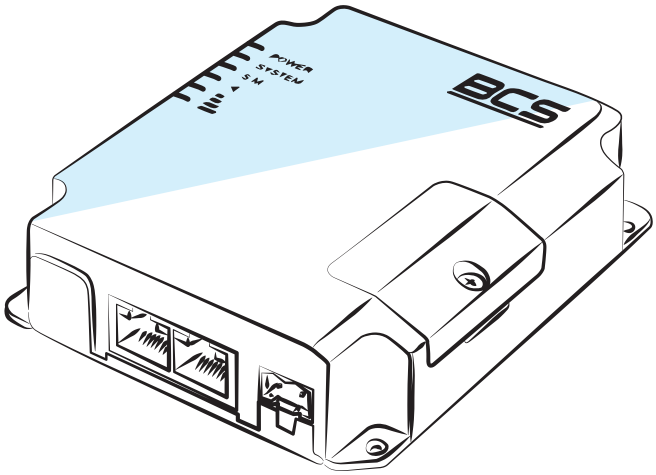
SK

BCS-R4G-1W1L(-P)

Priemyselný smerovač LTE s PoE

Používateľská príručka



www.bcs.pl

NSS Sp. z o.o. ul. Modularna 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

Aktualizácia: 20.04.2022

OBSAH

1. PREDSTAVENIE PRODUKTU

1.1 PROFIL PRODUKTU

BCS-R4G-1W1L je priemyselný LTE router s rozsiahlymi softvérovými funkciami, vďaka ktorým ho možno použiť v mnohých M2M / IoT inštaláciách. Podpora štandardov WCDMA a 4G LTE zaisťuje vysokú stabilitu spojenia s operátormi. Použitie dvoch Fast Ethernet portov, z ktorých jeden je možné nastaviť ako WAN port, umožňuje zvýšiť stabilitu internetového pripojenia konfiguráciou služby „Link Failover“, ktorá v prípade problémov s prístupom na internet od jedného poskytovateľa prepne smerovač k inému poskytovateľovi. Použitie komponentov priemyselnej kvality zaisťuje vysokú stabilitu pri nízkej spotrebe energie. Použité riešenia robia router BCS-R4G-1W1L ideálnym, okrem iného, pre priemyselnú automatizáciu, video monitorovacie inštalácie, telemetrické zariadenia, platobné zariadenia, predajné zariadenia a mnohé ďalšie.

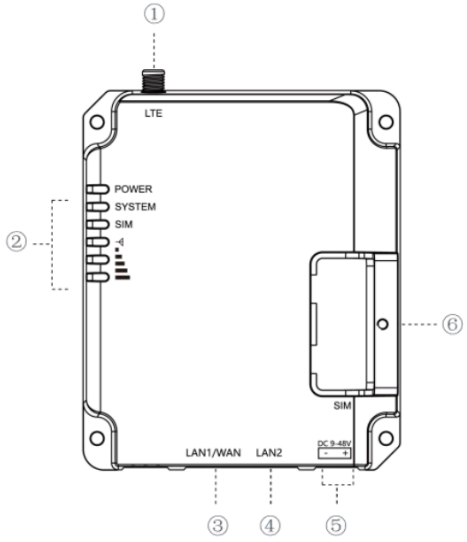
1.2 OBSAH KRABICE

Po otvorení krabice si prosím dôkladne skontrolujte jej obsah. Krabica obsahuje:

Obsah	Množstvo	Funkcia
Router	1	–
Napájanie 12V 1A	1	Napájanie routera
LTE anténa	1	Zvýšenie pokrytia siete
Montážny úchyt	1	Montáž na lištu TH35
Používateľská príručka	1	Táto príručka

1.3 PREZENTÁCIA ZARIADENIA

Opis jednotlivých častí:



1. Anténna zásuvka
2. LED indikátory
3. Port RJ45 LAN1 / WAN
4. Port RJ45 LAN2
5. Napájacia zásuvka
6. Kryt slotu pre SIM kartu a tlačidlo RESET

Anténna zásuvka
Zásuvka na pripojenie antény zlepšujúca dosah mobilnej siete, ktorá je súčasťou súpravy.

LED indikátory

Indikátor	Názov	Farba	Pracovné podmienky	Popis
POWER	LED indikátor napájania	Zelená	Svieti	Napájanie je normálne
			Nesvieti	Žiadne napájanie, napájanie smerovača je abnormálne
SYSTEM	Systémový indikátor	Zelená	Nesvieti	Ak svieti indikátor POWER, router je v režime zavádzania
			Bliká	Systém funguje dobre
		Červená	Svieti	Systém nefunguje správne
SIM	Indikátor nainštalovanej SIM karty	Zelená	Svieti	SIM karta je správne pripojená k operátorovi
			Bliká	Pomaly: SIM karta je zaregistrovaná, čaká sa na príkaz hovoru (časť 4.2. 1.2) Rýchlo: SIM karta je v spojení s operátorom
			Nesvieti	Žiadna SIM karta, žiadne spojenie s operátorom
	Indikátor sily signálu mobilnej siete	Zelená	Svieti	Čím viac indikátorov svieti, tým lepšie je pokrytie siete GSM
			Nesvieti	Neexistuje žiadne pokrytie mobilnej siete

Port RJ45 LAN1/WAN
Fast Ethernet port (10/100 Mbps), LAN1 port môže fungovať aj ako WAN port, vďaka čomu vieme zabezpečiť redundanciu internetového pripojenia *(sekcja 4.2.1.3).*

Port RJ45 LAN2
Port Fast Ethernet (10/100 Mbps).

Napájacia zásuvka
Štandardná PCB zásuvka pre pripojenie napájacieho zdroja. DC 9-48V.

Kryt slotu pre SIM kartu a tlačidlo RESET
Po odskrutkovaní krytu uvidíte slot pre inštaláciu SIM karty štandardnej veľkosti a resetovacie tlačidlo, ktoré obnoví továrenské nastavenia routera.

2. INŠTALÁCIA

2.1 PRÍPRAVA ZARIADENIA NA INŠTALÁCIU

UPOZORNENIE!
Vyhnite sa nesprávnemu použitiu zariadenia. Hrozí poškodenie zariadenia a zranenie osôb. Pozorne si prečítajte nasledujúce pokyny týkajúce sa prostredia, kde bude zariadenie inštalované.

Položky, ktoré si vyžadujú pozornosť počas inštalácie:
- Uistite sa, že zariadenie nie je pripojené k zdroju napájania, použite antistatický náramok a uistite sa, že dobre priľne k pokožke zápästia;
- Router funguje správne, keď je napájaný správnym napätím. Uistite sa, že napájacie napätie zodpovedá označeniu na zariadení;
- Pred pripojením napájania k routeru sa uistite, že nespôsobí skrat v elektrickom systéme, pretože môže poškodiť router;
- Zabráňte úrazu elektrickým prúdom, neotvárajte kryt routera, aj keď nie je pripojený k napájaciemu zdroju;
- Pred čistením zariadenie odpojte od zdroja napájania, nepoužívajte mokrú handričku ani tekuté čistiace prostriedky

Teplota a vlhkosť:
Pre zabezpečenie dlhodobej a stabilnej prevádzky routera je potrebné dodržiavať podmienky v prevádzkovom prostredí zariadenia. Príliš nízka alebo vysoká vlhkosť môže viesť k úniku elektriny cez izolátory, k hrdzaveniu komponentov a dokonca k urýchleniu procesu starnutia zariadenia. Práca pri vysokej teplote vedie k rýchlejšiemu opotrebovaniu elektronických obvodov. Rozsah teploty a vlhkosti je definovaný v tabuľke nižšie:

Popis prostredia	Teplota	Relatívna vlhkosť
Použite	-40°C-60°C	0% – 95% nekondenzujúce
Skladovanie	-40°C-85°C	0% – 95% nekondenzujúce

Nadmorská výška nad morom

Ak je táto ikona zobrazená na produkte, znamená to, že zariadenie je možné používať v nadmorskej výške maximálne 2000 m nad morom.

Peľ, prach
Padajúci prach a peľ na povrch routera môžu spôsobiť pohlcovanie statickej elektriny, čo sťažuje dotyk kovových častí spojovacích bodov. Výrobok je antistatický, ale pri prekročení maximálnej úrovne hrozí poškodenie komponentov DPS. Aby sa predišlo vplyvu statickej elektriny na zariadenie, je potrebné: pravidelne čistiť zariadenie od prachu; udržiavať primeranú čistotu vzduchu v miestnosti; zabezpečte dobré uzemnenie zariadenia, aby ste zabezpečili hladký prenos statickej elektriny.

Elektromagnetické rušenie
Silné elektromagnetické pole môže ovplyvniť vnútorné systémy routera. Aby ste znížili riziko poškodenia zariadenia, uistite sa, že: napájací systém je správne chránený; router by mal byť umiestnený mimo dosahu vysokofrekvenčného napájania, ako sú zariadenia s vysokým prúdom, indukčné systémy napájania. V prípade potreby zmerajte elektromagnetické tienenie.

Uzemnenie
V okamihu úderu blesku sa objaví veľmi veľký prúd a vzduch na výbojovej ceste sa okamžite zahreje na 20 000°C, tieto faktory určite poškodia zariadenie. Riziko môžete znížiť uplatnením niekoľkých pravidiel: uistite sa, že skrinka, v ktorej je zariadenie umiestnené, má dobrý kontakt so zemou; uistite sa, že zásuvka má prepäťovú ochranu; používajte kvalitnú kabeláž; v prípade vonkajších rozvodov sa odporúča použiť systém ochrany pred bleskom vedený do zeme.

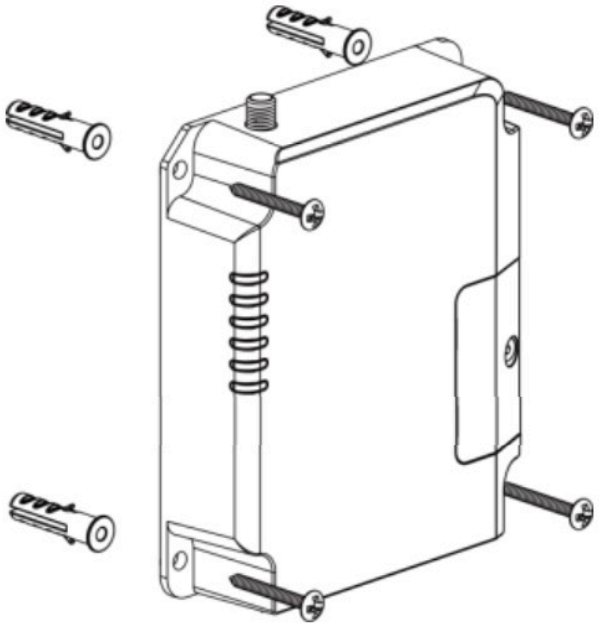
Požiadavky na montáž
Router sa inštaluje na lištu TH35 alebo rovnú plochu, ku ktorej sa dá priskrutkovať pomocou skrutiek. Uistite sa, že na mieste inštalácie je dostatok miesta a že koľajnica alebo doska, na ktorú je zariadenie namontované, unesie hmotnosť najmenej 1 kg; uistite sa, že miesto inštalácie má chladiaci / vykurovací systém, ktorý udrží jednotku v prevádzke v optimálnych podmienkach.

Užitočné nástroje
Pri inštalácii routera možno budete potrebovať nástroje ako: skrutkovače; antistatický remienok na zápästie; sieťový kábel. Uistite sa, že k týmto nástrojom máte prístup.

2.2 INŠTALÁCIA PRODUKTU

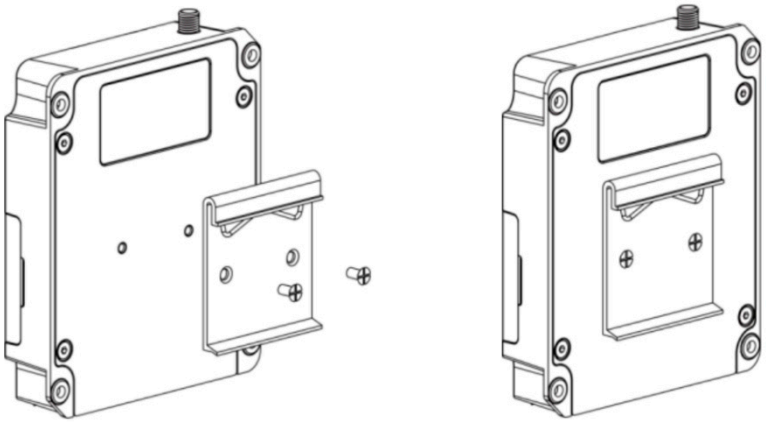
Zariadenie je možné umiestniť na stôl, namontovať na stenu alebo na DIN lištu.

Inštalácia na stenu
Ak ho chcete nainštalovať na stenu, vyvŕtajte montážne otvory a potom použite otvory pripravené v kryte na montáž na stenu.



Inštalácia na DIN lištu TH35
Router je navrhnutý na inštaláciu na štandardnú DIN lištu TH35 používanú v ovládacích a elektrických skriniach, možno ho jednoducho nainštalovať podľa nasledujúcich krokov:

1. Namontujte držiak koľajnice TH35 na zariadenie pomocou skrutiek zo sady silou 1-1,2 Nm



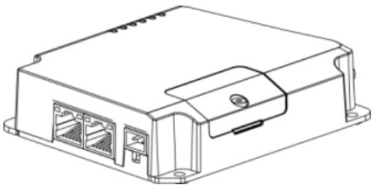
2. Namontujte router na DIN lištu TH35. Uistite sa, že je router vodorovný a stabilný

3. PRIPOJENIE ZARIADENIA

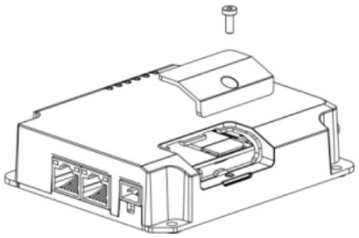
3.1 INŠTALÁCIA KARTY SIM

Router je prispôsobený na prácu so SIM kartami, ktoré nainštalujeme podľa nižšie uvedených krokov:

1. Odskrutkujte kryt chrániaci zásuvku a tlačidlo RESET



2. Vložte kartu do zásuvky SIM1 čipom smerom nadol, ako je znázornené na zásuvke, a priskrutkujte kryt



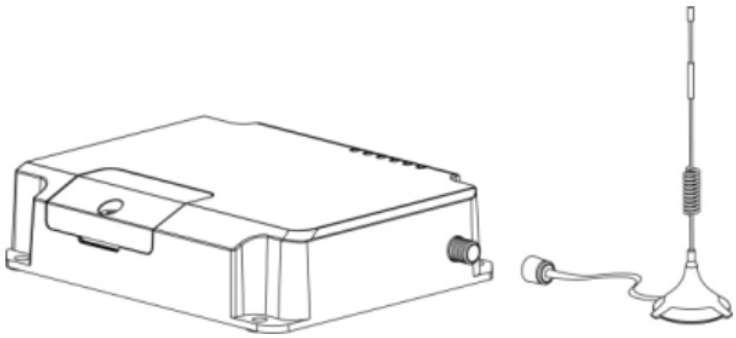
3.2 PORTY RJ45

Pomocou ethernetového kábla pripojte jeden koniec k portu na routeri a druhý koniec ku koncovému zariadeniu; port LAN1 / WAN je možné použiť ako port LAN aj ako port WAN (časť 4.2 .1.3), vďaka čomu možno poskytnúť redundanciu prístupu na internet zariadeniam za routerom, ktoré sú pripojené k portu LAN2.

UPOZORNENIE!
Ak sú k routeru pripojené zariadenia, ako je pracovná stanica, server, switch alebo iné sieťové zariadenie, dĺžka kábla nemôže presiahnuť 100 metrov.
Funkcia automatického preklopenia (Auto-MDI / MDIX) rozpozná, či je použitý ethernetový kábel CAT 5 štandardný alebo krížený. Port RJ45 nepoužívajte na pripojenie telefónneho kábla.

3.3 ANTÉNA

V súprave s routerom dostanete anténu s káblom zakončeným zástrčkou, ktorá pasuje do zásuvky na routeri. Ak chcete nainštalovať anténu, umiestnite ju na vhodné miesto a potom priskrutkujte kábel k zásuvke antény na routeri. Na zabezpečenie najlepšieho signálu by mala byť anténa namontovaná vertikálne.



UPOZORNENIE!
Anténa je pripevnená k povrchu pomocou magnetu. Uistite sa, že magnet neovplyvní zariadenie alebo povrch, ku ktorému bude anténa pripevnená.

3.4 PRED ZAPNUTÍM ROUTERA

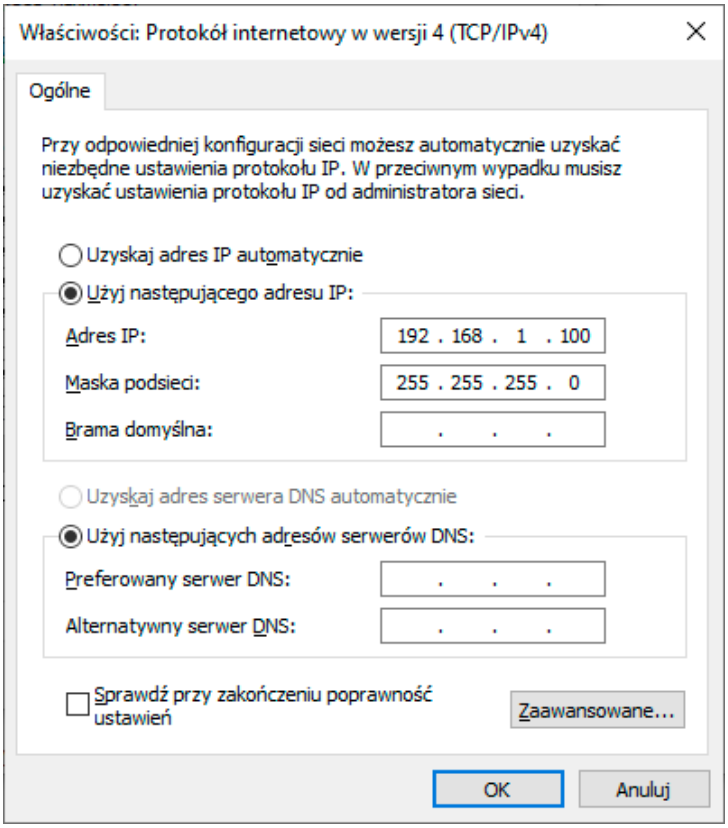
- Skontrolujte, či napájacie napätie zodpovedá špecifikácii zariadenia
- Skontrolujte, či sú napájací zdroj, router a miesto montáže správne uzemnené
- Skontrolujte, či je router správne pripojený k iným zariadeniam

3.5 UVEDENIE ZARIADENIA DO PREVÁDZKY

Po zapnutí sa router automaticky inicializuje. Inicializácia je prezentovaná nasledovne: po zapnutí napájania sa na cca 1 sekundu rozsvietia všetky LED kontrolky, potom sa rozsvieti už len kontrolka POWER, keď kontrolka SYSTEM začne blikať na zeleno, zariadenie je pripravené na použitie.

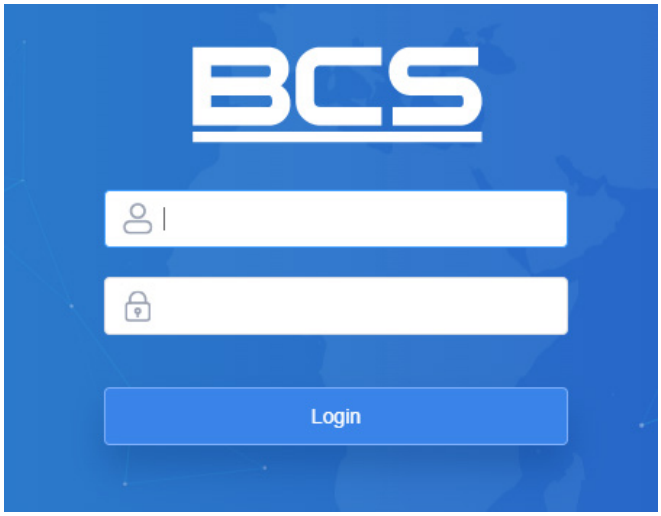
3.6 WEBOVÁ SLUŽBA ZARIADENIA

1. Pripojte počítač k routeru pomocou ethernetového kábla pomocou ľubovoľného portu RJ45
2. Ručne nastavte IP adresu počítača na ľubovoľnú v rozsahu 192.168.1.xxx, masku podsiete na 255.255.255.0



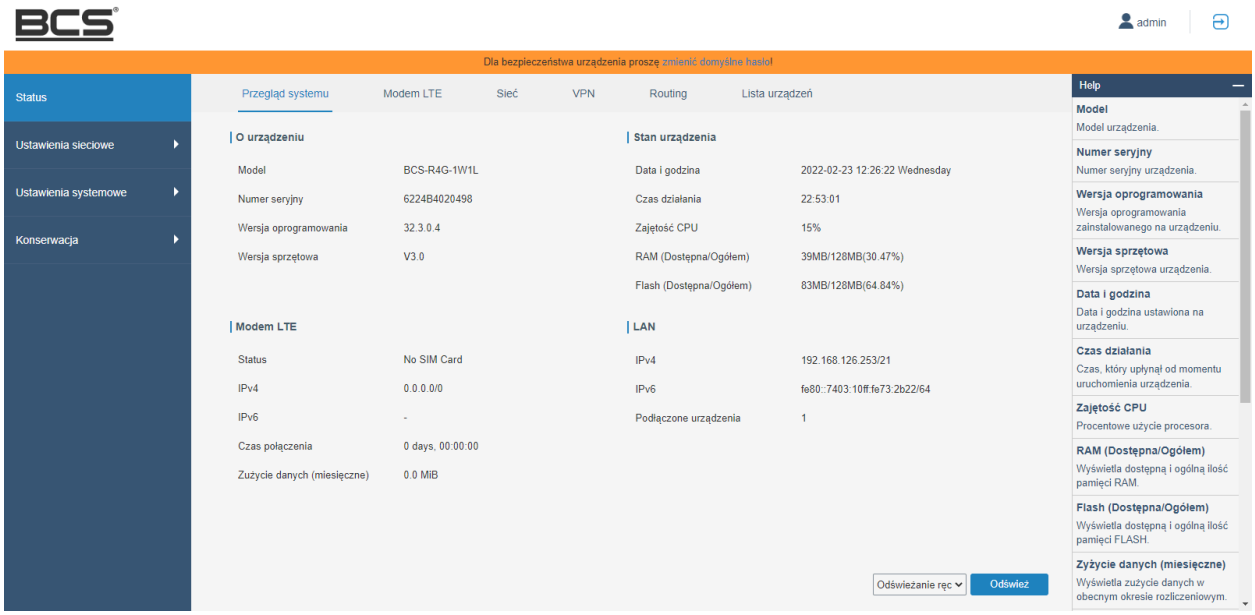
Obrázok 3.1 Nastavenia sieťového adaptéra

3. Otvorte webový prehliadač a do poľa adresy zadajte 192.168.1.1 a potvrďte klávesom Enter
4. Zadajte používateľa (predvolene admin) a heslo (predvolene password) a kliknite na tlačidlo Login



Obrázok 3.2 Okno logowania

5. Správne vykonaný postup bude mať za následok zobrazenie podobnej obrazovky; teraz môžete začať spravovať konfiguráciu routera



Obrázok 3.3 Hlavná stránka webu

UPOZORNENIE!
Pri prvom prihlásení by ste mali zmeniť predvolené heslo na dostatočne silné na dodatočné zabezpečenie zariadenia. Kým heslo nezmeníte, po prihlásení sa zobrazí okno s upozornením na zmenu hesla.

4. WEBSERVIS

4.1 STAV

Záložka stavu obsahuje aktuálne informácie o stave zariadenia v rôznych kategóriách. V pravom dolnom rohu môžete údaje aktualizovať manuálne alebo nastaviť automatické obnovovanie v konkrétnych intervaloch.

4.1.1 Prehľad systému

Záložka prehľadu systému zobrazuje základné informácie o zariadení rozdelené do skupín

Skupina	Informácie
O zariadení	• Model • Sériové číslo • Verzia softvéru • Verzia hardvéru
Stav zariadenia	• Aktuálny čas nastavený na zariadení • Čas od uvedenia do prevádzky • Vyuzitie procesora • Využitie pamäte RAM • Využitie pamäte FLASH
Modem LTE	• Stav SIM karty • Pridelené operátorom IPv4 • Pridelené operátorom IPv6 • Čas pripojenia • Množstvo údajov použitých za mesiac
WAN	• Stav portu WAN • Pridelené operátorom IPv4 • Priradená adresa IPv6 • MAC adresa rozhrania • Čas pripojenia
LAN	• Adresa IPv4 routera • Adresa IPv6 routera • Počet pripojených zariadení

4.1.2 Modem LTE

V záložke LTE modem nájdeme informácie o našom pripojení k mobilnej sieti rozdelené do skupín

Skupina	Informácie
Modem	• Model modemu • Verzia modemu • Sila signálu • Stav SIM karty • Číslo IMEI modemu • Číslo IMSI karty SIM • Číslo ICCID karty SIM • Poskytovateľ služieb • Typ pripojenia (LTE, 3G atď.) • Aktuálne identifikačné číslo PLMN • Kód miesta pre SIM kartu (LAC) • CELL ID číslo
Sieť	• Stav pripojenia k sieti operátora • IPv4 adresa so skráteným zadaním masky podsiete • Brána pre IPv4 • DNS pre IPv4 • IPv6 adresa • Brána pre IPv6 • DNS pre IPv6 • Čas pripojenia
Spotreba dát (mesačne)	• Množstvo odoslaných dát (Tx) • Množstvo prijatých dát (Rx) • Celkové množstvo údajov za posledných 30 dní

4.1.3 Sieť

Záložka siete zobrazuje informácie o pripojení k LAN a voliteľne k WAN cez kábel. Niektoré informácie sú viditeľné po nastavení portu LAN1 / WAN ako portu WAN.

Skupina	Informácie
WAN-IPv4 (viditeľné iba vtedy, keď je port LAN1 / WAN nastavený na WAN)	• Názov systémového portu • Stav pripojenia • Typ pripojenia (DHCP / statická IP) • IPv4 adresa • Brána pre IPv4 • DNS pre IPv4 • Čas pripojenia
WAN-IPv6 (viditeľné iba vtedy, keď je port LAN1 / WAN nastavený na WAN)	• Názov systémového portu • Stav pripojenia • Typ pripojenia (DHCP / statické IP) • IPv6 adresa • Brána pre IPv6 • DNS pre IPv6 • Čas pripojenia
Bridge	• Názov rozhrania • Stav STP • IPv4 adresa • IPv6 adresa • Zoznam VLAN patriacich do rozhrania

4.1.4 VPN

Záložka VPN obsahuje informácie o pripojeniach smerovača k sieti VPN ako klienta a o tom, ktoré zariadenia sú pripojené k routeru ako klienti VPN.

Skupina	Informácie
Klient	• Názov pripojenia smerovača ako klienta • Stav pripojenia k serveru VPN • Lokálna IP adresa routera • IP adresa servera VPN
Server	• Stav servera OpenVPN na routeri • Stav servera Ipsec na routeri
Zoznam spojení	• Server používaný klientom • IP klienta • Čas pripojenia klienta

4.1.5 Routing

Záložka routing obsahuje informácie z routing tabuľky zariadenia.

Skupina	Informácie
Smerovacia tabuľka	• Cieľová adresa zariadenia • Maska podsiete (IPv4) alebo predpona siete (IPv6) • Brána • Rozhranie používané klientom • Metrika smerovania
Pamäť ARP	• IP adresa klienta • MAC adresa priradená IP klientovi • Rozhranie používané klientom

4.1.6 Zoznam zariadení

Záložka zoznamu zariadení zobrazuje údaje o klientoch pripojených k routeru cez DHCP v dvoch skupinách. Skupina klientov DHCP obsahuje zoznam klientov, ktorým router automaticky priradil IP, a skupina MAC Binding zobrazuje zoznam klientov, ktorí majú IP adresu priradenú k MAC / DUID adrese

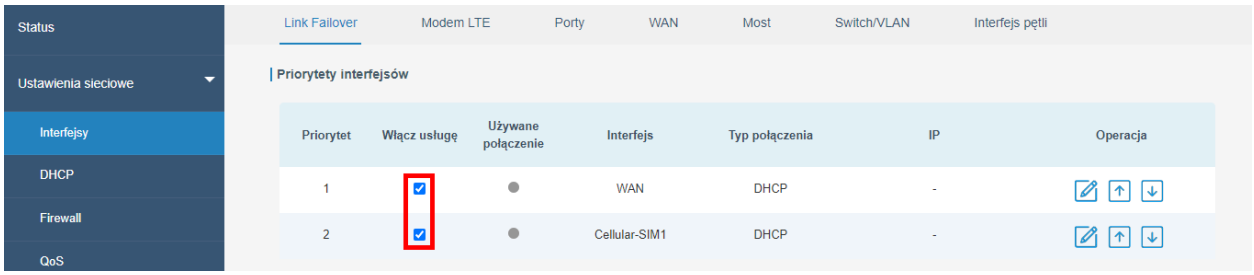
Skupina	Informácie
Klienti DHCP	• Adresa IP klienta • Adresa MAC/DUID klienta • Zostávajúci čas na rezervovanie IP adresy pre klienta
MAC Binding	• Adresa IP klienta • Adresa MAC/DUID klienta

4.2 NASTAVENIA SIETE

4.2.1 Rozhrania

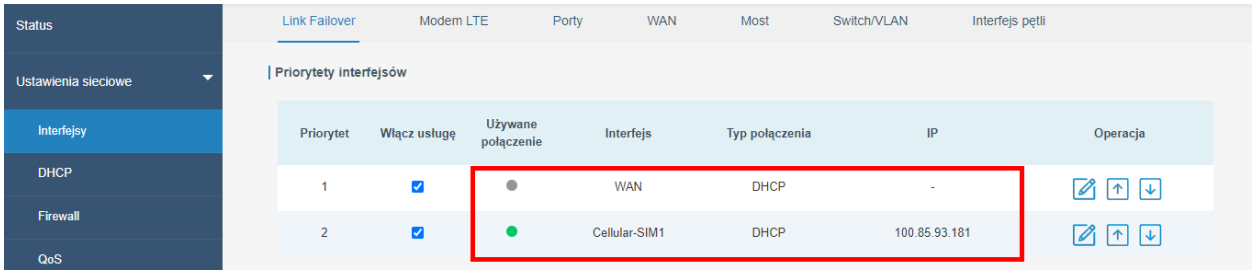
4.2.1.1 Link Failover

Záložka Link Failover umožňuje nastaviť redundanciu internetového pripojenia pomocou SIM karty alebo portu LAN1 / WAN, ak je tento port nastavený tak, aby fungoval ako WAN (časť 4.2.1.3), v opačnom prípade bude vidieť iba rozhranie SIM karty.
Skupina Interface **Priorities** je zodpovedná za výber poradia rozhraní, ktoré má router použiť pri prístupe na internet, zobrazuje základné údaje o pripojení na internet a umožňuje nastaviť parametre funkcie **PING Detection**, ktorá kontroluje, či sú rozhrania pripojené k internet.
Ak vyberiete možnosť **Povoliť službu** pri vybranom rozhraní, znamená to, že rozhranie sa bude podieľať na redundancii pripojení.



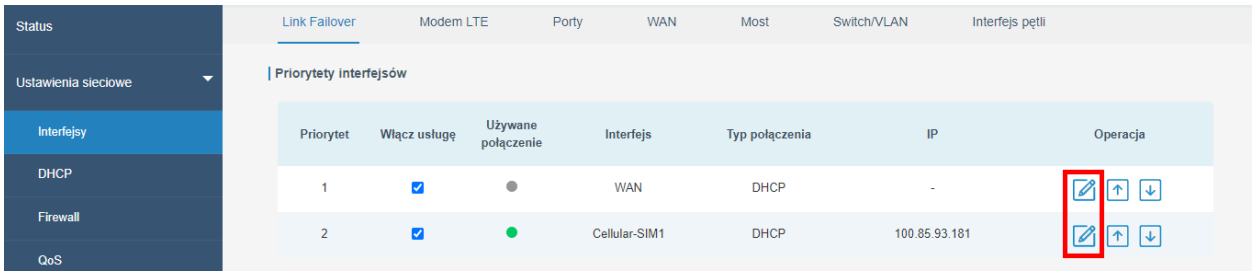
Obrázok 4.1 Povolenie servisnej funkcie

Centrálna časť tabuľky umožňuje získať informácie o aktuálne používanom rozhraní pri pripájaní na internet (**použité pripojenie**), názve rozhrania (**Interface)**, type pripojenia (**typ pripojenia**) a IP prijatej rozhraním (**IP**).



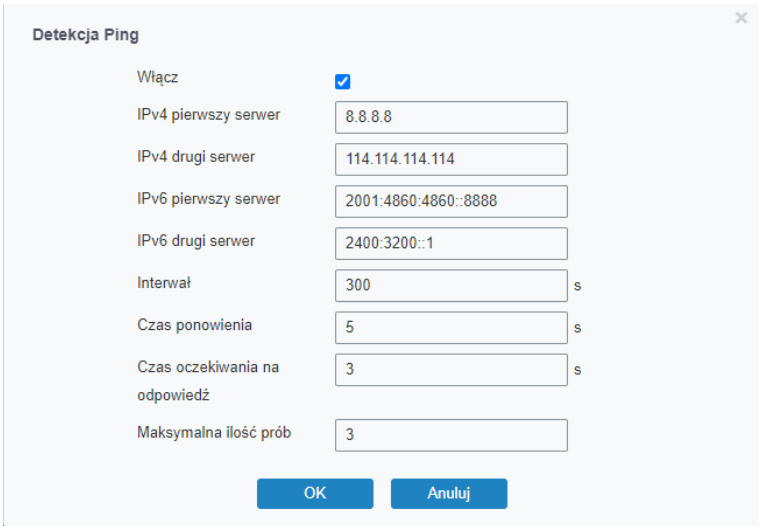
Obrázok 4.2 Informacje o interfejsach

Konfigurácia funkcie **PING Detection** sa spustí kliknutím na ikonu papiera a ceruzky vedľa zvoleného rozhrania.



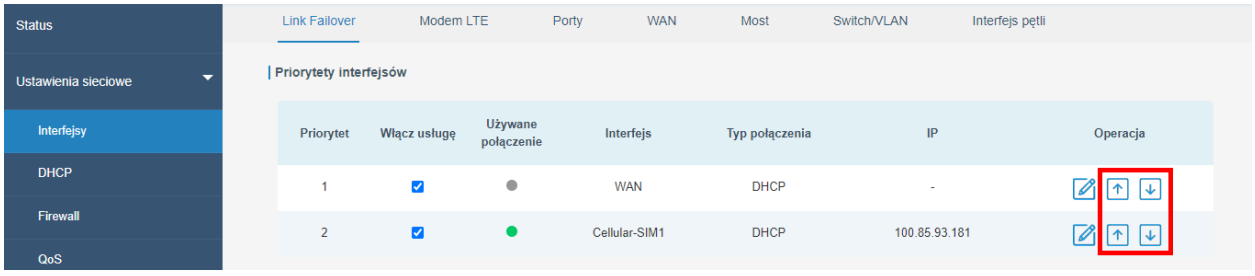
Obrázok 4.3 Ikona Ping Detecrion

Po kliknutí na vyššie uvedenú ikonu vyskočí okno pre konfiguráciu funkcie Softvér, v ktorom môžeme nastaviť: či sa má funkcia spustiť pre dané rozhranie (Softvér), adresy prvého a druhého servera dopytovaného funkciou pre IPv4 (**prvý server IPv4, druhý server IPv4**); prvý a druhý server, ktorý sa má dotazovať, bude funkcia pre IPv6 **(IPv6 1. server, IPv6 2. server**); časový interval medzi nasledujúcimi volaniami funkcií, vyjadrený v sekundách (**Interval**); časový interval opätovného volania funkcie, ak servery prvýkrát neodpovedajú, vyjadrený v sekundách (čas opakovania); čas, po ktorý bude funkcia čakať na odpoveď vyjadrený v sekundách (Čakacia doba na odpoveď); počet pokusov o vykonanie funkcie, kým router zistí, že rozhranie nemá pripojenie na internet (**Maximálny počet pokusov**).



Obrázok 4.4 Konfiguracja Detekcja PING

Ak chcete zmeniť poradie rozhraní, kliknite na šípky vedľa vybraného rozhrania, čím sa posunie nahor alebo nadol v zozname priorít.



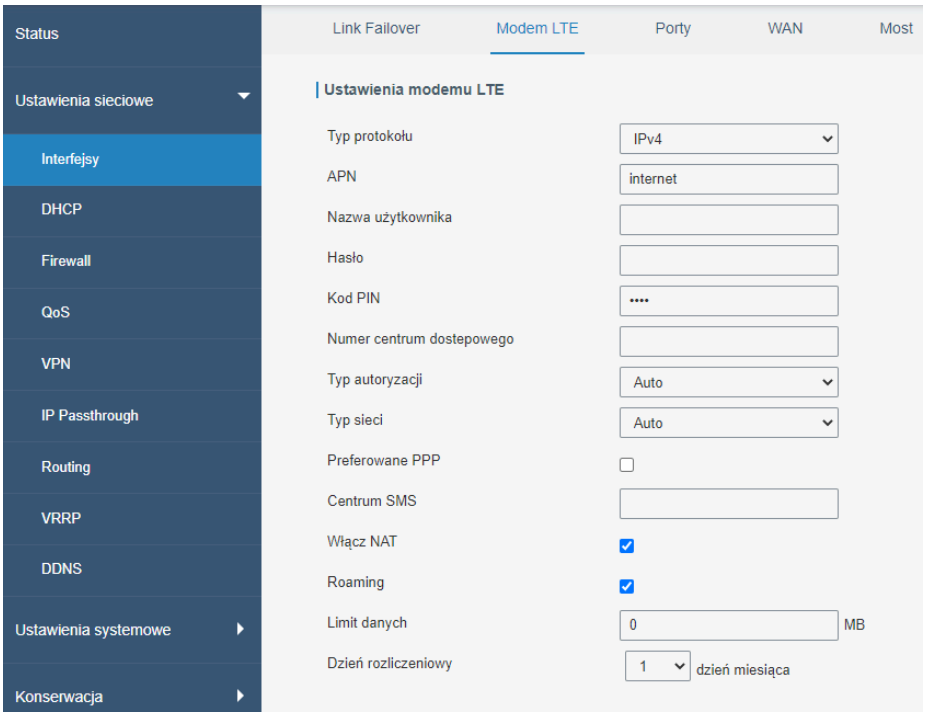
Obrázok 4.5 Zmiana priorytetów interfejsów

Skupina **Nastavenia** je zodpovedná za nastavenie času, po ktorom sa router pokúsi prepnúť na rozhranie s vyššou prioritou vyjadrenou v sekundách (**Return time**), ak je tento čas nastavený na 0s, funkcia sa nepokúsi prepnúť na vyššiu prioritu. Priorita, navyše v prípade nedostatku konektivity na všetkých rozhraniach môžeme prinútiť reštart routeru voľbou funkcie **núdzového reštartu**.

Obrázok 4.6 Nastavenia pre prepnutie na rozhranie s vyššou prioritou

4.2.1.2 Modem LTE

Záložka **Modem LTE** umožňuje konfigurovať rozhranie zodpovedné za pripojenie k internetu cez SIM kartu. V skupine **nastavení LTE modemu** si môžeme vybrať: či chceme použiť pripojenie IPv4 alebo IPv6 (**typ protokolu**); poskytnúť APN (**APN**) nášho poskytovateľa; užívateľské meno (**Username**); prístupové heslo (**Password**); PIN kód pre SIM kartu (**PIN kód**); telefónne číslo internetového centra poskytovateľa (číslo prístupového centra); typ oprávnenia pripojenia požadovaný prevádzkovateľom (**Typ oprávnenia**); typ pripojenia, ktoré bude router používať, napr. režim „iba 4G“ alebo „automatický“ (**typ siete**); či použiť PPP (**preferované PPP**); telefónne číslo SMS centra operátora, vďaka ktorému bude router zvládať SMS správy (**SMS Centrum**); spustiť službu NAT na routeri (**Povoliť NAT**); spustiť dátový roaming (**Roaming**); nastaviť dátový limit pre SIM kartu (**Dátový limit**); deň v mesiaci, ktorý je dňom fakturácie dodávateľa (**Billing Day**)

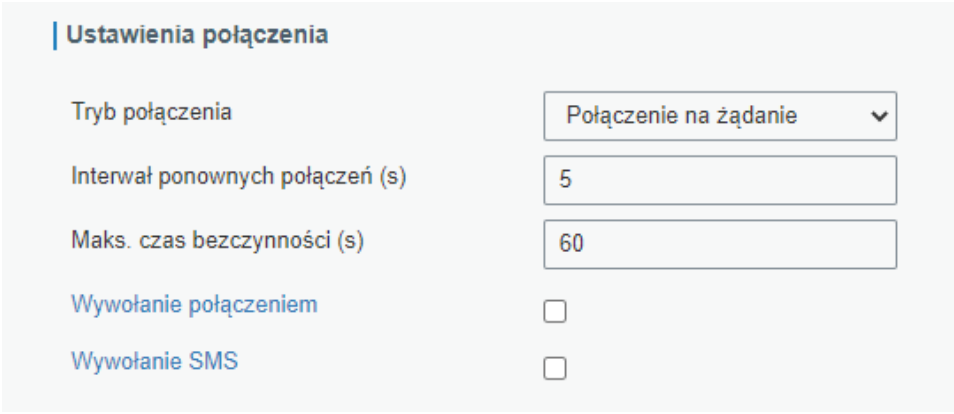


Obrázok 4.7 Konfigurácia pripojenia k poskytovateľovi internetu

Skupina **Nastavenia pripojenia** je zodpovedná za to, kedy sa má router pripojiť na internet pomocou SIM karty (**režim pripojenia**): môže byť pripojený stále pri výbere možnosti „**Vždy pripojený**“ alebo sa pripojiť na váš príkaz pri výbere možnosti „**Pripojenie na požiadanie**“ - možnosť po prijatí SMS (**SMS**) alebo telefonického hovoru (**Call**). Okrem toho môžno nastaviť pauzu medzi nasledujúcimi pokusmi o pripojenie k operátorovi vyjadrenú v sekundách (Reconnection interval) a dobu nečinnosti, po ktorej sa router odpojí od operátora pri výbere možnosti pripojenia na požiadanie, vyjadrenú v sekundách (**Maximum idle time**)

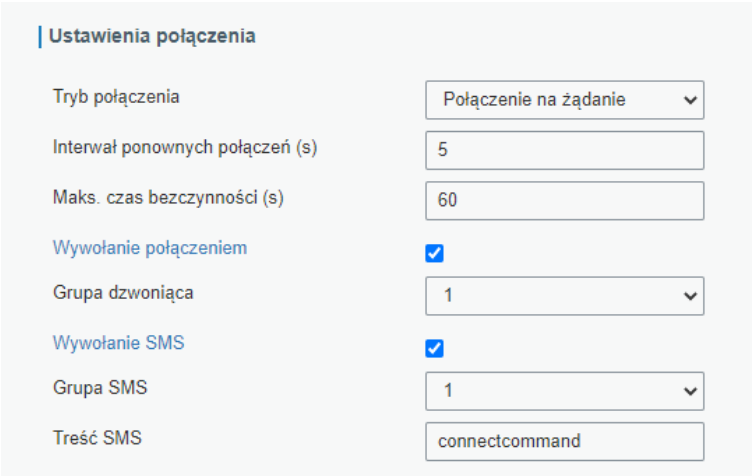
Obrázok 4.8 Vybrané nepretržité spojenie s operátorom

Pripojenie na požiadanie
Ak chcete nakonfigurovať spojenie s operátorom na požiadanie:
1. Vo voľbe Režim pripojenia vyberte „**Pripojenie na požiadanie**“,



Obrázok 4.9 Wybrane połączenie na żądanie

2. Vyberte, či sa spojenie má spustiť telefónnym hovorom (**Call**) a/alebo SMS (**SMS**),
3. V prípade voľby pomocou telefónneho spojenia zvoľte skupinu telefónnych čísel, ktorá to bude môcť vykonať (**Caller Group**), v prípade voľby pomocou SMS správ zvoľte skupinu čísel (**skupina SMS**) a text správy (**text SMS**). Skupiny čísel sú popísané v časti 4.3.2,



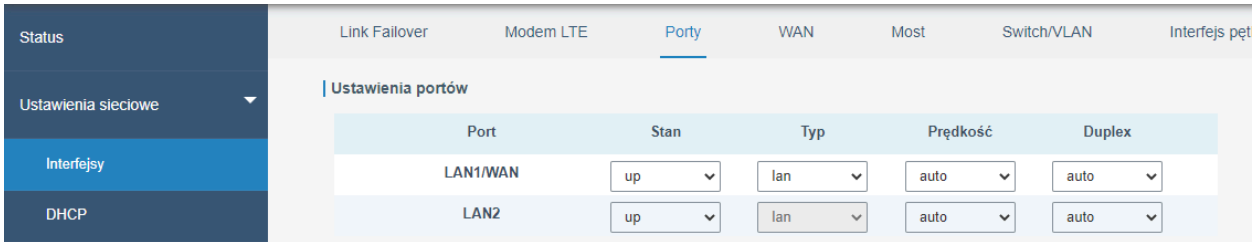
Obrázok 4.10 Konfiguracja połączenia na żądanie

4. Po výbere nastavení kliknite na tlačidlo SAVE

UPOZORNENIE!
Konfiguračné údaje uvedené vyššie sú dané ako príklady. Pre získanie správnych údajov pre pripojenie kontaktujte operátora, ktorý podporuje zvolenú SIM kartu.

4.2.1.3 Port

V záložke **Port** môžeme nakonfigurovať, ako majú fungovať porty RJ45 v routeri. Môžete ich vypnúť alebo zapnúť (**Stav**); pre port LAN1 / WAN môžeme nastaviť režim, v ktorom má LAN alebo WAN fungovať (**Typ**); rýchlosť, ktorou majú jednotlivé porty fungovať (**Speed**); typ pripojenia, ktorý majú používať porty **Full duplex / Half duplex / Auto (Duplex)**.



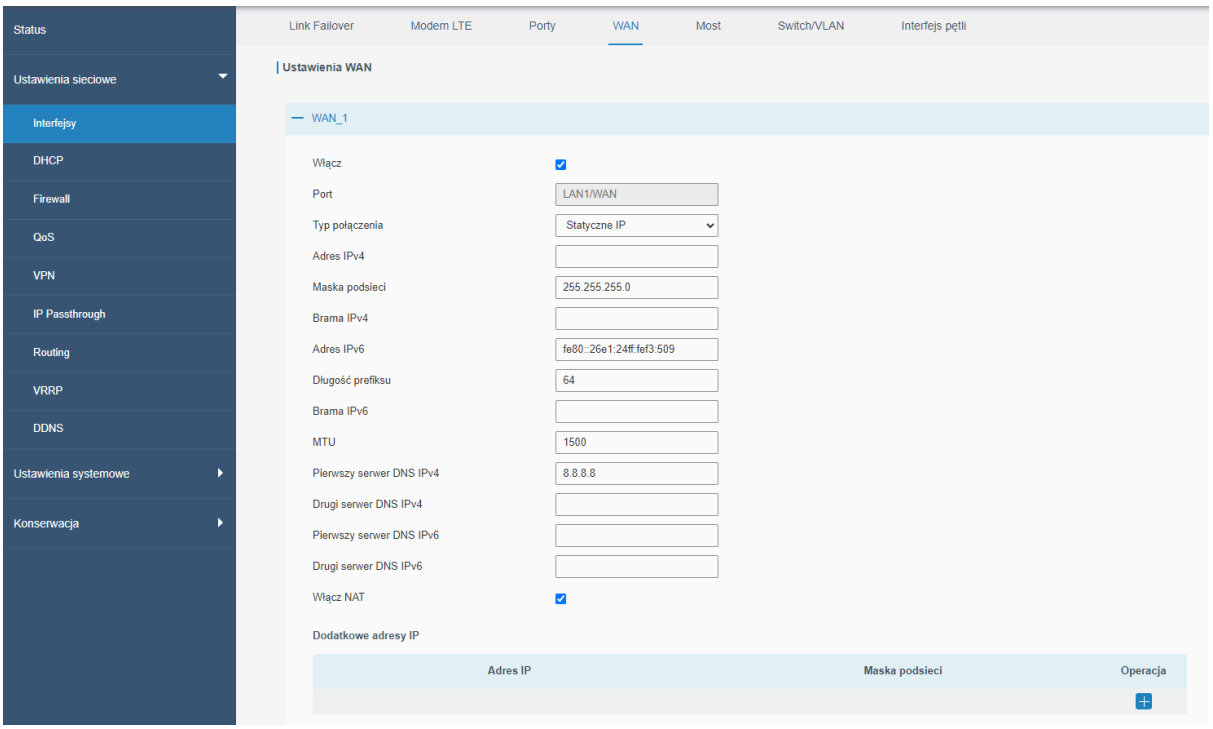
Obrázok 4.11 Konfiguracja działania portów RJ45

4.2.1.4 WAN

Záložka **WAN** sa používa na konfiguráciu portu WAN na pripojenie k internetu. Môžno tu nakonfigurovať 5 typov pripojenia: manuálna konfigurácia IP (**statická IP**); DHCP klient pre IPv4 (**DHCP klient**); pomocou protokolu PPPoE (**PPPoE**); DHCP klient pre IPv6 (**DHCPv6 klient**); pomocou technológie Dual-Stack Lite (**Dual-Stack Lite**). Všetky typy pripojenia budú popísané nižšie.

Manuálna konfigurácia IP/Pevná IP

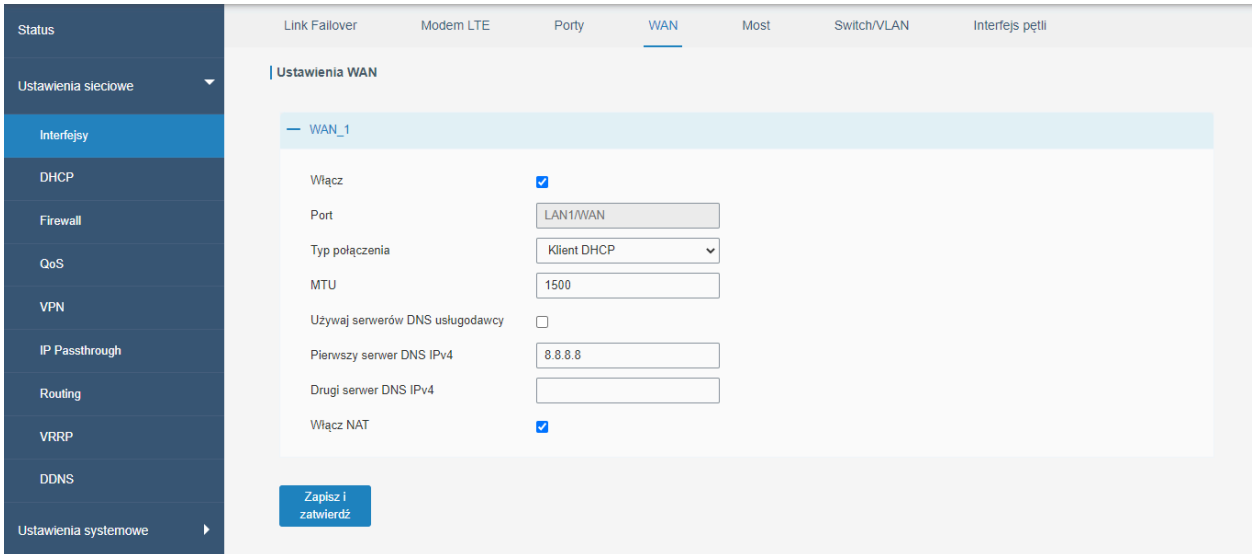
Ak chcete nakonfigurovať tento typ pripojenia, musíte zadať: adresu IPv4 rozhrania WAN v routeri (**adresa IPv4**); masku podsiete pre vyššie uvedený IPv4 (**maska podsiete**); predvolenú bránu pre IPv4 (**brána IPv4**); IPv6 adresu WAN rozhrania v routeri (**IPv6 adresa**), pole vyššie obsahuje predvolenú adresu rozhrania vypočítanú na základe MAC adresy rozhrania v routeri; dĺžku prefixu pre IPv6 (**Prefix Lengt**h), predvolenú bránu pre IPv6 (**IPv6 brána**); veľkosť internetového rámca (**MTU**); adresy serverov DNS pre IPv4 (**prvý server DNS IPv4, druhý server DNS IPv4**); adresy serverov DNS pre IPv6 (**prvý server DNS IPv6, druhý server IPv6**); povoľte funkciu NAT na strane routera (**Enable NAT**). Výberom tohto typu pripojenia môžeme priradiť aj ďalšie IPv4 adresy pre WAN rozhranie v routeri.



Obrázok 4.12 Konfigurácia portu WAN pre pevnú IP

Klient DHCP pre IPv4

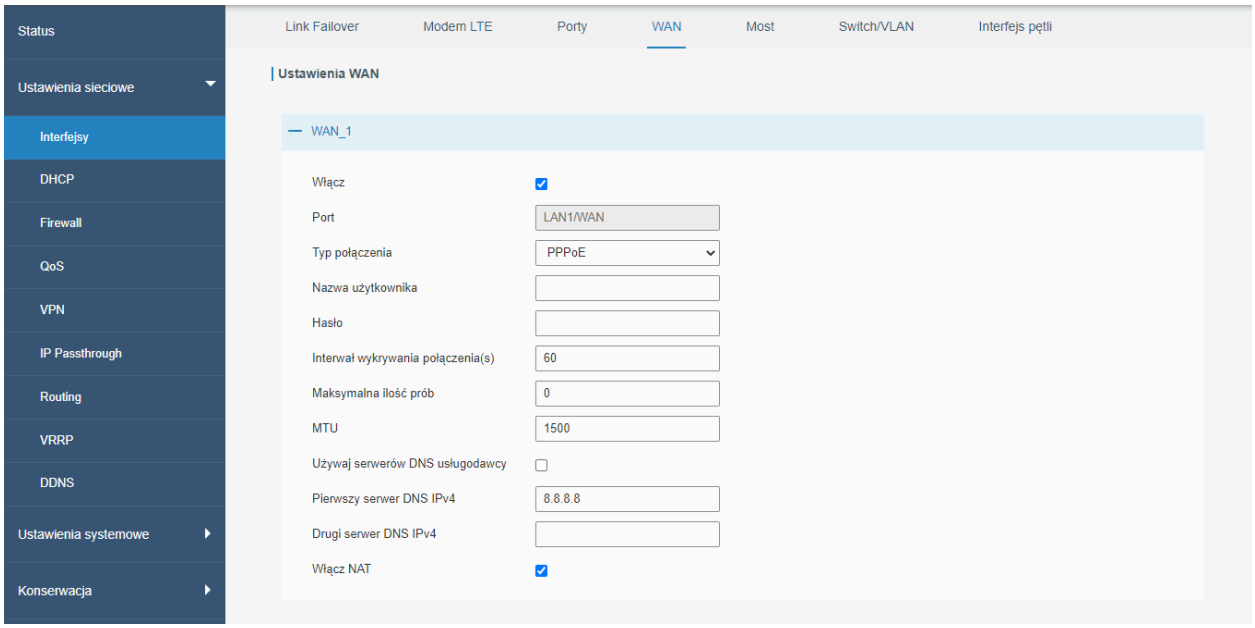
Konfigurácia tohto typu pripojenia by sa mala vykonávať automaticky, ale môžeme sem zadať údaje ako: veľkosť internetového rámca (**MTU**); vybrať, či chceme použiť DNS servery dané DHCP serverom alebo ich zadať ručne (**Použiť DNS servery poskytovateľa služby**); ak nepoužijeme vyššie uvedenú možnosť, musíme adresy serverov DNS zadať ručne (**prvý server DNS IPv4, druhý server DNS IPv4**); povoliť funkciu NAT na strane routera (**Povoliť NAT**).



Obrázok 4.13 Konfigurácia portu WAN pre klienta DHCP

PPPoE

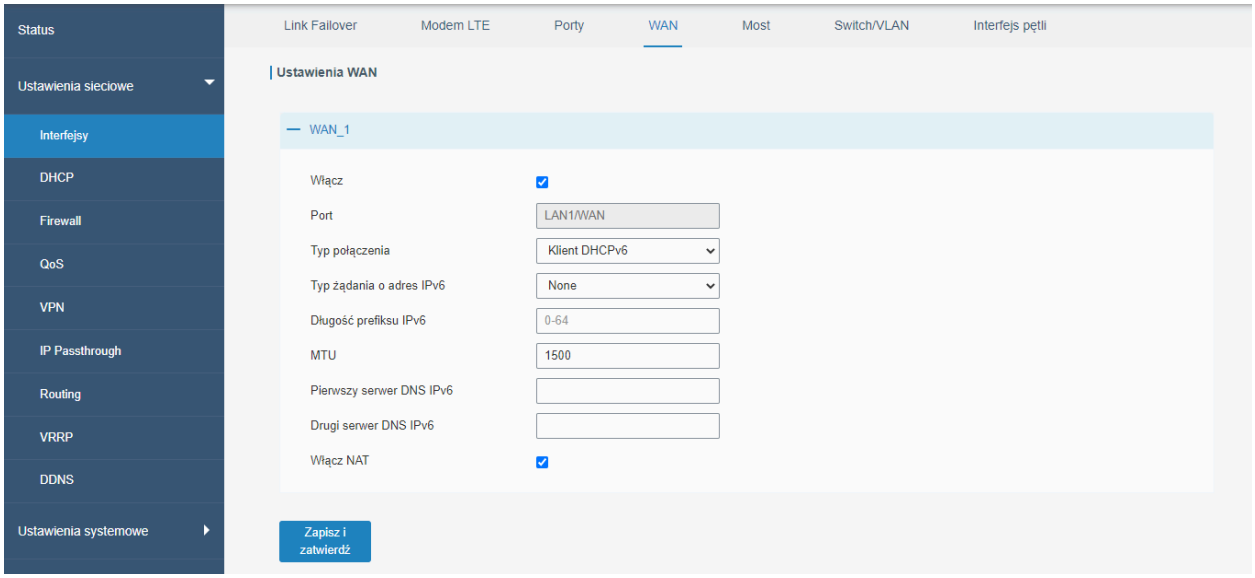
Ak chcete nakonfigurovať tento typ pripojenia, musíte poskytnúť prihlasovacie údaje do siete poskytovateľa služieb, tj: používateľské meno (**User name**); heslo (**Password**); časový interval medzi pokusmi o pripojenie k sieti vyjadrený v sekundách (**Interval detekcie pripojenia**); veľkosť rámu (**MTU**); zvoliť, či použiť adresy serverov DNS poskytnuté poskytovateľom služieb alebo ich zadať manuálne (**Použite servery DNS poskytovateľa služieb**); ak používate vlastné DNS servery, uveďte ich adresy (**prvý DNS server IPv4, druhý DNS server IPv4**); povoliť funkciu NAT na strane routera (**Povoliť NAT**).



Obrázok 4.14 Konfigurácia portu WAN pre PPPoE

Klient DHCP IPv6

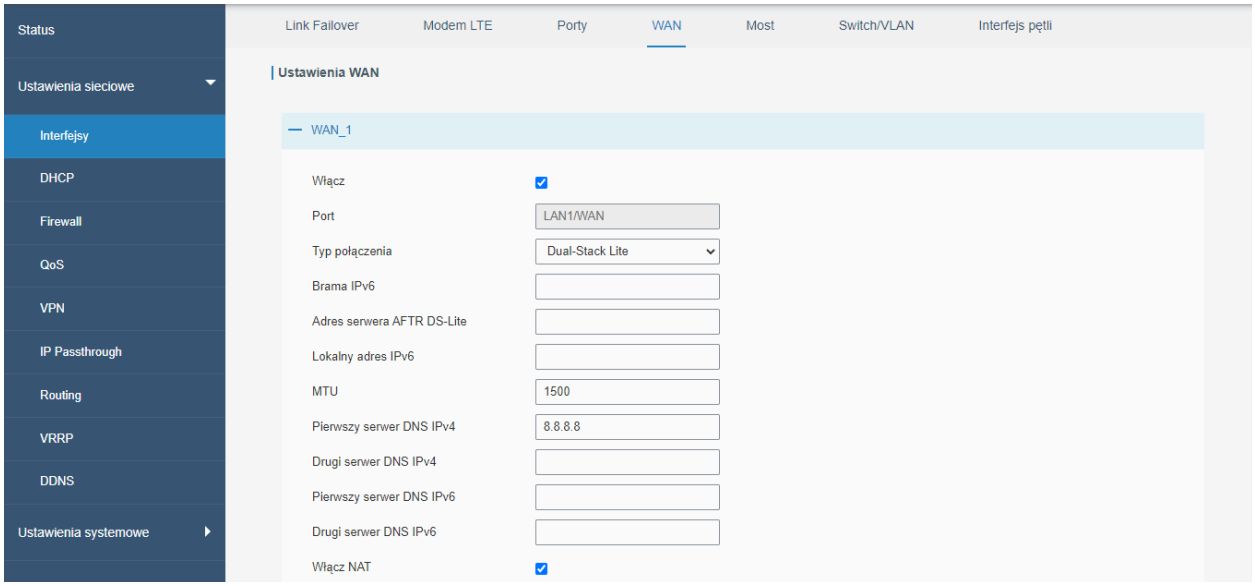
Konfigurácia tohto typu pripojenia by sa mala vykonávať automaticky, ale môžno tu poskytnúť údaje ako: spôsob pridelenia IP adresy pre router serverom DHCPv6 (**typ požiadavky na adresu IPv6)**; dĺžku prefixu pre IPv6 (**IPv6 Prefix Length**); veľkosť internetového rámca (**MTU**); vybrať, či chcete použiť DNS servery dané DHCP serverom alebo ich zadať ručne (**Použiť DNS servery poskytovateľa služby**); ak nepoužijete vyššie uvedenú možnosť, musíte adresy serverov DNS zadať ručne (**prvý server DNS IPv6, druhý server IPv6**); povoliť funkciu NAT na strane routera (**Povoliť NAT**).



Obrázok 4.15 Konfigurácia portu WAN pre klienta DHCPv6

Dual-Stack Lite

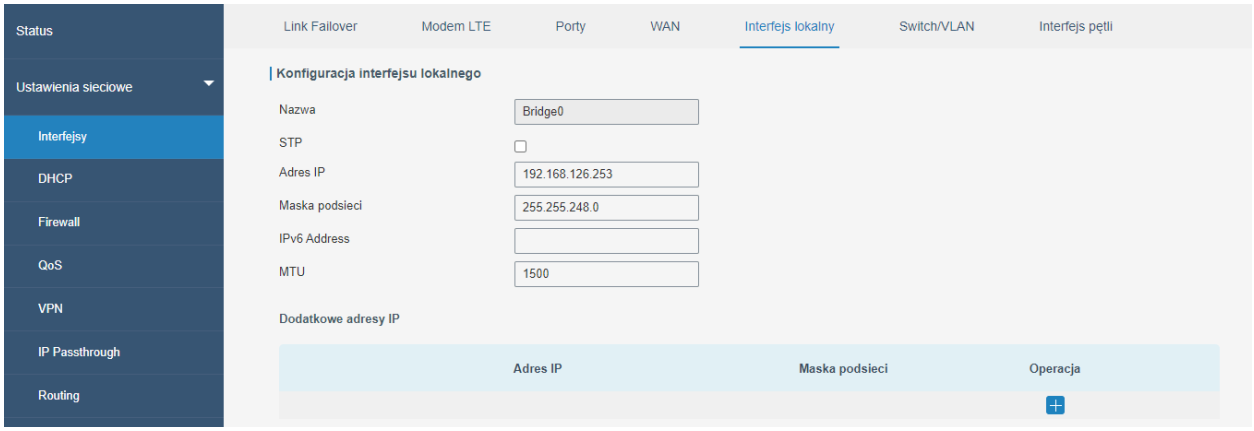
Ak chcete nakonfigurovať tento typ pripojenia, musíte zadať: adresu brány IPv6 (**brána IPv6**); adresu routera AFTR (**adresa servera AFTR DS-Lite**); IPv6 adresu (**lokálna IPv6 adresa**); veľkosť internetového rámca (**MTU**); adresy serverov DNS pre IPv4 (**prvý server DNS IPv4, druhý server DNS IPv4**); adresy serverov DNS pre IPv6 (**prvý server DNS IPv6, druhý server IPv6**); povoliť funkciu NAT na strane smerovača **(Povoliť NAT**).



Obrázok 4.16 Konfigurácia portu WAN pre Dual-Stack Lite

4.2.1.5 Lokálne rozhranie

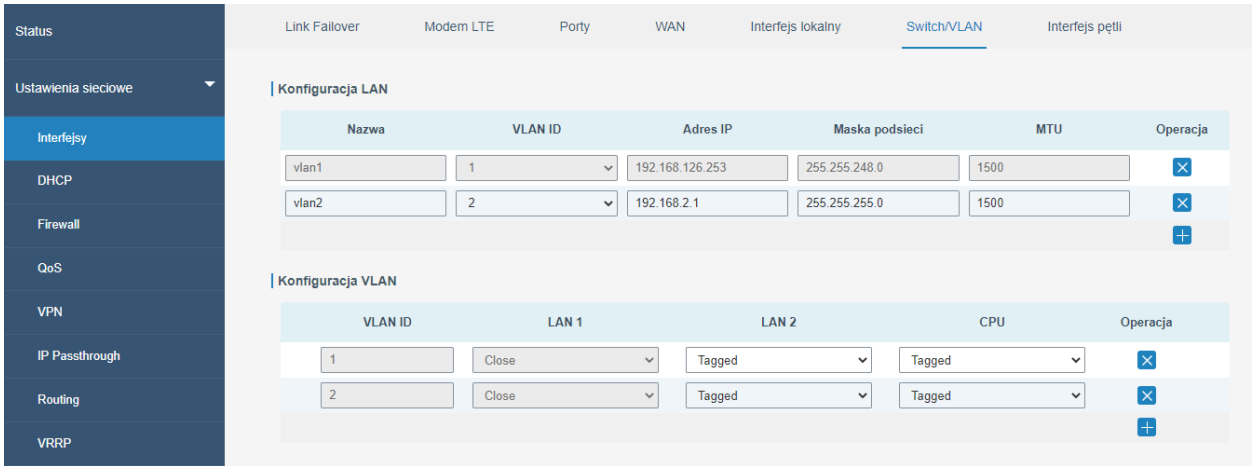
V záložke **Local interface** môžete nakonfigurovať LAN rozhranie routera. Môžete tu nastaviť: či má rozhranie používať protokol **STP** (SpanningTreeProtocol); adresu IPv4 rozhrania (**IP adresa**); masku podsiete (**Maska podsiete**); adresu IPv6 rozhrania (**adresa IPv6**); veľkosť internetového rámca (**MTU**). Okrem základnej konfigurácie môžete pridať aj podporu viacerých IP adries pre **lokálne rozhranie**.



Obrázok 4.17 Konfigurácia lokálneho rozhrania

4.2.1.6 Switch

Záložka **Switch / VLAN** sa používa na konfiguráciu možností VLAN. VLAN rozdeľuje fyzické rozhrania zariadenia do logických pracovných skupín. Keďže router podporuje funkciu VLAN v štandarde IEEE 802.1Q, viete ho nakonfigurovať tak, aby sa na jednom fyzickom porte stretávalo veľa logických sietí. So správnou konfiguráciou externého prepínača môžete poskytnúť redundantný prístup k internetu do mnohých VLAN cez jeden LAN port.



Obrázok 4.18 Konfigurácia VLAN

4.2.1.7 Rozhranie pre slučku

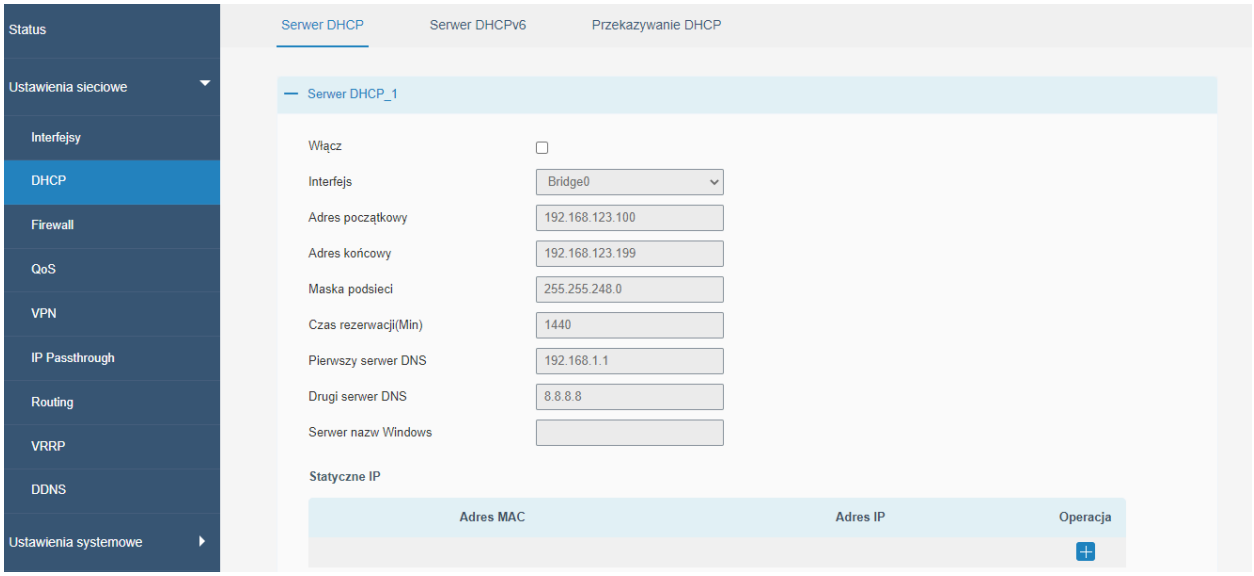
Záložka **rozhrania pre slučky** vám umožňuje konfigurovať nastavenia rozhrania slučky. Je to logické rozhranie routera, ktoré nemá žiadny fyzický odraz. V smerovacích protokoloch IP sa toto rozhranie často používa ako ID zariadenia. Okrem predvolených hodnôt môžete pridať svoje vlastné adresy.

4.2.2 DHCP

V záložke DHCP môžete nakonfigurovať činnosť routera ako server DHCP alebo DHCPv6 a ako zariadenie prenášajúce konfiguráciu DHCP. Ak nastavíte port LAN1 / WAN ako port WAN (časť 4.2.1.3), môžete v skutočnosti nakonfigurovať dva servery DHCP, pre každé rozhranie samostatne (WAN, Bridge0).

DHCP

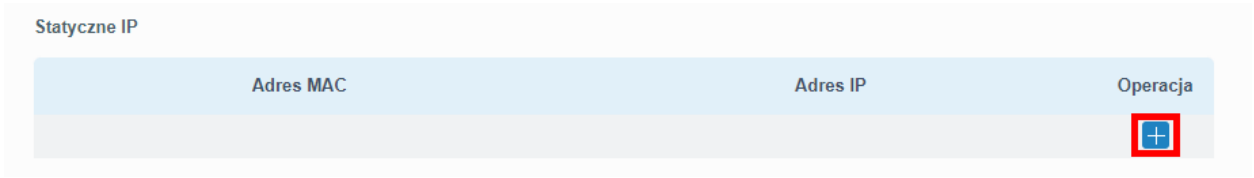
Ak chcete nakonfigurovať router ako server DHCP: povoľte službu (**Zapnúť**); vyberte rozhranie, ktoré má daný server obsluhovať (**Interface**); nastavte rozsah adresovania zadaním najnižšej možnej adresy pre zariadenie (**počiatočná adresa**) a najvyššej možnej adresy (**koncová adresa**); masku podsiete (**Maska podsiete**); čas, na ktorý bude danému zariadeniu pridelená adresa, vyjadrený v minútach v rozsahu 5-1440 (čas rezervácie); DNS adresy pre IPv4 (**prvý server DNS, druhý server DNS**); adresu názvového servera Windows (**názvový server Windows**).



Obrázok 4.19 Konfigurácia servera DHCP

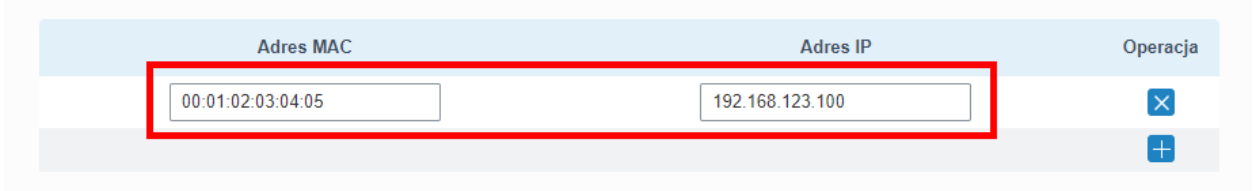
Ak chcete, aby zariadenie malo po pripojení k routeru vždy pridelenú rovnakú IP adresu, urobte nasledovné:

1. Kliknite na ⊞ v sekcii **Statická IP** v stĺpci **Operácia**



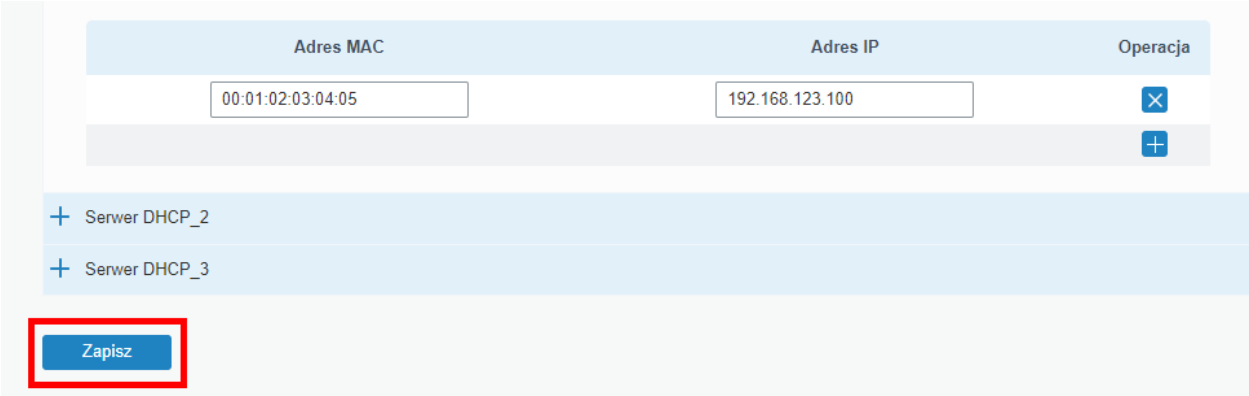
Obrázok 4.20 Pridanie pevnej adresy IP pre klienta DHCP Krok 1

2. Zadajte MAC adresu zariadenia a IP adresu, ktorú má zariadenie prijať



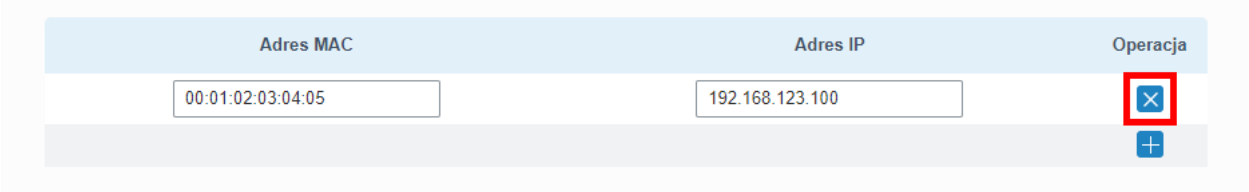
Obrázok 4.21 Pridanie pevnej adresy IP pre klienta DHCP Krok 2

3. Ak chcete pridať ďalšie zariadenia, znova kliknite na ⊞
4. Po pridaní všetkých adries kliknite na tlačidlo **Uložiť**



Obrázok 4.22 Pridanie pevnej adresy IP pre klienta DHCP Krok 4

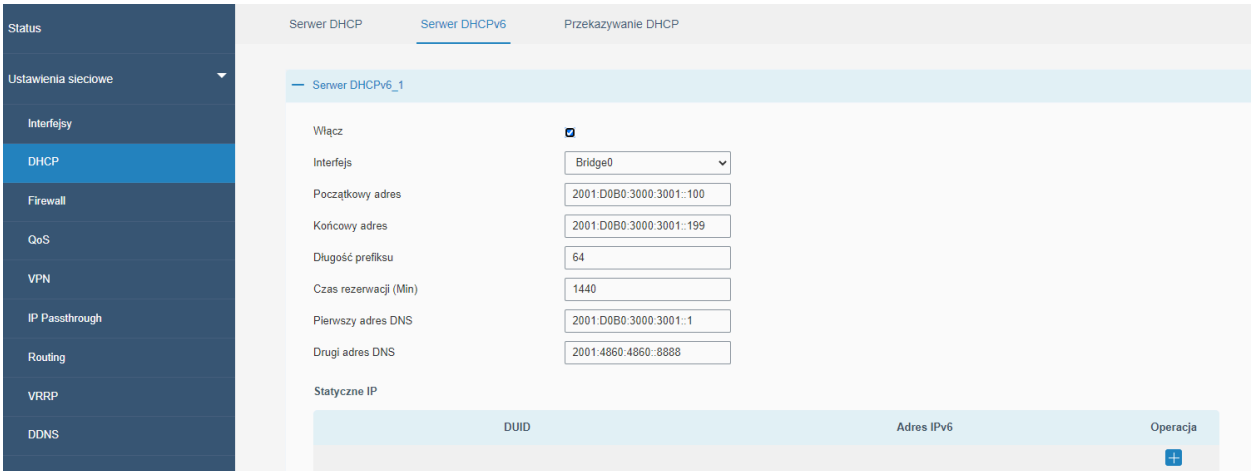
Ak chceme odstrániť zariadenie zo zoznamu pevných IP, klikneme na krížik pri danej položke



Obrázok 4.23 Odstránenie zariadenia zo zoznamu statických IP adries pre DHCP server

DHCPv6

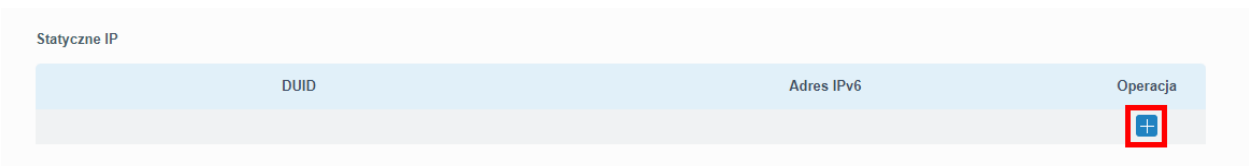
Ak chcete nakonfigurovať router ako server DHCPv6: povoľte službu (**Povoliť**); vyberte rozhranie, ktoré má daný server obsluhovať (**Interface**); nastavte rozsah adresovania zadaním najnižšej možnej adresy pre zariadenie (**počiatočná adresa**) a najvyššej možnej adresy (**koncová adresa**); dĺžku predpony pre IPv6 (**dĺžka predpony**); čas, na ktorý bude danému zariadeniu pridelená adresa, vyjadrený v minútach v rozsahu 5-1440 (čas rezervácie); adresy DNS pre IPv4 (**prvý server DNS, druhý server DNS**).



Obrázok 4.24 Konfigurácia servera DHCPv6

Ak chcete, aby zariadenie malo po pripojení k routeru vždy pridelenú rovnakú IP adresu, urobte nasledovné:

1. Kliknite na ⊞ v sekcii **Statická IP** v stĺpci **Operácia**

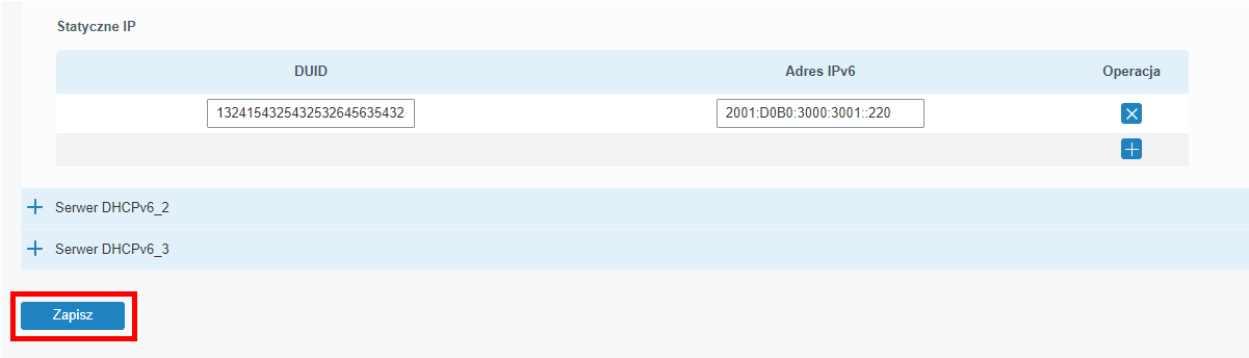


Obrázok 4.25 Pridanie pevnej IP adresy pre klienta DHCPv6 krok 1

2. Zadajte DUID zariadenia a IP adresu, ktorú má zariadenie prijať

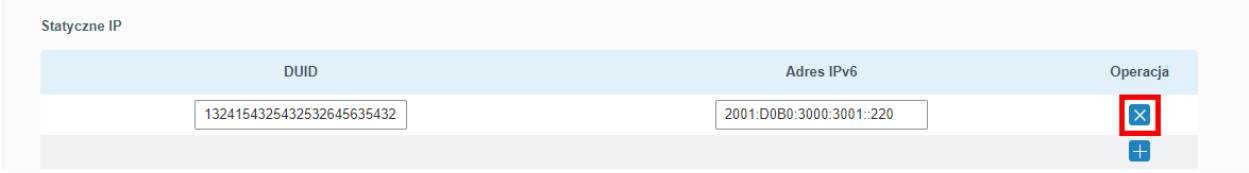
Obrázok 4.26 Pridanie pevnej IP adresy pre klienta DHCPv6 Krok 2

3. Ak chcete pridať ďalšie zariadenia, znova kliknite na
4. Po pridaní všetkých adries kliknite na tlačidlo **Uložiť**



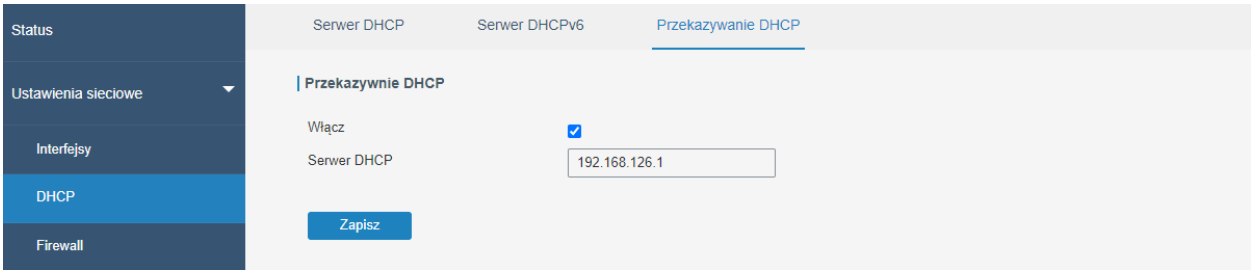
Obrázok 4.27 Pridanie pevnej IP adresy pre klienta DHCPv6 Krok 4

Ak chcete odstrániť zariadenie zo zoznamu pevných IP, kliknite na krížik pri danej položke



Obrázok 4.28 Odstránenie zariadenia zo zoznamu statických IP adries pre server DHCPv6

Presmerovanie DHCP
Funkcia prenosu DHCP vám umožňuje označiť server DHCP, ktorý je v inej sieti, ako je sieť vytvorená routerom s pripojenými hostiteľmi.
Ak chcete nakonfigurovať fungovanie tejto funkcie, musíte: povoliť funkciu (**Zapnúť**) a poskytnúť adresu externého servera DHCP (**server DHCP**). Voliteľne môžete zadať viac ako jednu adresu DHCP servera, môžete ich zadať maximálne 10 a každú ďalšiu oddeľte v poli **DHCP server** bodkočiarkou „;”.



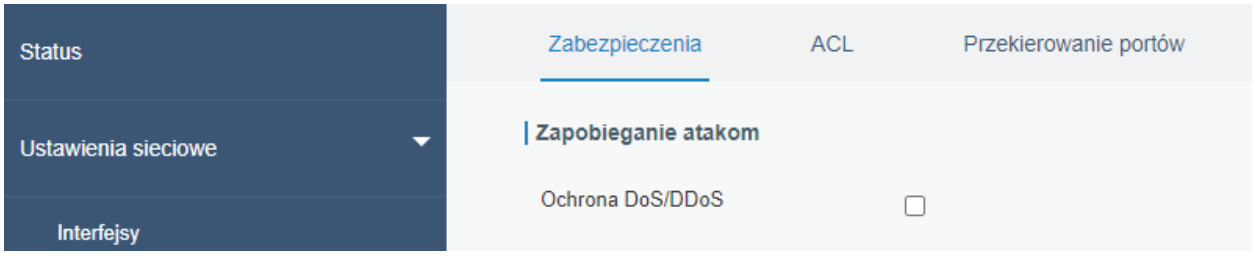
Obrázok 4.29 Preposielanie DHCP

4.2.3 Firewall

4.2.3.1 Bezpečnosť

Predchádzanie útokom

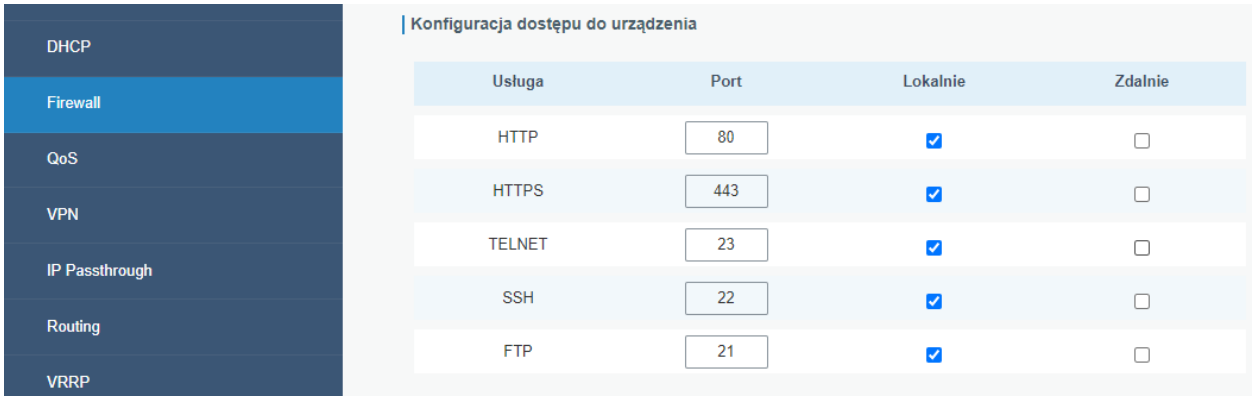
Možnosť **ochrany DoS / DDoS** umožňuje povoliť ochranu routera pred útokmi DoS a DDoS, ktoré by mohli blokovať správne fungovanie zariadenia



Obrázok 4.30 Ochrana DoS/DDoS

Konfigurácia prístupu k zariadeniu

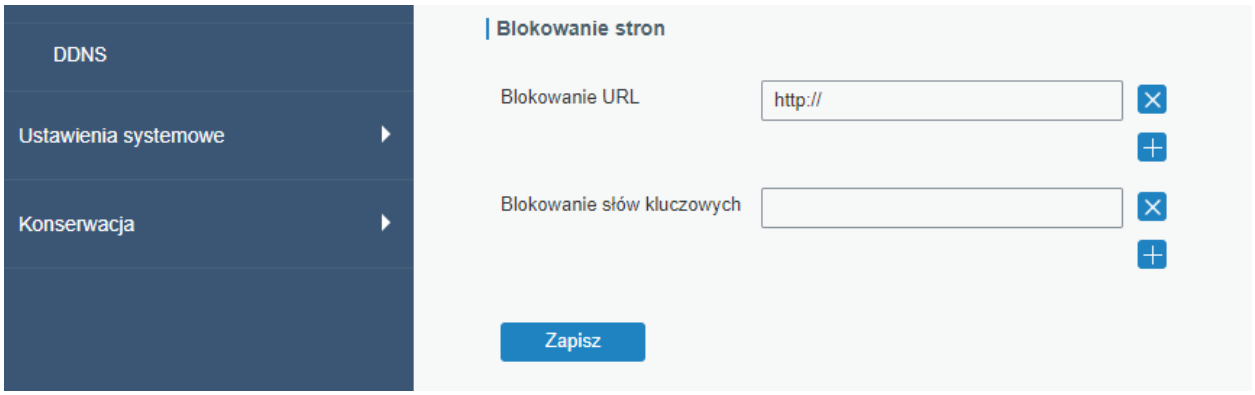
V tejto skupine nastavení môžete konfigurovať, ako bude možné s routerom komunikovať za účelom jeho konfigurácie (**Service**) a či to bude možné cez lokálne pripojenie k zariadeniu (**Local**) alebo vzdialene (**Remote**).



Obrázok 4.31 Konfigurácia prístupu k zariadeniu

Blokovanie stránok

Táto skupina je zodpovedná za zoznam webových stránok (**blokovanie URL**) a kľúčových slov (**blokovanie kľúčových slov**), ktoré budú routerom blokované. Ak chcete pridať stránku alebo kľúčové slovo, kliknite na vedľa možnosti a potom zadajte stránku / kľúčové slovo. Po dokončení konfigurácie kliknite na tlačidlo **Uložiť**.



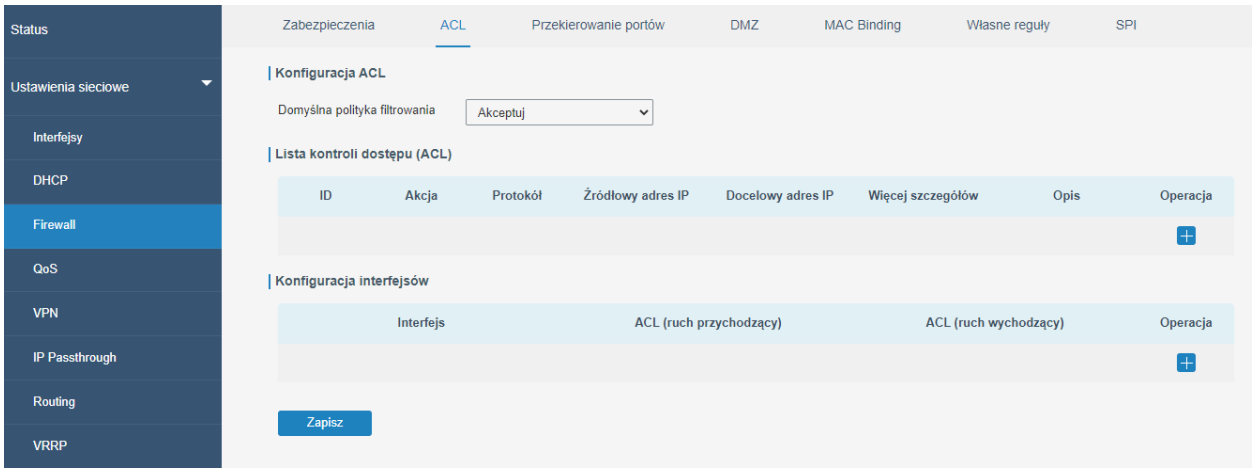
Obrázok 4.32 Blokovanie stránok

4.2.3.2 ACL

Zoznam riadenia prístupu, tiež známy ako ACL, implementuje pravidlá prístupu pre špecifickú sieťovú prevádzku. Keď router prijme paket, bude analyzovaný podľa pravidla ACL aplikovaného na aktuálne rozhranie. Po identifikácii, či je dátová sieťová prevádzka povolená alebo nie, môže byť paket odovzdaný koncovému zariadeniu alebo zablokovaný routerom.

Konfigurácia ACL

V tejto skupine môžete nastaviť, ako sa má zaobchádzať so sieťovou prevádzkou, ktorá nie je priradená žiadnemu pravidlu ACL. Nastavenie „Prijať" vo voľbe **Predvolená politika filtrovania** umožňuje štandardne spracovávať takúto komunikáciu, t. j. odovzdávať pakety koncovým zariadeniam.



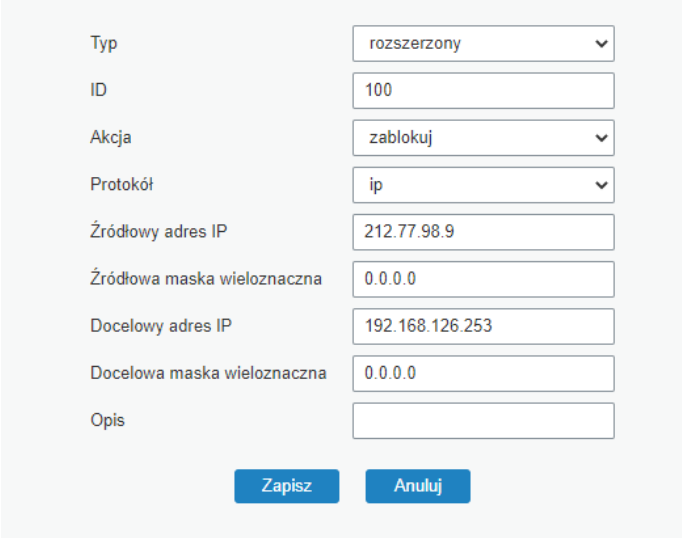
Obrázok 4.33 Konfigurácia ACL

Access Control List

Do tejto skupiny môžeme pridať pravidlá ACL. Ak chcete pridať takéto pravidlo, postupujte nasledovne:
1. Kliknite na + v stĺpci **Operácia**

Obrázok 4.34 Pridajte pravidlo ACL, krok 1

Vyberte štandardný typ alebo typ rozšíreného pravidla. V prípade výberu štandardného typu sú údaje, ktoré musíte poskytnúť obmedzené na: ID pravidlo v rozsahu 1-199; typ akcie: priznať (prijať), blokovať (odmietnuť); IP adresu siete, z ktorej paket pochádza (**Zdrojová IP adresa**); masku zástupných znakov **(maska zástupných znakov zdroja**); popis pravidla.
Ak zvolíte rozšírený typ, môžete si vybrať protokol, na ktorý sa bude pravidlo vzťahovať, na obrázku nižšie sú príklady nastavení rozšíreného typu a IP protokolu

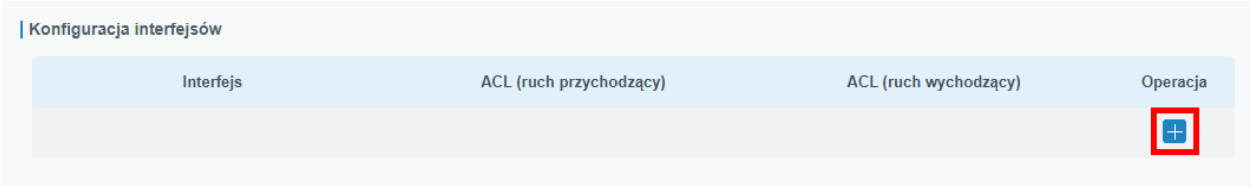


Obrázok 4.35 Pridajte pravidlo ACL, krok 2

1. Po zadaní údajov kliknite na tlačidlo **Uložiť**

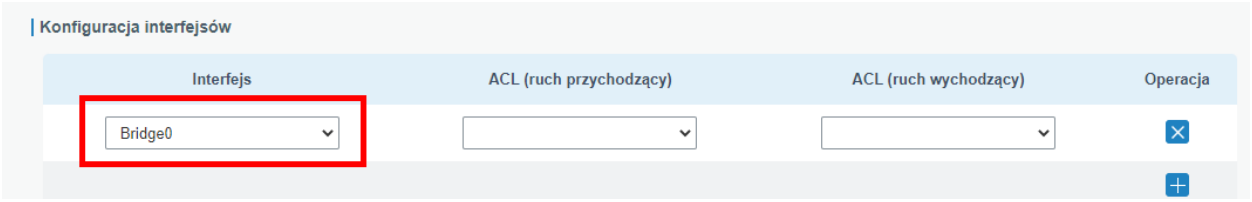
Konfigurácia rozhraní
V tejto skupine nastavení priraďujeme rozhraniam routera špecifické pravidlá. Ak chcete rozhraniu priradiť konkrétne pravidlo, musíte urobiť nasledujúce:

1. Kliknite na + v stĺpci **Operácia**



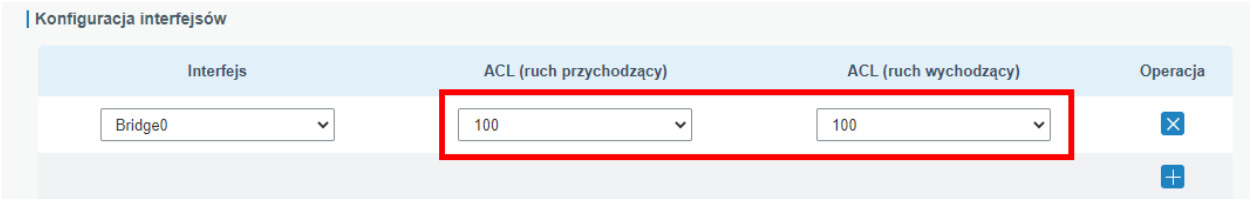
Obrázok 4.36 Pridajte pravidlo ACL, krok 1

2. Vyberte rozhranie, ktorému chcete priradiť pravidlo



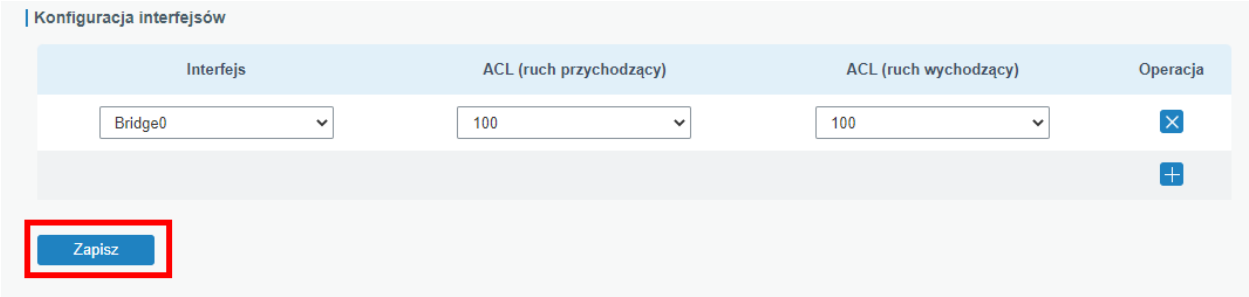
Obrázok 4. Pridajte pravidlo ACL, krok 2

3. Vyberte pravidlá pre prichádzajúcu a/alebo odchádzajúce prenosy



Obrázok 4.38 Pridajte pravidlo ACL, krok 3

4. Po zadaní údajov kliknite na tlačidlo **Uložiť**

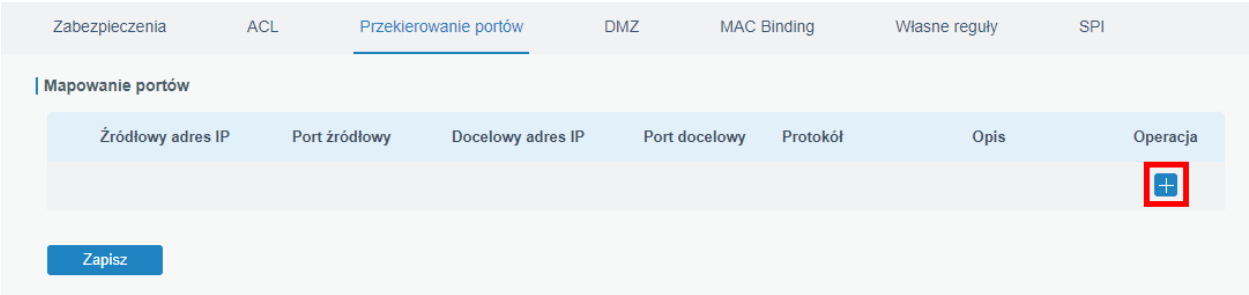


Obrázok 4.39 Pridajte pravidlo ACL, krok 4

4.2.3.3 Presmerovanie portov

V prípade použitia funkcie NAT v routeri (aby ste sa dostali k zariadeniam v tejto sieti mimo internej LAN siete) musíte pre dané zariadenie aktivovať presmerovanie portov. Príkladom použitia presmerovania portov môže byť webový server, ktorý sa nachádza v našej internej sieti a radi by sme túto stránku zdieľali mimo našej siete. Po nastavení presmerovania budú všetky pakety so správnym typom a portom presmerované na príslušné zariadenie v internej LAN. Na nastavenie takéhoto presmerovania je potrebné urobiť nasledovné:

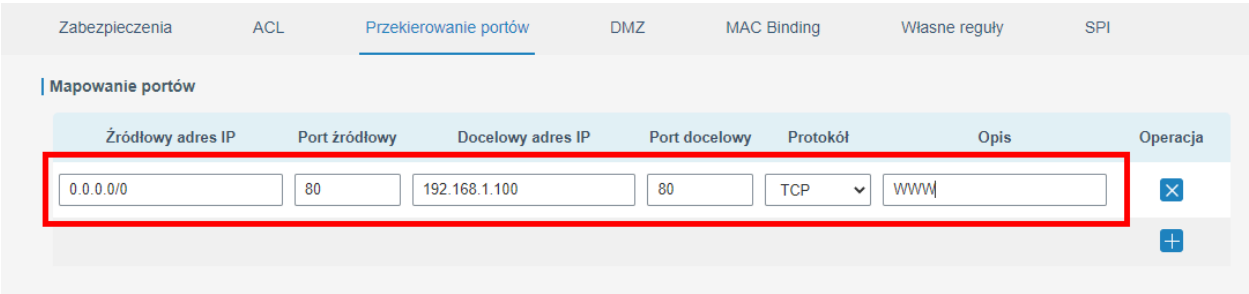
1. Kliknite na + v stĺpci **Operácia**



Obrázok 4.40 Presmerovanie portov krok 1

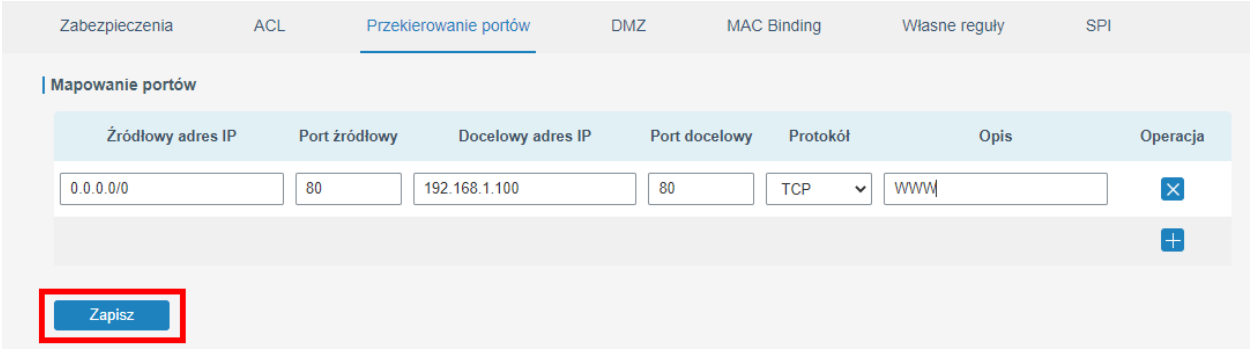
2. Uveďte:

– IP zariadenia, z ktorého prichádza požiadavka (zadaním adresy 0.0.0.0 budú presmerované pakety prichádzajúce z akejkoľvek adresy)
– Port, na ktorom sa externé zariadenie pokúša komunikovať
– IP zariadenia, na ktoré sa majú posielať pakety
– Port, na ktorý majú byť pakety presmerované (zvyčajne rovnaké ako tie, ktoré prichádzajú z externého zariadenia)
– TCP / UDP protokol / oba
– Popis presmerovania



Obrázok 4.41Presmerovanie portov krok 2

3. Po vyplnení údajov kliknite na tlačidlo **Uložiť**

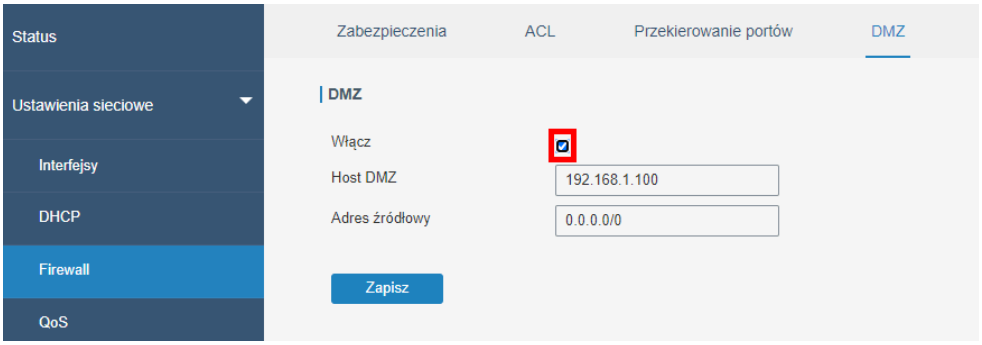


Obrázok 4.42Presmerovanie portov krok 3

4.2.3.4 DMZ

Funkcia DMZ funguje tak, ako keby sme ručne presmerovali na danú IP adresu všetky porty prichádzajúce z internetu. Pri používaní tejto funkcie buďte veľmi opatrní, pretože môže výrazne znížiť bezpečnosť vašej siete. Ak chcete zapnúť funkciu DMZ, urobye nasledujúce kroky:

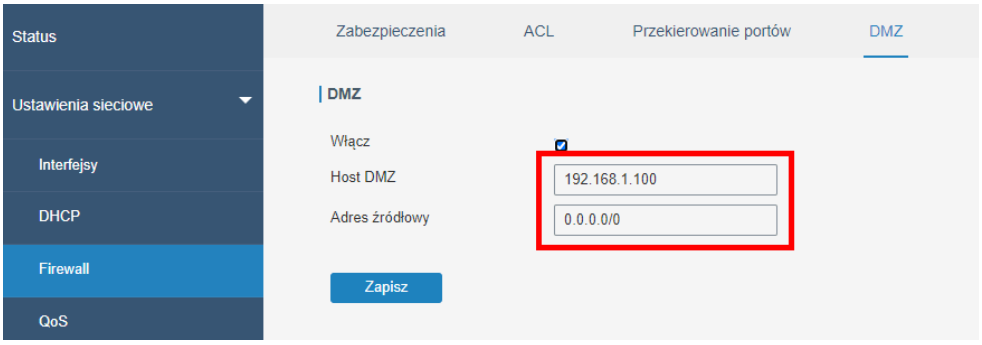
1. Aktivujte funkciu (**Aktivovať**)



Obrázok 4.43 Funkcia DMZ krok 1

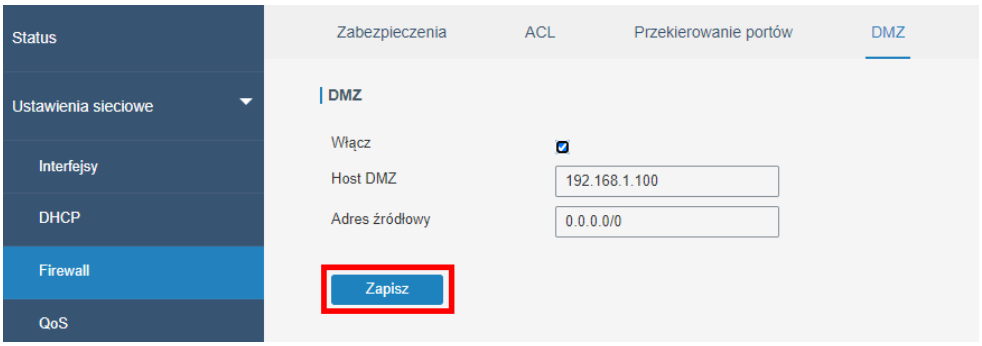
2. Zadajte:

– IP adresa zariadenia, na ktoré má byť presmerovaná prevádzka
– IP adresa zariadenia z externej siete, ktoré má mať prístup do DMZ (zadaním 0.0.0.0/0 akceptujeme všetky prichádzajúce adresy)



Obrázok 4.44 Funkcia DMZ krok 2

3. Po zadaní údajov kliknite na tlačidlo **Uložiť**

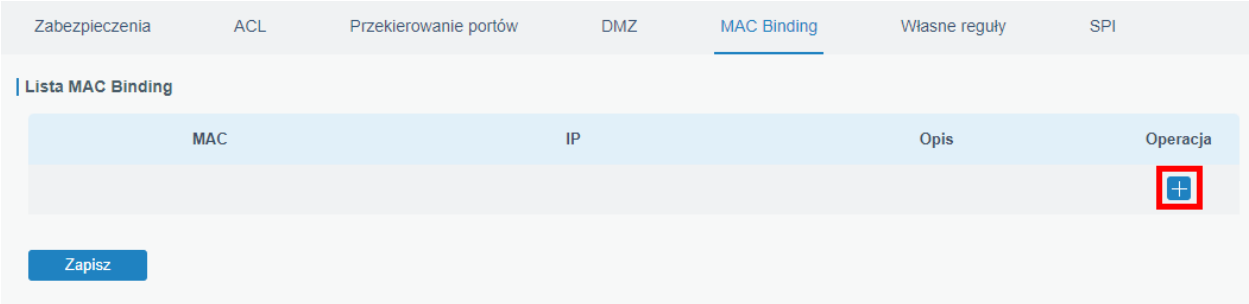


Obrázok 4.45 Funkcia DMZ krok 3

4.2.3.5 MAC Binding

Táto funkcia priraďuje prístup k sieti mimo routera konkrétnej skupine adries IP a MAC. Ak má nejaké zariadenie IP adresu zadanú v tomto zozname, ale jeho MAC adresa sa líši od adresy priradenej vyššie uvedenej IP adrese, takéto zariadenie nebude mať prístup k sieti mimo routera. Ak chcete pridať takéto filtrovanie, mali by ste urobiť nasledovné kroky:

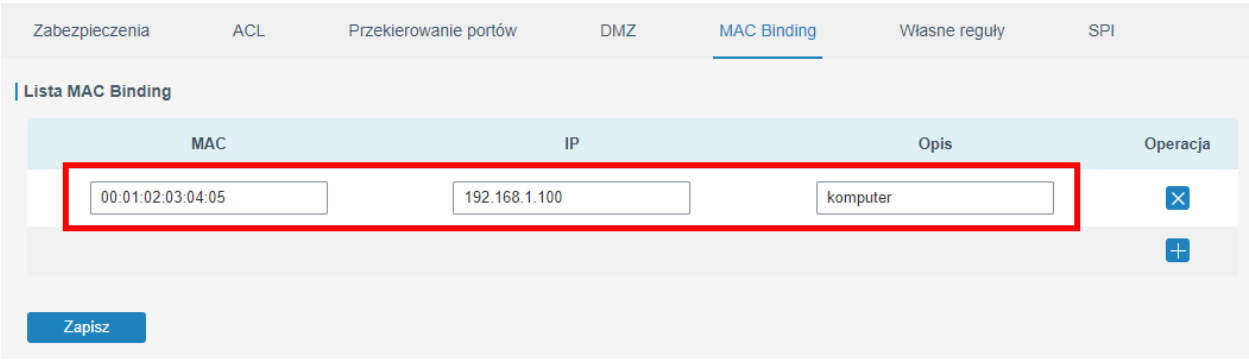
1. Kliknite na + v stĺpci **Operácia**



Obrázok 4.46 Pridajte položky do zoznamu MAC Binding krok 1

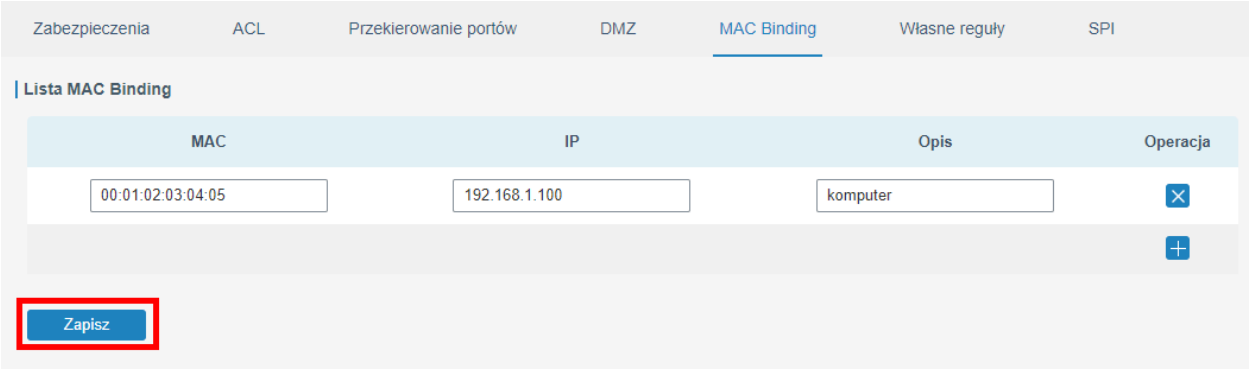
2. Zadajte:

– MAC adresu zariadenia
– IP adresu priradenú tejto MAC adrese



Obrázok 4. Pridajte položky do zoznamu MAC Binding krok 2

3. Po zadaní údajov kliknite na tlačidlo **Uložiť**

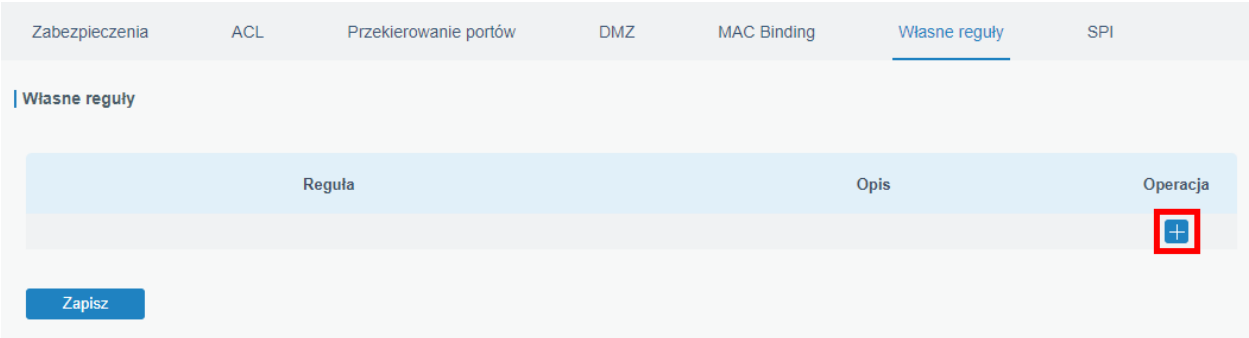


Obrázok 4.48 Pridajte položky do zoznamu MAC Binding krok 3

4.2.3.6 Vlastné pravidlá

V tejto záložke môžete použiť prispôsobené položky pravidiel firewall a iptables. Ak chcete pridať takéto pravidlo, mali by ste urobiť nasledujúce kroky:

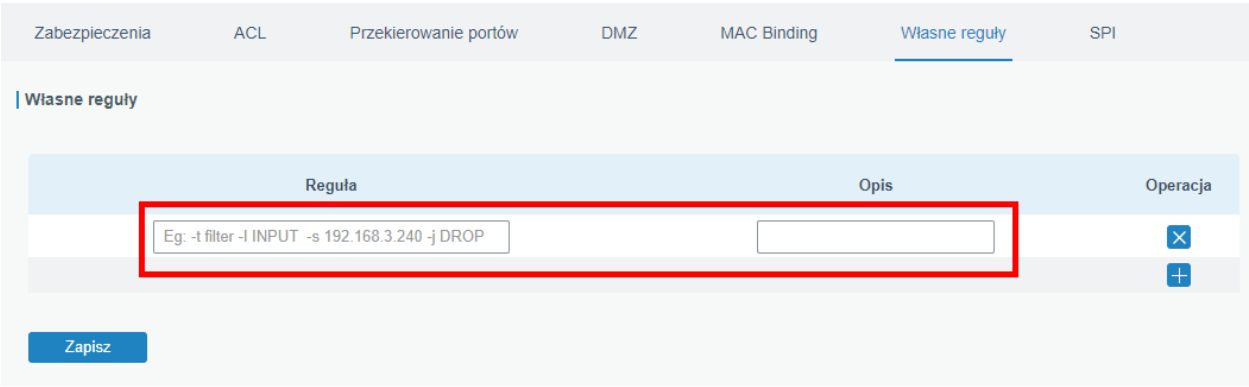
1. Kliknite na + v stĺpci **Operácia**



Obrázok 4.49 Pridanie vlastnej položky iptables krok 1

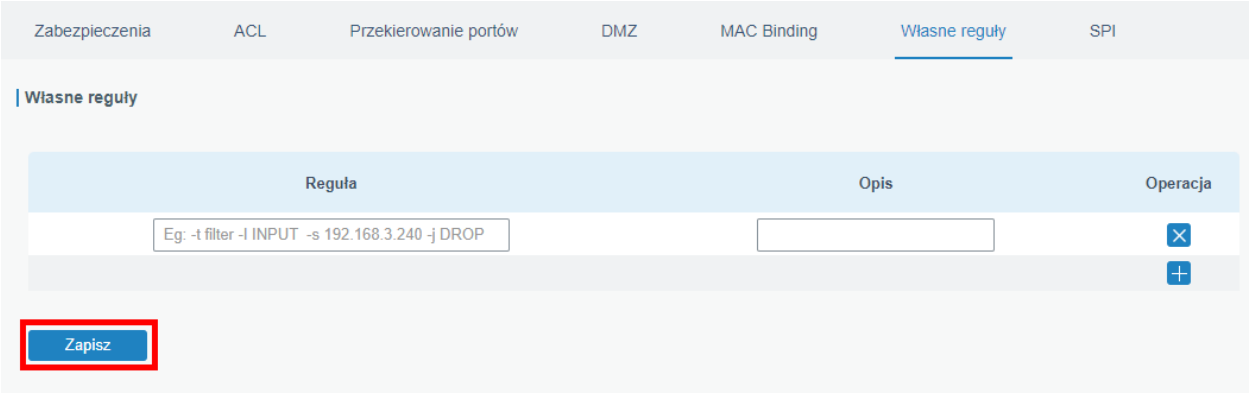
2. Zadajte:

– text pravidla
– popis pravidla



Obrázok 4.50 Pridanie vlastnej položky iptables krok 2

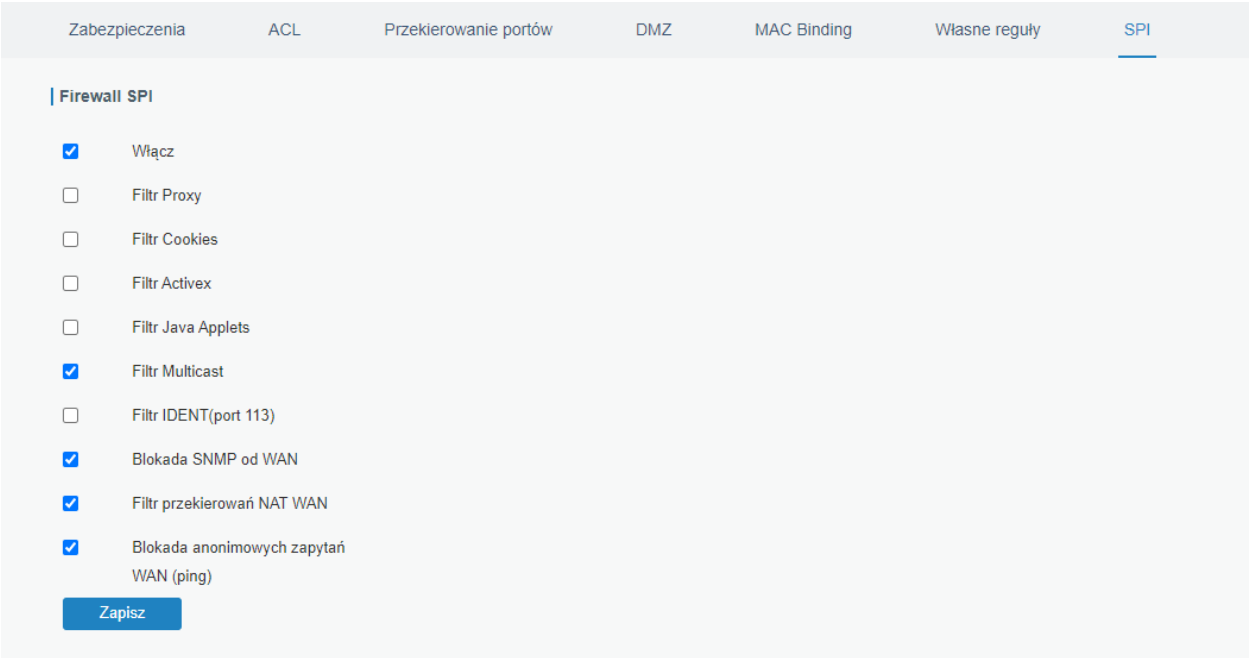
3. Po zadaní údajov kliknite na tlačidlo **Uložiť**



Obrázok 4.51 Pridanie vlastnej položky iptables krok 3

4.2.3.7 SPI

Táto záložka sa používa na povolenie a konfiguráciu služby SPI Firewall. V tabuľke nižšie je uvedený popis funkcií tejto záložky.



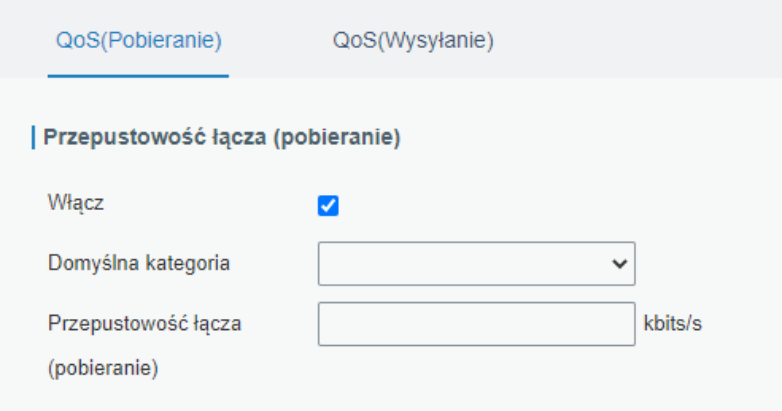
Obrázok 4.52 Konfigurácia SPI

Funkcia	Opis
Zapnúť	Povolí / zakáže funkciu brány firewall SPI
Filtr Proxy	Blokuje HTTP dotazy obsahujúce reťazec „Host”
FiltrCookies	Identifikuje požiadavky HTTP, ktoré obsahujú súbory cookie, a spracováva ich, aby zabránil útokom z ich vnútra v sieti
FiltrActivex	Blokuje požiadavky HTTP s príponou „.ocx“ alebo „.cab“ na konci adresy URL
Filtr Java Applets	Blokuje požiadavky HTTP s „.js“ alebo „.class“ na konci adresy URL
Filtr Multicast	Zabraňuje multicast paketom vstúpiť do LAN
Filtr IDENT (port 113)	Blokuje prístup k portu 113 zo strany WAN
Blokovanie SNMP od WAN	Blokuje požiadavky SNMP zo strany WAN
Filter presmerovania NAT WAN	Zabraňuje hostiteľom v sieti LAN používať adresu WAN smerovača na pripojenie k serverom v sieti LAN
Blokovanie anonymných požiadaviek WAN (ping)	Blokuje odpovede smerovača na požiadavky „ping“ prichádzajúce zo strany WAN

4.2.4 QoS

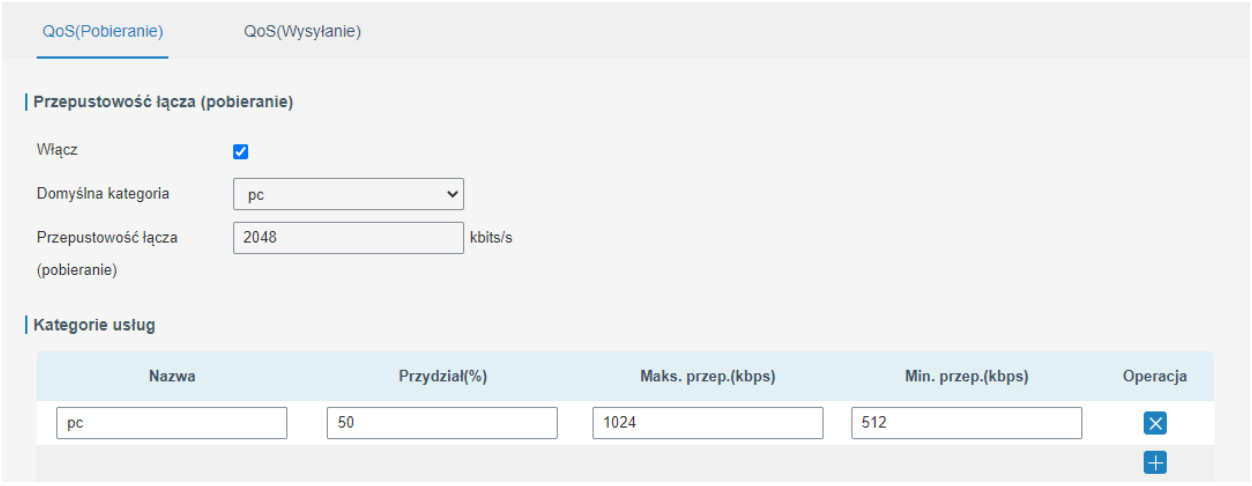
Funkcia Quality of Service (QoS) sa používa na riadenie šírky pásma pridelenej konkrétnej službe v sieti. Ak sa v našej sieti nachádzajú služby, ktoré na správne fungovanie vyžadujú špecifickú rýchlosť prenosu dát, táto funkcia zabezpečí ich správne fungovanie a taktiež viete obmedziť sieťovú prevádzku pre konkrétne služby tak, aby ich prevádzka neovplyvňovala chod celej siete. Pri konfigurácii služby QoS nezabúdajte, že v prípade konfigurácie v záložke **QoS (Download)** sú cieľovými zariadeniami zariadenia umiestnené v lokálnej sieti (**Cieľová IP adresa / Port**) a v prípade záložky QoS (**Odoslať**) , sú to zdrojové zariadenia (**Zdrojová IP adresa / Port**). Konfiguráciu tejto funkcie ukážem na príklade siete, v ktorej máme server s IP 192.168.1.100, ktorému pridelíme 50 % šírky pásma a pre zvyšné počítače bude k dispozícii ďalších 50 % šírky pásma. Konfigurácia je podobná pre kartu QoS (**Download**) a QoS (**Upload**), takže príklad nižšie bude vysvetlený na základe karty QoS (**Download**). Aby ste to urobili, postupujte nasledovne:

1. Spustite funkciu (**Enabled**)



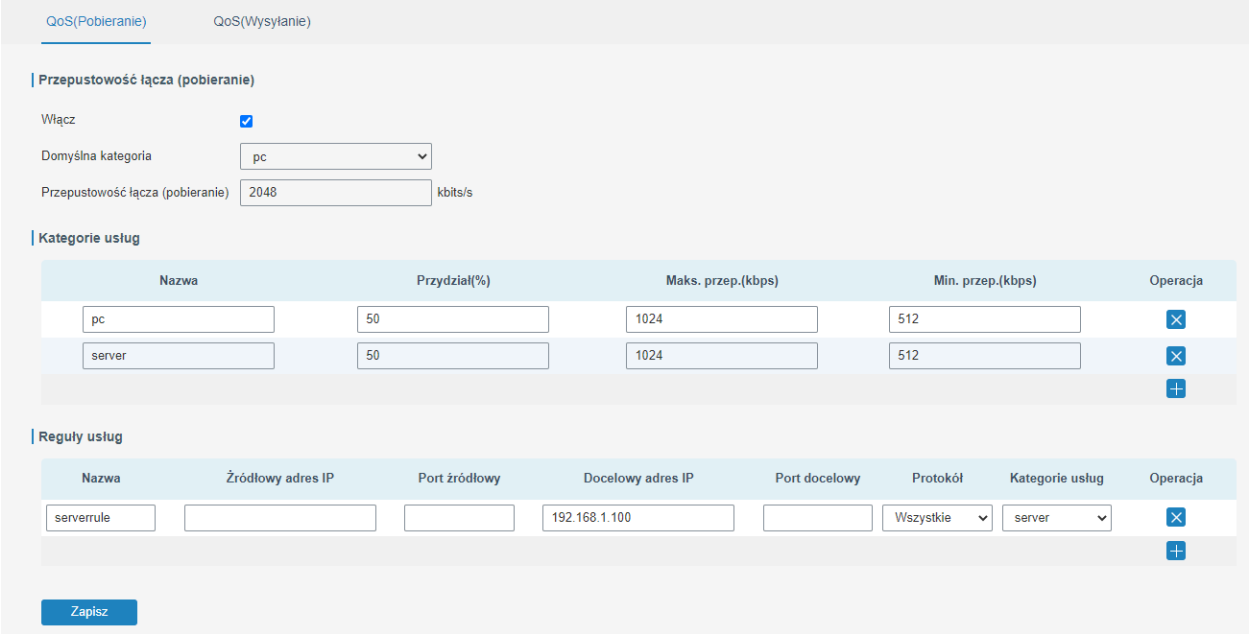
Obrázok 4.53 Funkcia QoS krok 1

2. Nastavte rýchlosť prepojenia (**Priepustnosť prepojenia (Sťahovanie) / Priepustnosť prepojenia (Odovzdávanie**)). V tomto príklade budeme predpokladať, že máme odkaz s kapacitou 2048 Kb/s sťahovanie a nahrávanie
3. Predvolenú kategóriu zariadenia pridáte stlačením ⊞ v stĺpci **Operácia** v skupine **Kategórie služieb**. V tomto prípade dostal názov „pc“ a bude podporovať všetky počítače okrem servera, takže ho musíme nastaviť ako predvolenú kategóriu pre zariadenia, ktorým nebudú priradené špeciálne pravidlá (**predvolená kategória**)



Obrázok 4.54 Funkcia QoS kroky 2 a 3

4. Pridajte ďalšiu kategóriu kategórie s názvom „server“ s nastaveniami ako „pc“, ktorá bude slúžiť serveru
5. Pridajte špeciálne pravidlo pre server s názvom „serverrule”. V tomto príklade má byť všetka sieťová prevádzka zo/na server poskytovaná so šírkou pásma, takže vyplníte iba: **cieľovú IP adresu** v prípade karty **QoS (sťahovanie)** a v prípade karty **QoS (odosielanie)**, vyplníte **zdrojovú IP adresu.**



Obrázok 4.55 Funkcia QoS kroky 4 a 5

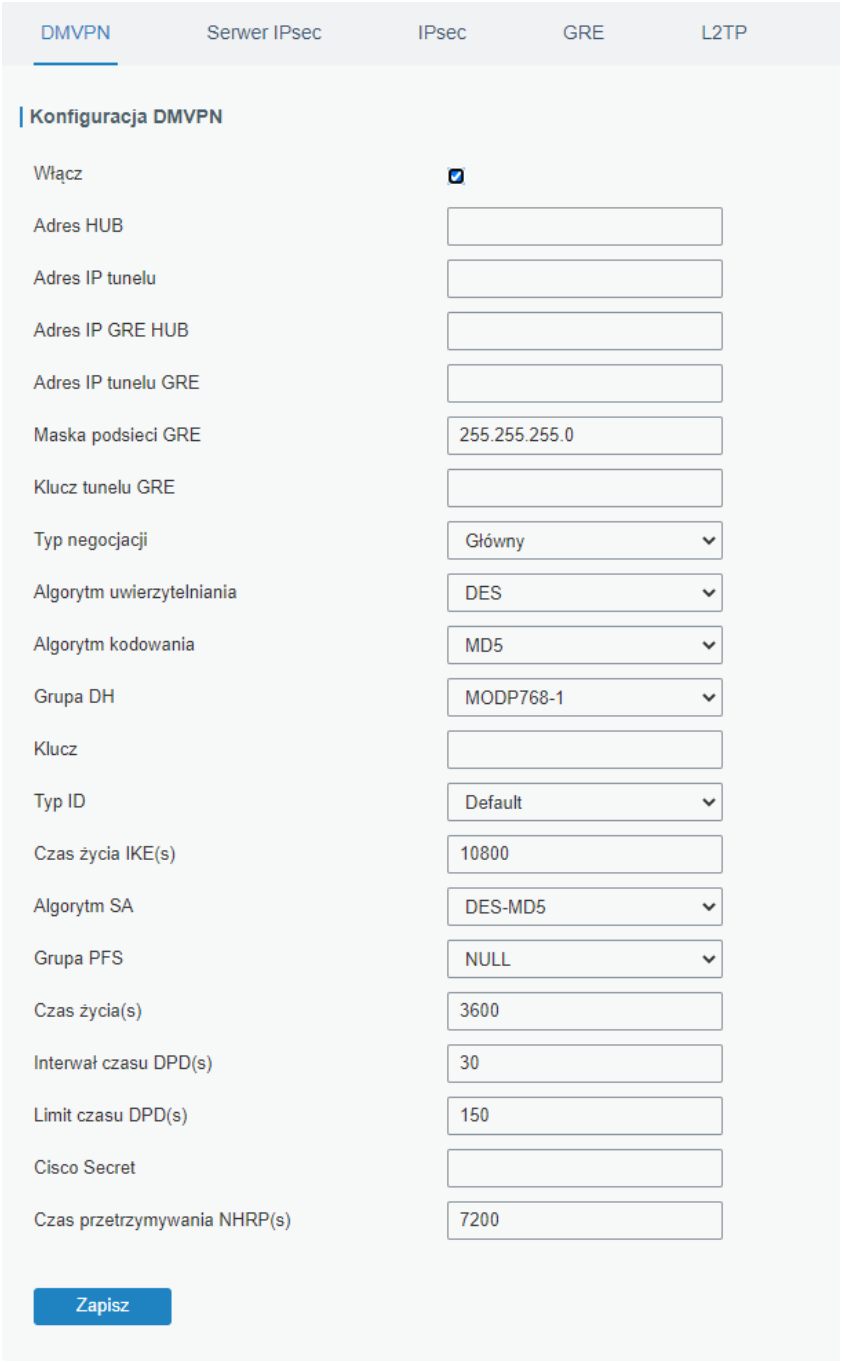
Skupina nastavení	Pole	Opis
Šírka pásma prepojenia (downstream) / šírka pásma prepojenia (upstream)	Zapnúť	Aktivuje / deaktivuje funkciu
	Predvolená kategória	Predvolená kategória obmedzení, ktorá sa použije, keď nie sú priradené žiadne pravidlá
	Šírka pásma prepojenia (sťahovanie) / Šírka pásma prepojenia (uplink)	Rýchlosť sťahovania / nahrávania internetového pripojenia
Kategórie služieb	Názov	Meno kategórie
	Pridelenie(%)	Percentuálne pridelenie odkazu, keď súčet Max. je väčšia ako šírka pásma (sťahovanie) / šírka pásma (nahrávanie), súčet pre všetky položky nemôže prekročiť 100 %
	Prietok (kbps)	Maximálna pridelená šírka pásma v kbps
	Min. prietok (kbps)	Minimálna pridelená šírka pásma v kbps
	Prevádzka	Pridáva / odstraňuje položky
Servisné pravidlá	Názov	Názov pravidla
	Zdrojová IP adresa	IP zdrojového zariadenia; pre záložku QoS (sťahovanie) sú to zariadenia mimo lokálnej siete, pre záložku QoS (odosielanie) sú to zariadenia v lokálnej sieti. Ak toto pole ponecháte prázdne, pravidlo bude platiť pre všetky zariadenia.
	Zdrojový port	Port, na ktorom sa zdrojové zariadenie pokúša komunikovať. Ak toto pole ponecháte prázdne, pravidlo bude platiť pre všetky porty.
	Cieľová IP adresa	IP cieľového zariadenia; pre záložku QoS (sťahovanie) sú to zariadenia v lokálnej sieti, pre záložku QoS (odosielanie) sú to zariadenia mimo lokálnej siete. Ak toto pole ponecháte prázdne, pravidlo bude platiť pre všetky zariadenia.
	Cieľový port	Port, na ktorom sa cieľové zariadenie pokúša komunikovať. Ak toto pole ponecháte prázdne, pravidlo bude platiť pre všetky porty.
	Protokol	Protokol, pre ktorý pravidlo platí (ANY - all, TCP, UDP, ICMP, GRE)
	Kategória služby	Kategória obmedzení, ktoré sa budú vzťahovať na dané pravidlo
	Prevádzka	Pridáva / odstraňuje položky

4.2.5 VPN

VPN (Virtual PrivateNetworsk) je služba, ktorá umožňuje bezpečne prepojiť dve privátne siete, vďaka čomu budú môcť zariadenia v jednej sieti komunikovať so zariadeniami v inej sieti cez zabezpečené komunikačné tunely. Smerovač BCS-R4G-1W1L podporuje DMVPN, IPsec, GRE, L2TP, PPTP, OpenVPN. Okrem toho môžeme router nakonfigurovať ako server pre IPsec a OpenVPN.

4.2.5.1 DMVPN

Dynamická viacbodová virtuálna privátna sieť (DMVPN), ktorá spája mGRE a IPsec, je zabezpečená sieť, ktorá si vymieňa údaje medzi lokalitami bez odosielania prevádzky cez server VPN alebo router v priestoroch organizácie.

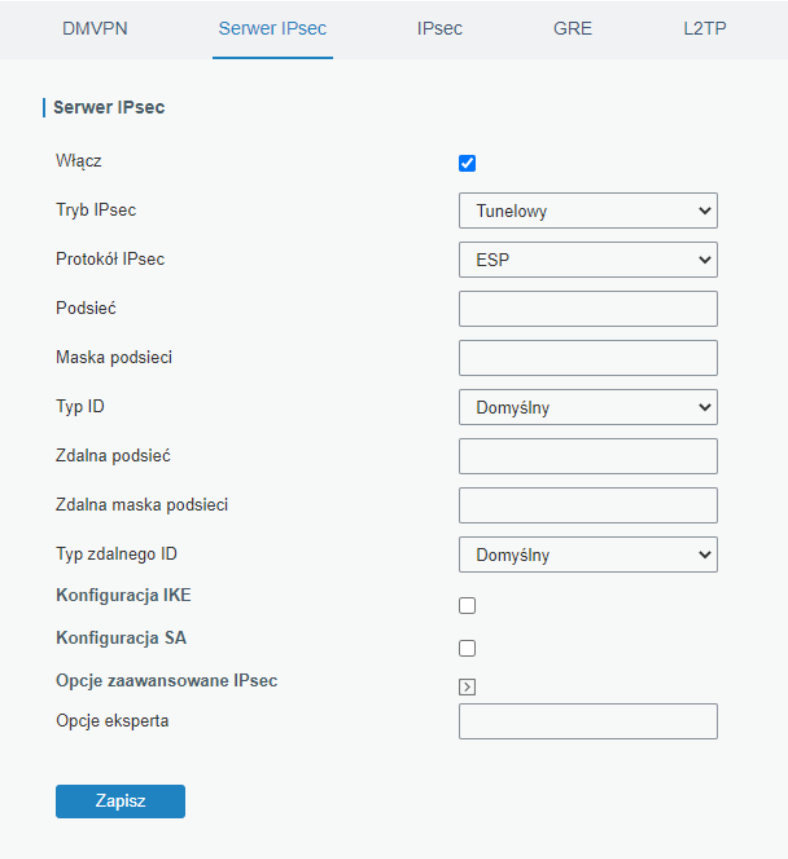


Obrázok 4.56 Konfigurácia služby DMVPN

Pole	Opis
Zapnúť	Povolí / zakáže službu DMVPN
Adresa HUB	IP adresa alebo doména rozbočovača DMVPN
IP adresa tunela	Lokálna adresa tunela DMVPN
IP adresa GRE HUB	IP adresa uzla GRE tunela
IP adresa tunela GRE	Lokálna adresa tunela GRE
Maska podsiete GRE	Maska lokálnej podsiete tunela GRE
Kľúč tunela GRE	Kľúč tunela GRE
Typ vyjednávania	Režim vyjednávania o pripojení
Algoritmus autentifikácie	Algoritmus autentifikácie
Kódovací algoritmus	Šifrovací algoritmus
DH skupina	Určuje skupinu DH (sila šifrovacieho kľúča), čím vyššie číslo, tým bezpečnejšie pripojenie, ale výpočet trvá dlhšie
Kľúč	Kľúčový obsah
Typ ID	Miestny typ ID, ak vyberiete iný ako „predvolený“, musíte zadať ID
Životnosť IKE (y)	Životnosť vyjednávania IKE, rozsah 60-86400 sekúnd
SA algoritmus	Výber SA algoritmu
Skupina PFS	Určuje skupinu PFS (sila šifrovacieho kľúča), čím vyššie číslo, tým je pripojenie bezpečnejšie, ale výpočet trvá dlhšie
Životnosť (s)	Životnosť IPsec SA, rozsah 60-86400
DPD časový interval (s)	DPD časový interval
Časový limit DPD (s)	Časový limit DPD
Cisco Secret	Kľúč Cisco nhrp
Čas držania NHRP (s)	Trvanie zadržania NHRP

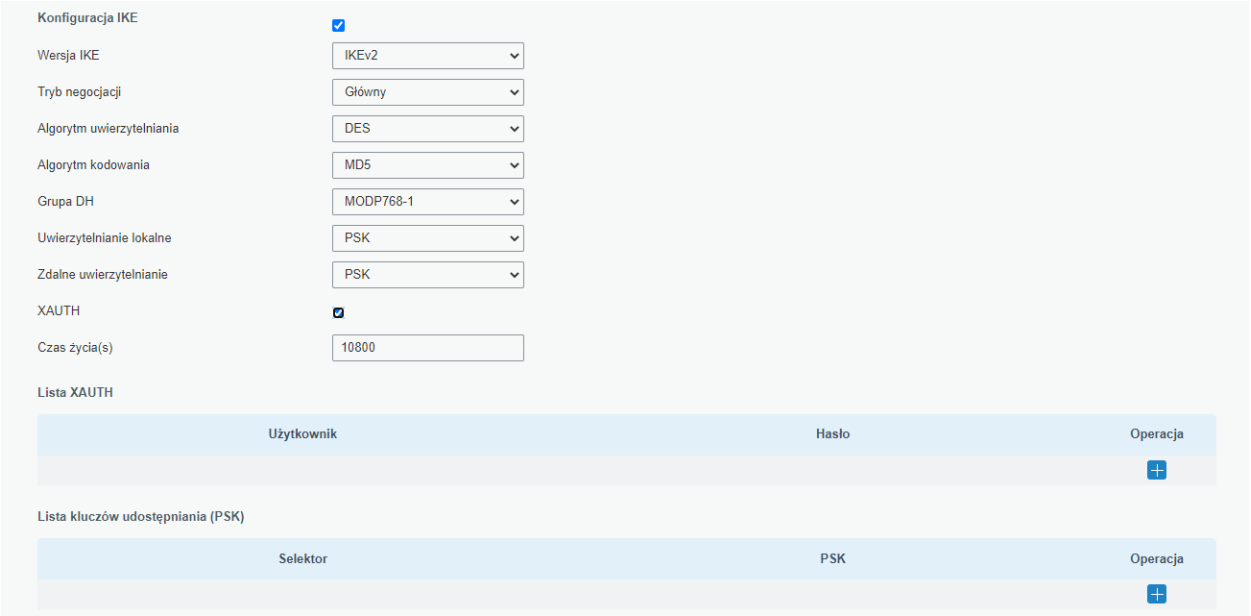
4.2.5.2 IPsec Server

IPsec je obzvlášť užitočný na nasadenie virtuálnych privátnych sietí a vzdialeného prístupu používateľov cez vytáčané súkromné siete. Veľkou výhodou IPsec je, že bezpečnosť je možné zvládnuť bez toho, aby ste museli vykonávať zmeny na jednotlivých používateľských počítačoch. IPsec poskytuje tri možnosti bezpečnostných služieb: Authentication Header (AH), EncapsulatingSecurityPayload (ESP) a Internet Key Exchange (IKE). AH v podstate umožňuje autentifikáciu údajov týchto subjektov. ESP podporuje autentifikáciu odosielateľa aj šifrovanie údajov. IKE sa používa na výmenu šifrovacích kódov. Všetky môžu chrániť jeden alebo viacero dátových tokov medzi hostiteľmi, medzi hostiteľom a bránou a medzi bránami.

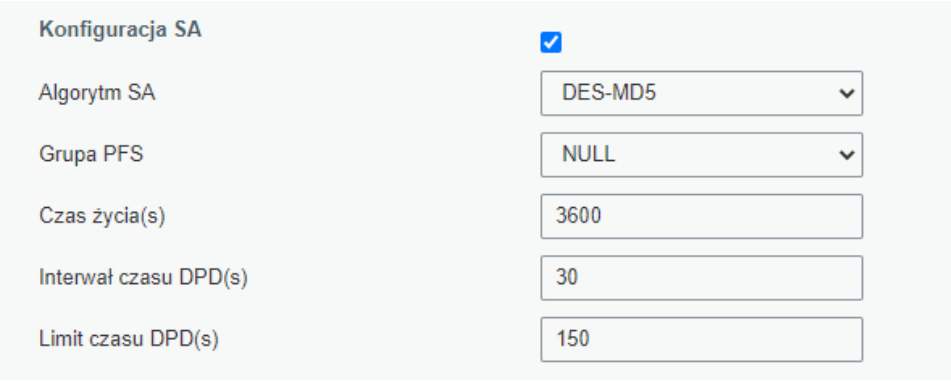


Obrázok 4.57 Konfigurácia služby serwerIPsec

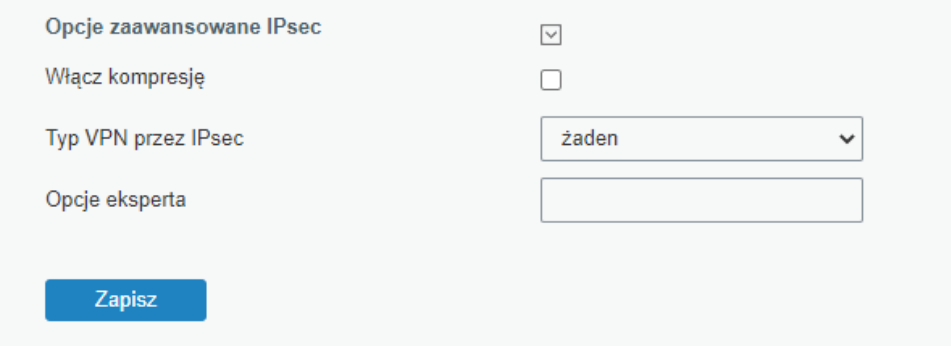
Pole	Opis
Zapnúť	Povolí / zakáže funkciu servera IPsec
Režim IPsec	Servisný režim prevádzky
Protokol IPsec	Výber protokolu
Podsieť	Adresa lokálnej podsiete, ktorú IPsec chráni
Maska podsiete	Maska vyššie uvedenej podsiete
Typ ID	Miestny typ ID, ak vyberiete iný ako „predvolený“, musíte zadať ID
Vzdialená podsieť	Vzdialená podsieť, ktorá je chránená protokolom IPsec
Maska vzdialenej podsiete	Maska vyššie uvedenej podsiete
Typ vzdialeného ID	Vzdialený typ ID, ak vyberiete iný ako „predvolený“, musíte zadať ID



Obrázok 4.58 Konfigurácia servera IPsec parametrov IKE



Obrázok 4.59 Konfigurácia servera IPsec parametrov SA

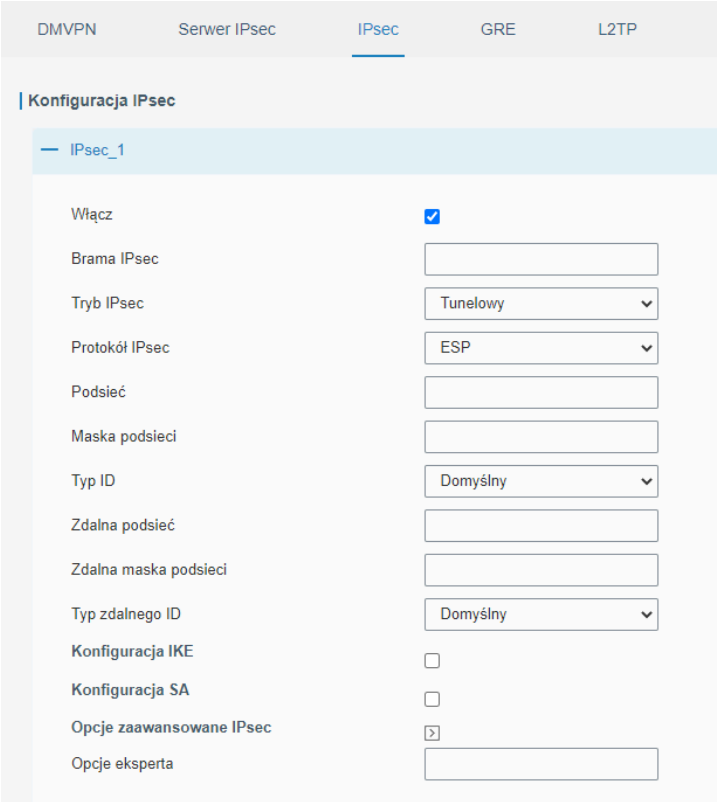


Obrázok 4.60 Konfigurácia servera IPsec pokročilé parametre

Pole	Opis
Konfigurácia IKE	
IKE verzia	Verzia protokolu IKE
Režim vyjednávania	Režim vyjednávania o pripojení
Algoritmus autentifikácie	Výber autentifikačného algoritmu
Kódovací algoritmus	Výber šifrovacieho kľúča
DH skupina	Určuje skupinu DH (sila šifrovacieho kľúča), čím vyššie číslo, tým bezpečnejšie pripojenie, ale výpočet trvá dlhšie
Miestna autentifikácia	Výber miestneho overenia
XAUTH	Povolí / zakáže overenie XAUTH
Životnosť (s)	Životnosť vyjednávania IKE, rozsah 60-86400
Zoznam XAUTH	
Používateľské meno	Používateľské meno na overenie
Heslo	Heslo na overenie
Prevádzka	Pridáva / odstraňuje položky
Zoznam PSK	
Selektor	Poznám PSK
PSK	Identifikačné číslo PSK
Prevádzka	Prístupový kľúč
Konfigurácia SA	
SA algoritmus	Výber SA algoritmu
Skupina PFS	Určuje skupinu PFS (sila šifrovacieho kľúča), čím vyššie číslo, tým je pripojenie bezpečnejšie, ale výpočet trvá dlhšie
Životnosť (s)	SA Negotiation Lifetime, rozsah 60-86400
DPD časový interval (s)	DPD časový interval
Časový limit DPD (s)	Časový limit DPD
Pokročilé nastavenia IPsec	
Povoliť kompresiu	Umožňuje kompresiu hlavičiek paketov IP
Typ VPN cez IPsec	Vyberte protokol, na ktorom chcete spustiť IPsec
Odborné možnosti	Pole sa používa na manuálne pridanie nasledujúcich položiek do protokolu IPsec, pričom každá položka by mala byť oddelená znakom „;“

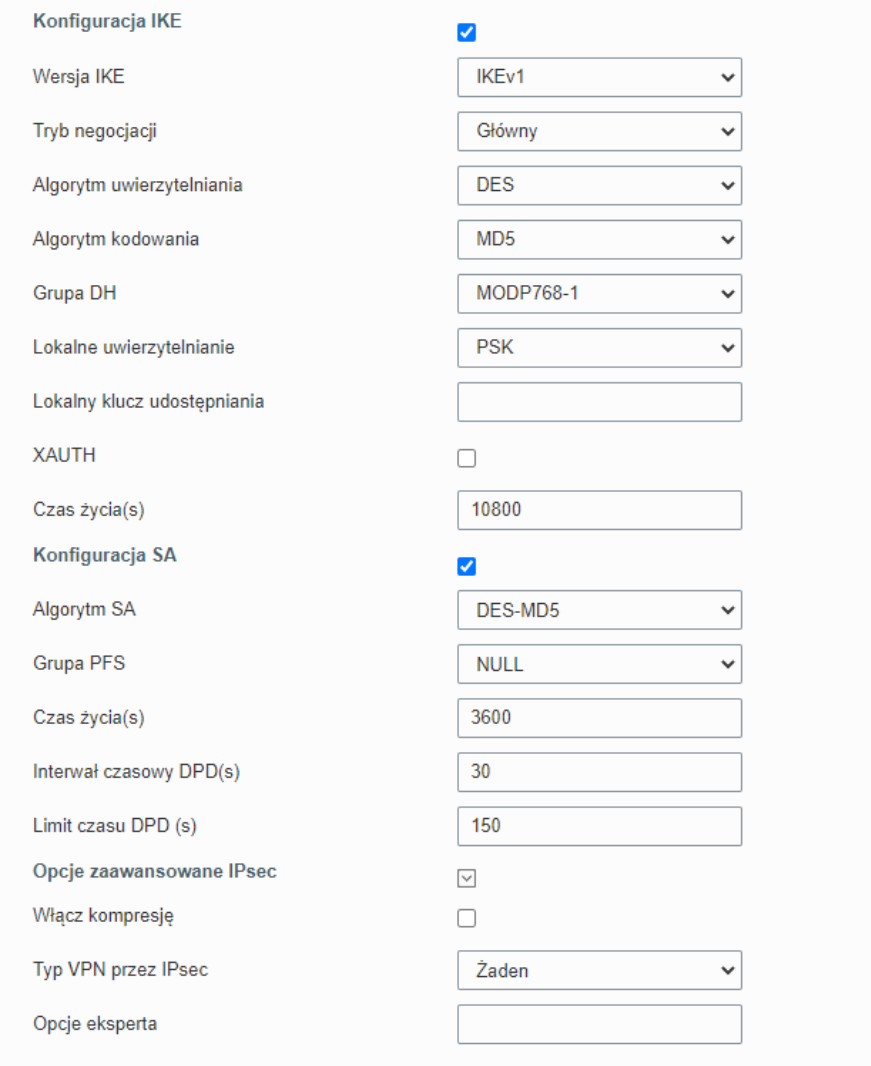
4.2.5.3 IPsec

V tejto záložke môžete nakonfigurovať pripojenie IPsec, v ktorom je router klientom. Môžete nakonfigurovať až 3 pripojenia klientov.



Obrázok 4.61 Konfigurácia služby IPsec

Pole	Opis
Zapnúť	Povolí / zakáže funkciu, môžete nakonfigurovať až 3 tunely IPsec
Režim IPsec	Servisný režim prevádzky
Protokol IPsec	Výber protokolu
Podsieť	Adresa lokálnej podsiete, ktorú IPsec chráni
Masku podsiete	Maska vyššie uvedenej podsiete
Typ ID	Miestny typ ID, ak vyberiete iný ako „predvolený“, musíte zadať ID
Vzdialená podsieť	Vzdialená podsieť, ktorá je chránená protokolom IPsec
Maska vzdialenej podsiete	Maska vyššie uvedenej podsiete
Typ vzdialeného ID	Vzdialený typ ID, ak vyberiete iný ako „predvolený“, musíte zadať ID



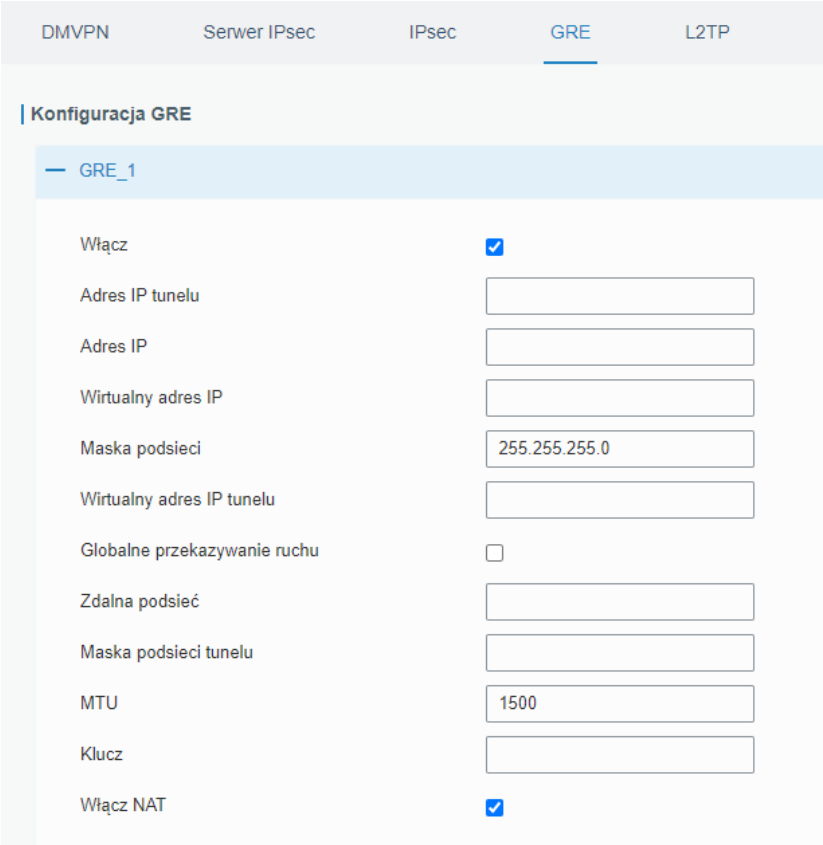
Obrázok 4.62 Konfigurácia služby IPsec, konfigurácia IKE, SA

Pole	Opis
Konfigurácia IKE	
IKE verzia	Verzia protokolu IKE
Režim vyjednávania	Režim vyjednávania o pripojení
Algoritmus autentifikácie	Výber kódovacieho algoritmu
Kódovací algoritmus	Výber šifrovacieho kľúča
DH skupina	Určuje skupinu DH (sila šifrovacieho kľúča), čím vyššie číslo, ým bezpečnejšie pripojenie, ale výpočet trvá dlhšie
Miestna autentifikácia	Výber miestneho overenia
XAUTH	Šifrovací kľúč
Životnosť (s)	Povolí / zakáže overenie XAUTH
Algoritmus autentifikácie	Životnosť vyjednávania IKE, rozsah 60-86400
Zoznam XAUTH	
Používateľské meno	Používateľské meno na overenie
Heslo	Heslo na overenie
Prevádzka	Pridáva / odstraňuje položky
Zoznam PSK	
Selektor	Identifikačné číslo PSK
PSK	Prístupový kľúč
Prevádzka	Pridáva / odstraňuje položky
Konfigurácia SA	
SA algoritmus	Výber SA algoritmu
Skupina PFS	Určuje skupinu PFS (sila šifrovacieho kľúča), čím vyššie číslo, tým je pripojenie bezpečnejšie, ale výpočet trvá dlhšie
Životnosť (s)	SA Negotiation Lifetime, rozsah 60-86400
DPD časový interval (s)	DPD časový interval
Časový limit DPD (s)	Časový limit DPD
Pokročilé nastavenia IPsec	
Povoliť kompresiu	Umožňuje kompresiu hlavičiek paketov IP
Typ VPN cez IPsec	Vyberte protokol, na ktorom chcete spustiť IPsec
Odborné možnosti	Pole sa používa na manuálne pridanie nasledujúcich položiek do protokolu IPsec, pričom každá položka by mala byť oddelená znakom „;“

4.2.5.4 GRE

Generic Routing Encapsulation (GRE) je protokol, ktorý zapuzdruje pakety na smerovanie iných protokolov cez siete IP. Ide o technológiu tunelovania, ktorá poskytuje kanál, cez ktorý možno prenášať zapuzdrenú dátovú správu a zapuzdrenie a dekapsuláciu možno vykonávať na oboch koncoch. Tunelový prenos GRE sa môže použiť za nasledujúcich okolností:

- Tunel GRE môže prenášať dátové pakety multicast, ako keby to bolo skutočné sieťové rozhranie. SingleuseofIPSec neposkytuje multicastové šifrovanie.
- Zadaný akceptovaný protokol nie je možné smerovať.
- Na prepojenie dvoch ďalších podobných sietí je potrebná sieť s rôznymi adresami IP.

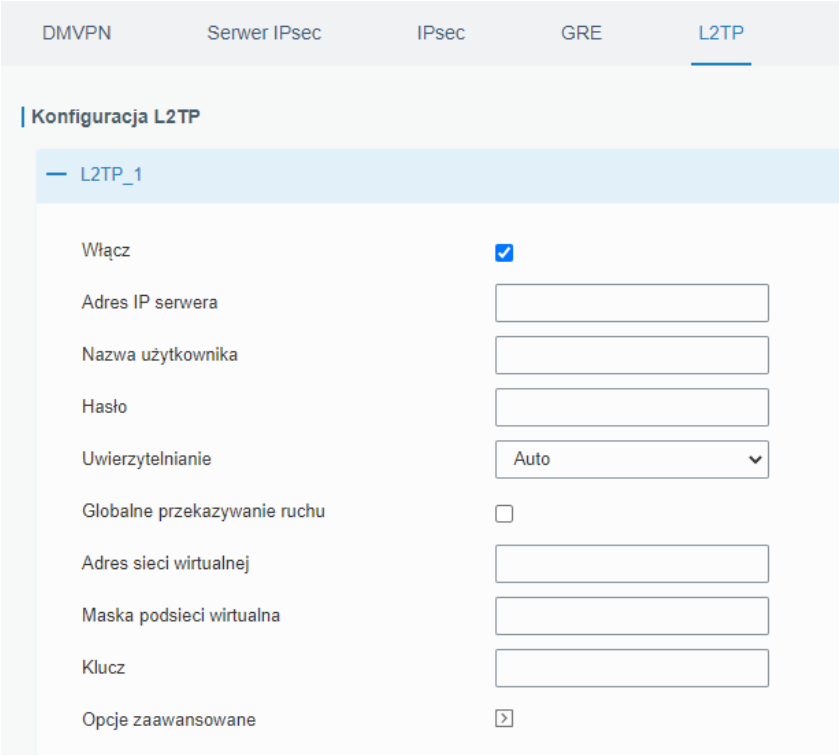


Obrázok 4.63 Konfigurácia služby GRE

Pole	Opis
Zapnúť	Povolí / zakáže službu
IP adresa tunela	Vzdialená IP adresa
IP adresa	IP adresa
Virtuálna IP adresa	IP adresa zariadenia uvedená v tuneli GRE
Masku podsiete	Masku podsiete
Virtuálna IP adresa tunela	IP adresa vzdialeného tunela GRE
Global Traffic Relay	Ak povolíte túto funkciu, všetka sieťová prevádzka sa bude posielať cez tunel GRE
Vzdialená podsieť	Adresa IP siete pre tunel GRE
Maska podsiete tunela	Maska podsiete pre tunel GRE
MTU	Maximálna veľkosť rámu
Kľúč	Šifrovací kľúč pre tunel GRE
Povoliť NAT	Povolí / zakáže NAT

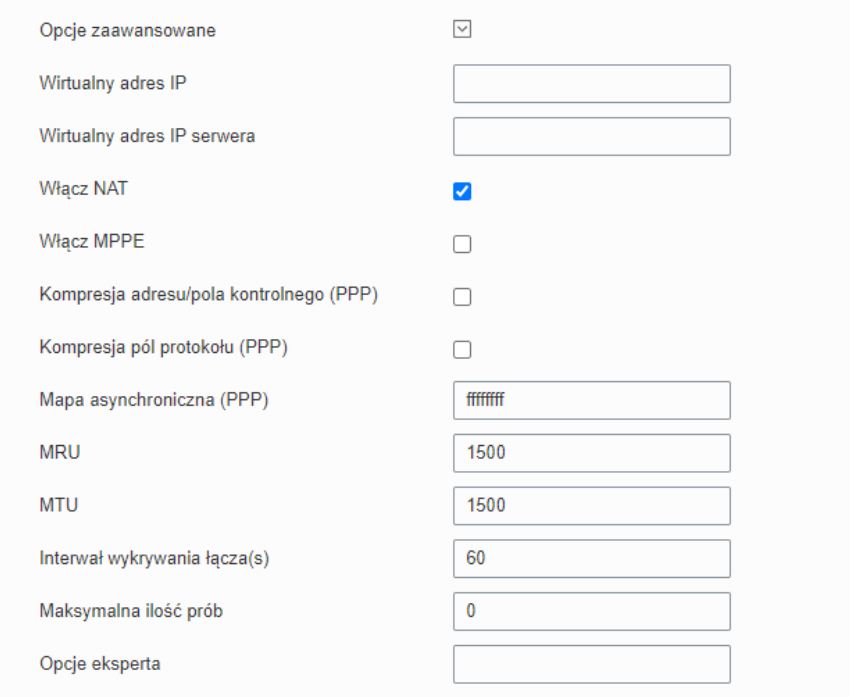
4.2.5.5 L2TP

LayerTwoTunnelingProtocol (L2TP) je rozšírenie Point-to-Point TunnelingProtocol (PPTP), ktoré používajú poskytovatelia internetových služieb (ISP) na vytváranie virtuálnych miestnych sietí (VPN) na internete.



Obrázok 4.64 Konfigurácie služby L2TP

Pole	Opis
Zapnúť	Povolí / zakáže službu
IP adresa servera	IP adresa / doména servera L2TP
Používateľské meno	Používateľské meno služby L2TP
Heslo	Heslo služby L2TP
Overenie	Výber režimu overenia
Global Traffic Relay	Ak povolíte túto funkciu, všetka sieťová prevádzka sa bude posielať cez tunel L2TP
Adresa virtuálnej siete	Adresa IP siete pre tunel L2TP
Maska virtuálnej podsiete	Maska podsiete pre tunel L2TP
Kľúč	Šifrovací kľúč tunela L2TP

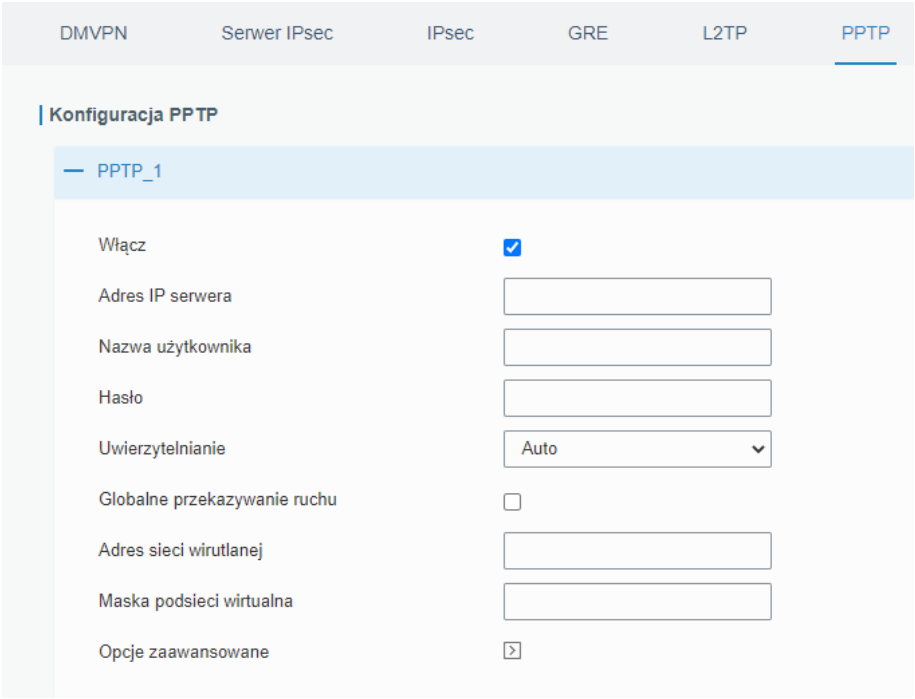


Obrázok 4.65 Konfigurácia služby L2TP, pokročilé nastavenia

Pole	Opis
Pokročilé nastavenia	Povolí / zakáže rozšírené možnosti
Virtuálna IP adresa	IP adresa klienta L2TP, ak je toto pole prázdne, adresa bude pridelená zo servera
Virtuálna IP adresa servera	IP adresa tunela L2TP
Povoliť NAT	Povolí / zakáže NAT
Povoliť MPPE	Povolí / zakáže šifrovanie MPPE
Kompresia adresy/riadiaceho poľa (PPP)	Potrebné pre inicializáciu PPP, môžete ponechať predvolenú hodnotu
Kompresia protokolového poľa (PPP)	Potrebné pre inicializáciu PPP, môžete ponechať predvolenú hodnotu
Asynchrónna mapa (PPP)	Jedna z hodnôt potrebných na inicializáciu PPP, môžete ponechať predvolenú hodnotu, rozsah 0-ffffffff
MRU	Maximálna veľkosť MRU
MTU	Maximálna veľkosť MTU
Interval detekcie spojenia (s)	Interval detekcie spojenia, rozsah 0-600
Maximálny počet pokusov	Maximálny počet pokusov o pripojenie cez L2TP, rozsah 0-10
Odborné možnosti	Pole sa používa na manuálne pridávanie nasledujúcich položiek do protokolu L2TP, pričom každá položka by mala byť oddelená znakom „;“

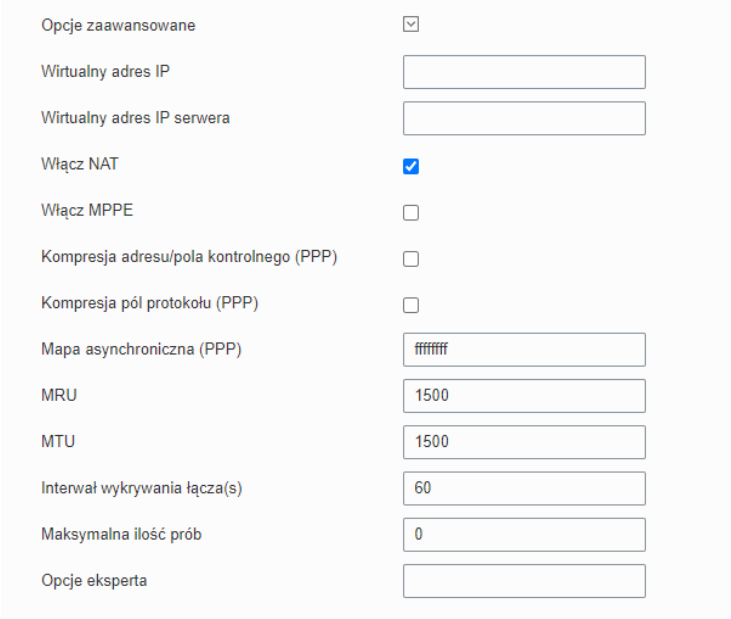
4.2.5.6 PPTP

Point-to-Point TunnelingProtocol (PPTP) je protokol, ktorý umožňuje korporáciám rozširovať ich vlastnú podnikovú sieť prostredníctvom súkromných „tunelov“ na verejnom internete. Výsledkom je, že spoločnosť využíva rozľahlú sieť ako jednu veľkú lokálnu sieť.



Obrázok 4.66 Konfigurácia služby PPTP

Pole	Opis
Zapnúť	Povolí / zakáže službu PPTP
IP adresa servera	IP adresa / doména PPTP servera
Používateľské meno	Používateľské meno pre službu PPTP
Heslo	Heslo pre službu PPTP
Overenie	Výber režimu overenia
Global Traffic Relay	Ak povolíte túto funkciu, všetka sieťová prevádzka sa bude posielať cez tunel PPTP
Adresa virtuálnej siete	Adresa IP siete pre tunel PPTP
Maska virtuálnej podsiete	Maska podsiete pre tunel PPTP



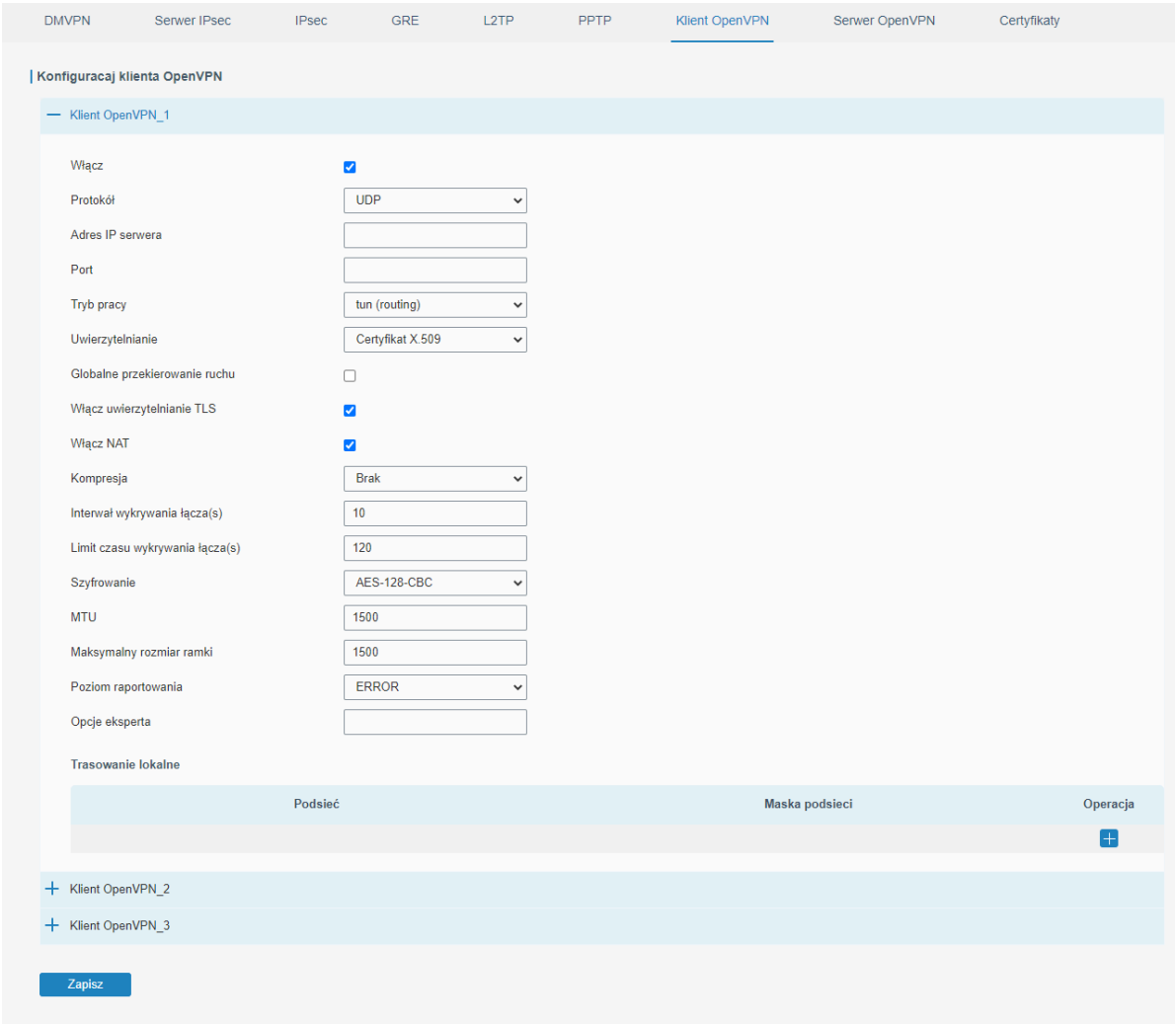
Obrázok 4.67 Konfigurácia služby PPTP, pokročilé nastavenia

Pole	Opis
Virtuálna IP adresa	IP adresa klienta PPTP
Virtuálna IP adresa servera	IP adresa tunela PPTP
Povoliť NAT	Povolí / zakáže NAT
Povoliť MPPE	Povolí / zakáže šifrovanie MPPE
Kompresia adresy/riadiaceho poľa (PPP)	Potrebné pre inicializáciu PPP, môžete ponechať predvolenú hodnotu
Kompresia protokolového poľa (PPP)	Potrebné pre inicializáciu PPP, môžete ponechať predvolenú hodnotu
Asynchrónna mapa (PPP)	Jedna z hodnôt potrebných na inicializáciu PPP, môžete ponechať predvolenú hodnotu, rozsah 0-ffffffff
MRU	Maximálna veľkosť MRU
MTU	Maximálna veľkosť MTU
Interval detekcie spojenia (s)	Interval detekcie spojenia, rozsah 0-600
Maximálny počet pokusov	Maximálny počet pokusov o pripojenie PPTP, rozsah 0-10
Odborné možnosti	Pole sa používa na manuálne pridávanie nasledujúcich položiek do protokolu PPTP, pričom každá položka by mala byť oddelená znakom „;”

4.2.5.7 Klient OpenVPN

OpenVPN je open source protokol virtuálnej súkromnej siete (VPN), ktorý ponúka zjednodušený bezpečnostný rámec, modulárny dizajn siete a multiplatformu.
Medzi výhody OpenVPN patrí:

- bezpečnostné opatrenia, ktoré fungujú proti aktívnym aj pasívnym útokom,
- kompatibilita so všetkými hlavnými operačnými systémami,
- vysoká rýchlosť (zvyčajne 1,4 MB za sekundu),
- možnosť konfigurovať viacero serverov na spracovanie viacerých pripojení súčasne,
- všetky funkcie šifrovania a autentifikácie knižnice OpenSSL,
- pokročilé riadenie šírky pásma,
- rôzne možnosti tunelovania,
- kompatibilné s čipovými kartami, ktoré podporujú Windows Crypt API.

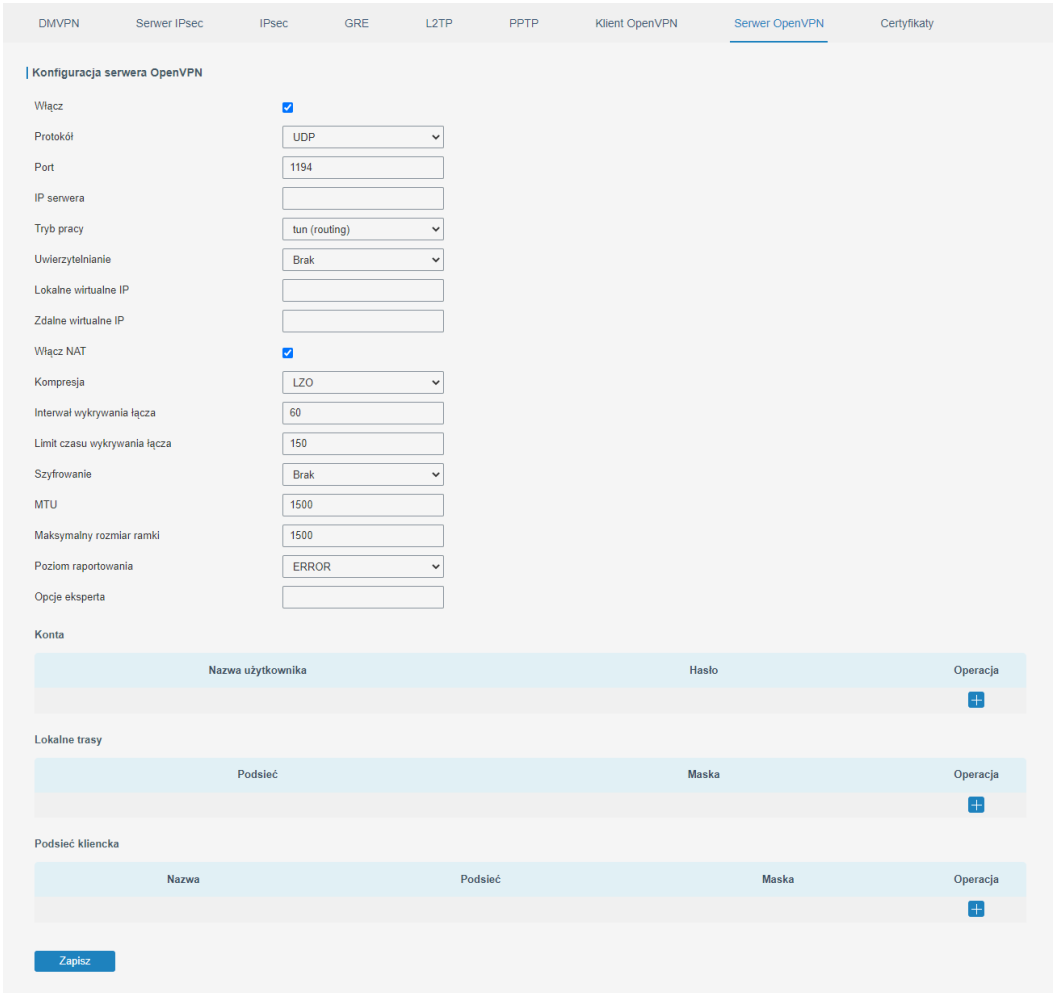


Obrázok 4.68 Konfigurácia služby klienta OpenVPN

Pole	Opis
Zapnúť	Povolí / zakáže klientsku službu OpenVPN, súčasne je možné spustiť maximálne 3 služby
Protokol	Vyberať protokol používaný pre pripojenie UDP / TCP
IP adresa servera	IP adresa / doména servera OpenVPN
Prístav	Port, na ktorom počúva server OpenVPN
Rozhranie	Vyber rozhrania používaného na pripojenie
Overenie	Výber spôsobu overovania
Virtuálna IP adresa	Virtuálna IP adresa klienta
Virtuálna adresa servera	Virtuálna IP adresa servera
Globálne presmerovanie dopravy	Keď je táto funkcia povolená, všetka sieťová prevádzka sa bude posielať cez tunel OpenVPN
Povoliť overenie TLS	Povoliť / zakázať overenie TLS
Používateľské meno	Používateľské meno pre službu OpenVPN
Heslo	Heslo OpenVPN
Povoliť NAT	Povolí / zakáže NAT
Kompresia	Povolí (VOC) / Zakáže kompresiu údajov
Interval detekcie spojenia (s)	Interval detekcie spojenia, rozsah 10-1800
Časový limit na nájdenie odkazu (s)	Časový limit na nájdenie odkazu, po uplynutí tohto časového limitu sa zariadenie pokúsi znova objaviť odkaz
Šifrovanie	Výber typu šifrovania
MTU	Maximálna veľkosť MTU
Maximálna veľkosť rámu	Maximálna veľkosť rámu
Úroveň podávania správ	Úroveň podrobností pre denníky služieb
Odborné možnosti	Pole sa používa na manuálne pridávanie ďalších položiek do protokolu OpenVPN, pričom každá položka by mala byť oddelená znakom „;“
Lokálne trasovanie	
Podsieť	Adresa lokálnej siete OpenVPN
Masku podsiete	Maska podsiete OpenVPN
Prevádzka	Pridáva / odstraňuje položky

4.2.5.8 Server OpenVPN

Router BCS-R4G-1W1L podporuje službu servera OpenVPN, takže môžeme vytvoriť bezpečné pripojenie typu point-to-point alebo sieť-to-sieť.

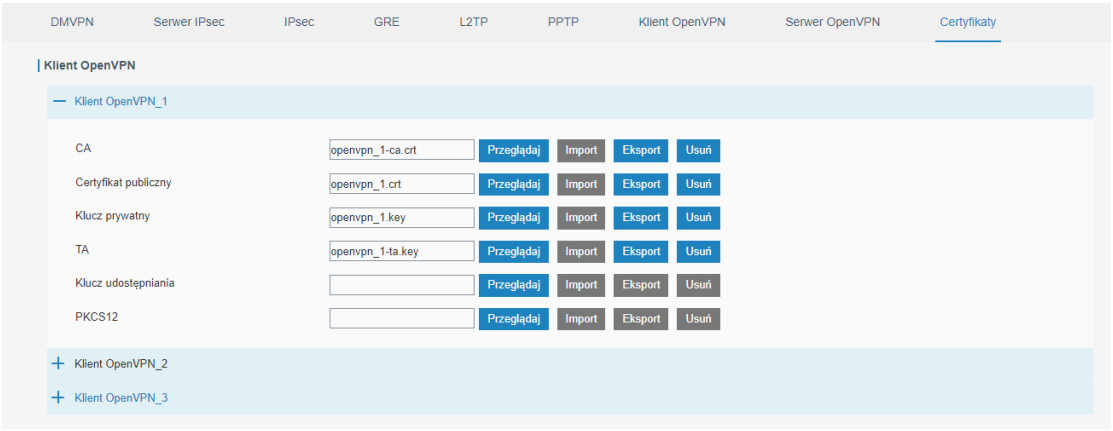


Obrázok 4.69 Konfigurácia servera OpenVPN

Pole	Opis
Zapnúť	Povolí / zakáže službu servera OpenVPN
Protokol	Výber komunikačného protokolu UDP / TCP
Prístav	Port, na ktorom má server načúvať
IP servera	IP adresa rozhrania, ktoré sa má zúčastniť pripojenia, ponechanie tohto poľa prázdne spôsobí, že všetky aktívne pripojenia sa zúčastnia tunelovania
Prevádzkový režim	Výber režimu tun / tap
Overenie	Výber typu autentifikácie
Lokálna virtuálna IP	Lokálna IP adresa tunela
Vzdialená virtuálna IP	IP adresa vzdialeného tunela
Klientska podsieť	Adresa IP siete pre tunel
Maska podsiete klienta	Maska podsiete pre tunel
Interval opätovného vyjednávania (s)	Interval medzi pokusmi o vyjednanie spojenia
Maximálny počet klientov	Maximálny počet klientov pripojených k serveru, rozsah 1-128
Povoliť CRL	Povolí / zakáže CRL
Povoliť komunikáciu medzi klientmi	Povolí / zakáže možnosť pripojenia medzi rôznymi klientmi OpenVPN
Povoliť duplikáciu klienta	Povolí / zakáže možnosť pripojenia viacerých klientov na jeden certifikát
Povoliť NAT	Povolí / zakáže NAT
Kompresia	Povolí (LZO) / zakáže (žiadna) kompresiu komunikácie
Interval detekcie spojenia (s)	Časový interval detekcie pripojenia
Šifrovanie	Výber typu šifrovania komunikácie
MTU	Maximálna veľkosť MTU
Maximálna veľkosť rámu	Maximálna veľkosť rámu
Úroveň podávania správ	Úroveň podrobností pre denníky služieb
Odborné možnosti	Pole sa používa na manuálne pridávanie ďalších položiek do protokolu OpenVPN, pričom každá položka by mala byť oddelená znakom „;“
Lokálne trasovanie	
Podsieť	Adresa lokálnej siete OpenVPN
Maska	Maska podsiete OpenVPN
Prevádzka	Pridáva / odstraňuje položky
Konto	
Používateľské meno	Používateľské meno klienta OpenVPN
Heslo	Heslo klienta OpenVPN
Prevádzka	Pridáva / odstraňuje položky

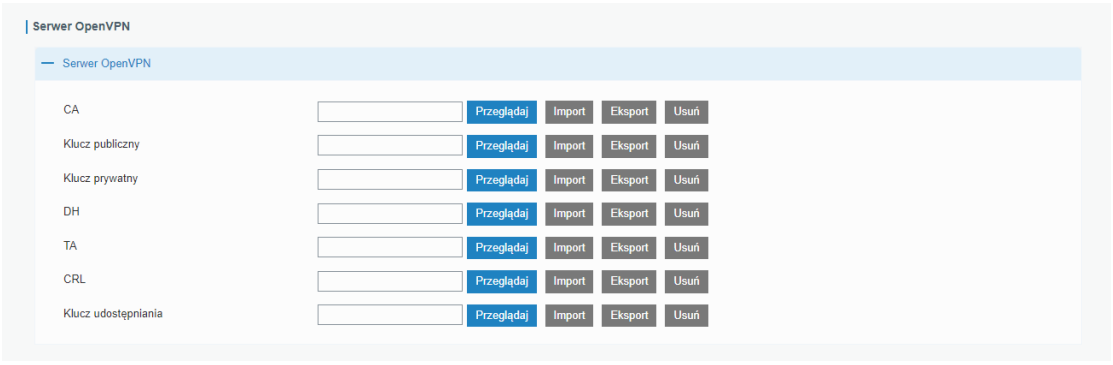
4.2.5.9 Certifikáty

Táto záložka sa používa na import/export certifikátov potrebných pre správne fungovanie služieb súvisiacich s OpenVPN a IPsec.



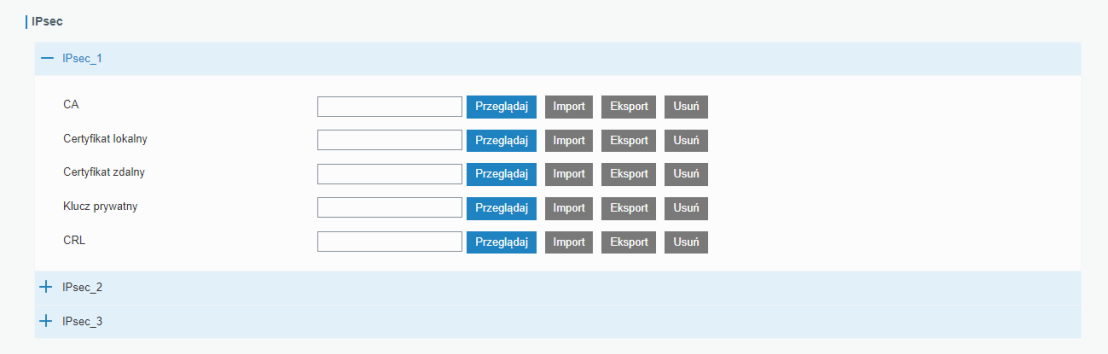
Obrázok 4.70 Import/ekxport certifikátov pre klientov OpenVPN

Pole	Opis
CA	Import / export certifikátu CA
Verejný kľúč	Import/export verejného kľúča
Súkromný kľúč	Import/export súkromného kľúča
TA	Import / export kľúča TA
Zdieľať kľúč	Import/export statického kľúča
PKCS12	Import / export certifikátu PKCS12



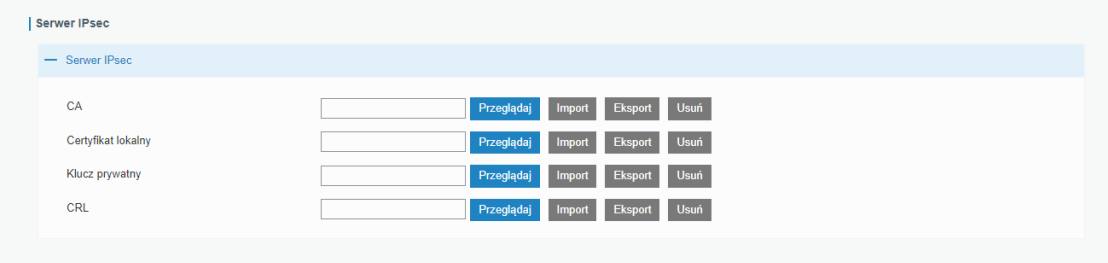
Obrázok 4.71 Import / export serverových certifikátov OpenVPN

Pole	Opis
CA	Import / export certifikátu CA
Verejný kľúč	Import/export verejného kľúča
Súkromný kľúč	Import/export súkromného kľúča
DH	Import / export kľúča DA
TA	Import / export kľúča TA
CRL	Import / export certifikátu CRL
Zdieľať kľúč	Import/export statického kľúča



Obrázok 4.72 Import / export certifikátov pre klientov IPsec

Pole	Opis
CA	Import / export certifikátu CA
Lokálny certifikát	Import / export lokálneho certifikátu
Vzdialený certifikát	Vzdialený import / export certifikátu
Súkromný kľúč	Import/export súkromného kľúča
CRL	Import / export certifikátu CRL

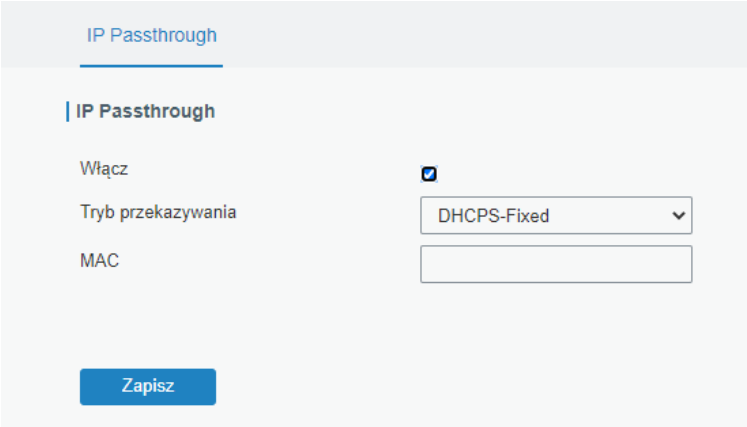


Obrázok 4.73 Import / export serverových certifikátov IPsec

Pole	Opis
CA	Import / export certifikátu CA
Lokálny certifikát	Import / export lokálneho certifikátu
Vzdialený certifikát	Vzdialený import / export certifikátu
CRL	Import / export certifikátu CRL

4.2.6 IP Passthrough

Funkcia IP Passthrough odovzdá IP adresu pridelenú poskytovateľom služby jednému zariadeniu pripojenému k rozhraniu LAN routera.
Ak chcete povoliť funkciu, musíte urobiť nasledujúce kroky:
1. Povoľte funkciu (**Povoliť**)
2. Nastavte režim, v ktorom má funkcia fungovať
3. Nastavte MAC adresu prijímajúceho zariadenia, ak bol zvolený režim „*DHCPS-Fixed*”

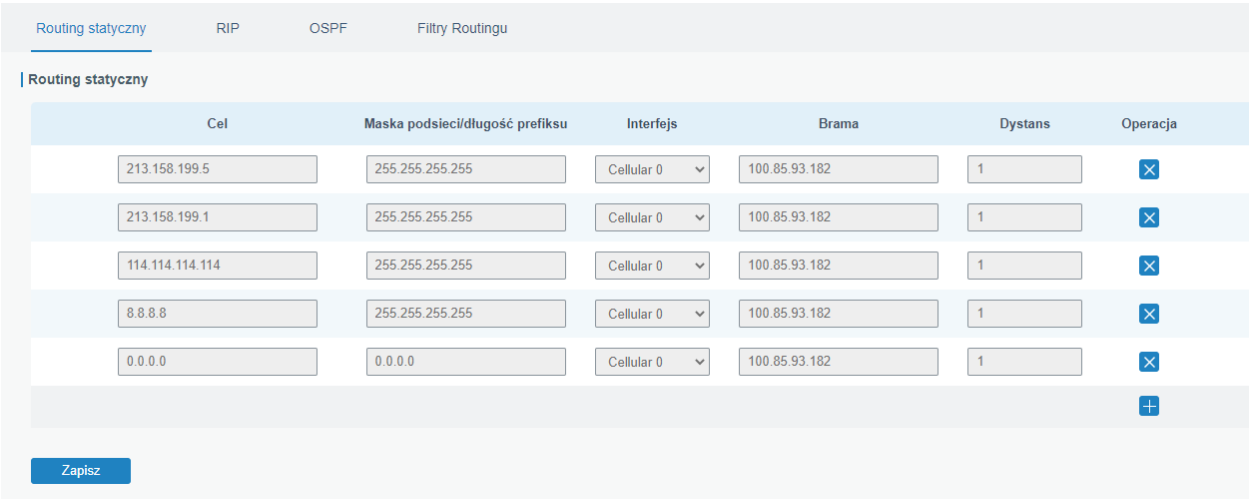


Obrázok 4.74 Konfigurácia funkcje IP Passthrough

4.2.7 Routing

4.2.7.1 Statický routing

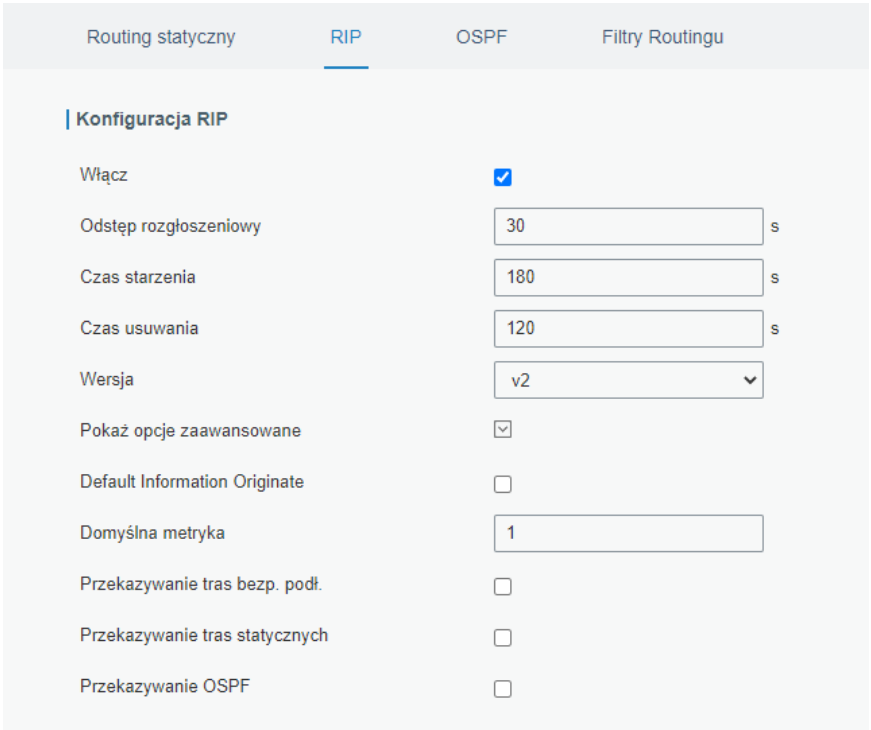
Statický routing sú manuálne pridané položky roteru. Informácie o smerovaní paketov sa pridávajú manuálne, nie automaticky určené prostredníctvom dynamického routeru. Po pridaní záznamov budú konkrétne balíky nasmerované na užívateľom definovanú trasu.
Ak chcete pridať položku do tabuľky, musíte:
1. Kliknite na + v stĺpci **Operácia**
2. Zadajte adresu IPv4 / IPv6 cieľovej siete (**Cieľ**)
3. Zadajte masku podsiete / dĺžku predpony pre cieľovú sieť (**Maska podsiete / Dĺžka predpony**)
4. Rozhranie routera, cez ktoré majú pakety unikať smerom k cieľovému zariadeniu (**Rozhranie**)
5. Adresa nasledujúceho routera, cez ktorý majú pakety prechádzať (**Brána**)
6. Nastavte prioritu trasy, čím menšie číslo, tým vyššia priorita (**Vzdialenosť**)
7. Kliknite na tlačidlo **Uložiť**



Obrázok 4.75 Konfigurácia položiek statického routeru

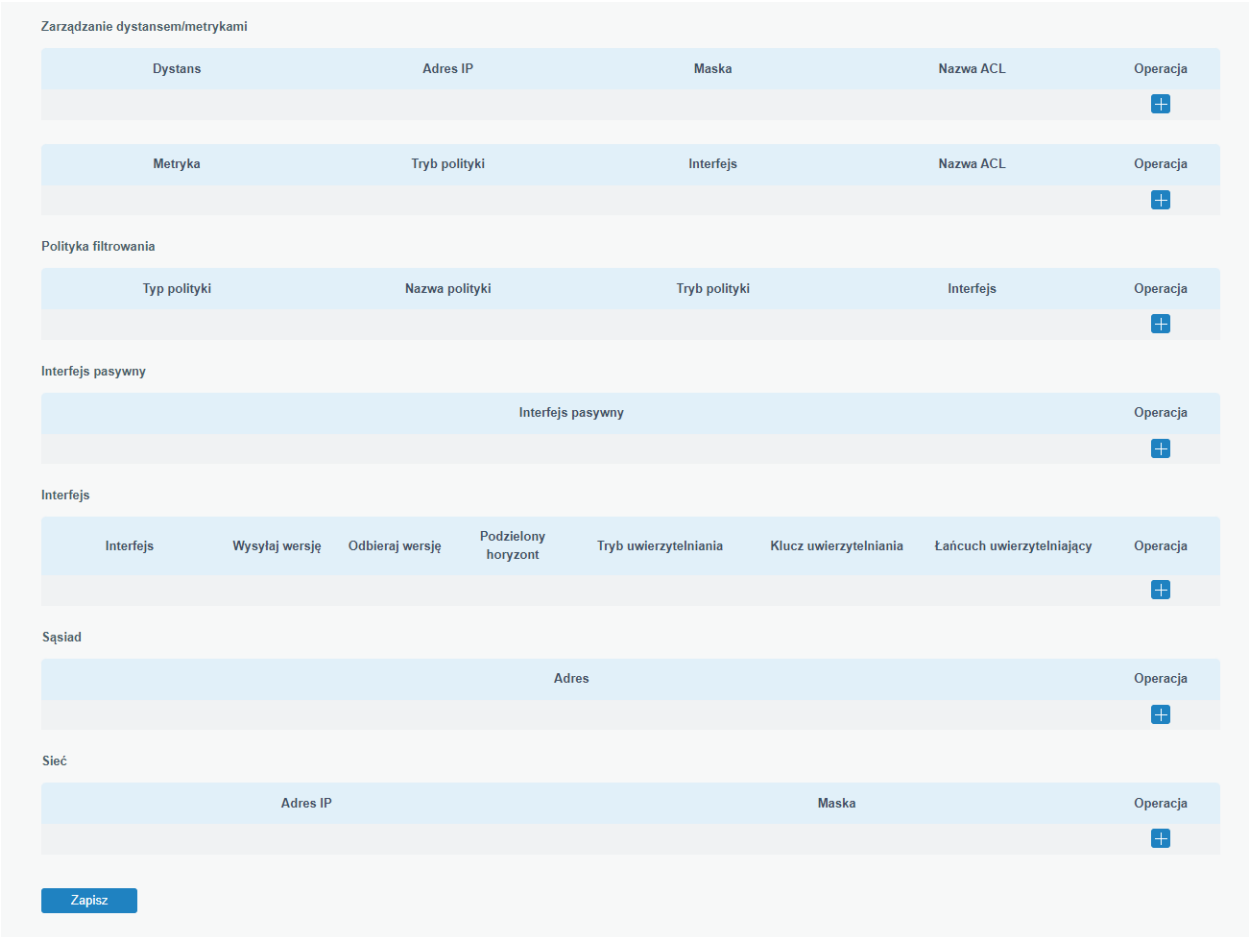
4.2.7.2 RIP

RIP (Routing Information Protocol) je dynamický smerovací protokol určený pre malé siete. Tento protokol používa počítadlo skokov na meranie vzdialenosti od zdrojového zariadenia k cieľovému zariadeniu, ktoré sa nazýva metrika. V RIP je počet skokov z routeru do priamo pripojenej siete 0 a počet skokov do po sebe nasledujúcich sietí sa zvýši o 1. Na obmedzenie času konvergencie môže byť metrikou celé číslo od 0 do 15, pričom každá metrika je väčšia než alebo rovné 16 je definované ako nekonečno, takže cieľová sieť alebo hostiteľ je nedostupný, takže RIP nie je dobrou voľbou pre rozľahlé siete. Aby sa zlepšil výkon a zabránilo sa slučkám smerovania, RIP podporuje funkciu zdieľania horizontu, ktorá bráni aktuálnemu routeru prijímať sieťové informácie od iných routerov. Každý router, ktorý používa RIP, udržiava smerovaciu tabuľku, ktorá obsahuje cesty na dosiahnutie všetkých cieľových sietí. Na spustenie protokolu RIP je potrebné službu zapnúť (**Povoliť**) a nakonfigurovať, router dáva aj možnosť rozšírenej konfigurácie protokolu po výbere možnosti **Zobraziť pokročilé možnosti**.



Obrázok 4.76 Počiatočná konfigurácia protokolu RIP

RIP Settings	
Pole	**Opis**
Zapnúť	Povolí / zakáže podporu RIP
Interval vysielania	Časový interval medzi postupným odoslaním informácií o trasách, hodnota vyjadrená v sekundách
Doba starnutia	Definuje čas starnutia trasy. Ak do tejto doby router nedostane aktualizačný paket pre danú trasu, metrika trasy sa nastaví na hodnotu 16, t.j. sieť bude určená ako nedostupná, hodnota je vyjadrená v sekundách
Čas odstránenia	Čas, po ktorom budú trasy s metrickou hodnotou 16 úplne odstránené zo smerovacej tabuľky, hodnota je vyjadrená v sekundách
Verzia	Verzia RIP, ktorú router používa (v1 alebo v2)
Zobraziť rozšírené možnosti	Zobrazí/skryje rozšírené možnosti
Predvolený zdroj informácií	Povolí / zakáže vysielanie príkazu Default Information Originate
Predvolená metrika	Náklady na prechod cez tento router, o toľkoto sa zvýši metrika pri prechode cez tento router
Presun priamych trás pripojený	Povolí / zakáže presmerovanie priamo pripojených sietí
Metriky	Po zapnutí možnosti „Presun priamych trás pripojený” nastavte pre ňu cenu prechodu
Prechádzanie statických trás	Povolí / zakáže presmerovanie trás zo statického smerovania
Metriky	Po povolení možnosti „Prejsť statické trasy“ nastavte pre ňu cenu prechodu
Prenos OSPF	Povolí / zakáže presmerovanie trasy z OSPF
Metriky	Keď je povolený „OSPF Pass-Through”, musíte preň nastaviť cenu prechodu



Obrázok 4.77 Pokročilá konfigurácia protokolu RIP

Skupina nastavení	Pole	Opis
Správa vzdialenosti / metrík	Vzdialenosť	Nastavuje administratívnu vzdialenosť
	IP adresa	IP adresa trasy RIP
	Maska	Maska podsiete trasy RIP
	Názov ACL	Názov ACL trasy RIP
	Prevádzka	Pridáva / odstraňuje položky
	Metriky	Nastavuje hodnotu metriky
	Režim politiky	Na čo odkazuje politika. Vyberte si z „in" alebo „out"
	Rozhranie	Výber rozhrania
	Názov ACL	Názov ACL pre cestu RIP
	Prevádzka	Pridáva / odstraňuje položky
Pravidlá filtrovania	Typ politiky	Typ politiky
	Názov politiky	Názov politiky
	Režim politiky	Na čo odkazuje politika. Vyberte si z „inn" alebo „out"
	Rozhranie	Výber rozhrania
	Prevádzka	Pridáva / odstraňuje položky
Pasívne rozhranie	Pasívne rozhranie	Výber pasívneho rozhrania, ktoré bude prijímať pakety RIP, ale nebude ich odosielať
	Prevádzka	Pridáva / odstraňuje položky
Rozhranie	Rozhranie	Výber rozhrania
	Odoslaná verzia	Verzia paketov RIP odoslaných z rozhrania
	Prijatá verzia	Verzia paketov RIP, ktoré rozhranie prijíma
	Rozdelený horizont	Povoliť / zakázať funkciu rozdeleného horizontu
	Režim overenia	Vyberte, či má byť komunikačný kľúč šifrovaný (text alebo md5)
	Autentifikačný kľúč	Komunikačný kľúčový obsah pre RIPv2
	Autentifikačný reťazec	Šifrovací kľúč pre RIPv2
	Prevádzka	Pridáva / odstraňuje položky
Sused	IP adresa	IP adresa suseda
	Prevádzka	Pridáva / odstraňuje položky
Sieť	IP adresa	Adresa IP rozhrania na vysielanie paketov RIP
	Maska	Maska podsiete rozhrania na vysielanie paketov RIP
	Prevádzka	Pridáva / odstraňuje položky

4.2.7.3 OSPF

OSPF (Open ShortestPath First) je smerovací protokol založený na Internal Gateway Protocol vyvinutom IETF. Ak váš router chce spustiť OSPF, malo by existovať ID routera, ktoré môžete nakonfigurovať manuálne. Ak ID routera nebolo nakonfigurované, systém automaticky vyberie adresu IP rozhrania ako ID routera. Poradie výberu je nasledovné:

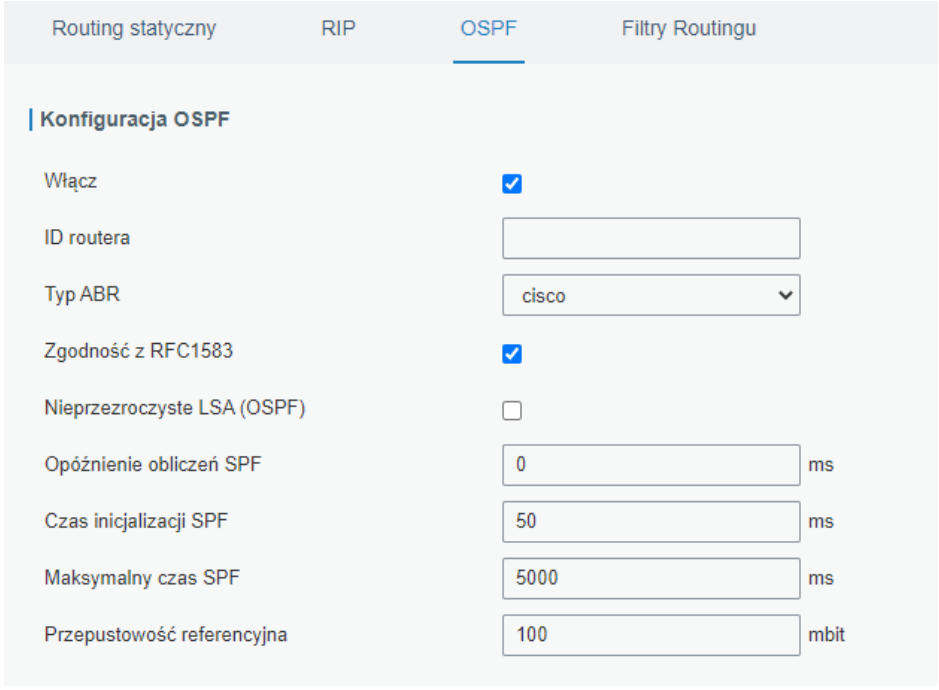
- Ak je nakonfigurovaná adresa pre rozhranie slučky, ako identifikátor routera sa použije naposledy nakonfigurovaná adresa IP pre rozhranie slučky;
- Ak nie je nakonfigurovaná žiadna adresa rozhrania slučky, systém vyberie rozhranie s najväčšou IP adresou ako ID routera.

Tento protokol vysiela päť typov paketov:

- Paket Hello
- Paket balík (balík s popisom databázy)
- Paket LSR (paket žiadosti o stav spojenia)
- Paket LSU (balíček aktualizácie stavu odkazu)
- Paket LSAck (balíček potvrdenia odkazu Sate)

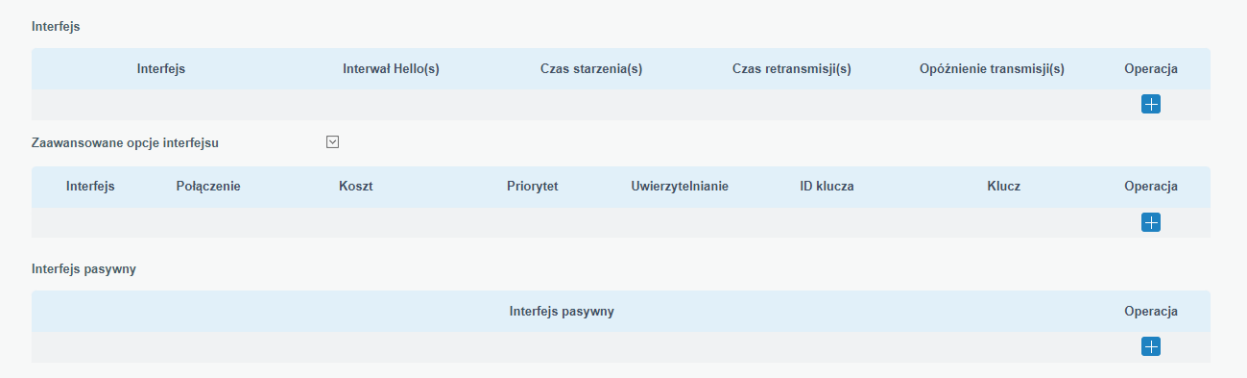
Sused a susedia

Keď sa OSPF router spustí, pošle Hello pakety cez rozhranie OSPF. Po prijatí Hello paketu OSPF router skontroluje parametre definované v pakete. Ak bude konzistentný, vytvorí sa susedský vzťah. Nie všetky zodpovedajúce strany v susedskom vzťahu môžu vytvoriť sieťový vzťah. Závisí to od typu siete. Len keď si obe strany úspešne vymenia DD pakety a dosiahne sa synchronizácia LSDB, môže sa vytvoriť skutočné susedstvo. LSA popisuje topológiu siete okolo routera, LSDB popisuje topológiu celej siete.



Obrázok 4.78 Predkonfigurácia protokolu OSPF

Konfigurácia OSPF	
Pole	**Opis**
Zapnúť	Povolí / zakáže OSPF
ID smerovača	ID smerovača (IP adresa) pre pakety LSA
Typ ABR	Typ ABR (cisco, ibm, standard, shortcut)
Súlad s RFC1583	Povolí / zakáže súlad s RFC1583
Nepriehľadné LSA (OSPF)	Povolí / zakáže nepriehľadné pakety LSA
Oneskorenie výpočtu SPF	Nastavuje čas oneskorenia pre výpočty SPF, rozsah 0-6000000 milisekúnd
Čas inicializácie SPF	Nastavuje čas inicializácie SPF, rozsah 0-6000000 milisekúnd
Maximálny čas SPF	Nastavuje maximálny čas SPF, rozsah 0-6000000 milisekúnd
Referenčná šírka pásma	Referenčná šírka pásma, rozsah 1-4294967 Mbit

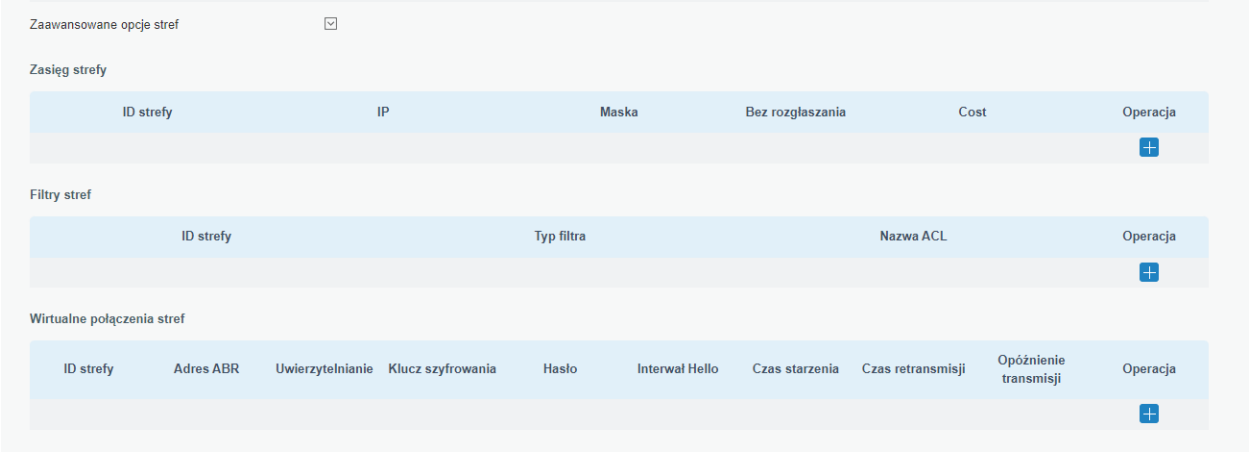


Obrázok 4.79 Konfigurácia rozhraní protokolu OSPF

Pole	Opis
Rozhranie	
Rozhranie	Výber rozhrania, na ktoré sa záznam vzťahuje
Interval Hello (s)	Časový interval medzi po sebe nasledujúcimi vysielaniami paketu Hello. Ak sa tento čas líši na susednom smerovači, nebude možné určiť suseda, rozsah 1-65535 sekúnd
Doba starnutia (s)	Čas, po ktorom router určil, že sused je nedostupný po tom, čo neprijal paket Hello od suseda. Ak je tento čas na susednom routeri iný, nebude možné určiť suseda
Čas opätovného prenosu (s)	Keď router upozorní svojho suseda na LSA, vyžaduje sa potvrdenie. Ak počas obdobia opakovaného prenosu nie je prijatý žiadny potvrdzovací paket, LSA bude znova odoslaný susedovi. Rozsah 3-65535 sekúnd
Oneskorenie prenosu (s)	Čas oneskorenia, po ktorom začne čas starnutia LSA
Prevádzka	Pridáva / odstraňuje položky
Pokročilé možnosti rozhrania	
Rozhranie	Výber rozhrania, na ktoré sa záznam vzťahuje
Sieť	Výber typu pripojenia pre OSPF
Náklady	Náklady OSPF na rozhranie. Rozsah 1-65535
Priorita	Priorita OSPF pre rozhranie. Rozsah 1-255
Overenie	Výber typu autentifikácie Jednoduché: zadáme heslo, ktoré následne potvrdíme MD5: zadajte šifrovací kľúč a heslo, ktoré je potom potrebné potvrdiť
Šifrovací kľúč	MD5 šifrovací kľúč
Heslo	Komunikačné heslo
Prevádzka	Pridáva / odstraňuje položky
Pasívne rozhranie	
Pasívne rozhranie	Pasívny výber rozhrania
Prevádzka	Pridáva / odstraňuje položky

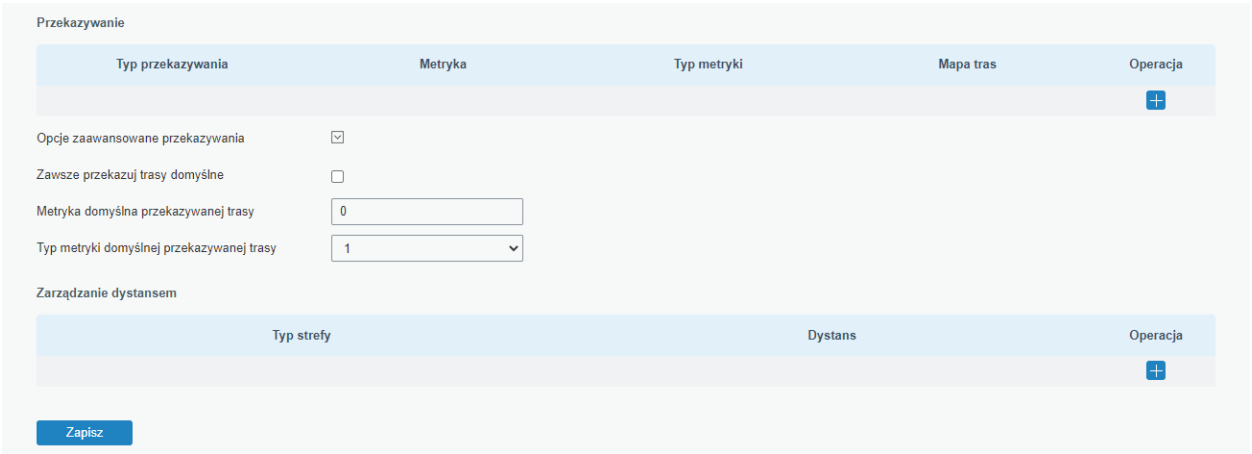
Obrázok 4.80 Konfigurácia siete protokolu OSPF

Pole	Opis
Sieť	
IP adresa	IP adresa lokálnej siete
Maska	Maska podsiete lokálnej siete
ID zóny	ID oblasti, do ktorej router patrí
Prevádzka	Pridáva / odstraňuje položky
Sused	
IP adresa	IP adresa suseda
Priorita	Priorita suseda
Anketa	Časový interval vysielania paketu Hello susedovi
Operácia	Pridáva / odstraňuje záznamy
Zóna	
ID zóny	ID číslo zóny OSPF (IP adresa)
Typ zóny	Typ zóny (STUB, NSSA), zóna backbone (ID 0.0.0.0) nemôže byť nastavená ako STUB alebo NSSA
Žiadne zhrnutie	Zakáže sumarizáciu trasy
Overenie	Výber typu overenia (jednoduché, MD5)
Prevádzka	Pridáva / odstraňuje položky



Obrázok 4.81 Konfigurácia OSPF konfigurácia rozšírenej zóny

Pole	Opis
Rozsah zóny	
ID zóny	ID zóny pre rozhranie, na ktorom je spustený OSPF (IP adresa)
IP	IP adresa
Maska	Masku podsiete
Bez trasy	Povolí / zakáže blokovanie trás vysielaných mimo zóny
Náklady	Cena, rozsah 0-16777215
Prevádzka	Pridáva / odstraňuje položky
Zónové filtre	
ID zóny	ID zóny, ktorá sa má filtrovať
Typ filtra	Typ zónového filtrovania
Názov ACL	Názov ACL, ktorý je nastavený na karte Routing Filtering (časť 4.2.7.4)
Prevádzka	Pridáva / odstraňuje položky
Pripojenie virtuálnej zóny	
ID zóny	ID číslo zóny OSFP
adresa ABR	Adresa smerovača ARB, ktorý je v kontakte s inými zónami
Overenie	Typ overenia (jednoduché, MD5)
Šifrovací kľúč	Šifrovací kľúč pre MD5
Heslo	Autentifikačné heslo
Interval Hello	Interval medzi vysielaním paketov Hello, rozsah 1-65535
Doba starnutia	Čas, po ktorom router určí, že sused je nedostupný po tom, čo neprijal paket Hello od suseda, rozsah 1-65535
Čas retransmisie	Interval medzi pokusmi o odoslanie LSA, rozsah 1-65535
Oneskorenie prenosu	Čas oneskorenia prenosu LSA, rozsah 1-65535
Prevádzka	Pridáva / odstraňuje položky

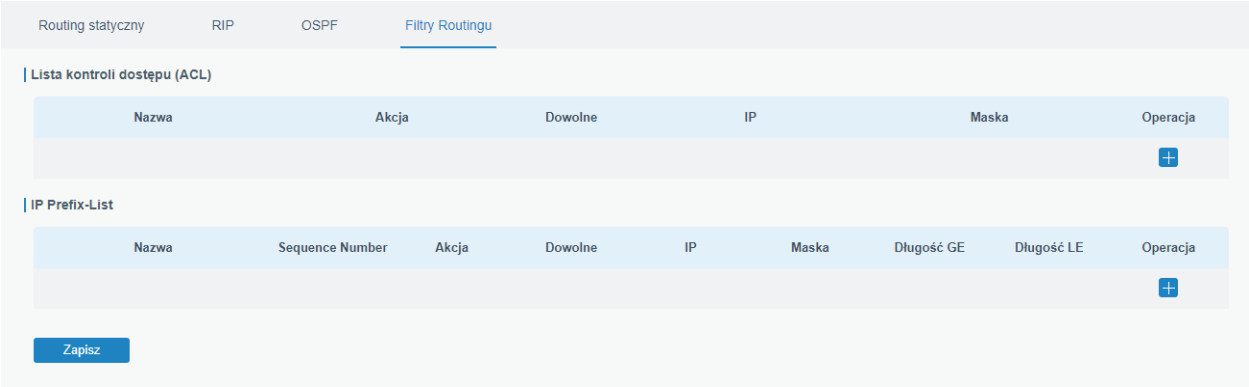


Obrázok 4.82 Konfigurácia protokolu OSFP pre smerovanie trás routeru

Pole	Opis
Prenos	
Typ preposielania	Typ routingu z jakiego mają być przekazywane trasy
Metriky	Metryka routera przekazującego. Zakres 0-16777214
Typ metriky	Typ metryki
Mapa trasy	Nazwa mapy trasy
Prevádzka	Dodaje/usuwa wpisy
Pokročilé možnosti preposielania	
Vždy posielať predvolené trasy	Povolí / zakáže vysielanie predvoleného presmerovania trasy po spustení
Predvolená metrika pre presmerovanú trasu	Predvolená metrika nahrávania. Rozsah 0-16777214
Typ predvolenej metriky pre presmerovanú trasu	Predvolený typ metriky (0,1,2)
Manažment vzdialenosti	
Typ zóny	Typ zóny
Vzdialenosť	Rozsah, do ktorého má presmerovanie trasy dosiahnuť. Rozsah 1-255
Prevádzka	Pridáva / odstraňuje položky

4.2.7.4 Filtre routingu

V tejto záložke môžete nakonfigurovať filtre pre smerovanie.



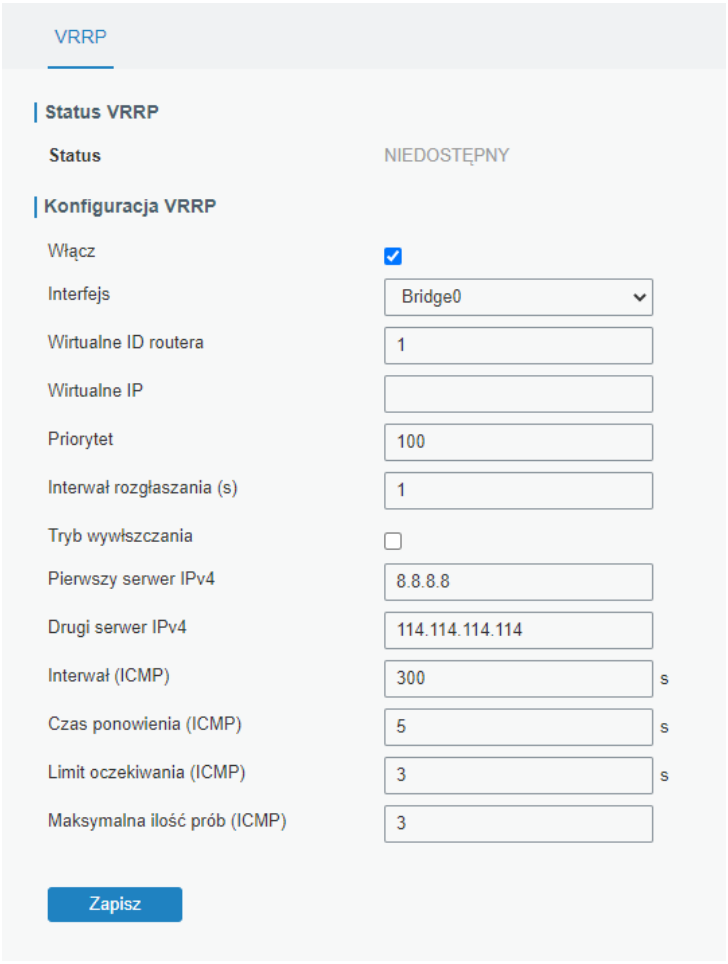
Obrázok 4.83 Konfigurácia filtrov pre routing

Pole	Opis
ACL Access Control List	
Názov	Názov položky ACL
Akcia	Typ akcie, na ktorú sa má záznam vzťahovať (povoliť, zamietnuť)
Akýkoľvek	Keď je začiarknuté, nemusíte zadávať IP adresu a masku podsiete
IP	IP adresa
Maska	Masku podsiete
Prevádzka	Pridáva / odstraňuje položky
IP Prefix-List	
Názov	Názov položky
SequenceNumber	Prefix list môže byť použitý v mnohých pravidlách, každé pravidlo zodpovedá jednému poradovému číslu, rozsah 1-4294967295
Akcia	Typ akcie, na ktorú sa má záznam vzťahovať (povoliť, zamietnuť)
Akýkoľvek	Keď je začiarknuté, nemusíte zadávať IP adresu a masku podsiete
IP	IP adresa
Maska	Masku podsiete
Dĺžka	Minimálny počet bitov v maske podsiete, rozsah 0-32
Dĺžka LE	Maximálny počet bitov v maske podsiete, rozsah je 0-32
Prevádzka	Pridáva / odstraňuje položky

4.2.8 VRRP

V tejto záložke môžete nakonfigurovať službu VRRP (Virtual Router RedundancyProtocol). Táto služba umožňuje hostiteľom automaticky prepínať medzi routermi v prípade zlyhania jedného z nich, čo zaisťuje vyššiu spoľahlivosť siete. Keď je VRRP správne nakonfigurovaný na všetkých routeroch v sieti, servisné mechanizmy automaticky vyberú virtuálny koreňový router, ktorý bude smerovať sieťovú prevádzku mimo sieť. Výber hlavného zariadenia sa vykonáva nastavením priority zariadenia. Po vytvorení hlavného routera pravidelne posiela „živú“ správu všetkým podriadeným routerom, ak záložné routery nedostanú „živú“ správu po určitom čase, mechanizmus VRRP vyberie nový hlavný router na základe prioritne priradených zariadení. Ak aktuálny koreňový router prijme správu zo zariadenia s vyššou prioritou, prejde na nižšiu úroveň a nové zariadenie s vyššou prioritou sa stane koreňovým routerom. Konfigurácia zariadení v sieti je obmedzená na zadanie virtuálnej IP adresy routera ako predvolenej adresy brány.
Ak chcete nakonfigurovať službu, postupujte nasledovne:

1. Povoľte službu (**Povoliť**)
2. Vyberte rozhranie routera, ku ktorému sú pripojené zariadenia v lokálnej sieti
3. Nastavte ID číslo skupiny routerov, ktoré musí byť rovnaké na všetkých routercoh v skupine (**ID skupiny**)
4. Nastavte IP adresu virtuálneho routera, čo musí byť adresa už pridelená jednému z routerov v skupine a nie dodatočná logická adresa (**virtuálna IP**).
5. Nastavte prioritu routera (**Priorita**)
6. Nastavte frekvenciu odosielania „živých“ správ vyjadrenú v sekundách (**Interval vysielania (s)**)
7. Povoľte / zakážte preemptívny režim, ktorý umožňuje záložnému routeru s vyššou prioritou zabrániť koreňovému routeru s nižšou prioritou
8. Nastavenie serverov DNS (**prvý server IPv4 / druhý server IPv4**)
9. Nastavte parametre súvisiace so službou PING Detection, ako napríklad: interval ping (**Interval**), interval medzi nasledujúcimi pokusmi o dopyt, ak prvý zlyhá (**Retry time**), maximálny čas čakania na odpoveď ping (**Waiting limit**), maximálny počet pokusov vykonať ping otázku (**Maximálny počet pokusov**)

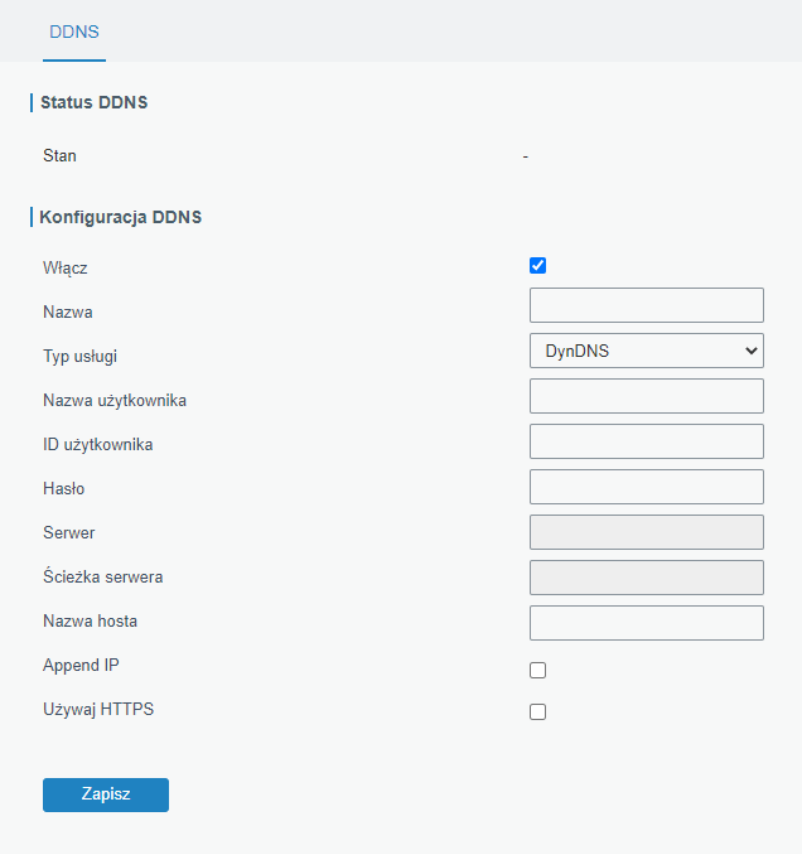


Obrázok 4.84 Konfigurácia služby VRRP

4.2.9 DDNS

V tejto záložke môžeme nakonfigurovať službu DDNS (DynamicDomainName System), vďaka ktorej sa môžeme pripojiť k nášmu routeru pomocou registrovaného názvu domény, ak náš poskytovateľ služby ponúka verejnú, variabilnú alebo pevnú IP adresu. Pred spustením nastavenia si musíte zaregistrovať účet u jedného z poskytovateľov služieb DDNS.
Ak chcete nakonfigurovať službu, postupujte nasledovne:

1. Povoľte službu (**Povoliť**)
2. Vyberte poskytovateľa služieb (**typ služby**)
3. Vyplňte polia, ktoré poskytovateľ služieb vyžaduje na pripojenie (pozrite si príručku poskytovateľa služieb)
4. Kliknite na tlačidlo **Uložiť**



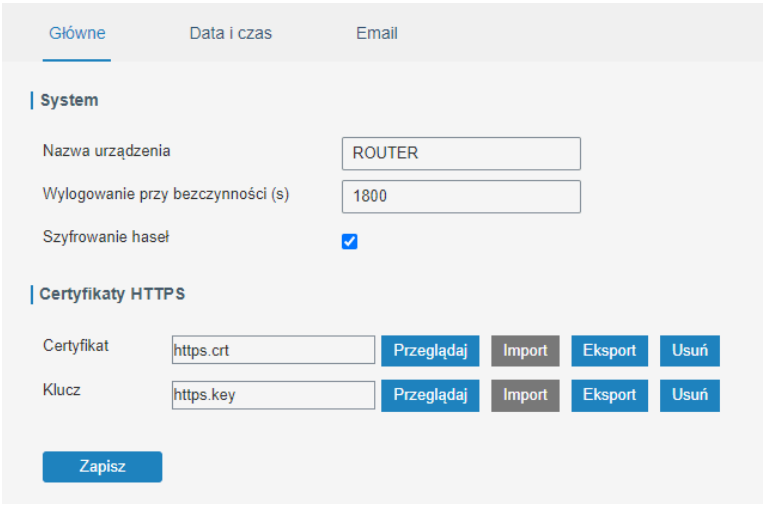
Obrázok 4.85 Konfigurácia služby DDNS

4.3 SYSTÉMOVÉ NASTAVENIA

4.3.1 Základné nastavenia

4.3.1.1 Hlavné

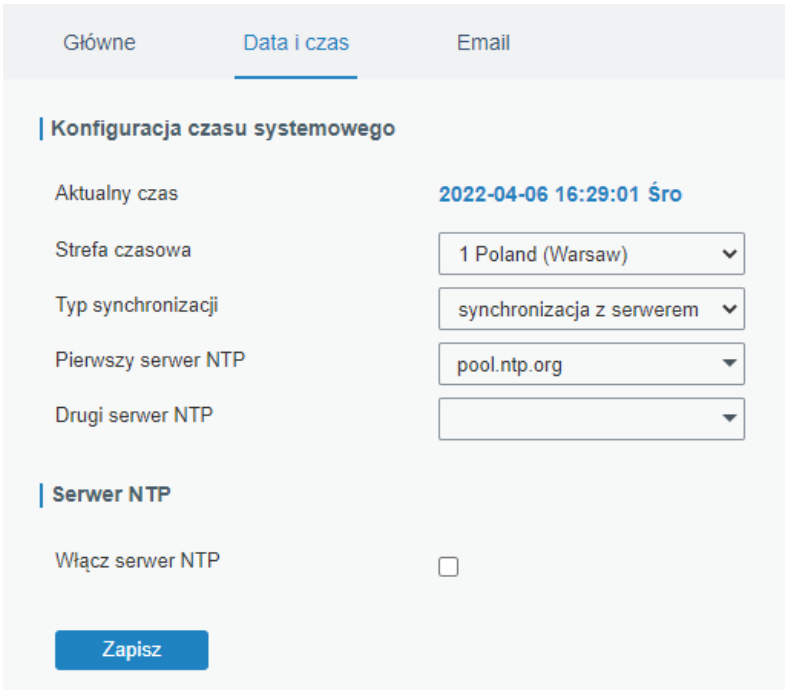
V tejto záložke môžeme konfigurovať základné údaje o zariadení, ako je jeho názov (**Device name**), čas do odhlásenia v prípade nečinnosti vyjadrený v sekundách (**Logout when idle(s)**) a povoliť / zakázať šifrovanie hesla (**Password šifrovanie**). Okrem toho tu môžeme sťahovať, mazať a importovať (kliknite na **Prehľadávať**, vyberte súbor na disku a potom kliknite na **Importovať**) súbory súvisiace s certifikátom a HTTPS kľúčom.



Obrázok 4.86 Hlavné nastavenia

4.3.1.2 Dátum a čas

V tejto záložke môžete zmeniť nastavenia dátumu a času. Router štandardne používa server NTP pool.ntp.org, ale môžeme nastaviť synchronizáciu s prehliadačom alebo manuálne nastaviť dátum a čas pomocou možnosti **Typ synchronizácie**. Voľba **Aktuálny čas** zobrazuje aktuálny dátum a čas, vo voľbe Časové pásmo môžete nastaviť časové pásmo, v ktorom sa router nachádza a pri možnosti **Prvý NTP server** a **Druhý NTP server** môžete zadať IP adresy NTP serverov. Okrem toho môžeme na zariadení spustiť funkciu NTP servera (**Enable NTP server**).

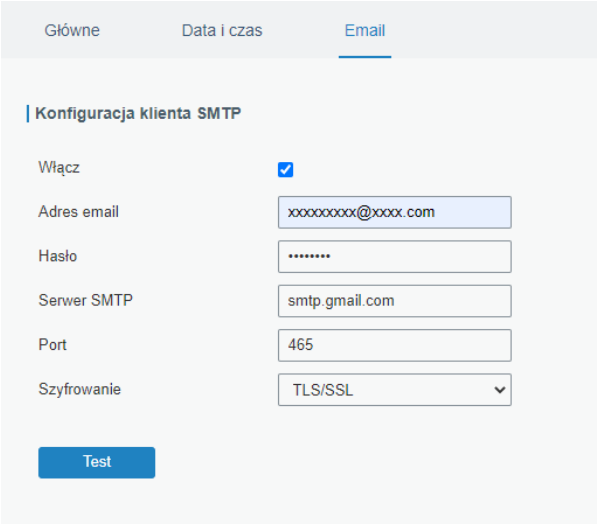


Obrázok 4.87 Funkcia Dátum a čas

4.3.1.3 Email

V tejto záložke môžete nakonfigurovať údaje pre e-mailový účet, ktorý môžeme použiť na odosielanie upozornení na alarmy, ktoré sa objavia na routeri (časť 4.3.7.2). Ak chcete spustiť službu odosielania e-mailových správ z routera na konkrétne e-mailové adresy, musíte urobiť nasledovné kroky:

1. Aktivujte funkciu (**Enable**)
2. Nakonfigurujte e-mailový účet, ktorý bude odosielateľom správy, špecifikujte: e-mailovú adresu, heslo pre tento účet, adresu servera SMTP, port, na ktorom služba SMTP funguje a typ šifrovania hesla. Správnosť konfigurácie je možné skontrolovať kliknutím na tlačidlo **Test**.

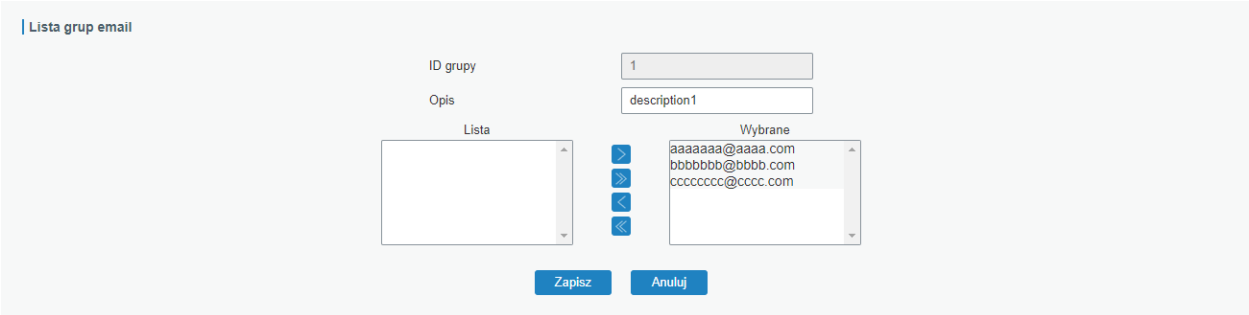


Obrázok 4.88 Konfigurácia e-mailových účtov krok 1 a 2

3. Príjemncov správy pridáte kliknutím na + v stĺpci **Operácia** v skupine **Zoznam e-mailových adries** a doplniac **e-mailovú adresu** a popis **príjemcu**

Obrázok 4.89 Konfigurácia e-mailových účtov krok 3

4. Cieľovú skupinu vytvoríte kliknutím na + v stĺpci **Operácia** v skupine **e-mailových adries** zadaním **ID skupiny** od 1 do 100 a **popisu** a pridaním e-mailovej adresy (vyberte konkrétnu adresu v okne **Zoznam** a kliknite na >, kliknutie na >> pridá všetky adresy do skupiny) a kliknite na tlačidlo **Uložiť**.



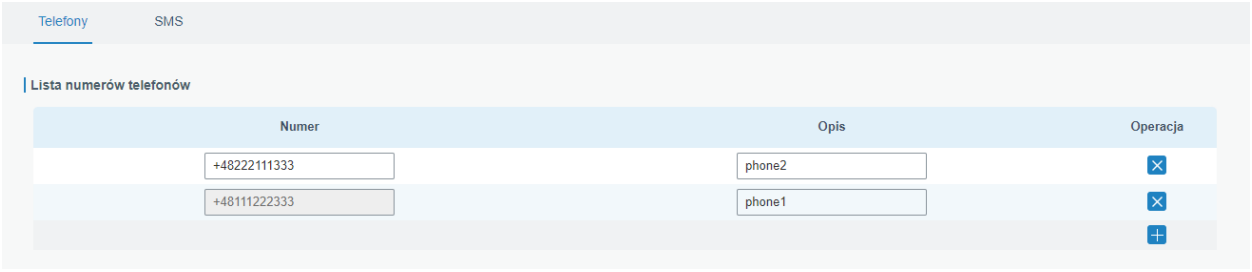
Obrázok 4.90 Konfigurácia e-mailových účtov krok 4

4.3.2 Telefóny a SMS

4.3.2.1 Telefóny

V tejto záložke môžete vytvoriť zoznam telefónnych čísel a zoskupiť ich tak, aby ste sa mohli pripojiť k internetu pomocou telefónneho spojenia alebo SMS a dostávať SMS upozornenia o stave zariadenia. Ak chcete pridať telefón do zoznamu a vytvoriť skupinu, postupujte nasledovne:

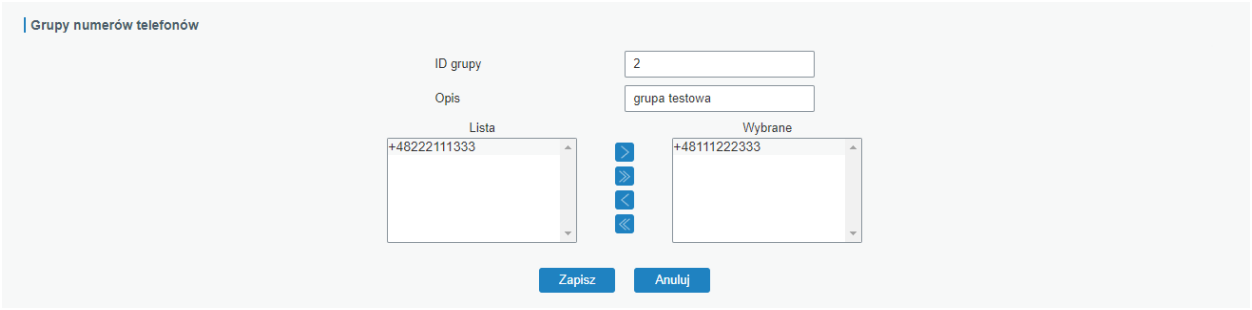
1. Kliknite na + v **Zozname telefónnych čísel**
2. Zadajte číslo s predvoľbou krajiny (napr. +48) a **popisom**



Obrázok 4.91 Pridanie telefónnych čísel kroky 1 a 2

Kliknite na + v **Zozname telefónnych čísel**

1. Pridajte telefónnu skupinu zadaním jej **ID skupiny** z rozsahu 1-100 a **popisu** a pridajte do nej predtým pridané telefónne čísla (vyberte konkrétne číslo v okne **Zoznam** a kliknite na >, kliknutím na >> pridáte všetky telefónne čísla do skupiny) a kliknite na tlačidlo **Uložiť**



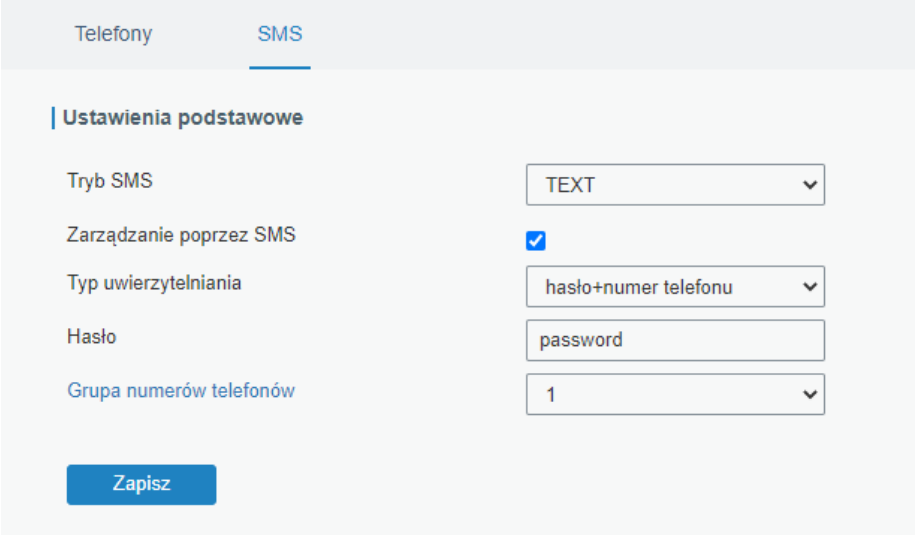
Obrázok 4.92 Pridanie telefónnych čísel kroky 3 a 4

4.3.2.2 SMS

V tejto záložke môžete spravovať SMS modul v routeri.

Základné nastavenia

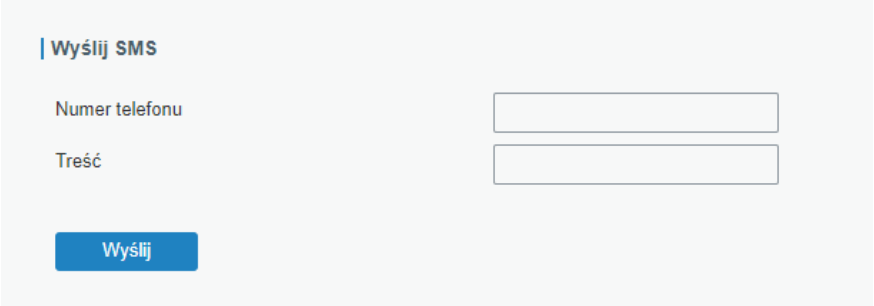
V tejto skupine nastavte typ SMS správy (**režim SMS**), spustite funkciu ovládania routera cez SMS (**Management via SMS**), typ autentifikácie pri ovládaní cez SMS (**Authentication type**), ak zvolíte autentifikáciu telefónnym číslom a heslo, zadajte heslo, ktoré sa bude používať (**Heslo**), vyberte skupinu čísel, ktorá sa má použiť pre SMS správy (**Skupina telefónnych čísel**).



Obrázok 4.93 Časť Základné nastavenia v záložke SMS

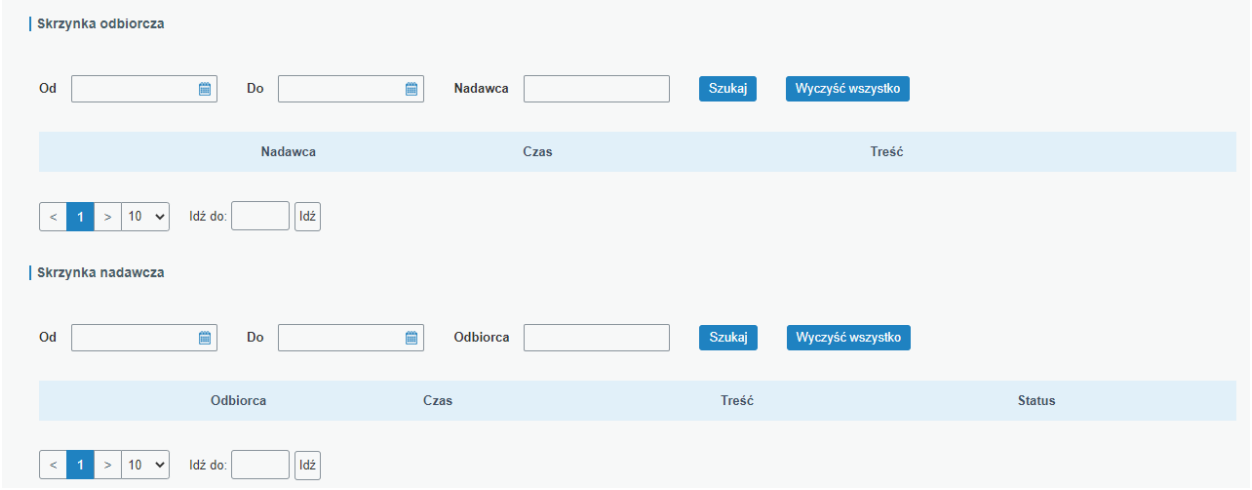
Posielanie SMS

V tejto skupine môžete poslať SMS z routera, aby sme napríklad skontrolovali, či SIM karta funguje správne. Ak chcete odoslať SMS, zadajte číslo príjemcu SMS (**Telefónne číslo**) a jej obsah (**Obsah**), potom kliknite na tlačidlo **Odoslať.**



Obrázok 4.94 Skupina Odoslať SMS v záložke SMS

Doručená pošta / Pošta na odoslanie
V týchto skupinách môžeme zobraziť doručenú poštu a poštu na odoslanie. V oboch prípadoch môžeme správu filtrovať zadaním dátumu začiatku, dátumu ukončenia a čísla odosielateľa alebo príjemcu. Ak chceme vyčistiť konkrétnu poštovú schránku, klikneme na tlačidlo **Vymazať všetko**.



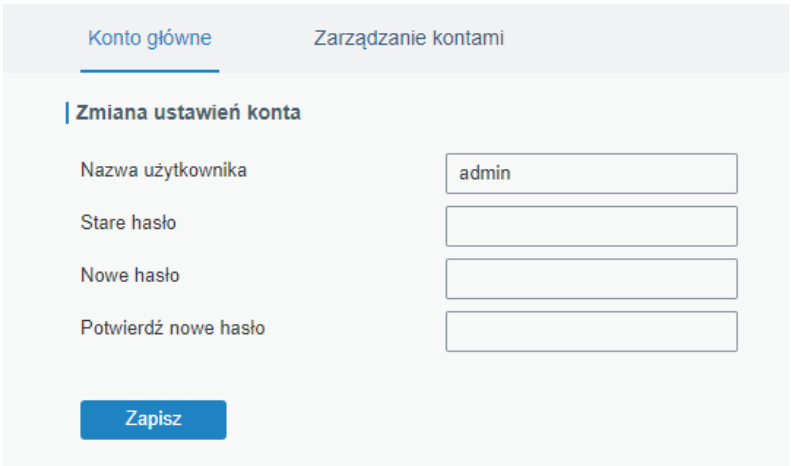
Obrázok 4.95 Pošta na odoslanie a Doručená pošta na karte SMS

Box	Pole	Opis
Prijímanie	Odosielateľ	Telefónne číslo odosielateľa správy
	Čas	Dátum a čas doručenia správy
	Obsah	Obsah správy
Vysielanie	Príjemca	Telefónne číslo príjemcu správy
	Čas	Dátum a čas odoslania správy
	Obsah	Obsah správy
	Status	Stav správy

4.3.3 Užívatelia

4.3.3.1 Hlavný účet

V tejto záložke môžete konfigurovať prístupové údaje k účtu, v ktorom ste práve prihlásení. V prípade administrátorského účtu tu môžete zmeniť užívateľské meno a heslo. Ak chcete zmeniť heslo k účtu, zadajte **staré heslo, nové hesl**o a **zopakujte nové heslo** a potom kliknite na tlačidlo **Uložiť**.

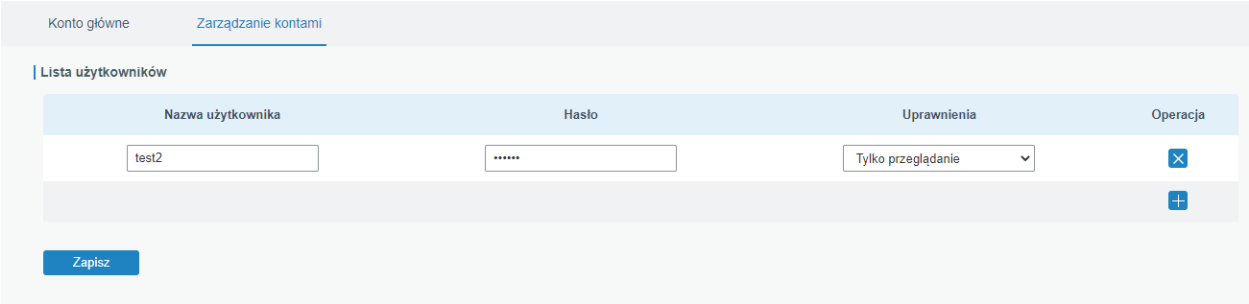


Obrázok 4.96 Zmena nastavenia hlavného účtu

4.3.3.2 Vedenie účtov

V tejto záložke môžete pridať ďalších používateľov na obsluhu routera (maximálne 5), stačí urobiť nasledovné:

1. Kliknite na ⊞ v stĺpci **Operácia**
2. Zadajte: meno nového používateľa, heslo nového používateľa a vyberte rozsah práv: iba na čítanie nastavení routera alebo na čítanie a zmenu nastavení routera



Obrázok 4.97 Pridanie nového používateľa

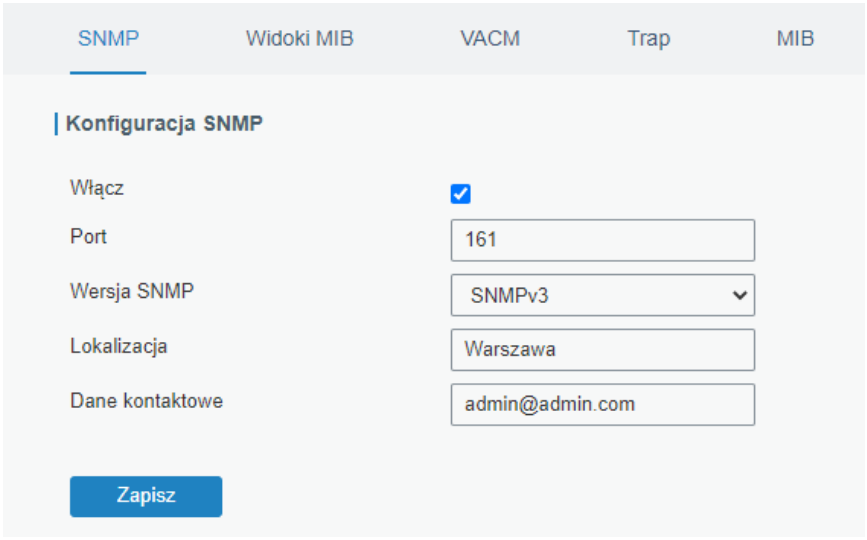
3. Kliknite na tlačidlo **Uložiť**

4.3.4 SNMP

4.3.4.1 SNMP

V tejto základke môžete povoliť službu SNMP na smerovači a vykonať jej počiatočnú konfiguráciu, na to je potrebné urobiť nasledujúce kroky:

1. Povoľte službu (**Povoliť**)
2. Nastavte port, na ktorom má služba fungovať (**Port**)
3. Vyberte verziu protokolu SNMP, ktorú chcete použiť (**verzia SNMP**)
4. Uveďte názov lokality, v ktorej sa zariadenie nachádza, a kontaktné údaje osoby zodpovednej za zariadenie

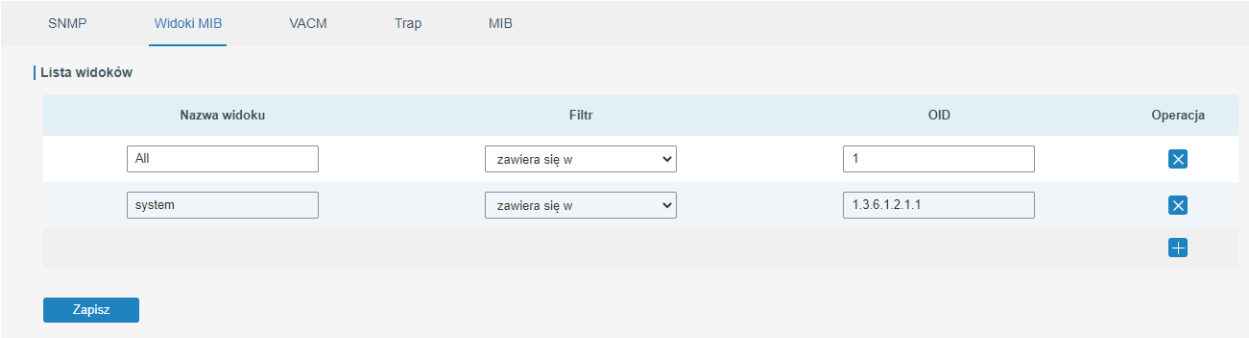


Obrázok 4.98 Počiatočná konfigurácia služby SNMP

4.3.4.2 MIB zobrazenia

V tejto záložke môžete pridať zobrazenia, vďaka čomu môžete obmedziť prístup k jednotlivým vetvám stromu MIB, pre pridanie ďalšieho zobrazenia urobte nasledovné:

1. Kliknite na ⊞ v stĺpci **Operácia**
2. Zadajte názov zobrazenia
3. Filtrovanie zobrazenia, ak zvolíte hodnotu „contained in" budete mať prístup k celému MIB stromu obsiahnutému v danom OID čísle a ak zvolíte hodnotu „outside" budete mať prístup ku všetkým vetvám stromu okrem tých patriace k danému OID číslu
4. Číslo OID pre pohľad



Obrázok 4.99 Konfigurácia zobrazení SNMP

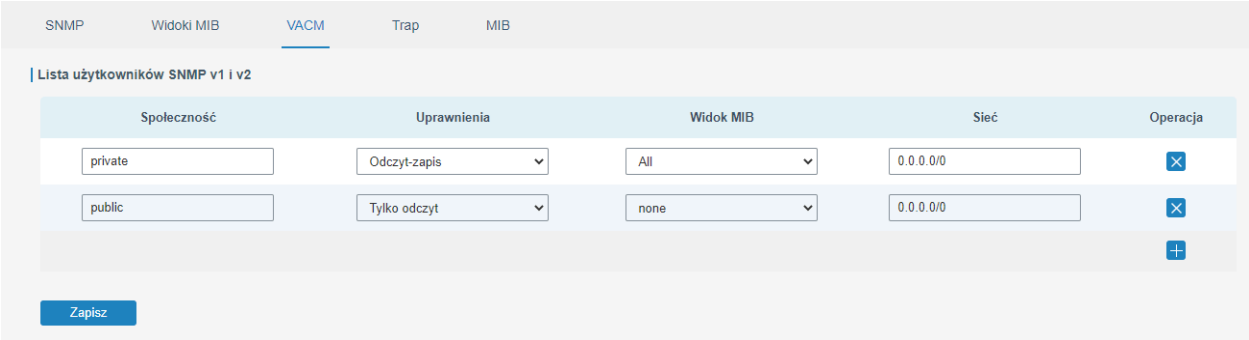
4.3.4.3 VACM

Táto základka sa používa na konfiguráciu komunikácie SNMP pre router. Môže mať dve verzie v závislosti od toho, ktorú verziu protokolu SNMP použijete na karte **SNMP** (časť 4.3.4.1)

Pre SNMPv1/SNMPv2

Vo verziách SNMPv1 / v2 tu môžete nakonfigurovať, ktoré **komunity** budú mať prístup ku ktorým zobrazeniam stromu MIB (časť 4.3.4.2). Ak chcete pridať komunitu, urobte nasledovné:

1. Kliknite na + v stĺpci **Operácia**
2. Zadajte názov komunity
3. Nastavte úroveň prístupu pre komunitu, môžeme nastaviť oprávnenia na čítanie dát (iba na čítanie) alebo čítanie a zmenu nastavení (čítanie-zápis)
4. Určite, ku ktorému zobrazeniu bude mať komunita prístup
5. Nastavte IP adresu (so skráteným zadaním masky podsiete) zariadenia, ktoré bude mať prístup do danej komunity, ak zadáte 0.0.0.0/0, každé zariadenie bude mať prístup do komunity
6. Po zadaní všetkých údajov kliknite na tlačidlo **Uložiť**



Obrázok 4.100 Konfigurácia záložky VACM pre SNMPv1 a SNMPv2

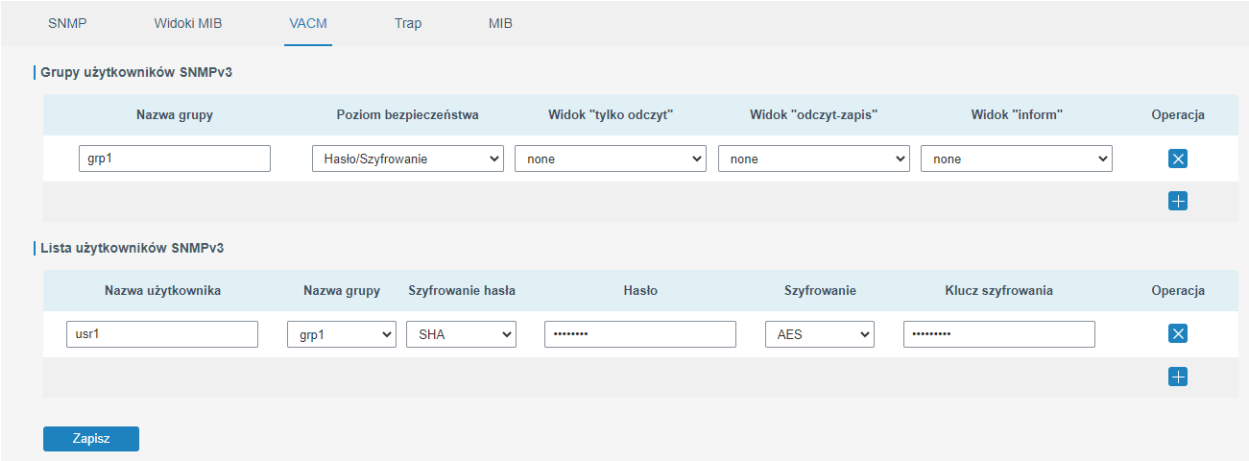
Pre SNMPv3

Vo verzii SNMPv3 tu môžete pridávať používateľov a následne ich priraďovať ku konkrétnym skupinám povolení. Ak chcete pridať skupinu povolení, musíte urobiť nasledovné kroky:

1. 1. Kliknite na + v **Skupine používateľov SNMPv3**
2. 2. Zadajte názov skupiny
3. 3. Vyberte spôsob autorizácie k zariadeniu (úroveň zabezpečenia); to bude mať vplyv na to, aké údaje budete musieť zadať pri vytváraní používateľa na autorizáciu a šifrovanie
4. 4. Vyberte zobrazenie, ku ktorému má skupina prístup z hľadiska nastavení čítania (**zobrazenie „zápis“**)
5. 5. Vyberte zobrazenie, ku ktorému má skupina prístup z hľadiska nastavení čítania a úprav (**zobrazenie „čítanie a zápis“**)
6. 6. Vyberte, ku ktorému zobrazeniu má skupina prístup v poli správ Inform (**Zobraziť „Inform”**)
7. 7. Kliknite na tlačidlo **Uložiť**

Ak chcete pridať používateľa, musíte urobiť nasledujúce kroky:

1. Kliknite na + v **Skupine používateľov SNMPv3**
2. Zadajte meno používateľa
3. Vyberte skupinu, do ktorej má používateľ patriť
4. Vyberte metódu šifrovania hesla, táto možnosť je dostupná, ak má skupina, do ktorej používateľ patrí, v poli Úroveň zabezpečenia vybraté možnosti „Auth / NoPriv" alebo „Auth / Priv"
5. Zadajte heslo používateľa (ak sa vyžaduje)
6. Vyberte spôsob šifrovania paketov, táto možnosť je dostupná, ak má skupina, do ktorej používateľ patrí, v poli Úroveň zabezpečenia vybratú možnosť „Auth / Priv"
7. Zadajte heslo na šifrovanie balíka (ak sa vyžaduje)
8. Kliknite na tlačidlo **Uložiť**

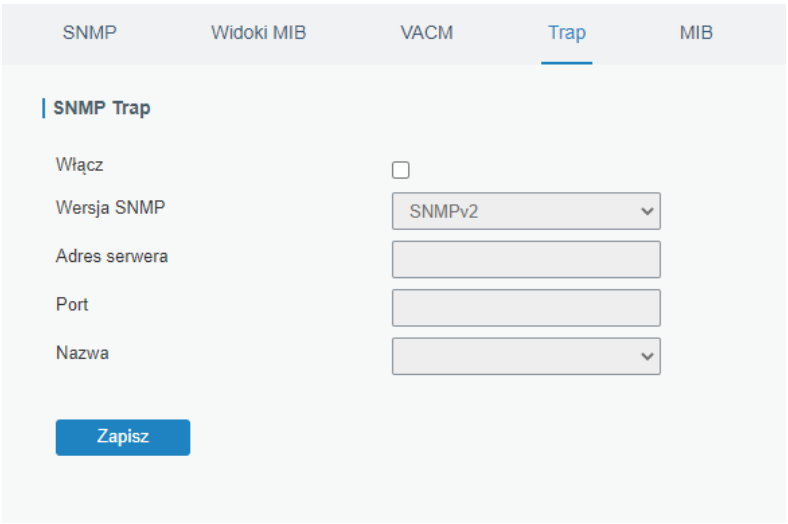


Obrázok 4.101 Konfigurácia záložky VACM pre SNMPv3

4.3.4.4 Trap

V tejto záložke môžete nakonfigurovať funkciu Trap pre SNMP, t.j. odosielanie upozornení o zmenách v konfigurácii na zariadenie, ktoré je SNMP serverom. Ak chcete nakonfigurovať túto službu, musíte urobiť nasledovné kroky:

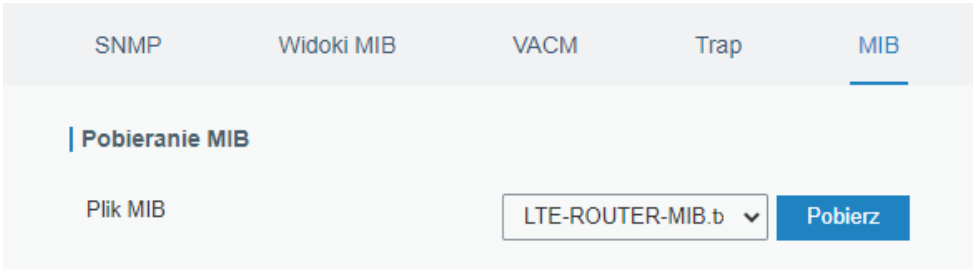
1. Povoľte službu (**Povoliť**)
2. Vyberte verziu SNMP, pre ktorú sa má služba spustiť
3. Zadajte adresu servera
4. Zadajte port, na ktorom beží služba na serveri
5. Ak si vyberiete verziu SNMPv3, mali by ste si dodatočne vybrať používateľa, s ktorým budeme službu obsluhovať a spôsob jeho autorizácie



Obrázok 4.102 Konfigurácia záložky SNMP Trap

4.3.4.5 MIB

V tejto záložke si môžete stiahnuť súbor MIB. Ak to chcete urobiť, vyberte súbor, ktorý chcete stiahnuť, a potom kliknite na tlačidlo **Stiahnuť.**



Obrázok 4.103 Záložka MIB

4.3.5 AAA

V tejto záložke môžete nakonfigurovať model AAA (AuthenticationAuthorization Accounting). Model AAA slúži na kontrolu používateľov, ktorí sa pokúšajú prihlásiť do zariadenia a v prípade správnej identifikácie kontroluje, ku ktorým službám má používateľ prístup a následne hlási ich prácu na zariadení. Tento model môže byť založený na lokálnej databáze užívateľov alebo na autentifikačných serveroch.
Model funguje v troch moduloch:

1. Autentifikácia – kontroluje, či má používateľ oprávnenie na prístup k zariadeniu
2. Autorizácia – kontroluje, ku ktorým službám má používateľ prístup
3. Hlásenie – hlási operácie vykonané používateľom

4.3.5.1 Radius

V tejto záložke môžete konfigurovať prístup k autentizačnému serveru Radius.
Ak chcete nakonfigurovať pripojenie, postupujte nasledovne:

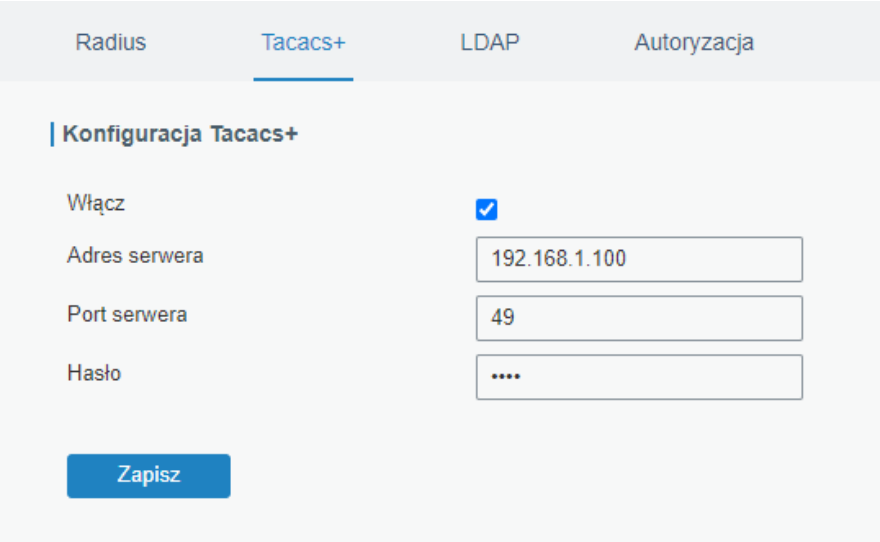
1. Aktivujte službu
2. Zadajte IP adresu servera
3. Zadajte port, na ktorom server počúva
4. Zadajte komunikačný šifrovací kľúč
5. Kliknite na tlačidlo **Uložiť**

Obrázok 4.104 Konfigurácia modelu AAA server Radius

4.3.5.2 Tacacs+

V tejto záložke môžete konfigurovať prístup k overovaciemu serveru Tacacs +
Ak chcete nakonfigurovať pripojenie, postupujte nasledovne:

1. Aktivujte službu
2. Zadajte IP adresu servera
3. Zadajte port, na ktorom server počúva
4. Zadajte komunikačný šifrovací kľúč
5. Kliknite na tlačidlo **Uložiť**

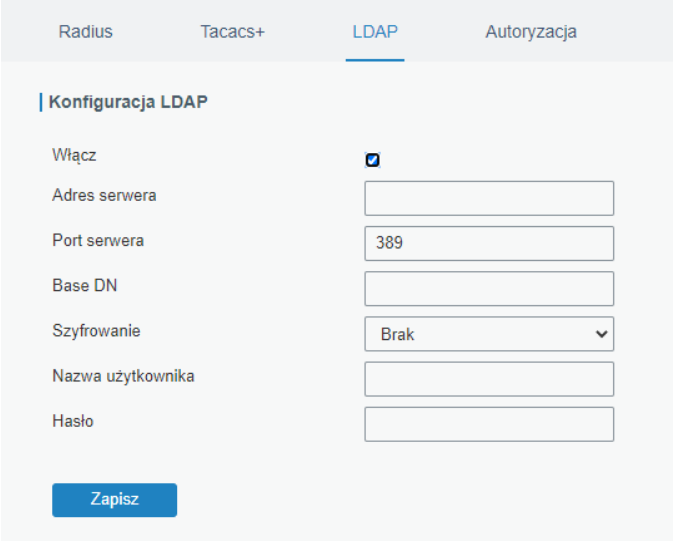


Obrázok 4.105 Konfigurácia modelu AAA server TACACS+

4.3.5.3 LDAP

V tejto záložke môžete konfigurovať prístup k LDAP autentifikačnému serveru.
Ak chcete nakonfigurovať pripojenie, postupujte nasledovne:

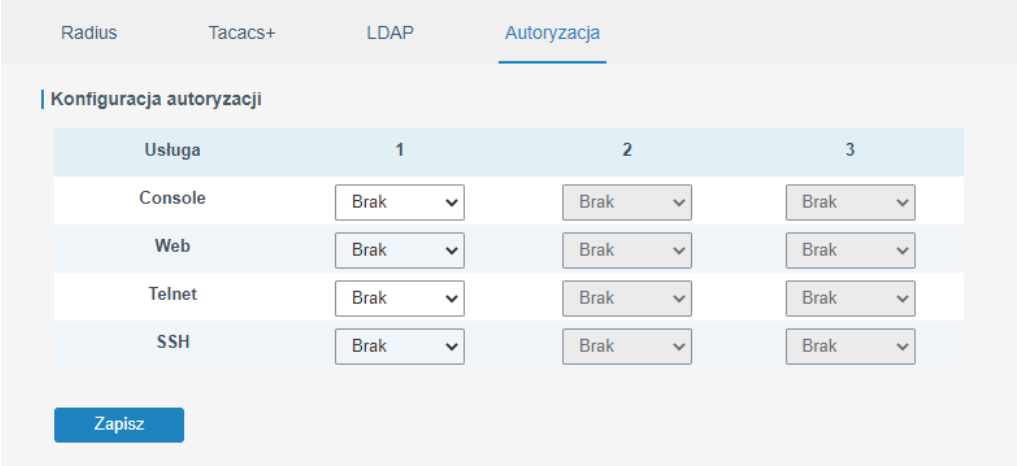
1. Aktivujte službu
2. Zadajte IP adresu servera
3. Zadajte port, na ktorom server počúva
4. Zadajte **Base DN** (mali by ste ho získať od správcu servera)
5. Vyberte spôsob šifrovania komunikácie so serverom
6. Poskytnite serveru používateľské meno
7. Zadajte heslo servera
8. Kliknite na tlačidlo **Uložiť**



Obrázok 4.106 Konfigurácia modelu AAA server LDAP

4.3.5.4 Autorizácia

V tejto záložke môžete nastaviť služby, ku ktorým budú mať prístup používatelia autentifikovaní konkrétnymi servermi (databázami). Môžete si vybrať žiadnu databázu, lokálnu databázu alebo použiť externé databázy, ktoré uchovávajú informácie o užívateľoch (RADIUS, TACACS + alebo LDAP). Ak službe priradíme tri typy autentifikácie, priorita používania databázy bude nasledovná: 1> 2> 3.



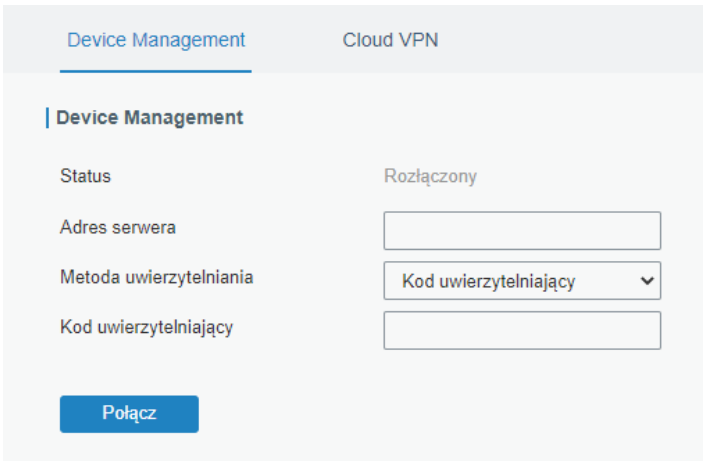
Obrázok 4.107 Konfigurácia modelu AAA záložka Autorizácia

4.3.6 Diaľkové riadenie

4.3.6.1 Device Managment

V tejto záložke môžete nakonfigurovať pripojenie k centralizovanému systému správy zariadení s názvom DeviceHub. Ak chcete správne nakonfigurovať pripojenie, pozrite si dokumentáciu výrobcu softvéru. Prvou položkou na karte je stav pripojenia k serveru DeviceHub (**Status**).
Ak chcete nakonfigurovať pripojenie smerovača k systému, postupujte nasledovne:

1. Zadajte IP adresu servera, na ktorom je spustený DeviceHub
2. Vyberte metódu autentifikácie
3. Ak vyššie vyberieme možnosť „autentifikačný kód“, zadajte overovací kód
4. Ak vyberiete možnosť „účet“, zadajte svoje používateľské meno a heslo
5. Kliknite na tlačidlo **Uložiť**

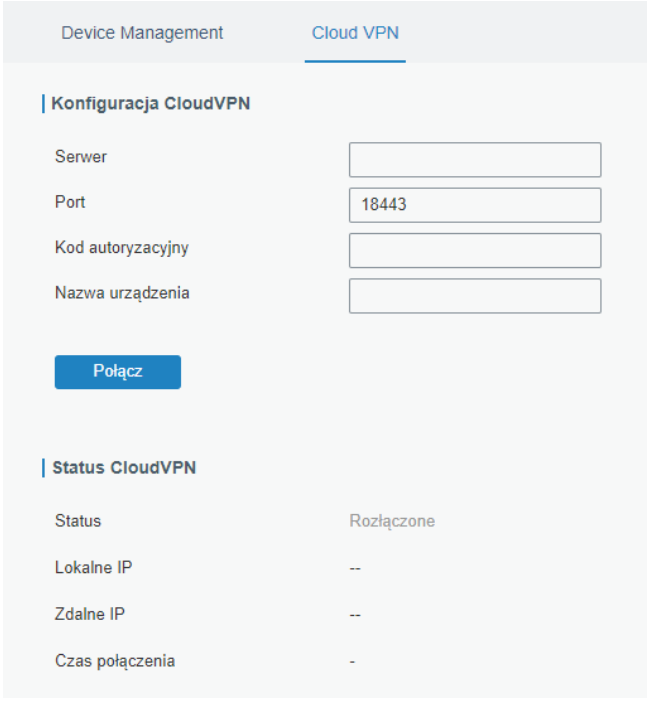


Obrázok 4.108 Záložka Diaľkové riadenie, konfigurácia pripojenia k DeviceHub

4.3.6.2 Cloud VPN

V tejto záložke môžete nakonfigurovať pripojenie k serveru CloudVPN. Ak chcete správne nakonfigurovať pripojenie, pozrite si dokumentáciu výrobcu softvéru.
Ak chcete nakonfigurovať pripojenie na strane smerovača, postupujte nasledovne:

1. Zadajte IP adresu servera CloudVPN
2. Port, na ktorom server počúva
3. Kód oprávňujúci pripojenie
4. Názov zariadenia v systéme
5. Kliknite na tlačidlo **Pripojiť**



Obrázok 4.109 Konfigurácia pripojenia CloudVPN

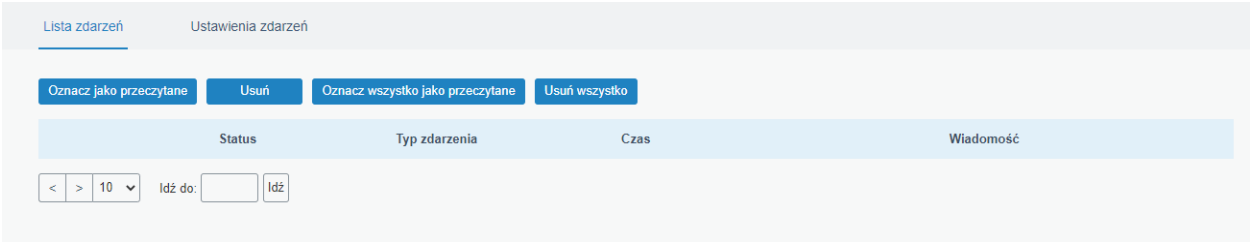
V skupine **Stav služby** môžete čítať stav pripojenia k serveru, virtuálnu IP, virtuálnu IP servera CloudVPN, čas, kedy je router pripojený k službe.

Obrázok 4.110 Status pripojenia CloudVPN

4.3.7 Udalosti

4.3.7.1 Zoznam udalostí

V tejto záložke si môžeme prečítať všetky alarmy, ktoré si zvolíme zaznamenať v záložke **Nastavenia udalostí** (časť 4.3.7.2). Pomocou príslušných tlačidiel môžeme: označiť vybranú udalosť ako prečítanú, zmazať vybranú udalosť, označiť všetky udalosti ako prečítané, zmazať všetky udalosti.

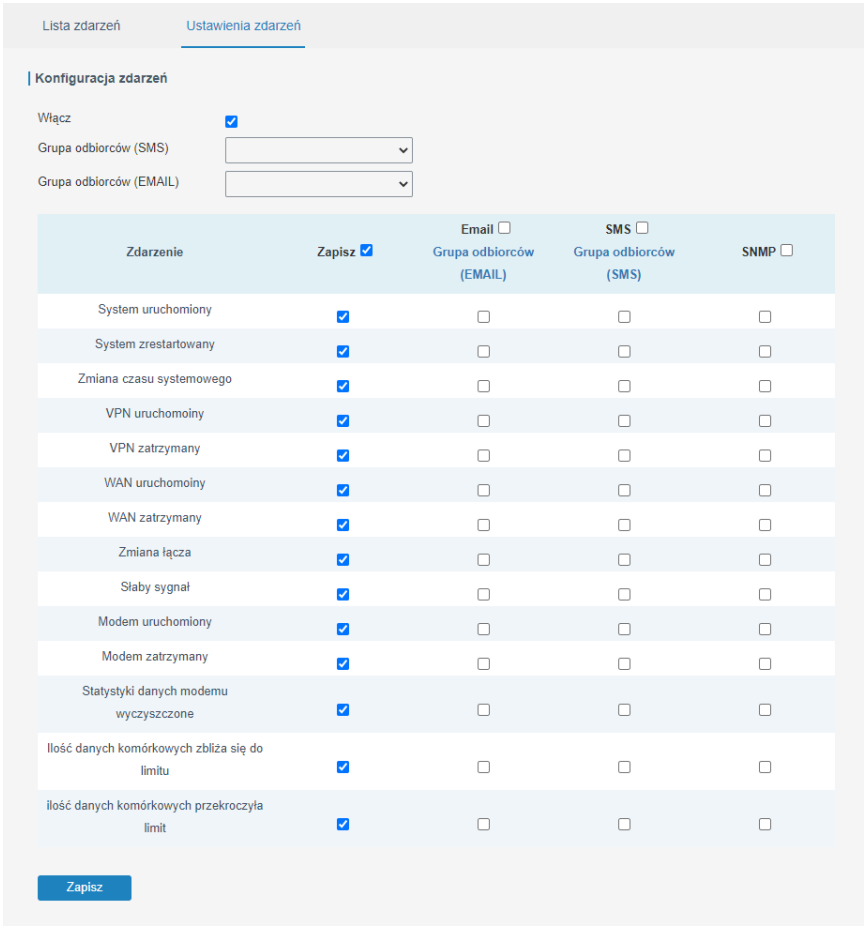


Obrázok 4.111 Záložka Zoznam udalostí

4.3.7.2 Nastavenia udalostí

V tejto záložke môžete nastaviť, aké udalosti z prevádzky zariadenia sa budú zaznamenávať a akým spôsobom budú hlásené. V predvolenom nastavení služba hlási všetky udalosti lokálne, ale po vhodnej konfigurácii môžeme prijímať e-mailové upozornenia, SMS správy alebo udalosti SNMP Trap.
Aby odosielanie udalosti fungovalo, je potrebné, postupujte nasledovne:

1. V tabuľke udalostí vyberte, aké udalosti sa majú daným spôsobom hlásiť
2. Vyberte skupinu telefónnych čísel, na ktoré sa má SMS správa odoslať (konfigurácia telefónnych skupín v časti 4.3.2.1).
3. Vyberte skupinu e-mailových adries, na ktoré sa majú posielať e-mailové správy (konfigurácia skupín e-mailových adries v časti 4.3.1.3).
4. Ak chcete hlásiť udalosti SNMP Trap, nakonfigurujte protokol SNMP v časti 4.3.4
5. Kliknite na tlačidlo **Uložiť**



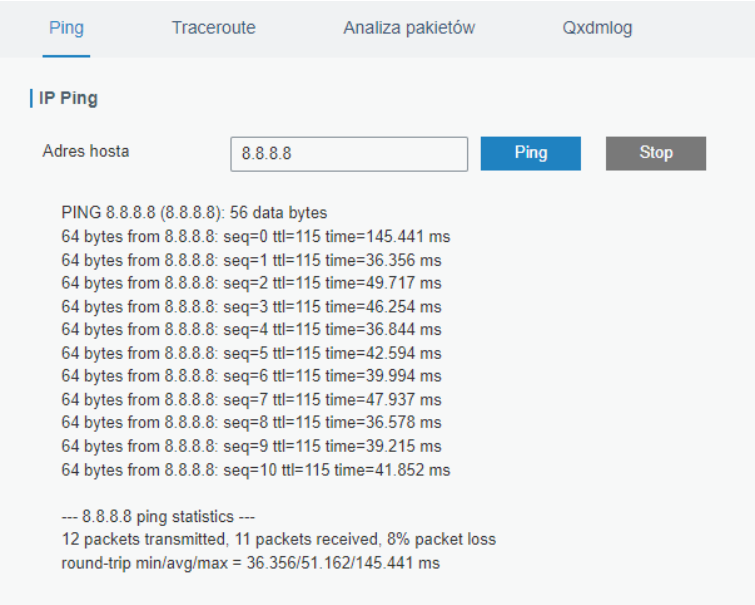
Obrázok 4.112 Konfigurácia záložky Nastavenia udalostí

4.4 ÚDRŽBA

4.4.1 Nástroje

4.4.1.1 Ping

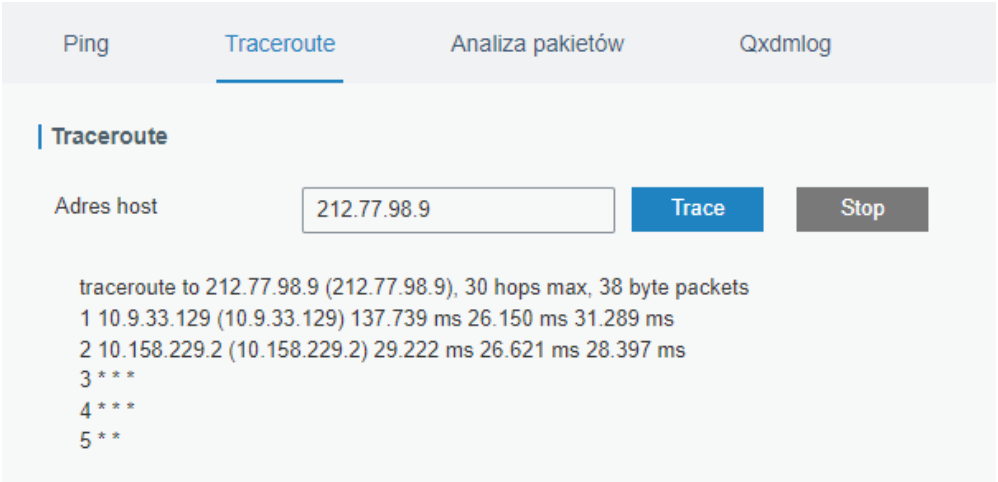
Záložka Ping umožňuje vyvolať príkaz Ping, ktorým môžete skontrolovať, napríklad, či zariadenie s danou IP komunikuje s routerom. Ak chcete vykonať takýto test, zadajte adresu IP zariadenia a potom kliknite na tlačidlo **Ping**. Príkaz sa bude vykonávať dovtedy, kým nestlačíte tlačidlo **Stop**.



Obrázok 4.113 Funkcia Ping

4.4.1.2 Traceroute

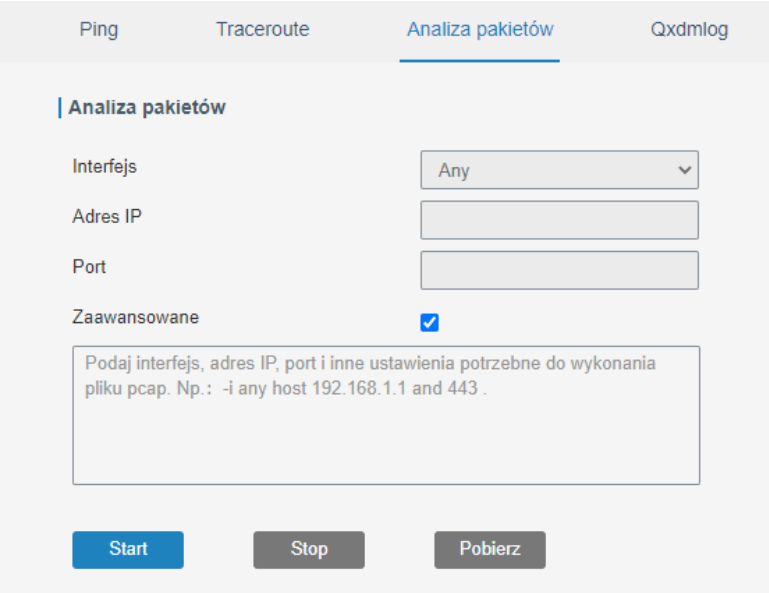
Táto funkcia vám umožňuje vyvolať príkaz Traceroute, ktorý je zodpovedný za zobrazenie cesty, ktorou musia pakety prejsť z daného zariadenia, aby sa dostali k zariadeniu špecifikovanému v poli **Adresa hostiteľa**. Pre vykonanie tohto príkazu zadajte IP adresu a následne kliknite na tlačidlo **Trace**, funkciu môžeme počas práce zastaviť kliknutím na tlačidlo **Stop**, avšak po zobrazení celej trasy sa funkcia automaticky zastaví.



Obrázok 4.114 Funkcia Traceroute

4.4.1.3 Analýza paketov

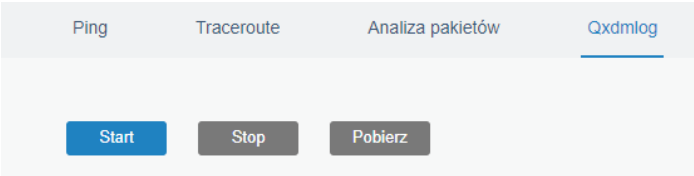
Pomocou tejto funkcie môžeme analyzovať paketovú prevádzku na danom rozhraní smerovača. Ak chcete vykonať takúto analýzu, vyberte rozhranie, ktoré chcete skontrolovať, potom voliteľne zadajte IP a port, ktorý chcete skontrolovať, a kliknite na tlačidlo **Start**. Všetka sieťová prevádzka sa uloží do súboru PCAP, ktorý je možné otvoriť napríklad pomocou softvéru Wireshark. Ak chcete zastaviť zaznamenávanie sieťovej prevádzky, kliknite na tlačidlo **Stop**. Stiahnite si vytvorený súbor pomocou tlačidla **Stiahnuť**. Pomocou funkcie **Advanced** môžeme manuálne zadať pravidlo iptables, ktoré vyfiltruje návštevnosť, ktorá nás zaujíma a uloží ju do súboru.



Obrázok 4.115 Funkcia Analýza paketov

4.4.1.4 Qxdmlog

V tejto záložke môžete vytvoriť log súbor v štandarde QXDM, ktorý si následne môžeme stiahnuť na disk a analyzovať pomocou príslušného softvéru. Pre vytvorenie takéhoto súboru kliknite na tlačidlo **Start**, počkajte časový úsek, ktorý vás zaujíma, a potom kliknite na tlačidlo **Stop**, stiahnite si takto pripravený súbor pomocou tlačidla **Stiahnuť**.

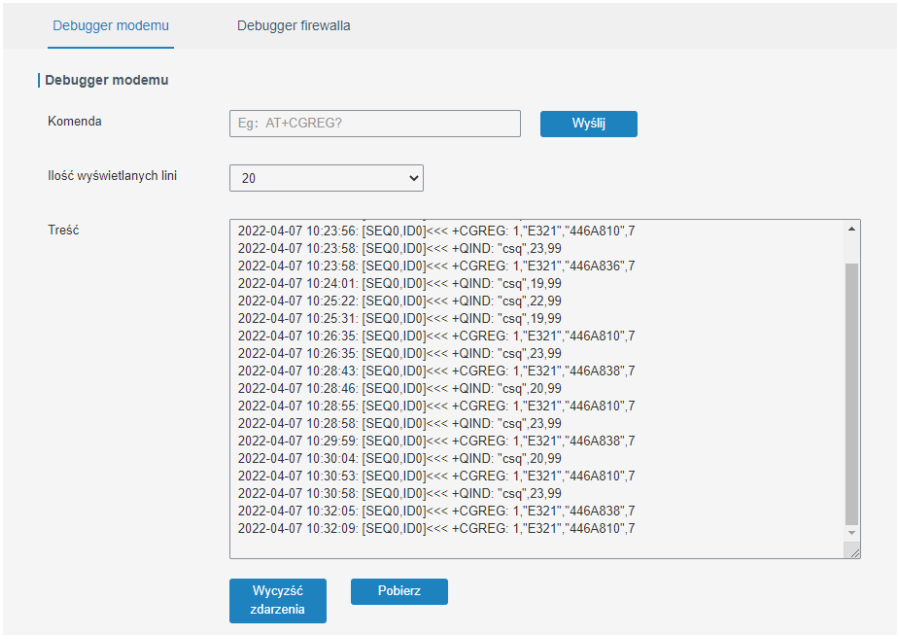


Obrázok 4.116 Funkcia QXDMlog

4.4.2 Debugger

4.4.2.1 Debbuger modemu

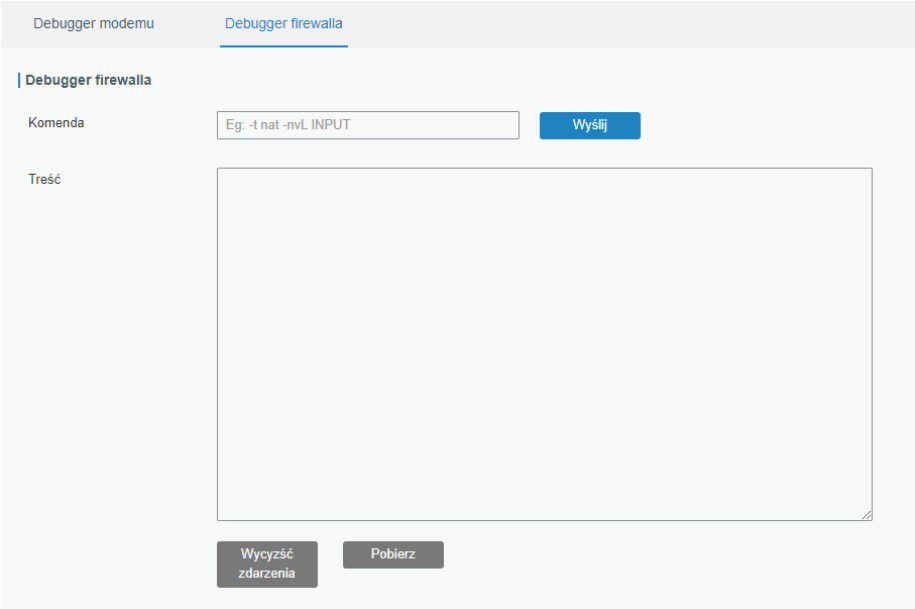
Na tejto karte môžete čítať protokoly týkajúce sa GSM modemu a tiež odosielať AT príkazy do modemu. Voľba **Počet zobrazených riadkov** umožňuje nastaviť, koľko riadkov sa zobrazí v okne Obsah. Okrem toho môže pomocou tlačidla **Stiahnuť** stiahnuť súbor denníka zodpovedný za modem GSM a tiež vymazať denníky. V pravom dolnom rohu môžeme nastaviť predvolený čas obnovenia okna denníka.



Obrázok 4.117 Funkcia Debugger modemu

4.4.2.2 Debugger firewallu

V tejto záložke môžete čítať protokoly súvisiace s prevádzkou brány firewall v routeri a tiež odosielať príkazy iptables do modulu brány firewall. Okrem toho si môžete stiahnuť súbor denníka brány firewall pomocou tlačidla **Stiahnuť** a vyčistiť protokoly pomocou tlačidla **Vymazať**

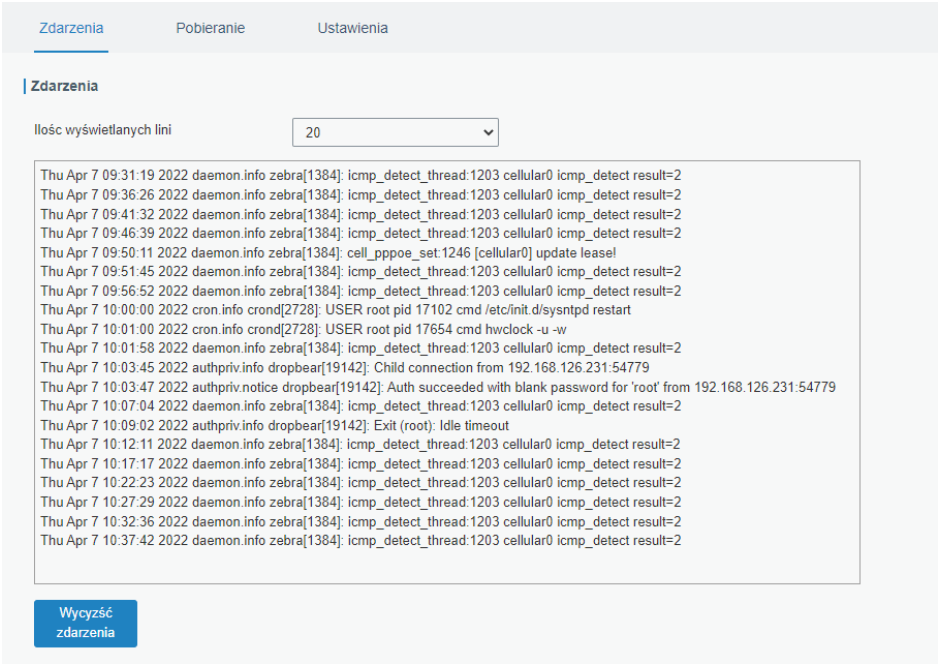


Obrázok 4.118 Funkcia Firewall Debugger

4.4.3 Systémový denník

4.4.3.1 Udalosti

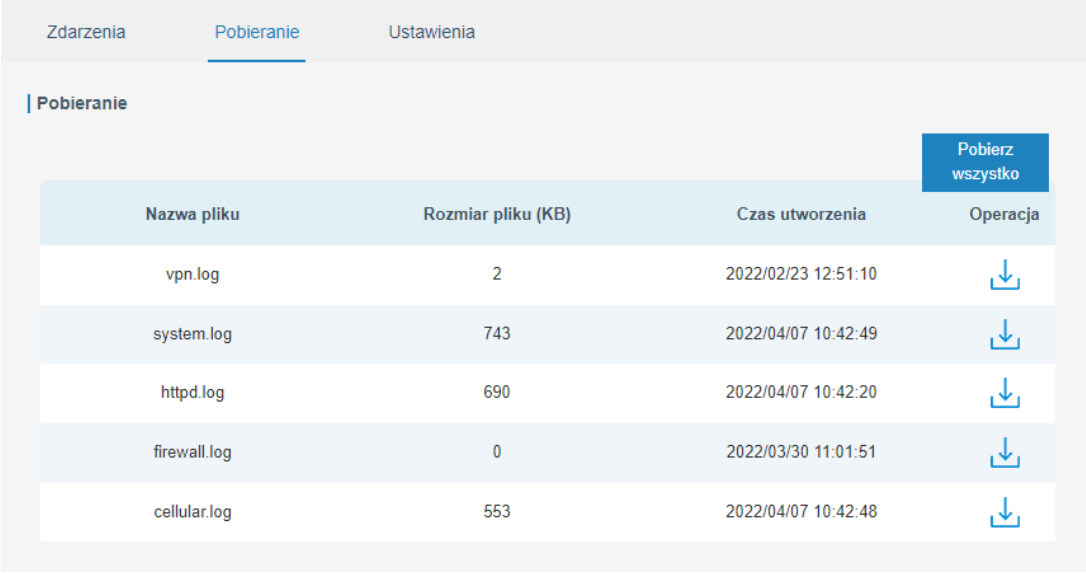
Táto záložka zobrazuje všetky systémové denníky. Pomocou položky **Počet zobrazených riadkov** môžete nastaviť počet riadkov, ktoré sa budú zobrazovať v okne denníka. V pravom dolnom rohu môžeme nastaviť, ako často sa má okno s protokolmi obnovovať, pričom tlačidlo **Clear** slúži na vymazanie okna protokolov.



Obrázok 4.119 Funkcia udalostí

4.4.3.2 Sťahovanie

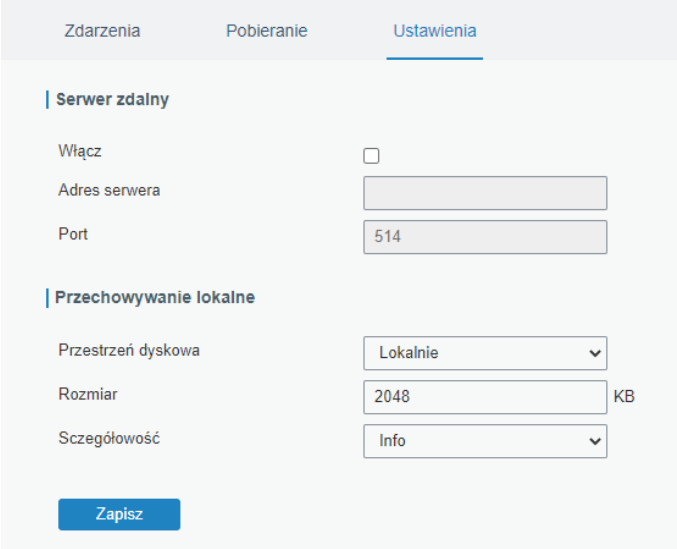
V tejto záložke si môžete stiahnuť protokolové súbory



Obrázok 4.120 Funkcja Pobieranie

4.4.3.3 Log Settings

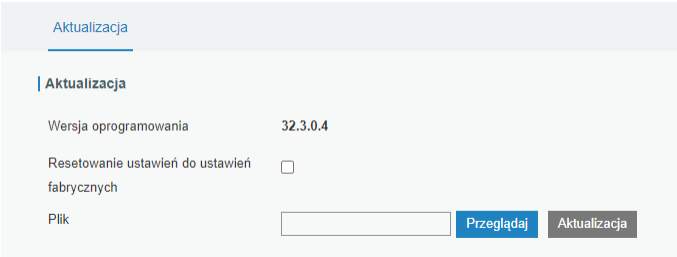
V tejto záložke môžete nakonfigurovať, ako sa budú ukladať systémové protokoly. Na externom serveri môžete ukladať konfiguráciou skupiny **Vzdialený server**, poskytnutím IP adresy takéhoto servera a portu, na ktorom služba počúva protokoly. Okrem toho môžeme definovať maximálnu veľkosť súboru uloženého v lokálnej pamäti zariadenia a typy udalostí, ktoré sa budú v systéme zaznamenávať.



Obrázok 4.121 Funkcia nastavenia

4.4.4 Aktualizácia

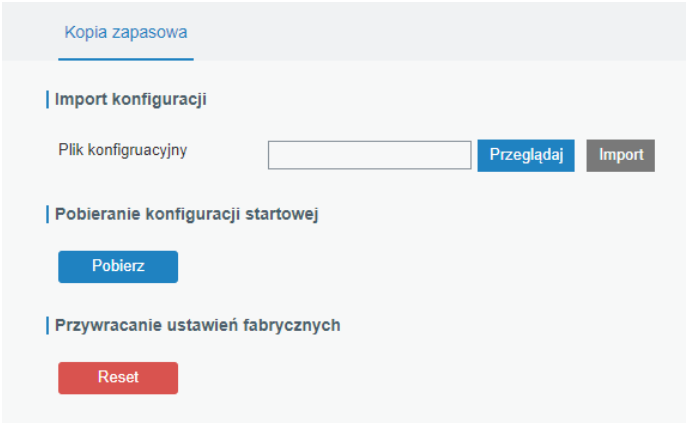
ejto záložke si môžete prečítať verziu softvéru aktuálne nainštalovanú na routeri a aktualizovať softvér. Ak počas aktualizácie vyberiete možnosť **Obnoviť výrobné nastavenia**, celá konfigurácia zariadenia sa obnoví na výrobné nastavenie.



Obrázok 4.122 Funkcja aktualizácia

4.4.5 Zálohovanie

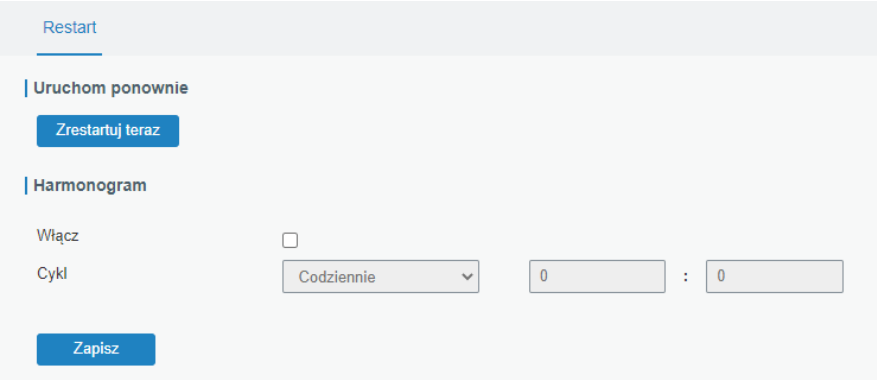
V tejto záložke môžete exportovať alebo importovať nastavenia pre router a resetovať ho na výrobné nastavenia.



Obrázok 4.123 Funkcia zálohovanie

4.4.6 Reštart

V tejto záložke môžete reštartovať zariadenie. Môžete to urobiť okamžite alebo nastaviť jednoduchý plán reštartu v troch rozsahoch: denne, týždenne, mesačne.



Obrázok 4.124 Funkcja restart

UPOZORNENIE!
Pred reštartovaním zariadenia sa uistite, že všetky nastavenia ste uložili pomocou tlačidla **Uložiť** a **potvrdili** v pravom hornom rohu.

5. TECHNICKÁ ŠPECIFIKÁCIA

5.1 TABUĽKA

	BCS-R4G-1W1L
Porty	2x 10/100Mbps; 1x WAN + 1x LAN lub 2x LAN; Full/Half duplex
GSM modul	1x slot na karte SIM 1x SMA
Vybavenie	CPU: ARM Cortex-A7 RAM: 128MB DDR3 Flash: 128MB
Ukazovatele	1x Napájanie 1x Systém 1x SIM 3x Sila signálu
Spotreba energie	štandardne 1,8W; maximálne 2.2W
Výkon	9-48 VDC; 2-pinový PTB konektor PTB 5.08mm
Kryt	Kovový
Rozmery	108 x 90 x 26 mm
Inštalácia	Stolová, nástenná, DIN lišta TH35
Extra ochrana	IP30 Ochrana proti prepätiu Ochrana proti prepólovaniu na napájacom zdroji
Pracovné podmienky	Pracovné: -40 ° C - 60 ° C Skladovanie: -40°C - 85°C Vlhkosť: 0% -95% nekondenzujúca pri 25°C

5.2 SOFTVÉR

	BCS-R4G-1W1L
Sieťové protokoly	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, atď.
VPN	DMVPN, IPsec, OpenVPN, PPTP, L2TP, GRE
DDNS	DynDNS, FreeDNS, 3322, DuckDNS, Oray, No-IP, ChangeIP, EasyDNS, Google, OVH, DnsExit, Sitesolutions, Dynsip, Zoneedit, LoopiaDNS, DHIS, vlastné
Bezpečnosť	Access Control, DMZ, Port Mapping, MAC Binding, SPI Firewalls, DoS&DDoSProtection, Filtering(IP&Domain), IP Passthrough
Ovládanie	Web, CLI, SMS, On-demanddialup, SNMP v1/v2/v3, DeviceHub
AAA	Radius, Tacacs+, LDAP, LocalAuthentication
Typy používateľov	Dva typy úrovní prístupu
Redundancia	VRRP, WAN Failover

5.3 KĽÚČOVÉ VLASTNOSTI

- Spolupráca s mnohými operátormi sietí GSM
- Automatické prepínanie medzi káblovou sieťou a GSM
- CPU v triede NXP
- Odolné puzdro IP30
- Tri možnosti montáže (na stôl, na stenu, na lištu DIN)
- Prevádzka v širokom rozsahu teplôt (-40 °C až 60 °C) a 0-95% nekondenzujúcej vlhkosti
- Vstavané protokoly VPN ako IPsec, OpenVPN, GRE, L2TP, PPTP, DMVPN
- Hardware Watchdog obnovuje plnú funkčnosť po poruchách
- Podpora ACL, DMZ, DDoS ochrana, filtre sieťovej prevádzky, SPI firewall
- Podpora AAA (Radius, TACACS +, LDAP, lokálne overenie)
- Jednoduchá konfigurácia a údržba pomocou DeviceHub, WEB GUI, CLI a SNMP

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

Aktualizácia: 20.04.2022