Blue Team

Fray José Ávila Hernández

Índice

1.Creación PFSENSE y Kali Linux

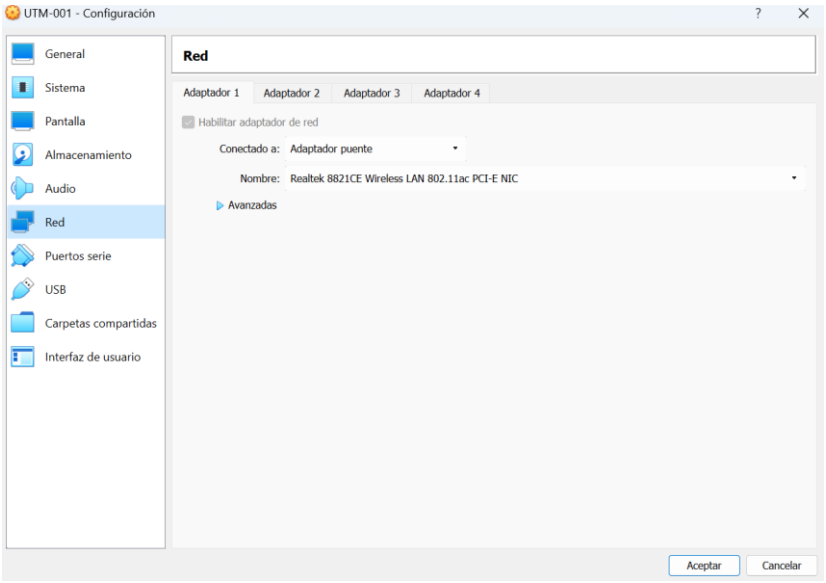
Lo primero que vamos a hacer es crear las redes LAN y DMZ como red interna a través del PFSENSE.

Para ello vamos a levantar dos máquinas virtuales una será UTM que es donde estará montado el PFSENSE y otra será un Kali Linux que estarán conectadas a nuestro ordenador Windows 11 a través de la red WAN.

1.1 Máquina Virtual PFSENSE

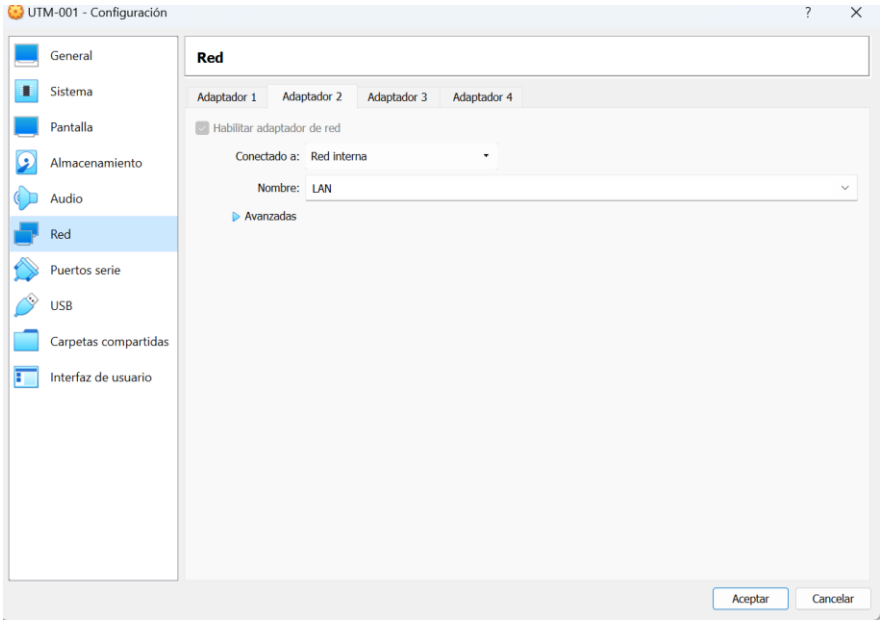
Una vez montado el PFSENSE creamos tres adaptadores red que es como si fuesen switches.

Adaptador 1 (adaptador puente).

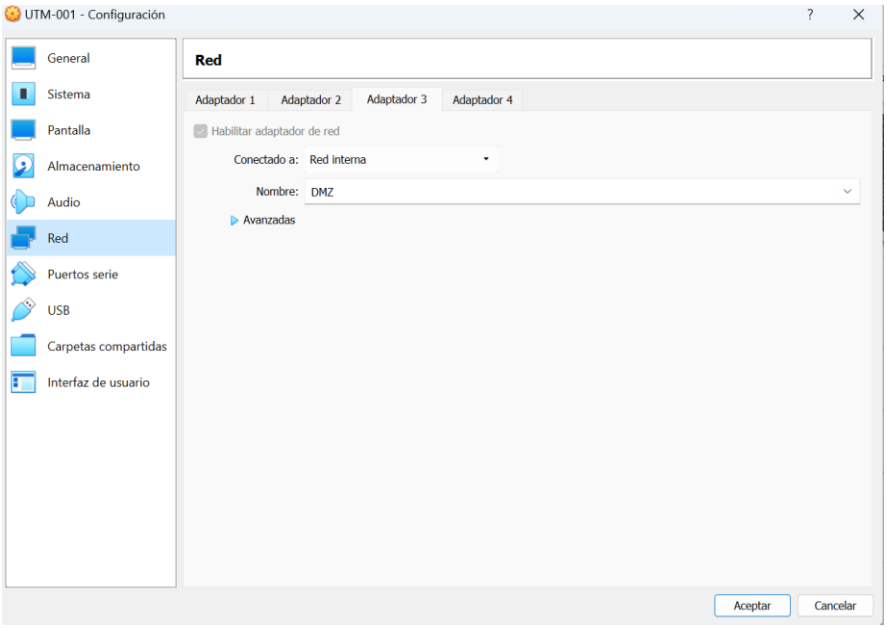


Este primero es el adaptador puente que lo que hace es conectar la máquina virtual a nuestra red.

Adaptador 2 (LAN).

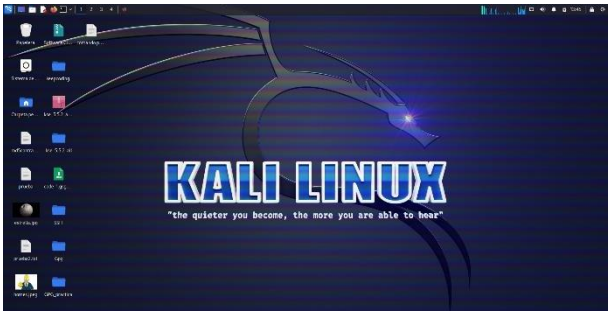


Adaptador 3 (DMZ).

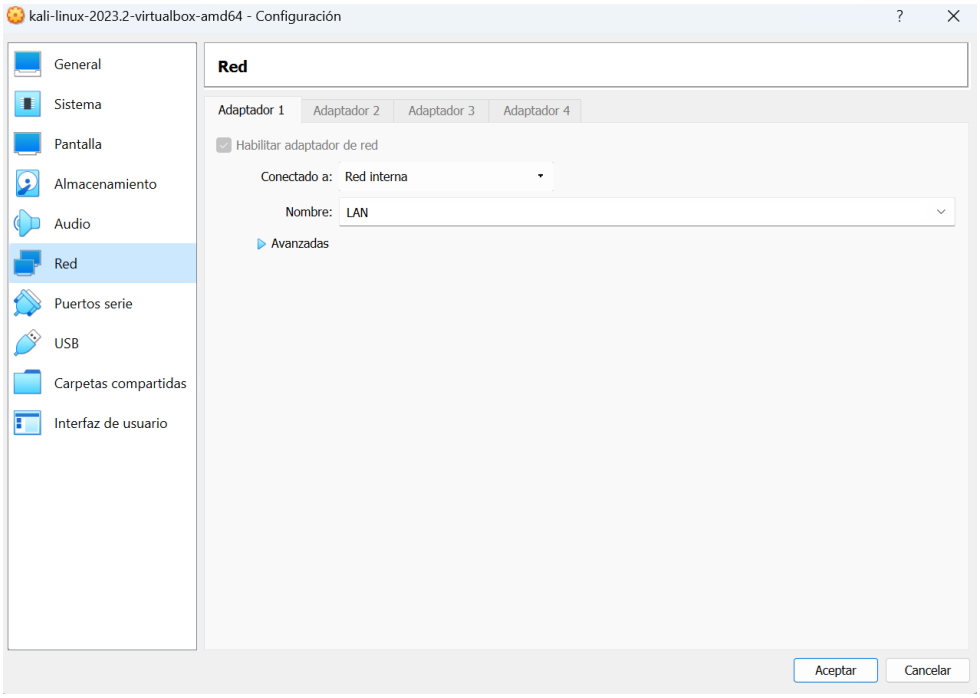


Estos dos adaptadores lo que hacen es crearnos unos switches internos.

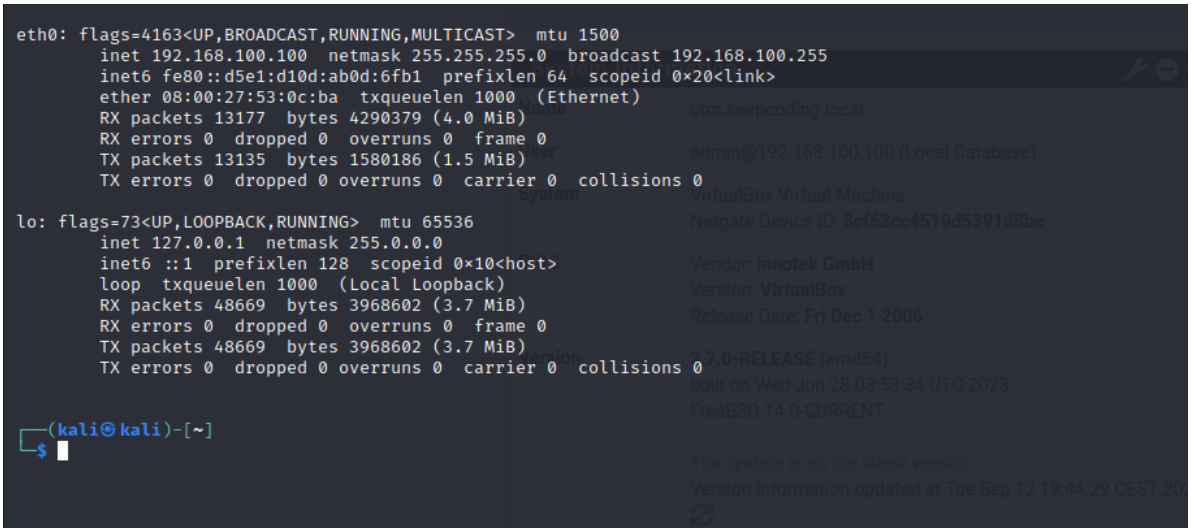
1.2 Máquina Virtual Kali Linux



Una vez levantado Kali Linux tenemos que ir a configuración red y conectar la maquina a la red interna LAN para que pueda estar conectado al servidor que hemos montado que es el PFSENSE.

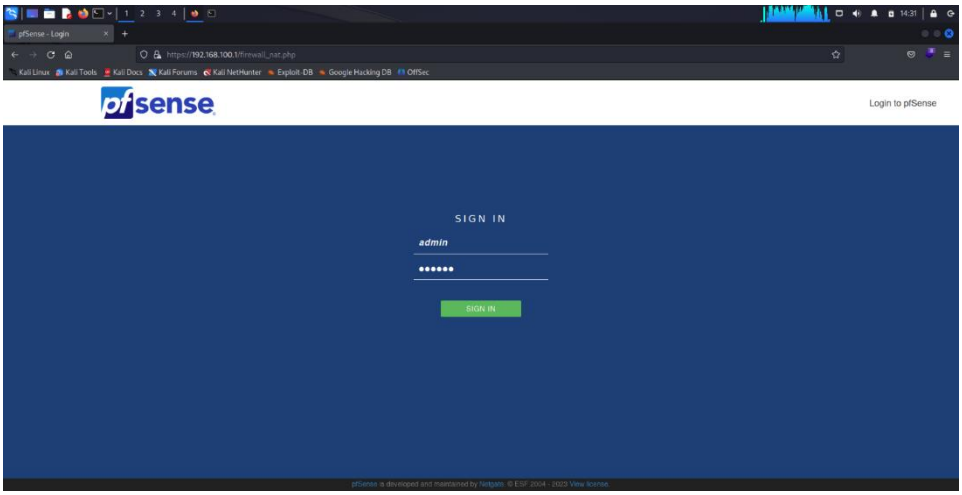


Una vez abrimos la consola de Kali y ponemos el comando ifconfig podemos ver que la IP que nos ha dado es: 192.168.100.

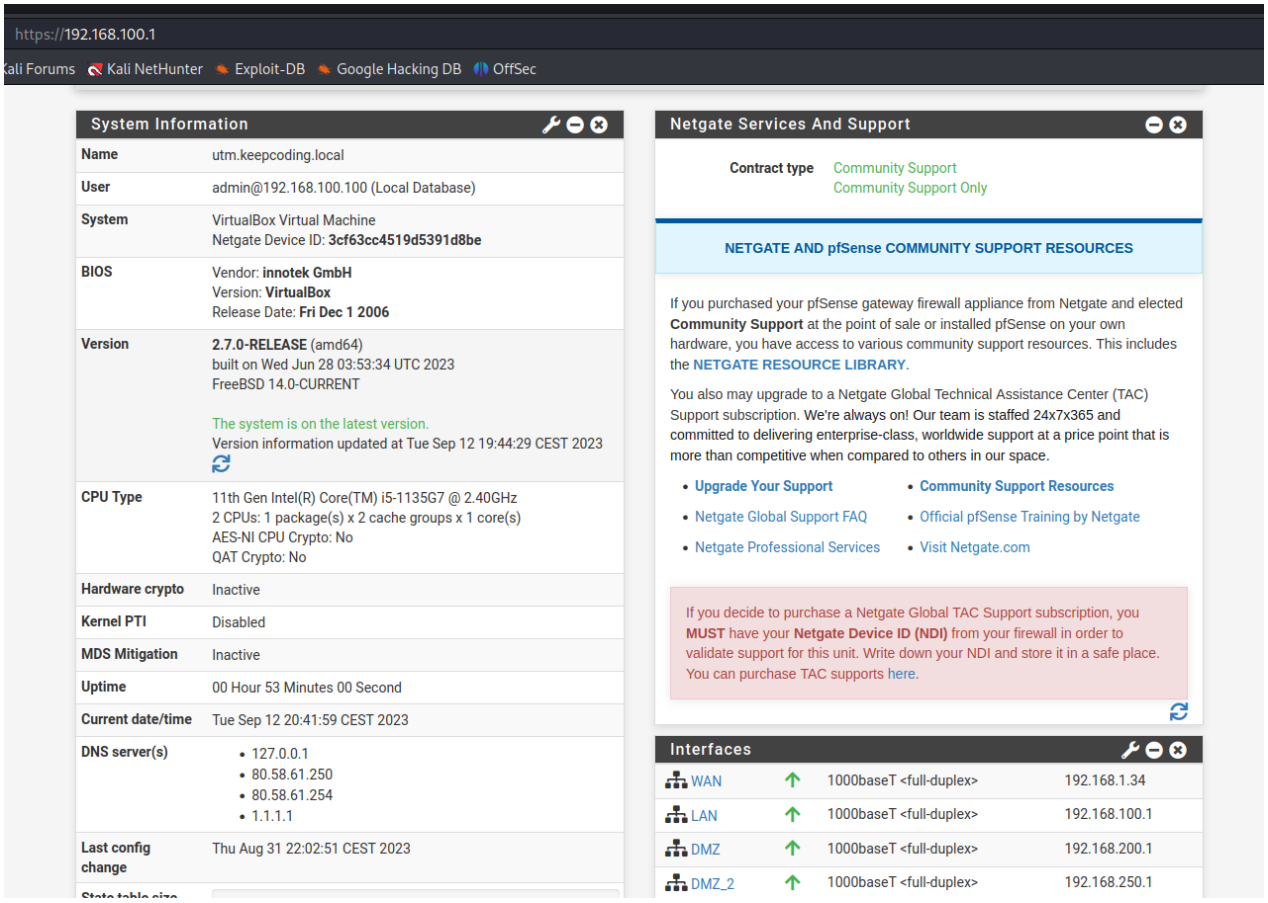


Ahora que sabemos la IP ponemos en nuestro navegador 192.168.100.1 para entrar al PFSENSE y configurarlo.

2.Configuración de Redes a través del PFSENSE



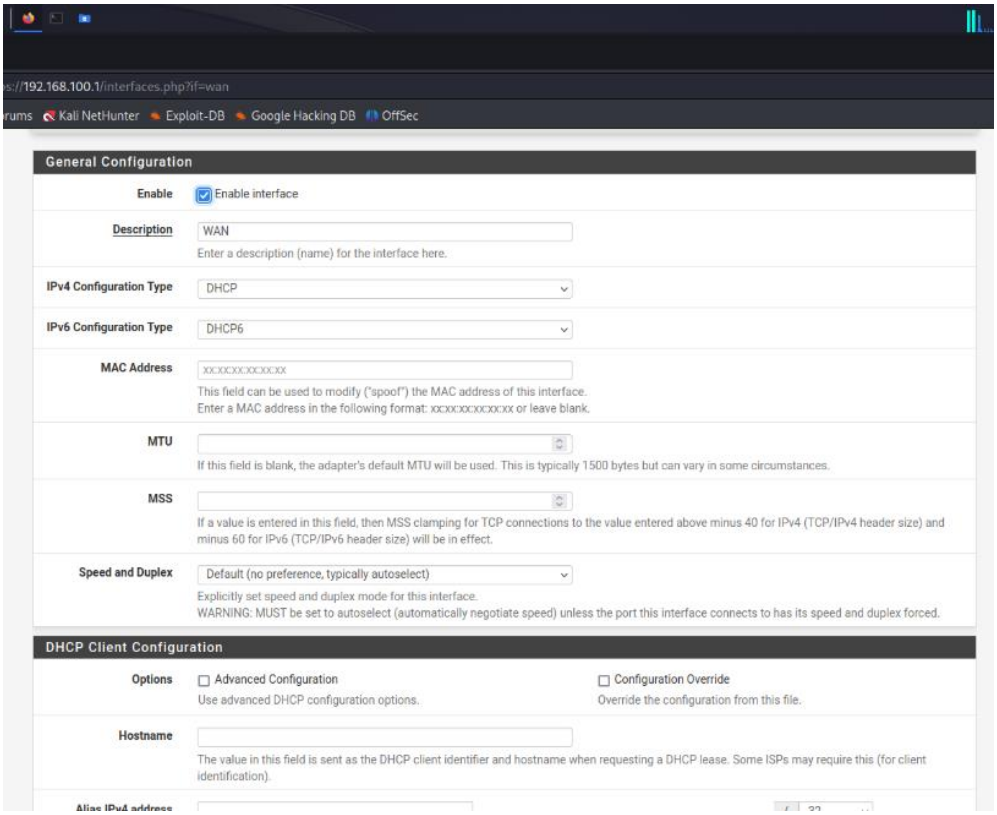
Después de crear el usuario y contraseña nos pondremos a configurar el PFSENSE



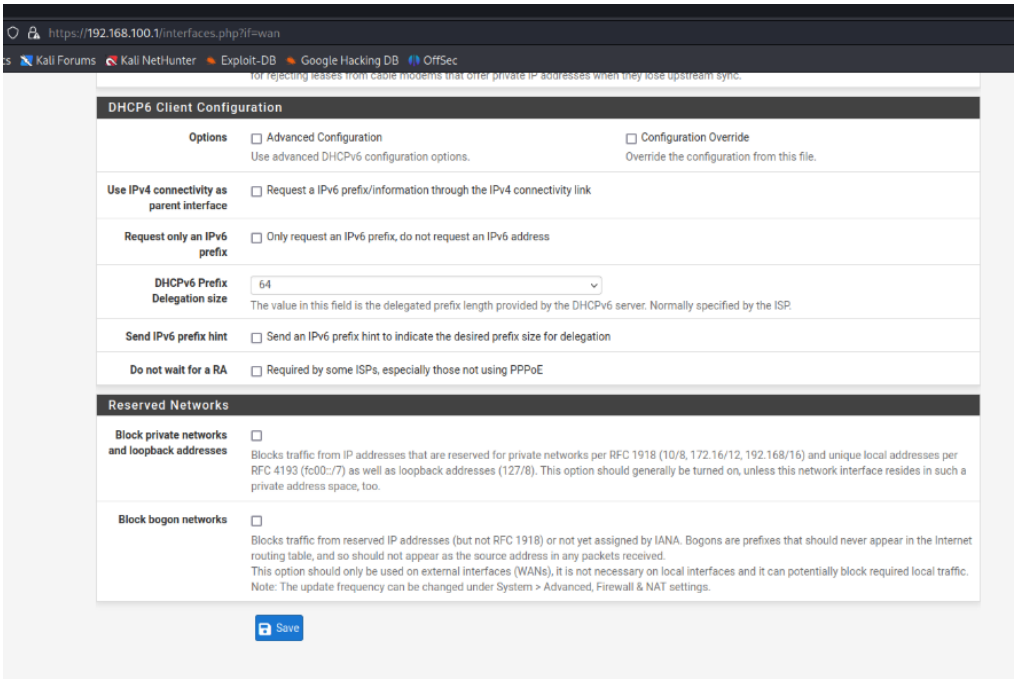
Aquí lo importante es poner en el DNS principal la IP 127.0.0.1 que es la que pertenece al propio PFSENSE y es la que va a resolver.

Como IP secundaria pondremos 1.1.1.1.

2.1 Configuración Red WAN

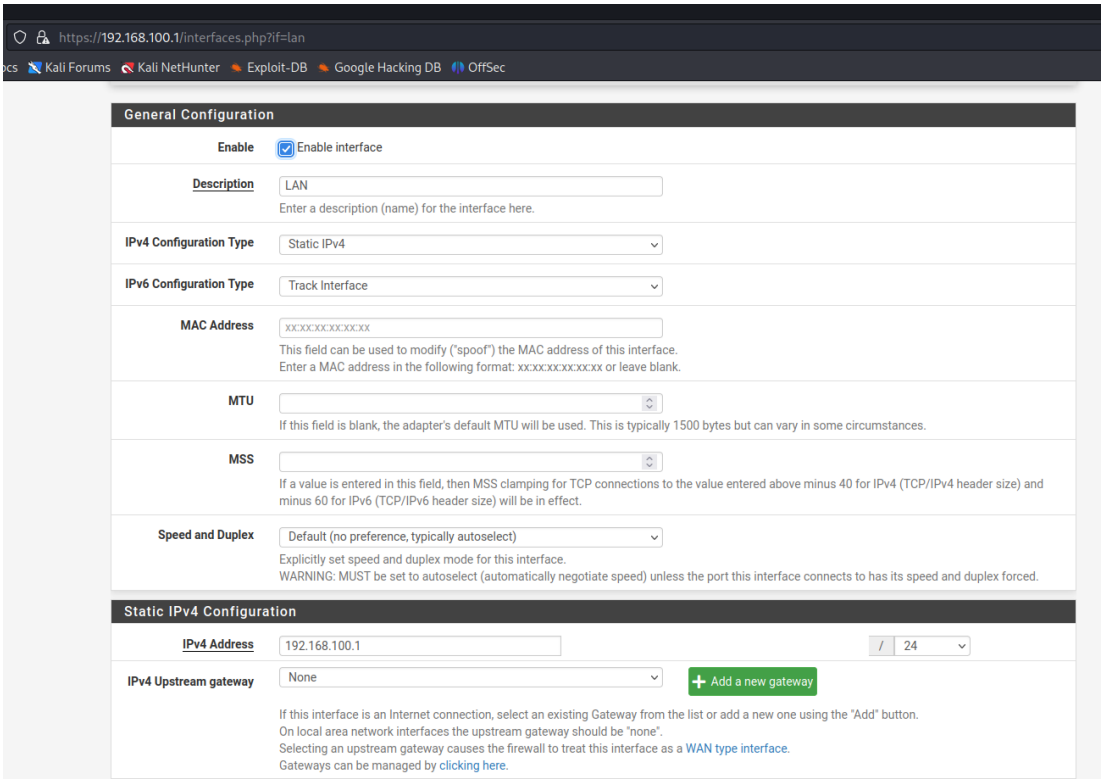


Una vez pasamos a la configuración interfaz WAN tendremos que dejar el tipo DHCP que es el que nos da acceso a nuestra red interna.



Tendremos que desbloquear las conexiones privadas y los bogon.

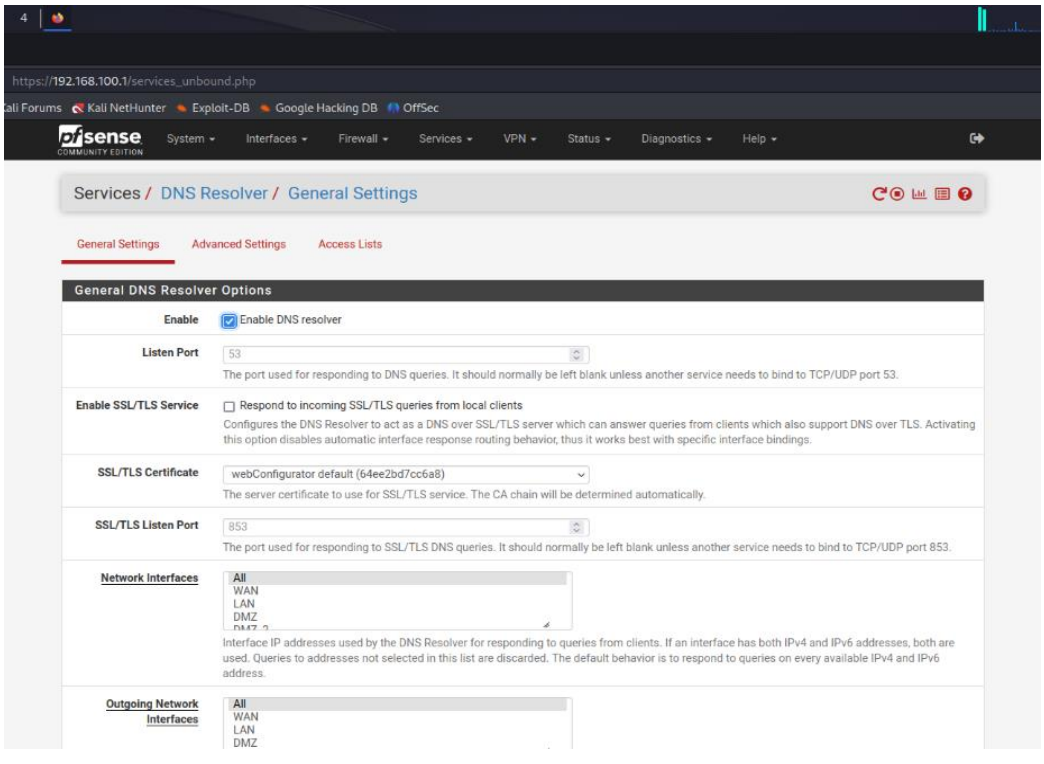
2.2 Configuración Red LAN



Aquí modificamos la dirección IP 192.168.100.1 para que no coincida con alguna IP de nuestra casa.

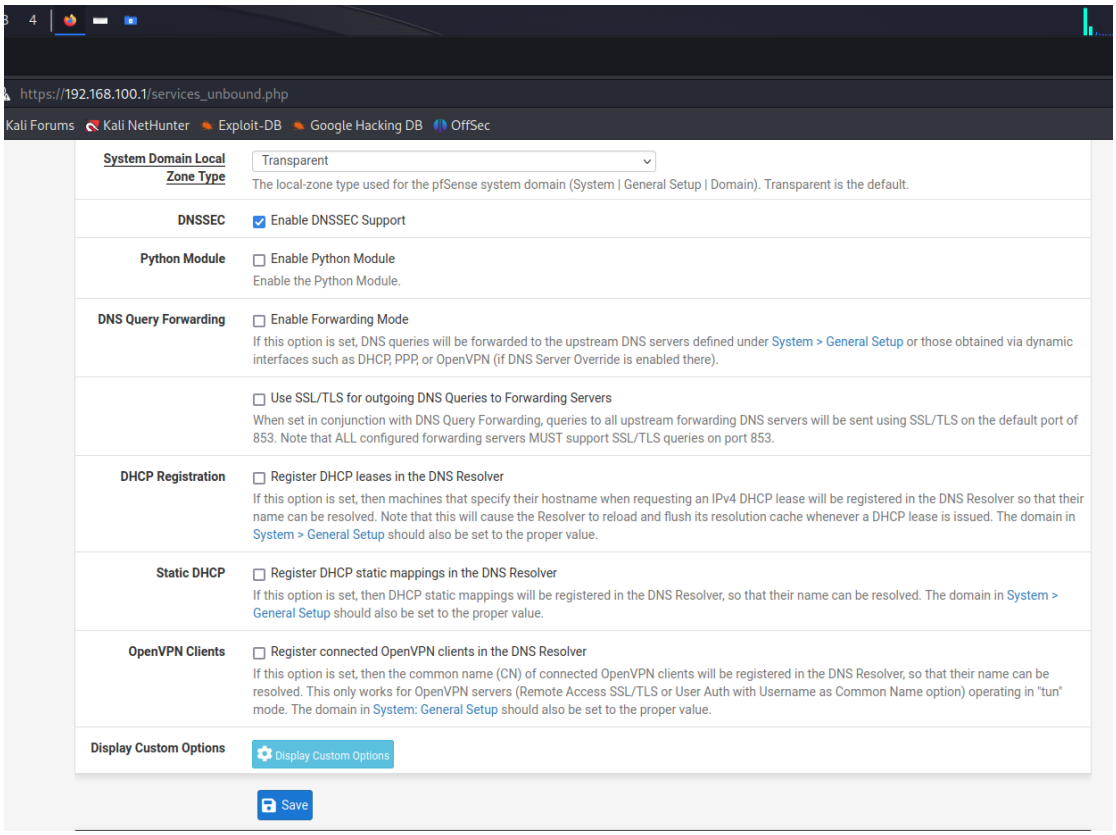
2.3 Configuración servidores DNS.

El siguiente paso una vez configurada la Red LAN y la WAN, vamos a configurar los servidores DNS, para habilitar que nuestro PFSENSE sea un servidor DNS interno de nuestra infraestructura.



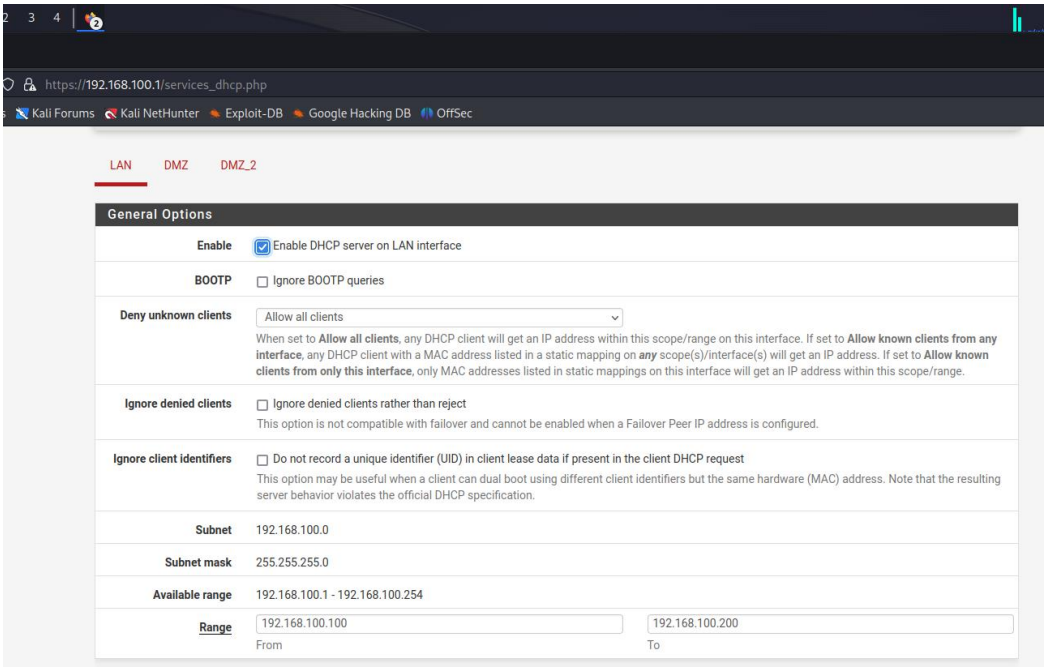
Para ello entramos en la pestaña DNS Resolver, vemos que en los ajustes generales el DNS está habilitado, el puerto que está escuchando es el 53. Tiene que estar habilitado el Network interfaces y el Outgoing Network interfaces.

Por último, comprobamos el DNSSEC esté habilitado y guardamos.

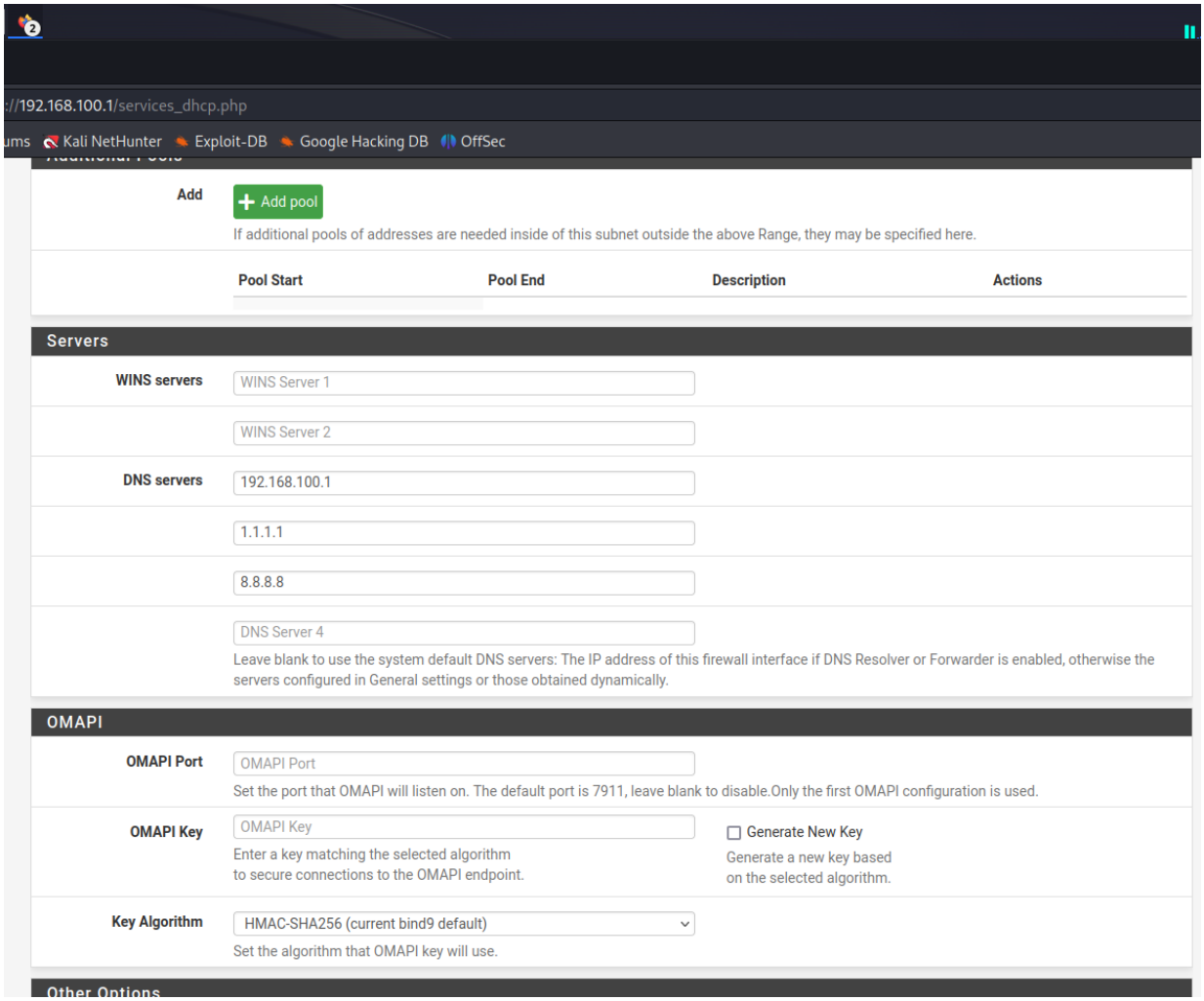


2.4 Configuración DHCP Server

LAN



Entramos en DHCP Server y la primera red que configuramos es la LAN, vemos que esta habilitada, comprobamos que la IP es la 192.168.100. que es la que hemos modificado anteriormente. Si queremos podemos cambiar el rango en este caso lo hemos puesto desde la 100 hasta la 200.

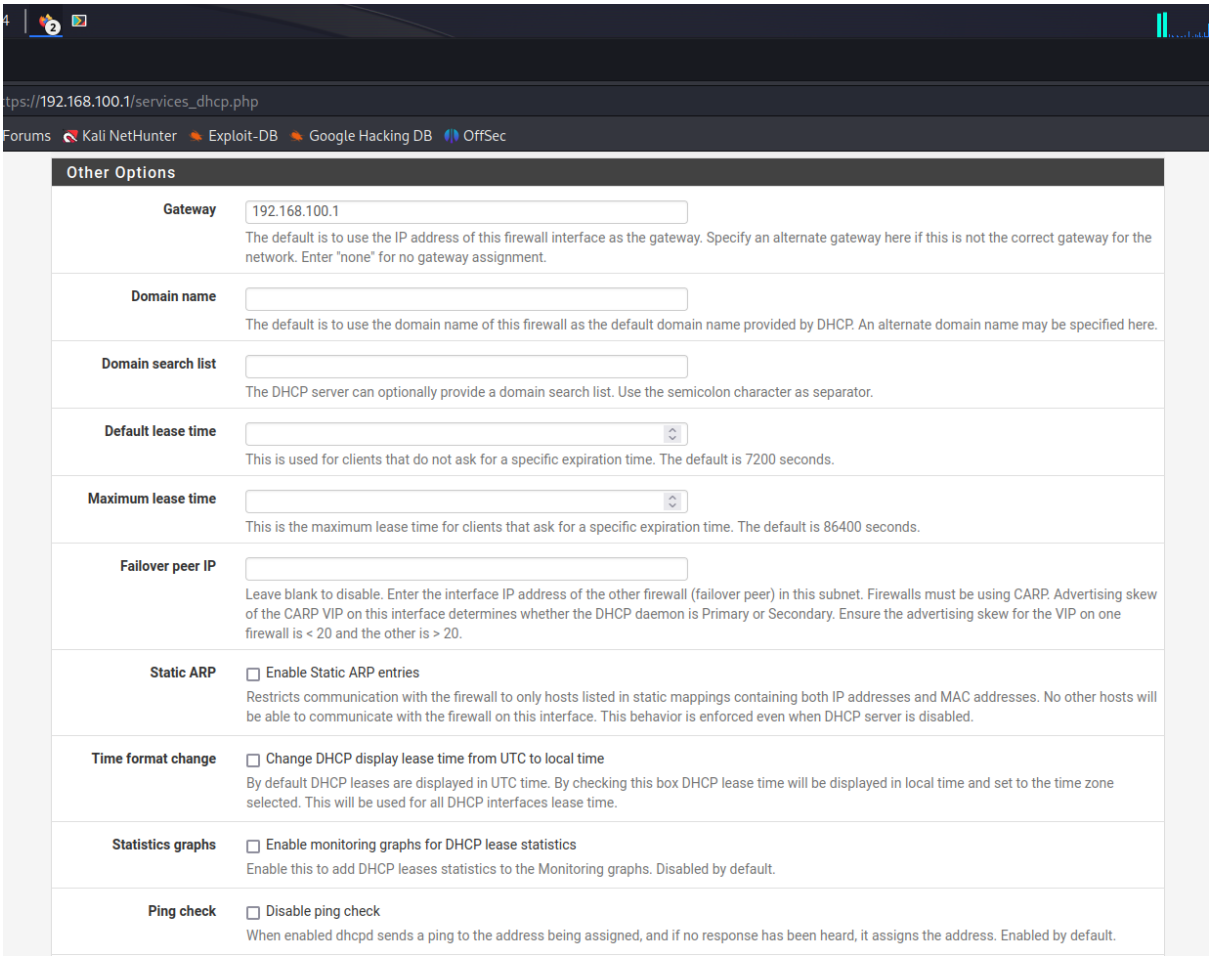


El siguiente paso que haremos es añadir diferentes de servidores DNS.

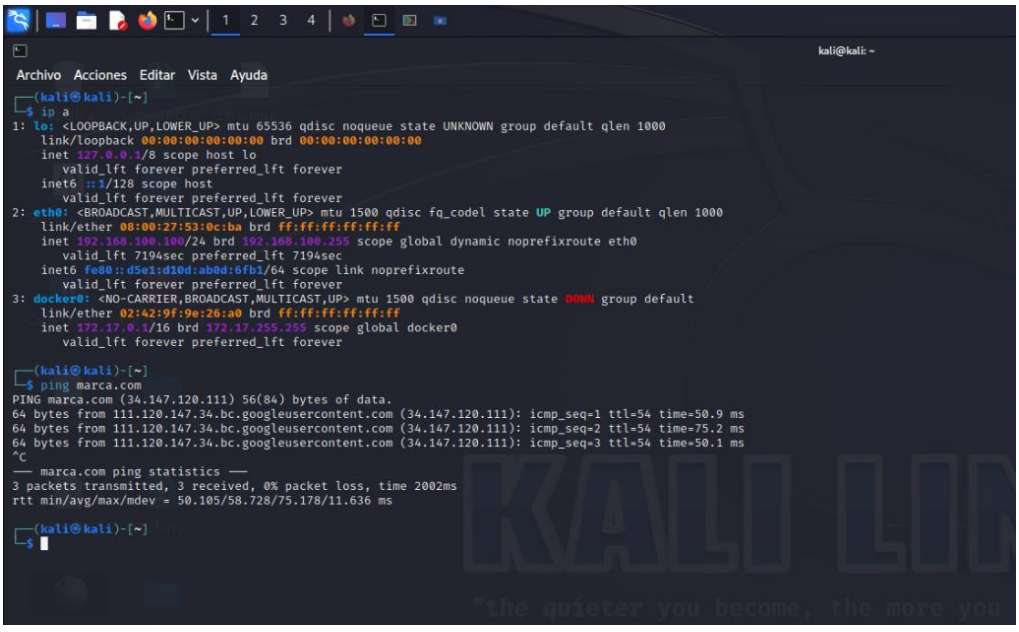
El primero será 192.168.100.1 (Local)

El segundo será 1.1.1.1 (Cloudflare)

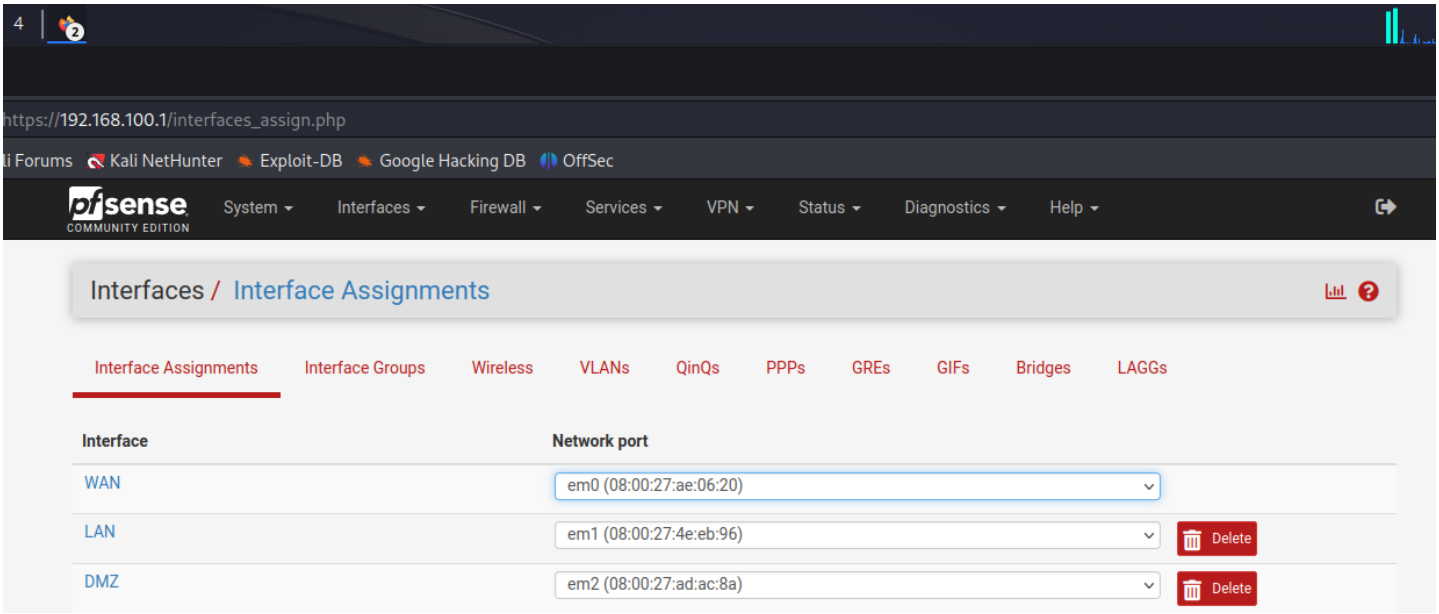
El tercero será 8.8.8.8 (Google)



El último paso que haremos para terminar la configuración será añadir en la puerta de enlace la IP 192.168.100.1 que esto nos va a dar por donde se va a conectar el equipo a internet en este caso PFSENSE.

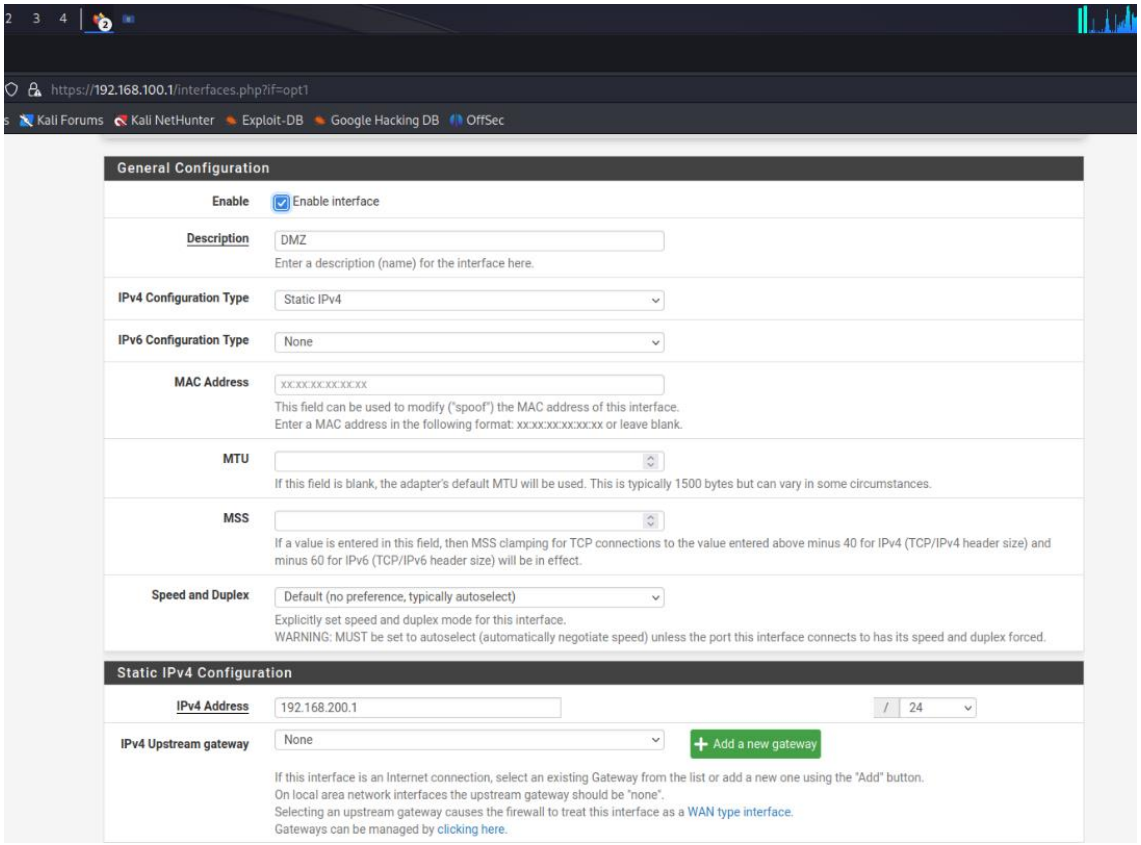


Comprobamos la conexión IP en la máquina y probamos que tengamos internet.



El siguiente paso es irnos asignación de interfaz y añadimos una red nueva que en este caso será DMZ y la personalizaremos.

DMZ



Lo primero que haremos es habilitar la interfaz y en la descripción la nombraremos como DMZ que es el nombre de nuestra red.

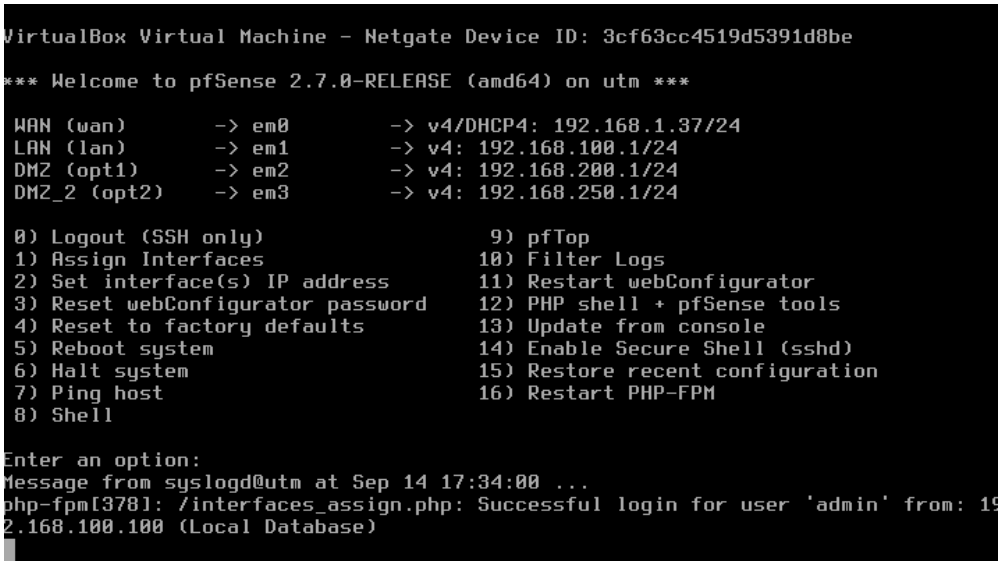
El siguiente paso será seleccionar en el tipo de configuración IPv4 el Static IPv4 ya que en VirtualBox no hay DHCP

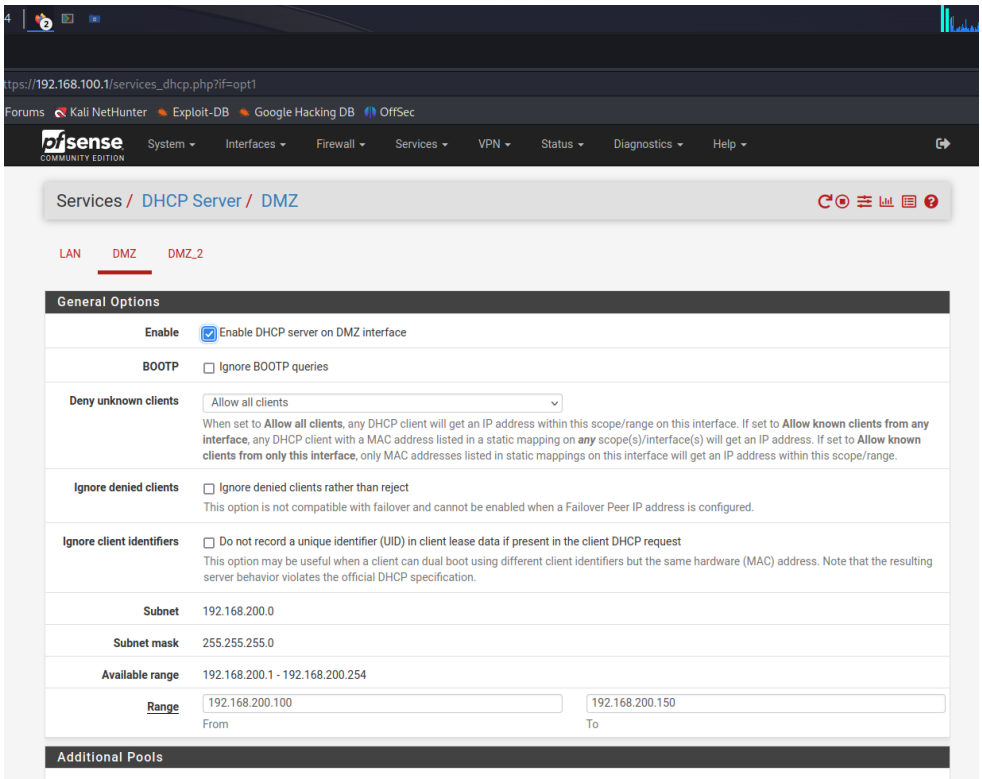
La IP que añadiremos en este caso será 192.168.200.1 e importante la IP será /24.

Y por último ya guardamos

Una vez creada esta red nos vamos al PFSENSES y vemos como ya están creadas todas las redes.

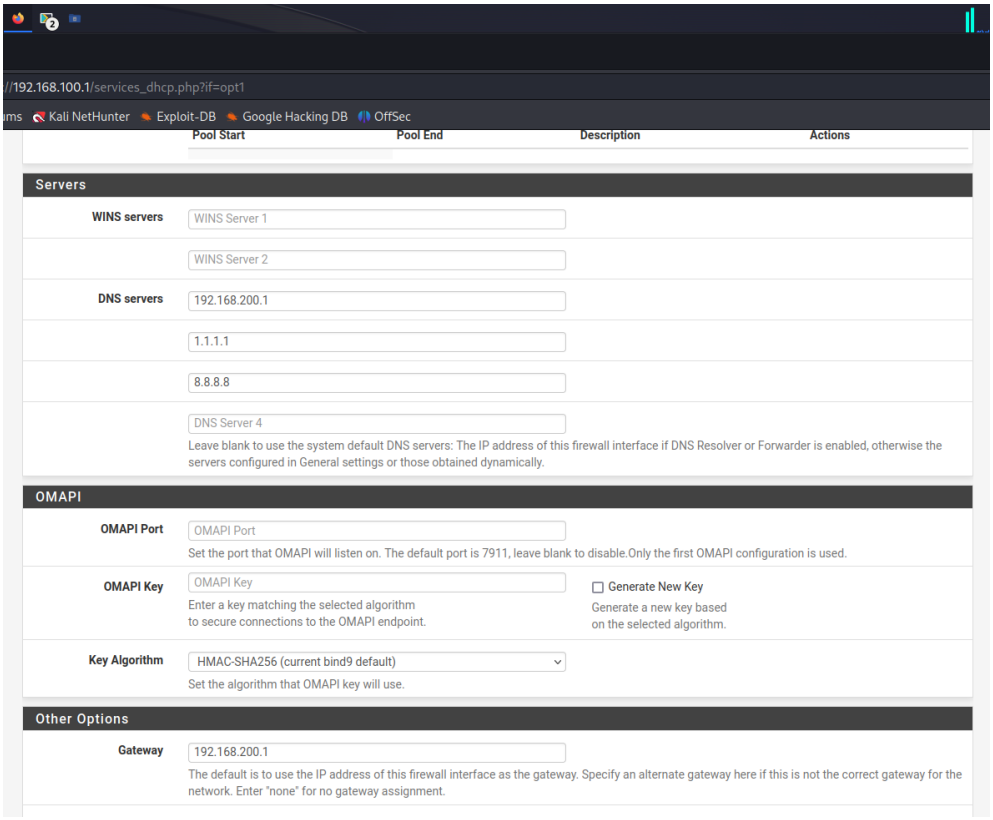
Podemos observar que tenemos 3 interfaces WAN, LAN y DMZ.





Lo siguiente que tenemos que hacer es irnos a DHCP Server para habilitar el DHCP en la red DMZ.

El rango lo pondremos de 100 a 150.



Ahora añadiremos los servidores DNS:

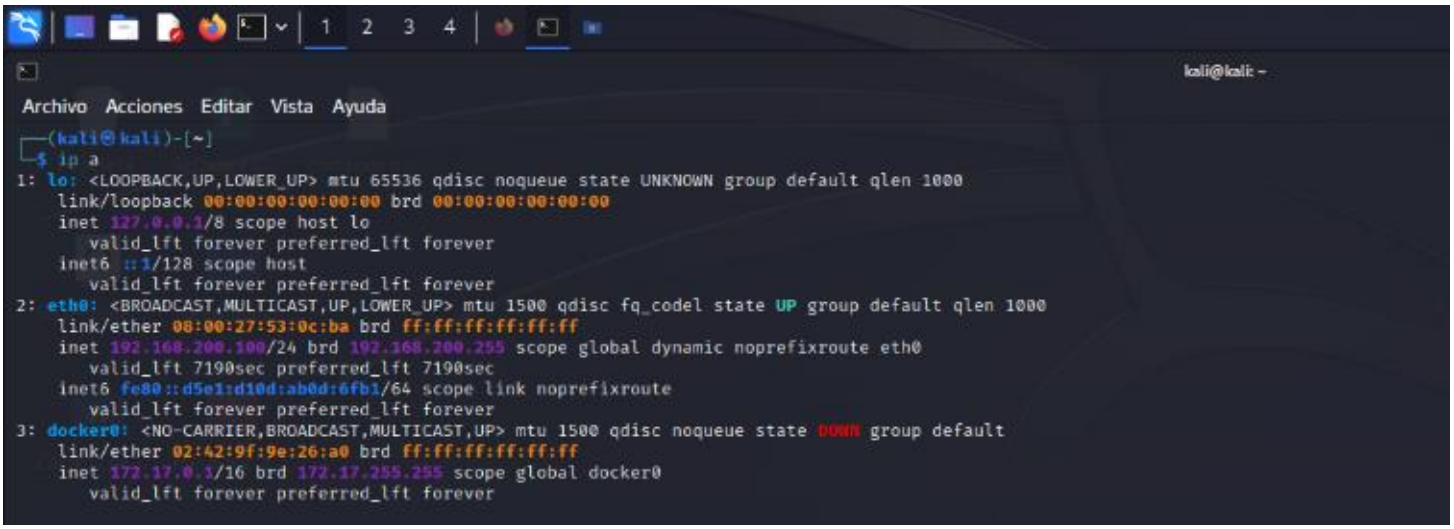
El primero será 192.168.200.1 (Local)

El segundo será 1.1.1.1 (Cloudflare)

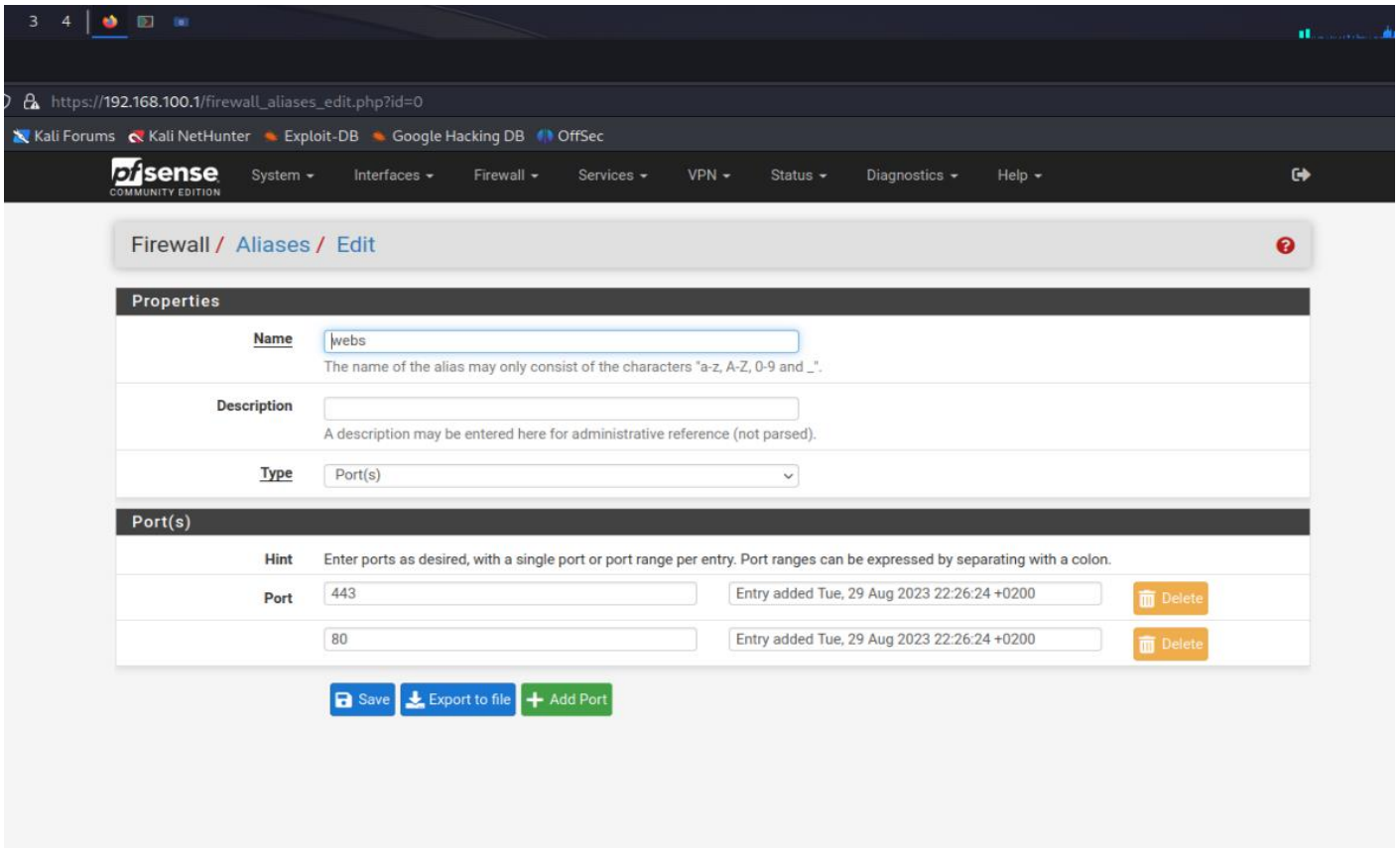
El tercero será 8.8.8.8 (Google)

La puerta de enlace para poder tener internet será la IP 192.168.200.1 (PFSESENSE)

Y por último guardamos.



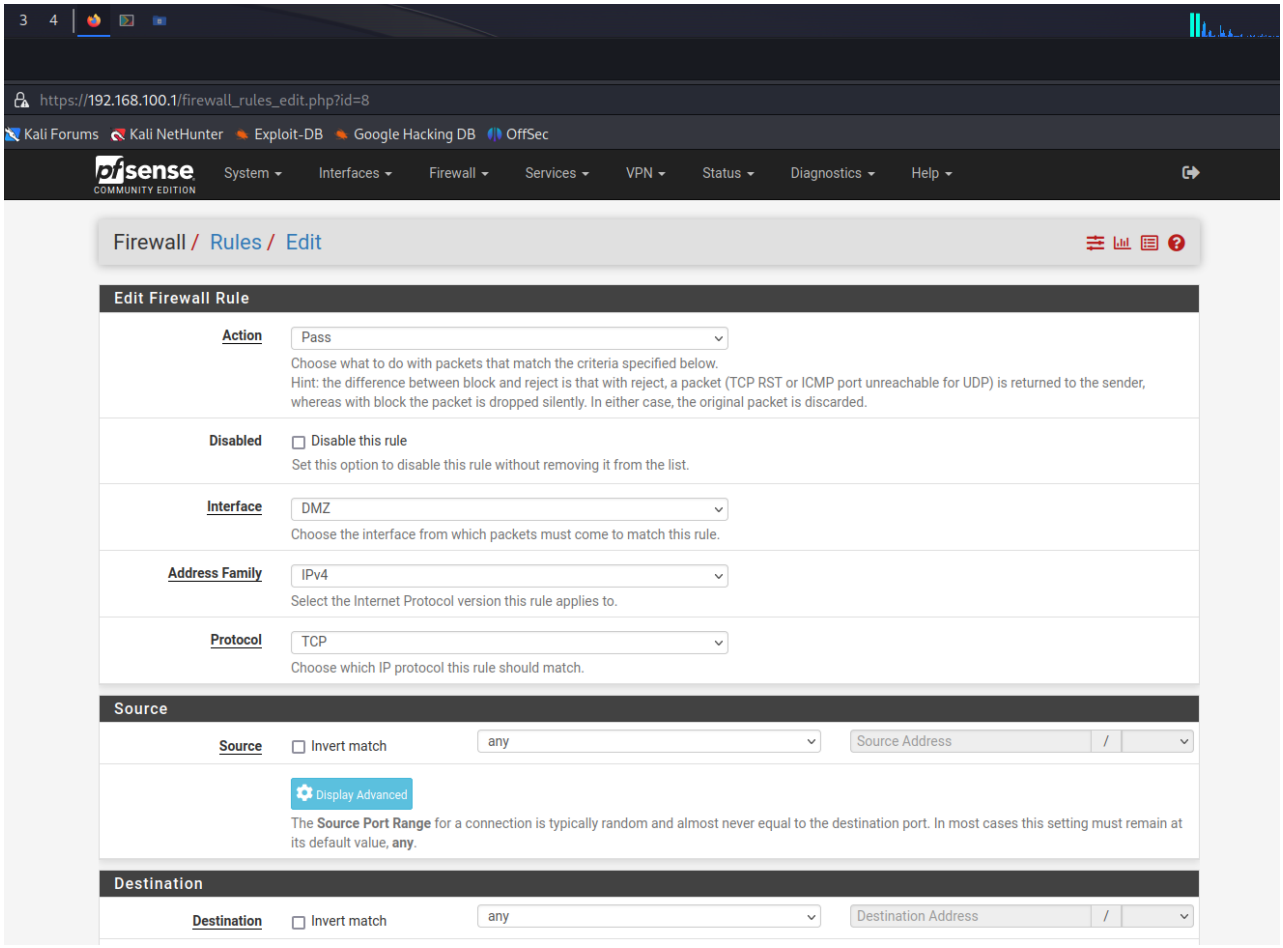
Comprobamos la conexión IP en la máquina.



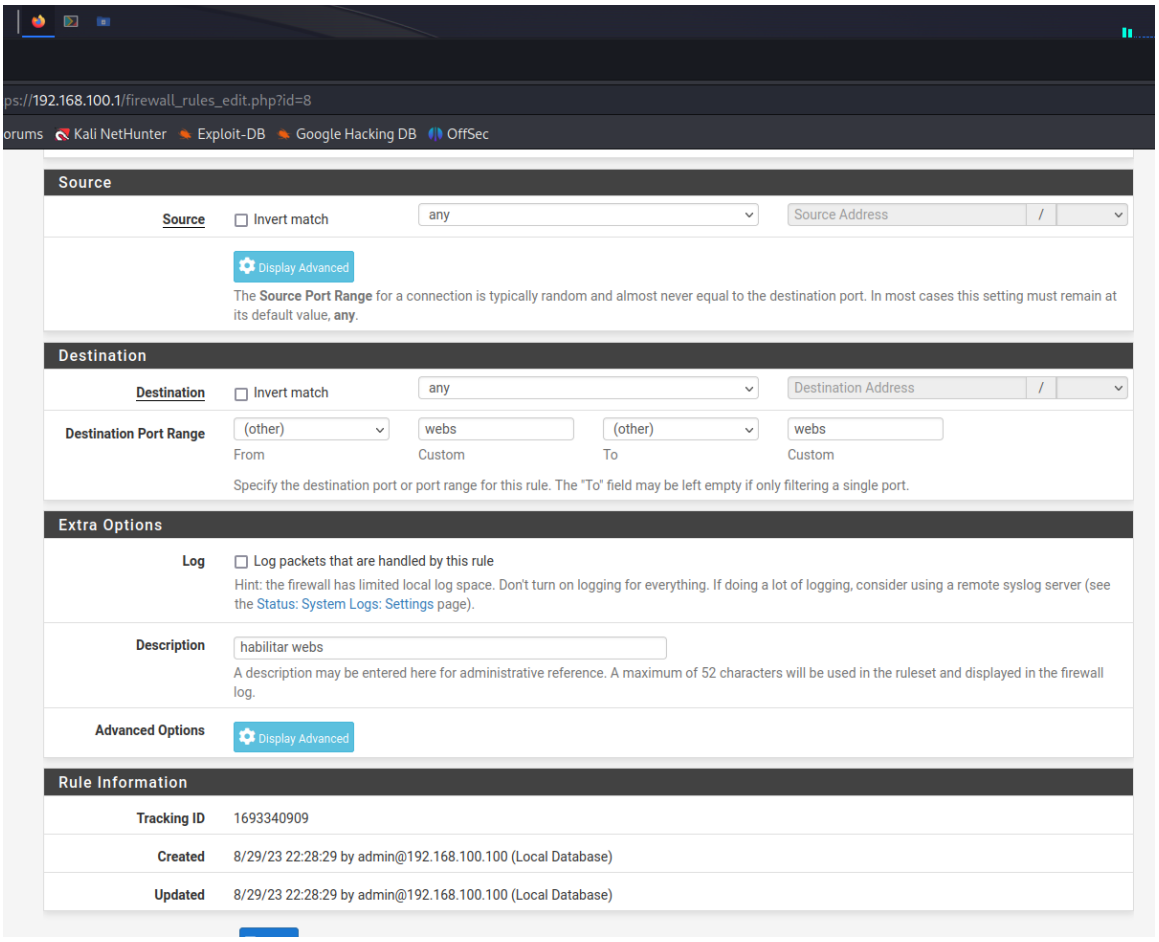
Ahora una vez configurada la RED DMZ debemos crear una serie de reglas para poder tener acceso a internet.

El primer paso que tenemos que hacer es crear un alias de puerto.

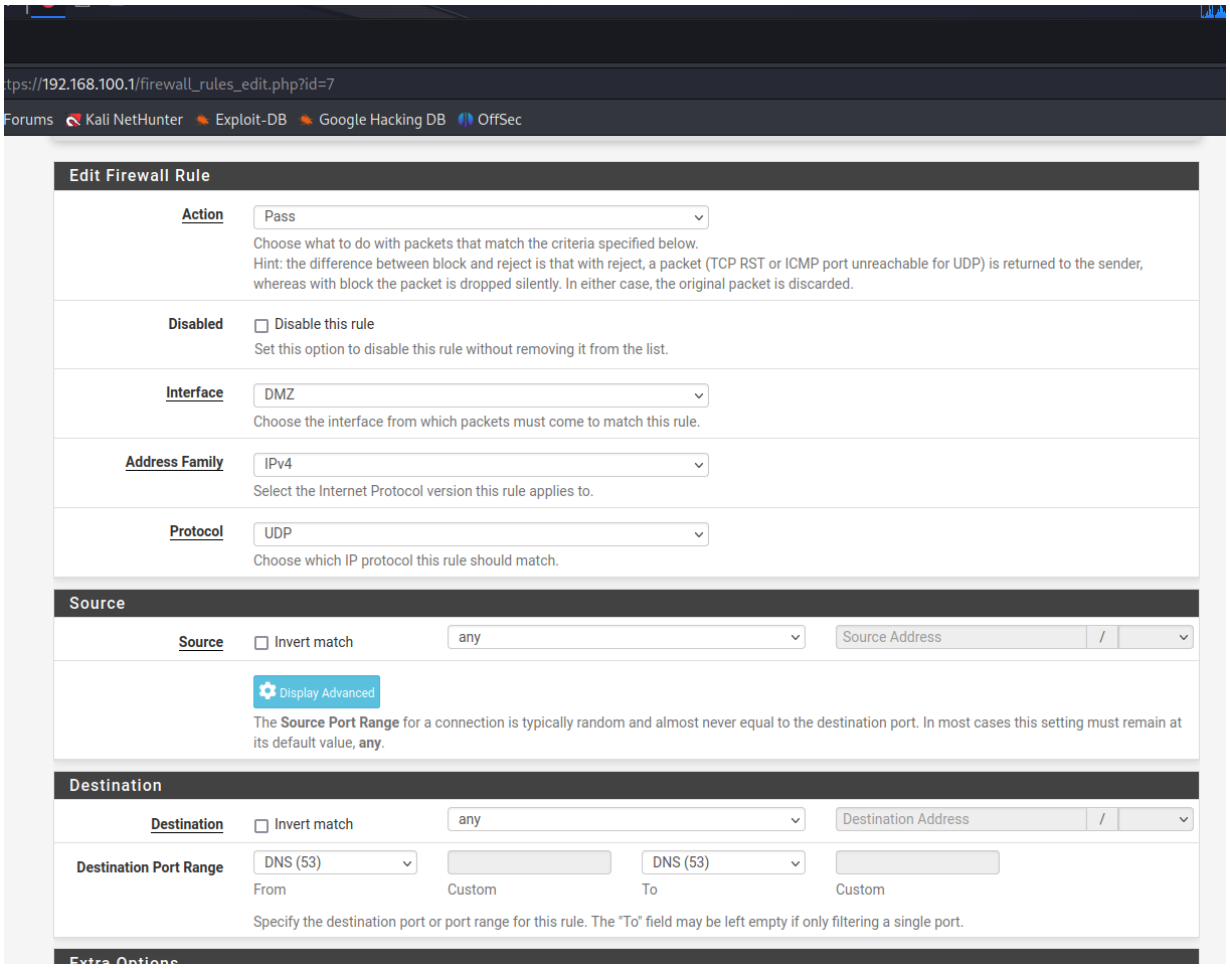
En este caso lo hemos definido como webs y hemos añadido los puertos 443 y 80 que son los que nos dan acceso a internet.



Vamos a crear la primera regla, dejaremos pasar el tráfico y el protocolo será TCP que es el que es orientando a la conexión. El origen y el destino de cualquier sitio.



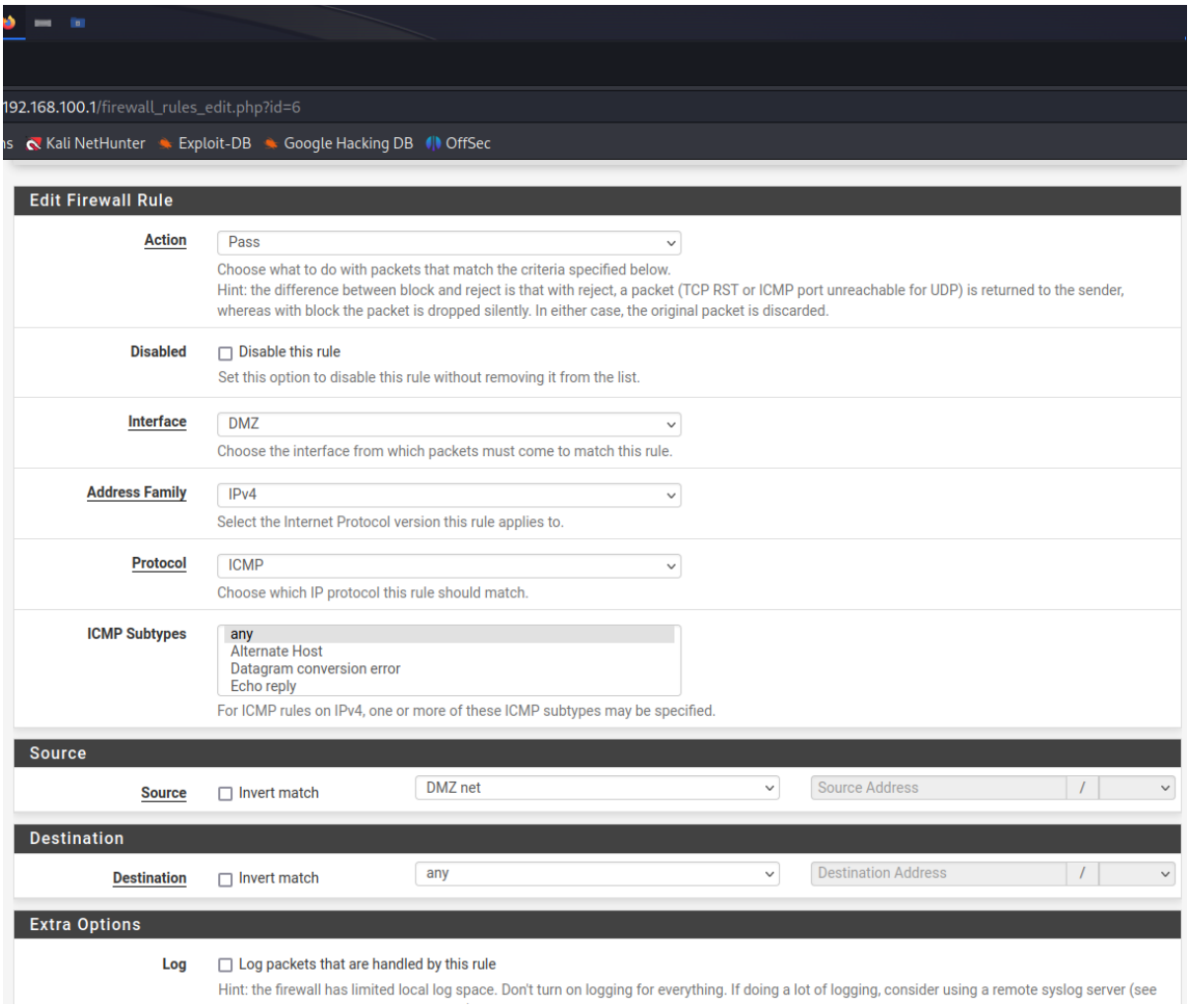
Aquí importante el destino de los puertos que es el que creamos anteriormente y definimos como webs (443 y 80) y guardamos.



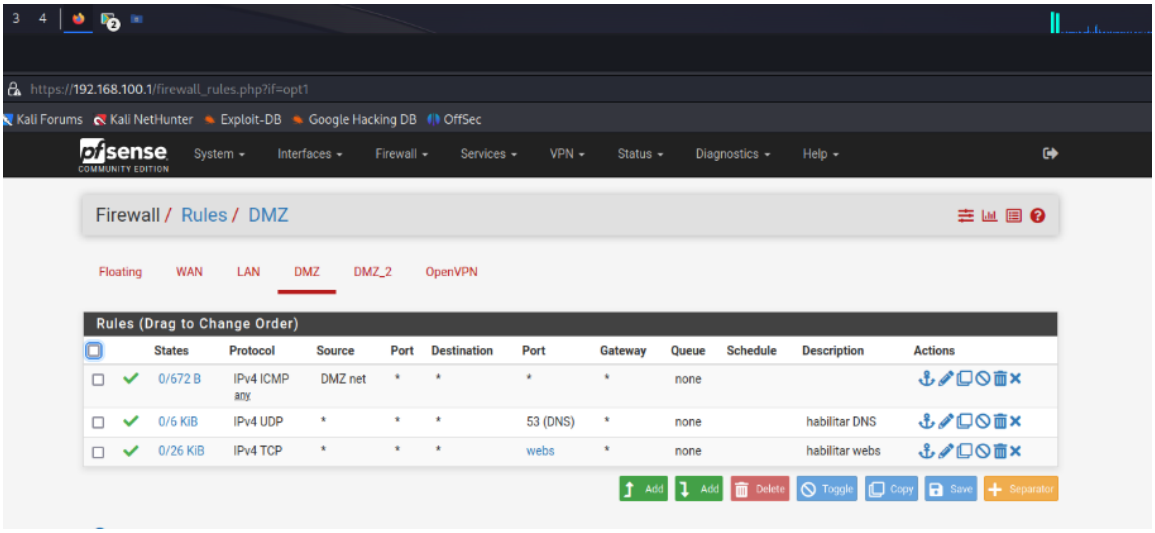
La siguiente regla que debemos crear es para el DNS.

Como en la anterior dejamos pasar el tráfico y el protocolo seleccionamos UDP que no está orientado a la conexión. El origen y el destino de cualquier lugar.

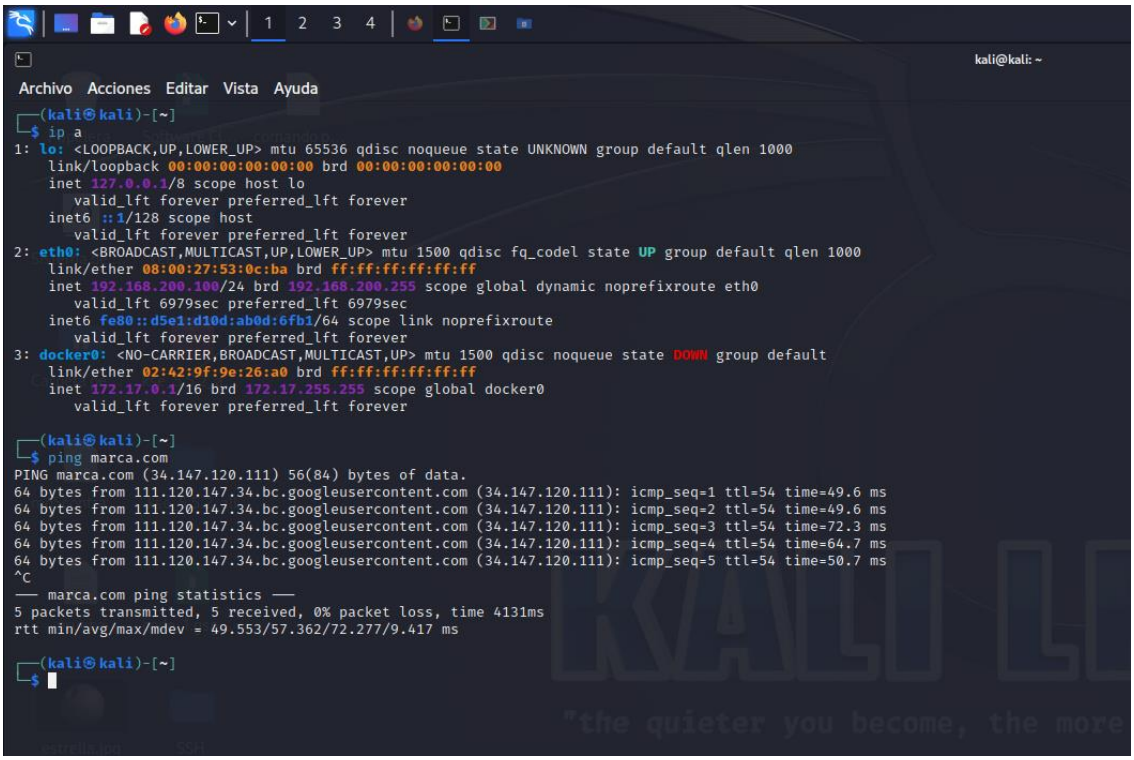
Y lo importante seleccionar el destino del puerto DNS (53) y guardamos.



La última regla que crearemos será con el protocolo ICMP el origen sería desde DMZ net y el destino cualquiera, guardamos y ya tendríamos las 3 reglas creadas que nos darían acceso a internet.



Aquí podemos observar las 3 reglas definidas.

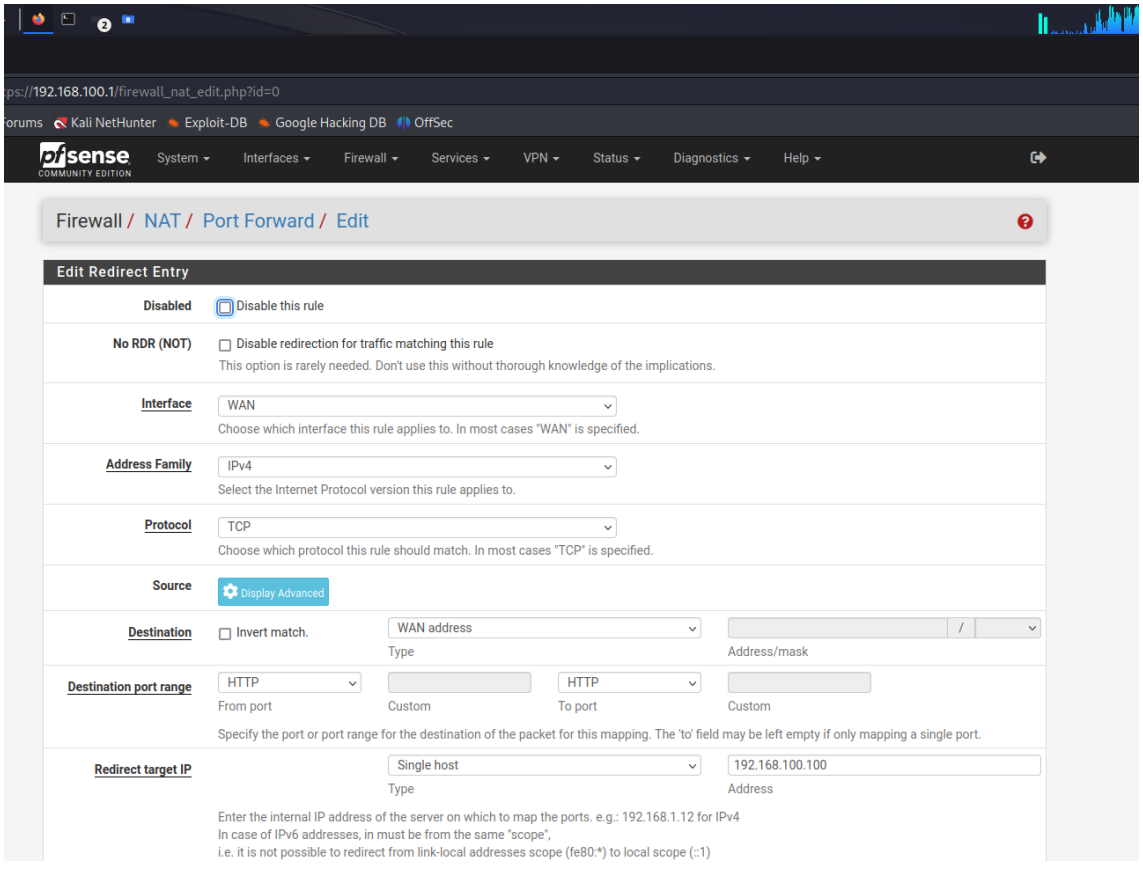


Hacemos la comprobación con PING y vemos que ya tenemos acceso a internet.

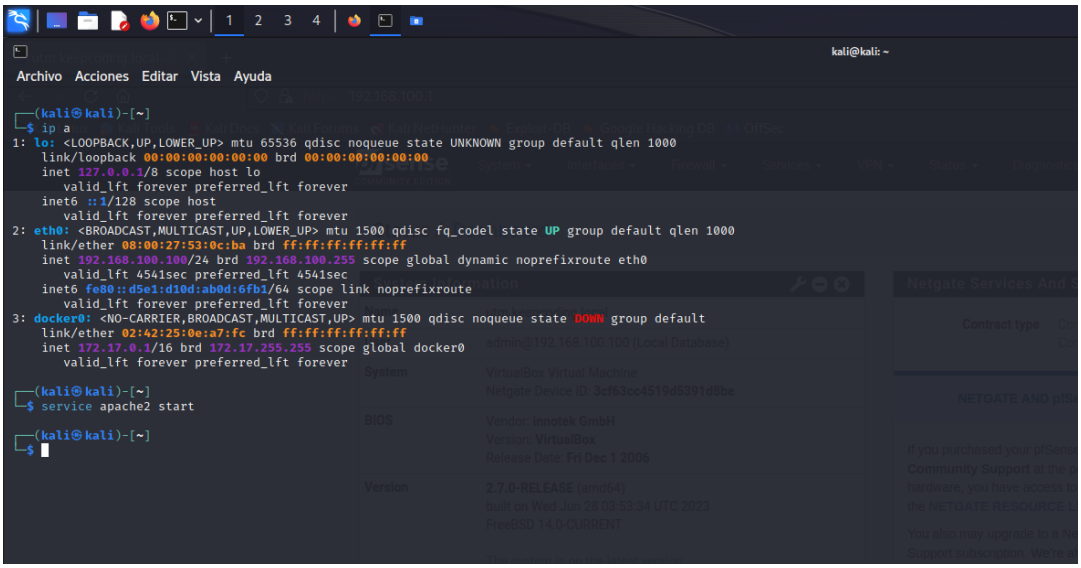
2.5 Configuración NAT/Port Forward

Vamos a configurar la NAT para poder servir una página web en internet, que es traducir una IP interna y hacer un reenvío de puerto. Con esta configuración podemos conectar la IP del PFSENSES con nuestro ordenador Windows.

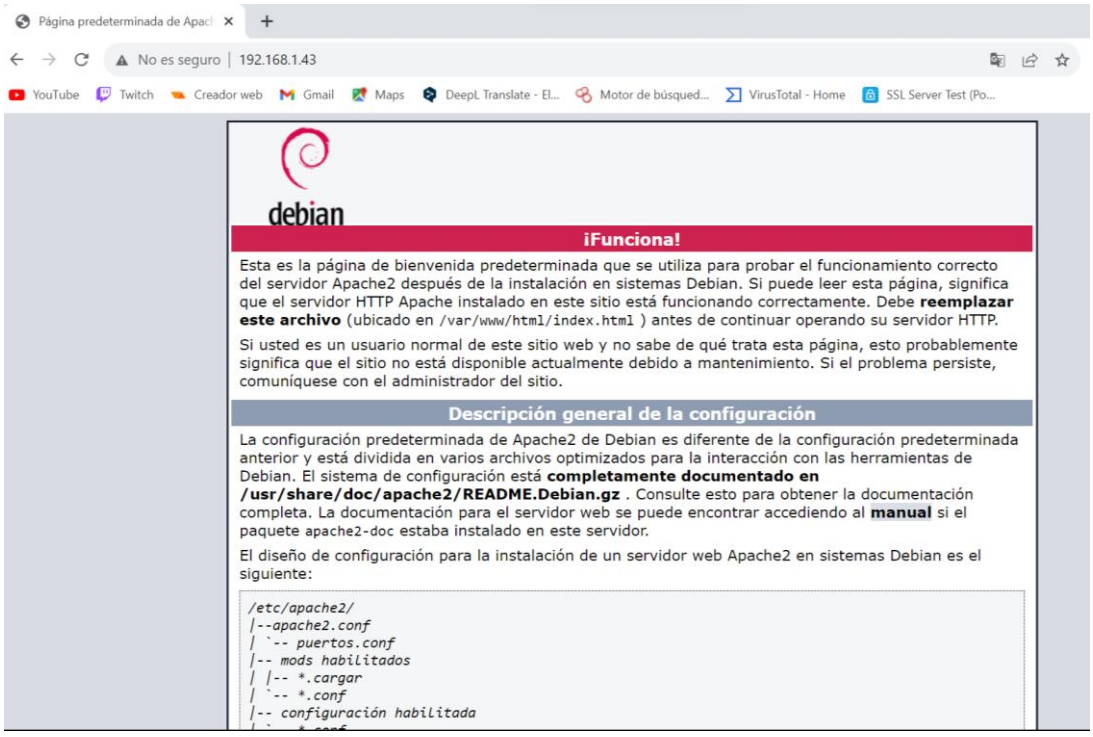
LAN



La interfaz por la que se va a acceder es por internet (WAN) y el protocolo que vamos a utilizar es TCP. El destino del puerto será HTTP (80) nos va a redirigir a la IP 192.168.100.100 (RED LAN) y guardamos.

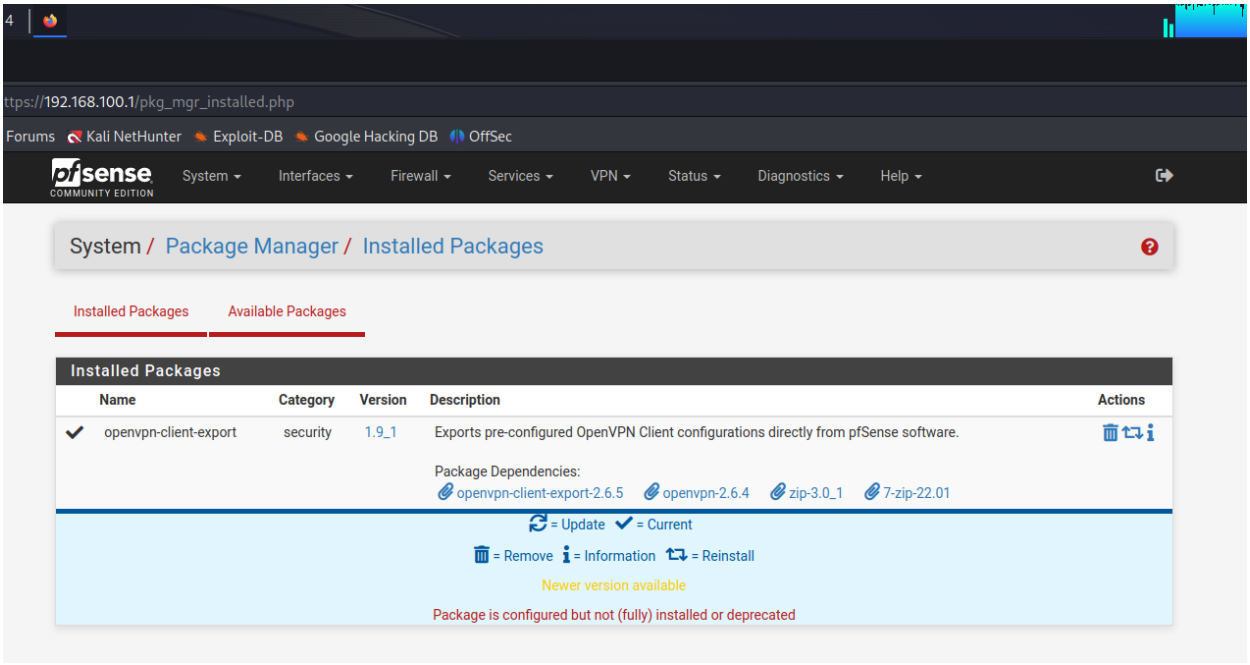


Para comprobar que funciona vamos a lanzar un apache2.

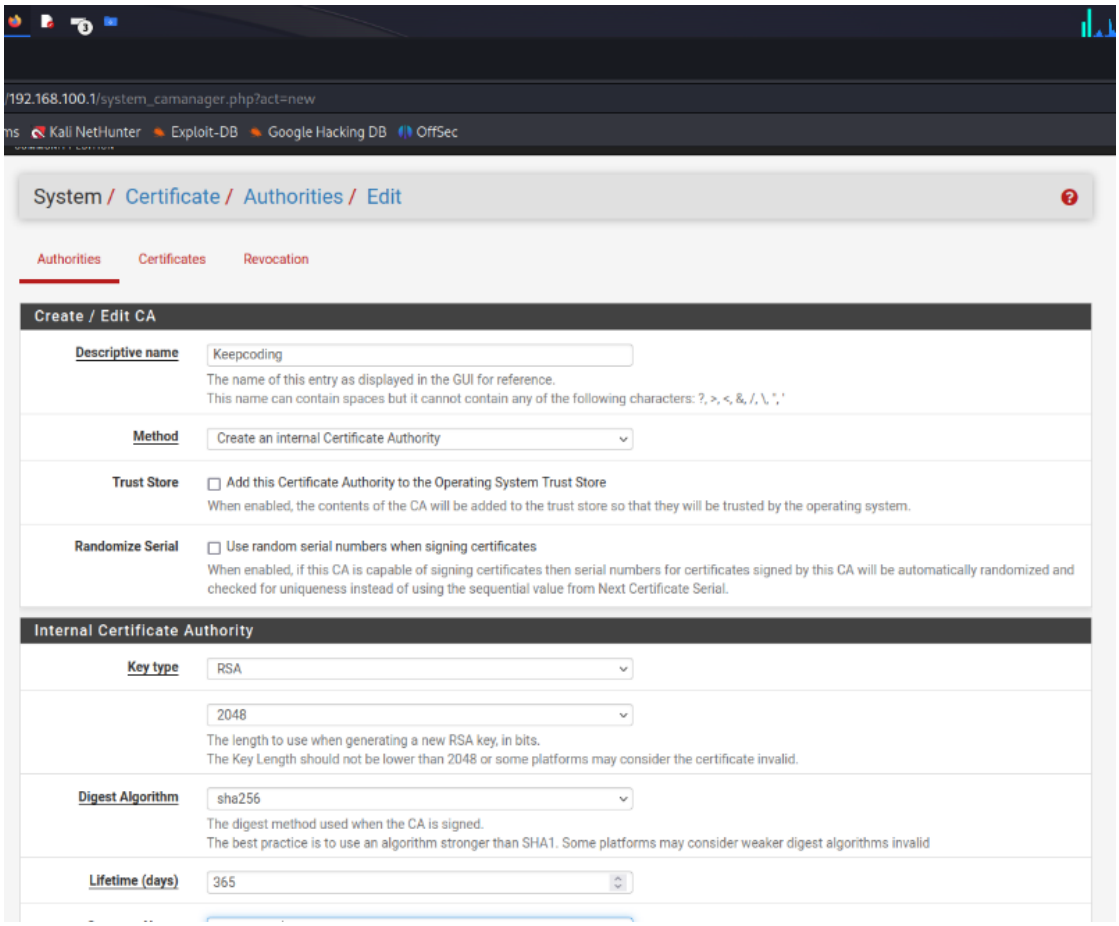


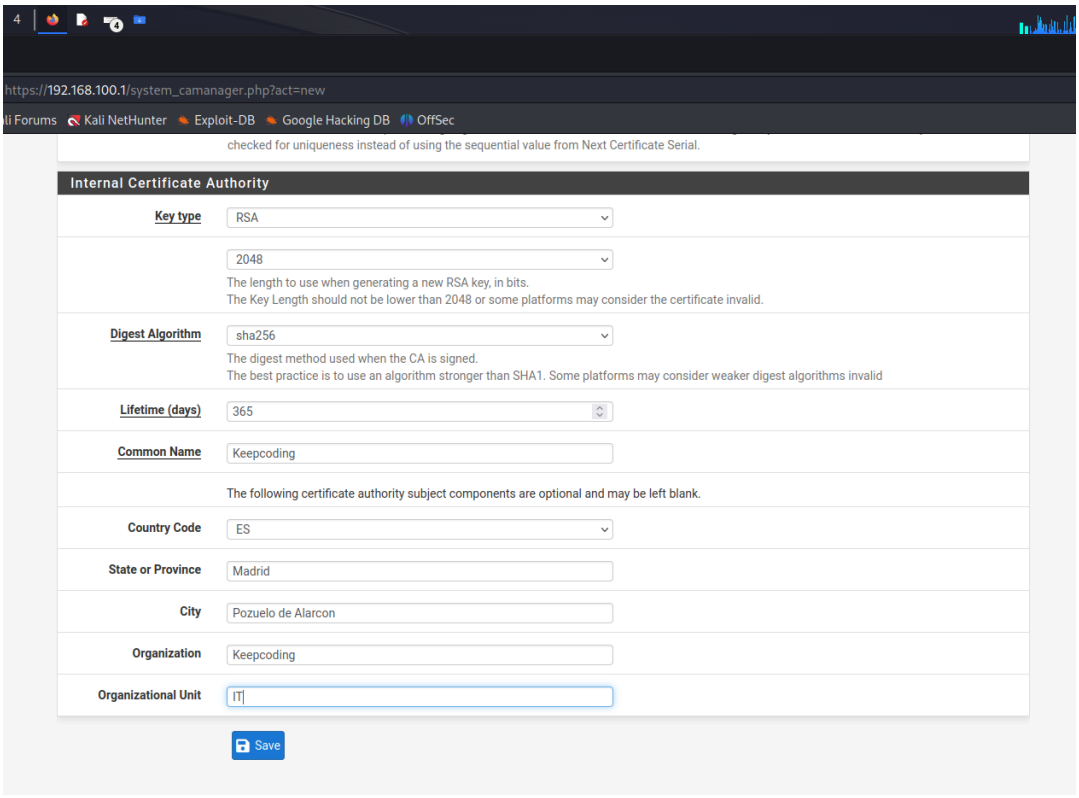
Aquí podemos observar que utilizando la IP WAN del PFSENSE en nuestro ordenador Windows podemos acceder al apache. Y comprobar que están conectados a través de la red WAN y el puerto 80.

3. Exportar VPN desde el PFSENSE

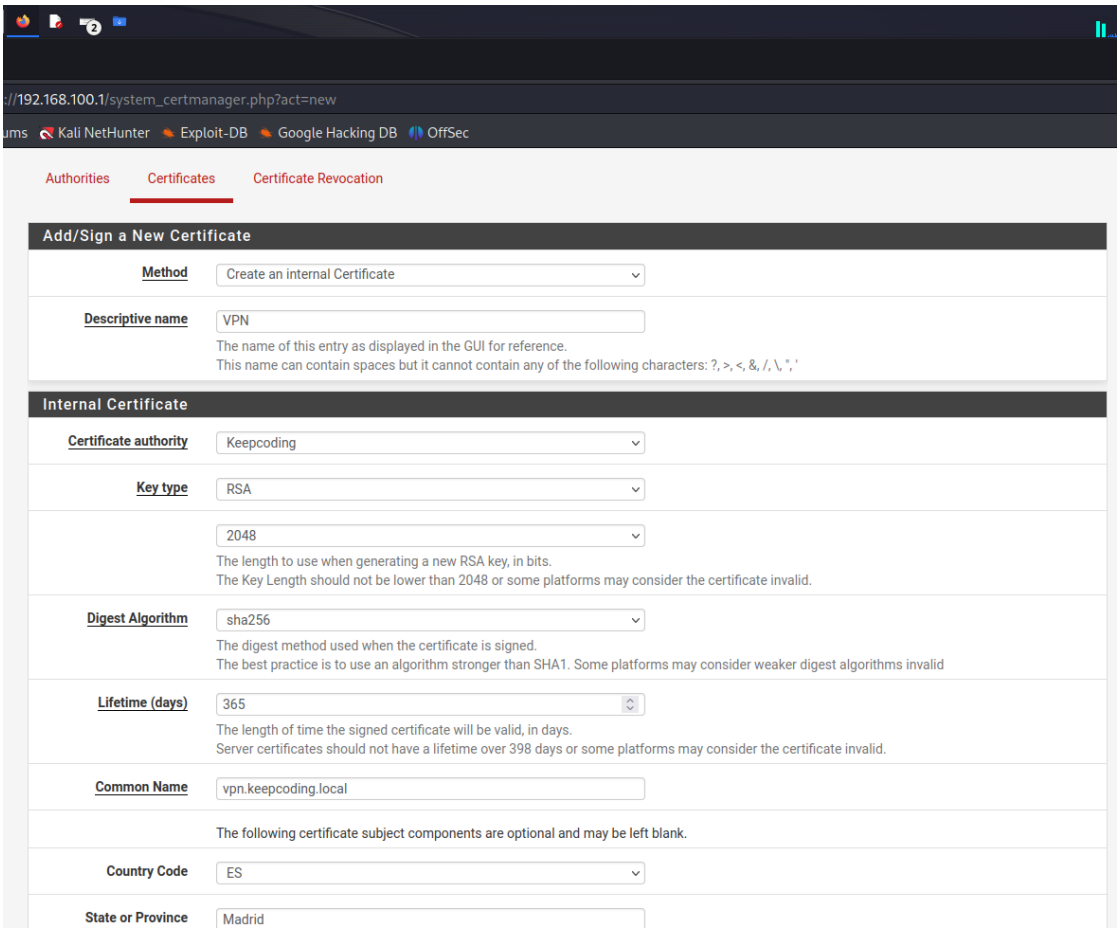


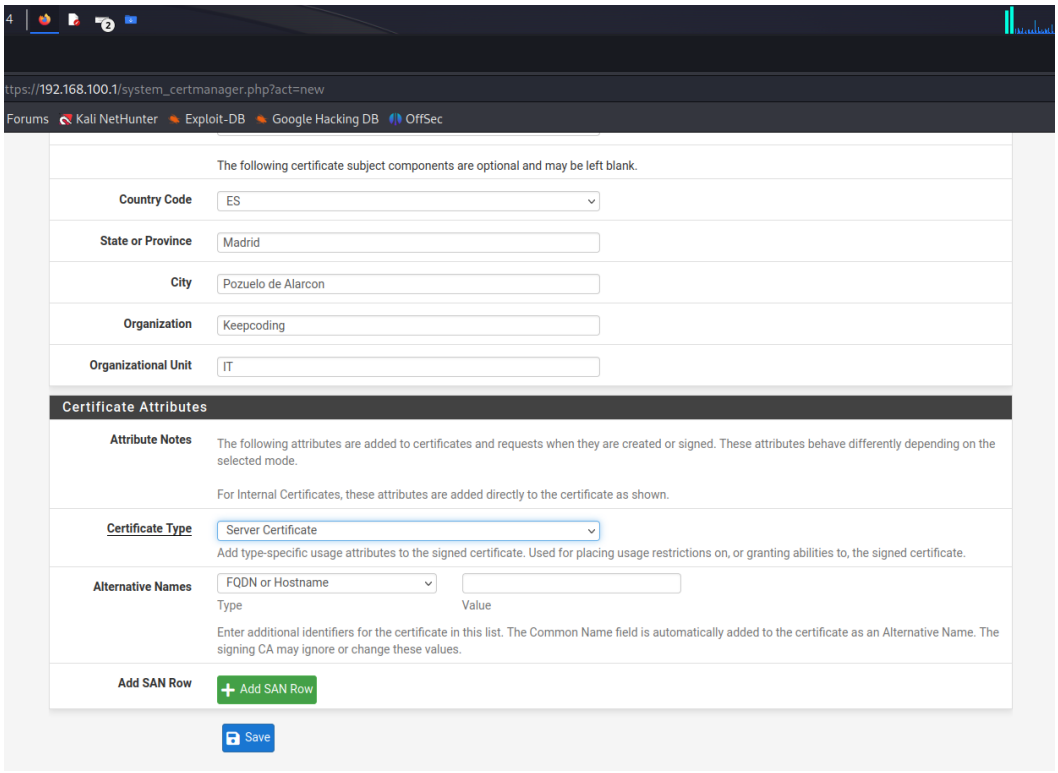
El 1º paso que tenemos que hacer es descargar el paquete de openvpn-client-export en el PFESENSE. Este paquete, aunque se instale desde Kali el que lo ejecuta es la máquina de UTM.



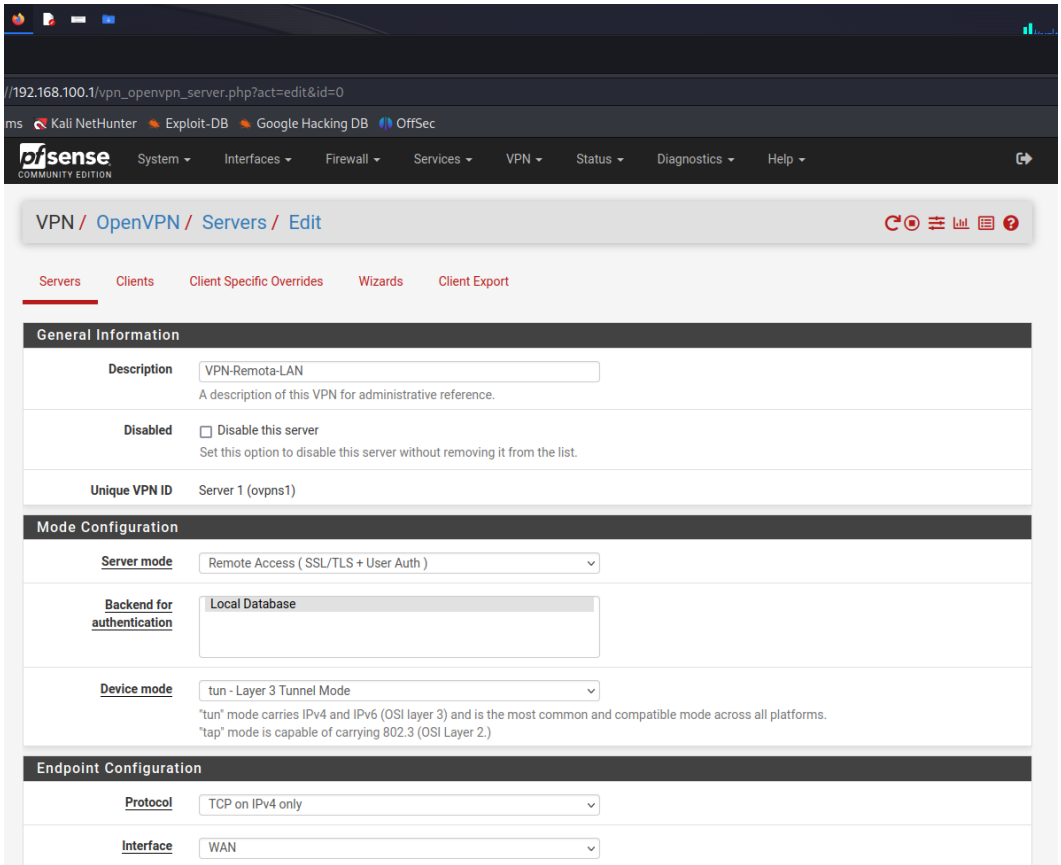


El 2º paso es crear un certificado de autorización interno lo vamos a denominar Keepcoding, de tipo RSA, tiempo de vida 365 días al año y ponemos los datos de donde nos encontramos y el departamento que queramos. Los demás datos vienen por defecto.

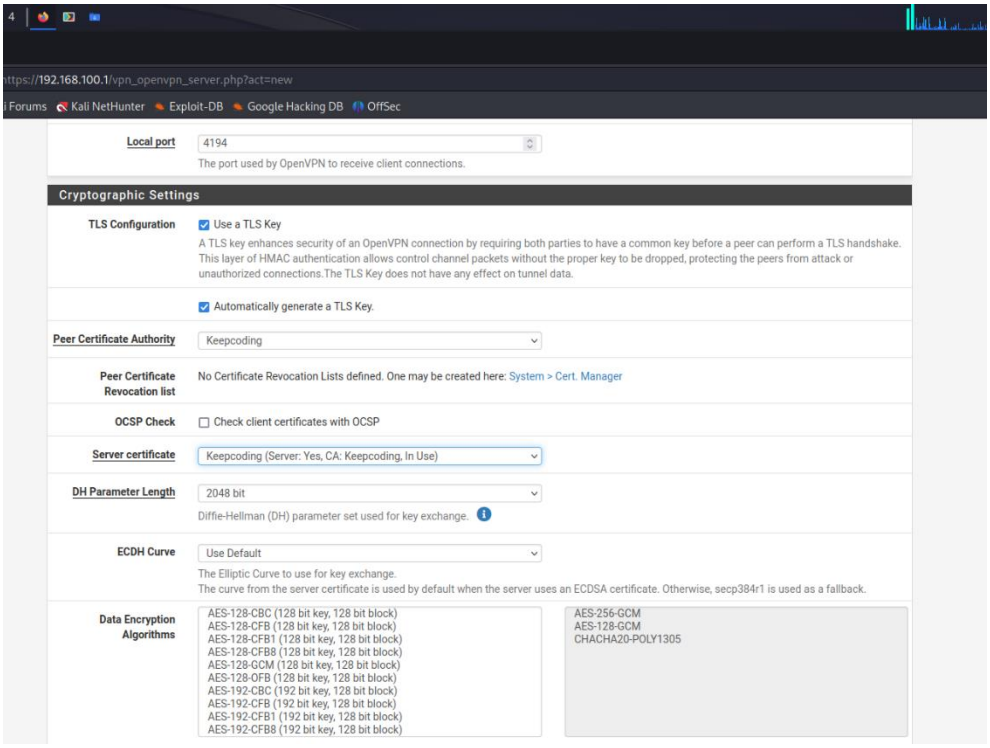




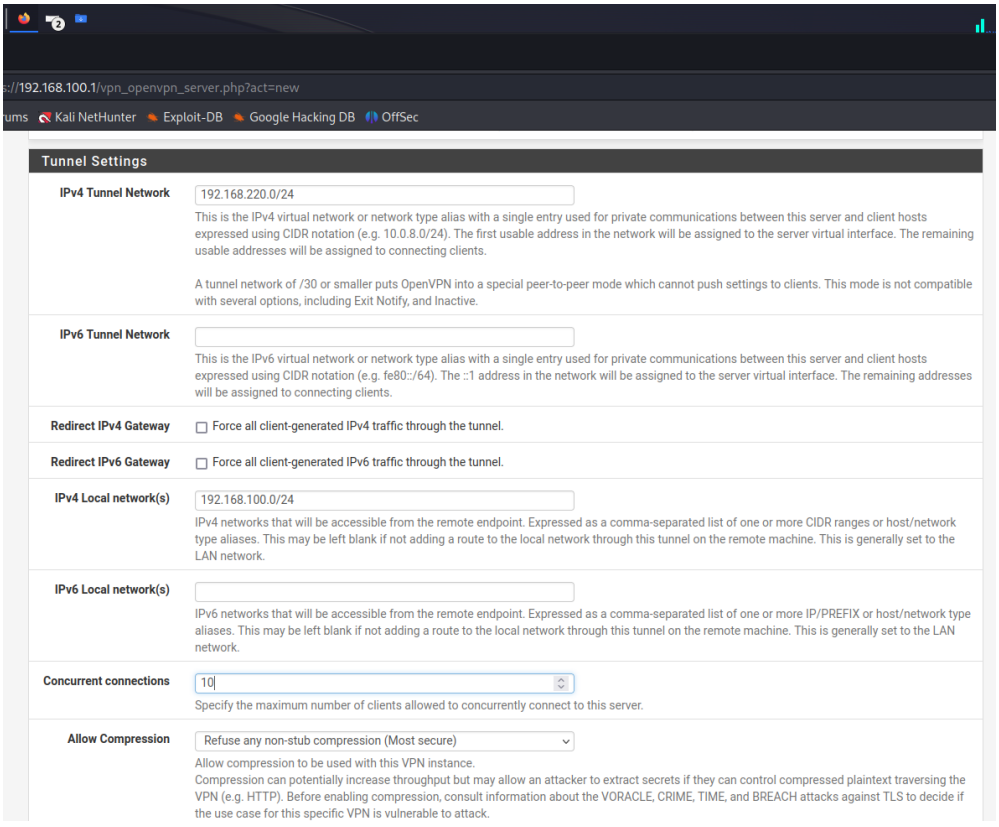
El 3º paso es crear un certificado interno este lo vamos a llamar VPN, importante certificado de autorización seleccionamos el que acabamos de crear al que hemos denominado Keepcoding, tipo RSA, lo nombramos vpn.keepcoding.local, tiempo de vida 365 días, rellenamos los datos de donde nos encontramos y por ultimo y más importante seleccionar, en tipo de certificado, el Server Certificate.



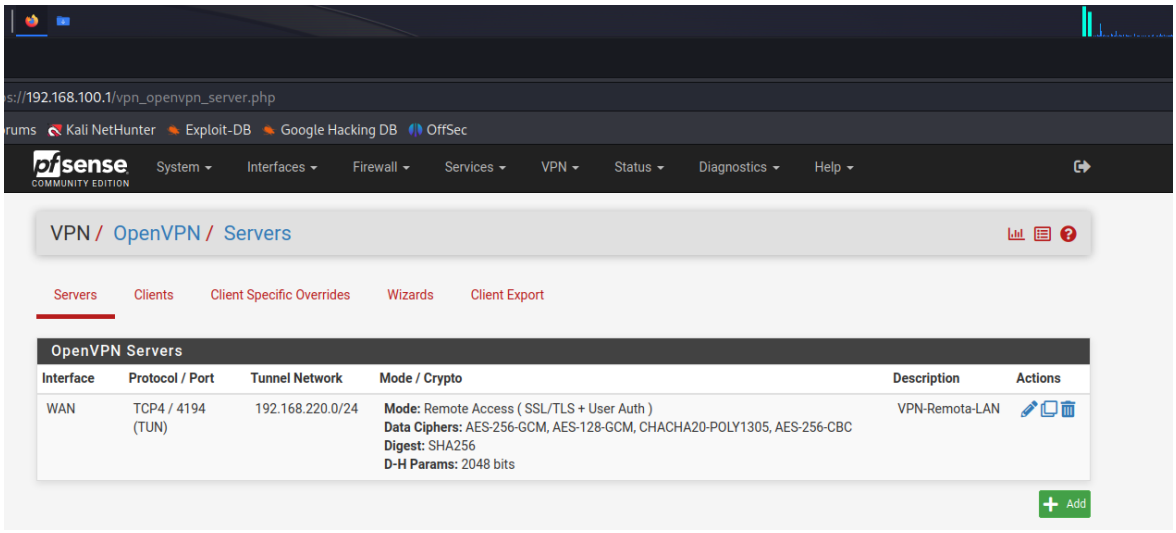
El 4º paso es irnos a OpenVPN y vamos a crear un servidor al que llamaremos VPN-Remota-LAN ya que estará conectada a nuestra red LAN por lo que estará enlazada a nuestra maquina Windows. El tipo de servidor es muy importante, seleccionaremos acceso remoto con contraseña y certificado, la autenticación por la base de datos local, el tipo de dispositivo tipo Layer 3 Tunnel mode de tipo IP, el protocolo seleccionamos TCP e interfaz WAN (nuestro rooter) el puerto local podremos 4194.



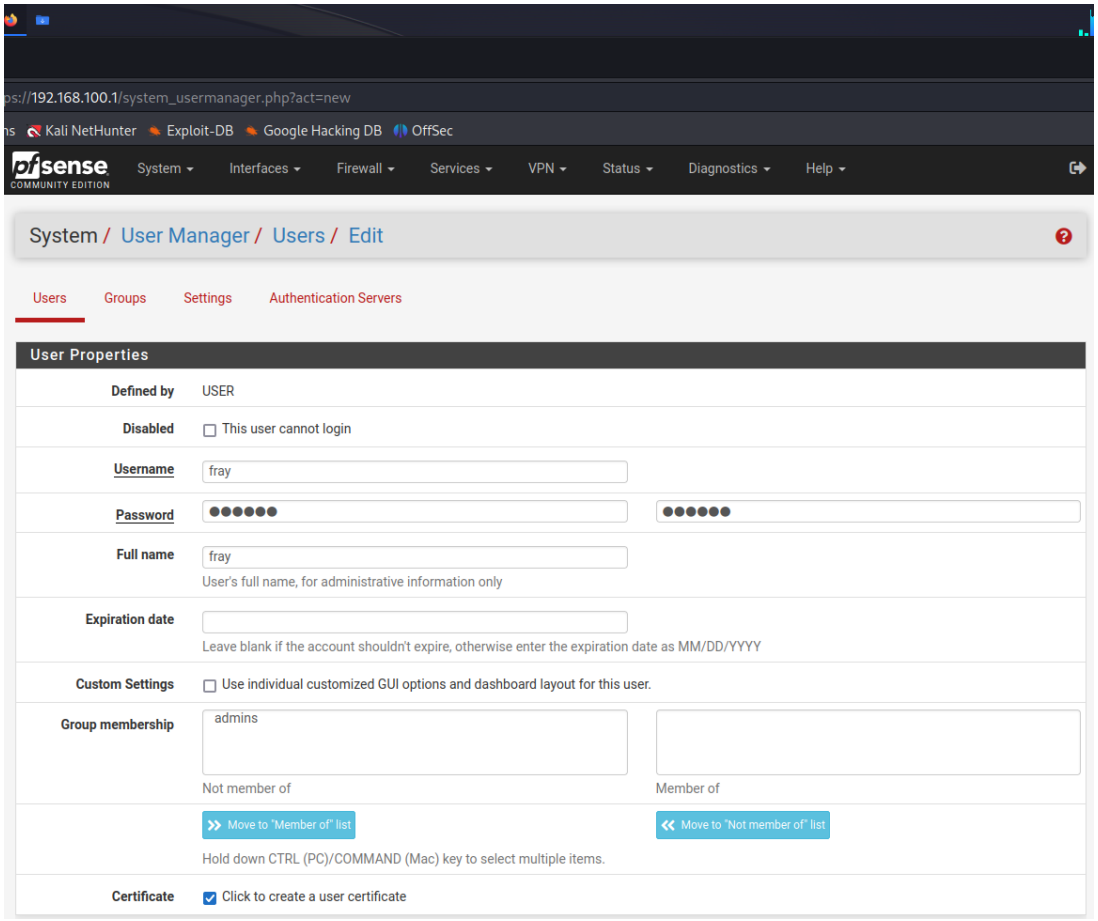
Aquí importante seleccionar el certificado para el servidor el que hemos creado de VPN.



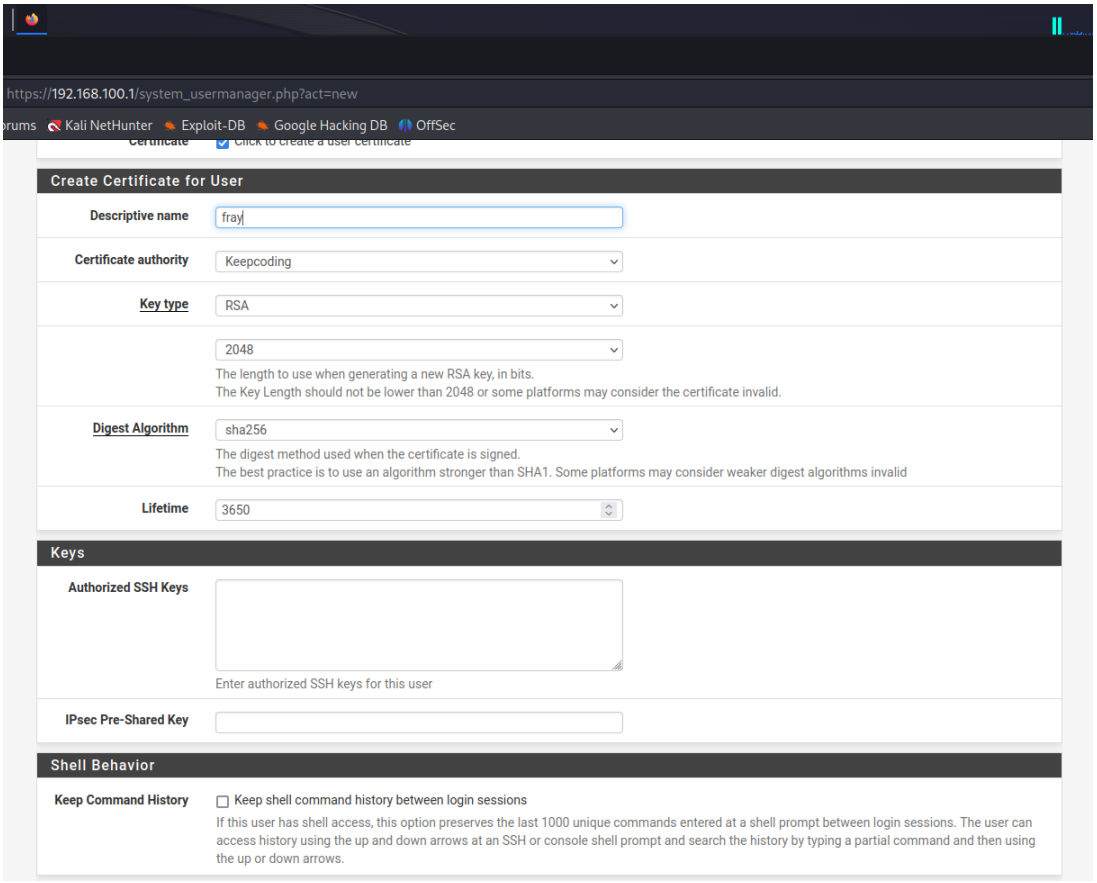
Como hemos elegido el tipo de dispositivo tipo Layer 3 Tunnel mode vamos a crear un IP nueva que en este caso será 192.168.220.0/24, la IP local a la que accederemos será 192.168.100.0/24 que es la red LAN. Los máximos de usuarios conectados serán 10. Las demás opciones vienen por defecto, por lo que ya guardaríamos toda la configuración.



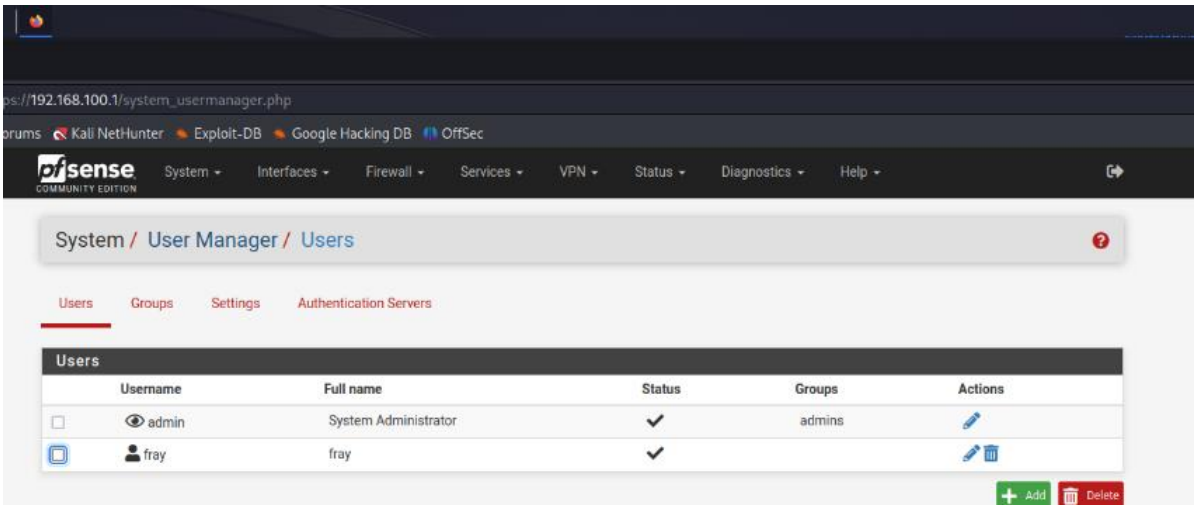
Ya podemos ver como tenemos nuestro servidor VPN creado.



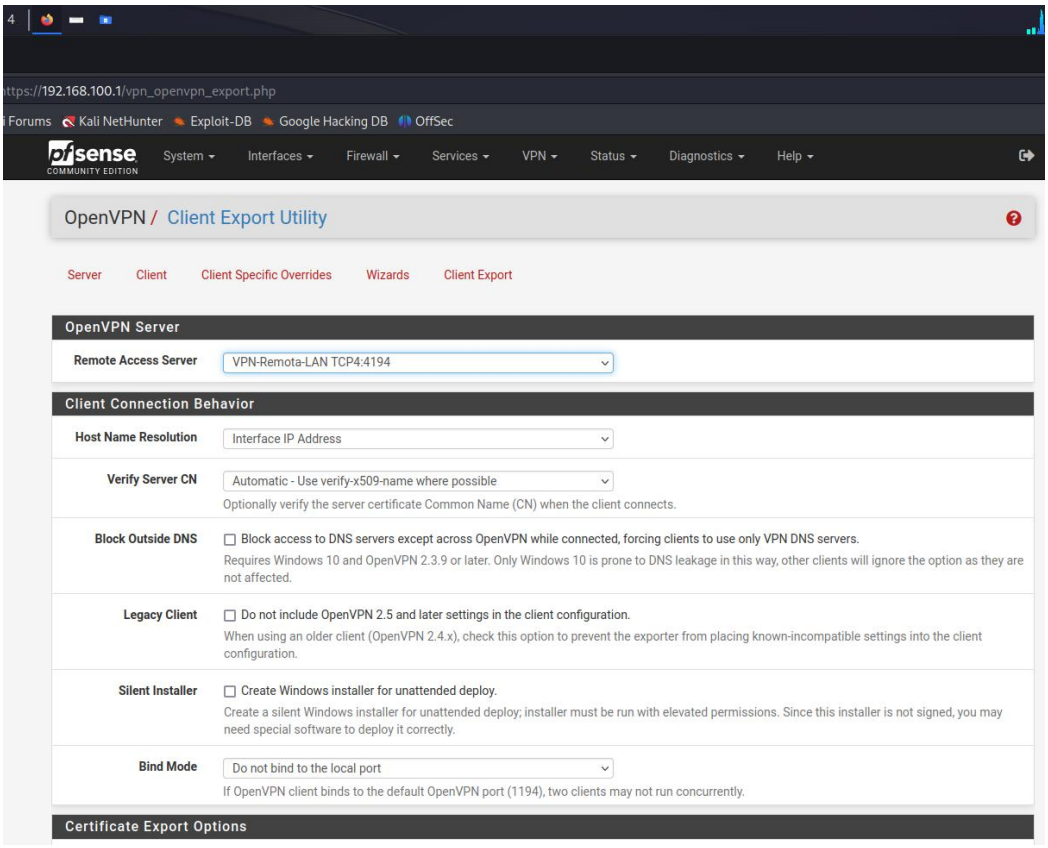
El 5º paso es crear un usuario, rellenamos los datos, ponemos la contraseña y lo más importante hay que marcar “crea un certificado para este usuario”



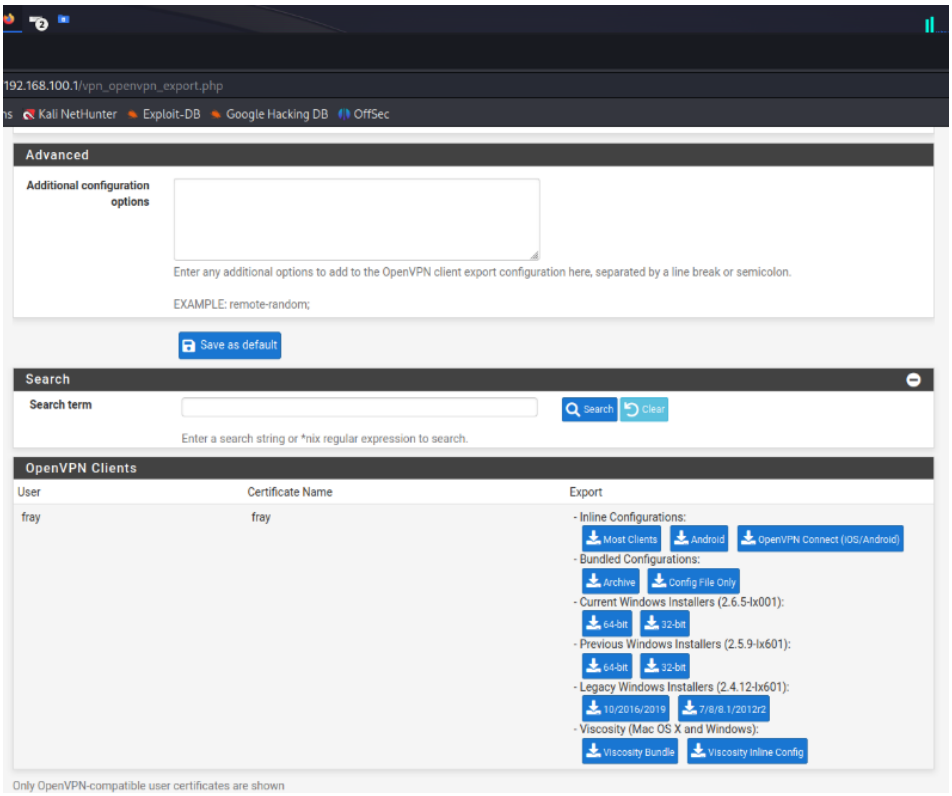
Lo siguiente es poner la descripción del nombre, el certificado de autorización el que hemos creado de Keepcoding y lo demás viene por defecto, guardamos.



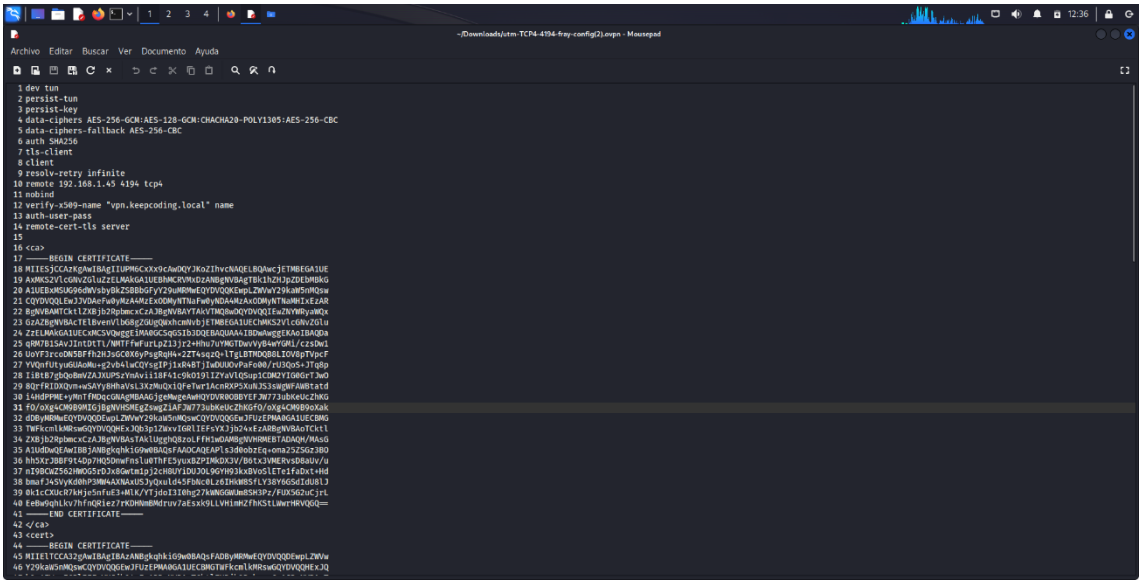
Vemos como aparece ya el usuario creado.



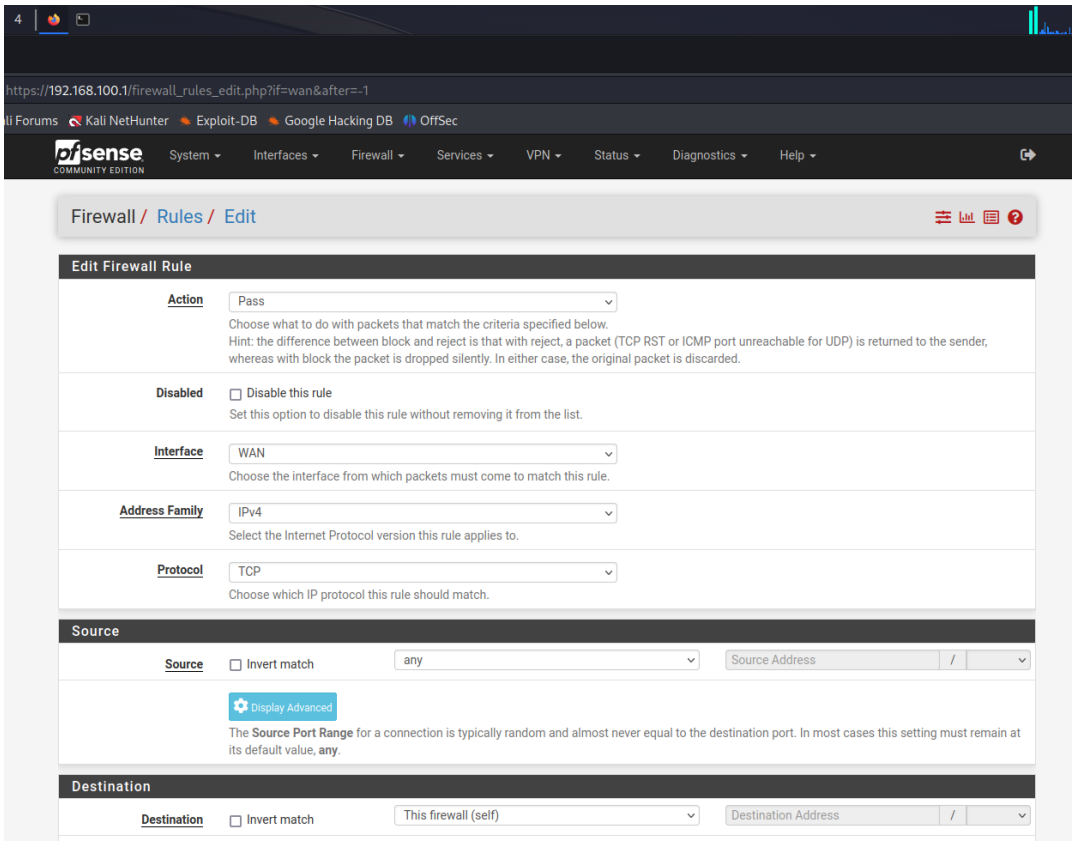
El último paso será exportar nuestro certificado creado, las opciones ya vienen por defecto.



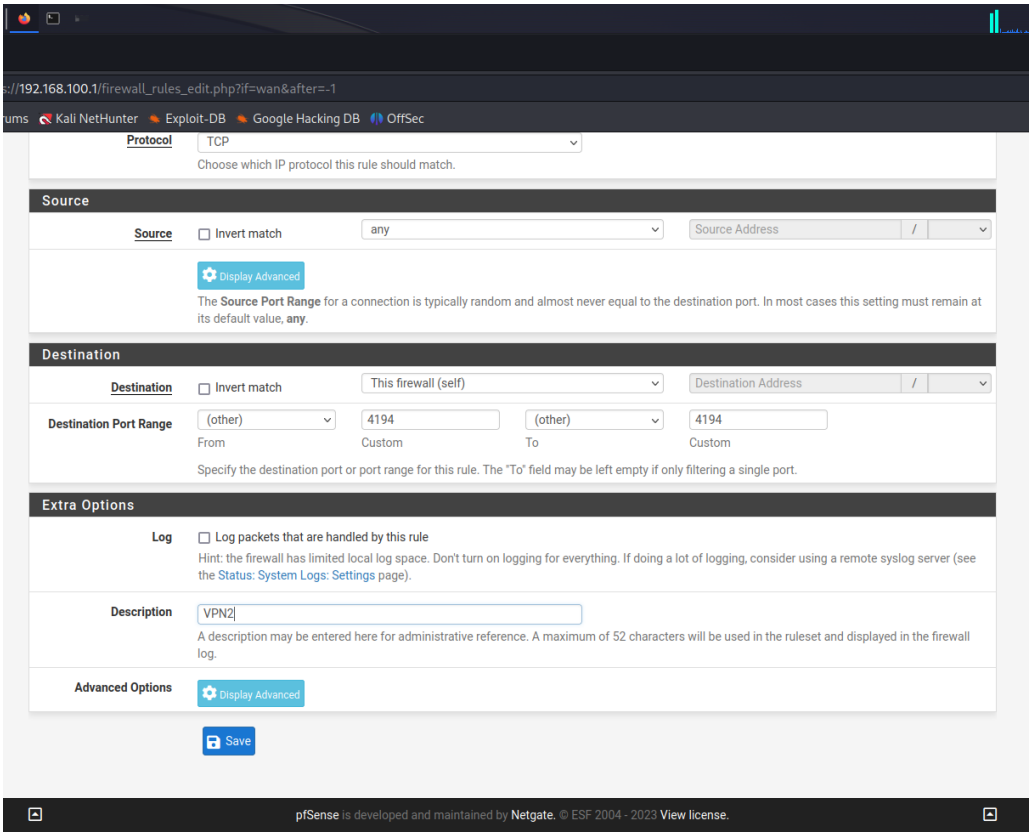
Aquí vemos como está nuestro certificado y la damos al mayor número de clientes para descargarlo.



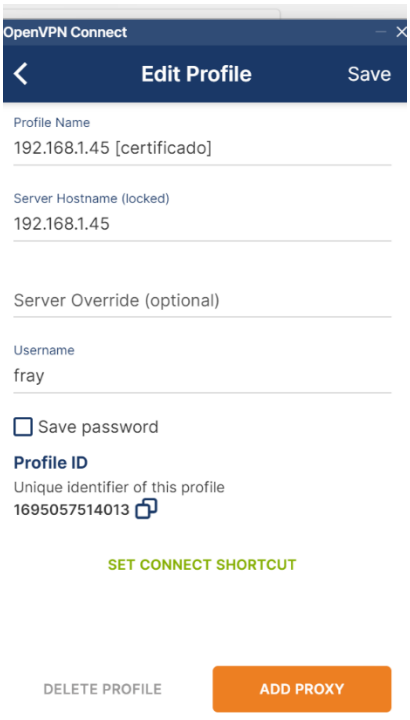
Certificado descargado.



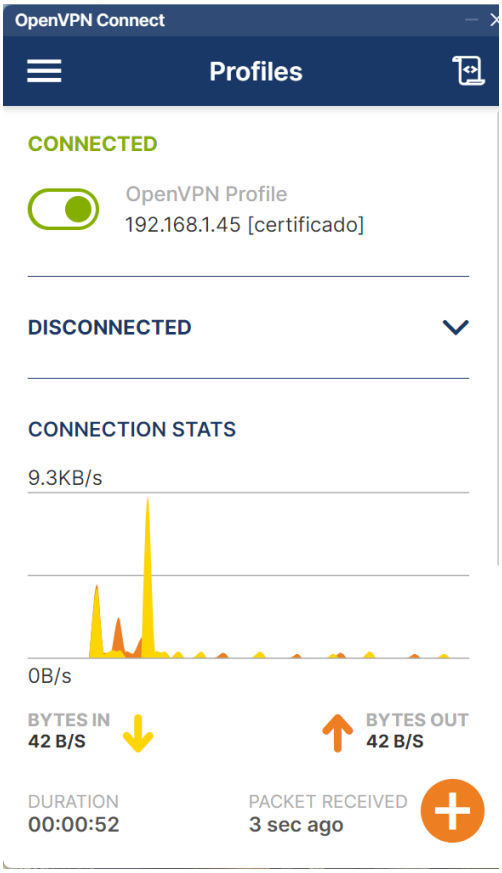
Ahora lo que tenemos que hacer es crear una regla en WAN para permitir pasar el tráfico. El destino tenemos que seleccionar “This firewall”



Destino del puerto del 4194 a 4194, la descripción pondremos VPN y guardamos.



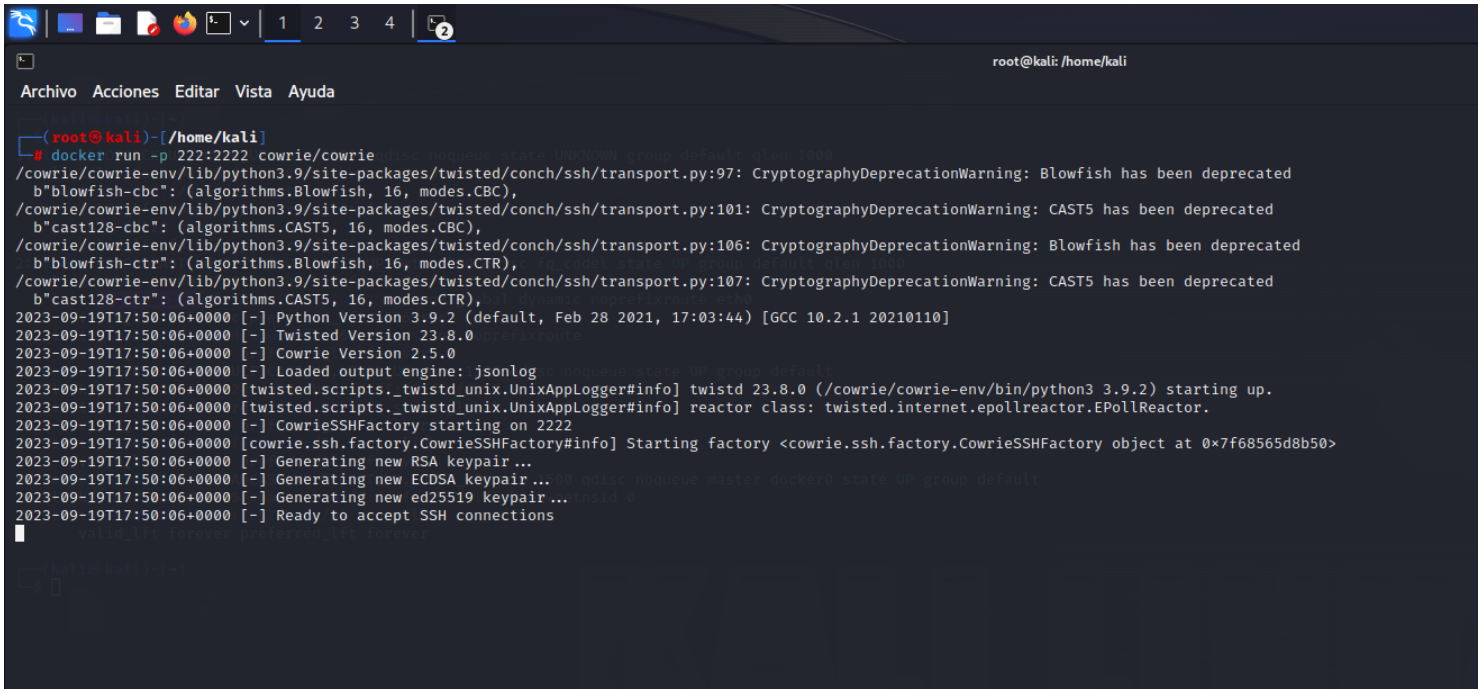
Para terminar, importamos el certificado al OpenVPN Conenct.



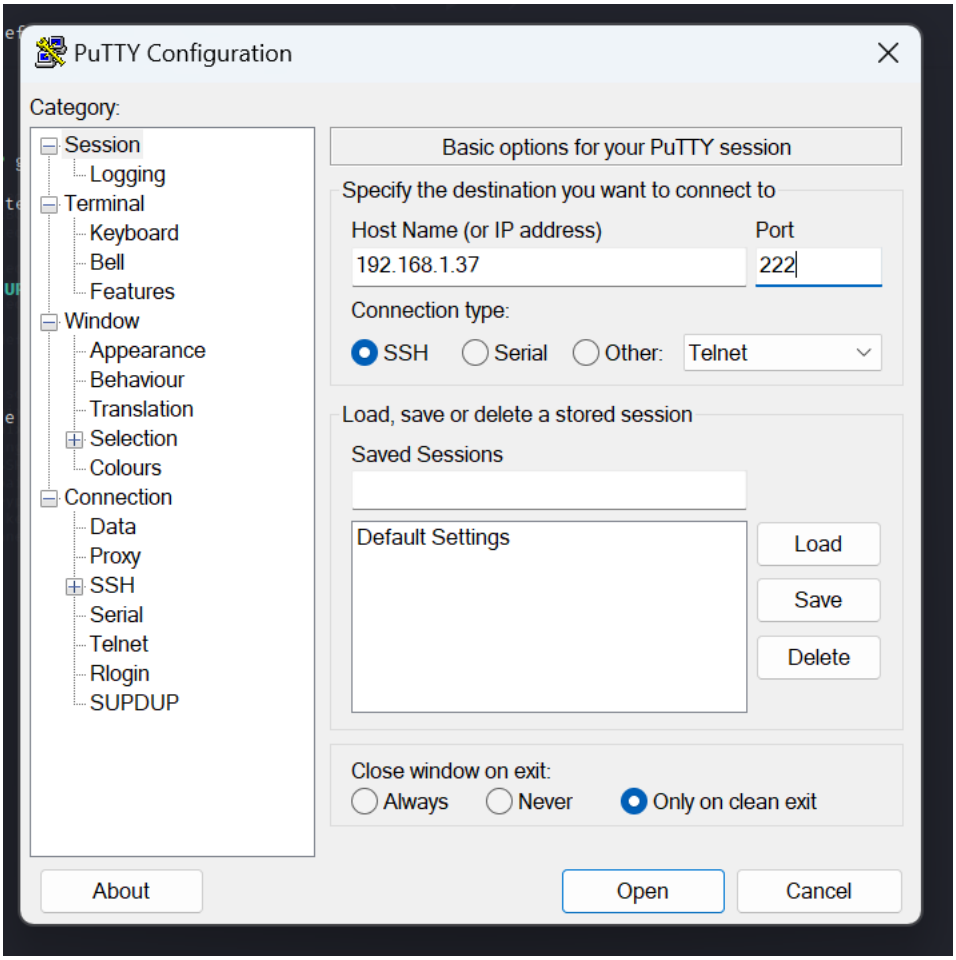
Aquí vemos como ya está conectada la VPN a nuestra red LAN a través de la WAN, en nuestro equipo Windows.

4.HONEYPOTS

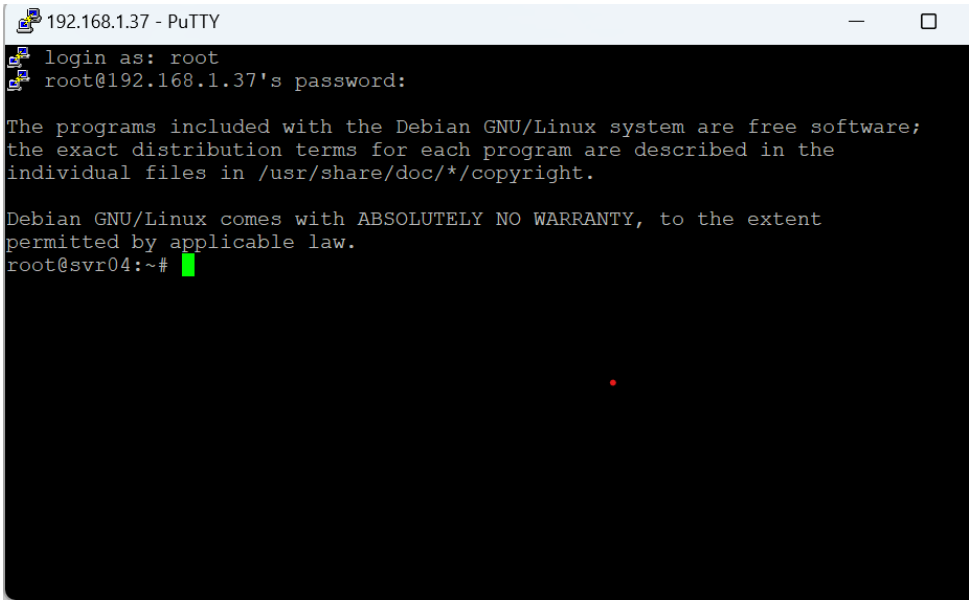
El Honeypot que vamos a lanzar en DMZ es el Cowrie “SSH” a través el Docker.



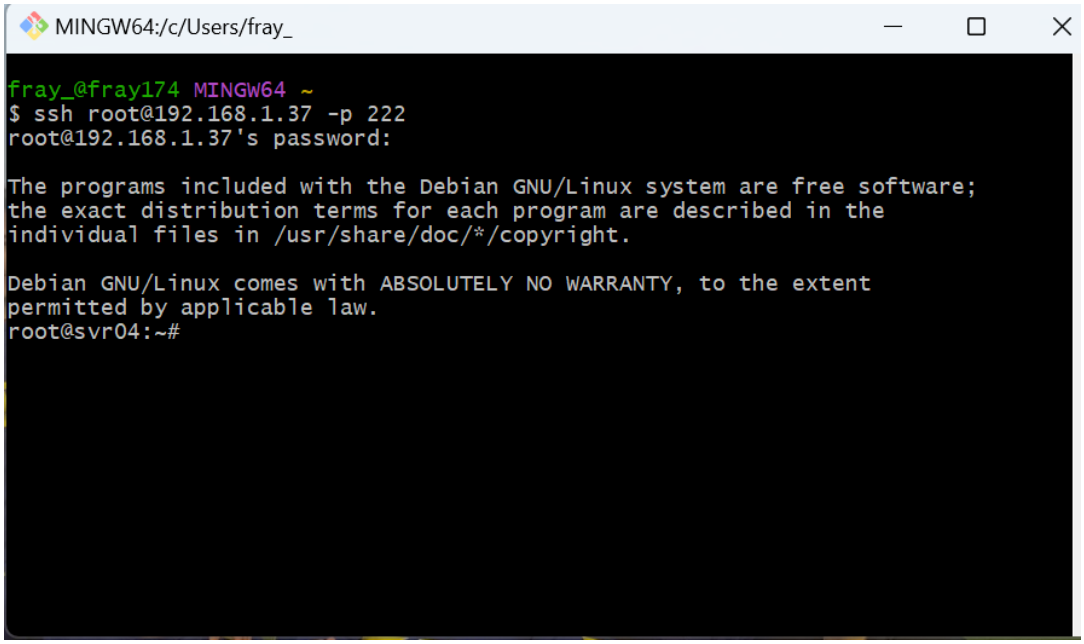
El primer paso que hemos hecho es lanzar el contenedor Docker para que arranque con este comando: docker run -p 222:2222 cowrie/cowrie. El puerto de la izquierda es del anfitrión y el de la derecha del invitado.



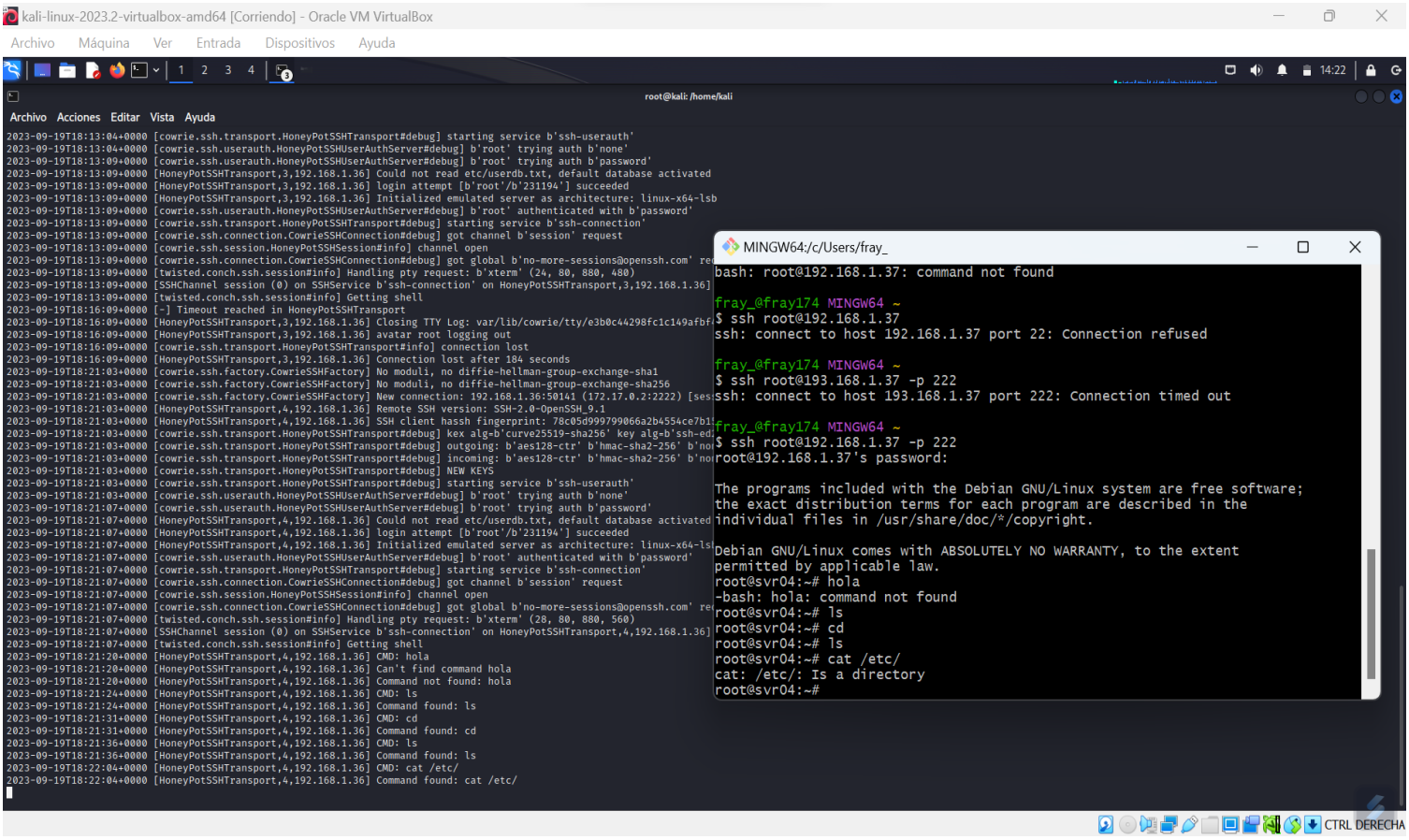
El siguiente paso es abrir la aplicación PuTTY ponemos la IP y el puerto de nuestro Kali. Que en este caso es 192.168.1.37 y 222.



Se nos abrirá una consola en PuTTY y tendremos que poner un usuario y contraseña para estar dentro.

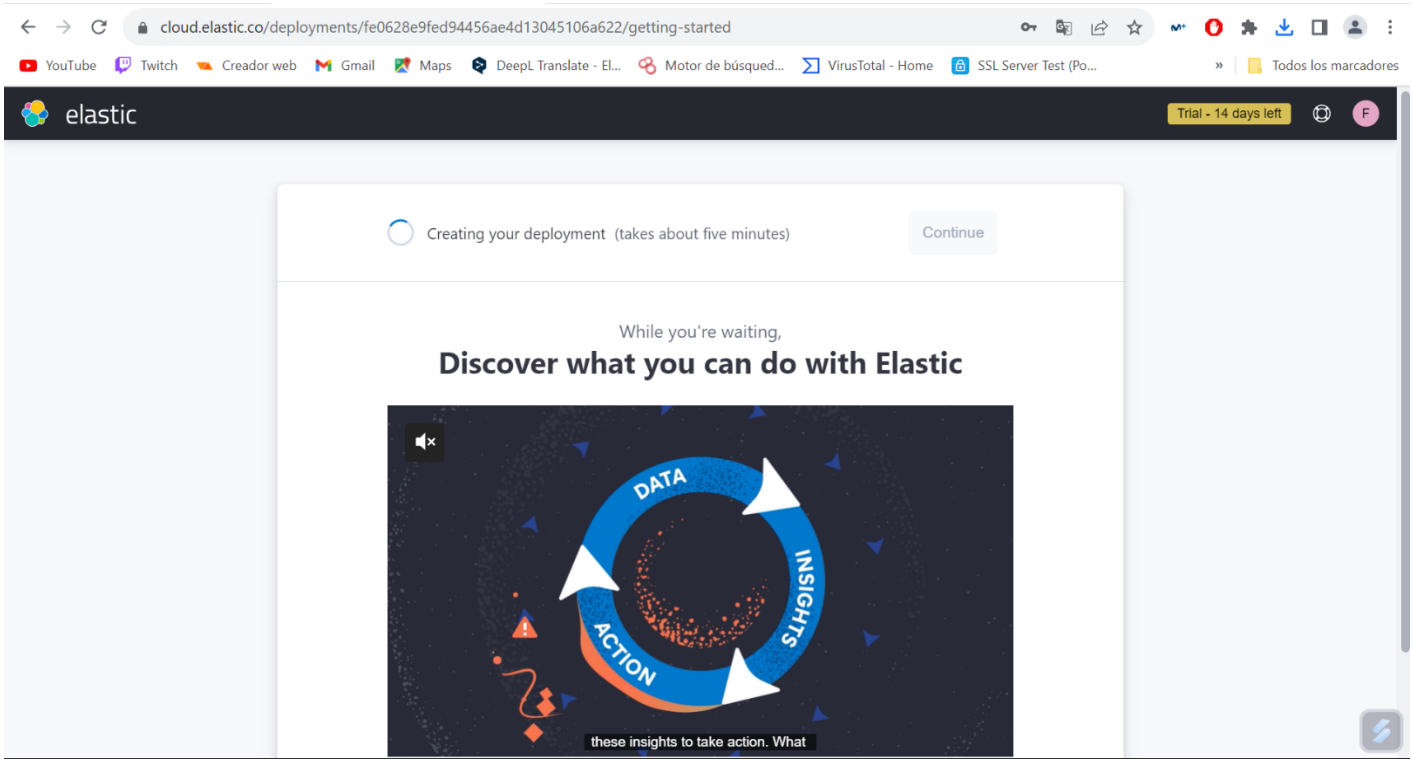


Lo siguiente que debemos hacer es abrir una terminal en Windows y poner el siguiente comando: SSH root@192.168.1.37 -p 222 (en este caso mi IP) y después la contraseña que hemos establecido, una vez hecho esto estamos dentro.

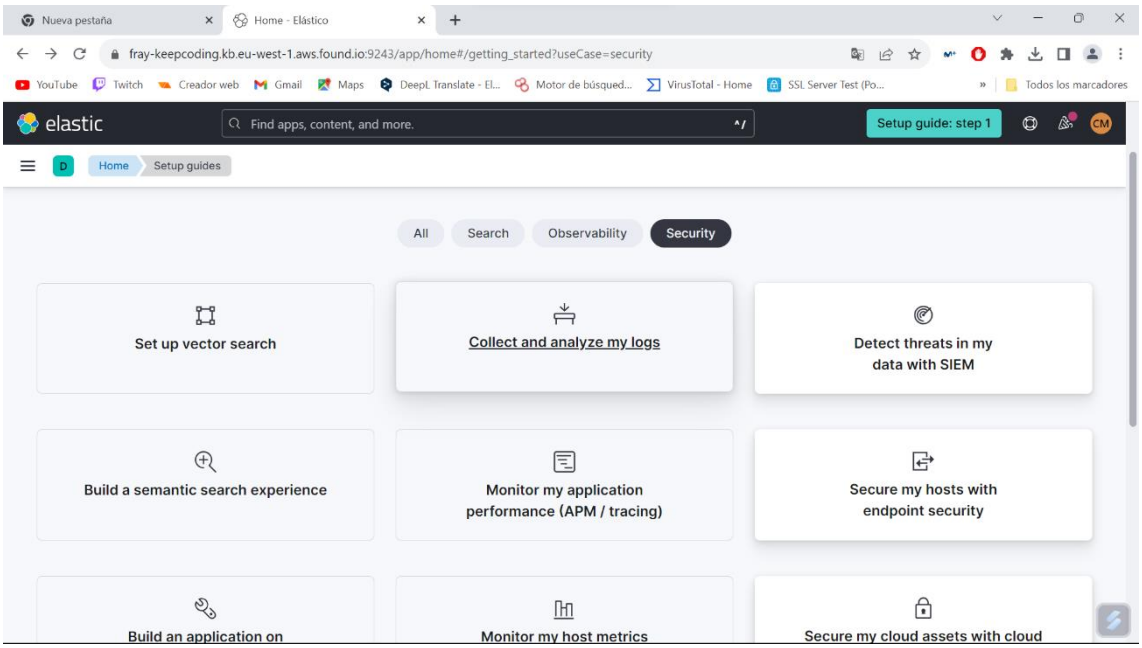


Por último, podemos ver cómo están conectadas las dos consolas a través de la red WAN, mientras que en la de Windows lanzo diferente comandos la de Kali me va detectando los logs, por lo que ya tendríamos nuestro Honeypot corriendo.

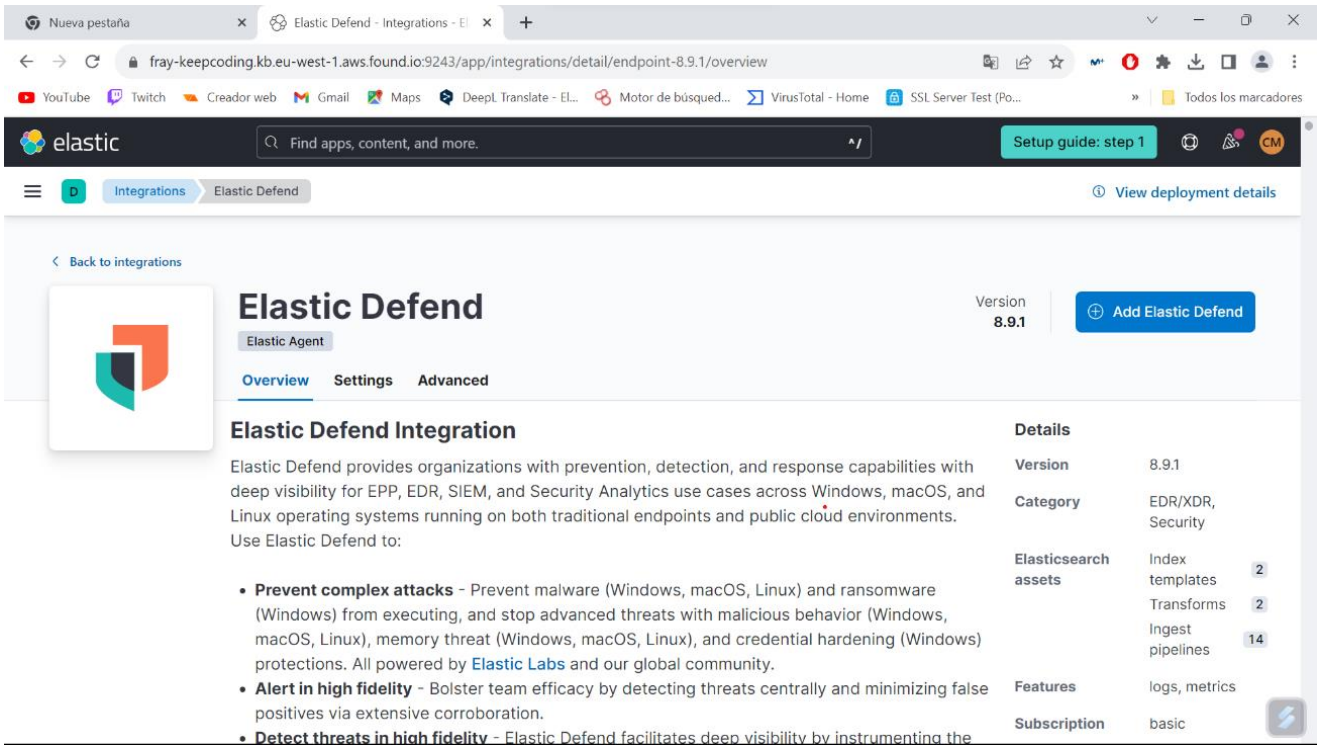
5.Elasticsearch en la nube



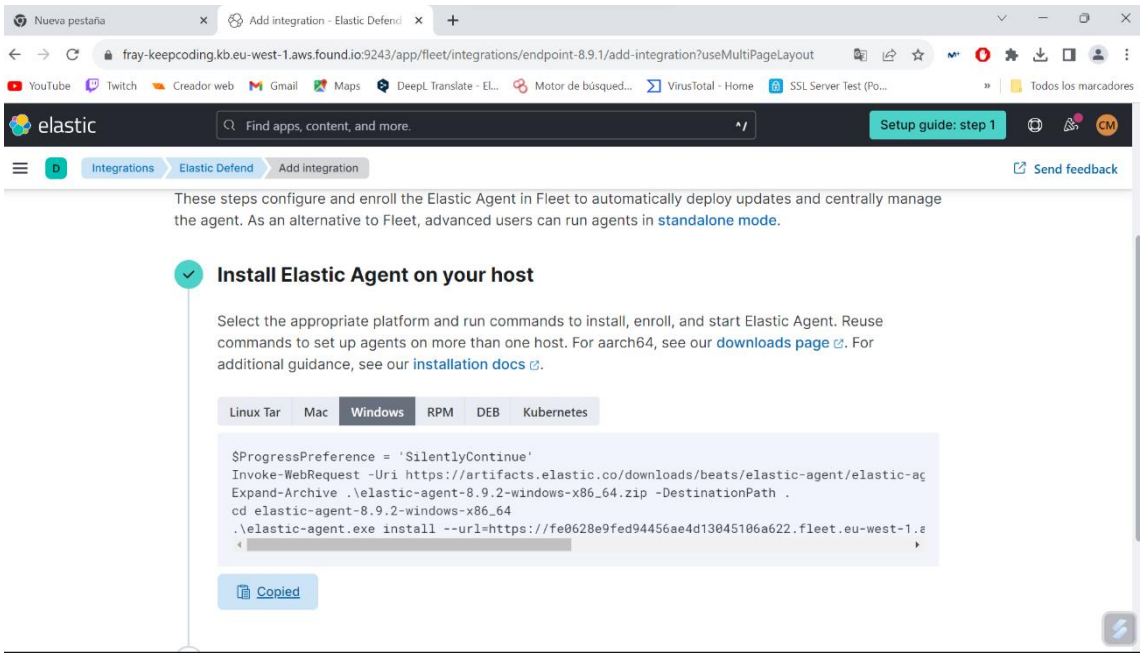
El primer paso que debemos hacer después de habernos creado una cuenta es crear un “Deployment”



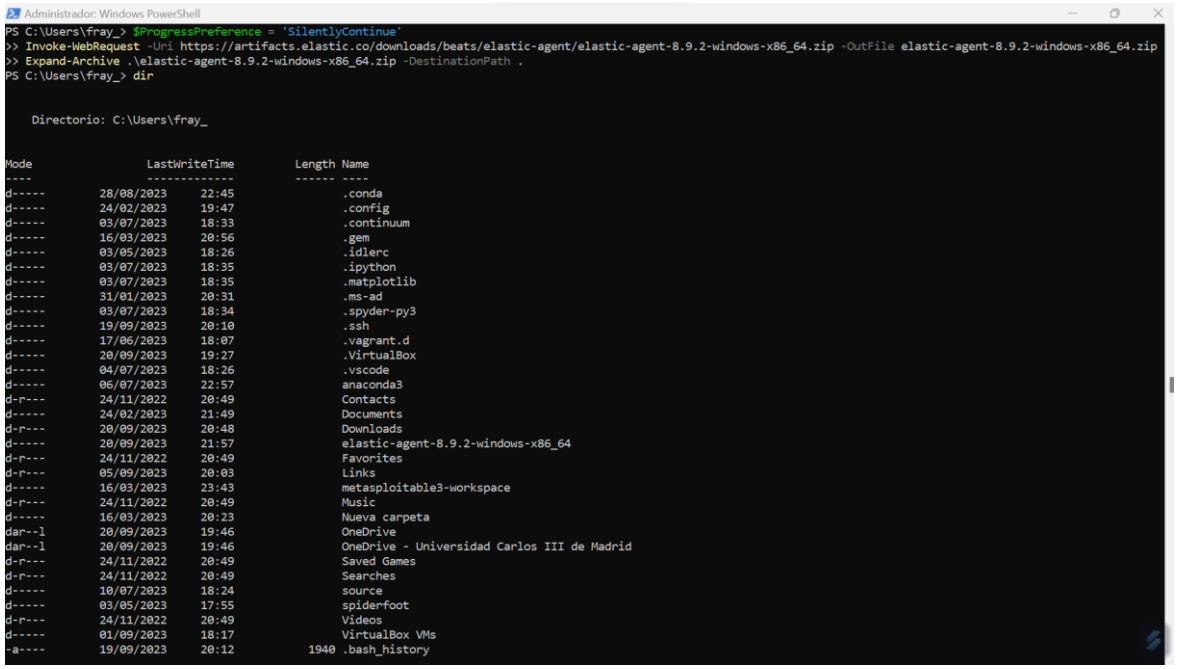
Una vez creado el “deployment” no aparecerá esta ventana con diferentes opciones. La que vamos a seleccionar nosotros es la de “Detect threats in my data with SIEM”

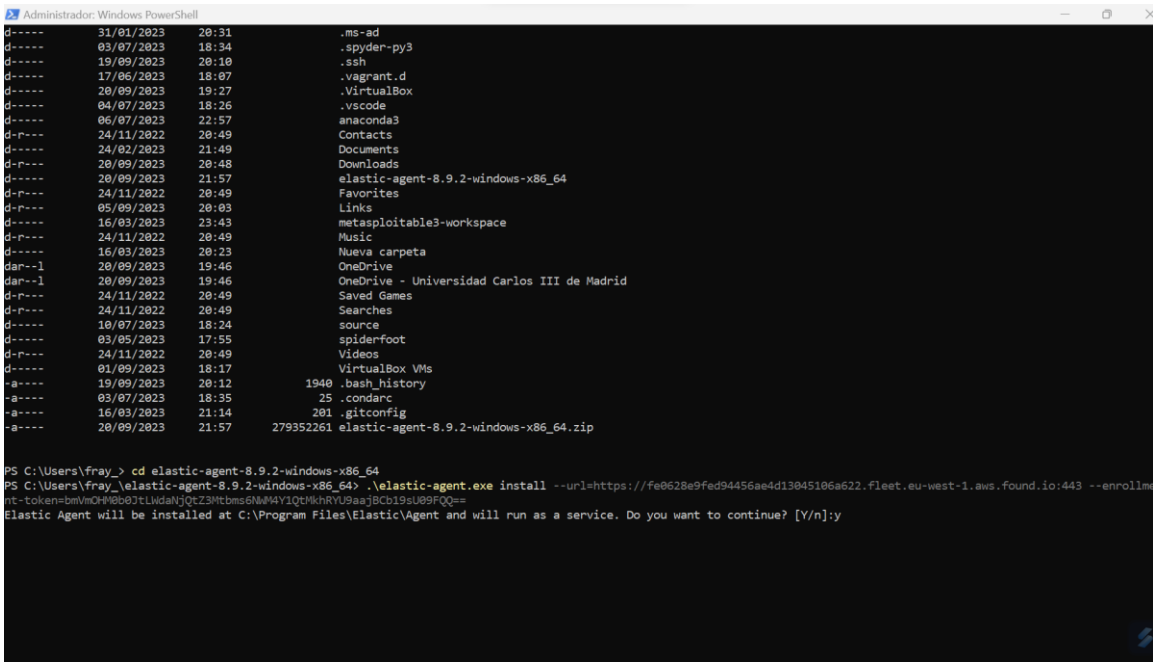


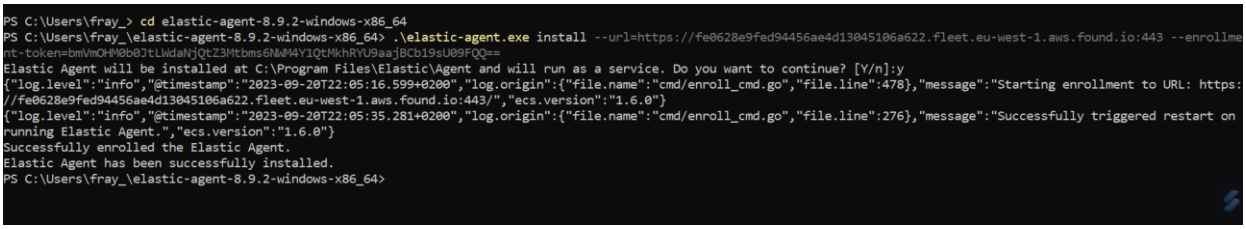
Lo siguiente que haremos es añadir el Elastic Defend.



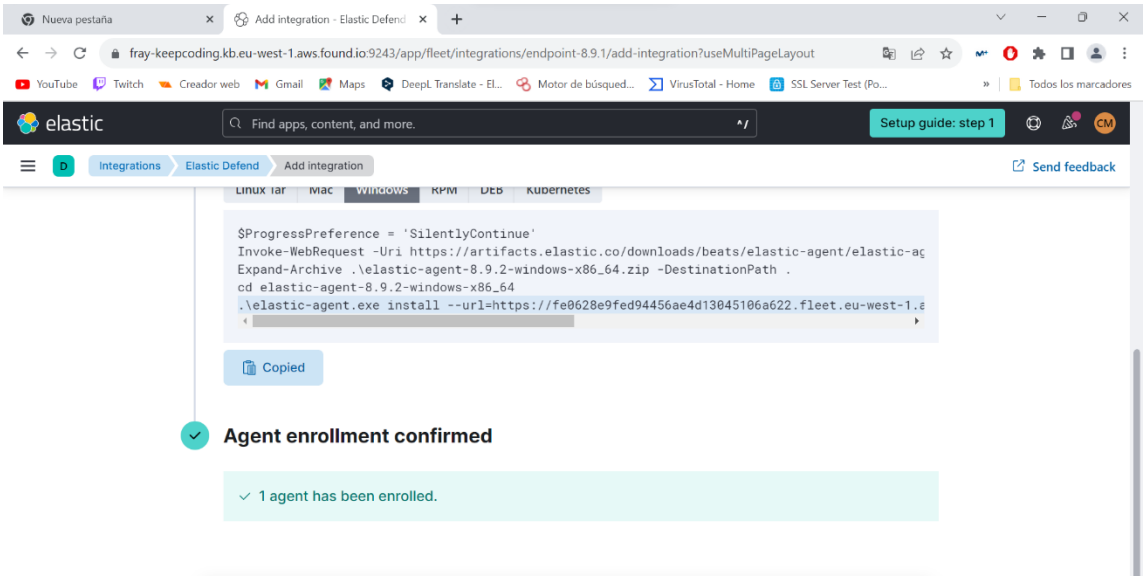
Después deberemos copiar los comandos que nos dan según el sistema operativo en el que lo vayamos a instalar, en nuestro caso lo haremos en Windows.



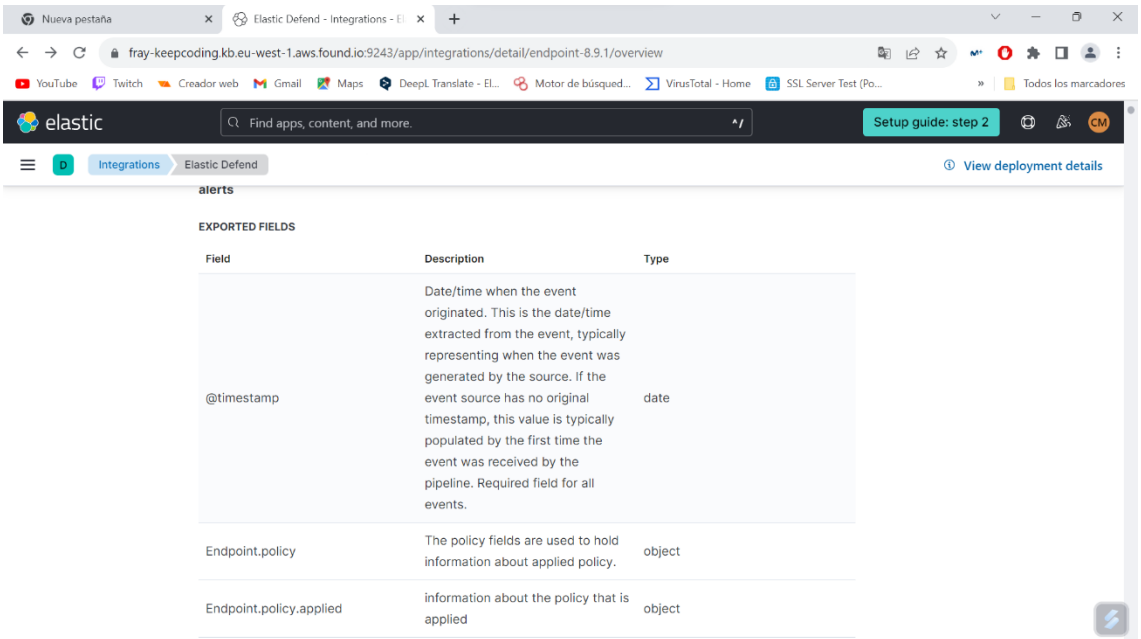




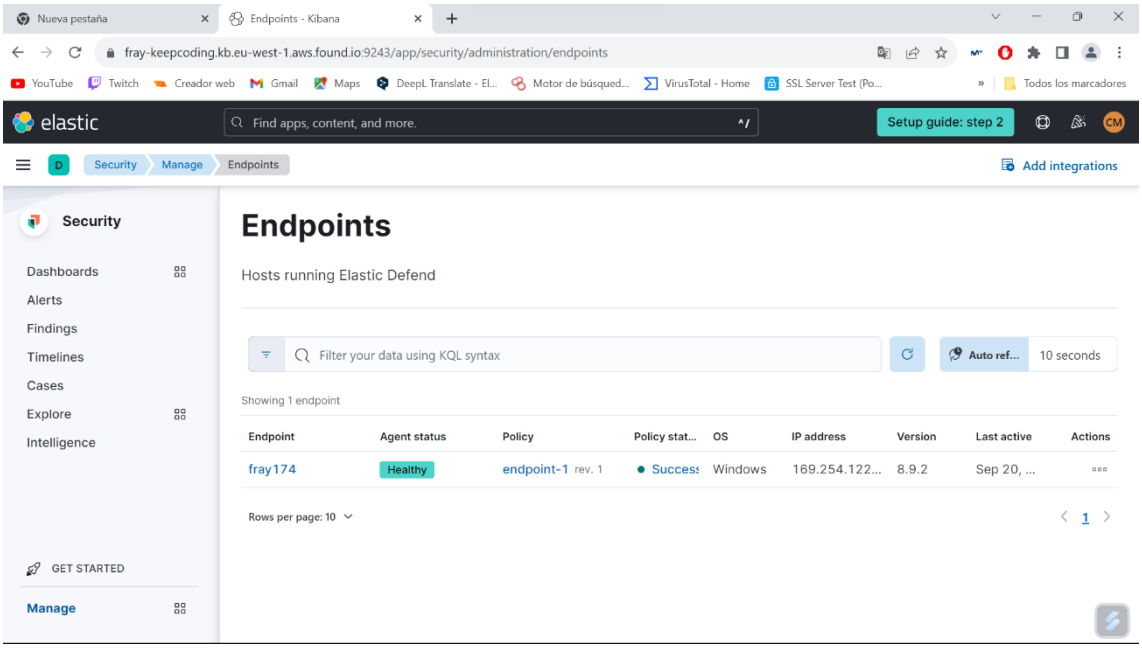
Lanzamos los distinto comandos en nuestra consola Windows para que corra, le damos a sí y ya lo tendríamos instalado.



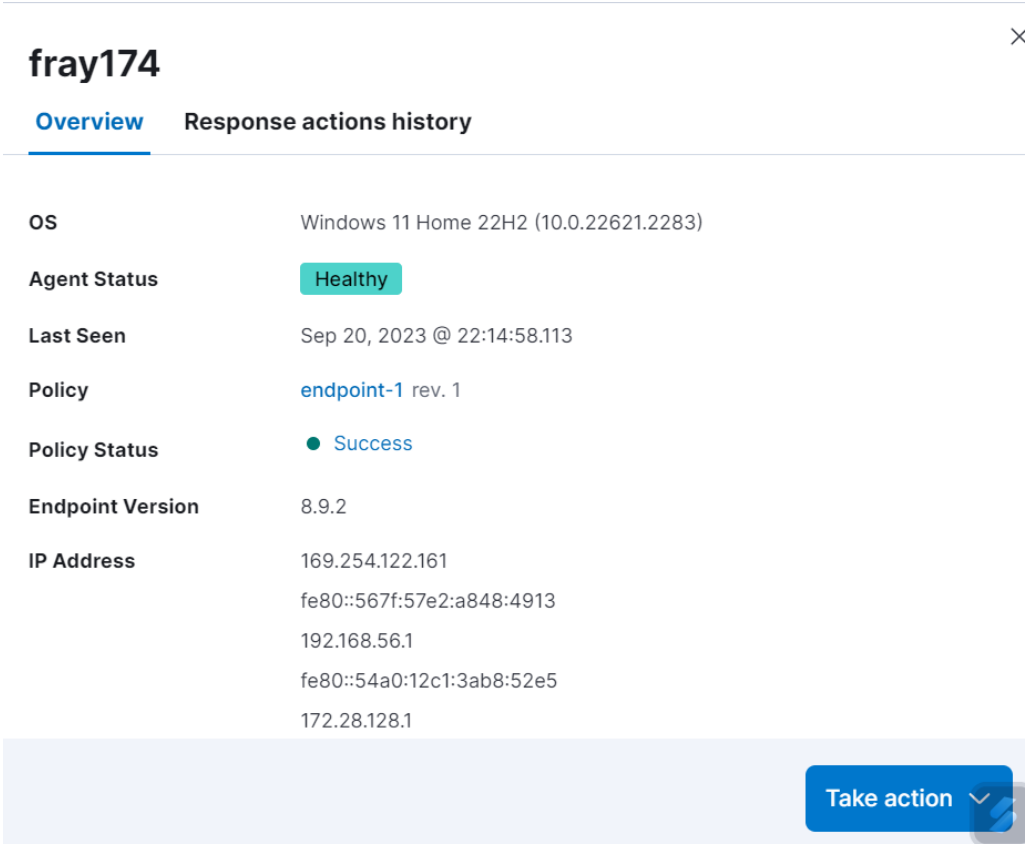
Ya vemos como se ha confirmado en la nube. Ahora Le daríamos añadir y confirmar datos.



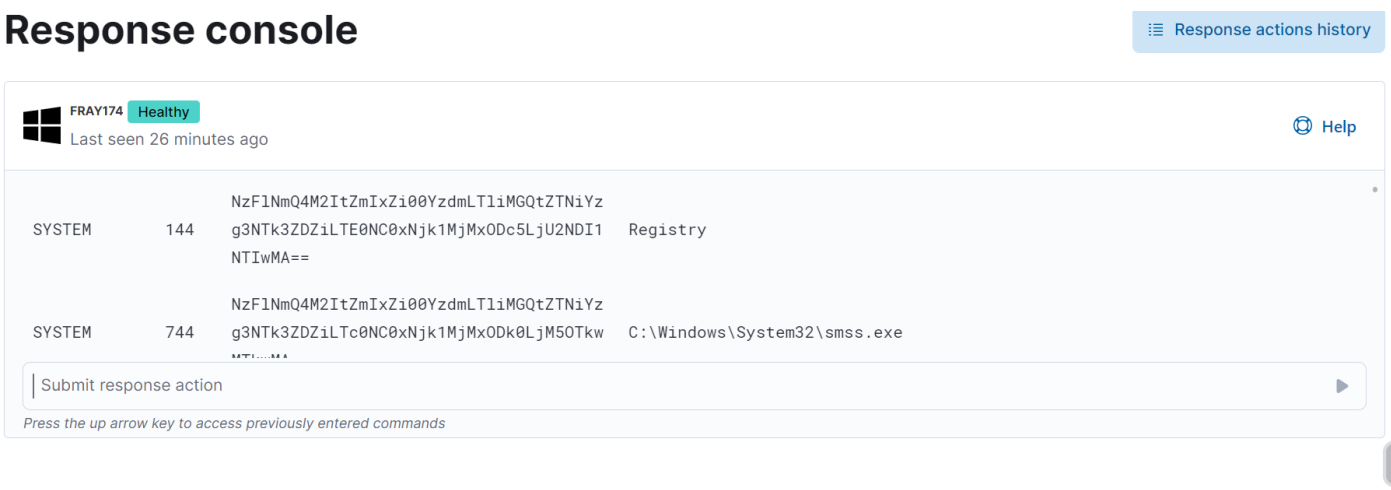
Vemos como ya empieza a lanzar distintos logs.



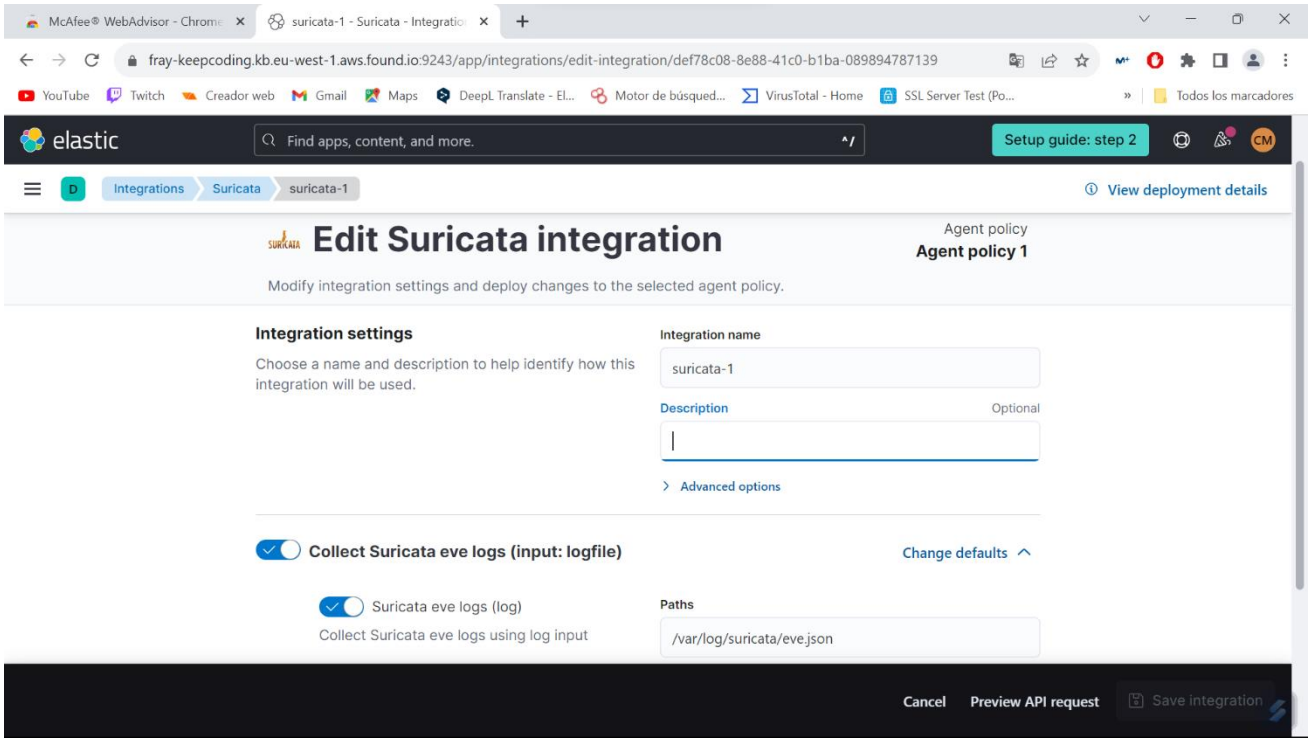
Podemos observar como ya están integrado los “Endpoints” en nuestra maquina Windows.



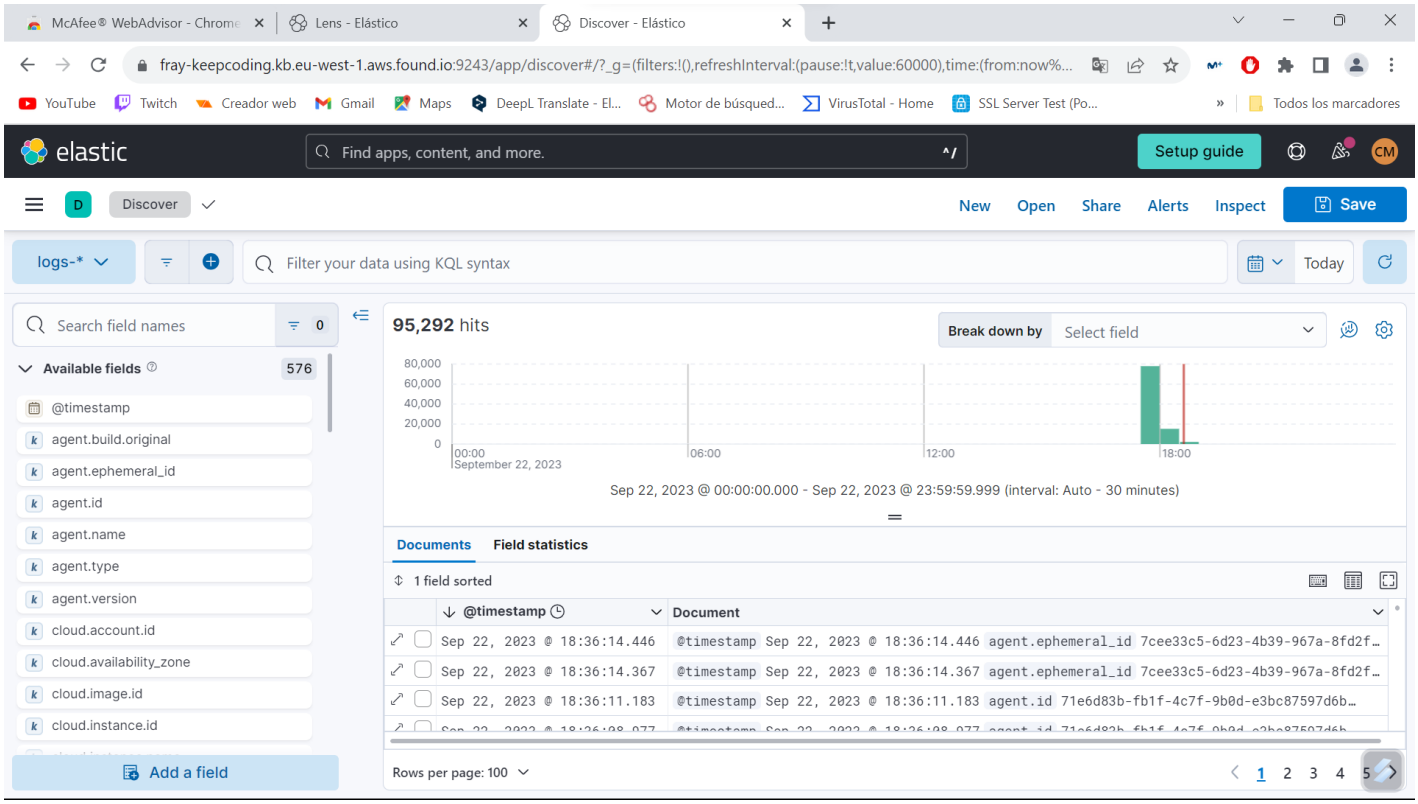
Aquí vemos la información que tiene de nuestro equipo.

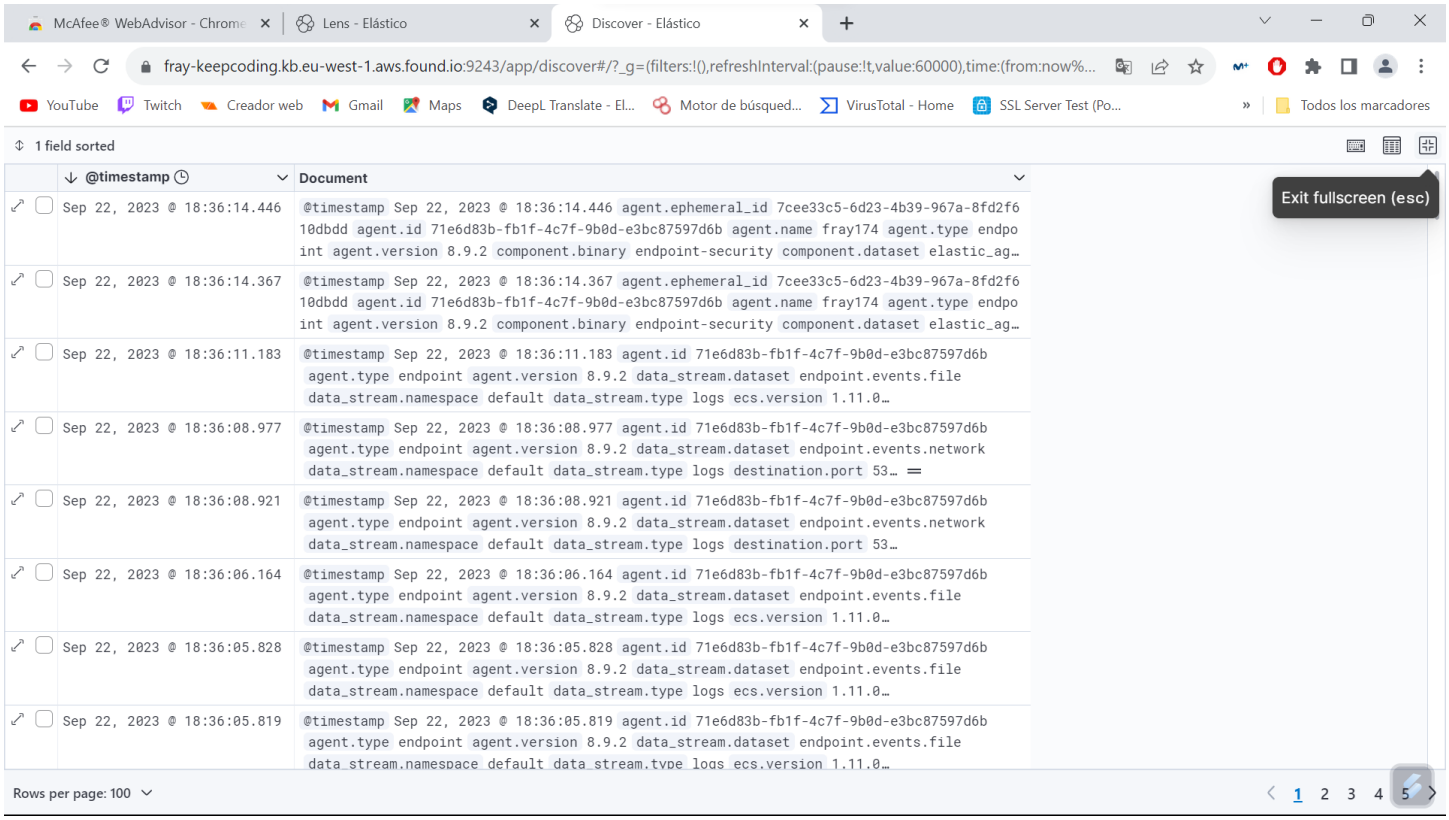


A través del Elastic podemos interactuar con la consola via kibana, en este caso estamos viendo los comportamientos del sistema y podríamos eliminar algún comportamiento anómalo si quisiéramos.

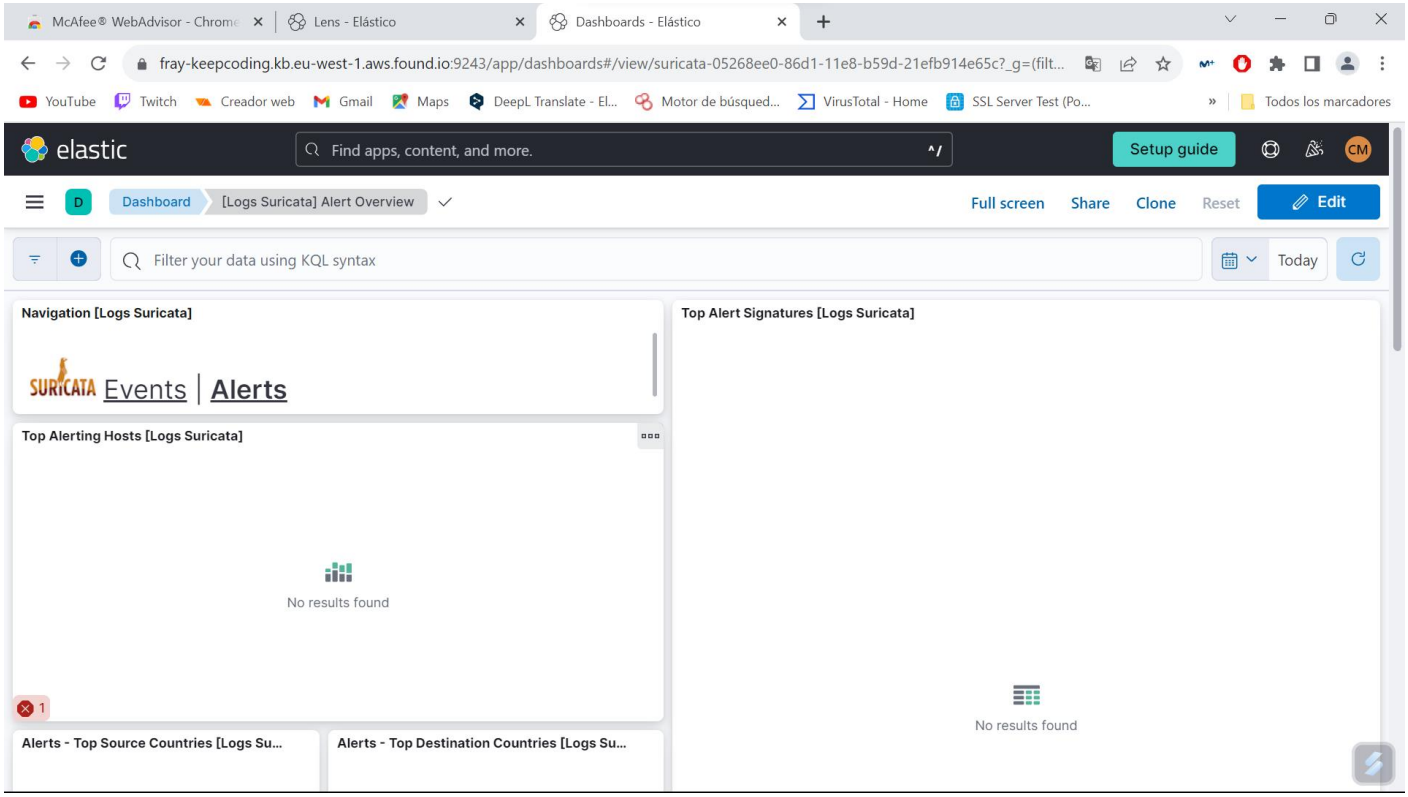


Lo siguiente que haremos es añadir la integración de Suricata y la política que vamos a describir es /var/log/jsonsuricata/eve. Para sacar la información.

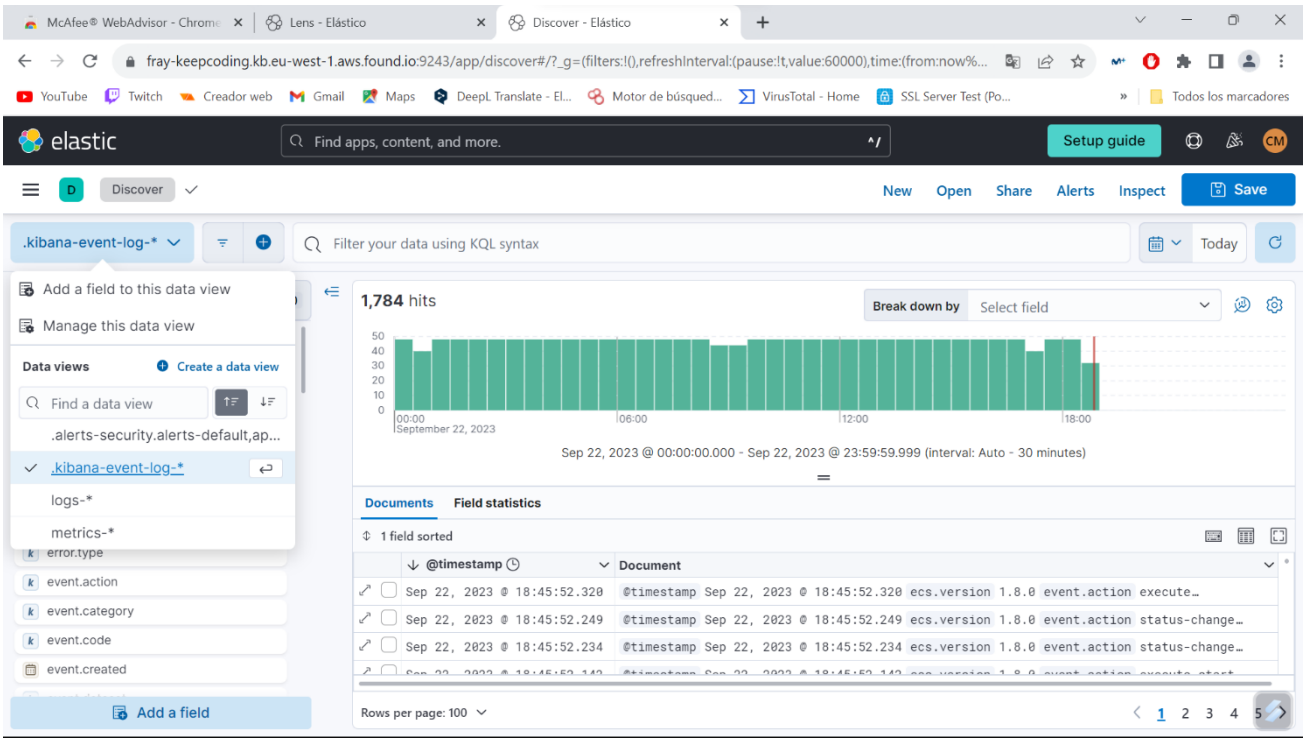




Ya podemos observar como Jason se integra dentro del Elastic en forma de contenido y nos empieza proporcionar información.

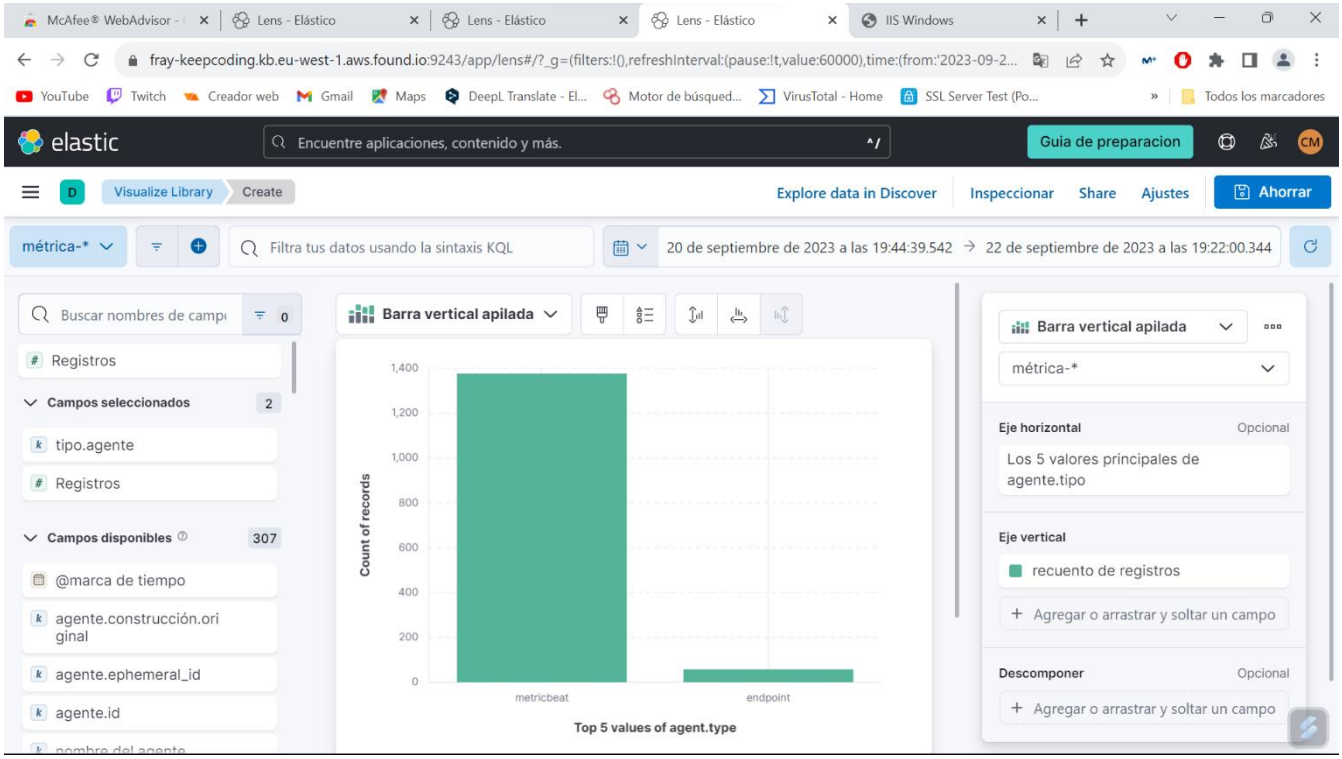


A través de Suricata en Elastic podríamos ver si tuviéramos alguna alerta en este caso no tenemos ninguna por lo que no se visualizan.

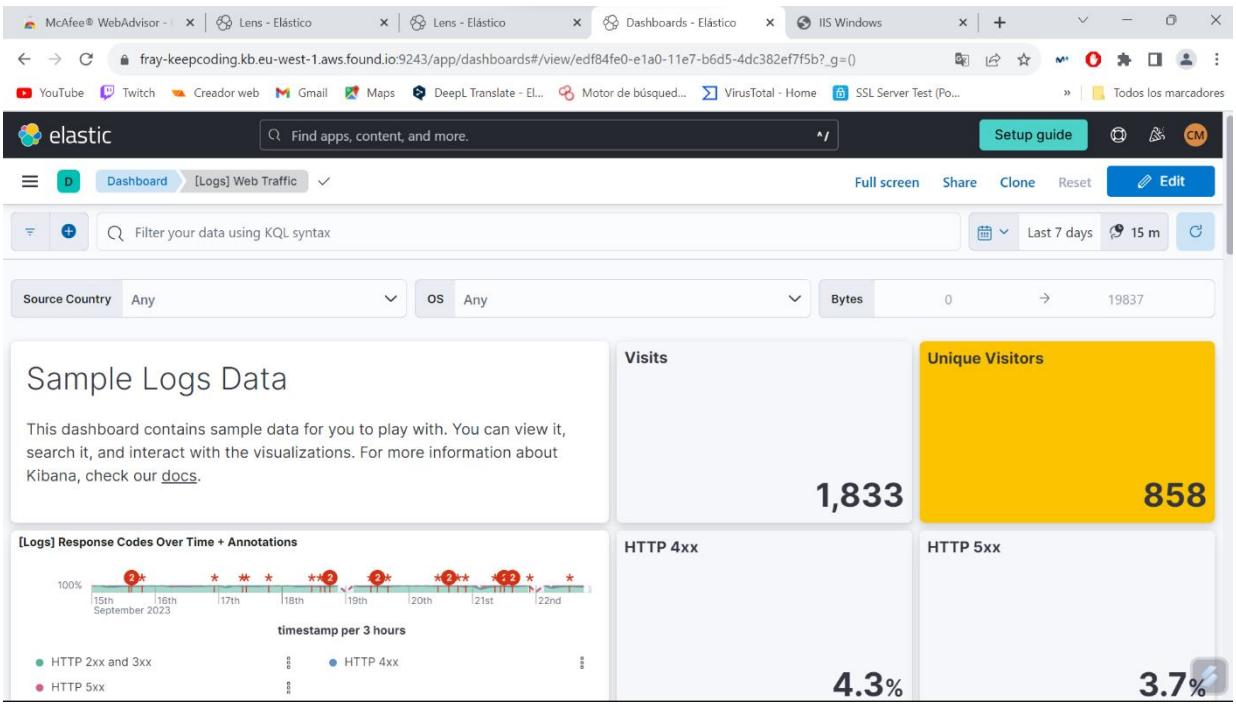


Dentro del Elastic podríamos generar mucha información de nuestro equipo, aquí podemos ver otros datos que nos proporciona a través de

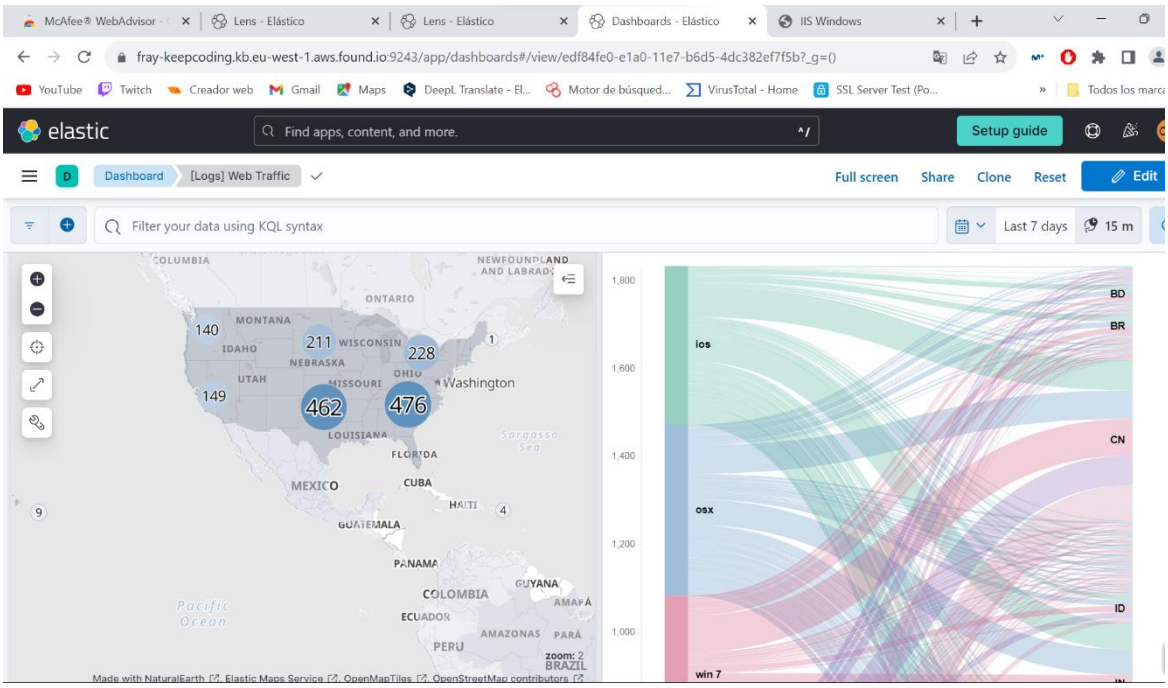
Kibana. Podemos ver también como nos monta un gráfico con todos los hits generados.



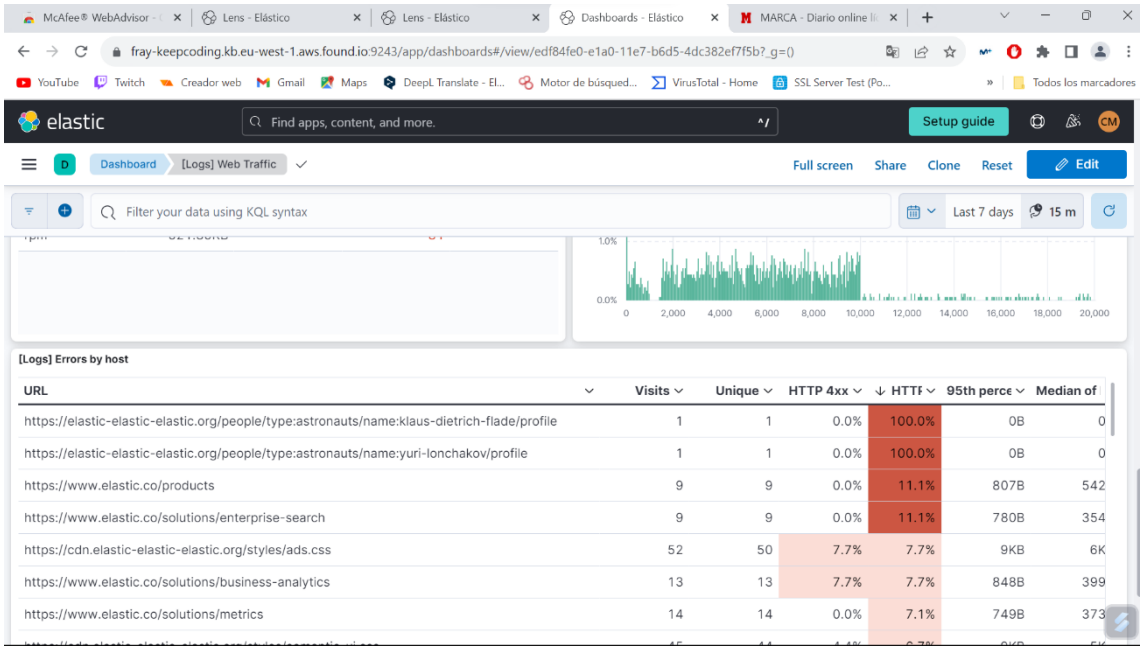
Mas información que nos transmite Elastic son métricas, aquí tenemos un gráfico de los tipos de agentes.



Podemos ver también los Logs del trafico de web, vemos el nº de visitante, visitantes únicos.



Vemos todas las consultas que se han hecho desde los distintos sitios.



Y por último aquí tenemos la correlación, que nos especifica que hemos descargado, errores que nos da.