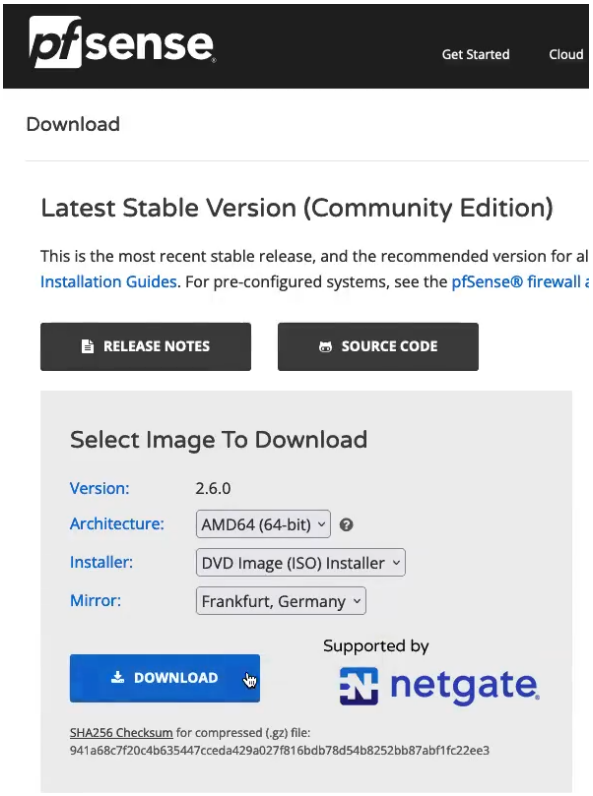
BLUE TEAM | 2022

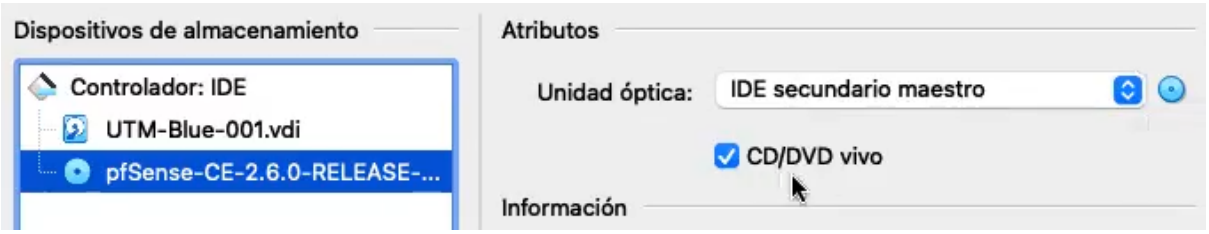
Alberto Doblado Vera

Primero de todo tenemos que descargar la máquina de **PfSense**. Para ello nos vamos a https://www.pfsense.org/download/ y descargamos.

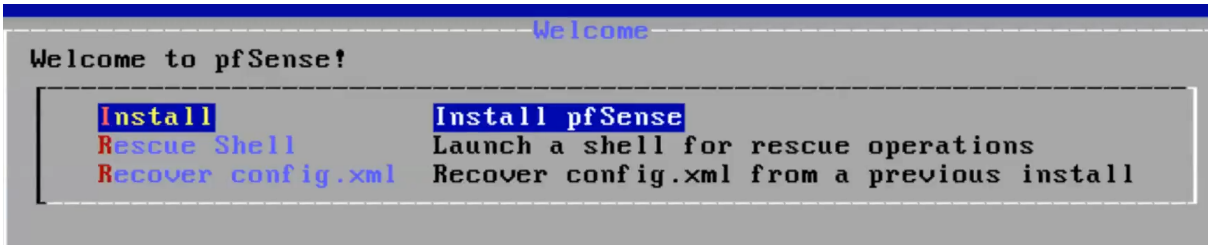


Ahora en **VirtualBox** al crear la máquina, es muy importante seleccionar bien el tipo y la versión.

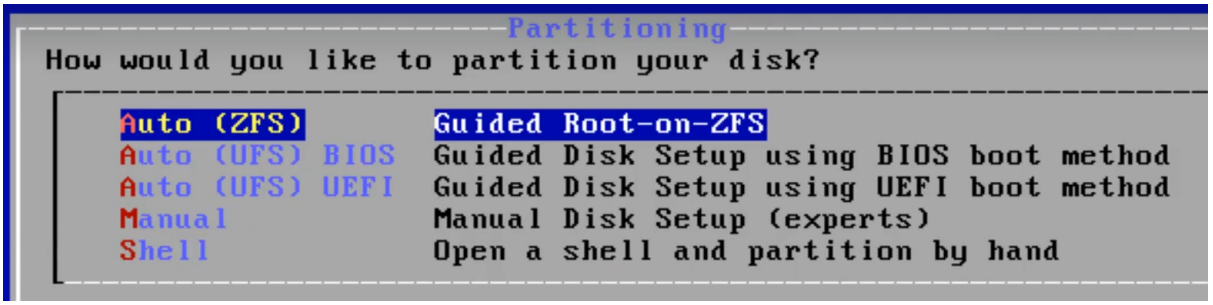
Y luego nos vamos a “Dispositivos de almacenamiento” y seleccionamos “CD/DVD vivo”



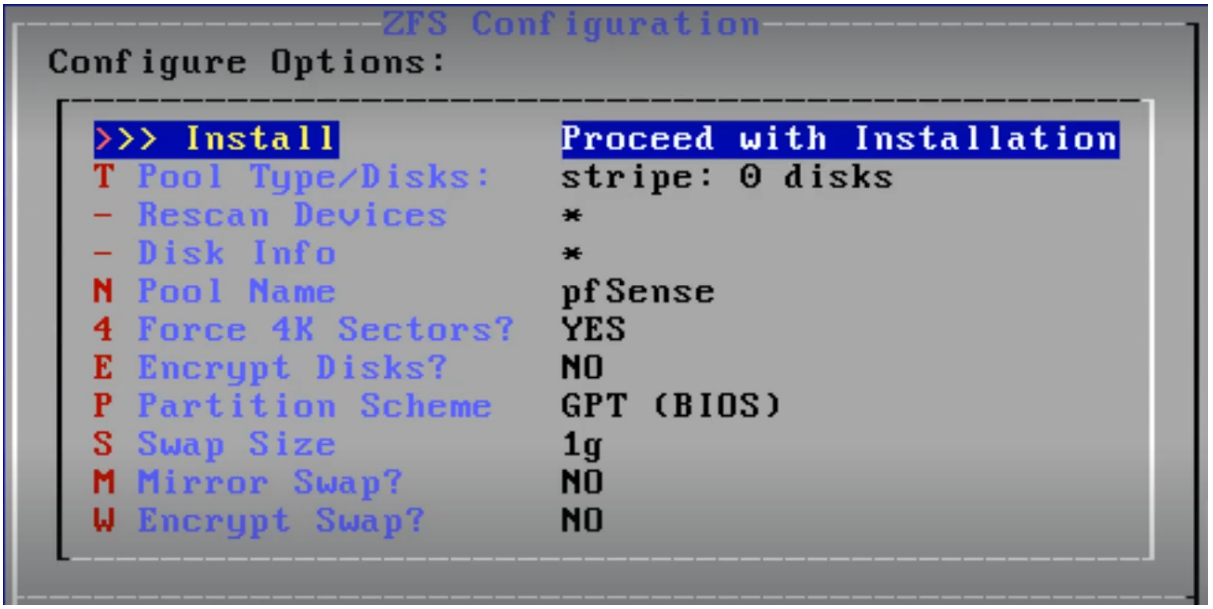
Una vez hecho el paso anterior arrancamos la máquina y seguimos los siguientes pasos en la instalación.



Tras este paso tendremos que seleccionar nuestra versión de teclado, y ahora nos pregunta si queremos particionar el disco y seleccionamos lo siguiente.

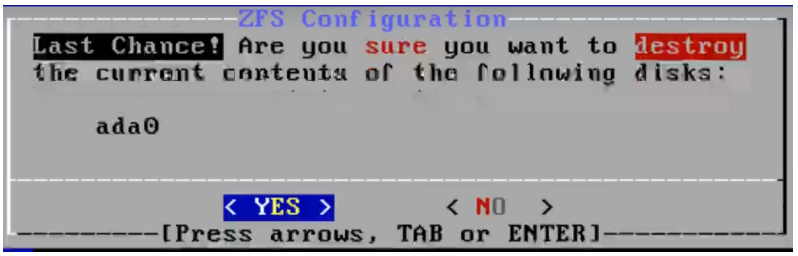


En la siguiente ventana seguimos con la primera opción.

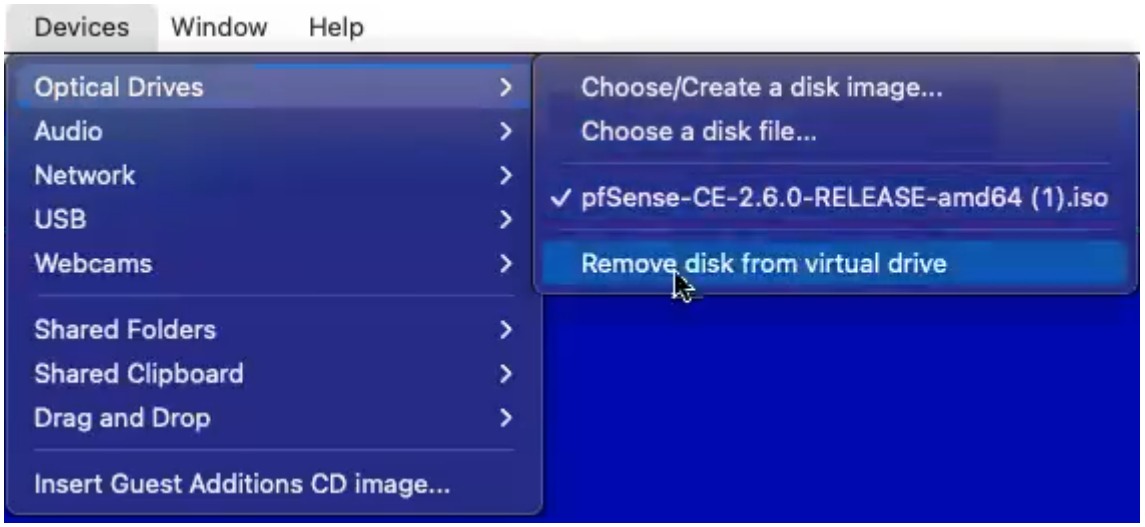


Ahora tenemos que seleccionar el disco, como es el único que hay pulsamos la tecla espacio y lo marcamos.

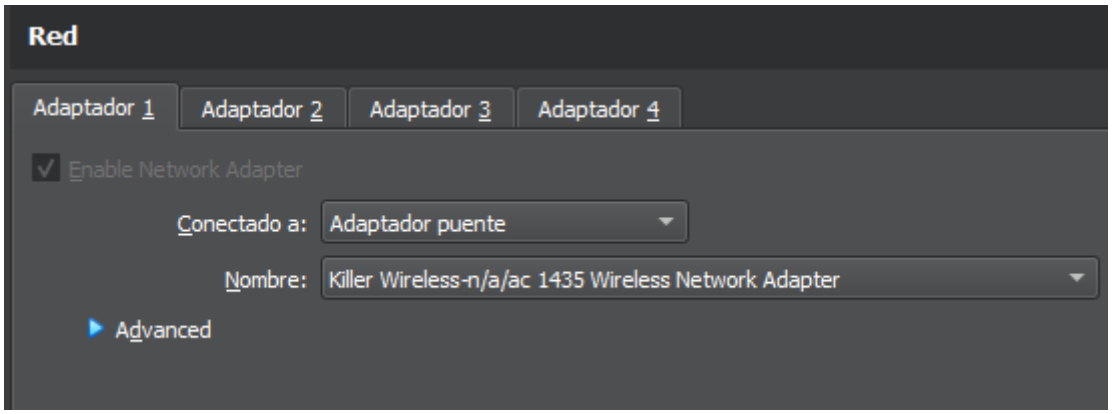
Y marcamos que “YES” para finalizar

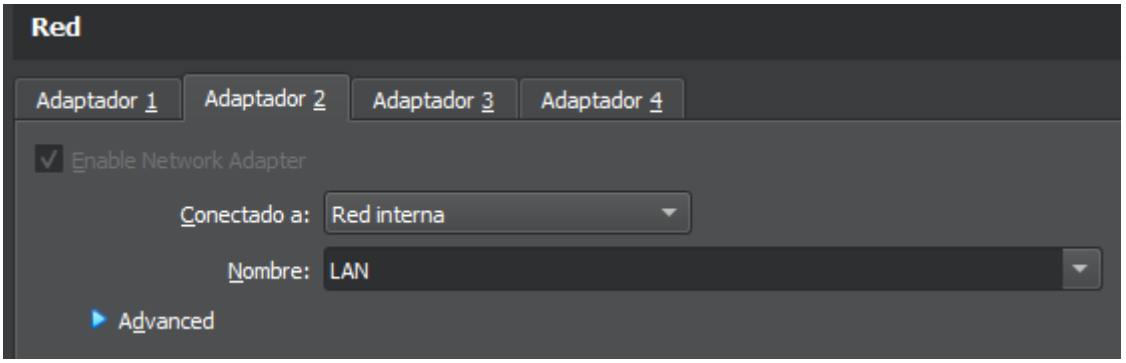


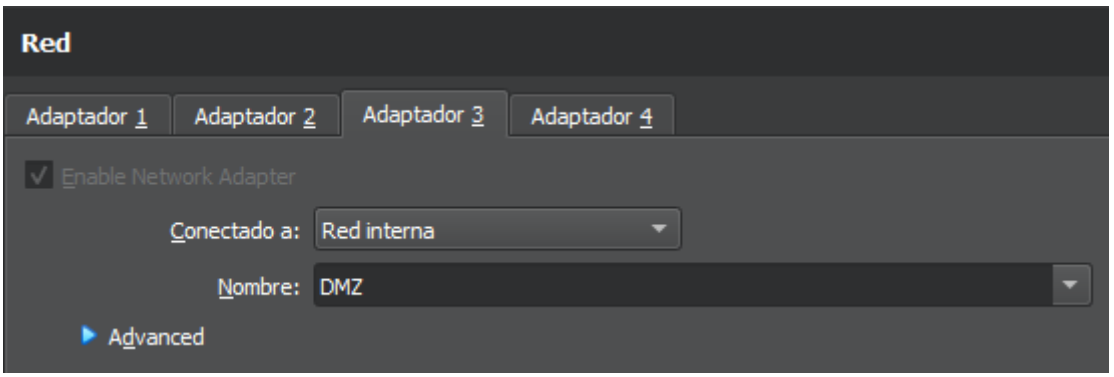
Ahora tenemos que eliminar el disco, ya que de no hacerlo volveríamos al proceso de configuración de nuevo.

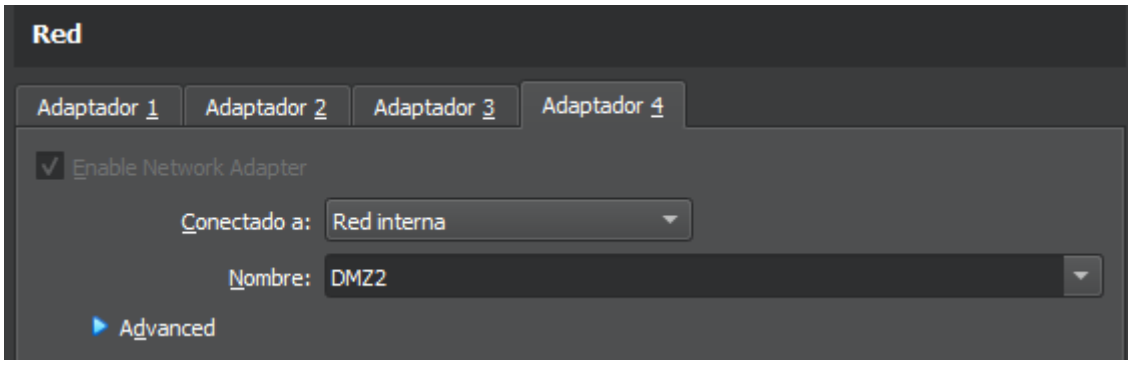


Y ahora con la máquina apagada vamos a activar los adaptadores de red de la siguiente manera para crear nuestra red.

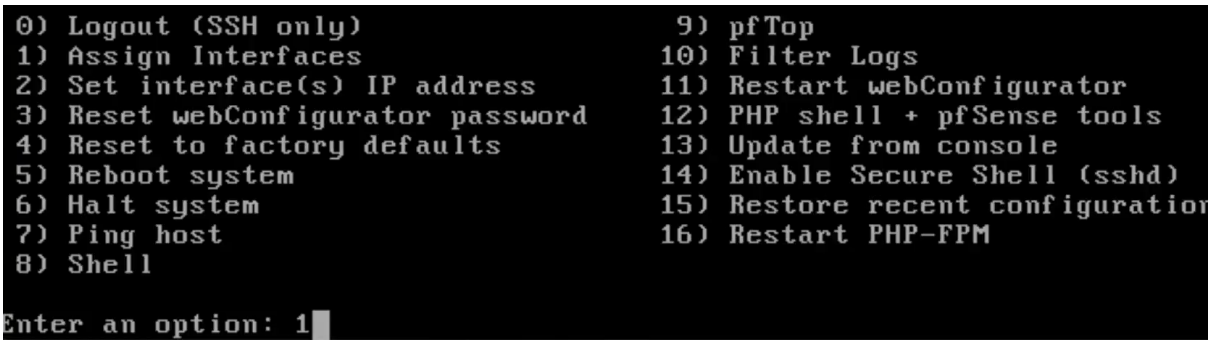


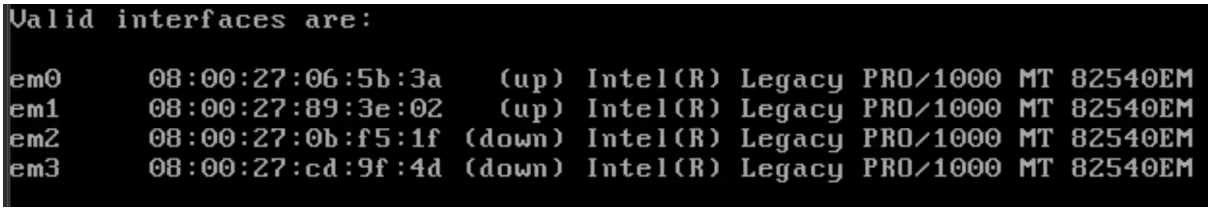






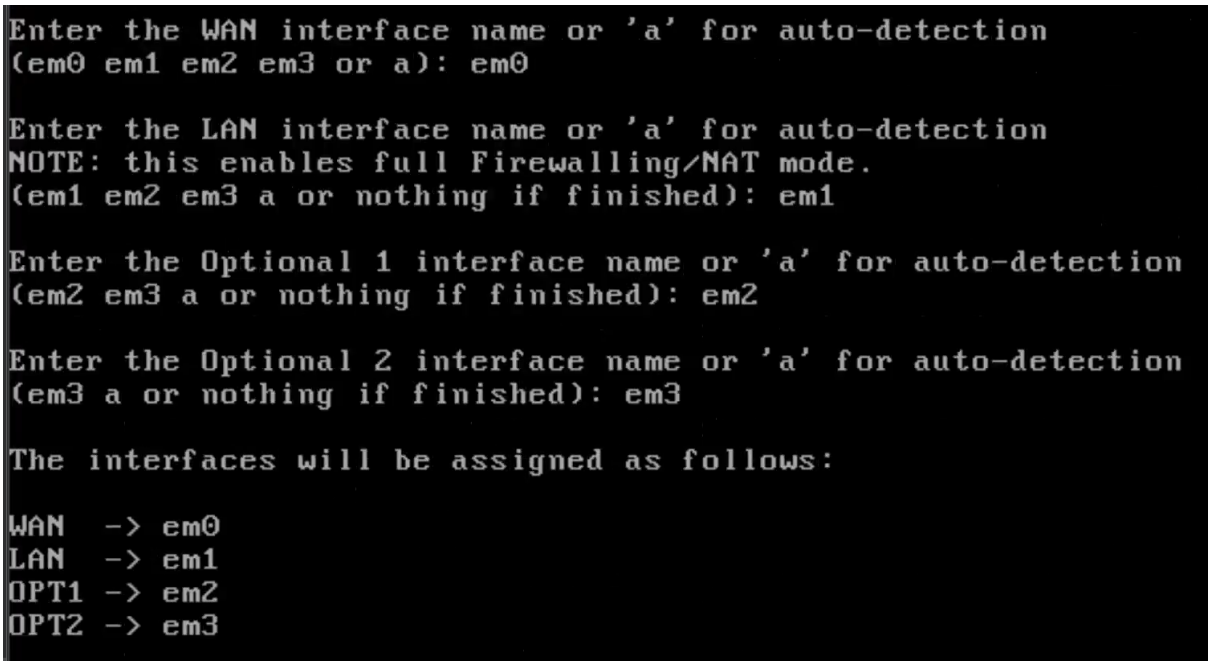
Ahora ya podemos arrancar la máquina y configurar las interfaces.



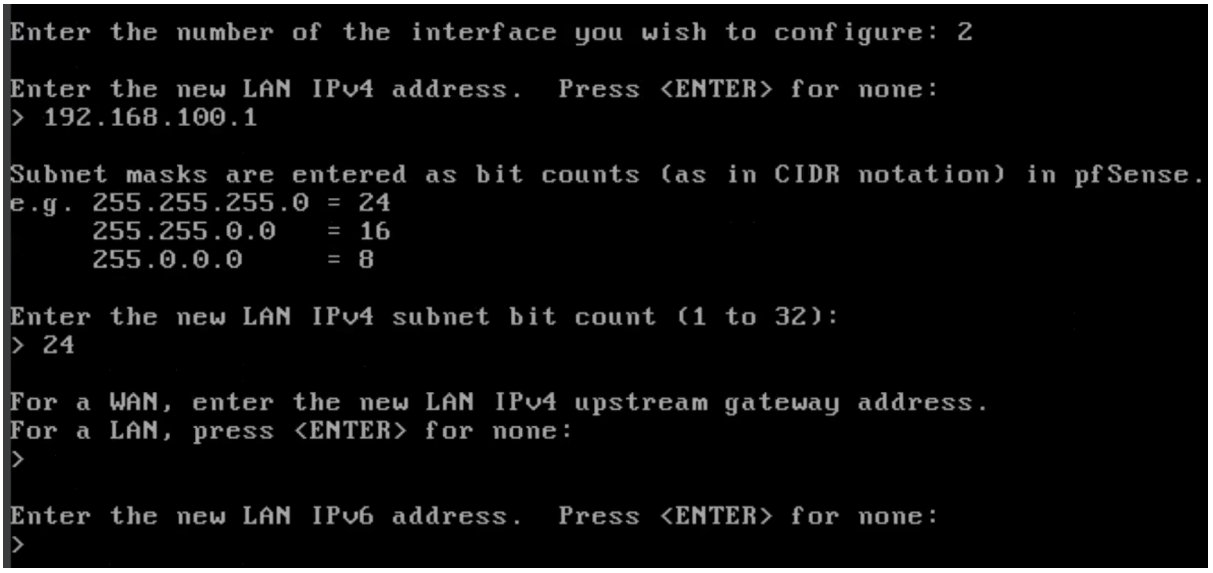


Marcamos que no queremos configurar las VLANs ahora.

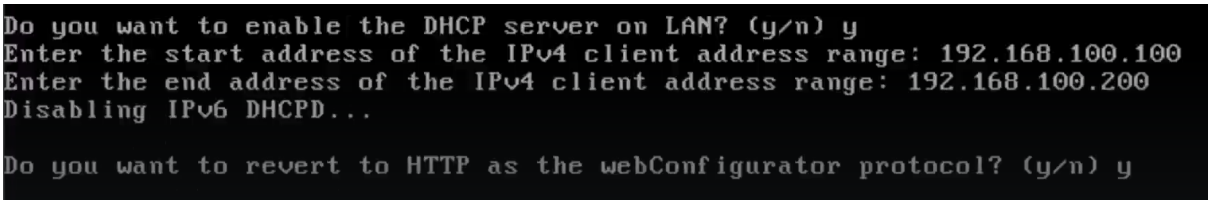
Y vamos asignando el resto de las interfaces.



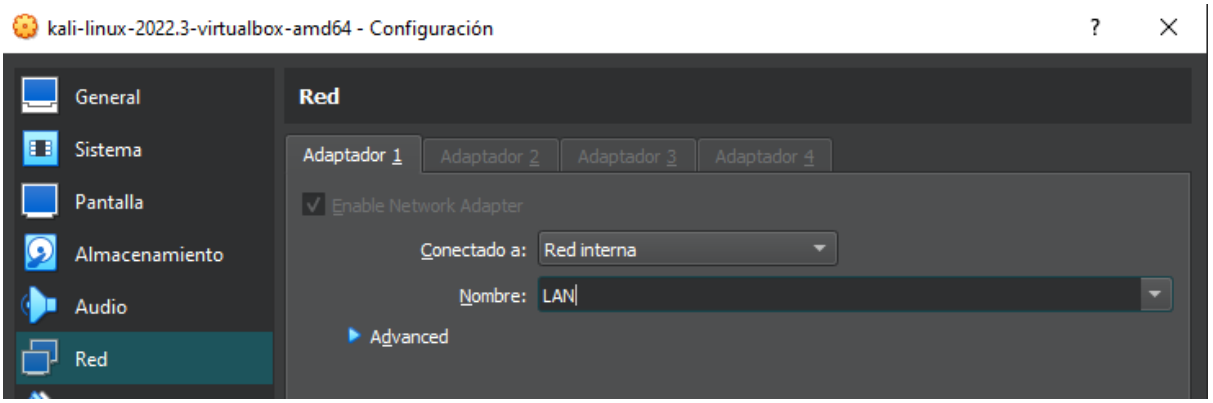
Y le ponemos la IP que nosotros queramos asignarle.



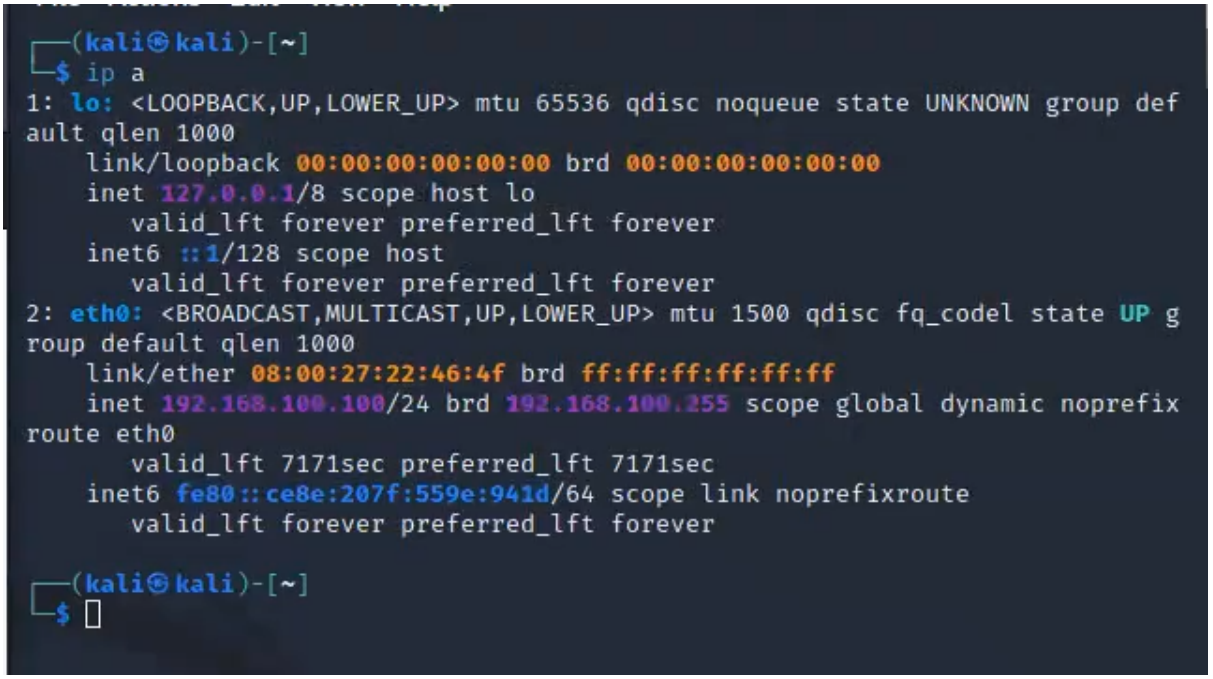
Y le decimos que queremos volver a HTTP.



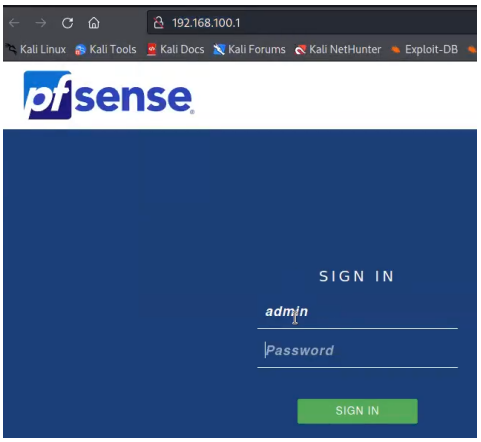
Ahora nos vamos con la máquina de Kali, activamos el adaptador de red con la siguiente configuración.



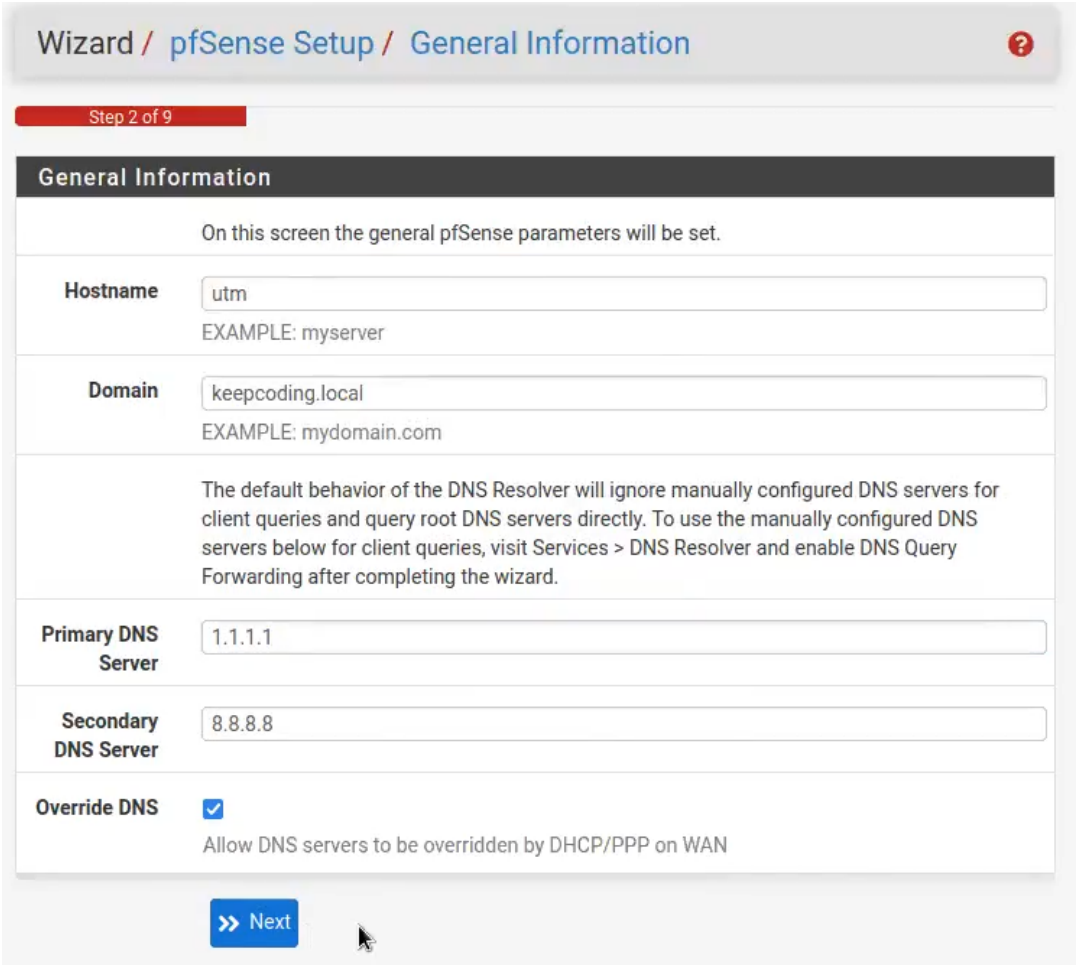
Al arrancar Kali hacemos un "**ip a**" y vemos que tenemos la IP que habíamos asignado en PfSense.



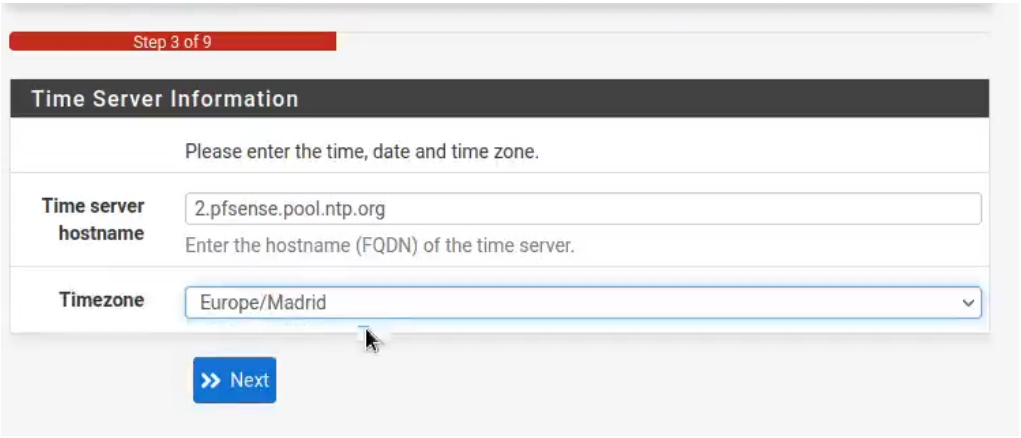
Ahora si nos vamos al navegador del Kali y escribimos **192.168.100.1** tendremos acceso a PfSense. Para entrar los credenciales son username: **admin** y password: **pfsense**



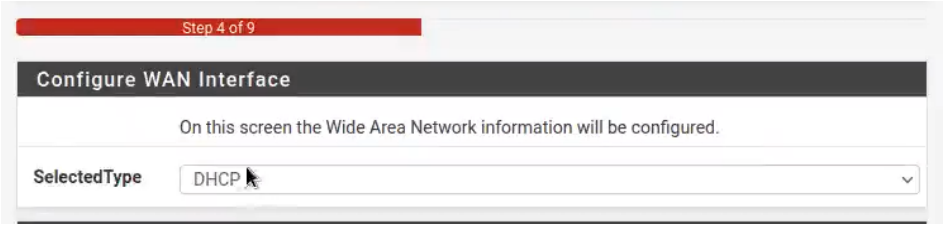
Y una vez dentro vamos configurando nuestro PfSense del siguiente modo.



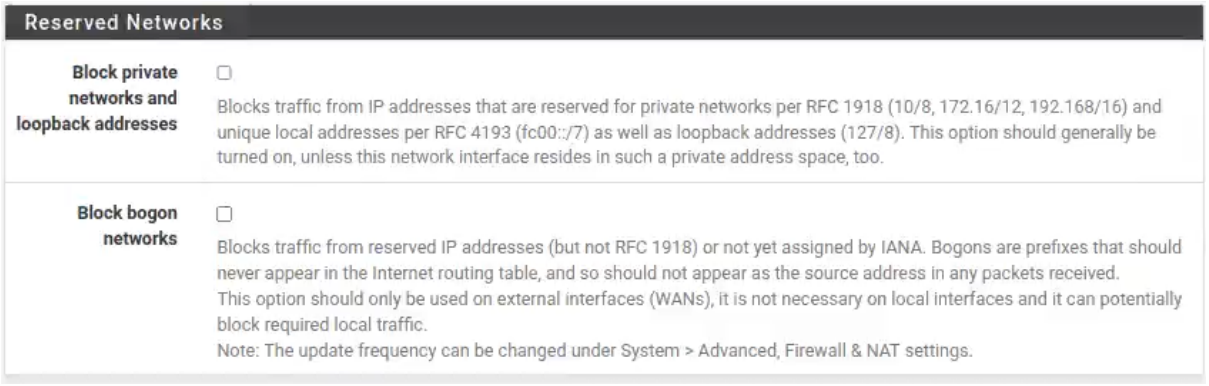
En la zona horaria seleccionamos el país (o uso horario) en el que nos encontremos.



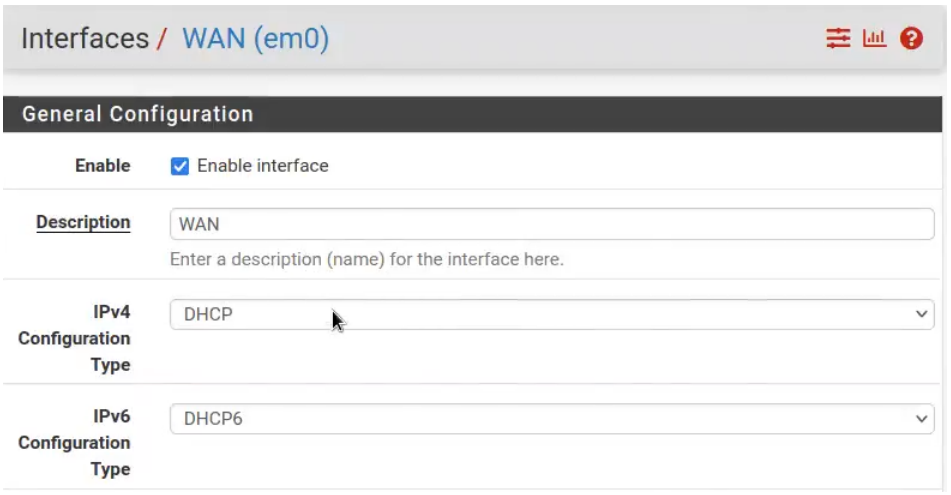
La interface WAN la ponemos tipo DHCP

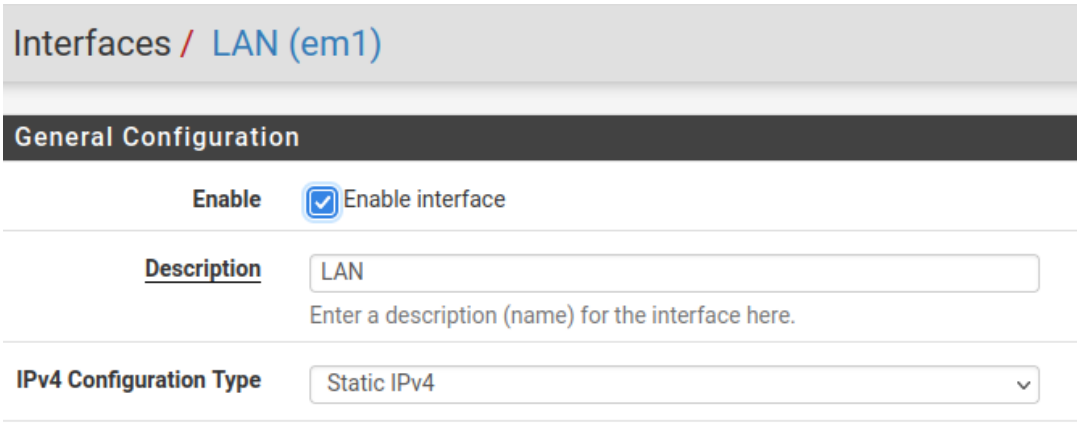


En **Reserved Networks** desmarcamos ambas, para que no nos bloquee el acceso de redes privadas.

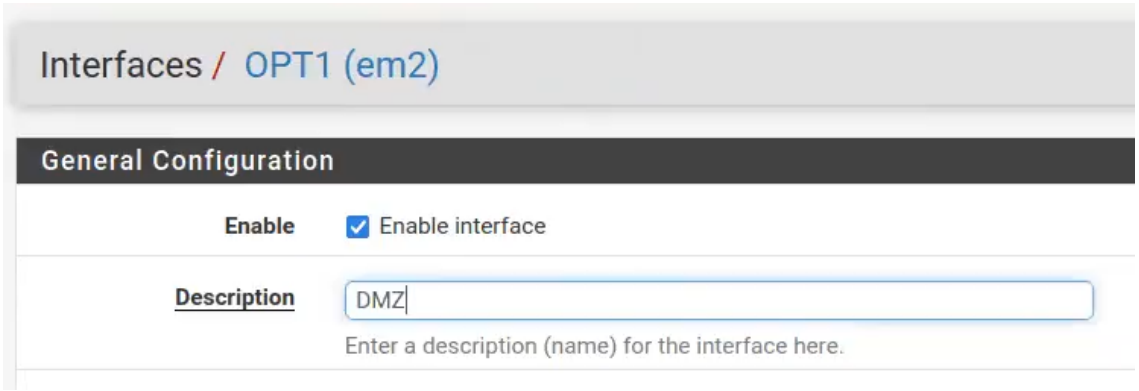


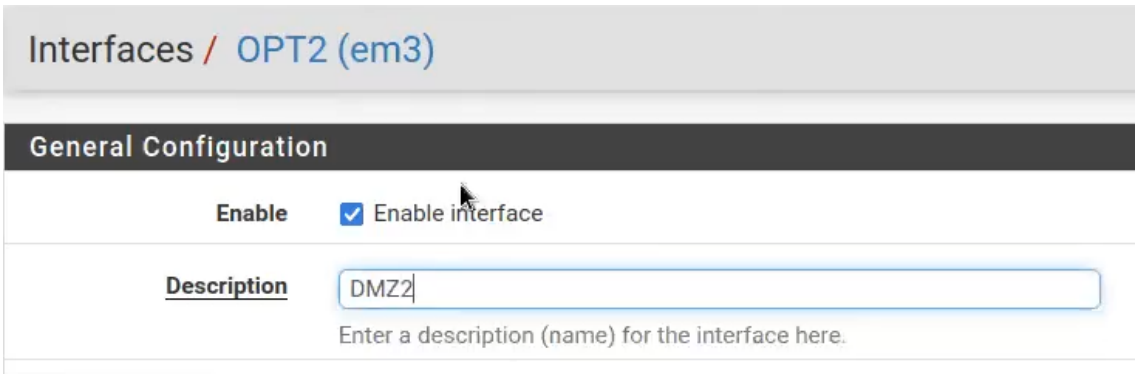
Y ahora vamos activando las distintas interfaces.



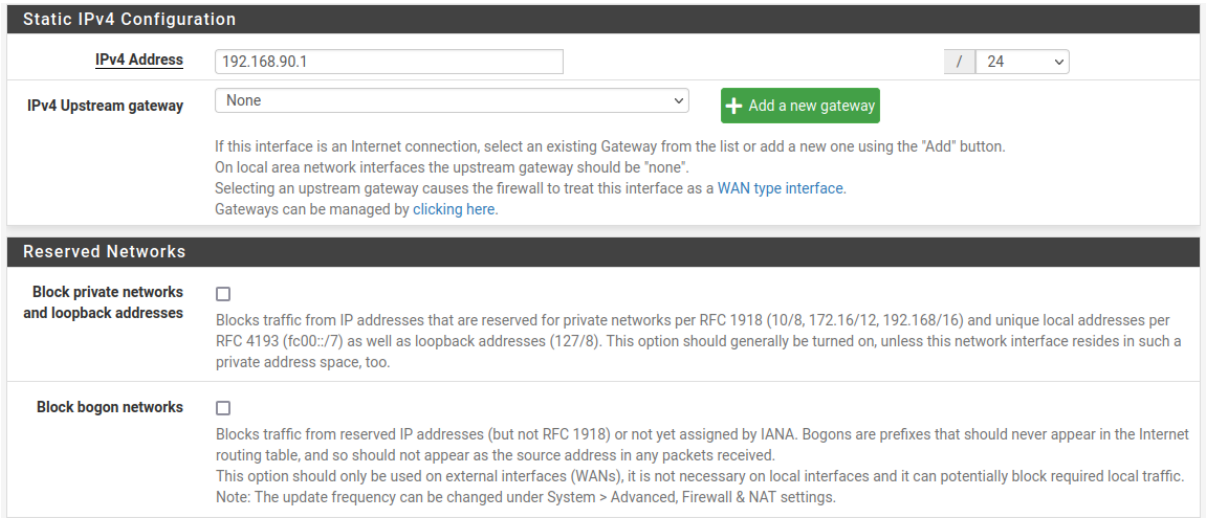


Tenemos que marcar **Static IPv4**

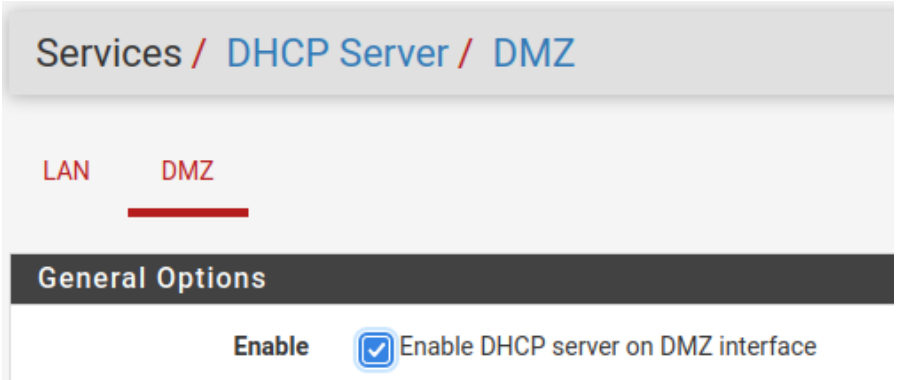




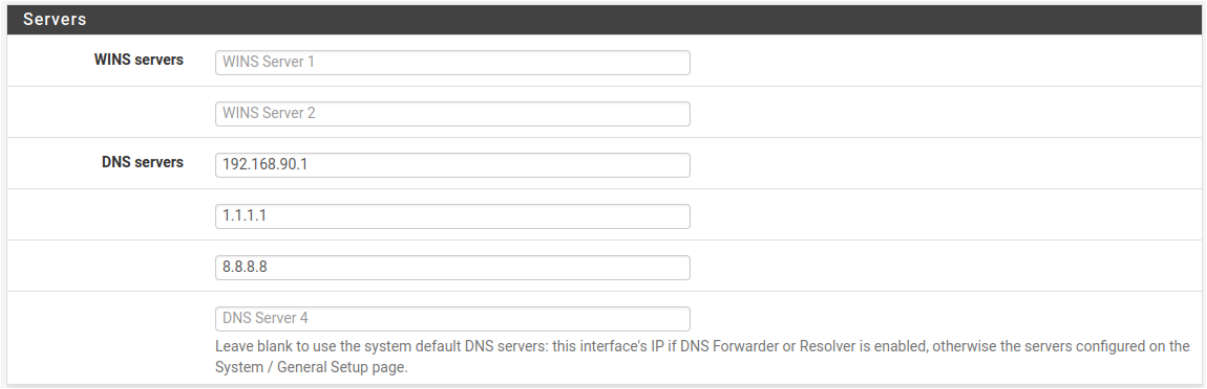
En **DMZ** le ponemos la siguiente dirección IP



Ahora nos vamos a **Services / DHCP** Server y seleccionamos DMZ y activamos el DHCP.



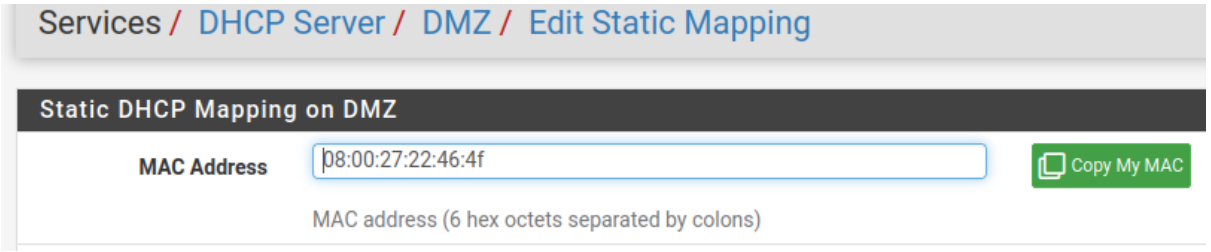
Le ponemos los siguientes servidores de DNS.



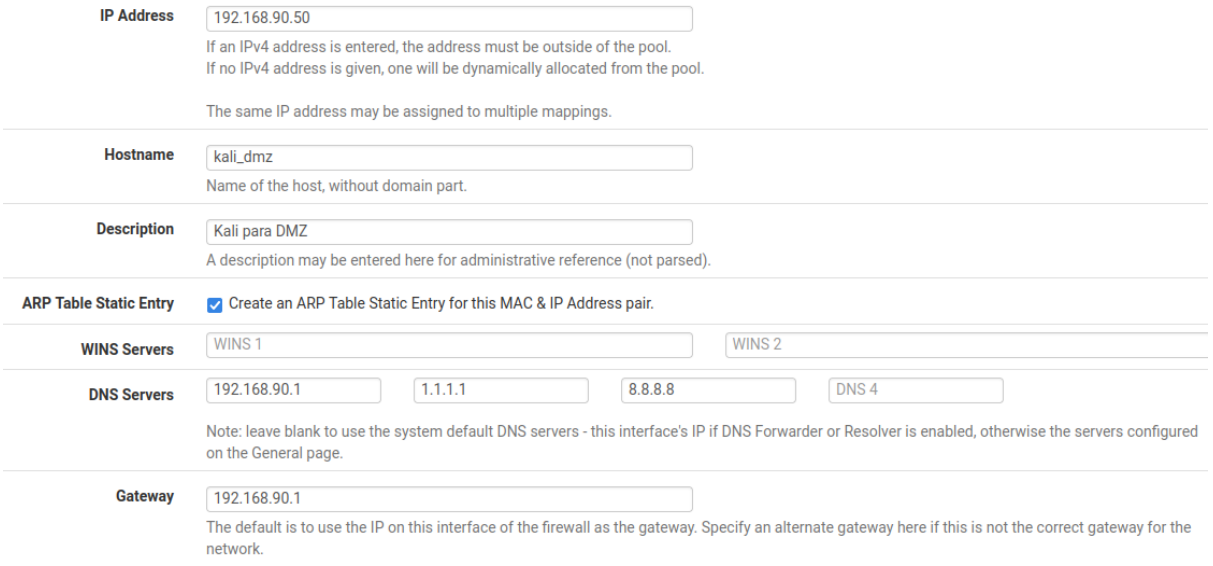
Y la puerta de enlace.

En el siguiente rango.

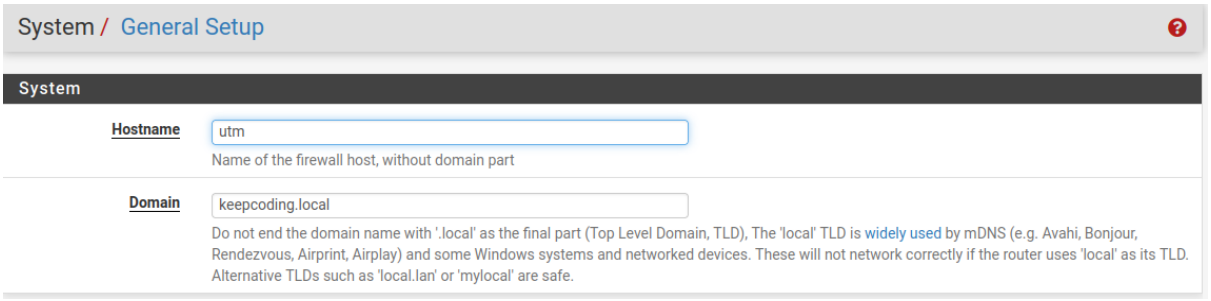
Editamos el mapeo estático de DHCP en DMZ e introducimos nuestra MAC.



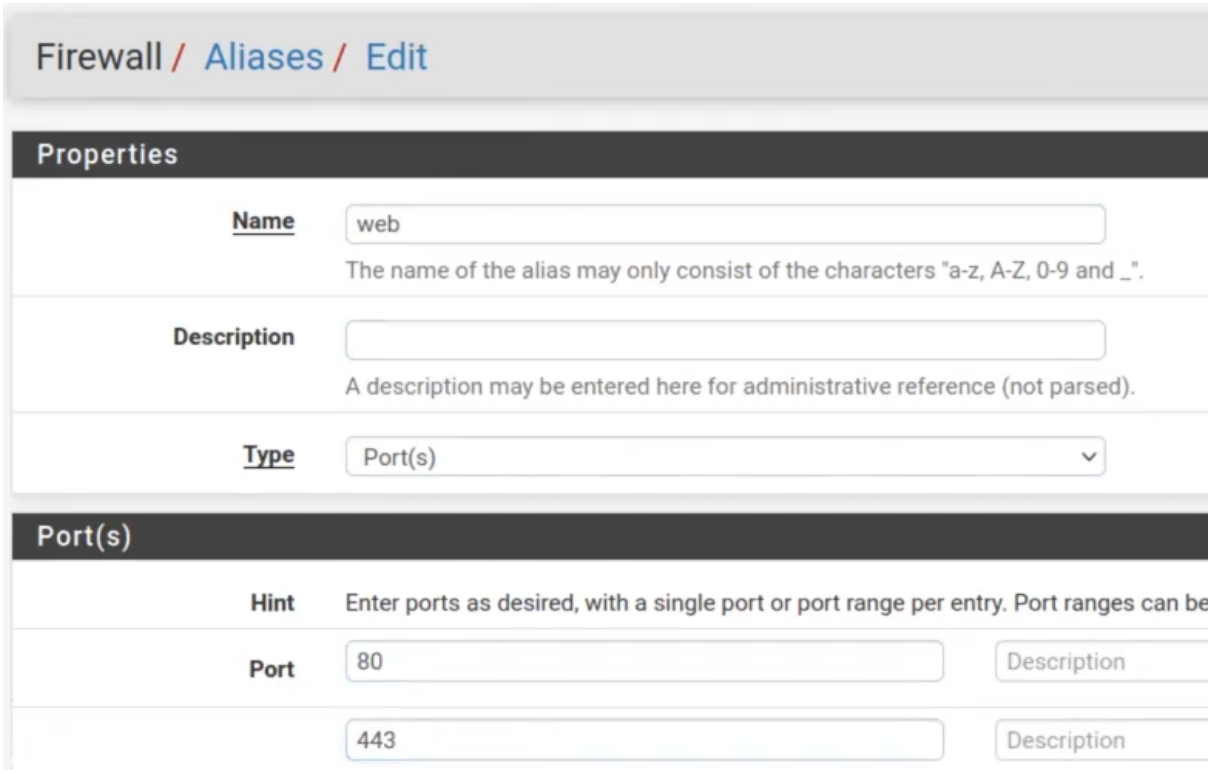
Y rellenamos los campos restantes de la siguiente manera.



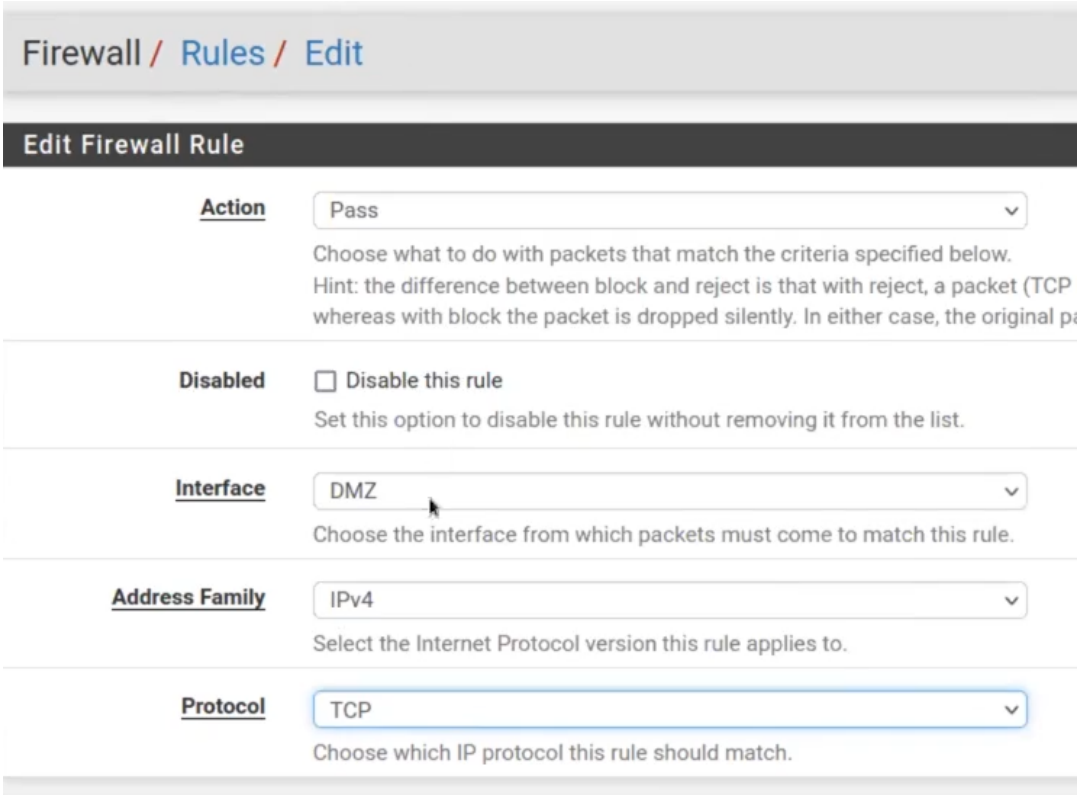
Una vez finalizado le damos a guardar y aplicamos los cambios. Tras esto nos vamos a **System / General Setup**. Ahí vamos a darle un nombre al firewall y un dominio.



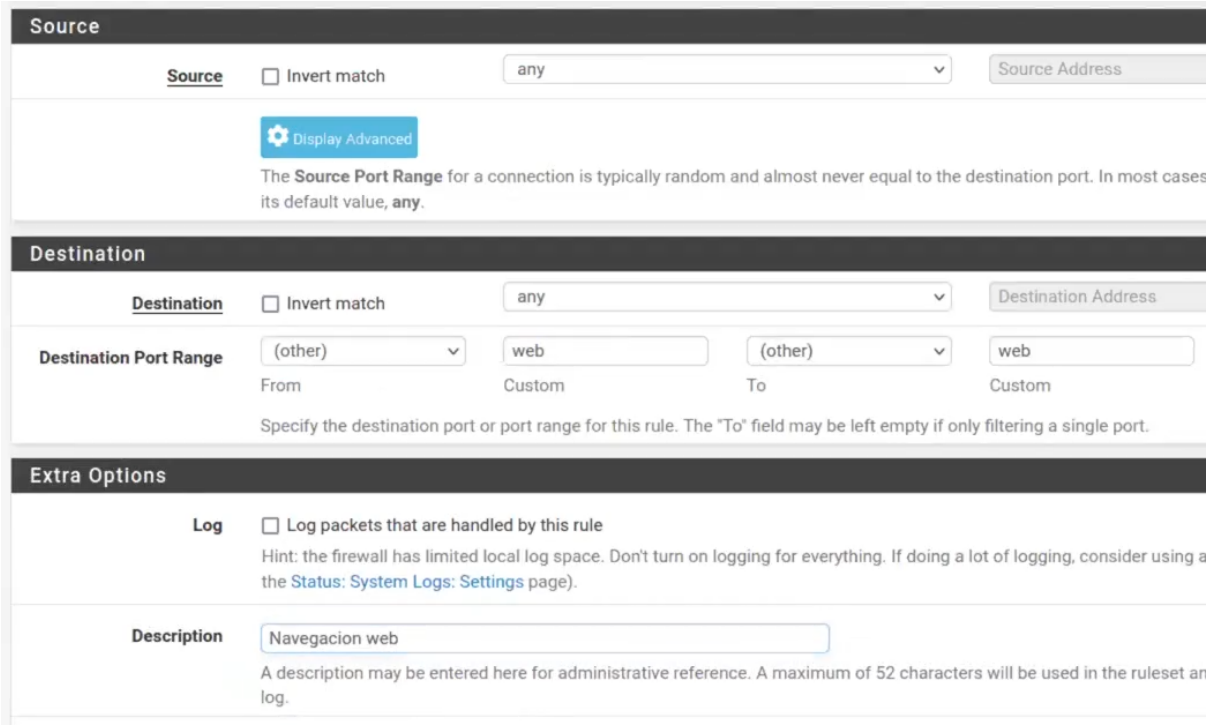
Tras esto vamos a **Firewall / Aliases** y creamos uno nuevo de tipo **Port(s)** y le metemos los puertos que queremos añadir, en este caso el 80 y el 433.



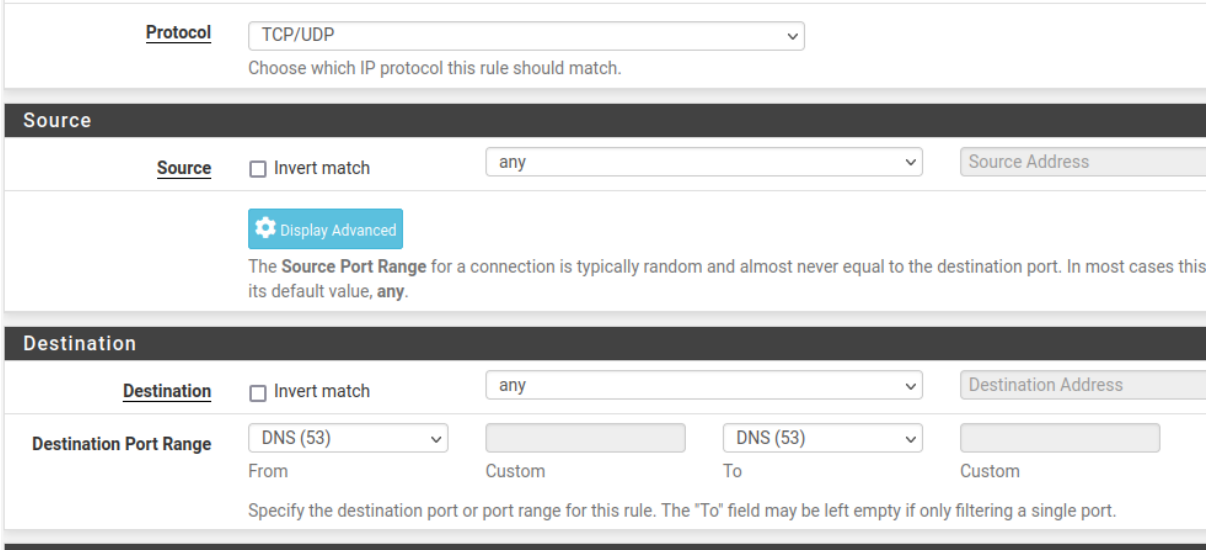
Y ahora en **Firewall / Rules** seleccionamos **DMZ** y vamos a crear algunas reglas.



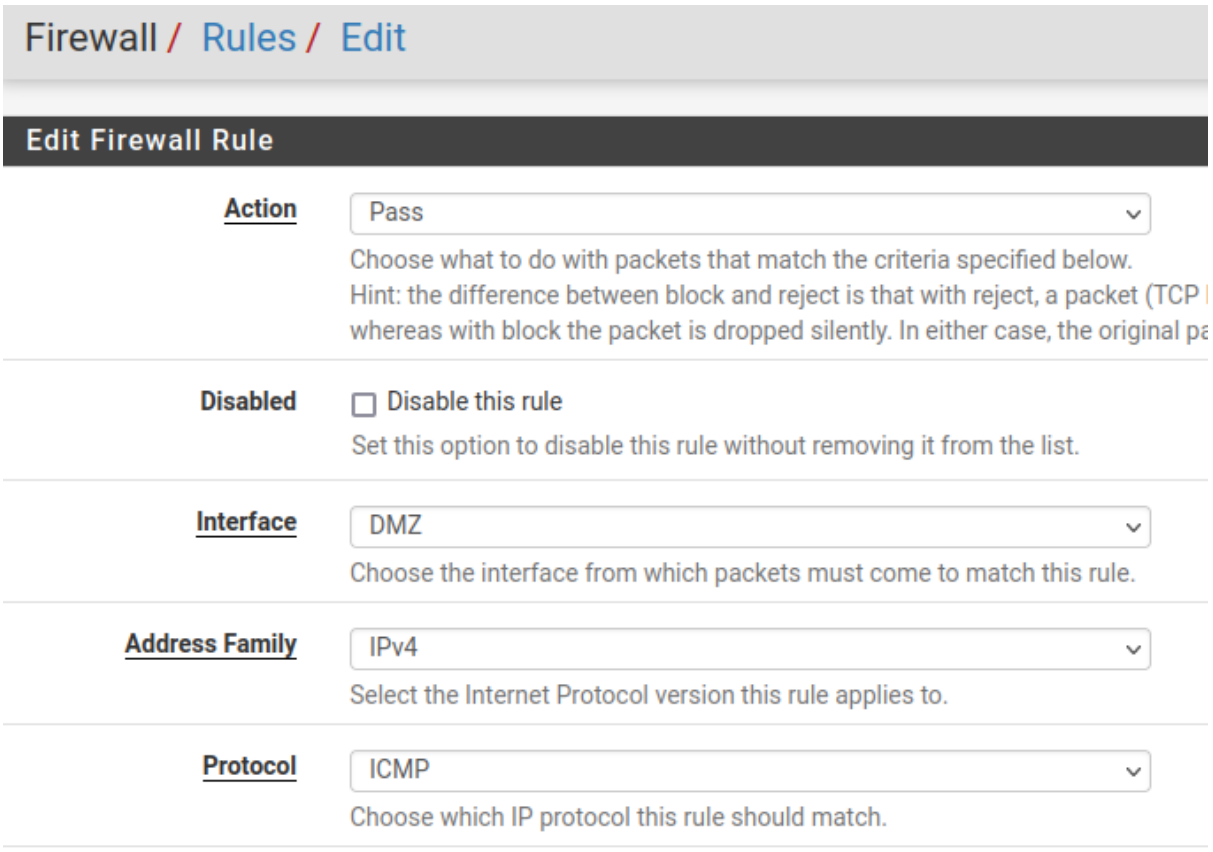
En este caso es una regla de paso utilizando el protocolo TCP y en fuente y destino seleccionamos “any”



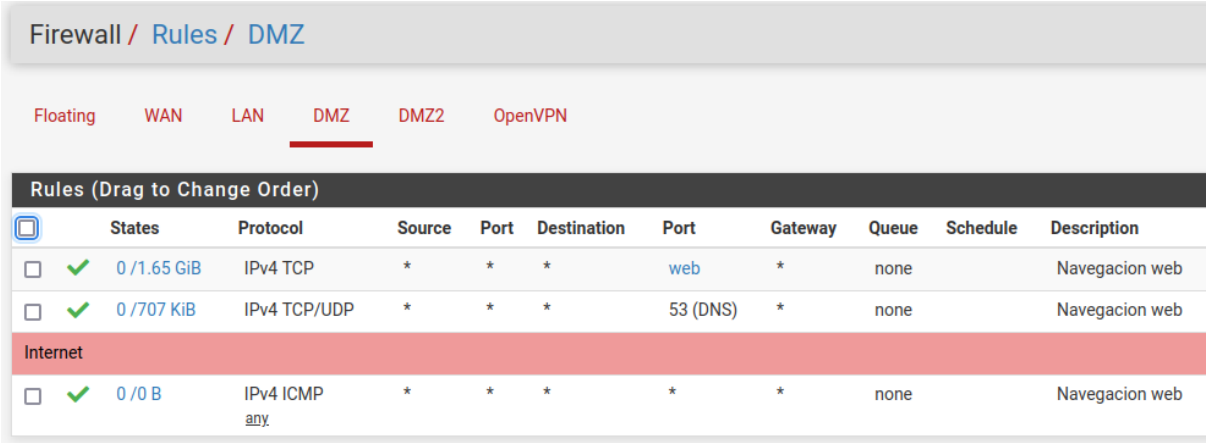
Ahora clonamos la regla anterior y cambiamos el protocolo por TCP/UDP y en el rango del puerto de destino ponemos 53 (El puerto de DNS).



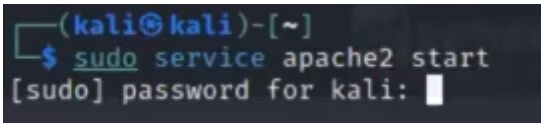
También creamos una regla para permitir hacer ping.



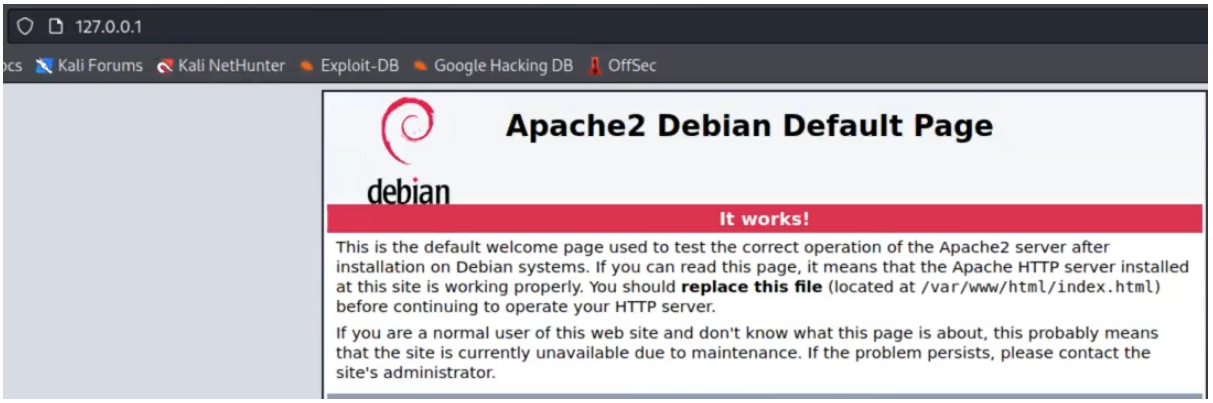
Así quedarían las reglas de nuestro DMZ si hemos seguido los pasos.



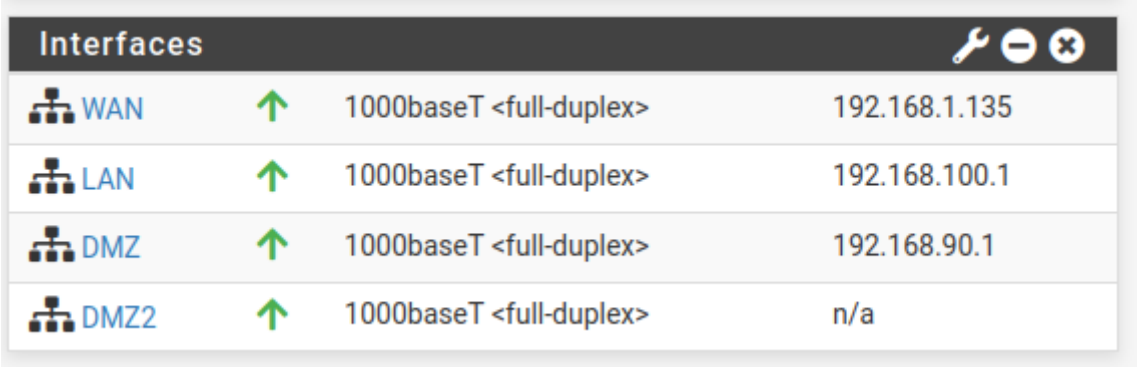
Ahora vamos a arrancar el servicio de **Apache** en la terminal de Kali.



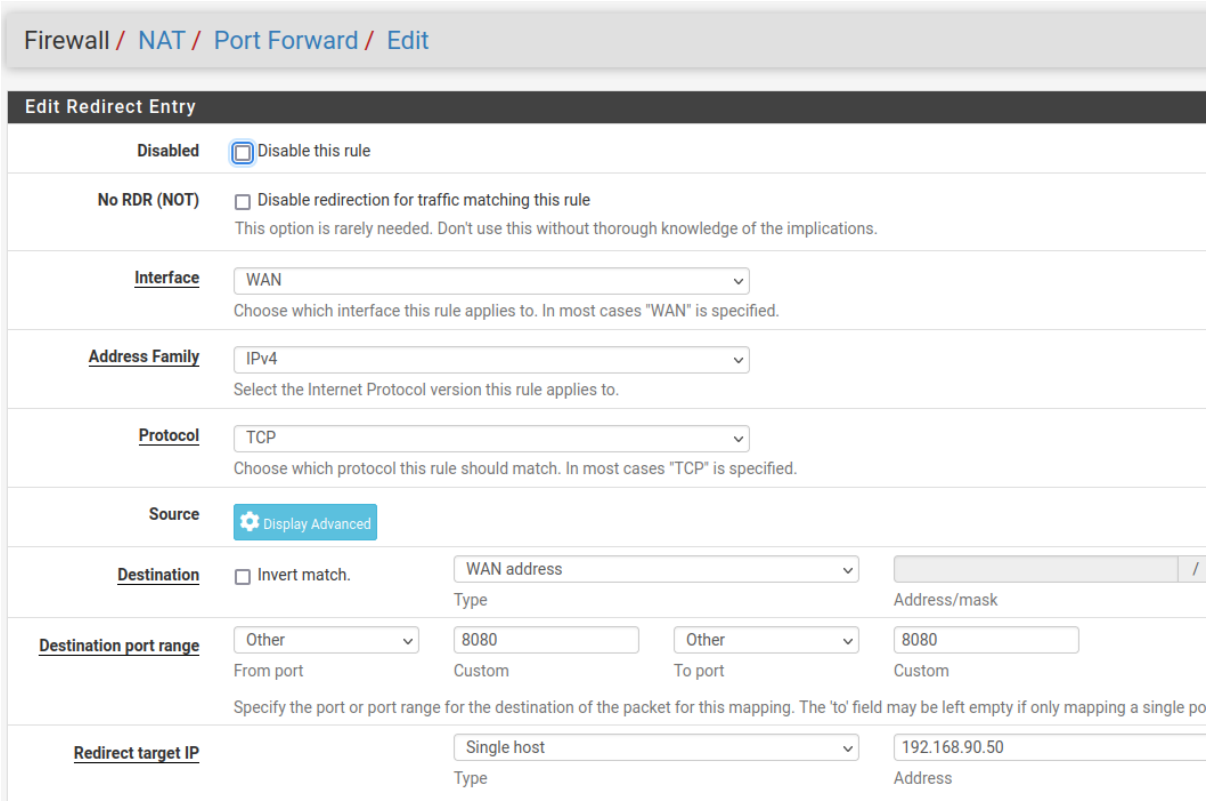
y probamos a acceder desde nuestro navegador en la IP 127.0.0.1

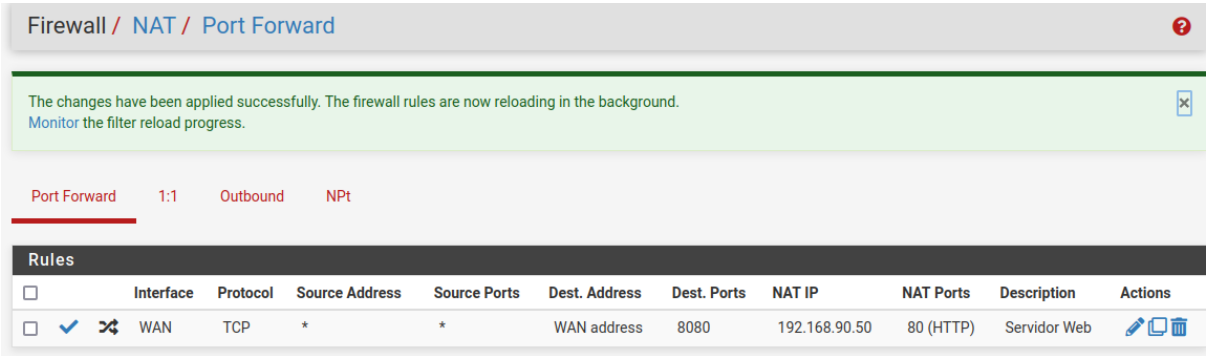


Nos vamos al dashboard de nuestro PfSense y miramos las IPs que tenemos asignadas.

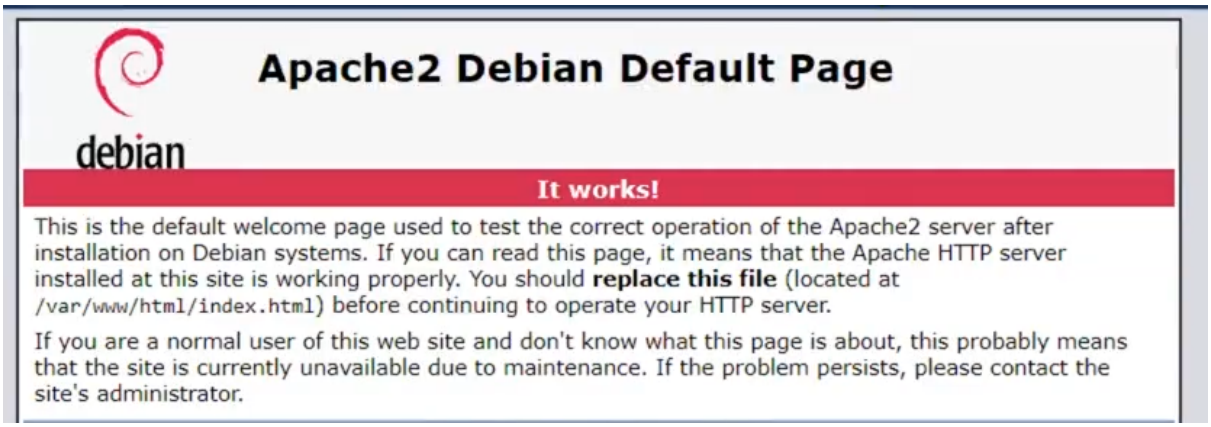


Ahora vamos a **Firewall / NAT / Port Forward** para redireccionar a una IP de nuestra DMZ

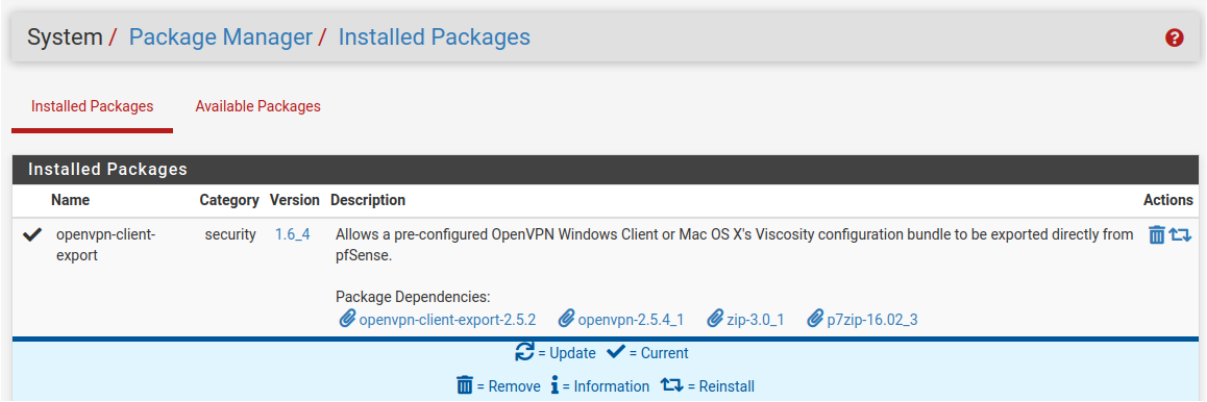




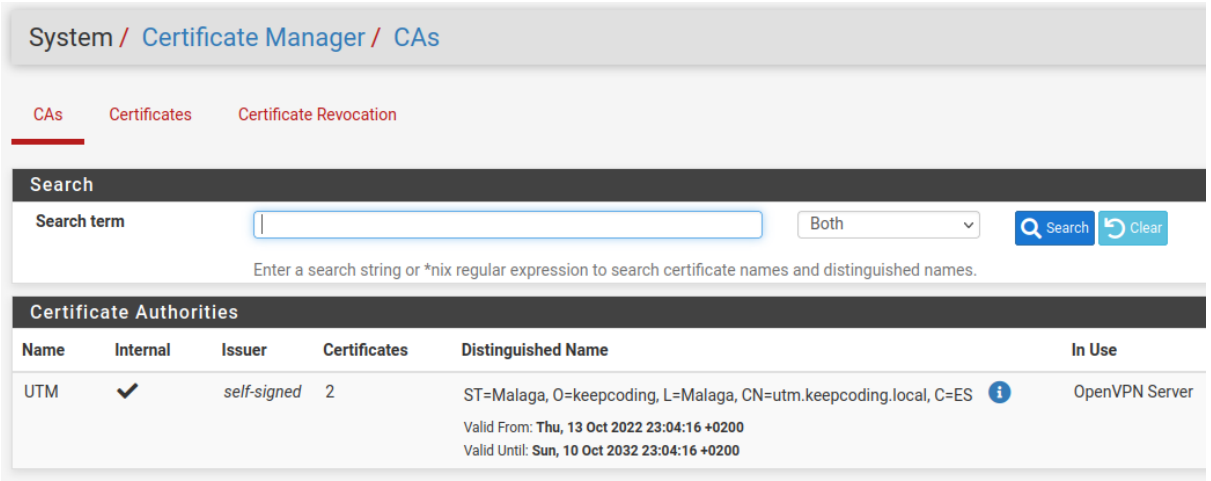
Y ahora podemos acceder a nuestro Apache desde el navegador de nuestro pc escribiendo "**IP:8080**"



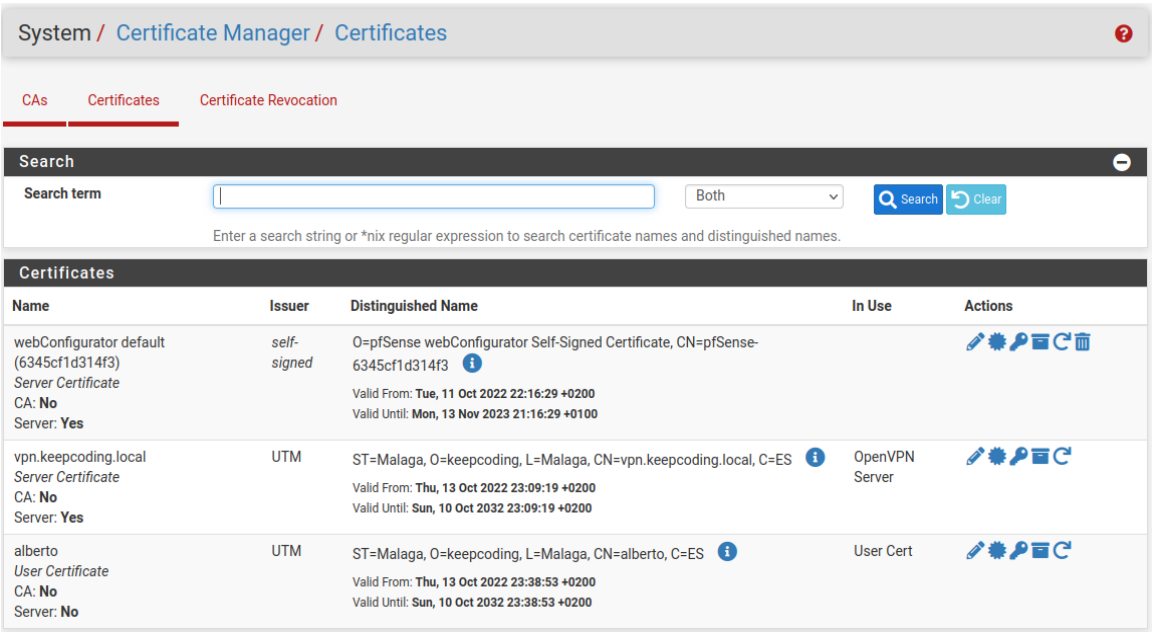
Vamos a configurar nuestro propio **OpenVPN**, para ello primero vamos a **System / Package Manager** (en mi caso ya lo tenía instalado) y vamos a **Available Packages** y escribimos vpn y nos aparecerá openvpn y lo instalamos.



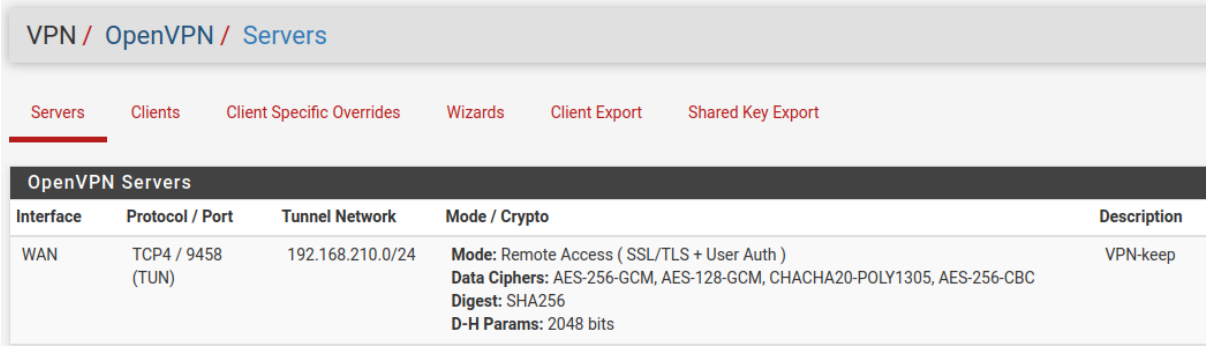
Ahora vamos a crear una entidad certificadora. Para ello nos vamos a **System / Certificate Manager / CAs** y creamos una nueva. (La configuración de la mía)



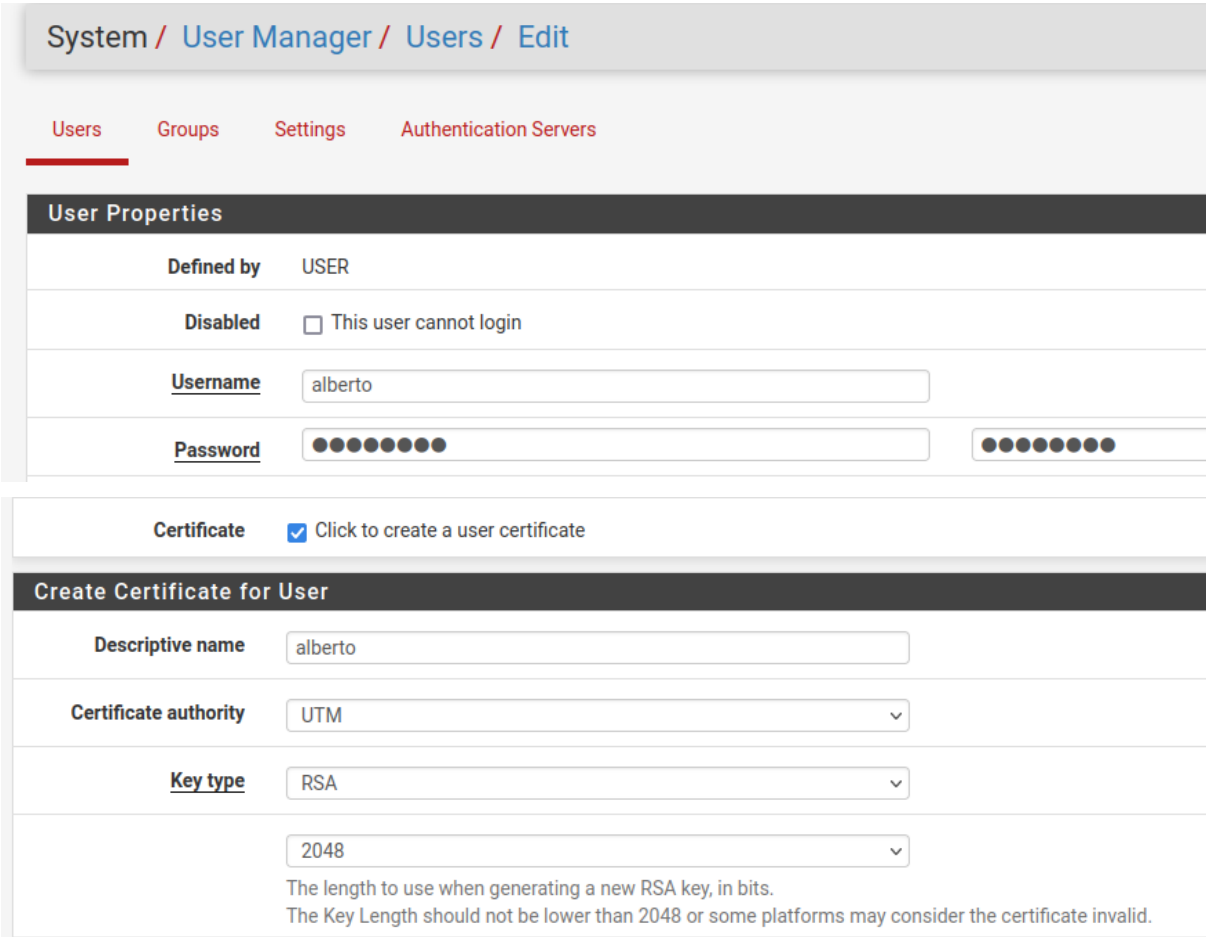
Tras tener la CA vamos a crear los certificados, uno de server y otro de usuario.



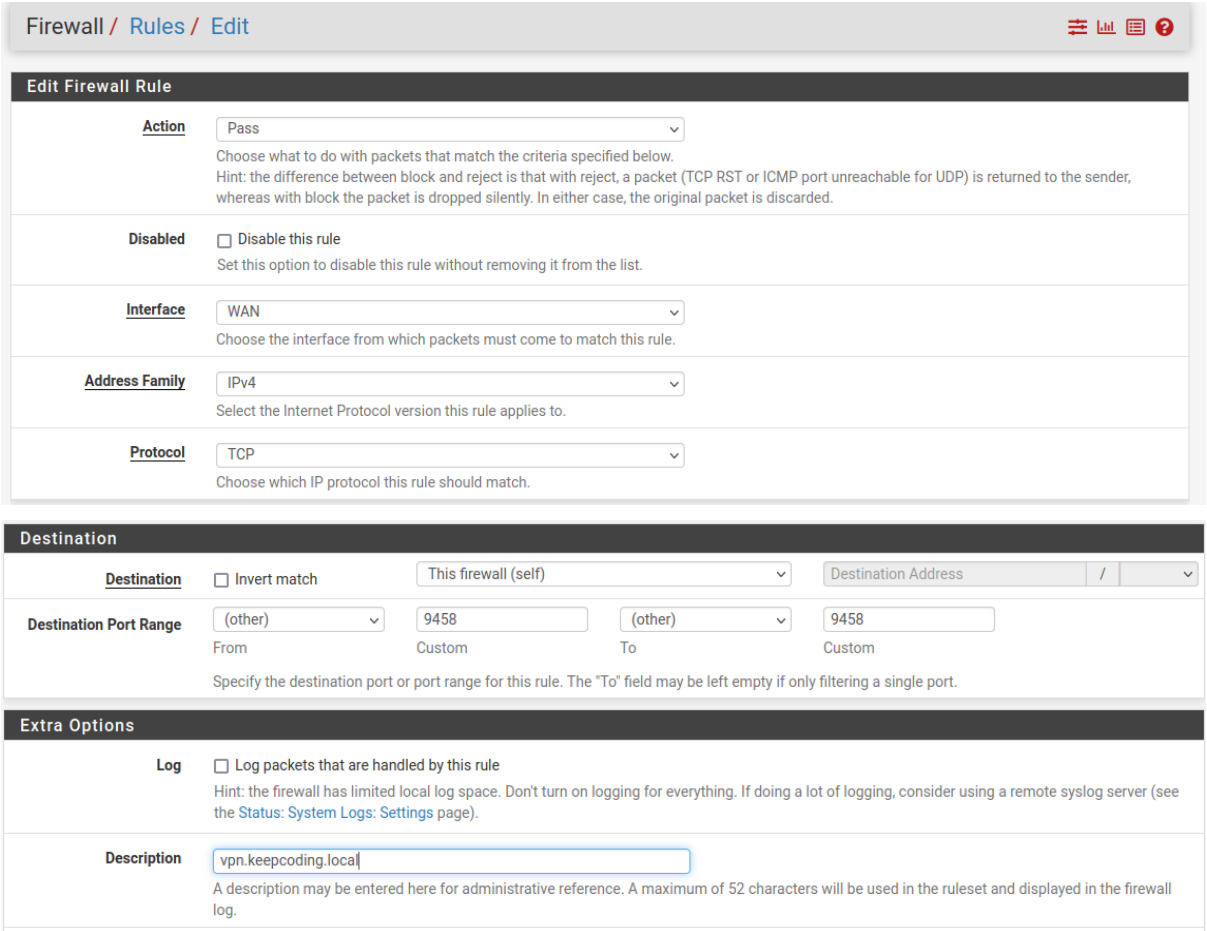
Y ahora vamos a crear el server, para ello vamos a **VPN / OpenVPN / Servers** y los creamos con los siguientes parámetros.



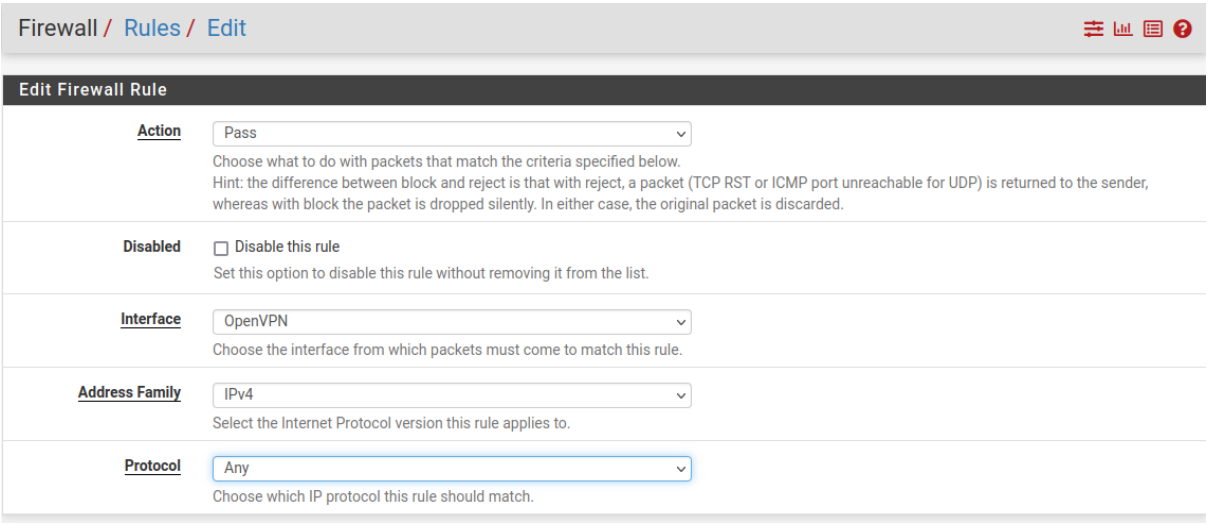
Para la creación de usuarios vamos **System / User Manager / Users**.



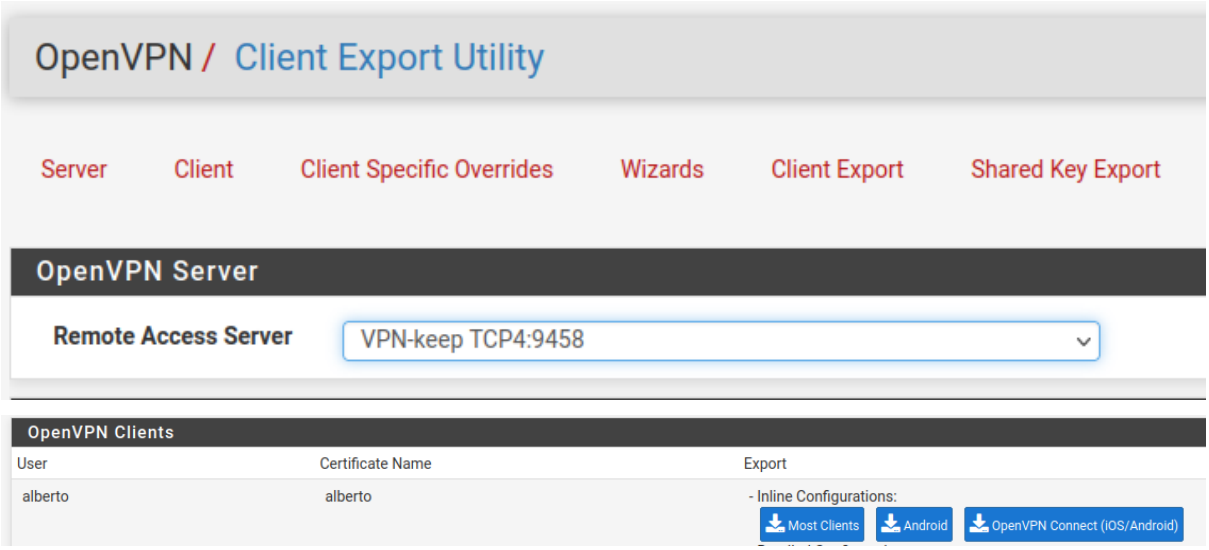
Y ahora nos vamos a **Firewall / Rules / WAN** y creamos una regla de paso con destinos a este firewall.



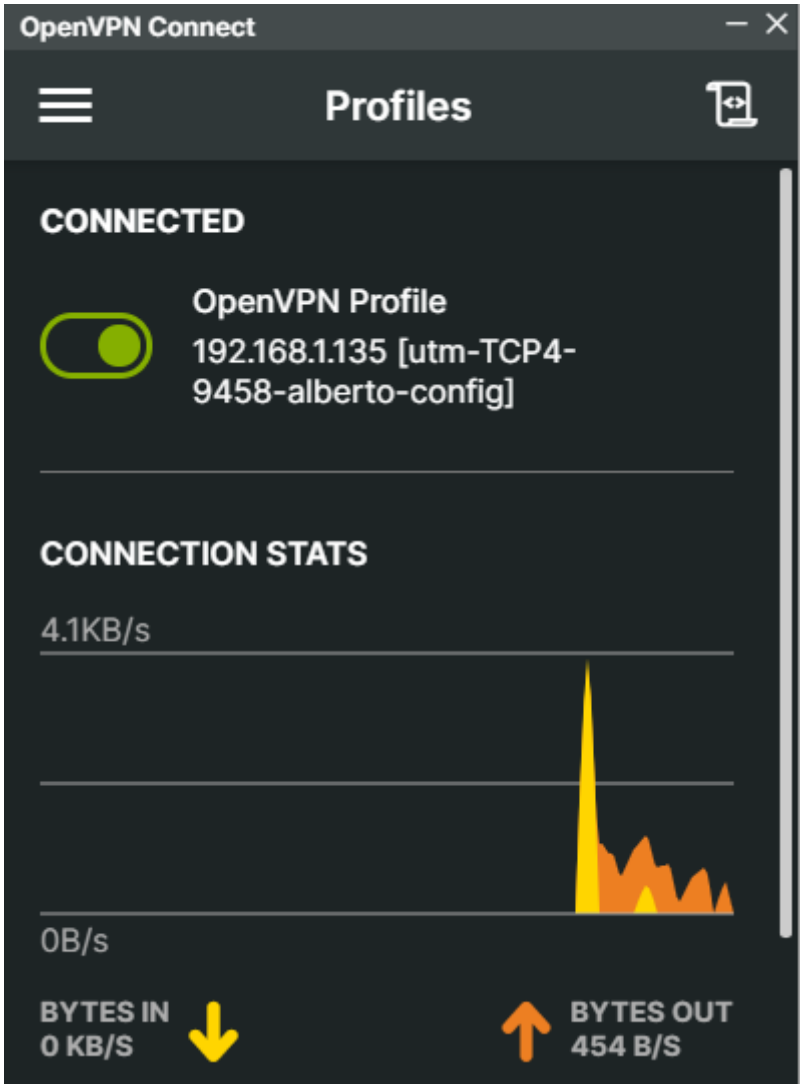
Seleccionamos la interface de **OpenVPN** y creamos una regla para que pase todo (no es recomendable crear este tipo de reglas)



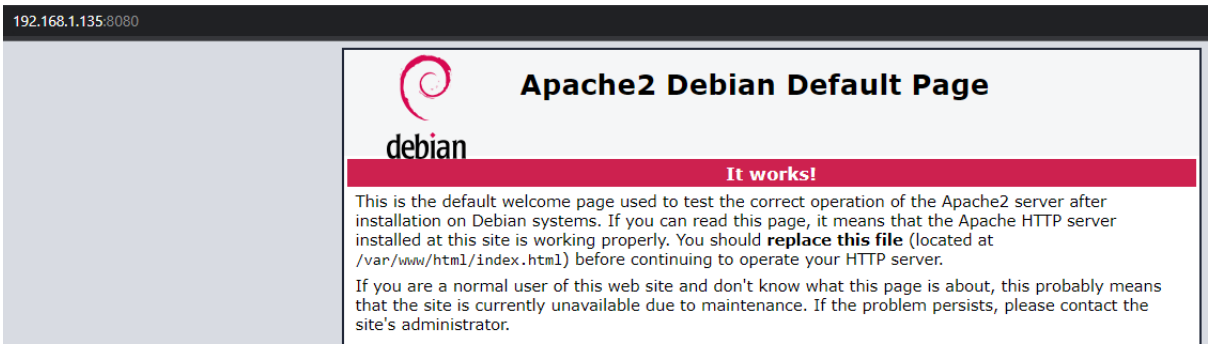
Y ahora nos vamos a **OpenVPN / Client Export Utility** y descargamos nuestro usuario.



Nos mandamos el archivo a nuestro PC y lo introducimos en el cliente **OpenVPN Connect** para tener nuestro propio túnel VPN.

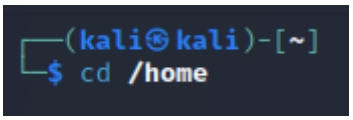


Ya podemos acceder a nuestra red desde el PC sin problema.



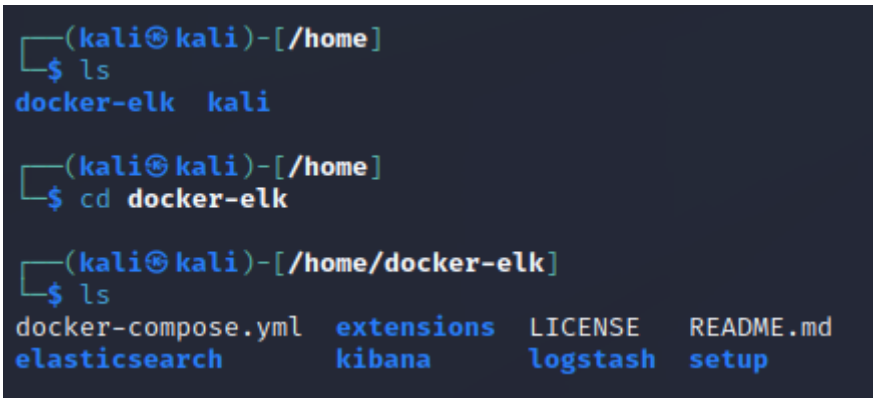
ELASTIC

Es el turno de **Elastic**, un potente software de gestión de información y eventos de seguridad. En mi caso voy a instalarlo en home. Para situarnos dentro hacemos el siguiente comando.



Una vez estemos dentro del directorio elegido, descargamos el repositorio (Hay que hacerlo con permiso de root).

Ahora vamos a la carpeta que nos ha creado y la listamos.



Ejecutamos el comando **docker-compose up -d**. Para ello también tenemos que ser root.

```
┌──(root㉿kali)-[/home/docker-elk]
└─# docker-compose up -d
Creating network "docker-elk_elk" with driver "bridge"
Creating volume "docker-elk_setup" with default driver
Creating volume "docker-elk_elasticsearch" with default driver
Building elasticsearch
Sending build context to Docker daemon  4.608kB
Step 1/2 : ARG ELASTIC_VERSION
Step 2/2 : FROM docker.elastic.co/elasticsearch/elasticsearch:${ELASTIC_VERSION}
8.4.3: Pulling from elasticsearch/elasticsearch
2ec5bc8cf243: Pull complete
e7a52014c641: Pull complete
fe22b900b382: Pull complete
1f95ca3684dd: Pull complete
2d6739673d83: Pull complete
a7ed8e9af4ef: Pull complete
f39cca40e65f: Pull complete
05f4cbaa0d4a: Pull complete
ce9edbaccd81: Pull complete
Digest: sha256:739ec9d428869f16e9e02247d5082849ebb4302c87e0abf9f70971cbb40c3bab
Status: Downloaded newer image for docker.elastic.co/elasticsearch/elasticsearch:8.4.3
```

Ahora vamos a ver los contenedores que nos ha creado.

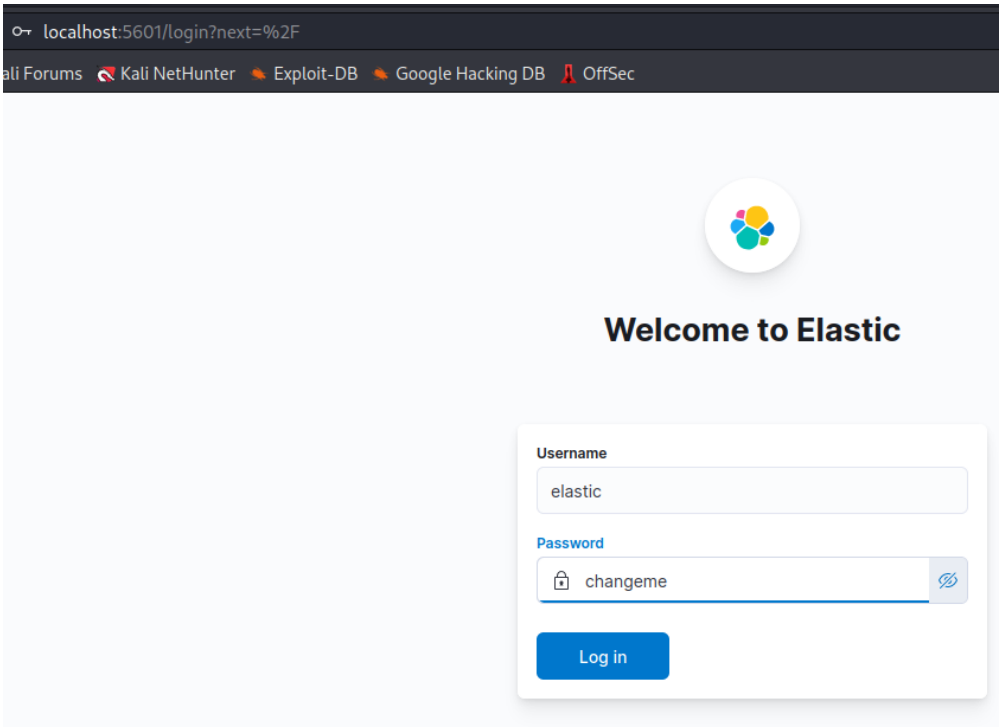
```
┌──(root㉿kali)-[/home/docker-elk]
└─# docker ps
CONTAINER ID   IMAGE                     COMMAND                  CREATED              STATUS              PORTS

                                NAMES
06fe2b0c4f9b   docker-elk_logstash       "/usr/local/bin/dock…"   About a minute ago   Up About a minute   0.0.0.0:5044→5044
/tcp, :::5044→5044/tcp, 0.0.0.0:9600→9600/tcp, :::9600→9600/tcp, 0.0.0.0:50000→50000/tcp, :::50000→50000/tcp, 0.0.0.0:500
00→50000/udp, :::50000→50000/udp   docker-elk_logstash_1
6ec42f0e9700   docker-elk_kibana         "/bin/tini -- /usr/l…"   About a minute ago   Up About a minute   0.0.0.0:5601→5601
/tcp, :::5601→5601/tcp
                                docker-elk_kibana_1
411676d5e72b   docker-elk_elasticsearch  "/bin/tini -- /usr/l…"   About a minute ago   Up About a minute   0.0.0.0:9200→9200
/tcp, :::9200→9200/tcp, 0.0.0.0:9300→9300/tcp, :::9300→9300/tcp
                                docker-elk_elasticsearch_1
```

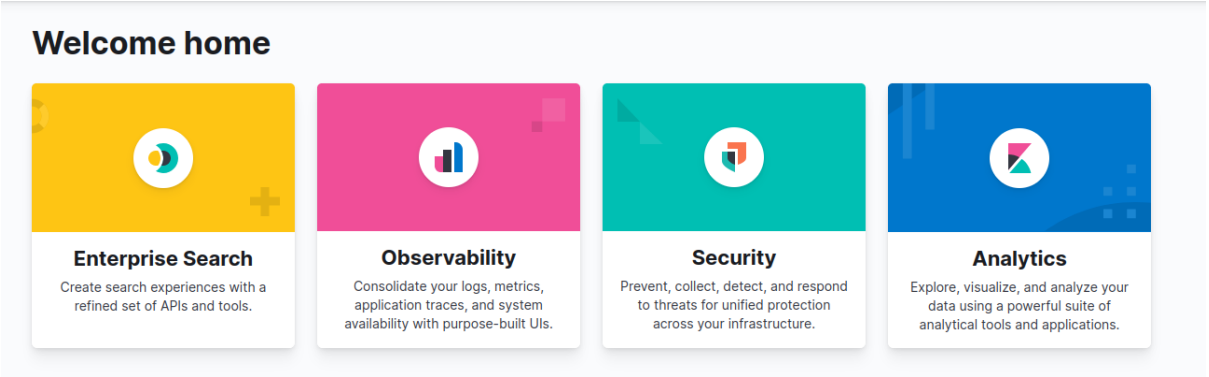
```
┌──(root㉿kali)-[/home/docker-elk]
└─# docker-compose ps
          Name                        Command               State                            Ports
-------------------------------------------------------------------------------------------------------------------
docker-elk_elasticsearch_1   /bin/tini -- /usr/local/bi ...   Up       0.0.0.0:9200→9200/tcp,:::9200→9200/tcp,
                                                                      0.0.0.0:9300→9300/tcp,:::9300→9300/tcp
docker-elk_kibana_1          /bin/tini -- /usr/local/bi ...   Up       0.0.0.0:5601→5601/tcp,:::5601→5601/tcp
docker-elk_logstash_1        /usr/local/bin/docker-entr ...   Up       0.0.0.0:50000→50000/tcp,:::50000→50000/tcp,
                                                                      0.0.0.0:50000→50000/udp,:::50000→50000/udp,
                                                                      0.0.0.0:5044→5044/tcp,:::5044→5044/tcp,
                                                                      0.0.0.0:9600→9600/tcp,:::9600→9600/tcp
docker-elk_setup_1           /entrypoint.sh                   Exit 0
```

El último que nos aparece “**docker-elk_setup_1**” nos indica que ya ha terminado de crearse. Así que ya podemos entrar en Elastic a través del navegador.

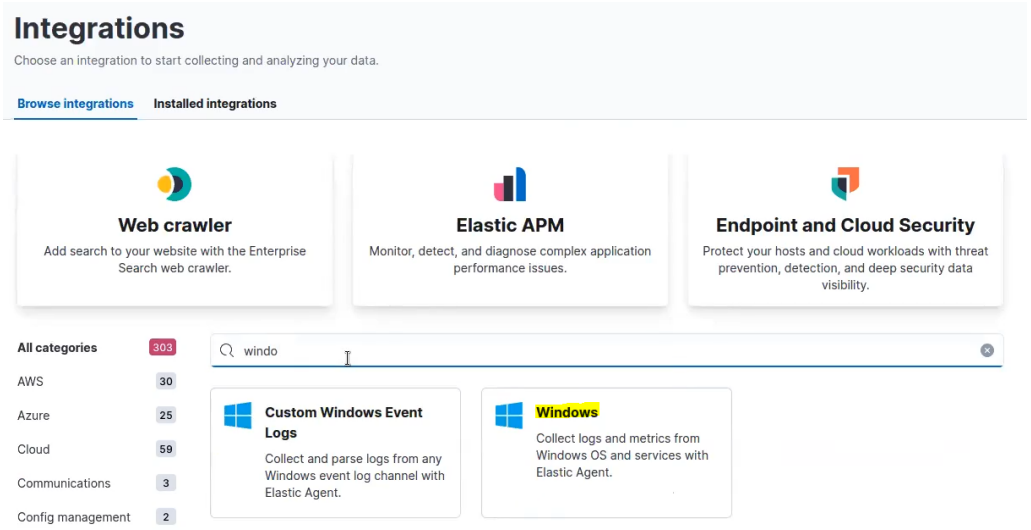
Para acceder tenemos que poner “**localhost:5601**” Username: **elastic** Password: **changeme**



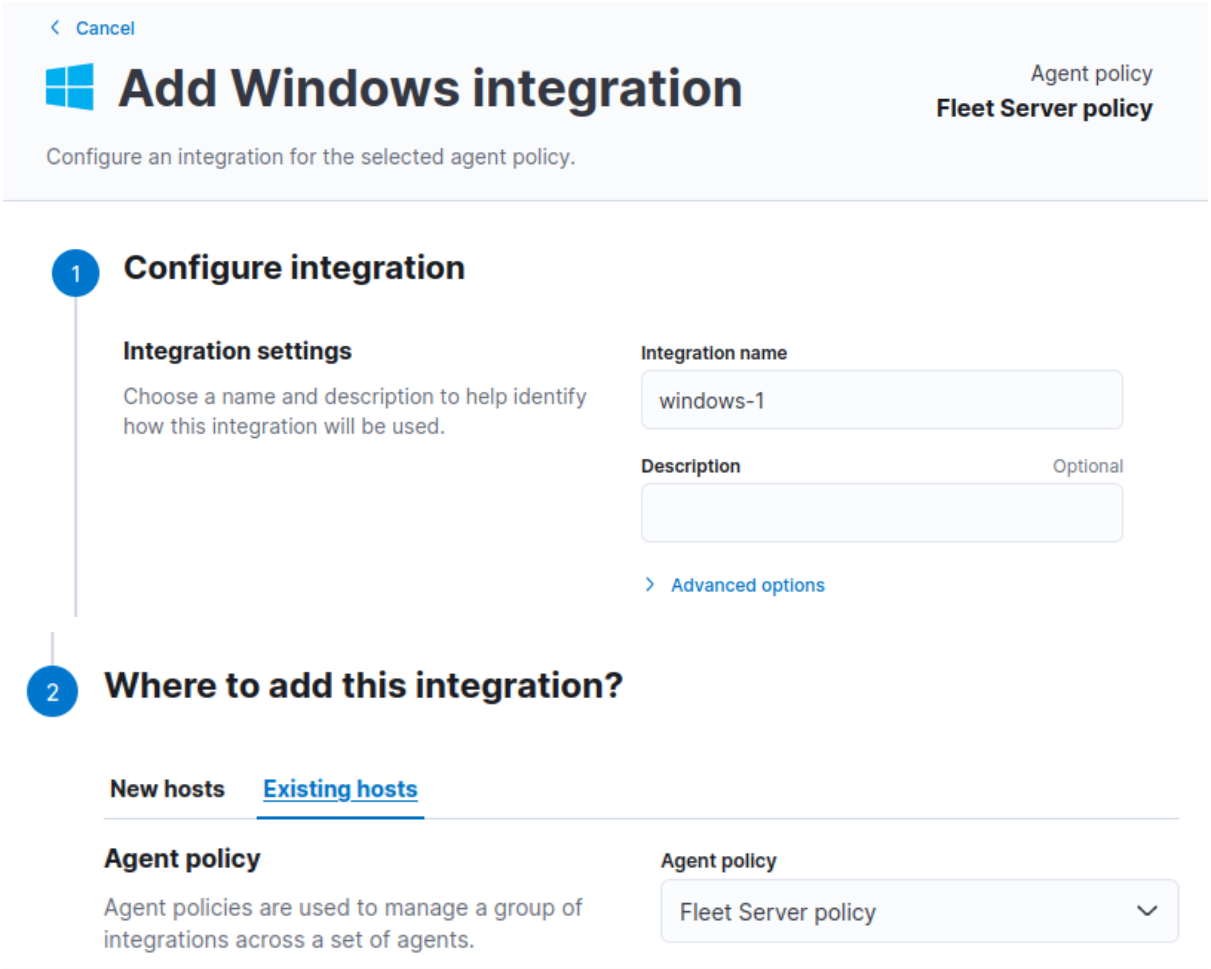
Si hemos seguido todos los pasos estaremos dentro de Elastic.



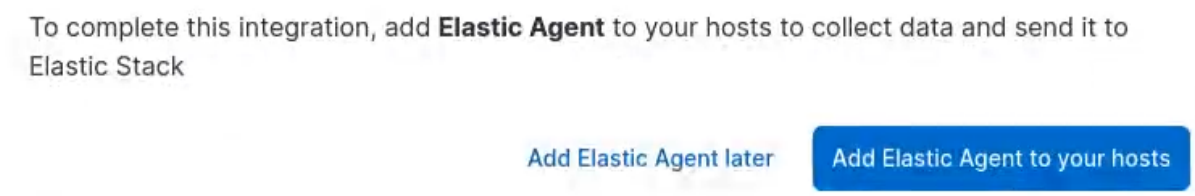
Ahora vamos a añadir una nueva integración. En este caso la de Windows.



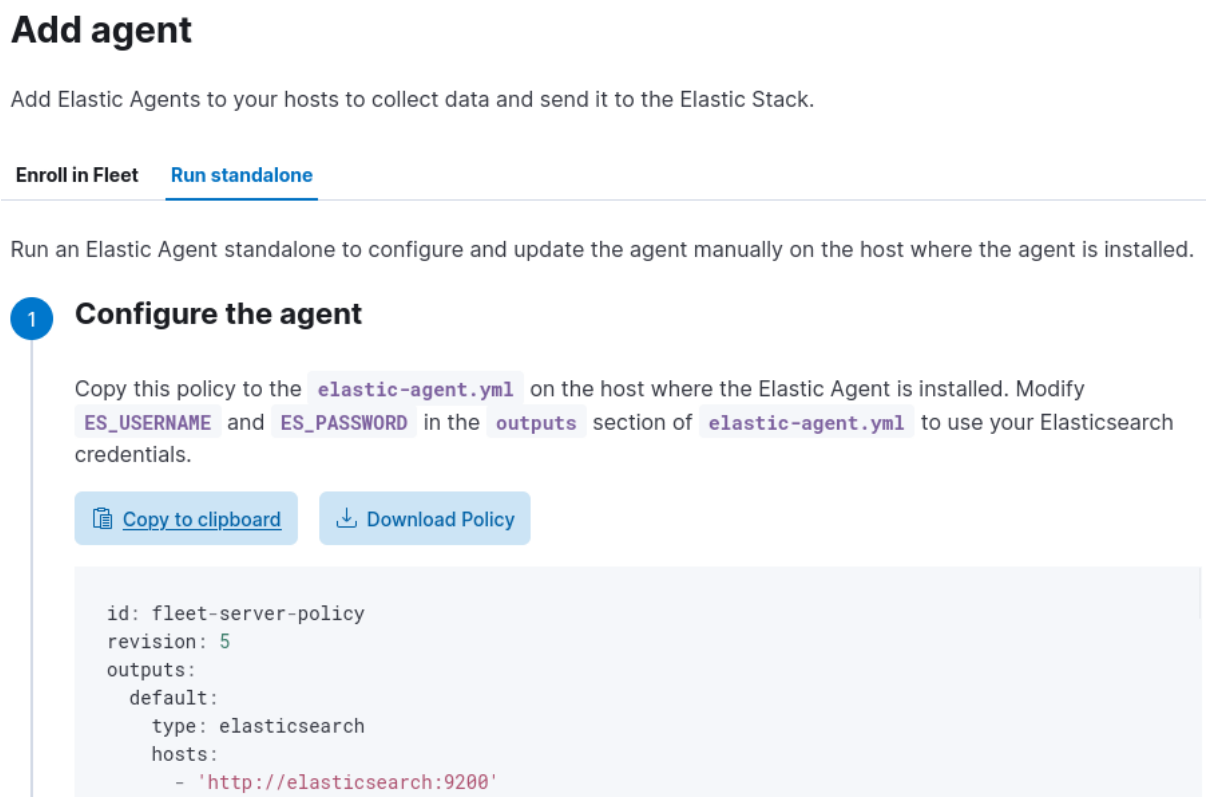
Para configurarlo podemos dejar lo primero como estaba o ponerle el nombre que queramos, y luego tenemos que seleccionar **Existing hosts** y "**Fleet Server policy**"



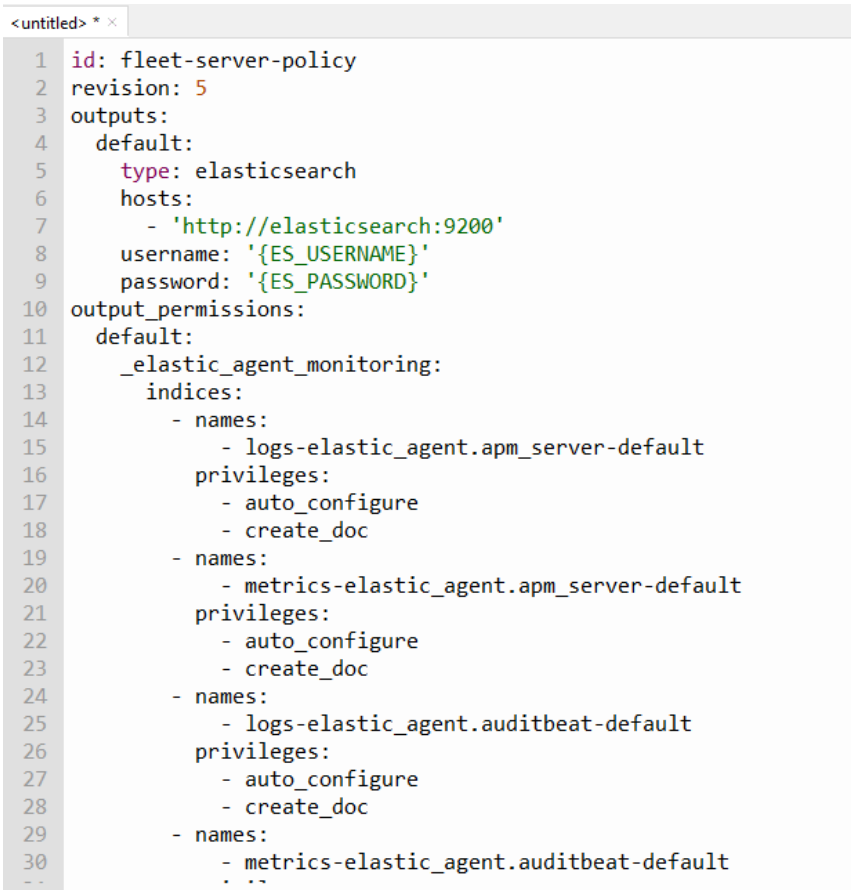
Ahora le damos a añadir a nuestro host



Seleccionamos “**Run Standalone**” y copiamos en el portapapeles.



Abrimos algún programa que le podamos pegar texto sin perder el formato, y lo copiamos ahí.



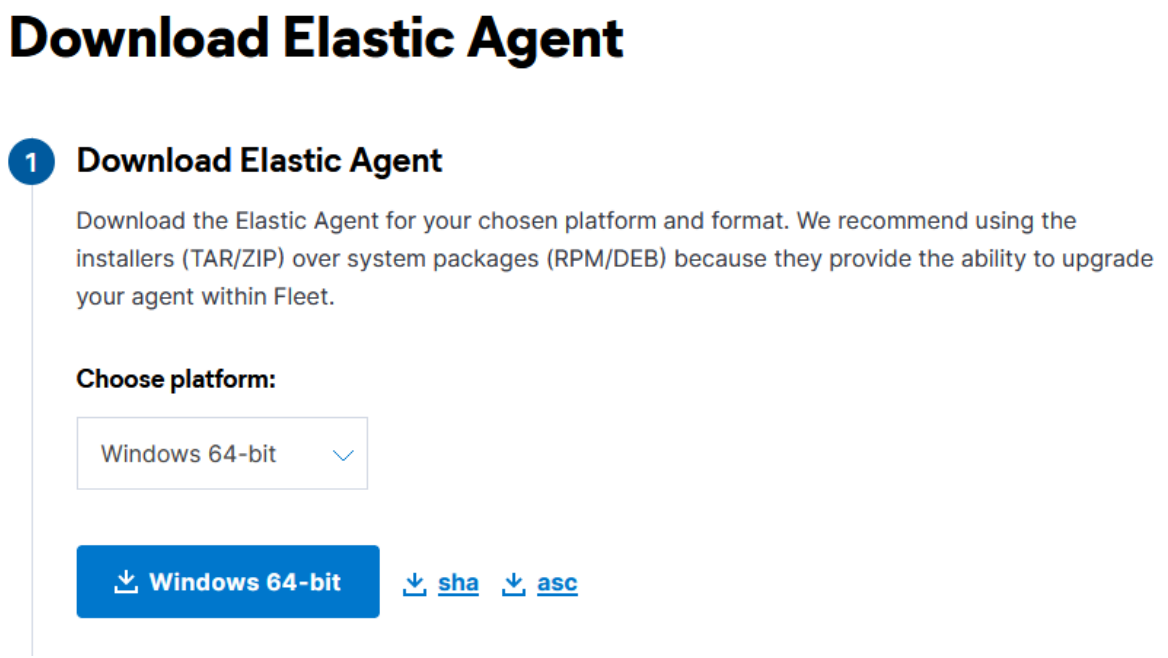
Lanzamos un comando **“ip a”** en nuestra terminal de Kali para ver la IP que tenemos.

```
eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
 link/ether 08:00:27:22:46:4f brd ff:ff:ff:ff:ff:ff
 inet 192.168.90.50/24 brd 192.168.90.255 scope global dynamic noprefixroute eth0
    valid_lft 4379sec preferred_lft 4379sec
 inet6 fe80::9f62:3a8c:99a3:cec2/64 scope link noprefixroute
    valid_lft forever preferred_lft forever
```

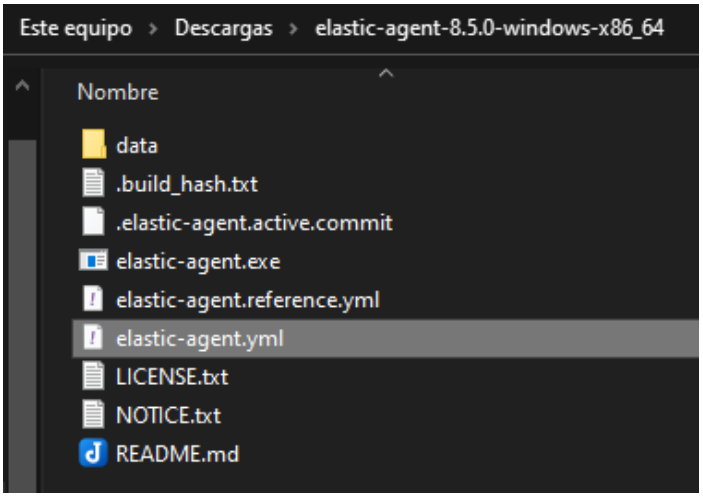
A continuación sustituimos el fichero anterior con nuestra IP y el usuario y contraseña de Elastic.

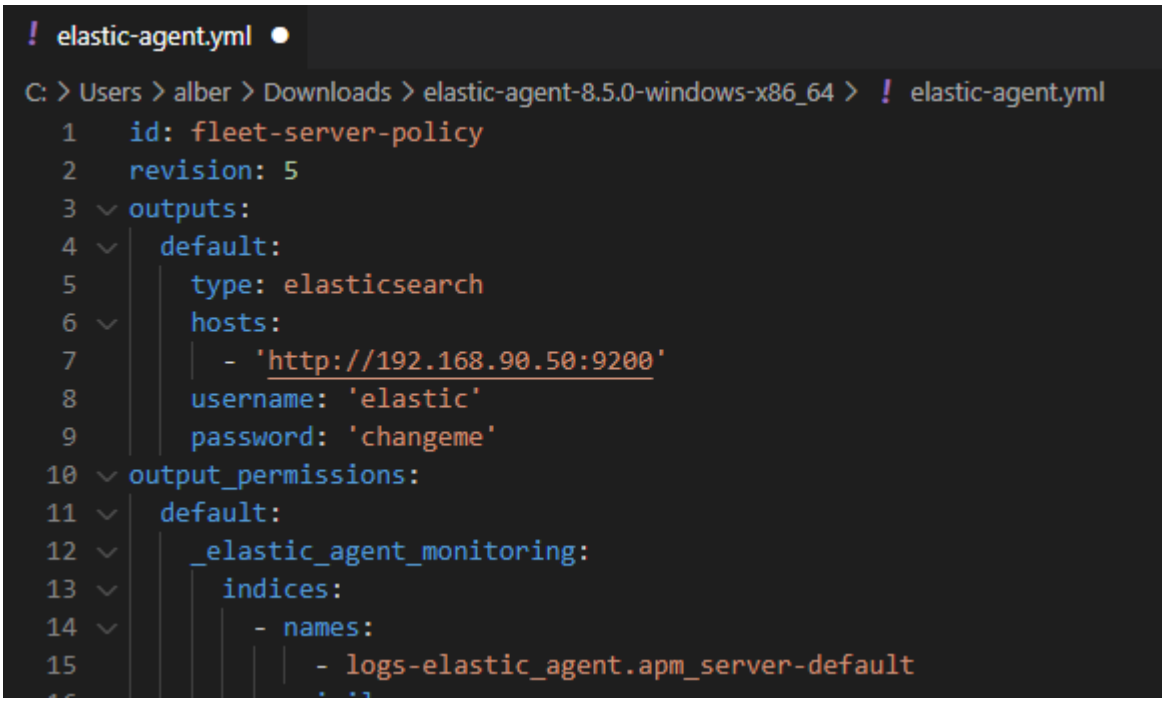
```
type: elasticsearch
hosts:
  - 'http://192.168.90.50:9200'
username: 'elastic'
password: 'changeme'
```

En nuestro PC Windows descargamos el agente de Elastic de la siguiente web https://www.elastic.co/es/downloads/elastic-agent

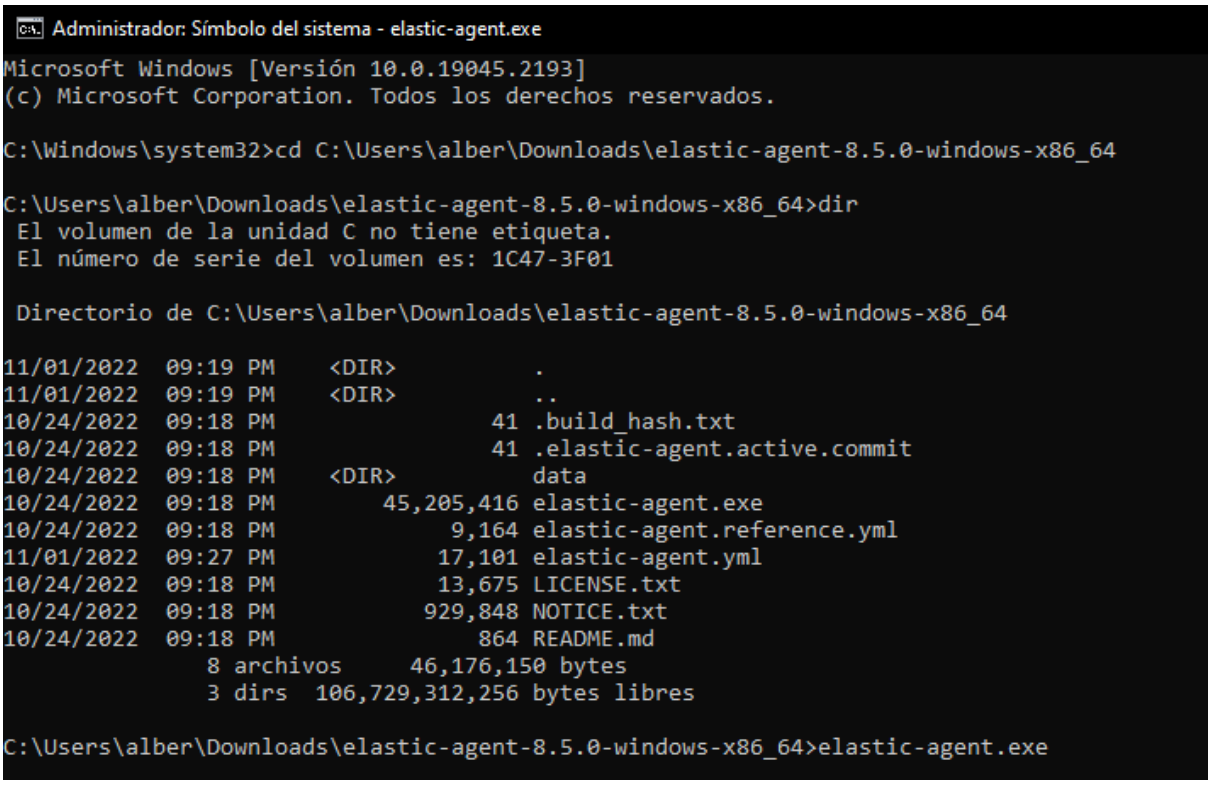


Descomprimimos el archivo, pero no lo ejecutamos. Entramos en la carpeta y abrimos el archivo **elastic-agent.yml** con Visual Studio Code y pegamos el texto que hemos editado.

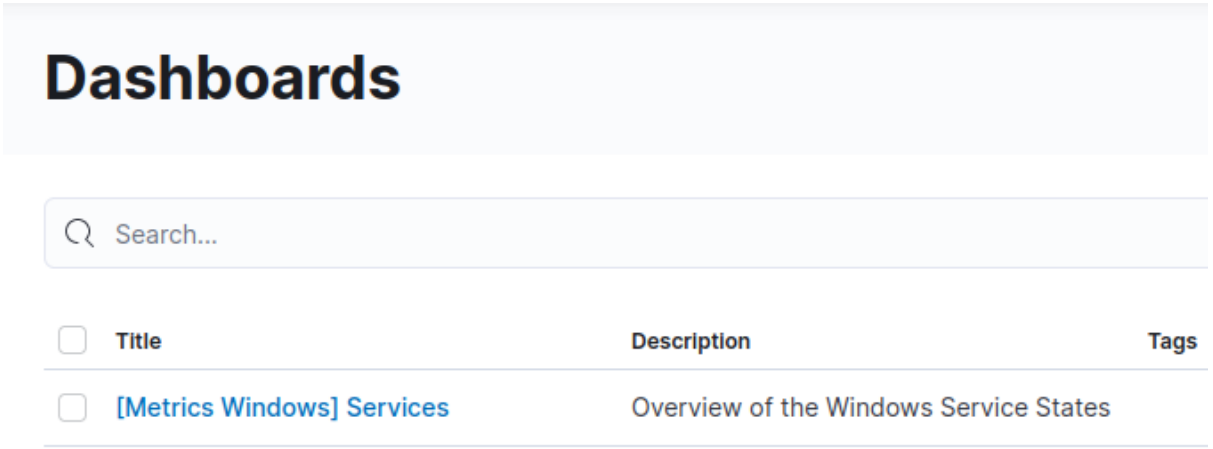




Guardamos y ahora ejecutamos una terminal en Windows con permiso de administrador. Copiamos la ruta donde está el archivo **elastic-agent.yml** y entramos en la ruta mediante terminal. Listamos el directorio, y ejecutamos **elastic-agent.exe**.



Ahora nos vamos a nuestro **Elastic** y abrimos **Dashboards**. Dentro se encuentra **[Metrics Windows] Services**. Pinchamos y lo abrimos para ver las gráficas.



Pero en mi caso hay un fallo que no he conseguido solucionar y no me muestra las gráficas y estadísticas.