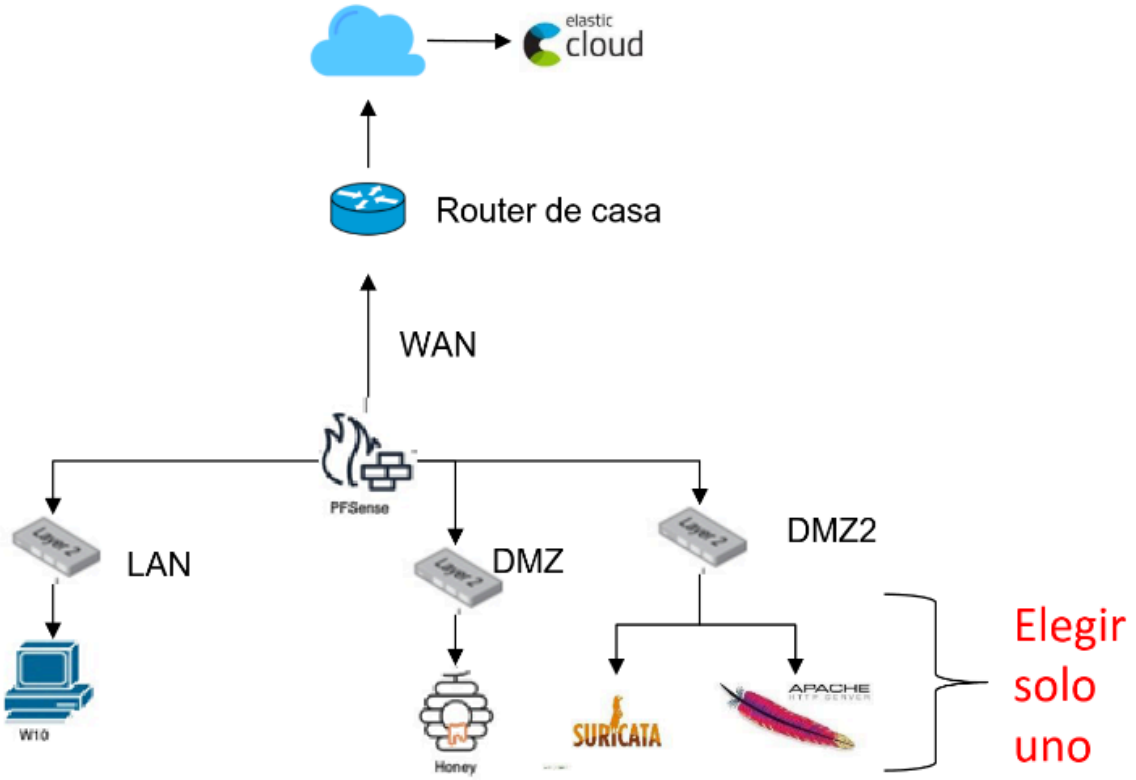
BLUE TEAM: MONTAJE DE UNA INFRAESTRUCTURA DE RED



Primero y antes de nada, descargamos el **PFSENSE** desde el siguiente enlace:

- https://drive.google.com/file/d/1c38GjIVtqJV4OotIOoKUvNbc_6REhRKC/view?usp=drive_link

Una vez descargado, **extraemos** la imagen ISO e inicializamos virtualbox, en el menú de virtualbox vamos a máquina y la damos a nueva para añadir una nueva máquina y comenzamos la instalación, en los primeros parámetros, **cargamos la imagen ISO** escogeremos **tipo BSD** y la **versión FreeBSD (64-bit).**

En la siguiente pantalla escogeremos una **memoria base de 1250 mb** (aproximadamente) y un **procesador de 1 cpu**. Después en la siguiente pantalla dejaremos por defecto un **tamaño de disco de 16 GB** y en la última pantalla le daremos a **finalizar**.

Una vez tenemos la máquina virtual en nuestro menú de máquinas virtuales de virtualbox, haciendo clic derecho vamos a **configuración > red,** aquí nos encontraremos cuatro **adaptadores** que deberán quedar de la siguiente forma:

- Adaptador 1: Adaptador puente
- Adaptador 2: Red interna con nombre “LAN”.
- Adaptador 3: Red interna con nombre “DMZ”.
- Adaptador 4: Red interna con nombre “DMZ2”.

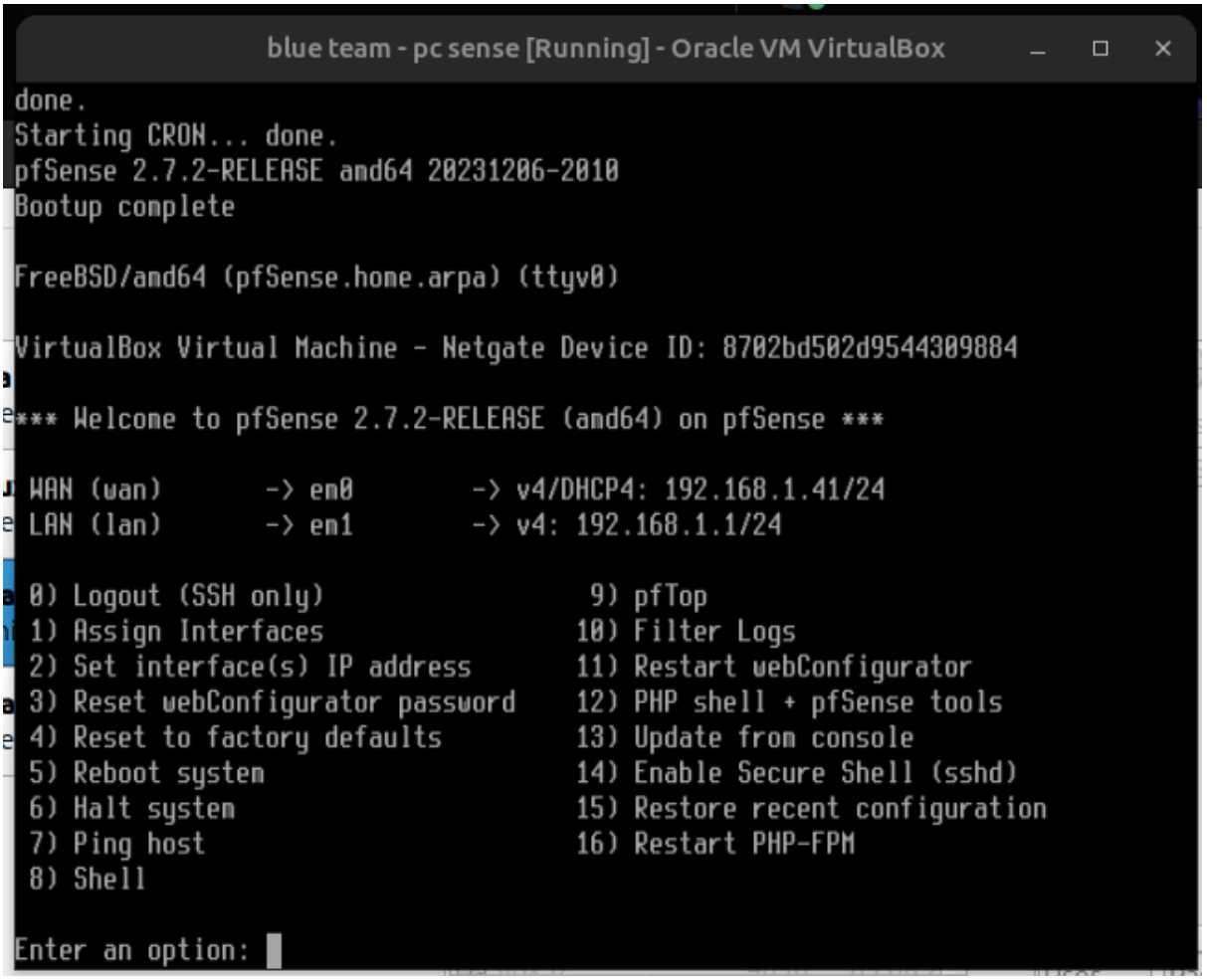
Después, arrancamos la máquina para que comience la **instalación de PFSENSE:**

- Primera pantalla: pulsamos aceptar.
- Segunda pantalla: pulsamos OK sin cambiar parámetros.
- Tercera pantalla: pulsamos OK sin cambiar parámetros.
- Cuarta pantalla: pulsamos SELECT sin cambiar parámetros.
- Quinta pantalla: pulsamos OK sin cambiar parámetros.
- Sexta pantalla (configuración): le damos a la barra espaciadora, debería salir un asterisco, después pulsamos OK.
- Última pantalla (destruir datos): pulsamos YES.

Después de esto empezará la instalación, cuando termine apagamos la máquina sin dejar que vuelva a la primera pantalla en negro. Volvemos a abrir VirtualBox y en la máquina de

PFSENSE hacemos clic derecho y vamos a **configuración > almacenamiento** y **borramos la imagen ISO.**

Si arrancamos la máquina y esperamos un minuto deberíamos ver esto:



A continuación, arrancamos una máquina Kali y en **configuración > red**, en el adaptador 1 escogeremos **red interna con nombre LAN**.

Para que nos asigne una **nueva dirección IP** desconectamos y volvemos a conectar el **adaptador de red** de la máquina Kali, en el menú inferior izquierdo, el cuarto icono empezando por la derecha, las dos pantallas, escogeremos “connect network adapter” para desconectar y volveremos a hacerlo para conectarlo de nuevo.

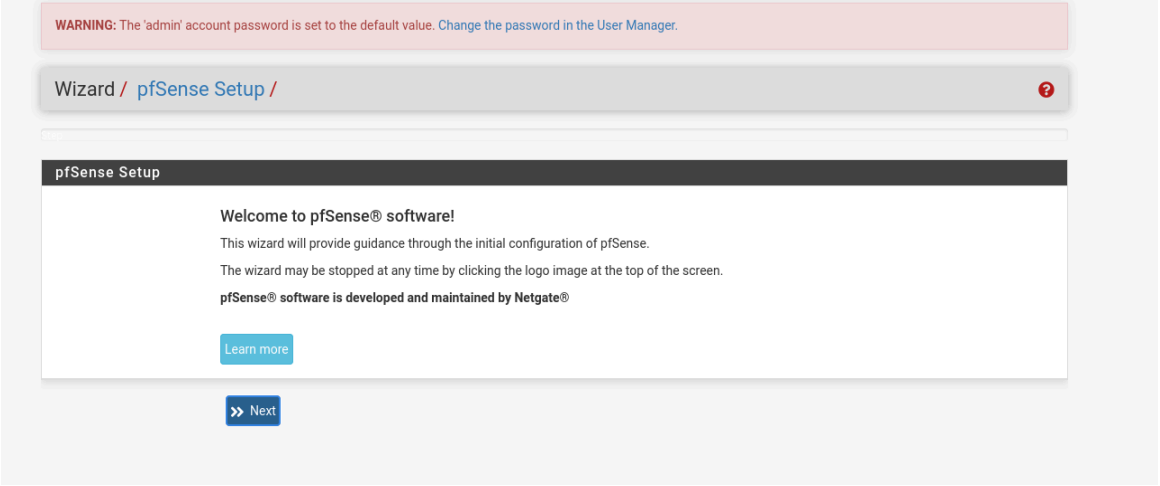
De esta manera nuestra máquina Kali estará conectada a la red LAN dentro del rango que marca nuestro PFSENSE, podemos comprobarlo ejecutando en la terminal de Kali el comando “ip a”.

Después, abrimos el navegador y ponemos la **dirección de la LAN** (192.168.1.1 en mi caso), nos saldrá una pantalla de advertencia, aquí clicamos en “**avanzado”** y hacemos clic en “**aceptar el riesgo”.**

El navegador nos llevará a una página de inicio de sesión:

- Usuario: **admin**
- Contraseña: **pfsense**

Debería salirnos una pantalla como esta:



En esta pantalla, hacemos clic en “NEXT”, en la siguiente volvemos a hacer clic en “NEXT”, y en la siguiente pondremos los siguientes parametros:

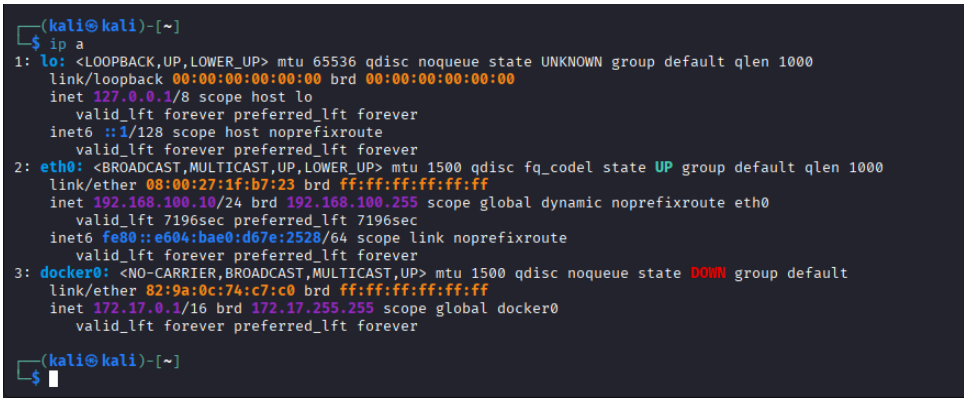
- Nombre: UTM

- Dominio: keepcoding.local
- Servidor primario DNS: 127.0.0.1
- Servidor secundario DNS: 1.1.1.1

Hacemos clic en “NEXT”, en la siguiente pantalla escogemos **zona horaria** y hacemos clic en “NEXT”, en esta pantalla debemos ir hacia al final, veremos **dos secciones** que están marcadas con un tic azul, debemos **descartarlas** quitándole el tic azul, después le damos a “NEXT”, en la siguiente pantalla ajustaremos la LAN a los parámetros de nuestra infraestructura de red, por ello pondremos en **“LAN IP ADDRESS” 192.168.100.1,** hacemos clic en “NEXT” y en esta pantalla tendremos que cambiar nuestra contraseña, importante no olvidarla ya que si esto nos pasara tendríamos que repetir la instalación, le damos clic a “NEXT” y en la última pantalla le damos clic a “RELOAD”.

Ahora necesitamos que se nos asigne una nueva dirección IP por lo que volveremos a repetir el proceso de **conectar y desconectar el adaptador de red.**

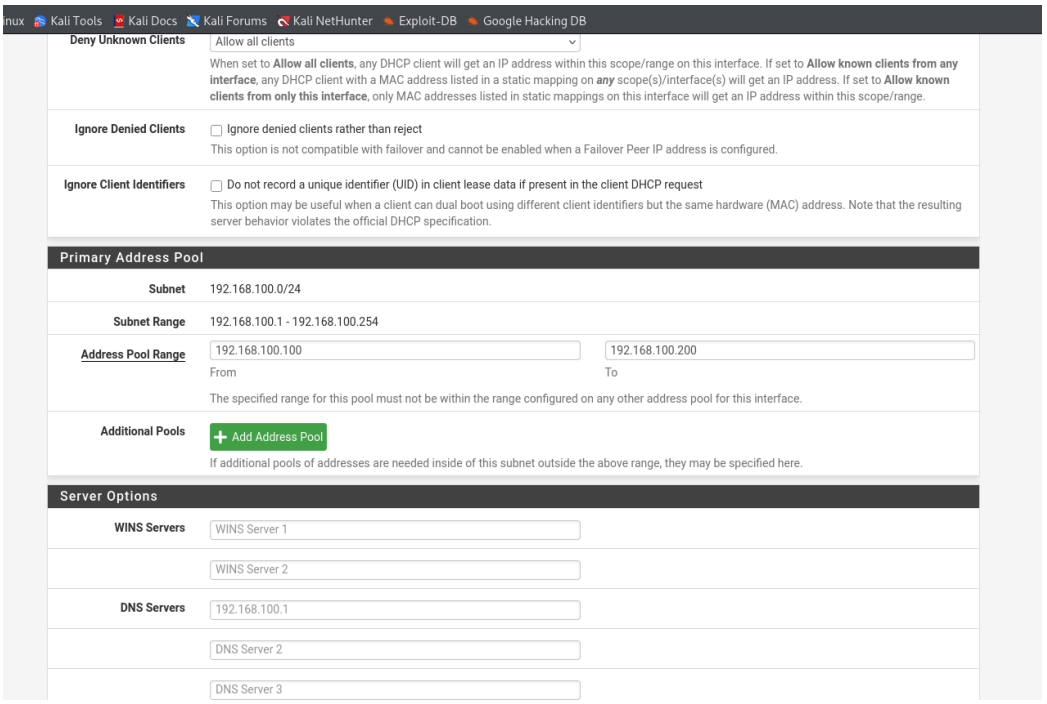
Si hacemos ‘‘ip a’’ en nuestra máquina Kali podremos comprobar que se nos ha asignado correctamente esta nueva dirección IP.

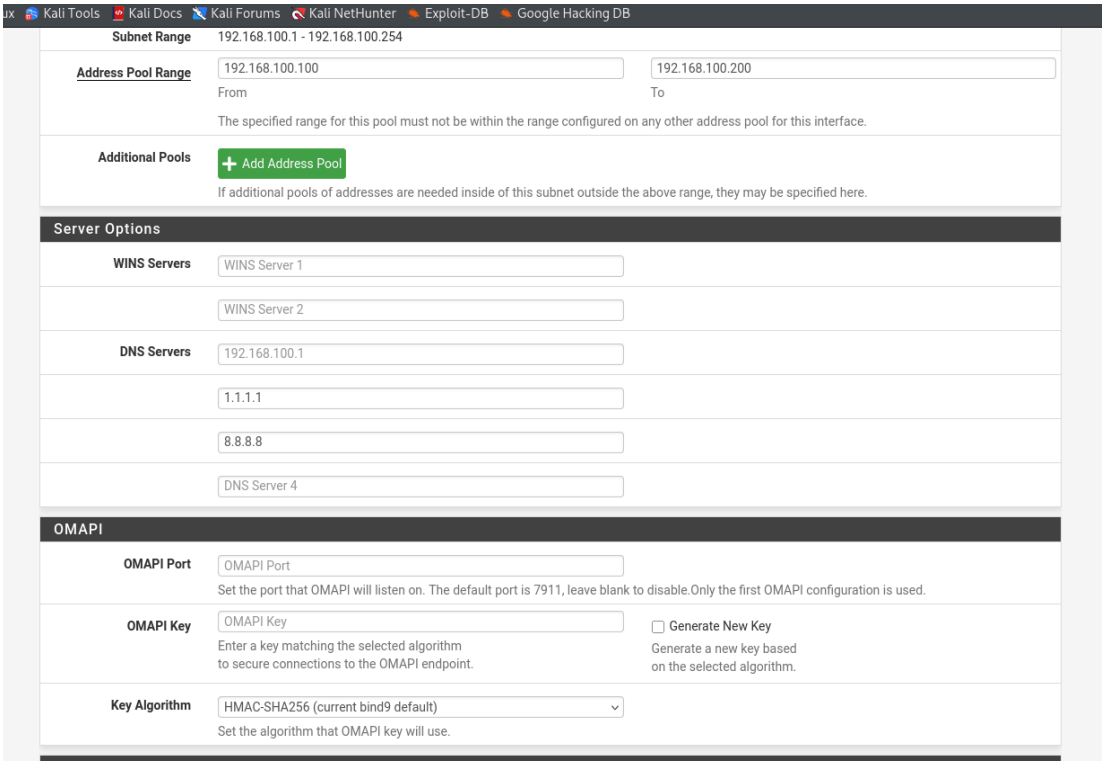


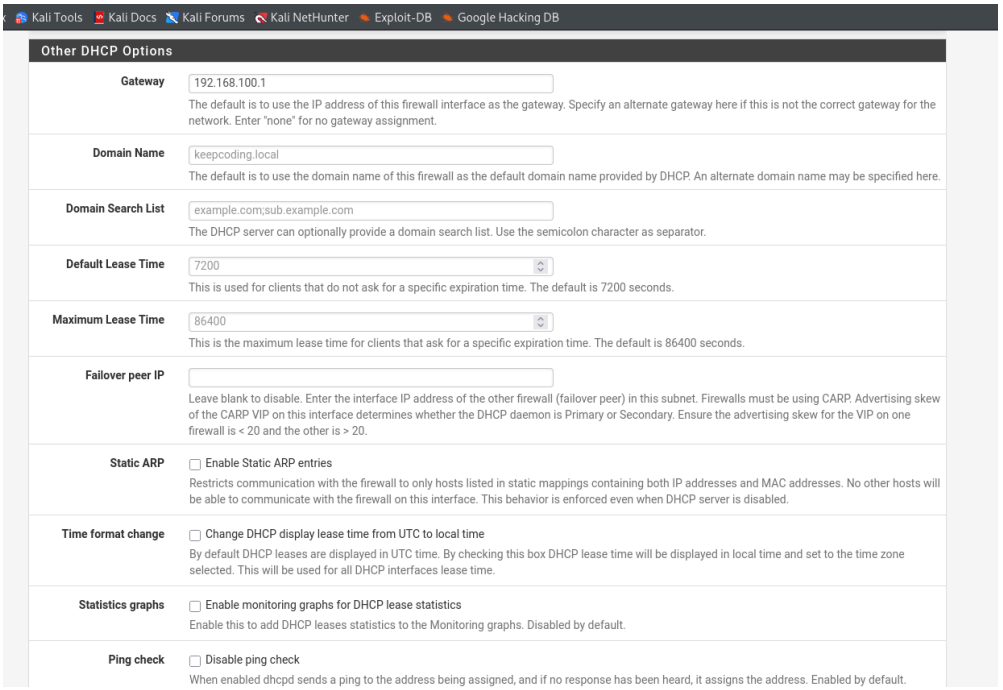
Una vez hecho esto, volvemos a entrar al PFSENSE desde el navegador, con la ip **192.168.100.1,** y ponemos el usuario (admin) con la nueva contraseña que pusimos anteriormente.

Una vez dentro en la parte superior vamos a **services > DNS Resolver**, aquí **deshabilitamos DNSSEC** y **habilitamos el DNS QUERY FORWARDING** hacemos clic en “SAVE” y después en “APPLY CHANGES”.

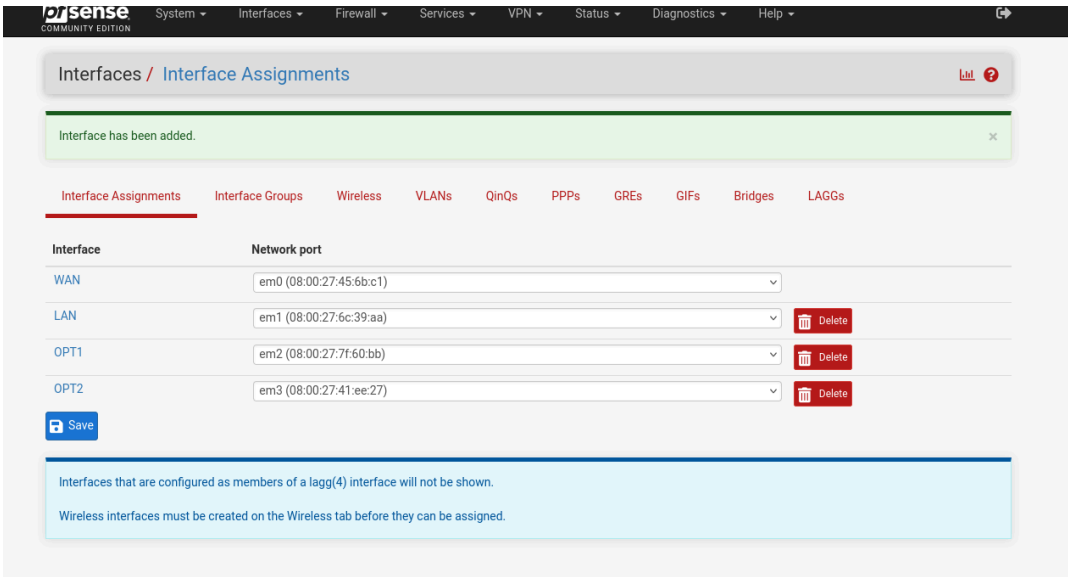
Después vamos a **services > DHCP Server** y cambiamos **primary address pool, DNS y Gateway** como aparecen en las siguientes imágenes y guardamos:



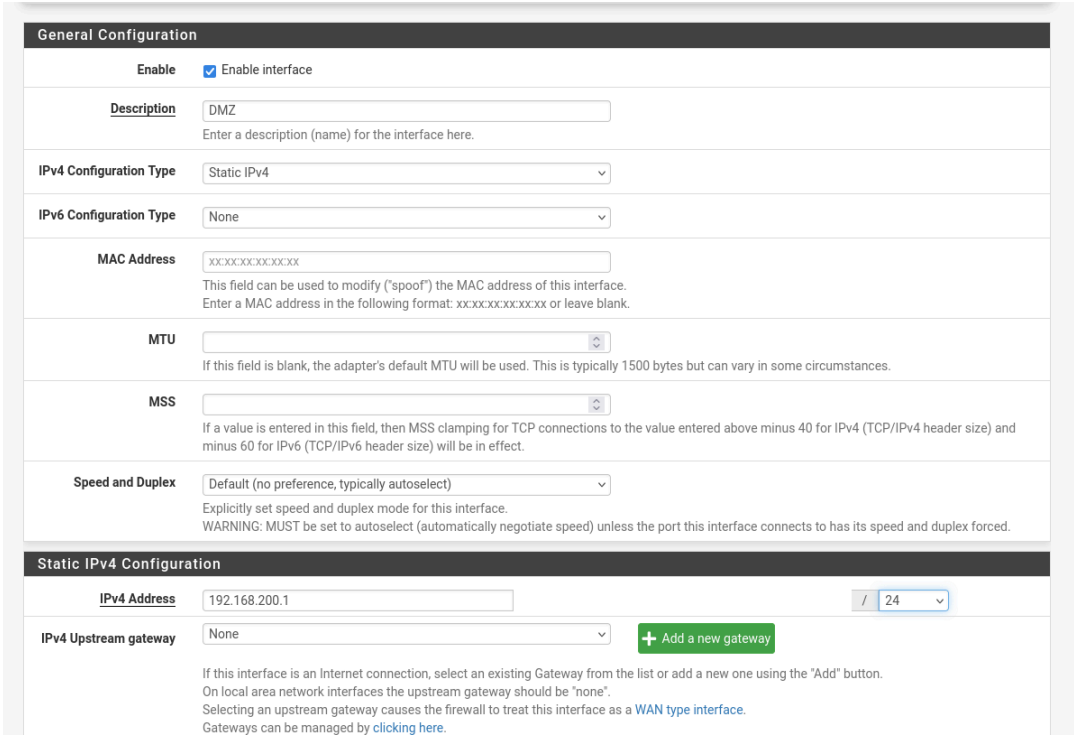




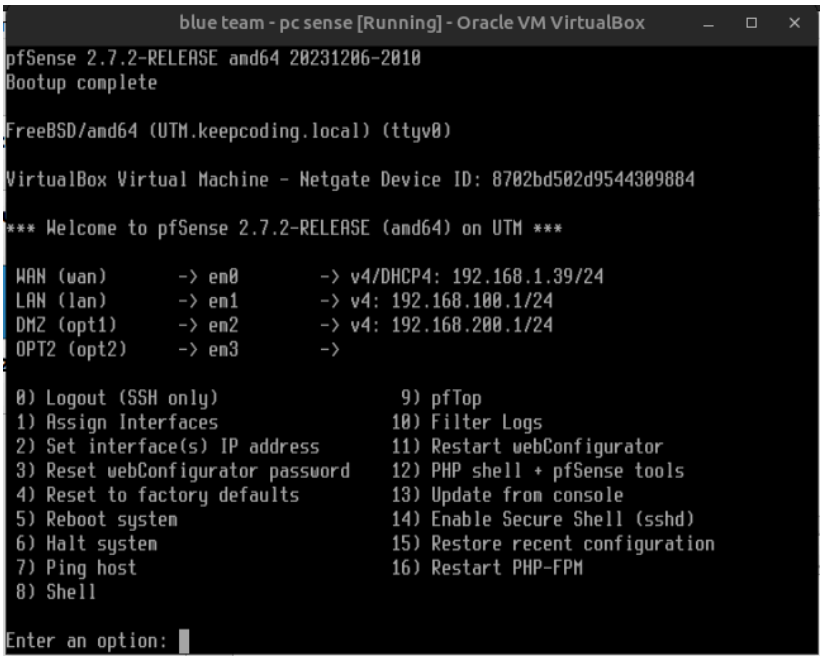
A continuación, vamos a **interfaces > assignments**, y vamos añadiendo hasta que quede como en la siguiente imagen y guardamos.



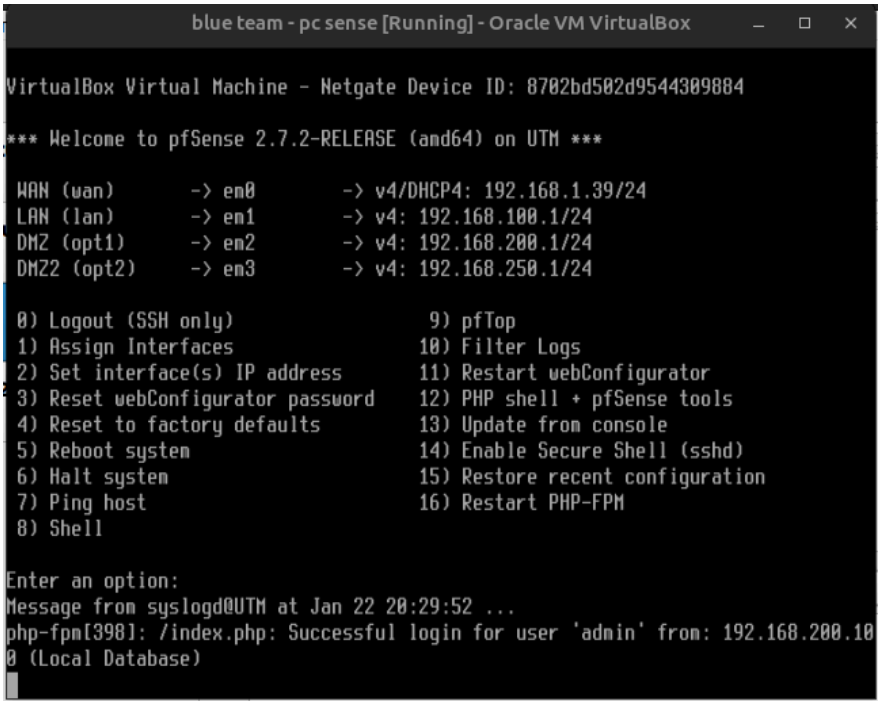
Ahora vamos a **interfaces > OPT1**, habilitamos la opción “Enable interface”, cambiamos la descripción a **DMZ**, ponemos la ipv4 en modo **estático**, ponemos la **nueva dirección IP** que aparece en el esquema de nuestra infraestructura (**192.168.200.1**) y cambiamos la **máscara de red** a “**/24**”, guardamos y aplicamos cambios.



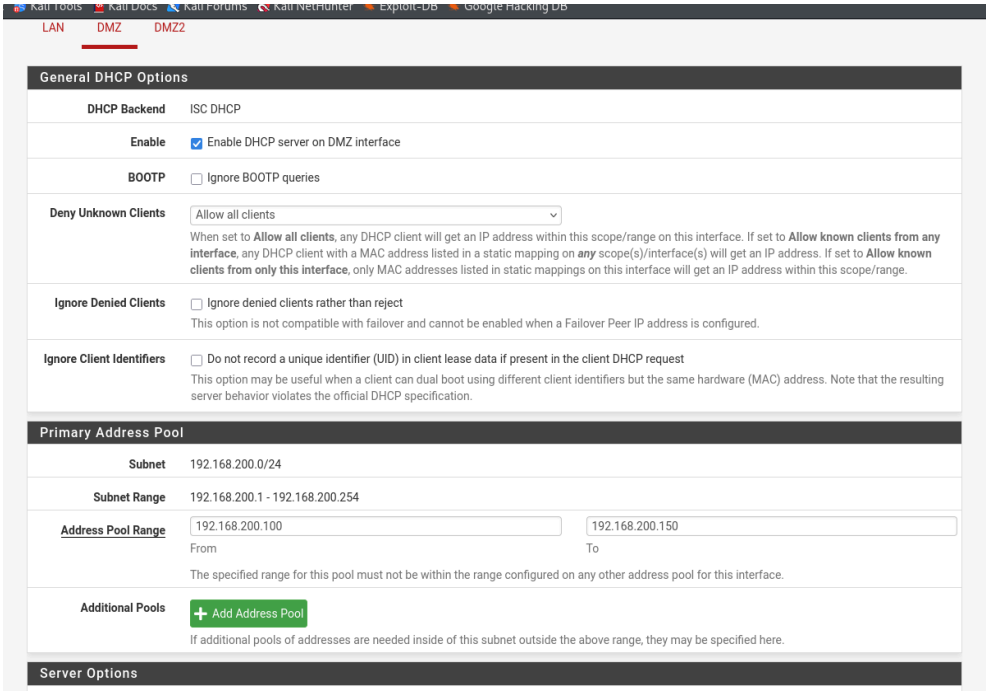
Si vamos a nuestro PFSENSE veremos que nos aparecen tres redes:

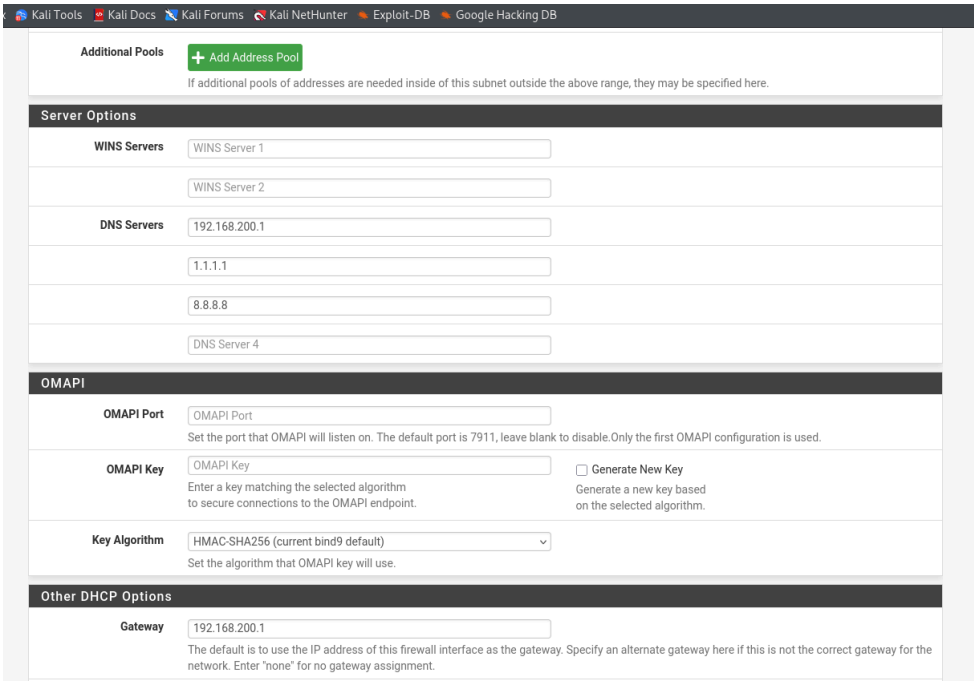


Ahora vamos a **interfaces > OPT2** y hacemos la misma operación, pero en la descripción ponemos **DMZ2** y la **dirección IP** será "**192.168.250.1**". Si volvemos al PFSENSE ya nos aparecerán las 4 redes con su respectiva IP y máscara de red:



A continuación, debemos ir a **Services > DHCP Server > DMZ**, habilitar la opción "**Enable DHCP server on DMZ interface**", definimos el **rango** 192.168.200.100 - 192.168.200.150, y ponemos los **DNS servers** con dirección IP (192.168.200.1), cloudflare (1.1.1.1) y google (8.8.8.8).



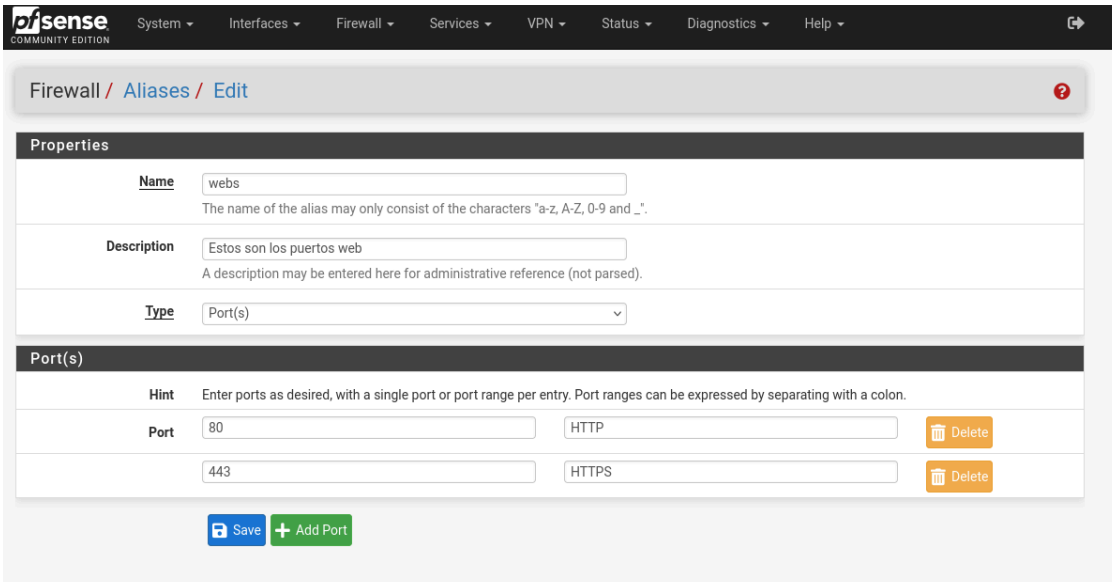


En **Services > DHCP Server > DMZ2** hacemos lo mismo pero con el **rango** 192.168.250.100 - 192.168.250.150.

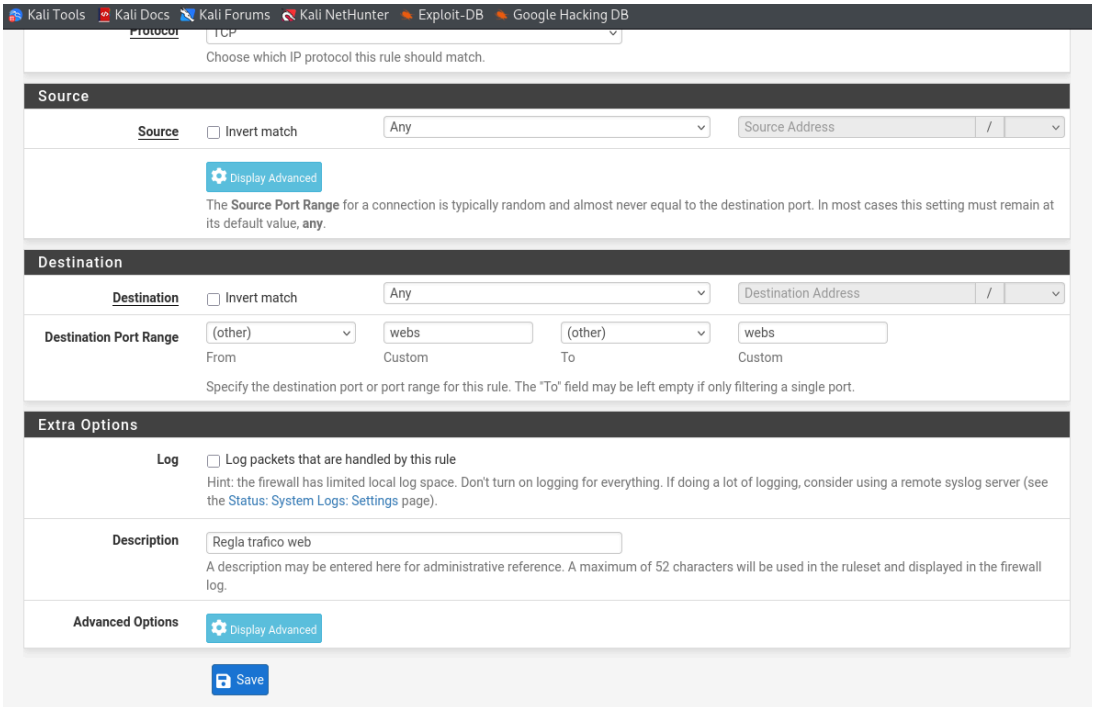
Si nos conectamos a las diferentes redes (machine > settings > network), por ejemplo la DMZ, y en la terminal ejecutamos “ip a”, veremos que tenemos la IP tal y como la definimos para el DMZ server y si abrimos el navegador veremos que no podemos acceder a páginas web ni tampoco al PFSENSE a través de la IP. Esto es debido a que PFSENSE por defecto cuando creamos distintas interfaces las reglas del firewall bloquean absolutamente todo el tráfico, excepto en este caso en la red LAN para poder conectarse a sí mismo al PFSENSE y hacer las configuraciones oportunas.

A continuación, vamos a crear las reglas del firewall para las redes DMZ y DMZ2 para que deje de ser tan restrictivo y nos deje pasar tráfico web ya que para estas dos redes ahora mismo no tenemos reglas que permitan que pase el tráfico lo que hace que el firewall rechace todo.

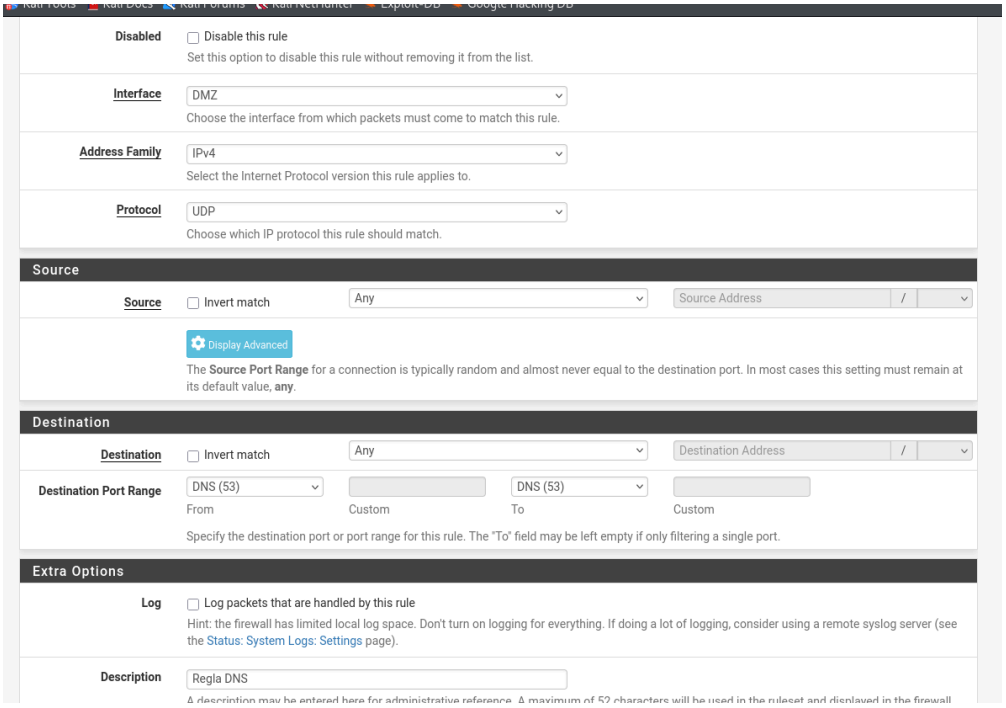
Accedemos a **Firewall > Aliases > Ports**, aquí vamos a permitir tráfico web y tráfico DNS, es decir, poder navegar, para ello usaremos los puertos 80 (HTTP) y 443 (HTTPS). Seleccionamos “ADD” y lo dejamos como en la siguiente imagen:



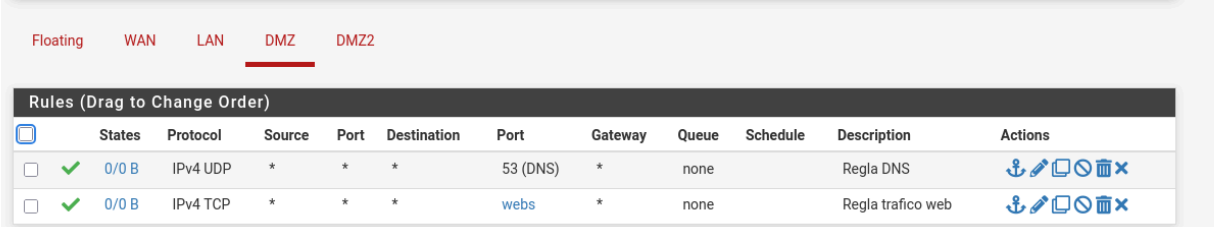
Ahora configuraremos las reglas del Firewall, para ello vamos a **Firewall > Rules > DMZ**, aquí le daremos al primer icono que pone “Add” para añadir la primera regla con protocolo TCP y dejaremos todo como en la siguiente imagen y guardamos.

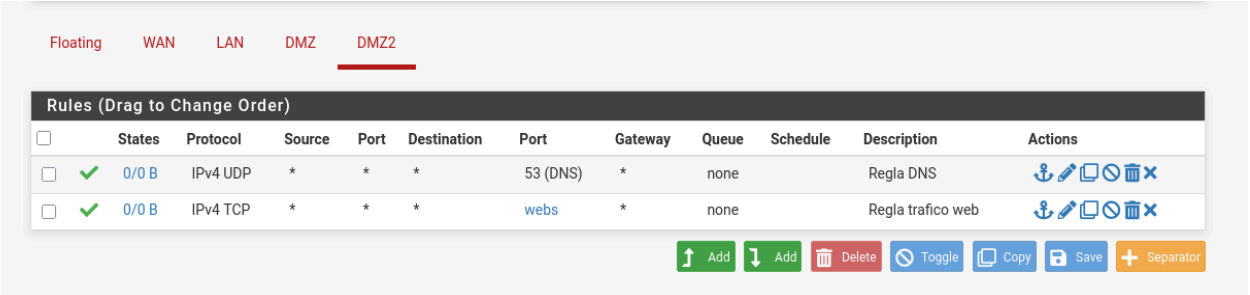


Después añadimos otra regla, la del DNS, que es con **UDP**, dejándolo de la siguiente forma:



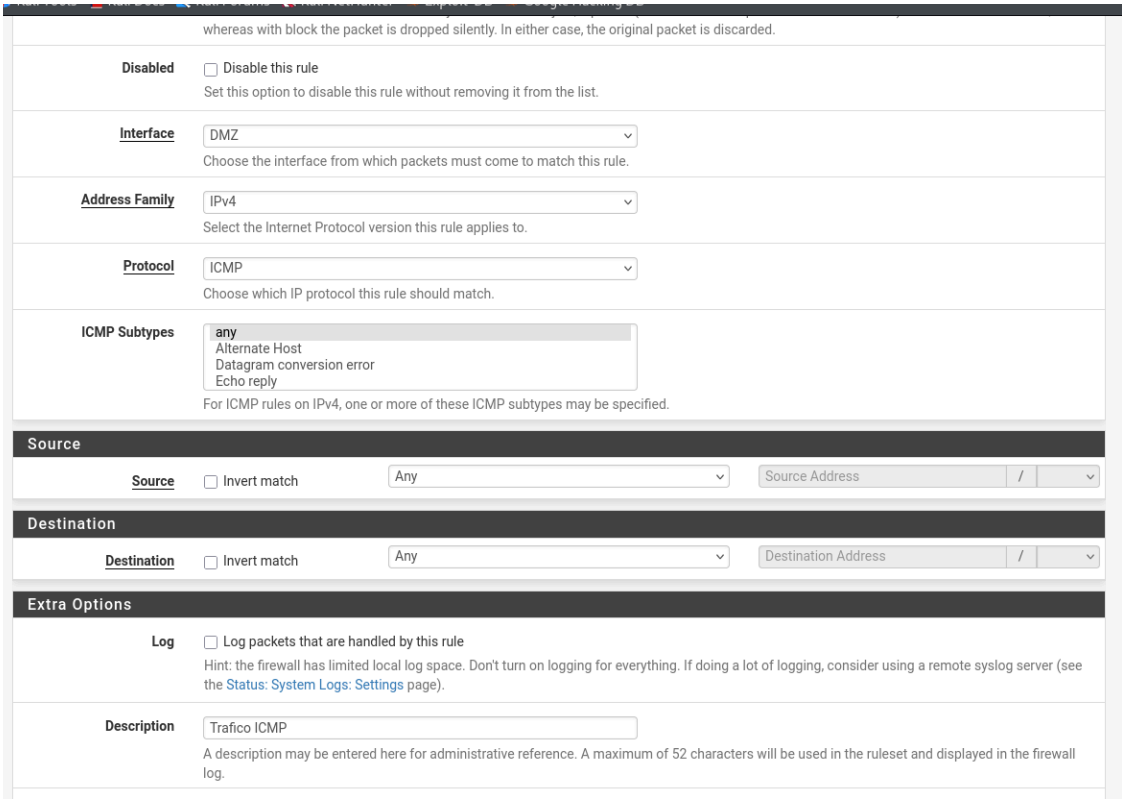
Una vez hecho esto accedemos a **Firewall > Rules > DMZ2** y hacemos exactamente lo mismo añadiendo estas dos reglas anteriores. Y después deberíamos tener las reglas del Firewall de DMZ y DMZ2 de la siguiente manera:



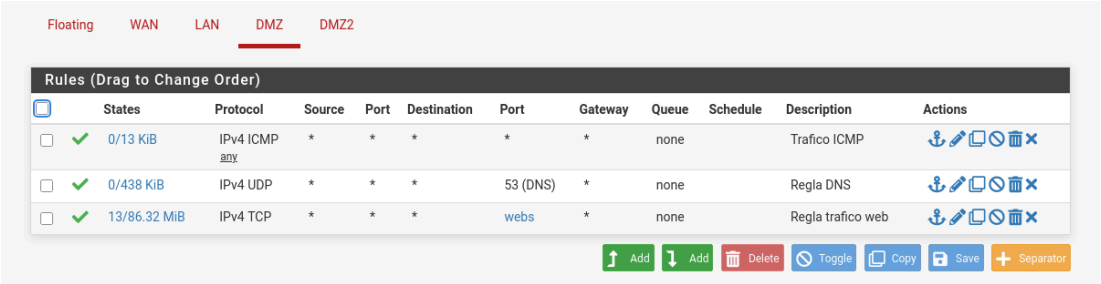


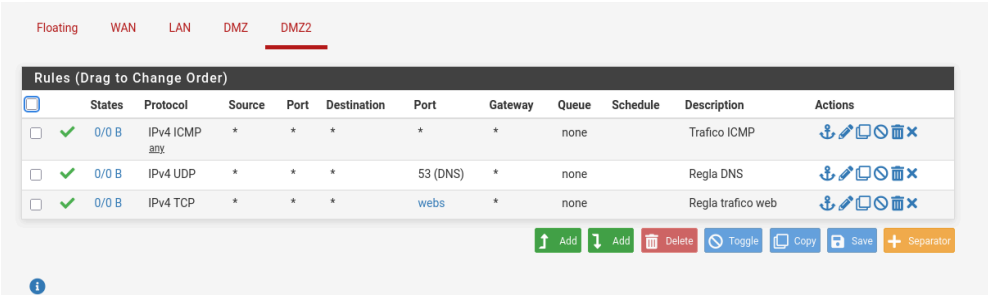
La diferencia entre los protocolos TCP y UDP es que el TCP cuando envía algo espera a que le digan que ha llegado, si no lo seguirá mandando, como por ejemplo cuando quieres entrar en el correo electrónico mientras que el UDP no realiza esta espera, se usa por ejemplo para retransmisiones en directo ya que solo queremos que nos vaya mandando información de manera rápida.

Ahora si intentamos acceder a una página web veremos que ya es posible pero si en nuestra terminal hacemos “ping” a esa misma página (por ejemplo marca.com), veremos que no obtenemos respuesta esto es debido a que nos falta una regla, el http y https van por TCP, el DNS va por UDP y el ping va por ICMP, por lo cual debemos crear una nueva regla, iremos a **Firewall > Rules > DMZ** y añadiremos una regla con protocolo ICMP con los siguientes parámetros, una vez añadida haremos lo mismo para la **red DMZ2**:

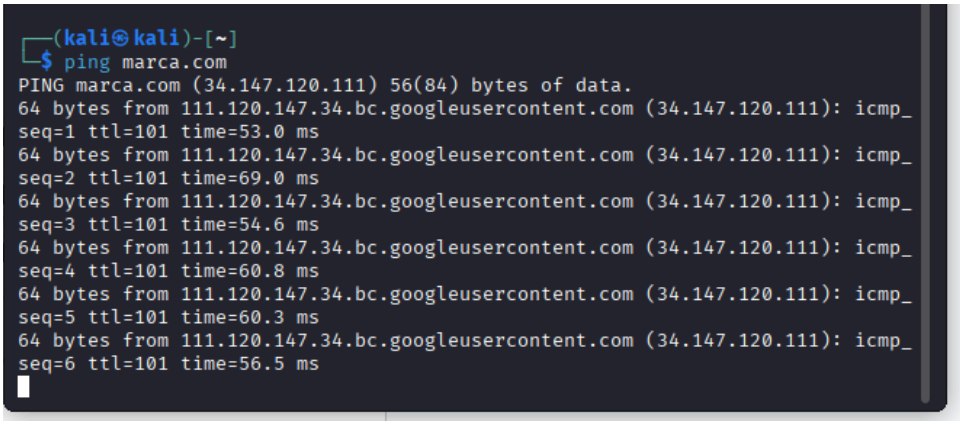


De esta manera las reglas quedarian asi en este momento:

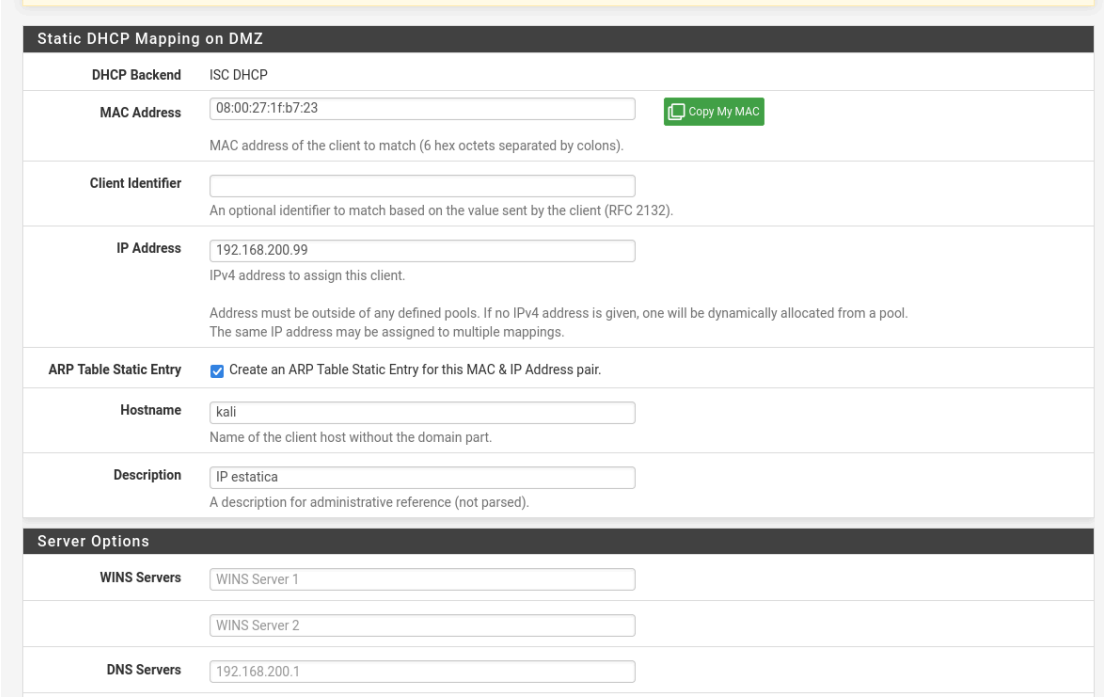




Si hacemos ping veremos que ahora funciona:

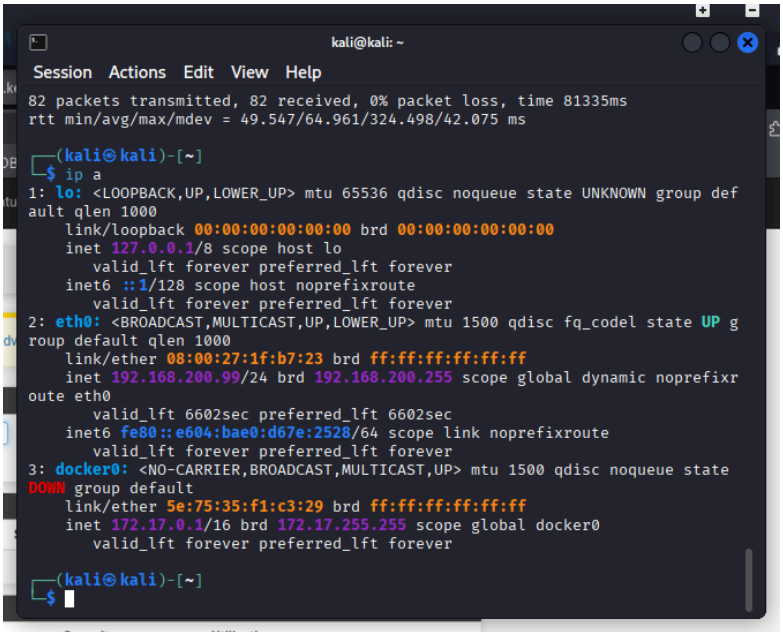


A continuación levantaremos un servidor **apache** para conectarnos a él, con una **dirección ip fija**, para eso la máquina que conectamos a la red LAN tendrá una IP fija. Para ello debemos ir a **Status > DHCP Leases** y en el apartado de Leases, vamos a actions y le damos al primer recuadro con un **+ (add static mapping)**, y aquí lo configuramos de la siguiente manera:

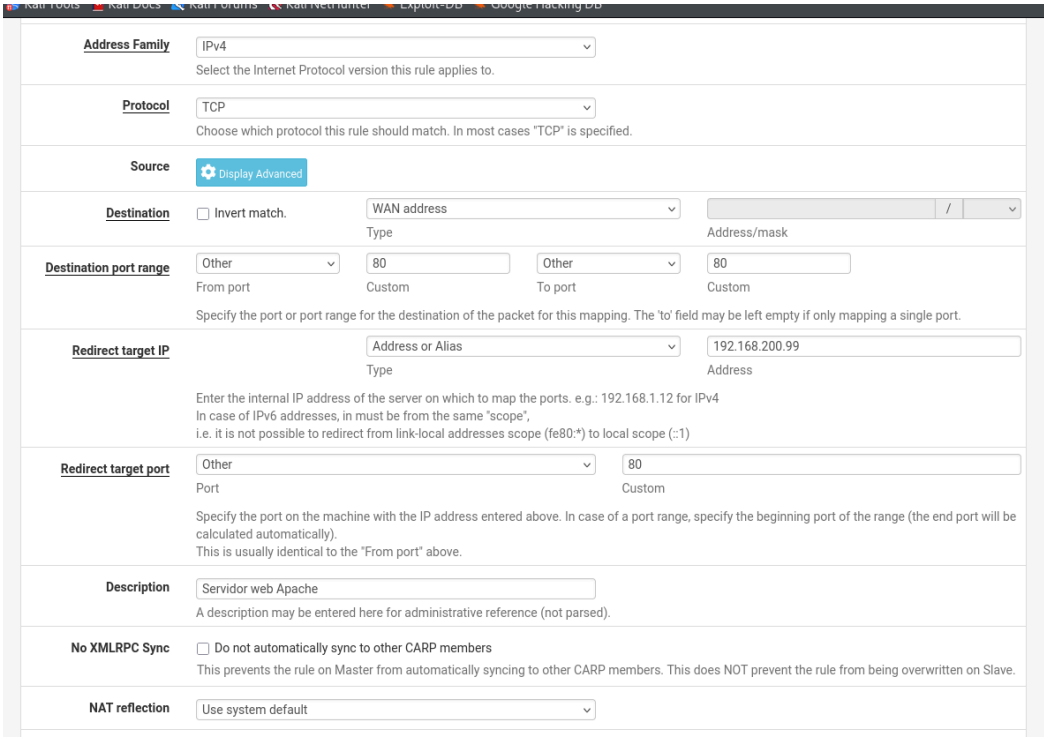


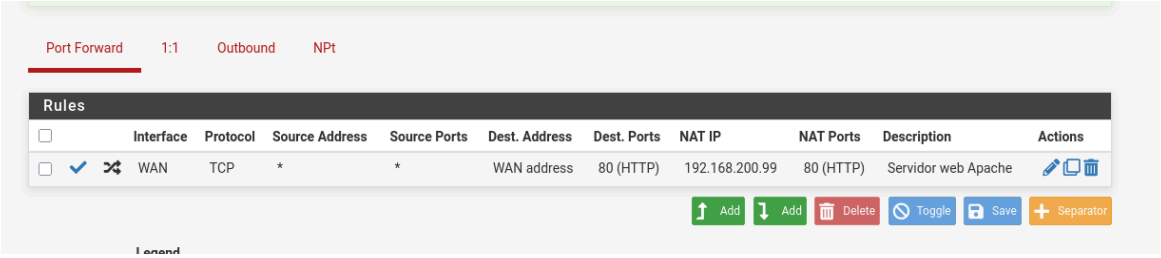
Nosotros anteriormente le asignamos una IP dinámica a la red DMZ entre los rangos 192.168.200.100 - 192.168.200.150, por lo cual si ahora queremos asignar una IP fija no podemos hacerlo dentro de este rango ya que crearíamos un conflicto, por lo cual escogemos una IP fuera de este rango que en este caso es 192.168.200.99, y gracias a la dirección MAC de nuestra Kali (MAC Address) lo que hará el servidor es que cuando nos conectemos con nuestra máquina nos asigna esa IP fija, y si se conecta otro dispositivo le

asignará una IP dentro del rango dinámico. Podemos comprobar que nos da esta IP fija haciendo “ip a” en la terminal:



Ahora vamos a **Firewall > Nat > Port Forward**, añadimos y ponemos los siguientes parámetros:





Con esto lo que le estamos haciendo es que todo lo que entre a la red WAN desde el puerto 80 nos lo mande a la red DMZ.

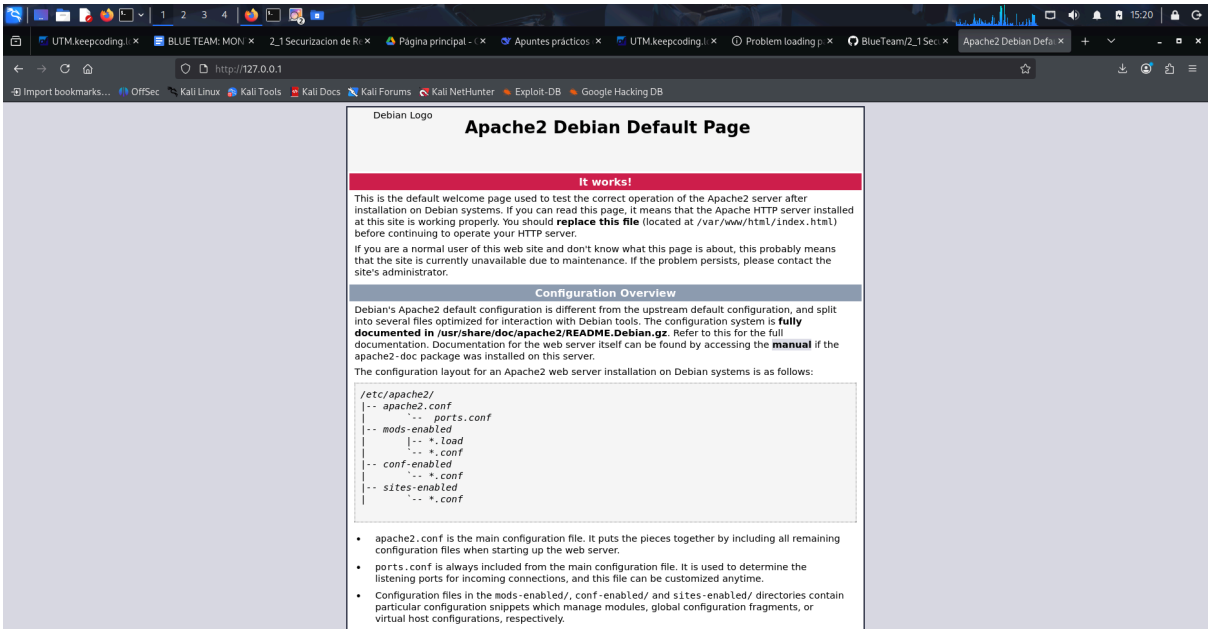
Ahora, nos vamos a la terminal y arrancamos un servidor apache con el comando (nos pedirá la contraseña de la kali):

- service apache2 start

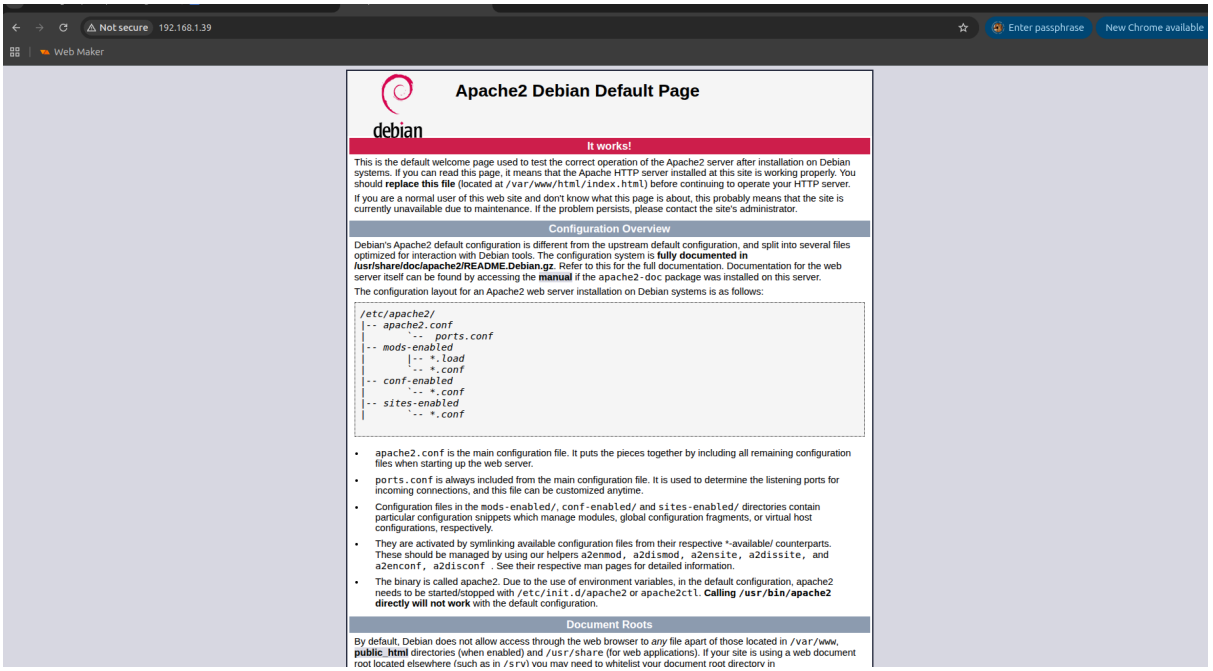
Comprobamos que ha funcionado con el comando:

- service apache2 status

Si vamos a la IP del localhost (127.0.0.1) veremos la default page de apache2:

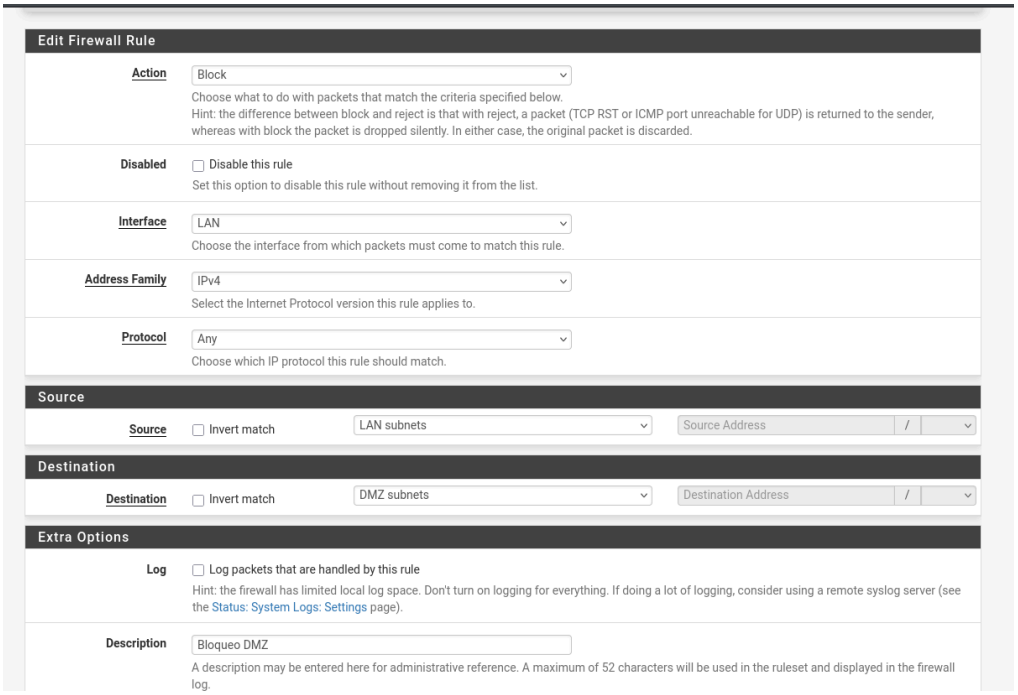


Si vamos al navegador de la máquina física y ponemos la **IP de nuestra WAN** deberíamos ver la página, y si usamos otro dispositivo y ponemos esta IP deberíamos ver esta misma pagina tambien:

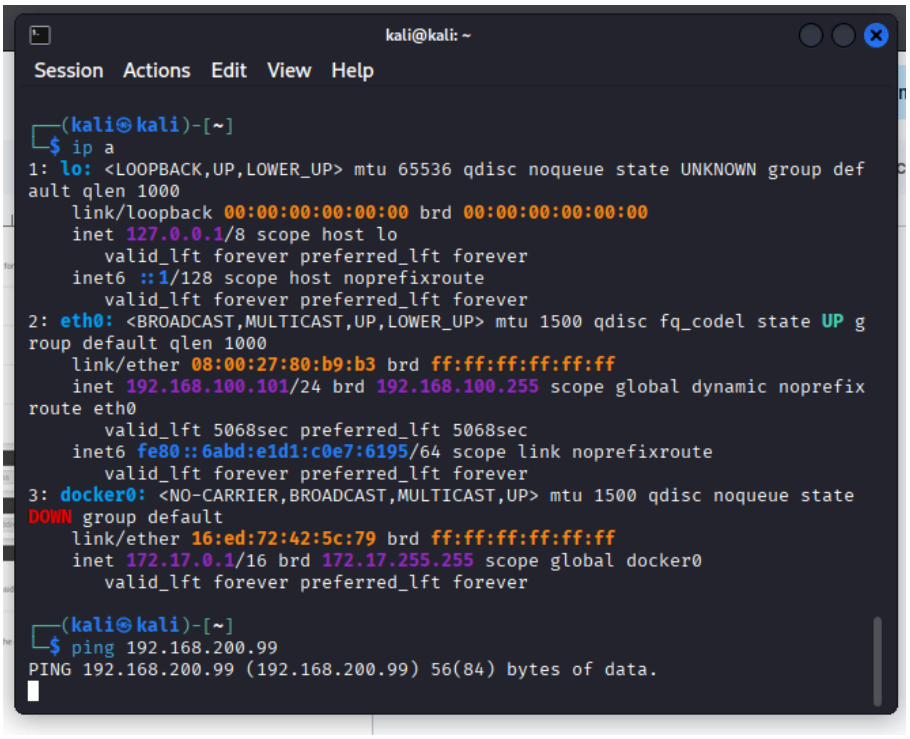


Bien, ahora debemos configurar las redes de tal manera que desde la red DMZ no se tenga acceso a la LAN ni a la red DMZ2 y viceversa, para lo cual debemos añadir reglas de firewall. Lo haremos de la siguiente manera:

1. **Añadimos una regla para bloquear el tráfico desde la LAN a la DMZ en FIrewall > Rules > LAN**. Para ello, la action debe ser “block”, el protocolo debe ser ICMP o Any en este caso el origen (source) son las subnets de la NAT es decir las IP que están dentro de la LAN (192.168.100.1), y el destino son las DMZ subnets.

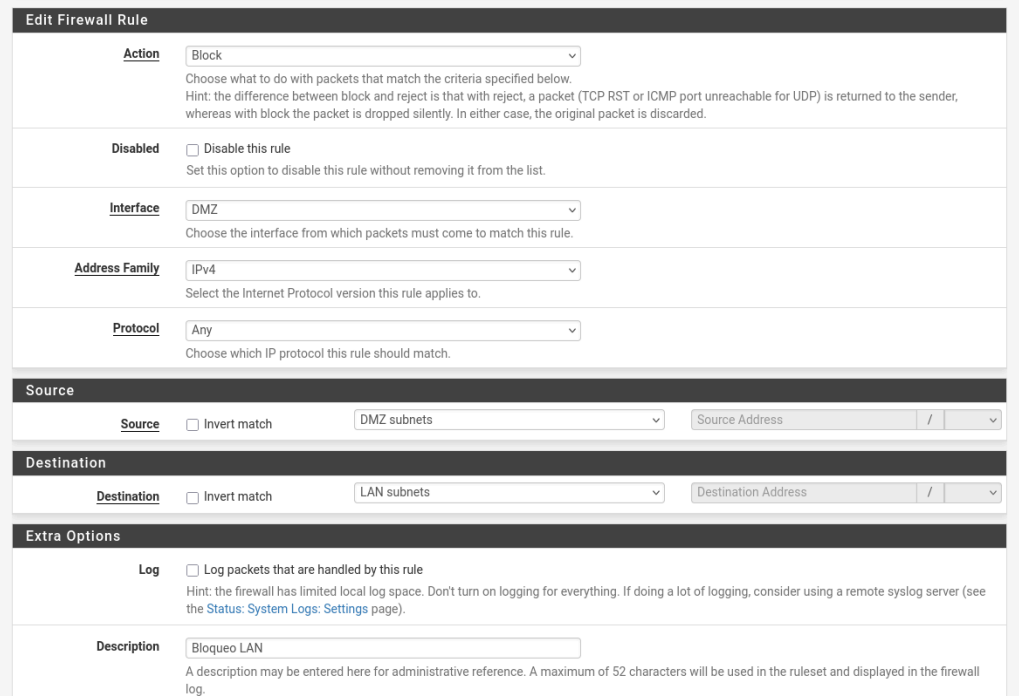


Si hacemos ping desde una máquina conectada a la red LAN a la dirección IP de la red DMZ (192.168.200.99) veremos que no llega o que no obtenemos respuesta:

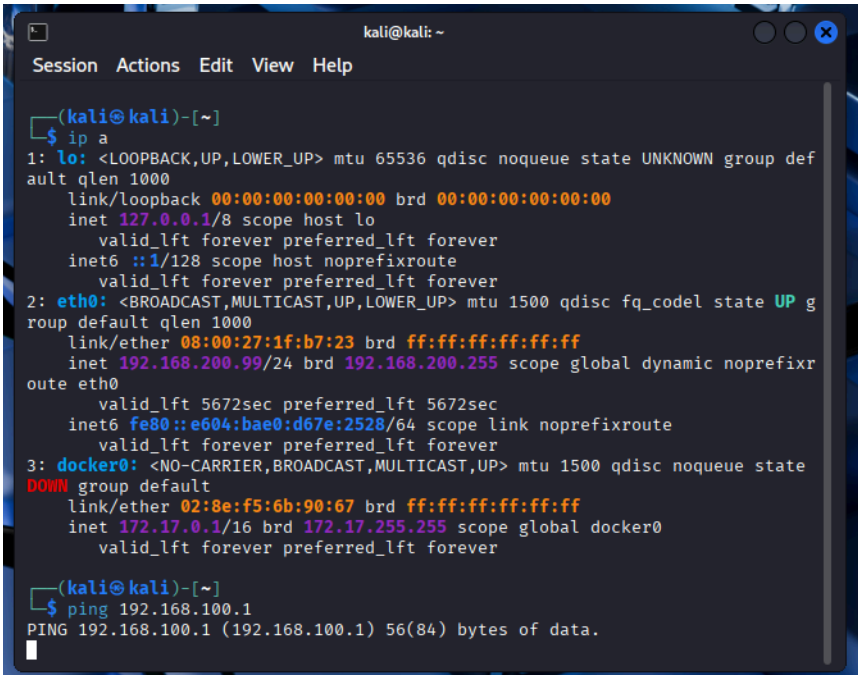


En mi caso para obtener otra máquina he clonado la Kali que ya tenía instalada.

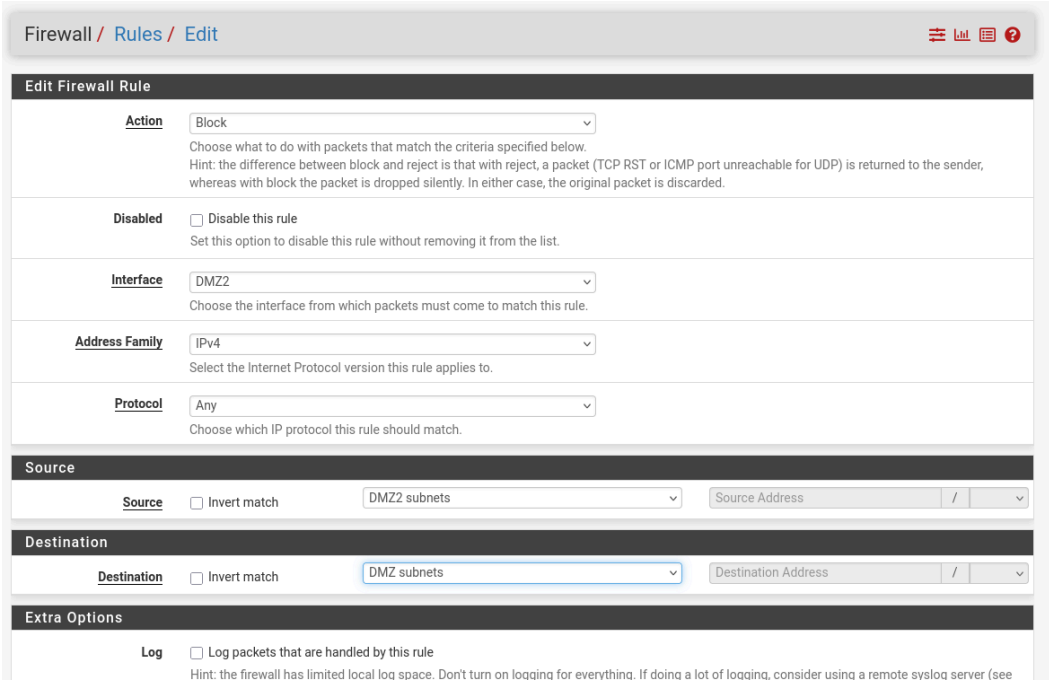
2. **Añadimos una regla para bloquear el tráfico desde la DMZ a la LAN en Firewall > Rules > DMZ.** Para ello haremos lo mismo que antes, pero el origen será DMZ Subnets y el destino LAN Subnets.



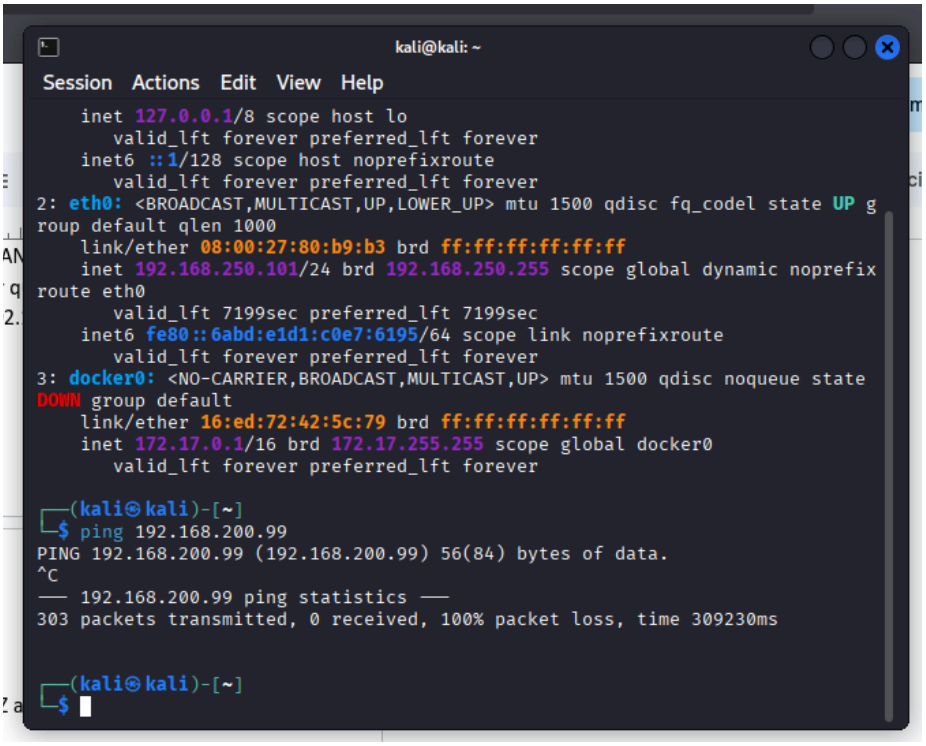
Repetimos el proceso de hacer ping pero esta vez desde la máquina DMZ, haremos ping a la IP de la LAN (192.168.100.1) y veremos que no obtenemos respuesta.



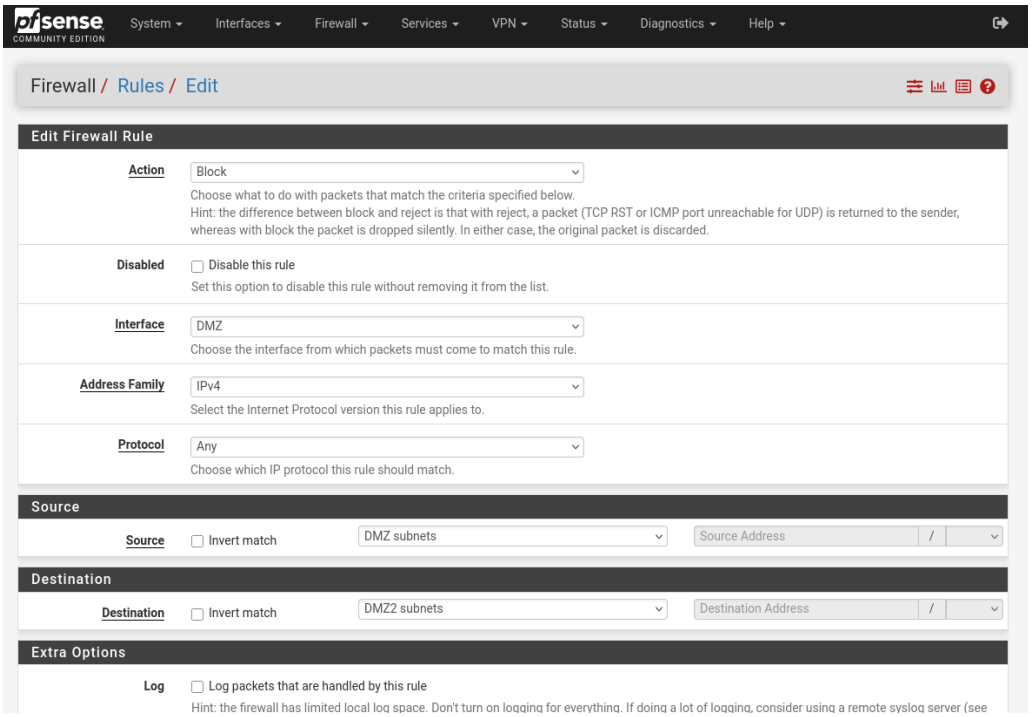
3. **Añadimos una regla para bloquear el tráfico desde la DMZ2 a la DMZ para ello iremos a Firewall > Rules > DMZ2**. Ponemos los mismos parámetros que antes, con origen DMZ2 Subnets y destino DMZ Subnets.



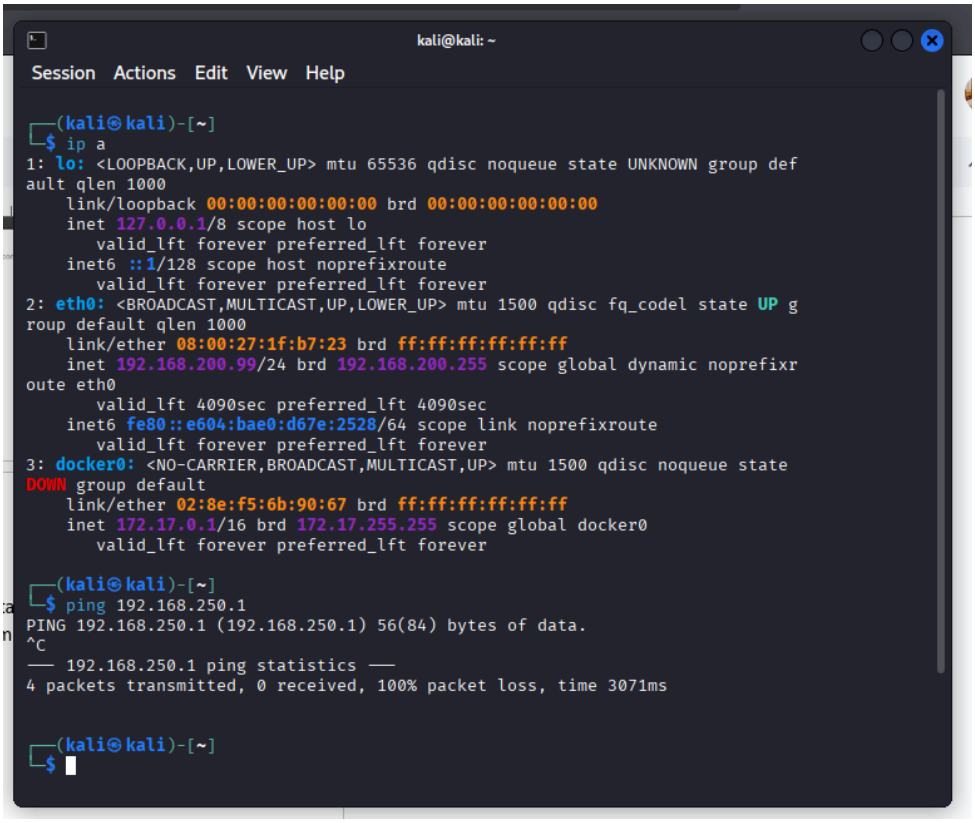
Ahora, la máquina Kali que teníamos conectada a la red LAN, debemos conectarla a la red DMZ2, hacemos ip a en la terminal para comprobar que estamos conectados a la IP de DMZ2 y despues hacemos ping a la IP de DMZ (192.168.200.99), veremos que no obtenemos respuesta.



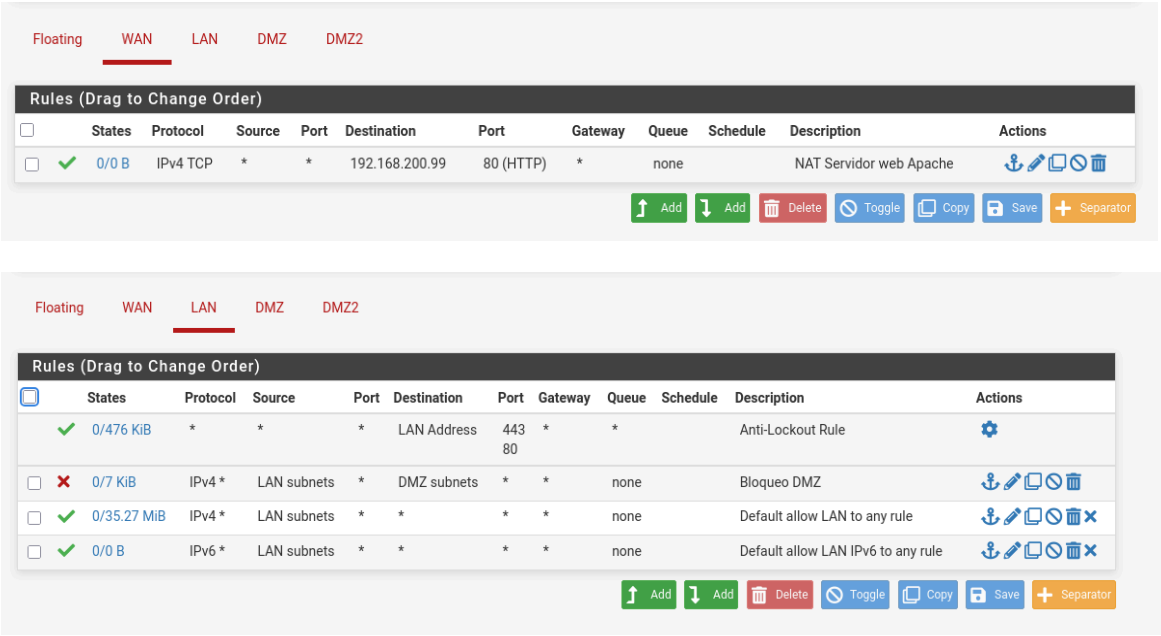
4. **Añadimos una regla para bloquear el tráfico desde la DMZ a la DMZ2, nos iremos a Firewall > Rules > DMZ**. Como anteriormente, mismos parámetros con origen DMZ Subnets y destino DMZ2 Subnets.

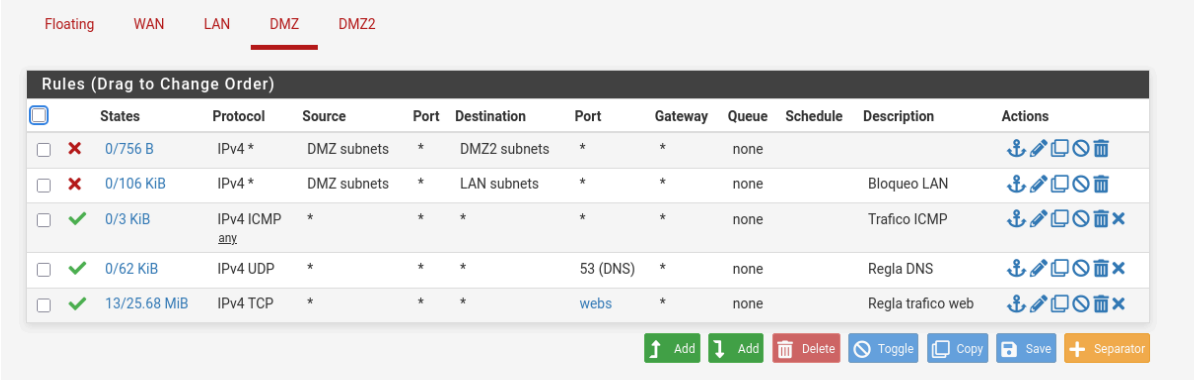


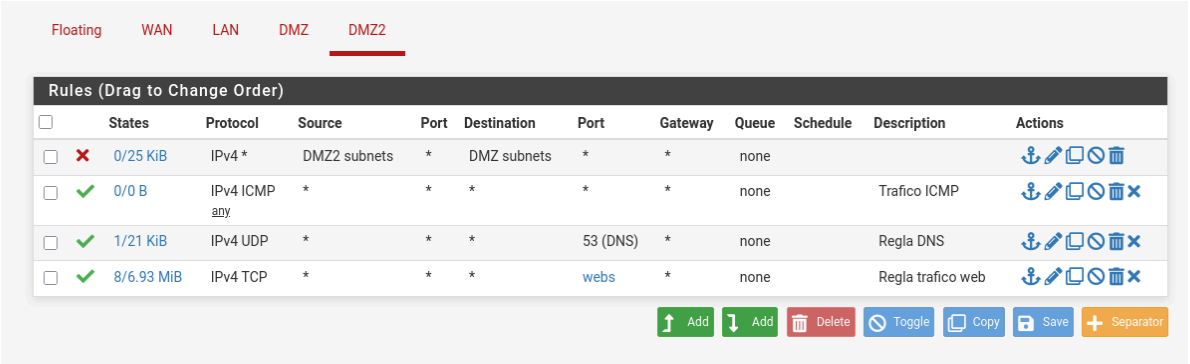
Ahora si vamos a la terminal de la Kali que tenemos conectada a la red DMZ y hacemos ping a la IP de la red DMZ2 (192.168.250.1) veremos que no obtenemos respuesta.



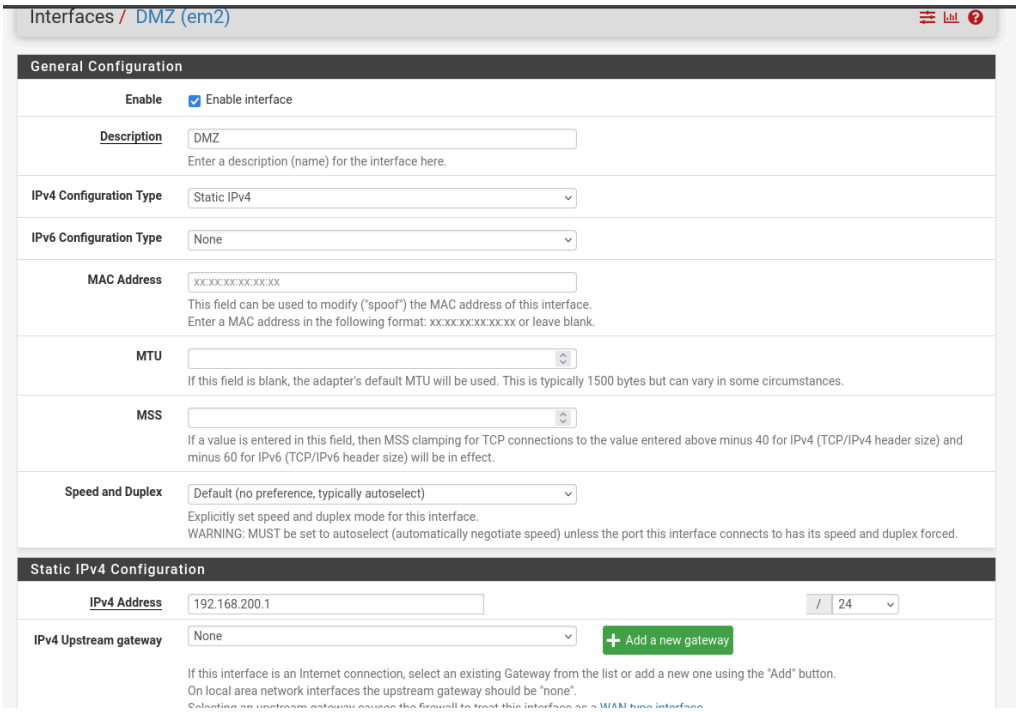
Actualizamos como deberían estar las **reglas del Firewall** en WAN, LAN, DMZ y DMZ2:







A continuación, vamos a **Interfaces > OPT1** y cambiamos los siguientes parámetros:



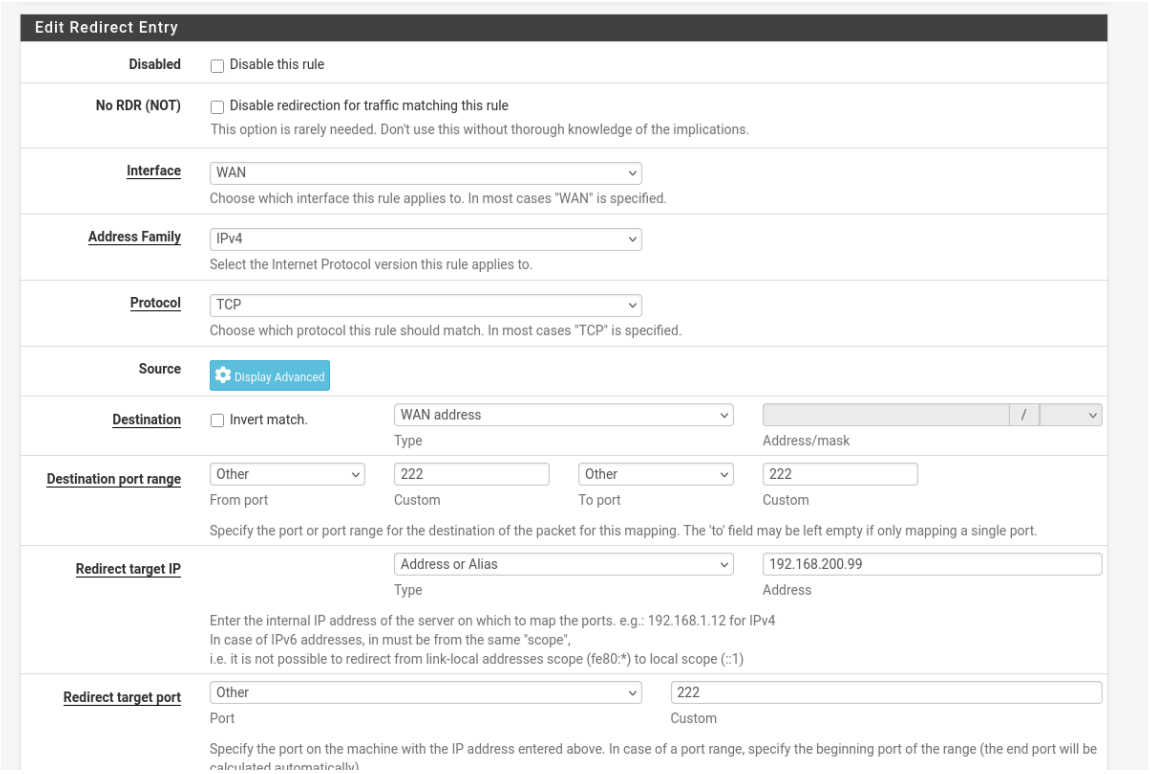
Vamos a instalar ahora en la máquina Kali conectada a la DMZ el honeypot, para ello abrimos la terminal y lo primero que debemos hacer es **instalar docker** con los comandos:

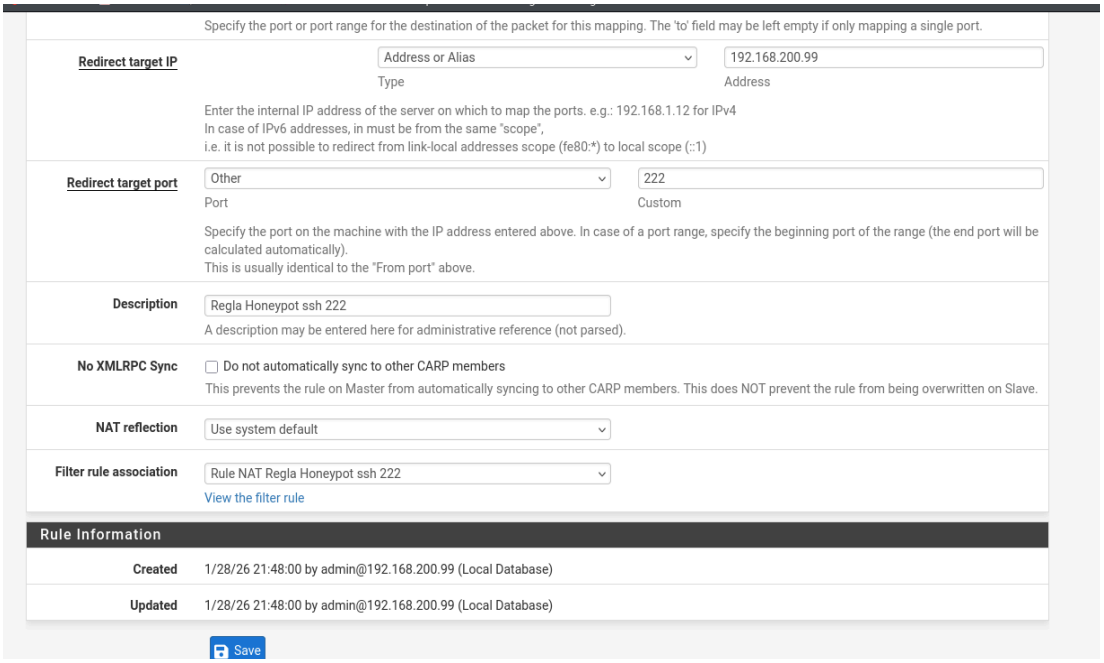
- **sudo apt update**
- **sudo apt install -y docker.io**

Ahora ejecutaremos el **honeypot de cowrie** que simulara un servicio de **SSH** con el comando:

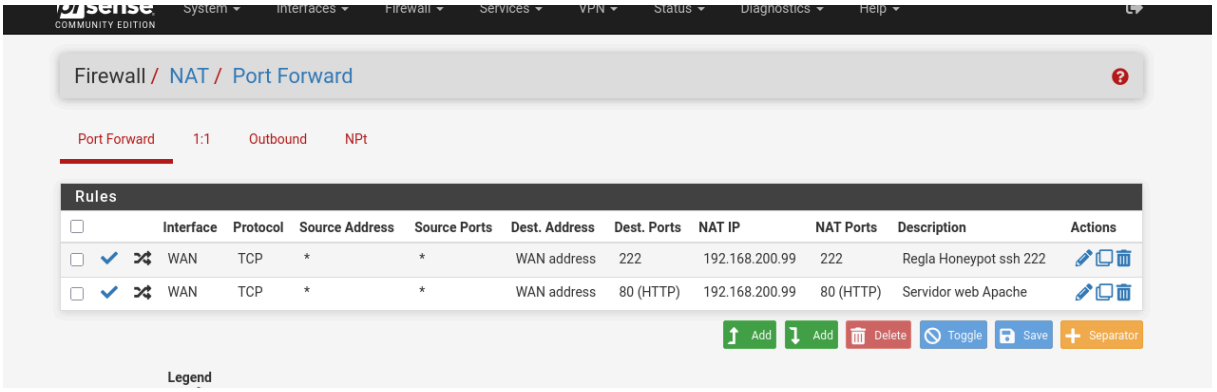
- **sudo docker run -p 222:2222 cowrie/cowrie**

Debemos configurar una regla en **Firewall > NAT > Port Forward,** que nos permitirá conectarnos desde ssh, puerto 222, al honeypot, básicamente con esta regla, al conectarte a la ip de la WAN, nos redirige al honeypot:

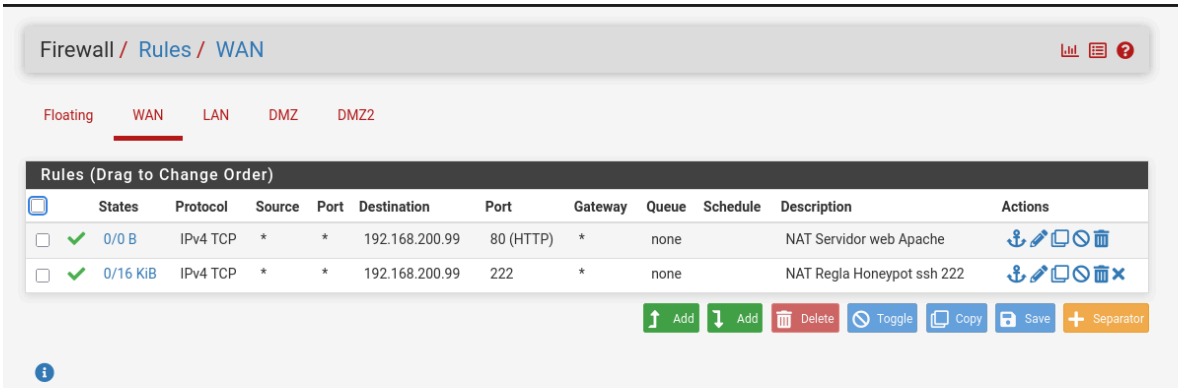




Así nos quedaría finalmente:



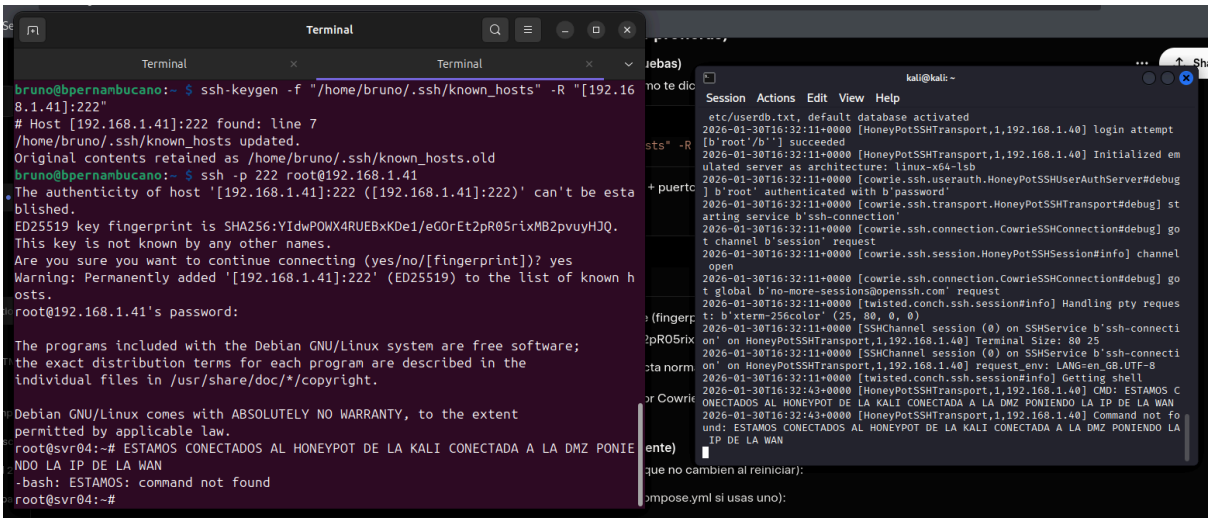
Ahora debemos configurar una regla en **Firewall > Rules > WAN**, que salvo sorpresa, al hacer la regla del port forwarding anteriormente ya estaría creada y quedaria asi:



Para comprobar que funciona, iremos a la **terminal de nuestra máquina física**, y a través de este comando nos conectaremos mediante ssh:

- **ssh -p 222 root@(dirección WAN)**

Si ejecutamos distintos comandos en la máquina física podremos ver los **logs** en la máquina virtual.



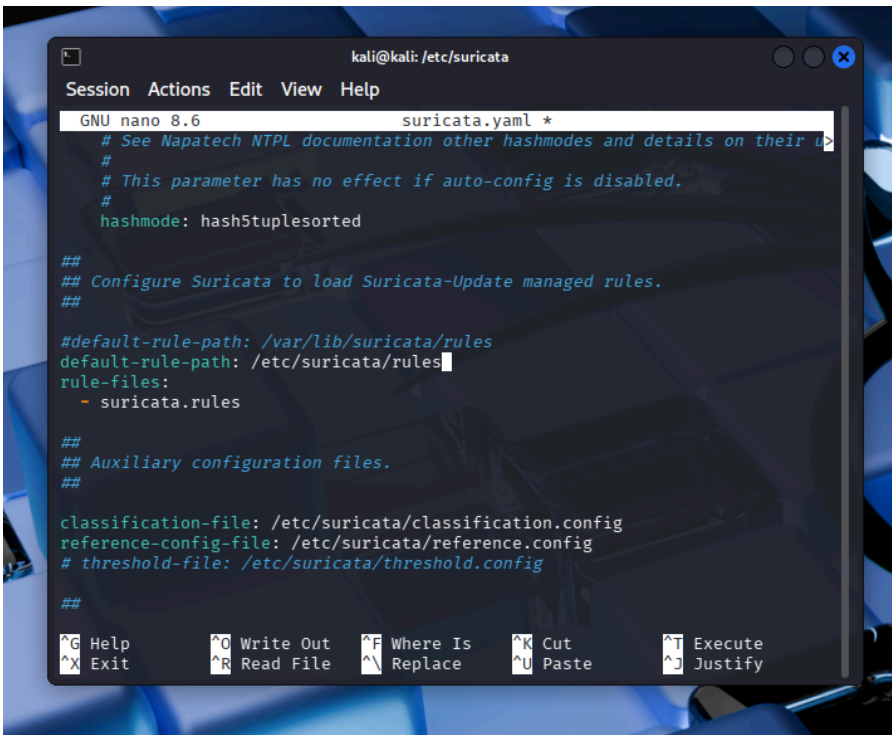
A continuación, nos cambiaremos a otra máquina Kali, conectada a la red **DMZ2** para instalar **suricata**, para ello ejecutaremos los comandos:

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

Matamos el anterior comando y hacemos un ‘’cd /etc/suricata’’ y aquí entramos a la carpeta rules (cd rules) y creamos un archivo que se llame **suricata.rules** (sudo touch suricata.rules). Después lo abrimos para editarlo (sudo nano suricata.rules) y escribimos la siguiente línea:

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

Ahora retrocedemos a la carpeta de suricata (cd ..) y modificaremos el archivo **suricata.yaml** para que quede de la siguiente manera, comentando el default rule path que viene por defecto y poniendo el nuestro con la regla que acabamos de crear:



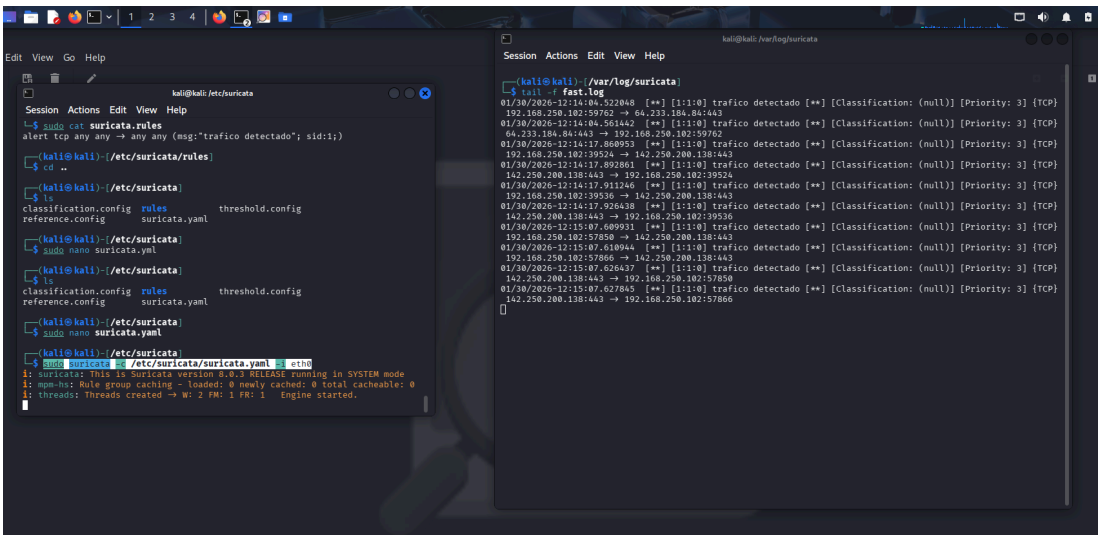
Ahora ejecutamos otra vez este comando en la terminal:

- **sudo suricata -c /etc/suricata/suricata.yaml -i eth0**

Y en otra terminal ejecutamos este otro comando (estando en la ruta var/log/suricata):

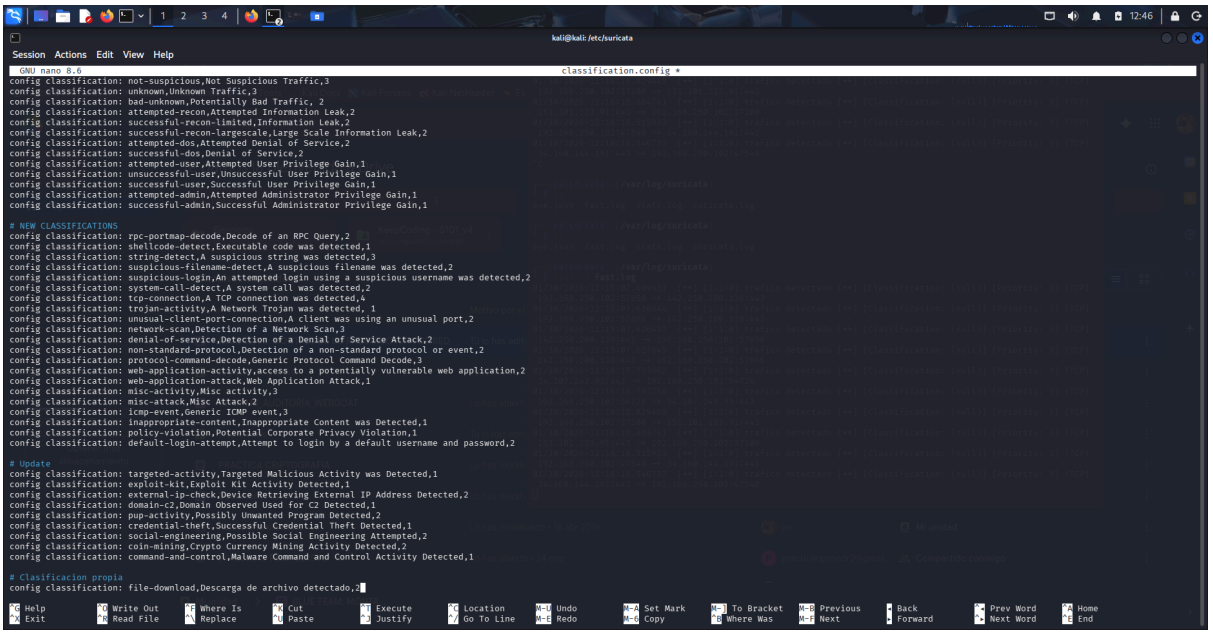
- **tail -f fast.log**

Podremos ver los **logs** que estamos generando en la terminal, en los cuales aparecerá entre otras cosas la frase ‘’tráfico detectado’’.

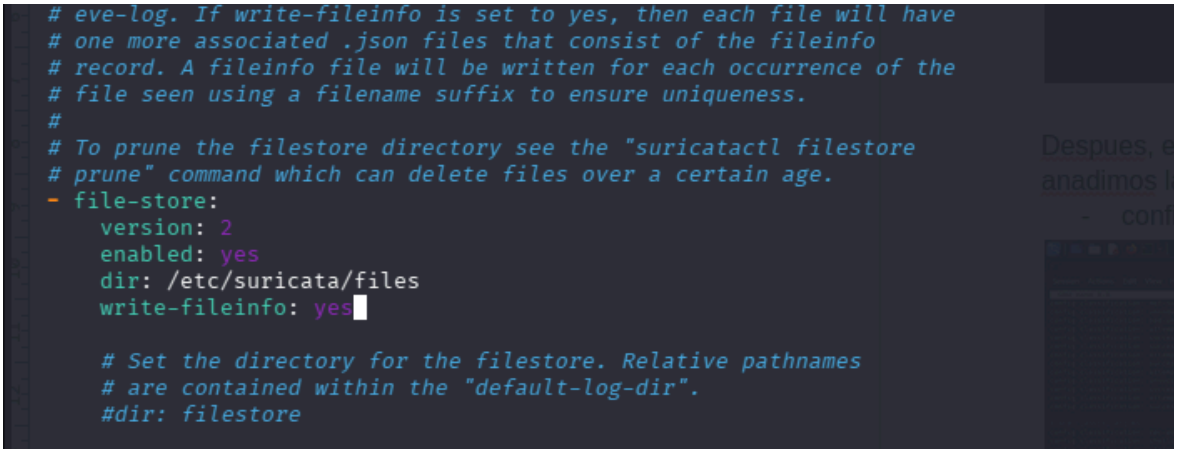


Después, en la ruta etc/suricata, modificamos el archivo **classification.config**, y añadimos la siguiente línea al final:

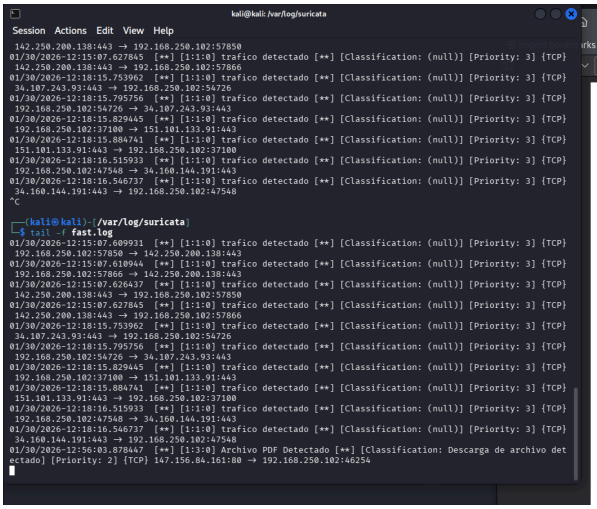
- **config classification: file-download,Descarga de archivo detectado,2**

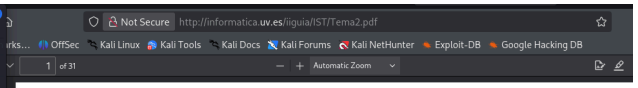


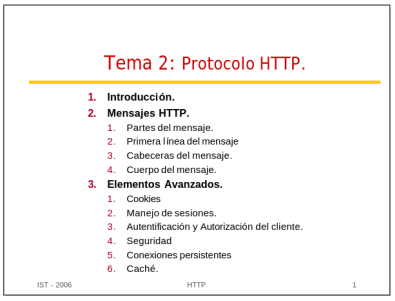
Después modificamos en la misma ruta el archivo **suricata.yaml** para que quede así:

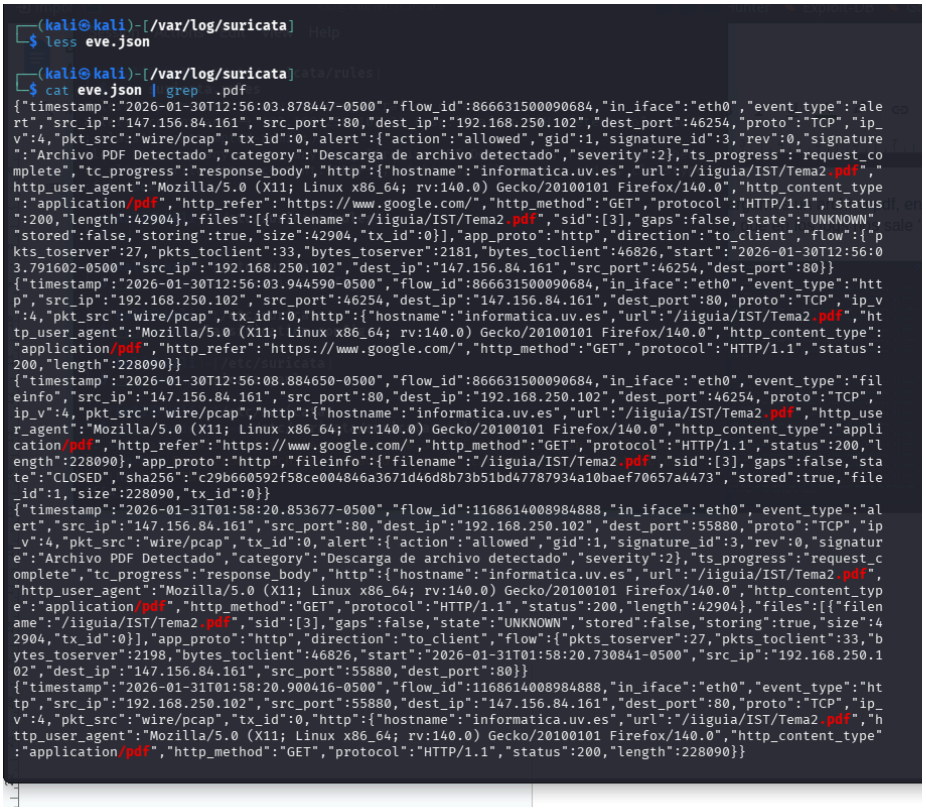


Ahora si descargamos un archivo pdf, en una página con **http** (no vale https),veremos que en los logs nos sale ‘’archivo pdf detectado’’.







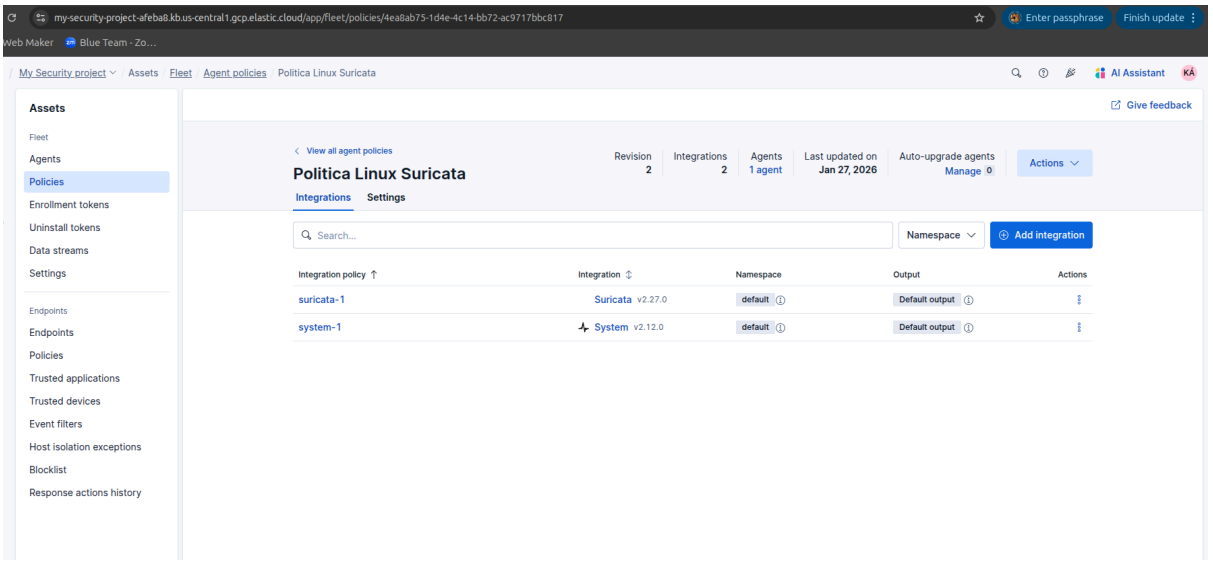


A continuación, necesitamos crear una cuenta en **Elastic**, por lo que iremos a la página de elastic en nuestro navegador de la maquina fisica (https://www.elastic.co/es) y accedemos a ‘’**hacer una prueba gratis**’’, usamos una cuenta de correo y completamos el registro. Cuando lleguemos a la parte que nos dice ‘’Which use can you looking to try first?’’ escogemos la que dice **‘’Elastic for Security’’ > SIEM and Security Analytics > No > Elastic Cloud Serverless > Launch**.

Ahora, en el menú de la izquierda, vamos a **More > Assets > Policies**, aquí se configuraran las políticas para crear los logs en elastic. Empezaremos creando la primera en **“Create agent policy” > Name: Politica Linux Suricata > Create agent policy.**

Si entramos a esta política, veremos que están puestos los logs del sistema por defecto, pero la idea es que se recojan los logs de suricata por lo que le daremos a la opción **“Add integration” > Integration: Suricata > Add integration**.

Bien, en este punto tenemos definidas las reglas que van a seguir todas las máquinas que estén definidas dentro del grupo de política linux suricata, ahora lo que falta es meter la máquina, para lo cual, le daremos a la opción **‘’Add agent’’**, nos aparecerá más abajo un cuadro de texto con un comando, en este cuadro veremos en la parte superior izquierda un menú desplegable, escogemos **linux 86_64**, copiamos el comando y lo pegamos en la máquina kali donde tenemos suricata y comenzamos una **instalación**, si volvemos a elastic y esperamos un poco veremos que se ponen en verde las opciones de “Agent enrolled confirmed” y “Incoming data confirmed”.

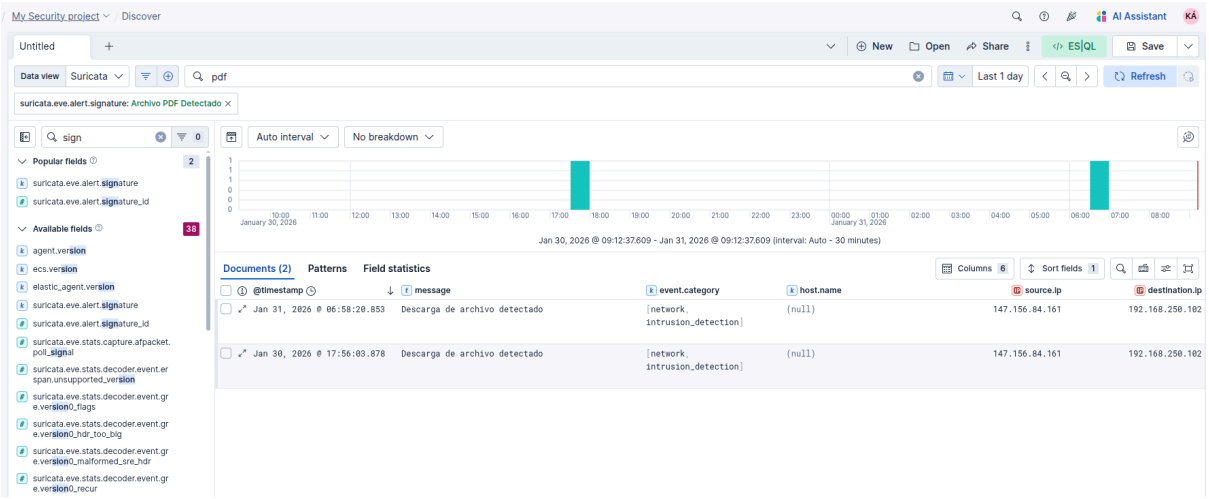


Ahora en el menú de la izquierda vamos a “Discover”, en la parte superior izquierda en “data view”, abrimos el menú desplegable y seleccionamos “create data view”:

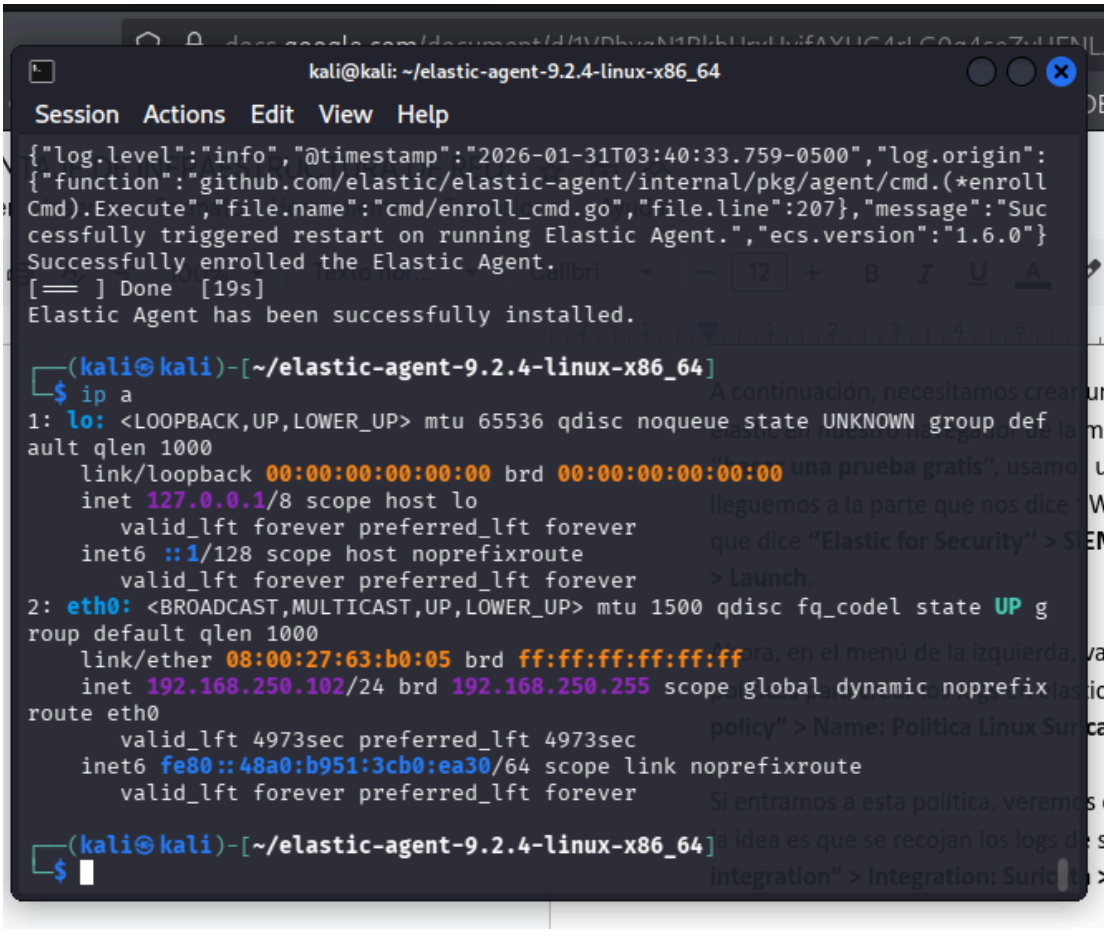
- Name: Suricata

- Index pattern: *suricata*

Ahora seleccionando este filtro, podemos poner arriba también filtro pdf, o seleccionar en el menú de la izquierda sign y coger suricata.eve.alert.signature y dentro de este añadir el que pone “pdf detectado”. Importante mirar

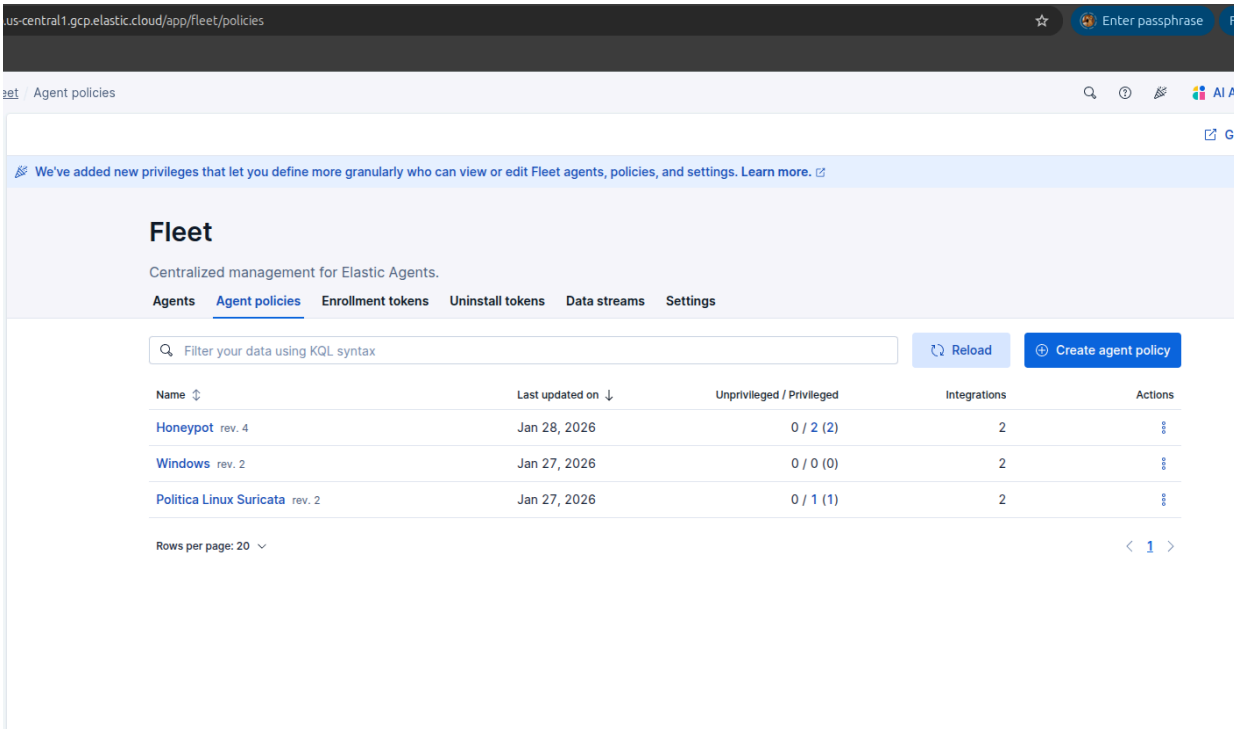


Si nos fijamos donde pone “source.ip” es la ip desde donde descargamos el archivo pdf y destination.ip es nuestra ip de la máquina virtual kali, podemos comprobarlo haciendo ‘’ip a’’ en la máquina kali.

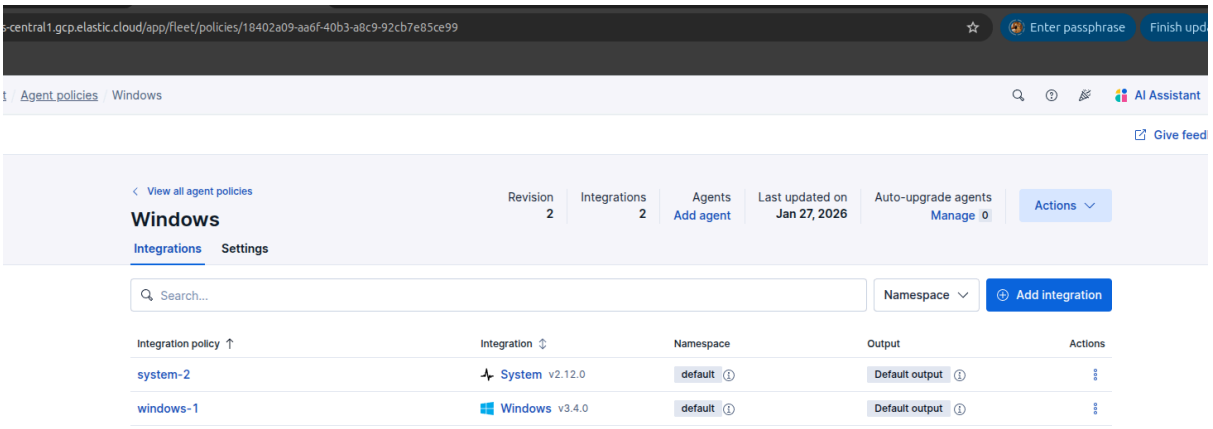


También podemos ver el archivo json del log, en él es importante fijarse en que nos aparece nuestra ip de la máquina kali, la ruta que marcamos e incluso la regla que creamos. (**VER ANEXO 1, JSON LOG SURICATA**).

Ahora volvemos a **More > Assets > Policies**, añadimos una política con nombre Windows y otra con nombre Honeypot. Debería quedarnos así:

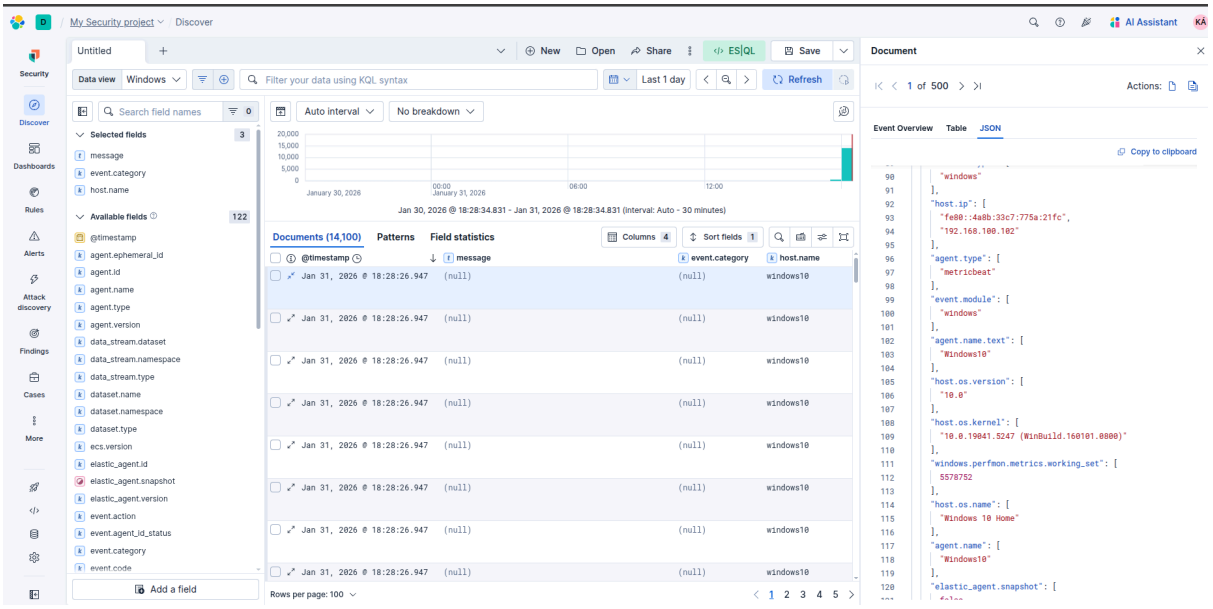


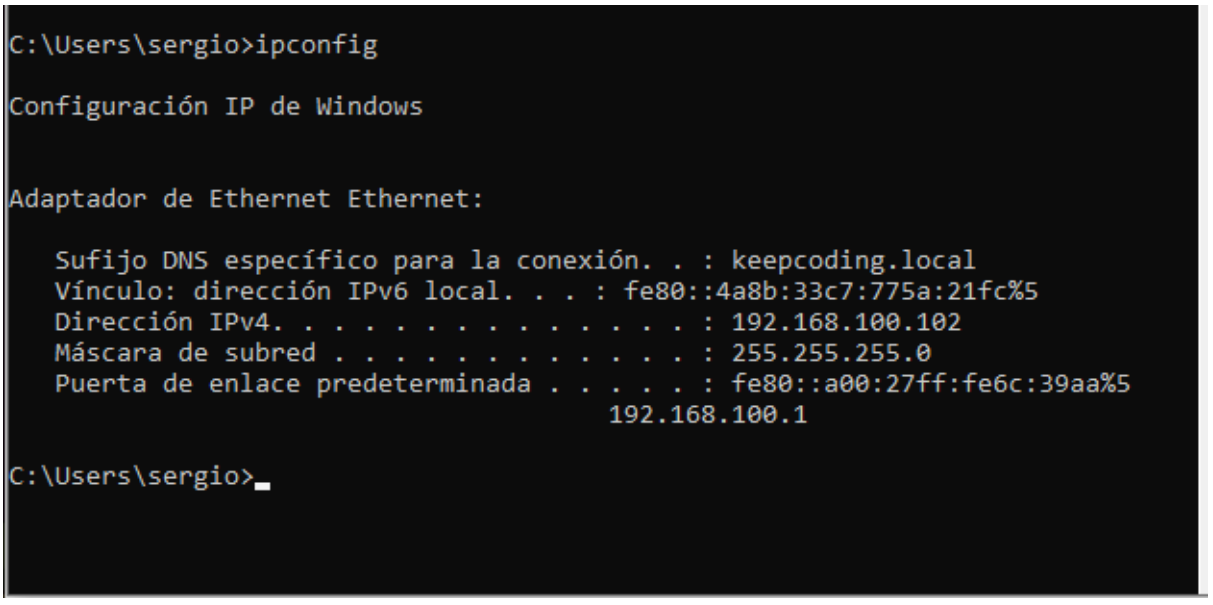
Dentro de la de Windows, añadimos una integración, la integración que debemos escoger es windows (a secas), y la añadimos.



Ahora añadimos un agente, copiamos el comando del cuadro de texto seleccionando windowsx86_64 y lo instalamos usando powershell en la máquina windows (arrancar powershell como administrador).

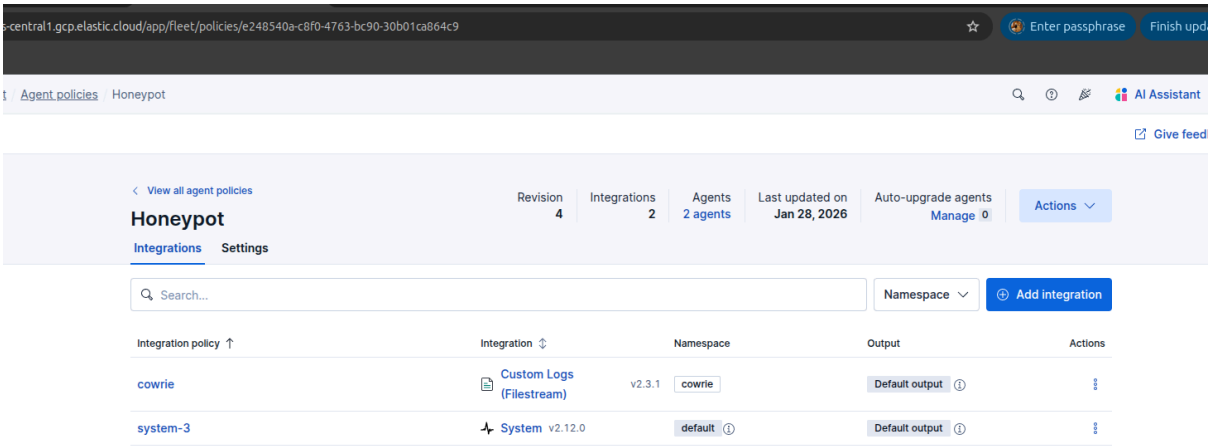
Una vez hecho esto, nos vamos a elastic, creamos un data view, *windows* y deberíamos ver los logs del sistema windows, en el archivo json deberíamos encontrar nuestra IP de la máquina windows, la cual podemos comprobar haciendo “ipconfig” en la terminal windows. (**VER ANEXO 2: JSON LOG WINDOWS)**





Ahora vamos a la política del **honeypot**, añadimos integración y escogemos como integración **Custom Logs (Filestream)**, como integration name le ponemos “Cowrie”, en

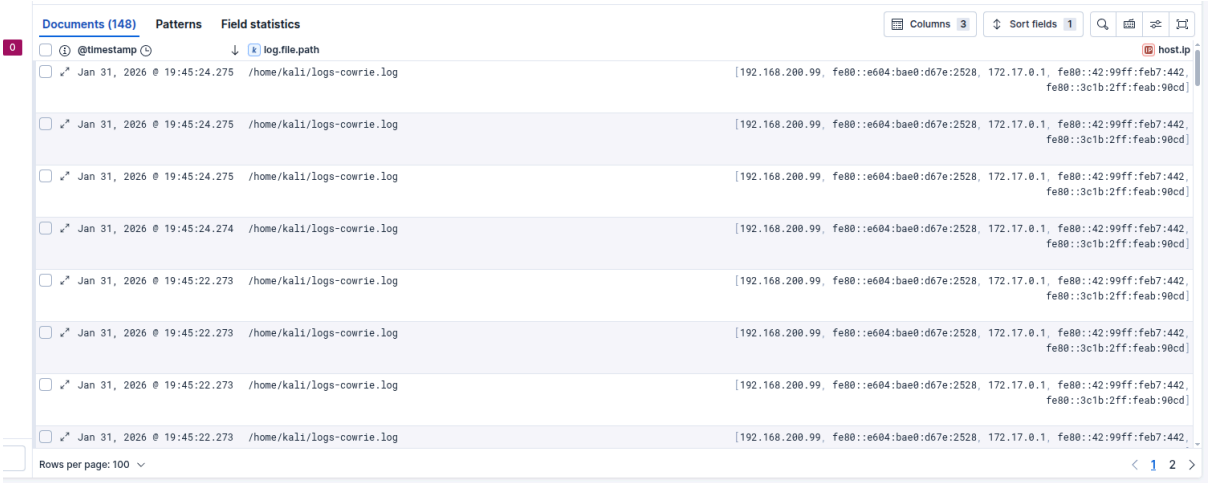
namespace ponemos “cowrie” y en custom Filestream Logs cambiamos la ruta a **/home/kali/logs-cowrie.log**



Creamos en el home de kali un archivo que se llame logs-cowrie.log, despues ejecutamos el comando:

- **docker run -p 222:2222 cowrie/cowrie > logs-cowrie.log**

Ahora añadimos un data view, con index *cowrie* y lo aplicamos, veremos los logs del cowrie. Igual que antes debemos comprobar, ruta, ip… (**VER ANEXO 3: JSON LOG HONEYPOT).**



ANEXOS:

ANEXO 1: JSON LOG SURICATA.


```
{
  "_index": ".ds-logs-suricata.eve-default-2026.01.27-000001",
  "_id": "AZwTNsRYTMj50tE-V1pq",
  "_version": 1,
  "_ignored": [
    "suricata.eve.direction",
    "suricata.eve.files",
    "suricata.eve.flow.dest_ip",
    "suricata.eve.flow.dest_port",
    "suricata.eve.flow.src_ip",
    "suricata.eve.flow.src_port",
    "suricata.eve.tc_progress",
    "suricata.eve.ts_progress"
  ],
  "_source": {
    "@timestamp": "2026-01-31T06:58:20.853Z",
    "agent": {
      "ephemeral_id": "b3806607-e209-4f89-90be-d481574f509d",
      "id": "aed4f834-4d52-4ad8-a47d-70977dd475a3",
      "name": "kali",
      "type": "filebeat",
      "version": "9.2.4"
    },
    "data_stream": {
      "dataset": "suricata.eve",
      "namespace": "default",
      "type": "logs"
    },
    "destination": {
      "address": "192.168.250.102",
      "bytes": 46826,
      "domain": "informatica.uv.es",
      "ip": "192.168.250.102",
      "packets": 33,
      "port": 55880
    },
    "ecs": {
      "version": "8.17.0"
    },
    "elastic_agent": {
      "id": "aed4f834-4d52-4ad8-a47d-70977dd475a3",
      "snapshot": false,
      "version": "9.2.4"
    },
    "event": {
```

```
    "agent_id_status": "verified",
    "category": [
      "network",
      "intrusion_detection"
    ],
    "created": "2026-01-31T08:40:44.657Z",
    "dataset": "suricata.eve",
    "ingested": "2026-01-31T08:40:47Z",
    "kind": "alert",
    "severity": 2,
    "start": "2026-01-31T06:58:20.730Z",
    "type": [
      "allowed"
    ]
  },
  "http": {
    "request": {
      "method": "GET"
    },
    "response": {
      "body": {
        "bytes": 42904
      },
      "status_code": 200
    }
  },
  "input": {
    "type": "log"
  },
  "log": {
    "file": {
      "path": "/var/log/suricata/eve.json"
    },
    "offset": 2487152
  },
  "message": "Descarga de archivo detectado",
  "network": {
    "bytes": 49024,
    "community_id": "1:lW5xBZQjVg34BmKhUzFJ8qvh/yk=",
    "packets": 60,
    "protocol": "http",
    "transport": "tcp"
  },
  "observer": {
    "hostname": "kali",
    "ip": [
      "192.168.250.102",
      "fe80::48a0:b951:3cb0:ea30"
    ],
    "mac": [
```

```
      "08-00-27-63-B0-05"
    ],
    "product": "Suricata",
    "type": "ids",
    "vendor": "OISF"
  },
  "related": {
    "hosts": [
      "informatica.uv.es"
    ],
    "ip": [
      "147.156.84.161",
      "192.168.250.102"
    ]
  },
  "rule": {
    "category": "Descarga de archivo detectado",
    "id": "3",
    "name": "Archivo PDF Detectado"
  },
  "source": {
    "address": "147.156.84.161",
    "as": {
      "number": 766,
      "organization": {
        "name": "Entidad Publica Empresarial Red.es"
      }
    },
    "bytes": 2198,
    "geo": {
      "city_name": "Valencia",
      "continent_name": "Europe",
      "country_iso_code": "ES",
      "country_name": "Spain",
      "location": {
        "lat": 39.46759999729693,
        "lon": -0.3771000634878874
      },
      "region_iso_code": "ES-V",
      "region_name": "Valencia"
    },
    "ip": "147.156.84.161",
    "packets": 27,
    "port": 80
  },
  "suricata": {
    "eve": {
      "alert": {
        "category": "Descarga de archivo detectado",
        "gid": 1,
```

```
        "rev": 0,
        "signature": "Archivo PDF Detectado",
        "signature_id": 3
      },
      "direction": "to_client",
      "event_type": "alert",
      "files": [
        {
          "filename": "/iiguia/IST/Tema2.pdf",
          "size": 42904,
          "stored": false,
          "state": "UNKNOWN",
          "tx_id": 0,
          "gaps": false,
          "storing": true,
          "sid": [
            3
          ]
        }
      ],
      "flow": {
        "dest_ip": "147.156.84.161",
        "dest_port": 80,
        "src_ip": "192.168.250.102",
        "src_port": 55880
      },
      "flow_id": "1168614008984888",
      "http": {
        "http_content_type": "application/pdf",
        "protocol": "HTTP/1.1"
      },
      "in_iface": "eth0",
      "ip_v": 4,
      "pkt_src": "wire/pcap",
      "tc_progress": "response_body",
      "ts_progress": "request_complete",
      "tx_id": 0
    }
  },
  "tags": [
    "forwarded",
    "suricata-eve"
  ],
  "url": {
    "domain": "informatica.uv.es",
    "original": "/iiguia/IST/Tema2.pdf",
    "path": "/iiguia/IST/Tema2.pdf"
  },
  "user_agent": {
    "device": {
```

```
      "name": "Other"
    },
    "name": "Firefox",
    "original": "Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0",
    "os": {
      "name": "Linux"
    },
    "version": "140.0"
  }
},
"fields": {
  "rule.id": [
    "3"
  ],
  "elastic_agent.version": [
    "9.2.4"
  ],
  "event.category": [
    "network",
    "intrusion_detection"
  ],
  "suricata.eve.files.tx_id": [
    0
  ],
  "suricata.eve.tx_id": [
    0
  ],
  "user_agent.original.text": [
    "Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0"
  ],
  "suricata.eve.flow.dest_ip": [
    "147.156.84.161"
  ],
  "observer.vendor": [
    "OISF"
  ],
  "source.geo.region_name": [
    "Valencia"
  ],
  "suricata.eve.alert.signature": [
    "Archivo PDF Detectado"
  ],
  "suricata.eve.http.protocol": [
    "HTTP/1.1"
  ],
  "source.ip": [
    "147.156.84.161"
  ],
  "agent.name": [
    "kali"
```

```
  ],
  "destination.address": [
    "192.168.250.102"
  ],
  "suricata.eve.event_type": [
    "alert"
  ],
  "network.community_id": [
    "1:lW5xBZQjVg34BmKhUzFJ8qvh/yk="
  ],
  "event.agent_id_status": [
    "verified"
  ],
  "http.response.status_code": [
    200
  ],
  "suricata.eve.flow_id": [
    "1168614008984888"
  ],
  "source.geo.city_name": [
    "Valencia"
  ],
  "user_agent.original": [
    "Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0"
  ],
  "event.severity": [
    2
  ],
  "source.packets": [
    27
  ],
  "input.type": [
    "log"
  ],
  "suricata.eve.in_iface": [
    "eth0"
  ],
  "tags": [
    "forwarded",
    "suricata-eve"
  ],
  "url.path": [
    "/iiguia/IST/Tema2.pdf"
  ],
  "agent.id": [
    "aed4f834-4d52-4ad8-a47d-70977dd475a3"
  ],
  "source.port": [
    80
  ],
```

```
  "suricata.eve.direction": [
    "to_client"
  ],
  "destination.bytes": [
    46826
  ],
  "event.start": [
    "2026-01-31T06:58:20.730Z"
  ],
  "source.as.number": [
    766
  ],
  "destination.port": [
    55880
  ],
  "suricata.eve.files.size": [
    42904
  ],
  "user_agent.os.name": [
    "Linux"
  ],
  "destination.packets": [
    33
  ],
  "suricata.eve.alert.category": [
    "Descarga de archivo detectado"
  ],
  "agent.type": [
    "filebeat"
  ],
  "related.ip": [
    "147.156.84.161",
    "192.168.250.102"
  ],
  "suricata.eve.files.storing": [
    true
  ],
  "observer.product": [
    "Suricata"
  ],
  "elastic_agent.snapshot": [
    false
  ],
  "suricata.eve.pkt_src": [
    "wire/pcap"
  ],
  "suricata.eve.flow.src_port": [
    55880
  ],
  "elastic_agent.id": [
```

```
    "aed4f834-4d52-4ad8-a47d-70977dd475a3"
  ],
  "suricata.eve.ip_v": [
    4
  ],
  "destination.ip": [
    "192.168.250.102"
  ],
  "observer.hostname": [
    "kali"
  ],
  "event.ingested": [
    "2026-01-31T08:40:47.000Z"
  ],
  "@timestamp": [
    "2026-01-31T06:58:20.853Z"
  ],
  "data_stream.dataset": [
    "suricata.eve"
  ],
  "log.file.path": [
    "/var/log/suricata/eve.json"
  ],
  "url.domain": [
    "informatica.uv.es"
  ],
  "suricata.eve.files.state": [
    "UNKNOWN"
  ],
  "agent.ephemeral_id": [
    "b3806607-e209-4f89-90be-d481574f509d"
  ],
  "suricata.eve.http.http_content_type": [
    "application/pdf"
  ],
  "user_agent.device.name": [
    "Other"
  ],
  "suricata.eve.tc_progress": [
    "response_body"
  ],
  "suricata.eve.alert.rev": [
    0
  ],
  "url.original.text": [
    "/iiguia/IST/Tema2.pdf"
  ],
  "http.request.method": [
    "GET"
  ],
```

```
  "suricata.eve.flow.src_ip": [
    "192.168.250.102"
  ],
  "observer.mac": [
    "08-00-27-63-B0-05"
  ],
  "user_agent.version": [
    "140.0"
  ],
  "source.geo.region_iso_code": [
    "ES-V"
  ],
  "suricata.eve.alert.gid": [
    1
  ],
  "event.kind": [
    "alert"
  ],
  "rule.name": [
    "Archivo PDF Detectado"
  ],
  "network.packets": [
    60
  ],
  "log.offset": [
    2487152
  ],
  "user_agent.name": [
    "Firefox"
  ],
  "destination.domain": [
    "informatica.uv.es"
  ],
  "data_stream.type": [
    "logs"
  ],
  "ecs.version": [
    "8.17.0"
  ],
  "observer.type": [
    "ids"
  ],
  "event.created": [
    "2026-01-31T08:40:44.657Z"
  ],
  "agent.version": [
    "9.2.4"
  ],
  "related.hosts": [
    "informatica.uv.es"
```

```
  ],
  "observer.ip": [
    "192.168.250.102",
    "fe80::48a0:b951:3cb0:ea30"
  ],
  "suricata.eve.flow.dest_port": [
    80
  ],
  "source.geo.location": [
    {
      "coordinates": [
        -0.3771000634878874,
        39.46759999729693
      ],
      "type": "Point"
    }
  ],
  "source.address": [
    "147.156.84.161"
  ],
  "user_agent.os.name.text": [
    "Linux"
  ],
  "suricata.eve.alert.signature_id": [
    3
  ],
  "event.module": [
    "suricata"
  ],
  "network.protocol": [
    "http"
  ],
  "suricata.eve.files.filename": [
    "/iiguia/IST/Tema2.pdf"
  ],
  "source.geo.country_iso_code": [
    "ES"
  ],
  "network.bytes": [
    49024
  ],
  "source.bytes": [
    2198
  ],
  "suricata.eve.files.sid": [
    3
  ],
  "source.as.organization.name.text": [
    "Entidad Publica Empresarial Red.es"
  ],
```

```
    "data_stream.namespace": [
      "default"
    ],
    "suricata.eve.files.stored": [
      false
    ],
    "source.as.organization.name": [
      "Entidad Publica Empresarial Red.es"
    ],
    "source.geo.continent_name": [
      "Europe"
    ],
    "message": [
      "Descarga de archivo detectado"
    ],
    "http.response.body.bytes": [
      42904
    ],
    "network.transport": [
      "tcp"
    ],
    "url.original": [
      "/iiguia/IST/Tema2.pdf"
    ],
    "suricata.eve.files.gaps": [
      false
    ],
    "suricata.eve.ts_progress": [
      "request_complete"
    ],
    "event.type": [
      "allowed"
    ],
    "source.geo.country_name": [
      "Spain"
    ],
    "rule.category": [
      "Descarga de archivo detectado"
    ],
    "event.dataset": [
      "suricata.eve"
    ]
  }
}
```


ANEXO 2: JSON LOG WINDOWS.


```
{
```

```
"_index": ".ds-metrics-windows.perfmon-default-2026.01.31-000001",
"_id": "99FQFZwB3VXsMkSyRmWd",
"_version": 1,
"_source": {
  "agent": {
    "name": "Windows10",
    "id": "62122fa5-836e-49a8-b75a-d4a5b8352b37",
    "ephemeral_id": "3367e998-67f9-46c0-bf02-9832b8cb7a66",
    "type": "metricbeat",
    "version": "9.2.4"
  },
  "@timestamp": "2026-01-31T18:28:26.947Z",
  "ecs": {
    "version": "8.0.0"
  },
  "service": {
    "type": "windows"
  },
  "data_stream": {
    "namespace": "default",
    "type": "metrics",
    "dataset": "windows.perfmon"
  },
  "elastic_agent": {
    "id": "62122fa5-836e-49a8-b75a-d4a5b8352b37",
    "version": "9.2.4",
    "snapshot": false
  },
  "host": {
    "hostname": "Windows10",
    "os": {
      "build": "19045.5247",
      "kernel": "10.0.19041.5247 (WinBuild.160101.0800)",
      "name": "Windows 10 Home",
      "family": "windows",
      "type": "windows",
      "version": "10.0",
      "platform": "windows"
    },
    "ip": [
      "fe80::4a8b:33c7:775a:21fc",
      "192.168.100.102"
    ],
    "name": "windows10",
    "id": "b03073f0-8c78-41e8-81ed-eb67037c01c4",
    "mac": [
      "08-00-27-AB-84-C2"
    ],
    "architecture": "x86_64"
  },
```

```
    "metricset": {
      "period": 10000,
      "name": "perfmon"
    },
    "event": {
      "duration": 1010218400,
      "agent_id_status": "verified",
      "ingested": "2026-01-31T18:28:28Z",
      "module": "windows",
      "dataset": "windows.perfmon"
    },
    "windows": {
      "perfmon": {
        "instance": "csrss",
        "metrics": {
          "working_set": 5578752
        },
        "object": "Process"
      }
    }
  },
  "fields": {
    "elastic_agent.version": [
      "9.2.4"
    ],
    "host.os.name.text": [
      "Windows 10 Home"
    ],
    "host.hostname": [
      "Windows10"
    ],
    "host.mac": [
      "08-00-27-AB-84-C2"
    ],
    "host.os.build": [
      "19045.5247"
    ],
    "service.type": [
      "windows"
    ],
    "host.ip": [
      "fe80::4a8b:33c7:775a:21fc",
      "192.168.100.102"
    ],
    "agent.type": [
      "metricbeat"
    ],
    "event.module": [
      "windows"
    ],
```

```
  "agent.name.text": [
    "Windows10"
  ],
  "host.os.version": [
    "10.0"
  ],
  "host.os.kernel": [
    "10.0.19041.5247 (WinBuild.160101.0800)"
  ],
  "windows.perfmon.metrics.working_set": [
    5578752
  ],
  "host.os.name": [
    "Windows 10 Home"
  ],
  "agent.name": [
    "Windows10"
  ],
  "elastic_agent.snapshot": [
    false
  ],
  "host.name": [
    "windows10"
  ],
  "event.agent_id_status": [
    "verified"
  ],
  "host.id": [
    "b03073f0-8c78-41e8-81ed-eb67037c01c4"
  ],
  "metricset.name.text": [
    "perfmon"
  ],
  "host.os.type": [
    "windows"
  ],
  "elastic_agent.id": [
    "62122fa5-836e-49a8-b75a-d4a5b8352b37"
  ],
  "windows.perfmon.object": [
    "Process"
  ],
  "data_stream.namespace": [
    "default"
  ],
  "windows.perfmon.instance": [
    "csrss"
  ],
  "metricset.period": [
    10000
```

```
    ],
    "data_stream.type": [
      "metrics"
    ],
    "event.duration": [
      1010218400
    ],
    "host.architecture": [
      "x86_64"
    ],
    "metricset.name": [
      "perfmon"
    ],
    "event.ingested": [
      "2026-01-31T18:28:28.000Z"
    ],
    "@timestamp": [
      "2026-01-31T18:28:26.947Z"
    ],
    "agent.id": [
      "62122fa5-836e-49a8-b75a-d4a5b8352b37"
    ],
    "ecs.version": [
      "8.0.0"
    ],
    "host.os.platform": [
      "windows"
    ],
    "data_stream.dataset": [
      "windows.perfmon"
    ],
    "agent.ephemeral_id": [
      "3367e998-67f9-46c0-bf02-9832b8cb7a66"
    ],
    "agent.version": [
      "9.2.4"
    ],
    "host.os.family": [
      "windows"
    ],
    "event.dataset": [
      "windows.perfmon"
    ]
  }
}
```


ANEXO 3: JSON LOG HONEYPOT

```
{
  "_index": ".ds-logs-filestream.generic-cowrie-2026.01.28-000001",
  "_id": "AZwVlsRYTMj50tHcmiPW",
  "_version": 1,
  "_source": {
    "@timestamp": "2026-01-31T19:45:24.275Z",
    "agent": {
      "ephemeral_id": "a1fd2140-bdee-4163-850a-ea55defb649a",
      "id": "981c7126-3b63-442e-bd41-cf2e37519202",
      "name": "kali",
      "type": "filebeat",
      "version": "9.2.4"
    },
    "data_stream": {
      "dataset": "filestream.generic",
      "namespace": "cowrie",
      "type": "logs"
    },
    "ecs": {
      "version": "8.0.0"
    },
    "elastic_agent": {
      "id": "981c7126-3b63-442e-bd41-cf2e37519202",
      "snapshot": false,
      "version": "9.2.4"
    },
    "event": {
      "agent_id_status": "verified",
      "dataset": "filestream.generic",
      "ingested": "2026-01-31T19:45:34Z"
    },
    "host": {
      "architecture": "x86_64",
      "containerized": false,
      "hostname": "kali",
      "id": "686fa41363f049e9a84be345a7078e04",
      "ip": [
        "192.168.200.99",
        "fe80::e604:bae0:d67e:2528",
        "172.17.0.1",
        "fe80::42:99ff:feb7:442",
        "fe80::3c1b:2ff:feab:90cd"
      ],
      "mac": [
        "02-42-99-B7-04-42",
        "08-00-27-1F-B7-23",
        "3E-1B-02-AB-90-CD"
```

```
      ],
      "name": "kali",
      "os": {
        "codename": "kali-rolling",
        "family": "debian",
        "kernel": "6.16.8+kali-amd64",
        "name": "Kali GNU/Linux",
        "platform": "kali",
        "type": "linux",
        "version": "2025.4"
      }
    },
    "input": {
      "type": "filestream"
    },
    "log": {
      "file": {
        "device_id": "2049",
        "fingerprint": "acef742d2c1ae69f4d3f0cf12cb64c9fb6b644e8ca612d21e30f8de98439ece6",
        "inode": "1839101",
        "path": "/home/kali/logs-cowrie.log"
      },
      "offset": "4000"
    },
    "message": "2026-01-31T19:45:24+0000 [HoneyPotSSHTransport,0,192.168.1.40] Command
found: ls "
  },
  "fields": {
    "elastic_agent.version": [
      "9.2.4"
    ],
    "host.os.name.text": [
      "Kali GNU/Linux"
    ],
    "host.hostname": [
      "kali"
    ],
    "host.mac": [
      "02-42-99-B7-04-42",
      "08-00-27-1F-B7-23",
      "3E-1B-02-AB-90-CD"
    ],
    "host.ip": [
      "192.168.200.99",
      "fe80::e604:bae0:d67e:2528",
      "172.17.0.1",
      "fe80::42:99ff:feb7:442",
      "fe80::3c1b:2ff:feab:90cd"
    ],
    "agent.type": [
```

```
      "filebeat"
    ],
    "event.module": [
      "filestream"
    ],
    "host.os.version": [
      "2025.4"
    ],
    "host.os.kernel": [
      "6.16.8+kali-amd64"
    ],
    "log.file.device_id": [
      "2049"
    ],
    "host.os.name": [
      "Kali GNU/Linux"
    ],
    "agent.name": [
      "kali"
    ],
    "elastic_agent.snapshot": [
      false
    ],
    "host.name": [
      "kali"
    ],
    "event.agent_id_status": [
      "verified"
    ],
    "host.id": [
      "686fa41363f049e9a84be345a7078e04"
    ],
    "host.os.type": [
      "linux"
    ],
    "elastic_agent.id": [
      "981c7126-3b63-442e-bd41-cf2e37519202"
    ],
    "data_stream.namespace": [
      "cowrie"
    ],
    "host.os.codename": [
      "kali-rolling"
    ],
    "input.type": [
      "filestream"
    ],
    "log.offset": [
      "4000"
    ],
```

```
  "message": [
    "2026-01-31T19:45:24+0000 [HoneyPotSSHTransport,0,192.168.1.40] Command found: ls "
  ],
  "data_stream.type": [
    "logs"
  ],
  "host.architecture": [
    "x86_64"
  ],
  "event.ingested": [
    "2026-01-31T19:45:34.000Z"
  ],
  "@timestamp": [
    "2026-01-31T19:45:24.275Z"
  ],
  "agent.id": [
    "981c7126-3b63-442e-bd41-cf2e37519202"
  ],
  "ecs.version": [
    "8.0.0"
  ],
  "host.containerized": [
    false
  ],
  "host.os.platform": [
    "kali"
  ],
  "log.file.inode": [
    "1839101"
  ],
  "data_stream.dataset": [
    "filestream.generic"
  ],
  "log.file.path": [
    "/home/kali/logs-cowrie.log"
  ],
  "agent.ephemeral_id": [
    "a1fd2140-bdee-4163-850a-ea55defb649a"
  ],
  "agent.version": [
    "9.2.4"
  ],
  "log.file.fingerprint": [
    "acef742d2c1ae69f4d3f0cf12cb64c9fb6b644e8ca612d21e30f8de98439ece6"
  ],
  "host.os.family": [
    "debian"
  ],
  "event.dataset": [
    "filestream.generic"
```

```
    ]
  }
}
```