Entrega: 17/12/2023

Alumnes: Francesco Oncins Spedo
Mariona Farré Tapias
Pau Alcázar Perdomo

INTERNET:
P3- Qüestionari sessió 2 - Configuració del tallafocs

1. Per quines cadenes hi ha definides regles a la taula filter del tallafocs? Per quina d'aquestes cadenes passaria un paquet dirigit a la IP 192.168.88.1?
   Cadenes:
   - input
   - forward
   - output

```
[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
```

   A la configuració per defecte del router, només hi ha regles per les cadenes input i forward. No n'hi ha per la cadena output.
   Si el paquet prové d'un dispositiu dins de la mateixa LAN (Xarxa Local), seria processat per la cadena input ja que està dirigit al propi router MikroTik (192.168.88.1). Aquesta és la cadena que gestiona els paquets destinats al mateix router.

2. Per a que serveix el "connection-state" a les regles del tallafocs? Quina diferència hi ha entre "connection-state=new" i "connection-state=established"?

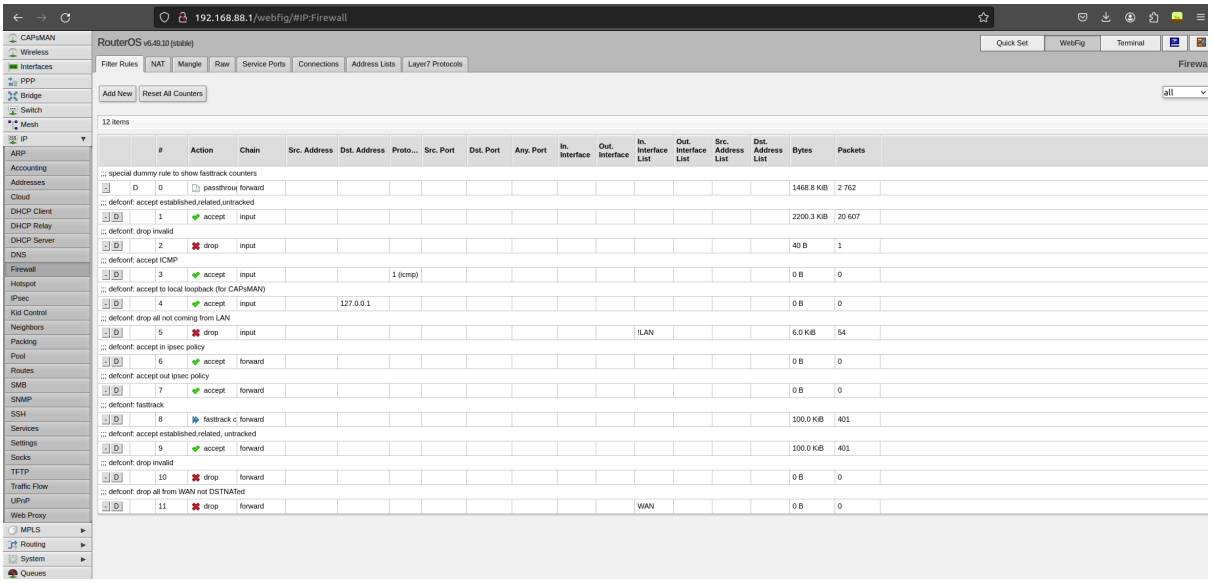
El connection-state ens diu com és la connexió i pot tenir 5 estats:

- New: connexió encara no vista
- Related: connexió nova però relacionada a una altre connexió correcte
- Established: connexió establerta
- Invalid: trànsit no identificat per x raó
- Untracked: tot i que és una connexió que encara no hem vist, no és new, nosaltres la marquem com a untracked.

La diferència és que *new* és una connexió que encara no ha estat vista i l'estat *established* vol dir que és una connexió establerta.

3. Quines interfícies físiques es corresponen amb "WAN" i "LAN"?
   Wide Area Network: Accés pel port 1
   Local Area Network: Accés pels ports 2, 3, 4 i 5 i wifi

4. El router respon pings? Què passaria si l'ordre de les regles 3 , 4 i 5 (per defecte del router) fos 4, 5 i 3?



Captura 1, mencionada en la resposta de la primera pregunta.

La configuració del tallafocs en la captura 1 mostra que hi ha una regla (regla número 3) que permet acceptar el tràfic ICMP, que són els paquets utilitzats per l'operació de ping. Aquesta regla no està restringida per cap adreça IP específica, per tant, hauria de permetre la resposta a pings de qualsevol font.

La regla actual número 4 permet el tràfic des de l'adreça IP local 127.0.0.1, que és l'adreça de loopback. La regla número 5 rebutja tot el tràfic que no prové de la xarxa LAN. I la regla número 3, com s'ha mencionat, accepta pings (ICMP).

Si l'ordre fos canviat a 4, 5, 3, això afecta el comportament del tallafocs. La regla número 5 es mou abans de la regla número 3, tots els pings que no provenen de la xarxa LAN serien rebutjats abans que la regla número 3 tingués l'oportunitat d'acceptar-los. Això significa que

només els dispositius dins de la xarxa LAN podrien fer ping al router amb èxit. I la regla número 4, que es mou al principi, continuaria permetent el tràfic de loopback, però això no tindria impacte en el tràfic de xarxa externa o pings.

Canviar l'ordre d'aquestes regles potencialment bloquejaria respostes de ping de fonts externes, però permetria els pings de dins de la xarxa LAN si el tràfic de LAN no es veu afectat per cap altra regla anterior en la nova ordenació.

5. Es poden establir connexions des de LAN cap a Internet? I al revés? Indica les regles (per defecte del router) que aplicarien en cada cas.

   Les connexions des de la xarxa LAN cap a Internet estan permeses. Això es pot deduir de la manca d'una regla explícita que prohibeixi aquest tràfic en la taula de filtrat. Hi ha regles que faciliten el tràfic sortint com la regla de "fasttrack" (regla número 8), que està dissenyada per accelerar el tractament dels paquets establerts i relacionats que passen per la cadena FORWARD, la qual cosa implica tràfic que passa de la xarxa LAN cap a Internet.

   les connexions entrants d'Internet cap a la LAN, la regla número 9 accepta el tràfic que és "established,related", el que suggereix que les respostes a les connexions iniciades des de la LAN són acceptades. Tanmateix, qualsevol connexió iniciada des d'Internet cap a la LAN que no sigui una resposta a una connexió existent probablement serà rebutjada, ja que no hi ha regles que explícitament permetin el nou tràfic entrant a la LAN.

   Les connexions des d'Internet cap a LAN generalment es gestionen mitjançant regles de Network Address Translation (NAT) i no es mostren en la taula de filtrat que es pot veure en la imatge. Seria necessari revisar la secció NAT de la configuració del tallafocs per determinar si hi ha regles que permeten aquest tipus de connexions.

6. Hi ha algun paquet que pogués passar per les cadenes que hi ha definides sense que l'afecti per cap regla? Si la resposta és sí, penseu quina deu ser la política per defecte que aplica el tallafocs per a que la configuració tingui sentit.
   Perquè un paquet passi per aquestes regles sense veure's afectat, no hauria de coincidir amb cap de les regles definide. D'acord amb aquestes, els paquets que són nous (no established, related o untracked), vàlids i que no utilitzen ICMP, no destinats a la interfície de loopback, que no provenen de la LAN, no coincideixen amb la política IPsec i no provenen de la WAN sense DSTNAT, no correspondria explícitament a cap de les regles enumerades. I per tant dependrà de la política per defecte si el paquet és transmès. I la política per defecte del router Miktrotik és Drop: on el paquet és descartat silenciosament, és a dir, que no ens notifica que el paquet ha estat descartat.

7. Escriviu i comenteu breument les regles que cal afegir al tallafocs per assolir els requeriments que es demanen en aquesta sessió

;;; defconf: drop all from WAN not DSTNATed

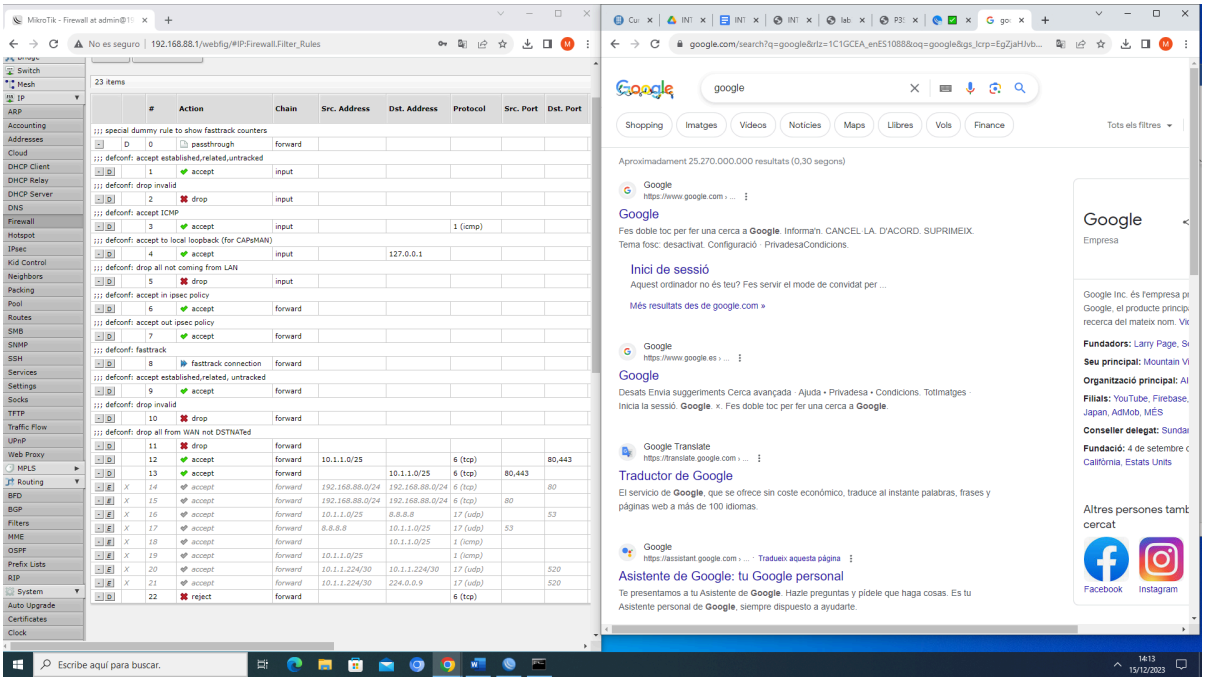
- D		11	drop	forward

No podem esborrar la regla perquè sino ens deixarà passar totes les connexions que venen d'internet i no ho podem permetre.

Perquè funcioni el firewall, la última regla la hem de filtrar per tcp, si no especifiquem el protocol no podem fer cap connexió que no compleixi alguna de les regles del firewall.

- D		24	reject	forward		6 (tcp)

Veiem que quan activem les 2 primeres regles i la per defecte (última) que hem configurat podem navegar per internet sense cap problema. Per tant vol dir que aquestes estan ben configurades i funcionen

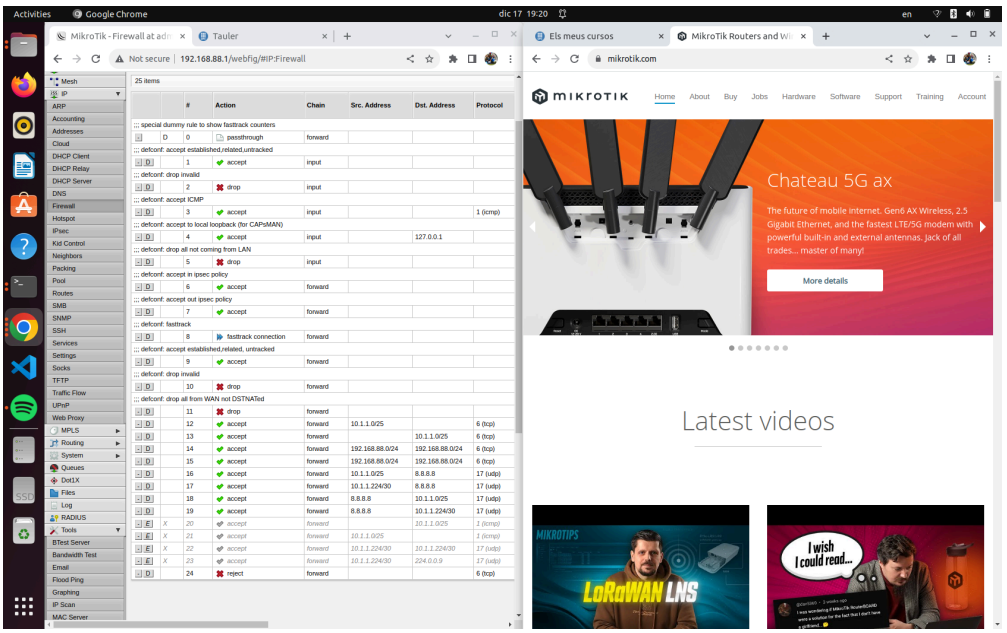


Per provar que les regles del dns funciona, hem canviat el server a 8.8.8.8, hem activat les regles del firewall al router canviant on fica "*nameserver 127.0.0.53*" per "*nameserver 8.8.8.8*" i llavors hem escrit la comanda nslookup google.com per comprovar que realment funciona.

```
francesco@francesco-GL75-Leopard-10SEK:~$ nslookup google.com
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
Name:   google.com
Address: 142.250.200.142
Name:   google.com
Address: 2a00:1450:4003:80f::200e
```

La comanda "*nslookup google.com*" envia una sol·licitud per trobar l'adreça IP associada amb el nom del lloc web google.com. Si el DNS funciona correctament, com és el cas la comanda retorna una adreça IP, que mostra que ha pogut traduir el nom de la pàgina web. En el nostre cas, el nom és google.com i l'adreça a la que ha traduït és 142.250.200.142.



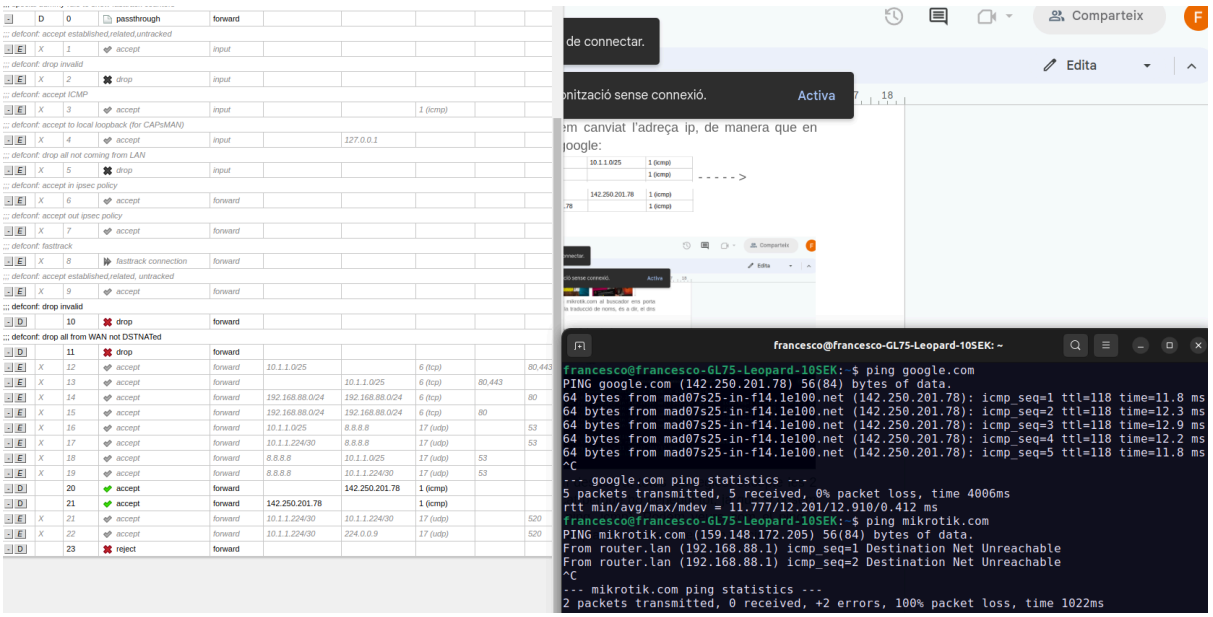
Una altra prova que funciona, quan escrivim mikrotik.com al buscador ens porta directament a la pàgina web, de manera que la traducció de noms, és a dir, el dns funciona correctament.

Per comprovar les 2 regles del ping, hem canviat l'adreça ip, de manera que en comptes de ser la 10.1.1.0/25 sigui la de google:

- D		20	accept	forward		10.1.1.0/25	1 (icmp)
- D		21	accept	forward	10.1.1.0/25		1 (icmp)

- - - - - >

- D		20	accept	forward		142.250.201.78	1 (icmp)
- D		21	accept	forward	142.250.201.78		1 (icmp)

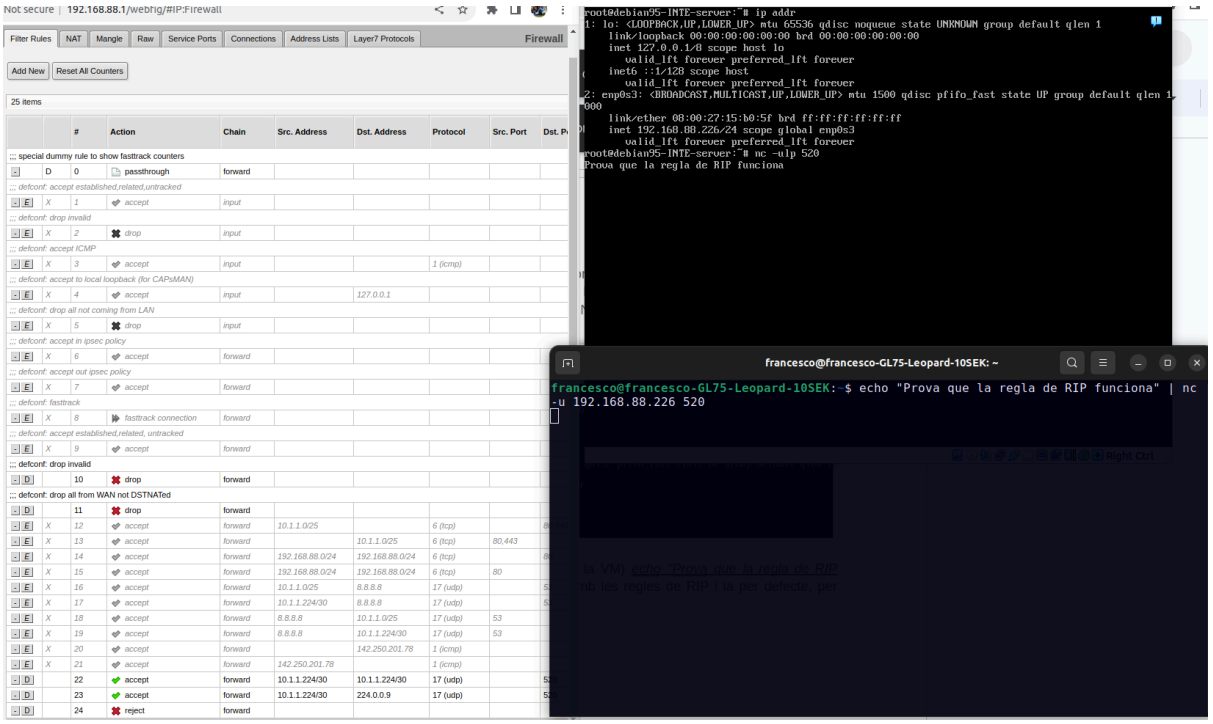


Per comprovar que el ping funciona, hem desactivat totes les regles, excepte les 2 del ping i la per defecte (que hem modificat perquè ho denegui tot, ja que si posem com a protocol tcp, no deixa passar el ping, icmp). Podem veure com el ping a google funciona mentre que si fem el ping a qualsevol altre adreça, per exemple mikrotik.com, no funciona.

Per comprovar que la última regla funciona, hem obert la màquina virtual que ens veu proporcionar, hem canviat les 2 adreces IP per una que estigui dins el rang de la regla (192.168.88.226 per la VM i 192.168.88.227 per al Linux) i hem executat Netcat en mode listen per al port 520 i protocol UDP.
Exemple de com hem canviat les adreces ip:

```
francesco@francesco-GL75-Leopard-10SEK:~$ sudo ip addr flush dev enp3s0
francesco@francesco-GL75-Leopard-10SEK:~$ sudo ip addr add 192.168.88.227/24 dev enp3s0
francesco@francesco-GL75-Leopard-10SEK:~$ ip link set enp3s0 up
RTNETLINK answers: Operation not permitted
francesco@francesco-GL75-Leopard-10SEK:~$ sudoip link set enp3s0 up
sudoip: command not found
francesco@francesco-GL75-Leopard-10SEK:~$ sudo ip link set enp3s0 up
francesco@francesco-GL75-Leopard-10SEK:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp3s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default
qlen 1000
    link/ether 2c:f0:5d:67:d0:4b brd ff:ff:ff:ff:ff:ff
    inet 192.168.88.227/24 scope global enp3s0
       valid_lft forever preferred_lft forever
    inet6 fe80::e313:8853:261c:ddb0/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: wlo1: <BROADCAST,MULTICAST> mtu 1500 qdisc noqueue state DOWN group default qlen 1000
    link/ether 34:2e:b7:78:8a:2a brd ff:ff:ff:ff:ff:ff
    altname wlp0s20f3
```

Executem a la terminal de linux (no de la VM) *echo "Prova que la regla de RIP funciona" | nc -u 192.168.88.226 520* amb les regles de RIP i la per defecte, per poder demostrar que realment funciona:



Com podem veure, les regles del RIP funcionen perfectament, deixant passar missatges per a les adreces especificades.

Configuració del firewall:

```
[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 log=no log-prefix=""
 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 log=no log-prefix=""
 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 log=no log-prefix="" ipsec-policy=in,ipsec
 7    ;;; defconf: accept out ipsec policy
      chain=forward action=accept log=no log-prefix="" 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
12    chain=forward action=accept protocol=tcp src-address=10.1.1.0/25 dst-port=80,443
log=no log-prefix=""
13    chain=forward action=accept protocol=tcp dst-address=10.1.1.0/25 src-port=80,443
log=no log-prefix=""
14    chain=forward action=accept protocol=tcp src-address=192.168.88.0/24
dst-address=192.168.88.0/24 dst-port=80 log=no log-prefix=""
15    chain=forward action=accept protocol=tcp src-address=192.168.88.0/24
dst-address=192.168.88.0/24 src-port=80 log=no log-prefix=""
16    chain=forward action=accept protocol=udp src-address=10.1.1.0/25 dst-address=8.8.8.8
dst-port=53 log=no log-prefix=""
17    chain=forward action=accept protocol=udp src-address=10.1.1.224/30
dst-address=8.8.8.8 dst-port=53 log=no log-prefix=""
```

```
18    chain=forward action=accept protocol=udp src-address=8.8.8.8 dst-address=10.1.1.0/25
src-port=53 log=no log-prefix=""

19    chain=forward action=accept protocol=udp src-address=8.8.8.8
dst-address=10.1.1.224/30 src-port=53 log=no log-prefix=""

20    chain=forward action=accept protocol=icmp dst-address=142.250.201.78 log=no
log-prefix=""

21    chain=forward action=accept protocol=icmp src-address=142.250.201.78 log=no
log-prefix=""

22    chain=forward action=accept protocol=udp src-address=10.1.1.224/30
dst-address=10.1.1.224/30 dst-port=520 log=no log-prefix=""

23    chain=forward action=accept protocol=udp src-address=10.1.1.224/30
dst-address=224.0.0.9 dst-port=520 log=no log-prefix=""

24    chain=forward action=reject reject-with=icmp-network-unreachable log=no log-prefix=""
```