



---

# PFSENSE: FIREWALL

---

SAD



2ºASIR

I.E.S. ANTONIO MACHADO  
ANA OROZCO ASENSIO

## Contenido

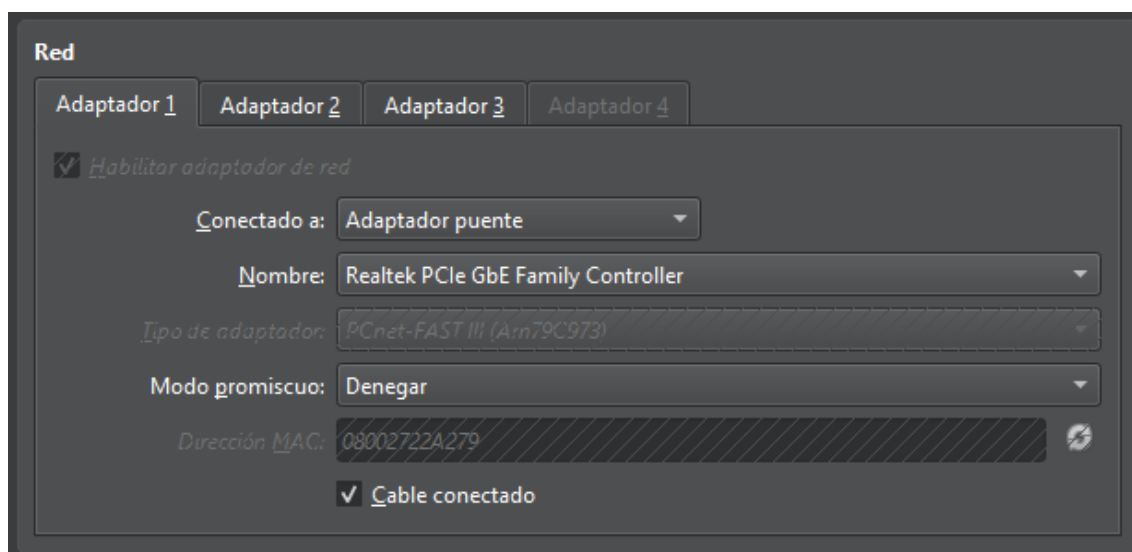
Introducción. ....	2
Instalación PFSense y configuración IPs.....	5
Configuración de Firewall PFSense. ....	8
Reglas Firewall. ....	10
Reglas NAT. ....	13
DHCP.....	15

## Introducción.

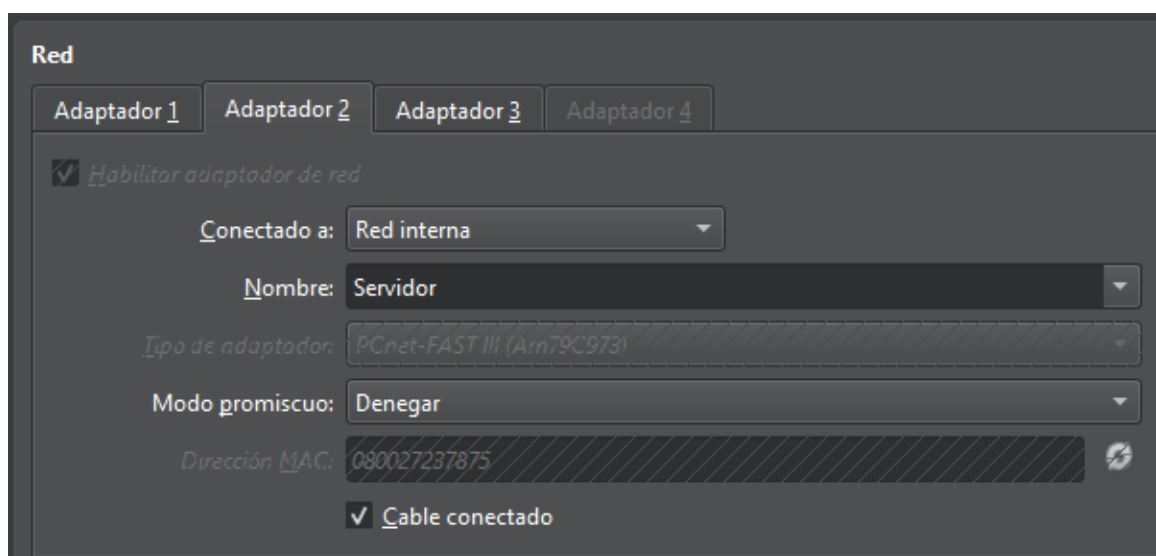
En esta práctica vamos a usar 4 máquinas para simular una empresa que necesita Firewall.

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

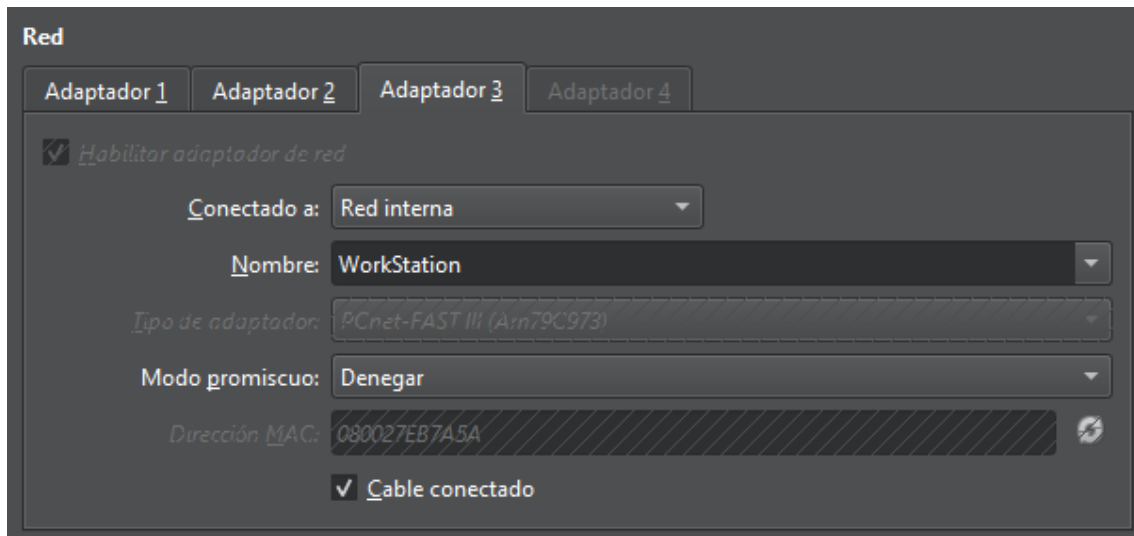
Red 1 → Adaptador puente, esta irá a internet y tendrá IP estática con el rango de los pc de clase (192.168.2.99/21) pero en casa usaré una ip dentro de mi rango (192.168.1.99/24).



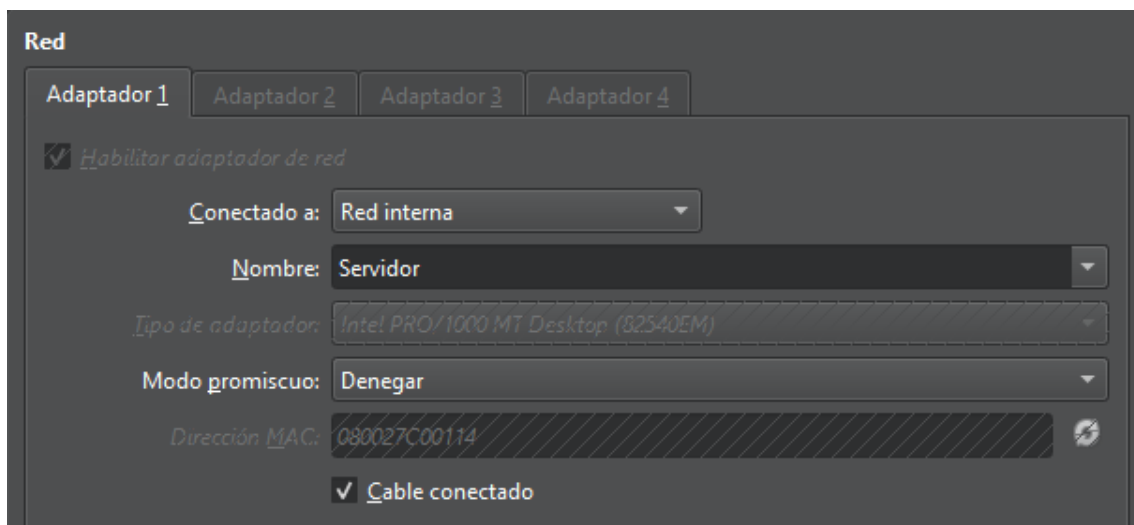
Red 2 → Red interna que llamaré Servidor. Le asignaré la IP 10.0.0.1/24 y activaremos DHCP en PfSense en el rango 10.0.0.2 – 10.0.0.254 /24 (más adelante mostraré capturas de este proceso).



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 Bacula 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 Bacula Cliente conectada por red interna Servidor, a la que se le asigna IP por dhcp.

**Red**

Adaptador 1   Adaptador 2   Adaptador 3   Adaptador 4

☒ *Habilitar adaptador de red*

Conectado a: Red interna

Nombre: Servidor

Tipo de adaptador: Intel PRO/1000 MT Desktop (82540EM)

Modo promiscuo: Denegar

Dirección MAC: 08002715A1AE

☒ Cable conectado

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

**Red**

Adaptador 1   Adaptador 2   Adaptador 3   Adaptador 4

☒ *Habilitar adaptador de red*

Conectado a: Red interna

Nombre: Servidor

Tipo de adaptador: Intel PRO/1000 MT Desktop (82540EM)

Modo promiscuo: Denegar

Dirección MAC: 0800274C8750

☒ Cable conectado

## 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.

```
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) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell

Enter an option: 1

Valid interfaces are:

em0      08:00:27:21:61:7f   (up) Intel(R) Legacy PRO/1000 MT 82540EM
em1      08:00:27:a5:d3:f4   (up) Intel(R) Legacy PRO/1000 MT 82540EM
em2      08:00:27:7b:67:96   (down) Intel(R) Legacy PRO/1000 MT 82540EM

Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.
Should VLANs be set up now [y|n]? █
```

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

```
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) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell
```

Seleccionaremos la opción 2 y seguiremos los pasos:

```
Available interfaces:
1 - WAN (le0 - static)
2 - LAN (le1 - static)
3 - WORKSTATION (le2 - static)

Enter the number of the interface you wish to configure: 1

Configure IPv4 address WAN interface via DHCP? (y/n) n

Enter the new WAN IPv4 address. Press <ENTER> for none:
> 192.162.1.99

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new WAN IPv4 subnet bit count (1 to 32):
> 25

For a WAN, enter the new WAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> █
```

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

```
Configure IPv6 address LAN interface via DHCP6? (y/n) n

Enter the new LAN IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 10.0.0.2
Enter the end address of the IPv4 client address range: 10.0.0.254
Disabling IPv6 DHCPD...

Please wait while the changes are saved to LAN...
Reloading filter...
Reloading routing configuration...
DHCPD...

The IPv4 LAN address has been set to 10.0.0.1/24
You can now access the webConfigurator by opening the following URL in your
browser:
      http://10.0.0.1/

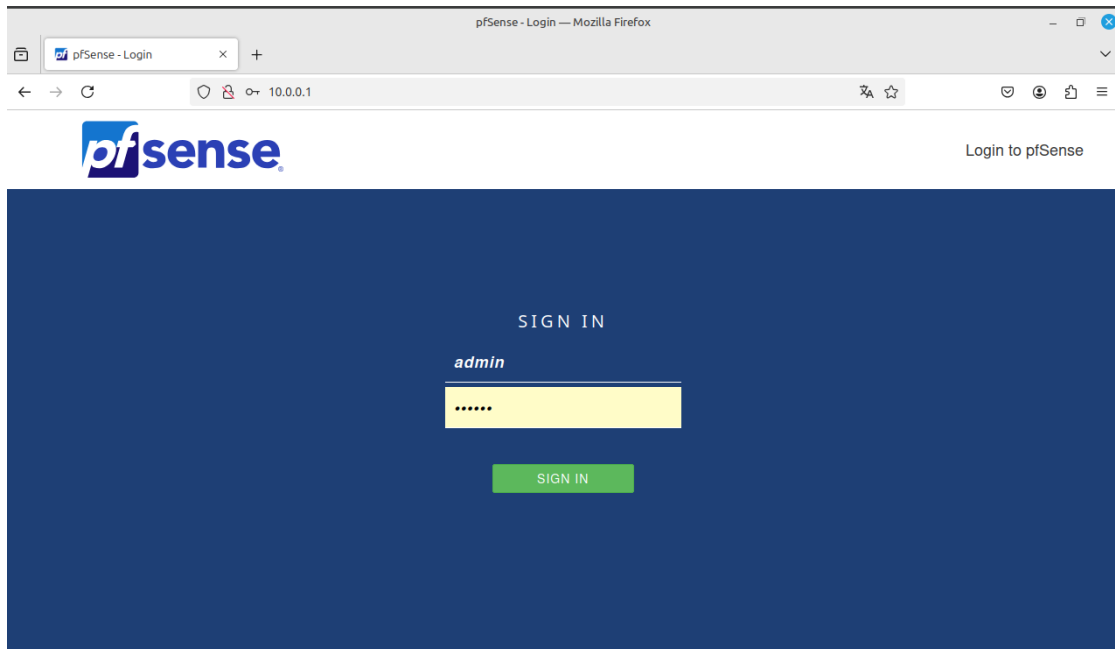
Press <ENTER> to continue. █
```

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.

System / [User Manager](#) / [Users](#) / [Edit](#)

[Users](#) [Groups](#) [Settings](#) [Authentication Servers](#)

### User Properties

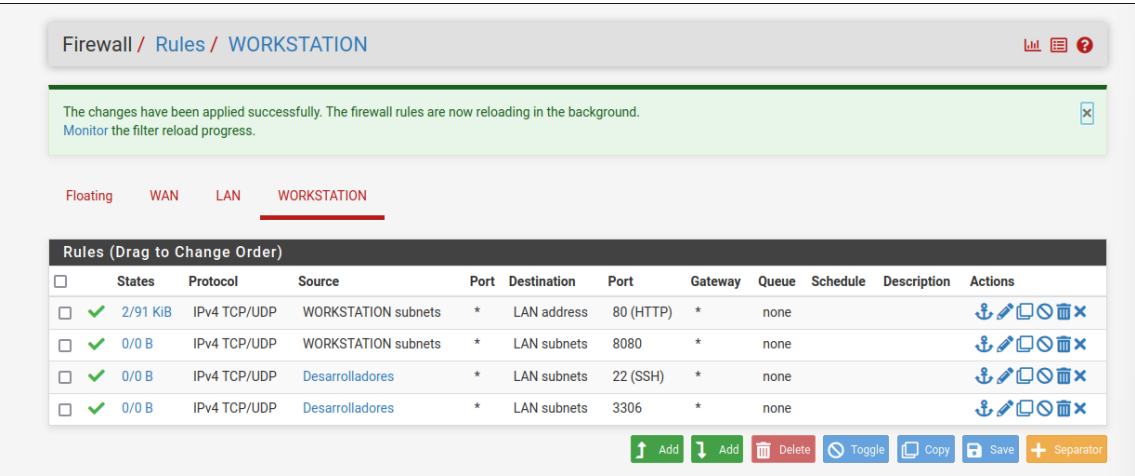
Defined by	SYSTEM	
Disabled	<input type="checkbox"/> This user cannot login	
Username	<input type="text" value="admin"/>	
Password	<input type="password" value="Password"/>	<input type="password" value="Confirm Password"/>
Full name	<input type="text" value="System Administrator"/> <small>User's full name, for administrative information only</small>	
Expiration date	<input type="text"/> <small>Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY</small>	
Custom Settings	<input type="checkbox"/> Use individual customized GUI options and dashboard layout for this user.	
Group membership	<input type="text" value="admins"/>	

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.

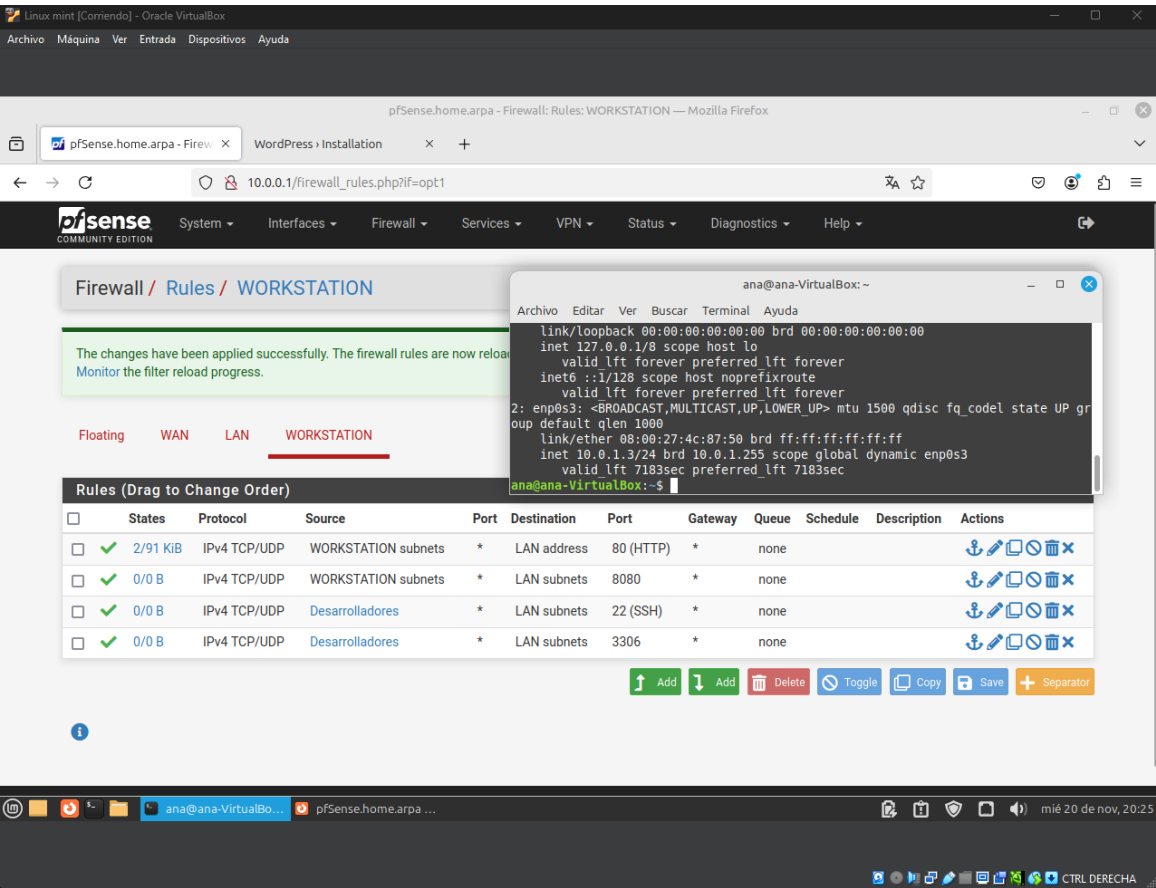
Localization	
<b><u>Timezone</u></b>	<div>Etc/UTC</div> <div>Select a geographic region name (Continent/Location) to determine the timezone for t Choose a special or "Etc" zone only in cases where the geographic zones do not prope</div>
<b><u>Timeservers</u></b>	<div>2.pfsense.pool.ntp.org</div> <div>Use a space to separate multiple hosts (only one required). Remember to set up at lea</div>
<b><u>Language</u></b>	<div>Spanish</div> <div>Choose a language for the webConfigurator</div>

# Reglas Firewall.

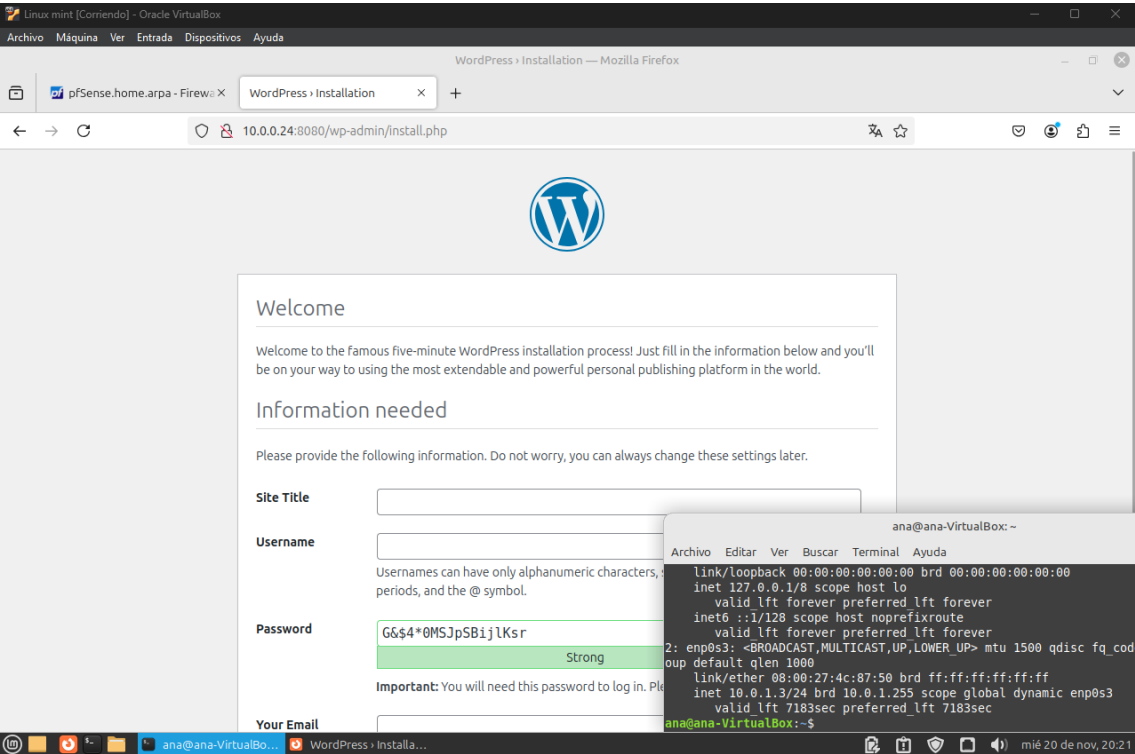
Así se verían todas:



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

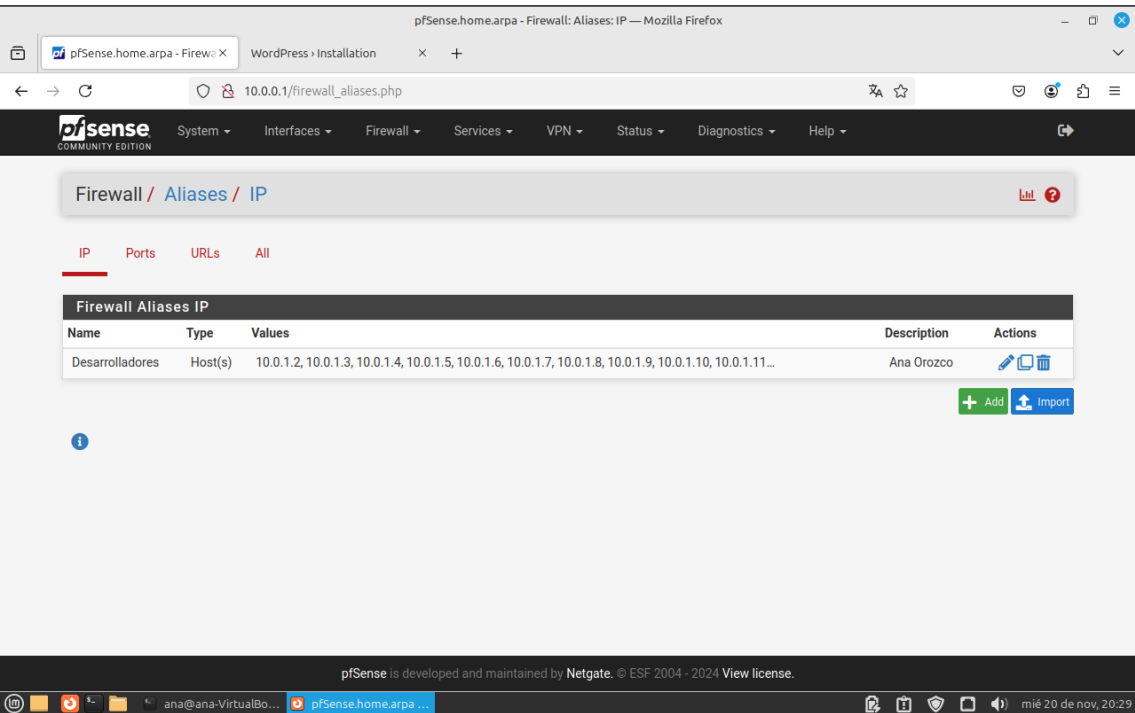


La segunda sirve para acceder desde máquina 4 que está en WorkStation a WordPress del Bacula Server que está en la red Servidor.



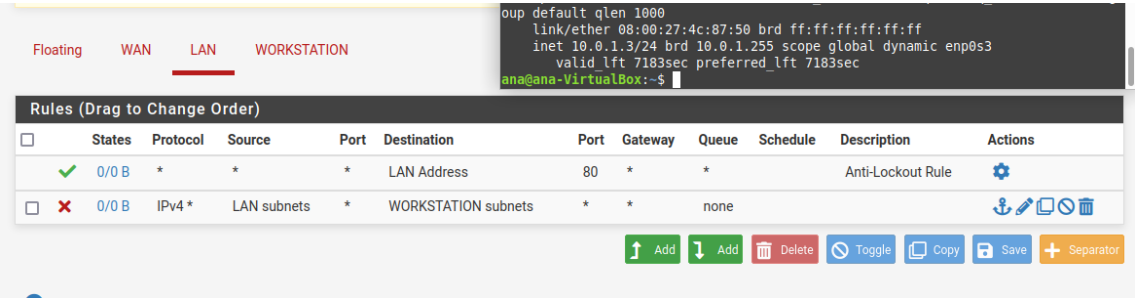
La 3º regla son para las IPs de Desarrolladores y será para que puedan acceder por SSH y que tengan acceso a Mysql de Wordpress,pero primero asignaré los alias, iremos a firewall > alianse.

De IPs usaré de la 10.0.1.2 – 10.0.1.22 para Desarrolladores.



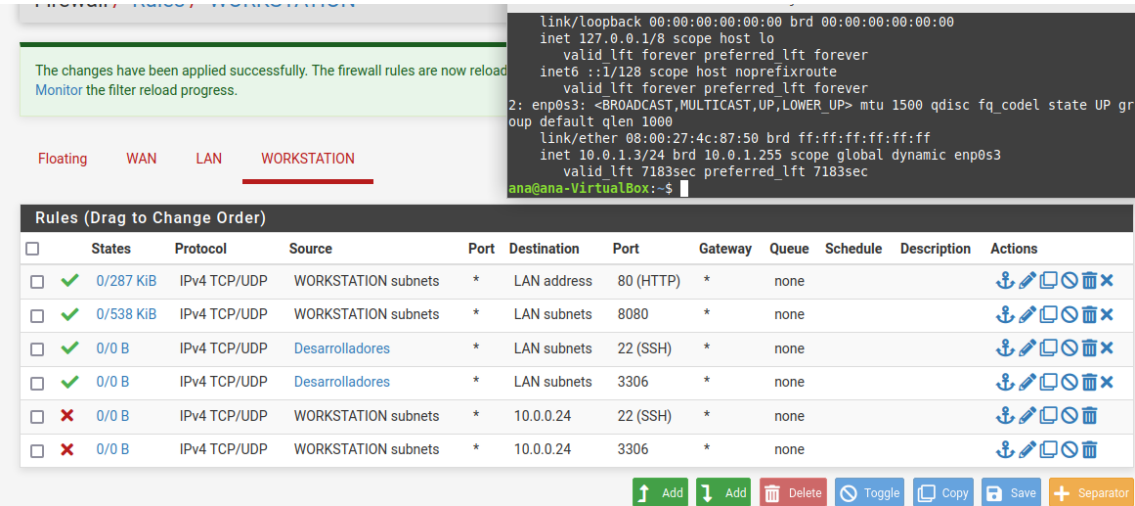
De esta manera cuando creamos la regla seleccionamos el alias Desarrolladores y solo funcionará en las IPs que hemos seleccionado.

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:

<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	WAN	TCP/UDP	*	*	*	80 (HTTP)	10.0.0.24	8080		
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	WAN	TCP/UDP	192.168.1.32	*	WAN address	2222	10.0.0.24	22 (SSH)		
<div> Add  Add  Delete  Toggle  Save  Separator</div>												

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

The screenshot shows a Netgate firewall configuration interface. On the left, a terminal window displays network configuration commands and their outputs. The main area shows a table of NAT rules. The first rule is for port 80 (HTTP) with a NAT IP of 10.0.0.24 and a NAT Port of 8080. The second rule is for port 2222 (SSH) with a NAT IP of 10.0.0.24 and a NAT Port of 22. Below the table are buttons for adding, deleting, toggling, saving, and separating rules. On the right, a browser window shows the WordPress installation process, with fields for Site Title, Username, Password, and Your Email.

Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
*	80 (HTTP)	10.0.0.24	8080		
WAN address	2222	10.0.0.24	22 (SSH)		

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:

			
CP Static Mappings			
Interface	MAC address	IP address	Hostname
enp0s3	08:00:27:c0:01:14	10.0.0.24	
enp0s3	08:00:27:15:a1:ae	10.0.0.25	

Bacula server:

```
root@vboxana:/home/ana# 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_codel
    link/ether 08:00:27:c0:01:14 brd ff:ff:ff:ff:ff:ff
    inet 10.0.0.24/24 brd 10.0.0.255 scope global dynamic enp0s3
        valid_lft 7196sec preferred_lft 7196sec
    inet6 fe80::a00:27ff:fec0:114/64 scope link
        valid_lft forever preferred_lft forever
```



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:

The screenshot shows the Oracle VM VirtualBox Workstation interface. On the left, there are four virtual machines listed, each with a 'Display Advanced' button. Below them is a 'Save' button. On the right, a terminal window titled 'ana@ana-VirtualBox: ~' is open, displaying the output of the 'ip a' command, which shows the network configuration for the 'ana' VM. The terminal output is identical to the one shown in the previous block. Below the terminal window, there is a table titled 'ings' (likely 'Networks') with the following columns: 'MAC address', 'IP address', 'Hostname', and 'Descripti' (likely 'Description'). The table contains one entry with MAC address '08:00:27:4c:87:50' and IP address '10.0.1.3'.

MAC address	IP address	Hostname	Descripti
08:00:27:4c:87:50	10.0.1.3		