Skrócona instrukcja obsługi

1. Logowanie na urządzenie

W zależności od sprzętu może to być login: admin bez hasła lub z hasłem, które jest podane przez producenta. Uwaga: zakupione urządzenie jest wstępnie skonfigurowane, czyli do podstawowego używania wystarczy je podłączyć i wszystko powinno działać.

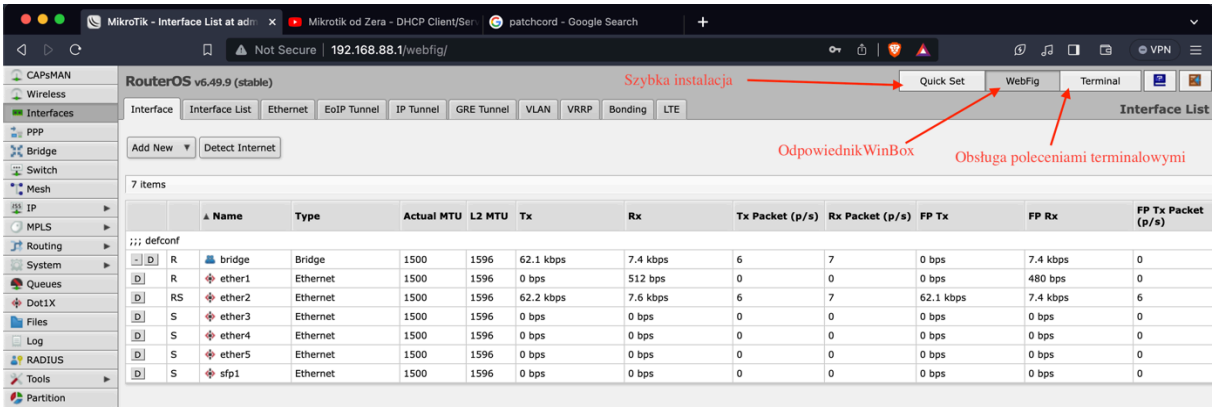
Sposoby logowania:

1. Przez przeglądarkę – zalecam i polecam.
2. Przez wiersz poleceń – warto korzystać tylko do zarządzania urządzeniem.
3. Za pomocą programu WinBox pobieranego ze strony łotewskiego producenta.

(**Uwaga!!! Bardzo ważne: nie wszystkie sprzęty MikroTika można obsłużyć przez *WinBox*. Są takie, które muszą być obsługiwać przez przeglądarkę zgodnie z zaleceniem producenta – należy zapoznać się z instrukcją producenta**).

Aby się zalogować do urządzenia należy podpiąć przewód patchcord RJ45-RJ45 do karty sieciowej komputera oraz do portu nr.2 (koniecznie) w urządzeniu MikroTik.

Ad.1. W celu zalogowania należy w przeglądarce w pasek adresu wpisujemy 192.168.88.1 następnie należy podać login i hasło, jeżeli jest wymagane. Po zalogowaniu mamy dostęp do szybkiej konfiguracji, interfejsu jak w WinBox oraz wiersza poleceń jak w terminalu:



Ad.3. WinBox należy pobrać ze strony producenta. (**Uwaga: Bardzo ważne – nie wszystkie sprzęty MikroTika można obsłużyć przez *WinBox*. Są takie, które muszą być obsługiwać przez przeglądarkę zgodnie z zaleceniem producenta**).

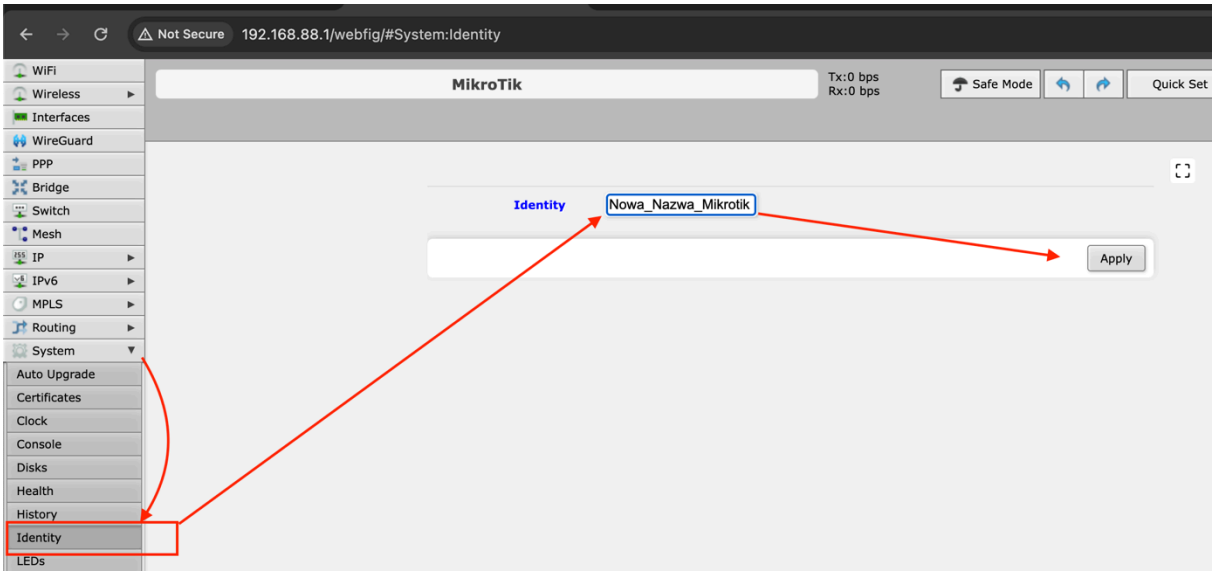
2. Pierwsze logowanie do urządzenia

Po podłączeniu urządzenia do portu ETH2 i zalogowaniu się na konto ***admin*** z hasłem lub bez (zależy od urządzenia) należy zatwierdzić licencję lub ją wpisać, jeżeli się ją posiada oraz ustawić nowe hasło.

O ile to możliwe w czasie konfiguracji należy korzystać ze sposobu Safe Mode:

Safe mode (tryb bezpieczny) - to tryb, w którym, gdy dokonamy zmiany powodującej rozłączenie sesji zarządzającej to wszystkie zmiany jakie wykonywaliśmy od chwili włączenia trybu bezpiecznego zostaną wycofane.

Następnie należy lub się powinno zmieć nazwę urządzenia:



Zmiana nazwy przy pomocy konsoli:

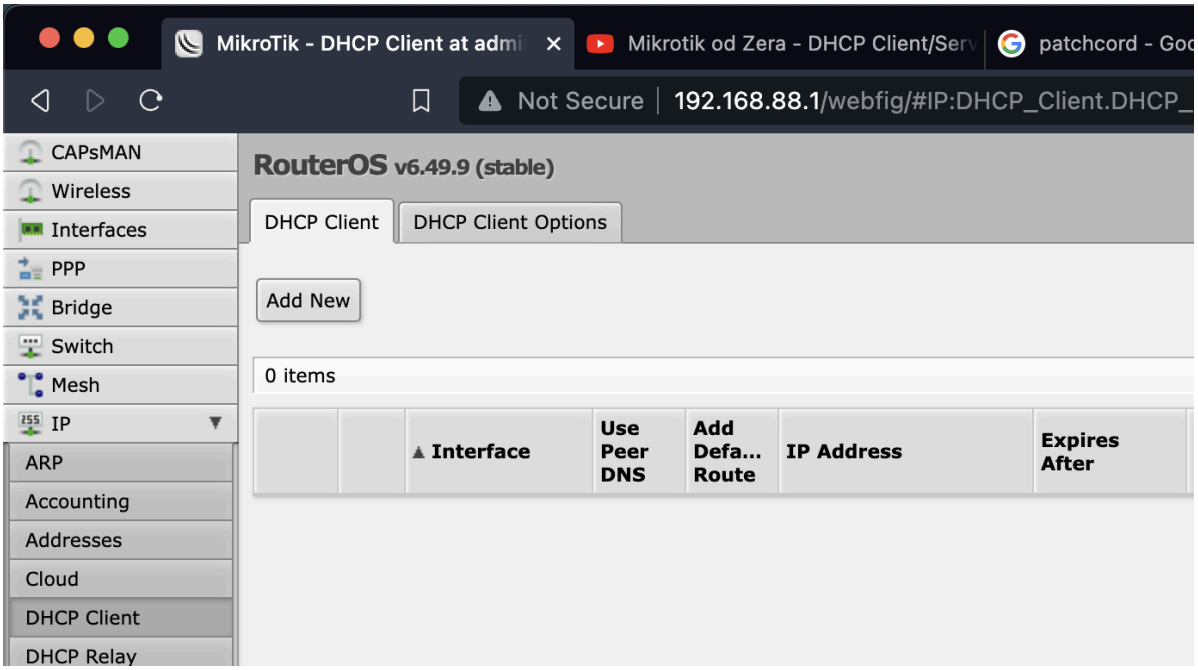
```
[admin@TestMK] /system/identity> set name=MiKrOtIk
[admin@MiKrOtIk] /system/identity>
```

nazwa została zmieniona co widać po zgłoszeniu.

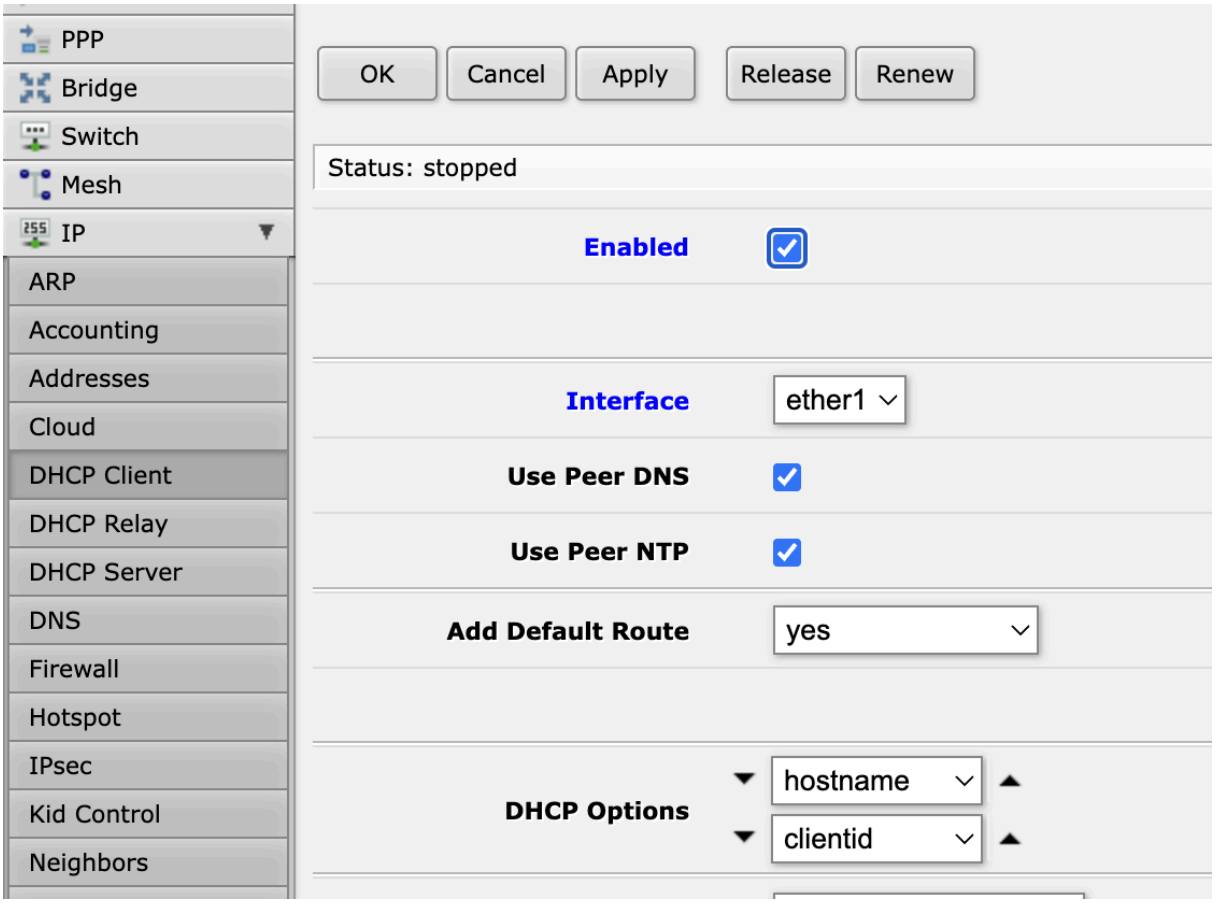
Na tym etapie, aby uzyskać dostęp do Internetu należy podpiąć patchkord RJ45-RJ45 do portu ETH1 oraz do źródła.

3. Pierwsza podstawowa konfiguracja

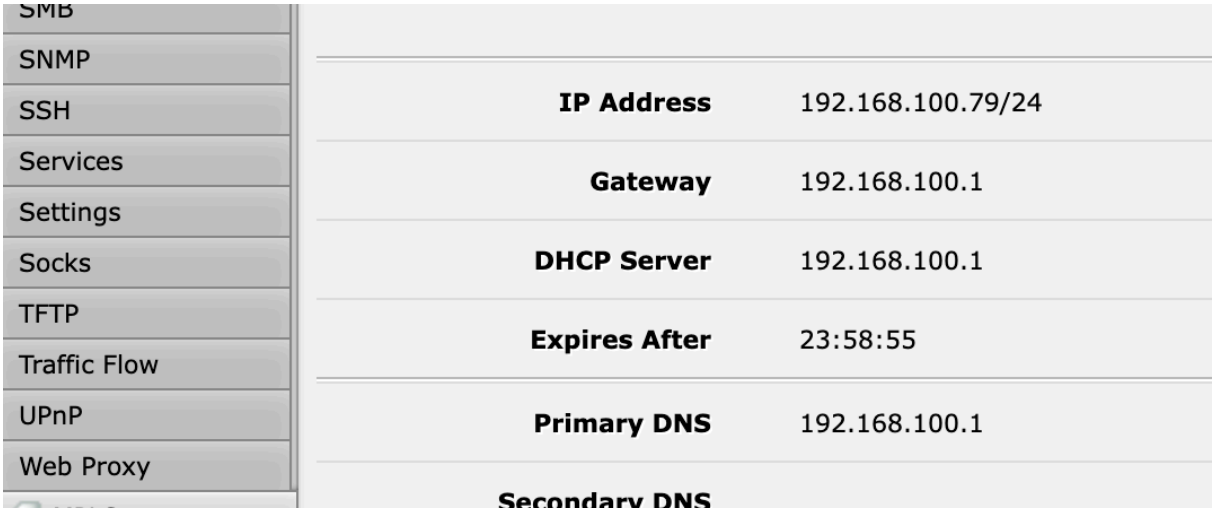
Konfiguracja portu jako portu WAN:
W celu dostarczenia Internetu do urządzenia należy Wejść w zakładkę: IP --> DHCP client



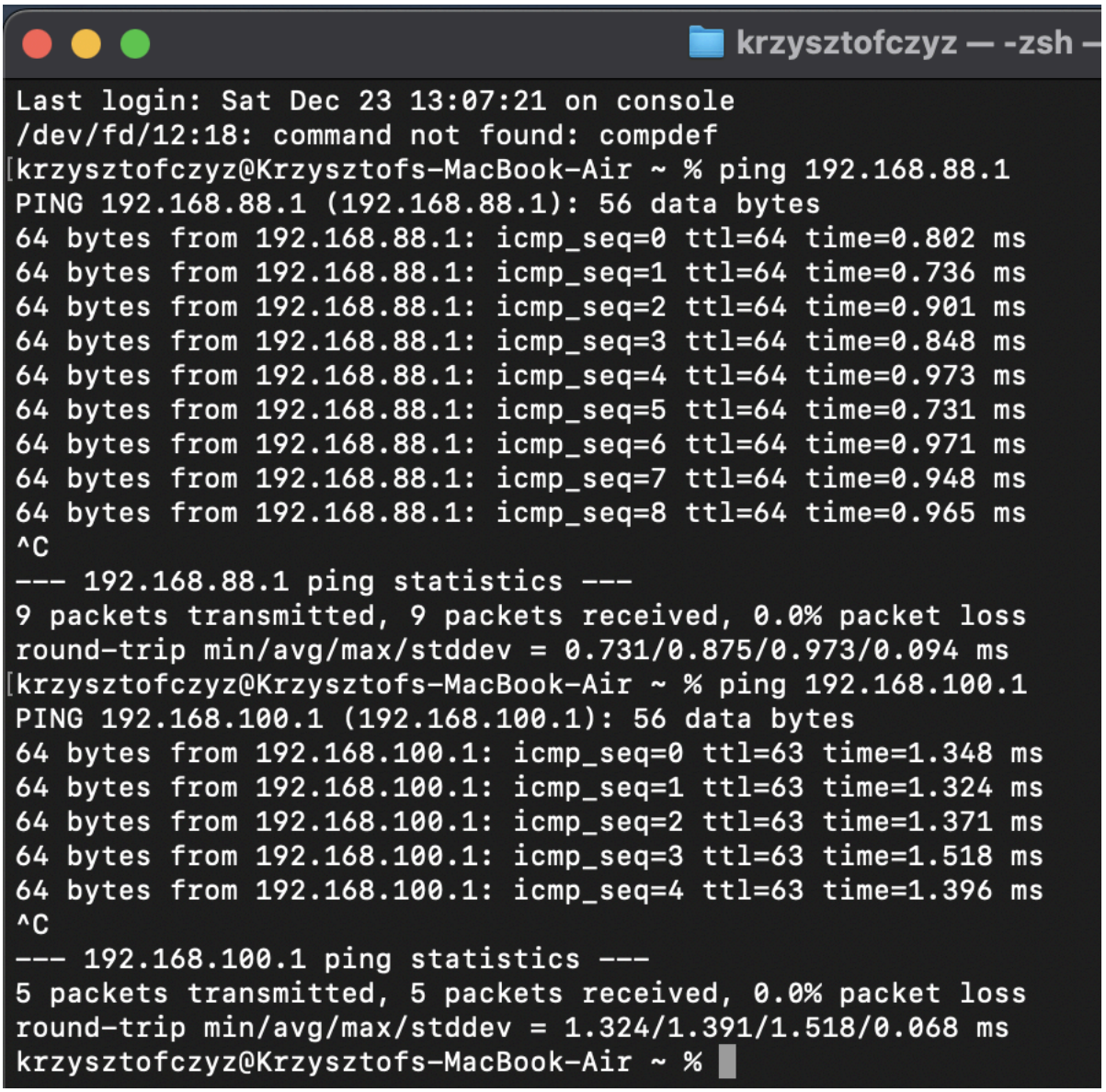
I dodać interfejs, który ma pełnić funkcję wejścia/wyjścia WAN (to samo może dotyczyć wkładki sfp). Ja użyję interfejsu nr.1.. Wybieramy przyciskiem Dodaj nowy i przechodzimy do konfiguracji:



Wybieramy zastosuj/Apply
W statusie powinniśmy zobaczyć adres IP który otrzymaliśmy z zewnątrz.
Np.:



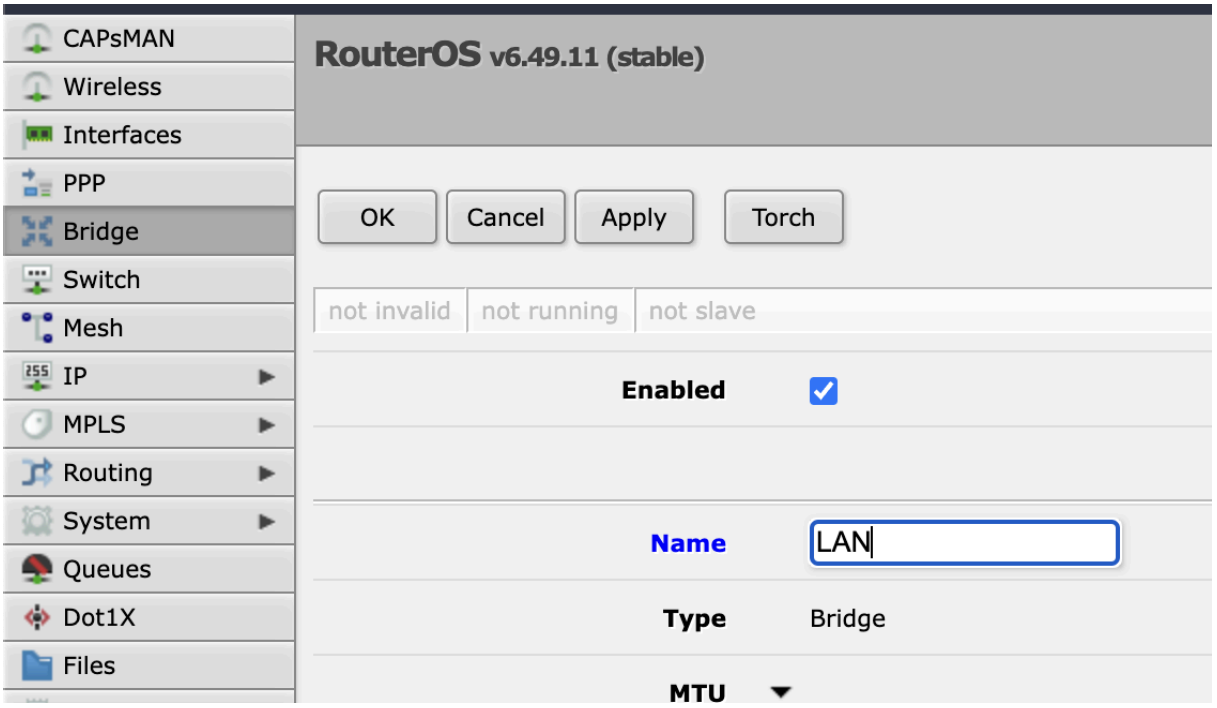
Powinniśmy mieć możliwość pingowania obu interfejsów:



Po wykonaniu tych ustawień urządzenie pracuje jako zwykły router.

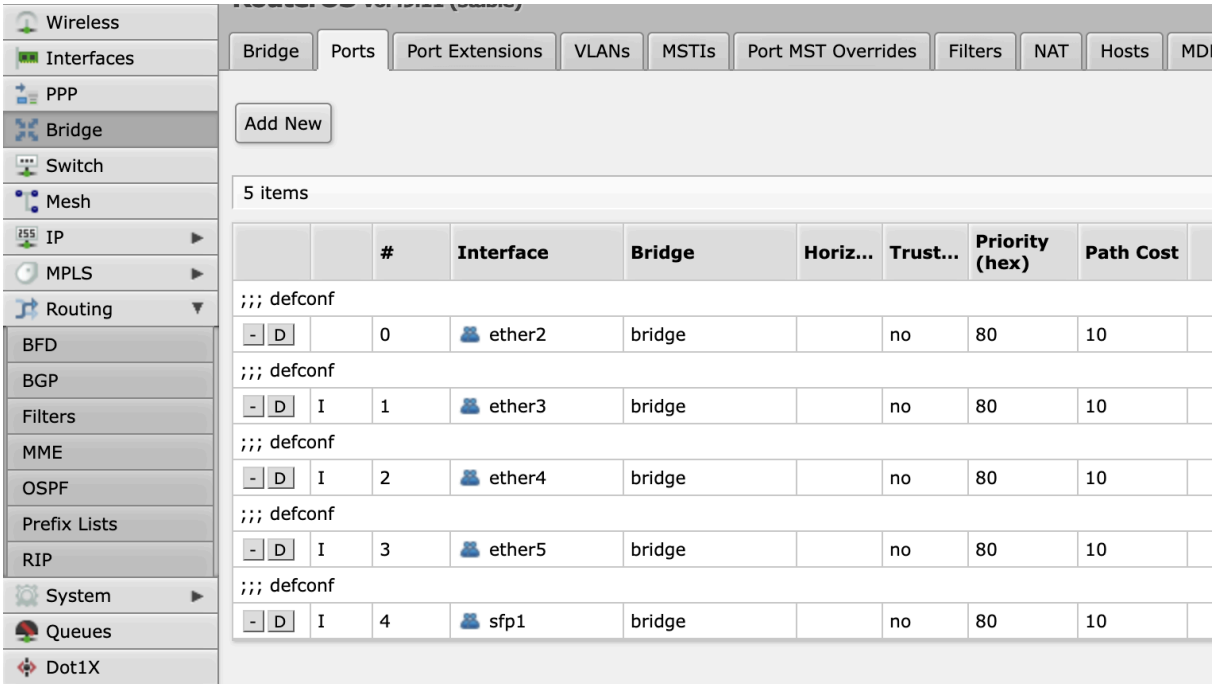
4. Własne ustawienia DHCP.

Po ustawieniu Interfejsu WAN (patrz pkt. 2)m przechodzimy do zakładki Bridge i dodajemy Funkcję mostu z nazwą LAN (robimy to tylko w urządzeniach w których takiej konfiguracji nie ma)



Zatwierdzamy przyciskiem Apply.

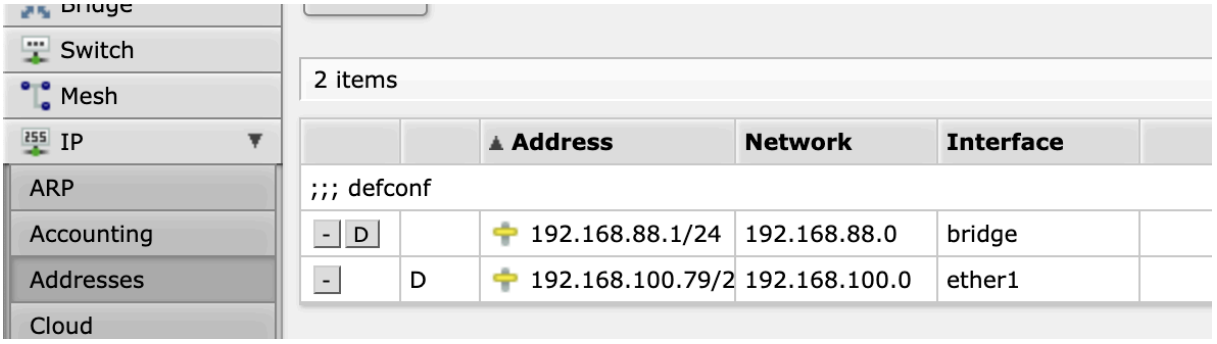
Następnie ustawiamy porty od ETH2-ETH5 w tryb Bridge (o ile nie są ustawione).



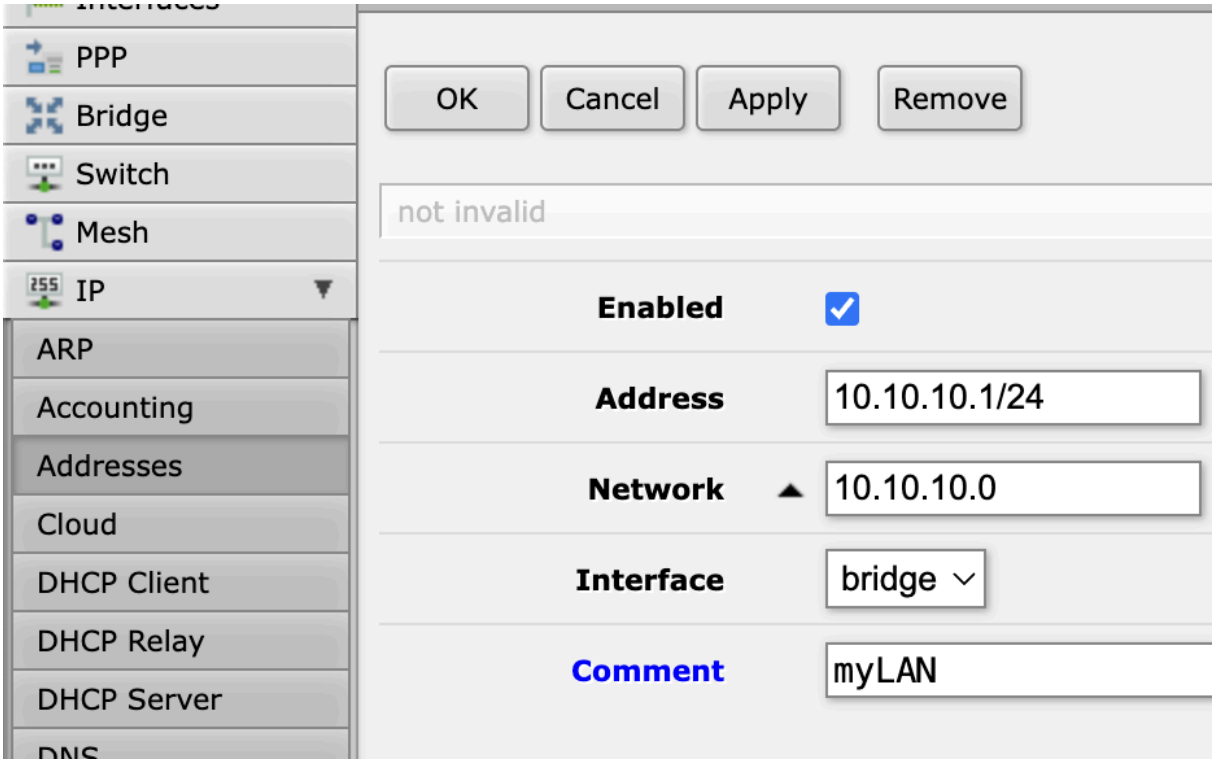
(Uwaga: nie konfigurujemy portu: ether1 - ponieważ pełni on funkcję portu WAN)

Teraz przechodzimy do nadania własnej adresacji. W menu IP wybieramy Addresses i w bridge ustawiamy własną adresację sieci np. 10.10.10.0

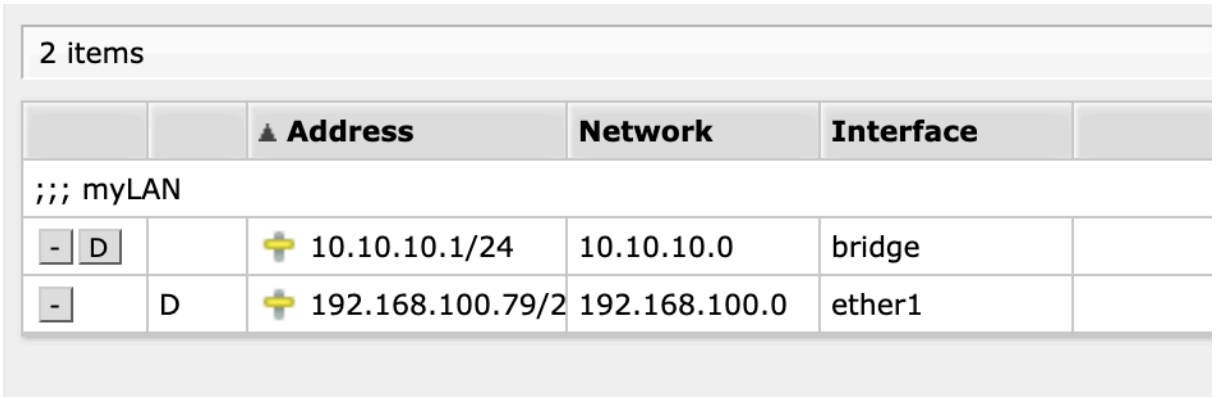
Przed zmianą ustwień:



Zmiana ustawień:



Po zmianie ustawień:



W celu odzyskania interfejsu w przeglądarce wpisujemy nowy adres IP: 10.10.10.1 oraz ponownie się logujemy.

Przechodzimy do ustawień serwera DHCP

5. Reset do ustawień fabrycznych

5.1. Reset za pomocą przycisku RESET

- odłącz urządzenie Mikrotik od wszelkich przewodów (zwłaszcza zasilacza)
- wciśnij i trzymaj wciśnięty przycisk RESET
- podłącz zasilanie z zasilacza
- przytrzymaj przycisk aż dioda zacznie mrugać i następnie zwolnij przycisk aby wyczyścić konfigurację – nie odłączaj zasilania.

(UWAGA: Jeśli zaczekasz, aż dioda LED przestanie migać i dopiero wtedy zwolnisz przycisk - uruchomi się tryb Netinstall, w celu ponownej instalacji RouterOS)

Powinien po resecie i zalogowaniu się pojawić się komunikat (zależnie od urządzenia):

5.2. Reset za pomocą systemu RouterOS

Jeżeli jasz dostęp do swojego routera możesz ustawić fabryczne ustawienia według poniższego sposobu:

- Run the command "/system reset-configuration" from a command-line interface;
- Do it from the System -> Reset Configuration menu in the graphical user interface;

5.3. Reset za pomocą poleceń w konsoli/terminalu:

```
  MMM      MMM       KKK                          TTTTTTTTTTT      KKK
  MMMM    MMMM       KKK                          TTTTTTTTTTT      KKK
  MMM MMMM MMM  III  KKK  KKK  RRRRRR     000000      TTT     III  KKK  KKK
  MMM  MM  MMM  III  KKKKK     RRR  RRR  000  000     TTT     III  KKKKK
  MMM      MMM  III  KKK KKK   RRRRRR    000  000     TTT     III  KKK KKK
  MMM      MMM  III  KKK  KKK  RRR  RRR   000000      TTT     III  KKK  KKK

  MikroTik RouterOS 6.49.9 (c) 1999-2023       http://www.mikrotik.com/

[?]             Gives the list of available commands
command [?]     Gives help on the command and list of arguments

[Tab]           Completes the command/word. If the input is ambiguous,
                a second [Tab] gives possible options

/               Move up to base level
..              Move up one level
/command        Use command at the base level
```

Kolejność poleceń:

? lub F1 lub <tab> - wywołanie poleceń

system - przejście do poleceń systemowych

```
[admin@MikroTik] /system>
[admin@MikroTik] /system> reset-configuration
Dangerous! Reset anyway? [y/N]:
```

==========

POLECENIA TERMINALOWE:

==========

Mikrotik RouterOS – podstawowe komendy z przykładami

Routery Mikrotik stanowią ciekawą alternatywę dla rozwiązań Cisco, za ułamek ich ceny. Możliwości konfiguracyjne są ogromne, routery te pracują na specjalnie przygotowanym do tego celu systemie operacyjnym RouterOS, pochodnym Linuksa. Konfigurację można przeprowadzić na kilka sposobów: poprzez interfejs web, za pomocą specjalnie przygotowanego programu Winbox oraz za pomocą konsoli np. poprzez ssh lub telnet. Najbardziej uniwersalnym i pewnym rozwiązaniem jest Winbox, dający dostęp do routera bez skonfigurowanych adresów IP. W Winbox można pracować w interfejsie graficznym jak i w konsoli. Interfejs graficzny jest wygodny, ale warto poświęcić kilka chwil na zapoznanie się ze składnią poleceń w trybie konsoli. Konfiguracja jest szybsza, prostsza, można przygotować sobie w pliku tekstowym zestaw komend do masowego wdrażania na innych routerach.

Artykuł jest dość długi, więc został podzielony na następujące części:
- Wyświetlenie pomocy i listy dostępnych komend
- Przykład pracy na wielu poziomach komend
- Wyświetlanie informacji o bieżącej konfiguracji
- Zmiana hasła admina
- Całkowity reset ustawień

- Zmiana nazwy routera
- Zegar systemowy
- Dodawanie, edycja i usuwanie adresów IP, interfejsy
- Mostki
- Wbudowany switch
- Konfiguracja WIFI
- DHCP serwer
- DHCP klient
- VLAN
- Routing statyczny
- Routing dynamiczny – OSPF
- Routing dynamiczny RIP
- NAT
- DNS
- Firewall – blokowanie
- Blokowanie przez PROXY

Wyświetlenie pomocy i listy dostępnych komend
[admin@MikroTik] > ? lub 2x TAB
można używać w każdym poziomie komend np: ip address ? [Enter]

Podpowiedzi/uzupełnienia wpisywanych komend – TAB

Przykład pracy na wielu poziomach komend
[admin@MikroTik] > ip [Enter]
[admin@MikroTik] ip > address [Enter]
[admin@MikroTik] ip address > To jest teraz nasz bieżący poziom
[admin@MikroTik] ip address > .. [Enter]
[admin@MikroTik] ip > .. [Enter]
[admin@MikroTik] > najwyższy poziom – root level
[admin@MikroTik] ip address > / [Enter]
[admin@MikroTik] > najwyższy poziom – root level

Wyświetlanie konfiguracji
Wyświetlenie bieżącej konfiguracji interfejsów:
[admin@MikroTik] >interface ethernet print

Wyświetlenie aktualnie zdefiniowanych adresów IP:
[admin@MikroTik] >ip address print

Wyświetlenie tablicy routingu:
[admin@MikroTik] >ip route print

Wyświetlenie ustawionych serwerów DNS:
[admin@MikroTik] >ip dns print

Zmiana hasła admina
[admin@MikroTik] >user set admin password=twoje-haslo

Całkowity reset ustawień (usuwa adresy IP interfejsów! dostęp tylko przez MAC!)
[admin@MikroTik] >system reset-configuration no-defaults=yes

Zmiana nazwy routera
[admin@MikroTik] >system identity set name=Router

Zegar systemowy
Konfiguracja zegara systemowego routera:
[admin@MikroTik] >system clock set time-zone-name=Europe/Warsaw
[admin@MikroTik] >system ntp client set enabled=yes mode=unicast primary-ntp=212.244.36.227 secondary-ntp=212.244.36.228

Dodawanie, edycja i usuwanie adresów IP, interfejsy

Dodanie adresu IP interfejsu:
[admin@MikroTik] >ip address add interface=ether1 address=10.130.0.124 netmask=255.255.0.0 network=10.130.0.0 broadcast=10.130.255.255
lub krócej:
[admin@MikroTik] >ip address add interface=ether1 address=10.130.0.124/16

Zmiana adresu interfejsu (wcześniej print i wtedy wiadomo jaki numer ma interfejs (1)):
[admin@MikroTik] >ip address print
[admin@MikroTik] >ip address set 1 address=192.168.1.20/24

Usunięcie adresu interfejsu (numer z print):
[admin@MikroTik] >ip address remove 1

Zmiana adresu MAC interfesju:
[admin@MikroTik] >interface ethernet set ether1 mac-address=xx.xx.xx.xx.xx

Wyłączenie interfejsu:
[admin@MikroTik] >interface disable ether5

Włączenie interfejsu:
[admin@MikroTik] >interface enable ether1

Nadawanie nazwy interfejsów:
[admin@MikroTik] >interface ethernet set 0 name=WAN
[admin@MikroTik] >interface ethernet set 1 name=eth2
[admin@MikroTik] >interface ethernet set 2 name=eth3
[admin@MikroTik] >interface ethernet set 3 name=eth4
[admin@MikroTik] >interface ethernet set 4 name=eth5
[admin@MikroTik] >interface wireless set 0 name=wlan1

Mostki
Tworzenie mostka:
[admin@MikroTik] >interface bridge add auto-mac=no l2mtu=1594 name=bridge-local protocol-mode=rstp

Dodanie interfejsów do mostka:
[admin@MikroTik] >interface bridge port add bridge=bridge-local interface=wlan1
[admin@MikroTik] >interface bridge port add bridge=bridge-local interface=eth3
[admin@MikroTik] >interface bridge port add bridge=bridge-local interface=eth4

Przypisanie adresu IP mostkowi:
[admin@MikroTik] >ip address add address=192.168.2.1/24 comment="" interface=bridge-local

Wbudowany switch
Konfiguracja, blokowanie portów lub całego switch'a (3 – to numer portu):

[admin@MikroTik] >interface ethernet switch port print

[admin@MikroTik] >interface ethernet switch port set vlan-mode=disabled 3

Konfiguracja WIFI
[admin@MikroTik] >interface wireless set 0 band=2ghz-b/g/n channel-width=20/40mhz-ht-above disabled=no distance=indoors ht-rxchains=0,1 ht-txchains=0,1 l2mtu=2290 mode=ap-bridge ssid=siec_wifi wireless-protocol=any

[admin@MikroTik] >interface wireless security-profiles set default authentication-types=wpa-psk,wpa2-psk eap-methods=passthrough mode=dynamic-keys supplicant-identity=MikroTik wpa-pre-shared-key="moje_tajne_hasło" wpa2-pre-shared-key="moje_tajne_hasło"

DHCP serwer
Tworzenie puli adresów dla DHCP:
[admin@MikroTik] >ip pool add name=default-dhcp ranges=192.168.2.101-192.168.2.130

Konfiguracja serwera DHCP:
[admin@MikroTik] >ip dhcp-server add address-pool=default-dhcp disabled=no interface=bridge-local name=default
[admin@MikroTik] >ip dhcp-server network add address=192.168.2.0/24 comment="" dns-server=192.168.2.1 gateway=192.168.2.1

DHCP klient
Uruchomienie klienta DHCP na porcie WAN:
[admin@MikroTik] >ip dhcp-client add comment="" disabled=no interface=WAN

VLAN
Dodanie VLAN na określonym porcie:
[admin@MikroTik] >interface vlan add interface=eth2 l2mtu=1594 name=”VLAN 10″ vlan-id=10
[admin@MikroTik] >interface vlan add interface=eth2 l2mtu=1594 name=”VLAN 20″ vlan-id=20

Przypisanie VLAN 10 do mostka:
[admin@MikroTik] >interface bridge port add bridge=bridge-local interface=”VLAN 10″

Przypisanie adresu VLAN 20:
[admin@MikroTik] >ip address add address=10.0.2.1/24 interface=”VLAN 20″

Routing statyczny
Dodanie trasy domyślnej 0.0.0.0 (lub innego wpisu sieci)
[admin@MikroTik] >ip route add dst-address=0.0.0.0/0 gateway=10.0.0.1

Usunięcie konkretnej trasy z tablicy routingu (numer z print)
[admin@MikroTik] >ip route remove
numbers: 0

Routing dynamiczny – OSPF
Krok 1 – dodanie i odblokowanie instancji (najlepiej nazwa default, w obu routerach tak samo):

[admin@MikroTik] >routing ospf instance add name=default

Dodanie wirtualnego interfejsu (bridge np. loopback) i nadanie go jako router-id:

[admin@MikroTik] > interface bridge add name=loopback

[admin@MikroTik] > ip address add address=10.255.255.1/32 interface=loopback

[admin@MikroTik] > routing ospf instance set 0 router-id=10.255.255.1

Dodanie fizycznych interfejsów do OSPF (ze zmianą kosztu):

[admin@MikroTik] > routing ospf interface add interface=ether1 cost=10

[admin@MikroTik] > routing ospf interface add interface=ether2 cost=20

Krok 2 – Konfiguracja strefy OSPF (w obu routerach będzie ta sama np. backbone – domyślna):
strefa backbone jest stworzona automatycznie i nie trzeba jej dodawać ponownie

Krok 3 – Dodanie do OSPF sieci, które router ma obsługiwać:

[admin@MikroTik] /routing ospf network> add network=210.13.1.0/28 area=backbone

[admin@MikroTik] /routing ospf network> add network=10.10.1.0/30 area=backbone

[admin@MikroTik] /routing ospf network> add network=10.10.1.4/30 area=backbone

Weryfikacja OSPF
Wyświetlenie informacji o instancjach:

[admin@MikroTik] >routing ospf instance print

Wyświetlenie informacji o rozpoznanych sąsiednich routerach:

[admin@MikroTikR1] >routing ospf neighbor print

Sprawdzenie aktualnej tablicy routingu:

[admin@MikroTik_CE1] > ip route print

Uwaga! Routing dynamiczny wymaga czasu na rozprzestrzenienie się informacji o sieci! Odczekaj minutę od zmian do testów!

Routing dynamiczny RIP
Uaktywnienie protokołu na danym interfejsie:

[MikroTik] routing rip> set redistribute-connected=yes

[MikroTik] routing rip interface> enable ether1

[MikroTik] routing rip interface> print

Dodawanie sąsiadów:

[MikroTik] routing rip neighbour> add address=10.0.0.1

[MikroTik] routing rip neighbour> print

Dodawanie sieci:

[admin@MikroTik] /routing rip network> add network=192.168.20.0/24

NAT
Dodanie SNAT czyli maskarada:
[admin@MikroTik] >ip firewall nat add action=masquerade chain=srcnat out-interface=WAN

DNS
Konfiguracja DNS:
[admin@MikroTik] >ip dns set primary-dns=8.8.8.8

Firewall – blokowanie
Blokowanie stron po adresie IP:
/ip firewall filter
add action=drop chain=forward comment=”Blokowanie IP Facebook” dst-address=74.119.76.0/22
add action=drop chain=forward comment=”Blokowanie IP Facebook” dst-address=173.252.64.0/18
add action=drop chain=forward comment=”Blokowanie IP Facebook” dst-address=204.15.20.0/22
add action=drop chain=forward comment=”Blokowanie IP Facebook” dst-address=66.220.144.0/20
add action=drop chain=forward comment=”Blokowanie IP Facebook” dst-address=69.171.224.0/19

Blokowanie stron w warstwie 7:

Przykładowa konfiguracja dla youtube:
/ip firewall layer7-protocol add name=youtube regexp=”(GET /videoplayback?|GET /crossdomain.xml)”

regaxp dla facebook i youtube: ^.+(youtube.com|facebook.com).*$

Uaktywnienie powyższej regułki w firewall:
/ip firewall filter add action=reject chain=forward layer7-protocol=youtube

w akcji dajemy drop lub reject (drop zadziała zawsze, ale jest za wolne i część ruchu przejdzie)

Aktywacja blokady w określonych godzinach (zadziała także w innych wpisach w firewall):
W przykładzie poniżej – we wszystkie dni tygodnia w godzinach od 5.00 do 23:59:59, podajemy czas od-do w formacie [godz] h [min] m [sek] s, bez spacji w całym wpisie czasu.

/ip firewall filter add action=reject chain=forward layer7-protocol=youtube time=5h-23h59m59s,sun,mon,tue,wed,thu,fri,sat

Blokowanie konkretnych portów lub ich zakresu:

/ip firewall filter
add action=drop chain=forward comment=”” disabled=no dst-port=445 protocol=tcp
add action=drop chain=forward comment=”” disabled=no dst-port=445 protocol=udp
add action=drop chain=forward comment=”” disabled=no dst-port=135-139 protocol=tcp
add action=drop chain=forward comment=”” disabled=no dst-port=135-139 protocol=udp

Przekierowanie dowolnego portu na określony adres wewnętrzny:

/ip firewall dst-nat add src-address=0.0.0.0 dst-port=4662 protocol=tcp action=nat to-dst-address=x.x.x.x to-dst-port=4662
(Czyli w skrócie wszystko co wchodzi na port 4662 na MT zostanie przekierowane na adres x.x.x.x)

Nadanie adresowi y.y.y.y z sieci lokalnej zewnętrznego adresu IP. x.x.x.x to jest adres z dostępnej puli adresów zewnętrznych:

/ip address add address=x.x.x.x/24 interface=ether1
/ip firewall dst-nat add dst-address=x.x.x.x/32 action=nat to-dst-address=y.y.y.y
/ip firewall src-nat add src-address=y.y.y.y/32 action=nat to-src-address=x.x.x.x

Blokowanie p2p na danym adresie:

/ip firewall rule forward add src-address=x.x.x.x p2p=all-p2p action=drop

Blokowanie przez PROXY
Konfiguracja Proxy:
/ip proxy
enabled: yes
src-address: 0.0.0.0
port: 8080
parent-proxy: 0.0.0.0:0
cache-drive: system
cache-administrator: „webmaster”
max-disk-cache-size: none
max-ram-cache-size: none
cache-only-on-disk: no
maximal-client-connections: 1000
maximal-server-connections: 1000
max-object-size: 512KiB
max-fresh-time: 3d

/ip firewall nat
chain=dstnat protocol=tcp dst-port=80 action=redirect to-ports=8080
/ip firewall filter
chain=input in-interface=<Your WAN Port> src-address=0.0.0.0/0 protocol=tcp dst-port=8080 action=drop

Blokowanie stron web:
/ip proxy access
dst-host=www.facebook.com action=deny

Zablokuje to stronę http://www.facebook.com. Możemy blokować tylko dla określonego źródła src-address. Będzie blokowany tylko konkretny źródłowy adres IP lub sieć.

Zatrzymanie ściąganie plików takich jak .mp3, .exe, .zip, .rar,…itp.:
/ip proxy access
path=*.exe action=deny
path=*.mp3 action=deny
path=*.zip action=deny
path=*.rar action=deny

Blokada po fragmencie nazwy URL:
/ip proxy access
dst-host=:mail action=deny
(Będą blokowane wszystkie strony zawierające słowo „mail” w adresie strony.)