Practica Blue Team

Profesor: Sergio Vilches

Alumno: Guillermo V. García Muñoz

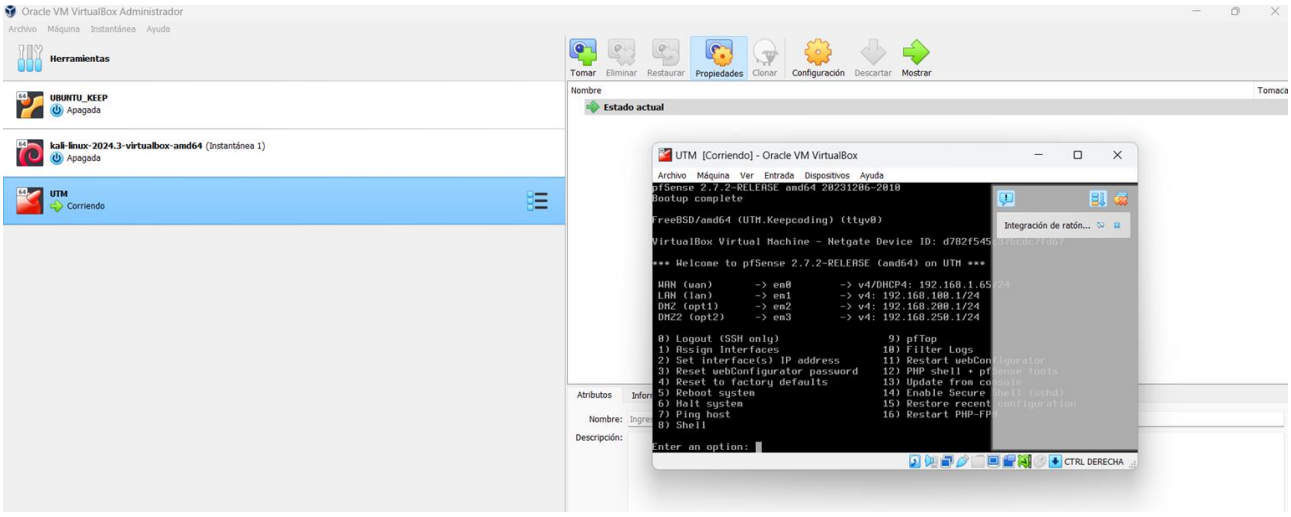
Práctica de KeepCoding Blue Team

KeepCoding Bootcamp Ciberseguridad | Edición IX

Índice

1. Instalación de Pfsense

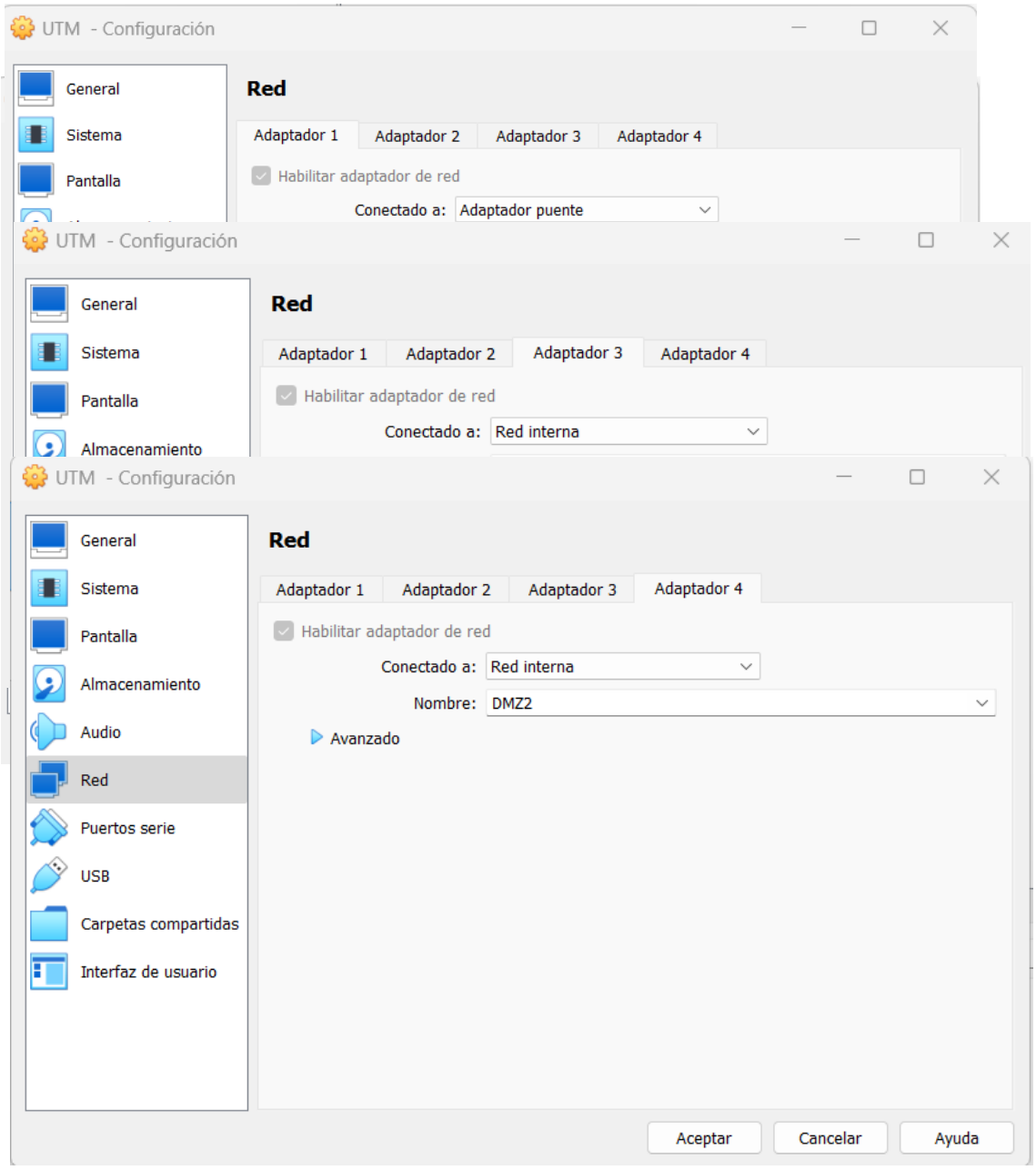
Se instala virtualBox y se crea una máquina nueva, en este caso llamada UTM, que es la que va a ser el Pfsense en el que se van a interconectar nuestro esquema de red con las redes LAN, DMZ y DMZ2.



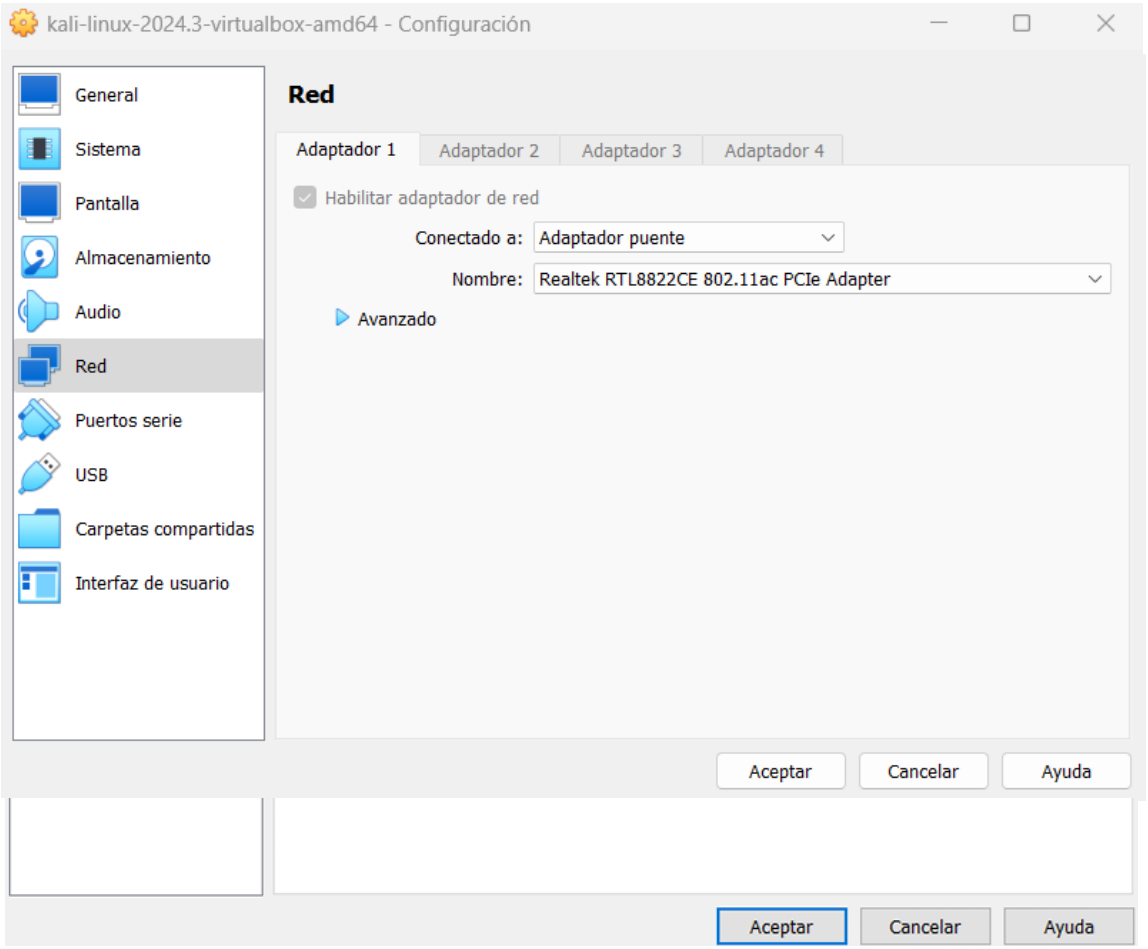
Para ello configuramos las interfaces de red en los adaptadores de red, configurando la red LAN, el DMZ y el DMZ2.

En configuración de máquina, en red, vamos a cambiar los adaptadores:

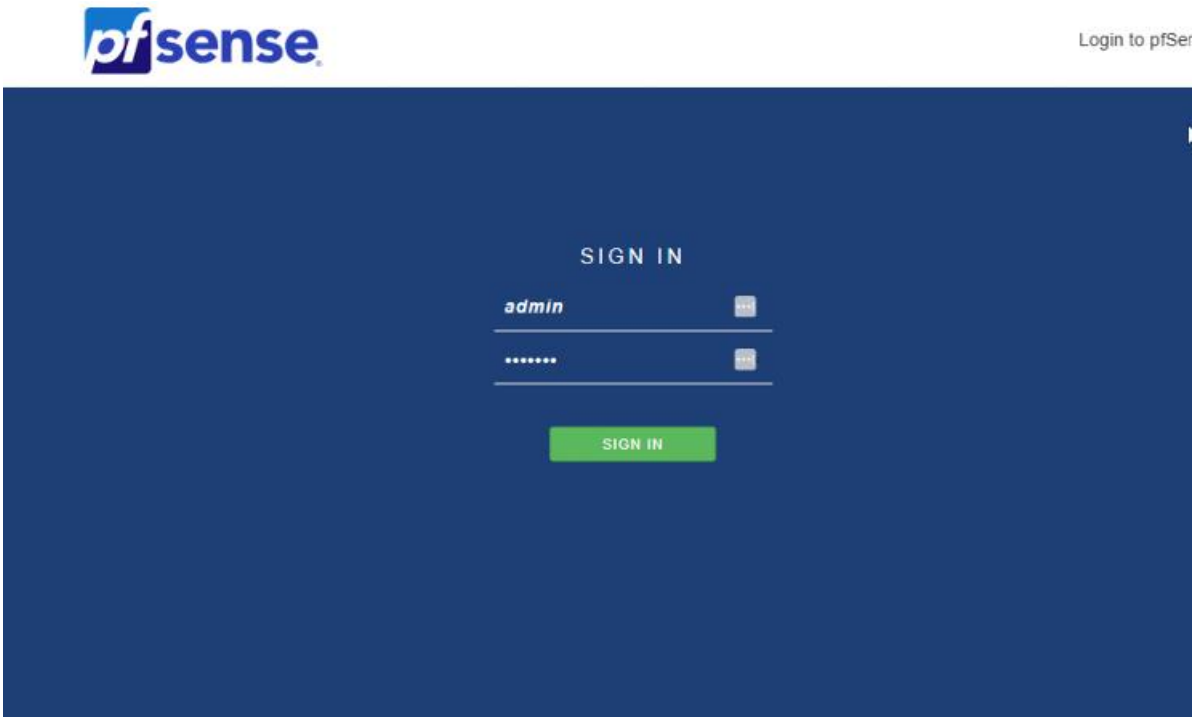
En el adaptador 1 habilitamos adaptador, lo conectamos a adaptador puente. En adaptador 2 habilitamos, red interna y ponemos LAN. En adaptador 3, habilitamos, red interna y ponemos DMZ. Finalmente en adaptador 4, habilitamos, red interna y ponemos DMZ2.



A continuación añadimos la máquina Kali para configurar Pfsense



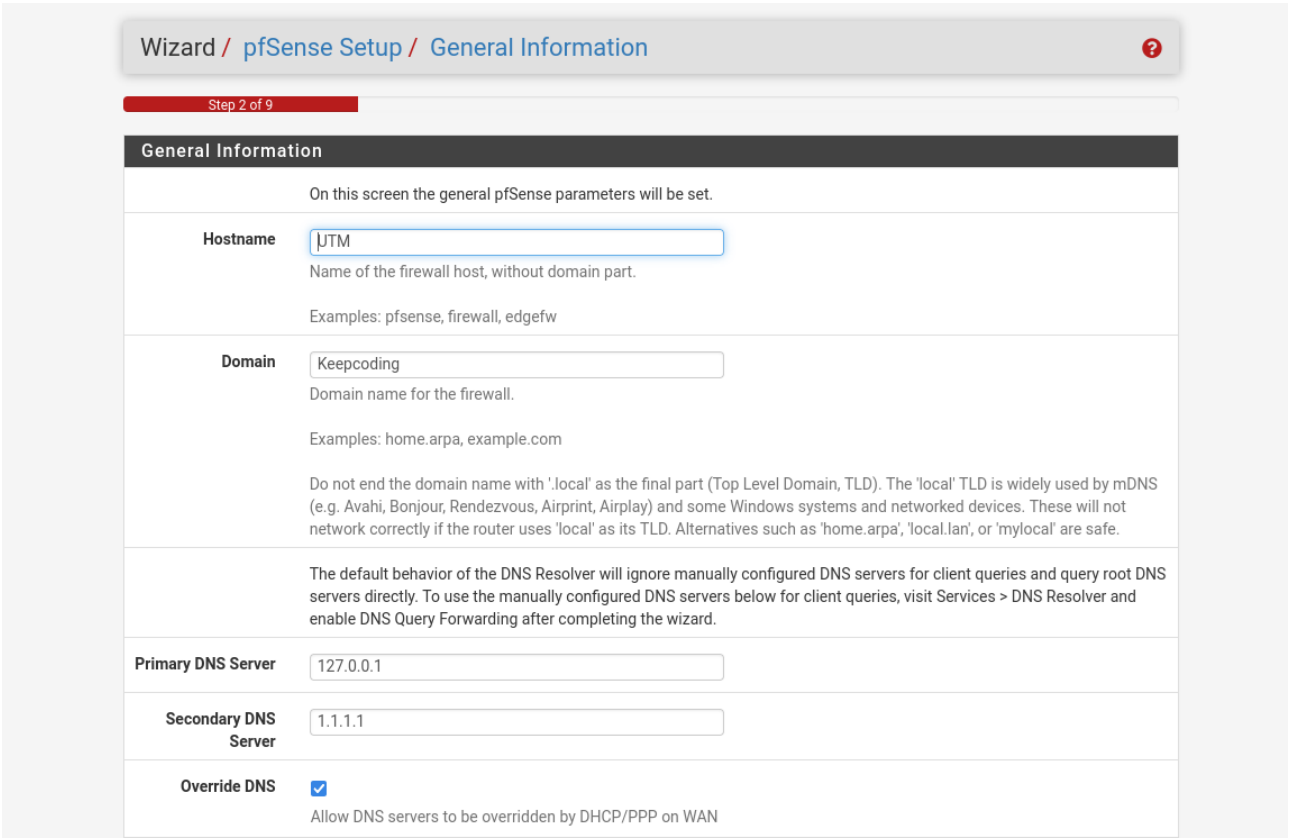
Añadimos la máquina virtual Kali previamente instalada. La red que nos proporciona nuestro router será la red WAN. A continuación configuramos la red y accedemos a Pfsense.

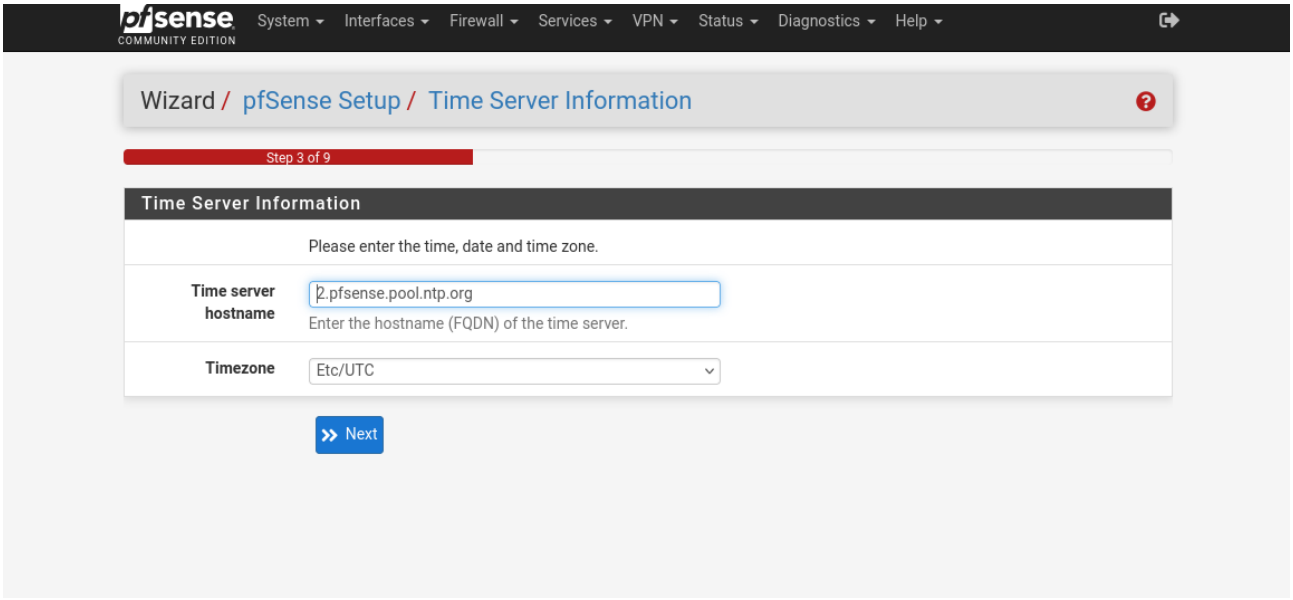


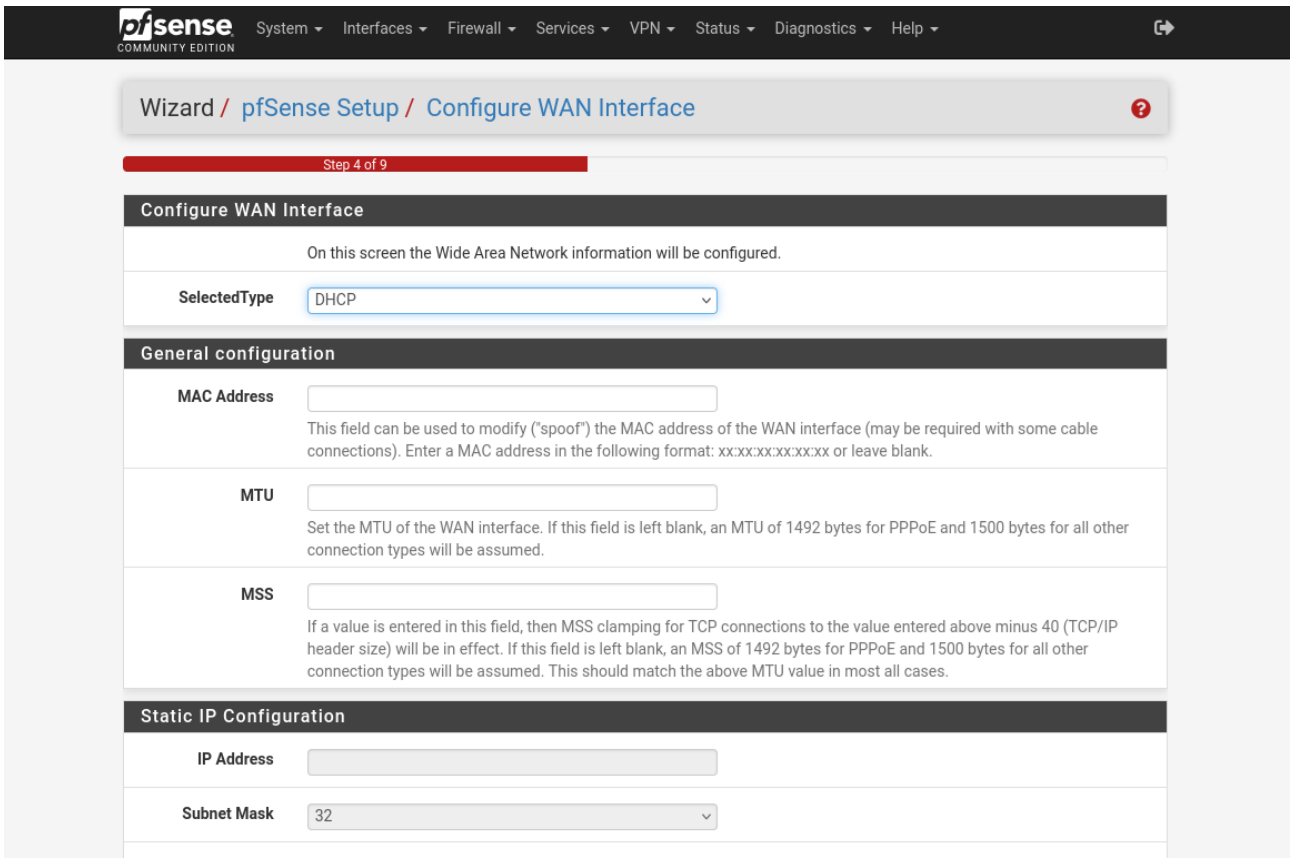
Para configurar Pfsense:

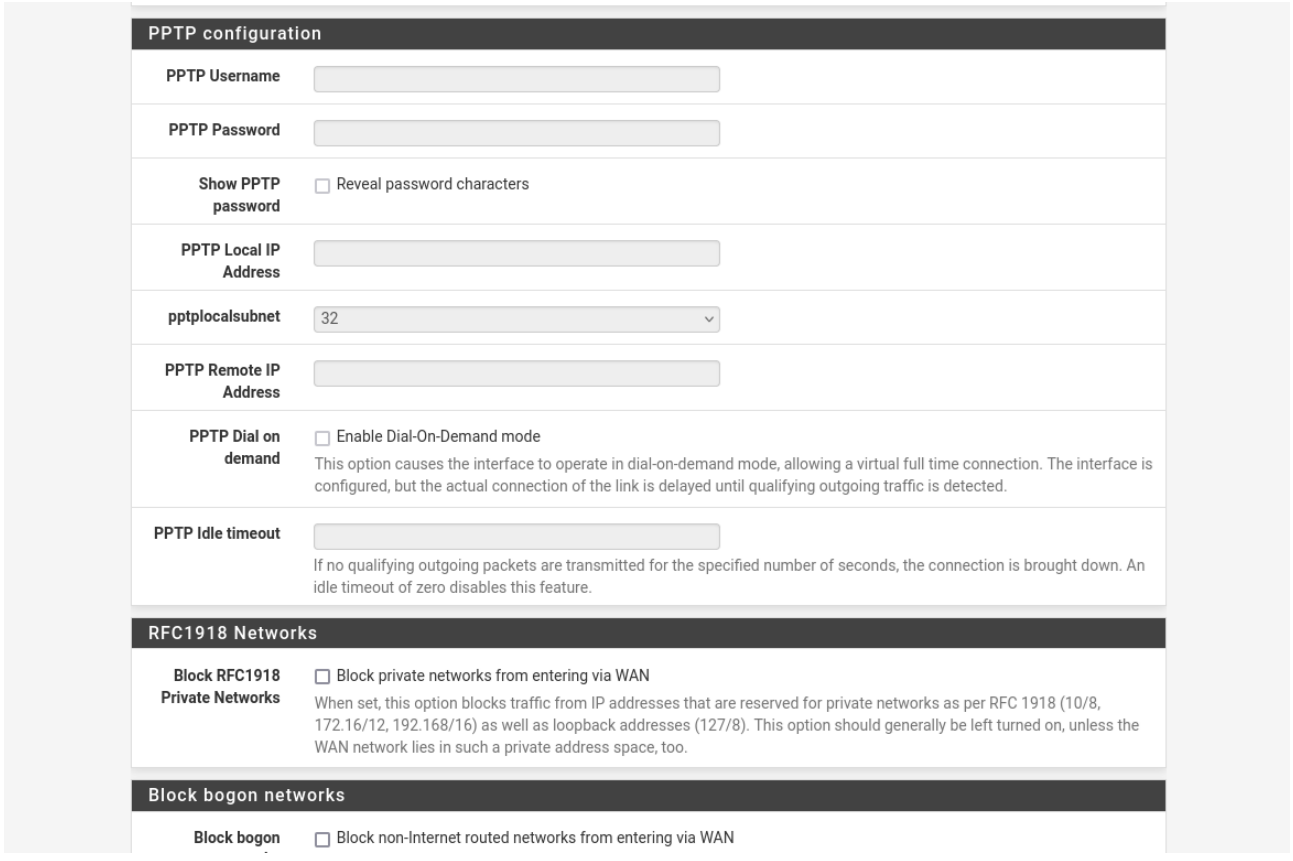
Desde el UTM : 192.168.1.1
Usuario: admin
pass: pfsense

Hostname: UTM
Domain: Keepcoding
DNS server : 127.0.0.1
DNS server: 1.1.1.1

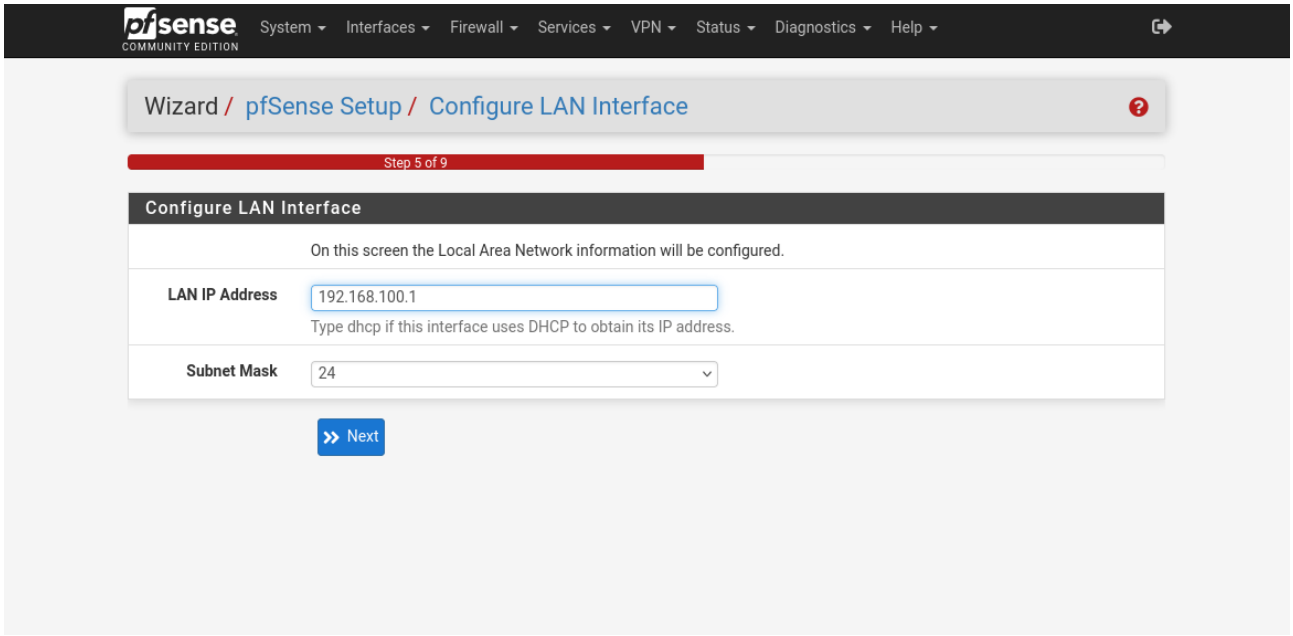

Wizard / pfSense Setup / General Information
Step 2 of 9
General Information
On this screen the general pfSense parameters will be set.
Hostname
UTM
Name of the firewall host, without domain part.
Examples: pfsense, firewall, edgefw
Domain
Keepcoding
Domain name for the firewall.
Examples: home.arpa, example.com
Do not end the domain name with '.local' as the final part (Top Level Domain, TLD). The 'local' TLD is widely used by mDNS (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses 'local' as its TLD. Alternatives such as 'home.arpa', 'local.lan', or 'mylocal' are safe.
The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard.
Primary DNS Server
127.0.0.1
Secondary DNS Server
1.1.1.1
Override DNS
Allow DNS servers to be overridden by DHCP/PPP on WAN

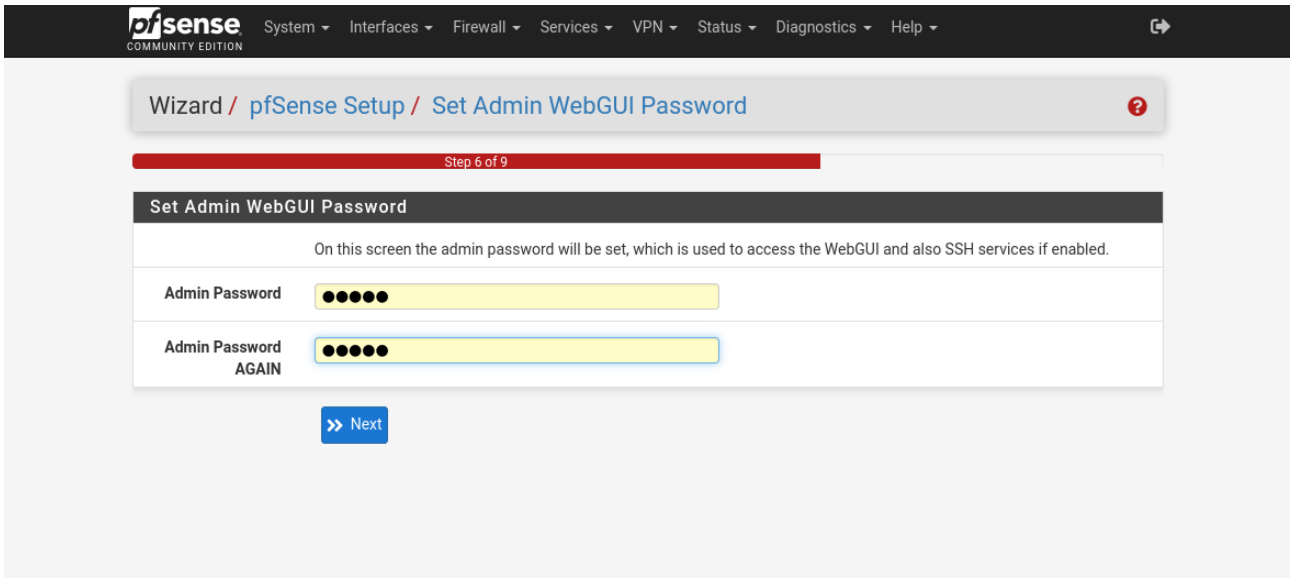

pfsense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Wizard / pfSense Setup / Time Server Information
Step 3 of 9
Time Server Information
Please enter the time, date and time zone.
Time server hostname
2.pfsense.pool.ntp.org
Enter the hostname (FQDN) of the time server.
Timezone
Etc/UTC
Next


pfsense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Wizard / pfSense Setup / Configure WAN Interface
Step 4 of 9
Configure WAN Interface
On this screen the Wide Area Network information will be configured.
SelectedType
DHCP
General configuration
MAC Address
This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with some cable connections). Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.
MTU
Set the MTU of the WAN interface. If this field is left blank, an MTU of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed.
MSS
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect. If this field is left blank, an MSS of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed. This should match the above MTU value in most all cases.
Static IP Configuration
IP Address
Subnet Mask
32


PPTP configuration
PPTP Username
PPTP Password
Show PPTP password
Reveal password characters
PPTP Local IP Address
pptplocalsubnet
32
PPTP Remote IP Address
PPTP Dial on demand
Enable Dial-On-Demand mode
This option causes the interface to operate in dial-on-demand mode, allowing a virtual full time connection. The interface is configured, but the actual connection of the link is delayed until qualifying outgoing traffic is detected.
PPTP Idle timeout
If no qualifying outgoing packets are transmitted for the specified number of seconds, the connection is brought down. An idle timeout of zero disables this feature.
RFC1918 Networks
Block RFC1918 Private Networks
Block private networks from entering via WAN
When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). This option should generally be left turned on, unless the WAN network lies in such a private address space, too.
Block bogon networks
Block bogon
Block non-Internet routed networks from entering via WAN

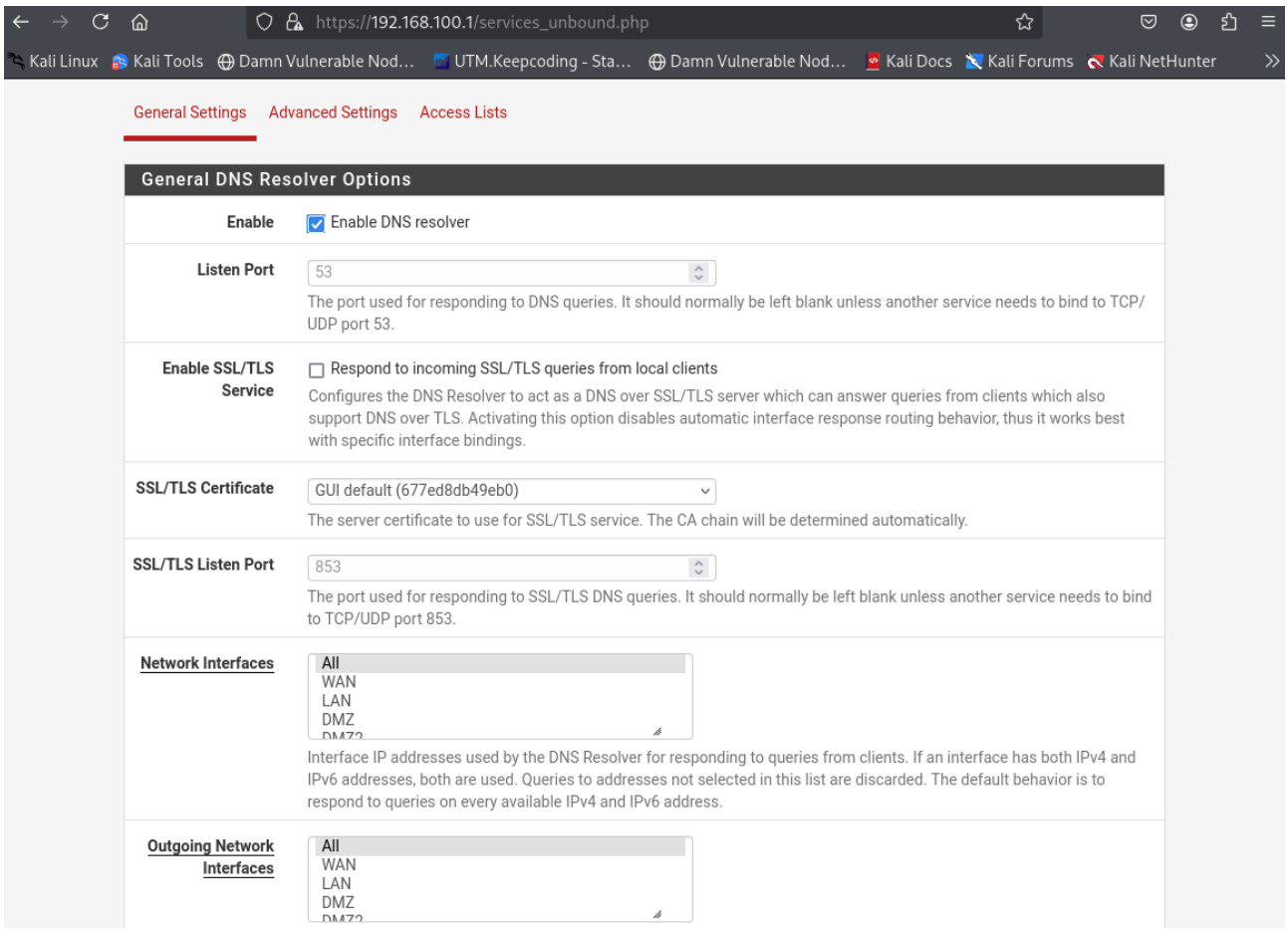
Configuramos la IP de la LAN para poder acceder correctamente, cambiamos el re-direccionamiento a la 192.168.100.1 y Subnet Mask : 24

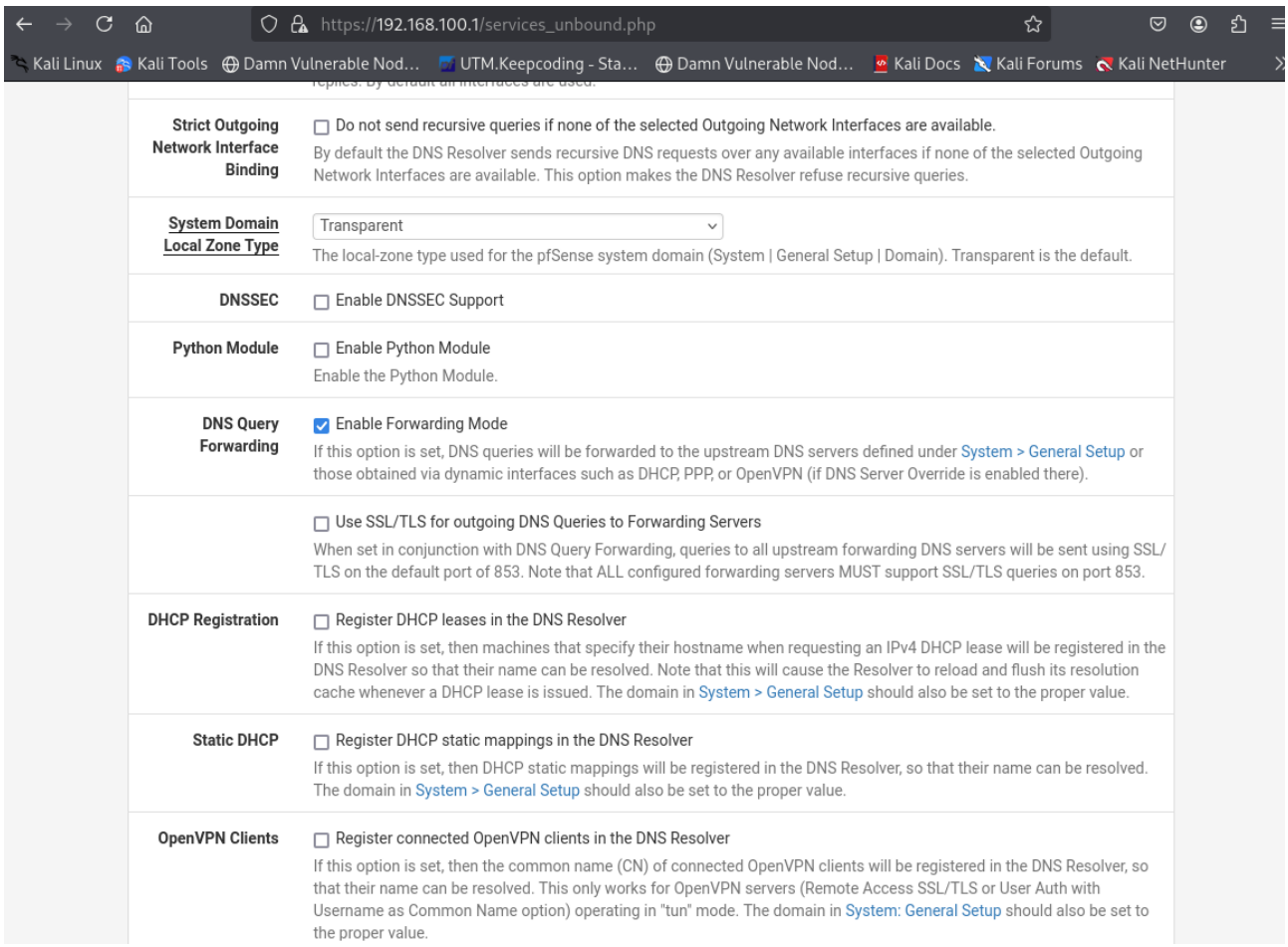


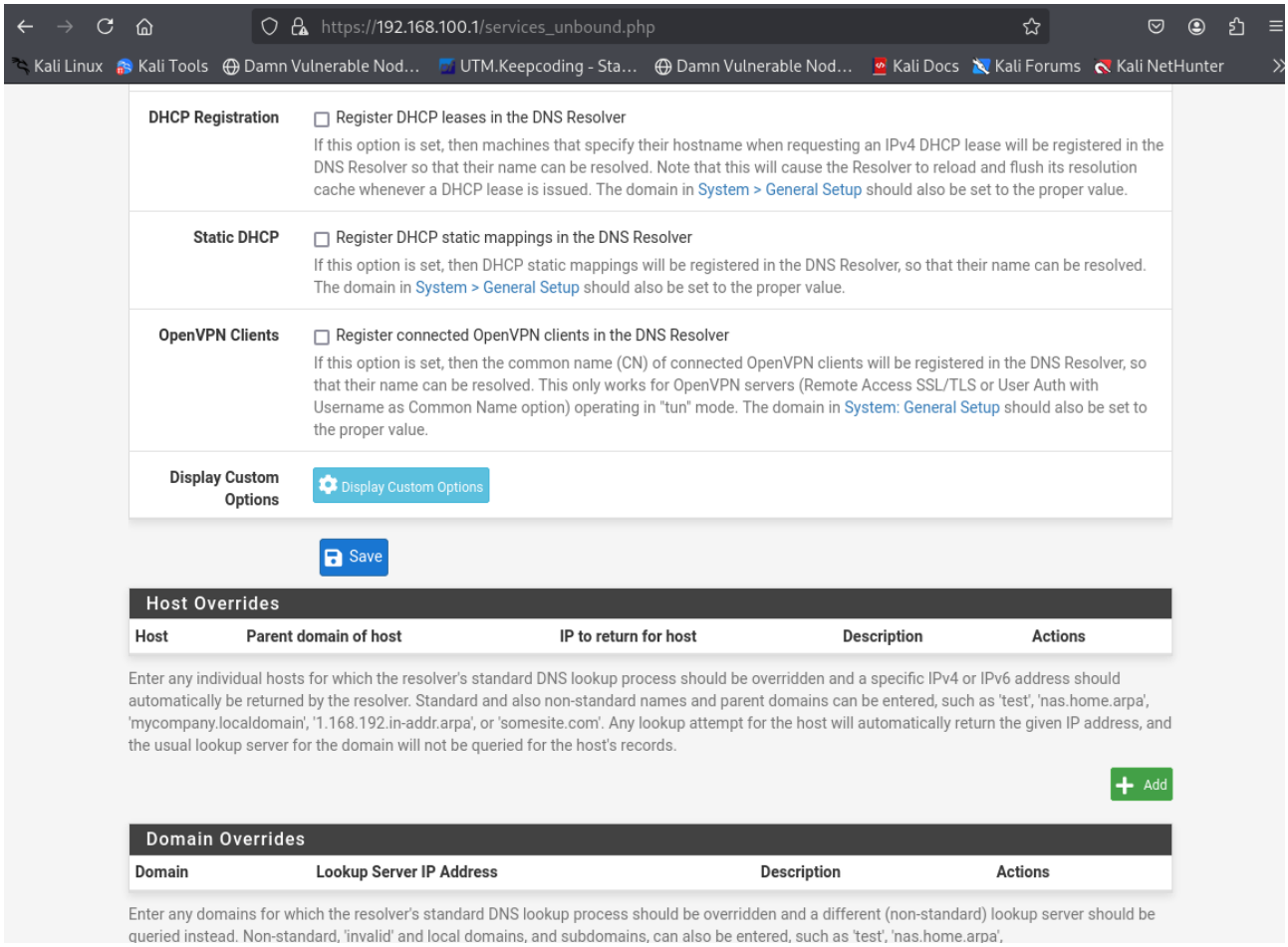


Configuramos la resolución DNS

En services – DNS resolver, comprobamos que está habilitado, quitamos DNSSEC y habilitamos forwarding mode


https://192.168.100.1/services_unbound.php
Kali Linux
Kali Tools
Damn Vulnerable Nod...
UTM.Keepcoding - Sta...
Damn Vulnerable Nod...
Kali Docs
Kali Forums
Kali NetHunter
General Settings
Advanced Settings
Access Lists
General DNS Resolver Options
Enable
Enable DNS resolver
Listen Port
53
The port used for responding to DNS queries. It should normally be left blank unless another service needs to bind to TCP/UDP port 53.
Enable SSL/TLS Service
Respond to incoming SSL/TLS queries from local clients
Configures the DNS Resolver to act as a DNS over SSL/TLS server which can answer queries from clients which also support DNS over TLS. Activating this option disables automatic interface response routing behavior, thus it works best with specific interface bindings.
SSL/TLS Certificate
GUI default (677ed8db49eb0)
The server certificate to use for SSL/TLS service. The CA chain will be determined automatically.
SSL/TLS Listen Port
853
The port used for responding to SSL/TLS DNS queries. It should normally be left blank unless another service needs to bind to TCP/UDP port 853.
Network Interfaces
All
WAN
LAN
DMZ
Interface IP addresses used by the DNS Resolver for responding to queries from clients. If an interface has both IPv4 and IPv6 addresses, both are used. Queries to addresses not selected in this list are discarded. The default behavior is to respond to queries on every available IPv4 and IPv6 address.
Outgoing Network Interfaces
All
WAN
LAN
DMZ

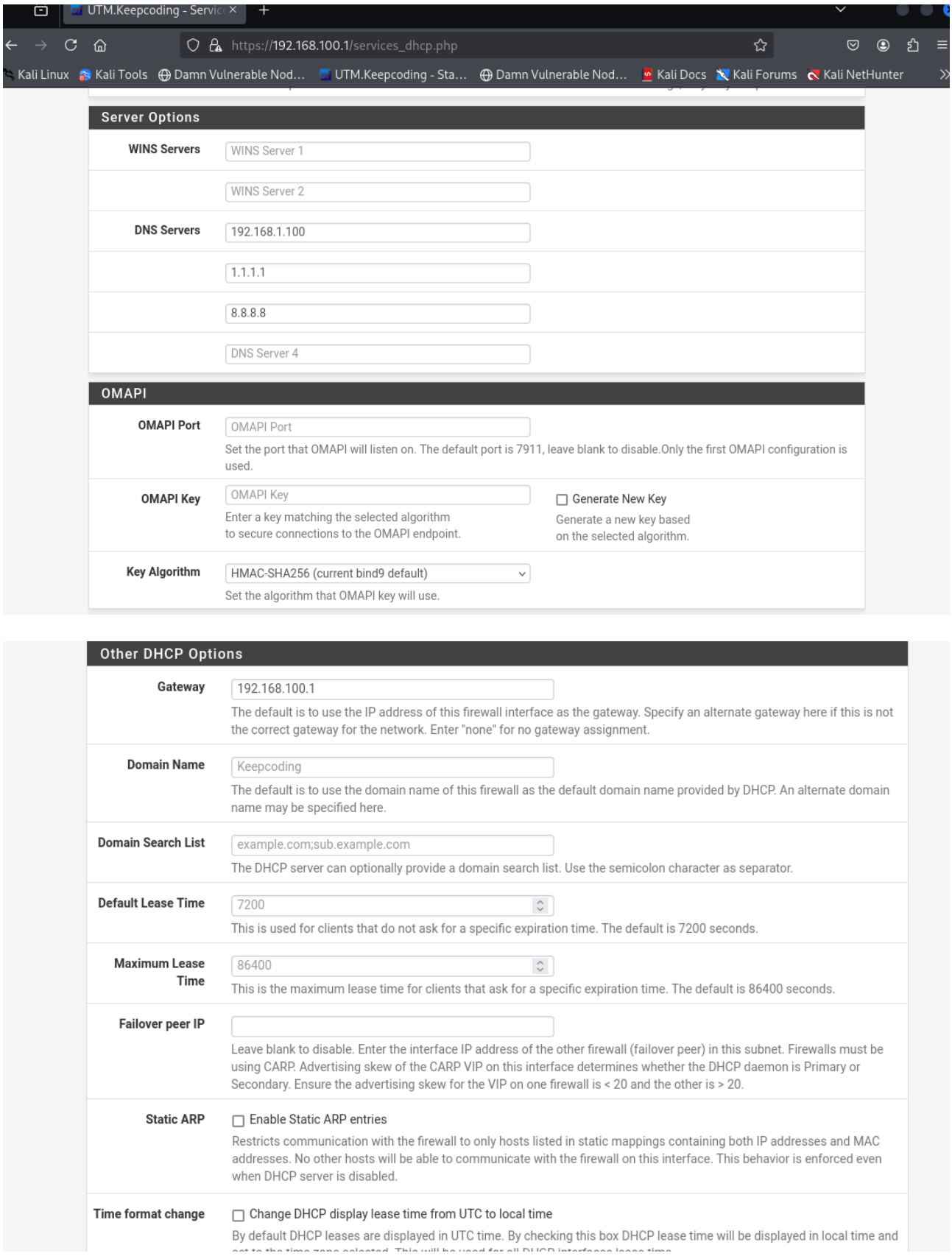

https://192.168.100.1/services_unbound.php
Kali Linux
Kali Tools
Damn Vulnerable Nod...
UTM.Keepcoding - Sta...
Damn Vulnerable Nod...
Kali Docs
Kali Forums
Kali NetHunter
Strict Outgoing Network Interface Binding
Do not send recursive queries if none of the selected Outgoing Network Interfaces are available.
By default the DNS Resolver sends recursive DNS requests over any available interfaces if none of the selected Outgoing Network Interfaces are available. This option makes the DNS Resolver refuse recursive queries.
System Domain Local Zone Type
Transparent
The local-zone type used for the pfSense system domain (System | General Setup | Domain). Transparent is the default.
DNSSEC
Enable DNSSEC Support
Python Module
Enable Python Module
Enable the Python Module.
DNS Query Forwarding
Enable Forwarding Mode
If this option is set, DNS queries will be forwarded to the upstream DNS servers defined under System > General Setup or those obtained via dynamic interfaces such as DHCP, PPP, or OpenVPN (if DNS Server Override is enabled there).
Use SSL/TLS for outgoing DNS Queries to Forwarding Servers
When set in conjunction with DNS Query Forwarding, queries to all upstream forwarding DNS servers will be sent using SSL/TLS on the default port of 853. Note that ALL configured forwarding servers MUST support SSL/TLS queries on port 853.
DHCP Registration
Register DHCP leases in the DNS Resolver
If this option is set, then machines that specify their hostname when requesting an IPv4 DHCP lease will be registered in the DNS Resolver so that their name can be resolved. Note that this will cause the Resolver to reload and flush its resolution cache whenever a DHCP lease is issued. The domain in System > General Setup should also be set to the proper value.
Static DHCP
Register DHCP static mappings in the DNS Resolver
If this option is set, then DHCP static mappings will be registered in the DNS Resolver, so that their name can be resolved. The domain in System > General Setup should also be set to the proper value.
OpenVPN Clients
Register connected OpenVPN clients in the DNS Resolver
If this option is set, then the common name (CN) of connected OpenVPN clients will be registered in the DNS Resolver, so that their name can be resolved. This only works for OpenVPN servers (Remote Access SSL/TLS or User Auth with Username as Common Name option) operating in "tun" mode. The domain in System: General Setup should also be set to the proper value.



El siguiente paso, vamos services, DHCP server. En este punto vamos a modificar los rangos dinámicos de la 192.168.100.100 a la 192.168.100.200

En el DNS server vamos a poner la dirección de nuestra WAN que es el 192.168.1.100 y en los secundarios ponemos el 1.1.1.1 y el 8.8.8.8

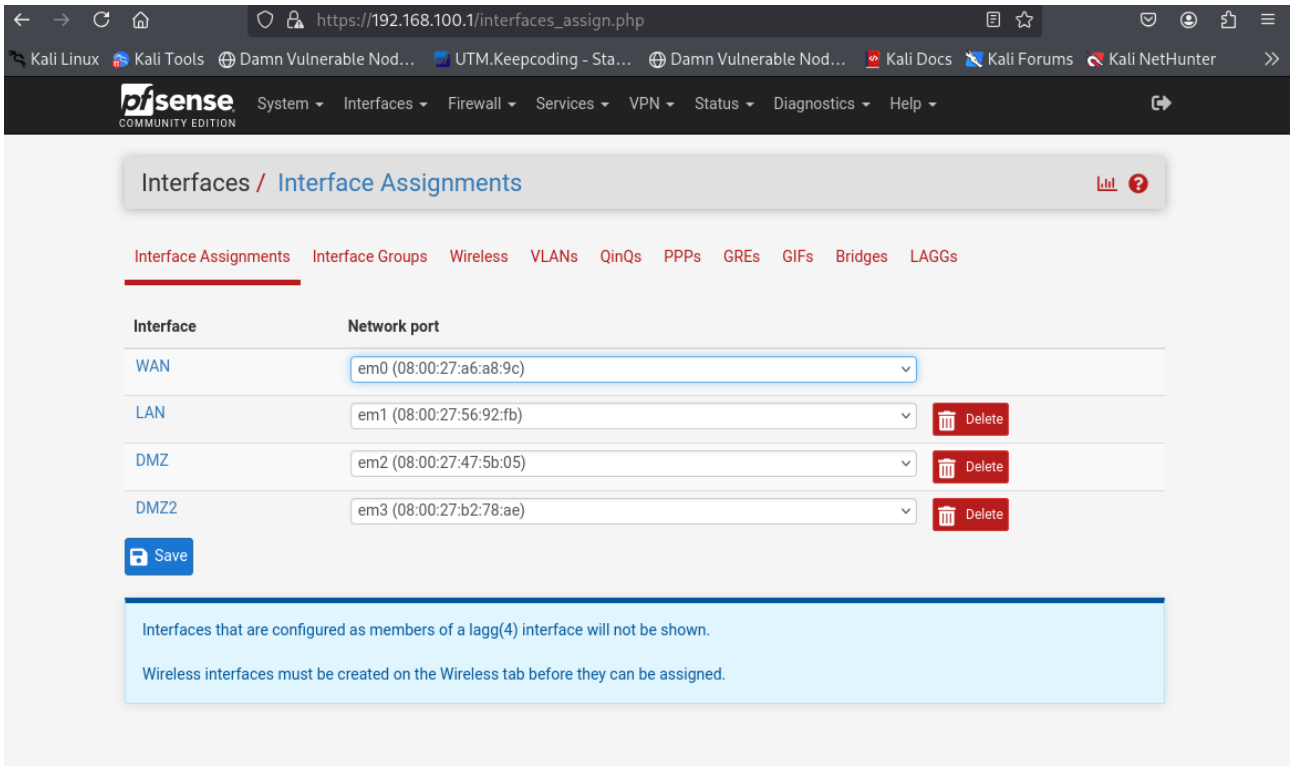
En Gateway ponemos 192.168.100.1


UTM.Keepcoding - Servic
https://192.168.100.1/services_dhcp.php
Kali Linux
Kali Tools
Damn Vulnerable Nod...
UTM.Keepcoding - Sta...
Damn Vulnerable Nod...
Kali Docs
Kali Forums
Kali NetHunter
Server Options
WINS Servers
WINS Server 1
WINS Server 2
DNS Servers
192.168.1.100
1.1.1.1
8.8.8.8
DNS Server 4
OMAPI
OMAPI Port
OMAPI Port
Set the port that OMAPI will listen on. The default port is 7911, leave blank to disable.Only the first OMAPI configuration is used.
OMAPI Key
OMAPI Key
Enter a key matching the selected algorithm to secure connections to the OMAPI endpoint.
Generate New Key
Generate a new key based on the selected algorithm.
Key Algorithm
HMAC-SHA256 (current bind9 default)
Set the algorithm that OMAPI key will use.
Other DHCP Options
Gateway
192.168.100.1
The default is to use the IP address of this firewall interface as the gateway. Specify an alternate gateway here if this is not the correct gateway for the network. Enter "none" for no gateway assignment.
Domain Name
Keepcoding
The default is to use the domain name of this firewall as the default domain name provided by DHCP. An alternate domain name may be specified here.
Domain Search List
example.com;sub.example.com
The DHCP server can optionally provide a domain search list. Use the semicolon character as separator.
Default Lease Time
7200
This is used for clients that do not ask for a specific expiration time. The default is 7200 seconds.
Maximum Lease Time
86400
This is the maximum lease time for clients that ask for a specific expiration time. The default is 86400 seconds.
Failover peer IP
Leave blank to disable. Enter the interface IP address of the other firewall (failover peer) in this subnet. Firewalls must be using CARP. Advertising skew of the CARP VIP on this interface determines whether the DHCP daemon is Primary or Secondary. Ensure the advertising skew for the VIP on one firewall is < 20 and the other is > 20.
Static ARP
Enable Static ARP entries
Restricts communication with the firewall to only hosts listed in static mappings containing both IP addresses and MAC addresses. No other hosts will be able to communicate with the firewall on this interface. This behavior is enforced even when DHCP server is disabled.
Time format change
Change DHCP display lease time from UTC to local time
By default DHCP leases are displayed in UTC time. By checking this box DHCP lease time will be displayed in local time and

2. Configuración de redes

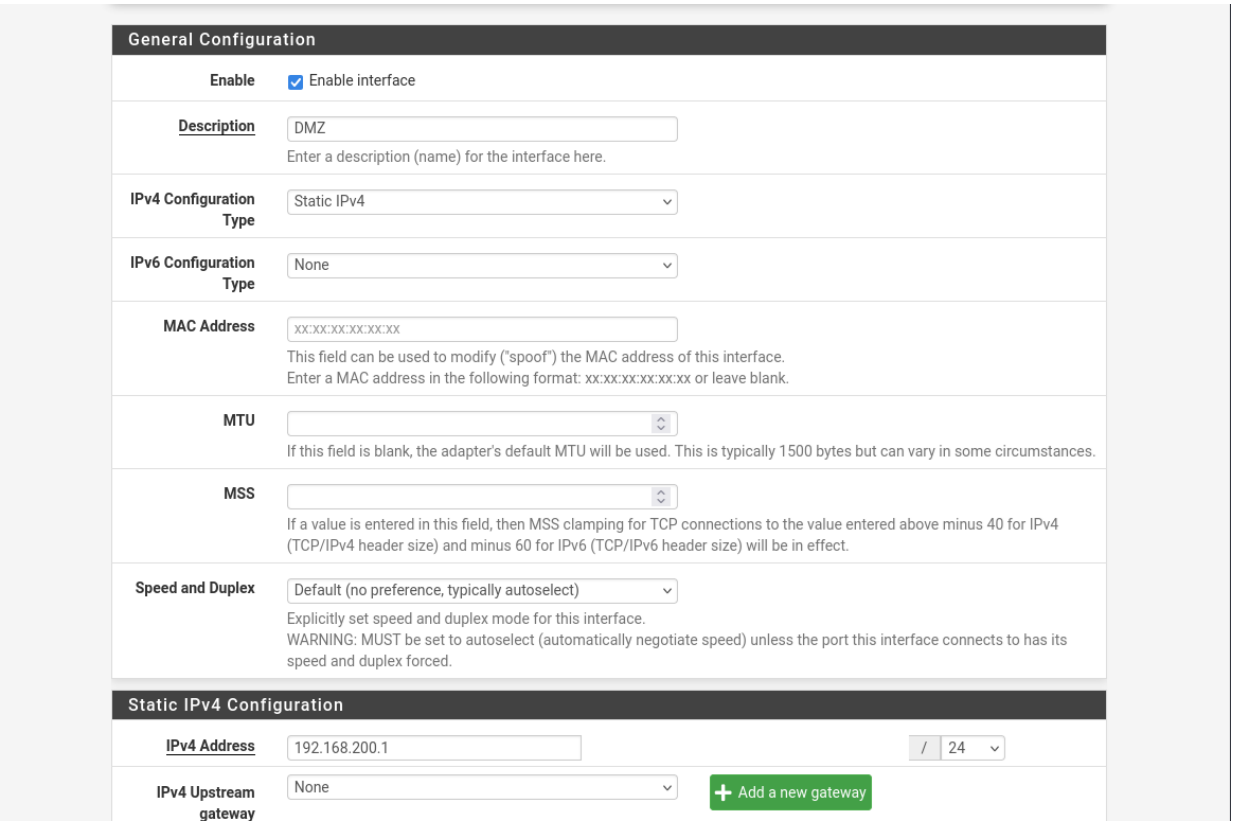
Ahora nos vamos a las Interfaces, vamos a asignarle una IP a la puerta de enlace, añadiendo una IP estática 192.168.200.1 / 24 en la DMZ y en la DMZ2 192.168.250.1 / 24

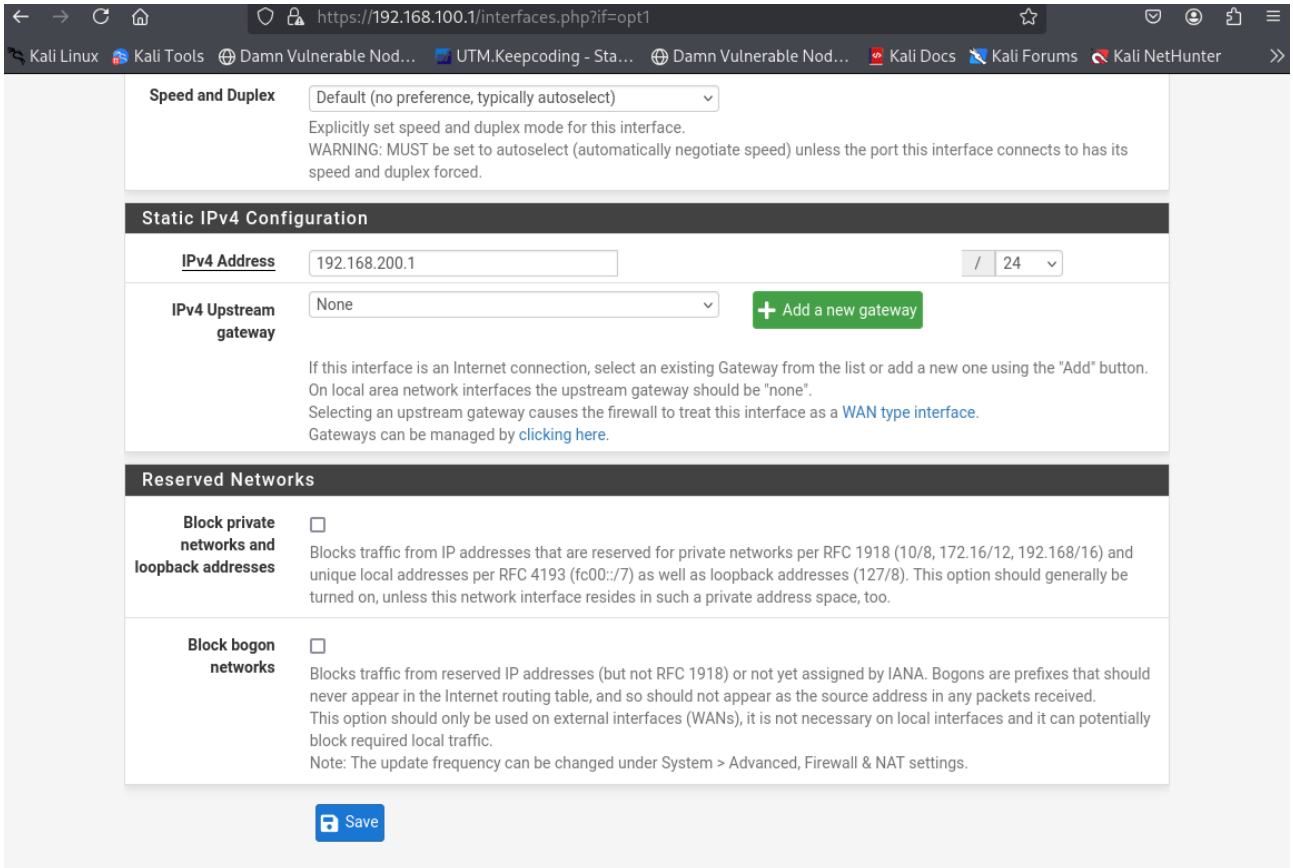
Interfaces Assignments para configurar WAN, LAN, DMZ and DMZ2



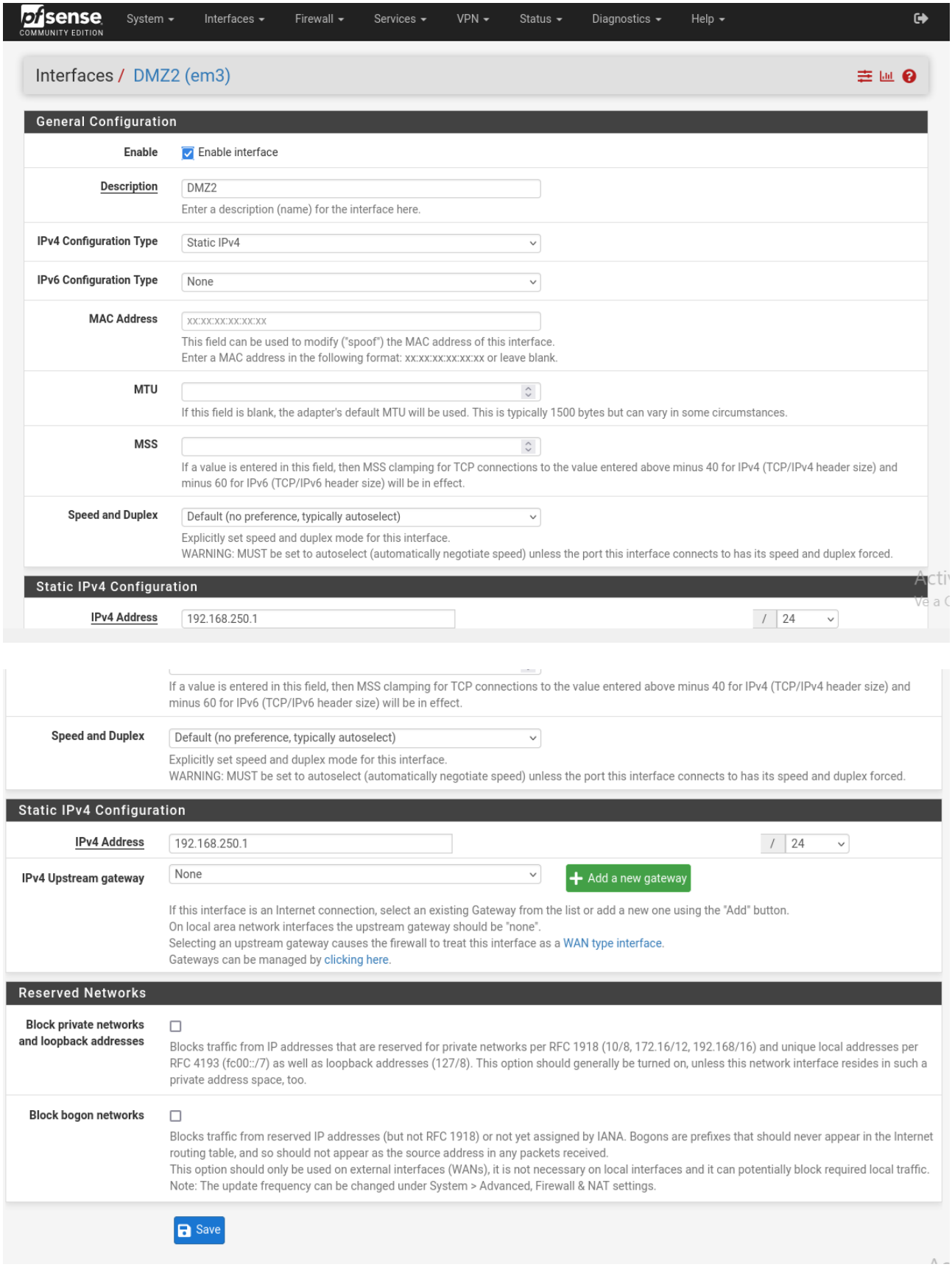
Configuración DMZ
Static IPv4
IPv4 adress 192.168.200.1

Establecimiento de la interfaz em2 como DMZ y asignación de un IPv4 estático

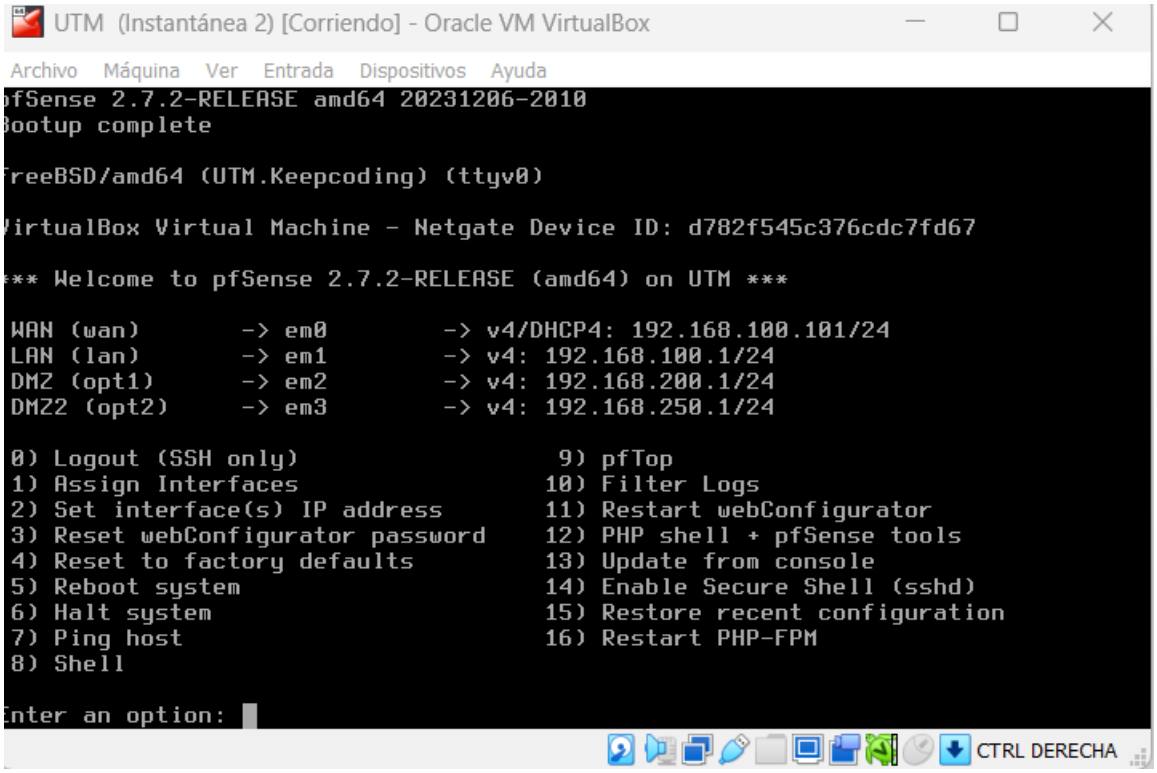




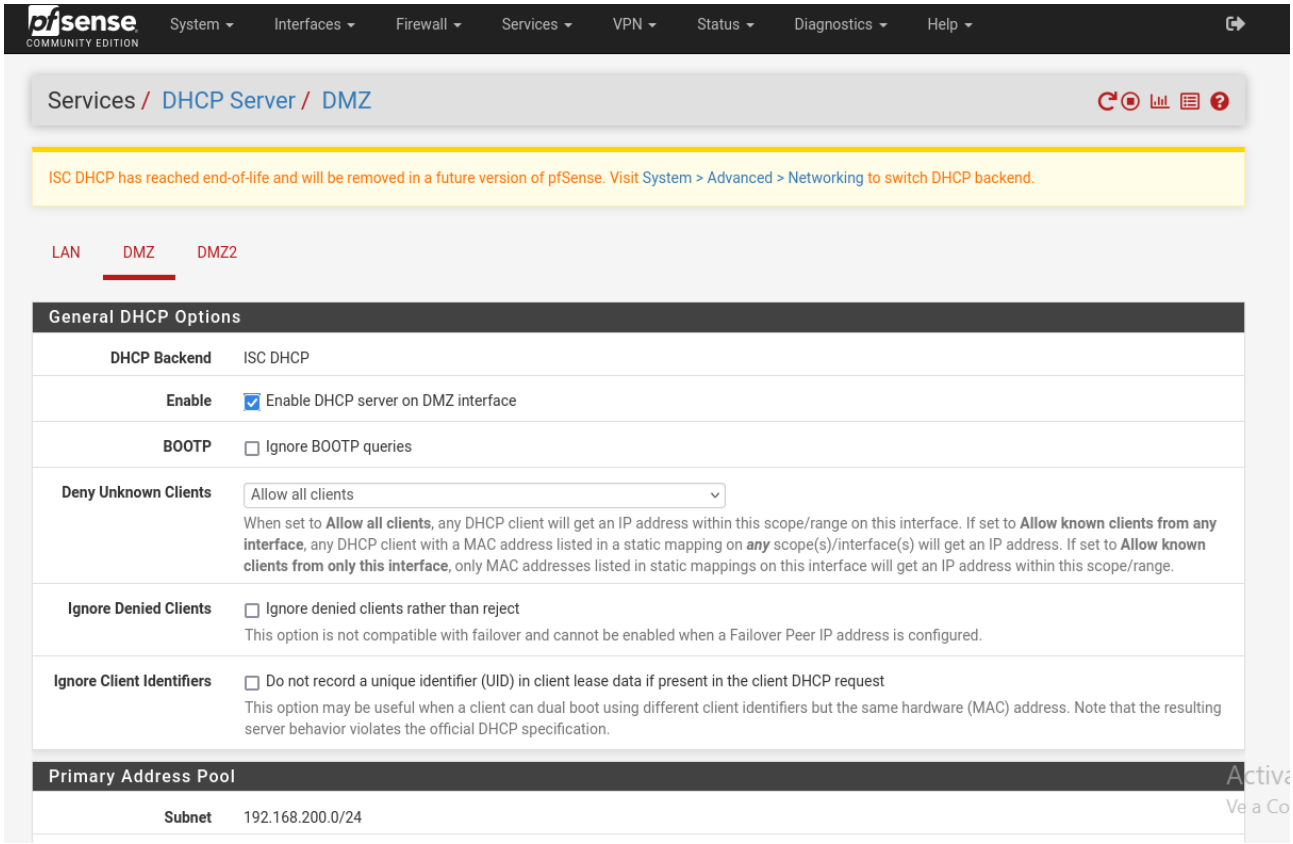
Establecimiento de la interfaz em3 como DMZ2 y asignación de un IPv4 estático

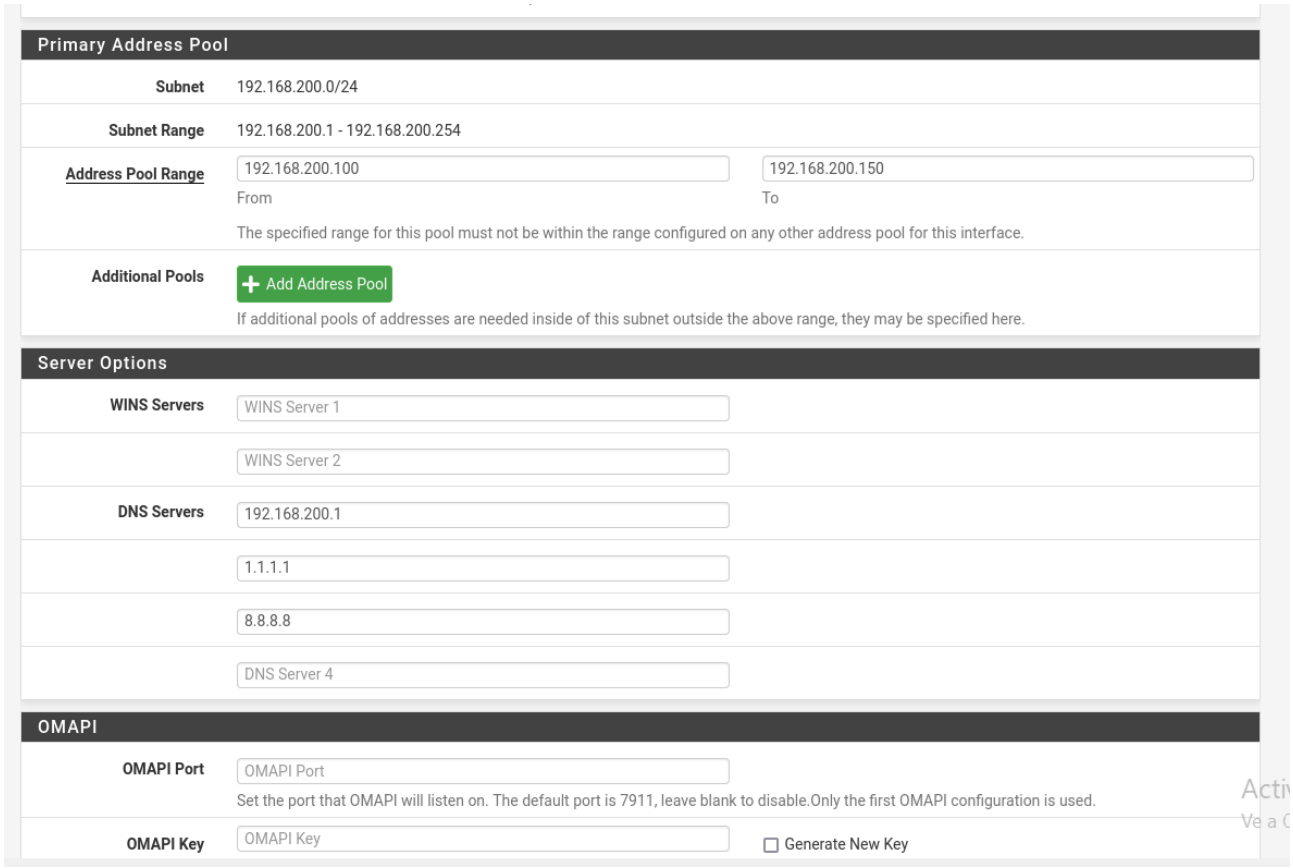


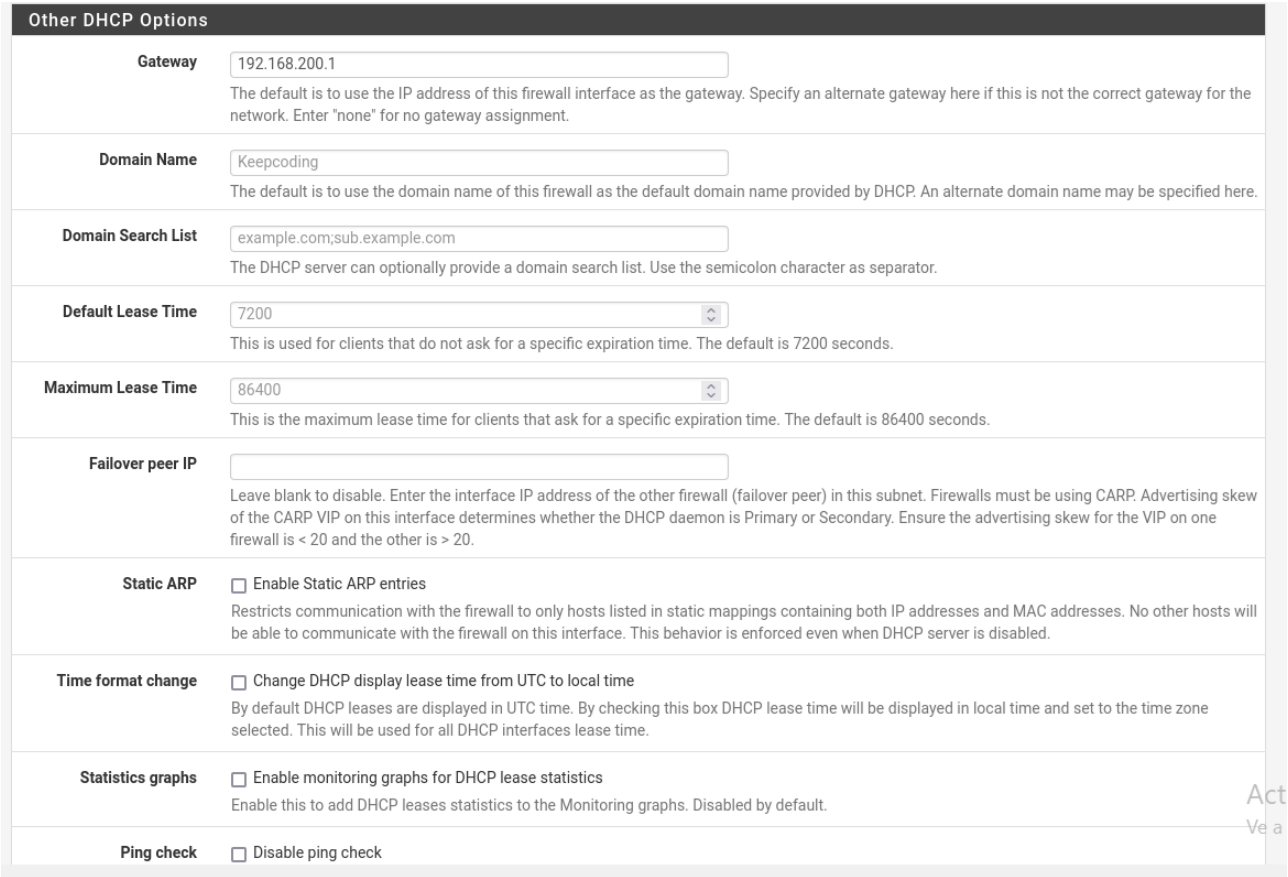
Configuración de las IP de WAN, LAN, DMZ and DMZ2



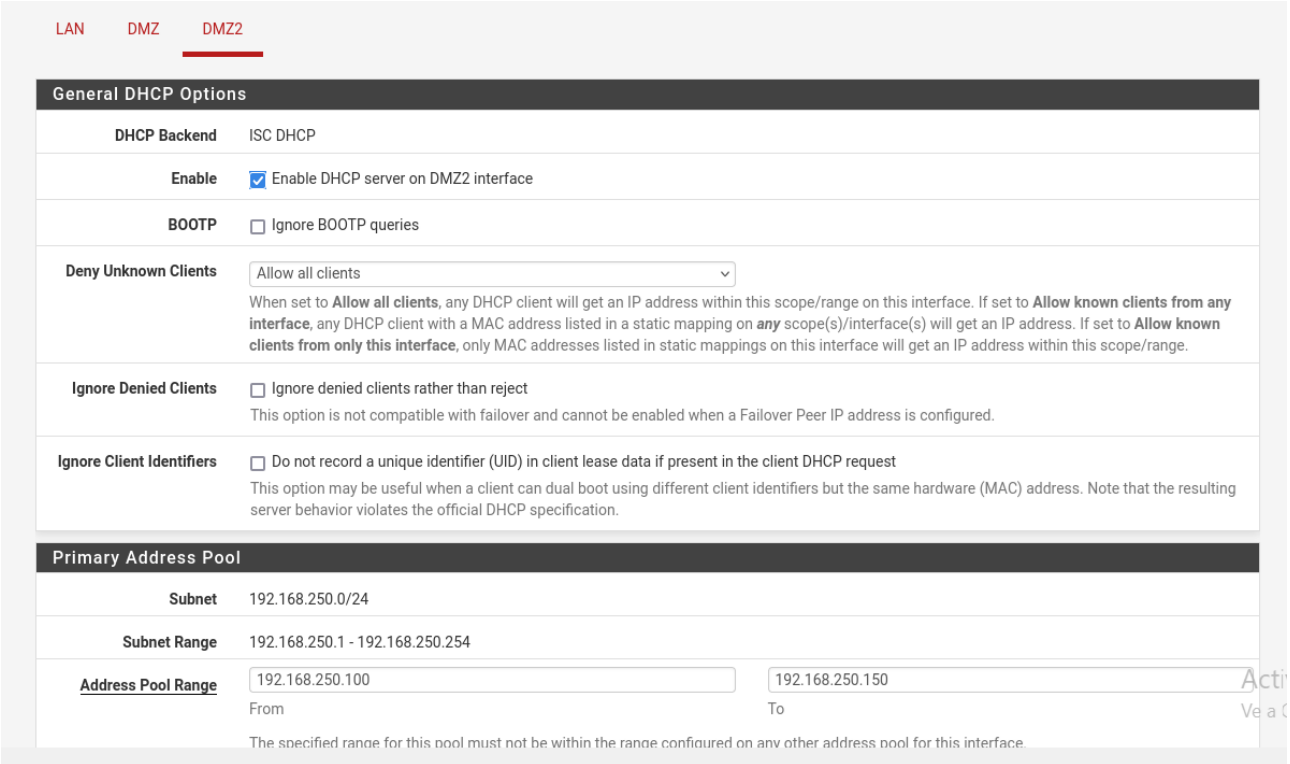
Configuración del servidor DHCP en DMZ, asignación de un rango IP específico y los servidores DNS

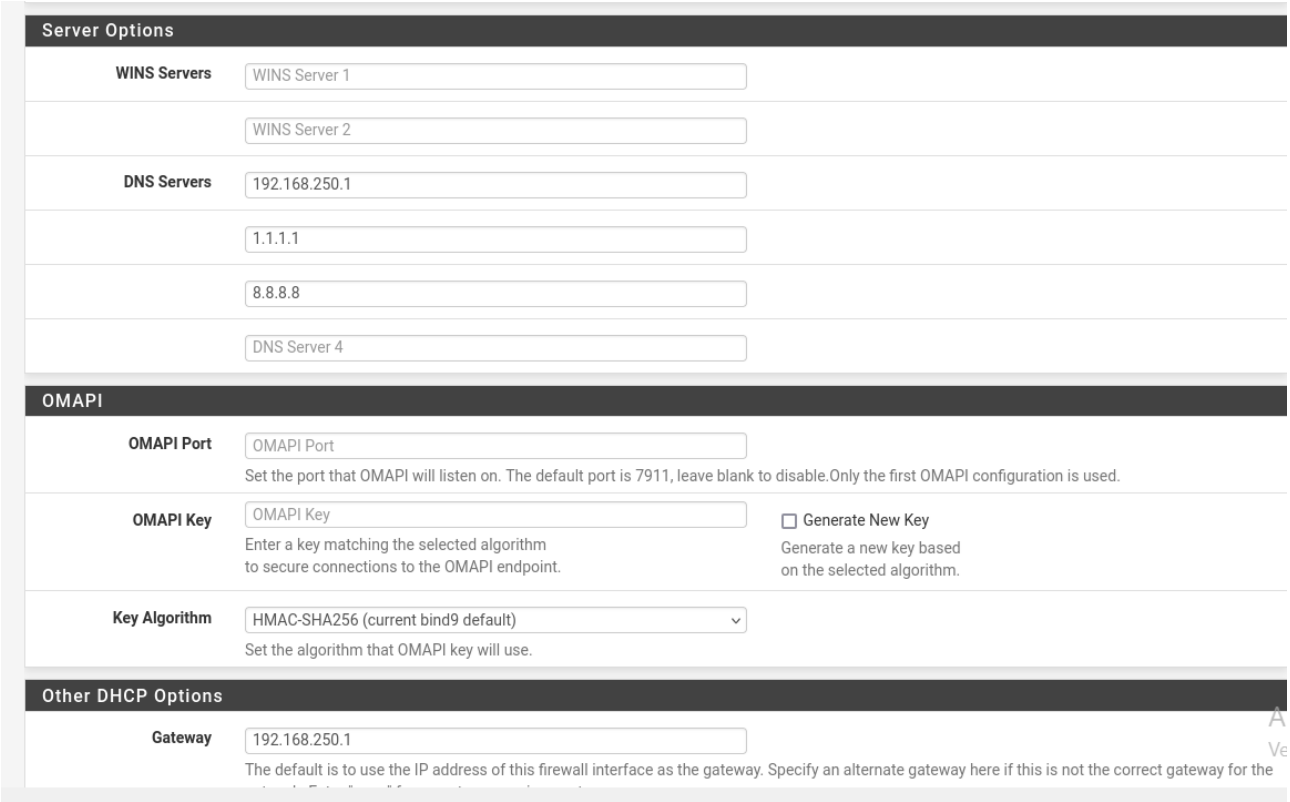




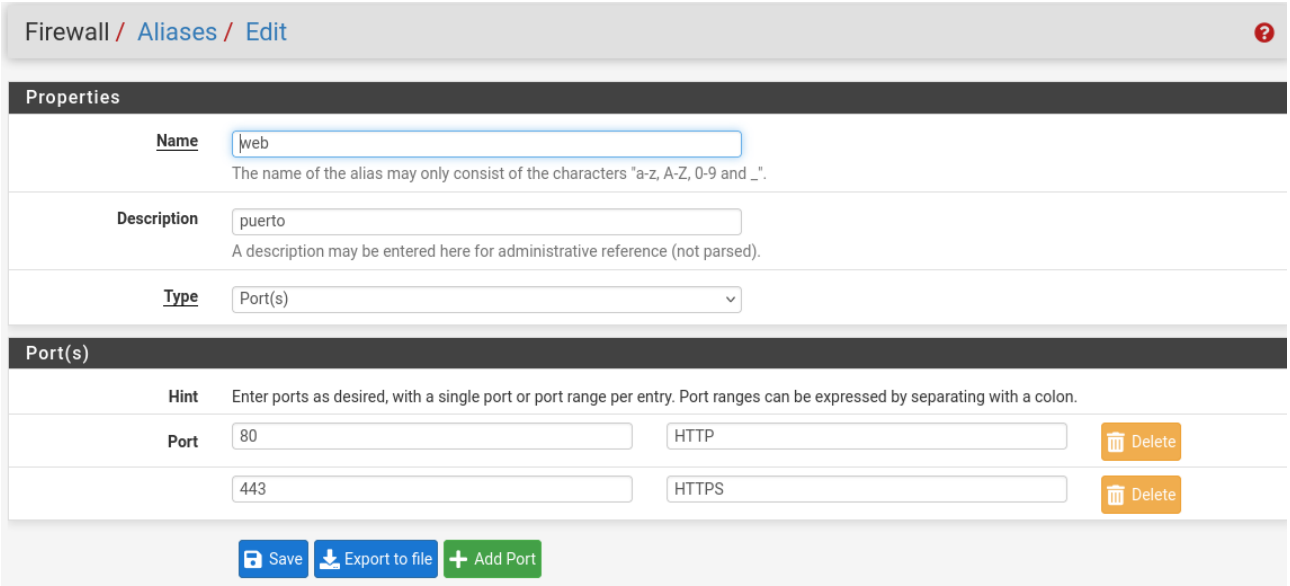


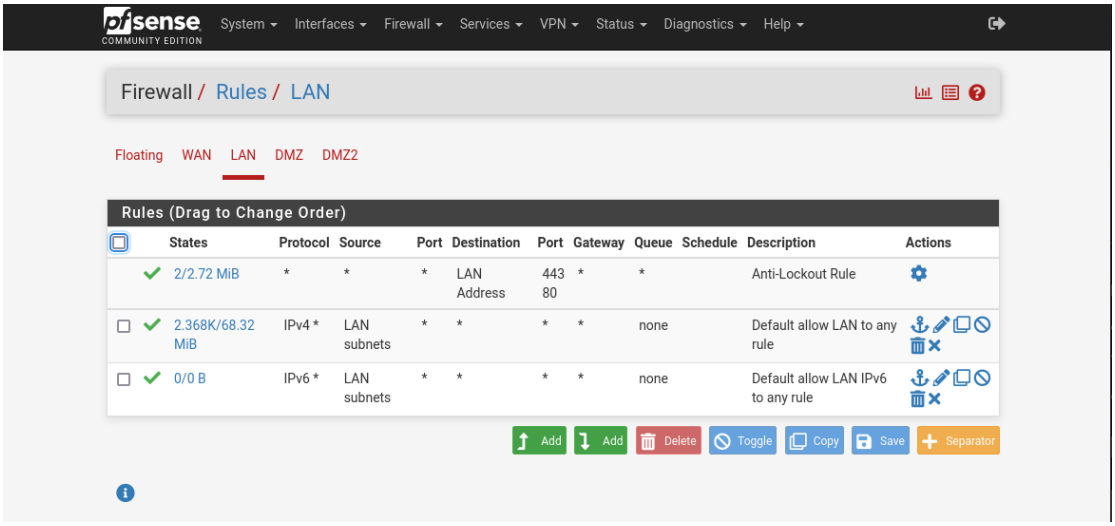
Configuracion del DHCP server en DMZ2, asignacion de un rango de IP y el DNS server





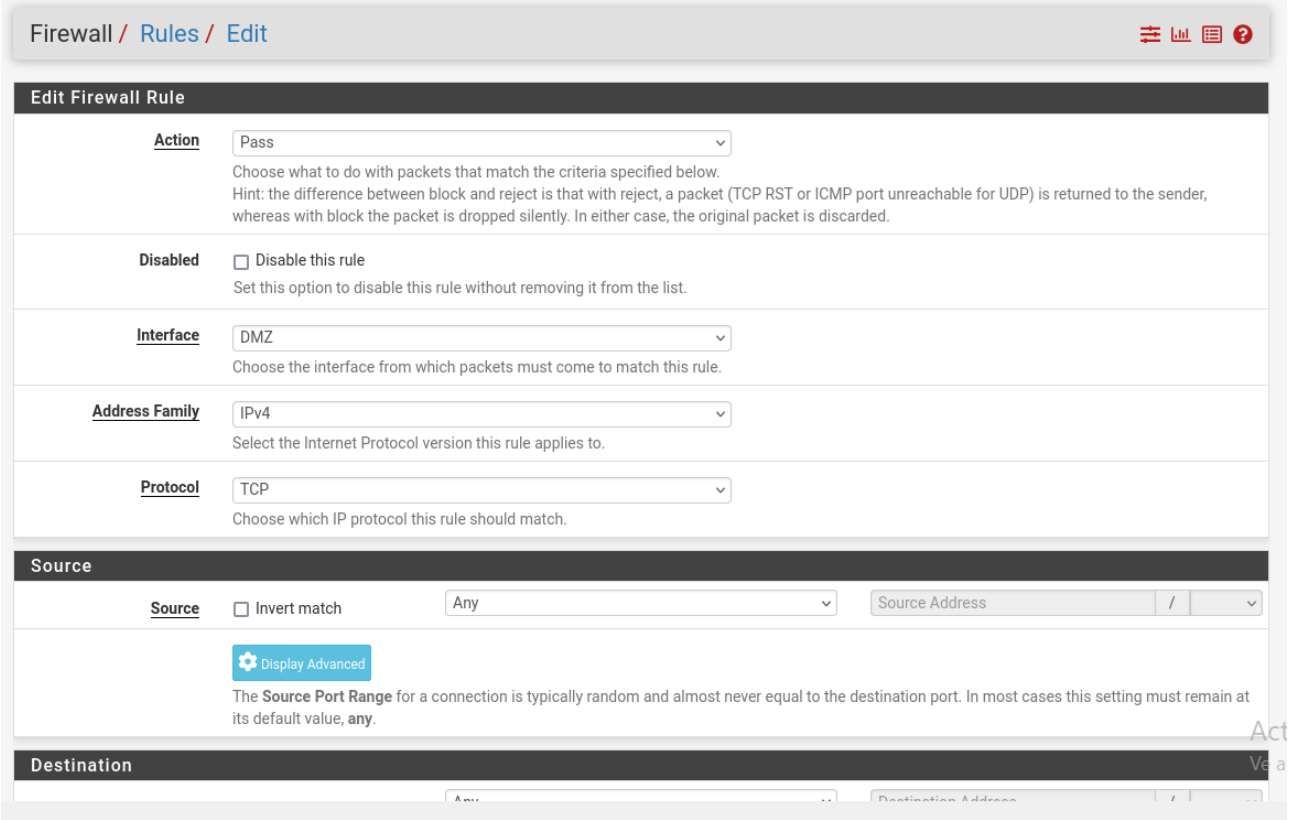
Vamos a configurar el firewall añadiendo los puertos 80 HTTP y 443 HTTPS

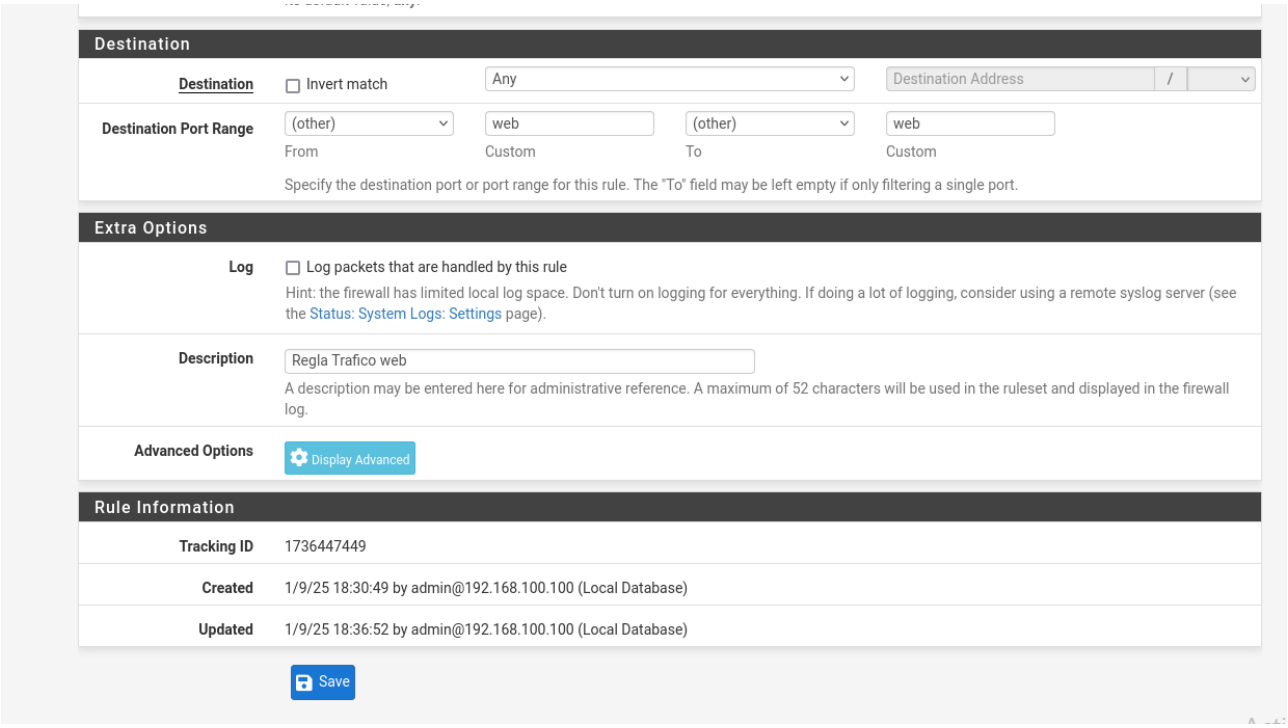




Vamos a establecer las reglas DMZ respecto al tráfico web en el firewall con la regla recién creada

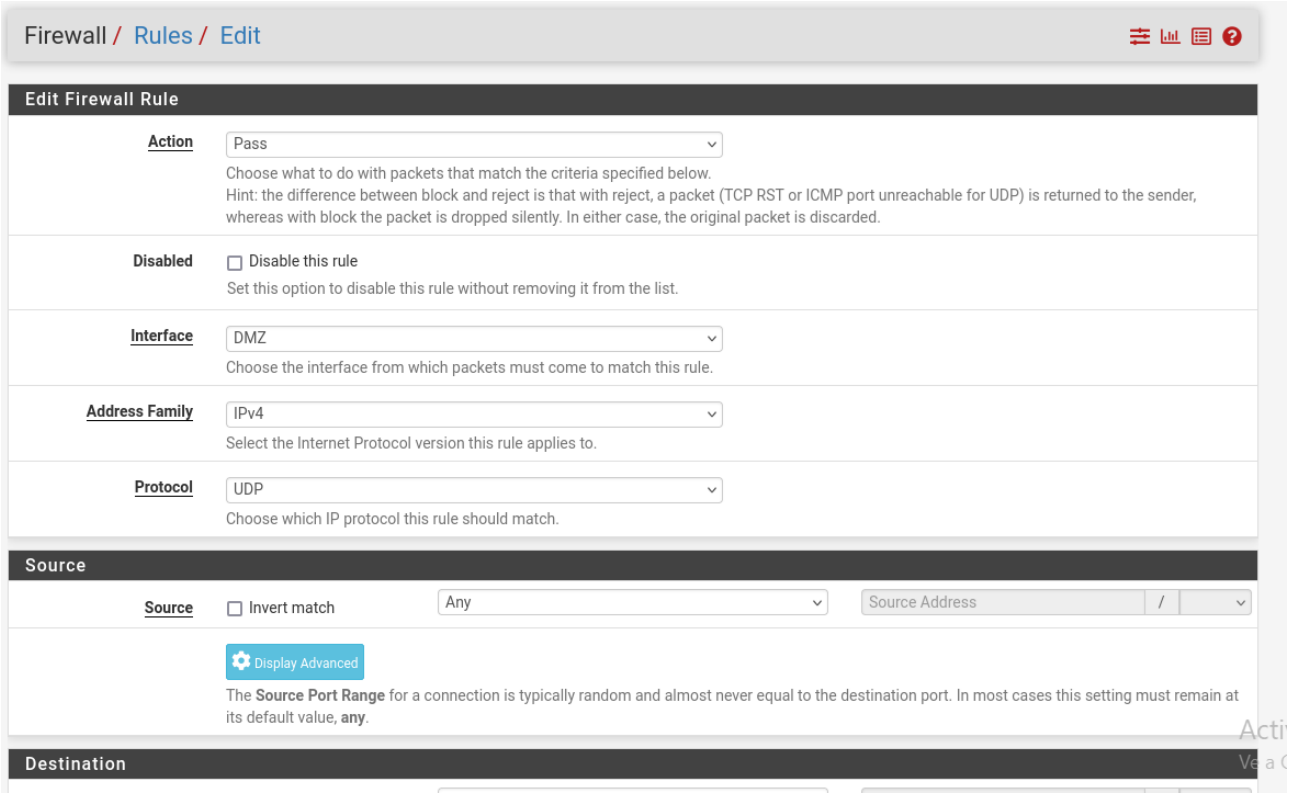
Regla del tráfico web

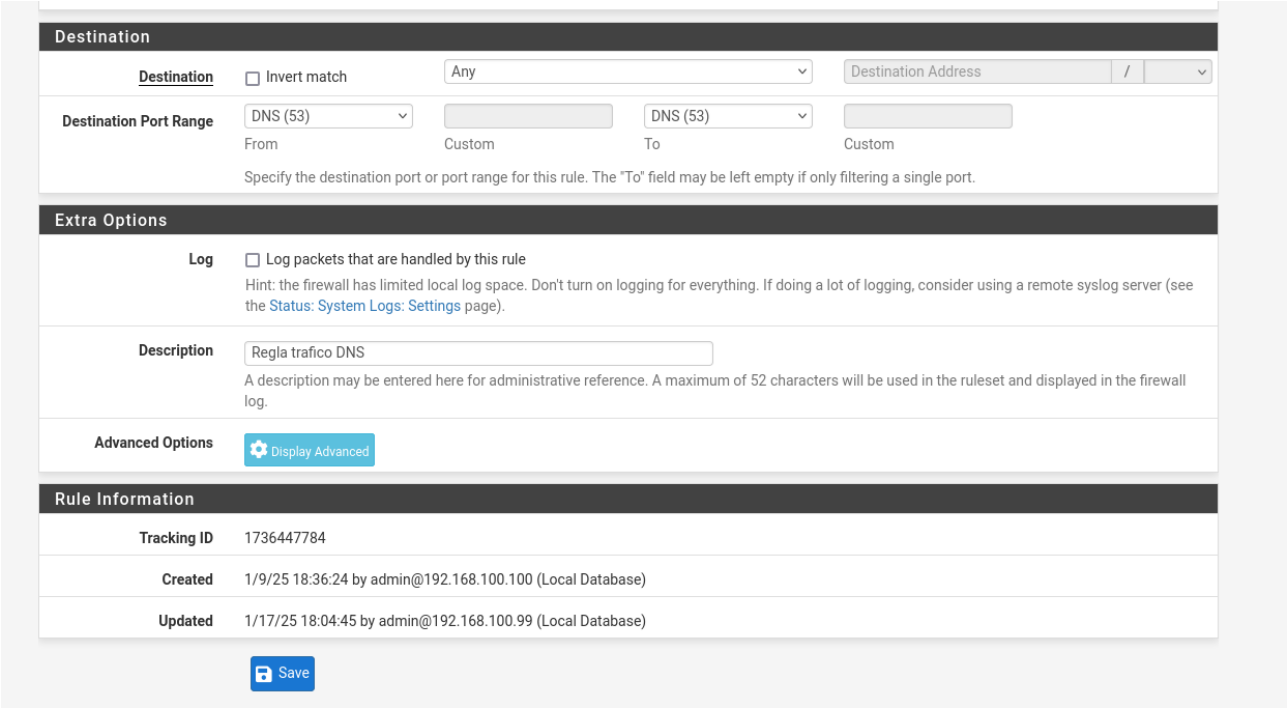




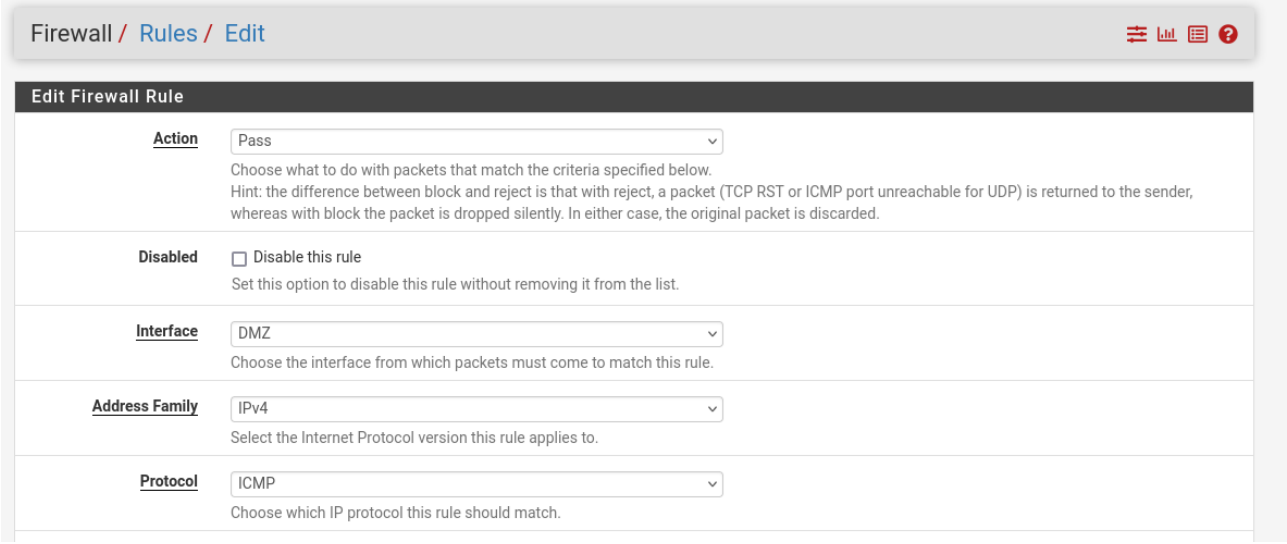
Establecimiento del DMZ Rules acerca del DNS en el firewall

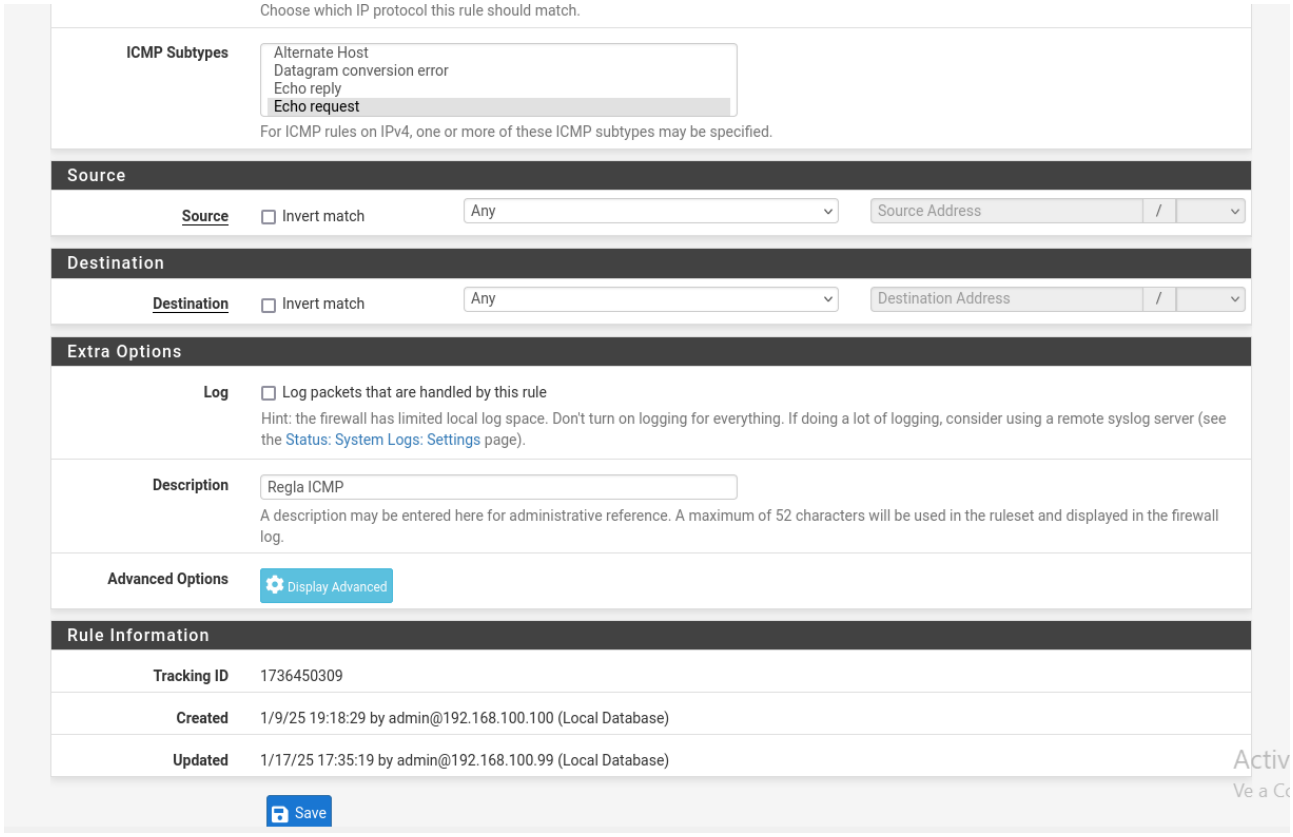
Regla del tráfico DNS



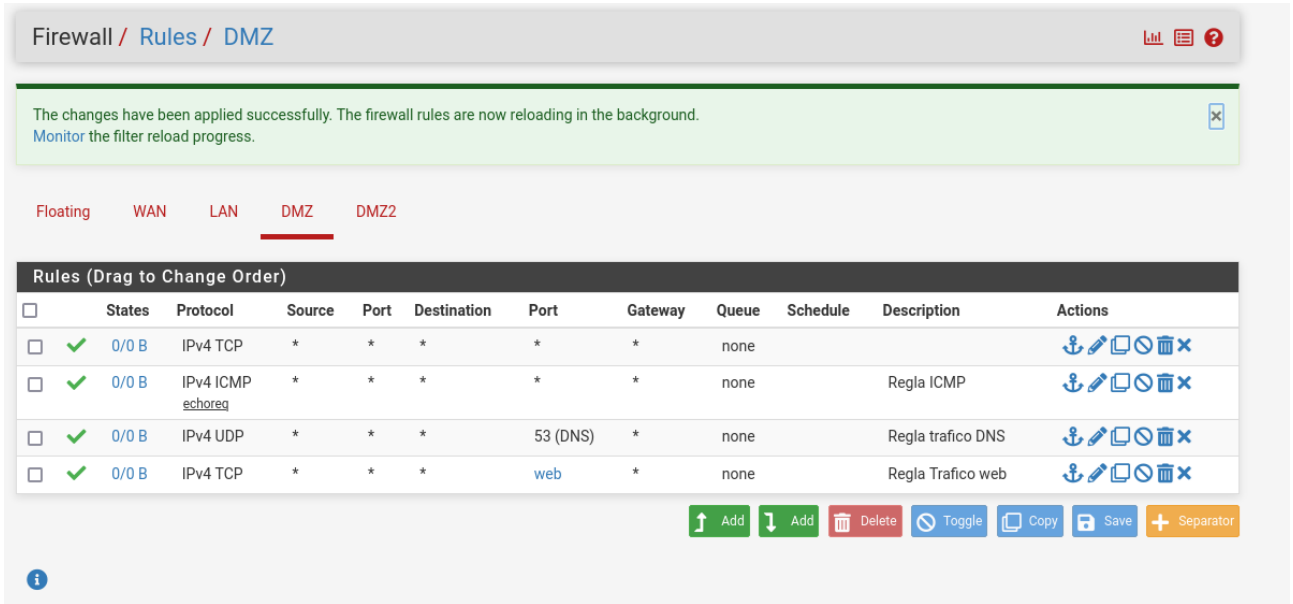


Establecimiento del DMZ Rules acerca del Protocolo ICMP en el firewall

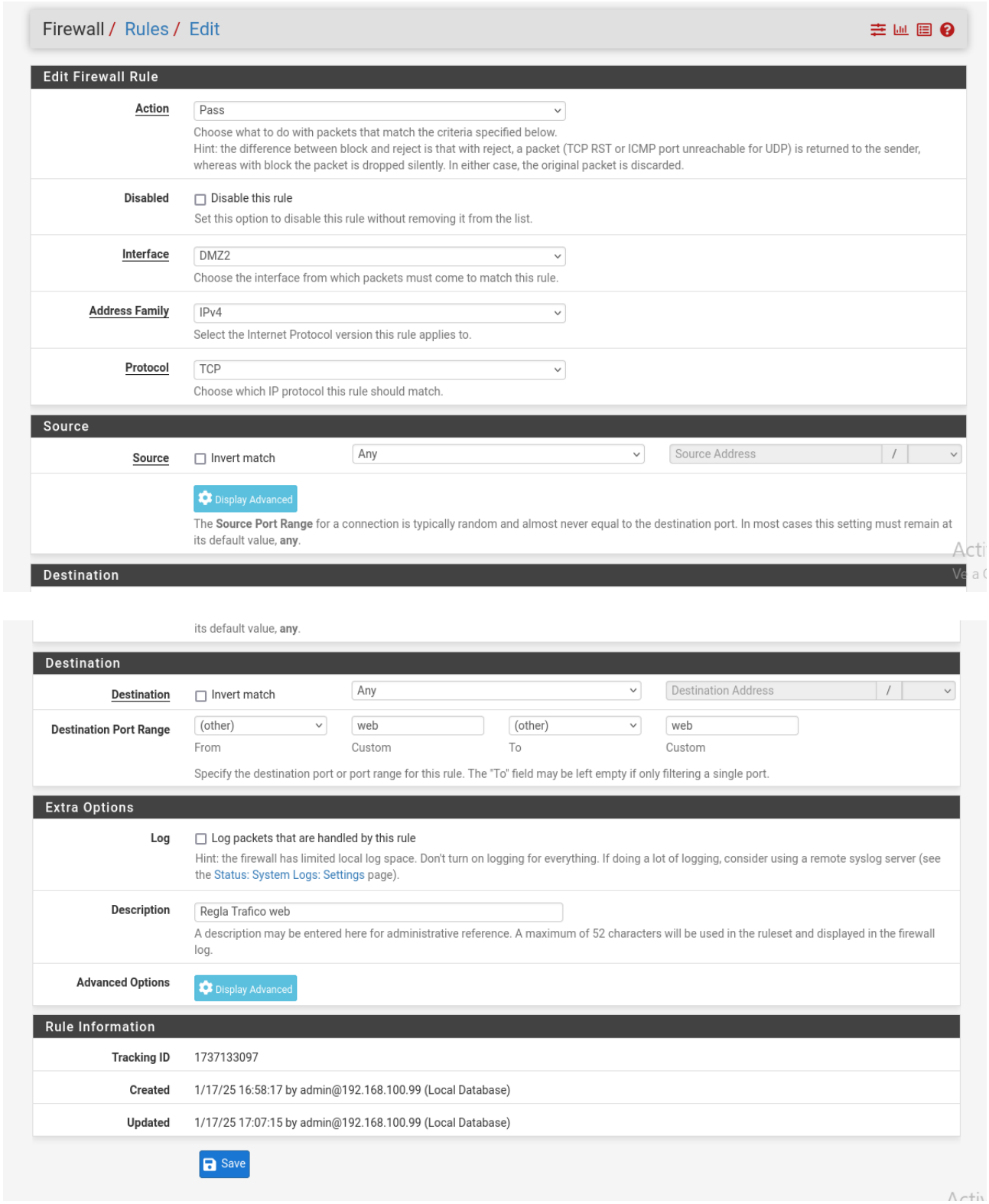




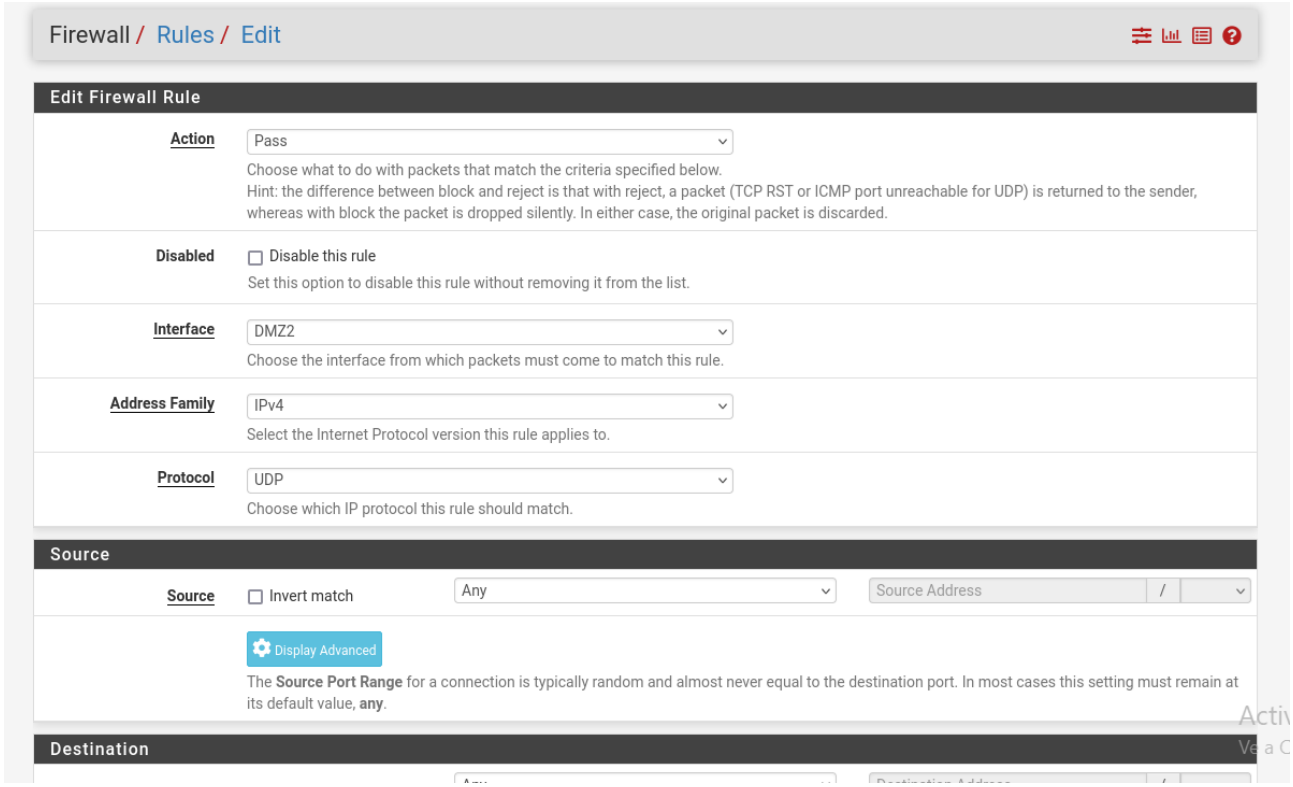
DMZ Firewall Rules

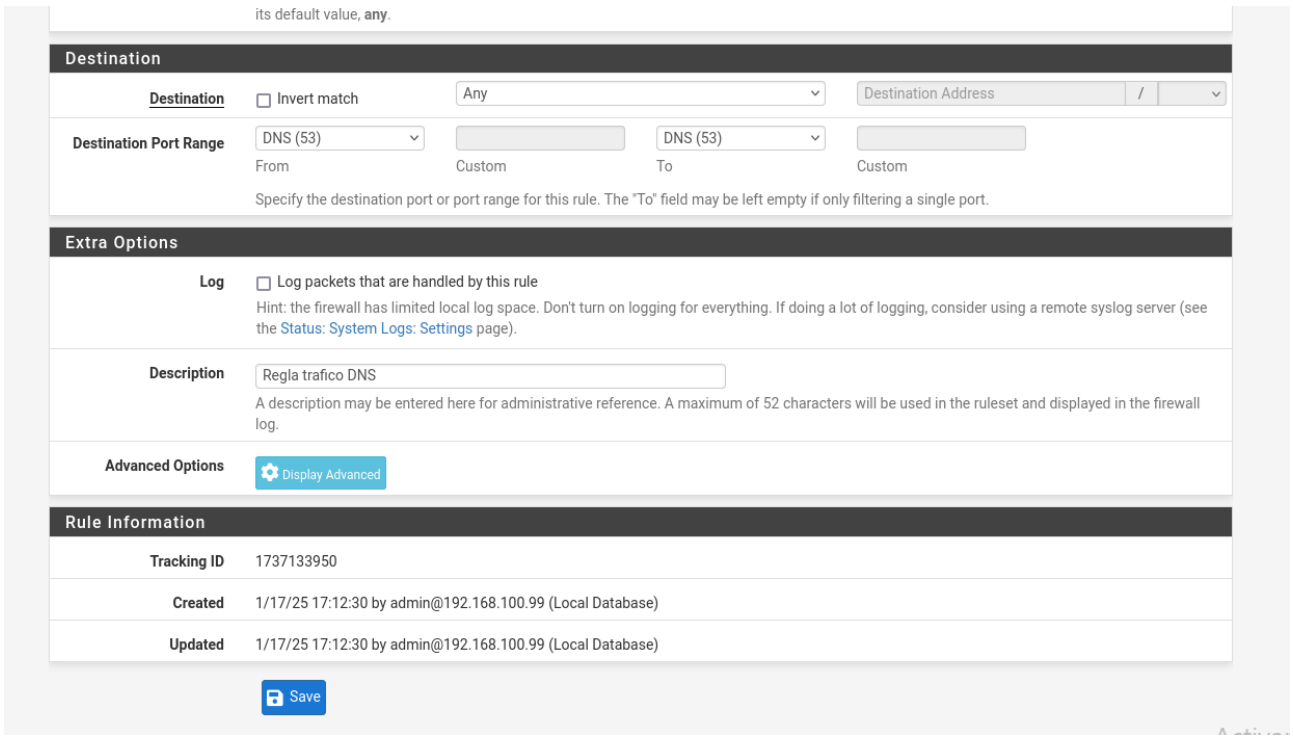


Establecimiento del DMZ2 Rules acerca del trafico Web en el firewall con la nueva regla creada

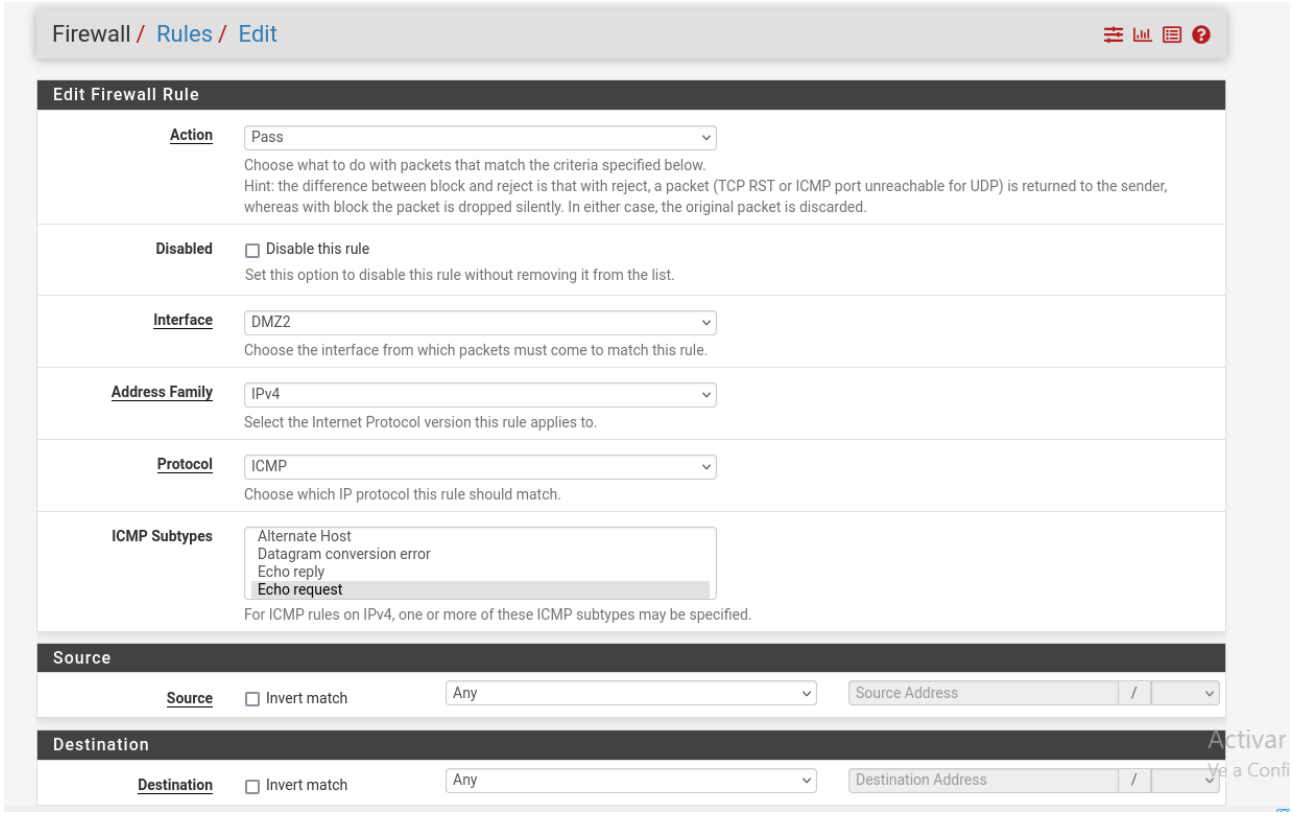


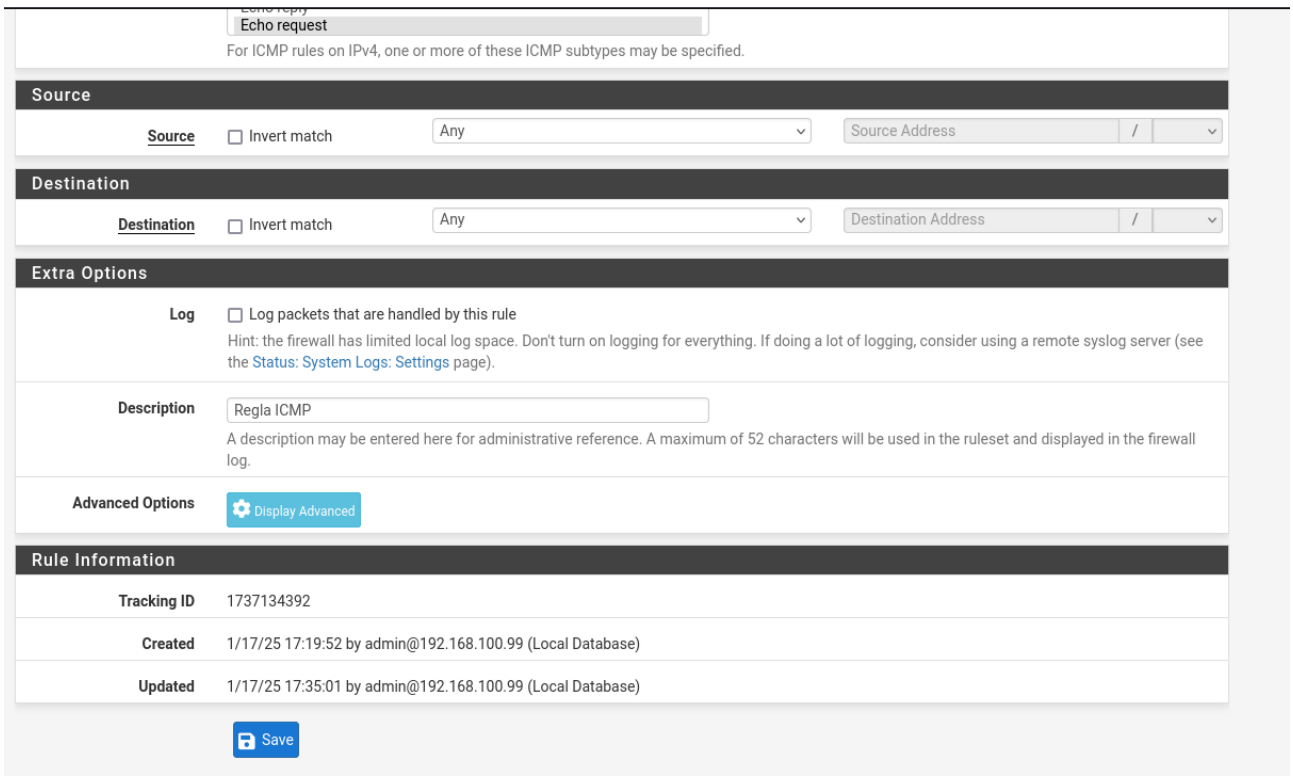
Establecimiento en el DMZ2 acerca del DNS en el Firewall



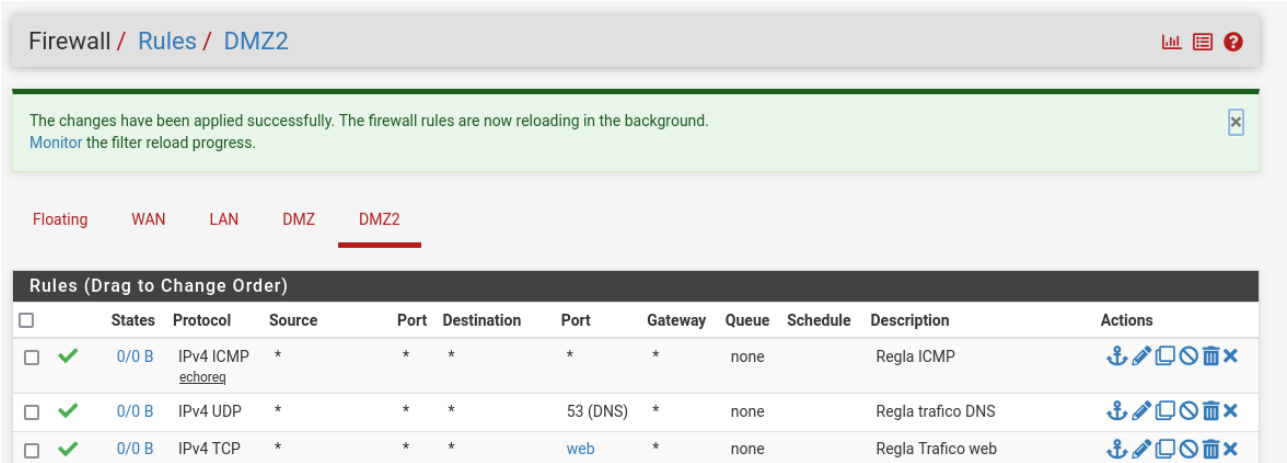


Establecimiento del DMZ2 rules acerca del protocolo ICMP en el firewall

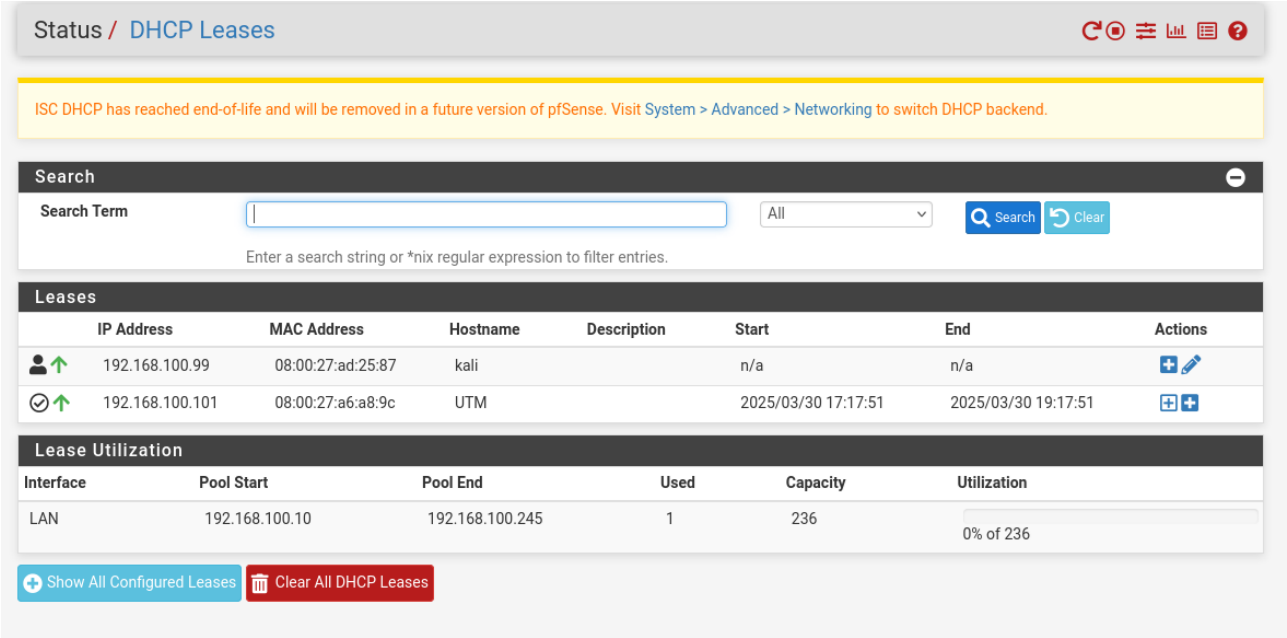




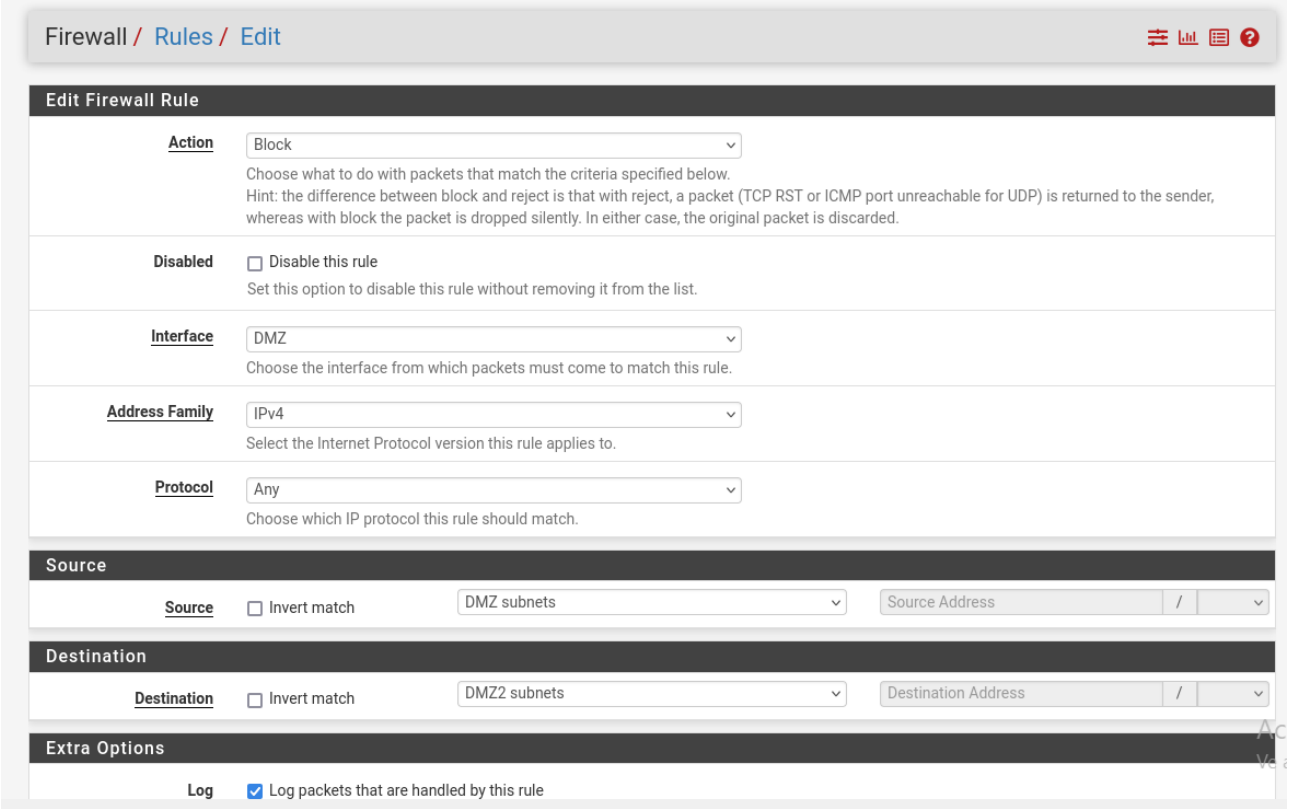
DMZ2 Firewall Rules



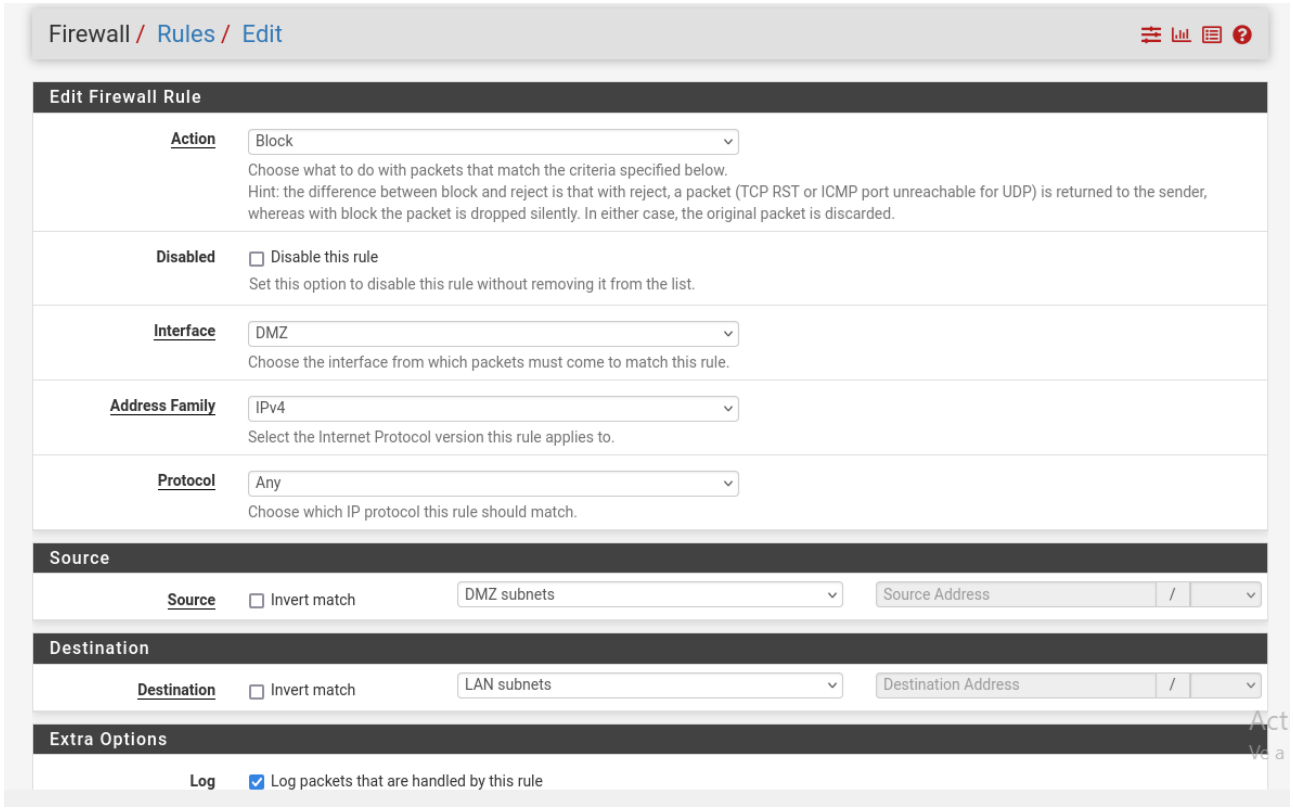
DHCP Status



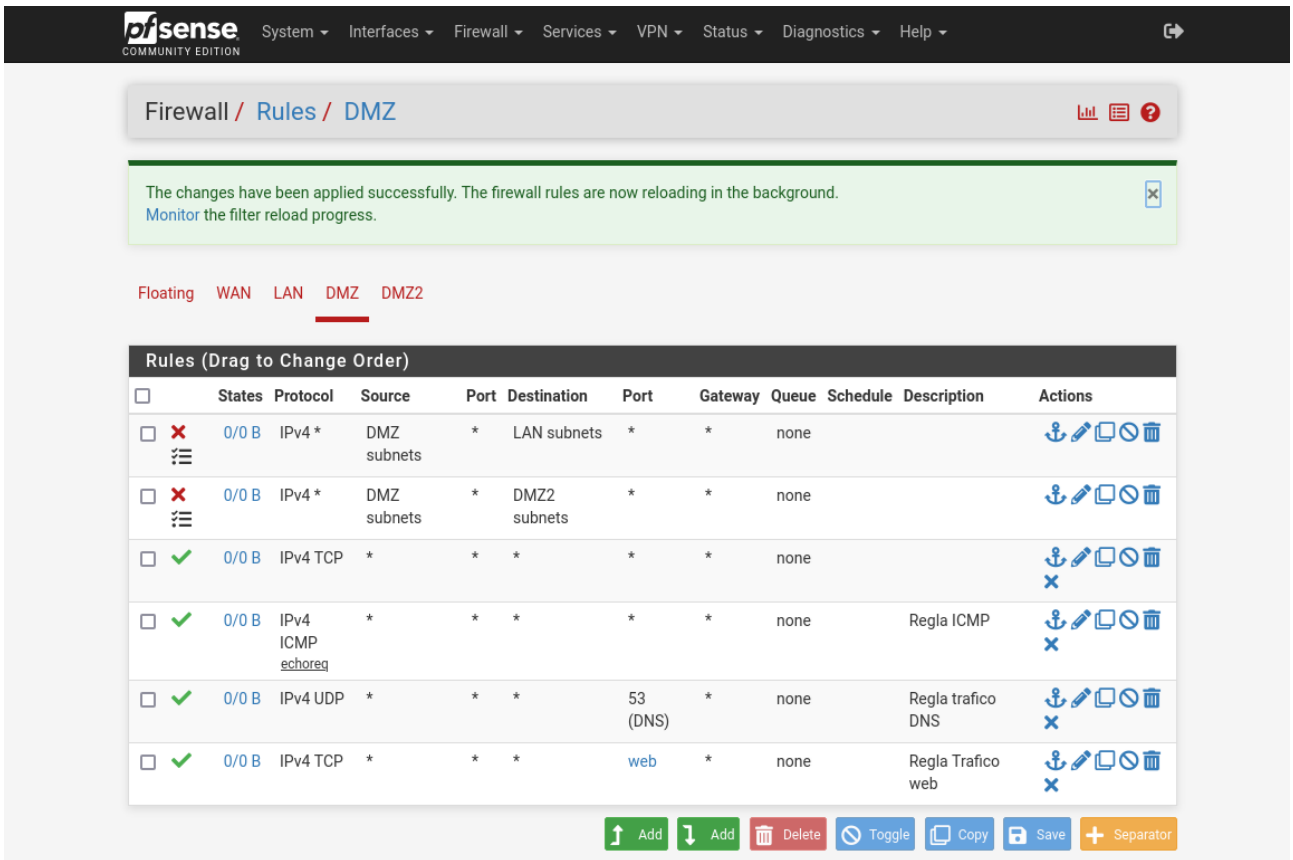
Bloqueo del DMZ2 para el acceso del DMZ



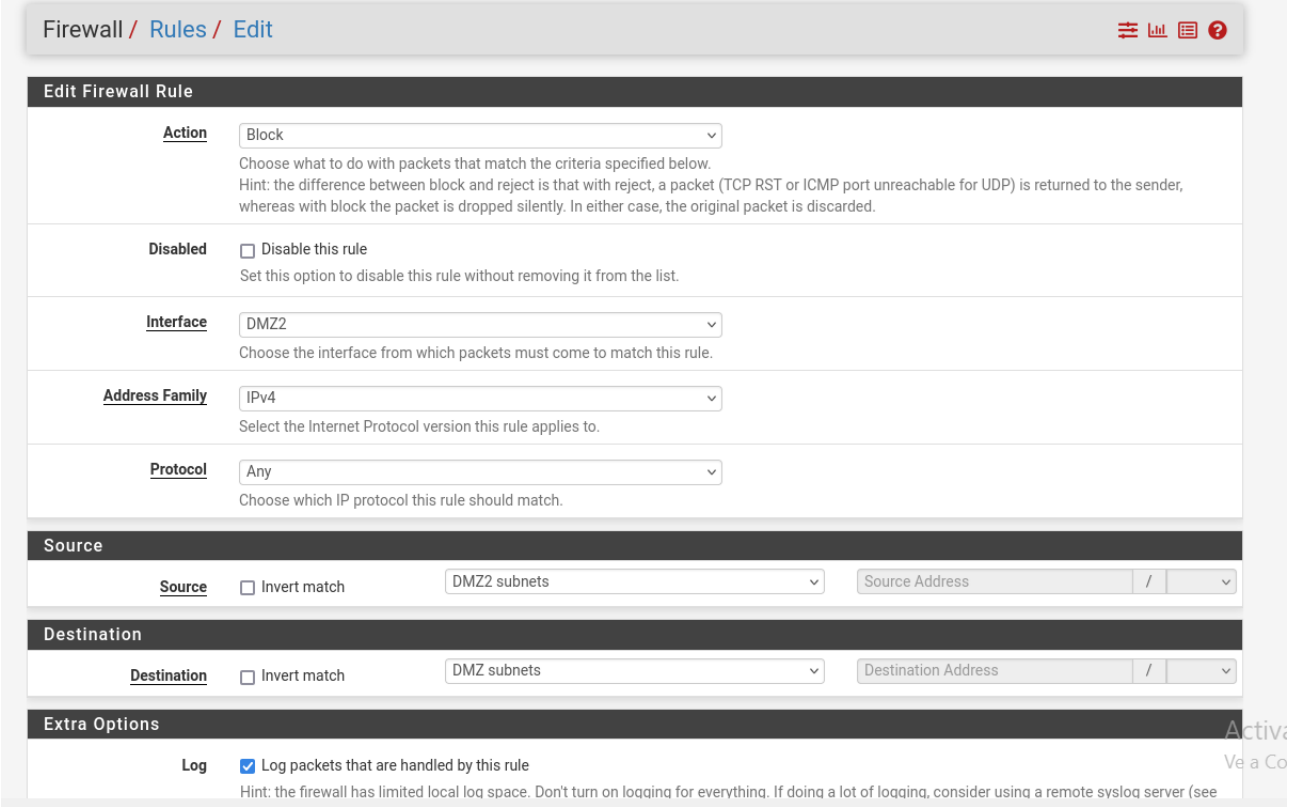
Bloqueo de LAN para el acceso al DMZ


Firewall / Rules / Edit
Edit Firewall Rule
Action
Block
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
DMZ
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
Any
Choose which IP protocol this rule should match.
Source
Source
Invert match
DMZ subnets
Source Address
Destination
Destination
Invert match
LAN subnets
Destination Address
Extra Options
Log
Log packets that are handled by this rule

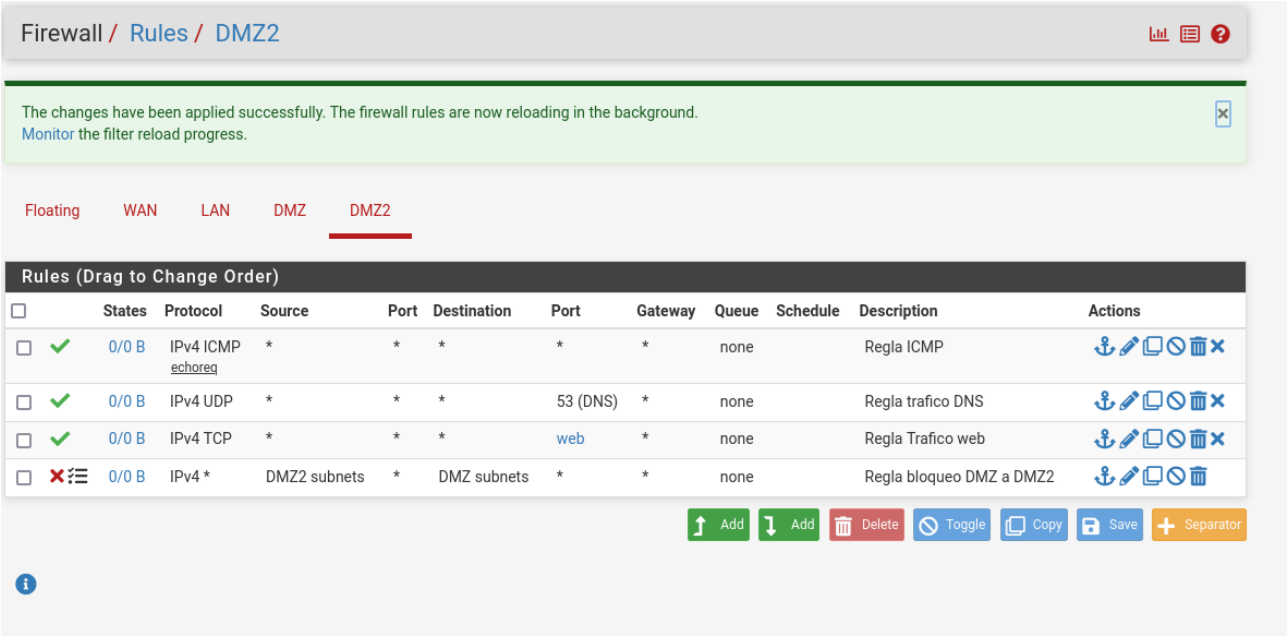
DMZ Rules


pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Firewall / Rules / DMZ
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 * DMZ subnets * LAN subnets * * none
0/0 B IPv4 * DMZ subnets * DMZ2 subnets * * none
0/0 B IPv4 TCP * * * * * none
0/0 B IPv4 ICMP echoreq * * * * * none Regla ICMP
0/0 B IPv4 UDP * * * 53 (DNS) * none Regla trafico DNS
0/0 B IPv4 TCP * * * web * none Regla Trafico web
Add
Add
Delete
Toggle
Copy
Save
Separator

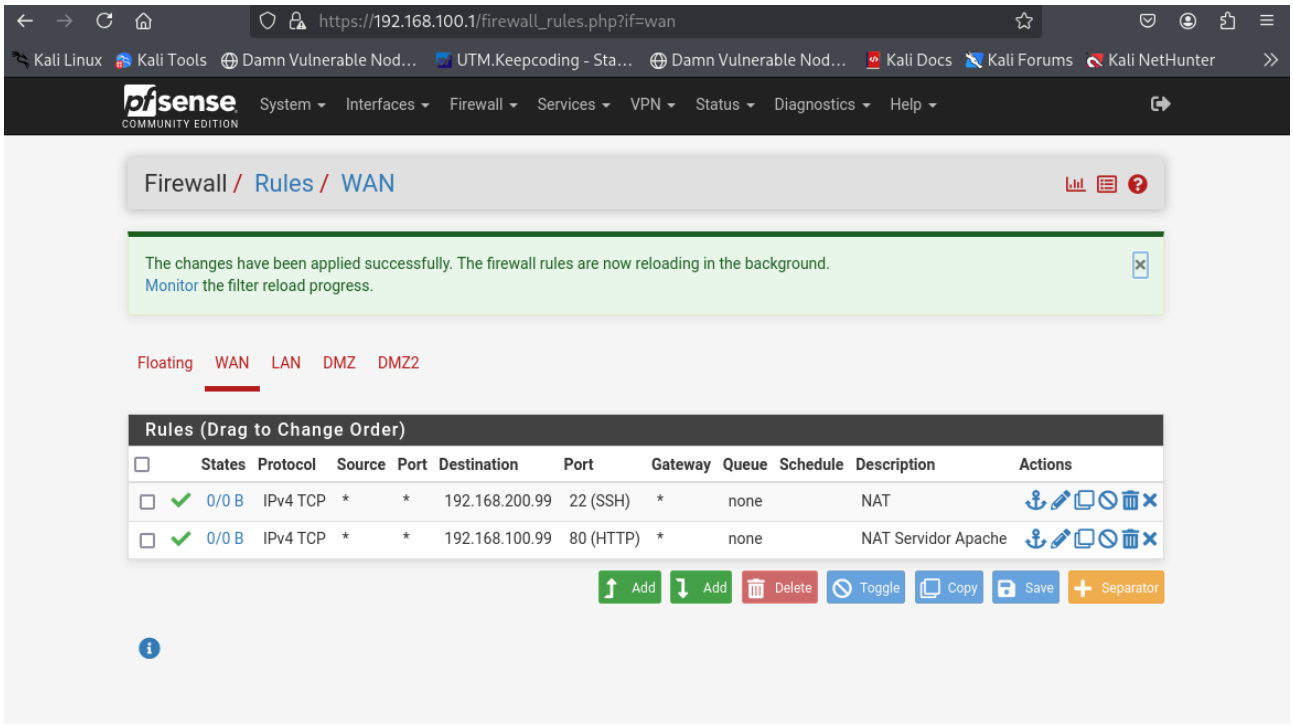
Bloqueo del DMZ2 al DMZ



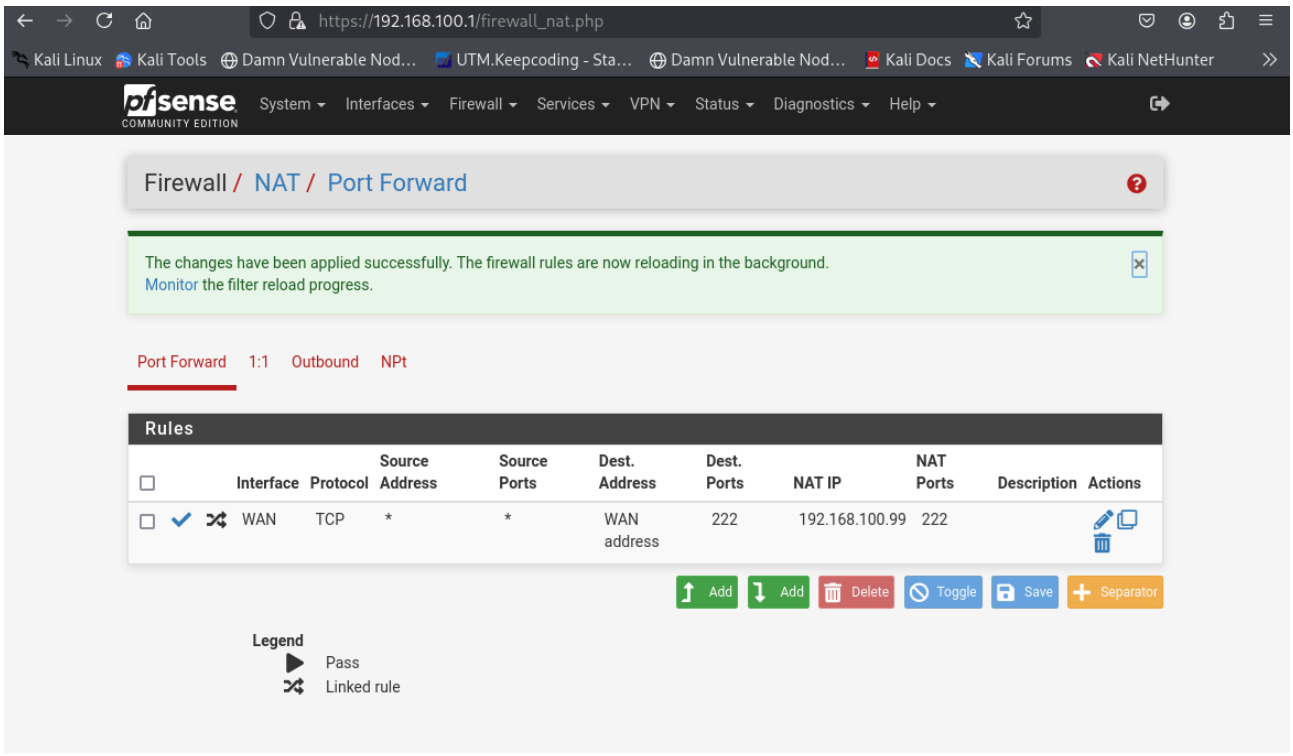
DMZ2 Rules



WAN Honeypot ssh



NAT Honeypot ssh

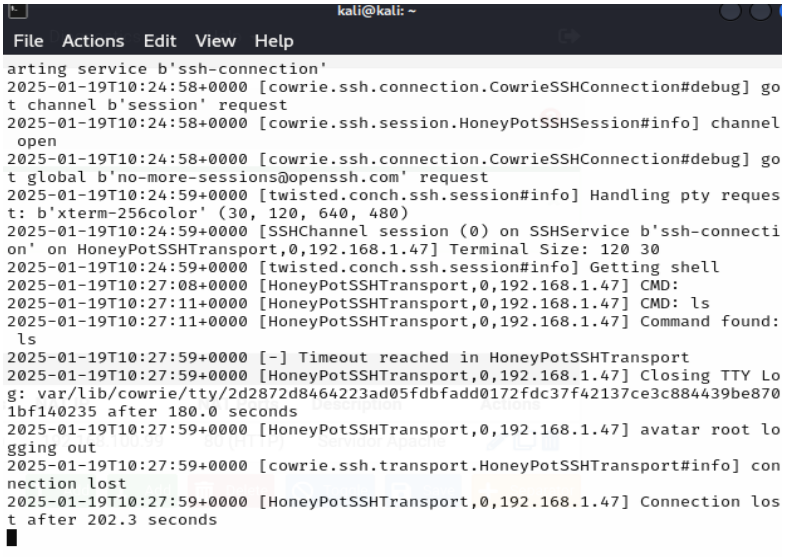


3. Instalación del Honeypot:

Vamos a comenzar ejecutando en nuestra máquina el comando:
docker run -p 222:2222 cowrie/cowrie

Implementamos un Honeypot por ssh:

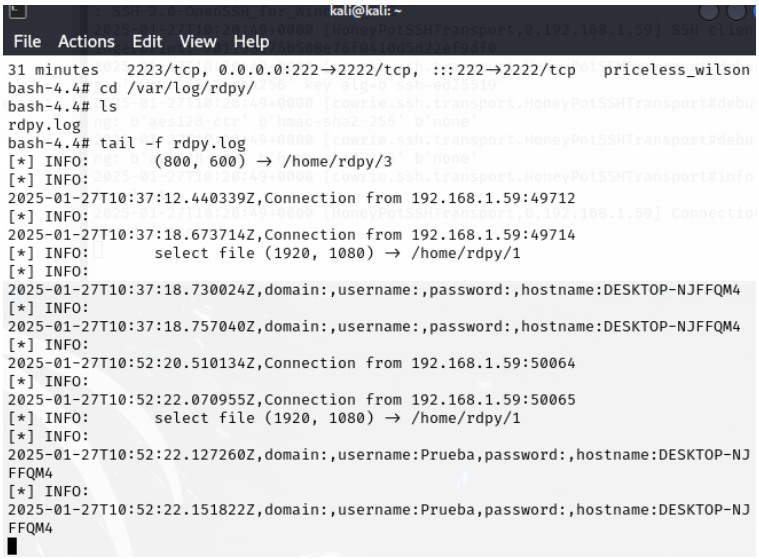
El siguiente paso es conectar nuestro servidor con nuestra máquina Kali:
Para ello ponemos la Kali en el adaptador 1 en adaptador puente, abrimos una consola en nuestro Windows y ejecutamos el comando ssh -p 222 root@192.168.1.68 para conectarnos con nuestra maquina Kali. Tenemos que poner nuestra dirección IP en el comando.



A través de los comandos en nuestra Kali:

docker run -p 333:3389 amazedostrich/rdpy
docker exec -it -u 0 c8b24ded835a /bin/bash (Tenemos que añadir nuestro identificador)

Nos conectamos a través de nuestra consola y nuestro escritorio remoto para poder ver los logs generados en rdpy:



Pasamos a instalar suricata con los comandos :

sudo apt update
sudo apt install suricata
suricata -c /etc/suricata/suricata.yaml -i eth0

```
┌──(kali㉿kali)-[~]
└─$ sudo suricata -c /etc/suricata/suricata.yaml -i eth0
i: suricata: This is Suricata version 7.0.8 RELEASE running in SYSTEM mode
W: detect: No rule files match the pattern /var/lib/suricata/rules/suricata.r
ules
W: detect: 1 rule files specified, but no rules were loaded!
i: threads: Threads created → W: 2 FM: 1 FR: 1   Engine started.
```

Añadimos las siguientes reglas que guardamos en suricata:

Vamos a seguir la siguiente línea de comandos entre otros para añadirlas;

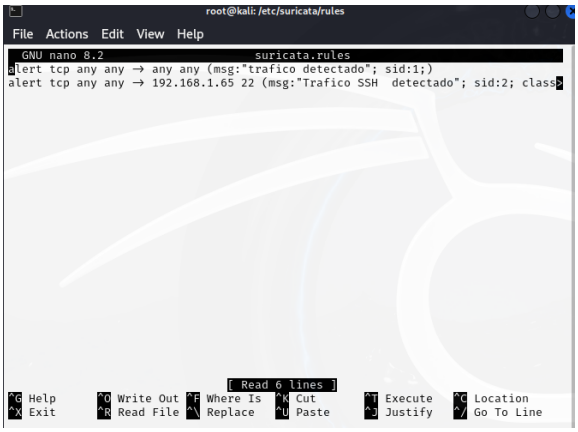
sudo -s para darle privilegios
cd /etc/suricata
ls
cd rules
less files.rules
touch suricata.rules
ls
nano suricata rules

Las dos reglas que añadimos son:

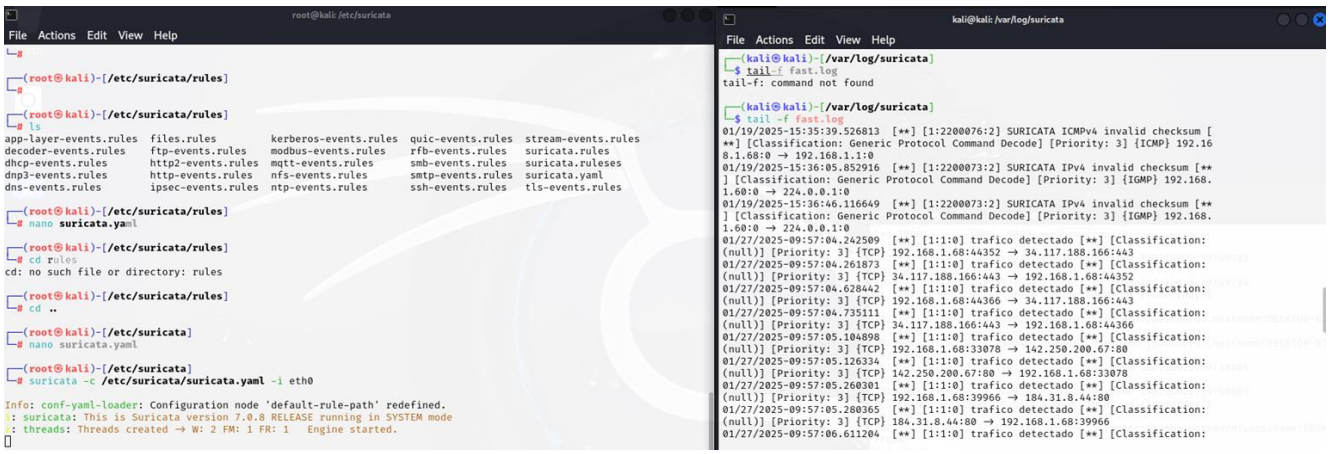
alert tcp any any -> any any (msg:"trafico detectado"; sid:1;)

alert tcp any any -> any any (msg:"PDF Archivo descargado"; flow:established,to_client; fileext:"pdf"; sid:3; classtype:file-download;)

alert tcp any any -> 192.168.1.65 22 (msg:"Trafico SSH detectado"; sid:2; classtype:attempted-admin;)



Una vez que aplicamos las reglas conseguimos conectarnos para ver los logs:



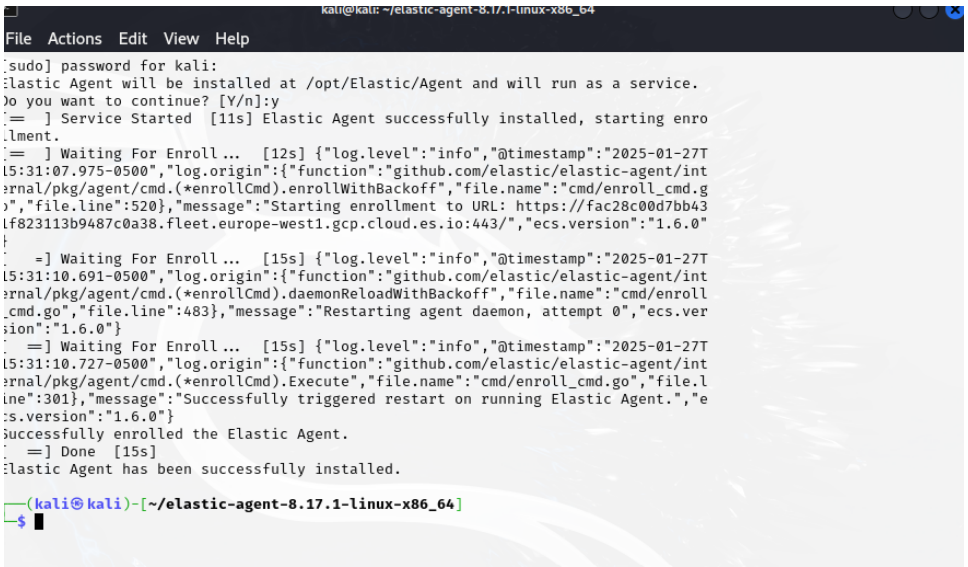
4. Instalación de Elastic (Suricata / Windows / Honeypot)

Nos identificamos en la web de elastic con un mail, bien propio o bien temporal.

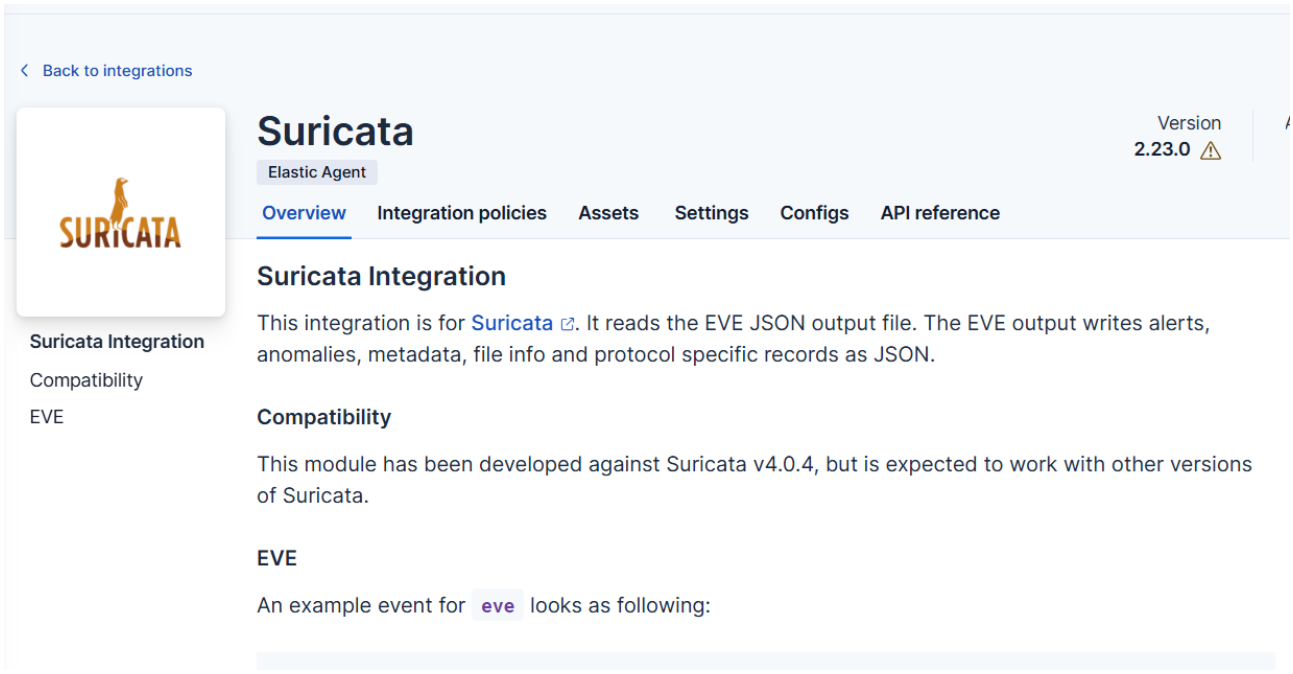
Los pasos a seguir desde la web son: Assets / Fleet / Agent Policies/ Create agent Policy / añadimos un nombre (Suricata/Linux) / pinchamos en las políticas / añadimos una integración / en búsqueda : suricata y añadimos la integración.

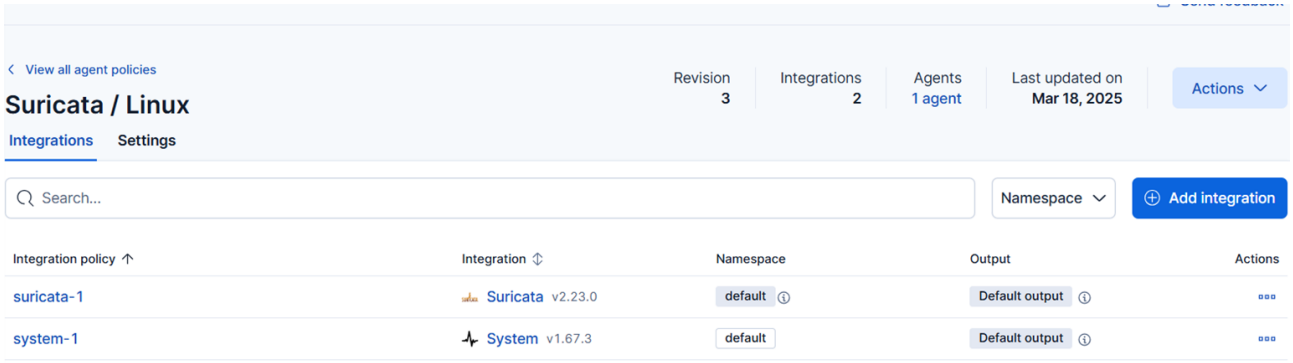
Debemos pegar el comando generado en nuestra Kali para la instalación.

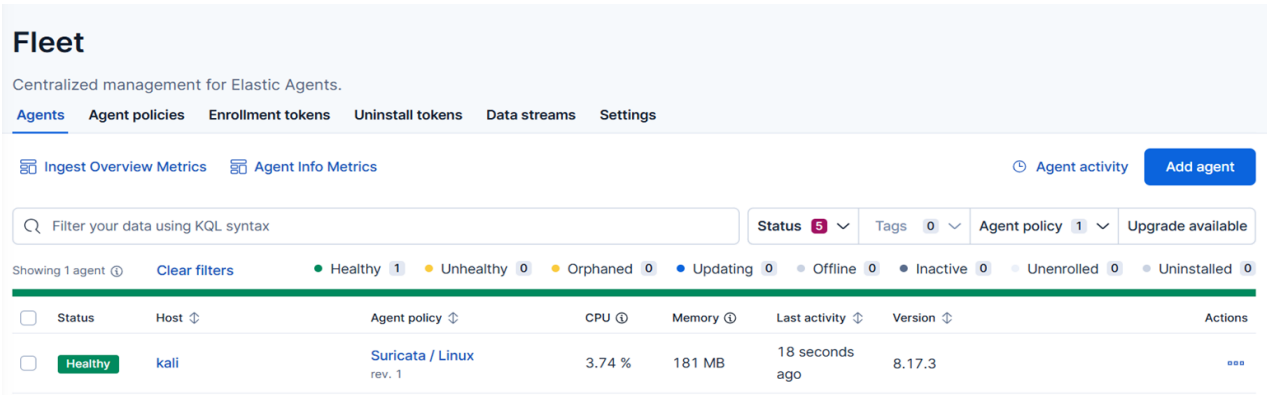
Nos vamos a una consola en nuestra máquina Kali, hacemos Ping para comprobar que hay conexión y copiamos en comando de elastic para instalarlo.



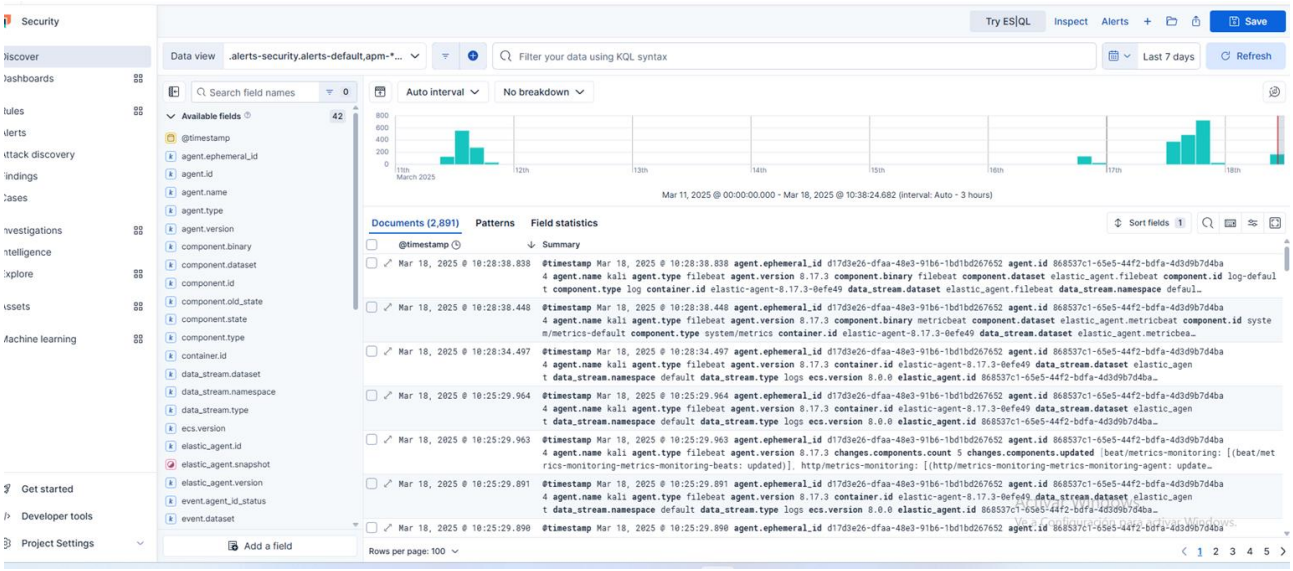
Volvemos a elastic, y podemos comprobar en Assets / Fleet que ya nos saldría nuestro agente añadido suricata/linux.







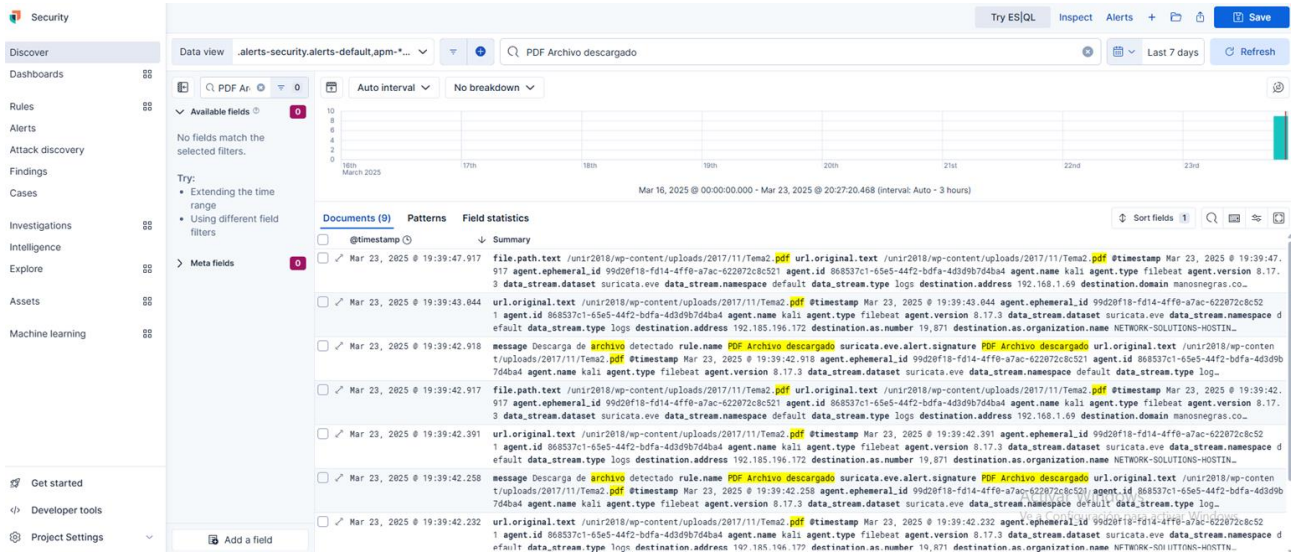
Finalmente en Discover podemos visualizar los logs:

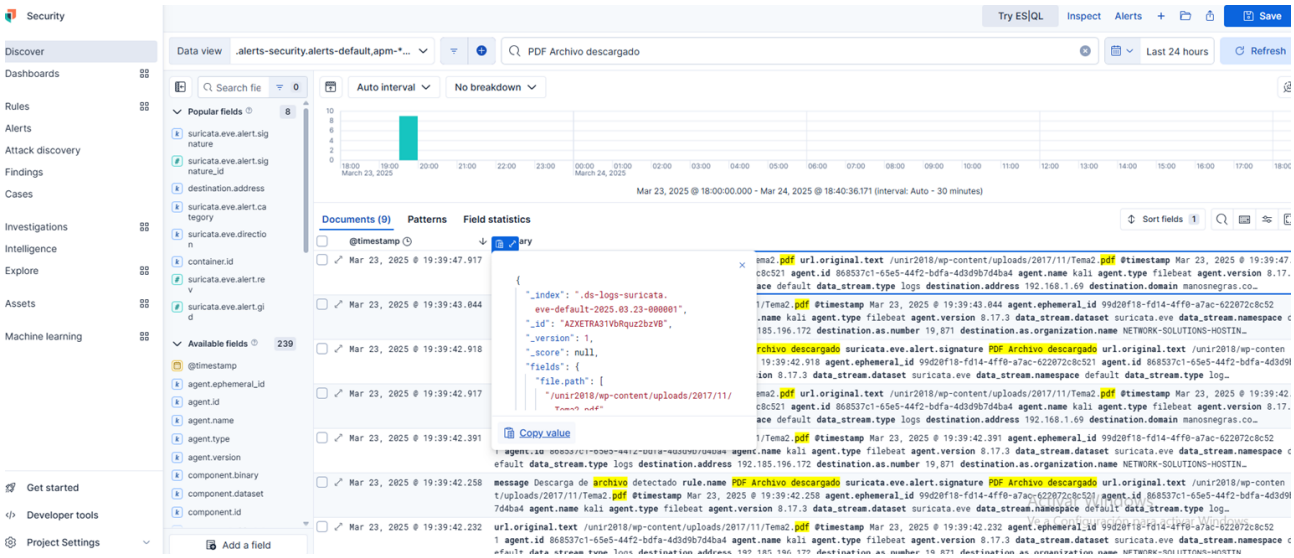


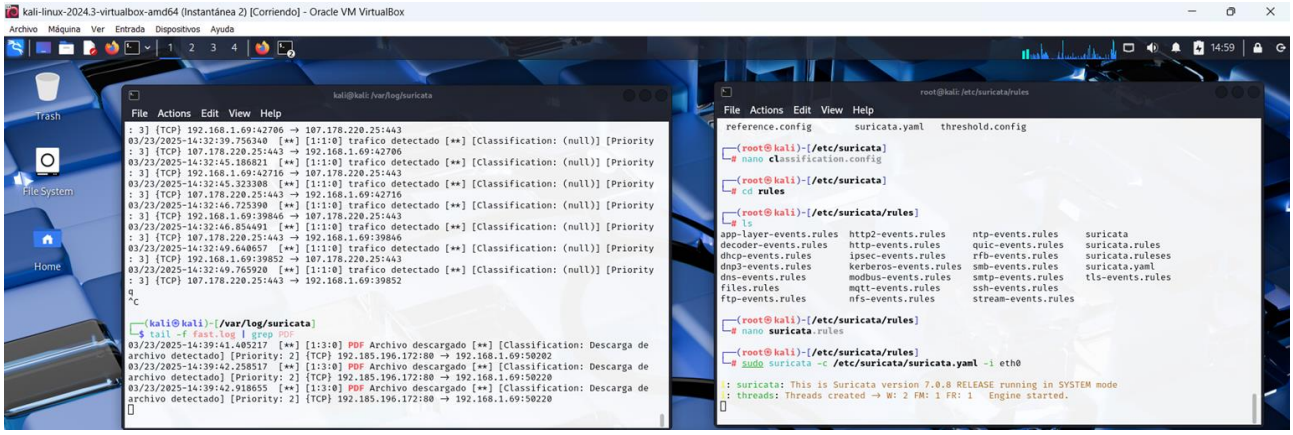
Hemos creado la regla :

alert tcp any any -> any any (msg:"PDF Archivo descargado"; flow:established,to_client; fileext:"pdf"; sid:3; classtype:file-download;)

Mas abajo podemos ver los logs "PDF Archivo descargado" generados por Suricata en nuestra máquina Kali.


Security
Discover
Dashboards
Rules
Alerts
Attack discovery
Findings
Cases
Investigations
Intelligence
Explore
Assets
Machine learning
Get started
Developer tools
Project Settings
Try ES|QL
Inspect
Alerts
Save
Data view
.alerts-security.alerts-default,apm-*...
PDF Archivo descargado
Last 7 days
Refresh
Auto interval
No breakdown
Available fields
No fields match the selected filters.
Try:
Extending the time range
Using different field filters
Meta fields
Add a field
Mar 16, 2025 @ 00:00:00.000 - Mar 23, 2025 @ 20:27:20.468 (interval: Auto - 3 hours)
Documents (9)
Patterns
Field statistics
Sort fields
@timestamp
Summary


Security
Discover
Dashboards
Rules
Alerts
Attack discovery
Findings
Cases
Investigations
Intelligence
Explore
Assets
Machine learning
Get started
Developer tools
Project Settings
Try ES|QL
Inspect
Alerts
Save
Data view
.alerts-security.alerts-default,apm-*...
PDF Archivo descargado
Last 24 hours
Refresh
Auto interval
No breakdown
Popular fields
Available fields
Add a field
Mar 23, 2025 @ 18:00:00.000 - Mar 24, 2025 @ 18:40:36.171 (interval: Auto - 30 minutes)
Documents (9)
Patterns
Field statistics
Sort fields
@timestamp
Copy value

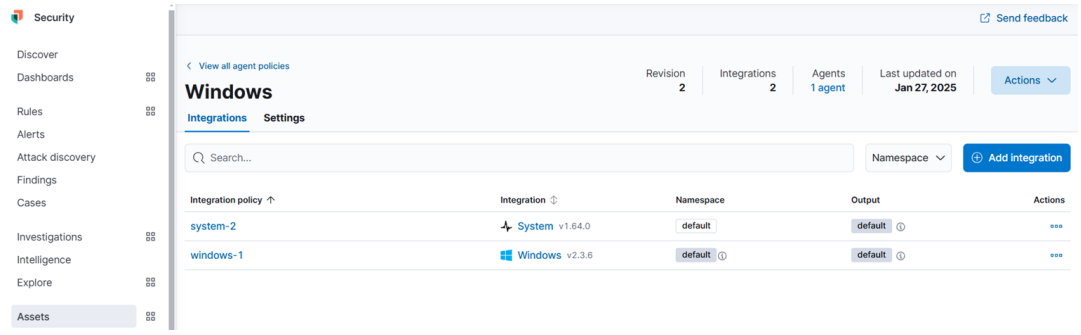

kali-linux-2024.3-virtualbox-amd64 (Instantánea 2) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Trash
File System
Home
kali@kali: /var/log/suricata
File Actions Edit View Help
root@kali: /etc/suricata/rules
File Actions Edit View Help
reference.config
suricata.yaml
threshold.config
app-layer-events.rules
decoder-events.rules
dhcp-events.rules
dnp3-events.rules
dns-events.rules
files.rules
ftp-events.rules
http2-events.rules
http-events.rules
ipsec-events.rules
kerberos-events.rules
modbus-events.rules
mqtt-events.rules
nfs-events.rules
ntp-events.rules
quic-events.rules
rfb-events.rules
smb-events.rules
smtp-events.rules
ssh-events.rules
stream-events.rules
suricata
suricata.rules
suricata.ruleset
suricata.yaml
tls-events.rules

Se adjunta el log generado por Suricata en elastic y descargado desde el elastic:

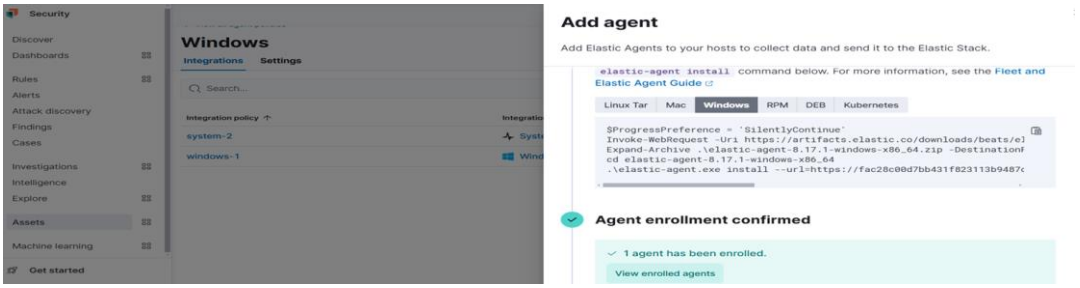
{ "@timestamp": ["2025-03-23T18:39:47.917Z"], "agent.ephemeral_id": ["99d20f18-fd14-4ff0-a7ac-622072c8c521"], "agent.id": ["868537c1-65e5-44f2-bdfa-4d3d9b7d4ba4"], "agent.name": ["kali"], "agent.type": ["filebeat"], "agent.version": ["8.17.3"], "data_stream.dataset": ["suricata.eve"], "data_stream.namespace": ["default"], "data_stream.type": ["logs"], "destination.address": ["192.168.1.69"], "destination.domain": ["manosnegras.com"], "destination.ip": ["192.168.1.69"], "destination.port": [50220], "ecs.version": ["8.17.0"], "elastic_agent.id": ["868537c1-65e5-44f2-bdfa-4d3d9b7d4ba4"], "elastic_agent.snapshot": [false], "elastic_agent.version": ["8.17.3"], "event.agent_id_status": ["verified"], "event.category": ["network"], "event.created": ["2025-03-23T18:39:48.425Z"], "event.dataset": ["suricata.eve"], "event.ingested": ["2025-03-23T18:39:58.000Z"], "event.kind": ["event"], "event.module": ["suricata"], "file.path": ["/unir2018/wp-content/uploads/2017/11/Tema2.pdf"], "file.path.text": ["/unir2018/wp-content/uploads/2017/11/Tema2.pdf"], "file.size": [65536], "http.request.method": ["GET"], "http.request.referrer": ["https://www.google.com/"], "http.response.body.bytes": [65536], "http.response.status_code": [206], "input.type": ["log"], "log.file.path": ["/var/log/suricata/eve.json"], "log.offset": [8321020], "network.community_id": ["1:ANFZ+smBtvKNXhm19NF0y49DIWM="], "network.protocol": ["http"], "network.transport": ["tcp"], "observer.hostname": ["kali"], "observer.ip": ["192.168.1.69", "fe80::b4b0:9a6a:b0aa:5394", "172.17.0.1", "fe80::42:e7ff:fee4:5dae"], "observer.mac": ["02-42-E7-E4-5D-AE", "08-00-27-AD-25-87"], "observer.product": ["Suricata"], "observer.type": ["ids"], "observer.vendor": ["OISF"], "related.hosts": ["manosnegras.com"], "related.ip": ["192.185.196.172", "192.168.1.69"], "source.address": ["192.185.196.172"], "source.as.number": [19871], "source.as.organization.name": ["NETWORK-SOLUTIONS-HOSTING"], "source.as.organization.name.text": ["NETWORK-SOLUTIONS-HOSTING"], "source.geo.continent_name": ["North America"], "source.geo.country_iso_code": ["US"], "source.geo.country_name": ["United States"], "source.geo.location": [{ "coordinates": [-97.8220000024885, 37.75099997408688], "type": "Point" }], "source.ip": ["192.185.196.172"], "source.port": [80], "suricata.eve.event_type": ["fileinfo"], "suricata.eve.fileinfo.end": ["1970-01-01T00:48:03.583Z"], "suricata.eve.fileinfo.gaps": [false], "suricata.eve.fileinfo.start": ["1970-01-01T00:46:58.048Z"], "suricata.eve.fileinfo.state": ["CLOSED"], "suricata.eve.fileinfo.stored": [false], "suricata.eve.fileinfo.tx_id": [1], "suricata.eve.flow_id": ["1433806486926790"], "suricata.eve.http.content_range.end": ["1970-01-01T00:48:03.583Z"], "suricata.eve.http.content_range.raw": ["bytes 2818048-2883583/2916403"], "suricata.eve.http.content_range.size": [2916403], "suricata.eve.http.content_range.start": ["1970-01-01T00:46:58.048Z"], "suricata.eve.http.http_content_type": ["application/pdf"], "suricata.eve.http.protocol": ["HTTP/1.1"], "suricata.eve.in_iface": ["eth0"], "suricata.eve.pkt_src": ["wire/pcap"], "tags": ["forwarded", "suricata-eve"], "url.domain": ["manosnegras.com"], "url.original": ["/unir2018/wp-content/uploads/2017/11/Tema2.pdf"], "url.original.text": ["/unir2018/wp-content/uploads/2017/11/Tema2.pdf"], "url.path": ["/unir2018/wp-content/uploads/2017/11/Tema2.pdf"], "user_agent.device.name": ["Other"], "user_agent.name": ["Firefox"], "user_agent.original": ["Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0"], "user_agent.original.text": ["Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0"], "user_agent.os.name": ["Linux"], "user_agent.os.name.text": ["Linux"], "user_agent.version": ["128.0"], "_id": "AZXETRA31VbRquz2bzVB", "_index": ".ds-logs-suricata.eve-default-2025.03.23-000001", "_score": null }

Para ver los logs del Windows nos vamos a la politica de suricata/linux creada y le añadimos otra integración para recopilar los logs del Windows:

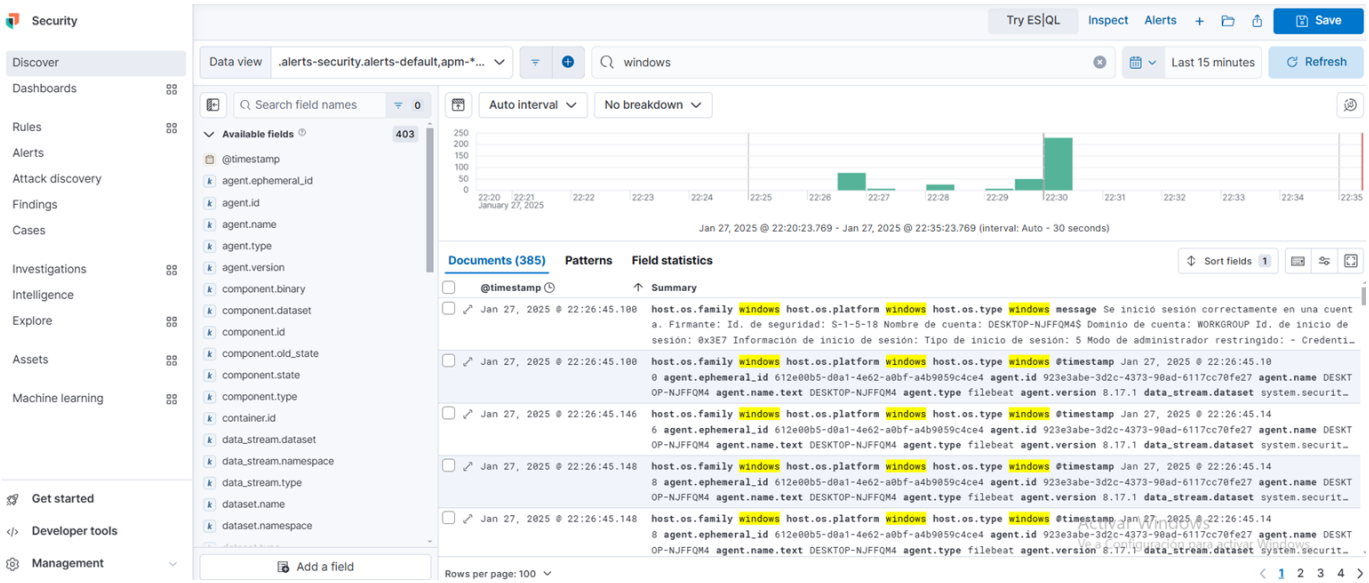
(Previamente hemos instalado en VirtualBox nuestra máquina de Windows, de modo que es independiente y logueada en elastic).

Una 

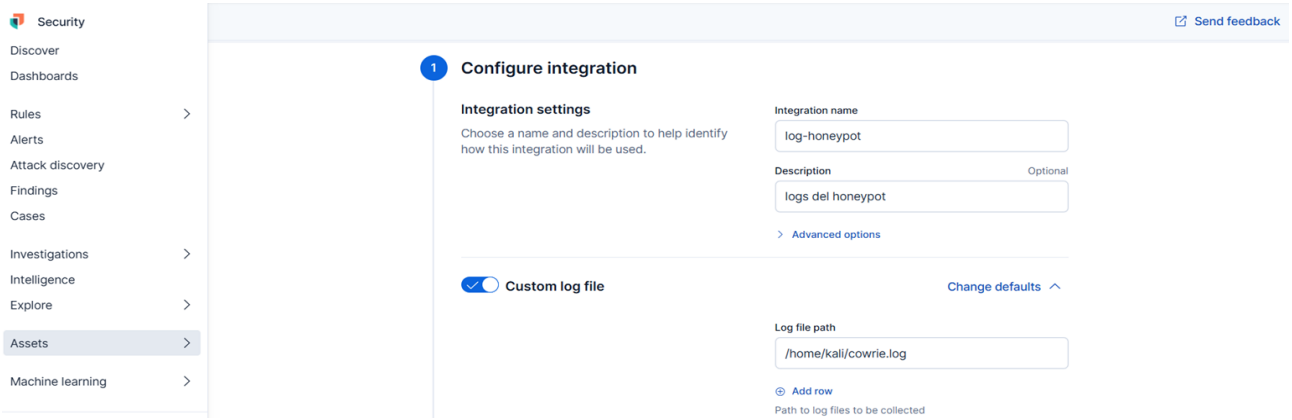
vez hemos instalada la politica copiamos el comando y lo pegamos en la consola powershell para instalarlo

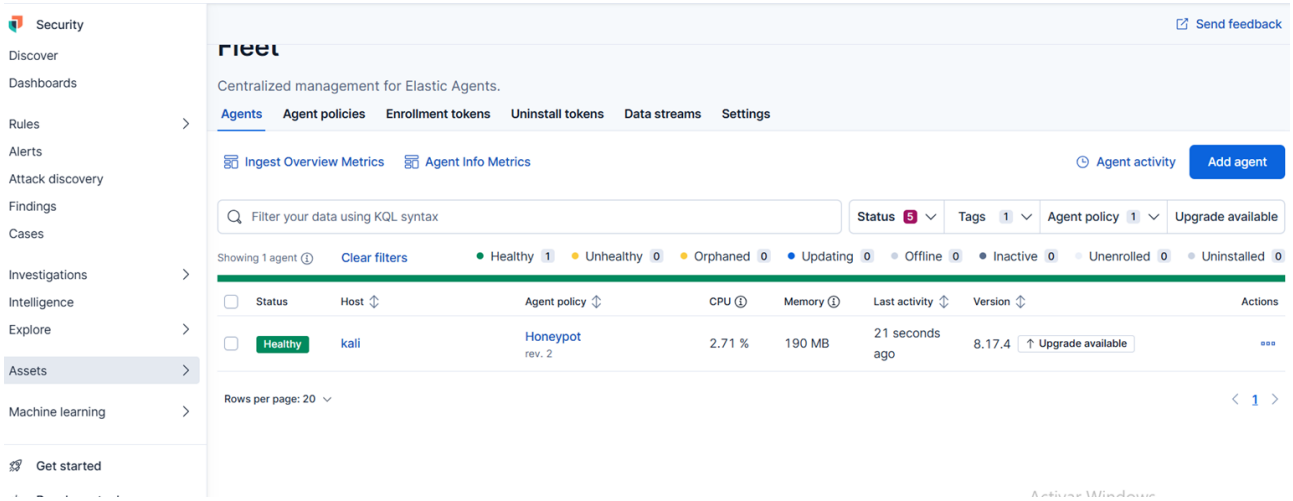


En el apartado de Discover podemos ver los logs de Windows:

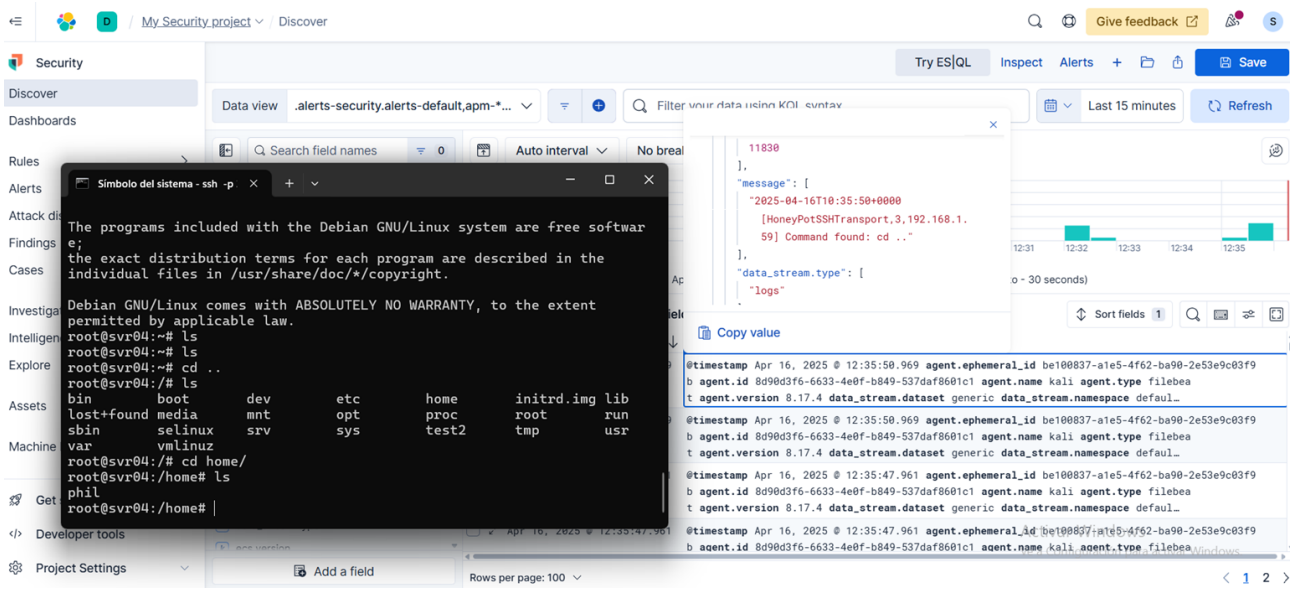


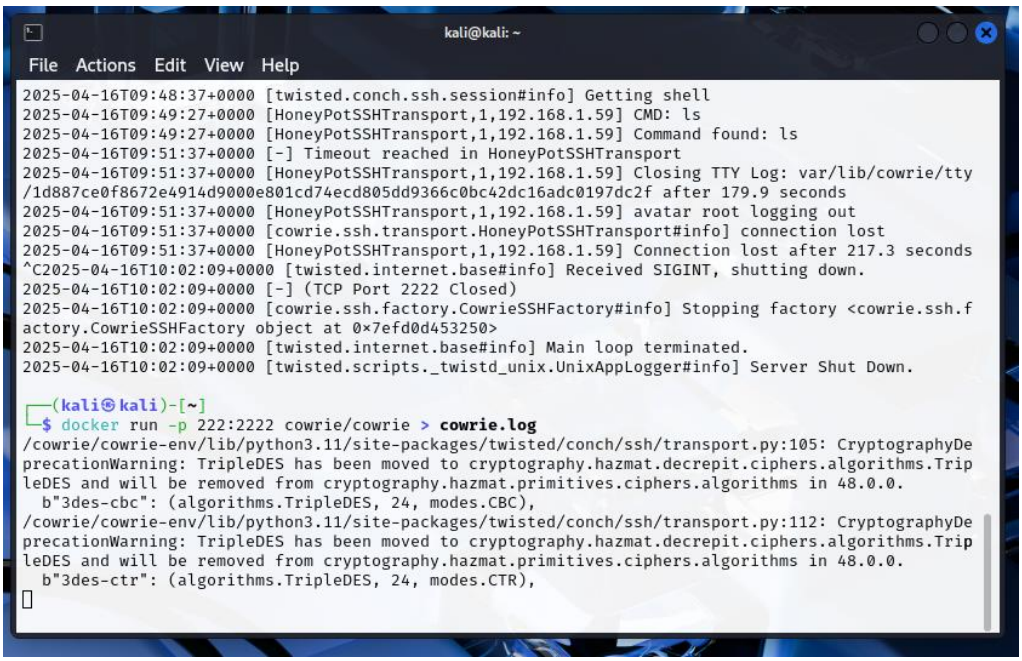
Finalmente vamos a instalar el Honeypot en el elastic como una integración en suricata-Linux ya que estamos usando la misma máquina kali, y lo haremos con la integración de Customlog:





Aquí podemos ver los logs del Honeypot:



Log  generado:

{ "@timestamp": ["2025-04-16T10:45:35.794Z"], "agent.ephemeral_id": ["be100837-a1e5-4f62-ba90-2e53e9c03f9b"], "agent.id": ["8d90d3f6-6633-4e0f-b849-537daf8601c1"], "agent.name": ["kali"], "agent.type": ["filebeat"], "agent.version": ["8.17.4"], "data_stream.dataset": ["generic"], "data_stream.namespace": ["default"], "data_stream.type": ["logs"], "ecs.version": ["8.0.0"], "elastic_agent.id": ["8d90d3f6-6633-4e0f-b849-537daf8601c1"], "elastic_agent.snapshot": [false], "elastic_agent.version": ["8.17.4"], "event.agent_id_status": ["verified"], "event.dataset": ["generic"], "event.ingested": ["2025-04-16T10:45:48.000Z"], "host.architecture": ["x86_64"], "host.containerized": [false], "host.hostname": ["kali"], "host.id": ["30e662c5c81d4191bd2444a79c97d2e0"], "host.ip": ["192.168.1.69", "fe80::b4b0:9a6a:b0aa:5394", "172.17.0.1", "fe80::42:35ff:fe34:b0b8", "fe80::9c1e:58ff:fe0a:7e3d"], "host.mac": ["02-42-35-34-B0-B8", "08-00-27-AD-25-87", "9E-1E-58-0A-7E-3D"], "host.name": ["kali"], "host.os.codename": ["kali-rolling"], "host.os.family": ["debian"], "host.os.kernel": ["6.12.13-amd64"], "host.os.name": ["Kali GNU/Linux"], "host.os.name.text": ["Kali GNU/Linux"], "host.os.platform": ["kali"], "host.os.type": ["linux"], "host.os.version": ["2025.1"], "input.type": ["log"], "log.file.path": ["/home/kali/cowrie.log"], "log.file.path.text": ["/home/kali/cowrie.log"], "log.offset": [16062], "message": ["2025-04-16T10:45:33+0000 [HoneyPotSSHTransport,4,192.168.1.59] Command found: cd opt"], "_id": "AZY-NO_7dOcSX215YFyY", "_index": ".ds-logs-generic-default-2025.04.16-000001", "_score": null }