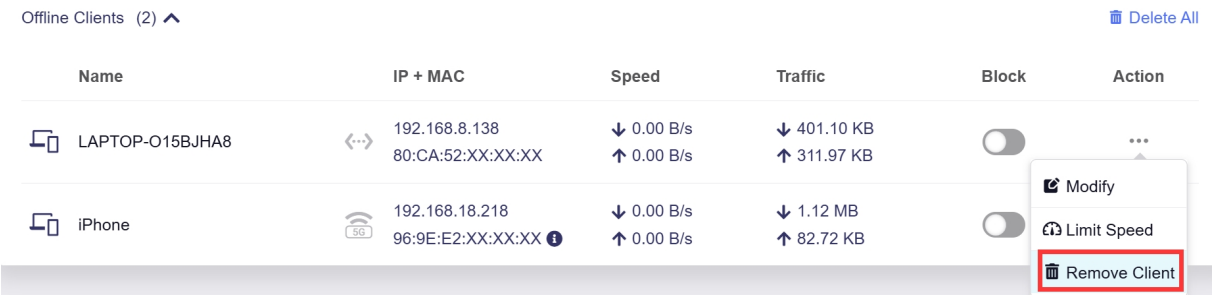


6.3 Usuwanie urządzeń klienckich

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

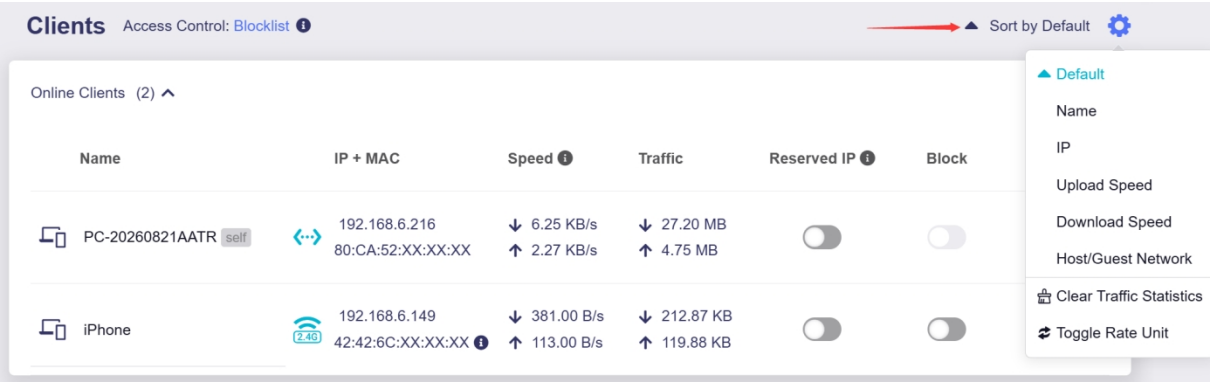


Aby usunąć określone urządzenie klienckie, kliknij ikonę trzech kropek w kolumnie **Action**, a następnie wybierz **Remove Client** z menu.



6.4 Sortowanie

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



Domyślna kolejność sortowania jest następująca:

- Urządzenie, z którego korzystasz do otwarcia panelu administracyjnego routera, zawsze znajduje się na początku listy.
- W sekcji **Online Clients** urządzenia, które połączyły się wcześniej, są wyświetlane wyżej.
- W sekcji **Offline Clients** urządzenia, które rozłączyły się wcześniej, są wyświetlane wyżej.

Oprócz reguł sortowania menu zawiera następujące funkcje:

- **Clear Traffic Statistics**: wyczyść statystyki transferu wszystkich podłączonych klientów jednym kliknięciem. Po zastosowaniu tej opcji wartości w kolumnie transferu zostaną wyzerowane, a zliczanie rozpocznie się od nowa.



- **Toggle Rate Unit**: przełącz jednostkę prędkości w kolumnie między **KB/s** a **Kbps**.

Rozdział 7

Poznaj VPN

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

7.1 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.

7.2 Przykłady zastosowań

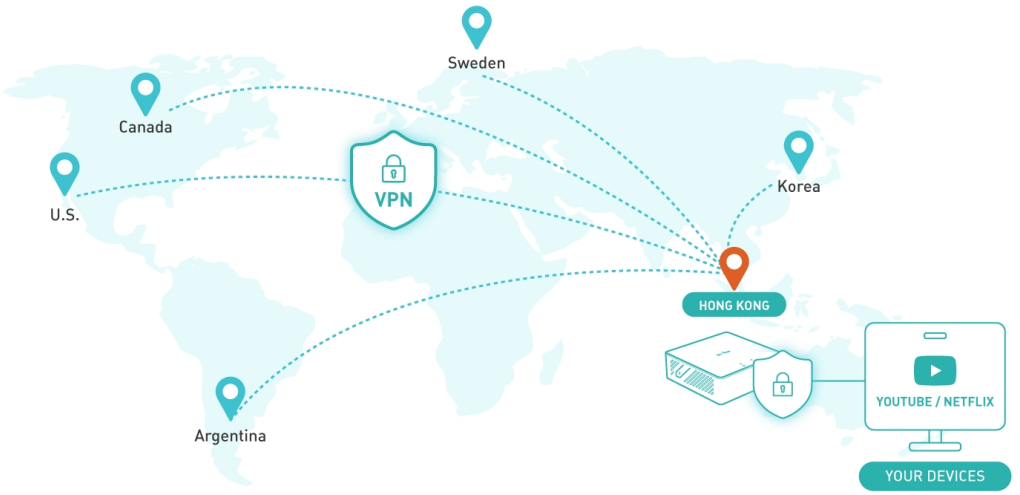
1. **Prywatność danych osobowych**

   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.



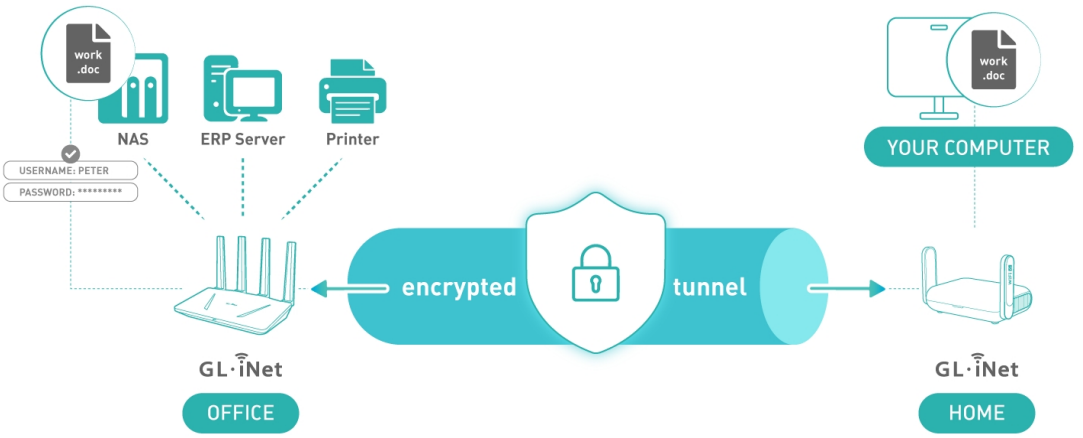
2. **Dostęp bez ograniczeń na całym świecie**

   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

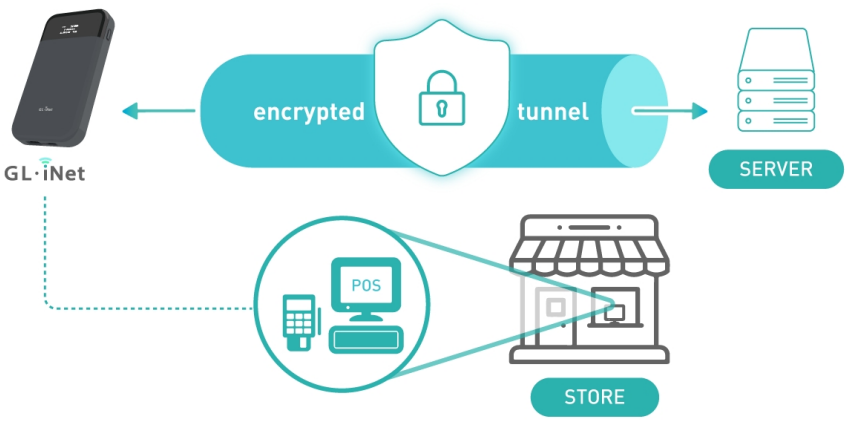
3. **Bezpieczeństwo danych małych firm**

Wiele osób pracuje w przestrzeniach coworkingowych lub kawiarniach, korzystając z bezpłatnego publicznego Wi-Fi. Takie sieci są podatne na ataki cyberprzestępców. Skonfigurowanie routera podróżnego jako klienta VPN pozwala bezpiecznie pracować z dowolnego miejsca.



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 8

Panel VPN

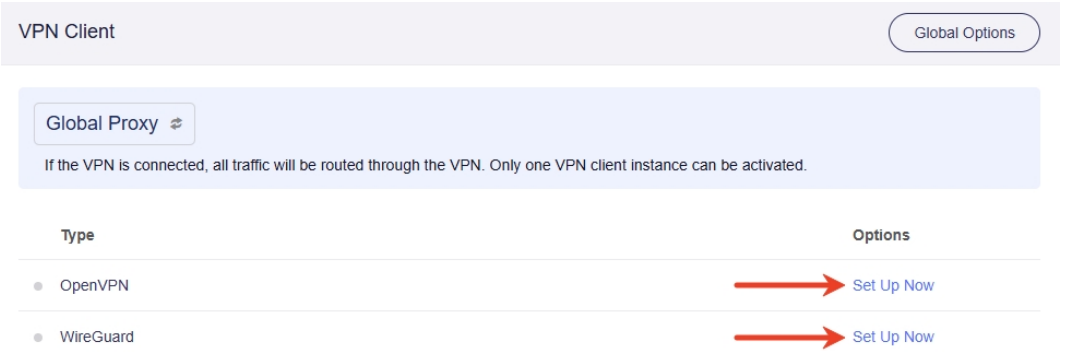
W tym rozdziale opisano zarządzanie połączeniami VPN w panelu administracyjnym.

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

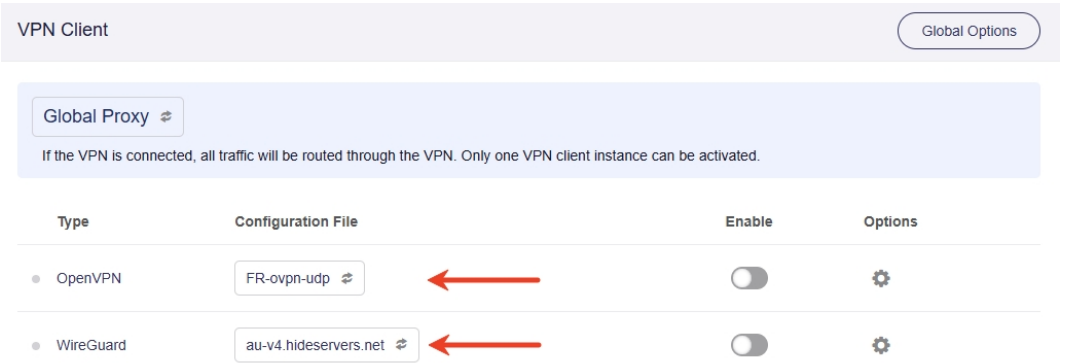
Gdy router działa jako aktywny klient VPN, panel VPN wyświetla szczegóły połączenia, takie jak adres serwera, statystyki transferu, wirtualny adres IP klienta i dziennik połączenia. Umożliwia też konfigurację ustawień zaawansowanych, takich jak Block non-VPN traffic, Allow Access WAN i Services from GL.iNet Use VPN.

8.1 Klient VPN

Po pierwszym otwarciu **VPN Dashboard**, gdy nie ma plików konfiguracyjnych OpenVPN ani WireGuard, strona wygląda jak poniżej. Kliknij **Set Up Now**, aby przejść do strony **OpenVPN Client** lub **WireGuard Client** i przesłać pliki konfiguracyjne VPN.

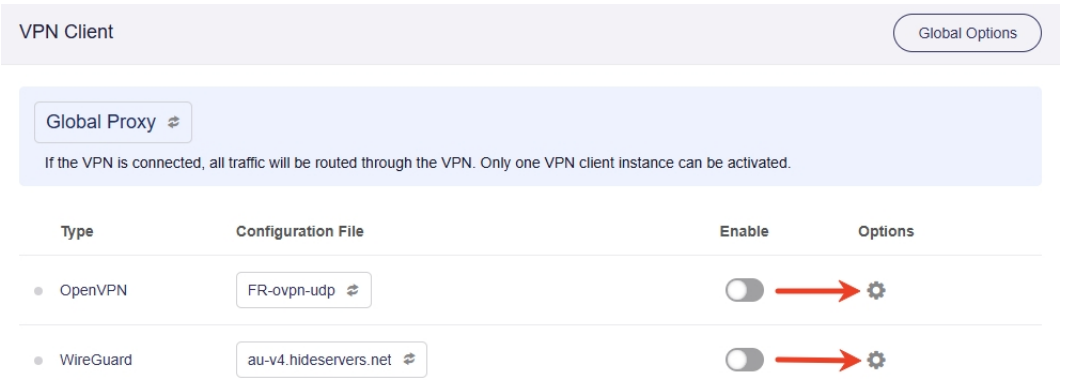


Po przesłaniu konfiguracja pojawi się w kolumnie **Configuration File**. Jeśli przesłano kilka plików konfiguracyjnych, możesz je przełączać, klikając pole wyboru.

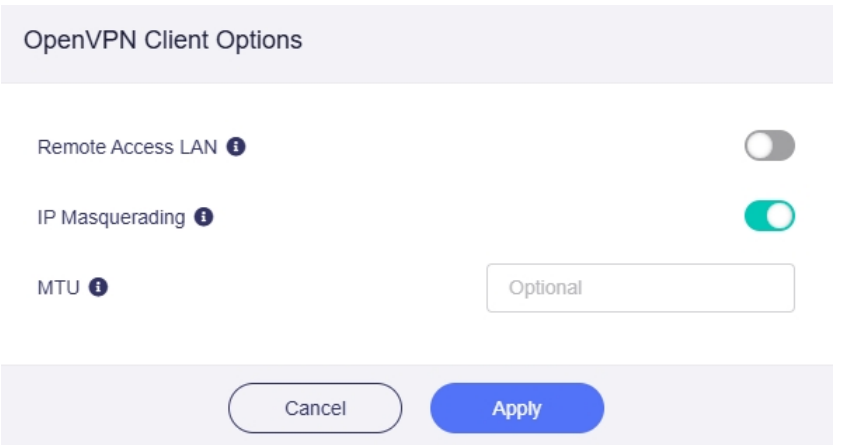


8.1.1 Opcje klienta

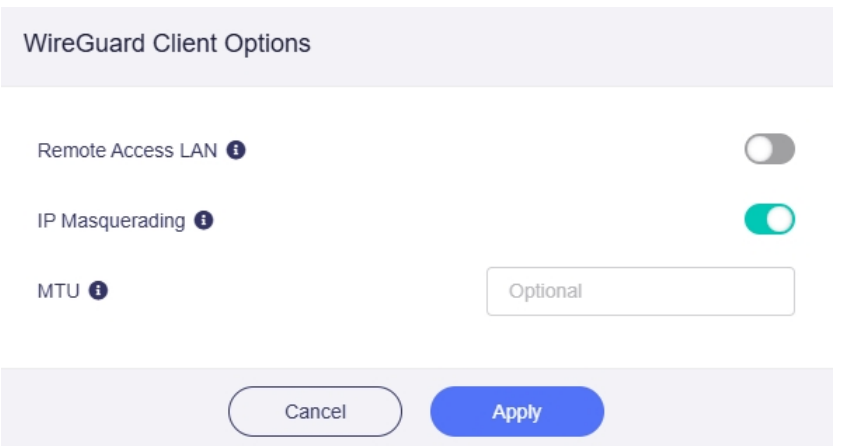
Kliknij ikonę koła zębatego po prawej stronie, aby otworzyć opcje klienta OpenVPN lub WireGuard.



Opcje klienta OpenVPN przedstawiono poniżej.

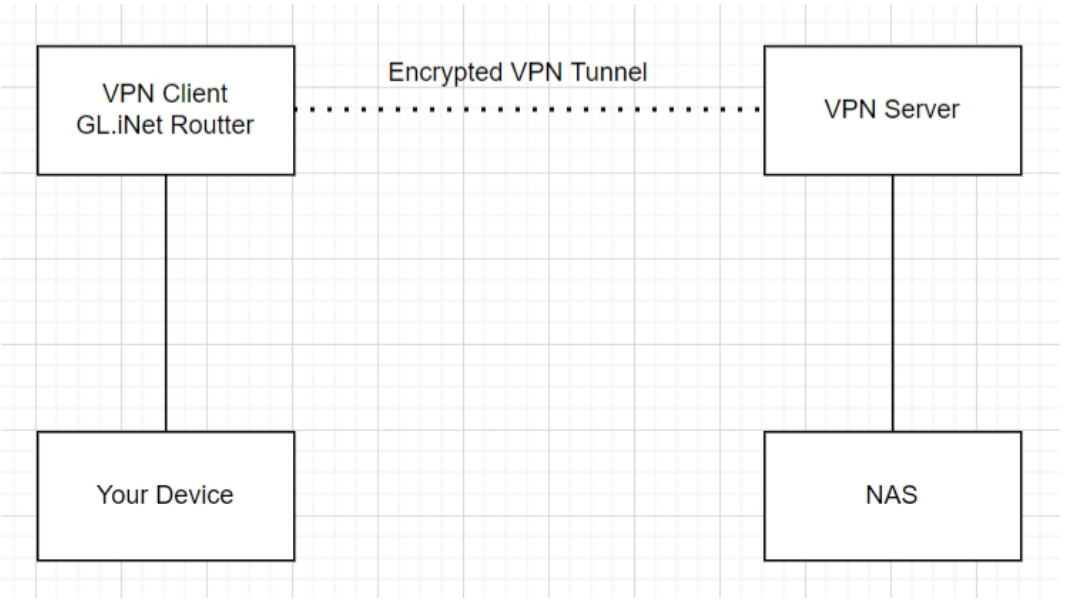


Opcje klienta WireGuard przedstawiono poniżej.



- **Remote Access LAN**: po włączeniu dozwolony jest zdalny dostęp przez VPN do routera i urządzeń w jego sieci LAN. Serwer VPN musi rozgłaszać trasę do podsieci LAN tego routera.

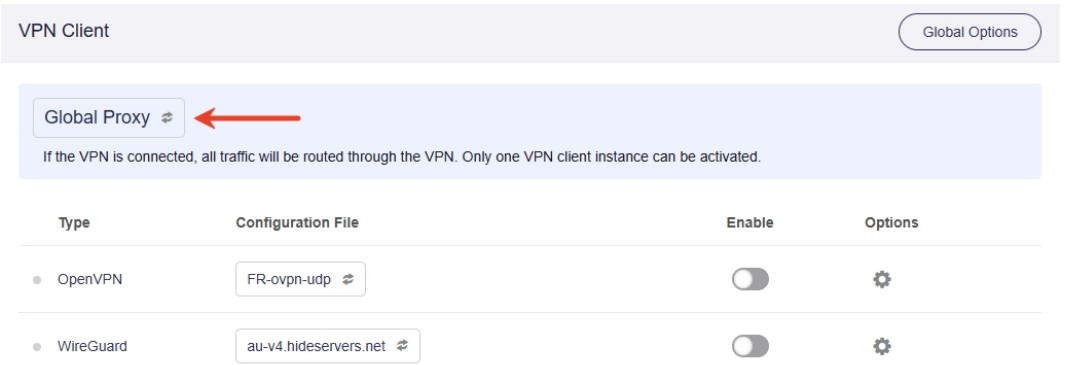
  Na przykład na poniższym schemacie router GL.iNet działa jako klient VPN i łączy się z serwerem VPN przez tunel VPN. Po włączeniu tej opcji urządzenia po stronie serwera VPN (np. NAS) mogą uzyskiwać dostęp zarówno do routera GL.iNet, jak i do urządzeń w jego sieci LAN. Wymaga to dodania na serwerze VPN reguły routingu do podsieci LAN routera GL.iNet.



- **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**: skrót od Maximum Transmission Unit, czyli maksymalnej jednostki transmisji. To opcjonalne ustawienie umożliwia zmianę MTU tunelu VPN i zastępuje wartość określoną w pliku konfiguracyjnym.

8.1.2 Tryb reguł

Domyślnym trybem proxy połączenia VPN jest **Global Proxy**. Aby wybrać inny tryb, kliknij pole w prawym górnym rogu.



Dostępne są trzy tryby proxy: Global Proxy, Policy Mode i Route Mode.

1. **Globalne proxy (Global Proxy)**

   W tym trybie cały ruch jest kierowany przez VPN. Można uruchomić tylko jedną instancję klienta VPN.

2. **Tryb reguł (Policy Mode)**

   Ten tryb obejmuje trzy rodzaje reguł.

   - **Na podstawie domeny docelowej lub adresu IP**

     W tym trybie przez VPN kierowany jest tylko ruch do określonych witryn, identyfikowanych na podstawie adresu IP lub nazwy domeny. Można uruchomić tylko jedną instancję klienta VPN.

   - **Na podstawie urządzenia klienckiego**

     W tym trybie przez VPN kierowany jest tylko ruch określonych urządzeń LAN, identyfikowanych na podstawie adresów MAC. Można uruchomić tylko jedną instancję klienta VPN.

   - **Na podstawie sieci VLAN**

     W tym trybie przez VPN kierowany jest tylko ruch określonej sieci VLAN. Można uruchomić tylko jedną instancję klienta VPN.

3. **Tryb routingu (Route Mode)**

   - **Wykrywanie automatyczne (Auto Detect)**

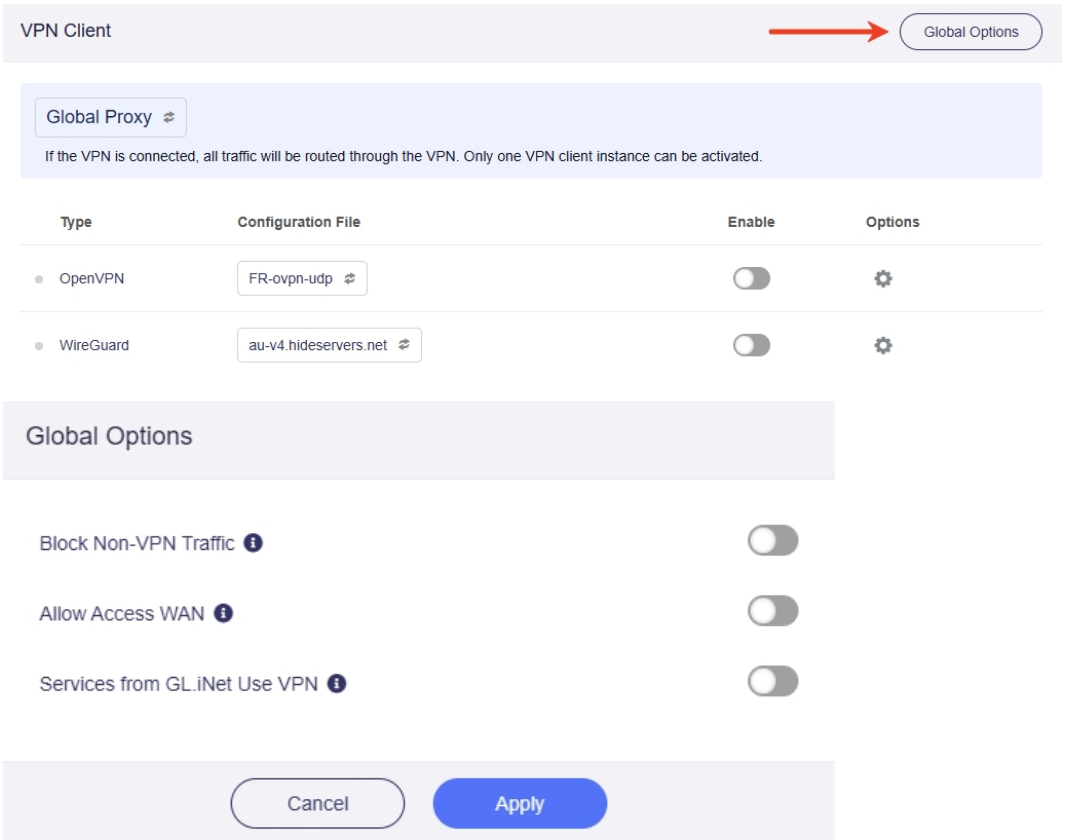
     Używane są reguły routingu określone w pliku konfiguracyjnym każdego klienta VPN lub przekazane przez serwer VPN.

   - **Niestandardowe reguły routingu**

     Możesz ręcznie skonfigurować reguły routingu dla każdej instancji klienta VPN.

8.1.3 Opcje globalne

Kliknij **Global Options** w prawym górnym rogu, aby skonfigurować zaawansowane ustawienia klienta VPN.



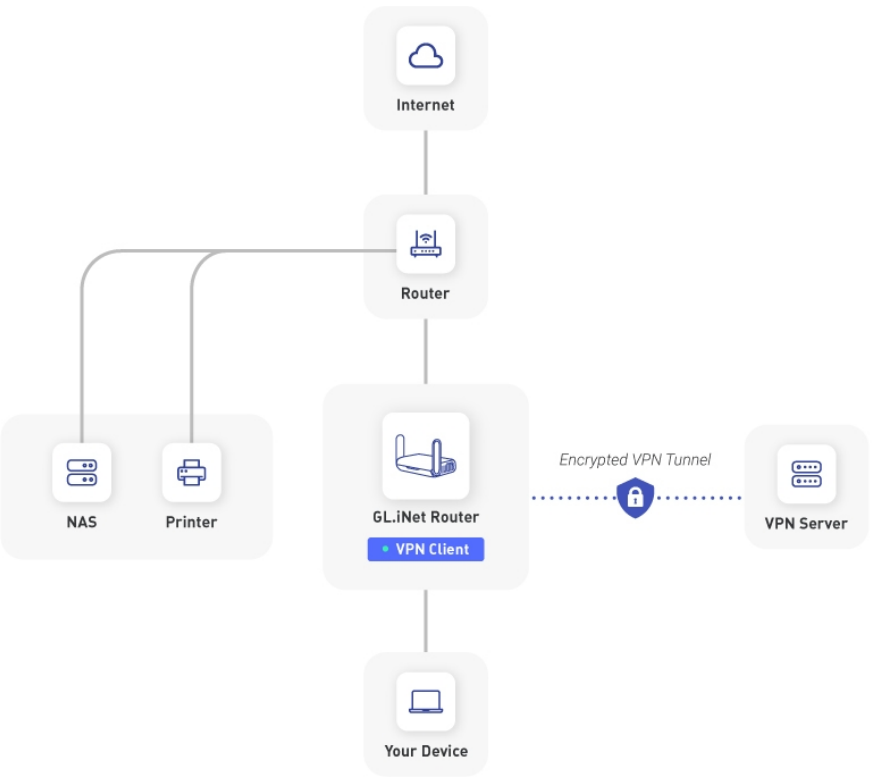
- **Block Non-VPN Traffic**: po włączeniu cały ruch internetowy musi przechodzić wyłącznie przez tunel VPN i nie może być kierowany przez inne interfejsy, np. WAN lokalnego dostawcy Internetu. Jeśli połączenie VPN niespodziewanie zostanie przerwane, cały ruch internetowy zostanie zablokowany, aby zapobiec przełączeniu na zwykłe połączenie WAN. Zapobiega to wyciekom poza VPN wynikającym z awarii VPN, nieprawidłowych ustawień DNS klienta i podobnych problemów.

  Ta funkcja jest również znana jako VPN Kill Switch. Chroni dane użytkownika przed ujawnieniem w Internecie. Typowy Kill Switch automatycznie odcina dostęp do Internetu po awarii połączenia VPN. Funkcja Block Non-VPN Traffic w routerach GL.iNet zapewnia szerszą ochronę przed wyciekami, obejmując następujące sytuacje:

  a. Wyciek DNS
  b. Wyciek IPv6
  c. Wyciek WebRTC

d. Zerwanie połączenia VPN
e. Uruchomienie aplikacji przed nawiązaniem połączenia VPN
f. Wycieki ruchu poszczególnych aplikacji

- **Allow Access WAN**: po włączeniu lokalne urządzenia klienckie nadal mogą uzyskiwać dostęp do usług po stronie WAN (np. drukarek, serwerów NAS i innych urządzeń w podsieci nadrzędnej), gdy VPN jest aktywny.



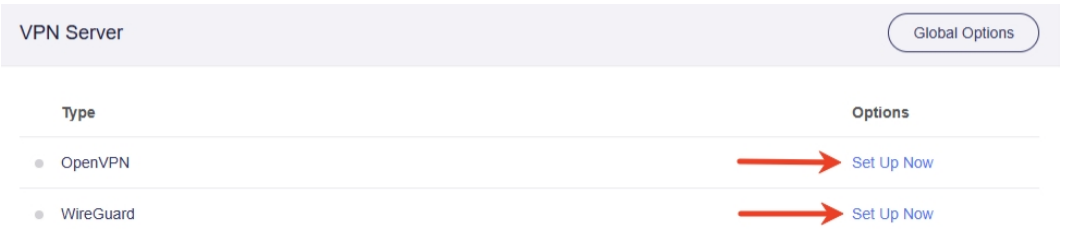
Jak pokazano na powyższym schemacie, włączenie tej funkcji pozwala urządzeniom lokalnym uzyskiwać dostęp do hostów w podsieci nadrzędnej, np. drukarek i serwerów NAS.

Ta opcja służy przede wszystkim zapewnieniu klientom dostępu do urządzeń w podsieci nadrzędnej. Router nie potrafi jednak odróżnić ruchu do tej podsieci od zwykłego ruchu internetowego. Jeśli urządzenia klienckie uzyskują dostęp do zasobów bezpośrednio przez publiczne adresy IP, istnieje ryzyko wycieku ruchu. Z tego powodu opcje **Allow Access WAN** i **Block Non-VPN Traffic** wzajemnie się wykluczają i nie można ich włączyć jednocześnie.

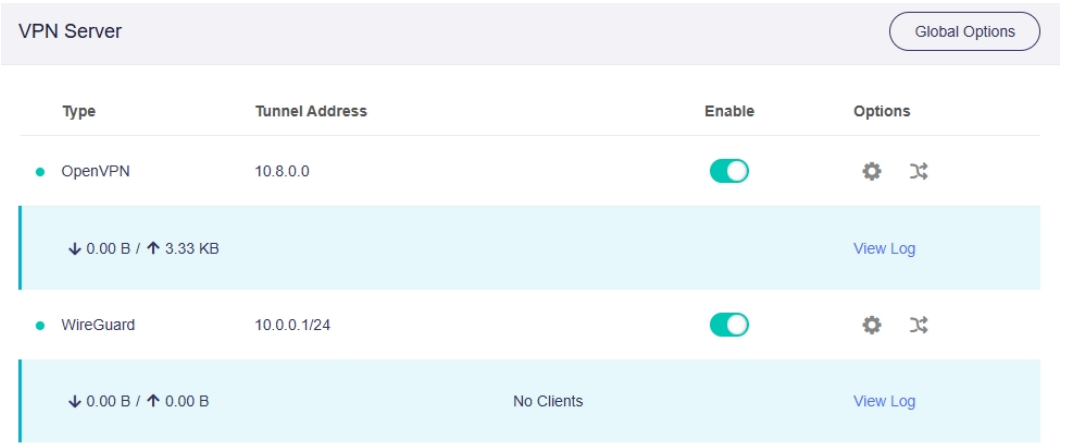
- **Services From GL.iNet Use VPN**: po włączeniu usługi GoodCloud, DDNS i rtty przesyłają pakiety przez tunele VPN. Ta opcja jest domyślnie wyłączona, ponieważ usługi te zwykle wymagają rzeczywistego adresu IP urządzenia do prawidłowego działania.

8.2 Serwer VPN

Jeśli router nie był jeszcze skonfigurowany jako serwer OpenVPN lub WireGuard, strona wygląda jak poniżej. Kliknij **Set Up Now**, aby przejść do strony **OpenVPN Server** lub **WireGuard Server** i zainicjować serwer VPN.

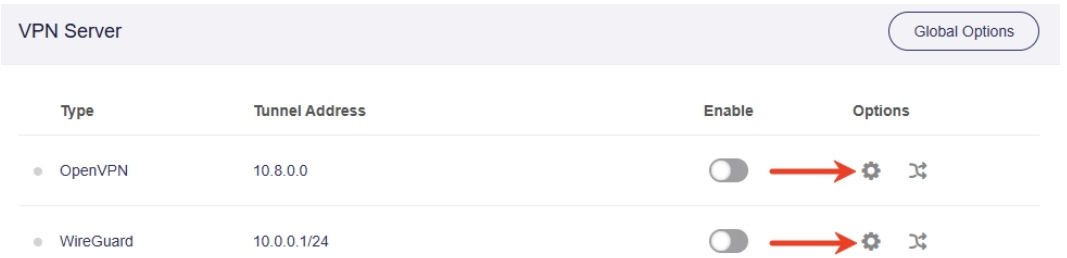


Po włączeniu serwera OpenVPN lub WireGuard na stronie pojawi się jego stan, jak pokazano poniżej.

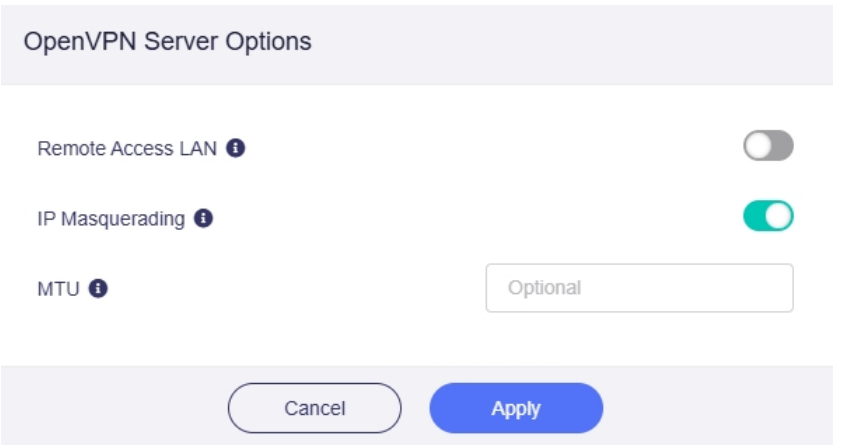


8.2.1 Opcje serwera

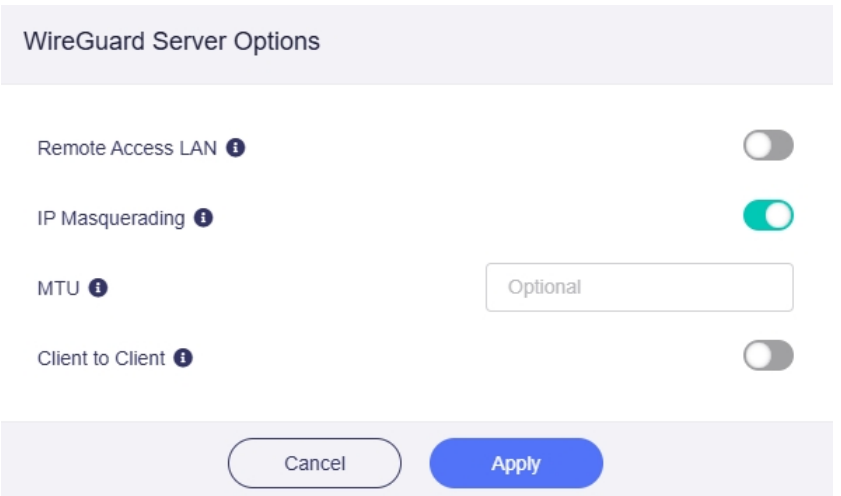
Kliknij ikonę koła zębatego po prawej stronie, aby otworzyć opcje serwera OpenVPN lub WireGuard.



Opcje serwera OpenVPN przedstawiono poniżej.



Opcje serwera WireGuard przedstawiono poniżej.

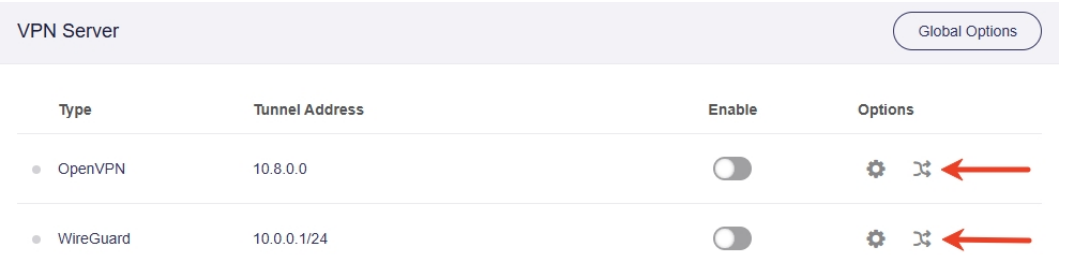


- **Remote Access LAN**: po włączeniu zasoby w podsieci LAN serwera są dostępne przez tunel VPN.

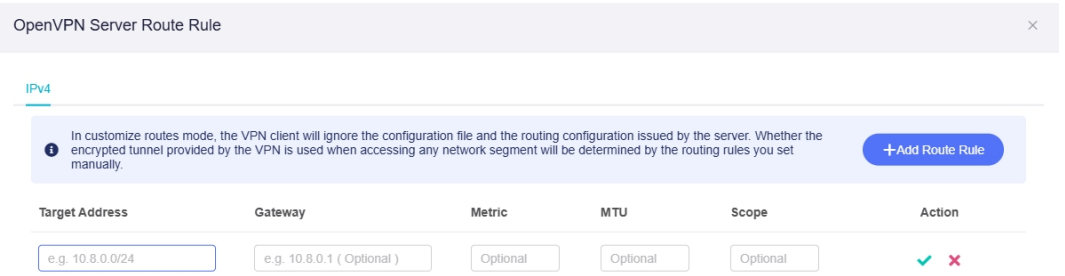
- **IP Masquerading**: po włączeniu źródłowe adresy IP klientów LAN są zastępowane adresem IP tunelu VPN routera. Wyłączaj tę opcję tylko w konfiguracjach sieć–sieć, w których zdalny węzeł zna Twoje podsieci LAN.
- **MTU**: skrót od Maximum Transmission Unit, czyli maksymalnej jednostki transmisji. Wartość MTU ustawiona dla tunelu zastępuje ustawienia MTU w pliku konfiguracyjnym.
- **Client to Client**: po włączeniu klienci VPN podłączeni do tego serwera mogą uzyskiwać wzajemny dostęp przez adresy IP swoich tuneli VPN. Aby umożliwić klientom dostęp również do ich podsieci LAN, trzeba dodać na serwerze VPN reguły routingu rozgłaszające te zdalne podsieci LAN.

8.2.2 Reguły tras serwera

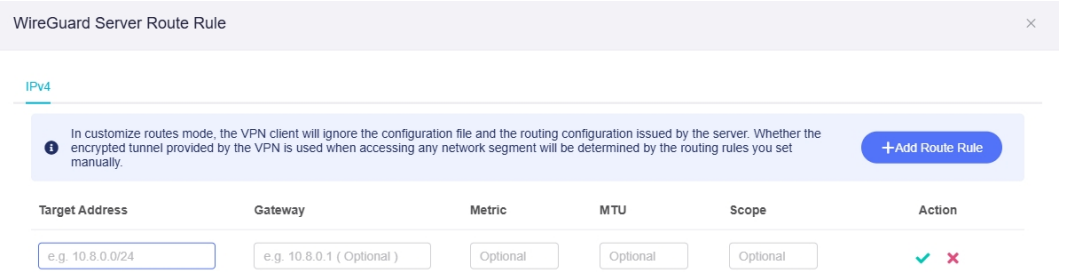
Kliknij ikonę trasy po prawej stronie, aby dostosować reguły tras OpenVPN lub WireGuard do swoich potrzeb.



Reguły tras serwera OpenVPN przedstawiono poniżej. Kliknij **Add Route Rule**, wprowadź **Target Address** i **Gateway**, a następnie kliknij zieloną ikonę zaznaczenia, aby zastosować ustawienia.



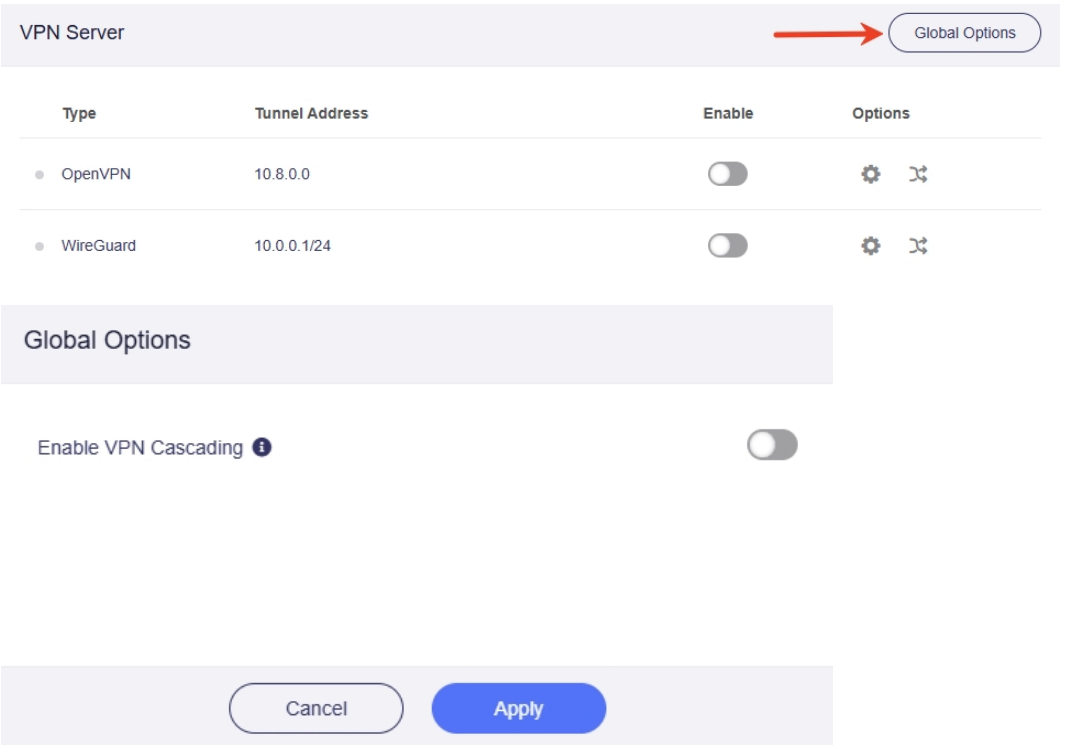
Reguły tras serwera WireGuard przedstawiono poniżej. Kliknij **Add Route Rule**, wprowadź **Target Address** i **Gateway**, a następnie kliknij zieloną ikonę zaznaczenia, aby zastosować ustawienia.



Uwaga: w trybie niestandardowych tras klient VPN ignoruje plik konfiguracyjny i konfigurację routingu przekazaną przez serwer. O tym, czy dostęp do danego segmentu sieci odbywa się przez zaszyfrowany tunel VPN, decydują ręcznie ustawione reguły routingu.

8.2.3 Opcje globalne

Kliknij **Global Options** w prawym górnym rogu, aby skonfigurować zaawansowane ustawienia serwera VPN.



Jeśli **VPN Cascading** jest włączone, a router jednocześnie działa jako serwer i klient VPN, ruch zdalnych klientów podłączonych do serwera VPN tego routera jest kierowany przez nadrzędny tunel VPN, z którego router korzysta jako klient VPN. Dowiedz się więcej o kaskadowaniu VPN.

Rozdział 9

Konfiguracja serwera VPN

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

9.1 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.

9.1.1 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:

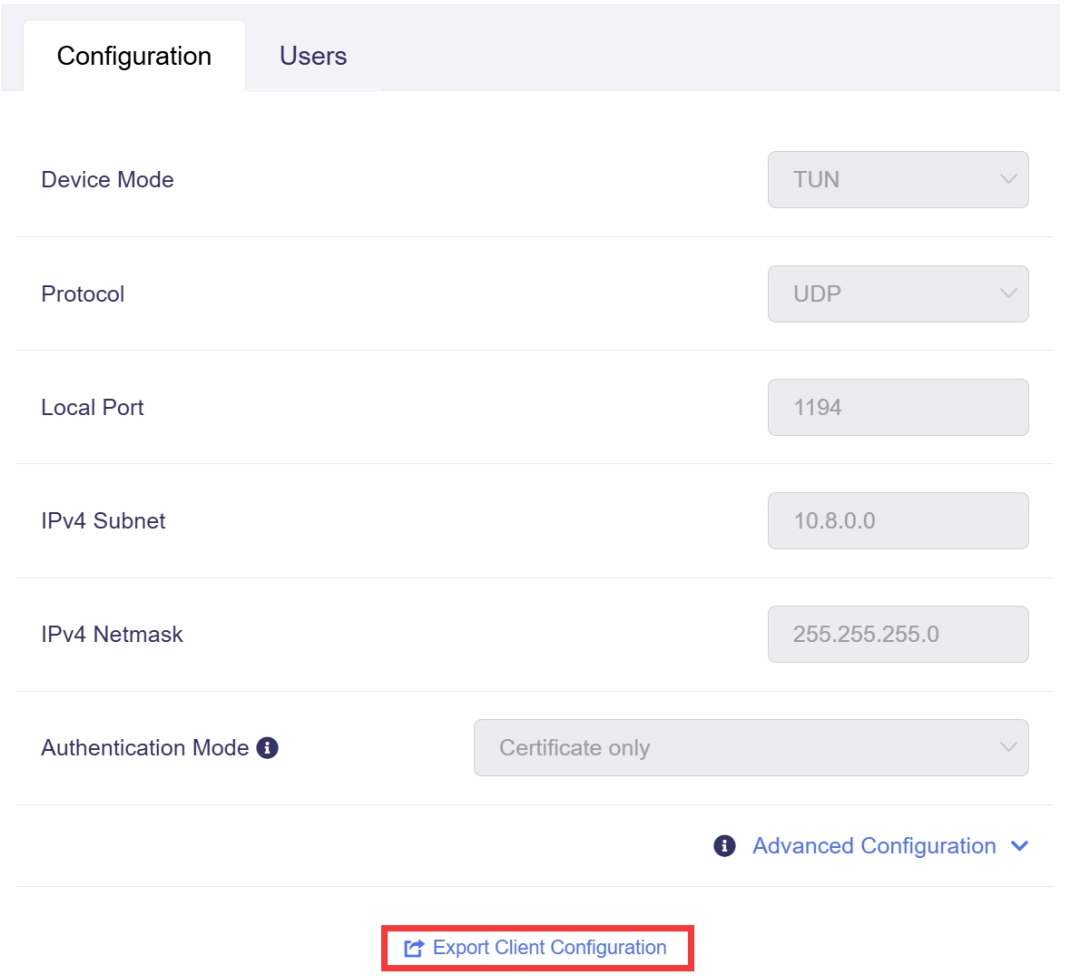
   - Jeśli przed routerem GL.iNet znajduje się główny router, zaloguj się do niego i sprawdź, czy ma publiczny adres IP przydzielony przez dostawcę Internetu.
   - Poproś dostawcę Internetu o publiczny adres IP. Może to wiązać się z dodatkową opłatą.

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.

9.1.2 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**.

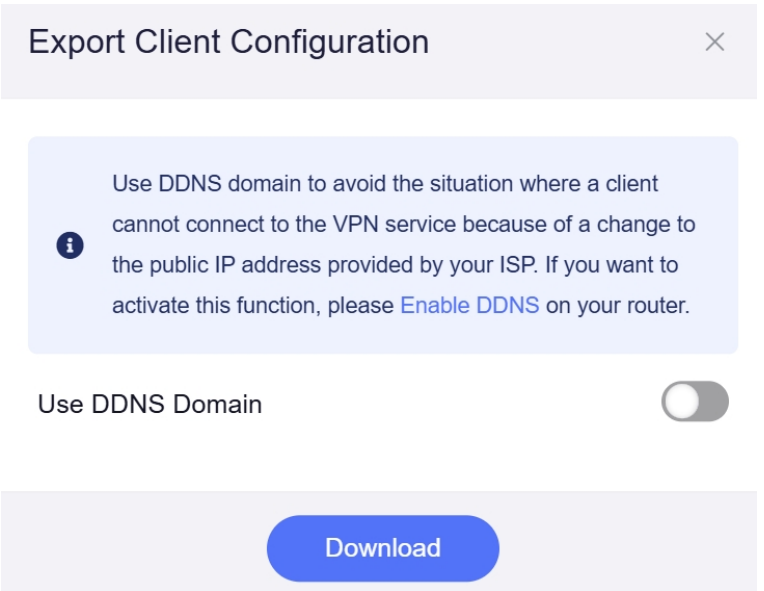


- **Device Mode**: TAP-S2S lub Tun. Różnice opisano tutaj.
- **Protocol**: UDP lub TCP. Różnice opisano tutaj.
- **Authentication Mode**: określa metodę uwierzytelniania klienta podczas łączenia z serwerem. Dostępne są trzy opcje:

- **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.

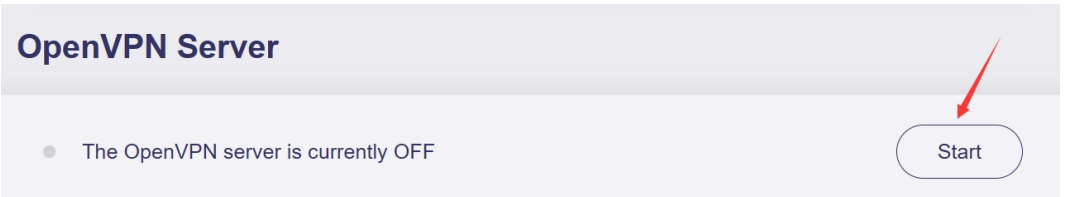
3. Wyeksportuj konfigurację klienta.
   Po kliknięciu **Export Client Configuration** u dołu karty Configuration (lub zastosowaniu zmienionej konfiguracji) pojawi się poniższe okno. Kliknij **Download**, aby wyeksportować konfigurację.



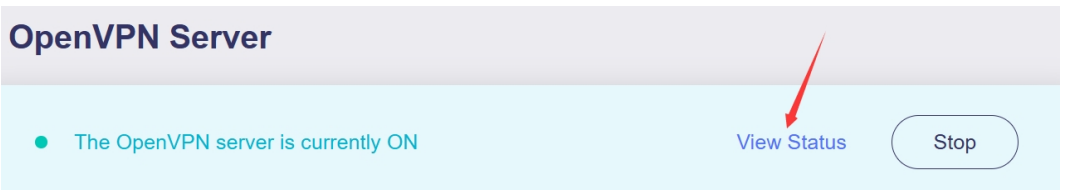
Wskazówka: jeśli Twój publiczny adres IP często się zmienia, przejdź do **APPLICATIONS** > **Dynamic DNS** i włącz DDNS. Możesz wtedy używać domeny DDNS jako adresu serwera.

4. Uruchom serwer OpenVPN.

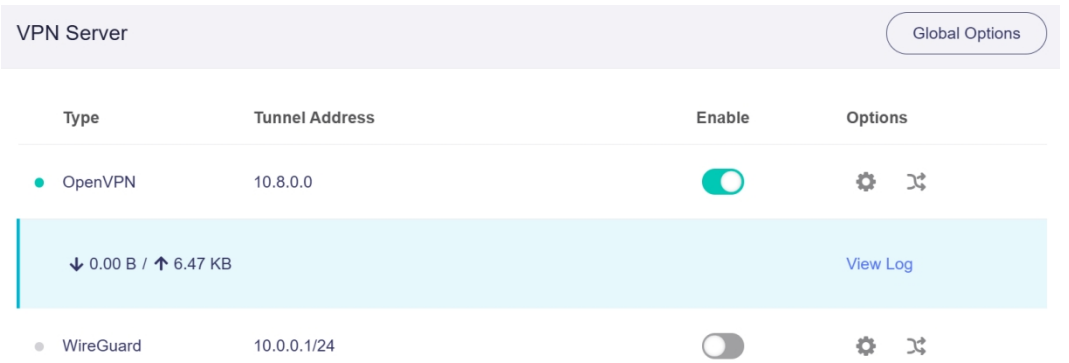
   Na stronie **OpenVPN Server** kliknij przycisk **Start** w prawym górnym rogu, aby uruchomić serwer.



Aby sprawdzić stan połączenia serwera, kliknij **View Status**.



Otworzy się panel VPN. Jeśli na tej stronie są wyświetlane statystyki wysyłania i pobierania, serwer OpenVPN działa.



9.1.3 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.

9.2 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.

9.2.1 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:

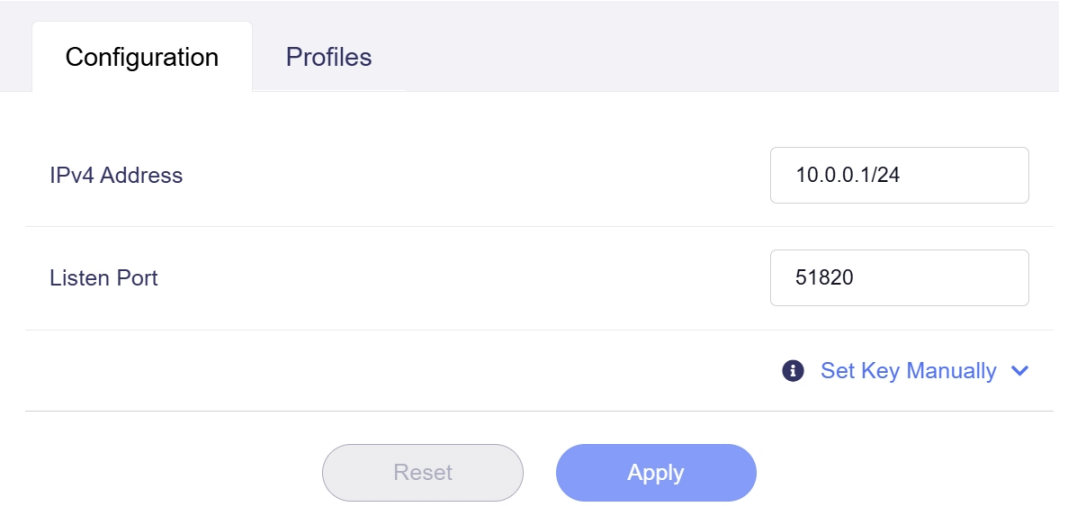
   - Jeśli przed routerem GL.iNet znajduje się główny router, zaloguj się do niego i sprawdź, czy ma publiczny adres IP przydzielony przez dostawcę Internetu.
   - Poproś dostawcę Internetu o publiczny adres IP. Może to wiązać się z dodatkową opłatą.

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

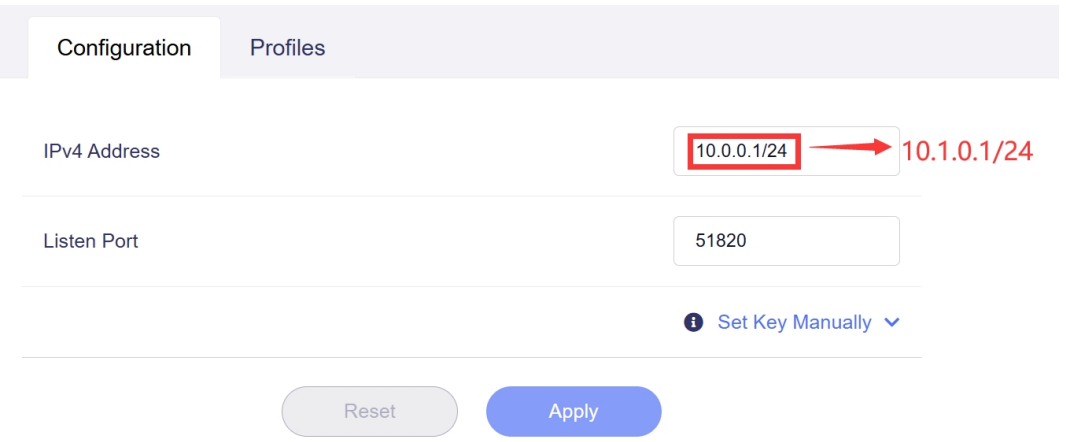
   - Jeśli router GL.iNet jest głównym routerem w sieci, konfiguracja przekierowania portów nie jest wymagana. Przejdź do następnego kroku.
   - Jeśli korzystasz już z głównego routera, a router GL.iNet działa jako router dodatkowy, trzeba skonfigurować przekierowanie portów na głównym routerze.
   - Jeśli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

9.2.2 Etapy konfiguracji

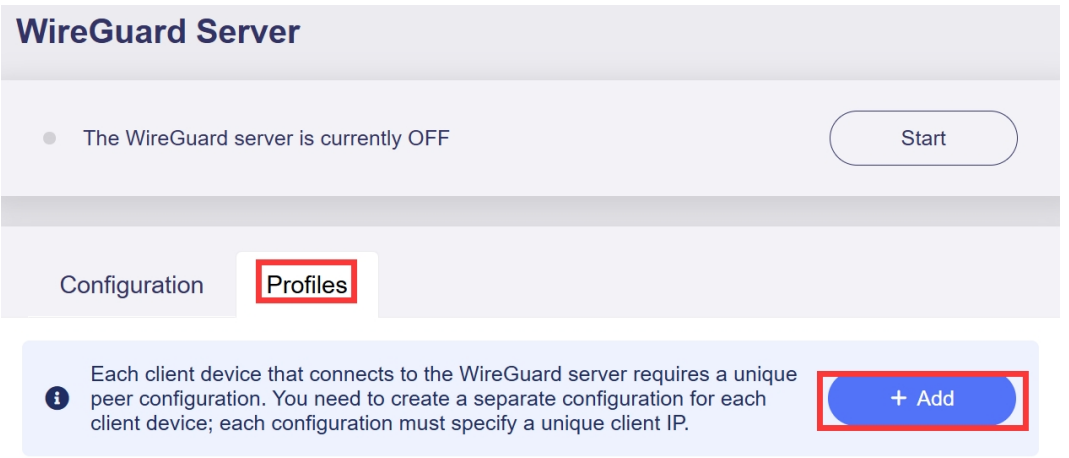
1. Zaloguj się do panelu administracyjnego routera, przejdź do **VPN** > **WireGuard Server**, a następnie kliknij **Generate Configuration** (tylko przy pierwszej konfiguracji serwera VPN).
2. Zastosuj konfigurację.
   Domyślna konfiguracja sprawdza się w większości przypadków. Nie trzeba zmieniać adresu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



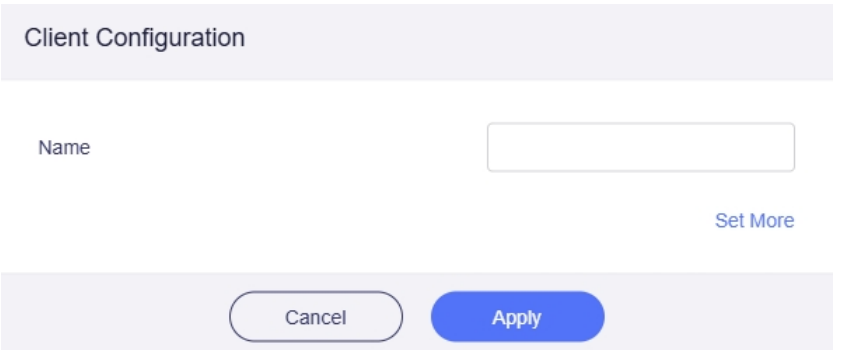
   Jeśli adres IPv4 koliduje z adresem bramy routera nadrzędnego, zmień go na inny (np. **10.1.0.1/24**) i kliknij **Apply**. Aby uniknąć problemów z łącznością, koniecznie zachowaj zapis CIDR „/24”.



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



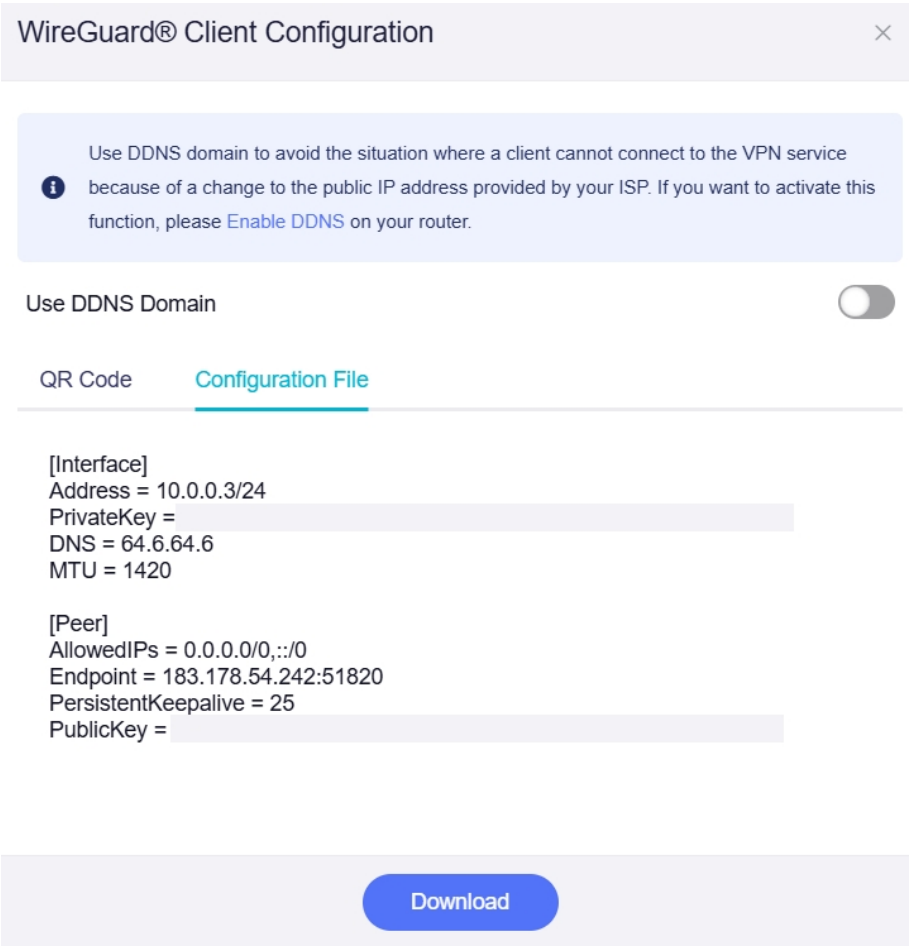
Nadaj opisową nazwę i kliknij **Apply**, aby kontynuować.



4. Pobierz konfigurację.

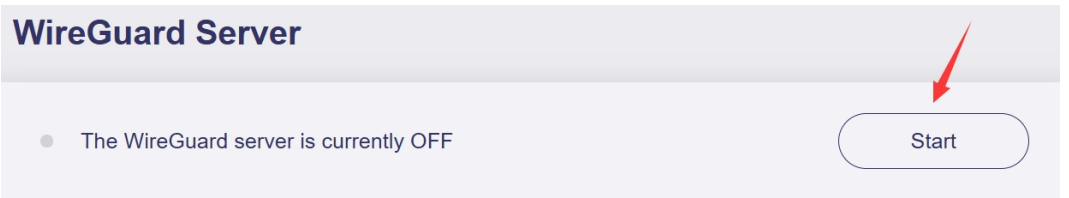
   Po dodaniu profilu router generuje plik konfiguracyjny w trzech postaciach: kodu QR, zwykłego tekstu i pliku .conf. Wybierz preferowany sposób uzyskania konfiguracji.

   - **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.

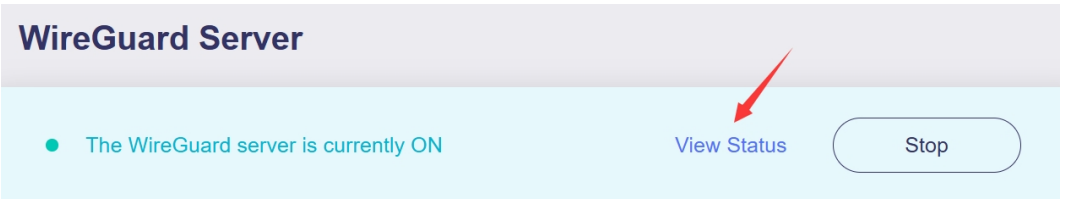


Wskazówka: jeśli Twój publiczny adres IP często się zmienia, przejdź do **APPLICATIONS** > **Dynamic DNS** i włącz DDNS. Możesz wtedy używać domeny DDNS jako adresu serwera.

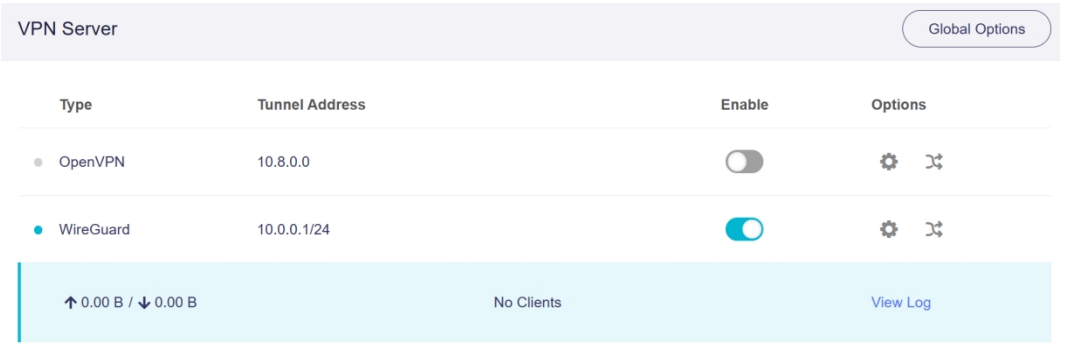
5. Uruchom serwer WireGuard.
   Na stronie **WireGuard Server** kliknij przycisk **Start** w prawym górnym rogu, aby uruchomić serwer.



Aby sprawdzić stan połączenia serwera, kliknij **View Status**.



Otworzy się panel VPN. Jeśli na tej stronie są wyświetlane statystyki wysyłania i pobierania, serwer OpenVPN działa.



9.2.3 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 10

Konfiguracja klienta VPN

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

10.1 Konfiguracja klienta OpenVPN

10.1.1 Przygotowanie

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

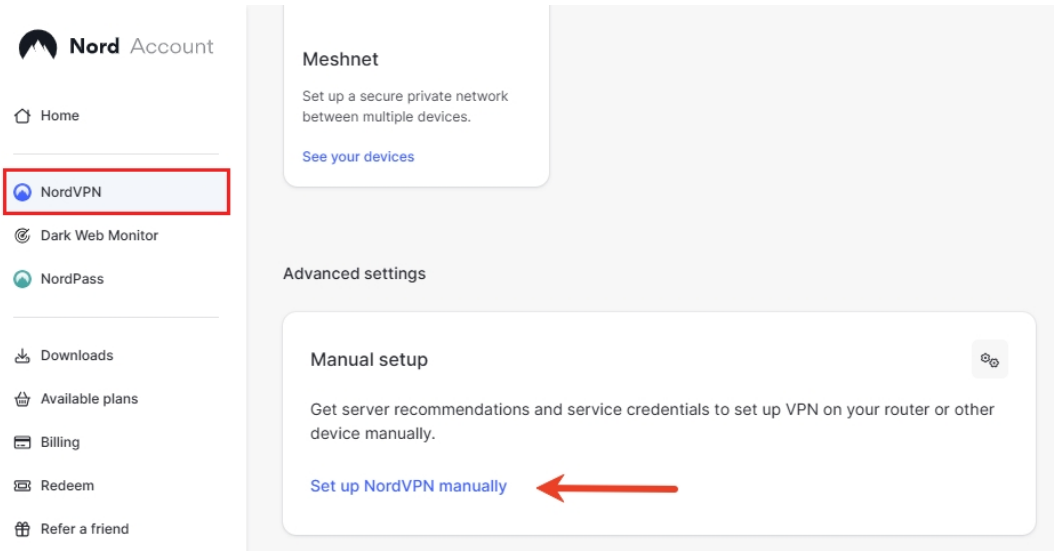
Następnie odwiedź oficjalną witrynę dostawcy VPN, którego usługę subskrybujesz, i uzyskaj dane dostępowe usługi lub plik konfiguracyjny. Jeśli nie wiesz, jak uzyskać plik konfiguracyjny, skorzystaj z tego łącza lub skontaktuj się z pomocą techniczną dostawcy.

10.1.2 Konfiguracja NordVPN

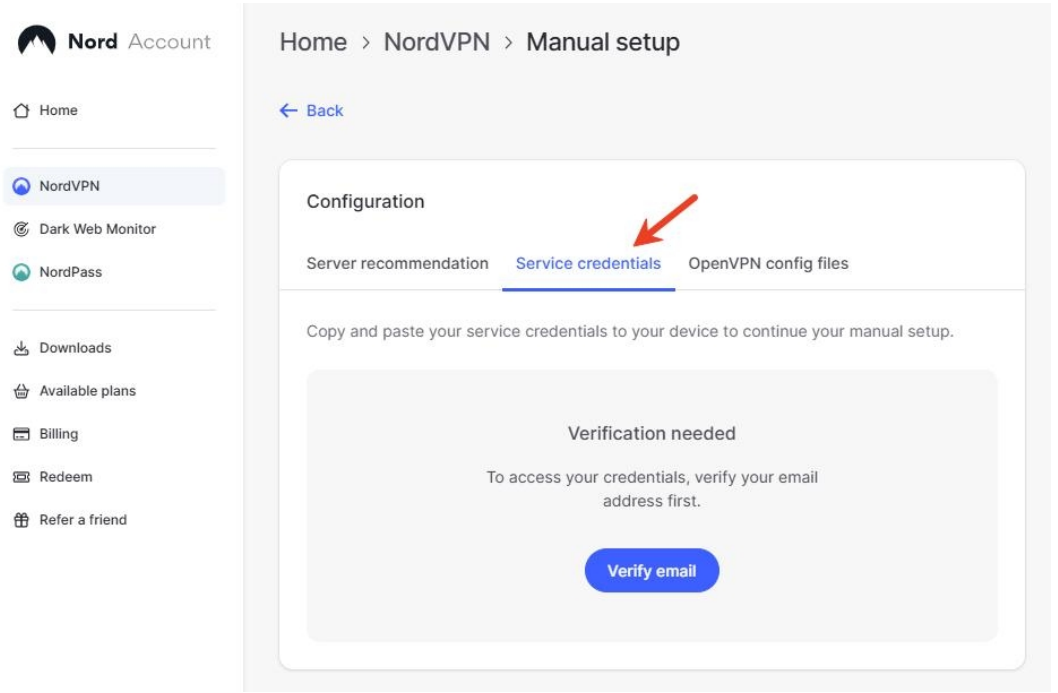
NordVPN jest zintegrowany z panelem administracyjnym GL.iNet. Pliki konfiguracyjne wszystkich serwerów NordVPN można uzyskać, wprowadzając dane dostępowe konta (z panelu NordVPN) w panelu administracyjnym routera lub aplikacji mobilnej GL.iNet. Eliminuje to potrzebę ręcznego przesyłania plików.

Aby skonfigurować router jako klienta NordVPN, wykonaj poniższe czynności.

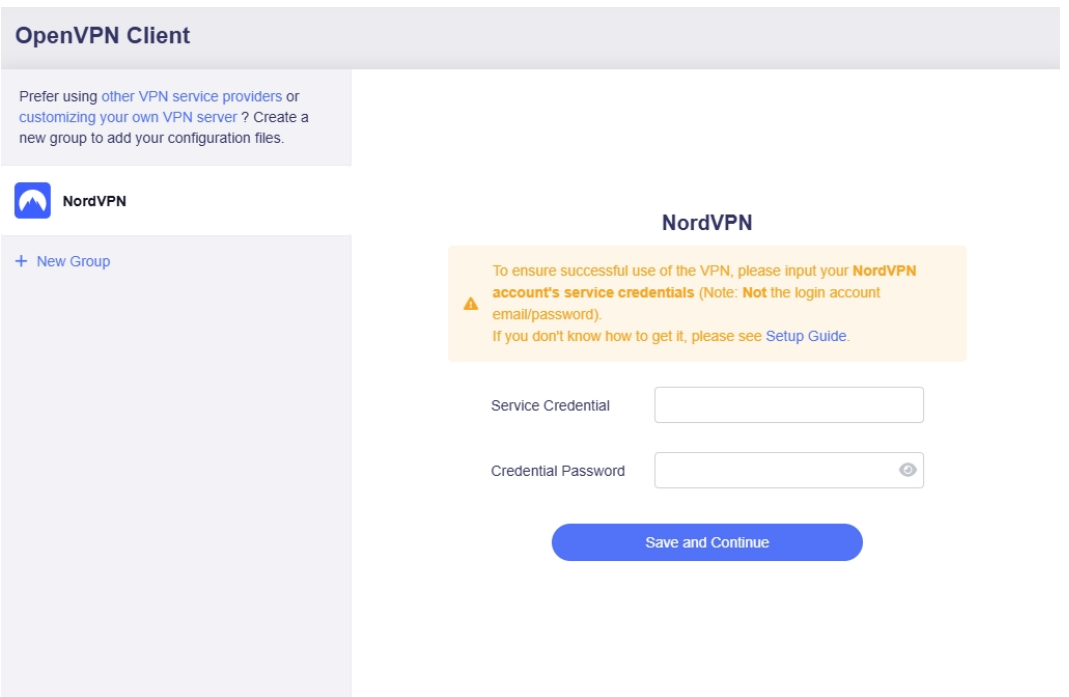
1. Zaloguj się na swoje konto internetowe NordVPN tutaj.
2. W panelu Nord kliknij **NordVPN**, a następnie **Set up NordVPN manually**.



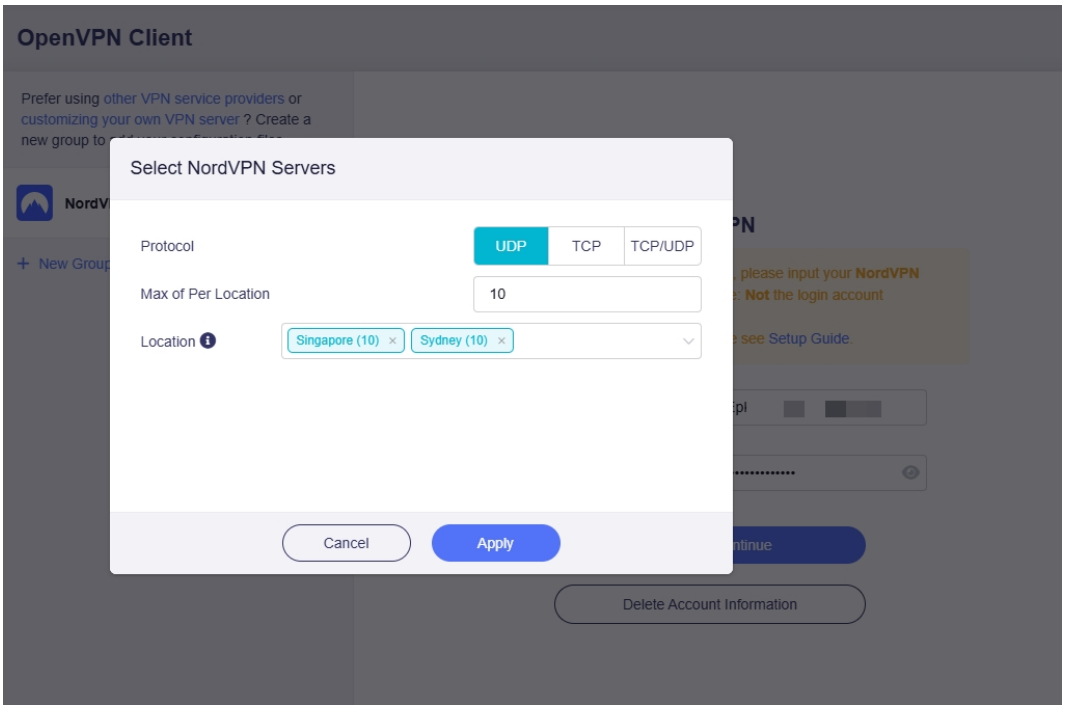
Znajdziesz tam **dane dostępowe usługi**. Skopiuj je do późniejszego użycia.



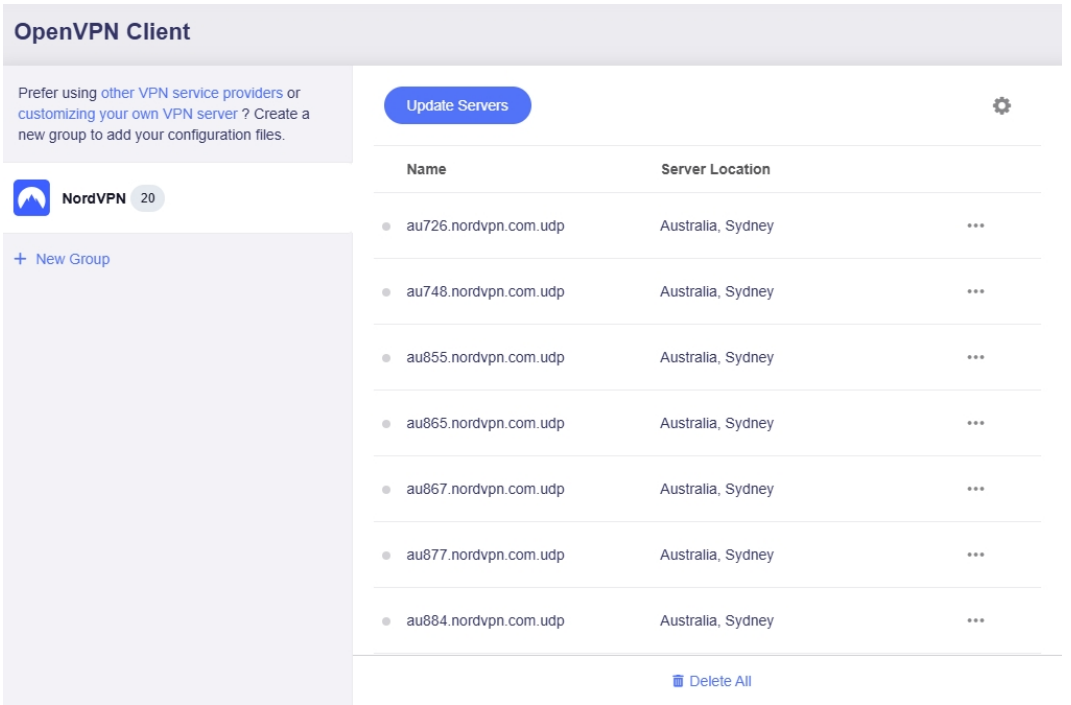
3. Zaloguj się do panelu administracyjnego routera i przejdź do **VPN** > **OpenVPN Client** > **NordVPN**. Wprowadź dane dostępowe usługi (uwaga: NIE jest to adres e-mail ani hasło do logowania na konto), a następnie kliknij **Save and Continue**.



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

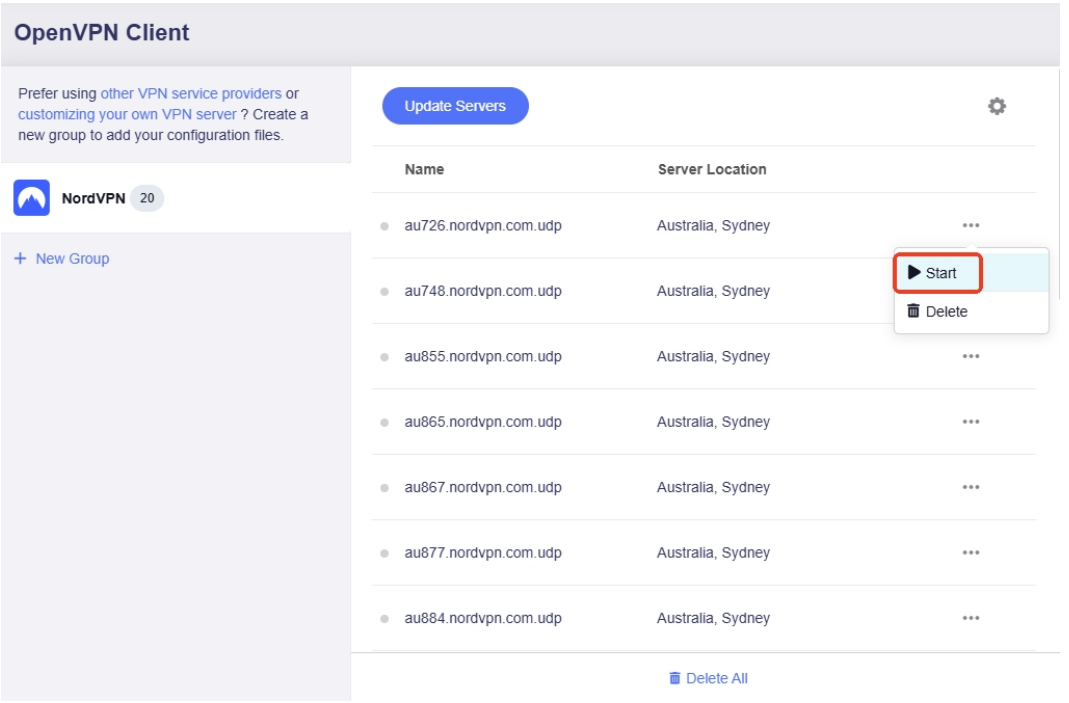


Rozpocznie się pobieranie plików konfiguracyjnych.

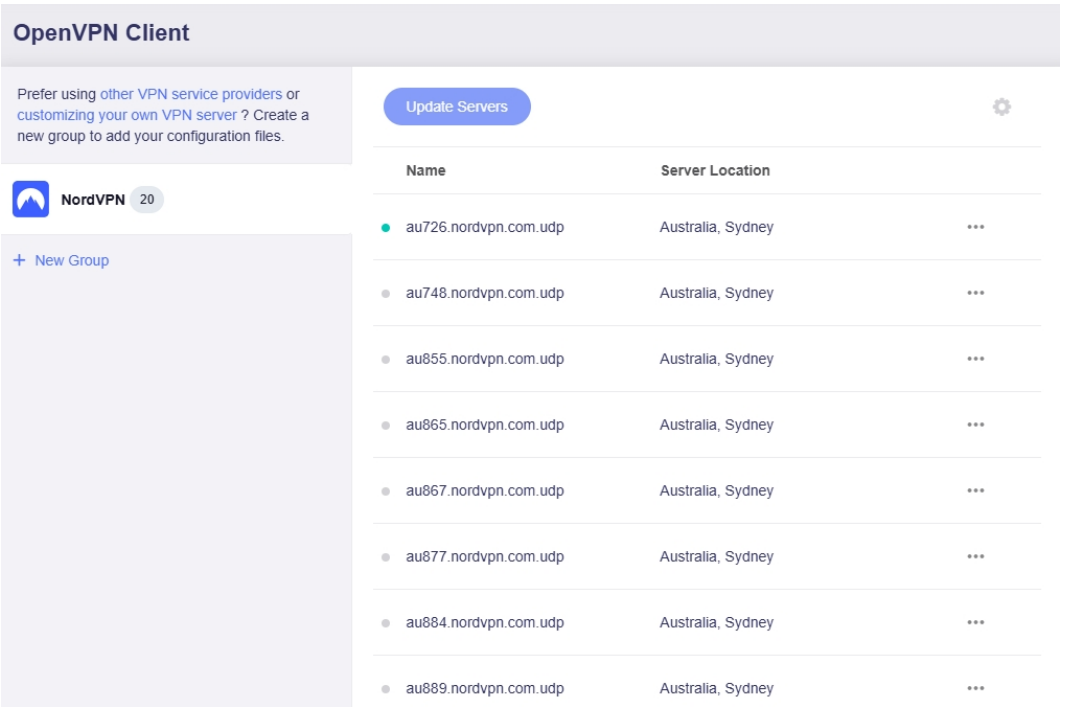


5. Nawiąż połączenie.

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



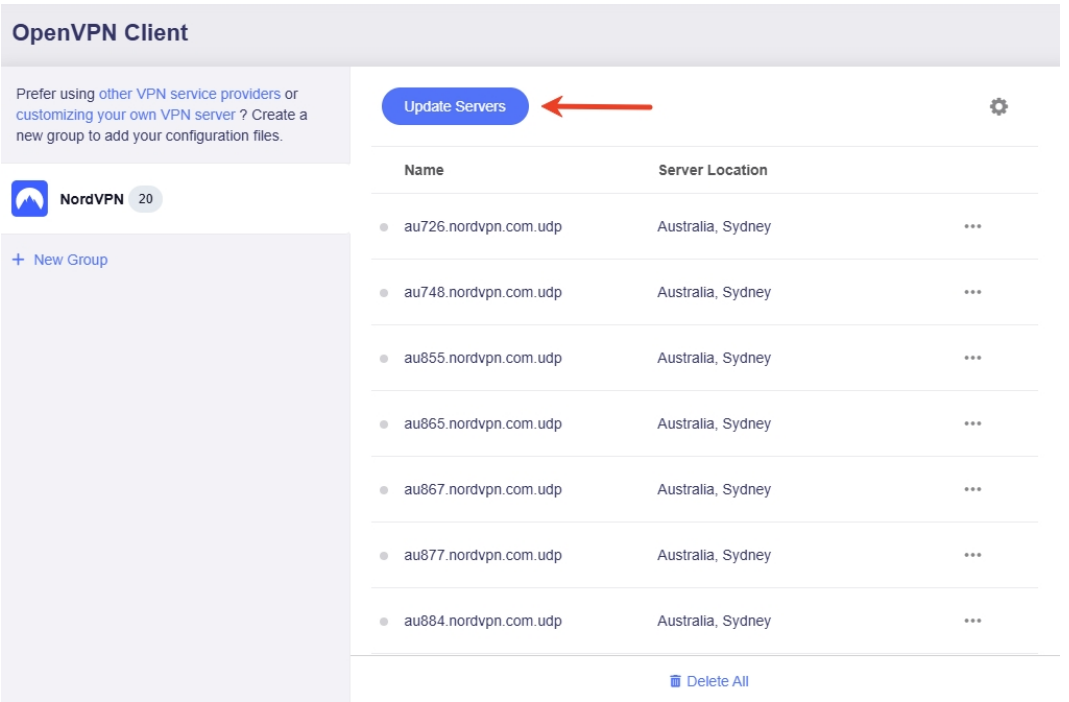
6. Po połączeniu obok pliku konfiguracyjnego pojawi się zielona kropka.



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

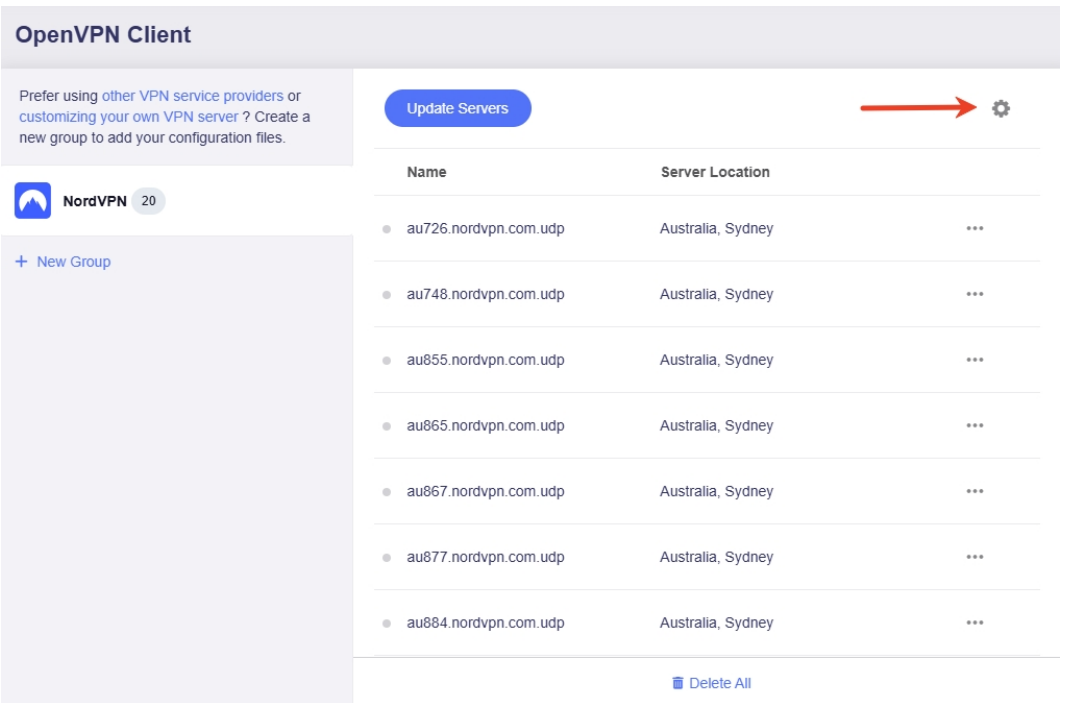
7. Zaktualizuj serwery.

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



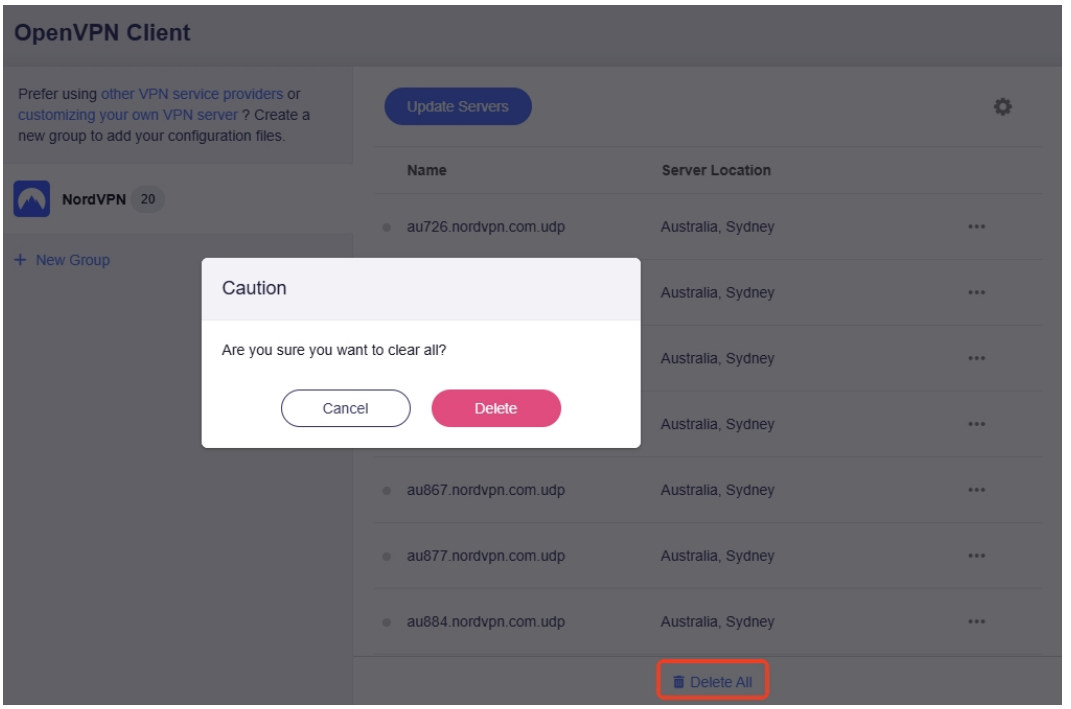
8. Zmień dane dostępowe.

   Kliknij ikonę koła zębatego, aby zmienić dane logowania.



9. Usuń wszystkie pliki.

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

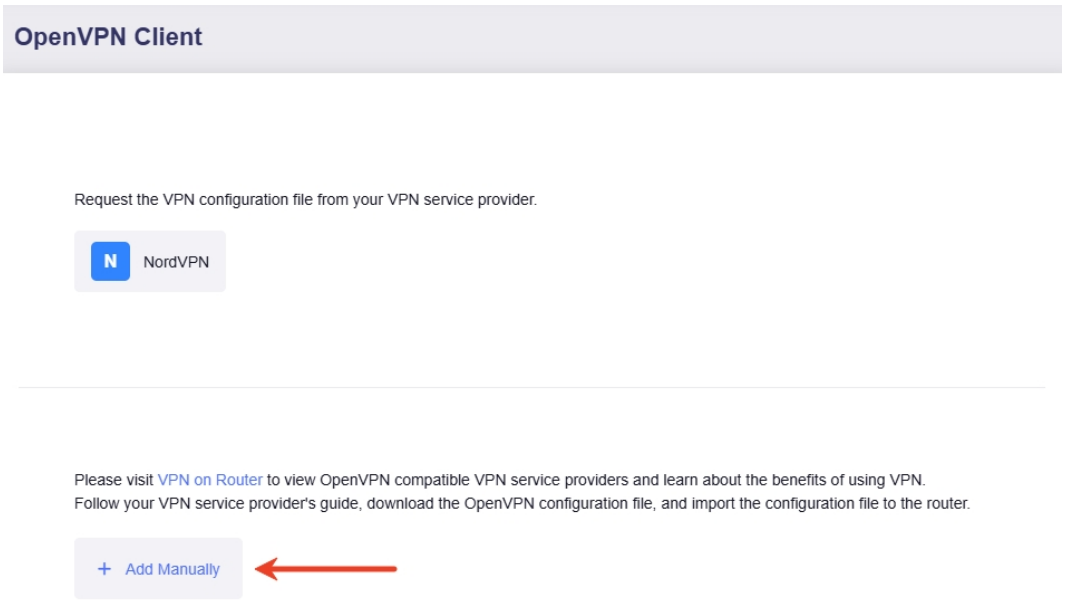


10.1.3 Ręczna konfiguracja klienta OpenVPN (inni dostawcy)

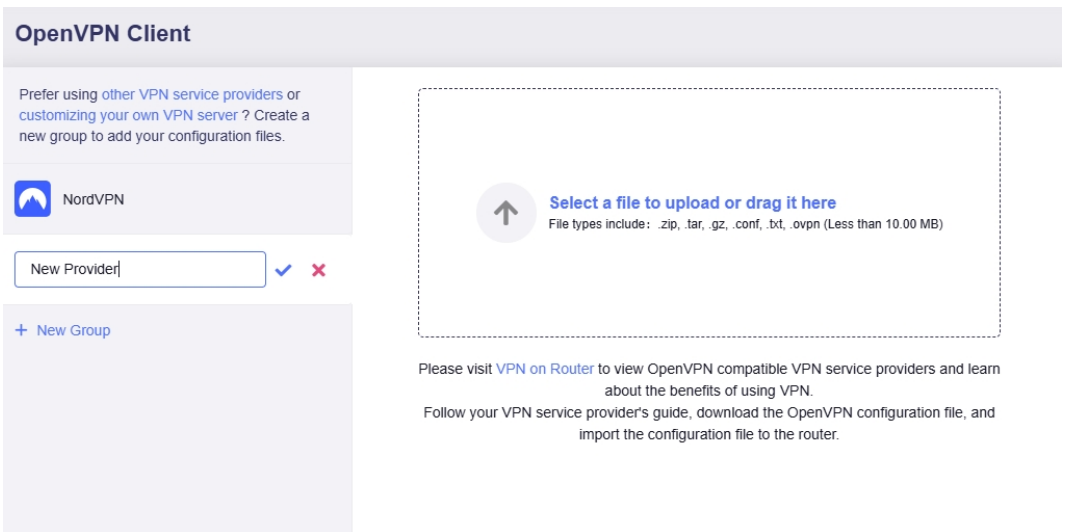
Jeśli Twój dostawca OpenVPN nie jest zintegrowany z panelem administracyjnym, najpierw odwiedź jego oficjalną witrynę i pobierz plik konfiguracyjny. Następnie prześlij go do routera, aby skonfigurować klienta OpenVPN.

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

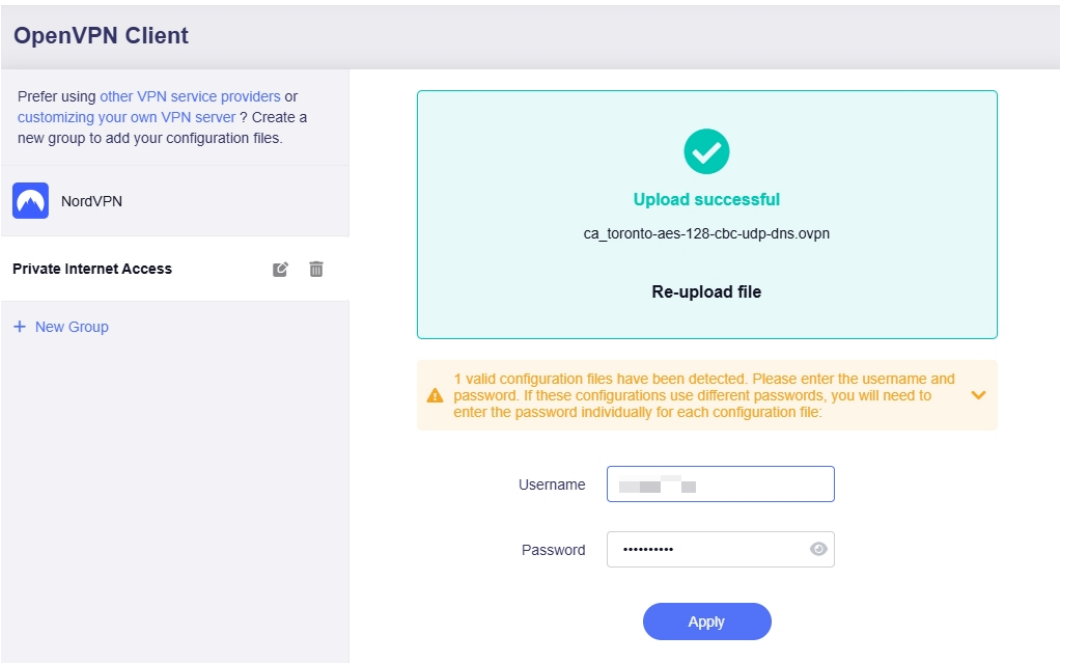
1. Pobierz plik konfiguracyjny z oficjalnej witryny Private Internet Access.
2. Zaloguj się do panelu administracyjnego routera, przejdź do **VPN** > **OpenVPN Client** i kliknij **Add Manually**.



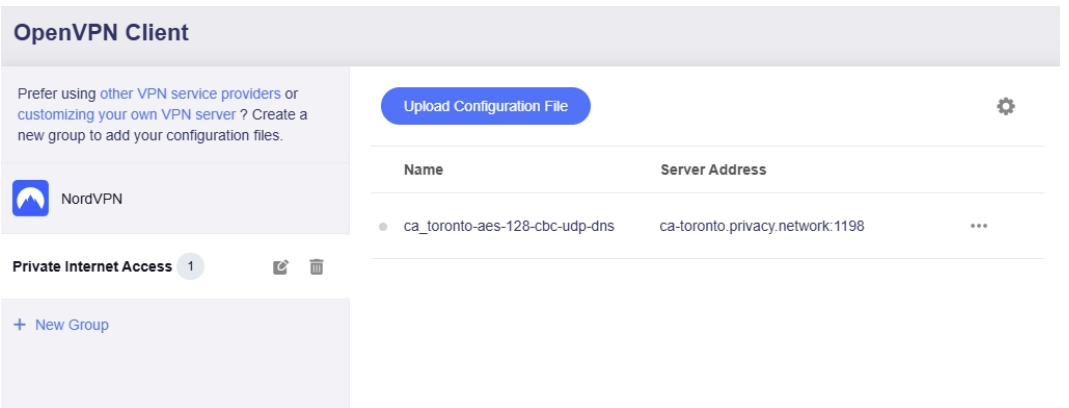
3. Na lewym pasku bocznym powstanie grupa. Nadaj jej opisową nazwę.



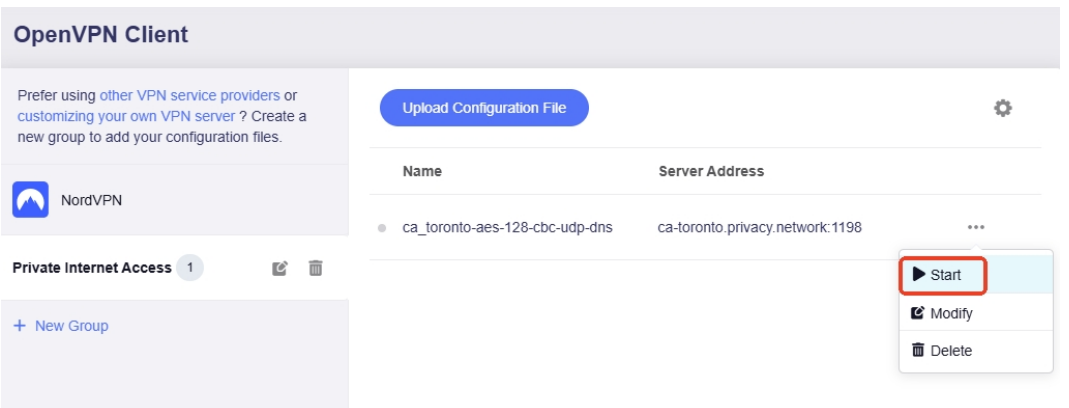
4. Prześlij plik konfiguracyjny OpenVPN. Jeśli jest to wymagane, wprowadź dane dostępowe, a następnie kliknij **Apply**.



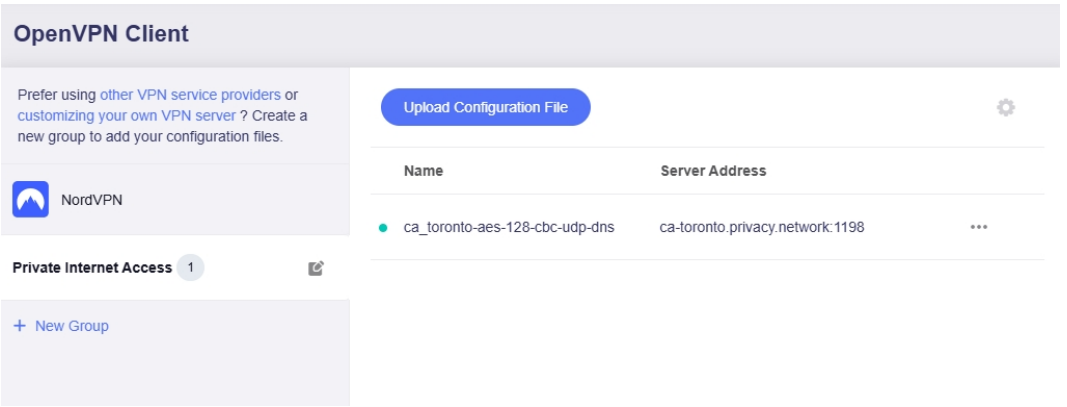
Pojawi się przesłany plik konfiguracyjny.



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**.

10.2 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.

10.2.1 Przygotowanie

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

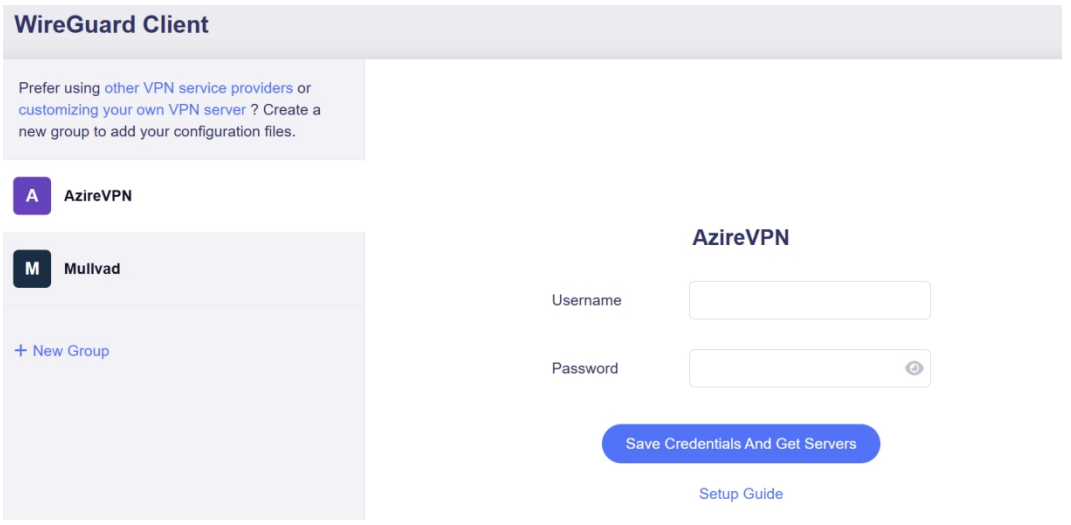
Następnie wybierz poniżej odpowiedniego dostawcę WireGuard, aby szybko przejść do instrukcji krok po kroku.

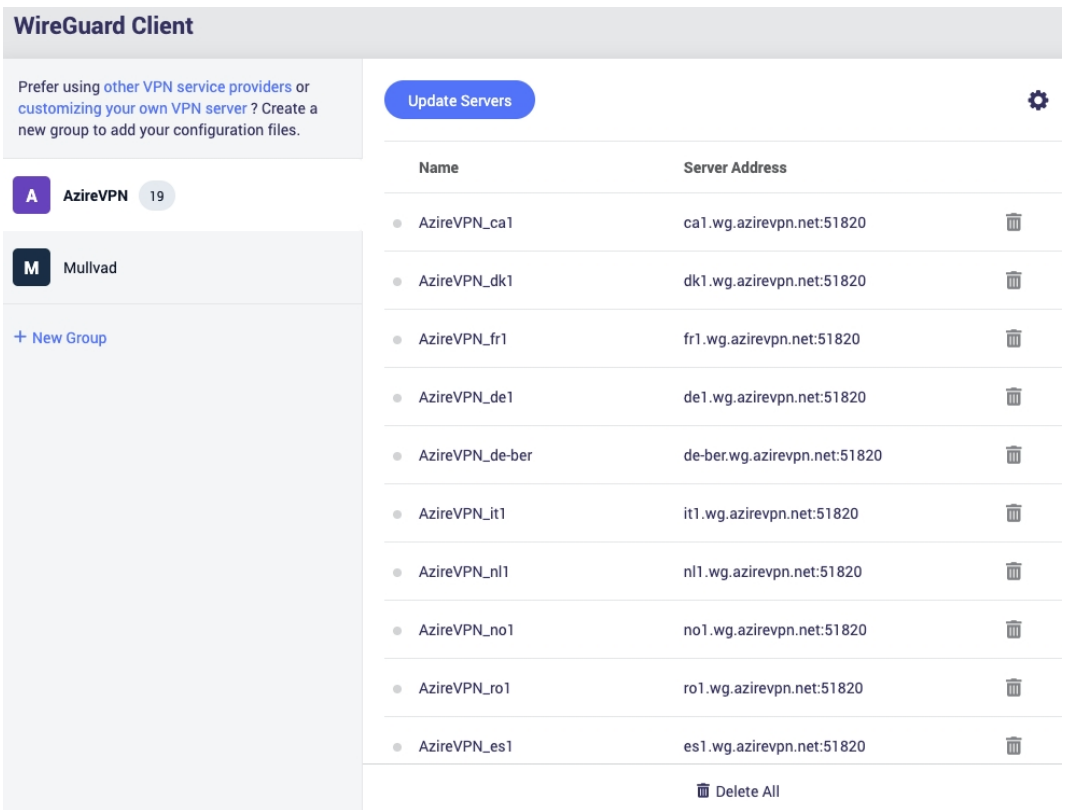
- Konfiguracja AzireVPN
- Konfiguracja Mullvad
- Ręczna konfiguracja klienta WireGuard (inni dostawcy)

10.2.2 Konfiguracja AzireVPN

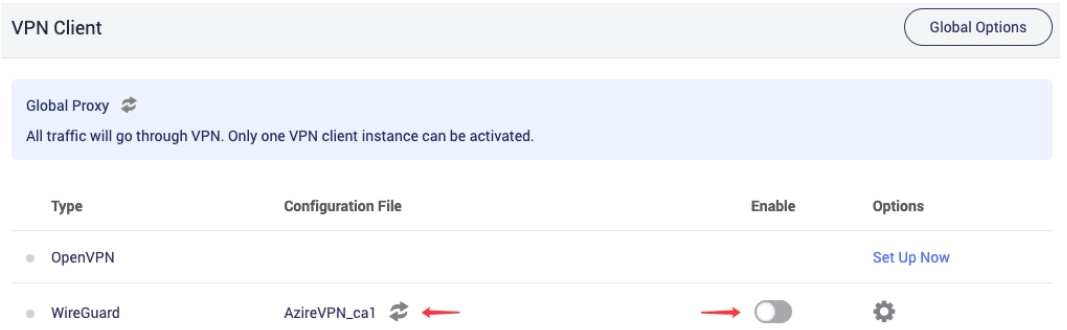
Aby skonfigurować router jako klienta AzireVPN, wykonaj poniższe czynności.

1. Zaloguj się do panelu administracyjnego routera i przejdź do **VPN** > **WireGuard Client** > **AzireVPN**.
2. Wprowadź nazwę użytkownika i hasło, a następnie kliknij **Save Credentials And Get Servers**. Zostaną wygenerowane pliki konfiguracyjne dla poszczególnych serwerów.

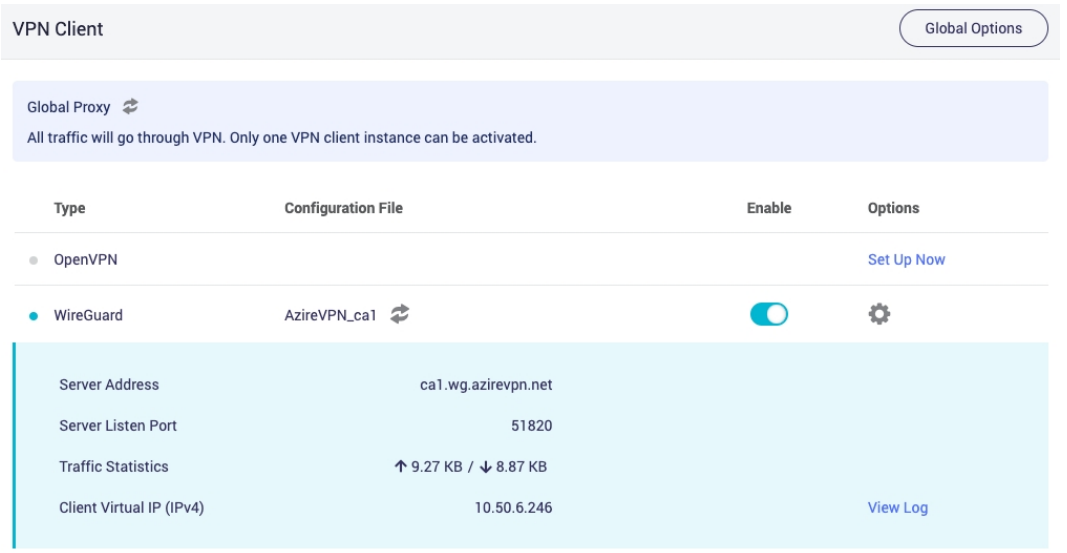




3. Przejdź do VPN Dashboard, aby włączyć połączenie.

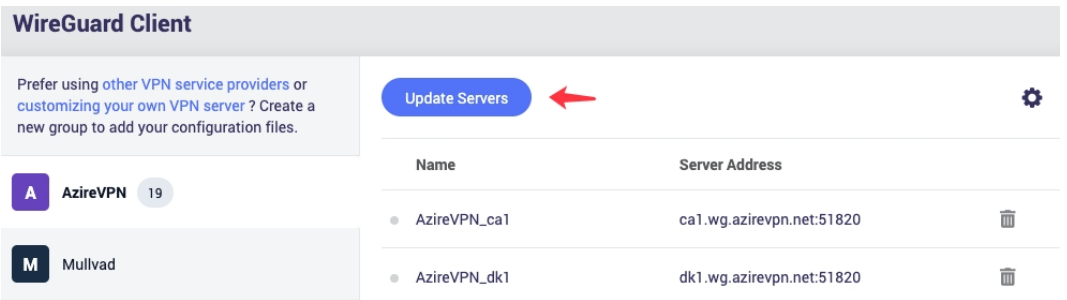


Po połączeniu powinny być widoczne Twój adres IP oraz liczba wysłanych i odebranych bajtów.



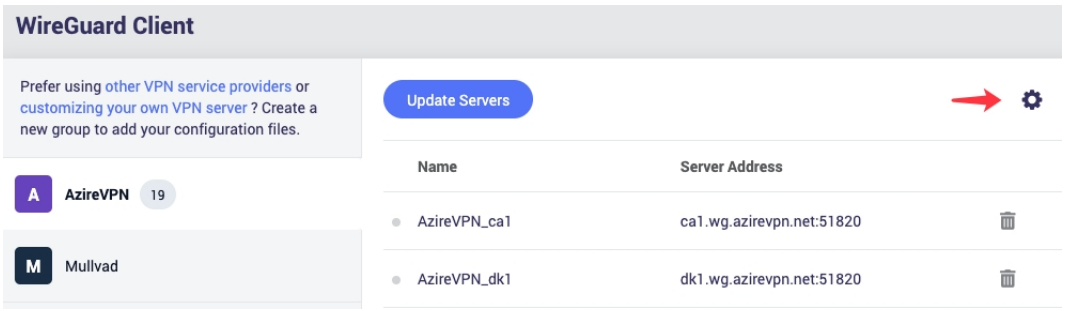
4. Zaktualizuj serwery.

   AzireVPN może prowadzić konserwację lub wyłączać niektóre serwery, powodując problemy z połączeniem. Kliknij **Update Servers**, aby pobrać aktualną listę dostępnych serwerów.



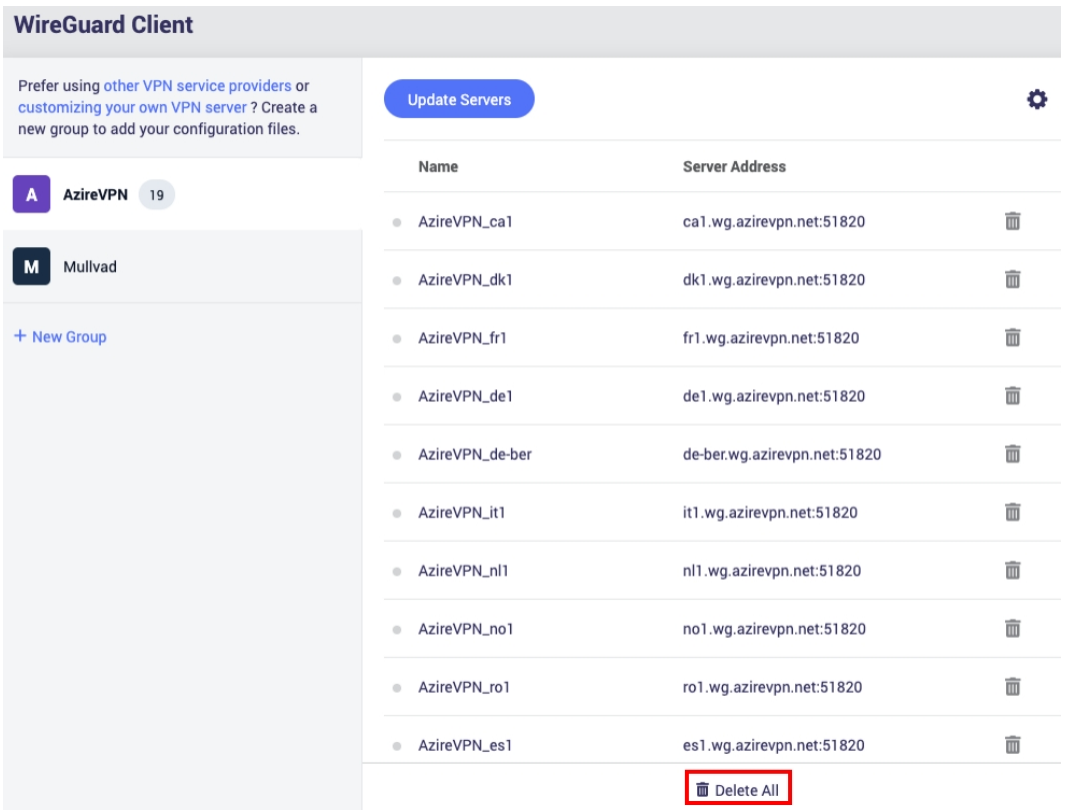
5. Zmień dane dostępowe.

   Kliknij ikonę koła zębatego, aby zmienić dane dostępowe.



6. Usuń wszystkie pliki.

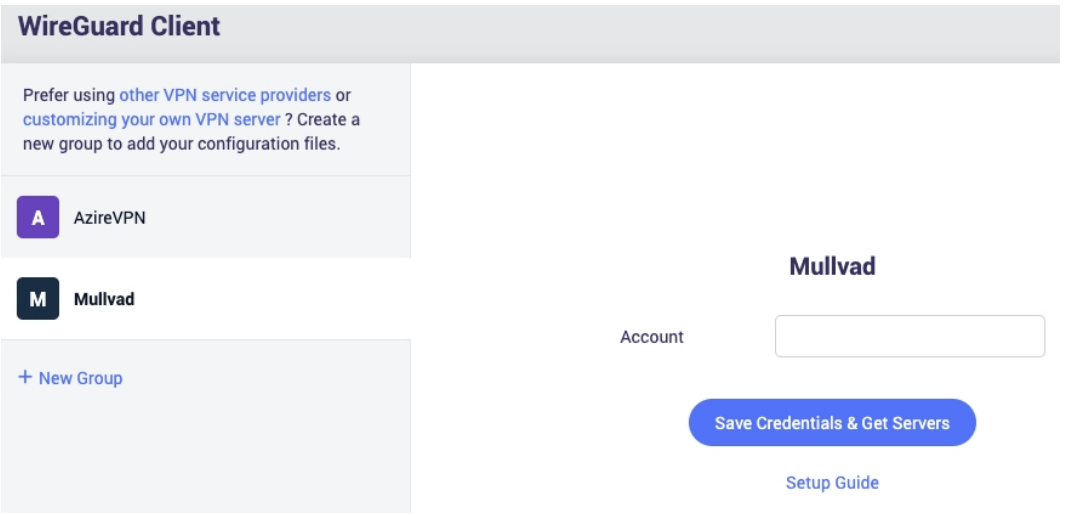
   Możesz kliknąć **Delete All**, aby jednym kliknięciem usunąć wszystkie pliki konfiguracyjne.



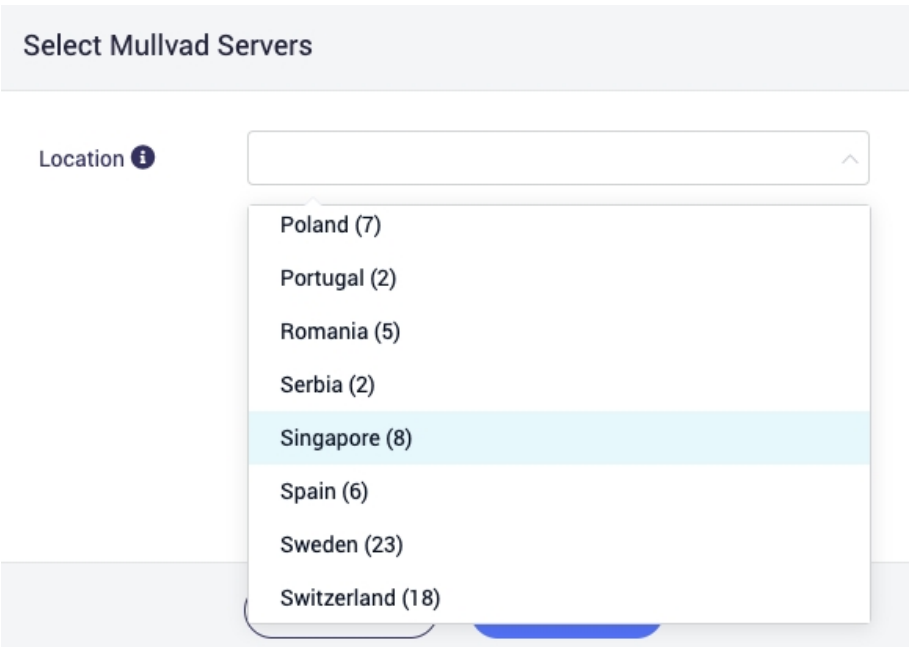
10.2.3 Konfiguracja Mullvad

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 numer konta Mullvad (16 cyfr), a następnie kliknij **Save Credentials & Get Servers**.

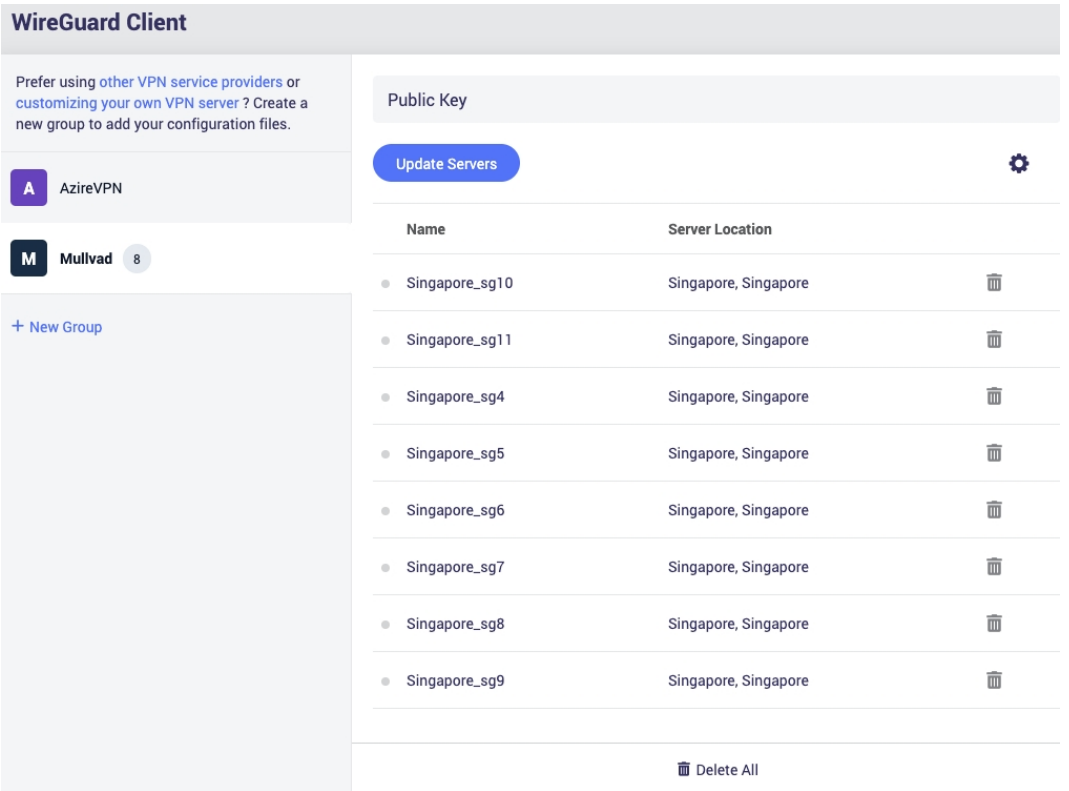


Pojawi się okno wyboru lokalizacji.

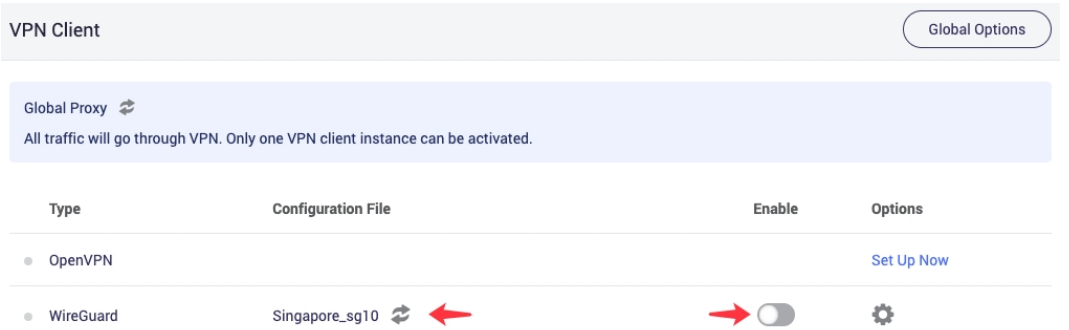


Następnie zostaną wygenerowane pliki konfiguracyjne serwera z wybranej lokalizacji.

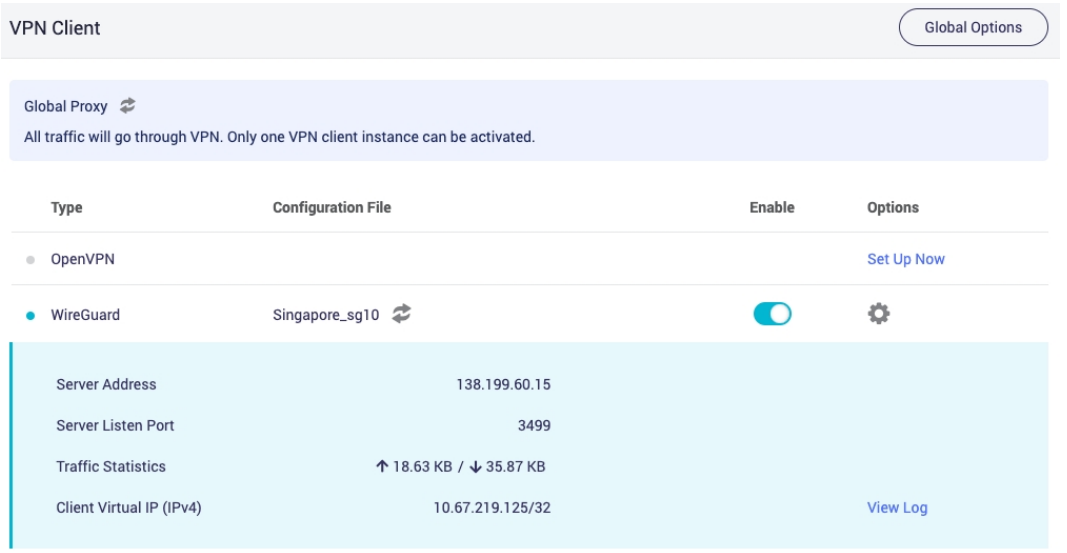
Pole **Public Key** zawiera klucz publiczny WireGuard przesyłany do serwera Mullvad. Jednocześnie możesz mieć do pięciu kluczy. Kluczami WireGuard można zarządzać na stronie konta Mullvad.



3. Przejdź do VPN Dashboard, aby włączyć połączenie.

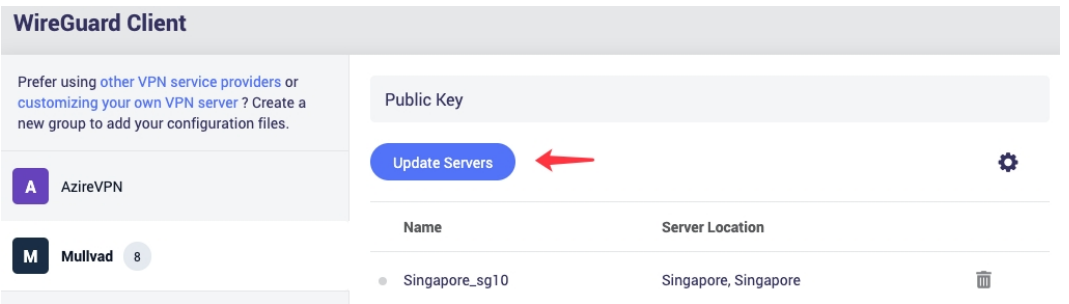


Po połączeniu powinny być widoczne Twój adres IP oraz liczba wysłanych i odebranych bajtów.



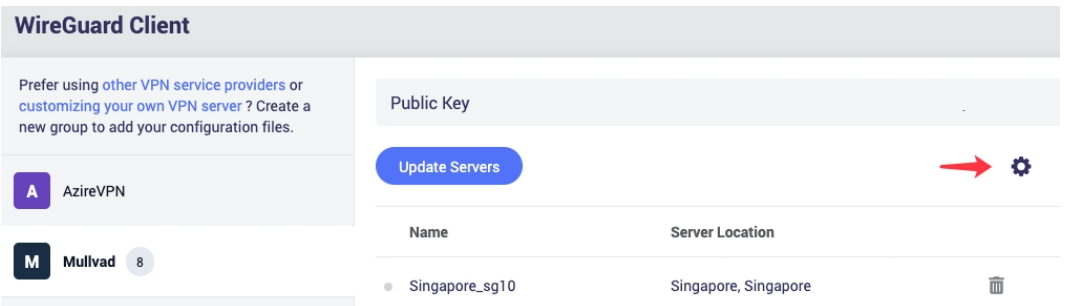
4. Zaktualizuj serwery.

   Mullvad może prowadzić konserwację lub wyłączać niektóre serwery, powodując problemy z połączeniem. Kliknij **Update Servers**, aby pobrać aktualną listę dostępnych serwerów.



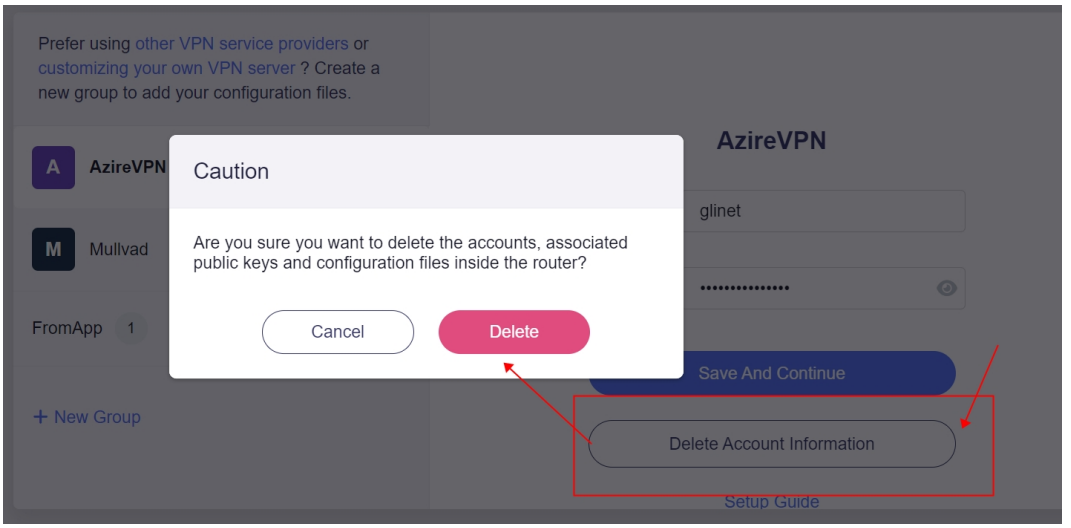
5. Zmiana danych dostępowych

   Kliknij ikonę koła zębatego, aby zmienić dane logowania.



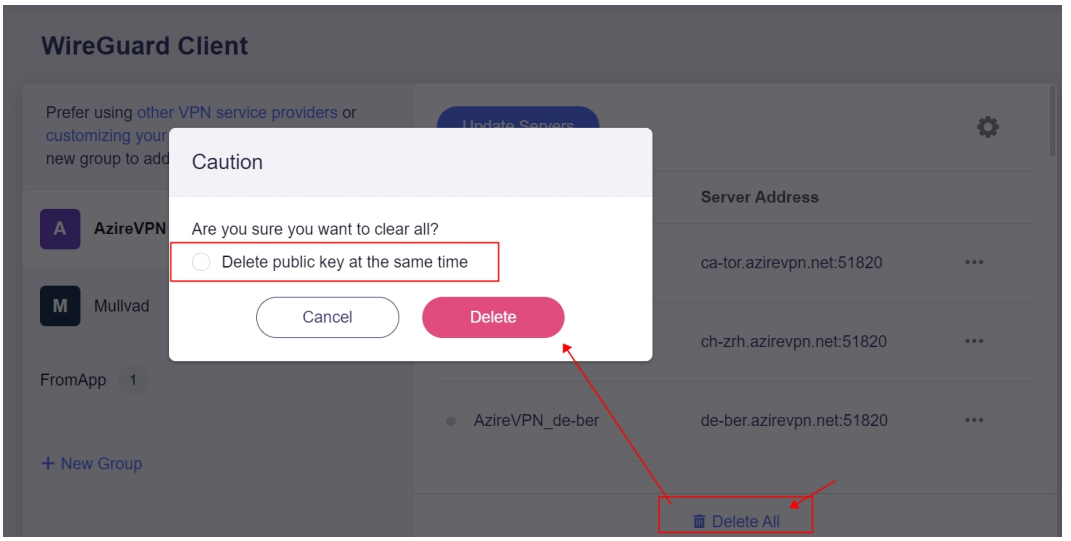
6. Usuwanie informacji o koncie

   Kliknięcie **Delete** usuwa dane dostępowe konta, klucz prywatny, klucz publiczny i pliki konfiguracyjne **z routera**.



7. Usuwanie

Umożliwia usunięcie wszystkich plików konfiguracyjnych jednym kliknięciem i wyświetla pytanie o usunięcie również klucza prywatnego i publicznego.

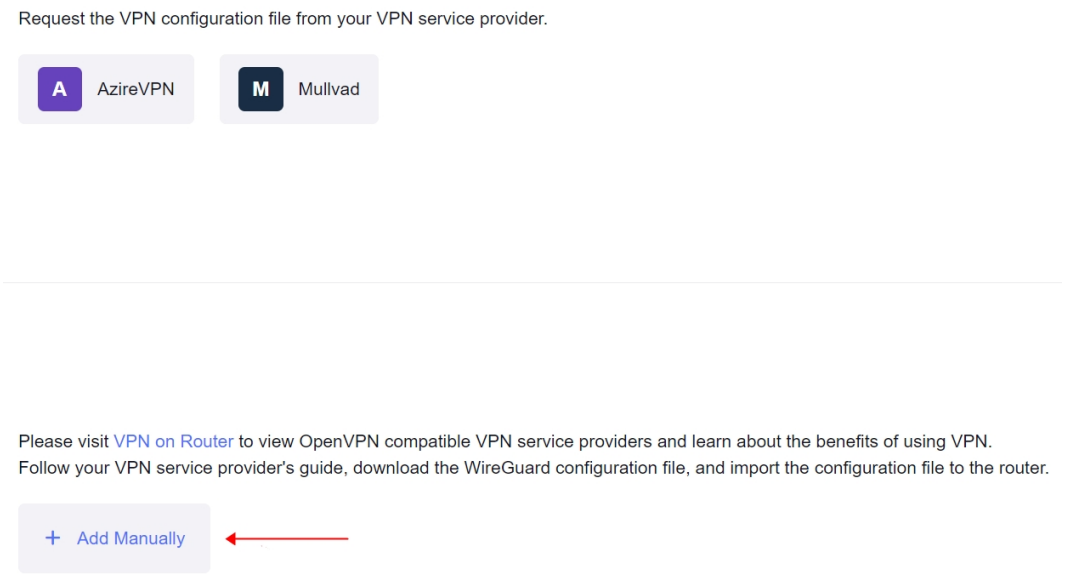


10.2.4 Ręczna konfiguracja klienta WireGuard (inni dostawcy)

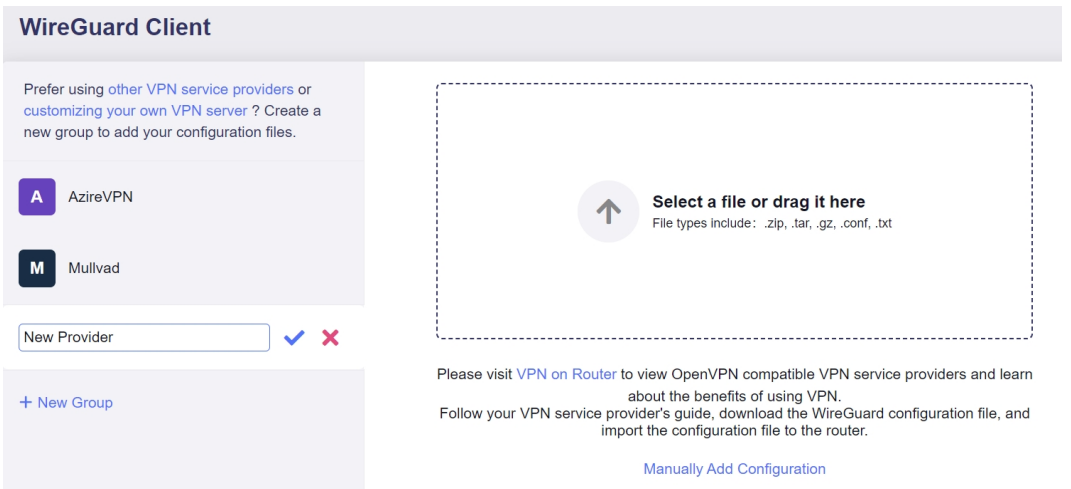
Jeśli Twój dostawca WireGuard nie jest zintegrowany z panelem administracyjnym, najpierw odwiedź jego oficjalną witrynę i pobierz plik konfiguracyjny. Następnie prześlij go do routera, aby skonfigurować klienta WireGuard. Jeśli nie wiesz, jak pobrać pliki konfiguracyjne, skorzystaj z tego poradnika lub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

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

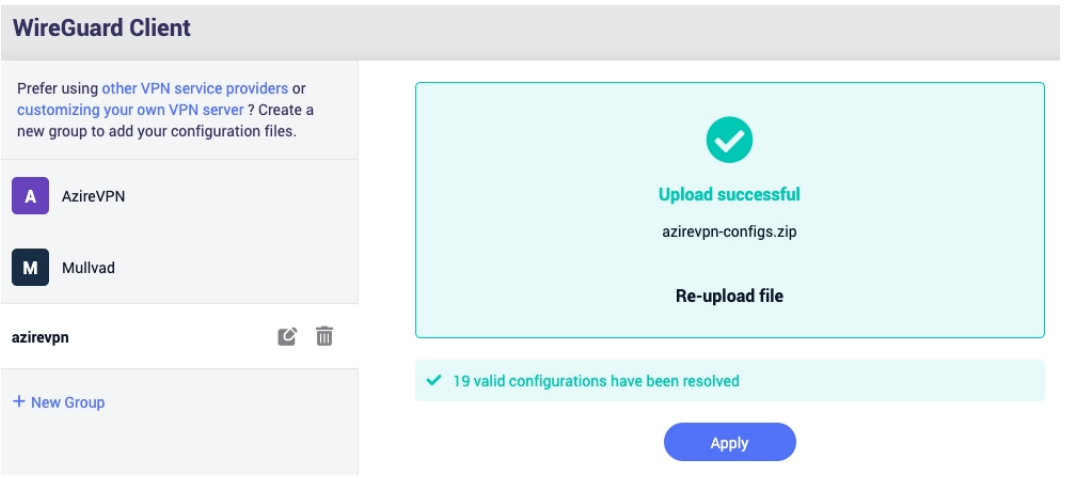
1. Zaloguj się do panelu administracyjnego routera i przejdź do **VPN** > **WireGuard Client** > **Add Manually**.



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

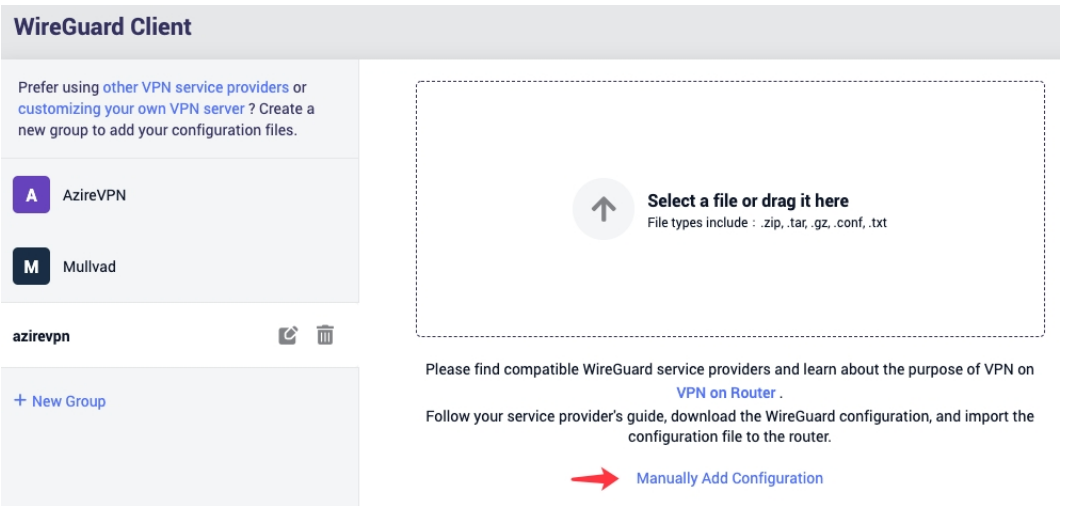


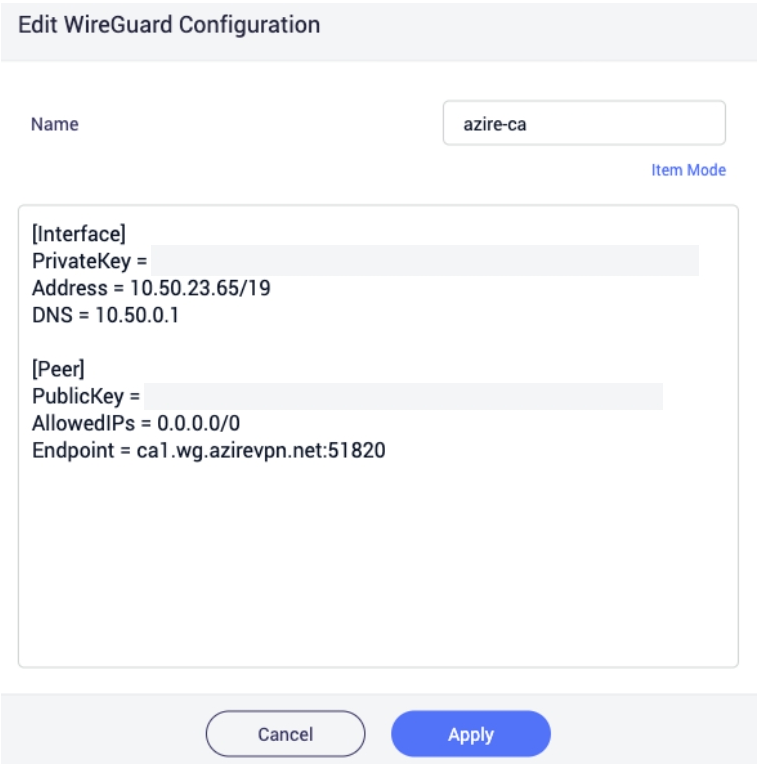
3. Kliknij obszar przesyłania, aby przesłać plik konfiguracyjny WireGuard (obsługiwane formaty: zip, tar, gz, conf, txt), i kliknij **Apply**.



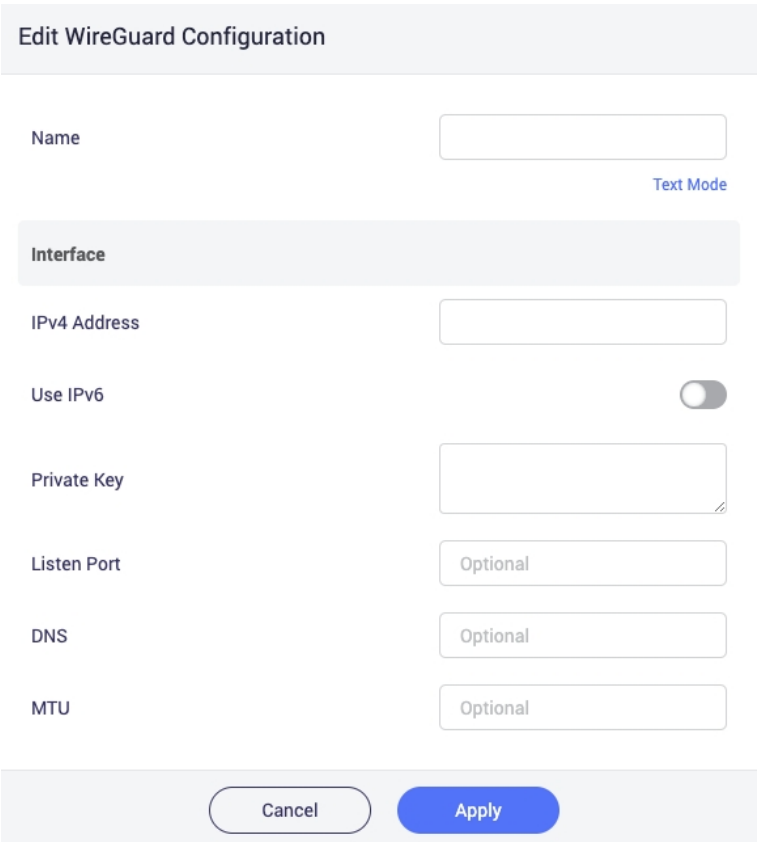
Jeśli prześlesz skompresowany plik zawierający wiele plików konfiguracyjnych, zostanie on automatycznie rozpakowany.

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

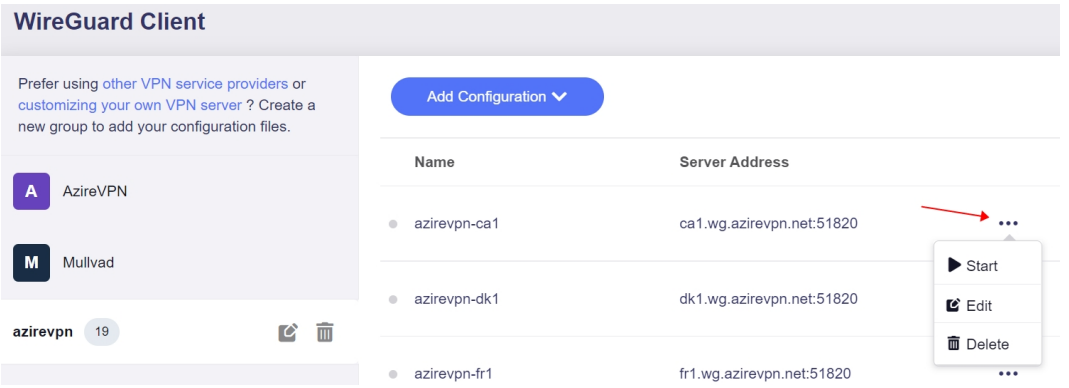




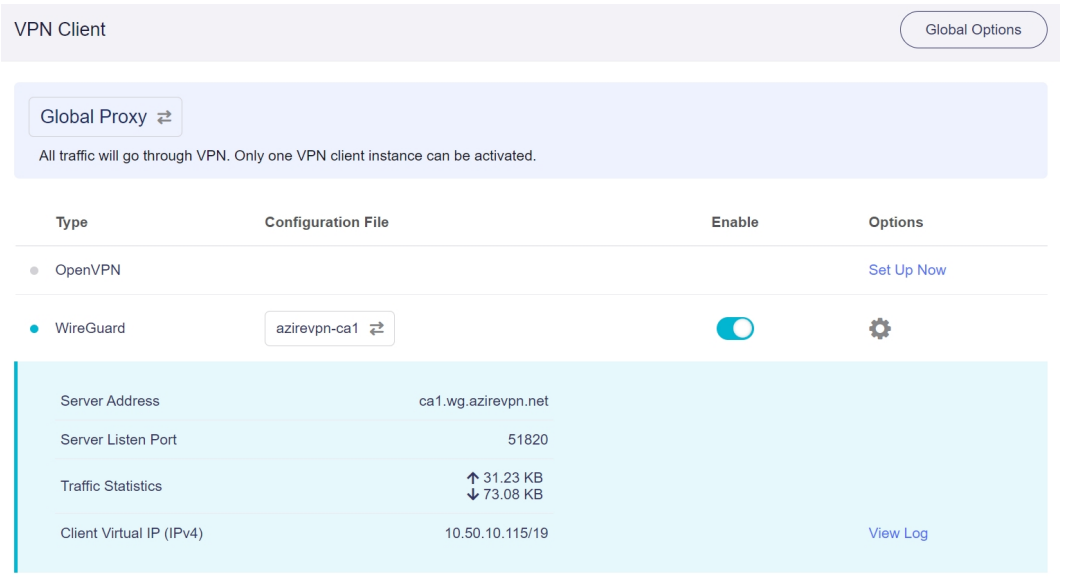
Aby sprawdzić poszczególne elementy, przełącz się do trybu Item, sprawdź szczegóły konfiguracji, a następnie kliknij **Apply**.



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 11

Tor

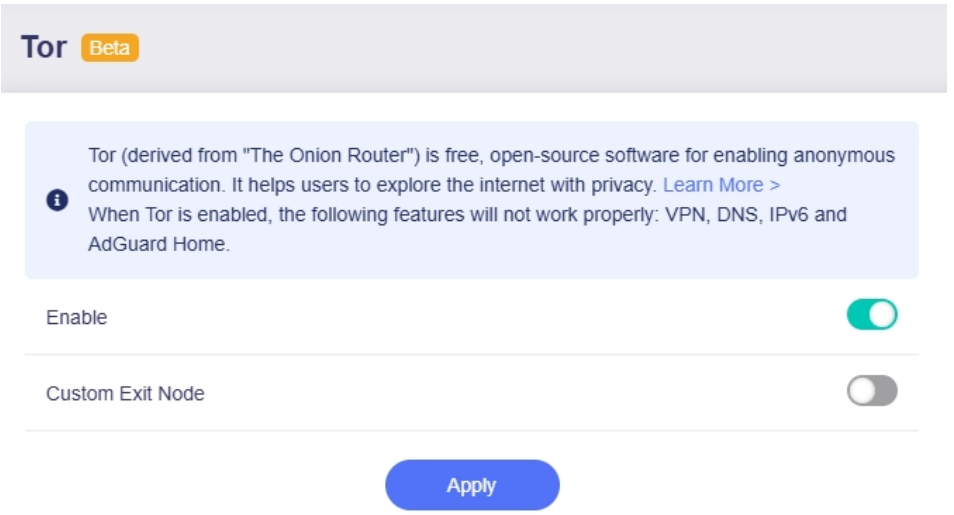
W tym rozdziale krótko przedstawiono Tor (The Onion Router), bezpłatne oprogramowanie o otwartym kodzie źródłowym umożliwiające anonimową komunikację.

Tor (od nazwy **The Onion Router**) to bezpłatne oprogramowanie o otwartym kodzie źródłowym umożliwiające anonimową komunikację. Pomaga przeglądać Internet z zachowaniem prywatności. Ta funkcja jest obecnie w fazie beta i może zawierać błędy.

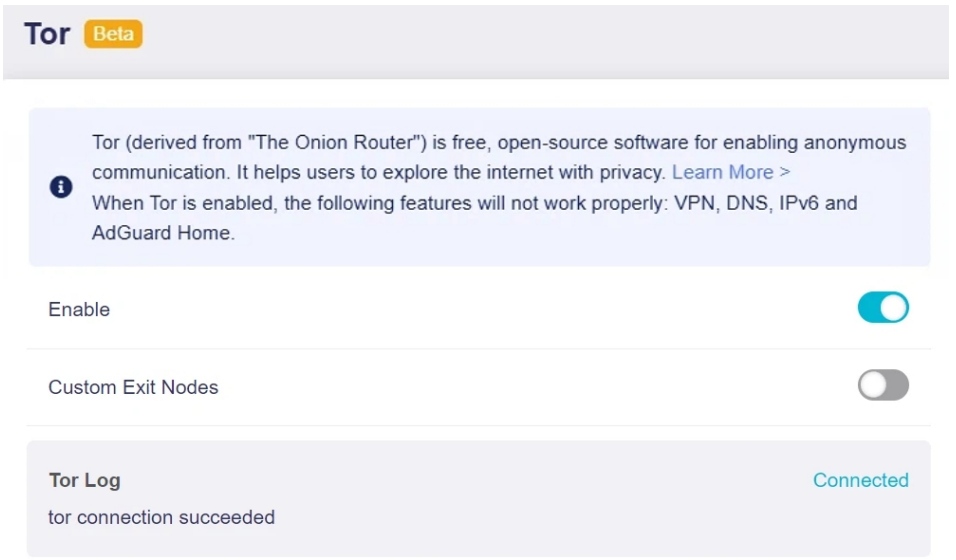
Gdy Tor jest włączony, następujące funkcje nie działają prawidłowo: VPN, DNS, IPv6 i AdGuard Home.

Aby w razie potrzeby skonfigurować Tor, wykonaj poniższe czynności.

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



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


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

Rozdział 12

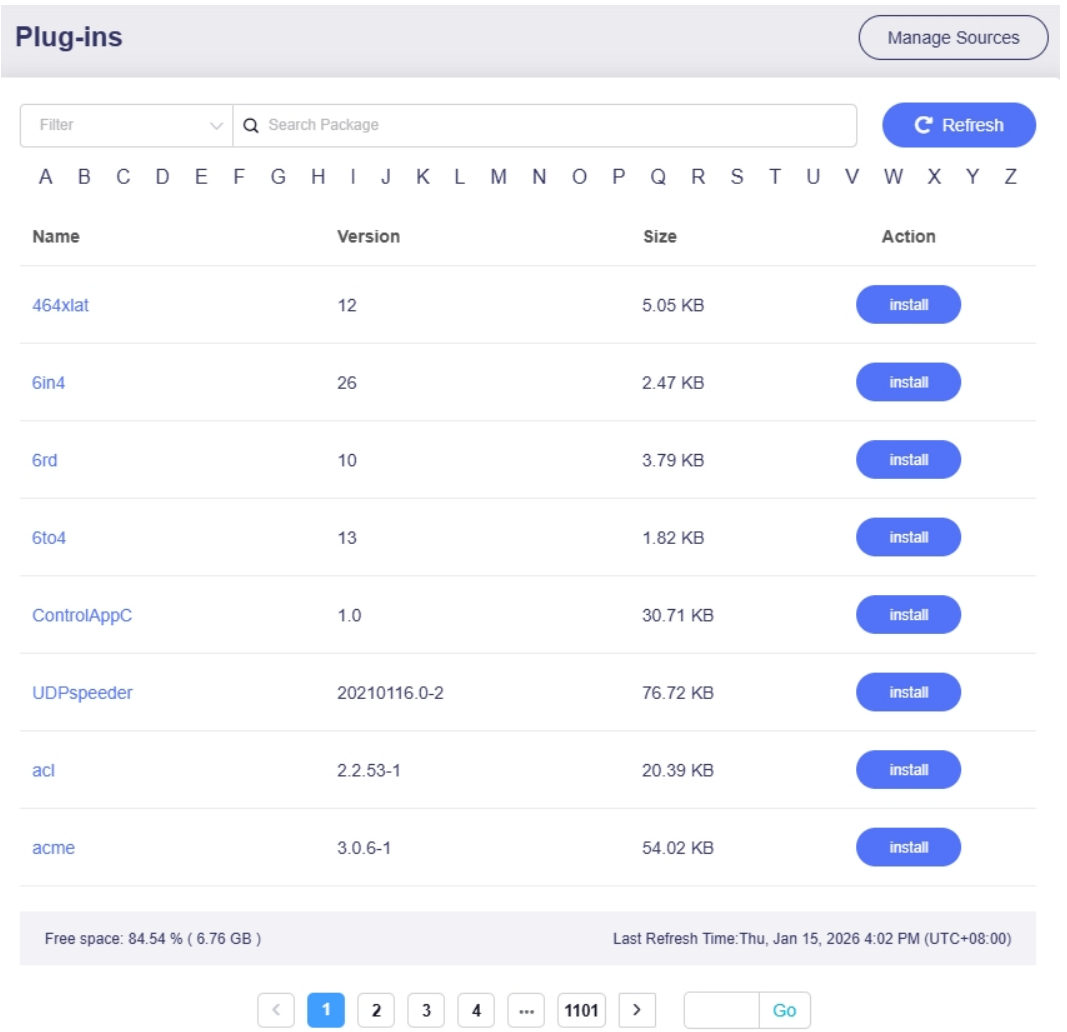
Aplikacje

W tym rozdziale przedstawiono wybrane aplikacje dostępne w routerach GL.iNet, takie jak wtyczki, Dynamic DNS, GoodCloud, AdGuard Home, kontrola rodzicielska, ZeroTier i Tailscale.

12.1 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:

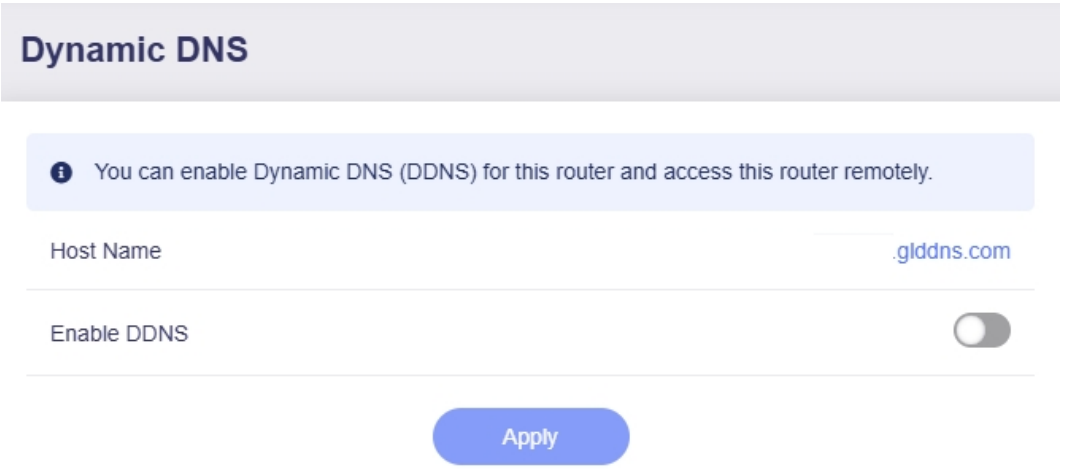
1. Nie zaleca się aktualizowania wtyczek zainstalowanych fabrycznie w oficjalnym oprogramowaniu GL.iNet, takich jak nginx, adguard home, tailscale itp.
2. Wtyczki zewnętrzne zainstalowane ręcznie przez użytkownika można aktualizować, jednak GL.iNet nie odpowiada za związane z nimi problemy z bezpieczeństwem.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

12.2 Dynamiczny DNS

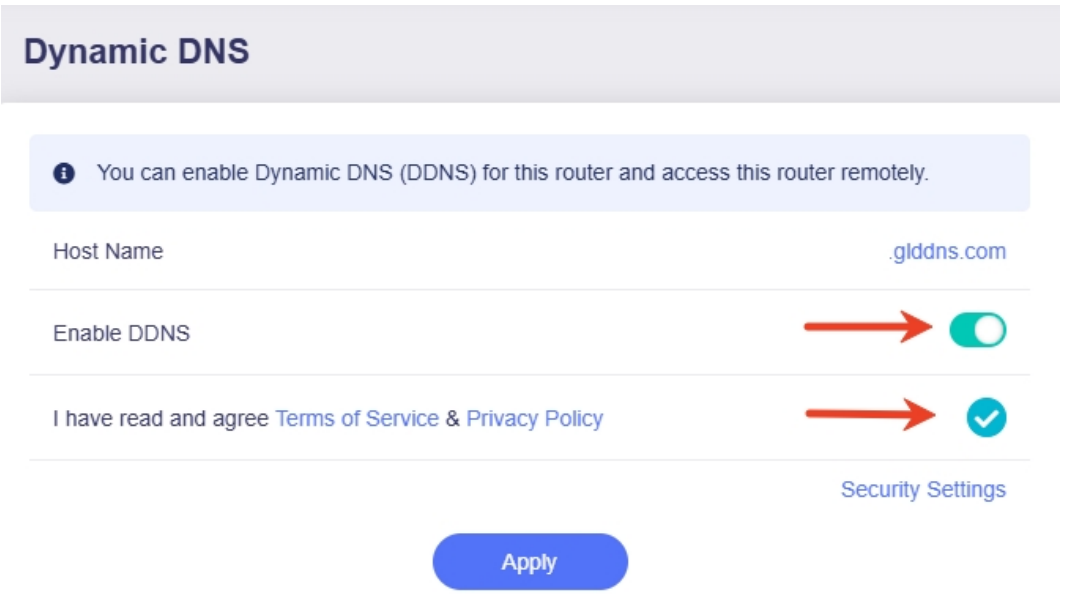
Dynamic Domain Name Service (DDNS, czyli dynamiczny DNS) to usługa mapująca nazwę domeny na dynamiczny adres IP urządzenia sieciowego. Dzięki niej można zdalnie uzyskiwać dostęp do routera. Ta funkcja wymaga publicznego adresu IP.

12.2.1 Włączanie DDNS

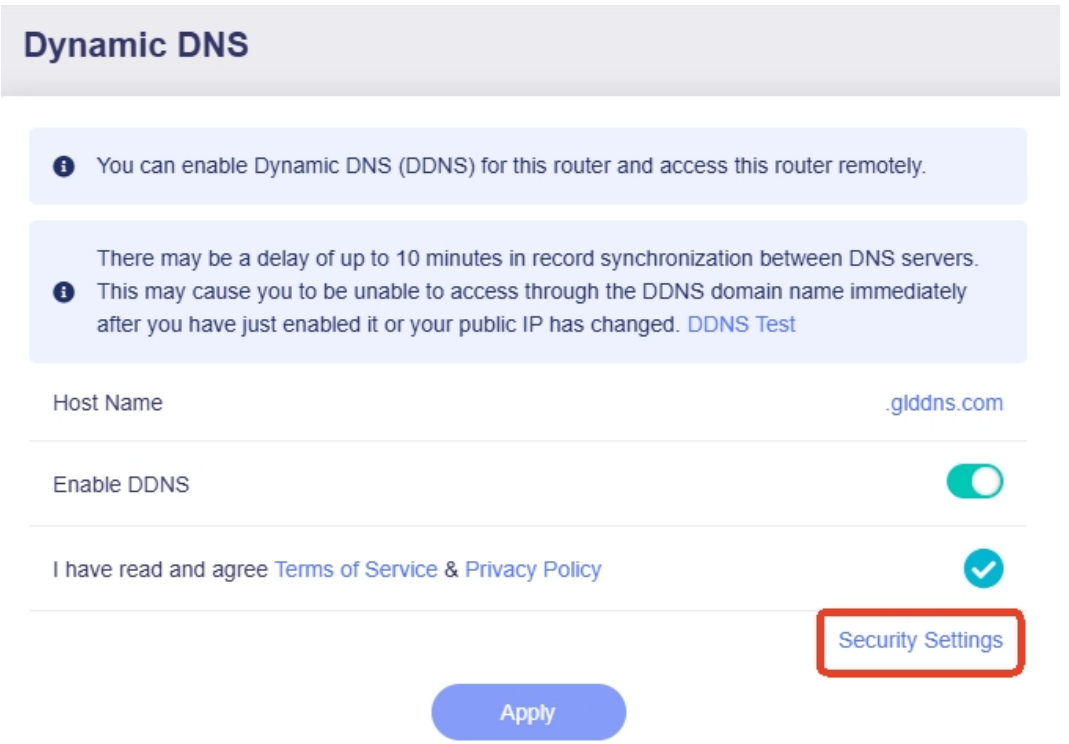
1. Zaloguj się do panelu administracyjnego routera i przejdź do **APPLICATIONS** > **Dynamic DNS**. Strona wygląda jak poniżej.



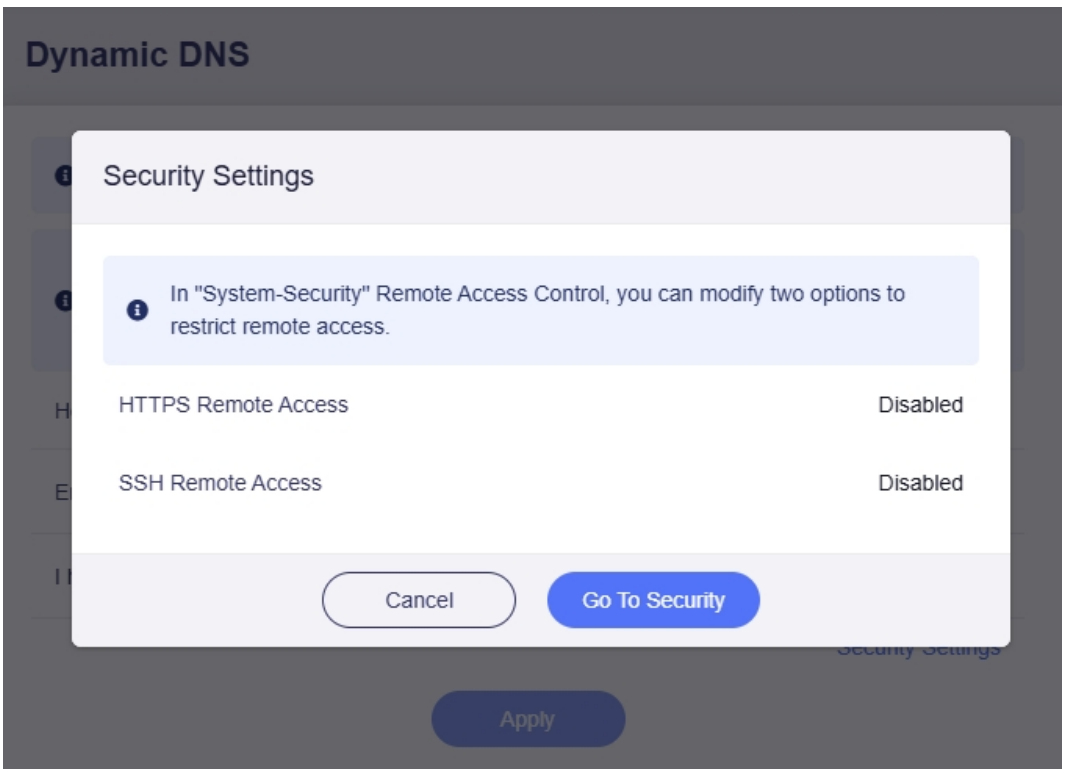
2. Włącz **Enable DDNS**, przeczytaj i zaakceptuj **Terms of Services & Privacy Policy**, a następnie kliknij **Apply**.



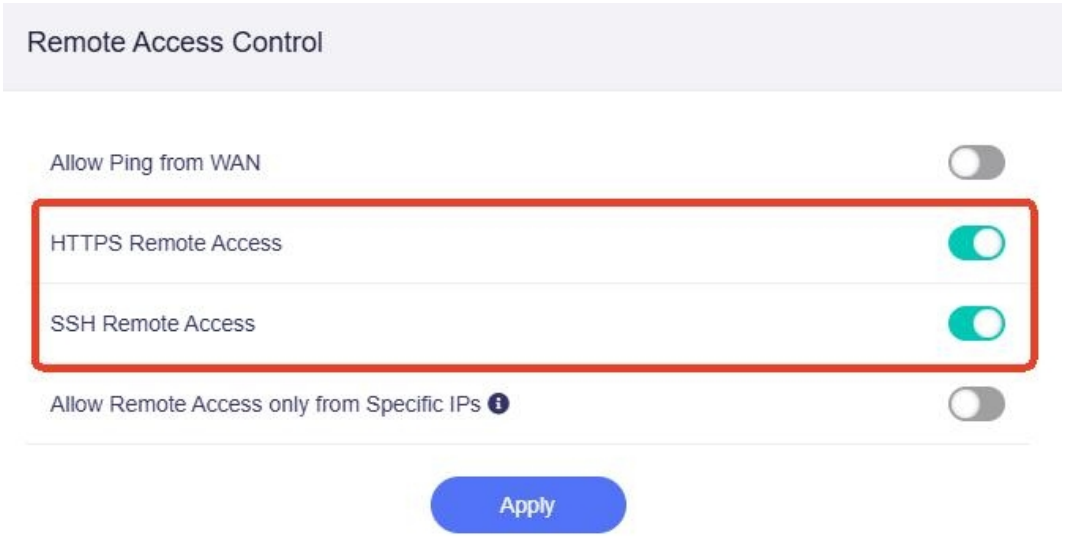
3. Kliknij **Security Settings** w prawym dolnym rogu.



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



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



Uwaga:

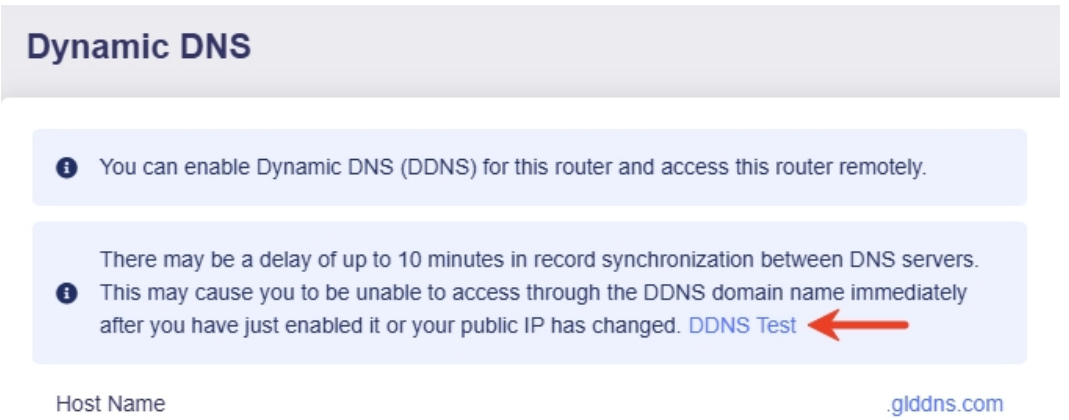
1. Synchronizacja rekordów między serwerami DNS może trwać do 10 minut. Może to uniemożliwić dostęp przez nazwę domeny DDNS bezpośrednio po włączeniu funkcji lub zmianie publicznego adresu IP.
2. Jeśli jednocześnie włączysz DDNS i klienta VPN, upewnij się, że opcja Services From GL.iNet Use VPN jest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

12.2.2 Sprawdzanie działania DDNS

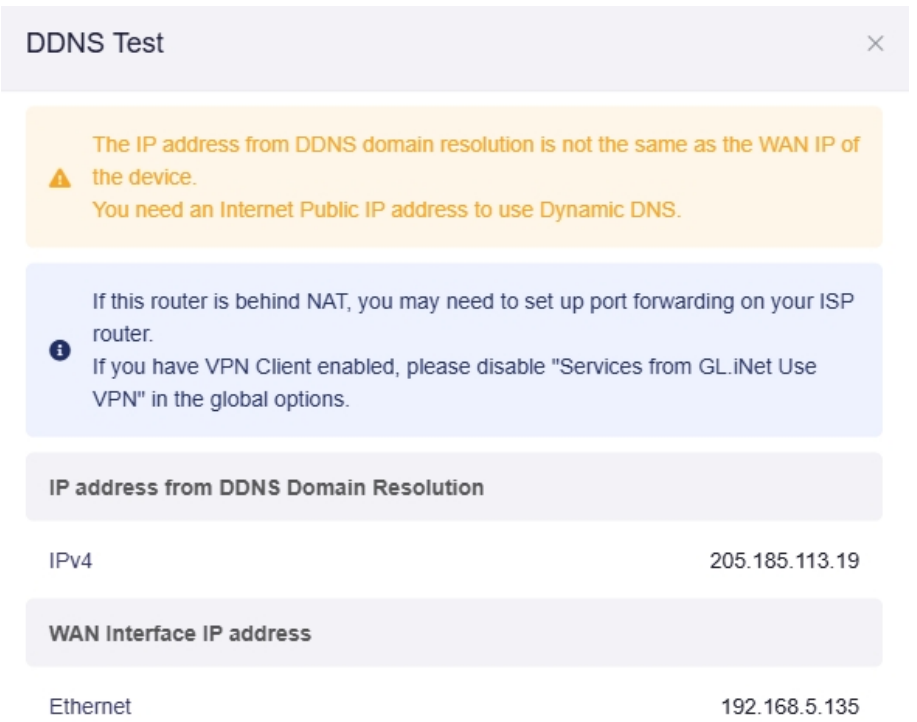
Działanie DDNS można sprawdzić za pomocą narzędzia testowego DDNS lub ręcznie, przy użyciu poleceń.

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, jak pokazano poniżej.



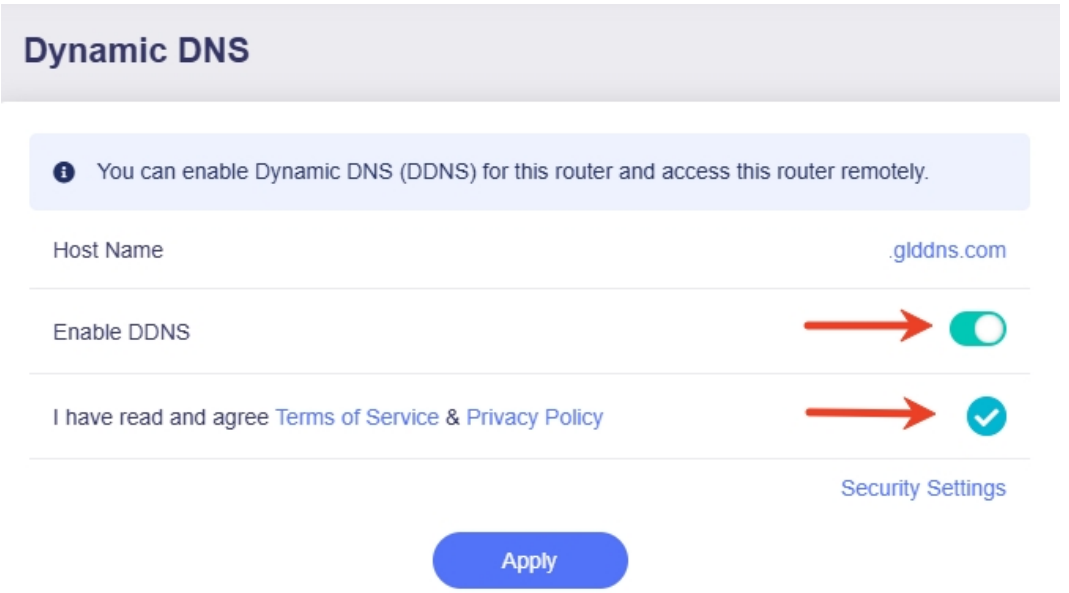
   - Zastąp „xxxxxxx.glddns.com” na powyższej ilustracji własną nazwą hosta.
   - „8.8.8.8” to serwer DNS Google. Użyj go lub zastąp innym adresem, a następnie naciśnij Enter.
2. Jeśli otrzymasz publiczny adres IP, taki jak „183.178.10.100” na powyższej ilustracji, domena DDNS została prawidłowo powiązana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

12.2.3 Zdalny dostęp przez HTTPS

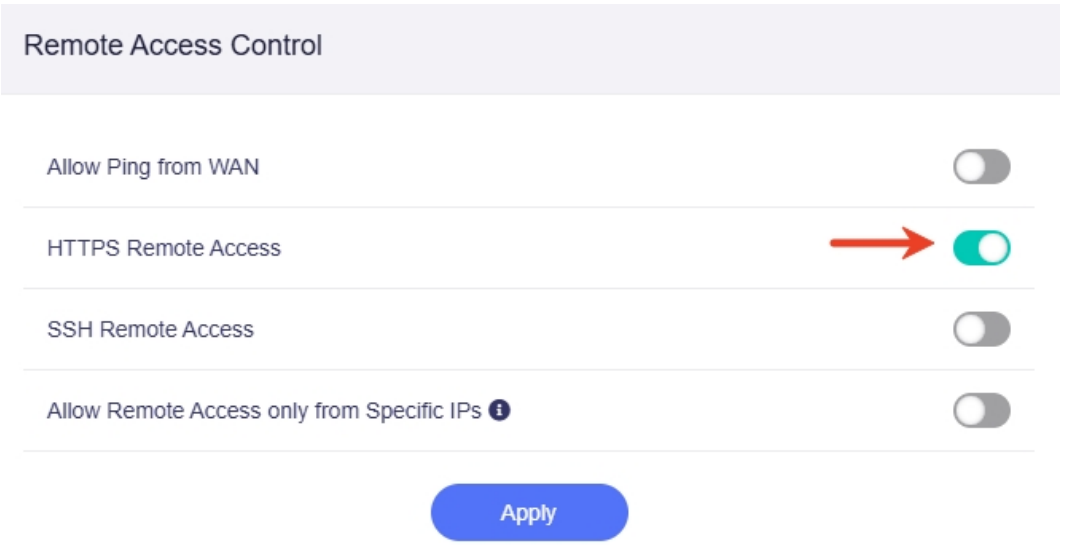
Do zdalnego dostępu przez HTTPS wymagany jest **publiczny adres IP**. Kliknij tutaj, aby sprawdzić, czy dostawca Internetu przydziela taki adres. Jeśli router znajduje się za NAT, skonfiguruj przekierowanie portów (**port 443**) na routerze nadrzędnym dla dostępu HTTPS.

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

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

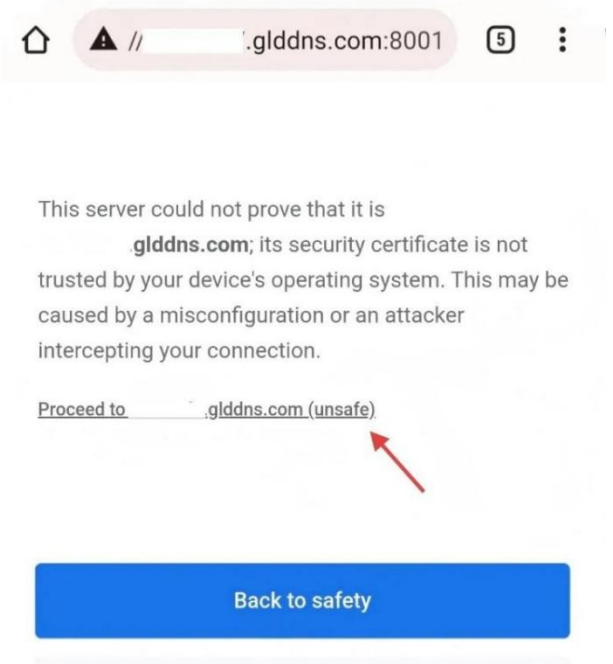


2. W panelu administracyjnym przejdź do **SYSTEM** > **Security** > **Remote Access Control**. Włącz **HTTPS Remote Access** i kliknij **Apply**.



3. 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** .



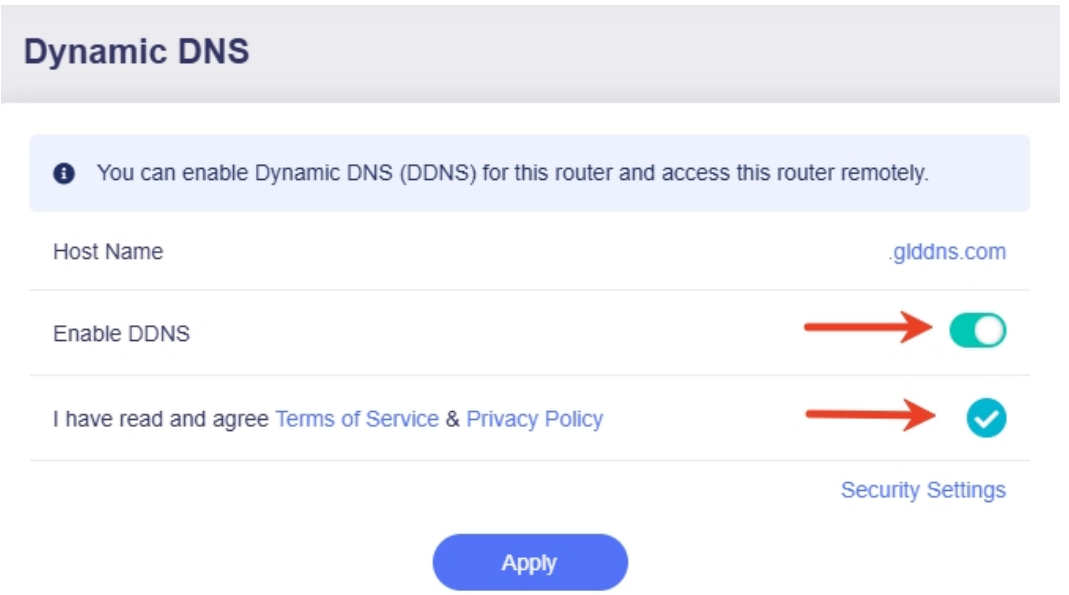
Możesz teraz uzyskiwać dostęp do panelu administracyjnego routera za pomocą nazwy hosta DDNS przez **HTTPS**.

12.2.4 Zdalny dostęp przez SSH

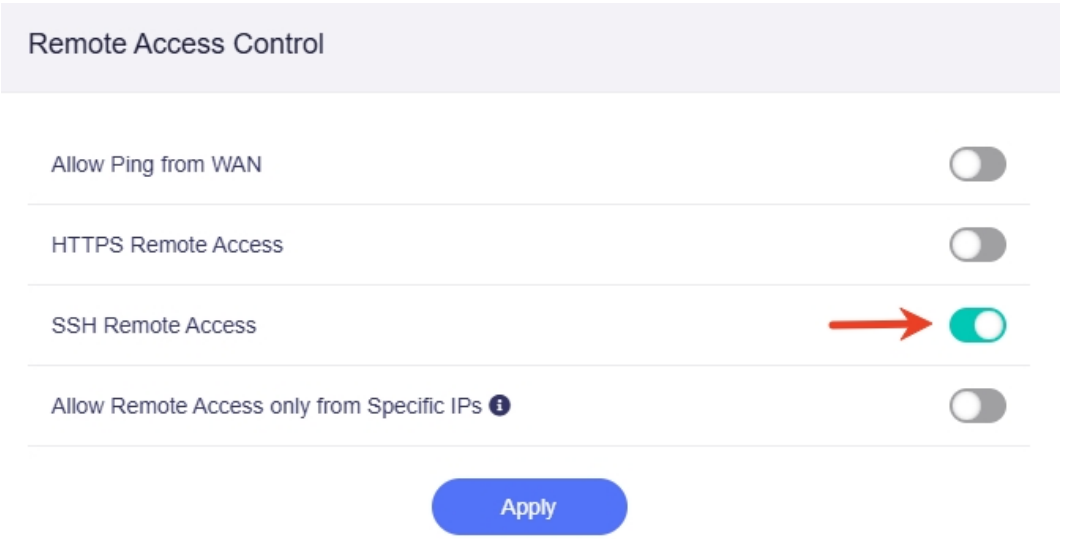
Do zdalnego dostępu przez SSH wymagany jest **publiczny adres IP**. Kliknij tutaj, aby sprawdzić, czy dostawca Internetu przydziela taki adres. Jeśli router znajduje się za NAT, skonfiguruj przekierowanie portów (**port 22**) na routerze nadrzędnym dla zdalnego dostępu SSH.

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

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



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



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

12.3 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.

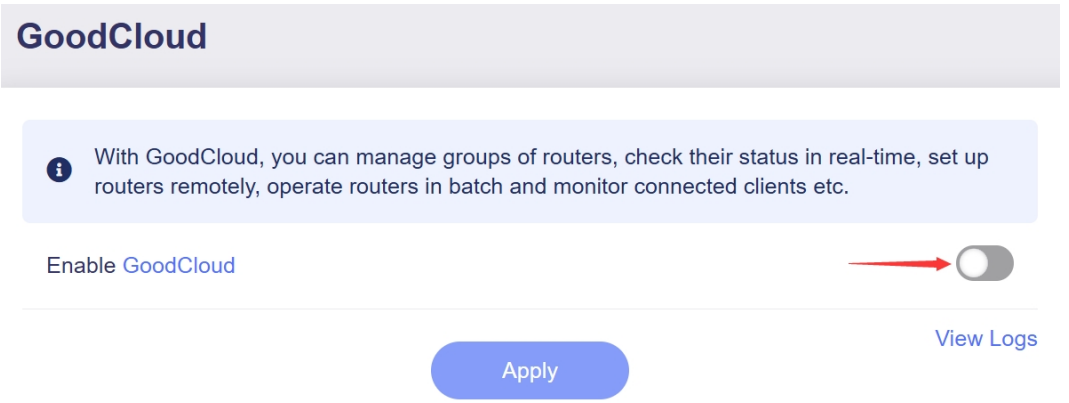
Dzięki GoodCloud możesz:

- 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

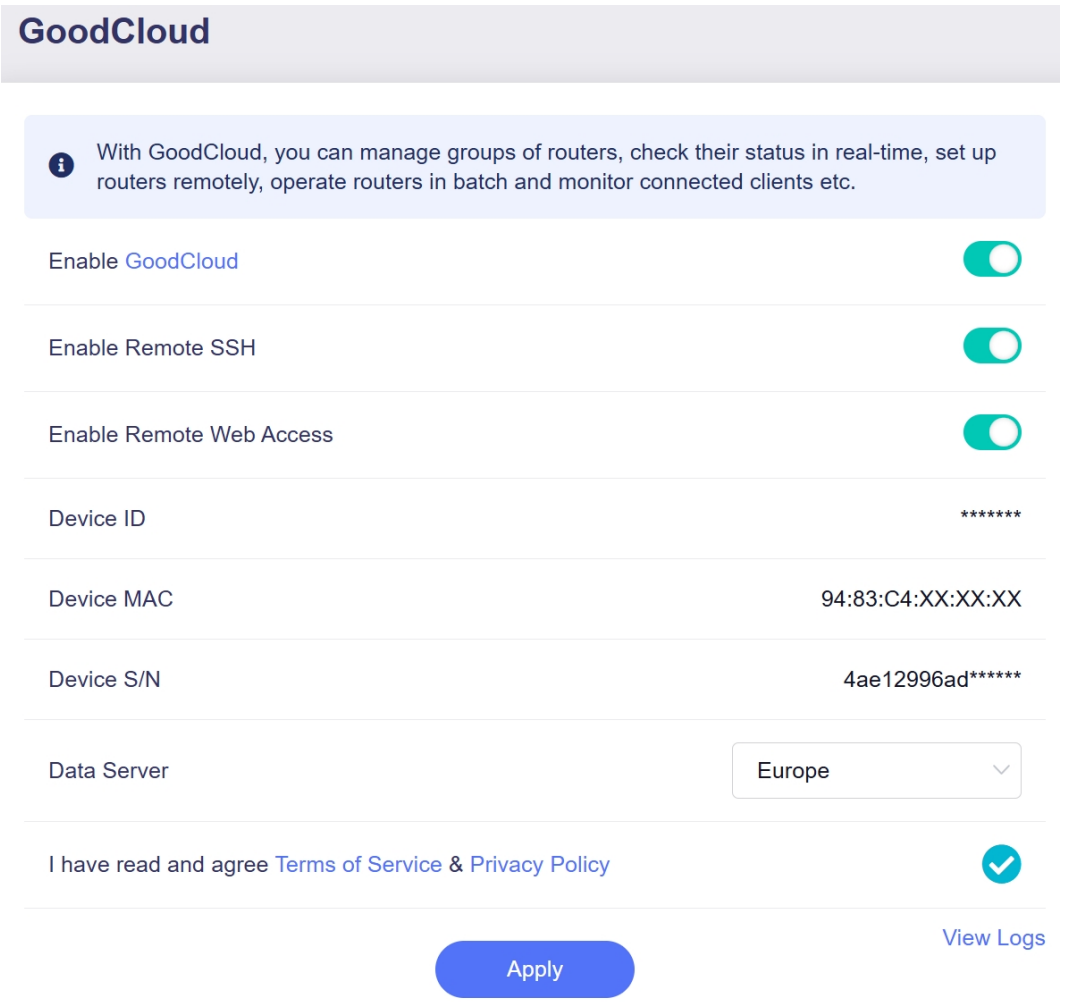
Niektóre funkcje są dostępne w planach Enterprise i VAR (Value Added Reseller). Szczegóły znajdziesz tutaj.

12.3.1 Włączanie GoodCloud

1. Zaloguj się do panelu administracyjnego routera i przejdź do **APPLICATIONS** > **GoodCloud**. Włącz GoodCloud przełącznikiem.

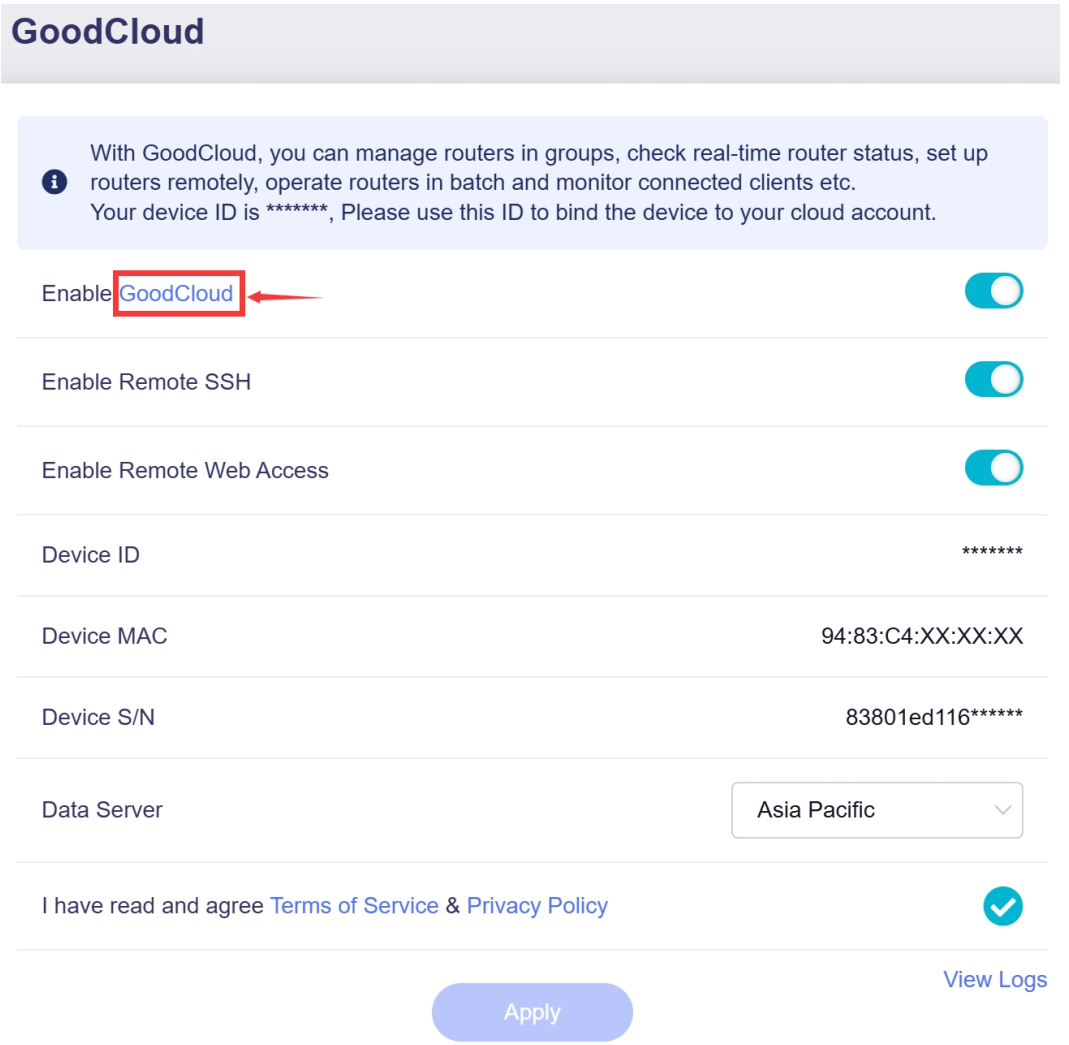


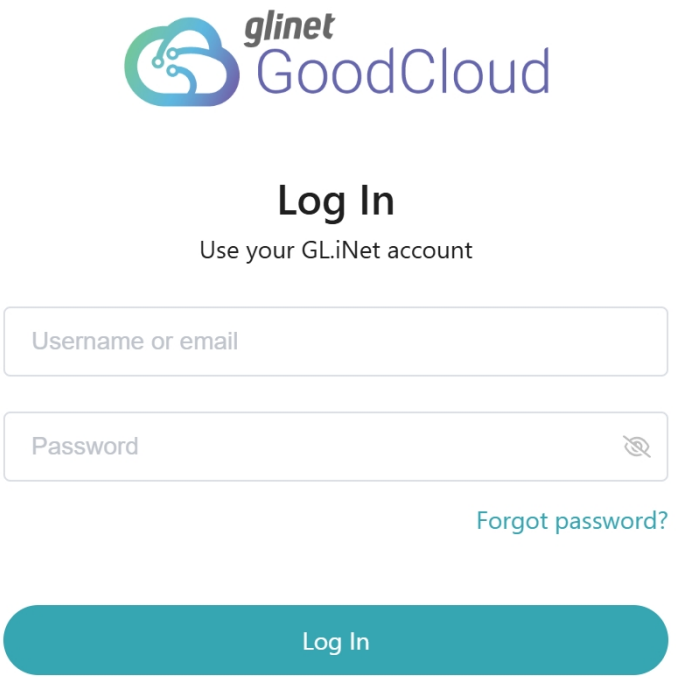
W razie potrzeby włącz **Remote SSH** i **Remote Web Access**, wybierz najbliższy serwer, przeczytaj i zaakceptuj **Terms of Service & Privacy Policy**, a następnie kliknij **Apply**.



- **Remote SSH**: umożliwia zdalny dostęp do terminala routera przez SSH z platformy GoodCloud.
- **Remote Web Access:** umożliwia zdalny dostęp do panelu administracyjnego routera przez HTTP/HTTPS z platformy GoodCloud.
- **Data Server**: wybierz serwer najbliższy lokalizacji urządzenia. Dostępne są trzy opcje: Azja i Pacyfik (Japonia), Ameryka (Oregon) oraz Europa (Irlandia).
- **View Logs**: otwiera stronę dziennika i wyświetla dziennik chmury.

2. Kliknij GoodCloud, aby otworzyć stronę logowania, i zaloguj się na konto GL.iNet Cloud. Jeśli nie masz konta, zarejestruj je i zaloguj się. Po zalogowaniu router zostanie automatycznie powiązany z kontem.

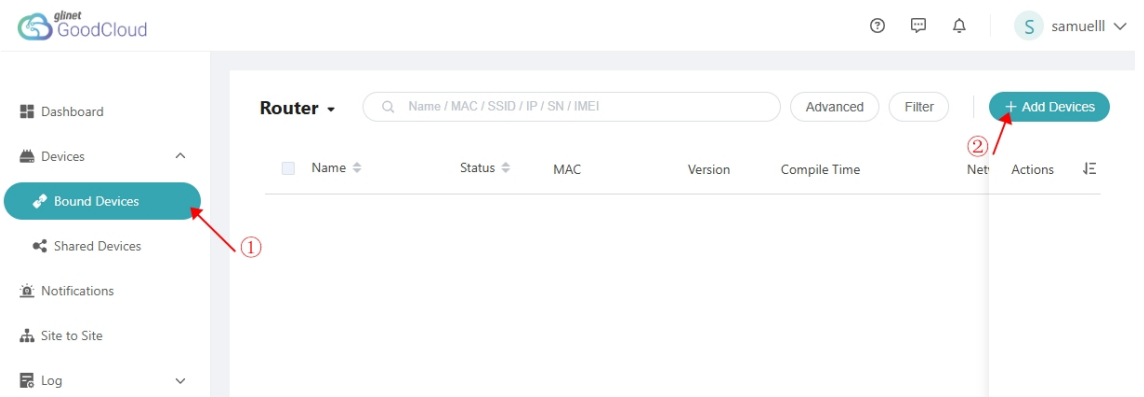




Wskazówki:

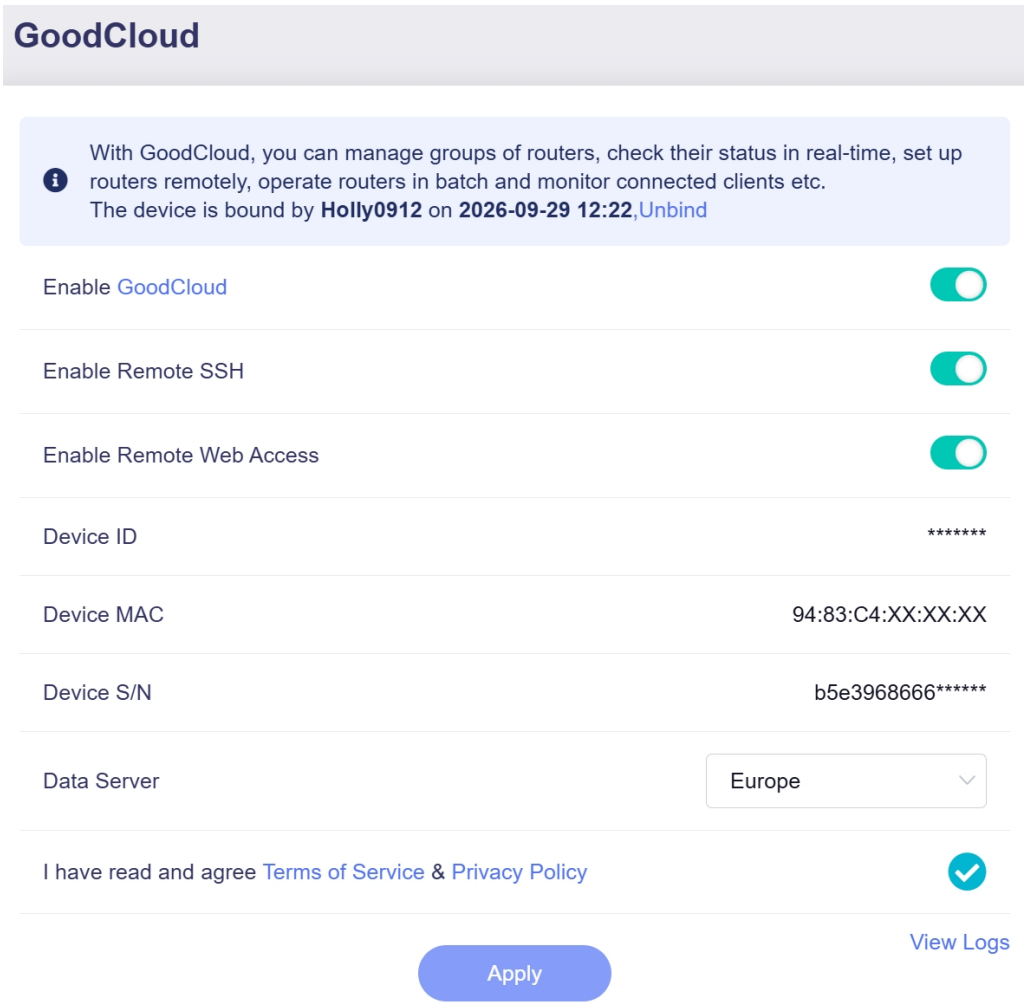
- Sposób powiązania z GoodCloud zależy od wersji oprogramowania.
- Jeśli nie otrzymasz wiadomości weryfikacyjnej, sprawdź folder spamu lub spróbuj później. Aby uzyskać dodatkową pomoc, napisz na support@gl-inet.com.

3. Na platformie chmurowej przejdź do **Devices** > **Bound Devices** > **Add Devices**.



Urządzenie można powiązać z kontem GoodCloud na trzy sposoby: Auto Discover, Manually Add i Bulk Import. Więcej informacji znajdziesz tutaj.

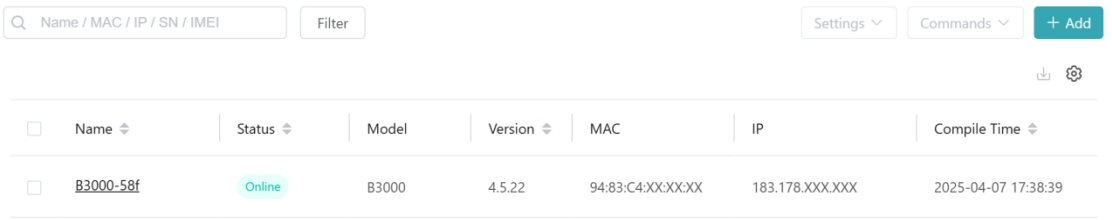
4. Po pomyślnym powiązaniu wróć do panelu administracyjnego routera i przejdź do **APPLICATIONS** > **GoodCloud**. Strona wyświetla szczegóły powiązania, w tym nazwę użytkownika i czas powiązania.


GoodCloud
With GoodCloud, you can manage groups of routers, check their status in real-time, set up routers remotely, operate routers in batch and monitor connected clients etc.
The device is bound by Holly0912 on 2026-09-29 12:22,Unbind
Enable GoodCloud
Enable Remote SSH
Enable Remote Web Access
Device ID
****
Device MAC
94:83:C4:XX:XX:XX
Device S/N
b5e3968666******
Data Server
Europe
I have read and agree Terms of Service & Privacy Policy
View Logs
Apply

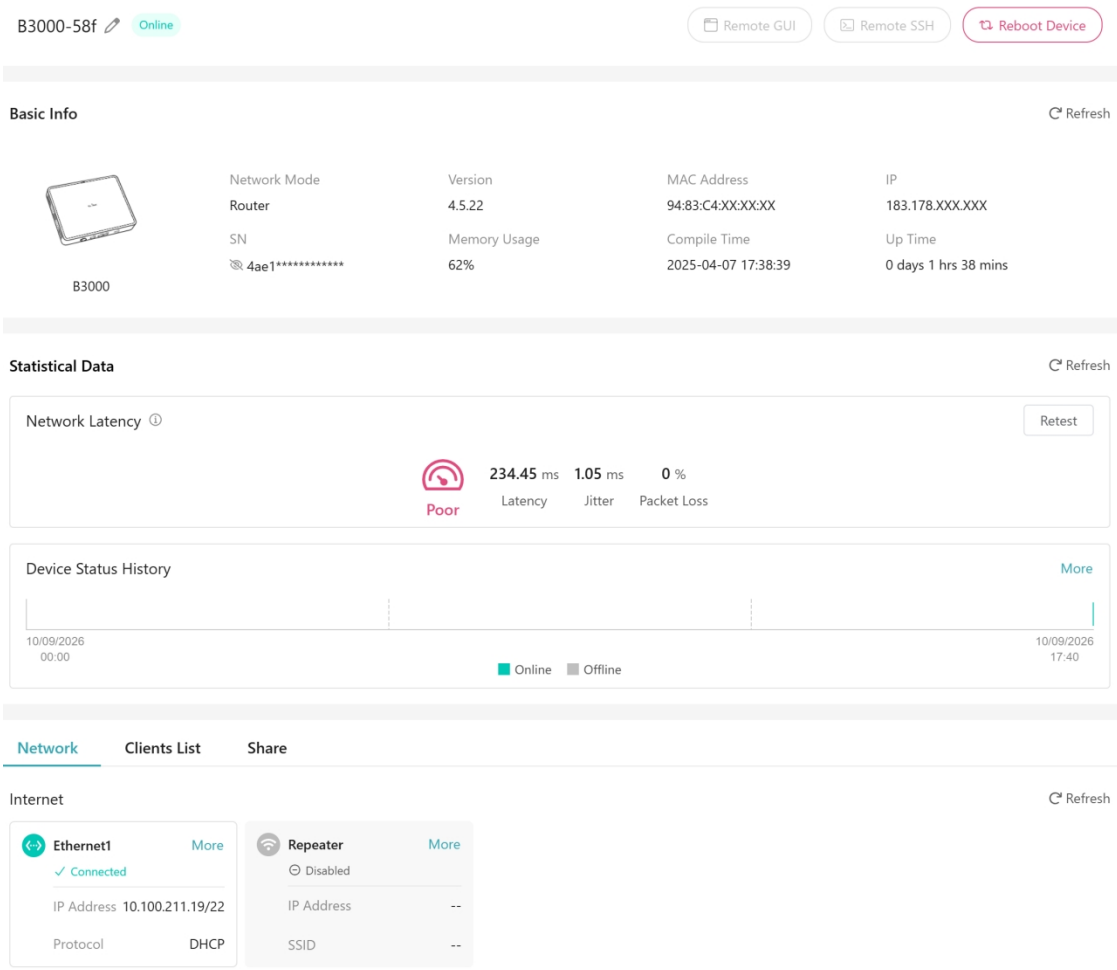
12.3.2 Zarządzanie routerem

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.

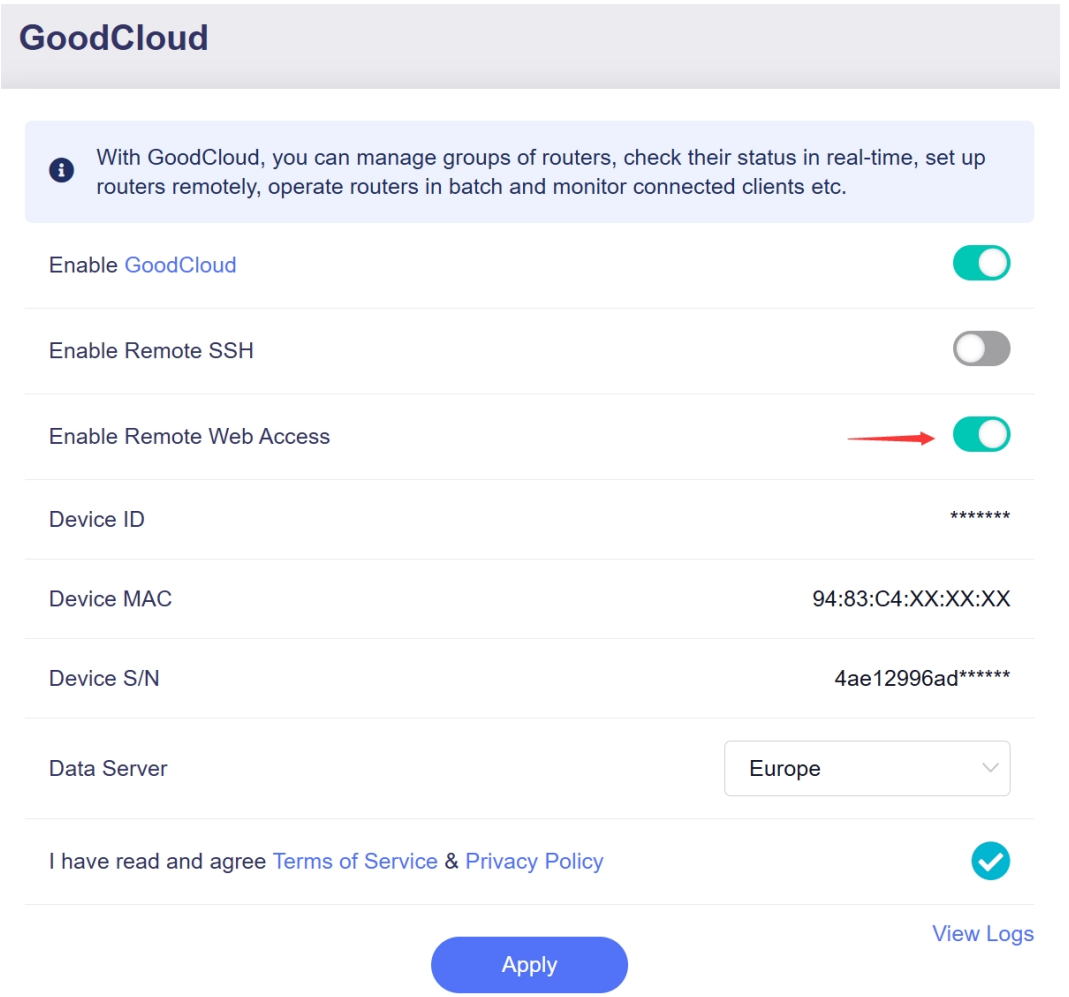


Kliknij nazwę urządzenia, aby otworzyć stronę szczegółów zawierającą podstawowe informacje, statystyki, przegląd sieci, listę klientów i oś czasu. Możesz też wykonywać zaawansowane działania, np. zdalnie uzyskiwać dostęp do routera i uruchamiać go ponownie.

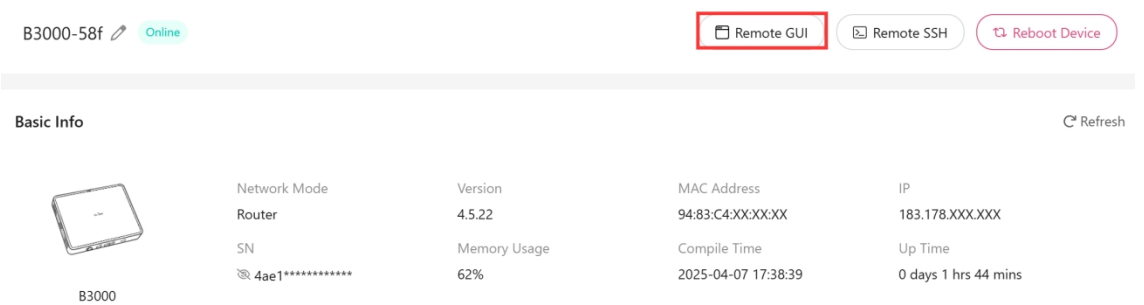

B3000-58f
Online
Remote GUI
Remote SSH
Reboot Device
Basic Info
Refresh
B3000
Network Mode
Router
Version
4.5.22
MAC Address
94:83:C4:XX:XX:XX
IP
183.178.XXX.XXX
SN
4ae1**********
Memory Usage
62%
Compile Time
2025-04-07 17:38:39
Up Time
0 days 1 hrs 38 mins
Statistical Data
Refresh
Network Latency
Retest
Poor
234.45 ms
Latency
1.05 ms
Jitter
0 %
Packet Loss
Device Status History
More
10/09/2026
00:00
10/09/2026
17:40
Online
Offline
Network
Clients List
Share
Internet
Refresh
Ethernet1
More
Connected
IP Address 10.100.211.19/22
Protocol DHCP
Repeater
More
Disabled
IP Address --
SSID --

Zdalny dostęp przez przeglądarkę

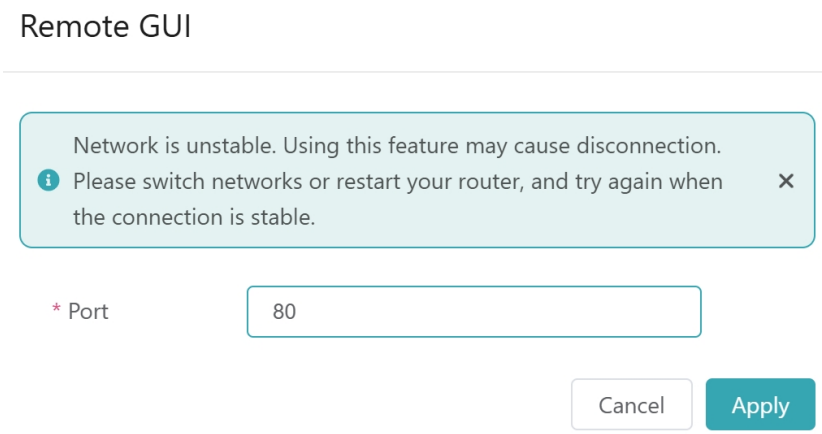
1. Zaloguj się do panelu administracyjnego routera, przejdź do **APPLICATIONS** > **GoodCloud**, włącz **Remote Web Access**, a następnie kliknij **Apply**.



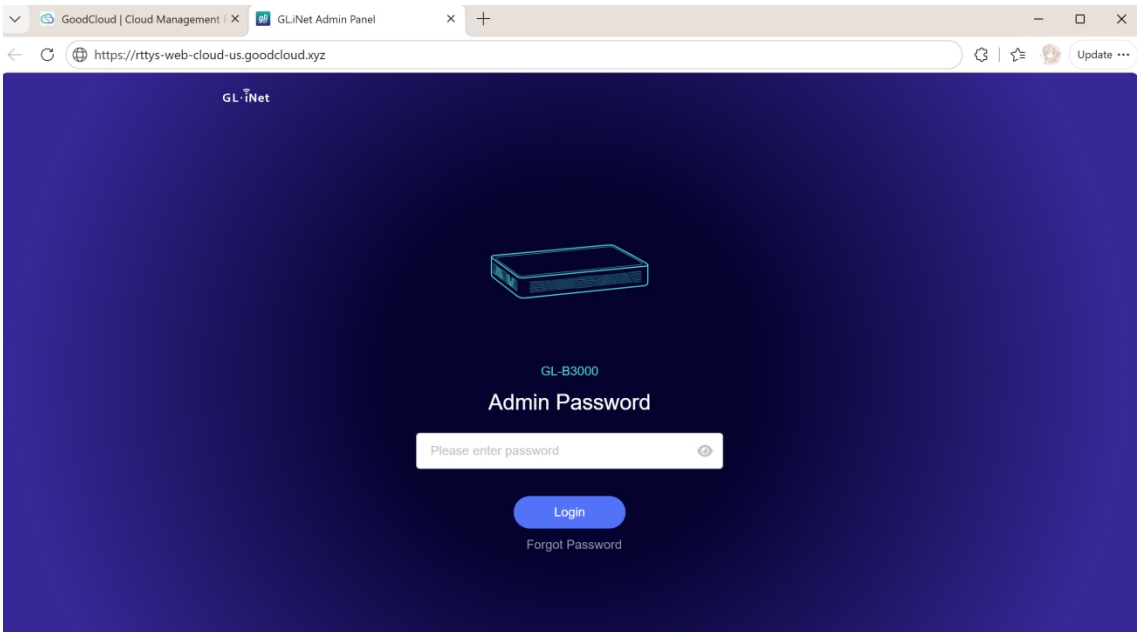
2. Zaloguj się na platformie GoodCloud i przejdź do **Devices** > **Bound Devices**. Kliknij urządzenie, do którego chcesz uzyskać dostęp, aby otworzyć stronę jego szczegółów.
3. Na stronie szczegółów urządzenia kliknij przycisk **Remote GUI** w prawym górnym rogu.



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

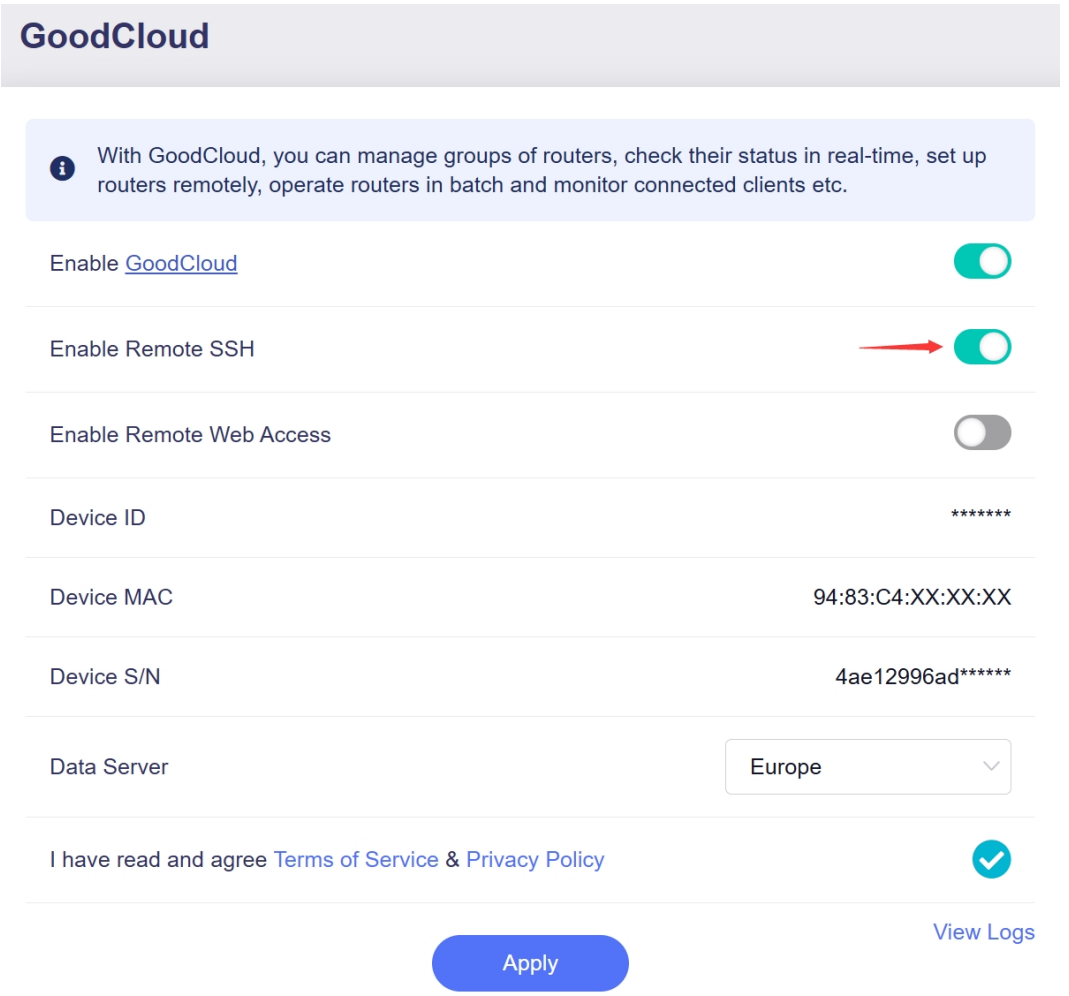


5. Otworzy się strona logowania routera. Wprowadź hasło administratora, aby uzyskać zdalny dostęp do panelu administracyjnego routera.

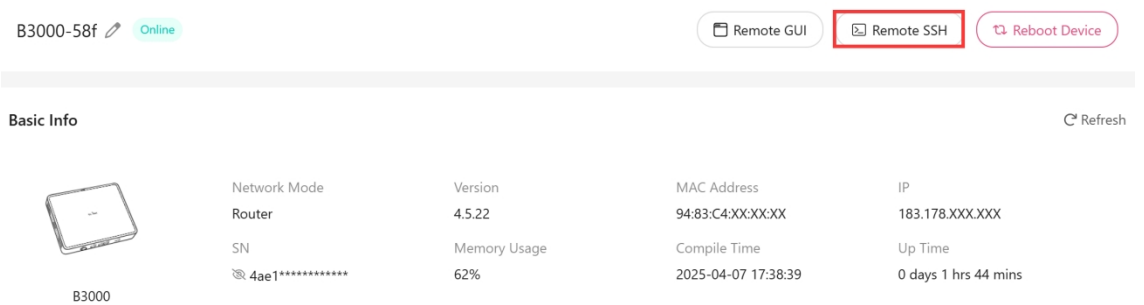


Zdalny dostęp SSH

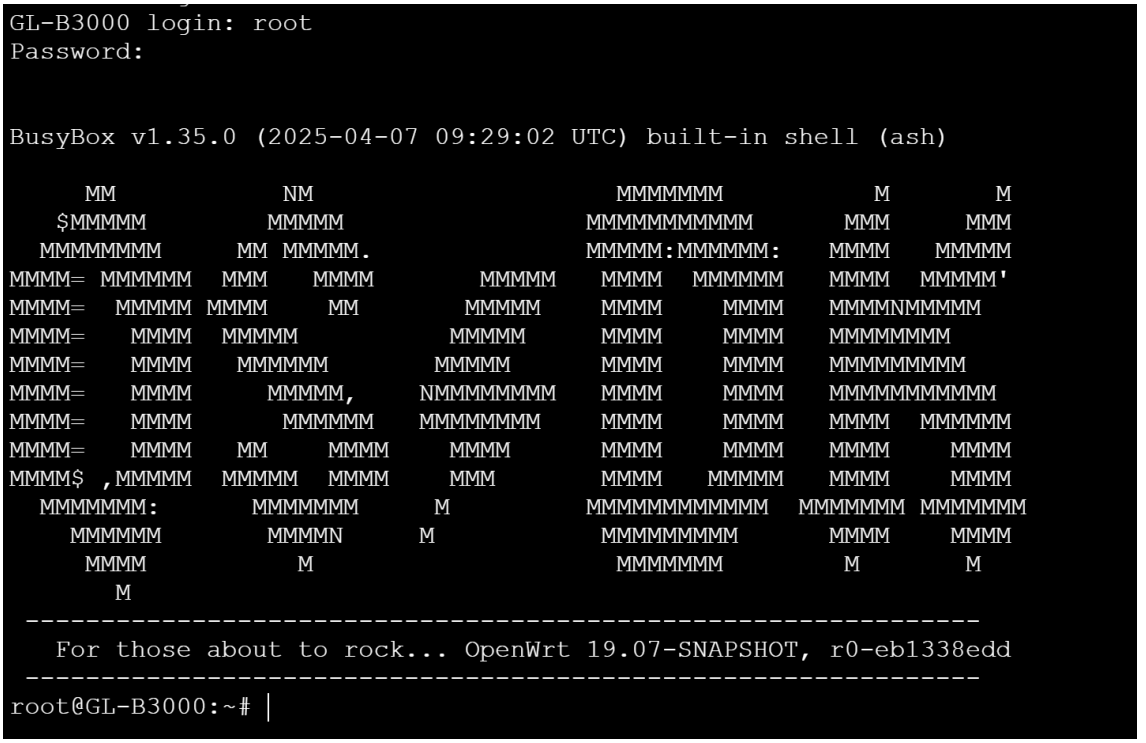
1. Zaloguj się do panelu administracyjnego routera, przejdź do **APPLICATIONS** > **GoodCloud**, włącz **Remote SSH**, a następnie kliknij **Apply**.



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

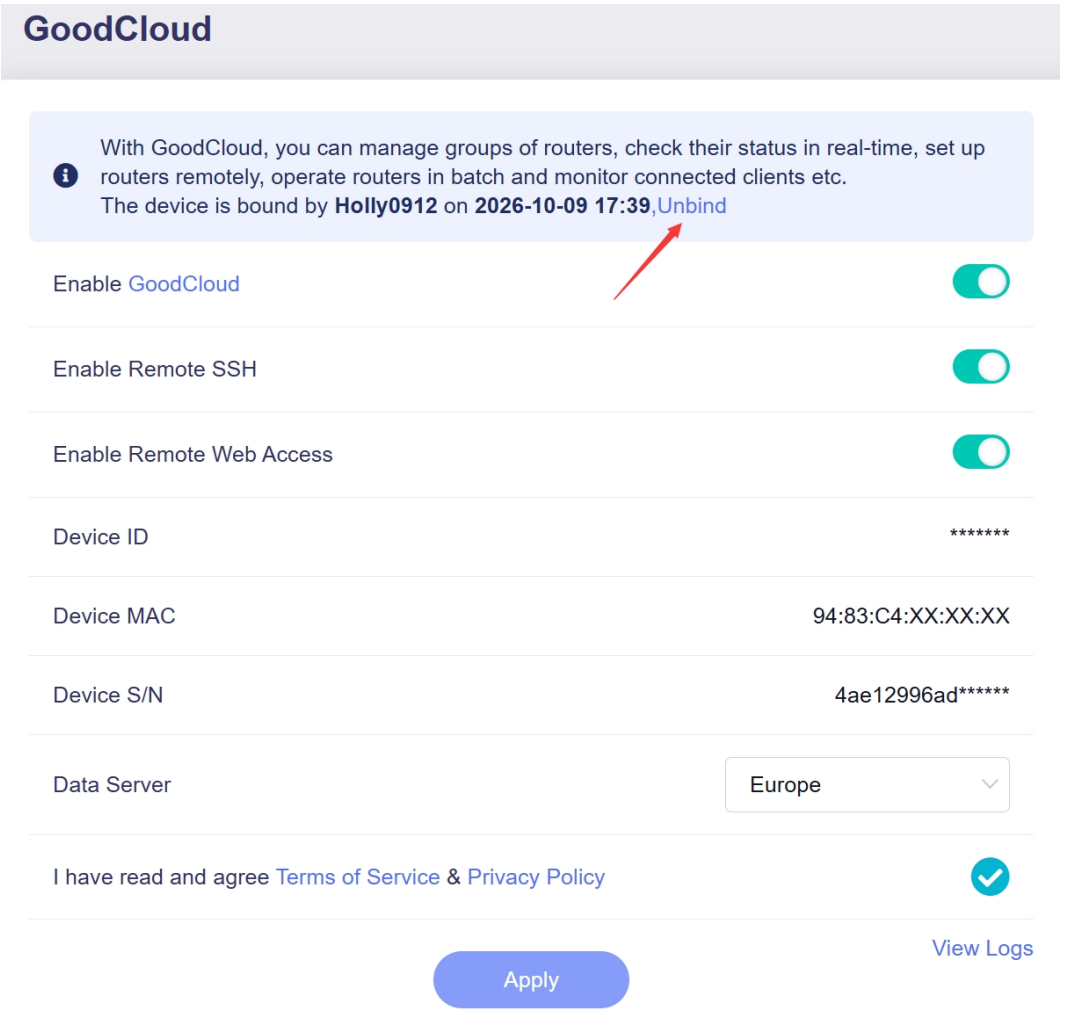


4. Zaloguj się jako **root** i wprowadź hasło, aby uzyskać dostęp do terminala routera.

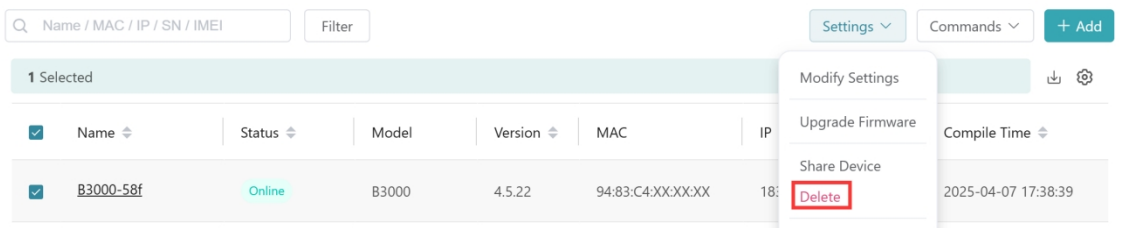


12.3.3 Usuwanie powiązania urządzenia

W panelu administracyjnym routera 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.

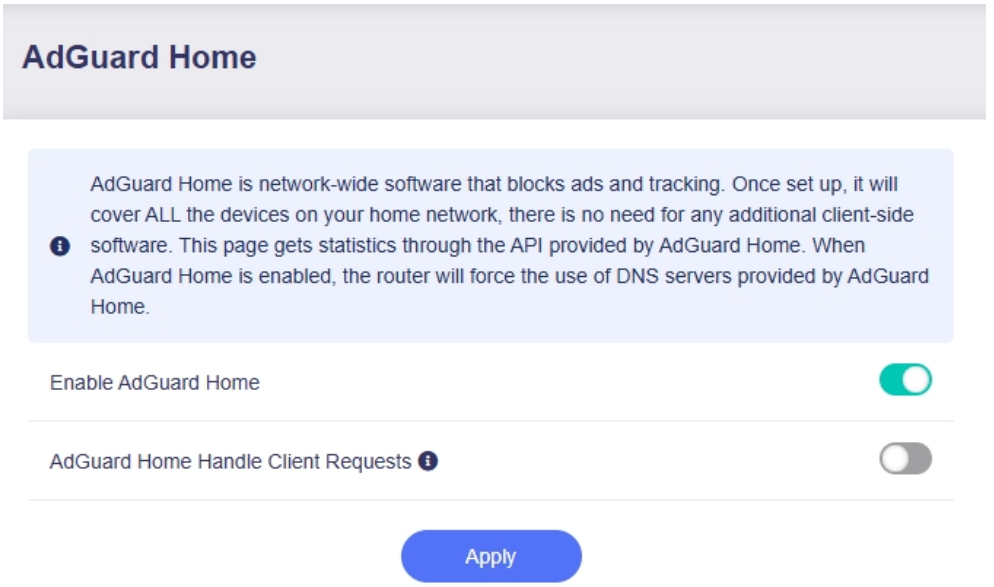


12.4 AdGuard Home

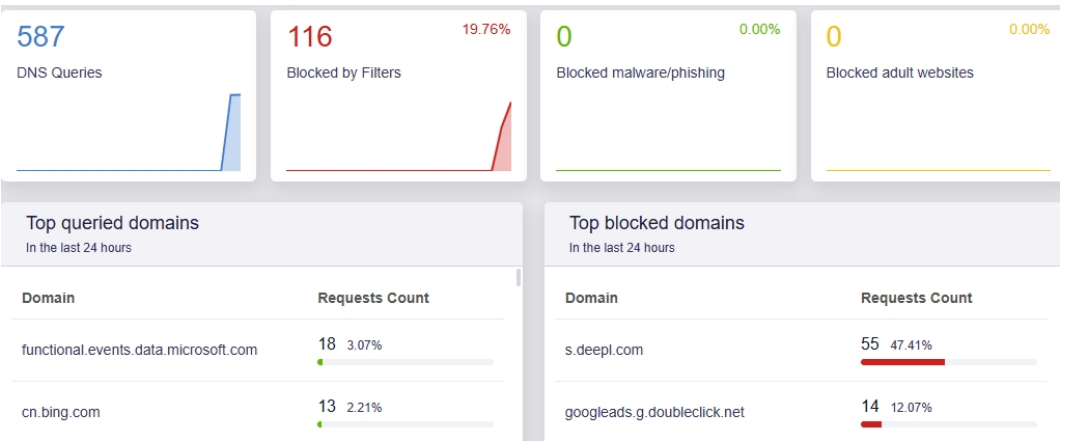
AdGuard Home to oprogramowanie blokujące reklamy i śledzenie w całej sieci. Po konfiguracji obejmuje wszystkie urządzenia klienckie bez konieczności instalowania na nich dodatkowego oprogramowania.

Aby skonfigurować AdGuard Home, wykonaj poniższe czynności.

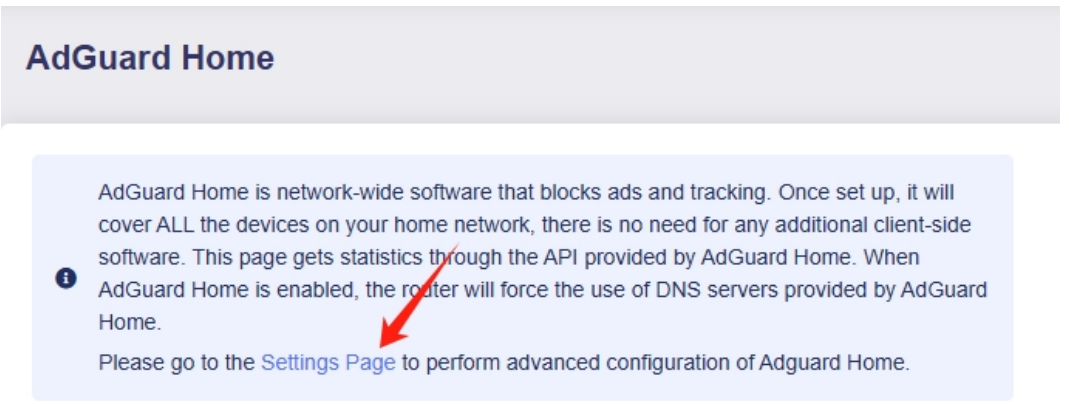
1. Zaloguj się do panelu administracyjnego routera i przejdź do **APPLICATIONS** > **AdGuard Home**. Włącz **Enable AdGuard Home** i kliknij **Apply**.



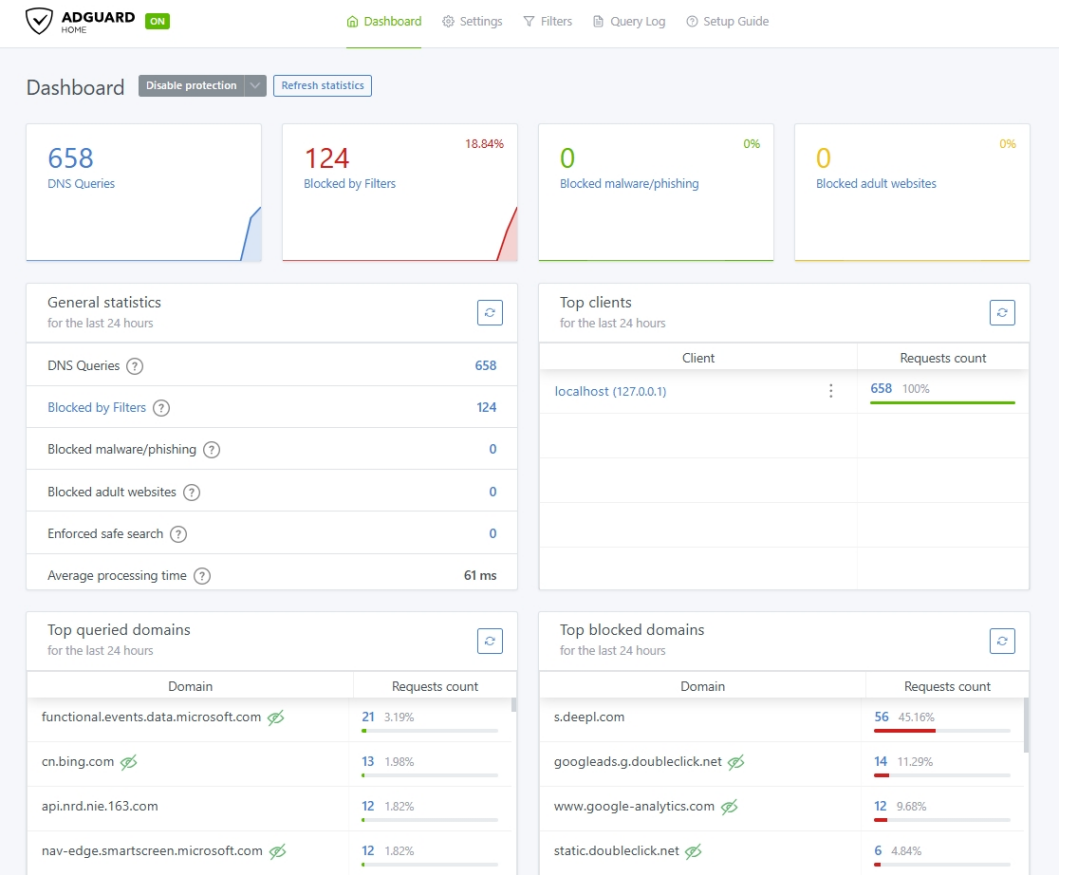
   - **AdGuard Home Handles Client Requests**: po włączeniu zapytania DNS urządzeń klienckich są obsługiwane bezpośrednio przez AdGuard Home, ale powoduje to niedziałanie reguł VPN opartych na domenach.
2. Strona automatycznie pobiera statystyki DNS (zapytania, zablokowane domeny itp.) przez API udostępniane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



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



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



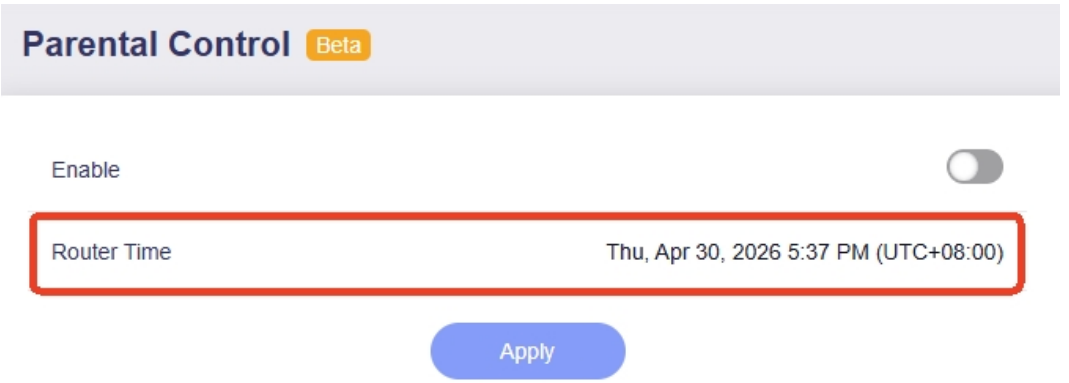
12.5 Kontrola rodzicielska

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

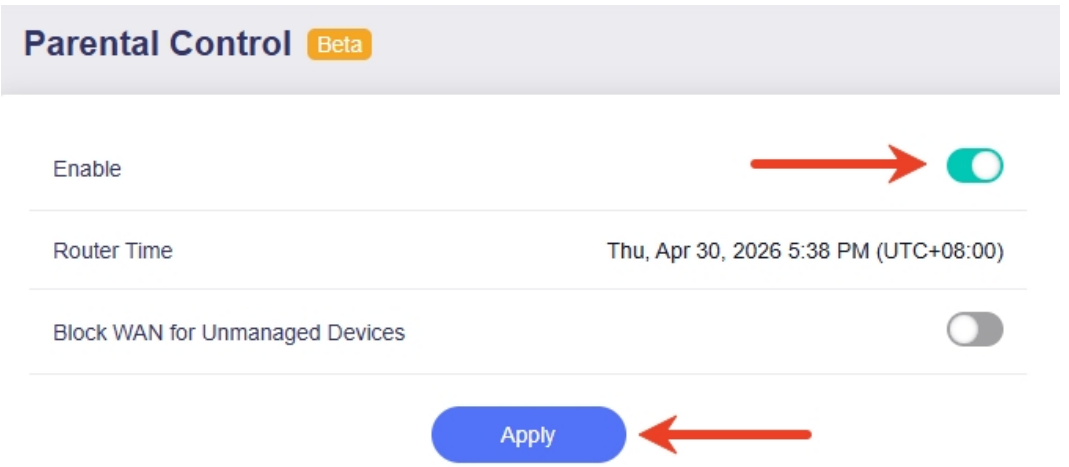
12.5.1 Szybka konfiguracja

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

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



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



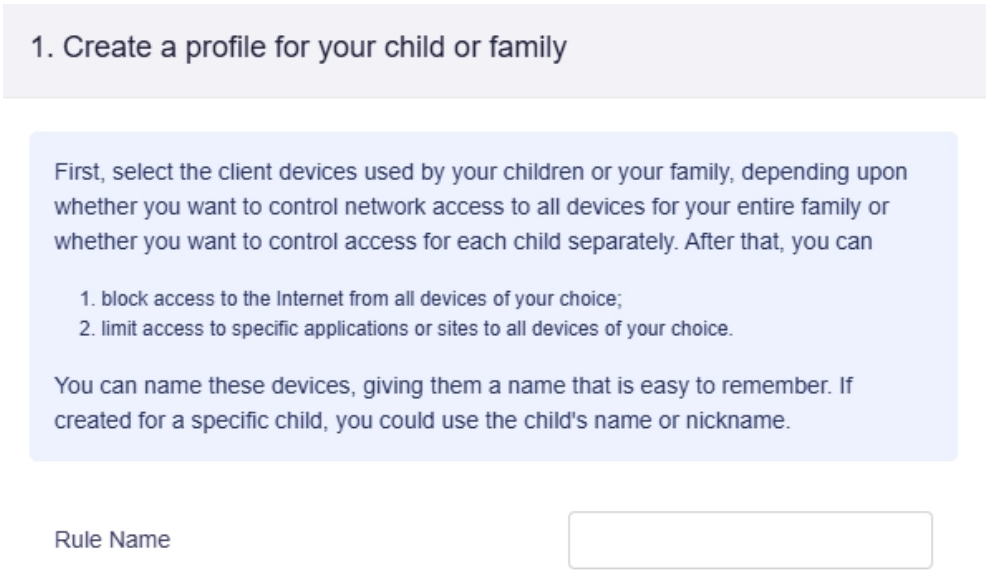
- **Block WAN for Unmanaged Devices**: blokuje dostęp do Internetu wszystkim urządzeniom, których nie ma na liście kontroli rodzicielskiej.

Poniżej przedstawiono przykładowe zastosowanie.

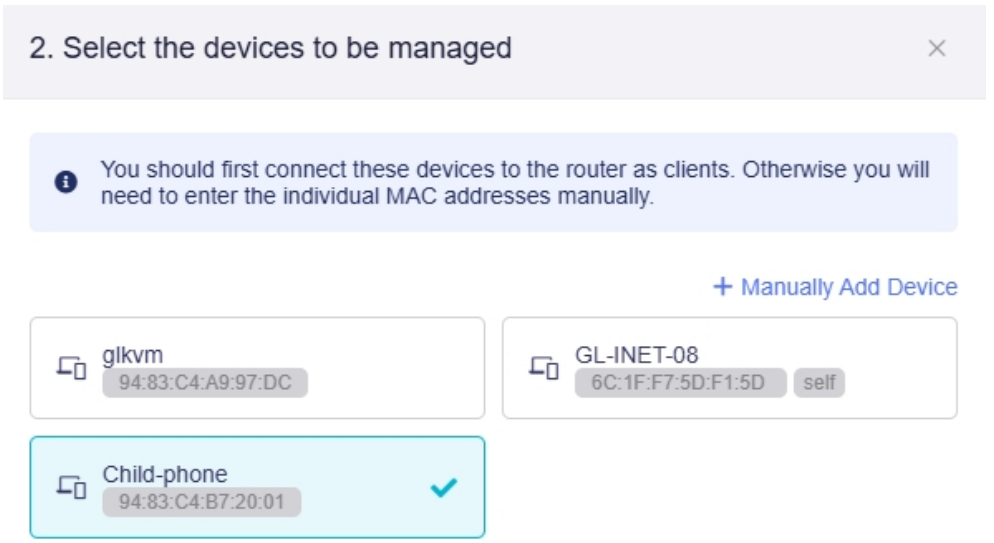
Scenariusz: urządzenia w tym profilu mogą korzystać z Internetu wyłącznie do nauki od 8:00 do 11:00 w dni robocze i do grania od 18:00 do 20:00 w weekendy. W pozostałych godzinach dostęp do Internetu jest domyślnie zablokowany.

Etapy konfiguracji:

1. Utwórz profil i nadaj mu nazwę.

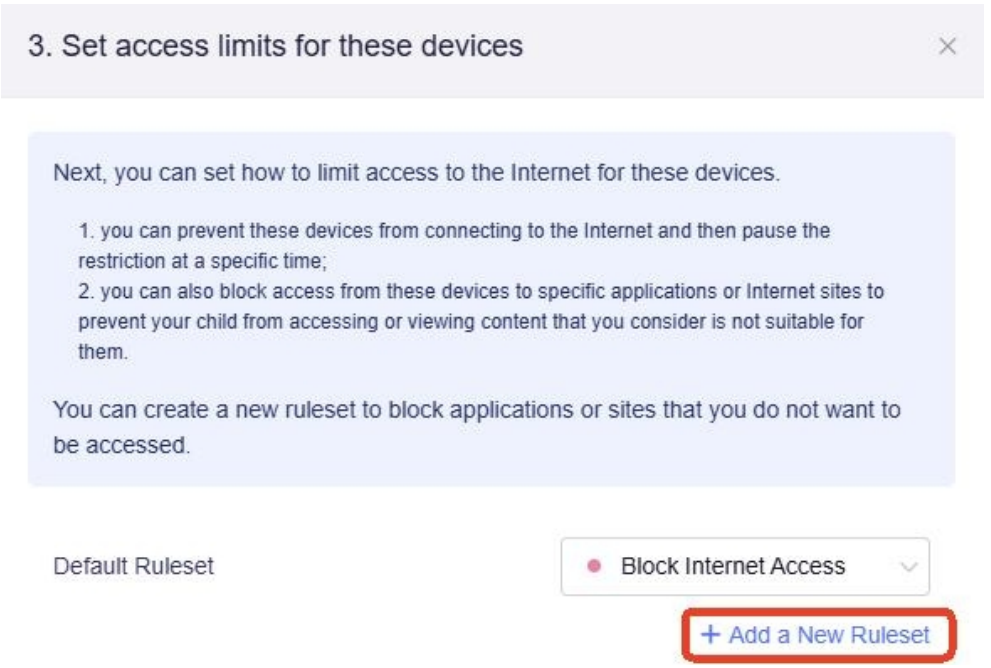


2. Wybierz urządzenia, którymi chcesz zarządzać. Najpierw podłącz je do routera. Jeśli nie były jeszcze podłączane, dodaj je ręcznie, wprowadzając ich adresy MAC.

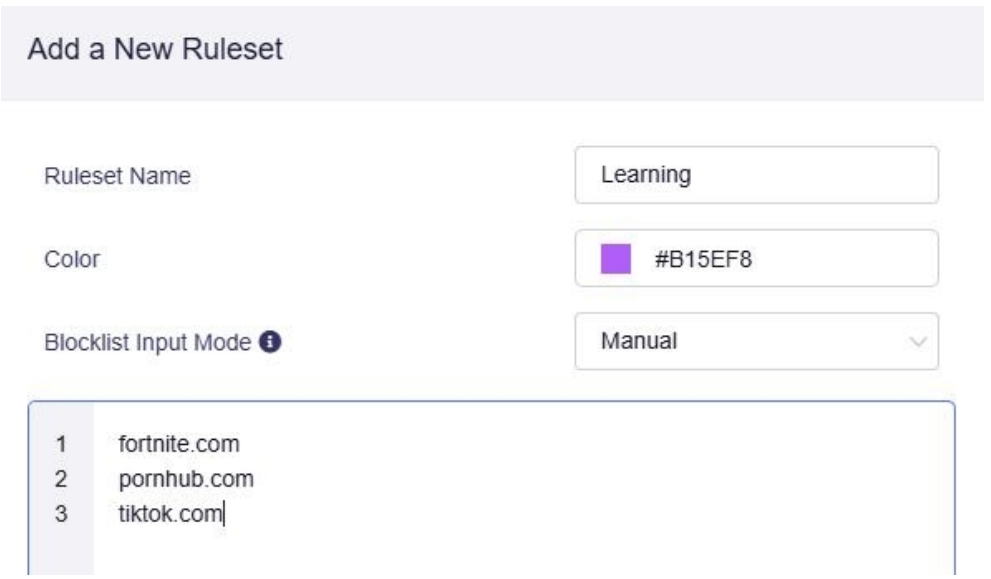


3. Ustaw ograniczenia dostępu.

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

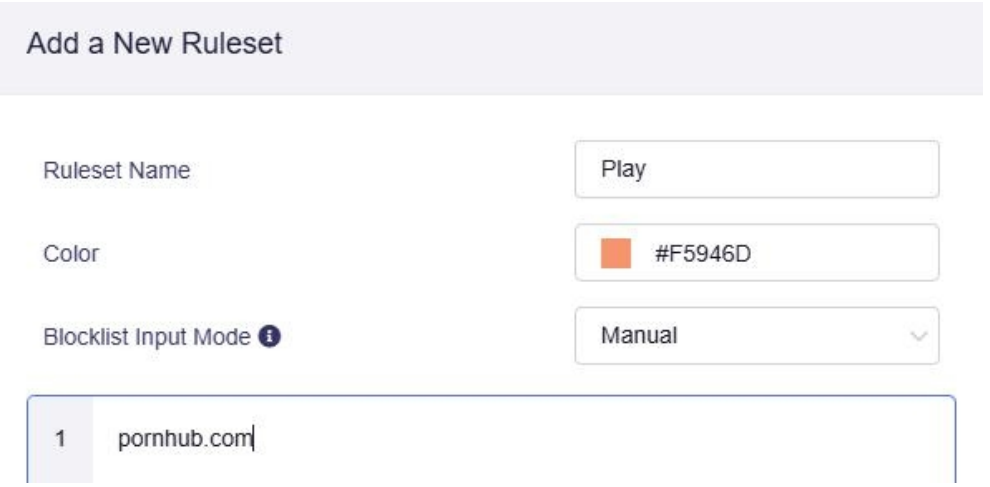


Określ nazwę zestawu reguł (np. Learning) i kolor, wprowadź witryny do zablokowania, a następnie kliknij **Apply**.

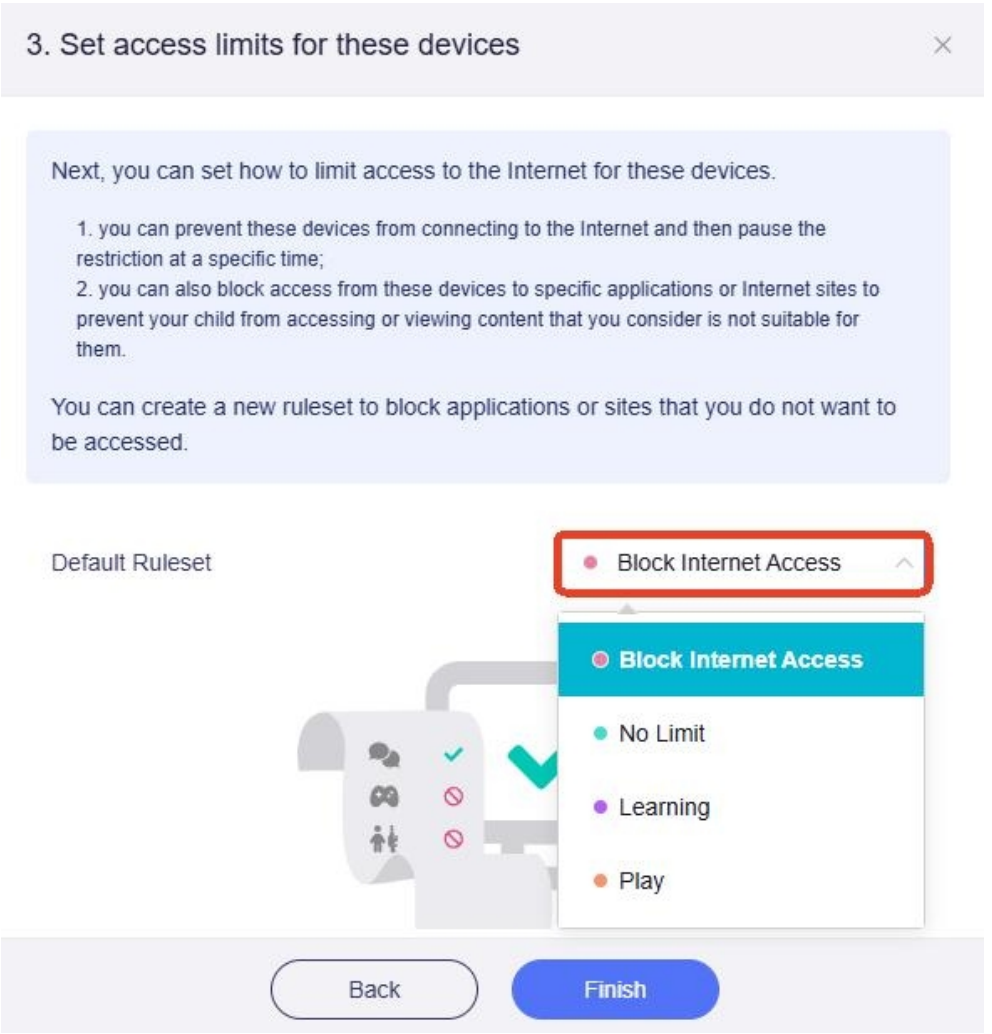


Uwaga: nazwy domen dodane do listy blokowanych obejmują również ich subdomeny. Na przykład wpis „example.com” obejmuje także każdą subdomenę, np. „subdomain.example.com”.

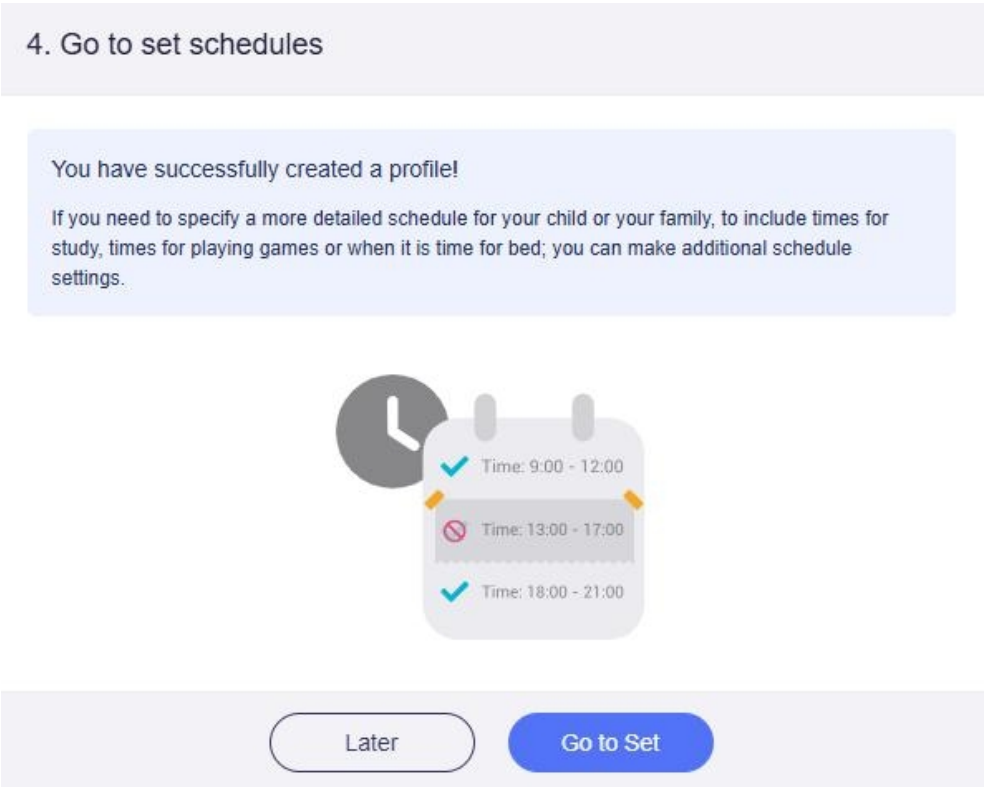
Podobnie utwórz drugi zestaw reguł. Określ jego nazwę (np. Play) i kolor, wprowadź witryny do zablokowania, a następnie kliknij **Apply**.



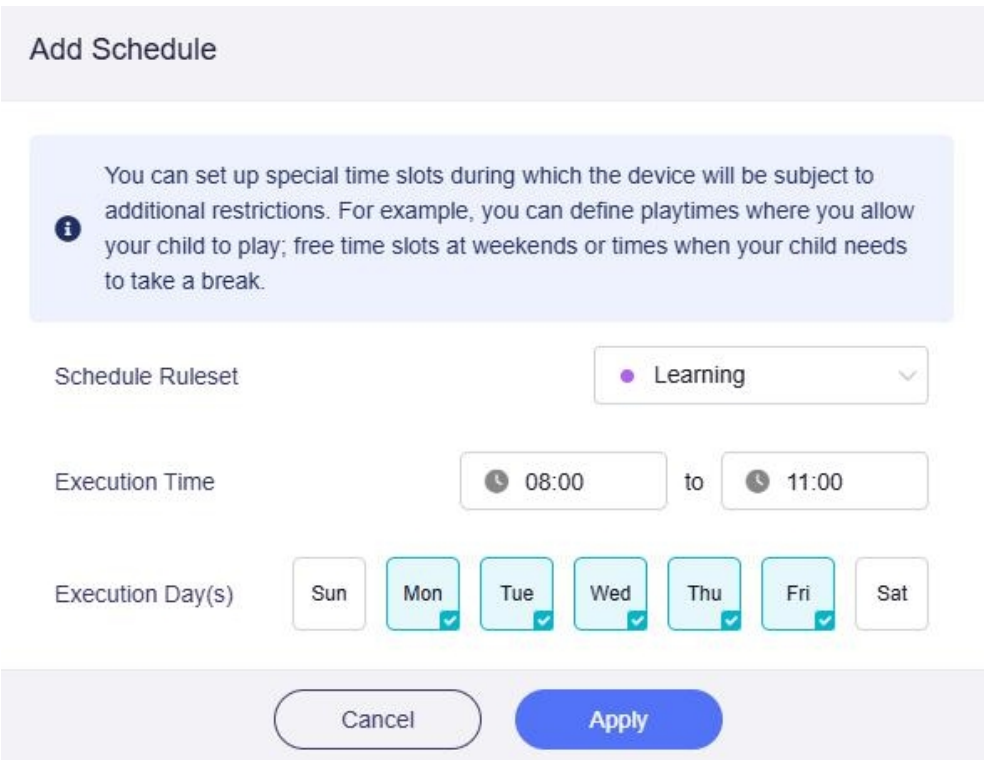
Po zastosowaniu ustawień dostępne będą cztery zestawy reguł. Wybierz **Block Internet Access** jako **Default Ruleset** i kliknij **Finish**.



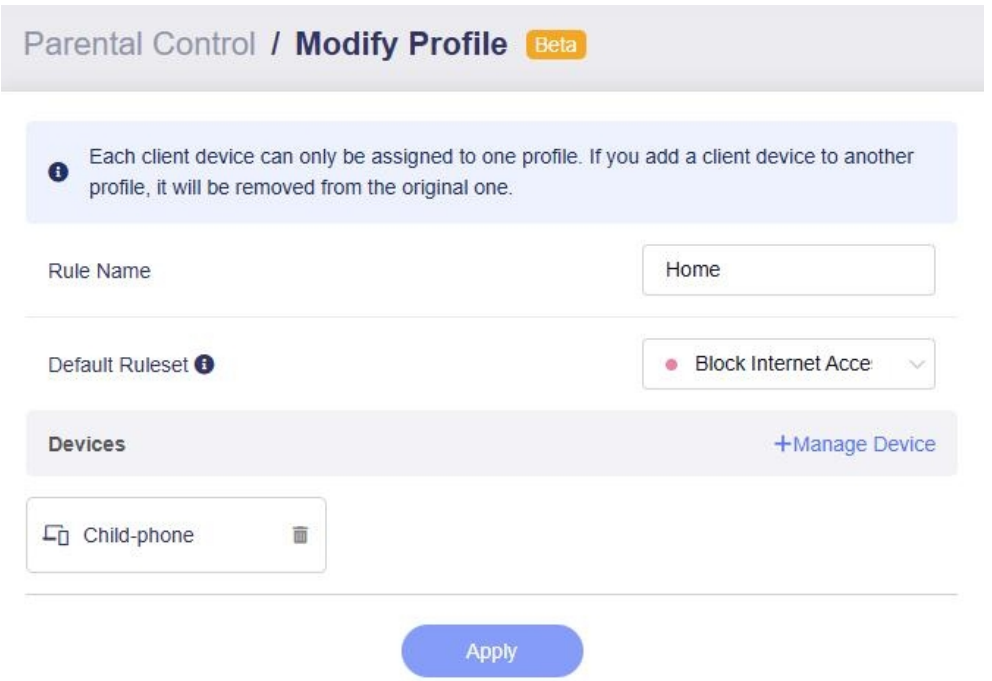
4. Następnie ustaw harmonogram profilu. Kliknij **Go to Set**.



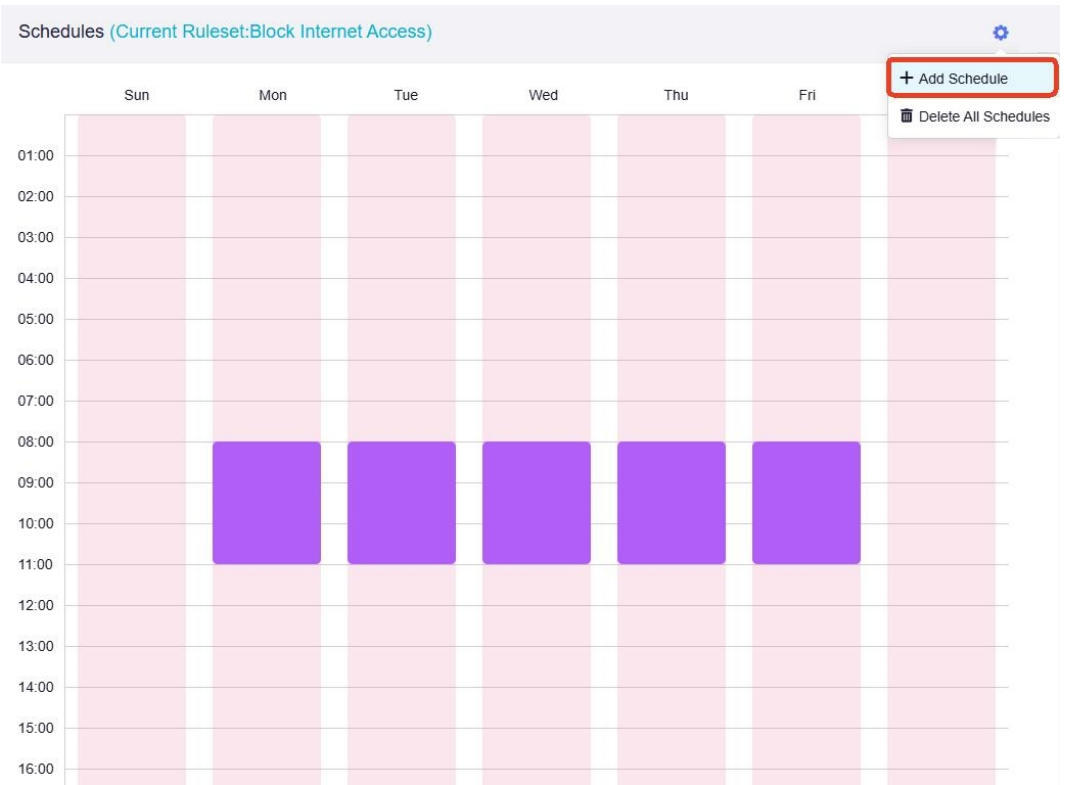
Dodaj zestaw reguł **Learning** do harmonogramu. Ustaw **Execution Time** od 8:00 do 11:00 w dni robocze, a następnie kliknij **Apply**.



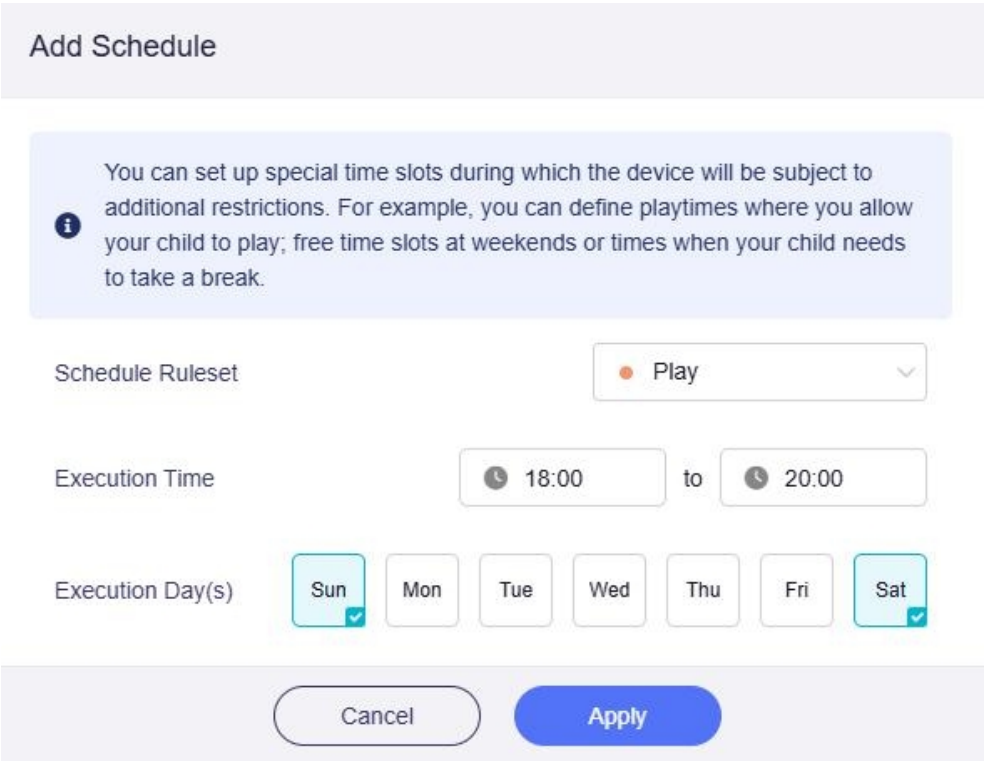
5. Otworzy się strona edycji utworzonego profilu.



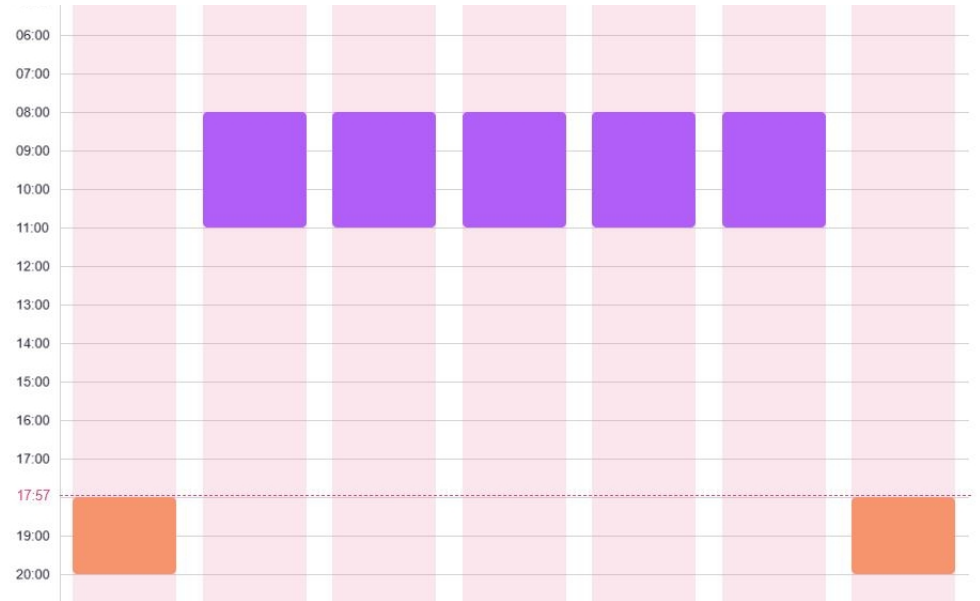
Przewiń w dół, aby zobaczyć utworzony harmonogram. Kliknij ikonę koła zębatego w prawym górnym rogu i wybierz **Add Schedule**.



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



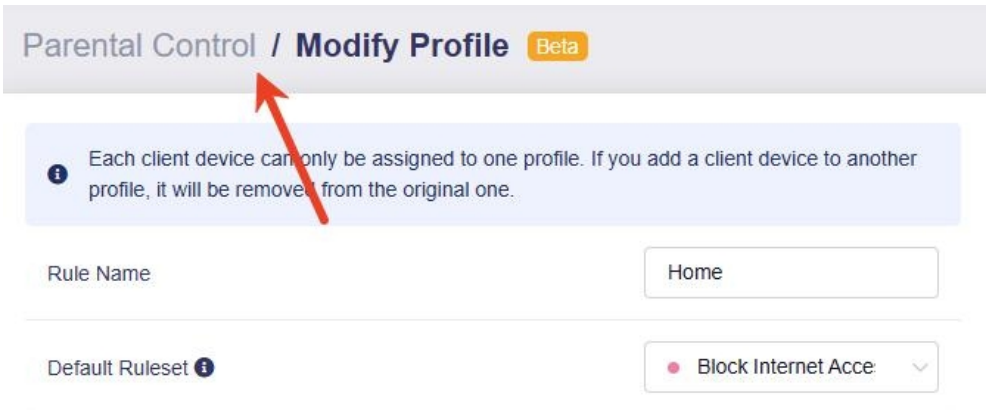
Zestaw reguł Play zostanie dodany do harmonogramu.



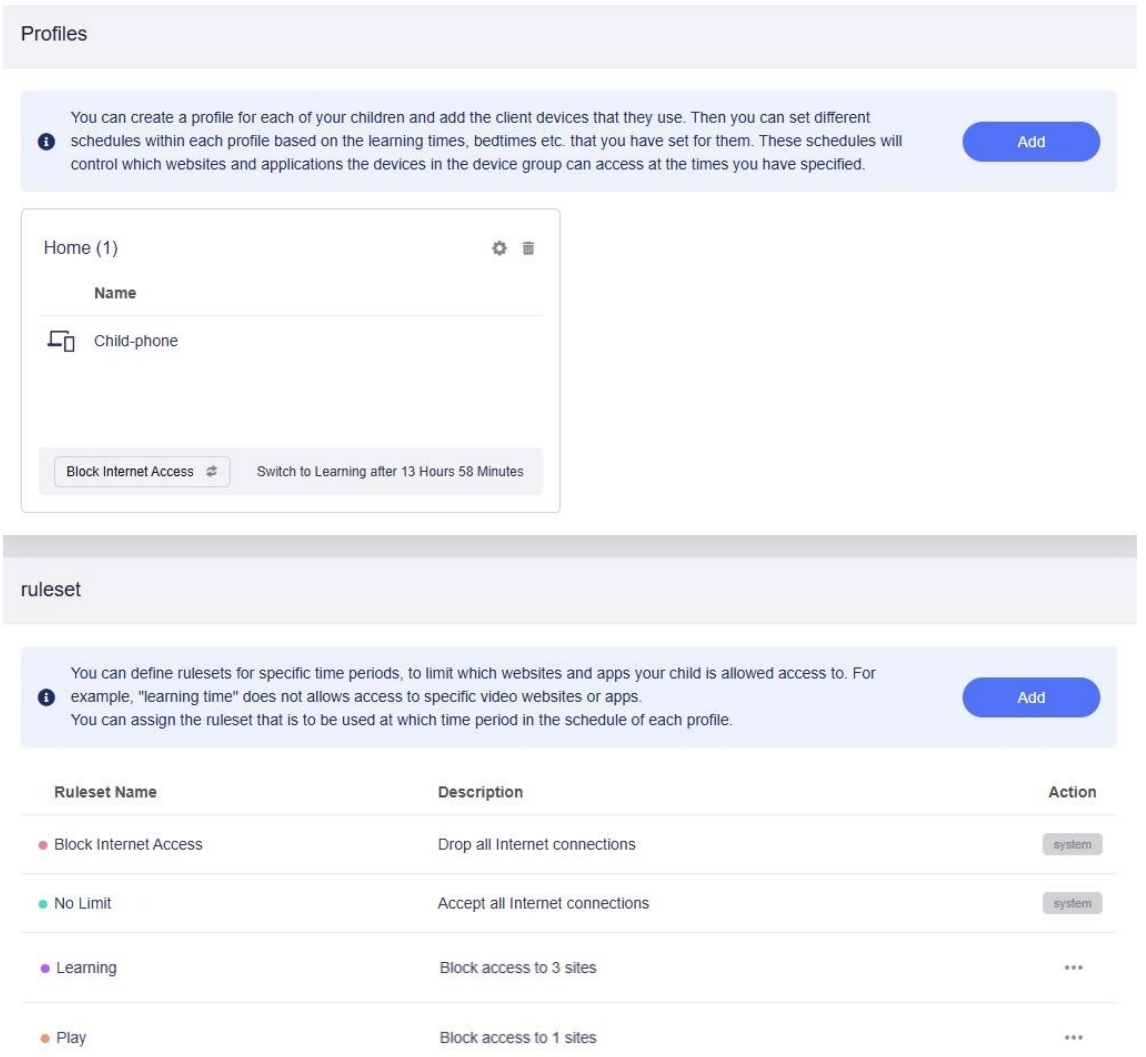
Wskazówki:

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

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



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



12.6.2 Rozwiązywanie problemów

Jeśli skonfigurowane ustawienia nie działają, sprawdź poniższe możliwe przyczyny.

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

12.7 ZeroTier

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

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

Uwaga:

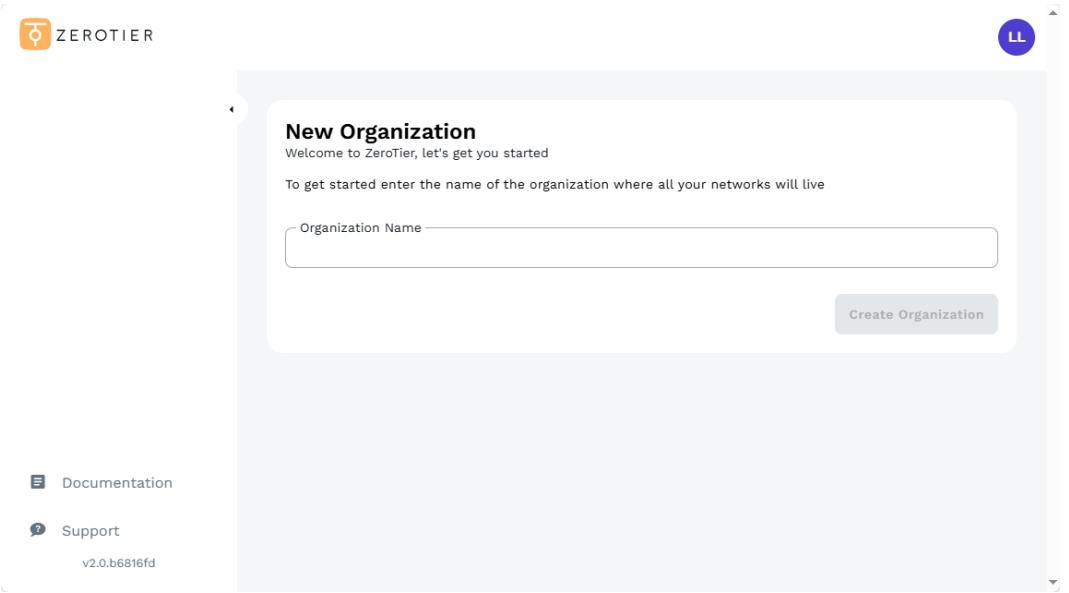
1. Nie zaleca się jednoczesnego używania ZeroTier z następującymi funkcjami lub usługami, ponieważ może to powodować konflikty routingu: klient OpenVPN, klient WireGuard, GoodCloud Site to Site i Tailscale.
2. Ta funkcja jest obecnie w fazie beta i może zawierać błędy.

12.7.1 Konfiguracja ZeroTier

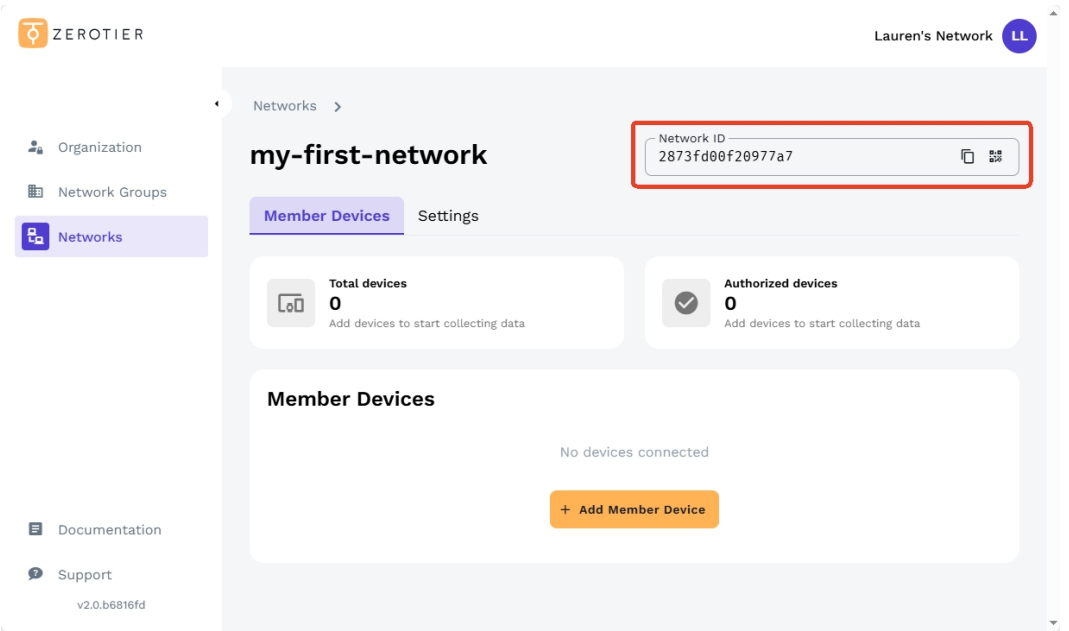
Dostępne są dwie wersje ZeroTier Central: New Central i Legacy Central.

W poniższych krokach jako przykład wykorzystano New Central.

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

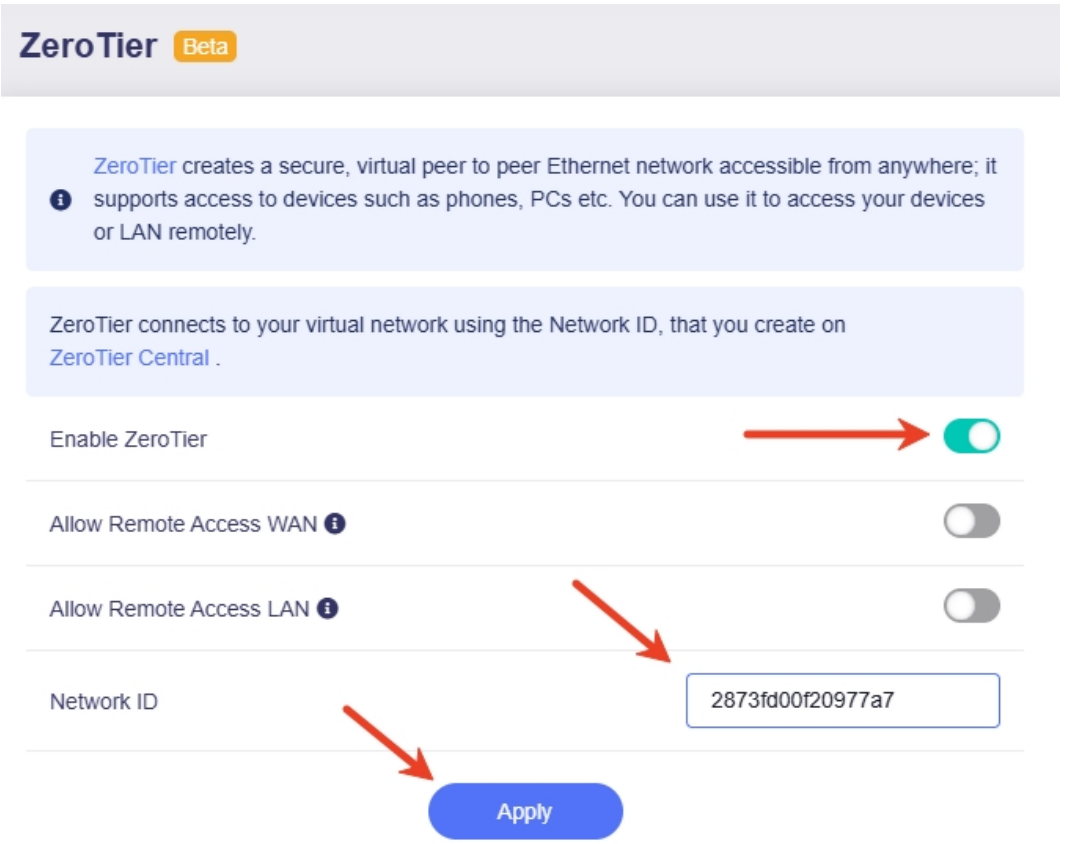


3. Wybierz plan. W tym przykładzie wybieramy **Personal plan**, obejmujący 10 urządzeń, 1 administratora sieci i 1 sieć. Aby tworzyć więcej sieci, dodawać więcej urządzeń lub niestandardowe trasy i DNS, wybierz inny płatny plan.
4. Sieć ZeroTier została utworzona.

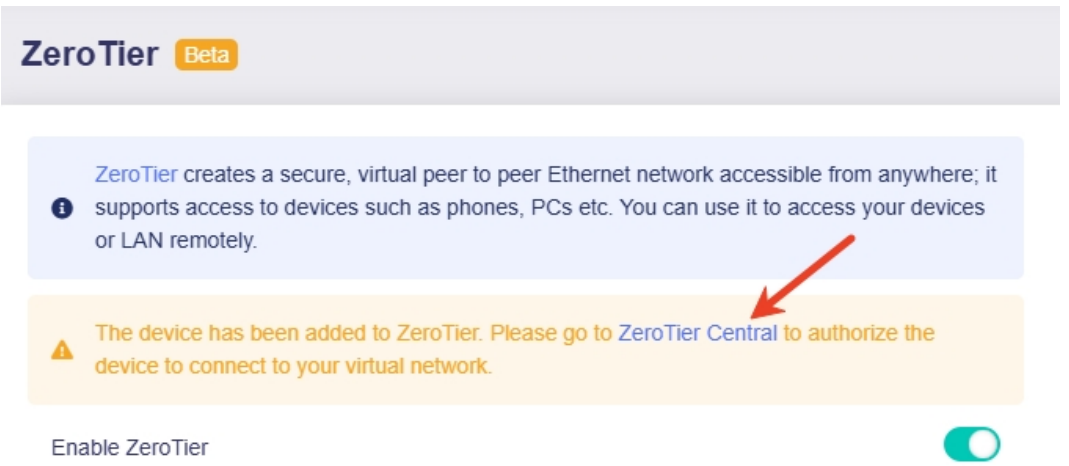


Zapisz **Network ID**, czyli 16-znakową kombinację liter i cyfr w prawym górnym rogu. Będzie potrzebna do późniejszego podłączania innych urządzeń.

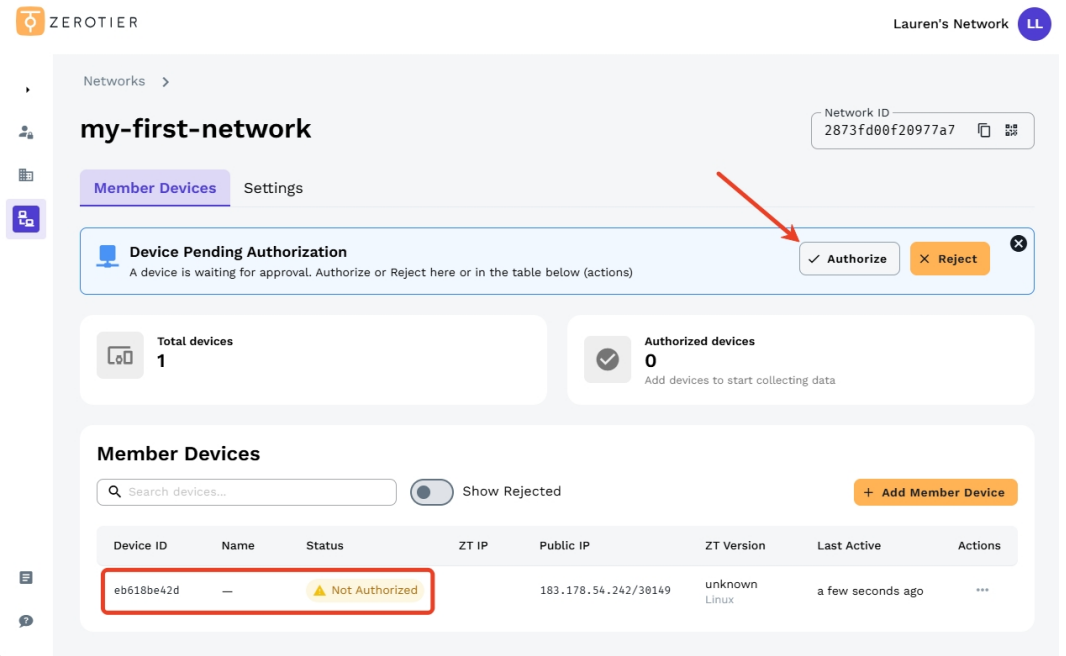
5. Zaloguj się do panelu administracyjnego routera i przejdź do **APPLICATIONS** > **ZeroTier**. Włącz ZeroTier, wprowadź **Network ID**, a następnie kliknij **Apply**.



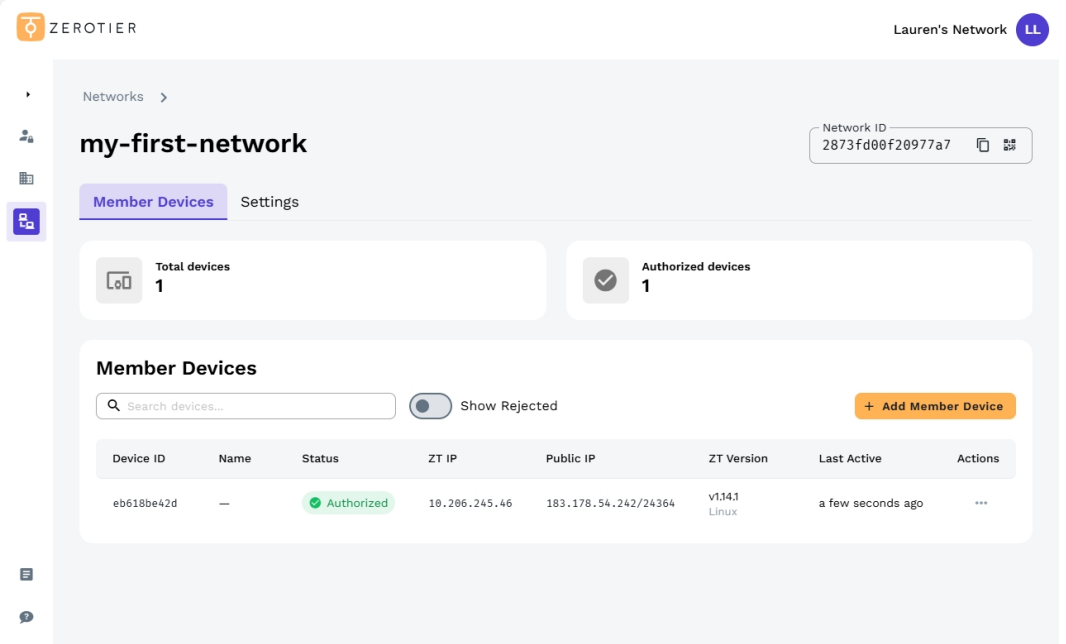
Po chwili na stronie pojawi się informacja o wymaganej autoryzacji. Kliknij hiperłącze **ZeroTier Central**, aby otworzyć ZeroTier Central.



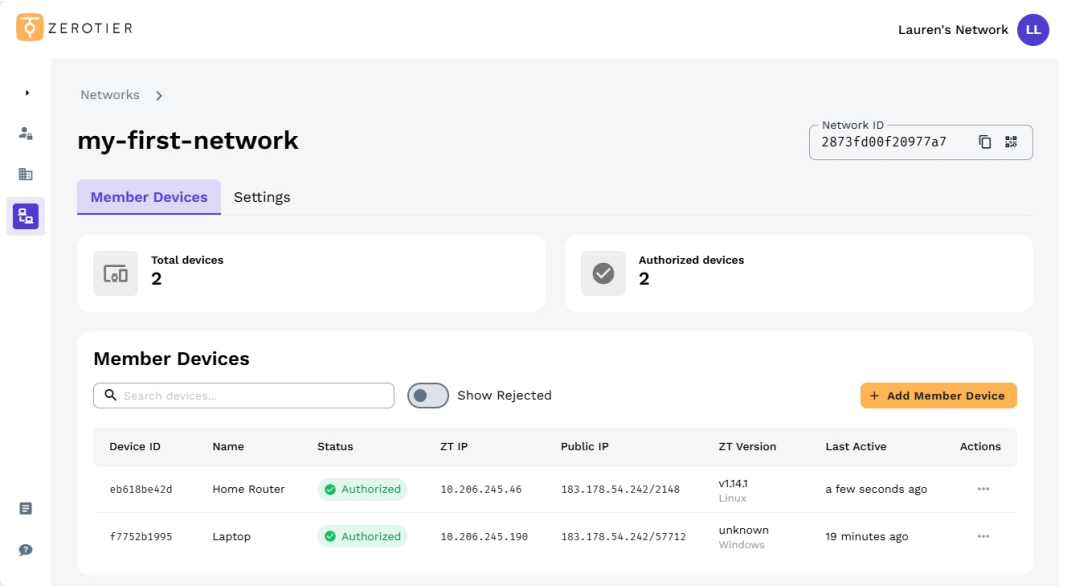
6. W ZeroTier Central znajdź oczekujące urządzenie i autoryzuj je.



Po autoryzacji strona będzie wyglądać jak poniżej.

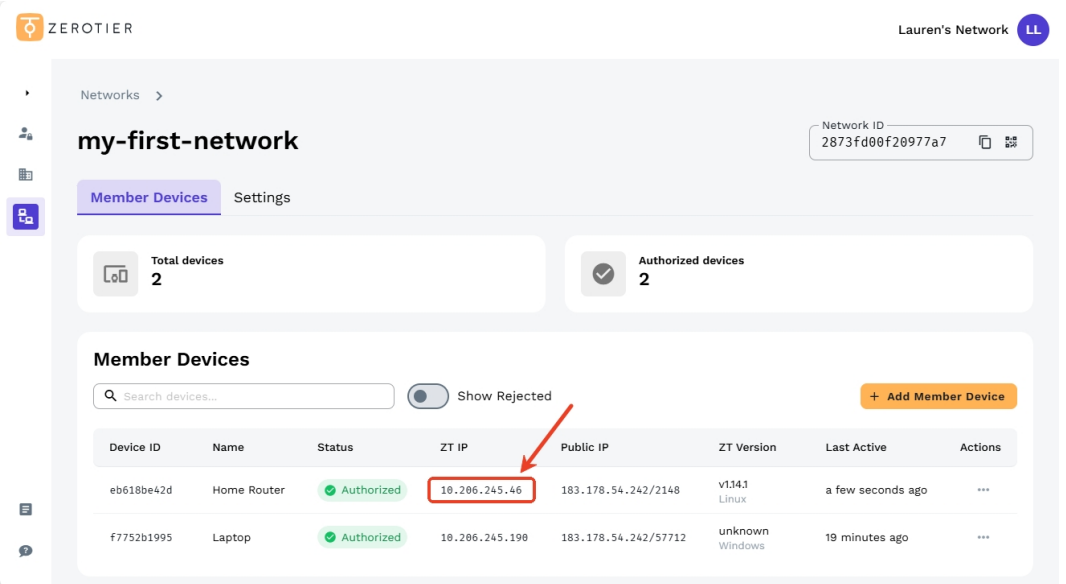


7. Dodaj kolejne urządzenie (np. komputer lub smartfon) do tej samej sieci ZeroTier zgodnie z tym poradnikiem. Po pomyślnym dodaniu strona będzie wyglądać jak poniżej. Pojawią się szczegóły urządzeń w sieci, takie **jak Device** ID**,** Name**,** Status, **Managed** IP i **Public IP**.



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

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



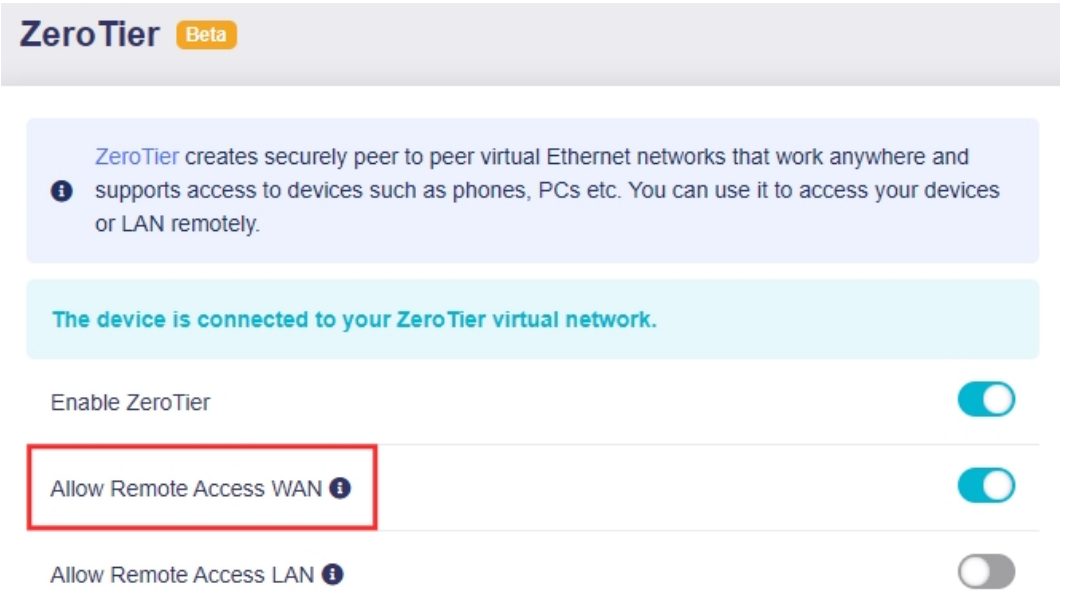
Możesz go następnie użyć do uzyskania dostępu do routera z laptopa w tej samej sieci ZeroTier.

9. Sprawdź łączność.

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

12.7.2 Zdalny dostęp do WAN

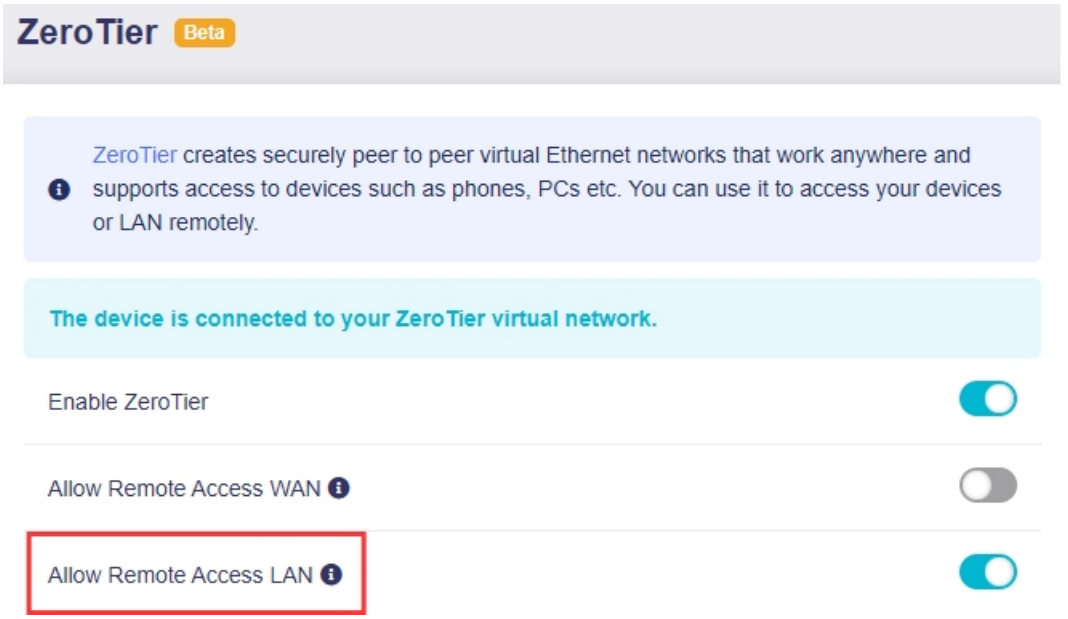
Po włączeniu tej opcji zasoby po stronie WAN urządzenia są dostępne przez wirtualną sieć ZeroTier. Więcej informacji znajdziesz tutaj.



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

12.7.3 Zdalny dostęp do LAN

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



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

12.8 Tailscale

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

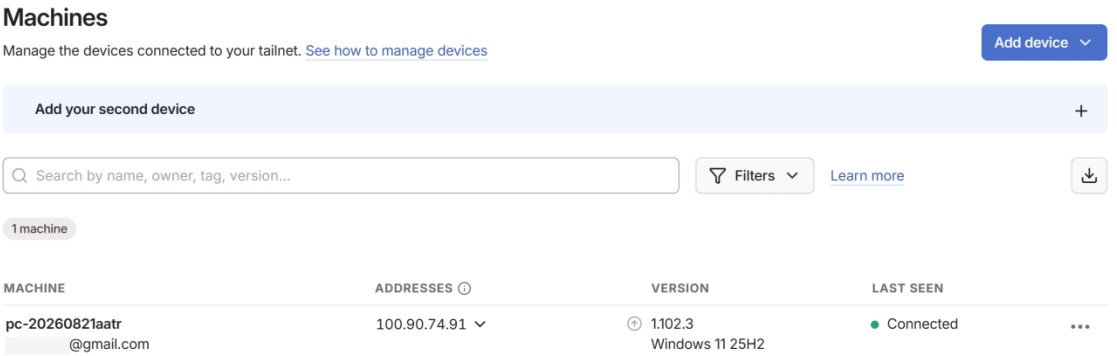
Funkcja Tailscale w routerach GL.iNet pozwala dołączyć router do wirtualnej sieci Tailscale, umożliwiając zdalny dostęp do routera oraz zasobów po jego stronie WAN i LAN.

Uwaga:

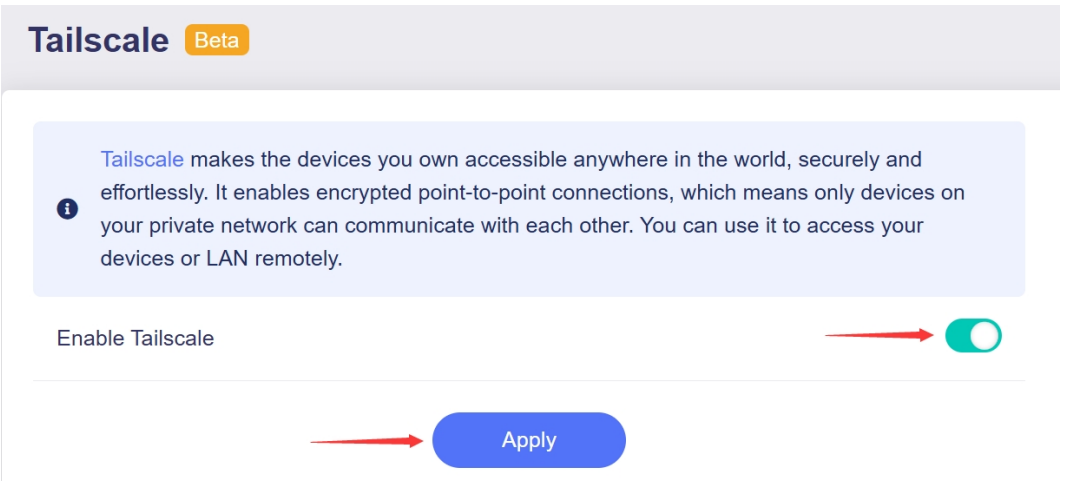
1. Tailscale opiera się na WireGuard, dlatego nie zaleca się jednoczesnego używania go z następującymi funkcjami lub usługami, ponieważ może to powodować konflikty routingu: klient OpenVPN, klient WireGuard, GoodCloud Site to Site i ZeroTier.
2. Ta funkcja jest obecnie w fazie beta i może zawierać błędy.

12.8.1 Konfiguracja Tailscale

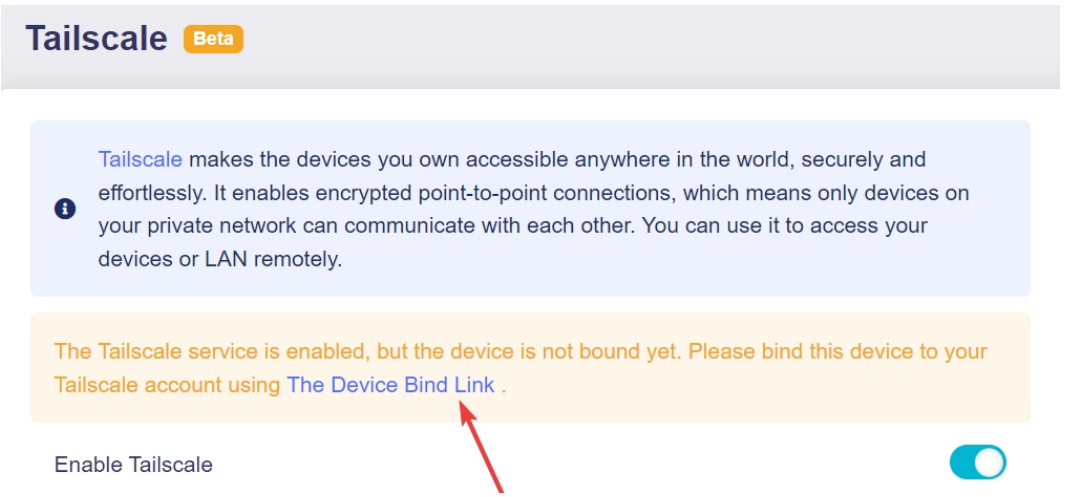
1. Najpierw zarejestruj konto Tailscale i powiąż z nim jedno lub dwa urządzenia do testów. Po powiązaniu zobaczysz je w konsoli Tailscale.



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



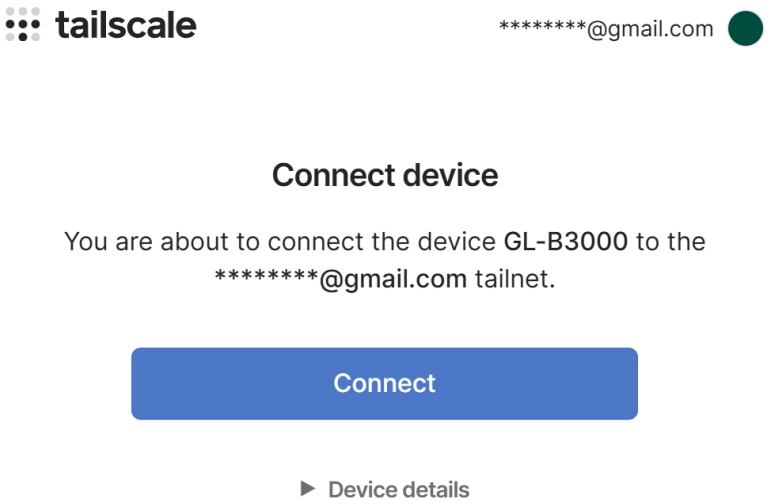
3. Strona poprosi o powiązanie urządzenia. Kliknij **Device Bind Link**.



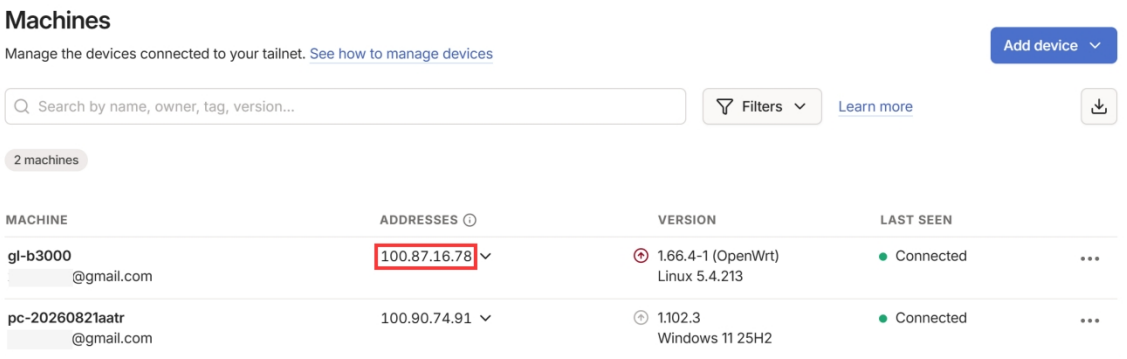
4. W wyświetlonym oknie kliknij łącze i zaloguj się na konto Tailscale.



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

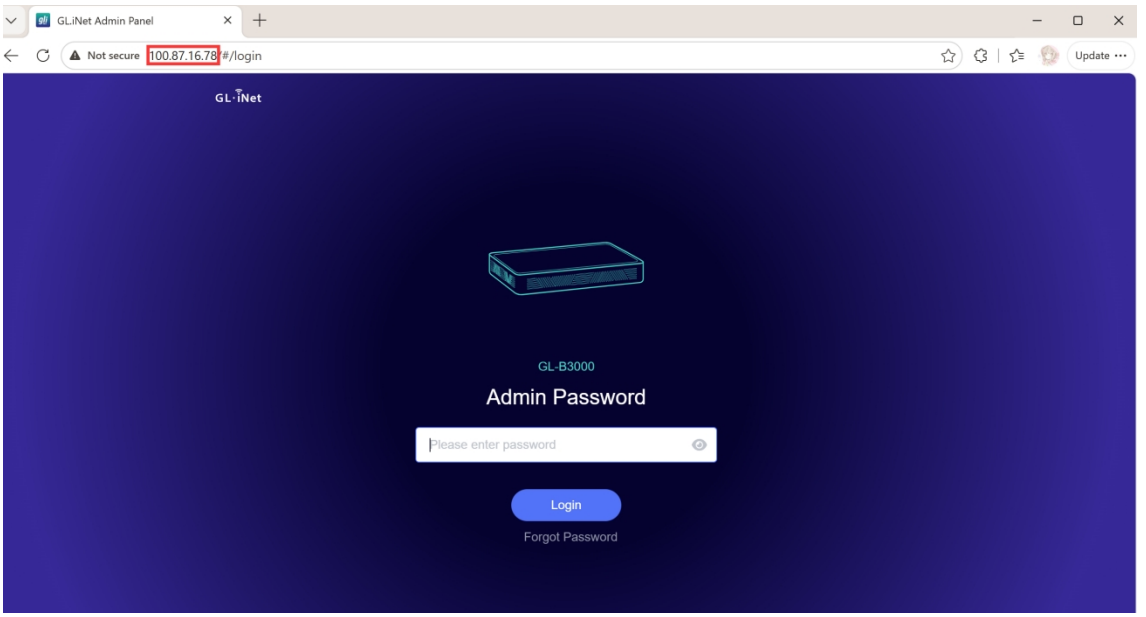


6. Następnie nastąpi przekierowanie do konsoli administracyjnej Tailscale. Router został już dodany do wirtualnej sieci Tailscale i jest dostępny zdalnie pod wirtualnym adresem IP Tailscale **100.87.16.78**.



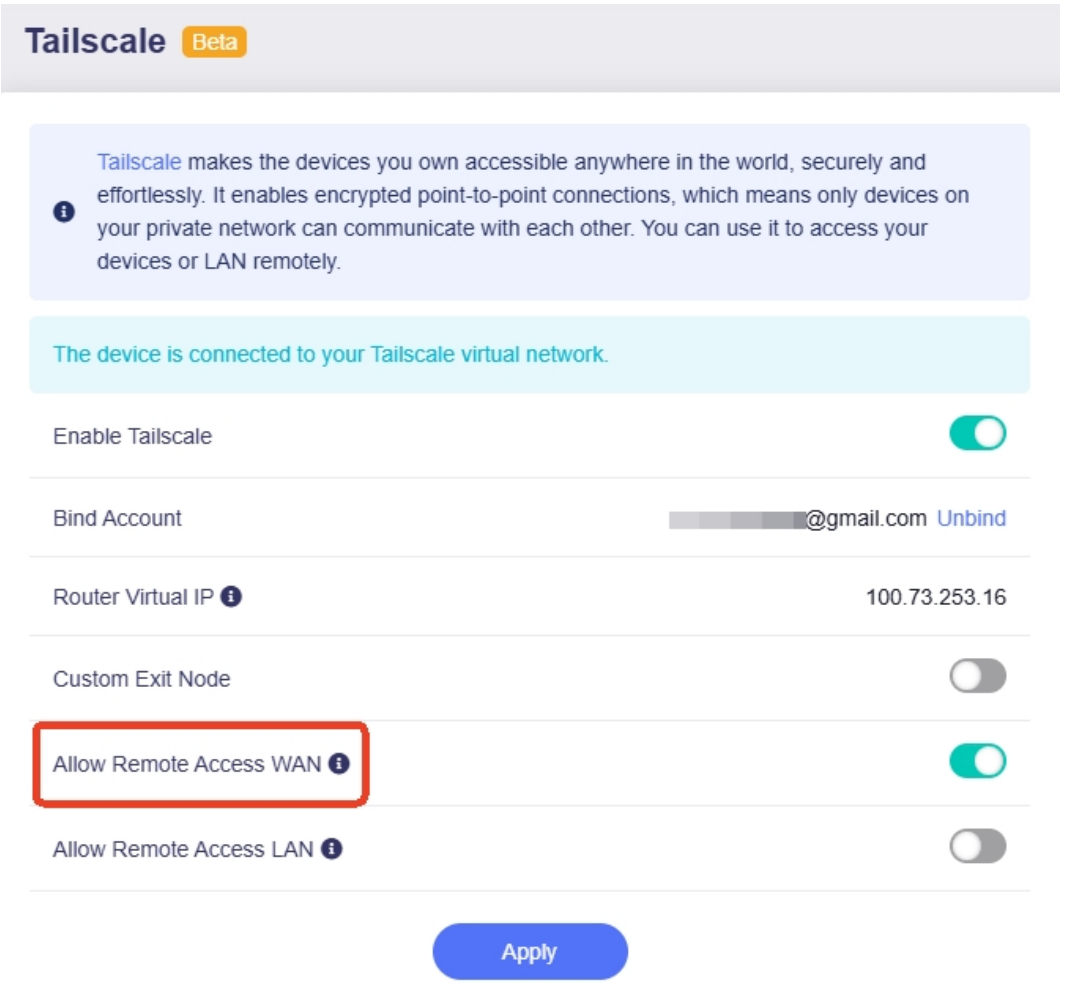
7. Sprawdź łączność.

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


GL.iNet Admin Panel
Not secure
100.87.16.78/#/login
Update
GL·iNet
GL-B3000
Admin Password
Please enter password
Login
Forgot Password

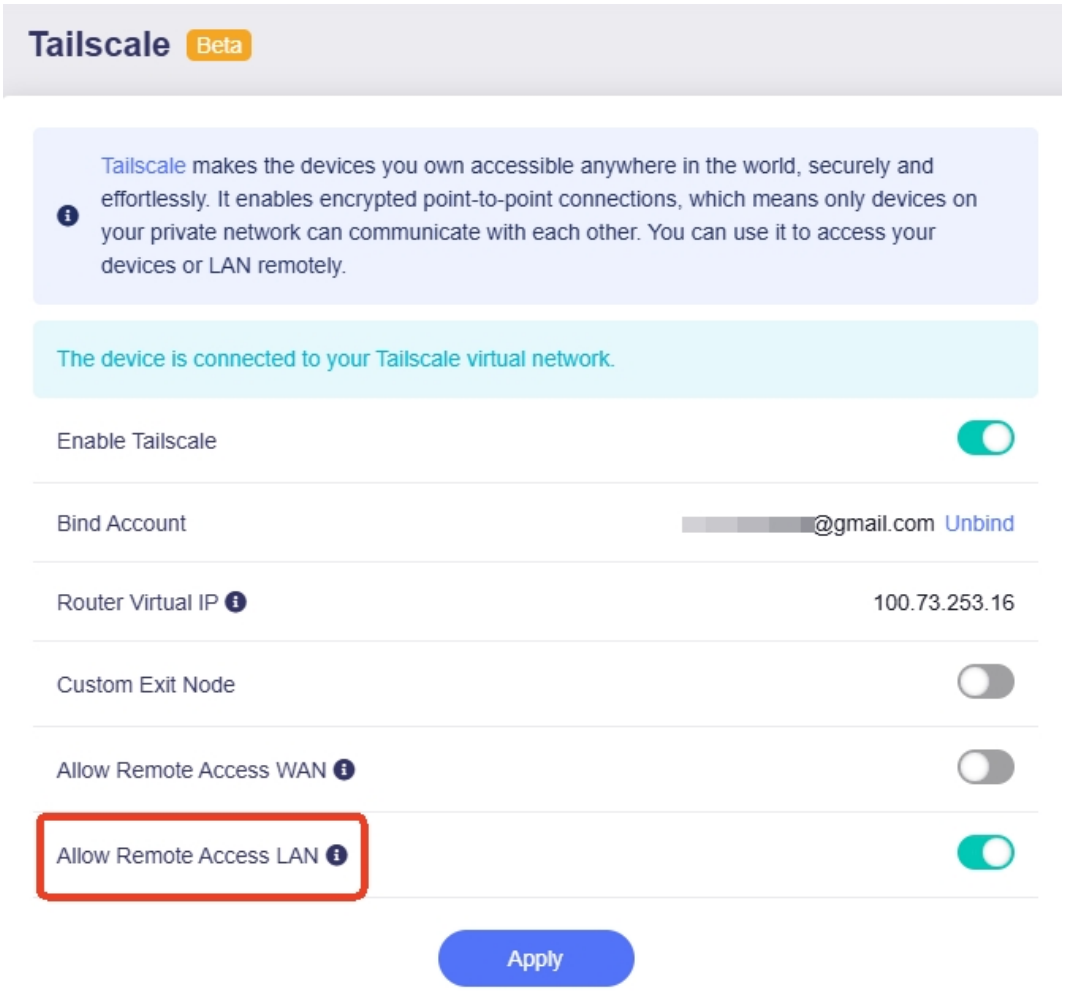
12.8.2 Zdalny dostęp do WAN

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



12.8.3 Zdalny dostęp do LAN

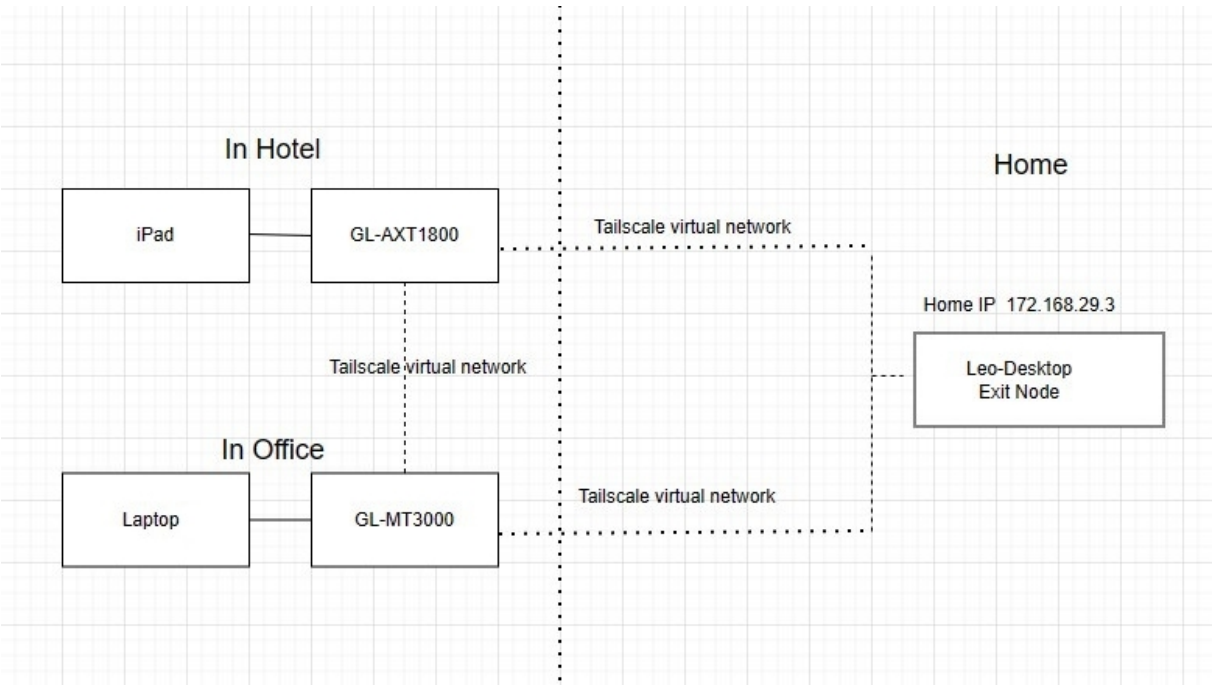
Po włączeniu tej opcji zasoby po stronie LAN urządzenia są dostępne przez wirtualną sieć Tailscale. Więcej informacji znajdziesz tutaj.



12.8.4 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 nosi nazwę „Exit Node”. Konfigurację niestandardowego węzła wyjściowego na routerach GL.iNet opisano w tym poradniku.

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).

Rozdział 13

Sieć

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

13.1 Zapora sieciowa

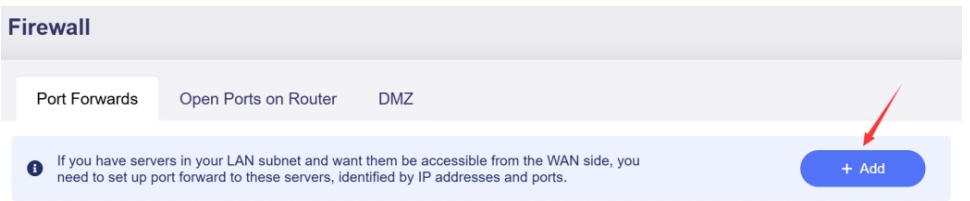
Zapora sieciowa to funkcja kierująca żądania zewnętrzne do określonych urządzeń w sieci lokalnej. Strona Firewall obejmuje trzy główne funkcje: **Port Forwards** (dostęp do wybranych portów urządzeń), **Open Ports on Router** (dostęp do usług działających na samym routerze) oraz **DMZ** (bezpośredni, pełny dostęp do jednego urządzenia).

13.1.1 Przekierowanie portów

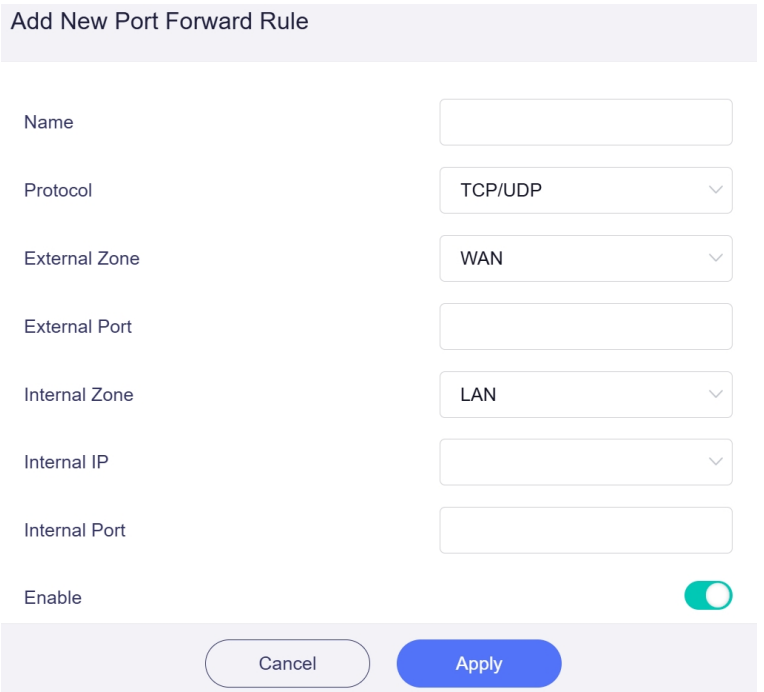
Przekierowanie portów umożliwia komputerom zdalnym łączenie się z komputerem lokalnym lub serwerem za zaporą LAN (np. serwerem WWW lub FTP).

Aby skonfigurować przekierowanie portów, wykonaj poniższe czynności.

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



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

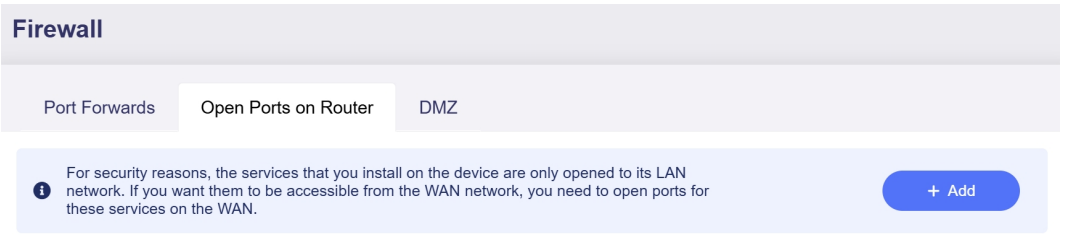


- **Name**: nazwa reguły określana przez użytkownika.
- **Protocol**: używany protokół. Możesz wybrać TCP, UDP lub oba protokoły.
- **External Zone**: dostępne opcje to WAN, WireGuard Client, WireGuard Server, OpenVPN Client, OpenVPN Server, LAN i Guest.
- **External Port**: numer lub numery portów zewnętrznych.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

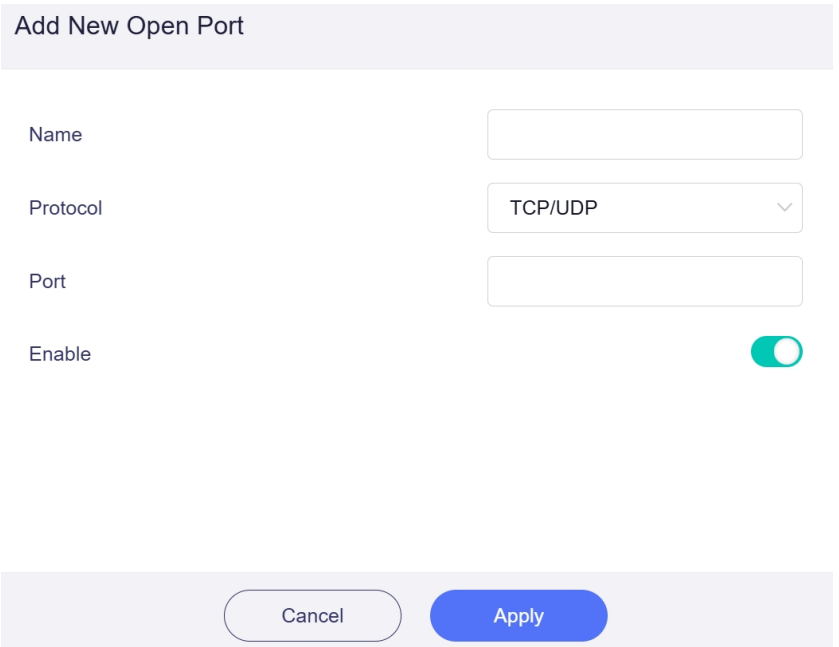
13.1.2 Otwieranie portów routera

Aby usługi routera, takie jak WWW i FTP, były dostępne publicznie, trzeba otworzyć na routerze odpowiadające im porty.

Aby otworzyć port, przejdź na kartę Open Ports on Router, a następnie kliknij Add.



W wyświetlonym oknie otwórz nowy port i kliknij Apply.



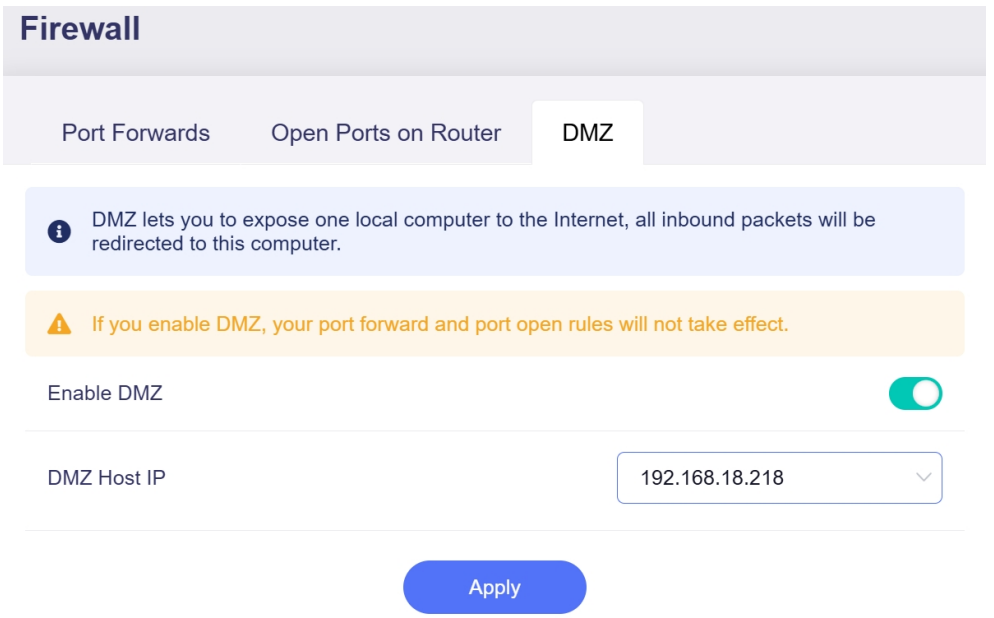
- **Name**: nazwa reguły określana przez użytkownika.
- **Protocol**: używany protokół. Możesz wybrać TCP, UDP lub oba protokoły.
- **Port**: numer portu, który chcesz otworzyć.

13.1.3 DMZ

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

Aby w razie potrzeby włączyć DMZ, wykonaj poniższe czynności.

1. Zaloguj się do panelu administracyjnego routera i przejdź do sekcji **NETWORK** > **Firewall** > **DMZ**.
2. Włącz **Enable DMZ**, a następnie wybierz **DMZ Host IP** z listy. Wybrane urządzenie będzie otrzymywać wszystkie pakiety przychodzące. Kliknij **Apply**, aby zapisać ustawienia.



13.2 Multi-WAN

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

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

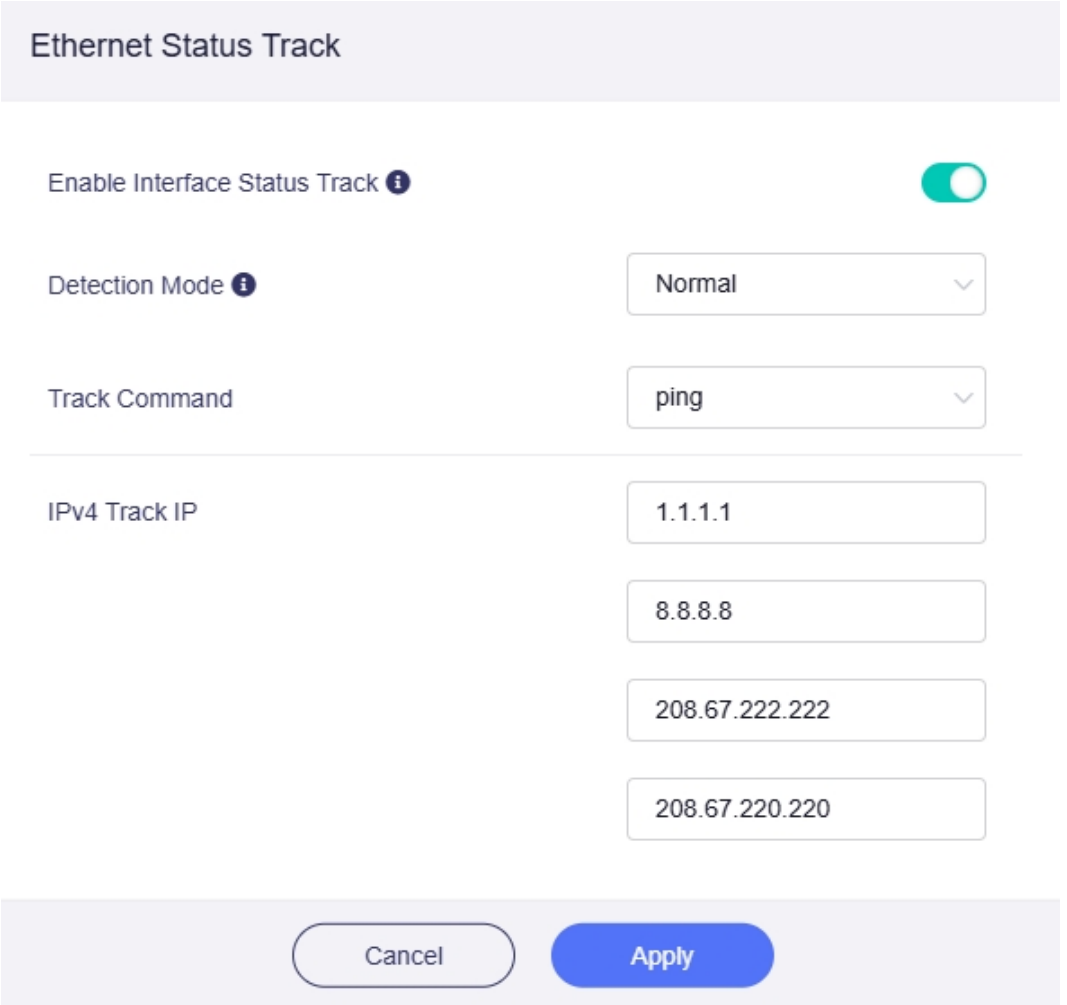
Zaloguj się do panelu administracyjnego routera i przejdź do **NETWORK** > **Multi-WAN**. Strona obejmuje dwie sekcje: Interface Status Track i Multi-WAN Mode.

13.2.1 Monitorowanie stanu interfejsów

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



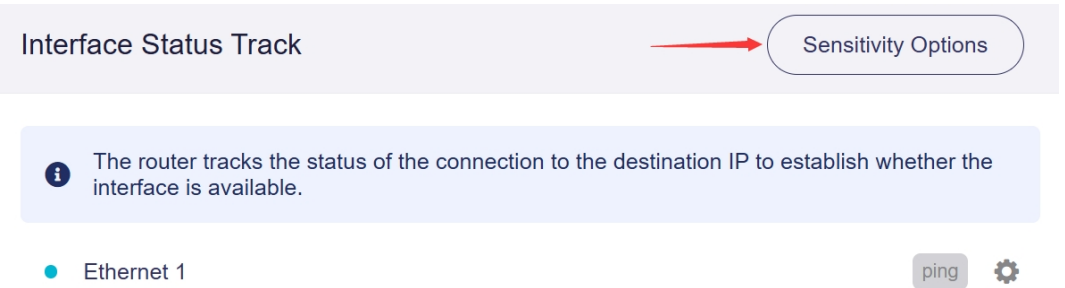
W sekcji **Interface Status Track** kliknij ikonę koła zębatego po prawej stronie, aby otworzyć ustawienia monitorowania poszczególnych interfejsów sieciowych. Poniżej pokazano ustawienia interfejsu Ethernet. Pozostałe interfejsy konfiguruje się według tych samych zasad.



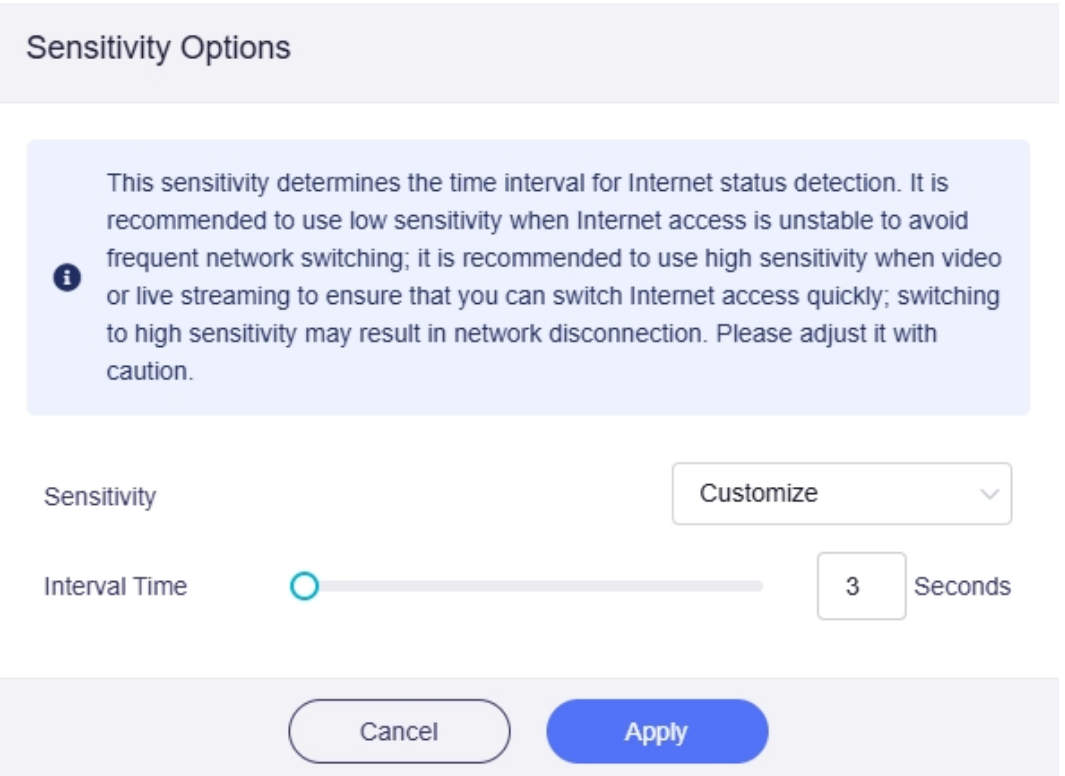
- **Enable Interface Status Track**: opcja jest domyślnie włączona. Po wyłączeniu router określa stan interfejsu na podstawie warunków fizycznych (np. podłączenia kabla Ethernet).
- **Detection Mode**: tę funkcję wprowadzono w wersji oprogramowania 4.5 jako Low Data Mode, a w wersji 4.7 zmieniono nazwę na Detection Mode. Dostępne są trzy tryby: Normal Mode, Low Data Mode i Strict Mode.
  - **Normal**: tryb używany domyślnie.
  - **Low Data**: uruchamia monitorowanie tylko po wystąpieniu błędu sieciowego w interfejsie. Używaj tego trybu, jeśli masz ograniczony pakiet danych. Pamiętaj, że ponowne połączenie po rozłączeniu może trwać nieco dłużej niż w trybie Normal. Ten tryb jest domyślnie włączony tylko dla interfejsu komórkowego.
  - **Strict**: określa stan interfejsu wyłącznie na podstawie wyników polecenia diagnostycznego 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.



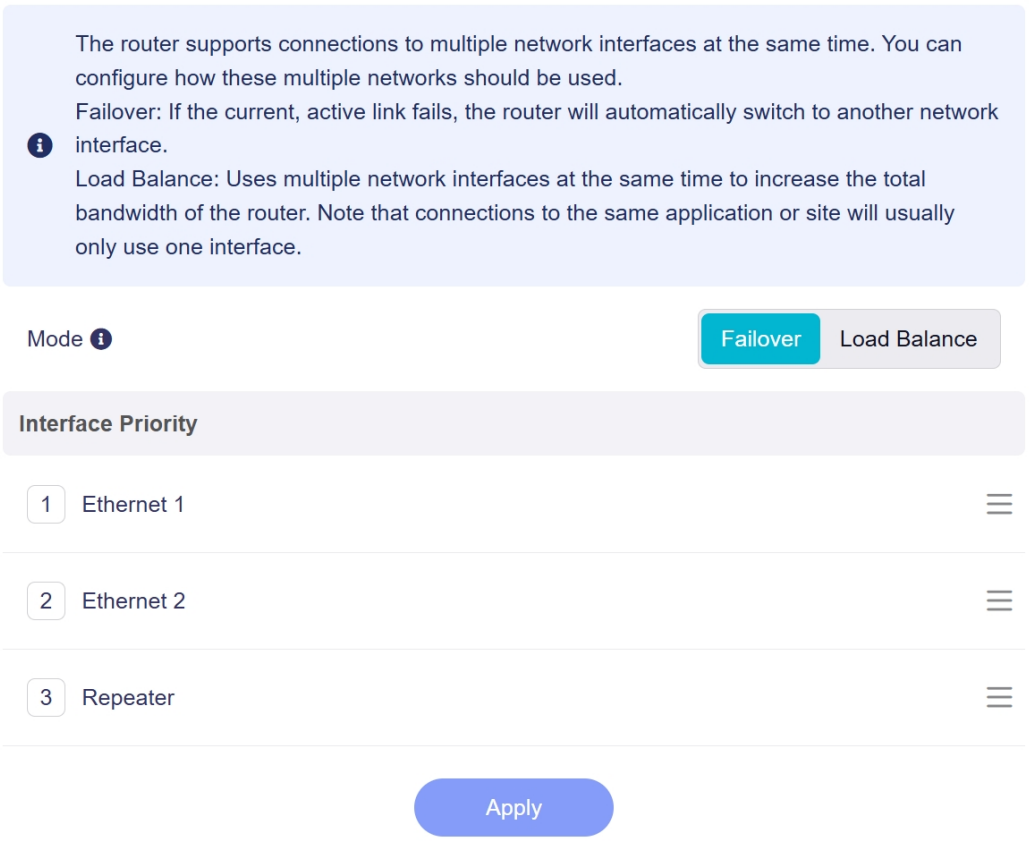
13.2.2 Tryb Multi-WAN

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

Przełączanie awaryjne (Failover)

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

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

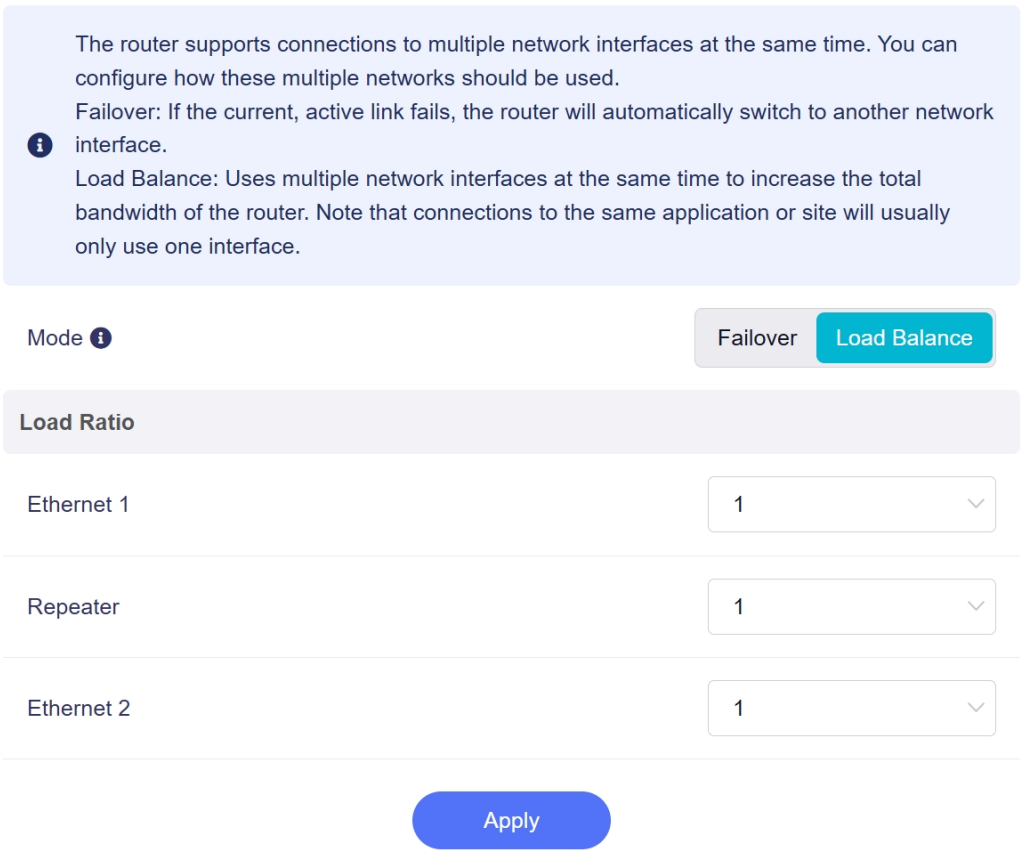


Równoważenie obciążenia (Load Balance)

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

Proporcje obciążenia określają udział poszczególnych interfejsów sieciowych. System przydziela interfejsom nowe połączenia zgodnie z tym ustawieniem.

Na przykład jeśli router jest jednocześnie połączony z trzema sieciami (np. Ethernet 1, Repeater i Ethernet 2), a wszystkie interfejsy zapewniają dostęp do Internetu, włączenie Load Balance i ustawienie proporcji 1:1:1 oznacza równy podział przepustowości między trzy interfejsy. System rozdziela nowe połączenia między te interfejsy zgodnie z ustawioną proporcją obciążenia 1:1:1.



W razie potrzeby możesz dostosować proporcje obciążenia. Na przykład jeśli Ethernet 1 ma przepustowość 100 Mb/s, Repeater 200 Mb/s, a inne połączenia nie są aktywne, ustaw

proporcje na 1 dla Ethernet 1, 2 dla Repeater i 0 dla Ethernet 2. System rozdzieli nowe połączenia między te interfejsy zgodnie z proporcją 1:2. Oznacza to, że Ethernet 1 obsłuży o połowę mniej połączeń niż Repeater. W odróżnieniu od trybu Failover ten tryb optymalizuje łączną wydajność transmisji, równoważąc obciążenie ruchem między wszystkimi dostępnymi interfejsami.

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

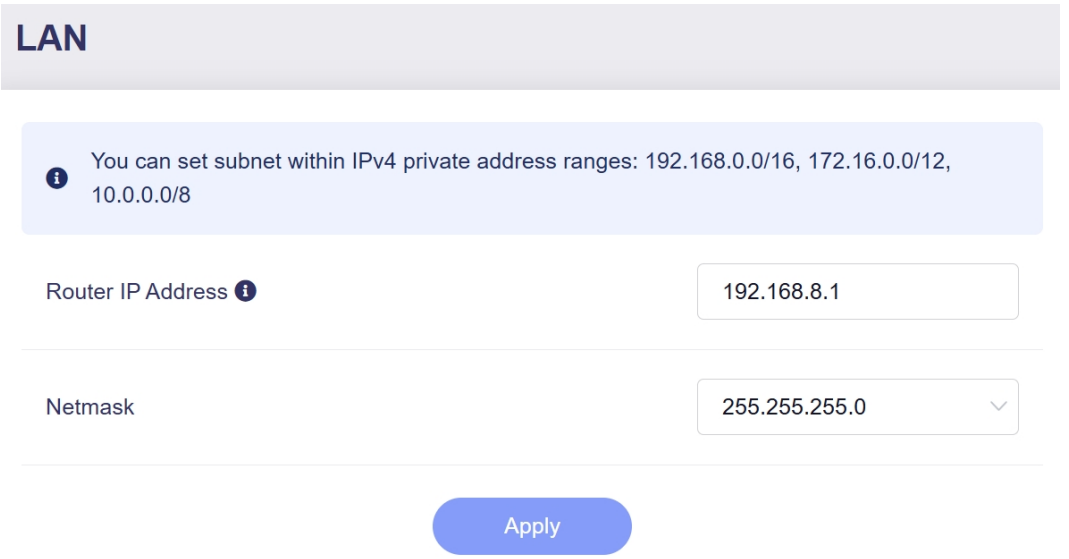
13.3 LAN

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

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

13.3.1 Ustawienia podstawowe

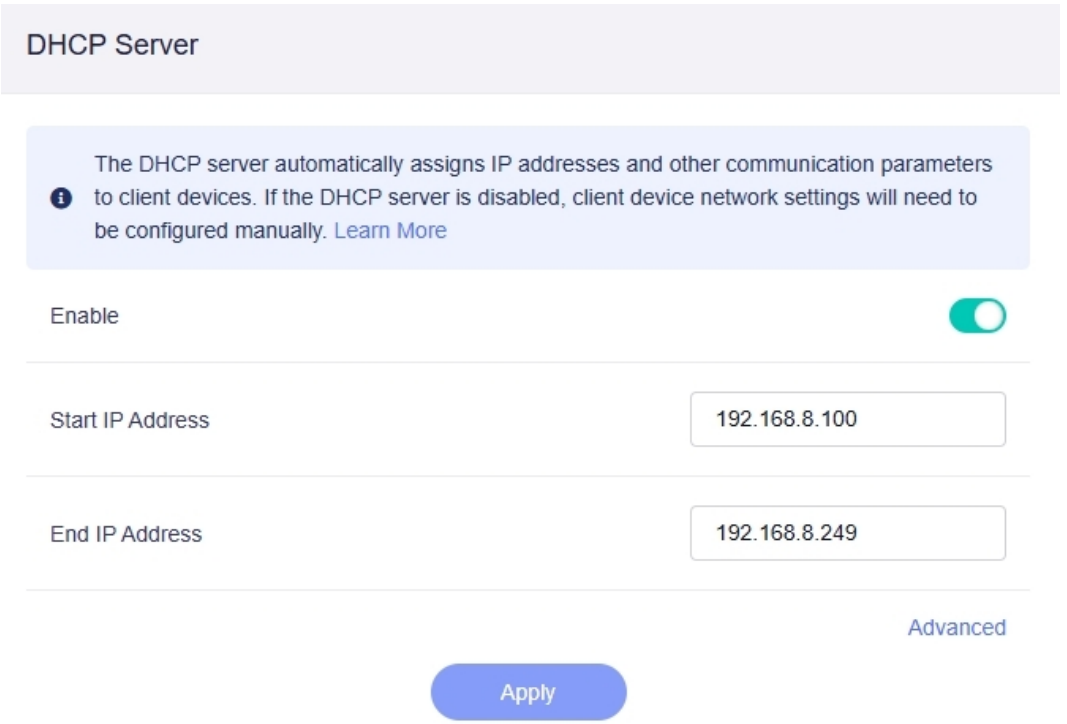
Ustawienia podstawowe obejmują adres IP routera i maskę sieci. Podsieć można ustawić w prywatnych zakresach adresów IPv4: 192.168.0.0/16, 172.16.0.0/12, 10.0.0.0/8.



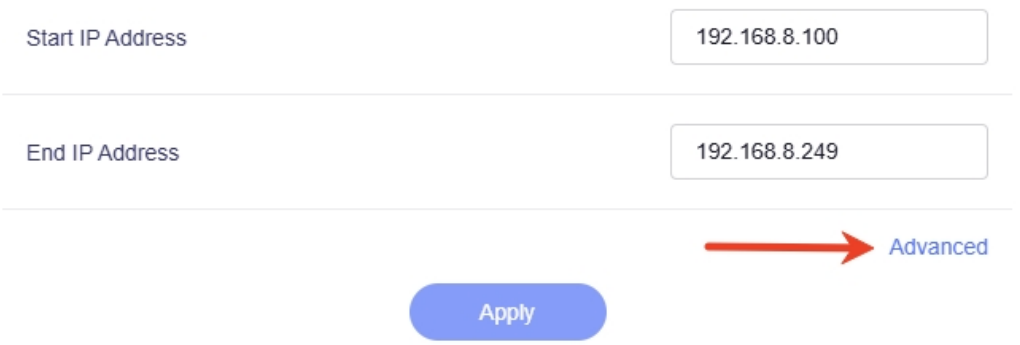
- **Router IP Address**: adres wpisywany w pasku adresu przeglądarki w celu otwarcia panelu administracyjnego routera. Domyślnie jest to 192.168.8.1. Można go zmienić, jeśli koliduje z siecią nadrzędną.
- **Netmask**: dostępne są dwie opcje: 255.255.255.0 i 255.255.0.0.

13.3.2 Serwer DHCP

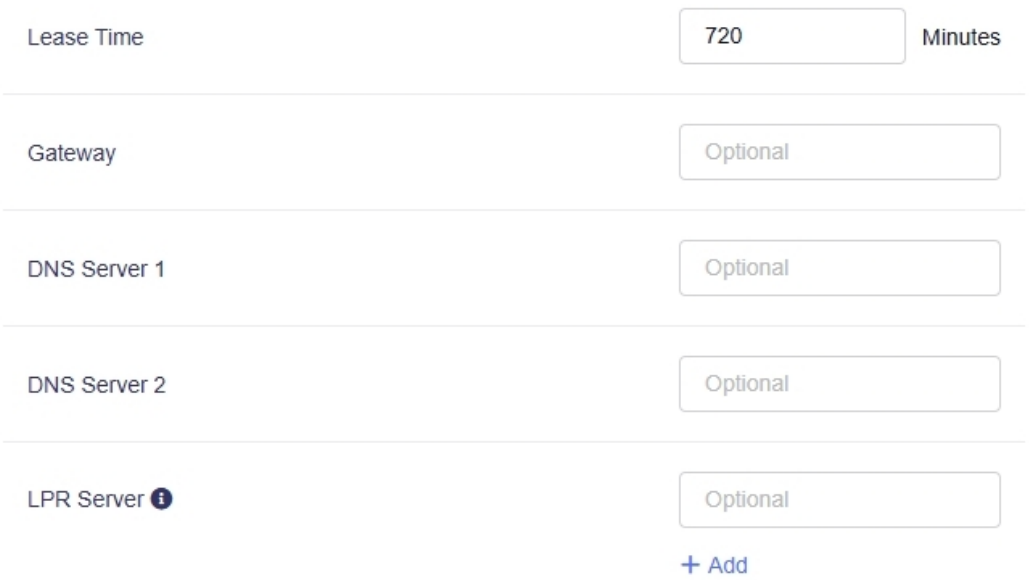
Serwer DHCP automatycznie przydziela adresy IP i inne parametry komunikacji każdemu podłączonemu klientowi. W routerze GL.iNet jest domyślnie włączony, a jego pula adresów IP obejmuje zakres od 192.168.8.100 do 192.168.8.249. W razie potrzeby można zmienić ten zakres.



Kliknij **Advanced** w prawym dolnym rogu.



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



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

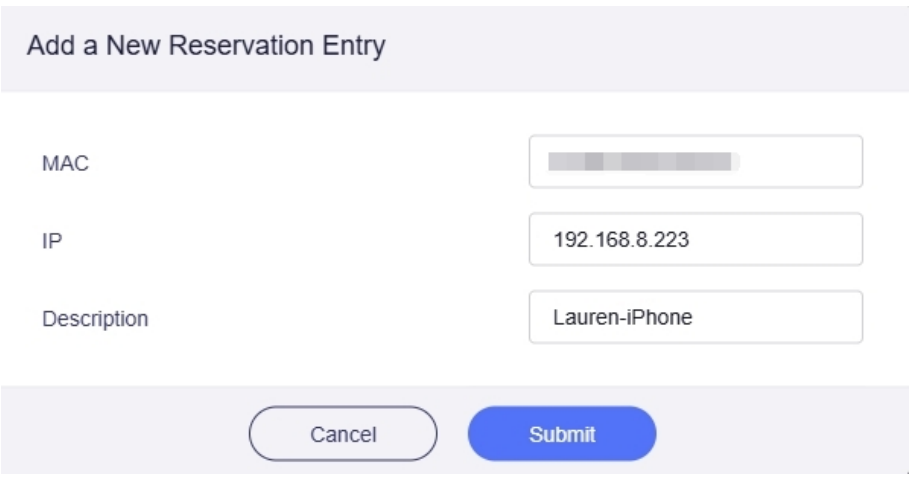
Uwaga: po wyłączeniu serwera DHCP trzeba ręcznie skonfigurować statyczny adres IP i inne parametry komunikacji na każdym urządzeniu klienckim. Szczegóły znajdziesz tutaj.

13.3.3 Rezerwacja adresów

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

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

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



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



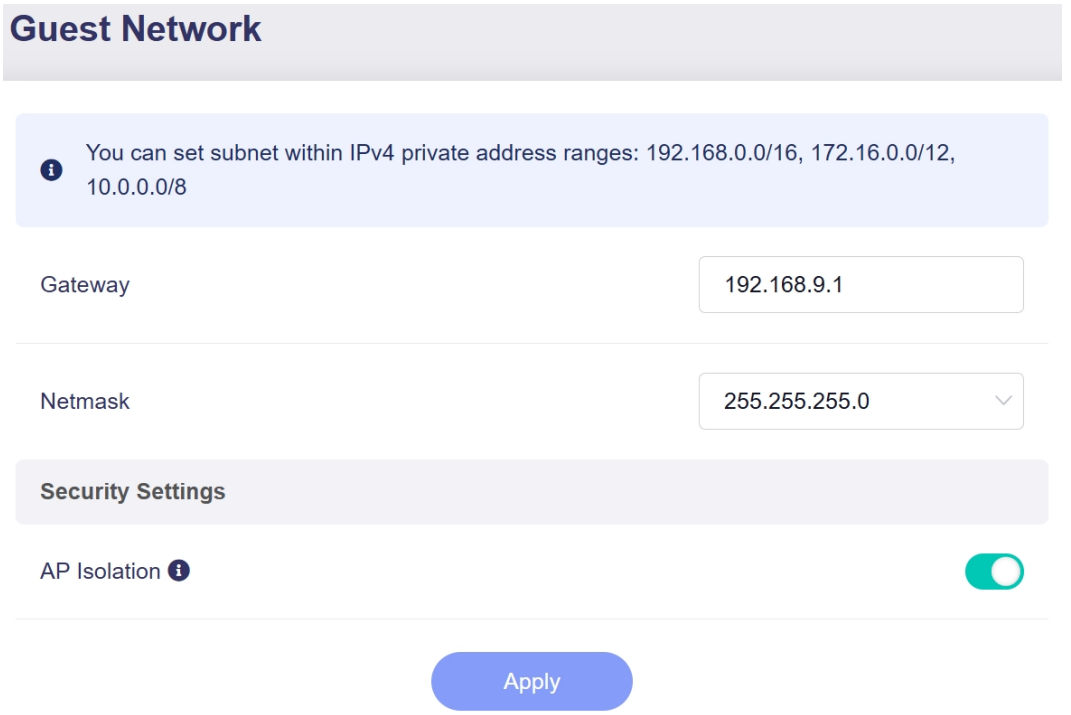
13.4 Sieć gościnna

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

Zaloguj się do panelu administracyjnego routera i przejdź do **NETWORK** > **Guest Network**. Tutaj możesz konfigurować ustawienia sieci gościnnej: ustawienia podstawowe i serwer DHCP.

13.4.1 Ustawienia podstawowe

Ustawienia podstawowe obejmują bramę, maskę sieci i izolację AP.

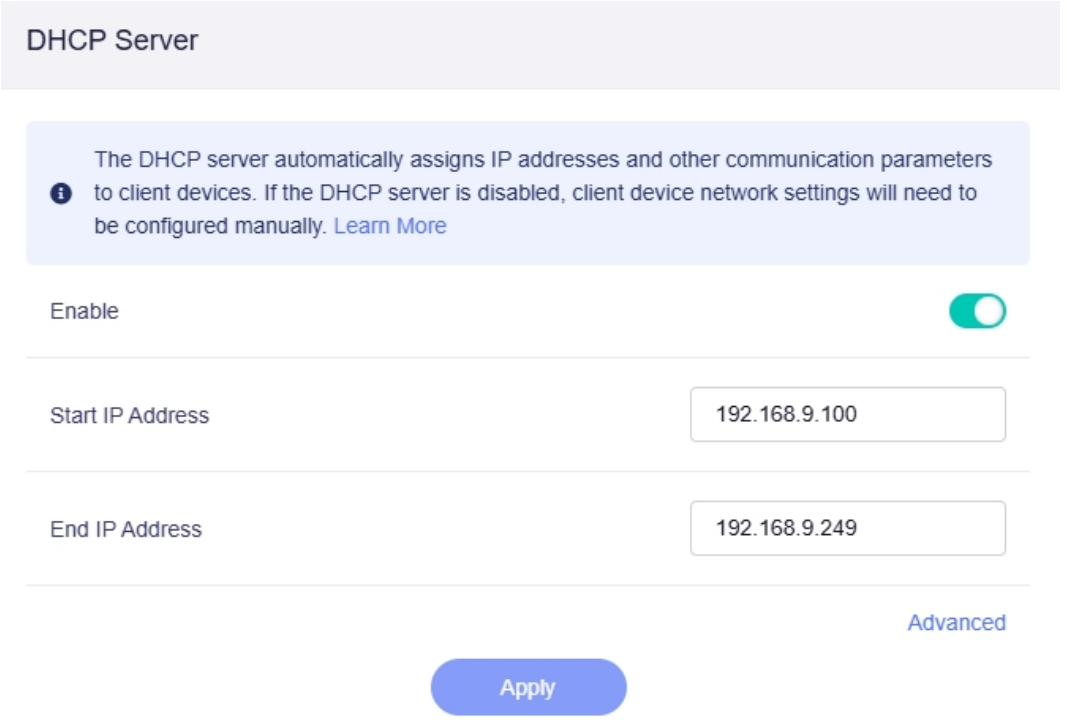


- **Gateway**: domyślny adres to 192.168.9.1. Można go zmienić, ale nie może kolidować z adresem bramy sieci głównej.
- **Netmask**: dostępne są dwie opcje: 255.255.255.0 i 255.255.0.0.
- **AP Isolation**: izoluje klientów sieci gościnnej w oddzielnych segmentach, aby nie mogli komunikować się z innymi urządzeniami w tej samej sieci.

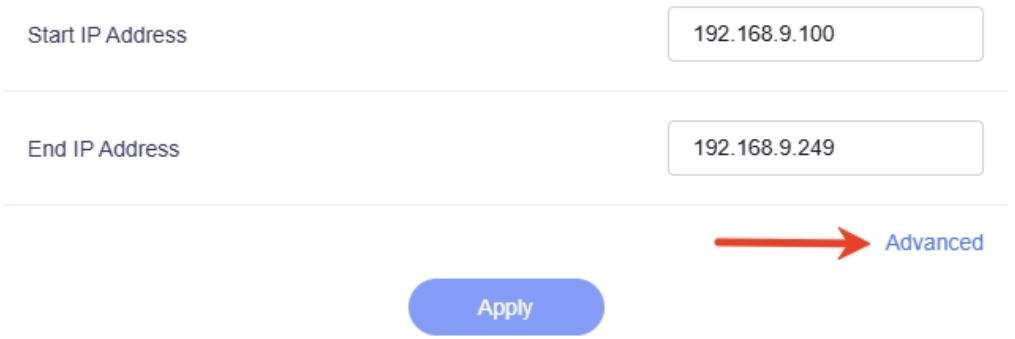
13.4.2 Serwer DHCP

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

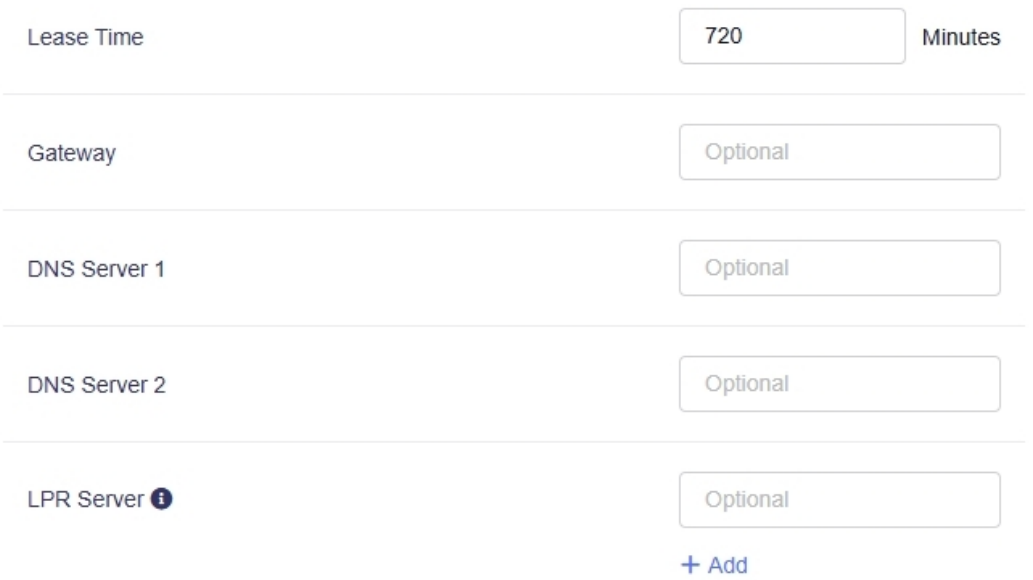
Po włączeniu serwer DHCP automatycznie przydziela adresy IP i inne parametry komunikacji każdemu podłączonemu klientowi. Pula adresów IP sieci gościnnej obejmuje zakres od 192.168.9.100 do 192.168.9.249. W razie potrzeby można go zmienić.



Kliknij **Advanced** w prawym dolnym rogu.



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



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

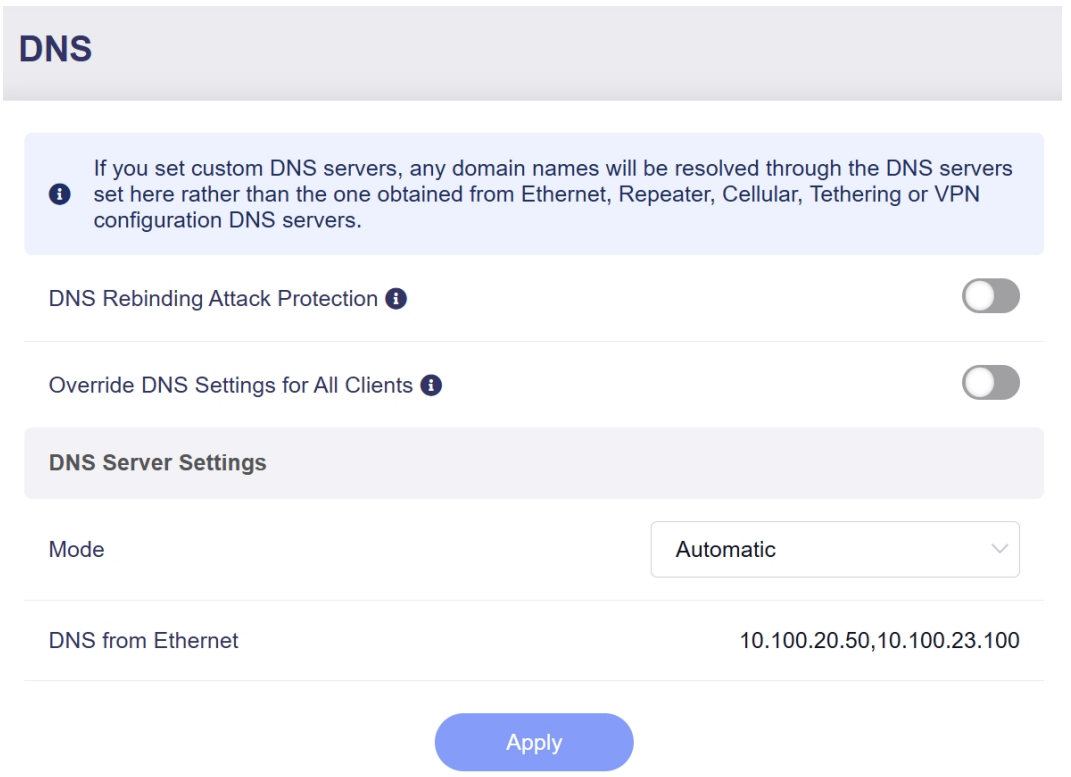
13.5 DNS

DNS (Domain Name System) to usługa tłumacząca czytelne dla człowieka nazwy domen, takie jak www.google.com, na adresy IP, dzięki czemu urządzenia mogą znajdować witryny i usługi internetowe oraz łączyć się z nimi.

Ustawienia DNS routera zwykle określają serwery DNS używane przez podłączone urządzenia. Router najczęściej pobiera ich adresy automatycznie od dostawcy Internetu lub sieci nadrzędnej albo pozwala ręcznie wskazać publiczne serwery DNS, np. 8.8.8.8, w interfejsie zarządzania. Skonfigurowane ustawienia są zazwyczaj automatycznie przekazywane podłączonym urządzeniom, dlatego nie trzeba ustawiać DNS na każdym z nich oddzielnie.

Zaloguj się do panelu administracyjnego routera i przejdź do **NETWORK** > **DNS**. Tutaj możesz konfigurować ustawienia DNS.

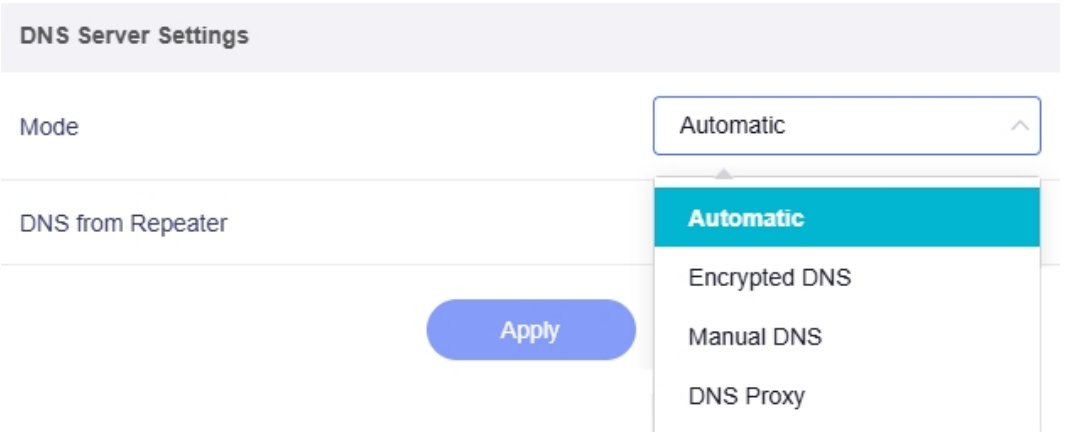
13.5.1 Ustawienia ogólne



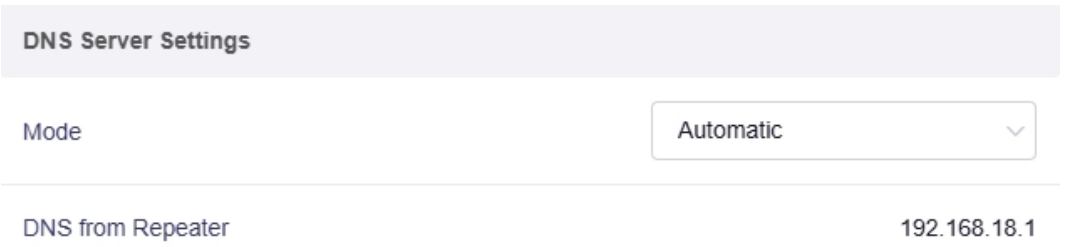
- **DNS Rebinding Attack Protection**: chroni przed atakami DNS rebinding przez blokowanie złośliwych prób rozwiązywania nazw DNS. Włączenie może spowodować problemy z prywatnymi zapytaniami DNS. Wyłącz tę opcję, jeśli sieć korzysta z portalu logowania (np. strony logowania do publicznego Wi-Fi).
- **Override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

13.5.2 Ustawienia serwera DNS

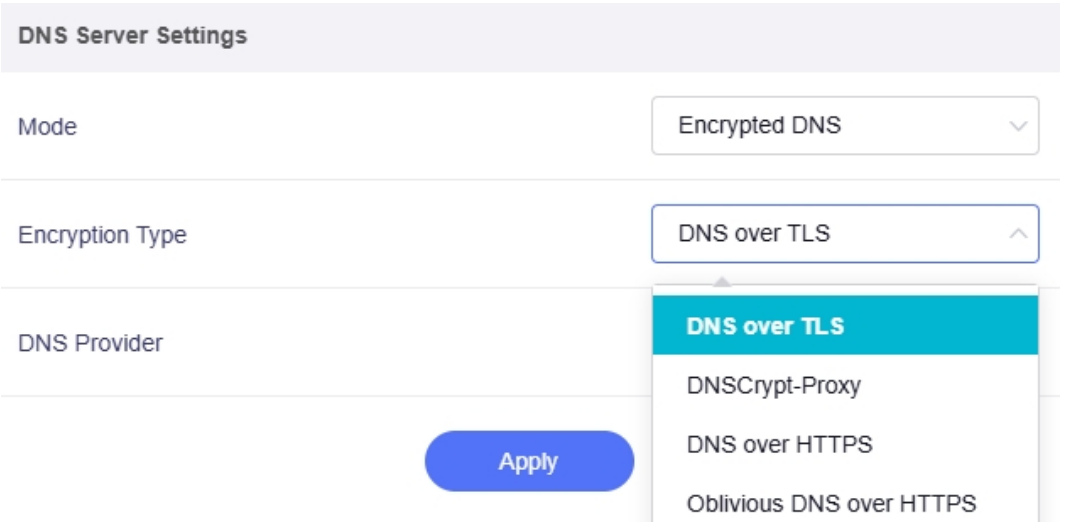
Dostępne są cztery tryby serwera DNS: Automatic, Encrypted DNS, Manual DNS i DNS Proxy.



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

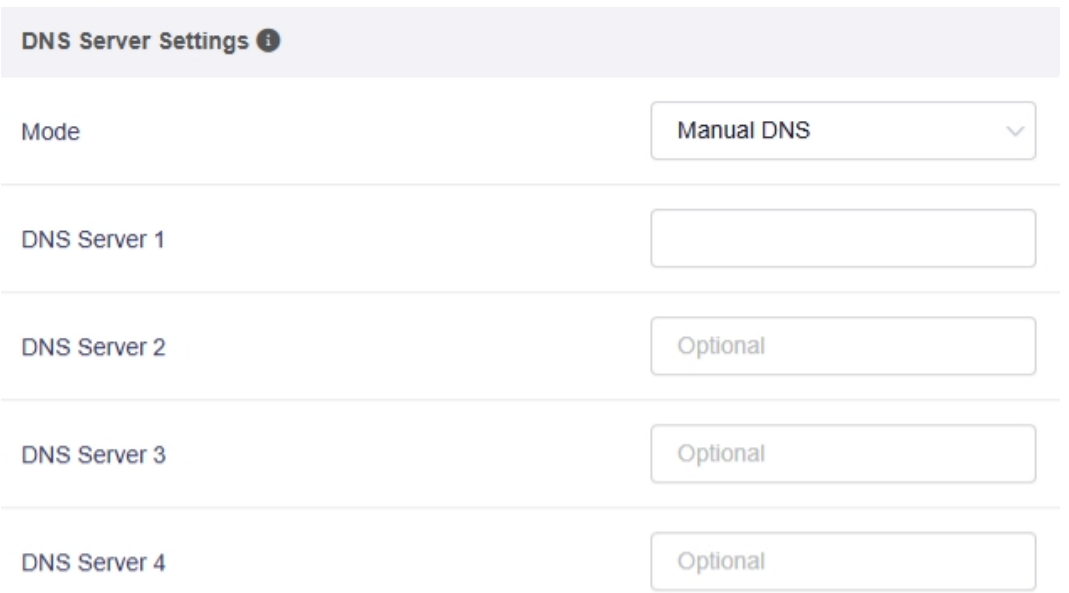


2. **Encrypted DNS**: router używa szyfrowanych protokołów do obsługi zapytań DNS, chroniąc dane rozwiązywania nazw przed podsłuchiwaniem i modyfikacją. Dostępne są cztery rodzaje szyfrowania: DNS over TLS, DNSCrypt-Proxy, DNS over HTTPS i Oblivious DNS over HTTPS.



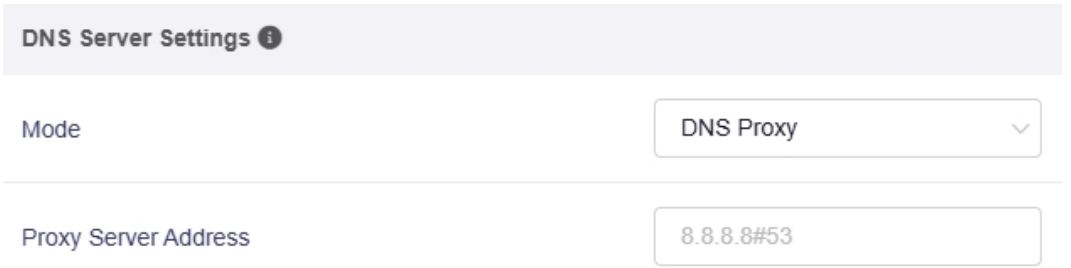
- Dla DNS over TLS wybierz dostawcę DNS spośród Control D, NextDNS i Cloudflare.
- Dla pozostałych trzech opcji (DNSCrypt-Proxy, DNS over HTTPS i Oblivious DNS over HTTPS) wybierz z repozytorium co najmniej jeden serwer DNS. Można wybrać maksymalnie 8 serwerów. Przy wielu serwerach router automatycznie używa najszybszego.

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



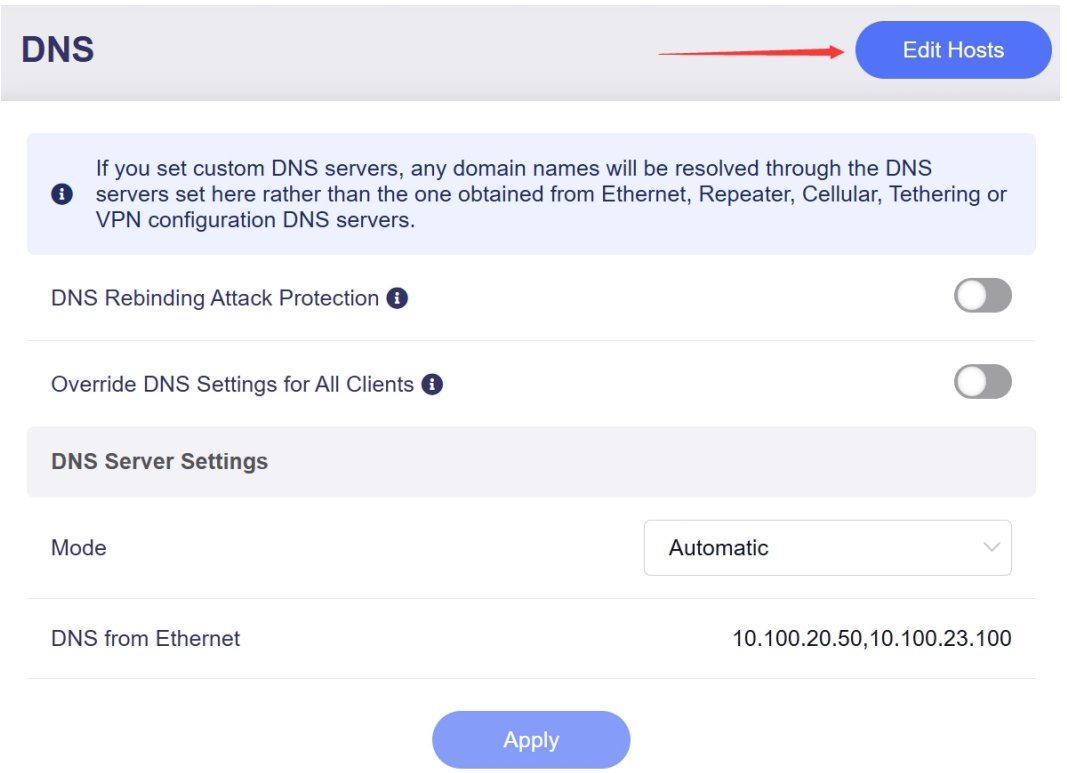
Uwaga: aby używać adresów IPv6 w ręcznej konfiguracji DNS, najpierw włącz IPv6 na routerze.

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

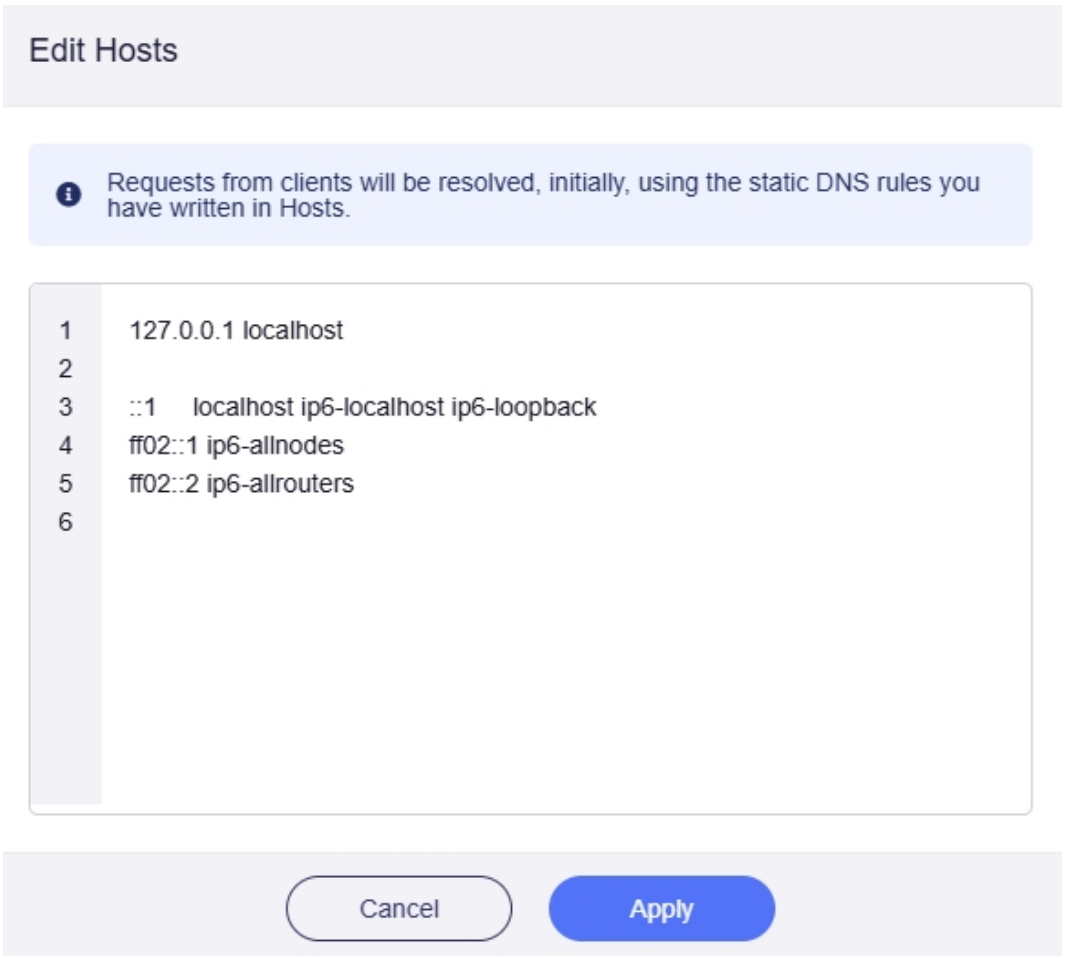


13.5.3 Edycja pliku hosts

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



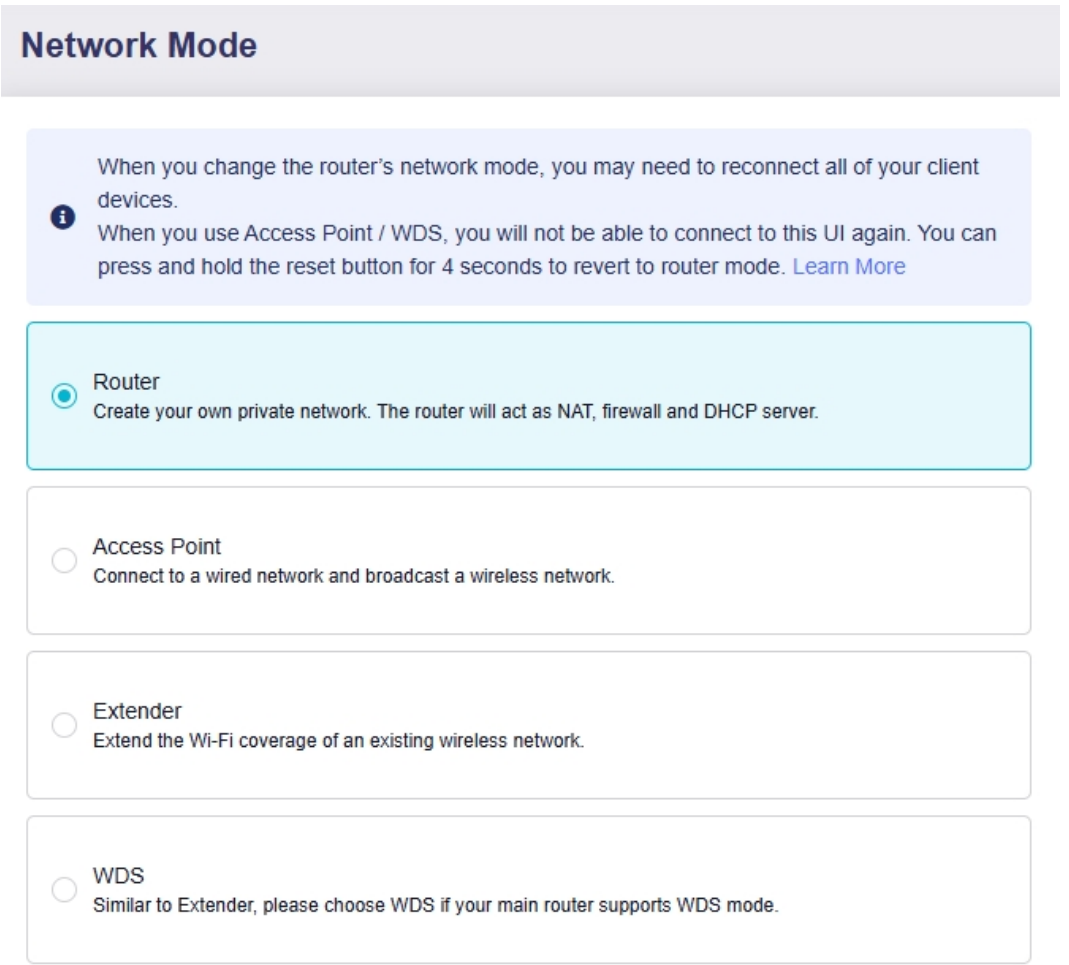
Żądania klientów są rozwiązywane w pierwszej kolejności według wpisanych tutaj statycznych reguł DNS. Pozwala to ręcznie mapować adresy IP na nazwy hostów (np. domyślny wpis 127.0.0.1 localhost dla lokalnej pętli zwrotnej) i samodzielnie kontrolować rozwiązywanie nazw domen.


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

13.6 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:

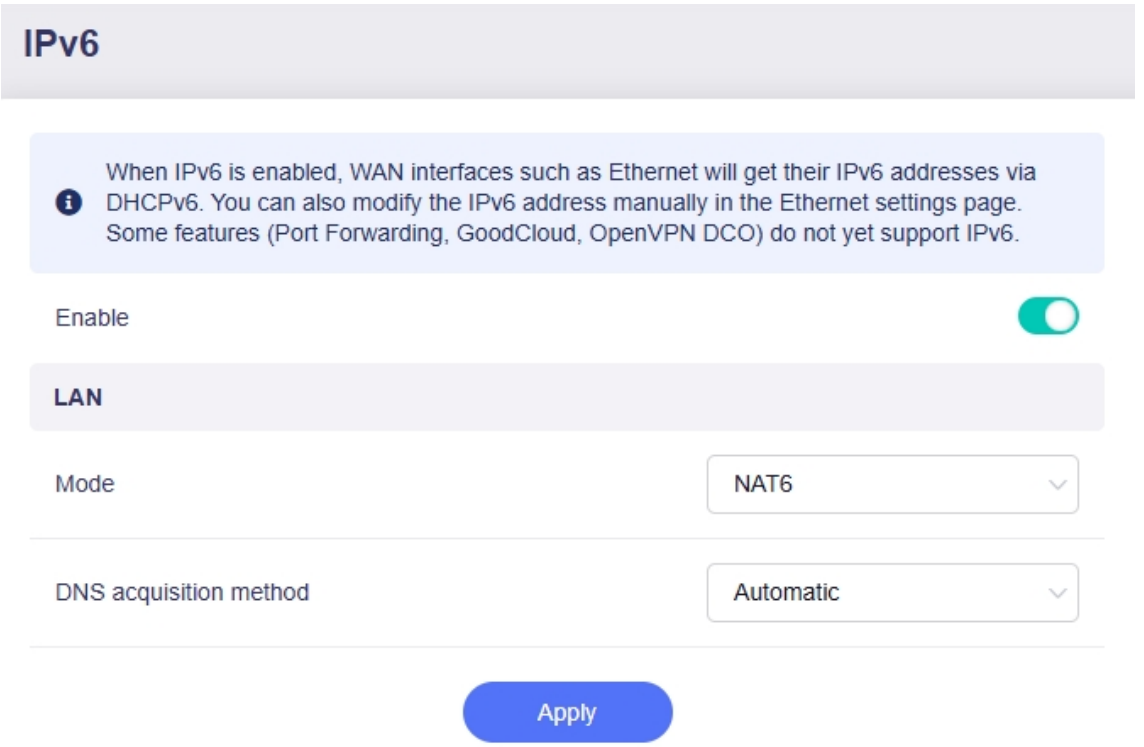
1. Po zmianie trybu sieciowego wszystkie urządzenia klienckie powinny ponownie połączyć się z routerem, aby zapewnić stabilną łączność.
2. **W trybie Access Point / WDS panel administracyjny nie jest dostępny pod pierwotnym adresem IP**. Zaloguj się do routera nadrzędnego, znajdź adres IP przydzielony 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 trybie Access Point / Extender / WDS niedostępne są następujące funkcje**: kontrola dostępu (Allowlist i Blocklist), VPN, AdGuard Home, kontrola rodzicielska, ZeroTier, Tailscale, zapora, Multi-WAN, serwer DHCP, rezerwacja adresów, sieć gościnna, DNS, IPv6, Drop-in Gateway, IGMP Snooping i ustawienia NAT.

13.7 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 i GoodCloud) nie obsługują jeszcze IPv6. Włączenie ich jednocześnie z IPv6 może powodować problemy z łącznością.

13.7.1 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.

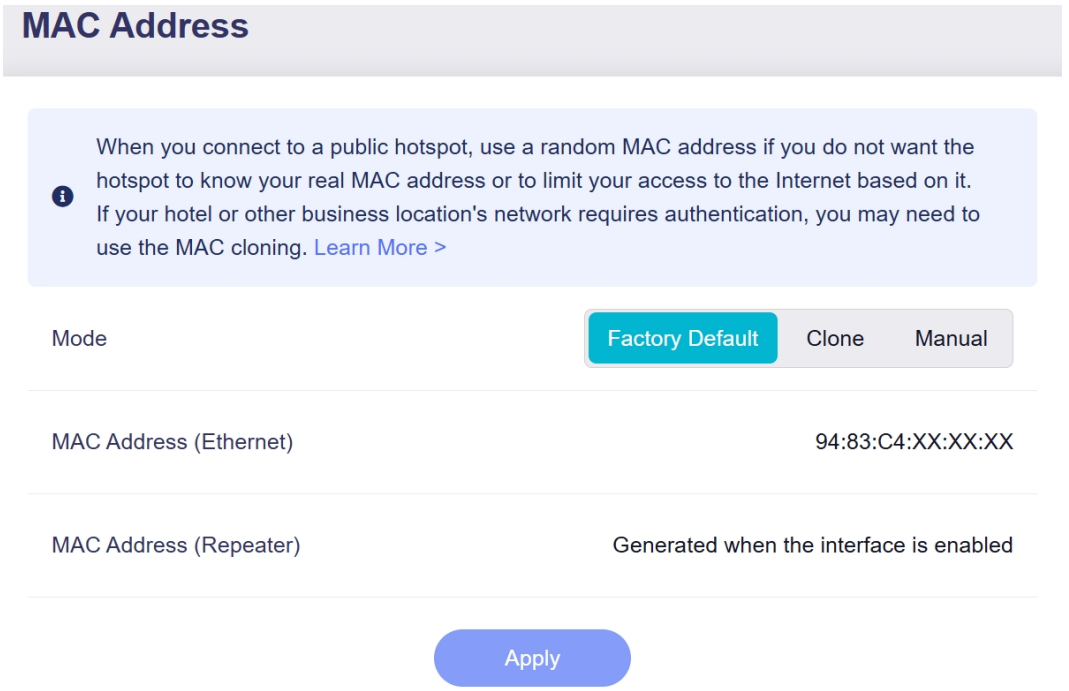
13.7.2 Sposób uzyskiwania DNS

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

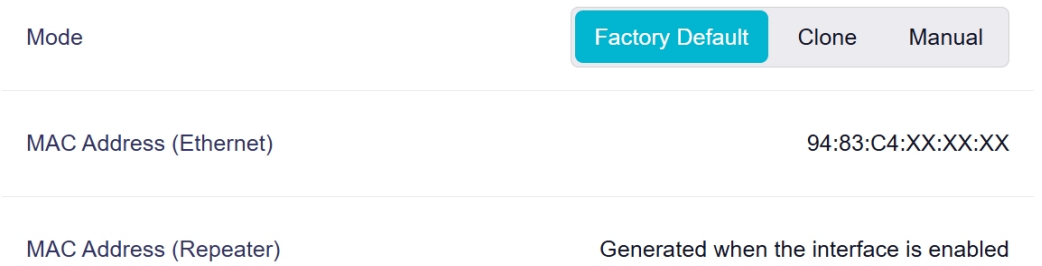
- **Automatic**: router dynamicznie uzyskuje adresy serwerów DNS IPv6 (np. przez DHCPv6).
- **Manual**: wprowadź własne adresy serwerów DNS IPv6. Ponieważ DNS służy do tłumaczenia nazw domen na odpowiadające im adresy IP, ręczna konfiguracja serwera DNS może powodować błędy rozwiązywania nazw. Używaj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

13.8 Adres MAC

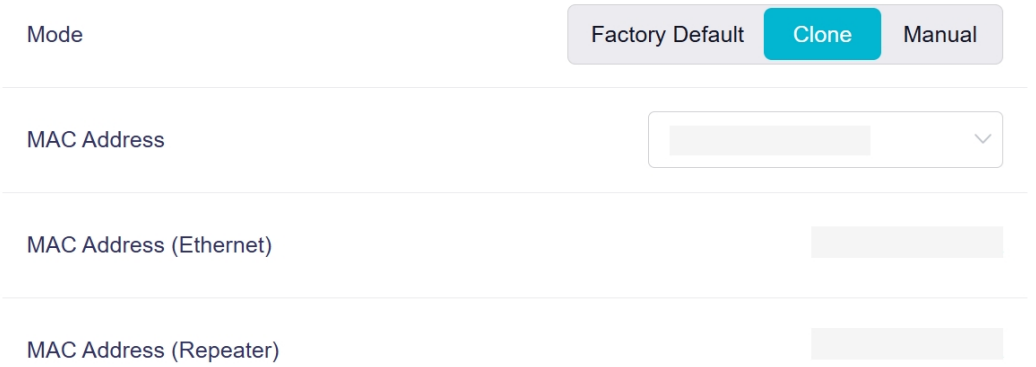
Strona MAC Address wyświetla domyślny adres MAC routera i umożliwia sklonowanie adresu klienta, ręczne wprowadzenie adresu lub wygenerowanie losowego adresu MAC. Jeśli urządzenie obsługuje używanie wielu portów Ethernet jako portów WAN, można ustawić adres MAC każdego z nich oddzielnie. Ustawienie adresu MAC obowiązuje tylko wtedy, gdy port Ethernet jest używany jako WAN.



- **Fabryczny adres MAC.**

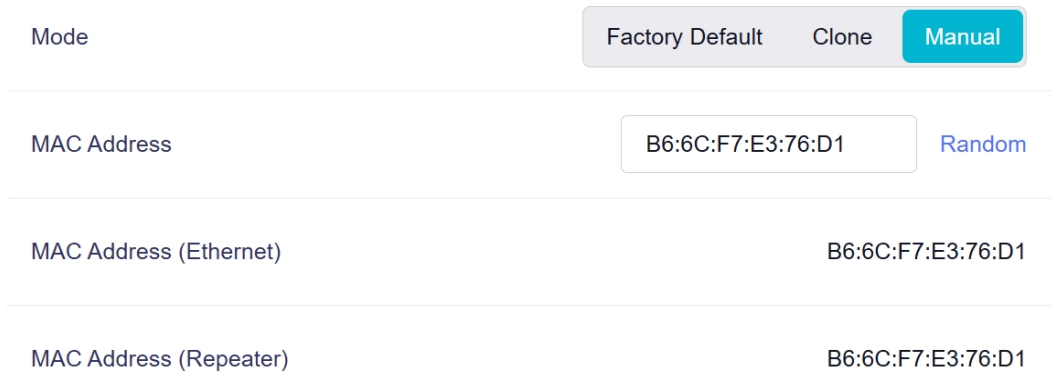


- **Klonowanie adresu MAC klienta.**



Uwaga: wiele nowych urządzeń używa różnych losowych adresów MAC do łączenia się z różnymi sieciami Wi-Fi, dlatego wyświetlony tutaj adres może nie być rzeczywistym adresem MAC urządzenia użytkownika. Na różnych urządzeniach losowy MAC może też nosić nazwę prywatnego adresu Wi-Fi lub losowego adresu sprzętowego.

- **Ręczne wprowadzenie lub wygenerowanie losowego adresu MAC.**

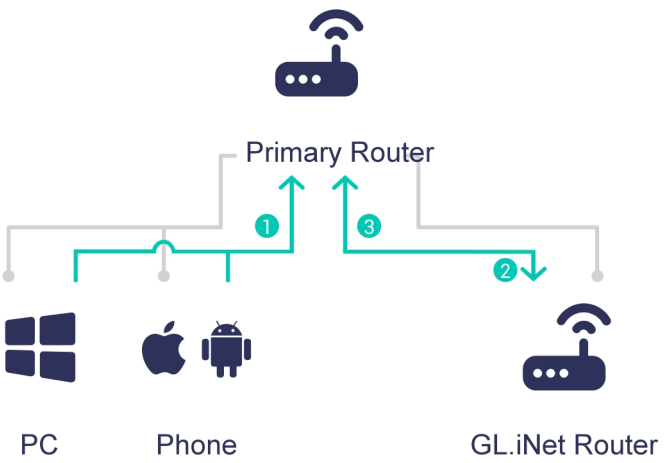


13.9 Drop-in Gateway

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

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

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



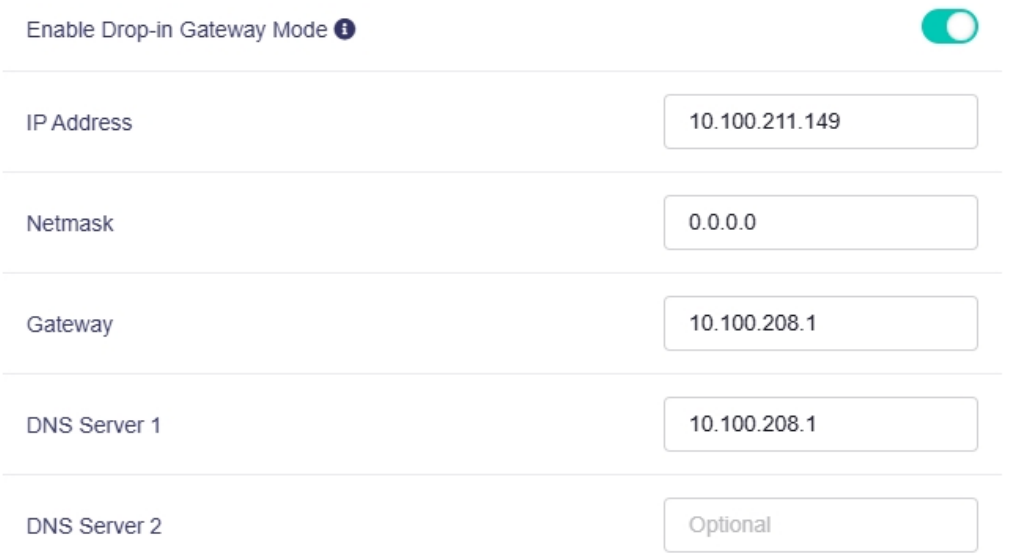
Powyższy schemat zawiera dwa rodzaje linii: szare oraz zielone z trzema strzałkami oznaczonymi numerami.

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

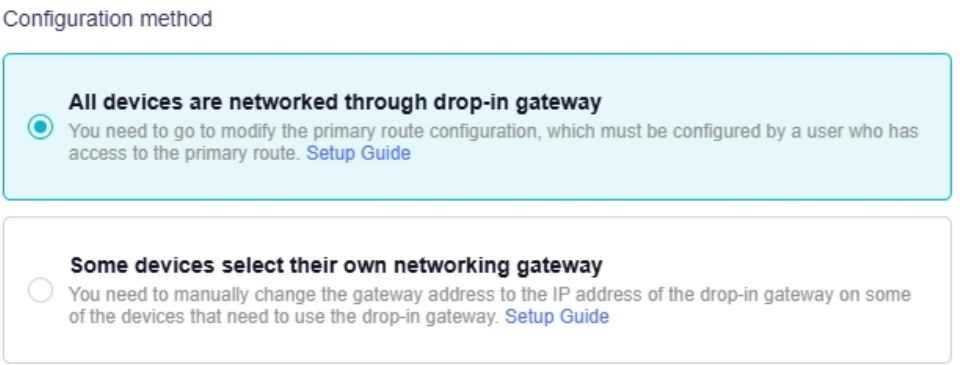
1. Ruch urządzeń klienckich jest najpierw kierowany do głównego routera;
2. Główny router przekazuje ruch do routera GL.iNet w celu przetworzenia (np. filtrowania reklam, szyfrowania VPN);
3. Po przetworzeniu ruch wraca do głównego routera, który dostarcza dane do pierwotnych urządzeń klienckich lub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

Aby w razie potrzeby włączyć Drop-in Gateway, wykonaj poniższe czynności.

1. Zaloguj się do panelu administracyjnego routera i przejdź do **NETWORK** > **Drop-in Gateway**. Włącz **Enable Drop-in Gateway Mode** i sprawdź parametry sieci.



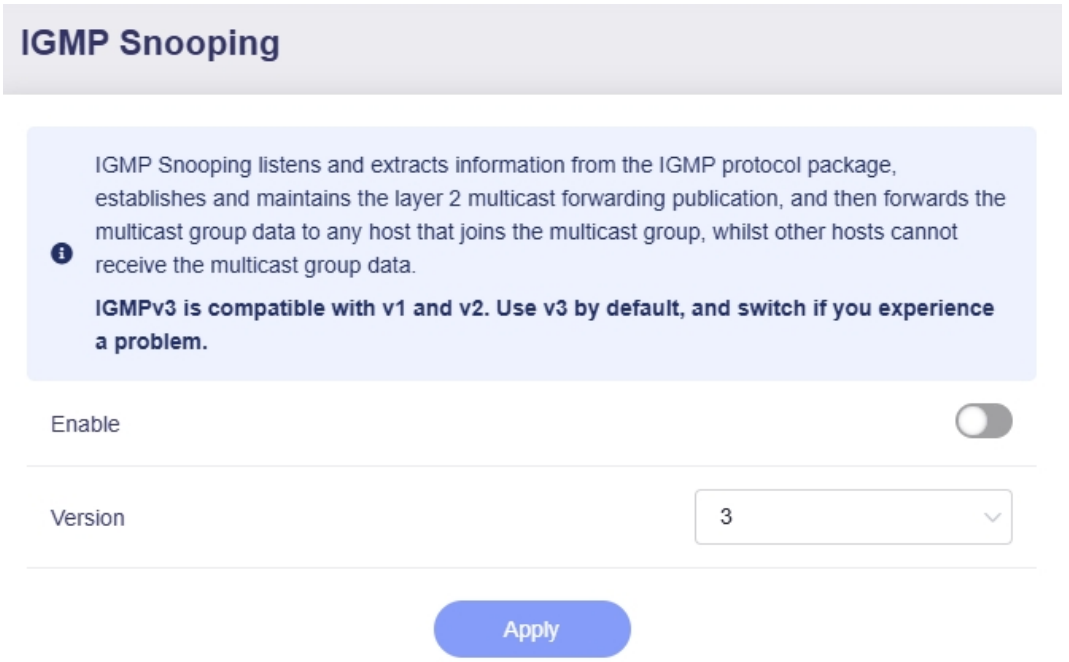
2. Wybierz sposób konfiguracji i kliknij **Apply**. Szczegóły znajdziesz w tym poradniku.



13.10 IGMP Snooping

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

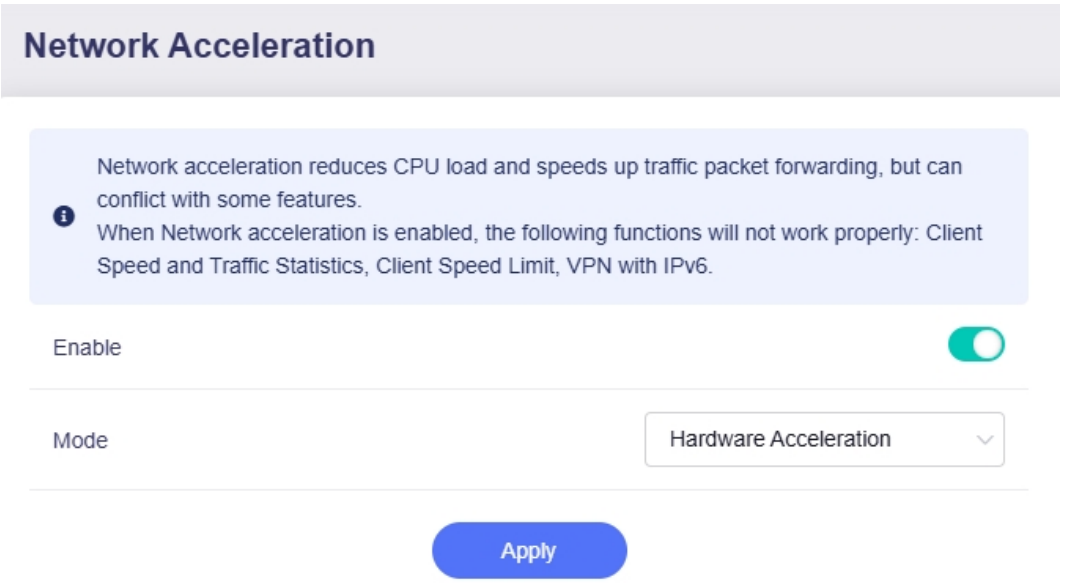
Zaloguj się do panelu administracyjnego routera i przejdź do **NETWORK** > **IGMP Snooping**. W razie potrzeby włącz tę opcję, aby korzystać z multicastu na routerze.



13.11 Przyspieszanie sieci

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

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

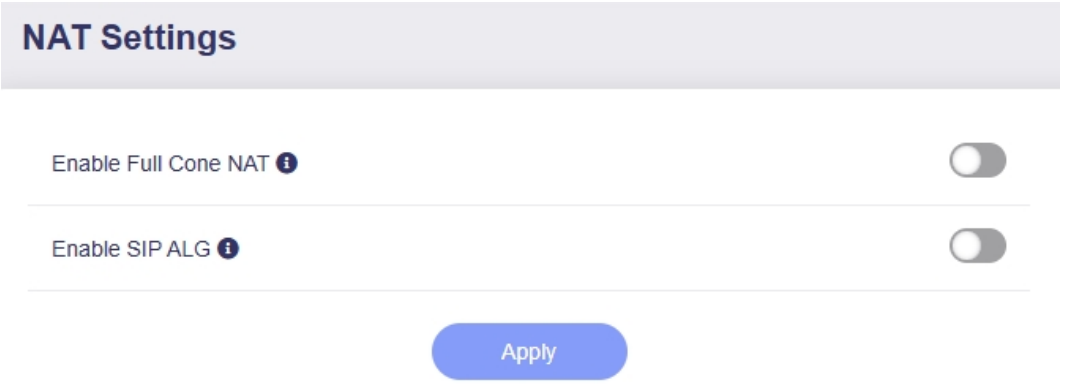


Tryb przyspieszania sprzętowego przenosi często wykonywane zadania sieciowe (np. NAT, przekazywanie pakietów i weryfikację sum kontrolnych) do wyspecjalizowanego sprzętu, takiego jak procesory NPU lub układy HWNAT. Działa w połączeniach Ethernet i Repeater. W takich zastosowaniach, ze stałymi ścieżkami i prostymi regułami, zapewnia wysoką przepustowość, małe opóźnienia i minimalne obciążenie procesora przy transmisji z pełną prędkością łącza.

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

13.12 Ustawienia NAT

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



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

Rozdział 14

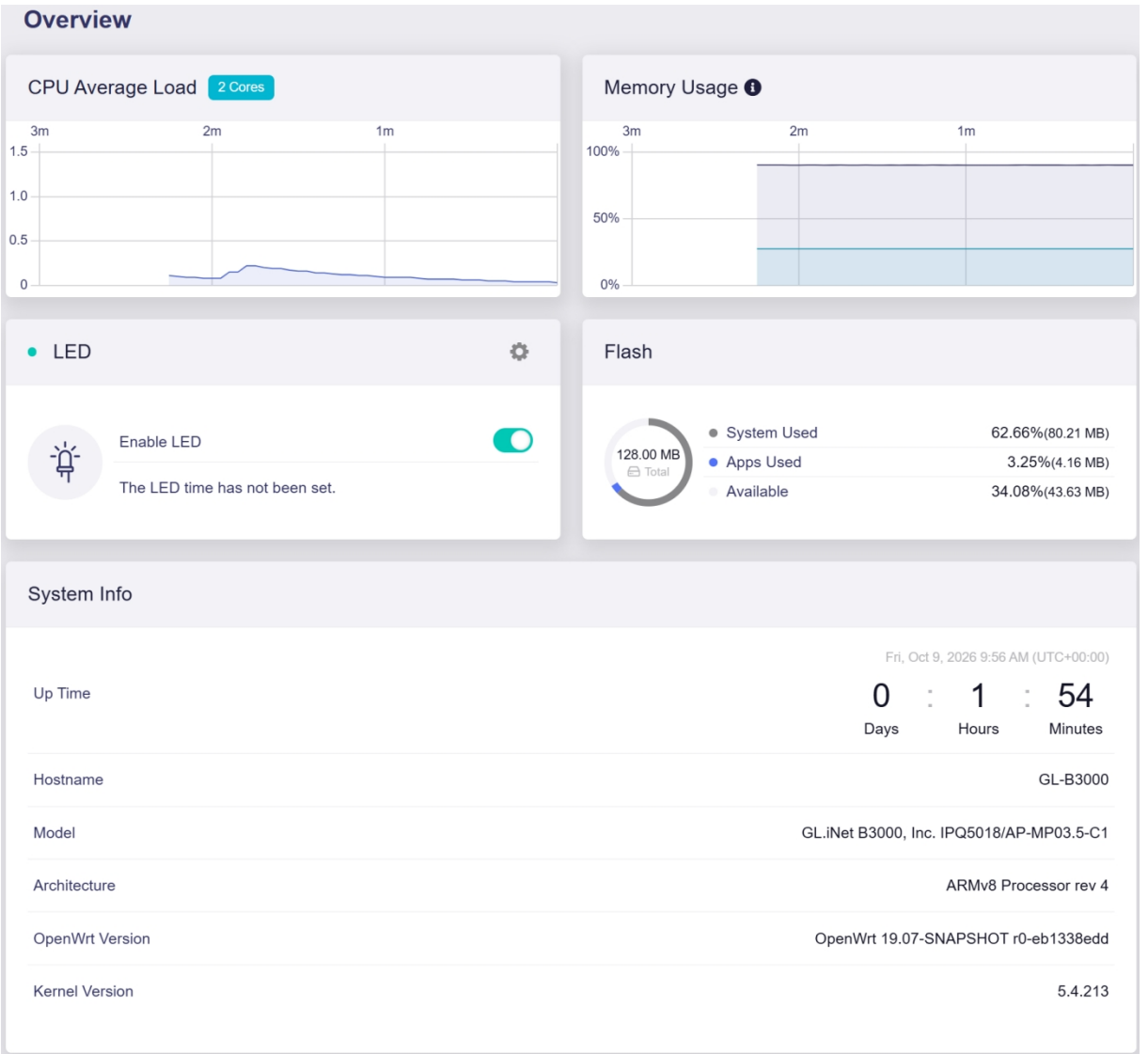
System

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

14.1 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

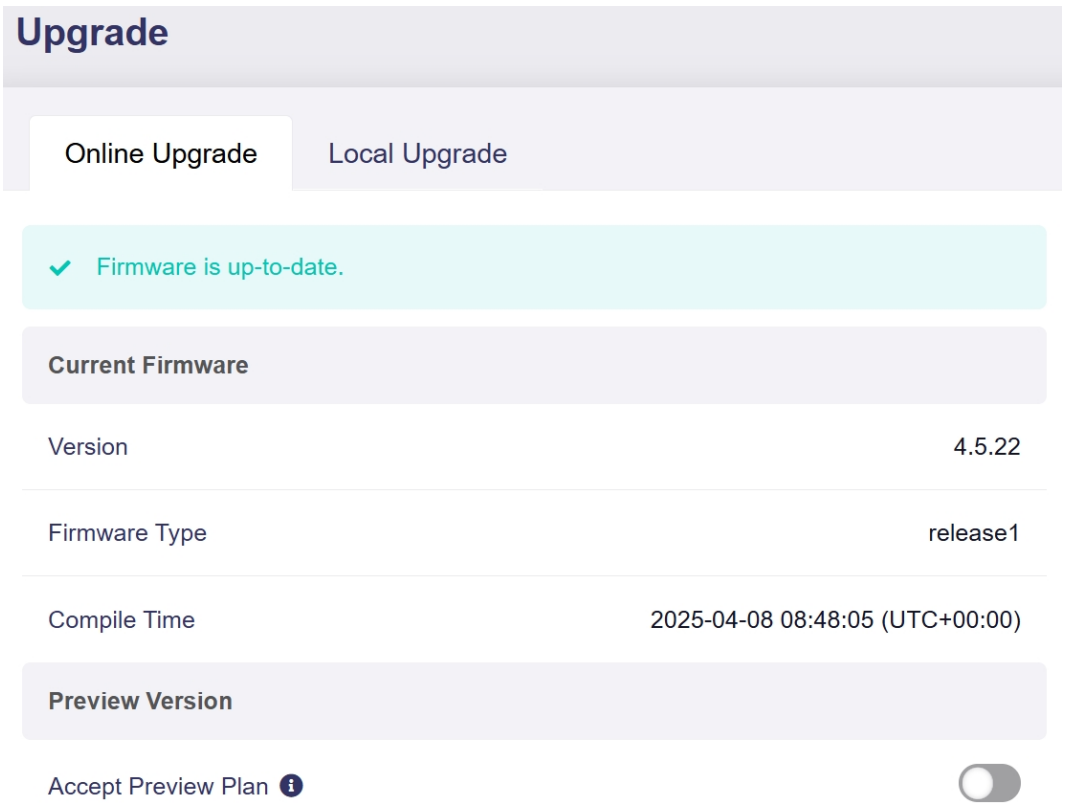


14.2 Aktualizacja

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

14.2.1 Aktualizacja online

Tutaj znajdziesz szczegóły bieżącego oprogramowania, w tym wersję, typ (np. wydanie stabilne, beta) i czas aktualizacji. Jeśli router ma połączenie z Internetem, sprawdzi dostępność nowszej wersji do pobrania.



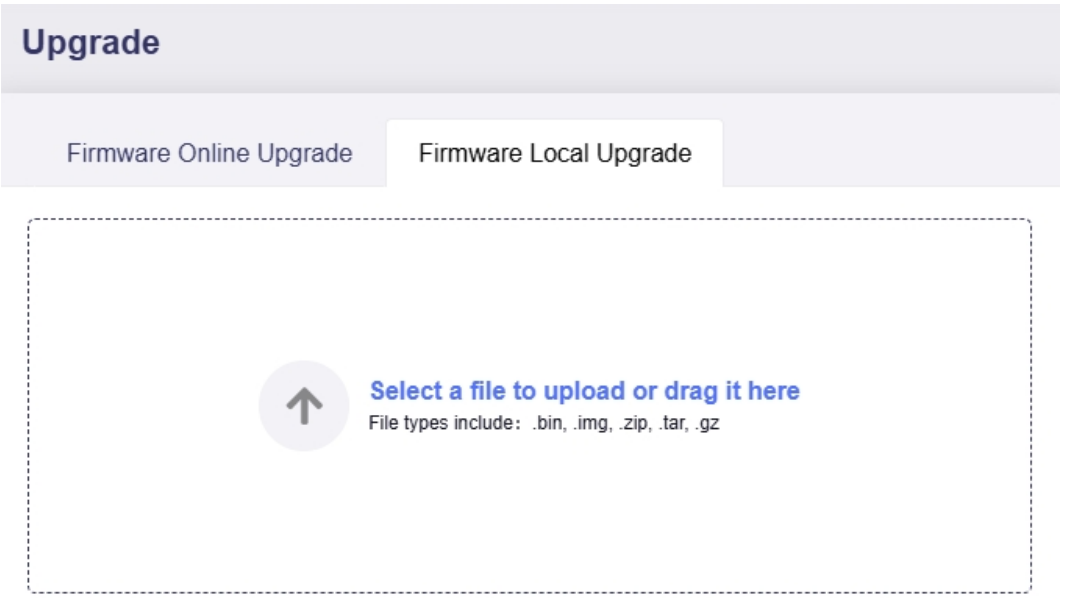
Po włączeniu **Accept Preview Plan** możesz testować nowe funkcje przed wydaniem wersji ostatecznej i przekazywać nam uwagi. Po jednorazowym włączeniu opcja pozostaje aktywna. Te aktualizacje mogą być niestabilne.

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

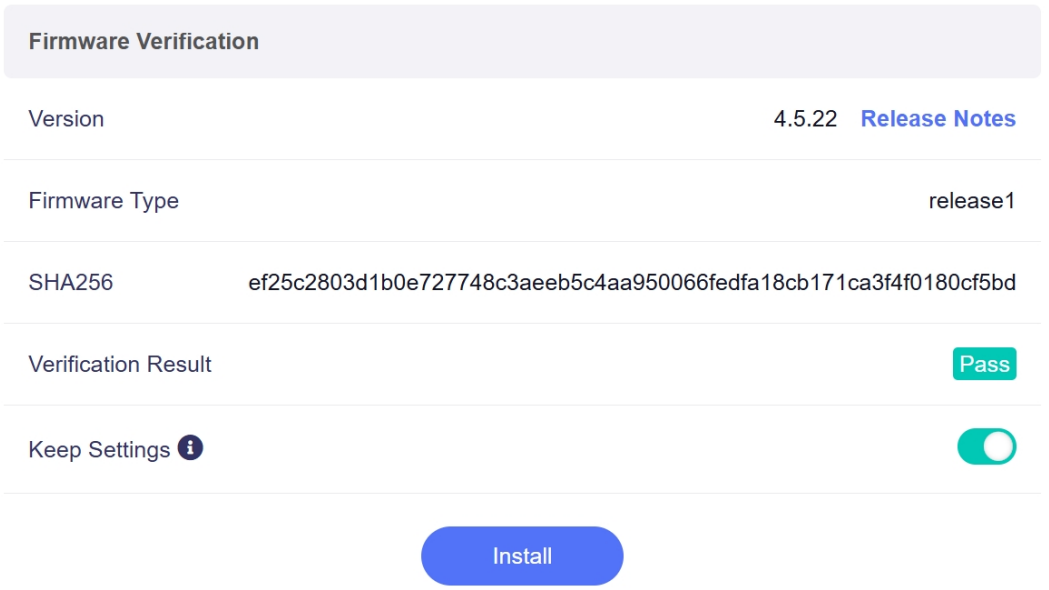
14.2.2 Aktualizacja lokalna

Aktualizacja lokalna nie wymaga połączenia routera z Internetem.

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



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



Jeśli opcja **Keep Settings** jest włączona, bieżące ustawienia zostają zachowane. Pakiety zainstalowane ręcznie trzeba jednak zainstalować ponownie po zakończeniu aktualizacji. Nie włączaj tej opcji przy instalowaniu starszej wersji oprogramowania.

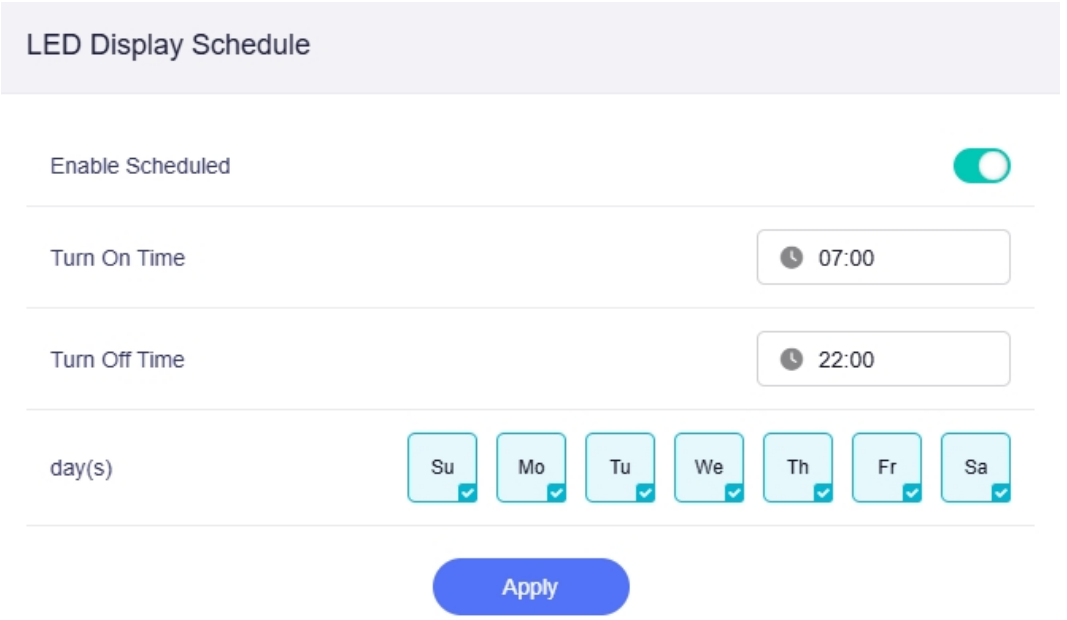
14.3 Zadania zaplanowane

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

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

14.3.1 Harmonogram diody LED

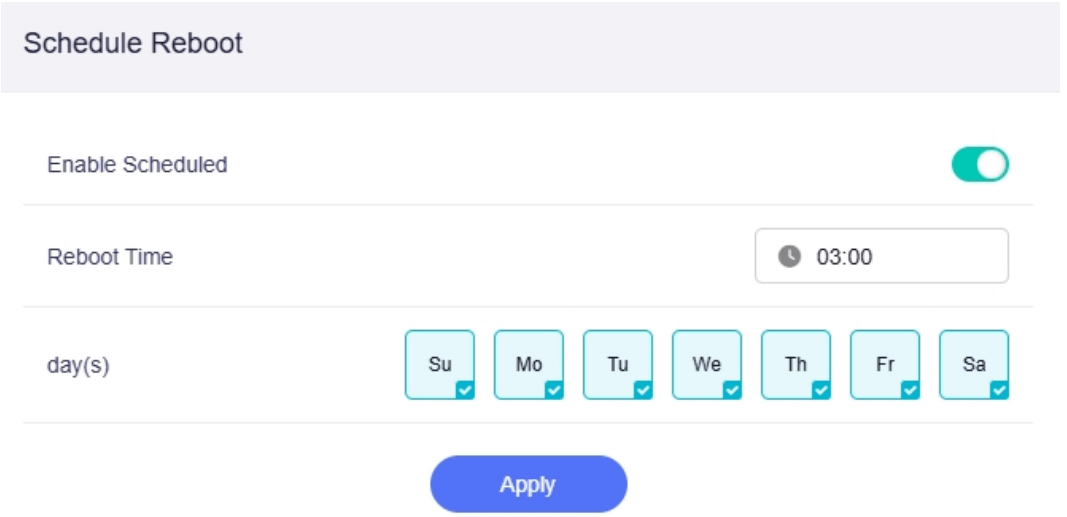
W razie potrzeby ustaw harmonogram diody LED routera i kliknij **Apply**.



- **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.

14.3.2 Harmonogram ponownego uruchamiania

W razie potrzeby ustaw harmonogram automatycznego ponownego uruchamiania routera i kliknij **Apply**.



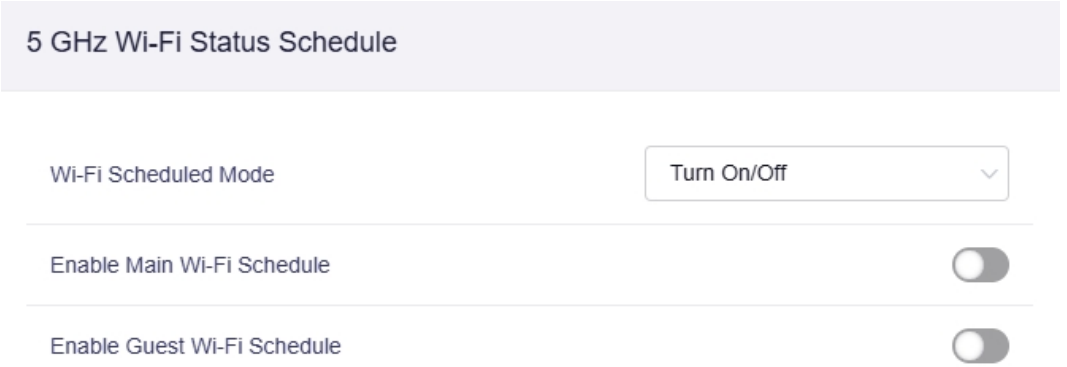
- **Enable Scheduled**: włącz ten przełącznik, aby uruchomić harmonogram ponownego uruchamiania.
- **Reboot Time**: ustaw konkretną godzinę ponownego uruchomienia routera (np. 03:00).
- **day(s)**: wybierz dni tygodnia, w których te ustawienia mają obowiązywać.

14.3.3 Harmonogram Wi-Fi 5 GHz

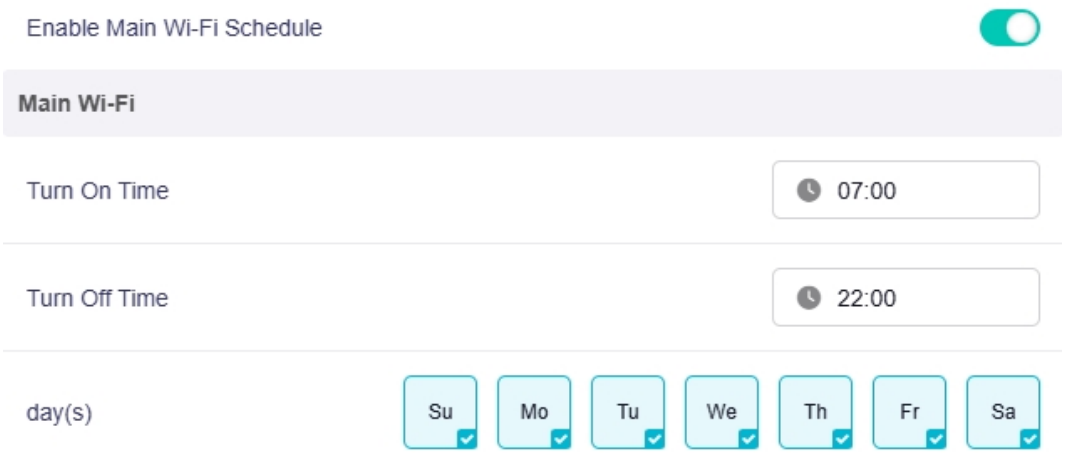
Ta funkcja umożliwia ustawienie harmonogramu Wi-Fi 5 GHz. Dostępne są dwa tryby: Turn On/Off i Switch TX Power.

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

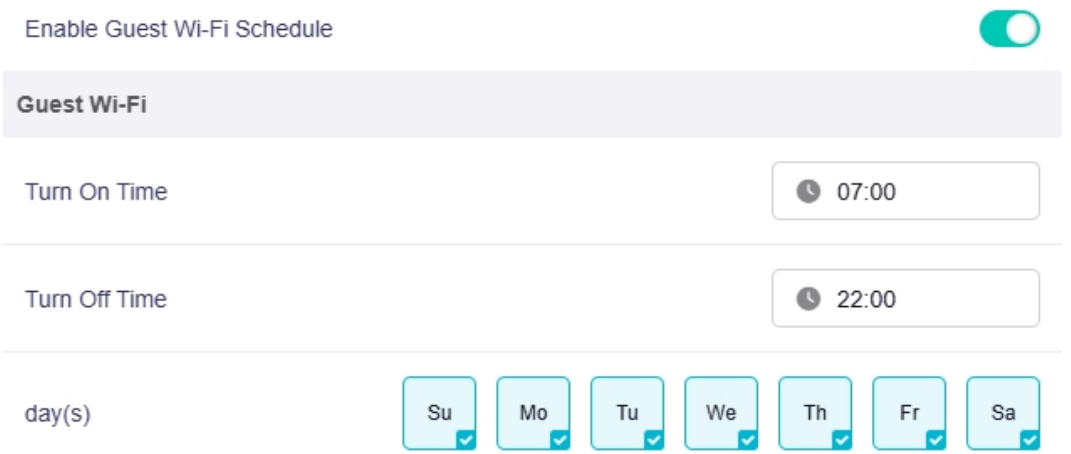
Możesz włączyć harmonogram włączania i wyłączania głównej oraz gościnnej sieci Wi-Fi 5 GHz.



- **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.

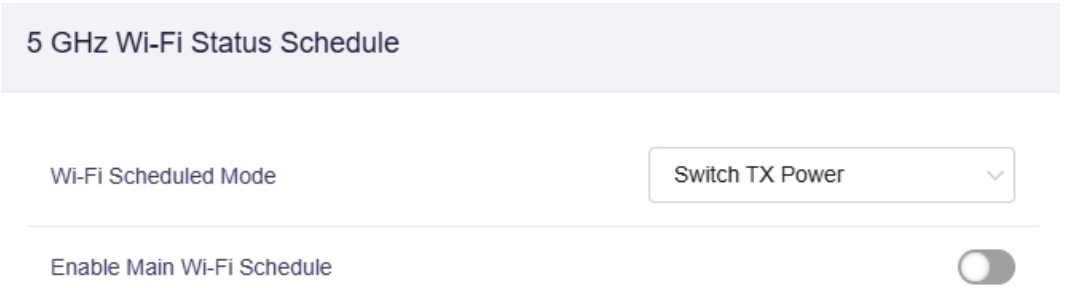


- **Guest Wi-Fi Schedule**: po włączeniu ustaw godziny włączania i wyłączania gościnnej sieci Wi-Fi 5 GHz oraz wybierz dni tygodnia, w których harmonogram obowiązuje.

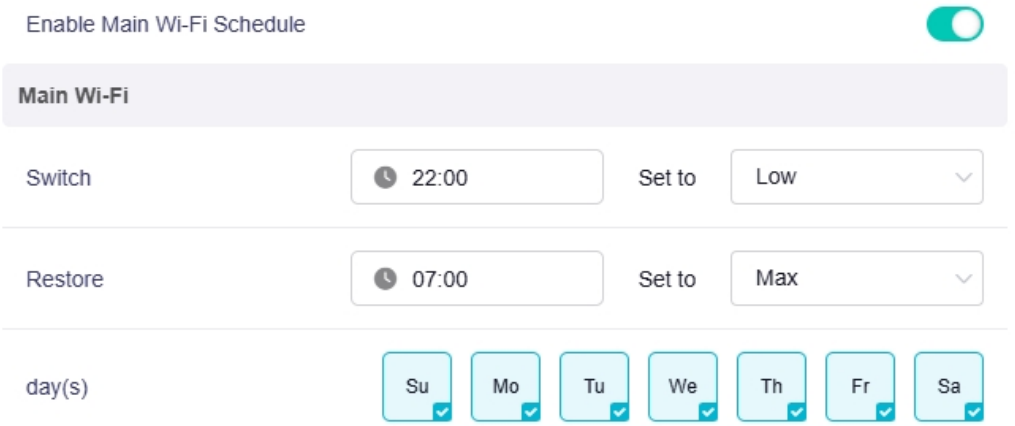


Tryb 2: przełączanie mocy nadawania (Switch TX Power)

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.



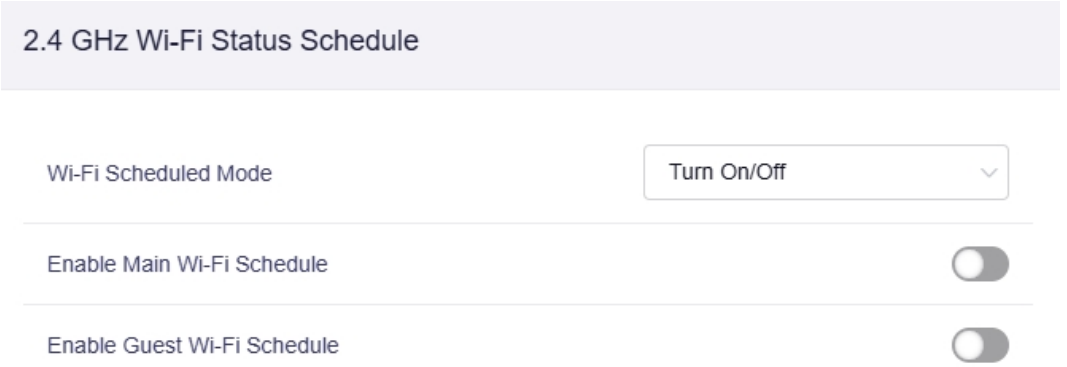
- **Switch**: o wybranej porze (np. 22:00) ustawia moc nadawania (np. Low).
- **Restore**: przywraca inny poziom mocy nadawania (np. Max) o innej godzinie (np. 07:00).
- **days**: wybierz dni tygodnia, w których te ustawienia mają obowiązywać.

14.3.4 Harmonogram Wi-Fi 2,4 GHz

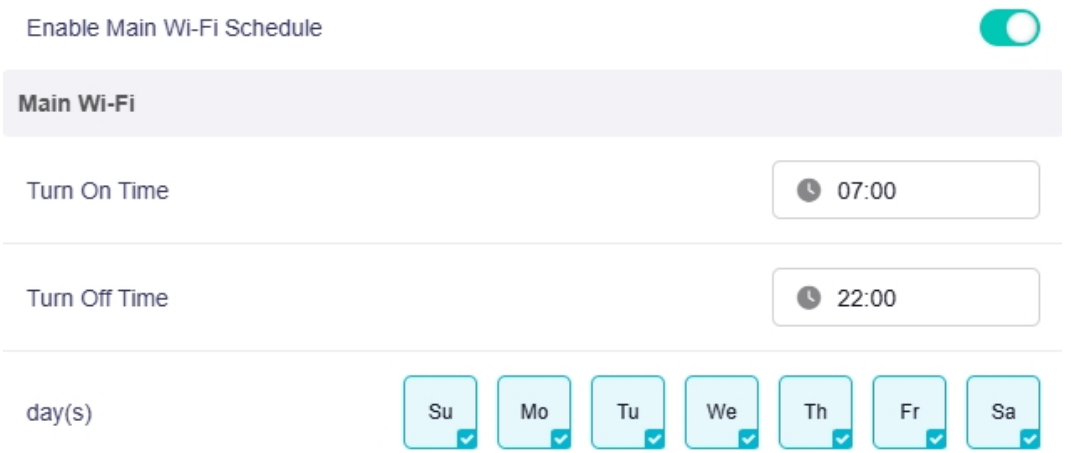
Ta funkcja umożliwia ustawienie harmonogramu Wi-Fi 2,4 GHz. Dostępne są dwa tryby: Turn On/Off i Switch TX Power.

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

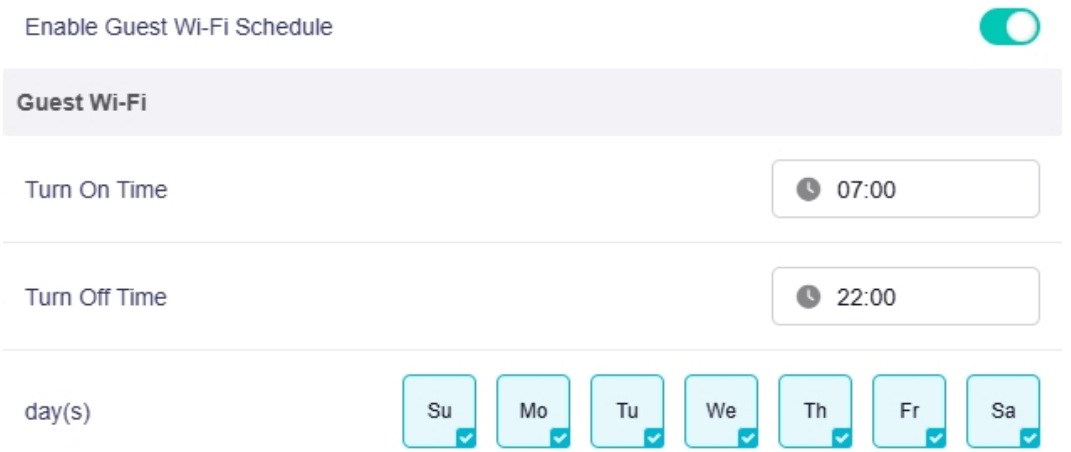
Możesz włączyć harmonogram włączania i wyłączania głównej oraz gościnnej sieci Wi-Fi 2,4 GHz.



- **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.

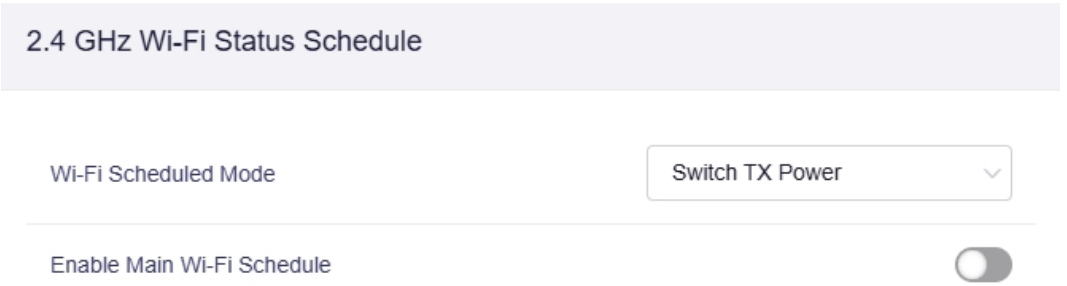


- **Guest Wi-Fi Schedule**: po włączeniu ustaw godziny włączania i wyłączania gościnnej sieci Wi-Fi 2,4 GHz oraz wybierz dni tygodnia, w których harmonogram obowiązuje.

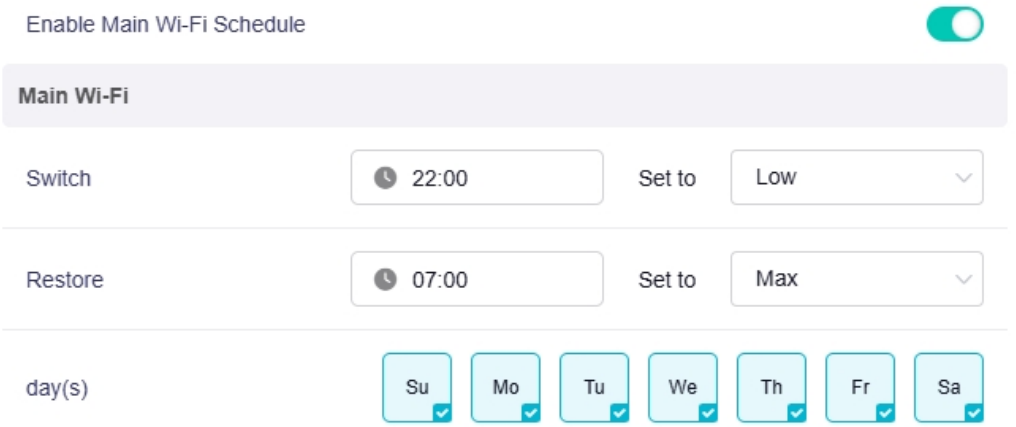


Tryb 2: przełączanie mocy nadawania (Switch TX Power)

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



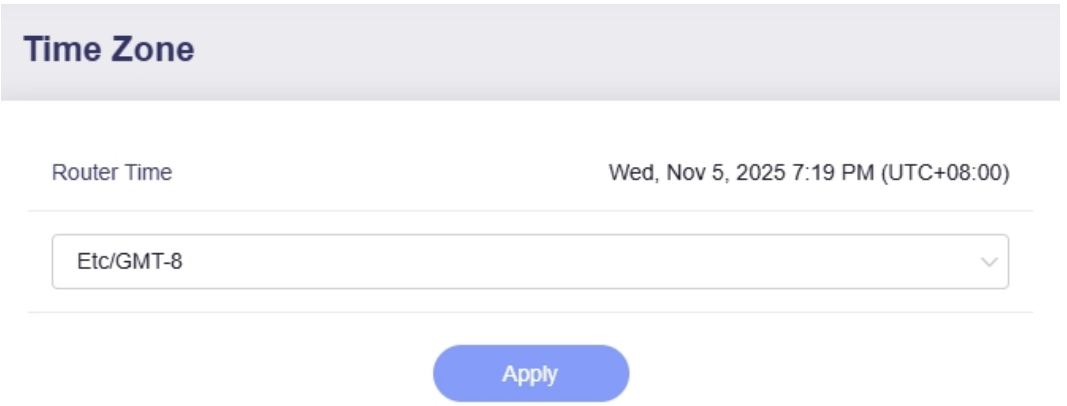
Po włączeniu ustaw dwie zaplanowane czynności zmiany mocy nadawania głównej sieci Wi-Fi 2,4 GHz oraz wybierz dni tygodnia, w których obowiązują.



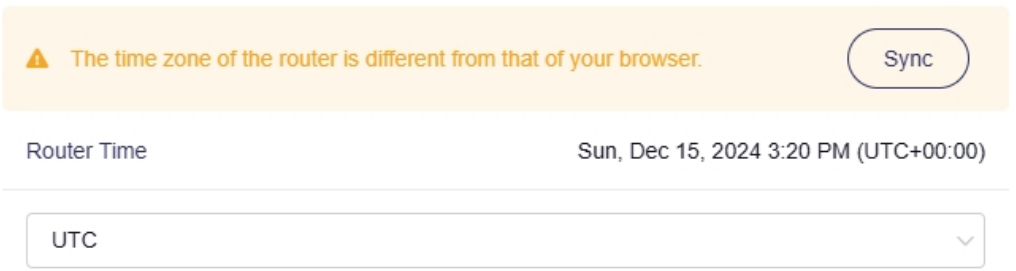
- **Switch**: o wybranej porze (np. 22:00) ustawia moc nadawania (np. Low).
- **Restore**: przywraca inny poziom mocy nadawania (np. Max) o innej godzinie (np. 07:00).
- **days**: wybierz dni tygodnia, w których te ustawienia mają obowiązywać.

14.4 Strefa czasowa

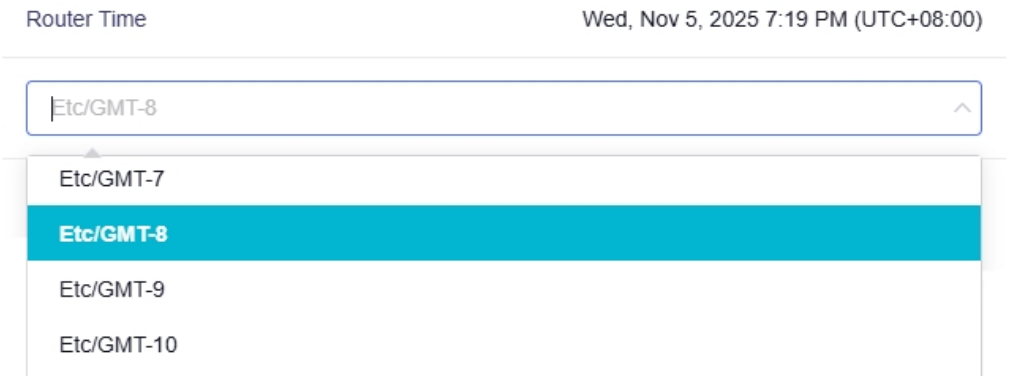
Zaloguj się do panelu administracyjnego routera i przejdź do **SYSTEM** > **Time Zone**. Strona wyświetla czas systemowy routera: datę, godzinę i odpowiadające im przesunięcie strefy czasowej.



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

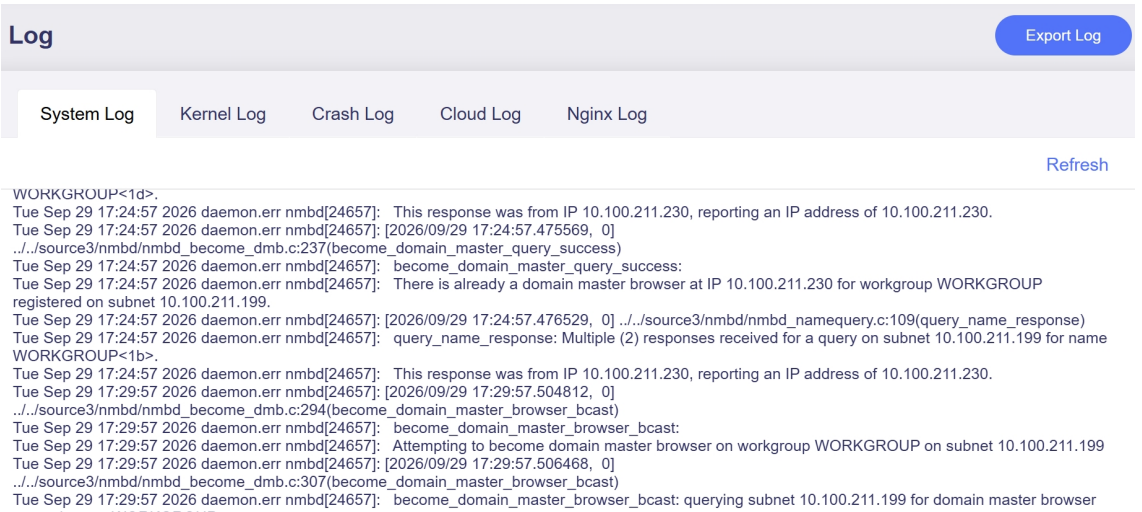


Aby zmienić strefę czasową, wybierz odpowiednią pozycję z listy, tak aby czas systemowy routera odpowiadał czasowi lokalnemu.


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

14.5 Dziennik

Zaloguj się do panelu administracyjnego routera i przejdź do **SYSTEM** > **Log**. Tutaj możesz przeglądać dzienniki System, Kernel, Crash, Cloud i Nginx na potrzeby analizy i rozwiązywania problemów.



- **Refresh**: kliknij ten przycisk, aby odświeżyć dzienniki.
- **Export Log**: kliknij ten przycisk, aby wyeksportować informacje diagnostyczne wraz z dziennikami.

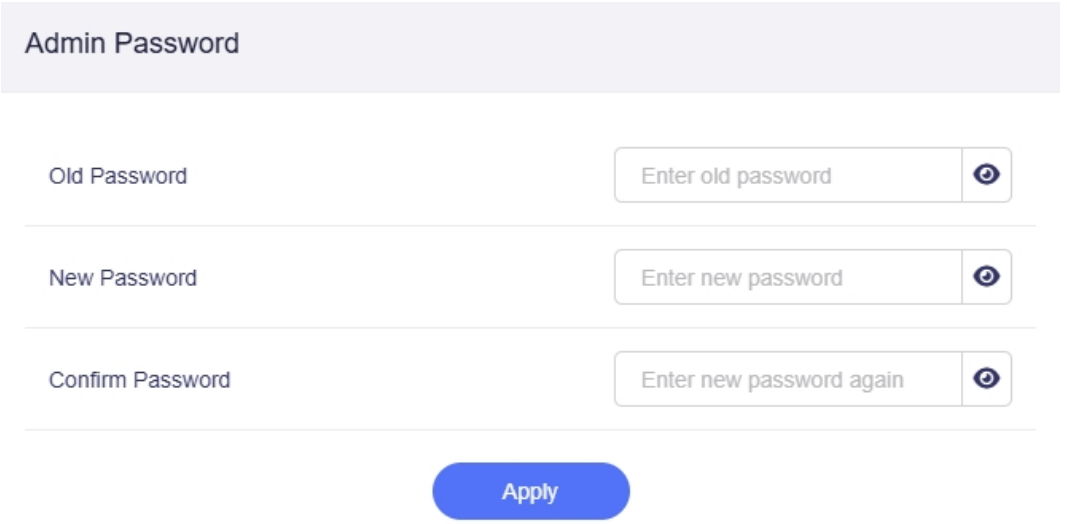
14.6 Bezpieczeństwo

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

- Hasło administratora
- Lokalny dostęp do panelu administracyjnego, LuCI i SSH
- Zdalny dostęp przez HTTPS/SSH
- Otwieranie portów routera

14.6.1 Hasło administratora

W tej sekcji możesz zmienić hasło logowania do panelu administracyjnego.

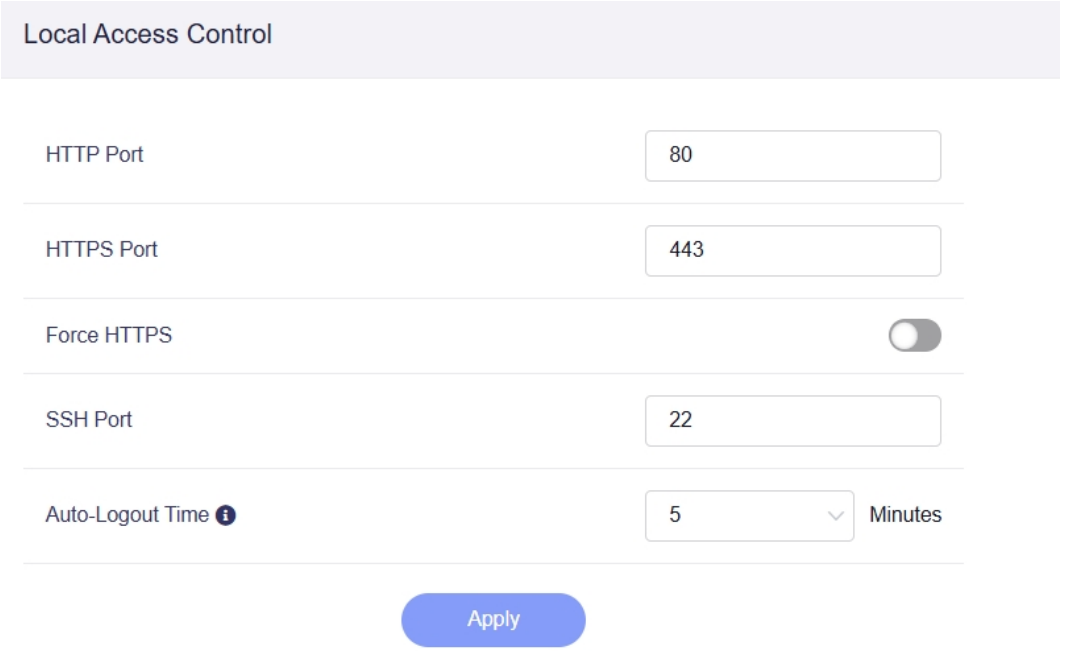


Wymagania dotyczące hasła administratora:

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

14.6.2 Kontrola dostępu lokalnego

Ta sekcja zarządza dostępem do interfejsów routera (panel administracyjny, SSH). Pomaga zapobiegać skanowaniu i próbom włamania na porcie domyślnym oraz problemom sieciowym wynikającym z konfliktów portów.

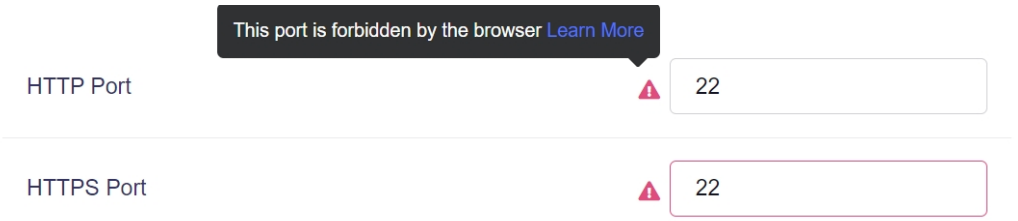


Panel administracyjny

- **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.
- **SSH Port**: domyślnie 22; port dostępu SSH do routera.
- **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.

Uwaga:

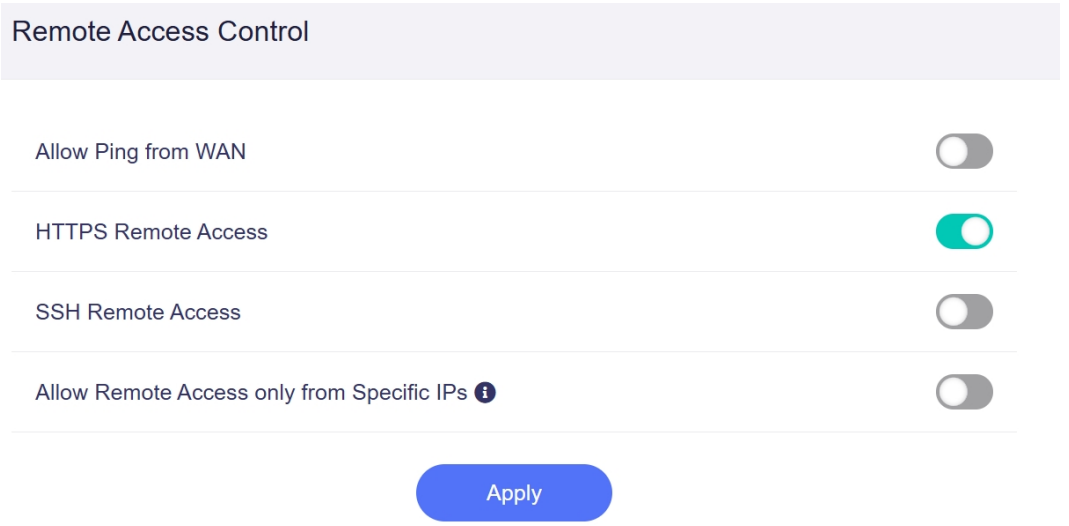
1. Jeśli przypiszesz numer kolidujący z portem zastrzeżonym (lub zarezerwowanym dla określonych usług przez przeglądarki albo konwencje sieciowe), pojawi się komunikat „This port is forbidden by the browser”.



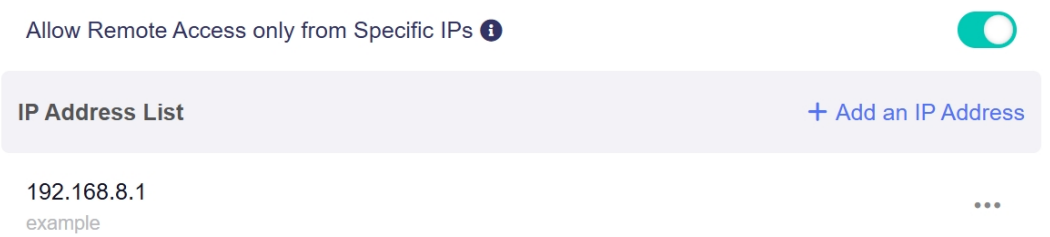
2. Po zmianie numeru portu w oprogramowaniu trzeba podawać prawidłowy numer, aby otworzyć panel administracyjny. Jeśli zapomnisz numeru, zresetuj router, aby przywrócić port domyślny.

14.6.3 Kontrola dostępu zdalnego

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



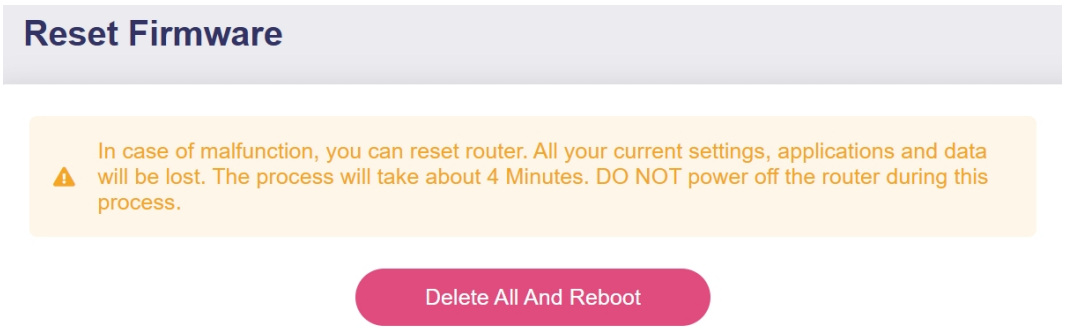
- **Allow Ping from WAN**: zezwolenie na ping od strony WAN pomaga sprawdzić dostępność routera przez WAN w razie problemów z siecią oraz określić opóźnienie i utratę pakietów.
- **HTTPS Remote Access**: umożliwia bezpieczny zdalny dostęp do panelu administracyjnego przez HTTPS. Zapewnia szyfrowaną transmisję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



14.7 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.

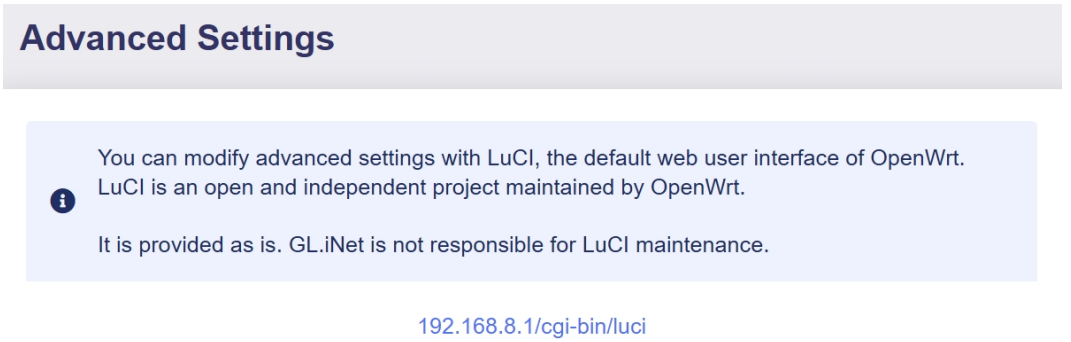
Jeśli panel administracyjny routera jest niedostępny, spróbuj zresetować router za pomocą fizycznego przycisku resetowania z boku urządzenia.

14.8 Ustawienia zaawansowane

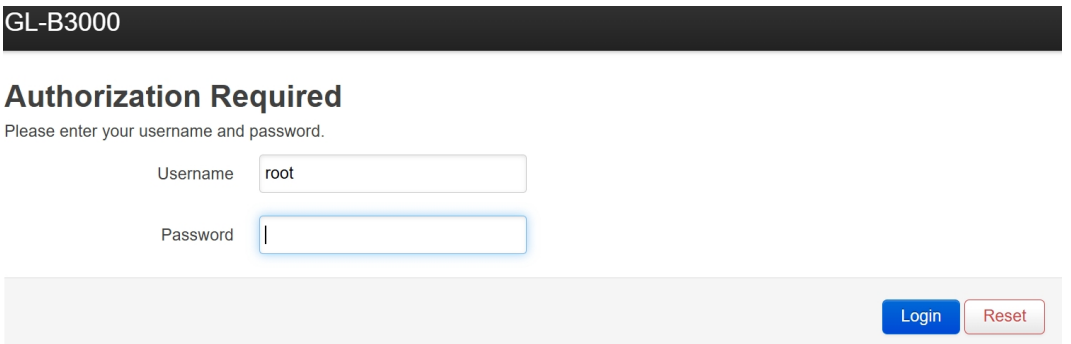
Zaloguj się do panelu administracyjnego routera i przejdź do **SYSTEM** > **Advanced Settings**. Tutaj możesz zmieniać ustawienia zaawansowane w LuCI, domyślnym interfejsie internetowym OpenWrt. LuCI to otwarty, niezależny projekt utrzymywany przez OpenWrt, udostępniany w obecnej postaci. GL.iNet nie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

Aby zalogować się do interfejsu LuCI, wykonaj poniższe czynności.

1. Kliknij łącze dostępu, aby otworzyć stronę logowania LuCI.



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



Otworzy się interfejs LuCI.

