# PFSENSE: FIREWALL

SAD

2ºASIR
I.E.S. ANTONIO MACHADO
ANA OROZCO ASENSIO

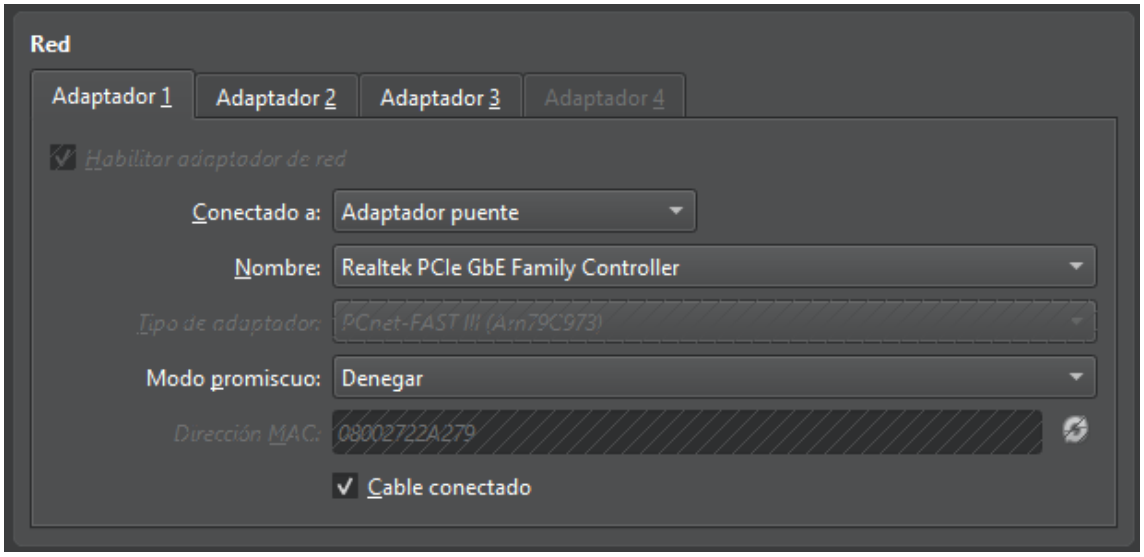
# Contenido

# Introducción.

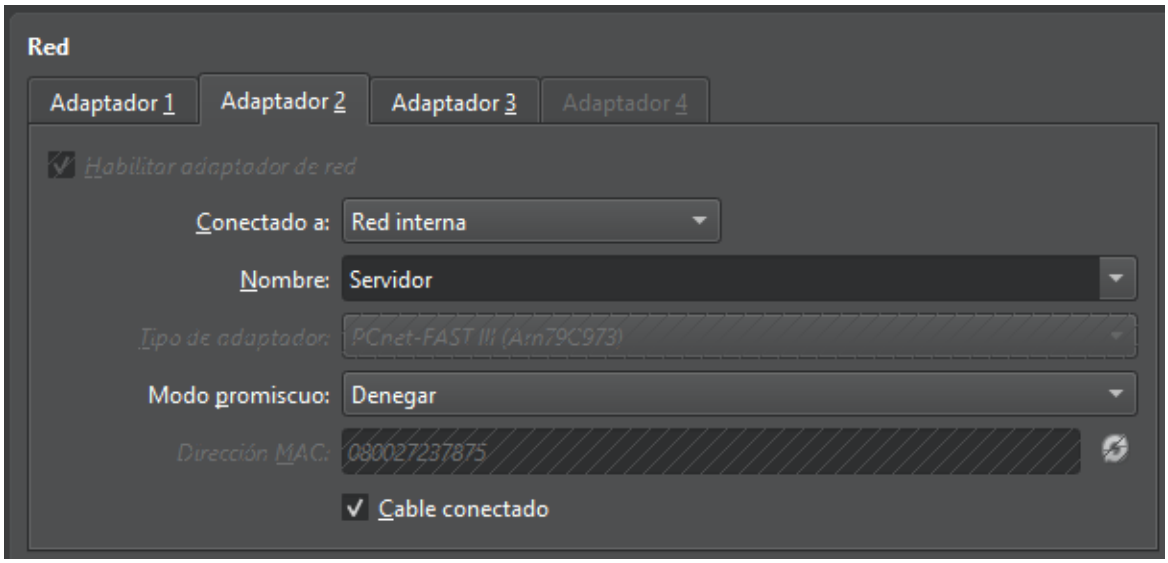
En esta práctica vamos a usar 4 máquinas para simular una empresa que necesita Firewall.

1ª máquina: Máquina Firewall con SO PFsense versión 2.7.2. donde tendremos 3 tarjetas de red:

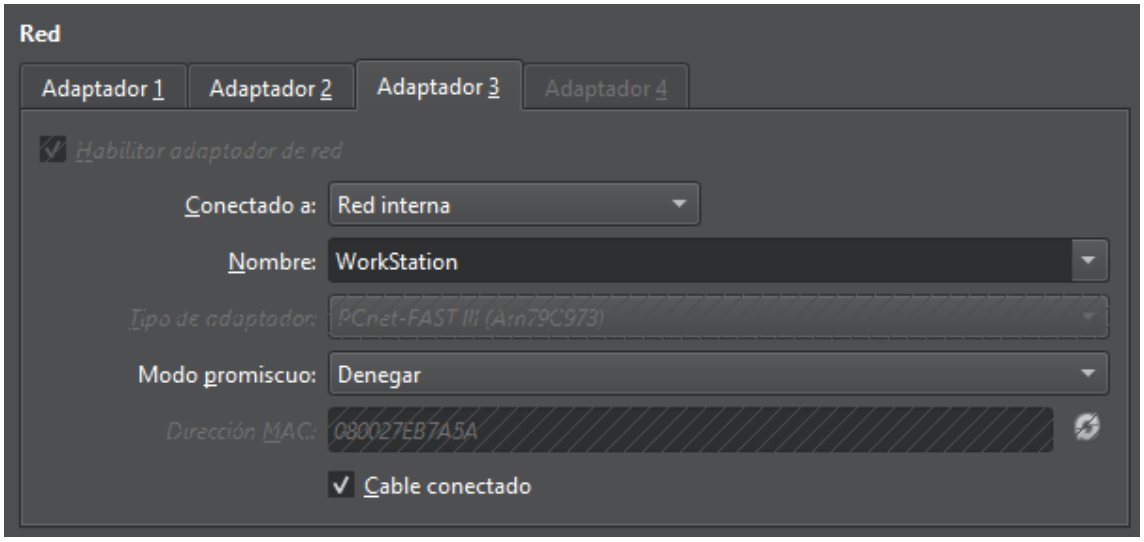
Red 1 → Adaptador puente, esta irá a internet y tendrá IP estática con el rango de los pc de clase (192.168.2.99/21) pero en casa usaré una ip dentro de mi rango (192.168.1.99/24).



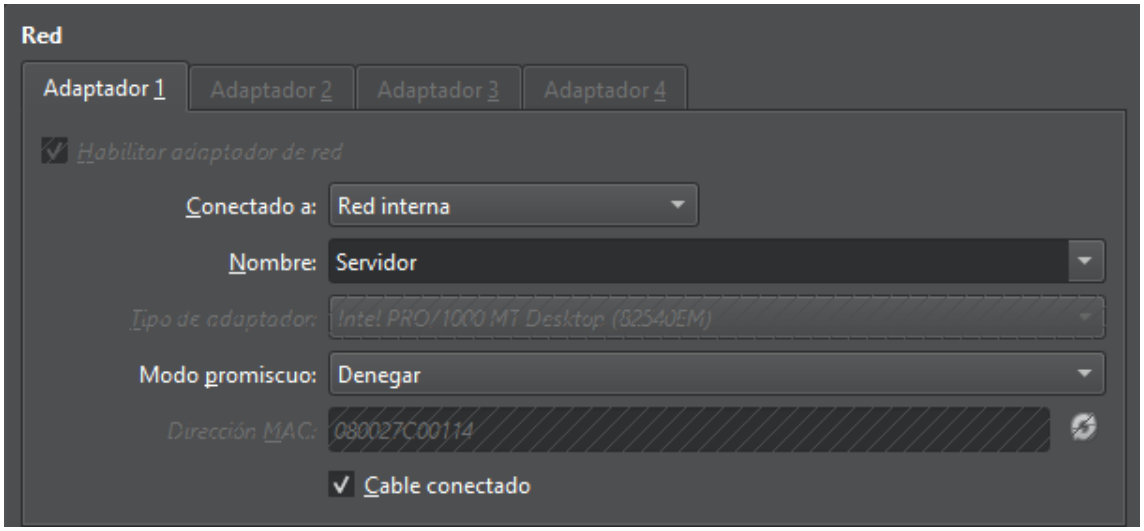

Red 2 → Red interna que llamaré Servidor. Le asignaré la IP 10.0.0.1/24 y activaremos DHCP en PFsense en el rango 10.0.0.2 – 10.0.0.254 /24 (más adelante mostraré capturas de este proceso).



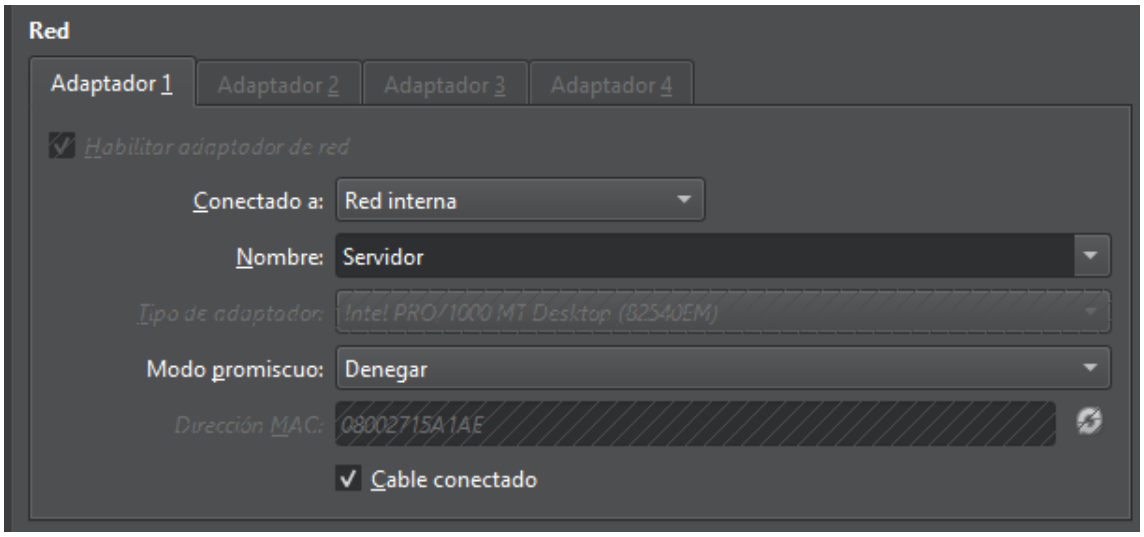
Red 3 → Red interna que llamaré WorkStation. Le asignaré la IP 10.0.1.1/24 y activaremos DHCP en PFsense en el rango 10.0.1.2 – 10.0.1.254 /24 (más adelante mostraré capturas de este proceso).



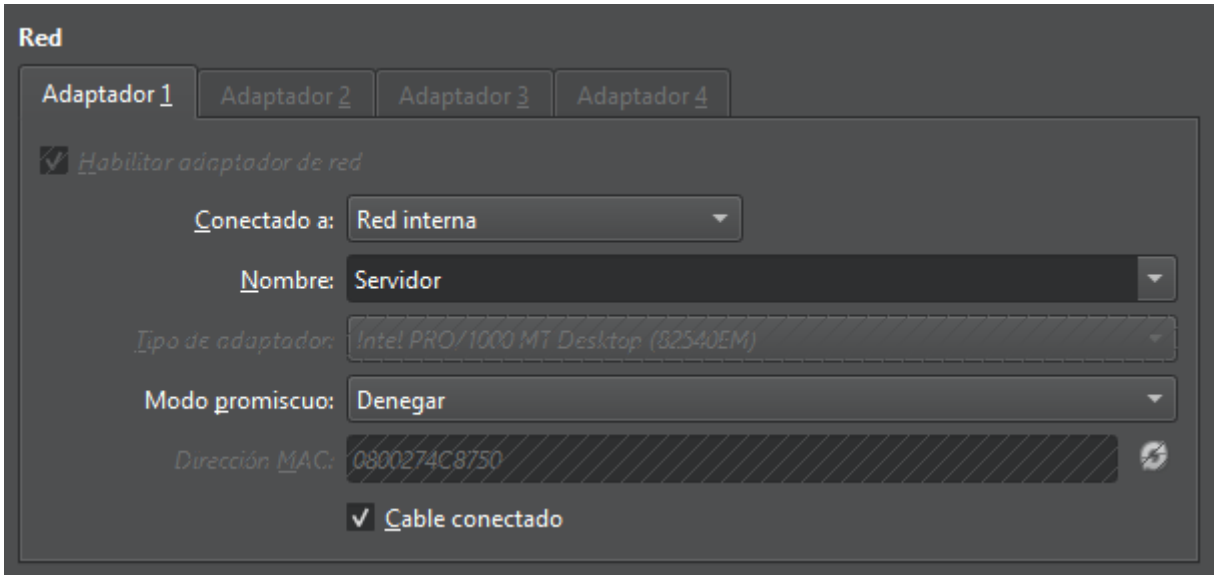

2ª máquina: Máquina de práctica de Bácula Server conectada por red interna Servidor, a la que se le asigna IP por dhcp y se inicia un Docker-compose.




3ª máquina: Máquina de práctica de Bácula Cliente conectada por red interna Servidor, a la que se le asigna IP por dhcp.

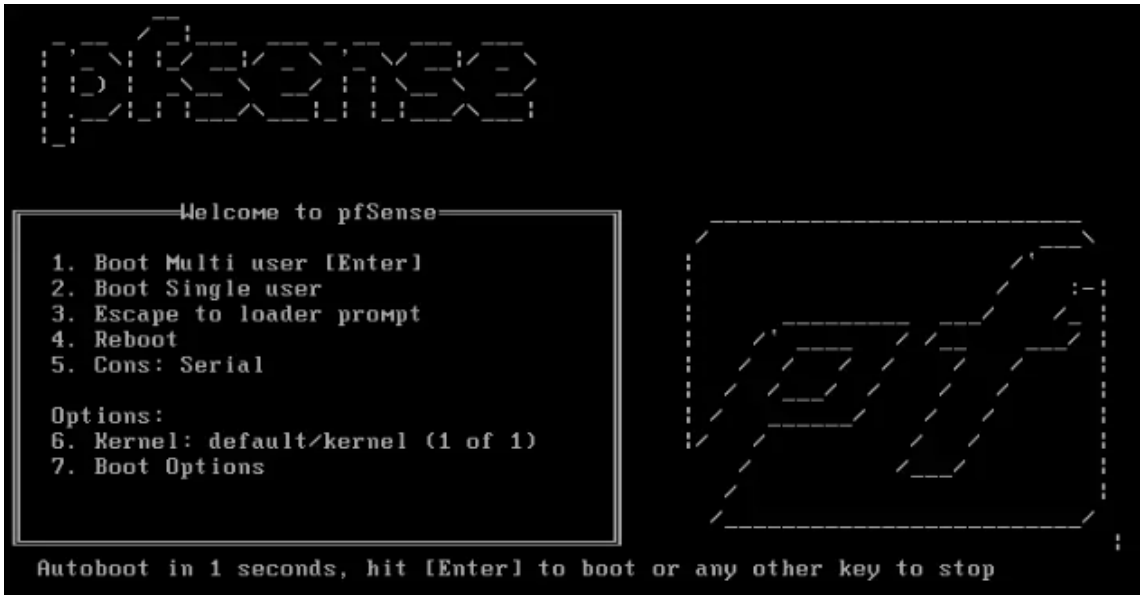



4ª máquina: Máquina Linux Mint en red WorkStation conectada por dhcp y con acceso a la configuración de PFsense via web.



# Instalación PFsense y configuración IPs.

Para realizar la instalación simplemente crearíamos la máquina con todas las redes y pondríamos el archivo ISO.



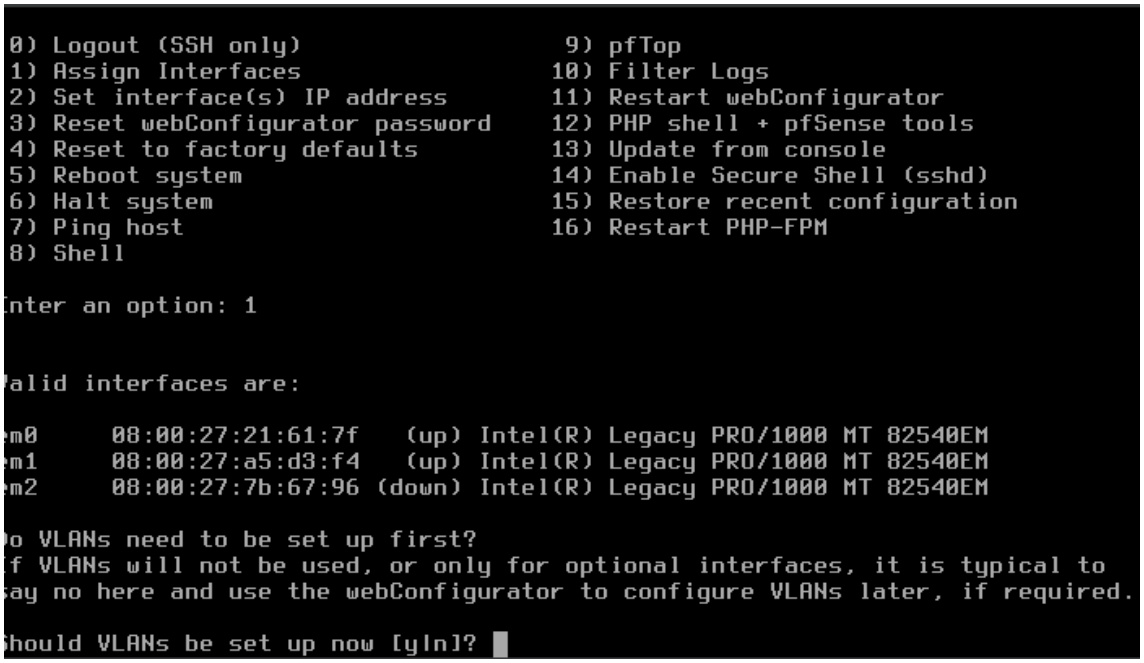

Aquí no haremos ninguna elección y comenzará la instalación.

Debemos aceptar el copyright y así seguiremos los pasos dándole a instalar y a todo continue o auto.

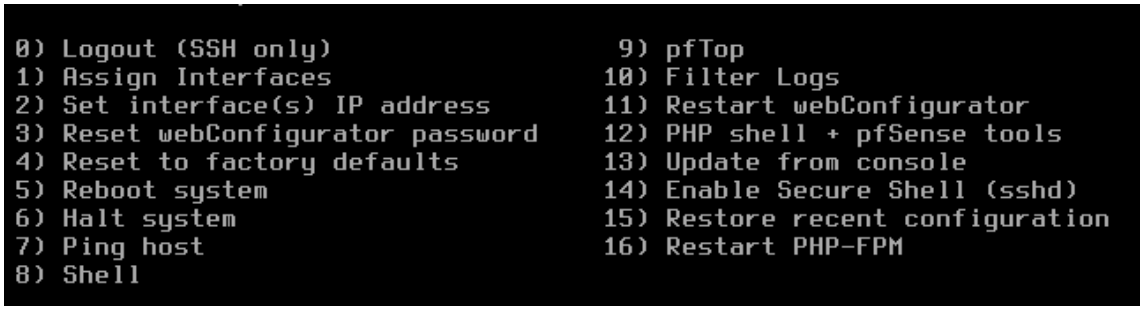
Una vez termine nos saldrá este mensaje si todo ha ido bien y le daremos a reboot.


*NOTA: Esta parte la hice al final porque en clase no hice capturas de este paso, así que algunas MACs no coinciden

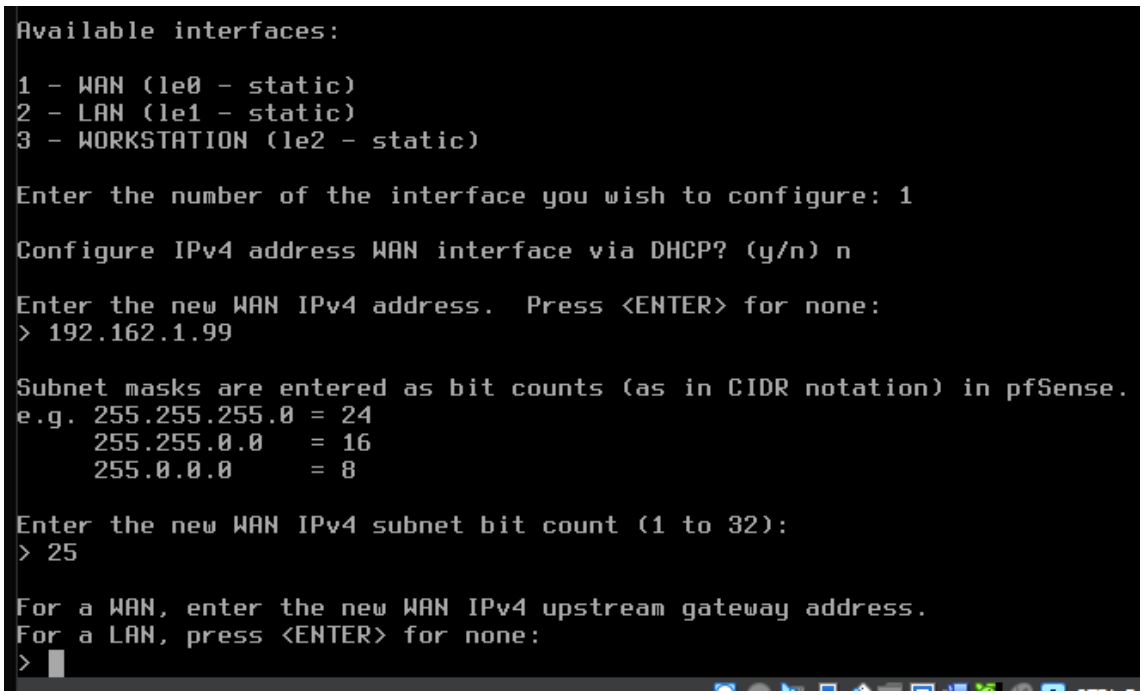
Cuando inicie debemos dar al 1 para seleccionar bien las interfaces y que estén operativas.



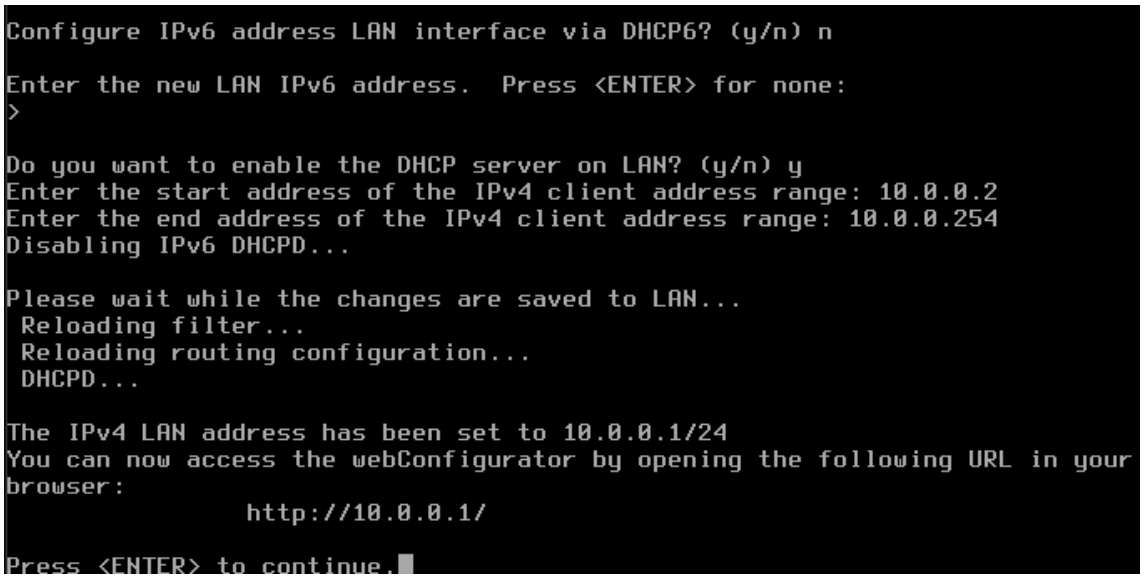

Una vez ya estén operativas ya podremos dar IP a las interfaces de la siguiente forma:



Seleccionaremos la opción 2 y seguiremos los pasos:



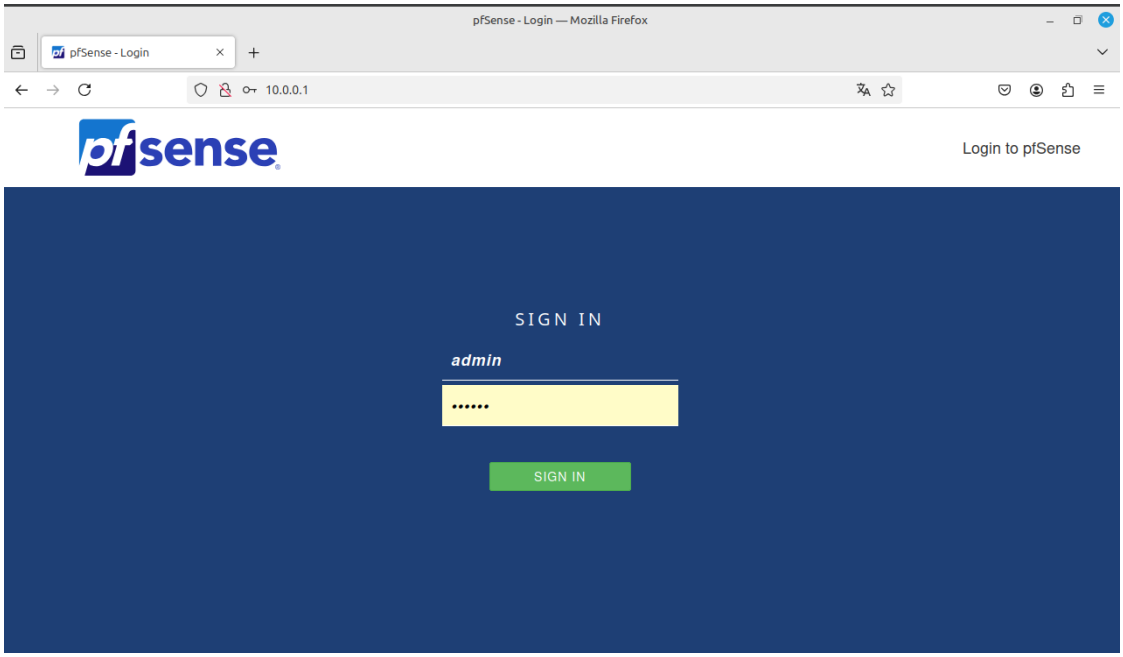

Para la interfaz 2: Servidor y 3: WorkStation pondremos también servidor DHCP y el rango.




Y así con ambas LAN.

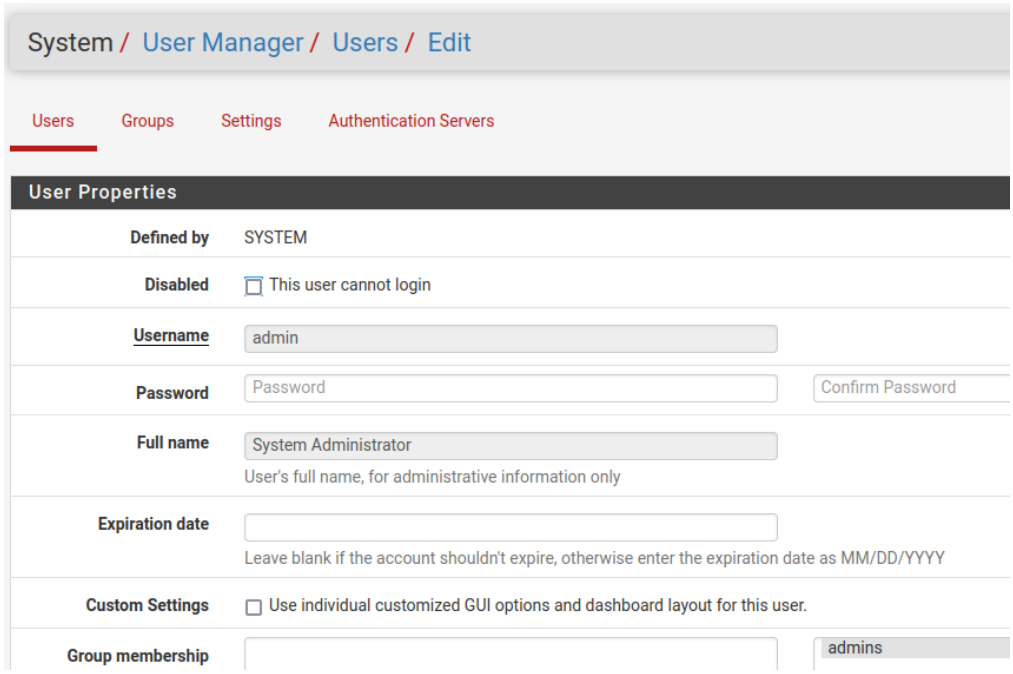
# Configuración de Firewall PFsense.

*NOTA: en un primer momento será necesario tener la máquina 4 dentro de la red Servidores.

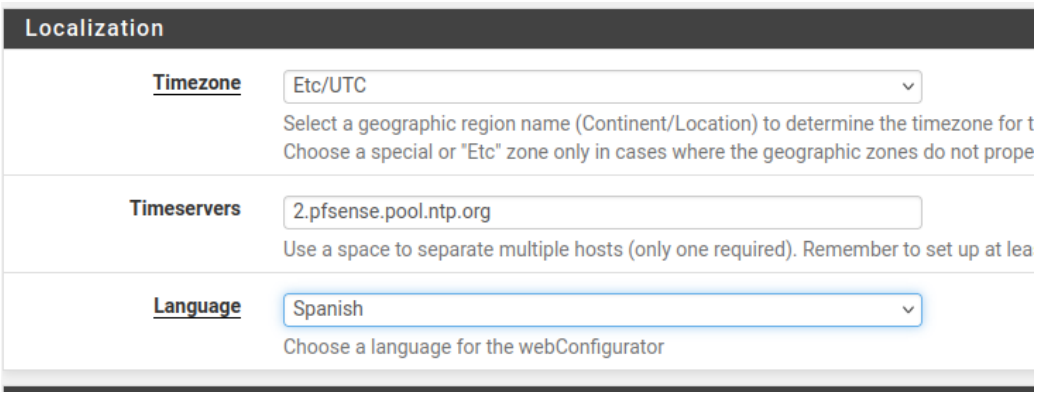



Las credenciales por defecto son usuario admin y contraseña pfsense. Esto es importante cambiarlo para que solo podamos acceder nosotros.

Para cambiar la contraseña iremos a System > User Manager > Users > System y le daremos a editar.

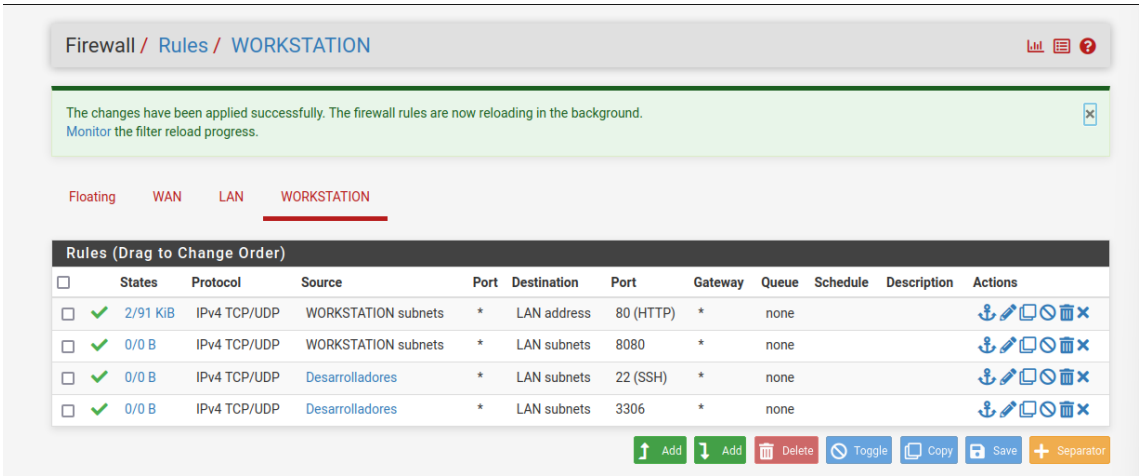


También sería interesante cambiar el idioma en caso de que se necesitara, para ello iremos a System > General Setup y bajaremos hasta Location. *Lo dejaré en inglés.

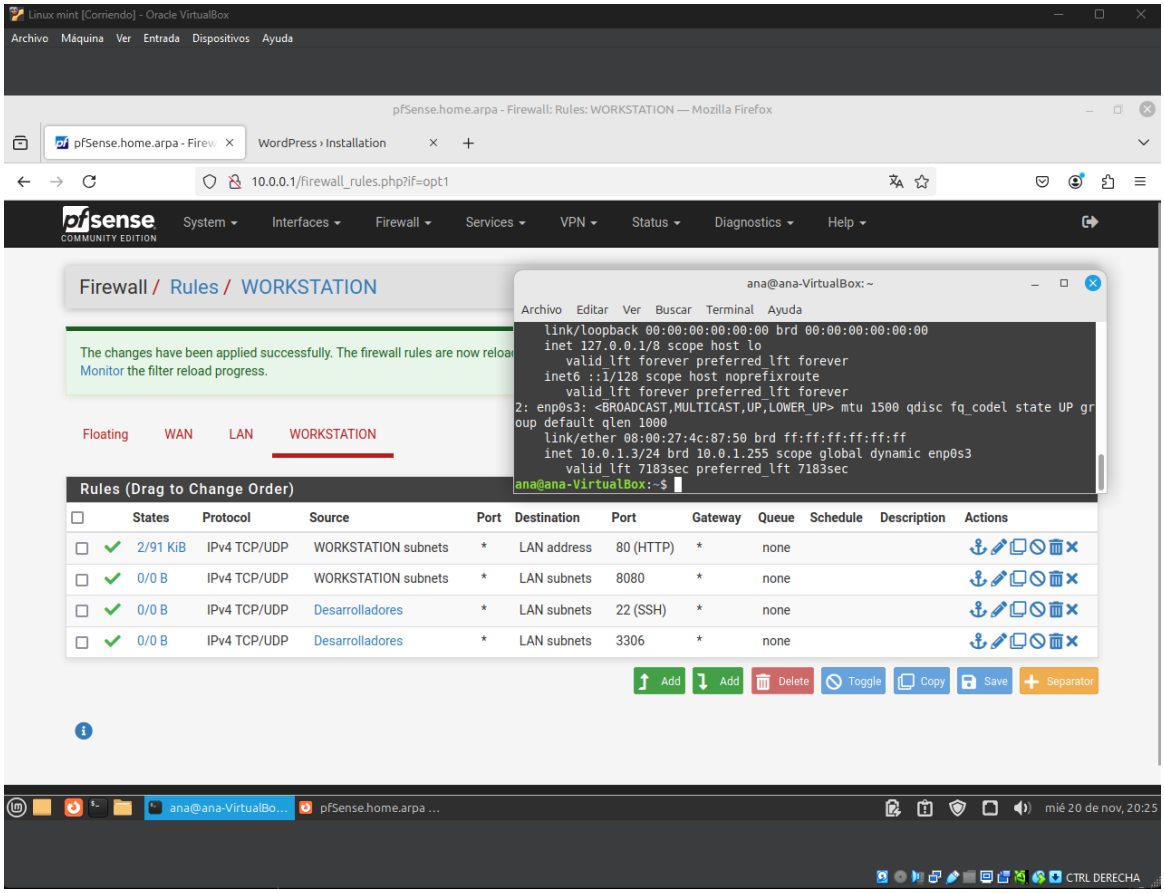


## Reglas Firewall.

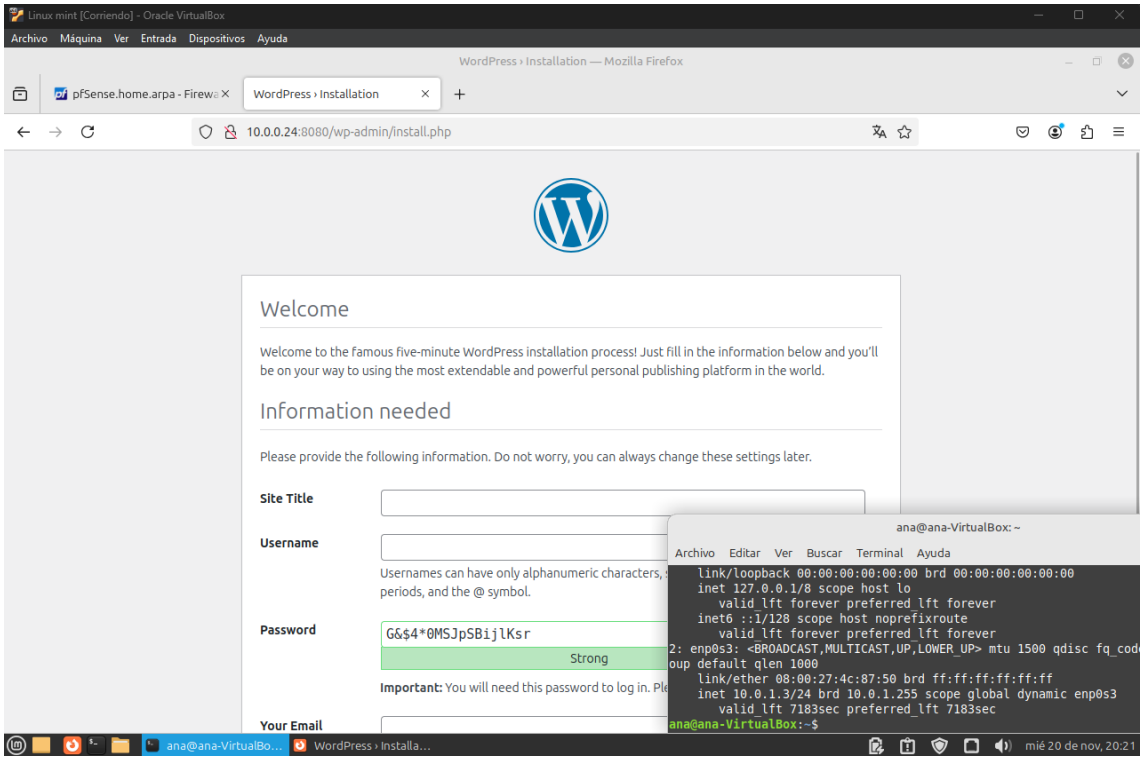
Así se verían todas:




La primera sirve para acceder desde la máquina 4 que está en red WorkStation a la configuración del PFsense.

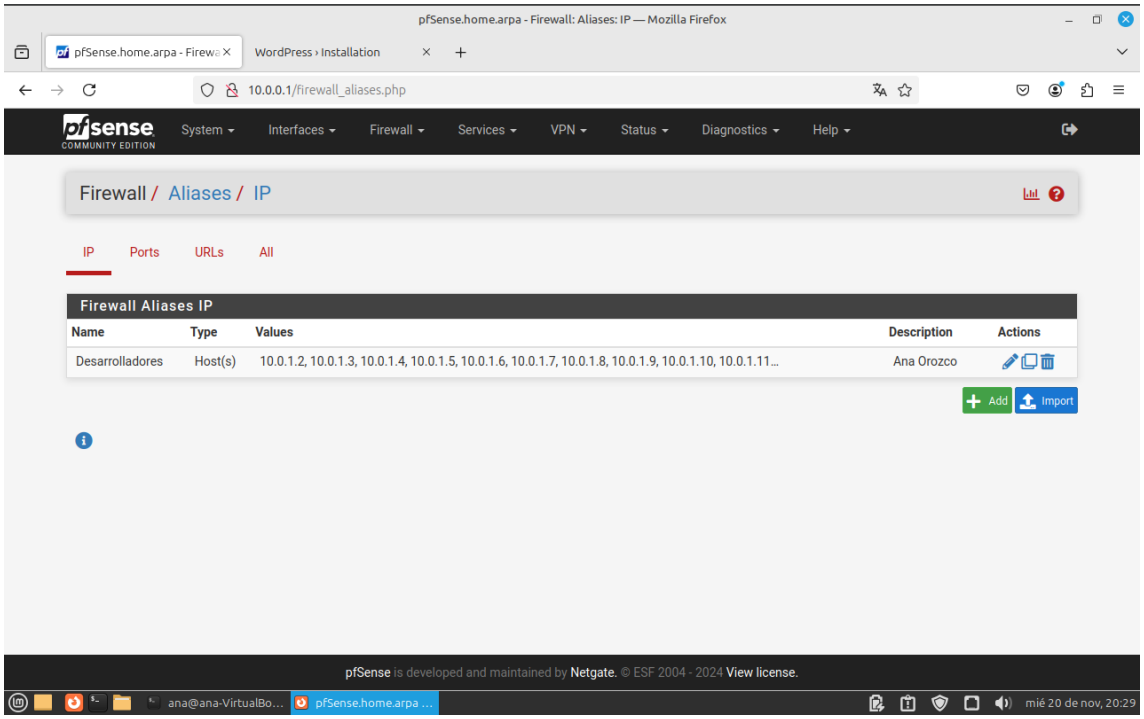


La segunda sirve para acceder desde máquina 4 que está en WorkStation a WordPress del Bacula Server que está en la red Servidor.



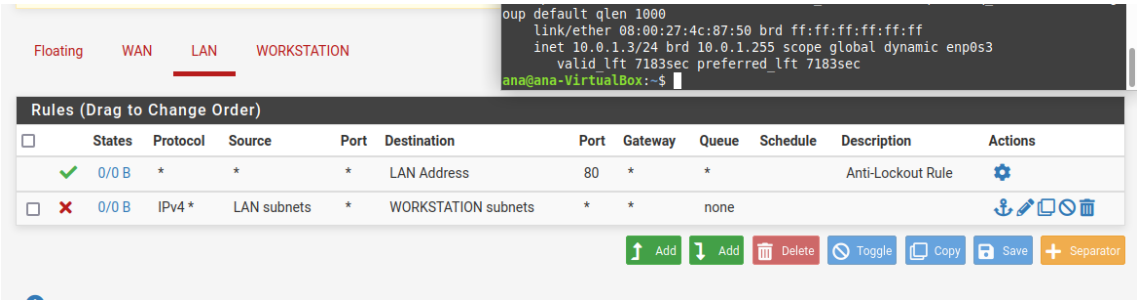

La 3º regla son para las IPs de Desarrolladores y será para que puedan acceder por SSH y que tengan acceso a Mysql de Wordpress,pero primero asignaré los alias, iremos a firewall > alianses.

De IPs usaré de la 10.0.1.2 – 10.0.1.22 para Desarrolladores.



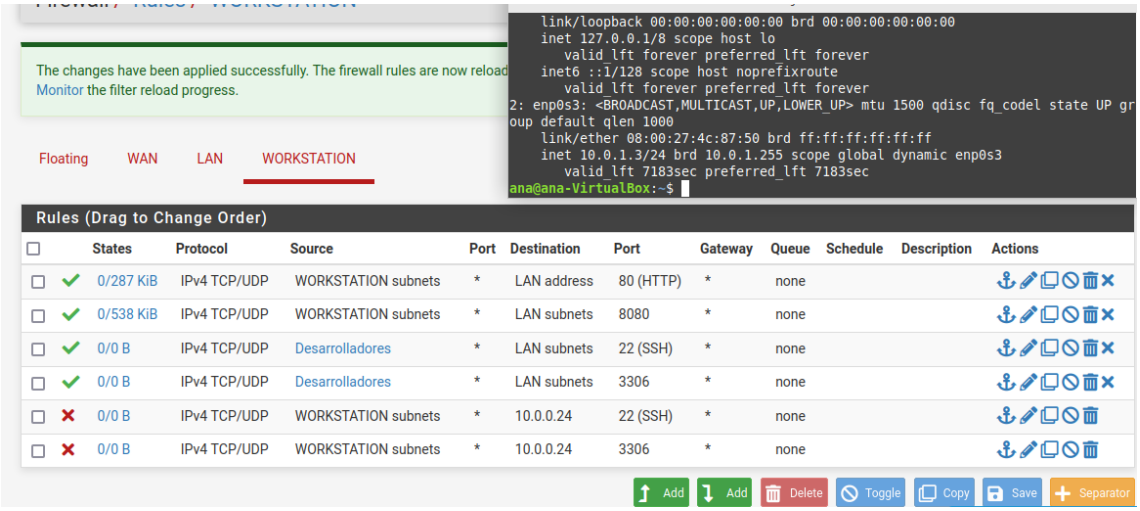
De esta manera cuando creamos la regla seleccionamos el alias Desarrolladores y solo funcionará en las IPs que hemos seleccionado.

Por último, la última regla que bloquea la conexión entre la red de servidores y la red Workstation. Yo he usado el bloqueo aunque también se puede denegar.



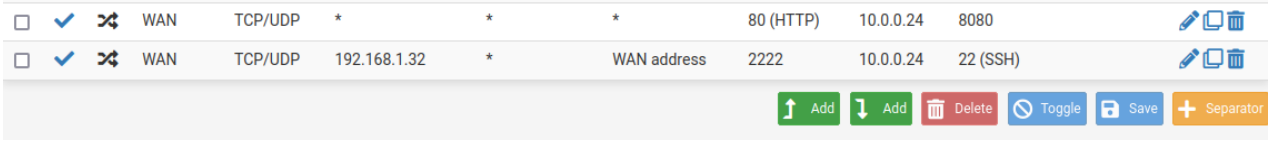

Como último paso para evitar que las demás IPs de WorkStation accedan a Mysql de Wordpress y que no se conecten por SSH crearé unas reglas que lo prohíban y las pondré DEBAJO de las que permiten, porque en PFsense es importante el orden, si pusiéramos estas reglas que bloquean arriba de las que permiten NO podrían acceder ni los Desarrolladores.

*Puse la IP de Wordpress porque luego en DHCP lo vamos a poner estática por MAC.

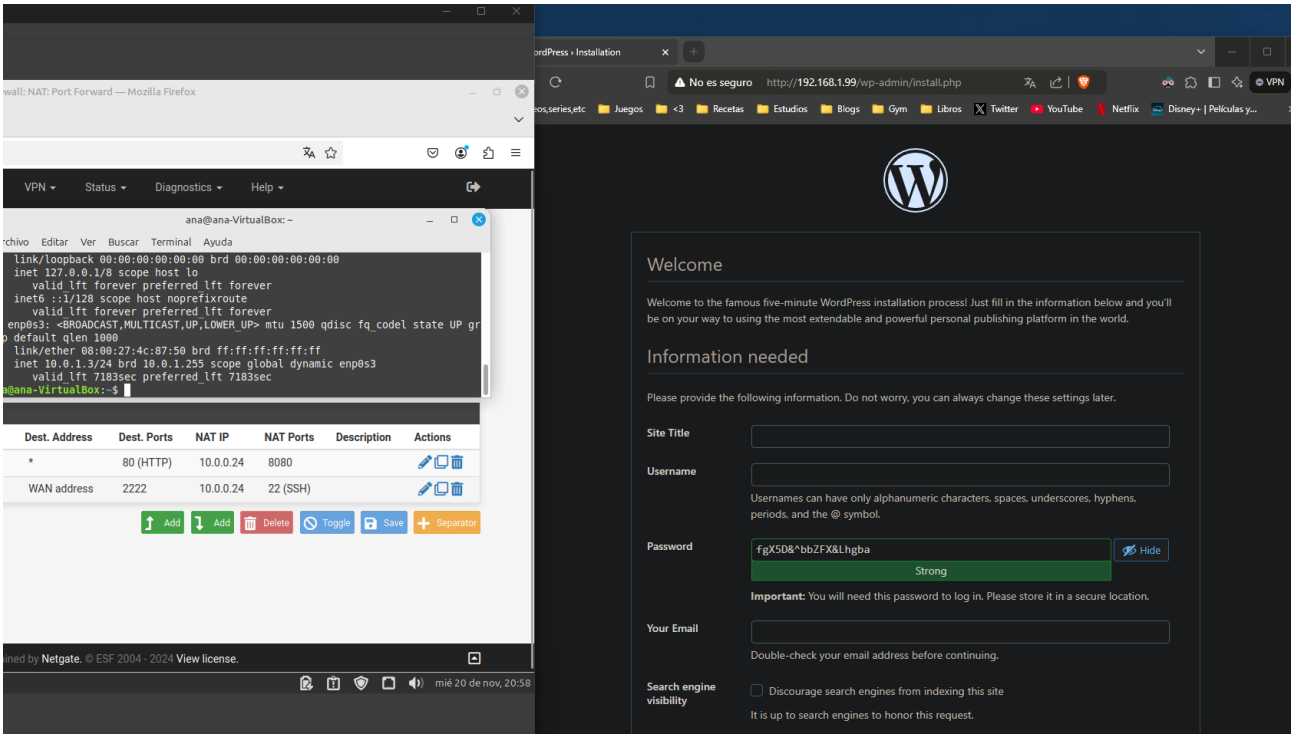


## Reglas NAT.

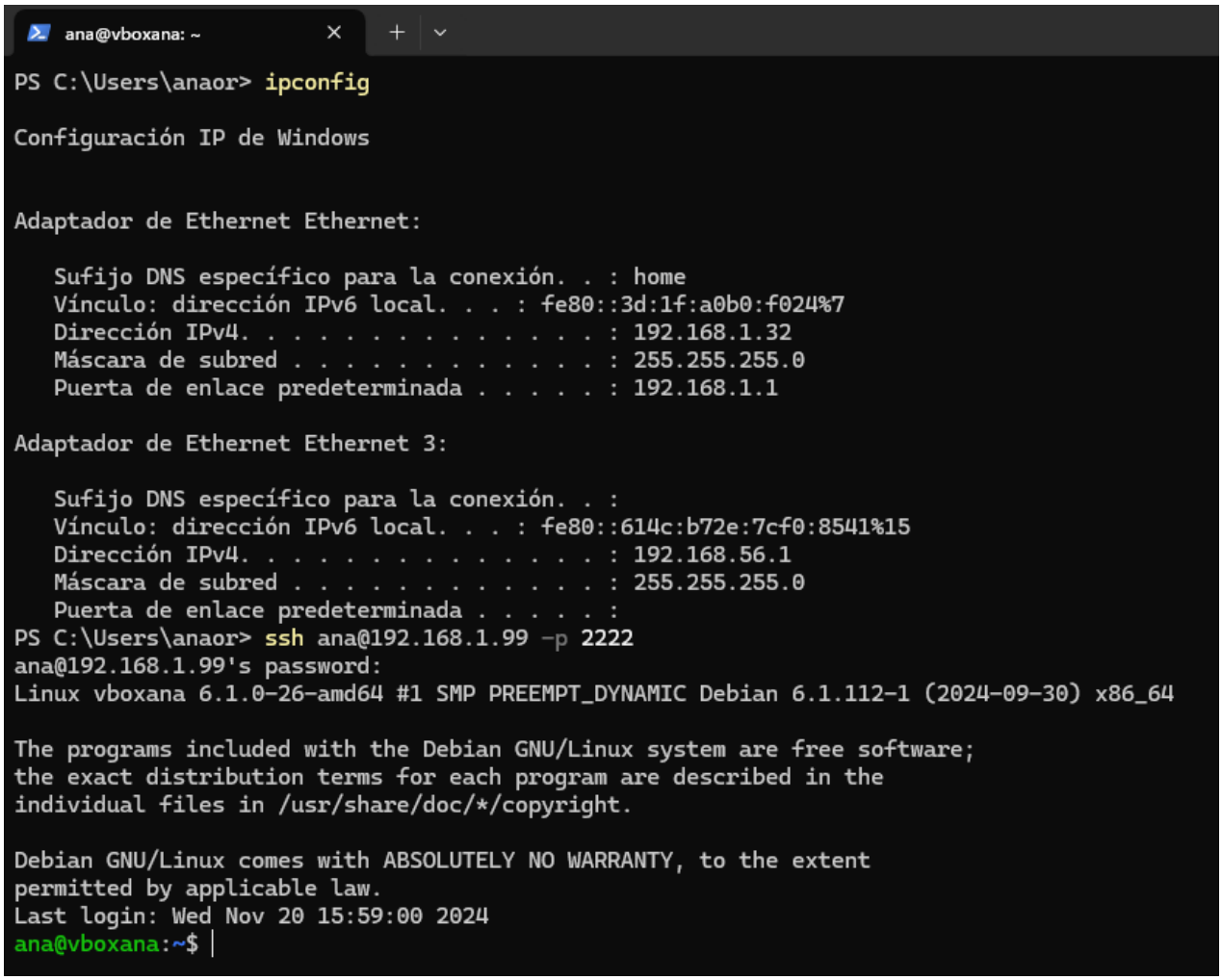
Para crear las reglas NAT iremos a Firewall > NAT. Así veríamos todas:




La primera regla nos deja acceder a wordpress desde el puerto 80, por lo que no pongo nada cuando pongo la ip.




La segunda regla me deja acceder desde la IP de mi casa por ssh a la ip del servidor Bacula.


ana@vboxana: ~
PS C:\Users\anaor> ipconfig
Configuración IP de Windows
Adaptador de Ethernet Ethernet:
Sufijo DNS específico para la conexión. . : home
Vínculo: dirección IPv6 local. . . : fe80::3d:1f:a0b0:f024%7
Dirección IPv4. . . . . : 192.168.1.32
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . . : 192.168.1.1
Adaptador de Ethernet Ethernet 3:
Sufijo DNS específico para la conexión. . :
Vínculo: dirección IPv6 local. . . : fe80::614c:b72e:7cf0:8541%15
Dirección IPv4. . . . . : 192.168.56.1
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . . :
PS C:\Users\anaor> ssh ana@192.168.1.99 -p 2222
ana@192.168.1.99's password:
Linux vboxana 6.1.0-26-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.112-1 (2024-09-30) x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Nov 20 15:59:00 2024
ana@vboxana:~$

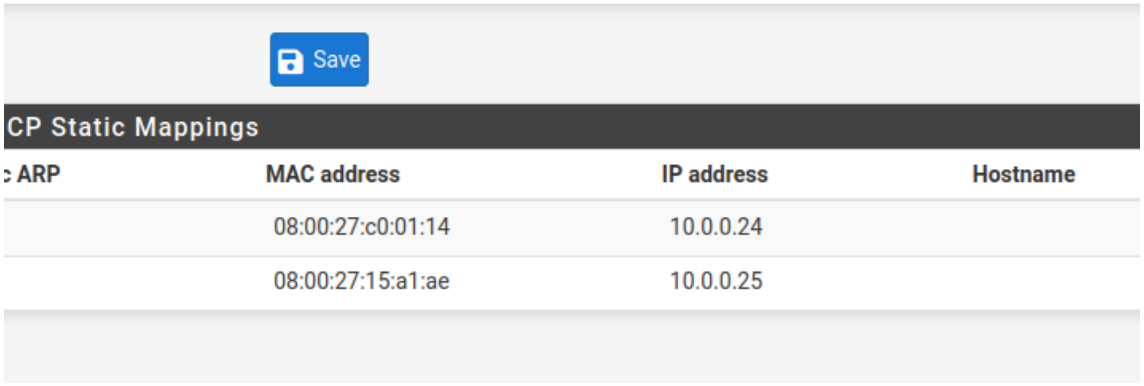
## DHCP.

Vamos a asignar IP estática a cada servidor mediante MAC y a los Desarrolladores (en este caso mi máquina Linux Mint que hasta ahora ha tenido IP fuera del rango de los Desarrolladores).

*NOTA: antes de hacer esto habrá que cambiar los rangos de DHCP en la configuración del servidor. Y después habrá que cambiar las reglas donde esté la IP antigua(en caso de ser necesario)

Iremos a Services > DHCP Server y cambiaremos entre interfaces dependiendo de cual queramos editar.

Así se verían las IPs de la LAN y la comprobación:




Bacula server:

Bacula cliente:

```
root@vboxana2:/home/ana2# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
    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 noprefixroute
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_code
    link/ether 08:00:27:15:a1:ae brd ff:ff:ff:ff:ff:ff
    inet 10.0.0.25/24 brd 10.0.0.255 scope global dynamic enp0s3
       valid_lft 6984sec preferred_lft 6984sec
    inet6 fe80::a00:27ff:fe15:a1ae/64 scope link
       valid_lft forever preferred_lft forever
root@vboxana2:/home/ana2#
```

Y así en WorkStation y su comprobación: