

MTCNA Lab 7

1



LABORATORIO



TAREA 1

- Mantén la configuración del Lab7 en R1
- Crea las reglas necesarias para *(serán 4 reglas)*:
- Aceptar el tráfico INPUT y FORWARD de las conexiones establecidas y relacionadas
- Denegar el tráfico INPUT y FORWARD de las conexiones inválidas



The screenshot shows the Mikrotik WinBox interface. On the left, the 'Firewall' tab is active, displaying a table of existing rules. The 'New Firewall Rule' dialog is open, showing the 'General' tab. The 'Chain' is set to 'forward'. The 'Action' is set to 'accept'. The 'Connection State' section shows 'established' and 'related' selected. The 'Firewall Rule' dialog is also open, showing the 'Action' set to 'accept'.

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...
0	✓ accept	forward							
1	✗ drop	input							
2	✗ drop	forward							

TAREA 2

- Proteger nuestro router de Internet
- Creamos una regla que bloquee todo el tráfico de INPUT desde la interfaz br-WAN

The screenshot shows the Mikrotik WinBox Firewall configuration interface. The 'New Firewall Rule' dialog box is open, and the 'Chain' is set to 'input' and the 'In. Interface' is set to 'br-WAN'. The 'Action' is set to 'drop'. The 'Log' checkbox is unchecked. The 'Log Prefix' field is empty. The 'OK' button is highlighted.

The 'New Firewall Rule' dialog box has the following fields:

- Chain: input
- Src. Address: [empty]
- Dst. Address: [empty]
- Protocol: [empty]
- Src. Port: [empty]
- Dst. Port: [empty]
- Any. Port: [empty]
- In. Interface: br-WAN
- Out. Interface: [empty]
- In. Interface List: [empty]
- Out. Interface List: [empty]
- Packet Mark: [empty]
- Connection Mark: [empty]
- Routing Mark: [empty]
- Routing Table: [empty]
- Connection Type: [empty]
- Connection State: [empty]
- Connection NAT State: [empty]

The 'Action' tab is selected, showing:

- Action: drop
- Log: [unchecked]
- Log Prefix: [empty]

The 'OK' button is highlighted.

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	In. Inter...	Out. Int...	Src. Ad...	Dst. Address
0	accept	input											
1	accept	forward											
2	drop	input											
3	drop	forward											

4 items (1 selected)

TAREA 3

- Proteger las LAN del router de Internet
- Creamos una regla que bloquee todo el tráfico de INPUT desde la interfaz br-WAN

The screenshot shows the Mikrotik WinBox Firewall configuration interface. The 'New Firewall Rule' dialog box is open, showing the 'General' tab. The 'Chain' is set to 'forward', the 'In. Interface' is set to 'br-WAN', and the 'Action' is set to 'drop'. The 'Connection State' is set to 'new'. The 'Log' checkbox is unchecked. The 'Log Prefix' is empty. The 'OK' button is highlighted.

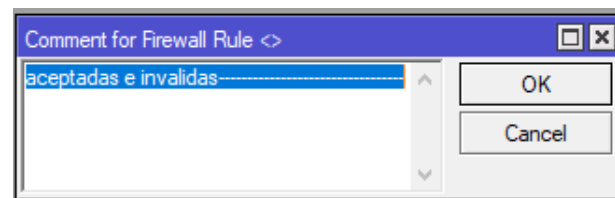
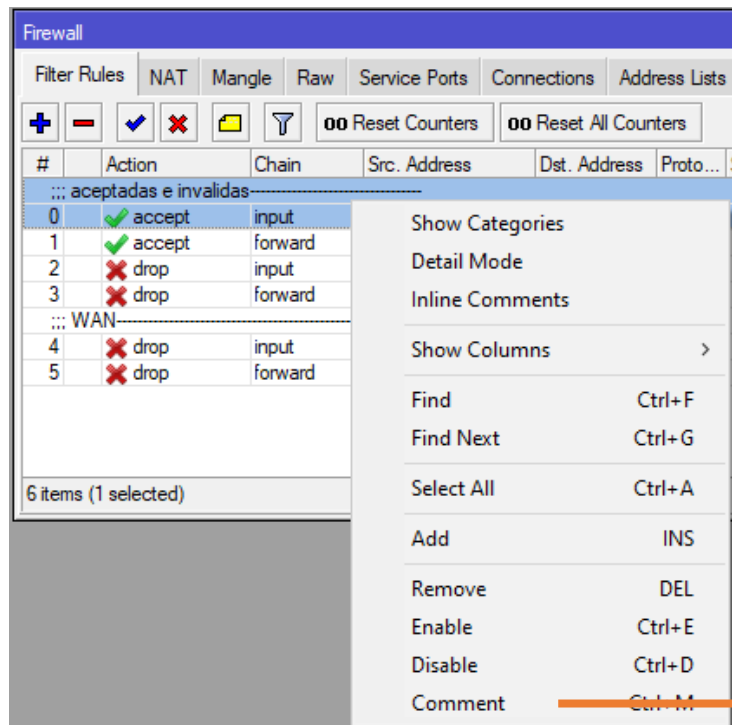
Below the dialog box, the 'Filter Rules' table is visible, showing a list of rules. The rule with ID 4 is selected, which is a 'drop' rule for the 'input' chain on the 'br-WAN' interface.

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...
0	accept	input							
1	accept	forward							
2	drop	input							
3	drop	forward							
4	drop	input						br-WAN	

5 items (1 selected)

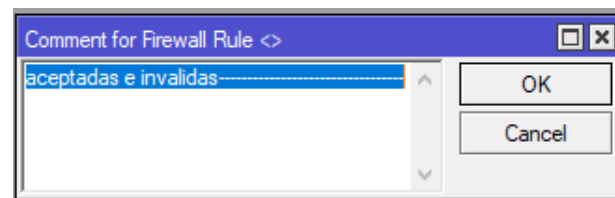
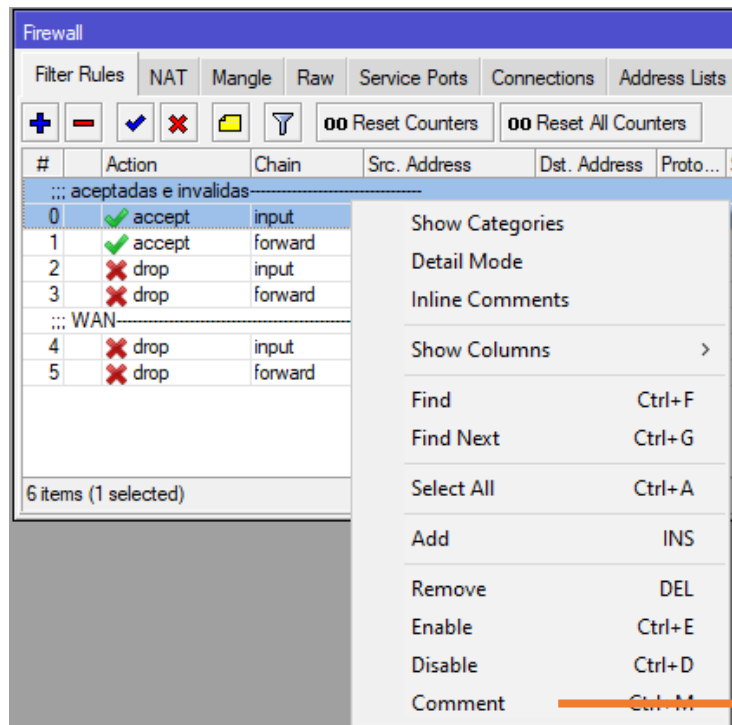
TAREA 4

- Pongamos un poquito de orden ;)
 - Hacemos click con botón derecho en la primera regla de firewall / filter y pinchamos Comment
 - Comentamos esta regla como: aceptadas e inválidas-----
 - Hacemos lo mismo con la regla de drop INPUT en br-WAN y la comentamos como WAN-----



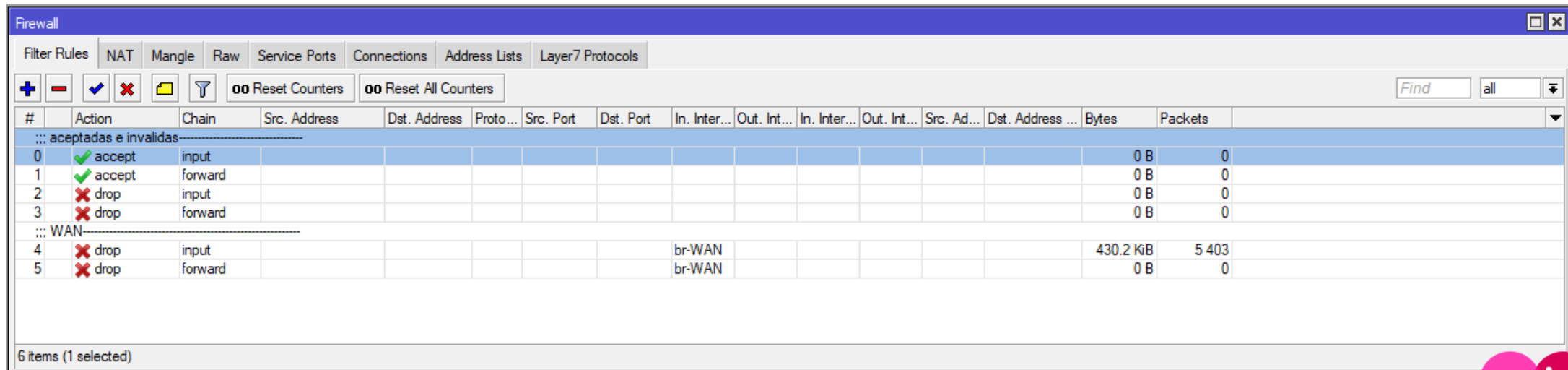
TAREA 4

- Pongamos un poquito de orden ;)
 - Hacemos click con botón derecho en la primera regla de firewall / filter y pinchamos Comment
 - Comentamos esta regla como: aceptadas e inválidas-----
 - Hacemos lo mismo con la regla de drop INPUT en br-WAN y la comentamos como WAN-----



CONCLUSIONES

- Si estabas accediendo a R1 por una interfaz conectada por el br-WAN antes de añadir estas reglas seguirás conectado, pregúntate por qué.
- Reinicia R1 y comprueba si puedes conectarte por br-WAN. Recuerda que puedes conectar por IP y po MAC (*solo podrás conectarte por MAC*)

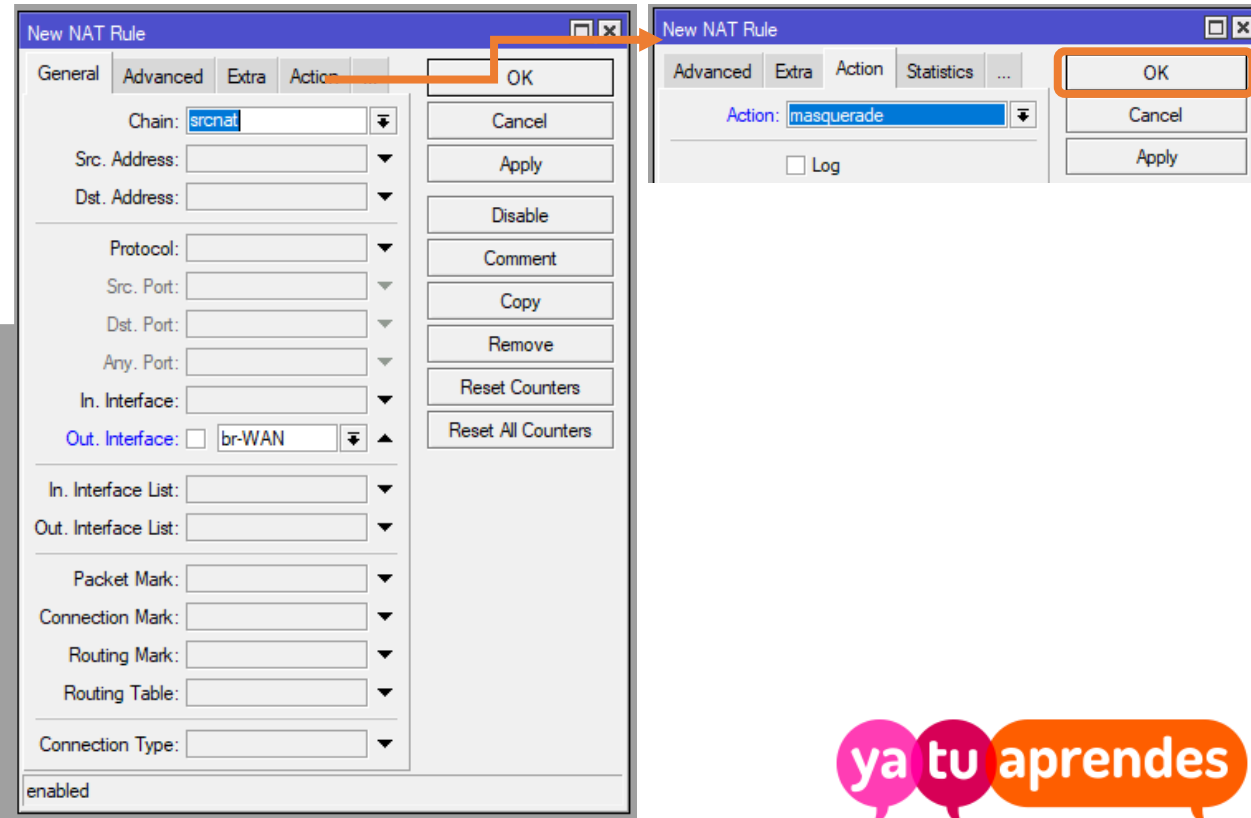
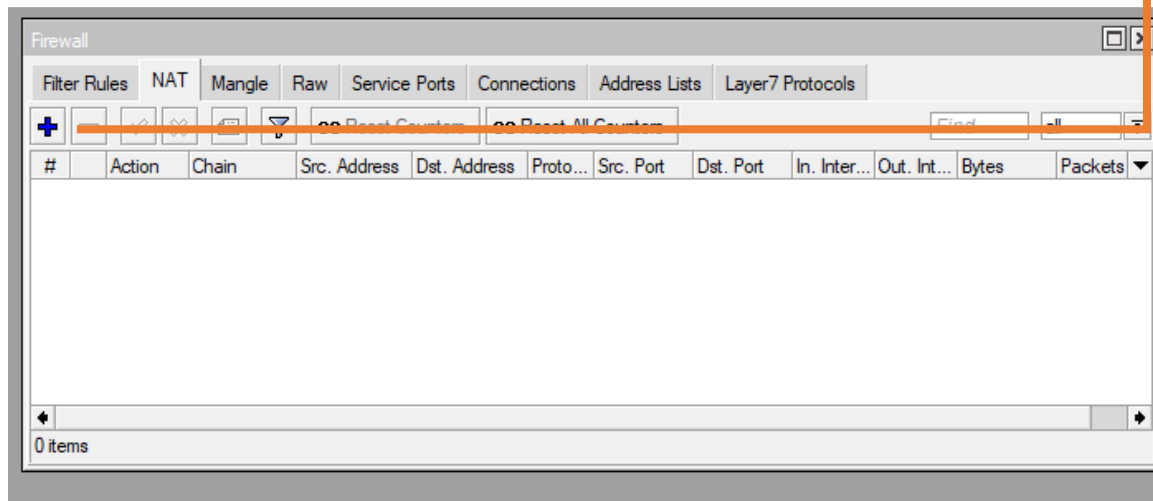


#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	In. Inter...	Out. Int...	Src. Ad...	Dst. Address ...	Bytes	Packets
::: aceptadas e invalidas															
0	✓ accept	input												0 B	0
1	✓ accept	forward												0 B	0
2	✗ drop	input												0 B	0
3	✗ drop	forward												0 B	0
::: WAN															
4	✗ drop	input						br-WAN						430.2 KiB	5 403
5	✗ drop	forward						br-WAN						0 B	0

6 items (1 selected)

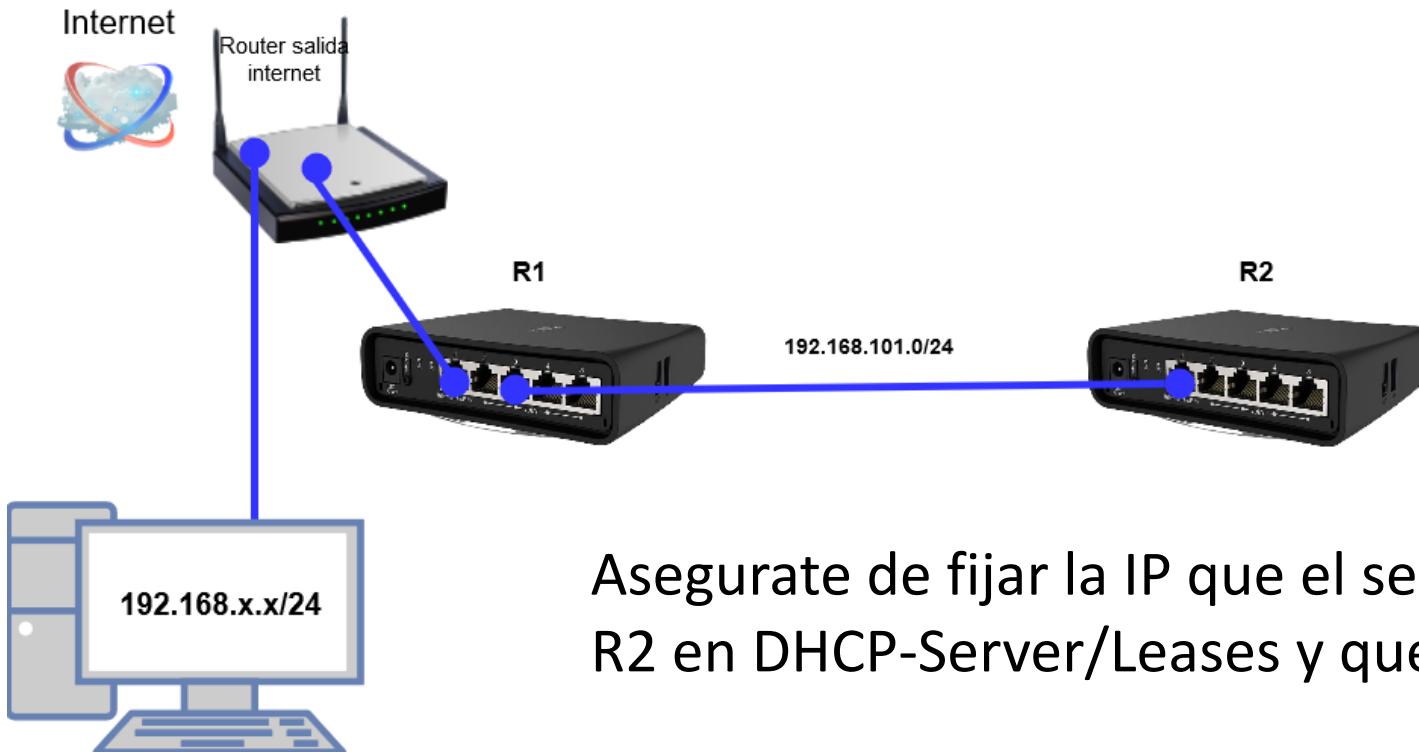
TAREA 5

- Recuerda que en el tema 5 ya habíamos configurado un masquerade en br-WAN:
- *(así que ya tenemos trabajo adelantado ;)*
 - En IP / Firewall creamos una regla con los siguiente parámetros en *General* y *Accion*.
- Por terminal sería así
`ip firewall nat add action=masquerade chain=srcnat out-interface=br-WAN`



TAREA 6

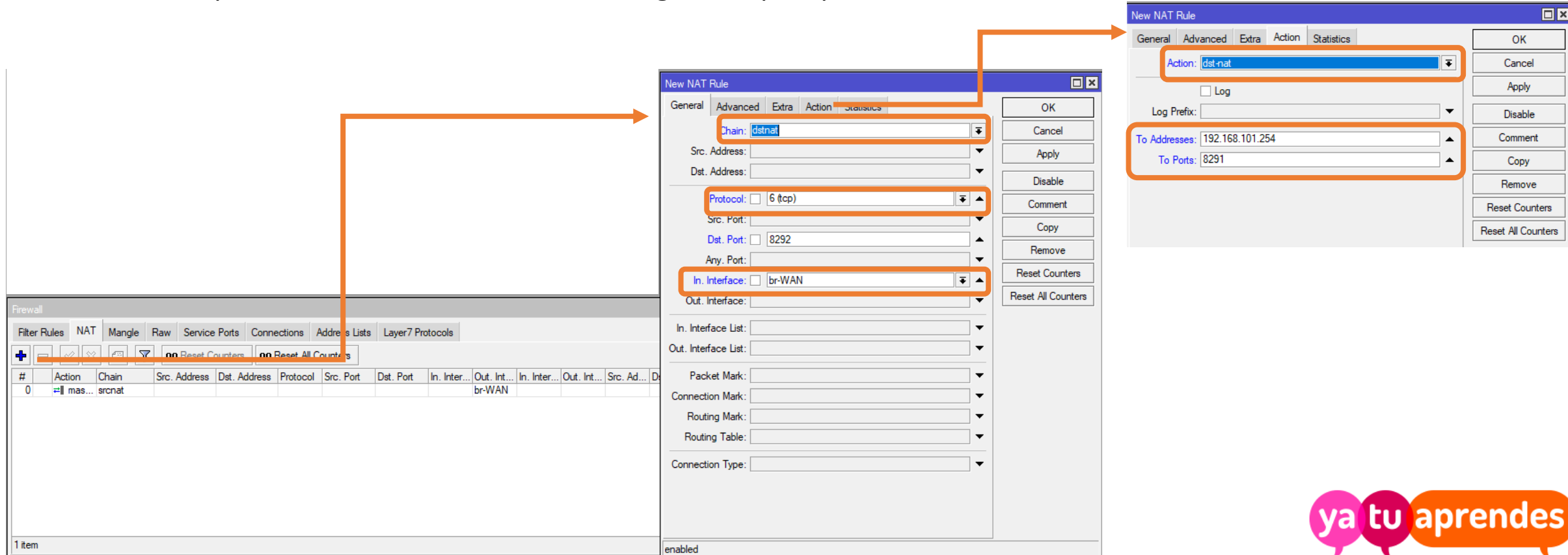
Vamos a retomar la confi de R2 que habíamos hecho en la tarea 2 del Lab5
Utilizaremos este esquema para interconectar los routers y el PC



Asegurate de fijar la IP que el servidor DHCP de R1 le ha ofrecido a R2 en DHCP-Server/Leases y que haces PING de R1 a R2:

TAREA 7

- Vamos a hacer una regla NAT para acceder a R2 desde la red del router de internet:
- utilizaremos el puerto de escucha 8292 en R1. Preguntate por qué



The screenshot shows the Mikrotik WinBox interface with the 'New NAT Rule' dialog box open. The dialog has several tabs: General, Advanced, Extra, Action, and Statistics. The 'General' tab is active. The following fields are highlighted with orange boxes:

- Chain:** dstnat
- Protocol:** 6 (tcp)
- Dst. Port:** 8292
- In. Interface:** br-WAN
- Action:** dst-nat
- To Addresses:** 192.168.101.254
- To Ports:** 8291

The 'Log' checkbox is unchecked. The 'Log Prefix' field is empty. The 'OK' button is highlighted. The background shows the Firewall tab in WinBox with a table of rules. The table has columns for #, Action, Chain, Src. Address, Dst. Address, Protocol, Src. Port, Dst. Port, In. Interface, Out. Interface, In. Interface, Out. Interface, Src. Address, and Dst. Address. The first row shows a rule with Action 'srcnat', Chain 'srcnat', and Out. Interface 'br-WAN'.

TAREA 8

- Si has intentado acceder a R2 desde la red del router de internet habrás comprobado que no funciona.
- Recuerda que habíamos creado una ruta que “Dropeaba” todas las conexiones new. En FORWARD.
- Podemos crear una regla que permita FORWARD al puerto 8292 desde br-WAN o podemos modificar la regla de drop FORWARD que ya teníamos. *(o una o la otra).*

TAREA 8

- Crear una nueva regla de firewall
- Recuerda que la tendrás que poner “antes” de la regla que “dropea” el tráfico

New Firewall Rule

General Advanced Extra Action Statistics

Chain: forward

Src. Address:

Dst. Address:

Protocol: 6 (tcp)

Src. Port:

Dst. Port: 8292

Any. Port:

In. Interface: br-WAN

Out. Interface:

In. Interface List:

Out. Interface List:

Packet Mark:

Connection Mark:

Routing Mark:

Routing Table:

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

New Firewall Rule

General Advanced Extra Action Statistics

Action: accept

Log

Log Prefix:

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

Firewall

Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols

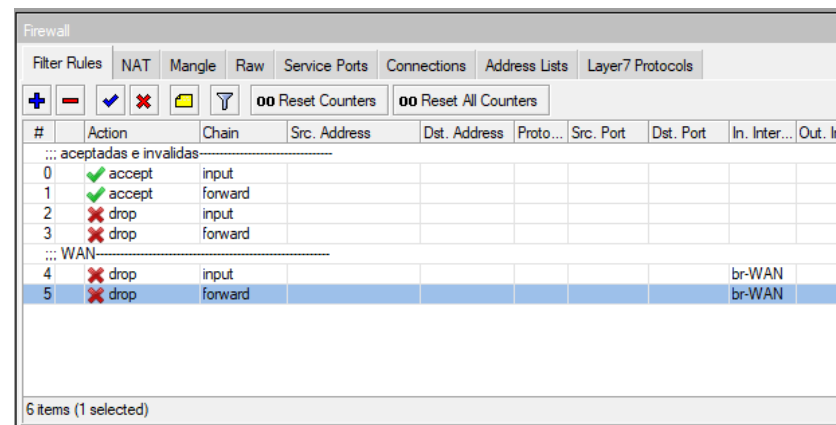
00 Reset Counters 00 Reset All Counters Find all

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	In. Inter...	Out. Int...	Src. Ad...	Dst. Address ...	Bytes	Packets
::: aceptadas e invalidas															
0	accept	input												0 B	0
1	accept	forward												0 B	0
2	drop	input												0 B	0
3	drop	forward												0 B	0
::: WAN															
4	drop	input						br-WAN						1212.2 KiB	16 181
5	accept	forward			6 (tcp)		8292	br-WAN						0 B	0
6	drop	forward						br-WAN						0 B	0

7 items (1 selected)

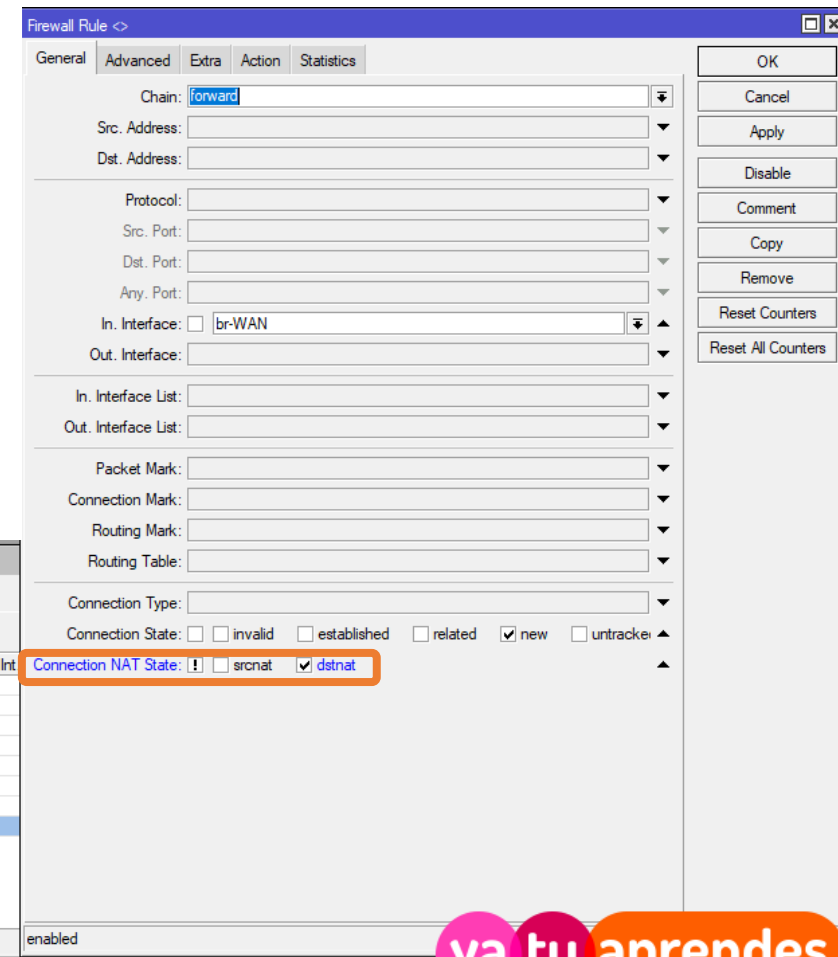
TAREA 8

- Podemos modificar la regla de “dropear” las conexiones nuevas en FORWARD de br-WAN
- Si añadimos en Connection NAT State la inversa de dstnat que estamos haciendo???, Le decimos que la condición es la siguiente:
 - *Para todas las conexiones nuevas de la cadena FORWARD que entren por la interfaz br-WAN y que no cumplan con una regla que exista en dstnat, las “dropeas”*



#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...
... aceptadas e invalidas									
0	✓ accept	input							
1	✓ accept	forward							
2	✗ drop	input							
3	✗ drop	forward							
... WAN									
4	✗ drop	input						br-WAN	
5	✗ drop	forward						br-WAN	

6 items (1 selected)



Firewall Rule <>

General Advanced Extra Action Statistics

Chain: **forward**

Src. Address:

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

In. Interface: ☐ br-WAN

Out. Interface:

In. Interface List:

Out. Interface List:

Packet Mark:

Connection Mark:

Routing Mark:

Routing Table:

Connection Type:

Connection State: ☐ invalid ☐ established ☐ related ☒ new ☐ untracked

Connection NAT State: ☐ srcnat ☒ dstnat

enabled

CONCLUSIONES

- Si configuramos una nueva regla para permitir el tráfico del puerto 8292, solo afectará a ese tráfico en concreto
- Si modificamos la regla de FORWARD afectará a TODAS las reglas de dstnat que hagamos en firewall/NAT

Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols																	
+ - ✓ ✗ 📁 🔍 00 Reset Counters 00 Reset All Counters Find all ▼																	
#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	In. Inter...	Out. Int...	Connection State	Connection NAT ...	Src. Ad...	Dst. Address ...	Bytes	Packets
... aceptadas e invalidas																	
0	✓ accept	input										established related				0 B	0
1	✓ accept	forward										established related				0 B	0
2	✗ drop	input										invalid				0 B	0
3	✗ drop	forward										invalid				0 B	0
... WAN																	
4	✗ drop	input							br-WAN							1619.8 KiB	21 306
5	✗ drop	forward							br-WAN			new	!dstnat			0 B	0