

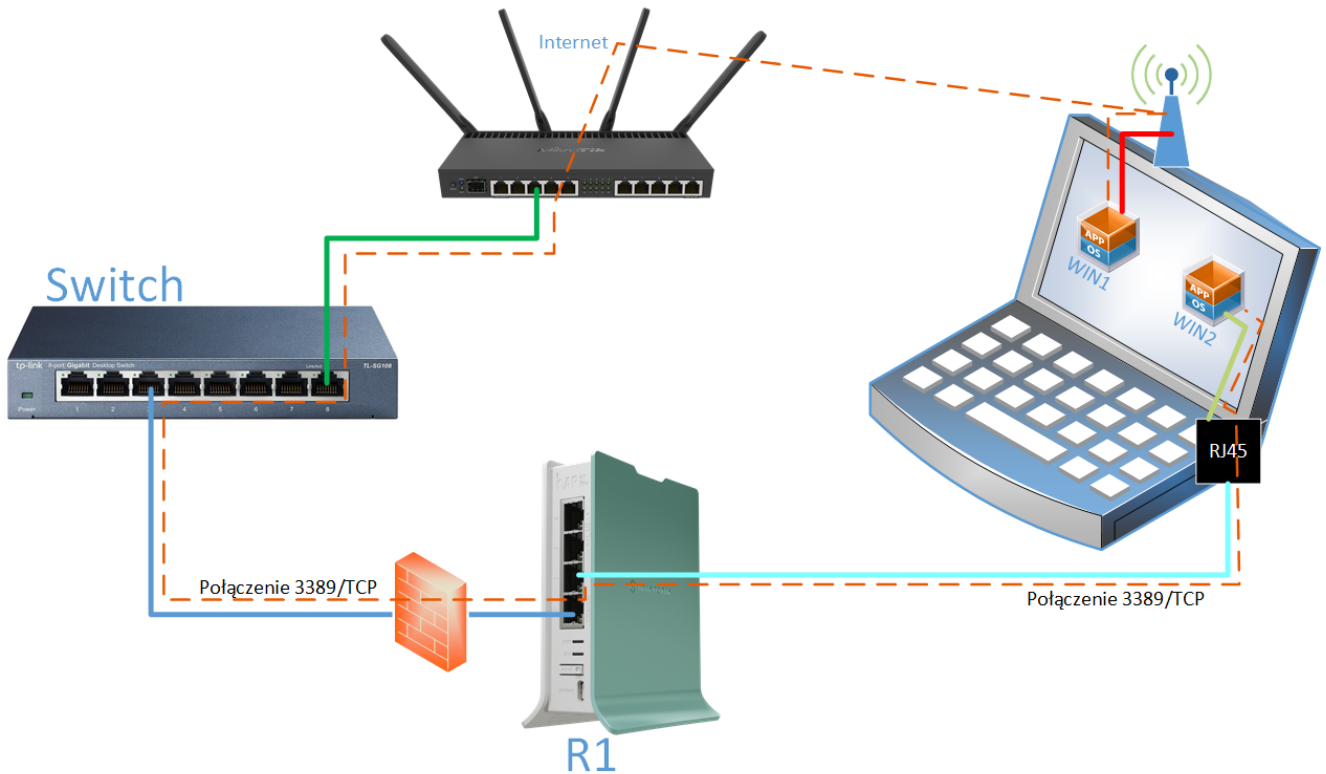
# Mikrotik – FireWall i kształtowanie ruchu – szkolenie

written by archi | 17 lutego 2025

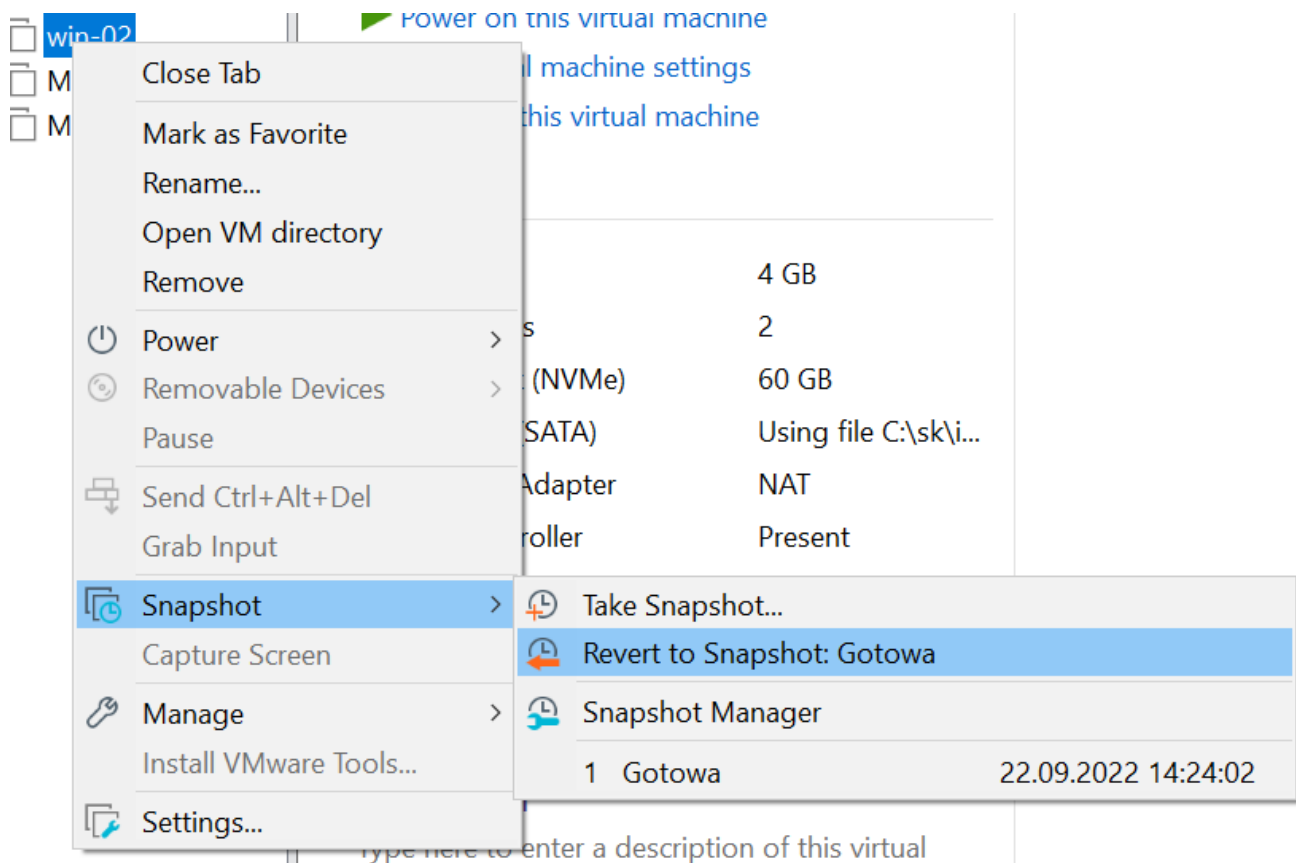
## **Mikrotik - FireWall i kształtowanie ruchu - szkolenie**

### **I. TUNELOWANIE**

Celem jest skonfigurowanie przekierowanie portów (port forwarding) z wykorzystaniem urządzenia Mikrotik. Wykorzystamy w tym celu dwie maszyny wirtualne Win1 i Win2, które posłużą do zestawienia połączenia (kreskowana czerwona linia) Remote Desktop Services (RDS, port 3389/tcp) do maszyny Win2 (sieć lokalna) z maszyny Win1 będącej poza siecią lokalną (z łącza zewnętrznego – czyli z Internetu).



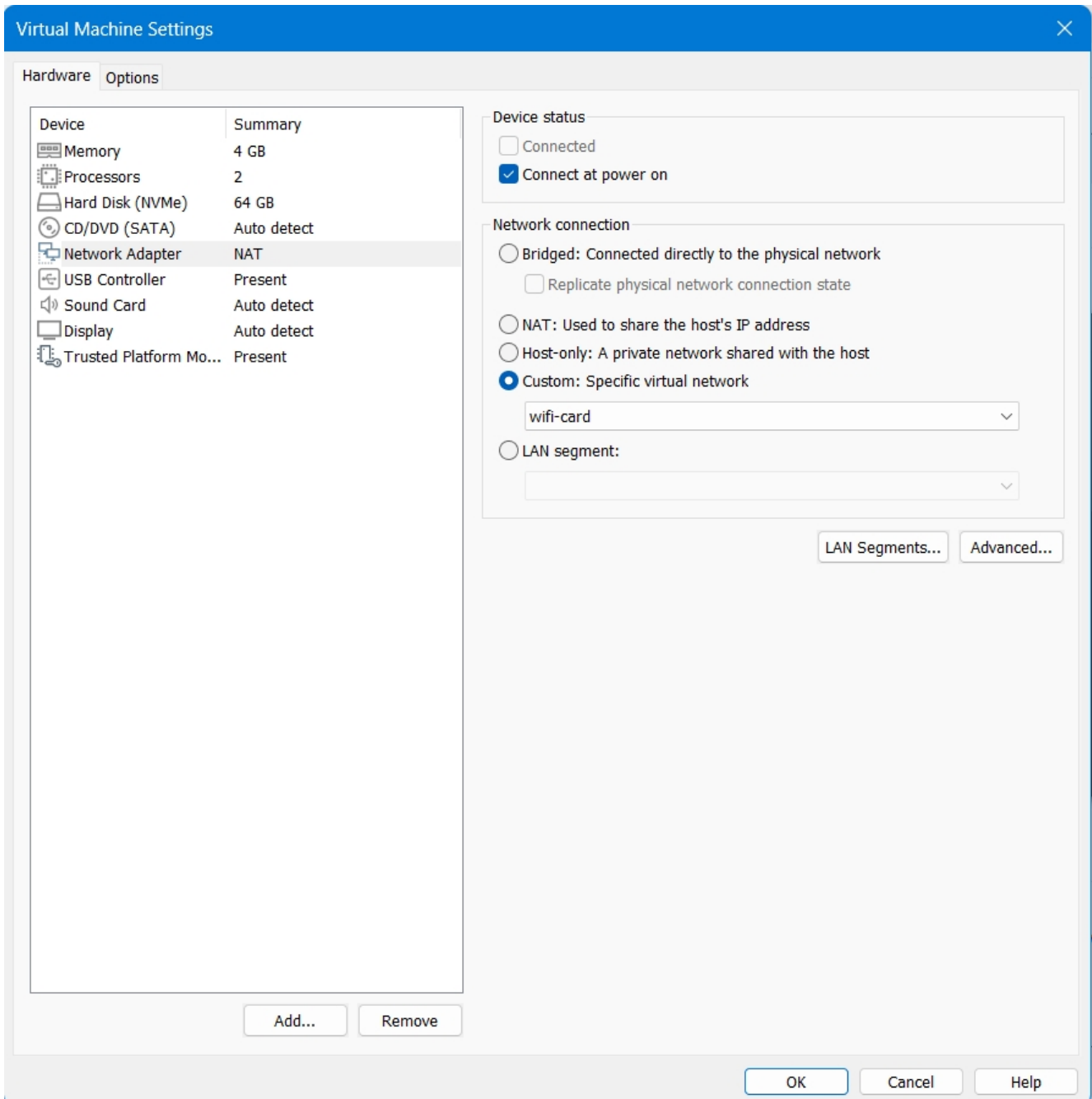
1. Podłącz komputer (port RJ45 z komputera lub przejściówki) do routera R1 na porcie Ether2
2. Podłącz router R1 (port **Ether1**) do Internetu (Switch).
3. Uruchom VMware Workstation. Przywróć migawkę dla obu maszyn win-01 i win-02, aby miały ustawienia domyślne



4. Zmień ustawienia maszyn wirtualnych, tak aby

- maszyna win-01 była podłączona do Custom->wifi-card,
- maszyna win-02 była podłączona do Bridged.

**Włącz obydwie maszyny.**



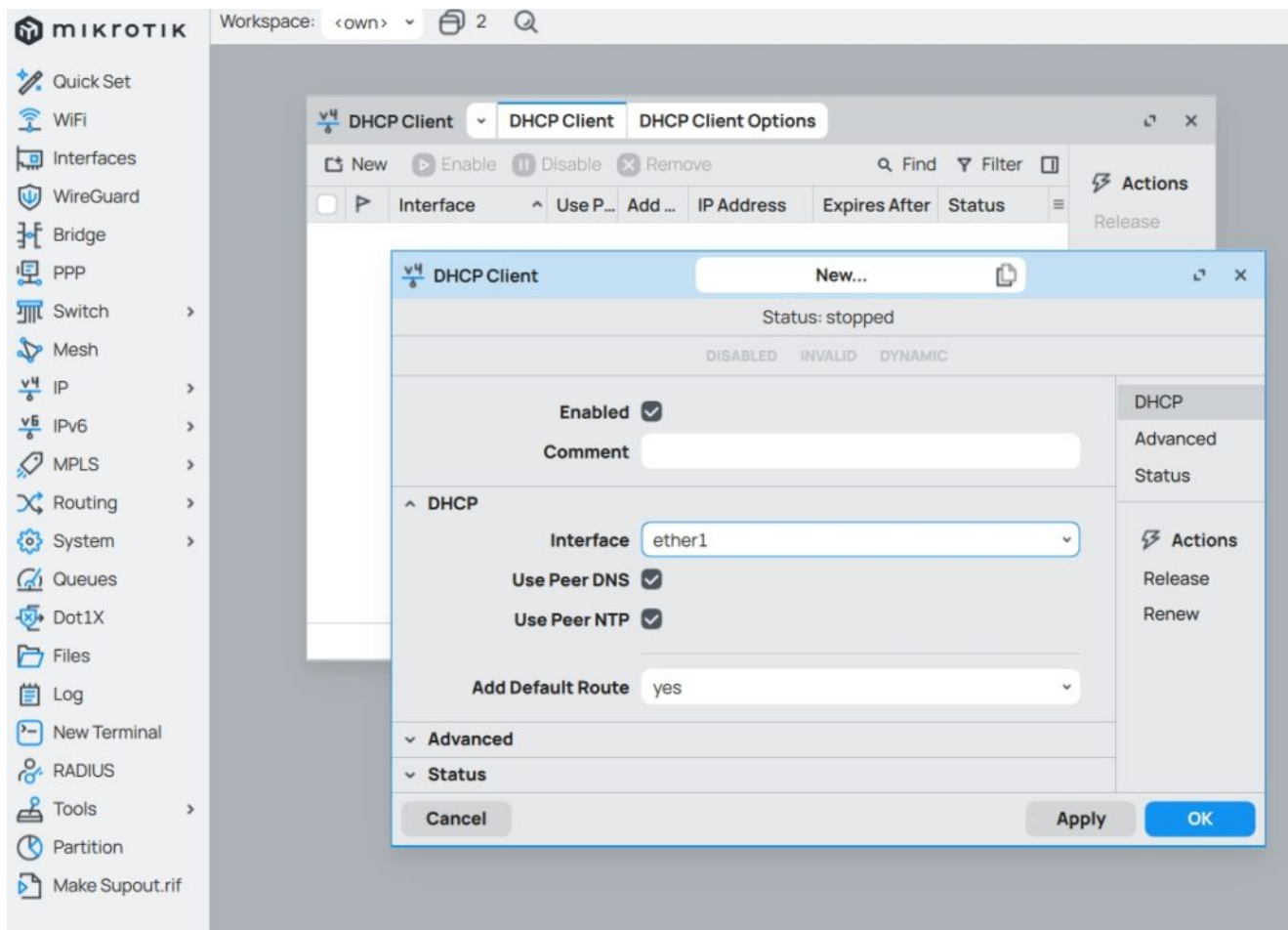
5. Uruchom aplikację Winbox (link do pobrania aplikacji (plik ZIP należy rozpakować np. na Pulpit):

[https://download.mikrotik.com/routeros/winbox/4.0beta17/WinBox\\_Windows.zip](https://download.mikrotik.com/routeros/winbox/4.0beta17/WinBox_Windows.zip))

6. Zlokalizuj swoje urządzenie MikroTik w sekcji „Neighbors”

7. Połącz się do routera R1 i wykonaj następujące czynności:

a) Ustaw DHCP-Client na porcie Ether1



b) Dodaj interfejs Bridge i przypisz do niego port Ether2

Bridge New...

DISABLED DYNAMIC INVALID RUNNING SLAVE PASSTHROUGH

Enabled

Comment

^ General

Name

Type Bridge

MTU  Actual MTU

L2 MTU

MAC Address

ARP

ARP Timeout  Admin. MAC Address

Ageing Time

Max Learned Entries

IGMP Snooping

DHCP Snooping

Fast Forward

General

STP

VLAN

Status

Traffic

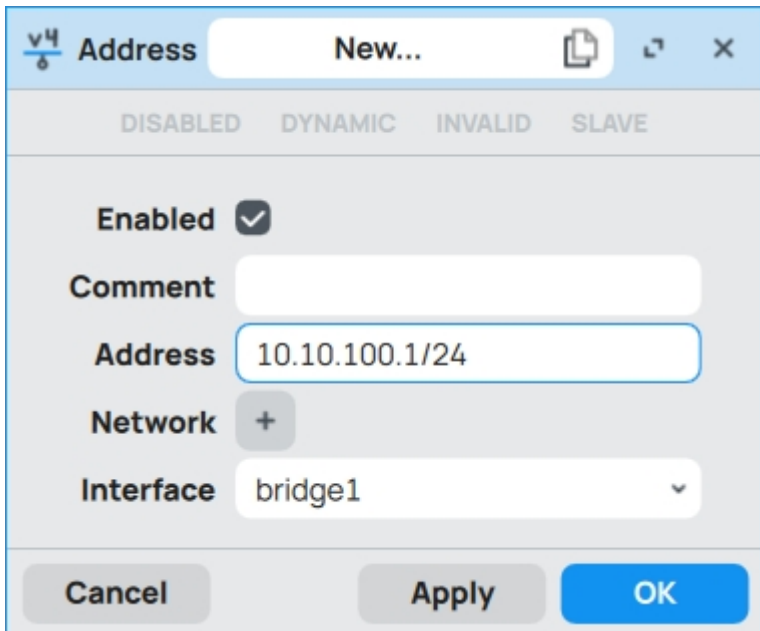
⚡ Actions

Torch

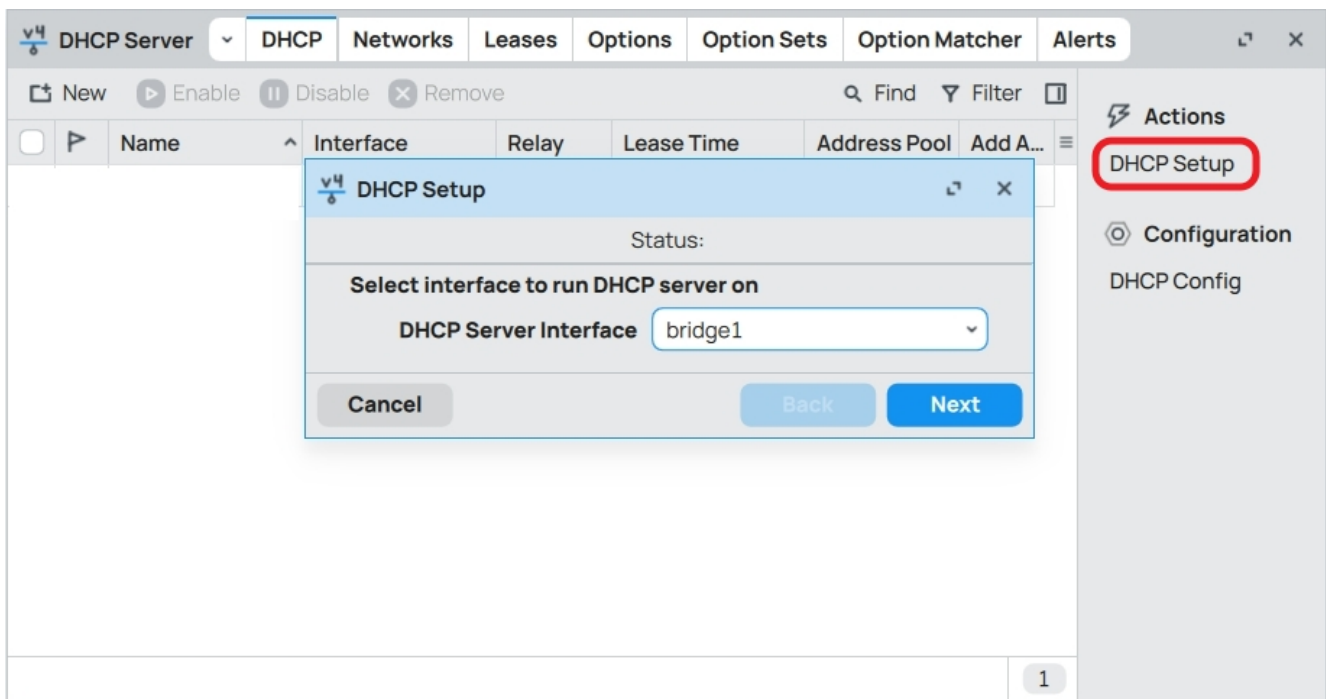
Reset Traffic Counters

Cancel Apply OK























c) Nadaj adres IP dla bridge1 10.10.100.1/24



d) Skonfiguruj serwer DHCP na interfejsie bridge1



e) W menu IP->Firewall w zakładce NAT utwórz maskowanie adresów IP „masquerade” dla pakietów wychodzących przez Ether1.

-  Quick Set
-  WiFi
-  Interfaces
-  WireGuard
-  Bridge
-  PPP
-  Switch >
-  Mesh
-  IP >
-  IPv6 >
-  MPLS >
-  Routing >
-  System >
-  Queues
-  Dot1X
-  Files
-  Log
-  New Terminal
-  RADIUS
-  Tools >
-  Partition
-  Make Supout.tif

ARP	Kid Control	Services
Addresses	Media	Settings
Cloud	NAT PMP	Socks
DHCP Client	Neighbors	TFTP
DHCP Relay	Packing	Traffic Flow
DHCP Server	Pool	UPnP
DNS	Routes	VRF
<b>Firewall</b>	SMB	Web Proxy
Hotspot	SNMP	
IPsec	SSH	



NAT New...

DISABLED DYNAMIC INVALID

Enabled

Comment

**General**

Chain

Src. Address

Dst. Address

Src. Address List

Dst. Address List

---

Protocol

Src. Port

Dst. Port

Any. Port

In. Interface

Out. Interface

---

In. Interface List

Out. Interface List

---

Packet Mark

Connection Mark

Routing Mark

---

Connection Type

**Advanced**

**Extra**

**Action**

Action

Log

Log Prefix

To Ports

**Statistics**

**Actions**

Reset Counters

Reset All Counters

Cancel Apply

f) W tym samym miejscu utwórz tunelowanie do win-02 (port forwarding):

- Chain: dstnat,
- Protocol: 6 (tcp),
- Dst. port: 3389 (usługa pulpitu zdalnego),
- In. Interface: ether1 (dla interfejsu wchodzącego)
- Action / Action: dst-nat
- Action / To Addresses: adres IP maszyny win-02 (ustal poleceniem ipconfig w wierszu poleceń „Command Prompt” w maszynie win-02, jeżeli twój adres to 169.254.x.x to znaczy że maszyna win-02 nie pobrała prawidłowego adresu z serwera DHCP),
- Action / To Ports: 3389.

NAT New...

DISABLED DYNAMIC INVALID

Enabled

Comment

**General**

Chain

Src. Address

Dst. Address

Src. Address List

Dst. Address List

Protocol

Src. Port

Dst. Port

Any. Port

In. Interface

Out. Interface

In. Interface List

Out. Interface List

Packet Mark

Connection Mark

Routing Mark

Connection Type

**Advanced**

**Extra**

**Action**

Action

Log

Log Prefix

To Addresses

To Ports

**Statistics**

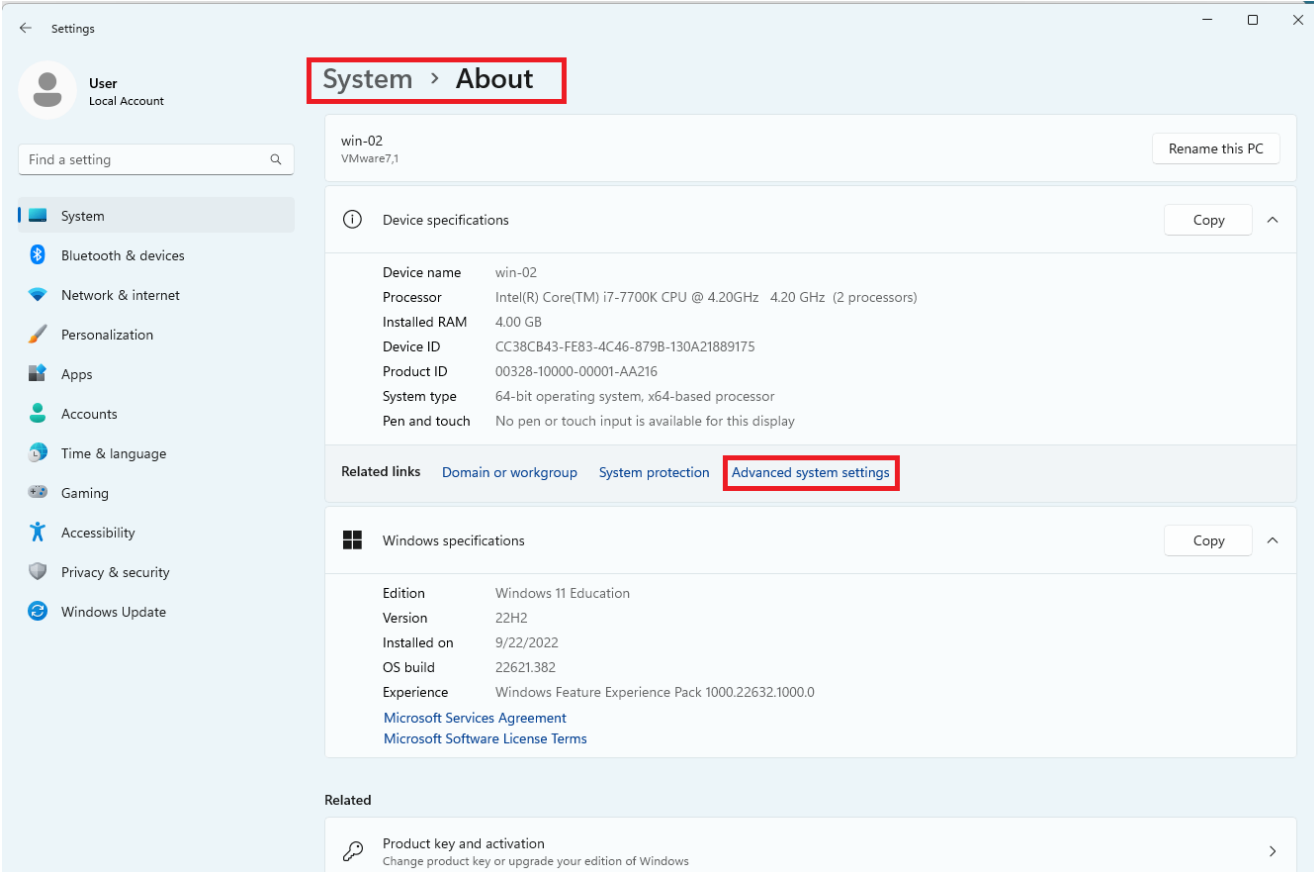
**Actions**

Reset Counters

Reset All Counters

Cancel Apply **OK**

## 8. Na maszynie win-02 skonfiguruj możliwość podłączania się do pulpitu zdalnego



The screenshot shows the Windows Settings application, specifically the 'System > About' page. The page displays system information for a machine named 'win-02' (VMware7,1). The 'Device specifications' section lists hardware details, and the 'Windows specifications' section lists OS details. The 'Advanced system settings' link is highlighted with a red box. The 'Related' section at the bottom shows 'Product key and activation'.

**System > About**

win-02  
VMware7,1 Rename this PC

**Device specifications** Copy ^

Device name	win-02
Processor	Intel(R) Core(TM) i7-7700K CPU @ 4.20GHz 4.20 GHz (2 processors)
Installed RAM	4.00 GB
Device ID	CC38CB43-FE83-4C46-879B-130A21889175
Product ID	00328-10000-00001-AA216
System type	64-bit operating system, x64-based processor
Pen and touch	No pen or touch input is available for this display

**Related links** [Domain or workgroup](#) [System protection](#) **[Advanced system settings](#)**

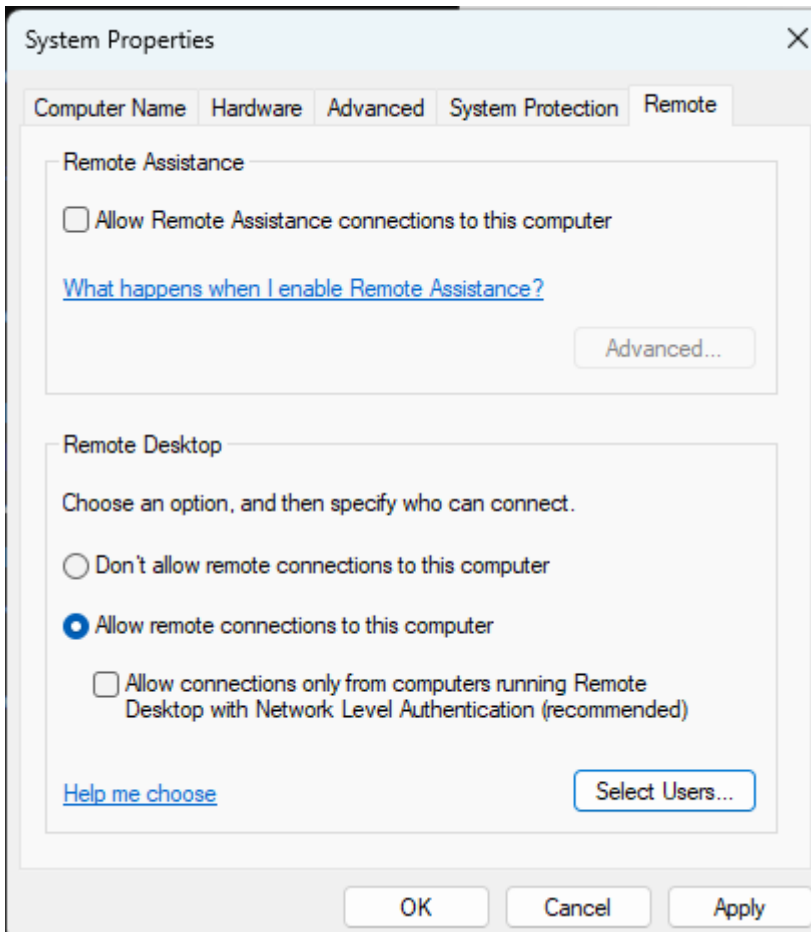
**Windows specifications** Copy ^

Edition	Windows 11 Education
Version	22H2
Installed on	9/22/2022
OS build	22621.382
Experience	Windows Feature Experience Pack 1000.22632.1000.0

[Microsoft Services Agreement](#)  
[Microsoft Software License Terms](#)

**Related**

[Product key and activation](#)  
Change product key or upgrade your edition of Windows >



9. Dodaj użytkownika do systemu win-02 aby móc na niego połączyć się na koniec laboratorium.

```
net user user1 user1 /add
```

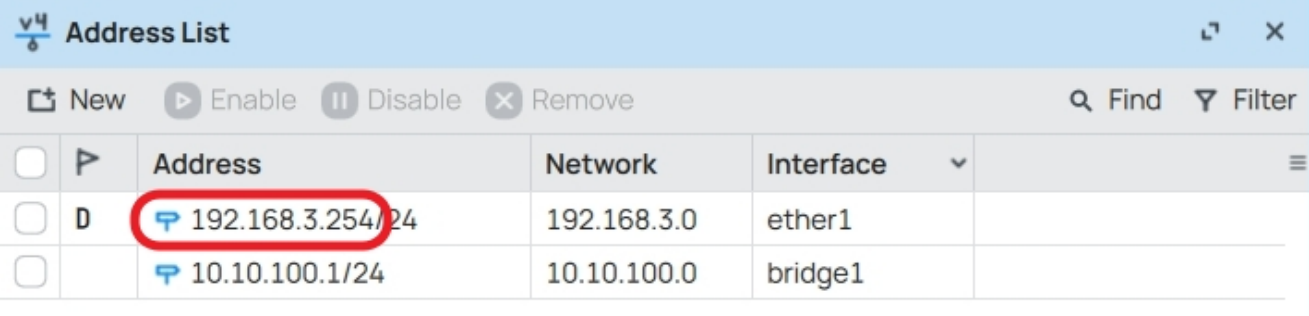
```
Administrator: Command Prompt
C:\Windows\System32>net user user1 user1 /add
The command completed successfully.
C:\Windows\System32>_
```

```
net localgroup administrators user1 /add
```

```
C:\Windows\System32>net localgroup administrators user1 /add
The command completed successfully.
C:\Windows\System32>_
```

Utworzyłeś konto user1 z hasłem user1 oraz dodałeś go do grupy administratorów tego komputera

10. Z maszyny win-01 uruchom połączenie pulpitu zdalnego na adres routera R1. Adres routera sprawdź w /IP/ADDRESSES przypisany na porcie Ether1




<input type="checkbox"/>	<input type="checkbox"/>	Address	Network	Interface	
<input type="checkbox"/>	D	192.168.3.254/24	192.168.3.0	ether1	
<input type="checkbox"/>		10.10.100.1/24	10.10.100.0	bridge1	

11. Powinna nastąpić inicjalizacja pulpitu zdalnego do maszyny win-02






Q remote|Desktop Connection

All Apps Documents Web More ▾

**Best match**


 **Remote Desktop Connection**  
App

**Settings**

- < Remote desktop settings >
-  Remote Desktop Developer Settings >
-  RemoteApp and Desktop Connections >
-  Allow Remote Assistance invitations to be sent from this >
-  Access RemoteApp and desktops >
-  Enable Device Portal >
- < Select users that can remotely access this PC >

**Search the web**






Q remote - See web results >





### Remote Desktop Connection

App

---

-  Open
-  Run as administrator
-  Open file location
-  Pin to Start
-  Pin to taskbar

 Podłączanie pulpitu zdalnego




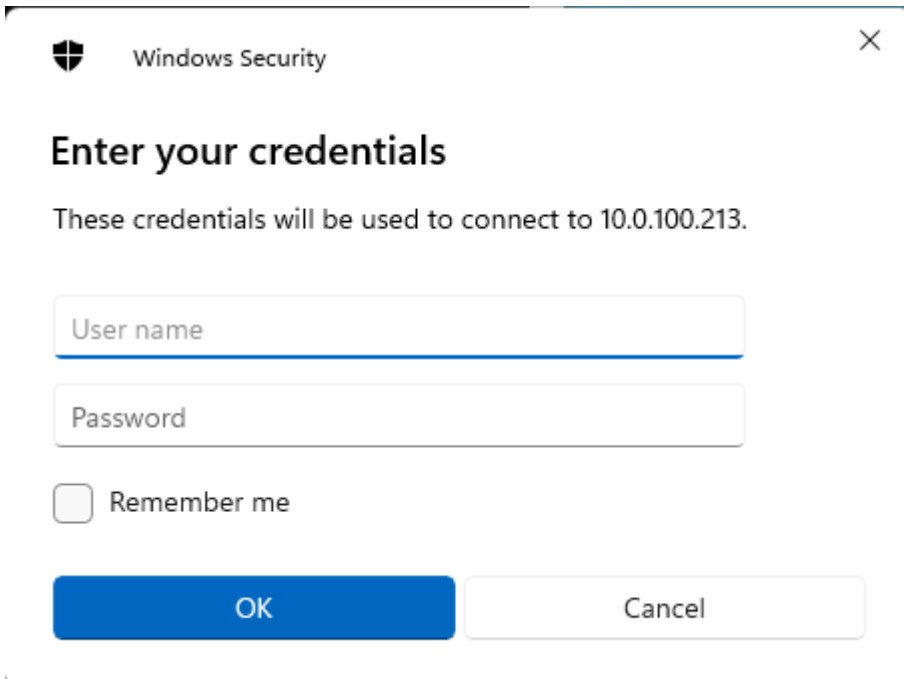
## Podłączanie pulpitu zdalnego

Komputer:

Nazwa użytkownika: Nie określono

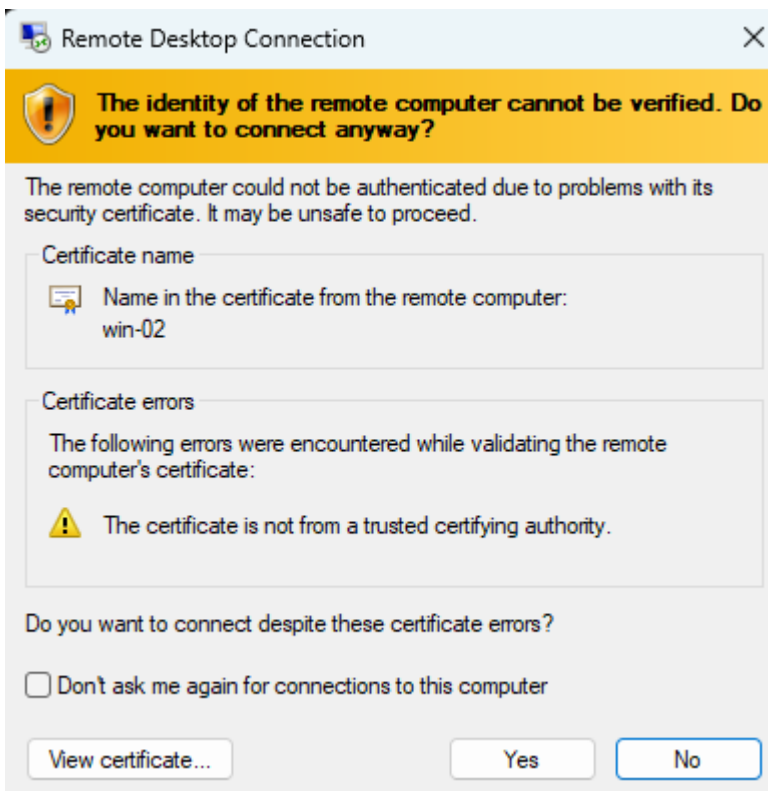
Podczas łączenia zostanie wyświetlony monit o podanie poświadczeń.

 Pokaż opcje



12. Użyj konta user1 i jego hasła do podłączenia się z drugim komputerem (maszyną win-02)

13. Potwierdź certyfikat stacji do której wykonujesz połączenie. Potwierdź wylogowanie domyślnie zalogowanego użytkownika i zatwierdź kolejne ekrany tak żeby uzyskać połączenie zdalnego pulpitu.







**user1**

Another user is signed in. If you continue, they'll be disconnected. Do you want to sign in anyway?

Yes

No



**user1**



**Please wait for WIN-02\User to respond.**

## Remote Desktop Connection

Do you want to allow WIN-02\user1 to connect to this machine?

Click OK to disconnect your session immediately or click Cancel to stay connected.

No action will disconnect your session in 30 seconds.

OK

Cancel



**user1**



**Welcome**

## Let Microsoft and apps use your location

Choose your settings, then select **Accept** to save them. Check the **Learn more** link for info on these settings, how to change them, how Windows helps protect you from unsafe apps and web content, and the related data transfers and uses.



Yes

Get location-based experiences like directions and weather. Let Windows & apps request your location. Microsoft will use location data to improve location services.

No

You won't be able to get location-based experiences like directions and weather or enjoy other services that require your location to work.

[Learn more](#)

Accept



14. **Rozłącz pulpit zdalny.** Przekierowanie portów można wykonać do wielu komputerów za routerem, tylko dla każdego z nich trzeba ustawić inny numer portu na którym nawiązesz połączenie. Zmień w NAT Rule parametr „**Dst. port**” z **3389** na **9000**. Ponownie nawiąż połączenie z pulpitem zdalnym. Tym razem połącz się na porcie a.b.c.d:9000

Firewall Filter Rules NAT 9000

DISABLED DYNAMIC INVALID

Enabled  Comment

**General**

Chain dstnat

Src. Address +

Dst. Address +

Src. Address List +

Dst. Address List +

Protocol 6 (tcp) -

Src. Port +

Dst. Port 9000 -

Any. Port +

In. Interface ether1 -

Out. Interface +

In. Interface List +

Out. Interface List +

Packet Mark +

Connection Mark +

Routing Mark +

Connection Type +

**Advanced**

**Extra**

**Action**

Action dst-nat

Log

Log Prefix +

To Addresses 10.10.100.???

To Ports 3389

**Statistics**

Actions

Reset Counters

Reset All Counters

General

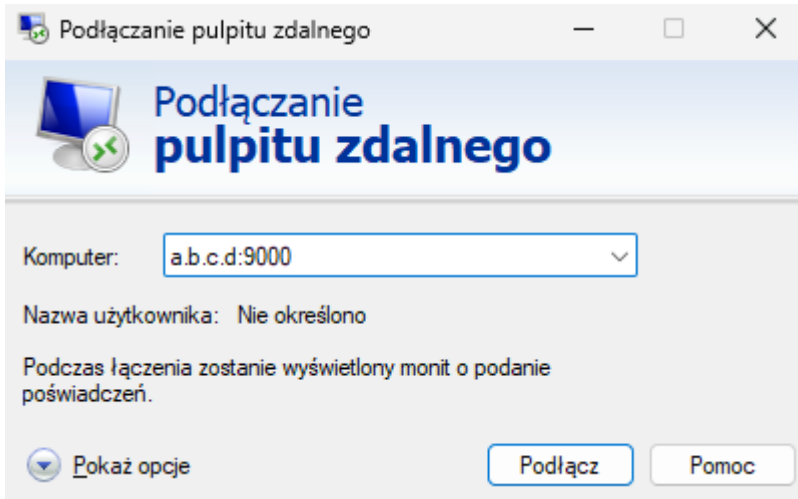
Advanced

Extra

Action

Statistics

Cancel Apply OK



14a. **Rozłącz pulpit zdalny.** Przejdź do następnych punktów laboratorium.

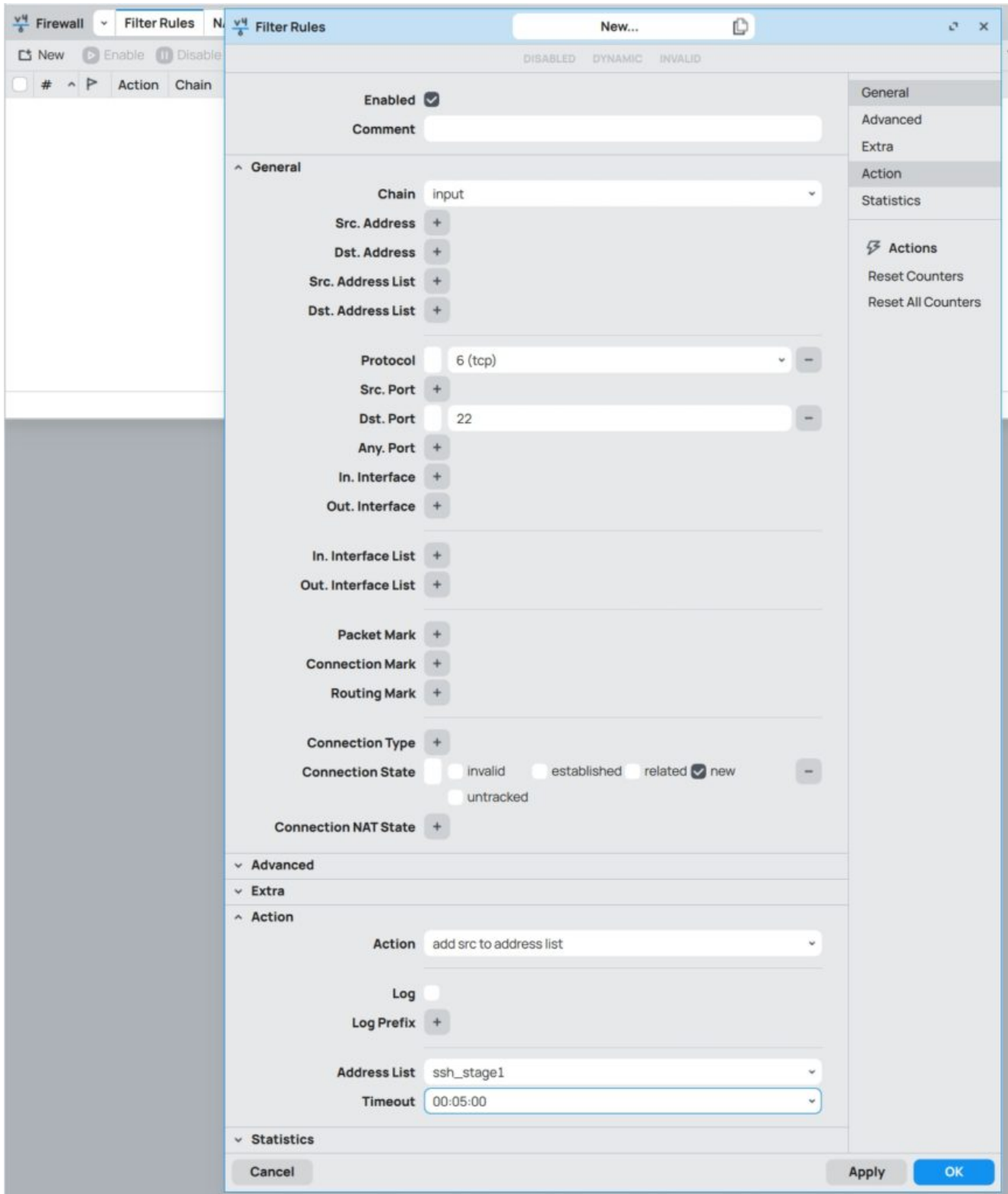
---

## II. WYKORZYSTANIE LIST - Honeypot

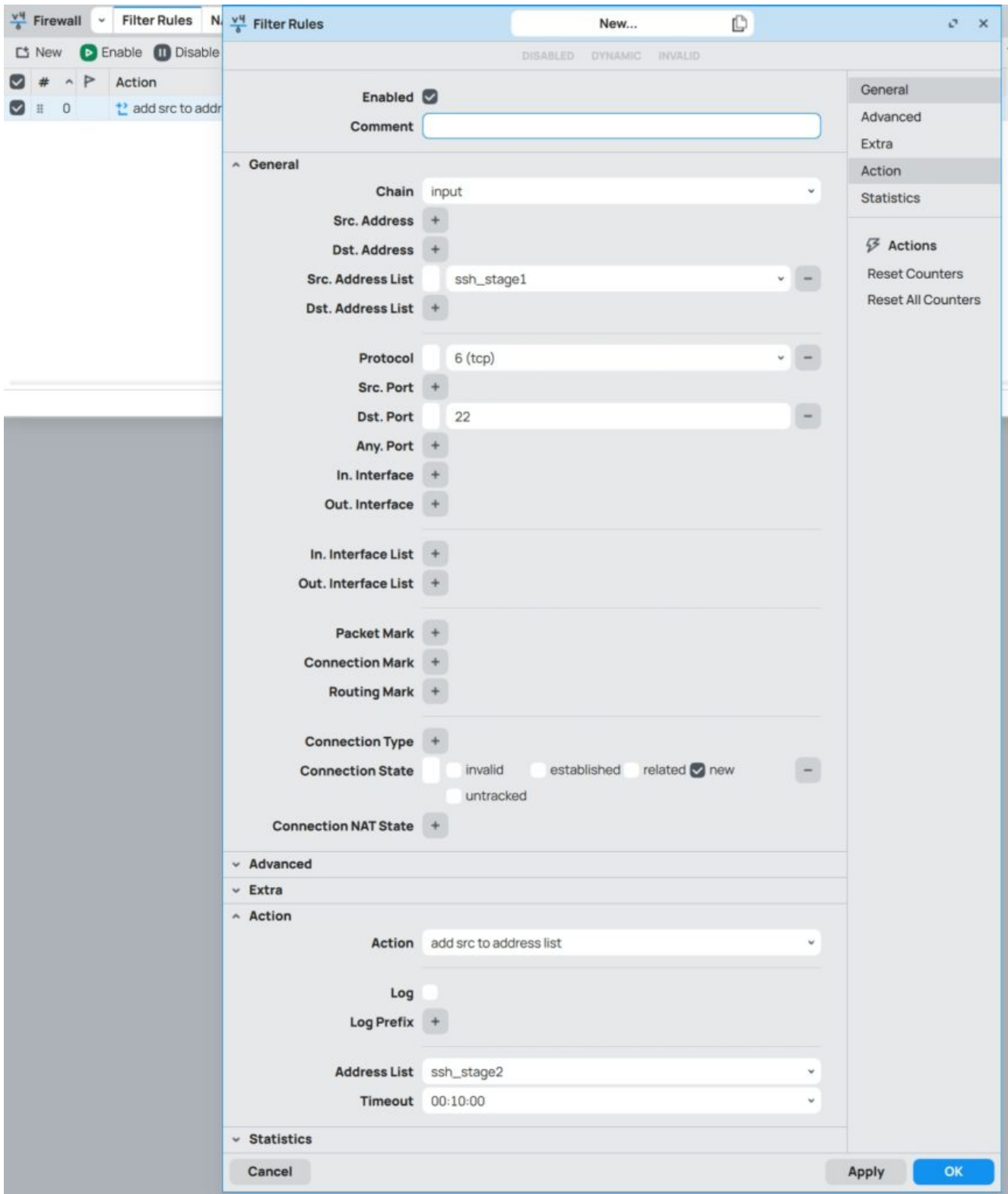
Celem jest zbudowanie autonomicznej obrony przez próbami ataku na nasze urządzenie MikroTik.

15. W oknie FireWall przejdź do zakładki „Filter Rules”. Ustawimy Honeypot (pułapkę) na jednym z portów często skanowanych w sieci w celu ataku. Musimy utworzyć kilka wpisów (w kolejności odwrotnej bo reguły FireWall przetwarzane są sekwencyjnie) pozwalających na wychwytywanie tylko tych adresów IP które kilkakrotnie będą próbować się łączyć na nasz router.

a) Utwórz regułę na łańcuchu „input”, protokół TCP, port docelowy „22”, stan połączenia „Connection State” nowy „new” z akcją „add src to address list”, do listy np. „ssh\_stage1” w polu „Address List” (trzeba wpisać z ręki) i czasem przebywania w liście 5min „Timeout” 00:05:00



b) Utwórz kolejną regułę jak w pkt a) tylko dodamy zależność dotyczącą listy tj. jeśli jest w liście ssh\_stage1 i ponownie się połączył do serwisu SSH to przeniesiemy go do kolejnej listy ssh\_stage2 z czasem przebywanie 10min.



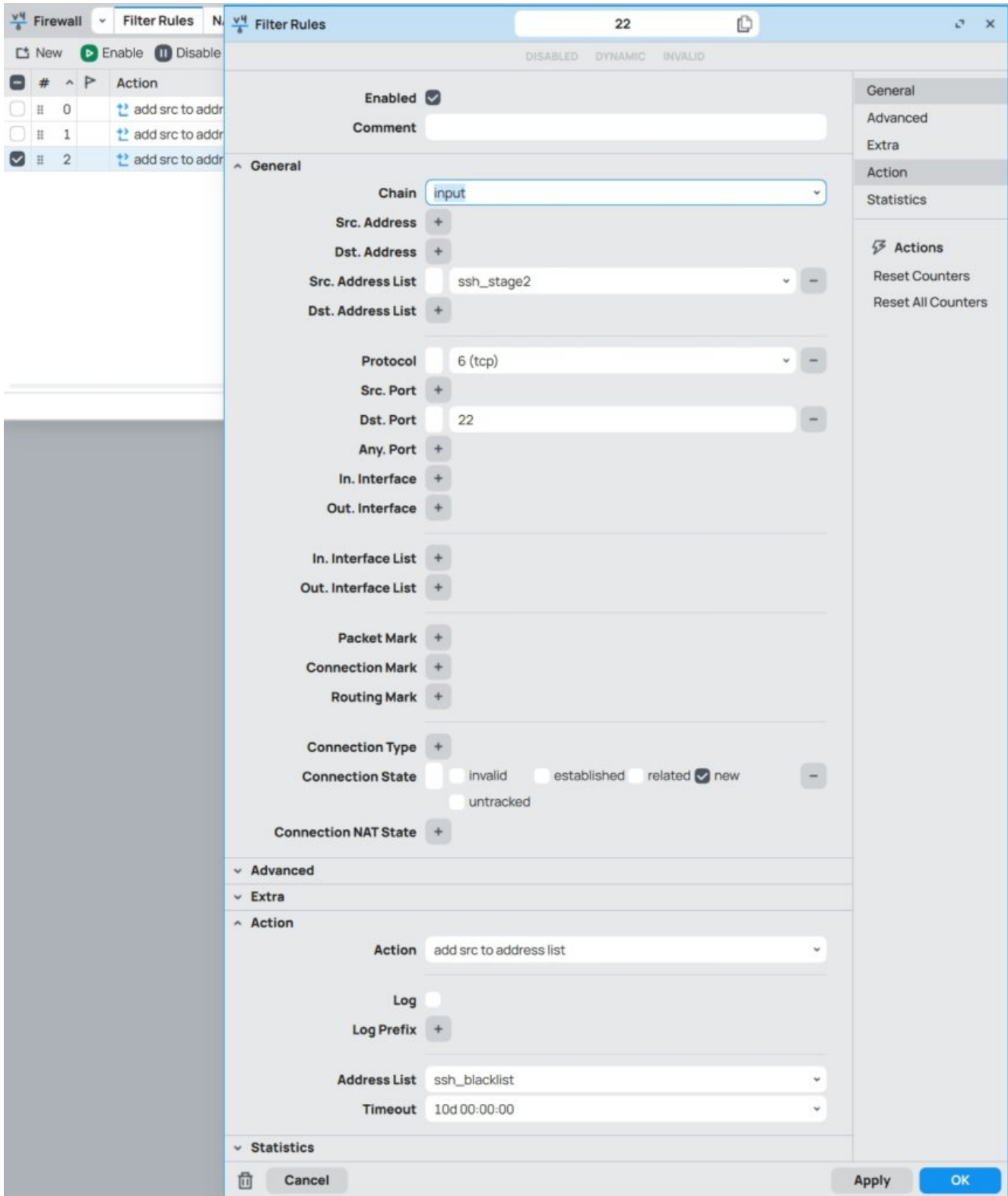
c) reguła utworzyła się domyślnie na końcu listy, co spowodowałoby niepoprawne działanie. Musimy ją przesunąć do góry. Zaznacz regułę myszką i przeciągnij ją wyżej.



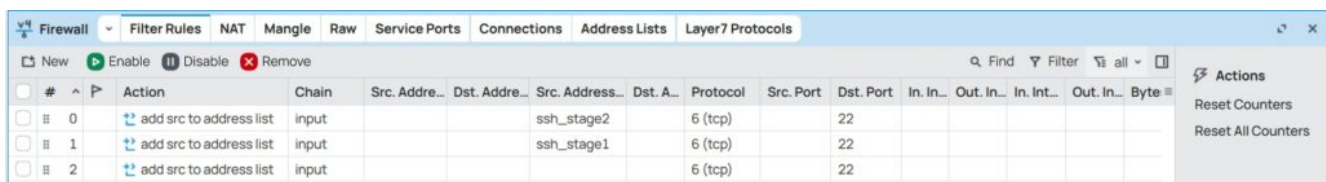
Firewall																
Filter Rules																
NAT																
Mangle																
Raw																
Service Ports																
Connections																
Address Lists																
Layer7 Protocols																
New Enable Disable Remove																
Find Filter all																
#	^	▶	Action	Chain	Src. Addre...	Dst. Addre...	Src. Address...	Dst. A...	Protocol	Src. Port	Dst. Port	In. In...	Out. In...	In. Int...	Out. In...	Byte
0			add src to address list	input			ssh_stage1		6 (tcp)		22					
1			add src to address list	input					6 (tcp)		22					

Firewall																
Filter Rules																
NAT																
Mangle																
Raw																
Service Ports																
Connections																
Address Lists																
Layer7 Protocols																
New Enable Disable Remove																
Find Filter all																
#	^	▶	Action	Chain	Src. Addre...	Dst. Addre...	Src. Address...	Dst. A...	Protocol	Src. Port	Dst. Port	In. In...	Out. In...	In. Int...	Out. In...	Byte
0			add src to address list	input			ssh_stage1		6 (tcp)		22					
1			add src to address list	input					6 (tcp)		22					

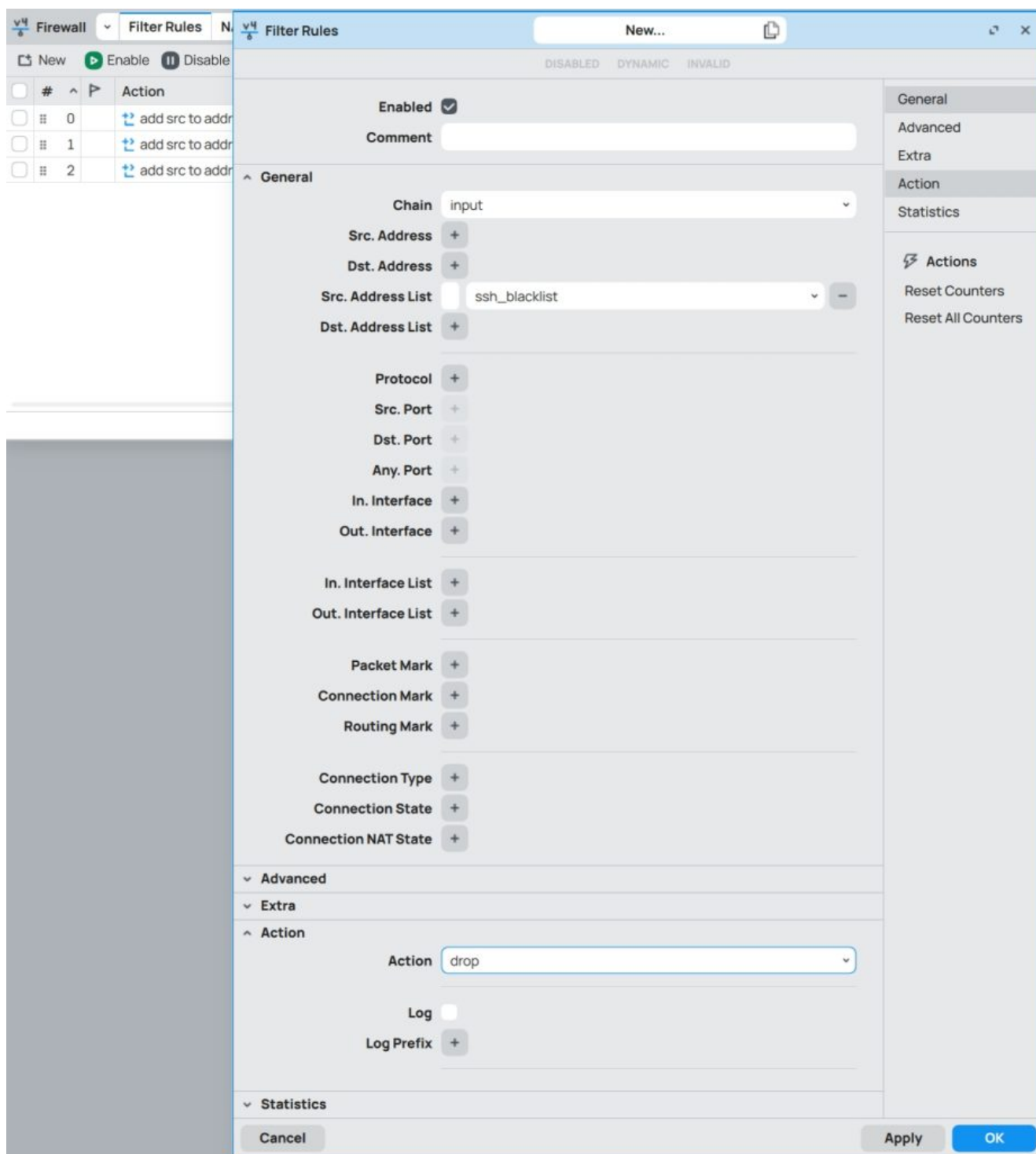
d) dodamy ostatnią regułę list „ssh\_blacklist” którą wykorzystamy w kolejnej (następnej) regule do blokowania połączeń. Powtórz czynności w pkt. b i c, tworząc zbieranie listy ssh\_blacklist i blokadą na 10dni



e) Ta reguła również utworzyła się domyślnie na końcu listy. Zaznacz regułę myszką i przeciągnij ją na samą górę.



f) Na koniec utworzymy regułę blokującą hosty z listy ssh\_black\_list. Utwórz kolejną regułę jak w pkt a tylko dodaj zależność dotyczącą listy tj. jeśli jest w liście ssh\_blacklist to wykonaj akcję drop.



g) Ta reguła również utworzyła się domyślnie na końcu listy. Zaznacz regułę myszką i przeciągnij ją na samą górę.

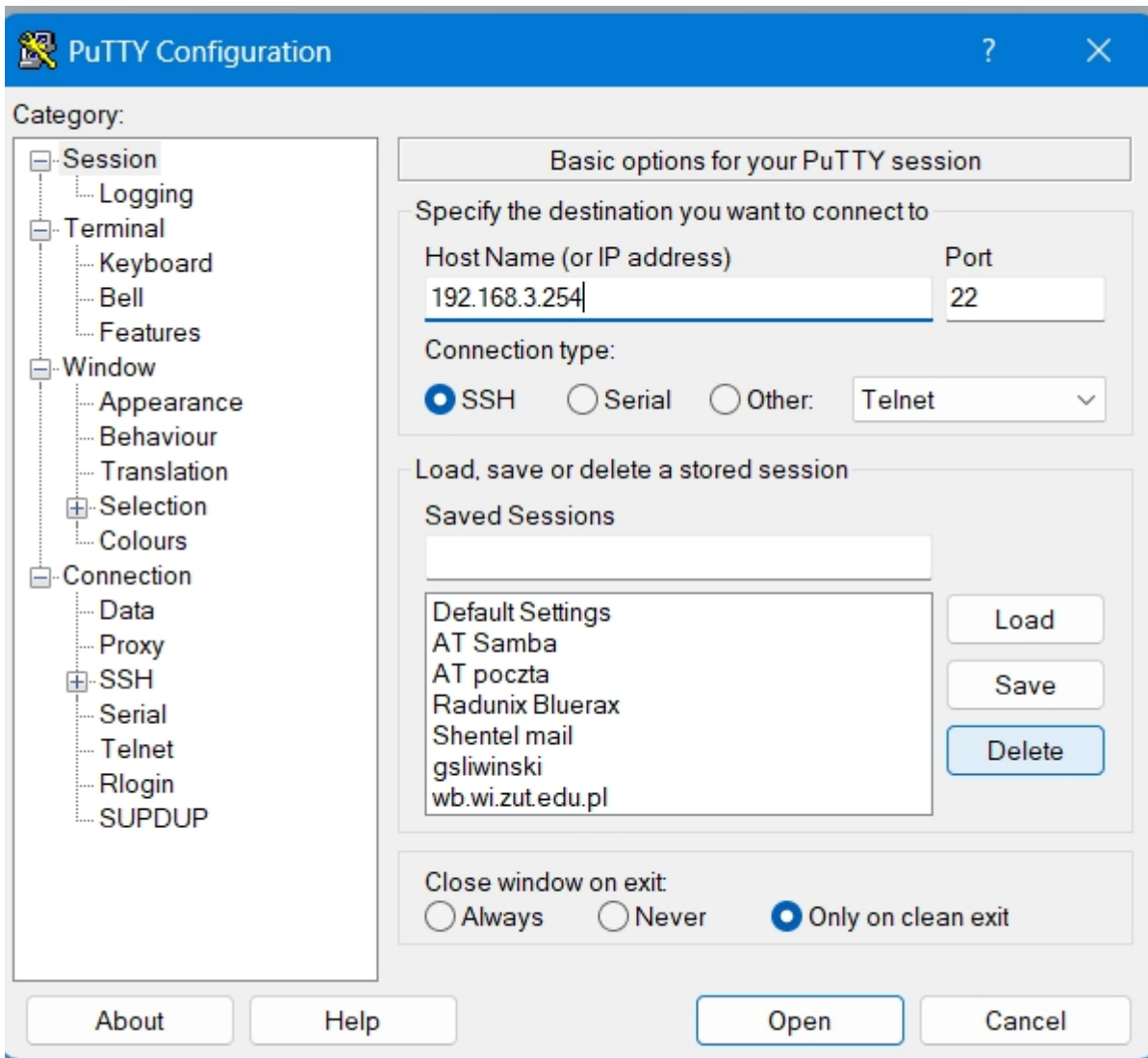
#	Action	Chain	Src. Address...	Dst. Address...	Src. Address...	Dst. A...	Protocol	Src. Port	Dst. Port	In. In...	Out. In...	In. Int...	Out. In...	Byte
0	drop	input			ssh_blacklist									
1	add src to address list	input			ssh_stage2		6 (tcp)		22					
2	add src to address list	input			ssh_stage1		6 (tcp)		22					
3	add src to address list	input					6 (tcp)		22					

## 16. Testujemy działanie list

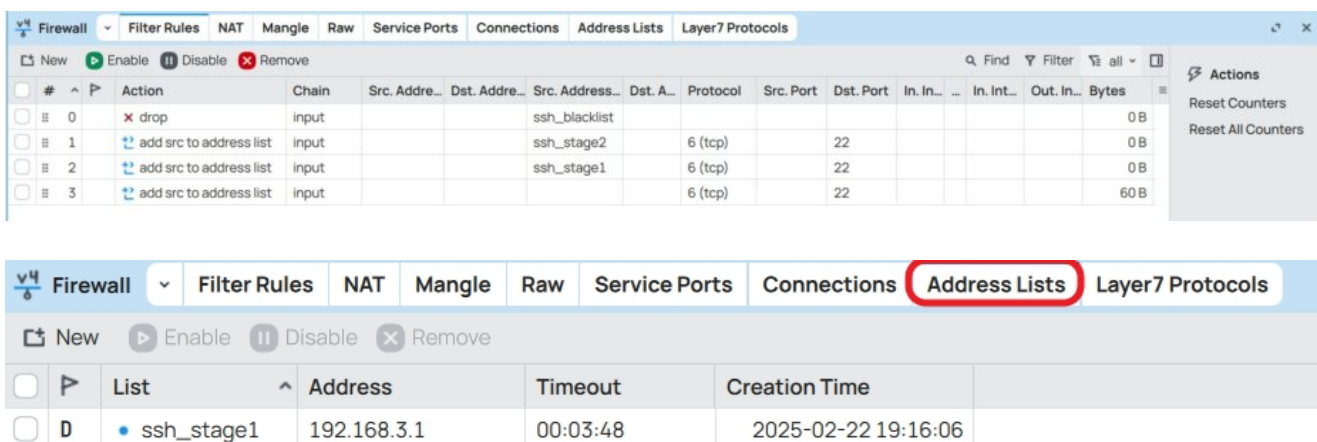
a) Na maszynie wirtualnej Win1 uruchom PUTTY (link do programu: <https://the.earth.li/~sgtatham/putty/latest/w64/putty.exe>)

b) Połącz się do swojego routera na jego adres IP, a następnie przerwij połączenie (nie loguj się) i obserwuj reguły firewall

	Address	Network	Interface
D	192.168.3.254/24	192.168.3.0	ether1
	10.10.100.1/24	10.10.100.0	bridge1



c) Zaobserwuj co się stało po pierwszym połączeniu



d) Wykonaj kolejne połączenie i obserwuj reguły

#	Action	Chain	Src. Address...	Dst. Address...	Src. Address...	Dst. A...	Protocol	Src. Port	Dst. Port	In. In...	In. Int...	Out. In...	Bytes
0	drop	input			ssh_blacklist								0 B
1	add src to address list	input			ssh_stage2		6 (tcp)		22				0 B
2	add src to address list	input			ssh_stage1		6 (tcp)		22				60 B
3	add src to address list	input					6 (tcp)		22				120 B

List	Address	Timeout	Creation Time
D • ssh_stage1	192.168.3.1	00:04:08	2025-02-22 19:16:06
D • ssh_stage2	192.168.3.1	00:09:08	2025-02-22 19:18:21

e) Wykonaj kolejne połączenie i obserwuj reguły

#	Action	Chain	Src. Address...	Dst. Address...	Src. Address...	Dst. A...	Protocol	Src. Port	Dst. Port	In. In...	In. Int...	Out. In...	Bytes
0	drop	input			ssh_blacklist								564 B
1	add src to address list	input			ssh_stage2		6 (tcp)		22				60 B
2	add src to address list	input			ssh_stage1		6 (tcp)		22				120 B
3	add src to address list	input					6 (tcp)		22				180 B

List	Address	Timeout	Creation Time
D • ssh_blacklist	192.168.3.1	9d 23:57:41	2025-02-22 19:20:08
D • ssh_stage1	192.168.3.1	00:02:41	2025-02-22 19:16:06
D • ssh_stage2	192.168.3.1	00:07:41	2025-02-22 19:18:21

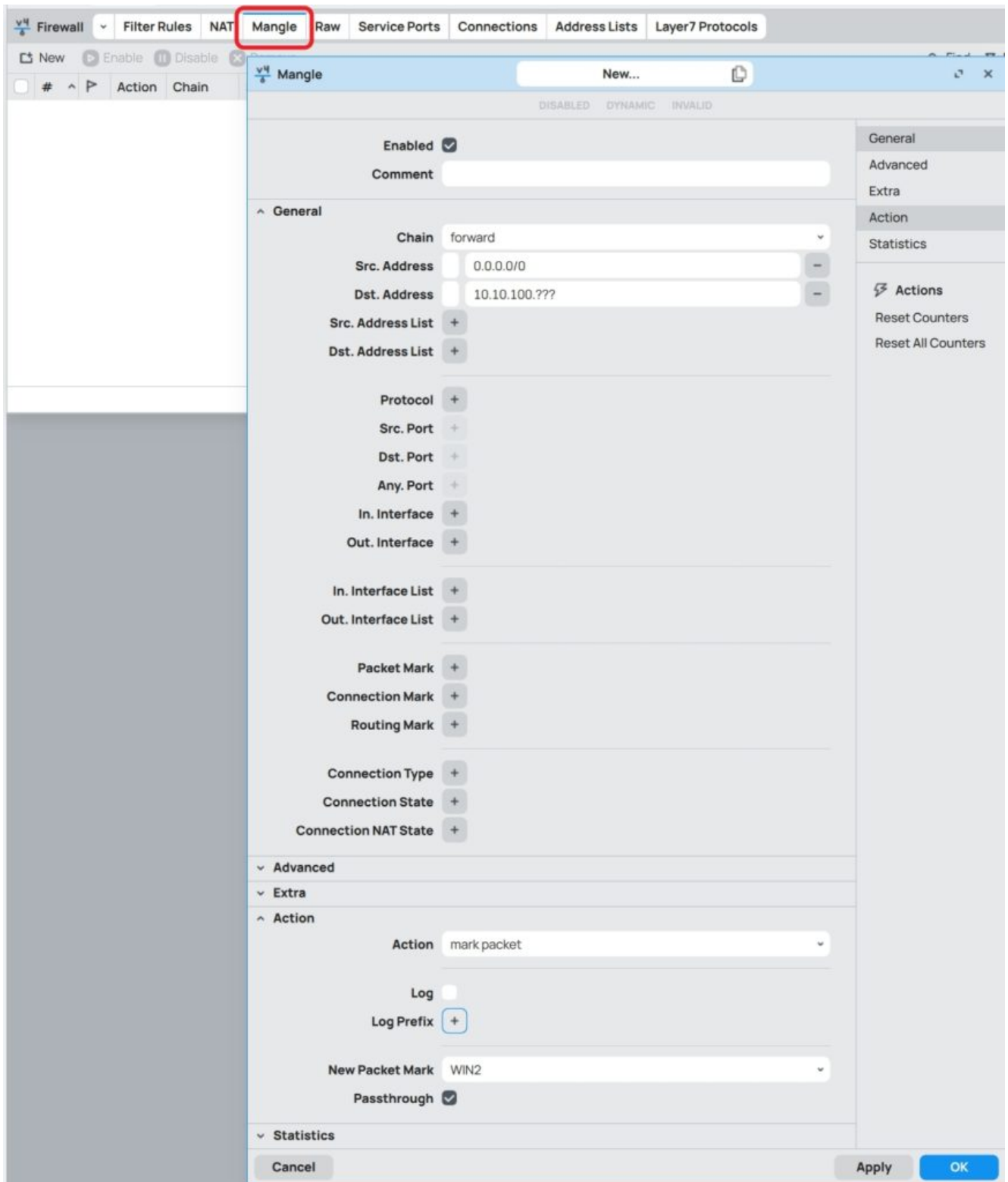
Zostałeś zablokowany na 10dni. Wszystkie kolejne próby połączenia do tego routera w tym okresie są odrzucane. Pamiętaj że przykładowe reguły działają na warstwie L3 modelu ISO/OSI, a ty jesteś połączony do routera poprzez adres MAC czyli na warstwie L2 modelu.

16a. **Zamknij otwarte okna PuTTY.** Przejdź do następnych punktów laboratorium.

### III. JAKOŚĆ POŁĄCZEŃ - oznaczanie pakietów i kolejkiwanie

Do oznaczania pakietów wykorzystamy Mangle (IP / Firewall / Mangle). Skorzystamy z maszyny wirtualnej win-02 i wprowadzimy ograniczenia transferu dla niej.

17. Utwórz nową regułę na łańcuchu „forward”, która będzie oznaczać pakiety przychodzące z Internetu do maszyny win-02. W tym celu za Internet przyjmujemy źródło jako adres sieci 0.0.0.0/0. Jako „Dst. Address” wskaż adres IP maszyny win-02. W zakładce „Action” nazwę oznaczenia pakietów „mark packet” ustawimy z ręki np. na wartość „WIN2”.



18. Podobną regułę tworzymy dla ruchu w drugim kierunku



Mangle New... [DISABLED] [DYNAMIC] [INVALID]

Enabled

Comment

**General**

Chain

Src. Address  -

Dst. Address  -

Src. Address List

Dst. Address List

Protocol

Src. Port

Dst. Port

Any. Port

In. Interface

Out. Interface

In. Interface List

Out. Interface List

Packet Mark

Connection Mark

Routing Mark

Connection Type

Connection State

Connection NAT State

**Action**

Action

Log

Log Prefix

New Packet Mark

Passthrough

**Statistics**

**Actions**

Reset Counters

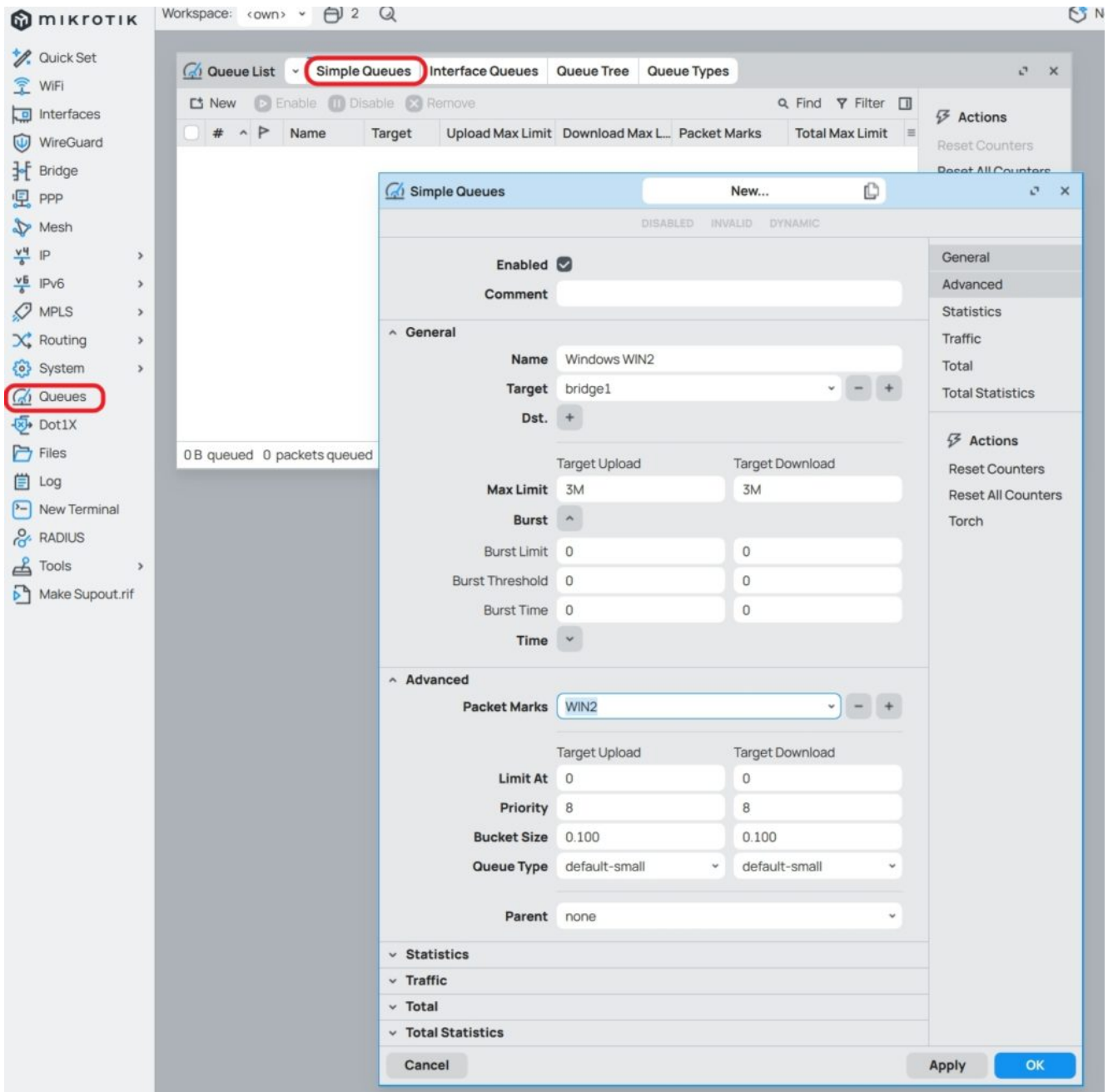
Reset All Counters

Cancel Apply OK

Firewall																	
Filter Rules																	
NAT																	
Mangle																	
Raw																	
Service Ports																	
Connections																	
Address Lists																	
Layer7 Protocols																	
New Enable Disable Remove Find Filter all																	
#	^	▶	Action	Chain	Src. Address	Dst. Address	Src. A...	Dst. A...	Prot...	Src. Port	Dst. Port	In. Int...	Out. In...	In. Int...	Out. In...	Bytes	Packet:≡
0			mark packet	forward	0.0.0.0/0	10.10.100...										0B	
1			mark packet	forward	10.10.100...	0.0.0.0/0										0B	

Reguły oznaczania są gotowe. Oznaczamy cały ruch w kierunku do klienta (czyli download z Internetu) oraz ruch od klienta do Internetu (czyli upload do Internetu). Przechodzimy do profilowania ruchu dla tych reguł.

19. Otwórz konfigurację Kolejek (Queues / Simple Queues). Dodaj nową regułę kolejki. Określ nazwę (dowolna, ale identyfikująca klienta), target (tu wskażemy interface na którym kolejka zostanie przypięta, w naszym przypadku bridge1) oraz limity dla pobierania i wysyłania (3M - M jako Mega). W zakładce „Advanced” ustawiamy „Packet Marks” na znacznik „WIN2” ustawiony w FireWall.



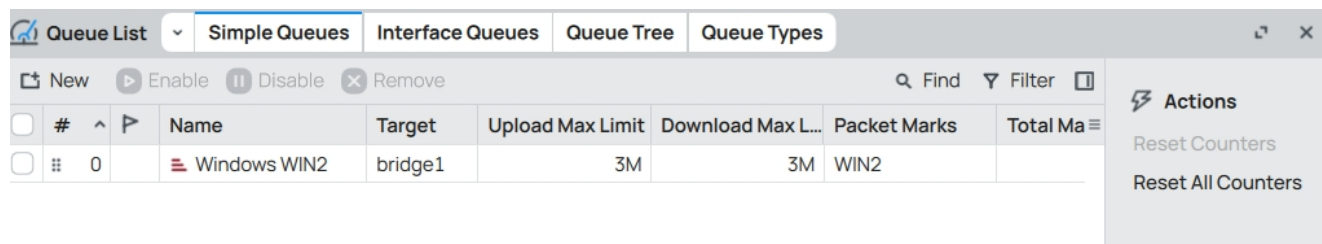
#	Name	Target	Upload Max Limit	Download Max L...	Packet Marks	Total Max Limit
0	Windows WIN2	bridge1	3M	3M	WIN2	

Kolejka ma status zielony (koło nazwy) co oznacza że transmisja nie przekracza limitów.

20. Przetestujemy ograniczenia. Na win-02 uruchom proces pobierania dużego pliku np. z podanego linku:

<https://gslivinski.wi.zut.edu.pl/vm/ubuntu-24.04.1-live-server-amd64.iso> i

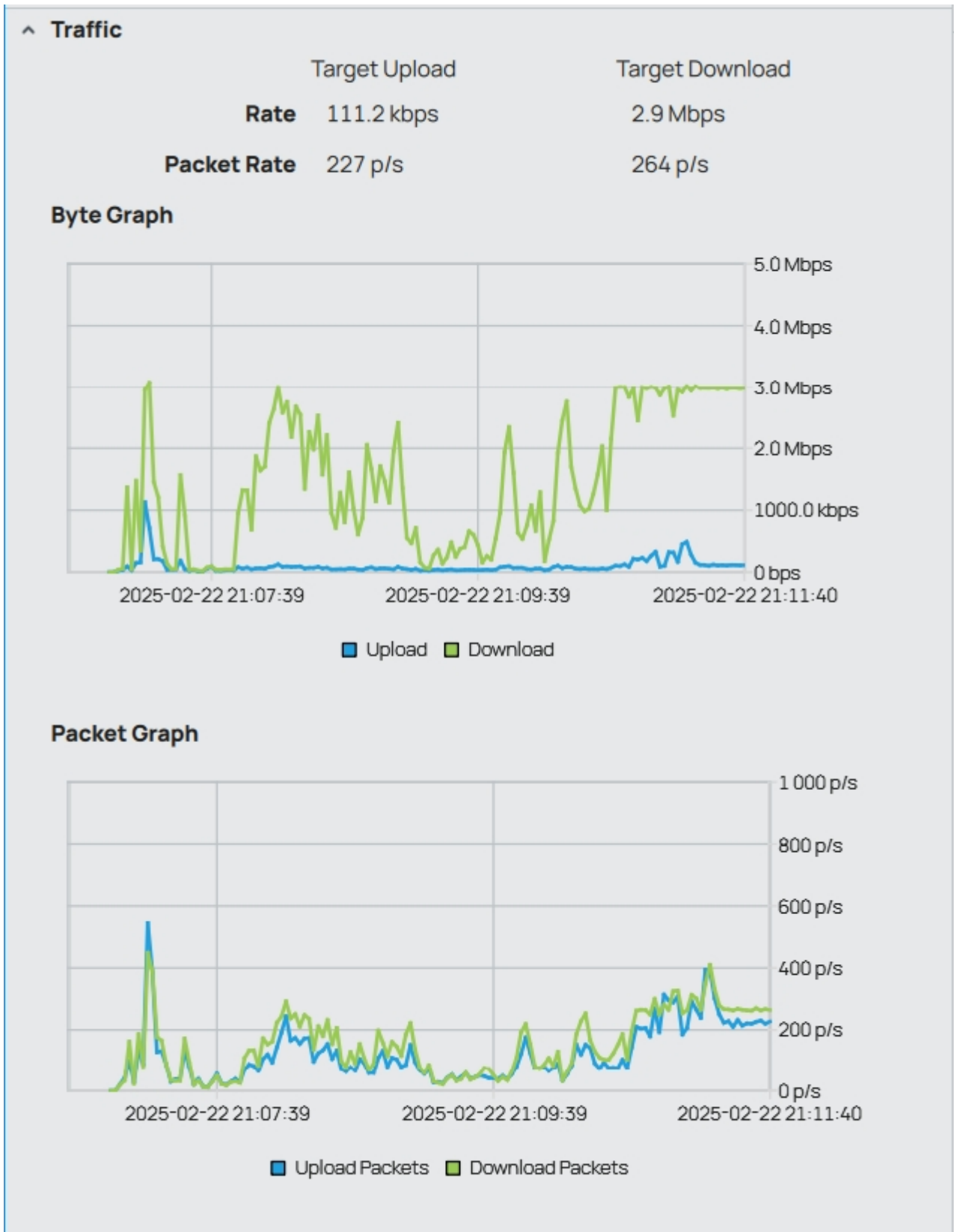
obserwuj działanie kolejki.



The screenshot shows the Mikrotik WinBox Queue List interface. The 'Simple Queues' tab is active. A table lists a queue named 'Windows WIN2' with a target of 'bridge1' and upload/download limits of 3M. The 'Packet Marks' column shows 'WIN2'. An 'Actions' menu is open on the right, showing 'Reset Counters' and 'Reset All Counters' options.

#	Name	Target	Upload Max Limit	Download Max L...	Packet Marks	Total Ma
0	Windows WIN2	bridge1	3M	3M	WIN2	

Jest czerwono czyli przekraczamy dozwolony limit. W zakładce Traffic możemy zobaczyć co się dzieje



21. Przejdź na zakładkę General. Zwiększ limit Download na 5M, kliknij Apply i przejdź ponownie na zakładkę Traffic

Enabled

Comment

General

Name

Target  - +

Dst. +

Max Limit Target Upload 3M Target Download 5M

Burst ^

Burst Limit 0 0

Burst Threshold 0 0

Burst Time 0 0

Time v

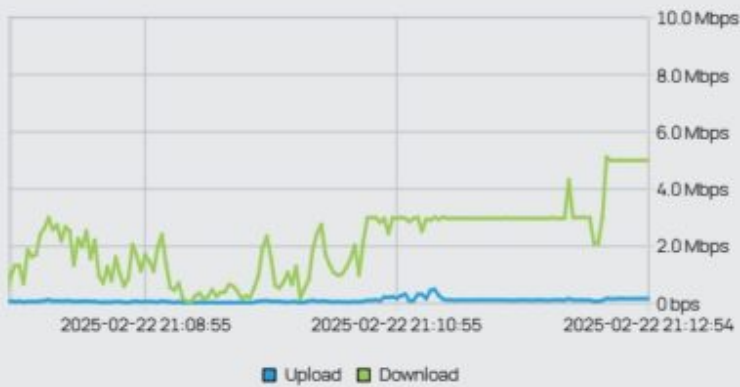
Advanced

Statistics

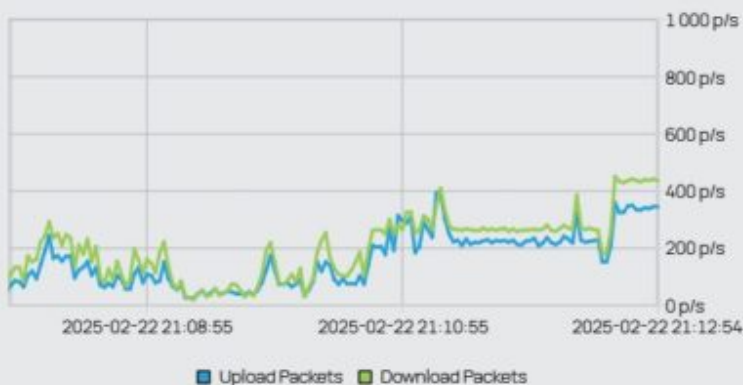
Traffic

	Target Upload	Target Download
Rate	166.8 kbps	4.9 Mbps
Packet Rate	345 p/s	437 p/s

Byte Graph

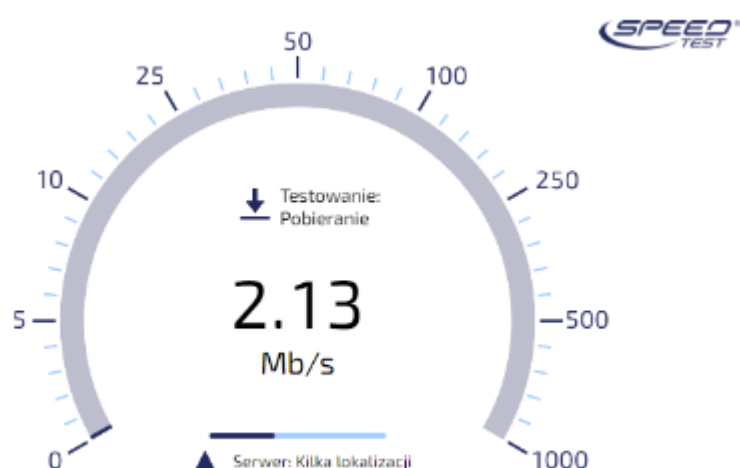


Packet Graph



Zmieniła się szybkość transferu

22. Otwórz w drugiej zakładce (nie przerywając wcześniejszego transferu) stronę <https://speedtest.pl/> i wykonaj test. Zastanawiające jest czemu pokazuje przy download tylko kilka Mega a nie cała dozwolone 5M. Wynika to z współdzielenia kolejki. Cała kolejka ma 5M niezależnie ile transferów jest uruchomionych.



23. Zatrzymaj pobieranie w pierwszej zakładce pliku ISO.

24. Zmień ustawienia kolejki. Wykorzystamy funkcjonalność „Burst” czyli formę nagrody dla klienta. Ustawimy taką politykę. Jeżeli klient w ciągu 90s nie przekroczy szybkości 5M to w nagrodę dostanie 10M

^ **General**

**Name** Windows WIN2

**Target** bridge1 ▼ - +

**Dst.** +

---

	Target Upload	Target Download
<b>Max Limit</b>	3M	5M
<b>Burst</b>	<span>^</span>	
Burst Limit	10M	10M
Burst Threshold	3M	5M
Burst Time	90	90
<b>Time</b>	<span>▼</span>	

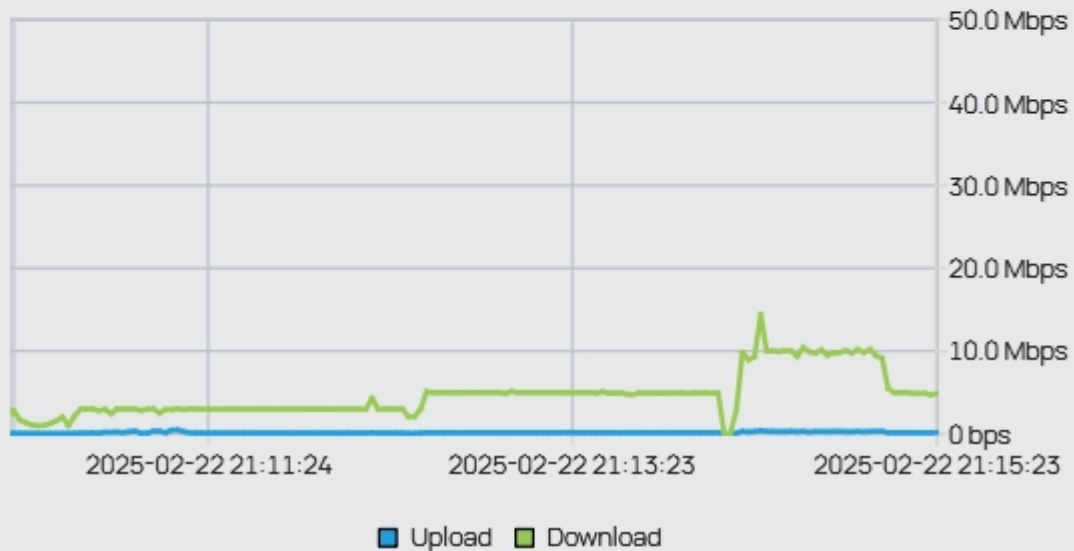
Kliknij Apply i przejdź na zakładkę Traffic - obserwuj transfer



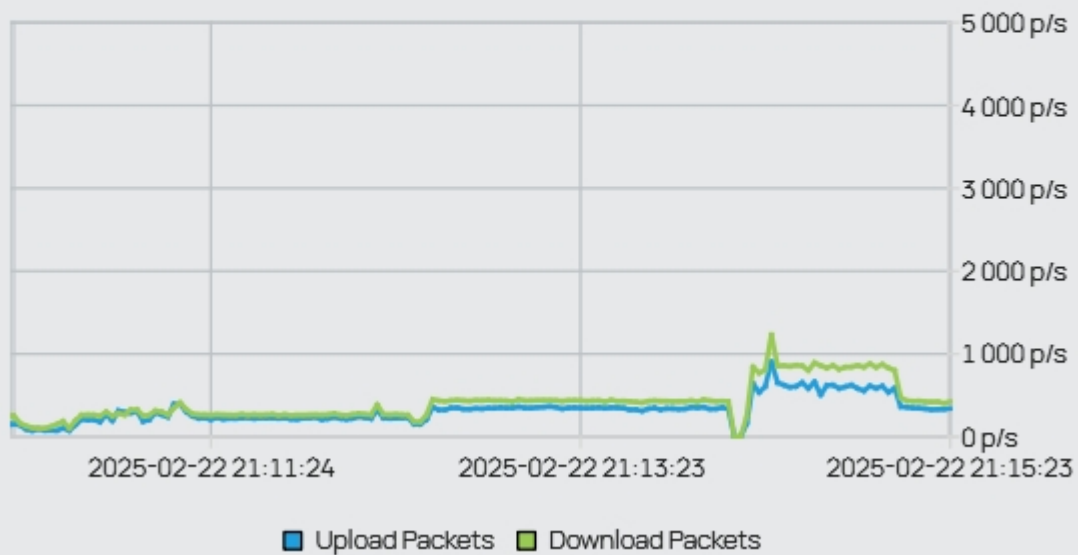
## ^ Traffic

	Target Upload	Target Download
<b>Rate</b>	159.9 kbps	4.8 Mbps
<b>Packet Rate</b>	342 p/s	423 p/s

### Byte Graph



### Packet Graph



25. Zmień limit (próg) „Burst Threshold” dla Download na 6M – obserwuj Traffic

^ General

**Name** Windows WIN2

**Target** bridge1 ▼ - +

**Dst.** +

Target Upload

Target Download

**Max Limit** 3M

5M

**Burst** ^

Burst Limit 10M

10M

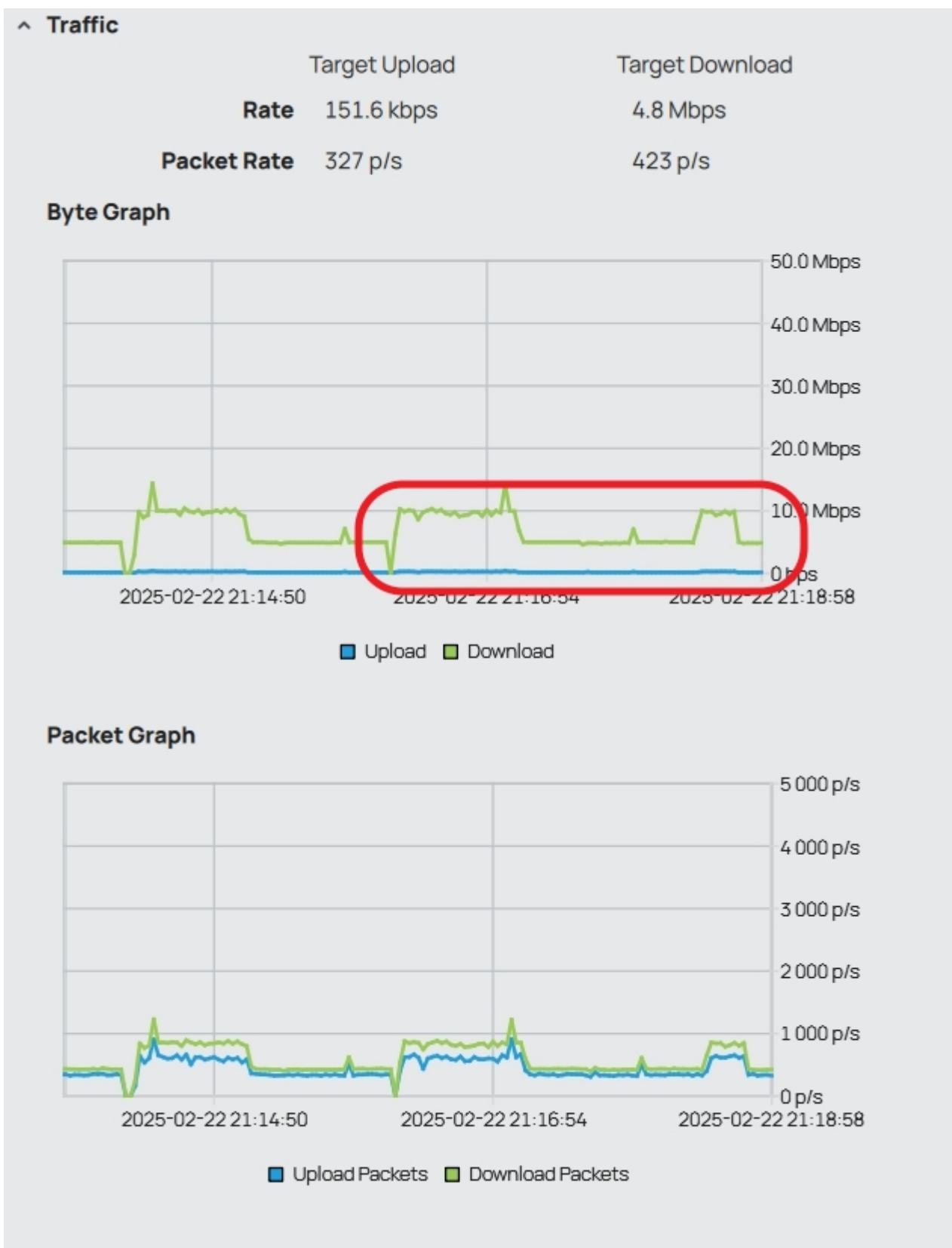
Burst Threshold 3M

6M

Burst Time 90

90

**Time** ▼



Powinno zachować się jak na rysunku powyżej. Klienta na początku nie przekraczał 6M więc dostał w nagrodę 10M na 90s, potem prędkość spadła do jego limitu 5M czyli poniżej progu. System monitorował ruch i stwierdził że klienta przez kolejne 90s nie przekroczył progu 6M dlatego dostał ponownie w

nagrodę 10M.