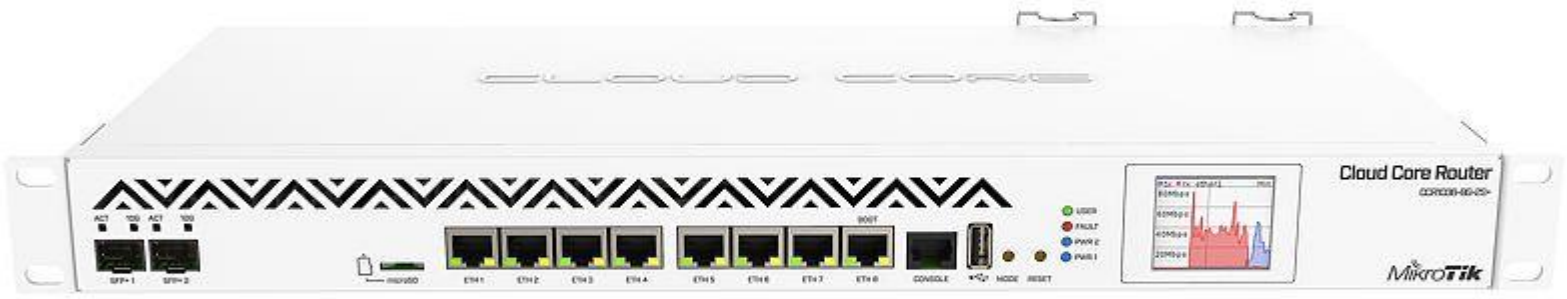
MTCNA Lab 7

LABORATORIO

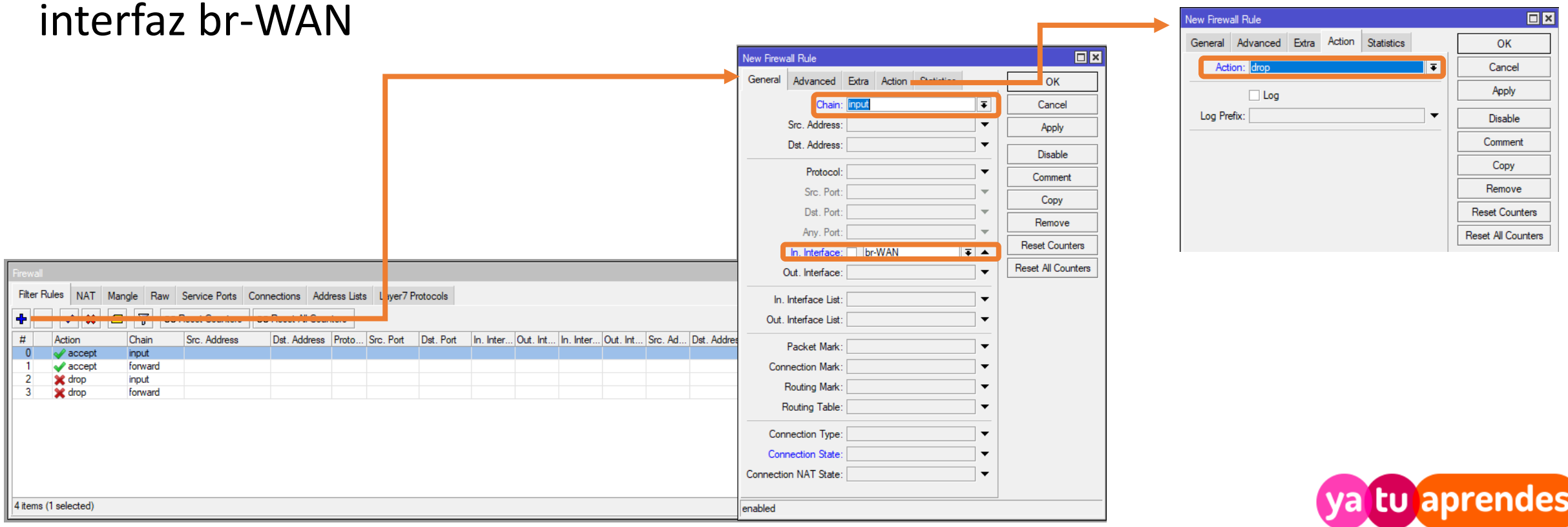


TAREA 1

- 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

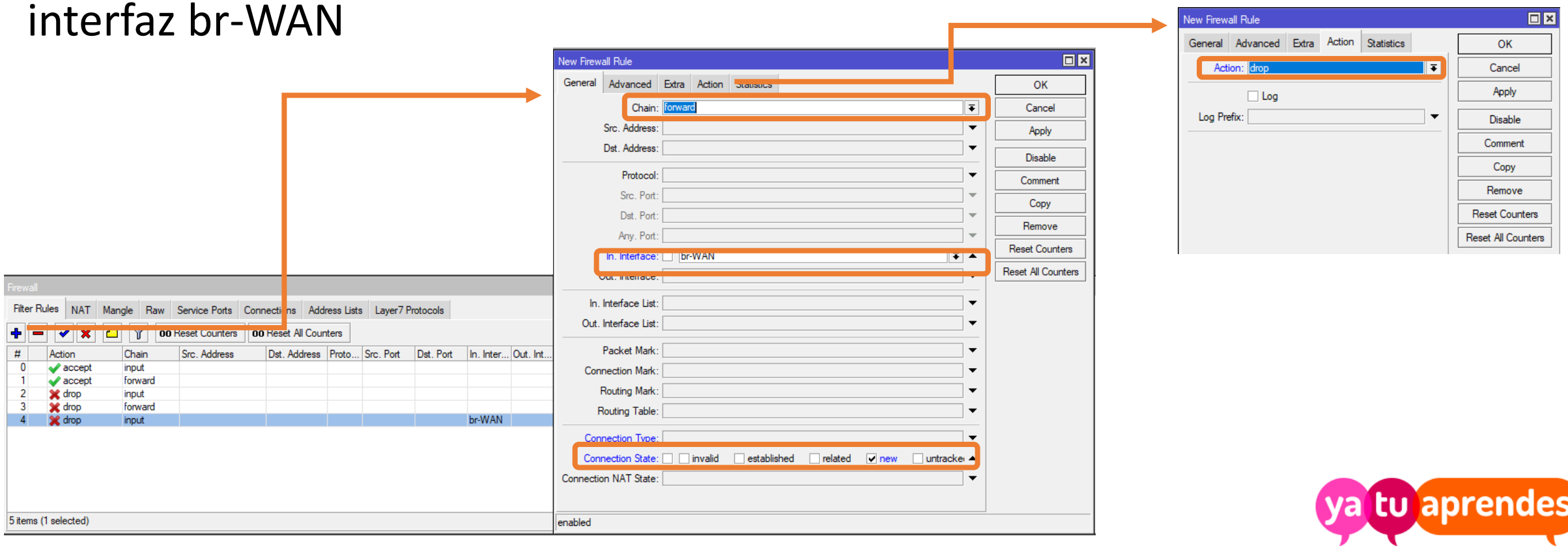
TAREA 2

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



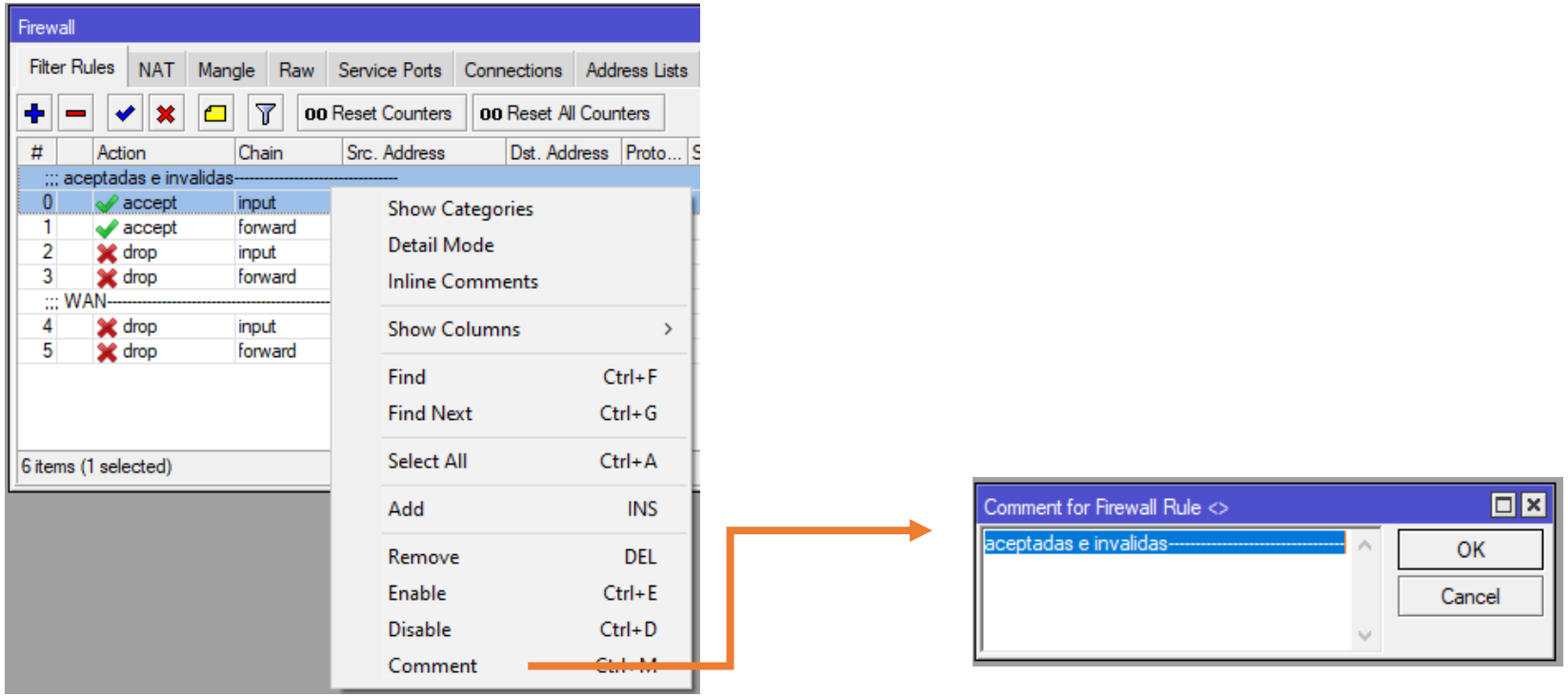
TAREA 3

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



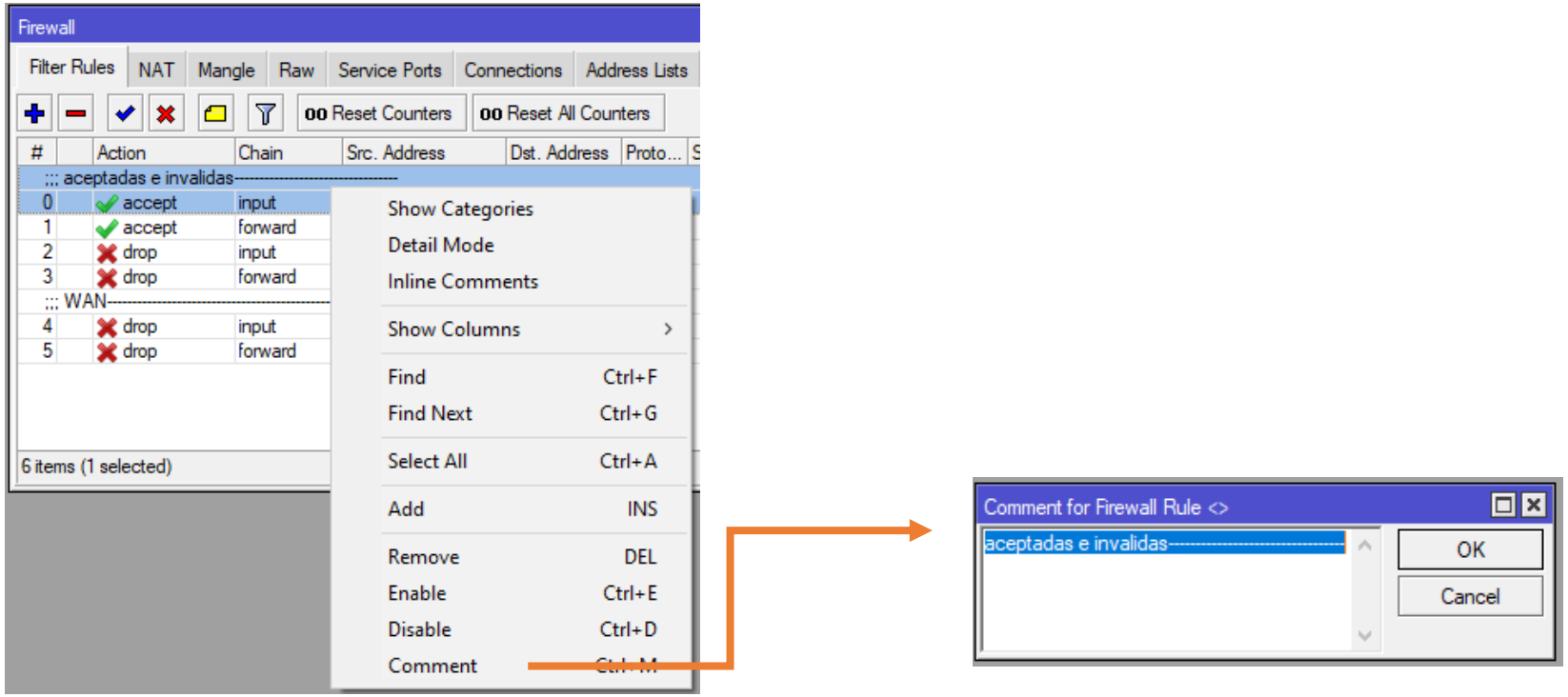
TAREA 4

- 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------*



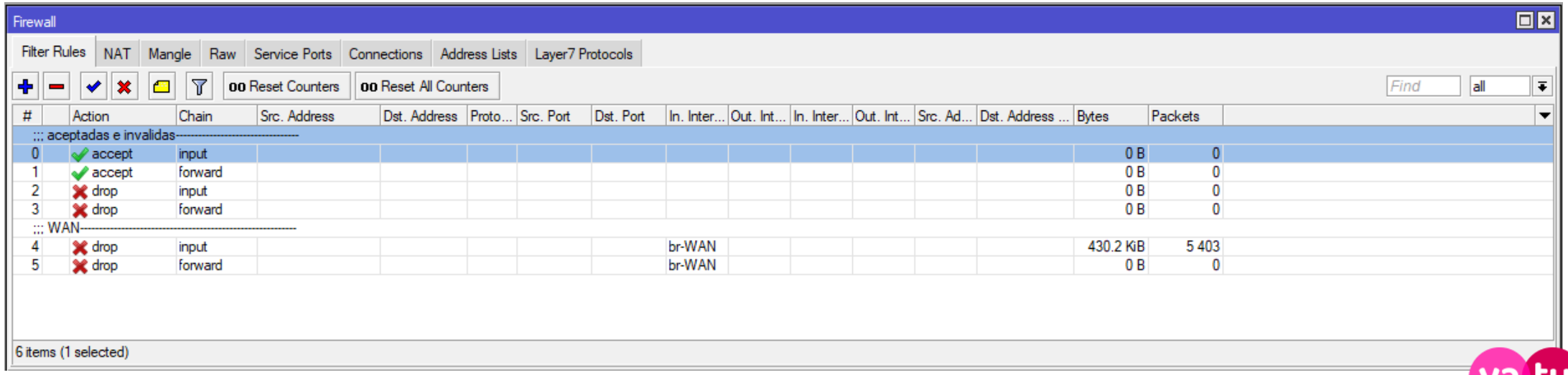
TAREA 4

- 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

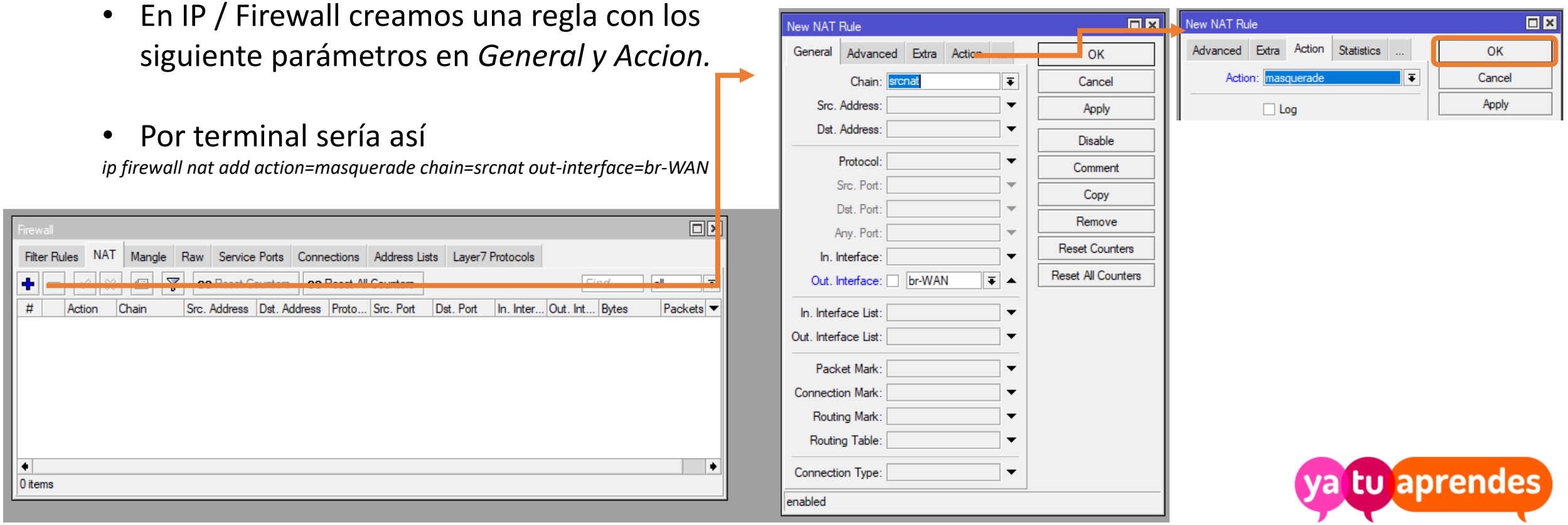
- Si estabas accediendo a R1 por una interfaz conectada por el br-WAN antes de añadir estas reglas seguirás conectado, pregúntate por qué.
- Reinicia R1 y comprueba si puedes conectarte por br-WAN. Recuerda que puedes conectar por IP y po MAC *(solo podrás conectarte por MAC)*



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

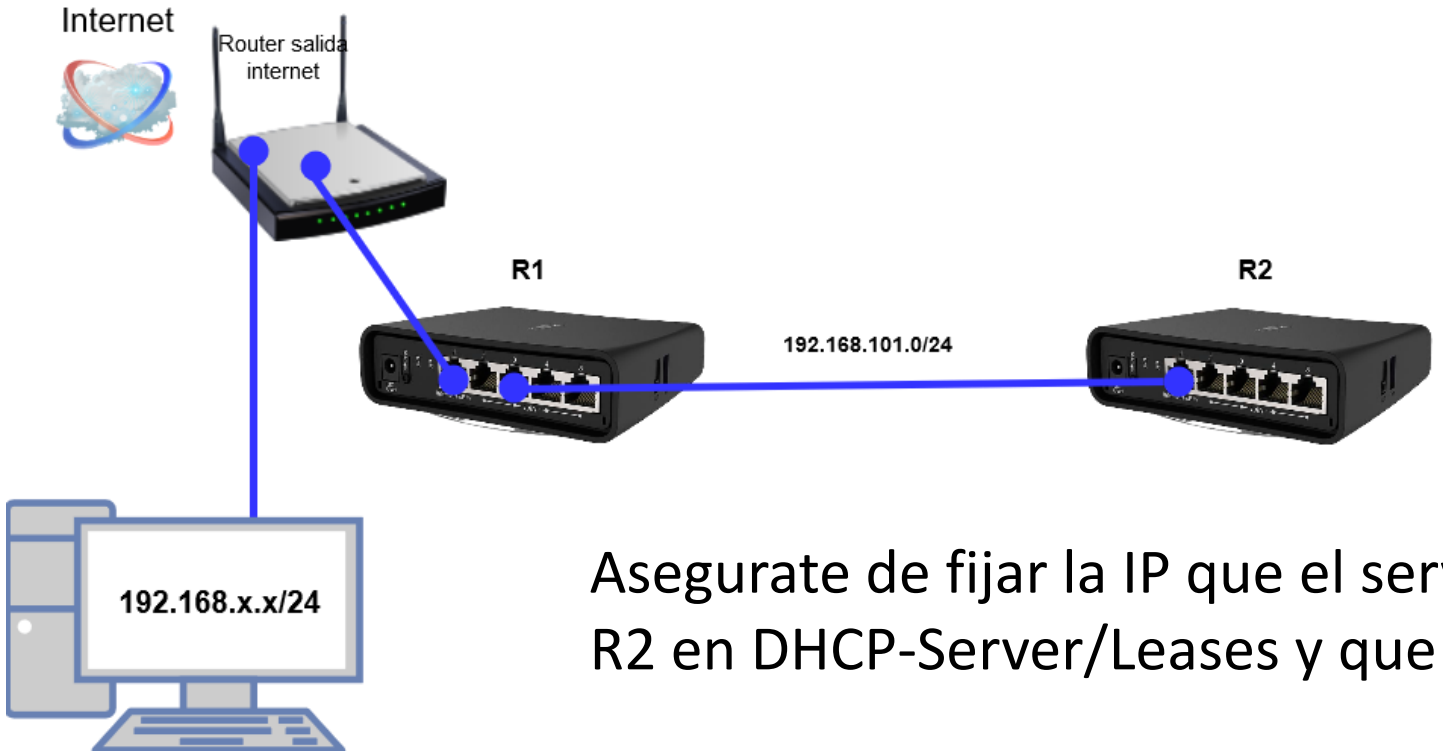
ip firewall nat add action=masquerade chain=srcnat out-interface=br-WAN



TAREA 6

Vamos a retomar la confi de R2 que habíamos hecho en la tarea 2 del Lab5

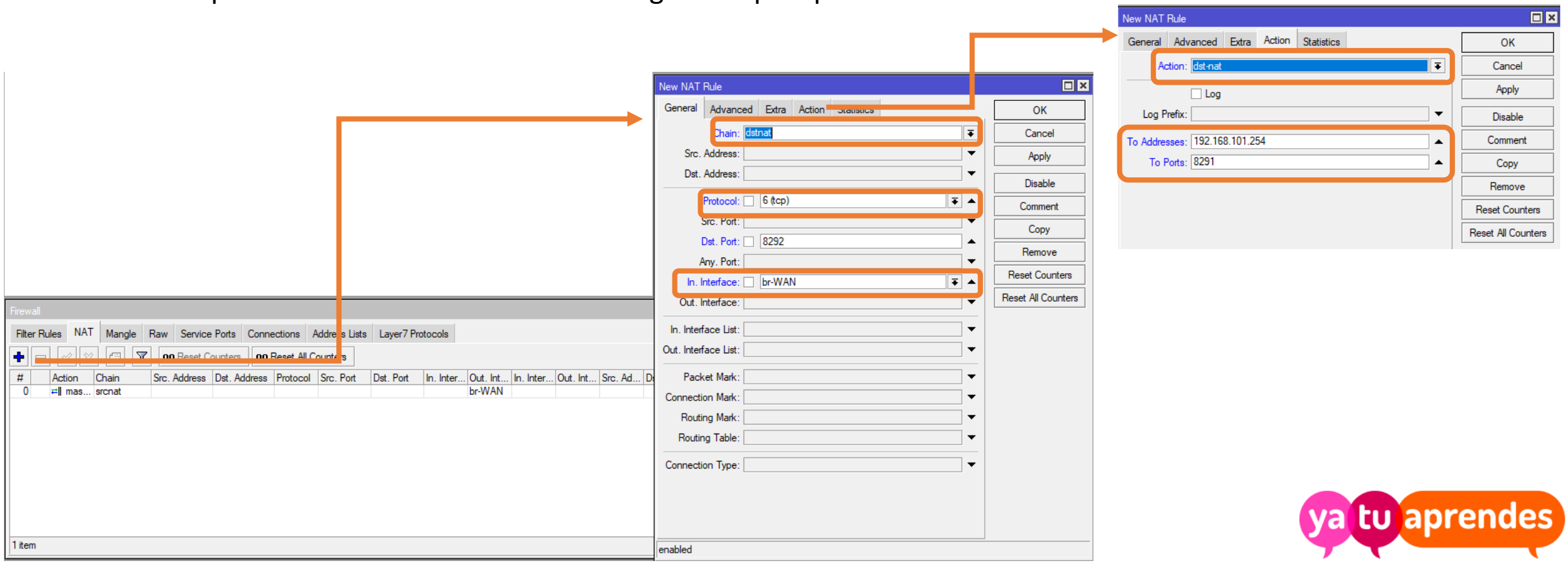
Utilizaremos este esquema para interconectar los routers y el PC



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

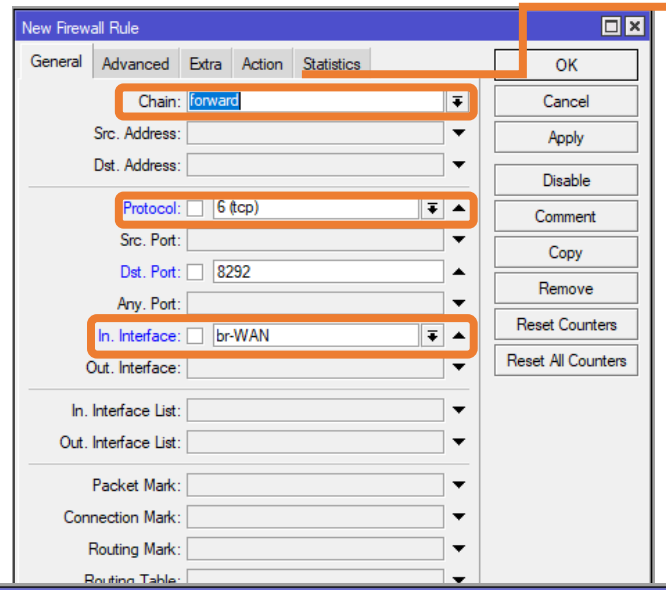


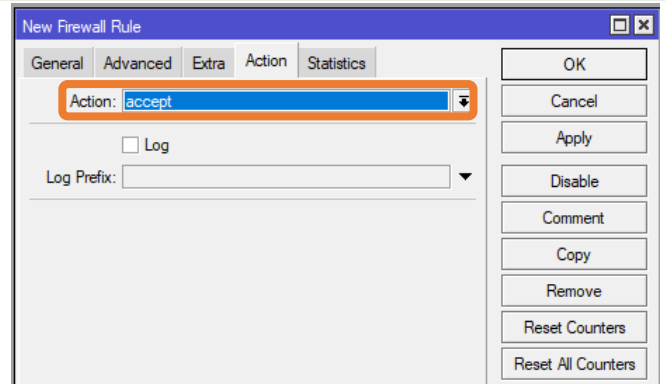
TAREA 8

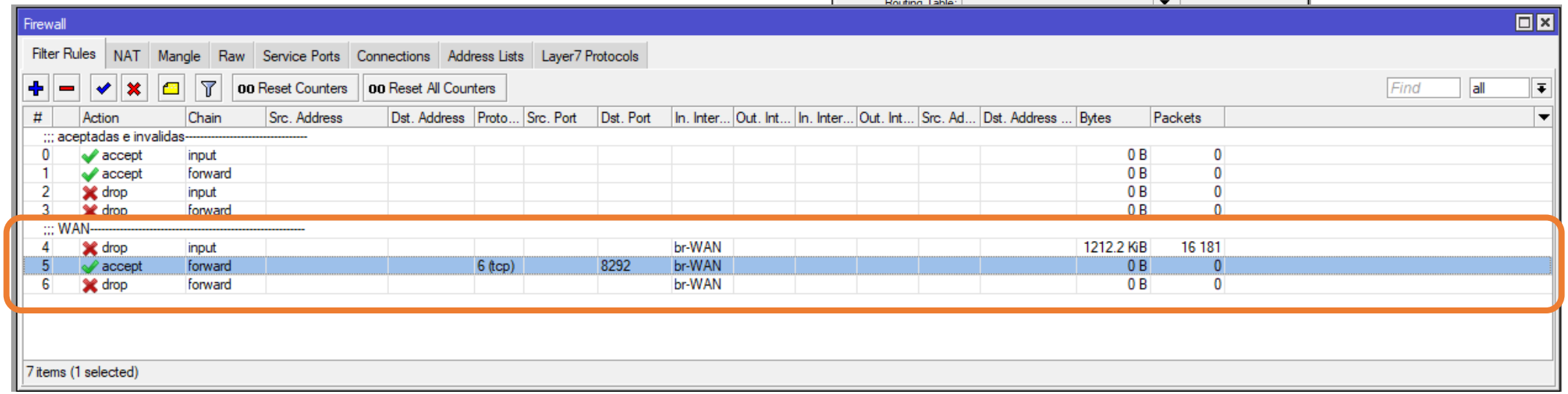
- Si has intentado acceder a R2 desde la red del router de internet habrás comprobado que no funciona.
- Recuerda que habíamos creado una ruta que “Dropeaba” todas las conexiones new. En FORWARD.
- Podemos crear una regla que permita FORWARD al puerto 8292 desde br-WAN o podemos modificar la regla de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

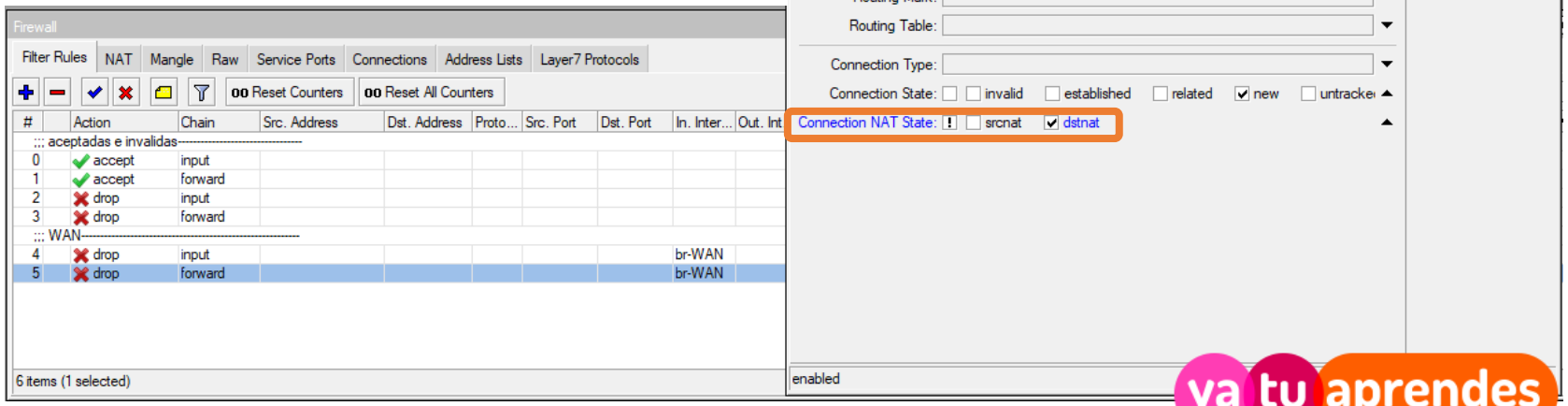






TAREA 8

- Podemos modificar la regla de “dropear” las conexiones nuevas en FORWARD de br-WAN
- Si añadimos en Conection 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”*



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