Fèlix Andrés Navarro 53324858W Sergio Jimenez Mansilla 21775216N

1.-

```
Password changed
[admin@MikroTik] > ip firewall filter print
Flags: X - disabled, I - invalid, D - dynamic
 0  D ;;; special dummy rule to show fasttrack counters
      chain=forward action=passthrough

 1    ;;; defconf: accept established,related,untracked
      chain=input action=accept connection-state=established,related,untracked

 2    ;;; defconf: drop invalid
      chain=input action=drop connection-state=invalid

 3    ;;; defconf: accept ICMP
      chain=input action=accept protocol=icmp

 4    ;;; defconf: accept to local loopback (for CAPsMAN)
      chain=input action=accept dst-address=127.0.0.1

 5    ;;; defconf: drop all not coming from LAN
      chain=input action=drop in-interface-list=!LAN

 6    ;;; defconf: accept in ipsec policy
      chain=forward action=accept ipsec-policy=in,ipsec

 7    ;;; defconf: accept out ipsec policy
      chain=forward action=accept ipsec-policy=out,ipsec

 8    ;;; defconf: fasttrack
      chain=forward action=fasttrack-connection connection-state=established,related

 9    ;;; defconf: accept established,related, untracked
      chain=forward action=accept connection-state=established,related,untracked

10    ;;; defconf: drop invalid
      chain=forward action=drop connection-state=invalid

11    ;;; defconf: drop all from WAN not DSTNATed
      chain=forward action=drop connection-state=new connection-nat-state=!dstnat in-interface-list=WAN
[admin@MikroTik] >
```

Al tallafocs les regles estan definides en dues cadenes principals: input i forward. La cadena input s'utilitza per controlar el trànsit destinat directament al propi router, és a dir, el trànsit que intenta arribar a les adreces IP de les interfícies del router. D'altra banda, la cadena forward maneja el trànsit que travessa el router, com el trànsit que va de la xarxa LAN a la WAN o viceversa.

Un paquet dirigit a la IP 192.168.88.1, que és una adreça IP local a la xarxa del router, passarà per la cadena input, ja que aquesta IP és pròpia del router i el paquet està destinat directament a ell. Les regles definides a la cadena input avaluaran si es permet o es bloqueja el trànsit entrant, depenent de les seves característiques i origen.

En aquest cas, la regla 5 del tallafocs, que bloqueja tot el trànsit entrant que no provingui de la xarxa LAN, afectaria el paquet si aquest no prové de la xarxa local. És a dir que si el paquet dirigit a 192.168.88.1 prové d'una interfície que no estigui a la llista LAN, serà bloquejat. Si el trànsit prové de la LAN, es permetrà segons les altres regles del tallafoc.

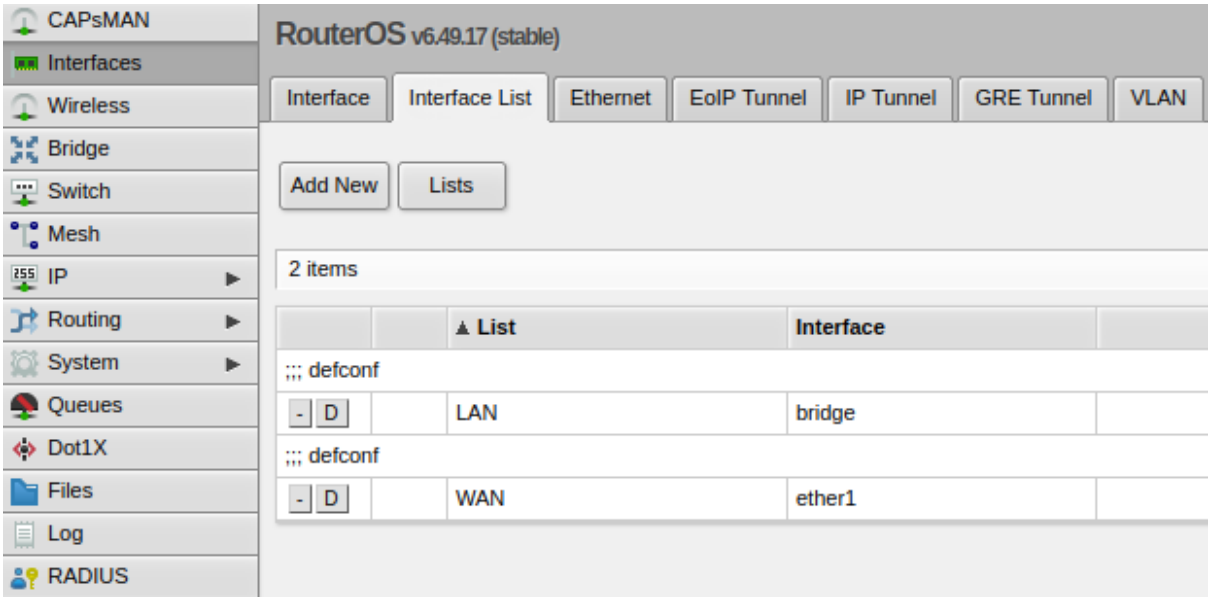
2.-

El paràmetre connection-state a les regles del tallafocs classifica els paquets segons l'estat de la seva connexió, permetent gestionar el trànsit de forma més eficient.

Connection-state=new identifica paquets que inicien una nova connexió i se sol utilitzar per decidir si es permet o bloqueja aquest trànsit inicial. D'altra banda, connection-state=established s'aplica a paquets que pertanyen a una connexió prèviament permesa, assegurant que el trànsit legítim i reconegut flueixi sense restriccions.

3.-
La interfície física ether1 s'associa amb la llista WAN. Aquesta interfície està configurada per connectar-vos al proveïdor d'Internet. La regla a la cadena forward que bloqueja paquets nous no destinats a NAT (regla 11) està dissenyada per protegir contra accessos no desitjats des de la xarxa externa.

Les interfícies físiques ether2, ether3, ether4 i ether5 s'agrupen sota un pont per defecte (bridge), que està vinculat a la llista LAN. Això permet gestionar de manera centralitzada el trànsit intern de la xarxa local. La regla a la cadena input que bloqueja trànsit que no prové de LAN (regla 5) assegura que només dispositius interns tinguin accés directe al router.



4.-
Sí, el router respon als pings en la configuració per defecte. Això es deu a la regla 3, aquesta regla permet paquets ICMP (usats per l'ordre ping) que arriben a qualsevol IP configurada en l'encaminador. Atès que aquesta regla està abans que altres regles restrictives, els pings dirigits a l'encaminador seran acceptats.

Si es canvia l'ordre de les regles, el router deixaria de respondre pings provinents de la WAN i probablement també des de la LAN, perquè la regla 5 bloquejaria el trànsit abans que pugui ser processat per la regla 3.

5.-

Des de LAN cap a Internet, les connexions estan permeses gràcies a les regles a la cadena forward, especialment la regla 9 (que accepta connexions establertes i relacionades) i la regla 8 (que aplica el fasttrack a connexions establertes). Això assegura que qualsevol

trànsit iniciat des de LAN pugui sortir cap a Internet i rebre respostes de manera eficient, sense ser bloquejat pel tallafoc.

D'altra banda, les connexions des d'Internet cap a LAN no es permeten per defecte. La regla 11 bloqueja tot el trànsit entrant des de la interfície WAN que no estigui específicament redirigit (mitjançant una regla de DSTNAT). Això vol dir que per permetre connexions des d'Internet a un dispositiu a la xarxa LAN, cal configurar prèviament un NAT que redirigeixi el trànsit cap a l'adreça interna desitjada. Sense aquest NAT, el trànsit des d'Internet serà bloquejat.

6.-

En aquest escenari, amb la configuració de regles mostrada al router MikroTik, sí que podria haver-hi paquets que passessin per les cadenes definides sense ser afectats per cap regla explícita. Això pot passar perquè les regles configurades no cobreixen tots els possibles casos de tràfic.

Per tal que aquesta configuració tingui sentit, la política per defecte del tallafocs és la clau. En els routers MikroTik, la política per defecte és acceptar el tràfic si cap regla l'afecta. Això significa que qualsevol paquet que no coincideixi amb cap regla definida serà permès per defecte.

Això comporta que, per garantir la seguretat, és imprescindible assegurar-se que totes les situacions no desitjades estan explícitament bloquejades a través de regles específiques al tallafocs, ja que la política per defecte no protegeix contra el tràfic no autoritzat. En aquest cas concret, per exemple, la regla 11 bloqueja tràfic des de WAN que no està destinat a NAT, però podria faltar una regla genèrica per bloquejar altres casos

7.-

Permet trànsit TCP des de la xarxa 10.1.1.208/28 cap a qualsevol destinació amb els ports 80 (HTTP) i 443 (HTTPS).
Ús: Habilitar accés a serveis web externs des d'aquesta xarxa.
10 chain=forward action=accept protocol=tcp src-address=10.1.1.208/28 dst-port=80,443 log=no log-prefix=""

Permet trànsit TCP cap a la xarxa 10.1.1.208/28 des de qualsevol origen que utilitzi els ports 80 (HTTP) i 443 (HTTPS).
Ús: Habilitar el retorn de trànsit web a la xarxa 10.1.1.208/28.

11 chain=forward action=accept protocol=tcp dst-address=10.1.1.208/28 src-port=80,443 log=no log-prefix=""

Permet trànsit TCP cap a la IP 10.1.1.210 als ports 80 (HTTP) i 443 (HTTPS).

Ús: Habilitar accés a serveis web allotjats al servidor en producció.

12 chain=forward action=accept protocol=tcp dst-address=10.1.1.210 dst-port=80,443 log=no log-prefix=""

Permet trànsit TCP des de la IP 10.1.1.210 als ports 80 (HTTP) i 443 (HTTPS).

Ús: Habilitar el retorn del trànsit web des del servidor en producció.

13 chain=forward action=accept protocol=tcp src-address=10.1.1.210 src-port=80,443 log=no log-prefix=""

Permet trànsit TCP des de la xarxa 192.168.88.0/24 cap a l'adreça 192.168.88.1 al port 80 (HTTP).

Ús: Permetre accés a la web de configuració del Microtik.

14 chain=input action=accept protocol=tcp src-address=192.168.88.0/24 dst-address=192.168.88.1 dst-port=80 log=no log-prefix=""

Permet trànsit TCP des de 192.168.88.1 cap a la xarxa 192.168.88.0/24 usant el port 80 (HTTP).

Ús: Habilitar el retorn del trànsit HTTP cap als clients de la web de configuració del Microtik.

15 chain=output action=accept protocol=tcp src-address=192.168.88.1 dst-address=192.168.88.0/24 src-port=80 log=no log-prefix=""

Permet trànsit UDP des de la xarxa 10.1.1.208/28 cap a la direcció 8.8.8.8 al port 53 (DNS).

Ús: Habilita consultes DNS des d'aquesta xarxa cap al servidor de Google.

16 chain=forward action=accept protocol=udp src-address=10.1.1.208/28 dst-address=8.8.8.8 src-port="" dst-port=53 log=no log-prefix=""

Permet trànsit UDP des de 8.8.8.8 cap a la xarxa 10.1.1.208/28 al port 53 (DNS).

Ús: Habilitar el retorn de respostes DNS des de Google cap a aquesta xarxa.

17 chain=forward action=accept protocol=udp src-address=8.8.8.8 dst-address=10.1.1.208/28 src-port=53 log=no log-prefix=""

Permet trànsit TCP cap a la xarxa 10.1.1.208/28 des de les adreces IP llistades (10.1.1.2, 10.1.1.3) al port 22 (SSH).

Ús: Habilitar accés SSH cap a dispositius a la xarxa 10.1.1.208/28 des de hosts específics.

18 chain=forward action=accept protocol=tcp dst-address=10.1.1.208/28 src-address-list=10.1.1.2, 10.1.1.3 dst-port=22 log=no log-prefix=""

Permet trànsit TCP des de la xarxa 10.1.1.208/28 cap a les adreces IP llistades (10.1.1.2, 10.1.1.3) al port 22 (SSH).

Ús: Habilitar el retorn del trànsit SSH cap als hosts permesos.

19 chain=forward action=accept protocol=tcp src-address=10.1.1.208/28 dst-address-list=10.1.1.2, 10.1.1.3 src-port=22 log=no log-prefix=""

Permet trànsit ICMP (ping, etc.) des de qualsevol origen cap a les adreces llistades (10.1.1.210, 10.1.1.211, etc.).

Ús: Habilitar diagnòstics ICMP cap a aquests dispositius.

20 chain=forward action=accept protocol=icmp src-address-list="" dst-address-list=10.1.1.210, 10.1.1.211, 10.1.1.1, 10.1.1.129, 10.1.1.193, 10.1.1.209, 10.1.1.225, 10.1.1.226 log=no log-prefix=""

Permet trànsit ICMP des de les adreces llistades (10.1.1.210, 10.1.1.211, etc.) cap a qualsevol destinació.

Ús: Habilitar diagnòstics ICMP des d'aquests dispositius.

21 chain=forward action=accept protocol=icmp src-address-list=10.1.1.210, 10.1.1.211, 10.1.1.1, 10.1.1.129, 10.1.1.193, 10.1.1.209, 10.1.1.225, 10.1.1.226 log=no log-prefix=""

Permet trànsit UDP des de 10.1.1.225 cap a les adreces llistades (10.1.1.226/30, 224.0.0.9) al port 520 (RIP).

Ús: Habilita protocols d'encaminament RIP des d'aquesta IP.

22 chain=forward action=accept protocol=udp src-address=10.1.1.225 dst-address-list=10.1.1.226/30, 224.0.0.9 dst-port=520 log=no log-prefix=""

Permet trànsit UDP des de 10.1.1.226 cap a les adreces llistades (10.1.1.225/30, 224.0.0.9) al port 520 (RIP).

Ús: Habilitar protocols d'encaminament RIP cap a aquesta IP.

23 chain=forward action=accept protocol=udp src-address=10.1.1.226 dst-address-list=10.1.1.225/30, 224.0.0.9 dst-port=520 log=no log-prefix=""

Bloqueja tot el trànsit TCP no permès per regles anteriors.

Ús: És una regla de caiguda per reforçar la seguretat, evitant trànsit TCP no autoritzat.

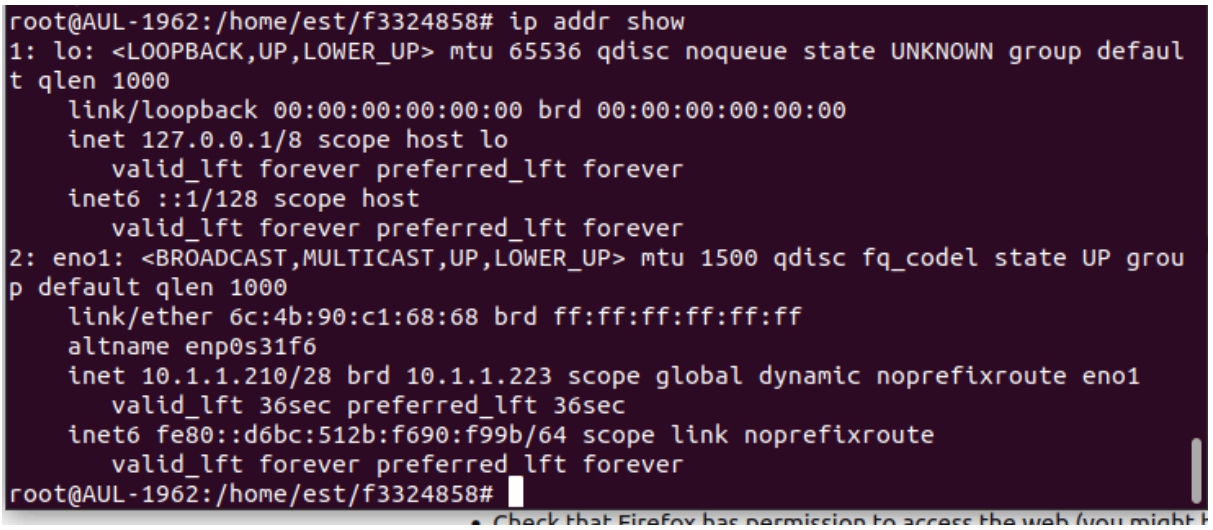
24 chain=forward action=drop protocol=tcp log=no log-prefix=""

Les regles afegides tenen com a objectiu reforçar la seguretat del tallafocs. Hem afegit una regla genèrica de drop al final de les cadenes forward, input i output per bloquejar qualsevol tràfic no autoritzat, incloent protocols diferents del TCP, com UDP o ICMP. També s'ha incorporat una regla específica per bloquejar tràfic ICMP no autoritzat, limitant-lo només a les adreces permeses. A més, s'ha configurat una regla de registre (*log*) abans del bloqueig per facilitar la monitorització i la detecció de tràfic rebutjat. Finalment, es garanteix que la política per defecte sigui estricta (drop), assegurant que només el tràfic explícitament permès pugui passar. Aquestes modificacions milloren la robustesa del tallafocs i redueixen possibles vulnerabilitats.

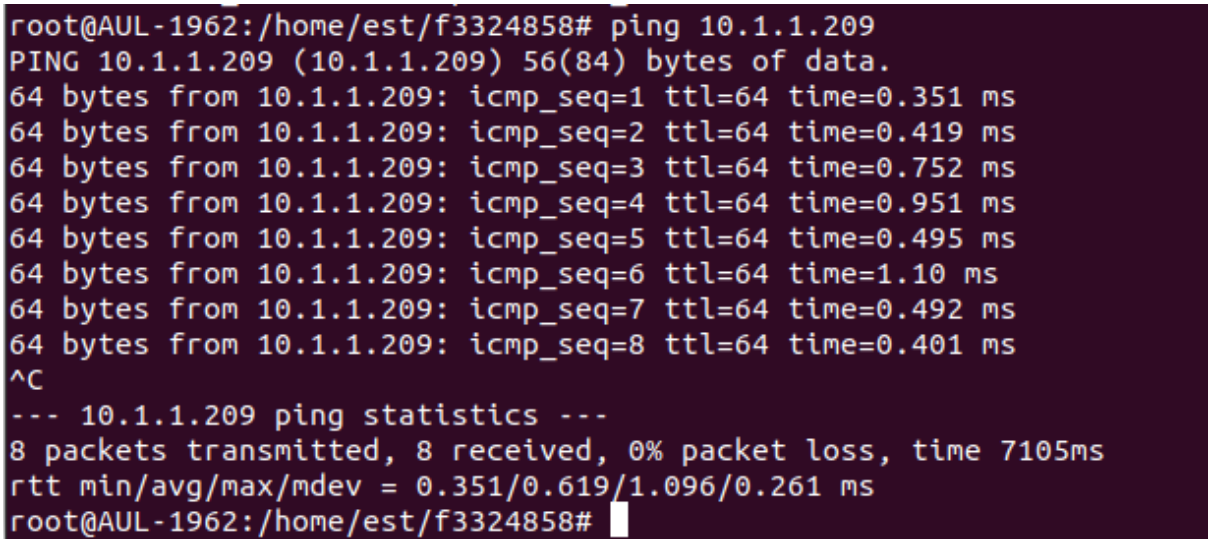
- D		10	accept	forward	10.1.1.208/28		6 (tcp)		80,443							
- D		11	accept	forward		10.1.1.208/2	6 (tcp)	80,443								
- D		12	accept	forward		10.1.1.210	6 (tcp)		80,443							
- D		13	accept	forward	10.1.1.210		6 (tcp)	80,443								
- D		14	accept	input	192.168.88.0/24	192.168.88.	6 (tcp)		80							
- D		15	accept	output	192.168.88.1	192.168.88.	6 (tcp)	80								
- D		16	accept	forward	10.1.1.208/28	8.8.8.8	17 (udp)		53							
- D		17	accept	forward	8.8.8.8	10.1.1.208/2	17 (udp)	53								
- D		18	accept	forward		10.1.1.208/2	6 (tcp)		22					10.1.1.2, 10.1.1.3		
- D		19	accept	forward	10.1.1.208/28		6 (tcp)	22							10.1.1.2, 10.1.1.3	
- D		20	accept	forward			1 (icmp)								10.1.1.210, 10.1.1.211, 10.1.1.1, 10.1.1.129, 10.1.1.193, 10.1.1.209, 10.1.1.225, 10.1.	
- D		21	accept	forward			1 (icmp)							10.1.1.210, 10.1.1.211, 10.1.1.1, 10.1.1.129, 10.1.1.193, 10.1.1.209, 10.1.1.225, 10.1.1.226		
- D		22	accept	forward	10.1.1.225		17 (udp)		520						10.1.1.226/30, 224.0.0.9	
- D		23	accept	forward	10.1.1.226		17 (udp)		520						10.1.1.225/30, 224.0.0.9	
- D		24	drop	forward			6 (tcp)									

```
[admin@MikroTik] > ip firewall filter print
Flags: X - disabled, I - invalid, D - dynamic
 0 X  ;;; defconf: accept established,related,untracked
      chain=input action=accept connection-state=established,related,untracked log=no log-prefix=""

 1 X  ;;; defconf: drop invalid
      chain=input action=drop connection-state=invalid log=no log-prefix=""

 2 X  ;;; defconf: accept ICMP
      chain=input action=accept protocol=icmp

 3 X  ;;; defconf: accept to local loopback (for CAPsMAN)
      chain=input action=accept dst-address=127.0.0.1

 4 X  ;;; defconf: drop all not coming from LAN
      chain=input action=drop in-interface-list=!LAN

 5 X  ;;; defconf: accept in ipsec policy
      chain=forward action=accept ipsec-policy=in,ipsec

 6 X  ;;; defconf: accept out ipsec policy
      chain=forward action=accept ipsec-policy=out,ipsec

 7 X  ;;; defconf: fasttrack
      chain=forward action=fasttrack-connection connection-state=established,related

 8 X  ;;; defconf: accept established,related, untracked
      chain=forward action=accept connection-state=established,related,untracked

 9 X  ;;; defconf: drop all from WAN not DSTNATed
      chain=forward action=drop connection-state=new connection-nat-state=!dstnat in-interface-list=WAN

10    chain=forward action=accept protocol=tcp src-address=10.1.1.208/28 dst-port=80,443 log=no log-prefix=""

11    chain=forward action=accept protocol=tcp dst-address=10.1.1.208/28 src-port=80,443 log=no log-prefix=""

12    chain=forward action=accept protocol=tcp dst-address=10.1.1.210 dst-port=80,443 log=no log-prefix=""

13    chain=forward action=accept protocol=tcp src-address=10.1.1.210 src-port=80,443 log=no log-prefix=""

14    chain=input action=accept protocol=tcp src-address=192.168.88.0/24 dst-address=192.168.88.1 dst-port=80 log=no log-prefix=""
```

Comprovacions del correcte funcionament:
-Tenim una IP del CPD assignada correctament:



-Podem fer ping al router:



-Podem fer ping a google:

```
root@AUL-1962:/home/est/f3324858# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=116 time=10.2 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=116 time=10.2 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=116 time=11.1 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=116 time=10.2 ms
^C
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 10.159/10.406/11.140/0.423 ms
root@AUL-1962:/home/est/f3324858#
```

-Podem navegar per internet sense cap problema, i al buscar per exemple adidas.es, ens dirigeix a la pàgina corresponent, per tant també funciona la traducció de noms: