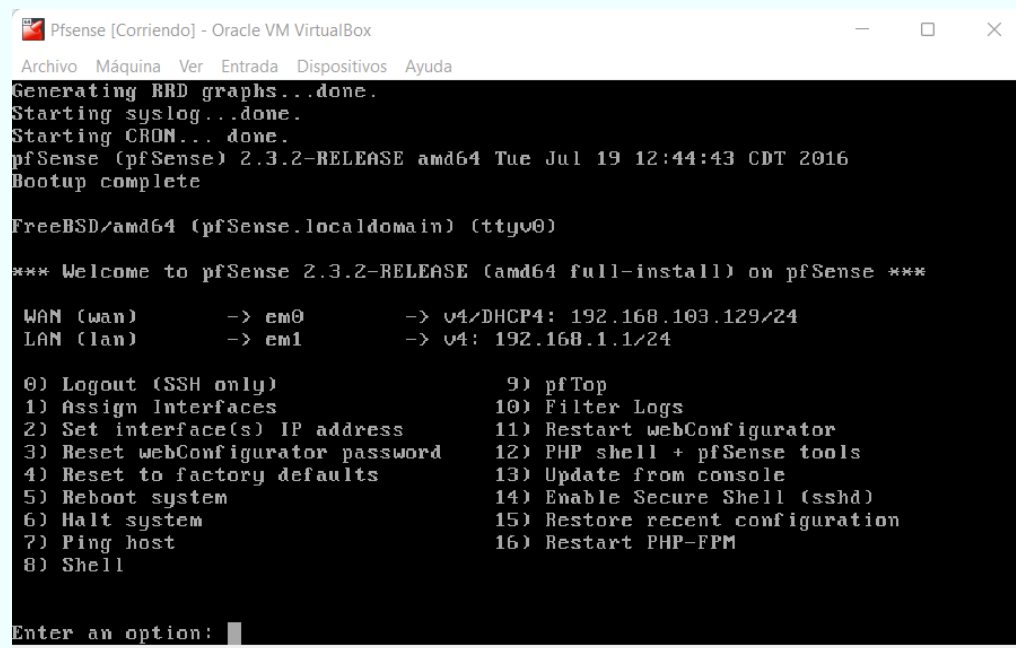


CONFIGURACIÓN DE PFBLOCKER CON PFSENSE



SEGURIDAD INFORMÁTICA
JUAN CARLOS NAVIDAD GARCÍA

1. Configuración de Pfsense:



```
PfSense [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
Generating RRD graphs...done.
Starting syslog...done.
Starting CRON... done.
pfSense (pfSense) 2.3.2-RELEASE amd64 Tue Jul 19 12:44:43 CDT 2016
Bootup complete

FreeBSD/amd64 (pfSense.localdomain) (ttyv0)

*** Welcome to pfSense 2.3.2-RELEASE (amd64 full-install) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.103.129/24
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) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: 2
```

Una vez iniciado **Pfsense**, nos encontraremos con que nos listará unas opciones, de las cuáles solo tocaremos la **segunda**.

La **segunda opción** sirve para **configurar y asignar las direcciones IP** a los adaptadores de red.

De los cuales tenemos dos, uno que nos proporcionará **conexión a internet y que está conectado mediante DHCP** y otro adaptador conectado a un **segmento de LAN que sería equivalente a una red NAT en VirtualBox**, este adaptador se configuraría con la **IP estática**.

Así que, como ya he dicho, escribiremos el número **dos** para seleccionar la opción.

Enter an option: 2

Nos preguntará por la interfaz de red que queremos configurar, en nuestro caso solo configuraremos la segundo, la **LAN**, está es la interfaz por la que va a salir el servidor **Pfsense**.

Seleccionaremos la interfaz también escribiendo el número **2**:

```
Available interfaces:
1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure: 2
```

Continuando, nos pedirá la **dirección IP** que le queremos asignar a la interfaz, le podemos asignar cualquier dirección, en mi caso le he asignado la **192.168.1.1** que pertenece a la red interna.

```
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.1.1
```

Después, nos pedirá la **máscara de subred** en la que nos encontramos, como ya he dicho es la **/24**, así que escribiremos **24**:

```
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 LAN IPv4 subnet bit count (1 to 31):
> 24
```

En las opciones "**For a LAN, press <Enter> for none**" y "**Enter the new LAN IPv6 address, press <Enter> for none**" pulsaremos **Enter** para saltar, ya que no a configurar las **direcciones IPv6**.

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

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

Por último, nos preguntará si queremos configurar el **servidor DHCP**, en nuestro caso lo necesitaremos para que funcione el **portal cautivo**, así que lo configuraremos.

Para habilitarlo pulsaremos la tecla "**Y**", e introduciremos el rango de **IPs** que puede asignar nuestro **servidor DHCP**:

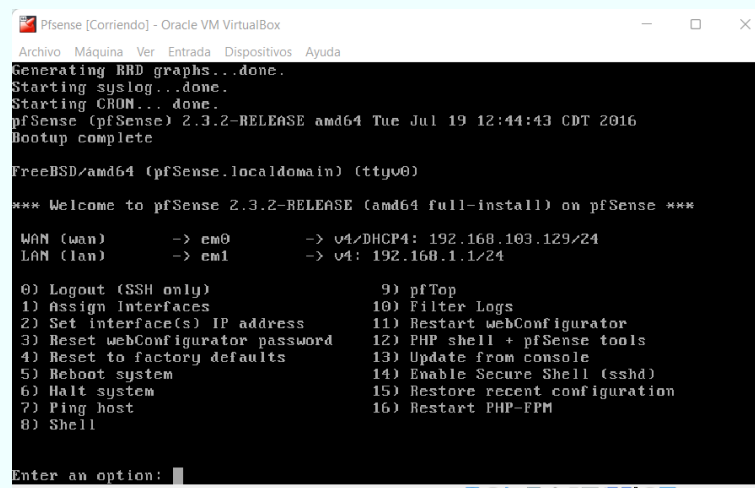
```
Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 192.168.1.100
Enter the end address of the IPv4 client address range: 192.168.1.200
Disabling IPv6 DHCPD...
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) y
```

Finalmente, nos preguntará si queremos que el **protocolo Web** sea **HTTP** y le diremos que si dando a la tecla "**Y**".

Después de todo, acabaremos con la configuración de la interfaz y podremos acceder a **Pfsense**.

```
The IPv4 LAN address has been set to 192.168.1.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
    http://192.168.1.1/
Press <ENTER> to continue.
```

Reiniciaremos la máquina para que se apliquen bien los cambios y nos daremos cuenta de que, al reiniciar, nos saldrá la dirección IP que le hemos asignado a la interfaz "**LAN**":



```
Pfsense [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Generating RRD graphs...done.
Starting syslog...done.
Starting CRON... done.
pfSense (pfSense) 2.3.2-RELEASE amd64 Tue Jul 19 12:44:43 CDT 2016
Bootup complete

FreeBSD/amd64 (pfSense.localdomain) (ttyv0)

*** Welcome to pfSense 2.3.2-RELEASE (amd64 full-install) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.103.129/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

0) Logout (SSH only)
1) Assign Interfaces
2) Set interface(s) IP address
3) Reset webConfigurator password
4) Reset to factory defaults
5) Reboot system
6) Halt system
7) Ping host
8) Shell
9) pfTop
10) Filter Logs
11) Restart webConfigurator
12) PHP shell + pfSense tools
13) Update from console
14) Enable Secure Shell (sshd)
15) Restore recent configuration
16) Restart PHP-FPM

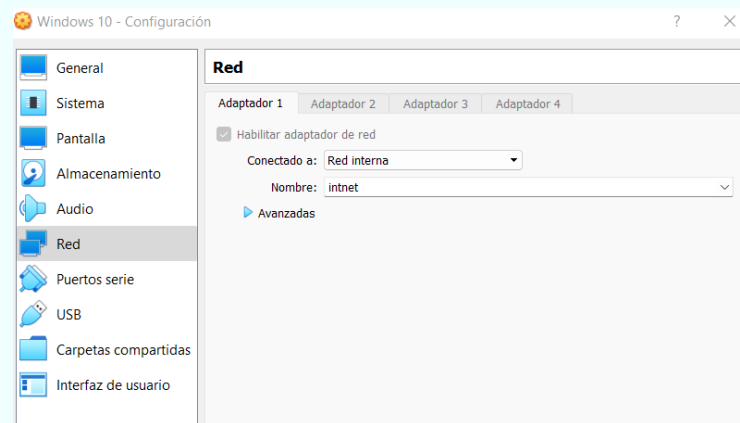
Enter an option:
```

Esta dirección IP será la que utilizaremos para acceder al **configurador Web de Pfsense**.

2. Configuración inicial de Pfsense:

Para crear el **portal cautivo** y realizar las diversas configuraciones que quedan en **Pfsense** necesitaremos otra máquina (cliente) en la misma red.

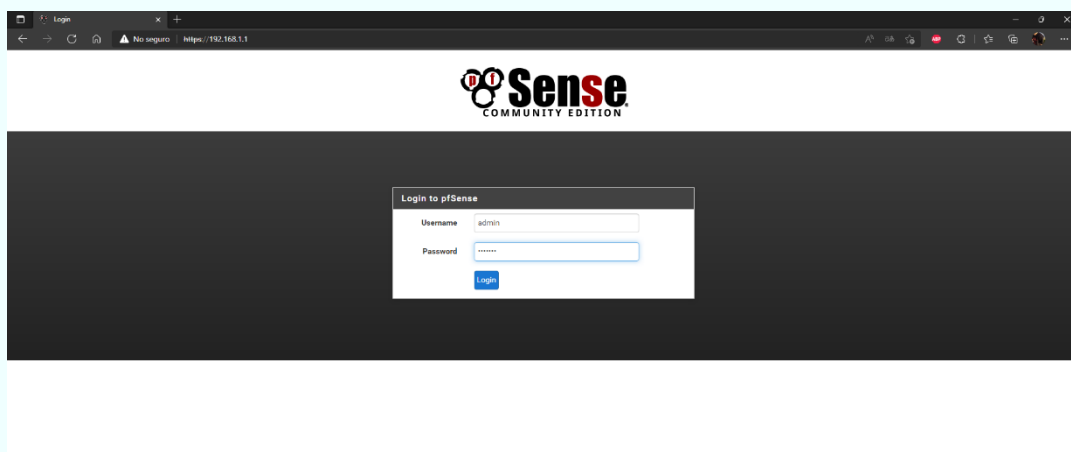
Para esto he utilizado una máquina virtual con **Windows 10** también configurada la red como **"Red Interna"**.



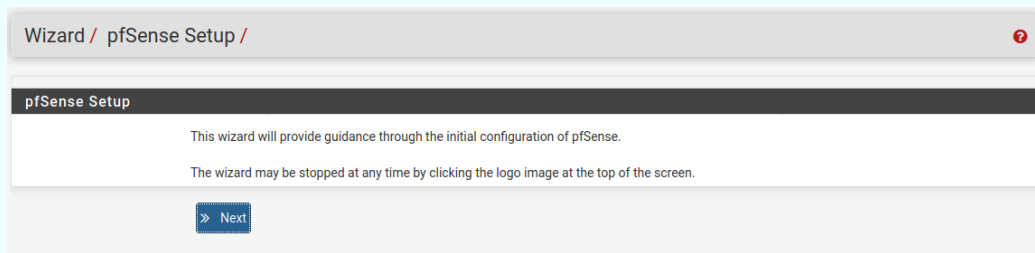
Iniciaremos la máquina virtual e ingresaremos en el navegador;

En la barra de búsqueda insertaremos la **IP configurada anteriormente**, en mi caso la **192.168.1.1**.

Una vez dentro nos pedirá **iniciar sesión**, el usuario y la contraseña por defecto son **usuario: admin ; contraseña: pfsense**

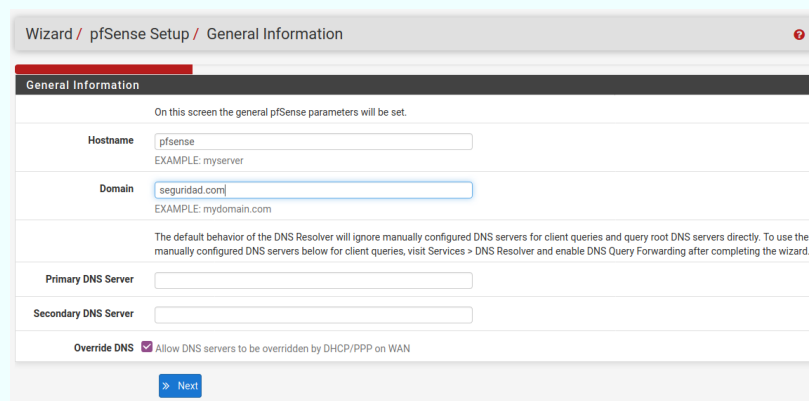


Una vez iniciada la sesión, comenzará el **setup** de la configuración web de **Pfsense**:



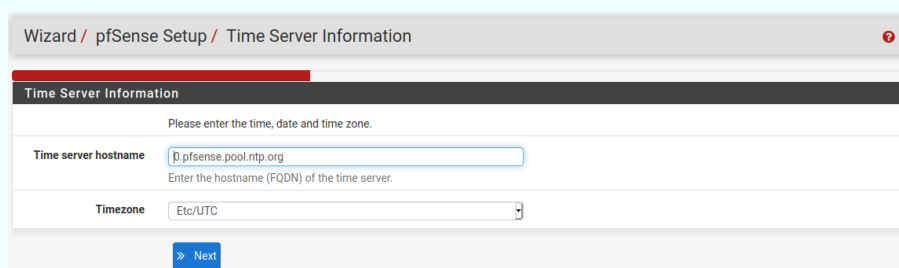
The screenshot shows the 'Wizard / pfSense Setup' window. The title bar includes a help icon. Below the title bar, the text reads: 'This wizard will provide guidance through the initial configuration of pfSense. The wizard may be stopped at any time by clicking the logo image at the top of the screen.' At the bottom, there is a blue button labeled 'Next' with a right-pointing arrow.

Lo primero sería darle un **nombre de dominio a Pfsense**, no tendríamos que tocar nada más de esa pantalla, aunque si queremos podemos añadir **direcciones DNS**, aunque no es necesario.



The screenshot shows the 'Wizard / pfSense Setup / General Information' window. The title bar includes a help icon. Below the title bar, the text reads: 'On this screen the general pfSense parameters will be set.' The form contains the following fields: 'Hostname' with the value 'pfsense' and an example 'EXAMPLE: myserver'; 'Domain' with the value 'seguridad.com' and an example 'EXAMPLE: mydomain.com'; 'Primary DNS Server' and 'Secondary DNS Server' fields, both empty; and an 'Override DNS' checkbox which is checked, with the text 'Allow DNS servers to be overridden by DHCP/PPP on WAN'. At the bottom, there is a blue button labeled 'Next' with a right-pointing arrow.

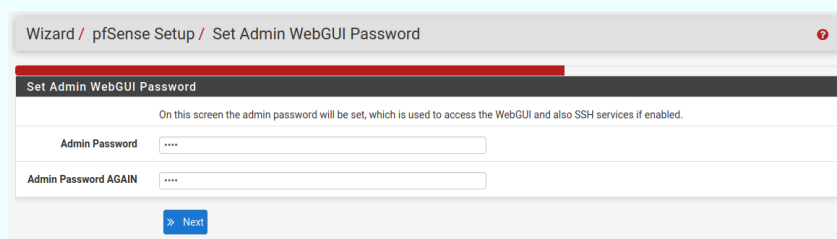
A continuación, nos aparecerá la selección del **servidor de horario** y nuestra **zona horaria**, todo lo dejaremos **por defecto**, no tocaremos nada.



The screenshot shows the 'Wizard / pfSense Setup / Time Server Information' window. The title bar includes a help icon. Below the title bar, the text reads: 'Please enter the time, date and time zone.' The form contains the following fields: 'Time server hostname' with the value 'p.pfsense.pool.ntp.org' and a note 'Enter the hostname (FQDN) of the time server.'; and 'Timezone' with the value 'Etc/UTC'. At the bottom, there is a blue button labeled 'Next' with a right-pointing arrow.

Los siguientes dos apartados serán sobre la **configuración de las interfaces de red**, las cuales ya hemos configurado **manualmente** en pasos anteriores. Así que también se dejará todo tal cual está.

Para finalizar, nos hará introducir una **nueva contraseña para el usuario administrador**, para que no se quedé la contraseña por defecto.



Wizard / pfSense Setup / Set Admin WebGUI Password

Set Admin WebGUI Password

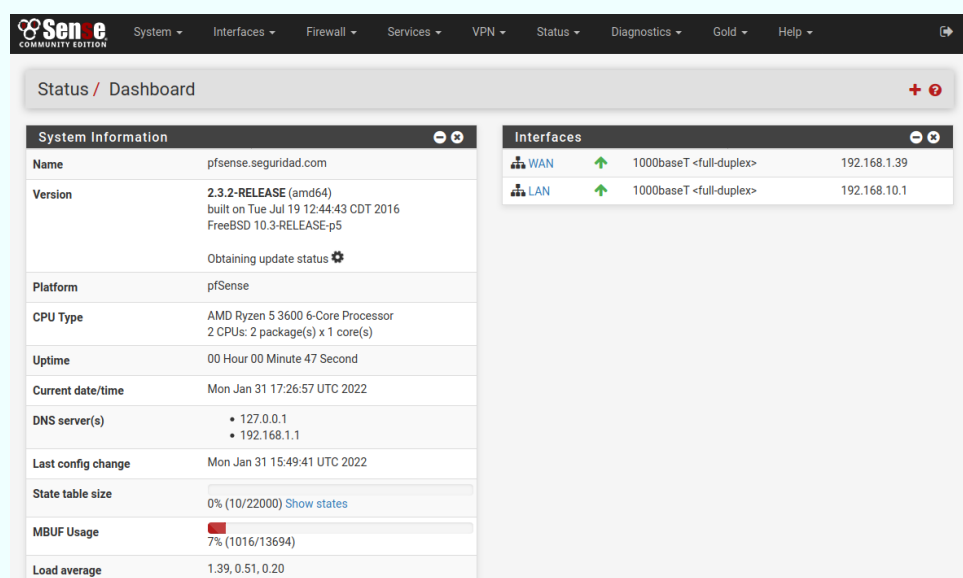
On this screen the admin password will be set, which is used to access the WebGUI and also SSH services if enabled.

Admin Password:

Admin Password AGAIN:

[Next](#)

Una vez introducida la nueva contraseña, se nos abrirá el **panel principal de Pfsense**:



Status / Dashboard

System Information

Name	pfSense.seguridad.com
Version	2.3.2-RELEASE (amd64) built on Tue Jul 19 12:44:43 CDT 2016 FreeBSD 10.3-RELEASE-p5 Obtaining update status
Platform	pfSense
CPU Type	AMD Ryzen 5 3600 6-Core Processor 2 CPUs: 2 package(s) x 1 core(s)
Uptime	00 Hour 00 Minute 47 Second
Current date/time	Mon Jan 31 17:26:57 UTC 2022
DNS server(s)	• 127.0.0.1 • 192.168.1.1
Last config change	Mon Jan 31 15:49:41 UTC 2022
State table size	0% (10/22000) Show states
MBUF Usage	7% (1016/13694)
Load average	1.39, 0.51, 0.20

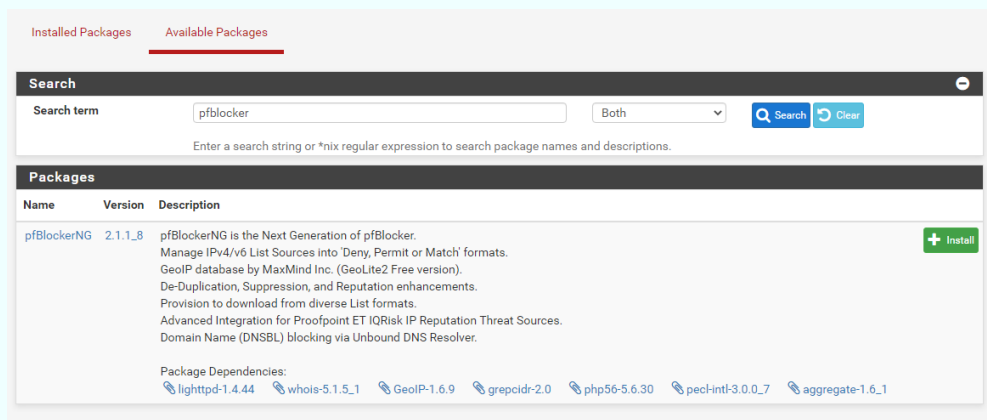
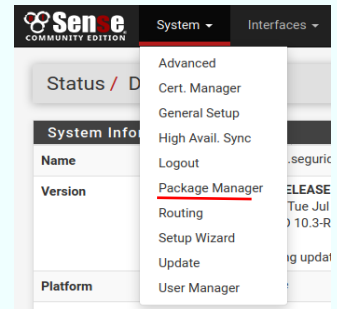
Interfaces

WAN	1000baseT <full-duplex>	192.168.1.39
LAN	1000baseT <full-duplex>	192.168.10.1

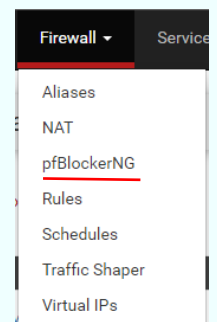
3. Instalación de Pfblocker:

Pfblocker no viene directamente incluido en Pfsense, por lo que hay que instalarlo desde el administrador de paquetes.

Entonces nos iremos a sistema → Administrador de paquetes
Y dentro del administrador de paquetes nos iremos a paquetes disponibles. Buscaremos Pfblocker y le daremos a instalar:



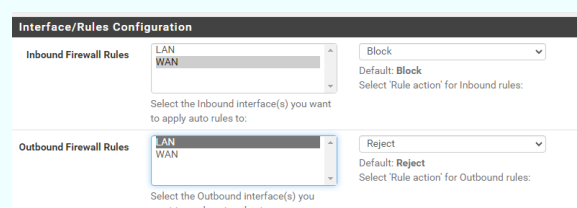
Una vez esté instalado, el Pfblocker se va a encontrar en el apartado de Cortafuegos como pfBlockerNG:



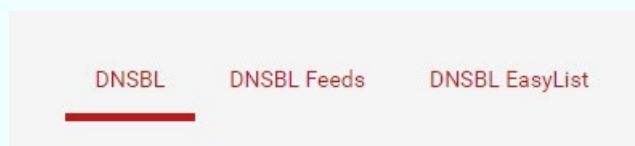
Cuando estemos dentro del pfBlockerNG, lo primero que haremos será habilitarlo:

Enable pfBlockerNG ☒ Enable/Disable

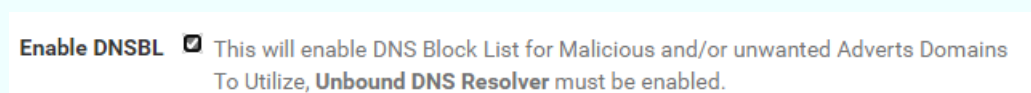
En la misma pantalla nos aseguraremos que las interfaces estén de la siguiente manera:



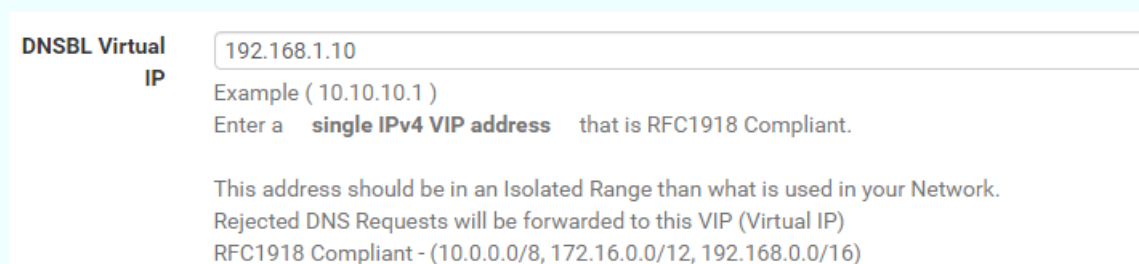
Posteriormente nos iremos al apartado de DNSBL



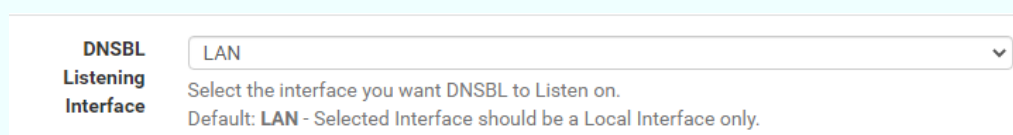
Lo habilitaremos:



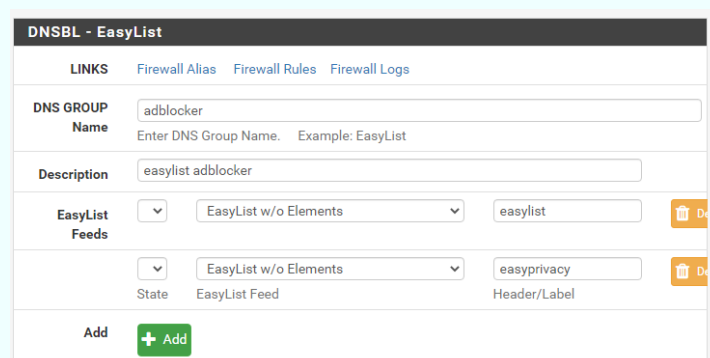
Después le asignaremos una IP Virtual al Pfblocker, la cual tiene que estar en el mismo rango de IP que nuestra red.



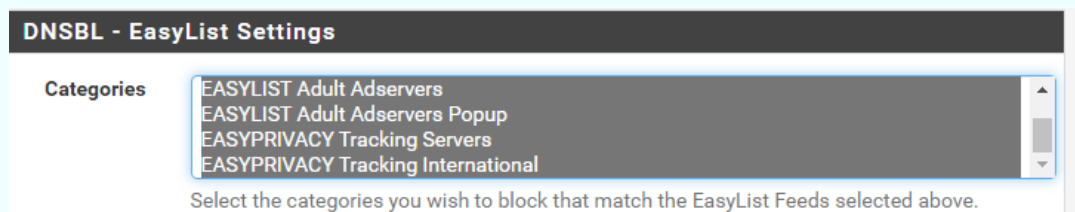
Nos aseguraremos también de que las interfaces del DNSBL están en la LAN:



Cuando tengamos configurado el DNSBL base, nos iremos a DNSBL EasyList, dentro le asignaremos un nombre al grupo DNS y añadiremos dos interfaces: easylist y easy privacy.



Por último, en la configuración, seleccionaremos todas las categorías:



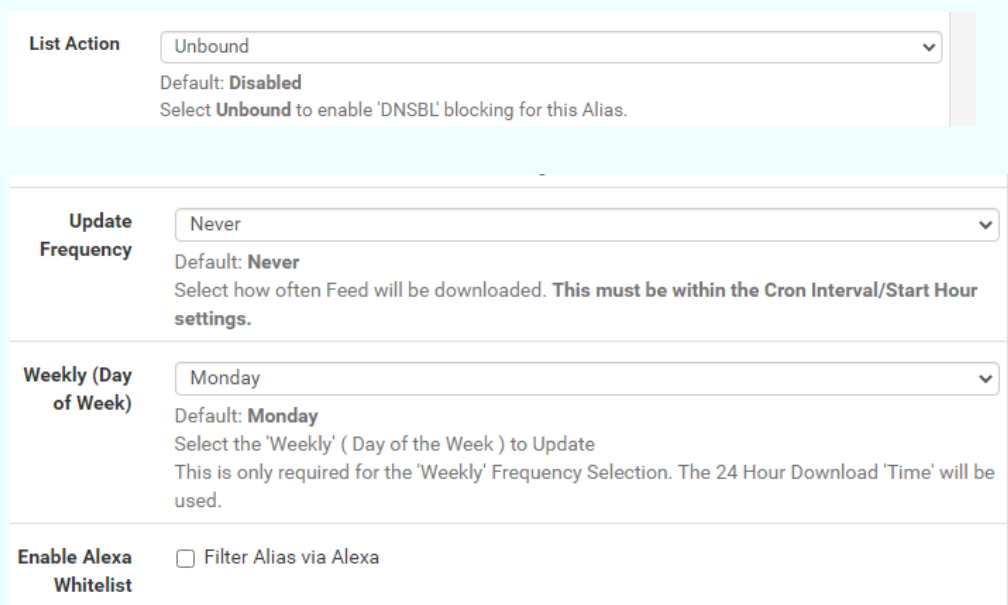
DNSBL - EasyList Settings

Categories

- EASYLIST Adult Adservers
- EASYLIST Adult Adservers Popup
- EASYPRIVACY Tracking Servers
- EASYPRIVACY Tracking International

Select the categories you wish to block that match the EasyList Feeds selected above.

En list action pondremos en unbound y todo lo demás lo dejamos por defecto.



List Action

Unbound

Default: **Disabled**

Select **Unbound** to enable 'DNSBL' blocking for this Alias.

Update Frequency

Never

Default: **Never**

Select how often Feed will be downloaded. **This must be within the Cron Interval/Start Hour settings.**

Weekly (Day of Week)

Monday

Default: **Monday**

Select the 'Weekly' (Day of the Week) to Update

This is only required for the 'Weekly' Frequency Selection. The 24 Hour Download 'Time' will be used.

Enable Alexa Whitelist

☐ Filter Alias via Alexa

Con todo esto ya hecho, le daremos a save para que todo se guarde y se ponga en marcha.

4. Comprobación:

Para comprobarlo, he puesto una IP en el DNSBL que sería la 192.168.1.100, esta será la IP bloqueada por pfBlocker.

He asignado esta IP ya que le pertenece a una máquina virtual que tengo creada, así podré ver si esta IP está bloqueada y no tiene conexión a Internet:

Si nos hacemos un ping o un nslookup y no debería de dar respuesta:

```
jnav@jnavrog:~$ nslookup 192.168.1.100
;; connection timed out; no servers could be reached
```