

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.

```
FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)
pfSense - Netgate Device ID: 3d8e396099ba79e3db65
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.203/24
                v6/DHCP6: 2a0c:5a81:bb11:d100:20c:29ff:fe90:a39f/64
LAN (lan)      -> em1      -> v4: 192.168.100.1/24
DMZ (opt1)     -> em2      -> v4: 192.168.200.1/24
DMZ2 (opt2)    -> em3      -> v4: 192.168.250.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell
```

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.

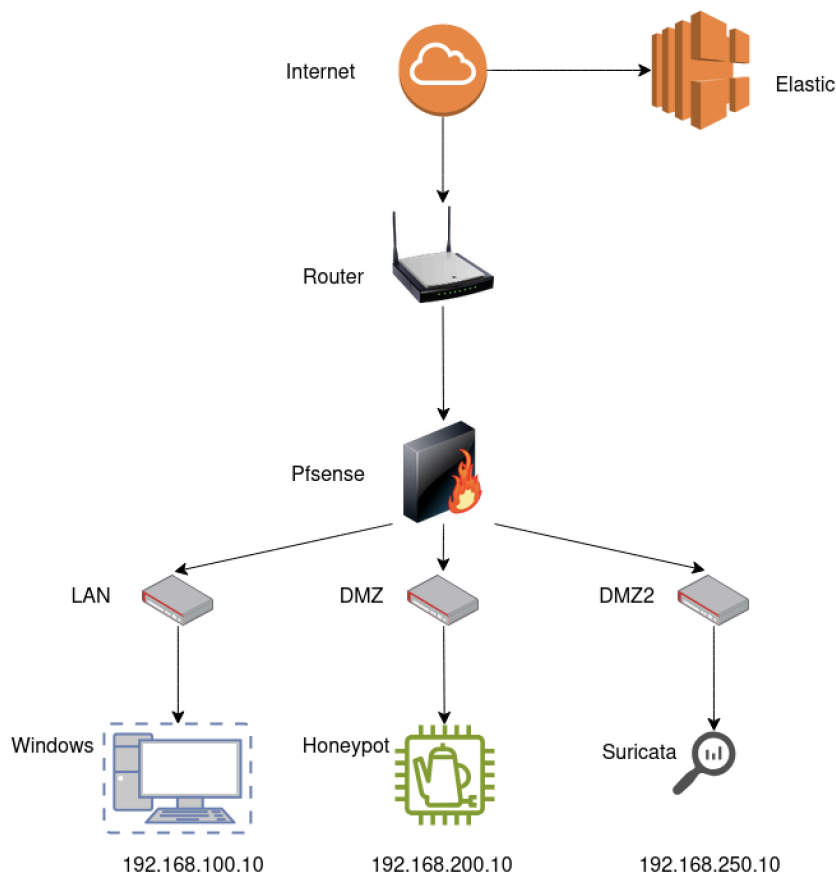
Gracias a esta integración, es posible centralizar los registros de eventos y detectar anomalías o patrones de ataque dentro de las diferentes subredes.

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**:

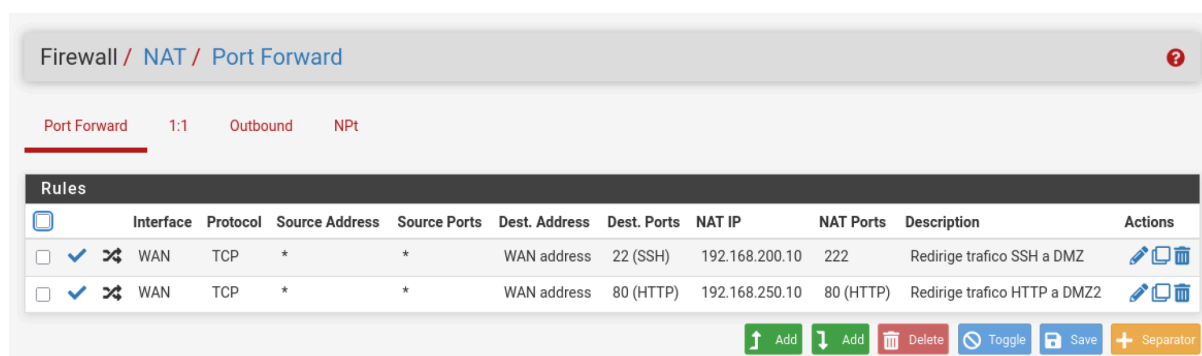
- **Tráfico HTTP (puerto 80):** redirigido desde la interfaz WAN hacia la dirección IP **192.168.250.10** (servidor Apache en la DMZ2).

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.




































Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	WAN address	*	192.168.200.10	222	*	none		Permite trafico a cowrie	     
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	192.168.100.10	*	192.168.200.10	22 (SSH)	*	none		Permite acceso por SSH desde LAN	     
<input type="checkbox"/>	✗ 0/1 KiB	IPv4 *	DMZ subnets	*	LAN subnets	*	*	none		Bloquea todo el trafico hacia LAN	    
<input type="checkbox"/>	✗ 0/0 B	IPv4 *	DMZ subnets	*	DMZ2 subnets	*	*	none		Bloquea todo el trafico hacia DMZ2	    
<input type="checkbox"/>	✓ 7/84 KiB	IPv4 UDP	DMZ subnets	*	*	53 (DNS)	*	none		Permite trafico DNS	     
<input type="checkbox"/>	✓ 25/3.90 MiB	IPv4 TCP	DMZ subnets	*	*	webs	*	none		Permite trafico HTTP y HTTPS	     


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.


Floating WAN LAN DMZ DMZ2


Rules (Drag to Change Order)


<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	 0/0 B	IPv4 TCP	WAN address	*	192.168.250.10	80 (HTTP)	*	none		Permite trafico HTTP desde WAN	     
<input type="checkbox"/>	 0/1020 B	IPv4 *	DMZ2 subnets	*	LAN subnets	*	*	none		Rechaza todo el trafico hacia LAN	     
<input type="checkbox"/>	 0/0 B	IPv4 *	DMZ2 subnets	*	DMZ subnets	*	*	none		Rechaza todo el trafico hacia DMZ	     
<input type="checkbox"/>	 12/328 KiB	IPv4 UDP	*	*	*	53 (DNS)	*	none		Permite trafico DNS	     
<input type="checkbox"/>	 18/13.67 MiB	IPv4 TCP	*	*	*	webs	*	none		Permite trafico HTTP y HTTPS	     


 Add


 Add

 Delete

 Toggle

 Copy

 Save

 Separator

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.

```
dani@kali: /etc/suricata/rules
File: suricata-kc-http.rules
1 #alert tcp any any -> any any (msg:"Tráfico detectado"; sid:1;)
2 #alert tcp any any -> 192.168.50.210 22 (msg:"Tráfico SSH detectado"; sid:2; classtype:attempted-admin;)
3 #alert tcp any any -> any any (msg:"Archivo PDF descargado"; flow:established,to_client; fileext:"pdf"; sid:3; classtype:file-download;)
4
5 alert http any any -> 192.168.250.10 80 (\
6   msg:"Tráfico HTTP ENTRANTE"; \
7   classtype:web-application-activity; sid:001; rev:1;)
8
9 # Genera alerta cuando se hace fuzzing y se hacen 25 conexiones en 30s.
10 alert tcp any any -> 192.168.250.10 80 (\
11   msg:"Intento de Fuzzing Web"; \
12   flow:established,to_server; \
13   threshold:type threshold, track by_src, count 25, seconds 30; \
14   classtype:web-application-attack; sid:002; rev:1;)
15
16 # Genera nueva alerta por cada 60s. Trackeada por src es por IP e inicia el contador en 1.
17 alert http any any -> 192.168.250.10 80 (\
18   msg:"Iniciando contador Login"; \
19   flow:established,to_server; \
20   content:"POST"; http_method; \
21   content:"/login.php"; http_uri; \
22   nocase; \
23   threshold:type limit, track by_src,count 1, seconds 60; \
24   classtype:web-application-activity; sid:003; rev:1;)
25
26 # Genera alerta al superar 5 intentos de esa IP en menos de 60s.
27 alert http any any -> 192.168.250.10 80 (\
28   msg:"Ataque de fuerza bruta. Mas de 5 intentos en 60s"; \
29   flow:established,to_server; \
30   content:"POST"; http_method; \
31   content:"/login.php"; http_uri; \
32   nocase; \
33   threshold:type threshold, track by_src, count 5, seconds 60; \
34   classtype:web-application-attack; sid:004; rev:1;)
35
```

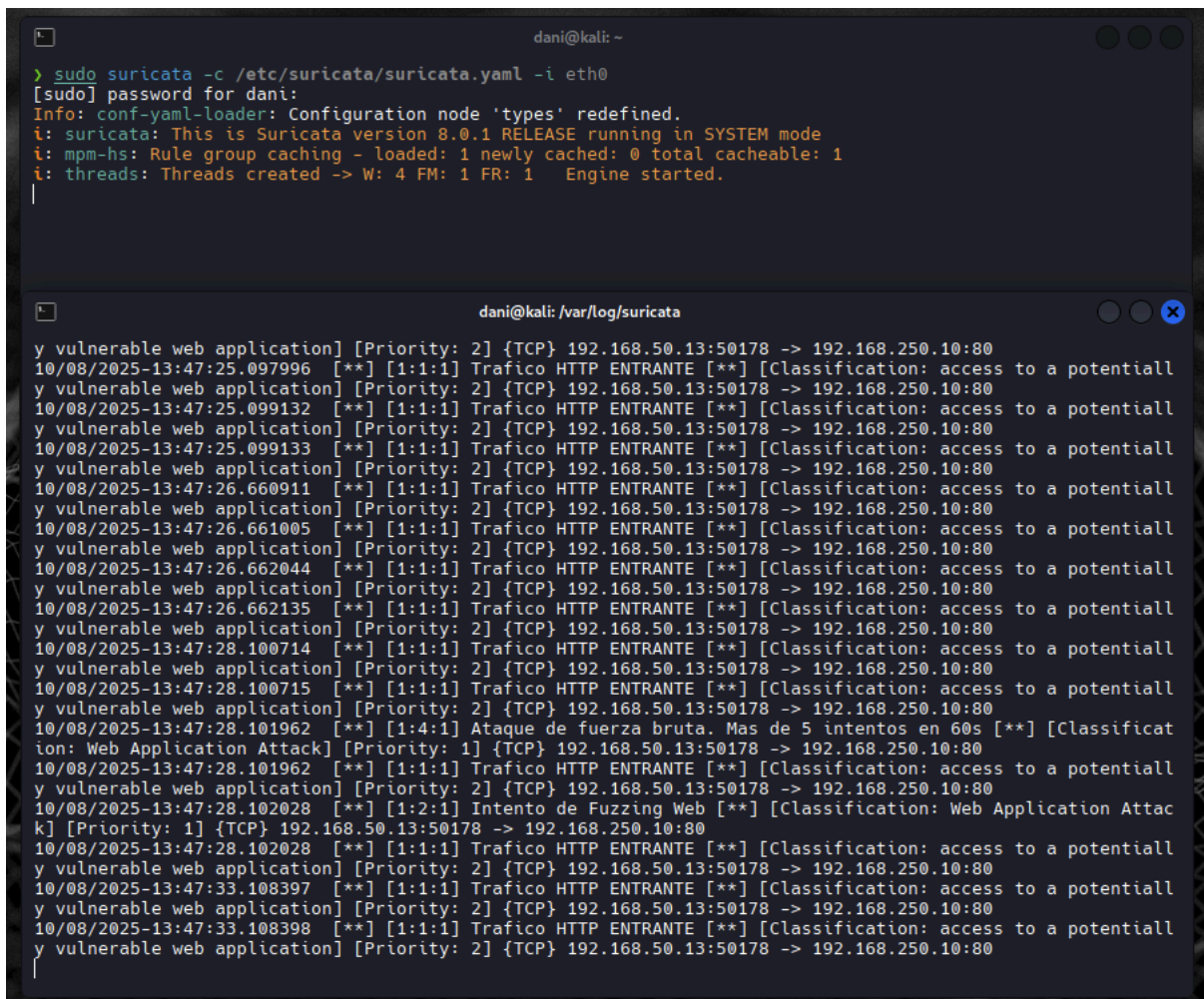
El objetivo de esta implementación es **detectar posibles intentos de ataque contra el servicio web** y registrar dicha actividad para su posterior análisis en el SIEM. Suricata utiliza un conjunto de reglas personalizadas diseñadas para cubrir distintos escenarios de ataque web y actividades sospechosas.

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.



The image shows two terminal windows from a Kali Linux system. The top window shows the command to start Suricata with a specific configuration file and interface, followed by status messages indicating it's running in SYSTEM mode. The bottom window shows a log file with various network events, including HTTP traffic and a brute force attack attempt.

```
dani@kali: ~  
> sudo suricata -c /etc/suricata/suricata.yaml -i eth0  
[sudo] password for dani:  
Info: conf-yaml-loader: Configuration node 'types' redefined.  
i: suricata: This is Suricata version 8.0.1 RELEASE running in SYSTEM mode  
i: mpm-hs: Rule group caching - loaded: 1 newly cached: 0 total cacheable: 1  
i: threads: Threads created -> W: 4 FM: 1 FR: 1 Engine started.  
|  
  
dani@kali: /var/log/suricata  
y vulnerable web application] [Priority: 2] {TCP} 192.168.50.13:50178 -> 192.168.250.10:80  
10/08/2025-13:47:25.097996 [**] [1:1:1] Trafico HTTP ENTRANTE [**] [Classification: access to a potentiall  
y vulnerable web application] [Priority: 2] {TCP} 192.168.50.13:50178 -> 192.168.250.10:80  
10/08/2025-13:47:25.099132 [**] [1:1:1] Trafico HTTP ENTRANTE [**] [Classification: access to a potentiall  
y vulnerable web application] [Priority: 2] {TCP} 192.168.50.13:50178 -> 192.168.250.10:80  
10/08/2025-13:47:25.099133 [**] [1:1:1] Trafico HTTP ENTRANTE [**] [Classification: access to a potentiall  
y vulnerable web application] [Priority: 2] {TCP} 192.168.50.13:50178 -> 192.168.250.10:80  
10/08/2025-13:47:26.660911 [**] [1:1:1] Trafico HTTP ENTRANTE [**] [Classification: access to a potentiall  
y vulnerable web application] [Priority: 2] {TCP} 192.168.50.13:50178 -> 192.168.250.10:80  
10/08/2025-13:47:26.661005 [**] [1:1:1] Trafico HTTP ENTRANTE [**] [Classification: access to a potentiall  
y vulnerable web application] [Priority: 2] {TCP} 192.168.50.13:50178 -> 192.168.250.10:80  
10/08/2025-13:47:26.662044 [**] [1:1:1] Trafico HTTP ENTRANTE [**] [Classification: access to a potentiall  
y vulnerable web application] [Priority: 2] {TCP} 192.168.50.13:50178 -> 192.168.250.10:80  
10/08/2025-13:47:26.662135 [**] [1:1:1] Trafico HTTP ENTRANTE [**] [Classification: access to a potentiall  
y vulnerable web application] [Priority: 2] {TCP} 192.168.50.13:50178 -> 192.168.250.10:80  
10/08/2025-13:47:28.100714 [**] [1:1:1] Trafico HTTP ENTRANTE [**] [Classification: access to a potentiall  
y vulnerable web application] [Priority: 2] {TCP} 192.168.50.13:50178 -> 192.168.250.10:80  
10/08/2025-13:47:28.100715 [**] [1:1:1] Trafico HTTP ENTRANTE [**] [Classification: access to a potentiall  
y vulnerable web application] [Priority: 2] {TCP} 192.168.50.13:50178 -> 192.168.250.10:80  
10/08/2025-13:47:28.101962 [**] [1:4:1] Ataque de fuerza bruta. Mas de 5 intentos en 60s [**] [Classificat  
ion: Web Application Attack] [Priority: 1] {TCP} 192.168.50.13:50178 -> 192.168.250.10:80  
10/08/2025-13:47:28.101962 [**] [1:1:1] Trafico HTTP ENTRANTE [**] [Classification: access to a potentiall  
y vulnerable web application] [Priority: 2] {TCP} 192.168.50.13:50178 -> 192.168.250.10:80  
10/08/2025-13:47:28.102028 [**] [1:2:1] Intento de Fuzzing Web [**] [Classification: Web Application Attac  
k] [Priority: 1] {TCP} 192.168.50.13:50178 -> 192.168.250.10:80  
10/08/2025-13:47:28.102028 [**] [1:1:1] Trafico HTTP ENTRANTE [**] [Classification: access to a potentiall  
y vulnerable web application] [Priority: 2] {TCP} 192.168.50.13:50178 -> 192.168.250.10:80  
10/08/2025-13:47:33.108397 [**] [1:1:1] Trafico HTTP ENTRANTE [**] [Classification: access to a potentiall  
y vulnerable web application] [Priority: 2] {TCP} 192.168.50.13:50178 -> 192.168.250.10:80  
10/08/2025-13:47:33.108398 [**] [1:1:1] Trafico HTTP ENTRANTE [**] [Classification: access to a potentiall  
y vulnerable web application] [Priority: 2] {TCP} 192.168.50.13:50178 -> 192.168.250.10:80
```

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

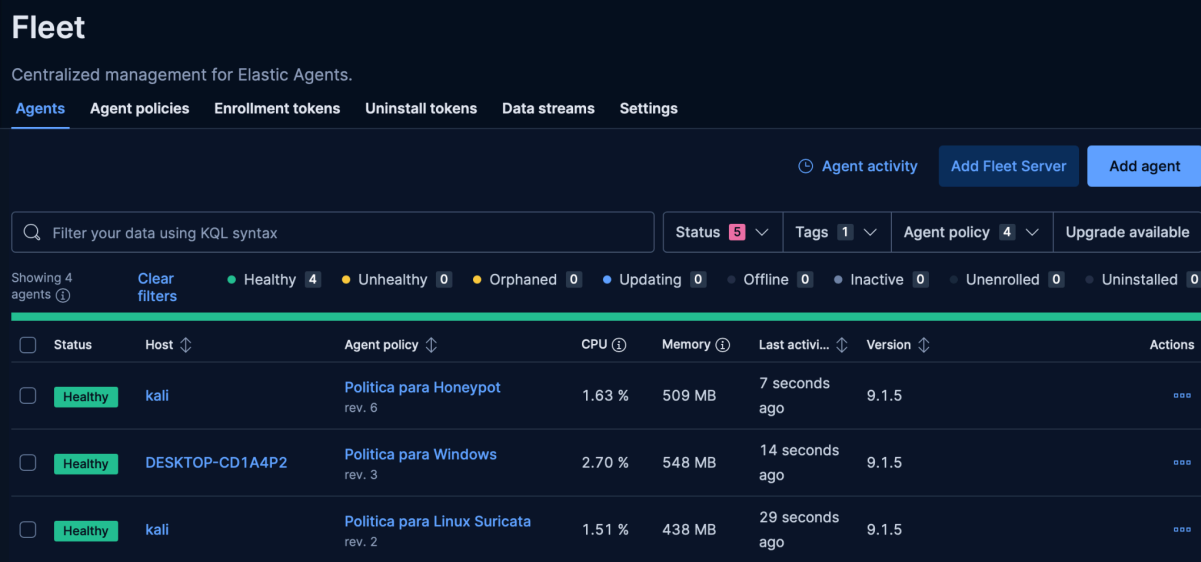
La correcta configuración de Suricata permite:

- **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.



The screenshot shows the Kibana Fleet management interface. At the top, there's a header with the title 'Fleet' and a subtitle 'Centralized management for Elastic Agents.' Below this is a navigation bar with links: 'Agents', 'Agent policies', 'Enrollment tokens', 'Uninstall tokens', 'Data streams', and 'Settings'. The 'Agents' link is active. On the right side of the header, there are buttons for 'Agent activity', 'Add Fleet Server', and 'Add agent'. Below the header is a search bar with the placeholder 'Filter your data using KQL syntax'. To the right of the search bar are filters for 'Status' (5), 'Tags' (1), 'Agent policy' (4), and 'Upgrade available'. Below these filters is a status bar showing counts for various agent states: Healthy (4), Unhealthy (0), Orphaned (0), Updating (0), Offline (0), Inactive (0), Unenrolled (0), and Uninstalled (0). The main part of the interface is a table with columns: Status, Host, Agent policy, CPU, Memory, Last activi..., Version, and Actions. The table contains three rows of agents, all with a 'Healthy' status. The first row is for a host named 'kali' with policy 'Política para Honeypot', CPU usage of 1.63%, and memory of 509 MB. The second row is for a host named 'DESKTOP-CD1A4P2' with policy 'Política para Windows', CPU usage of 2.70%, and memory of 548 MB. The third row is for a host named 'kali' with policy 'Política para Linux Suricata', CPU usage of 1.51%, and memory of 438 MB.

Status	Host	Agent policy	CPU	Memory	Last activi...	Version	Actions
Healthy	kali	Política para Honeypot rev. 6	1.63 %	509 MB	7 seconds ago	9.1.5	...
Healthy	DESKTOP-CD1A4P2	Política para Windows rev. 3	2.70 %	548 MB	14 seconds ago	9.1.5	...
Healthy	kali	Política para Linux Suricata rev. 2	1.51 %	438 MB	29 seconds ago	9.1.5	...

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.

We've added new privileges that let you define more granularly who can view or edit Fleet agents, policies, and settings. [Learn more.](#)

Fleet

Centralized management for Elastic Agents.

Agents **Agent policies** Enrollment tokens Uninstall tokens Data streams Settings

Filter your data using KQL syntax Reload Create agent policy

Name ↕	Last updated on ↓	Unprivileged / Privileged	Integrations	Actions
Politica para Honeygot rev. 6	Oct 10, 2025	0 / 1 (1)	2	...
Politica para Windows rev. 3	Oct 07, 2025	0 / 1 (1)	2	...
Politica para Linux Suricata rev. 2	Oct 07, 2025	0 / 1 (1)	2	...
Elastic Cloud agent policy rev. 4 Default agent policy for agents hosted on Elastic Cloud	Oct 07, 2025	1 / 0 (1)	2	...

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.

@timestamp	source.ip	destination.ip	suricata.eve.alert.signature_id	suricata.eve.alert.signature	log.file.path
Oct 8, 2025 @ 19:47:33.188	192.168.58.13	192.168.258.18	1	Trafico HTTP ENTRANTE	/var/log/suricata/eve.json
Oct 8, 2025 @ 19:47:33.188	192.168.58.13	192.168.258.18	1	Trafico HTTP ENTRANTE	/var/log/suricata/eve.json
Oct 8, 2025 @ 19:47:28.182	192.168.58.13	192.168.258.18	1	Trafico HTTP ENTRANTE	/var/log/suricata/eve.json
Oct 8, 2025 @ 19:47:28.182	192.168.58.13	192.168.258.18	2	Intento de Fuzzing Web	/var/log/suricata/eve.json
Oct 8, 2025 @ 19:47:28.181	192.168.58.13	192.168.258.18	1	Trafico HTTP ENTRANTE	/var/log/suricata/eve.json
Oct 8, 2025 @ 19:47:28.181	192.168.58.13	192.168.258.18	4	Ataque de fuerza bruta. Mas de 5 intentos en 68s	/var/log/suricata/eve.json
Oct 8, 2025 @ 19:47:28.188	192.168.58.13	192.168.258.18	1	Trafico HTTP ENTRANTE	/var/log/suricata/eve.json
Oct 8, 2025 @ 19:47:28.188	192.168.58.13	192.168.258.18	1	Trafico HTTP ENTRANTE	/var/log/suricata/eve.json
Oct 8, 2025 @ 19:47:26.662	192.168.58.13	192.168.258.18	1	Trafico HTTP ENTRANTE	/var/log/suricata/eve.json
Oct 8, 2025 @ 19:47:26.662	192.168.58.13	192.168.258.18	1	Trafico HTTP ENTRANTE	/var/log/suricata/eve.json
Oct 8, 2025 @ 19:47:26.661	192.168.58.13	192.168.258.18	1	Trafico HTTP ENTRANTE	/var/log/suricata/eve.json
Oct 8, 2025 @ 19:47:26.661	192.168.58.13	192.168.258.18	1	Trafico HTTP ENTRANTE	/var/log/suricata/eve.json
Oct 8, 2025 @ 19:47:26.666	192.168.58.13	192.168.258.18	1	Trafico HTTP ENTRANTE	/var/log/suricata/eve.json
Oct 8, 2025 @ 19:47:25.899	192.168.58.13	192.168.258.18	1	Trafico HTTP ENTRANTE	/var/log/suricata/eve.json
Oct 8, 2025 @ 19:47:25.899	192.168.58.13	192.168.258.18	1	Trafico HTTP ENTRANTE	/var/log/suricata/eve.json
Oct 8, 2025 @ 19:47:25.897	192.168.58.13	192.168.258.18	1	Trafico HTTP ENTRANTE	/var/log/suricata/eve.json
Oct 8, 2025 @ 19:47:25.897	192.168.58.13	192.168.258.18	1	Trafico HTTP ENTRANTE	/var/log/suricata/eve.json
Oct 8, 2025 @ 19:47:22.848	192.168.58.13	192.168.258.18	1	Trafico HTTP ENTRANTE	/var/log/suricata/eve.json
Oct 8, 2025 @ 19:47:22.848	192.168.58.13	192.168.258.18	1	Trafico HTTP ENTRANTE	/var/log/suricata/eve.json
Oct 8, 2025 @ 19:47:22.839	192.168.58.13	192.168.258.18	1	Trafico HTTP ENTRANTE	/var/log/suricata/eve.json
Oct 8, 2025 @ 19:47:22.839	192.168.58.13	192.168.258.18	1	Trafico HTTP ENTRANTE	/var/log/suricata/eve.json
Oct 8, 2025 @ 19:47:28.586	192.168.58.13	192.168.258.18	1	Trafico HTTP ENTRANTE	/var/log/suricata/eve.json
Oct 8, 2025 @ 19:47:28.586	192.168.58.13	192.168.258.18	1	Trafico HTTP ENTRANTE	/var/log/suricata/eve.json
Oct 8, 2025 @ 19:47:28.583	192.168.58.13	192.168.258.18	3	Iniciando contador Login	/var/log/suricata/eve.json
Oct 8, 2025 @ 19:47:28.583	192.168.58.13	192.168.258.18	1	Trafico HTTP ENTRANTE	/var/log/suricata/eve.json
Oct 8, 2025 @ 19:47:28.522	192.168.58.13	192.168.258.18	1	Trafico HTTP ENTRANTE	/var/log/suricata/eve.json
Oct 8, 2025 @ 19:47:28.522	192.168.58.13	192.168.258.18	1	Trafico HTTP ENTRANTE	/var/log/suricata/eve.json
Oct 8, 2025 @ 19:47:15.515	192.168.58.13	192.168.258.18	1	Trafico HTTP ENTRANTE	/var/log/suricata/eve.json
Oct 8, 2025 @ 19:47:15.515	192.168.58.13	192.168.258.18	1	Trafico HTTP ENTRANTE	/var/log/suricata/eve.json
Oct 8, 2025 @ 18:45:83.319	192.168.58.13	192.168.258.18	1	Trafico HTTP ENTRANTE	/var/log/suricata/eve.json
Oct 8, 2025 @ 18:45:83.319	192.168.58.13	192.168.258.18	1	Trafico HTTP ENTRANTE	/var/log/suricata/eve.json

- **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.

@timestamp	log.file.path	message
Oct 8, 2025 @ 12:28:29.840	/home/k3p4/honeybot_100	2025-10-08T10:13:31+0000 [HoneyPotSSHTransport, 1, 192.168.58.13] 200: exit
Oct 8, 2025 @ 12:28:29.839	/home/k3p4/honeybot_100	2025-10-08T10:13:28+0000 [HoneyPotSSHTransport, 1, 192.168.58.13] 200: hola
Oct 8, 2025 @ 12:28:29.839	/home/k3p4/honeybot_100	2025-10-08T10:13:25+0000 [HoneyPotSSHTransport, 1, 192.168.58.13] 200: cd ../
Oct 8, 2025 @ 12:28:29.819	/home/k3p4/honeybot_100	2025-10-08T10:13:12+0000 [HoneyPotSSHTransport, 0, 192.168.58.13] 200: exit
Oct 8, 2025 @ 12:28:29.817	/home/k3p4/honeybot_100	2025-10-08T10:13:07+0000 [HoneyPotSSHTransport, 0, 192.168.58.13] 200: f
Oct 8, 2025 @ 12:28:29.817	/home/k3p4/honeybot_100	2025-10-08T10:13:02+0000 [HoneyPotSSHTransport, 0, 192.168.58.13] 200: d
Oct 8, 2025 @ 12:28:29.817	/home/k3p4/honeybot_100	2025-10-08T10:13:02+0000 [HoneyPotSSHTransport, 0, 192.168.58.13] 200: s
Oct 8, 2025 @ 12:28:29.815	/home/k3p4/honeybot_100	2025-10-08T10:12:49+0000 [HoneyPotSSHTransport, 0, 192.168.58.13] 200: tes

- **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.

Selected fields	Popular fields	Available fields
@timestamp	message	@timestamp
host.ip	winlog.event_id	agent.ephemeral_id
winlog.task	winlog.task	agent.id
message	host.name	agent.name
winlog.event_id	host.ip	agent.type
host.name		agent.version
		data_stream.dataset
		data_stream.namespaces
		data_stream.type
		dataset.name
		dataset.namespaces

Documents (173)	Patterns	Field statistics
@timestamp	host.ip	winlog.task
message	winlog.event_id	host.name

Columns	Sort fields
6	1

Document	Timestamp	Host IP	Task	Message	Event ID	Host Name
✓	Oct 10, 2025 @ 16:45:42.053	fe80::bcc8:8233:21c:fe79:192.168.100.10	Ciclo de vida del motor	El estado del motor ha cambiado de No...	400	desktop-cd1a4p2
✓	Oct 10, 2025 @ 16:45:42.020	fe80::bcc8:8233:21c:fe79:192.168.100.10	Ciclo de vida del proveedor	El proveedor "Variable" está Started. ...	600	desktop-cd1a4p2
✓	Oct 10, 2025 @ 16:45:42.020	fe80::bcc8:8233:21c:fe79:192.168.100.10	Ciclo de vida del proveedor	El proveedor "Function" está Started. ...	600	desktop-cd1a4p2
✓	Oct 10, 2025 @ 16:45:42.020	fe80::bcc8:8233:21c:fe79:192.168.100.10	Ciclo de vida del proveedor	El proveedor "FileSystem" está Started. ...	600	desktop-cd1a4p2
✓	Oct 10, 2025 @ 16:45:42.008	fe80::bcc8:8233:21c:fe79:192.168.100.10	Ciclo de vida del proveedor	El proveedor "Environment" está Started. ...	600	desktop-cd1a4p2
✓	Oct 10, 2025 @ 16:45:42.008	fe80::bcc8:8233:21c:fe79:192.168.100.10	Ciclo de vida del proveedor	El proveedor "Alias" está Started. ...	600	desktop-cd1a4p2
✓	Oct 10, 2025 @ 16:45:42.008	fe80::bcc8:8233:21c:fe79:192.168.100.10	Ciclo de vida del proveedor	El proveedor "Registry" está Started. ...	600	desktop-cd1a4p2
✓	Oct 10, 2025 @ 16:42:12.855	fe80::bcc8:8233:21c:fe79:192.168.100.10	Ejecutando canalización	CommandInvocation(Add-Type): "Add-Type"...	4103	desktop-cd1a4p2
✓	Oct 10, 2025 @ 16:42:12.851	fe80::bcc8:8233:21c:fe79:192.168.100.10	Ejecutando canalización	CommandInvocation(Add-Type): "Add-Type"...	4103	desktop-cd1a4p2
✓	Oct 10, 2025 @ 16:42:12.844	fe80::bcc8:8233:21c:fe79:192.168.100.10	Detalles de ejecución de la canalización	Detalles de ejecución de canalización ...	800	desktop-cd1a4p2
✓	Oct 10, 2025 @ 16:42:12.844	fe80::bcc8:8233:21c:fe79:192.168.100.10	Detalles de ejecución de la canalización	Detalles de ejecución de canalización ...	800	desktop-cd1a4p2

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.

The screenshot shows a Security dashboard with a sidebar menu on the left containing options like Discover, Dashboards, Rules, Alerts, Attack discovery, Findings, Cases, Explore, Investigations, Intelligence, Assets, and Machine Learning. The main area displays a table titled 'KC' with the following data:

From	Destination	Message	SID	Numero de Conexiones
192.168.50.13	192.168.250.10	Trafico HTTP ENTRANTE	1	98
192.168.50.13	192.168.250.10	Iniciando contador Login	3	6
192.168.50.13	192.168.250.10	Ataque de fuerza bruta. Mas de 5 intentc	4	3
192.168.50.13	192.168.250.10	Intento de Fuzzing Web	2	3

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.