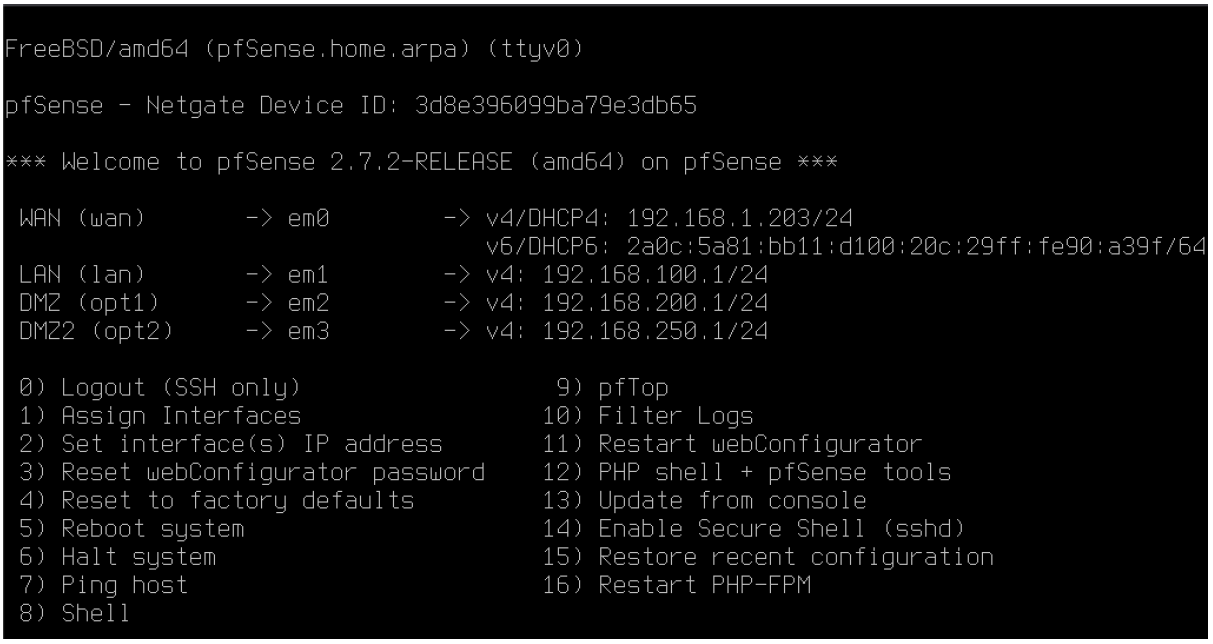
Home Lab

Creación y configuración de firewall y SIEM

En este laboratorio se ha diseñado y desplegado una infraestructura de red orientada a la defensa y monitorización de sistemas.
El laboratorio cuenta con un **firewall y router basados en pfSense**, que permiten enrutar el tráfico procedente del exterior hacia los dispositivos internos, además de aplicar las políticas de filtrado necesarias para garantizar la seguridad y el correcto funcionamiento de la red.



La topología de red se ha dividido en tres segmentos principales:

- **Subred LAN (192.168.100.0/24):** contiene un único equipo con sistema operativo Windows, configurado con la IP estática **192.168.100.10**. Esta red simula la parte interna y segura del entorno corporativo.
- **Subred DMZ (192.168.200.0/24):** aloja un **honeypot** destinado a recopilar información sobre posibles atacantes. El dispositivo tiene la IP **192.168.200.10** y está configurado para recibir conexiones externas simulando un sistema vulnerable.
- **Subred DMZ2 (192.168.250.0/24):** incluye un equipo con sistema operativo Linux con IP **192.168.250.10**, sobre el que se ejecuta un **servidor Apache2** y un

IDS Suricata. Este último se ha configurado para generar alertas ante tráfico o comportamientos sospechosos.

Todos los dispositivos del laboratorio tienen instalado un **agente del stack de Elastic (ELK)**, lo que permite monitorizar su actividad en tiempo real.

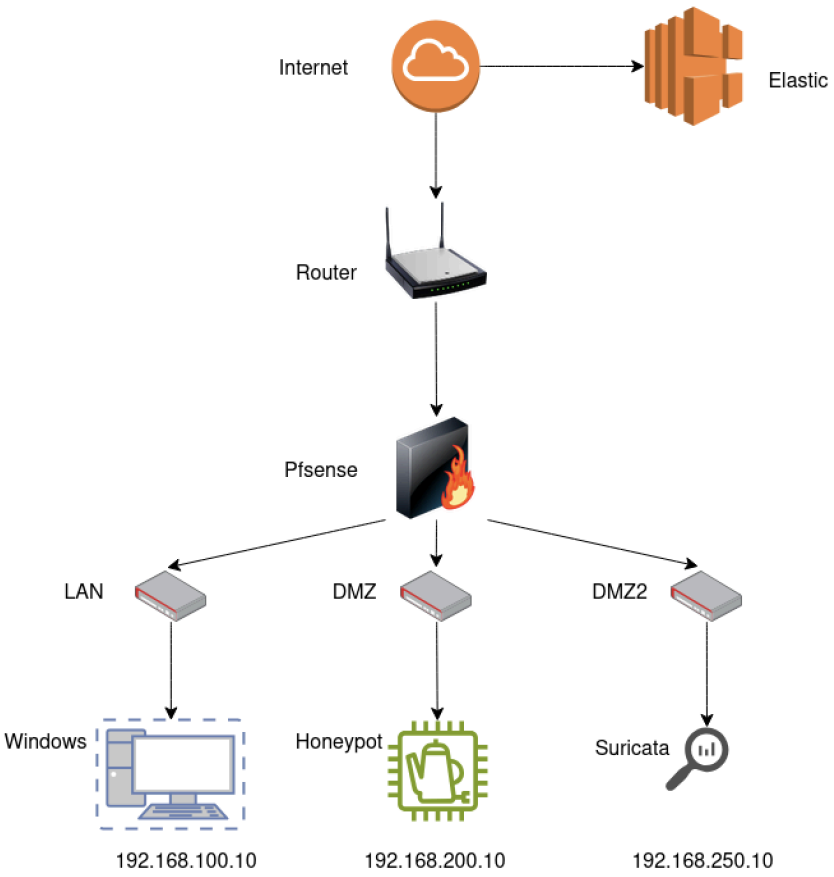
Gracias a esta integración, es posible centralizar los registros de eventos y detectar anomalías o patrones de ataque dentro de las diferentes subredes.

Para la parte del **SIEM**, se ha utilizado **Kibana** como interfaz de visualización y análisis. En ella se han configurado los diferentes agentes de cada máquina, con sus respectivas políticas de recolección de logs y parámetros de funcionamiento, lo que facilita el seguimiento y la correlación de eventos de seguridad.

Configuración de reglas de firewall en pfSense

El **firewall pfSense** actúa como punto central de control del tráfico entre las diferentes subredes y la red externa (WAN).

Su configuración tiene como objetivo garantizar la segmentación de la red, el aislamiento de los servicios expuestos y la protección de los equipos internos frente a posibles amenazas.

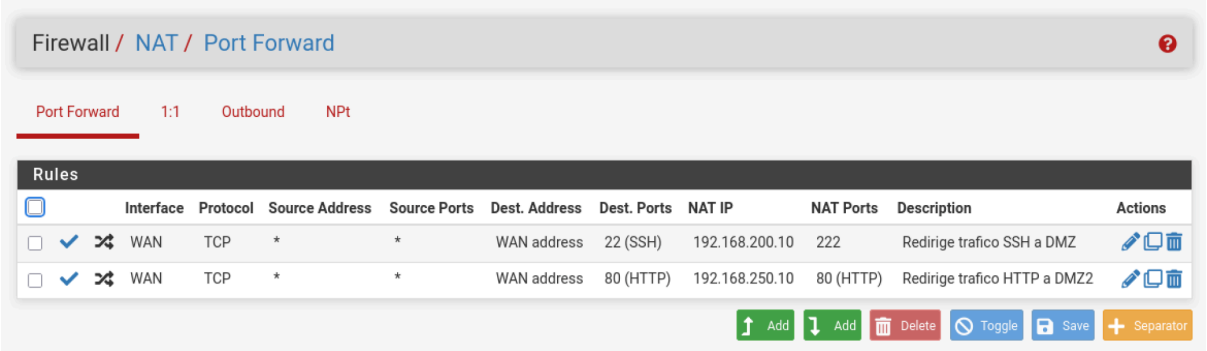


Reglas de NAT y redirección de tráfico

Se han creado **dos reglas de NAT** para redirigir el tráfico entrante desde la interfaz **WAN** hacia los dispositivos correspondientes dentro de las zonas DMZ:

- **Tráfico HTTP (puerto 80):** redirigido desde la interfaz WAN hacia la dirección IP **192.168.250.10** (servidor Apache en la DMZ2).
  Esto permite que los usuarios externos accedan al servicio web alojado en el laboratorio.
- **Tráfico SSH (puerto 22 externo → 222 interno):** redirigido desde la WAN hacia la dirección **192.168.200.10** (Honeypot en la DMZ).
  Esta configuración simula un servicio vulnerable expuesto, permitiendo a posibles atacantes interactuar con el honeypot y generar eventos útiles para el análisis de comportamiento.

Las reglas NAT generan automáticamente las reglas correspondientes en la interfaz **WAN**, lo que garantiza que las conexiones se gestionen según las políticas de seguridad definidas.

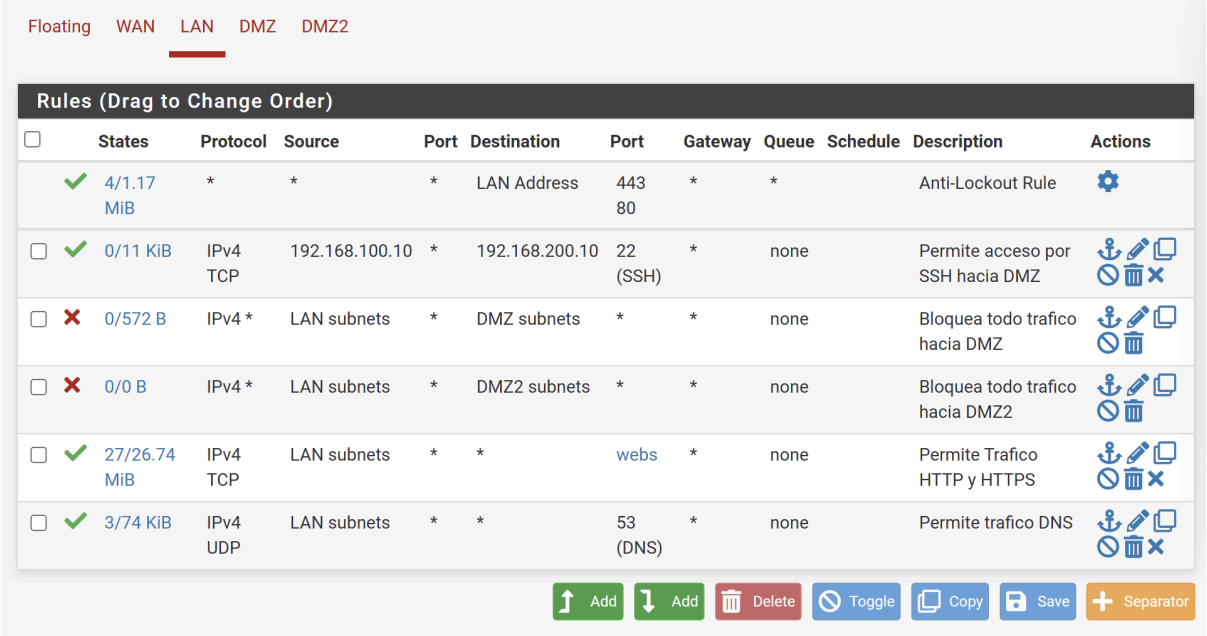


Reglas por subred

Subred LAN (192.168.100.0/24)

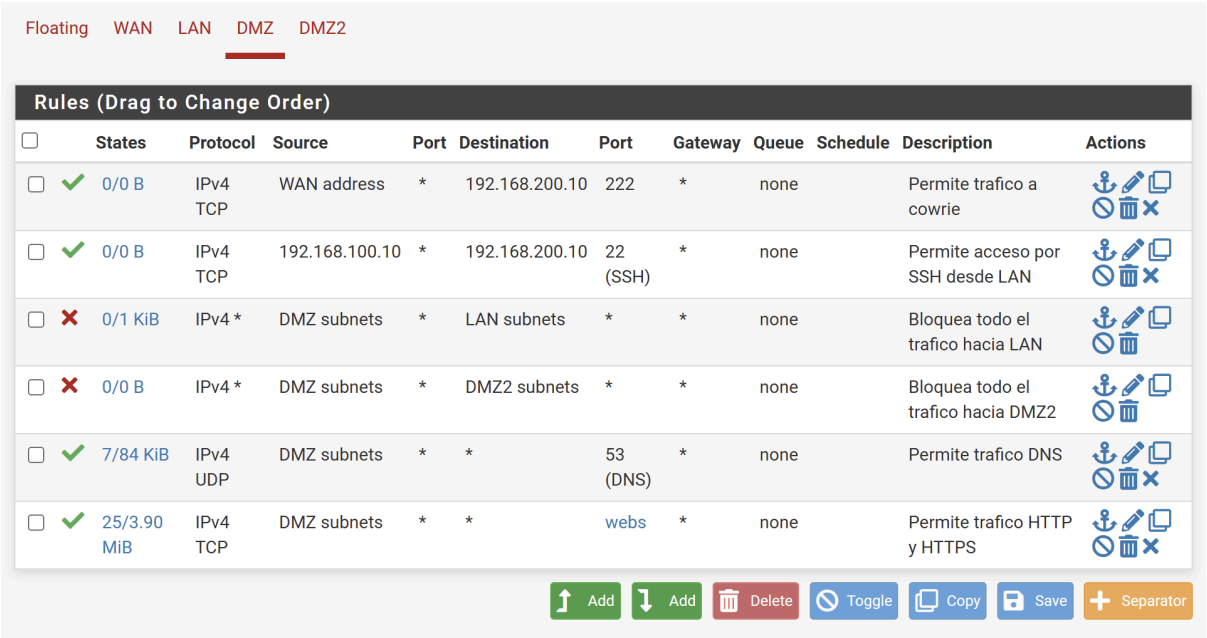
- Permitir tráfico **SSH** hacia la DMZ (IP 192.168.200.10) para tareas de administración del honeypot.
- Bloquear todo el tráfico hacia las subredes **DMZ** y **DMZ2**, evitando la comunicación directa entre segmentos de red.
- Permitir tráfico de salida **DNS (UDP 53)**, **HTTP (TCP 80)** y **HTTPS (TCP 443)**.

Estas reglas se colocan al final de la lista, ya que pfSense aplica las políticas de arriba hacia abajo.



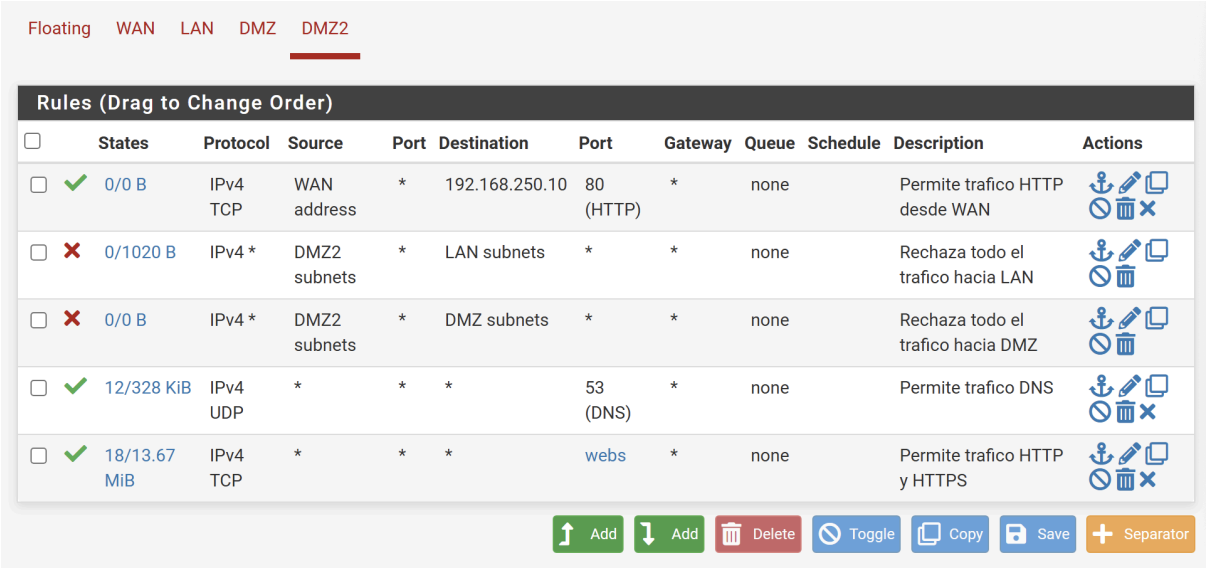
Subred DMZ (192.168.200.0/24)

- Permitir tráfico entrante desde la **WAN address** (IP pública de pfSense) hacia la máquina **192.168.200.10**, por el puerto **222/TCP**.
- Permitir acceso desde la **LAN** (192.168.100.10) por protocolo **SSH**, únicamente para gestión del honeypot.
- Bloquear todo el tráfico hacia **LAN** y **DMZ2**, manteniendo el aislamiento de las zonas.
- Permitir tráfico **DNS (UDP)**, **HTTP (TCP)** y **HTTPS (TCP)** al final de la lista de reglas.



Subred DMZ2 (192.168.250.0/24)

- Permitir tráfico desde la **WAN address** hacia la IP **192.168.250.10** (servidor web Apache).
- Bloquear todo el tráfico hacia las subredes **LAN** y **DMZ**, garantizando la separación total de entornos.
- Permitir tráfico **DNS (UDP)**, **HTTP (TCP)** y **HTTPS (TCP)** como última regla.



Resultado

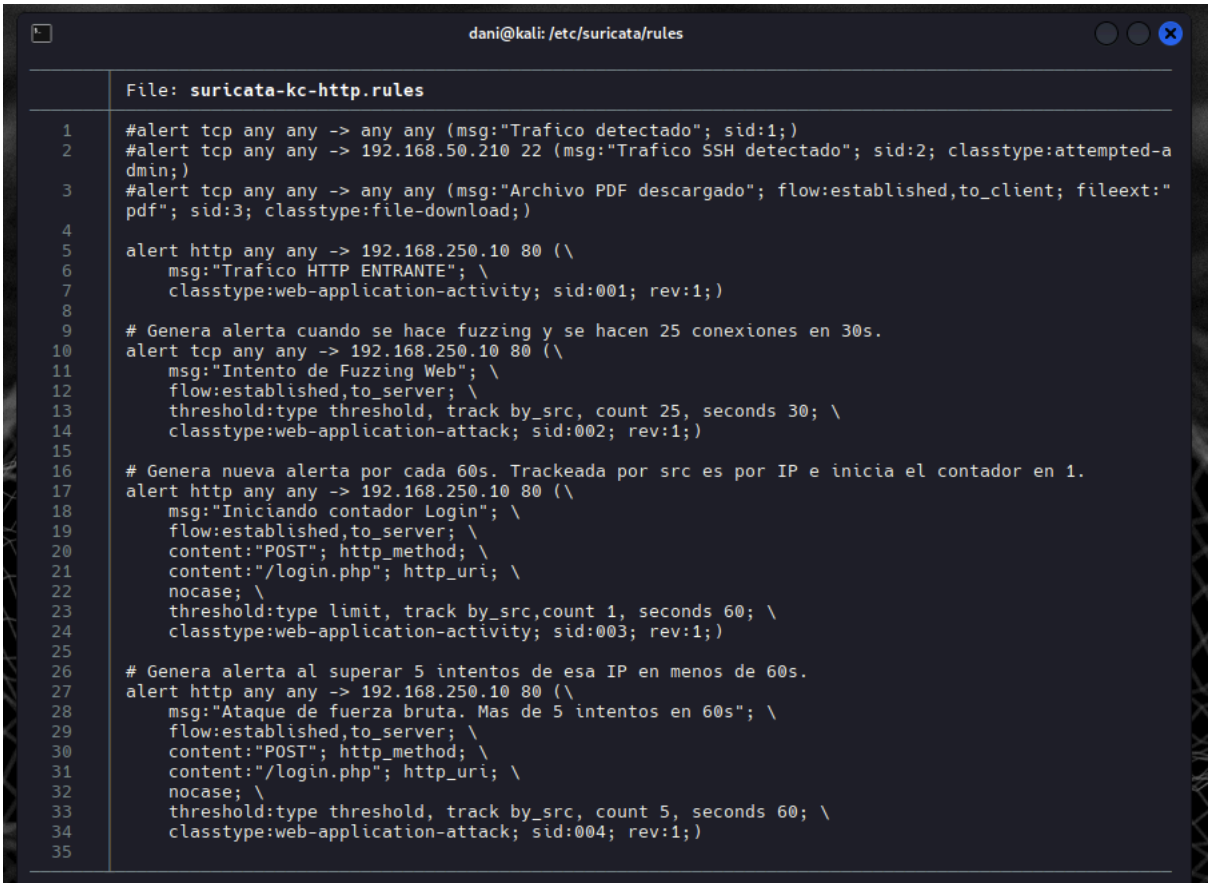
Esta configuración asegura:

- Un **flujo controlado y segmentado** del tráfico entre redes.
- Que solo los **servicios necesarios** (web y honeypot) estén accesibles desde el exterior.
- Que los **equipos internos** permanezcan aislados y protegidos.

Con estas políticas, la arquitectura cumple los principios de **defensa en profundidad** y **segmentación de red**, fundamentales en un entorno Blue Team.

Suricata

En la subred **DMZ2**, donde se encuentra alojado el servidor web Apache, se ha implementado el sistema de detección de intrusiones **Suricata**.
Este IDS se ha configurado en **modo pasivo (sólo detección)**, de manera que genera alertas ante comportamientos anómalos o patrones de ataque, sin bloquear el tráfico.



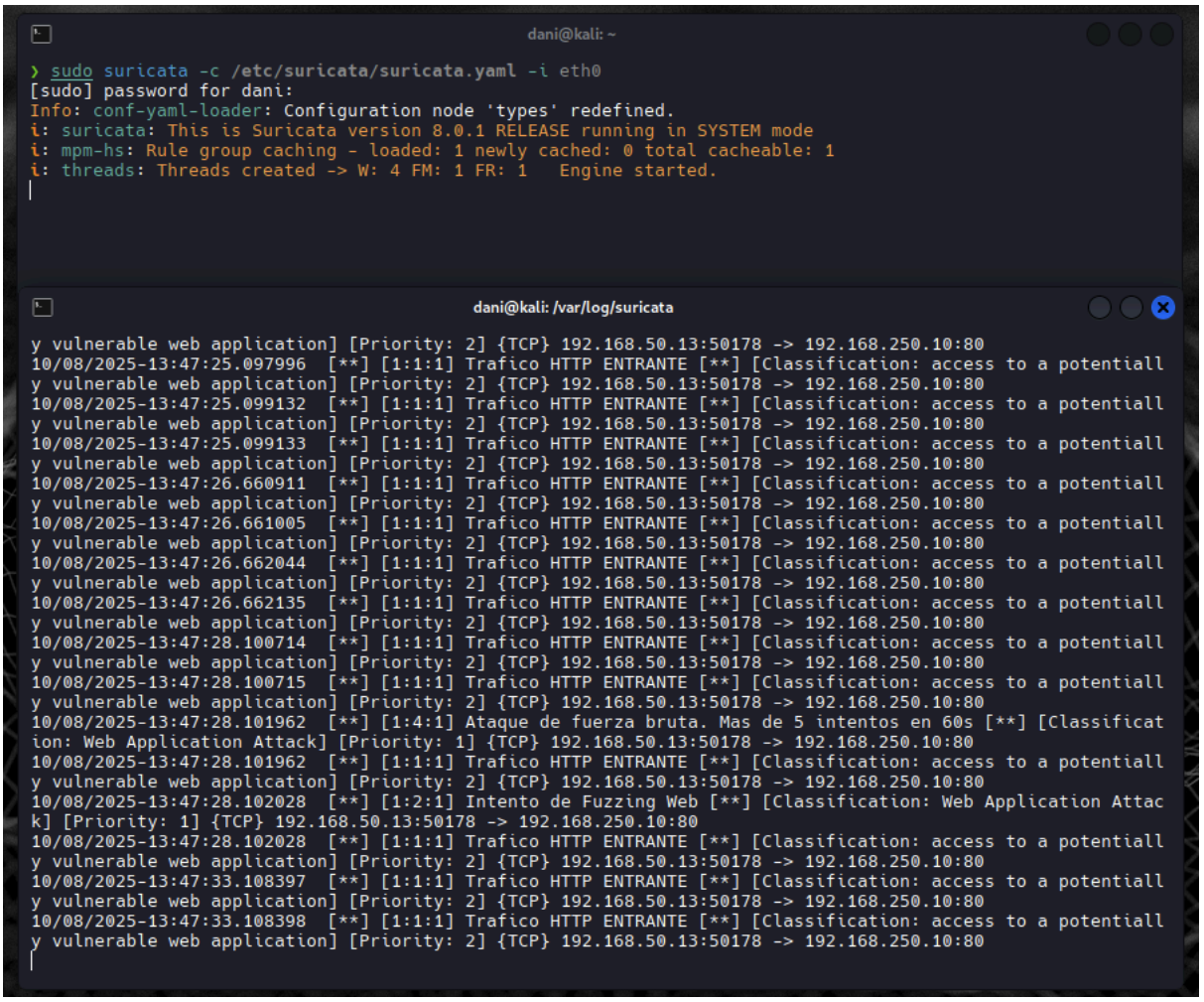
El objetivo de esta implementación es **detectar posibles intentos de ataque contra el servicio web** y registrar dicha actividad para su posterior análisis en el SIEM. Suricata utiliza un conjunto de reglas personalizadas diseñadas para cubrir distintos escenarios de ataque web y actividades sospechosas.

Reglas configuradas

Se ha creado un conjunto de reglas específicas con los siguientes criterios:

- **Tráfico HTTP:** se genera una alerta cada vez que se detecta una conexión HTTP hacia el servidor Apache. Esto permite tener trazabilidad de cada solicitud entrante.
- **Intentos de autenticación:** cuando se detecta un evento de *login* en la aplicación web, se define una variable que actúa como contador, asociada a la dirección IP origen.
- **Detección de fuerza bruta:** si el contador alcanza los **5 intentos fallidos consecutivos**, se genera una alerta indicando un posible ataque de fuerza bruta o de *credential stuffing*.
- **Detección de fuzzing o escaneo:** si se identifica un volumen anómalo de peticiones en un intervalo corto de tiempo, Suricata genera una alerta

indicando un posible intento de enumeración o fuzzing del servicio.



Estas reglas se almacenan en el archivo de configuración correspondiente y se gestionan mediante las políticas definidas en Kibana para su envío y visualización centralizada.

Las alertas generadas se registran en formato **EVE JSON**, lo que permite su integración directa con **Elastic Agent** para el envío al stack ELK.

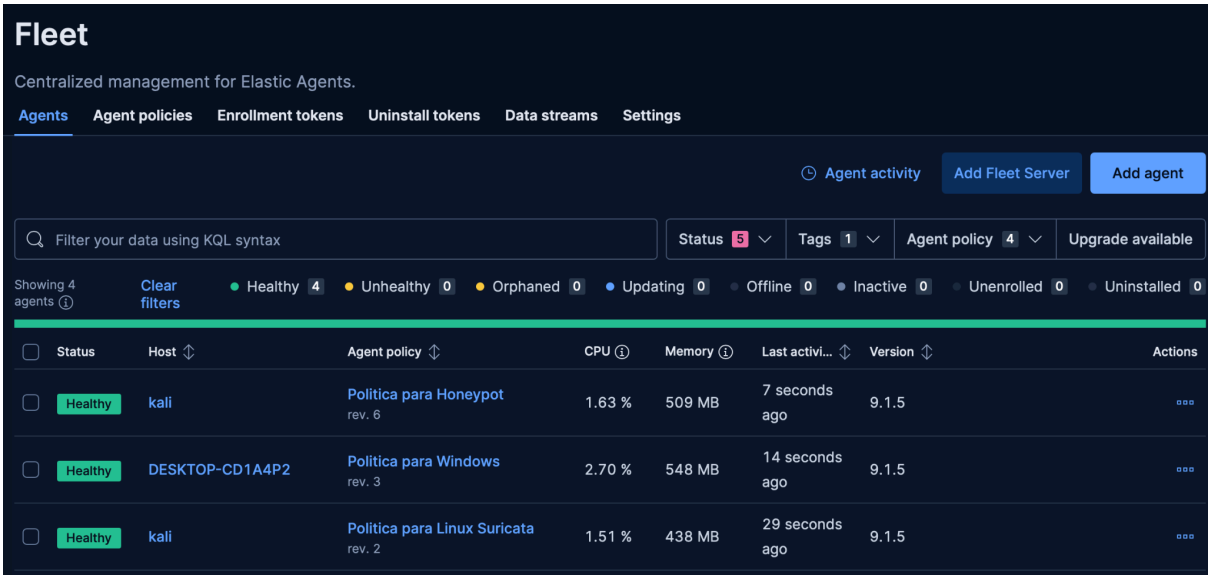
Resultados esperados

La correcta configuración de Suricata permite:

- **Monitorear el tráfico HTTP** hacia el servidor web de forma continua.
- **Identificar intentos de intrusión** o comportamientos anómalos en tiempo real.
- **Correlacionar eventos** dentro del SIEM para detectar patrones más amplios de ataque.
- Mejorar las capacidades defensivas del entorno mediante la **detección temprana de amenazas**.

Kibana

Para la gestión y análisis centralizado de los eventos de seguridad, se ha utilizado **Kibana** como interfaz principal del **SIEM basado en ELK (Elastic Stack)**.
Desde Kibana se visualizan los registros enviados por los distintos **Elastic Agents** instalados en los dispositivos del laboratorio, lo que permite correlacionar eventos, generar dashboards y detectar anomalías de forma proactiva.



Políticas e integraciones de los agentes

Se han creado **tres políticas personalizadas**, cada una adaptada al tipo de dispositivo y su función dentro de la red.
Cada política incluye integraciones específicas para la correcta recopilación y envío de logs:

- **Política de Suricata:** recopila y envía las alertas generadas por el IDS desplegado en la DMZ2, incluyendo campos de evento, origen, destino y firmas detectadas.
- **Política de Windows:** recoge logs del sistema operativo Windows (seguridad, eventos del sistema, ejecuciones de PowerShell, etc.) en la subred LAN.
- **Política del Honeypot (FileStream):** permite capturar los comandos ejecutados y la actividad registrada dentro del honeypot.

Una vez creadas, las políticas se asignaron a los agentes correspondientes, y tras su instalación, estos comenzaron a enviar los datos hacia Elasticsearch de manera continua.

Descubrimiento y análisis de datos

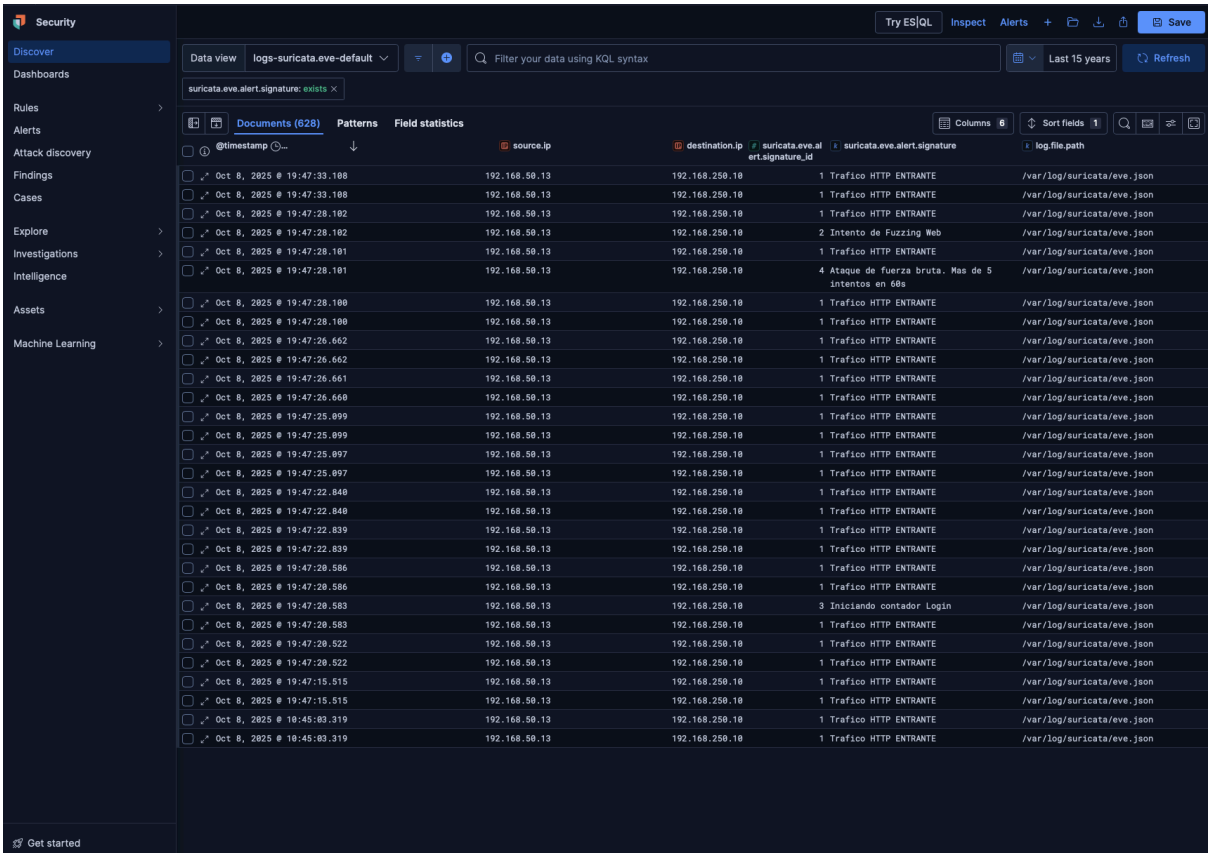
A través de la pestaña **Discover** de Kibana, se realizó la revisión inicial de los eventos generados.

Se configuraron **data views personalizados** para facilitar la lectura y análisis de los logs según la procedencia de cada agente.

- **Data view de Suricata.** Incluye los campos:
  - `@timestamp`
  - `source.ip`
  - `destination.ip`
  - `suricata.eve.alert.signature_id`
  - `suricata.eve.alert.signature`
  - `log.file.path`

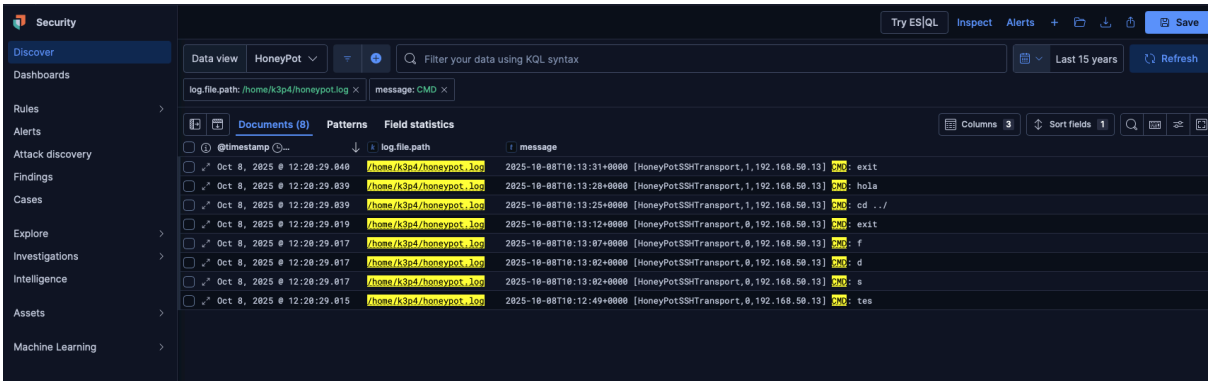
Estos campos permiten identificar qué alertas se han disparado, desde qué dirección IP se originaron y en qué momento ocurrieron.

Filtrando por `suricata.eve.alert.signature`, se obtienen los eventos correspondientes a detecciones reales de Suricata.



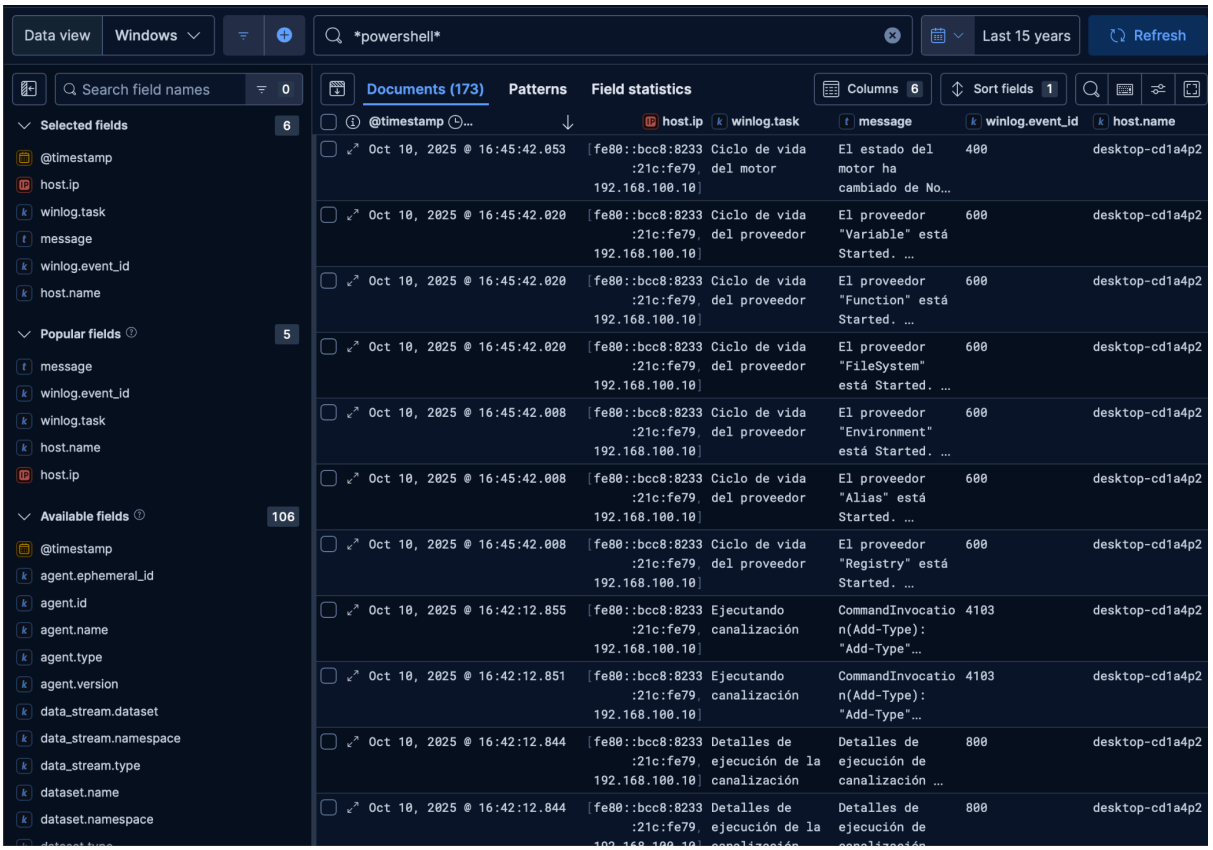
- **Data view del Honeypot.** Incluye los campos:
  - `@timestamp`
  - `log.file.path`
  - `message`

Filtrando por la palabra clave `CMD` en el campo *message*, se pueden visualizar los comandos ejecutados por los atacantes dentro del honeypot, lo que facilita el análisis de su comportamiento y técnicas empleadas.



- **Data view de Windows.** Permite identificar acciones realizadas en la máquina de la LAN.
  En el ejemplo, se filtraron eventos relacionados con **PowerShell**, lo que ayuda a detectar posibles actividades sospechosas o automatizadas dentro del

entorno Windows.

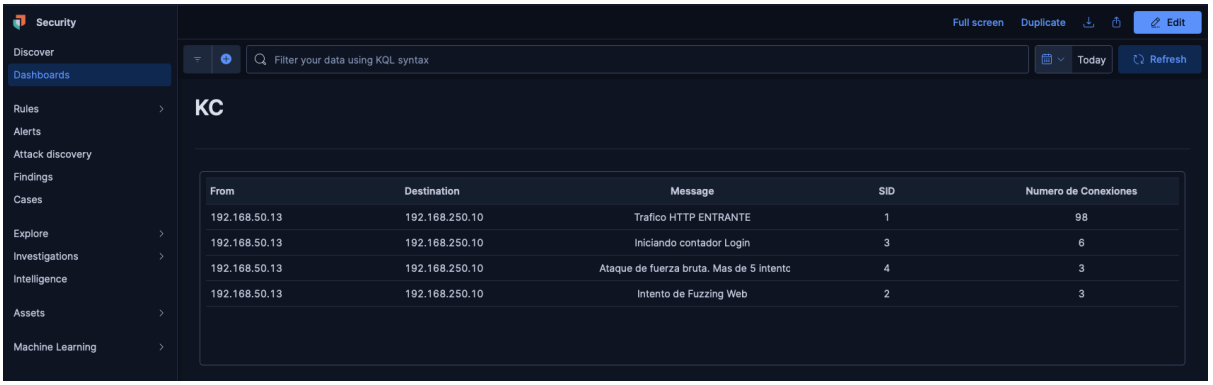


Dashboards y visualización

Se creó un **dashboard personalizado** en Kibana para representar visualmente los eventos más relevantes.
Entre las métricas configuradas destacan:

- El conteo total de alertas generadas por Suricata.
- Los **Top 10** de direcciones IP origen y destino.
- La evolución temporal de eventos por firma de detección.

Estas visualizaciones permiten **correlacionar actividades** entre las distintas subredes, detectar patrones de ataque y evaluar la efectividad de las reglas definidas en el IDS y en el firewall.



Resultados y conclusiones

Gracias a la integración del stack **Elastic** + **Suricata** + **pfSense**, el laboratorio permite:

- Detectar y analizar incidentes en tiempo real.
- Centralizar la información de seguridad de todas las subredes.
- Observar la interacción de los atacantes con el honeypot y correlacionarla con alertas del IDS.
- Disponer de una visión global del entorno mediante dashboards dinámicos.

En conjunto, este despliegue constituye un **entorno Blue Team funcional y educativo**, ideal para comprender la relación entre los distintos componentes defensivos de una infraestructura moderna.

Este laboratorio me ha permitido comprender en profundidad el funcionamiento de un **firewall stateful** y la importancia que tiene la **jerarquía en el orden de las reglas** para un control efectivo del tráfico.
Asimismo, me ha ayudado a **valorar la relevancia de una buena configuración de políticas de seguridad** y a entender cómo la **correlación entre los eventos generados por el firewall, el IDS y el SIEM** resulta fundamental para la detección y análisis de incidentes dentro de una red corporativa.