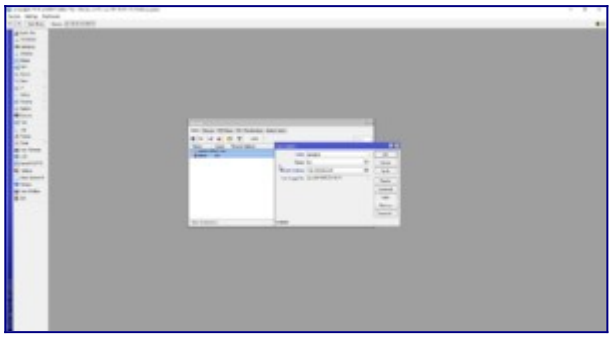
Bezpieczny Mikrotik – RouterOS

Podobnie jak w przypadku innych producentów sprzętu sieciowego, Mikrotika zaraz po wyjęciu z pudełka należy skonfigurować pod kątem bezpieczeństwa. Niestety w ostatnim czasie pojawiło się sporo zagrożeń związanych z przejęciem całkowitej kontroli nad urządzeniem. Podobne problemy dotyczą praktycznie wszystkich producentów sprzętu, dlatego niezależnie od vendora, zawsze warto poświęcić trochę czasu na zabezpieczenie sprzętu.
Zaczniemy od rzeczy, które należy wykonać **przed** podłączeniem Mikrotika do Internetu.

1. Zmiana kont systemowych

Domyślnym kontem w RouterOS jest admin, bez hasła. Zaczynamy od zmiany nazwy usera z admin na dowolnie inną. Używamy silnego hasła, najlepiej z generatora. Znam adminów, co mają kilka ulubionych haseł i tworzą z nich kolejne nowe odmiany, ale lepiej używać menadżera haseł np. KeePass. Konta userów zmieniamy w menu **System**->*Users*.



Terminal:
[code]/user print[/code]
Powinieneś zobaczyć listę wszystkich userów w systemie
[code]
Flags: X – disabled
NAME GROUP
0 ;;; system default user
grzegorz full
1 admin_zapasowy read
[/code]
Wybierając 0 edytujemy ustawienia usera grzegorz, natomiast 1 to user admin_zapasowy
[code]
/user set 0 name=nowaNazwaUsera
/user set 0 password="HasloZGeneratora!!!"
[/code]
Dodatkowym zabezpieczeniem jest ustawienie dozwolonych adresów IP, z których można zalogować się do konta.
[code]
/user set 0 allowed-address=x.x.x.x/yy
[/code]

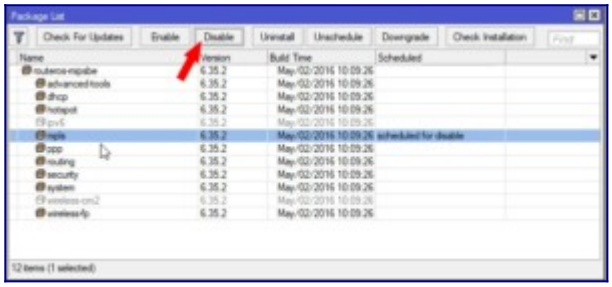
2. Aktualizacja RouterOS’a oraz Winbox’a

W ostatnim czasie pojawiło się sporo explitów, dlatego koniecznie zaktualizuj wersje routerOS do najnowszej, najlepiej z gałęzi **current**. Aktualizację możemy wykonać na kilka sposobów, ponieważ skupiliśmy się na krokach jakie należy zrobić przed podłączeniem Mikrotika do Internetu, pozostaje nam manualna instalacja. Przechodzimy na stronę https://mikrotik.com/download i pobieramy najnowszą wersję. Paczkę wybieramy w zależność od architektury sprzętu, którą najszybciej znajdziemy w nazwie okna winbox’a.

Sama instalacja paczki działa na zasadzie przeciągnij&upuść. Plik należy dodać do **Files**, ważne, aby był w głównym katalogu. Instalacja następni po ponownym uruchomieniu routera.
Uwaga!!! *instalacja paczki wydłuża pierwszy start routera.*

3. Wyłączenie nieużywanych usług(packages)

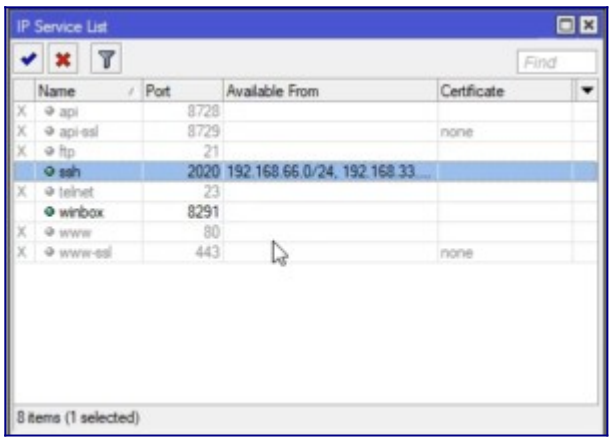
Jeżeli nie korzystasz z opcji hotspot albo z ipv6, to nie ma sensu, aby były aktywne w systemie. Przechodzimy na **System**->*Package*, podświetlamy paczkę ipv6 i klikamy w **disable.**



[code]
/system package disable hotspot
/system package disable ipv6
[/code]

4. Wyłączenie nieużywanych usług(services)

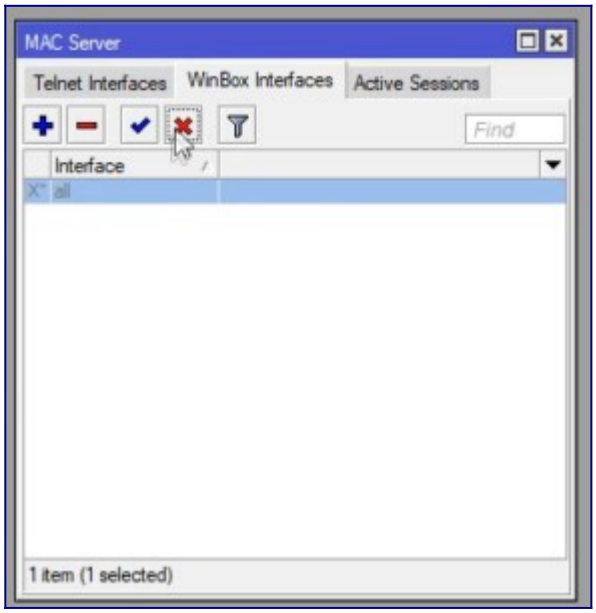
Podobnie jak w przypadku nieużywanych paczke, wyłączamy nieużywane usługi takie jak telnet, ftp, api. Przechodzimy na **IP**->*Services*, podświetlamy usługę, następnie klikamy w czerwony krzyżyk. W przypadku, gdy np. jest nam potrzebne połączenie po ssh, zmieniamy domyślny port usługi, oraz dodajemy ograniczenie logowania po konkretnym adresie IP bądź podsieci. Nie zalecam, a wręcz odradzamy wystawianie serwisów po publicznych adresach. Dedykowany vlan/adresacja do zarządzania(managmentu), to konieczność.



[code]
/ip service disable telnet,ftp,www,api,api-ssl
/ip service set ssh port=2020
/ip service set winbox address=192.168.66.0/24
/ip service set ssh address=192.168.66.0/24
[/code]

5. Wyłączenie logowania do winbox'a po mac addresie

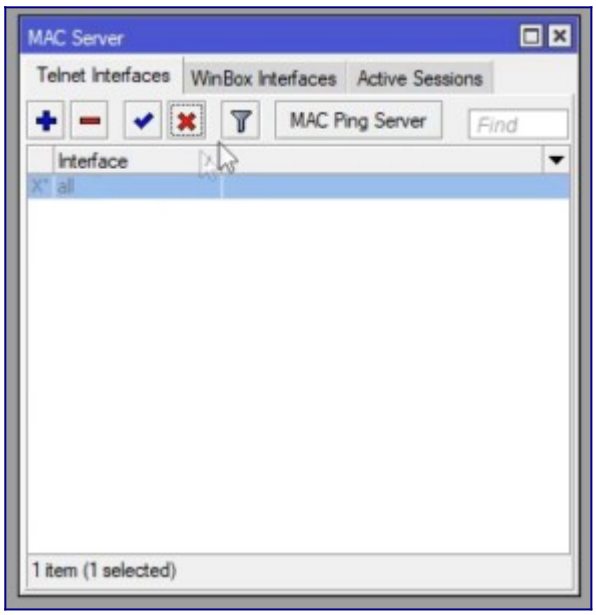
Zarządzanie RouterOSem może odbywać się po adresie IP(L3), ale i także po warstwie drugiej czyli po mac addessie. Domyślnie ta opcja jest włączona na **wszystkich** interfejsach. Przechodzimy na **Tool**->*MAC Server*. Analogicznie jak w przypadku poprzednich ustawień czerwony X wyłącza opcję, ewentualnie dodajmy interfejsy, z których można się zalogować.



[code]
/tool mac-server mac-winbox set [find] disabled=yes
[/code]

6. Wyłączenie logowania MAC-Telnet

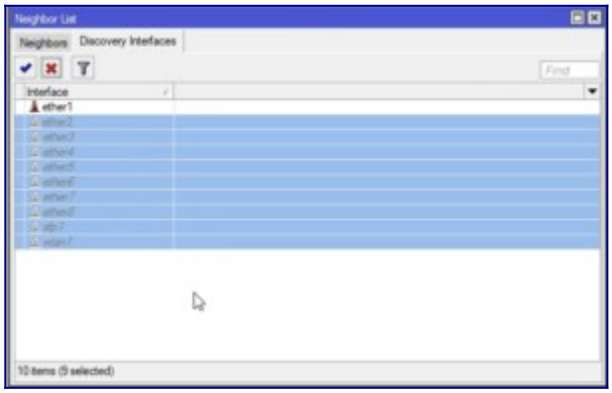
Zostając w tym samy oknie przechodzimy na zakładkę **Telnet Interfaces** zaznaczamy **all** i wyłączamy opcje. Uchroni to nas przed dalszym rozproszeniem się intruzów w sieci, ponieważ jeden skompromitowany router nie będzie otwartą bramą do pozostałej infrastruktury.



[code]
/tool mac-server set [find] disabled=yes
/tool mac-server ping set enabled=no
[/code]

7. Wyłączenie Neighbor Discovery

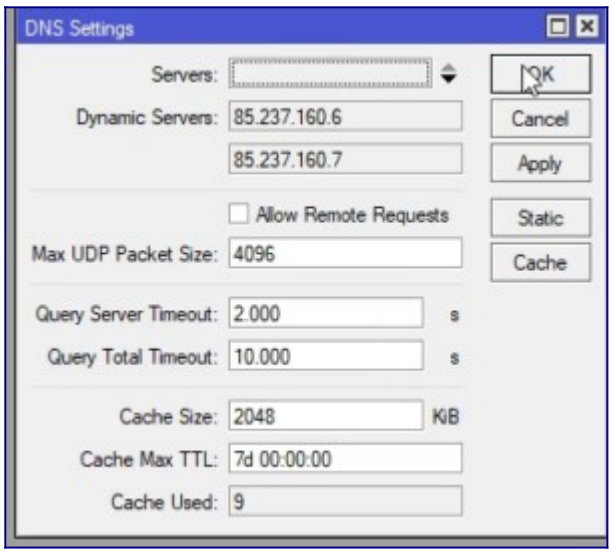
Kolejną dobrą praktyką jest wyłączenie możliwości wyszukania routera za pomocą Mikrotik Neighbor Discovery Protocol (NDP) albo Cisco Discovery Protocol (CDP). Przechodzimy na zakładkę **IP**->*Neighbors* następnie **Discovery Interfaces**, zaznaczamy interfejsy i czerwonym krzyżykiem wyłączamy.



[code]
/ip neighbor discovery settings set default=no default-for-dynamic=no
/ip neighbor discovery set [find] discover=no
[/code]

8. DNS Remote Requests

Domyślnie ta opcja jest odznaczona, ale warto sprawdzić. Przechodzimy na **IP**->*DNS* i sprawdzamy czy checkbox przy **Allow Remote Requests** jest odznaczony.



[code]
/ip dns set allow-remote-requests=no
[/code]

9. Domyślna konfiguracja Firewall’a

Warto zostawić domyślna konfigurację firewall oraz ograniczyć dostęp do router tylko adresom z allow_list(dzięki temu nie będziesz musiał ograniczać dostępu do usług per ip/sieć, zrobi to za nas allow lista)
[code]
/ip firewall filter
add action=accept chain=input comment="default configuration" connection-state=established,related
add action=accept chain=input src-address-list=allowed_to_router
add action=accept chain=input protocol=icmp
add action=drop chain=input
/ip firewall address-list
add address=192.168.66.2-192.168.66.254 list=allowed_to_router
[/code]
Dodatkowe ograniczenia wewnątrz sieci
[code]
/ip firewall filter
add action=fasttrack-connection chain=forward comment=FastTrack connection-state=established,related
add action=accept chain=forward comment="Established, Related" connection-state=established,related
add action=drop chain=forward comment="Drop invalid" connection-state=invalid log=yes log-prefix=invalid
add action=drop chain=forward comment="Drop tries to reach not public addresses from LAN" dst-address-list=not_in_internet in-interface=bridge1 log=yes log-prefix=!public_from_LAN out-interface=!bridge1
add action=drop chain=forward comment="Drop incoming packets that are not NATted" connection-nat-state=!dstnat connection-state=new in-interface=ether1 log=yes log-

prefix=!NAT
add action=drop chain=forward comment="Drop incoming from internet which is not public IP" in-interface=ether1 log=yes log-prefix=!public src-address-list=not_in_internet
add action=drop chain=forward comment="Drop packets from LAN that do not have LAN IP" in-interface=bridge1 log=yes log-prefix=LAN_!LAN src-address=!192.168.88.0/24

/ip firewall address-list
add address=0.0.0.0/8 comment=RFC6890 list=not_in_internet
add address=172.16.0.0/12 comment=RFC6890 list=not_in_internet
add address=192.168.0.0/16 comment=RFC6890 list=not_in_internet
add address=10.0.0.0/8 comment=RFC6890 list=not_in_internet
add address=169.254.0.0/16 comment=RFC6890 list=not_in_internet
add address=127.0.0.0/8 comment=RFC6890 list=not_in_internet
add address=224.0.0.0/4 comment=Multicast list=not_in_internet
add address=198.18.0.0/15 comment=RFC6890 list=not_in_internet
add address=192.0.0.0/24 comment=RFC6890 list=not_in_internet
add address=192.0.2.0/24 comment=RFC6890 list=not_in_internet
add address=198.51.100.0/24 comment=RFC6890 list=not_in_internet
add address=203.0.113.0/24 comment=RFC6890 list=not_in_internet
add address=100.64.0.0/10 comment=RFC6890 list=not_in_internet
add address=240.0.0.0/4 comment=RFC6890 list=not_in_internet
add address=192.88.99.0/24 comment="6to4 relay Anycast [RFC 3068]" list=not_in_internet
[/code]

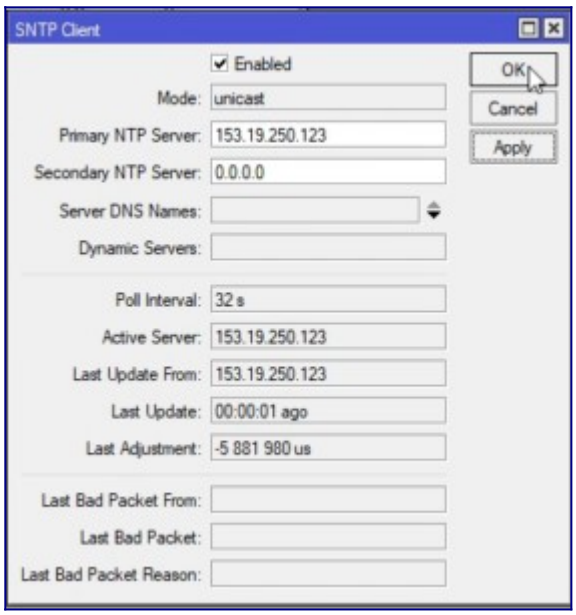
10. Wyłączenie nieużywanych interfejsów

Nieużywane port należy wyłączyć, a najlepiej w ogóle nie dodawać do konfiguracji.

[code]
/interface set 2,3,4,5,6,7,8 disabled=yes
[/code]

11. Włączenie klienta NTP

Aktualna data i godzina jest bardzo ważna, bez nich analiza logów będzie mocno utrudniona, a czasami wręcz niemożliwa.



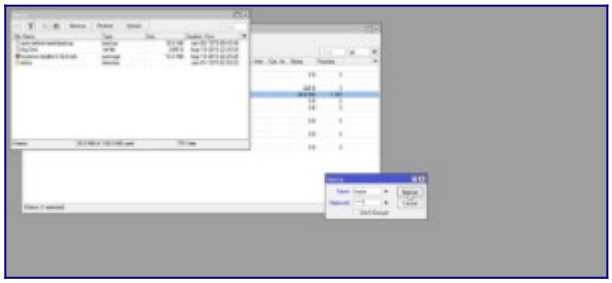
[code]
/system ntp client set enabled=yes server-dns-names=ntp.task.gda.pl
[/code]

12. Logowanie zdarzeń

Najlepszym i najbezpieczniejszym rozwiązaniem jest logowanie zdarzeń do zewnętrznego sysloga. W innym przypadku zdarzenia można logować na dysk, ale wbudowana pamięć jest bardzo mała, dlatego do Mikrotików z portem usb możemy podłączyć pendriva.

13. Szyfruj kopie zapasową przy użyciu hasła

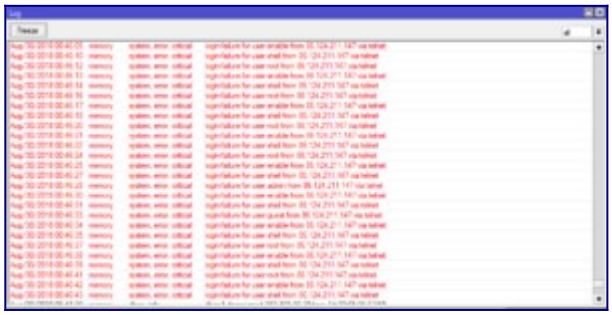
Przy eksporcie konfiguracji zawsze podawaj hasło.



14. Wyłącz LCD

15. Wyłącz BTest Server

Podsumowanie



Stawiaj bezpieczeństwo na pierwszym miejscu, lepiej jest posiedzieć dłużej nad konfiguracją, dodaniem sieci managmentowej, ale później spać spokojnie. W większej części przejęte routery robiły za koparki kryptowalut, czasami za dnsy do phisingowych stron, ale to chyba najlepsze co może Cię spotkać. Inwigilacja sieci za routerem, kradzież danych osobnych, to tylko jedne z nielicznych konsekwencji złego zabezpieczenia RouterOSa.

Polecany sprzęt

Z własnego doświadczenia mogę wam polecić poniższy sprzęt, z podziałem na ewentualne przeznaczenie routera.

Do domu i małej firmy(SOHO): hAP AX Lite , hAP AC3, RB4011, RB260GS, RB2011 hAP AC3 LTE, hAP AX2, hAP AX3, L009UiGS-2HaxD-IN, RB5009UG+S+IN, Audience

LTE: SXT LTE kit, SXT LTE6 kit, LHG 5, LHG LTE kit, Audience LTE, Chateau LTE6 ax, LTAP LTE6

Access Pointy: mAP lite, mAP, cAP AX, cAP XL AC

POE: hEX PoE

LAB: hEX lite

Średnia/Duża firma: CCR1036-12G-4S, CCR2004-16G-2S+