



PFSENSE: FIREWALL

SAD



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

Contenido

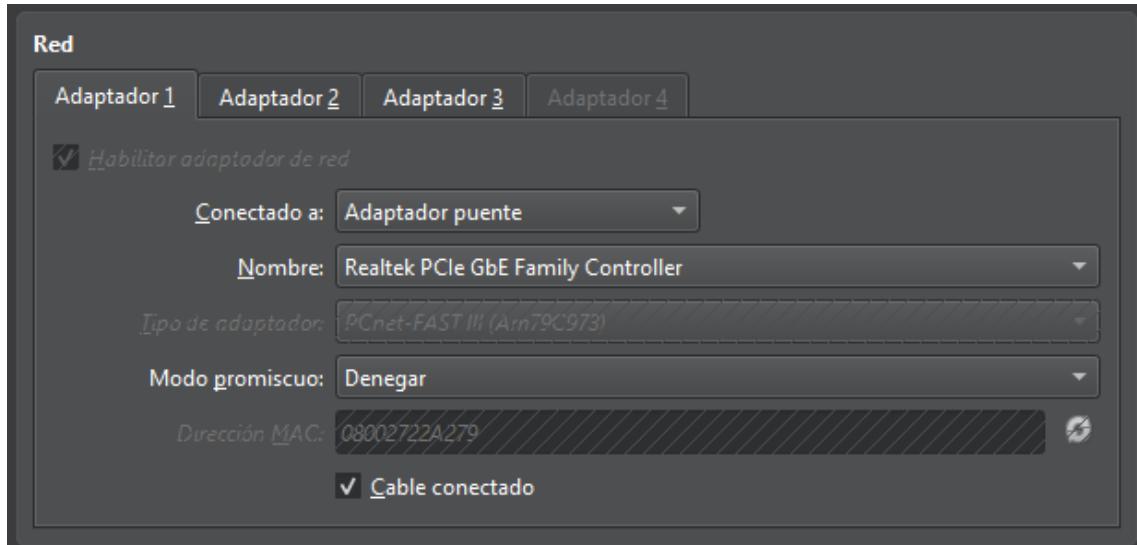
Introducción.....	2
Instalación PFsense y configuración IPs.....	5
Configuración de Firewall PFsense.	8
Reglas Firewall.	10
Reglas NAT.	13
DHCP.....	15

Introducción.

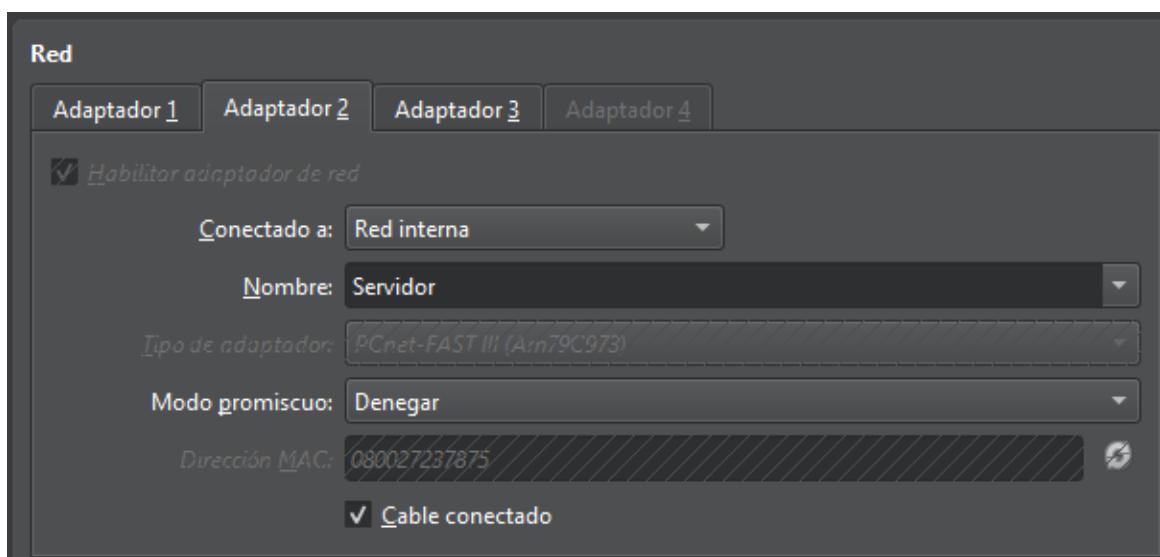
En esta práctica vamos a usar 4 máquinas para simular una empresa que necesita Firewall.

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

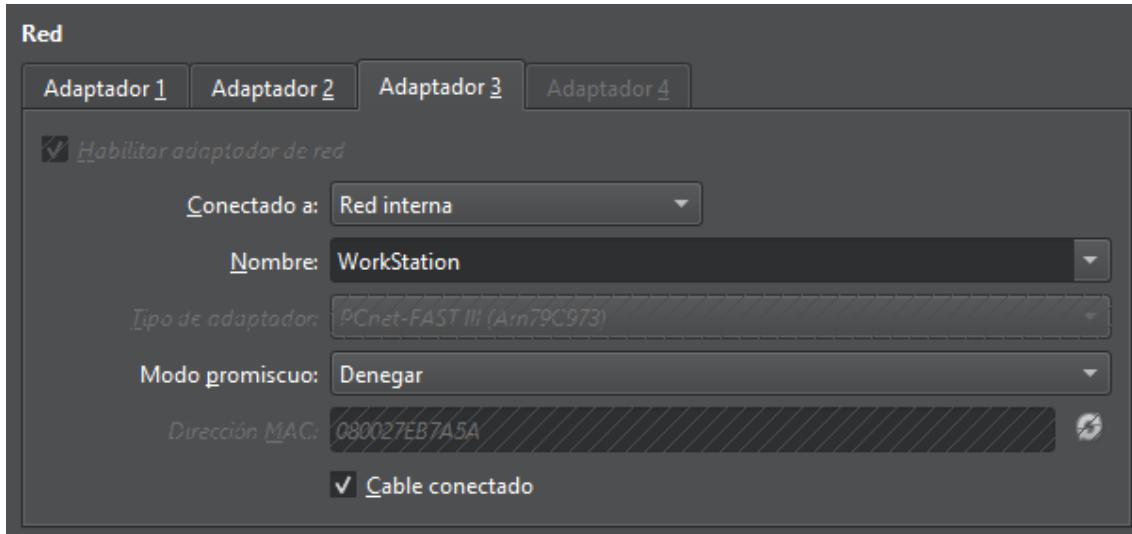
Red 1 → Adaptador puente, esta irá a internet y tendrá IP estática con el rango de los pc de clase (192.168.2.99/21) pero en casa usare una ip dentro de mi rango (192.168.1.99/24).



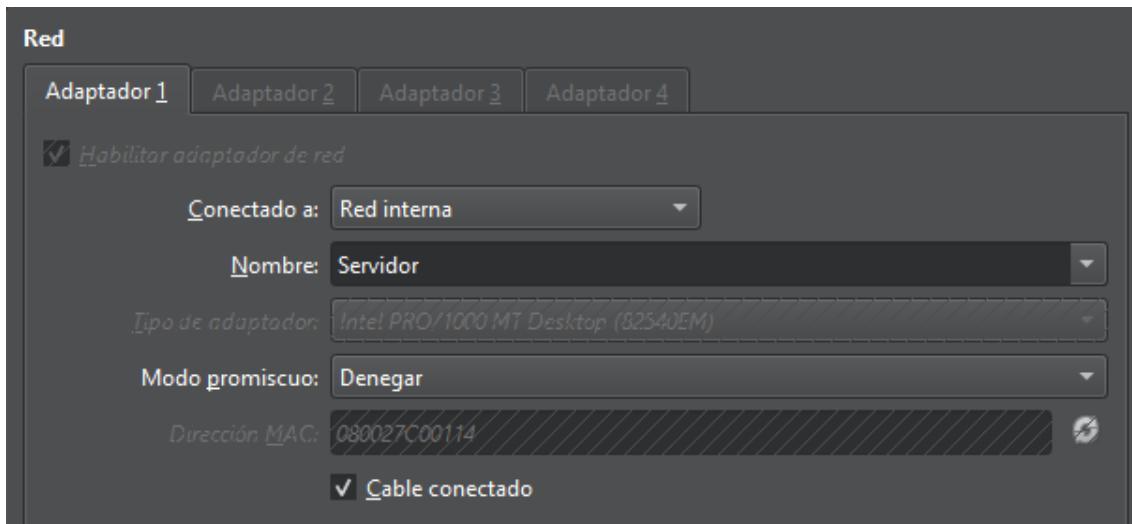
Red 2 → Red interna que llamaré Servidor. Le asignaré la IP 10.0.0.1/24 y activaremos DHCP en PFsense en el rango 10.0.0.2 – 10.0.0.254 /24 (más adelante mostraré capturas de este proceso).



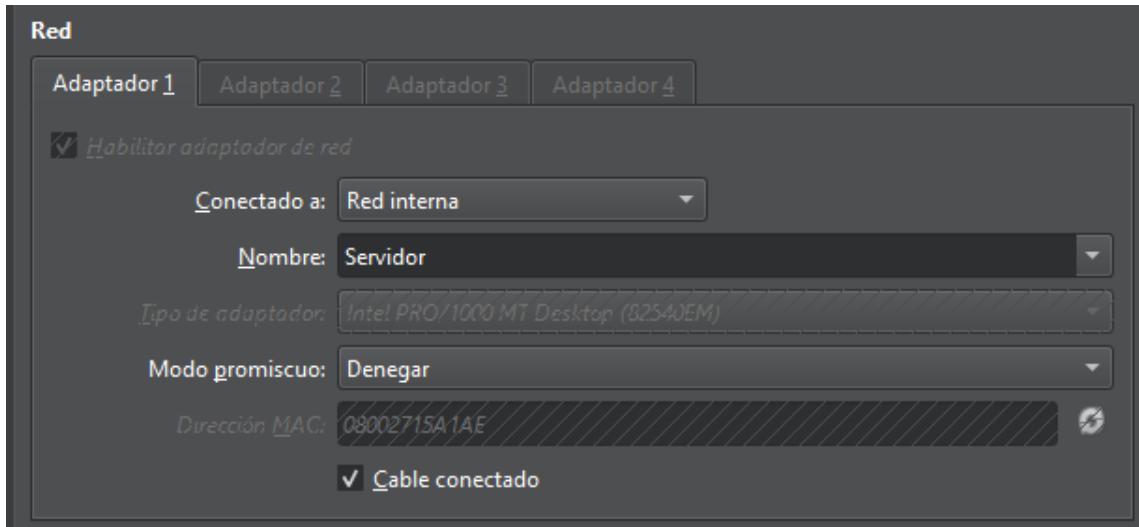
Red 3 → Red interna que llamaré WorkStation. Le asignaré la IP 10.0.1.1/24 y activaremos DHCP en PFsense en el rango 10.0.1.2 – 10.0.1.254 /24 (más adelante mostraré capturas de este proceso).



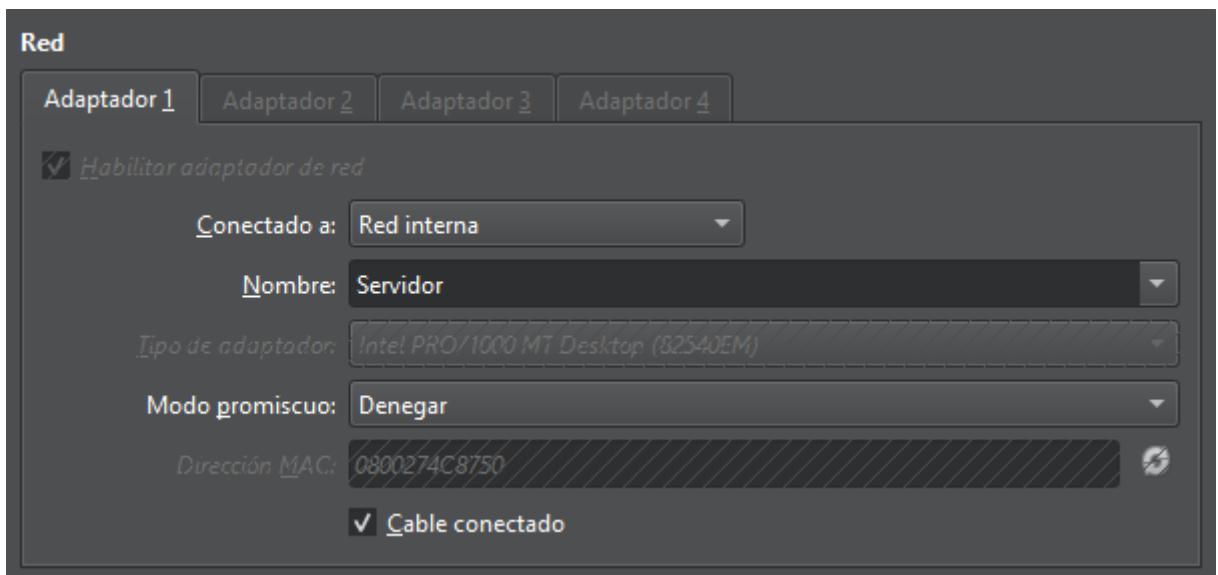
2^a máquina: Máquina de práctica de Bácula Server conectada por red interna Servidor, a la que se le asigna IP por dhcp y se inicia un Docker-compose.



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



4^a 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.

```
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

No 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\ln]? █
```

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:  
> █
```

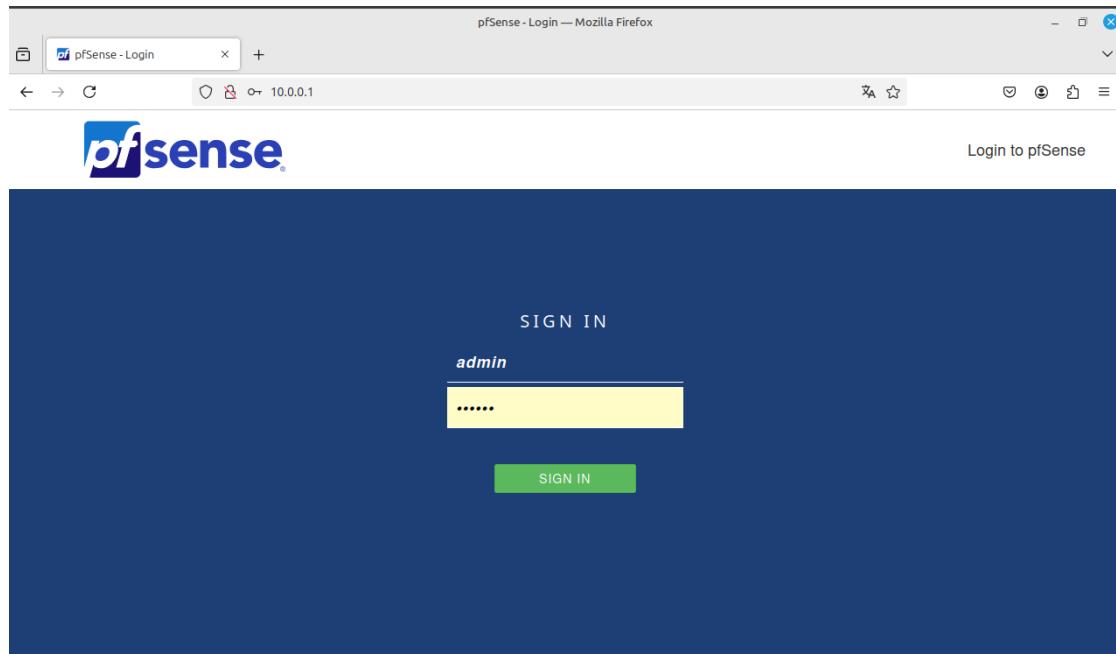
Para la interfaz 2: Servidor y 3: WorkStation pondremos también servidor DHCP y el rango.

```
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.

A screenshot of the pfSense User Manager - Edit screen. The URL in the address bar is "System / User Manager / Users / Edit". The top navigation bar includes "Users", "Groups", "Settings", and "Authentication Servers", with "Users" being the active tab. A sub-header "User Properties" is visible. The form contains the following fields:

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

Timezone	Etc/UTC
Select a geographic region name (Continent/Location) to determine the timezone for this system. Choose a special or "Etc" zone only in cases where the geographic zones do not properly represent your location.	
Timeservers	2.pfsense.pool.ntp.org
Use a space to separate multiple hosts (only one required). Remember to set up at least one NTP server.	
Language	Spanish
Choose a language for the webConfigurator	

Reglas Firewall.

Así se verán todas:

The screenshot shows the pfSense Firewall Rules interface. At the top, there are tabs for Floating, WAN, LAN, and WORKSTATION, with WORKSTATION selected. Below the tabs is a table titled "Rules (Drag to Change Order)". The table has columns for States, Protocol, Source, Port, Destination, Port, Gateway, Queue, Schedule, Description, and Actions. There are four rows in the table:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 2/91 KiB	IPv4 TCP/UDP	WORKSTATION subnets	*	LAN address	80 (HTTP)	*	none			
✓ 0/0 B	IPv4 TCP/UDP	WORKSTATION subnets	*	LAN subnets	8080	*	none			
✓ 0/0 B	IPv4 TCP/UDP	Desarrolladores	*	LAN subnets	22 (SSH)	*	none			
✓ 0/0 B	IPv4 TCP/UDP	Desarrolladores	*	LAN subnets	3306	*	none			

At the bottom of the interface are buttons for Add, Delete, Toggle, Copy, Save, and Separator.

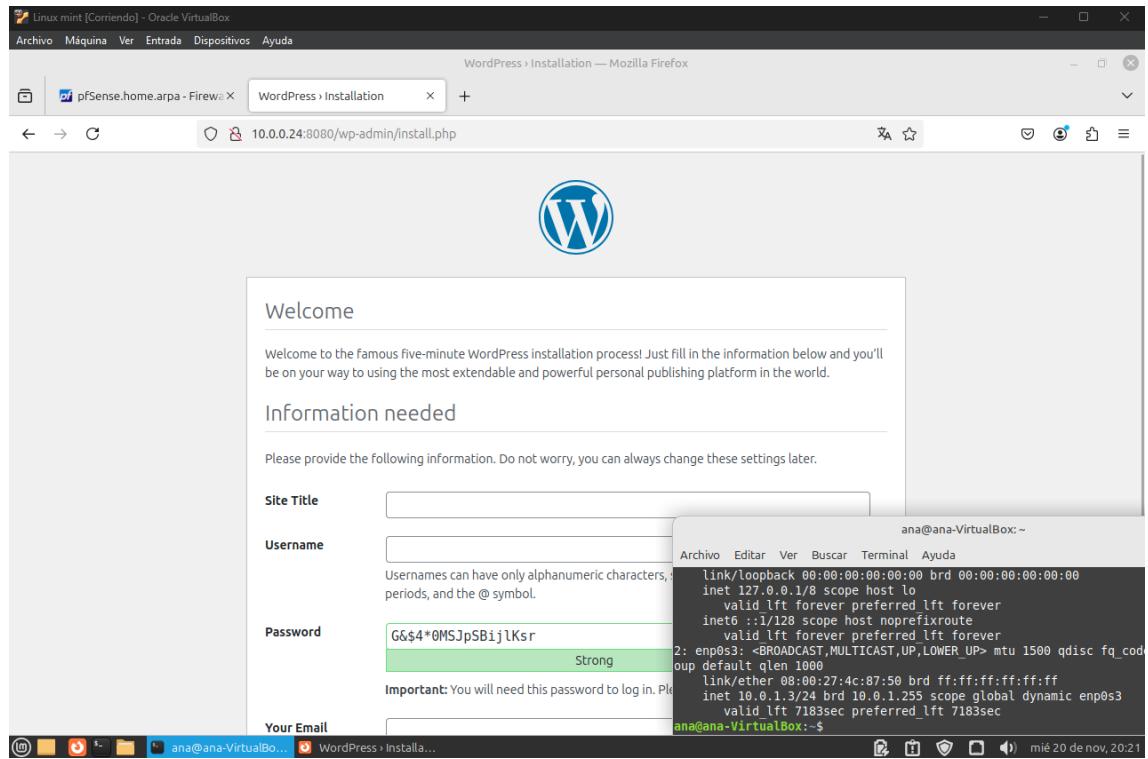
La primera sirve para acceder desde la máquina 4 que está en red WorkStation a la configuración del PFsense.

The screenshot shows a Linux Mint desktop environment. In the foreground, a terminal window is open with the command "ana@ana-VirtualBox:~" and the output of the "cat /etc/pfSense/rules.pf" command. The output shows several kernel-level firewall rules, including ones for the loopback interface and various network interfaces (en0, enp0s3, etc.).

```
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 state UP group default qlen 1000
    link/ether 08:00:27:4c:87:50 brd ff:ff:ff:ff:ff:ff
    inet 10.0.1.3/24 brd 10.0.1.255 scope global dynamic enp0s3
        valid_lft 7183sec preferred_lft 7183sec
```

In the background, a Mozilla Firefox browser window is open, showing the pfSense Firewall Rules interface. The URL is "10.0.0.1/firewall_rules.php?if=opt1". The browser window title is "pfSense.home.arpa - Firewall: Rules: WORKSTATION — Mozilla Firefox". The interface is identical to the one shown in the first screenshot, displaying the same four rules for the WORKSTATION zone.

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 > aliases.

De IPs usaré de la 10.0.1.2 – 10.0.1.22 para Desarrolladores.

Name	Type	Values	Description	Actions
Desarrolladores	Host(s)	10.0.1.2, 10.0.1.3, 10.0.1.4, 10.0.1.5, 10.0.1.6, 10.0.1.7, 10.0.1.8, 10.0.1.9, 10.0.1.10, 10.0.1.11...	Ana Orozco	

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.

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓	0/0 B	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
✗	0/0 B	IPv4 *	LAN subnets	*	WORKSTATION subnets	*	*	none		

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.

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓	0/287 KIB	IPv4 TCP/UDP	WORKSTATION subnets	*	LAN address	80 (HTTP)	*			
✓	0/538 KIB	IPv4 TCP/UDP	WORKSTATION subnets	*	LAN subnets	8080	*			
✓	0/0 B	IPv4 TCP/UDP	Desarrolladores	*	LAN subnets	22 (SSH)	*			
✓	0/0 B	IPv4 TCP/UDP	Desarrolladores	*	LAN subnets	3306	*			
✗	0/0 B	IPv4 TCP/UDP	WORKSTATION subnets	*	10.0.0.24	22 (SSH)	*			
✗	0/0 B	IPv4 TCP/UDP	WORKSTATION subnets	*	10.0.0.24	3306	*			

Reglas NAT.

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

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

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 two windows side-by-side. On the left is a terminal window titled 'wall: NAT: Port Forward — Mozilla Firefox' showing the output of a netstat command. On the right is a browser window titled 'WordPress > Installation' showing the WordPress setup page.

Terminal Output (wall: NAT: Port Forward):

```
ana@ana-VirtualBox:~$ netstat -an | grep ':80' | grep 'ESTABLISHED'
tcp        0      0 192.168.1.32:80  10.0.0.24:53214      ESTABLISHED
ana@ana-VirtualBox:~$
```

Browser Window (WordPress Installation):

Welcome

Welcome to the famous five-minute WordPress installation process! Just fill in the information below and you'll be on your way to using the most extendable and powerful personal publishing platform in the world.

Information needed

Please provide the following information. Do not worry, you can always change these settings later.

Site Title:

Username: Usernames can have only alphanumeric characters, spaces, underscores, hyphens, periods, and the @ symbol.

Password: fgX5D8^bbZFX&Lhgba Strong Hide

Important: You will need this password to log in. Please store it in a secure location.

Your Email: Double-check your email address before continuing.

Search engine visibility: Discourage search engines from indexing this site It is up to search engines to honor this request.

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

```
ana@vboxana: ~          + | v
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:

The screenshot shows a table titled "CP Static Mappings" with a "Save" button at the top. The table has columns: ARP, MAC address, IP address, and Hostname. There are two entries: one for MAC 08:00:27:c0:01:14 with IP 10.0.0.24 and another for MAC 08:00:27:15:a1:ae with IP 10.0.0.25.

ARP	MAC address	IP address	Hostname
	08:00:27:c0:01:14	10.0.0.24	
	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_code
    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:fe0:114/64 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:

