

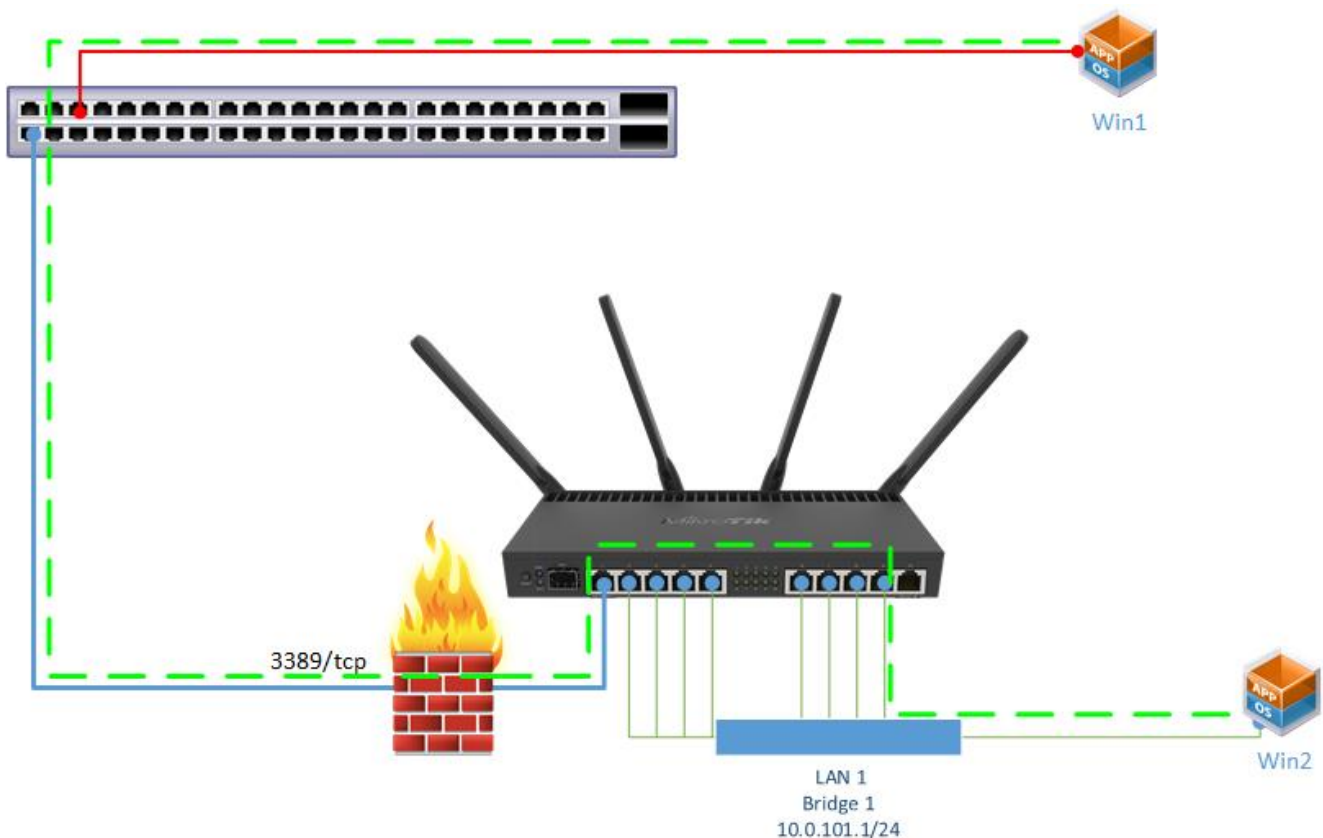
Mikrotik – FireWall i kształtowanie ruchu

written by archi | 26 listopada 2022

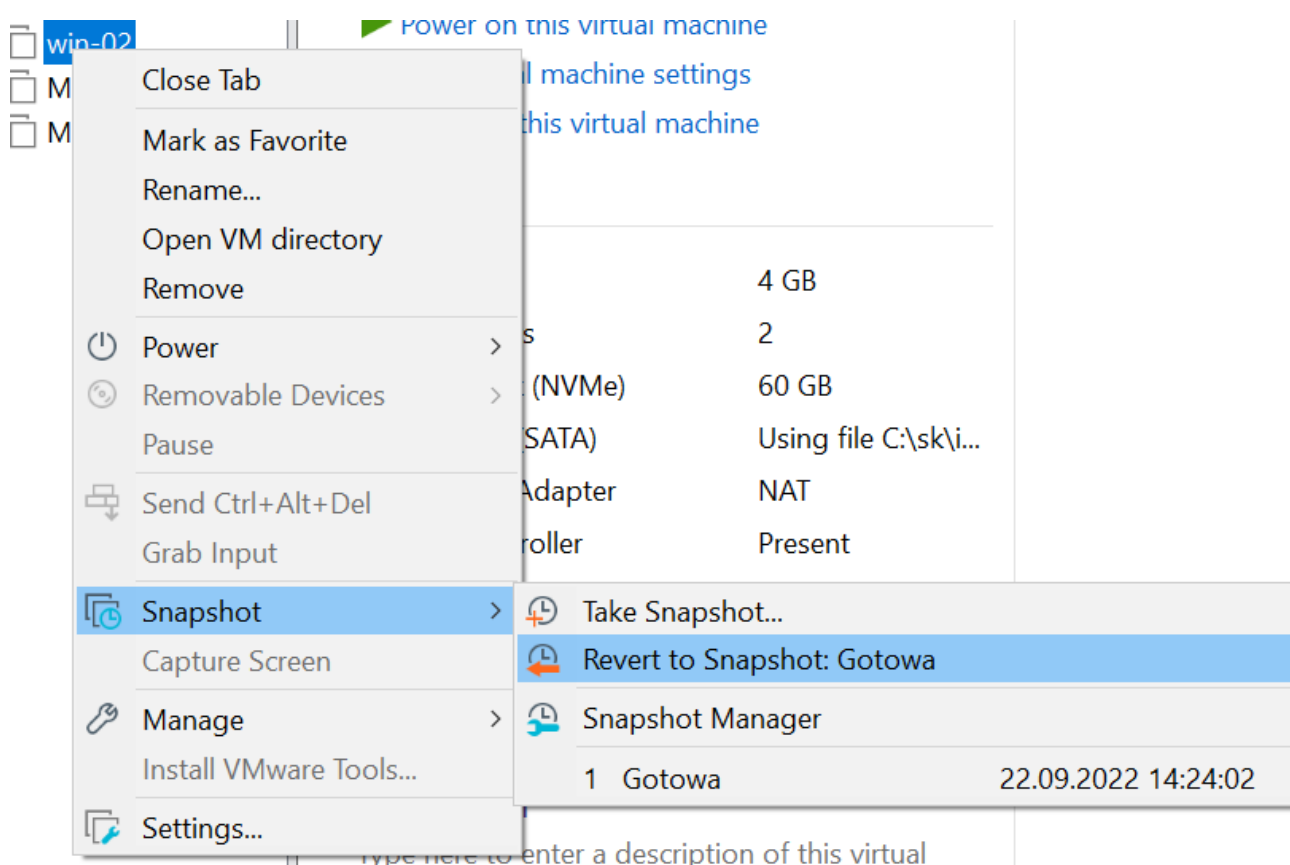
Mikrotik – FireWall i kształtowanie ruchu

I. TUNELOWANIE

Celem laboratorium 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 Remote Desktop Services (RDS, port 3389/tcp) do maszyny Win2 (sieć lokalna) z maszyny Win1 będącej poza siecią lokalną (z łącza zewnętrznego).

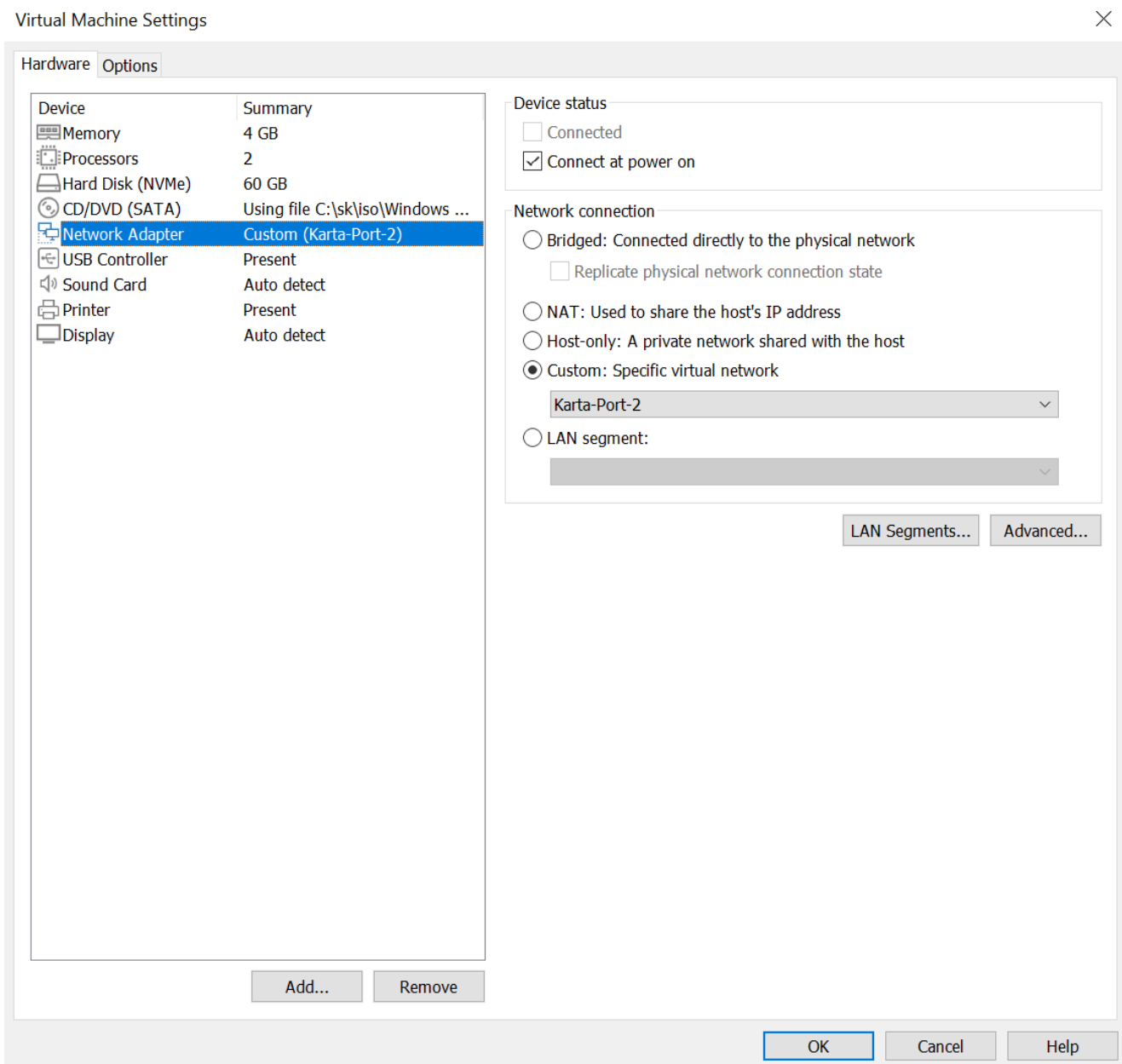


1. Podłącz komputer (krosownica port1) do twojego prywatnego switch a następnie kolejny port switcha do routera R1 na porcie Ether2 (wykonaj reset do konfiguracji domyślnej)
2. Podłącz **port 2** komputera (krosownica) do **przełącznika sieciowego (48-portów)** w wolny port.
3. Podłącz **port 3** komputera (krosownica) do portu **Ether3** w routerze.
4. Podłącz router R1 (port **Ether1**) do Internetu.
5. Uruchom VMware Workstation. Przywróć migawkę dla obu maszyn win-01 i win-02, aby miały ustawienia domyślne



6. Zmień ustawienia maszyn wirtualnych, tak aby
 - maszyna win-01 była podłączona do Karta-Port2,
 - maszyna win-02 była podłączona do Karta-Port3.

Włącz obydwie maszyny.



7. Przejdź do routera R1 i wykonaj następujące czynności:

- Ustaw DHCP-Client na porcie Ether1
- Dodaj interfejs Bridge i przypisz do niego port Ether3
- Nadaj adres IP dla bridge1 10.10.100.1/24
- Skonfiguruj serwer DHCP na interfejsie bridge1

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

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.

New NAT Rule



General **Advanced** Extra Action Statistics

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: ▾

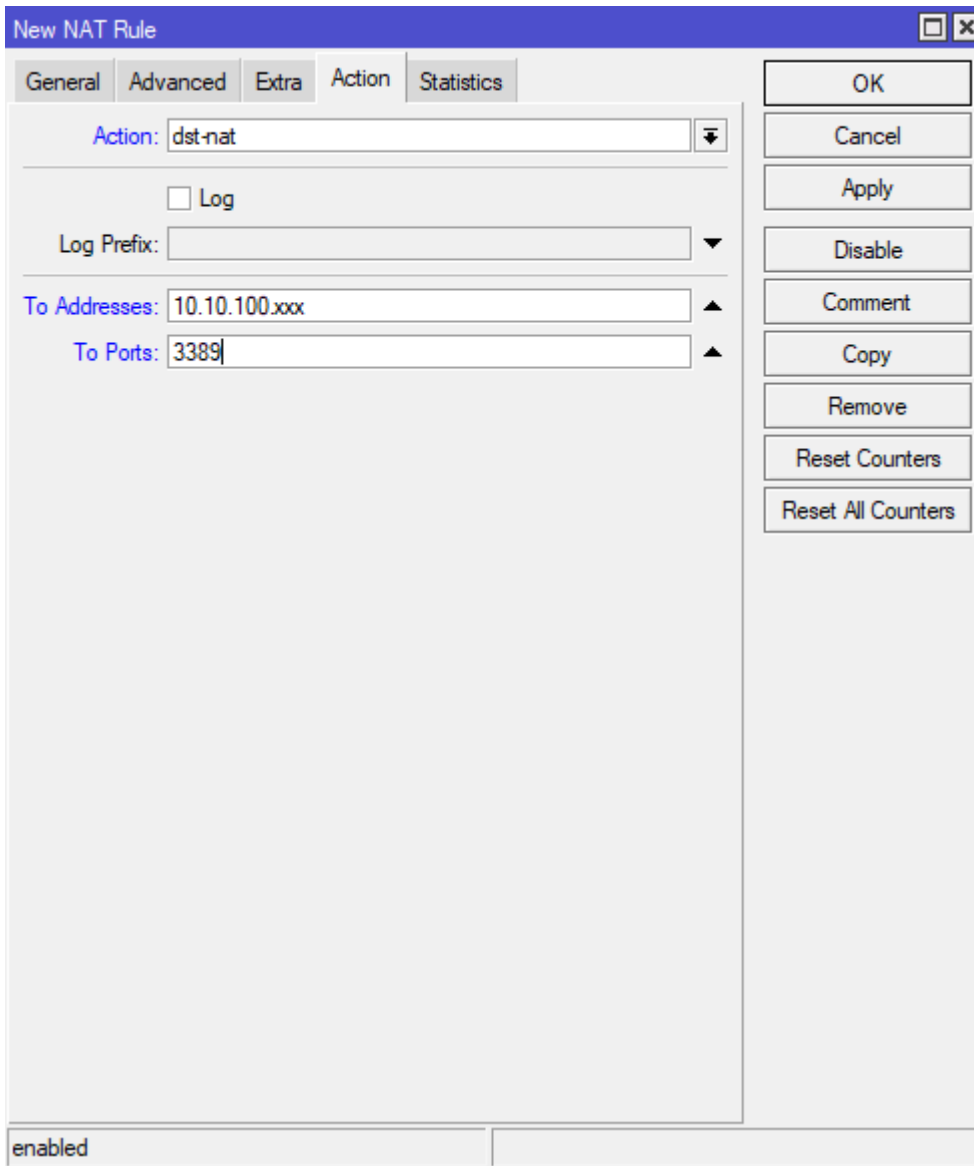
Connection Mark: ▾

Routing Mark: ▾

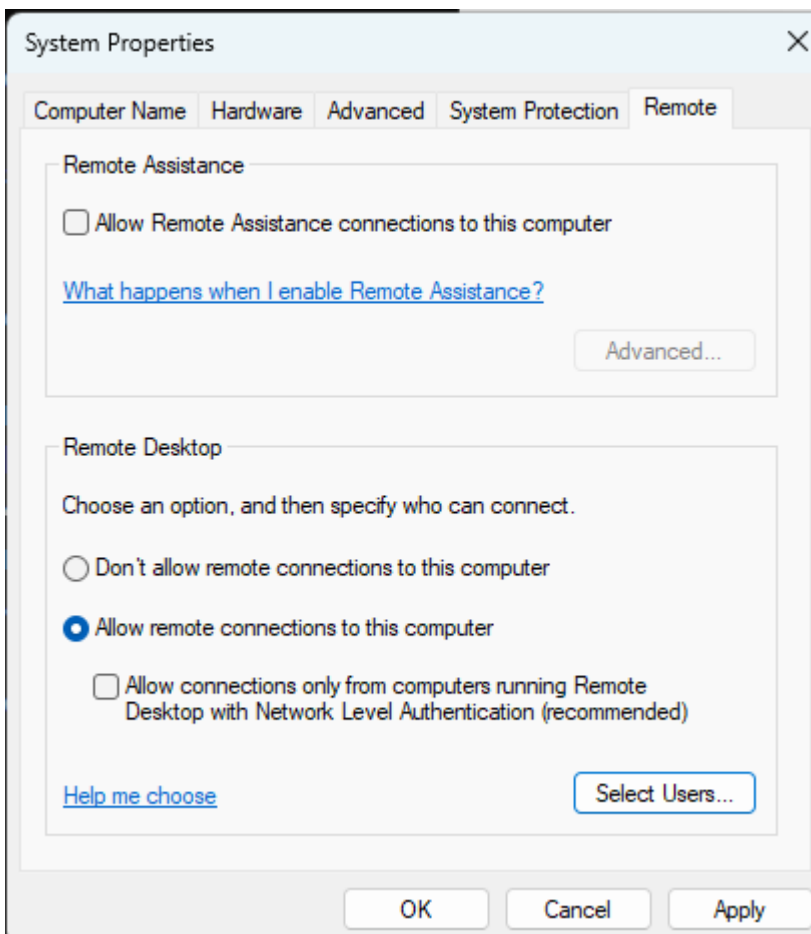
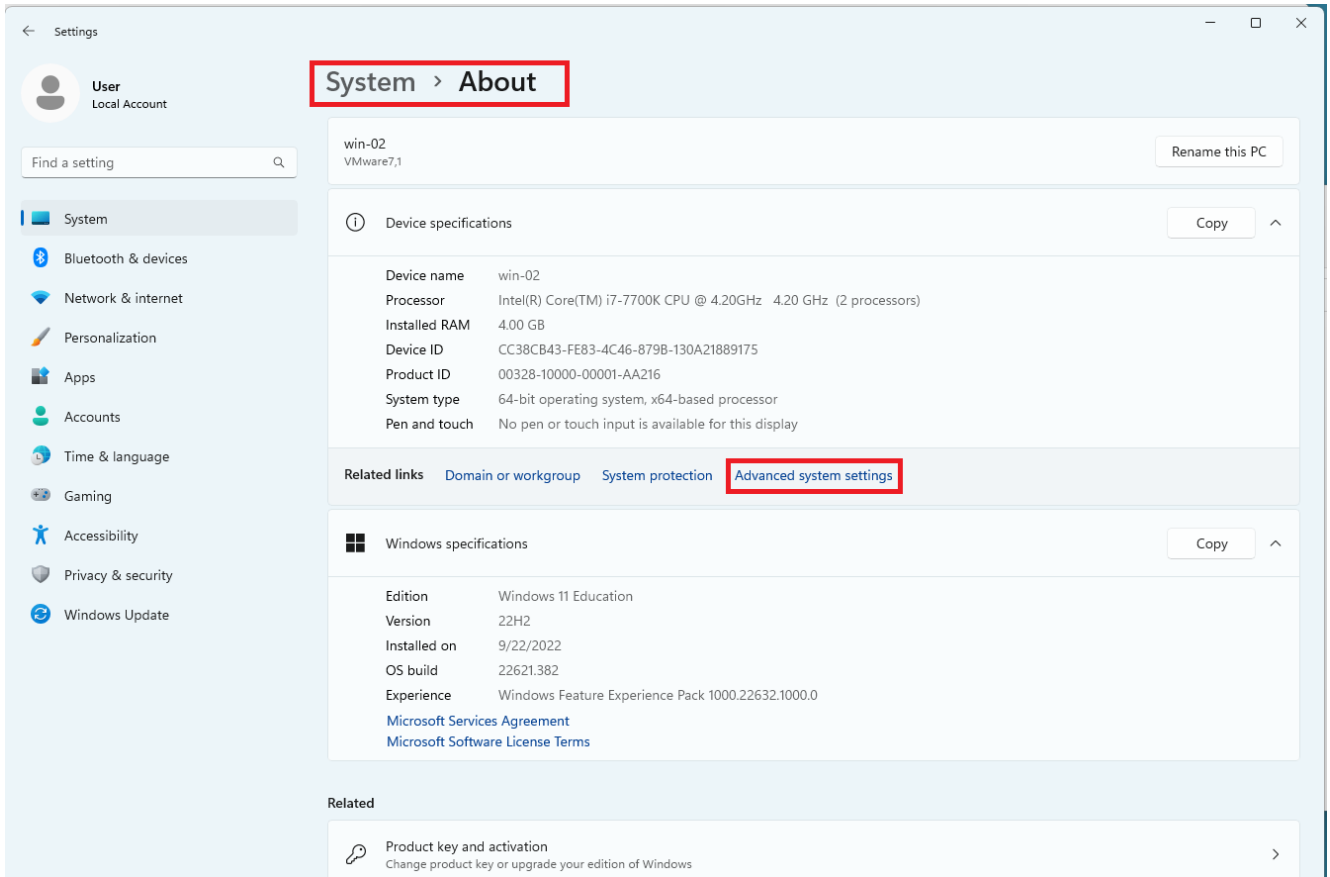
Connection Type: ▾

- OK
- Cancel
- Apply
- Disable
- Comment
- Copy
- Remove
- Reset Counters
- Reset All Counters

enabled



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



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>_
```

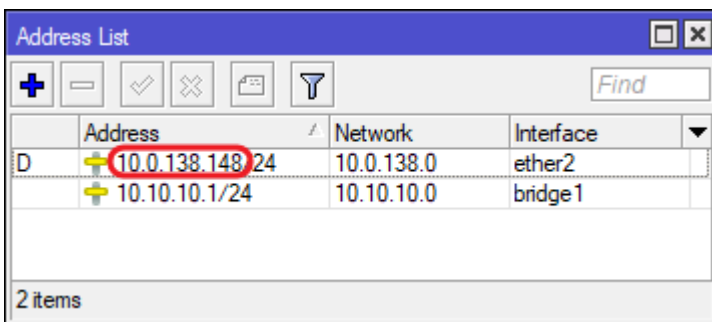
```
net localgroup administrators user1 /add
```

```
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



	Address	Network	Interface
D	10.0.138.148/24	10.0.138.0	ether2
	10.10.10.1/24	10.10.10.0	bridge1


2 items

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

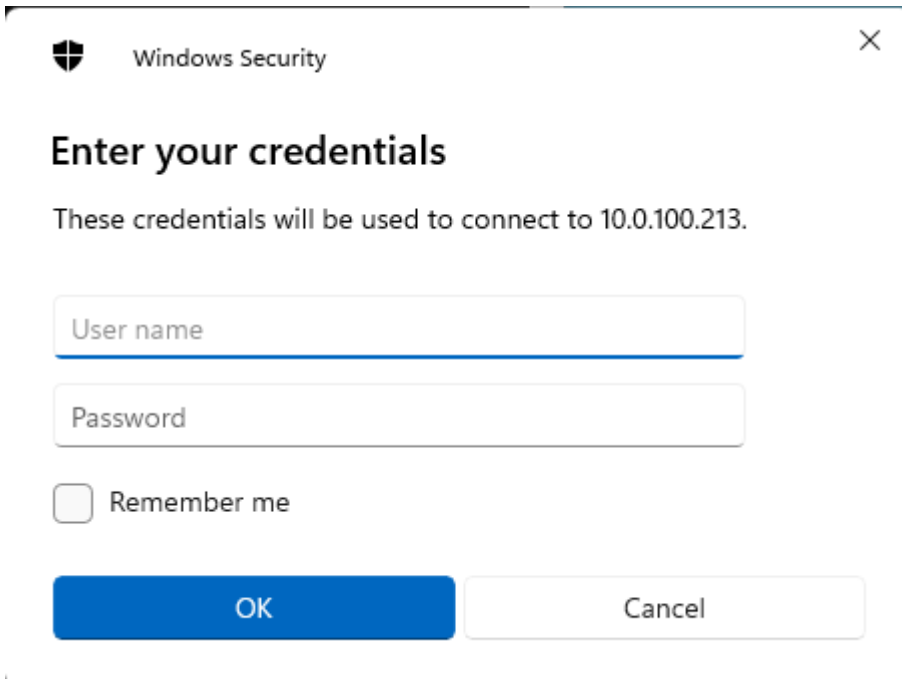
 **Podłączanie pulpitu zdalnego**

Komputer:

Nazwa użytkownika: Nie określono

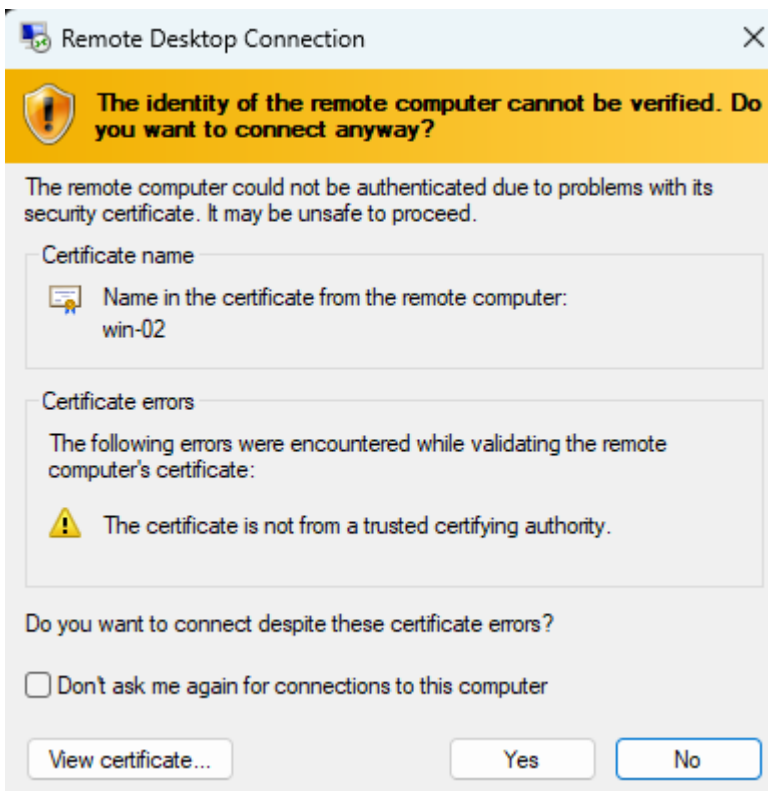
Podczas łączenia zostanie wyświetlony monit o podanie poświadczeń.

 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

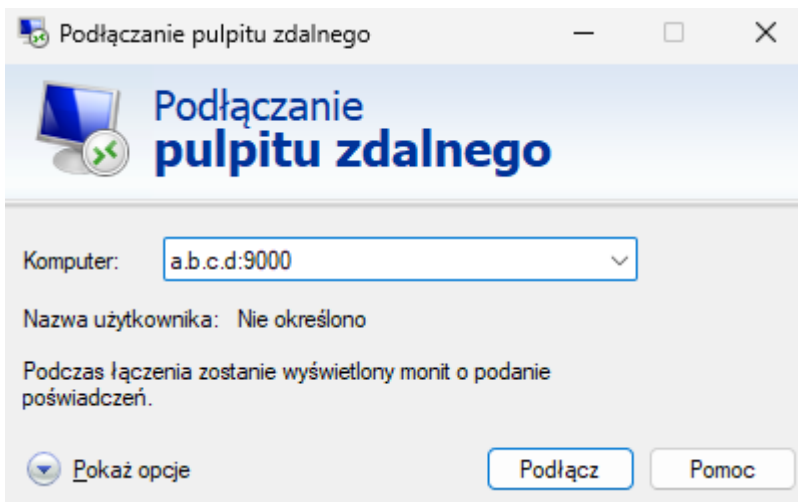
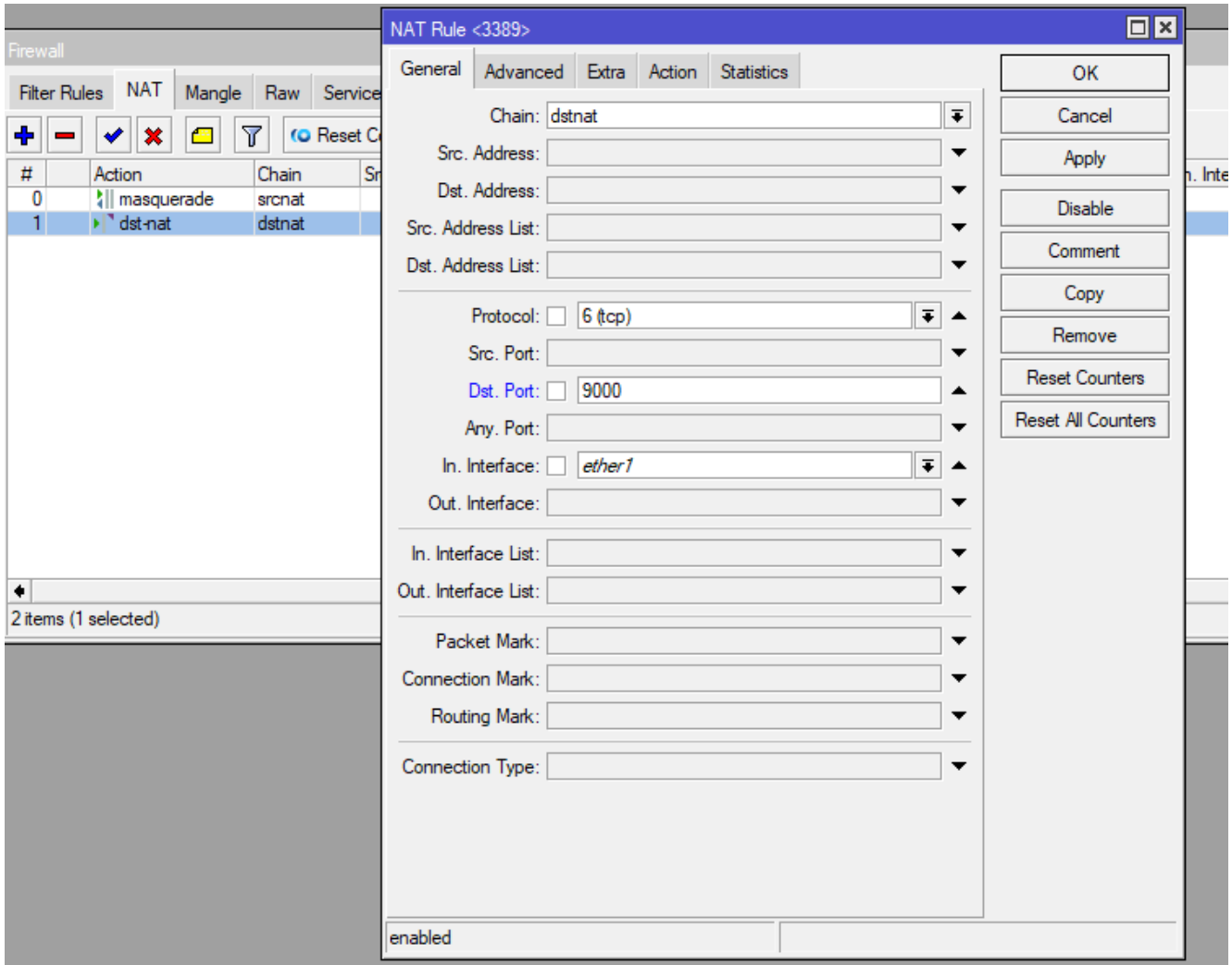
You won't be able to get location-based experiences like directions and weather or enjoy other services that require your location to work.

[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



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

II. WYKORZYSTANIE LIST - Honeypot

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.

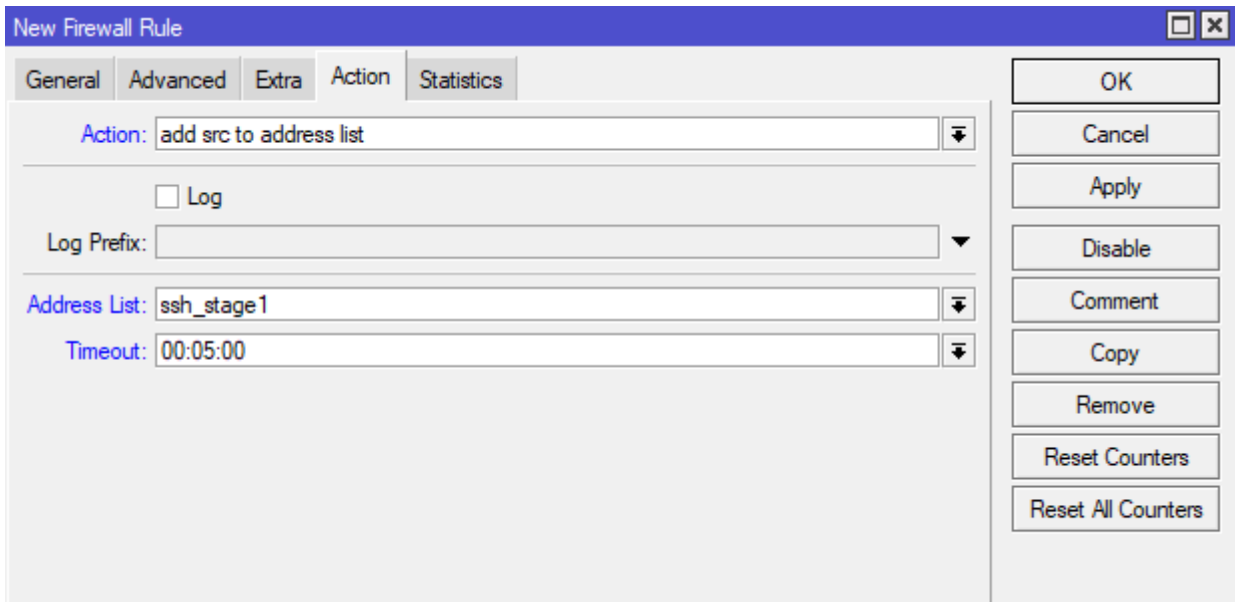
a) Utwórz regułę na łańcuchu „input”, protokół TCP, port docelowy „22”, stan połączenia „Connection State” nowy „new” z akcją „add src to address list”, do listy np. „ssh_stage1” w polu „Address List” (trzeba wpisać z ręki) i czasem przebywania w liście 5min „Timeout” 00:05:00

The screenshot shows the 'New Firewall Rule' dialog box with the following configuration:

- Chain:** input
- Src. Address:** (empty)
- Dst. Address:** (empty)
- Src. Address List:** (empty)
- Dst. Address List:** (empty)
- Protocol:** 6 (tcp)
- Src. Port:** (empty)
- Dst. Port:** 22
- Any. Port:** (empty)
- In. Interface:** (empty)
- Out. Interface:** (empty)
- In. Interface List:** (empty)
- Out. Interface List:** (empty)
- Packet Mark:** (empty)
- Connection Mark:** (empty)
- Routing Mark:** (empty)
- Connection Type:** (empty)
- Connection State:** new
- Connection NAT State:** (empty)

Buttons on the right: OK, Cancel, Apply, Disable, Comment, Copy, Remove, Reset Counters, Reset All Counters.

At the bottom left, the rule is marked as **enabled**.



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 przebywania 10min.

New Firewall Rule



- General
- Advanced
- Extra
- Action
- Statistics

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: invalid established related new untracked

Connection NAT State:

OK

Cancel

Apply

Disable

Comment

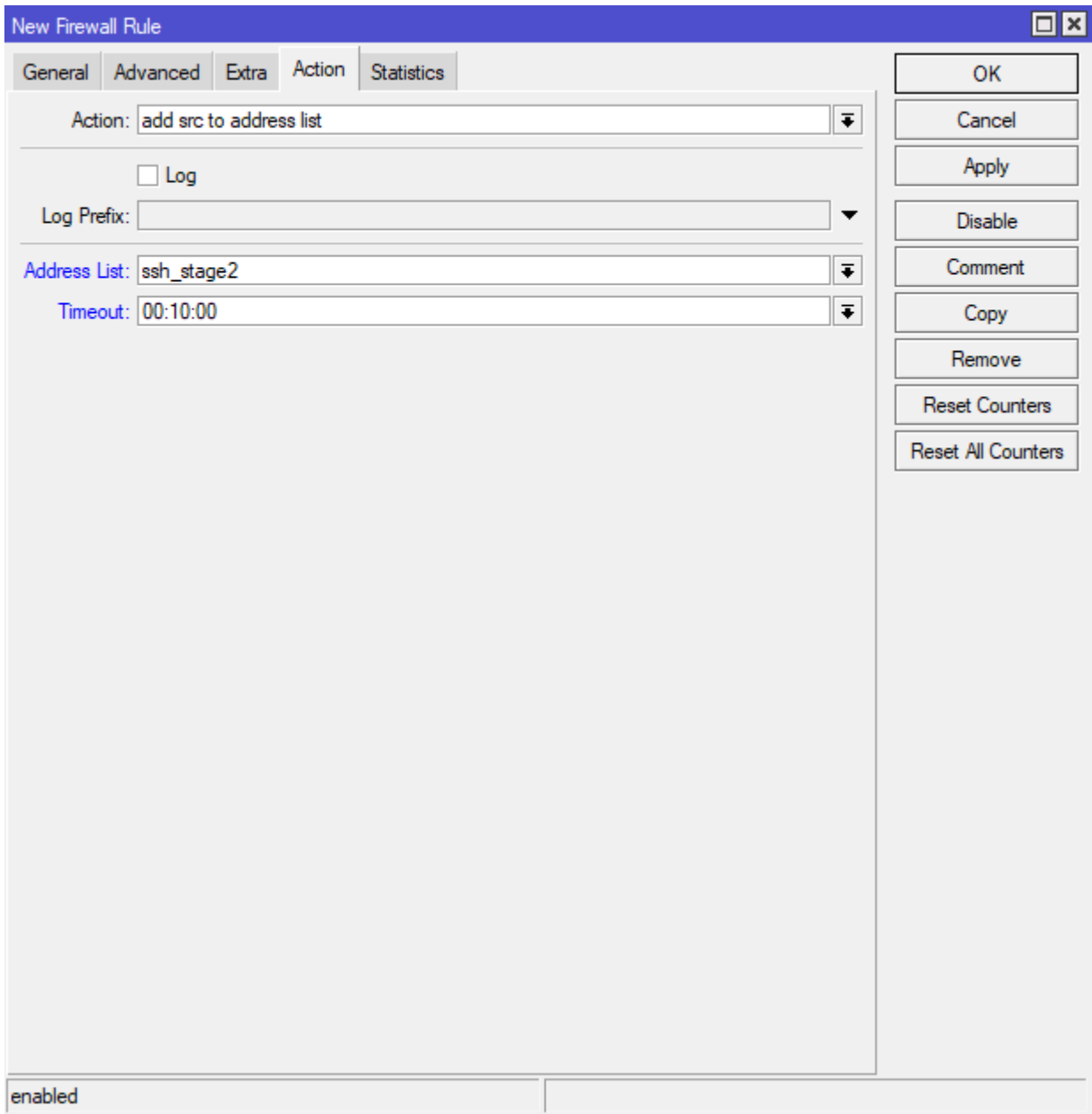
Copy

Remove

Reset Counters

Reset All Counters

enabled



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

#	Action	Chain	Src. Address	Dst. Address	Src. Address L...	Dst. Ad...	Proto...	Src. Port	Dst. Port	In. Inter... C
0	+ add src to address list	input					6 (tcp)		22	
1	+ add src to address list	input			ssh_stage1		6 (tcp)		22	

Firewall												
Filter Rules												
NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols												
<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> Reset Counters <input type="checkbox"/> Reset All Counters												
#	Action	Chain	Src. Address	Dst. Address	Src. Address L...	Dst. Ad...	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	In. Inter...
0	add src to address list	input			ssh_stage 1		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

New Firewall Rule
□ ×

General
Advanced
Extra
Action
Statistics

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:
 invalid
 established
 related
 new
 untracked

Connection NAT State:

OK

Cancel

Apply

Disable

Comment

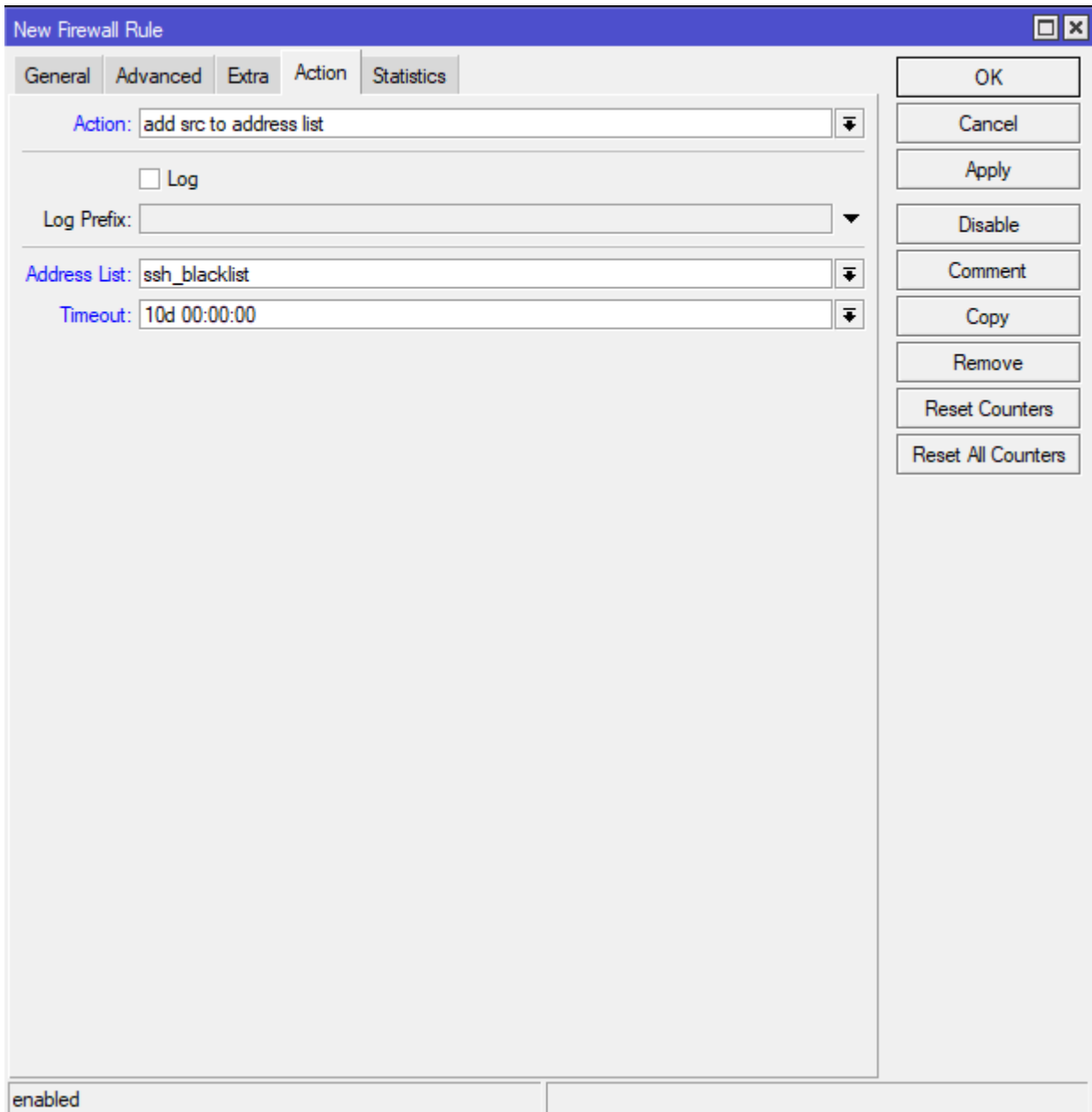
Copy

Remove

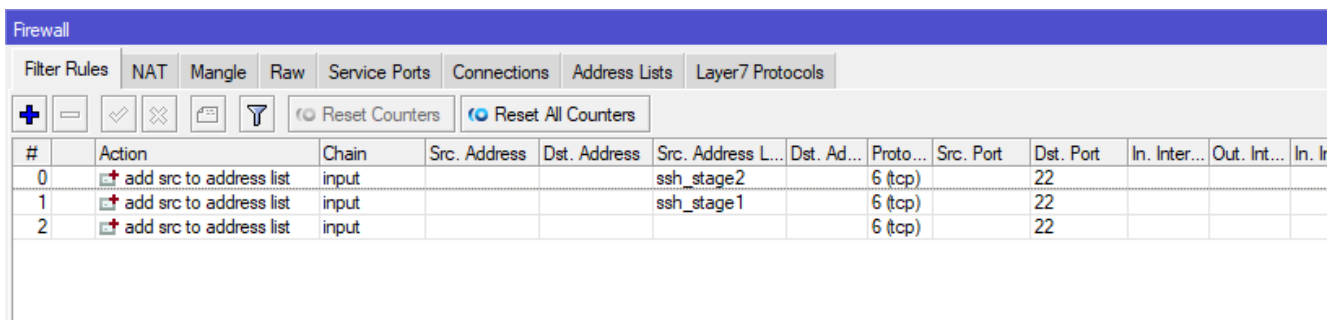
Reset Counters

Reset All Counters

enabled



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.

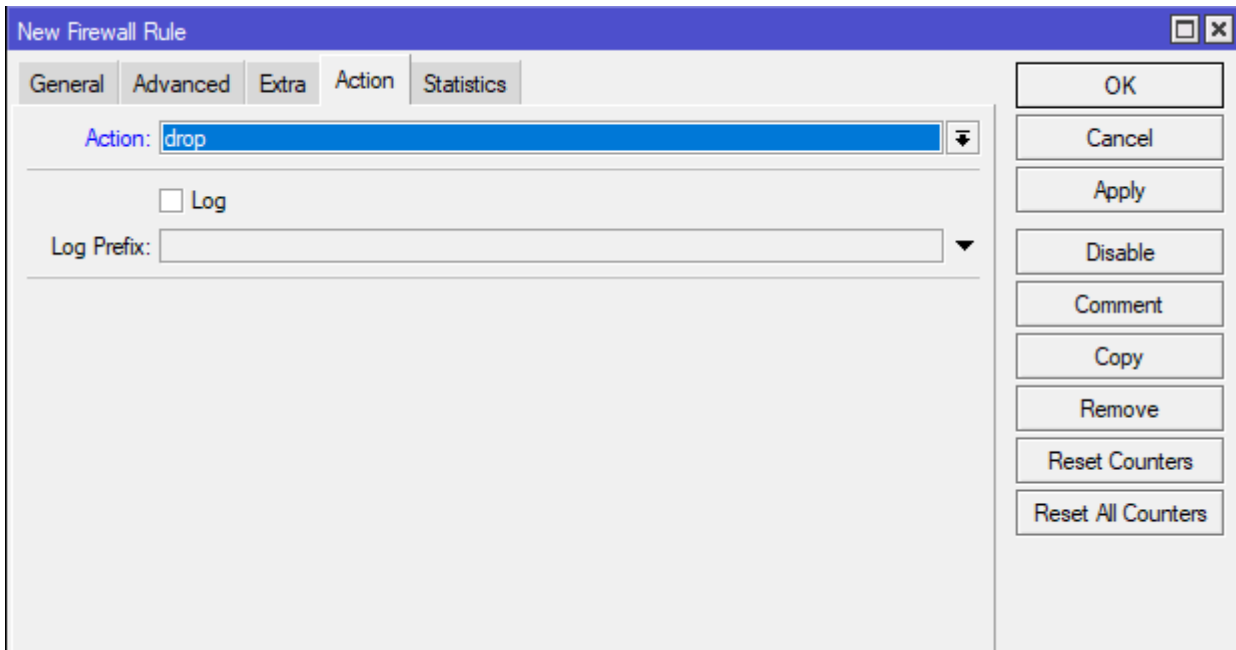
The image shows a 'New Firewall Rule' dialog box with the following fields and settings:

- Chain:** input
- Src. Address:** (empty)
- Dst. Address:** (empty)
- Src. Address List:** ssh_blacklist
- Dst. Address List:** (empty)
- Protocol:** (empty)
- Src. Port:** (empty)
- Dst. Port:** (empty)
- Any. Port:** (empty)
- In. Interface:** (empty)
- Out. Interface:** (empty)
- In. Interface List:** (empty)
- Out. Interface List:** (empty)
- Packet Mark:** (empty)
- Connection Mark:** (empty)
- Routing Mark:** (empty)
- Connection Type:** (empty)
- Connection State:** (empty)
- Connection NAT State:** (empty)

Buttons on the right side of the dialog:

- OK
- Cancel
- Apply
- Disable
- Comment
- Copy
- Remove
- Reset Counters
- Reset All Counters

At the bottom left, there is a checkbox labeled 'enabled' which is checked.



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 L...	Dst. Ad...	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int.
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

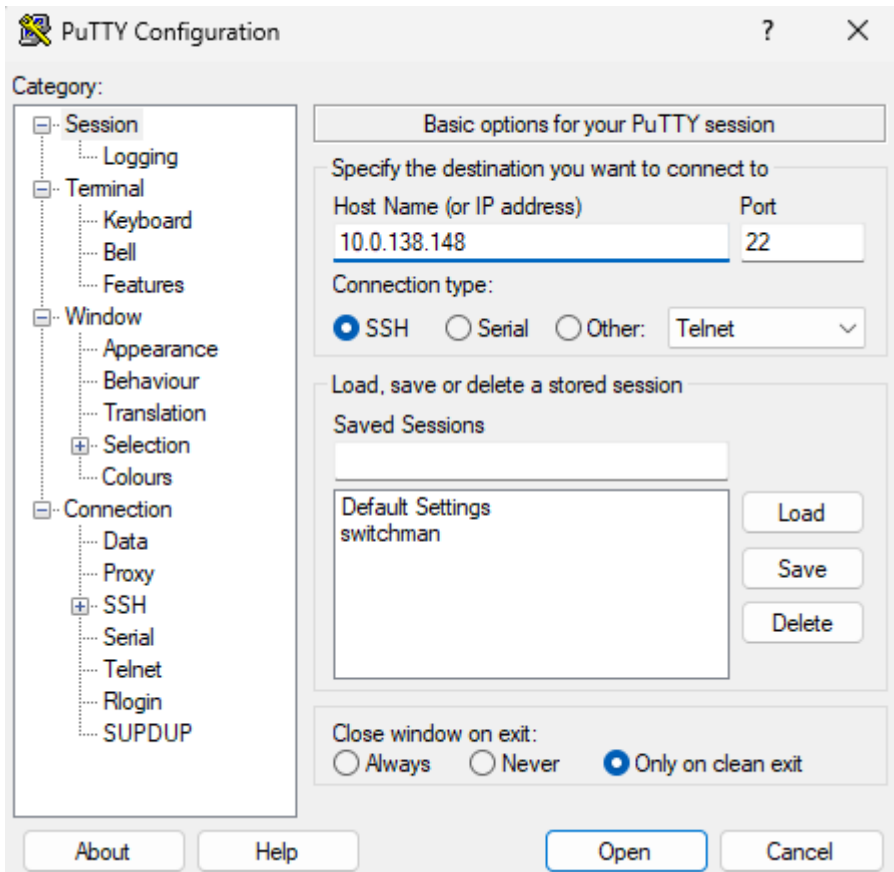
a) Na maszynie wirtualnej Win1 uruchom PUTTY (link do programu:

<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	10.0.138.148/24	10.0.138.0	ether2
	10.10.10.1/24	10.10.10.0	bridge1

2 items



c) Zaobserwuj co się stało po pierwszym połączeniu

#	Action	Chain	Src. Address	Dst. Address	Src. Address L...	Dst. Ad...	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	In. Inter...	Out. Int...	Bytes	Pa
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						0 B	
3	add src to address list	input					6 (tcp)	22						52 B	

List	Address	Timeout	Creation Time
D ssh_stage1	10.0.138.29	00:03:43	Dec/04/2024 09:57:55

d) Wykonaj kolejne połączenie i obserwuj reguły

#	Action	Chain	Src. Address	Dst. Address	Src. Address L...	Dst. Ad...	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	In. Inter...	Out. Int...	Bytes	Pa
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						52 B	
3	add src to address list	input					6 (tcp)	22						104 B	

Firewall				
Filter Rules				
List	Address	Timeout	Creation Time	
D	ssh_stage1 10.0.138.29	00:04:29	Dec/04/2024 09:57:55	
D	ssh_stage2 10.0.138.29	00:09:29	Dec/04/2024 10:00:16	

e) Wykonaj kolejne połączenie i obserwuj reguły

Firewall															
Filter Rules															
#	Action	Chain	Src. Address	Dst. Address	Src. Address L...	Dst. Ad...	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	In. Inter...	Out. Int...	Bytes	Pa...
0	drop	input			ssh_blacklist									4510 B	
1	add src to address list	input			ssh_stage2		6 (tcp)		22					52 B	
2	add src to address list	input			ssh_stage1		6 (tcp)		22					104 B	
3	add src to address list	input					6 (tcp)		22					156 B	

Firewall				
Filter Rules				
List	Address	Timeout	Creation Time	
D	ssh_blacklist 10.0.138.29	9d 23:59:05	Dec/04/2024 10:01:38	
D	ssh_stage1 10.0.138.29	00:04:05	Dec/04/2024 09:57:55	
D	ssh_stage2 10.0.138.29	00:09:05	Dec/04/2024 10:00:16	

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 kolejki

Do oznaczania pakietów wykorzystamy Mangle (IP / Firewall / Mangle).

Skorzystamy z maszyny wirtualnej win-02 i wprowadzimy ograniczenia transferu dla niej.

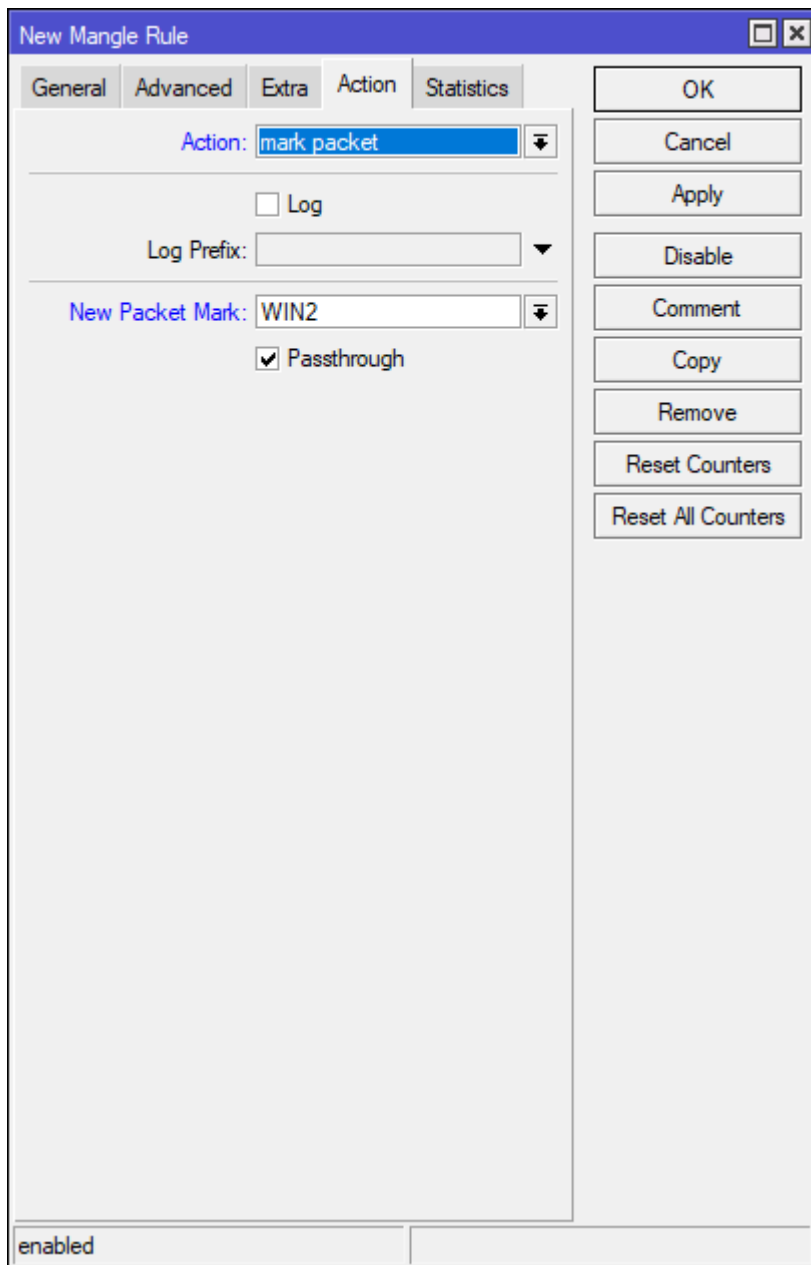
17. Utwórz nową regułę na łańcuchu „forward”, która będzie oznaczać pakiety przychodzące z Internetu do maszyny win-02. W tym celu za Internet przyjmujemy źródło jako adres sieci 0.0.0.0/0. Jako „Dst. Address” wskaż adres IP maszyny win-02. W zakładce „Action” nazwę oznaczenia pakietów „mark packet”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

The image shows the 'New Mangle Rule' dialog box with the following configuration:

- Chain:** forward
- Src. Address:** 0.0.0.0/0
- Dst. Address:** 10.10.100.xx
- Protocol:** (empty)
- Src. Port:** (empty)
- Dst. Port:** (empty)
- Any. Port:** (empty)
- In. Interface:** (empty)
- Out. Interface:** (empty)
- In. Interface List:** (empty)
- Out. Interface List:** (empty)
- Packet Mark:** WIN2
- Connection Mark:** (empty)
- Routing Mark:** (empty)
- Connection Type:** (empty)
- Connection State:** (empty)
- Connection NAT State:** (empty)

Buttons on the right: OK, Cancel, Apply, Disable, Comment, Copy, Remove, Reset Counters, Reset All Counters.

At the bottom left, the 'enabled' checkbox is checked.



18. Podobną regułę tworzymy dla ruchu w drugim kierunku

New Mangle Rule □ ×

General **Advanced** Extra Action Statistics

Chain: forward ▾

Src. Address: 10.10.100.xx ▲

Dst. Address: 0.0.0.0/0 ▲

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: ▾

enabled

OK

Cancel

Apply

Disable

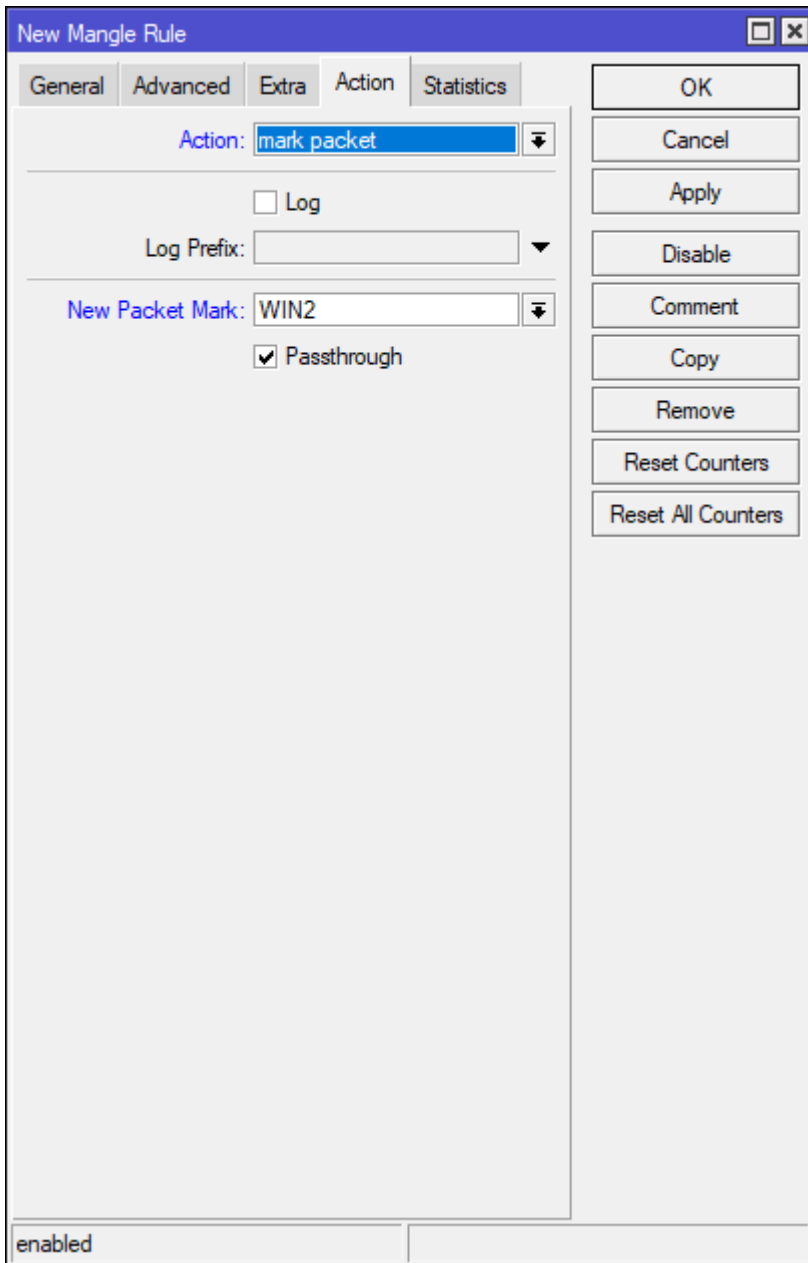
Comment

Copy

Remove

Reset Counters

Reset All Counters

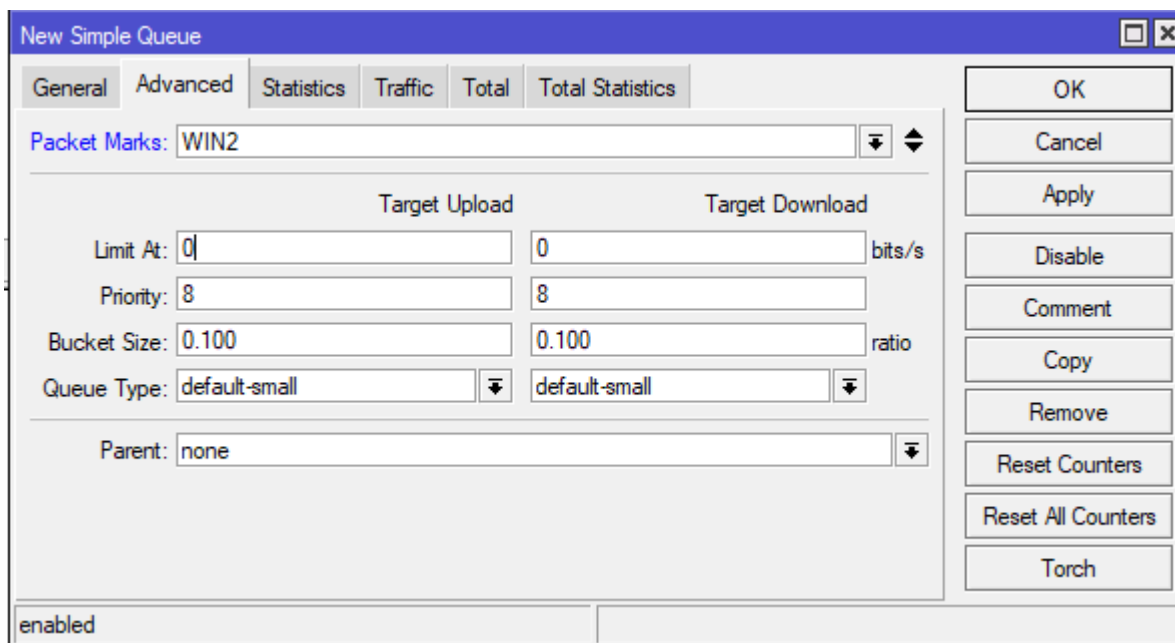
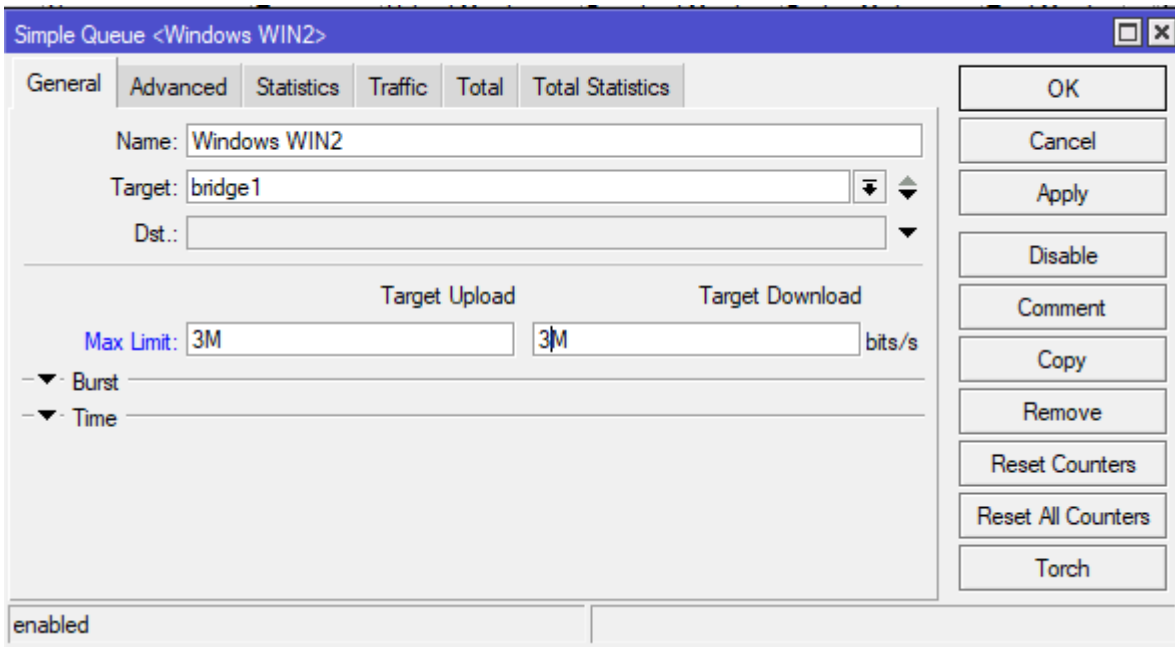


#	Action	Chain	Src. Address	Dst. Address	Src. Ad...	Dst. Ad...	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	In. Inter...	Out. Int...	Bytes	Packets
0	mar...	forward	0.0.0.0/0	10.10.100...										0 B	0
1	mar...	forward	10.10.100...	0.0.0.0/0										0 B	0

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 (dowolną, ale identyfikującą klienta), target (tu

wskazemy 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.



Queue List

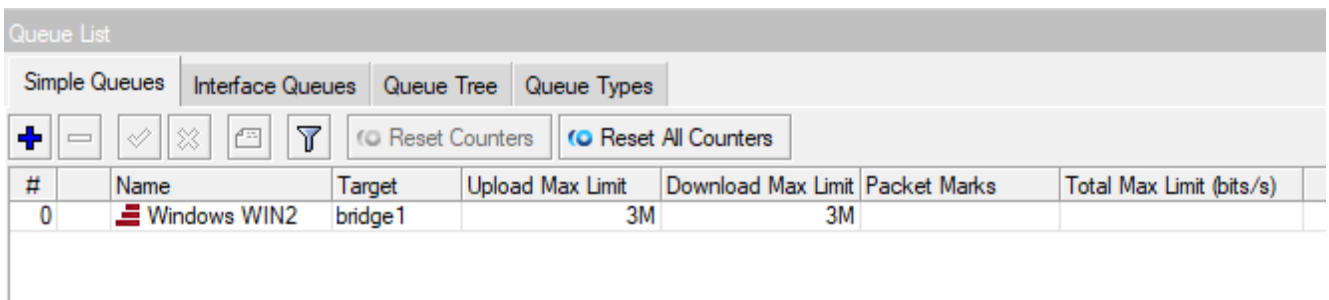
Simple Queues | Interface Queues | Queue Tree | Queue Types

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

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

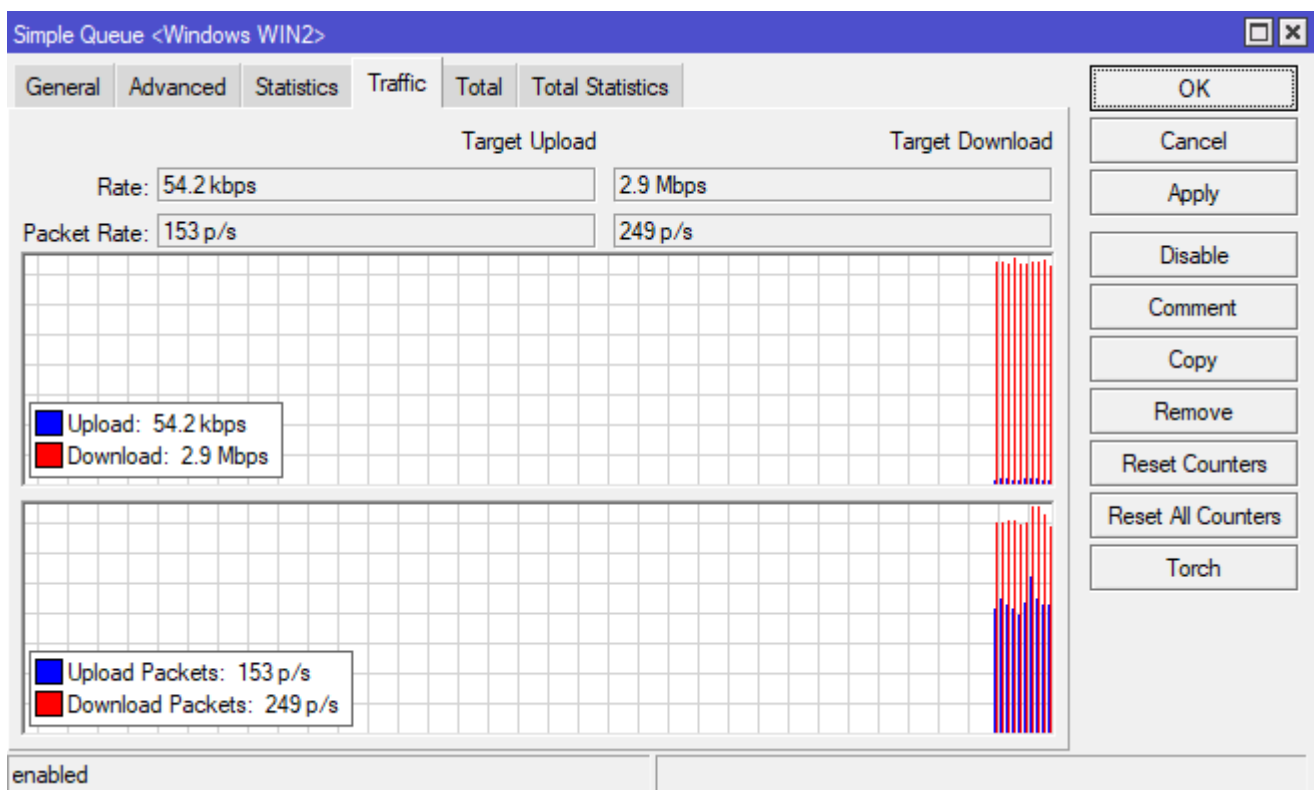
20. Przetestujemy ograniczenia. Na win-02 uruchom proces pobierania dużego pliku np. z podanego linku:

<https://gsliwinski.wi.zut.edu.pl/vm/ubuntu-24.04.1-live-server-amd64.iso> i obserwuj działanie kolejki.

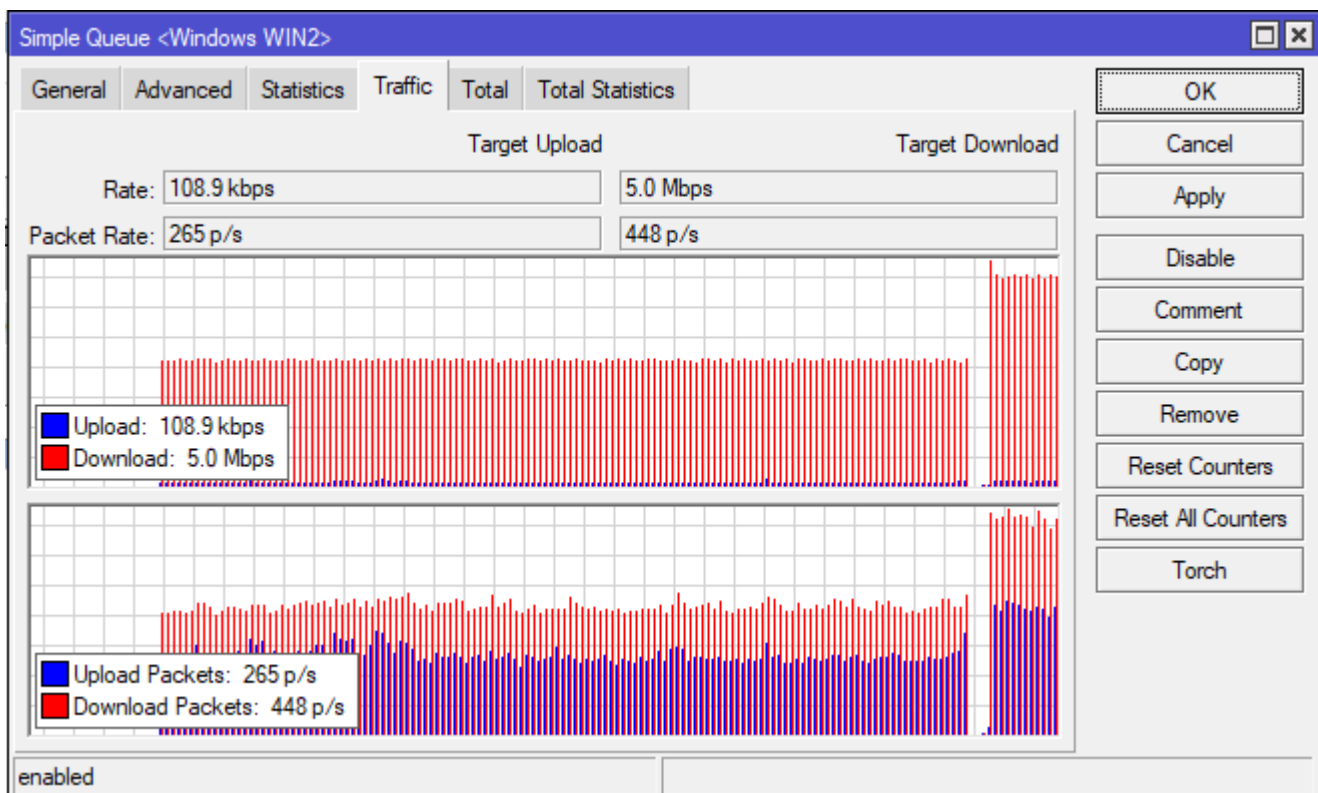
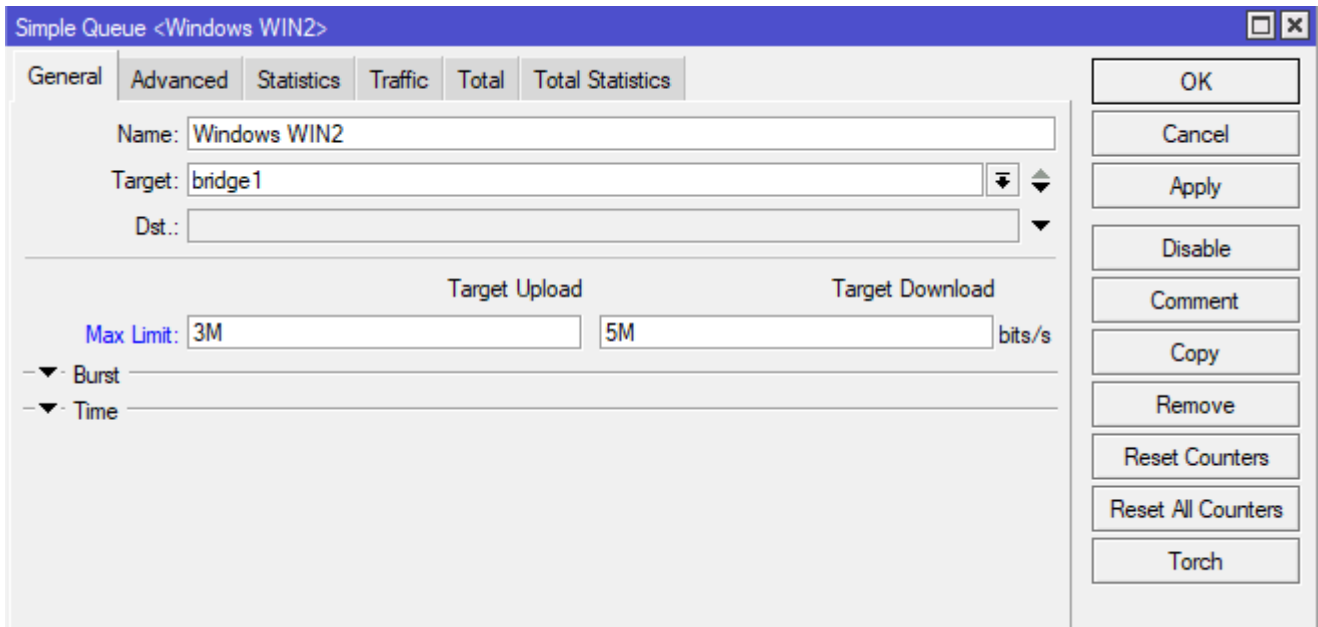


#	Name	Target	Upload Max Limit	Download Max Limit	Packet Marks	Total Max Limit (bits/s)
0	Windows WIN2	bridge1	3M	3M		

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

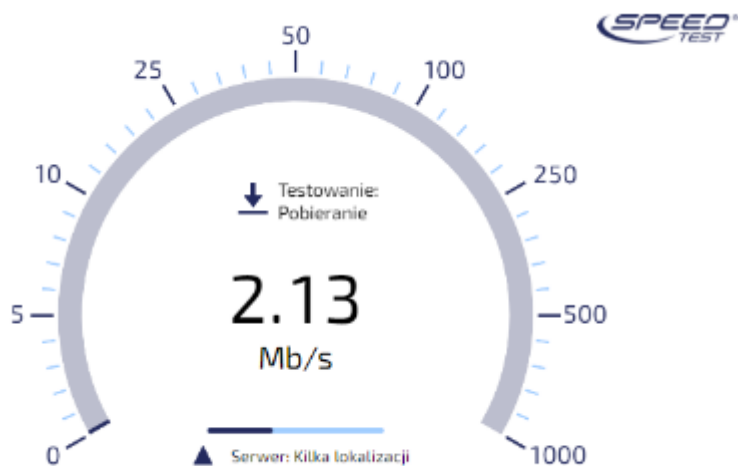


21. Przejdź na zakładkę General. Zwiększ limit Download na 5M, kliknij Apply i przejdź ponownie na zakładkę Traffic



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.

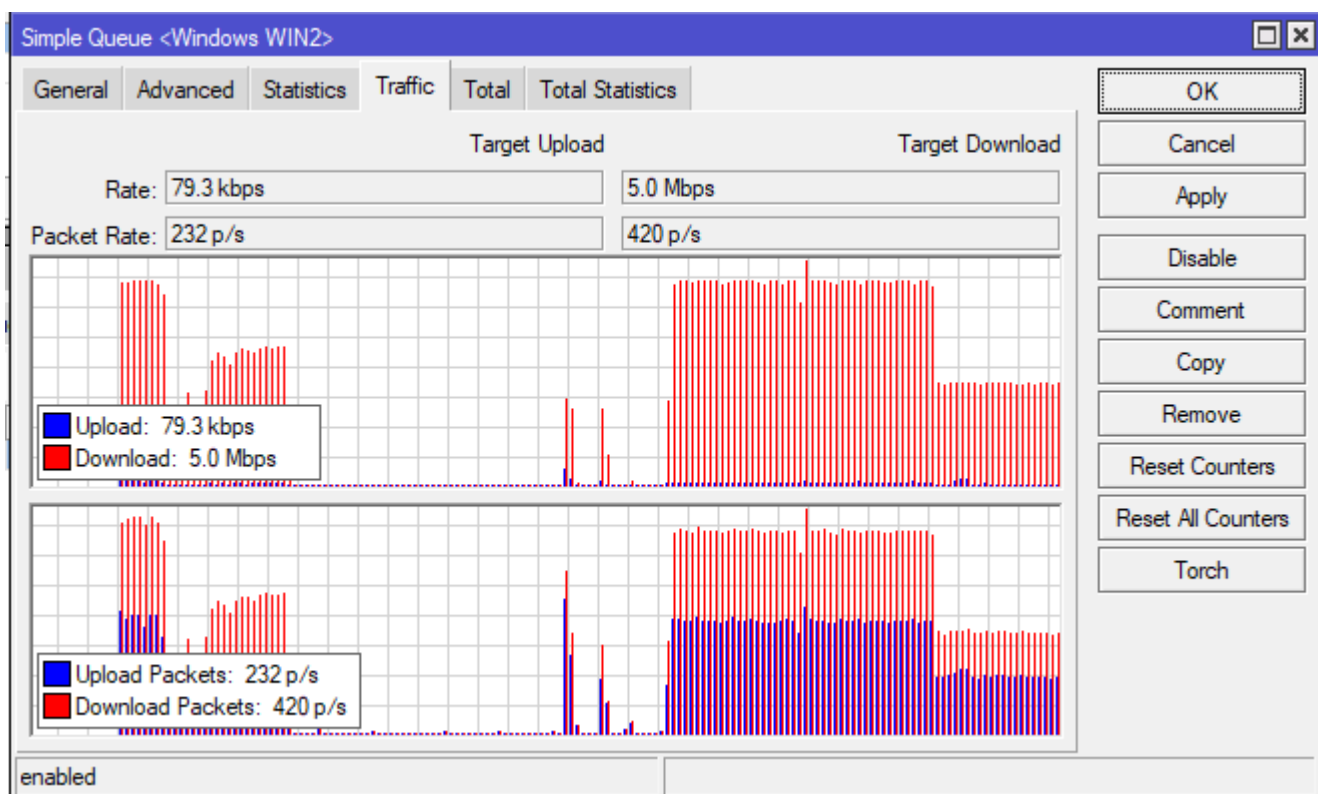
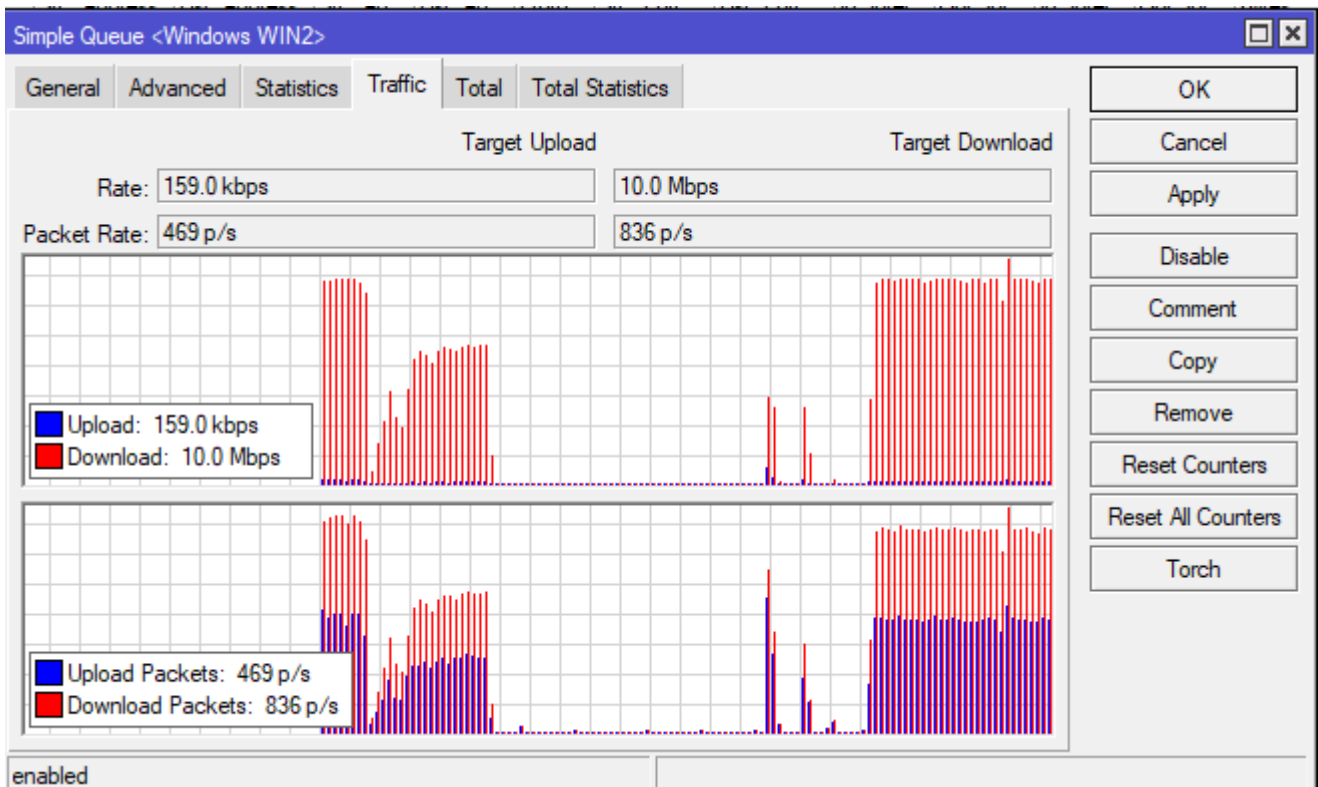


23. Zatrzymaj pobieranie w pierwszej zakładce pliku ISO.

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

The screenshot shows a configuration window titled 'Simple Queue <Windows WIN2>'. It has several tabs: 'General', 'Advanced', 'Statistics', 'Traffic', 'Total', and 'Total Statistics'. The 'Advanced' tab is active. The 'Name' field contains 'Windows WIN2'. The 'Target' dropdown is set to 'bridge1'. The 'Dst.' field is empty. Below this, there are two columns: 'Target Upload' and 'Target Download'. Under 'Burst' (expanded), there are four rows of settings: 'Max Limit' (3M for Upload, 5M for Download), 'Burst Limit' (10M for Upload, 10M for Download), 'Burst Threshold' (3M for Upload, 5M for Download), and 'Burst Time' (90 for Upload, 90 for Download). At the bottom left, there is a checkbox labeled 'enabled' which is checked. On the right side, there is a vertical stack of buttons: 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', 'Copy', 'Remove', 'Reset Counters', 'Reset All Counters', and 'Torch'.

Kliknij Apply i przejdź na zakładkę Traffic - obserwuj transfer



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

Simple Queue <Windows WIN2>

General | Advanced | Statistics | Traffic | Total | Total Statistics

Name: Windows WIN2

Target: bridge1

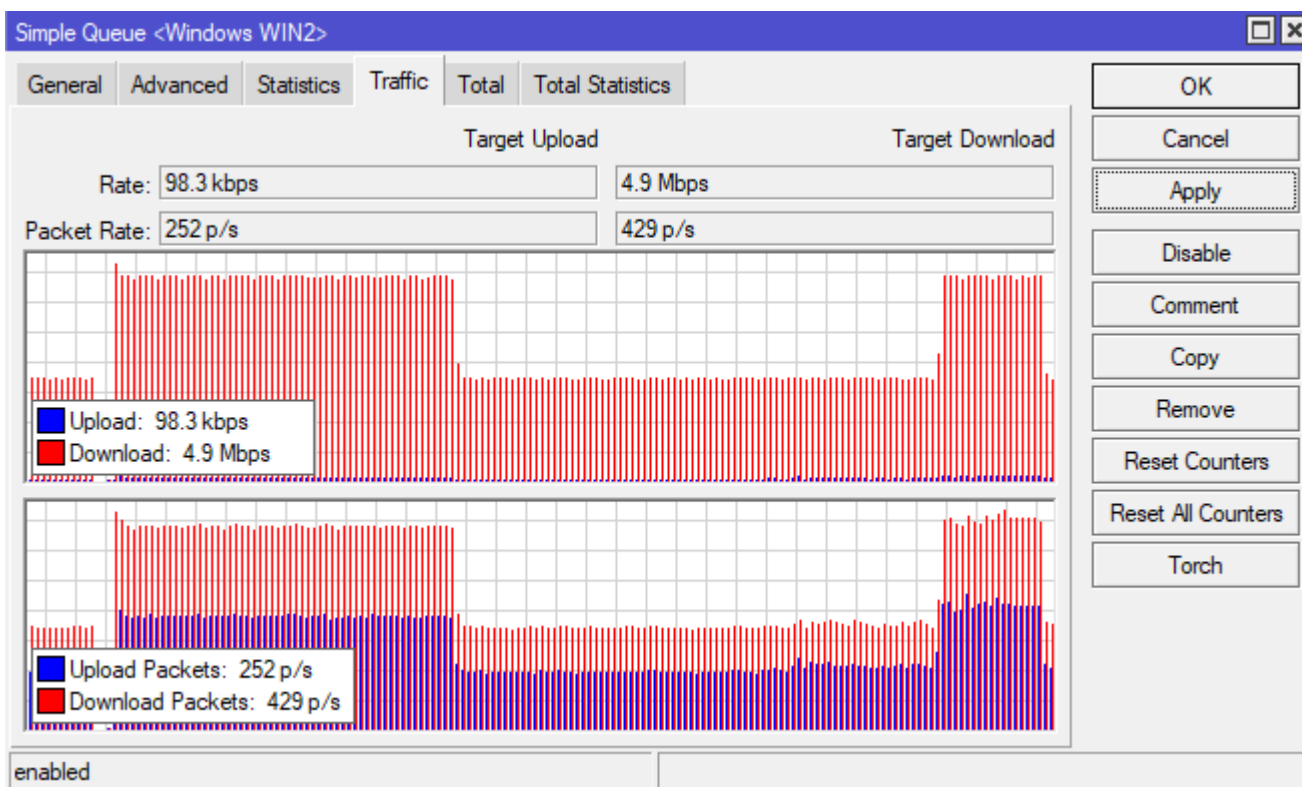
Dst.:

	Target Upload	Target Download
Max Limit:	3M	5M bits/s
Burst		
Burst Limit:	10M	10M bits/s
Burst Threshold:	3M	6M bits/s
Burst Time:	90	90 s

Time

enabled

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters
Torch



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.

Zgłoś do prowadzącego wykonanie zadania.

Zadanie dodatkowe

25. Uruchom na win-02 serwer [FTP](#). Na mikrotiku R1 ustaw przekierowanie portu 21, tak żeby z maszyny wirtualnej win-01 można było zalogować się i pobrać plik z serwera FTP.