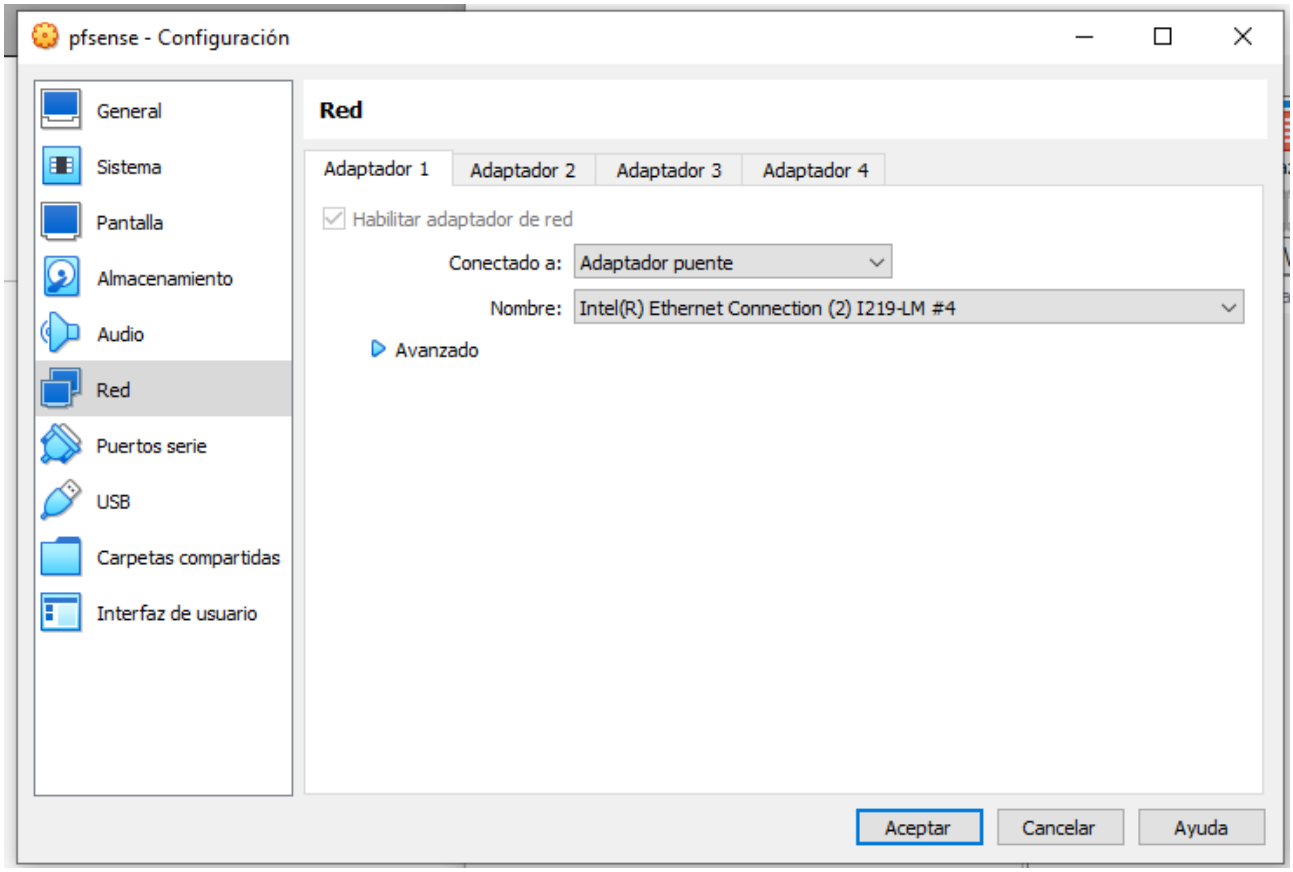
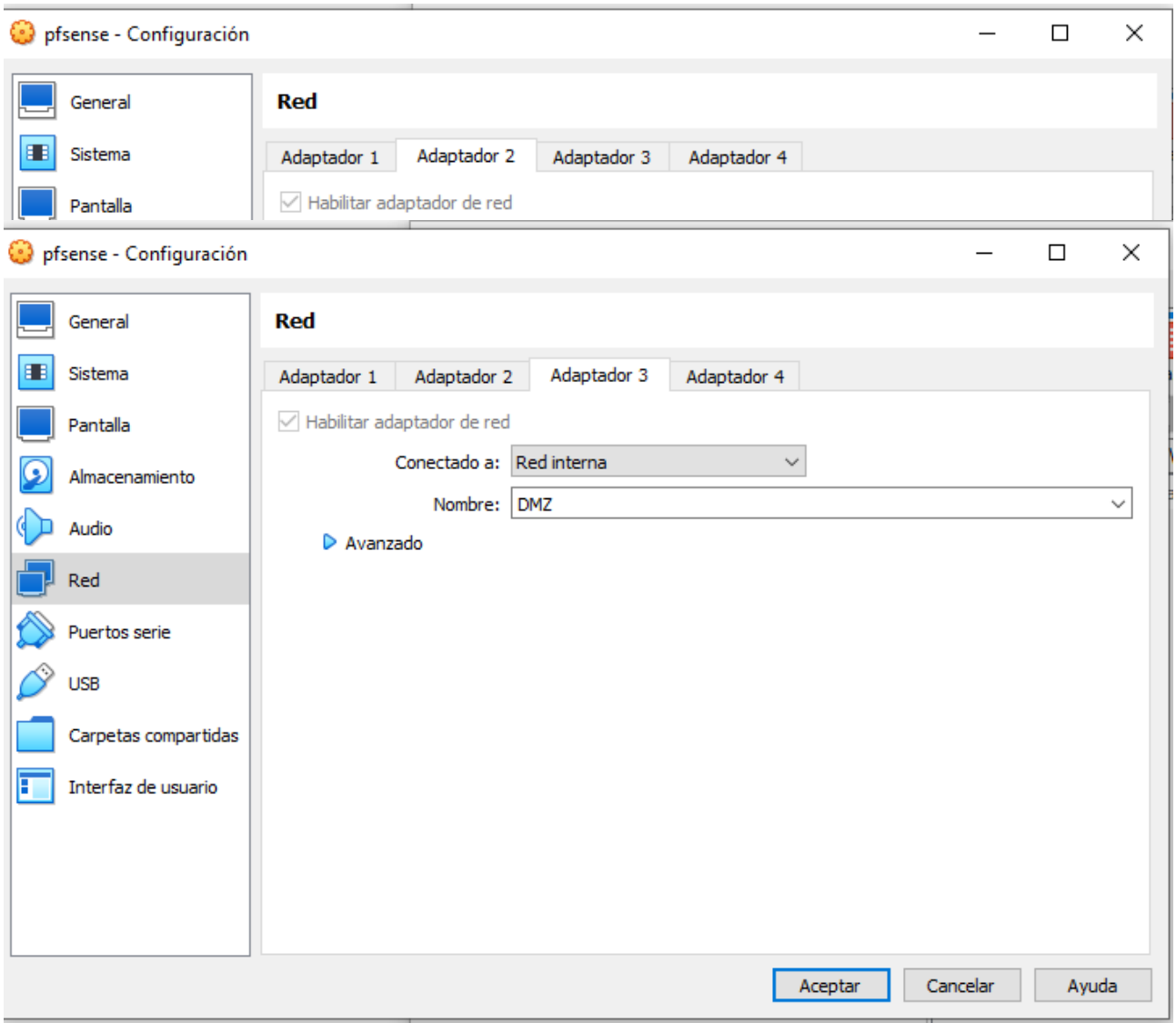
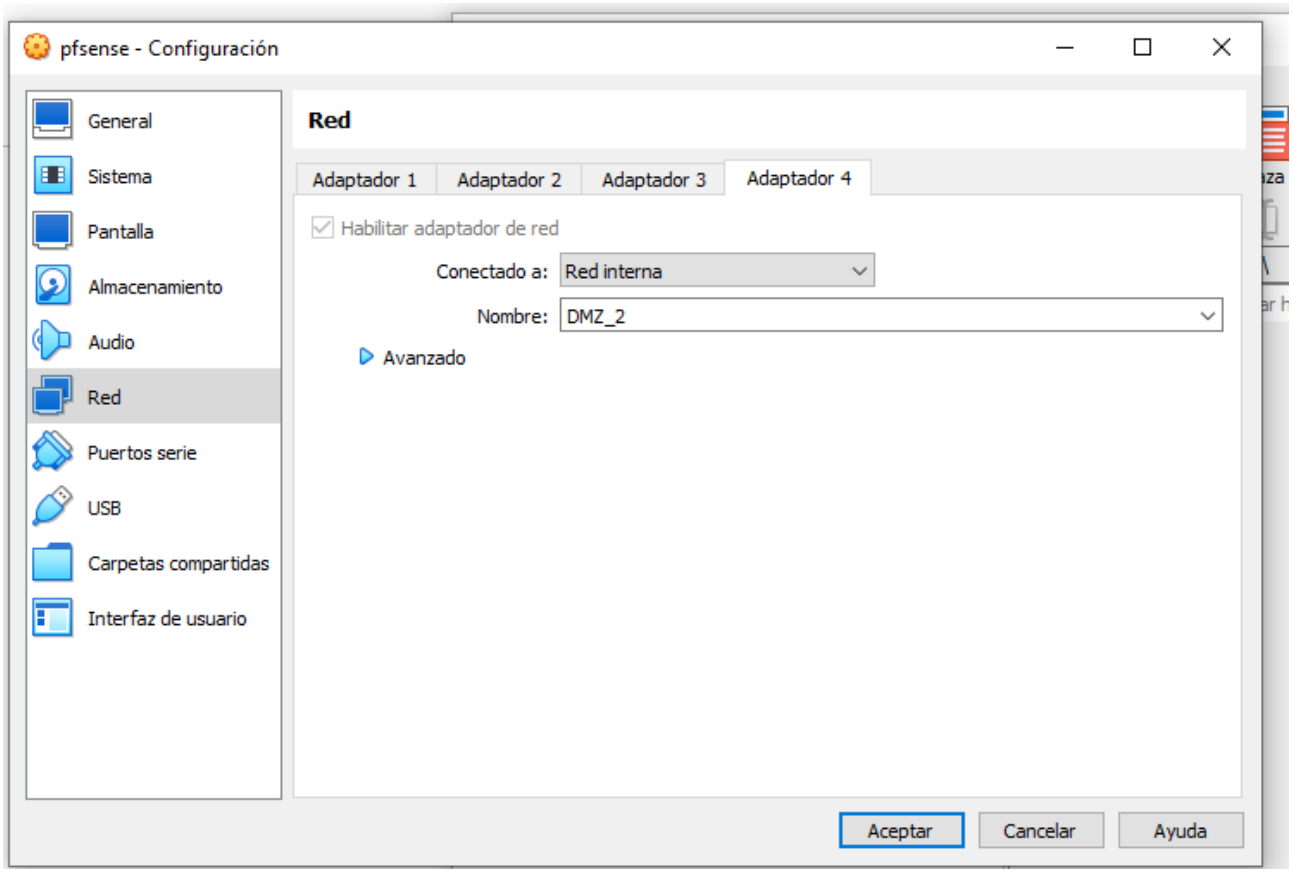
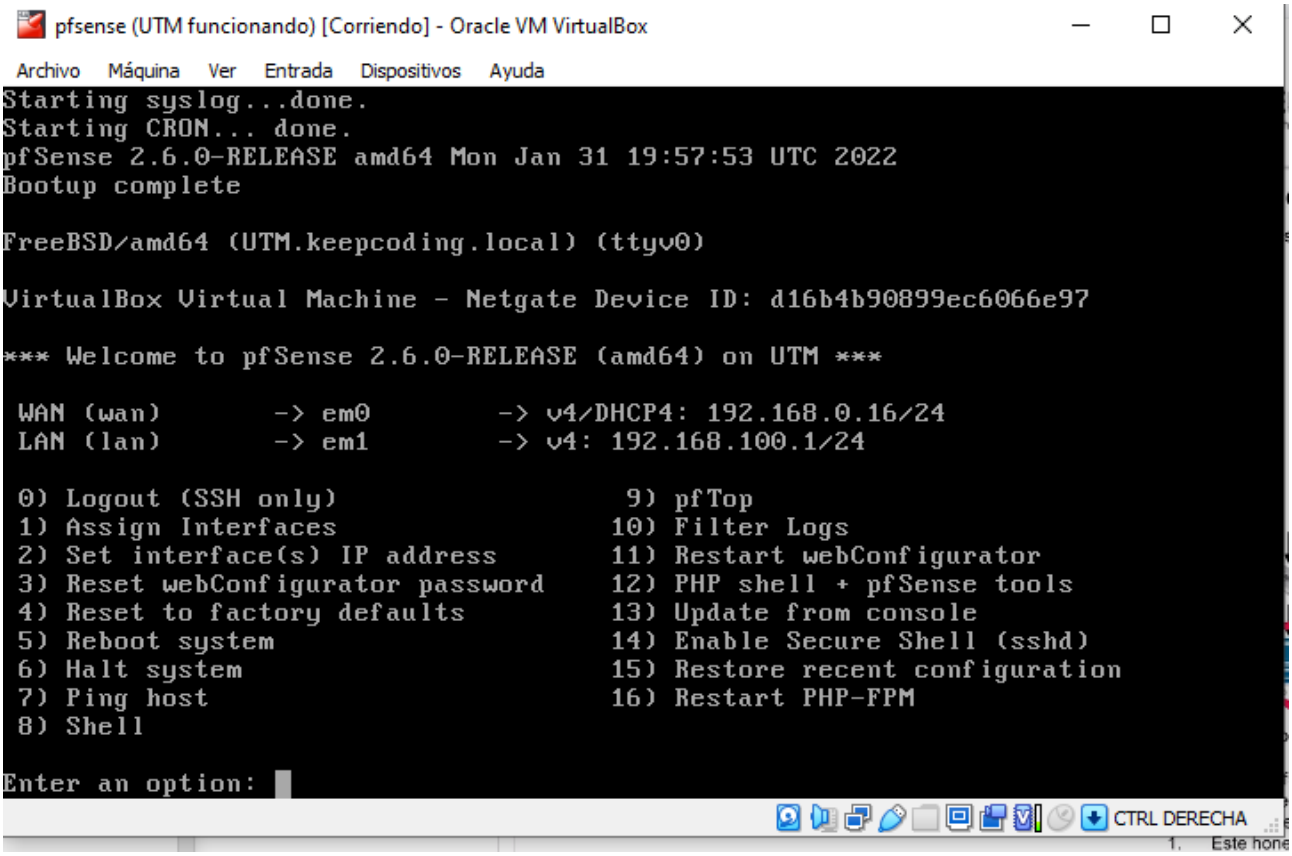
MONTAJE DE INFRAESTRUTURA



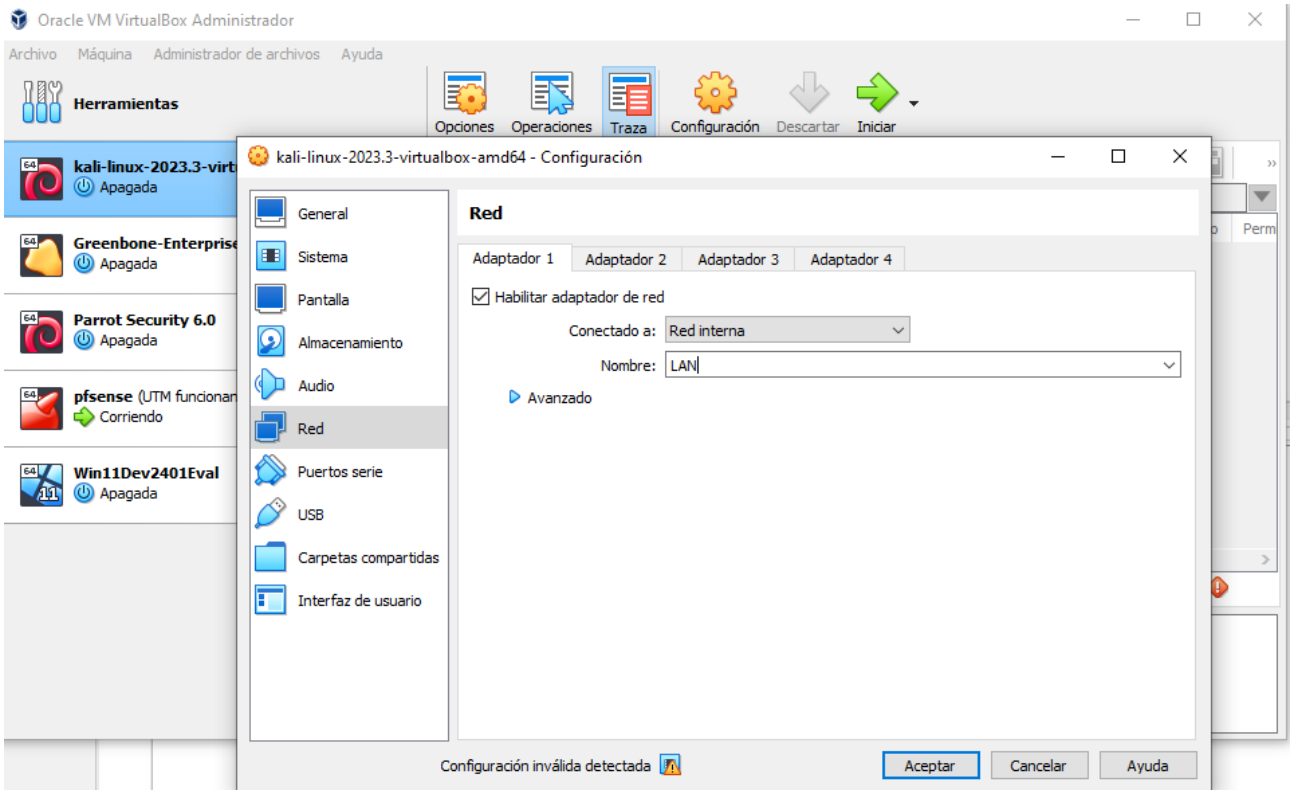




arrancamos la Unified Threat Management (UTM)

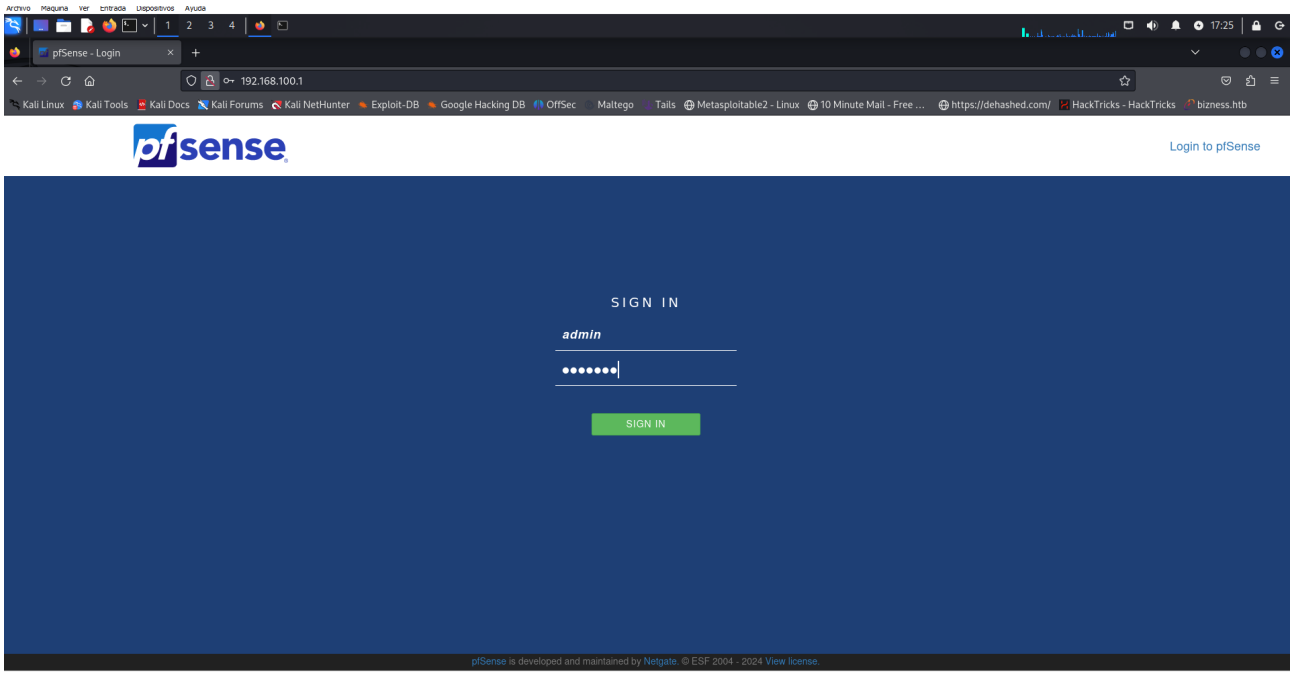


configuramos la kali en red interna LAN

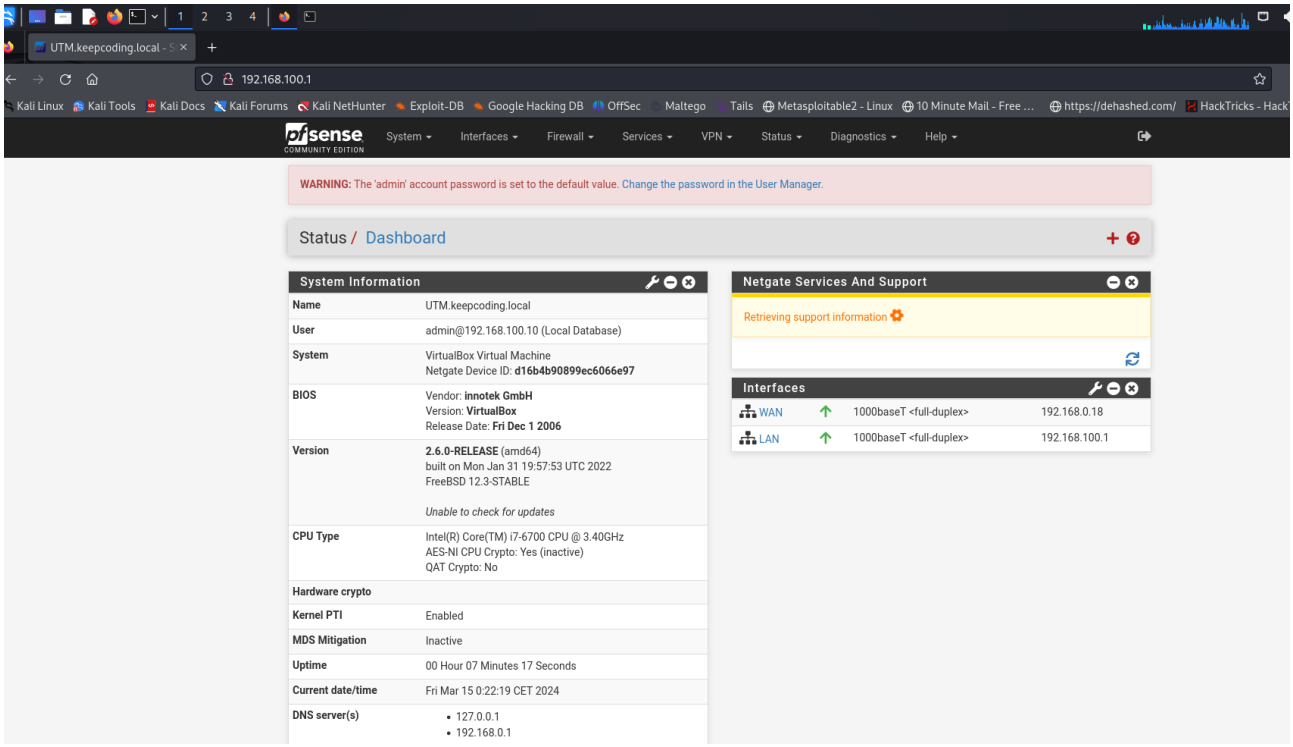


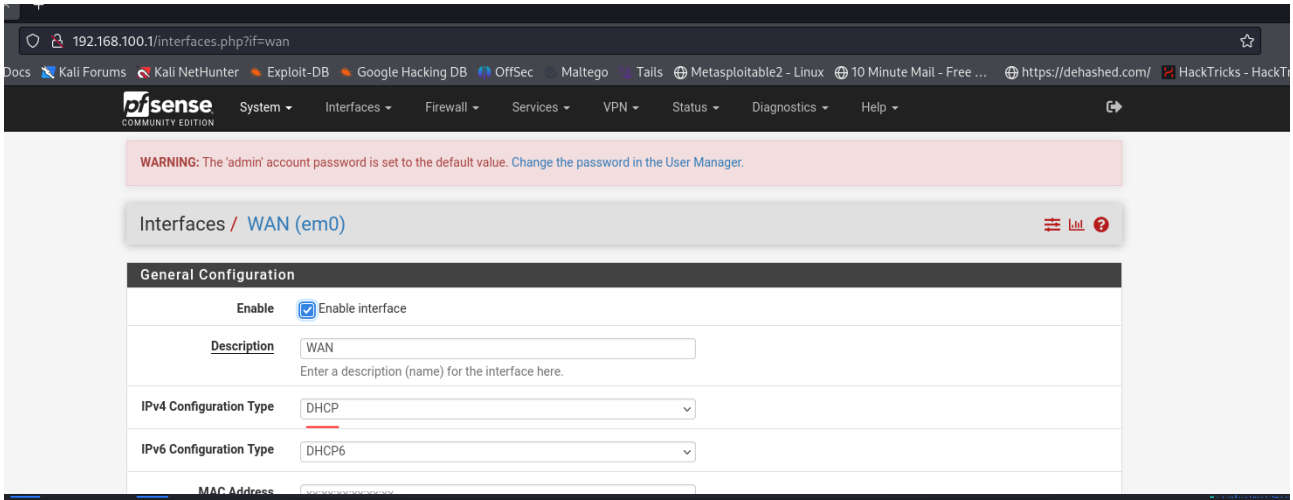
Arrancamos la kali e introducimos en el navegador la ip del adaptador LAN, en mi caso:

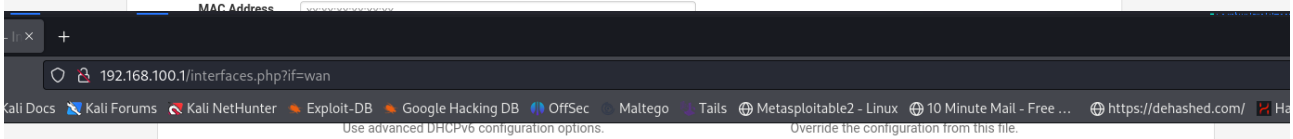
192.168.100.1



usuario admin, password pfsense







Use IPv4 connectivity as parent interface	☐ Request a IPv6 prefix/information through the IPv4 connectivity link
Request only an IPv6 prefix	☐ Only request an IPv6 prefix, do not request an IPv6 address
DHCPv6 Prefix Delegation size	64 The value in this field is the delegated prefix length provided by the DHCPv6 server. Normally specified by the ISP.
Send IPv6 prefix hint	☐ Send an IPv6 prefix hint to indicate the desired prefix size for delegation
Debug	☐ Start DHCP6 client in debug mode
Do not wait for a RA	☐ Required by some ISPs, especially those not using PPPoE
Do not allow PD/Address release	☐ dhcp6c will send a release to the ISP on exit, some ISPs then release the allocated address or prefix. This option prevents that signal ever being sent

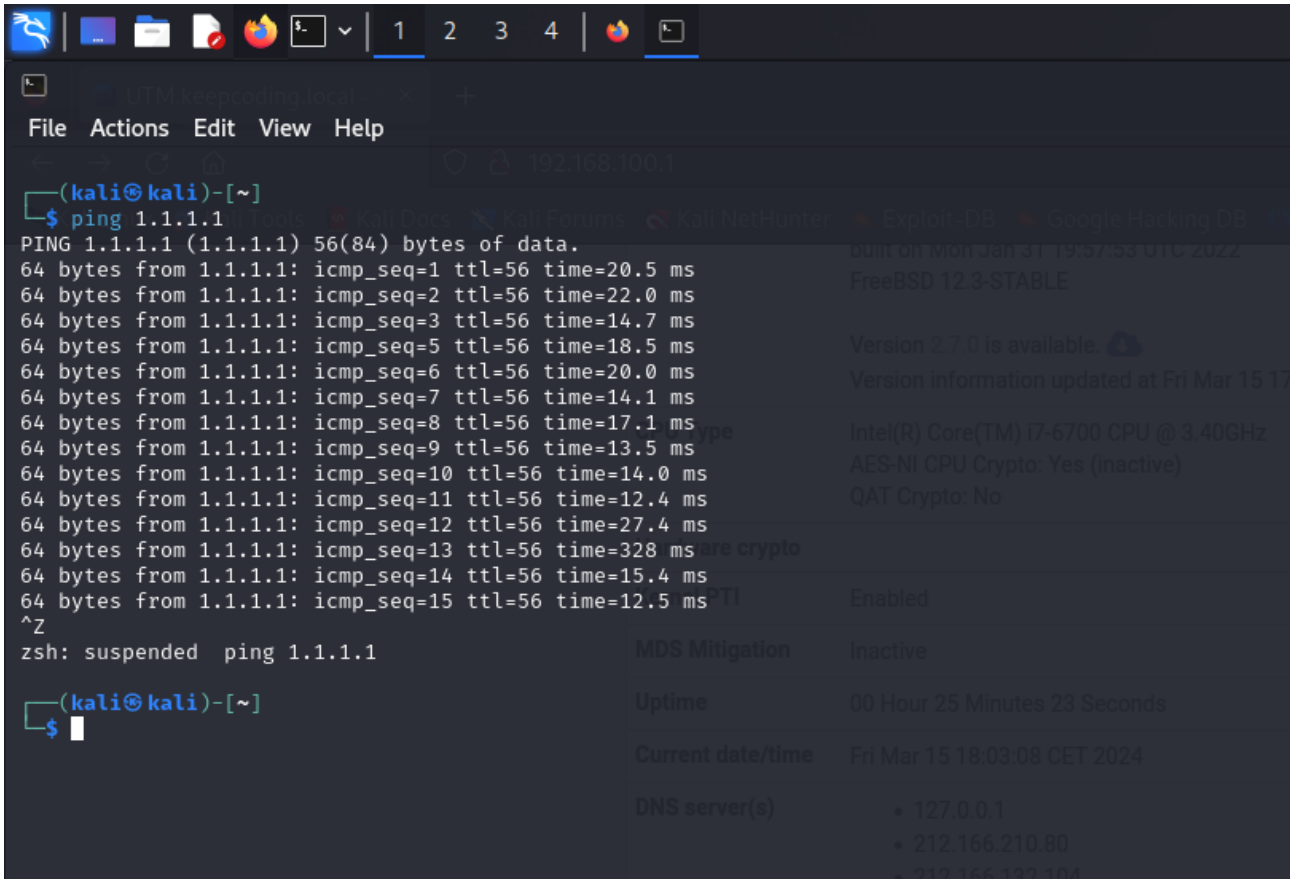
Reserved Networks

Block private networks and loopback addresses	☐ Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.
Block bogon networks	☐ Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received. This option should only be used on external interfaces (WANs), it is not necessary on local interfaces and it can potentially block required local traffic. Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.

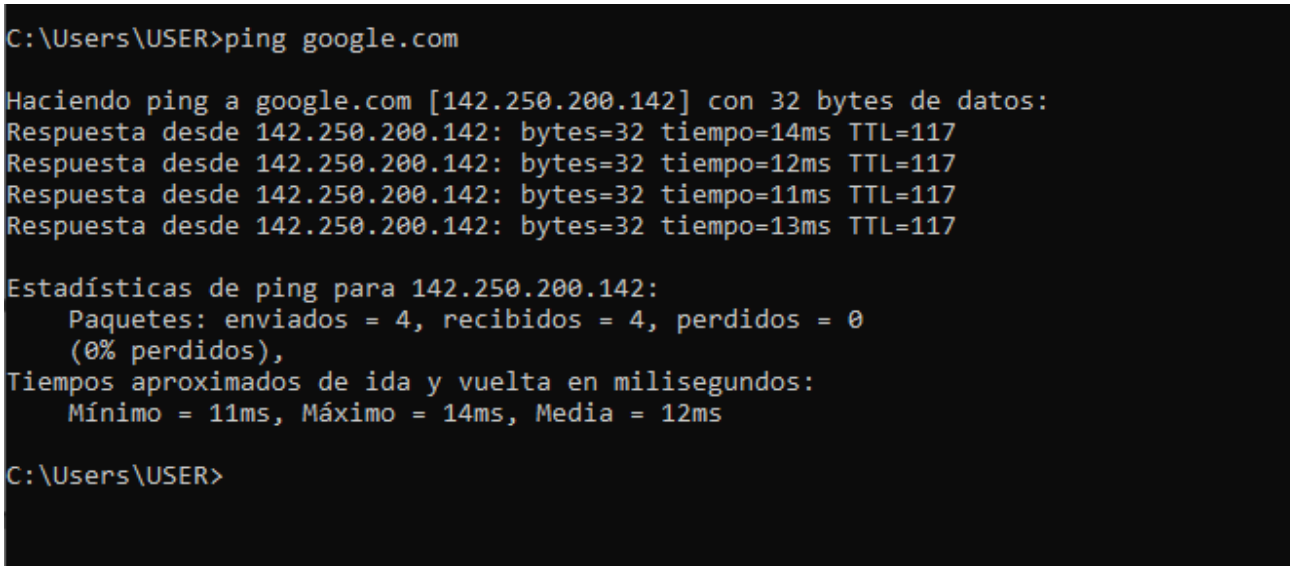
Save

CONFIGURACIÓN DE LAS INTERFACES

Comprobamos si tenemos accesos a internet en la kali haciendo un ping a 1.1.1.1:



hacemos ping en nuestro sistema windows a google.com

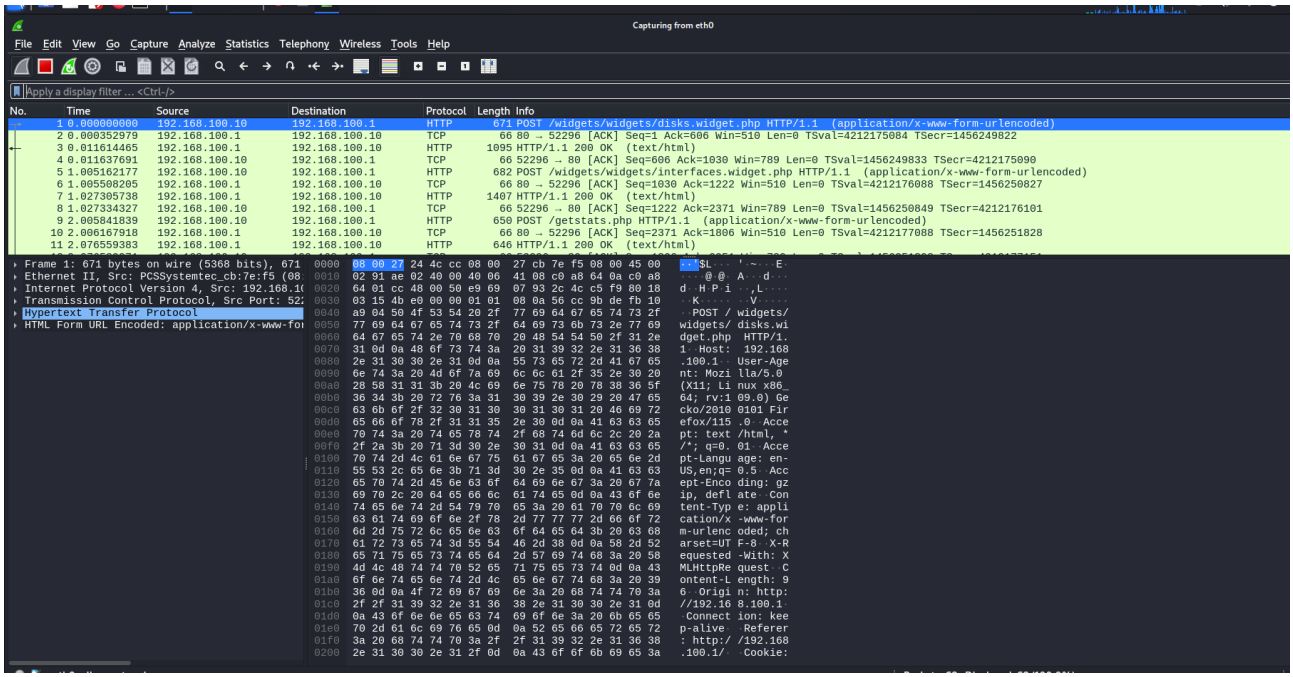


cogemos la ip y la pegamos en kali

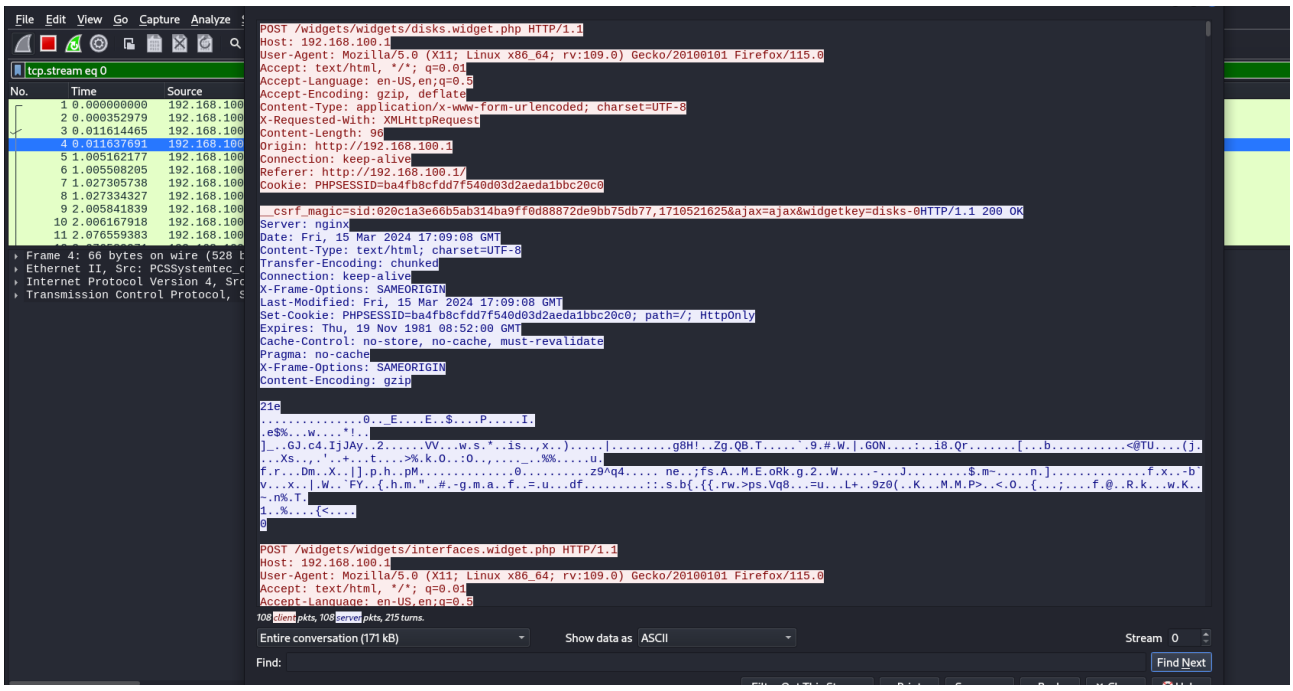
```
┌──(kali㉿kali)-[~]
└─$ ping 142.250.200.142
PING 142.250.200.142 (142.250.200.142) 56(84) bytes of data.
64 bytes from 142.250.200.142: icmp_seq=1 ttl=116 time=19.3 ms
64 bytes from 142.250.200.142: icmp_seq=2 ttl=116 time=14.8 ms
64 bytes from 142.250.200.142: icmp_seq=3 ttl=116 time=20.9 ms
64 bytes from 142.250.200.142: icmp_seq=4 ttl=116 time=24.7 ms
64 bytes from 142.250.200.142: icmp_seq=5 ttl=116 time=16.2 ms
64 bytes from 142.250.200.142: icmp_seq=6 ttl=116 time=14.7 ms
64 bytes from 142.250.200.142: icmp_seq=7 ttl=116 time=13.6 ms
^Z
zsh: suspended  ping 142.250.200.142

┌──(kali㉿kali)-[~]
└─$
```

en wireshark podemos ver el tráfico que está pasando por la interface de red eth0:



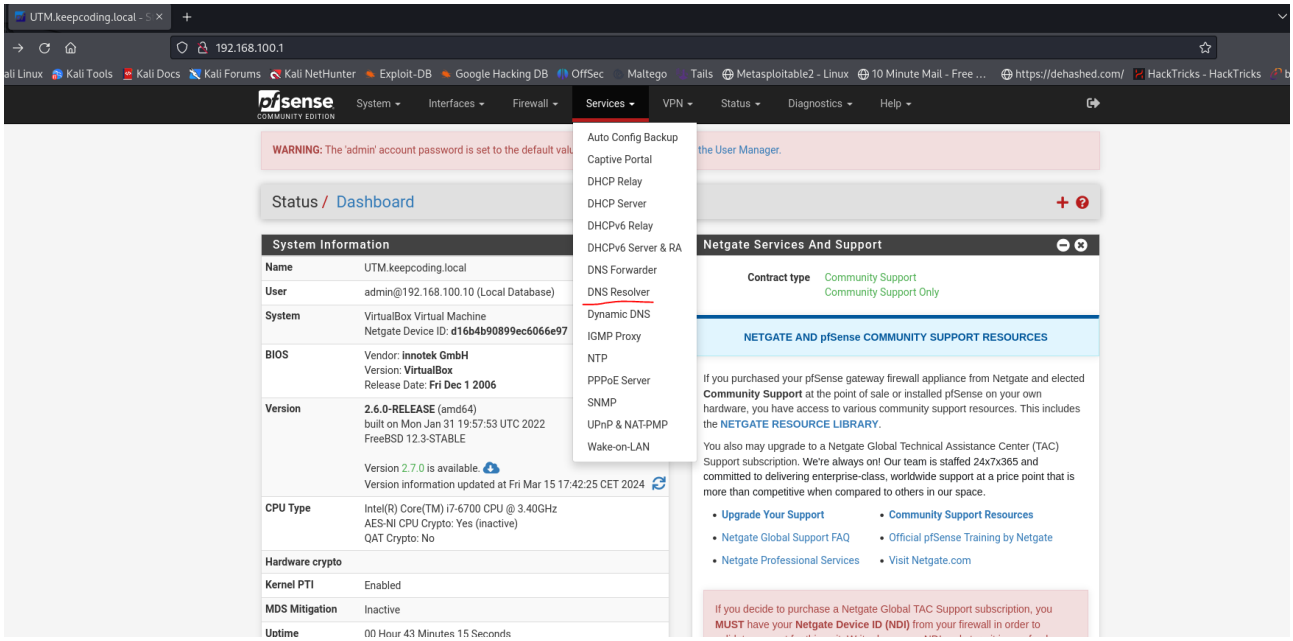
hacemos click botón derecho en alguna de las tramas, Follow y TCP Stream y vemos todos los paquetes del tráfico:



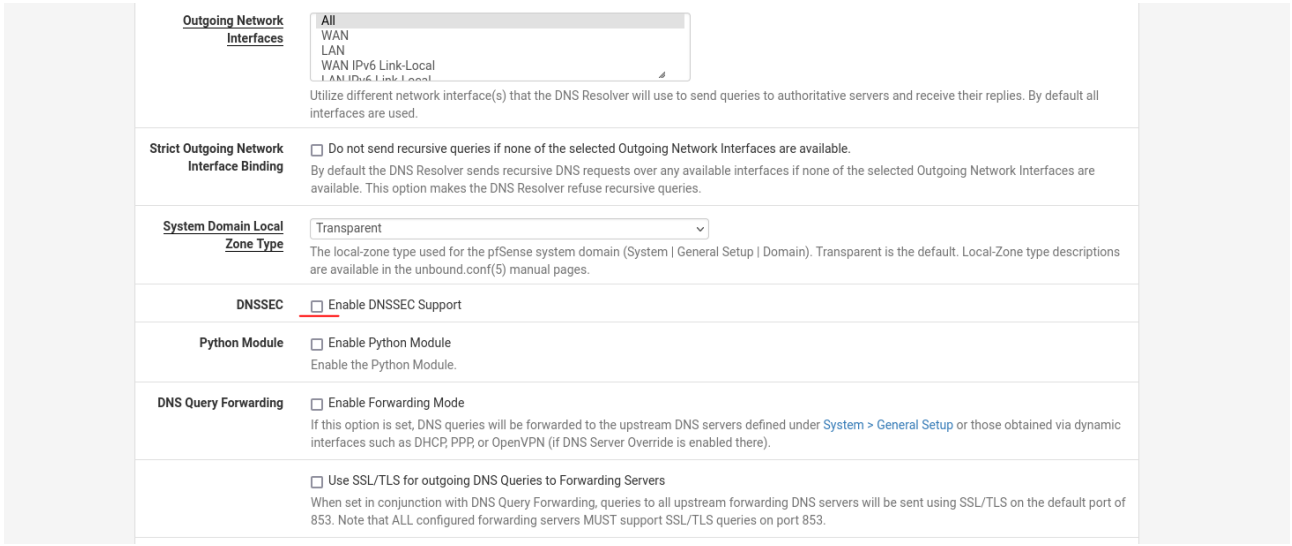
para ver la información del tráfico.

Configuramos el UTM:

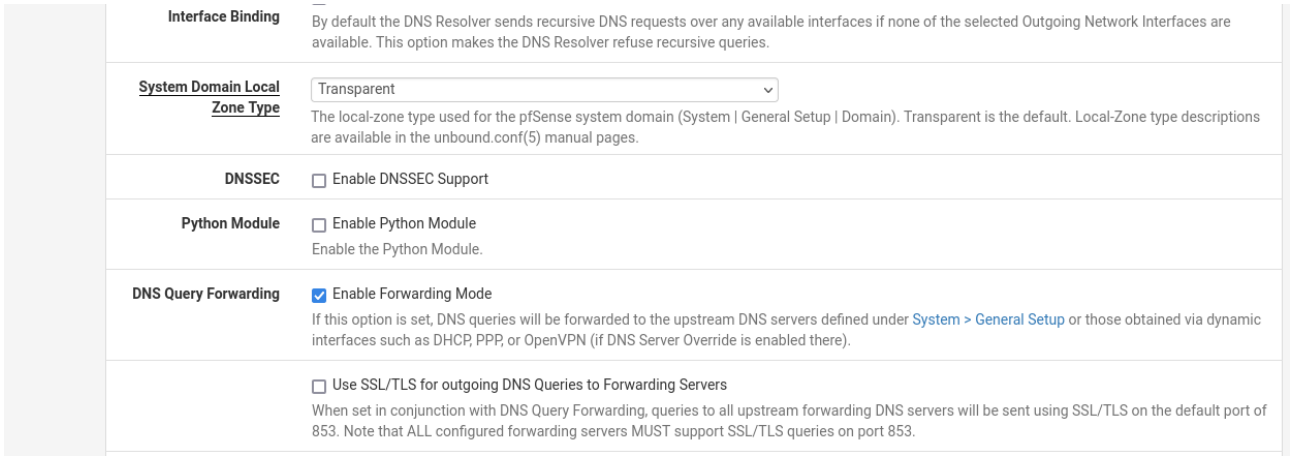
vamos a Services y DNS Resolver



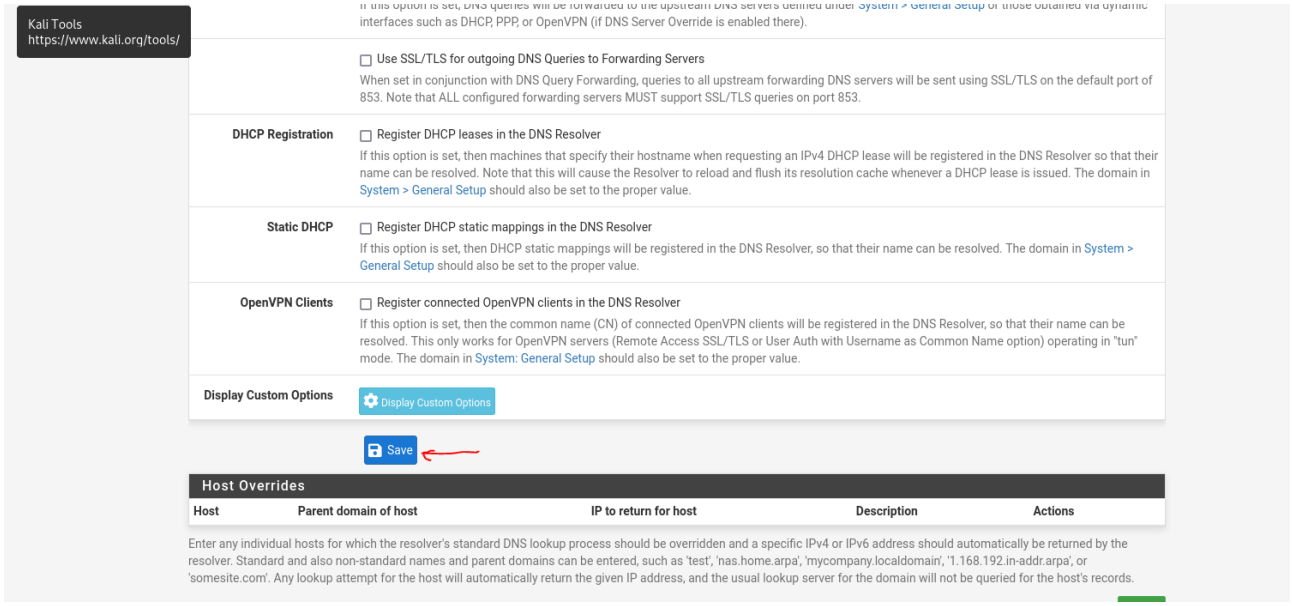
deschekamos el DNSSEC que es un protocolo utilizado para firmar la respuesta DNS (asegura que la respuesta no ha sido modificada):



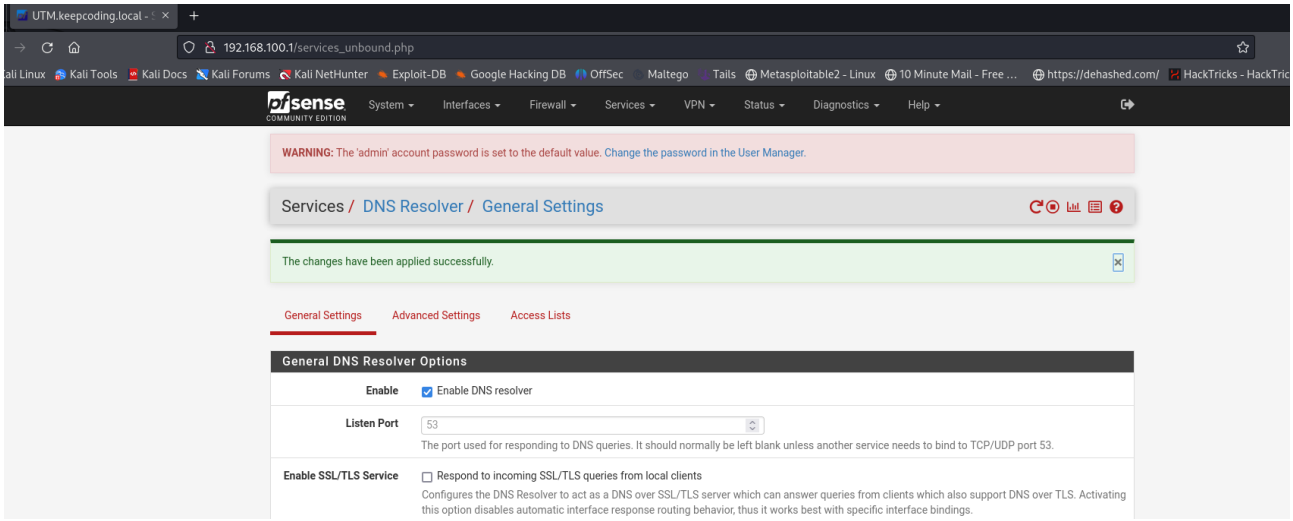
habilitamos el DNS Query Forwarding para enviar la consulta al servidor secundario el 1.1.1.1, en el caso de que PFSENSE no sea capaz de enviarla:



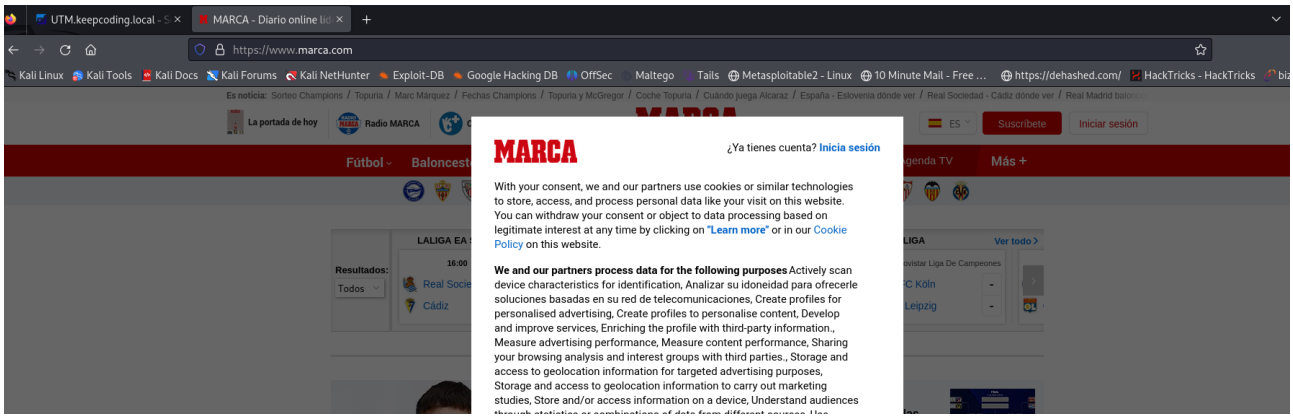
hacemos click en Save para guardar la configuración DNS:



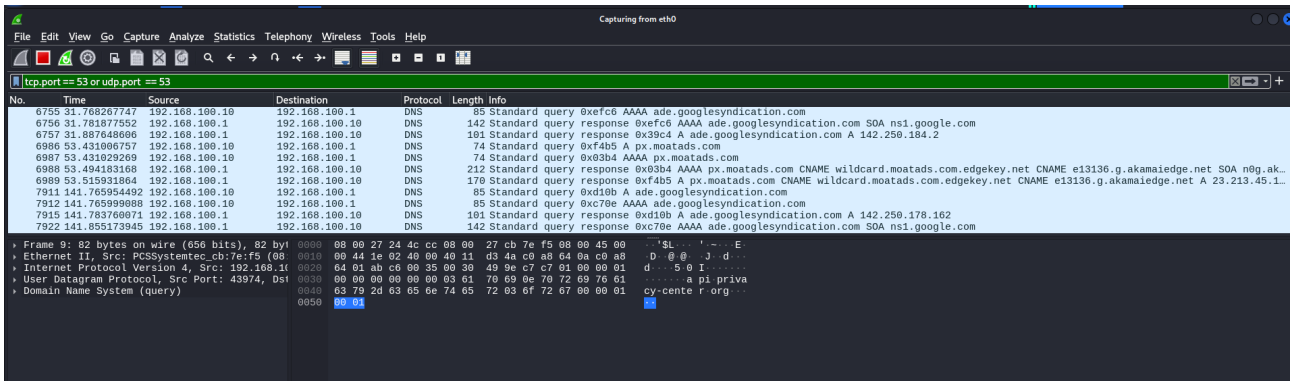
y damos a Apply Changes:



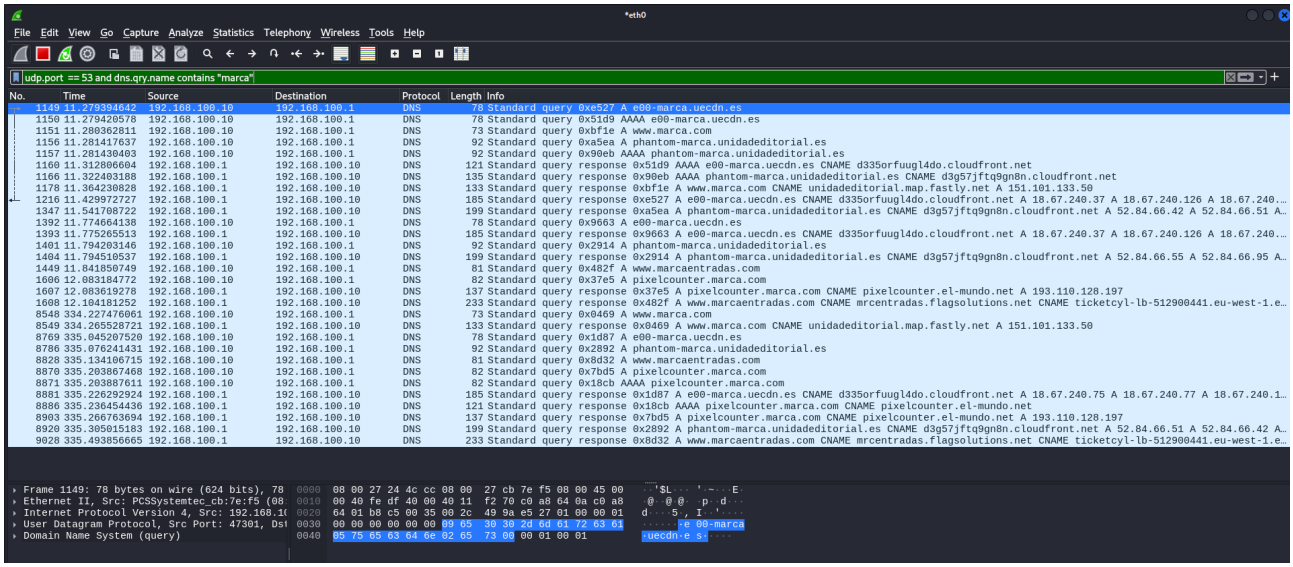
comprobamos en el navegador que tenemos acceso a marca.com



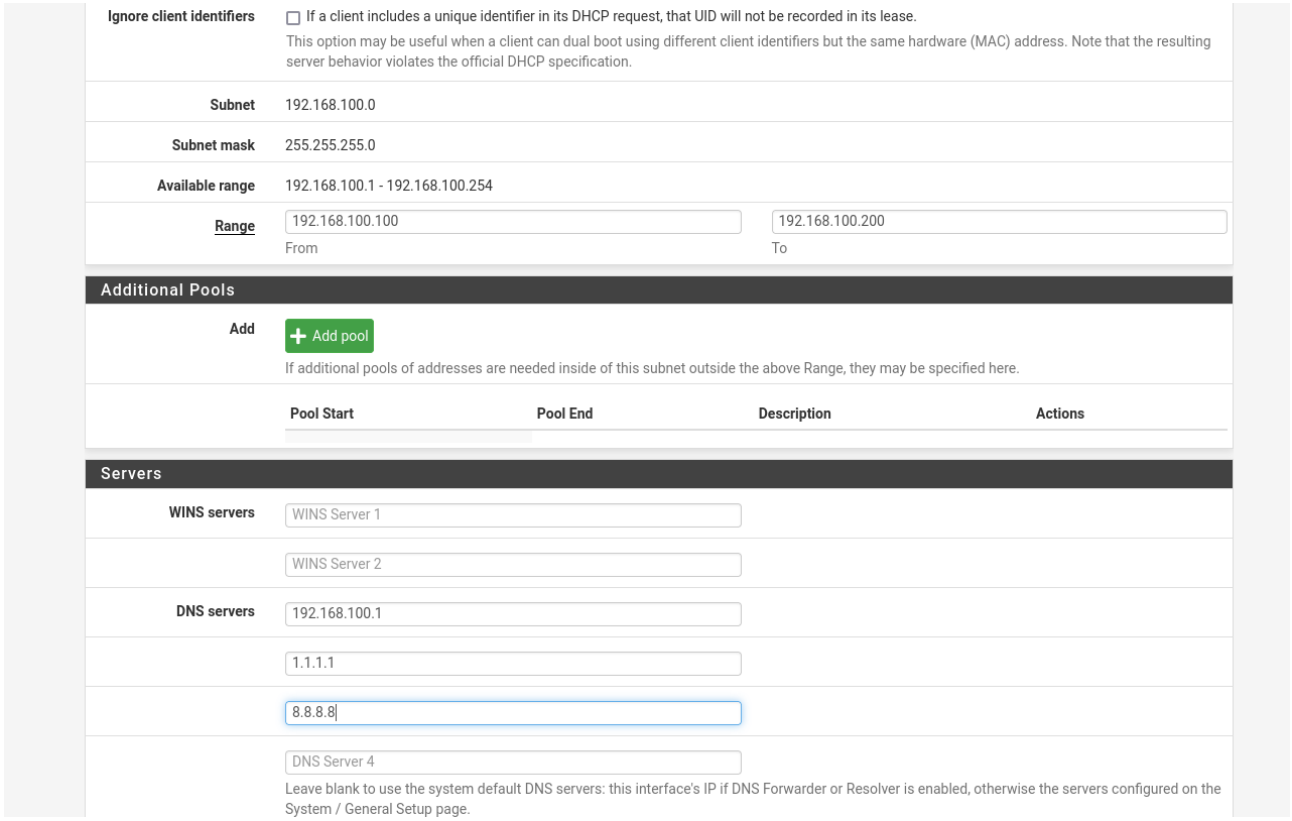
y vemos el tráfico en wireshark con el filtro tcp.port == 53 or udp.port == 53:



o con el filtro udp.port == 53 and qry.name contains “marca”



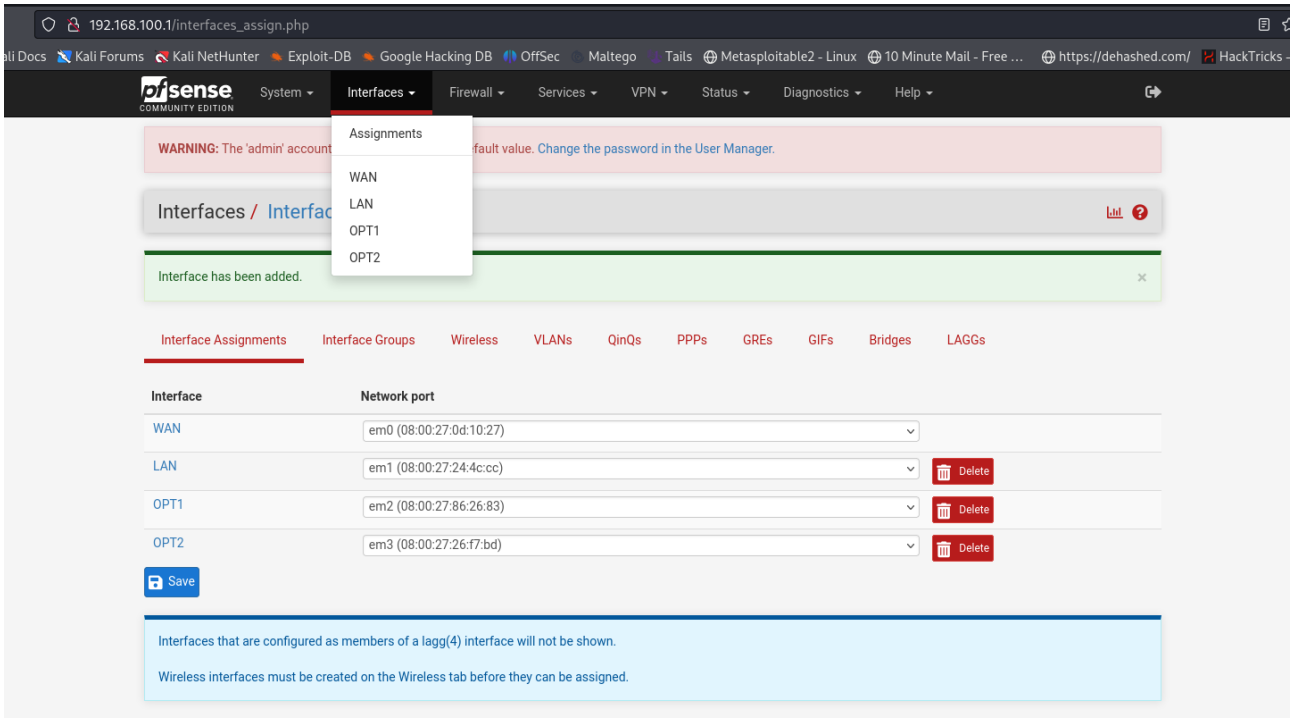
vemos todo el tráfico que interceptamos con pfsense hacia marca.com.
Configuramos el rang de ips en DHCP Server, desde la 192.168.100.100 hasta la 192.168.100.200 para conseguir la sured que hemos definido en el esquema, también configuramos un DNS secundario 1.1.1.1 y terciario 8.8.8.8 (google):

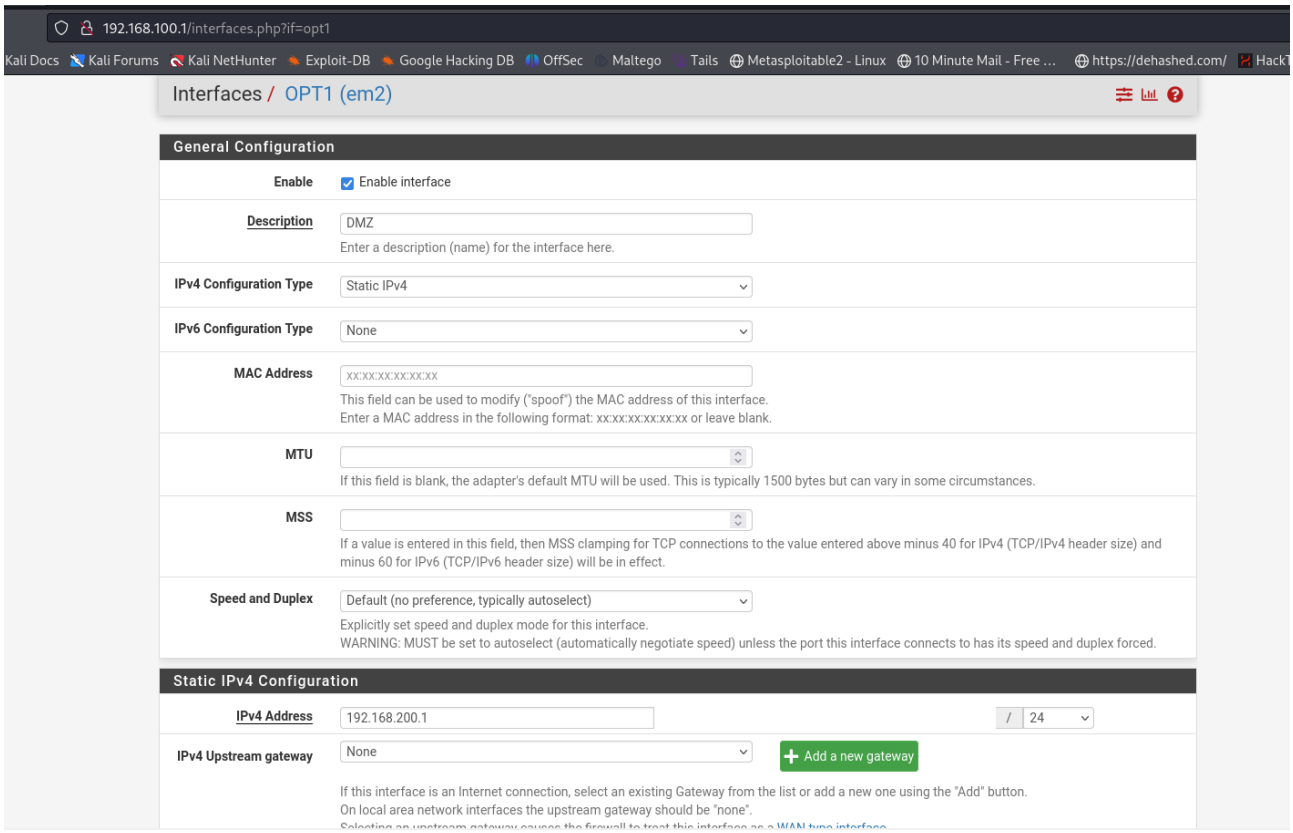


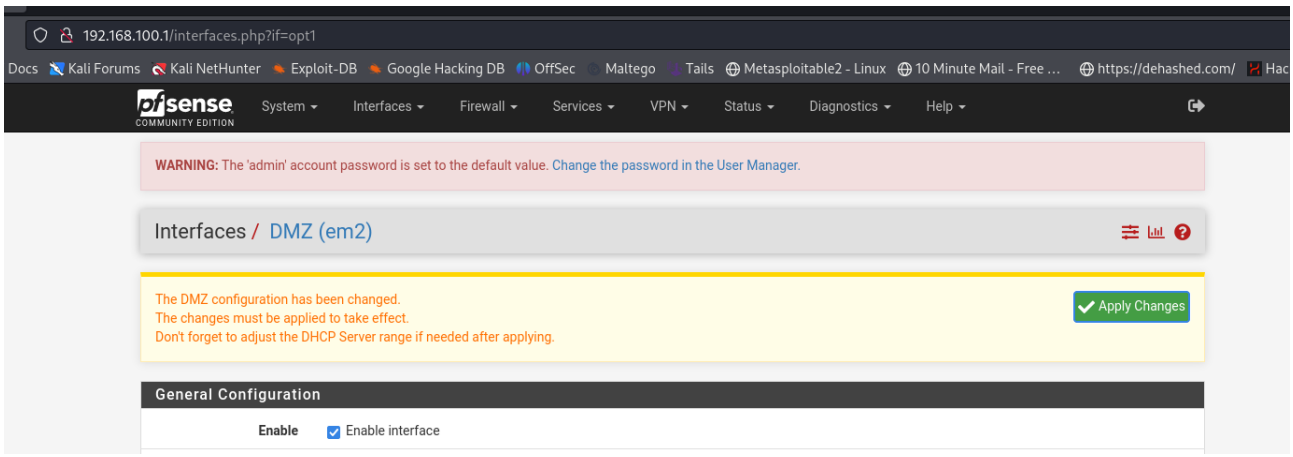
así tendría configurada la red LAN

Configuración de DMZ y DMZ2:

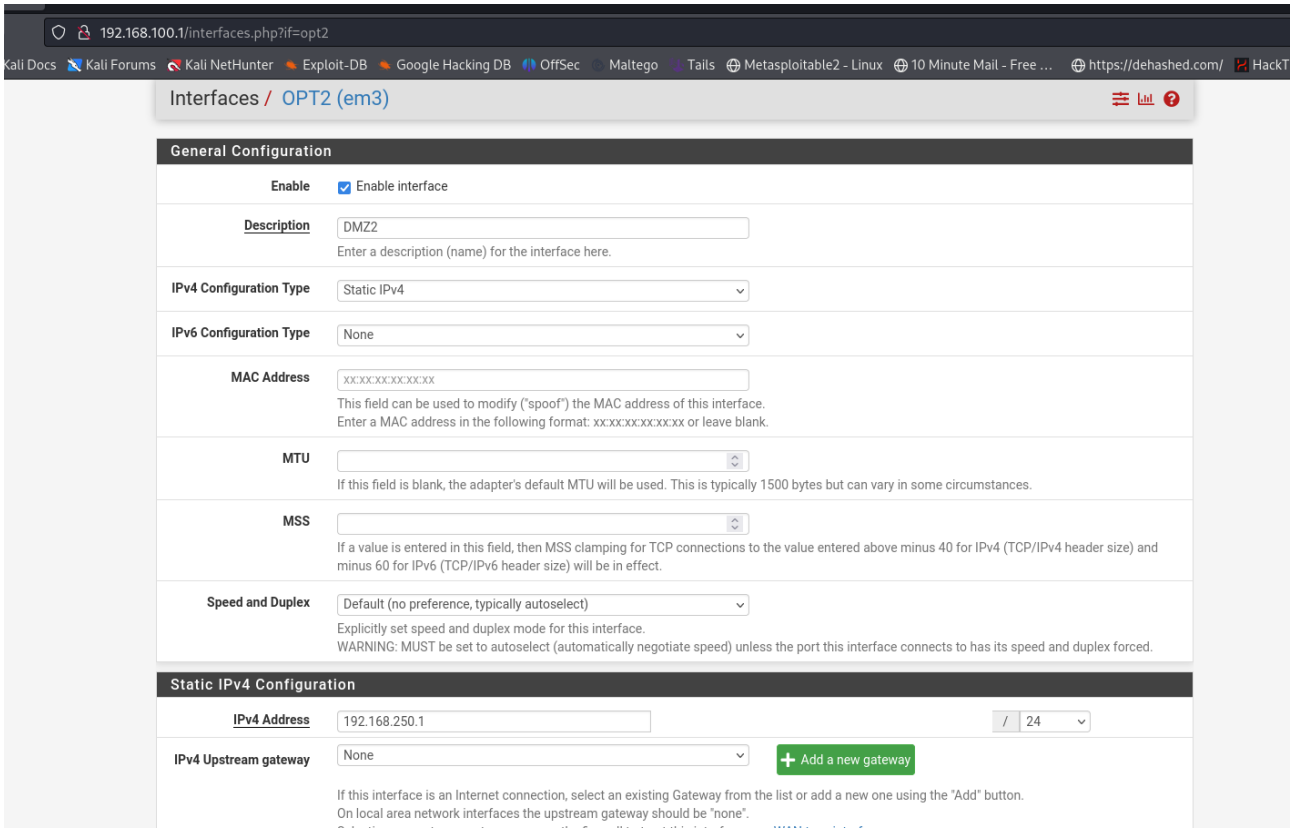
Vamos a Interfaces – Assignments y añadimos, nos saldrán OPT1 y OPT2:

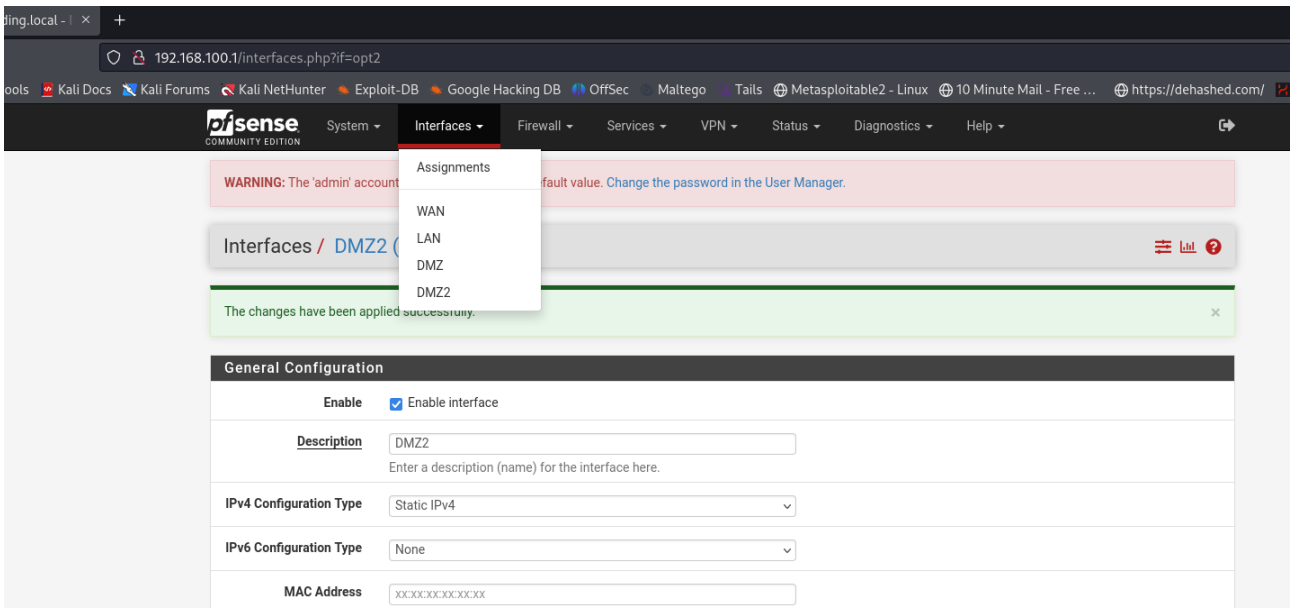

192.168.100.1/interfaces_assign.php
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Maltego
Tails
Metasploitable2 - Linux
10 Minute Mail - Free ...
https://dehashed.com/
HackTricks
pfSense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Assignments
WAN
LAN
OPT1
OPT2
WARNING: The 'admin' account
fault value. Change the password in the User Manager.
Interfaces / Interfac
Interface has been added.
Interface Assignments
Interface Groups
Wireless
VLANs
QinQs
PPPs
GREs
GIFs
Bridges
LAGGs
Interface
Network port
WAN
em0 (08:00:27:0d:10:27)
LAN
em1 (08:00:27:24:4c:cc)
Delete
OPT1
em2 (08:00:27:86:26:83)
Delete
OPT2
em3 (08:00:27:26:f7:bd)
Delete
Save
Interfaces that are configured as members of a lagg(4) interface will not be shown.
Wireless interfaces must be created on the Wireless tab before they can be assigned.


192.168.100.1/interfaces.php?if=opt1
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Maltego
Tails
Metasploitable2 - Linux
10 Minute Mail - Free ...
https://dehashed.com/
Interfaces / OPT1 (em2)
General Configuration
Enable
Enable interface
Description
DMZ
Enter a description (name) for the interface here.
IPv4 Configuration Type
Static IPv4
IPv6 Configuration Type
None
MAC Address
xx:xx:xx:xx:xx:xx
This field can be used to modify ("spoof") the MAC address of this interface.
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.
MTU
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.
MSS
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.
Speed and Duplex
Default (no preference, typically autoselect)
Explicitly set speed and duplex mode for this interface.
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.
Static IPv4 Configuration
IPv4 Address
192.168.200.1
/ 24
IPv4 Upstream gateway
None
Add a new gateway
If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.
On local area network interfaces the upstream gateway should be "none".

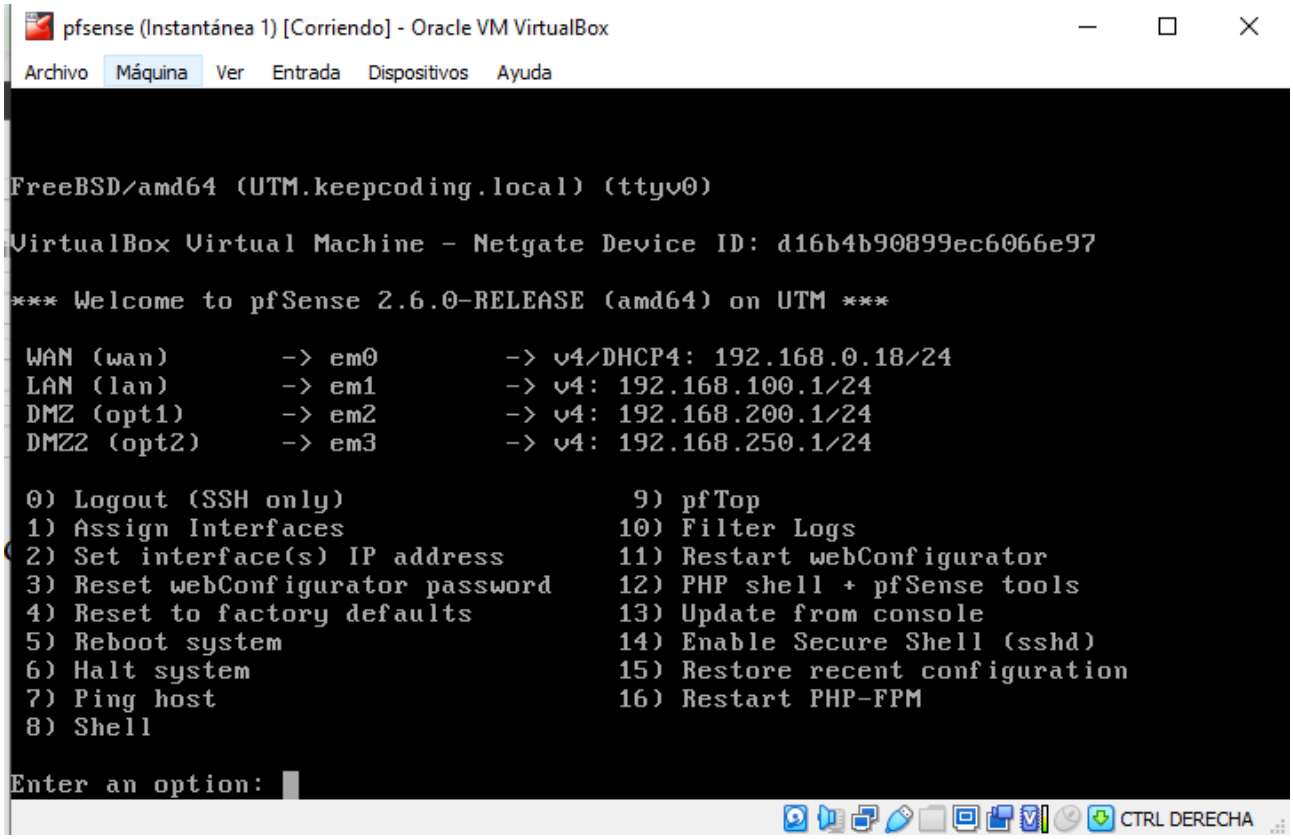


Configuramos la DMZ2:

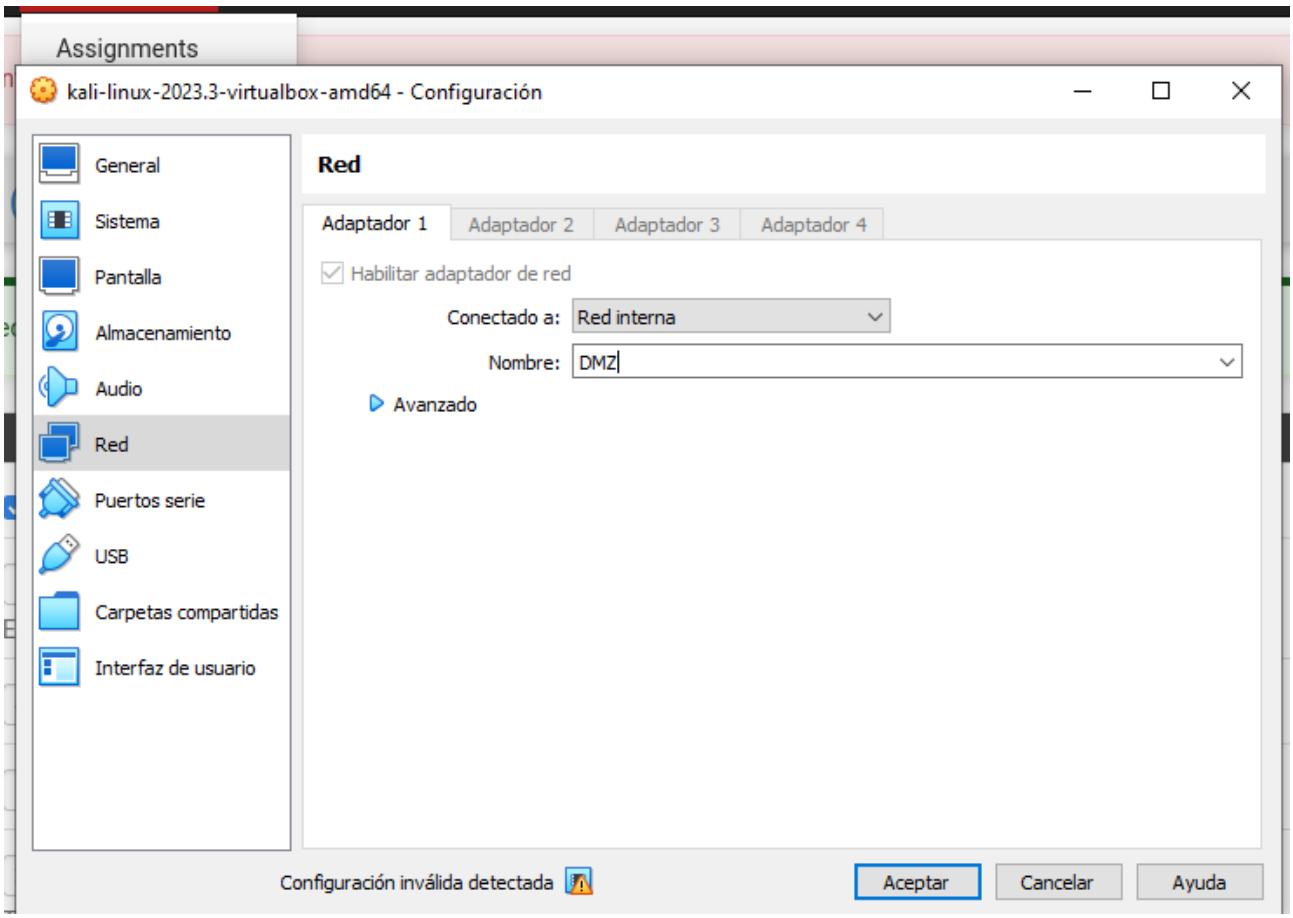




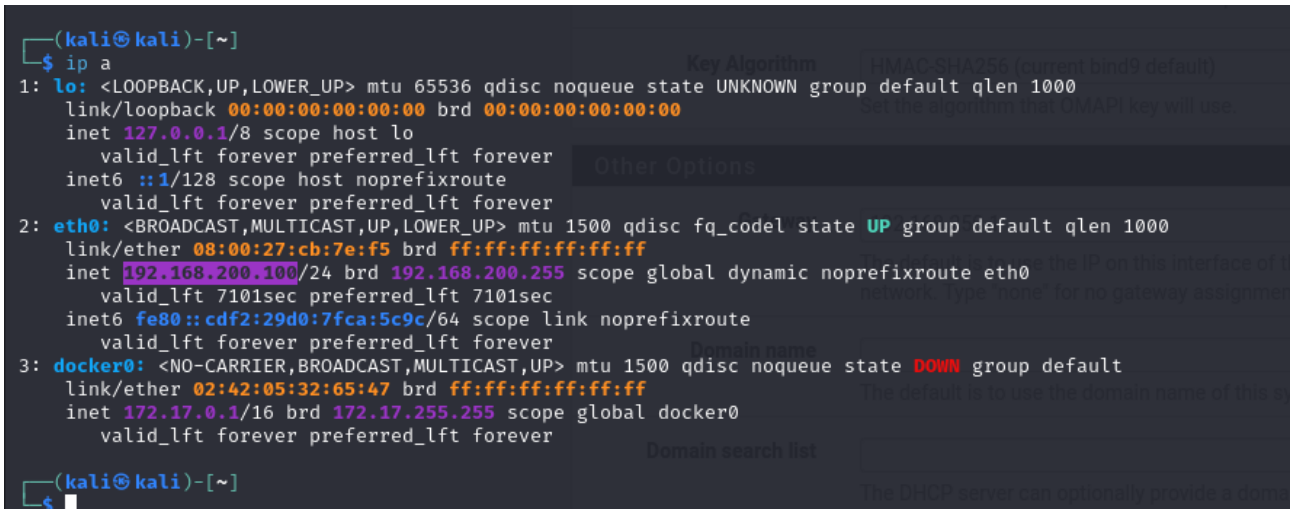
vamos a pfsense y comprobamos todas las redes configuradas:



vamos a la kali y cambiamos la red LAN a DMZ



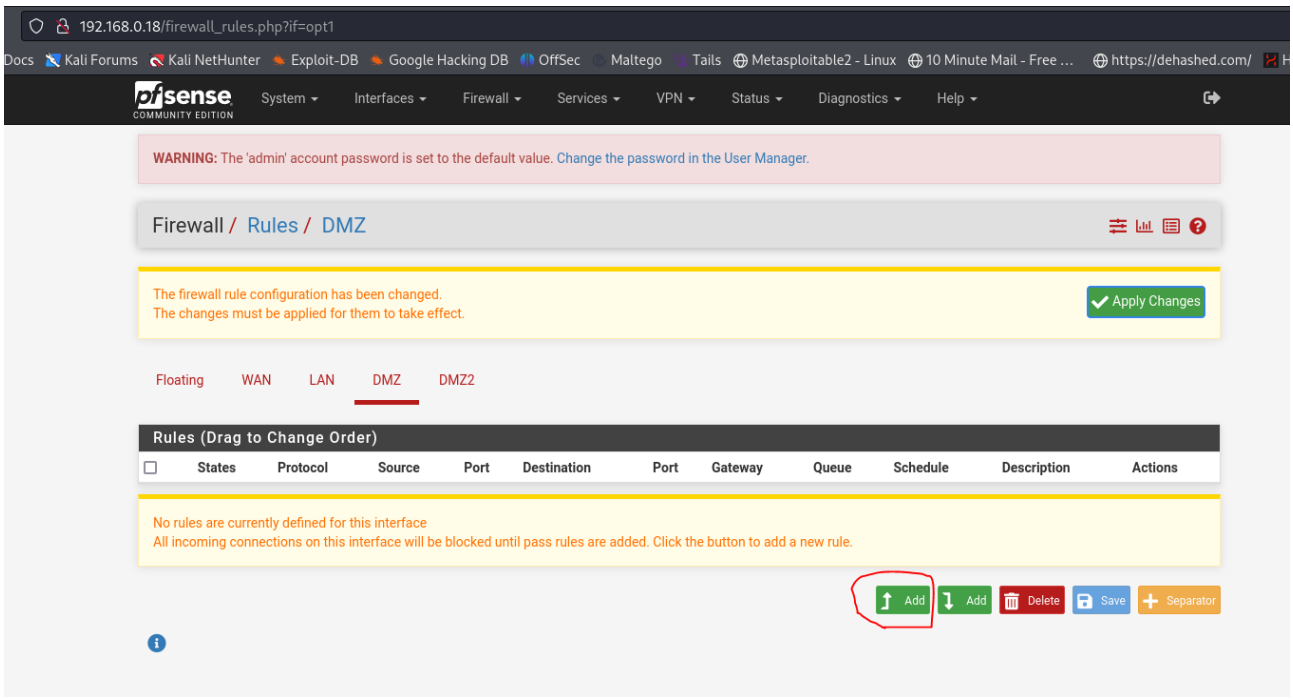
desconectamos el adaptador de red de la kali, lo volvemos a conectar y comprobamos en cmd, que ha cambiado la ip:



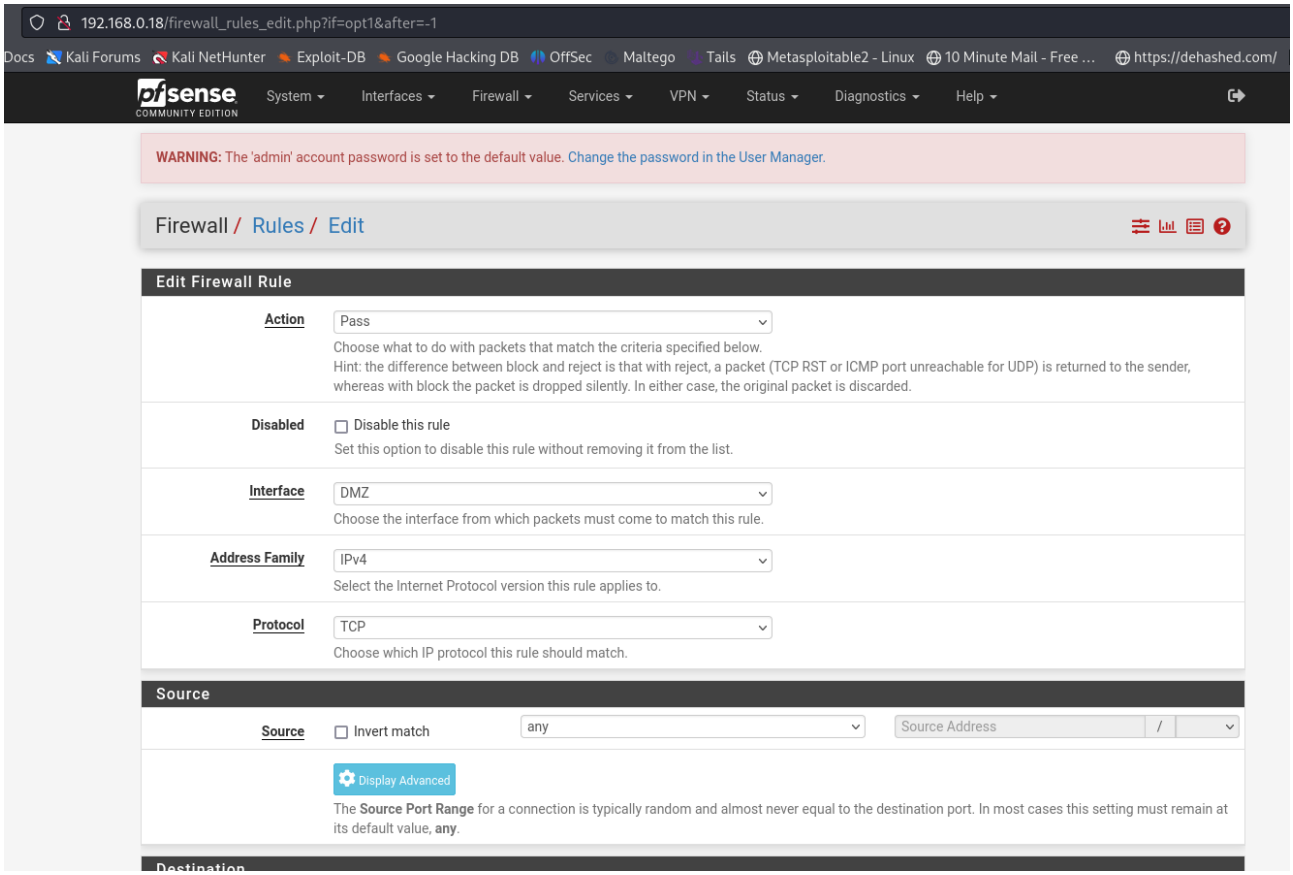
Para configurar las reglas, primero configuramos alias y puertos para el firewall

Creamos la reglas para DMZ

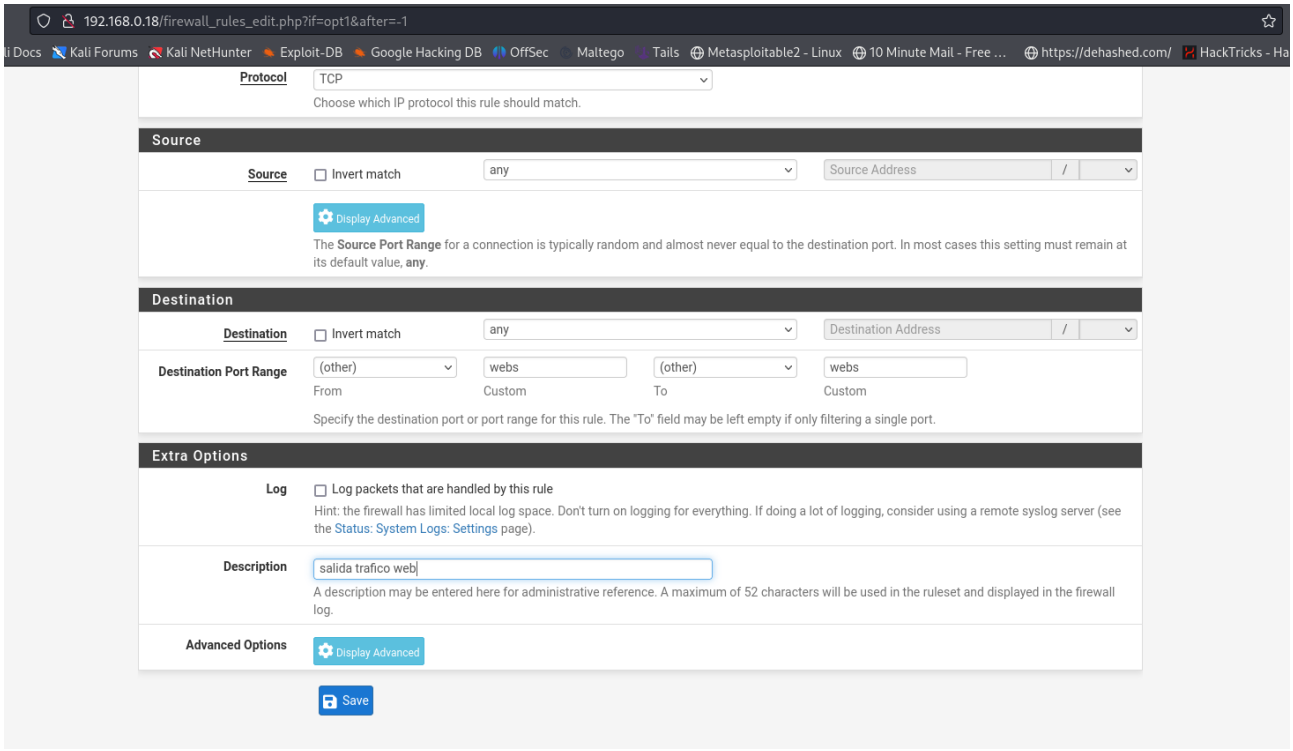
damos click en ADD



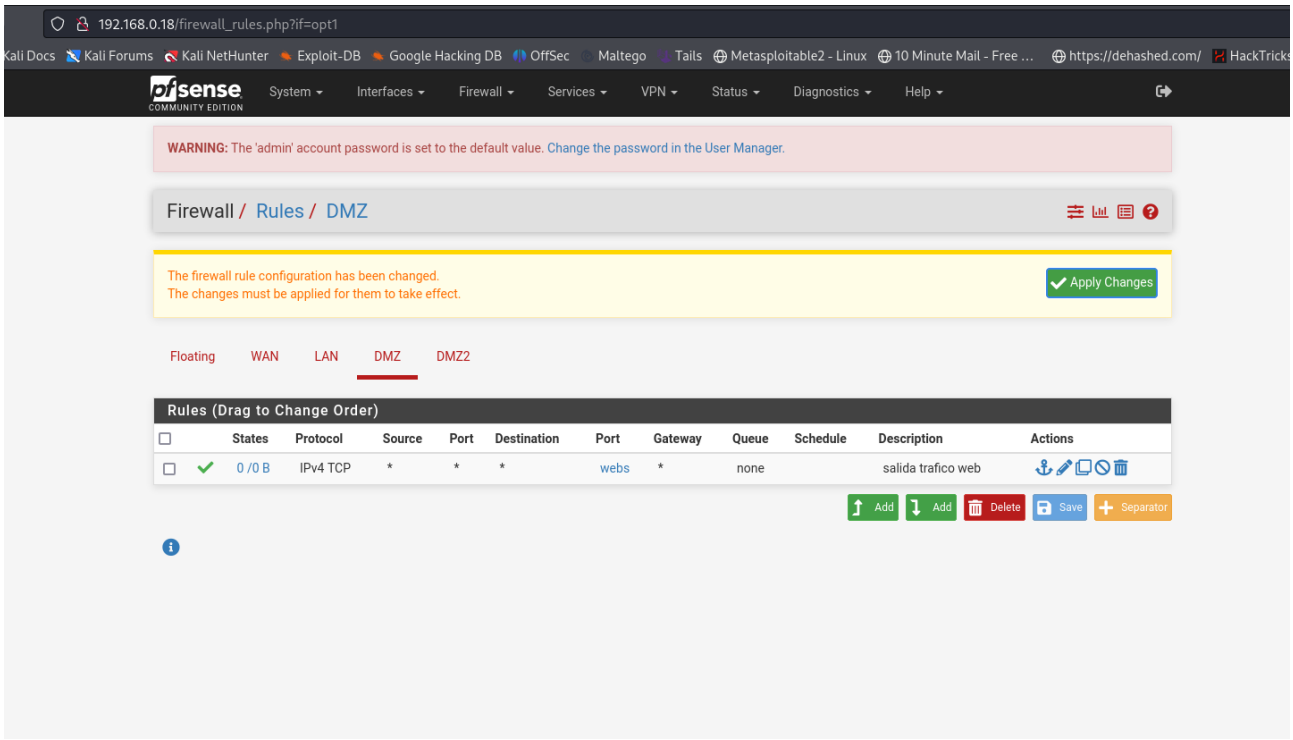
en Action lo dejamos en Pass para permitir el tráfico, y seleccionamos la DMZ, el protocolo TCP, en Source ponemos any (no me sale la opción DMZ subnets que es la más segura)

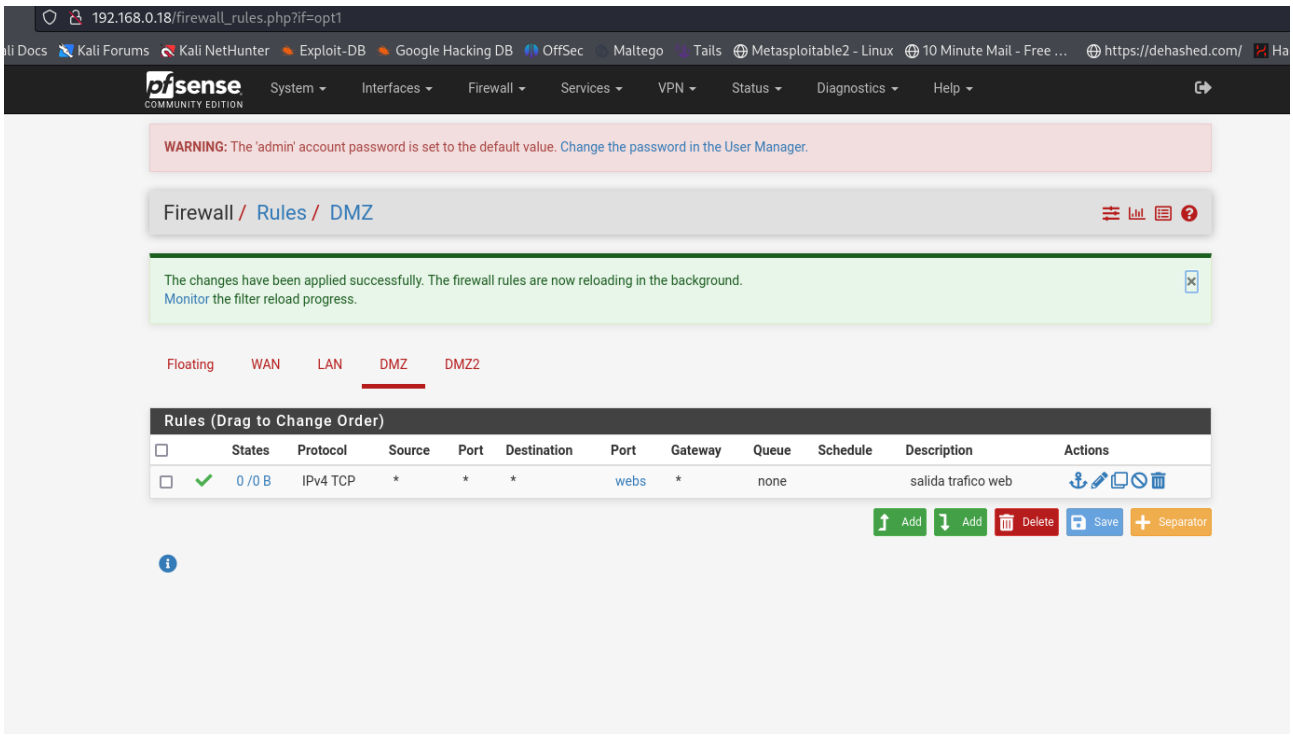


En Destination ponemos los puertos webs, que son el 443 y el 80, ponemos la Descripción de la regla: Salida tráfico web



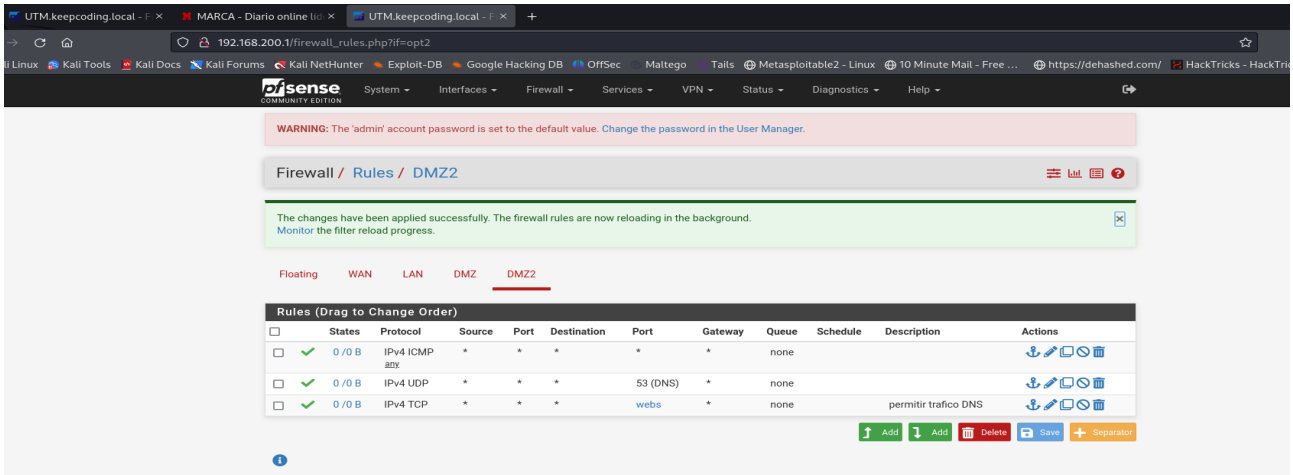
hacemos click en Save y Apply changes



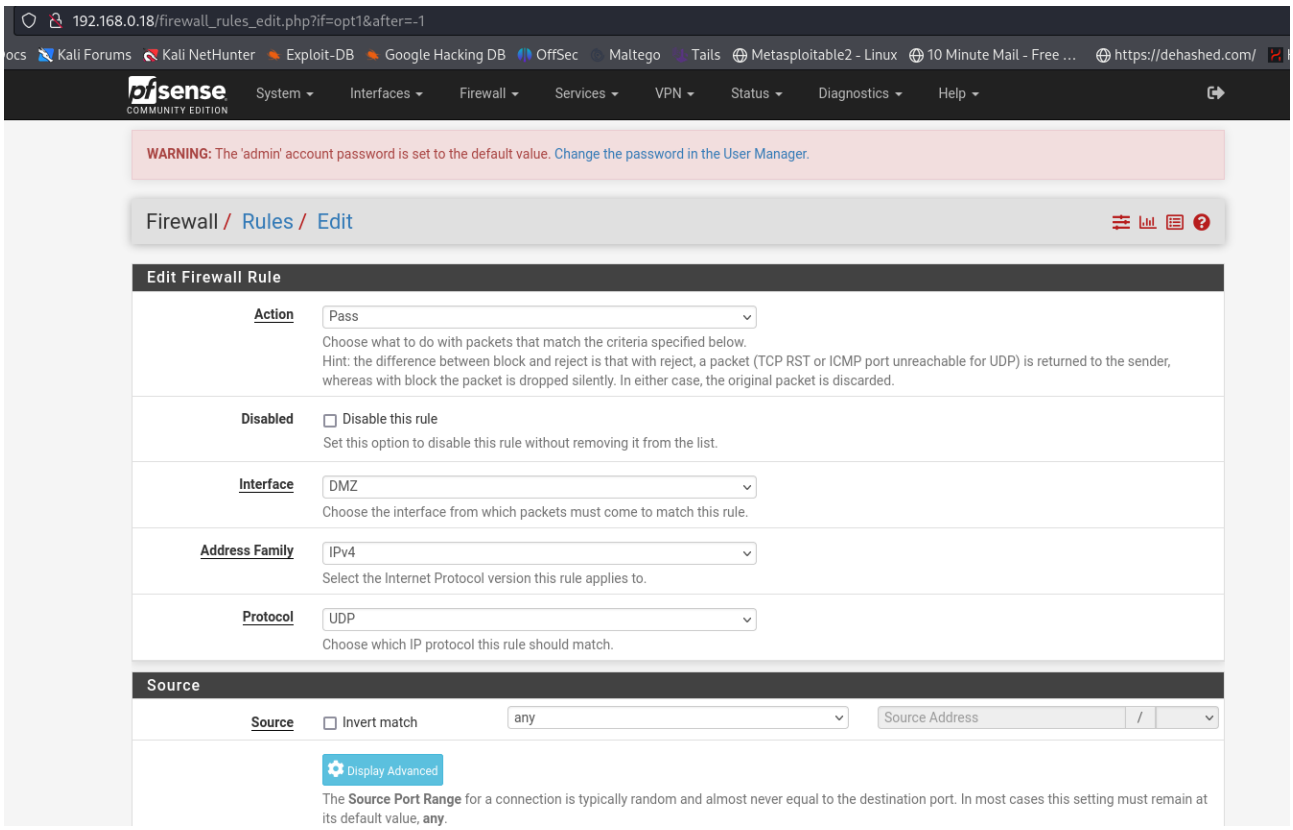


cambiamos a LAN en la kali, y comprobamos que tenemos acceso a internet:

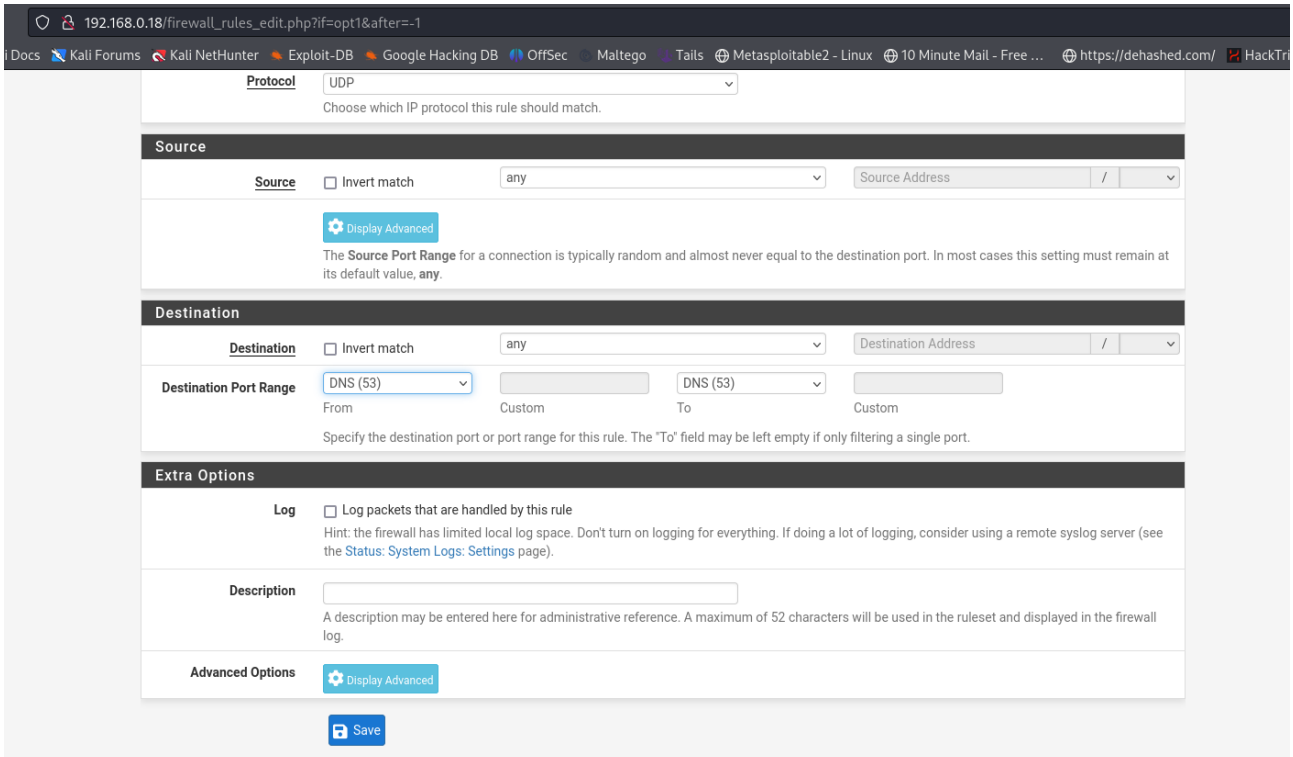
REGLAS DMZ2:



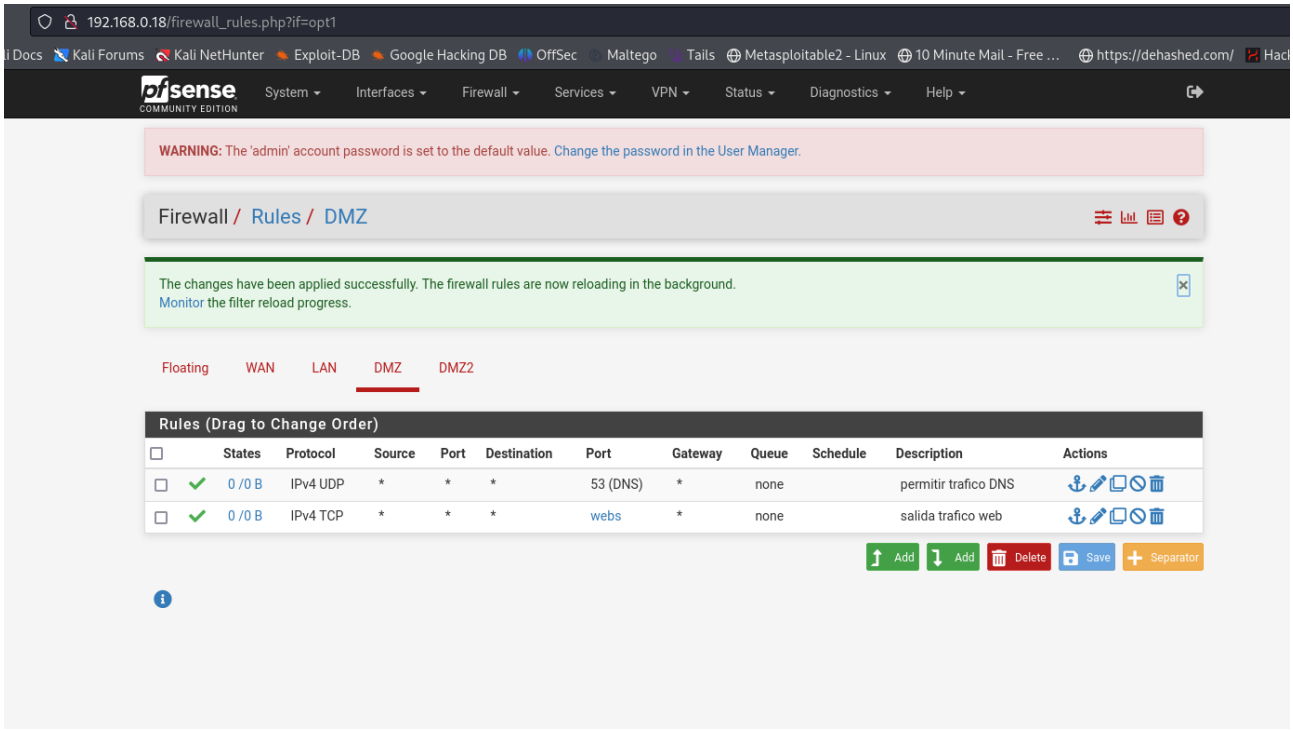
ahora añadimos la regla del protocolo UDP:



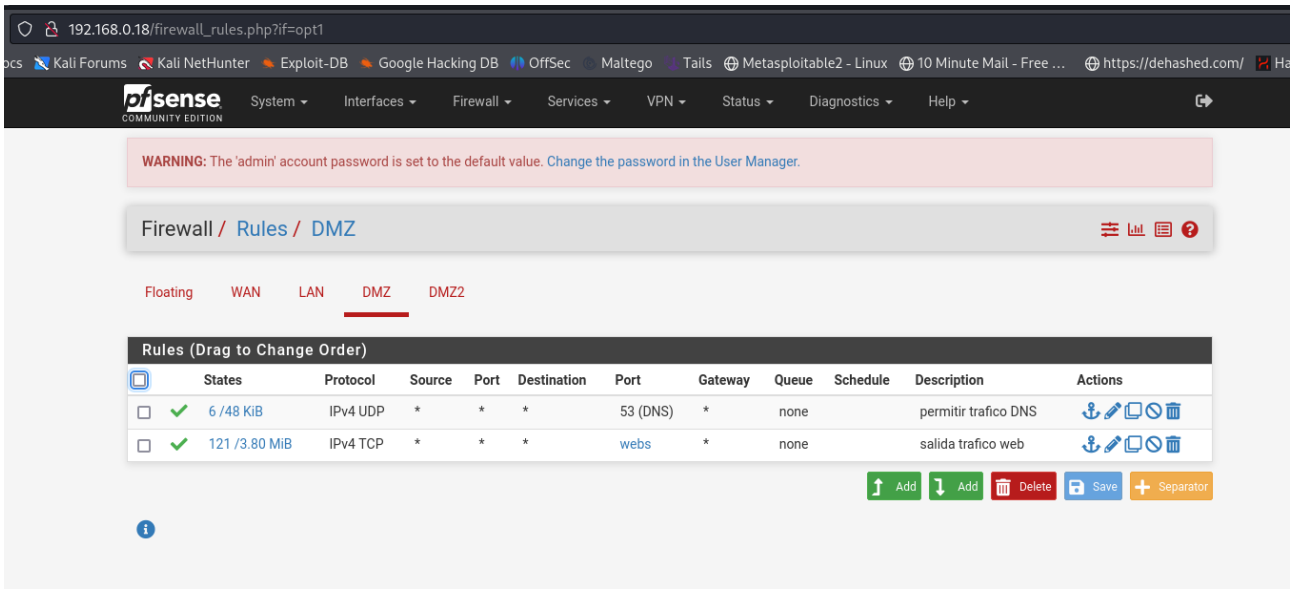
en Destination elegimos DNS (53)



en Descripción, ponemos permitir tráfico DNS, damos a Save y Apply changes:

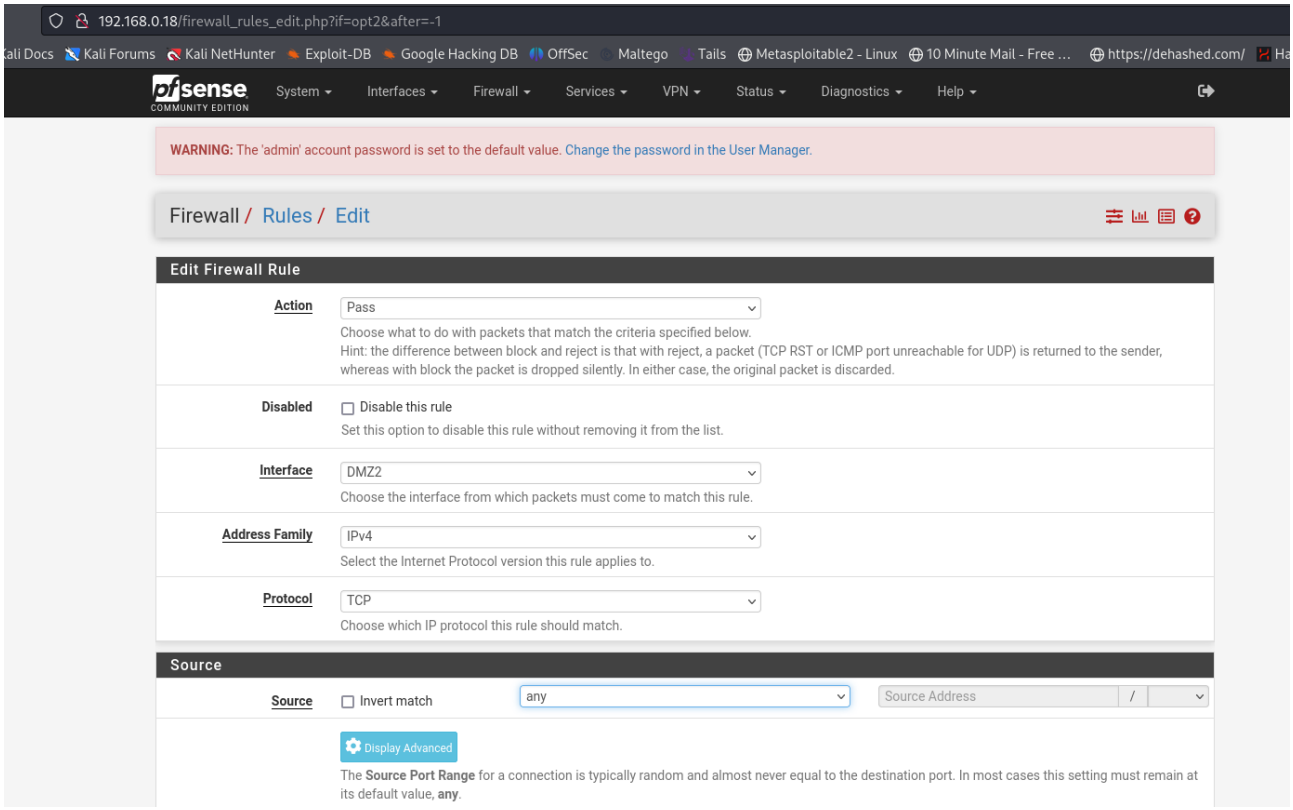


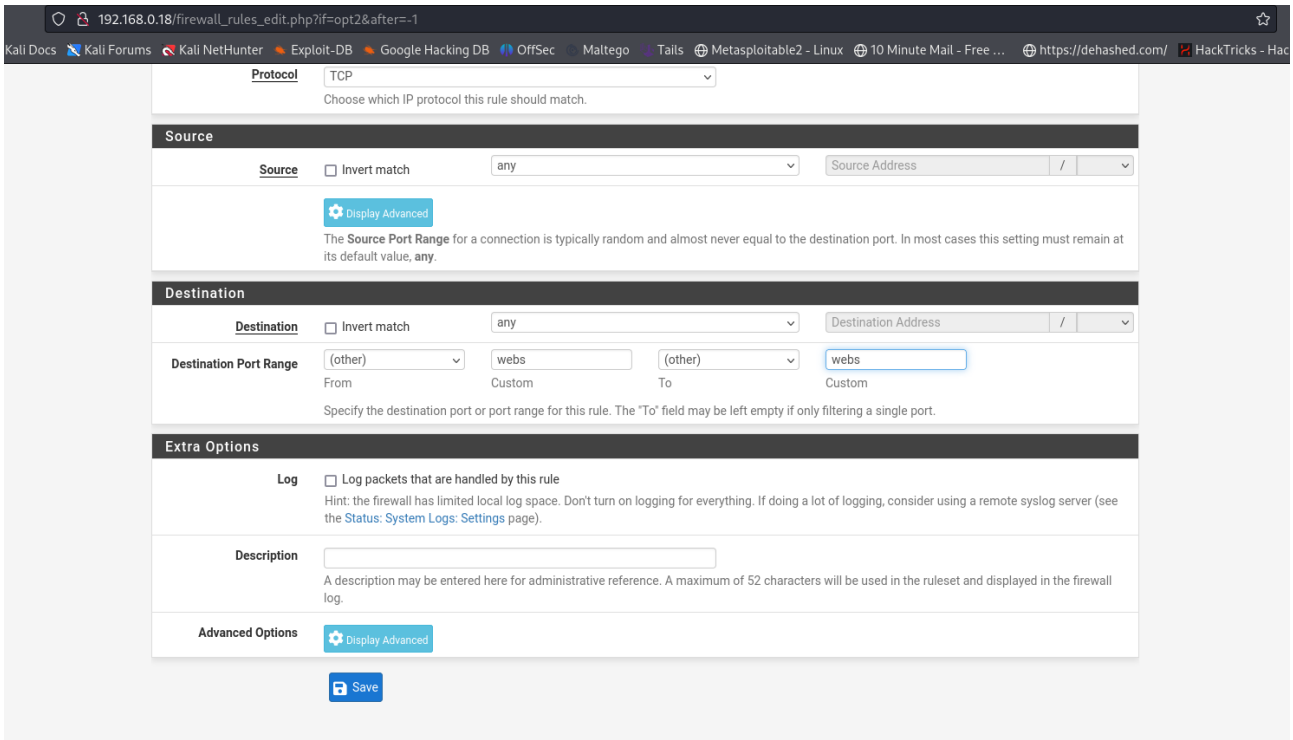
volvemos a entrar a Pfsense y comprobamos las reglas creadas, es importante el orden:



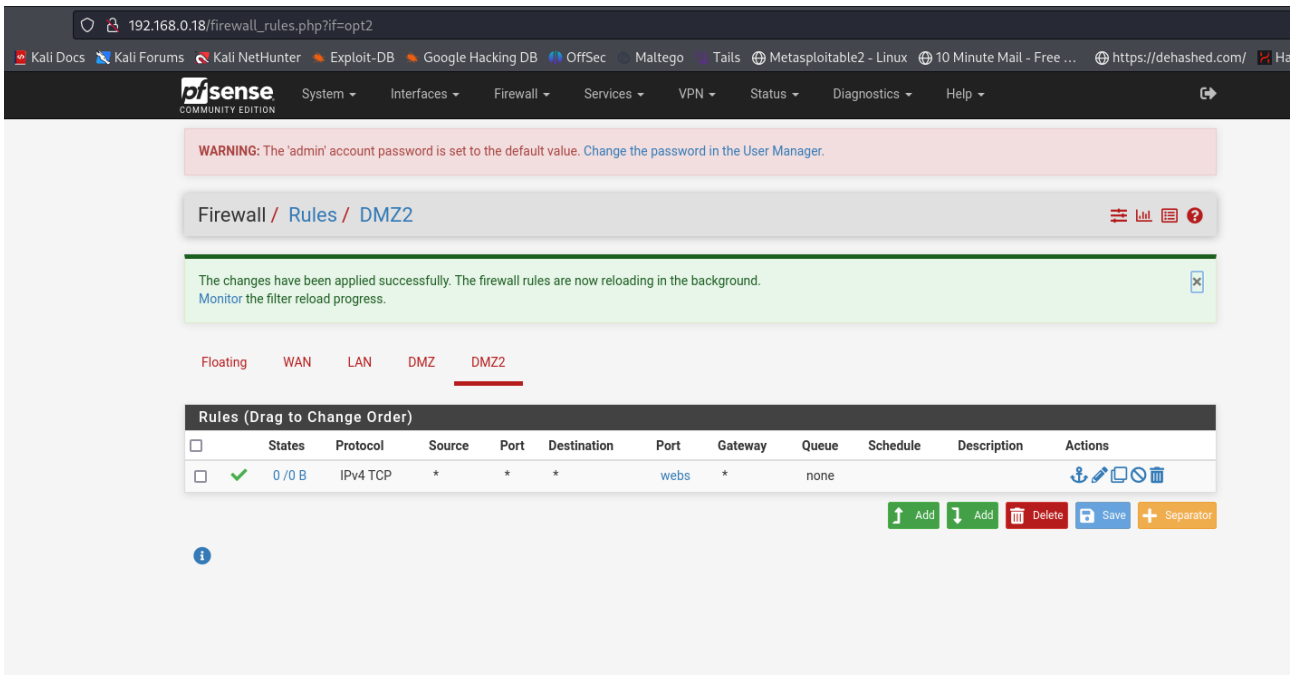
Creamos las reglas de DMZ2

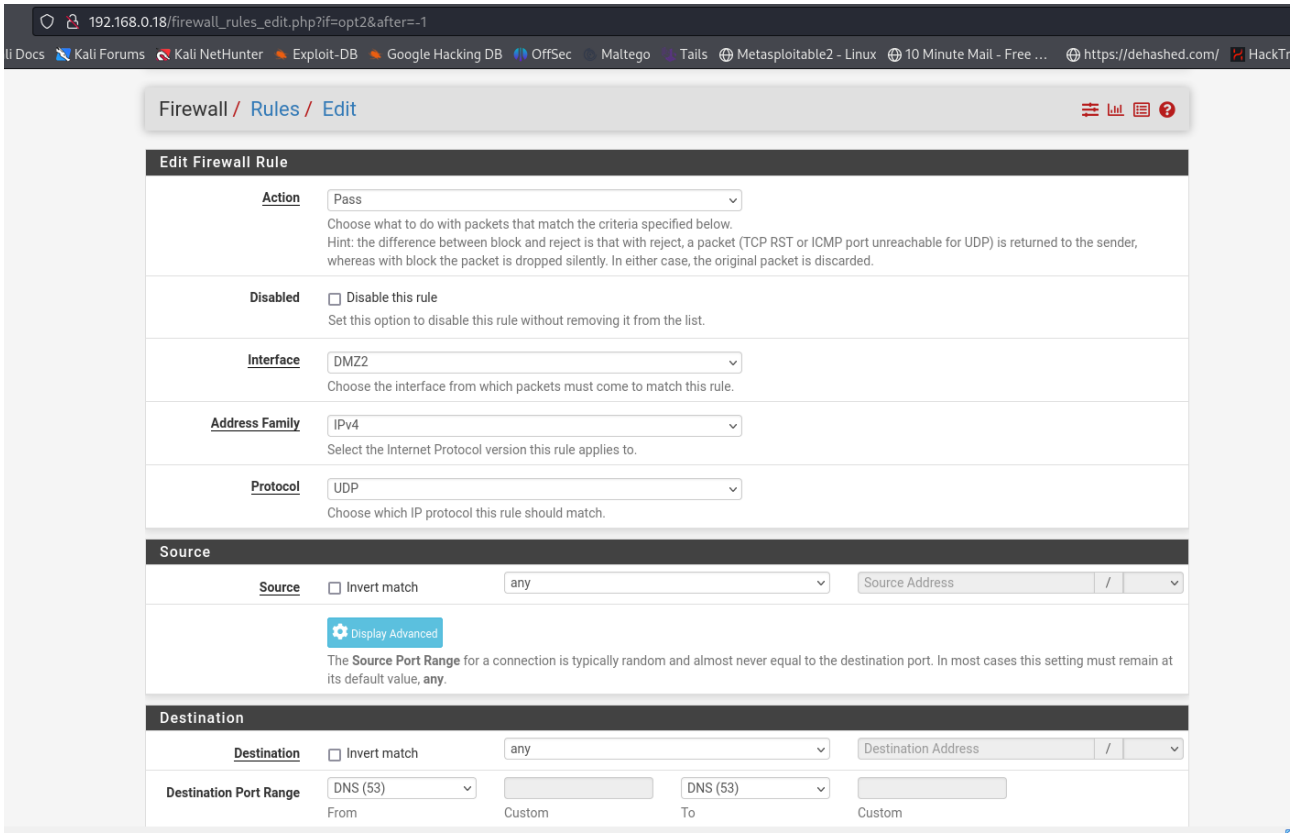
Hacemos click en Add

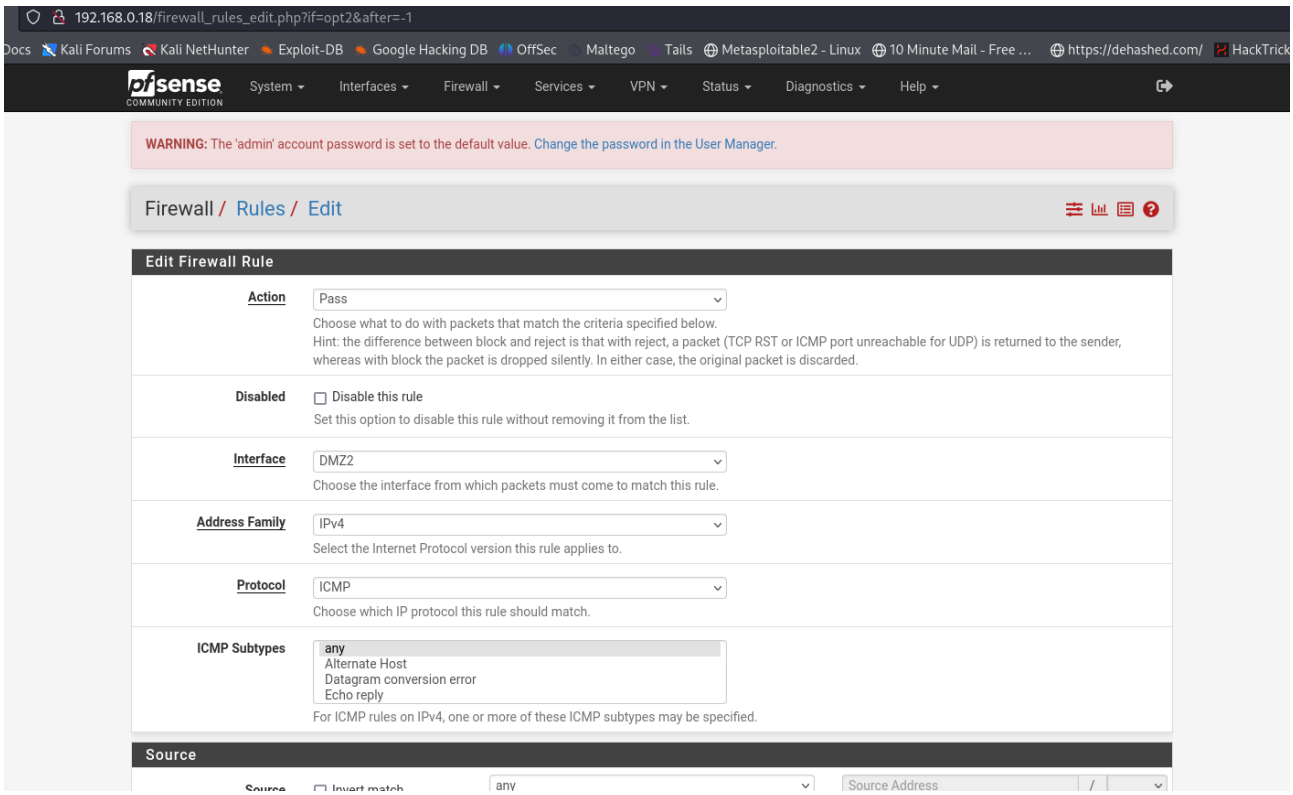




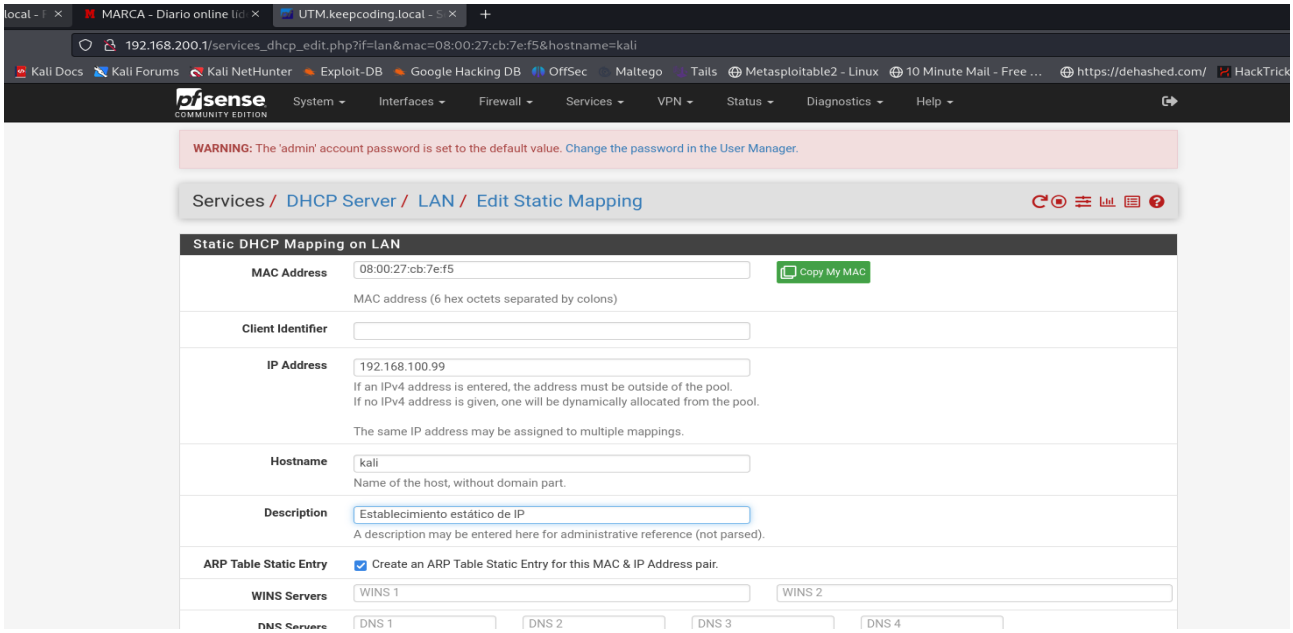
Hacemos click en Save y Apply changes:

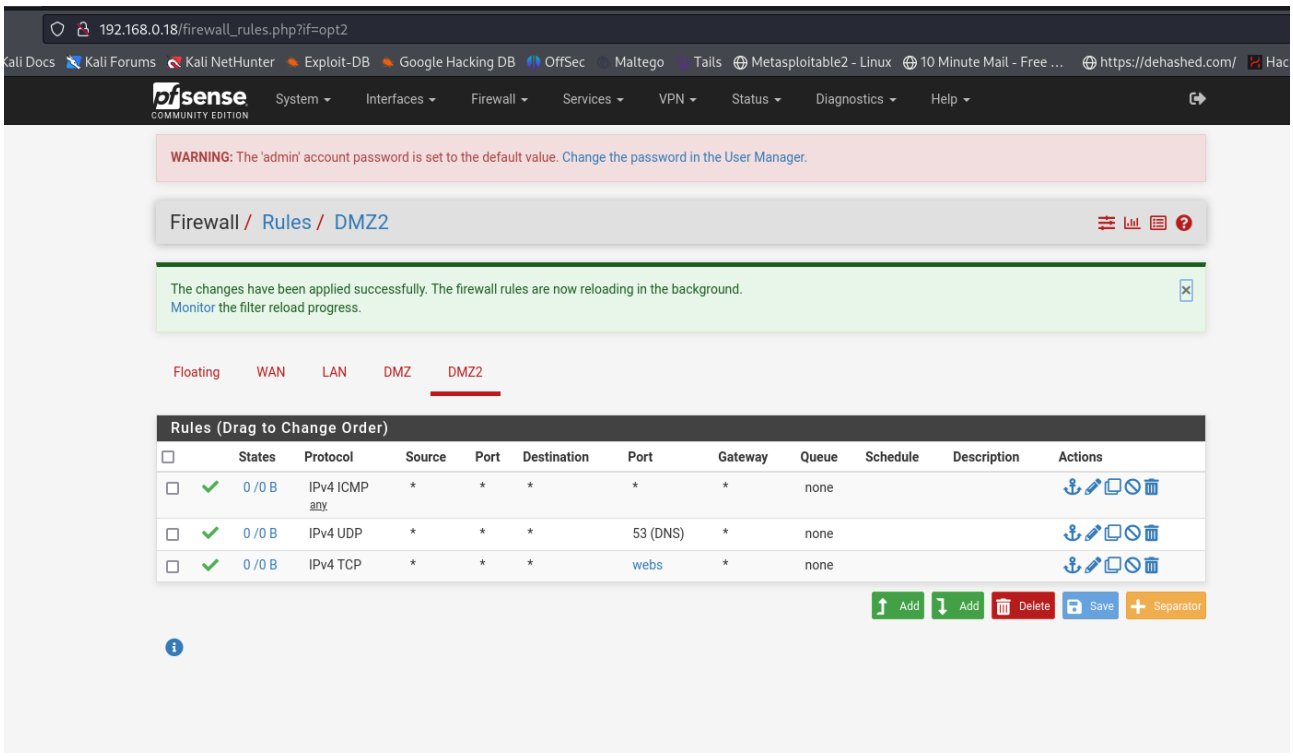

192.168.0.18/firewall_rules.php?if=opt2
Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Maltego Tails Metasploitable2 - Linux 10 Minute Mail - Free ... https://dehashed.com/
pfsense COMMUNITY EDITION
System Interfaces Firewall Services VPN Status Diagnostics Help
WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.
Firewall / Rules / DMZ2
The changes have been applied successfully. The firewall rules are now reloading in the background.
Monitor the filter reload progress.
Floating WAN LAN DMZ DMZ2
Rules (Drag to Change Order)
States Protocol Source Port Destination Port Gateway Queue Schedule Description Actions
0 /0 B IPv4 TCP * * * webs * none
Add Add Delete Save Separator


192.168.0.18/firewall_rules_edit.php?if=opt2&after=-1
Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Maltego Tails Metasploitable2 - Linux 10 Minute Mail - Free ... https://dehashed.com/
Firewall / Rules / Edit
Edit Firewall Rule
Action
Pass
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.
Disabled
Disable this rule
Set this option to disable this rule without removing it from the list.
Interface
DMZ2
Choose the interface from which packets must come to match this rule.
Address Family
IPv4
Select the Internet Protocol version this rule applies to.
Protocol
UDP
Choose which IP protocol this rule should match.
Source
Source
Invert match
any
Source Address
Display Advanced
The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.
Destination
Destination
Invert match
any
Destination Address
Destination Port Range
DNS (53)
From
Custom
DNS (53)
To
Custom

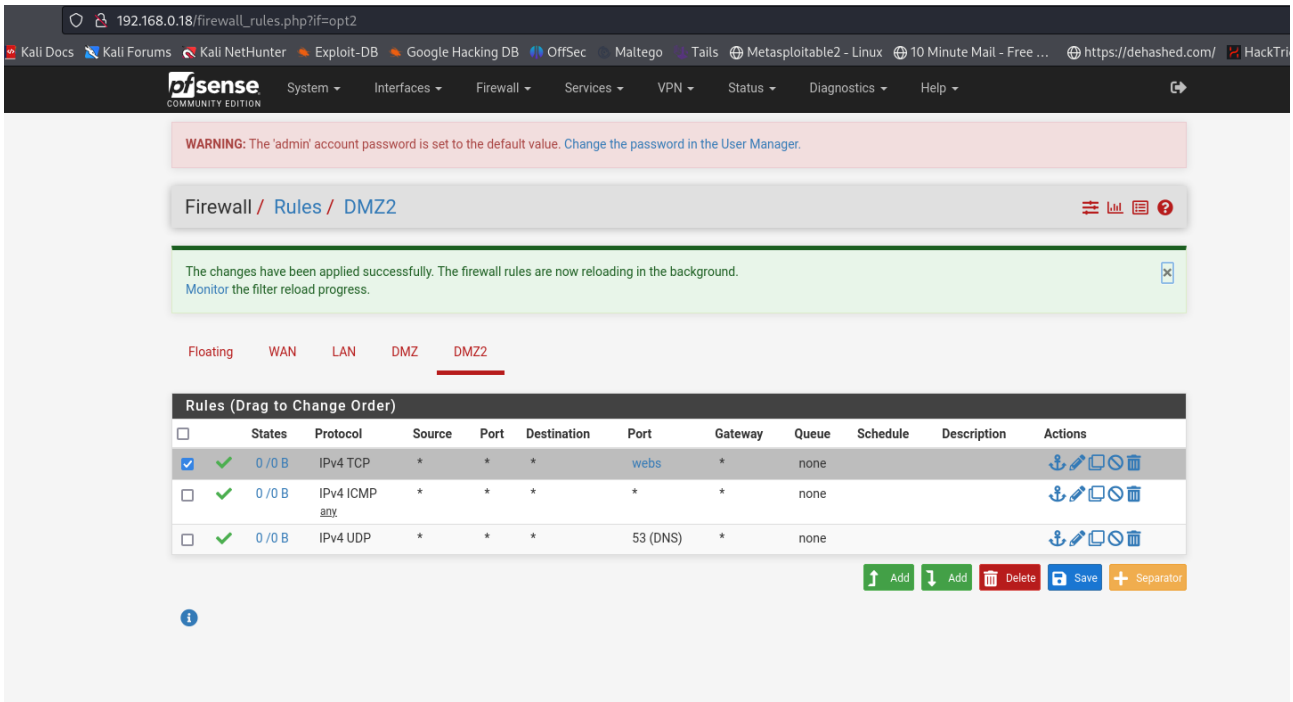


mapeamos una IP estática:

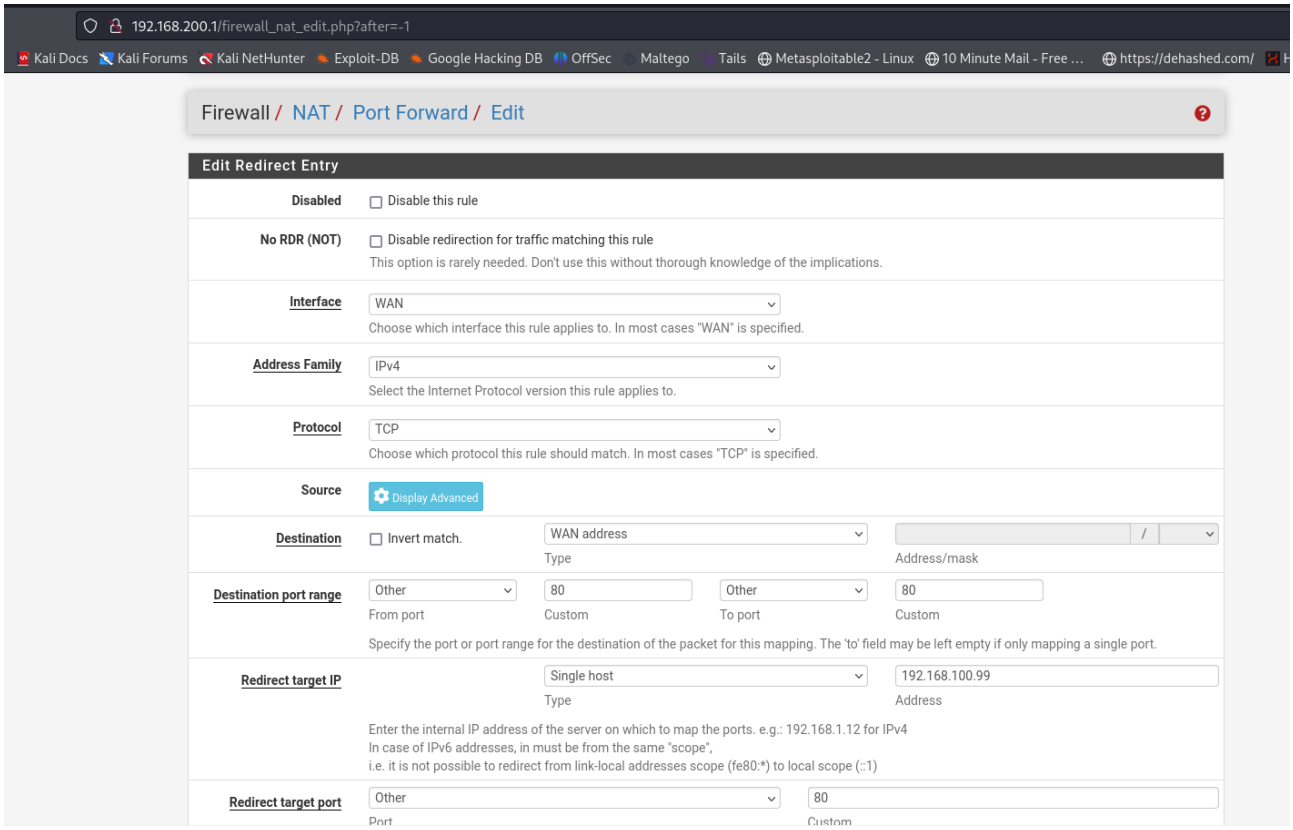


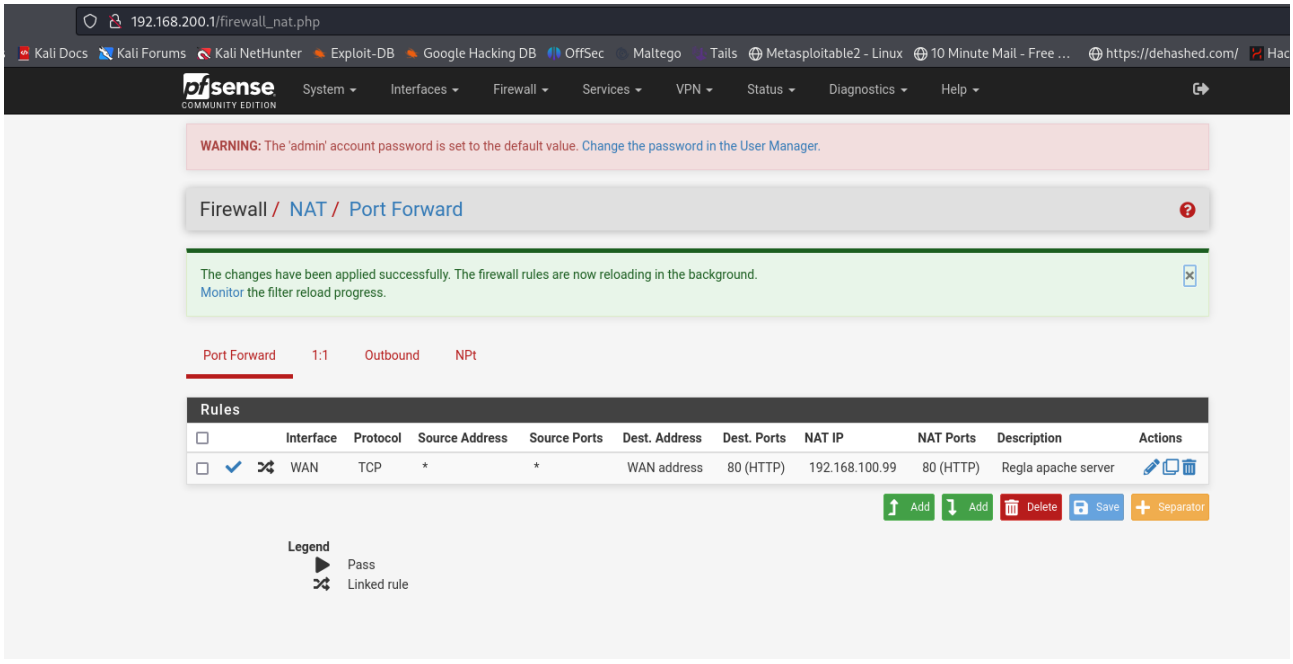


cambiamos el orden, ponemos la más restrictiva arriba:

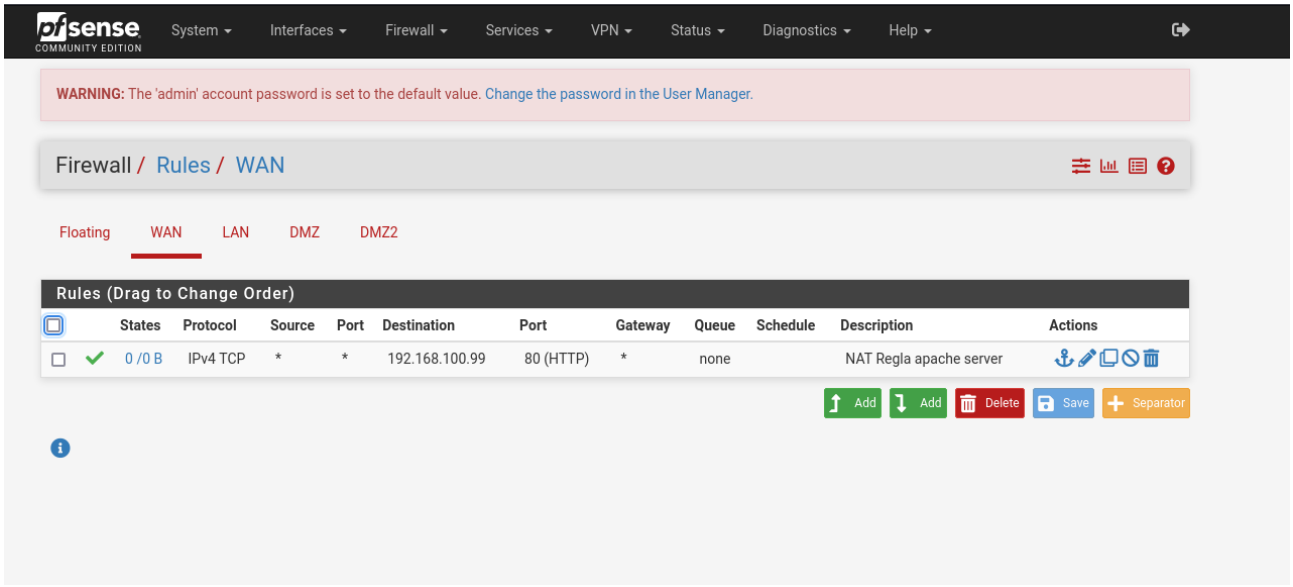


Crearemos una regla para que todo el tráfico que nos llegue a nuestro puerto 80, es decir la red WAN, nos redirija a nuestra red LAN:

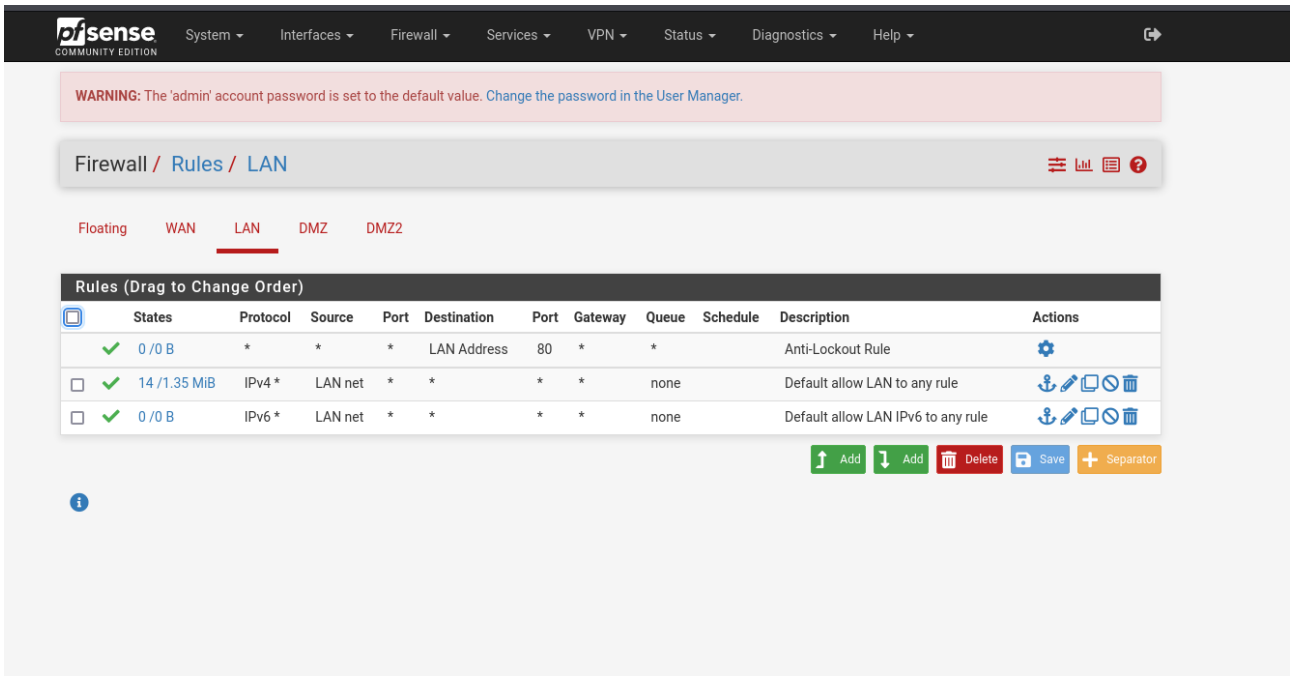

192.168.200.1/firewall_nat_edit.php?after=-1
Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Maltego Tails Metasploitable2 - Linux 10 Minute Mail - Free ... https://dehashed.com/
Firewall / NAT / Port Forward / Edit
Edit Redirect Entry
Disabled
Disable this rule
No RDR (NOT)
Disable redirection for traffic matching this rule
This option is rarely needed. Don't use this without thorough knowledge of the implications.
Interface
WAN
Choose which interface this rule applies to. In most cases "WAN" is specified.
Address Family
IPv4
Select the Internet Protocol version this rule applies to.
Protocol
TCP
Choose which protocol this rule should match. In most cases "TCP" is specified.
Source
Display Advanced
Destination
Invert match.
WAN address
Type
Address/mask
Destination port range
Other
80
Other
80
From port
Custom
To port
Custom
Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.
Redirect target IP
Single host
192.168.100.99
Type
Address
Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4
In case of IPv6 addresses, in must be from the same "scope",
i.e. it is not possible to redirect from link-local addresses scope (fe80:*) to local scope (::1)
Redirect target port
Other
80
Port
Custom


192.168.200.1/firewall_nat.php
Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Maltego Tails Metasploitable2 - Linux 10 Minute Mail - Free ... https://dehashed.com/
pfsense COMMUNITY EDITION
System Interfaces Firewall Services VPN Status Diagnostics Help
WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.
Firewall / NAT / Port Forward
The changes have been applied successfully. The firewall rules are now reloading in the background.
Monitor the filter reload progress.
Port Forward 1:1 Outbound NPt
Rules
Interface Protocol Source Address Source Ports Dest. Address Dest. Ports NAT IP NAT Ports Description Actions
WAN TCP * * WAN address 80 (HTTP) 192.168.100.99 80 (HTTP) Regla apache server
Add Add Delete Save Separator
Legend
Pass
Linked rule

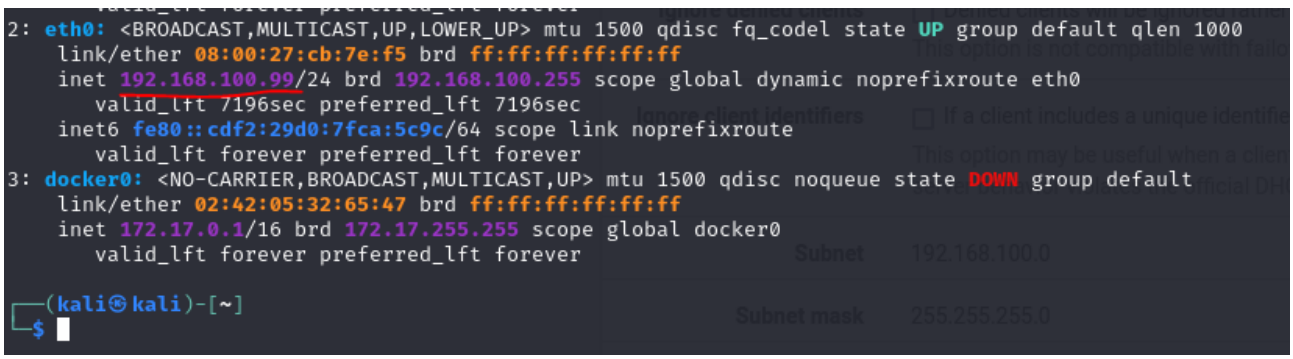
REGLAS WAN:



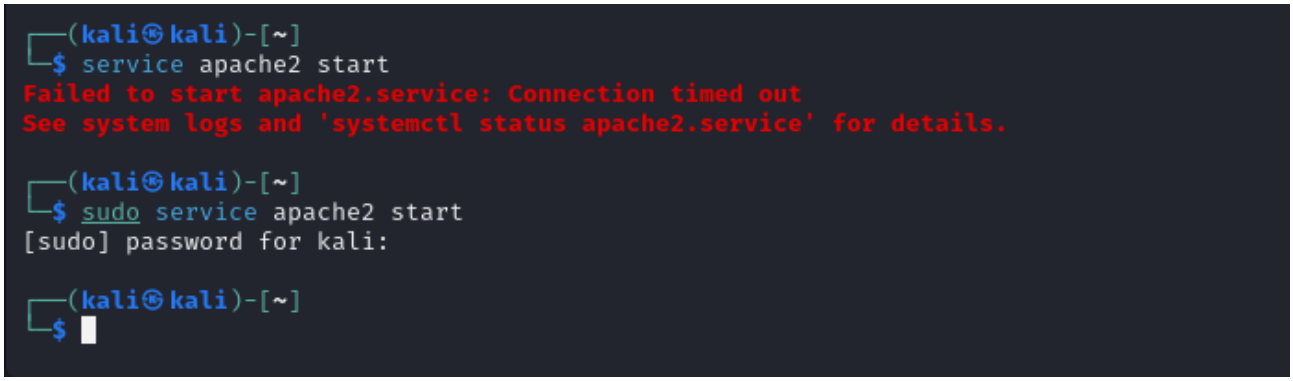
REGLAS LAN:



comprobamos el cambio de ip

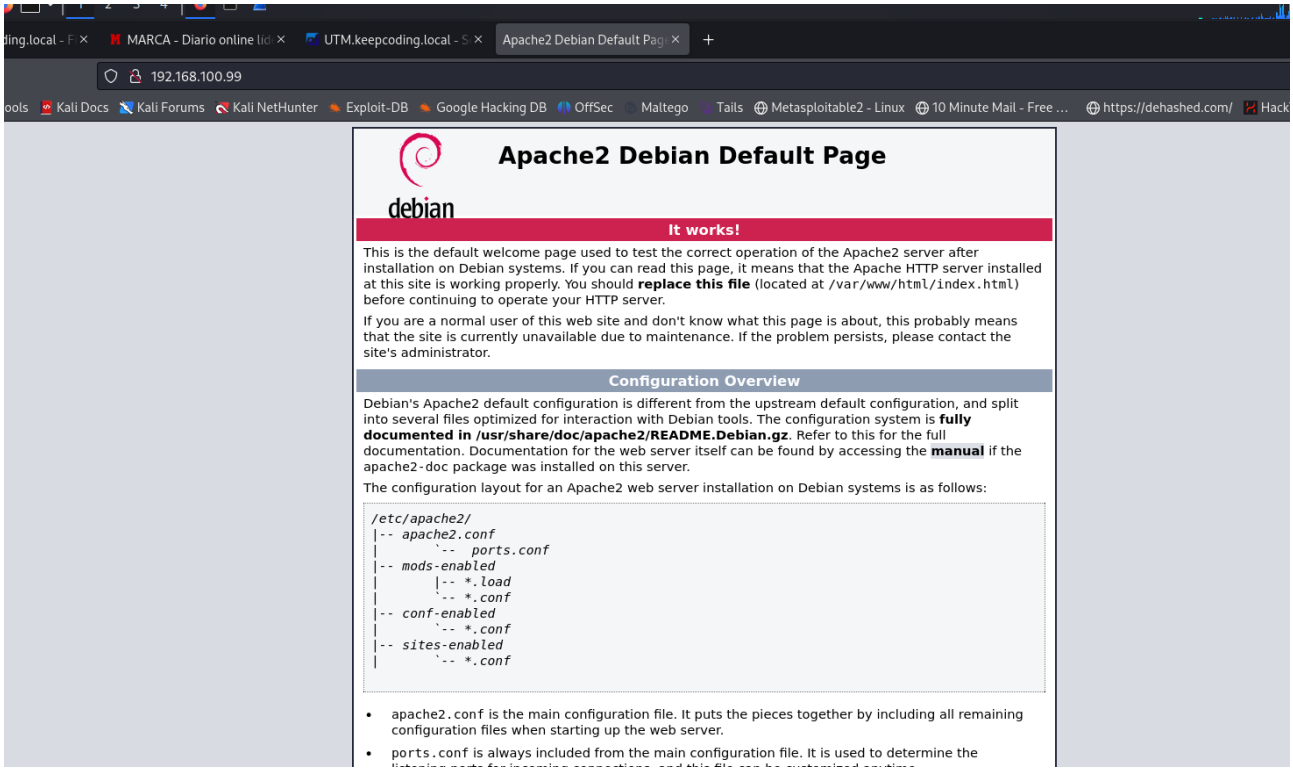


levantamos el servidor APACHE:

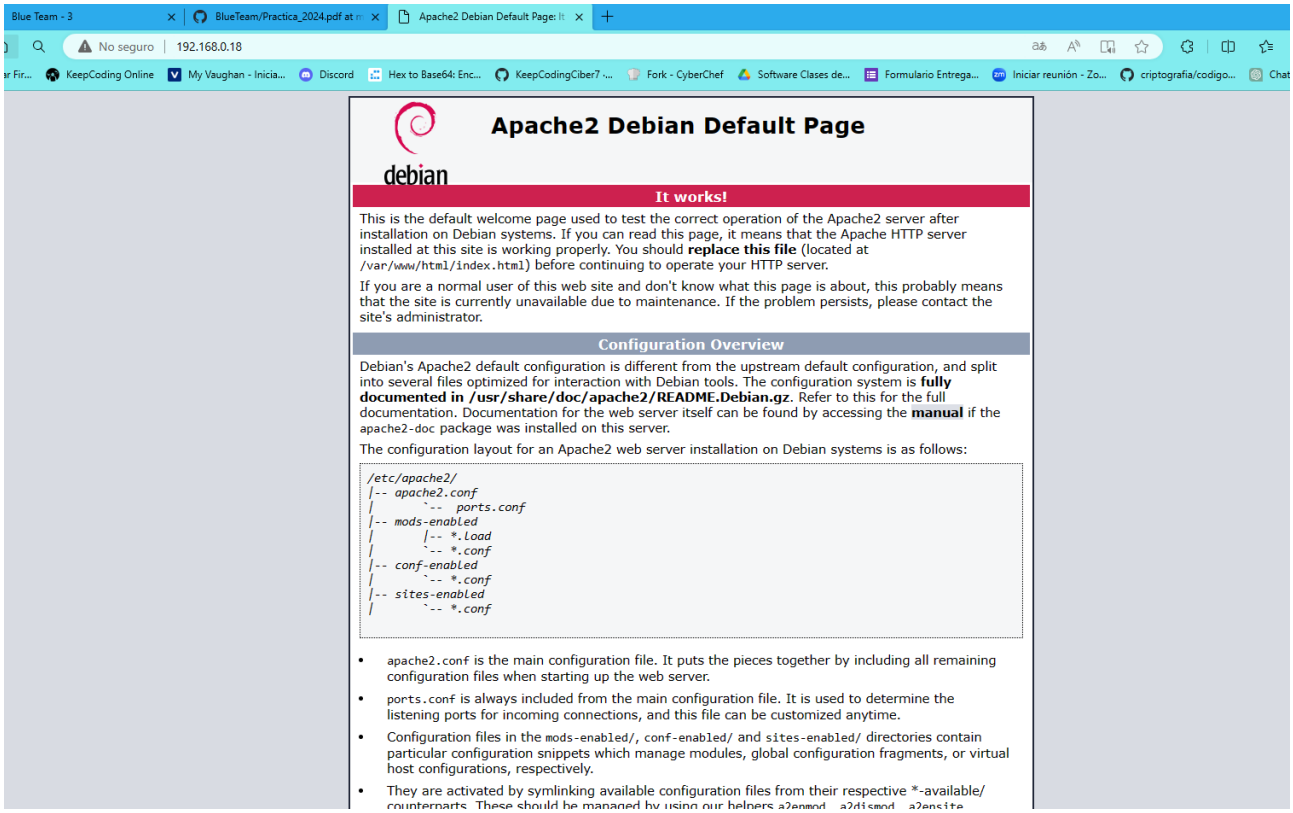


y comprobamos que está levantado el servidor:

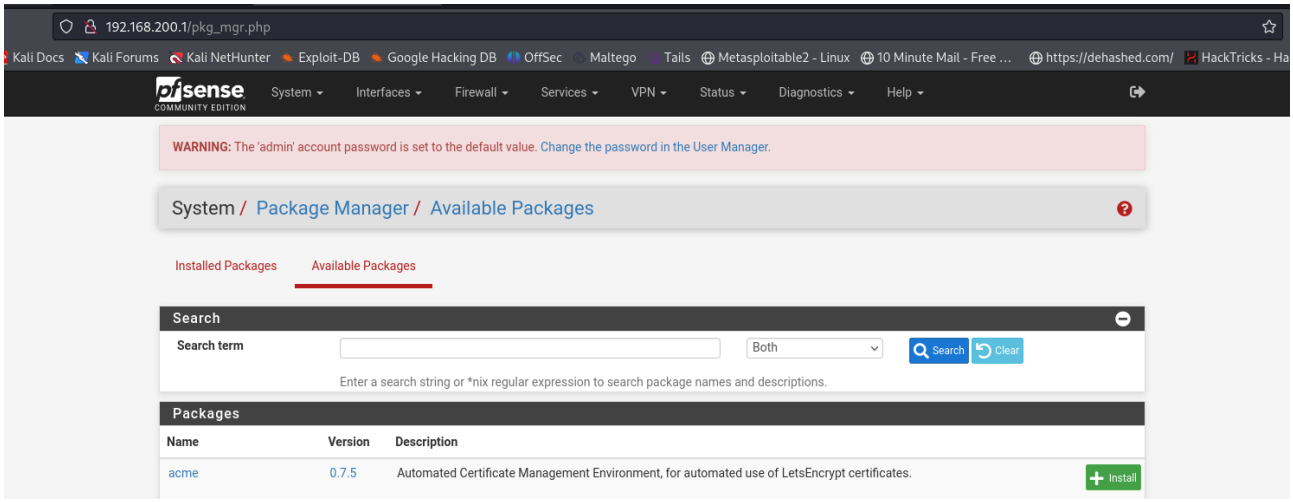
y comprobamos que se levanta en la ip 192.168.100.99



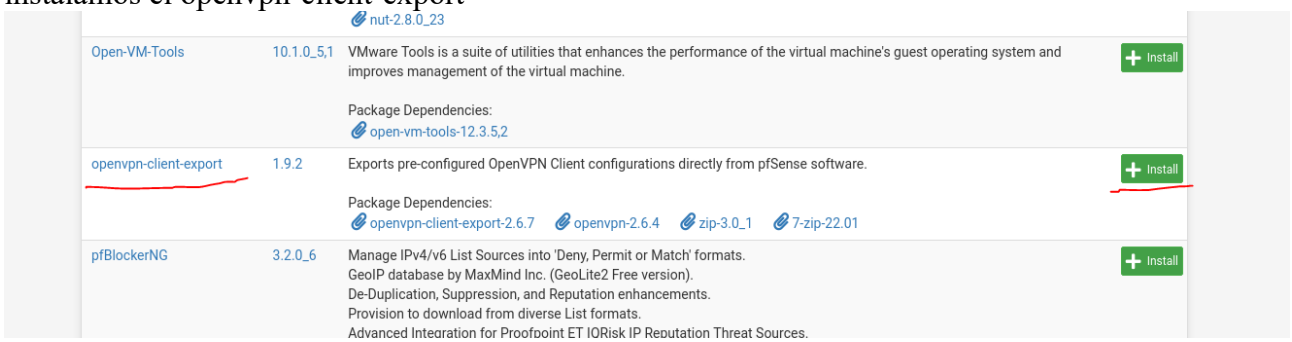
ahora sí accedemos desde nuestra máquina a la ip del servidor apache



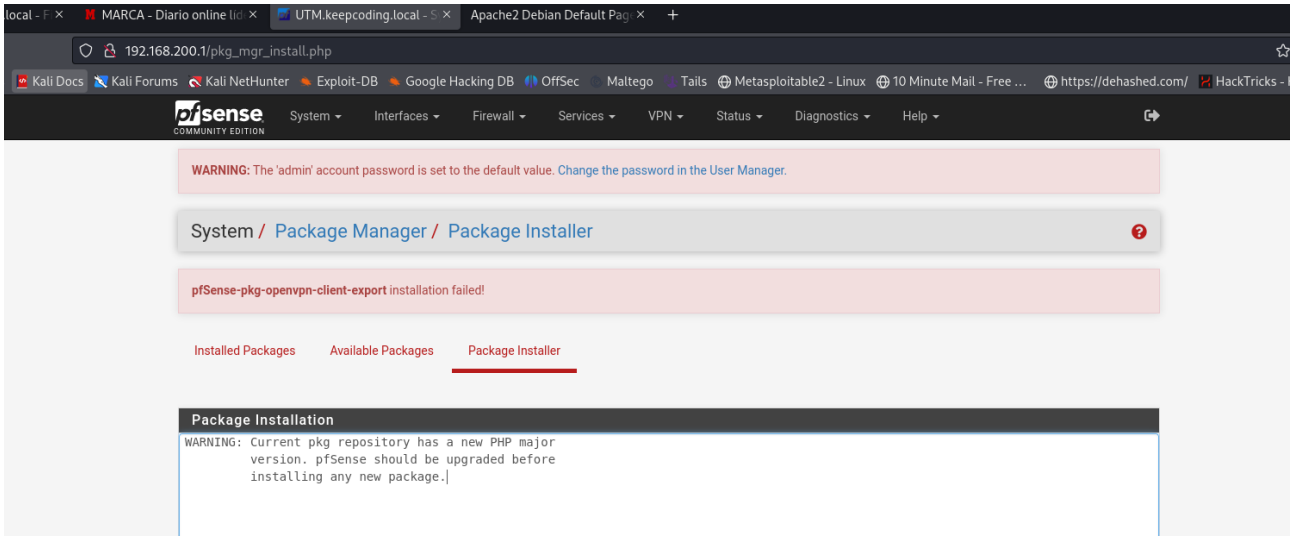
Creamos ahora la VPN, nos vamos a System / Package Manager / Available Packages



instalamos el openvpn-client-export

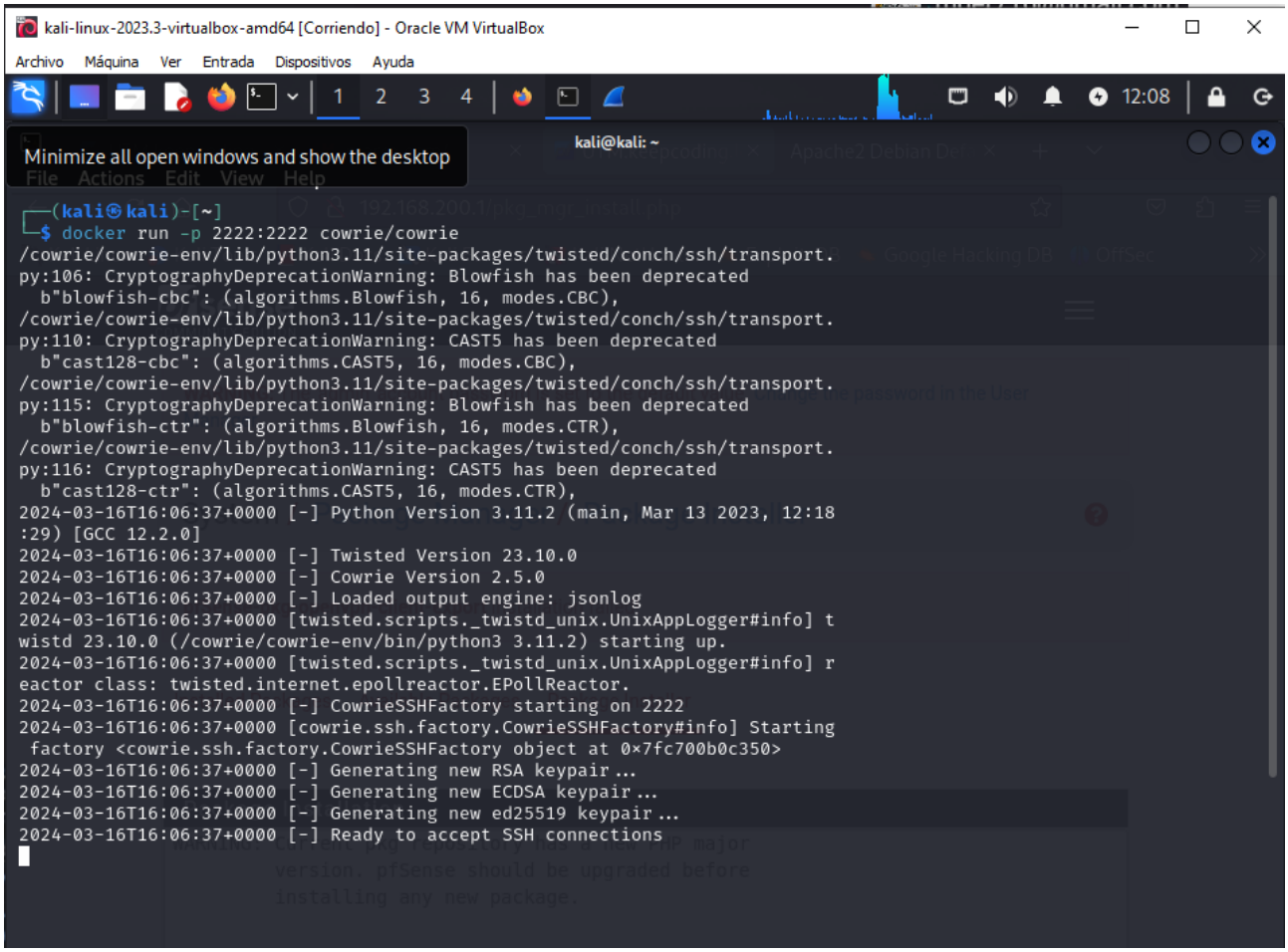


me da error al intentar instalar la vpn



Lanzamos en nuestra kali el honeypot Cowrie con el comando:

docker run -p 2222:2222 cowrie/cowrie



se quedará listo para aceptar conexiones.

Con el siguiente comando corremos el amazedostrich:

docker run -p 333:3389 amazedostrich/rdpy

Hago un docker ps para ver las imágenes docker en ejecución:

```
┌──(kali㉿kali)-[~]
└─$ docker ps
CONTAINER ID   IMAGE                COMMAND                  CREATED          STATUS          PORTS
                                    NAMES
d1fab0c055ad   amazedostrich/rdpy   "/bin/sh -c '/usr/bi…"   14 minutes ago   Up 14 minutes   0.0.0.0:333→3389/tcp
, :::333→3389/tcp                   crazy_vaughan
9b9cb5e1f707   cowrie/cowrie        "/cowrie/cowrie-env/…"   41 minutes ago   Up 41 minutes   0.0.0.0:2222→2222/tc
p, :::2222→2222/tcp, 2223/tcp       eager_elgamal

┌──(kali㉿kali)-[~]
└─$
```

con este comando nos abrirá una terminal dentro del docker:

```
┌──(kali㉿kali)-[~]
└─$ docker ps
CONTAINER ID   IMAGE                COMMAND                  CREATED
  NAMES
d1fab0c055ad   amazedostrich/rdpy   "/bin/sh -c '/usr/bi…"   21 minutes ag
  crazy_vaughan
9b9cb5e1f707   cowrie/cowrie        "/cowrie/cowrie-env/…"   49 minutes ag
  eager_elgamal

┌──(kali㉿kali)-[~]
└─$ docker exec -it -u 0 d1fab0c055ad /bin/bash
bash-4.4#
```

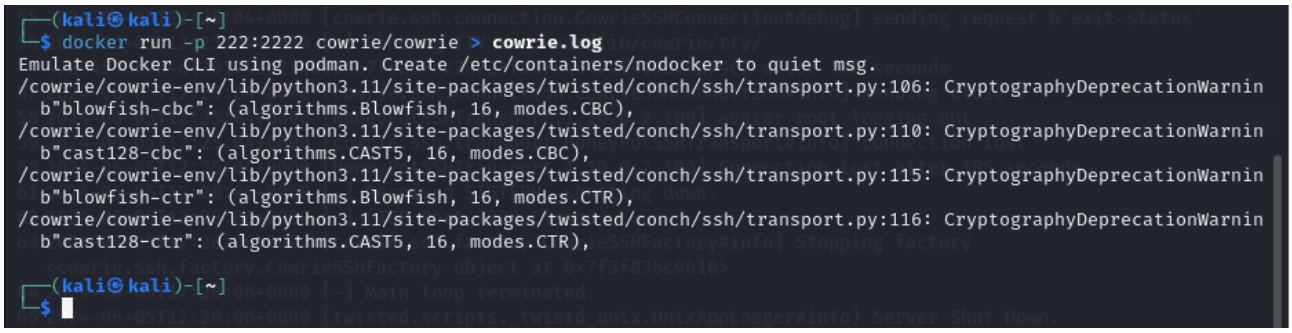
con este comando iremos a los logs del honeypot

```
bash-4.4# ls
bin   dev   etc   home  lib   media  mnt   opt   proc  root  run   sbin  srv   sys   tmp   usr   var
bash-4.4# cd rdpy
bash: cd: rdpy: No such file or directory
bash-4.4# cd /var/log
bash-4.4# ls
rdpy
bash-4.4# cd rdpy
bash-4.4# ls
rdpy.log
bash-4.4#
```

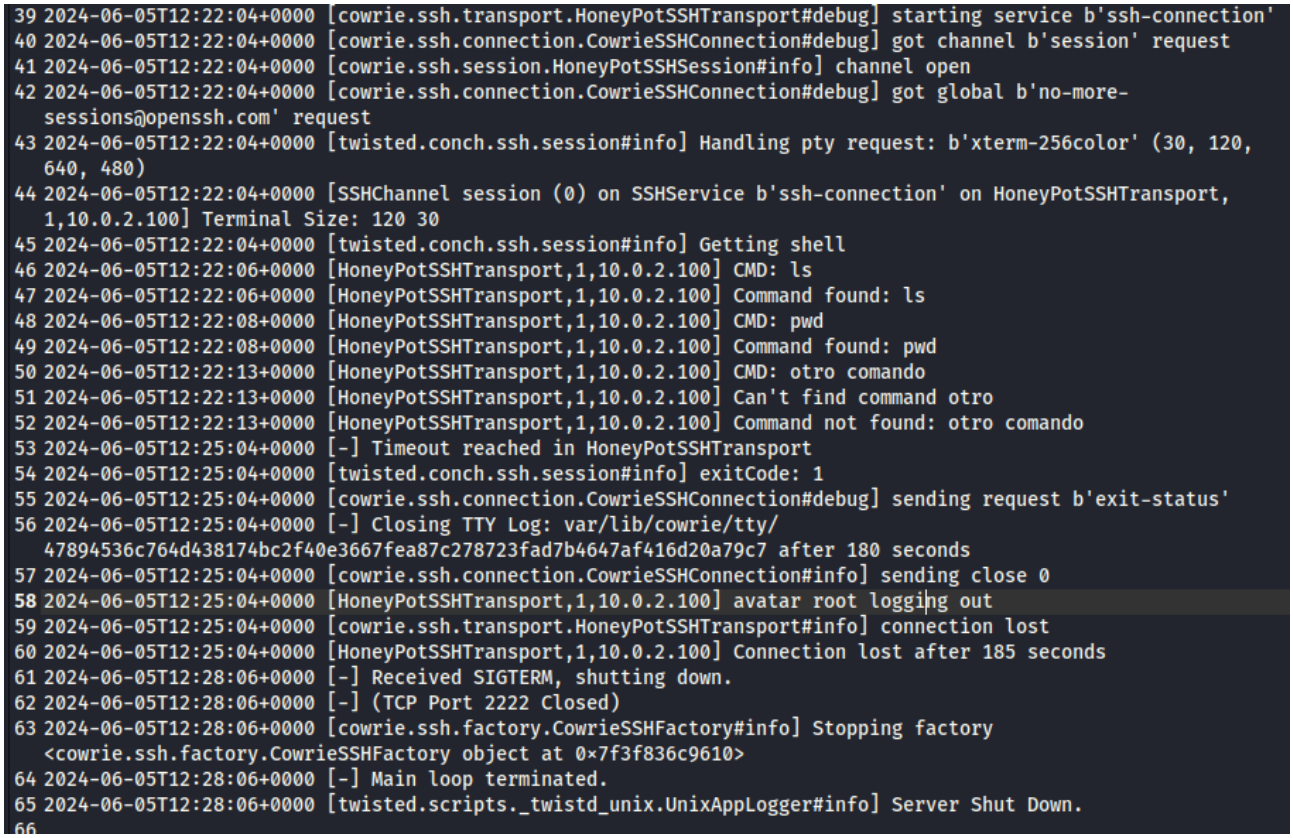
con el comando tail -f rdpy.log vemos los logs del honeypot

```
bash-4.4# tail -f rdpy.log
[*] INFO:       Build size map
[*] INFO:       (1024, 800) → /home/rdpy/1
[*] INFO:       (800, 600) → /home/rdpy/2
[*] INFO:       (800, 600) → /home/rdpy/3
```

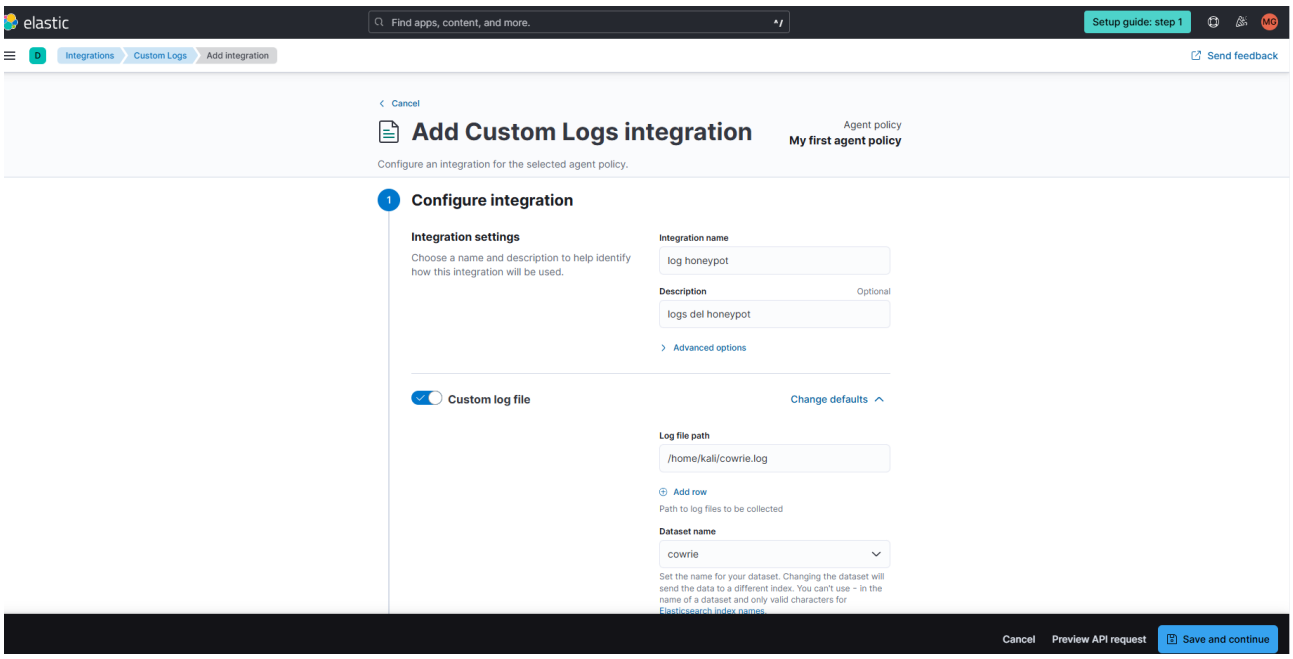
lanzo el siguiente comando para recoger en el archivo cowrie.log, los logs del honeypot en el contenedor de docker:



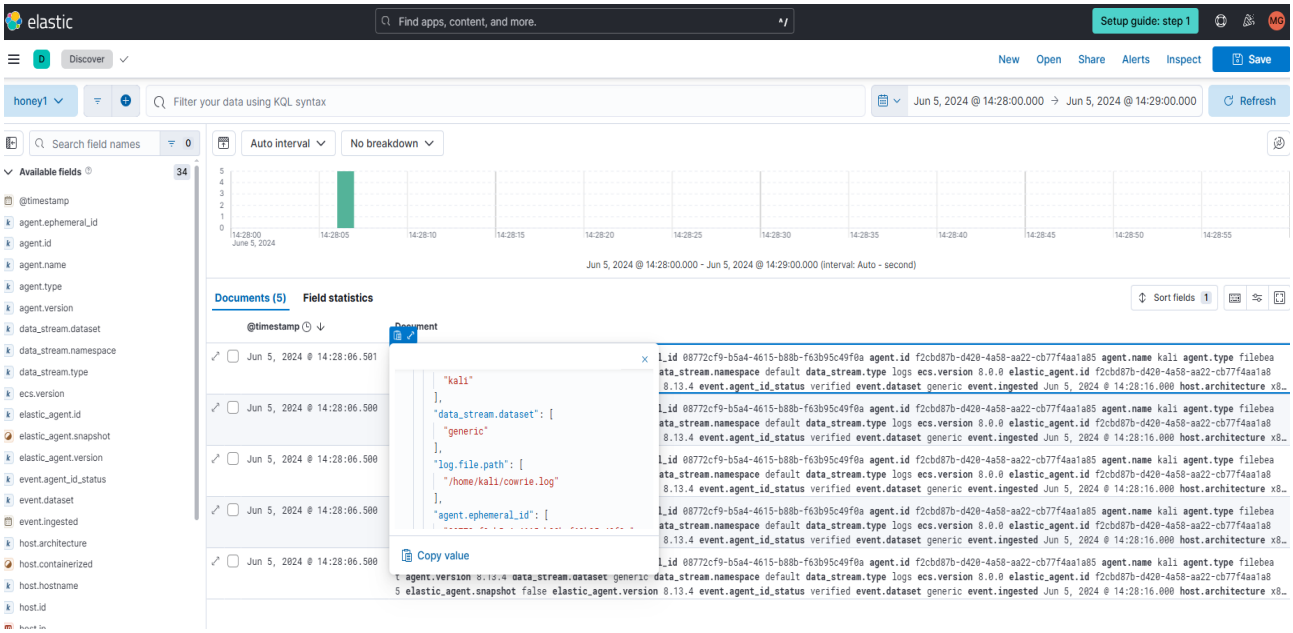
en la siguiente pantalla muestro el archivo cowrie.log, donde se guardan los logs:

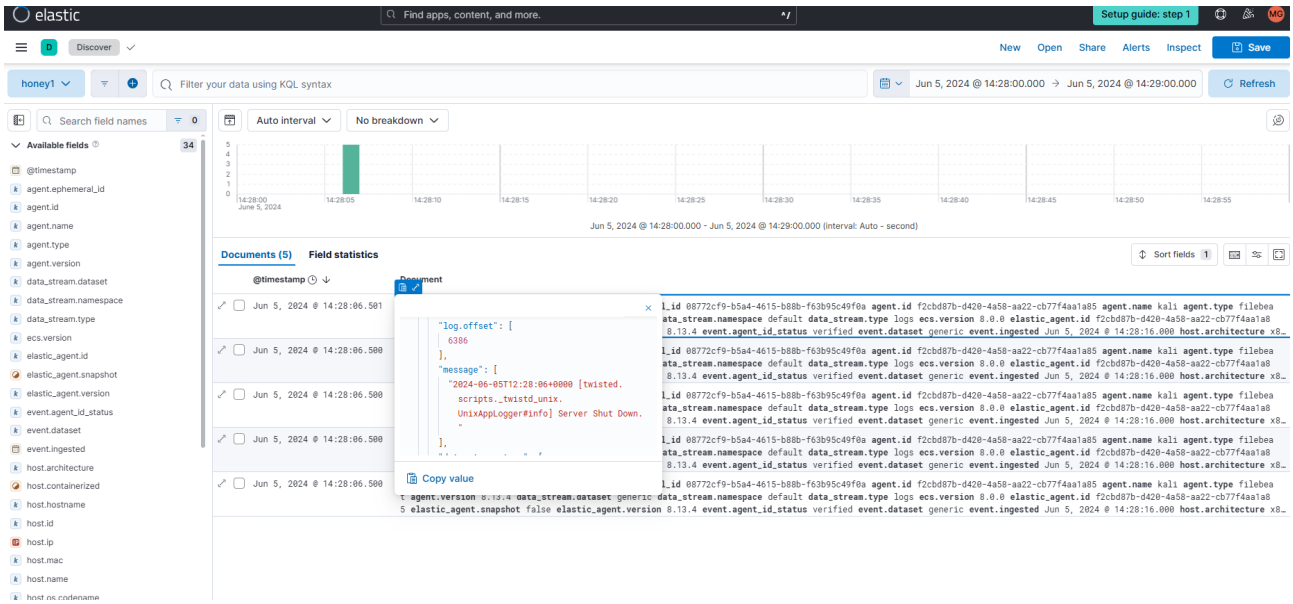


Añadimos los logs a Elastic con “Custom Logs” :

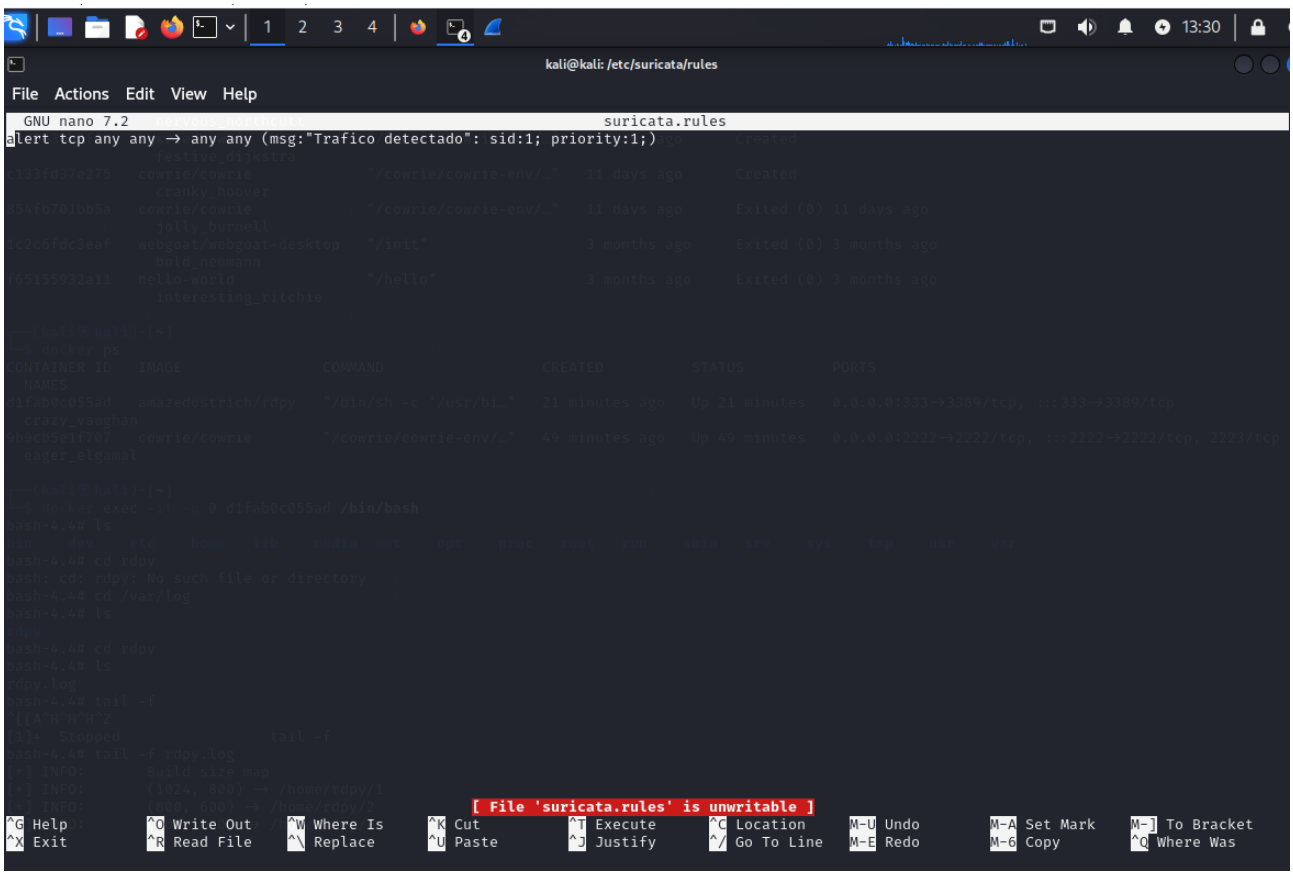


vemos los logs en Elastic

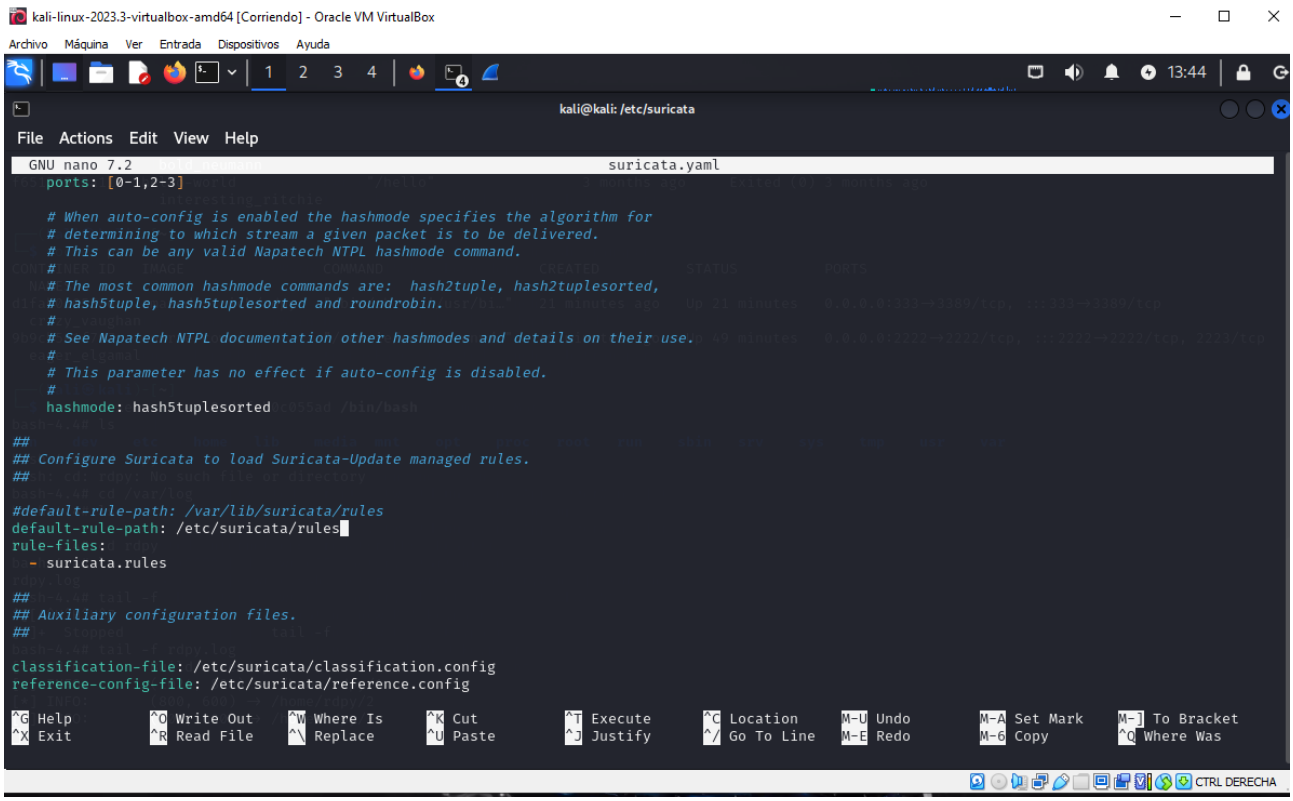




creamos la regla para suricata

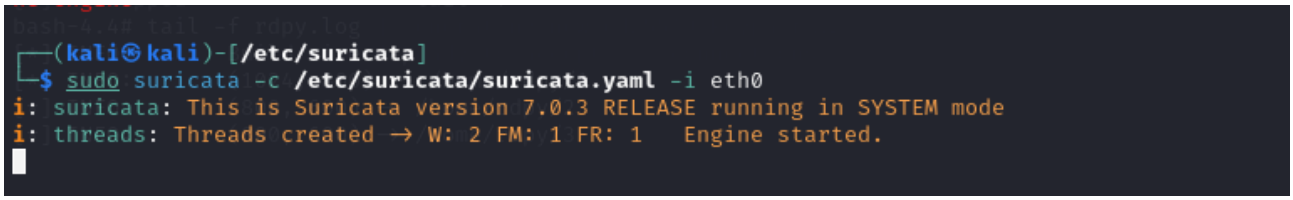


en el archivo suricata.yaml, cambiamos lo siguiente:

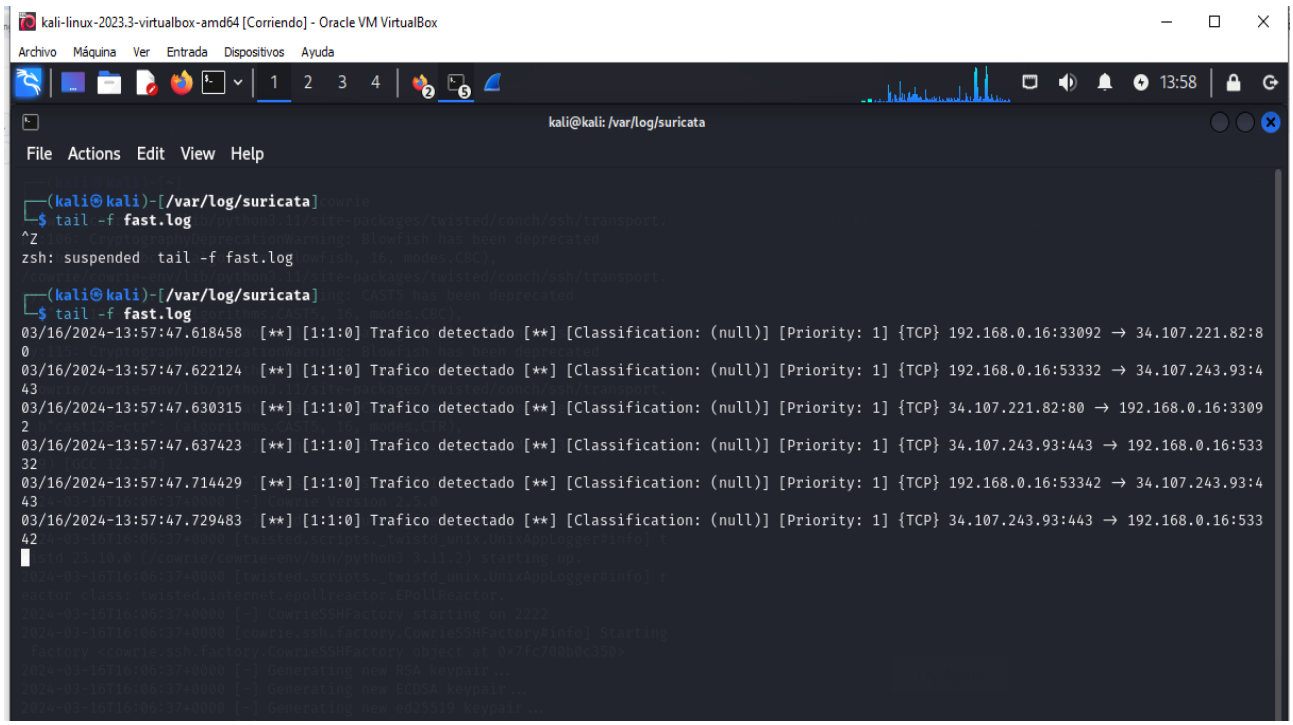


para que nos coja por defecto el archivo suricata.rules que hemos creado

ejecutamos Suricata:

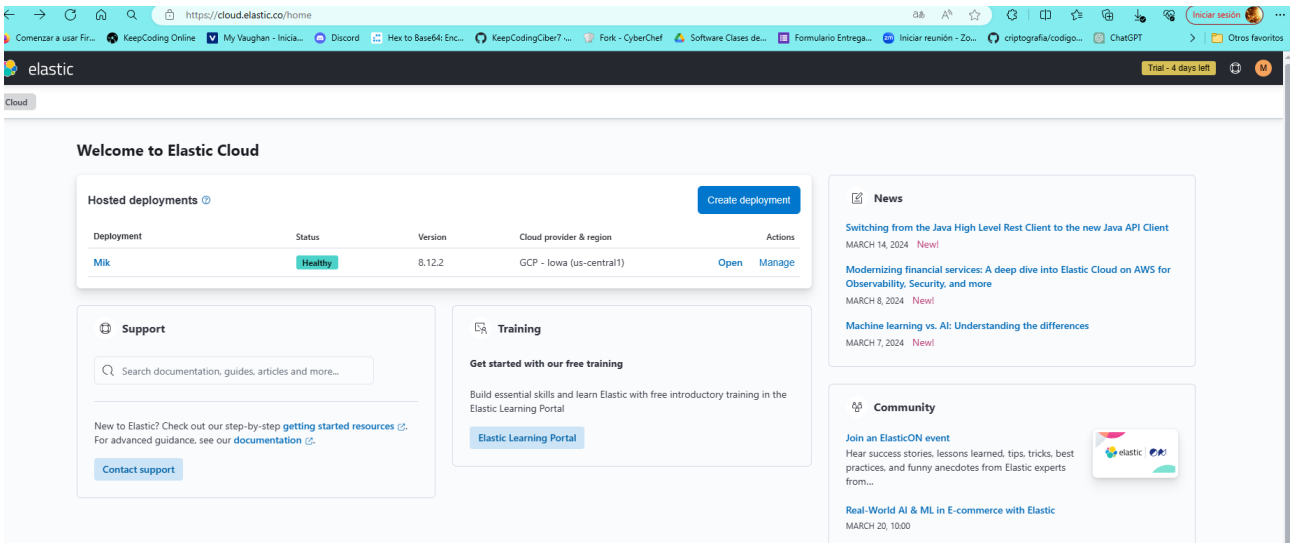


vemos los logs:

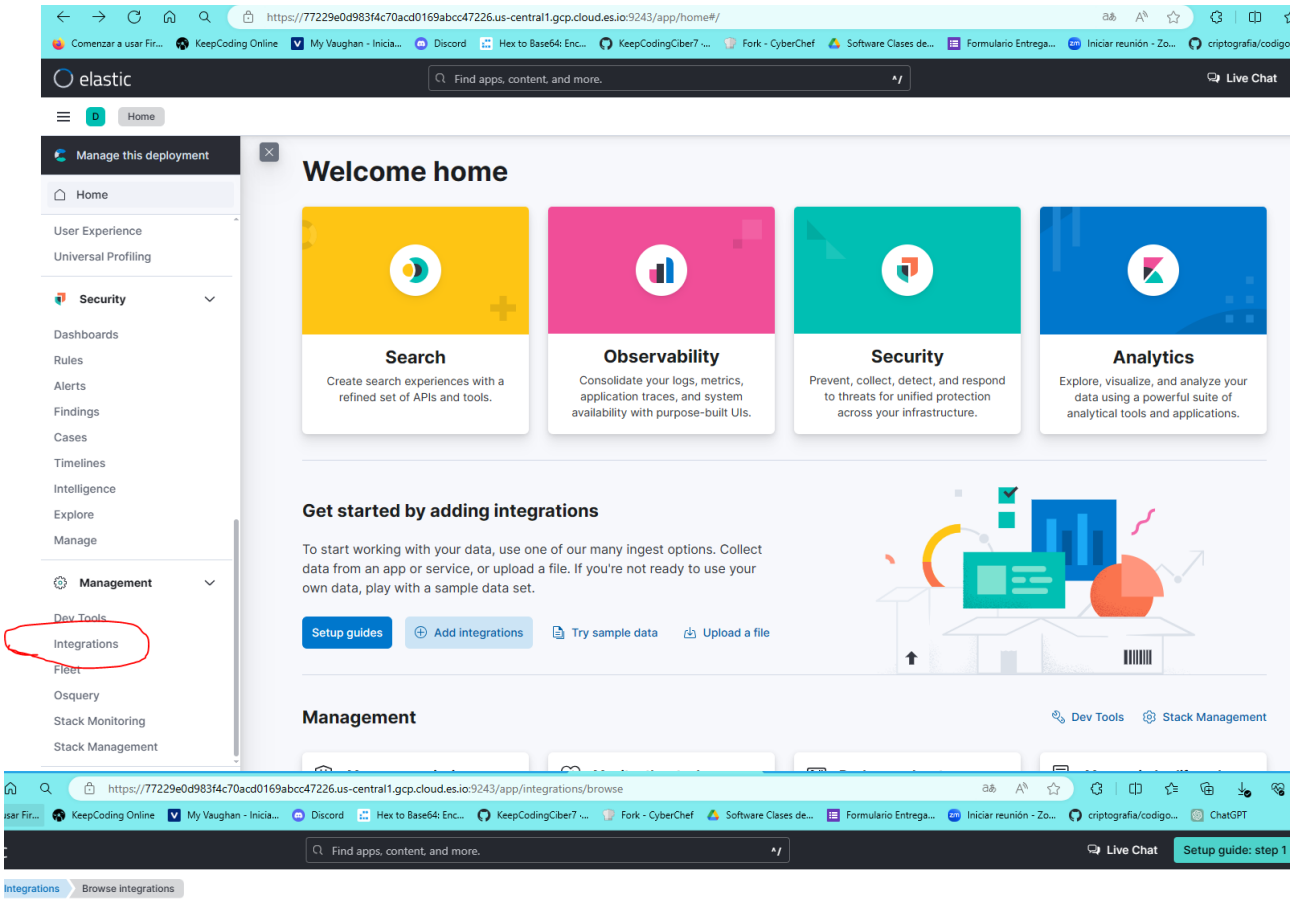


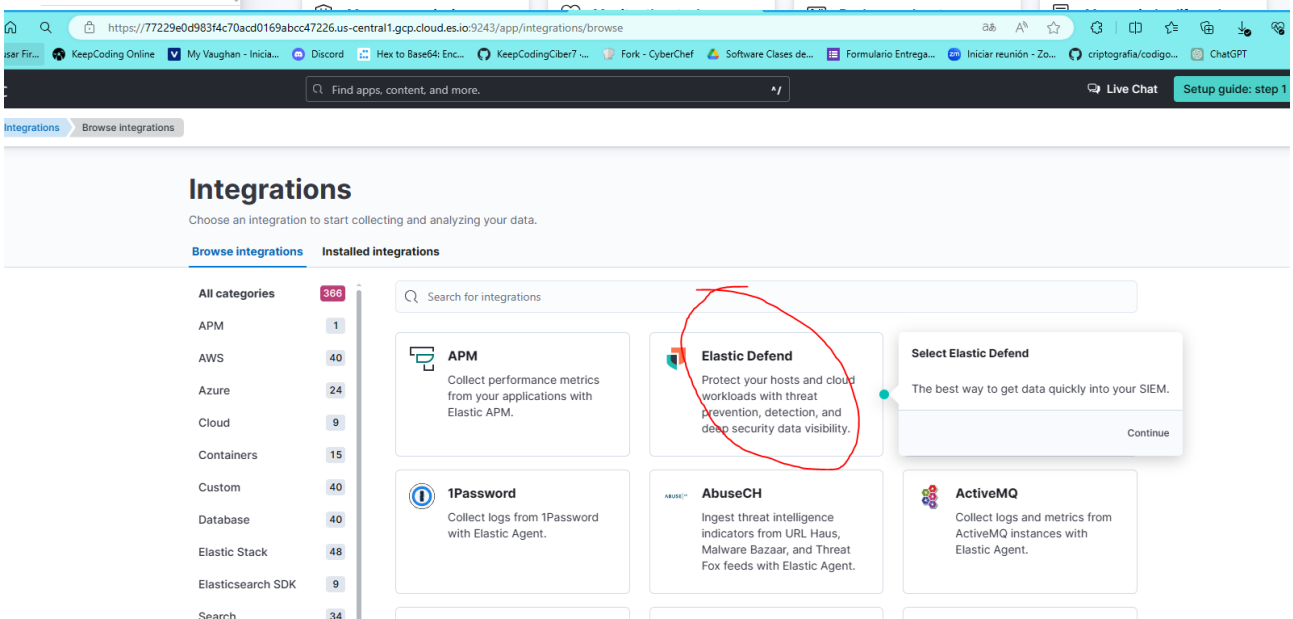
se me peta windows 11 y no puedo hacer nada con él

ELASTIC CLOUD

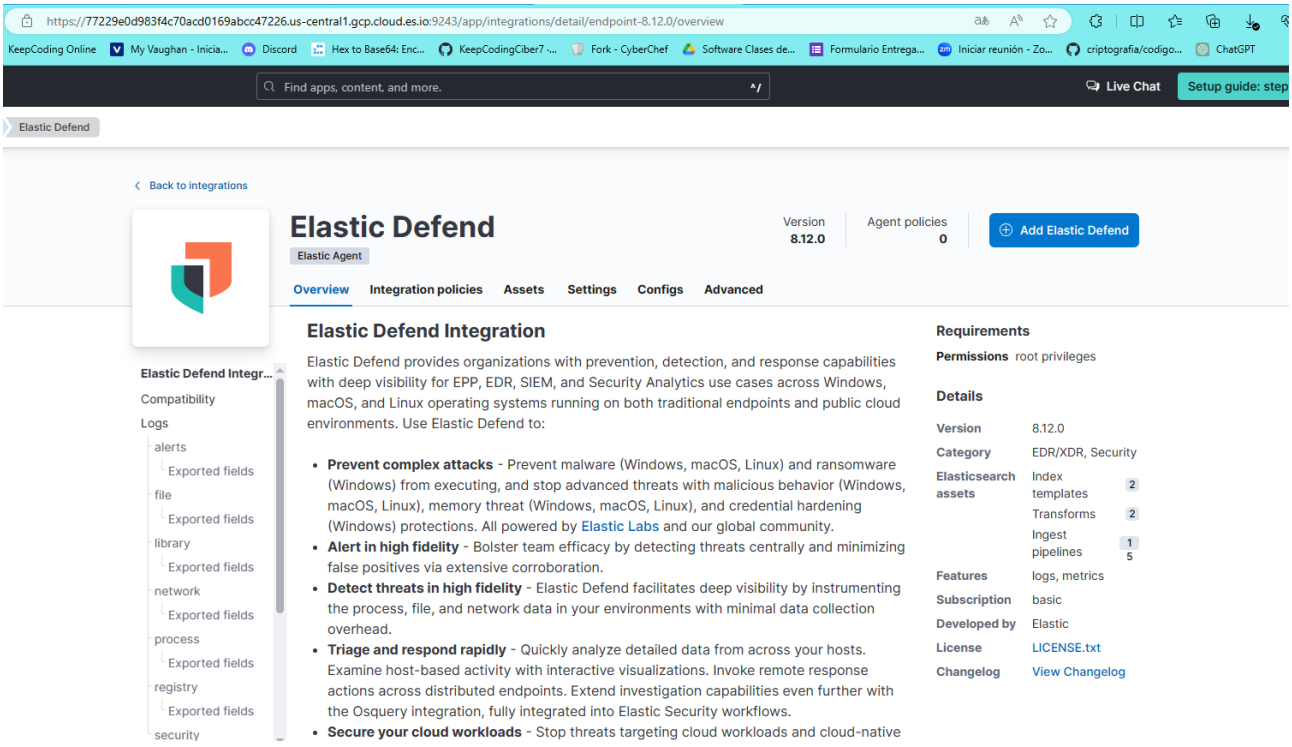


vamos a Management – Integrations

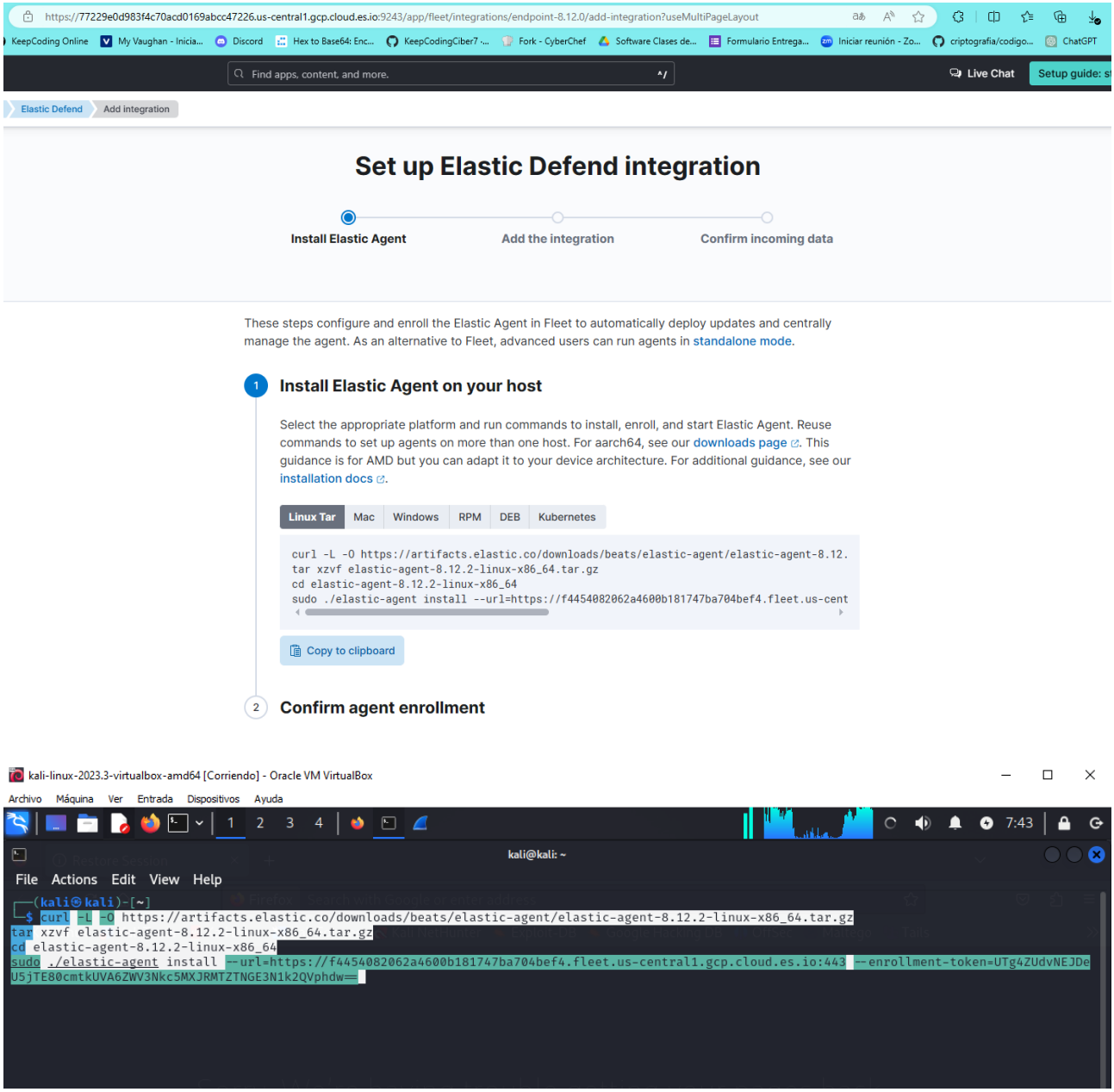




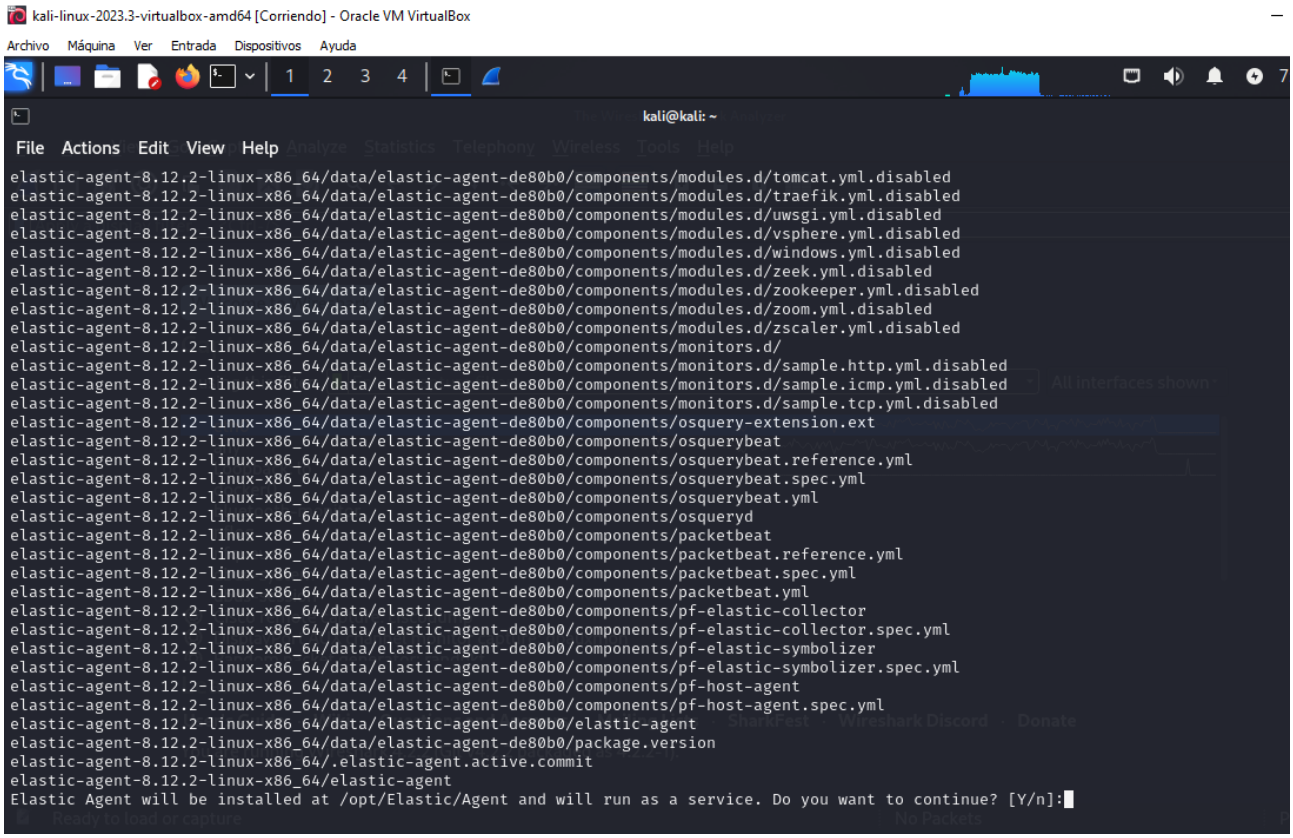
y luego a Elastic Defend



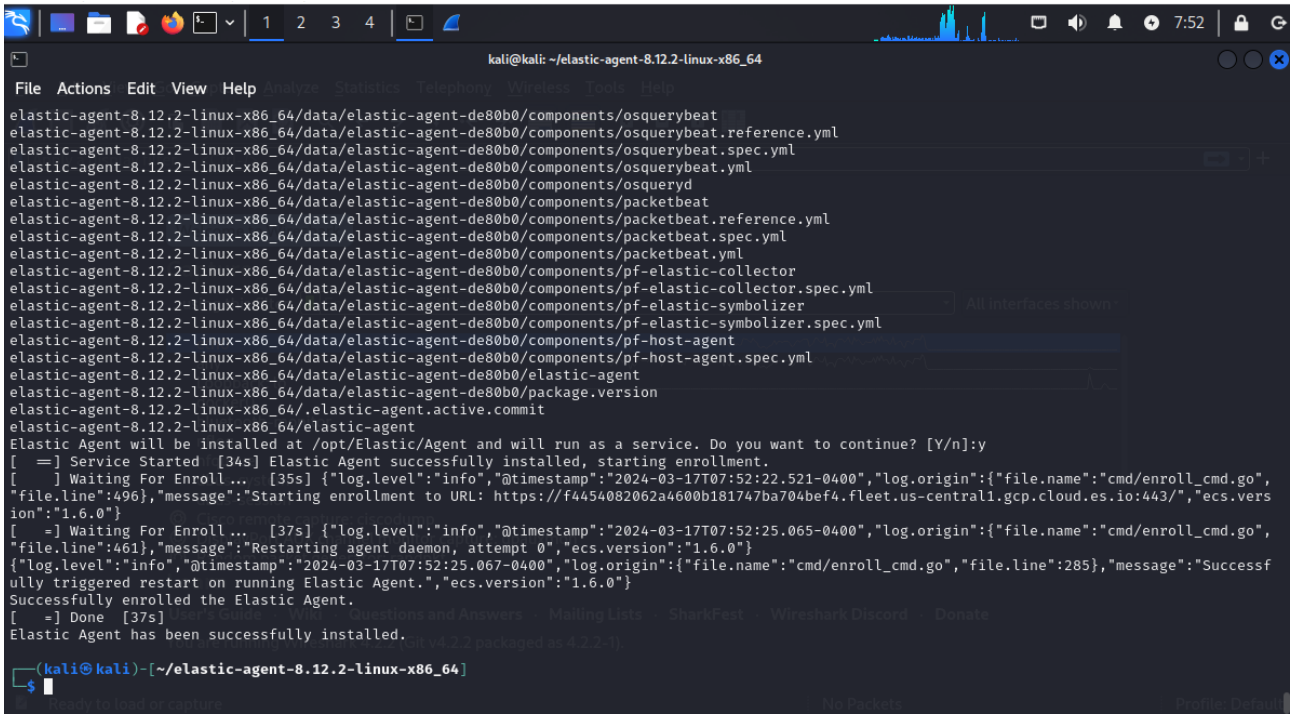
instalamos el agente en la kali, copiando el script:


https://77229e0d983f4c70acd0169abcc47226.us-central1.gcp.cloud.es.io:9243/app/fleet/integrations/endpoint-8.12.0/add-integration?useMultiPageLayout
Find apps, content, and more.
Live Chat
Setup guide:
Elastic Defend
Add integration
Set up Elastic Defend integration
Install Elastic Agent
Add the integration
Confirm incoming data
These steps configure and enroll the Elastic Agent in Fleet to automatically deploy updates and centrally manage the agent. As an alternative to Fleet, advanced users can run agents in standalone mode.
1
Install Elastic Agent on your host
Select the appropriate platform and run commands to install, enroll, and start Elastic Agent. Reuse commands to set up agents on more than one host. For aarch64, see our downloads page. This guidance is for AMD but you can adapt it to your device architecture. For additional guidance, see our installation docs.
Linux Tar
Mac
Windows
RPM
DEB
Kubernetes
curl -L -O https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.12.
tar xzvf elastic-agent-8.12.2-linux-x86_64.tar.gz
cd elastic-agent-8.12.2-linux-x86_64
sudo ./elastic-agent install --url=https://f4454082062a4600b181747ba704bef4.fleet.us-cent
Copy to clipboard
2
Confirm agent enrollment

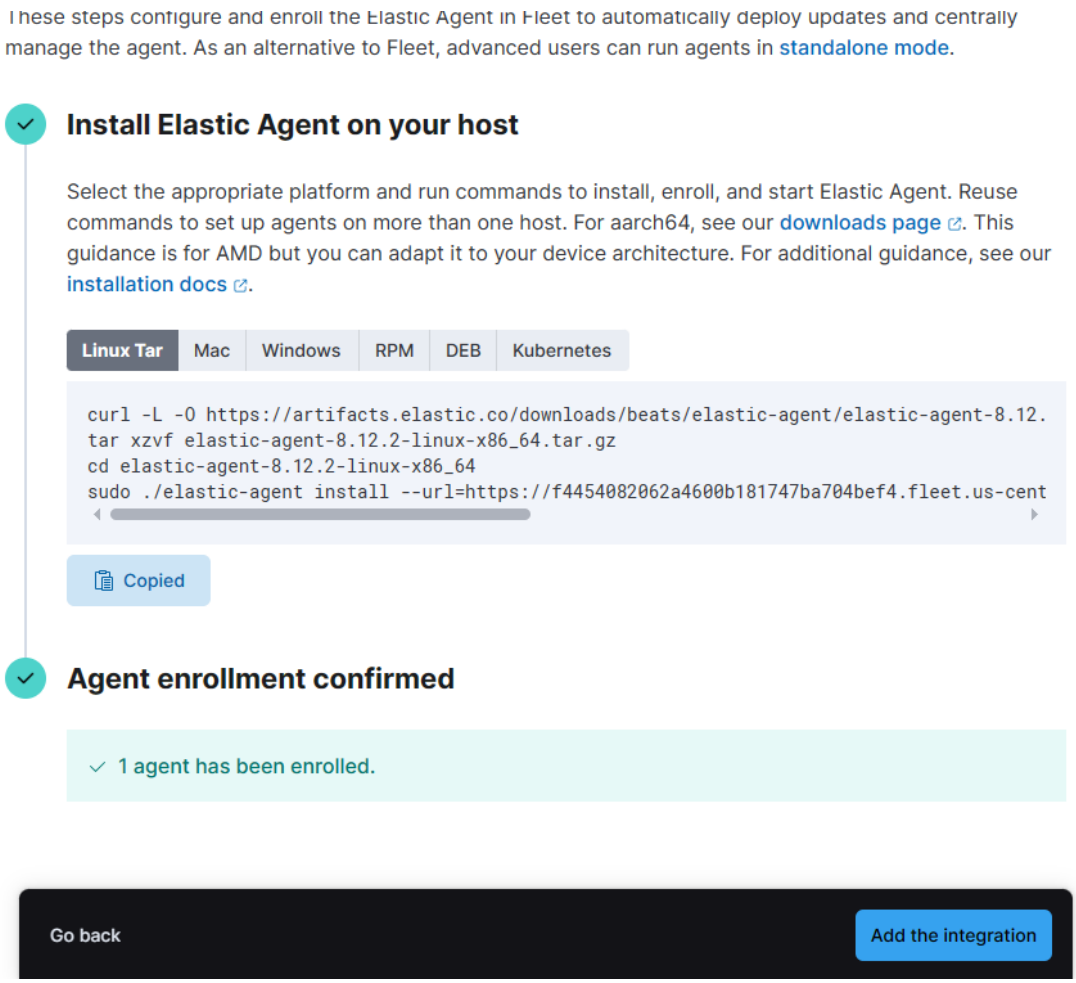
kali-linux-2023.3-virtualbox-amd64 [Corriendo] - Oracle VM VirtualBox
Archivo
Máquina
Ver
Entrada
Dispositivos
Ayuda
7:43
kali@kali: ~
File
Actions
Edit
View
Help
curl -L -O https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.12.2-linux-x86_64.tar.gz
tar xzvf elastic-agent-8.12.2-linux-x86_64.tar.gz
cd elastic-agent-8.12.2-linux-x86_64
sudo ./elastic-agent install --url=https://f4454082062a4600b181747ba704bef4.fleet.us-central1.gcp.cloud.es.io:443 --enrollment-token=UTg4ZUdvNEJDe
U5jTE80cmtkUVA6ZWV3Nkc5MXJRMTZTNGE3N1k2QVphdw==

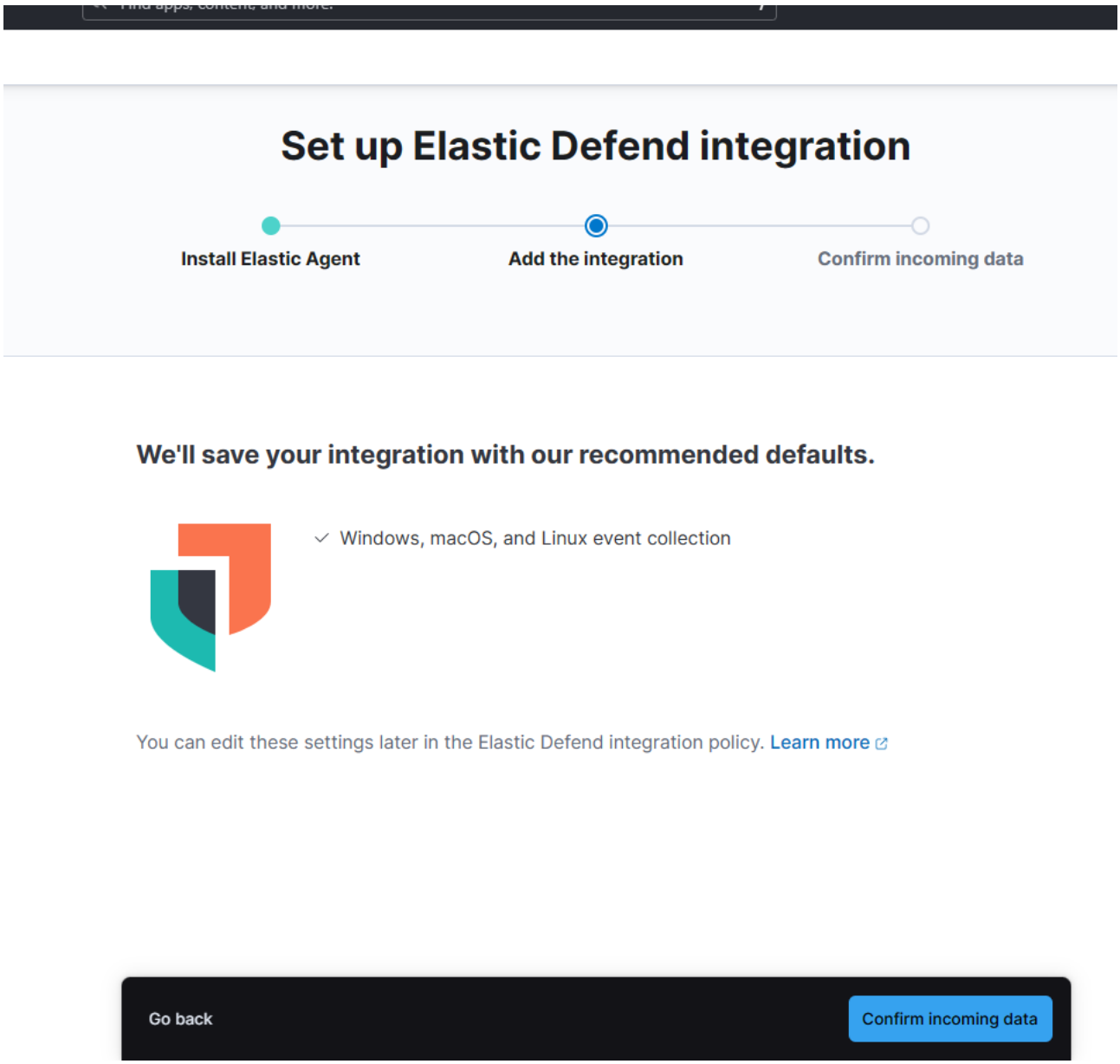


instalado el agente:

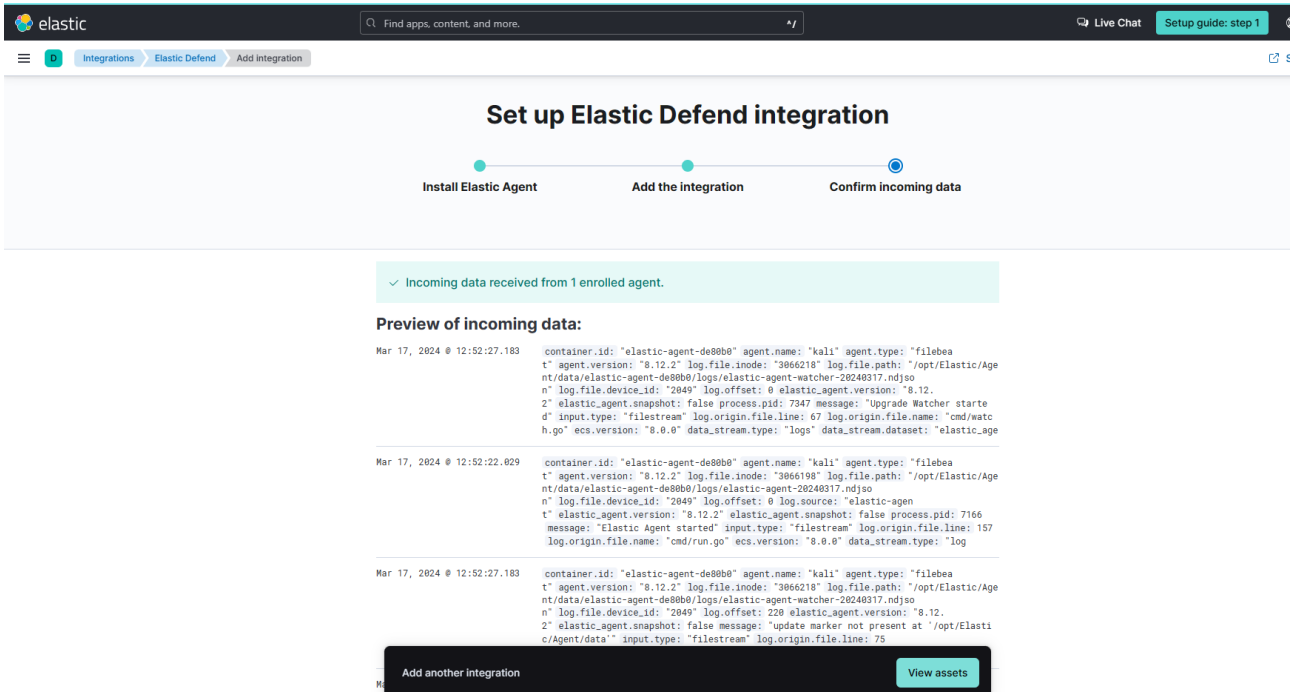


damos en Add the itegration



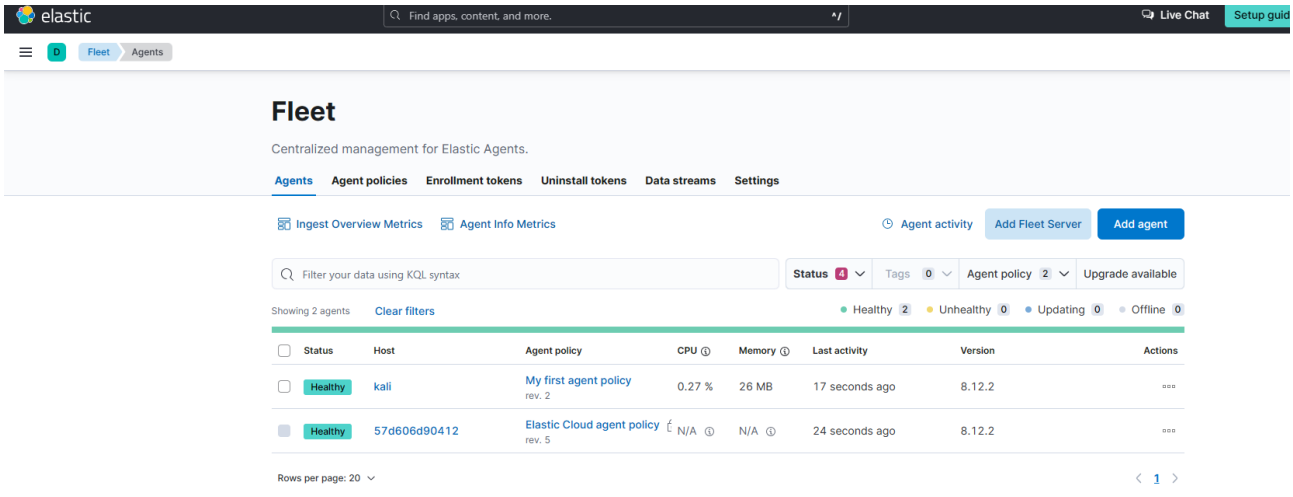


aquí vemos los logs que vienen de kali:

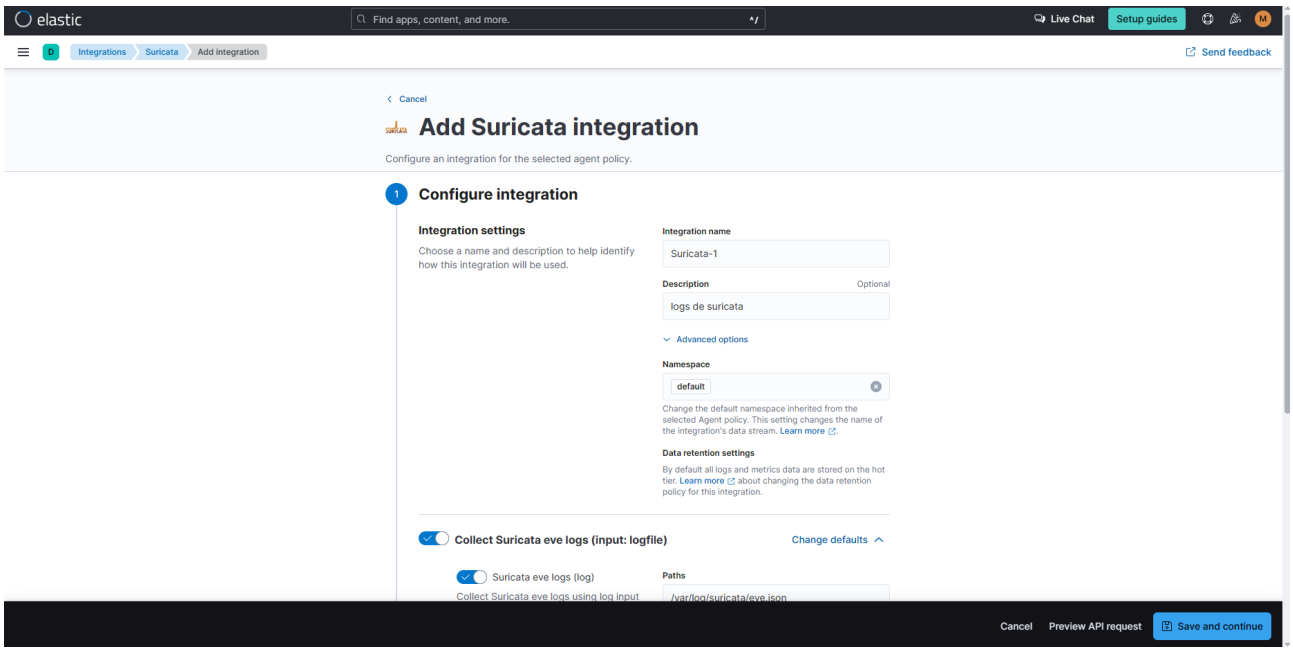


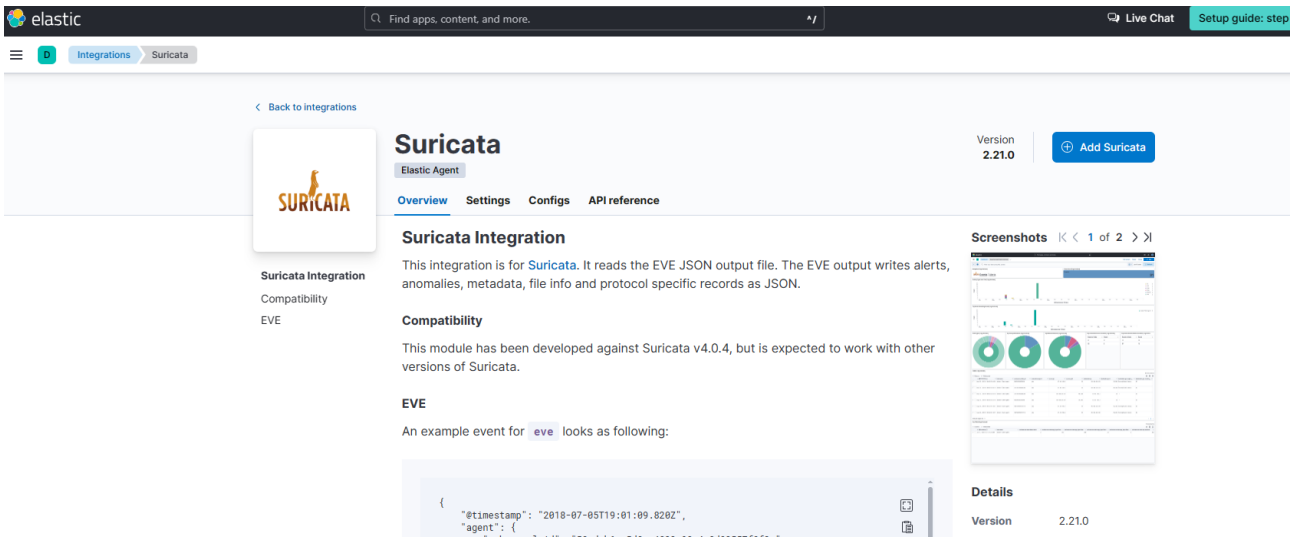
damos click a ver assets (ver activos)

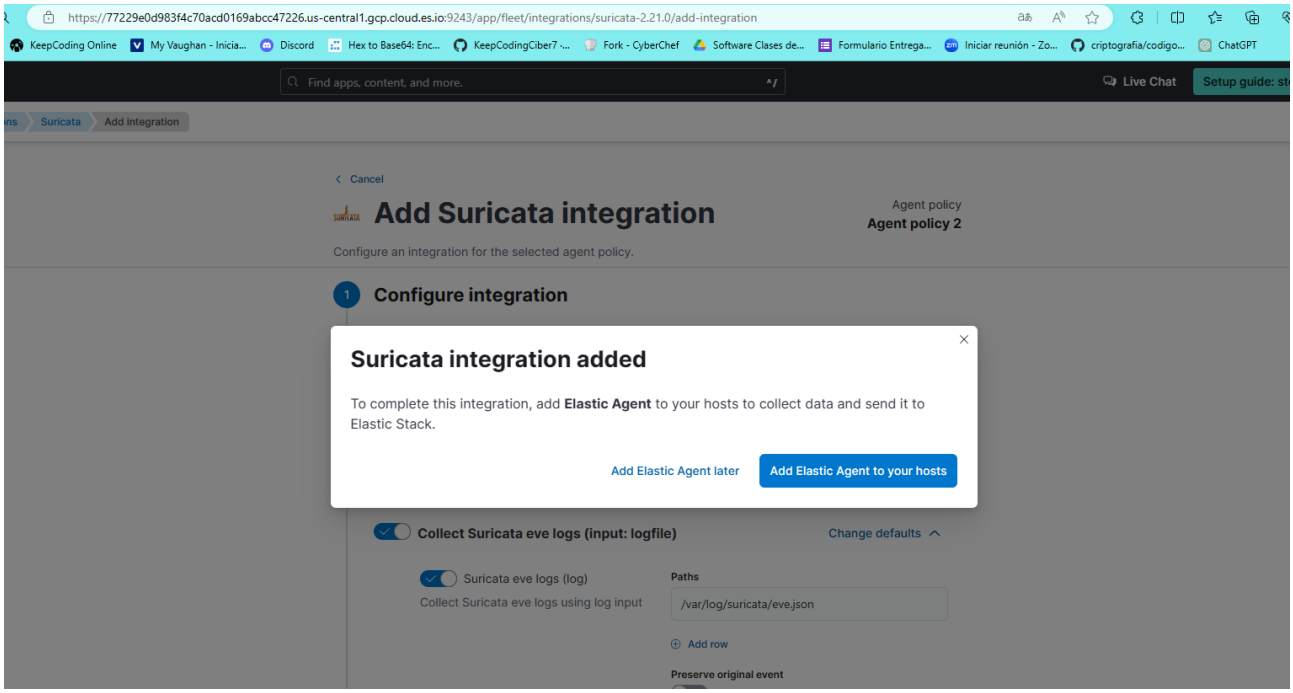
nos vamos a Fleet para ver las políticas, que son las reglas para recoger los logs:

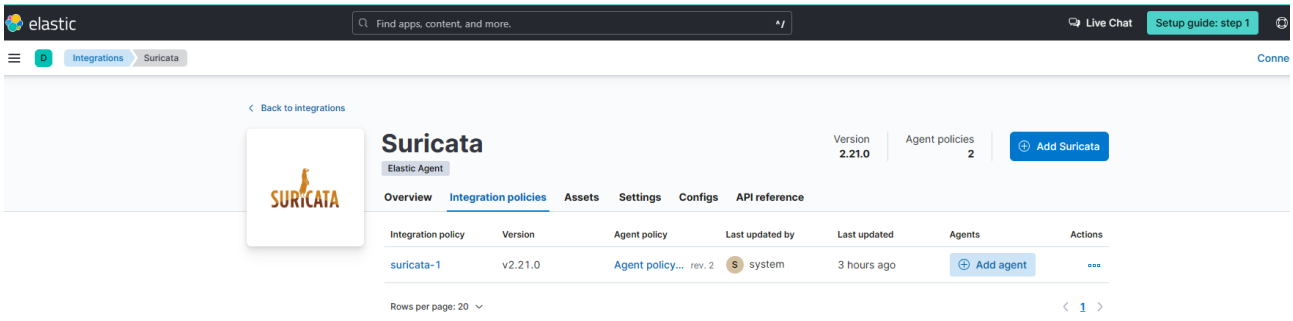


podemos integrar Suricata para recoger los logs de Suricata.

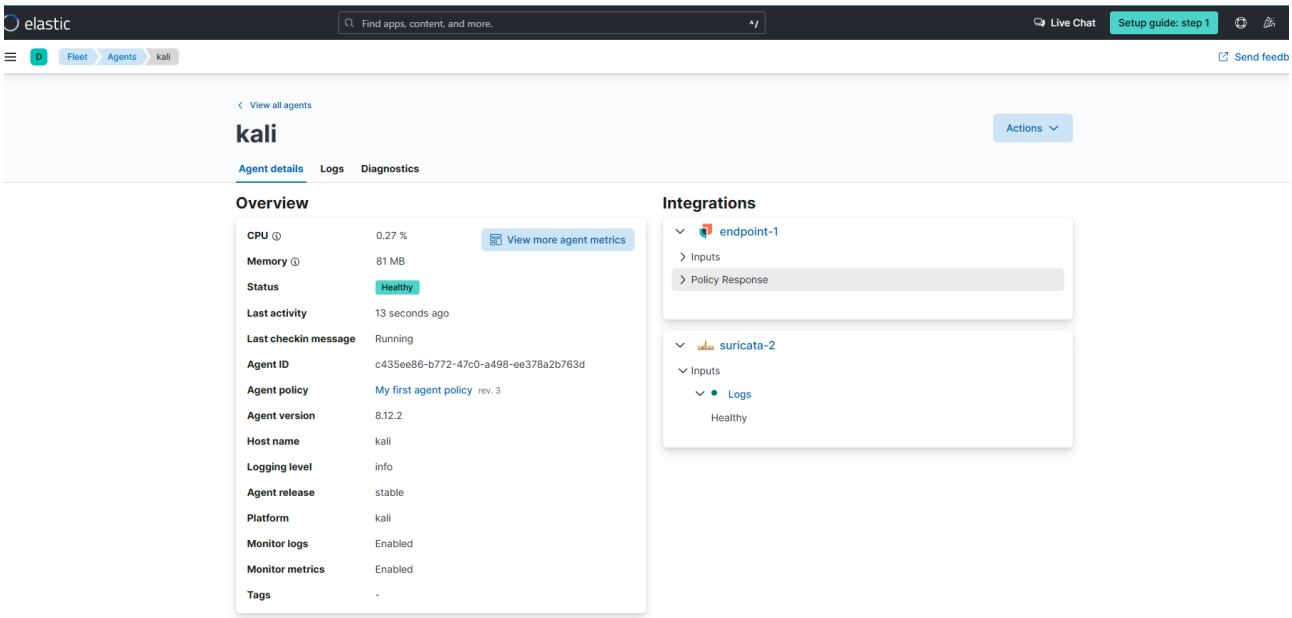

elastic
Find apps, content, and more.
Live Chat
Setup guides
Integrations
Suricata
Add integration
Send feedback
Cancel
Add Suricata integration
Configure an integration for the selected agent policy.
1
Configure integration
Integration settings
Choose a name and description to help identify how this integration will be used.
Integration name
Suricata-1
Description
Optional
logs de suricata
Advanced options
Namespace
default
Change the default namespace inherited from the selected Agent policy. This setting changes the name of the integration's data stream. Learn more.
Data retention settings
By default all logs and metrics data are stored on the hot tier. Learn more about changing the data retention policy for this integration.
Collect Suricata eve logs (input: logfile)
Change defaults
Suricata eve logs (log)
Collect Suricata eve logs using log input
Paths
/var/log/suricata/eve.json
Cancel
Preview API request
Save and continue

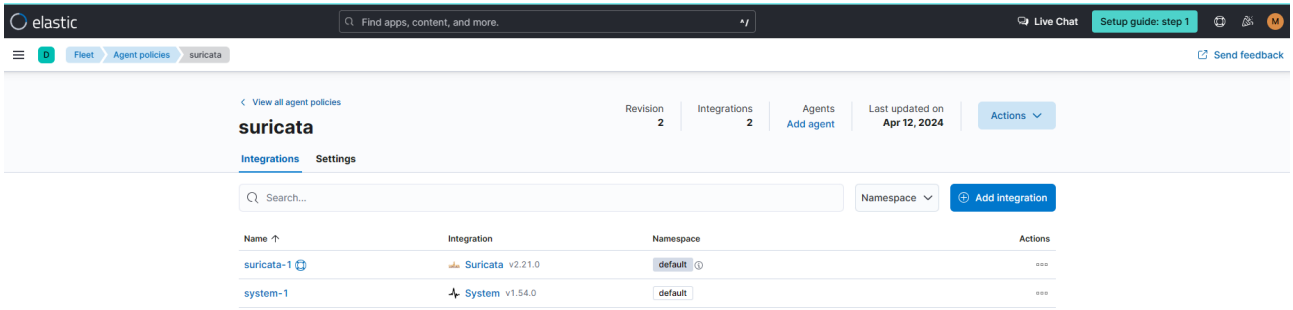




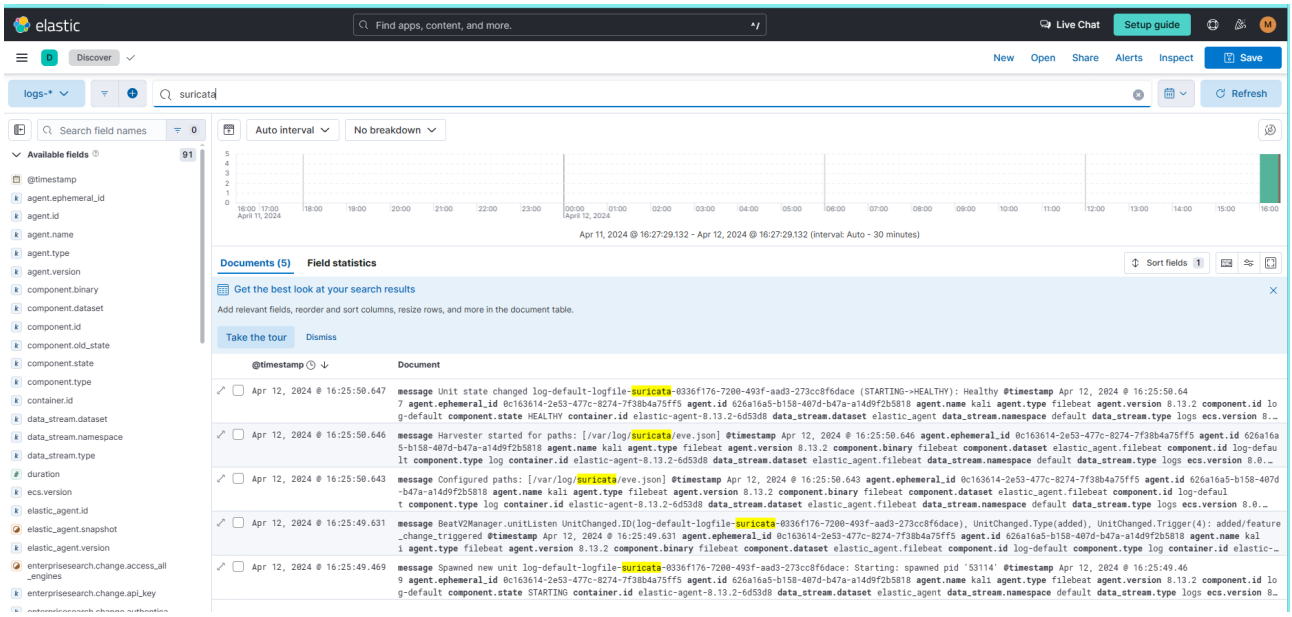


Aquí vemos la integración que tiene nuestra máquina kali con suricata, para poder tener logs de suricata.

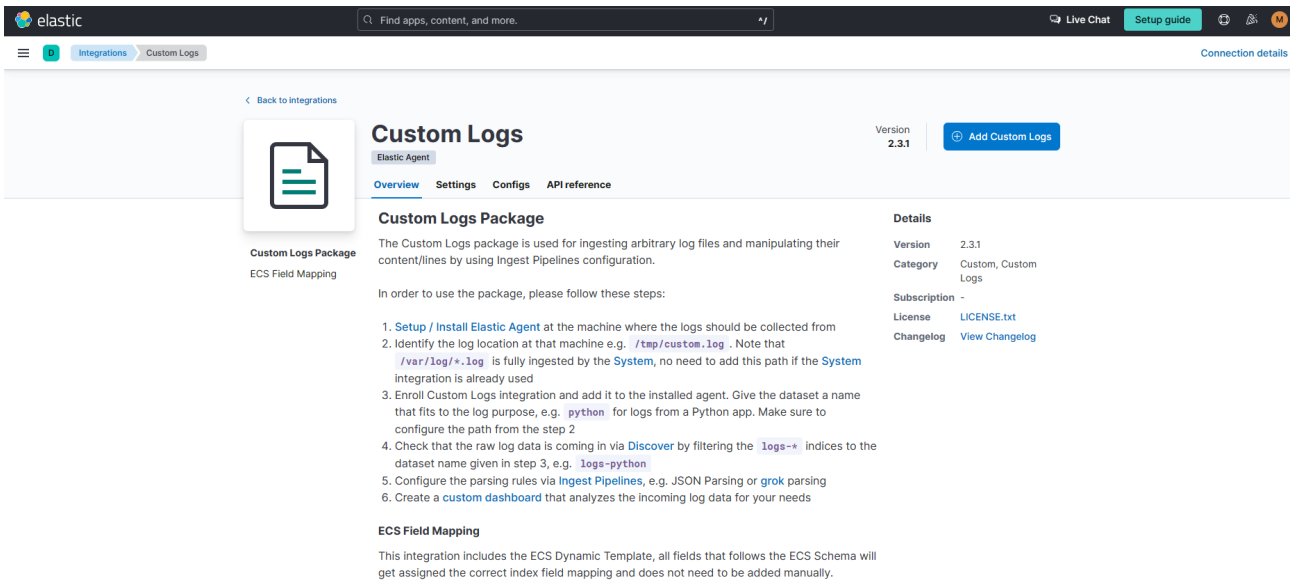

elastic
Find apps, content, and more.
Live Chat
Setup guide: step 1
Fleet
Agents
kali
Send feedb
View all agents
kali
Actions
Agent details
Logs
Diagnostics
Overview
CPU
0.27 %
View more agent metrics
Memory
81 MB
Status
Healthy
Last activity
13 seconds ago
Last checkin message
Running
Agent ID
c435ee86-b772-47c0-a498-ee378a2b763d
Agent policy
My first agent policy
rev. 3
Agent version
8.12.2
Host name
kali
Logging level
info
Agent release
stable
Platform
kali
Monitor logs
Enabled
Monitor metrics
Enabled
Tags
-
Integrations
endpoint-1
Inputs
Policy Response
suricata-2
Inputs
Logs
Healthy

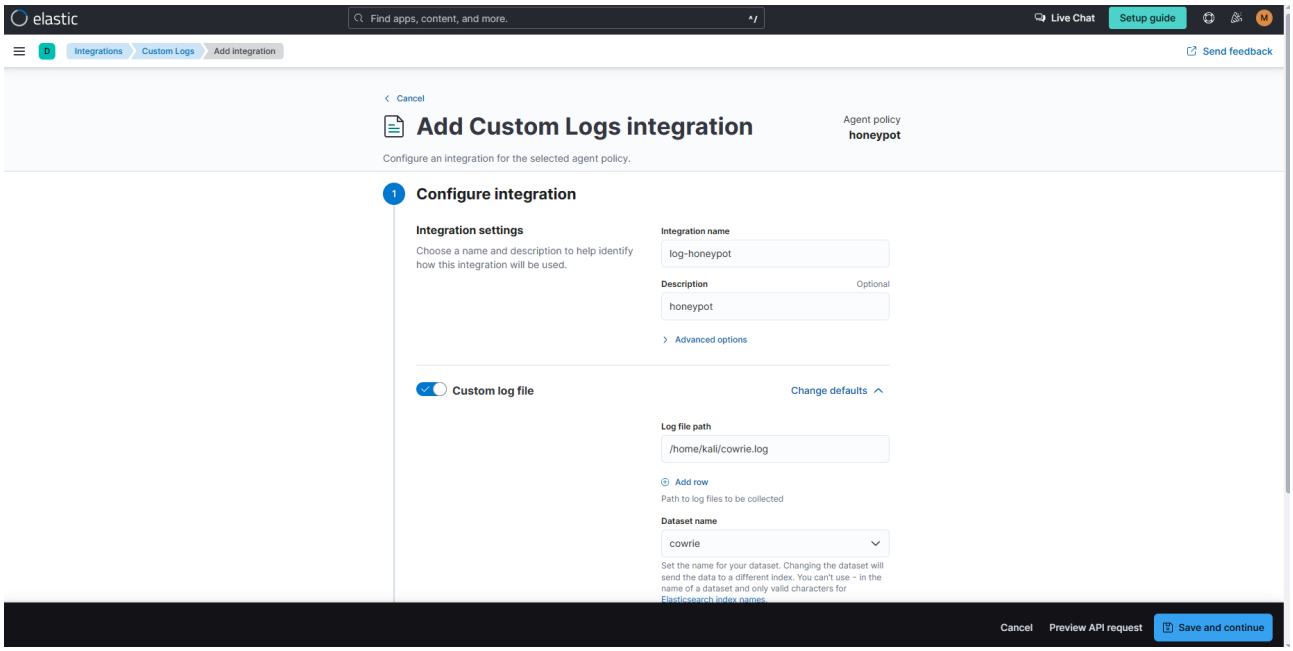


Aquí podemos ver los logs de Suricata:

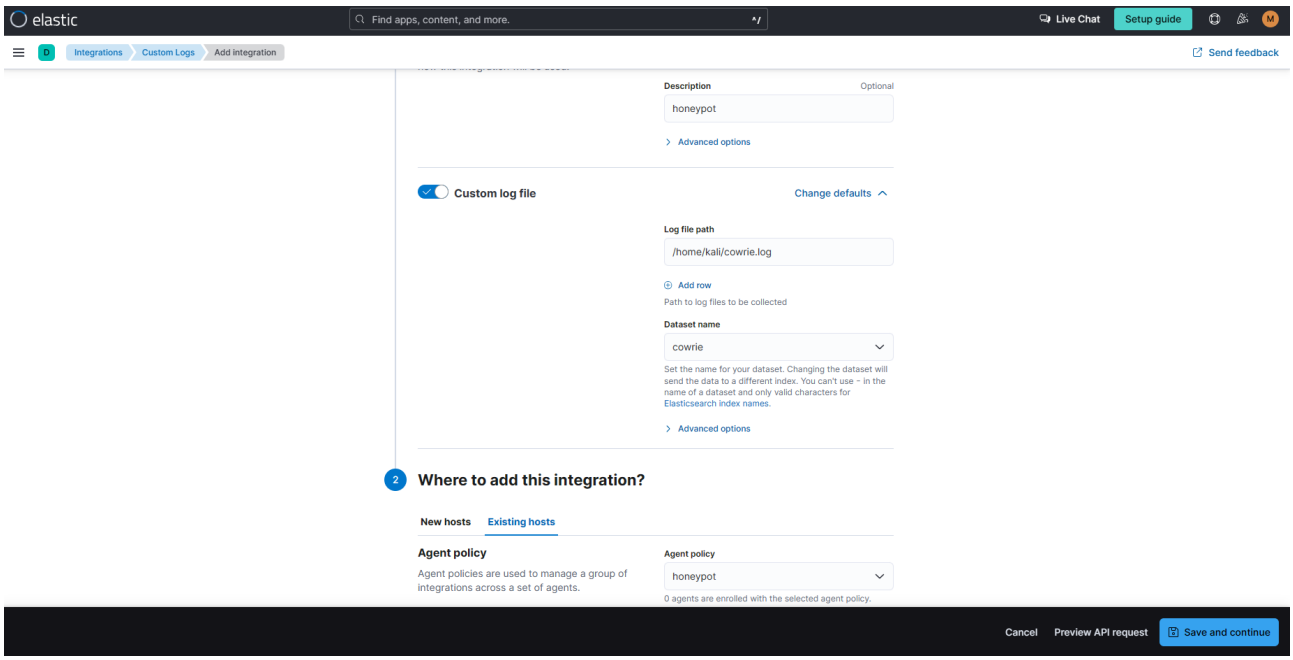


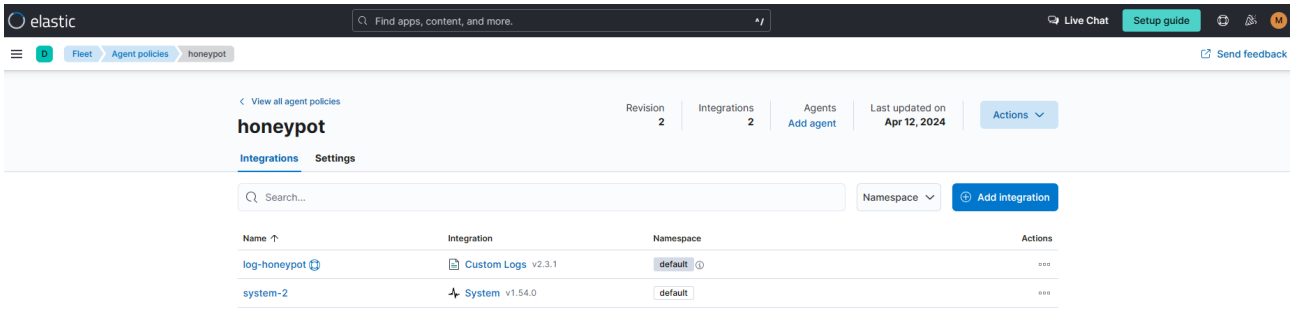
Integracion de los logs de Honeypot en Elastic



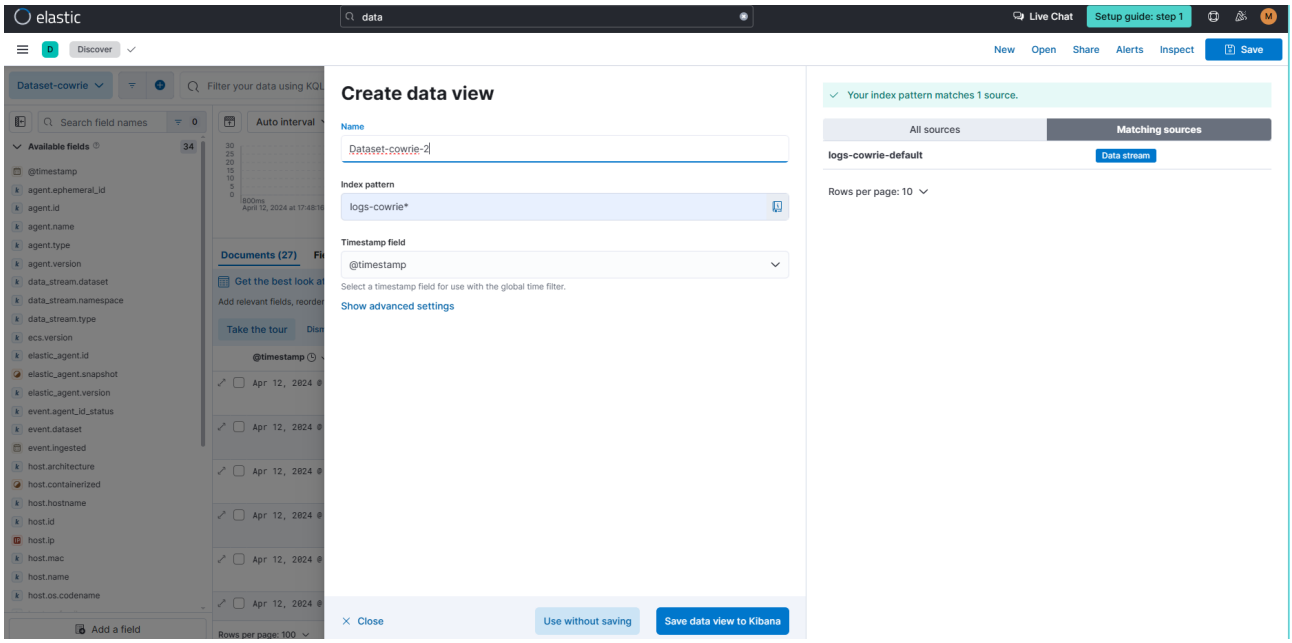


podemos crear los conjuntos de datos que queremos ver

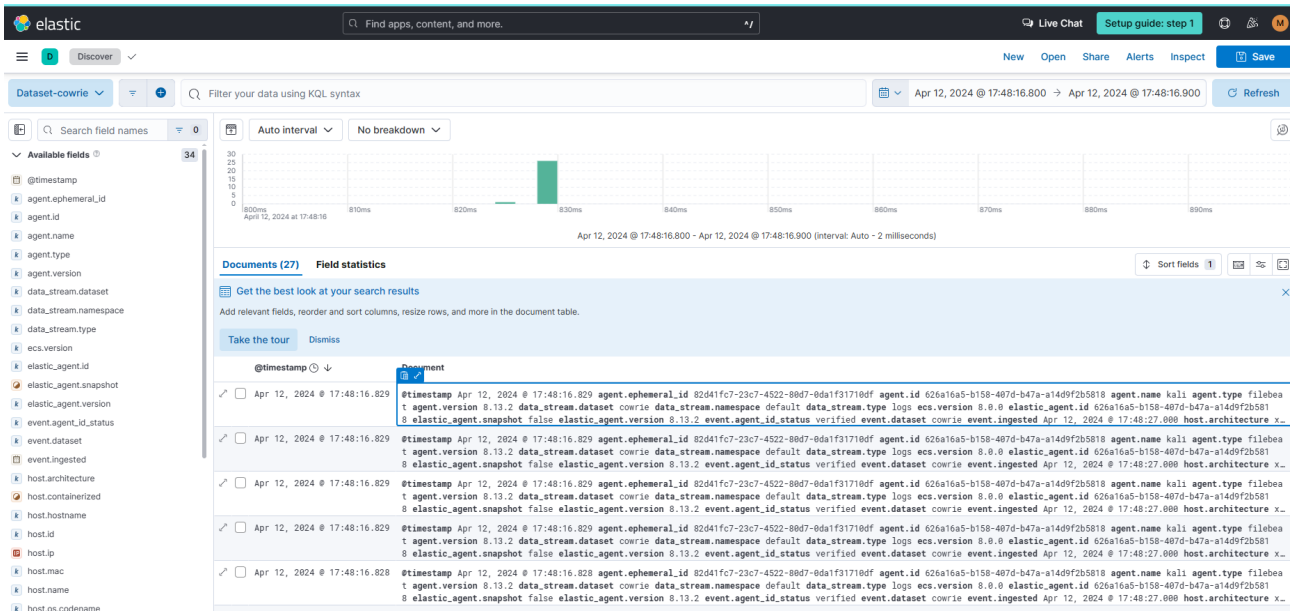




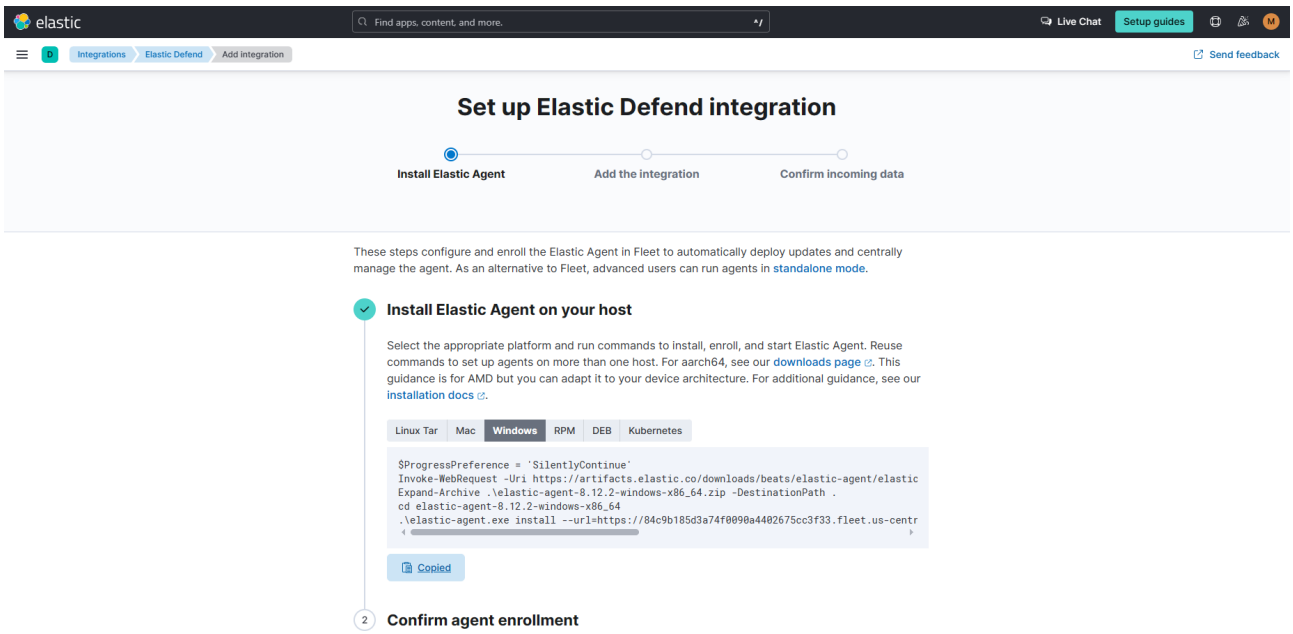
creamos un Dataset para el honeypot (Cowrie)



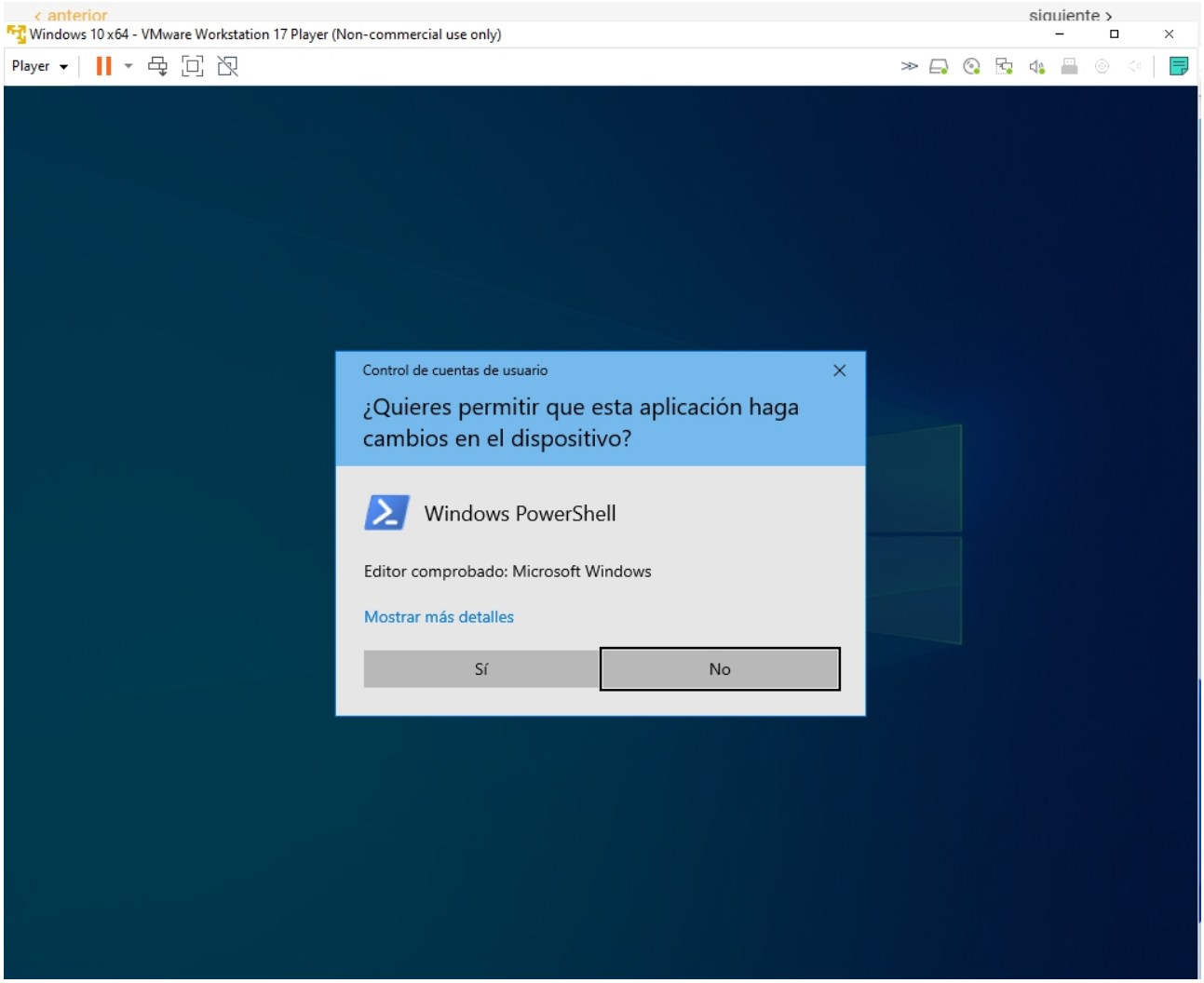
comprobamos los logs del honeypot (Cowrie)

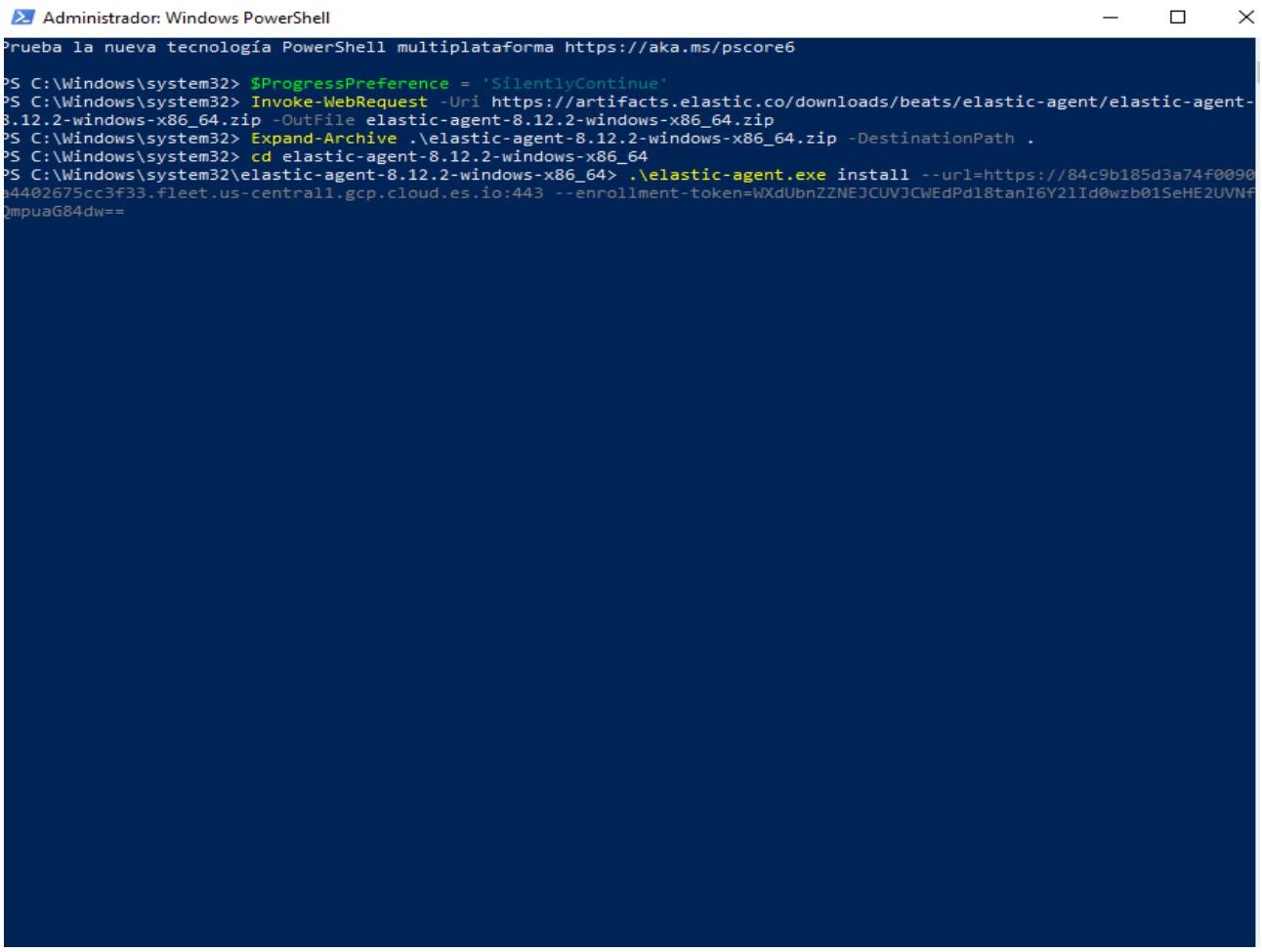


Integración con Windows 10:

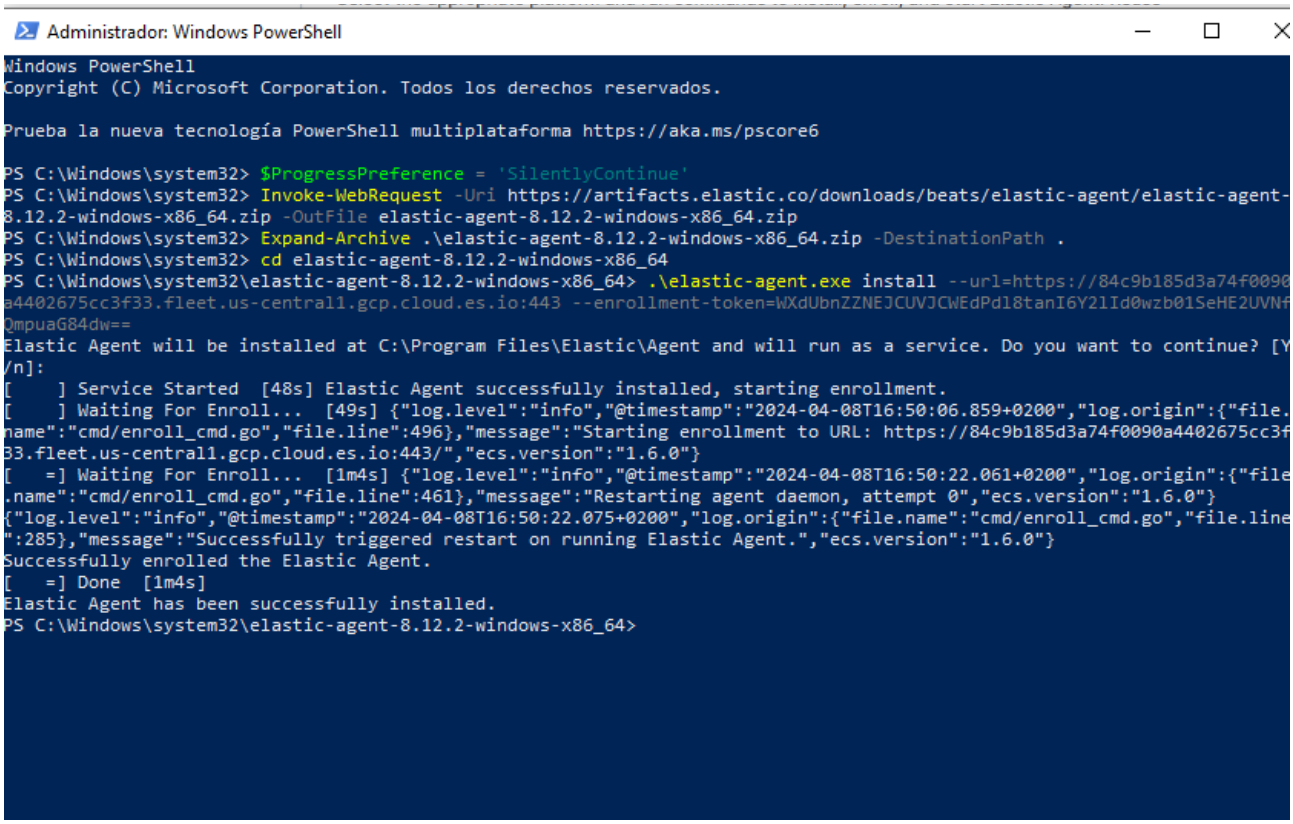


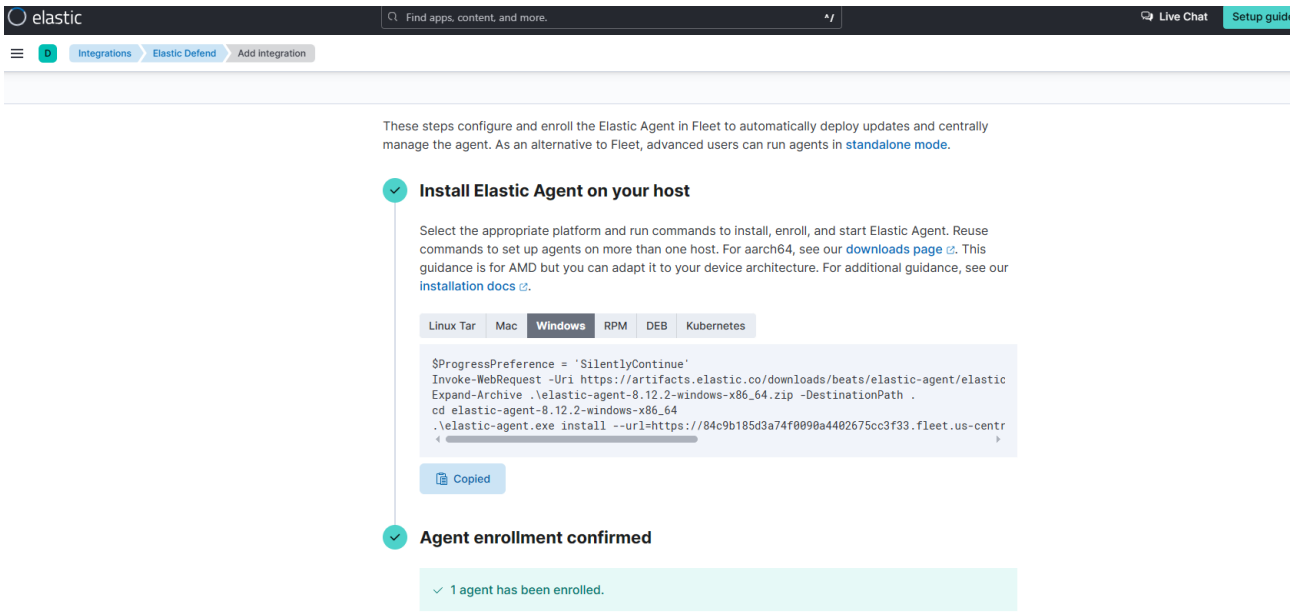
copiamos el comando, y nos vamos a PowerShell de windows 10, lo ejecutamos como administrador:

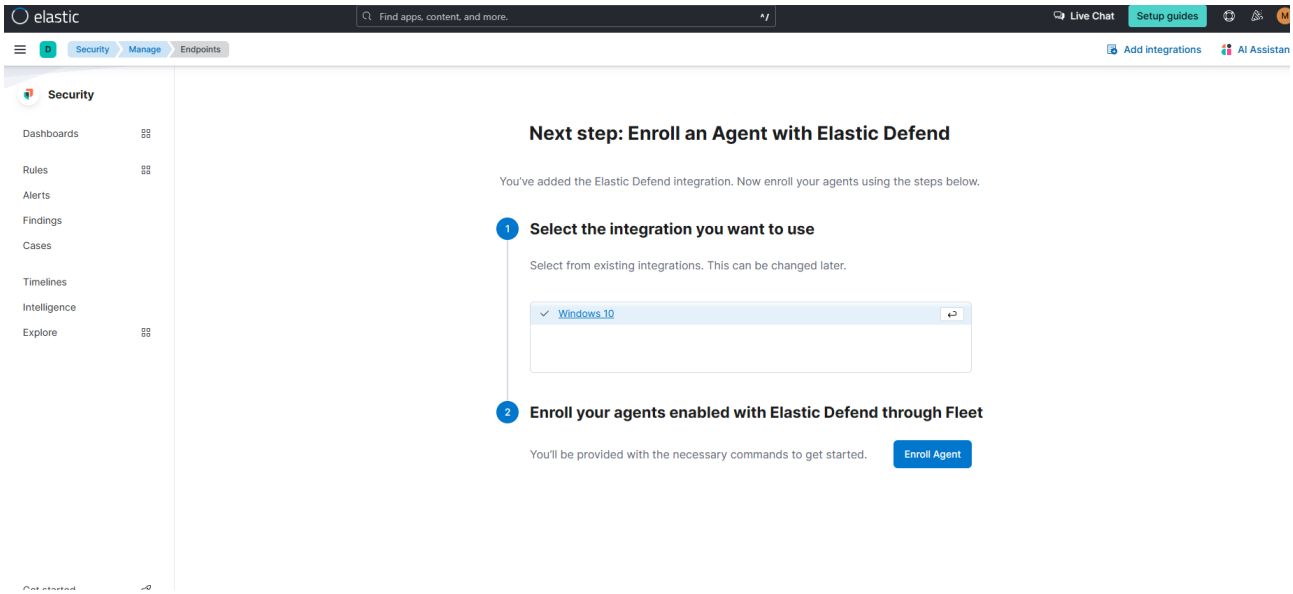




comprobamos que Elastic Agent ha sido instalado:

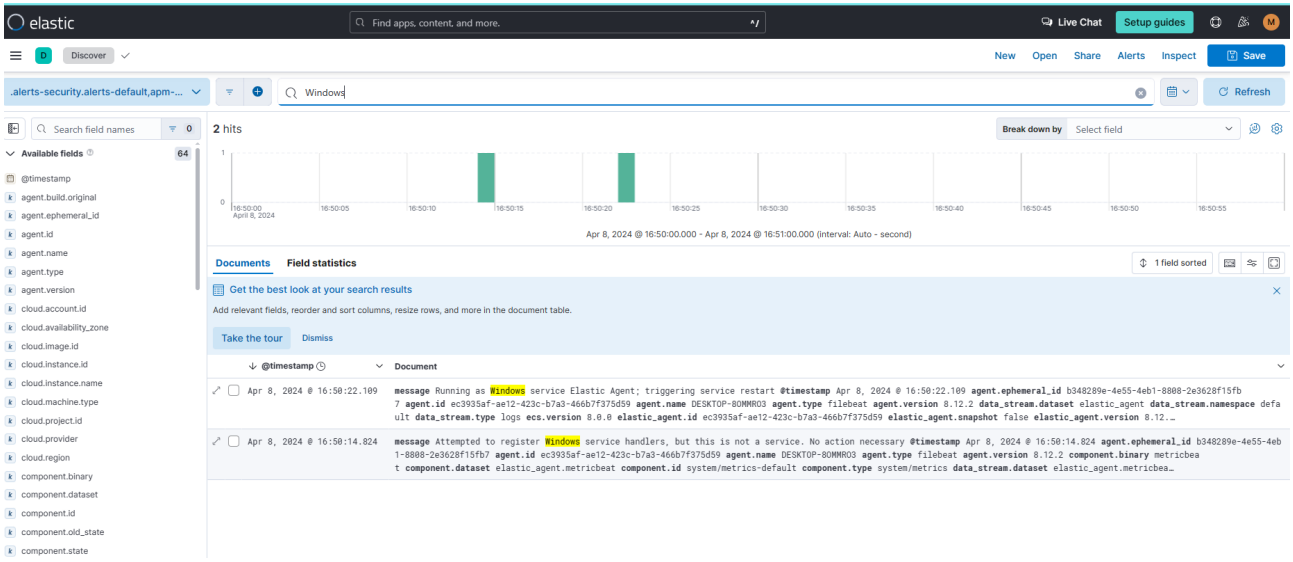






Damos click a Enroll Agent

Aquí podemos ver los logs de windows:



FIN DE PRÁCTICA