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.

Virtual Machine Settings		×
Hardware Options		
Device Memory Processors Hard Disk (NVMe) CD/DVD (SATA) Network Adapter Sound Card Display Trusted Platform Mo	Summary 4 GB 2 64 GB Auto detect NAT Present Auto detect Auto detect Present Present	Device status Connected Connected Connection Bridged: Connected directly to the physical network Replicate physical network connection state Host-only: A private network shared with the host Custom: Specific virtual network wifi-card LAN segment: Advanced
		OK Cancel Help

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

https://download.mikrotik.com/routeros/winbox/4.0beta17/WinBox_Windows.z ip)

- 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

0	тікготій	¢	Workspace: <ow< th=""><th>n></th><th>· ① 2</th><th>Q</th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th></ow<>	n>	· ① 2	Q								
1.	Quick Set													
1	WiFi			HCF	Client ~	DHCP Client	DHCP	Client Options					с ×	
	Interfaces			ew	Enable	Disable (Rem	ove	Q Find	Y Filter		~		
Ŵ	WireGuard		0 P	-	Interface	^ Use P	Add	IP Address	Expires After	Status	=	2	Actions	
ł	Bridge					1						Reli	ease	
토	PPP				VH DHCP CI	lient			New	Ċ			o	×
T	Switch	>						Status	stopped					
S	Mesh							DISABLED IN	VALID DYNAMI					
<u>v4</u>	IP	>											DHCP	
<u>v6</u>	IPv6	>				Enabled							Advanced	
0	MPLS	>				Comment	t						Status	
X	Routing	>			^ DHCP									_
@ }	System	>				Interface	ethe	erl			*		🖗 Actio	ns
<u>Ch</u>	Queues					Use Peer DNS	5						Release	
-®-	Dot1X			_		Use Peer NTF	•						Renew	
D	Files			_										
Ë	Log				Add	Default Route	e yes				~			
>	New Terminal				~ Advance	d								
es.	RADIUS				- Status									
ക്	Tools	>			Cancel						AD	ply	ок	
3	Partition								_					
	Make Supout.rif	f												

b) Dodaj interfejs Bridge i przypisz do niego port Ether2

]-[Bridge		Ν	lew		¢	c ×
DISA	BLED DY	NAMIC INVALID	RUNNING	SLAVE	PASSTHROUGH	
Enabled Comment						General STP VLAN
 General Name 	bridge1					Status
Туре	Bridge					S Actions
Actual MTU						Torch
L2 MTU MAC Address						Reset frame Counters
ARP ARP Timeout	enabled	l			~	
Admin. MAC Address	+					
Ageing Time	00:05:00	0				
Max Learned Entries	auto				~	
IGMP Snooping						
DHCP Snooping						
Fast Forward						
✓ STP						
VLAN						
 Status Traffic 						
Cancel						
Calleer						

c) Nadaj adres IP dla bridge1 10.10.100.1/24

$\frac{\sqrt{4}}{\delta}$ Address	New	C	с ×
DISABLED	D DYNAMIC INVALID	SLA	VE
Enabled			
Comment			
Address	10.10.100.1/24		
Network	+		
Interface	bridge1		*
Cancel	Apply		ОК

d) Skonfiguruj serwer DHCP na interfejsie bridge1

VH DHCP Server V	DHCP	Networks	Leases	Options	Option Sets	option Ma	atcher	Alert	ts r×
La New Denable	Dis	able 🗙 Rem	ove			Q Find Y	Filter		G Actions
P Name	^ II	nterface	Relay	Lease	Time	Address Pool	Add A.	. =	
	2	DHCP Setu	р			c	×		DHCP Setup
				Statu	S:				O Configuration
		Select inte	rface to ru	IN DHCP se	rver on				DHCP Config
		DHCP	Server Int	erface br	idge1		~		
		Cancel			Bac	k Ne	xt		
								1	

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



VH NAT		١	lew		C		e ×
				INVALID			
Enabled						General	
Comment						Advance	d
∧ General						Extra	
Chain	srcnat					Action	
Src Address	+					Statistic	S
Dst. Address	+					Ø Acti	ons
Src Address List	+					Reset C	ounters
Det Address List						Reset A	II Counters
Dat. Address List							
Protocol	+						
Src. Port	+						
Dst. Port	+						
Any. Port	+						
In. Interface	+						
Out. Interface	ether1						
In. Interface List	+						
Out. Interface List	+						
Packet Mark	+						
Connection Mark	+						
Routing Mark	+						
Connection Type							
Connection type							
 Advanced 							
v Extra							
^ Action	macauarada						
Action	masquerade						
Log							
Log Prefix	+						
-							
To Ports	+						
 Statistics 							
						Annha	OK

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.

V ⁴ a NAT		١	New	Û			σ×
Enabled						General	
Comment	-					Advanced	i
						Extra	
∧ General						Action	
Chain	dstnat				Ť	Statistics	
Src. Address						G Activ	ne
Dst. Address						Reset Co	
Src. Address List	+					Reset Al	Counters
Dst. Address List	+						
Protocol	6 (tcp)						
Src. Port	+						
Dst. Port	3389						
Any Port	+						
In Interface	ether1						
Out Interface	-						
out. interface	•						
In. Interface List	+						
Out. Interface List	+						
Packet Mark	+						
Connection Mark	+						
Routing Mark	+						
Connection Type	+						
~ Advanced							
v Extra							
^ Action							
Action	dst-nat				*)		
Log							
Log Prefix	+						
To Addresses	10.10.100.22	?					
To Ports	3389	89 C					
 Statistics 							
Cancel						Apply	ок

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 4.20 GHz (2 processors) 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 System settings Statematications	Сору	
 Privacy & security Windows 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	;	

System Properties	×
Computer Name Hardware Advanced System Protection Remote	
Remote Assistance	
Allow Remote Assistance connections to this computer	
What happens when I enable Remote Assistance?	
Advanced	
Remote Desktop	
Choose an option, and then specify who can connect.	
O Don't allow remote connections to this computer	
 Allow remote connections to this computer 	
Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)	
Help me choose Select Users	
OK Cancel Apply	

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



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 połączanie pulpitu zdalnego na adres routera

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

<u>∨4</u> ठ	Addre	ess List				ø	×
다	New	Enable 🕕 Disable 🗴	Remove		Q Find	Y	Filter
\bigcirc	P	Address	Network	Interface v			=
\bigcirc	D	〒 192.168.3.254/24	192.168.3.0	ether1			
\bigcirc		₽ 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 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	
01	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





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 kilkukrotnie 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

v ⁴ / _δ Firewall v Filter Rules N	VH Filter Rules	New		c X
🗅 New 🕞 Enable 🕕 Disable				
# ^ P Action Chain	Enabled	0		General
	Comment	ī		Advanced
	Or a second			Extra
	General Chain	lineut		Action
	Crain	input .		Statistics
	Src. Address			G Actions
	Sro Address List			Reset Counters
	Det Address List			Reset All Counters
	Dat. Address List			
	Protocol	6 (tcp)		
	Src. Port	+		
	Dst. Port	22	-	
	Any. Port	+		
	In. Interface	+		
	Out. Interface	+		
	In. Interface List	+		
	Out. Interface List	+		
	Dacket Mark			
	Connection Mark			
	Pouting Mark			
	Routing mark			
	Connection Type	+		
	Connection State	invalid established related 💟 new	-	
		untracked		
	Connection NAT State	•		
	~ Advanced			_
	~ Extra			
	 Action 			
	Action	add src to address list	*	
	Log			
	Log Prefix			
	Address List	ssh_stage1	~	
	Timeout	00:05:00	~	
	v Statistics			_
	Canaal			Analy Collins
	Cancel			Арріу

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.

V4 Firewall ~ Filter Rules N	Y4 Filter Rules	New		o x
🗅 New 🕟 Enable 🕕 Disable				
# ^ P Action # 0 * add src to addr	Enabled	0		General
	Comment	(Advanced
	∧ General			Action
	Chain	input		Statistics
	Src. Address	+		Statistics
	Dst. Address	+		
	Src. Address List	ssh_stage1		Reset Counters
	Dst. Address List	+		Reset All Counters
	Protocol	6 (tcp) ~		
	Src. Port	+		
	Dst. Port	22	-	
	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 rew	-	
	Connection NAT State	+		
	 Advanced 			
	~ Extra			
	~ Action			
	Action	add src to address list	-	
	Log			
	Log Prefix	•		
	Address List	ssh_stage2		
	Timeout	00:10:00		
	 Statistics 			
	Cancel		-	Apply OK

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

8 FIL	ewa	311		Filter Rules NAT Mai	ngle Raw	Service Por	ts Connec	tions Addres	ISLISTS	Layer / Prot	tocols							
CS Ne	w	0	E	nable 🕕 Disable 😣 Ren	iove									Q, Fin	d Y Filt	ter ኁ a	I ~ 🛛	Actions
#		· F	P	Action	Chain	Src. Addre	Dst. Addre	Src. Address	Dst. A	Protocol	Src. Port	Dst. Port	In. In	Out. In	In. Int_	Out. In	Byte ≡	P Actions
	0	1		😢 add src to address list	input					6 (tcp)		22						Reset Counters
1	1			2 add src to address list	input			ssh_stage1		6 (tcp)		22						Reset All Counters
4 Fir	rew	all	~	Filter Rules NAT Ma	ngle Raw	Service Por	rts Connec	tions Addres	ss Lists	Layer7 Prot	tocols							0
Fir	rew ew	all		Filter Rules NAT Ma	ngle Raw	Service Por	rts Connec	tions Addres	ss Lists	Layer7 Pro	tocols			Q. Fin	id 🍸 Fil	iter V e a	nı ~ 🖸	0
Fir	ew	all		Filter Rules NAT Ma Enable III Disable 😢 Ren Action	ngle Raw nove Chain	Service Por	rts Connec	Src. Address	ss Lists . Dst. A	Layer7 Prot	tocols Src. Port	Dst. Port	in. in	Q. Fin Out. In	id ⊽ Fil . In. Int	ter ≌a Out. In	all ~ □ . Byte =	€ Actions
Fir C ¹ No #	ew ew			Filter Rules NAT Ma Enable 11 Disable 28 Rer Action 12 add src to address list	ngle Raw nove Chain input	Service Por	Dst. Addre	Src. Address ssh_stage1	ss Lists . Dst. A	Layer7 Prot Protocol 6 (tcp)	tocols Src. Port	Dst. Port 22	in. in	Q. Fin Out. In	id ⊽ Fil	ter ∿≣a Out.in	ell × □ . Byte ≡	Actions Reset Counters

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

VH Firewall V Filter Rules N	VH Filter Rules	22		c x
🗅 New 🕞 Enable 🕕 Disable				
🛢 # ^ P Action	Fashlad	-		General
🗌 🖩 0 🔮 add src to addr	Enabled	0		Advanced
II 1 2 add src to addr	Comment			Extra
I 2 2 add src to addr	∽ General			Action
	Chain	input	<u> </u>	Statistics
	Src. Address	+		
	Dst. Address	•		
	Src. Address List	ssh_stage2		Reset Counters
	Dst. Address List	•		Reset All Counters
	Protocol	6 (tcp)		
	Src. Port	•		
	Dst. Port	22	-	
	Any. Port	+		
	In. Interface	+		
	Out. Interface	•		
	In. Interface List			
	Out. Interface List	•		
	Packet Mark			
	Connection Mark			
	Connection Mark			
	Routing mark			
	Connection Type	•		
	Connection State	invalid established related I new		
		untracked		
	Connection NAT State			
	Advant			
	 Advanced Extra 			
	^ Action			
	Action	add src to address list		
	Log			
	Log Prefix	•		
	Address List	ssh_blacklist	~	
	Timeout	10d 00:00:00	~	
	 Statistics 			
	D Cancel			Apply ОК

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

<u>∨4</u> F	ire	wa	ill (Filter Rules NAT	Mangle	Raw	Service Por	rts Connec	tions Addres	s Lists	Layer7 Pro	tocols							c ×
1	New	N	Ø	Enable 🕕 Disable 🚺	Remove										Q Fin	d 🍸 Fil	ter Si a		Antions
	#	^	P	Action	Cł	nain	Src. Addre	Dst. Addre	Src. Address	Dst. A	Protocol	Src. Port	Dst. Port	In. In	Out. In	In. Int	Out. In.	Byte ≡	P Actions
	1	0		2 add src to addres	is list ing	out			ssh_stage2		6 (tcp)		22						Reset Counters
0	1	1		t add src to addres	s list ing	but			ssh_stage1		6 (tcp)		22						Reset All Counters
0	H.	2		t add src to addres	s list ing	out					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.

VY Filter Rules N	VH Filter Rules	New	¢	e x
🗅 New 🕟 Enable 🕕 Disable				
	Enabled			General
III 0 2 add src to addr	Comment	9		Advanced
II 1 2 add src to addr	Comment			Extra
□ II 2 2 add src to addr	∧ General			Action
	Chain	input	<u>ب</u>	Statistics
	Src. Address	+		
	Dst. Address	+		
	Src. Address List	ssh_blacklist	v =	Reset Counters
	Dst. Address List	+		Reset All Counters
	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 Type			
	Connection State			
	Connection NAT State	•		
	 Advanced 			
	~ Extra			
	 Action 	Constant		
	Action	drop	~	
	log			
	Log Brofin			
	Log Frenx			
	v Statistics			
	Oracial			
	Cancel			Арріу

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

<u>v4</u>	Fire	wa		Filter Rules NAT Ma	ngle Raw	Service Por	ts Connec	tions Addres	s Lists	Layer7 Prof	tocols							o x
	Nev	w	0	Enable 🕕 Disable 😣 Ren	nove									Q, Fin	d 🍸 Filt	er 😼 al	I ~ 🔲	C Actions
	#	^	P	Action	Chain	Src. Addre	Dst. Addre	Src. Address	Dst. A	Protocol	Src. Port	Dst. Port	In. In	Out. In	In. Int	Out. In	Byte ≡	Preset Counters
	H	0		× drop	input			ssh_blacklist										Reset All Counters
	Ш	1		🔁 add src to address list	input			ssh_stage2		6 (tcp)		22						Reset All Counters
	=	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

<u>∨</u> ⁴ Addre	ess List				ø	×
Ct New	Enable 🕕 Disable 🗙	Remove		Q Find	Y	Filter
• P	Address	Network	Interface ~			≡
D	₽ 192.168.3.254/24	192.168.3.0	ether1			
\bigcirc	₽ 10.10.100.1/24	10.10.100.0	bridge1			

Real PuTTY Configuration		? ×
Category: Session Logging Terminal Keyboard Bell Features Window Preatance Behaviour Translation Selection Colours Connection Data Proxy SSH Serial Telnet Rlogin SUPDUP	Basic options for your PuTTY ses Specify the destination you want to connect to Host Name (or IP address) 192.168.3.254 Connection type: SSH SSH Serial Other: Telnet Load, save or delete a stored session Saved Sessions Default Settings AT Samba AT poczta Radunix Bluerax Shentel mail gsliwinski wb.wi.zut.edu.pl Close window on exit: Always Never Only on cle	sion Port 22 Load Save Delete an exit
About Help	Open	Cancel

c) Zaobserwuj co się stało po pierwszym połączeniu

1 PI	ire	wall		Filte	Rules NAT M	langle R	taw Service	Ports Connec	ctions Addre	ess Lists	Layer7 Pro	tocols							o :
	lev	1	0	Enable	🕕 Disable 😣 R	emove									Q, Find	Y Filter	∑i all ∽		G Actions
4	#	^	P	Actio	n	Chain	Src. Addr	e Dst. Addre	Src. Address	Dst. A	Protocol	Src. Port	Dst. Port	In. In	In. Int	Out. In	Bytes	=	Peret Counters
		0		× dro	p.	input			ssh_blacklist								01	в	Reset All Counters
1	Ľ.	1		t ad	d src to address list	input			ssh_stage2		6 (tcp)		22				01	В	Reset All Counters
] I		2		t ad	d src to address list	input			ssh_stage1		6 (tcp)		22				01	В	
1		3		t ad	d src to address list	input					6 (tcp)		22				601	в	
<u>∨4</u> ∂	F	ire	ewa	all	 Filter R 	ules	NAT	langle	Raw Se	ervice	Ports	Conn	ections	Add	dress	Lists	Laye	er7	Protocols
상	F	ire Ne	ewa w	all D	- Filter R	ules Disat	NAT N	fangle emove	Raw Se	ervice	Ports	Conn	ections	Add	dress	Lists	Laye	er7 I	Protocols
** Ct	F	ire Vev	w	all D List	 Filter R Enable () 	ules Disat	NAT Note Report to the NAT Note Report to the National Na	fangle emove	Raw Se	ervice t	Ports	Conne	ections Time	Add	dress	Lists	Laye	er7 l	Protocols

d) Wykonaj kolejne połączenie i obserwuj reguły

<u>v4</u>	Fire	wal	II ~	Filter Rules NAT M	angle Raw	Service Por	ts Connec	tions Addres	s Lists	Layer7 Prot	tocols							
Ľ	New	N	0	inable 🕕 Disable 😣 Re										c	Find	Y Filter	∑i all ×	
	#	^	P	Action	Chain	Src. Addre	Dst. Addre	Src. Address	Dst. A	Protocol	Src. Port	Dst. Port	In. In		In. Int	Out. In	Bytes	=
	н	0		× drop	input			ssh_blacklist									0	в
	Ш	1		🔁 add src to address list	input			ssh_stage2		6 (tcp)		22					0	в
	н	2		🔁 add src to address list	input			ssh_stage1		6 (tcp)		22					60	в
	Ш	3		2 add src to address list	input					6 (tcp)		22					120	в

<u>∨4</u> ŏ	Firew	vall 👻	Filter Rule	es NAT	Mangle	Raw	Service Port	s Co	nnections	Addr	ess Lists	Laye	r7 Proto	cols
다	New	🕨 Ena	able 🔲 🛙	Disable 🗙	Remove									
	P	List	^	Address		Time	eout	Creatio	on Time					
\bigcirc	D	 ssh_s 	stage1	192.168.	3.1	00:00	4:08	2025	5 <mark>-02-22 1</mark> 9:	16:06				
\bigcirc	D	 ssh_s 	stage2	192.168.	3.1	00:0	9:08	2025	5 <mark>-02-22 1</mark> 9:	18:21				

e) Wykonaj kolejne połączenie i obserwuj reguły

<u>v4</u>	Fire	ewa	11	Filter Rules NAT Ma	ingle Raw	Service Por	ts Connec	tions Addres	s Lists	Layer7 Prof	tocols						
C	Ne	w	0	Enable 🕕 Disable 😣 Rer										Q. Find	Y Filter	∑≣ all ×	
	#	^	P	Action	Chain	Src. Addre	Dst. Addre	Src. Address	Dst. A	Protocol	Src. Port	Dst. Port	In. In	 In. Int	Out. In	Bytes	=
	=	0		× drop	input			ssh_blacklist								564	в
	н	1		🔁 add src to address list	input			ssh_stage2		6 (tcp)		22				60	в
		2		🔁 add src to address list	input			ssh_stage1		6 (tcp)		22				120	в
	Ш	3		🔁 add src to address list	input					6 (tcp)		22				180	в

<u>v4</u>	Firew	vall 🗸 I	Filter Rule	s NAT	Mangle	Raw	Service Port	s Conn	ections	Address	Lists	Layer7 Protocols
다	New	🕨 Ena	ble 🕕 Di	isable 🗙	Remove							
	\triangleright	List	^	Address		Time	eout	Creation	Time			
\bigcirc	D	ssh_b	lacklist	192.168.3	3.1	9d 2	3:57:41	2025-0	2-22 19:	20:08		
\bigcirc	D	ssh_s	tage1	192.168.3	3.1	00:0	2:41	2025-0	2-22 19:	16:06		
\bigcirc	D	ssh_s	tage2	192.168.3	3.1	00:0	7:41	2025-0	2-22 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 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".



18. Podobną regułę tworzymy dla ruchu w drugim kierunku

V ⁴ Mangle			New	C	e x
		DISABLED	DYNAMIC		
Enabled					General
Comment	-				Advanced
					Extra
General	famound				Action
Chain Chain	Torward	100 222			Statistics
Src. Address	10.10.	100.777			G Actions
Ste Address List	0.0.0.0	10			Reset Counters
Src. Address List					Reset All Counters
DSL. AUDIESS LISL					
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	+				
 Advanced Extra 					
^ Action					
Action	mark pack	et			
	-				
Log					
Log Prefix	+				
New Packet Mark	WIN2				-)
Passthrough	0				
v Statistics					
Cancel					Apply OK

<u>v4</u>	Fire	wall		Filter Rules	NAT	Mangle	Raw Serv	ice Ports C	onnections	Addre	ess Lists	Layer7	Protocols							0.0
C	New	1	C E	nable 🔘 Disab	ie 🛛	Remove										C	Find Y	Filter 5	all -	G Actions
0	#	^	P	Action	C	Chain	Src. Address	Dst. Addres	s Src. A	Dst. A	Prot	Src. Port	Dst. Port	In. Int	Out. In	In. Int	Out. In	Bytes	Packet:≡	Papet Counters
	Η	0		Ø mark packet	fo	orward	0.0.0.0/0	10.10.100										08		Reset Oburters
	Η	1		Ø mark packet	fo	orward	10.10.100	0.0.0.0/0										08		Reset All Counters

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.

🗑 тікготік	Workspace: <own></own>	~ (D) 2 Q					()
🚀 Quick Set	Classica in a	C					
🔶 WiFi	(A) Queue List	 Simple Queues 	Interface Queues	Queue Tree Q	ueue Types		c ×
Interfaces	C New 🕞 Er	able 🕕 Disable 🌘	3 Remove		Q. Find	Y Filter	
WireGuard	○ # ^ P	Name Target	Upload Max Limit	Download Max L	Packet Marks Total	Max Limit ≡	Reset Counters
Bridge							Reset All Counters
PPP		<u>Ch</u>	Simple Queues		New	C	e x
S Mesh					ABLED INVALID DYNAMIC		
YH IP >				-			General
<u>v6</u> IPv6 >			Enabled				Advanced
Ø MPLS >			Comment				Statistics
X. Routing		~ 0	eneral				Traffic
System			Name	Windows WIN2			Total
C/ Queues			Target	bridge1		- +	Total Statistics
-IXI Dot1X			Dst.	+			
Files	0.P. guoued .0.ps	ackata augu ad					SF Actions
	UB queued U pa	ickets queued		Target Upload	Target Downloa	d	Reset Counters
E Now Terminal			Max Limit	3M	3M		Reset All Counters
			Burst	^			Torch
P Tasla			Burst Limit	0	0		
			Burst Threshold	0	0		
Make Supout.rif			Burst Time	0	0		
			Time	*			
		^ A	dvanced				
			Packet Marks	WINZ			
				Target Upload	Target Downloa	d	
			Limit At	0	0		
			Priority	8	8		
			Bucket Size	0.100	0.100		
			Queue Type	default-small	 default-small 	~	
			Parent	none			
		~ S	tatistics				
		~ T	raffic				
		v 1	otal				
		•	otarstatistics				
		C	ancel				Apply OK
🕢 Queue List 👻	Simple Queues	Interface Queu	es Queue Tree	Queue Types			s x
Ct New D Enab	le M Disable R	Remove			Q. Find	Y Filter	
	me	Farget Lipica	d Max Limit Down	oad Max I Pa	acket Marks Total	/ax Limit =	G Actions
	Windows WIND	oridge1	ZL4	ZLA 144			Reset Counters
	WINDOWS WINZ	nuger	NIC	SIM W	111/2		Reset All Counters

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.

<u>(</u>	Que	ue	List	- Simple Queues	Interface G	Queues Qu	ueue Tre	e Queue Types				o	×
ᆣ	New	/	D	nable 🕕 Disable 🗙	Remove				Q Find	Y Filter	G Actions		
	#	^	Þ	Name	Target	Upload Ma	x Limit	Download Max L	Packet Marks	Total Ma≡	Poset Count	ore	
\bigcirc	H	0		🛋 Windows WIN2	bridge1		3M	3M	WIN2		Reset All Cou	untor	
											Reset All Cot	inter	15

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

Simple Queues		Windows WIN2	C
Enabled			
Comment			
General			
Name	Windows WIN2		
Target	bridge1	v	-
Dst.	+		
MaxLimit	Target Upload	Target Download	
Buret	SM	SIM	
Durst	-		
Burst Limit	0	0	
Durst Time	0	0	
Durschine		0	
Time	0		
Advanced			
Statistics			
Tranic	Target Upload	Target Download	
Rate	166.8 kbps	4.9 Mbps	
Packet Rate	345 p/s	437 p/s	
Byte Graph			
		10	0 Mbps
		8.0	Mbps
			mops
		4.0	Mbps
Mum	A.A.	V 2.0	Mbps
" wy yw	VW ·····	06	ps
2025-02-22 21:08:55	5 2025-02-22.21	:10:55 2025-02-22.21	:12:54
	Upload Downle	oad	
Packet Graph			
Packet Graph		1	000 p/s
Packet Graph		1	000 p/s
Packet Graph		1	000 p/s 00 p/s
Packet Graph		1 80 66	000 p/s 00 p/s 00 p/s
Packet Graph		1 80 60	000 p/s 00 p/s 00 p/s 00 p/s
Packet Graph		1 80 60 44 21	000 p/s 00 p/s 00 p/s 00 p/s 00 p/s
Packet Graph	Magan	1 80 60 61 21	000 p/s 00 p/s 00 p/s 00 p/s 00 p/s

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

NameWindows WIN2Targetbridge1Dst.+	• - +
Target bridge1 Dst. +	• - +
Dst. +	
Target Upload Target Downl	oad
Max Limit 3M 5M	
Burst ^	
Burst Limit 10M 10M	
Burst Threshold 3M 5M	
Burst Time 90 90	
Time 👻	

Kliknij Apply i przejdź na zakładkę Traffic – obserwuj transfer



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.