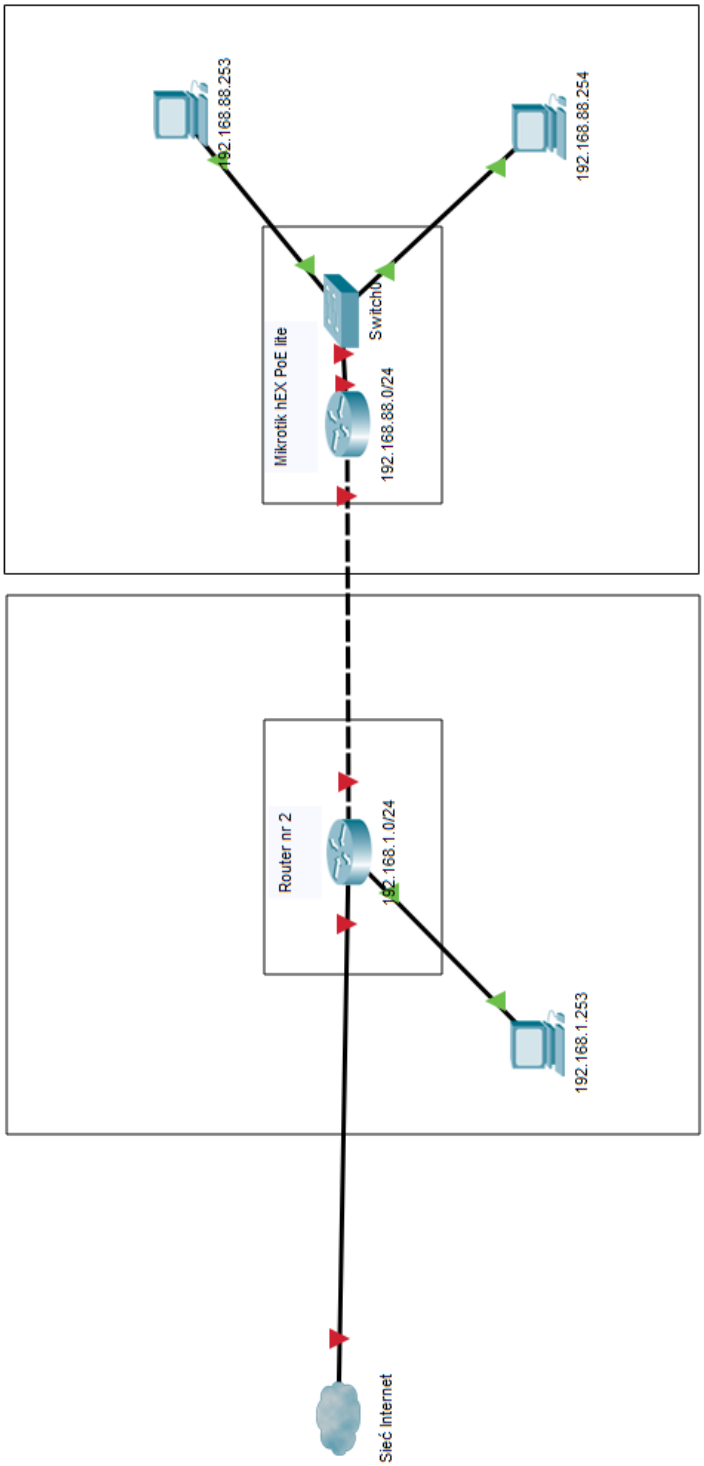
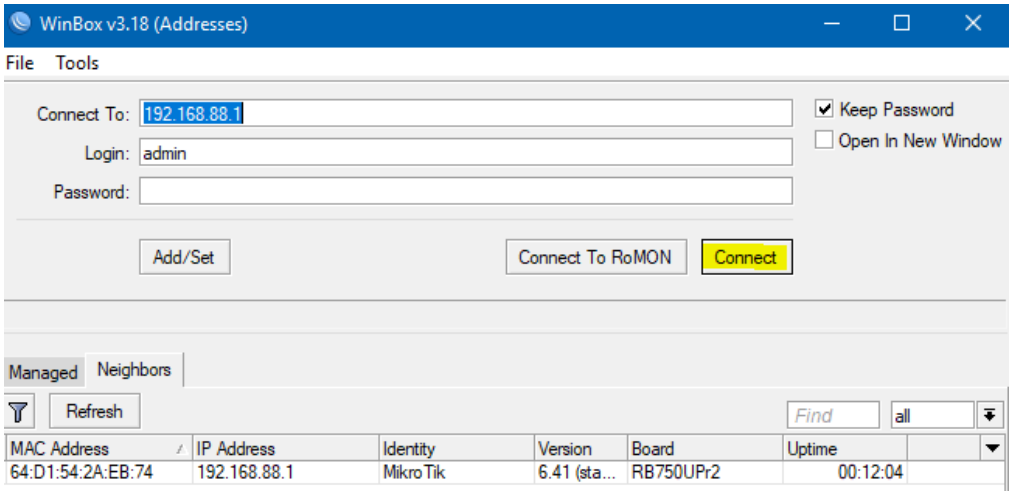
Konfiguracja Firewalla na routerze MikroTik

1. Schemat sieci do testów firewalla

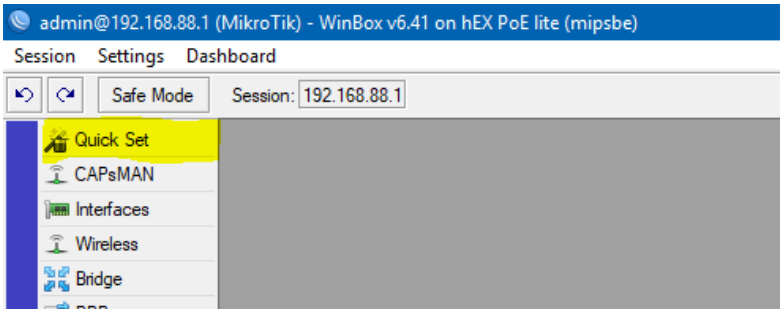


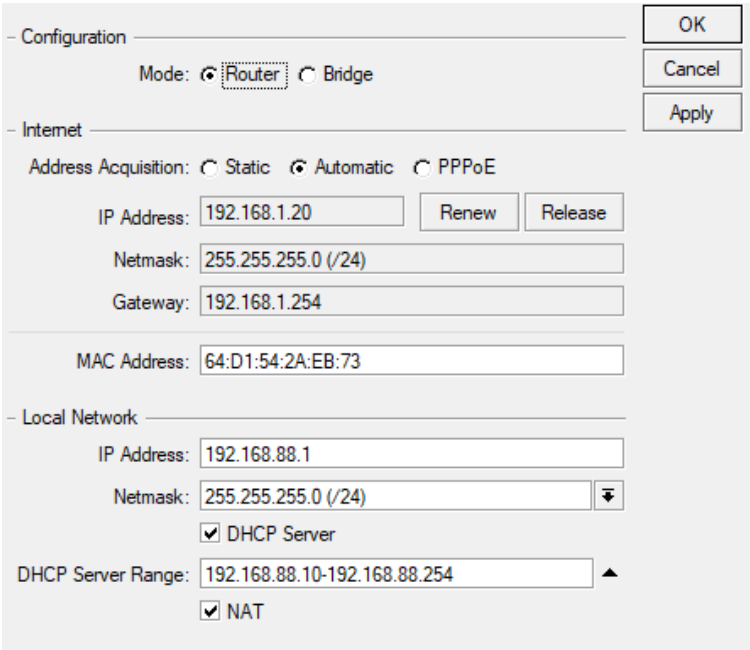
2. Przygotowanie środowiska MikroTik

a) Zaloguj się używając automatycznego wyszukiwania urządzenia po adresie MAC lub ręcznie zaloguj się za pomocą adresu IP



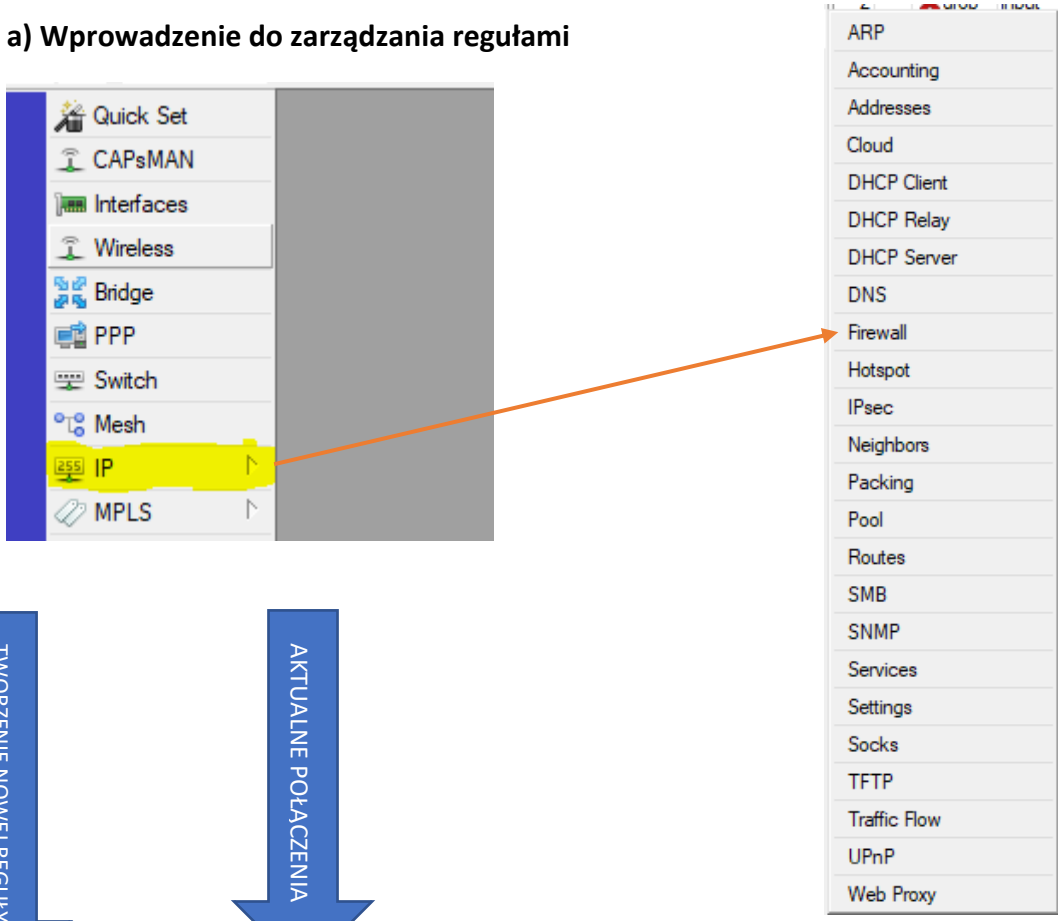
b) Skonfiguruj router tak aby mógł komunikować się z siecią Internet tak aby sprawdzić działajcie w jej zakresie usługi tj. HTTP, FTP, SSH itd.
(Jest to potrzebne aby sprawdzić w dalszej części ćwiczenia poprawność konfiguracji reguł)





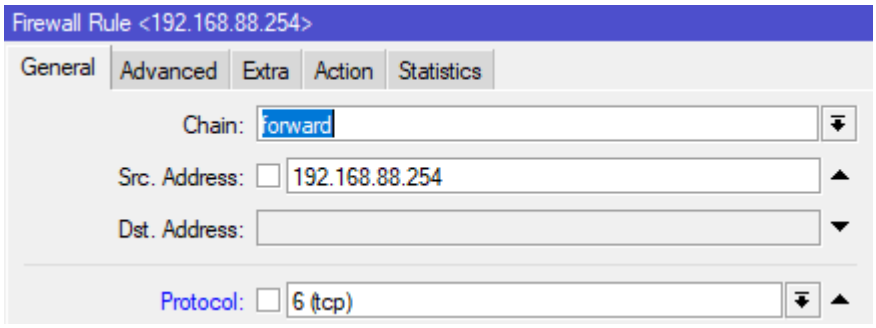
3. Konfiguracja reguł firewalla

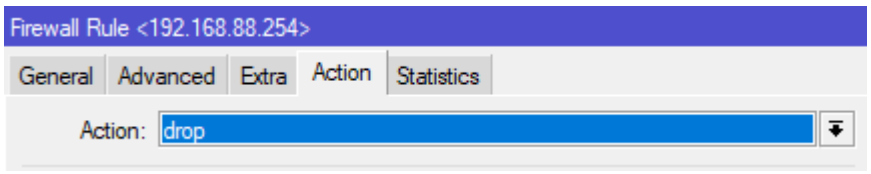
a) Wprowadzenie do zarządzania regułami



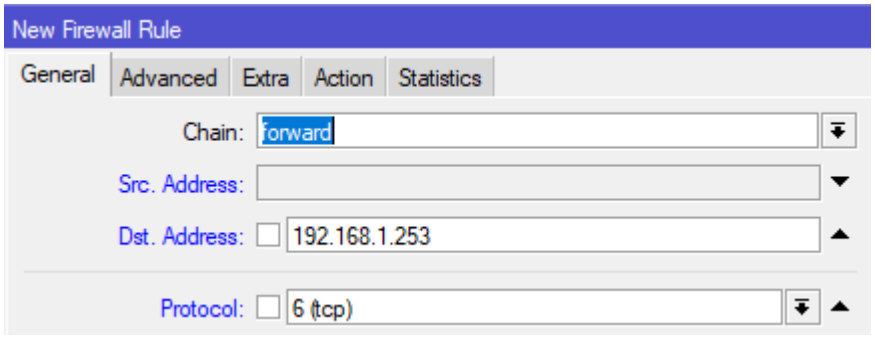
4. Przykłady reguł

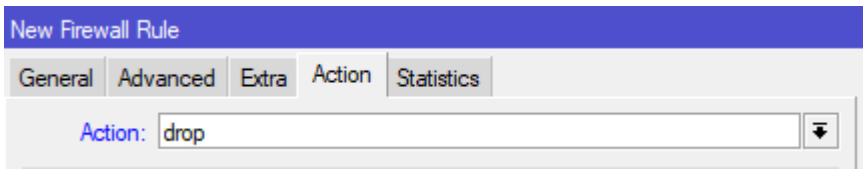
1) Zablokowanie możliwości komunikacji TCP dla hosta o przykładowym adresie 192.168.88.254 ze wszystkimi hostami z poza sieci (w sieci porty routera ustawione są w tryb bridge co pomija reguły firewalla)



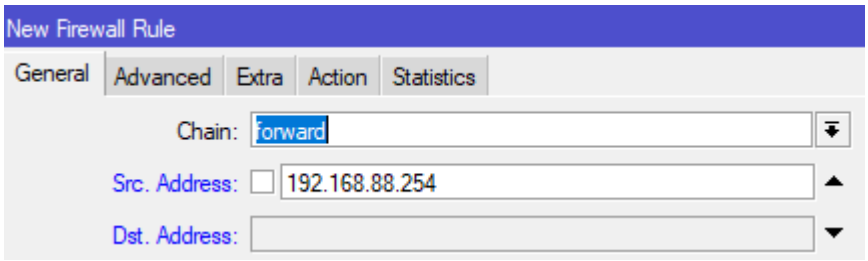


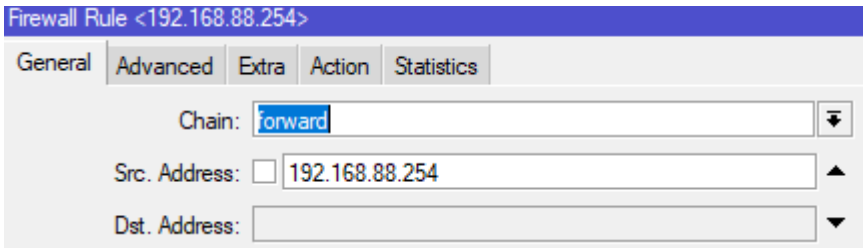
2) Zablokowanie możliwości komunikacji TCP z hostem o przykładowym adresie 192.168.1.253 dla wszystkich hostów w sieci 192.168.88.0/24



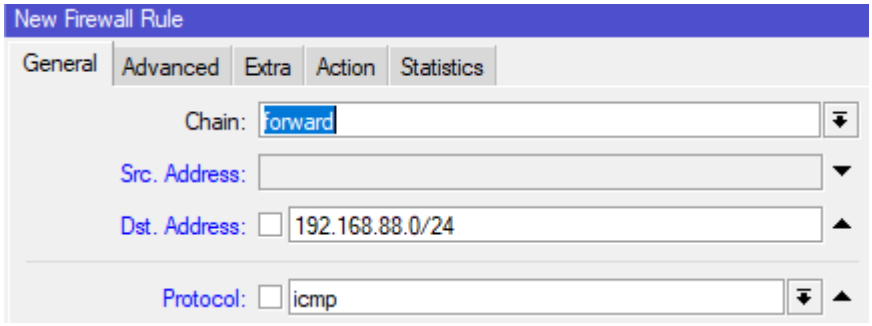


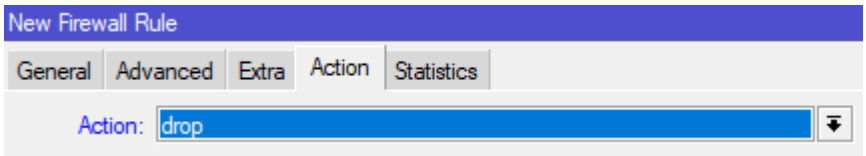
3) Zablokowanie dla hosta 192.168.88.254 możliwości komunikacji dowolnym protokołem ze wszystkimi hostami z poza sieci



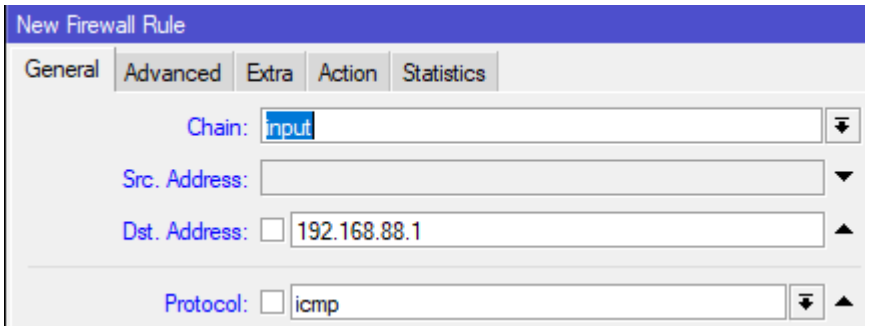


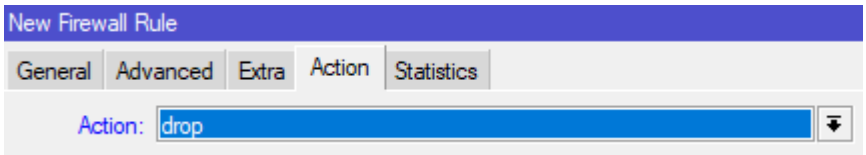
4) Zablokowanie możliwości pingowania (ICMP) hostów znadujących się w sieci 192.168.88.0/24



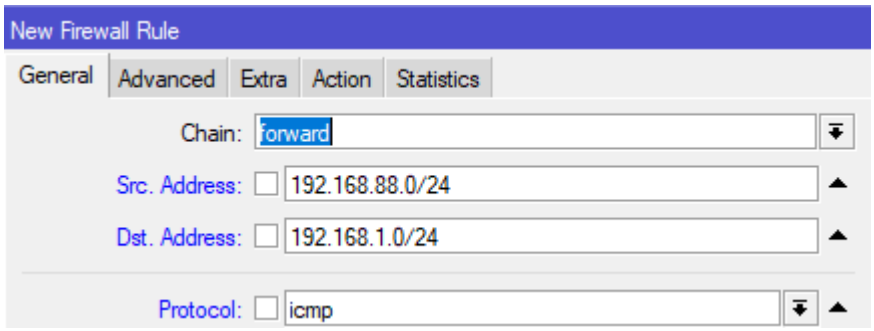


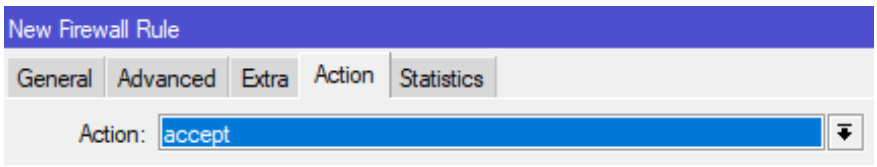
5) Całkowite zablokowanie możliwości pingowania routera 192.168.88.1



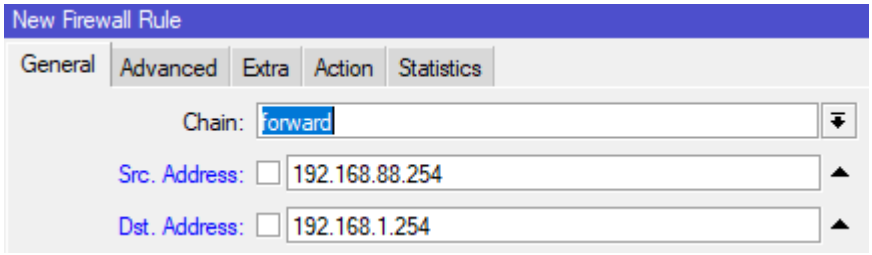


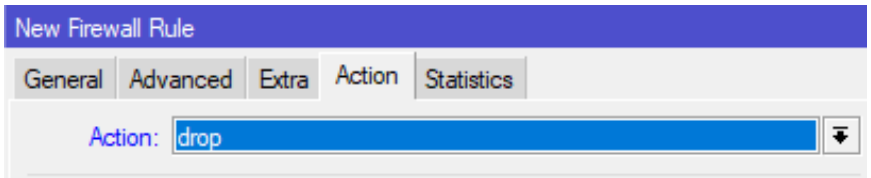
6) Zablokowanie możliwości pingowania z sieci 192.168.88.0/24 do sieci 192.168.1.0/24



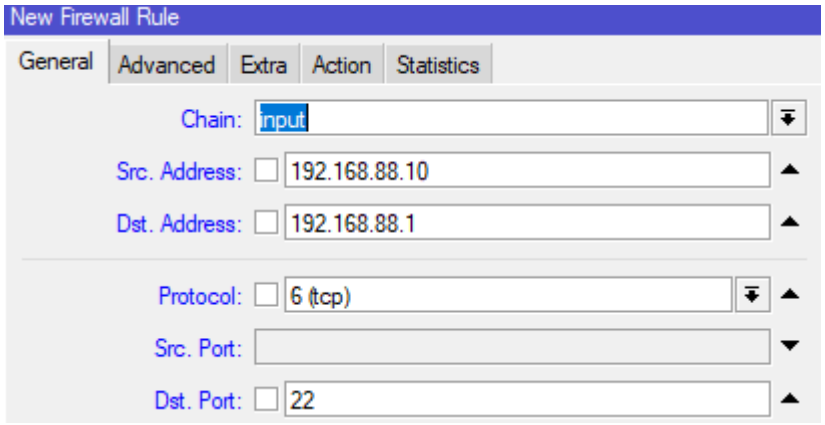


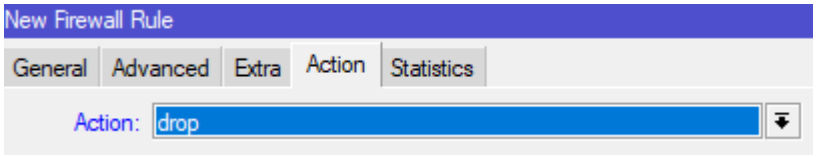
7) **Zablokowanie komunikacji hosta 192.168.88.254 z hostem 192.168.1.254**



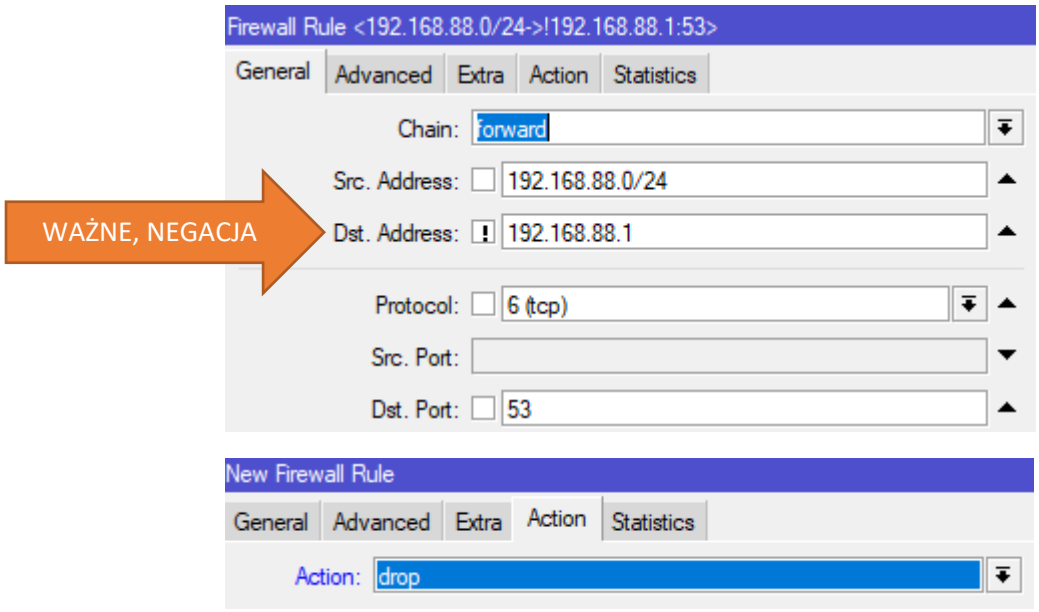


8) Zablokowanie możliwości komunikowania się z routerem (192.168.88.1) przez hosta (192.168.88.10) za pomocą protokołu SSH(22)

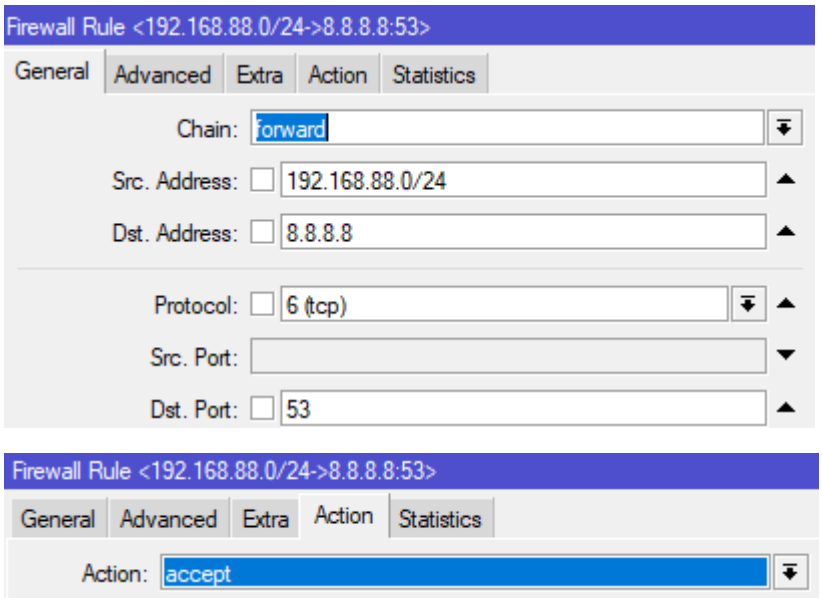




9) Zablokowanie możliwości korzystania z zewnętrznych serwerów DNS (Jedynym serwerem DNS wtedy może być nasz router o IP 192.168.88.1)

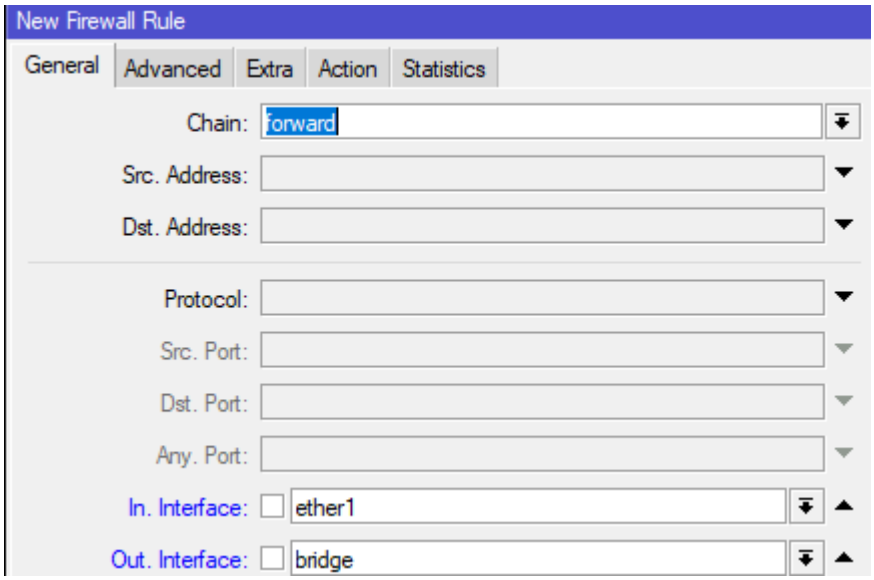


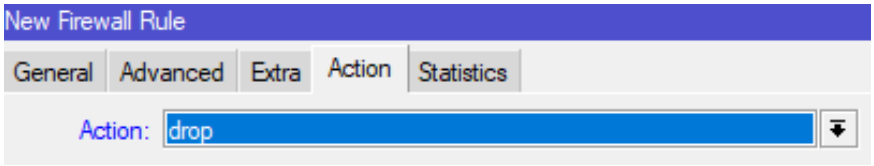
10) Wybór serwerów DNS jakimi będą mogli posługiwać się użytkownicy sieci (Jedynym serwerem DNS może być nasz router o IP 192.168.88.1 oraz zewnętrzny DNS 8.8.8.8).



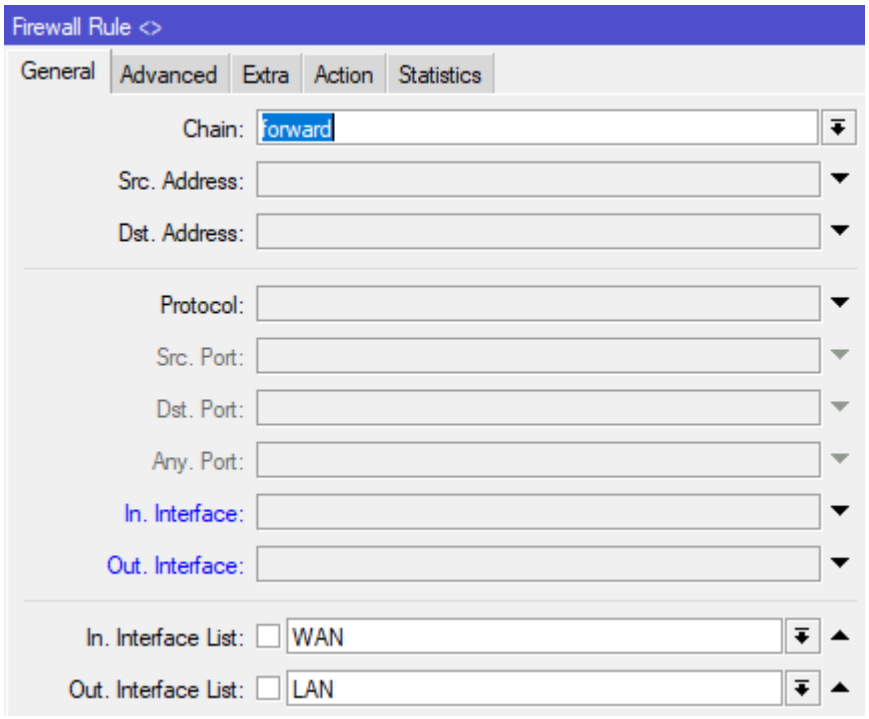
Następnie wykonaj punkt 9 aby zablokować inne DNSy niż 8.8.8.8

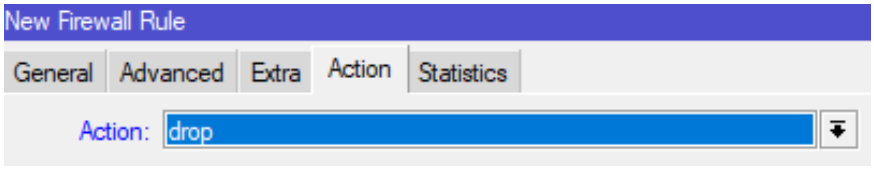
11) Zablokowanie ruchu pomiędzy interfejsem 1 (do sieci 192.168.1.0/24) a mostem portów 2/5 routera.



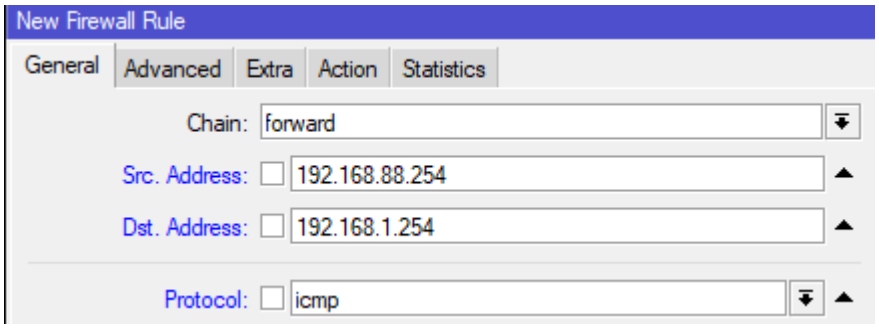


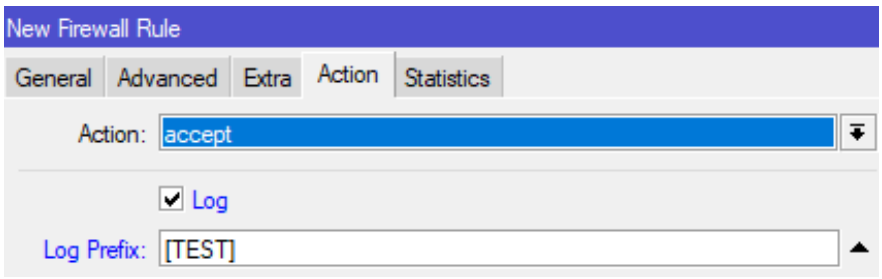
12) Zablokowanie ruchu na zdefiniowanych listach interfejsów np. LAN -> WAN





13) Zapisywanie zdarzenia wysłania pakietu do dziennika zdarzeń

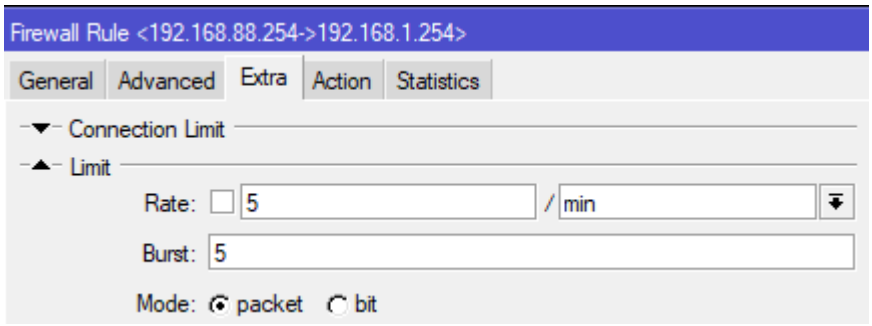




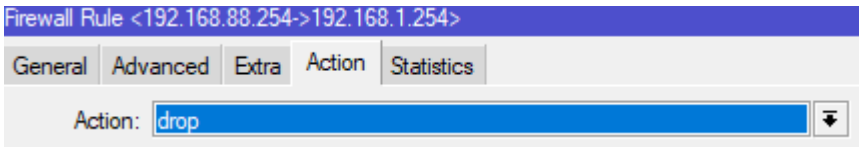
Na głównym pasku narzędzi „LOG”

Jun/11/2019 09:59:33	memory	firewall, info	[TEST] forward: in:bridge out:ether1, src-mac d4:3d:7e:34:40:dd, proto ICMP (type 8, code 0), 192.168.88.254->192.168.1.254, len 60
Jun/11/2019 09:59:34	memory	firewall, info	[TEST] forward: in:bridge out:ether1, src-mac d4:3d:7e:34:40:dd, proto ICMP (type 8, code 0), 192.168.88.254->192.168.1.254, NAT (192.168.88.254->192.168.1.20)->192.168.1.254, len 60
Jun/11/2019 09:59:35	memory	firewall, info	[TEST] forward: in:bridge out:ether1, src-mac d4:3d:7e:34:40:dd, proto ICMP (type 8, code 0), 192.168.88.254->192.168.1.254, NAT (192.168.88.254->192.168.1.20)->192.168.1.254, len 60
Jun/11/2019 09:59:36	memory	firewall, info	[TEST] forward: in:bridge out:ether1, src-mac d4:3d:7e:34:40:dd, proto ICMP (type 8, code 0), 192.168.88.254->192.168.1.254, NAT (192.168.88.254->192.168.1.20)->192.168.1.254, len 60

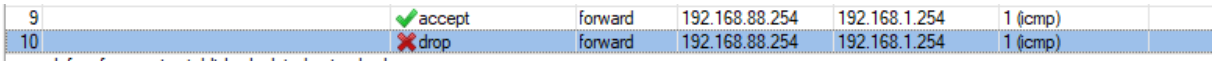
14) Ogarniczenie ilości wysłanych pakietów w danej regule i określonym czasie. (Można stworzyć dwukrotnie regułę 13 a następnie do pierwszej dodać:



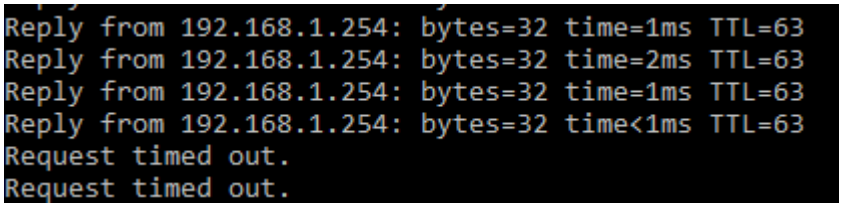
Do drugiej ustalić action na drop.



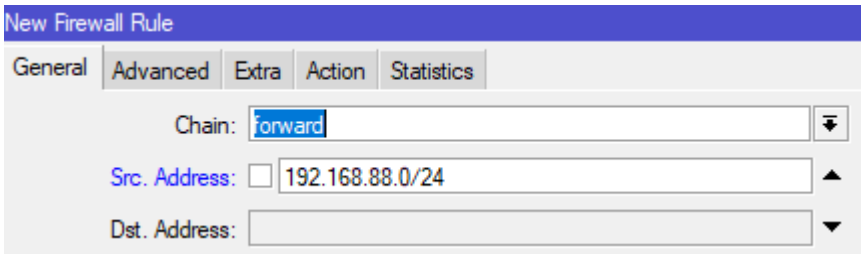
Wygląd i kolejność reguł.

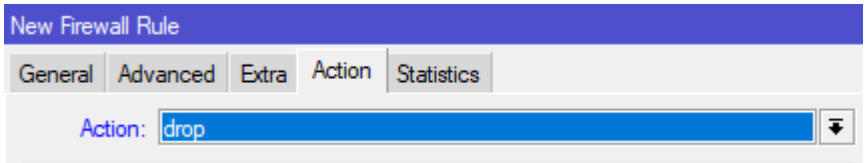


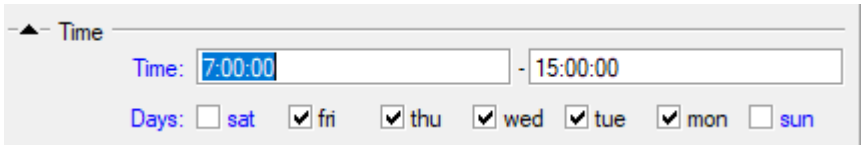
9	accept	forward	192.168.88.254	192.168.1.254	1 (icmp)
10	drop	forward	192.168.88.254	192.168.1.254	1 (icmp)



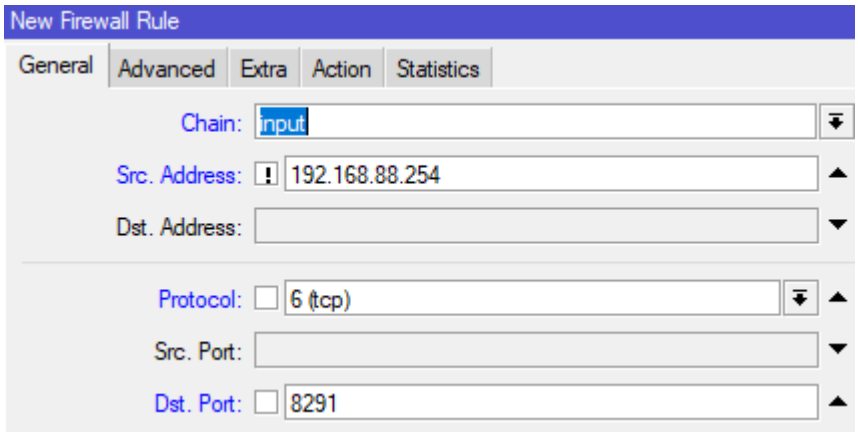
15) Zablokowanie ruchu „na zewnątrz" z sieci 192.168.88.0/24 w godzinach 7:00-15:00 bez weekendów

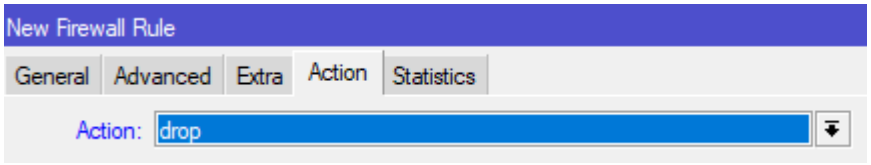




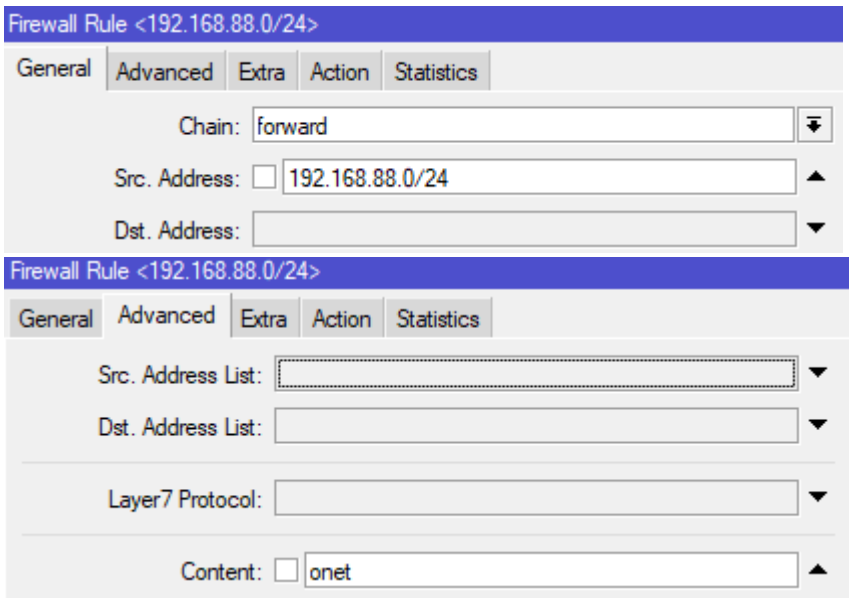


16) Zablokowanie połączenia poprzez Winbox innym hostom niż 192.168.88.254



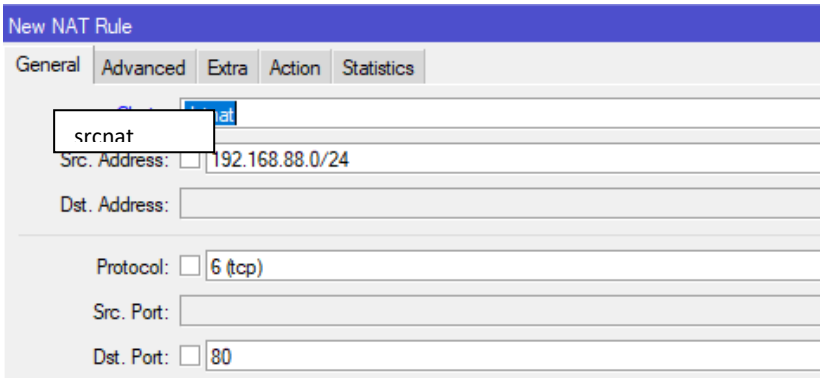


17) Blokada poprzez firewall warstwy 7 słowa klucz „onet” co blokuje dostęp do domeny „onet.pl”

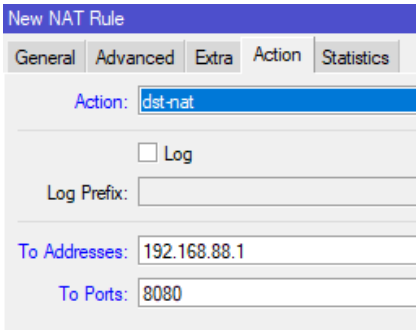


18) Blokada stron pornograficznych poprzez OpenDNS oraz Web Proxy po przekierowaniu ruchu za pomocą NAT.

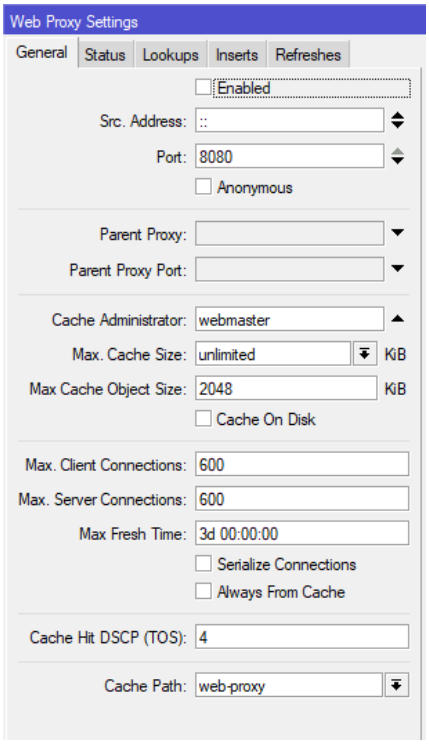
Przejdź do zakładki NAT w oknie firewall



Ustalenie przekierowania na adres serwera Web Proxy na routerze



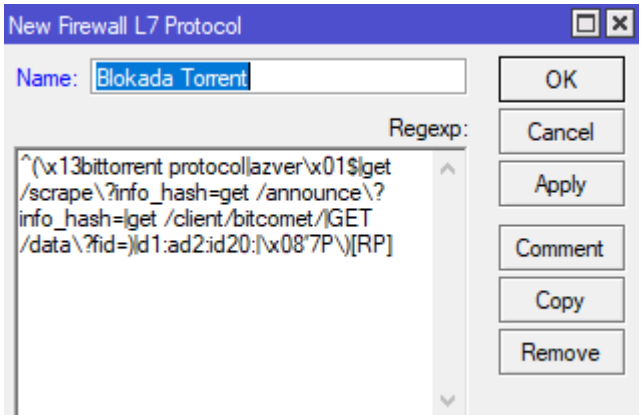
Konfiguracja Web Proxy (Trzeba ustawić OpenDNS po uprzednim zarejestrowaniu się aby nie tłumaczył nazw z domenami o treści niepożądanej)



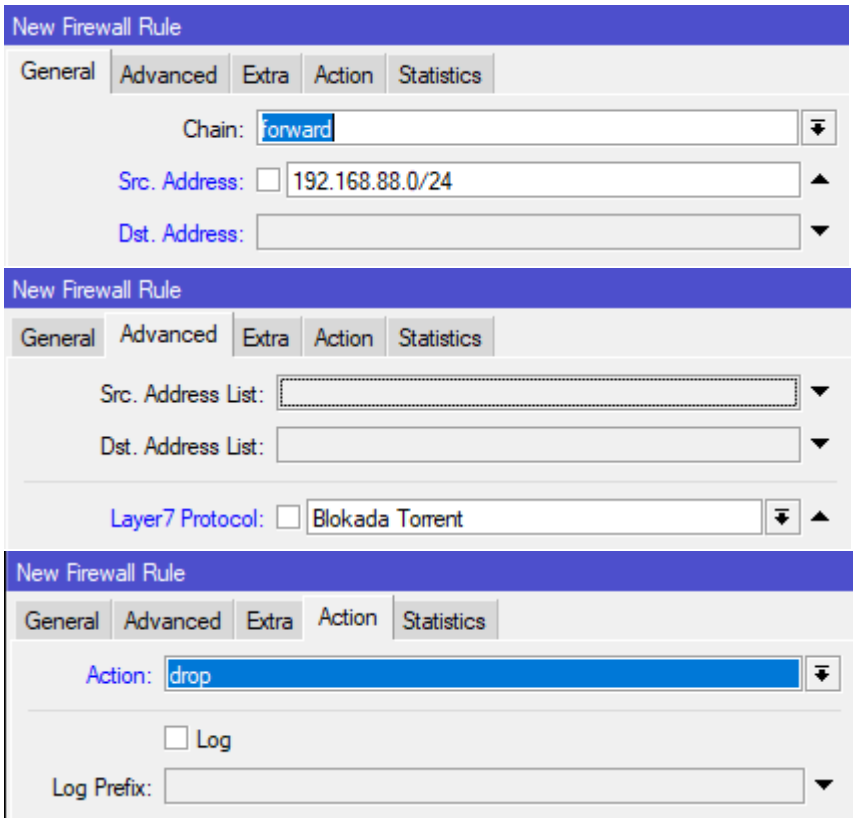
19) Blokada protokołu BitTorrent (torrenty) poprzez firewall warstwy 7

Strona z filtrami L7 http://l7-filter.sourceforge.net/protocols

Przejdź do zakładki Firewall L7

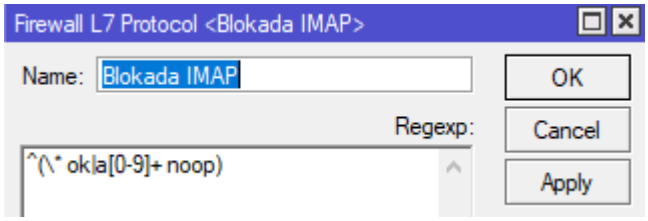


Przejdź ponownie do podstawowej konfiguracji i stwórz nową regułę

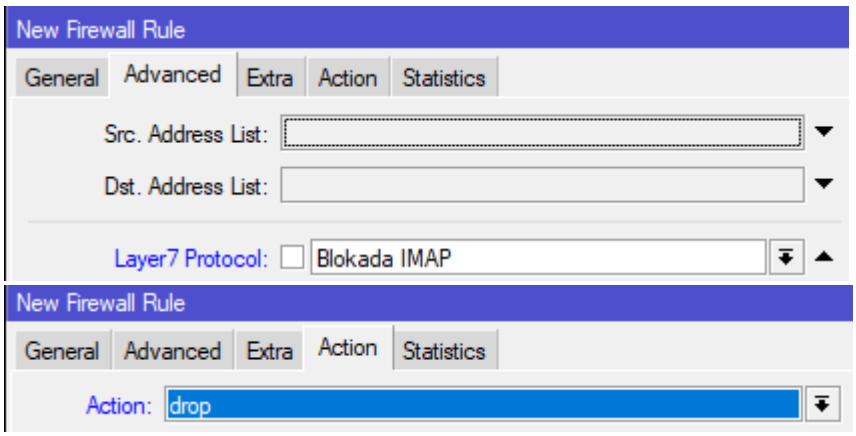


20) Blokada protokołu poczty IMAP w warstwie 7 dla urządzeń z poza sieci LAN

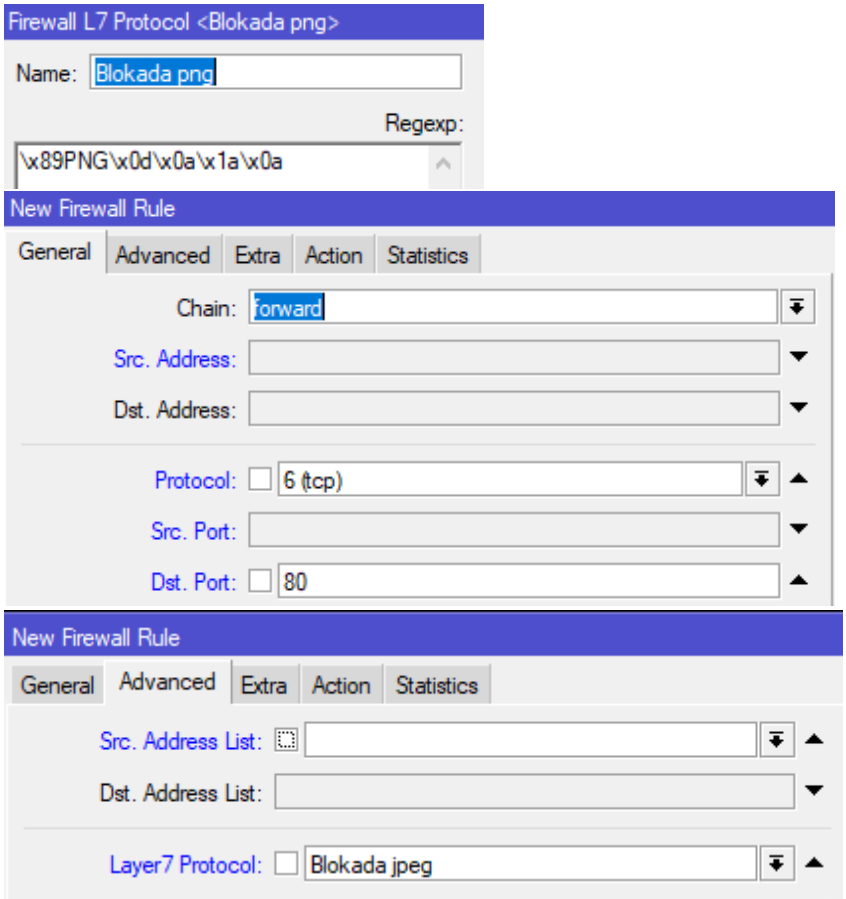
Przejdź do zakładki Firewall L7

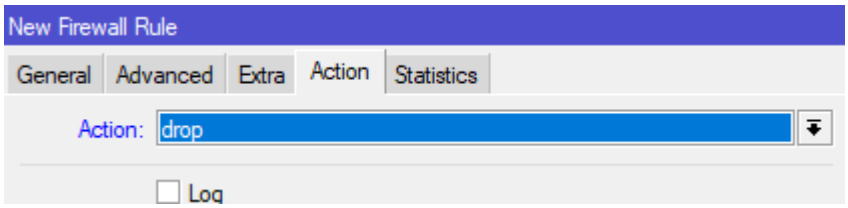


Przejdź ponownie do podstawowej konfiguracji i stwórz nową regułę

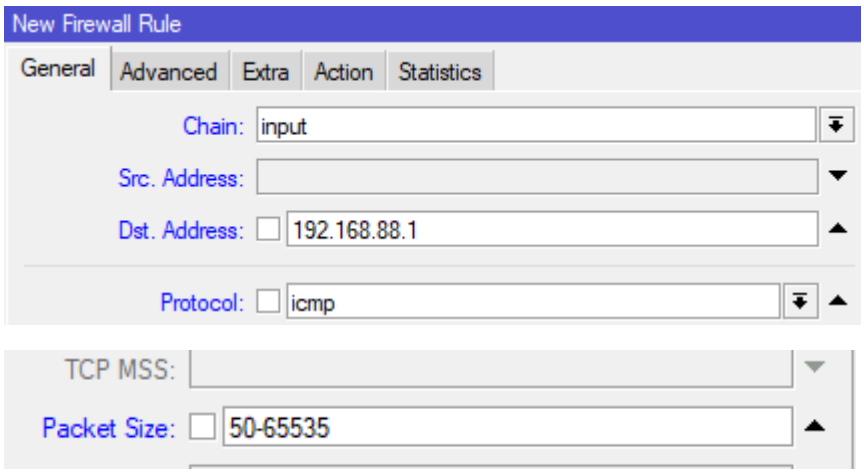


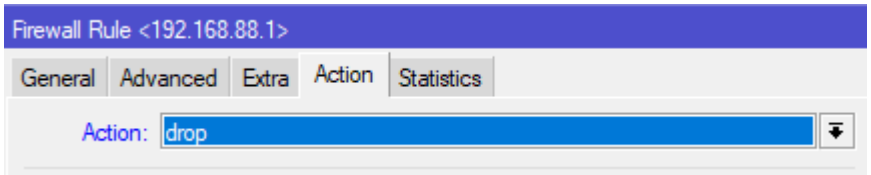
21) Blokada pobierania plików z rozszerzeniem .png





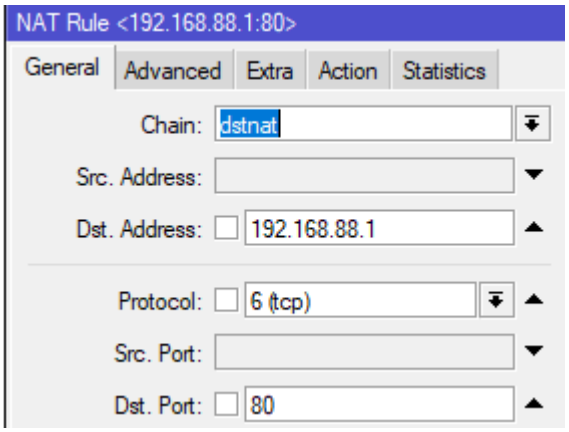
22) Zablokowanie pingu routera jeżeli pakiet jest większy niż 50 bajtów

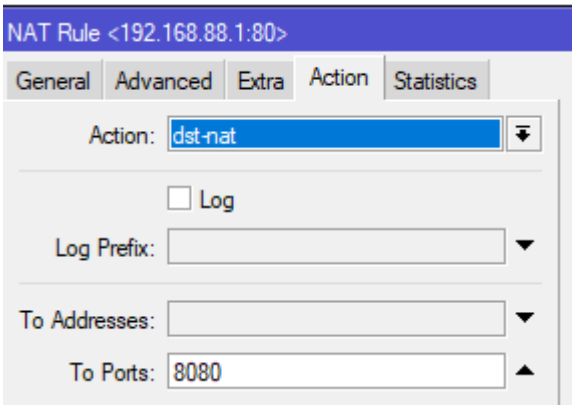




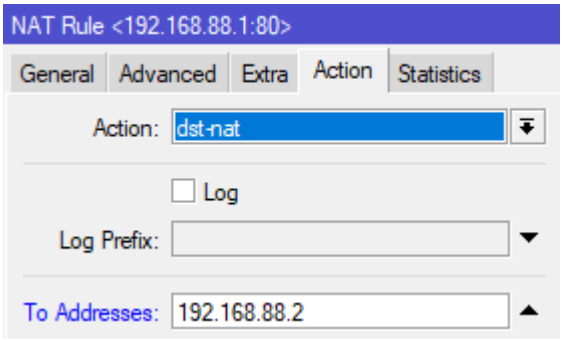

```
C:\Users\Pawel>ping 192.168.88.1 -l 100

Pinging 192.168.88.1 with 100 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.88.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Pawel>ping 192.168.88.1 -l 10

Pinging 192.168.88.1 with 10 bytes of data:
Reply from 192.168.88.1: bytes=10 time<1ms TTL=64
Reply from 192.168.88.1: bytes=10 time<1ms TTL=64
Reply from 192.168.88.1: bytes=10 time=1ms TTL=64
Reply from 192.168.88.1: bytes=10 time=1ms TTL=64

Ping statistics for 192.168.88.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Pawel>
```

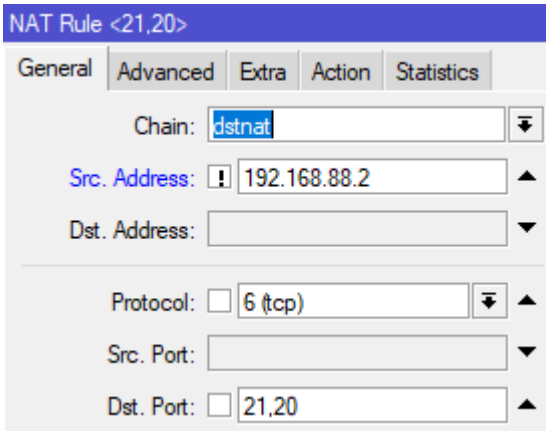
23) Przekierowanie ruchu z usługi HTTP port 80 na port 8080 w zakładce „NAT”



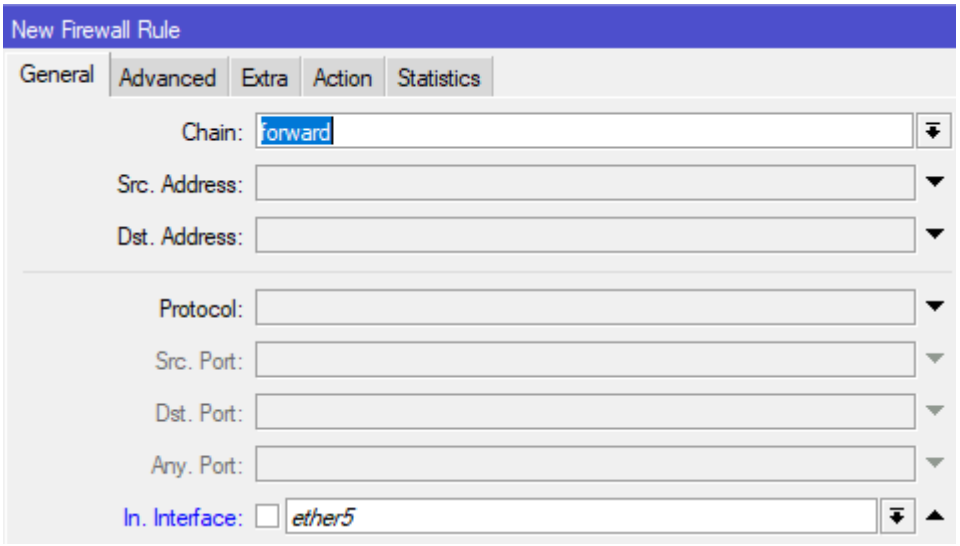


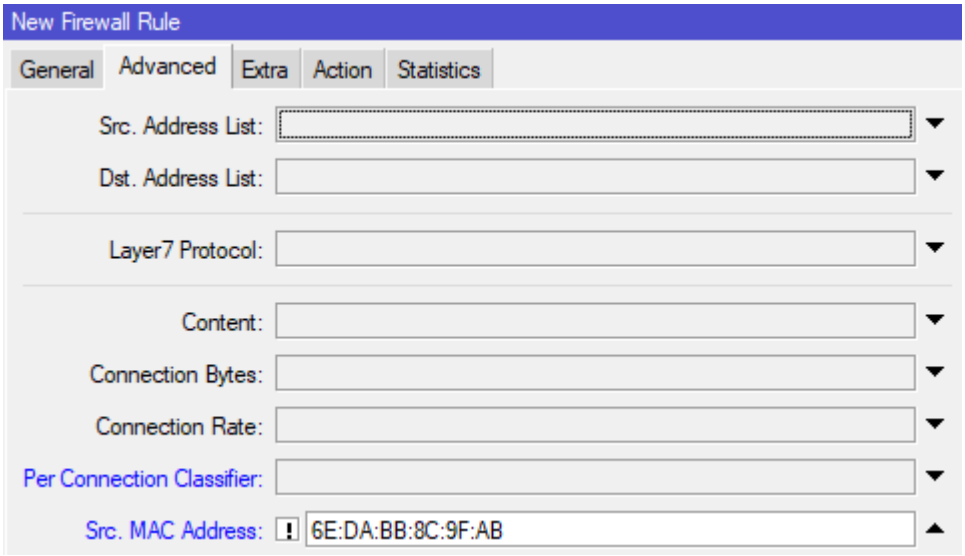
24) Przekierowanie całego ruchu dla FTP na serwer plików o adresie 192.168.88.2

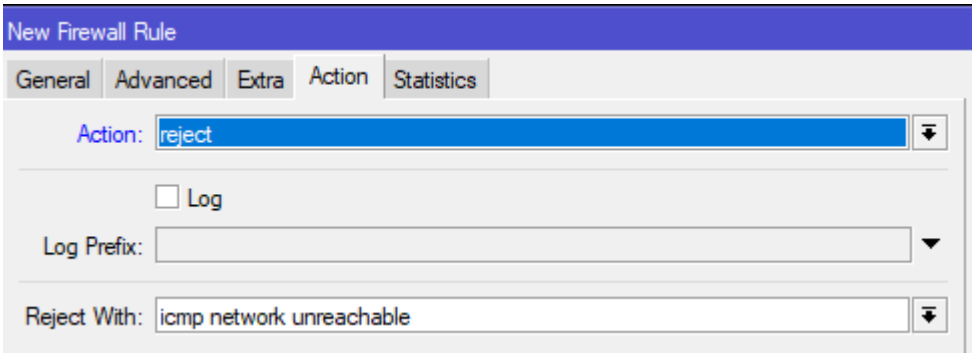




25) Udostępnienie sieci na interfejsie ether5 tylko dla urządzenia z danym adresem MAC i wysłanie komunikatu destination-unreachable kiedy inne urządzenie będzie chciało komunikować się z siecią zewnętrzną

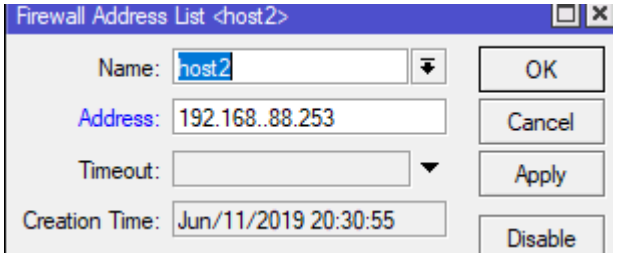




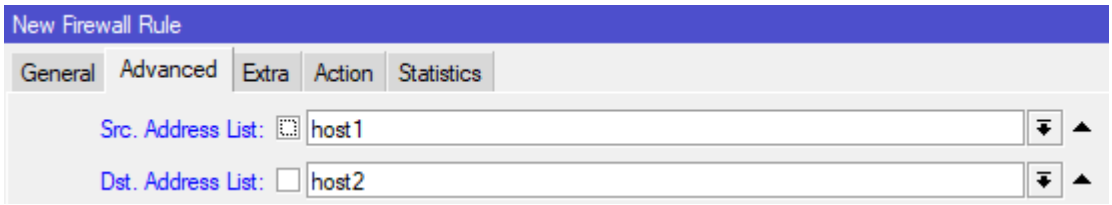


26) Używanie adresów, które zostały już wcześniej zdefiniowane w liście adresów

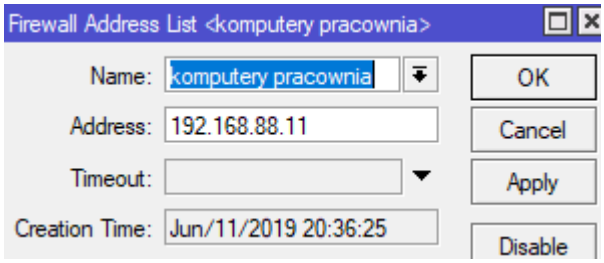
Wejdź w zakładkę Address List i zdefiniuj dwa adresy

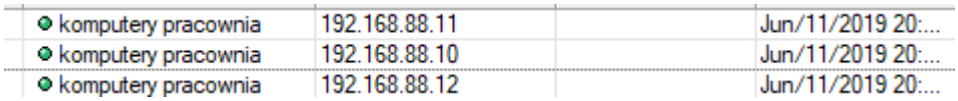


Posłuż się adresami w konfiguracji reguły

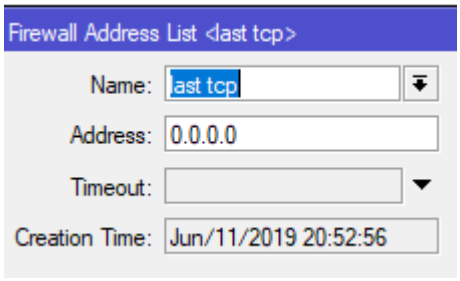


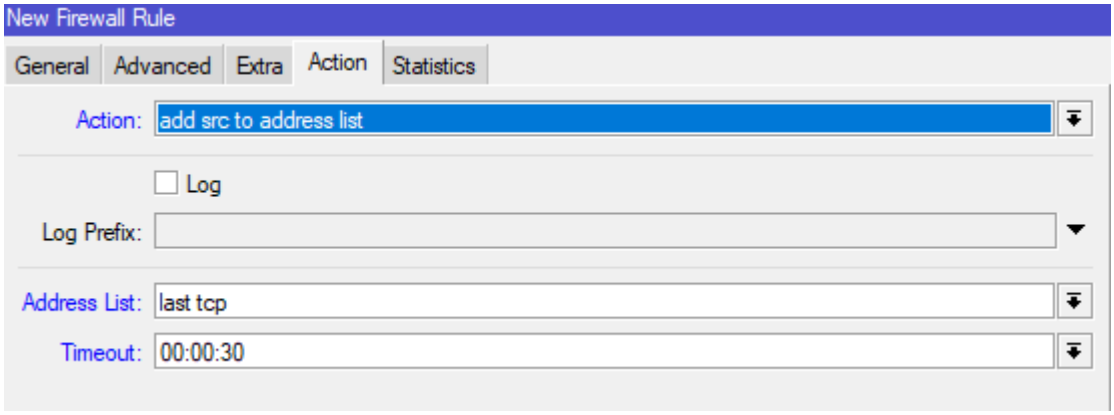
27) W liście adresów stwórz kilka adresów w tej samej grupie i skorzystaj z nich do stworzenia dowolnej reguły (za każdym razem używając tej samej nazwy)





28) Zapisanie w liście adresów połączeń TCP z ostatnich 30 sekund działania

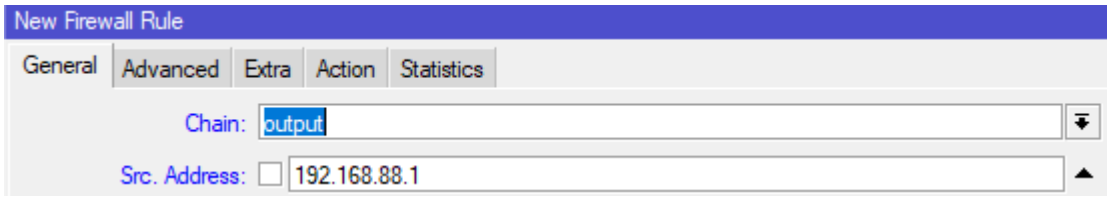


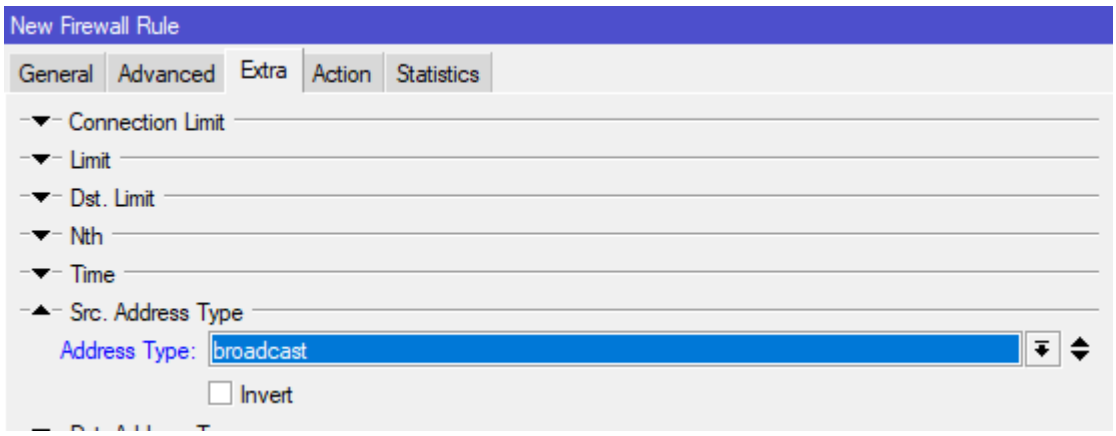


Do listy zostaną automatycznie dodane adresy

	last tcp	0.0.0.0		Jun/11/2019 20:...
D	last tcp	192.168.88.254	00:00:26	Jun/11/2019 20:...
D	last tcp	31.13.81.9	00:00:27	Jun/11/2019 20:...

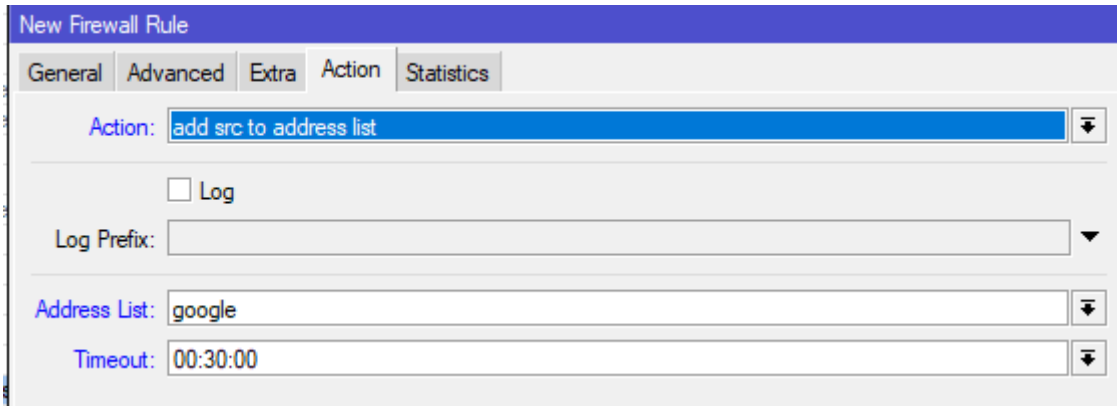
29) Reguła blokująca wybrany tryb transmisji np. broadcast dla routera





30) Jeżeli użytkownik użyje wyrazu „google” przez pół godziny ruch jego komputera zostanie zablokowany

Dodaj regułę wychwytującą użycie wyrazu „google” i dodającą host do listy o takiej samej nazwie na pół godziny



Następnie utwórz regułę, której warunkiem jest przynależność adresu IP do listy „google”