**P3- Qüestionari sessió 2 i 3 - Configuració del tallafocs**

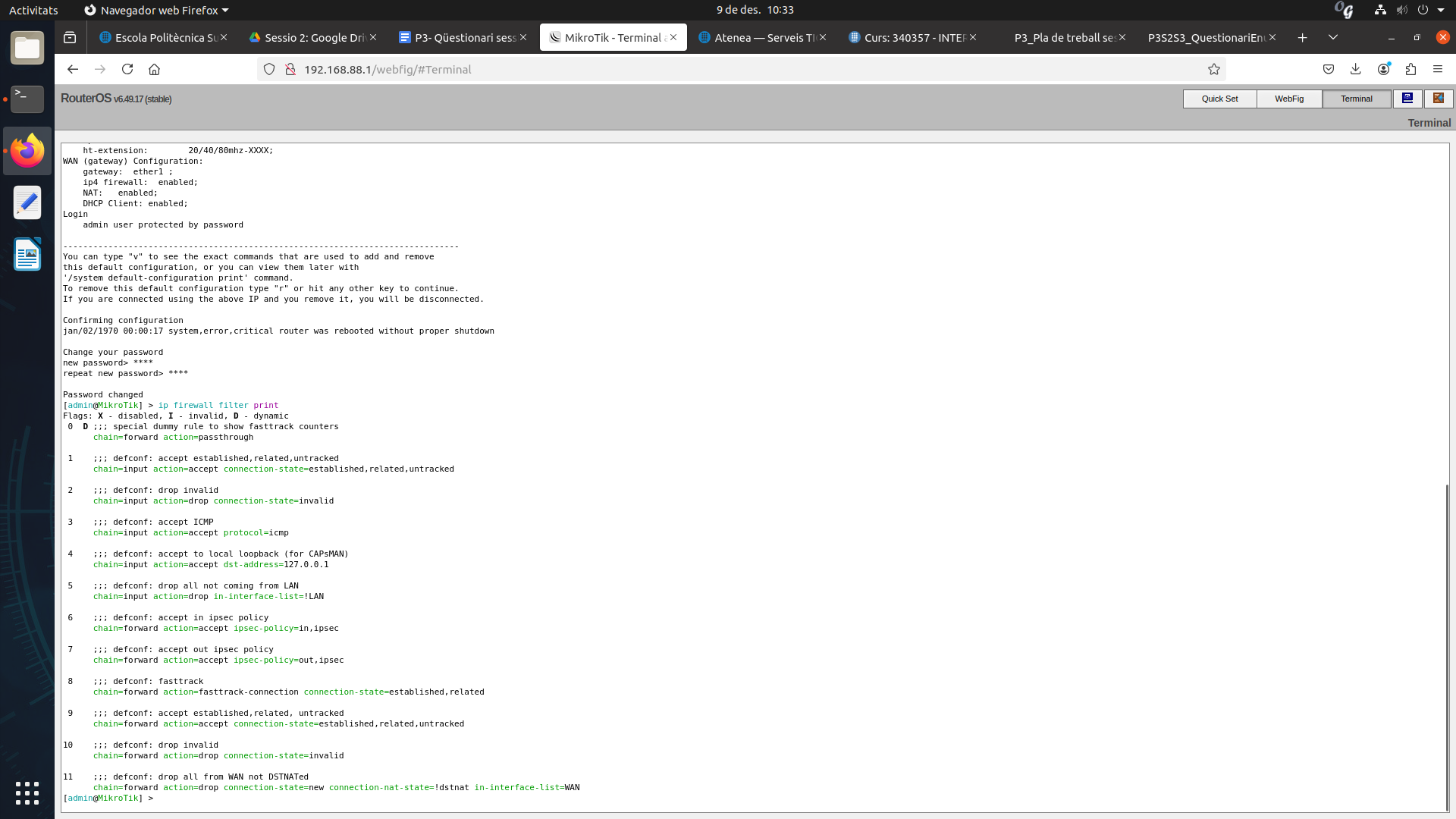
USUARI: admin

Password:

**1.**

A la taula que hi ha per defecte al mikrotik només hi ha cadenes forward i input.

La cadena forward significa que el paquet entraria al firewall sortiria, i la cadena output significa que el paquet surt del rúter, és a dir l’IP origen seria 192.168.88.1, per tant, queden descartades. La cadena input vol dir que el destí és el rúter, i com la IP destí que ens diuen és la del rúter, el paquet passaria per la cadena input.



**2.**

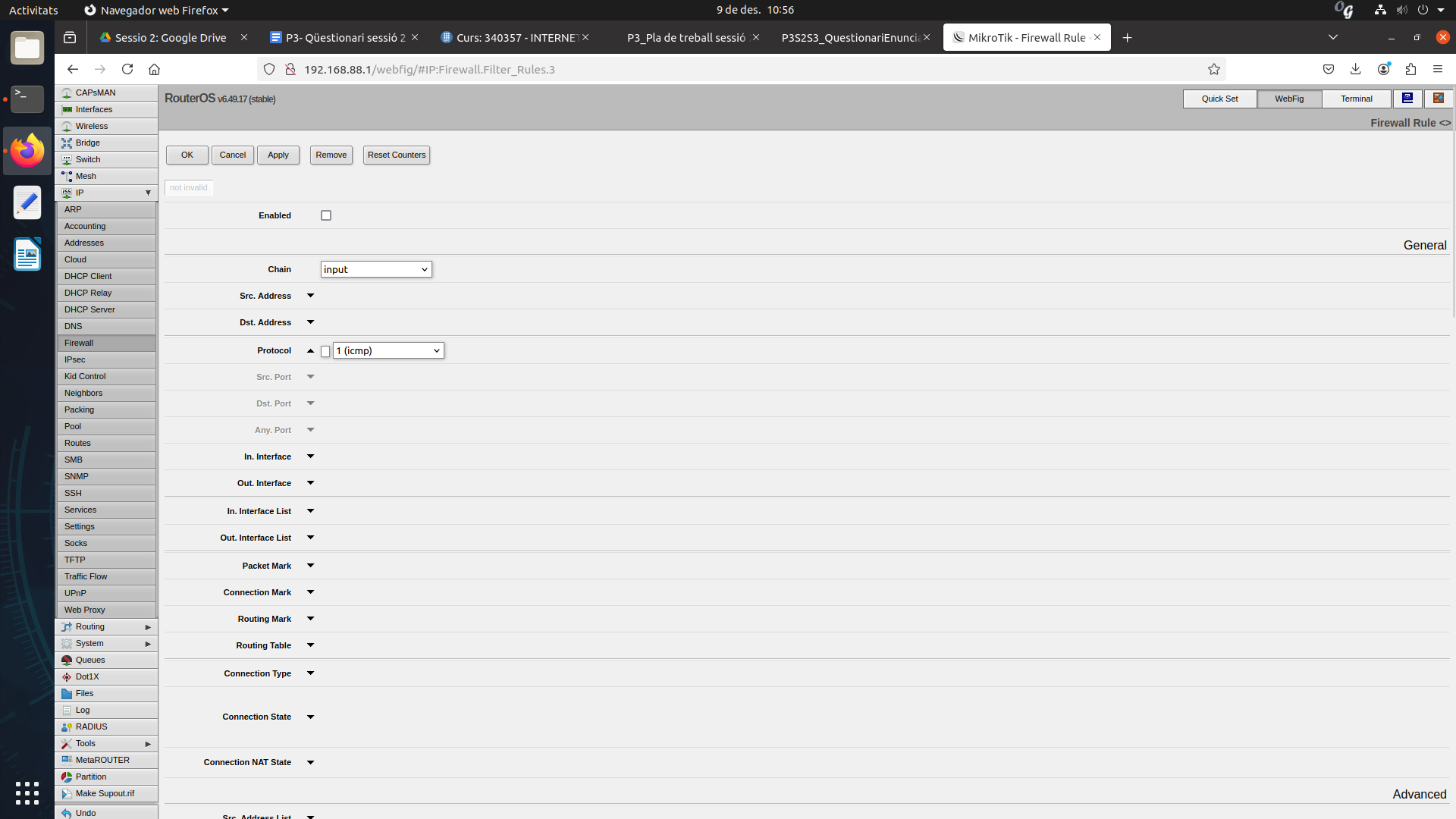
El "connection-state" en les regles del firewall s'utilitza para identificar i classificar les connexions. "Connection-state=new" significa que el paquet és d'una connexió nova i que no s'havia vist mai, i "Connection-state=established" vol dir que el paquet rebut és d'una connexió ja establerta.

**3.**

WAN és l’interfície que es connecta a la xarxa externa, com l’internet del laboratori, i en el mikrotik es correspon al port 1 del mikrotik.

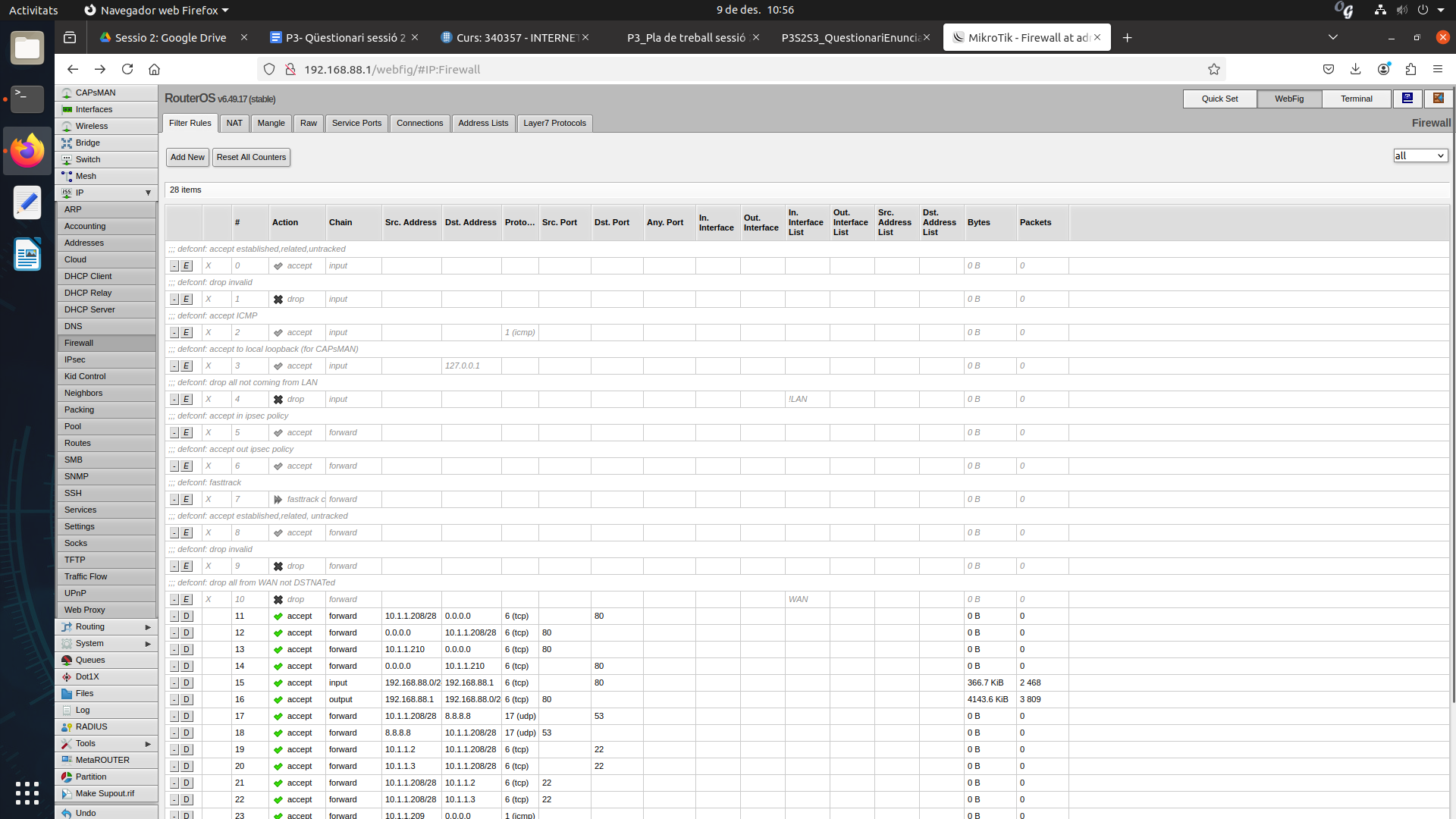
LAN és l’interfície que es connecta a la xarxa privada, i sol tenir IP privades. Aquesta es correspon els port 2, 3, 4 i 5 del Mikrotik.

**4.**

Sí, el router respon a pings. Si ens fixem en la configuració del firewall, la regla número 3 permet el trànsit ICMP.

* Regla 3 (actual): Permet el tràfic ICMP.
* Regla 4 (actual): Permet trànsit cap a l’adreça de loopback (127.0.0.1).
* Regla 5 (actual): Bloqueja tot el trànsit no procedent de la LAN.

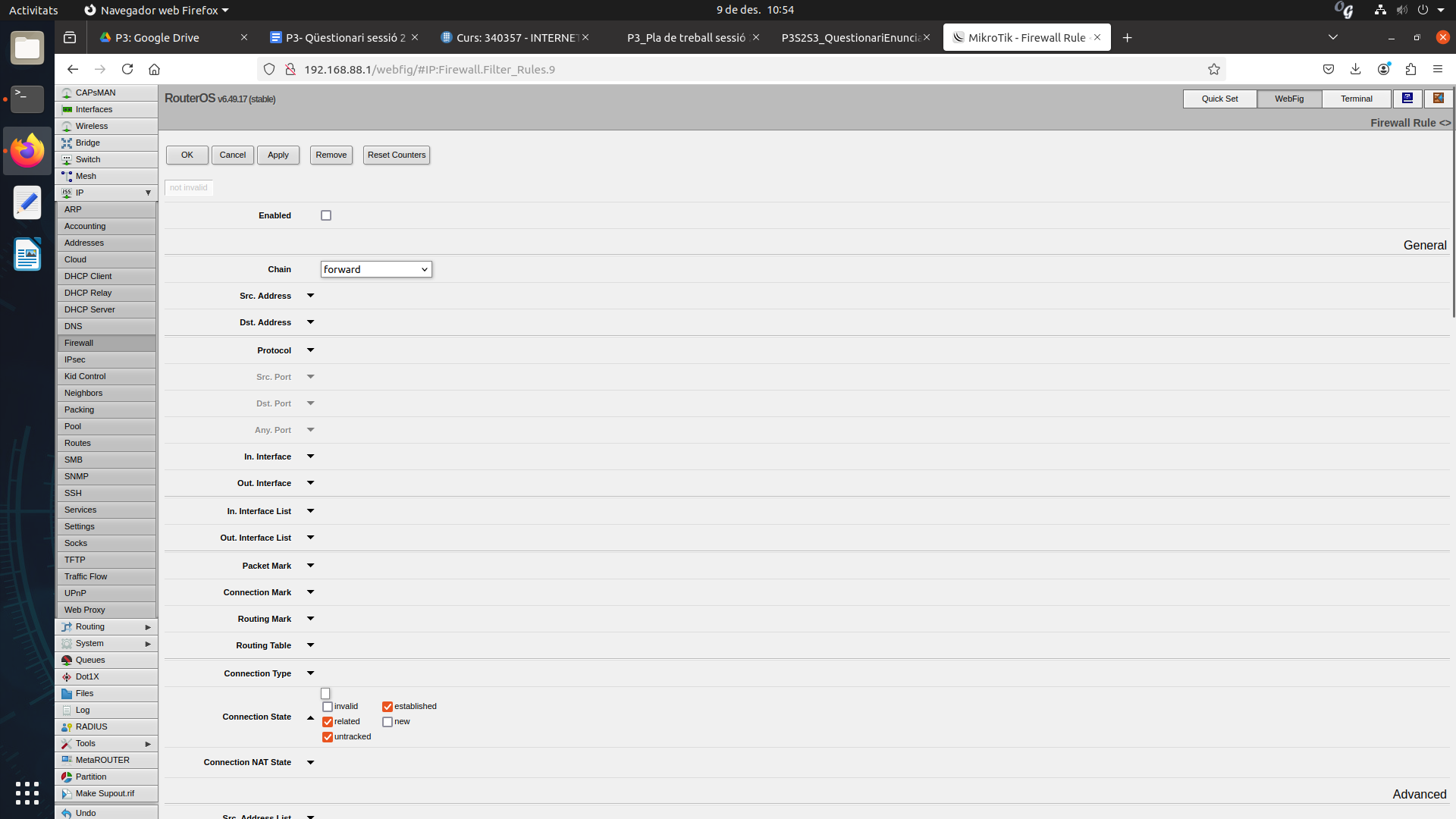
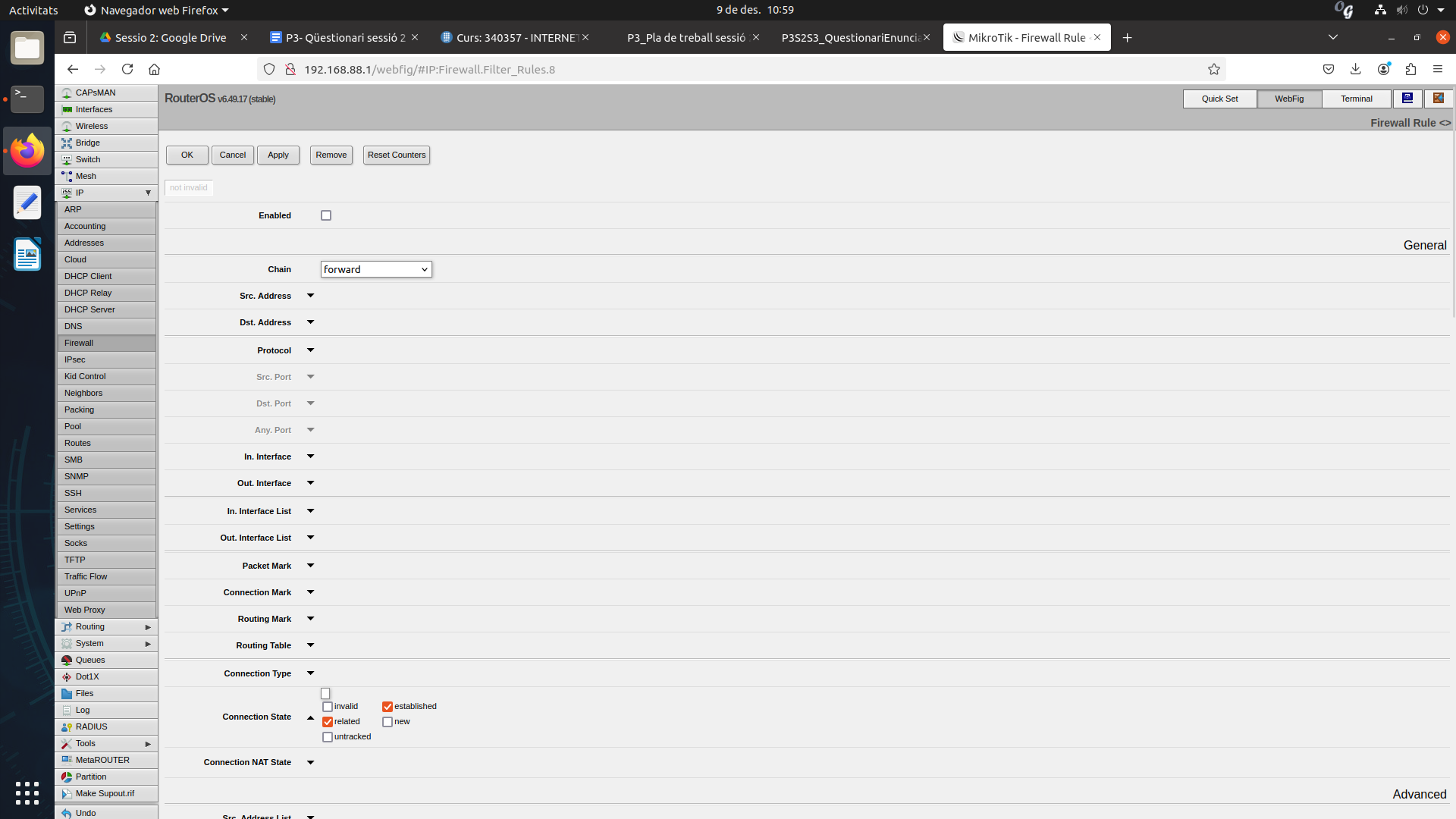
Si canviem l’ordre afectaria el comportament del tallafocs. Al moure la regla 5 que bloqueja el trànsit no provinent de la LAN, fent que s’executi abans de la regla 3 que permet ICMP, tots els pings que no provinguin de la LAN serien bloquejats. el qual significa que només els dispositius dins de la LAN podrien fer ping al router.

****

**5.**

Connexions des de LAN cap a Internet:

La regla número 8 (fasttrack-connection) permet el trànsit established i related a la cadena forward, per tant, les connexions establertes i relacionades des de la LAN cap a Internet són permeses. A més la regla número 9 també permet aquestes connexions.

****

Regla 8 Regla 9

Connexions des d'Internet cap a LAN:

La regla número 11 (drop all from WAN not DSTNATed) a la cadena forward bloqueja el trànsit des de la WAN no destinat (no dstnat), el que significa que les connexions iniciades des d'Internet cap a la LAN seran bloquejades.

Tot i això, la regla número 9 (accept established, related, untracked) permet el trànsit established i related, per tant, les respostes a les connexions ja iniciades des de la LAN seran acceptades.

En resum, les connexions des de la LAN cap a Internet estan permeses, i les respostes a aquestes connexions des d'Internet cap a la LAN també ho estan. En canvi les connexions des d'Internet cap a LAN estan bloquejades.

**6.**

Sí, és possible que hi hagi paquets que passin per les cadenes definides sense que els afecti cap regla. Això es deu a si un paquet no coincideix amb cap de les regles del firewall i, per tant, el tallafocs determina el destí d'aquests paquets, aquest destí potser accept: i, per tant, qualsevol paquet que no coincideixi amb cap regla serà acceptat. D'altra banda, esta drop: el que significa que qualsevol paquet que no coincideix amb cap regla serà descartat i bloquejat.

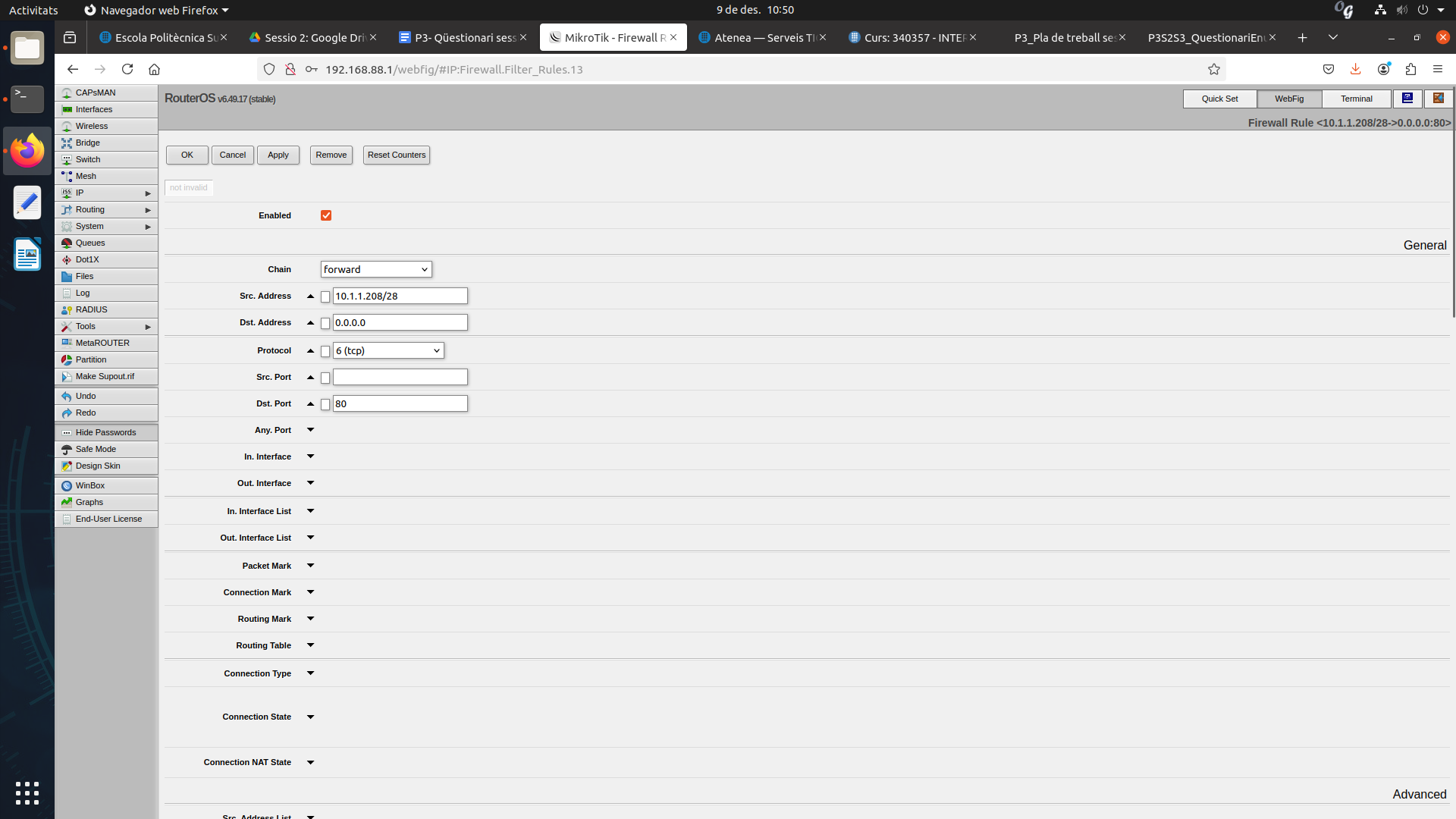
**7.**

S’han d’afegir una regla per cada fila de la taula que vam fer a la sessió anterior.

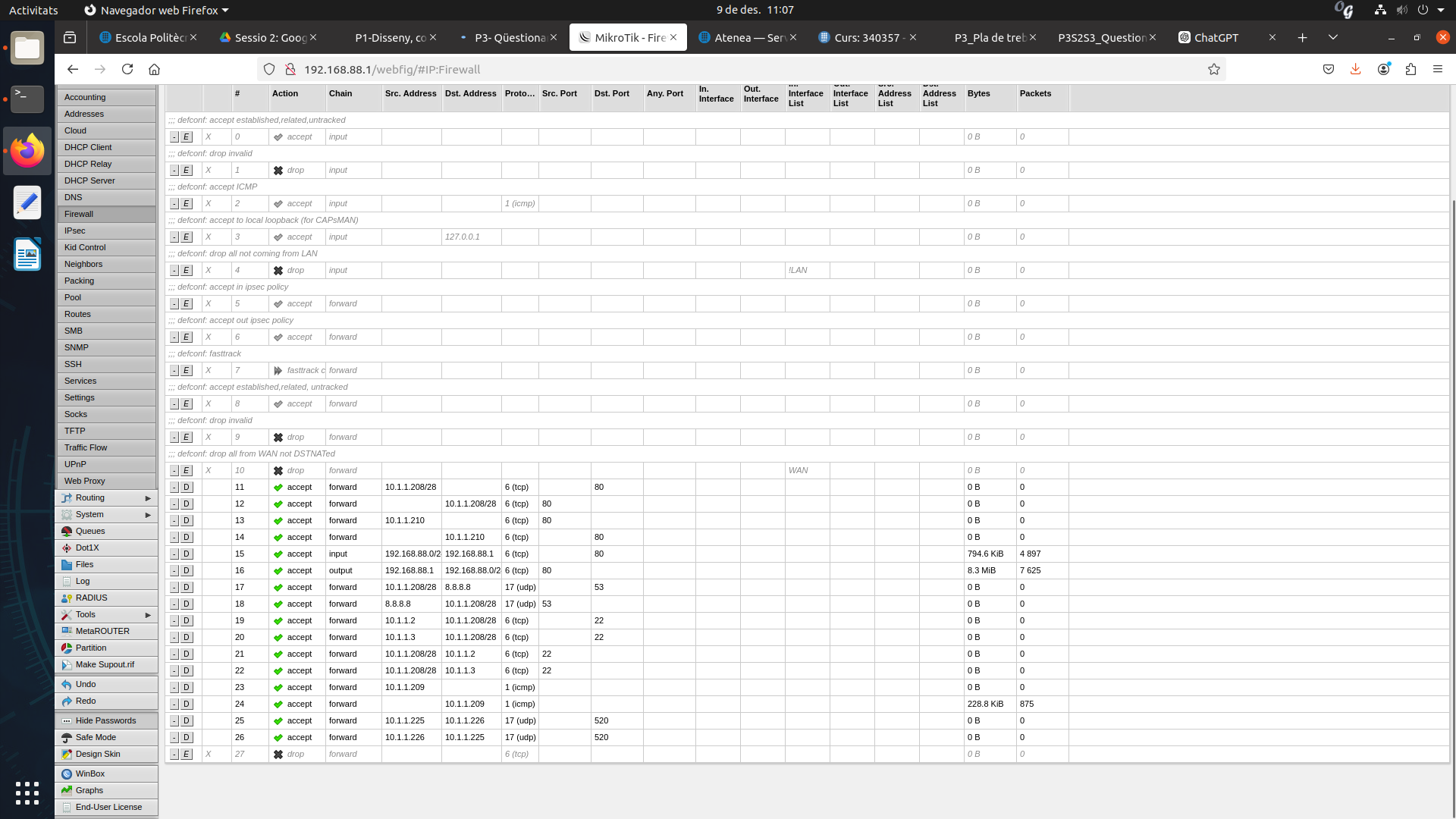
I hem de posar la informació d’aquesta taula en la informació de la regla de la següent manera.

Per exemple fem aquesta fila:

| **Servei** | **Acció** | **@IP origen** | **Port origen** | **@IP destí** | **Port destí** |
| --- | --- | --- | --- | --- | --- |
| Web (Client) | Permetre | 10.1.1.0/25  10.1.1.128/26  10.1.1.192/28  10.1.1.207/28  10.1.1.224/30 | \* | \* | TCP /80  TCP /443 |

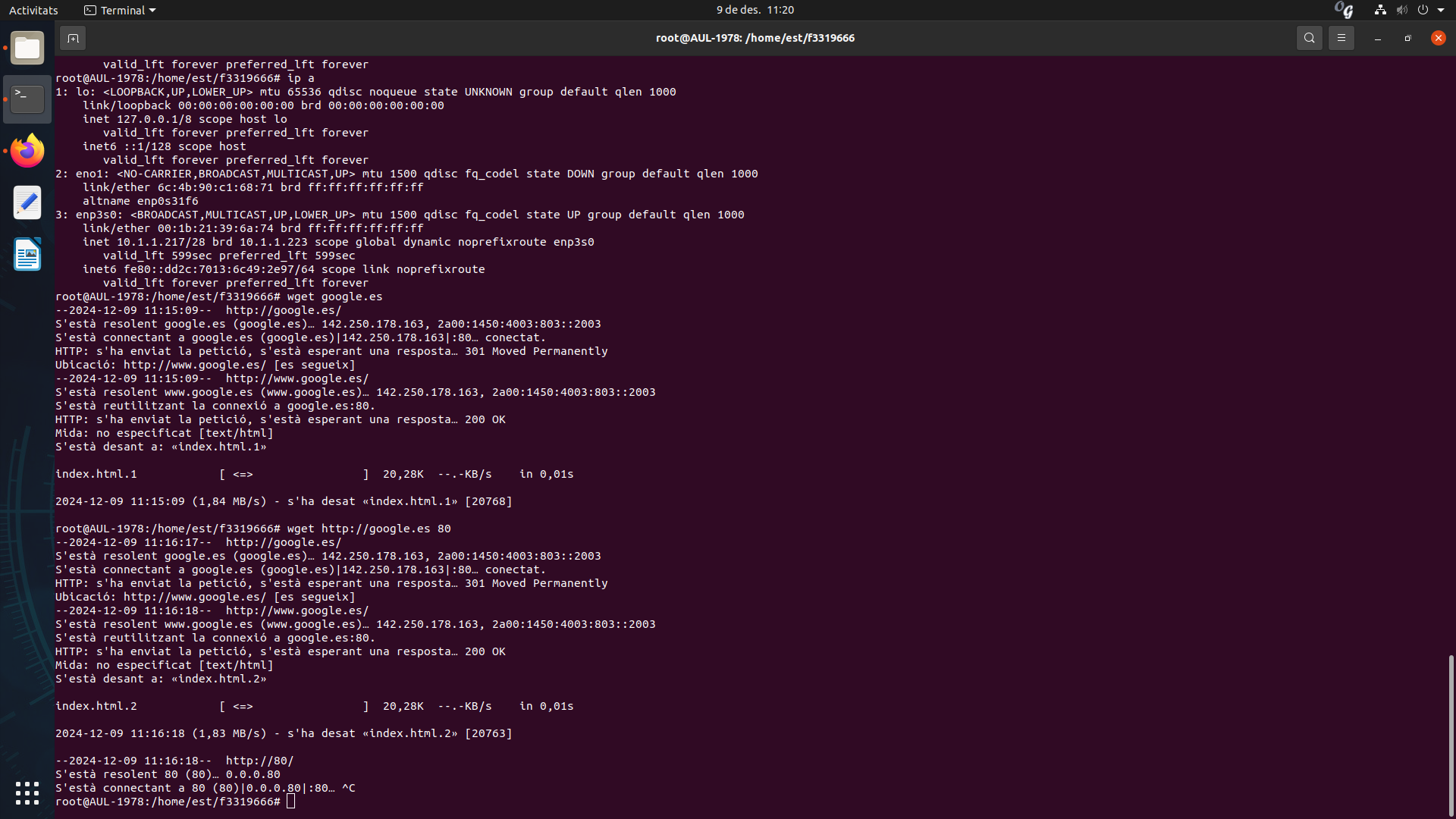
La configuració de la fila s’hauria de veure així:  


Totes les regles necessàries afegides es veurien així:

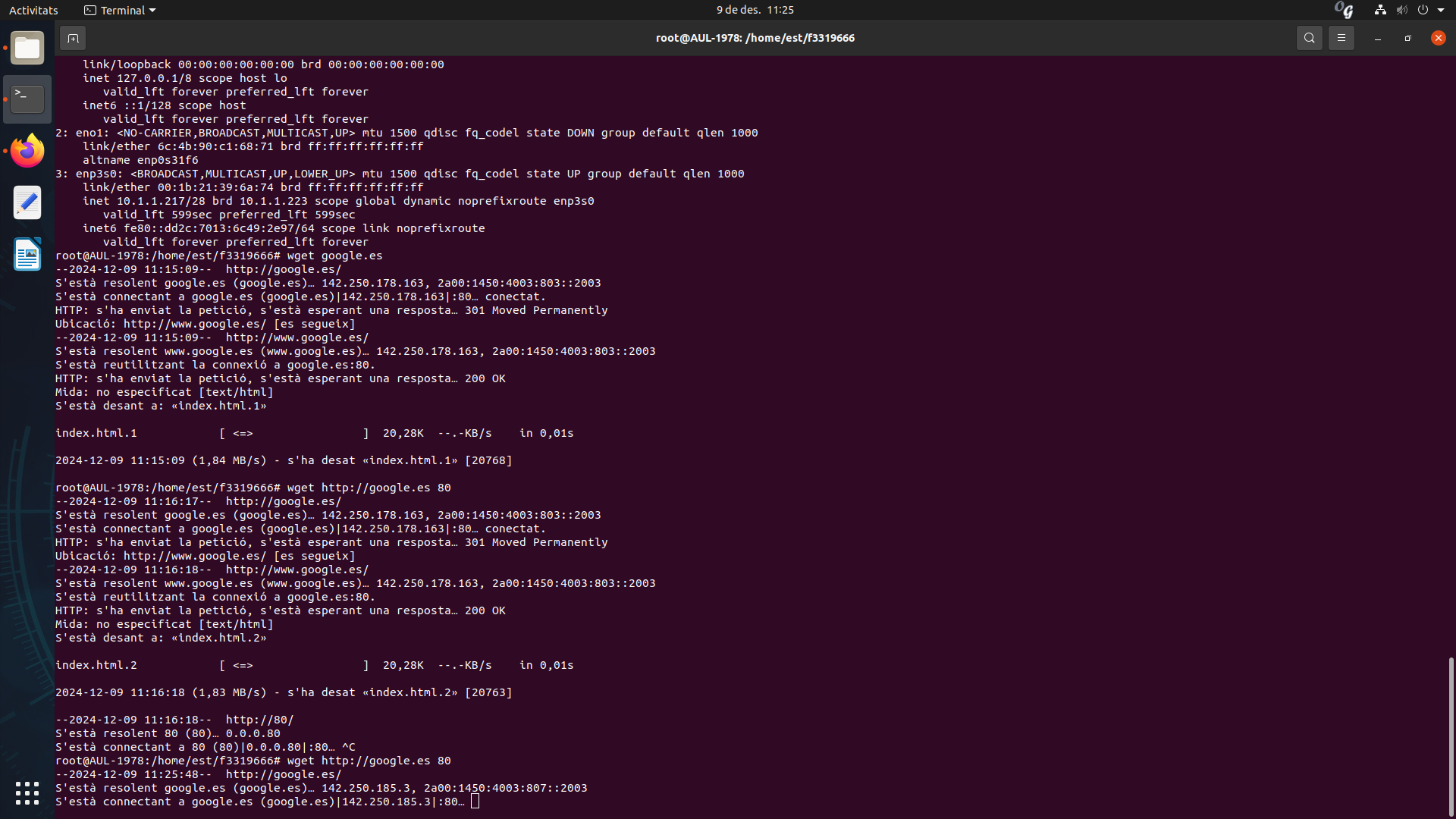


**Comprovacions del firewall:**

WEB:

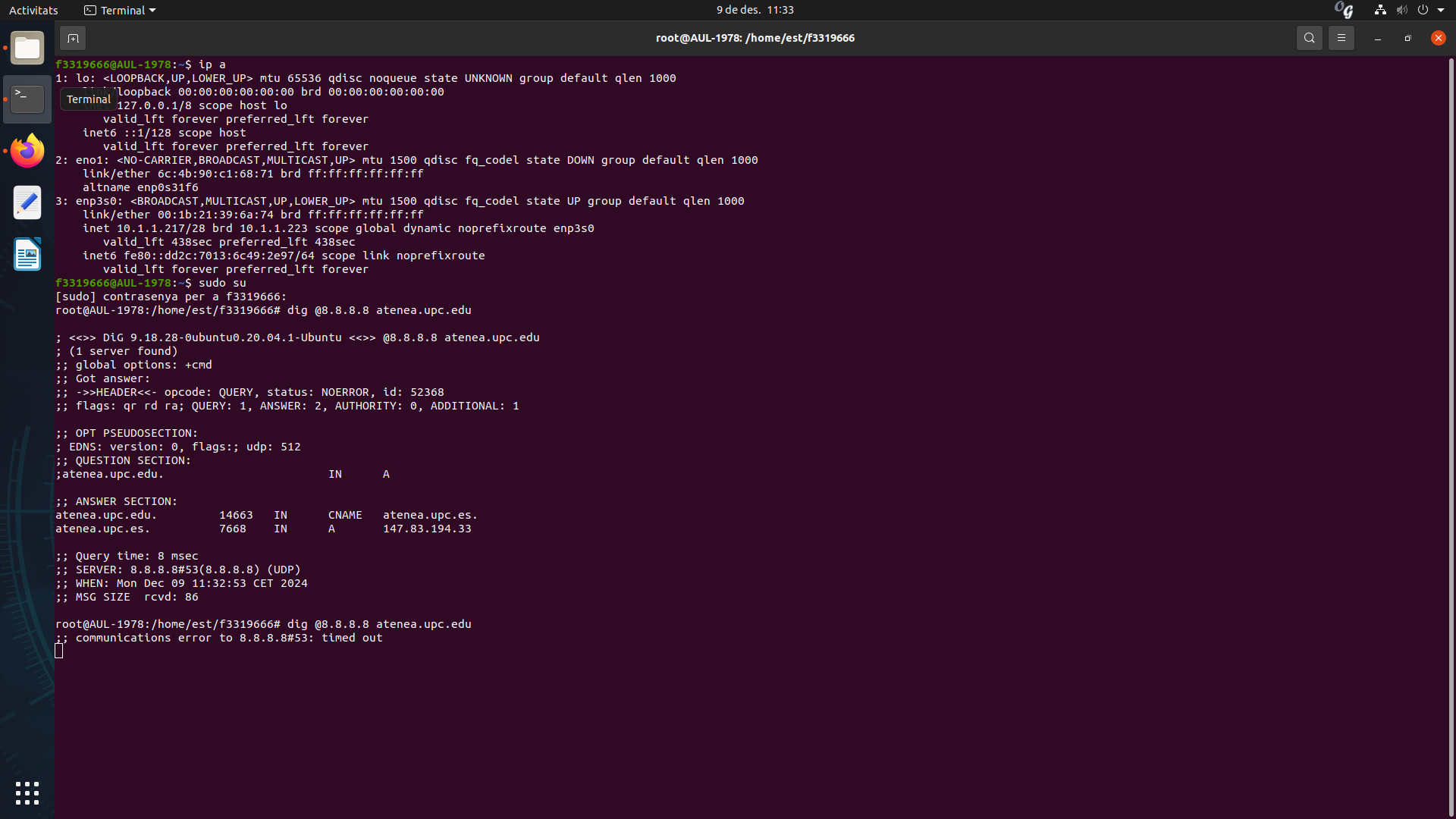


I si activem el drop, i desactivem la regla del web, deixa de funcionar.

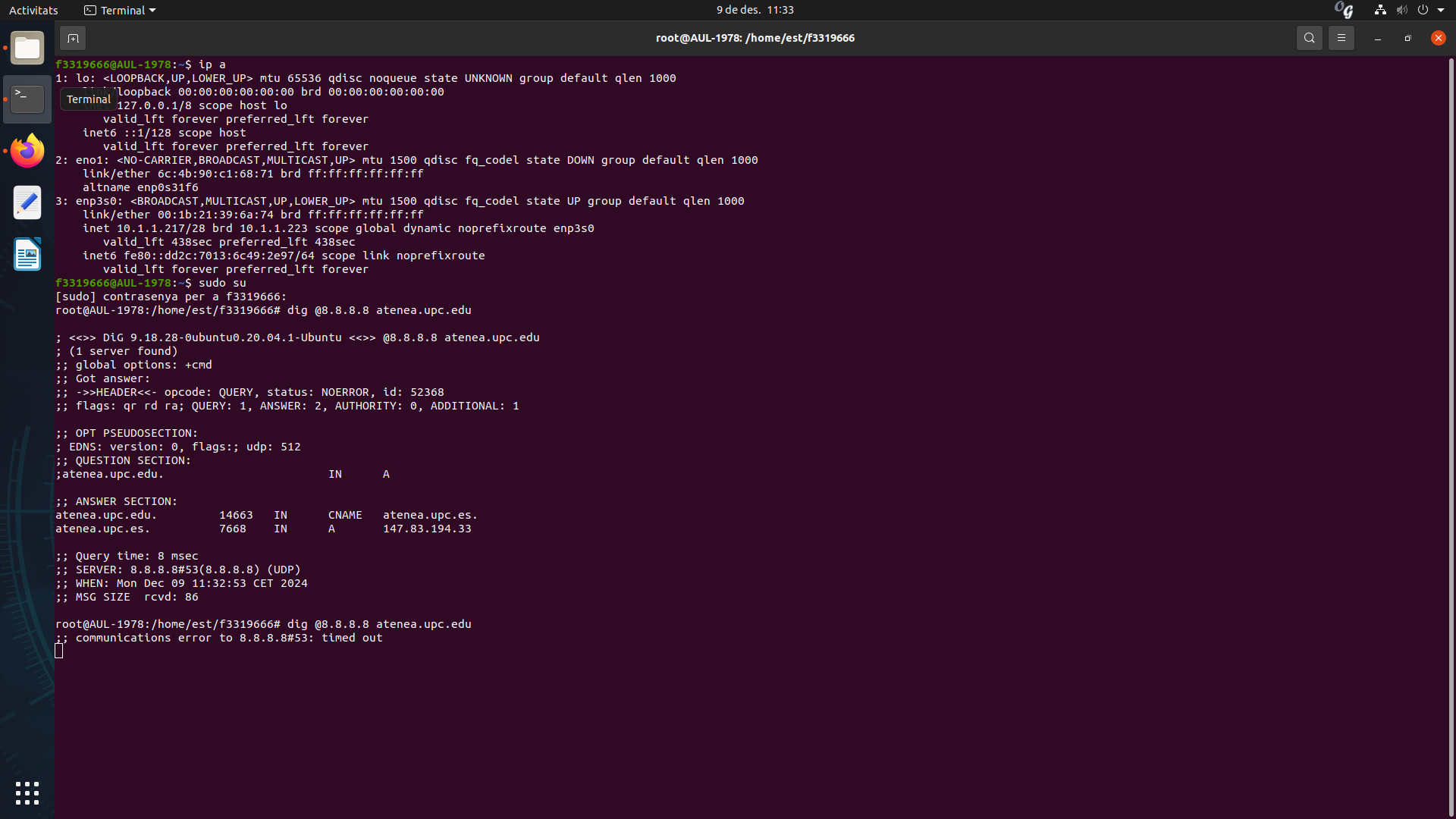


DNS:

Provem amb la comanda dig i la IP 8.8.8.8, ja que és la que ens diu l’enunciat

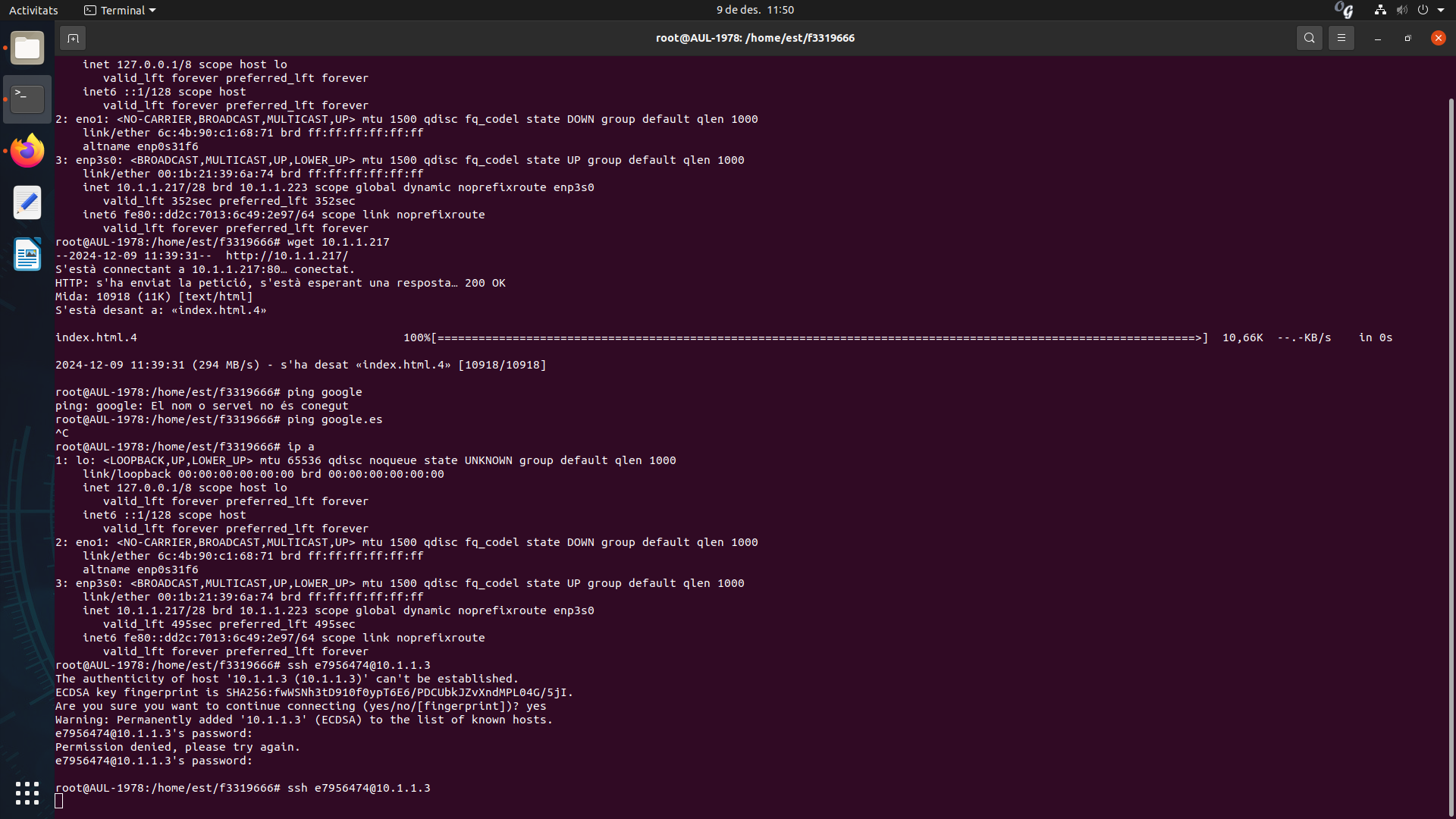


I si desactivem la regla i activem el drop amb el protocol UDP

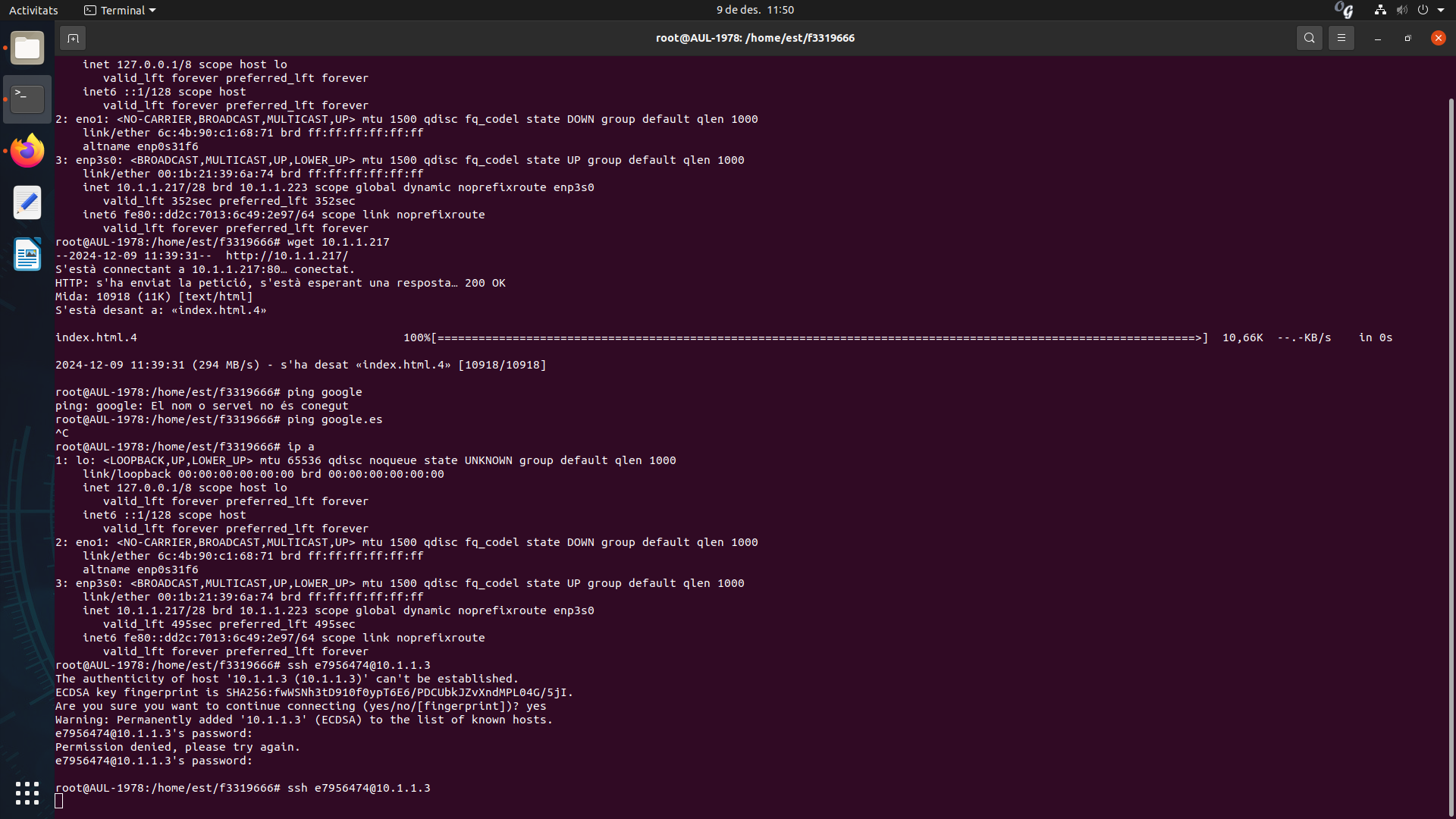


SSH:

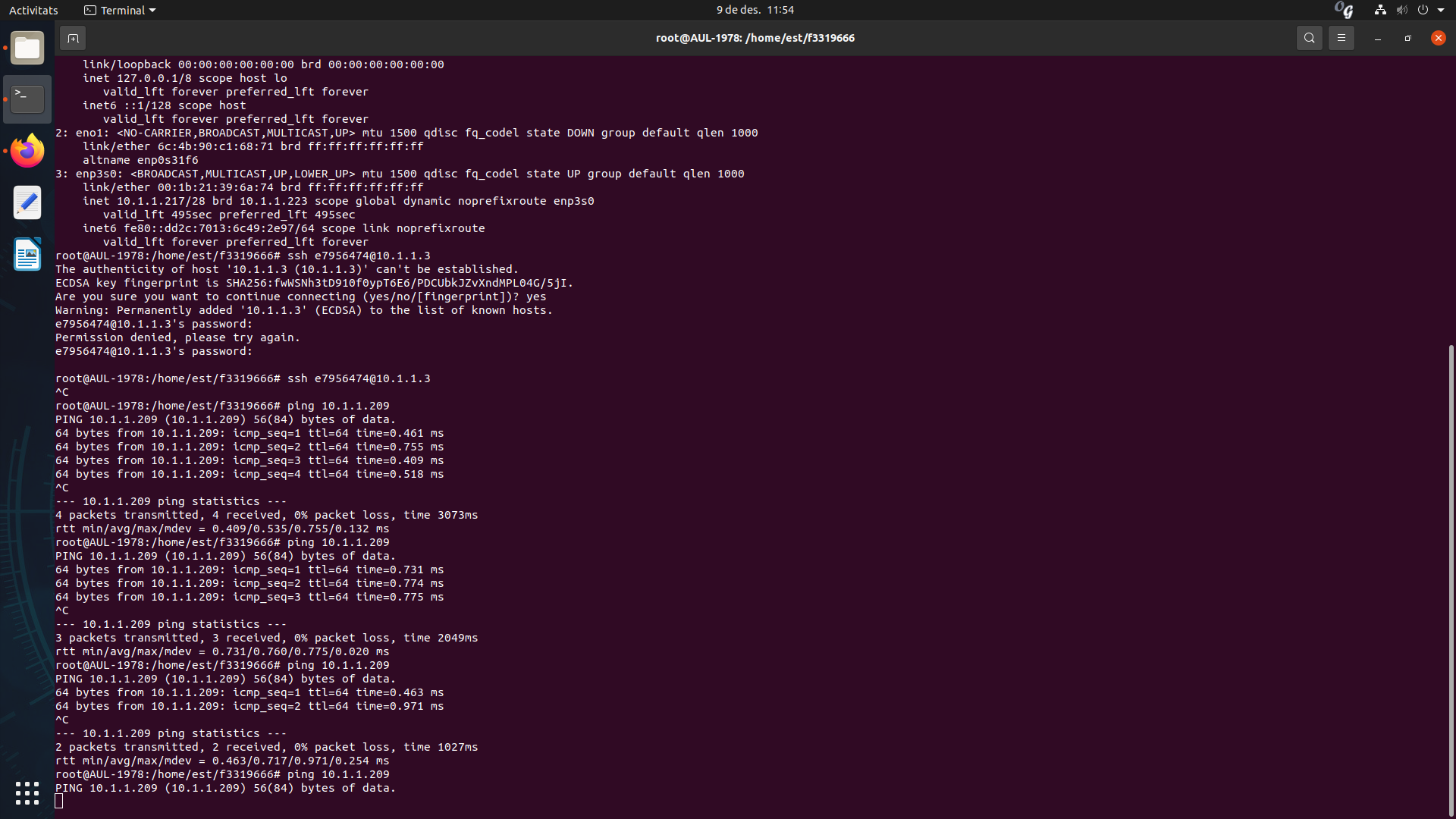
Utilitzem la comanda ssh



I si activem el drop amb el protocol tcp.



PING:



I si desactivem la regla i activem el drop amb el protocol icmp.

A més hem de canviar la cadena del drop de forward a input.

