1 ASIX

**MÒDUL 11: SEGURETAT I ALTA DISPONIBILITAT**

ACTIVITAT 2: Iptables

línea horizontal

# 



**Alumne**: Daniel Mascarilla del Olmo

**Professor**: Sergi Andrés

**Curs**: 1 ASIX

**Centre**: Jaume Viladoms

**ÍNDEX**

[**Exercici 1: Iptables 3**](#_n6x11lfxif98)

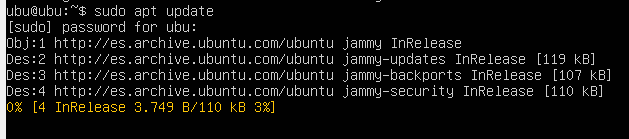
[**Exercici 2: Bloquejar ICMP + permetre TCP port 80 8**](#_46j57n6g7f2c)

[**Exercici 3: ICMP echo request 12**](#_klaxrigwlq6g)

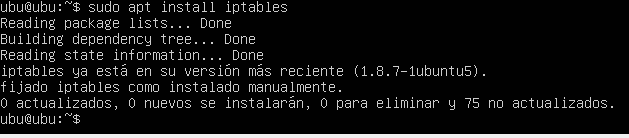
[**Exercici 4: Respondre connexions obertes 17**](#_i9vmg3p9887d)

# **Exercici 1: Iptables**

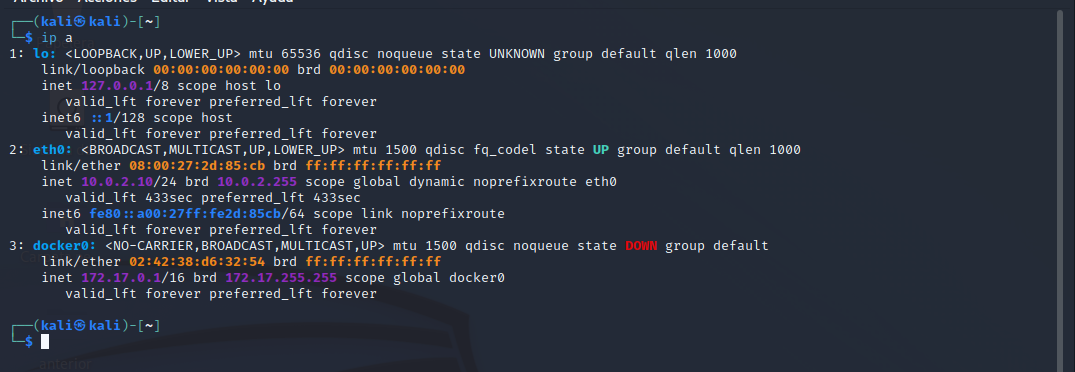
Farem un sudo apt update al Ubuntu:



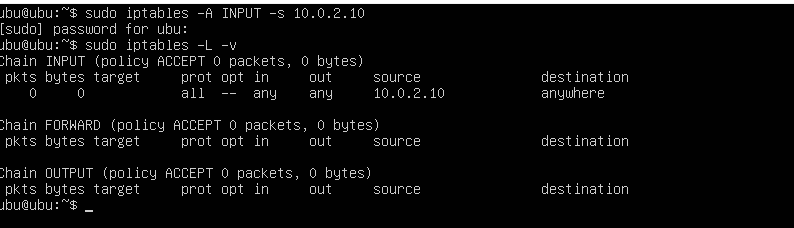
Farem un sudo apt install iptables



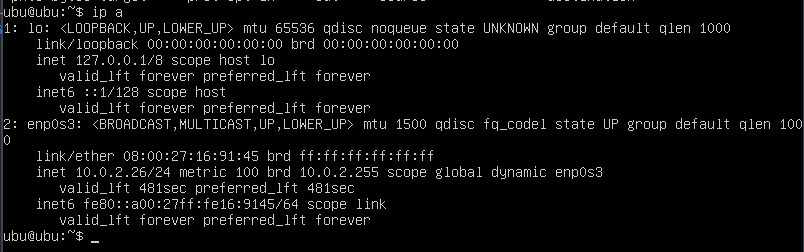
Farem un ip a al kali linux:

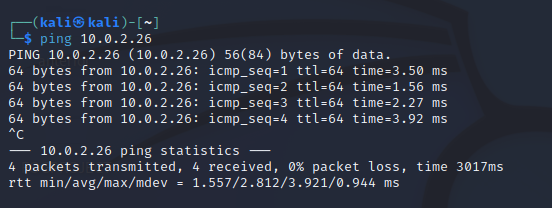


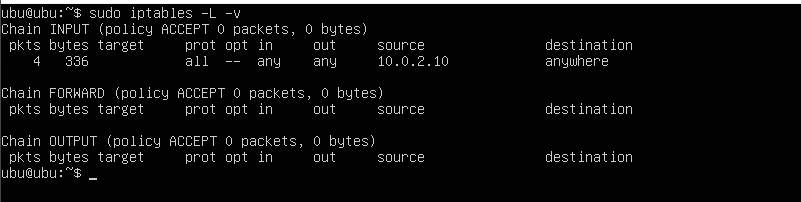
Ara des del Ubuntu Server executarem aquesta comanda:



Agafarem la ip del ubuntu i farem un ping des de kali:





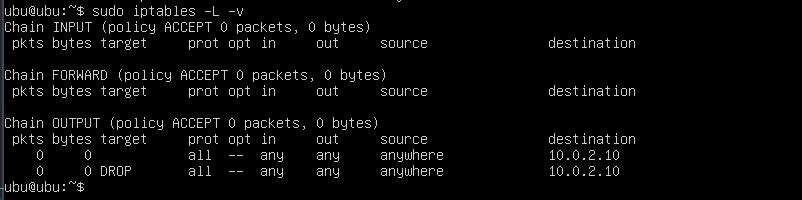
Ara executarem la comanda sudo iptables -L -v

Podem veure que una es de la 10.0.2.10, farem un input de la 1:

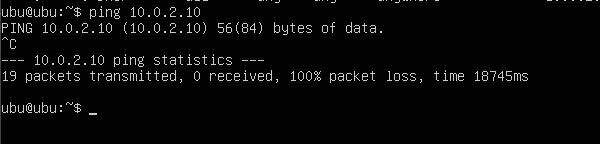


Executarem per fer un output de



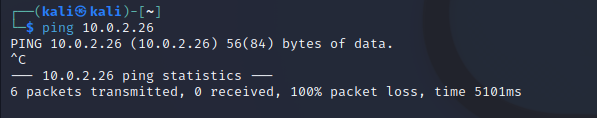


Ara farem un ping des del Ubuntu a Kali:

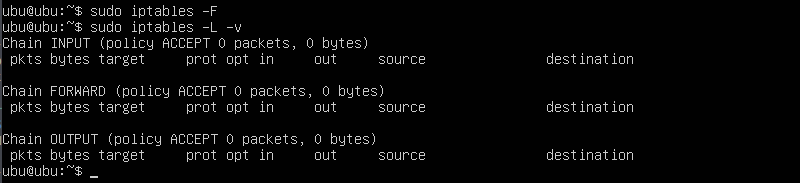


Podem veure que no deixa, rebutja tots els paquets.

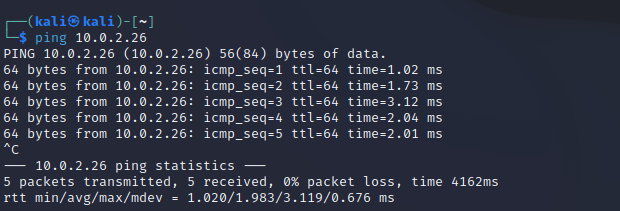
Probem desde kali a Ubuntu:



No deixa, executarem aquesta comanda:

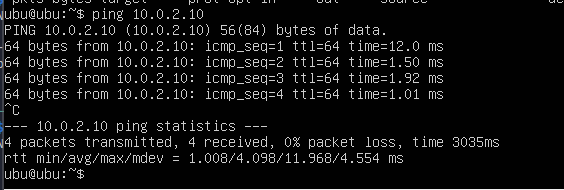


Si tornem a fer un ping:



Ja deixa fer el ping des de kali a ubuntu.

Probarem a la inversa.

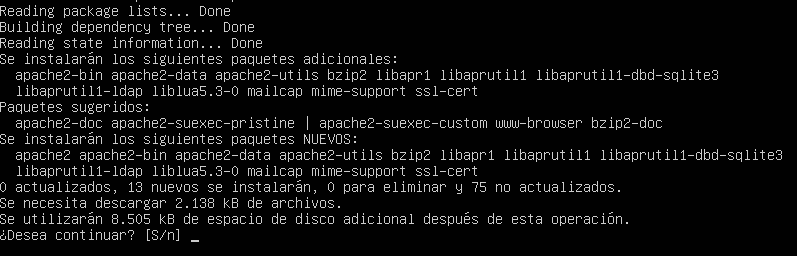


Ja deixa fer els ping.

# Exercici 2: Bloquejar ICMP + permetre TCP port 80

Primer de tot farem un sudo apt install del apache2:

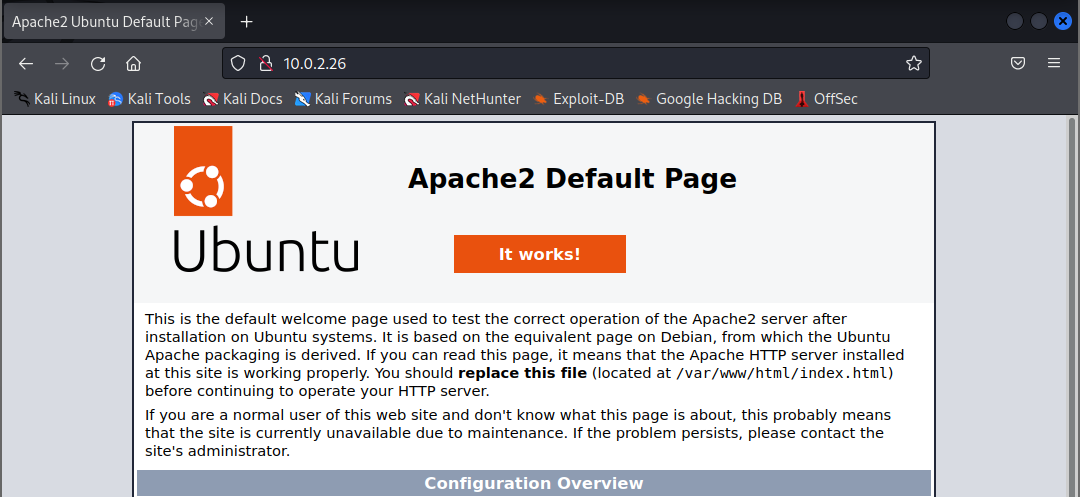




Després farem un systemctl del apache2



Posarem la ip en el navegador del kali linux:



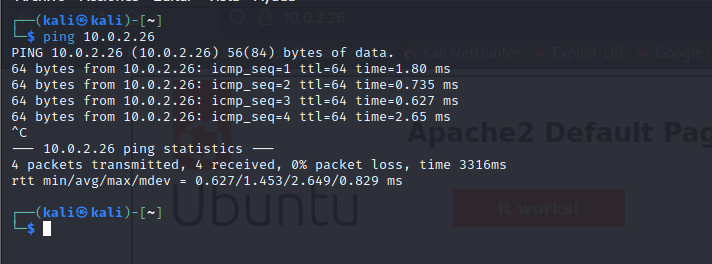
Executarem aquesta comanda:



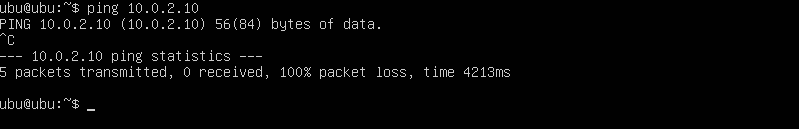
Per bloquejar la resta de entrades:



Comprovarem que podem rebre pings, però no enviar:

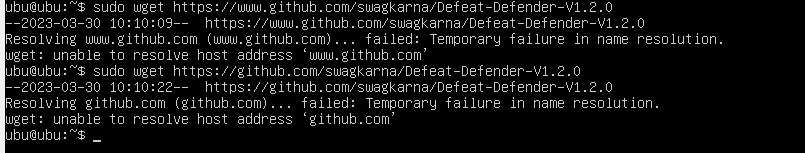


Pot rebre pings,però:



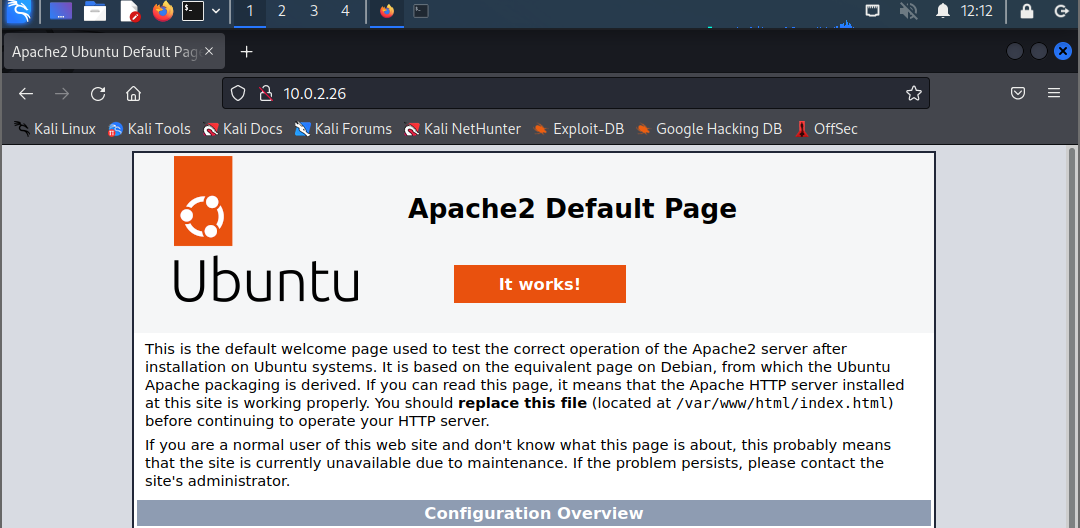
No pot enviar pings.

Probarem de descarregar amb el wget un arxiu:



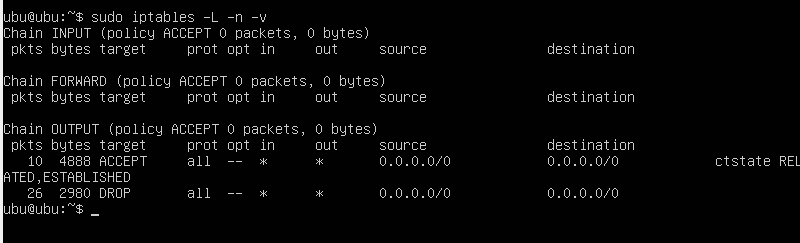
Veiem que no deixa.

Després de aplicar la regla, anirem un altre cop al kali i recarregarem la pàgina de la ip:

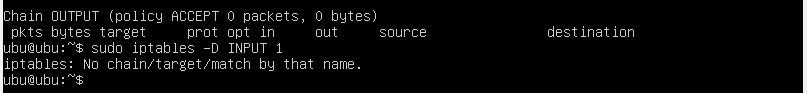


Segueix funcionant.

Mirarem les regles de iptables amb la següent comanda:



Executarem aquesta comanda:



Seguidament farem un flush:



Executarem això



Després farem un drop:



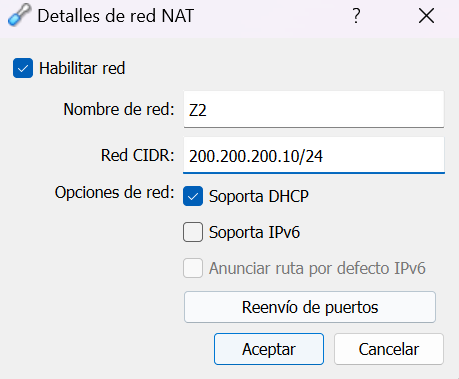
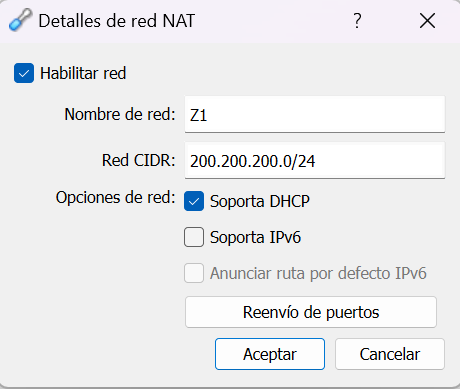
Farem un input del port 443

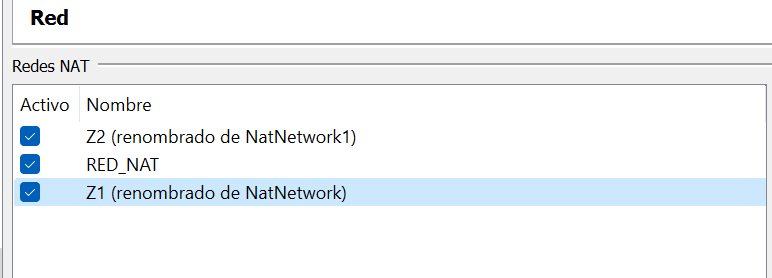


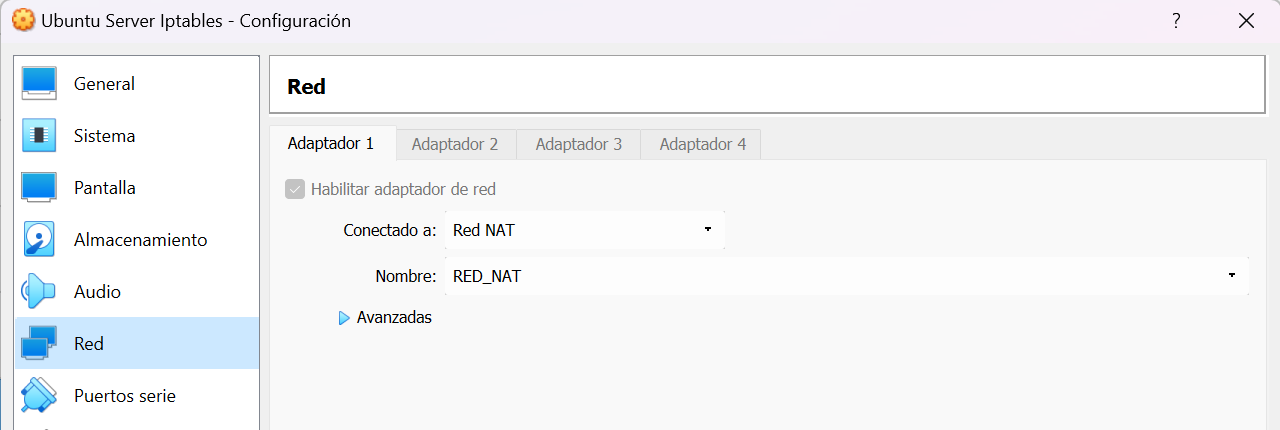
Finalment farem un flush

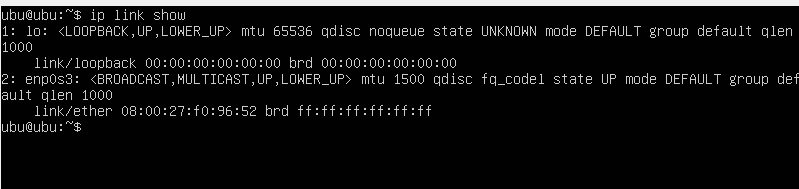


# Exercici 3: ICMP echo request

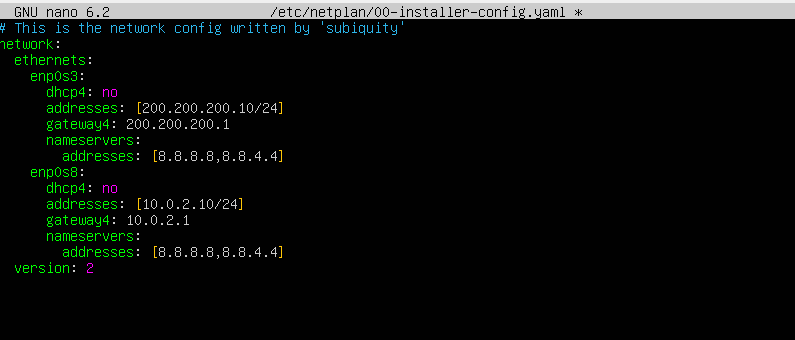




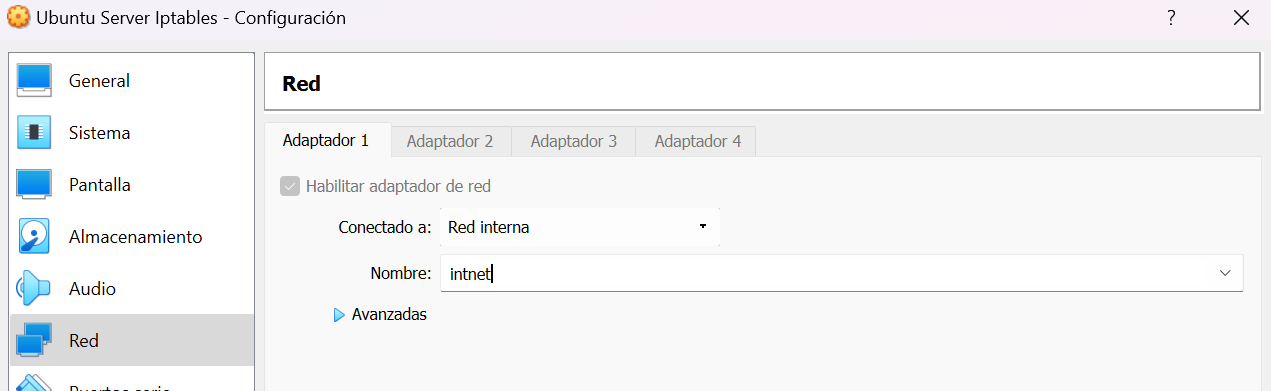






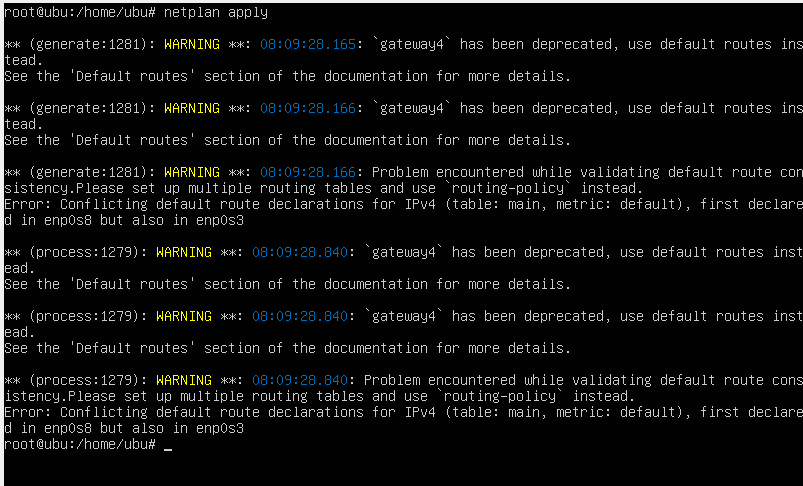


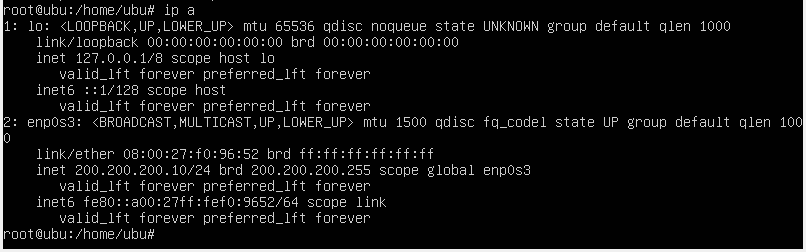
Per l’apartat b:







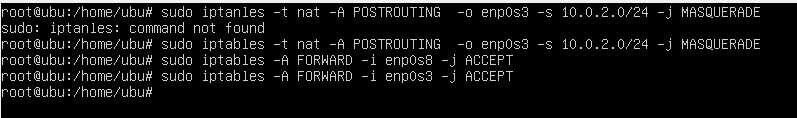




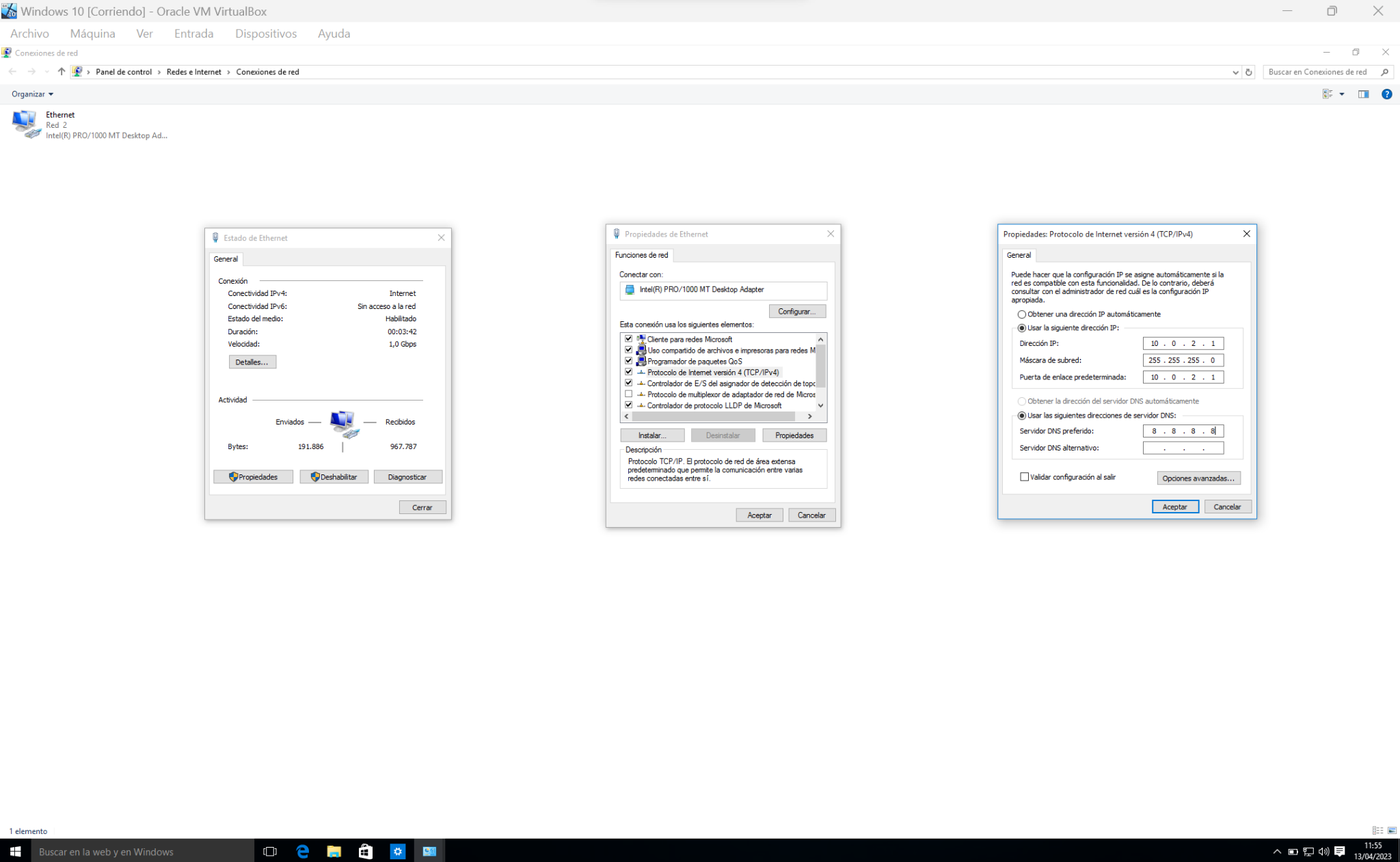
Per l’apartat c:



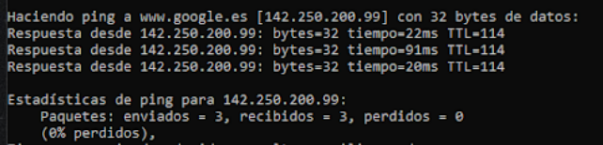




Per l’apartat d:



Per l’apartat e:

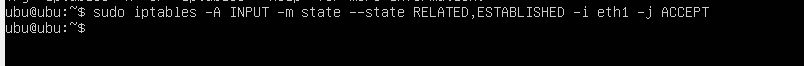


# Exercici 4: Respondre connexions obertes

Bloquejar tot el trànsit de entrada per defecte:



Permetre el trànsit d’entrada ja establert desde la xarxa privada:



Bloquejar tot el trànsit de sortida per defecte



Permetre el transit de sortida desde la xarxa privada:



Fer NAT del trànsit de la xarxa privada a la xarxa RedNAT

****