GL·iNet



Instrukcja obsługi

GL-AR300M16 / Shadow

Bezprzewodowy minirouter

Wersja oprogramowania 4.3.27

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 12

1.2 Dane techniczne 12

1.3 Zawartość opakowania 13

Rozdział 2 Podłączanie sprzętu 15

2.1 Wybór miejsca 16

2.2 Podłączanie routera 16

Rozdział 3 Logowanie do routera 17

Rozdział 4 Konfiguracja połączenia z Internetem 20

4.1 Połączenie z Internetem przez kabel Ethernet 22

4.1.1 Podstawowa konfiguracja 22

4.1.2 Protokół 24

4.2 Połączenie z Internetem przez istniejącą sieć Wi-Fi 27

4.2.1 Podstawowa konfiguracja 28

4.2.2 Opcje wzmacniacza sygnału 31

4.3 Połączenie z Internetem przez tethering USB 32

4.3.1 Tethering z iPhone'a 32

4.3.2 Tethering z telefonu z systemem Android 34

4.3.3 Rozwiązywanie problemów 35

4.4 Połączenie z Internetem przez modem USB 36

Rozdział 5 Sieć bezprzewodowa 38

Rozdział 6 Urządzenia klienckie 41

6.1 Szczegóły urządzenia 43

6.2 Działania 45

6.3 Usuwanie urządzeń klienckich 47

6.4 Sortowanie 48

Rozdział 7 Poznaj VPN 49

7.1 Wprowadzenie 50

7.2 Przykłady zastosowań 51

Rozdział 8 Panel VPN 54
8.1 Klient VPN 55
8.1.1 Opcje klienta 56
8.1.2 Tryb reguł 58
8.1.3 Opcje globalne 59
8.2 Serwer VPN 62
8.2.1 Opcje serwera 63
8.2.2 Reguły tras serwera 64
8.2.3 Opcje globalne 66
Rozdział 9 Konfiguracja serwera VPN 67
9.1 Konfiguracja serwera OpenVPN 68
9.1.1 Przygotowanie 68
9.1.2 Etapy konfiguracji 69
9.1.3 Rozwiązywanie problemów 71
9.2 Konfiguracja serwera WireGuard 72
9.2.1 Przygotowanie 72
9.2.2 Etapy konfiguracji 73
9.2.3 Rozwiązywanie problemów 76
Rozdział 10 Konfiguracja klienta VPN 77
10.1 Konfiguracja klienta OpenVPN 78
10.1.1 Przygotowanie 78
10.1.2 Konfiguracja NordVPN 78
10.1.3 Ręczna konfiguracja klienta OpenVPN (inni dostawcy) 84
10.2 Konfiguracja klienta WireGuard 87
10.2.1 Przygotowanie 87
10.2.2 Konfiguracja AzireVPN 88
10.2.3 Konfiguracja Mullvad 91
10.2.4 Ręczna konfiguracja klienta WireGuard (inni dostawcy) 95
Rozdział 11 Aplikacje 99
11.1 Wtyczki 100
11.2 Dynamiczny DNS 101
11.2.1 Włączanie DDNS 101
11.2.2 Sprawdzanie działania DDNS 103
11.2.3 Zdalny dostęp przez HTTP 105

11.2.4 Zdalny dostęp przez HTTPS 106
11.2.5 Zdalny dostęp przez SSH 108
11.3 GoodCloud 109
11.3.1 Włączanie GoodCloud 110
11.3.2 Zarządzanie routerem 114
11.3.3 Usuwanie powiązania urządzenia 120
Rozdział 12 Sieć 121
12.1 Zapora sieciowa 122
12.1.1 Przekierowanie portów 122
12.1.2 Otwieranie portów routera 124
12.1.3 DMZ 125
12.2 Multi-WAN 126
12.2.1 Monitorowanie stanu interfejsów 126
12.2.2 Tryb Multi-WAN 129
12.3 LAN 132
12.3.1 Sieć prywatna 132
12.3.2 Sieć gościnna 134
12.3.3 Rezerwacja adresów 136
12.4 DNS 138
12.4.1 Ustawienia ogólne 138
12.4.2 Ustawienia serwera DNS 139
12.4.3 Edycja pliku hosts 141
12.5 Tryb sieciowy 143
12.6 IPv6 145
12.6.1 Tryb IPv6 145
12.6.2 Sposób uzyskiwania DNS 146
12.7 Adres MAC 147
12.8 Drop-in Gateway 149
12.9 IGMP Snooping 151
Rozdział 13 System 152
13.1 Przegląd 153
13.2 Aktualizacja 154
13.2.1 Aktualizacja online 154
13.2.2 Aktualizacja lokalna 155

13.3 Zadania zaplanowane 156
13.3.1 Harmonogram diody LED 156
13.3.2 Harmonogram ponownego uruchamiania 157
13.3.3 Harmonogram Wi-Fi 2,4 GHz 158
13.4 Hasło administratora 160
13.5 Strefa czasowa 161
13.6 Ustawienia przełącznika 162
13.7 Dziennik 163
13.8 Resetowanie oprogramowania 164
13.9 Ustawienia zaawansowane 165

Rozdział 1

Poznaj swój router

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

1.1 Opis produktu

Shadow (GL-AR300M16) to kieszonkowy minirouter zaprojektowany z myślą o przenoszeniu i podróżach, obsługujący bezprzewodową transmisję danych do 300 Mb/s. Oferuje zaawansowane zabezpieczenia, w tym obsługę OpenVPN, WireGuard® i serwera DNS. Pozwala przekształcić sieć publiczną w prywatną sieć Wi-Fi do bezpiecznego przeglądania Internetu. Umożliwia także przesyłanie plików konfiguracyjnych od ponad 30 dostawców VPN i pracę jako klient VPN, zapewniając dodatkową ochronę prywatności i bezpieczeństwa przez szyfrowanie ruchu między urządzeniem a serwerem VPN.

1.1.1 Wygląd

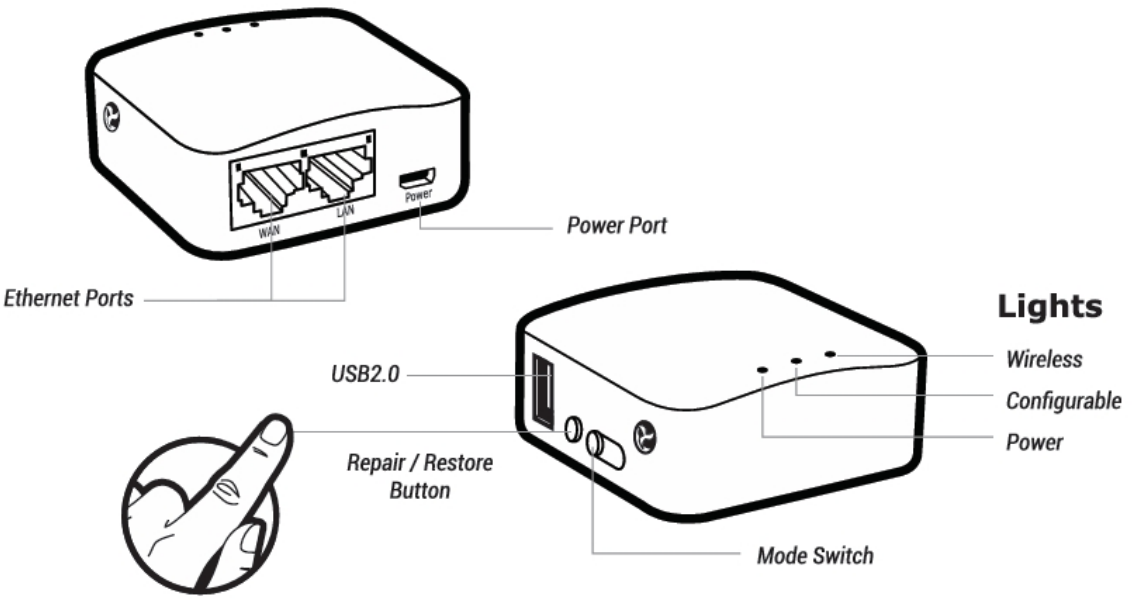








1.1.2 Złącza i przyciski



Element	Opis
Złącze zasilania	Służy do podłączenia zasilacza.
Port Ethernet WAN	Służy do połączenia z modemem lub gniazdem Ethernet zapewniającym dostęp do Internetu.
Port Ethernet LAN	W razie potrzeby służy do podłączenia urządzeń przewodowych.
USB 2.0	Do podłączania nośników USB, udostępniania Internetu przez USB z telefonu oraz zgodnych modemów komórkowych USB.
Przełącznik trybu	Fizyczny przełącznik umożliwiający zmianę wybranych ustawień routera jednym ruchem. W panelu administracyjnym można go skonfigurować, aby jednym ruchem włączać lub wyłączać określone funkcje.

Przycisk naprawy / przywracania	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

Wskaźnik LED	Znaczenie
Dioda zasilania	Świeci: zasilanie włączone Nie świeci: zasilanie wyłączone
Środkowa dioda LED (konfigurowalna)	Świeci: dioda została skonfigurowana Nie świeci: dioda nie została skonfigurowana (tryb domyślny)
Dioda sieci bezprzewodowej	Świeci: Wi-Fi 2,4 GHz jest połączone Nie świeci: Wi-Fi 2,4 GHz jest rozłączone

1.2 Dane techniczne

Złącza	1 × port Ethernet WAN 1 × port Ethernet LAN 3 × dioda LED 1 × port USB 2.0 1 × złącze zasilania micro-USB 1 × przycisk resetowania 1 × przełącznik
Procesor	QCA9531, SoC 650 MHz
Pamięć RAM / pamięć masowa	DDR2 128 MB / NOR Flash 16 MB
Protokół	IEEE 802.11/b/g/n
Prędkość Wi-Fi	300 Mb/s (2,4 GHz)
Prędkość Ethernet	10/100 Mb/s
Zasilanie	Micro-USB, 5 V / 2 A
Diody LED	Zasilanie / Wi-Fi
Pobór mocy	< 2W
Temperatura pracy	0 ~ 40°C (32 ~ 104°F)

Temperatura przechowywania	-20 ~ 70°C (-4 ~ 158°F)
Wymiary / masa	58 × 58 × 25 mm / 40 g
Inne materiały i narzędzia	Karta katalogowa / Oprogramowanie / Aplikacja

*Rzeczywista prędkość i zasięg sieci bezprzewodowej mogą się różnić w zależności od przeszkód w otoczeniu, obciążenia sieci i możliwości urządzeń klienckich.

1.3 Zawartość opakowania

Zasilacz dołączony do opakowania zależy od kraju dostawy.

Opakowanie zawiera:

- 1 × Shadow (GL-AR300M16)
- 1 × instrukcja obsługi
- 1 × karta z podziękowaniem
- 1 × kabel Ethernet
- 1 × kabel USB



1 x User manual


1 x Shadow (GL-AR300M16)



1 x Thank you card


1 x Ethernet cable


1 x USB cable

(GL-AR300M16-Ext)



1 x User manual



1 x Shadow (GL-AR300M16)



1 x Thank you card



1 x Ethernet cable



1 x USB cable

(GL-AR300M16)

Rozdział 2

Podłączanie sprzętu

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

2.1 Wybór miejsca

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

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

2.2 Podłączanie routera

1. **Włącz zasilanie**

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

2. **Podłącz urządzenie do routera**

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

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

3. **Zaloguj się do routera**

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

Rozdział 3

Logowanie do routera

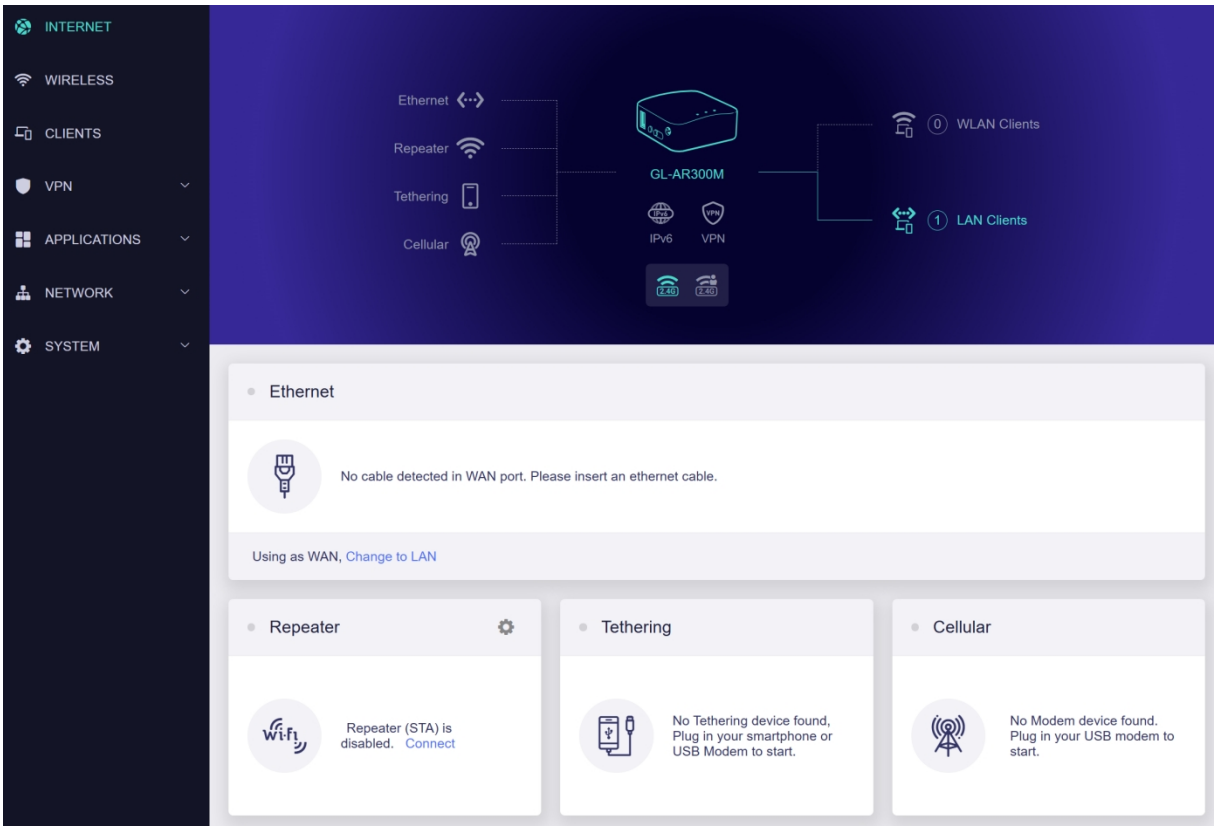
W tym rozdziale opisano logowanie do routera przez panel administracyjny w przeglądarce.

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

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

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

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


INTERNET
WIRELESS
CLIENTS
VPN
APPLICATIONS
NETWORK
SYSTEM
Ethernet
Repeater
Tethering
Cellular
GL-AR300M
IPv6
VPN
0 WLAN Clients
1 LAN Clients
Ethernet
No cable detected in WAN port. Please insert an ethernet cable.
Using as WAN, Change to LAN
Repeater
Repeater (STA) is disabled. Connect
Tethering
No Tethering device found, Plug in your smartphone or USB Modem to start.
Cellular
No Modem device found. Plug in your USB modem to start.

Rozdział 4

Konfiguracja połączenia z Internetem

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

Shadow obsługuje cztery sposoby łączenia z Internetem: Ethernet, wzmacniacz sygnału, tethering USB i modem USB. Wybierz sposób odpowiedni do swoich potrzeb.

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

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

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

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

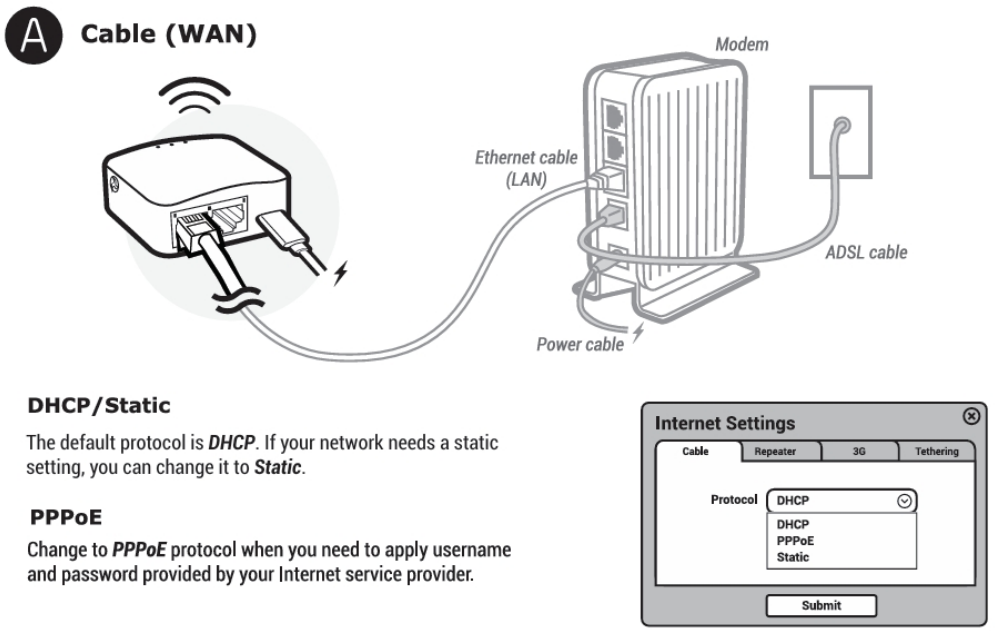
4.1 Połączenie z Internetem przez kabel Ethernet

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.

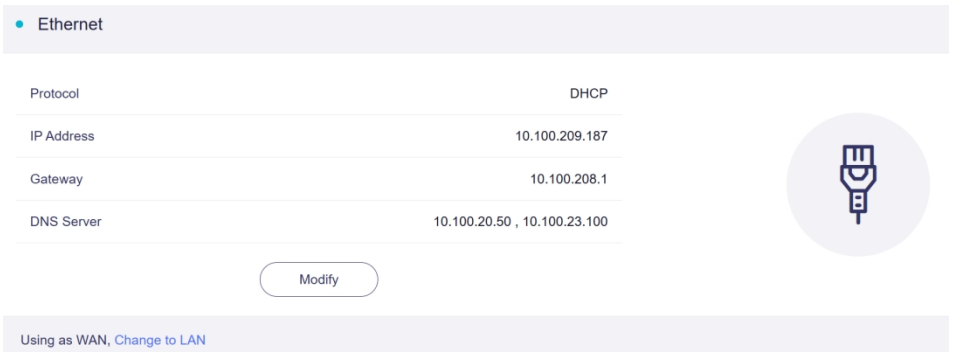
4.1.1 Podstawowa konfiguracja

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.

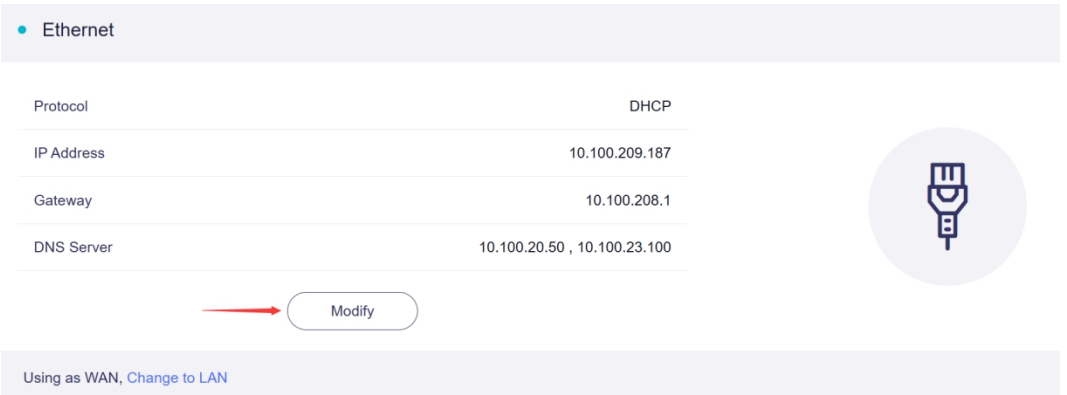


2. Zaloguj się do panelu administracyjnego routera i przejdź do **INTERNET** > **Ethernet**. Po pomyślnym nawiązaniu połączenia w sekcji Ethernet pojawią się szczegóły sieci, w tym protokół, adres IP, brama i serwer DNS.


Ethernet
Protocol
DHCP
IP Address
10.100.209.187
Gateway
10.100.208.1
DNS Server
10.100.20.50 , 10.100.23.100
Modify
Using as WAN, Change to LAN

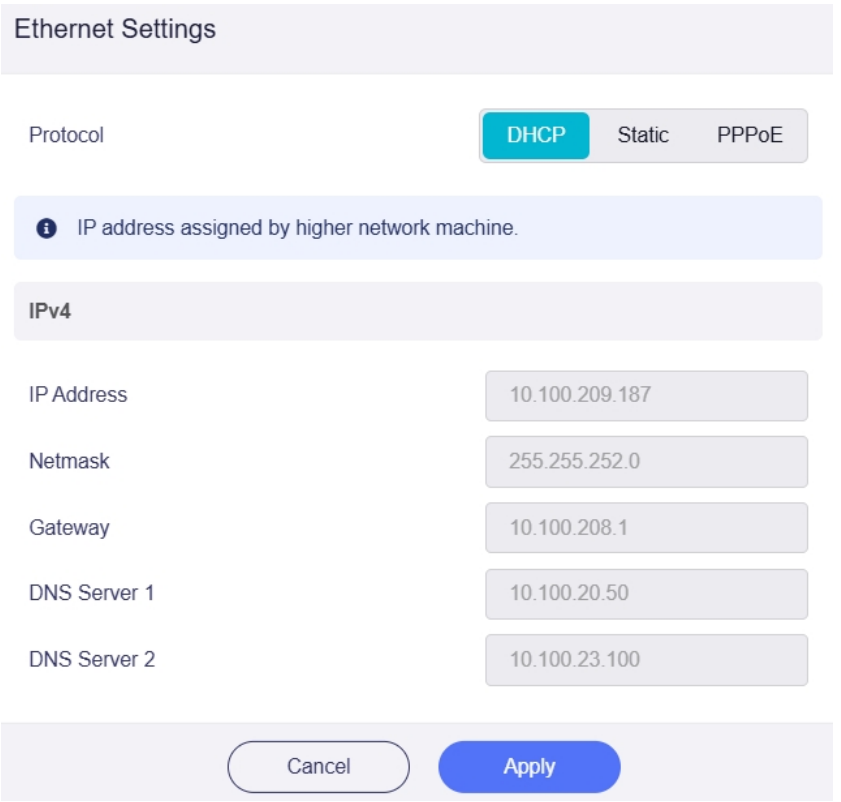
4.1.2 Protokół

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



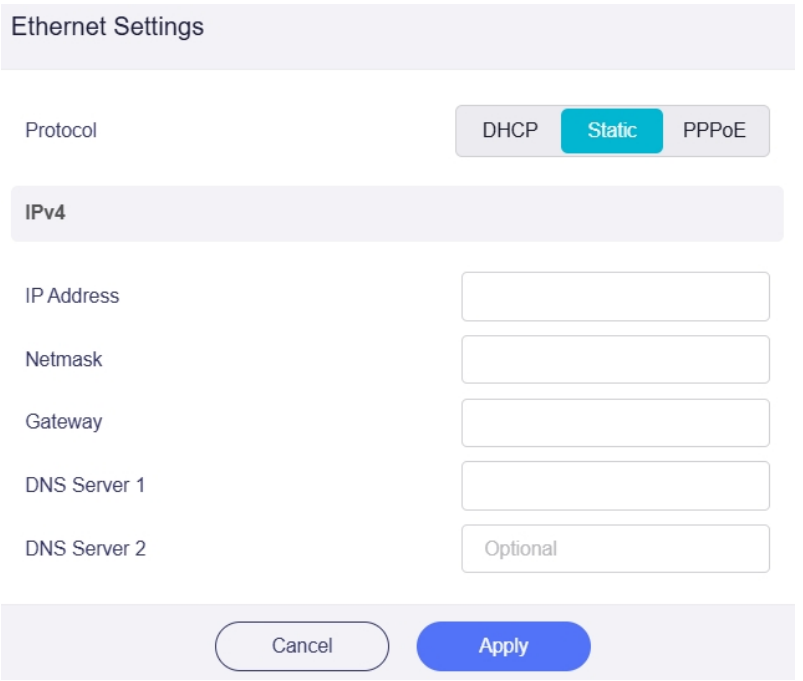
- **DHCP**

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



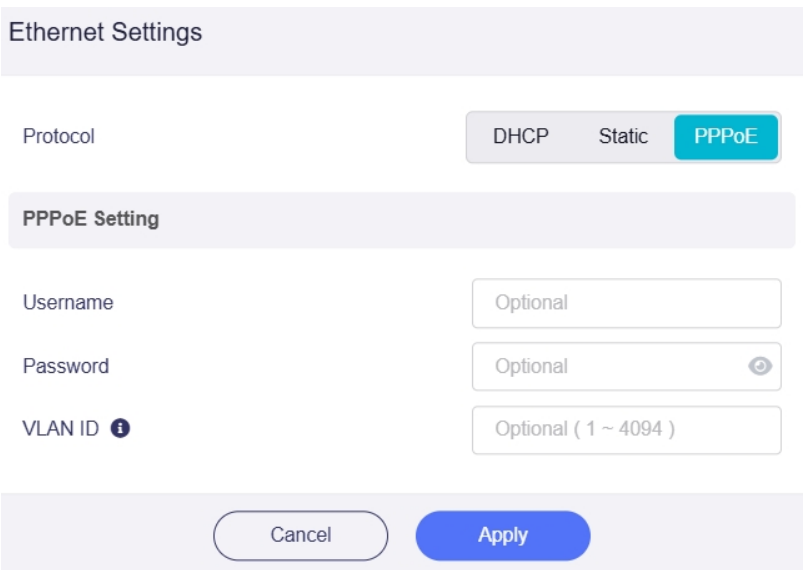
- **Statyczny adres IP**

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



- **PPPoE**

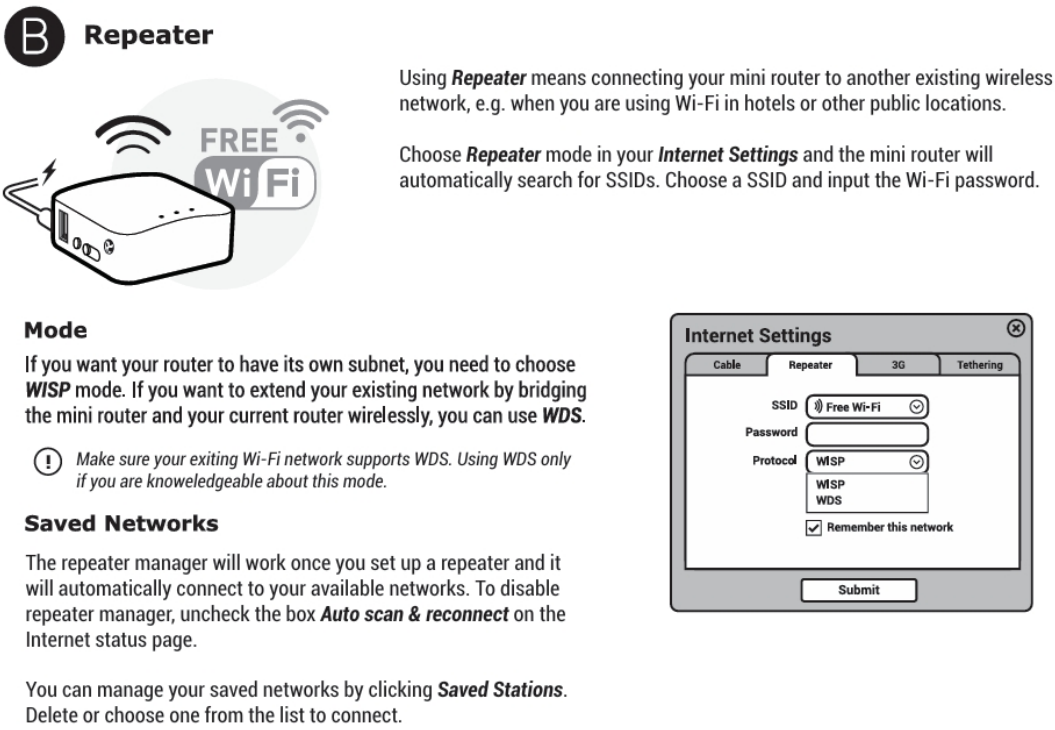
  PPPoE (Point-to-Point Protocol over Ethernet) to protokół sieciowy powszechnie stosowany przez dostawców Internetu. Dostawca zazwyczaj udostępnia modem oraz indywidualną nazwę użytkownika i hasło wymagane do skonfigurowania połączenia z Internetem.



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

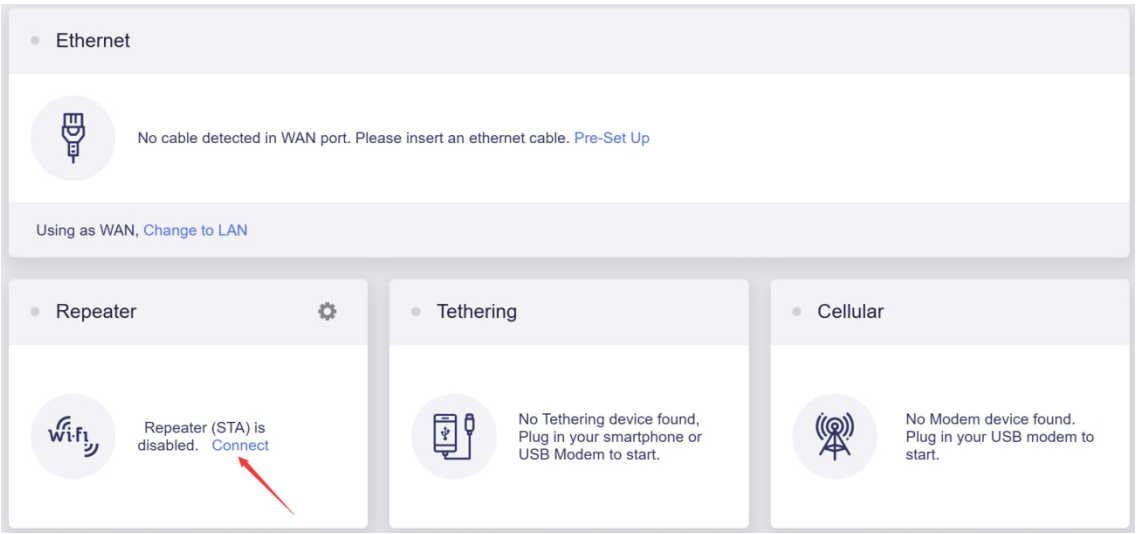
Podłącz router jako wzmacniacz do istniejącej sieci bezprzewodowej, aby wzmocnić sygnał Wi-Fi i utworzyć sieć lokalną odizolowaną od sieci głównej. W hotelach i kawiarniach oferujących bezpłatne publiczne hotspoty wzmacniacz zwiększa zasięg Wi-Fi, zapewnia przewodowy i bezprzewodowy dostęp wielu urządzeniom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



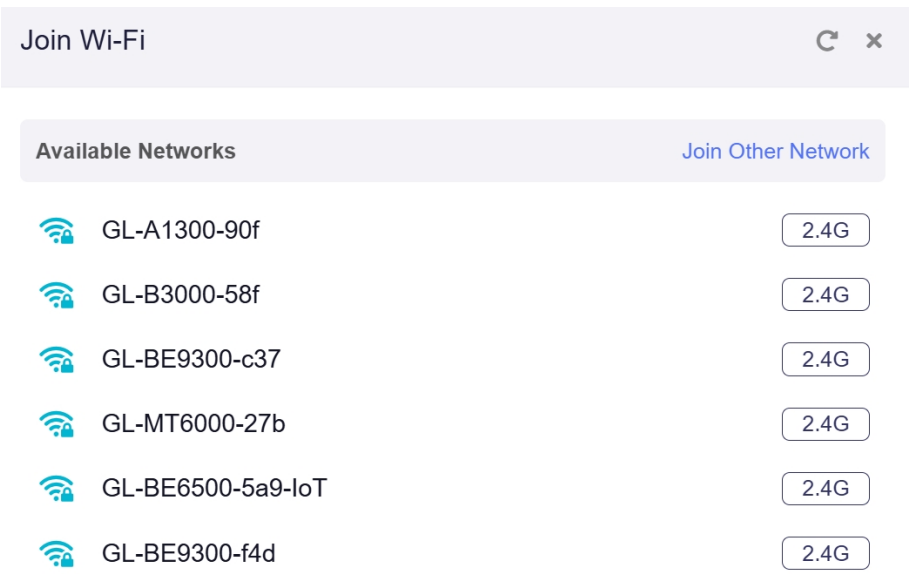
Funkcja wzmacniacza GL.iNet domyślnie działa w trybie WISP (Wireless Internet Service Provider). Oznacza to, że router tworzy własną podsieć i działa jako zapora, chroniąc przed zagrożeniami z sieci publicznej.

4.2.1 Podstawowa konfiguracja

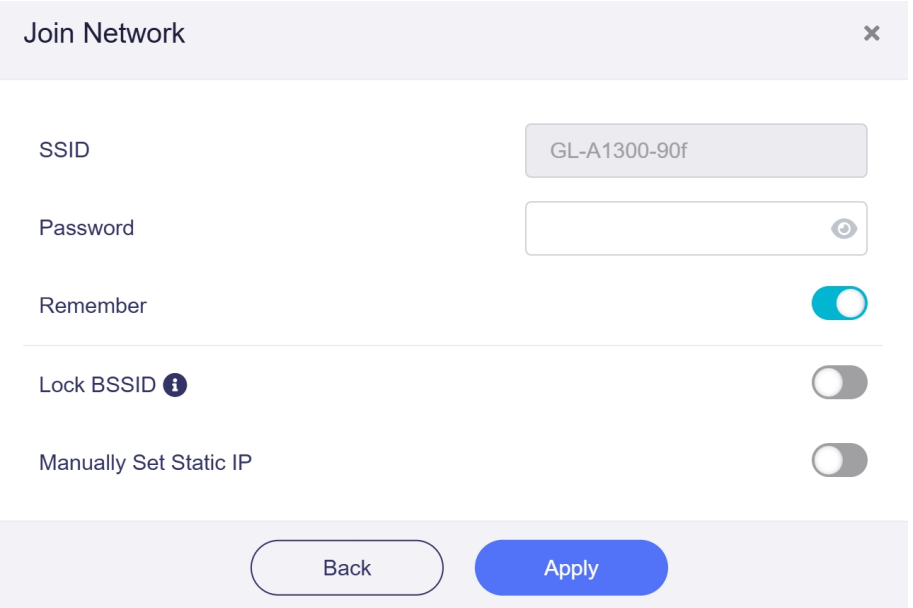
1. Zaloguj się do panelu administracyjnego routera i przejdź do **INTERNET** > **Repeater**. Kliknij **Connect**.



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

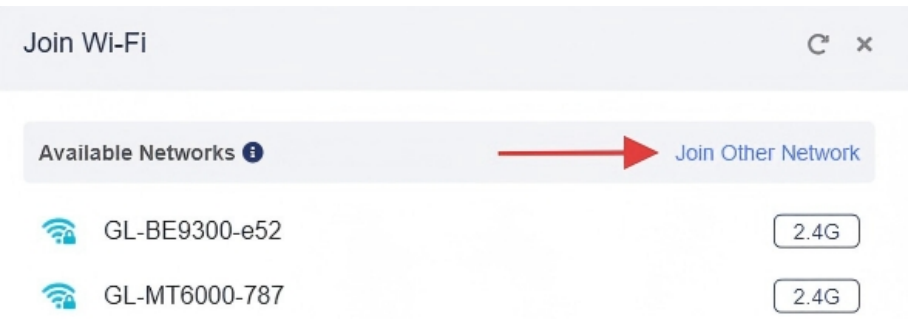


3. Wprowadź prawidłowe hasło Wi-Fi i kliknij **Apply**.

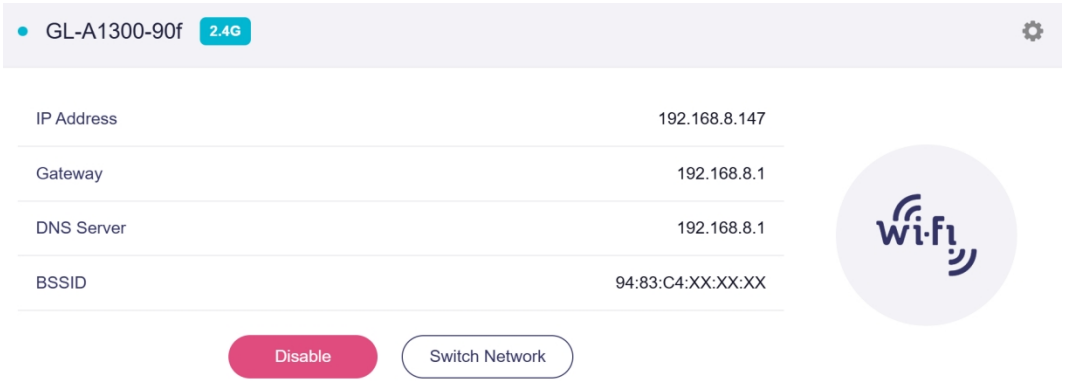


- **Remember**: włącz tę opcję, aby zapamiętać bieżącą sieć Wi-Fi, której sygnał jest wzmacniany.
- **Lock BSSID**: po włączeniu router będzie łączyć się wyłącznie z konkretnym punktem dostępu (AP) odpowiadającym wybranemu BSSID, nawet jeśli inne punkty dostępu mają taki sam identyfikator SSID.
- **Manually 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**.

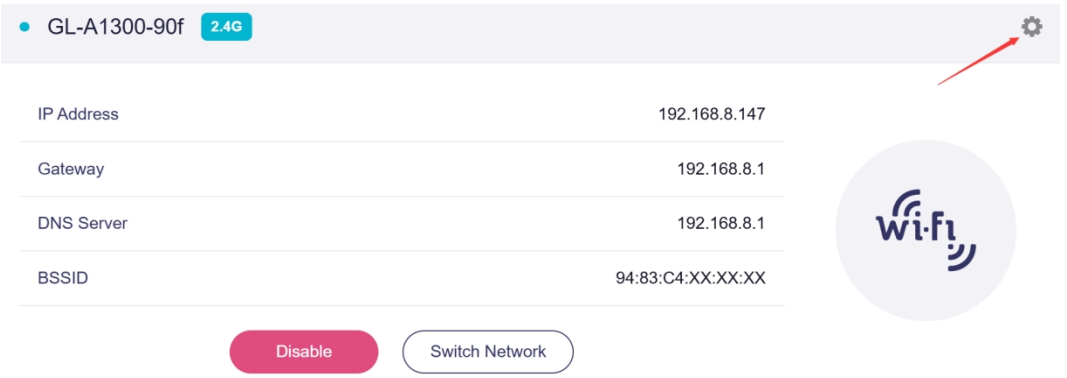


5. Poczekaj chwilę na połączenie routera. Po połączeniu strona będzie wyglądać jak poniżej.

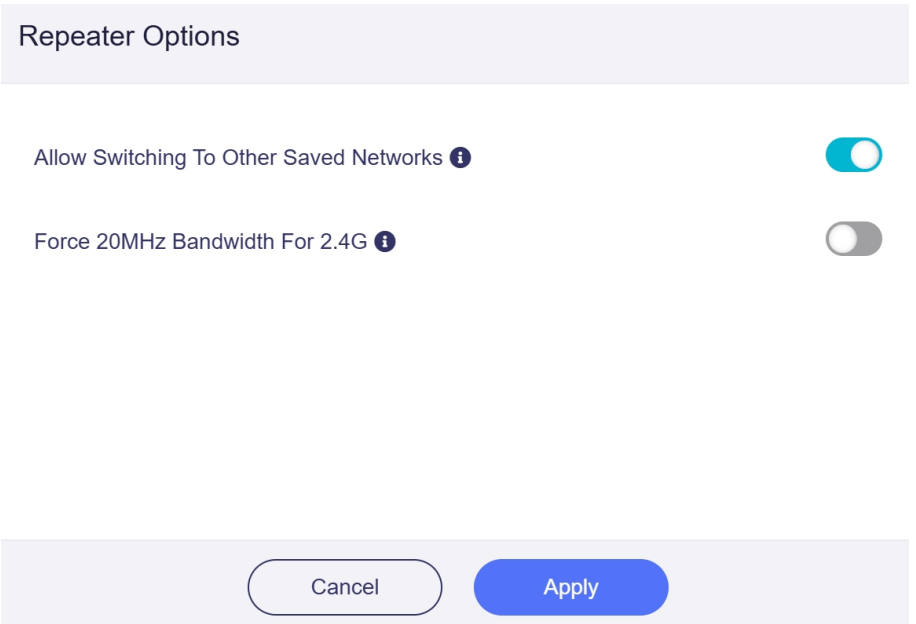

GL-A1300-90f
2.4G
IP Address
192.168.8.147
Gateway
192.168.8.1
DNS Server
192.168.8.1
BSSID
94:83:C4:XX:XX:XX
Disable
Switch Network

4.2.2 Opcje wzmacniacza sygnału

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



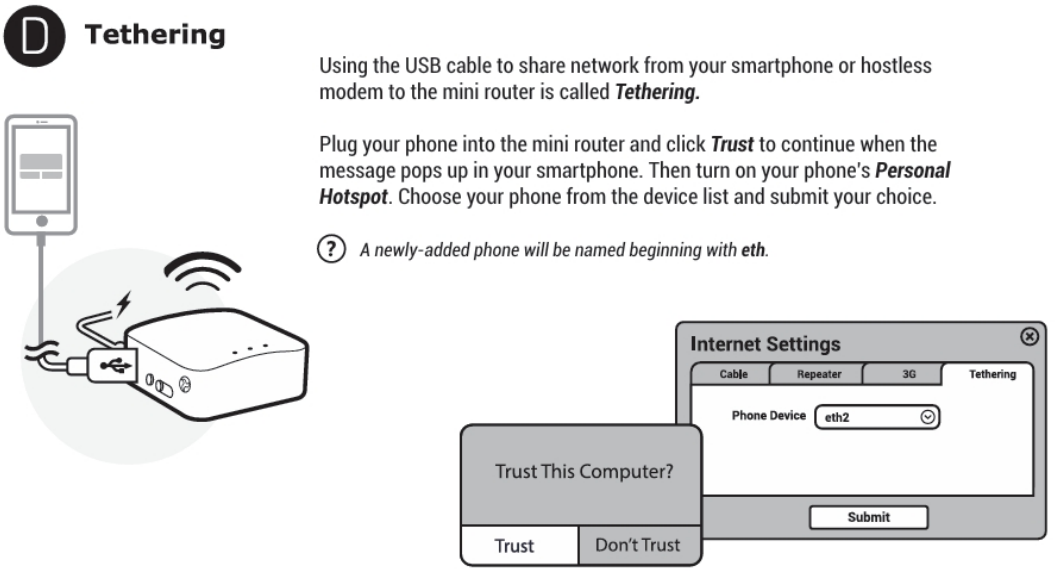
Wygląd strony może się różnić w zależności od wersji oprogramowania.



- **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.
- **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.

4.3 Połączenie z Internetem przez tethering USB

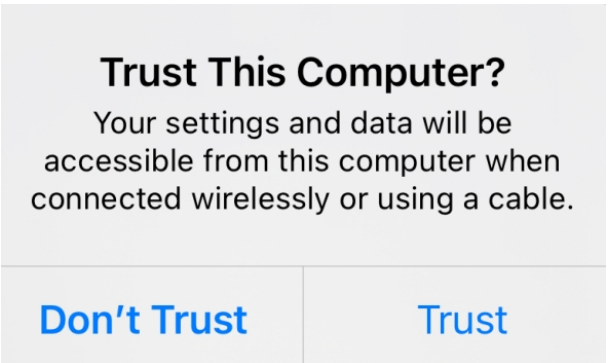
Podłączenie smartfona do routera kablem USB w celu udostępnienia routerowi komórkowej transmisji danych (np. 4G/5G) nazywa się tetheringiem. To wygodny sposób uzyskania tymczasowego dostępu do Internetu, szczególnie w terenie lub w miejscach bez stałego łącza szerokopasmowego.



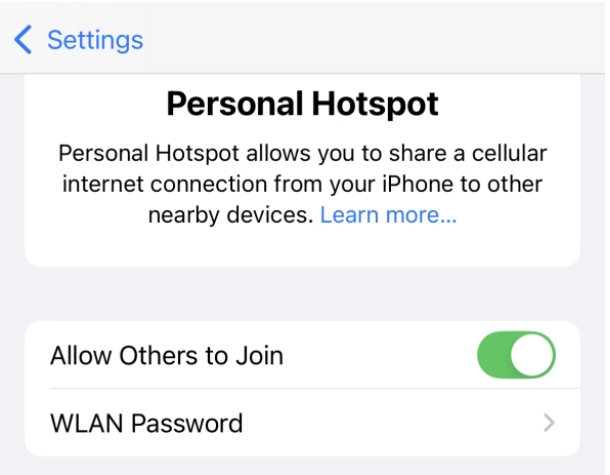
Modem typu hostless również korzysta z interfejsu Tethering podczas konfiguracji modemu.
Uwaga: niektórzy operatorzy komórkowi ograniczają tethering lub pobierają za niego dodatkowe opłaty. Zalecamy sprawdzenie warunków u operatora.

4.3.1 Tethering z iPhone'a

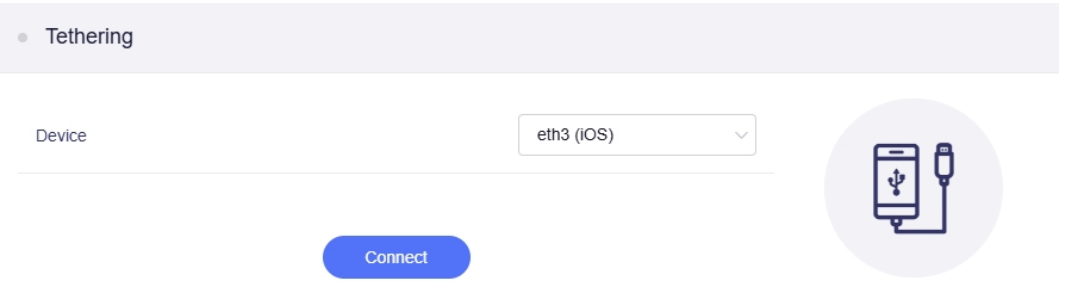
1. Podłącz iPhone'a do portu USB routera za pomocą kabla USB. Pojawi się komunikat systemowy z pytaniem, czy zaufać urządzeniu. Stuknij **Trust**, aby kontynuować.



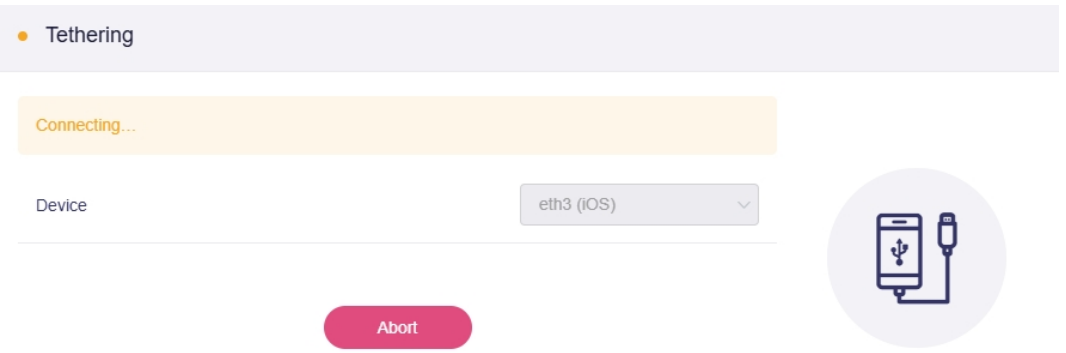
2. Na iPhonie przejdź do **Settings** > **Personal Hotspot**. Włącz **Allow Others to Join**.



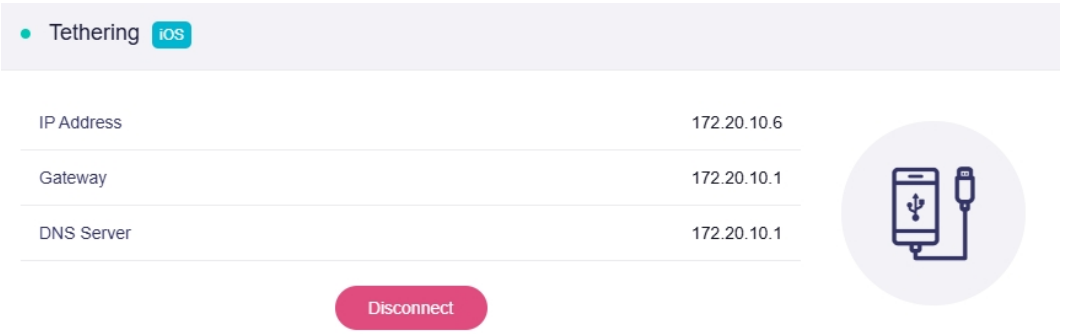
3. Podłącz komputer lub inny telefon do routera. Zaloguj się do panelu administracyjnego routera i przejdź do **INTERNET** > **Tethering**, a następnie kliknij **Connect**.



4. Rozpocznie się nawiązywanie połączenia.

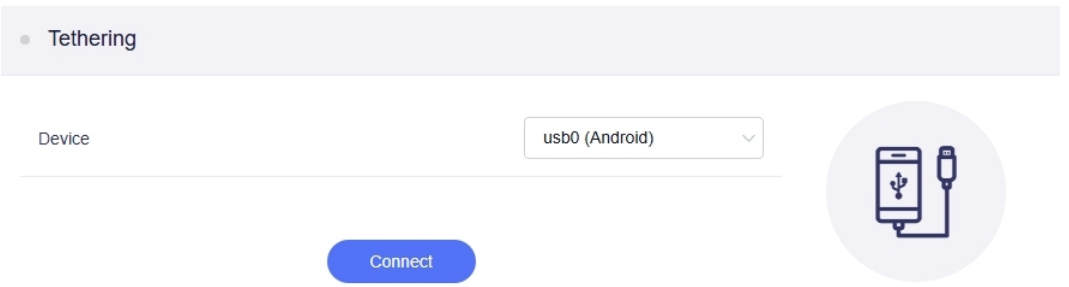


Po połączeniu na tej stronie pojawią się szczegóły połączenia tethering.

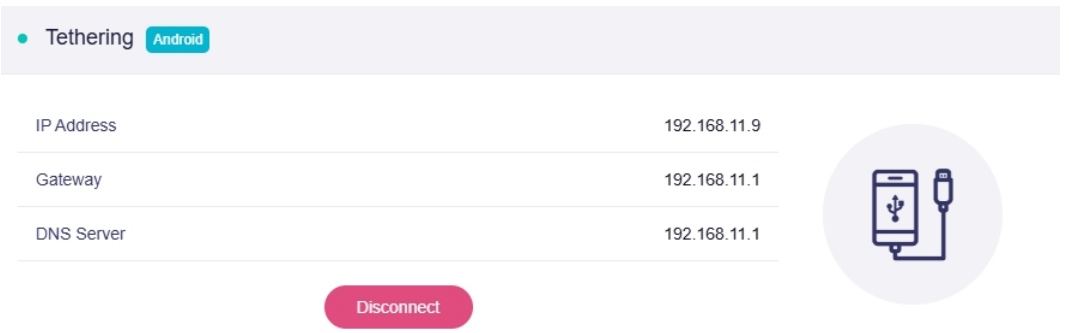


4.3.2 Tethering z telefonu z systemem Android

1. Podłącz telefon z systemem Android do portu USB routera za pomocą kabla USB. Może pojawić się okno systemowe z pytaniem o preferencje USB. Jeśli zostanie wyświetlone, wybierz **USB Tethering** lub **File Transfer**.
2. W telefonie przejdź do **Settings** > **Network & Internet** > **Personal Hotspot**. Włącz **Personal Hotspot** lub **USB Tethering**.
   (Sposób włączania tetheringu USB zależy od producenta. Dokładną lokalizację opcji sprawdź w ustawieniach urządzenia, a w razie potrzeby skontaktuj się z pomocą techniczną producenta.)
3. Podłącz komputer lub inny telefon do routera, a następnie zaloguj się do panelu administracyjnego routera i przejdź do **INTERNET** > **Tethering**. Kliknij **Connect**.



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



4.3.3 Rozwiązywanie problemów

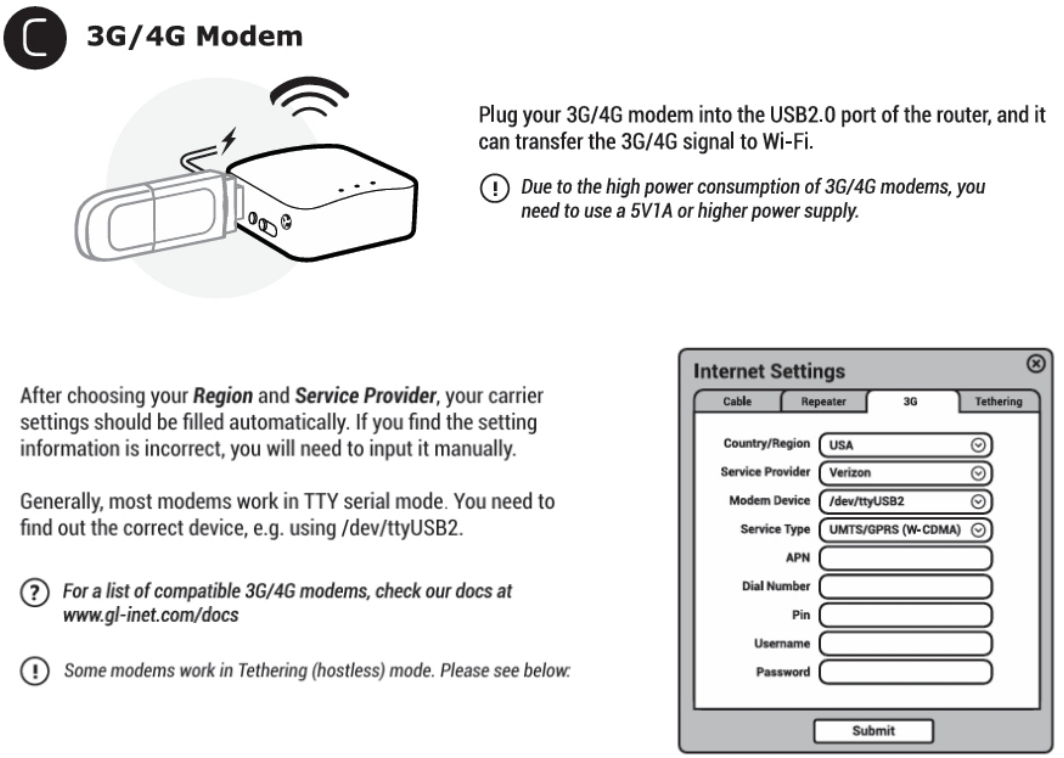
Jeśli nie uda się nawiązać połączenia tethering, wykonaj poniższe czynności:

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

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

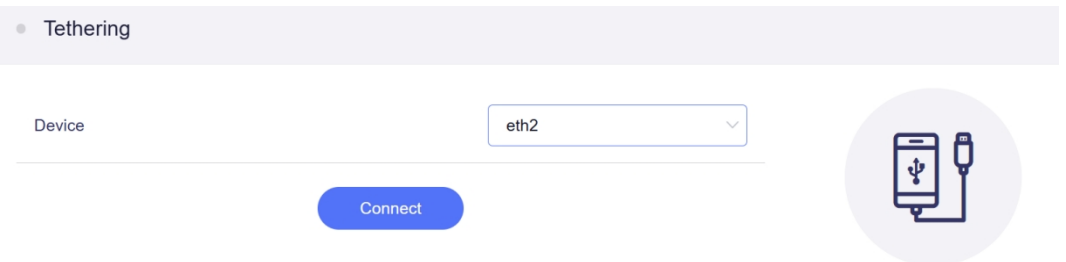
4.4 Połączenie z Internetem przez modem USB

Aby połączyć router z Internetem, podłącz komórkowy modem USB do jego portu USB. Umożliwia to korzystanie z Internetu przez sieci 3G/4G bez stałego łącza szerokopasmowego. Rozwiązanie sprawdza się w pojazdach lub podczas aktywności w terenie. Połączenie jest realizowane za pośrednictwem interfejsu Tethering lub Cellular routera.

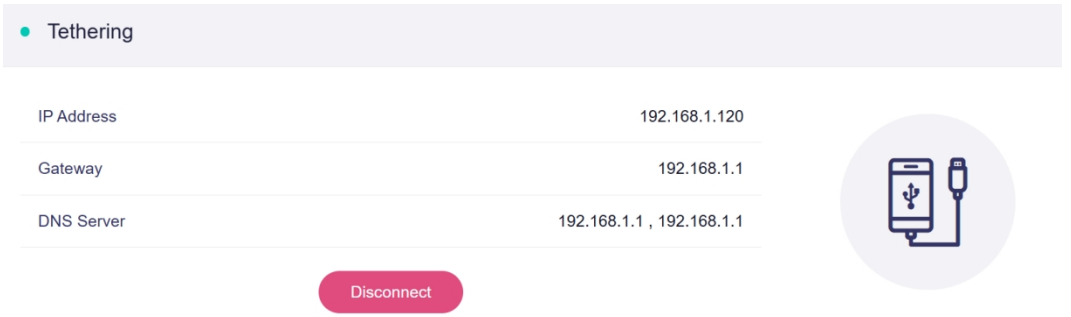


Aby połączyć router z Internetem przez modem USB, wykonaj poniższe czynności.

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



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



Wskazówka: po wstępnej konfiguracji, jeśli uruchomisz ponownie router z podłączonym modemem USB lub ponownie włożysz modem do routera, modem zostanie automatycznie rozpoznany i połączenie sieciowe zostanie nawiązane bez ponownego klikania „Connect”.

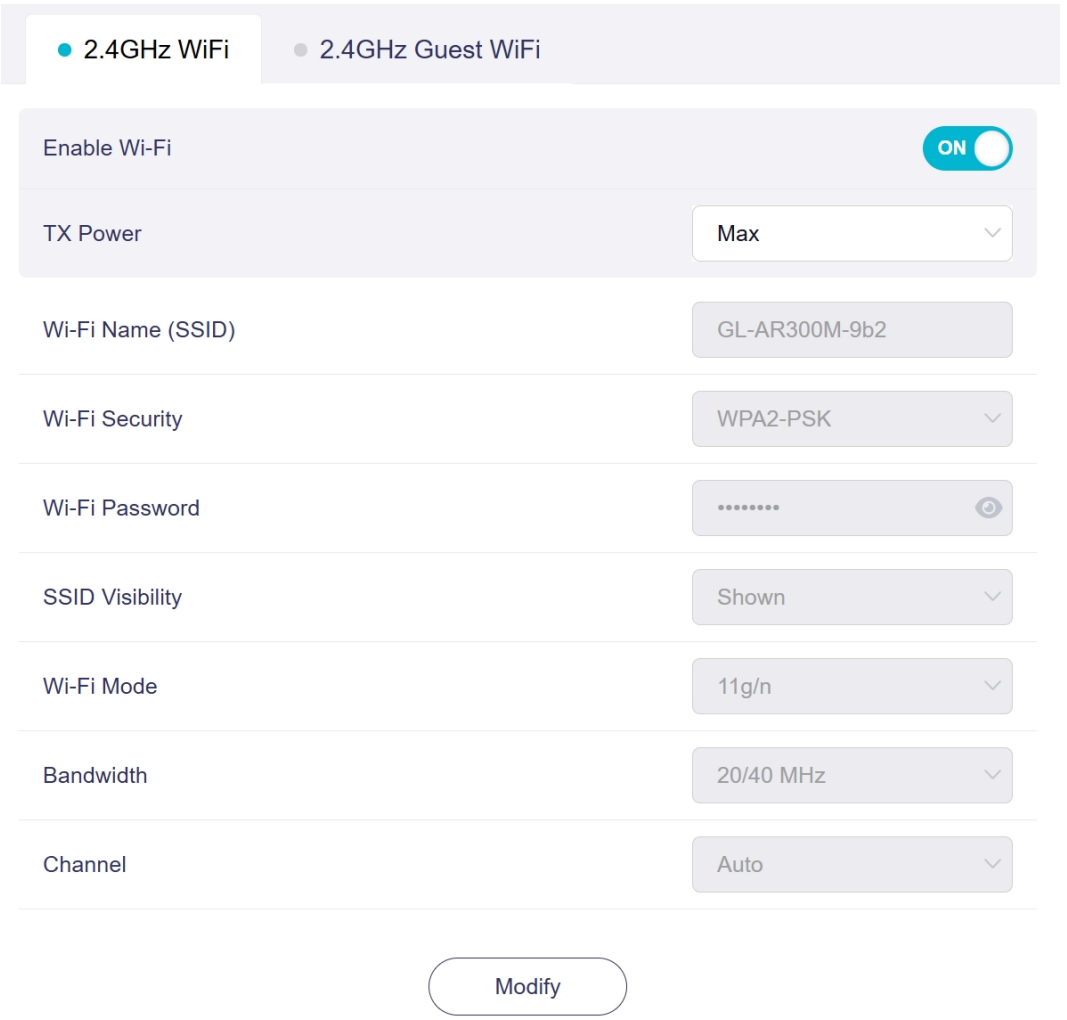
Rozdział 5

Sieć bezprzewodowa

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

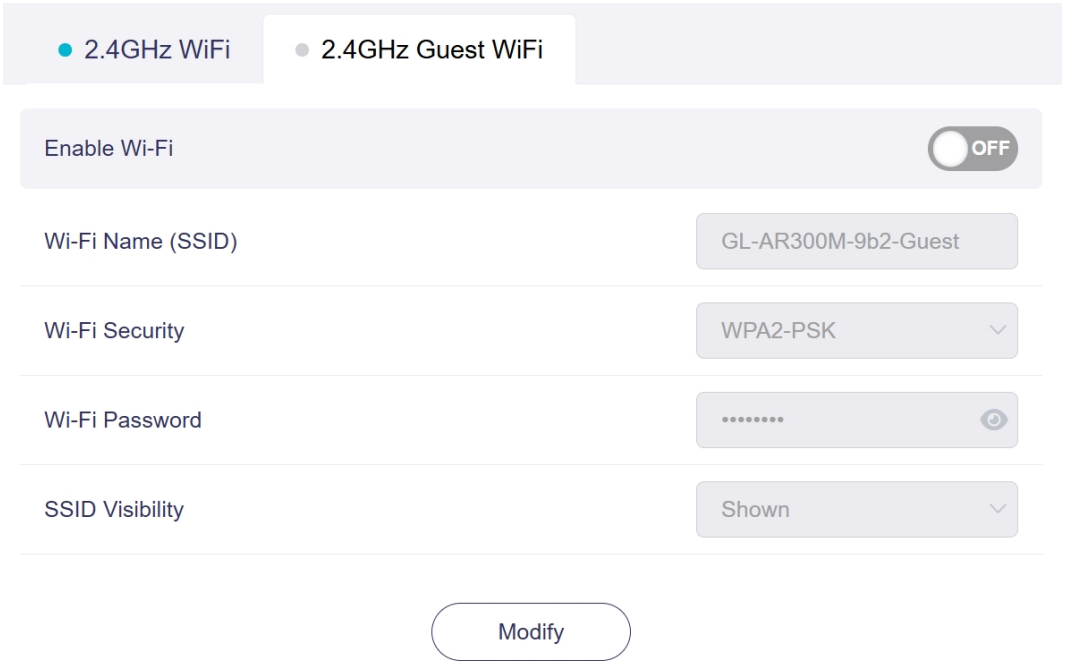
Zaloguj się do panelu administracyjnego routera i przejdź do **WIRELESS**.
Strona sieci bezprzewodowej wyświetla ustawienia Wi-Fi routera w paśmie 2,4 GHz, podzielone na sieć główną i gościnną, co zapewnia elastyczne zarządzanie.

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-AR300M-9b2-Guest
Wi-Fi Security
WPA2-PSK
Wi-Fi Password
••••••••
SSID Visibility
Shown
Modify

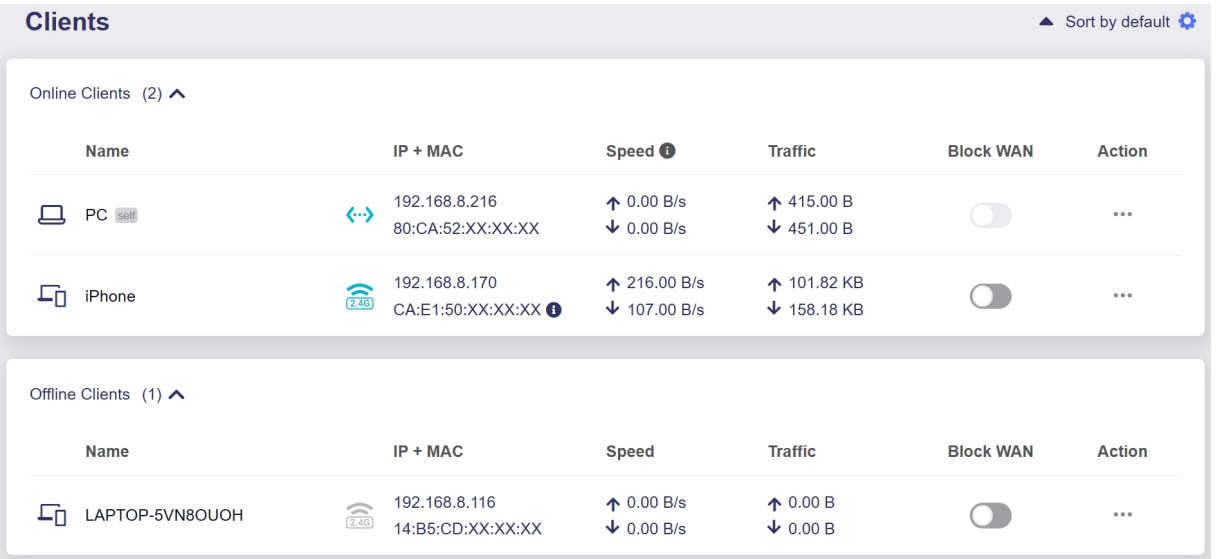
Rozdział 6

Urządzenia klienckie

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

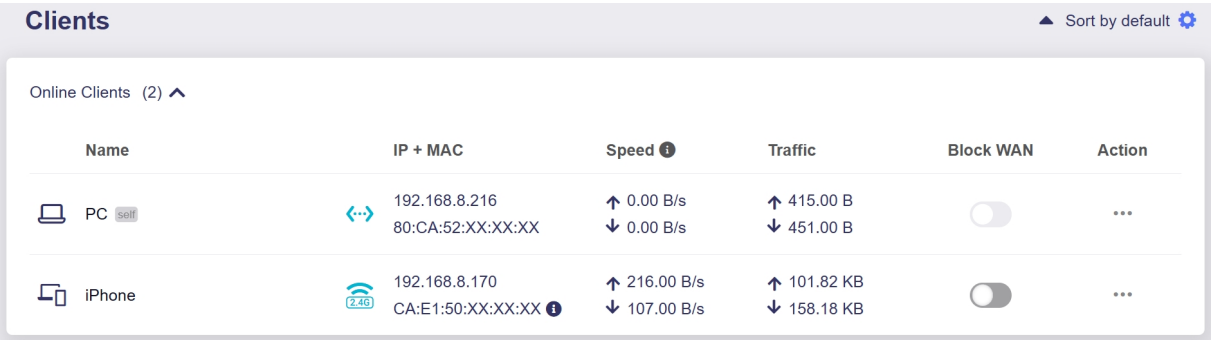
Zaloguj się do panelu administracyjnego routera i przejdź do **CLIENTS**.

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**

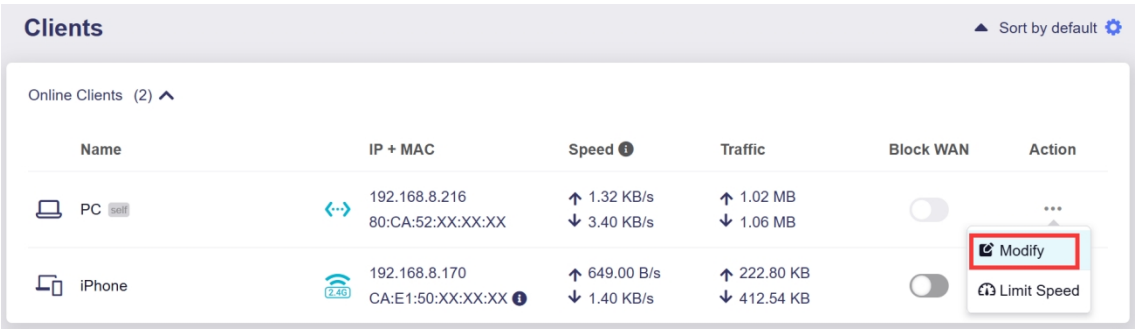
   W piątej kolumnie możesz jednym kliknięciem zablokować wybrane podłączone urządzenie. Po włączeniu blokady urządzenia o adresach MAC znajdujących się na liście blokowanych nie mogą łączyć się z routerem. Blokowanie klienta opiera się na adresie

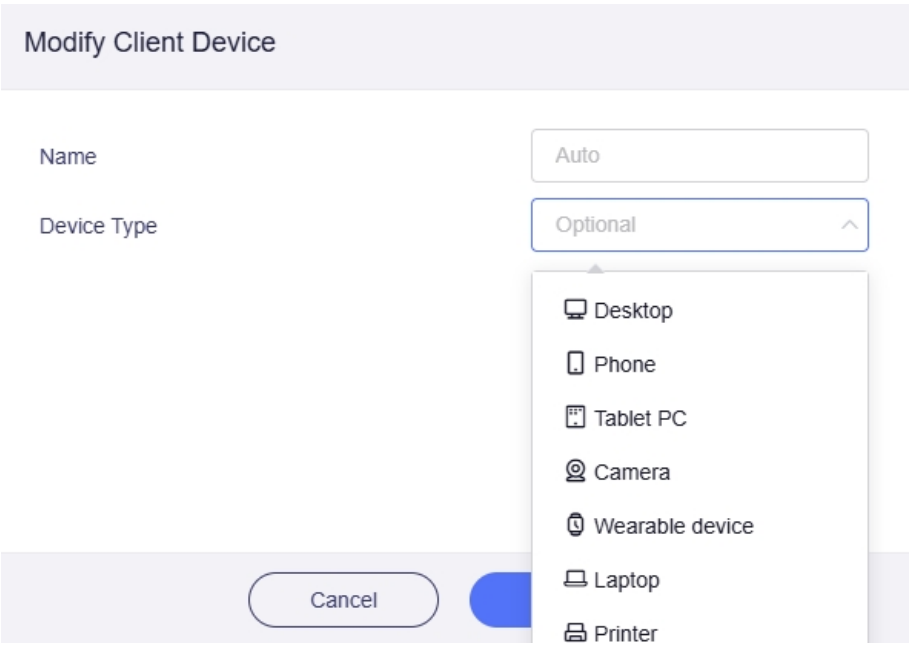
MAC urządzenia. Jeśli zablokowane urządzenie następnym razem użyje innego adresu MAC, nadal będzie mogło połączyć się z routerem.

6.2 Działania

1. **Modyfikowanie**

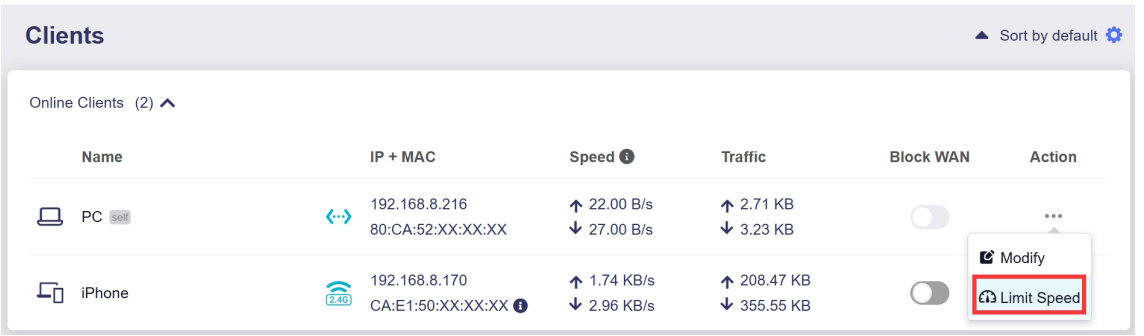
   Kliknij ikonę trzech kropek w kolumnie **Action**, a następnie wybierz **Modify** z menu, aby zmienić nazwę i typ urządzenia.



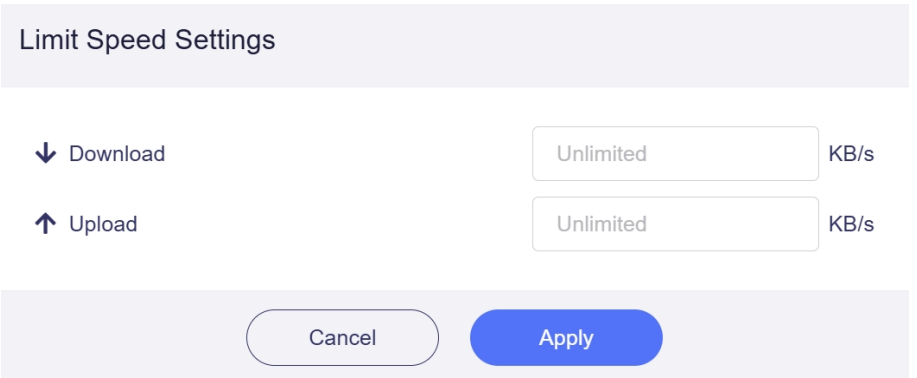


2. **Ograniczanie prędkości**

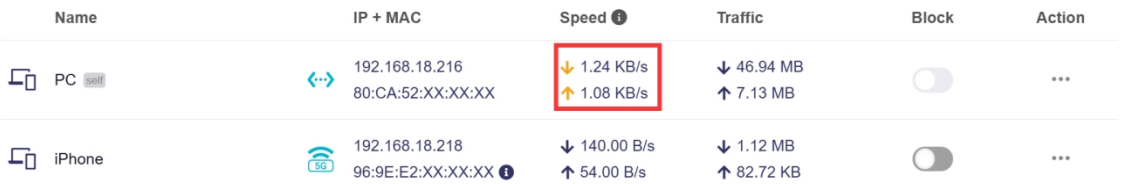
Kliknij ikonę trzech kropek w kolumnie **Action**, a następnie wybierz **Limit Speed** z menu.



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

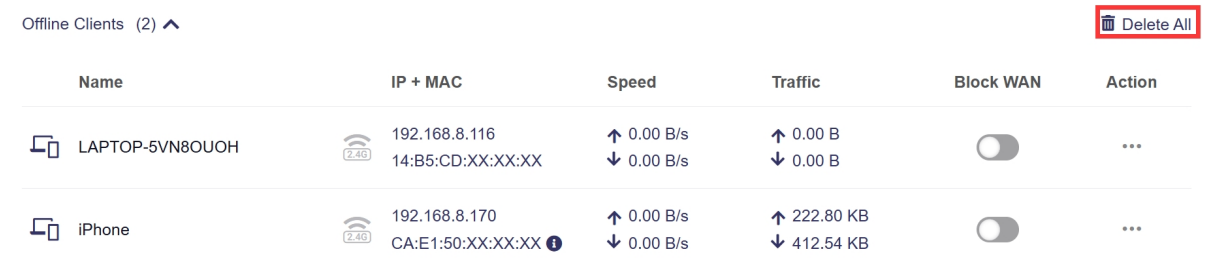


Jeśli dla urządzenia ustawiono ograniczenie prędkości, strzałki prędkości wysyłania i pobierania zmienią kolor na żółty.

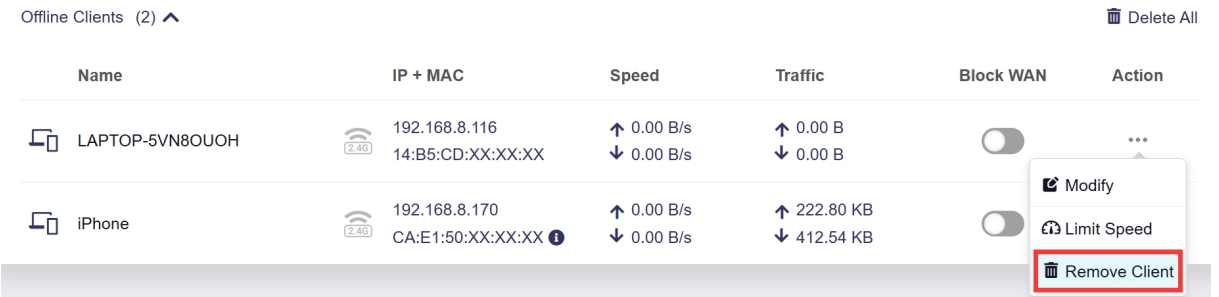


6.3 Usuwanie urządzeń klienckich

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

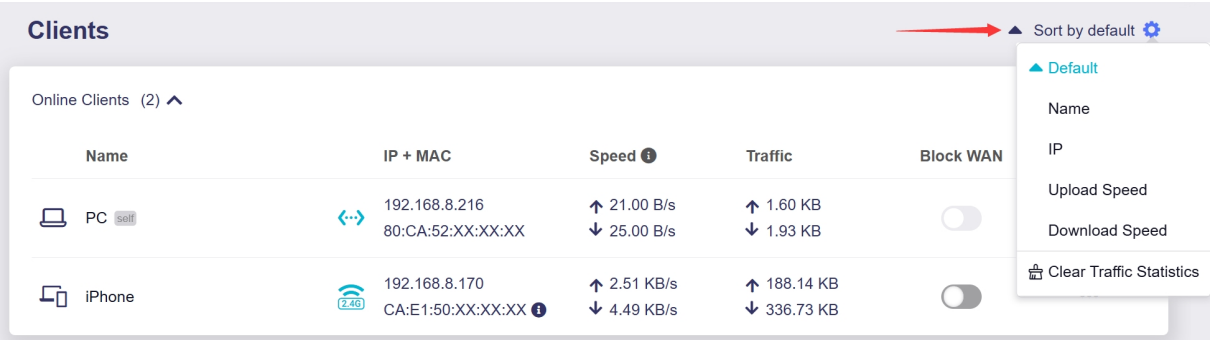


Aby usunąć określone urządzenie klienckie, kliknij ikonę trzech kropek w kolumnie **Action**, a następnie wybierz **Remove Client** z menu.



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



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

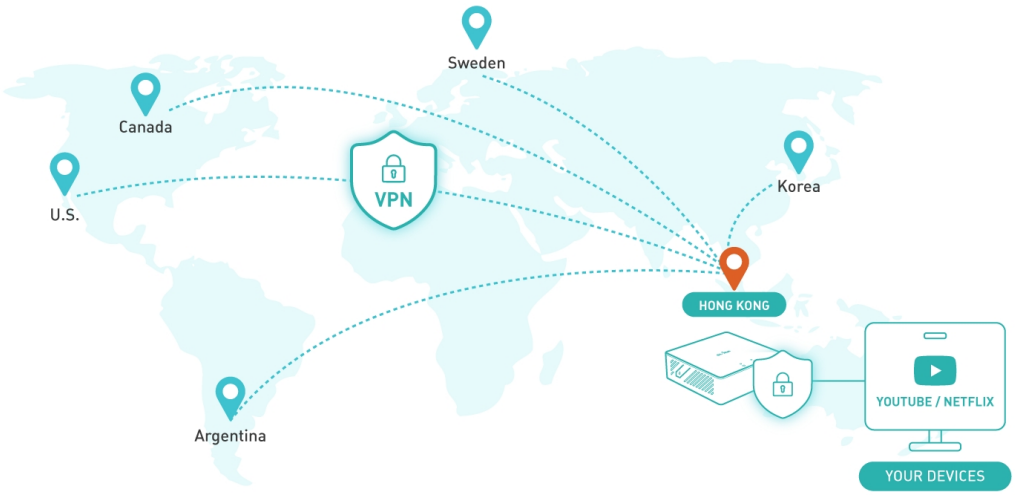
1. **Prywatność danych osobowych**

   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.



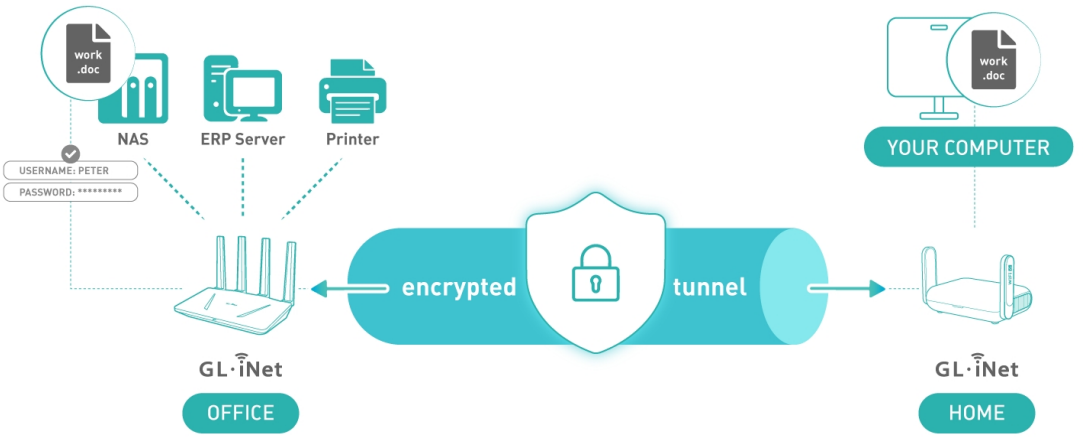
2. **Dostęp bez ograniczeń na całym świecie**

   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

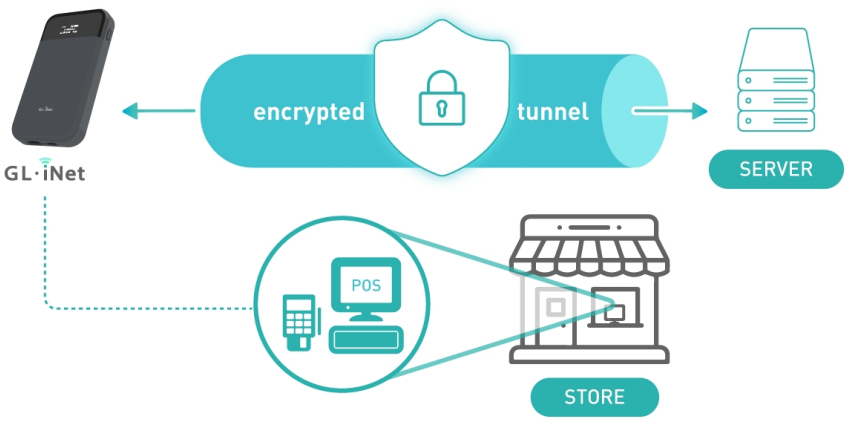
3. **Bezpieczeństwo danych małych firm**

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

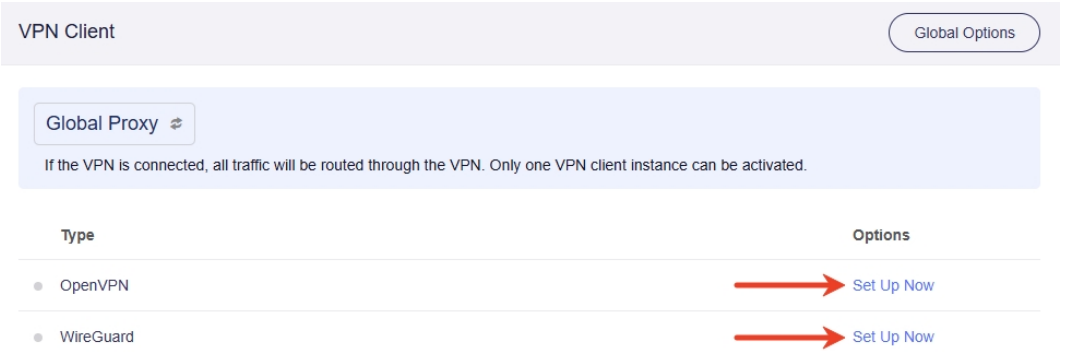
W tym rozdziale opisano zarządzanie połączeniami VPN w panelu administracyjnym.

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

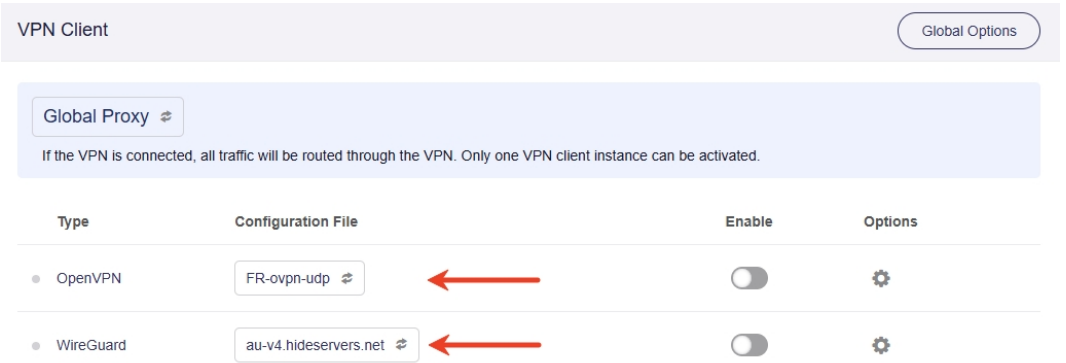
Gdy router działa jako aktywny klient VPN, panel VPN wyświetla szczegóły połączenia, takie jak adres serwera, statystyki transferu, wirtualny adres IP klienta i dziennik połączenia. Umożliwia też konfigurację ustawień zaawansowanych, takich jak Block non-VPN traffic, Allow Access WAN i Services from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

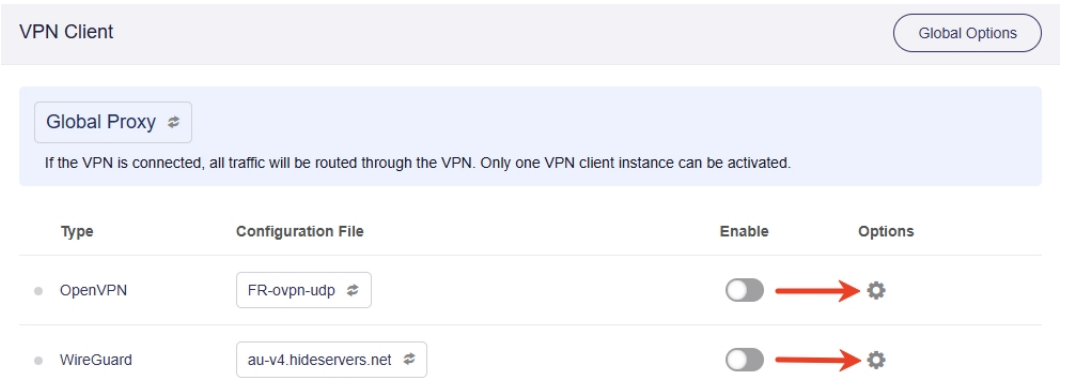


Po przesłaniu konfiguracja pojawi się w kolumnie **Configuration File**. Jeśli przesłano kilka plików konfiguracyjnych, możesz je przełączać, klikając pole wyboru.

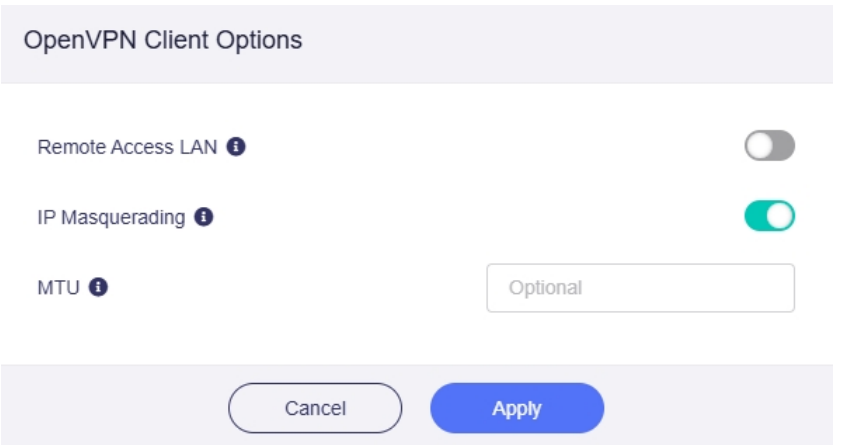


8.1.1 Opcje klienta

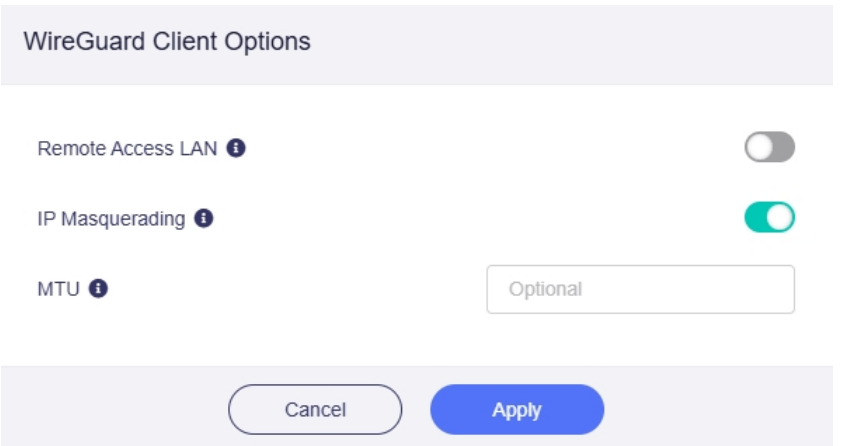
Kliknij ikonę koła zębatego po prawej stronie, aby otworzyć opcje klienta OpenVPN lub WireGuard.



Opcje klienta OpenVPN przedstawiono poniżej.

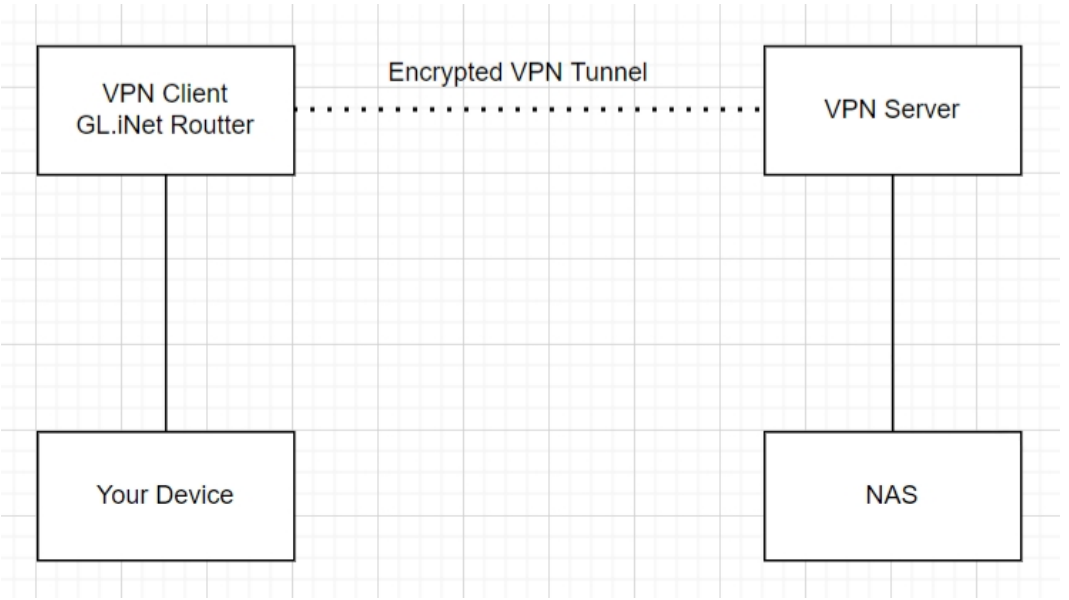


Opcje klienta WireGuard przedstawiono poniżej.



- **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.

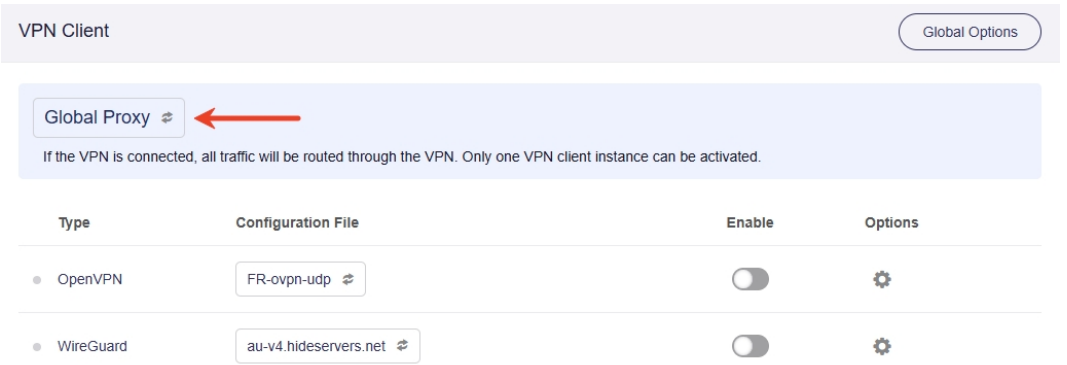
  Na przykład na poniższym schemacie router GL.iNet działa jako klient VPN i łączy się z serwerem VPN przez tunel VPN. Po włączeniu tej opcji urządzenia po stronie serwera VPN (np. NAS) mogą uzyskiwać dostęp zarówno do routera GL.iNet, jak i do urządzeń w jego sieci LAN. Wymaga to dodania na serwerze VPN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

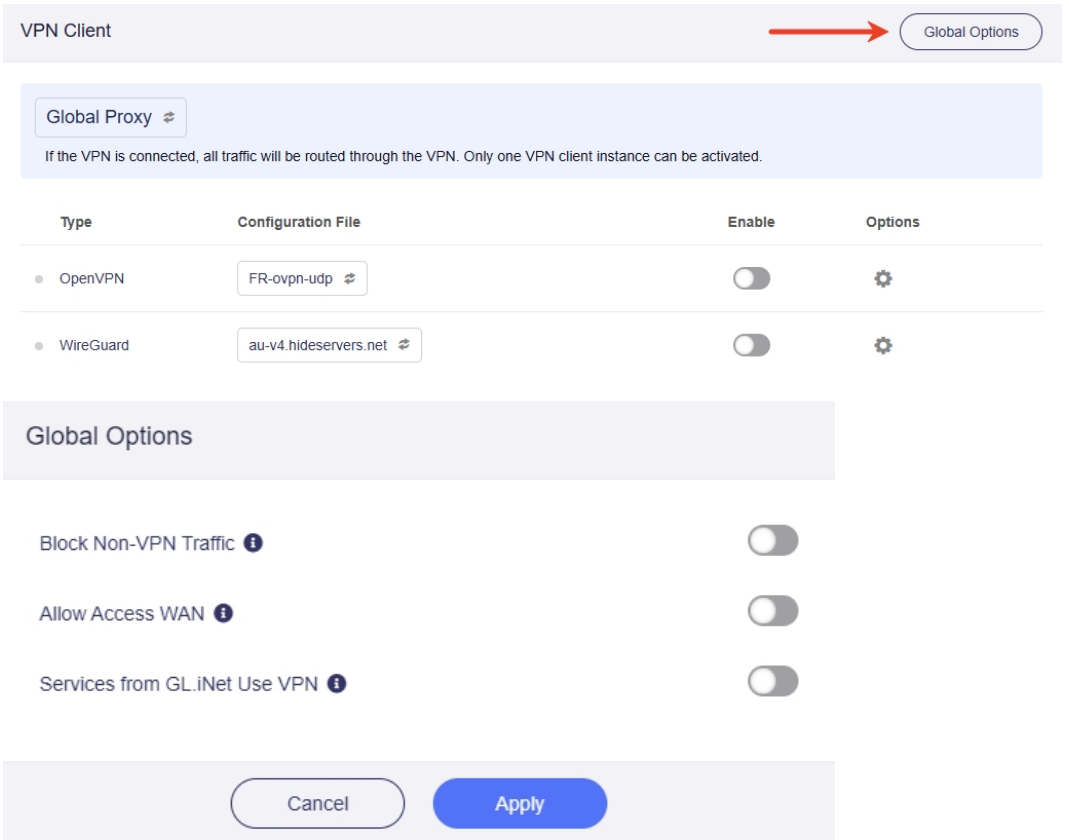
     Używane są reguły routingu określone w pliku konfiguracyjnym każdego klienta VPN lub przekazane przez serwer VPN.

   - **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.



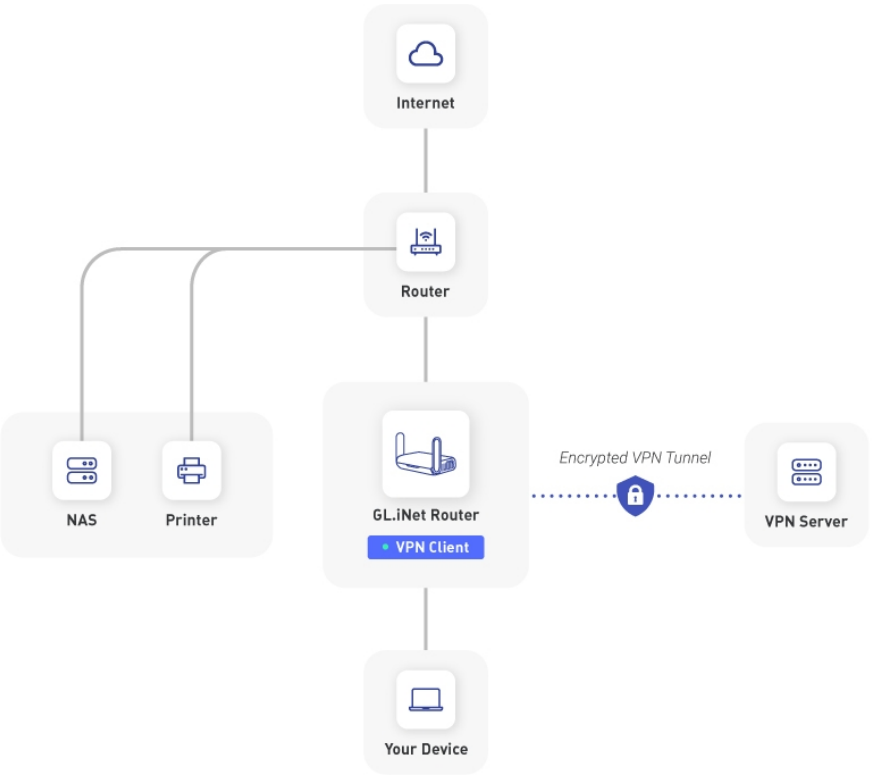
- **Block Non-VPN Traffic**: po włączeniu cały ruch internetowy musi przechodzić wyłącznie przez tunel VPN i nie może być kierowany przez inne interfejsy, np. WAN lokalnego dostawcy Internetu. Jeśli połączenie VPN niespodziewanie zostanie przerwane, cały ruch internetowy zostanie zablokowany, aby zapobiec 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.



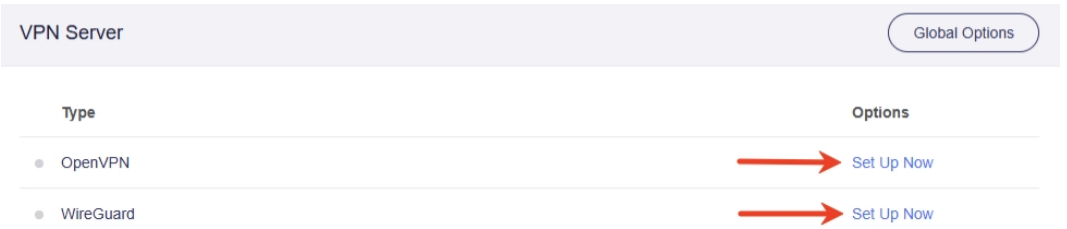
Jak pokazano na powyższym schemacie, włączenie tej funkcji pozwala urządzeniom lokalnym uzyskiwać dostęp do hostów w podsieci nadrzędnej, np. drukarek i serwerów NAS.

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.

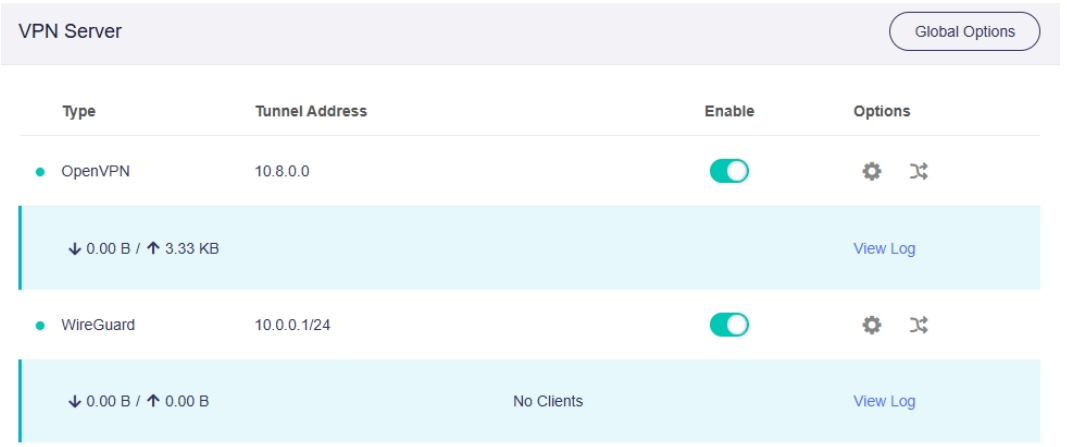
- **Services From GL.iNet Use VPN**: po włączeniu usługi GoodCloud, DDNS i rtty przesyłają pakiety przez tunele VPN. Ta opcja jest domyślnie wyłączona, ponieważ usługi te zwykle wymagają rzeczywistego adresu IP urządzenia do prawidłowego działania.

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.

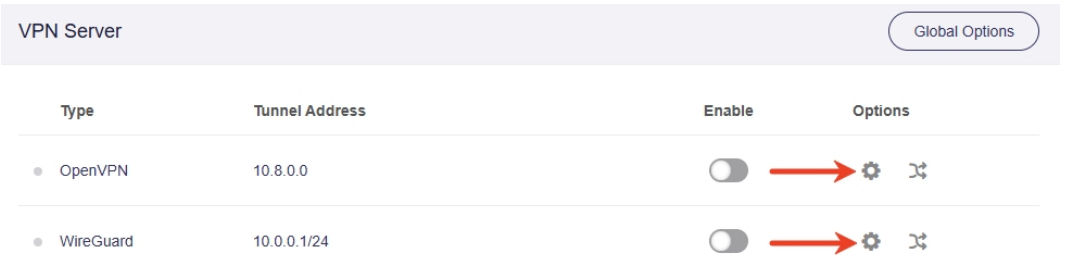


Po włączeniu serwera OpenVPN lub WireGuard na stronie pojawi się jego stan, jak pokazano poniżej.

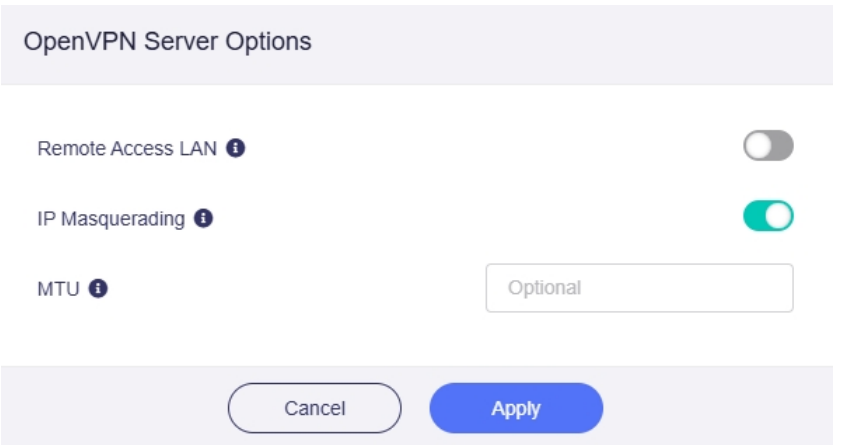


8.2.1 Opcje serwera

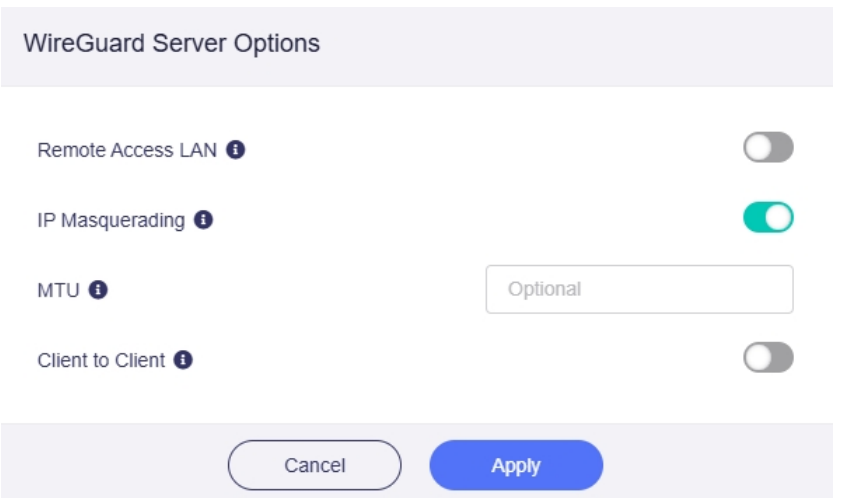
Kliknij ikonę koła zębatego po prawej stronie, aby otworzyć opcje serwera OpenVPN lub WireGuard.



Opcje serwera OpenVPN przedstawiono poniżej.



Opcje serwera WireGuard przedstawiono poniżej.

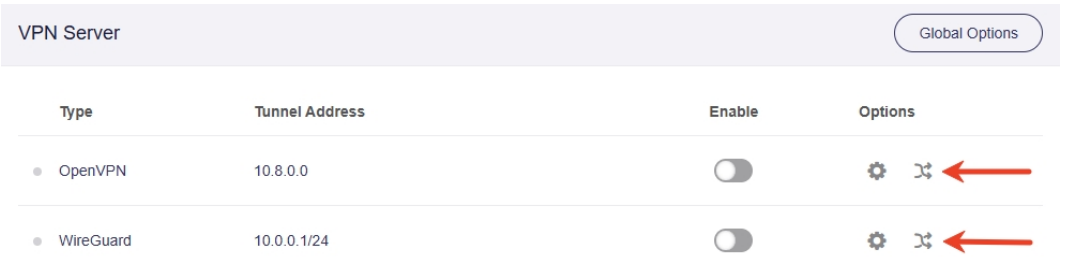


- **Remote Access LAN**: po włączeniu zasoby w podsieci LAN serwera są dostępne przez tunel VPN.

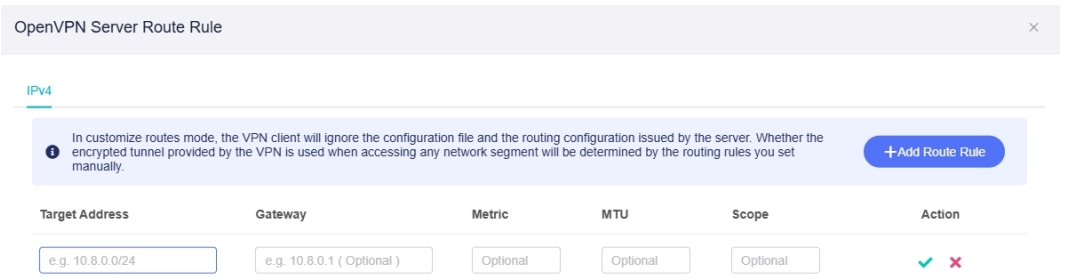
- **IP Masquerading**: po włączeniu źródłowe adresy IP klientów LAN są zastępowane adresem IP tunelu VPN routera. Wyłączaj tę opcję tylko w konfiguracjach sieć–sieć, w których zdalny węzeł zna Twoje podsieci LAN.
- **MTU**: skrót od Maximum Transmission Unit, czyli maksymalnej jednostki transmisji. Wartość 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

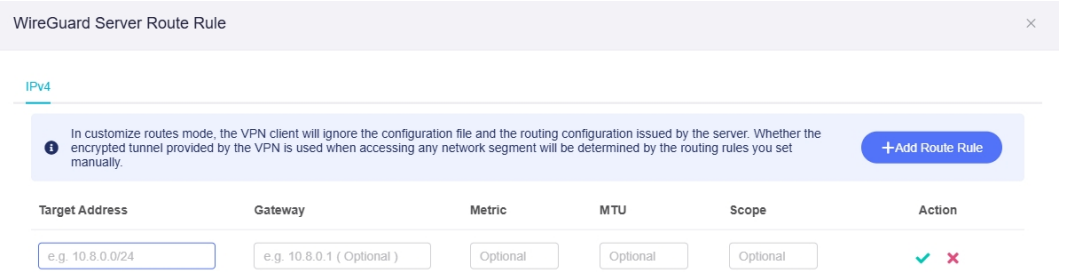
Kliknij ikonę trasy po prawej stronie, aby dostosować reguły tras OpenVPN lub WireGuard do swoich potrzeb.



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



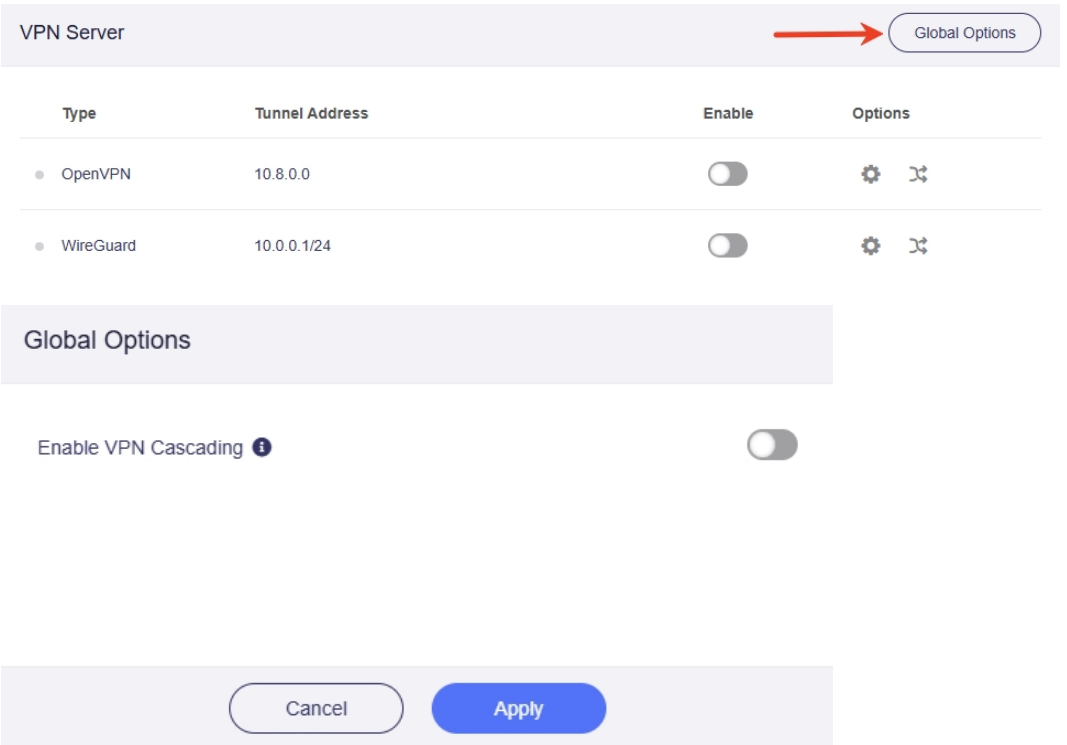
Reguły tras serwera WireGuard przedstawiono poniżej. Kliknij **Add Route Rule**, wprowadź **Target Address** i **Gateway**, a następnie kliknij zieloną ikonę zaznaczenia, aby zastosować ustawienia.



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:

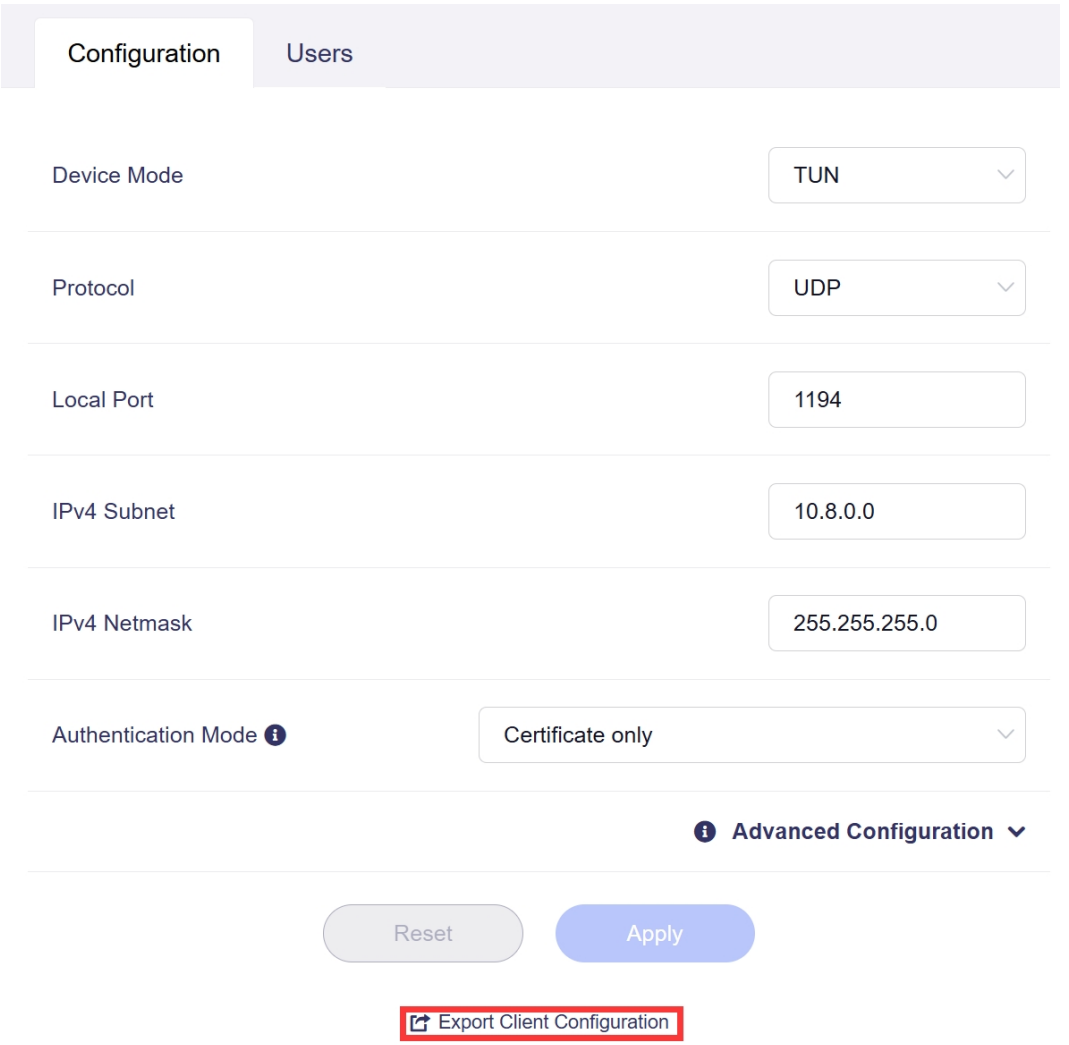
   - Jeśli przed routerem GL.iNet znajduje się główny router, zaloguj się do niego i sprawdź, czy ma publiczny adres IP przydzielony przez dostawcę Internetu.
   - Poproś dostawcę Internetu o publiczny adres IP. Może to wiązać się z dodatkową opłatą.

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**.

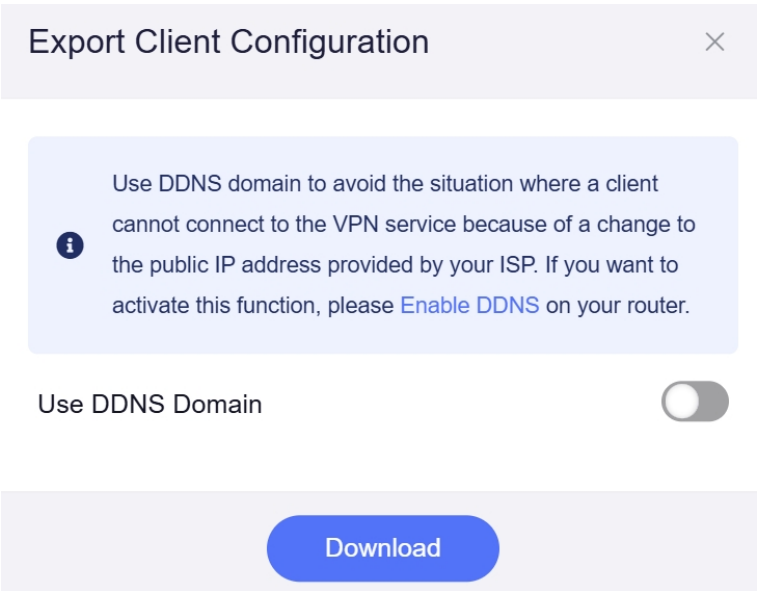


- **Device Mode**: TAP-S2S lub Tun. Różnice opisano tutaj.
- **Protocol**: UDP lub TCP. Różnice opisano tutaj.
- **Authentication Mode**: określa metodę uwierzytelniania klienta podczas łączenia z serwerem. Dostępne są trzy opcje:

- **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.

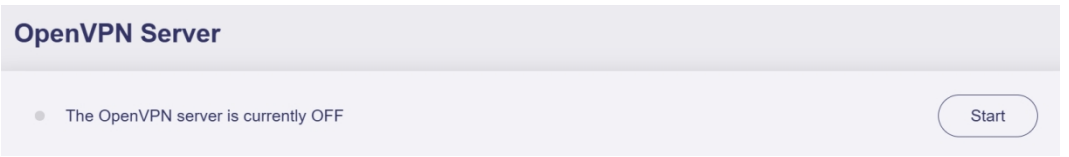
3. Wyeksportuj konfigurację klienta.
   Po kliknięciu **Export Client Configuration** u dołu karty Configuration (lub zastosowaniu zmienionej konfiguracji) pojawi się poniższe okno. Kliknij **Download**, aby wyeksportować konfigurację.



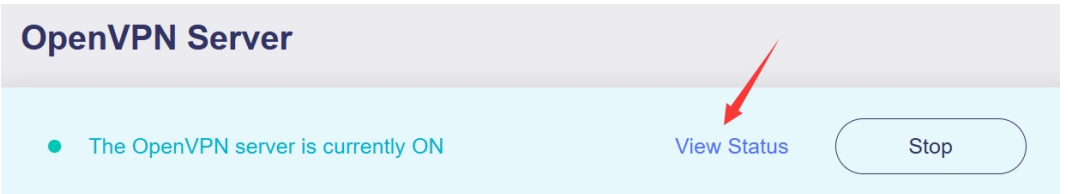
   Wskazówka: jeśli Twój publiczny adres IP często się zmienia, przejdź do **APPLICATIONS** > **Dynamic DNS** i włącz DDNS. Możesz wtedy używać domeny DDNS jako adresu serwera.

4. Uruchom serwer OpenVPN.

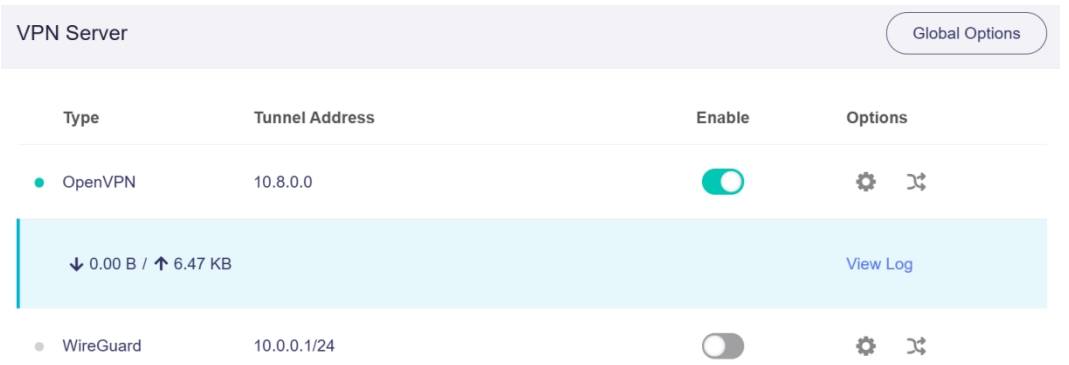
Na stronie **OpenVPN Server** kliknij przycisk **Start** w prawym górnym rogu, aby uruchomić serwer.



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. Wskazówki dotyczące rozwiązywania problemów znajdziesz tutaj.
- Może być konieczne skonfigurowanie przekierowania portów. Wskazówki dotyczące rozwiązywania problemów 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:

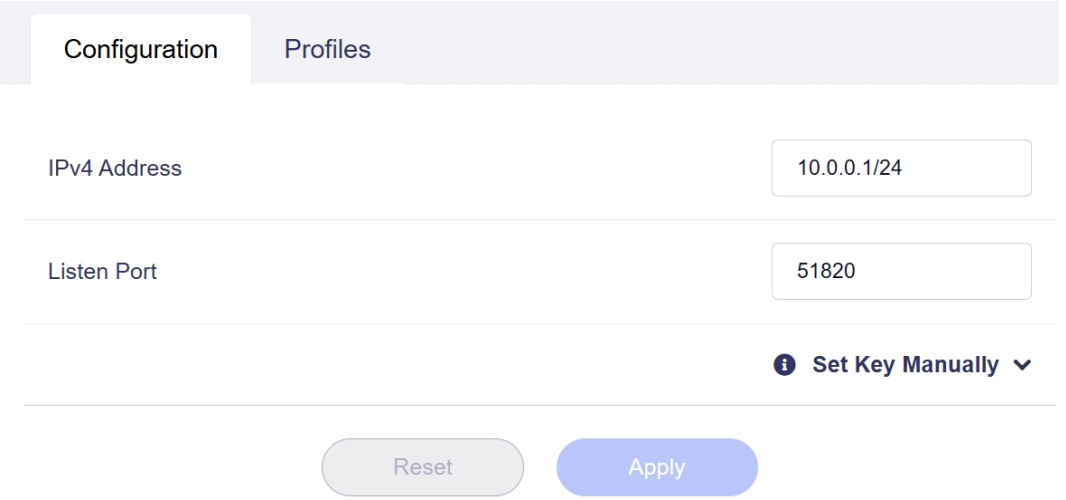
   - Jeśli przed routerem GL.iNet znajduje się główny router, zaloguj się do niego i sprawdź, czy ma publiczny adres IP przydzielony przez dostawcę Internetu.
   - Poproś dostawcę Internetu o publiczny adres IP. Może to wiązać się z dodatkową opłatą.

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

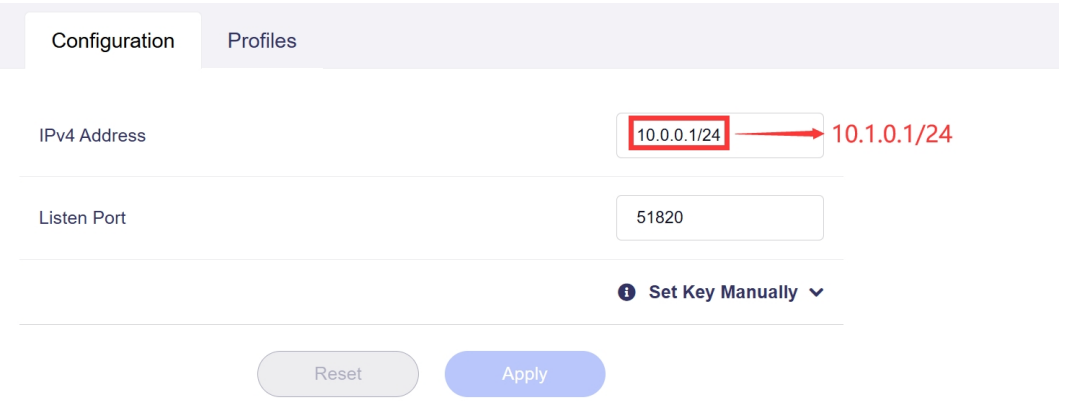
   - Jeśli router GL.iNet jest głównym routerem w sieci, konfiguracja przekierowania portów nie jest wymagana. Przejdź do następnego kroku.
   - Jeśli korzystasz już z głównego routera, a router GL.iNet działa jako router dodatkowy, trzeba skonfigurować przekierowanie portów na głównym routerze.
   - Jeśli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

9.2.2 Etapy konfiguracji

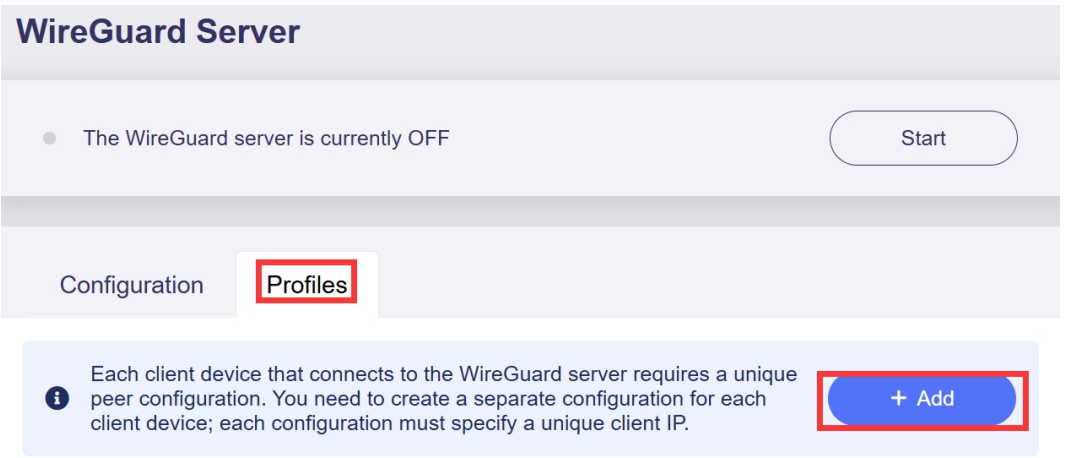
1. Zaloguj się do panelu administracyjnego routera, przejdź do **VPN** > **WireGuard Server**, a następnie kliknij **Generate Configuration** (tylko przy pierwszej konfiguracji serwera VPN).
2. Zastosuj konfigurację.
   Domyślna konfiguracja sprawdza się w większości przypadków. Nie trzeba zmieniać adresu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



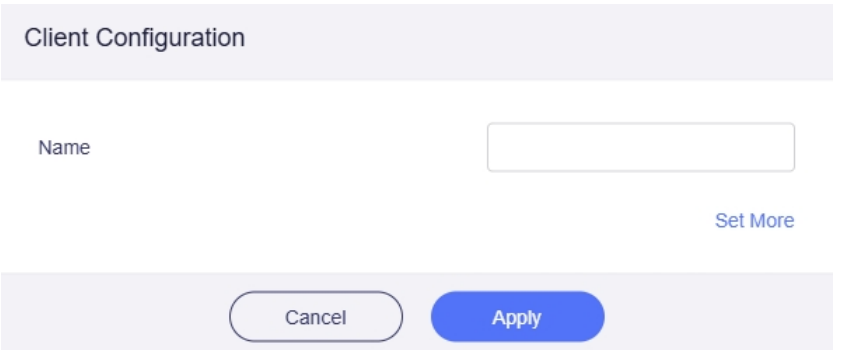
   Jeśli adres IPv4 koliduje z adresem bramy routera nadrzędnego, zmień go na inny (np. **10.1.0.1/24**) i kliknij **Apply**. Aby uniknąć problemów z łącznością, koniecznie zachowaj zapis CIDR „/24”.



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



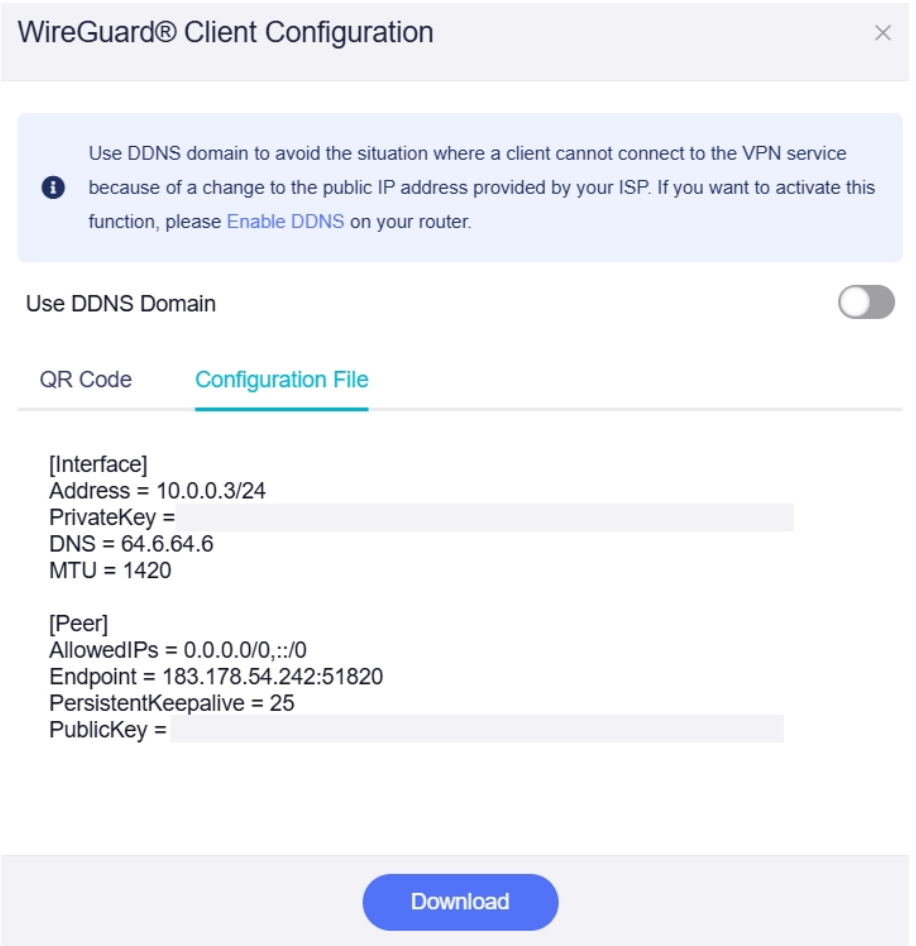
Nadaj opisową nazwę i kliknij **Apply**, aby kontynuować.



4. Pobierz konfigurację.

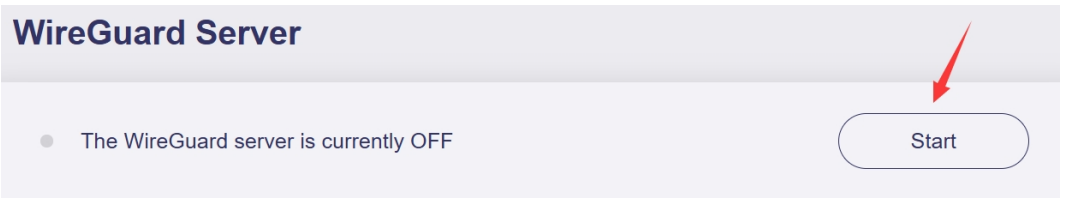
   Po dodaniu profilu router generuje plik konfiguracyjny w trzech postaciach: kodu QR, zwykłego tekstu i pliku .conf. Wybierz preferowany sposób uzyskania konfiguracji.

   - **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.

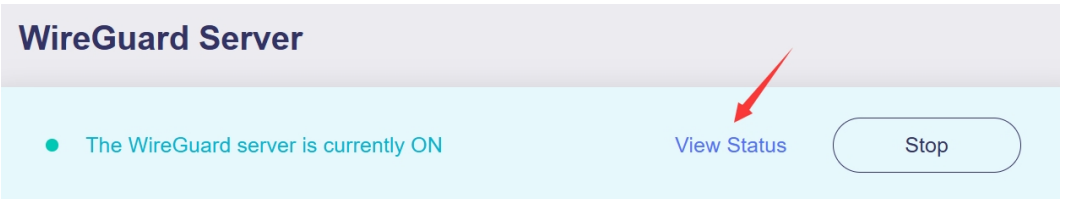


Wskazówka: jeśli Twój publiczny adres IP często się zmienia, przejdź do **APPLICATIONS** > **Dynamic DNS** i włącz DDNS. Możesz wtedy używać domeny DDNS jako adresu serwera.

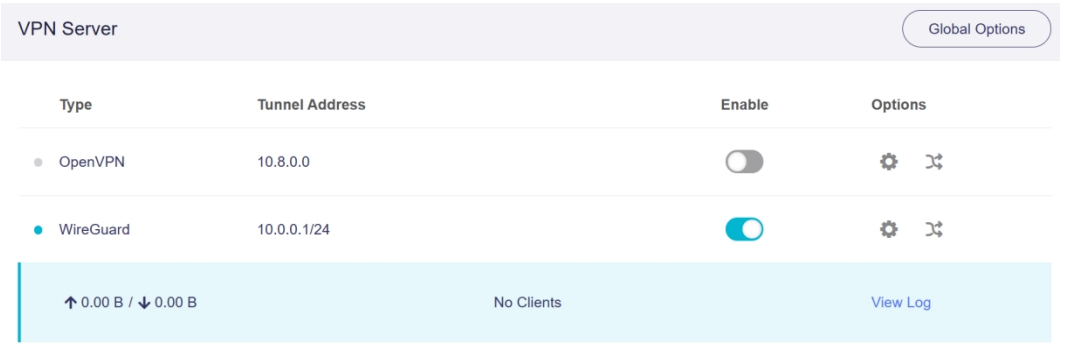
5. Uruchom serwer WireGuard.
   Na stronie **WireGuard Server** kliknij przycisk **Start** w prawym górnym rogu, aby uruchomić serwer.



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. Wskazówki dotyczące rozwiązywania problemów znajdziesz tutaj.
- Może być konieczne skonfigurowanie przekierowania portów. Wskazówki dotyczące rozwiązywania problemów 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.

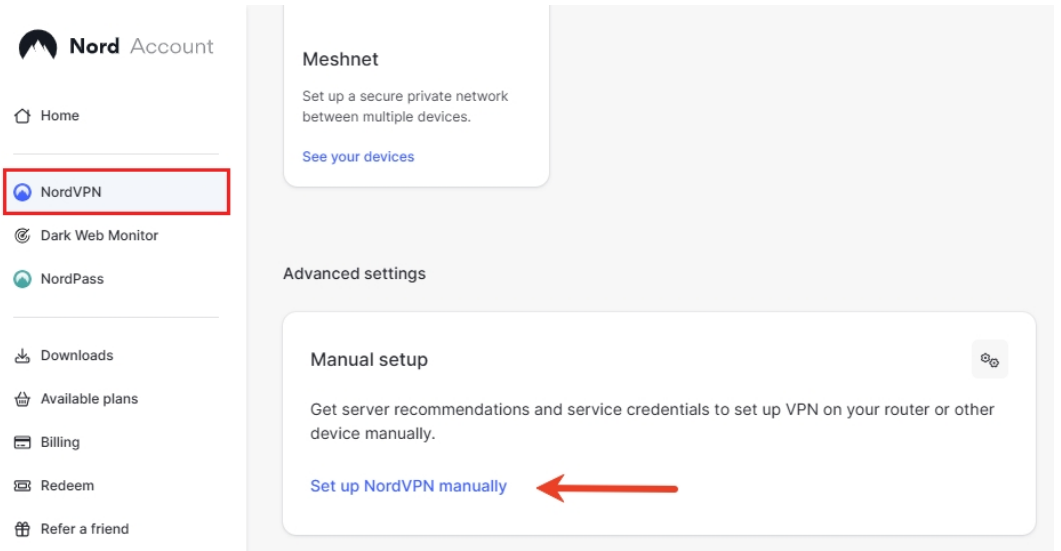
Następnie odwiedź oficjalną witrynę dostawcy VPN, którego usługę subskrybujesz, i uzyskaj dane dostępowe usługi lub plik konfiguracyjny. Jeśli nie wiesz, jak uzyskać plik konfiguracyjny, skorzystaj z tego łącza lub skontaktuj się z pomocą techniczną dostawcy.

10.1.2 Konfiguracja NordVPN

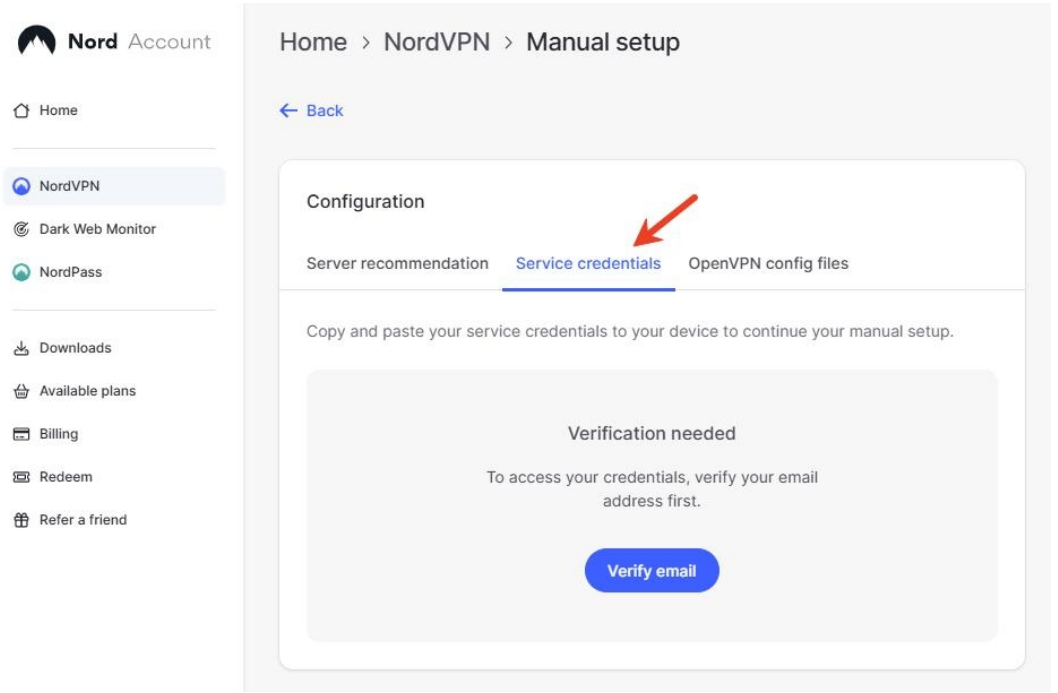
NordVPN jest zintegrowany z panelem administracyjnym GL.iNet. Pliki konfiguracyjne wszystkich serwerów NordVPN można uzyskać, wprowadzając dane dostępowe konta (z panelu NordVPN) w panelu administracyjnym routera lub aplikacji mobilnej GL.iNet. Eliminuje to potrzebę ręcznego przesyłania plików.

Aby skonfigurować router jako klienta NordVPN, wykonaj poniższe czynności.

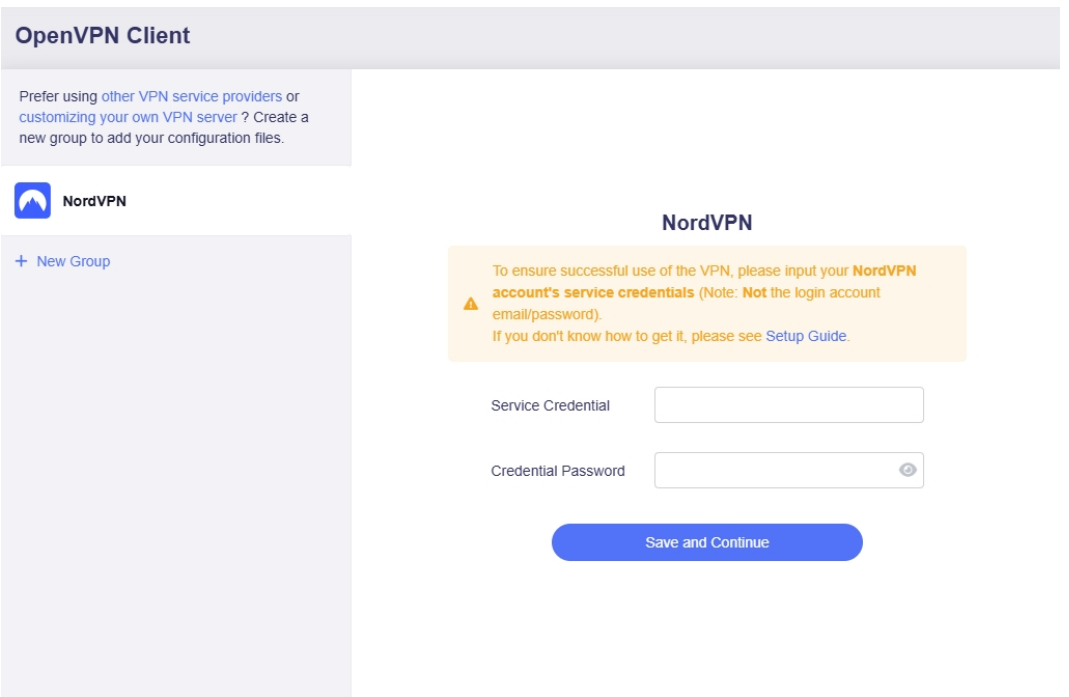
1. Zaloguj się na swoje konto internetowe NordVPN tutaj.
2. W panelu Nord kliknij **NordVPN**, a następnie **Set up NordVPN manually**.



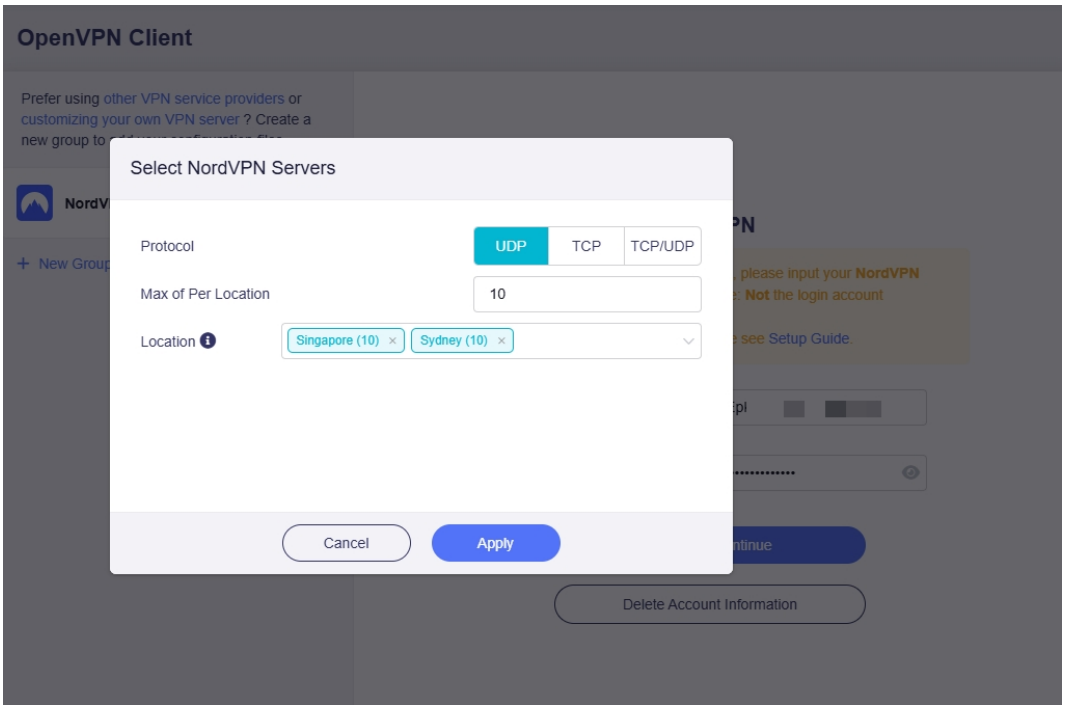
Znajdziesz tam **dane dostępowe usługi**. Skopiuj je do późniejszego użycia.



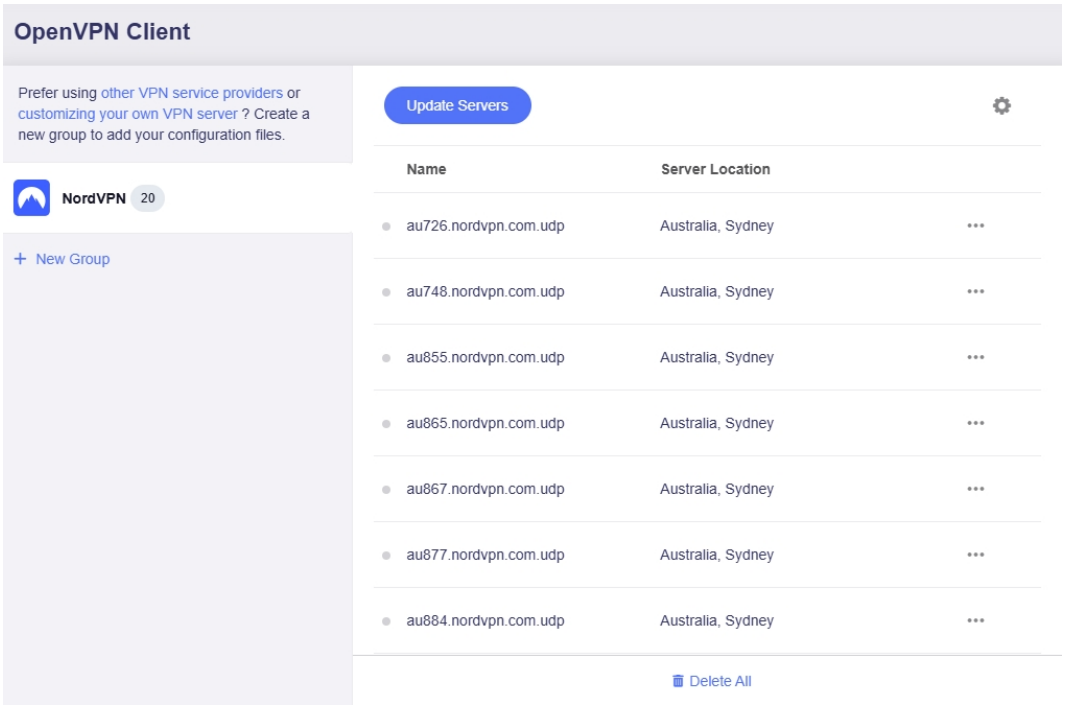
3. Zaloguj się do panelu administracyjnego routera i przejdź do **VPN** > **OpenVPN Client** > **NordVPN**. Wprowadź dane dostępowe usługi (uwaga: NIE jest to adres e-mail ani hasło do logowania na konto), a następnie kliknij **Save and Continue**.



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

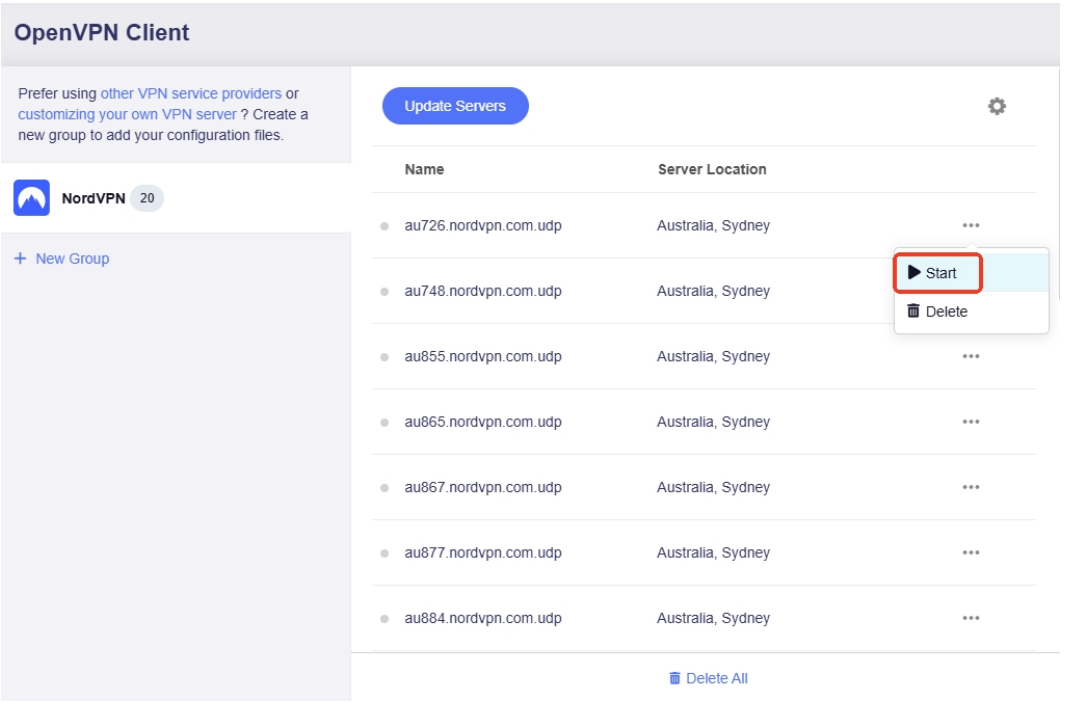


Rozpocznie się pobieranie plików konfiguracyjnych.

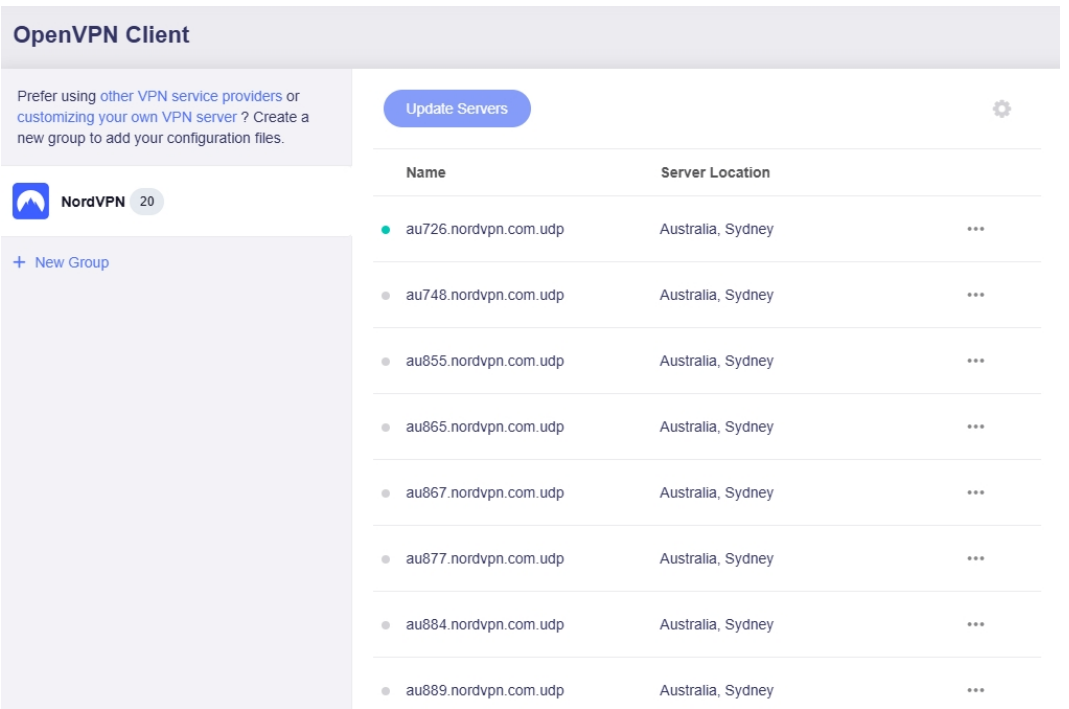


5. Nawiąż połączenie.

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



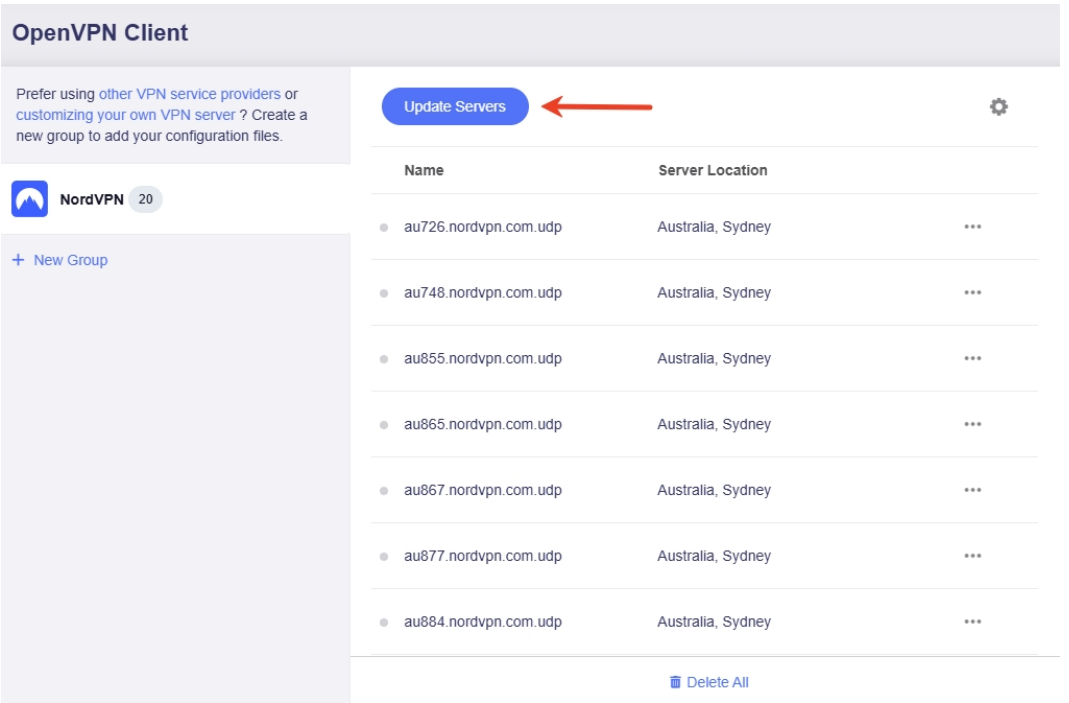
6. Po połączeniu obok pliku konfiguracyjnego pojawi się zielona kropka.



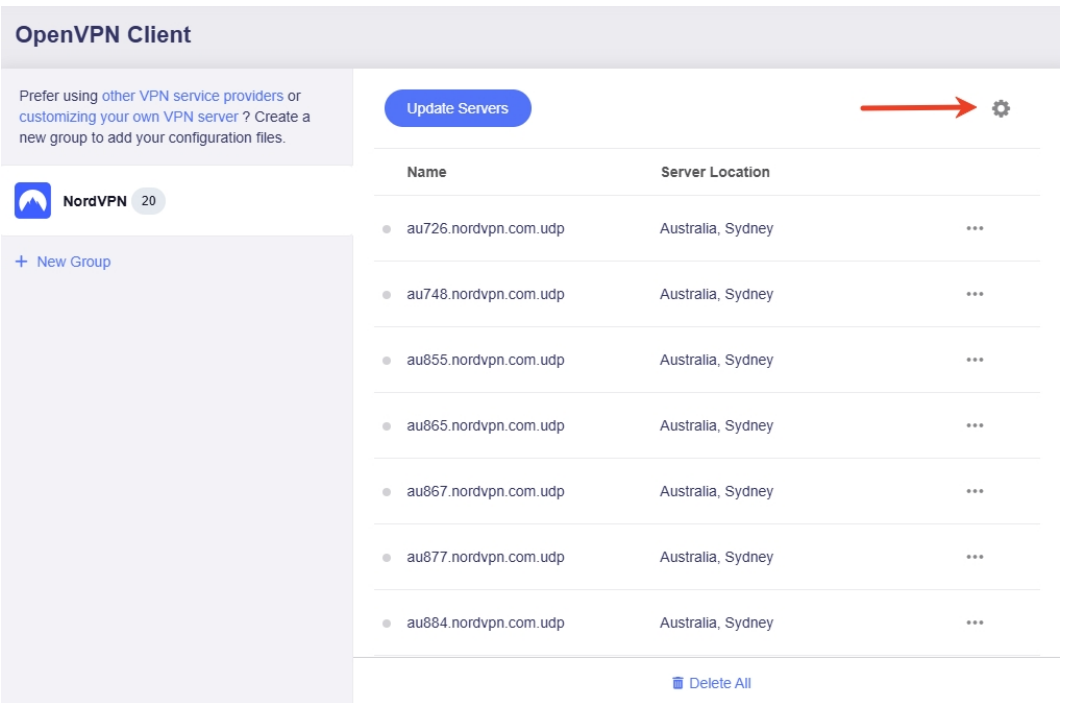
Szczegóły połączenia VPN możesz również sprawdzić w **VPN Dashboard**.

7. Zaktualizuj serwery.

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

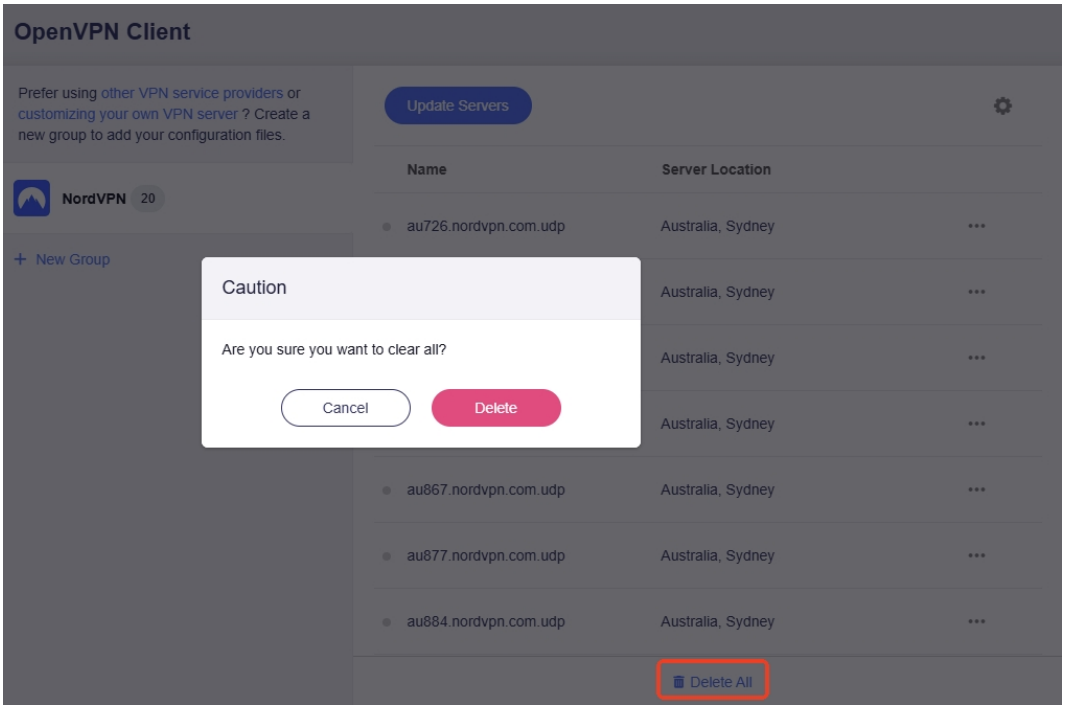


8. Zmień dane dostępowe.
   Kliknij ikonę koła zębatego, aby zmienić dane logowania.



9. Usuń wszystkie pliki.

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

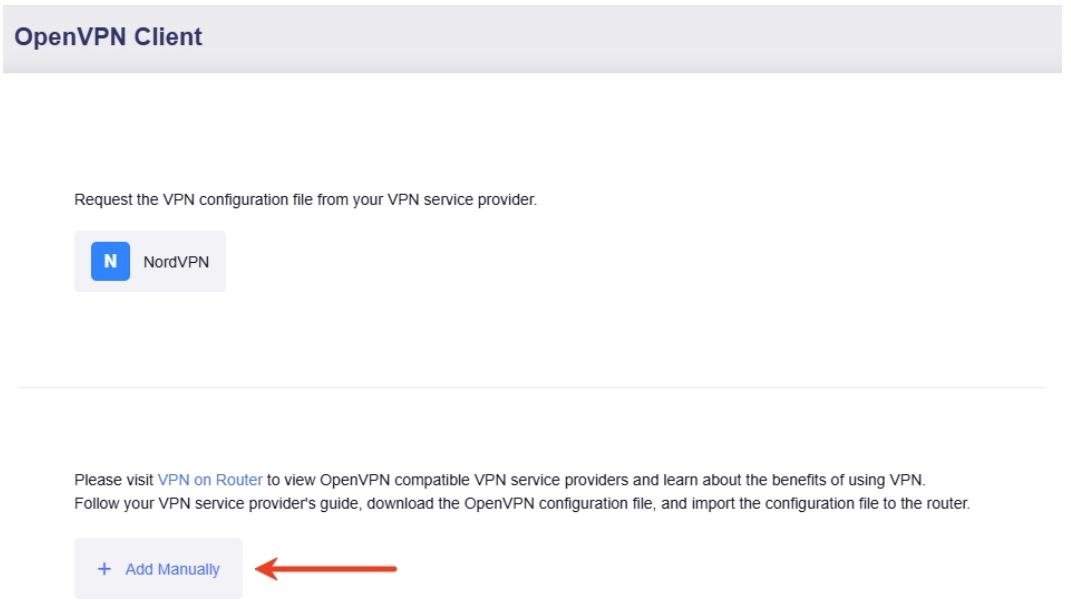


10.1.3 Ręczna konfiguracja klienta OpenVPN (inni dostawcy)

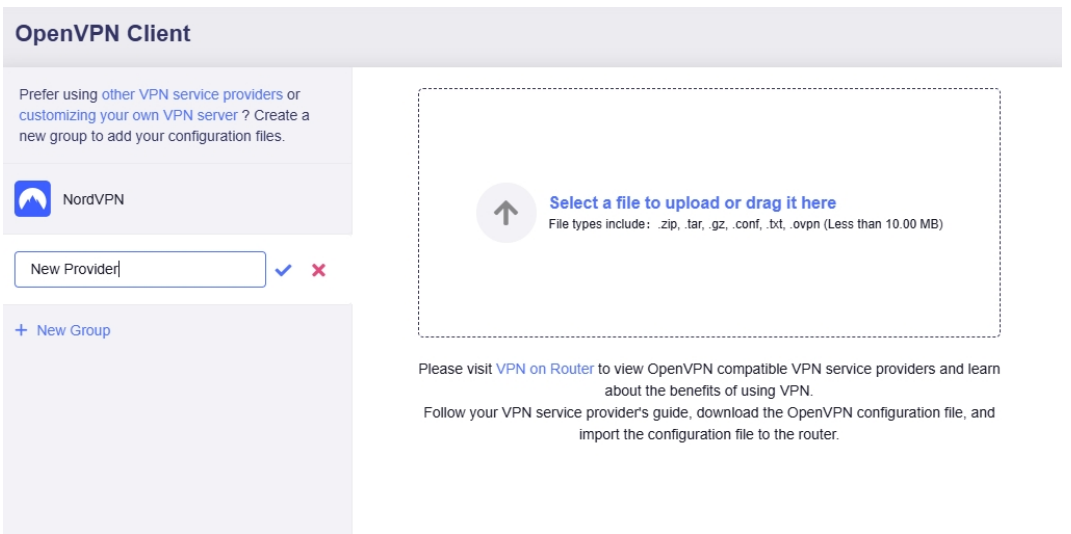
Jeśli Twój dostawca OpenVPN nie jest zintegrowany z panelem administracyjnym, najpierw odwiedź jego oficjalną witrynę i pobierz plik konfiguracyjny. Następnie prześlij go do routera, aby skonfigurować klienta OpenVPN.

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

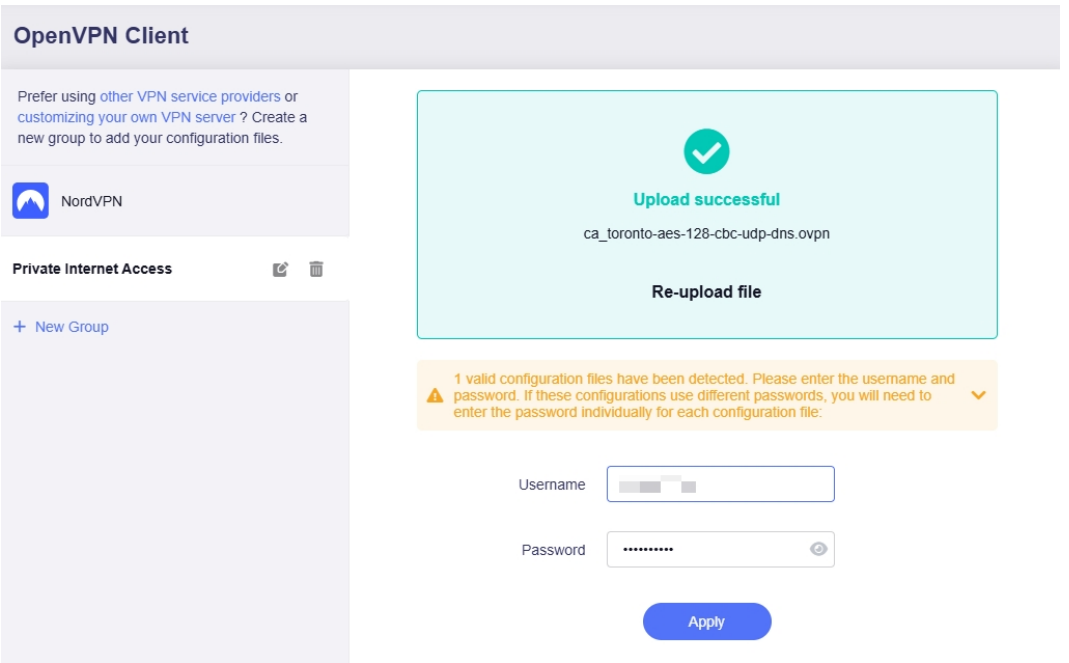
1. Pobierz plik konfiguracyjny z oficjalnej witryny Private Internet Access.
2. Zaloguj się do panelu administracyjnego routera, przejdź do **VPN** > **OpenVPN Client** i kliknij **Add Manually**.



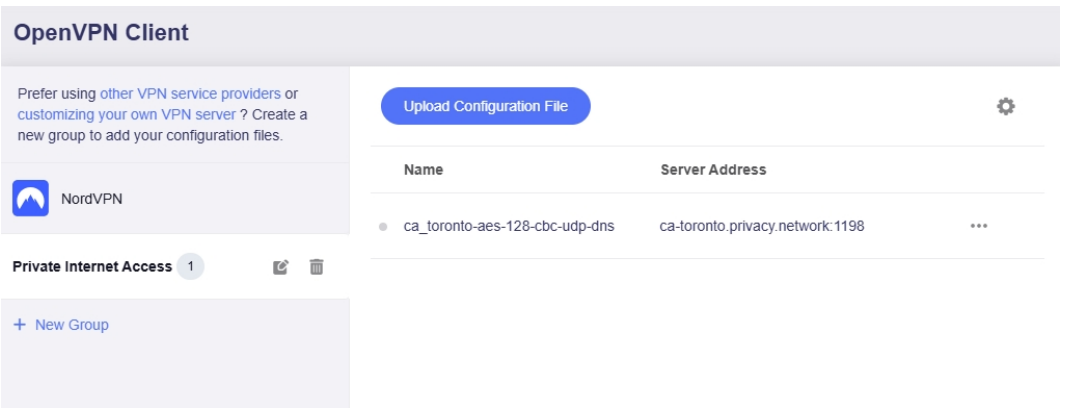
3. Na lewym pasku bocznym powstanie grupa. Nadaj jej opisową nazwę.



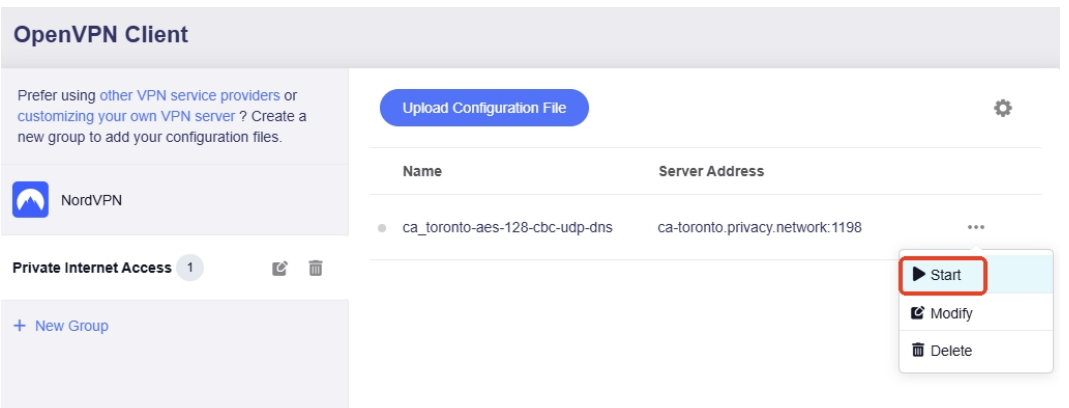
4. Prześlij plik konfiguracyjny OpenVPN. Jeśli jest to wymagane, wprowadź dane dostępowe, a następnie kliknij **Apply**.



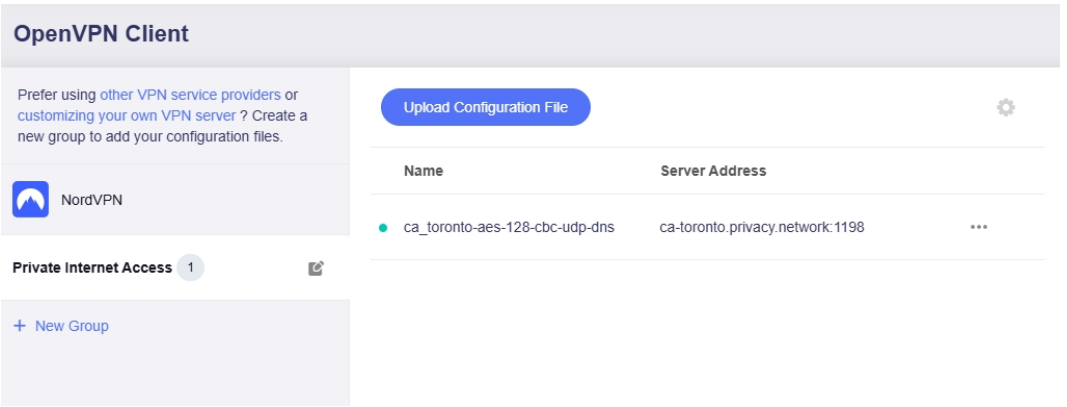
Pojawi się przesłany plik konfiguracyjny.



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.

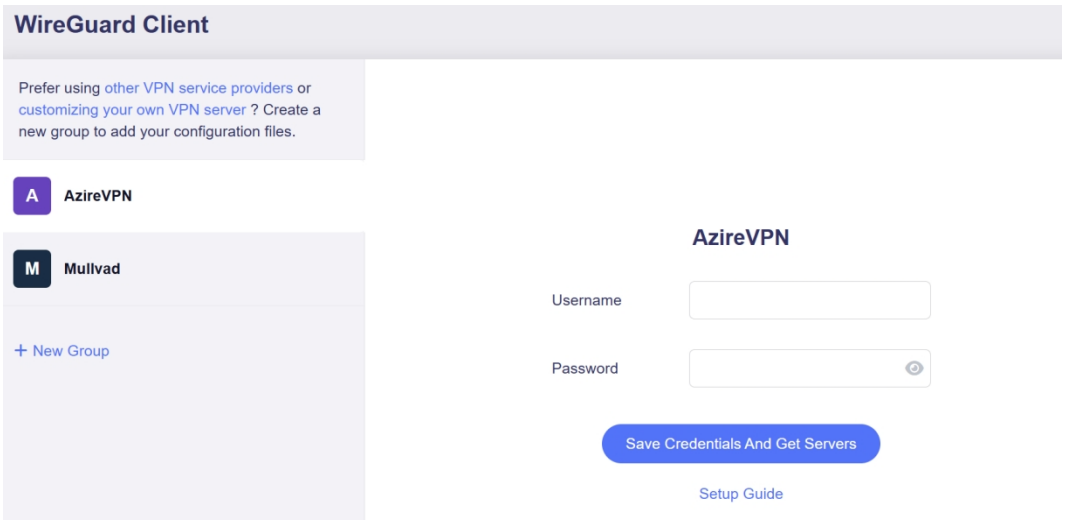
Następnie wybierz poniżej odpowiedniego dostawcę WireGuard, aby szybko przejść do instrukcji krok po kroku.

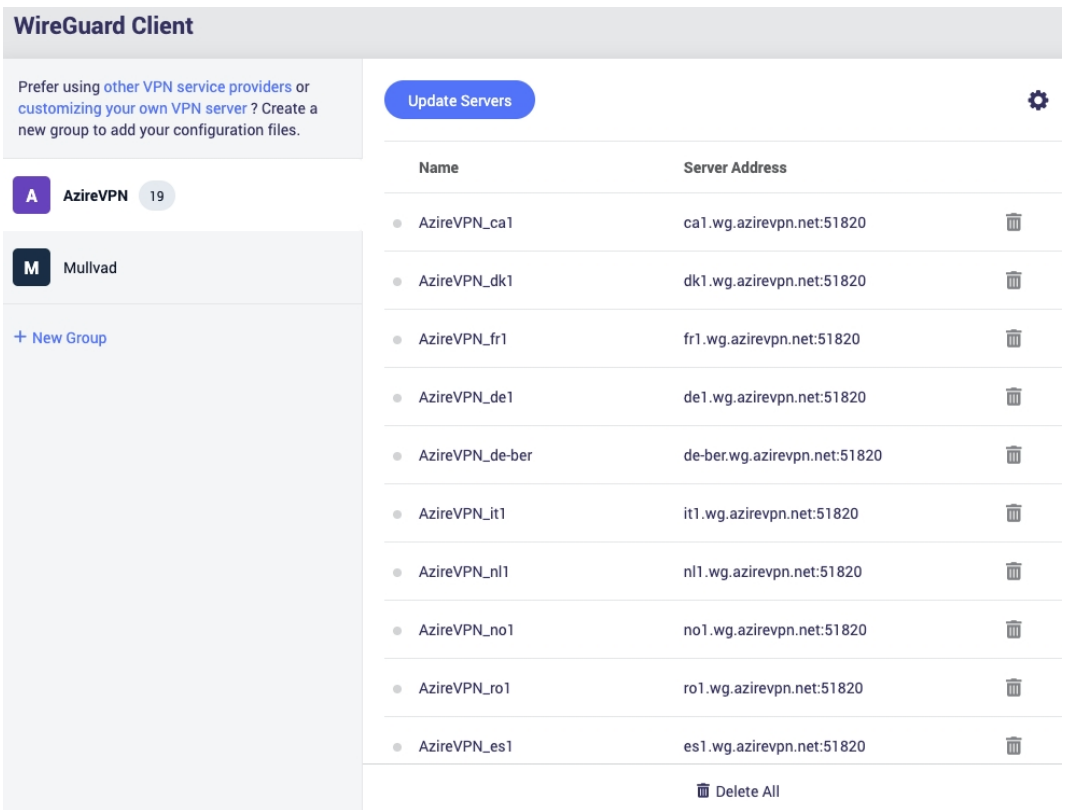
- Konfiguracja AzireVPN
- Konfiguracja Mullvad
- Ręczna konfiguracja klienta WireGuard (inni dostawcy)

10.2.2 Konfiguracja AzireVPN

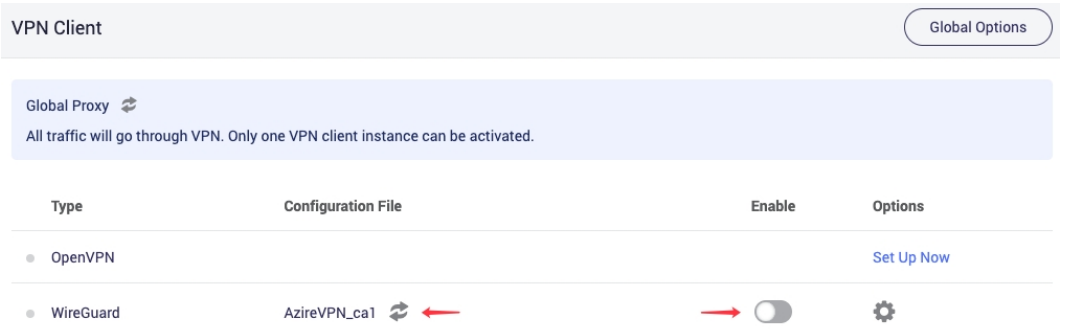
Aby skonfigurować router jako klienta AzireVPN, wykonaj poniższe czynności.

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.

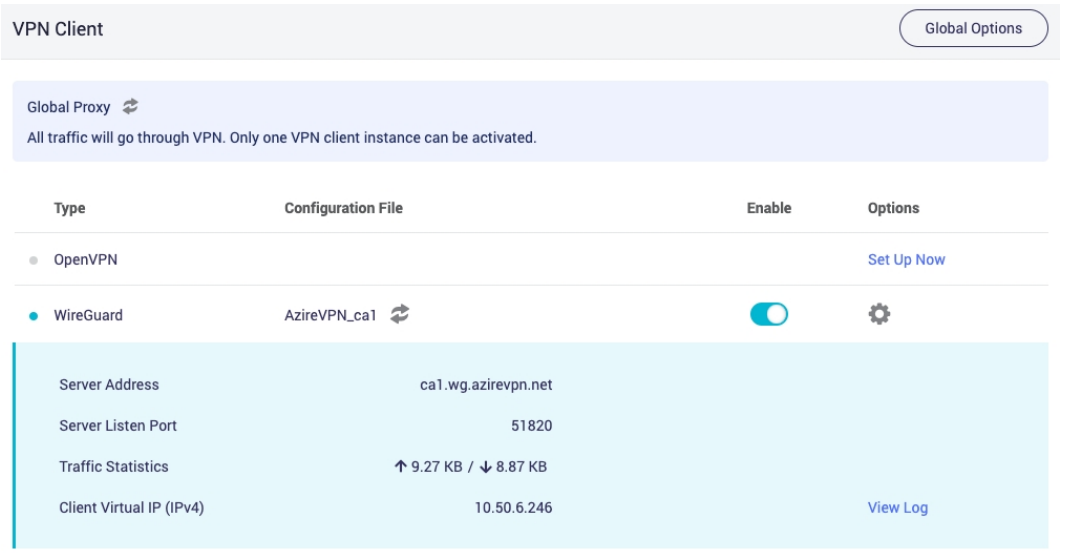




3. Przejdź do VPN Dashboard, aby włączyć połączenie.

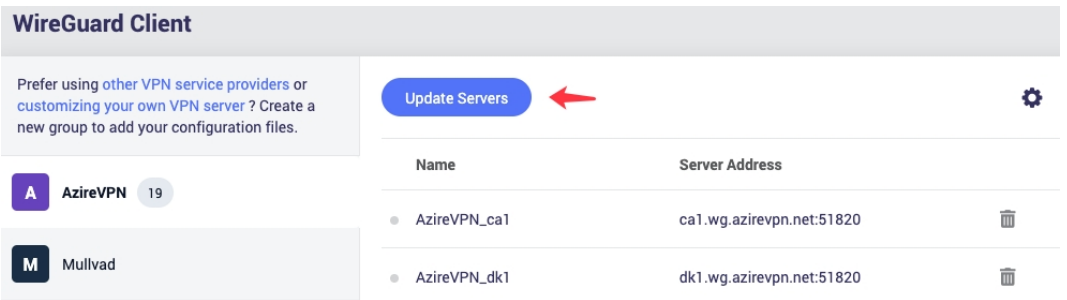


Po połączeniu powinny być widoczne Twój adres IP oraz liczba wysłanych i odebranych bajtów.



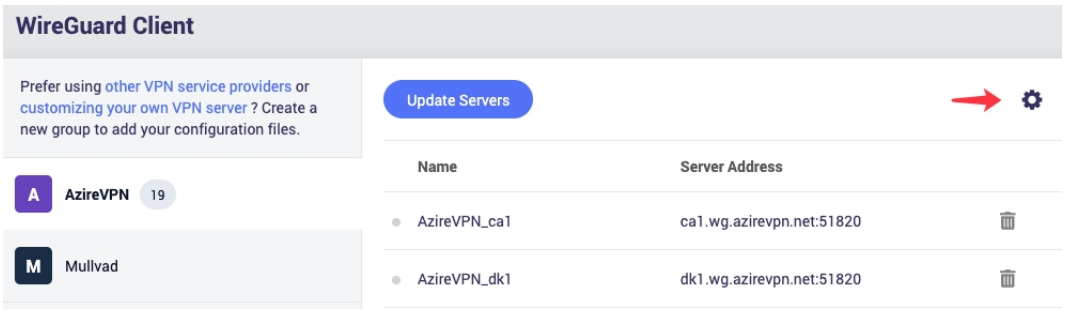
4. Zaktualizuj serwery.

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



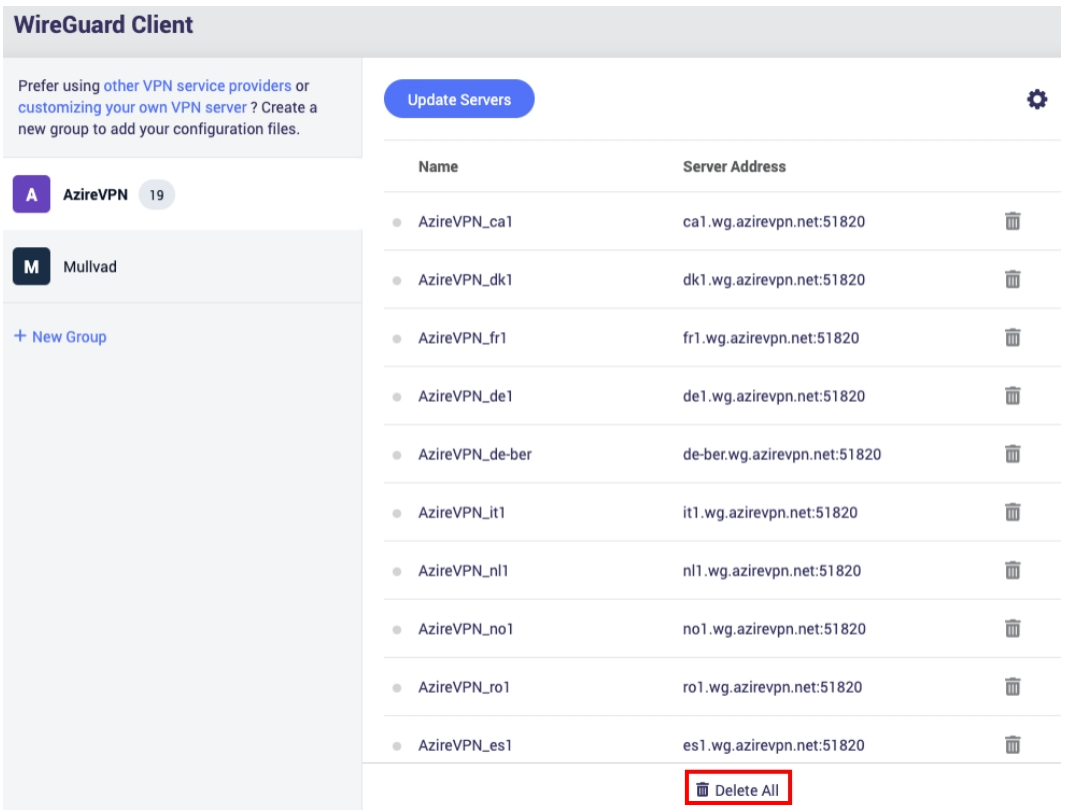
5. Zmień dane dostępowe.

   Kliknij ikonę koła zębatego, aby zmienić dane dostępowe.



6. Usuń wszystkie pliki.

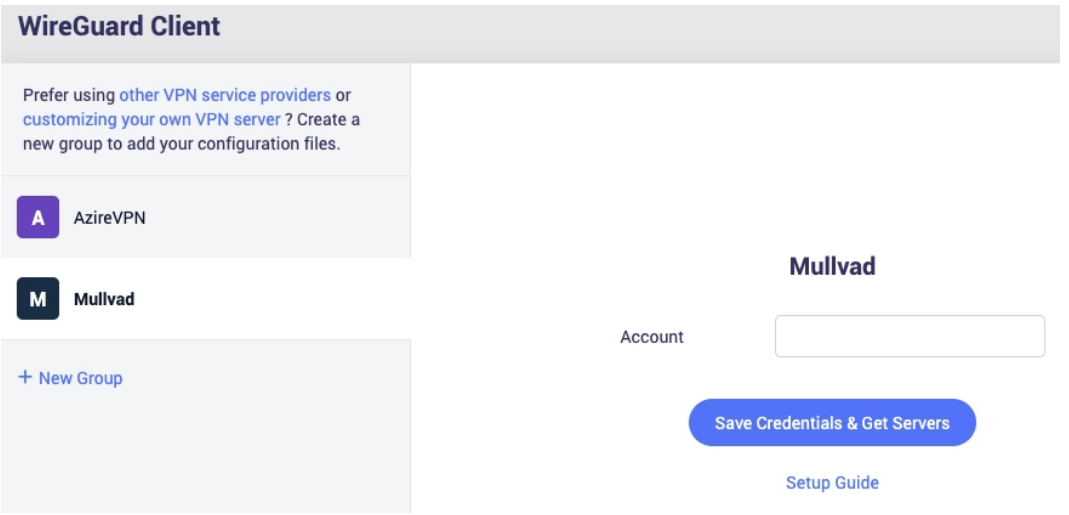
   Możesz kliknąć **Delete All**, aby jednym kliknięciem usunąć wszystkie pliki konfiguracyjne.



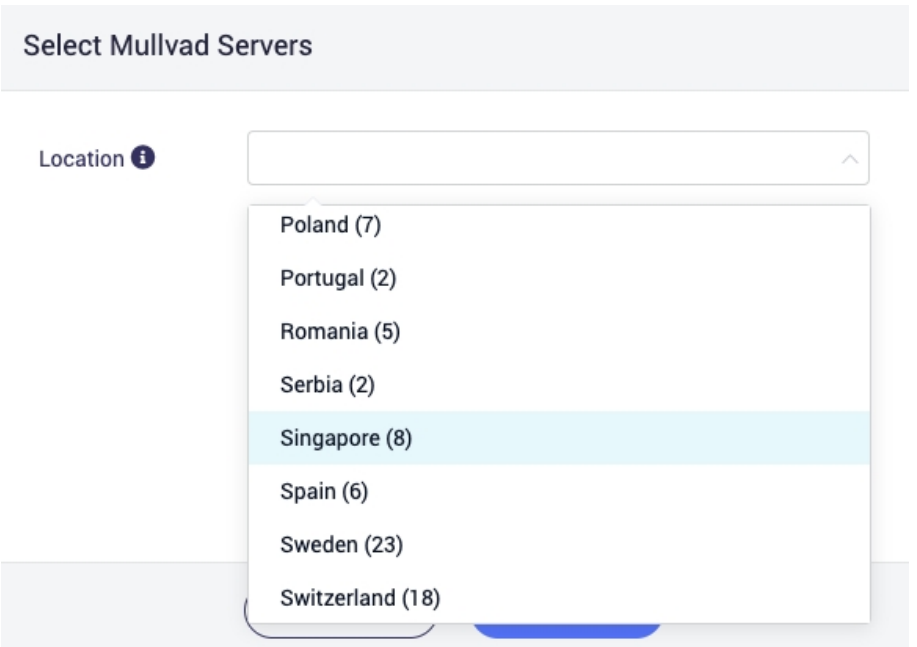
10.2.3 Konfiguracja Mullvad

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**.

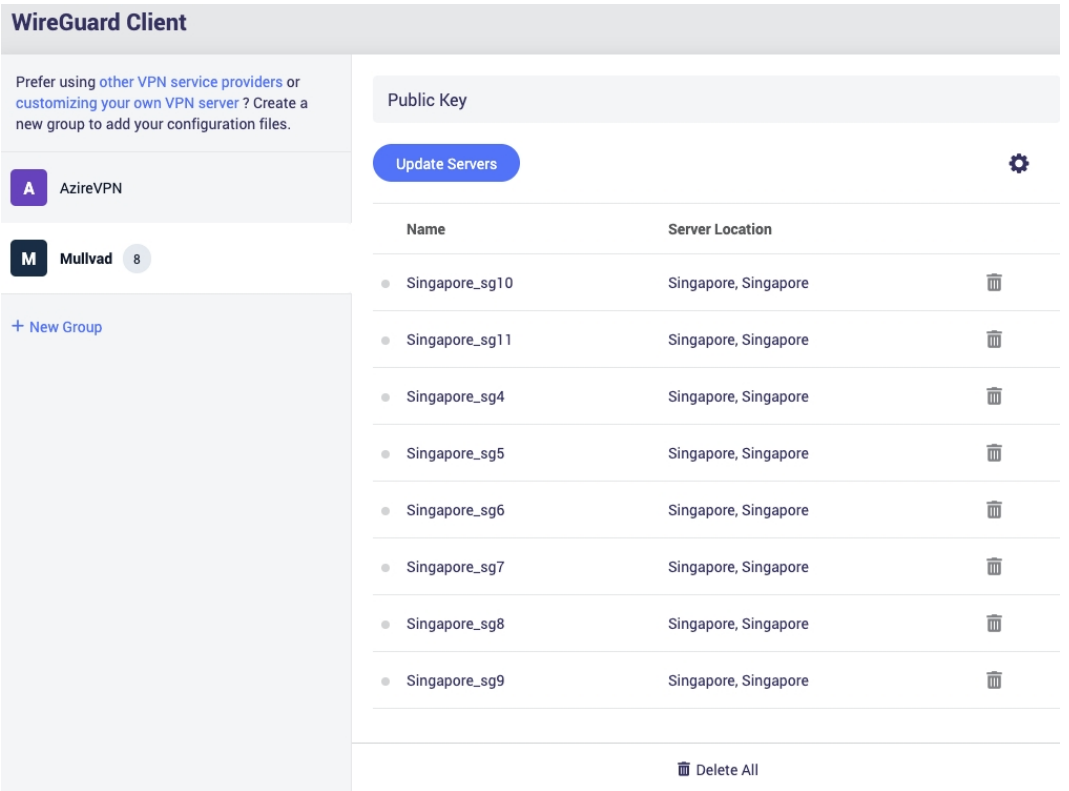


Pojawi się okno wyboru lokalizacji.

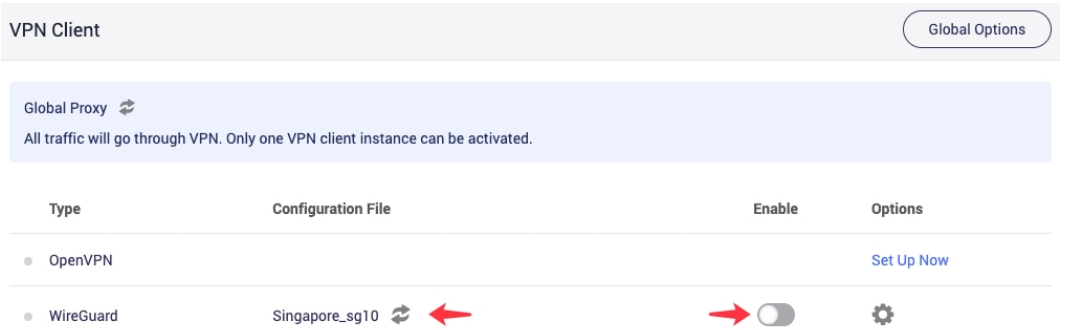


Następnie zostaną wygenerowane pliki konfiguracyjne serwera z wybranej lokalizacji.

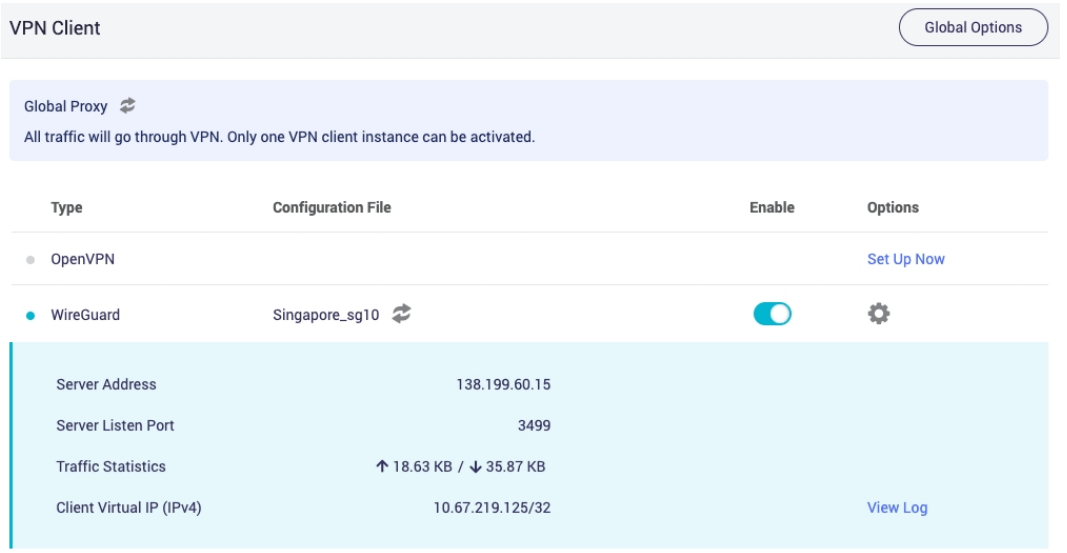
Pole **Public Key** zawiera klucz publiczny WireGuard przesyłany do serwera Mullvad. Jednocześnie możesz mieć do pięciu kluczy. Kluczami WireGuard można zarządzać na stronie konta Mullvad.



3. Przejdź do VPN Dashboard, aby włączyć połączenie.

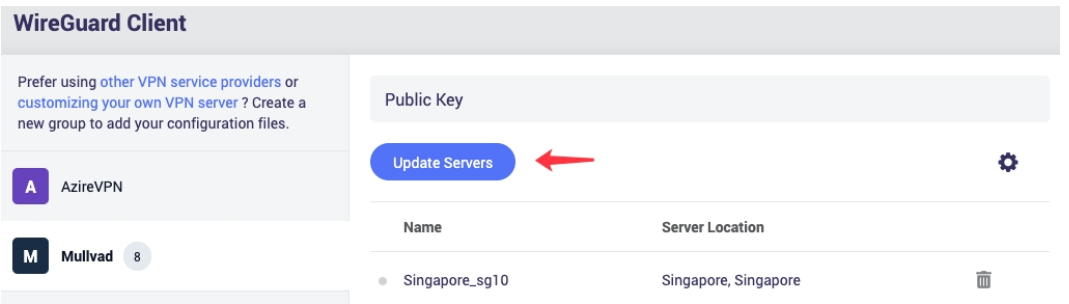


Po połączeniu powinny być widoczne Twój adres IP oraz liczba wysłanych i odebranych bajtów.



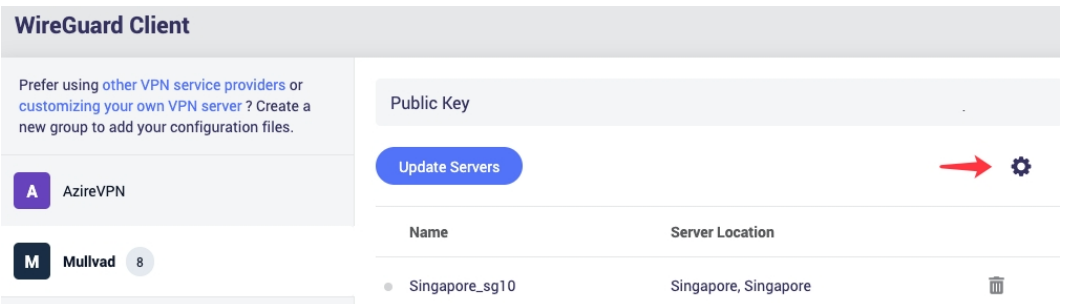
4. Zaktualizuj serwery.

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



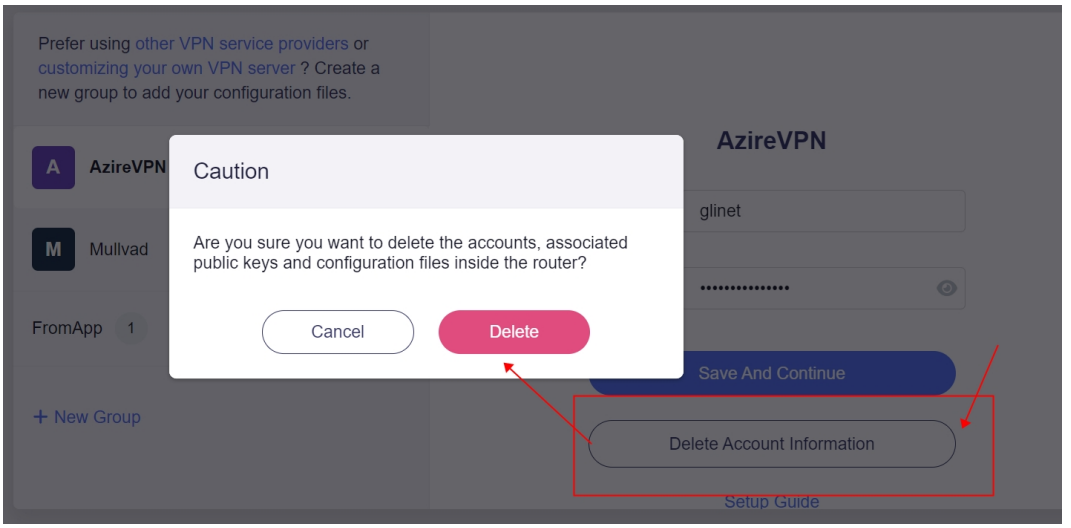
5. Zmiana danych dostępowych

   Kliknij ikonę koła zębatego, aby zmienić dane logowania.



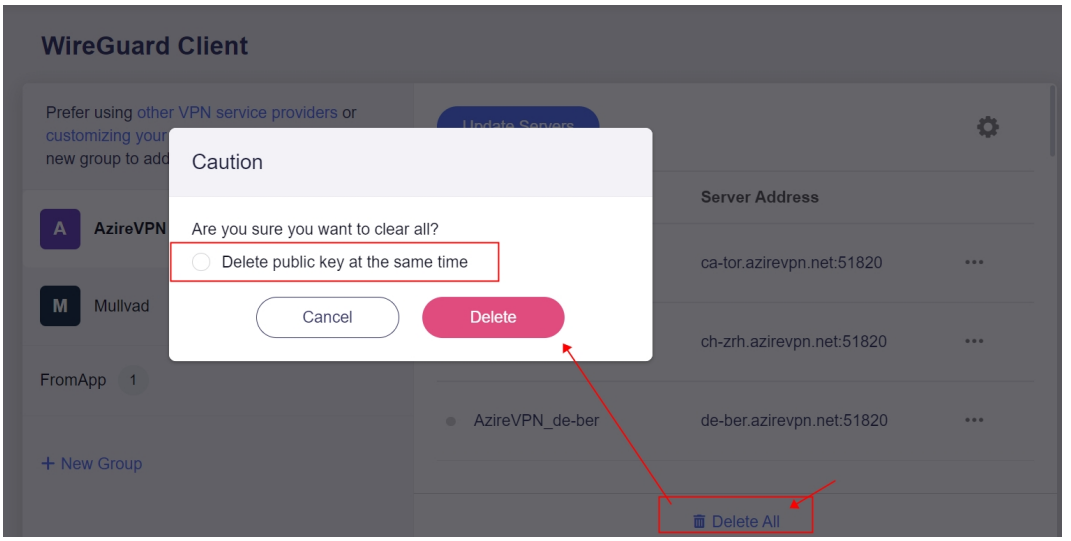
6. Usuwanie informacji o koncie

   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.

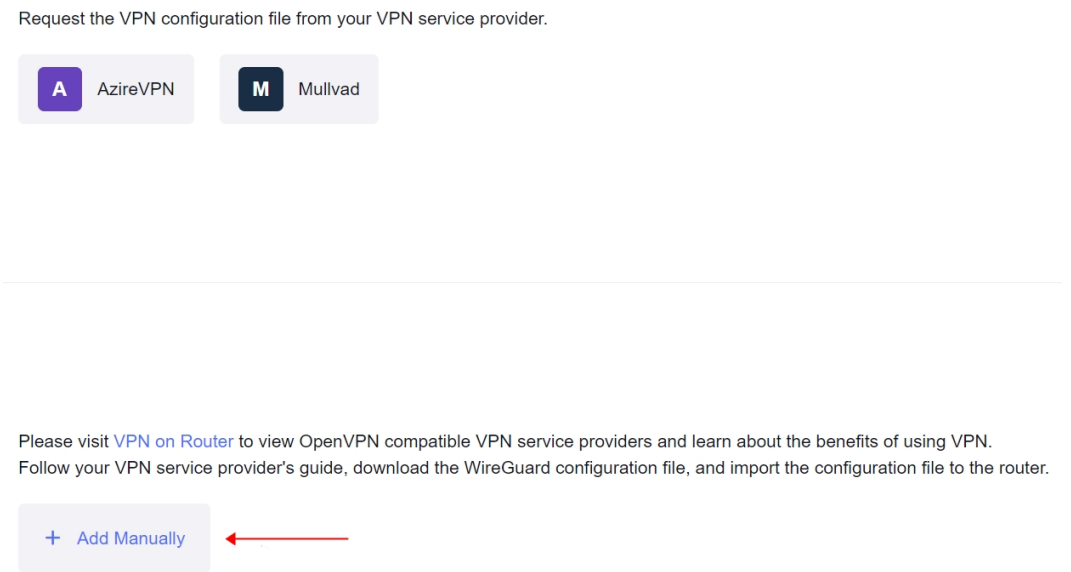


10.2.4 Ręczna konfiguracja klienta WireGuard (inni dostawcy)

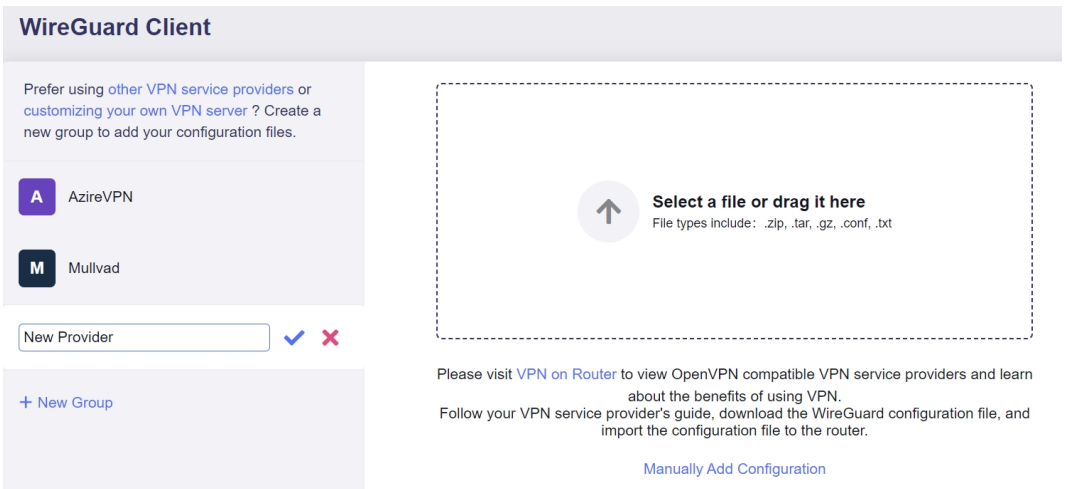
Jeśli Twój dostawca WireGuard nie jest zintegrowany z panelem administracyjnym, najpierw odwiedź jego oficjalną witrynę i pobierz plik konfiguracyjny. Następnie prześlij go do routera, aby skonfigurować klienta WireGuard. Jeśli nie wiesz, jak pobrać pliki konfiguracyjne, skorzystaj z tego poradnika lub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

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

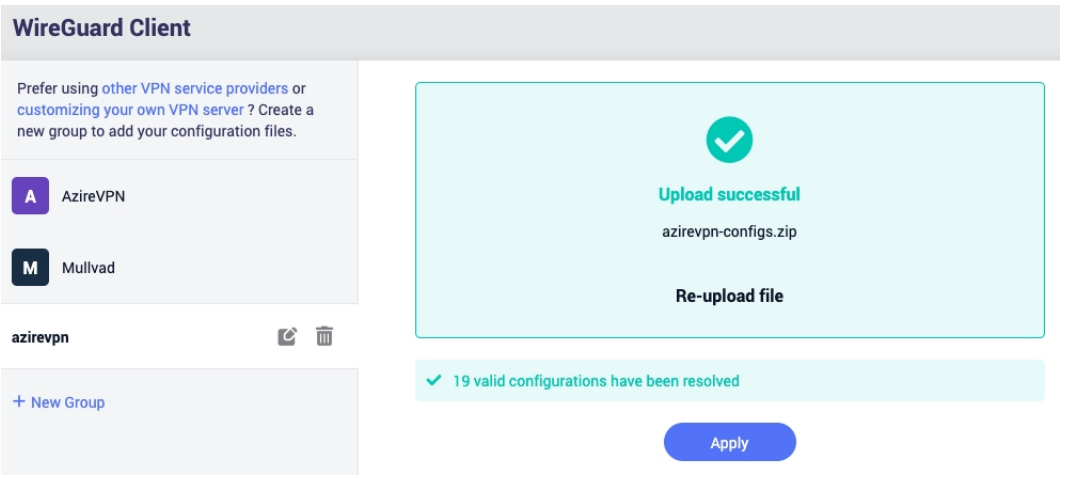
1. Zaloguj się do panelu administracyjnego routera i przejdź do **VPN** > **WireGuard Client** > **Add Manually**.



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

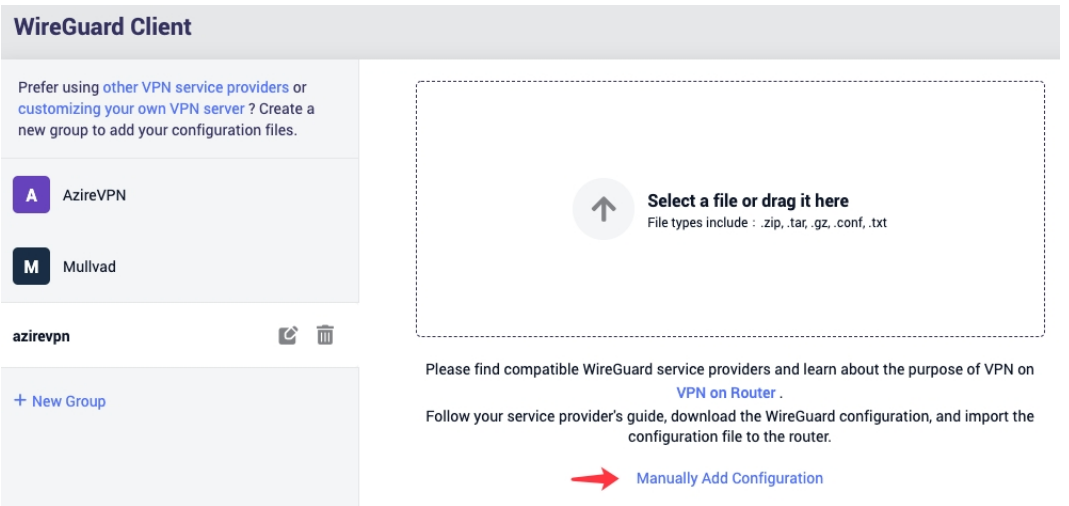


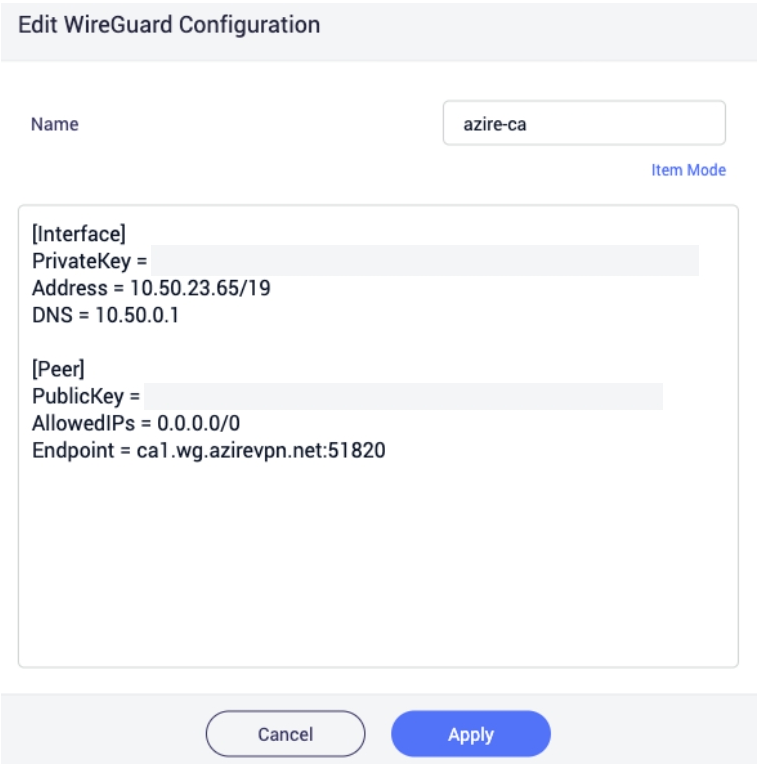
3. Kliknij obszar przesyłania, aby przesłać plik konfiguracyjny WireGuard (obsługiwane formaty: zip, tar, gz, conf, txt), i kliknij **Apply**.



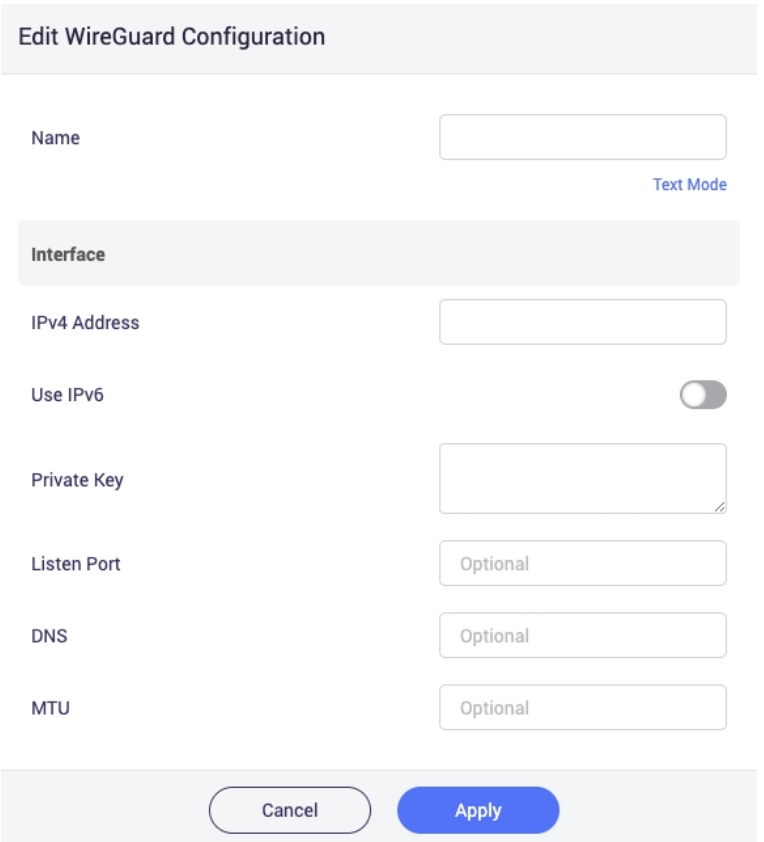
Jeśli prześlesz skompresowany plik zawierający wiele plików konfiguracyjnych, zostanie on automatycznie rozpakowany.

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

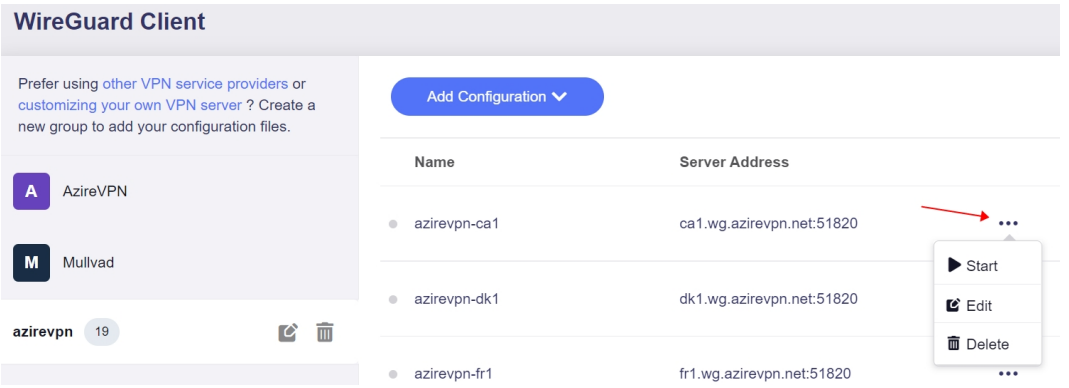




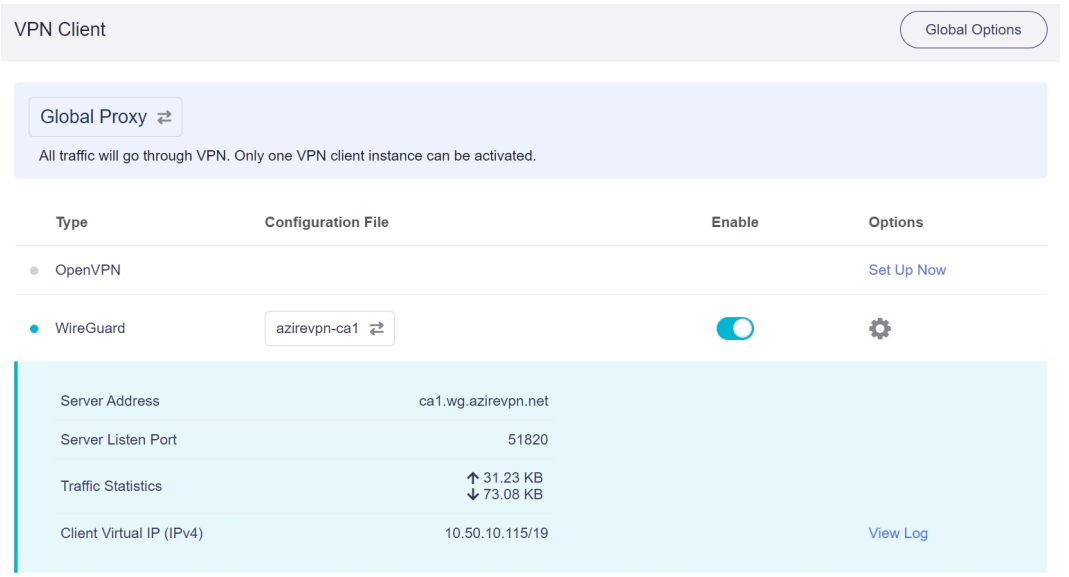
Aby sprawdzić poszczególne elementy, przełącz się do trybu Item, sprawdź szczegóły konfiguracji, a następnie kliknij **Apply**.



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

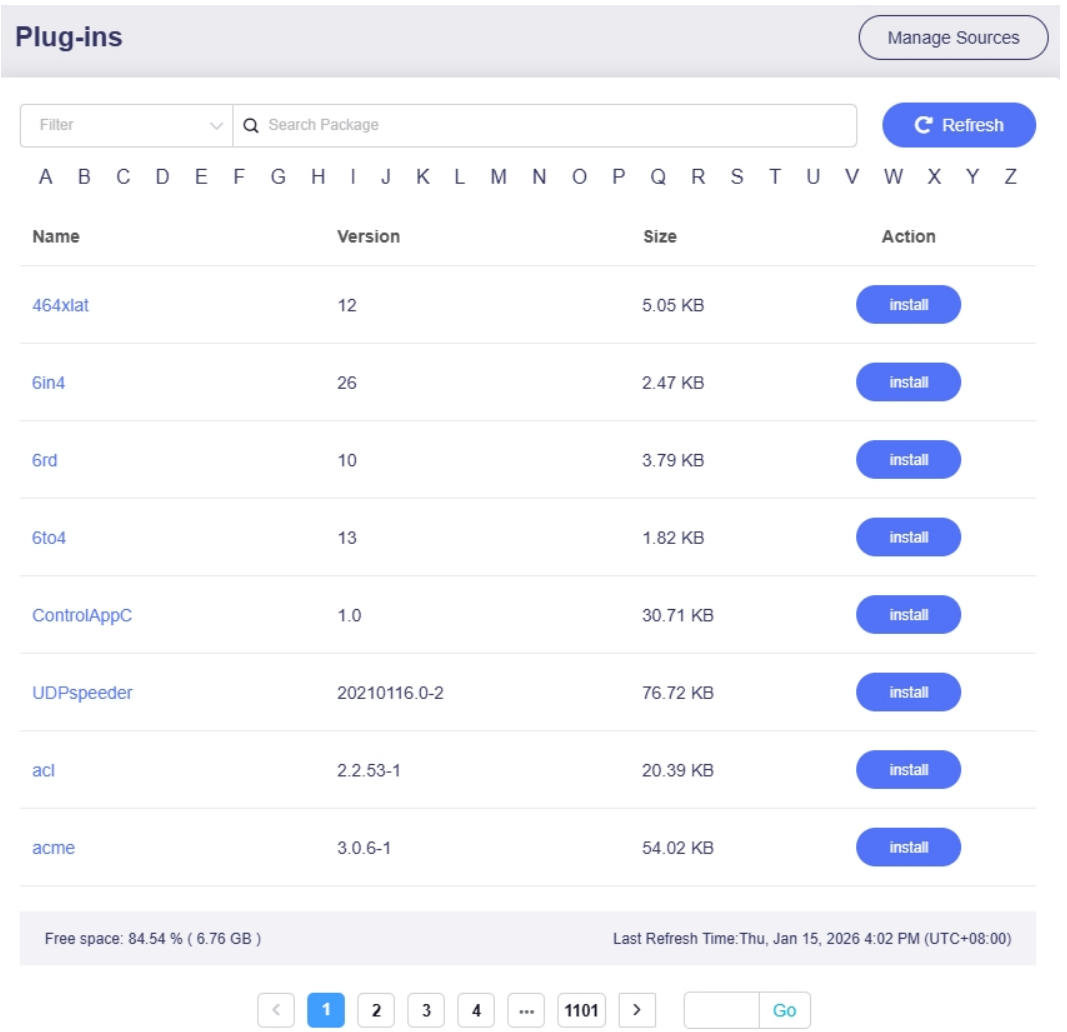
Aplikacje

W tym rozdziale przedstawiono aplikacje dostępne w routerach GL.iNet, np. wtyczki, Dynamic DNS i GoodCloud.

11.1 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:

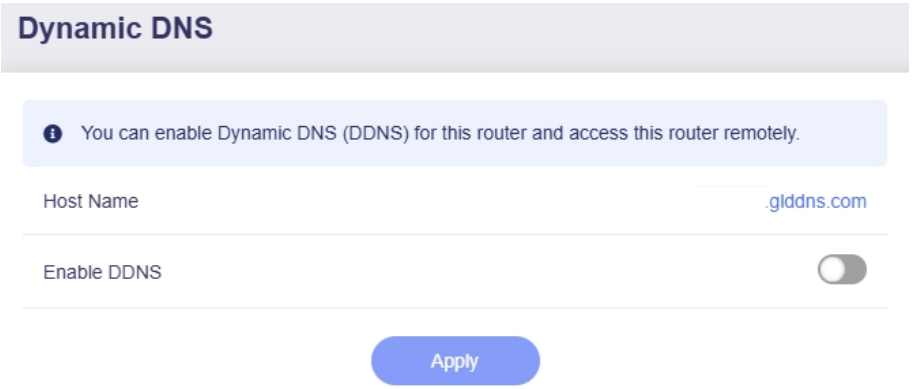
1. Nie zaleca się aktualizowania wtyczek zainstalowanych fabrycznie w oficjalnym oprogramowaniu GL.iNet, takich jak nginx itp.
2. Wtyczki zewnętrzne zainstalowane ręcznie przez użytkownika można aktualizować, jednak GL.iNet nie odpowiada za związane z nimi problemy z bezpieczeństwem. Pytania należy kierować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

11.2 Dynamiczny DNS

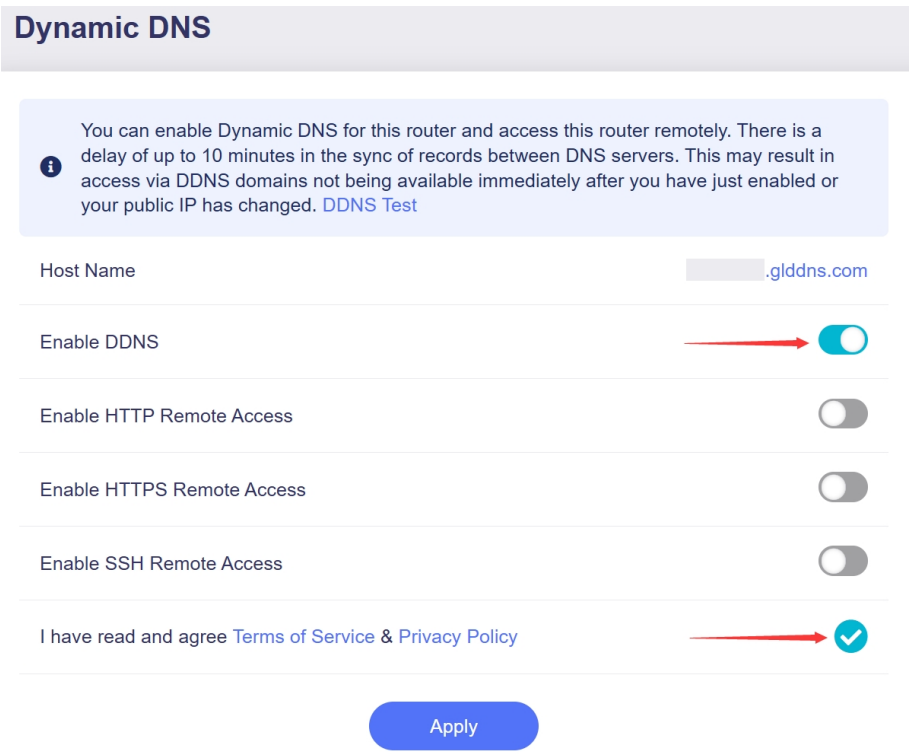
Dynamic Domain Name Service (DDNS, czyli dynamiczny DNS) to usługa mapująca nazwę domeny na dynamiczny adres IP urządzenia sieciowego. Dzięki niej można zdalnie uzyskiwać dostęp do routera. Ta funkcja wymaga publicznego adresu IP.

11.2.1 Włączanie DDNS

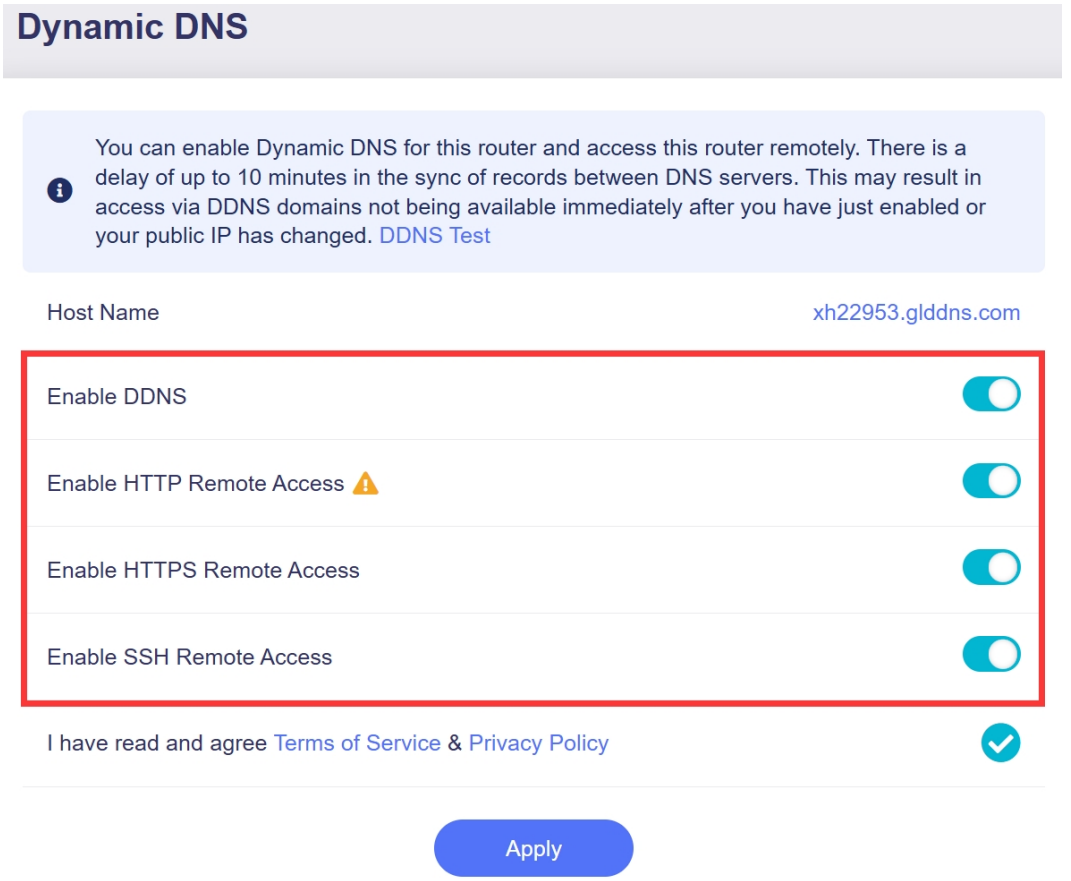
1. Zaloguj się do panelu administracyjnego routera i przejdź do **APPLICATIONS** > **Dynamic DNS**. Strona wygląda jak poniżej.



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



3. Jeśli potrzebujesz dostępu zdalnego, włącz wymagane usługi na tej stronie: **HTTP**, **HTTPS** i **SSH**.



Uwaga:

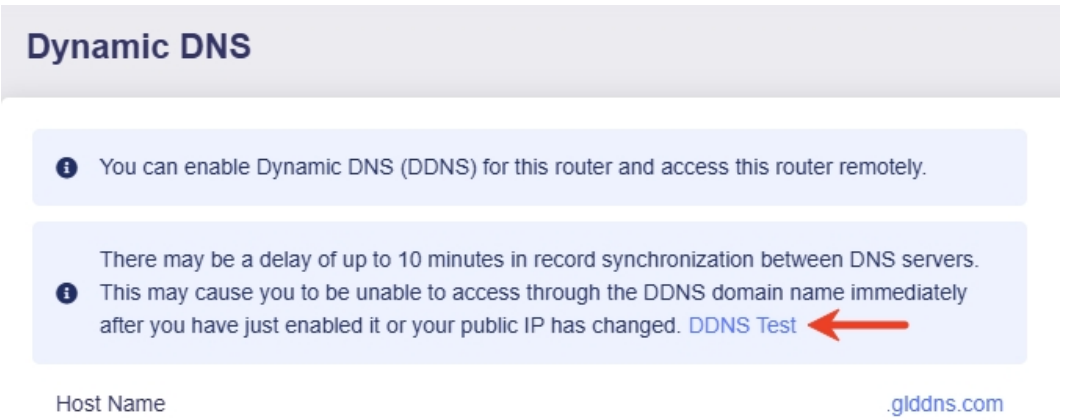
1. Synchronizacja rekordów między serwerami DNS może trwać do 10 minut. Może to uniemożliwić dostęp przez nazwę domeny DDNS bezpośrednio po włączeniu funkcji lub zmianie publicznego adresu IP.
2. Jeśli jednocześnie włączysz DDNS i klienta VPN, upewnij się, że opcja Services From GL.iNet Use VPN jest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

11.2.2 Sprawdzanie działania DDNS

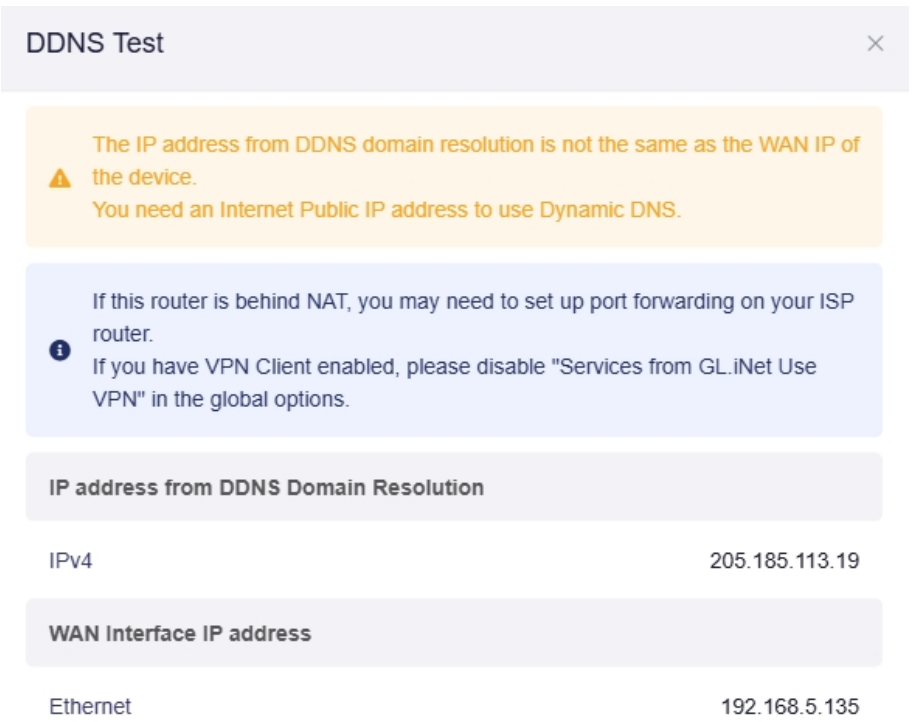
Działanie DDNS można sprawdzić za pomocą narzędzia testowego DDNS lub ręcznie, przy użyciu poleceń.

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.



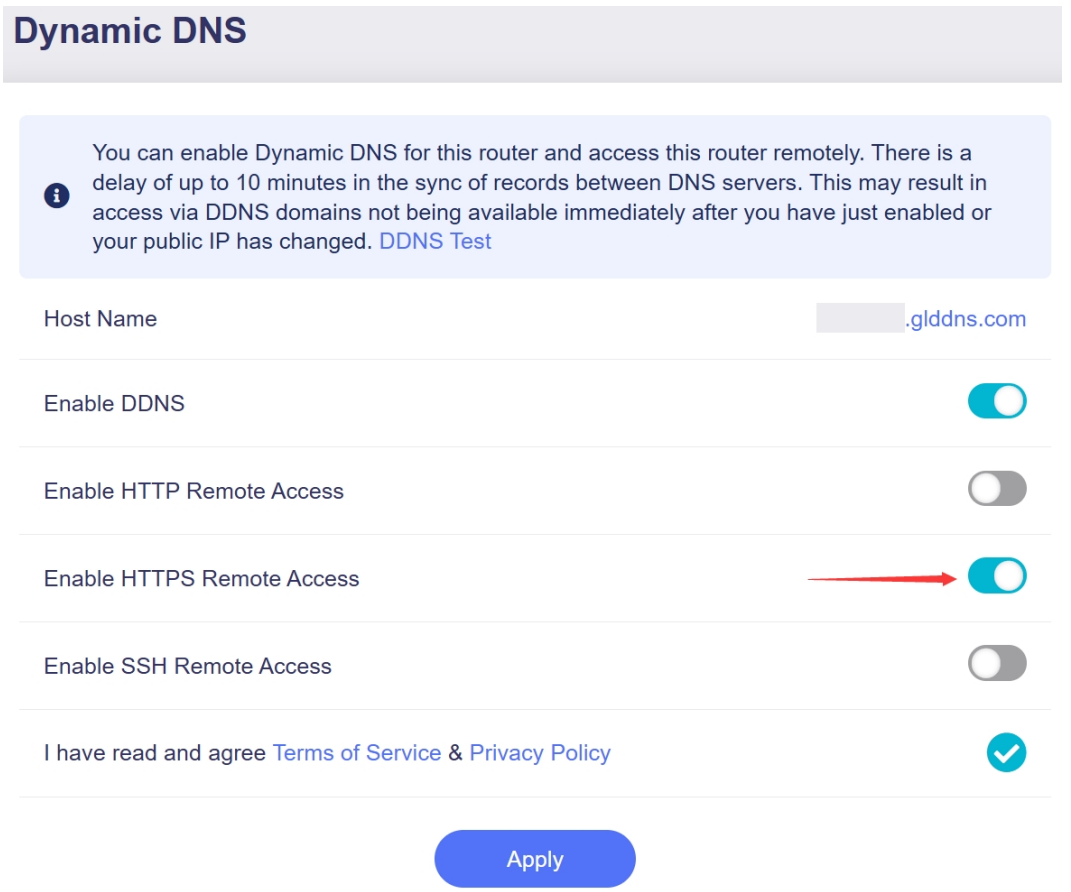
   - Zastąp „xxxxxxx.glddns.com” na powyższej ilustracji własną nazwą hosta.
   - „8.8.8.8” to serwer DNS Google. Użyj go lub zastąp innym adresem, a następnie naciśnij Enter.
2. Jeśli otrzymasz publiczny adres IP, taki jak „183.178.10.100” na powyższej ilustracji, domena DDNS została prawidłowo powiązana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

11.2.3 Zdalny dostęp przez HTTP

Do zdalnego dostępu przez HTTP 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 80**) na routerze nadrzędnym dla dostępu HTTP.

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

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



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

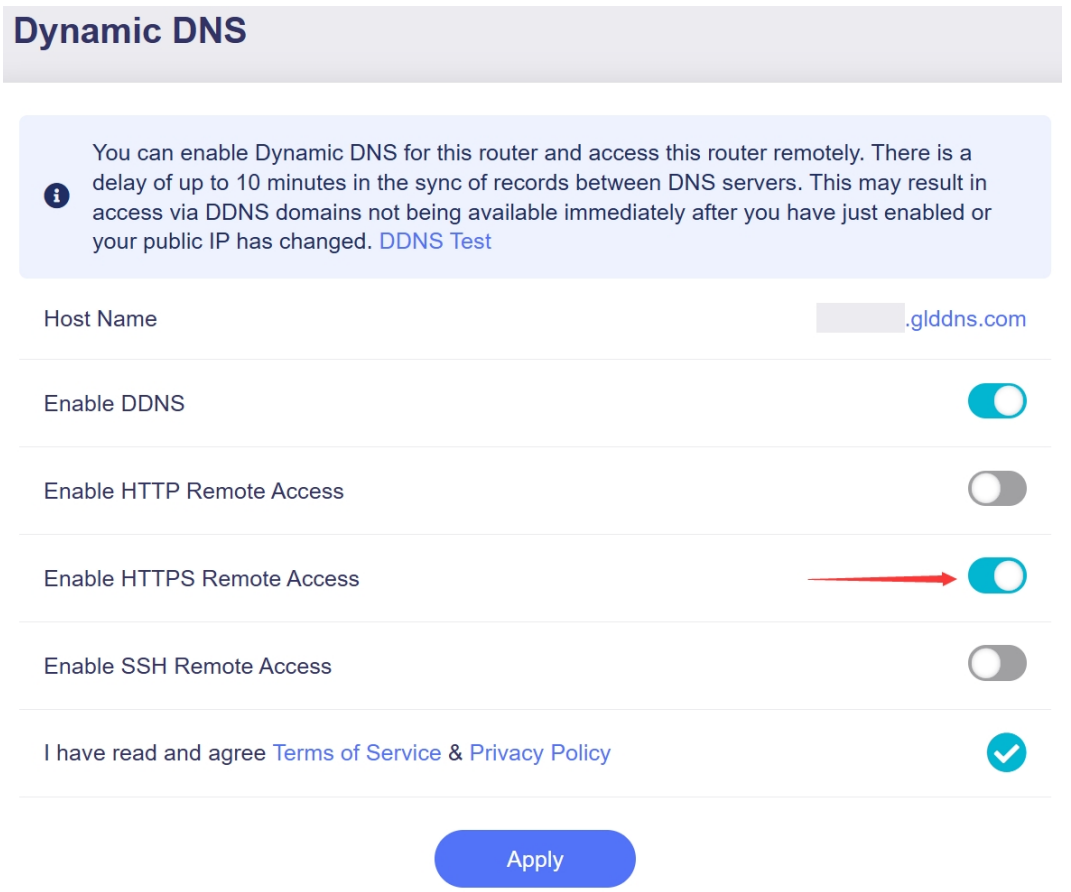
Uwaga: HTTP jest protokołem nieszyfrowanym. Wszystkie przesyłane dane, w tym dane logowania, są wysyłane jawnym tekstem, co stwarza zagrożenie dla bezpieczeństwa. Korzystaj ostrożnie ze zdalnego dostępu HTTP.

11.2.4 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.

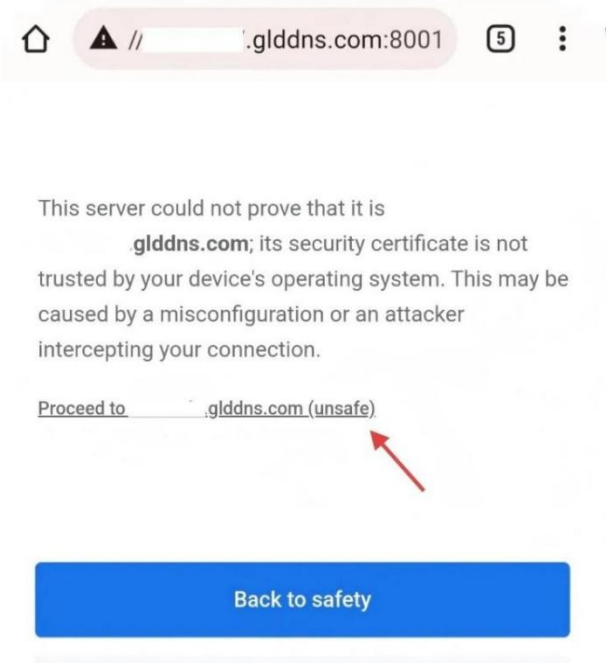
1. Na stronie Dynamic DNS włącz **Enable DDNS** i **HTTPS Remote Access**, zaakceptuj **Terms of Services & Privacy Policy**, a następnie kliknij **Apply**.



2. 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** .



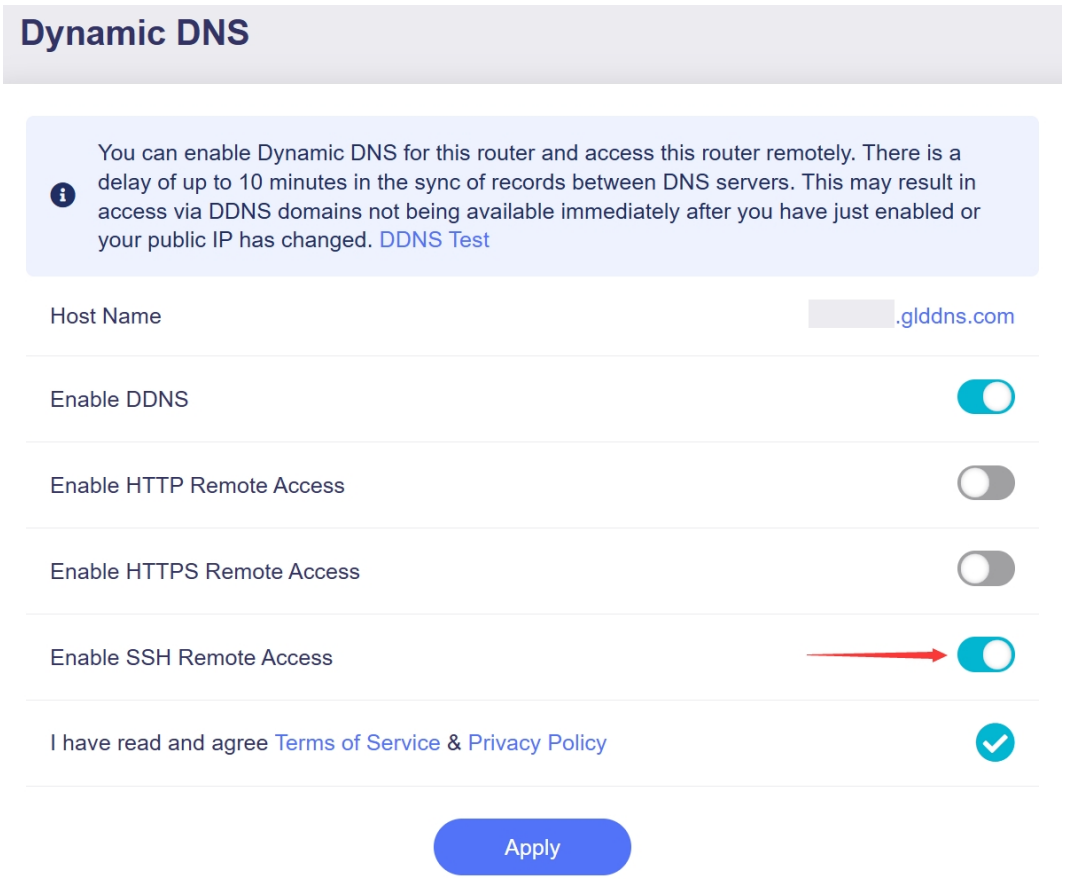
Możesz teraz uzyskiwać dostęp do panelu administracyjnego routera za pomocą nazwy hosta DDNS przez **HTTPS**.

11.2.5 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** i **SSH Remote Access**, zaakceptuj **Terms of Services & Privacy Policy**, a następnie 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).

11.3 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.

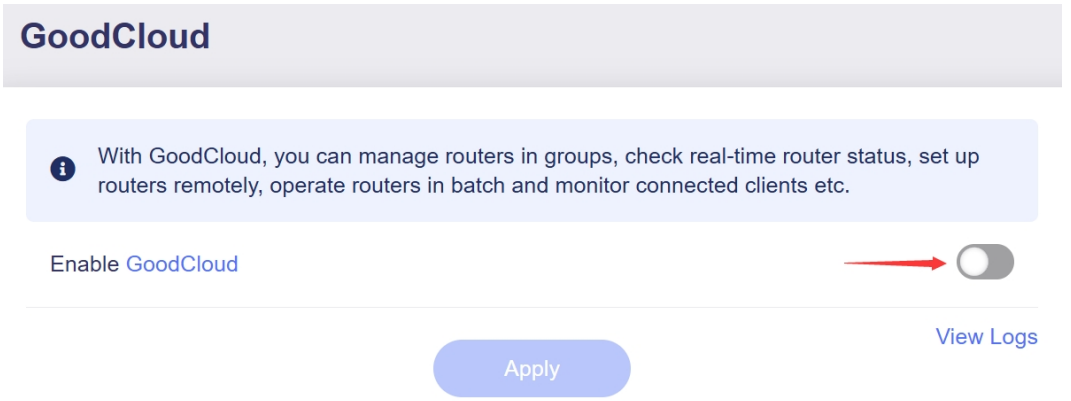
Dzięki GoodCloud możesz:

- 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

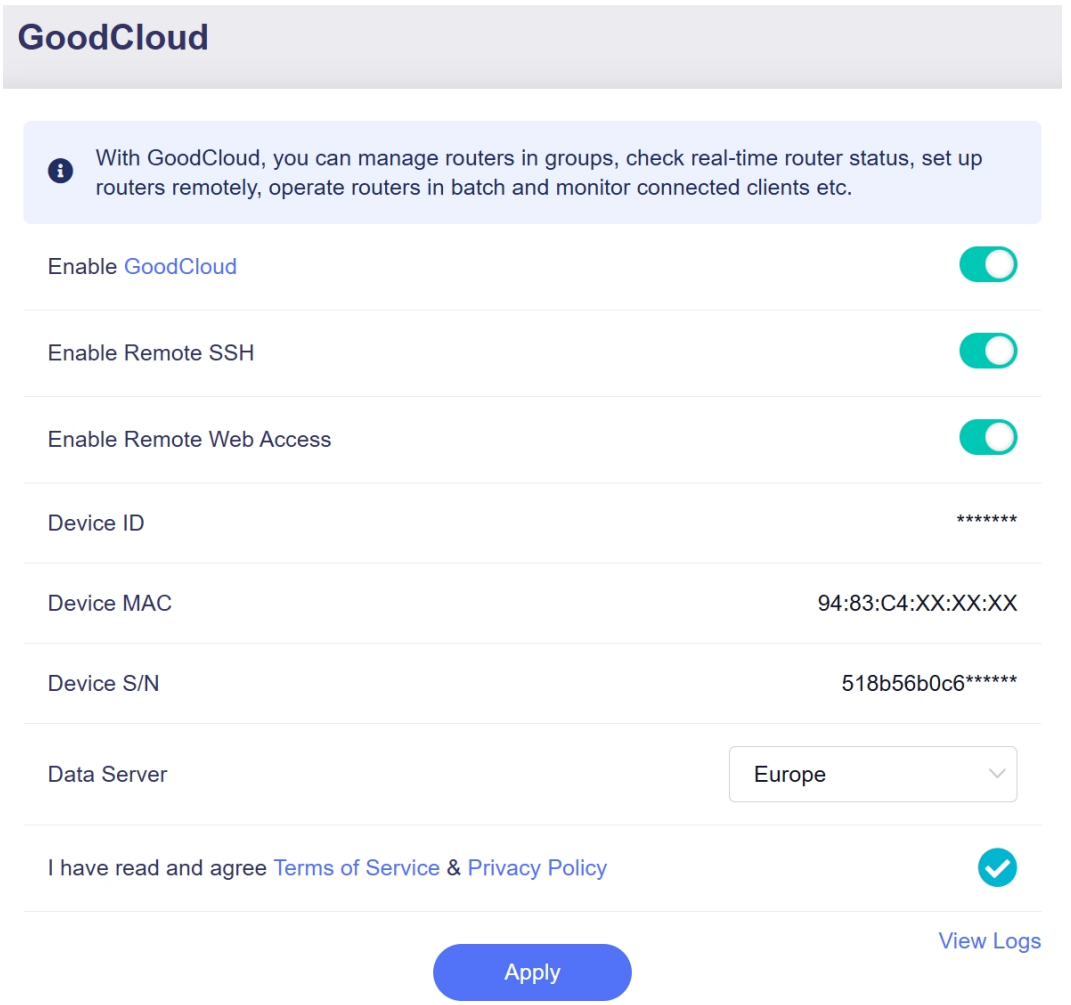
Niektóre funkcje są dostępne w planach Enterprise i VAR (Value Added Reseller). Szczegóły znajdziesz tutaj.

11.3.1 Włączanie GoodCloud

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

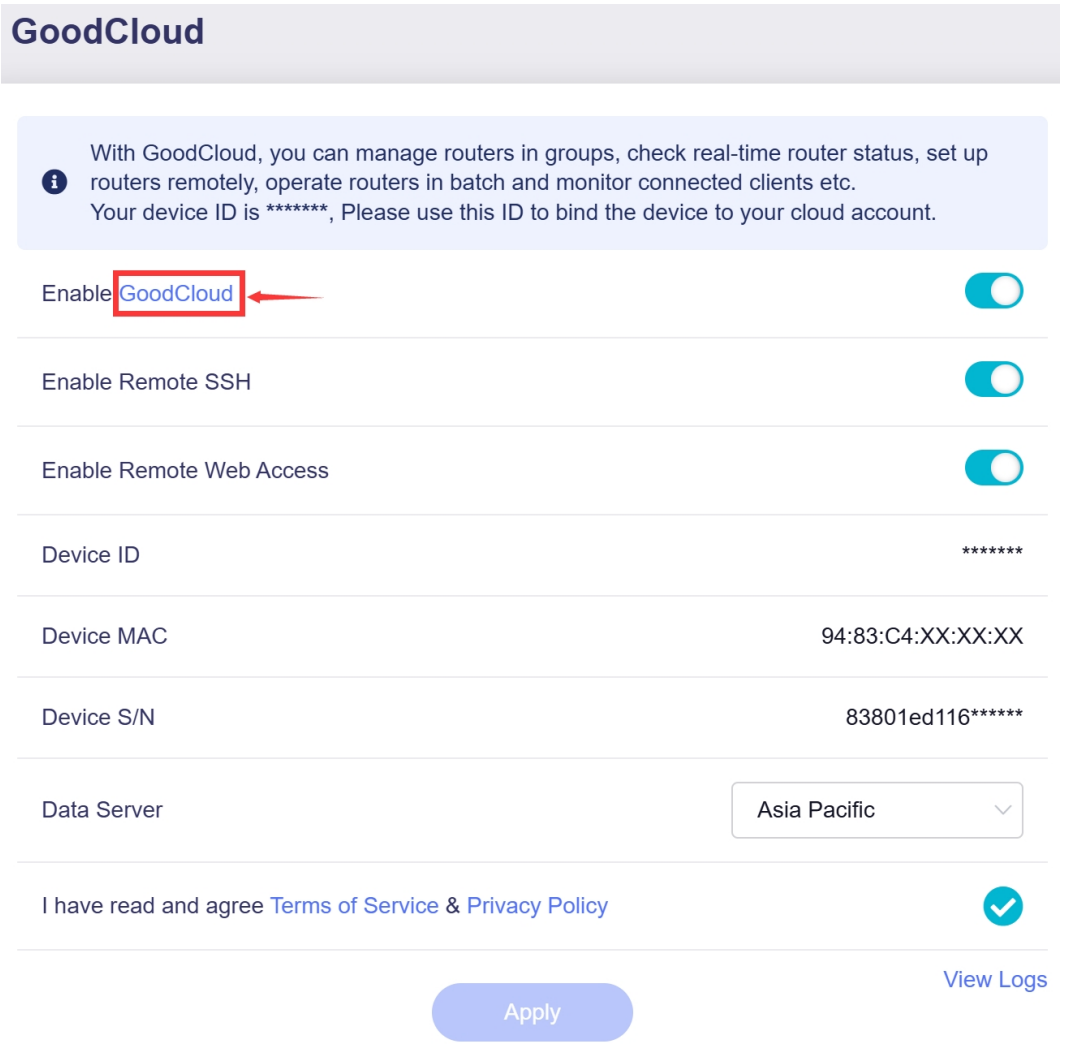


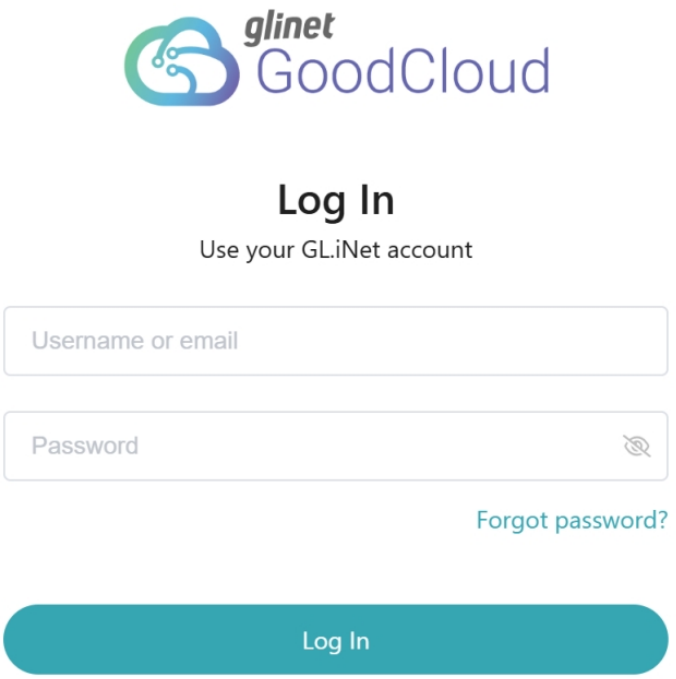
W razie potrzeby włącz **Remote SSH** i **Remote Web Access**, wybierz najbliższy serwer, przeczytaj i zaakceptuj **Terms of Service & Privacy Policy**, a następnie kliknij **Apply**.



- **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.

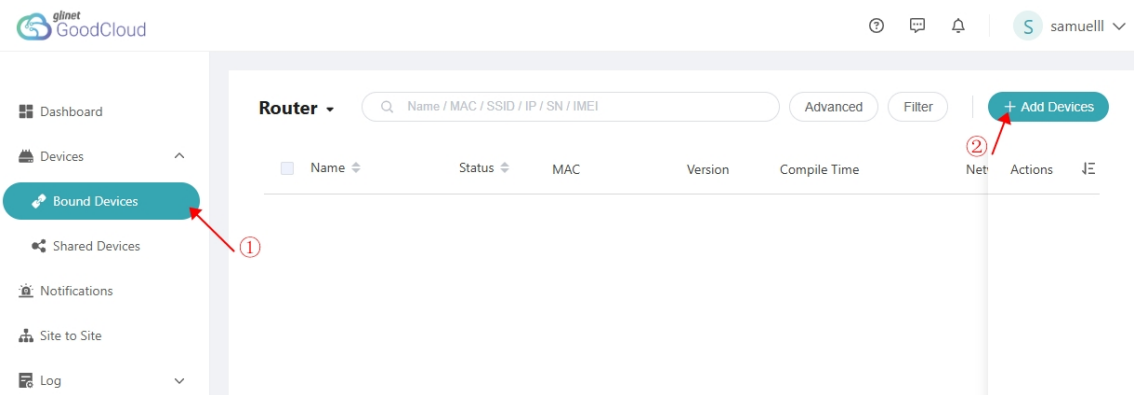




Wskazówki:

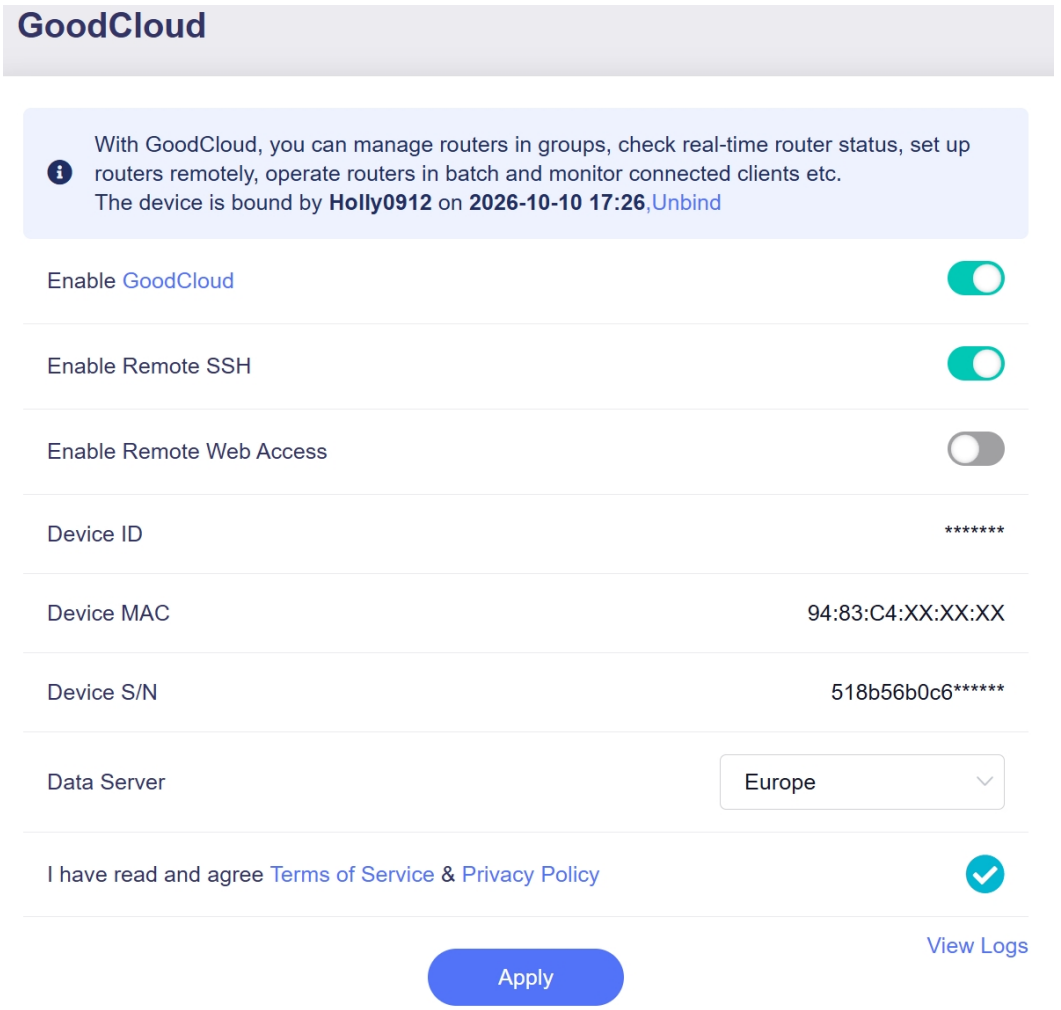
- Sposób powiązania z GoodCloud zależy od wersji oprogramowania.
- Jeśli nie otrzymasz wiadomości weryfikacyjnej, sprawdź folder spamu lub spróbuj później. Aby uzyskać dodatkową pomoc, napisz na support@gl-inet.com.

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.

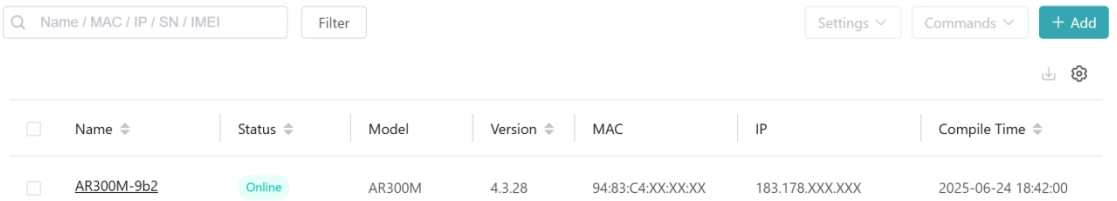
4. Po pomyślnym powiązaniu wróć do panelu administracyjnego routera i przejdź do **APPLICATIONS** > **GoodCloud**. Strona wyświetla szczegóły powiązania, w tym nazwę użytkownika i czas powiązania.


GoodCloud
With GoodCloud, you can manage routers in groups, check real-time router status, set up routers remotely, operate routers in batch and monitor connected clients etc.
The device is bound by Holly0912 on 2026-10-10 17:26,Unbind
Enable GoodCloud
Enable Remote SSH
Enable Remote Web Access
Device ID
****
Device MAC
94:83:C4:XX:XX:XX
Device S/N
518b56b0c6******
Data Server
Europe
I have read and agree Terms of Service & Privacy Policy
View Logs
Apply

11.3.2 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.

AR300M-9b2 Online

Remote GUI | Remote SSH | Reboot Device

Basic Info

Refresh



AR300M

Network Mode	Version	MAC Address	IP
Router	4.3.28	94:83:C4:XX:XX:XX	183.178.XXX.XXX
SN	**Memory Usage**	**Compile Time**	**Up Time**
518b**********	31%	2025-06-24 18:42:00	0 days 0 hrs 44 mins

Statistical Data

Refresh

Network Latency

Retest

Poor

241.61 ms Latency | 2.27 ms Jitter | 0 % Packet Loss

Device Status History

More



Network | Clients List | Share | Cellular Health

Internet

Refresh

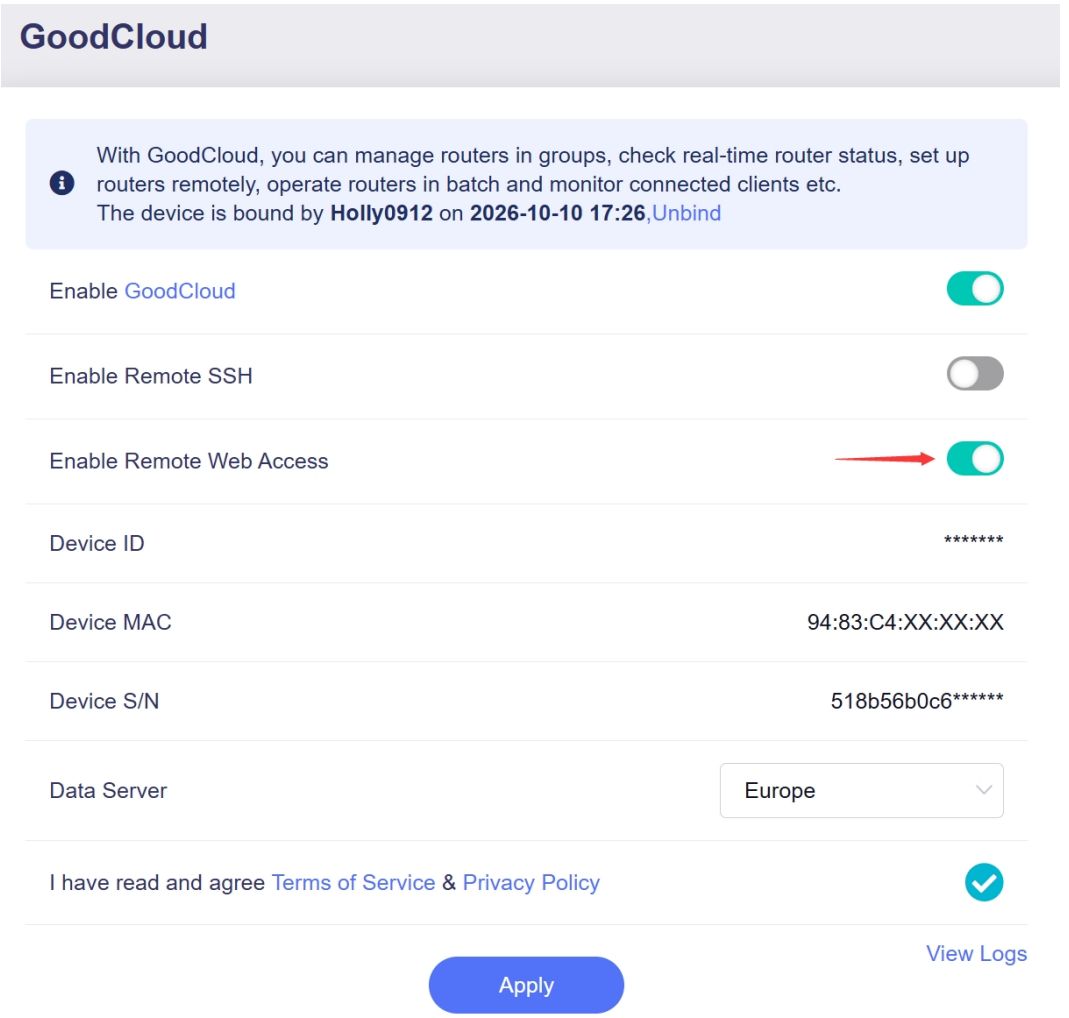
Ethernet1 More
✓ Connected
IP Address 10.100.210.196/22
Protocol DHCP

Repeater More
Disabled
IP Address --
SSID --

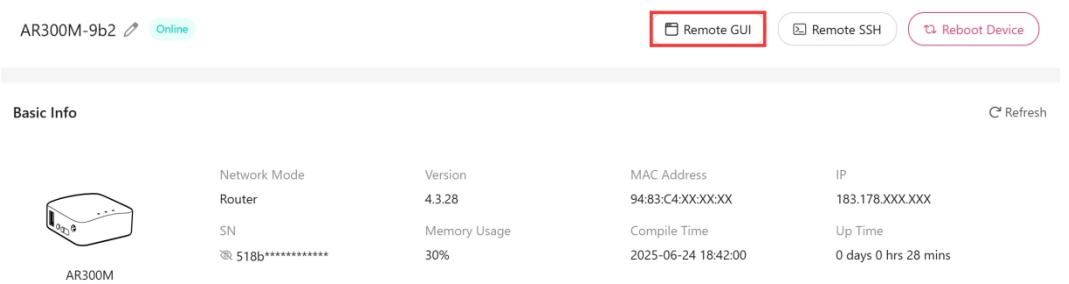
Tethering More
Disabled
IP Address --
Device List Details

Zdalny dostęp przez przeglądarkę

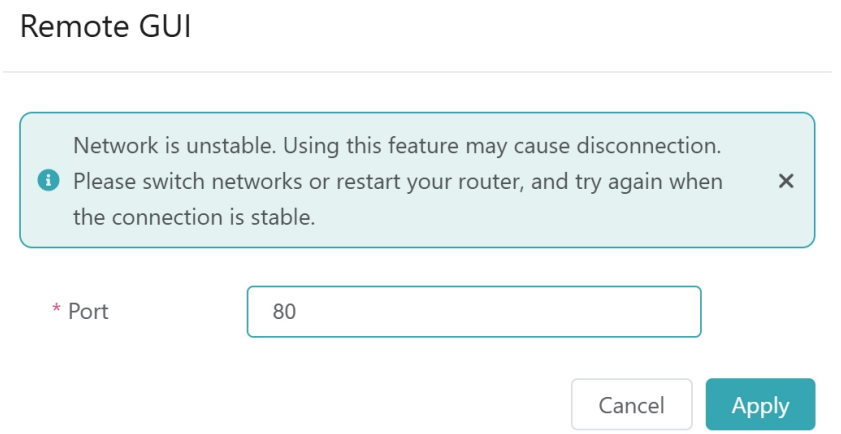
1. Zaloguj się do panelu administracyjnego routera, przejdź do **APPLICATIONS** > **GoodCloud**, włącz **Remote Web Access**, a następnie kliknij **Apply**.



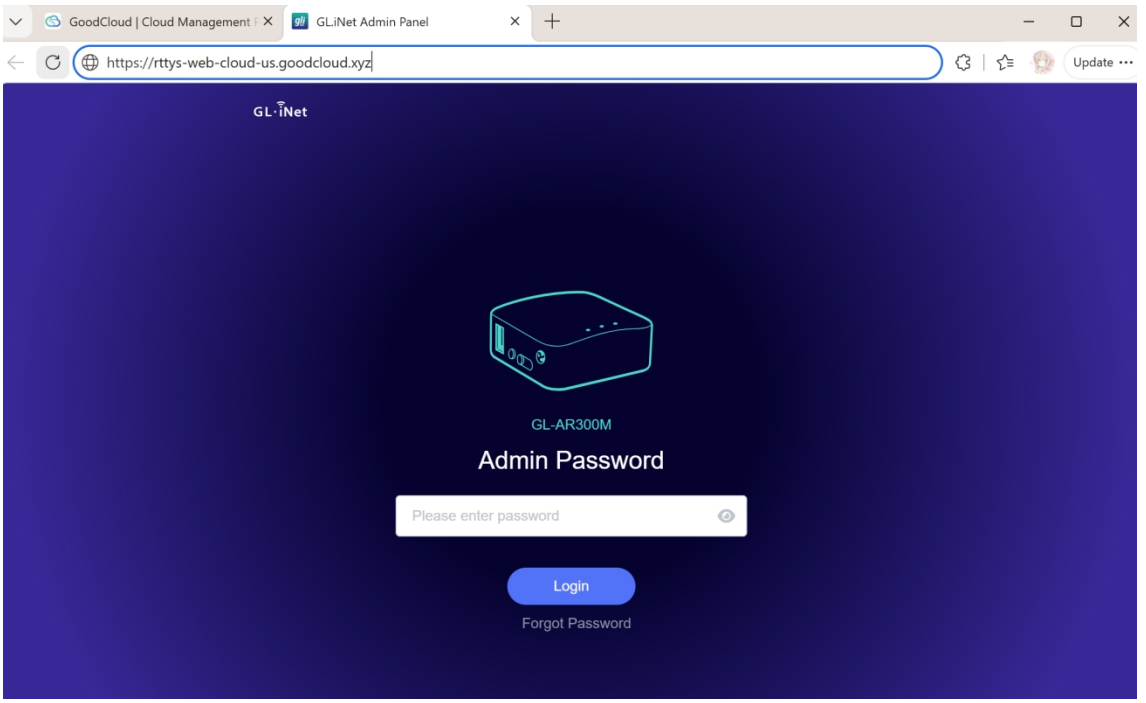
2. Zaloguj się na platformie GoodCloud i przejdź do **Devices** > **Bound Devices**. Kliknij urządzenie, do którego chcesz uzyskać dostęp, aby otworzyć stronę jego szczegółów.
3. Na stronie szczegółów urządzenia kliknij przycisk **Remote GUI** w prawym górnym rogu.



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**.

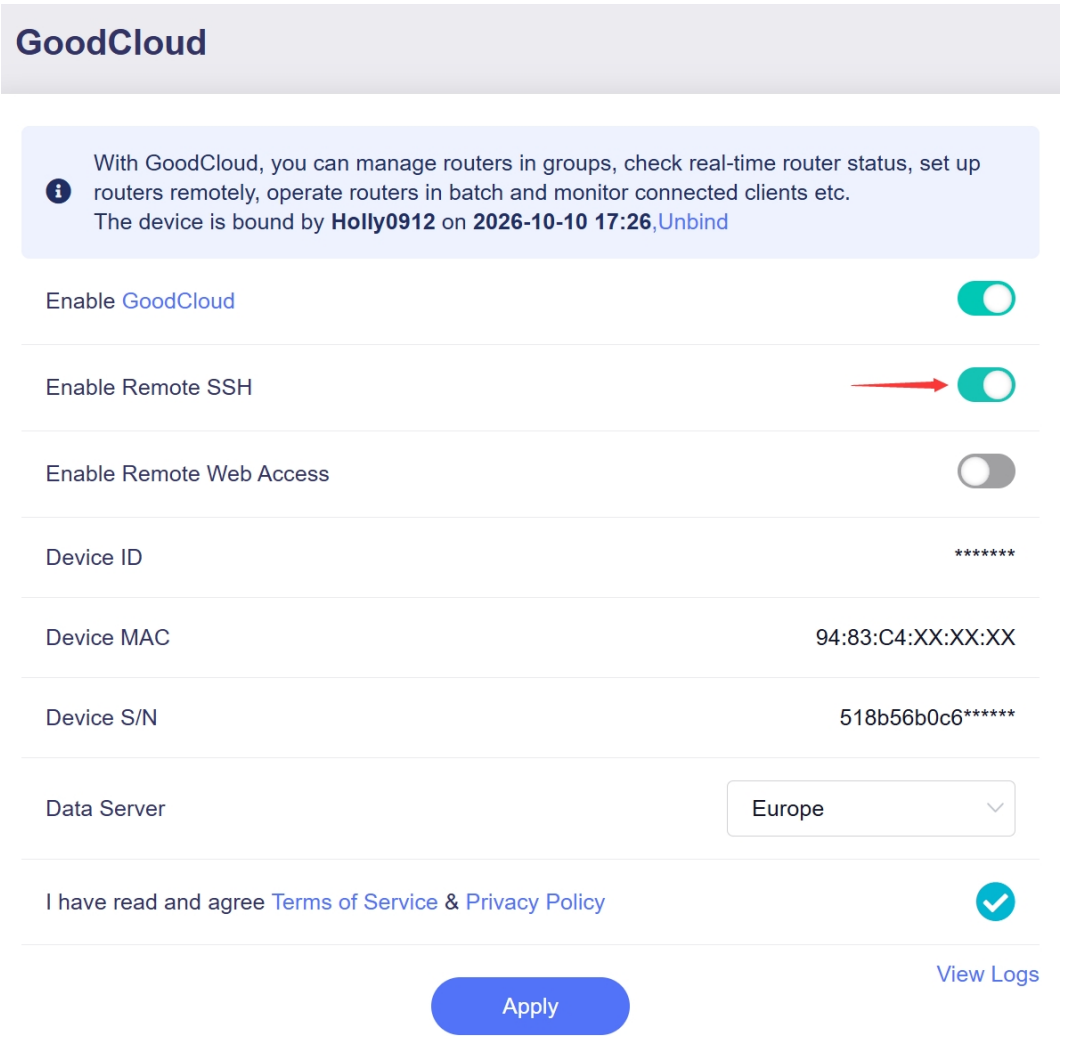


5. Otworzy się strona logowania routera. Wprowadź hasło administratora, aby uzyskać zdalny dostęp do panelu administracyjnego routera.

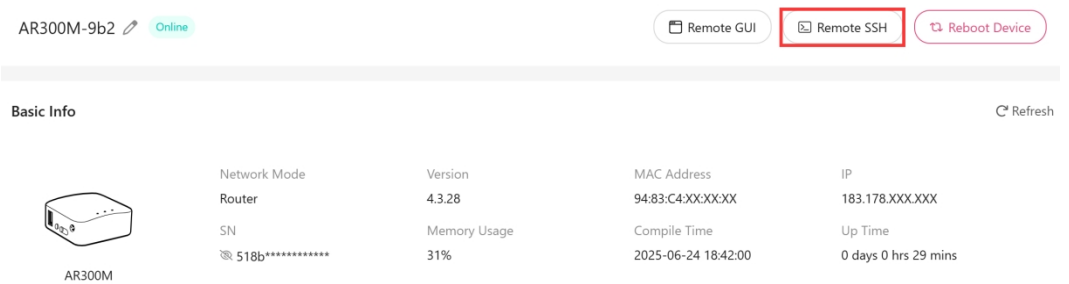


Zdalny dostęp SSH

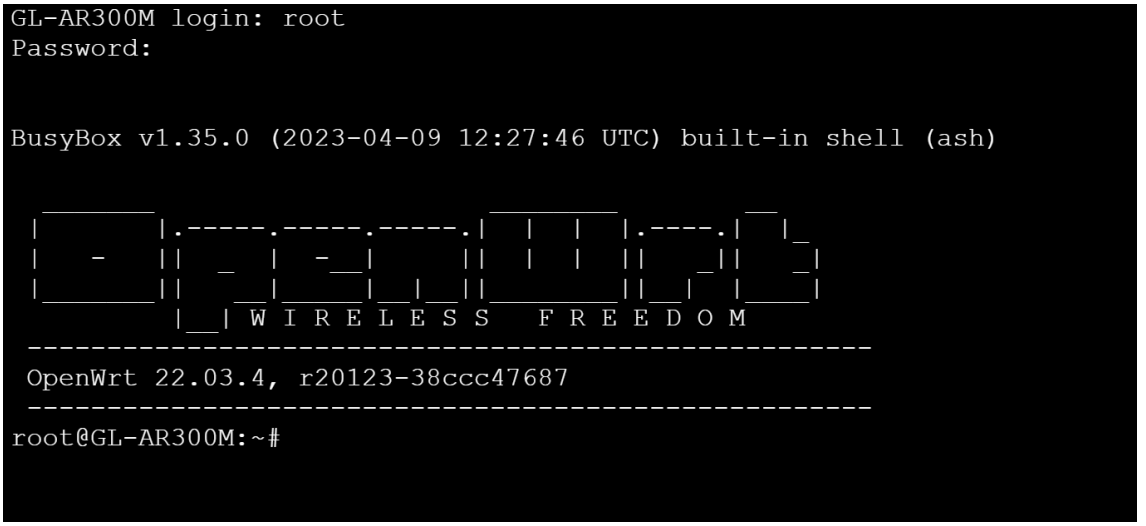
1. Zaloguj się do panelu administracyjnego routera, przejdź do **APPLICATIONS** > **GoodCloud**, włącz **Remote SSH**, a następnie kliknij **Apply**.



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.

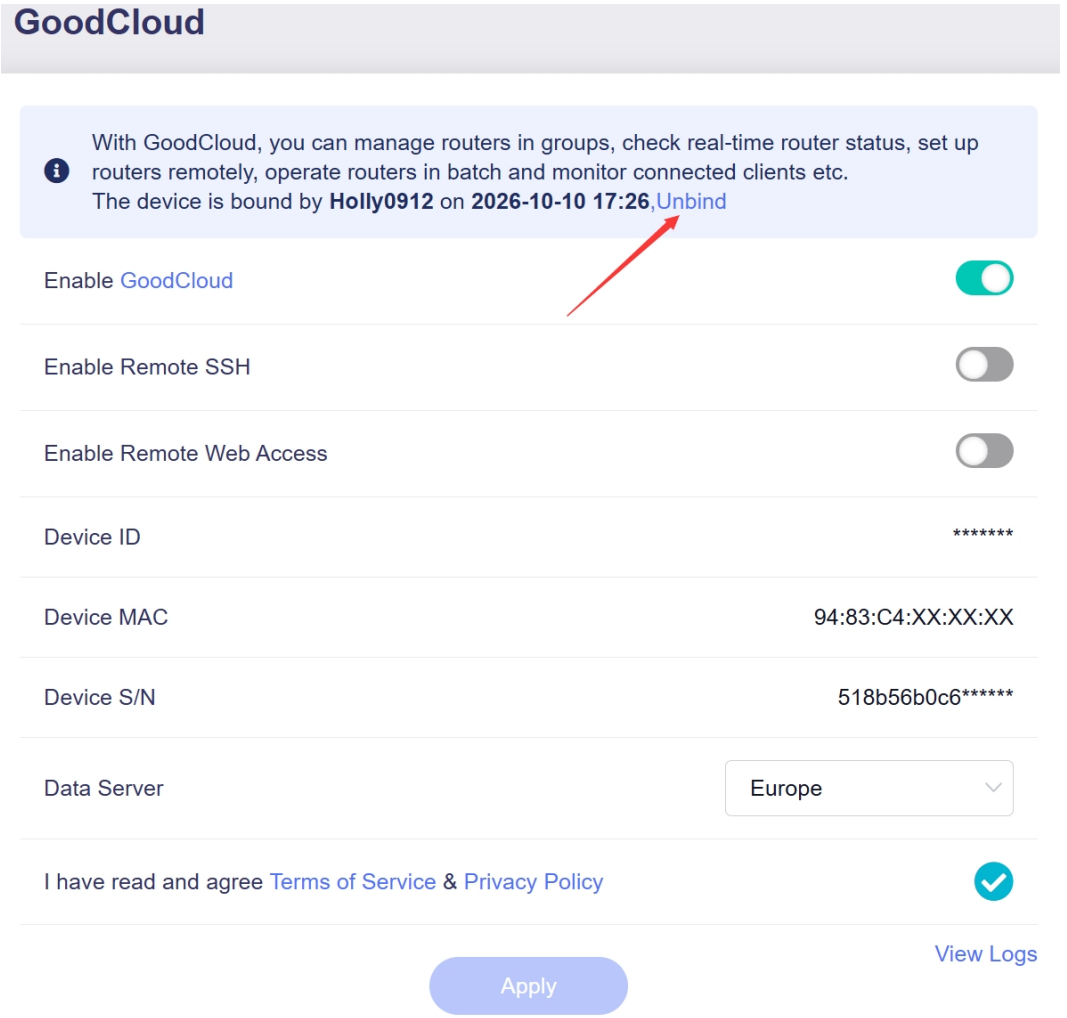


4. Zaloguj się jako **root** i wprowadź hasło, aby uzyskać dostęp do terminala routera.

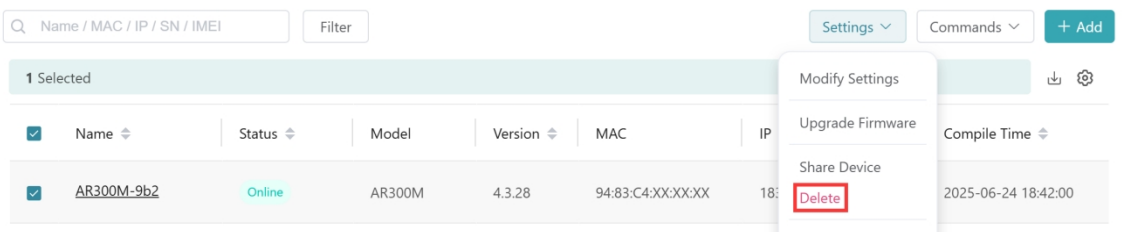


11.3.3 Usuwanie powiązania urządzenia

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.



Rozdział 12

Sieć

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

12.1 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).

12.1.1 Przekierowanie portów

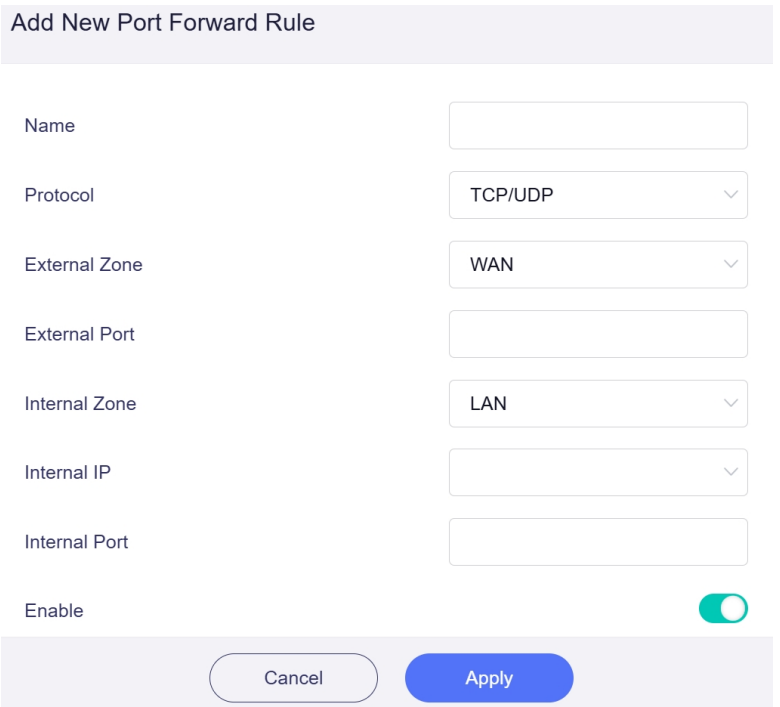
Przekierowanie portów umożliwia komputerom zdalnym łączenie się z komputerem lokalnym lub serwerem za zaporą LAN (np. serwerem WWW lub FTP).

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**.

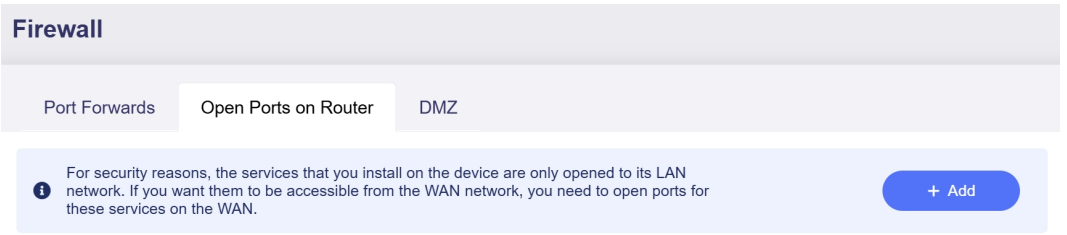


- **Name**: nazwa reguły określana przez użytkownika.
- **Protocol**: używany protokół. Możesz wybrać TCP, UDP lub oba protokoły.
- **External Zone**: dostępne opcje to WAN, WireGuard Client, WireGuard Server, OpenVPN Client, OpenVPN Server, LAN i Guest.
- **External Port**: numer lub numery portów zewnętrznych. 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.

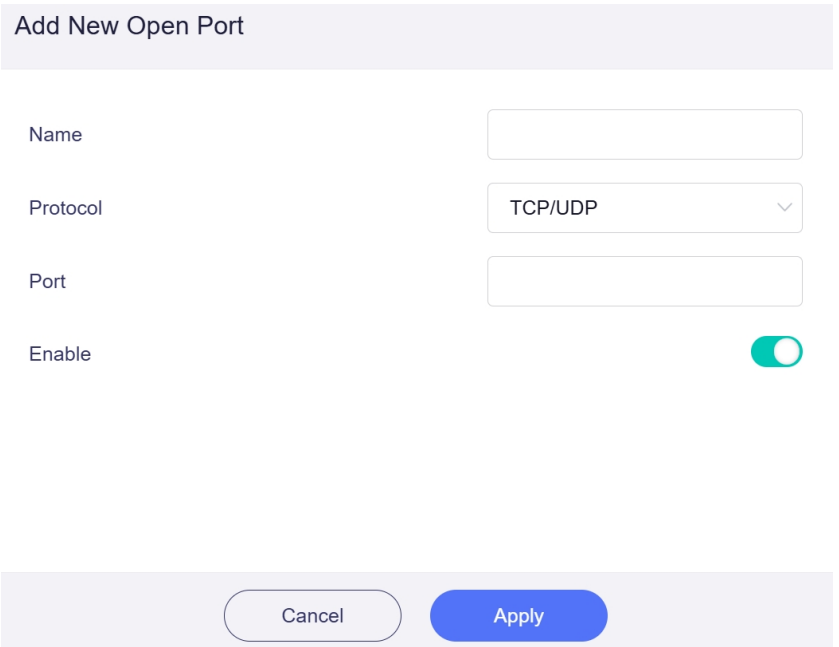
12.1.2 Otwieranie portów routera

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.



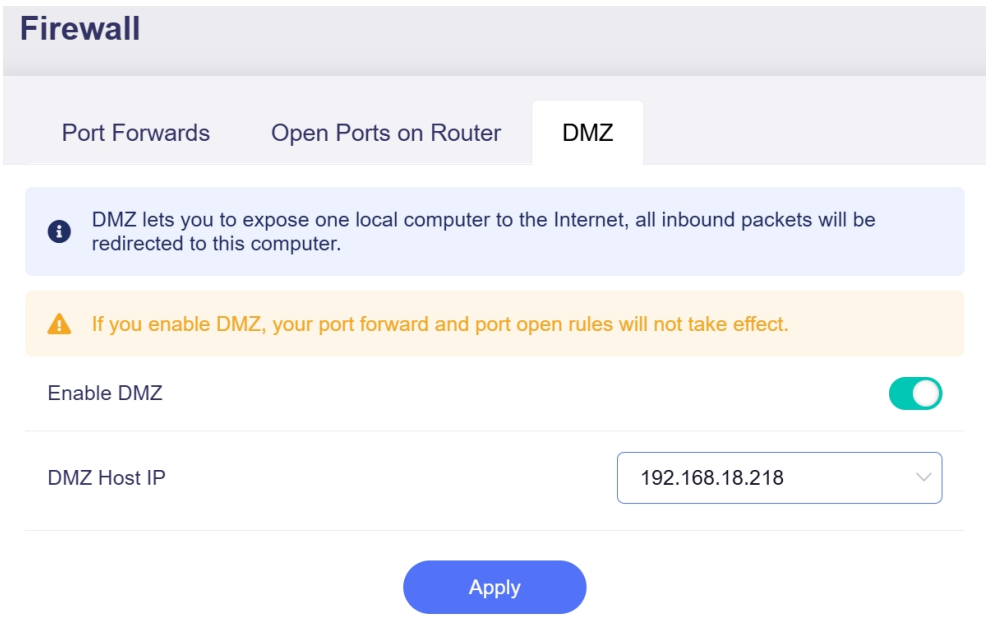
- **Name**: nazwa reguły określana przez użytkownika.
- **Protocol**: używany protokół. Możesz wybrać TCP, UDP lub oba protokoły.
- **Port**: numer portu, który chcesz otworzyć.
- **Enable**: włącza lub wyłącza tę regułę.

12.1.3 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.



12.2 Multi-WAN

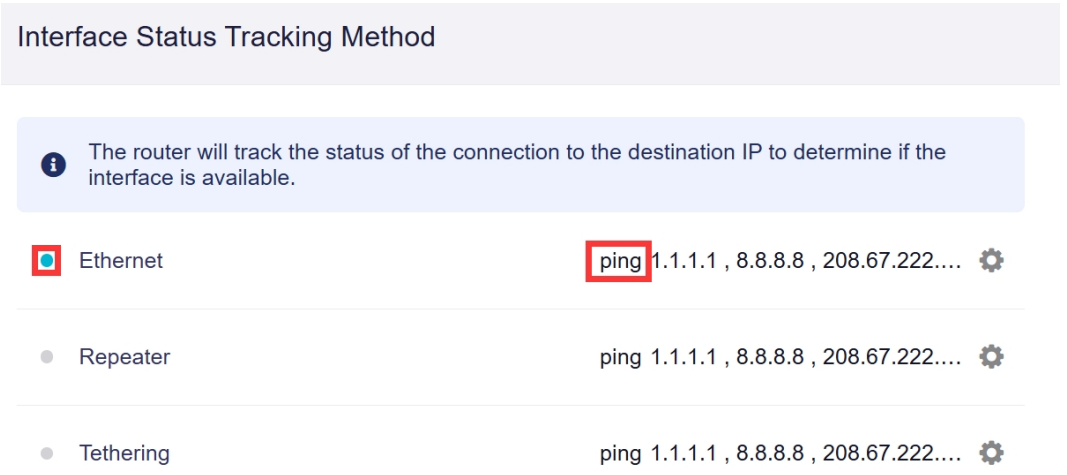
Multi-WAN umożliwia jednoczesne korzystanie z wielu sposobów dostępu do Internetu i konfigurowanie różnych połączeń na routerze. Oferuje dwa tryby pracy:

- **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.

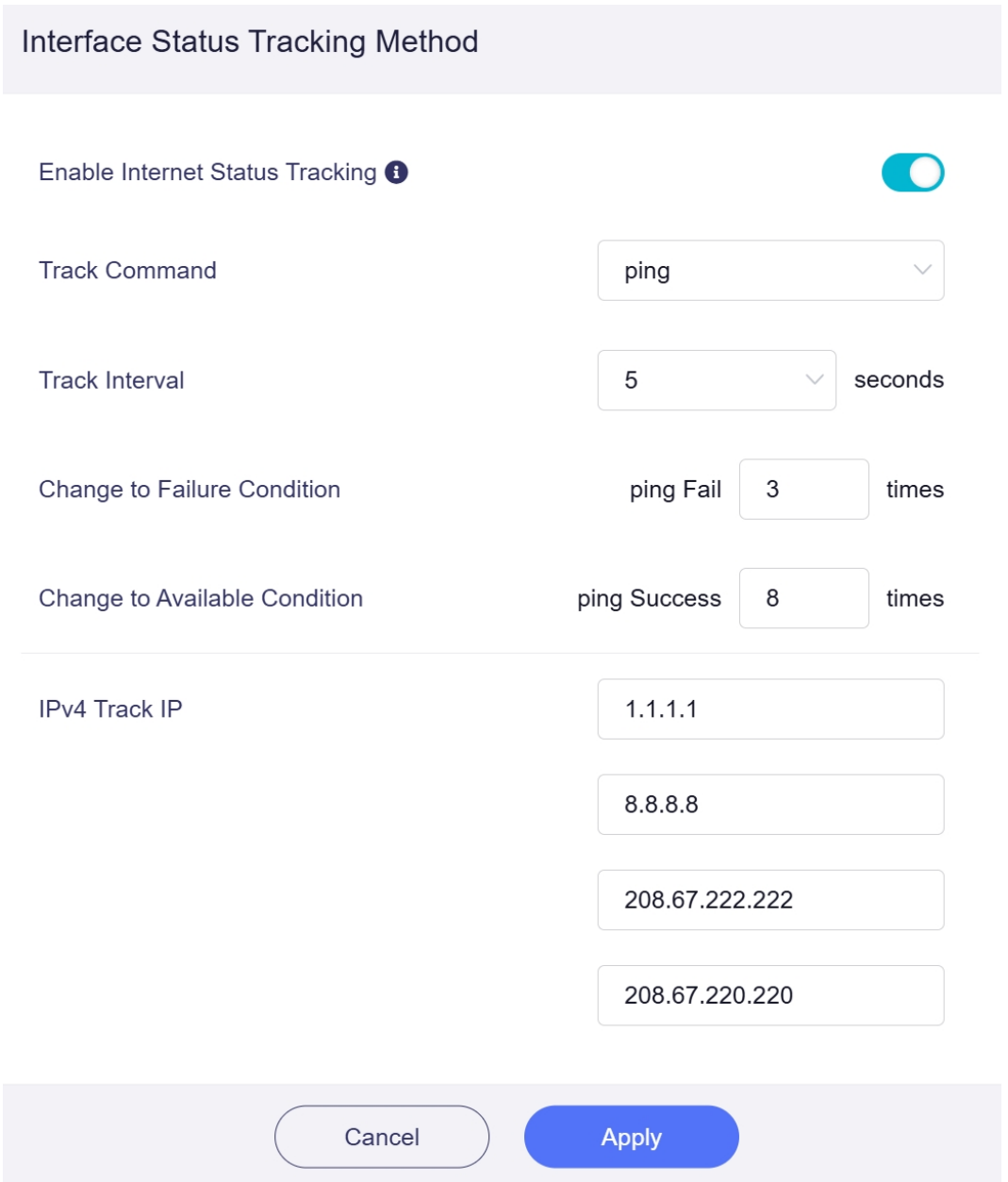
Zaloguj się do panelu administracyjnego routera i przejdź do **NETWORK** > **Multi-WAN**. Strona obejmuje dwie sekcje: Interface Status Track i Multi-WAN Mode.

12.2.1 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).
- **Track Command**: polecenie ping służy do monitorowania połączenia z docelowym adresem IP i sprawdzania dostępności interfejsu.
- **Track Interval**: określa, jak często router wykonuje polecenie monitorujące. Jednostką są sekundy.
- **Change to Failure Condition**: router oznacza interfejs jako rozłączony po określonej liczbie kolejnych nieudanych prób ping.

- **Change to Available Condition**: router przywraca stan połączenia interfejsu po określonej liczbie kolejnych udanych prób ping.
- **IPv4 Track IP**: w razie potrzeby dostosuj adresy IPv4 używane do monitorowania.

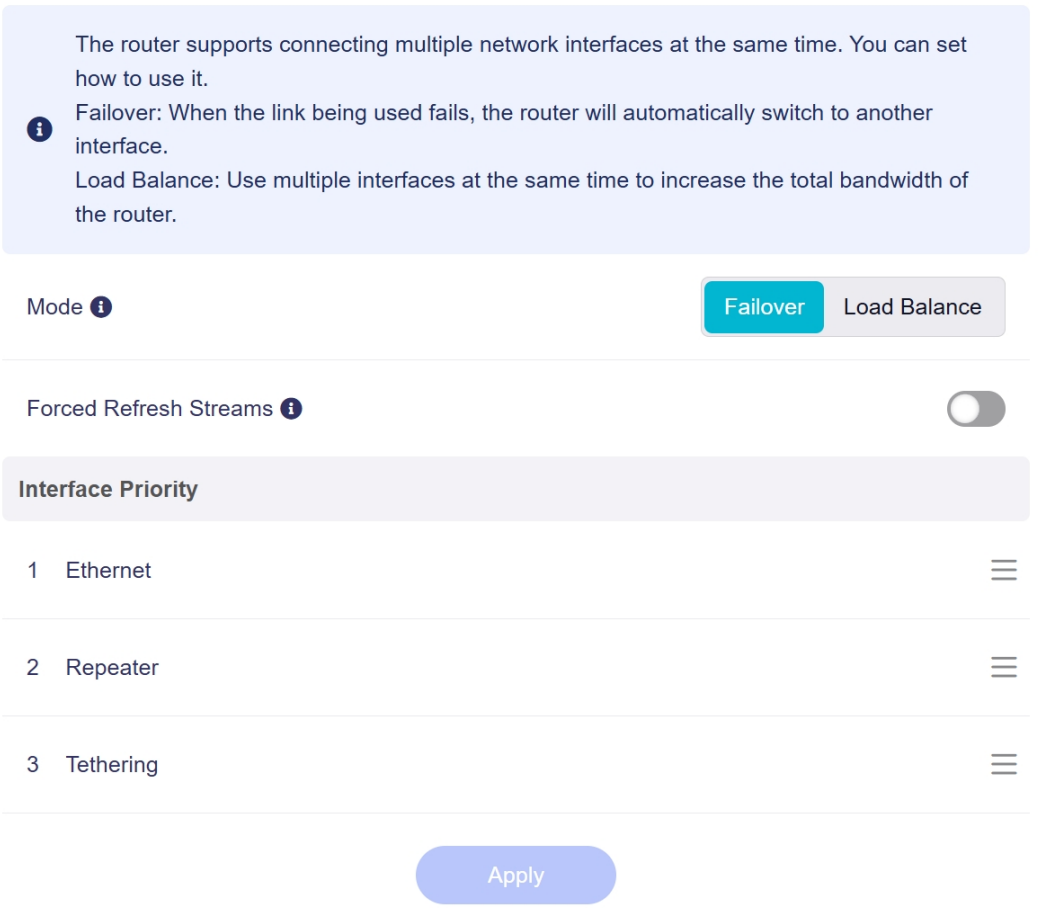
12.2.2 Tryb Multi-WAN

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.

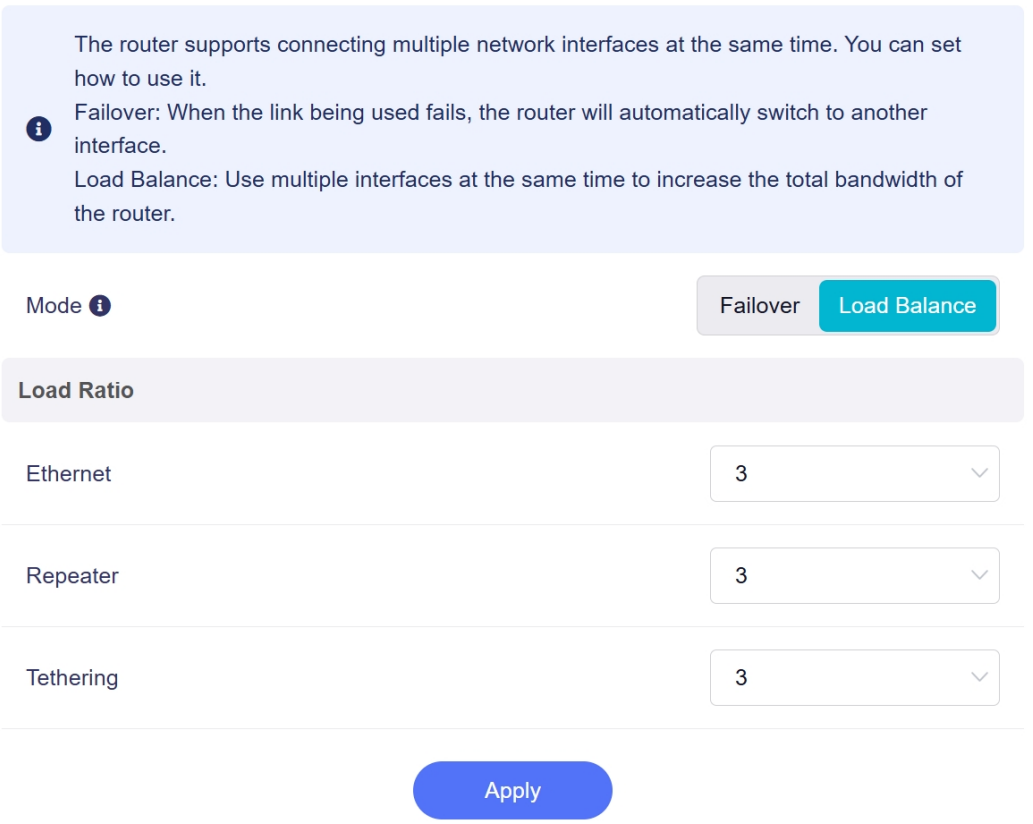


Równoważenie obciążenia (Load Balance)

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 (Ethernet, Repeater i Tethering), a wszystkie interfejsy zapewniają dostęp do Internetu, włączenie Load Balance i ustawienie proporcji 1:1:1 oznacza równy udział trzech interfejsów w obsłudze pasma sieciowego. System rozdziela nowe połączenia między te interfejsy zgodnie z ustawioną proporcją 1:1:1.



W razie potrzeby możesz dostosować proporcje obciążenia. Na przykład jeśli Ethernet ma przepustowość 100 Mb/s, Repeater 200 Mb/s, a połączenie Tethering jest nieaktywne, ustaw 1 dla Ethernet, 2 dla Repeater i 0 dla Tethering. System będzie rozdzielać nowe połączenia w

proporcji 1:2, czyli Ethernet obsłuży o połowę mniej połączeń niż Repeater. W odróżnieniu od trybu Failover ten tryb optymalizuje łączną przepustowość przez równoważenie ruchu 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.

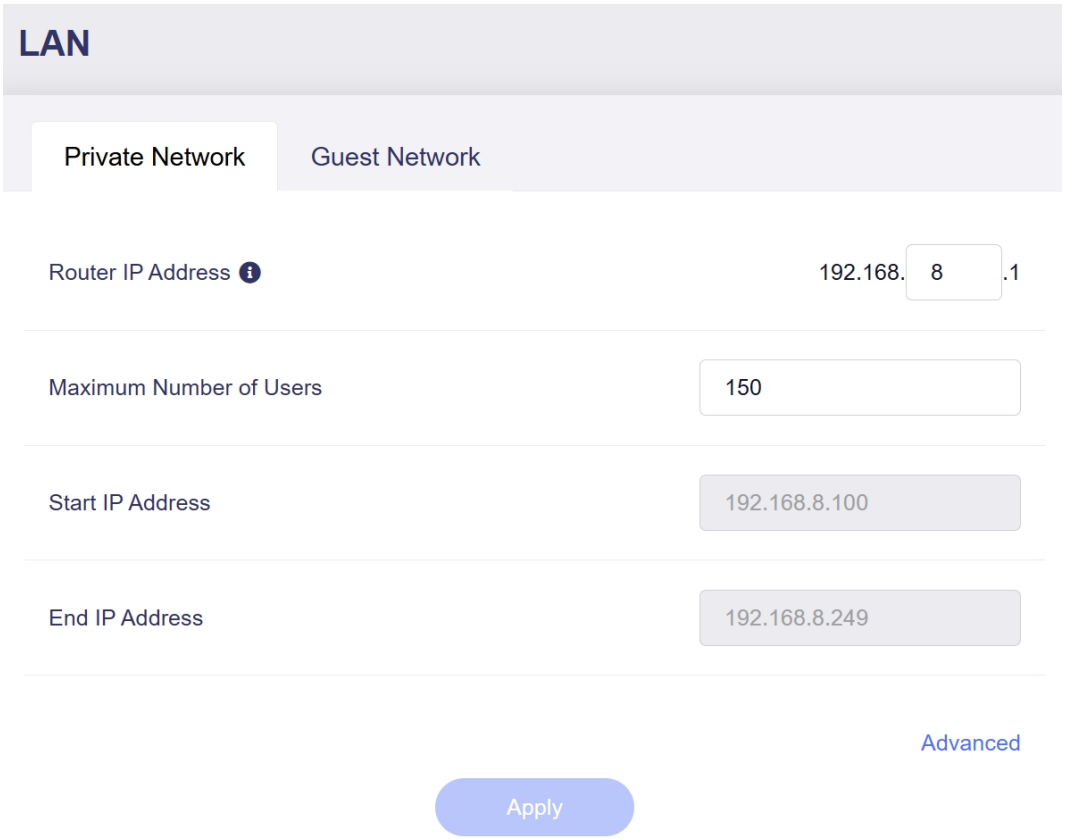
12.3 LAN

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, w tym sieć prywatną i sieć gościnną.

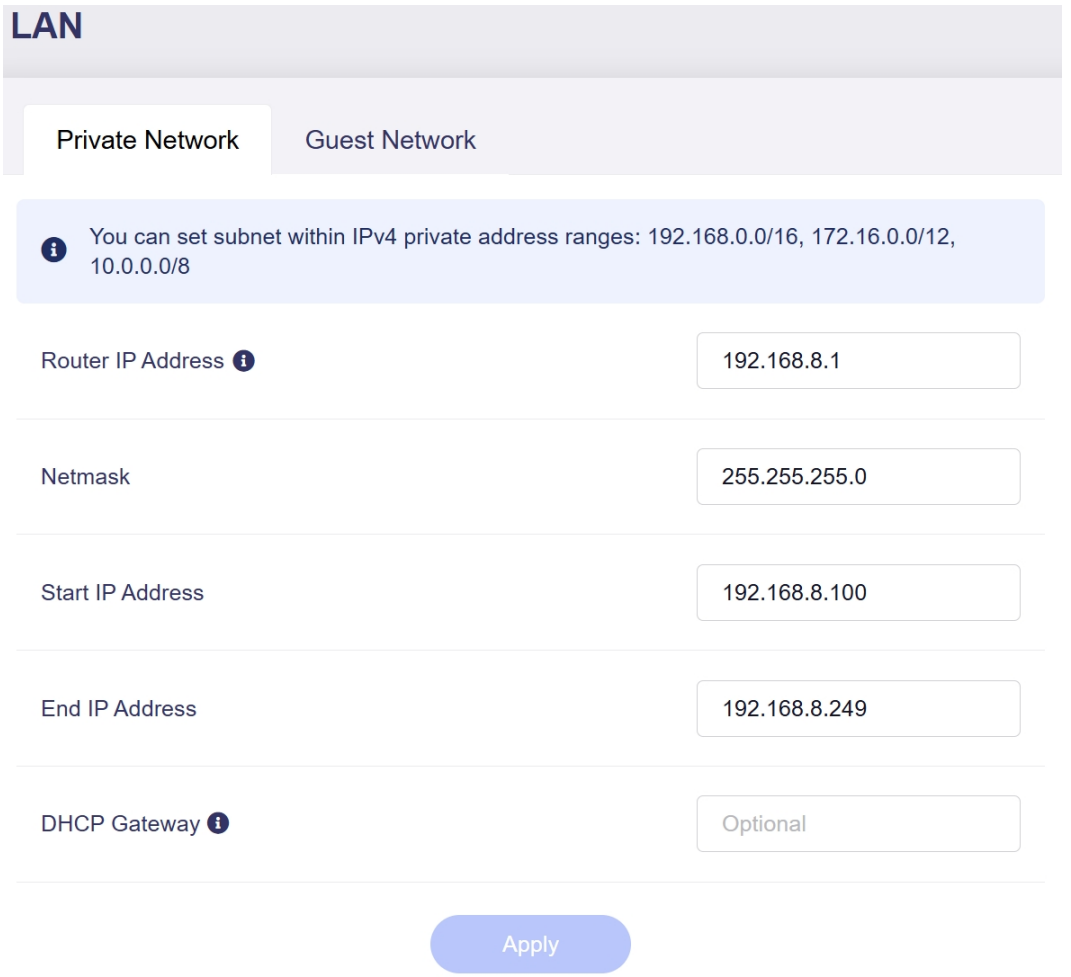
12.3.1 Sieć prywatna

Sieć prywatna to główna sieć lokalna podłączonych urządzeń. Możesz ustawić adres IP routera, zakres adresów DHCP i maksymalną liczbę podłączonych klientów.



- **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.
- **Maximum Number of Users**: ustawia maksymalną liczbę klientów, którzy mogą połączyć się z siecią gościnną.

Kliknij **Advanced**, aby zmienić ustawienia zaawansowane: bramę domyślną, maskę sieci, początkowy i końcowy adres IP oraz bramę DHCP.

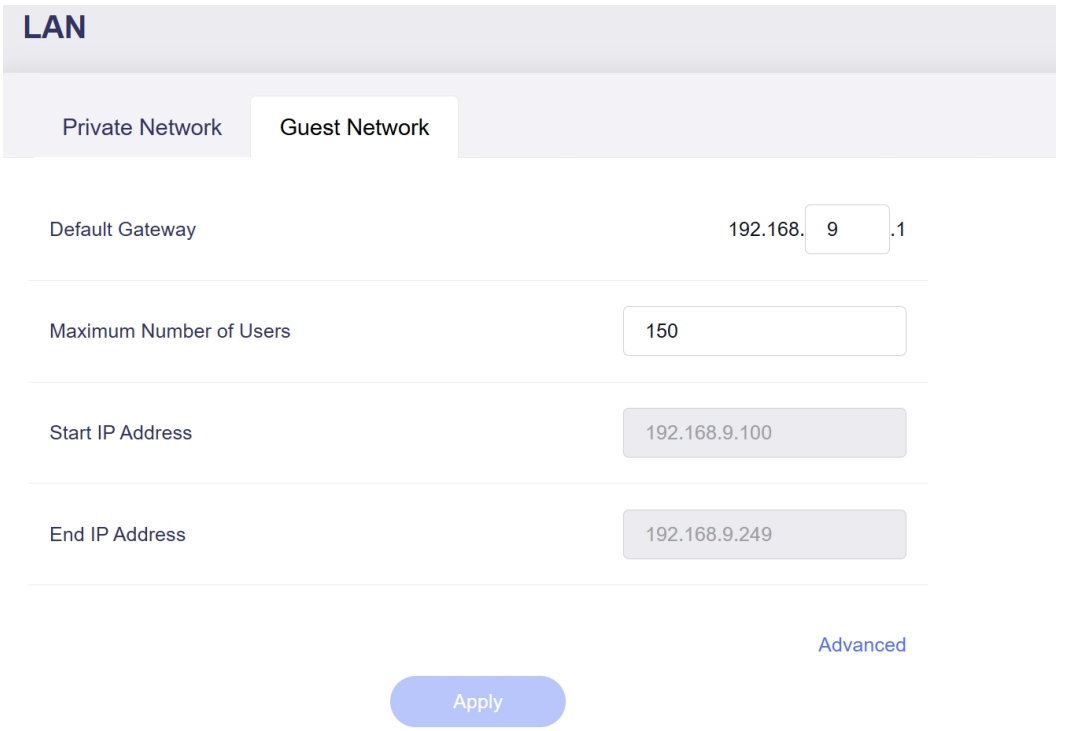


- **DHCP Gateway**: adres bramy domyślnej przydzielany klientom przez serwer DHCP. Kieruje ruch z sieci lokalnej do sieci zewnętrznych, np. Internetu.
- **Netmask**: maska podsieci prywatnej. Domyślnie 255.255.255.0.

12.3.2 Sieć gościnna

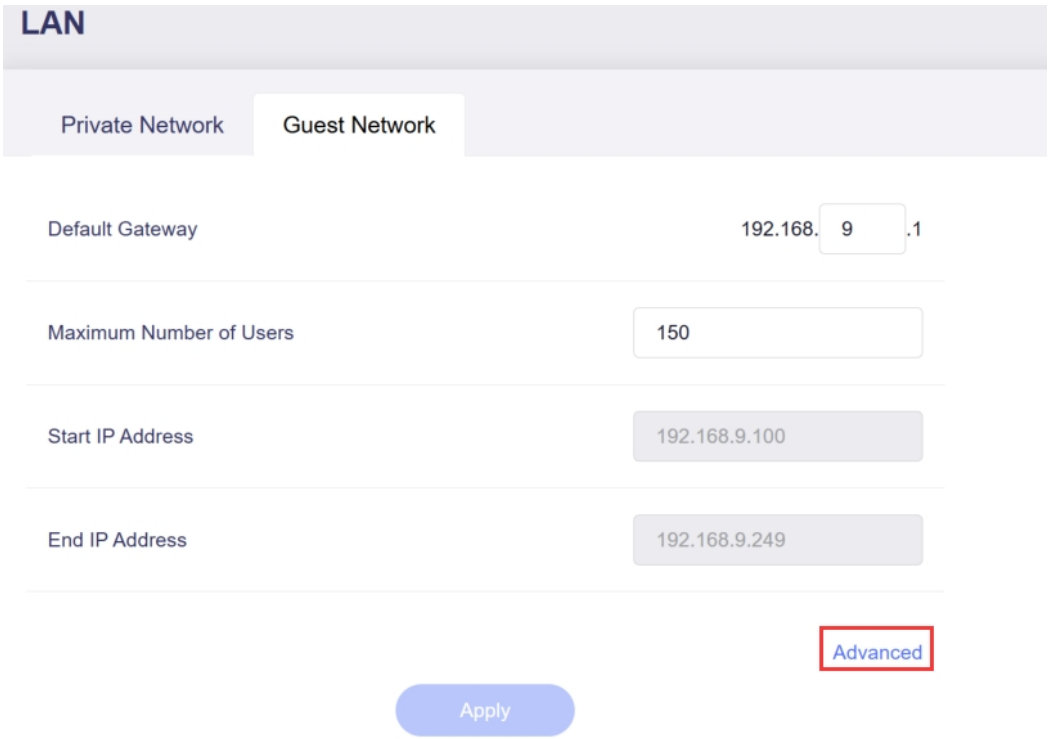
Sieć gościnna to oddzielna sieć dla gości, odizolowana od głównej sieci LAN w celu ochrony bezpieczeństwa sieci prywatnej.

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

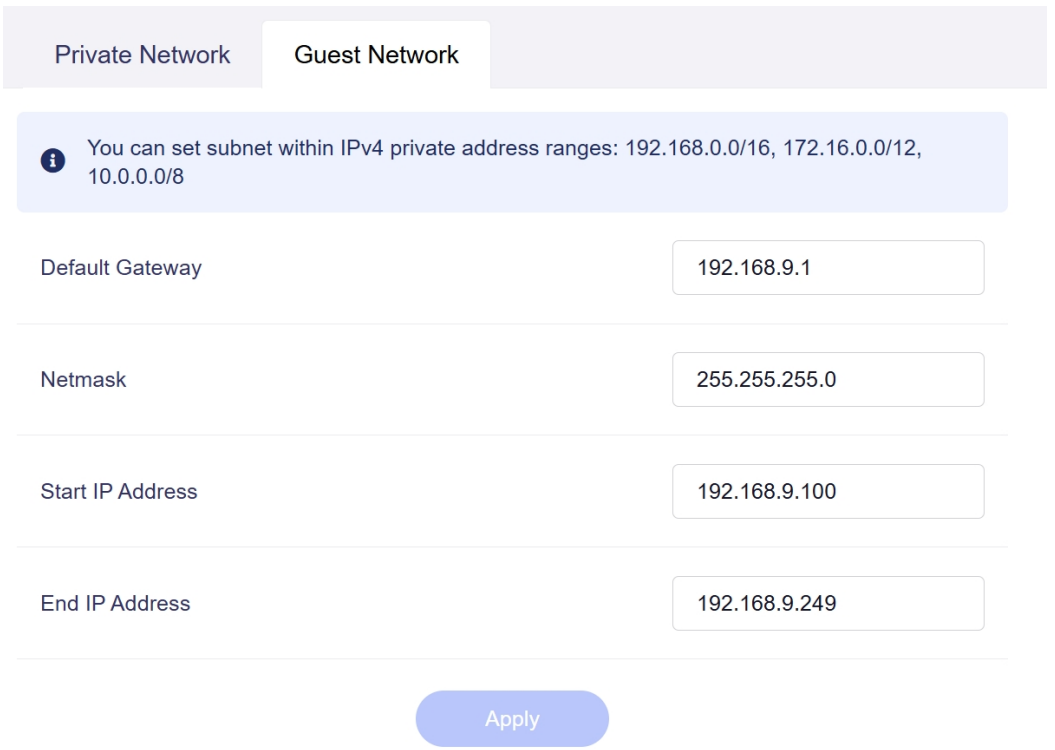


- **Default Gateway**: domyślny adres to 192.168.9.1. Można go zmienić, ale nie może kolidować z adresem bramy sieci głównej.
- **Maximum Number of Users**: ustawia maksymalną liczbę klientów, którzy mogą połączyć się z siecią gościnną.

Kliknij **Advanced** w prawym dolnym rogu.



Możesz skonfigurować ustawienia zaawansowane: bramę domyślną, maskę sieci oraz początkowy i końcowy adres IP.



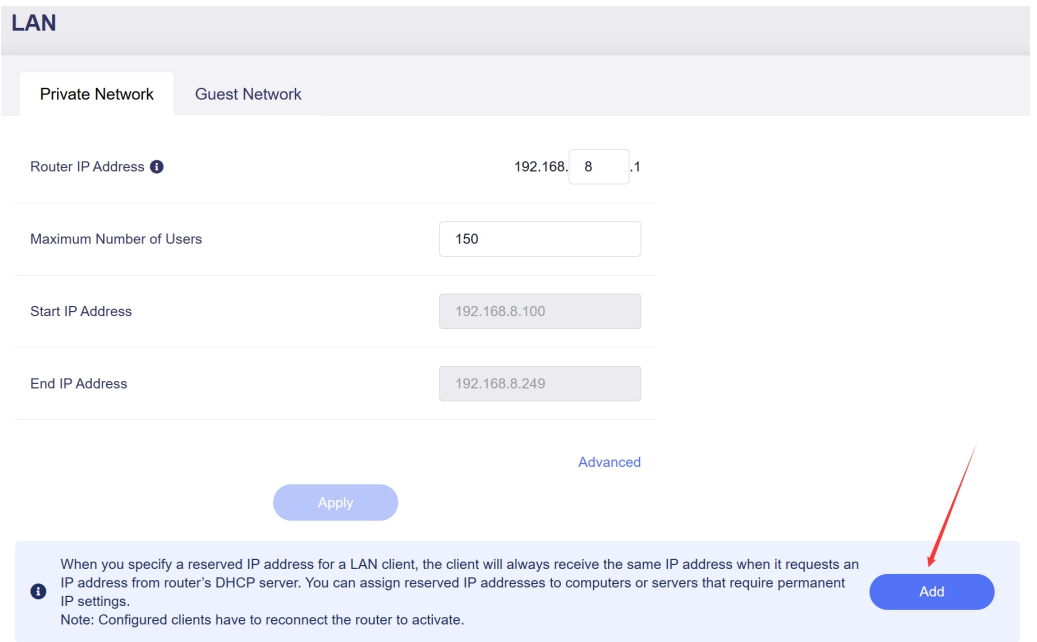
Maska **Netmask** domyślnie wynosi 255.255.255.0. Jeśli potrzebujesz większej podsieci z większą liczbą adresów IP, możesz wybrać 255.255.0.0.

12.3.3 Rezerwacja adresów

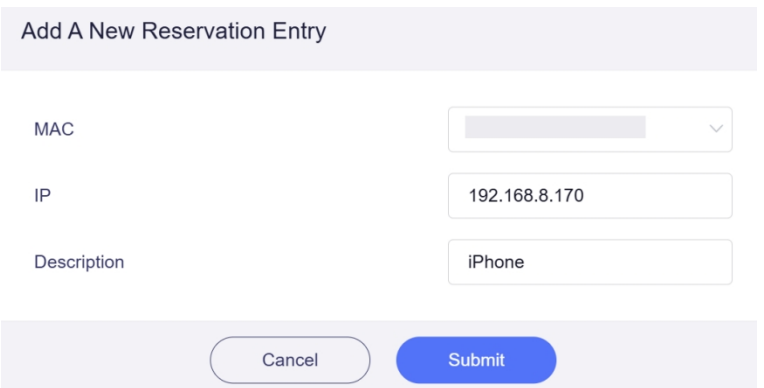
Rezerwacja adresów umożliwia przypisanie stałego adresu IP klientowi LAN, dzięki czemu przy każdym kontakcie z serwerem DHCP routera otrzymuje on ten sam adres. Zarezerwowane adresy można przypisywać komputerom lub serwerom wymagającym stałych ustawień IP. Aby ustawienie zaczęło działać, urządzenia z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

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

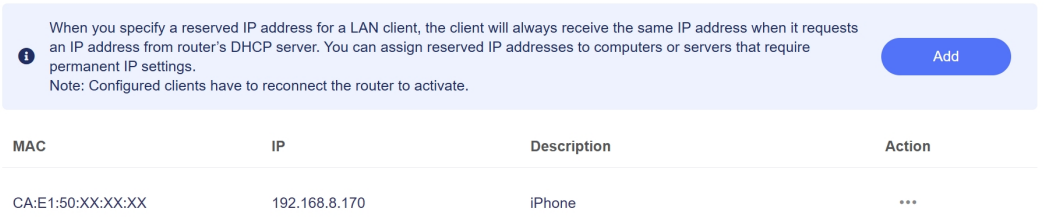
1. Zaloguj się do panelu administracyjnego routera, przejdź do **NETWORK** > **LAN** > **Address Reservation** i kliknij **Add**.



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.



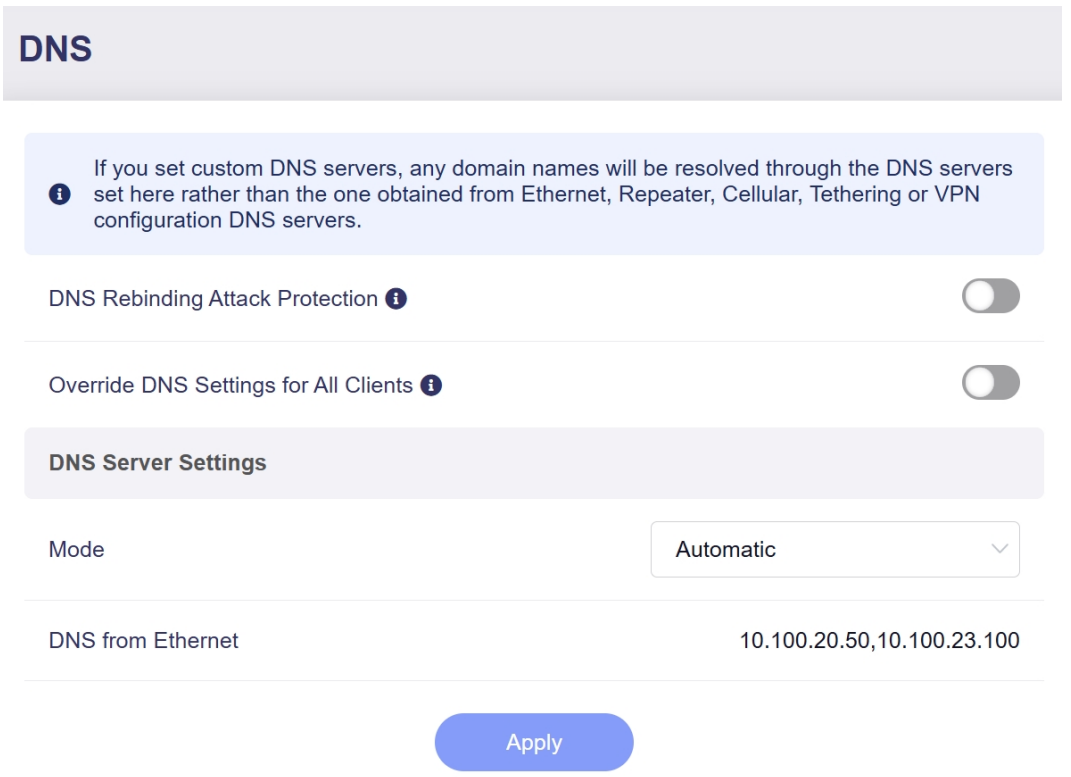
12.4 DNS

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.

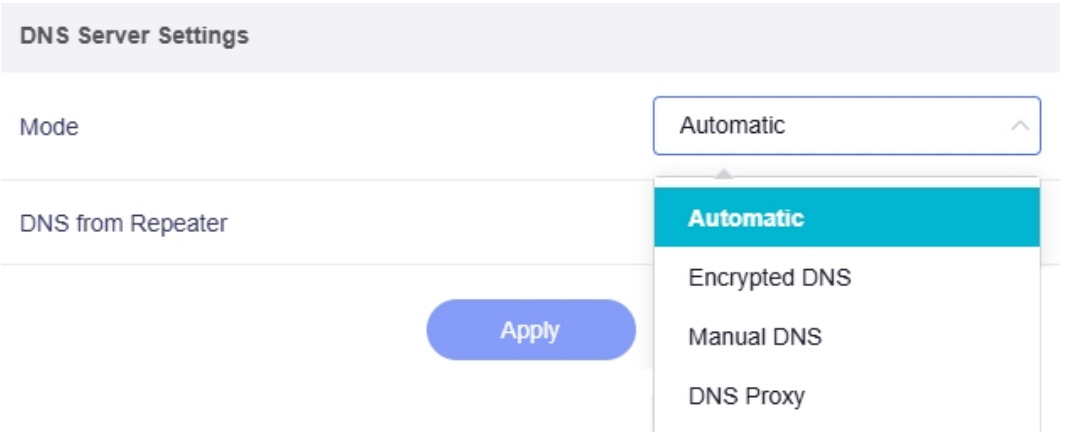
12.4.1 Ustawienia ogólne



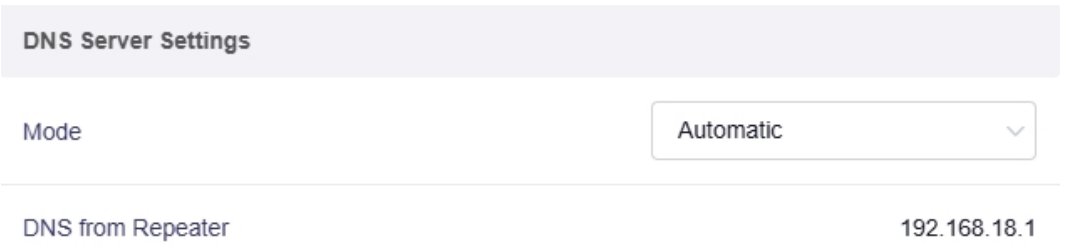
- **DNS Rebinding Attack Protection**: chroni przed atakami DNS rebinding przez blokowanie złośliwych prób rozwiązywania nazw DNS. Włączenie może spowodować problemy z prywatnymi zapytaniami DNS. Wyłącz tę opcję, jeśli sieć korzysta z portalu logowania (np. strony logowania do publicznego Wi-Fi).
- **Override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

12.4.2 Ustawienia serwera DNS

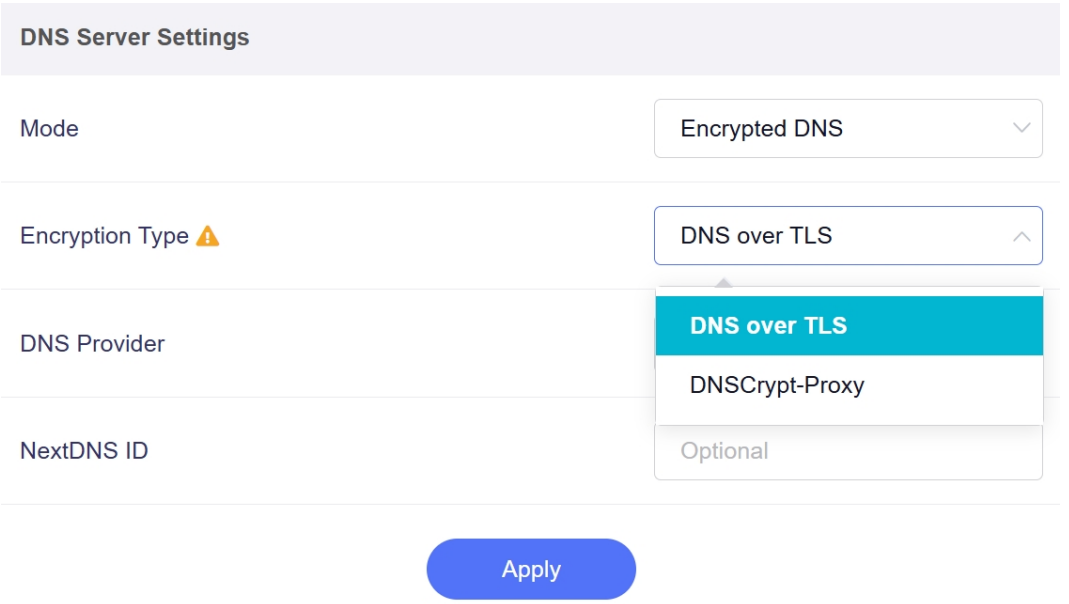
Dostępne są cztery tryby serwera DNS: Automatic, Encrypted DNS, Manual DNS i DNS Proxy.



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

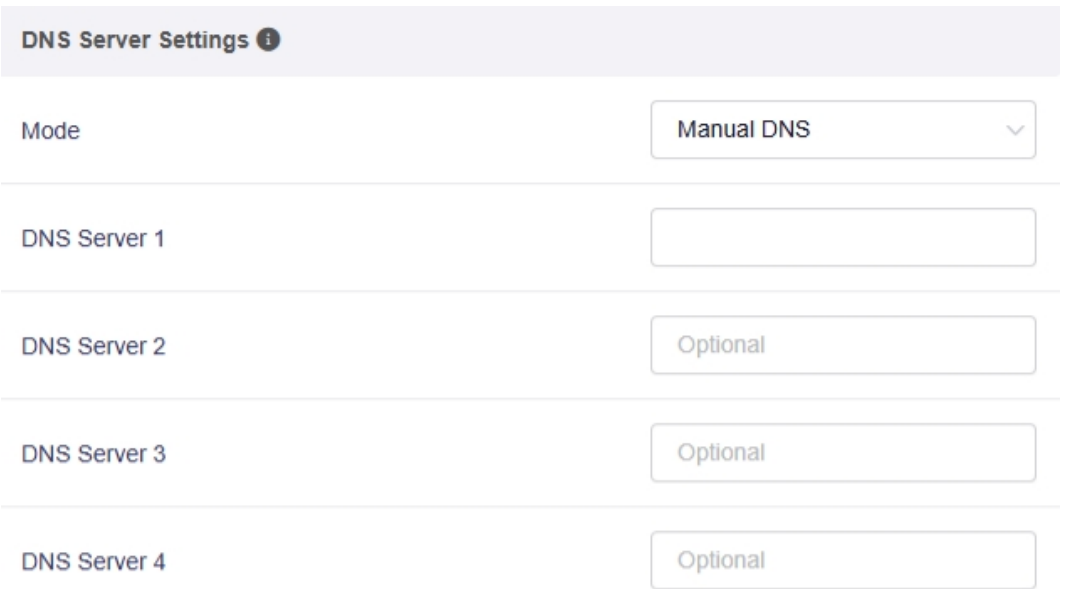


2. **Encrypted DNS**: router używa szyfrowanych protokołów do obsługi zapytań DNS, chroniąc dane rozwiązywania nazw przed podsłuchiwaniem i modyfikacją. Dostępne są dwa rodzaje szyfrowania: DNS over TLS i DNSCrypt-Proxy.



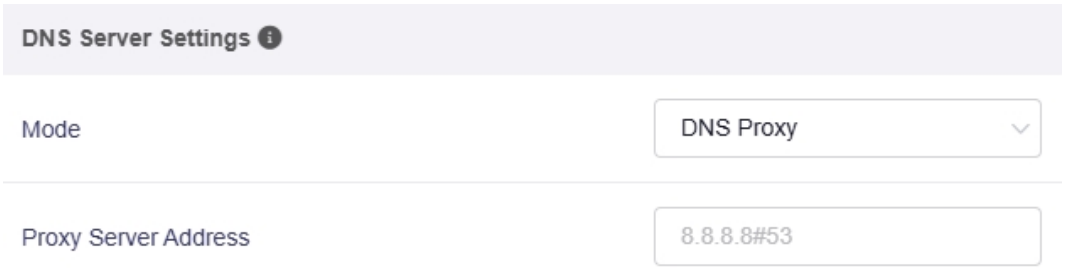
- Dla DNS over TLS wybierz dostawcę DNS spośród Control D, NextDNS i Cloudflare.
- Dla DNSCrypt-Proxy wybierz z repozytorium co najmniej jeden serwer DNS. Można wybrać maksymalnie 8 serwerów. Przy wielu serwerach router automatycznie używa najszybszego.

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



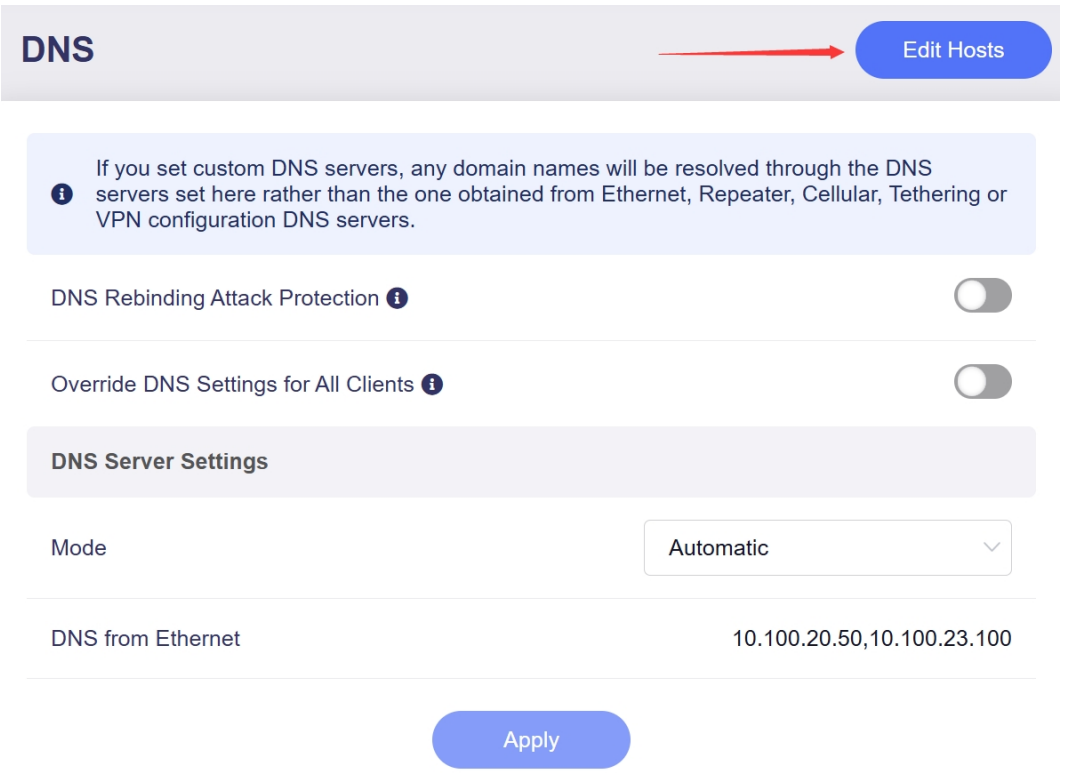
Uwaga: aby używać adresów IPv6 w ręcznej konfiguracji DNS, najpierw włącz IPv6 na routerze.

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

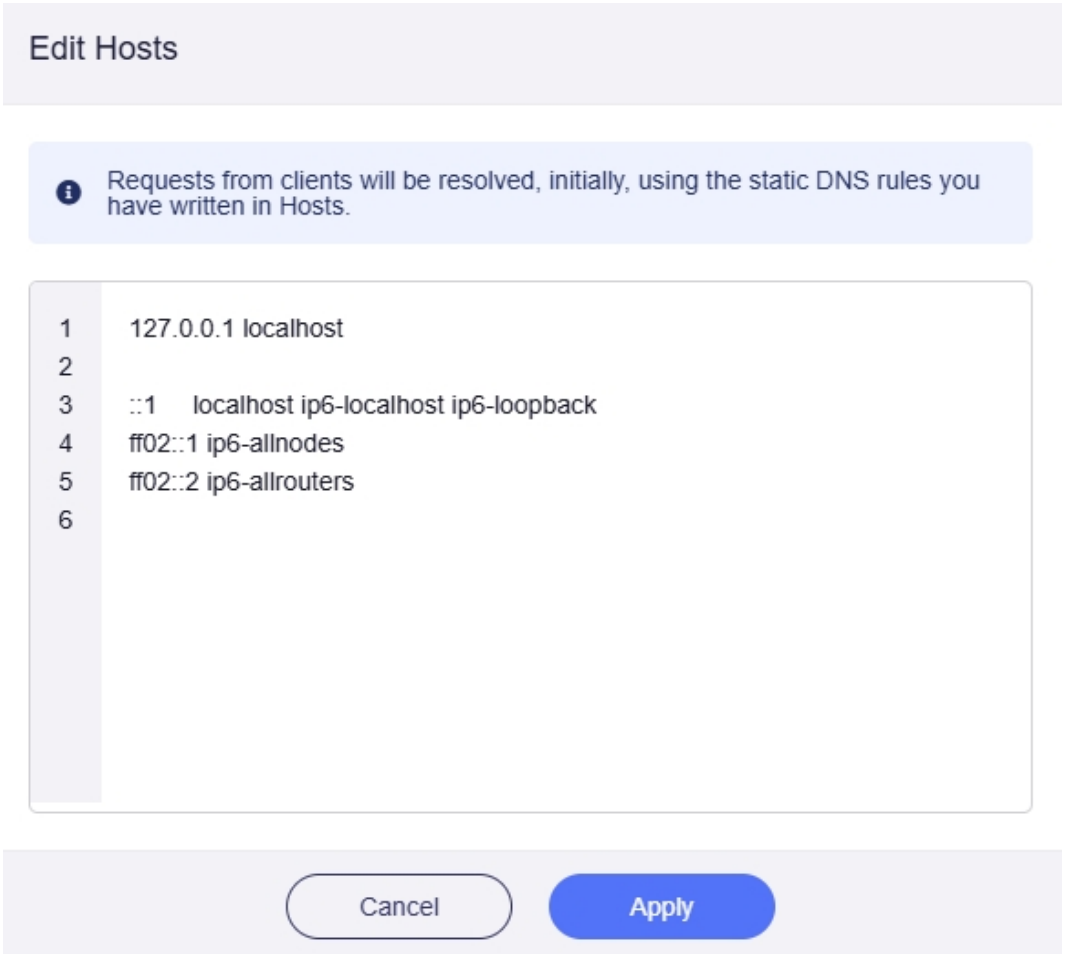


12.4.3 Edycja pliku hosts

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



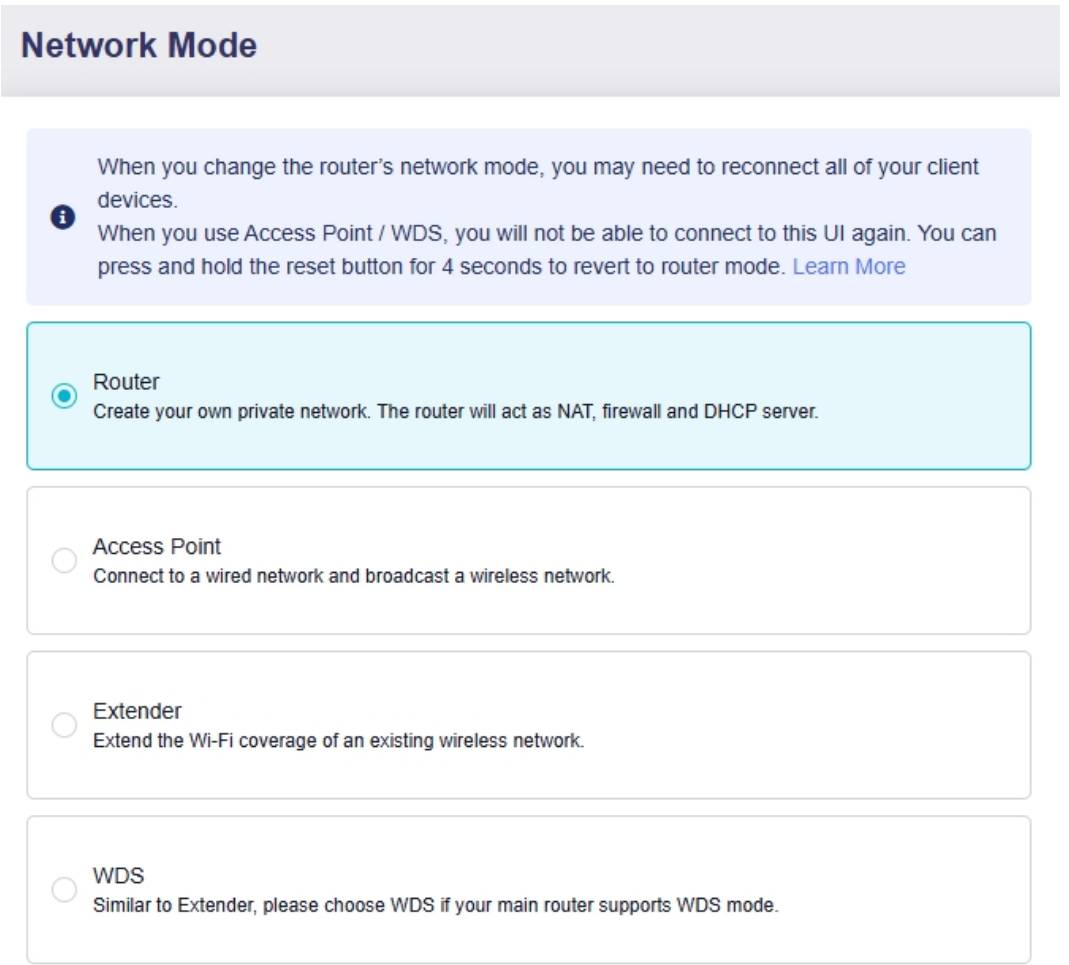
Żądania klientów są rozwiązywane w pierwszej kolejności według wpisanych tutaj statycznych reguł DNS. Pozwala to ręcznie mapować adresy IP na nazwy hostów (np. domyślny wpis 127.0.0.1 localhost dla lokalnej pętli zwrotnej) i samodzielnie kontrolować rozwiązywanie nazw domen.


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

12.5 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:

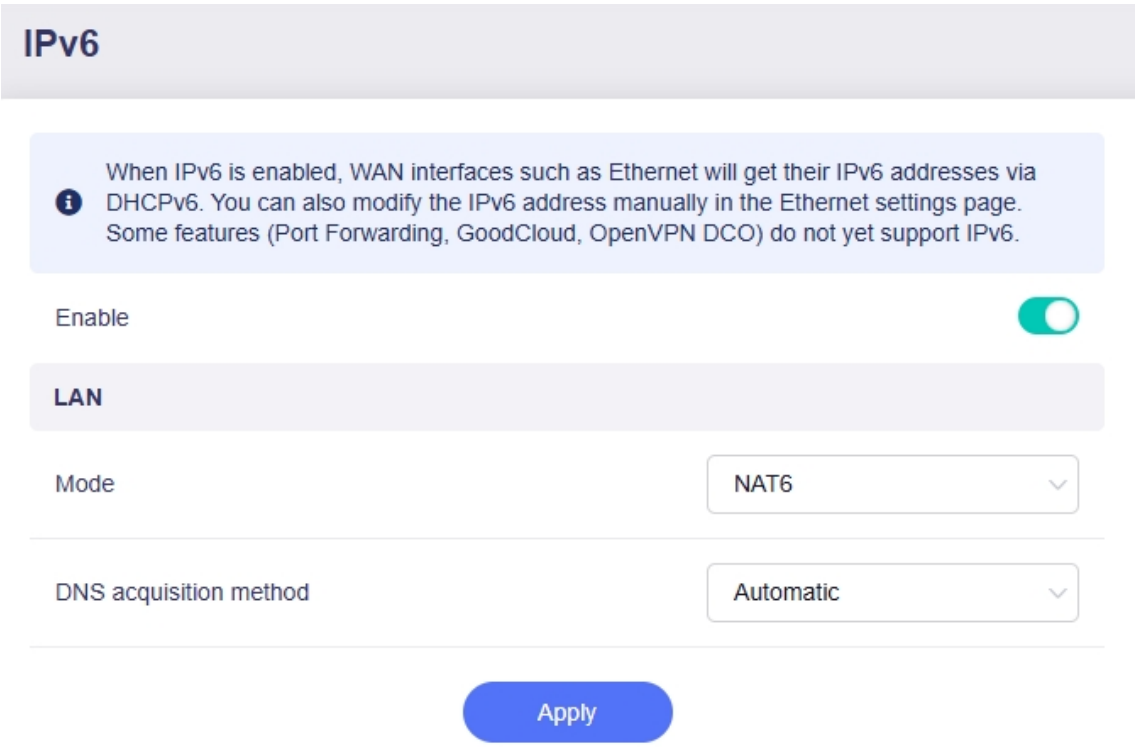
1. Po zmianie trybu sieciowego wszystkie urządzenia klienckie powinny ponownie połączyć się z routerem, aby zapewnić stabilną łączność.
2. **W trybie Access Point / WDS panel administracyjny nie jest dostępny pod pierwotnym adresem IP**. Zaloguj się do routera nadrzędnego, znajdź adres IP przydzielony 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, zapora, Multi-WAN, serwer DHCP, rezerwacja adresów, sieć gościnna, DNS, IPv6, Drop-in Gateway i IGMP Snooping.

12.6 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.

12.6.1 Tryb IPv6

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

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

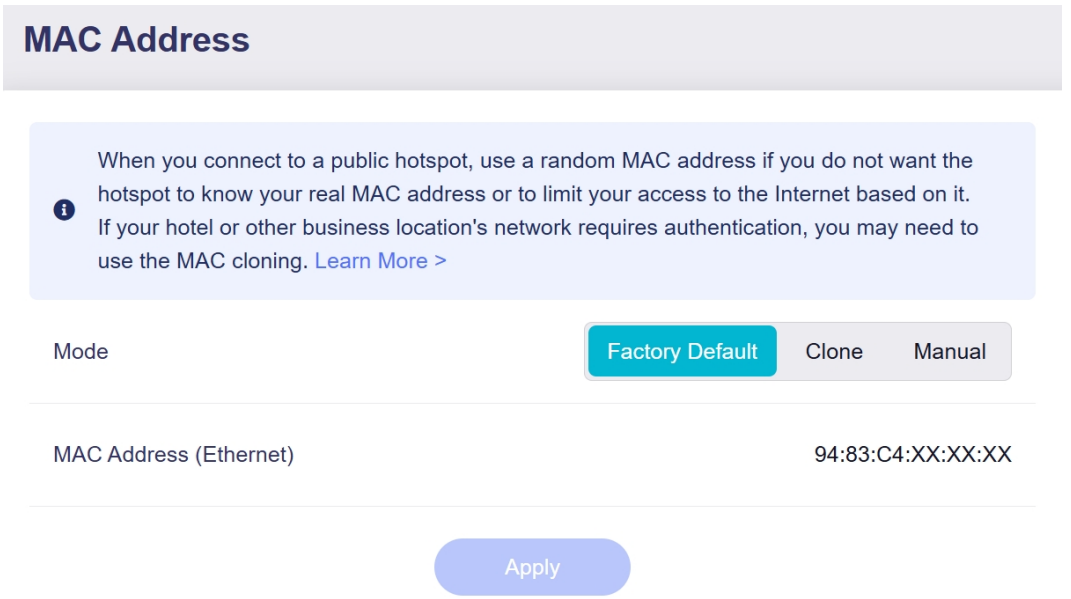
12.6.2 Sposób uzyskiwania DNS

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

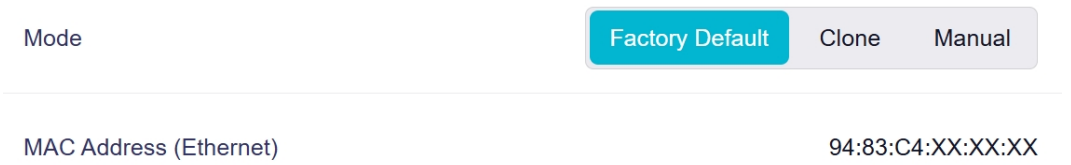
- **Automatic**: router dynamicznie uzyskuje adresy serwerów DNS IPv6 (np. przez DHCPv6).
- **Manual**: wprowadź własne adresy serwerów DNS IPv6. Ponieważ DNS służy do tłumaczenia nazw domen na odpowiadające im adresy IP, ręczna konfiguracja serwera DNS może powodować błędy rozwiązywania nazw. Używaj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

12.7 Adres MAC

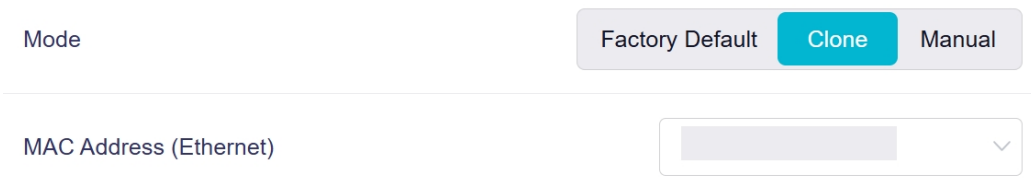
Strona MAC Address wyświetla domyślny adres MAC routera i umożliwia sklonowanie adresu klienta, ręczne wprowadzenie adresu lub wygenerowanie losowego adresu MAC. Jeśli urządzenie obsługuje używanie wielu portów Ethernet jako portów WAN, można ustawić adres MAC każdego z nich oddzielnie. Ustawienie adresu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



- **Fabryczny adres MAC.**

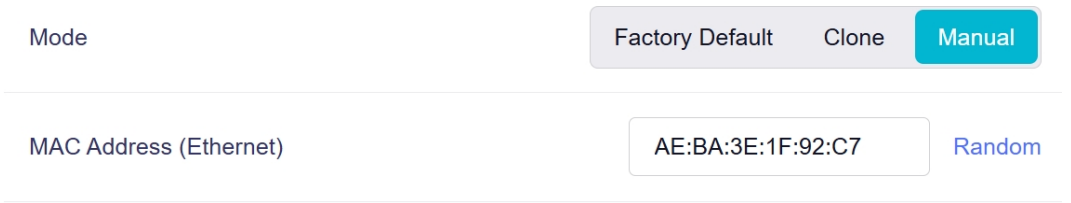


- **Klonowanie adresu MAC klienta.**



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.**

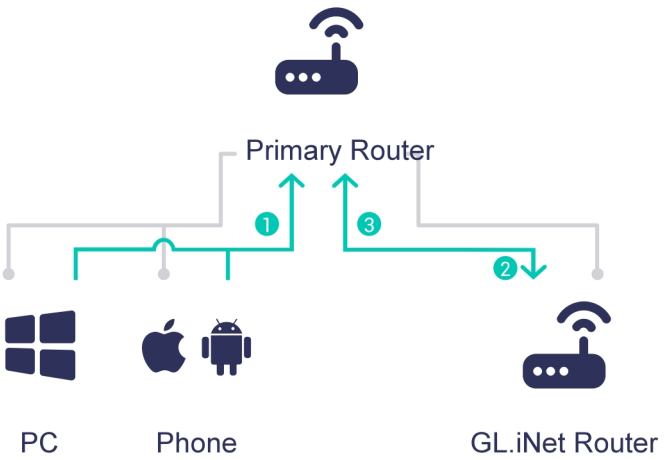


12.8 Drop-in Gateway

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:

- 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.



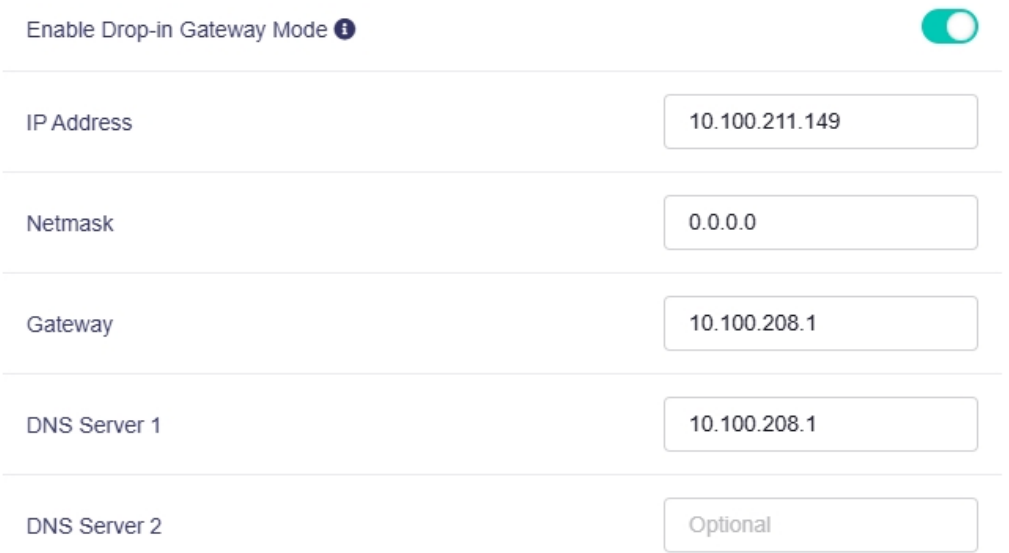
Powyższy schemat zawiera dwa rodzaje linii: szare oraz zielone z trzema strzałkami oznaczonymi numerami.

- **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;

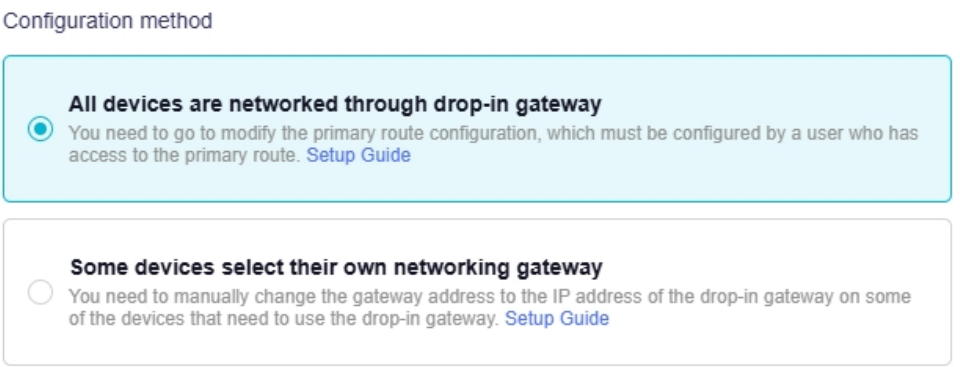
2. Główny router przekazuje ruch do routera GL.iNet w celu przetworzenia (np. filtrowania reklam, szyfrowania VPN);
3. Po przetworzeniu ruch wraca do głównego routera, który dostarcza dane do pierwotnych urządzeń klienckich lub kieruje je do Internetu.

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.



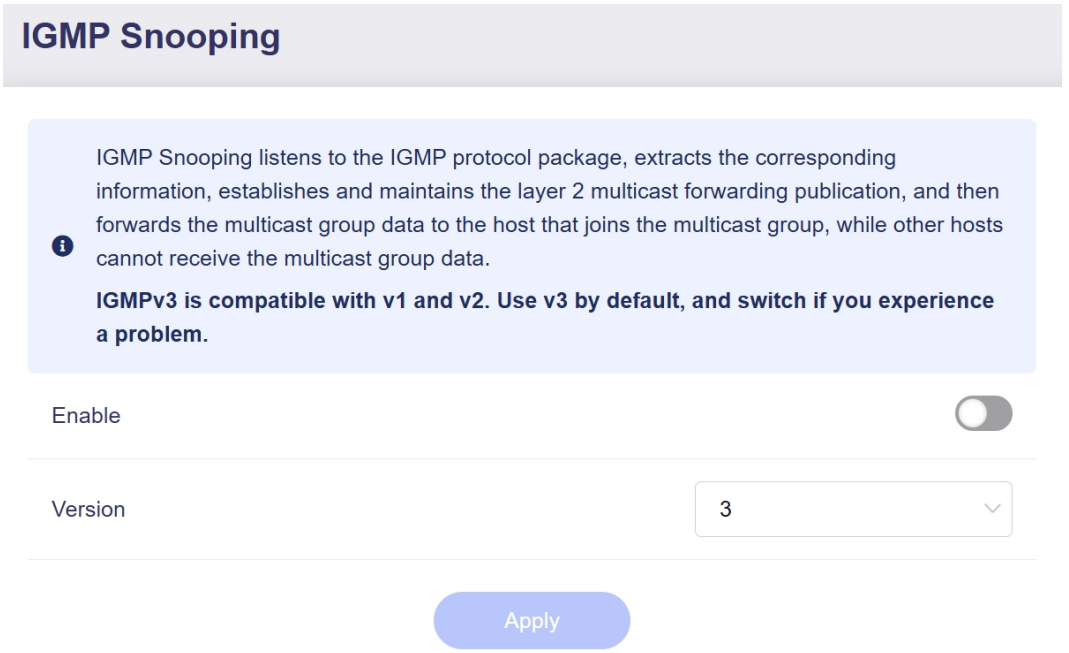
2. Wybierz sposób konfiguracji i kliknij **Apply**. Szczegóły znajdziesz w tym poradniku.



12.9 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.



Rozdział 13

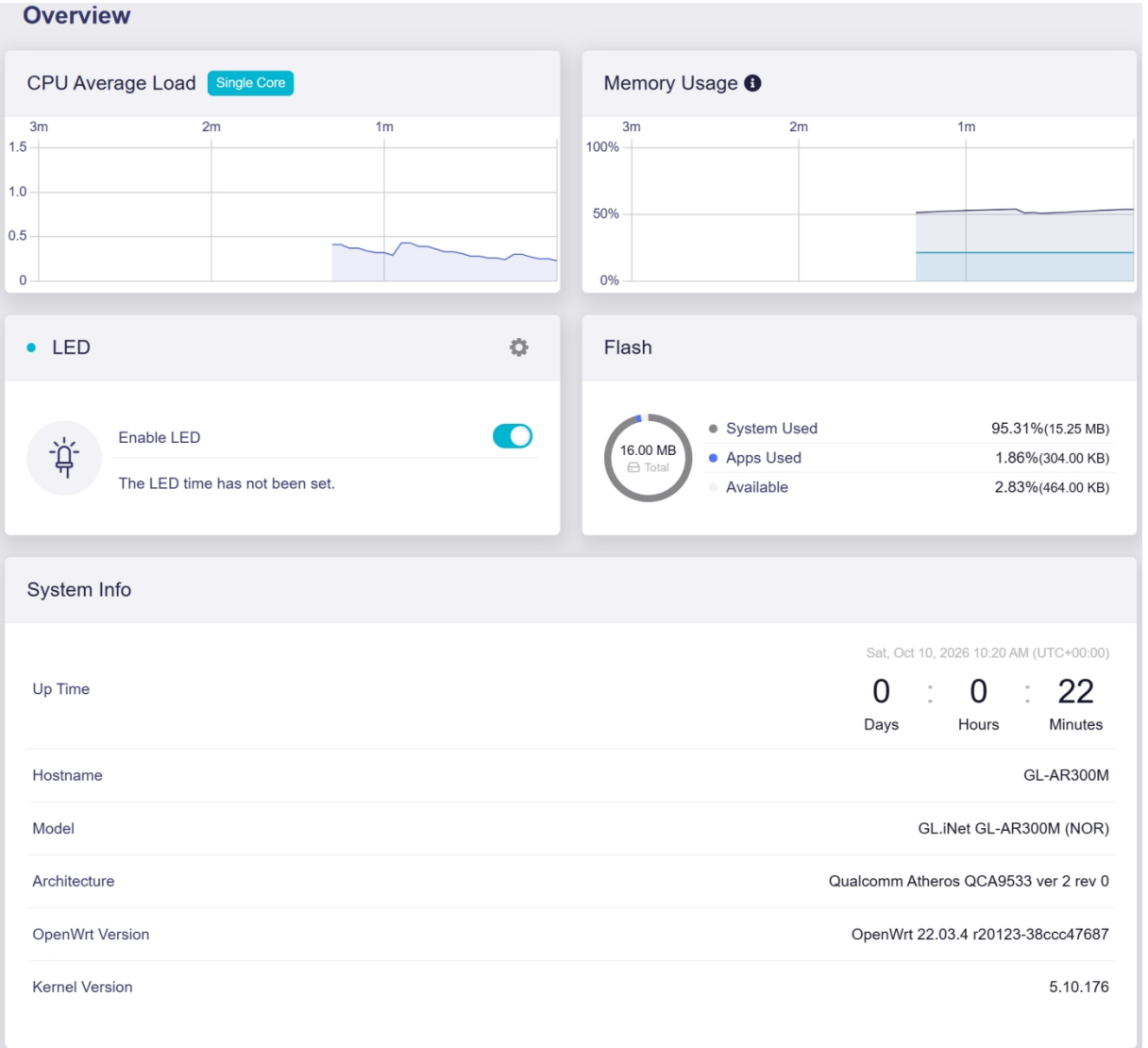
System

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

13.1 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

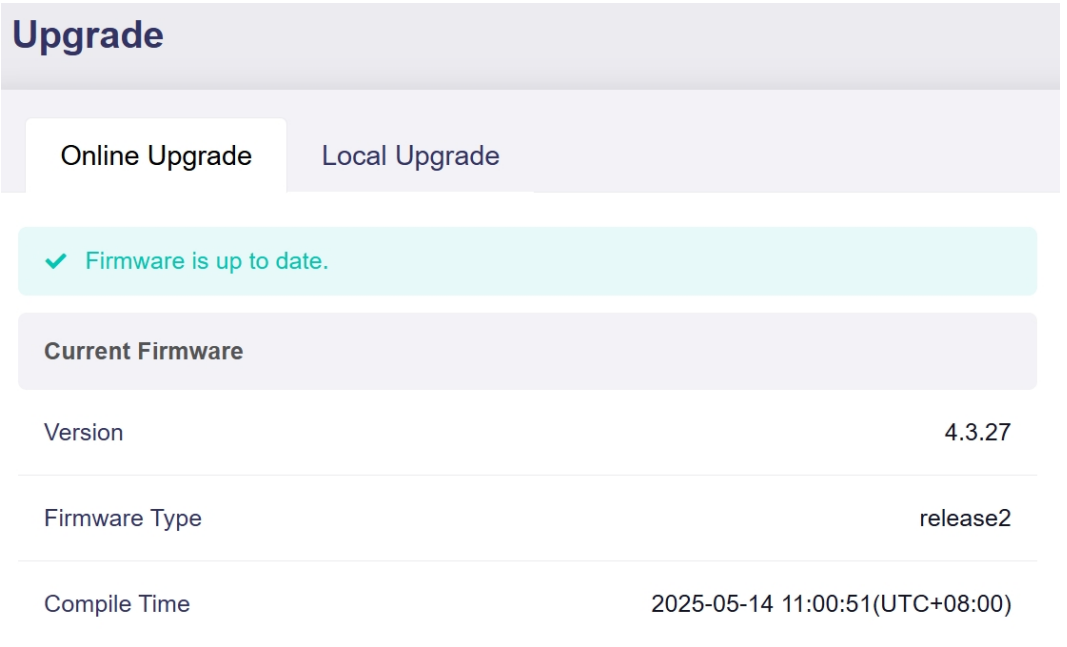


13.2 Aktualizacja

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

13.2.1 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.

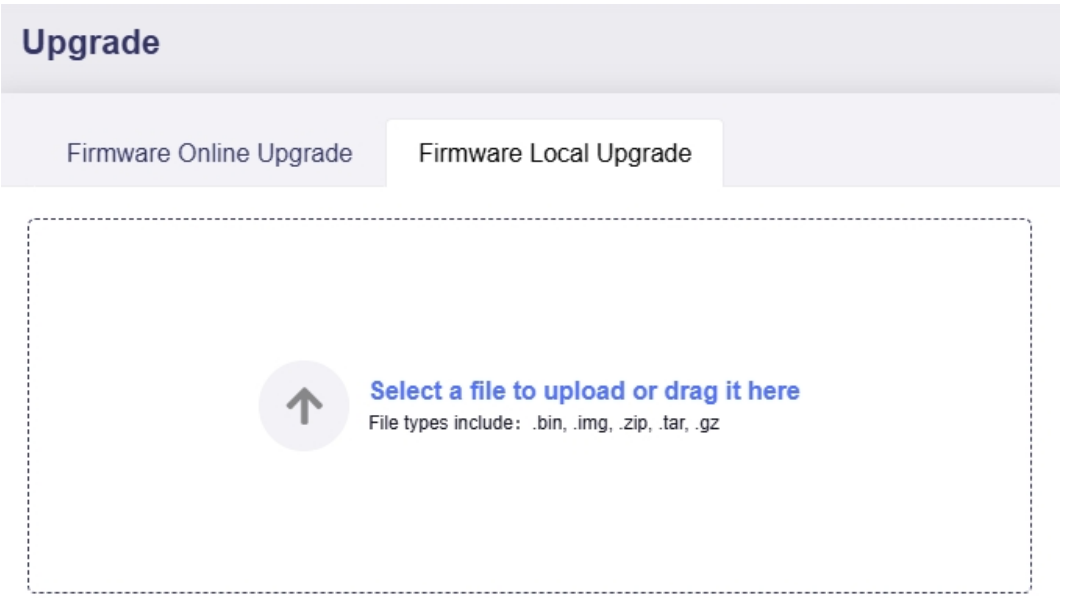


Wskazówka: jeśli podczas aktualizacji online pojawi się komunikat **Download Failed**, przejdź do **SYSTEM** > **Time Zone** i popraw błąd strefy czasowej (zsynchronizuj z przeglądarką).

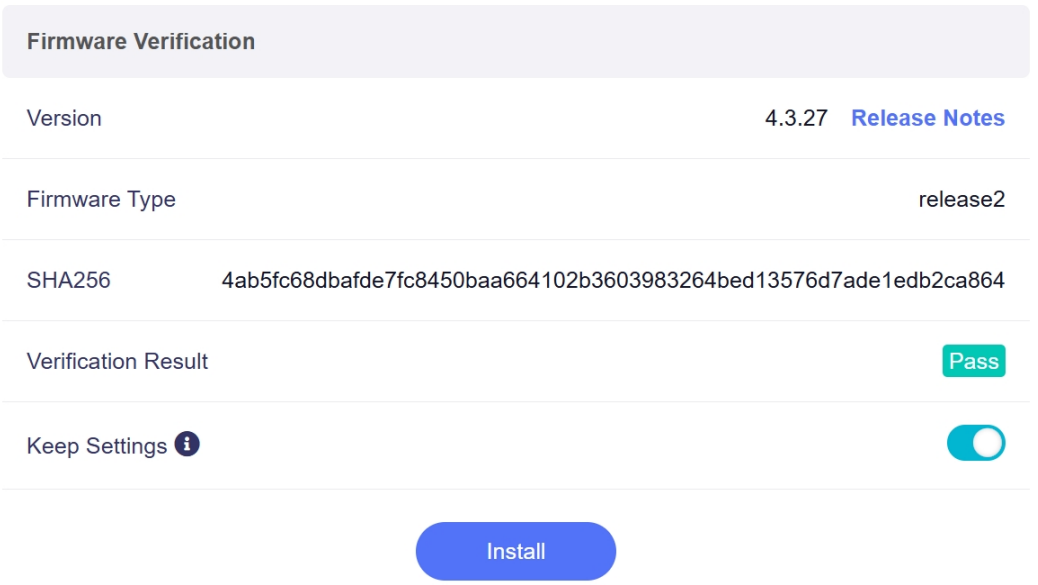
13.2.2 Aktualizacja lokalna

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.

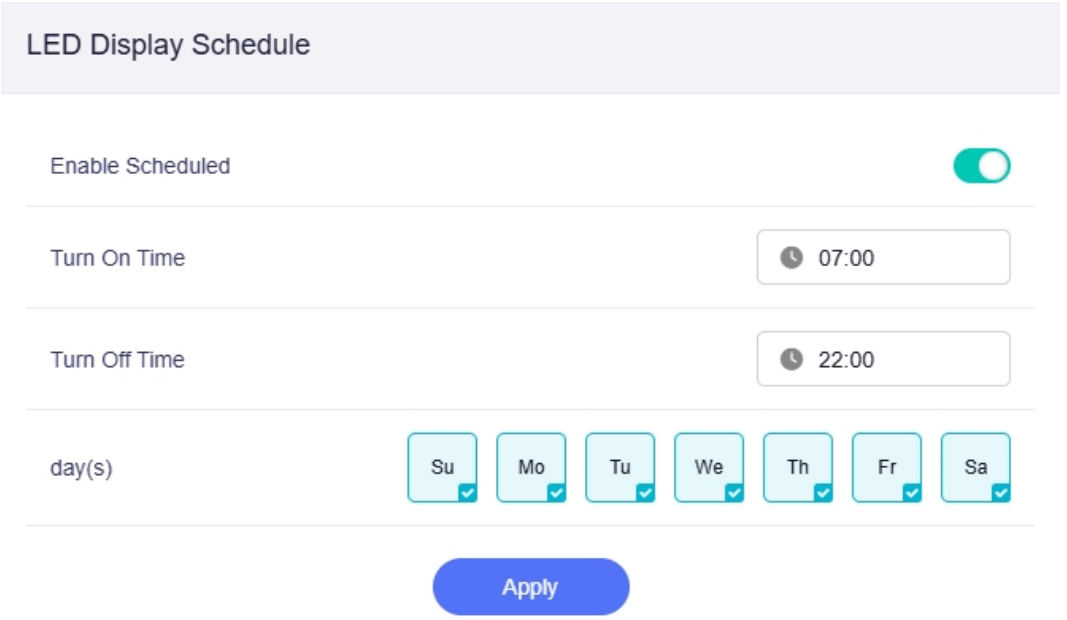
13.3 Zadania zaplanowane

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.

13.3.1 Harmonogram diody LED

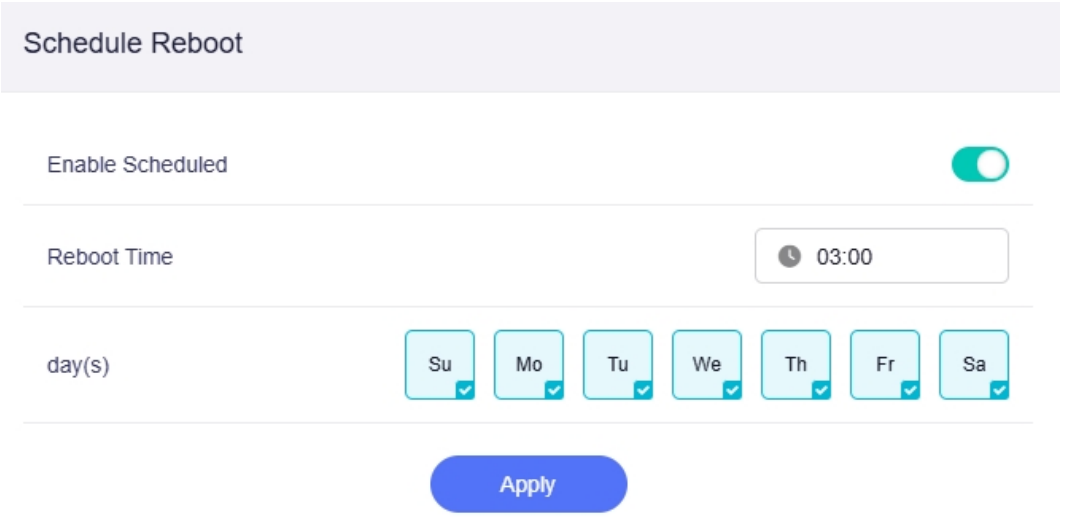
W razie potrzeby ustaw harmonogram diody LED routera i kliknij **Apply**.



- **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.

13.3.2 Harmonogram ponownego uruchamiania

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



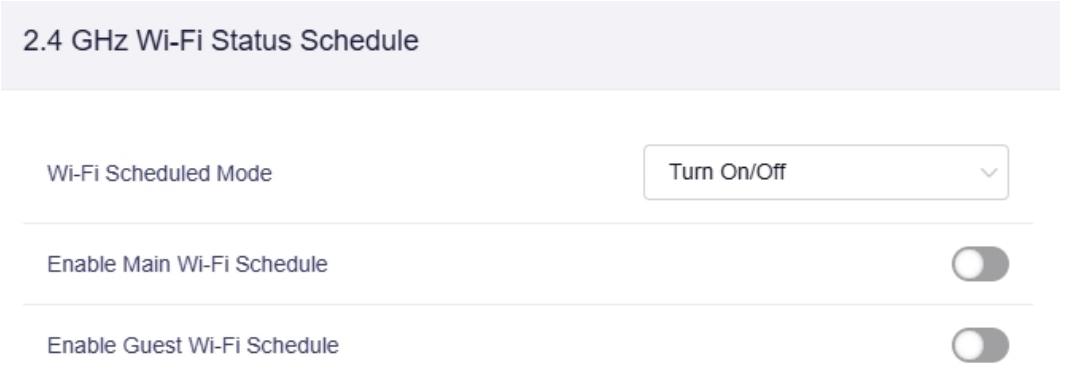
- **Enable Scheduled**: włącz ten przełącznik, aby uruchomić harmonogram ponownego uruchamiania.
- **Reboot Time**: ustaw konkretną godzinę ponownego uruchomienia routera (np. 03:00).
- **day(s)**: wybierz dni tygodnia, w których te ustawienia mają obowiązywać.

13.3.3 Harmonogram Wi-Fi 2,4 GHz

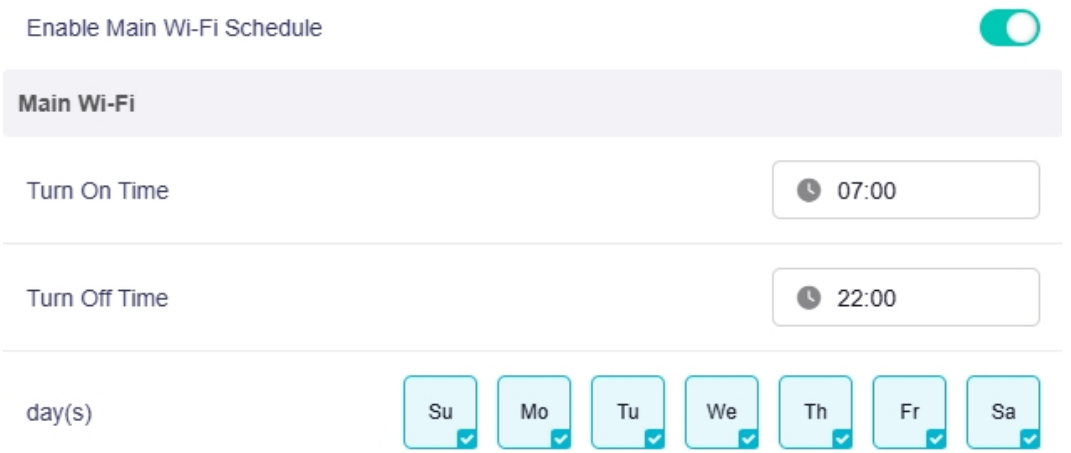
Ta funkcja umożliwia ustawienie harmonogramu Wi-Fi 2,4 GHz. Dostępne są dwa tryby: Turn On/Off i Switch TX Power.

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

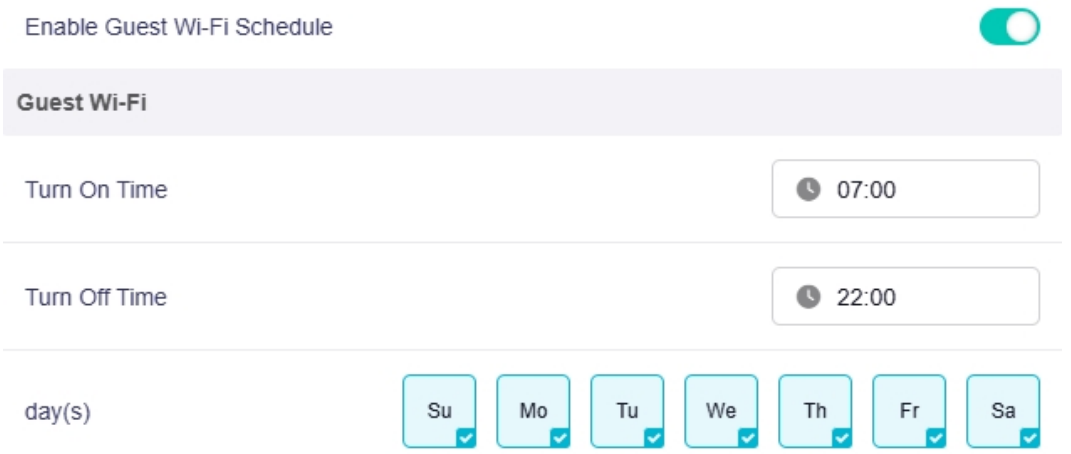
Możesz włączyć harmonogram włączania i wyłączania głównej oraz gościnnej sieci Wi-Fi 2,4 GHz.



- **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.

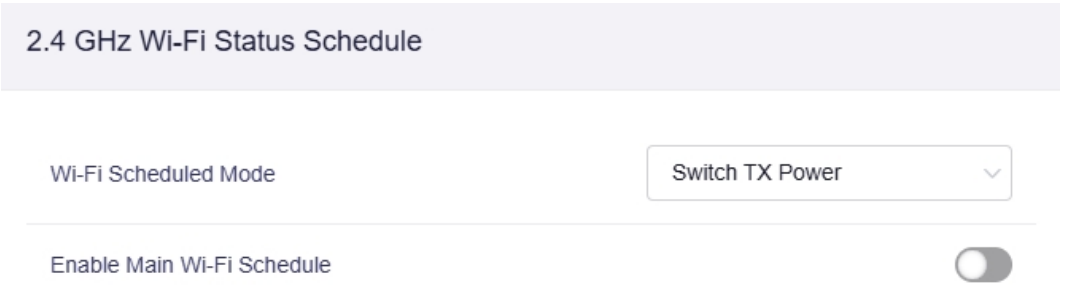


- **Guest Wi-Fi Schedule**: po włączeniu ustaw godziny włączania i wyłączania gościnnej sieci Wi-Fi 2,4 GHz oraz wybierz dni tygodnia, w których harmonogram obowiązuje.

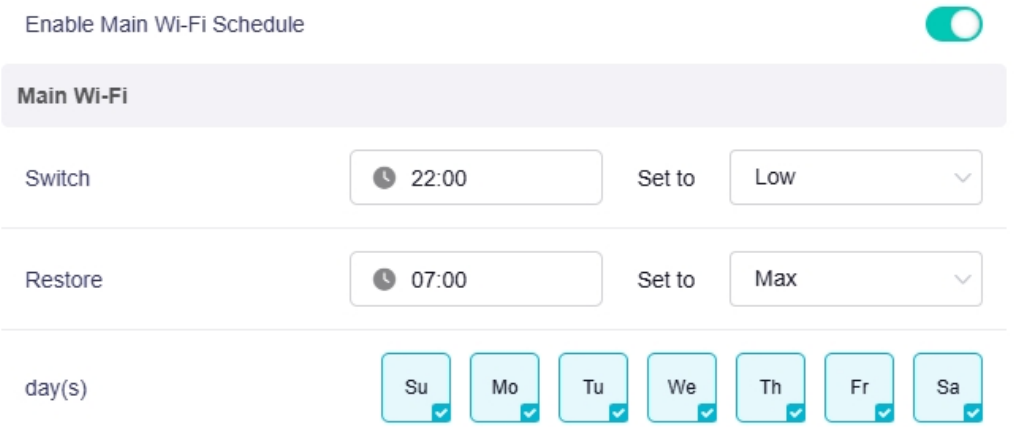


Tryb 2: przełączanie mocy nadawania (Switch TX Power)

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



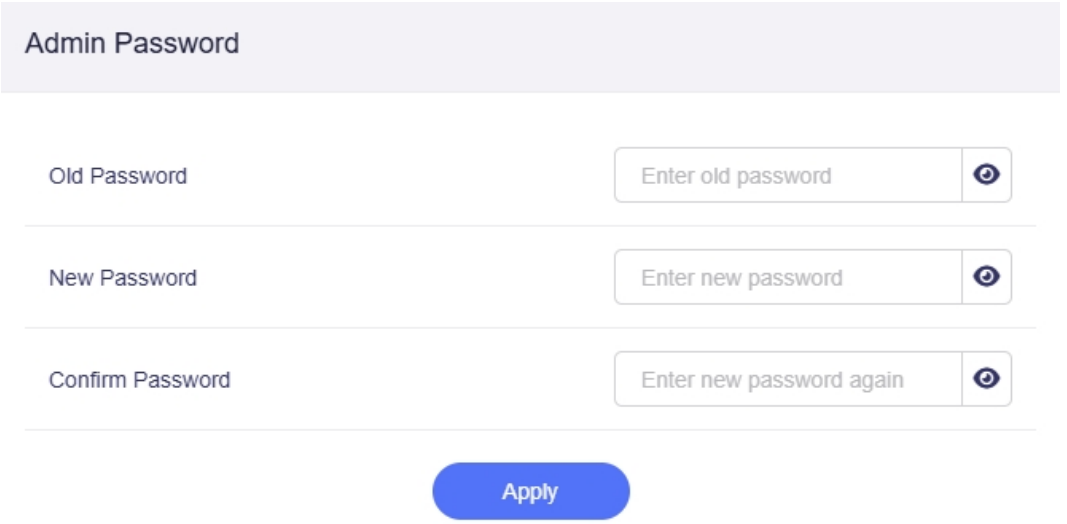
Po włączeniu ustaw dwie zaplanowane czynności zmiany mocy nadawania głównej sieci Wi-Fi 2,4 GHz oraz wybierz dni tygodnia, w których obowiązują.



- **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.

13.4 Hasło administratora

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

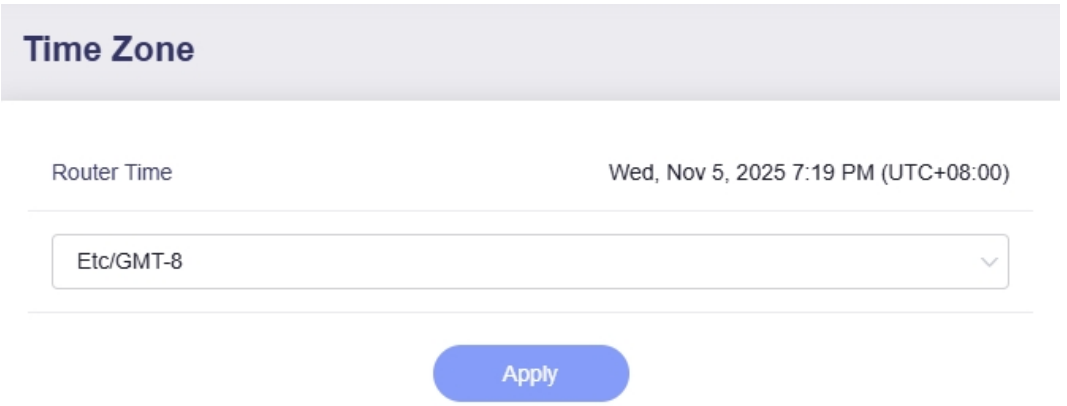


Wymagania dotyczące hasła administratora:

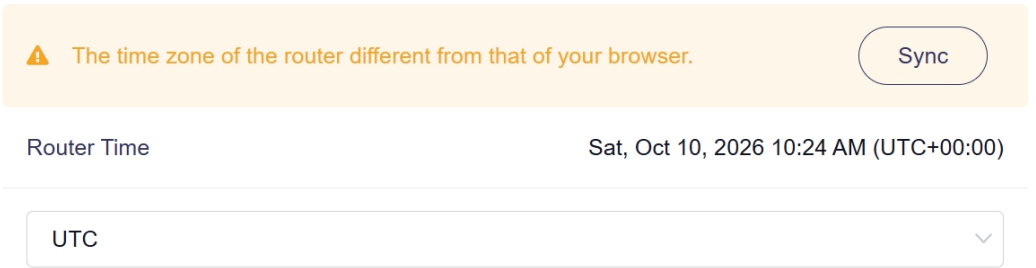
1. Długość od 10 do 63 znaków.
2. Dozwolone są litery (z rozróżnianiem wielkości), cyfry i symbole (np. ! @ # $ % ^ & * ( ) _ + - = , . > < | ? / \ [ ] { } : ; " ' ` ~).
3. Wymagane są co najmniej dwa rodzaje znaków spośród: wielkie litery, małe litery, cyfry i symbole.

13.5 Strefa czasowa

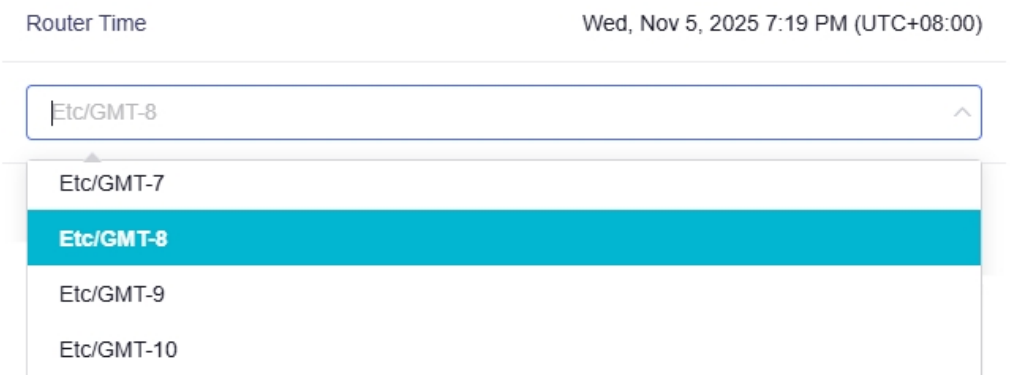
Zaloguj się do panelu administracyjnego routera i przejdź do **SYSTEM** > **Time Zone**. Strona wyświetla czas systemowy routera: datę, godzinę i odpowiadające im przesunięcie strefy czasowej.



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

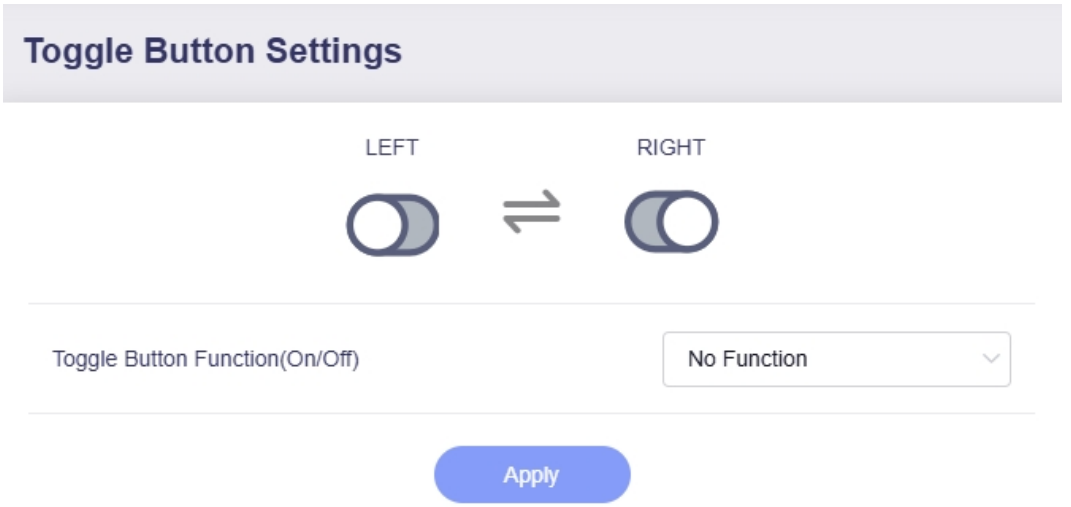


Aby zmienić strefę czasową, wybierz odpowiednią pozycję z listy, tak aby czas systemowy routera odpowiadał czasowi lokalnemu.

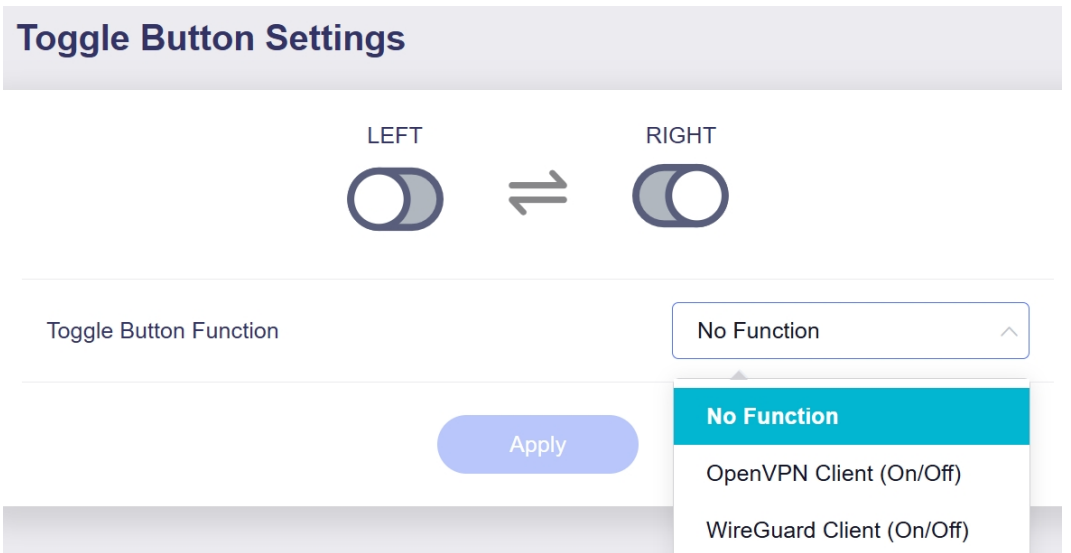


13.6 Ustawienia przełącznika

Zaloguj się do panelu administracyjnego routera i przejdź do **SYSTEM** > **Toggle Button Settings**. Tutaj możesz dostosować działanie fizycznego przełącznika z boku routera, aby ułatwić obsługę.

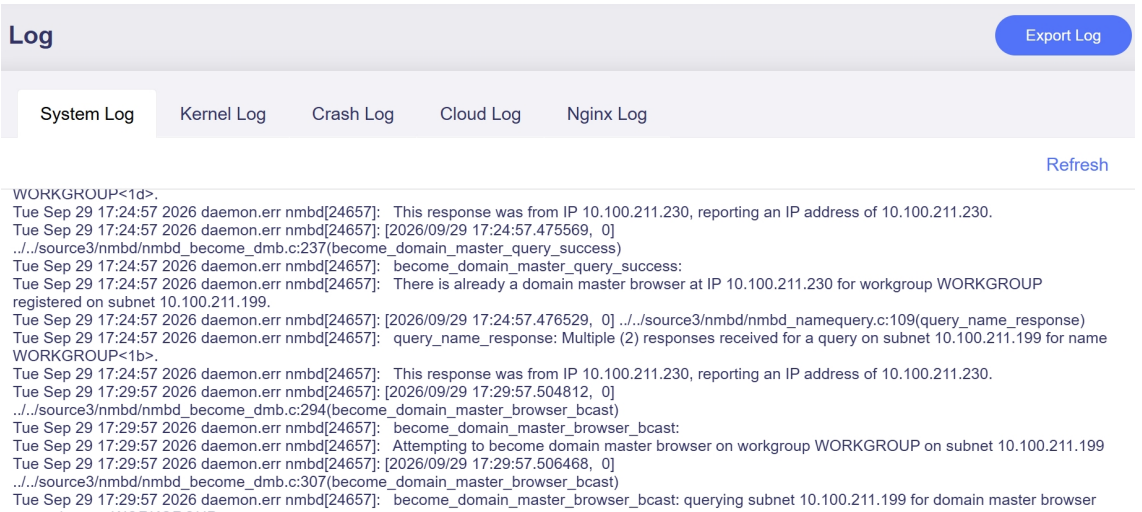


Domyślnie przełącznik nie ma przypisanej funkcji. W razie potrzeby możesz skonfigurować go tak, aby jednym ruchem włączać lub wyłączać określone funkcje.



13.7 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.

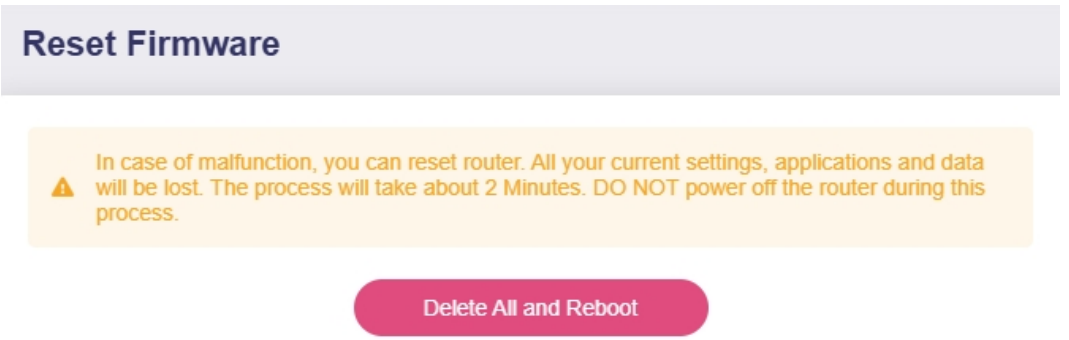


- **Refresh**: kliknij ten przycisk, aby odświeżyć dzienniki.
- **Export Log**: kliknij ten przycisk, aby wyeksportować informacje diagnostyczne wraz z dziennikami.

13.8 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.

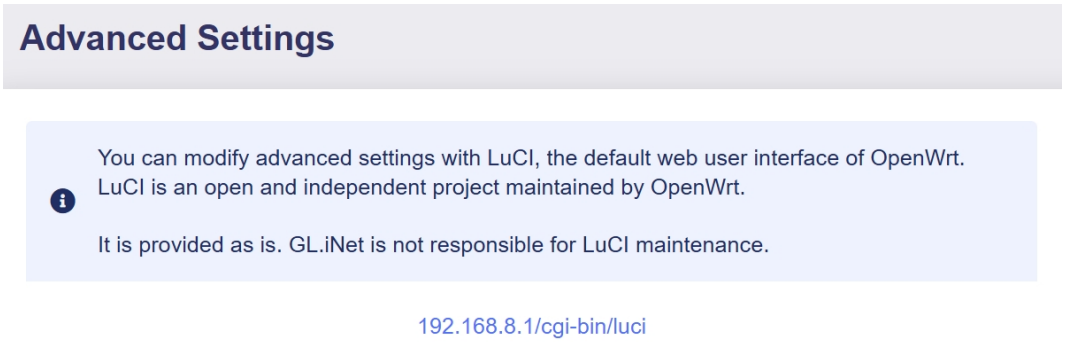
Jeśli panel administracyjny routera jest niedostępny, spróbuj zresetować router za pomocą fizycznego przycisku resetowania z boku urządzenia.

13.9 Ustawienia zaawansowane

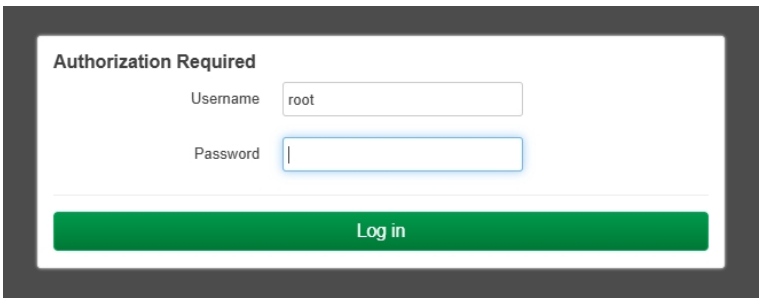
Zaloguj się do panelu administracyjnego routera i przejdź do **SYSTEM** > **Advanced Settings**. Tutaj możesz zmieniać ustawienia zaawansowane w LuCI, domyślnym interfejsie internetowym OpenWrt. LuCI to otwarty, niezależny projekt utrzymywany przez OpenWrt, udostępniany w obecnej postaci. GL.iNet nie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

Aby zalogować się do interfejsu LuCI, wykonaj poniższe czynności.

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



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



Otworzy się interfejs LuCI.

