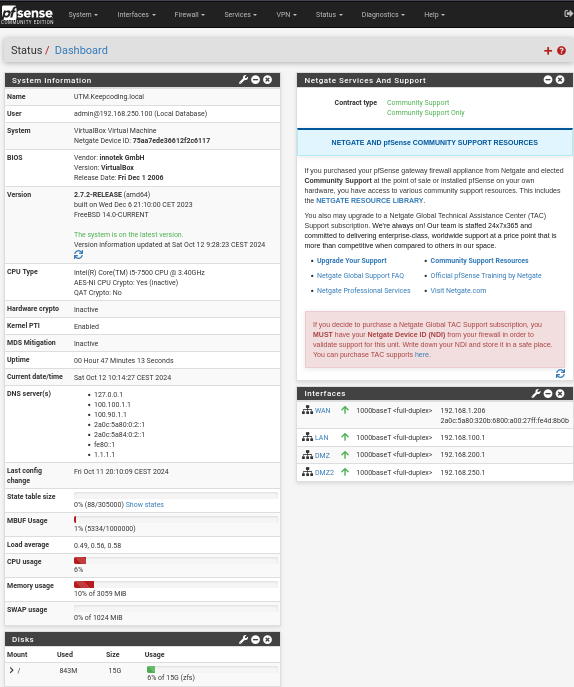
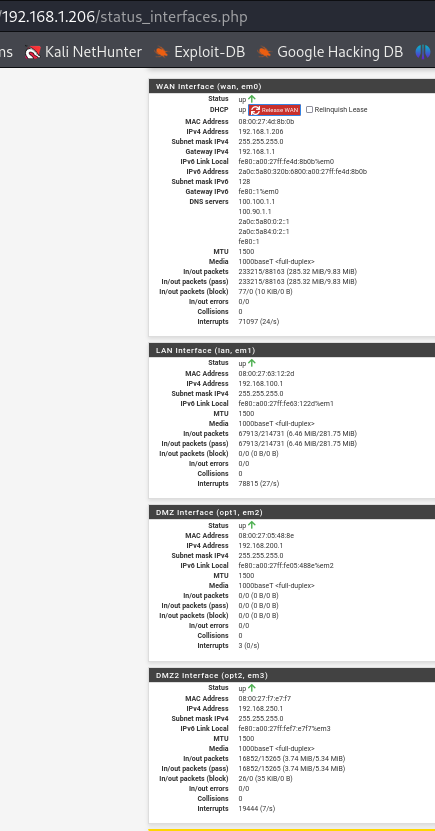
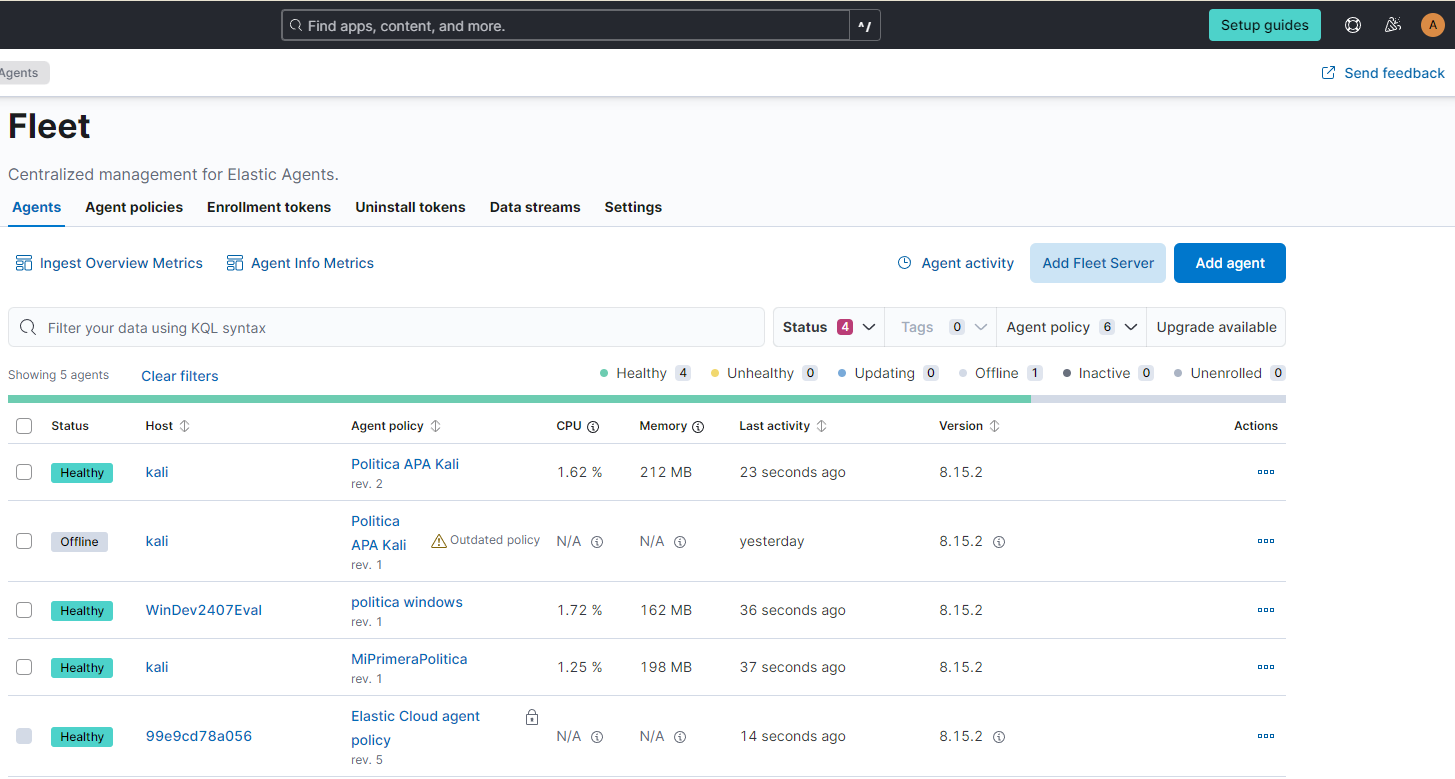
1. Debe tener un Pfsense en que se interconecten las redes LAN, DMZ y DMZ2.

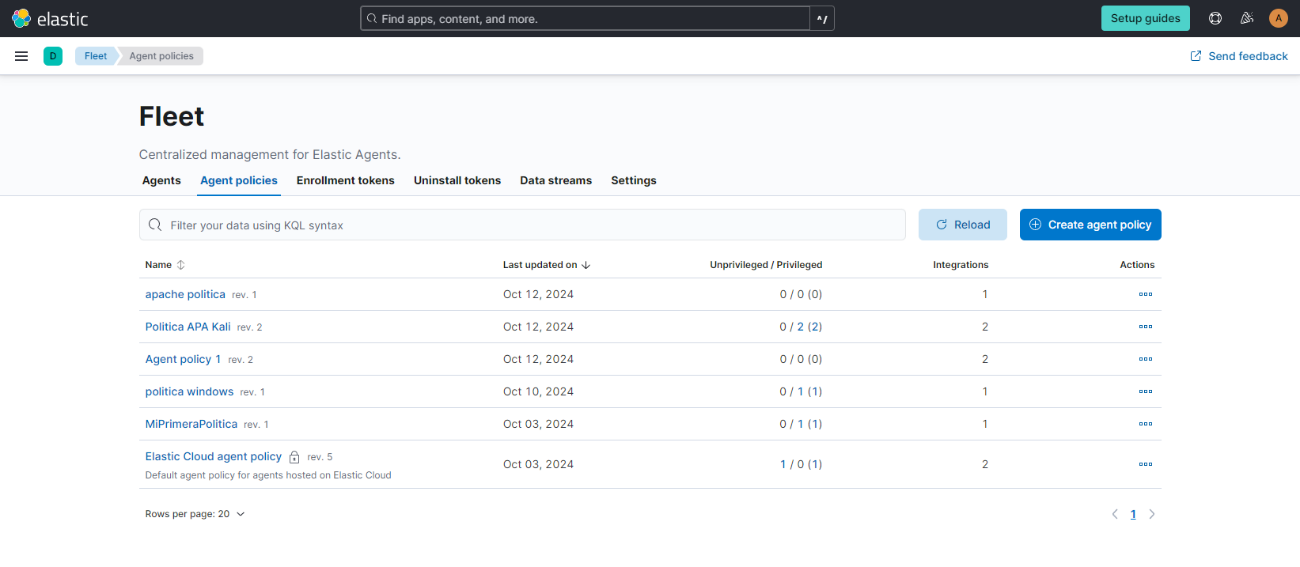
Aquí podemos ver La Wan que se asigna automáticamente, y las direcciones de cada interfaz de red que les asigne.



Aquí de una forma mas detallada, en status – interfaces:



Los agentes de elastic  


Políticas de elastic:  


2. En la red LAN debe haber un equipo Windows 11 que envíe logs al servidor de Elastic.

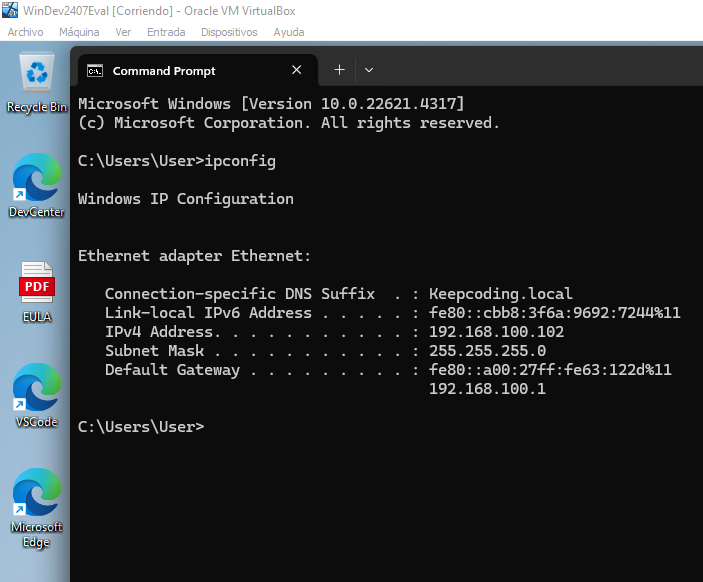
Este es un ejemplo de log desde elastic:



* host.os.name: "Windows 11 Enterprise Evaluation"
* host.os.version: "10.0"
* host.os.build: "22621.4317"
* agent.name: "WinDev2407Eval"
* event.provider: "Microsoft-Windows-Security-Auditing"
* host.ip: ["fe80::cbb8:3f6a:9692:7244", "192.168.100.102"]
* host.mac: ["08-00-27-C3-FF-56"]

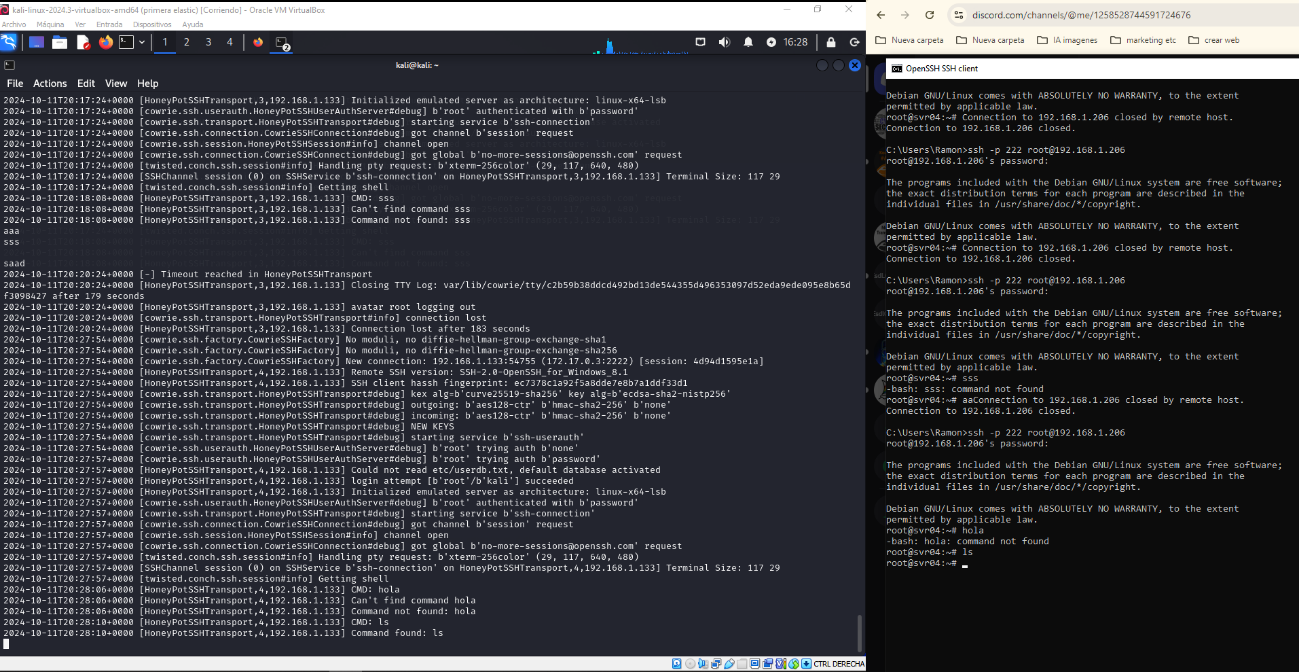
Estos campos indican claramente que el log está generado por una máquina con Windows 11 Enterprise Evaluation, con la dirección de mi maquina.

A continuación presento la maquina de Windows 11 presentando su dirección.

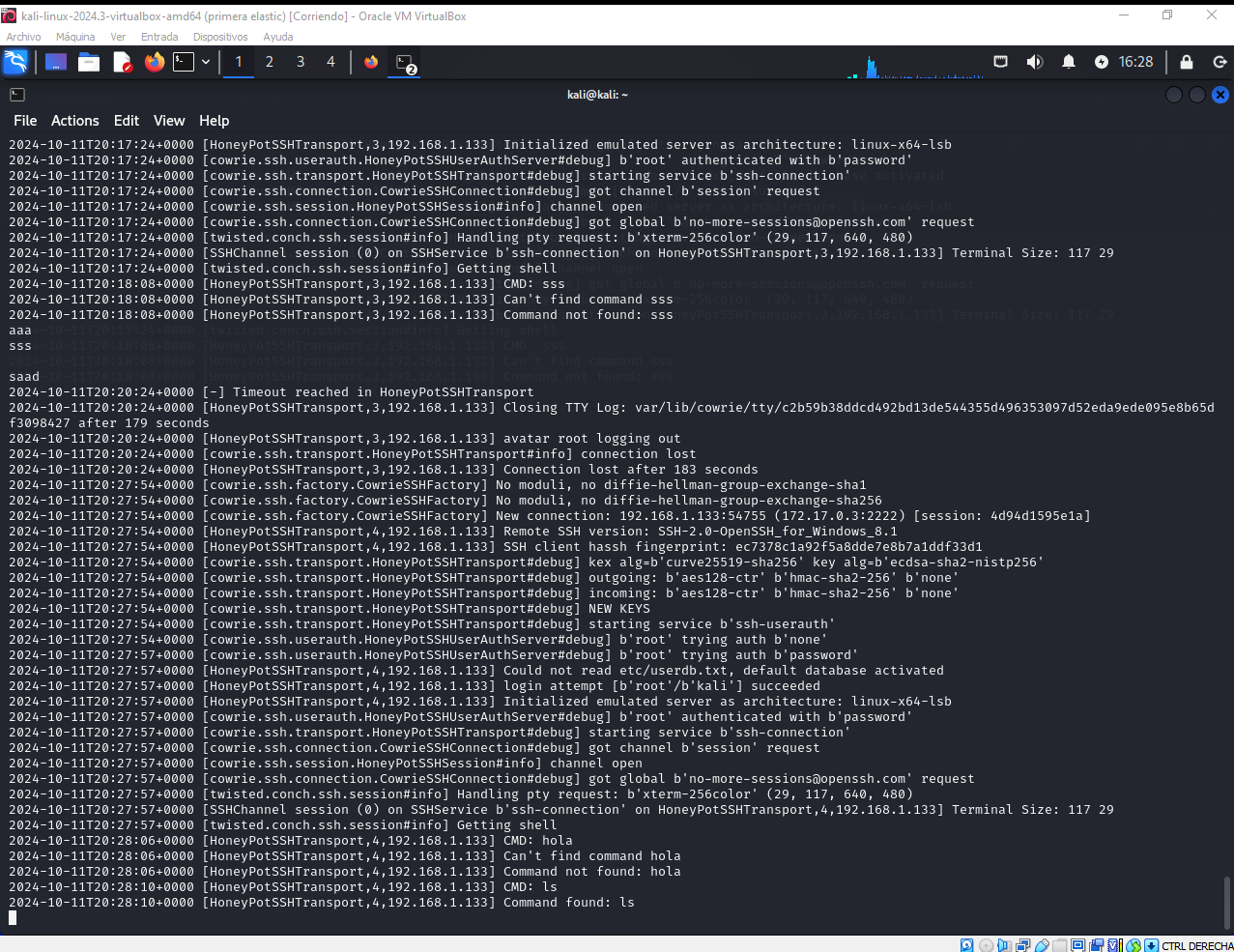


3. En la red DMZ debe haber un honeypot que envíe los logs al servidor de Elastic.

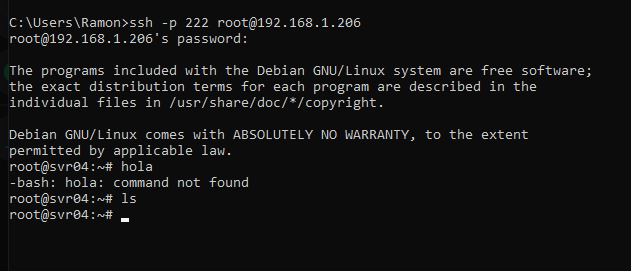
He de decir que al principio le di la dirección 192.168.200.102 despues lo cambie a la 192.168.200.99 cuando estuve haciendo la parte del apache.



docker logs -f 81ad3158bfbe



El ssh desde la terminal de windws



¿Cómo enviar los logs a elastic?

Usando Filebeat.  
  
1. Instalar filebeat en el Kali que tiene el docker:

**Agregar el repositorio de Elastic:**

Lo primero que debes hacer es agregar el repositorio oficial de Elastic a las fuentes de paquetes de tu sistema. Esto te permitirá instalar Filebeat fácilmente.

Fragmento de código

wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -

echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee -a /etc/apt/sources.list.d/elastic-7.x.list

sudo apt update

**Instalar Filebeat:**

Con el repositorio agregado, puedes proceder a instalar Filebeat:

Bash

sudo apt install filebeat

**Configurar Filebeat:**

/etc/filebeat/filebeat.yml.

Incluyo esta información, mi cloud.id de elastic, mi contraseña de elastic, el host.  
  
filebeat.inputs:

- type: container

paths:

- /var/lib/docker/containers/\*/\*.log

output.elasticsearch:

cloud.id: "e3d25933dee34e56bc60782300201e54:dXMtY2VudHJhbDEuZ2NwLmNsb3VkLmVzLmlvJGNhNzkzODZkY2Q2OTQwMTA5Mzk4ZTJkZWZiYmNlODUxJDg2NDU4ZWQ2MTZhZTQ3MDU4ZDQ1MjlmZWM0OGYxZDlj"

cloud.auth: "elastic:Ela100!\"·"

hosts: ["https://ca79386dcd6940109398e2defbbce851.us-central1.gcp.cloud.es.io:443"]

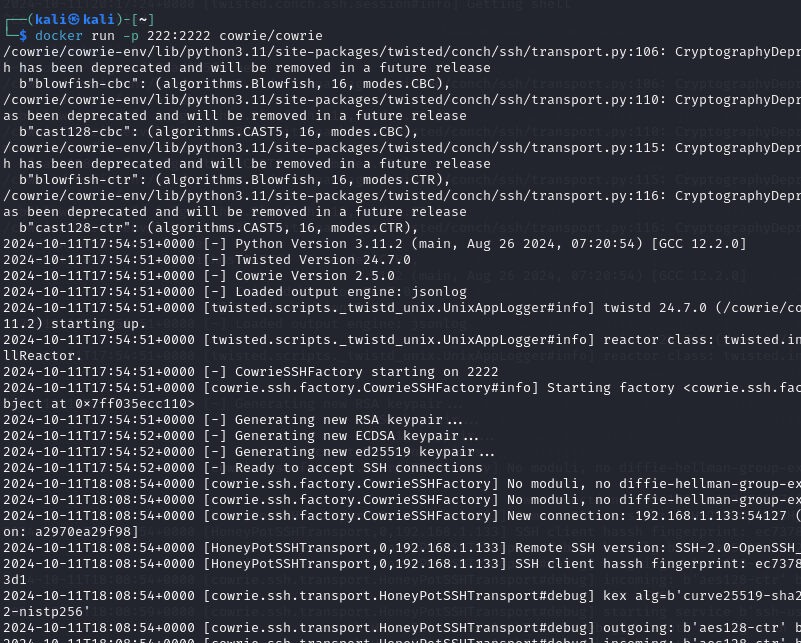
**Iniciar Filebeat**:

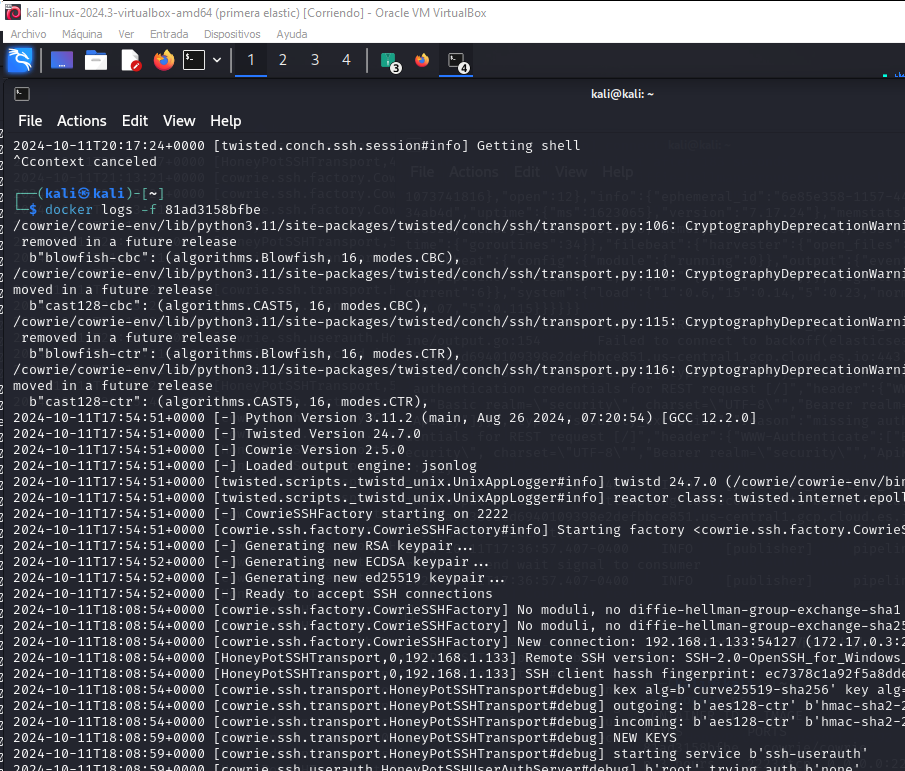
Ejecuta Filebeat para comenzar a recoger y enviar los logs:

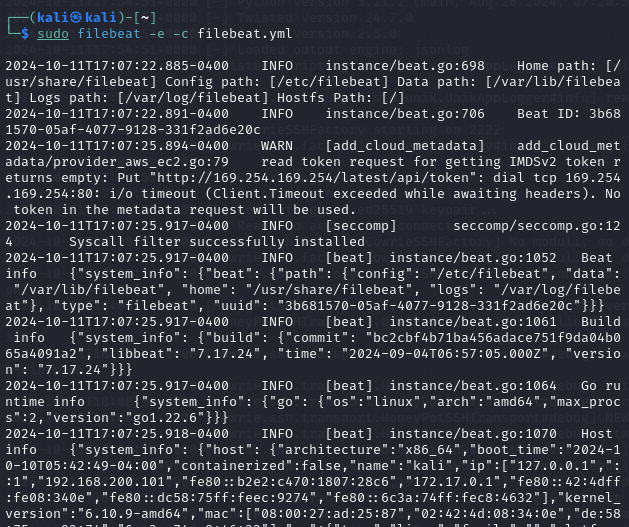
bash

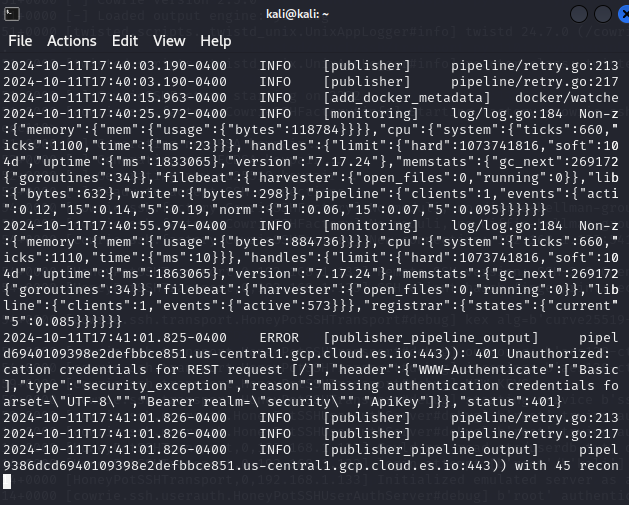
Copiar

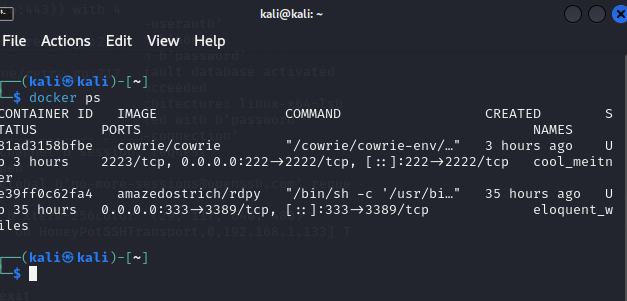
sudo filebeat -e -c /etc/filebeat/filebeat.yml



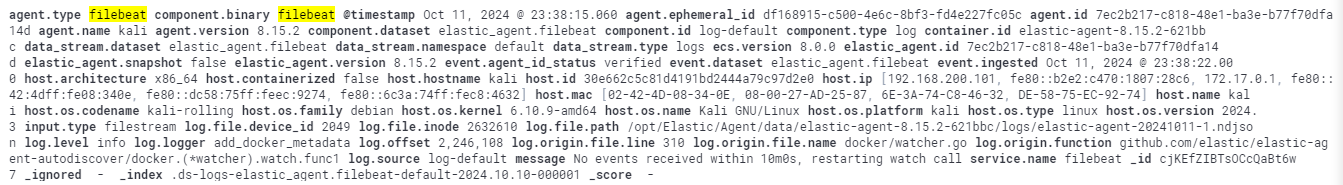






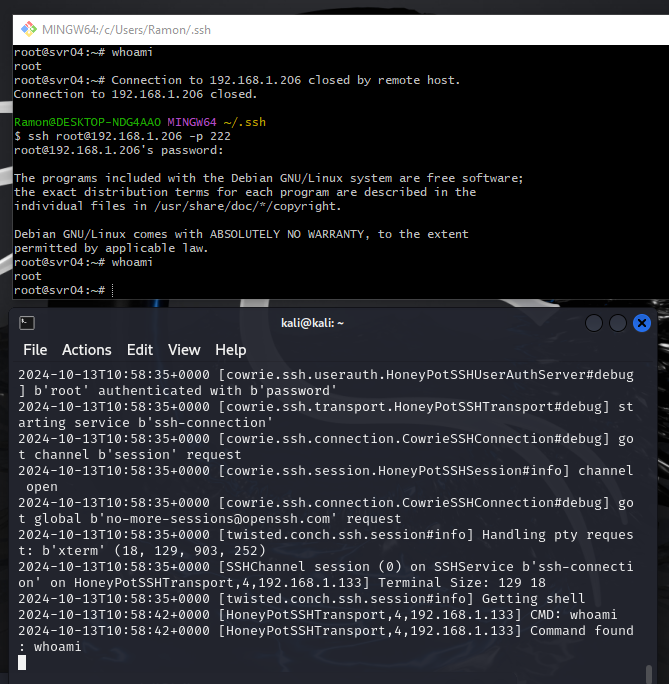


Aquí presento un ejemplo de un log

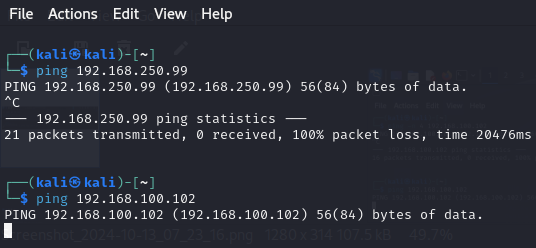


* [**agent.name**](https://agent.name/): indica que Filebeat está corriendo en la máquina con nombre "kali".
* [**host.name**](https://host.name/): muestra que el host es "kali".
* [**container.id**](https://container.id/): indica que los logs están siendo recogidos desde un contenedor Docker.
* [**input.type**](https://input.type/): es "filestream", lo que sugiere que Filebeat está usando la entrada filestream para leer los logs.

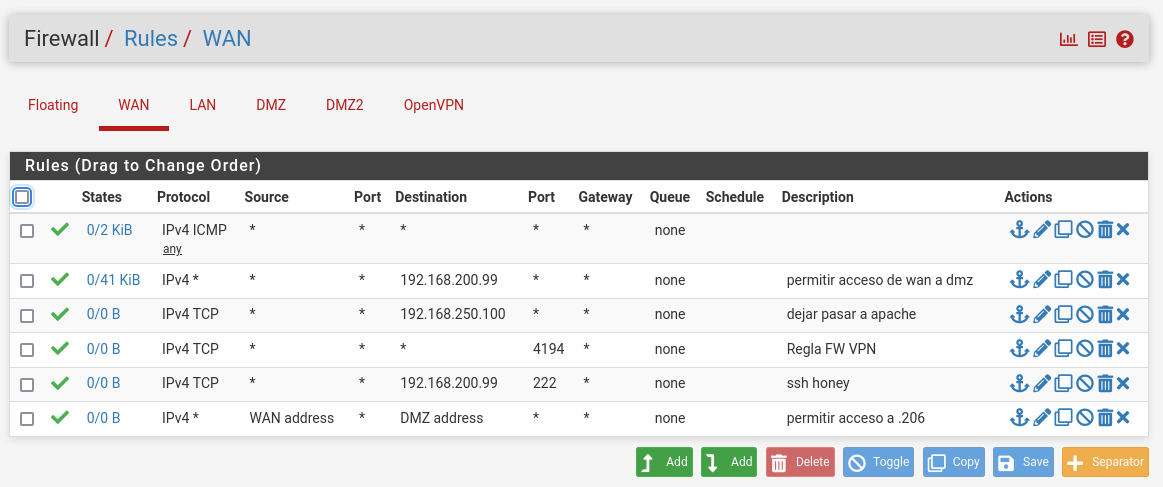
3.1. Este honeypot no debe tener acceso a ninguna red interna (LAN, DMZ2…) y debe ser

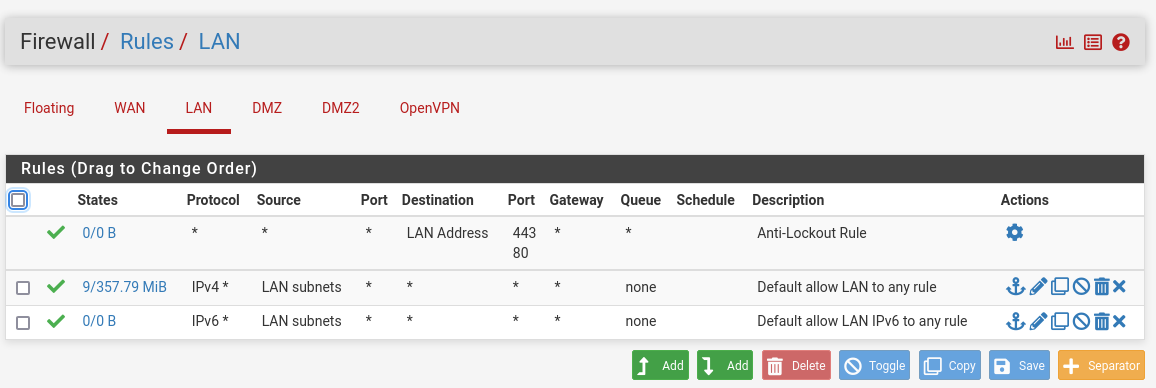
accesible desde el exterior (red WAN) en ambos sentidos.  
vuelvo a entrar desde mi pc, desde fuera:  


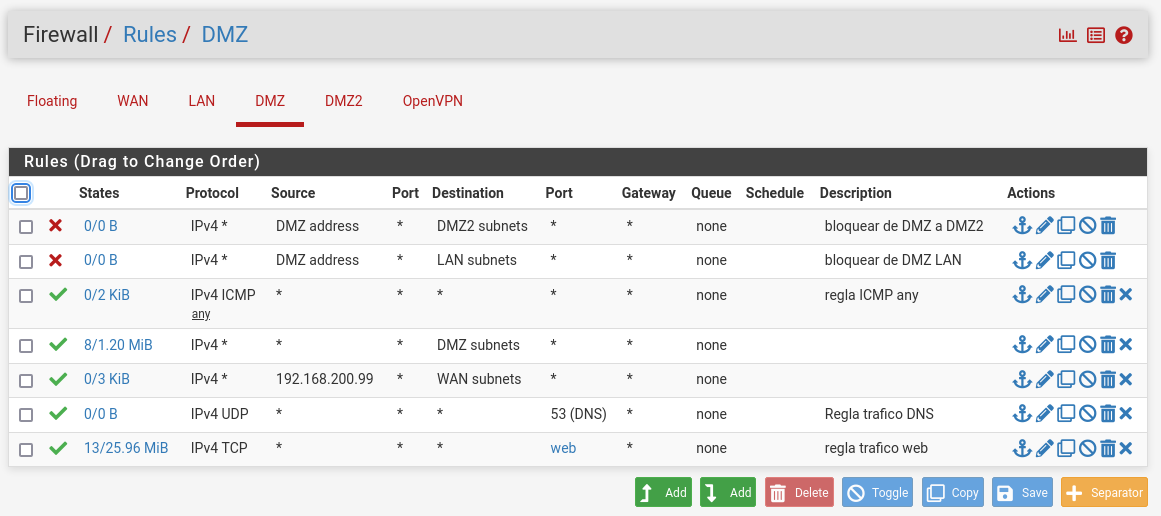
desde la maquina del honeypot a WAN  

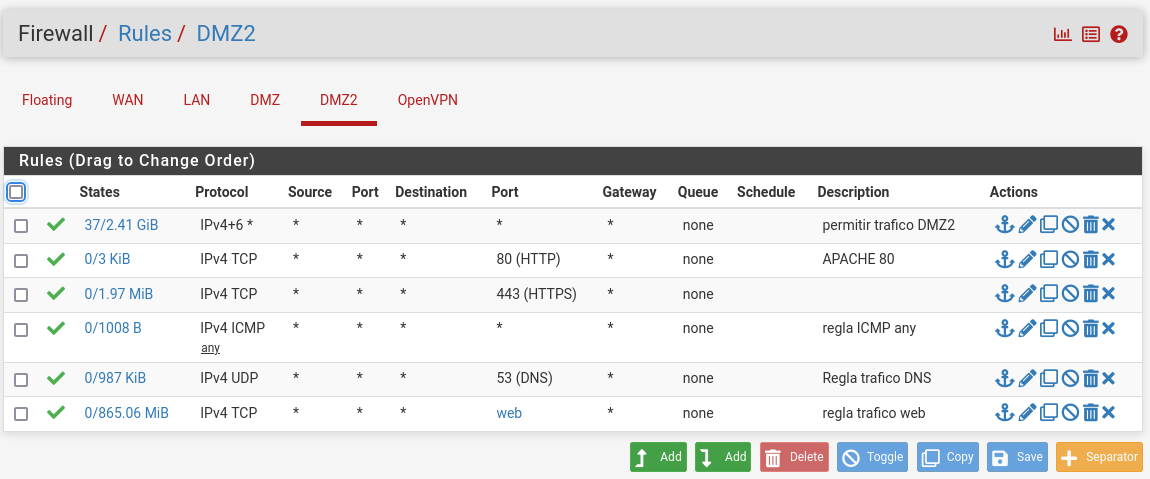

la DMZ no puede hacer ping a las demás maquinas:  


FIREWALL





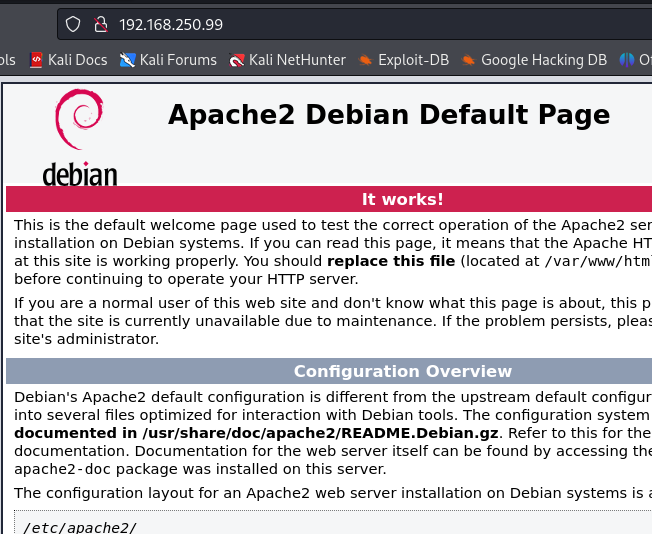




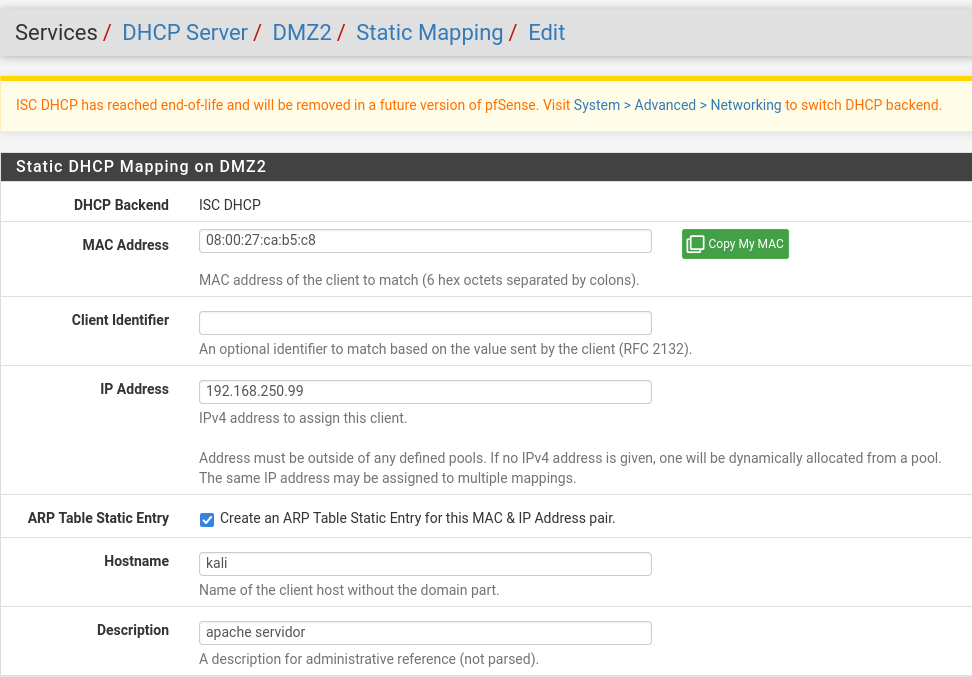
4. En la red DMZ2 debe haber otra fuente diferente de logs a las dos mencionadas anteriormente.

Se propone Suricata o Apache Server como posibles fuentes pero se deja a elección del alumno.

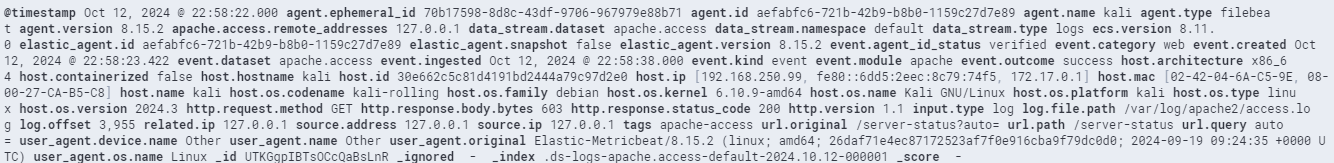
Lo hago con el apache.



Con esta regla asigno una dirección IP a un dispositivo dentro de mi red DMZ2, así recibirá la misma dirección ip, asegurando una gestión mas predecible y controlada de mi red.



Este es un log que proviene del apache, se ve que pone apache, y la dirección: 192.168.250.99.



5. El servidor de Elastic debe recibir, almacenar y poder visualizar los logs del honeypot, el

Windows 11 y la fuente elegida ubicada en la DMZ2.

Este ejercicio se responde con los anteriores.