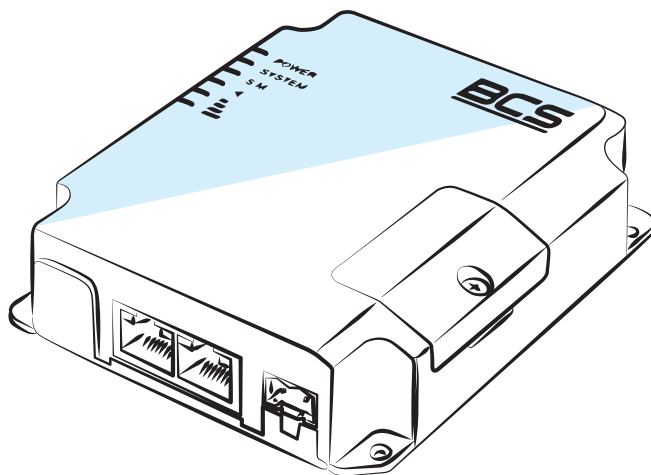


BCS-R4G-1W1L(-P)

Przemysłowy Router LTE z PoE

Instrukcja obsługi



www.bcs.pl

NSS Sp. z o.o. ul. Modułama 11 (Hala IV), 02-238 Warszawa
tel. +48 22 846 25 31, fax. +48 22 846 23 31 wew.140
e-mail: info@bcscctv.pl, NIP: 521-312-46-74

SPIS TREŚCI

1. Przedstawienie produktu	5
1.1 Profil produktu	5
1.2 Zawartość pudełka	5
1.3 Prezentacja urządzenia	5
2. Instalacja	7
2.1 Przygotowanie urządzenia do instalacji	7
2.2 Instalacja produktu	8
3. Podłączanie urządzenia	9
3.1 Instalacja karty SIM	9
3.2 Porty RJ45	9
3.3 Antena	9
3.4 Przed włączeniem zasilania routera	9
3.5 Uruchomienie urządzenia	9
3.6 Webserwis urządzenia	10
4. Webserwis	12
4.1 Status	12
4.1.1 Przegląd systemu	12
4.1.2 Modem LTE	12
4.1.3 Sieć	13
4.1.4 VPN	13
4.1.5 Routing	13
4.1.6 Lista urządzeń	14
4.2 Ustawienia sieciowe	14
4.2.1 Interfejsy	14
4.2.1.1 Link Failover	14
4.2.1.2 Modem LTE	16
4.2.1.3 Port	18
4.2.1.4 WAN	18
4.2.1.5 Interfejs lokalny	21
4.2.1.6 Switch	21
4.2.1.7 Interfejs pętli	21
4.2.2 DHCP	21
4.2.3 Firewall	25
4.2.3.1 Zabezpieczenia	25
4.2.3.2 ACL	26
4.2.3.3 Przekierowywanie portów	28
4.2.3.4 DMZ	29
4.2.3.5 MAC Binding	30
4.2.3.6 Własne reguły	31
4.2.3.7 SPI	32
4.2.4 QoS	33
4.2.5 VPN	35
4.2.5.1 DMVPN	35
4.2.5.2 IPsec Server	36
4.2.5.3 IPsec	39
4.2.5.4 GRE	42
4.2.5.5 L2TP	44
4.2.5.6 PPTP	46
4.2.5.7 Klient OpenVPN	47
4.2.5.8 Serwer OpenVPN	50
4.2.5.9 Certyfikaty	52
4.2.6 IP Passthrough	54
4.2.7 Routing	54
4.2.7.1 Routing statyczny	54
4.2.7.2 RIP	55
4.2.7.3 OSPF	57
4.2.7.4 Filtry routingu	62
4.2.8 VRRP	63
4.2.9 DDNS	64

4.3 Ustawienia systemowe	65
4.3.1 Ustawienia podstawowe	65
4.3.1.1 Główne	65
4.3.1.2 Data i czas	65
4.3.1.3 Email	66
4.3.2 Telefony i SMS	67
4.3.2.1 Telefony	67
4.3.2.2 SMS	68
4.3.3 Użytkownicy	69
4.3.3.1 Konto główne	69
4.3.3.2 Zarządzanie kontami	70
4.3.4 SNMP	70
4.3.4.1 SNMP	70
4.3.4.2 Widoki MIB	70
4.3.4.3 VACM	71
4.3.4.4 Trap	72
4.3.4.5 MIB	73
4.3.5 AAA	73
4.3.5.1 Radius	73
4.3.5.2 Tacacs+	74
4.3.5.3 LDAP	74
4.3.5.4 Autoryzacja	75
4.3.6 Zarządzanie zdalne	75
4.3.6.1 Device Managment	75
4.3.6.2 Cloud VPN	76
4.3.7 Zdarzenia	77
4.3.7.1 Lista zdarzeń	77
4.3.7.2 Ustawienia zdarzeń	77
4.4 Konserwacja	78
4.4.1 Narzędzia	78
4.4.1.1 Ping	78
4.4.1.2 Traceroute	78
4.4.1.3 Analiza pakietów	79
4.4.1.4 Qxdmlog	79
4.4.2 Debugger	80
4.4.2.1 Debbuger modemu	80
4.4.2.2 Debugger firewalla	80
4.4.3 Dziennik systemowy	81
4.4.3.1 Zdarzenia	81
4.4.3.2 Pobieranie	81
4.4.3.3 Log Settings	82
4.4.4 Aktualizacja	82
4.4.5 Kopia zapasowa	82
4.4.6 Restart	83
5. Specyfikacja techniczna	84
5.1 Tabela	84
5.2 Oprogramowanie	84
5.3 Najważniejsze funkcjonalności	84

1. PRZEDSTAWIENIE PRODUKTU

1.1 PROFIL PRODUKTU

BCS-R4G-1W1L to przemysłowy router LTE z rozbudowanymi funkcjami oprogramowania, dzięki którym możemy go zastosować w wielu instalacjach M2M/IoT. Obsługa standardu WCDMA i 4G LTE zapewnia dużą stabilność łącza z operatorami. Zastosowanie dwóch portów Fast Ethernet z czego jeden możemy ustawić jako port WAN pozwala na zwiększenie stabilności połączenia z Internetem, poprzez skonfigurowanie usługi „Link Failover”, która w przypadku problemów z dostępem do Internetu od jednego dostawcy przełączy router na drugiego dostawcę. Użycie podzespołów klasy przemysłowej zapewnia dużą stabilność przy niskim zużyciu energii. Zastosowane rozwiązania sprawiają, że router BCS-R4G-1W1L świetnie nadaje się m.in. do automatyki przemysłowej, instalacji monitoringu wizyjnego, sprzętu telemetrycznego, urządzeń płatniczych, urządzeń vendingowych i wielu innych.

1.2 ZAWARTOŚĆ PUDEŁKA

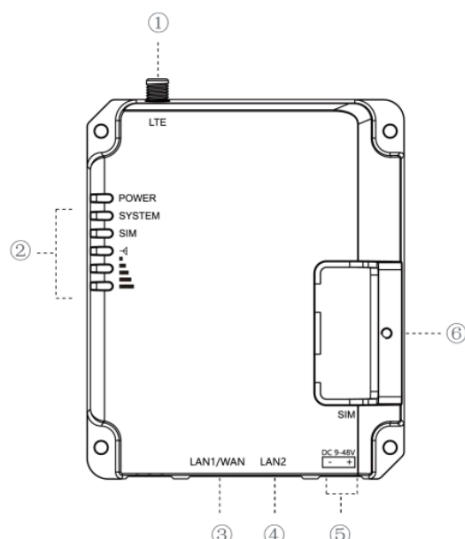
Po otwarciu pudełka proszę dokładnie sprawdzić jego zawartość. W pudełku znajdują się:

Zawartość	Ilość	Przeznaczenie
Router	1	-
Zasilacz 12V 1A	1	Zasilanie routera
Antena LTE	1	Zwiększenie zasięgu sieci
Uchwyt montażowy	1	Montaż na szynie TH35
Instrukcja obsługi	1	Niniejsza instrukcja

1.3 PREZENTACJA URZĄDZENIA

Opis elementów:






1. Gniazdo anteny
2. Wskaźniki LED
3. Port RJ45 LAN1/WAN
4. Port RJ45 LAN2
5. Gniazdo zasilania
6. Osłona gniazda karty SIM i przycisku RESET

Gniazdo anteny

Gniazdo służące do podłączenia anteny poprawiającej zasięg sieci komórkowej, która dołączona jest do zestawu.

Wskaźniki LED

Wskaźnik	Nazwa	Kolor	Stan pracy	Opis
POWER	Wskaźnik LED zasilania	Zielony	Świeci	Zasilanie w normie
			Nie świeci	Brak zasilania, zasilanie routera nie prawidłowe
SYSTEM	Wskaźnik systemowy	Zielony	Nie świeci	Jeśli wskaźnik POWER świeci router jest w trybie uruchamiania systemu
			Mruga	System działa prawidłowo
		Czerwony	Świeci	System nie działa prawidłowo
SIM	Wskaźnik zainstalowania karty SIM	Zielony	Świeci	Karta SIM prawidłowo połączyła się operatorem
			Mruga	Powoli: karta SIM zarejestrowana, oczekuje na polecenie połączenia (sekcja 4.2.1.2) Szybko: karta SIM jest w trybie łączenia z operatorem
			Nie świeci	Brak karty SIM, brak połączenia z operatorem
	Wskaźnik siły sygnału sieci komórkowej	Zielony	Świeci	Im więcej wskaźników zapalonych tym lepszy zasięg sieci GSM
			Nie świeci	Brak zasięgu sieci komórkowej

Port RJ45 LAN1/WAN

Port Fast Ethernet (10/100 Mbps), port LAN1 może również pełnić rolę portu WAN dzięki czemu możemy zapewnić redundancję połączenia z Internetem (sekcja 4.2.1.3).

Port RJ45 LAN2

Port Fast Ethernet (10/100 Mbps).

Gniazdo zasilania

Gniazdo w standardzie PCB służące do podłączenia zasilacza. Prąd stały DC 9-48V.

Osłona gniazda karty SIM i przycisku RESET

Po odkręceniu osłony ukaże się gniazdo służące do zamontowania karty SIM w standardowym rozmiarze oraz przycisk reset, który przywraca ustawienia fabryczne routera.

2. INSTALACJA

2.1 PRZYGOTOWANIE URZĄDZENIA DO INSTALACJI



UWAGA!

Unikaj niewłaściwego użytkownika urządzenia. Istnieje ryzyko uszkodzenia sprzętu jak i doznanie obrażeń ciała. Uważnie zapoznaj się z poniższymi wytycznymi dotyczącymi środowiska instalacji urządzenia.

Elementy wymagające uwagi podczas instalacji:

- Upewnij się, że urządzenie nie jest podłączone do zasilania, użyj opaski antystatycznej upewniając się, że dobrze przylega do skóry nadgarstka;
- Router działa prawidłowo gdy zasilany jest prawidłowym prądem. Upewnij się, że napięcie zasilania zgodne jest z oznaczeniem na urządzeniu;
- Przed podłączeniem zasilania do routera, upewnij się, że nie spowoduje to zwarcia w instalacji elektrycznej gdyż może to uszkodzić router;
- Unikaj porażenia prądem elektrycznym, nie otwieraj obudowy routera nawet gdy nie jest podłączony do zasilania;
- Przed czyszczeniem urządzenia odłącz je od źródła zasilania, nie używaj mokrej ściereki ani płynnych czyszczywi

Temperatura i wilgotność:

W celu zapewnienia długotrwałej i stabilnej pracy routera należy przestrzegać warunków w środowisku pracy urządzenia. Zbyt niska lub wysoka wilgotność może doprowadzić do upływu prądu przez izolatory, doprowadzić do rdzewienia elementów, a nawet przyspieszyć proces starzenia się urządzenia. Praca w wysokiej temperaturze prowadzi do szybszego zużywania się układów elektronicznych. Zakres temperatury i wilgotności definiuje poniższa tabelka:

Opis środowiska	Temperatura	Względna wilgotność
Użytkowanie	-40°C-60°C	0% – 95% nieskondensowana
Przechowywanie	-40°C-85°C	0% – 95% nieskondensowana

Wysokość n.p.m.



Jeśli na produkcie widnieje niniejsza ikona oznacza to, że urządzenie może być używane na wysokości nie większej niż 2000 m nad poziomem morza.

Zapylenie, zakurzenie

Opadający kurz i pyły na powierzchnię routera mogą powodować absorpcję elektrostatyczną, utrudniając dotykaniu metalowych elementów punktów przyłączeniowych. Produkt dokonuje pomiaru antystatyczności, ale po przekroczeniu maksymalnego poziomu występuje ryzyko zniszczenia części składowych płytki PCB. W celu uniknięcia wpływu elektryczności statycznej na urządzenie należy: regularnie czyścić urządzenie z kurzu; utrzymywać odpowiednią czystość powietrza w pomieszczeniu; zapewnić dobre uziemienie dla urządzenia, gwarantujące płynne przenoszenie elektryczności statycznej.

Zakłócenia elektromagnetyczne

Silne pole elektromagnetyczne może wpływać na wewnętrzne układy routera. Aby zmniejszyć ryzyko uszkodzenia urządzenia upewnij się, że: system zasilania posiada odpowiednie zabezpieczenia; router powinien znajdować się z dala od zasilania o wysokiej częstotliwości takich jak urządzenia wysokoprądowe, systemy zasilania indukcyjnego. W razie potrzeby proszę wykonać pomiar ekranowania elektromagnetycznego.

Uziemienie

W momencie uderzenia pioruna pojawia się bardzo duży prąd, a powietrze na drodze wyładowania momentalnie podgrzewa się do 20 000°C, czynniki te z pewnością uszkodzą urządzenie. Można zmniejszyć ryzyko stosując kilka zasad: upewnij się, że szafa, w której znajduje się urządzenie ma dobry kontakt z podłożem; upewnij się, że gniazdko zasilania posiada instalację przeciwprzebieciową; używaj dobrej jakości okablowania; w przypadku zastosowania okablowania na zewnątrz zaleca się stosowanie instalacji odgromowej wprowadzonej do ziemi.

Wymagania montażowe

Router instalowany jest na szynie TH35 lub płaskiej powierzchni, do której można go przykręcić śrubami. Upewnij się, że w miejscu montażowym jest wystarczająca ilość miejsca oraz, że szyna lub płyta, do której montowane jest urządzenie wytrzyma ciężar przynajmniej 1kg; upewnij się, że miejsce instalacji posiada system chłodzenia/ogrzewania, które zapewnią urządzeniu pracę w optymalnych warunkach.

Przydatne narzędzia

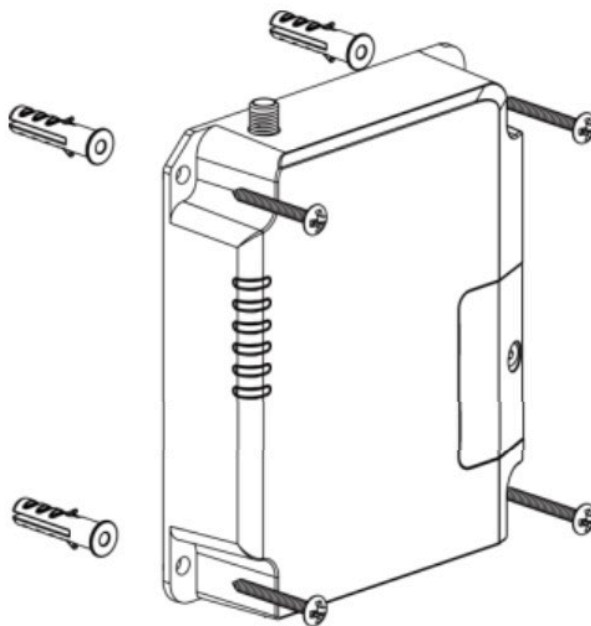
Podczas instalowania routera mogą być potrzebne narzędzia takie jak: śrubokręty; opaska antystatyczna na nadgarstek; kabel sieciowy. Proszę samodzielnie zadbać o dostęp do tych narzędzi.

2.2 INSTALACJA PRODUKTU

Urządzenie można położyć na biurku, zamontować na ścianie lub szynie DIN.

Instalacja na ścianie

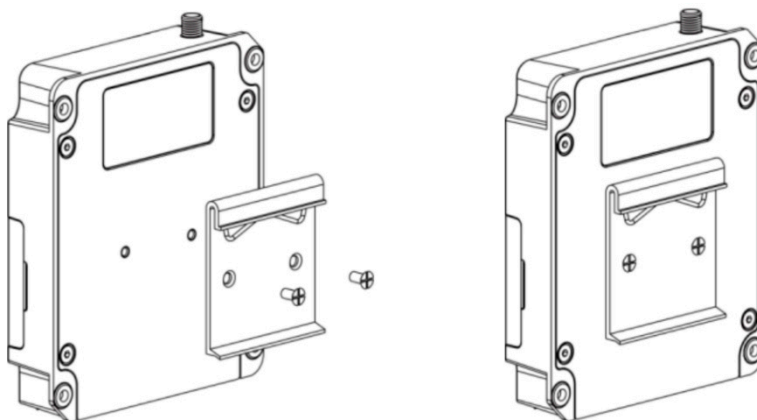
W przypadku chęci zainstalowania na ścianie należy wywiercić dziury montażowe, a następnie użyć dziur przygotowanych w obudowie do montażu naściennego.



Instalacja na szynie DIN TH35

Router zaprojektowany jest tak, aby można było go zainstalować na standardowej szynie DIN TH35 używanej w szafach sterowniczych i elektrycznych, można go łatwo zainstalować wykonując poniższe czynności:

1. Uchwyt na szynę TH35 zamontuj do urządzenia używając do tego śrubek z zestawu z siłą 1-1,2 Nm



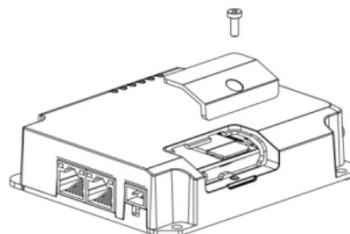
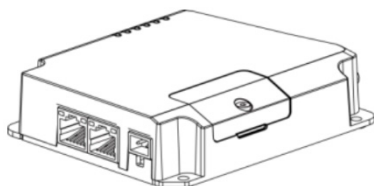
2. Zamontuj router na szynie DIN TH35. Upewnij się, że router zamontowany jest równo i stabilnie

3. PODŁĄCZANIE URZĄDZENIA

3.1 INSTALACJA KARTY SIM

Router przystosowany jest do pracy z kartami SIM, którą instalujemy wykonując poniższe kroki:

1. Odkręć osłonę chroniącą gniazdo oraz przycisk RESET
2. Wsuń kartę w gniazdo SIM1 chipem do dołu w sposób zaprezentowany na gnieździe i przykręć osłonę



3.2 PORTY RJ45

Używając kabla Ethernet podłącz jeden koniec z portem w routerze, a drugi z urządzeniem końcowym; port LAN1/WAN może służyć zarówno jako port LAN, a także jako port WAN (sekcja 4.2.1.3) dzięki czemu możemy zapewnić redundancję dostępu do sieci Internet urządzeniom za routerem, które podłączone są do portu LAN2.



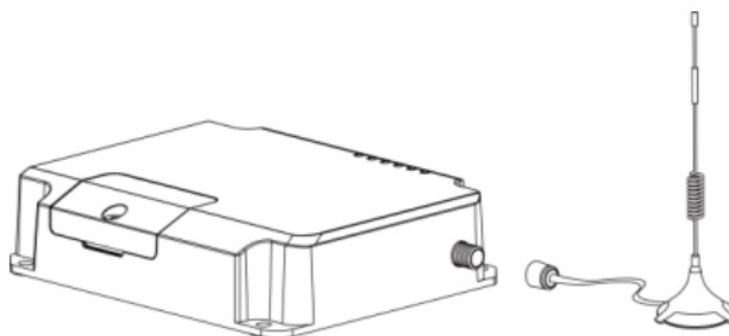
UWAGA!

Jeśli do routera podłączone są urządzenia takie jak stacja robocza, serwer, switch lub inne urządzenie sieciowe to długość kabla nie może przekroczyć 100 metrów.

Funkcja auto-flip (Auto-MDI/MDIX) rozpoznaje czy zastosowany kabel Ethernet kat.5 jest kablem standardowym czy z przeplotem. Nie używaj portu RJ45 do podłączania kabla telefonicznego.

3.3 ANTENA

W zestawie z routerem otrzymujesz antenę, która ma kabel zakończony wtykiem pasującym do gniazda w routerze. Aby zainstalować antenę należy umieścić ją w dogodnym miejscu, a następnie przykręcić kabel do gniazda anteny w routerze. Aby zapewnić jak najlepszy sygnał antena powinna być zamontowana pionowo.



UWAGA!

Antena mocowana jest do powierzchni za pomocą magnesu. Należy upewnić się, że magnes ten nie będzie miał wpływu na urządzenie lub powierzchnie, do której zamocowana będzie antena.

3.4 PRZED WŁĄCZENIEM ZASILANIA ROUTERA

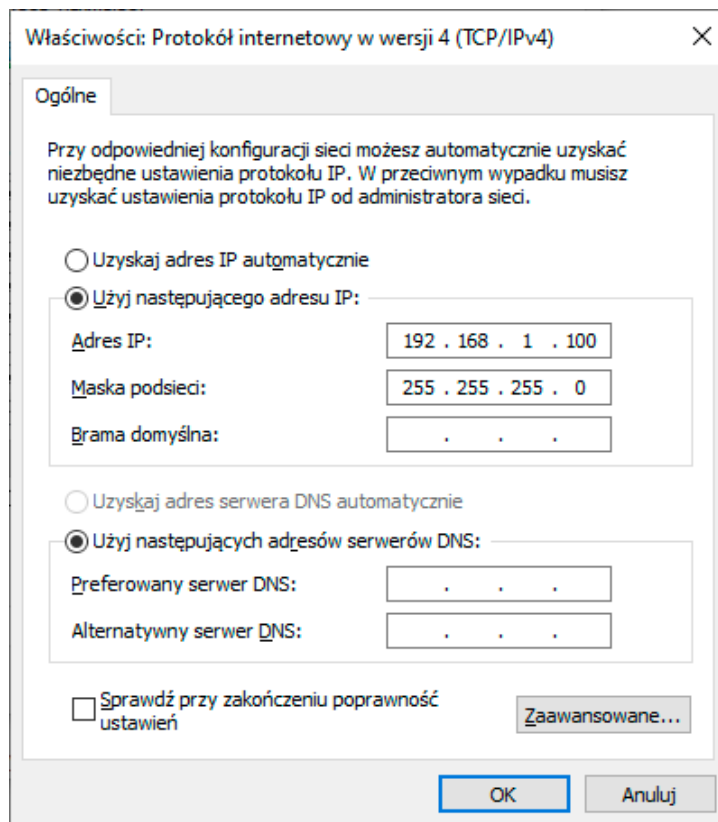
- Sprawdź czy napięcie zasilania jest zgodne ze specyfikacją urządzenia
- Sprawdź czy zasilacz, router, miejsce montażu są odpowiednio uziemione
- Sprawdź czy router jest prawidłowo podłączony do innych urządzeń

3.5 URUCHOMIENIE URZĄDZENIA

Po włączeniu zasilania router automatycznie się zainicjuje. Inicjalizacja prezentowana jest w następujący sposób: po włączeniu zasilania na ok. 1s zaświecą się wszystkie wskaźniki LED, następnie zapalony pozostanie jedynie wskaźnik POWER, w momencie kiedy wskaźnik SYSTEM zacznie migać na zielono urządzenie jest gotowe do użytku.

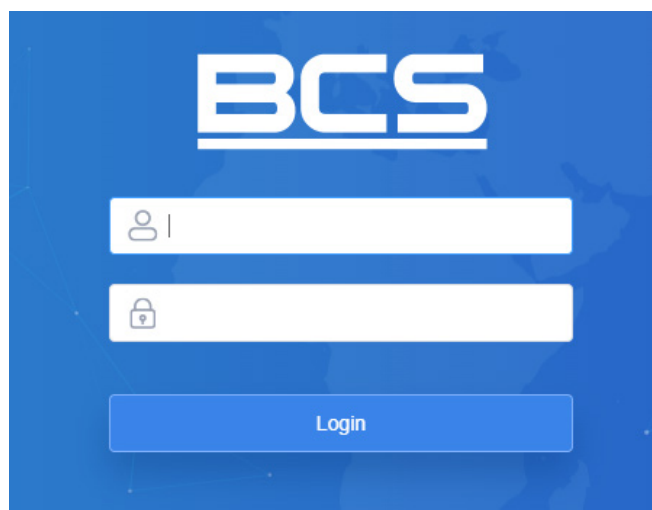
3.6 WEBSERWIS URZĄDZENIA

1. Podłącz komputer do routera za pomocą kabla Ethernet, wykorzystując dowolny port RJ45
2. Ręcznie ustaw adres IP komputera na dowolny z zakresu 192.168.1.xxx, maska podsieci 255.255.255.0



Rysunek 3.1 Ustawienia karty sieciowej

3. Otwórz przeglądarkę internetową i w polu adresu wpisz 192.168.1.1 i potwierdź klawiszem Enter
4. Wprowadź użytkownika (domyślnie admin) i hasło (domyślnie password) i kliknij Login



Rysunek 3.2 Okno logowania

5. Prawidłowa przeprowadzona procedura doprowadzi do wyświetlenia podobnego ekranu; teraz można rozpocząć zarządzanie konfiguracją routera

The screenshot shows the BCS web interface. At the top, there is a navigation bar with the BCS logo and a user profile 'admin'. Below the navigation bar, a warning message reads: 'Dla bezpieczeństwa urządzenia proszę zmienić domyślne hasło'. The main content area is divided into several sections:

- Przegląd systemu:** A table with columns for 'O urządzeniu' and 'Stan urządzenia'.

O urządzeniu	Stan urządzenia
Model: BCS-R4G-1W1L	Data i godzina: 2022-02-23 12:26:22 Wednesday
Numer seryjny: 6224B4020498	Czas działania: 22:53:01
Wersja oprogramowania: 32.3.0.4	Zajętość CPU: 15%
Wersja sprzętowa: V3.0	RAM (Dostępna/Ogółem): 39MB/128MB(30.47%)
	Flash (Dostępna/Ogółem): 83MB/128MB(64.84%)
- Modem LTE:**

Status: No SIM Card
IPv4: 0.0.0.0/0
IPv6: -
Czas połączenia: 0 days, 00:00:00
Zużycie danych (miesięczne): 0.0 MIB
- LAN:**

IPv4: 192.168.126.253/21
IPv6: fe80::7403:10ff:fe73:2b22/64
Podłączone urządzenia: 1
- Help:** A sidebar menu with expandable sections:
 - Model:** Model urządzenia.
 - Numer seryjny:** Numer seryjny urządzenia.
 - Wersja oprogramowania:** Wersja oprogramowania zainstalowanego na urządzeniu.
 - Wersja sprzętowa:** Wersja sprzętowa urządzenia.
 - Data i godzina:** Data i godzina ustawiona na urządzeniu.
 - Czas działania:** Czas, który upłynął od momentu uruchomienia urządzenia.
 - Zajętość CPU:** Procentowe użycie procesora.
 - RAM (Dostępna/Ogółem):** Wyświetla dostępną i ogólną ilość pamięci RAM.
 - Flash (Dostępna/Ogółem):** Wyświetla dostępną i ogólną ilość pamięci FLASH.
 - Zużycie danych (miesięczne):** Wyświetla zużycie danych w obecnym okresie rozliczeniowym.

At the bottom right, there are buttons for 'Odświeżanie ręcz.' and 'Odśwież'.

Rysunek 3.3 Strona główna webserwisu

**UWAGA!**

Podczas pierwszego logowania należy zmienić domyślne hasło na odpowiednio silne, aby dodatkowo zabezpieczyć urządzenie. Do momentu zmiany hasła po zalogowaniu wyświetlane będzie okienko przypominające o zmianie hasła.

4. WEBSERWIS

4.1 STATUS

Zakładka status zawiera aktualne informacje o statusie urządzenia w różnych kategoriach. W prawym dolnym rogu możemy odświeżyć dane manualnie lub ustawić odświeżanie automatyczne w określonych interwałach czasowych.

4.1.1 Przegląd systemu

W zakładce przegląd systemu prezentowane są podstawowe informacje na temat urządzenia podzielone na grupy

Grupa	Informacje
O urządzeniu	<ul style="list-style-type: none"> • Model • Numer seryjny • Wersja oprogramowania • Wersja sprzętowa
Stan urządzenia	<ul style="list-style-type: none"> • Aktualny czas ustawiony w urządzeniu • Czas od uruchomienia • Zajętość procesora • Zajętość pamięci RAM • Zajętość pamięci FLASH
Modem LTE	<ul style="list-style-type: none"> • Status karty SIM • Przydzielone przez operatora IPv4 • Przydzielone przez operatora IPv6 • Czas połączenia • Ilość zużytych danych w miesiącu
WAN	<ul style="list-style-type: none"> • Status portu WAN • Przydzielony przez operatora IPv4 • Przydzielony adres IPv6 • Adres MAC interfejsu • Czas połączenia
LAN	<ul style="list-style-type: none"> • Adres IPv4 routera • Adres IPv6 routera • Ilość podłączonych urządzeń

4.1.2 Modem LTE

W zakładce modem LTE znajdziemy informacje dotyczące naszego połączenia z siecią komórkową podzielone na grupy

Grupa	Informacje
Modem	<ul style="list-style-type: none"> • Model modemu • Wersja modemu • Siła sygnału • Status karty SIM • Numer IMEI modemu • Numer IMSI karty SIM • Numer ICCID karty SIM • Dostawca usługi • Typ połączenia (LTE, 3G itp.) • Aktualny numer PLMN ID • Kod lokalizacji dla karty SIM (LAC) • Numer CELL ID
Sieć	<ul style="list-style-type: none"> • Status połączenia do sieci operatora • Adres IPv4 ze skróconym zapisem maski podsieci • Brama dla IPv4 • DNS dla IPv4 • Adres IPv6 • Brama dla IPv6 • DNS dla IPv6 • Czas połączenia
Zużycie danych (miesięczne)	<ul style="list-style-type: none"> • Ilość danych wysłanych (Tx) • Ilość danych odebranych (Rx) • Ilość danych łącznie z ostatnich 30 dni

4.1.3 Sieć

Zakładka sieć wyświetla informacje dotyczące naszego połączenia z siecią LAN i opcjonalnie z siecią WAN za pomocą kabla. Część informacji widoczna jest po ustawieniu portu LAN1/WAN jako port WAN.

Grupa	Informacje
WAN-IPv4 (widoczne tylko w momencie ustawienia portu LAN1/WAN jako WAN)	<ul style="list-style-type: none"> • Systemowa nazwa portu • Status połączenia • Typ połączenia (DHCP/IP statyczne) • Adres IPv4 • Brama dla IPv4 • DNS dla IPv4 • Czas połączenia
WAN-IPv6 (widoczne tylko w momencie ustawienia portu LAN1/WAN jako WAN)	<ul style="list-style-type: none"> • Systemowa nazwa portu • Status połączenia • Typ połączenia (DHCP/IP statyczne) • Adres IPv6 • Brama dla IPv6 • DNS dla IPv6 • Czas połączenia
Bridge	<ul style="list-style-type: none"> • Nazwa interfejsu • Status protokołu STP • Adres IPv4 • Adres IPv6 • Lista VLANów należących do interfejsu

4.1.4 VPN

Zakładka VPN zawiera informacje o połączeniach routera do sieci VPN jako klient oraz o tym jakie urządzenia podłączone są do routera jako klienci VPN.

Grupa	Informacje
Klient	<ul style="list-style-type: none"> • Nazwa połączenia routera jako klient • Status połączenia do serwera VPN • IP lokalne routera • Adres IP serwera VPN
Serwer	<ul style="list-style-type: none"> • Status serwera OpenVPN na routerze • Status serwera Ipsec na routerze
Lista połączeń	<ul style="list-style-type: none"> • Serwer z jakiego korzysta klient • IP klienta • Czas połączenia klienta

4.1.5 Routing

Zakładka routing zawiera informacje z tablicy routingu urządzenia.

Grupa	Informacje
Tabela routingu	<ul style="list-style-type: none"> • Docelowy adres urządzenia • Maska podsieci (IPv4) lub prefiks sieci (IPv6) • Brama • Interfejs z jakiego korzysta klient • Metryka routingu
Pamięć ARP	<ul style="list-style-type: none"> • Adres IP klienta • MAC adres przypisany do IP klienta • Interfejs z jakiego korzystał klient

4.1.6 Lista urządzeń

Zakładka lista urządzeń wyświetla dane o klientach podłączonych do routera za pomocą protokołu DHCP w dwóch grupach. Grupa klienci DHCP wypisuje klientów, którym router przydzielił IP automatycznie, a grupa MAC Binding wyświetla listę klientów, którzy adres IP mają przypisany do adresu MAC/DUID

Grupa	Informacje
Klienci DHCP	<ul style="list-style-type: none"> • Adres IP klienta • Adres MAC/DUID klienta • Pozostały czas rezerwacji adresu IP dla klienta
MAC Binding	<ul style="list-style-type: none"> • Adres IP klienta • Adres MAC/DUID klienta

4.2 USTAWIENIA SIECIOWE

4.2.1 Interfejsy

4.2.1.1 Link Failover

Zakładka **Link Failover** pozwala nam ustawić redundancję połączenia z Internetem za pomocą karty SIM lub portu LAN1/WAN jeśli port ten ustawimy w tryb pracy jako WAN (sekcja 4.2.1.3), w przeciwnym wypadku w funkcji tej zobaczymy tylko interfejs karty SIM.

Grupa **Priorytety interfejsów** odpowiada za wybór kolejności interfejsów z jakich ma korzystać router podczas dostępu do Internetu, wyświetla podstawowe dane połączenia z Internetem oraz pozwala ustawić parametry funkcji **Detekcja PING**, która sprawdza czy interfejsy mają połączenie z Internetem.

Zaznaczenie przy wybranym interfejsie opcji **Włącz usługę** oznacza, że interfejs będzie brał udział w redundancji połączeń.

Priorytet	Włącz usługę	Używane połączenie	Interfejs	Typ połączenia	IP	Operacja
1	<input checked="" type="checkbox"/>	●	WAN	DHCP	-	[edit] [up] [down]
2	<input checked="" type="checkbox"/>	●	Cellular-SIM1	DHCP	-	[edit] [up] [down]

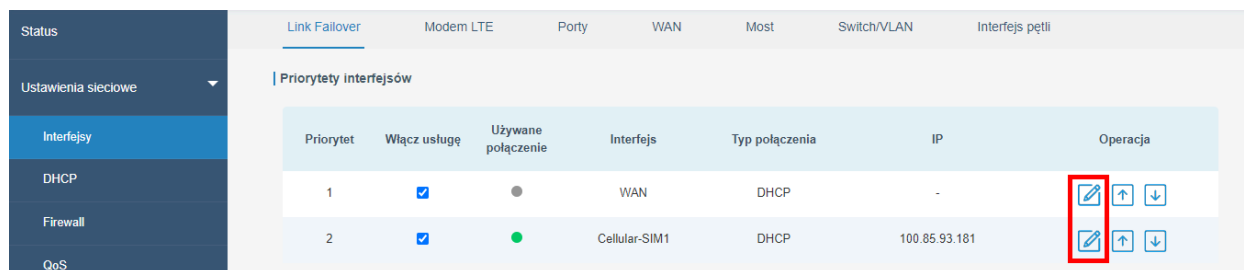
Rysunek 4.1 Funkcja Włącz usługę

Środkowa część tabelki pozwala uzyskać informację aktualnie wykorzystywanym interfejsie przy połączeniu z siecią Internet (**Używane połączenie**), nazwie interfejsu (**Interfejs**), typie połączenia (**Typ połączenia**) oraz IP jakie otrzymał interfejs (**IP**).

Priorytet	Włącz usługę	Używane połączenie	Interfejs	Typ połączenia	IP	Operacja
1	<input checked="" type="checkbox"/>	●	WAN	DHCP	-	[edit] [up] [down]
2	<input checked="" type="checkbox"/>	●	Cellular-SIM1	DHCP	100.85.93.181	[edit] [up] [down]

Rysunek 4.2 Informacje o interfejsach

Konfigurację funkcji **Detekcja PING** uruchamiamy klikając na ikonę kartki i ołówka przy wybranym interfejsie.



Rysunek 4.3 Ikona Ping Detecion

Po kliknięciu w powyższą ikonę wyskoczy nam okno służące do konfiguracji funkcji **Detekcja PING**, w którym możemy ustawić: czy funkcja ma być uruchomiona dla danego interfejsu (**Włącz**), adresy pierwszego oraz drugiego serwera, który odpytywała będzie funkcja dla IPv4 (**IPv4 pierwszy serwer**, **IPv4 drugi serwer**); pierwszego oraz drugiego serwera, który odpytywała będzie funkcja dla IPv6 (**IPv6 pierwszy serwer**, **IPv6 drugi serwer**); czas odstępu między kolejnymi wywołaniami funkcji wyrażony w sekundach (**Interwał**); czas odstępu do ponownego wywołania funkcji jeśli za pierwszym razem nie będzie odpowiedzi od serwerów wyrażony w sekundach (**Czas ponowienia**); czas jaki funkcja będzie oczekiwała na odpowiedź wyrażony w sekundach (**Czas oczekiwania na odpowiedź**); ilość prób wykonania funkcji przed stwierdzeniem przez router, że interfejs nie ma połączenia z siecią Internet (**Maksymalna ilość prób**).

Detekcja Ping

Włącz

IPv4 pierwszy serwer: 8.8.8.8

IPv4 drugi serwer: 114.114.114.114

IPv6 pierwszy serwer: 2001:4860:4860::8888

IPv6 drugi serwer: 2400:3200::1

Interwał: 300 s

Czas ponowienia: 5 s

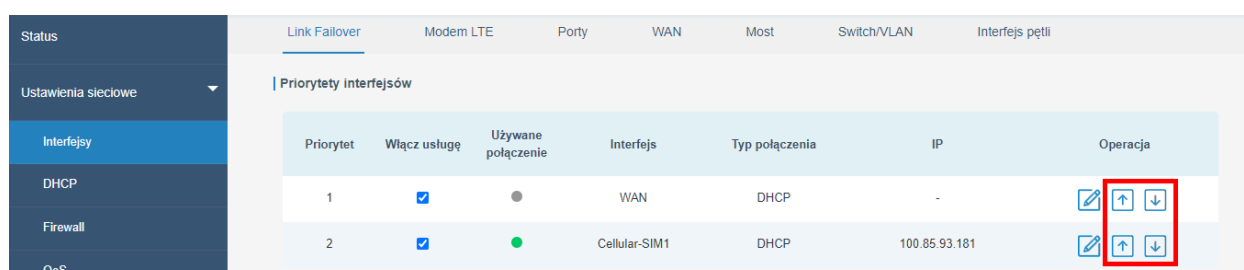
Czas oczekiwania na odpowiedź: 3 s

Maksymalna ilość prób: 3

OK Anuluj

Rysunek 4.4 Konfiguracja Detekcja PING

Aby zmienić kolejność interfejsów należy kliknąć na strzałki przy wybranym interfejsie co spowoduje jego przesunięcie w górę lub dół na liście priorytetów.



Rysunek 4.5 Zmiana priorytetów interfejsów

Grupa **Ustawienia** odpowiada za ustawienia czasu, po którym router spróbuje przełączyć się na interfejs o wyższym priorytecie wyrażony w sekundach (**Czas powrotu**), jeśli ustawimy ten czas na 0s to funkcja nie będzie próbowała przełączyć się na wyższy priorytet, dodatkowo w przypadku braku łączności na wszystkich interfejsach możemy zmusić router do restartu zaznaczając funkcję **Awaryjny restart**.

Ustawienia

Czas powrotu s

Awaryjny restart

Rysunek 4.6 Ustawienia przełączania na interfejs o wyższym priorytecie

4.2.1.2 Modem LTE

Zakładka **Modem LTE** pozwala nam skonfigurować interfejs odpowiedzialny za połączenie z siecią Internet poprzez kartę SIM. W grupie **Ustawienia modemu LTE** możemy wybrać: czy chcemy korzystać z połączenia IPv4 czy IPv6 (**Typ protokołu**); podać nazwę APN naszego dostawcy (**APN**); nazwę użytkownika (**Nazwa użytkownika**); hasło dostępu (**Hasło**); kod PIN do karty SIM (**Kod PIN**); numer telefonu centrum Internetowego dostawcy (**Numer centrum dostępowego**); typ autoryzacji połączenia wymagany przez operatora (**Typ autoryzacji**); rodzaj połączenia z jakiego będzie korzystał router np. „tylko 4G” albo tryb „auto” (**Typ sieci**); czy korzystać z protokołu PPP (**Preferowane PPP**); numer telefonu centrum SMS operatora, dzięki któremu router będzie mógł obsługiwać wiadomości SMS (**Centrum SMS**); uruchomić usługę NAT na routerze (**Włącz NAT**); uruchomić przesyłanie danych w roamingu (**Roaming**); ustawić limit danych dla karty SIM (**Limit danych**); dzień miesiąca, który jest dniem rozliczeniowym u dostawcy (**Dzień rozliczeniowy**)

Status	Link Failover	Modem LTE	Porty	WAN	Most
Ustawienia sieciowe	Ustawienia modemu LTE				
Interfejsy	Typ protokołu	IPv4			
DHCP	APN	internet			
Firewall	Nazwa użytkownika				
QoS	Hasło				
VPN	Kod PIN			
IP Passthrough	Numer centrum dostępowego				
Routing	Typ autoryzacji	Auto			
VRRP	Typ sieci	Auto			
DDNS	Preferowane PPP	<input type="checkbox"/>			
Ustawienia systemowe	Centrum SMS				
Konserwacja	Włącz NAT	<input checked="" type="checkbox"/>			
	Roaming	<input checked="" type="checkbox"/>			
	Limit danych	0 MB			
	Dzień rozliczeniowy	1 dzień miesiąca			

Rysunek 4.7 Konfiguracja połączenia z dostawcą Internetu

Grupa **Ustawienia połączenia** odpowiada za to kiedy router ma łączyć się z siecią Internet za pomocą karty SIM (**Tryb połączenia**), może on być połączony cały czas przy wyborze opcji „**Zawsze połączone**” lub łączyć się na nasze polecenie przy wyborze opcji „**Połączenie na żądanie**” po otrzymaniu wiadomości SMS (**Wywołanie SMS**) lub połączenia telefonicznego (**Wywołanie połączeniem**). Dodatkowo możemy ustawić przerwę między kolejnymi próbami połączenia z operatorem wyrażoną w sekundach (**Interwał ponownych połączeń**) oraz czas bezczynności po jakim router rozłączy się z operatorem przy wyborze opcji połączenia na żądanie wyrażony w sekundach (**Maksymalny czas bezczynności**).

Ustawienia połączenia	
Tryb połączenia	Zawsze połączone ▾
Interwał ponownych połączeń (s)	5

Rysunek 4.8 Wybrane ciągłe połączenie z operatorem

Połączenie na żądanie

Aby skonfigurować łączenie z operatorem na żądanie należy:

1. Wybrać „Połączenie na żądanie” w opcji **Tryb połączenia**

Ustawienia połączenia	
Tryb połączenia	Połączenie na żądanie ▾
Interwał ponownych połączeń (s)	5
Maks. czas bezczynności (s)	60
Wywołanie połączeniem	<input type="checkbox"/>
Wywołanie SMS	<input type="checkbox"/>

Rysunek 4.9 Wybrane połączenie na żądanie

2. Wybrać czy połączenie ma być wyzwalane za pomocą połączenia telefonicznego (**Wywołanie połączeniem**) i/lub wiadomości SMS (**Wywołanie SMS**),
3. W przypadku wyboru wywołania za pomocą połączenia telefonicznego należy wybrać grupę numerów telefonów, które będą miały taką możliwość (**Grupa dzwoniąca**), a w przypadku wywołania za pomocą wiadomości SMS należy wybrać grupę numerów (**Grupa SMS**) oraz treść wiadomości (**Treść SMS**). Grupy numerów opisane są w sekcji 4.3.2,

Ustawienia połączenia	
Tryb połączenia	Połączenie na żądanie ▾
Interwał ponownych połączeń (s)	5
Maks. czas bezczynności (s)	60
Wywołanie połączeniem	<input checked="" type="checkbox"/>
Grupa dzwoniąca	1 ▾
Wywołanie SMS	<input checked="" type="checkbox"/>
Grupa SMS	1 ▾
Treść SMS	connectcommand

Rysunek 4.10 Konfiguracja połączenia na żądanie

4. Po wybraniu ustawień należy kliknąć na przycisk **SAVE**



UWAGA!

Dane konfiguracyjne podane w powyższej sekcji są przykładowe, aby uzyskać prawidłowe dane do połączenia należy skontaktować się z operatorem obsługującym wybraną kartę SIM.

4.2.1.3 Port

W zakładce **Port** możemy skonfigurować jak mają działać porty RJ45 w routerze. Można je wyłączyć lub włączyć (**Stan**); dla portu LAN1/WAN możemy ustawić w jakim trybie ma działać LAN czy WAN (**Typ**); prędkość z jaką mają działać poszczególne porty (**Prędkość**); typ połączenia z jakiego mają korzystać porty **Full duplex/Half duplex/auto (Duplex)**.

Port	Stan	Typ	Prędkość	Duplex
LAN1/WAN	up	lan	auto	auto
LAN2	up	lan	auto	auto

Rysunek 4.11 Konfiguracja działania portów RJ45

4.2.1.4 WAN

Zakładka **WAN** służy do skonfigurowania portu WAN, aby uzyskać połączenie z Internetem. Możemy skonfigurować tutaj 5 typów połączenia: ręczna konfiguracja IP (**Styczne IP**); klient DHCP dla IPv4 (**Klient DHCP**); korzystanie z protokołu PPPoE (**PPPoE**); klient DHCP dla IPv6 (**Klient DHCPv6**); korzystanie z technologii Dual-Stack Lite (**Dual-Stack Lite**). Poniżej opisane zostaną wszystkie typy połączeń.

Ręczna konfiguracja IP/Styczne IP

Aby skonfigurować ten typ połączenia należy podać: adres IPv4 interfejsu WAN w routerze (**Adres IPv4**); maskę podsieci dla powyższego IPv4 (**Maska podsieci**); bramę domyślną dla IPv4 (**Brama IPv4**); adres IPv6 interfejsu WAN w routerze (**Adres IPv6**), w powyższym polu wpisany jest domyślny adres interfejsu wyliczany na podstawie adresu MAC interfejsu w routerze; długość prefiksu dla IPv6 (**Długość prefiksu**), bramę domyślną dla IPv6 (**Brama IPv6**); wielkość ramki Internetowej (**MTU**); adresy serwerów DNS dla IPv4 (**Pierwszy serwer DNS IPv4, Drugi serwer DNS IPv4**); adresy serwerów DNS dla IPv6 (**Pierwszy serwer DNS IPv6, Drugi serwer IPv6**); włączyć funkcję NAT po stronie routera (**Włącz NAT**). Wybierając ten typ połączenia możemy nadać również dodatkowe adresy IP dla interfejsu WAN w routerze.

Ustawienia WAN

WAN_1

Włącz

Port: LAN1/WAN

Typ połączenia: Styczne IP

Adres IPv4:

Maska podsieci: 255.255.255.0

Brama IPv4:

Adres IPv6: fe80::26e1:24ff:fe13:509

Długość prefiksu: 64

Brama IPv6:

MTU: 1500

Pierwszy serwer DNS IPv4: 8.8.8.8

Drugi serwer DNS IPv4:

Pierwszy serwer DNS IPv6:

Drugi serwer DNS IPv6:

Włącz NAT

Dodatkowe adresy IP

Adres IP	Maska podsieci	Operacja
<input type="text"/>	<input type="text"/>	<input type="button" value="+"/>

Rysunek 4.12 Konfiguracja portu WAN dla stałego IP

Klient DHCP dla IPv4

Konfiguracja tego typu połączenia powinna wykonać się automatycznie, ale możemy tutaj podać takie dane jak: wielkość ramki Internetowej (**MTU**); wybrać czy chcemy używać serwerów DNS nadanych przez serwer DHCP czy wprowadzić je ręcznie (**Używaj serwerów DNS usługodawcy**); jeśli nie skorzystamy z powyższej opcji musimy podać adresy serwerów DNS ręcznie (**Pierwszy serwer DNS IPv4, Drugi serwer DNS IPv4**); włączyć funkcję NAT po stronie routera (**Włącz NAT**)

The screenshot shows the 'Ustawienia WAN' (WAN Settings) page for 'WAN_1'. The 'Typ połączenia' (Connection Type) is set to 'Klient DHCP'. The 'Włącz' (Enable) checkbox is checked. The 'Port' is set to 'LAN1/WAN'. The 'MTU' is set to '1500'. The 'Używaj serwerów DNS usługodawcy' (Use ISP DNS Servers) checkbox is unchecked. The 'Pierwszy serwer DNS IPv4' (First IPv4 DNS Server) is set to '8.8.8.8'. The 'Drugi serwer DNS IPv4' (Second IPv4 DNS Server) is empty. The 'Włącz NAT' (Enable NAT) checkbox is checked. A 'Zapisz i zatwierdź' (Save and Confirm) button is visible at the bottom.

Rysunek 4.13 Konfiguracja portu WAN dla Klienta DHCP

PPPoE

Aby skonfigurować ten typ połączenia należy podać dane logowania do sieci usługodawcy czyli: nazwę użytkownika (**Nazwa użytkownika**); hasło (**Hasło**); odstęp czasu między próbami połączenia się do sieci wyrażony w sekundach (**Interwał wykrywania połączenia**); wielkość ramki (**MTU**); wybrać czy korzystamy z adresów serwerów DNS nadanych przez usługodawcę czy wprowadzamy je ręcznie (**Używaj serwerów DNS usługodawcy**); jeśli korzystamy z własnych serwerów DNS należy podać ich adresy (**Pierwszy serwer DNS IPv4, Drugi serwer DNS IPv4**); włączyć funkcję NAT po stronie routera (**Włącz NAT**).

The screenshot shows the 'Ustawienia WAN' (WAN Settings) page for 'WAN_1'. The 'Typ połączenia' (Connection Type) is set to 'PPPoE'. The 'Włącz' (Enable) checkbox is checked. The 'Port' is set to 'LAN1/WAN'. The 'Nazwa użytkownika' (Username) and 'Hasło' (Password) fields are empty. The 'Interwał wykrywania połączenia(s)' (Connection Discovery Interval) is set to '60'. The 'Maksymalna ilość prób' (Maximum Number of Attempts) is set to '0'. The 'MTU' is set to '1500'. The 'Używaj serwerów DNS usługodawcy' (Use ISP DNS Servers) checkbox is unchecked. The 'Pierwszy serwer DNS IPv4' (First IPv4 DNS Server) is set to '8.8.8.8'. The 'Drugi serwer DNS IPv4' (Second IPv4 DNS Server) is empty. The 'Włącz NAT' (Enable NAT) checkbox is checked. A 'Zapisz i zatwierdź' (Save and Confirm) button is visible at the bottom.

Rysunek 4.14 Konfiguracja portu WAN dla PPPoE

Klient DHCP IPv6

Konfiguracja tego typu połączenia powinna wykonać się automatycznie, ale możemy tutaj podać takie dane jak: sposób przydzielenia adresu IP dla routera przez serwer DHCPv6 (**Typ żądania o adres IPv6**); długość prefiksu dla IPv6 (**Długość prefiksu IPv6**); wielkość ramki Internetowej (**MTU**); wybrać czy chcemy używać serwerów DNS nadanych przez serwer DHCP czy wprowadzić je ręcznie (**Używaj serwerów DNS usługodawcy**); jeśli nie skorzystamy z powyższej opcji musimy podać adresy serwerów DNS ręcznie (**Pierwszy serwer DNS IPv6, Drugi serwer IPv6**); włączyć funkcję NAT po stronie routera (**Włącz NAT**).

The screenshot shows the 'Ustawienia WAN' (WAN Settings) page for 'WAN_1'. The configuration is as follows:

Parameter	Value
Włącz	<input checked="" type="checkbox"/>
Port	LAN1/WAN
Typ połączenia	Klient DHCPv6
Typ żądania o adres IPv6	None
Długość prefiksu IPv6	0-64
MTU	1500
Pierwszy serwer DNS IPv6	
Drugi serwer DNS IPv6	
Włącz NAT	<input checked="" type="checkbox"/>

Buttons: Zapisz i zatwierdź

Rysunek 4.15 Konfiguracja portu WAN dla klienta DHCPv6

Dual-Stack Lite

Aby skonfigurować ten typ połączenia należy podać: adres IPv6 bramy (**Brama IPv6**); adres routera AFTR (**Adres serwera AFTR DS-Lite**); adres IPv6 (**Lokalny adres IPv6**); rozmiar ramki Internetowej (**MTU**); adresy serwerów DNS dla IPv4 (**Pierwszy serwer DNS IPv4, Drugi serwer DNS IPv4**); adresy serwerów DNS dla IPv6 (**Pierwszy serwer DNS IPv6, Drugi serwer IPv6**); włączyć funkcję NAT po stronie routera (**Włącz NAT**).

The screenshot shows the 'Ustawienia WAN' (WAN Settings) page for 'WAN_1'. The configuration is as follows:

Parameter	Value
Włącz	<input checked="" type="checkbox"/>
Port	LAN1/WAN
Typ połączenia	Dual-Stack Lite
Brama IPv6	
Adres serwera AFTR DS-Lite	
Lokalny adres IPv6	
MTU	1500
Pierwszy serwer DNS IPv4	8.8.8.8
Drugi serwer DNS IPv4	
Pierwszy serwer DNS IPv6	
Drugi serwer DNS IPv6	
Włącz NAT	<input checked="" type="checkbox"/>

Rysunek 4.16 Konfiguracja portu WAN dla Dual-Stack Lite

4.2.1.5 Interfejs lokalny

W zakładce **Interfejs lokalny** możemy dokonać konfiguracji interfejsu LAN routera. Możemy ustawić tutaj: czy interfejs ma korzystać z protokołu **STP** (Spanning Tree Protocol); adres IPv4 interfejsu (**Adres IP**); maskę podsieci (**Maska podsieci**); adres IPv6 interfejsu (**Adres IPv6**); wielkość ramki Internetowej (**MTU**). Oprócz podstawowej konfiguracji możemy również dodać obsługę większej ilości adresów IP dla interfejsu **lokalnego**.

Adres IP	Maska podsieci	Operacja
		+

Rysunek 4.17 Konfiguracja interfejsu lokalnego

4.2.1.6 Switch

Zakładka **Switch/VLAN** służy do konfiguracji opcji VLAN. VLAN dzieli fizyczne interfejsy urządzenia na logiczne grupy robocze. Jako, że router obsługuje funkcję VLAN w standardzie IEEE 802.1Q możemy skonfigurować go w taki sposób, aby na jednym porcie fizycznym spotykało się wiele sieci logicznych. Przy poprawnej konfiguracji switcha zewnętrznego możemy zapewnić redundanthy dostęp do Internetu wielu sieciom VLAN za pomocą jednego portu LAN.

Nazwa	VLAN ID	Adres IP	Maska podsieci	MTU	Operacja
vlan1	1	192.168.126.253	255.255.248.0	1500	✕
vlan2	2	192.168.2.1	255.255.255.0	1500	✕
					+

VLAN ID	LAN 1	LAN 2	CPU	Operacja
1	Close	Tagged	Tagged	✕
2	Close	Tagged	Tagged	✕
				+

Rysunek 4.18 Konfiguracja VLAN

4.2.1.7 Interfejs pętli

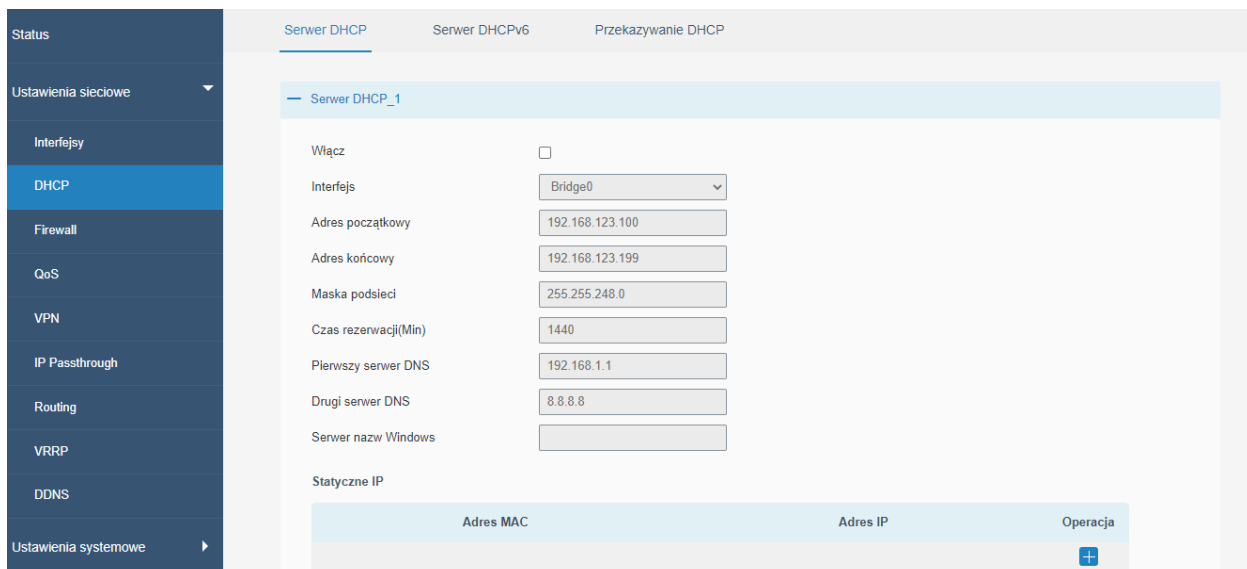
Zakładka **interfejs pętli** pozwala skonfigurować ustawienia interfejsu pętli. Jest to interfejs logiczny routera, który nie ma swojego fizycznego odzwierciedlenia. W protokołach routingu IP tego interfejsu często stosowane jest jako numer ID urządzenia. Oprócz domyślnych wartości można dodać własne adresy.

4.2.2 DHCP

W zakładce DHCP możemy skonfigurować pracę routera jako serwera DHCP lub DHCPv6 oraz jako urządzenie przekazujące konfigurację DHCP. Jeśli port LAN1/WAN ustawimy jako port WAN ([sekcja 4.2.1.3](#)) to możemy skonfigurować tak naprawdę dwa serwery DHCP, dla każdego interfejsu osobno (WAN, Bridge0).

DHCP

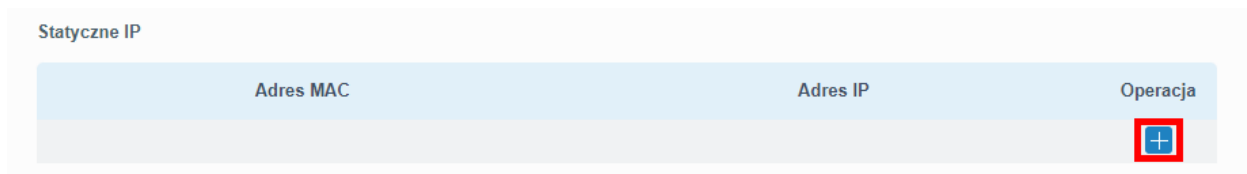
Aby skonfigurować nasz router jako serwer DHCP należy: włączyć usługę (**Włącz**); wybrać interfejs, który ma obsługiwać dany serwer (**Interfejs**); ustawić zakres adresacji podając najniższy możliwy adres dla urządzenia (**Adres początkowy**) oraz najwyższy możliwy adres (**Adres końcowy**); maskę podsieci (**Maska podsieci**); czas na jaki zostanie przydzielony adres danemu urządzeniu wyrażony w minutach z zakresu 5-1440 (**Czas rezerwacji**); adresy DNS dla IPv4 (**Pierwszy serwer DNS, Drugi serwer DNS**); adres serwera nazw Windows (**Serwer nazw Windows**).



Rysunek 4.19 Konfiguracja serwera DHCP

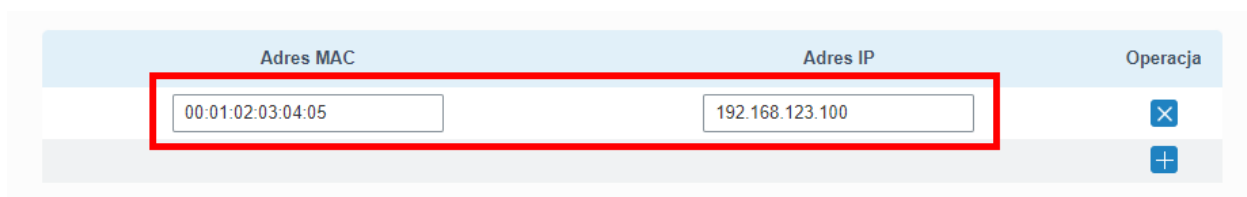
Jeśli chcemy, aby jakieś urządzenie zawsze miało przydzielany ten sam adres IP po podłączeniu do routera należy:

1. Kliknąć na **+** w sekcji **Statyczne IP** przy opcji **Operacja**



Rysunek 4.20 Dodawanie stałego IP dla klienta DHCP krok 1

2. Podać adres MAC urządzenia oraz adres IP jaki ma otrzymywać urządzenie



Rysunek 4.21 Dodawanie stałego IP dla klienta DHCP krok 2

3. Jeśli chcemy dodać więcej urządzeń należy ponownie kliknąć na **+**
4. Po dodaniu wszystkich adresów należy kliknąć przycisk **Zapisz**

Adres MAC	Adres IP	Operacja
00:01:02:03:04:05	192.168.123.100	✕
		+
+ Serwer DHCP_2		
+ Serwer DHCP_3		
Zapisz		

Rysunek 4.22 Dodawanie stałego IP dla klienta DHCP krok 4

Jeśli chcemy usunąć urządzenie z listy stałych IP klikamy na krzyżyk przy danym wpisie

Adres MAC	Adres IP	Operacja
00:01:02:03:04:05	192.168.123.100	✕
		+

Rysunek 4.23 Usuwanie urządzenia z listy stałych IP dla serwera DHCP

DHCPv6

Aby skonfigurować nasz router jako serwer DHCPv6 należy: włączyć usługę (**Włącz**); wybrać interfejs, który ma obsługiwać dany serwer (**Interfejs**); ustawić zakres adresacji podając najniższy możliwy adres dla urządzenia (**Adres początkowy**) oraz najwyższy możliwy adres (**Adres końcowy**); długość prefiksu dla IPv6 (**Długość prefiksu**); czas na jaki zostanie przydzielony adres danemu urządzeniu wyrażony w minutach z zakresu 5-1440 (**Czas rezerwacji**); adresy DNS dla IPv4 (**Pierwszy serwer DNS, Drugi serwer DNS**).

Status	Serwer DHCP	Serwer DHCPv6	Przekazywanie DHCP
Ustawienia sieciowe			
Interfejsy			
DHCP			
Firewall			
QoS			
VPN			
IP Passthrough			
Routing			
VRRP			
DDNS			

Serwer DHCPv6_1		
Włącz	<input checked="" type="checkbox"/>	
Interfejs	Bridge0	
Początkowy adres	2001:00B0:3000:3001::100	
Końcowy adres	2001:00B0:3000:3001::199	
Długość prefiksu	64	
Czas rezerwacji (Min)	1440	
Pierwszy adres DNS	2001:00B0:3000:3001::1	
Drugi adres DNS	2001:4860:4860:8888	
Styczne IP		
DUID	Adres IPv6	Operacja
		+

Rysunek 4.24 Konfiguracja serwera DHCPv6

Jeśli chcemy, aby jakieś urządzenie zawsze miało przydzielany ten sam adres IP po podłączeniu do routera należy:

1. Kliknąć na **+** w sekcji **Styczne IP** przy opcji **Operacja**

Styczne IP		
DUID	Adres IPv6	Operacja
		+

Rysunek 4.25 Dodawanie stałego adresu IP dla klienta DHCPv6 krok 1

2. Podać DUID urządzenia oraz adres IP jaki ma otrzymywać urządzenia

DUID	Adres IPv6	Operacja
1324154325432532645635432	2001:00B0:3000:3001::220	✖
		+

Rysunek 4.26 Dodawanie stałego adresu IP dla klienta DHCPv6 krok 2

3. Jeśli chcemy dodać więcej urządzeń należy ponownie kliknąć na +

4. Po dodaniu wszystkich adresów należy kliknąć przycisk **Zapisz**

DUID	Adres IPv6	Operacja
1324154325432532645635432	2001:00B0:3000:3001::220	✖
		+

+ Serwer DHCPv6_2

+ Serwer DHCPv6_3

Zapisz

Rysunek 4.27 Dodawanie stałego adresu IP dla klienta DHCPv6 krok 4

Jeśli chcemy usunąć urządzenie z listy stałych IP klikamy na krzyżyk przy danym wpisie

DUID	Adres IPv6	Operacja
1324154325432532645635432	2001:00B0:3000:3001::220	✖
		+

Rysunek 4.28 Usuwanie urządzenia z listy stałych IP dla serwera DHCPv6

Przekazywanie DHCP

Funkcja przekazywania DHCP pozwala wskazać serwer DHCP, który znajduje się w innej sieci niż ta utworzona przez router z podłączonymi do niego hostami.

Aby skonfigurować działanie tej funkcji należy: włączyć działanie funkcji (**Włącz**) oraz podać adres zewnętrznego serwera DHCP (**Serwer DHCP**). Opcjonalnie można podać więcej niż jeden adres serwera DHCP, maksymalnie można podać ich 10 i każdy kolejny należy oddzielić w polu **Serwer DHCP** średnikiem „,;”.

Status

Ustawienia sieciowe

Interfejsy

DHCP

Firewall

Serwer DHCP Serwer DHCPv6 Przekazywanie DHCP

Przekazywanie DHCP

Włącz

Serwer DHCP

Zapisz

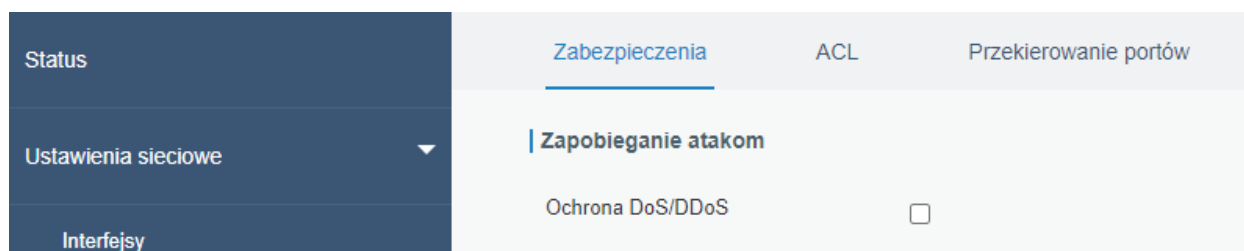
Rysunek 4.29 Przekazywanie DHCP

4.2.3 Firewall

4.2.3.1 Zabezpieczenia

Zapobieganie atakom

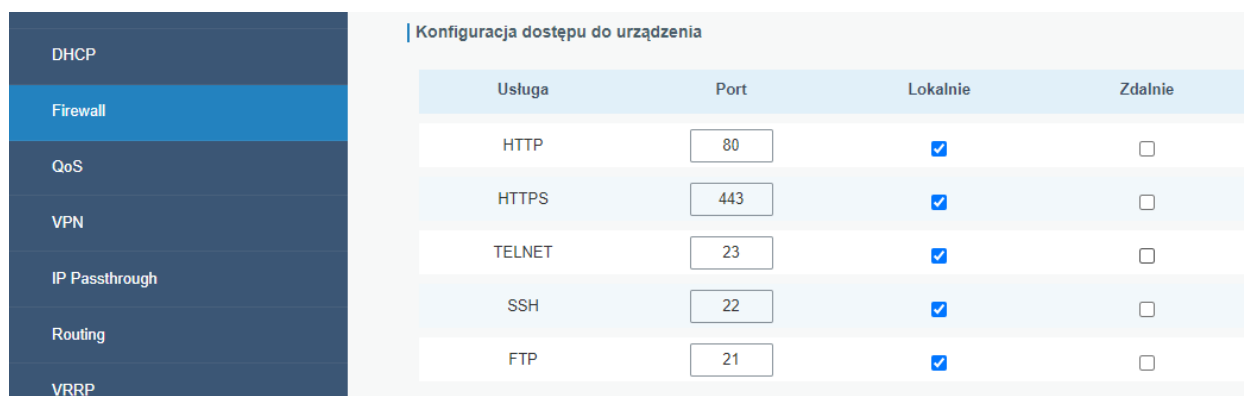
Opcja **Ochrona DoS/DDoS** pozwala włączyć ochronę routera przed atakami typu DoS i DDoS, które mogłyby zablokować prawidłowe funkcjonowanie urządzenia



Rysunek 4.30 Ochrona DoS/DDoS

Konfiguracja dostępu do urządzenia

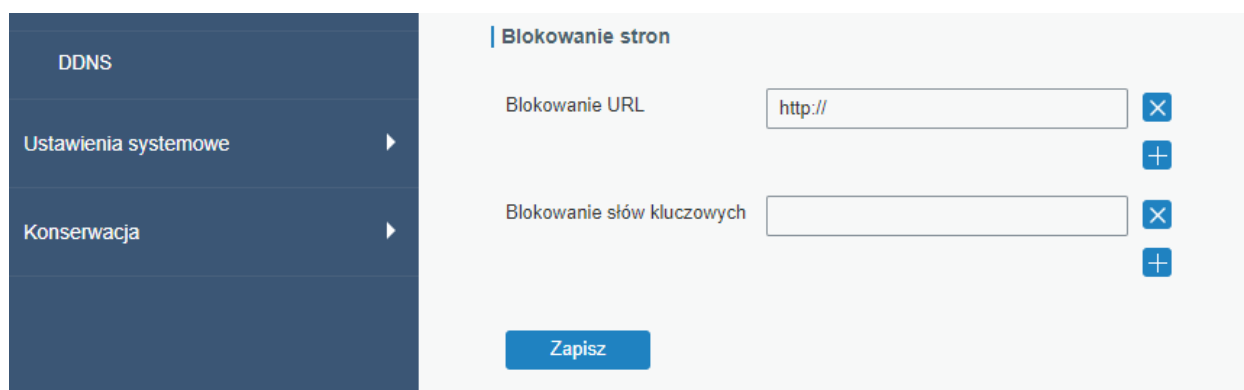
W tej grupie ustawień możemy skonfigurować to w jaki sposób będzie możliwa komunikacja z routerem w celu jego konfiguracji (**Usługa**) oraz czy będzie to możliwe poprzez połączenie lokalne z urządzeniem (**Lokalnie**) lub zdalnie (**Zdalnie**).



Rysunek 4.31 Konfiguracja dostępu do urządzenia

Blokowanie stron

Grupa ta odpowiedzialna jest za listę stron (**Blokowanie URL**) oraz słów kluczowych (**Blokowanie słów kluczowych**), które będą blokowane przez router. Aby dodać stronę lub słowo kluczowe należy przy odpowiedniej opcji kliknąć na **+** przy danej opcji, a następnie wpisać stronę/słowo kluczowe. Po skończonej konfiguracji należy kliknąć **Zapisz**.



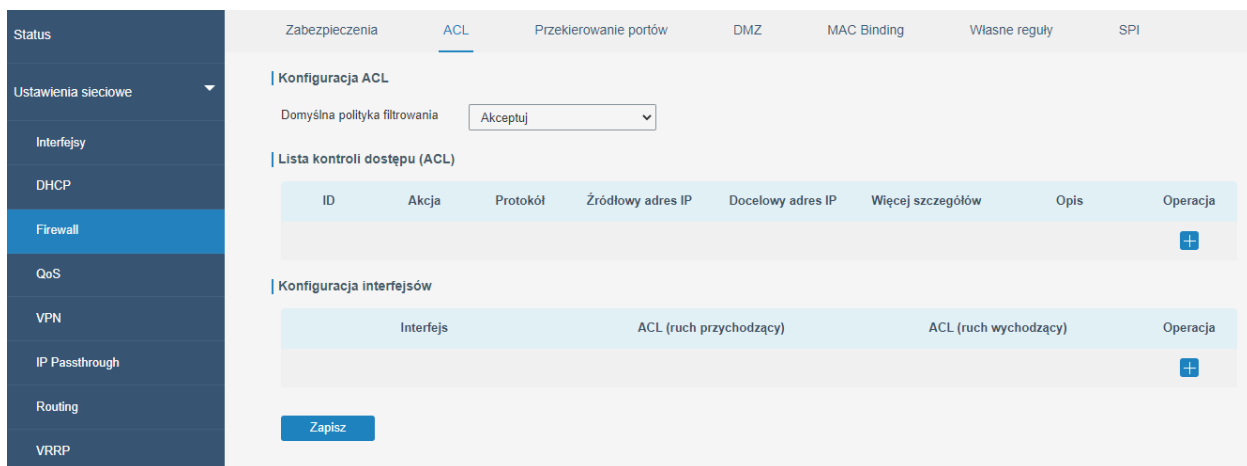
Rysunek 4.32 Blokowanie stron

4.2.3.2 ACL

Lista kontroli dostępu, zwana również ACL, implementuje reguły dostępu dla określonego ruchu sieciowego. Gdy router odbierze pakiet, zostanie on przeanalizowany zgodnie z regułą ACL zastosowaną do bieżącego interfejsu. Po identyfikacji czy danych ruch sieciowy jest dozwolony, czy nie, pakiet może być przepuszczony do urządzenia końcowego lub zablokowany przez router.

Konfiguracja ACL

W tej grupie możemy ustawić w jaki sposób ma być traktowany ruch sieciowy, który nie jest przypisany do żadnej reguły ACL. Ustawienie „Akceptuj” w opcji **Domyślna polityka filtrowania** pozwala traktować taki ruch domyślnie czyli przepuszczać pakiety do urządzeń końcowych.

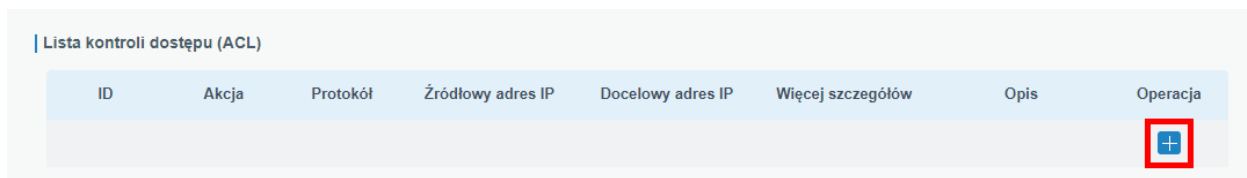


Rysunek 4.33 Konfiguracja ACL

Access Control List

W tej grupie możemy dodawać reguły ACL. Aby dodać taką regułę należy:

1. Kliknąć na **+** w kolumnie **Operacja** tabeli



Rysunek 4.34 Dodawanie reguły ACL krok 1

2. Wybrać typ reguły *standardowy* lub *rozszerzony*. W przypadku wyboru typu standardowego dane, które musimy podać ograniczają się do: *ID* reguły z zakresu 1-199; rodzaju akcji: dopuszczenie (*akceptuj*), blokiwanie (*odrzuć*); adres IP sieci od, którego przychodzi pakiet (**Źródłowy adres IP**); maski wieloznacznicy sieci (**Źródłowa maska wieloznacznicy**); opisu reguły

W przypadku wyboru typu rozszerzonego możemy wybrać protokół jakiego będzie dotyczyła reguła, poniższa ilustracja prezentuje przykładowe ustawienia dla typu rozszerzonego i protokołu *IP*

Typ	rozszerzony
ID	100
Akcja	zablokuj
Protokół	ip
Źródłowy adres IP	212.77.98.9
Źródłowa maska wieloznaczna	0.0.0.0
Docelowy adres IP	192.168.126.253
Docelowa maska wieloznaczna	0.0.0.0
Opis	


Rysunek 4.35 Dodawanie reguły ACL krok 2

- Po wprowadzeniu danych należy kliknąć na przycisk **Zapisz**

Konfiguracja interfejsów



W tej grupie ustawień przypisujemy konkretne reguły do interfejsów routera. Aby przypisać konkretną regułę do interfejsu należy:

- Kliknąć na  w kolumnie **Operacja** tabeli

Konfiguracja interfejsów			
Interfejs	ACL (ruch przychodzący)	ACL (ruch wychodzący)	Operacja
			



Rysunek 4.36 Przypisywanie reguły ACL krok 1

- Wybrać interfejs, do którego przypisujemy regułę

Konfiguracja interfejsów			
Interfejs	ACL (ruch przychodzący)	ACL (ruch wychodzący)	Operacja
Bridge0			
			

Rysunek 4.37 Przypisywanie reguły ACL krok 2

- Wybrać reguły dla ruchu przychodzącego i/lub wychodzącego

Konfiguracja interfejsów			
Interfejs	ACL (ruch przychodzący)	ACL (ruch wychodzący)	Operacja
Bridge0	100	100	
			

Rysunek 4.38 Przypisywanie reguły ACL krok 3

4. Po wprowadzeniu danych kliknąć na przycisk **Zapisz**

The screenshot shows the 'Konfiguracja interfejsów' (Interface Configuration) section. It features a table with columns: 'Interfejs', 'ACL (ruch przychodzący)', 'ACL (ruch wychodzący)', and 'Operacja'. The first row contains 'Bridge0', '100', and '100'. Below the table is a blue 'Zapisz' (Save) button, which is highlighted with a red rectangular box.

Rysunek 4.39 Przypisywanie reguły ACL krok 4

4.2.3.3 Przekierowywanie portów

W przypadku stosowania funkcji NAT w routerze, aby dostać się spoza sieci wewnętrznej LAN do urządzeń znajdujących się w tej sieci należy uruchomić przekierowanie portów dla danego urządzenia. Przykładem zastosowania przekierowania portów może być serwer strony WWW, który znajduje się w naszej sieci wewnętrznej, a chcielibyśmy tę stronę udostępnić poza naszą siecią. Po ustawieniu przekierowania wszystkie pakiety, które będą miały odpowiedni rodzaj i port będą przekierowywane na odpowiednie urządzenie w sieci wewnętrznej LAN. Aby ustawić takie przekierowanie należy:

1. Kliknąć na **+** w kolumnie **Operacja** tabeli

The screenshot shows the 'Przekierowanie portów' (Port Forwarding) section. It has a table with columns: 'Źródłowy adres IP', 'Port źródłowy', 'Docelowy adres IP', 'Port docelowy', 'Protokół', 'Opis', and 'Operacja'. The 'Operacja' column contains a blue '+' button, which is highlighted with a red rectangular box. Below the table is a blue 'Zapisz' (Save) button.

Rysunek 4.40 Przekierowanie portów krok 1

2. Podać:

- IP urządzenia, od którego pochodzi zapytanie (wpisując adres 0.0.0.0 pakiety przychodzące z dowolnego adresu będą przekierowywane)
- Port, na którym próbuje skomunikować się urządzenie zewnętrzne
- IP urządzenia, na które pakiety mają zostać przekierowane
- Port, na który pakiety mają zostać przekierowane (zazwyczaj ten sam jak przychodzące z urządzenia zewnętrznego)
- Protokół TCP/UDP/oba
- Opis przekierowania

The screenshot shows the 'Przekierowanie portów' (Port Forwarding) section. The table has columns: 'Źródłowy adres IP', 'Port źródłowy', 'Docelowy adres IP', 'Port docelowy', 'Protokół', 'Opis', and 'Operacja'. The first row contains the following values: '0.0.0.0/0', '80', '192.168.1.100', '80', 'TCP', and 'WWW'. These input fields are highlighted with a red rectangular box. The 'Operacja' column contains a blue '+' button.

Rysunek 4.41 Przekierowanie portów krok 2

3. Po uzupełnieniu danych kliknąć przycisk **Zapisz**

Źródłowy adres IP	Port źródłowy	Docelowy adres IP	Port docelowy	Protokół	Opis	Operacja
0.0.0.0/0	80	192.168.1.100	80	TCP	WWW	<input type="checkbox"/>
<input type="button" value="+"/>						

Rysunek 4.42 Przekierowanie portów krok 3

4.2.3.4 DMZ

Funkcja DMZ działa tak jakbyśmy ręcznie przekierowali na dany adres IP wszystkie porty przychodzące z sieci Internet. Przy stosowaniu tej funkcji należy zachować szczególną ostrożność, ponieważ może ona znacząco obniżyć bezpieczeństwo naszej sieci. Aby włączyć funkcję DMZ należy:

1. Włączyć funkcję (**Włącz**)

DMZ

Włącz

Host DMZ: 192.168.1.100

Adres źródłowy: 0.0.0.0/0

Rysunek 4.43 Funkcja DMZ krok 1

2. Podać:

- adres IP urządzenia, na które ma być przekierowany ruch
- adres IP urządzenia z sieci zewnętrznej, które ma mieć dostęp do strefy DMZ (podając 0.0.0.0/0 akceptujemy wszystkie przychodzące adresy)

DMZ

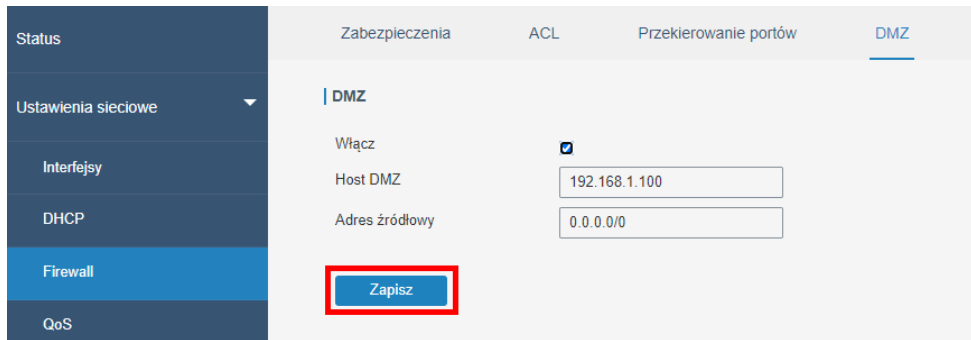
Włącz

Host DMZ: 192.168.1.100

Adres źródłowy: 0.0.0.0/0

Rysunek 4.44 Funkcja DMZ krok 2

3. Po wpisaniu danych klikamy na przycisk **Zapisz**

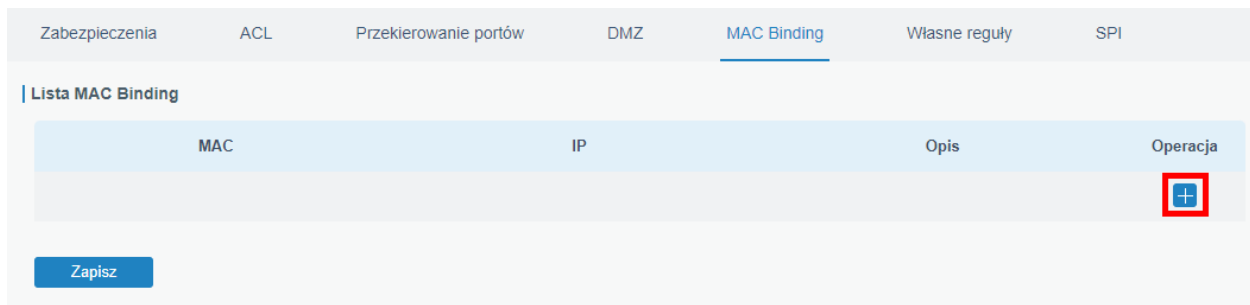


Rysunek 4.45 Funkcja DMZ krok 3

4.2.3.5 MAC Binding

Funkcja ta powoduje przypisanie dostępu do sieci poza routerem konkretnemu zestawowi adresu IP i adresu MAC. Jeśli jakieś urządzenie będzie miało adres IP wpisany na tą listę, ale jego MAC adres będzie różny od tego przypisanego do powyższego adresu IP to urządzenie takie nie będzie miało dostępu do sieci poza routerem. Aby dodać takie filtrowanie należy:

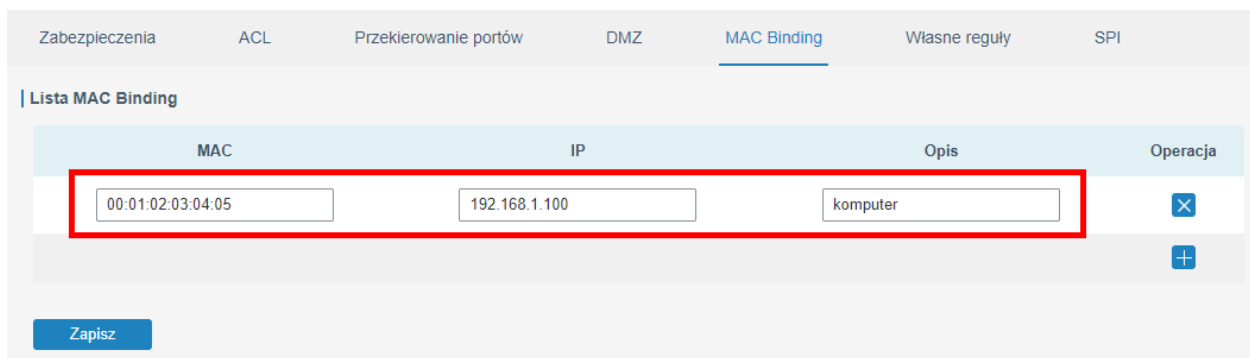
1. Kliknąć na **+** w kolumnie **Operacja** tabeli



Rysunek 4.46 Dodawanie wpisów do listy MAC Binding krok 1

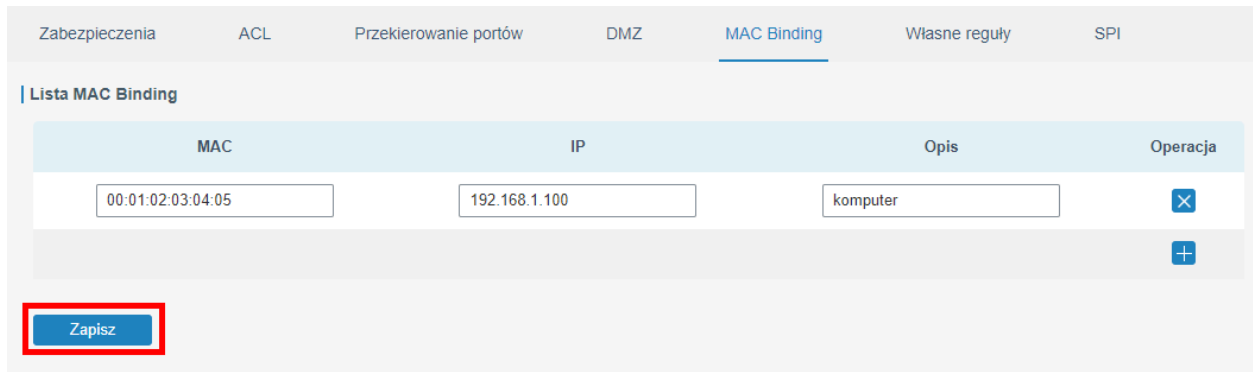
2. Podać:

- adres MAC urządzenia
- adres IP przypisany do tego MAC adresu



Rysunek 4.47 Dodawanie wpisów do listy MAC Binding krok 2

3. Po wprowadzeniu danych kliknąć przycisk **Zapisz**

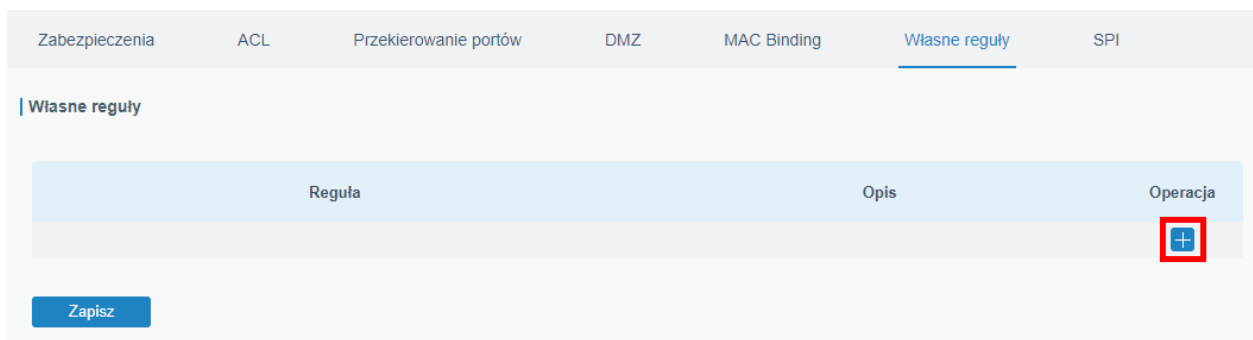


Rysunek 4.48 Dodawanie wpisów do listy MAC Binding krok 3

4.2.3.6 Własne reguły

W tej zakładce można zastosować spersonalizowane wpisy reguł firewala iptables. Aby dodać taką regułę należy:

1. Kliknąć na **+** w kolumnie **Operacja**

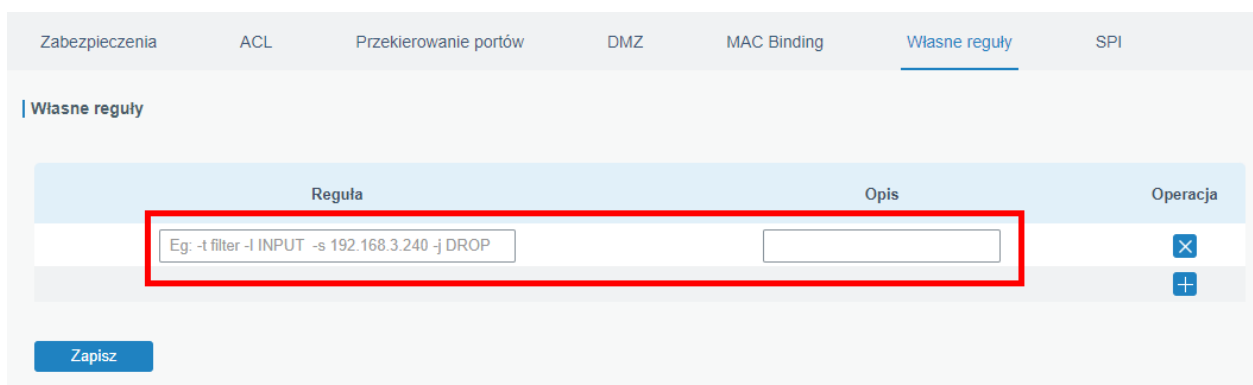


Rysunek 4.49 Dodawanie własnego wpisu iptables krok 1

2. Wpisać:

– treść reguły

– opis reguły



Rysunek 4.50 Dodawanie własnego wpisu iptables krok 2

3. Po wprowadzeniu danych kliknąć przycisk **Zapisz**

The screenshot shows the 'Własne reguły' (Custom Rules) configuration page. At the top, there are tabs for 'Zabezpieczenia', 'ACL', 'Przekierowanie portów', 'DMZ', 'MAC Binding', 'Własne reguły', and 'SPI'. The 'Własne reguły' tab is active. Below the tabs, there is a section titled 'Własne reguły'. A table is displayed with the following structure:

Reguła	Opis	Operacja
Eg: -t filter -I INPUT -s 192.168.3.240 -j DROP		<input type="button" value="X"/>
		<input type="button" value="+"/>

Below the table, there is a 'Zapisz' (Save) button highlighted with a red rectangle.

Rysunek 4.51 Dodawanie własnego wpisu iptables krok 3

4.2.3.7 SPI

Zakładka ta służy do włączenia i skonfigurowania usługi SPI Firewall. Poniższa tabela prezentuje opis funkcji tej zakładki.

The screenshot shows the 'SPI' configuration page. At the top, there are tabs for 'Zabezpieczenia', 'ACL', 'Przekierowanie portów', 'DMZ', 'MAC Binding', 'Własne reguły', and 'SPI'. The 'SPI' tab is active. Below the tabs, there is a section titled 'Firewall SPI'. A list of options is displayed with checkboxes:

- Włącz
- Filtr Proxy
- Filtr Cookies
- Filtr Activex
- Filtr Java Applets
- Filtr Multicast
- Filtr IDENT(port 113)
- Blokada SNMP od WAN
- Filtr przekierowań NAT WAN
- Blokada anonimowych zapytań WAN (ping)

At the bottom of the list, there is a 'Zapisz' (Save) button.

Rysunek 4.52 Konfiguracja SPI

Funkcja	Opis
Włącz	Włącza/wyłącza funkcję SPI firewall
Filtr Proxy	Blokuje zapytania HTTP zawierające łańcuch „Host”
Filtr Cookies	Identyfikuje zapytania HTTP, które zawierają ciasteczka i przerabia je, aby uniemożliwić atak z ich poziomu na sieć
Filtr Activex	Blokuje zapytania HTTP zawierające na końcu URL „.ocx” lub „.cab”
Filtr Java Applets	Blokuje zapytania HTTP zawierające na końcu URL „.js” lub „.class”
Filtr Multicast	Zapobiega dostawianiu się pakietów multicast do sieci LAN
Filtr IDENT (port 113)	Blokuje dostęp do portu 113 od strony WAN
Blokada SNMP od WAN	Blokuje zapytania SNMP od strony WAN
Filtr przekierowań NAT WAN	Uniemożliwia hostom w sieci LAN używać adresu WAN routera do łączenia się z serwerami w sieci LAN
Blokada anonimowych zapytań WAN (ping)	Blokuje odpowiedzi routera na zapytania „ping” przychodzące od strony WAN

4.2.4 QoS

Funkcja Quality of service (QoS) służy do zarządzania pasmem jakie przydzielone jest do konkretnej usługi w sieci. Jeśli w naszej sieci są usługi, które wymagają konkretnej prędkości przesyłu danych do poprawnego działania funkcja ta pozwoli zapewnić jej prawidłowe działanie. Dzięki tej funkcji możemy też ograniczyć ruch sieciowy dla konkretnych usług, aby ich działanie nie wpływało na działanie całej sieci. Konfigurując usługę QoS należy pamiętać, że w przypadku konfiguracji w zakładce **QoS (Pobieranie)** urządzenia znajdujące się w sieci lokalnej są urządzeniami docelowymi (**Docelowy adres IP/Port**), a w przypadku zakładki **QoS (Wysyłanie)** są to urządzenia źródłowe (**Źródłowy adres IP/Port**). Konfigurację tej funkcji pokażę na przykładzie sieci, w której mamy serwer o IP 192.168.1.100, któremu przydzielimy 50% pasma, a dla pozostałych komputerów zostanie kolejne 50% pasma. Konfiguracja jest analogiczna dla zakładki **QoS (Pobieranie)** i **QoS (Wysyłanie)** więc przykład poniżej zostanie wytłumaczony na podstawie zakładki **QoS (Pobieranie)**.

Aby to zrobić należy:

1. Uruchomić funkcję (**Enabled**)

Rysunek 4.53 Funkcja QoS krok 1

2. Ustawić prędkość łącza (**Przepustowość łącza (pobieranie)/Przepustowość łącza (wysyłanie)**). W tym przykładzie przyjmijmy, że posiadamy łącze o przepustowości 2048Kb/s pobieranie i wysyłanie
3. Dodać domyślną kategorię urządzeń poprzez kliknięcie **+** w kolumnie **Operacja** w grupie **Kategorie usług**. W tym przypadku została ona nazwana „pc” i będzie obsługiwała wszystkie komputery poza serwerem więc musimy ją ustawić jako domyślną kategorię dla urządzeń, którym nie będą przypisane specjalne reguły (**Domyślna kategoria**)

Nazwa	Przydział(%)	Maks. przep.(kbps)	Min. przep.(kpbs)	Operacja
pc	50	1024	512	X

Rysunek 4.54 Funkcja QoS kroki 2 i 3

4. Dodać kolejną kategorię kategorii o nazwie „server” z ustawieniami takimi jak kategoria „pc”, która będzie obsługiwała serwer
5. Dodać specjalną regułę dla serwera o nazwie „serverrule”. W tym przykładzie cały ruch sieciowy z/do serwera ma mieć zapewnioną przepustowość więc uzupełniamy tylko: **Docelowy adres IP** w przypadku zakładki **QoS (pobieranie)**, a w przypadku zakładki **QoS (wysyłanie)** uzupełniamy **Źródłowy adres IP**.

QoS(Pobieranie) QoS(Wysyłanie)

Przepustowość łącza (pobieranie)

Włącz

Domyślna kategoria

Przepustowość łącza (pobieranie) kbits/s

Kategorie usług

Nazwa	Przydział(%)	Maks. przep.(kbps)	Min. przep.(kbps)	Operacja
<input type="text" value="pc"/>	<input type="text" value="50"/>	<input type="text" value="1024"/>	<input type="text" value="512"/>	<input type="button" value="X"/>
<input type="text" value="server"/>	<input type="text" value="50"/>	<input type="text" value="1024"/>	<input type="text" value="512"/>	<input type="button" value="X"/>
				<input type="button" value="+"/>

Reguły usług

Nazwa	Źródłowy adres IP	Port źródłowy	Docelowy adres IP	Port docelowy	Protokół	Kategorie usług	Operacja
<input type="text" value="serwermule"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="192.168.1.100"/>	<input type="text"/>	<input type="text" value="Wszystkie"/>	<input type="text" value="server"/>	<input type="button" value="X"/>
							<input type="button" value="+"/>

Rysunek 4.55 Funkcja QoS kroki 4 i 5

Grupa ustawień	Pole	Opis
Przepustowość łącza (pobieranie)/ Przepustowość łącza (wysyłanie)	Włącz	Włącza/wyłącza funkcję
	Domyślna kategoria	Domyślna kategoria ograniczeń, która będzie stosowana w przypadku braku przypisania reguły
	Przepustowość łącza (pobieranie)/ Przepustowość łącza (wysyłanie)	Prędkość pobierania/wysyłania łącza internetowego
Kategorie usług	Nazwa	Nazwa kategorii
	Przydział(%)	Procentowy przydział łącza w przypadku, gdy suma z pól Maks. przep. jest większa niż Przepustowość łącza (pobieranie)/ Przepustowość łącza (wysyłanie) , suma dla wszystkich wpisów nie może przekraczać 100%
	Maks. przep.(kbps)	Maksymalne przydzielone pasmo w kb/s
	Min. przep.(kbps)	Minimalne przydzielone pasmo w kb/s
	Operacja	Dodaje/usuwa wpisy
Reguły usług	Nazwa	Nazwa reguły
	Źródłowy adres IP	IP urządzenia źródłowego; dla zakładki QoS (pobieranie) są to urządzenia spoza sieci lokalnej, dla zakładki QoS (wysyłanie) są to urządzenia w sieci lokalnej. Jeśli pozostawimy to pole puste reguła będzie miała zastosowanie do wszystkich urządzeń.
	Port źródłowy	Port, na którym próbuje komunikować się urządzenie źródłowe. Jeśli pozostawimy to pole puste reguła będzie miała zastosowanie do wszystkich portów.
	Docelowy adres IP	IP urządzenia docelowego; dla zakładki QoS (pobieranie) są to urządzenia w sieci lokalnej, dla zakładki QoS (wysyłanie) są to urządzenia spoza sieci lokalnej. Jeśli pozostawimy to pole puste reguła będzie miała zastosowanie do wszystkich urządzeń.
	Port docelowy	Port, na którym próbuje komunikować się urządzenie docelowe. Jeśli pozostawimy to pole puste reguła będzie miała zastosowanie do wszystkich portów.
	Protokół	Protokół dla którego zastosowanie ma reguła (ANY – wszystkie, TCP, UDP, ICMP, GRE)
	Kategoria usług	Kategoria ograniczeń jaka będzie stosowana do danej reguły
Operacja	Dodaje/ usuwa wpisy	

4.2.5 VPN

VPN (Virtual Private Network) to usługa, która pozwala połączyć bezpiecznie dwie sieci prywatne dzięki czemu urządzenia znajdujące się w jednej sieci będą mogły komunikować się z urządzeniami w innej sieci za pośrednictwem bezpiecznych tuneli komunikacyjnych. Router BCS-R4G-1W1L wspiera DMVPN, IPsec, GRE, L2TP, PPTP, OpenVPN. Dodatkowo możemy skonfigurować router jako serwer dla IPsec oraz OpenVPN.

4.2.5.1 DMVPN

Dynamiczna wielopunktowa wirtualna sieć prywatna (DMVPN), łącząca mGRE i IPsec, to bezpieczna sieć, która wymienia dane między lokalizacjami bez przesyłania ruchu przez serwer lub router VPN w siedzibie organizacji.

DMVPN	Serwer IPsec	IPsec	GRE	L2TP
Konfiguracja DMVPN				
Włącz	<input checked="" type="checkbox"/>			
Adres HUB	<input type="text"/>			
Adres IP tunelu	<input type="text"/>			
Adres IP GRE HUB	<input type="text"/>			
Adres IP tunelu GRE	<input type="text"/>			
Maska podsieci GRE	<input type="text" value="255.255.255.0"/>			
Klucz tunelu GRE	<input type="text"/>			
Typ negocjacji	<input type="text" value="Główny"/>			
Algorytm uwierzytelniania	<input type="text" value="DES"/>			
Algorytm kodowania	<input type="text" value="MD5"/>			
Grupa DH	<input type="text" value="MODP768-1"/>			
Klucz	<input type="text"/>			
Typ ID	<input type="text" value="Default"/>			
Czas życia IKE(s)	<input type="text" value="10800"/>			
Algorytm SA	<input type="text" value="DES-MD5"/>			
Grupa PFS	<input type="text" value="NULL"/>			
Czas życia(s)	<input type="text" value="3600"/>			
Interwał czasu DPD(s)	<input type="text" value="30"/>			
Limit czasu DPD(s)	<input type="text" value="150"/>			
Cisco Secret	<input type="text"/>			
Czas przetrzymywania NHRP(s)	<input type="text" value="7200"/>			
<input type="button" value="Zapisz"/>				

Rysunek 4.56 Konfiguracja usługi DMVPN

Pole	Opis
Włącz	Włącza/wyłącza usługę DMVPN
Adres HUB	Adres IP lub domena huba DMVPN
Adres IP tunelu	Lokalny adres tunelu DMVPN
Adres IP GRE HUB	Adres IP huba tunelu GRE
Adres IP tunelu GRE	Lokalny adres tunelu GRE
Maska podsieci GRE	Lokalna maska podsieci tunelu GRE
Klucz tunelu GRE	Klucz tunelu GRE
Typ negocjacji	Tryb negocjacji połączenia
Algorytm uwierzytelniania	Algorytm autentykacji
Algorytm kodowania	Algorytm szyfrowania
Grupa DH	Określa grupę DH (siłę klucza szyfrowania), im wyższy numer tym bezpieczniejsze połączenie, ale obliczenia trwają dłużej
Klucz	Treść klucza
Typ ID	Typ lokalnego ID, przy wybraniu innego niż „default” należy podać ID
Czas życia IKE (s)	Długość życia negocjacji IKE, zakres 60-86400 sekund
Algorytm SA	Wybór algorytmu SA
Grupa PFS	Określa grupę PFS (siłę klucza szyfrowania), im wyższy numer tym bezpieczniejsze połączenie, ale obliczenia trwają dłużej
Czas życia (s)	Czas życia IPsec SA, zakres 60-86400
Interwał czasu DPD (s)	Odstęp czasu DPD
Limit czasu DPD (s)	Limit czasu DPD
Cisco Secret	Klucz Cisco nhrp
Czas przetrzymywania NHRP (s)	Czas przetrzymywania NHRP

4.2.5.2 IPsec Server

Protokół IPsec jest szczególnie przydatny do wdrażania wirtualnych sieci prywatnych i zdalnego dostępu użytkowników za pośrednictwem połączenia telefonicznego z sieciami prywatnymi. Dużą zaletą protokołu IPsec jest to, że zabezpieczenia mogą być obsługiwane bez konieczności wprowadzania zmian na poszczególnych komputerach użytkowników. IPsec zapewnia trzy opcje usług bezpieczeństwa: nagłówek uwierzytelniania (AH), Encapsulating Security Payload (ESP) i wymiana kluczy internetowych (IKE). AH zasadniczo umożliwia uwierzytelnianie danych tych podmiotów. ESP obsługuje zarówno uwierzytelnianie nadawcy, jak i szyfrowanie danych. IKE służy do wymiany kodów szyfrów. Wszystkie z nich mogą chronić jeden lub więcej przepływów danych między hostami, między hostem a bramą oraz między bramami.

DMVPN
Serwer IPsec
IPsec
GRE
L2TP

Serwer IPsec

Włącz

Tryb IPsec Tunelowy

Protokół IPsec ESP

Podsieć

Maska podsieci

Typ ID Domyślny

Zdalna podsieć

Zdalna maska podsieci

Typ zdalnego ID Domyślny

Konfiguracja IKE

Konfiguracja SA

Opcje zaawansowane IPsec

Opcje eksperta

Zapisz

Rysunek 4.57 Konfiguracja usługi serwer IPsec

Pole	Opis
Włącz	Włącza/wyłącza funkcję serwer IPsec
Tryb IPsec	Tryb działania usługi
Protokół IPsec	Wybór protokołu
Podsieć	Adres podsieci lokalnej, którą chroni IPsec
Maska podsieci	Maska powyższej podsieci
Typ ID	Typ lokalnego ID, przy wybraniu innego niż „default” należy podać ID
Zdalna podsieć	Zdalna podsieć, którą chroni IPsec
Zdalna maska podsieci	Maska powyższej podsieci
Typ ID zdalnego	Typ zdalnego ID, przy wybraniu innego niż „default” należy podać ID

Konfiguracja IKE

Wersja IKE: IKEv2

Tryb negocjacji: Główny

Algorytm uwierzytelniania: DES

Algorytm kodowania: MD5

Grupa DH: MODP768-1

Uwierzytelnianie lokalne: PSK

Zdalne uwierzytelnianie: PSK

XAUTH:

Czas życia(s): 10800

Lista XAUTH

Użytkownik	Hasło	Operacja
		+

Lista kluczów udostępniania (PSK)

Selektor	PSK	Operacja
		+

Rysunek 4.58 Konfiguracja serwera IPsec parametrów IKE

Konfiguracja SA

Algorytm SA: DES-MD5

Grupa PFS: NULL

Czas życia(s): 3600

Interwał czasu DPD(s): 30

Limit czasu DPD(s): 150

Rysunek 4.59 Konfiguracja serwera IPsec parametrów SA

Opcje zaawansowane IPsec

Włącz kompresję:

Typ VPN przez IPsec: żaden

Opcje eksperta:

Zapisz

Rysunek 4.60 Konfiguracja serwera IPsec parametry zaawansowane

Pole	Opis
Konfiguracja IKE	
Wersja IKE	Wersja protokołu IKE
Tryb negocjacji	Tryb negocjacji połączenia
Algorytm uwierzytelniania	Wybór algorytmu uwierzytelniania
Algorytm kodowania	Wybór klucza szyfrowania
Grupa DH	Określa grupę DH (siłę klucza szyfrowania), im wyższy numer tym bezpieczniejsze połączenie, ale obliczenia trwają dłużej
Uwierzytelnianie lokalne	Wybór lokalnego uwierzytelniania
XAUTH	Włącza/wyłącza uwierzytelnianie XAUTH
Czas życia (s)	Czas życia negocjacji IKE, zakres 60-86400
Lista XAUTH	
Nazwa użytkownika	Nazwa użytkownika do uwierzytelniania
Hasło	Hasło do uwierzytelniania
Operacja	Dodaje/usuwa wpisy
Lista PSK	
Selektor	Numer identyfikacyjny PSK
PSK	Klucz dostępu
Operacja	Dodaje/usuwa wpisy
Konfiguracja SA	
Algorytm SA	Wybór algorytmu SA
Grupa PFS	Określa grupę PFS (siłę klucza szyfrowania), im wyższy numer tym bezpieczniejsze połączenie, ale obliczenia trwają dłużej
Czas życia (s)	Czas życia negocjacji SA, zakres 60-86400
Interwał czasu DPD (s)	Odstęp czasu DPD
Limit czasu DPD (s)	Limit czasu DPD
Opcje zaawansowane IPsec	
Włącz kompresję	Włącza kompresję nagłówek pakietów IP
Typ VPN przez IPsec	Wybór protokołu, dla którego uruchomione zostanie IPsec
Opcje eksperta	Pole służy do ręcznego dodawania kolejnych wpisów do protokołu IPsec, każdy wpis powinien być oddzielony „:”

4.2.5.3 IPsec

W tej zakładce możemy skonfigurować połączenie IPsec, w którym router jest klientem. Można skonfigurować maksymalnie 3 połączenia klienckie.

Rysunek 4.61 Konfiguracja usługi IPsec

Pole	Opis
Włącz	Włącza/wyłącza funkcję, maksymalnie można skonfigurować 3 tunele IPsec
Tryb IPsec	Tryb działania usługi
Protokół IPsec	Wybór protokołu
Podsieć	Adres podsieci lokalnej, którą chroni IPsec
Maska podsieci	Maska powyższej podsieci
Typ ID	Typ lokalnego ID, przy wybraniu innego niż „default” należy podać ID
Zdalna podsieć	Zdalna podsieć, którą chroni IPsec
Zdalna maska podsieci	Maska powyższej podsieci
Typ zdalnego ID	Typ zdalnego ID, przy wybraniu innego niż „default” należy podać ID

Konfiguracja IKE	<input checked="" type="checkbox"/>
Wersja IKE	IKEv1
Tryb negocjacji	Główny
Algorytm uwierzytelniania	DES
Algorytm kodowania	MD5
Grupa DH	MODP768-1
Lokalne uwierzytelnianie	PSK
Lokalny klucz udostępniania	
XAUTH	<input type="checkbox"/>
Czas życia(s)	10800
Konfiguracja SA	<input checked="" type="checkbox"/>
Algorytm SA	DES-MD5
Grupa PFS	NULL
Czas życia(s)	3600
Interwał czasowy DPD(s)	30
Limit czasu DPD (s)	150
Opcje zaawansowane IPsec	<input checked="" type="checkbox"/>
Włącz kompresję	<input type="checkbox"/>
Typ VPN przez IPsec	Żaden
Opcje eksperta	

Rysunek 4.62 Konfiguracja usługi IPsec, konfiguracja IKE, SA

Pole	Opis
Konfiguracja IKE	
Wersja IKE	Wersja protokołu IKE
Tryb negocjacji	Tryb negocjacji połączenia
Algorytm uwierzytelniania	Wybór algorytmu kodowania
Algorytm kodowania	Wybór klucza szyfrowania
Grupa DH	Określa grupę DH (siłę klucza szyfrowania), im wyższy numer tym bezpieczniejsze połączenie, ale obliczenia trwają dłużej
Uwierzytelnianie lokalne	Wybór lokalnej autentykacji
XAUTH	Klucz szyfrowania
Czas życia (s)	Włącza/wyłącza uwierzytelnianie XAUTH
Algorytm uwierzytelniania	Czas życia negocjacji IKE, zakres 60-86400
Lista XAUTH	
Nazwa użytkownika	Nazwa użytkownika do uwierzytelniania
Hasło	Hasło do uwierzytelniania
Operacja	Dodaje/usuwa wpisy
Lista PSK	
Selektor	Numer identyfikacyjny PSK
PSK	Klucz dostępu
Operacja	Dodaje/usuwa wpisy
Konfiguracja SA	
Algorytm SA	Wybór algorytmu SA
Grupa PFS	Określa grupę PFS (siłę klucza szyfrowania), im wyższy numer tym bezpieczniejsze połączenie, ale obliczenia trwają dłużej
Czas życia (s)	Czas życia negocjacji SA, zakres 60-86400
Interwał czasu DPD (s)	Odstęp czasu DPD
Limit czasu DPD (s)	Limit czasu DPD
Opcje zaawansowane IPsec	
Włącz kompresję	Włącza kompresję nagłówek pakietów IP
Typ VPN przez IPsec	Wybór protokołu, dla którego uruchomione zostanie IPsec
Opcje eksperta	Pole służy do ręcznego dodawania kolejnych wpisów do protokołu IPsec, każdy wpis powinien być oddzielony „,”

4.2.5.4 GRE

Generic Routing Encapsulation (GRE) to protokół, który hermetyzuje pakiety w celu routingu innych protokołów w sieciach IP. Jest to technologia tunelowania, która zapewnia kanał, przez który może być przesyłana enkapsulowana wiadomość danych, a enkapsulacja i dekapulacja mogą być realizowane na obu końcach. W następujących okolicznościach można zastosować transmisję tunelową GRE:

- Tunel GRE może przesyłać pakiety danych multicast tak, jakby był prawdziwym interfejsem sieciowym. Funkcja Singleuseof IPsec nie zapewnia szyfrowania multimijsji.
- Określony przyjęty protokół nie może być routowany.
- Do połączenia dwóch innych podobnych sieci wymagana jest sieć o różnych adresach IP.

DMVPN Serwer IPsec IPsec **GRE** L2TP

Konfiguracja GRE

— GRE_1

Włącz

Adres IP tunelu

Adres IP

Wirtualny adres IP

Maska podsieci

Wirtualny adres IP tunelu

Globalne przekazywanie ruchu

Zdalna podsieć

Maska podsieci tunelu

MTU

Klucz

Włącz NAT

Rysunek 4.63 Konfiguracja usługi GRE

Pole	Opis
Włącz	Włącza/wyłącza usługę
Adres IP tunelu	Zdalny adres IP
Adres IP	Adres IP
Wirtualny adres IP	Adres IP urządzenia prezentowany w tunelu GRE
Maska podsieci	Maska podsieci
Wirtualny adres IP tunelu	Adres IP zdalnego tunelu GRE
Globalne przekazywanie ruchu	Przy włączeniu tej funkcji cały ruch sieciowy będzie przesyłany przez tunel GRE
Zdalna podsieć	Adres IP sieci dla tunelu GRE
Maska podsieci tunelu	Maska podsieci dla tunelu GRE
MTU	Maksymalna wielkość ramki
Klucz	Klucz szyfrowania dla tunelu GRE
Włącz NAT	Włącza/wyłącza NAT

4.2.5.5 L2TP

Layer Two Tunneling Protocol (L2TP) jest rozszerzeniem protokołu Point-to-Point Tunneling Protocol (PPTP) używany przez dostawców Internetu (ISP), aby tworzyć wirtualne sieci lokalne (VPN) w Internecie.

Rysunek 4.64 Konfiguracja usługi L2TP

Pole	Opis
Włącz	Włącza/wyłącza usługę
Adres IP serwera	Adres IP/domena serwera L2TP
Nazwa użytkownika	Nazwa użytkownika usługi L2TP
Hasło	Hasło usługi L2TP
Uwierzytelnianie	Wybór trybu uwierzytelniania
Globalne przekazywanie ruchu	Przy włączeniu tej funkcji cały ruch sieciowy będzie przesyłany przez tunel L2TP
Adres sieci wirtualnej	Adres IP sieci dla tunelu L2TP
Maska podsieci wirtualnej	Maska podsieci dla tunelu L2TP
Klucz	Klucz szyfrowania tunel L2TP

Opcje zaawansowane	<input checked="" type="checkbox"/>
Wirtualny adres IP	<input type="text"/>
Wirtualny adres IP serwera	<input type="text"/>
Włącz NAT	<input checked="" type="checkbox"/>
Włącz MPPE	<input type="checkbox"/>
Kompresja adresu/pola kontrolnego (PPP)	<input type="checkbox"/>
Kompresja pól protokołu (PPP)	<input type="checkbox"/>
Mapa asynchroniczna (PPP)	<input type="text" value="ffffff"/>
MRU	<input type="text" value="1500"/>
MTU	<input type="text" value="1500"/>
Interwał wykrywania łącza(s)	<input type="text" value="60"/>
Maksymalna ilość prób	<input type="text" value="0"/>
Opcje eksperta	<input type="text"/>

Rysunek 4.65 Konfiguracja usługi L2TP, ustawienia zaawansowane

Pole	Opis
Opcje zaawansowane	Włącza/wyłącza opcje zaawansowane
Wirtualny adres IP	Adres IP klienta L2TP, jeśli to pole jest puste adres zostanie przydzielony z serwera
Wirtualny adres IP serwera	Adres IP tunelu L2TP
Włącz NAT	Włącza/wyłącza NAT
Włącz MPPE	Włącza/wyłącza szyfrowanie MPPE
Kompresja adresu/pola kontrolnego (PPP)	Potrzebne do inicjalizacji PPP, można zostawić wartość domyślną
Kompresja pól protokołu (PPP)	Potrzebne do inicjalizacji PPP, można zostawić wartość domyślną
Mapa asynchroniczna (PPP)	Jedna z wartości potrzebnych do inicjalizacji PPP, można zostawić wartość domyślną, zakres 0-ffffff
MRU	Maksymalny rozmiar MRU
MTU	Maksymalny rozmiar MTU
Interwał wykrywania łącza (s)	Interwał wykrywania łącza, zakres 0-600
Maksymalna ilość prób	Maksymalna ilość prób połączenia przez L2TP, zakres 0-10
Opcje eksperta	Pole służy do ręcznego dodawania kolejnych wpisów do protokołu L2TP, każdy wpis powinien być oddzielony „;”

4.2.5.6 PPTP

Point-to-Point Tunneling Protocol (PPTP) to protokół, który umożliwi korporacjom rozszerzenie własnej sieci firmowej przez prywatne „tunele” w publicznym Internecie. W efekcie korporacja wykorzystuje sieć rozległą jako jedną dużą sieć lokalną.

Rysunek 4.66 Konfiguracja usługi PPTP

Pole	Opis
Włącz	Włącza/wyłącza usługę PPTP
Adres IP serwera	Adres IP/domena serwera PPTP
Nazwa użytkownika	Nazwa użytkownika do usługi PPTP
Hasło	Hasło do usługi PPTP
Uwierzytelnianie	Wybór trybu uwierzytelniania
Globalne przekazywanie ruchu	Przy włączeniu tej funkcji cały ruch sieciowy będzie przesyłany przez tunel PPTP
Adres sieci wirtualnej	Adres IP sieci dla tunelu PPTP
Maska podsieci wirtualna	Maska podsieci dla tunelu PPTP

Opcje zaawansowane	<input checked="" type="checkbox"/>
Wirtualny adres IP	<input type="text"/>
Wirtualny adres IP serwera	<input type="text"/>
Włącz NAT	<input checked="" type="checkbox"/>
Włącz MPPE	<input type="checkbox"/>
Kompresja adresu/pola kontrolnego (PPP)	<input type="checkbox"/>
Kompresja pól protokołu (PPP)	<input type="checkbox"/>
Mapa asynchroniczna (PPP)	<input type="text" value="ffffff"/>
MRU	<input type="text" value="1500"/>
MTU	<input type="text" value="1500"/>
Interwał wykrywania łącza(s)	<input type="text" value="60"/>
Maksymalna ilość prób	<input type="text" value="0"/>
Opcje eksperta	<input type="text"/>

Rysunek 4.67 Konfiguracja usługi PPTP, ustawienia zaawansowane

Pole	Opis
Wirtualny adres IP	Adres IP klienta PPTP
Wirtualny adres IP serwera	Adres IP tunelu PPTP
Włącz NAT	Włącza/wyłącza NAT
Włącz MPPE	Włącza/wyłącza szyfrowanie MPPE
Kompresja adresu/pola kontrolnego (PPP)	Potrzebne do inicjalizacji PPP, można zostawić wartość domyślną
Kompresja pól protokołu (PPP)	Potrzebne do inicjalizacji PPP, można zostawić wartość domyślną
Mapa asynchroniczna (PPP)	Jedna z wartości potrzebnych do inicjalizacji PPP, można zostawić wartość domyślną, zakres 0-ffffff
MRU	Maksymalny rozmiar MRU
MTU	Maksymalny rozmiar MTU
Interwał wykrywania łącza (s)	Interwał wykrywania łącza, zakres 0-600
Maksymalna ilość prób	Maksymalna ilość prób połączenia przez PPTP, zakres 0-10
Opcje eksperta	Pole służy do ręcznego dodawania kolejnych wpisów do protokołu PPTP, każdy wpis powinien być oddzielony „;”

4.2.5.7 Klient OpenVPN

OpenVPN to protokół wirtualnej sieci prywatnej (VPN) typu open source, który oferuje uproszczone ramy bezpieczeństwa, modułową konstrukcję sieci i multiplatformowość.

Zalety OpenVPN obejmują:

- zabezpieczenia, które działają zarówno przeciwko aktywnym, jak i pasywnym atakom,
- kompatybilność ze wszystkimi głównymi systemami operacyjnymi,
- wysoka prędkość (zwykle 1,4 megabajta na sekundę),
- możliwość konfiguracji wielu serwerów do obsługi wielu połączeń jednocześnie,
- wszystkie funkcje szyfrowania i uwierzytelniania biblioteki OpenSSL,
- zaawansowane zarządzanie pasmem,
- różnorodne opcje tunelowania,
- kompatybilność z kartami inteligentnymi, które obsługują interfejs programowy (API) Windows Crypt.

DMVPN Serwer IPsec IPsec GRE L2TP PPTP **Klient OpenVPN** Serwer OpenVPN Certyfikaty

Konfiguracja klienta OpenVPN

— Klient OpenVPN_1

Włącz	<input checked="" type="checkbox"/>
Protokół	UDP
Adres IP serwera	<input type="text"/>
Port	<input type="text"/>
Tryb pracy	tun (routing)
Uwierzytelnianie	Certyfikat X.509
Globalne przekierowanie ruchu	<input type="checkbox"/>
Włącz uwierzytelnianie TLS	<input checked="" type="checkbox"/>
Włącz NAT	<input checked="" type="checkbox"/>
Kompresja	Brak
Interwał wykrywania łącza(s)	10
Limit czasu wykrywania łącza(s)	120
Szyfrowanie	AES-128-CBC
MTU	1500
Maksymalny rozmiar ramki	1500
Poziom raportowania	ERROR
Opcje eksperta	<input type="text"/>

Trasowanie lokalne

Podsieć	Maska podsieci	Operacja
		<input data-bbox="1295 1019 1316 1041" type="button" value="+"/>

+ Klient OpenVPN_2

+ Klient OpenVPN_3

Rysunek 4.68 Konfiguracja usługi klienta OpenVPN

Pole	Opis
Włącz	Włącza/wyłącza usługę klienta OpenVPN, maksymalnie można uruchomić 3 usługi równocześnie
Protokół	Wybór protokołu użytego do połączenia UDP/TCP
Adres IP serwera	Adres IP/domena serwera OpenVPN
Port	Port, na którym nasłuchuj serwer OpenVPN
Interfejs	Wybór interfejsu użytego do połączenia
Uwierzytelnianie	Wybór sposobu uwierzytelniania
Wirtualny adres IP	Wirtualny adres IP klienta
Wirtualny adres serwera	Wirtualny adres IP serwera
Globalne przekierowanie ruchu	Przy włączeniu tej funkcji cały ruch sieciowy będzie przesyłany przez tunel OpenVPN
Włącz uwierzytelnianie TLS	Włącza/wyłącza uwierzytelnianie przez TLS
Nazwa użytkownika	Nazwa użytkownika usługi OpenVPN
Hasło	Hasło usługi OpenVPN
Włącz NAT	Włącza/wyłącza NAT
Kompresja	Włącza (LZO)/Wyłącza kompresję danych
Interwał wykrywania łącza (s)	Interwał wykrywania łącza, zakres 10-1800
Limit czasu wykrywania łącza (s)	Limit czasu wykrywania łącza, po upływie tego czasu urządzenie ponowi próbę wykrycia łącza
Szyfrowanie	Wybór typu szyfrowania
MTU	Maksymalna wielkość MTU
Maksymalny rozmiar ramki	Maksymalna wielkość ramki
Poziom raportowania	Poziom szczegółowości dla logów usługi
Opcje eksperta	Pole służy do ręcznego dodawania kolejnych wpisów do protokołu OpenVPN, każdy wpis powinien być oddzielony „;”
Trasowanie lokalne	
Podsieć	Adres sieci lokalnej OpenVPN
Maska podsieci	Maska podsieci OpenVPN
Operacja	Dodaje/usuwa wpisy

4.2.5.8 Server OpenVPN

Router BCS-R4G-1W1L wspiera usługę serwera OpenVPN więc możemy utworzyć bezpieczne połączenie punkt-do-punktu lub sieć-do-sieci.

The screenshot shows the 'Konfiguracja serwera OpenVPN' (OpenVPN Server Configuration) page. The interface is divided into several sections:

- Włącz**: A checked checkbox to enable the server.
- Protokół**: A dropdown menu set to 'UDP'.
- Port**: A text input field containing '1194'.
- IP serwera**: An empty text input field.
- Tryb pracy**: A dropdown menu set to 'tun (routing)'.
- Uwierzytelnianie**: A dropdown menu set to 'Brak'.
- Lokalne wirtualne IP**: An empty text input field.
- Zdalne wirtualne IP**: An empty text input field.
- Włącz NAT**: A checked checkbox.
- Kompresja**: A dropdown menu set to 'LZO'.
- Interwał wykrywania łącza**: A text input field containing '60'.
- Limit czasu wykrywania łącza**: A text input field containing '150'.
- Szyfrowanie**: A dropdown menu set to 'Brak'.
- MTU**: A text input field containing '1500'.
- Maksymalny rozmiar ramki**: A text input field containing '1500'.
- Poziom raportowania**: A dropdown menu set to 'ERROR'.
- Opcje eksperta**: An empty text input field.

Below the configuration fields are three tables for user accounts, local routes, and client networks, each with a '+-' button to add or remove entries:

- Konta**: Table with columns 'Nazwa użytkownika', 'Hasło', and 'Operacja'.
- Lokalne trasy**: Table with columns 'Podsieć', 'Maska', and 'Operacja'.
- Podsieć kliencka**: Table with columns 'Nazwa', 'Podsieć', 'Maska', and 'Operacja'.

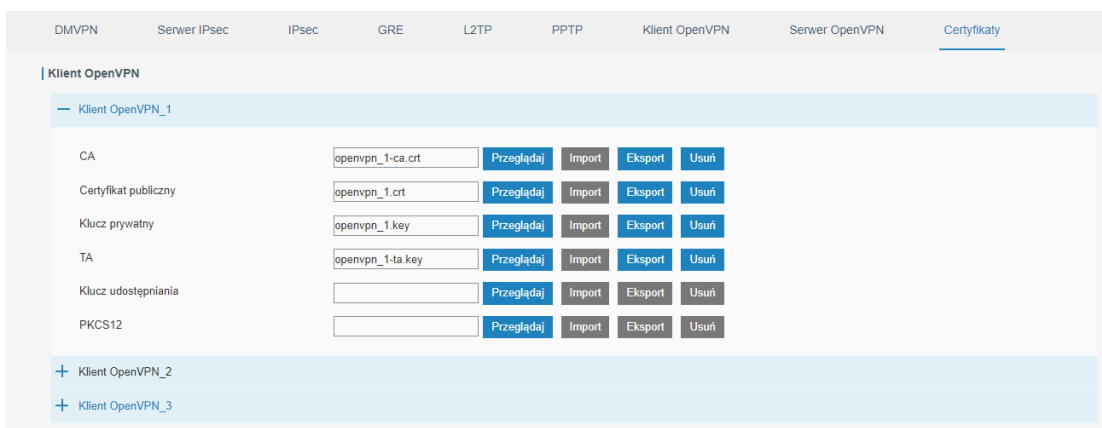
A 'Zapisz' (Save) button is located at the bottom left of the configuration area.

Rysunek 4.69 Konfiguracja serwera OpenVPN

Pole	Opis
Włącz	Włącza/wyłącza usługę serwera OpenVPN
Protokół	Wybór protokołu komunikacyjnego UDP/TCP
Port	Port na jakim ma nasłuchiwać serwer
IP serwera	Adres IP interfejsu, który ma brać udział w połączeniu, pozostawieni tego pola pustego spowoduje, że wszystkie aktywne połączenia będą brały udział w tunelowaniu
Tryb pracy	Wybór trybu pracy tunelu tun/tap
Uwierzytelnianie	Wybór typu uwierzytelniania
Lokalne wirtualne IP	Lokalny adres IP tunelu
Zdalne wirtualne IP	Zdalny adres IP tunelu
Podsieć kliencka	Adres IP sieci dla tunelu
Maska podsieci klienckiej	Maska podsieci dla tunelu
Interwał renegocjacji (s)	Odstęp czasu między kolejnymi próbami negocjacji połączenia
Maksymalna liczba klientów	Maksymalna liczba klientów podłączonych do serwera, zakres 1-128
Włącz CRL	Włącza/wyłącza CRL
Włącz klient-do-klient	Włącza/wyłącza możliwość połączenia między różnymi klientami OpenVPN
Włącz duplikację klientów	Włącza/wyłącza możliwość połączenia kilku klientów na jednym certyfikacie
Włącz NAT	Włącza/wyłącza NAT
Kompresja	Włącza (LZO)/wyłącza (none) kompresję komunikacji
Interwał wykrywania łączy (s)	Interwał czasowy wykrywania połączenia
Szyfrowanie	Wybór typu szyfrowania komunikacji
MTU	Maksymalny rozmiar MTU
Maksymalny rozmiar ramki	Maksymalny rozmiar ramki
Poziom raportowania	Poziom szczegółowości dla logów usługi
Opcje eksperta	Pole służy do ręcznego dodawania kolejnych wpisów do protokołu OpenVPN, każdy wpis powinien być oddzielony „;”
Trasowanie lokalne	
Podsieć	Adres sieci lokalnej OpenVPN
Maska	Maska podsieci OpenVPN
Operacja	Dodaje/usuwa wpisy
Konta	
Nazwa użytkownika	Nazwa użytkownika klienta OpenVPN
Hasło	Hasło klienta OpenVPN
Operacja	Dodaje/usuwa wpisy

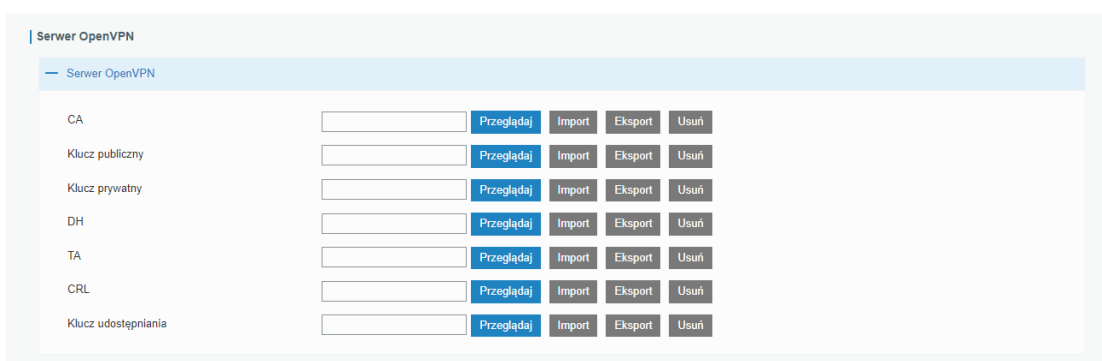
4.2.5.9 Certyfikaty

Ta zakładka służy do importu/eksportu certyfikatów wymaganych do prawidłowego działania usług związanych z OpenVPN oraz IPsec.



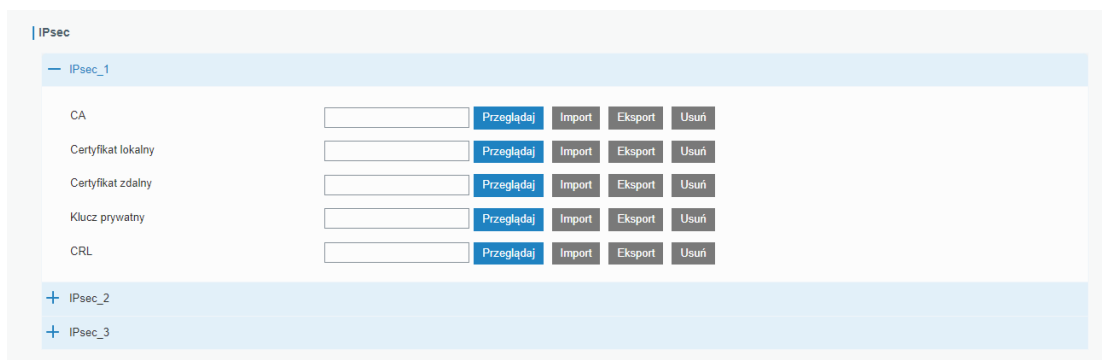
Rysunek 4.70 Import/eksport certyfikatów dla klientów OpenVPN

Pole	Opis
CA	Import/eksport certyfikatu CA
Klucz publiczny	Import/eksport klucza publicznego
Klucz prywatny	Import/eksport klucza prywatnego
TA	Import/eksport klucza TA
Klucz udostępniania	Import/eksport klucza statycznego
PKCS12	Import/eksportu certyfikatu PKCS12



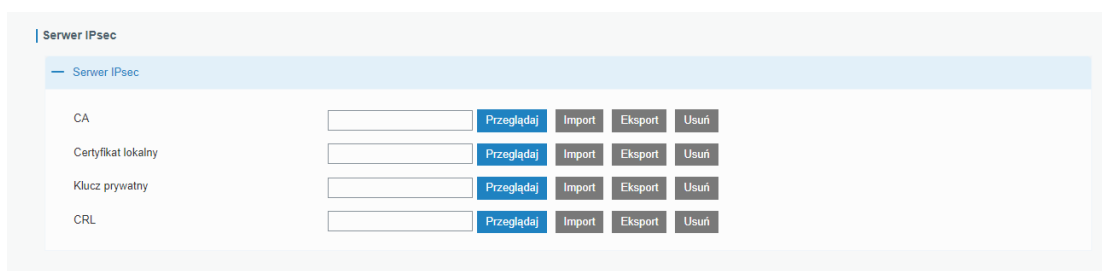
Rysunek 4.71 Import/eksport certyfikatów dla serwera OpenVPN

Pole	Opis
CA	Import/eksport certyfikatu CA
Klucz publiczny	Import/eksport klucza publicznego
Klucz prywatny	Import/eksport klucza prywatnego
DH	Import/eksport klucza DA
TA	Import/eksport klucza TA
CRL	Import/eksport certyfikatu CRL
Klucz udostępiania	Import/eksport klucza statycznego



Rysunek 4.72 Import/eksport certyfikatów dla klientów IPsec

Pole	Opis
CA	Import/eksport certyfikatu CA
Certyfikat lokalny	Import/eksport certyfikatu lokalnego
Certyfikat zdalny	Import/eksport certyfikatu zdalnego
Klucz prywatny	Import/eksport klucza prywatnego
CRL	Import/eksport certyfikatu CRL



Rysunek 4.73 Import/eksport certyfikatów dla serwera IPsec

Pole	Opis
CA	Import/eksport certyfikatu CA
Certyfikat lokalny	Import/eksport certyfikatu lokalnego
Certyfikat zdalny	Import/eksport certyfikatu zdalnego
CRL	Import/eksport certyfikatu CRL

4.2.6 IP Passthrough

Funkcja IP Passthrough przekazuje adres IP przydzielony przez usługodawcę do jednego urządzenia podłączonego pod interfejs LAN routera.

Aby włączyć funkcję należy:

1. Włączyć funkcję (**Włącz**)
2. Ustawić w jakim trybie ma działać funkcja
3. Ustawić MAC adres urządzenia odbiorczego jeśli została wybrany tryb „DHCP-Fixed”

The screenshot shows the 'IP Passthrough' configuration page. At the top, there's a header 'IP Passthrough'. Below it, the 'Włącz' (Enable) checkbox is checked. The 'Tryb przekazywania' (Mode) dropdown is set to 'DHCP-Fixed'. There is an empty text input field for 'MAC'. At the bottom, there is a blue 'Zapisz' (Save) button.

Rysunek 4.74 Konfiguracja funkcji IP Passthrough

4.2.7 Routing

4.2.7.1 Routing statyczny

Routing statyczny to ręcznie dodane wpisy routingu. Informacje o trasie pakietu dodawane są ręcznie, a nie ustalane automatycznie za pomocą routingu dynamicznego. Po dodaniu wpisów konkretne pakiety będą kierowane na trasę zdefiniowaną przez użytkownika.

Aby dodać wpis do tablicy należy:

1. Kliknąć na **+** w kolumnie **Operacja**
2. Podać adres IPv4/IPv6 sieci docelowej (**Cel**)
3. Podać maskę podsieci/długość prefiksu dla sieci docelowej (**Maska podsieci/Długość prefiksu**)
4. Interfejs routera przez, który pakiety mają wydostać się w kierunku urządzenia docelowego (**Interfejs**)
5. Adres kolejnego routera przez, który pakiety mają wędrować (**Brama**)
6. Ustawić priorytet trasy, im mniejszy numer tym większy priorytet (**Dystans**)
7. Kliknąć przycisk **Zapisz**

The screenshot shows the 'Routing statyczny' configuration page. It has tabs for 'Routing statyczny', 'RIP', 'OSPF', and 'Filtry Routingu'. The 'Routing statyczny' tab is active. Below it is a table with the following columns: 'Cel', 'Maska podsieci/długość prefiksu', 'Interfejs', 'Brama', 'Dystans', and 'Operacja'. There are five rows of data, each with a plus icon in the 'Operacja' column. At the bottom, there is a blue 'Zapisz' (Save) button.

Cel	Maska podsieci/długość prefiksu	Interfejs	Brama	Dystans	Operacja
213.158.199.5	255.255.255.255	Cellular 0	100.85.93.182	1	+
213.158.199.1	255.255.255.255	Cellular 0	100.85.93.182	1	+
114.114.114.114	255.255.255.255	Cellular 0	100.85.93.182	1	+
8.8.8.8	255.255.255.255	Cellular 0	100.85.93.182	1	+
0.0.0.0	0.0.0.0	Cellular 0	100.85.93.182	1	+

Rysunek 4.75 Konfiguracja wpisów statycznego routingu

4.2.7.2 RIP

Protokół RIP (Routing Information Protocol) to protokół routingu dynamicznego przeznaczony dla małych sieci. Protokół ten używa licznika przeskoków do pomiaru odległości od urządzenia źródłowego do urządzenia docelowego, który nazwany jest Metryką. W protokole RIP liczba przeskoków od routera do bezpośrednio podłączonej sieci wynosi 0, a liczba przeskoków do kolejnych sieci zwiększa się o 1. Aby ograniczyć czas zbieżności metryka może mieć wartość całkowitą 0-15, każda metryka równa lub wyższa niż 16 jest określana jako nieskończoność więc sieć docelowa lub host są nieosiągalne co powoduje, że protokół RIP nie jest dobrym wyborem do rozległych sieci. Aby poprawić wydajność i zapobiec pętlom routingu, protokół RIP obsługuje funkcję podziału horyzontu, która nie pozwala odbierać od innych routerów informacji na temat sieci, o których informuje bieżący router. Każdy router, na którym działa protokół RIP zarządza tabelą routingu, która zawiera trasy umożliwiające dotarcie do wszystkich sieci docelowych. Aby uruchomić protokół RIP należy włączyć usługę (**Włącz**) i przeprowadzić jej konfigurację, router daje także możliwość rozszerzonej konfiguracji protokołu po zaznaczeniu opcji **Pokaż opcje zaawansowane**.

Routing statyczny	RIP	OSPF	Filtry Routingu
Konfiguracja RIP			
Włącz	<input checked="" type="checkbox"/>		
Odstęp rozgłoszeniowy	<input type="text" value="30"/>		s
Czas starzenia	<input type="text" value="180"/>		s
Czas usuwania	<input type="text" value="120"/>		s
Wersja	<input type="text" value="v2"/>		▼
Pokaż opcje zaawansowane	<input checked="" type="checkbox"/>		
Default Information Originate	<input type="checkbox"/>		
Domyślna metryka	<input type="text" value="1"/>		
Przekazywanie tras bezp. podl.	<input type="checkbox"/>		
Przekazywanie tras statycznych	<input type="checkbox"/>		
Przekazywanie OSPF	<input type="checkbox"/>		

Rysunek 4.76 Wstępna konfiguracja protokołu RIP

RIP Settings	
Pole	Opis
Włącz	Włącza/wyłącza obsługę protokołu RIP
Odstęp rozgłoszeniowy	Odstęp czasowy między kolejnymi rozesłaniami informacji o trasach, wartość wyrażona w sekundach
Czas starzenia	Określa czas starzenia się trasy. Jeśli w tym okresie do routera nie dotrze pakiet aktualizujący daną trasę to metryka trasy zostanie ustawiona na wartość 16, czyli sieć zostanie określona jako niedostępna, wartość wyrażona w sekundach
Czas usuwania	Czas po jakim trasy z metryką o wartości 16 zostaną całkowicie usunięte z tablicy routingu, wartość wyrażona w sekundach
Wersja	Wersja protokołu RIP jakiej używa router (v1 lub v2)
Pokaż opcje zaawansowane	Pokazuje/ukrywa opcje zaawansowane
Default Information Originate	Włącza/wyłącza rozsyłanie komendy Default Information Originate
Domyślna metryka	Koszt przejścia przez ten router, o tyle zwiększy się metryka podczas przejścia przez ten router
Przekazywanie tras bezp. podł.	Włącza/wyłącza przekazywanie tras sieci bezpośrednio podłączonych
Metryka	Po włączeniu opcji „Przekazywanie tras bezp. podł.” należy ustalić dla niej koszt przejścia
Przekazywanie tras statycznych	Włącza/wyłącza przekazywanie tras z routingu statycznego
Metryka	Po włączeniu opcji „Przekazywanie tras statycznych” należy ustalić dla niej koszt przejścia
Przekazywanie OSPF	Włącza/wyłącza przekazywanie tras z protokołu OSPF
Metryka	Po włączeniu opcji „Przekazywanie OSPF” należy ustalić dla niej koszt przejścia

Zarządzanie dystansem/metrykami

Dystans	Adres IP	Maska	Nazwa ACL	Operacja
				+

Metryka	Tryb polityki	Interfejs	Nazwa ACL	Operacja
				+

Polityka filtrowania

Typ polityki	Nazwa polityki	Tryb polityki	Interfejs	Operacja
				+

Interfejs pasywny

Interfejs pasywny	Operacja
	+

Interfejs

Interfejs	Wysyłaj wersję	Odbieraj wersję	Podzielony horyzont	Tryb uwierzytelniania	Klucz uwierzytelniania	Łańcuch uwierzytelniający	Operacja
							+

Sąsiad

Adres	Operacja
	+

Sieć

Adres IP	Maska	Operacja
		+

[Zapisz](#)

Rysunek 4.77 Zaawansowana konfiguracja protokołu RIP

Grupa ustawień	Pole	Opis
Zarządzanie dystansem/ metrykami	Dystans	Ustala dystans administracyjny
	Adres IP	Adres IP trasy RIP
	Maska	Maska podsieci trasy RIP
	Nazwa ACL	Nazwa ACL trasy RIP
	Operacja	Dodaje/usuwa wpisy
	Metryka	Ustala wartość metryki
	Tryb polityki	Do czego odnosi się polityka. Wybierz spośród „in” lub „out”
	Interfejs	Wybór interfejsu
	Nazwa ACL	Nazwa ACL dla trasy RIP
	Operacja	Dodaje/usuwa wpisy
Polityka filtrowania	Typ polityki	Rodzaj polityki
	Nazwa polityki	Nazwa polityki
	Tryb polityki	Do czego odnosi się polityka. Wybierz spośród „in” lub „out”
	Interfejs	Wybór interfejsu
	Operacja	Dodaje/usuwa wpisy
Interfejs pasywny	Interfejs pasywny	Wybór interfejsu pasywnego, czyli takiego, który będzie odbierał pakiety RIP, ale nie będzie ich wysyłał
	Operacja	Dodaje/usuwa wpisy
Interfejs	Interfejs	Wybór interfejsu
	Wersja wysyłana	Wersja pakietów RIP wysyłanych z interfejsu
	Wersja odbierana	Wersja pakietów RIP jakie odbiera interfejs
	Podzielony horyzont	Włączenie/wyłączenie funkcji podziału horyzontu
	Tryb uwierzytelniania	Wybór czy klucz komunikacji ma być szyfrowany (tekst lub md5)
	Klucz uwierzytelniający	Treść klucza komunikacji dla RIPv2
	Łańcuch uwierzytelniający	Klucz szyfrowania dla RIPv2
	Operacja	Dodaje/usuwa wpisy
Sąsiad	Adres IP	Adres IP sąsiada
	Operacja	Dodaje/usuwa wpisy
Sieć	Adres IP	Adres IP interfejsu do rozgłaszania pakietów RIP
	Maska	Maska podsieci interfejsu do rozgłaszania pakietów RIP
	Operacja	Dodaje/usuwa wpisy

4.2.7.3 OSPF

Protokół OSPF (Open Shortest Path First), to protokół routingu oparty na protokole bramy wewnętrznej opracowany przez IETF. Jeśli router chce uruchomić protokół OSPF, powinien istnieć identyfikator routera, który można skonfigurować ręcznie. Jeśli nie skonfigurowano identyfikatora routera, system automatycznie wybierze adres IP interfejsu jako identyfikator routera. Kolejność wyboru jest następująca:

- Jeśli skonfigurowany jest adres interfejsu pętli, jako identyfikator routera zostanie użyty ostatnio skonfigurowany adres IP interfejsu pętli;
- Jeśli nie skonfigurowano adresu interfejsu pętli, system wybierze interfejs z największym adresem IP jako identyfikator routera.

Protokół ten rozsyła pięć typów pakietów:

- Pakiet Hello
- Pakiet DD (pakiet opisu bazy danych)
- Pakiet LSR (pakiet żądania stanu łącza)
- Pakiet LSU (pakiet aktualizacji stanu łącza)
- Pakiet LSAck (pakiet potwierdzenia łącza Sate)

Sąsiad i sąsiedzi

Po uruchomieniu router OSPF wyśle pakiety Hello przez interfejs OSPF. Po otrzymaniu pakietu Hello router OSPF sprawdzi parametry zdefiniowane w pakiecie. Jeśli jest spójny, zostanie utworzona relacja sąsiedztwa. Nie wszystkie dopasowane strony w relacji sąsiedzkiej mogą tworzyć relację międzysieciową. Zależy to od typu sieci. Tylko wtedy, gdy obie strony pomyślnie wymienią pakiety DD i osiągnięta zostanie synchronizacja LSDB, można w prawdziwym sensie ukształtować sąsiedztwo. LSA opisuje topologię sieci wokół routera, LSDB opisuje topologię całej sieci.

Routing statyczny	RIP	OSPF	Filtry Routingu
Konfiguracja OSPF			
Włącz		<input checked="" type="checkbox"/>	
ID routera		<input type="text"/>	
Typ ABR		<input type="text" value="cisco"/>	
Zgodność z RFC1583		<input checked="" type="checkbox"/>	
Nieprzezrocyste LSA (OSPF)		<input type="checkbox"/>	
Opóźnienie obliczeń SPF		<input type="text" value="0"/>	ms
Czas inicjalizacji SPF		<input type="text" value="50"/>	ms
Maksymalny czas SPF		<input type="text" value="5000"/>	ms
Przepustowość referencyjna		<input type="text" value="100"/>	mbit

Rysunek 4.78 Protokół OSPF konfiguracja wstępna

Konfiguracja OSPF	
Pole	Opis
Włącz	Włącza/wyłącza OSPF
ID routera	ID routera (adres IP) dla pakietów LSA
Typ ABR	Typ ABR (do wyboru cisco, ibm, standard, shortcut)
Zgodność z RFC1583	Włącza/wyłącza zgodność ze standardem RFC1583
Nieprzezrocyste LSA (OSPF)	Włącza/wyłącza nieprzezrocyste pakiety LSA
Opóźnienie obliczeń SPF	Ustawia czas opóźnienia dla obliczeń SPF, zakres 0-6000000 milisekund
Czas inicjalizacji SPF	Ustawia czas inicjalizacji SPF, zakres 0-6000000 milisekund
Maksymalny czas SPF	Ustawia maksymalny czas SPF, zakres 0-6000000 milisekund
Przepustowość referencyjna	Przepustowość referencyjna, zakres 1-4294967 Mbit

Interfejs

Interfejs	Interwał Hello(s)	Czas starzenia(s)	Czas retransmisji(s)	Opóźnienie transmisji(s)	Operacja
					+

Zaawansowane opcje interfejsu

Interfejs	Połączenie	Koszt	Priorytet	Uwierzytelnianie	ID klucza	Klucz	Operacja
							+

Interfejs pasywny

Interfejs pasywny	Operacja	
		+

Rysunek 4.79 Protokół OSPF konfiguracja interfejsów

Pole	Opis
Interfejs	
Interfejs	Wybór interfejsu, którego dotyczy wpis
Interwał Hello (s)	Odstęp czasowy między kolejnymi rozgłoszeniami pakietu Hello. Jeśli na routerze sąsiadującym ten czas będzie inny to nie będzie można ustalić sąsiada, zakres 1-65535 sekund
Czas starzenia (s)	Czas, po którego upływnięciu i nieotrzymaniu pakietu Hello od sąsiada router stwierdzi, że sąsiad jest niedostępny. Jeśli na routerze sąsiadującym ten czas będzie inny to nie będzie można ustalić sąsiada
Czas retransmisji (s)	Gdy router powiadamia sąsiada o LSA, wymagane jest potwierdzenie. Jeżeli w okresie retransmisji nie zostanie odebrany żaden pakiet potwierdzenia, to LSA zostanie ponownie przesłane do sąsiada. Zakres 3-65535 sekund
Opóźnienie transmisji (s)	Czas opóźnienia, po którym rozpocznie się odliczanie czasu starzenia się LSA
Operacja	Dodaje/usuwa wpisy
Zaawansowane opcje interfejsu	
Interfejs	Wybór interfejsu, którego dotyczy wpis
Sieć	Wybór typu połączenia dla OSPF
Koszt	Koszt OSPF dla interfejsu. Zakres 1-65535
Priorytet	Priorytet OSPF dla interfejsu. Zakres 1-255
Uwierzytelnianie	Wybór typu uwierzytelniania Simple: podajemy hasło, które potem potwierdzamy MD5: podajemy klucz szyfrowania i hasło, które potem trzeba potwierdzić
Klucz szyfrowania	Klucz szyfrowania MD5
Hasło	Hasło komunikacji
Operacja	Dodaje/usuwa wpisy
Interfejs pasywny	
Interfejs pasywny	Wybór interfejsu pasywnego
Operacja	Dodaje/usuwa wpisy

Sieć				
Adres IP	Maska	ID strefy	Operacja	
			+	

Sąsiad				
Adres IP	Priorytet	Poll	Operacja	
			+	

Strefa				
ID strefy	Strefa	Bez sumowania	Uwierzytelnianie	Operacja
				+

Rysunek 4.80 Protokół OSPF konfiguracja sieci

Pole	Opis
Sieć	
Adres IP	Adres IP lokalnej sieci
Maska	Maska podsieci lokalnej sieci
ID strefy	ID obszaru, do którego należy router
Operacja	Dodaje/usuwa wpisy
Sąsiad	
Adres IP	Adres IP sąsiada
Priorytet	Priorytet sąsiada
Poll	Odstęp czasu rozsyłania pakietu Hello do sąsiada
Operacja	Dodaje/usuwa wpisy
Strefa	
ID strefy	Numer ID strefy OSPF (Adres IP)
Typ strefy	Rodzaj strefy (STUB, NSSA), strefa backbone (ID 0.0.0.0) nie może być ustawiona jako STUB lub NSSA
Bez sumowania	Wyłącza sumaryzację tras
Uwierzytelnianie	Wybór rodzaju autentykacji (simple, MD5)
Operacja	Dodaje/usuwa wpisy

Zaawansowane opcje stref

Zasięg strefy

ID strefy	IP	Maska	Bez rozgłaszania	Cost	Operacja
					+

Filtry stref

ID strefy	Typ filtra	Nazwa ACL	Operacja
			+

Wirtualne połączenia stref

ID strefy	Adres ABR	Uwierzytelnianie	Klucz szyfrowania	Hasło	Interwał Hello	Czas starzenia	Czas retransmisji	Opóźnienie transmisji	Operacja
									+

Rysunek 4.81 Konfiguracja protokołu OSPF zaawansowana konfiguracja stref

Pole	Opis
Zasięg strefy	
ID strefy	ID strefy dla interfejsu, który ma uruchomiony protokół OSPF (Adres IP)
IP	Adres IP
Maska	Maska podsieci
Bez rozgłaszania	Włącza/wyłącza blokowanie rozgłaszania tras poza strefę
Koszt	Koszt, zakres 0-16777215
Operacja	Dodaje/usuwa wpisy
Filtry stref	
ID strefy	ID strefy do filtracji
Typ filtra	Typ filtrowania strefy
Nazwa ACL	Nazwa ACL, którą ustawiana jest w zakładce Routing Filtering (sekcja 4.2.7.4)
Operacja	Dodaje/usuwa wpisy
Wirtualne połączenia stref	
ID strefy	Numer ID strefy OSFP
Adres ABR	Adres routera ARB, który styka się z innymi strefami
Uwierzytelnianie	Typ autentykacji (simple, MD5)
Klucz szyfrowania	Klucz szyfrowania dla MD5
Hasło	Hasło uwierzytelniania
Interwał Hello	Odstęp czasu między kolejnymi rozesłaniami pakietu Hello, zakres 1-65535
Czas starzenia	Czas, po którego upływnięciu i nieotrzymaniu pakietu Hello od sąsiada router stwierdzi, że sąsiad jest niedostępny, zakres 1-65535
Czas retransmisji	Odstęp czasu między kolejnymi próbami wysłania LSA, zakres 1-65535
Opóźnienie transmisji	Czas opóźnienia transmisji LSA, zakres 1-65535
Operacja	Dodaje/usuwa wpisy

Przekazywanie

Typ przekazywania	Metryka	Typ metryki	Mapa tras	Operacja
+				

Opcje zaawansowane przekazywania

Zawsze przekazuj trasy domyślne

Metryka domyślna przekazywanej trasy

Typ metryki domyślnej przekazywanej trasy

Zarządzanie dystansem

Typ strefy	Dystans	Operacja
+		

Zapisz

Rysunek 4.82 Protokół OSPF konfiguracja przekazywania tras routing

Pole	Opis
Przekazywanie	
Typ przekazywania	Typ routingu z jakiego mają być przekazywane trasy
Metryka	Metryka routera przekazującego. Zakres 0-16777214
Typ metryki	Typ metryki
Mapa tras	Nazwa mapy trasy
Operacja	Dodaje/usuwa wpisy
Opcje zaawansowane przekazywania	
Zawsze przekazuj trasy domyślne	Włącza/wyłącza rozsyłanie domyślnego przekazywania tras po uruchomieniu
Metryka domyślna przekazywanej trasy	Domyślna metryka przekazywania. Zakres 0-16777214
Typ metryki domyślnej przekazywanej trasy	Domyślny typ metryki (0,1,2)
Zarządzanie dystansem	
Typ strefy	Typ strefy
Dystans	Zasięg na jaki docierać ma przekazywanie tras. Zakres 1-255
Operacja	Dodaje/usuwa wpisy

4.2.7.4 Filtry routingu

W tej zakładce możemy przeprowadzić konfigurację filtrów dla routingu.

The screenshot shows a web interface for configuring routing filters. At the top, there are tabs for 'Routing statyczny', 'RIP', 'OSPF', and 'Filtry Routingu'. The 'Filtry Routingu' tab is active. Below it, there are two main sections: 'Lista kontroli dostępu (ACL)' and 'IP Prefix-List'. Each section contains a table with columns for configuration parameters and an 'Operacja' column with a '+' icon. A 'Zapisz' button is located at the bottom left of the interface.

Rysunek 4.83 Konfiguracja filtrów dla routingu

Pole	Opis
Lista kontroli dostępu ACL	
Nazwa	Nazwa wpisu ACL
Akcja	Rodzaj akcji jakiej ma dotyczyć wpis (permit, deny)
Dowolne	Po zaznaczeniu nie trzeba podawać adresu IP i maski podsieci
IP	Adres IP
Maska	Maska podsieci
Operacja	Dodaje/usuwa wpisy
IP Prefix-List	
Nazwa	Nazwa wpisu
Sequence Number	Lista prefiksów może być używana w wielu regułach, każda reguła odpowiada jednemu numerowi sekwencji, zakres 1-4294967295
Akcja	Rodzaj akcji jakiej ma dotyczyć wpis (permit, deny)
Dowolne	Po zaznaczeniu nie trzeba podawać adresu IP i maski podsieci
IP	Adres IP
Maska	Maska podsieci
Długość GE	Minimalna ilość bitów w masce podsieci, zakres 0-32
Długość LE	Maksymalna ilość bitów w masce podsieci, zakres 0-32
Operacja	Dodaje/usuwa wpisy

4.2.8 VRRP

W tej zakładce możemy skonfigurować usługę VRRP (Virtual Router Redundancy Protocol). Usługa ta pozwala na automatyczne przełączanie się hostów między routerami w razie awarii jednego z nich co zapewnia większą niezawodność sieci. Po poprawnym skonfigurowaniu VRRP na wszystkich routerach w sieci mechanizmy usługi automatycznie wybiorą wirtualny router główny, który będzie kierował ruch sieciowy na zewnątrz sieci. Wybór urządzenia głównego odbywa się poprzez ustawienie priorytetu urządzenia. Kiedy router główny zostanie już ustalony wysyła on regularnie do wszystkich routerów podrzędnych komunikat „alive”, jeśli routery zapasowe nie otrzymają w określonym czasie komunikatu „alive” mechanizm VRRP wybierze nowy router główny na podstawie priorytetu przydzielonego urządzeniom. Jeśli obecny router główny otrzyma komunikat od urządzenia o wyższym priorytecie zostanie zdegradowany i routerem głównym zostanie nowe urządzenie o wyższym priorytecie. Konfiguracja urządzeń w sieci ogranicza się tylko do podania wirtualnego adresu IP routera jako adres bramy domyślnej.

Aby skonfigurować usługę należy:

1. Włączyć usługę (**Włącz**)
2. Wybrać interfejs routera, do którego podłączone są urządzenia w sieci lokalnej
3. Ustawić numer ID grupy routerów, który na wszystkich routerach w grupie musi być taki sam (**ID grupy**)
4. Ustawić adres IP wirtualnego routera, który musi być adresem przedzielonym już do jednego z routerów w grupie, a nie dodatkowym adresem logicznym (**Wirtualne IP**)
5. Ustawić priorytet dla routera (**Priorytet**)
6. Ustawić częstotliwość wysyłania wiadomości „alive” wyrażony w sekundach (**Interwał rozgłaszania (s)**)
7. Włączyć/wyłączyć tryb wywłaszczenia, dzięki któremu router zapasowy o wyższym priorytecie może wywłaszczyć router główny o niższym priorytecie
8. Ustawić serwery DNS (**Pierwszy serwer IPv4/Drugi serwer IPv4**)
9. Ustawić parametry związane z usługą **Detekcja PING** takie jak: odstęp między zapytaniami ping (**Interwał**), odstęp między kolejnymi próbami zapytania jeśli pierwsze się nie uda (**Czas ponowienia**), maksymalny czas oczekiwania na odpowiedź po zapytaniu ping (**Limit oczekiwania**), maksymalną ilość prób wykonania zapytania ping (**Maksymalna ilość prób**)

VRRP

| Status VRRP

Status

NIEDOSTĘPNY

| Konfiguracja VRRP

Włącz

Interfejs Bridge0

Wirtualne ID routera 1

Wirtualne IP

Priorytet 100

Interwał rozgłaszania (s) 1

Tryb wywłaszczenia

Pierwszy serwer IPv4 8.8.8.8

Drugi serwer IPv4 114.114.114.114

Interwał (ICMP) 300 s

Czas ponowienia (ICMP) 5 s

Limit oczekiwania (ICMP) 3 s

Maksymalna ilość prób (ICMP) 3

Zapisz

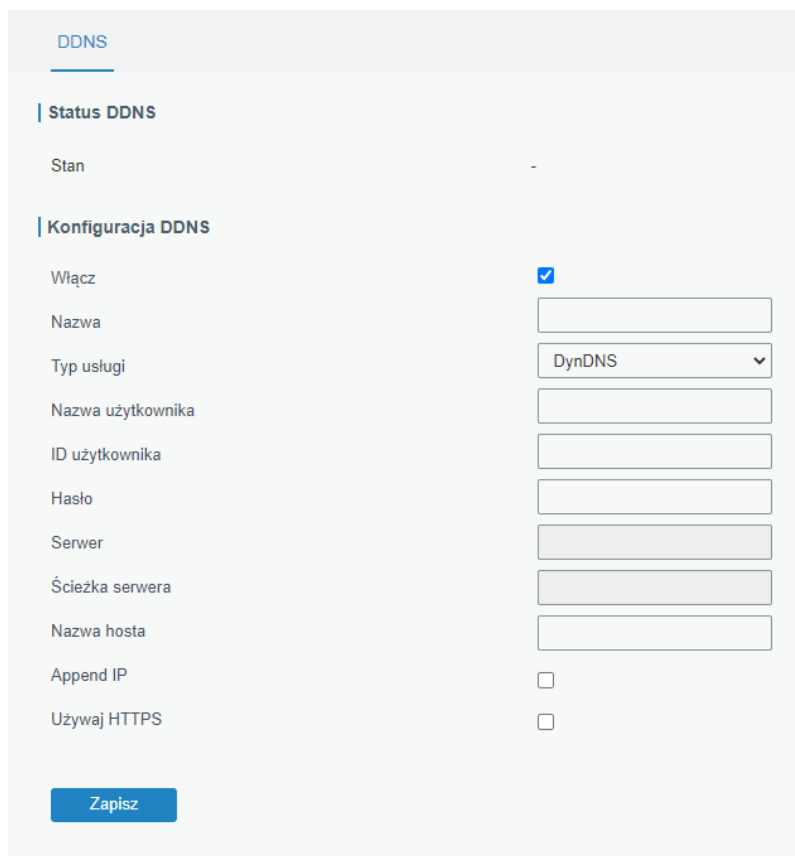
Rysunek 4.84 Konfiguracja usługi VRRP

4.2.9 DDNS

W tej zakładce możemy skonfigurować usługę DDNS (Dynamic Domain Name System), dzięki której możemy połączyć się z naszym routerem za pomocą zarejestrowanej nazwy domeny, jeśli nasz usługodawca oferuje publiczny, zmienny lub stały adres IP. Przed rozpoczęciem konfiguracji należy zarejestrować konto u jednego z usługodawców DDNS.

Aby skonfigurować usługę należy:

1. Włączyć usługę (**Włącz**)
2. Wybrać usługodawcę (**Typ usługi**)
3. Wypełnić pola, które usługodawca wymaga do uzyskania połączenia (należy zapoznać się z instrukcją usługodawcy)
4. Kliknąć przycisk **Zapisz**



The screenshot shows a web interface for configuring DDNS. At the top, there is a tab labeled "DDNS". Below it, the "Status DDNS" section shows "Stan" as "-". The "Konfiguracja DDNS" section contains several settings:

- Włącz**: A checked checkbox.
- Nazwa**: An empty text input field.
- Typ usługi**: A dropdown menu with "DynDNS" selected.
- Nazwa użytkownika**: An empty text input field.
- ID użytkownika**: An empty text input field.
- Hasło**: An empty text input field.
- Serwer**: A greyed-out text input field.
- Ścieżka serwera**: A greyed-out text input field.
- Nazwa hosta**: An empty text input field.
- Append IP**: An unchecked checkbox.
- Używaj HTTPS**: An unchecked checkbox.

At the bottom of the configuration section is a blue button labeled "Zapisz".

Rysunek 4.85 Konfiguracja usługi DDNS

4.3 USTAWIENIA SYSTEMOWE

4.3.1 Ustawienia podstawowe

4.3.1.1 Główne

W tej zakładce możemy skonfigurować podstawowe dane dotyczące urządzenia jak jego nazwa (**Nazwa urządzenia**), czas do wylogowania przy braku aktywności wyrażony w sekundach (**Wylogowanie przy bezczynności (s)**) i włączyć/wyłączyć szyfrowanie haseł (**Szyfrowanie haseł**). Dodatkowo możemy tutaj pobrać, usunąć oraz zaimportować (klikamy **Przeglądaj**, wybieramy plik na dysku, następnie klikamy **Import**) pliki związane z certyfikatem i kluczem HTTPS.

Rysunek 4.86 Ustawienia główne

4.3.1.2 Data i czas

W tej zakładce możemy zmienić ustawienia w zakresie daty i czasu. Domyślnie router korzysta z serwera NTP *pool.ntp.org*, ale możemy ustawić synchronizację z przeglądarką lub ręcznie ustawić datę i godzinę za pomocą opcji **Typ synchronizacji**. Opcja **Aktualny czas** wyświetla aktualną datę i godzinę, w opcji **Strefa czasowa** możemy ustawić strefę czasową w jakiej znajduje się router, a w opcjach **Pierwszy serwer NTP** i **Drugi serwer NTP** możemy podać adresy IP serwerów NTP. Dodatkowo możemy uruchomić funkcję serwera NTP (**Włącz serwer NTP**) na urządzeniu.

Rysunek 4.87 Funkcja Data i czas

4.3.1.3 Email

W tej zakładce możemy skonfigurować dane do konta email, którego możemy użyć do wysyłania powiadomień o alertach, które pojawią się na routerze (*sekcja 4.3.7.2*). Aby uruchomić usługę wysyłania wiadomości email z routera na konkretne adresy email należy:

1. Włączyć funkcję (**Włącz**)
2. Skonfigurować konto pocztowe, które będzie nadawcą wiadomości podając: adres email, hasło do tego konta, adres serwera SMTP, port na jakim działa usługa SMTP oraz rodzaj szyfrowania hasła. Poprawność konfiguracji możemy sprawdzić klikając w przycisk **Test**.

The screenshot shows the 'Email' configuration page with the following fields:

- Włącz:** Checked (blue checkmark)
- Adres email:** xxxxxxxx@xxxx.com
- Hasło:**
- Serwer SMTP:** smtp.gmail.com
- Port:** 465
- Szyfrowanie:** TLS/SSL (dropdown menu)
- Test:** Button

Rysunek 4.88 Konfiguracja kont email krok 1 i 2

3. Dodać odbiorców wiadomości klikając na **+** w kolumnie **Operacja** w grupie **Lista adresów email** i uzupełniając **adres email** oraz opis **odbiorcy**

Adres email	Opis	Operacja
aaaaaaa@aaaa.com	description1	X
bbbbbbb@bbb.com	description2	X
ccccccc@ccc.com	description3	X
		+

Rysunek 4.89 Konfiguracja kont email krok 3

4. Utworzyć grupę odbiorców klikając na **+** w kolumnie **Operacja** w **Grupa adresów email** podając **ID grupy** z zakresu 1-100 oraz **opis** i dodać do niej dodane wcześniej adresy email (wybieramy konkretny adres w oknie **Lista** i klikamy na **>**, kliknięcie **>** spowoduje dodanie wszystkich adresów do grupy) i kliknąć przycisk **Zapisz**.

The screenshot shows the 'Lista grup email' page with the following fields and actions:

- ID grupy:** 1
- Opis:** description1
- Lista:** Empty list box
- Wybrane:** List containing aaaaaaaa@aaaa.com, bbbbbbbb@bbb.com, and cccccccc@ccc.com
- Operacje:** > > < <
- Buttons:** Zapisz, Anuluj

Rysunek 4.90 Konfiguracja kont email krok 4

4.3.2 Telefony i SMS

4.3.2.1 Telefony

W tej zakładce możemy utworzyć listę numerów telefonów oraz pogrupować je, aby można było w uruchamiać połączenie z Internetem za pomocą połączenia telefonicznego lub wiadomość SMS, a także odbierać powiadomienia SMS o stanie urządzenia. Aby dodać telefon do listy i utworzyć grupę należy:

1. Kliknąć na **+** w **Lista numerów telefonów**
2. Wpisać **numer** z prefiksem kraju (np. +48) i **opis**

Numer	Opis	Operacja
+48222111333	phone2	
+48111222333	phone1	

Rysunek 4.91 Dodawanie numerów telefonów kroki 1 i 2

3. Kliknąć na **+** w **Grupy numerów telefonów**
4. Dodać grupę telefonów podając jej **ID grupy** z zakresu 1-100 oraz **opis** i dodać do niej dodane wcześniej numery telefonów (wybieramy konkretny numer w oknie **Lista** i klikamy na , kliknięcie spowoduje dodanie wszystkich numerów telefonu do grupy) i kliknąć przycisk **Zapisz**

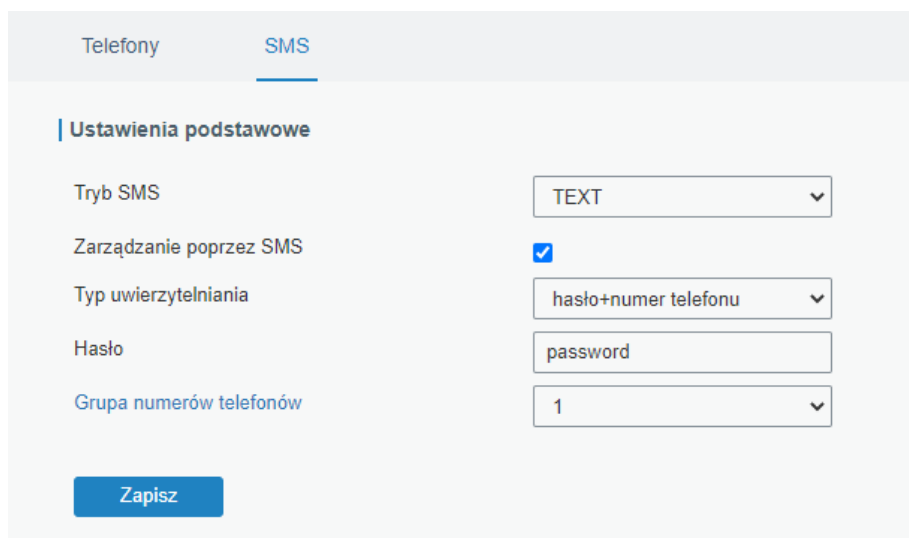
Rysunek 4.92 Dodawanie numerów telefonów krok 3 i 4

4.3.2.2 SMS

W tej zakładce możemy zarządzać modulem wiadomości SMS w routerze.

Ustawienia podstawowe

W tej grupie ustawić rodzaj wiadomości SMS (**Tryb SMS**), uruchomić funkcję kontroli routera za pomocą SMS (**Zarządzanie poprzez SMS**), rodzaj uwierzytelniania podczas kontroli za pomocą SMS (**Typ uwierzytelniania**), jeśli wybierzemy uwierzytelnianie za pomocą numeru telefonu i hasła należy podać hasło jakie będzie używane (**Hasło**), wybrać grupę numerów, która ma służyć do obsługi wiadomościami SMS (**Grupa numerów telefonów**).

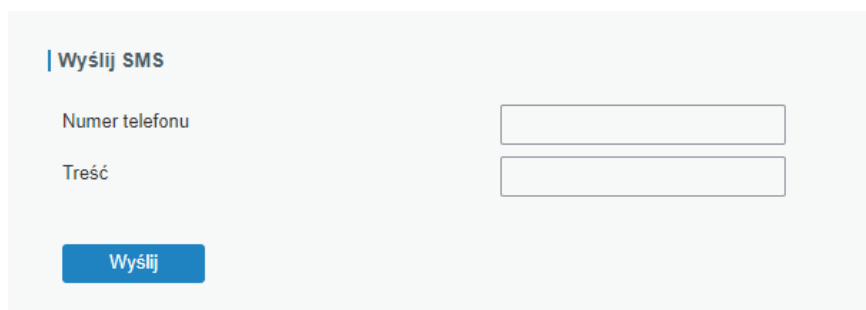


Telefony	SMS
Ustawienia podstawowe	
Tryb SMS	TEXT
Zarządzanie poprzez SMS	<input checked="" type="checkbox"/>
Typ uwierzytelniania	hasło+numer telefonu
Hasło	password
Grupa numerów telefonów	1
Zapisz	

Rysunek 4.93 Sekcja Ustawienia podstawowe w zakładce SMS

Wyślij SMS

W tej grupie możemy wysłać wiadomość SMS z routera, aby np. sprawdzić czy karta SIM działa prawidłowo. Aby wysłać wiadomość SMS należy podać numer odbiorcy SMS (**Numer telefonu**) oraz jej treść (**Treść**), następnie kliknąć przycisk **Wyślij**.



Wyślij SMS	
Numer telefonu	<input type="text"/>
Treść	<input type="text"/>
Wyślij	

Rysunek 4.94 Grupa Wyślij SMS w zakładce SMS

Skrzynka odbiorcza/nadawcza

W tych grupach możemy przejrzeć skrzynkę odbiorczą oraz skrzynkę nadawczą. W obu przypadkach możemy filtrować wiadomość podając datę początku zakresu, datę końca zakresu oraz numer nadawcy lub odbiorcy. Jeśli chcemy wyczyścić konkretną skrzynkę należy kliknąć przycisk **Czyść wszystko**.

Rysunek 4.95 Skrzynka nadawcza i odbiorcza w zakładce SMS

Skrzynka	Pole	Opis
Odbiorcza	Nadawca	Numer telefonu nadawcy wiadomości
	Czas	Data i czas dostarczenia wiadomości
	Treść	Treść wiadomości
Nadawcza	Odbiorca	Numer telefonu adresata wiadomości
	Czas	Data i czas wysłania wiadomości
	Treść	Treść wiadomości
	Status	Status wiadomości

4.3.3 Użytkownicy

4.3.3.1 Konto główne

W tej zakładce możemy konfigurować dane dostępowe do konta, na którym jesteśmy aktualnie zalogowani. W przypadku konta administratora możemy tutaj zmienić nazwę użytkownika oraz hasło. Aby zmienić hasło do konta należy podać **stare hasło**, **nowe hasło** oraz **powtórzyć nowe hasło**, a następnie kliknąć przycisk **Zapisz**.

Rysunek 4.96 Zmiana ustawień konta głównego

4.3.3.2 Zarządzanie kontami

W tej zakładce możemy dodać kolejnych użytkowników do obsługi routera (maksymalnie 5), aby to zrobić należy:

1. Kliknąć na **+** w kolumnie **Operacja**
2. Podać: nazwę nowego użytkownika, hasło nowego użytkownika oraz wybrać zakres uprawnień: tylko do odczytu ustawień routera lub do odczytu i zmiany ustawień routera

Nazwa użytkownika	Hasło	Uprawnienia	Operacja
test2	Tylko przeglądanie	+

Zapisz

Rysunek 4.97 Dodawanie nowego użytkownika

3. Kliknąć przycisk **Zapisz**

4.3.4 SNMP

4.3.4.1 SNMP

W tej zakładce możemy włączyć usługę SNMP na routerze i przeprowadzić jej wstępną konfigurację, aby to zrobić należy:

1. Włączyć usługę (**Włącz**)
2. Ustawić port na jakim usługa ma działać (**Port**)
3. Wybrać wersję protokołu SNMP, którego chcemy używać (**Wersja SNMP**)
4. Podać nazwę lokalizacji w jakiej znajduje się urządzenie oraz dane kontaktowe do osoby odpowiedzialnej za urządzenie

SNMP Widoki MIB VACM Trap MIB

Konfiguracja SNMP

Włącz

Port

Wersja SNMP

Lokalizacja

Dane kontaktowe

Zapisz

Rysunek 4.98 Konfiguracja wstępna usługi SNMP

4.3.4.2 Widoki MIB

W tej zakładce możemy dodawać widoki, dzięki którym możemy ograniczać dostęp do poszczególnych gałęzi drzewa MIB, aby dodać kolejny widok należy:

1. Kliknąć na **+** w kolumnie **Operacja**
2. Podać nazwę widoku
3. Filtrację widoku, jeśli wybierzemy wartość „zawiera się w” będziemy mieli dostęp do całego drzewa MIB zawartego w podanym numerze OID, a jeśli wybierzemy wartość „poza” będziemy mieli dostęp do wszystkich gałęzi drzewa poza tymi należącymi do podanego numeru OID
4. Numer OID dla widoku

Nazwa widoku	Filtr	OID	Operacja
All	zawiera się w	1	X
system	zawiera się w	1.3.6.1.2.1.1	X
			+

Zapisz

Rysunek 4.99 Konfiguracja widoków SNMP

4.3.4.3 VACM

Zakładka ta służy do konfiguracji komunikacji SNMP dla routera. Może ona mieć dwie wersje w zależności od tego jakiej wersji protokołu SNMP użyjemy w zakładce **SNMP** ([sekcja 4.3.4.1](#))

Dla SNMPv1/SNMPv2

W wersjach SNMPv1/v2 możemy skonfigurować tutaj jakie **społeczności** będą miały dostęp do jakich widoków drzewa MIB ([sekcja 4.3.4.2](#)). Aby dodać społeczność należy:

1. Kliknąć **+** w kolumnie **Operacja**
2. Podać nazwę społeczności
3. Ustawić poziom dostępu dla społeczności, możemy ustawić uprawnienia z zakresu odczytu danych (*tylko odczyt*) lub odczytu i zmiany ustawień (*odczyt-zapis*)
4. Ustalić do jakiego widoku będzie miała dostęp społeczność
5. Ustawić adres IP (ze skróconym zapisem maski podsieci) urządzenia, które będzie miało dostęp do danej społeczności, jeśli wpisujemy 0.0.0.0/0 każde urządzenie będzie miało dostęp do społeczności
6. Po wpisaniu wszystkich danych należy kliknąć przycisk **Zapisz**

Społeczność	Uprawnienia	Widok MIB	Sieć	Operacja
private	Odczyt-zapis	All	0.0.0.0/0	X
public	Tylko odczyt	none	0.0.0.0/0	X
				+

Zapisz

Rysunek 4.100 Konfiguracja zakładki VACM dla SNMPv1 i SNMPv2

Dla SNMPv3

W wersji SNMPv3 możemy tutaj dodać użytkowników, a potem przypisać ich do konkretnych grup uprawnień. Aby dodać grupę uprawnień należy:

1. Kliknąć na **+** w **Grupy użytkowników SNMPv3**
2. Podać nazwę grupy
3. Wybrać sposób autoryzacji do urządzenia (**Poziom bezpieczeństwa**); będzie to miało wpływ na to jakie dane będzie trzeba wprowadzić przy tworzeniu użytkownika z zakresu autoryzacji i szyfrowania
4. Wybrać do jakiego widoku grupa ma dostęp tylko w zakresie odczytu ustawień (**Widok „tylko odczyt”**)
5. Wybrać do jakiego widoku grupa ma dostęp w zakresie odczytu i edycji ustawień (**Widok „odczyt-zapis”**)
6. Wybrać do jakiego widoku grupa ma dostęp w zakresie komunikatów Inform (**Widok „inform”**)
7. Kliknąć przycisk **Zapisz**

Aby dodać użytkownika należy:

1. Kliknąć na **+** w **Lista użytkowników SNMPv3**
2. Podać nazwę użytkownika
3. Wybrać do jakiej grupy ma należeć użytkownik
4. Wybrać sposób szyfrowania hasła, opcja ta jest dostępna jeśli grupa, do której należy użytkownik w polu **Poziom bezpieczeństwa** będzie miała wybrane opcje „Auth/NoPriv” lub „Auth/Priv”
5. Podać hasło dla użytkownika (jeśli wymagane)
6. Wybrać sposób szyfrowania pakietów, opcja ta jest dostępna jeśli grupa, od której należy użytkownik w polu **Poziom bezpieczeństwa** będzie miała wybraną opcję „Auth/Priv”
7. Podać hasło szyfrowania pakietu (jeśli wymagane)
8. Kliknąć przycisk **Zapis**

Rysunek 4.101 Konfiguracja zakładki VACM dla SNMPv3

4.3.4.4 Trap

W tej zakładce możemy przeprowadzić konfigurację funkcji Trap dla SNMP, czyli wysyłania zgłoszeń o zmianach w konfiguracji do urządzenia będącego serwerem SNMP. Aby przeprowadzić konfigurację tej usługi należy:

1. Włączyć usługę (**Włącz**)
2. Wybrać wersję SNMP, dla której ma działać usługa
3. Podać adres serwera
4. Podać port na jakim działa usługa w serwerze
5. W przypadku wyboru wersji SNMPv3 należy dodatkowo wybrać użytkownika, za pomocą którego będziemy obsługiwali usługę oraz sposób jego autoryzacji

Rysunek 4.102 Konfiguracja zakładki SNMP Trap

4.3.4.5 MIB

W tej zakładce możemy pobrać plik MIB. Aby to zrobić należy wybrać plik, który chcemy pobrać, a następnie kliknąć przycisk **Pobierz**.

Rysunek 4.103 Zakładka MIB

4.3.5 AAA

W tej zakładce możemy przeprowadzić konfigurację modelu AAA (Authentication Authorization Accounting). Model AAA służy do kontroli użytkowników, którzy próbują zalogować się do urządzenia i w przypadku poprawnej identyfikacji sprawdza do jakich usług użytkownik posiada dostęp, a następnie raportuje ich pracę na urządzeniu. Model ten może opierać się na lokalnej bazie danych o użytkownikach lub na bazie opartej o serwery uwierzytelniające.

Model działa w trzech modułach:

1. Uwierzytelnianie – sprawdza czy użytkownik jest uprawniony do dostępu do urządzenia
2. Autoryzacja – sprawdza do jakich usług ma dostęp użytkownik
3. Raportowanie – raportuje operacje wykonywane przez użytkownika

4.3.5.1 Radius

W tej zakładce możemy skonfigurować dostęp do serwera uwierzytelniającego Radius.

Aby skonfigurować połączenie należy:

1. Włączyć usługę
2. Podać adres IP serwera
3. Podać port na jakim nasłuchuje serwer
4. Podać klucz szyfrowania komunikacji
5. Kliknąć przycisk **Zapisz**

Rysunek 4.104 Konfiguracja modelu AAA serwer Radius

4.3.5.2 Tacacs+

W tej zakładce możemy przeprowadzić konfigurację dostępu do serwera uwierzytelniającego Tacacs+. Aby skonfigurować połączenie należy:

1. Włączyć usługę
2. Podać adres IP serwera
3. Podać port na jakim nasłuchuje serwer
4. Podać klucz szyfrowania komunikacji
5. Kliknąć przycisk **Zapisz**

Radius	Tacacs+	LDAP	Autoryzacja
Konfiguracja Tacacs+			
Włącz	<input checked="" type="checkbox"/>		
Adres serwera	<input type="text" value="192.168.1.100"/>		
Port serwera	<input type="text" value="49"/>		
Hasło	<input type="text" value="...."/>		
<input type="button" value="Zapisz"/>			

Rysunek 4.105 Konfiguracja modelu AAA serwer TACACS+

4.3.5.3 LDAP

W tej zakładce możemy przeprowadzić konfigurację dostępu do serwera uwierzytelniającego LDAP. Aby skonfigurować połączenie należy:

1. Włączyć usługę
2. Podać adres IP serwera
3. Podać port na jakim nasłuchuje serwer
4. Podać **Base DN** (powinniśmy uzyskać od administratora serwera)
5. Wybrać sposób na szyfrowanie komunikacji z serwerem
6. Podać nazwę użytkownika do serwera
7. Podać hasło do serwera
8. Kliknąć przycisk **Zapisz**

Radius	Tacacs+	LDAP	Autoryzacja
Konfiguracja LDAP			
Włącz	<input checked="" type="checkbox"/>		
Adres serwera	<input type="text"/>		
Port serwera	<input type="text" value="389"/>		
Base DN	<input type="text"/>		
Szyfrowanie	<input type="text" value="Brak"/>		
Nazwa użytkownika	<input type="text"/>		
Hasło	<input type="text"/>		
<input type="button" value="Zapisz"/>			

Rysunek 4.106 Konfiguracja modelu AAA serwer LDAP

4.3.5.4 Autoryzacja

W tej zakładce możemy ustawić do jakich usług będą mieli dostęp użytkownicy uwierzytelniani przez konkretne serwery (bazy danych). Możemy wybrać tutaj brak bazy danych, bazę danych lokalną lub skorzystać z zewnętrznych baz danych przechowujących informacje o użytkownikach (RADIUS, TACACS+ lub LDAP). Jeśli do jakiejś usługi przypiszemy trzy rodzaje uwierzytelniania priorytet wykorzystania bazy będzie wyglądał następująco 1>2>3.

Usługa	1	2	3
Console	Brak	Brak	Brak
Web	Brak	Brak	Brak
Telnet	Brak	Brak	Brak
SSH	Brak	Brak	Brak

Zapisz

Rysunek 4.107 Konfiguracja modelu AAA zakładka Autoryzacja

4.3.6 Zarządzanie zdalne

4.3.6.1 Device Management

W tej zakładce możemy skonfigurować połączenie do scentralizowanego systemu zarządzania urządzeniami o nazwie DeviceHub. Aby poprawnie skonfigurować połączenie należy zapoznać się z dokumentacją producenta oprogramowania. Jako pierwsza pozycja w zakładce wyświetla nam się status połączenia do serwera DeviceHub (**Status**).

Aby skonfigurować połączenie routera z systemem należy:

1. Podać adres IP serwera z oprogramowaniem DeviceHub
2. Wybrać metodę uwierzytelniania
3. Jeśli wyżej wybierzemy opcję „kod uwierzytelniający” należy podać kod uwierzytelniania
4. Jeśli wyżej wybierzemy opcję „konto” należy podać nazwę użytkownika oraz hasło
5. Kliknąć przycisk **Zapisz**

Device Management Cloud VPN

Device Management

Status Rozłączony

Adres serwera

Metoda uwierzytelniania Kod uwierzytelniający

Kod uwierzytelniający

Połącz

Rysunek 4.108 Zakładka Zarządzanie zdalne, konfiguracja połączenia do DeviceHub

4.3.6.2 Cloud VPN

W tej zakładce możemy skonfigurować połączenie do serwera CloudVPN. Aby poprawnie skonfigurować połączenie należy zapoznać się z dokumentacją producenta oprogramowania.

Aby skonfigurować połączenie po stronie routera należy:

1. Podać adres IP serwera CloudVPN
2. Port na jakim nasłuchuje serwer
3. Kod autoryzujący połączenie
4. Nazwę urządzenia w systemie
5. Kliknąć przycisk **Połącz**

Konfiguracja CloudVPN	
Serwer	<input type="text"/>
Port	<input type="text" value="18443"/>
Kod autoryzacyjny	<input type="text"/>
Nazwa urządzenia	<input type="text"/>
Połącz	
Status CloudVPN	
Status	Rozłączone
Lokalne IP	--
Zdalne IP	--
Czas połączenia	-

Rysunek 4.109 Konfiguracja połączenia CloudVPN

W grupie **Status usługi** możemy odczytać status połączenia do serwera, wirtualne IP, wirtualne IP serwera CloudVPN, czas jaki router jest podłączony do usługi.

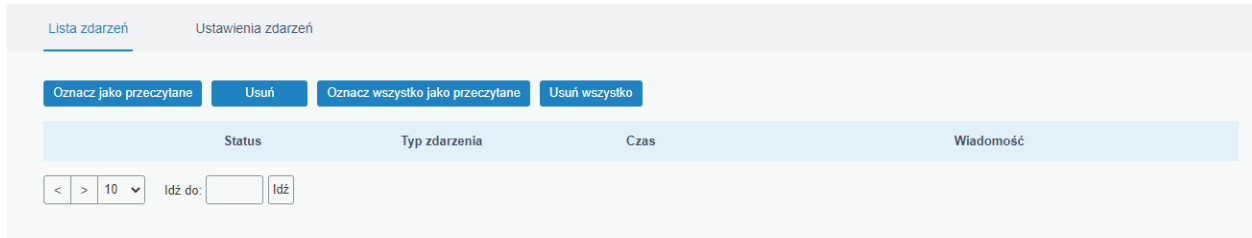
Status CloudVPN	
Status	Rozłączone
Lokalne IP	--
Zdalne IP	--
Czas połączenia	-

Rysunek 4.110 Status połączenia CloudVPN

4.3.7 Zdarzenia

4.3.7.1 Lista zdarzeń

W tej zakładce możemy odczytać wszystkie alarmy, których rejestrację zlecimy w zakładce **Ustawienia zdarzeń** ([sekcja 4.3.7.2](#)). Korzystając z odpowiednich przycisków możemy: oznaczyć zaznaczone zdarzenie jako odczytane, usunąć zaznaczone zdarzenie, oznaczyć wszystkie zdarzenia jako odczytane, usunąć wszystkie zdarzenia.



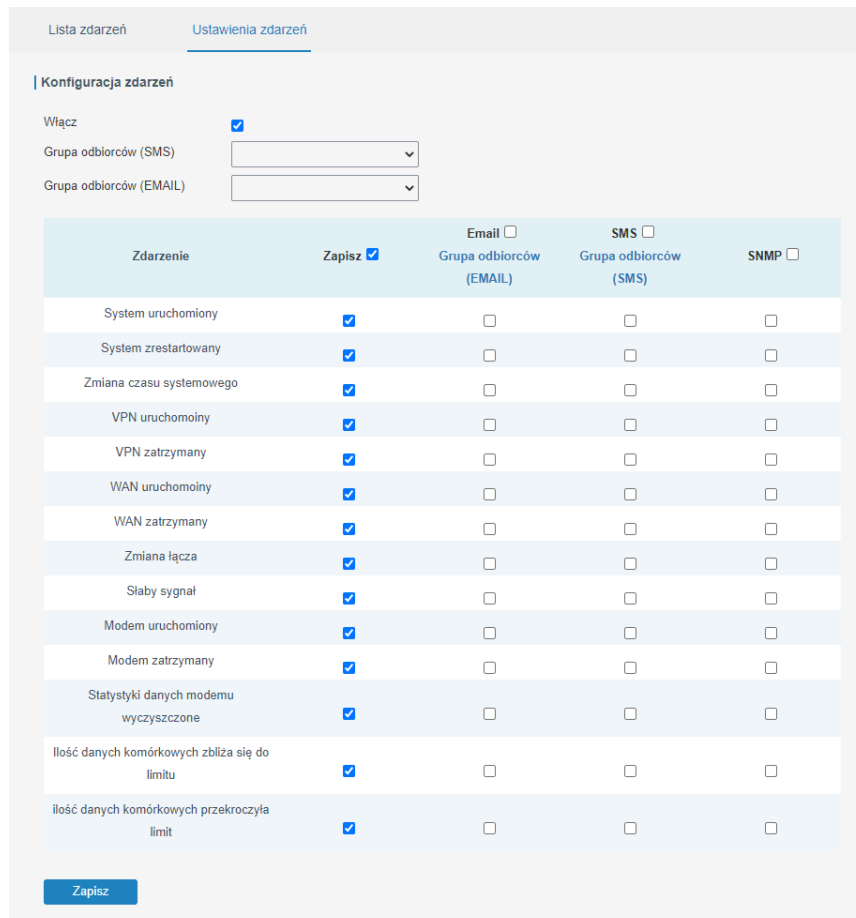
Rysunek 4.111 Zakładka Lista zdarzeń

4.3.7.2 Ustawienia zdarzeń

W tej zakładce możemy ustawić jakie zdarzenia z działania urządzenia będą zapisywane i w jaki sposób będą raportowane. Domyślnie usługa wszystkie zdarzenia raportuje lokalnie, ale po odpowiedniej konfiguracji możemy otrzymywać powiadomienia email, wiadomości SMS lub zdarzenia Trap SNMP.

Aby działało wysyłanie zdarzeń należy:

1. Wybrać w tabeli zdarzeń jaki rodzaj zdarzeń ma być raportowany w dany sposób
2. Wybrać do jakiej grupy numerów telefonów ma być wysyłana wiadomość SMS (konfiguracja grup telefonów w [sekcji 4.3.2.1](#))
3. Wybrać do jakiej grupy adresów email mają być wysyłane wiadomości email (konfiguracja grup adresów email w [sekcji 4.3.1.3](#))
4. Jeśli chcemy raportować zdarzenia Trap SNMP należy skonfigurować protokół SNMP w [sekcji 4.3.4](#)
5. Kliknąć przycisk **Zapisz**



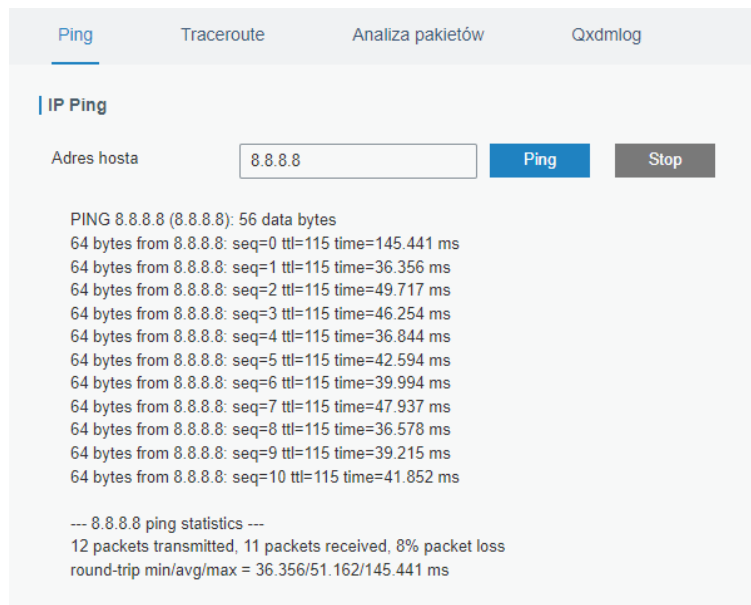
Rysunek 4.112 Konfiguracja zakładki Ustawienia zdarzeń

4.4 KONSERWACJA

4.4.1 Narzędzia

4.4.1.1 Ping

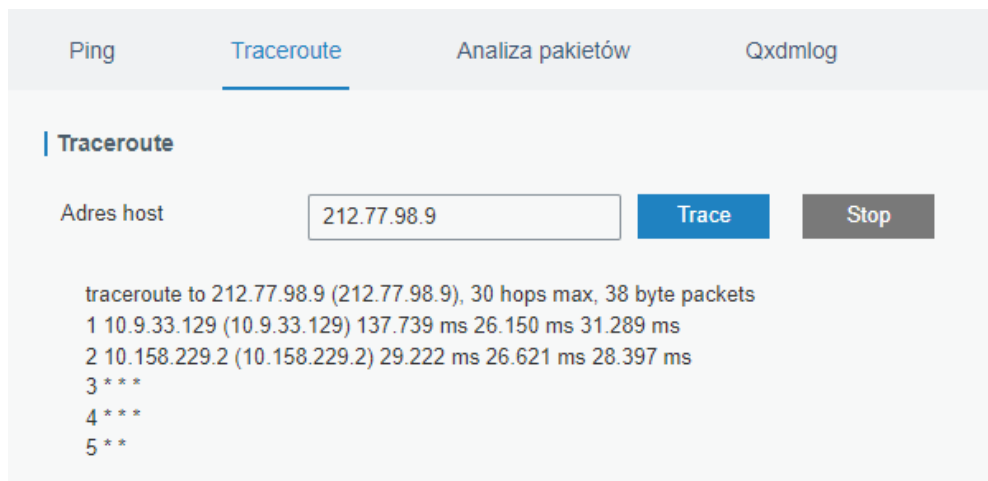
Zakładka Ping pozwala wywołać polecenie Ping, którym możemy sprawdzić np. czy urządzenie o danym IP ma komunikację z routerem. Aby wykonać taki test należy wpisać adres IP urządzenia, a następnie kliknąć przycisk **Ping**. Komenda będzie wykonywana do momentu wciśnięcia przycisku **Stop**.



Rysunek 4.113 Funkcja Ping

4.4.1.2 Traceroute

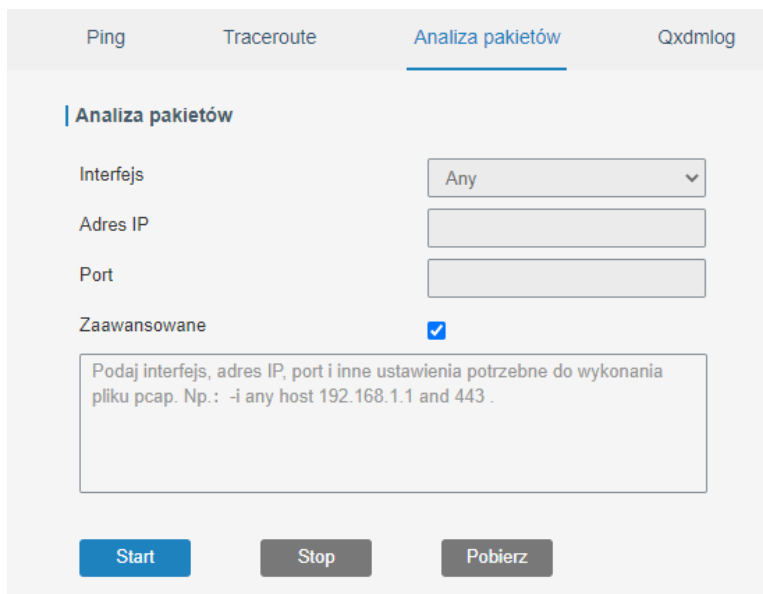
Funkcja ta pozwala nam wywołać polecenie Traceroute, które odpowiedzialne jest za wyświetlenie drogi jaką pakiety muszą pokonać z danego urządzenia, aby dotrzeć do urządzenia podanego w polu **Adres hosta**. Aby wykonać to polecenie należy podać adres IP następnie kliknąć na przycisk **Trace**, możemy przerwać wykonywanie funkcji w czasie pracy klikając przycisk **Stop**, jednakże funkcja po wyświetleniu całej trasy zatrzyma się automatycznie.



Rysunek 4.114 Funkcja Traceroute

4.4.1.3 Analiza pakietów

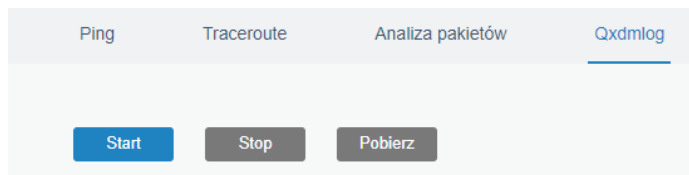
Za pomocą tej funkcji możemy przeprowadzić analizę ruchu pakietów na danym interfejsie routera. Aby przeprowadzić taką analizę należy wybrać interfejs, który chcemy sprawdzać, następnie opcjonalnie podać IP oraz port jakie chcemy sprawdzić i kliknąć przycisk **Start**. Cały ruch sieciowy będzie zapisywany w pliku typu *PCAP*, który możemy otworzyć za pomocą np. oprogramowania Wireshark. Jeśli chcemy zatrzymać zapisywanie ruchu sieciowego należy kliknąć przycisk **Stop**. Tak utworzony plik pobieramy za pomocą przycisku **Pobierz**. Za pomocą funkcji **Zaawansowane** możemy ręcznie wpisać regułę iptables, która będzie filtrowała interesujący nas ruch i zapisywała go do pliku.



Rysunek 4.115 Funkcja Analiza pakietów

4.4.1.4 Qxdmlog

W tej zakładce możemy utworzyć plik logów w standardzie QXDM, który potem możemy pobrać na dysk i przeanalizować odpowiednim oprogramowaniem. Aby utworzyć taki plik należy kliknąć przycisk **Start** odczekać interesujący nas okres czasu, a następnie kliknąć przycisk **Stop**, tak przygotowany plik pobieramy przyciskiem **Pobierz**.

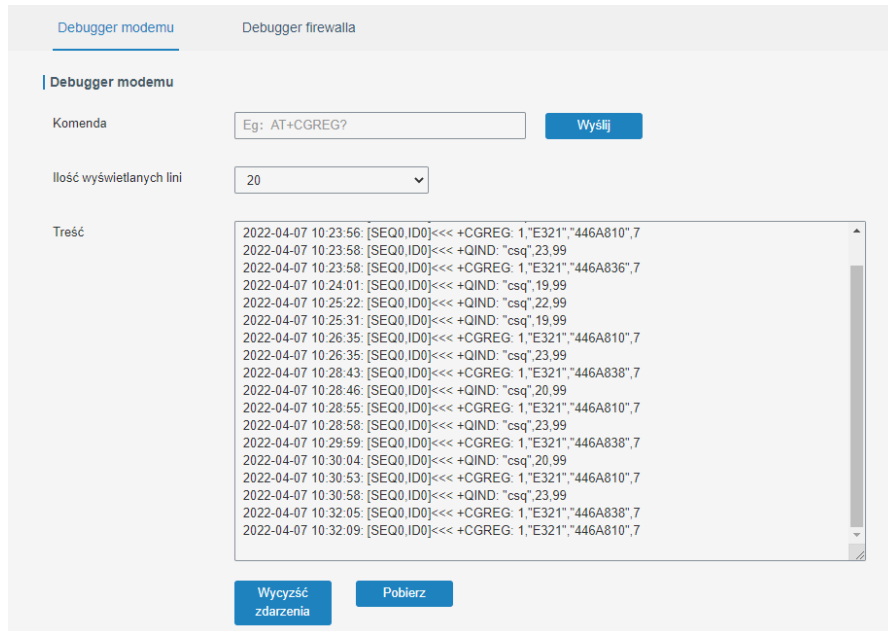


Rysunek 4.116 Funkcja QXDMlog

4.4.2 Debugger

4.4.2.1 Debugger modemu

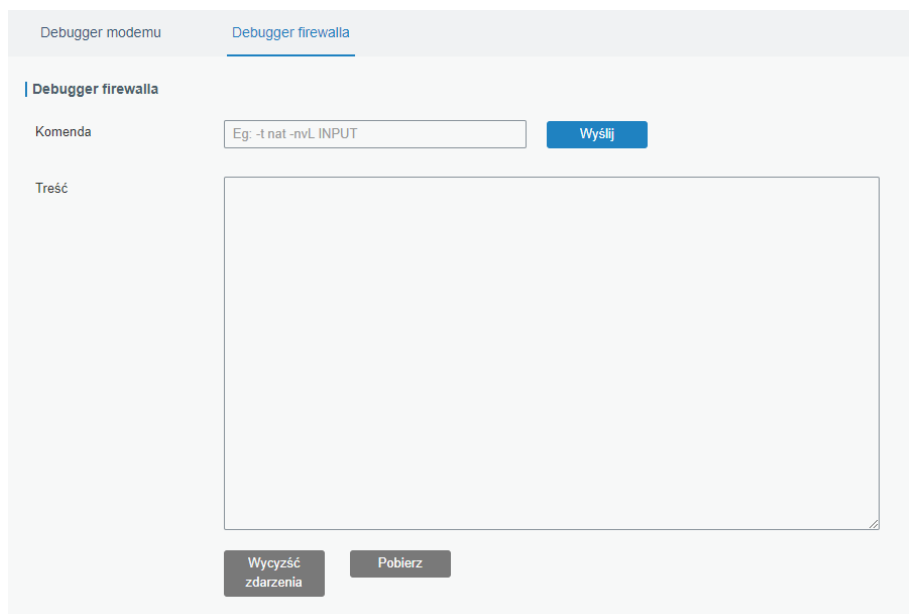
W tej zakładce możemy logi związane z modemem GSM, a także wysyłać do modemu komendy AT. Opcją **Ilość wyświetlanych linii** możemy ustawić ile linii będzie wyświetlane w oknie **Treść**. Dodatkowo może pobrać plik logów odpowiedzialny za modem GSM przyciskiem **Pobierz**, a także wyczyścić logi. W prawym dolnym rogu możemy ustawić domyślny czas odświeżania okna z logami.



Rysunek 4.117 Funkcja Debugger modemu

4.4.2.2 Debugger firewala

W tej zakładce możemy odczytać logi związane z pracą firewalla w routerze, a także wysłać komendy iptables do modułu firewala. Dodatkowo możemy ściągnąć plik z logami firewala za pomocą przycisku **Pobierz** i wyczyścić logi przyciskiem **Czyść**



Rysunek 4.118 Funkcja Firewall Debugger

4.4.3 Dziennik systemowy

4.4.3.1 Zdarzenia

W tej zakładce wyświetlane są wszystkie logi systemowe. Za pomocą **Ilość wyświetlanych linii** możemy ustawić ilość wierszy, które będą wyświetlane w oknie z logami. W prawym dolnym rogu możemy ustawić jak często ma być odświeżane okno z logami, natomiast przycisk **Czyść** służy do wyczyszczenia okna logów.

Zdarzenia Pobieranie Ustawienia

Zdarzenia

Ilość wyświetlanych linii

```
Thu Apr 7 09:31:19 2022 daemon.info zebra[1384]: icmp_detect_thread:1203 cellular0 icmp_detect result=2
Thu Apr 7 09:36:26 2022 daemon.info zebra[1384]: icmp_detect_thread:1203 cellular0 icmp_detect result=2
Thu Apr 7 09:41:32 2022 daemon.info zebra[1384]: icmp_detect_thread:1203 cellular0 icmp_detect result=2
Thu Apr 7 09:46:39 2022 daemon.info zebra[1384]: icmp_detect_thread:1203 cellular0 icmp_detect result=2
Thu Apr 7 09:50:11 2022 daemon.info zebra[1384]: cell_pppoe_set:1246 [cellular0] update lease!
Thu Apr 7 09:51:45 2022 daemon.info zebra[1384]: icmp_detect_thread:1203 cellular0 icmp_detect result=2
Thu Apr 7 09:56:52 2022 daemon.info zebra[1384]: icmp_detect_thread:1203 cellular0 icmp_detect result=2
Thu Apr 7 10:00:00 2022 cron.info crond[2728]: USER root pid 17102 cmd /etc/init.d/sysntpd restart
Thu Apr 7 10:01:00 2022 cron.info crond[2728]: USER root pid 17654 cmd hwclock -u -w
Thu Apr 7 10:01:58 2022 daemon.info zebra[1384]: icmp_detect_thread:1203 cellular0 icmp_detect result=2
Thu Apr 7 10:03:45 2022 authpriv.info dropbear[19142]: Child connection from 192.168.126.231:54779
Thu Apr 7 10:03:47 2022 authpriv.notice dropbear[19142]: Auth succeeded with blank password for 'root' from 192.168.126.231:54779
Thu Apr 7 10:07:04 2022 daemon.info zebra[1384]: icmp_detect_thread:1203 cellular0 icmp_detect result=2
Thu Apr 7 10:09:02 2022 authpriv.info dropbear[19142]: Exit (root): Idle timeout
Thu Apr 7 10:12:11 2022 daemon.info zebra[1384]: icmp_detect_thread:1203 cellular0 icmp_detect result=2
Thu Apr 7 10:17:17 2022 daemon.info zebra[1384]: icmp_detect_thread:1203 cellular0 icmp_detect result=2
Thu Apr 7 10:22:23 2022 daemon.info zebra[1384]: icmp_detect_thread:1203 cellular0 icmp_detect result=2
Thu Apr 7 10:27:29 2022 daemon.info zebra[1384]: icmp_detect_thread:1203 cellular0 icmp_detect result=2
Thu Apr 7 10:32:36 2022 daemon.info zebra[1384]: icmp_detect_thread:1203 cellular0 icmp_detect result=2
Thu Apr 7 10:37:42 2022 daemon.info zebra[1384]: icmp_detect_thread:1203 cellular0 icmp_detect result=2
```

Wyczyść zdarzenia

Rysunek 4.119 Funkcja Zdarzenia

4.4.3.2 Pobieranie

W tej zakładce możemy pobrać pliki logów

Zdarzenia Pobieranie Ustawienia

Pobieranie

Pobierz wszystko

Nazwa pliku	Rozmiar pliku (KB)	Czas utworzenia	Operacja
vpn.log	2	2022/02/23 12:51:10	↓
system.log	743	2022/04/07 10:42:49	↓
httpd.log	690	2022/04/07 10:42:20	↓
firewall.log	0	2022/03/30 11:01:51	↓
cellular.log	553	2022/04/07 10:42:48	↓

Rysunek 4.120 Funkcja Pobieranie

4.4.3.3 Log Settings

W tej zakładce możemy przeprowadzić konfigurację tego w jaki sposób zapisywane będą logi systemowe. Możemy zastosować zapisywanie na serwerze zewnętrznym konfigurując grupę **Serwer zdalny** podając adres IP takiego serwera oraz port na jakim nasłuchuje usługa do rejestrowania logów. Dodatkowo możemy określić maksymalną wielkość pliku przechowywaną w pamięci lokalnej urządzenia oraz rodzaje zdarzeń jakie będą rejestrowane w systemie.

Zdarzenia Pobieranie Ustawienia

Serwer zdalny

Włącz

Adres serwera

Port

Przechowywanie lokalne

Przeźródź dyskowa

Rozmiar KB

Szczegółowość

Zapisz

Rysunek 4.121 Funkcja ustawienia

4.4.4 Aktualizacja

W tej zakładce możemy odczytać wersję oprogramowania zainstalowaną obecnie na routerze oraz zaktualizować oprogramowanie. Jeśli podczas aktualizacji zaznaczymy opcję **Resetowanie ustawień do ustawień fabrycznych** to cała konfiguracja urządzenia zostanie przywrócona do ustawień fabrycznych.

Aktualizacja

Aktualizacja

Wersja oprogramowania

Resetowanie ustawień do ustawień fabrycznych

Plik

Przeglądaj Aktualizacja

Rysunek 4.122 Funkcja aktualizacja

4.4.5 Kopia zapasowa

W tej zakładce możemy wyeksportować lub zaimportować ustawienia dla routera oraz zresetować go do ustawień fabrycznych.

Kopia zapasowa

Import konfiguracji

Plik konfiguracyjny

Przeglądaj Import

Pobieranie konfiguracji startowej

Pobierz

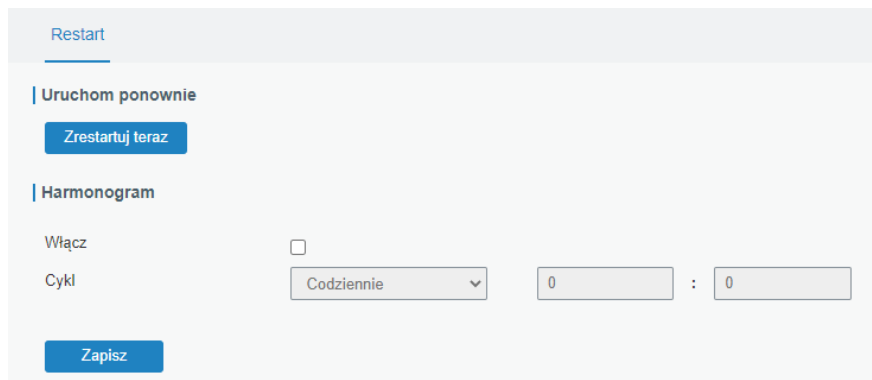
Przywracanie ustawień fabrycznych

Reset

Rysunek 4.123 Funkcja kopia zapasowa

4.4.6 Restart

W tej zakładce możemy zrestartować urządzenie. Możemy zrobić to natychmiast lub ustawić prosty harmonogram restartów w trzech zakres: codziennie, co tydzień, co miesiąc.



Rysunek 4.124 Funkcja restart



UPOZORNENIE!

Przed restartem urządzenia upewnij się, że wszystkie ustawienia zostały zapisane poprzez przycisk Zapisz oraz Zatwierdź znajdujący się w prawym górnym rogu.

5. SPECYFIKACJA TECHNICZNA

5.1 TABELA

	BCS-R4G-1W1L
Porty	2x 10/100Mbps; 1x WAN + 1x LAN lub 2x LAN; Full/Half duplex
Moduł GSM	1x slot na karte SIM 1x SMA
PoE (BCS-R4G-1W1L-P)	Porty PoE 2 Standard PoE 802.3 af/at
Sprzęt	CPU: ARM Cortex-A7 RAM: 128MB DDR3 Flash: 128MB
Wskaźniki	1x Zasilanie 1x System 1x SIM 3x Siła sygnału
Pobór mocy	standardowo 1,8W; maksymalnie 2.2W (bez PoE)
Zasilanie	9-48V DC; 2-pinowe złącze PTB 5.08 mm
Obudowa	metalowa
Wymiary	108 x 90 x 26 mm
Montaż	Desktop, ściana, szyna DIN TH35
Dodatkowa ochrona	IP30 Ochrona przeciwprzepięciowa Ochrona przed odwróconą polaryzacją na zasilaniu
Środowisko	Pracy: -40°C - 60°C Przechowywania: -40°C - 85°C Wilgotność: 0%-95% nieskondensowanej przy 25°C

5.2 OPROGRAMOWANIE

	BCS-R4G-1W1L
Protokoły sieciowe	IPv4/IPv6, PPP, PPPoE, SNMP v1/v2c/v3, TCP, UDP, DHCP, RIPv1/v2, OSPF, DDNS, VRRP, HTTP, HTTPS, DNS, ARP, QOS, Sntp, Telnet, VLAN, SSH, atd.
VPN	DMVPN, IPsec, OpenVPN, PPTP, L2TP, GRE
DDNS	DynDNS, FreeDNS, 3322, DuckDNS, Oray, No-IP, ChangelP, EasyDNS, Google, OVH, DnsExit, Sitesolutions, Dynsip, Zoneedit, LoopiaDNS, DHIS, własne
Zabezpieczenia	Access Control, DMZ, Port Mapping, MAC Binding, SPI Firewalls, DoS&DDoS Protection, Filtering (IP&Domain), IP Passthrough
Zarządzanie	Web, CLI, SMS, On-demand dial up, SNMP v1/v2/v3, DeviceHub
AAA	Radius, Tacacs+, LDAP, LocalAuthentication
Rodzaje użytkowników	Dwa rodzaje poziomów dostępu
Redundancja	VRRP, WAN Failover

5.3 NAJWAŻNIEJSZE FUNKCJONALNOŚCI

- Współpraca z wieloma operatorami sieci GSM
- Automatyczne przełączanie między siecią kablową, a GSM
- CPU w klasie NXP
- Wytrzymała obudowa IP30
- Trzy możliwości montażu (desktop, ściana, szyna DIN)
- Praca w szerokim zakresie temperatur (-40°C do 60°C) oraz wilgotności 0-95% nieskondensowanej
- Wbudowane protokoły VPN takie jak IPsec, OpenVPN, GRE, L2TP, PPTP, DMVPN
- Sprzętowy Watchdog przywracający pełną funkcjonalność po awariach
- Obsługa ACL, DMZ, ochrony DDoS, filtry ruchu sieciowego, SPI firewall
- Obsługa AAA (Radius, TACACS+, LDAP, uwierzytelnianie lokalne)
- Łatwa konfiguracja i konserwacja dzięki DeviceHub, WEB GUI, CLI oraz SNMP



Žiadna reprodukcia tohto návodu, celého ani jeho častí
(okrem krátkych citácií v článkoch alebo recenziách),
nie je možné uskutočniť bez písomného súhlasu NSS Sp. z o.o.



NSS Sp. z o.o.
ul. Modularna 11 (hala IV)
02-238 Warszawa

Copyright © NSS Sp. z o.o.



Aktualizacja: 21.04.2022