

*UF5. Tallafocs i Monitoratge
(Pràctica 5.3 IPTables)*

Iptables.....	2
Pràctica 5.3.....	2
Objectius.....	2
Temporització.....	2
Part I: Firewall personal.....	3
Entorn de treball.....	3
Anàlisi IPTables.....	4
Configuració polítiques i IPTables.....	4
Peticions PING.....	6
Servei HTTP.....	6
Serveis SSH i FTP.....	7
Creació SCRIPT.....	7
Part II: Firewall perimetral.....	9
Entorn de treball.....	9
Encaminament.....	10
Configurar Firewall Perimetral.....	11
Serveis HTTP, SSH i FTP.....	12
Creació SCRIPT.....	13

Iptables

Pràctica 5.3

Objectius

Treballar amb les IPTables tant com a Firewall personal com perimetral.

Temporització

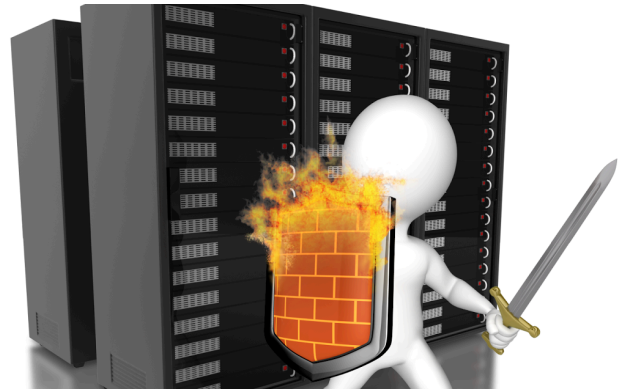
Part I Firewall personal: 4 hores

Part II Firewall perimetral: 4 hores

*UF5. Tallafocs i Monitoratge
(Pràctica 5.3 IPTables)*

Part I: Firewall personal

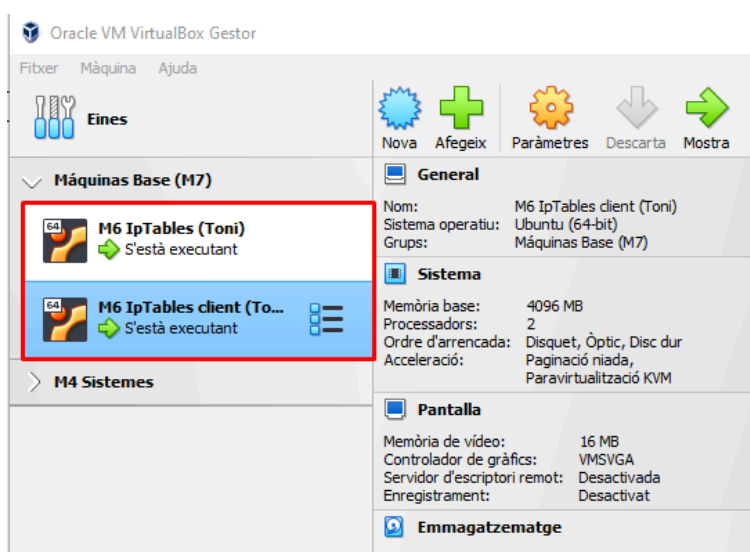
El que farem primer de tot en aquesta pràctica és implementar un firewall personal. Un firewall personal és aquell que s'instal·la dins d'un equip i que només afecta als paquets que arriben i surten d'aquell equip. Per tant aquests firewalls no serveixen per limitar el tràfic a nivell de la xarxa local, només el d'un equip concret. Un exemple de firewall personal és el que s'incorpora amb les versions de Windows per a usuari, com les de Windows 7, Windows 10 o Windows 11. En el cas de Linux, Iptables es pot implementar en qualsevol equip que funcioni amb Linux, ja que està incorporat al propi nucli del sistema operatiu. Així, encara que hi hagi un firewall a nivell de xarxa, sempre es podrà filtrar el que arribi a un equip terminal que funcioni amb alguna distribució de linux.



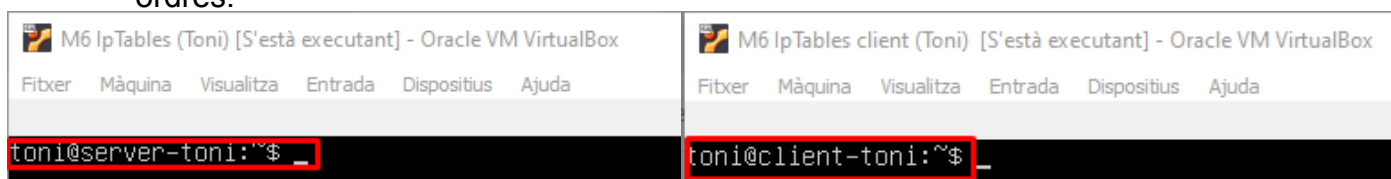
*UF5. Tallafocs i Monitoratge
(Pràctica 5.3 IPTables)*

Entorn de treball

- Crea dues màquines Linux sense interfície gràfica.
 - Fes servir com a interfície de xarxa adaptador pont o NAT.
- Anomena a una d'elles **nomCognomSRV** i l'altra **nomCognomsCLT**. (Si estàs més còmode amb una altra nomenclatura que permeti veure qui ets i diferenciar entre server i client, endavant!)



- Posa aquest nom tant a la finestra de VirtualBox com al prompt de la línia de ordres.



- Instal·la a la màquina servidor els següents serveis (*pots consultar altres Pràctiques i Activitats d'aquesta UF5 si tens dubtes en aquest apartat*)
 - http
 - ftp
 - ssh

*UF5. Tallafocs i Monitoratge
(Pràctica 5.3 IPTables)*

```
M6 IpTables (Toni) [S'està executant] - Oracle VM VirtualBox
Fitxer  Màquina  Visualitza  Entrada  Dispositius  Ajuda

toni@server-toni:~$ sudo su
[sudo] password for toni:
root@server-toni:/home/toni# apt install apache2 vsftpd openssh-server_
```

```
M6 IpTables (Toni) [S'està executant] - Oracle VM VirtualBox
Fitxer  Màquina  Visualitza  Entrada  Dispositius  Ajuda

toni@server-toni:~$ systemctl status vsftpd
• vsftpd.service - vsftpd FTP server
   Loaded: loaded (/lib/systemd/system/vsftpd.service; enabled; vendor preset: enab
   Active: active (running) since Fri 2024-01-26 16:07:13 UTC; 10min ago
   Process: 665 ExecStartPre=/bin/mkdir -p /var/run/vsftpd/empty (code=exited, statu
   Main PID: 672 (vsftpd)
   Tasks: 1 (limit: 4558)
   Memory: 1.8M
   CPU: 18ms
   CGroup: /system.slice/vsftpd.service
           └─672 /usr/sbin/vsftpd /etc/vsftpd.conf

Warning: some journal files were not opened due to insufficient permissions.
toni@server-toni:~$ systemctl status apache2
• apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: ena
   Active: active (running) since Fri 2024-01-26 16:07:13 UTC; 10min ago
   Docs: https://httpd.apache.org/docs/2.4/
   Process: 651 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 731 (apache2)
   Tasks: 55 (limit: 4558)
   Memory: 7.5M
   CPU: 203ms
   CGroup: /system.slice/apache2.service
           └─731 /usr/sbin/apache2 -k start
             └─736 /usr/sbin/apache2 -k start
               └─737 /usr/sbin/apache2 -k start

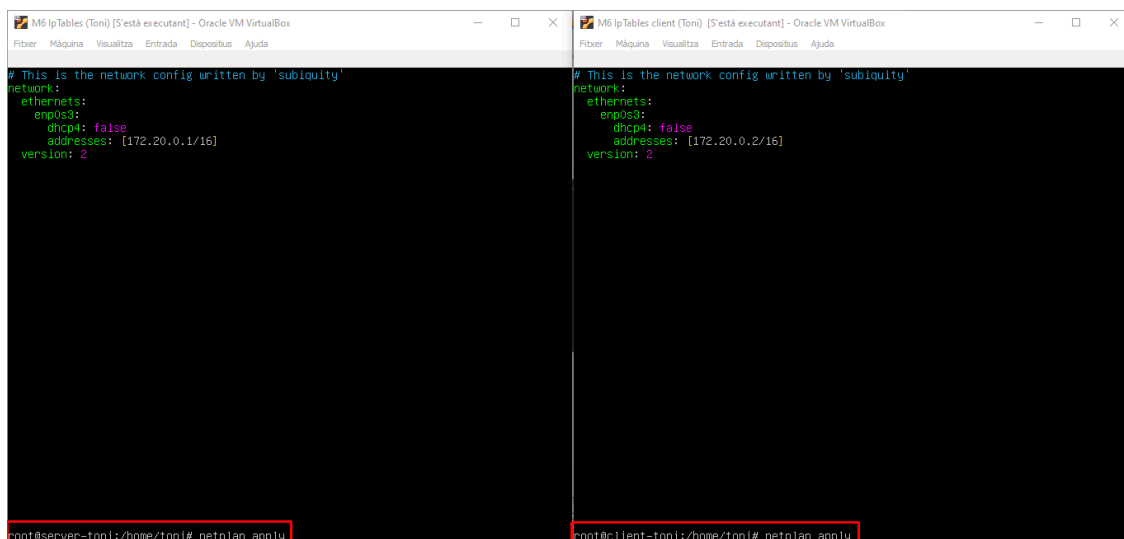
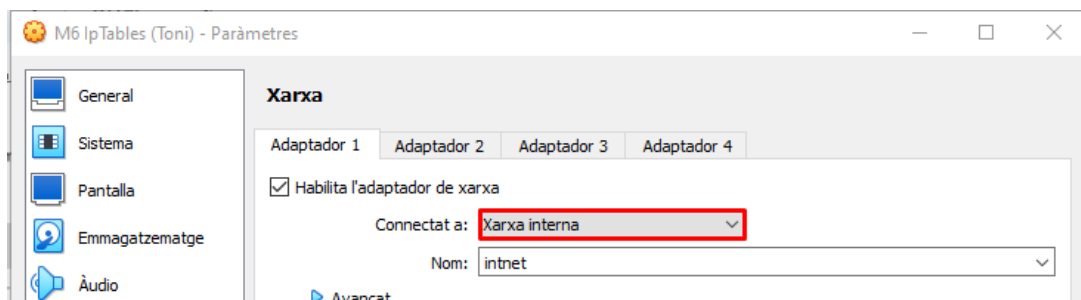
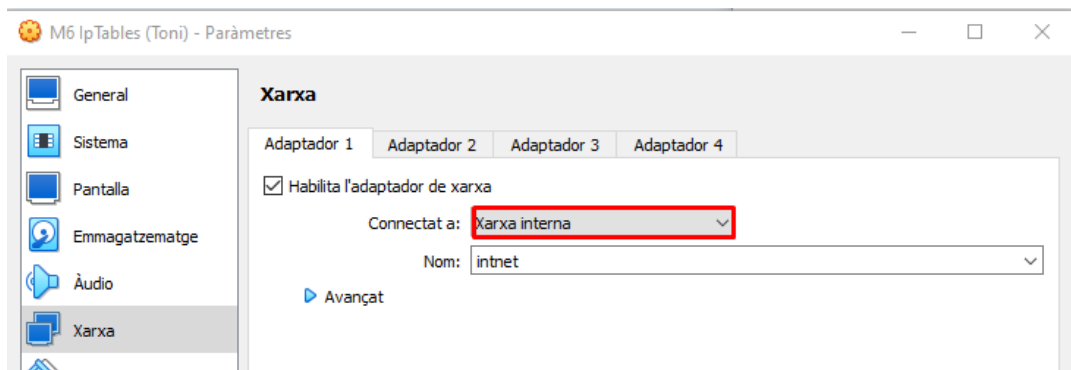
Warning: some journal files were not opened due to insufficient permissions.
toni@server-toni:~$ _
```

```
Warning: some journal files were not opened due to insufficient permissions.
toni@server-toni:~$ systemctl status ssh
• ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled
   Active: active (running) since Fri 2024-01-26 16:07:13 UTC; 11min ago
   Docs: man:sshd(8)
         man:sshd_config(5)
   Process: 665 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 688 (sshd)
   Tasks: 1 (limit: 4558)
   Memory: 3.6M
   CPU: 51ms
   CGroup: /system.slice/ssh.service
           └─688 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Warning: some journal files were not opened due to insufficient permissions.
toni@server-toni:~$ _
```

*UF5. Tallafocs i Monitoratge
(Pràctica 5.3 IPTables)*

- Instal·la el client ftp a la màquina client.
- Posa totes dues màquines en xarxa local i configura manualment les seves IPs.



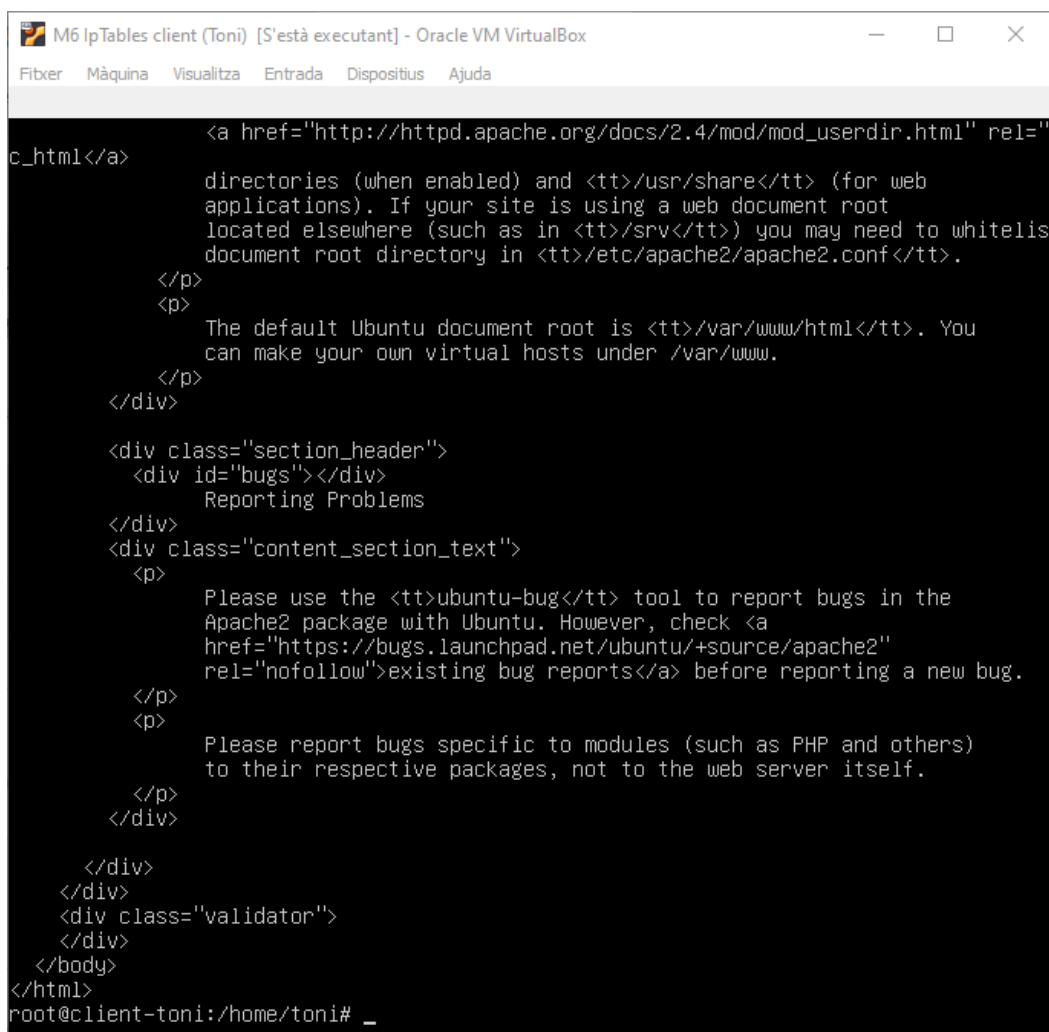
*UF5. Tallafocs i Monitoratge
(Pràctica 5.3 IPTables)*

- Comprova que les dues màquines es fan ping entre elles.

Anàlisis IPtables

- Comprova que des de la màquina client es pot accedir a tots aquests serveis.
 - Per a accedir al servei http fes servir l'ordre curl seguida de la url:

http://ip_servidor



```
M6 IPTables client (Toni) [S'està executant] - Oracle VM VirtualBox
Fiber  Màquina  Visualitza  Entrada  Dispositius  Ajuda

<a href="http://httpd.apache.org/docs/2.4/mod/mod_userdir.html" rel="
c_html</a>
directories (when enabled) and <tt>/usr/share</tt> (for web
applications). If your site is using a web document root
located elsewhere (such as in <tt>/srv</tt>) you may need to whielis
document root directory in <tt>/etc/apache2/apache2.conf</tt>.
</p>
<p>
The default Ubuntu document root is <tt>/var/www/html</tt>. You
can make your own virtual hosts under /var/www.
</p>
</div>
<div class="section_header">
<div id="bugs"></div>
Reporting Problems
</div>
<div class="content_section_text">
<p>
Please use the <tt>ubuntu-bug</tt> tool to report bugs in the
Apache2 package with Ubuntu. However, check <a
href="https://bugs.launchpad.net/ubuntu/+source/apache2"
rel="nofollow">existing bug reports</a> before reporting a new bug.
</p>
<p>
Please report bugs specific to modules (such as PHP and others)
to their respective packages, not to the web server itself.
</p>
</div>
</div>
<div class="validator">
</div>
</body>
</html>
root@client-toni:/home/toni# _
```

*UF5. Tallafocs i Monitoratge
(Pràctica 5.3 IPTables)*

```
M6 IpTables client (Toni) [S'està executant] - Oracle VM VirtualBox
Fitxer  Màquina  Visualitza  Entrada  Dispositius  Ajuda

root@client-toni:/home/toni# ftp 172.20.0.1
Connected to 172.20.0.1.
220 (vsFTPD 3.0.5)
Name (172.20.0.1:toni): toni
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

```
M6 IpTables client (Toni) [S'està executant] - Oracle VM VirtualBox
Fitxer  Màquina  Visualitza  Entrada  Dispositius  Ajuda

Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.15.0-84-generic x86_64)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:        https://ubuntu.com/advantage

System information as of miè 31 ene 2024 18:16:30 UTC

System load:  0.080078125   Processes:            118
Usage of /:    30.3% of 23.45GB Users logged in:       1
Memory usage:  5%          IPv4 address for enp0s3: 172.20.0.1
Swap usage:    0%

* Introducing Expanded Security Maintenance for Applications.
  Receive updates to over 25,000 software packages with your
  Ubuntu Pro subscription. Free for personal use.

  https://ubuntu.com/pro

El mantenimiento de seguridad expandido para Applications está desactivado

Se pueden aplicar 81 actualizaciones de forma inmediata.
Para ver estas actualizaciones adicionales, ejecute: apt list --upgradable

Active ESM Apps para recibir futuras actualizaciones de seguridad adicionales.
Vea https://ubuntu.com/esm o ejecute «sudo pro status»

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Inter
or proxy settings

Last login: Wed Jan 31 18:06:50 2024
toni@server-toni:~$ _
```

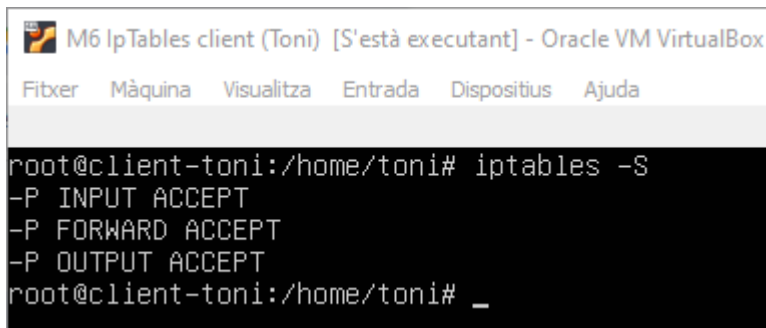
- Comprovem a la màquina client les regles de filtratge que té iptables per defecte:
 - Cal fer servir l'ordre iptables.

*UF5. Tallafocs i Monitoratge
(Pràctica 5.3 IPTables)*

- Cal passar-li l'opció **-L**, que serveix per a consultar el contingut de la taula filter, que és on es guarden les regles de filtratge.
- També és convenient passar els paràmetres **-nv** perquè mostrin més informació sobre els paquets filtrats.

```
root@client-toni:/home/toni# iptables -L -nv
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target      prot opt in      out     source      destination
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target      prot opt in      out     source      destination
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target      prot opt in      out     source      destination
root@client-toni:/home/toni#
```

- Comprova el nom de les cadenes que hi ha definides a la taula filter de iptables, així com la política que tenen definida per defecte.



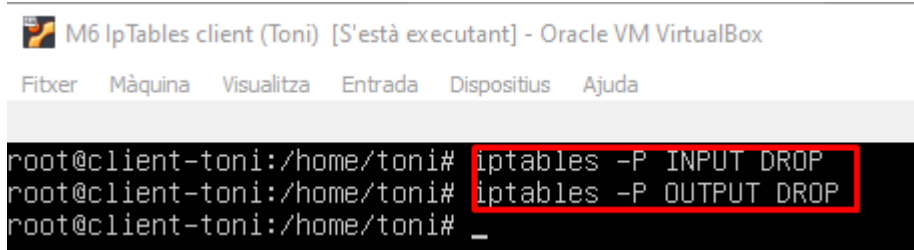
```
root@client-toni:/home/toni# iptables -S
-P INPUT ACCEPT
-P FORWARD ACCEPT
-P OUTPUT ACCEPT
root@client-toni:/home/toni# _
```

Configuració polítiques i IPtables

- **Definim una política per defecte de negació.** És a dir: no es permet que cap paquet amb un origen aliè pugui accedir a l'ordinador ni que cap paquet pugui abandonar-lo. Per a implementar aquesta política per defecte caldrà escriure l'ordre iptables de la següent manera:
- Amb l'ordre que permet definir les polítiques per defecte que és **-P**, de policy.

*UF5. Tallafocs i Monitoratge
(Pràctica 5.3 IPTables)*

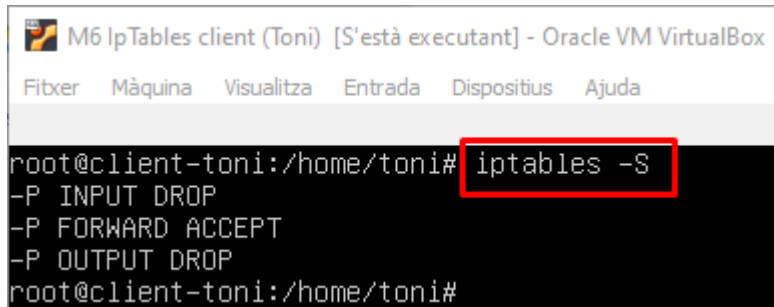
- El nom de la cadena de filtratge, tant la que filtra els paquets que entren a l'ordinador, **INPUT**, com la que filtra els que en surten, **OUTPUT**.
- En tercer lloc cal posar la política que es vol establir, **ACCEPT** és per a definir una política que accepta els paquets per defecte, i **DROP** per a una que els rebutja.



```
M6 IpTables client (Toni) [S'està executant] - Oracle VM VirtualBox
Fitxer  Màquina  Visualitza  Entrada  Dispositius  Ajuda

root@client-toni:/home/toni# iptables -P INPUT DROP
root@client-toni:/home/toni# iptables -P OUTPUT DROP
root@client-toni:/home/toni# _
```

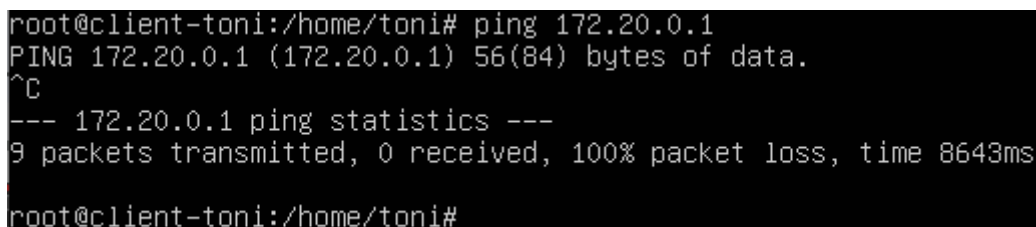
- Comprova a la màquina client que s'ha canviat la política per defecte de les cadenes **INPUT** i **OUTPUT**.



```
M6 IpTables client (Toni) [S'està executant] - Oracle VM VirtualBox
Fitxer  Màquina  Visualitza  Entrada  Dispositius  Ajuda

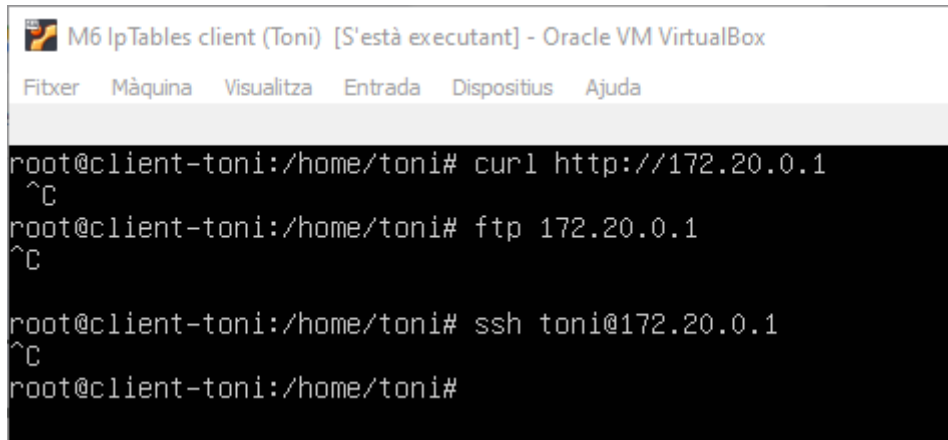
root@client-toni:/home/toni# iptables -S
-P INPUT DROP
-P FORWARD ACCEPT
-P OUTPUT DROP
root@client-toni:/home/toni#
```

- Torna a provar de fer ping des de la màquina client al servidor, així com a accedir als serveis **WEB**, **FTP** i **SSH**.



```
root@client-toni:/home/toni# ping 172.20.0.1
PING 172.20.0.1 (172.20.0.1) 56(84) bytes of data.
^C
--- 172.20.0.1 ping statistics ---
9 packets transmitted, 0 received, 100% packet loss, time 8643ms
root@client-toni:/home/toni#
```

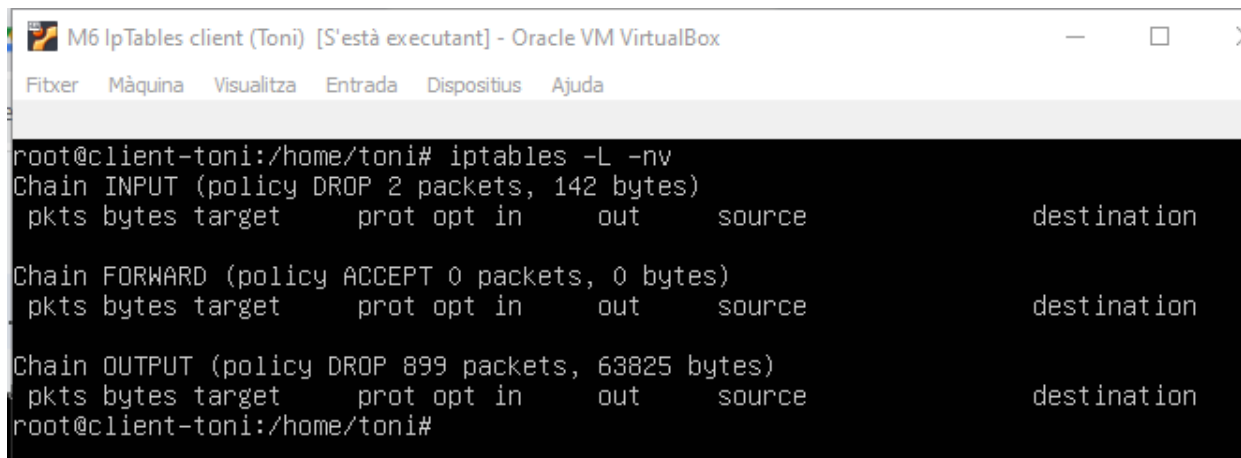
*UF5. Tallafocs i Monitoratge
(Pràctica 5.3 IPTables)*



```
M6 IpTables client (Toni) [S'està executant] - Oracle VM VirtualBox
Fitxer  Màquina  Visualitza  Entrada  Dispositius  Ajuda

root@client-toni:/home/toni# curl http://172.20.0.1
^C
root@client-toni:/home/toni# ftp 172.20.0.1
^C
root@client-toni:/home/toni# ssh toni@172.20.0.1
^C
root@client-toni:/home/toni#
```

- Escriu l'ordre **iptables -L -nv** per a consultar els paquets que iptables ha descartat.



```
M6 IpTables client (Toni) [S'està executant] - Oracle VM VirtualBox
Fitxer  Màquina  Visualitza  Entrada  Dispositius  Ajuda

root@client-toni:/home/toni# iptables -L -nv
Chain INPUT (policy DROP 2 packets, 142 bytes)
  pkts bytes target     prot opt in     out     source         destination
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
  pkts bytes target     prot opt in     out     source         destination
Chain OUTPUT (policy DROP 899 packets, 63825 bytes)
  pkts bytes target     prot opt in     out     source         destination
root@client-toni:/home/toni#
```

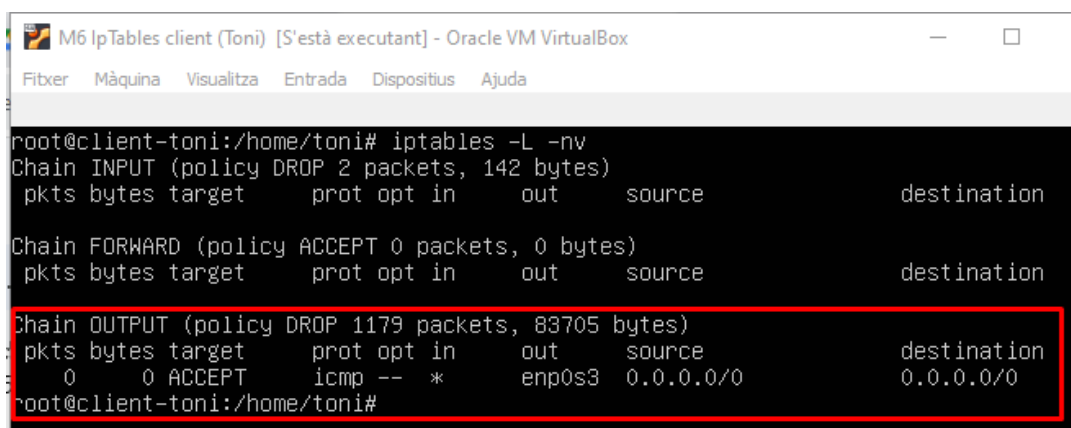
- Configurarem iptables perquè permeti fer ping. Cal escriure l'ordre iptables amb les següents ordres i paràmetres:
 - L'ordre emprant el paràmetre **-A** permet afegir regles per a filtrar els paquets, seguida del nom de la cadena per a la qual es vol aplicar la regla, **INPUT**, **OUTPUT** o **FORWARD**.
 - Posarem la cadena **OUTPUT** per a permetre que surtin les peticions de ping.

*UF5. Tallafocs i Monitoratge
(Pràctica 5.3 IPTables)*

- El paràmetre **-o**, de output, que indica la interfície per la qual es vol que surti el paquet, en aquest cas la petició ping al servidor.
- El paràmetre **-p**, de protocol, seguida del nom del protocol que estem filtrant, en aquest cas icmp, que és el que fa servir per a fer pings.
- El paràmetre **-j**, de jump, que indica que fer amb el paquet si aquest aconsegueix els criteris indicats a la regla, seguit del que es vol fer amb ell, acceptar-lo, **ACCEPT**, o denegar-lo, **DROP**.

```
root@client-toni:/home/toni# iptables -A OUTPUT -o enp0s3 -p icmp -j ACCEPT
root@client-toni:/home/toni#
```

- Escriu l'ordre **iptables -L -nv** i comprova com ha quedat enregistrada la regla a la cadena.

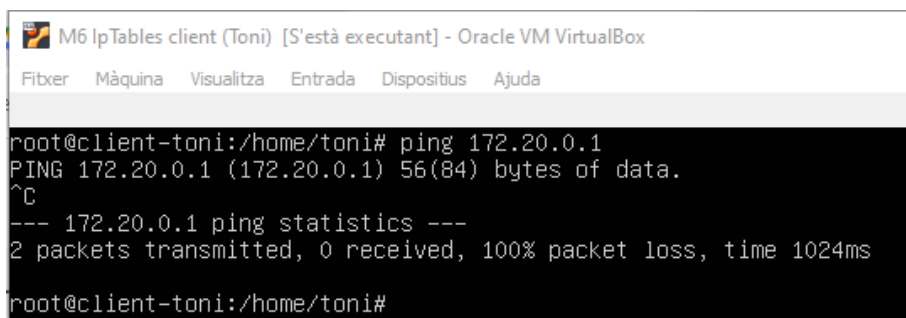


```
root@client-toni:/home/toni# iptables -L -nv
Chain INPUT (policy DROP 2 packets, 142 bytes)
 pkts bytes target    prot opt in     out     source   destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source   destination

Chain OUTPUT (policy DROP 1179 packets, 83705 bytes)
 pkts bytes target    prot opt in     out     source   destination
    0      0 ACCEPT    icmp -- *      enp0s3  0.0.0.0/0  0.0.0.0/0
root@client-toni:/home/toni#
```

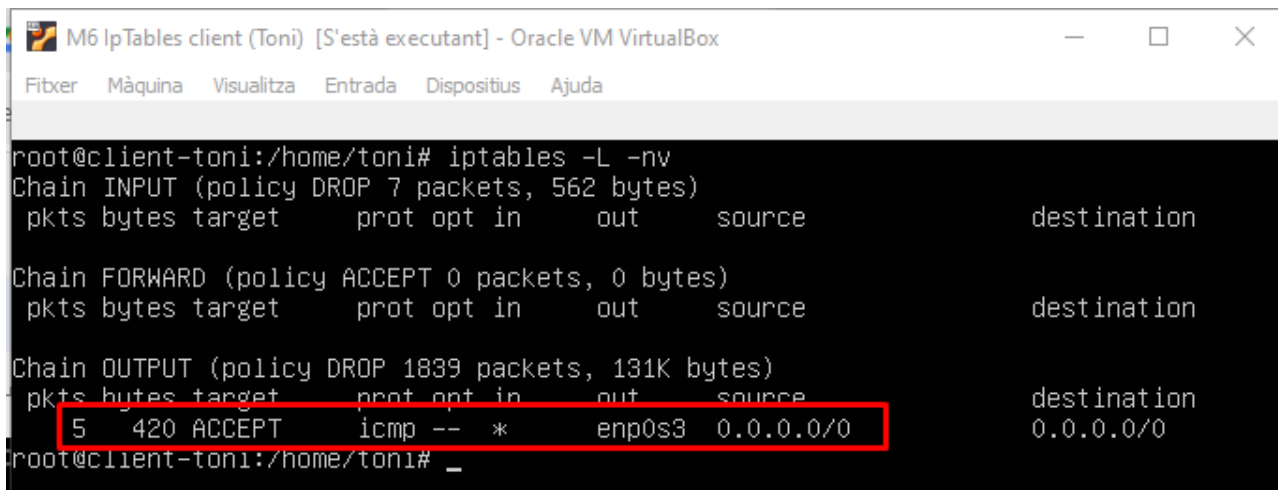
- Fes ping a la màquina servidor per comprovar si ara es pot fer.



```
root@client-toni:/home/toni# ping 172.20.0.1
PING 172.20.0.1 (172.20.0.1) 56(84) bytes of data.
^C
--- 172.20.0.1 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1024ms
root@client-toni:/home/toni#
```

UF5. Tallafocs i Monitoratge
(Pràctica 5.3 IPTables)

- Torna es fer **iptables -L -nv** i comprova quina informació apareix a la cadena **OUTPUT** i quina a la cadena **INPUT**.



```
root@client-toni:/home/toni# iptables -L -nv
Chain INPUT (policy DROP 7 packets, 562 bytes)
  pkts bytes target     prot opt in     out     source         destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
  pkts bytes target     prot opt in     out     source         destination

Chain OUTPUT (policy DROP 1839 packets, 131K bytes)
  pkts bytes target     prot opt in     out     source         destination
  5    420 ACCEPT     icmp -- *      enp0s3  0.0.0.0/0      0.0.0.0/0
root@client-toni:/home/toni# _
```

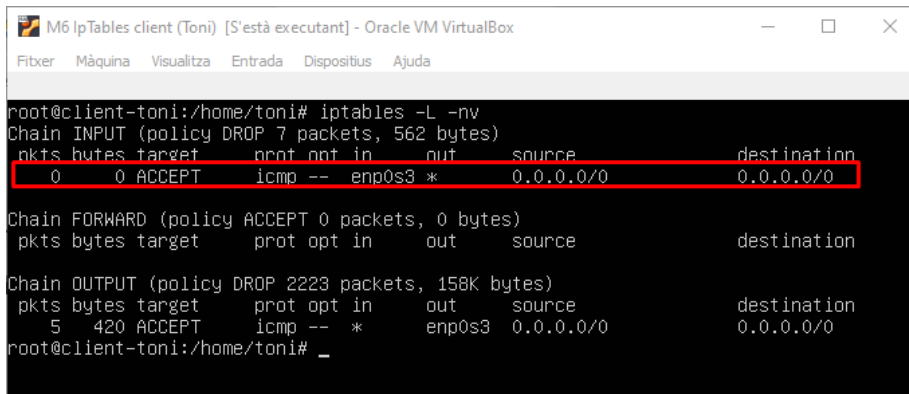
Peticions PING

- Perquè es pugui fer ping, és necessari que a més de permetre la sortida de les respostes de ping també es permetin les peticions de ping que arriben al servidor. Per a fer això cal escriure una ordre com la que permet la sortida de les peticions de ping però amb les següents modificacions:
- La cadena a la que s'afegirà aquesta regla és **INPUT**, ja que es tracta de filtrar paquets que entren a la màquina.
 - El paràmetre per a indicar la interfície serà **-i**, d'**INPUT**, doncs cal indicar per quina interfície es vol fer entrar el paquet.

```
root@client-toni:/home/toni# iptables -A INPUT -i enp0s3 -p icmp -j ACCEPT
root@client-toni:/home/toni#
```

UF5. Tallafocs i Monitoratge
(Pràctica 5.3 IPTables)

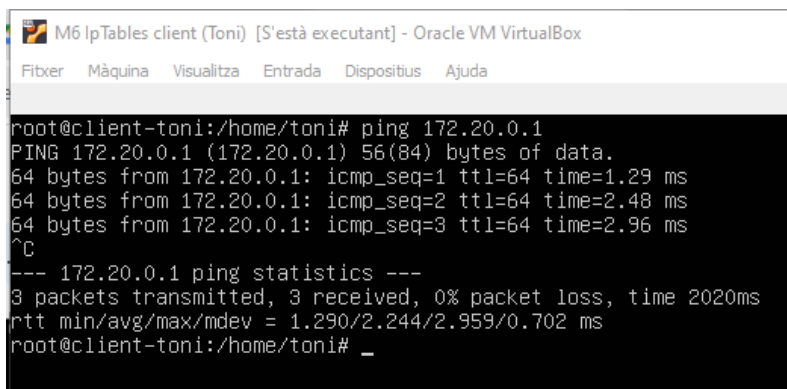
- Comprova que s'ha afegit aquesta regla a la cadena **INPUT** i també que ara ja es pot fer ping.



```
root@client-toni:/home/toni# iptables -L -nv
Chain INPUT (policy DROP 7 packets, 562 bytes)
 pkts bytes target     prot opt in     out     source            destination
  0      0 ACCEPT     icmp -- enp0s3 *        0.0.0.0/0         0.0.0.0/0

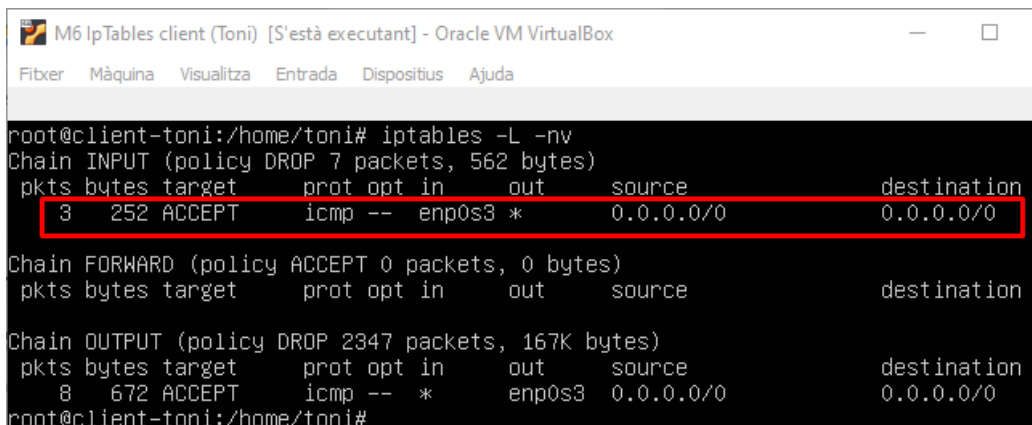
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source            destination

Chain OUTPUT (policy DROP 2223 packets, 158K bytes)
 pkts bytes target     prot opt in     out     source            destination
  5    420 ACCEPT     icmp -- *        enp0s3  0.0.0.0/0         0.0.0.0/0
root@client-toni:/home/toni#
```



```
root@client-toni:/home/toni# ping 172.20.0.1
PING 172.20.0.1 (172.20.0.1) 56(84) bytes of data.
64 bytes from 172.20.0.1: icmp_seq=1 ttl=64 time=1.29 ms
64 bytes from 172.20.0.1: icmp_seq=2 ttl=64 time=2.48 ms
64 bytes from 172.20.0.1: icmp_seq=3 ttl=64 time=2.96 ms
^C
--- 172.20.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2020ms
rtt min/avg/max/mdev = 1.290/2.244/2.959/0.702 ms
root@client-toni:/home/toni#
```

- Observa també, amb **iptables -L -nv**, el nombre de paquets que s'han acceptat amb les dues regles que s'han creat.



```
root@client-toni:/home/toni# iptables -L -nv
Chain INPUT (policy DROP 7 packets, 562 bytes)
 pkts bytes target     prot opt in     out     source            destination
  3    252 ACCEPT     icmp -- enp0s3 *        0.0.0.0/0         0.0.0.0/0

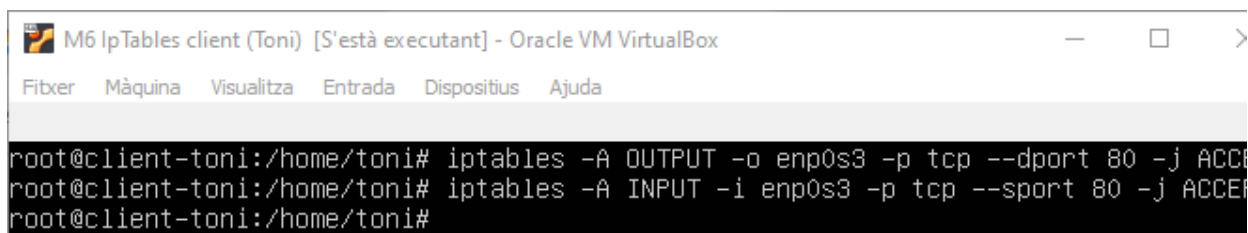
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source            destination

Chain OUTPUT (policy DROP 2347 packets, 167K bytes)
 pkts bytes target     prot opt in     out     source            destination
  8    672 ACCEPT     icmp -- *        enp0s3  0.0.0.0/0         0.0.0.0/0
root@client-toni:/home/toni#
```

*UF5. Tallafocs i Monitoratge
(Pràctica 5.3 IPTables)*

Servei HTTP

- Procedim a habilitar amb iptables el tràfic **http**. Caldrà escriure dues regles, com en el cas dels pings, una per a permetre els paquets que surten i una altra pels que entren de la següent manera:
- L'opció **-A** seguida de **INPUT** i **OUTPUT**, així com el paràmetre **-i** o **-o** seguida de la interfície tal com s'ha fet n els cas del filtratge dels pings.
 - El valor del paràmetre **-p** ha de ser ara **TCP**, que és el protocol de transport que fa servir **HTTP**.
 - En el cas de la regla que permet la sortida dels paquets cal especificar l'extensió **--dport**, que indica el port destí, és a dir el servei al qual s'envia el paquet, en aquest cas serà el **port 80**, doncs es tracta d'un servidor web. Pel que fa la regla d'entrada cal especificar, **--sport**, de source port, port origen, seguit del port del servei que envia els paquets cap als clients.
 - El paràmetre **-j** indicant què es vol fer amb el paquet. En ambdues regles especificarem que els volem acceptar.

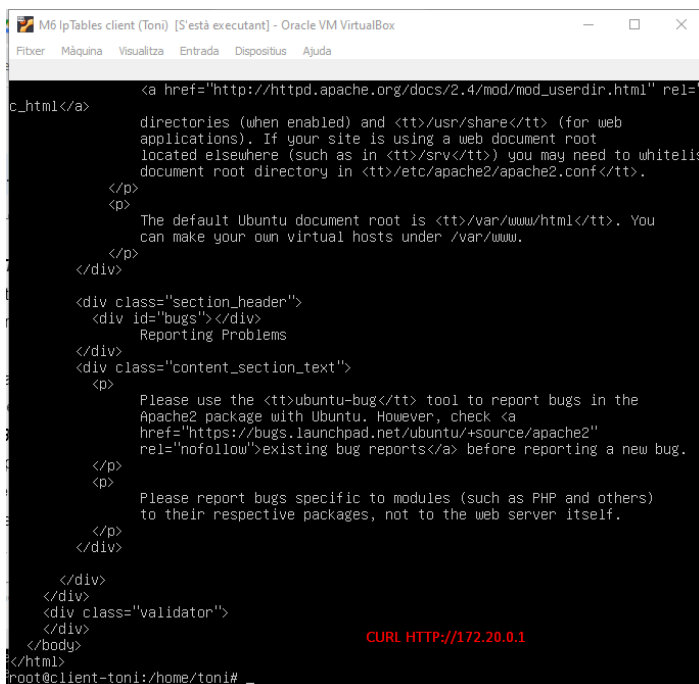


```
M6 IpTables client (Toni) [S'està executant] - Oracle VM VirtualBox
Fitxer  Màquina  Visualitza  Entrada  Dispositius  Ajuda

root@client-toni:/home/toni# iptables -A OUTPUT -o enp0s3 -p tcp --dport 80 -j ACCEPT
root@client-toni:/home/toni# iptables -A INPUT -i enp0s3 -p tcp --sport 80 -j ACCEPT
root@client-toni:/home/toni#
```

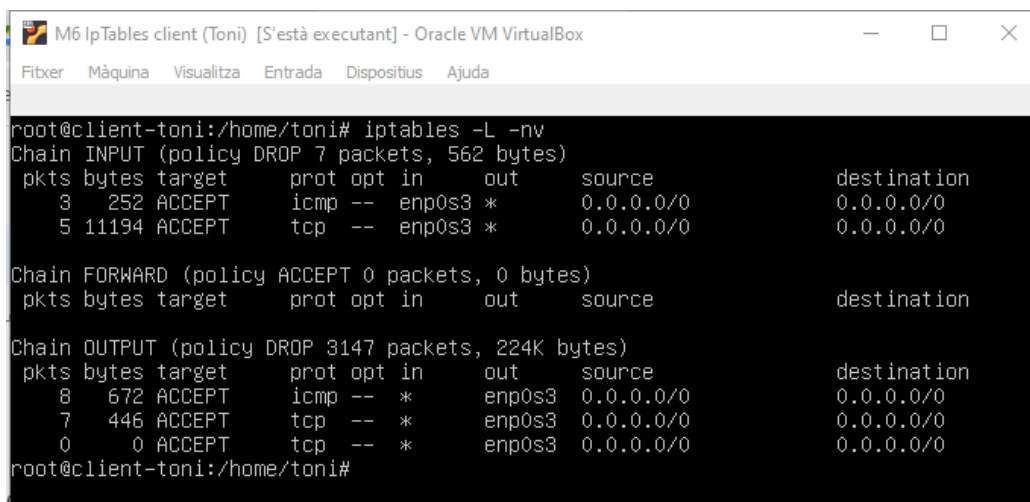
UF5. Tallafocs i Monitoratge
(Pràctica 5.3 IPTables)

- Comprova que ara ja es pot accedir al servei web de la màquina client i que el filtratge d'aquests paquets han quedat recollits a iptables.



```
M6 IpTables client (Toni) [S'està executant] - Oracle VM VirtualBox
Fitxer Màquina Visualitza Entrada Dispositius Ajuda

<a href="http://httpd.apache.org/docs/2.4/mod/mod_userdir.html" rel="
c_html</a>
directories (when enabled) and <tt>/usr/share</tt> (for web
applications). If your site is using a web document root
located elsewhere (such as in <tt>/srv</tt>) you may need to whiteliss
document root directory in <tt>/etc/apache2/apache2.conf</tt>.
</p>
<p>
The default Ubuntu document root is <tt>/var/www/html</tt>. You
can make your own virtual hosts under /var/www.
</p>
</div>
<div class="section_header">
<div id="bugs"></div>
Reporting Problems
</div>
<div class="content_section_text">
<p>
Please use the <tt>ubuntu-bug</tt> tool to report bugs in the
Apache2 package with Ubuntu. However, check <a
href="https://bugs.launchpad.net/ubuntu/+source/apache2"
rel="nofollow">existing bug reports</a> before reporting a new bug.
</p>
<p>
Please report bugs specific to modules (such as PHP and others)
to their respective packages, not to the web server itself.
</p>
</div>
</div>
<div class="validator">
</div>
</body>
</html>
root@client-toni:/home/toni#
```



```
M6 IpTables client (Toni) [S'està executant] - Oracle VM VirtualBox
Fitxer Màquina Visualitza Entrada Dispositius Ajuda

root@client-toni:/home/toni# iptables -L -nv
Chain INPUT (policy DROP 7 packets, 562 bytes)
 pkts bytes target    prot opt in     out     source    destination
   3   252 ACCEPT    icmp -- enp0s3 *      0.0.0.0/0  0.0.0.0/0
   5 11194 ACCEPT    tcp  -- enp0s3 *      0.0.0.0/0  0.0.0.0/0

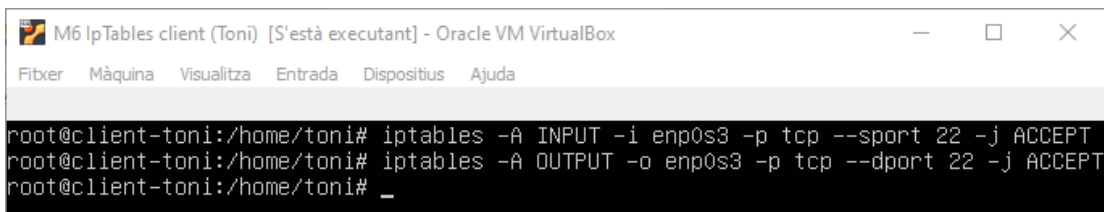
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source    destination

Chain OUTPUT (policy DROP 3147 packets, 224K bytes)
 pkts bytes target    prot opt in     out     source    destination
   8   672 ACCEPT    icmp -- *      enp0s3  0.0.0.0/0  0.0.0.0/0
   7   446 ACCEPT    tcp  -- *      enp0s3  0.0.0.0/0  0.0.0.0/0
   0    0 ACCEPT    tcp  -- *      enp0s3  0.0.0.0/0  0.0.0.0/0
root@client-toni:/home/toni#
```


*UF5. Tallafocs i Monitoratge
(Pràctica 5.3 IPTables)*

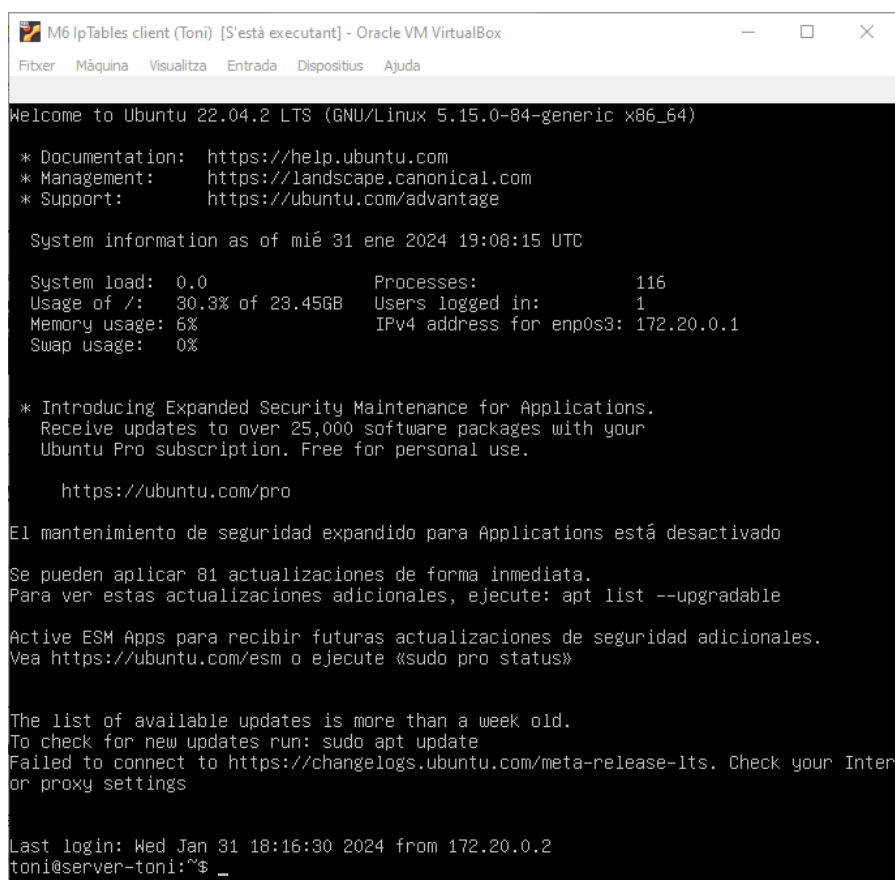
Serveis SSH i FTP

- Habilita el servei **SSH**. Tingues en compte que aquest servei fa servir el protocol **TCP** i el **port 22**.
 - Comprova com ha quedat enregistrat el filtratge d'aquests paquets a iptables.



```
root@client-toni:/home/toni# iptables -A INPUT -i enp0s3 -p tcp --sport 22 -j ACCEPT
root@client-toni:/home/toni# iptables -A OUTPUT -o enp0s3 -p tcp --dport 22 -j ACCEPT
root@client-toni:/home/toni# _
```

```
root@client-toni:/home/toni# ssh toni@172.20.0.1_
```



```
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.15.0-84-generic x86_64)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:        https://ubuntu.com/advantage

System information as of mié 31 ene 2024 19:08:15 UTC

System load:  0.0               Processes:            116
Usage of /:   30.3% of 23.45GB   Users logged in:     1
Memory usage: 6%               IPv4 address for enp0s3: 172.20.0.1
Swap usage:   0%

* Introducing Expanded Security Maintenance for Applications.
  Receive updates to over 25,000 software packages with your
  Ubuntu Pro subscription. Free for personal use.

  https://ubuntu.com/pro

El mantenimiento de seguridad expandido para Applications está desactivado

Se pueden aplicar 81 actualizaciones de forma inmediata.
Para ver estas actualizaciones adicionales, ejecute: apt list --upgradable

Active ESM Apps para recibir futuras actualizaciones de seguridad adicionales.
Vea https://ubuntu.com/esm o ejecute «sudo pro status»

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Inter
or proxy settings

Last login: Wed Jan 31 18:16:30 2024 from 172.20.0.2
toni@server-toni:~$ _
```

UF5. Tallafocs i Monitoratge
(Pràctica 5.3 IPTables)

```
root@client-toni:/home/toni# iptables -L -nv
Chain INPUT (policy DROP 2 packets, 168 bytes)
  pkts bytes target     prot opt in     out     source            destination
    2   168 ACCEPT     icmp -- enp0s3 *      0.0.0.0/0         0.0.0.0/0
    5 11194 ACCEPT     tcp  -- enp0s3 *      0.0.0.0/0         0.0.0.0/0
    30 5953  ACCEPT     tcp  -- enp0s3 *      0.0.0.0/0         0.0.0.0/0
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
  pkts bytes target     prot opt in     out     source            destination
Chain OUTPUT (policy DROP 988 packets, 70168 bytes)
  pkts bytes target     prot opt in     out     source            destination
   36 4573 ACCEPT     tcp  -- *      enp0s3 0.0.0.0/0         0.0.0.0/0
    4   336 ACCEPT     icmp -- *      enp0s3 0.0.0.0/0         0.0.0.0/0
    7   446 ACCEPT     tcp  -- *      enp0s3 0.0.0.0/0         0.0.0.0/0
    0     0 ACCEPT     tcp  -- *      enp0s3 0.0.0.0/0         0.0.0.0/0
root@client-toni:/home/toni# _
```

- Habilita el servei **FTP**. Aquest servei també fa servir el protocol tcp, però emprava dos ports, el **21** per a enviar l'ordre i el **20** per les dades.
- Torna a comprovar, amb **iptables -L -nv**, el filtratge que iptables ha fet d'aquests paquets.

```
root@client-toni:/home/toni# iptables -A INPUT -i enp0s3 -p tcp --sport 21 -j ACCEPT
root@client-toni:/home/toni# iptables -A INPUT -i enp0s3 -p tcp --sport 20 -j ACCEPT
root@client-toni:/home/toni# iptables -A OUTPUT -o enp0s3 -p tcp --dport 21 -j ACCEPT
root@client-toni:/home/toni# iptables -A OUTPUT -o enp0s3 -p tcp --dport 20 -j ACCEPT
root@client-toni:/home/toni#
```

```
root@client-toni:/home/toni# iptables -A INPUT -i enp0s3 -p tcp --sport 21 -j ACCEPT
root@client-toni:/home/toni# iptables -A INPUT -i enp0s3 -p tcp --sport 20 -j ACCEPT
root@client-toni:/home/toni# iptables -A OUTPUT -o enp0s3 -p tcp --dport 21 -j ACCEPT
root@client-toni:/home/toni# iptables -A OUTPUT -o enp0s3 -p tcp --dport 20 -j ACCEPT
root@client-toni:/home/toni# iptables -L -nv
Chain INPUT (policy DROP 2 packets, 168 bytes)
  pkts bytes target     prot opt in     out     source            destination
    2   168 ACCEPT     icmp -- enp0s3 *      0.0.0.0/0         0.0.0.0/0
    5 11194 ACCEPT     tcp  -- enp0s3 *      0.0.0.0/0         0.0.0.0/0
    30 5953  ACCEPT     tcp  -- enp0s3 *      0.0.0.0/0         0.0.0.0/0
    0     0 ACCEPT     tcp  -- enp0s3 *      0.0.0.0/0         0.0.0.0/0
    0     0 ACCEPT     tcp  -- enp0s3 *      0.0.0.0/0         0.0.0.0/0
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
  pkts bytes target     prot opt in     out     source            destination
Chain OUTPUT (policy DROP 1188 packets, 84368 bytes)
  pkts bytes target     prot opt in     out     source            destination
   36 4573 ACCEPT     tcp  -- *      enp0s3 0.0.0.0/0         0.0.0.0/0
    4   336 ACCEPT     icmp -- *      enp0s3 0.0.0.0/0         0.0.0.0/0
    7   446 ACCEPT     tcp  -- *      enp0s3 0.0.0.0/0         0.0.0.0/0
    0     0 ACCEPT     tcp  -- *      enp0s3 0.0.0.0/0         0.0.0.0/0
    0     0 ACCEPT     tcp  -- *      enp0s3 0.0.0.0/0         0.0.0.0/0
    0     0 ACCEPT     tcp  -- *      enp0s3 0.0.0.0/0         0.0.0.0/0
    0     0 ACCEPT     tcp  -- *      enp0s3 0.0.0.0/0         0.0.0.0/0
root@client-toni:/home/toni# _
```

*UF5. Tallafocs i Monitoratge
(Pràctica 5.3 IPTables)*

- Consulta totes les regles que han estat creades fins ara amb l'ordre **-S**, enlloc de **-L**, que mostra aquestes tal com s'escriuen a l'hora d'afegir-les a iptables.

```
root@client-toni:/home/toni# iptables -S
-P INPUT DROP
-P FORWARD ACCEPT
-P OUTPUT DROP
-A INPUT -i enp0s3 -p icmp -j ACCEPT
-A INPUT -i enp0s3 -p tcp -m tcp --sport 80 -j ACCEPT
-A INPUT -i enp0s3 -p tcp -m tcp --sport 22 -j ACCEPT
-A INPUT -i enp0s3 -p tcp -m tcp --sport 21 -j ACCEPT
-A INPUT -i enp0s3 -p tcp -m tcp --sport 20 -j ACCEPT
-A OUTPUT -o enp0s3 -p tcp -m tcp --dport 22 -j ACCEPT
-A OUTPUT -o enp0s3 -p icmp -j ACCEPT
-A OUTPUT -o enp0s3 -p tcp -m tcp --dport 80 -j ACCEPT
-A OUTPUT -o enp0s3 -p tcp -m tcp --dport 22 -j ACCEPT
-A OUTPUT -o enp0s3 -p tcp -m tcp --dport 21 -j ACCEPT
-A OUTPUT -o enp0s3 -p tcp -m tcp --dport 20 -j ACCEPT
```

Creació SCRIPT

- Les regles que s'han escrit fins ara no són permanents, per això si es tanca la màquina aquestes regles es perdran i caldrà escriure-les de nou. Per a evitar això aprofitarem l'opció vista en el punt anterior per a fer un **script** que permeti automatitzar la introducció de les regles a iptables.

- Escriu l'ordre del punt anterior seguida de la canonada, **pipe** en anglès, **'>'** seguida del nom del fitxer on es guardarà aquest contingut:

- Anomena'l **nomCognomReglesFirewall.sh**

```
root@client-toni:/home/toni# iptables -S > /home/toni/TBYReglesFirewall.sh
root@client-toni:/home/toni# ls
TBYReglesFirewall.sh
```

-

*UF5. Tallafocs i Monitoratge
(Pràctica 5.3 IPTables)*

- Edita aquest fitxer posant l'ordre iptables davant de cada línia.

```
GNU nano 6.2                                TBYReglesFirewall.sh *
iptables -P INPUT DROP
iptables -P FORWARD ACCEPT
iptables -P OUTPUT DROP
iptables -A INPUT -i enp0s3 -p icmp -j ACCEPT
iptables -A INPUT -i enp0s3 -p tcp -m tcp --sport 80 -j ACCEPT
iptables -A INPUT -i enp0s3 -p tcp -m tcp --sport 22 -j ACCEPT
iptables -A INPUT -i enp0s3 -p tcp -m tcp --sport 21 -j ACCEPT
iptables -A INPUT -i enp0s3 -p tcp -m tcp --sport 20 -j ACCEPT
iptables -A OUTPUT -o enp0s3 -p tcp -m tcp --dport 22 -j ACCEPT
iptables -A OUTPUT -o enp0s3 -p icmp -j ACCEPT
iptables -A OUTPUT -o enp0s3 -p tcp -m tcp --dport 80 -j ACCEPT
iptables -A OUTPUT -o enp0s3 -p tcp -m tcp --dport 22 -j ACCEPT
iptables -A OUTPUT -o enp0s3 -p tcp -m tcp --dport 21 -j ACCEPT
iptables -A OUTPUT -o enp0s3 -p tcp -m tcp --dport 20 -j ACCEPT
```

- Fes que sigui executable només per al seu propietari, que és **root**, amb **chmod**.

```
root@client-toni:/home/toni# chmod 700 /home/toni/TBYReglesFirewall.sh
root@client-toni:/home/toni# ls
TBYReglesFirewall.sh
```

- Reinicia la màquina i amb **iptables -L -nv** comprova que hi ha la configuració per defecte.

```
root@client-toni:/home/toni# reboot now_
```

```
root@client-toni:/home/toni# iptables -L -nv
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in      out     source                   destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in      out     source                   destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in      out     source                   destination
root@client-toni:/home/toni# _
```

*UF5. Tallafocs i Monitoratge
(Pràctica 5.3 IPTables)*

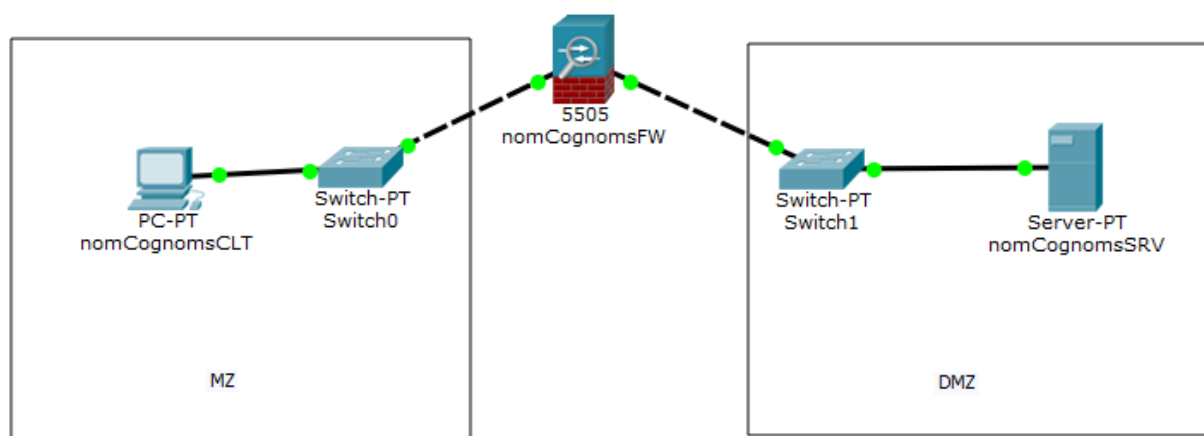
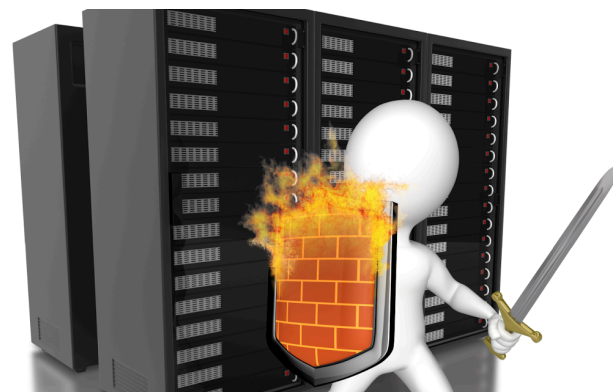
- Executa l'script i ja sigui amb l'ordre **-S** o **-L** mostra com a iptables hi ha de nou les regles de filtratge.

```
root@client-toni:/home/toni# ./TBYReglesFirewall.sh
root@client-toni:/home/toni# iptables -S
-P INPUT DROP
-P FORWARD ACCEPT
-P OUTPUT DROP
-A INPUT -i enp0s3 -p icmp -j ACCEPT
-A INPUT -i enp0s3 -p tcp -m tcp --sport 80 -j ACCEPT
-A INPUT -i enp0s3 -p tcp -m tcp --sport 22 -j ACCEPT
-A INPUT -i enp0s3 -p tcp -m tcp --sport 21 -j ACCEPT
-A INPUT -i enp0s3 -p tcp -m tcp --sport 20 -j ACCEPT
-A INPUT -i enp0s3 -p icmp -j ACCEPT
-A INPUT -i enp0s3 -p tcp -m tcp --sport 80 -j ACCEPT
-A INPUT -i enp0s3 -p tcp -m tcp --sport 22 -j ACCEPT
-A INPUT -i enp0s3 -p tcp -m tcp --sport 21 -j ACCEPT
-A INPUT -i enp0s3 -p tcp -m tcp --sport 20 -j ACCEPT
-A OUTPUT -o enp0s3 -p tcp -m tcp --dport 80 -j ACCEPT
-A OUTPUT -o enp0s3 -p tcp -m tcp --dport 22 -j ACCEPT
-A OUTPUT -o enp0s3 -p tcp -m tcp --dport 21 -j ACCEPT
-A OUTPUT -o enp0s3 -p tcp -m tcp --dport 20 -j ACCEPT
-A OUTPUT -o enp0s3 -p tcp -m tcp --dport 22 -j ACCEPT
-A OUTPUT -o enp0s3 -p icmp -j ACCEPT
-A OUTPUT -o enp0s3 -p tcp -m tcp --dport 80 -j ACCEPT
-A OUTPUT -o enp0s3 -p tcp -m tcp --dport 22 -j ACCEPT
-A OUTPUT -o enp0s3 -p tcp -m tcp --dport 21 -j ACCEPT
-A OUTPUT -o enp0s3 -p tcp -m tcp --dport 20 -j ACCEPT
root@client-toni:/home/toni# _
```

*UF5. Tallafocs i Monitoratge
(Pràctica 5.3 IPTables)*

Part II: Firewall perimetral

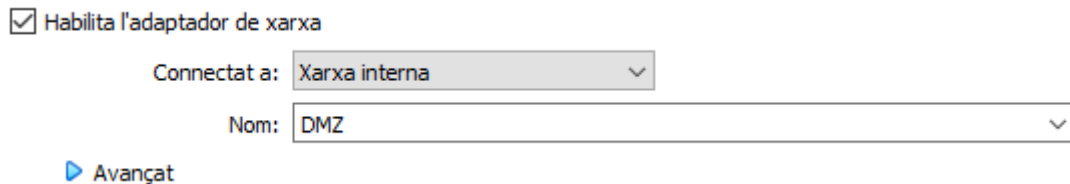
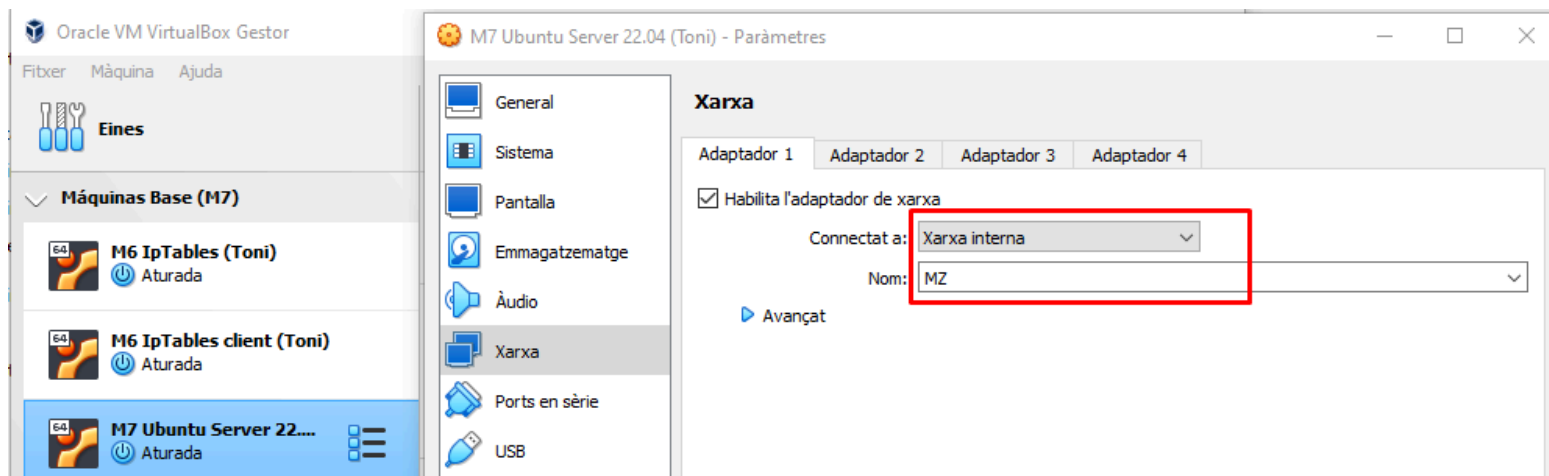
A diferència dels firewalls personals, els perimetrals són aquells que es posen a l'entrada d'una xarxa local per a filtrar els paquets que entrin i surtin d'aquesta xarxa local. Acostuma a ser un dispositiu de maquinari específic per aquesta tasca o bé un servidor dedicat a fer aquesta funció amb un programari específic, com per exemple iptables. Això és el que implementarem en aquesta part de la pràctica. L'esquema de xarxa que es farà servir és el següent:



Entorn de treball

- Crea una altra màquina Linux sense entorn gràfic i anomena-la, tant a la finestra de VirtualBox com al prompt del terminal **nomCognomFW**, ja que serà el firewall perimetral de la xarxa.
- Posa-li dues interfícies de xarxa interna:
 - Anomena a la primera **MZ** i a la segona **DMZ**.

*UF5. Tallafocs i Monitoratge
(Pràctica 5.3 IPTables)*



- Modifica el fitxer `/etc/network/interfaces` de **nomCognomFW**, de tal manera que la interfície corresponent a la **MZ** tingui la **@IP 192.168.10.1** i la corresponent a la **DMZ** la **192.168.20.1**.

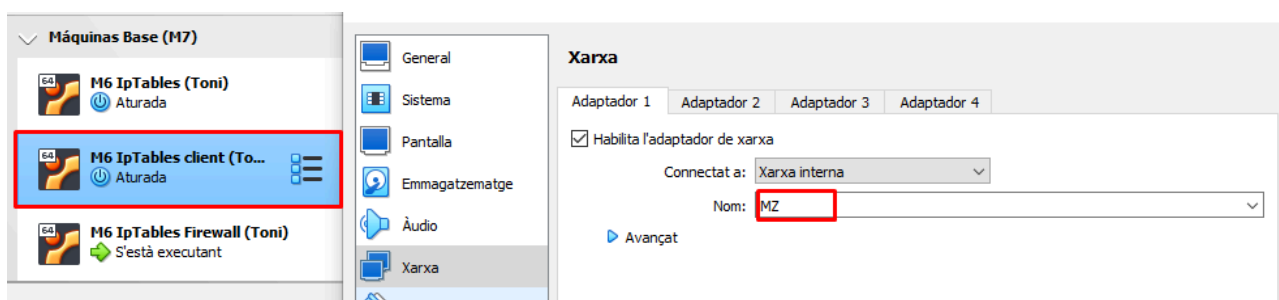
UF5. Tallafocs i Monitoratge
(Pràctica 5.3 IPTables)

M6 IpTables Firewall (Toni) [S'està executant] - Oracle VM VirtualBox

Fitxer Màquina Visualitza Entrada Dispositius Ajuda

```
GNU nano 6.2 /etc/netplan/00-installer-config.yaml
# This is the network config written by 'subiquity'
network:
  ethernets:
    enp0s3:
      dhcp4: false
      addresses: [192.168.10.1/24]
    enp0s8:
      dhcp4: false
      addresses: [192.168.20.1/24]
  version: 2
```

- Canvia el nom de la xarxa interna que té a VirtualBox **nomCognomCLT** per **MZ**.



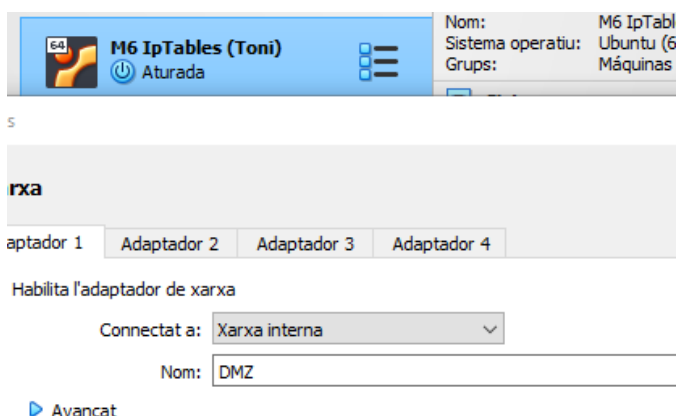
- Modifica el fitxer **/etc/network/interfaces** de **nomCognomCLT**, de tal manera que tingui la **@IP 192.168.10.100** i posa com a gateway la **@IP** de **nomCognomFW** corresponent a la **MZ**.

```
GNU nano 6.2 /etc/net
# This is the network config written by 'su
network:
  ethernets:
    enp0s3:
      dhcp4: false
      addresses: [192.168.10.100/24]
      gateway: 192.168.10.1
  version: 2
```


UF5. Tallafocs i Monitoratge
(Pràctica 5.3 IPTables)

```
root@client-toni:/home/toni# networkctl status enp0s3
• 2: enp0s3
    Link File: /usr/lib/systemd/network/99-default.link
    Network File: /run/systemd/network/10-netplan-enp0s3.network
    Type: ether
    State: routable (configured)
    Online state: online
    Path: pci-0000:00:03.0
    Driver: e1000
    Vendor: Intel Corporation
    Model: 82540EM Gigabit Ethernet Controller (PRO/1000 MT Desktop Adapter)
    HW Address: 08:00:27:6e:79:36 (PCS Systemtechnik GmbH)
    MTU: 1500 (min: 46, max: 16110)
    QDisc: fq_codel
```

- Canvia el nom de la xarxa interna que té a VirtualBox **nomCognomSRV** per **DMZ**.



- Modifica el fitxer **/etc/network/interfaces** de **nomCognomSRV**, de tal manera que tingui la **@IP 192.168.20.100** i posa com a gateway la **@IP** de **nomCognomFW** corresponent a la **DMZ**.

*UF5. Tallafocs i Monitoratge
(Pràctica 5.3 IPTables)*

```
M6 IpTables (Toni) [S'està executant] - Oracle VM VirtualBox
Fitxer  Màquina  Visualitza  Entrada  Dispositius  Ajuda
GNU nano 6.2 /etc/netplan/00-installer-config.yaml
# This is the network config written by 'subiquity'
network:
  ethernets:
    enp0s3:
      dhcp4: false
      addresses: [192.168.20.100/24]
      gateway: 192.168.20.1
  version: 2
```

```
root@server-toni:/home/toni# networkctl status enp0s3
• 2: enp0s3
    Link File: /usr/lib/systemd/network/99-default.link
    Network File: /run/systemd/network/10-netplan-enp0s3.network
    Type: ether
    State: routable (configured)
    Online state: online
    Path: pci-0000:00:03.0
    Driver: e1000
    Vendor: Intel Corporation
    Model: 82540EM Gigabit Ethernet Controller (PRO/1000 MT Desktop Adapter)
    HW Address: 08:00:27:22:6a:a2 (PCS Systemtechnik GmbH)
```

- Comprova que la màquina **nomCognomFW** pot fer ping tant a **nomCognomCLT** com a **nomCognomSRV**.

UF5. Tallafocs i Monitoratge
(Pràctica 5.3 IPTables)

```
root@server-toni:/home/toni# ping 192.168.10.100
PING 192.168.10.100 (192.168.10.100) 56(84) bytes of data.
64 bytes from 192.168.10.100: icmp_seq=1 ttl=64 time=2.40 ms
64 bytes from 192.168.10.100: icmp_seq=2 ttl=64 time=1.09 ms
64 bytes from 192.168.10.100: icmp_seq=3 ttl=64 time=1.13 ms
^C
--- 192.168.10.100 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 1.088/1.541/2.404/0.610 ms
root@server-toni:/home/toni# ping 192.168.20.100
PING 192.168.20.100 (192.168.20.100) 56(84) bytes of data.
64 bytes from 192.168.20.100: icmp_seq=1 ttl=64 time=2.63 ms
64 bytes from 192.168.20.100: icmp_seq=2 ttl=64 time=1.00 ms
64 bytes from 192.168.20.100: icmp_seq=3 ttl=64 time=0.970 ms
^C
--- 192.168.20.100 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 0.970/1.535/2.633/0.776 ms
root@server-toni:/home/toni# _
```

- Fes ping entre **nomCognomCLT** i **nomCognomSRV** i comprova si funciona.

```
root@client-toni:/home/toni# ping 192.168.20.100
PING 192.168.20.100 (192.168.20.100) 56(84) bytes of data.
^C
--- 192.168.20.100 ping statistics --- NO FA PING
4 packets transmitted, 0 received, 100% packet loss, time 3065ms
root@client-toni:/home/toni#
```

Encaminament

- El principi dues màquines que formen part de xarxes diferents com **nomCognomSRV** i **nomCognomCLT** no es poden fer ping. Tanmateix totes dues sí que ho poden fer amb **nomCognomFW** i a més tenen aquesta màquina com a porta d'enllaç. Per tant **nomCognomFW** pot encaminar els pings entre aquelles dues màquines encara que formin part de xarxes diferents, però per aconseguir-lo cal habilitar la capacitat d'encaminament:

*UF5. Tallafocs i Monitoratge
(Pràctica 5.3 IPTables)*

- La capacitat d'encaminament d'una màquina a Linux es configura amb el fitxer **/proc/sys/net/ipv4/ip_forward**. Aquest per defecte té el valor zero, que significa que no encamina. Cal posar el valor d'aquest fitxer a u per tal d'habilitar aquesta característica:

■ **echo 1 > /proc/sys/net/ipv4/ip_forward**


```
root@server-toni:/home/toni# echo 1 > /proc/sys/net/ipv4/ip_forward
root@server-toni:/home/toni#
```

- Comprova ara que les màquines **nomCognomSRV** i **nomCognomCLT** es poden fer ping.

```
root@client-toni:/home/toni# ping 192.168.20.100
PING 192.168.20.100 (192.168.20.100) 56(84) bytes of data.
64 bytes from 192.168.20.100: icmp_seq=1 ttl=63 time=2.97 ms
64 bytes from 192.168.20.100: icmp_seq=2 ttl=63 time=2.48 ms
64 bytes from 192.168.20.100: icmp_seq=3 ttl=63 time=2.71 ms
^C
--- 192.168.20.100 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2007ms
rtt min/avg/max/mdev = 2.476/2.717/2.969/0.201 ms
root@client-toni:/home/toni# _
```

Configurar Firewall Perimetral

- Configurem ara iptables a **nomCognomFW** per a implementar el firewall perimetral.
 - Estableix una política per defecte de denegació a les cadenes, **INPUT** i **OUTPUT** de la taula filter.

 M6 IpTables Firewall (Toni) [S'està executant] - Oracle VM VirtualBox
Fitxer Màquina Visualitza Entrada Dispositius Ajuda

```
root@server-toni:/home/toni# iptables -P INPUT DROP
root@server-toni:/home/toni# iptables -P OUTPUT DROP
root@server-toni:/home/toni#
```

- Comprova que encara es poden fer ping entre elles les màquines **nomCognomSRV** i **nomCognomCLT**. Això es deu a que amb **INPUT** i **OUTPUT**

UF5. Tallafocs i Monitoratge
(Pràctica 5.3 IPTables)

es prohibeixen els paquets que tenen origen o destí en la màquina **nomCognomFW**. Però no els pings que tenen origen i destí en les màquines **nomCognomSRV** i **nomCognomCLT**, per això les regles de les cadenes **INPUT** i **OUTPUT** no afecten aquests paquets. El que fa **nomCognomFW** amb aquests paquets és encaminar-los, i la cadena que s'encarrega de filtrar-los és **FORWARD**.

```
root@client-toni:/home/toni# ping 192.168.20.100
PING 192.168.20.100 (192.168.20.100) 56(84) bytes of data.
64 bytes from 192.168.20.100: icmp_seq=1 ttl=63 time=2.97 ms
64 bytes from 192.168.20.100: icmp_seq=2 ttl=63 time=2.48 ms
64 bytes from 192.168.20.100: icmp_seq=3 ttl=63 time=2.71 ms
^C
--- 192.168.20.100 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2007ms
rtt min/avg/max/mdev = 2.476/2.717/2.969/0.201 ms
root@client-toni:/home/toni# _
```

- Estableix una política de denegació per defecte a la cadena **FORWARD** d'iptables de **nomCognomFW** i comprova que **nomCognomSRV** i **nomCognomCLT** ja no es poden fer ping.
- Comprova amb **iptables -L -nv** com efectivament ha quedat enregistrat la denegació dels pings.

```
root@server-toni:/home/toni# iptables -P FORWARD DROP
```

```
root@client-toni:/home/toni# ping 192.168.20.100
PING 192.168.20.100 (192.168.20.100) 56(84) bytes of data.
^C
--- 192.168.20.100 ping statistics --- NO FA PING
4 packets transmitted, 0 received, 100% packet loss, time 3065ms

root@client-toni:/home/toni#
```

*UF5. Tallafocs i Monitoratge
(Pràctica 5.3 IPTables)*

```
root@server-toni:/home/toni# iptables -L -nv
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source                   destination

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source                   destination

Chain OUTPUT (policy DROP 384 packets, 27312 bytes)
 pkts bytes target    prot opt in     out     source                   destination
root@server-toni:/home/toni#
```

- Habilitem amb l'ordre iptables les dues regles a **nomCognomFW** que facin possible els pings entre **nomCognomSRV** i **nomCognomCLT**.
- Cal especificar amb l'ordre el paràmetre **-A** que la regla de filtratge que s'afegeix és per a la cadena **FORWARD**.
 - Caldrà especificar el paràmetre **-i** per a indicar per quina interfície li arriba a **nomCognomFW** el paquet:
 - Si el ping li arriba a **nomCognomFW** des de la **MZ** cal posar el paràmetre **-i** seguit del nom de la interfície de **nomCognomFW** que té assignada la **@IP** pertanyent a la xarxa de la **MZ**. En cas que el ping li arribi des de la **DMZ** al paràmetre **-i** caldrà assignar-li el nom de la interfície de **nomCognomFW** que té assignada la **@IP** pertanyent a la xarxa **DMZ**.
 - Seguint el criteri explicat al punt anterior caldrà assignar el valor corresponents als paràmetre **-o**.
 - Com només habilitarem els pings entre **nomCognomSRV** i les màquines de la **MZ** s'afegiran dos nous paràmetres:
 - El **paràmetre -s** que indica la màquina o la xarxa origen del ping. En el cas que el ping tingui origen a la **MZ** el valor serà **@IPxarxa/bits_màscara**, doncs així qualsevol màquina de la **MZ** podrà fer ping a **nomCognomSRV**. En cas que l'origen sigui la màquina **nomCognomSRV** el valor del paràmetre ha de ser **@ip_nomCognomSRV**, doncs només s'habilita aquesta màquina de la **DMZ** per a enviar i respondre pings cap a la **MZ**.

*UF5. Tallafocs i Monitoratge
(Pràctica 5.3 IPTables)*

- El **paràmetre -d** que indica la màquina o la xarxa destí del paquet ping. El valor que cal assignar a aquest paràmetre ha de seguir el mateix criteri que l'explicat al punt anterior.
- Cal especificar amb el **paràmetre -p** quin protocol s'està fent servir. Heu de posar el valor pertinent per a poder fer pings.
- Finalment amb el **paràmetre -j** s'indicarà què es vol permetre el tràfic dels paquets que compleixin els requisits especificats amb aquestes regles.

```
root@server-toni:/home/toni# iptables -A FORWARD -i enp0s8 -o enp0s3 -s 192.168.10.0/24 -d 192.168.20.100/24 -p icmp -j ACCEPT
root@server-toni:/home/toni# iptables -A FORWARD -i enp0s8 -o enp0s3 -s 192.168.20.100/24 -d 192.168.10.0/24 -p icmp -j ACCEPT
root@server-toni:/home/toni# _
```

```
root@client-toni:/home/toni# ping 192.168.20.100
PING 192.168.20.100 (192.168.20.100) 56(84) bytes of data.
64 bytes from 192.168.20.100: icmp_seq=1 ttl=63 time=2.50 ms
64 bytes from 192.168.20.100: icmp_seq=2 ttl=63 time=2.39 ms
64 bytes from 192.168.20.100: icmp_seq=3 ttl=63 time=2.58 ms
^C
--- 192.168.20.100 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2018ms
rtt min/avg/max/mdev = 2.393/2.491/2.584/0.078 ms
root@client-toni:/home/toni# _
```



M6 IpTables (Toni) [S'està executant] - Oracle VM VirtualBox

Fitxer Màquina Visualitza Entrada Dispositius Ajuda

```
root@server-toni:/home/toni# ping 192.168.10.100
PING 192.168.10.100 (192.168.10.100) 56(84) bytes of data.
64 bytes from 192.168.10.100: icmp_seq=1 ttl=63 time=2.49 ms
64 bytes from 192.168.10.100: icmp_seq=2 ttl=63 time=2.76 ms
64 bytes from 192.168.10.100: icmp_seq=3 ttl=63 time=3.05 ms
^C
--- 192.168.10.100 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2009ms
rtt min/avg/max/mdev = 2.493/2.769/3.054/0.229 ms
root@server-toni:/home/toni#
```

*UF5. Tallafocs i Monitoratge
(Pràctica 5.3 IPTables)*

Serveis HTTP, SSH i FTP

- Habilitem la resta de serveis disponibles a **nomCognomSRV, HTTP, FTP i SSH**.

La manera d'implementar les regles és la mateixa que l'especificada a l'apartat anterior. Cal crear una regla a **nomCognomFW** pels paquets que tenen com origen la **MZ** i **nomCognomSRV** com a destí per cadascun dels serveis indicats. Anàlogament caldrà crear les regles per permetre el tràfic dels paquets que tenen l'origen a **nomCognomSRV** i el destí a la **MZ**.

- Caldrà indicar amb **-p** el protocol que aquests serveis fan servir, així com els seus ports amb **--sport** i **--dport**.

```
root@server-toni:/home/toni# iptables -A FORWARD -i enp0s3 -o enp0s8 -s 192.168.10.0/24 -d 192.168.20.100/24 -p tcp --dport 80 -j ACCEPT
root@server-toni:/home/toni# iptables -A FORWARD -i enp0s8 -o enp0s3 -s 192.168.20.100/24 -d 192.168.10.0/24 -p tcp --sport 80 -j ACCEPT
root@server-toni:/home/toni# _
```

```
root@client-toni:/home/toni# curl http://192.168.20.100
```

```
c_html</a>
<a href="http://httpd.apache.org/docs/2.4/mod/mod_userdir.html" rel="nofollow">publi
directories (when enabled) and <tt>/usr/share</tt> (for web
applications). If your site is using a web document root
located elsewhere (such as in <tt>/srv</tt>) you may need to whitelist your
document root directory in <tt>/etc/apache2/apache2.conf</tt>.
</p>
<p>
The default Ubuntu document root is <tt>/var/www/html</tt>. You
can make your own virtual hosts under /var/www.
</p>
</div>
<div class="section_header">
<div id="bugs"></div>
Reporting Problems
</div>
<div class="content_section_text">
<p>
Please use the <tt>ubuntu-bug</tt> tool to report bugs in the
Apache2 package with Ubuntu. However, check <a
href="https://bugs.launchpad.net/ubuntu/+source/apache2"
rel="nofollow">existing bug reports</a> before reporting a new bug.
</p>
<p>
Please report bugs specific to modules (such as PHP and others)
to their respective packages, not to the web server itself.
</p>
</div>
</div>
</div>
<div class="validator">
</div>
</body>
</html>
root@client-toni:/home/toni# _
```


*UF5. Tallafocs i Monitoratge
(Pràctica 5.3 IPTables)*

```
root@server-toni:/home/toni# iptables -A FORWARD -i enp0s3 -o enp0s8 -s 192.168.10.0/24 -d 192.168.20.100/24 -p tcp --dport 20 -j ACCEPT
root@server-toni:/home/toni# iptables -A FORWARD -i enp0s3 -o enp0s8 -s 192.168.10.0/24 -d 192.168.20.100/24 -p tcp --dport 21 -j ACCEPT
root@server-toni:/home/toni# iptables -A FORWARD -i enp0s8 -o enp0s3 -s 192.168.20.100/24 -d 192.168.10.0/24 -p tcp --sport 20 -j ACCEPT
root@server-toni:/home/toni# iptables -A FORWARD -i enp0s8 -o enp0s3 -s 192.168.20.100/24 -d 192.168.10.0/24 -p tcp --sport 21 -j ACCEPT
root@server-toni:/home/toni#
```

```
root@client-toni:/home/toni# ftp 192.168.20.100
Connected to 192.168.20.100.
220 (vsFTPD 3.0.5)
Name (192.168.20.100:toni): toni
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

```
root@server-toni:/home/toni# iptables -A FORWARD -i enp0s3 -o enp0s8 -s 192.168.10.0/24 -d 192.168.20.100/24 -p tcp --dport 22 -j ACCEPT
root@server-toni:/home/toni# iptables -A FORWARD -i enp0s8 -o enp0s3 -s 192.168.20.100/24 -d 192.168.10.0/24 -p tcp --sport 22 -j ACCEPT
root@server-toni:/home/toni# _
```

```
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.15.0-84-generic x86_64)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:       https://ubuntu.com/advantage

System information as of jue 01 feb 2024 19:26:08 UTC

System load:  0.0          Processes:    121
Usage of /:   30.3% of 23.45GB  Users logged in: 1
Memory usage: 11%          IPv4 address for enp0s3: 192.168.20.100
Swap usage:   0%

* Introducing Expanded Security Maintenance for Applications.
  Receive updates to over 25,000 software packages with your
  Ubuntu Pro subscription. Free for personal use.

  https://ubuntu.com/pro

El mantenimiento de seguridad expandido para Applications está desactivado
Se pueden aplicar 81 actualizaciones de forma inmediata.
Para ver estas actualizaciones adicionales, ejecute: apt list --upgradable

Active ESM Apps para recibir futuras actualizaciones de seguridad adicionales.
Vea https://ubuntu.com/esm o ejecute «sudo pro status»

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection
or proxy settings

Last login: Thu Feb  1 18:56:48 2024
toni@server-toni:~$ _
```

