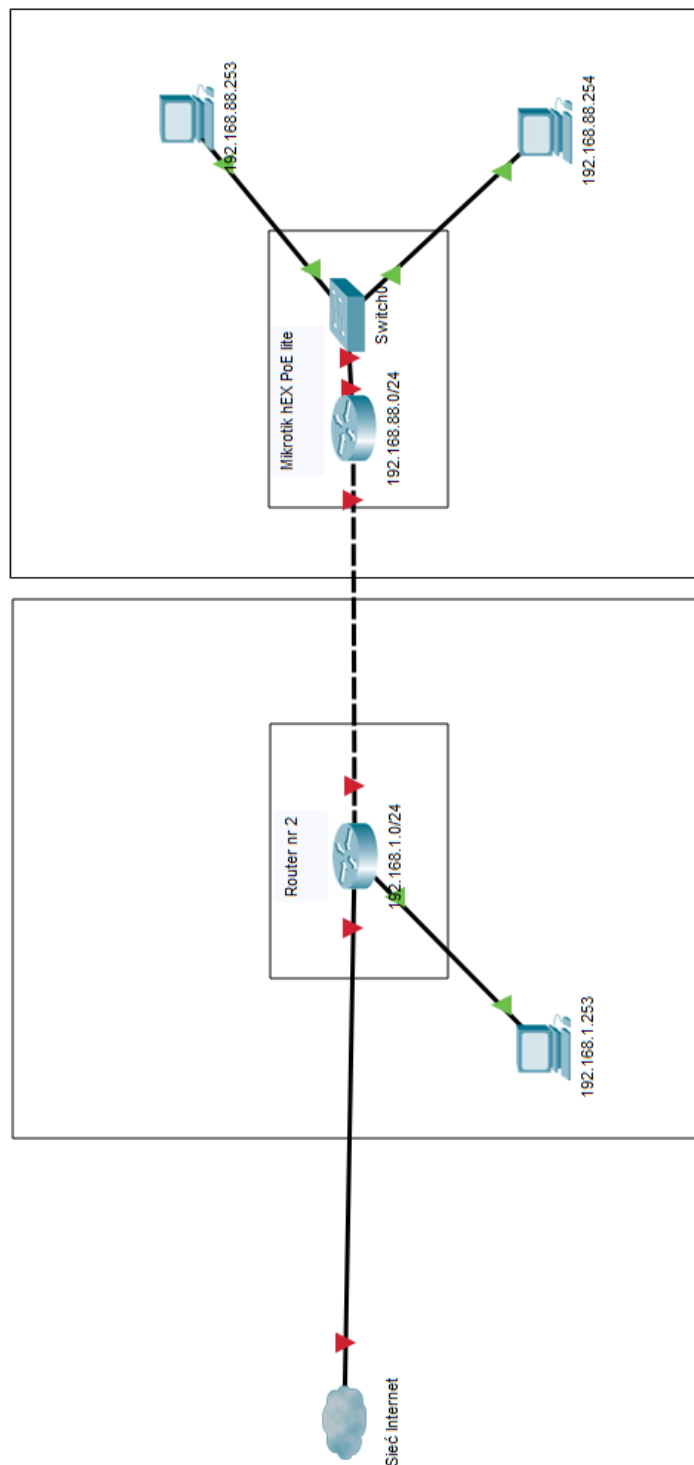


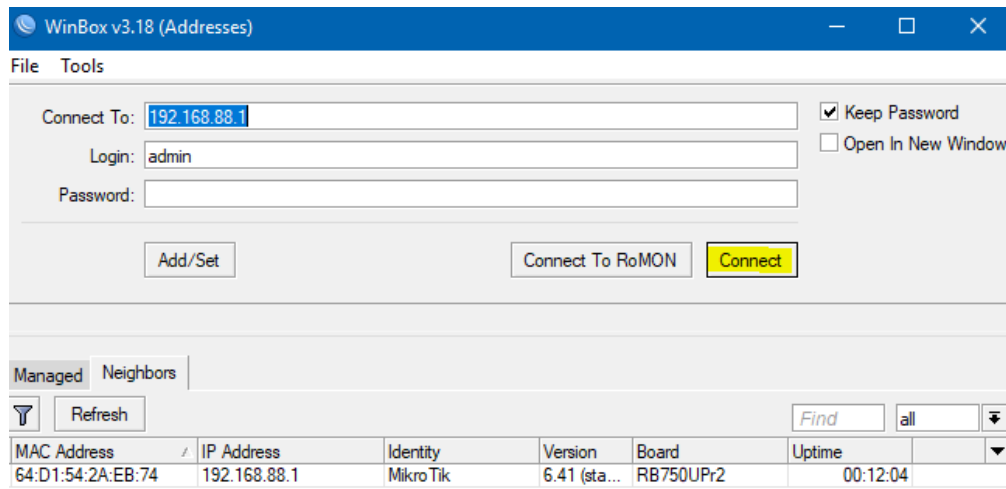
Konfiguracja Firewalla na routerze MikroTik

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



WinBox v3.18 (Addresses)

File Tools

Connect To: 192.168.88.1 ☒ Keep Password ☐ Open In New Window

Login: admin

Password:

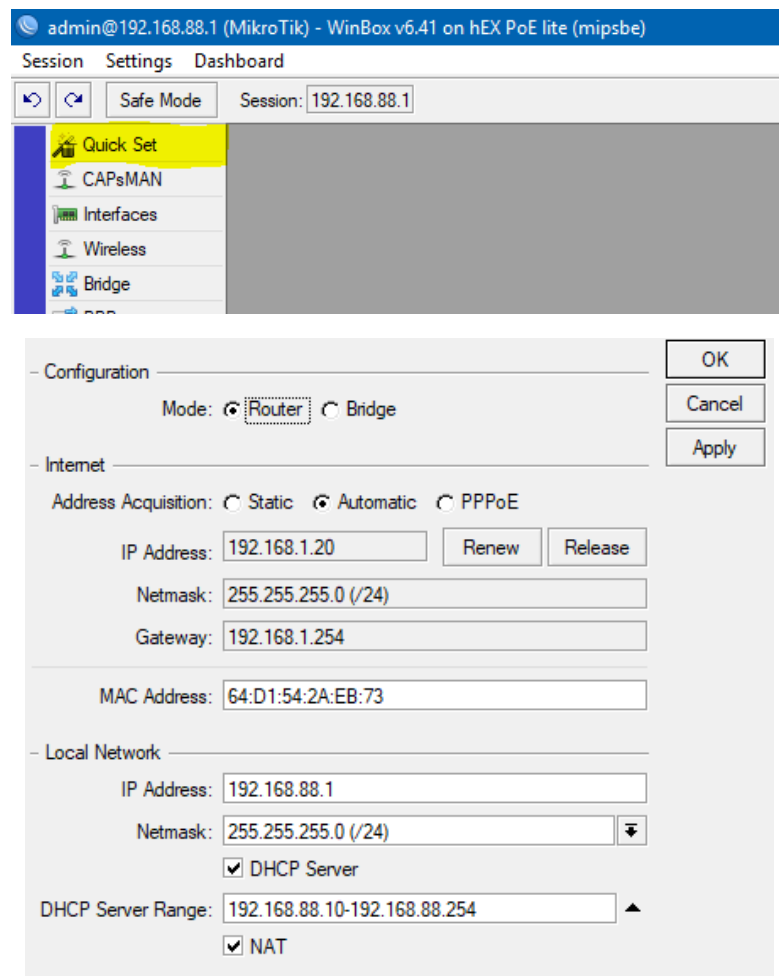
Add/Set Connect To RoMON **Connect**

Managed Neighbors

Refresh Find all

MAC Address	IP Address	Identity	Version	Board	Uptime
64:D1:54:2A:EB:74	192.168.88.1	Mikro Tik	6.41 (sta...	RB750UPr2	00:12:04

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



admin@192.168.88.1 (MikroTik) - WinBox v6.41 on hEX PoE lite (mipsbe)

Session Settings Dashboard

Safe Mode Session: 192.168.88.1

Quick Set CAPsMAN Interfaces Wireless Bridge

Configuration Mode: ☒ Router ☐ Bridge

Internet Address Acquisition: ☐ Static ☒ Automatic ☐ PPPoE

IP Address: 192.168.1.20 Renew Release

Netmask: 255.255.255.0 (/24)

Gateway: 192.168.1.254

MAC Address: 64:D1:54:2A:EB:73

Local Network IP Address: 192.168.88.1

Netmask: 255.255.255.0 (/24)

☒ DHCP Server

DHCP Server Range: 192.168.88.10-192.168.88.254

☒ NAT

OK Cancel Apply

3. Konfiguracja reguł firewala

a) Wprowadzenie do zarządzania regułami

The image illustrates the process of managing firewall rules in Mikrotik WinBox. It features a sidebar menu on the left with categories like Quick Set, CAPsMAN, Interfaces, Wireless, Bridge, PPP, Switch, Mesh, IP, and MPLS. The 'IP' category is highlighted in yellow. An orange arrow points from this category to a dropdown menu on the right, which lists various services including ARP, Accounting, Addresses, Cloud, DHCP Client, DHCP Relay, DHCP Server, DNS, Firewall, Hotspot, IPsec, Neighbors, Packing, Pool, Routes, SMB, SNMP, Services, Settings, Socks, TFTP, Traffic Flow, UPnP, and Web Proxy. Below these elements, a large blue arrow labeled 'TWORZENIE NOWEJ REGUŁY' (Create New Rule) points to the 'Rules' tab in the main window. Another blue arrow labeled 'AKTUALNE POŁĄCZENIA' (Active Connections) points to the 'Connections' tab. A third blue arrow labeled 'FILTR LISTY REGUŁ' (Filter Rule List) points to the 'Rules' tab. The main window displays a table titled 'LISTA AKTUALNYCH REGUŁ' (List of Active Rules) with columns for #, Action, Chain, Src. Address, Dst. Address, Proto..., Src. Port, Dst. Port, In. Inter..., Out. Inter..., Bytes, and Packets. The table is currently empty, and the status bar at the bottom indicates '11 Items'.

Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Switch
Mesh
IP
MPLS

ARP
Accounting
Addresses
Cloud
DHCP Client
DHCP Relay
DHCP Server
DNS
Firewall
Hotspot
IPsec
Neighbors
Packing
Pool
Routes
SMB
SNMP
Services
Settings
Socks
TFTP
Traffic Flow
UPnP
Web Proxy

TWORZENIE NOWEJ REGUŁY

AKTUALNE POŁĄCZENIA

FILTR LISTY REGUŁ

LISTA AKTUALNYCH REGUŁ

11 Items

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)

Firewall Rule <192.168.88.254>

General	Advanced	Extra	Action	Statistics
---------	----------	-------	--------	------------

Chain:

Src. Address: ☐

Dst. Address:

Protocol: ☐

Firewall Rule <192.168.88.254>

General	Advanced	Extra	Action	Statistics
---------	----------	-------	--------	------------

Action:

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

New Firewall Rule

General	Advanced	Extra	Action	Statistics
---------	----------	-------	--------	------------

Chain:

Src. Address:

Dst. Address: ☐

Protocol: ☐

New Firewall Rule

General	Advanced	Extra	Action	Statistics
---------	----------	-------	--------	------------

Action:

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

New Firewall Rule

General Advanced Extra Action Statistics

Chain:

Src. Address: ☐

Dst. Address:

Firewall Rule <192.168.88.254>

General Advanced Extra Action Statistics

Chain:

Src. Address: ☐

Dst. Address:

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

New Firewall Rule

General Advanced Extra Action Statistics

Chain:

Src. Address:

Dst. Address: ☐

Protocol: ☐

New Firewall Rule

General Advanced Extra Action Statistics

Action:

5) Całkowite zablokowanie możliwości pingowania routera 192.168.88.1

New Firewall Rule

General Advanced Extra Action Statistics

Chain:

Src. Address:

Dst. Address: ☐

Protocol: ☐

New Firewall Rule

General Advanced Extra Action Statistics

Action:

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

New Firewall Rule

General Advanced Extra Action Statistics

Chain:

Src. Address: ☐

Dst. Address: ☐

Protocol: ☐

New Firewall Rule

General Advanced Extra Action Statistics

Action:

7) Zablokowanie komunikacji hosta 192.168.88.254 z hostem 192.168.1.254

New Firewall Rule

General Advanced Extra Action Statistics

Chain:

Src. Address: ☐

Dst. Address: ☐

New Firewall Rule

General Advanced Extra Action Statistics

Action:

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

New Firewall Rule

General Advanced Extra Action Statistics

Chain:

Src. Address: ☐

Dst. Address: ☐

Protocol: ☐

Src. Port:

Dst. Port: ☐

New Firewall Rule

General Advanced Extra Action Statistics

Action:

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

Firewall Rule <192.168.88.0/24->192.168.88.1:53>

General	Advanced	Extra	Action	Statistics
Chain: forward				
Src. Address: ☐ 192.168.88.0/24				
Dst. Address: ☒ 192.168.88.1				
Protocol: ☐ 6 (tcp)				
Src. Port:				
Dst. Port: ☐ 53				

WAŻNE, NEGACJA

New Firewall Rule

General	Advanced	Extra	Action	Statistics
Action: drop				

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).

Firewall Rule <192.168.88.0/24->8.8.8.8:53>

General	Advanced	Extra	Action	Statistics
Chain: forward				
Src. Address: ☐ 192.168.88.0/24				
Dst. Address: ☐ 8.8.8.8				
Protocol: ☐ 6 (tcp)				
Src. Port:				
Dst. Port: ☐ 53				

Firewall Rule <192.168.88.0/24->8.8.8.8:53>

General	Advanced	Extra	Action	Statistics
Action: accept				

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.

New Firewall Rule

General Advanced Extra Action Statistics

Chain:

Src. Address:

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

In. Interface: ☐ ether1

Out. Interface: ☐ bridge

New Firewall Rule

General Advanced Extra Action Statistics

Action:

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

Firewall Rule <>

General Advanced Extra Action Statistics

Chain:

Src. Address:

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

In. Interface:

Out. Interface:

In. Interface List: ☐ WAN

Out. Interface List: ☐ LAN

New Firewall Rule

General Advanced Extra Action Statistics

Action:

13) Zapisywanie zdarzenia wysłania pakietu do dziennika zdarzeń

New Firewall Rule

General Advanced Extra Action Statistics

Chain:

Src. Address: ☐

Dst. Address: ☐

Protocol: ☐

New Firewall Rule

General Advanced Extra Action Statistics

Action:

☒ Log

Log Prefix:

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:

Firewall Rule <192.168.88.254->192.168.1.254>

General Advanced Extra Action Statistics

Connection Limit

Limit

Rate: ☐ 5 / min

Burst: 5

Mode: ☒ packet ☐ bit

Do drugiej ustalić action na drop.

Firewall Rule <192.168.88.254->192.168.1.254>

General Advanced Extra Action Statistics

Action: 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)	

```
Reply from 192.168.1.254: bytes=32 time=1ms TTL=63
Reply from 192.168.1.254: bytes=32 time=2ms TTL=63
Reply from 192.168.1.254: bytes=32 time=1ms TTL=63
Reply from 192.168.1.254: bytes=32 time<1ms TTL=63
Request timed out.
Request timed out.
```

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

New Firewall Rule

General Advanced Extra Action Statistics

Chain: forward

Src. Address: 192.168.88.0/24

Dst. Address:

New Firewall Rule

General Advanced Extra Action Statistics

Action: drop

Time

Time: 7:00:00 - 15:00:00

Days: ☐ sat ☒ fri ☒ thu ☒ wed ☒ tue ☒ mon ☐ sun

16) Zablokowanie połączenia poprzez Winbox innym hostom niż 192.168.88.254

New Firewall Rule

General Advanced Extra Action Statistics

Chain:

Src. Address:

Dst. Address:

Protocol: ☐ 6 (tcp)

Src. Port:

Dst. Port: ☐ 8291

New Firewall Rule

General Advanced Extra Action Statistics

Action:

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

Firewall Rule <192.168.88.0/24>

General Advanced Extra Action Statistics

Chain:

Src. Address: ☐ 192.168.88.0/24

Dst. Address:

Firewall Rule <192.168.88.0/24>

General Advanced Extra Action Statistics

Src. Address List:

Dst. Address List:

Layer7 Protocol:

Content: ☐ onet

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

Przejdź do zakładki NAT w oknie firewall

The screenshot shows the 'New NAT Rule' window with the 'General' tab selected. The 'Name' field is set to 'srcnat'. The 'Src. Address' field is set to '192.168.88.0/24'. The 'Dst. Address' field is empty. The 'Protocol' dropdown is set to '6 (tcp)'. The 'Src. Port' field is empty. The 'Dst. Port' field is set to '80'.

Ustalenie przekierowania na adres serwera Web Proxy na routerze

The screenshot shows the 'New NAT Rule' window with the 'Action' tab selected. The 'Action' dropdown is set to 'dst-nat'. The 'Log' checkbox is unchecked. The 'Log Prefix' field is empty. The 'To Addresses' field is set to '192.168.88.1'. The 'To Ports' field is set to '8080'.

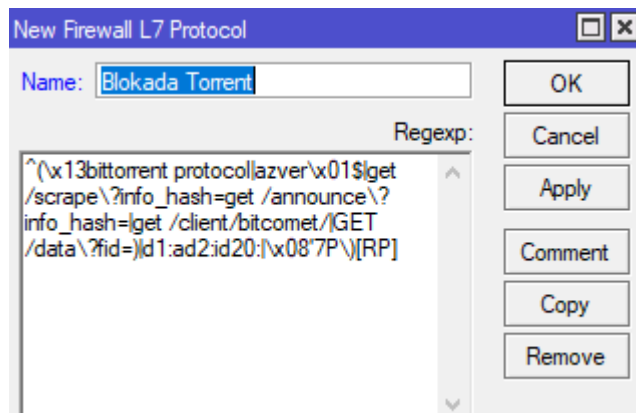
Konfiguracja Web Proxy (Trzeba ustawić OpenDNS po uprzednim zarejestrowaniu się aby nie tłumaczył nazw z domenami o treści niepożądaney)

The screenshot shows the 'Web Proxy Settings' window with the 'General' tab selected. The 'Enabled' checkbox is checked. The 'Src. Address' field is set to '::'. The 'Port' field is set to '8080'. The 'Anonymous' checkbox is unchecked. The 'Parent Proxy' and 'Parent Proxy Port' fields are empty. The 'Cache Administrator' field is set to 'webmaster'. The 'Max. Cache Size' field is set to 'unlimited' with a unit of 'KiB'. The 'Max Cache Object Size' field is set to '2048' with a unit of 'KiB'. The 'Cache On Disk' checkbox is unchecked. The 'Max. Client Connections' field is set to '600'. The 'Max. Server Connections' field is set to '600'. The 'Max Fresh Time' field is set to '3d 00:00:00'. The 'Serialize Connections' and 'Always From Cache' checkboxes are unchecked. The 'Cache Hit DSCP (TOS)' field is set to '4'. The 'Cache Path' field is set to 'web-proxy'.

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

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

Przejdź do zakładki Firewall L7



New Firewall L7 Protocol

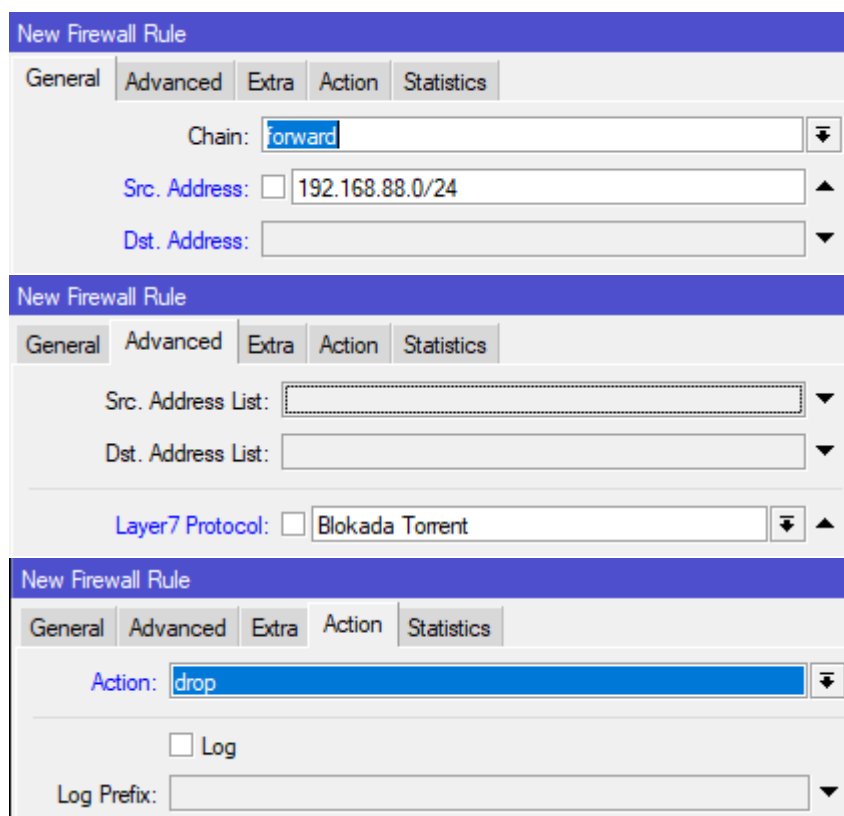
Name:

Regexp:

```
^(\x13bittorrent protocol|azver\x01$|get  
/scrape\?info_hash=get /announce\?  
info_hash=get /client/bitcomet/|GET  
/data\?fid=)|d1:ad2:id20:|\x08'7P\|)[RP]
```

OK
Cancel
Apply
Comment
Copy
Remove

Przejdź ponownie do podstawowej konfiguracji i stwórz nową regułę



New Firewall Rule

General Advanced Extra Action Statistics

Chain:

Src. Address: ☐

Dst. Address:

New Firewall Rule

General Advanced Extra Action Statistics

Src. Address List:

Dst. Address List:

Layer7 Protocol: ☐

New Firewall Rule

General Advanced Extra Action Statistics

Action:

☐ Log

Log Prefix:

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

Przejdź do zakładki Firewall L7

Firewall L7 Protocol <Blokada IMAP>

Name:

Regexp:

Buttons: OK, Cancel, Apply

Przejdź ponownie do podstawowej konfiguracji i stwórz nową regułę

New Firewall Rule

General | Advanced | Extra | Action | Statistics

Src. Address List:

Dst. Address List:

Layer7 Protocol: ☐ Blokada IMAP

New Firewall Rule

General | Advanced | Extra | Action | Statistics

Action:

21) Blokada pobierania plików z rozszerzeniem .png

Firewall L7 Protocol <Blokada png>

Name:

Regexp:

New Firewall Rule

General | Advanced | Extra | Action | Statistics

Chain:

Src. Address:

Dst. Address:

Protocol: ☐ 6 (tcp)

Src. Port:

Dst. Port:

New Firewall Rule

General | Advanced | Extra | Action | Statistics

Src. Address List: ☐

Dst. Address List:

Layer7 Protocol: ☐ Blokada jpeg

New Firewall Rule

General Advanced Extra Action Statistics

Action:

☐ Log

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

New Firewall Rule

General Advanced Extra Action Statistics

Chain:

Src. Address:

Dst. Address: ☐

Protocol: ☐

TCP MSS:

Packet Size: ☐

Firewall Rule <192.168.88.1>

General Advanced Extra Action Statistics

Action:

```
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”

NAT Rule <192.168.88.1:80>

General Advanced Extra Action Statistics

Chain:

Src. Address:

Dst. Address: ☐

Protocol: ☐

Src. Port:

Dst. Port: ☐

NAT Rule <192.168.88.1:80>

General Advanced Extra Action Statistics

Action:

☐ Log

Log Prefix:

To Addresses:

To Ports:

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

NAT Rule <192.168.88.1:80>

General Advanced Extra Action Statistics

Action:

☐ Log

Log Prefix:

To Addresses:

NAT Rule <21,20>

General Advanced Extra Action Statistics

Chain:

Src. Address: ☐

Dst. Address:

Protocol: ☐

Src. Port:

Dst. Port: ☐

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

New Firewall Rule

General Advanced Extra Action Statistics

Chain:

Src. Address:

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

In. Interface: ☐

New Firewall Rule

General Advanced Extra Action Statistics

Src. Address List:

Dst. Address List:

Layer7 Protocol:

Content:

Connection Bytes:

Connection Rate:

Per Connection Classifier:

Src. MAC Address: ☐

New Firewall Rule

General Advanced Extra Action Statistics

Action:

☐ Log

Log Prefix:

Reject With:

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

Wejdź w zakładkę Address List i zdefiniuj dwa adresy

Firewall Address List <host2>

Name: OK

Address: Cancel

Timeout: Apply

Creation Time: Disable

Postępuj zgodnie z adresami w konfiguracji reguły

New Firewall Rule

General Advanced Extra Action Statistics

Src. Address List: ▲

Dst. Address List: ▲

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)

Firewall Address List <komputery pracownia>

Name: OK

Address: Cancel

Timeout: Apply

Creation Time: Disable

komputery pracownia	192.168.88.11	Jun/11/2019 20:...
komputery pracownia	192.168.88.10	Jun/11/2019 20:...
komputery pracownia	192.168.88.12	Jun/11/2019 20:...

Firewall Rule <192.168.88.1>

General Advanced Extra Action Statistics

Src. Address List: ▲

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

Firewall Address List <last tcp>

Name:

Address:

Timeout:

Creation Time:

New Firewall Rule

General Advanced Extra Action Statistics

Action:

☐ Log

Log Prefix:

Address List:

Timeout:

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

New Firewall Rule

General Advanced Extra Action Statistics

Chain:

Src. Address: ☐

New Firewall Rule

General Advanced Extra Action Statistics

Connection Limit

Limit

Dst. Limit

Nth

Time

Src. Address Type

Address Type:

☐ Invert

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

New Firewall Rule

General Advanced Extra Action Statistics

Action: add src to address list

☐ Log

Log Prefix:

Address List: google

Timeout: 00:30:00

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

New Firewall Rule

General Advanced Extra Action Statistics

Src. Address List:

New Firewall Rule

General Advanced Extra Action Statistics

Action: drop

add src to address...	forward	192.168.88.0/24					336 B	6
drop	forward						2537 B	47