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).



 Podłącz komputer (krosownica port1) do twojego prywatnego switch a następnie kolejny port switcha do routera R1 na porcie Ether2 (wykonaj reset do konfiguracji domyślnej)

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.

Virtual	Machine	Settings
---------	---------	----------

Hardware Options		
Hardware Options	Summary 4 GB 2 60 GB Using file C:\sk\iso\Windows Custom (Karta-Port-2) Present Auto detect Present Auto detect View of the second seco	Device status Connected Connect at power on Network connection Bridged: Connected directly to the physical network Replicate physical network connection state NAT: Used to share the host's IP address Host-only: A private network shared with the host Custom: Specific virtual network Karta-Port-2 LAN segment: Advanced
		OK Cancel Help

 \times

- 7. Przejdź do routera R1 i wykonaj następujące czynności:
- a) Ustaw DHCP-Client na porcie Ether1
- b) Dodaj interfejs Bridge i przypisz do niego port Ether3
- 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 (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 Stati	Stics OK
Chain: dstnat	∓ Cancel
Src. Address:	- Apply
Dst. Address:	▼ Disable
Src. Address List:	Comment
	Сору
Protocol: 6 (tcp)	Remove
Dst. Port: 3389	Reset Counters
Any. Port:	← Reset All Counters
In. Interface:	T
Out. Interface:	
In. Interface List:	
Out. Interface List:	
Packet Mark:	
Connection Mark:	
Routing Mark:	▼
Connection Type:	
enabled	

New NAT Rule	
General Advanced Extra Action Statistics	ОК
Action: dst-nat	Cancel
	Apply
Log Prefix:	Disable
To Addresses: 10.10.100.xxx	Comment
To Ports: 3389	Сору
	Remove
	Reset Counters
	Reset All Counters
enabled	

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

← Settings		- 0	×
User Local Account	System > About		
Find a setting Q	win-02 VMware7,1	Rename this PC	
System	Device specifications	Сору	~
 Bluetooth & devices Network & internet Personalization Apps Accounts Time & language Gaming Accessibility 	Device name win-02 Processor Intel(R) Core(TM) i7-7700K CPU @ 4.20GHz Installed RAM 4.00 GB Device ID CC38CB43-FE83-4C46-8798-130A21889175 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	Сору	~
Privacy & securityWindows Update	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	:	>
System Properties			

System Propertie	25				×
Computer Name	Hardware	Advanced	System Protect	tion Remot	e
Remote Assist	ance				
Allow Remo	ote Assistanc	ce connection	ns to this comput	ter	
What happens	when I ena	ble Remote /	Assistance?		
				Advanced	
Remote Deskt	ор				
Choose an opt	ion, and the	n specify who	can connect.		
O Don't allow	remote con	nections to th	is computer		
 Allow remoti 	te connectio	ns to this cor	nputer		
Allow co Desktop	onnections o with Netwo	nly from com rk Level Auth	outers running R nentication (reco	emote mmended)	
Help me choos	<u>se</u>		C	Select User	s
		ок	Cano	cel	Apply

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

koniec laboratorium.

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

net localgroup administrators user1 /add



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

10. Z maszyny win-01 uruchom połączanie pulpitu zdalnego na adres routera

R1. Adres routera sprawdź w /IP/ADDRESSES przypisany na porcie Ether1

Address List		
	7	Find
Address	A 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 M —	1ore ~	
Best match		
Remote Desktop Connection App		
Settings		Remote Desktop Connection
✓ Remote desktop settings	>	Арр
رور Remote Desktop Developer Ve Settings	>	 Open Run as administrator
RemoteApp and Desktop Connections	>	 Open file location Pin to Start
Allow Remote Assistance invitations to be sent from this	>	🔗 Pin to taskbar
Access RemoteApp and desktops	>	
ဗြੰ∄ Enable Device Portal	>	
Select users that can remote ly access this PC	>	
Search the web		
Ø remote - See web results	>	
nodłączanie pulpitu zdalnego	_	
Podłączanie pulpitu zdalne	go	
Komputer: a.b.c.d	、 、	
Nazwa użytkownika: Nie określono		
Podczas łączenia zostanie wyświetlony monit o po poświadczeń.	odanie	
Pokaż opcje	Podłącz	Pomoc



Enter your credentials

These credentials will be used to connect to 10.0.100.213.

User name	
Password	
Remember me	
	Consul
OK	Cancel

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.

Nemote Desktop Connection X		
The identity of the remote computer cannot be verified. Do you want to connect anyway?		
The remote computer could not be authenticated due to problems with its security certificate. It may be unsafe to proceed.		
Name in the certificate from the remote computer: win-02		
Certificate errors		
The following errors were encountered while validating the remote computer's certificate:		
The certificate is not from a trusted certifying authority.		
Do you want to connect despite these certificate errors?		
Don't ask me again for connections to this computer		
View certificate Yes No		

X

user1
Another user is signed in. If you continue, they'll be disconnected. Do you want to sign in anyway?
Yes No







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.



O 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 nawiążesz 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

	NAT Rule <3389>	
Firewall	General Advanced Extra Action Statistics	ОК
Hiter Rules NAT Mangle Raw Service	Chain: dstnat	Cancel
	Src. Address:	Apply
0 1 masquerade srcnat	Dst. Address:	Disable
1 ▶]" dst-nat dstnat	Src. Address List:	Comment
	Dst. Address List:	Сору
	Protocol: 6 (tcp)	Remove
	Src. Port:	Reset Counters
	Dst. Port: 9000	Reset All Counters
	Any. Port:	
	Out Interface:	
2 items (1 selected)		
	Packet Mark:	
	Connection Mark:	
	Connection Type:	
	enabled	
퉣 Podłączanie pulpitu zdalnego	- 🗆 🗙	
Dedlacrania		
	Inogo	
	intego	
Komputer: a.b.c.d:9000	~	
Nazwa użytkownika: Nie określono		
Podczas łączenia zostanie wyświetlony m poświadczeń.	ionit o podanie	
💿 <u>P</u> okaż opcje	Podłącz Pomoc	

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 kilkukrotnie będą próbować się łączyć na nasz router.

a) Utwórz regułę na łańcuchu "input", protokół TCP, port docelowy "22", stan połaczenia "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

New Firewall Rule	
General Advanced Extra Action Statistics	ОК
Chain: input	Cancel
Src. Address:	Apply
Dst. Address:	Disable
Src. Address List:	Comment
Dst. Address List:	Сору
Protocol: 6 (tcp)	Remove
Src. Port:	Reset Counters
Dst. Port: 22	Reset All Counters
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:	
enabled	

New Firewall Rule	
General Advanced Extra Action Statistics	ОК
Action: add src to address list	Cancel
	Apply
Log Prefix:	Disable
Address List: ssh_stage1	Comment
Timeout: 00:05:00 ₹	Сору
	Remove
	Reset Counters
	Reset All Counters

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.

New Firewall Rule	
General Advanced Extra Action Statistics	ОК
Chain: input	Cancel
Src. Address:	Apply
Dst. Address:	Disable
Src. Address List: ssh_stage1	Comment
Dst. Address List:	Сору
Protocol: 6 (tcp)	Remove
Src. Port:	Reset Counters
Dst. Port: 22	Reset All Counters
In Interface:	
Out. Interface:	
In Interface List:	
Out. Interface List:	
Paakat Made	
Routing Mark:	
Connection State: invalid established related view untracked	
Connection NAT State:	
enabled	J

New Firewall Rule	
General Advanced Extra Action Statistics	ОК
Action: add src to address list	Cancel
Log	Apply
Log Prefix:	Disable
Address List: ssh_stage2	Comment
Timeout: 00:10:00	Сору
	Remove
	Reset Counters
	Reset All Counters
enabled	

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

Firewall																			
Filter Rul	es NAT	Mangle	Raw	Service Port	s C	Connection	s	Address Li	ists	Layer7 Prot	ocols								
+ -	* X	- 7	0	Reset Counte	irs	(O Reset	All C	Counters											
#	Action			Chain	Src.	Address	Dst.	Address	Src.	Address L	Dst. A	d	Proto	Src.	Port	Dst. Port	In.	Inter	С
0	📑 add sro	to address	list	input									6 (tcp)			22			
1	📑 add sro	to address	list	input					ssh_	_stage1			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	ОК
Chain: input	Cancel
Src. Address:	Apply
Dst. Address:	Disable
Src. Address List: ssh_stage2	Comment
Dst. Address List:	Сору
Protocol: 6 (tcp)	Remove
Src. Port:	Reset Counters
Dst. Port: 22	Reset All Counters
Any. Port:	
Out. Interface:	
Packet Mark:	
Connection Mark:	
Connection Type:	
Connection State:invalidestablishedrelatedinewuntracked ▲	
enabled	

New Firewall Rule	
General Advanced Extra Action Statistics	ОК
Action: add src to address list	Cancel
Log	Apply
Log Prefix:	Disable
Address List: ssh_blacklist	Comment
Timeout: 10d 00:00:00	Сору
	Remove
	Reset Counters
	Reset All Counters
enabled	1

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

Firewa	all													
Filter	Rules	NAT Mangle	Raw	Service Port	s Connection	ns Address L	ists Layer7 Prot	ocols						
+		/ 🛛 🖻 🍸	(0	Reset Counte	ers (O Rese	t All Counters]							
#	Ac	tion		Chain	Src. Address	Dst. Address	Src. Address L	Dst. Ad	Proto	Src. Port	Dst. Port	In. Inter	Out. Int	. In. Ir
0		add src to address	list	input			ssh_stage2		6 (tcp)		22			
1		add src to address	list	input			ssh_stage1		6 (tcp)		22			
2		add src to address	list	input					6 (tcp)		22			

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.

New Firewall Rule		
General Advanced	Extra Action Statistics	ОК
Chain	input 🗧	Cancel
Src. Address	▼	Apply
Dst. Address	▼	Disable
Src. Address List	ssh_blacklist	Comment
Dst. Address List		Сору
Protocol		Remove
Src. Port	▼	Reset Counters
Dst. Port	▼	Reset All Counters
Any. Port		Nesel Air Counters
In. Interface		
Out. Interface		
In. Interface List	·	
Out. Interface List		
Packet Mark		
Connection Mark	▼	
Routing Mark	·	
Connection Type	· · · · · · · · · · · · · · · · · · ·	
Connection State	·	
Connection NAT State	·	
enabled		

New Firewall Rule	
General Advanced Extra Action Statistics	ОК
Action: drop	Cancel
Log	Apply
Log Prefix:	Disable
	Comment
	Сору
	Remove
	Reset Counters
	Reset All Counters

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

Firewall											
Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols											
+ -	+ - × × Counters Counters Counters										
#	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

Addres	ss List			
+	- 🖉 💥 🖻	7]	Find
	Address	- A	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	3			

🕵 PuTTY Configuration		? ×
Category:		
⊡- Session	Basic options for your PuTTY	session
Logging	- Specify the destination you want to cor	nnect to
Keyboard	Host Name (or IP address)	Port
Bell	10.0.138.148	22
Features	Connection type:	
Window	SSH ○ Serial ○ Other: Te	lnet 🗸
Behaviour Translation Translation Colours Connection Data Proxy SSH Serial Telnet Rlogin SUPDUP	Load, save or delete a stored session - Saved Sessions Default Settings switchman	Load Save Delete
About Help	Open	Cancel

c) Zaobserwuj co się stało po pierwszym połączeniu

Firewall															
Filter Rule	es NAT Mangle Raw	Service Port	s Connection	s Address Li	sts Layer7 Prot	ocols									
+ -	X	Reset Counte	ers (O Reset	All Counters									Find	all	
#	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	В
1	add src to address list	input			ssh_stage2		6 (tcp)		22					0	В
2	add src to address list	input			ssh_stage1		6 (tcp)		22					_	В
3	📑 add src to address list	input					6 (tcp)		22					52	B)

Firewall									
Filter Rules N/	AT	Mangle Ra	aw Servi	ce Ports	Connection	ns Addr	ess Lists	Layer7 Prot	ocols
+ - /	83	27							
List	A	Address		Timeout		Creation 1	Time		
D 😐 ssh_stage	e1	10.0.138.29			00:03:43	D	ec/04/20	24 09:57:55	

d) Wykonaj kolejne połączenie i obserwuj reguły

	Firewall															
	Filter Rule	es NAT Mangle Raw	Service Ports	Connection	s Address Li	ists Layer7 Prot	ocols									
ĺ	+ -	×	Reset Counte	rs (O Reset	All Counters									Find	all	
	#	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	
Ш	1	add src to address list	input			ssh_stage2		6 (tcp)		22					0 B	
Ш	2	add src to address list	input			ssh_stage1		6 (tcp)		22					52 B	
Ш	3	add src to address list	input					6 (tcp)		22					104 B	

Mangle	Raw Servi	ce Ports	Connectio	ns Address Lists	Layer7 Prot	ocols
- 7						
Address		Timeout		Creation Time		
10.0.138.29)		00:04:29	Dec/04/20	024 09:57:55	
10.0.138.29			00:09:29	Dec/04/20	024 10:00:16	
	Mangle	Mangle Raw Servi Address 10.0.138.29 10.0.138.29	Mangle Raw Service Ports	Mangle Raw Service Ports Connectio Image: Construction Image: Construction Image: Construction Image: Construction Address Timeout Image: Construction Image: Construction Image: Construction Address Timeout Image: Construction Image: Construction Image: Construction 10.0.138.29 00:04:29 00:09:29 Image: Construction Image: Construction	Mangle Raw Service Ports Connections Address Lists Image: Contract in the service Ports Image: Contract in the service Ports Creation Time Address Timeout Creation Time 10.0.138.29 00:04:29 Dec/04/20 10.0.138.29 00:09:29 Dec/04/20	Mangle Raw Service Ports Connections Address Lists Layer7 Prot Image: Service Ports Timeout Creation Time Address Timeout Creation Time 10.0.138.29 00:04:29 Dec/04/2024 09:57:55 10.0.138.29 00:09:29 Dec/04/2024 10:00:16

e) Wykonaj kolejne połączenie i obserwuj reguły

Firewall															
Filter Rul	es NAT Mangle Raw	Service Port	s Connection	ns Address L	ists Layer7 Prot	ocols									
+ -	X	Reset Counte	ers (© Reset	t All Counters									Find	all	1
#	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 F	3
1	add src to address list	input			ssh_stage2		6 (tcp)		22					52 E	3
2	add src to address list	input			ssh_stage1		6 (tcp)		22					104 E	3
3	add src to address list	input					6 (tcp)		22					156 E	3
Eiround	II.														

Fil	ter Rules NAT	Mangle	Raw	Service Por	ts Connections	Address List	Layer7 Protocols
÷			ſ				
	List	🗠 Add	ress		Timeout	Creation T	ìme
D	ssh_blacklist	10.0).138.29)	9d 23:59	:05 De	ec/04/2024 10:01:38
D	ssh_stage1	10.0).138.29)	00:04	:05 De	ec/04/2024 09:57:55
D	ssh_stage2	10.0).138.29)	00:09	:05 De	ec/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 kolejkowanie

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".

New Mangle Rule					
General Advanced	Extra	Action	Statistics		ОК
Chain:	forwar	d		₹	Cancel
Src. Address:	0.	0.0.0/0		•	Apply
Dst. Address:	10	.10.100.x	×] ▲	Disable
Src. Address List:				. ▼	Comment
Dst. Address List:				•	Copy
Protocol:] 🗕 📔	Bemove
Src. Port:] 🛨 📗	Rent Counter
Dst. Port:				-	Reset Counters
Any. Port:				-	Reset All Counters
In. Interface:				-	
Out. Interface:				•	
In. Interface List:				-	
Out. Interface List:				•	
Packet Mark:				-	
Connection Mark:				-	
Routing Mark:				•	
Connection Type:				-	
Connection State:				-	
Connection NAT State:] 🗕 📔	
enabled					



18. Podobną regułę tworzymy dla ruchu w drugim kierunku

New Mangl	e Rule					
General	Advanced	Extra	Action	Statistics	L	ОК
	Chain:	forwar	d		Ŧ	Cancel
:	Src. Address:	10	.10.100.x	x] • [Apply
l	Dst. Address:	0.	0.0.0/0] •	Disable
Src.	Address List:					Comment
Ust.	Address List:					Сору
	Protocol:				•	Remove
	Src. Port:					Reset Counters
	Any Port					Reset All Counters
	In. Interface:				-	
0	ut. Interface:				-	
In. I	nterface List:				-	
Out. I	nterface List:				-	
F	Packet Mark:				•	
Conn	nection Mark:				-	
F	Routing Mark:				-	
Conn	ection Type:				•	
Conn	ection State:				-	
Connection	n NAT State:				-	
enabled						

New Mang	le Rule															
General	Advanced	Extra	Action	Statistics			ОК									
	Action:	mark p	oacket		₹		Cance									
		Log	,				Apply									
	Log Prefix:				-		Disable	;								
New	Packet Mark:	WIN2			∓		Commer	nt								
		✓ Pas	ssthrough				Сору									
							Remove	e								
						Re	eset Cour	nters								
						Res	et All Co	unters								
enabled																
chabled																
Firewall																
Filter Rules	NAT Mangle	Raw Ser	vice Ports C	Connections A	ddress L	ists Laye	er7 Protocols								Cin. 1	
# - <	ion Chain	Src. Add	et Counters ress Dst. Ad	CReset All Co dress Src. Ad	Dist. A	d Proto	Src. Port	Dst. Port	In. Inter	Out. Int	. In. Inter.	. Out. Int	. Bytes		Find Packets	
0 🥒	mar forward mar forward	0.0.0.0/0) 10.10.1)0 0.0.0.0/	00 ⁄0										0 B 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 (dowolna, ale identyfikująca klienta), target (tu

wskażemy interface na którym kolejka zostanie przypieta, 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.

Simple Que	eue <window< th=""><th>s WIN2></th><th></th><th></th><th></th><th></th></window<>	s WIN2>				
General	Advanced	Statistics	Traffic Tot	al Total Statistics	I	ОК
	Name: Wind	lows WIN2				Cancel
	Target: bridge	e1			= =	Apply
	Dst.:					Disable
			Target Uplo	ad	Target Download	Comment
Ma	x Limit: 3M			3M	bits/s	Сору
- ▼ · Burs	e					Remove
						Reset Counters
						Reset All Counters
						Torch
enabled]	
New Simp	le Queue					
General	Advanced	Statistics	Traffic Tot	tal Total Statistics		ОК
Packet M	Marks: WIN2				₹ \$	Cancel
			Target Uplo	ad	Target Download	Apply
Lir	mit At: 0			0	bits/s	Disable

Queue Lis	t				
Simple Q	ueues Interface Que	eues Queue	Tree Queue Type	3	
+ -	🖌 🗶 🗖 🏅	' (O Reset	Counters (O Rese	t All Counters	
#	Name	Target	Upload Max Limit	Download Max Lin	nit Packet Marks
0	📕 Windows WIN2	bridge1	3M	3	М

8

Ŧ

0.100

default-small

Comment

Сору

Remove

Reset Counters Reset All Counters Torch

ratio

Ŧ

Ŧ

Priority: 8

Bucket Size: 0.100

enabled

Queue Type: default-small

Parent: none

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.



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

Simple Queue <windows win2=""></windows>	
General Advanced Statistics Traffic Total Total Statistics	OK
Target Upload Target Download	Cancel
Rate: 54.2 kbps 2.9 Mbps	Apply
Packet Rate: 153 p/s 249 p/s	Disable
	Comment
	Сору
Unload: 54.2 kbps	Remove
Download: 2.9 Mbps	Reset Counters
	Reset All Counters
	Torch
Upload Packets: 153 p/s	
Download Packets: 249 p/s	
enabled	-

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

Simple Queue <windows win2=""></windows>		
General Advanced Statistics Traffic Total Total Statistics	ОК	
Name: Windows WIN2	Cancel	
Target: bridge1	Apply	
Dst.:	▼ Disable	
Target Upload Target Download	Comment	
Max Limit: 3M 5M bit	copy	
-▼ Burst	Remove	
	Reset Coun	ters
	Reset All Cou	nters
	Torch	



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

Simple Queue <wind< th=""><th>ows WIN2></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th></wind<>	ows WIN2>								
General Advance	d Statistics	Traffic	Total	Total S	Statistics				ОК
Name: ₩	indows WIN2								Cancel
Target: bri	dge1						Ŧ	\$	Apply
Dst.:								•	Disable
			Target (Upload		Ta	rget Download		Comment
Max Limit: 3N	1				5M		b	oits∕s	Сору
Burst Limit: 10	М				10M		ь	its/s	Remove
Burst Threshold: 3M	1				5M		b	oits/s	Reset Counters
Burst Time: 90					90		s		Reset All Counters
-▼· Time									Torch
enabled									

Kliknij Apply i przejdź na zakładkę Traffic – obserwuj transfer





25. Zmień limit (próg) "Burst Threshold" dla Download na 6M - obserwuj Traffic

Simple Queue <v< th=""><th>Vindows WIN2></th><th></th><th></th><th></th><th></th></v<>	Vindows WIN2>				
General Adva	anced Statistics	Traffic Total	Total Statistics		ОК
Name	: Windows WIN2				Cancel
Target	: bridge1			₹ \$	Apply
Dst.	:			▼	Disable
		Target (Jpload	Target Download	Comment
Max Limit	: 3M		5M	bits/s	Сору
-▲·Burst	. 10M		10M	hito /o	Remove
Burst Threshold	: 3M		6M	bits/s	Reset Counters
Burst Time	: 90		90	s	Reset All Counters
-▼· Time					Torch
enabled					
			I		
Simple Queue <\	Windows WIN2>				
General Adva	anced Statistics	Traffic Total	Total Statistics		ОК
		Target	Upload	Target Download	Cancel



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.