1. TALLAFOCS AMB GUI PER UBUNTU

1. Instal·la el programari Gufw en una màquina virtual Ubuntu Desktop (l'anomenarem "Servidor") i arrenca'l.
2. En una altre equip virtual Ubuntu (serà "Client") instal·la el programari nmap. Ens servirà per fer "escanneig" de ports i comprovar si es pot accedir als serveis del Server.

```
user@user-virtualbox:~$ sudo apt install nmap
```

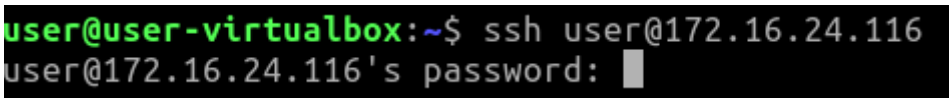
3. Instal·la Apache i openssh-server al "Server".

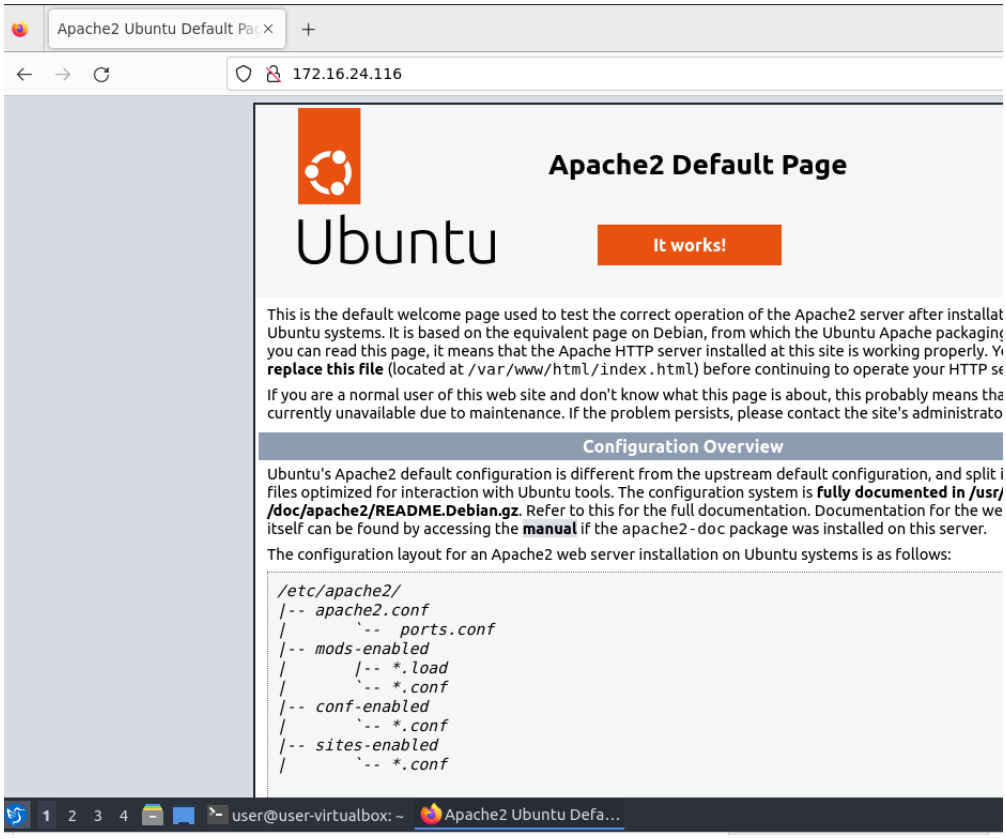
```
user@user-virtualbox:~$ sudo apt install gufw apache2 openssh-server
```

4. Comprova que pots veure els serveis actius al servidor des del "Client", accedint amb un navegador web i un client ssh.

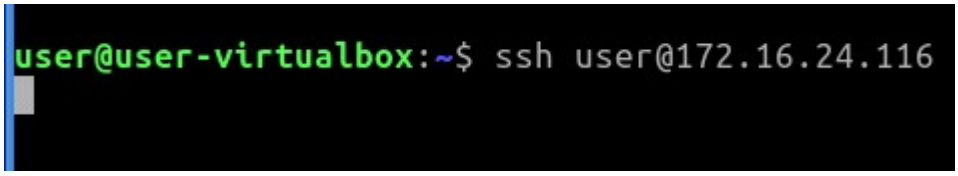
```
user@user-virtualbox:~$ nmap 172.16.24.116 -Pn
Starting Nmap 7.80 ( https://nmap.org ) at 2024-02-27 12:12 CET
Nmap scan report for 172.16.24.116
Host is up (0.00032s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
```

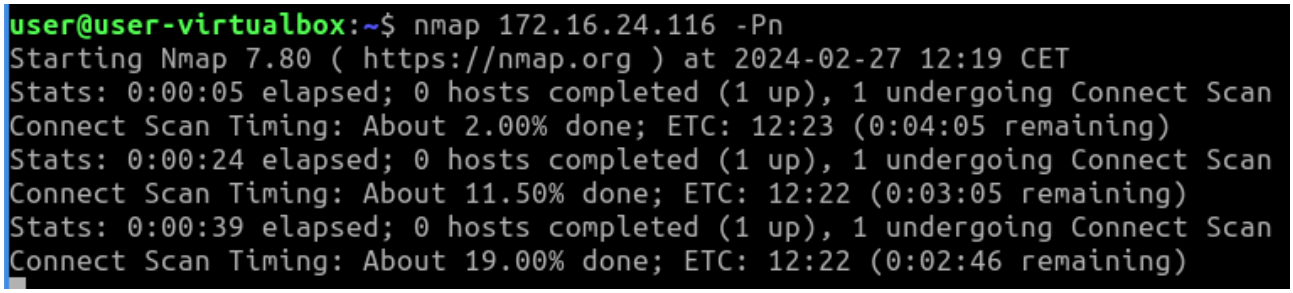
5. Comprova que nmap, et mostra que els ports dels serveis web i sshd estan oberts (escoltant).



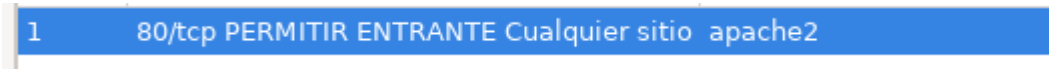


6. Activa ara el Firewall al "Server" i posa l'opció "Incoming" a "Deny" i "Outgoing" a "Allow" (opcions per defecte). Des del client comprova que els ports dels serveis ja no són accessibles i tampoc es pot accedir amb els clients web i ssh.

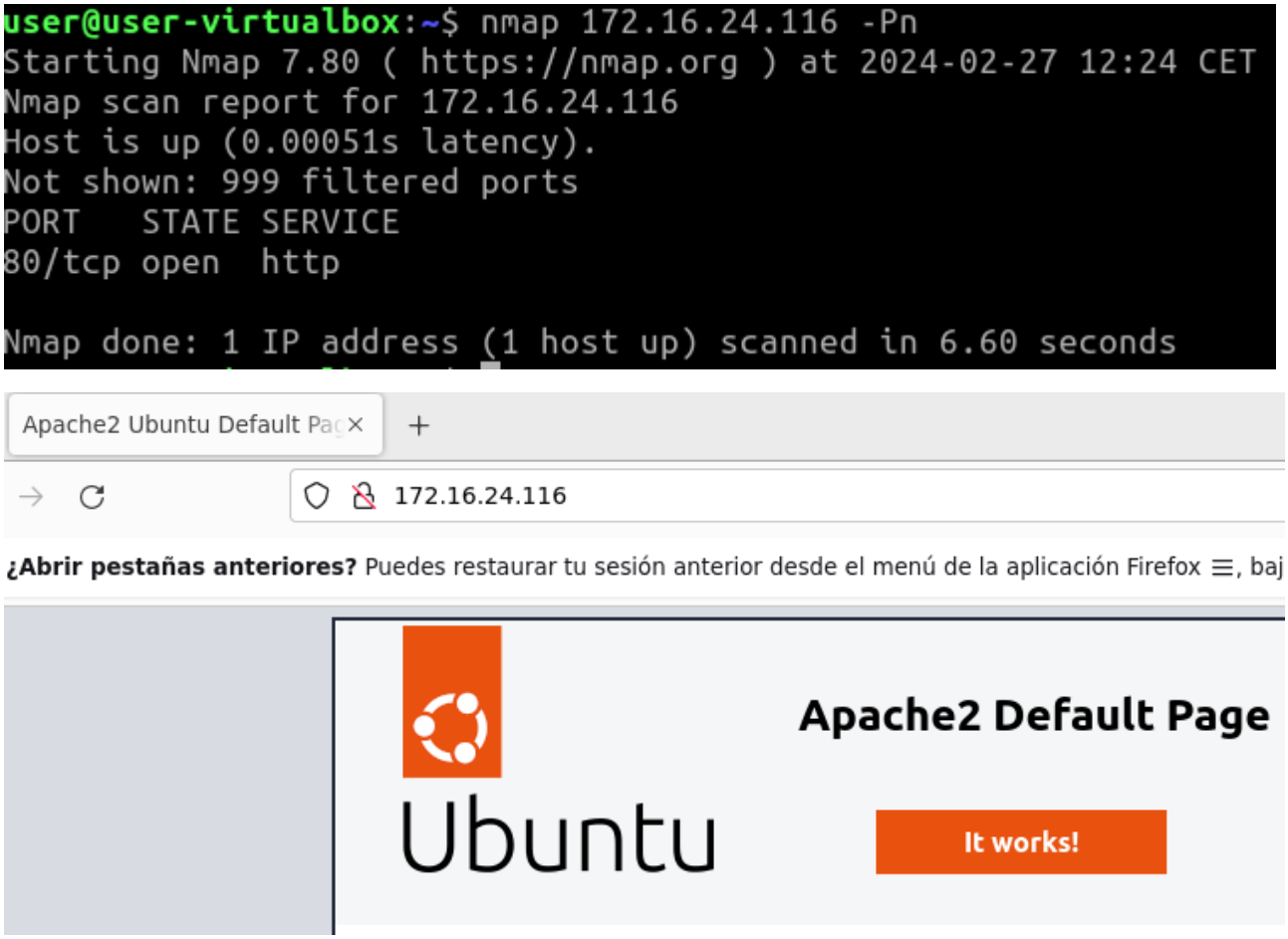




7. Al "Listening report" del Firewall tenim una llista dels serveis que estan funcionant. Si escollim apache2 i piquem el botó "+" podem afegir una regla que fa referència al port on escolta apache. Volem afegir una regla per permetre que les peticions arribin al servidor apache2.

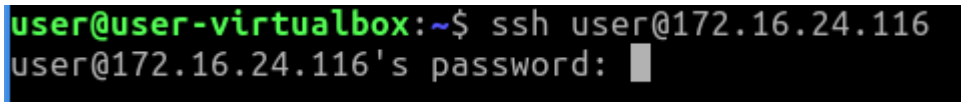


8. Comprova que el servei ara està disponible amb nmap i el client web.



9. Fes el mateix amb el servei sshd (permetre'l), però amb l'opció per configuració ràpida d'aplicacions. pica el botó "+" del desplegable "Regles" (pestanya "preconfigurat"). Prova a afegir una regla per a permetre SSH (busca entre les categories).

10. Comprova des del client que el port de ssh ara és accessible i connecta des del client SSH.



FITA 1: Demana al professor que validi aquesta part anterior de la pràctica quan l'hagis acabat.

---

2. Configuració de Pfsense

Farem servir dos equips virtuals: un amb Pfsense i un altre amb Ubuntu Desktop (pot ser la màquina creada a l'apartat anterior). També farem servir l'equip físic.

1. Creeu una nova màquina virtual per a instal·lar-hi el Pfsense. En les opcions de VirtualBox:

- Activeu una interfície pont (xarxa WAN o externa pel firewall)
- Activeu una interfície interna (xarxa LAN o interna pel Pfsense).
- Ara Instal·leu la distribució Pfsense (mode fàcil).

2. Apareixerà el pfsense en mode consola i us ensenyarà el menú inicial. Per defecte agafarà les interfícies de forma correcta.

```
*** Welcome to pfSense 2.4.4-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> em0        -> v4/DHCP4: 172.19.254.240/16
 LAN (lan)       -> em1        -> v4: 192.168.1.1/24

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
```

```
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Disable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option:
```

NOTA: Si fas la pràctica a casa, vigila que l'identificador de xarxa que fas servir a la teva xarxa de casa podria ser 192.168.1.0/24 o bé 192.168.0.0/24.

Caldrà llavors canviar l'adreça IP de la interfície LAN del Pfsense (per exemple 192.168.100.0) i el servei DHCP del Pfsense per que el rang d'adreces sigui concordant.

- Ho pots fer amb l'opció 1 (Assign interfaces)
- O bé ho pots fer des de l'aplicació web anant a Services->DHCP Server->Pestanya LAN i canviant el rang (però cal fer-ho des de la màquina virtual client).

---

3. Si no s'ha fet correctament, haureu d'assignar les interfícies WAN i LAN respectivament al pfsense (opció 1).

- Pfsense anomena les interfícies **em0 i em1**. Poseu WAN a la primera (és la interfície pont cap a internet) i poseu em1 a la segona (xarxa LAN interna).
- Comproveu fent ping desde la consola del pfsense (opció 7 o opció 8 escrivint ping...) que veieu per exemple el host 8.8.8.8 i www.google.es. Ja tindrem internet.

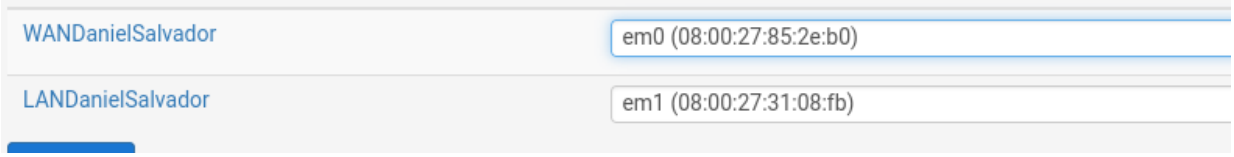
4. Creeu una màquina virtual amb Ubuntu Desktop i poseu-li una interfície VBox interna a la mateixa xarxa interna que el Pfsense (serà la màquina de la xarxa local).

- Comproveu que podeu fer ping a la IP interna del PfSense.
- Obriu el navegador i escriviu https://ip-interna-pfsense.
- Així veurem la configuració via web del pfsense. El nom d'usuari **per defecte és admin i password pfsense**.
- Configureu com a nom de host el vostre NOM-COGNOM.

5. Ara podrem configurar via web de forma remota el pfsense. Segurament us apareixerà la primera vegada el Wizard o assistent de configuració inicial. Si no, podeu anar a "System->Setup Wizard".

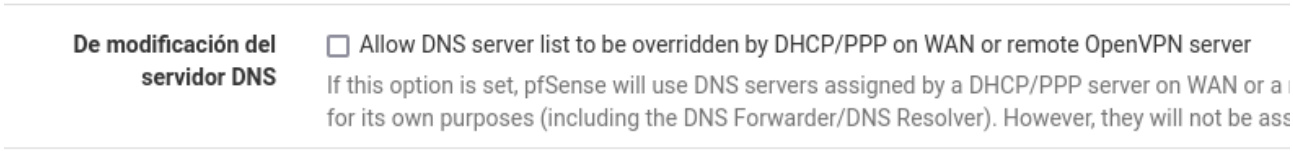
ATENCIÓ:

- Aneu al menú interfaces i **canvieu el nom de les interfícies WAN i LAN a WAN-NOM-COGNOM i LAN-NOM-COGNOM**



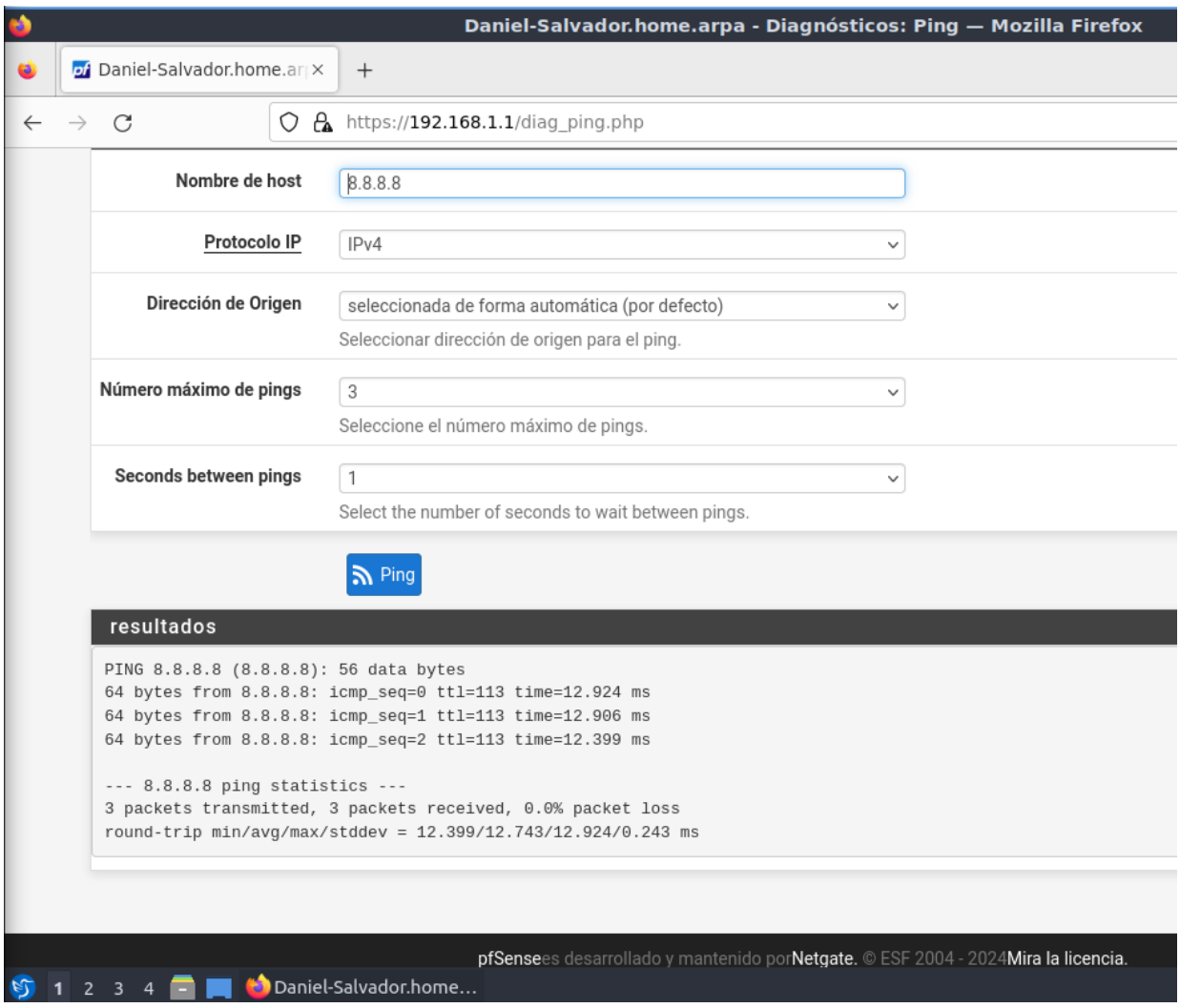
- Aneu al menú interfaces->WAN i a la secció "Reserved Networs" desactiveu el checkbox "block private networks". Així podreu accedir a la interfície WAN des del vostres equips físics (si no, el firewall ignora qualsevol paquet provinent d'una xarxa privada cap a la interfície WAN).

6. Aneu a "System->General Setup" per a comprovar la configuració del pfsense. Assegureu-vos que l'opció "Do not use the DNS Forwarder or Resolver as a DNS server for the firewall" està marcada (si no, anirà tot més lent per que el pfsense no te activat un servidor DNS propi).

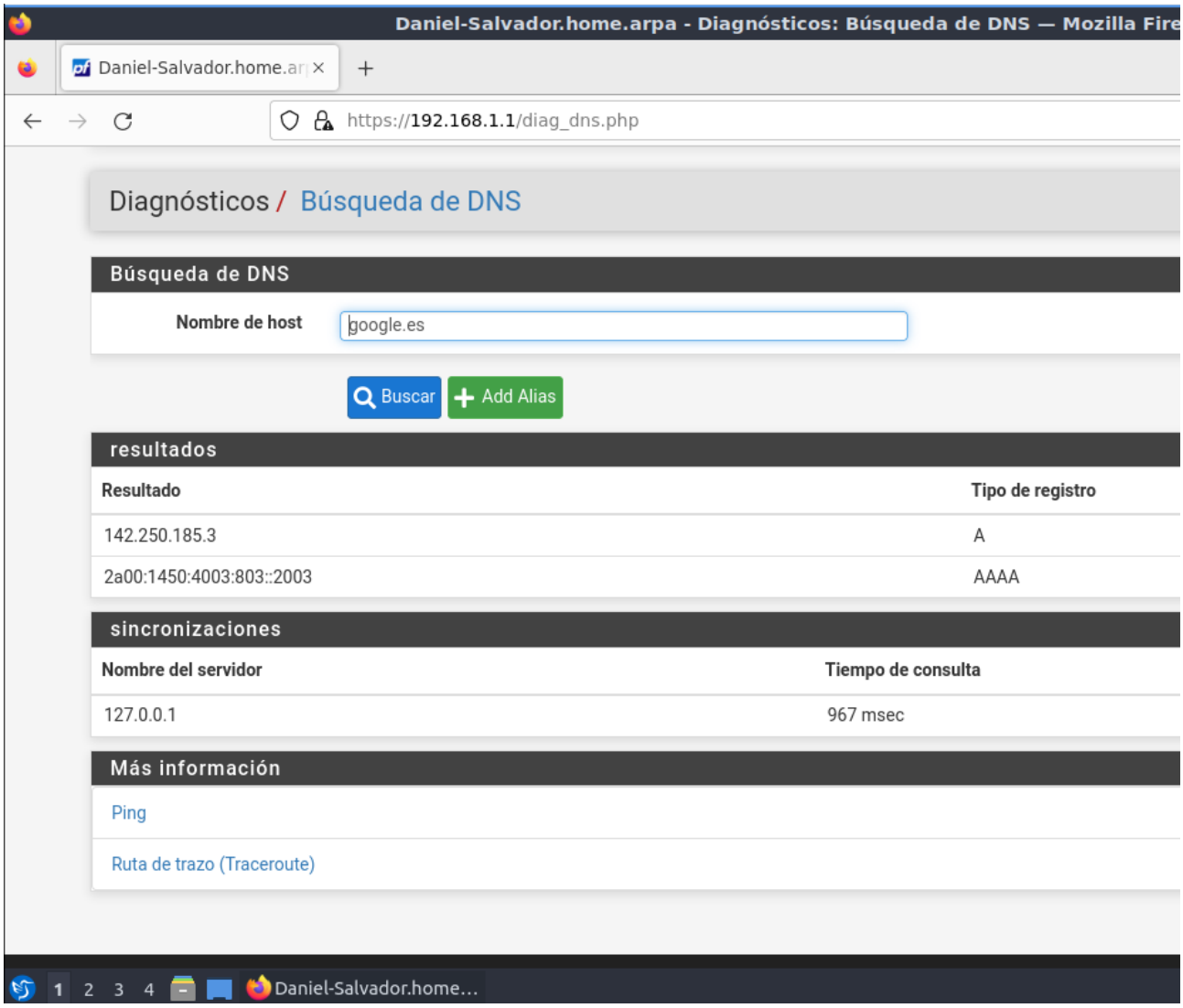


7. Aneu a "Diagnostics->Ping":

- Proveu a fer ping a 8.8.8.8 (comprovació de que funciona l'enrutament).



- Després "Diagnostics->DNS Lookup" i prova google.es (comprovació de que funciona la resolució DNS).



- Així ens assegurem que el pfsense te internet (des de la consola web).

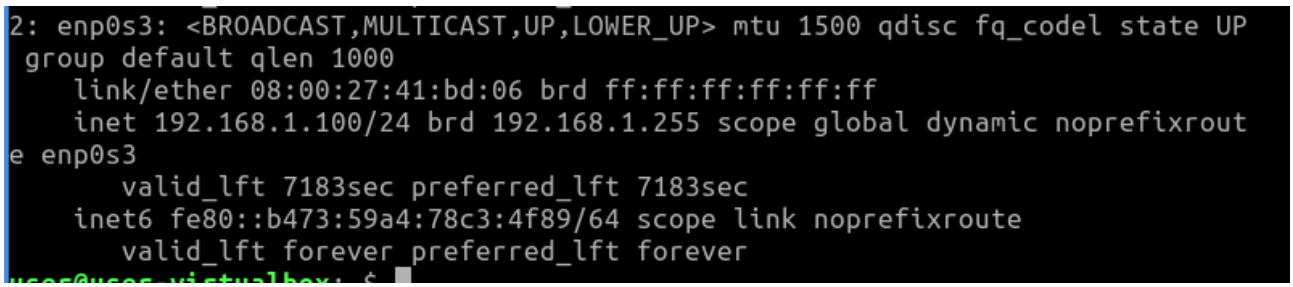
FITA 2: Demana al professor que validi aquesta part anterior de la pràctica quan l'hagis acabat.

---

3. Proves i configuració de política permissiva

8. Si tot és correcte, ja tenim el nostre firewall corporatiu funcionant, però sense filtrar res.

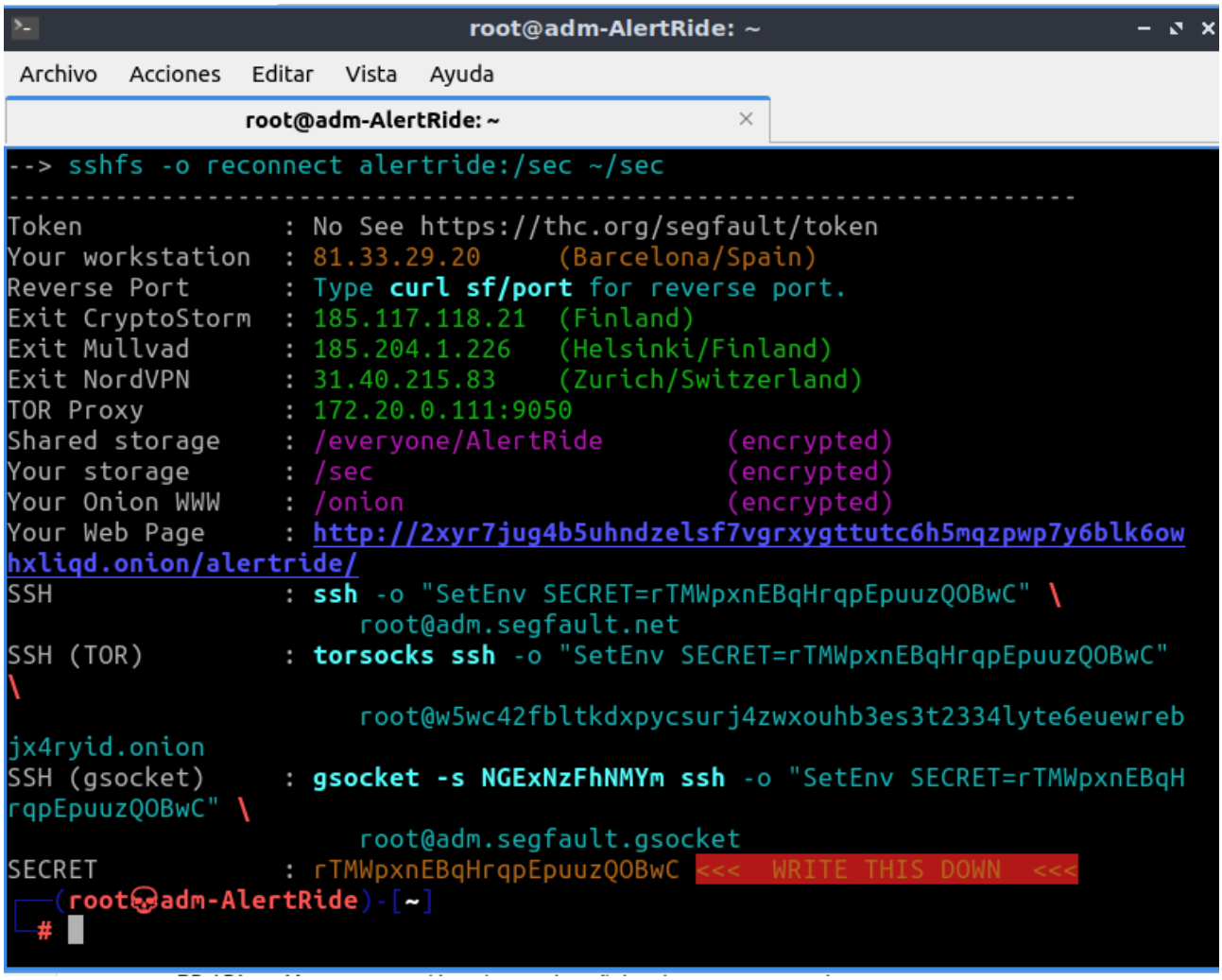
- El client es configura per DHCP ja que Pfsense activa per defecte el servei DHCP per la interfície LAN (si no ho ha fet, activa'l).
- Comprova des del client la configuració IP (adreça, màscara, gateway i DNS) i que pots accedir a alguna web.



NOTA: Si la màquina client no resol noms DNS, podeu canviar la configuració del servidor DHCP del (Pfsense Services->DHCP Server->Pestanya LAN). El paràmetre de servidor DNS que dona als clients DHCP es pot configurar per exemple a 1.1.1.1 o 8.8.4.4 que és un servidor DNS públic.

- Comprova que el paràmetre Gateway per defecte conté l'adreça interna del Pfsense.
- Prova a connectar a ftp.rediris.es mitjançant la consola amb el client ftp (usuari "anonymous"). Comprova que s'hi pot accedir, escriu la comanda "passive" per activar el mode passiu del client FTP i que pots baixar algun fitxer amb la comanda get.
- Prova el servei SSH amb "ssh usuari@tty.sdf.org" (un servidor ssh a internet. Podeu crear si voleu un compte a http://sdf.org/?signup i entrar amb el vostre usuari). Comprova que funciona.

NOTA: També pots provar https://www.thc.org/segfault/ (consola root per a fer experiments)

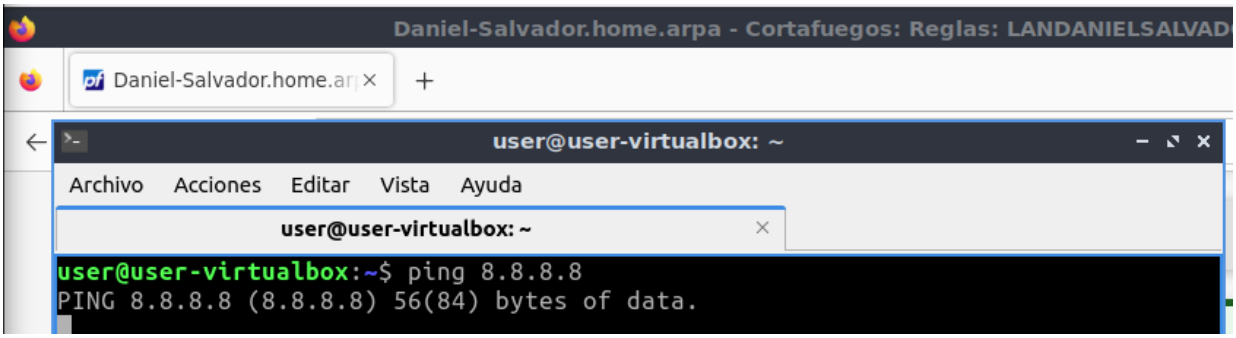


Política PERMISSIVA al Firewall: blocar el que no volem

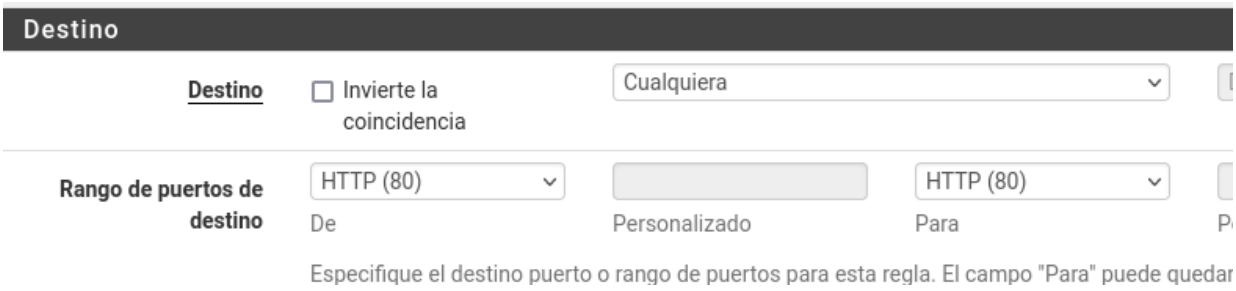
9. Apliquem la política oberta (tot permés, apliquem restriccions). Posarem restriccions de certs protocols. Bloca els ICMP de la xarxa LAN interna. Això es fa a "Firewall->Rules".

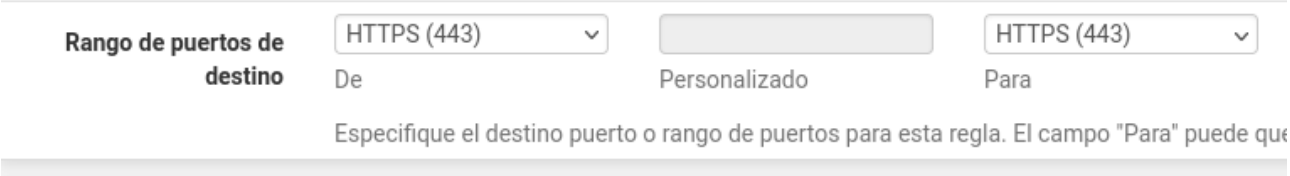
- A la pestanya LAN (interfície LAN pel pfsense), afegirem una regla nova que bloqui el protocol ICMP: origen "LAN Net", que és qualsevol adreça de la xarxa LAN i destí qualsevol.

- Comprova que no pots fer ping a 8.8.8.8 (ni cap màquina pública).



- Bloca ara el servei web segur i no segur. Són dues regles, una per a cada port (origen LAN Net, destinació qualsevol, port destí 80 http, port destí 443 https). Comprova que no pots navegar per pàgines web. Però si pots fer servir ssh i la resta de serveis.





- Canvia les regles anteriors per posar Reject en lloc de Block. Quina diferència trobes entre les respostes a Reject i Block quan intentes navegar per la web? La diferencia es que cuando esta en Block, no encuentra la web ni da respuesta. Cuando esta en Reject, encuentra la web pero no da respuesta. Explica-ho. Per un atacant, quina és pitjor? Per què? Es peor la opción Block, porque no sabe si el servicio esta activo o no.

NOTA: Pot aparèixer una campana a la barra superior del Pfsense indicant que hi ha avisos. Si veiem que algun d'ells parla de que no es pot assignar memòria, aneu a "System > Advanced > Firewall & NAT > Firewall Maximum Table Entries". Veureu el valor per defecte de 200.000 entrades. Poseu 300.000 i apliqueu els canvis. S'hauria de solucionar.

FITA 3: Demana al professor que validi aquesta part anterior de la pràctica quan l'hagis acabat.

---

4. Política RESTRICTIVA al Firewall, permetre el que volem

10. Ara mirarem de blocar tot el tràfic de la xarxa interna cap a internet, per configurar una política restrictiva (tot tancat, obrim excepcions).

- Desactiva (sense eliminar) totes les regles de la interfície LAN. Pfsense sempre treballa en mode restrictiu, i per tant l'última regla, que s'ha d'assumir, és blocar tot.
- Pots desactivar les regles que havíem posat abans picant a sobre la icona de desactivar a la dreta de la regla.
- Les regles es tornen grises quan es desactiven.
- També les pots esborrar si estàs segur que no les necessites més. Comprovem de nou els serveis i ens assegurem que no funcionen.

11. Obrirem l'accés de la xarxa interna cap a serveis web i web segura.

- Comprovem que es pot accedir a serveis web. Recorda que s'ha de poder resoldre el nom de domini (DNS, port 53 TCP i UDP)...
- Prova ftp i ssh. (La resta de protocols continuarà sense funcionar).

12. Obrirem l'accés a ssh. Recorda posar-la abans de la que bloca tots els protocols.

- Comprovem que es pot accedir a un servidor ssh a internet (ssh tty.sdf.org).
- Instal·la ssh a la teva màquina física i connectat amb ssh des del client virtual.

13. Comprova amb Wireshark, des de la màquina física quines IP's són les que realment fan la petició ssh. Hauria de ser la IP de la interfície WAN del nostre PFsense? o la del nostre client Ubuntu?
